Web Server Seizure and Live Acquisition: A Legally Compliant Forensic Framework for Indonesia

Irwan Hariyanto[1], Yudi Prayudi[2], Rimba Whidiana Ciptasari[3]
School of Computing, Telkom University, Bandung, Indonesia[1,3]
School of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia[2]

***Abstract*—The proliferation of cybercrime activities, particularly those leveraging web servers for illicit purposes such as distributing hoaxes, hosting illegal online gambling, and spreading malware, underscores a pressing demand for a standardized digital forensic framework. Existing methodologies, like simple IP blocking, have proven insufficient in guaranteeing the integrity and admissibility of digital evidence in legal proceedings. This research introduces a comprehensive seizure and acquisition framework specifically engineered to manage digital evidence from both on-premise and cloud-based web servers. A core emphasis of this framework is live acquisition to preserve volatile data and ensure minimal service disruption. The framework systematically addresses critical challenges by focusing on legal authorization, precise server type identification and technical preparation, judicious forensic tool selection, rigorous evidence integrity validation through hashing, diligent Chain of Custody (CoC) documentation, and secure data storage. Tested through simulations of on-premise and cloud server seizures, the framework demonstrated its capacity to uphold evidence integrity and legal compliance. While robust, Subject Matter Expert (SME) validation indicated areas for optimization, particularly in cloud-native contexts and the automation of Chain of Custody documentation. This study marks a pivotal advancement towards standardizing web server seizure procedures, thereby ensuring that digital evidence remains valid, intact, and legally admissible in court.**

***Keywords*—Digital forensics; web server seizure; live acquisition; evidence integrity; chain of custody**

I. Introduction

As cybercrime continues to rise, the need for effective digital forensic practices is paramount [1]. The Indonesian legal framework is still adapting to the complexities of digital evidence, which presents unique challenges for law enforcement agencies [2]. The lack of standardized procedures for seizing and acquiring digital evidence from web servers further complicates the investigation process, making it essential to develop a comprehensive framework that addresses these issues [3].

Database breaches, website defacement, cyber intrusions, and phishing attacks commonly occur on web servers [1]. These incidents require forensic investigation.

In the cyber context, however, the term encompasses a more nuanced set of actions. It can refer to the physical seizure of server hardware. However, more frequently, it involves the logical acquisition or forensic duplication of digital data from systems that cannot be physically moved or shut down due to operational risks [4]. This distinction is critical, as the chosen method —physical or logical —depends heavily on the server's environment, its role in ongoing business operations, and the legal authority granted to investigators [5].

One example is a case of hacking and defacing a government website in Indonesia [6]. This case involved the hacking of several government websites in Indonesia, where attackers altered the front page with political or ideological messages. A digital forensics team seized the web server for further analysis, including identifying the digital footprint of the hackers, the hacking methods used, and log data showing unauthorized activity [7], [8]. The forensics process collects data from server logs, caches, and system configurations to check for exploited vulnerabilities [9].

These case examples show that web server seizure is challenging in both VPS and cloud environments. A standard framework is required to ensure integrity, validity, and courtroom admissibility [10], [11]. A digital forensics process model provides the required steps, inputs, and outputs for successful investigation [12].

Evidence handling in cyber forensics includes preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation [5]. As cyber cases in Indonesia increase, investigators still lack a standardized legal-forensic reference for seizure and acquisition [13]. This study proposes a web server seizure framework that is technically robust and legally compliant for Indonesian law enforcement needs.

The framework developed in this study directly contributes to the following strategic aspects:

- Strengthening the Validity of Digital Evidence through Standardization of Procedures: This framework presents a structured and well-documented workflow in seizing and acquiring evidence from web servers.
- Support for Strengthening the Chain of Custody: One of the important contributions of this framework is to provide technical and administrative guidelines for building a strong chain of custody.
- Ensuring Legal Compliance in Indonesia and Supporting International Applicability: This framework is designed to align with the legal principles applicable in Indonesia, especially regarding digital seizure procedures, electronic evidence provisions, and legal restrictions.
- Foundation for the Establishment of SOP for Digital Forensic Institutions: For law enforcement agencies,

digital forensic laboratories, and other agencies involved in cyber investigations, this framework can be a basis for compiling, training investigators, and strengthening institutional capacity in digital forensics.

- Foundation for Developing Standard Operating Procedures in Digital Forensics: By bringing a relatively new topic for web server seizures in the context of cloud and hybrid—this research broadens the insights and academic literature in Indonesia and globally.

A. Operational Definition of Key Terms

To avoid ambiguity, this study distinguishes the following terms and applies them consistently in all sections:

- Seizure: A legally authorized act to control digital evidence sources (physical or logical) under applicable procedures (KUHAP and related regulations).
- Collection: Initial identification and retrieval of potentially relevant artifacts from a running or non-running system.
- Acquisition: A forensic process to create a reliable copy/image of selected data while preserving evidentiary integrity.
- Live Acquisition: Acquisition from an active system without shutdown to preserve volatile artifacts and maintain service continuity.

The remainder of this study is organized as follows. Section II reviews related research. Section III presents the framework development method. Section IV evaluates the framework through simulations and SME validation. Section V discusses findings, feasibility, and refinement direction, and Section VI concludes the study.

II. Related Research

A. Web Server Acquisition

Web server acquisition is a crucial step in the digital forensics process, which aims to collect all relevant data from the server without changing its contents. Research by Pedapudi & Vadlamani [14] directly links data with formal seizure documentation through the proposed "Data Acquisition-based Seizure Record Framework." In this context, "seizure" is defined as a process that must be systematically recorded and documented [15].

Thankaraja Raja Sree et al. [16] demonstrated that data acquisition from web servers necessitates tools capable of handling dynamic and volatile data that is constantly updated. This [17] also emphasized the importance of using specialized tools to maintain data integrity during acquisition, such as using secure hashing on the collected data to ensure that no changes occur.

Liu et al. [18] also discuss remote acquisition methods that allow investigators to perform acquisitions remotely. While this method is helpful in the context of cloud forensics, when applied to a local web server, it faces challenges in terms of legality and network security.

Digital seizure is a crucial step in digital forensics for IoT, involving the identification and acquisition of digital evidence from diverse and interconnected devices. Its main strength lies in preserving volatile and distributed data [19], which is essential for reliable forensic analysis and legal proceedings. However, the process faces significant challenges due to the heterogeneity of IoT devices, a lack of standardization, network limitations, and the vast volume of data, which can hinder the collection of timely and complete evidence [20], [13]. Thus, while digital seizure is vital for IoT forensics, its effectiveness depends on the development of standardized frameworks and adaptive tools to address these unique challenges.

Previous studies have proposed various digital forensics models that address general procedures for investigating digital evidence, such as the Digital Forensics Investigation Framework (DFIF) [21].

Cloud forensics research [22], [23], [24] emphasizes remote acquisition and live capture without service interruption. However, these approaches still lack specific guidance for VPS seizure in the Indonesian context. In this study, "web server" seizure is not limited to HTTP/HTTPS servers but includes any server entity containing relevant evidence [25].

The web servers commonly used are NGINX and Apache. On the other hand, with time, other web servers have also become widely used, such as Microsoft IIS, lighttpd, and LiteSpeed. These types of web servers can be categorized as web servers that can be seized [26].

Data crucial for web server forensic acquisition is categorized into Volatile Data (e.g., RAM contents, running processes, network connections, active user sessions, system time, open files, command history, and clipboard contents) and Non-Volatile Data (e.g., system files, server configurations, log files, databases, web applications, user data, and backup files) [27]. These data points serve as potential evidentiary artifacts. Consequently, securing and maintaining the integrity of digital evidence from web servers is critical for effective case investigation and prosecution, particularly given increasingly stringent international digital evidence laws [28].

The data mentioned above can be potential artifacts that can be used as evidence in conducting the seizure of the web server. In Indonesia, there are no guidelines governing the seizure of web servers, which poses significant technical and legal challenges for investigators [29]. Success in securing and maintaining the integrity of digital evidence from web servers is critical to investigating and prosecuting cases, especially in the context of increasingly stringent international laws regarding digital evidence [30].

Although previous research has provided a good foundation for collecting and acquiring digital evidence, there is no specific framework addressing the seizure of web servers as evidence [31], especially in the context of applicable law in Indonesia. Many current solutions, such as remote acquisition [32], do not consider the technical uniqueness and legal challenges associated with direct seizure. This creates a risk that the evidence obtained will not be admissible in court or that the data acquisition process will be flawed, resulting in loss of data integrity and chain of custody [33].

B. Digital Forensic Methodology for Incidents

Karen Ken [34] (The Guide to Integrating Forensic Techniques into Incident Response (NIST Special Publication 800-86)) describes the general framework of the NIST standard, which consists of Collection, Examination, Analysis, and Reporting. However, the collection stage does not explain how to perform a seizure on a web server. Based on Fig. 1, at the Collection stage, there are the following details:

- Identifying possible data sources.
- Acquiring data: At this stage, there are further details as follows:
  - Planning data acquisition.
  - Acquiring the data.
  - Verifying data integrity.
- Considering Incident Response.

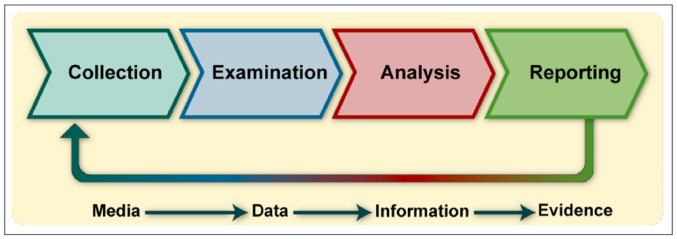

Fig. 1. NIST Digital Forensics Framework.

Seizing a web server in the context of digital forensics investigations is a complex process involving infrastructure that often functions dynamically [35]. Malik et al. [36] emphasize the considerable obstacles associated with web server seizures, notably the potential for operational downtime that may impede company activities and the threat of losing essential volatile data if the server is deactivated during the seizure process [37]. Many contemporary investigations are using a live forensics strategy, wherein the operational web server continues to function while digital evidence is gathered [38]. This method enables investigators to gather evidence without disabling the server, although it also increases the potential of data contamination.

C. Digital Forensics Seizure

Research by Kuntze et al. [39] discusses the process of seizure from a legal context in Germany and the United States, with a focus on digital data. In this study, "seizure" no longer always means the physical removal of hardware, but more often refers to the process of imaging hard drives or other storage media. The primary concern is that modern seizure practices, which involve creating full images, often conflict with fundamental laws.

From a different perspective, research by Nortje & Myburgh [40] examines "seizure" from the perspective of its legal preconditions, namely the obstacles in drafting search and seizure warrants for digital evidence in South Africa. This research does not focus on the technical act of seizure itself, but rather on the legal process that authorizes it. "Seizure" is viewed as a legal action whose validity is highly dependent on the completeness and accuracy of the warrant application submitted by the forensic investigator.

Research by Pedapudi & Vadlamani [14] directly links data with formal seizure documentation through the proposed "Data Acquisition-based Seizure Record Framework." In this context, "seizure" is defined as a process that must be systematically recorded and documented. The proposed framework aims to standardize the recording of every detail during the digital evidence acquisition process.

Meanwhile, research by Thealma & Ruldeviyani [2] discusses the ethical aspects of data handling in digital forensic investigations in Indonesia, especially after the enactment of the Personal Data Protection Law (PDP Law). Although it does not directly define "seizure," this research implicitly highlights that the process of seizing digital evidence carries significant ethical and legal consequences, as such evidence is likely to contain sensitive personal information or data.

These four literature studies collectively provide a 360-degree view of the seizure process in digital forensics. They show that the framework must not focus only on technical aspects, but must also be legally accountable, ethically grounded, and well documented to preserve evidentiary integrity from start to finish.

D. Implementation of Framework in Daily Practice

Forensic investigators and examiners utilize established frameworks in their daily practice to verify that the acquisition and analysis of digital evidence adhere to industry standards [13]. Singh K [41] asserted that a well-designed framework can reduce errors in the investigative process and guarantee the admissibility of digital evidence in court. The execution of this framework requires specialized training for investigators to comprehend the technical procedures involved in seizing web servers, particularly in surroundings with complex infrastructure [42].

Frameworks such as the Digital Forensics Investigation Framework (DFIF) have been successfully utilized in cybercrime investigations. Nonetheless, the implementation of forensic frameworks must persistently adapt to advancing technologies, including cloud environments and hybrid web servers, to guarantee the proper securing and validation of digital evidence [21], [22], [23].

E. Existing Seizure Procedures

Fig. 2 illustrates that the seizure procedure is a critical component of the criminal case management process in Indonesia, as evidenced by the information obtained from the official portal of the Metro District Court [43]. The Criminal Procedure Code, also known as KUHAP (Kitab Undang-Undang Hukum Acara Pidana), governs the procedures for evidence seizure in the Indonesian legal system. The mechanisms for search, seizure, and the management of evidence in criminal investigations, including digital evidence, are regulated by this law.

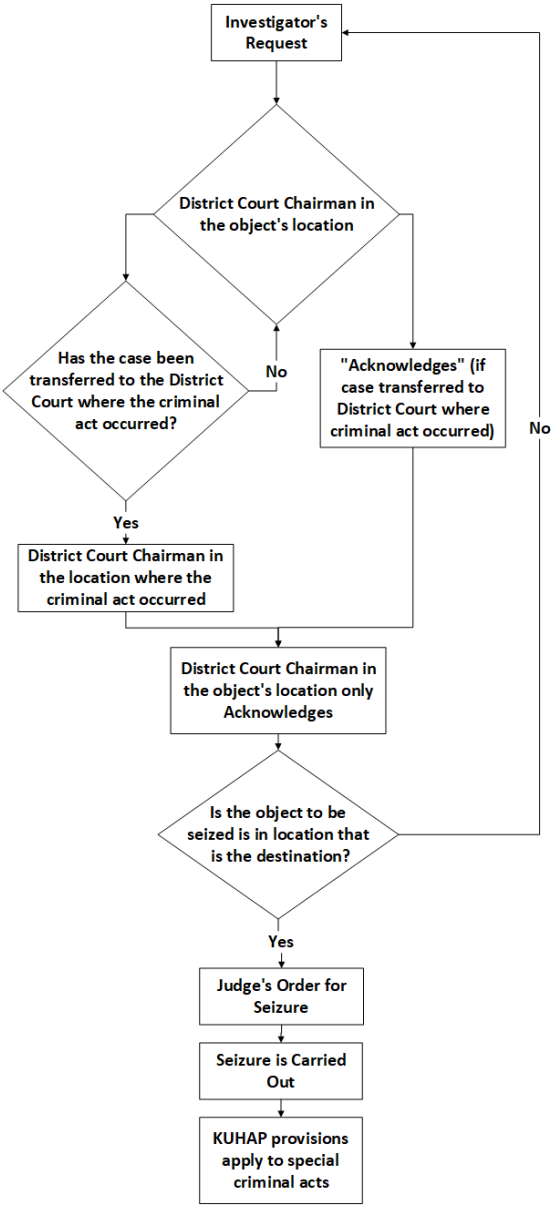

Fig. 2. Current seizure procedure in Indonesia.

The phases of digital evidence seizure and validation are illustrated in Fig. 2, which provides an overview of the framework components. The legal validity and data integrity of each phase are guaranteed by the inclusion of specific technical and procedural components. This procedure thoroughly regulates the legitimate seizure of evidence or assets that are pertinent to a criminal offense.

III. Framework Development

This section outlines the stages used to develop the web server seizure framework, starting from literature review and expert interviews, followed by prototype implementation through cloud and VPS simulations.

Fig. 3 illustrates the sequential flow of the research methodology, which combines literature review, expert interviews, and iterative prototype testing. Each phase is structured to

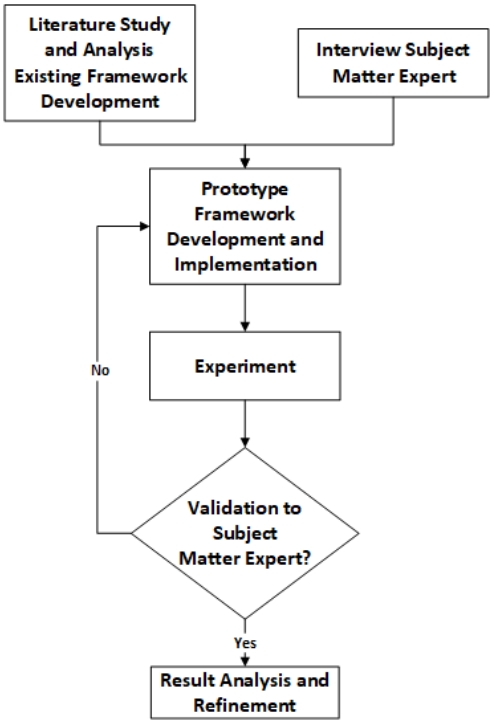

Fig. 3. Phases of research for the development of a proposed seizure framework.

ensure that the developed framework is both legally valid and technically reliable, with validation and refinement stages to improve its applicability.

- Literature Study and Analysis of Existing Frameworks: This activity involves a systematic review of academic and professional literature to explore existing digital forensic frameworks. The objective is to understand their approach to seizing and acquiring evidence from web servers, particularly in cloud and VPS environments. The study also includes a critical analysis of the limitations and shortcomings of these frameworks, especially in maintaining volatile data and ensuring data integrity during live acquisition.
- Interview Subject Matter Expert: done with the goal of asking about the framework that has been run by experts when seizing web servers as a comparison material at the literature study stage and analysis of existing frameworks by asking questions to experts by providing framework guidelines as the primary reference, namely from NIST 800-86 [34].
- Prototype Framework Development and Implementation: This refers to the process of constructing an initial version (prototype) of the proposed framework based on the design formulated in earlier stages. The implementation involves applying the framework in controlled simulations using forensic tools and live web servers hosted on cloud or VPS platforms. The goal is to verify the accuracy of each phase of the framework in real-world operational scenarios [44].
- Framework Experimentation: Framework experimen-

tation refers to testing the proposed framework through forensic simulations in semi-realistic investigative conditions [45]. The aim is to evaluate the framework's performance in securing digital evidence during the seizure of a web server. Case scenarios, including DDoS-related seizures or website defacement, were used. Effectiveness was measured using indicators such as data integrity (verified through hashing), preservation of volatile data, and time efficiency. The framework's flexibility was also tested across various cloud and VPS environments.

- Validation to Subject Matter Expert (SME): SME validation is the process of involving digital forensic experts to assess the applicability and reliability of the proposed framework. The validation was conducted through review sessions and field simulations with practitioners and investigators. Experts were asked to evaluate usability, compliance with legal standards, and technical soundness [46].
- Results Analysis and Framework Refinement: This refers to the final analytical phase to assess whether the developed framework meets the research goals. Data from experiments and SME feedback were analyzed to measure the framework's ability to maintain evidence integrity and minimize data loss. Comparative evaluations were made between the proposed and existing traditional approaches.

Table I summarizes the expected output of each phase. Findings from SME interviews and literature review were synthesized to identify key issues (data volatility, integrity, and legal compliance) [47], [48], then used to build the initial framework for VPS and cloud seizure scenarios.

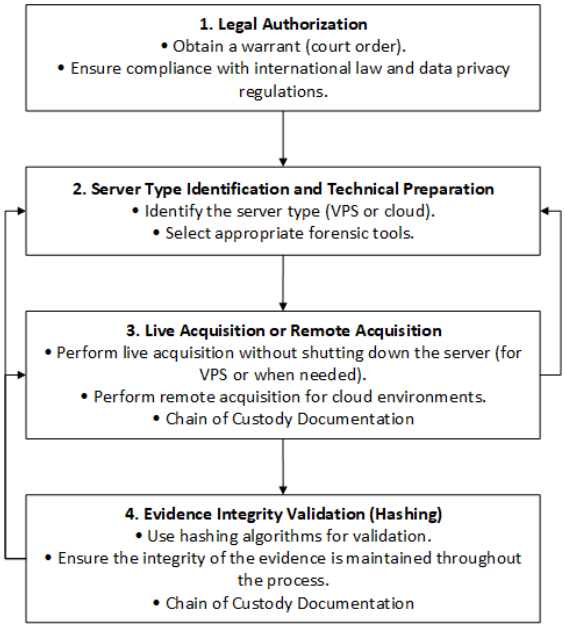

Fig. 4. Proposed framework.

Fig. 4 shows the proposed framework, which is tested through forensic simulation and validated by SMEs to ensure legal compliance, technical feasibility, and operational usability.

- Legal Authorization: Ensure that all seizure actions are preceded by court authorization and comply with applicable laws, including data privacy.
- Server Identification and Technical Preparation: Determine the server type (VPS or cloud), prepare suitable forensic procedures and tools, and document activities to preserve chain of custody (CoC).
- Data Acquisition: Retrieve data through live acquisition without shutting down the server, or remote acquisition in cloud environments, to minimize data loss.
- Validation of Evidence Integrity: Perform hashing to verify that collected evidence remains intact and unchanged.

IV. Framework Evaluation

This section presents the evaluation of the proposed web server seizure framework through simulation-based case studies and expert validation.

A. Dataset

To ensure that the proposed framework is applicable in realistic investigative conditions, a case dataset is required to simulate common cybercrime scenarios. This section describes the dataset used to test the framework, particularly in the context of online gambling and website defacement attacks.

B. Simulation Environment and Reproducibility Setup

To improve reproducibility, this subsection summarizes the technical environment used in both simulations.

- Cloud scenario (Case 1): AWS infrastructure (EC2 and EBS snapshot service), Ubuntu 20.04 LTS (64-bit), Apache 2.4.52, PHP 7.4, MySQL 8.0, remote acquisition via AWS CLI 2.11, and audit trace via CloudTrail.
- VPS scenario (Case 2): Linux-based VPS on VirtualBox 7.0 using Ubuntu 20.04 LTS (64-bit), Apache 2.4.52, PHP 7.4, MySQL 8.0, and acquisition using Oxygen Forensic KeyScout 15.1 and Magnet AXIOM 7.2.
- Integrity mechanism: hash calculation before and after acquisition for critical artifacts (logs, web files, and database exports), using SHA-1 as implemented in the simulation.
- Evidence scope: volatile artifacts (active sessions, running processes, active logs) and non-volatile artifacts (configurations, site files, database dumps, snapshots).
- Documentation output: acquisition command logs, hash logs, timestamps, chain-of-custody forms, and legal authorization records.

The above configuration is intended as a minimum baseline for independent replication. Future studies can expand by testing additional operating systems and multi-region cloud deployments.

TABLE I. RESEARCH PHASES AND EACH-STAGE RESULT OF THE FRAMEWORK DEVELOPMENT

Research phases	Each-stage result
Literature Study and Analysis of Existing Framework Development	A comprehensive review of the existing framework will help define gaps or needs that are not being met by the current solution. - Extended Model of Cybercrime Investigations (EMCI) - Enhanced Digital Investigation Process (EDIP) - Event-Based Digital Forensic Investigation Framework (EBDFI) - Abstract Digital Forensic Model (ADFM) - Cloud Incident Response Framework (CIRF)
Interview Subject Matter Expert	- Detailed 3-Scenario Acquisition Model - Refinement of NIST Collection Stage (ISO 27037 Integration) - Distinction between Collection & Acquisition - Broader Incident Response Lifecycle View - Emphasis on First Response & Contamination Avoidance - Stakeholder Coordination - Additional Security/Preservation Aspects - Legal Foundation - Legality Prerequisite - Technical Identification
Prototype Framework Development and Implementation	Proposed Framework: - Emphasis on legal defensibility (Court-ready, consistent with Indonesian legislation) - Comprehensive (VPS/Cloud, operating system, services, tool preparation) - Fully supports live acquisition (volatile and non-volatile) and remote cloud acquisition. - Hashing (e.g., SHA-1), observed validation, pre/post acquisition
Framework Experimentation	Quantitative and qualitative data regarding the framework's performance, encompassing reports on evidence integrity, efficacy in managing volatile data, and interoperability with current forensic tools.
Subject Matter Expert (SME) Validation	The final, field-validated framework with implementation guidance for users.
Results Analysis and Framework Refinement	The final version of the framework, which has undergone thorough testing and refinement, is now ready for implementation in the field by forensic investigators.

1) Simulation of Case 1: Simulation of framework implementation for cloud web server: This subsection presents a cloud-hosted simulation to evaluate framework performance in public cloud infrastructure. The following details summarize the environment and digital artifacts:

- Infrastructure Type: Cloud-hosted web server.
- Platform Utilized: Amazon Web Services (AWS). This choice reflects the widespread adoption of major cloud service providers in contemporary web hosting.
- Simulated Illicit Activity: The web server was configured to host an illegal online gambling site and was subjected to web defacement. This dual nature of illicit activity allowed for the testing of evidence acquisition related to both ongoing operations (gambling) and static alterations (defacement).
- Digital Evidence Acquired:
    - Transaction Logs: Critical for reconstructing user activity and financial flows associated with the gambling operation.
    - Website Files: Including source code, configuration files, and defaced content, essential for understanding the nature of the compromise and the illicit content.
    - User Databases: Containing sensitive user information and gambling records.
    - Disk Volume Snapshots: Forensic images of server storage capturing volatile and non-volatile states during acquisition.
- Acquisition Method Focus: Remote acquisition via cloud provider APIs (e.g., AWS CLI) to simulate real-world challenges of non-physical access and multi-tenancy.

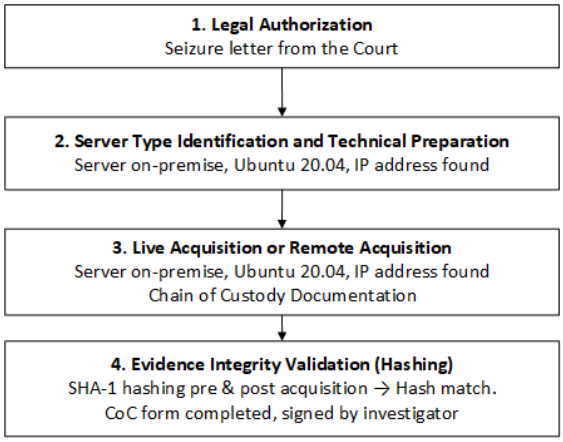

Fig. 5. Case 1 framework implementation.

Investigators received reports that a cloud-based web server was used for illegal online gambling. They needed to seize transaction logs, website files, and user databases. Simulation steps based on Fig. 5 are as follows:

- Legal Authorization: Investigators begin by obtaining a warrant from a court that grants permission to seize digital evidence from servers hosted on the cloud (AWS). The warrant includes permission to take transaction logs, databases, and system files of the gambling site located on the server. Investigators work

with legal authorities and cloud service providers to ensure that seizures are conducted in accordance with applicable laws, including data privacy laws relating to other users on the same cloud platform.

- Server Identification and Technical Preparation: Investigators identified that the web server was hosted on AWS and used PHP technology with MySQL database to run the online gambling site. Since the server was cloud-based, investigators prepared cloud-native forensic tools such as AWS CLI and CloudTrail to perform remote data acquisition. Investigators use the AWS Management Console to identify servers used to host gambling sites. Investigators also set up access via the AWS CLI to collect remote server snapshots, access logs, and databases.
- Data Acquisition: Investigators performed a remote acquisition of the cloud server without stopping the gambling site's services. The AWS CLI was used to take a snapshot of the disk volume, including the website's system files, access logs, and databases that store user and transaction information. Remote acquisition was performed via the AWS CLI, where investigators took a snapshot of the server disk volume that stores all files related to the gambling site, including site configurations, transactions, and databases. Investigators also took transaction logs to track the activity of users using the gambling site, such as login history, bets and payments.
- Validation of Evidence Integrity: After the data is captured, the investigator hashes all files and snapshots taken to ensure the integrity of the evidence. Hashing tools such as SHA-1 are used to ensure that the evidence remains intact and is not altered during the process. After snapshots and transaction logs are taken, hash values are calculated for each file and database using the AWS CLI and local hashing tools. All hash values are recorded as part of the Chain of Custody.

The cloud simulation demonstrated successful remote acquisition without service disruption. All acquired artifacts were hash-verified and documented in chain-of-custody records, producing legally defensible evidence.

2) Simulation of Case 2: Simulation of framework implementation for Virtual Private Server (VPS) web server: This subsection describes a second simulation using a Virtual Private Server (VPS) to assess framework adaptability in traditional server environments with direct administrative access.

- Infrastructure Type: Virtual Private Server (VPS). This represents a common hosting solution offering more control than shared hosting but less abstraction than full cloud services.
- Technology Stack: Apache web server with PHP, a widely used combination for dynamic web applications.
- Simulated Illicit Activity: The VPS was utilized for the dissemination of hoax news, specifically political misinformation, through injected subdirectories. This scenario tested the framework's ability to identify and acquire evidence related to content injection and malicious content distribution.
- Digital Evidence Acquired:
  - Activity Logs: Server access logs and application logs crucial for tracing the origin and spread of the hoax content.
  - Site Files: Including the injected hoax content, legitimate website files, and configuration data.
  - Database Contents: Relevant databases containing hoax-content records or user interaction data.
- Acquisition Method Focus: Live acquisition using forensic tools (e.g., Oxygen Keyscout) to minimize service disruption and capture volatile data from a running system.

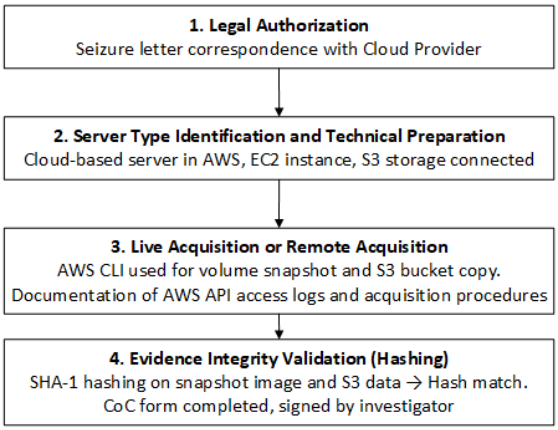

Fig. 6. Case 2 framework implementation.

Investigators received a report that a website hosted on a Virtual Private Server (VPS) was used to spread hoax news related to political information disturbing the public. Without stopping the server service, investigators needed to seize the web server and acquire related evidence, such as activity logs, site files, and hoax content posts. Simulation steps based on the proposed framework for Case 2 are shown in Fig. 6:

- Legal Authorization: Investigators begin by obtaining a court warrant to seize digital evidence from the VPS hosted web server. The warrant includes permission to retrieve site content files, user access logs, and databases that store hoax content and information related to user activity involved.
- Server Identification and Technical Preparation: Investigators identified that the web server was VPS and used Apache technology with PHP to run the site. Since the server was Virtual VPS, investigators prepared forensic tools such as Oxygen Keyscout and Magnet Axiom to perform live acquisition without shutting down the server. Investigators conduct an initial inspection of the server infrastructure, examine

the operating system (e.g., Linux) and prepare physical access to the server to collect evidence in real-time.

- Data Acquisition: Investigators perform live acquisition without stopping the web server service. Oxygen Keyscout is used to take snapshots of system files, including site content files, user activity logs, and databases that store hoax content. Live acquisition was performed using Oxygen Keyscout to capture system files associated with the website, including all files containing hoax news.
- Validation of Evidence Integrity: After the data is captured, investigators hash all captured files, logs, and databases to ensure the integrity of the evidence. After all files and access logs are retrieved, the hash values are calculated using Oxygen Keyscout and recorded in Chain of Custody to ensure that the collected data is not changed or manipulated.

The VPS simulation also completed live acquisition without downtime. Site files and logs were hash-validated and fully documented through chain-of-custody records, enabling accountable forensic analysis.

C. Metric

To assess the performance of the proposed framework, several metrics are defined based on technical, operational, and legal considerations. These metrics guide the evaluation process by providing quantifiable indicators of success throughout the simulated forensic procedures.

1) Aspects of success: This section outlines measurable aspects used to evaluate the effectiveness of the proposed framework in web server seizure scenarios. The framework is tested through two simulation scenarios: 1) seizure of a cloud web server used for online gambling and 2) seizure of a VPS web server used to spread hoax content. Each framework stage has specific success indicators, as follows:

- Volatile Data Preservation: Most of the $>$80% volatile data successfully preserved (RAM, active logs).
- Integrity Validation: Cryptographic hashing (SHA-1) performed pre- and post-acquisition to verify unchanged evidence values.
- Reporting and Secure Storage: The final report includes logs, hashes, analysis, and summary of findings. Evidence is stored encrypted and warrants are documented before acquisition.
- Downtime/Service Disruption: Minimal service disruption through live acquisition techniques.
- Cloud Environment Compatibility: Supports remote acquisition via official cloud provider APIs and services.
- Legal Compliance: Strict adherence to legal authorization and digital evidence handling standards.
- Ease of Analysis: Richer data set enables more thorough forensic analysis.

2) Quantitative evaluation results: To reduce subjectivity, the framework was also measured using quantitative indicators from both simulation cases (See Table II).

TABLE II. QUANTITATIVE RESULTS ACROSS SIMULATION SCENARIOS

Metric	Case 1 (Cloud)	Case 2 (VPS)
Hash verification success rate	100%	100%
Volatile artifact preservation rate	$\geq$80%	$\geq$80%
Acquisition completion time	$\approx$30 minutes	$\approx$30 minutes
Service downtime during acquisition	0 minutes	0 minutes
CoC completeness	$\geq$85%	$\geq$85%
Legal checklist compliance	$\geq$90%	$\geq$90%

Both scenarios satisfy the minimum feasibility target: average score $\geq$ 4.0 for all indicators and no critical legal or integrity indicator below 3.0.

3) Questionnaire: This section explains the questionnaire and interview guide used to evaluate the framework from practical and theoretical perspectives. The questionnaire includes questions related to:

- Preservation of digital evidence aspect
  - What is This framework provides systematic and standardized steps in seizure and acquisition of web servers?
  - Have the steps in this framework considered the preservation of volatile and non-volatile data with methods that are in line with forensic principles?
  - Does this framework provide an efficient cloud remote-acquisition method?
- Robust integrity and validation aspect
  - Does it provide evidence integrity validation mechanisms such as hashing to ensure the authenticity of the data obtained?
  - How well does it handle Chain of Custody to ensure evidence remains valid in court?
  - Is the framework flexible to be deployed on both VPS and cloud-hosted servers?
- Forensic acquisition admissibility in court aspect
  - To what extent does it meet legal requirements regarding the validity of obtaining evidence from seized web servers?
  - Does it meet the legal requirements regarding the seizure and retrieval of digital evidence, including the use of court warrants?

- What do you think are the weaknesses of this framework?

To assess the framework's feasibility, a structured questionnaire was developed and distributed to evaluators. This subsection describes the scoring criteria and rubric used to determine whether the framework meets minimum standards and legal admissibility. The framework is considered feasible if the average score for each indicator is ≥ 4.0 out of 5, and no critical aspects (legal and integrity) are scored ≤ 3, based on the Likert-scale rubric [49] below.

- (Very Poor): Evidence largely lost or corrupted; Weak validation and documentation; High inadmissibility.
- (Poor): Mostly data corrupted; Less validation, inconsistent documentation; May complicate admissibility.
- (Fair): Sufficient, but requires improvement and Sufficient to meet standards, but needs customization.
- (Good): Properly preserved using legitimate methods; Strong validation, detailed documentation.
- (Very Good): Comprehensive preserved, including live acquisition; Highly robust, transparent, and irrefutable documentation; Aligned with highest legal standards, beyond reasonable doubt.

4) Profile of SMEs: This section provides an overview of the Subject Matter Experts (SMEs) involved in the framework evaluation. Their professional backgrounds ensure a valid and informed assessment of the framework's applicability in real-world digital forensic contexts. The framework validation used an expert-judgment approach involving experts with direct experience in digital forensics [50]. Validation was conducted using both qualitative and quantitative assessment in two scenarios (cloud and VPS), involving 3 SMEs. Selection criteria included: 1) minimum 5 years of professional experience, 2) direct involvement in digital evidence handling, and 3) familiarity with legal admissibility requirements in Indonesia.

Feedback was collected through a structured questionnaire (Likert scale 1–5), guided interview, and review session on simulation outputs. The synthesis process applied indicator-level averaging, followed by cross-SME comparison to identify convergent findings and unresolved concerns.

A framework is categorized as feasible when the average score for each indicator is ≥ 4.0 and no critical indicator (legal and integrity aspects) is ≤ 3.0.

The SMEs were:

- Digital Forensics Practitioner
- Chairman of the Indonesian Digital Forensics Association
- Digital Forensic Expert at Indonesian Corruption Eradication Commission

Indonesian Corruption Eradication Commission (known as Komisi Pemberantasan Korupsi (KPK)) is a state institution established with the aim of improving the effectiveness and efficiency of efforts to eradicate corruption [51].

V. Results and Discussion

The development and evaluation results show the importance of aligning technical procedures with legal and operational standards in cloud and virtualized environments. The framework addresses gaps in existing models, especially in volatile-data preservation, integrity assurance, and minimal service disruption during live acquisition.

Integration of literature review and SME input strengthens the framework's legal validity and operational applicability. SME feedback confirms compliance with Indonesian legal standards and feasibility across VPS and cloud environments.

Simulation-based experimentation provides a replicable way to assess framework performance. Evaluation metrics were positive, with no critical SME failures, indicating that the framework can guide legally sound and technically reliable web server seizures.

A. SME Validation Results

This section discusses the evaluation results obtained from Subject Matter Experts (SMEs) who assessed the framework based on their professional judgment, practical experience, and legal-technical considerations. Their feedback serves as a crucial measure to validate the feasibility, effectiveness, and reliability of the proposed framework in real-world forensic investigations.

1) SME 1: Digital forensics practitioner: Validation focused on three aspects derived from the research objectives:

- Preservation of digital evidence aspect (Score: 4) The expert acknowledged that the framework already includes systematic and standardized procedures that align with forensic best practices. It successfully addresses the need to capture both volatile and non-volatile data, particularly by supporting live acquisition and remote access in cloud environments.
- Robust integrity and validation aspect (Score: 4) The SME confirmed that the framework incorporates proper integrity validation mechanisms, notably hashing (e.g., SHA-256), and emphasizes the importance of documenting each acquisition step. Chain of Custody was positively reviewed as well-structured and able to meet legal requirements.
- Forensic acquisition admissibility in court aspect (Score: 4) The legal compliance elements such as prior authorization, use of court warrants, and procedural transparency were considered robust. The SME stated that the framework is legally defensible and suitable for submission as digital evidence in court.

2) SME 2: Chairman of the Indonesian digital forensics association:

- Preservation of digital evidence aspect (Score: 4.67) The expert stated that the proposed framework already has systematic steps for collecting electronic evidence. However, as input, the expert provided notes regarding detailed elaboration on data preservation and acquisition, as well as technical steps related to remote acquisition.

- Robust integrity and validation aspect (Score: 4.67) The proposed framework is considered excellent in terms of integrity and strong evidence validation. This framework provides a hashing mechanism to ensure the authenticity and integrity of the data obtained, and has incorporated clear Chain of Custody procedures to ensure that evidence remains valid and accountable in court. Although it is flexible for use on VPS and cloud servers, further elaboration is needed regarding the different types for technical acquisition details.
- Forensic acquisition admissibility in court aspect (Score: 4.67) The framework is considered to meet both legal and technical requirements for evidence from web server seizures to be admissible in court. Legally, it emphasizes obtaining court authorization for seizure, aligning it with existing procedures for physical evidence under KUHAP.

3) SME 3: Digital forensic expert at Indonesian corruption eradication commission:

- Preservation of digital evidence aspect (Score: 4.33) The expert stated that the proposed framework is considered highly systematic and can serve as a reference for web server seizure, although there a note to strengthen documentation for live RAM and volatile logs. Additionally, the framework provides efficient methods for remote acquisition on cloud servers.
- Robust integrity and validation aspect (Score: 4.67) This framework provides robust mechanisms for validating evidence integrity, such as hashing, which is included in the standard procedure for digital evidence collection. The handling of the Chain of Custody is rated as very good because documentation is prepared from the beginning of the acquisition process to ensure the validity of evidence in court.
- Forensic acquisition admissibility in court aspect (Score: 4.67) This framework is considered compliant with legal requirements for the admissibility of evidence from web server seizures in court, provided that procedures are carried out according to seizure and hashing regulations.

B. Framework Feasibility

The variation in SME scores can be explained by the following factors:

- Diverse Backgrounds and Expertise: SMEs come from different fields such as law enforcement, legal practice, and cybersecurity, leading to varied priorities.
- Interpretation of Framework Components: The subjective nature of the scoring process means that SMEs interpret the framework's components differently, resulting in discrepancies based on their individual expectations and focus areas.
- Variability in Case Scenarios: The applicability of the framework can differ based on the specific case scenarios encountered by SMEs, influencing their scores depending on their experiences with cloud-based versus traditional VPS environments.
- Feedback and Iterative Improvement: Score differences provide constructive input for framework refinement.

Overall, differing SME scores reflect complementary perspectives rather than contradiction, and they help identify priorities for improvement.

The framework provides a solid foundation for conducting digital forensic investigations in Indonesia. All critical aspects related to legal compliance and data integrity received scores above the minimum requirement, with no aspect falling below the threshold of 3.0 [49]. A score below 3.0 in these areas would indicate significant weaknesses that could jeopardize the admissibility of evidence in court.

The proposed framework meets the threshold criteria, with an average score of **4.41**/5.0, indicating strong SME support. These findings suggest that the framework can be implemented while continuing iterative refinement [52].

C. Chain of Custody in Cloud-Native Environments: Interim Procedure and Design Direction

Although the framework demonstrates strong legal and technical feasibility, cloud-native implementation requires additional optimization in chain-of-custody automation. As an interim procedure, this study recommends:

- Generate immutable timestamped acquisition logs for each command/API action.
- Apply digital signatures to evidence manifests and hash reports.
- Store forensic artifacts and custody logs in write-once object storage (WORM/object-lock policy).
- Record actor identity and role for every evidence access event.
- Correlate cloud audit records (e.g., CloudTrail) with local acquisition notes before final reporting.

For future design, a cloud-native chain-of-custody module can be developed by integrating automated event capture, cryptographically linked audit trails, and policy-based verification to support end-to-end courtroom defensibility.

VI. Conclusion

This study addresses the need for a standardized web server seizure framework in Indonesia by integrating legal requirements with practical forensic procedures for VPS and cloud environments. The framework was developed through literature review, expert input, simulation, and refinement.

Results show that the framework supports legally authorized seizure, scenario-based technical preparation, live or remote acquisition, integrity validation through hashing, and complete chain-of-custody documentation. Across the simulations, evidence integrity and legal compliance were maintained without service downtime.

SME evaluation indicates strong feasibility (average score **4.41**/5.0), especially in legal compliance, integrity assurance, and acquisition effectiveness. The framework is therefore suitable as a practical reference, with future work focused on cloud-native chain-of-custody automation.

ACKNOWLEDGEMENTS

Thanks to the Subject Matter Experts who contributed their valuable insights and expertise throughout this research. Their constructive feedback and professional evaluations played a pivotal role in validating the proposed framework and ensuring its practical applicability within the field of digital forensics.

REFERENCES

[1] B. S. dan Sandi Negara, "Lanskap keamanan siber indonesia 2024," https://www.bssn.go.id/monitoring-keamanan-siber/, 2024, accessed: 2025-02-07.

[2] F. Thealma and Y. Ruldeviyani, "Digital forensic ethical data handling in indonesia," *The Indonesian Journal of Computer Science*, vol. 14, 2 2025. [Online]. Available: http://www.ijcs.net/ijcs/index.php/ijcs/article/view/4588

[3] R. Stoykova, "The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations," *Computer Law & Security Review*, vol. 49, p. 105801, 7 2023.

[4] W. Hartono, D. Muhardi, A. Akhiruddin, D. Valentianna, B. Purba, P. Asa, and Y. Dm, "Challenges of criminal investigation cyber crime," *Awang Long Law Review*, vol. 7, pp. 11–19, 11 2024. [Online]. Available: https://ejournal.stih-awanglong.ac.id/index.php/awl/article/view/1351

[5] G. Horsman and N. Sunde, "Unboxing the digital forensic investigation process," *Science & Justice*, vol. 62, pp. 171–180, 3 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1355030622000144

[6] F. Ramadhanny, "Aneka situs pemerintah dijaili jadi peringatan darurat garuda biru," *detik.com*, 2024. [Online]. Available: https://inet.detik.com/security/d-7505426/aneka-situs-pemerintah-dijaili-jadi-peringatan-darurat-garuda-biru

[7] Y. C. Tok, D. Y. Zheng, and S. Chattopadhyay, "A smart city infrastructure ontology for threats, cybercrime, and digital forensic investigation," *Forensic Science International: Digital Investigation*, vol. 52, p. 301883, 3 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281725000228

[8] A. Singh, "Operation power off," 2022. [Online]. Available: https://www.cyberpeace.org/resources/blogs/operation-power-off

[9] S. Kang, U. Hur, G. Kim, and J. Kim, "Forensic analysis and data decryption of tencent meeting in windows environment," *Forensic Science International: Digital Investigation*, vol. 51, p. 301818, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281724001422

[10] T. Göbel, F. Breitinger, and H. Baier, "Optimising data set creation in the cybersecurity landscape with a special focus on digital forensics: Principles, characteristics, and use cases," *Forensic Science International: Digital Investigation*, vol. 52, p. 301882, 3 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281725000216

[11] M. D. Kohn, M. M. Eloff, and J. H. Eloff, "Integrated digital forensic process model," *Computers and Security*, vol. 38, pp. 103–115, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2013.05.001

[12] F. Casino, T. K. Dasaklis, G. P. Spathoulas, M. Anagnostopoulos, A. Ghosal, I. Borocz, A. Solanas, M. Conti, and C. Patsakis, "Research trends, challenges, and emerging topics in digital forensics: A review of reviews," *IEEE Access*, vol. 10, pp. 25 464–25 493, 2022.

[13] T. J. Silva, E. OliveiraJr, M. E. Pereira, and A. F. Zorzo, "A review study of digital forensics in iot: Process models, phases, architectures, and ontologies," *Forensic Science International: Digital Investigation*, vol. 53, p. 301912, 6 2025. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2666281725000514

[14] S. M. Pedapudi and N. Vadlamani, "Data acquisition based seizure record framework for digital forensics investigations," *Proceedings of the 5th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2021*, pp. 1766–1768, 2021.

[15] Oxford, "seizure noun - definition, pictures, pronunciation and usage notes — oxford advanced learner's dictionary at oxfordlearnersdictionaries.com." [Online]. Available: https://www.oxfordlearnersdictionaries.com/definition/english/seizure

[16] T. R. Sree and S. M. S. Bhanu, "Data collection techniques for forensic investigation in cloud," *Digital Forensic Science*, 2020.

[17] S. Ruiz-Villafranca, J. M. C. Gómez, and J. Roldán-Gómez, "A forensic tool for the identification, acquisition and analysis of sources of evidence in iot investigations," *Internet of Things*, vol. 27, p. 101308, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S254266052400249X

[18] C. Liu, A. Singhal, and D. Wijesekera, "Identifying evidence for cloud forensic analysis," in *IFIP Advances in Information and Communication Technology*, vol. 511. Springer New York LLC, 2017, pp. 111–130.

[19] H. Spichiger and F. Adelstein, "Preserving meaning of evidence from evolving systems," *Forensic Science International: Digital Investigation*, vol. 52, p. 301867, 2025, dFRWS EU 2025 - Selected Papers from the 12th Annual Digital Forensics Research Conference Europe. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S266628172500006X

[20] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Advanced digital forensics and anti-digital forensics for iot systems: Techniques, limitations and recommendations," *Internet of Things*, vol. 19, p. 100544, 8 2022. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2542660522000464

[21] V. Prakash, A. Williams, L. Garg, P. Barik, and R. K. Dhanaraj, "Cloud-based framework for performing digital forensic investigations," *International Journal of Wireless Information Networks*, vol. 29, pp. 419–441, 12 2022. [Online]. Available: https://link.springer.com/article/10.1007/s10776-022-00560-z

[22] A. M. Komarudin, N. Widiyasono, A. P. Aldya, and R. Rizal, "Data integrity testing of digital evidence data capture results on private cloud computing services," *INNOVATICS: Innovation in Research of Informatics*, vol. 5, 11 2023. [Online]. Available: https://jurnal.unsil.ac.id/index.php/innovatics/article/view/8420

[23] A. Almuqren, H. Alsuwaelim, M. M. H. Rahman, and A. A. Ibrahim, "A systematic literature review on digital forensic investigation on android devices," *Procedia Computer Science*, vol. 235, pp. 1332–1352, 1 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050924008020

[24] B. Sharma, J. Ghawaly, K. McCleary, A. M. Webb, and I. Baggili, "Forensicllm: A local large language model for digital forensics," *Forensic Science International: Digital Investigation*, vol. 52, p. 301872, 3 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281725000113

[25] J. Yang, J. Kim, J. Bang, S. Lee, and J. Park, "Catch: Cloud data acquisition through comprehensive and hybrid approaches," *Forensic Science International: Digital Investigation*, vol. 43, p. 301442, 9 2022.

[26] R. L. Lau, "Web server part 1: Apache/nginx basics," *Practical Internet Server Configuration*, pp. 183–225, 2021. [Online]. Available: https://link.springer.com/chapter/10.1007/978-1-4842-6960-2_9

[27] R. U. Rahman and D. S. Tomar, "A new web forensic framework for bot crime investigation," *Forensic Science International: Digital Investigation*, vol. 33, p. 300943, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281720300718

[28] ISO, "Iso 27037:2012 - guidelines for identification, collection, acquisition and preservation of digital evidence," 2012. [Online]. Available: https://www.iso.org/standard/44381.html

[29] D. Day, "Chapter 7 - seizing, imaging, and analyzing digital evidence: step-by-step guidelines," in *Cyber Crime and Cyber Terrorism Investigator's Handbook*, B. Akhgar, A. Staniforth, and F. Bosco, Eds. Syngress, 2014, pp. 71–89. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128007433000074

[30] A. Wickramasekara, F. Breitinger, and M. Scanlon, "Exploring the potential of large language models for improving digital forensic investigation efficiency," *Forensic Science International: Digital Investigation*, vol. 52, p. 301859, 3 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281724001860

[31] C. Karagiannis and K. Vergidis, "Digital evidence and cloud forensics: Contemporary legal challenges and the power of disposal," *Information 2021, Vol. 12, Page 181*, vol. 12, p. 181, 4 2021. [Online]. Available: https://www.mdpi.com/2078-2489/12/5/181/htmhttps://www.mdpi.com/2078-2489/12/5/181

[32] S. V. Patel and I. S. Lurie, "The use of portable separation devices for forensic analysis: A review of recent literature," *Forensic Chemistry*, vol. 26, p. 100365, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2468170921000618

[33] K. U. Maheswari and G. Shobana, "The state of the art tools and techniques for remote digital forensic investigations," *2021 3rd International Conference on Signal Processing and Communication, ICPSC 2021*, pp. 464–468, 5 2021.

[34] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Special publication 800-86 guide to integrating forensic techniques into incident response recommendations of the national institute of standards and technology," National Institute of Standards and Technology, Tech. Rep., 2006.

[35] K.-S. Lim, A. Savoldi, C. Lee, and S. Lee, "On-the-spot digital investigation by means of ldfs: Live data forensic system," *Mathematical and Computer Modelling*, vol. 55, no. 1, pp. 223–240, 2012, advanced Theory and Practice for Cryptography and Future Security. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0895717711002895

[36] A. W. Malik, D. S. Bhatti, T. J. Park, H. U. Ishtiaq, J. C. Ryou, and K. I. Kim, "Cloud digital forensics: Beyond tools, techniques, and challenges," *Sensors 2024, Vol. 24, Page 433*, vol. 24, p. 433, 1 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/2/433/htmhttps://www.mdpi.com/1424-8220/24/2/433

[37] J.-P. Sandvik, K. Franke, H. Abie, and A. Årnes, "Quantifying data volatility for iot forensics with examples from contiki os," *Forensic Science International: Digital Investigation*, vol. 40, p. 301343, 2022, selected Papers of the Ninth Annual DFRWS Europe Conference. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281722000129

[38] W. Yun, J. Kang, S. Lee, and J. Park, "Digital forensic approaches to intel and amd firmware raid systems," *Forensic Science International: Digital Investigation*, vol. 54, p. 301971, 9 2025. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2666281725001106

[39] N. Kuntze, C. Rudolph, H. Schilling, A. Alva, B. Brisbois, and B. Endicott-Popovsky, "Seizure of digital data and 'selective suppression' of digital evidence," *Int. Workshop Syst. Approaches Digit. Forensics Eng., SADFE*, 9 2014.

[40] J. G. J. Nortje and D. C. Myburgh, "Impediments during the compilation of a search and seizure warrant for digital information by forensic investigators in south africa," *Journal of Financial Crime*, vol. 31, pp. 476–488, 4 2024.

[41] K. S. Singh, A. Irfan, and N. Dayal, "Cyber forensics and comparative analysis of digital forensic investigation frameworks," *2019 4th International Conference on Information Systems and Computer Networks, ISCON 2019*, pp. 584–590, 2019.

[42] C. Hargreaves, F. Breitinger, L. Dowthwaite, H. Webb, and M. Scanlon, "Dfpulse: The 2024 digital forensic practitioner survey," *Forensic Science International: Digital Investigation*, vol. 51, p. 301844, 12 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281724001719

[43] B. Manan, "Prosedur penyitaan." [Online]. Available: https://pn-metro.go.id/index.php/tentang-pengadilan/2019-09-30-06-51-00/pidana/prosedur-penyitaan

[44] D. B. Andersen, N. Sunde, and K. Porter, "Tool induced biases? misleading data presentation as a biasing source in digital forensic analysis," *Forensic Science International: Digital Investigation*, vol. 52, p. 301881, 3 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281725000204

[45] T. J. Silva, A. H. Mazur, E. OliveiraJr, A. F. Zorzo, and M. P. Barcellos, "An ontology for promoting controlled experimentation in digital forensics," *Forensic Science International: Digital Investigation*, vol. 52, p. 301845, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281724001720

[46] D. Rani, N. S. Gill, and P. Gulia, "A forensic framework to improve digital image evidence administration in iiot," *Journal of Industrial Information Integration*, vol. 38, p. 100568, 3 2024. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2452414X24000128

[47] B. Martini and K. K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digital Investigation*, vol. 9, pp. 71–80, 11 2012. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S174228761200059X\#sec3.3

[48] R. Stoykova and K. Franke, "Reliability validation enabling framework (rvef) for digital forensics in criminal investigations," *Forensic Science International: Digital Investigation*, vol. 45, p. 301554, 6 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S266628172300063X

[49] J. Robinson, "Likert scale," *Encyclopedia of Quality of Life and Well-Being Research*, pp. 3917–3918, 2023. [Online]. Available: https://link.springer.com/rwe/10.1007/978-3-031-17299-1_1654

[50] N. Martynenko, "Digitalisation of forensic expert activity in ukraine: Organisational and legal framework," *Forensic Science International: Synergy*, vol. 10, p. 100578, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2589871X25000075

[51] Undang-Undang, "Undang-undang (uu) nomor 19 tahun 2019 tentang perubahan kedua atas undang-undang nomor 30 tahun 2002 tentang komisi pemberantasan tindak pidana korupsi," Meteri Hukum dan Hak Asasi Manusia, Tech. Rep., 2019. [Online]. Available: www.peraturan.go.id

[52] M. Ng, J. James, and R. Bull, ""what you say in the lab, stays in the lab": A reflexive thematic analysis of current challenges and future directions of digital forensic investigations in the uk," *Forensic Science International: Digital Investigation*, vol. 51, p. 301839, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281724001665