

A Juridical Analysis of Digital Forensics in the Evidentiary Process for Online Child Sexual Abuse Cases

Emy Rosna Wati¹⁾ & Isabela Efendi²⁾

¹⁾Faculty of Law, Universitas Muhammadiyah Sidoarjo, Indonesia, E-mail: emyrosnawati@umsida.ac.id

²⁾Faculty of Law, Universitas Muhammadiyah Sidoarjo, Indonesia, E-mail: Isabela_09@gmail.com

Abstract. *The rapid advancement of digital technology has been closely followed by a rise in online sexual crimes against children, particularly through the practice of cyber grooming. This study analyzes the forms of digital evidence and the legal procedures for presenting such evidence in cases of online child sexual abuse. A normative juridical method was employed, using a statute approach supported by systematic, grammatical, and futuristic interpretation. The primary legal materials examined include Law Number 19 of 2016 on the Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, Government Regulation Number 71 of 2019 concerning the Operation of Electronic Systems and Transactions, the draft Ministerial Regulation of Communication and Informatics on the Handling of Electronic Evidence, Law Number 35 of 2014 on Child Protection, the Indonesian Criminal Code, and National Police Regulation Number 10 of 2009 concerning Electronic Evidence. Secondary legal materials, including academic literature, journal articles, legal textbooks, and expert opinions, were also examined using deductive analysis. The findings indicate that digital evidence, such as screenshots, metadata, disk clones, and cloud-stored content, carries varying degrees of evidentiary strength, with disk clones obtained through lawful forensic procedures regarded as the most conclusive. The study underscores the importance of the ISO/IEC 27037 standard in guiding the identification, acquisition, and preservation of digital evidence, as well as the urgency of URL permanence and comprehensive chain-of-custody documentation. Nevertheless, persistent constraints remain, including limited human resources, technical barriers, and inadequate cross-platform cooperation. Strengthening the capacity of law enforcement officers and updating existing regulations are therefore essential steps toward ensuring the validity and effectiveness of digital evidence in court.*

Keywords: *Crime; Digital; Evidence; Forensics; Sexual.*

1. Introduction

The digital era has brought significant changes to patterns of human social interaction, particularly among children and adolescents as members of the digital-native generation. The expansion of internet networks and social media has created new spaces for cybercrime, including online sexual offenses against children carried out through the practice known as grooming, in which perpetrators exploit digital platforms such as social media, messaging applications, discussion forums, and online games (Afisako et al., 2025) Data from the Ministry of Women's Empowerment and Child Protection (2021) indicate a 23% increase in cases of child exploitation through social media, while UNICEF (2023) reported that approximately 500,000 children worldwide have experienced sexual exploitation and inappropriate treatment in cyberspace.

Online sexual crimes against children frequently involve the manipulation of victims through social media platforms such as WhatsApp, Instagram, and Telegram. A case that went viral in 2024, circulated through a social media account on platform X (@olafaa_), illustrated how a sixth-grade elementary school girl was sexually abused by a twenty-year-old man she had met through the online game Mobile Legends. The account holder shared screenshots of a conversation showing how the perpetrator used inappropriate, sexually suggestive language to manipulate the victim until she eventually sent explicit images of herself. The perpetrator reportedly began by praising the victim daily until she was persuaded to comply with his request. According to the account holder, the victim's older sibling had reported the incident to the authorities, but at the time of writing no resolution had been reached.

The central challenge in addressing such cases lies in the evidentiary process within law enforcement. Perpetrators frequently operate under false identities, maintain anonymity, and erase their digital traces after committing acts of grooming. Digital forensics has therefore become an essential tool for uncovering electronic evidence that is often dispersed across multiple platforms and inherently volatile (Nova, 2025). The collection of digital evidence requires specialized forensic expertise that not all law enforcement officers currently possess, while bureaucratic and legal obstacles in cooperating with digital platforms and internet service providers further slow the process. Limited public understanding, a tendency to blame victims, and restrictions on data protection and privacy further complicate the collection of evidence that is both lawful and admissible in court (Gusman et al., 2026) The growing use of technology makes digital forensics increasingly vital in uncovering the traces left by offenders (St. Fatimah, La Ode Husen, 2024). Evidentiary processes involve both the verification of digital evidence and its legal interpretation. Given the serious psychological impact on child victims, an adaptive legal system and reliable evidentiary methods are urgently needed to address the growing prevalence of online grooming cases.

Previous studies have examined the issue of cyber grooming and the role of digital forensics in law enforcement, each with a distinct focus. Holivia and Suratman (2021), in a study titled “Child Cyber Grooming as a New Modus Operandi of Cyberspace Crimes,” found that the handling of child cyber grooming cases in Indonesia tends to be more preventive than repressive, requiring greater involvement from various societal elements, particularly parents, in supervising children's use of social media. A second study by Ishmah et al. (2024), titled “Reviewing the Existence of Government Policy on the Vulnerability of Cyber Child Grooming,” revealed weaknesses in existing regulation, considered ineffective because legal action can only proceed once physical evidence of the crime has already circulated. A third study by Awaluddin, Amsori, and Mulyana (2024), titled “Challenges and the Role of Digital Forensics in Law Enforcement against Digital Crime,” explained that digital forensics plays a vital role in proving cybercrime cases; despite a rise in cybercrime in recent years, including online indecency offenses, handling such cases remains more complex than conventional crime because it requires specialized expertise in digital evidence analysis, and perpetrators often attempt to erase their digital traces.

This study offers novelty relative to previous research by specifically analyzing the presentation of digital evidence in proving cases of online child sexual abuse. Unlike earlier studies, which focused primarily on preventive measures such as community supervision or regulatory reform, the present study focuses on the techniques for presenting digital evidence in accordance with prevailing legislation, as well as the technical obstacles in evidence collection that have received limited attention in previous literature.

This study aims to analyze the procedures for presenting digital evidence in cases of online child sexual abuse, with particular attention to technical challenges such as the volatility and encryption of digital evidence, as well as methods for accurately presenting evidentiary information for use in court. This study further aims to identify obstacles in the collection and analysis of digital evidence and to formulate strategic recommendations for optimizing the judicial system, including the development of evidentiary methods that remain adaptive to technological change. This research is significant given that cases of online child sexual abuse require a specialized evidentiary approach: digital evidence that is volatile, dispersed across multiple platforms, and often encrypted demands reliable forensic techniques, while ongoing technological advancement requires continuous updates to evidence collection and analysis methods so that they remain aligned with the prevailing judicial system.

2. Research Methods

This study employs a normative juridical method with a statute approach, supported by systematic, grammatical, and futuristic interpretation. The primary legal materials analyzed include Law Number 19 of 2016 on the Amendment to

Law Number 11 of 2008 concerning Electronic Information and Transactions, Government Regulation Number 71 of 2019 concerning the Operation of Electronic Systems and Transactions, the draft Ministerial Regulation of Communication and Informatics on the Handling of Electronic Evidence, Law Number 35 of 2014 on Child Protection, the Indonesian Criminal Code, and National Police Regulation Number 10 of 2009 concerning Electronic Evidence. Secondary legal materials, comprising academic literature, journal articles, legal textbooks, and expert opinions, were used to support the analysis. All legal materials were examined using deductive analysis, whereby general legal principles and statutory provisions were applied to assess the specific factual patterns observed in reported cases of online child sexual abuse (Dewa et al., 2023).

3. Results and Discussion

3.1. Regulatory Framework Governing Digital Evidence in Cases of Online Child Sexual Abuse

Technological development has increased children's vulnerability to online sexual crimes carried out through social media, messaging applications, online games, and other digital platforms, particularly through the *modus operandi* known as child grooming, a form of psychological manipulation typically employed by perpetrators against minors for the purpose of sexual exploitation. This phenomenon underscores the need for clear regulation regarding the admissibility of digital evidence in criminal proceedings. Grooming generally begins when an adult visits online forums frequented by children, builds a friendship with a young person, and gradually earns the child's trust through attention, persuasion, gifts, and other forms of care. This manipulation eventually develops into sexualized interaction and culminates in control and exploitation of the victim, often ending in sexually explicit conversations. Crimes of this nature pose considerable challenges to the evidentiary process, since the evidence left behind is not physical but digital in form and frequently transient in nature.

Within the Indonesian legal context, particularly regarding online sexual offenses against children, the evidence most commonly relied upon consists of digital data stored on electronic devices or transmitted through electronic systems. Accordingly, the legal recognition of digital evidence as a valid means of proof is established under Law Number 19 of 2016 on the Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (the ITE Law), particularly Article 5(1), which stipulates that electronic information and/or electronic documents, along with their printed results, constitute legally valid evidence. Article 6 further provides that electronic information is deemed equivalent to a written document so long as the information contained therein can be accessed, displayed, its integrity guaranteed, and its legal accountability ensured. This provision underscores the importance of the principles of integrity

and authentication for digital evidence; the validity of electronic evidence is therefore determined not merely by its existence, but also by the technical procedures that guarantee the absence of any modification from the moment of discovery until its presentation in court.

This principle is reinforced by Government Regulation Number 71 of 2019 concerning the Operation of Electronic Systems and Transactions (the PSTE Regulation), which governs the administration of electronic systems and the integrity of digital evidence within electronic transactions, requiring that submitted digital evidence originate from a reliable system that meets information security standards. This is closely related to the principle of auditability, that is, the capacity of a system to be traced and audited by an independent party. In practical support of this framework, the draft Ministerial Regulation of Communication and Informatics on the Initial Handling of Electronic Evidence technically governs how electronic evidence must be handled to ensure legal accountability, embodying the core principles of relevance, reliability, and sufficiency: electronic evidence must not merely be accessible, but must also reflect an authentic and unaltered condition and demonstrate a logical connection to the offense under investigation. Applying this principle requires comprehensive forensic documentation and the involvement of expert personnel in the validation process (Muhammad Iqbal et al., 2025).

Law Number 35 of 2014 concerning Child Protection, particularly Article 76E, prohibits any person from committing or allowing indecent acts against a child, whether through violence, deceit, persuasion, or digital communication. This provision has been interpreted to extend to explicit sexual conduct carried out through social media or messaging applications, which may be qualified as a criminal act. In evidentiary terms, electronic evidence such as text messages, images, videos, screenshots, and social media metadata may serve as a means of proof in prosecuting offenders. Further technical regulation concerning digital evidence is provided in National Police Regulation Number 10 of 2009 concerning Procedures and Requirements for the Management of Electronic Evidence within the Indonesian National Police, which sets out detailed standard procedures for handling digital evidence, from identification and securing to storage and eventual presentation at trial, with the principal aim of preserving the authenticity, integrity, and completeness of electronic evidence (POPA & PhD, 2025).

The Indonesian Criminal Procedure Code (KUHP), through Article 184(1), provides juridical recognition of digital evidence when examined from the perspective of criminal procedural law. This provision enumerates the legally valid means of proof as witness testimony, expert testimony, documents, indications, and the defendant's statement. In practice, electronic information or documents may be categorized as evidence in the form of a document or an indication,

provided that it was obtained through a lawful procedure and can be legally accounted for in accordance with criminal procedural law.

Beyond national provisions, law enforcement practice also recognizes the Indonesian National Standard (SNI) and international standards such as ISO/IEC 27037, "Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence." This standard provides guidance for the lawful identification, collection, acquisition, and preservation of digital evidence, from the initial retrieval of evidence at the crime scene to laboratory-based forensic analysis. Addressing the challenges posed by technological development and cybercrime requires synchronization between national positive law and international best practice (Adyesta et al., 2026) requiring that every stage of digital evidence handling follow procedures that are verifiable, reproducible, and auditable by third parties, thereby ensuring objectivity and legality. It may therefore be concluded that regulatory recognition of digital evidence in cases of online child sexual abuse is already available within Indonesia's positive law. Nevertheless, synchronization between existing regulation and field practice remains necessary, particularly in strengthening law enforcement officers' capacity to understand, manage, and legally account for digital evidence presented at trial.

3.2. Forms and Types of Digital Evidence in Online Child Sexual Offenses

In cases of online child sexual abuse, perpetrators frequently exploit digital spaces such as social media, messaging applications, and online forums to approach victims, manipulate them emotionally, and ultimately exploit them sexually (Duani et al., 2026). Digital evidence therefore constitutes the primary instrument for uncovering and proving such crimes before the law, making it a central component of the evidentiary process. The forms of digital evidence relevant to this context include the following:

- 1) Screenshots of conversations.
- 2) File metadata containing technical information such as creation date, GPS location, and device type.
- 3) Disk clones, or comprehensive copies of electronic devices.
- 4) System or application activity logs indicating patterns of use and online interaction.
- 5) Audio/video recordings, including voice notes or video calls.
- 6) Permanent URLs of content or accounts associated with the offense.
- 7) Cloud-stored content held on online digital storage platforms.

The existence of digital evidence must be supported by documentation and forensic procedures that comply with recognized standards, one of which is ISO/IEC 27037, which governs the process from identification and collection to acquisition and preservation of electronic evidence. Evidence obtained or stored outside proper procedure risks being declared inadmissible in court. As a concrete illustration, a case that went viral in 2024 through a social media account on platform X (@olafaa_) demonstrated how evidence such as screenshots of conversations may circulate widely yet remain legally uncertain if not supported by adequate forensic procedures. This case underscores the importance of employing appropriate forensic methods, such as disk cloning and metadata collection, to strengthen the evidentiary position of such material before the law. (Okprianti et al., 2025)

For evidence to be admissible at trial, it must satisfy the principles of authenticity and integrity. Digital evidence such as screenshots, metadata, or electronic recordings may be qualified as legally valid evidence so long as it is obtained lawfully and satisfies the requirements of procedural law. Under Article 184(1) of the KUHP, digital evidence may be categorized as a document or an indication, depending on its form, content, and manner of presentation. Digital evidence in cases of online sexual crime possesses complex and easily alterable characteristics, requiring specialized handling; the classification of evidence types must therefore be conducted carefully, and collection techniques must follow forensic standards to prevent contamination or doubt regarding authenticity (Charenitha & Firmansyah, 2025)

3.3. Validity and Evidentiary Strength of Digital Evidence

Within Indonesia's criminal evidentiary system, evidence must satisfy both formal and material elements of validity before it can be accepted and weighed by a judge in judicial proceedings. As electronic-based crime continues to evolve, including online sexual offenses against children, digital evidence must be assessed specifically, both in terms of its form and its evidentiary strength. In this respect, classifying the strength of digital evidence is essential in guiding law enforcement officers in evaluating its reliability. Normatively, within the framework of criminal procedural law, digital evidence can be classified into three levels of evidentiary strength: indicative evidence, supporting evidence, and conclusive evidence. This classification not only reflects the evidentiary weight of each type of evidence, but also determines the extent to which it may be accepted and relied upon by a judge in criminal proceedings (D. R. Anggraeni & Salsabila, 2024)

First, indicative evidence refers to the initial form of digital evidence that functions as an indication of a suspected criminal act. This evidence is preliminary in nature and does not, on its own, possess sufficient evidentiary force to establish the complete elements of an offense. Examples include screenshots of electronic conversations, URLs of websites or social media accounts suspected of being used

to commit the offense, or circulating digital content that has not yet undergone a validation process. A screenshot or photograph of an electronic conversation can only be regarded as preliminary evidence if it is not corroborated through a lawful digital forensic process, given its susceptibility to manipulation and the difficulty of verifying its authenticity (Syavica et al., 2025). A URL that has not been made permanent through mechanisms such as web archiving or hash validation likewise functions only as a preliminary indication rather than as standalone legal evidence (Agustiono et al., 2024). In investigative practice, indicative evidence is often used as the basis for initial investigative measures but is not sufficiently robust to serve as the juridical basis for naming a suspect without the support of stronger corroborating evidence (Ramadani & Nur, 2026).

Second, supporting evidence refers to digital evidence used to strengthen or affirm primary evidence already lawfully obtained. Although not of primary standing, such evidence plays an important role in reinforcing the evidentiary logic of a case. This category includes electronic document metadata, digital device activity logs, geolocation data, and records of online communication obtained through a lawful digital forensic process (Popa, 2024). The evidentiary strength of supporting evidence increases significantly when it is obtained and processed in accordance with international forensic standards such as ISO/IEC 27037, supported by an auditable procedural trail. Metadata and log files are themselves critical sources of information in reconstructing digital events, provided that their acquisition is carried out using lawful and well-documented forensic techniques (Nila Arzaqi, Deny Puspitasari, 2025).

Third, conclusive evidence refers to digital evidence obtained through legally and forensically valid procedures that carries the highest evidentiary strength, as it satisfies the principles of integrity, authenticity, and direct relevance to the elements of the offense. This category of evidence is obtained through forensic acquisition methods such as disk cloning in the form of a bitstream image, verified through hash values (for example, SHA-256), and documented through a complete chain of custody (Al Jumah et al., 2019). In criminal justice practice, conclusive evidence can stand alone as the legal basis for designating a person as a suspect or defendant. For example, a forensic copy of a perpetrator's device, digital files found in cloud storage, or electronic documents obtained through a lawful interception by investigators may serve as primary evidence that decisively determines the outcome of proof at trial (Romadhon, 2024). This confirms that an acquisition process following the ISO/IEC 27037 standard enables data retrieved from cloud storage to possess a high degree of validity as primary evidence; it may therefore be concluded that a disk clone based on bit-by-bit acquisition provides a complete and verifiable copy of digital evidence, the validity of which cannot easily be disputed in court (Nasution et al., 2025).

Based on criminal procedural law and pursuant to Articles 5 and 6 of Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016, digital evidence may be considered valid if obtained through a procedure that guarantees its integrity and legal accountability. Building on this analysis, Table 1 presents the types of digital evidence, their sources or media, their functional description, and their level of validity according to the principles of criminal evidentiary law and digital forensic standards:

Types of digital evidence and their level of validity

No.	Type of Digital Evidence	Example Media/Source	Description	Validity Level
1.	Conversation screenshot	WhatsApp, Instagram, Telegram	Digital image of conversation content	Indicative
2.	Metadata	Digital file, device log	Contains technical data such as time, location, and device	Supporting
3.	Disk clone	Smartphone, laptop, HDD	Bitstream copy of the entire device content	Conclusive
4.	Permanent URL	Social media, online forum	Link to archived digital content	Indicative–Supporting
5.	Activity log	Application, server system	Trace of user interaction with a system or application	Supporting
6.	Audio/video recording	Voice note, video call	Multimedia file of perpetrator–victim communication	Supporting
7.	Cloud content	Google Drive, Dropbox	Online file uploaded/downloaded by the perpetrator	Conclusive

3.4. URL Permanence and the Validation of Electronic Evidence

In cases of online child sexual abuse, digital evidence is not always stored locally on a device; much of it exists in the form of links or URLs directing to online content such as social media posts, forum entries, or specific websites. Given their dynamic and easily deletable nature, evidence in the form of URLs requires a permanence process to guarantee its integrity as valid evidence (Kusuma et al., 2024). URL permanence is the process of archiving digital content from a given web address or platform so that it can be retrieved again in a fixed form, even after the original content has been deleted or modified. This process ensures that the content of a URL remains traceable and verifiable when needed for evidentiary purposes. The steps typically involved in URL permanence include the following:

- 1) Capturing a comprehensive screenshot of the content linked by the URL.
- 2) Recording metadata such as the time of access, the accessing IP address, and the complete URL.
- 3) Using web archiving services such as Archive. today, Web Preserver, or Hunchly to archive a static version of the page.
- 4) Recording the hash value of the archived file to preserve data integrity and validity.
- 5) Storing the archived results on secure and verifiable digital media.

Indonesian legal practice does not yet specifically regulate URL permanence within statute; however, this process may be regarded as part of the acquisition and preservation of digital evidence as covered under ISO/IEC 27037 and supported by the principle of evidentiary integrity set out in Article 6 of the ITE Law. This is further reinforced by the draft Ministerial Regulation of Communication and Informatics on the Initial Handling of Electronic Evidence, which requires that every act of securing electronic evidence be documented and auditable. Permanence becomes crucial when a URL serves as the sole available reference demonstrating a perpetrator's communication or actions; without such a process, a URL risks becoming unverifiable once its content is deleted or is no longer publicly available. URL permanence is therefore not merely a technical measure, but also a form of legal protection for the validity of digital evidence. Investigators and other parties involved in law enforcement must understand the importance of this method to avoid losing crucial evidence capable of accurately proving the elements of an offense before the law (A. Anggraeni et al., 2025).

3.5. Stages and Principles of Digital Forensics Based on ISO/IEC 27037

Proof within criminal law forms part of criminal policy as a “science of response” encompassing multiple disciplines, given the broad scope and variety of crimes arising from information technology. Indonesian law enforcement often faces difficulty in securing convictions against perpetrators of online child sexual abuse because the available evidence fails to satisfy the requirements of the criminal justice system, even though efforts to prosecute such perpetrators must nevertheless continue. The digital forensic process therefore becomes essential in presenting electronic evidence that is both lawful and admissible in court (Ponno, 2023).

Digital forensics is not limited to uncovering evidence of digital crime alone but may also be applied to conventional crimes involving electronic evidence. Digital forensics comprises a series of procedures for collecting, analyzing, and reporting digital data to support law enforcement. Although it does not function as direct evidence in itself, digital forensics assists law enforcement throughout the enforcement process. The management of digital forensic procedures must comply with internationally recognized standards, as set out in ISO/IEC 27037, which provides technical guidance for the identification, collection, acquisition, and preservation of digital evidence.

The first stage is identification, the process of determining and recognizing digital devices or systems suspected of containing information relevant to a criminal offense. At this stage, investigators record the location of the evidence, the type of device, its status (active or inactive), and its physical condition (Prasetyawan & Indrayani, 2023). Identification begins at the crime scene and forms the foundation of the entire forensic process. Following identification, the collection stage secures digital evidence from the crime scene with care to avoid altering the

data; all processes are documented, including the recording of time, photographing of devices, and packaging in anti-static containers in accordance with procedure.

The next stage is acquisition, the process of creating a comprehensive copy of digital data (a bitstream image) from the collected device. Acquisition is performed using a write-blocker to prevent any alteration of the original data during the copying process. Once the copy has been completed, verification is performed by calculating a hash value (such as MD5 or SHA-256) to confirm that the copy is identical to the original data (Prasetya & Priyana, 2021). The final stage is preservation, that is, the storage of digital evidence and its copies on secure, tamper-resistant storage media. This storage must guarantee data integrity through to trial and must be accompanied by complete documentation, including a chain of custody and a record of all parties granted access to the evidence.

These four stages must be carried out systematically, documented thoroughly, and executed in accordance with procedure so that digital evidence possesses undoubted evidentiary strength. Should any stage fail to be properly executed, the risk of the evidence being invalidated in judicial proceedings becomes considerably high. The ISO/IEC 27037 standard provides a systematic framework for the lawful handling of digital evidence. To illustrate this process, Figure 1 presents a flowchart depicting the sequence of identification, collection, acquisition, and preservation of digital evidence:

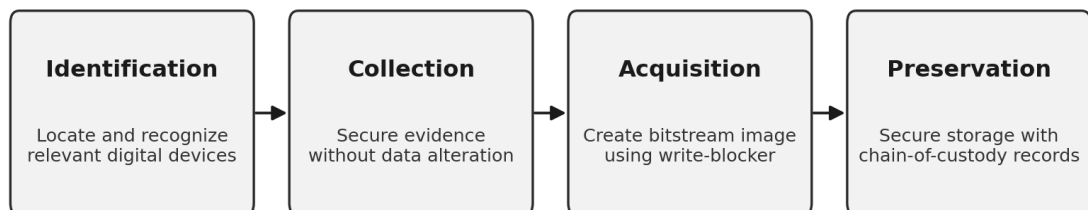


Figure Flowchart of the digital forensic process stages

Figure illustrates that each stage must be carried out with complete documentation to satisfy the principle of chain of custody. The ISO/IEC 27037-based stages of digital forensics serve as a technical guideline that simultaneously guarantees the integrity and legality of electronic evidence within criminal proceedings, particularly in handling cases of online child sexual abuse. By following the stages set out in the national standard adaptation of ISO/IEC 27037, the digital forensic process in Indonesia can be conducted professionally and in accordance with international standards, thereby increasing judicial confidence in digital evidence and supporting the effectiveness of proof in cases of online child sexual abuse. Adherence to these forensic stages, supported by disciplined

application of their underlying principles, enables digital evidence to be presented lawfully, accurately, and effectively to prove instances of online child sexual abuse; such standardization forms an essential component of modern, technology-based law enforcement.

By following the ISO/IEC 27037-based digital forensic stages, law enforcement officers can ensure that the digital evidence obtained possesses a high degree of legal validity, a process that is key to delivering justice in cases of online child sexual abuse. URL permanence techniques constitute a crucial step in preserving the validity of digital content as evidence (Mualfah & Ramadhan, 2020); without this method, evidence obtained from the internet lacks sufficient legal force to support proof in criminal proceedings. Digital evidence such as screenshots and metadata can only be regarded as valid when obtained through verifiable and auditable methods. Disk cloning is therefore regarded as the strongest and most essential form of digital evidence in criminal evidentiary processes, particularly in cases of online child sexual abuse (Fattah Ys et al., 2024).

A formal standard operating procedure for digital forensic investigation is not yet available in Indonesia. Law enforcement agencies have developed various methods to standardize the process, and international bodies such as the International Organization for Standardization have begun to develop relevant frameworks, which are expected to provide clearer and more uniform guidance for digital forensic practice across jurisdictions. Digital forensics has proven essential in modern investigation, whether for digital or conventional crime; its foundation in core principles, structured stages, and the use of valid electronic evidence makes it an indispensable element of law enforcement in the current technological era.

3.6. Clone Disk Procedure and Its Validity in Evidentiary Proceedings

In the process of proving cases of online child sexual abuse, the integrity of digital evidence is of paramount importance. One of the principal methods used in securing and acquiring digital evidence is the disk cloning procedure, a comprehensive copying process performed on a storage device suspected of containing relevant data. This procedure serves not only to preserve data integrity but also to ensure that the resulting copy is admissible as legally valid evidence. Disk cloning is the process of creating an identical copy of the entire contents of a storage medium, such as a hard disk, solid-state drive, or mobile device, in the form of a bitstream image. Unlike ordinary file copying, a bitstream copy encompasses the entire storage sector, including deleted files, unallocated space, hidden partitions, and file system metadata, allowing digital evidence to be duplicated comprehensively without risking alteration or damage to the original data.

Forensically, the disk cloning procedure follows several important stages that must be performed by an authorized investigator or digital forensic expert. The first step involves preparing and securing the necessary digital devices, both hardware and software, along with the media to be cloned, using a write-blocker to ensure the original media cannot be written to or modified during the acquisition process. The next stage involves the cloning process itself, using prepared forensic tools to create a bit-by-bit copy of the original storage medium onto the destination media, encompassing all data including deleted files. Following cloning, a verification process is conducted by calculating and matching hash values (such as SHA-256 or MD5) between the original medium and the resulting copy. The clone is then stored on secure digital media, with the entire procedure documented in detail through a documentation form or examination report to ensure that no bit-level alteration occurred during acquisition (Sachowski, 2003). Figure 2 illustrates the steps involved in the disk cloning procedure:

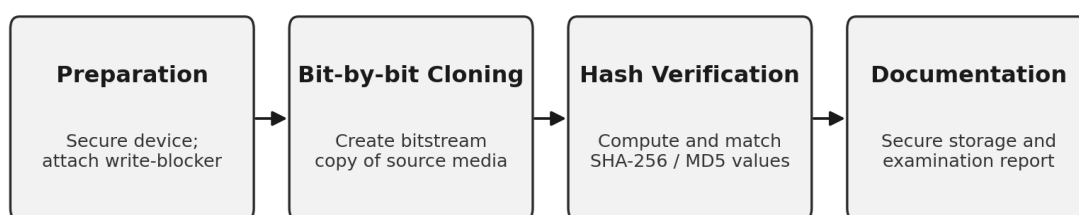


Figure Flowchart of the disk cloning procedure

This entire process is not merely technical in nature but must also be documented administratively as part of the chain-of-custody principle. This documentation serves as proof that the digital evidence presented at trial has not been altered, lost, or contaminated from the moment of its discovery until its use in court. Within the Indonesian legal context, the disk cloning procedure is consistent with Articles 5 and 6 of the ITE Law, which provide that electronic information and/or documents, along with their printed output, constitute legally valid evidence provided that their integrity can be demonstrated and legally accounted for. This is reinforced by the draft Ministerial Regulation of Communication and Informatics on the Initial Handling of Electronic Evidence, which affirms that the acquisition and analysis of digital evidence must be technically testable and legally auditable (Schweitzer, 2003).

Where disk cloning is performed without a lawful procedure or without complete documentation, the validity of the resulting evidence may easily be invalidated at trial. Conversely, where the procedure follows correct standards and can be verified through hash values and an official forensic report, a disk clone attains the status of conclusive evidence. Such a copy may also reveal important evidence, including a perpetrator's communication history, illegal file downloads, and other

digital activity supporting the elements of an offense. A disk cloning procedure that follows international standards and lawful forensic practice forms an essential foundation for preserving the validity and evidentiary strength of digital evidence. In cases of online child sexual abuse, this procedure is often the only means of proving a perpetrator's digital involvement, making it crucial to a fair and accountable judicial process.

3.7. Evidence Acquisition and Securing Process (Chain of Custody)

As previously discussed within criminal procedural law, every piece of evidence submitted to court must satisfy elements of formal and material validity, a requirement equally applicable to digital evidence in cases of online child sexual abuse. One key principle guaranteeing the validity of digital evidence is chain of custody: comprehensive and verified documentation of every stage of possession, transfer, and storage of evidence from the moment of its discovery until its presentation at trial (Ramadhan et al., 2022). Broadly speaking, chain of custody functions to ensure that the digital evidence presented remains identical to the evidence originally discovered by investigators, free from alteration, damage, or manipulation. This principle is especially critical in the digital context, given how easily electronic data can be altered, moved, or modified without leaving a clear physical trace. Figure 3 illustrates the chain-of-custody process:

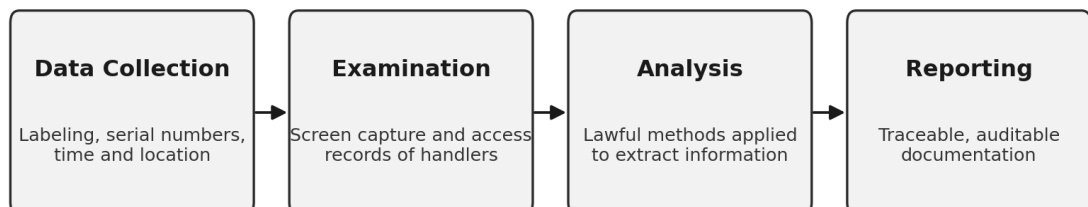


Figure Chain-of-custody process

The chain-of-custody process comprises several key aspects. The first stage is data collection, involving identification, including device labeling, recording of serial numbers, media type, and the location and time of data acquisition from all available sources, to preserve the integrity of the collected data and evidence. The second stage is examination, the documentation of every process undertaken, including screen captures taken throughout the process and records of who first accessed and handled the evidence, as well as everyone involved in its transfer between parties, including the date and time (Andarek, 2025). The third stage is analysis, in which the results of the examination stage are produced; at this stage, legally justifiable methods and techniques are used to obtain information relevant to the questions raised in a given case. The fourth stage is reporting, the documentation of the examination and analysis stages, in which all

documentation must be traceable and auditable by an independent party if required. Chain-of-custody documentation is typically recorded in a form containing the following information:

- 1) Description of the storage medium (type, capacity, condition).
- 2) Date and time of discovery or seizure.
- 3) Name and signature of the forensic officer or investigator.
- 4) Record of transfer history between parties.
- 5) Storage location and access log.

International practice regards chain of custody as a non-negotiable element of the digital forensic process, a principle also reflected in ISO/IEC 27037, which emphasizes the importance of maintaining a documented chain of custody as part of the principles of integrity and accountability. In Indonesia, although the KUHP contains no explicit provision referring directly to the term “chain of custody,” this principle can nonetheless be applied on the basis of the general principle of evidentiary validity, particularly through the application of Articles 5 and 6 of the ITE Law and general principles of criminal procedural law (Casey, 2011). Where chain of custody is not properly implemented, digital evidence may be regarded as legally defective, as it cannot be established with certainty that the data has remained unaltered; defense counsel may exploit this weakness to challenge the validity of the evidence, potentially resulting in its rejection by the presiding judge.

To clarify the procedure for securing and documenting digital evidence through the chain-of-custody system, Figure 3 above illustrates the sequential and documented stages through which digital evidence passes. The acquisition and securing of digital evidence through the chain-of-custody mechanism constitutes an absolute requirement in proving electronic-based criminal offenses. Proper implementation not only preserves evidentiary strength but also reflects a fair, transparent, and accountable legal process.

3.8. Constraints in the Collection and Presentation of Digital Evidence

Although digital evidence is recognized as legally valid within the judicial system, its collection and presentation in cases of online child sexual abuse continue to face numerous challenges, both from internal technical and external factors. One internal technical constraint is the limited understanding and expertise of investigators in information technology, resulting from a shortage of digital forensic specialists. Competent human resources are essential to ensuring the smooth progress of investigation, prosecution, and the eventual apprehension of perpetrators (Saragih & Simamora, 2025). A lack of training and standardized procedures for law enforcement officers presents a further challenge, as not all investigators possess the skills necessary to analyze digital evidence, even as cases

of online child sexual abuse continue to increase. The imbalance between the number of cases and the number of available specialists hampers the investigative process and, in some instances, leaves cases unresolved.

The prolonged duration of investigation and prosecution resulting from limited access to evidence constitutes a further significant obstacle. Lengthy legal processes can delay justice for victims (Suryani et al., 2024). Limited forensic facilities and technology exacerbate the situation, particularly in the collection of evidence relating to online child sexual abuse. Investigators' limited understanding of how to properly acquire, analyze, and present digital evidence further complicates the investigative process. Unlike physical evidence in conventional criminal cases, digital evidence requires specialized handling: errors in handling devices, such as switching off or unplugging an electronic device used by a perpetrator, can result in the loss of stored evidence, while encryption configured by a perpetrator may alter or erase data when accessed by investigators (Frananda et al., 2021).

External constraints in collecting digital evidence in cases of online child sexual abuse have similarly proven difficult, at times causing investigations to stall entirely. Because cybercrime places the crime scene within the digital realm, investigators must conduct online tracing and cooperate with various institutions; where the evidence obtained proves insufficient, the investigation may be forced to halt. The anonymity and use of false identities by perpetrators present a further major obstacle, as offenders can easily create accounts using false names and addresses, relocate, and use sophisticated devices to evade detection. Investigators also face difficulty accessing communication content due to the end-to-end encryption employed by many digital platforms, which further complicates investigation (Noval et al., 2023). Perpetrators frequently erase their digital traces, such as by discarding SIM cards or using self-deleting message features available in applications such as WhatsApp and Telegram. Data fragmentation exacerbates the situation, as digital evidence is dispersed across various formats and devices, including screenshots, file metadata, video recordings, and cloud-stored data, requiring investigators to connect these disparate elements so that the evidence can be assembled coherently and accepted in court.

Law enforcement agencies have adopted various technical measures, both internal and external, to address these constraints. Internally, strengthening human resource capacity remains a priority, through the provision of training to enable investigators to handle cybercrime cases professionally. Strengthening digital investigation facilities and infrastructure, such as digital forensic software and online activity monitoring systems, is essential to support more effective investigation. During the investigative process, investigators must be able to identify electronic evidence at the crime scene and ensure proper seizure procedures to avoid damaging or losing digital data. Securing evidence involves

preliminary documentation, recording within a seizure report, and packaging evidence in accordance with applicable standards. Investigators must promptly secure devices before a suspect can access them and conduct a thorough search of related items; in some cases, the seizure of social media accounts, email accounts, or websites used by a perpetrator is also necessary, including tracing IP addresses to determine the location of devices used.

Cooperation with various stakeholders constitutes an important step in overcoming external constraints. Collaboration with the Ministry of Communication and Informatics and internet service providers is required to detect and remove illegal content (Winiari & Mufid, 2022). Academic institutions and digital forensic experts can also assist in analyzing digital evidence, and evaluating each handled case is important in identifying weaknesses and improving the effectiveness of future investigations. Addressing the challenges of law enforcement against online child sexual abuse requires a comprehensive and adaptive approach. Strengthening investigator competence, developing investigative technology, and fostering inter-agency cooperation are expected to advance efforts to combat this crime more effectively and provide maximum protection for children as a vulnerable group.

4. Conclusion

Digital evidence plays a critical role in proving cases of online child sexual abuse, with different forms, including screenshots, metadata, audio/video recordings, disk clones, and cloud-stored content, carrying varying degrees of evidentiary strength, among which the disk clone stands out as the most conclusive form of proof. The validity of digital evidence depends heavily on adherence to standardized forensic procedures, including URL permanence, the use of write-blockers, hash verification, and comprehensive chain-of-custody documentation, with the ISO/IEC 27037 standard serving as the technical foundation for preserving evidentiary validity through the stages of identification, collection, acquisition, and preservation. Considerable obstacles remain in the evidentiary process, including limited human resources, insufficient technical understanding, and challenges arising from technology and offender anonymity. Digital forensics must therefore be recognized as a vital legal instrument in responding to online sexual crime, requiring strengthened law enforcement capacity, regulatory reform, and cross-sectoral cooperation to ensure that digital evidence can be used lawfully and effectively in court, an essential strategic step in protecting children as a vulnerable group and reinforcing the criminal justice system in the digital era.

5. References

- Adyesta, E. A., Aini, R., Hutasoit, F. P., & Nainggolan, V. (2026). *Analisisyuridis Kekerasaan Seksual Berbasis Elektronik Di Lingkungan Perguruan Tinggi: Sudi Kasus Fakultas Hukum Indonesia Tahun 2026*. 10(2), 1375–1385.

- Afisako, V. P., Rahma, A. N., Sabilla, R. K., Syahnaz, K. F., & Utami, R. A. (2025). Analisi Normatif Terhadap Kekosongan Pengaturan Pedoman Teknis Alat Bukti Elektronik Dalam Penanganan Kasus Kekerasan Seksual Di Indonesia. *Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan*, 2(1 SE-Articles), 228–237. <https://Jurnal.Globalscients.Com/Index.Php/Jkhp/article/View/780>
- Anggraeni, A., Putri, A. H., & Nainggolan, I. L. (2025). Proses Penyidikan Terhadap Pelaku Tindak Pidana Kekerasan Seksual Berdasarkan Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual. *Terduga Pelaku Tindakan Teroris ... Journal Of Law And Security Studies*, 2(2), 187–203. <https://doi.org/10.31599/jlss.v2i2.4463>
- Anggraeni, D. R., & Salsabila, M. (2024). Analisis Yuridis Peran Digital Forensik Dalam Pembuktian Tindak Pidana Di Indonesia. *Media Hukum Indonesia (MHI)*, 2(2), 593. <https://ojs.daarulhuda.or.id/index.php/MHI/article/view/580>
- Charenitha, A., & Firmansyah, H. (2025). A Juridical Analysis Of The Criminal Liability Of Perpetrators Of Online Child Sexual Exploitation. *Awang Long Law Review*, 8(1), 275–282. <https://doi.org/10.56301/awl.v8i1.1910>
- Dewa, I., Renantya, B., & Putra, H. (2023). Perlindungan Hukum Terhadap Hilangnya Objek Gadai Akibat Force Majeure Ditinjau Dari Perspektif Kitab Undang-Undang Hukum Perdata. *Jurnal Kertha Negara*, 11(6), 695–706.
- Duani, N. R., Tamza, F. B., Siswanto, H., & Meidiantama, R. (2026). Penerapan Digital Forensik Oleh Unit Siber Dalam Pembuktian Tindak Pidana Pemerasan Berbasis Sextortion: Studi Pada Kepolisian Daerah Lampung. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 4(3), 2777–2787.
- Gusman, A., Pratama, B. P., & Madjid, N. V. (2026). Penerapan Unsur Tindak Pidana Oleh Penyidik Terhadap Pelaku Eksploitasi Seksual Dengan Korban Anak Melalui Media Sosial. *Unes Journal Of Swara Justisia*, 10(1), 171–179.
- Muhammad Iqbal, Anis En Nabillah, Radhali, R., & T. M. Rafsanjani. (2025). Penerapan Ilmu Forensik Dalam Pembuktian Tindak Pidana Kasus Kekerasan Seksual. *Meukuta Alam : Jurnal Ilmiah Mahasiswa*, 7(1), 75–93. <https://doi.org/10.33059/majim.v7i1.11773>
- NILA ARZAQI, DENY PUSPITASARI, L. N. H. (2025). *DINAMIKA PEMBUKTIAN DALAM DELIK PIDANA KESUSILAAN BERBASIS ELEKTRONIK (CYBER SEXUAL ABUSE) DI INDONESIA* NILA. 4.
- Nova, E. (2025). Implikasi Yuridis Pembuktian Tindak Pidana Kekerasan Seksual Dalam Perspektif Undang-Undang Nomor 12 Tahun 2022 Bagi Pembenuhan Keadilan Korban. *Unes Journal Of Swara Justisia*, 9(1), 208–219. <https://doi.org/10.31933/vfq8k12>
- Okprianti, R., Emilson, N. H., Nurhaliza, Nova, T. E., Rahmawati, P. Y., & Ananda, I. D. (2025). Analisis Perlindungan Hukum Bagi Korban Kekerasan Seksual Berbasis Internet Ditinjau Dari Hukum Pidana Dan Kebijakan Keamanan

- Digital Indonesia. *The Juris*, 9(2), 580–584.
<https://doi.org/10.56301/Juris.V9i2.1982>
- POPA, D. O. L., & Phd. (2025). FORENSIC CHARACTERISTICS OF SEXUAL ABUSE CRIMES AGAINST CHILDREN COMMITTED USING INFORMATION TECHNOLOGIES. *Journal Of Interdisciplinary Cross-Border Studies*, 9(4).
- Popa, L. (2024). NATIONAL AND INTERNATIONAL COOPERATION IN INVESTIGATING CRIMES OF CHILD SEXUAL ABUSE OR SEXUAL EXPLOITATION COMMITTED BY USING INFORMATION TECHNOLOGIES. 2(1), 306–312.
- Ramadani, N. I., & Nur, H. (2026). Analisis Yuridis Pembuktian Digital Dalam Penegakan Hukum Tindak Pidana Kekerasan Dan Pelecehan Seksual Di Indonesia. *Journal Of Law And Justice*, 1, 114–121.
- St. Fatimah, La Ode Husen, N. F. M. (2024). The Juridical Implications Of An Acquittal For The Legal Protection Of Children In Sexual Abuse Cases. *Journal Of Lex Philosophy (JLP)*, 5(1), 260–275.
- Syavica, Z., Sahlepi, M. A., & Rahmayanti. (2025). The Crime Of Child Grooming As Digital Sexual Harassment In The Perspective Of Perpetrator Accountability According To Laws And Regulations In Indonesia. *Journal Of Research In Social Science And Humanities*, 5(3), 1–4.
[Http://dx.doi.org/10.47679/Jrssh.V5i3](http://dx.doi.org/10.47679/Jrssh.V5i3).