Jurnal Daulat Hukum
Volume 9 No. 1, March 2026
ISSN: 2614-560X
SINTA 3 Decree No. 0547/ES/DT.05.00/2024
Dated May 15, 2024

Convergence and Divergence: Strategies for Proving Digital Evidence in Common Law and Indonesian Law Systems

Rommy Hardyansah [1)] & Rio Saputra [2)]
[1*,2)] Faculty of Law, Universitas Sunan Giri Surabaya, Indonesia, E-mail: dr.rommyhardyansah@gmail.com

*Corresponding Author

Abstract. *This literature study conducts a normative comparative analysis of digital evidence adduction strategies in Indonesian civil law and United States common law systems. The research examines the legal construction of authentication, integrity assessment, and the strategic challenges and opportunities in utilizing various digital evidence types, such as chats, emails, CCTV footage, blockchain data, and metadata. Using a qualitative library research method with content and comparative analysis, the study finds that Indonesia's approach is codification-based, placing the judge as an active seeker of material truth who evaluates digital evidence against formal and material requirements stipulated in the Electronic Information and Transactions Law and its implementing regulations. In contrast, the U.S. common law system employs a rigorous adversarial strategy, where digital evidence is tested through extensive discovery and cross-examination, with the judge acting as a procedural gatekeeper under the Federal Rules of Evidence. The core difference lies in the locus of substantive evaluation: Indonesian judges assess probative value directly, while common law juries do so after judicial admissibility screening. The study concludes that both systems are converging on the necessity of technical expertise but recommends that Indonesia enhance judicial digital literacy and consider limited e-discovery mechanisms to strengthen its evidentiary framework.*

Keywords: *Authentication; Common Law System; Digital Evidence; Digital Forensics; Indonesian Legal System; Judge's Role; Proof Strategy.*

1. Introduction

The evolution of information and communication technology has fundamentally transformed the landscape of human interaction, commercial transactions, and data recording. This shift is not merely social or economic; it has extended into the legal domain, particularly concerning evidence in judicial proceedings. The traditional concept of physical and analog evidence, such as letters, deeds, or direct witness testimony, now confronts a new reality of intangible yet decisive digital traces. Digital evidence, manifested as electronic messages, digital financial transaction records, closed-circuit surveillance video footage, or data recorded on a blockchain, has become a crucial component for uncovering material truth in court (Abdullah et al., 2025). Its existence can prove or refute a legal claim with a level of detail and accuracy

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

often unattainable by conventional evidence. This signifies a paradigmatic transition in the law of evidence, from the era of paper documents to the era of continuously flowing and evolving electronic data.

The characteristics of digital evidence that fundamentally distinguish it from traditional evidence create unique legal challenges. Digital evidence is volatile, easily replicated, modified, or destroyed with a few clicks. It is also systemic, meaning its existence and significance are highly dependent on the hardware, software, networks, and protocols that create, store, or transmit it. This soft and mutable nature directly confronts the principles of evidence law built on the foundation of a piece of evidence's authenticity, integrity, and reliability. The authentication process, proving that the digital data indeed originates from the claimed source and has not been altered since its creation, becomes a complex technical and legal problem (Mohsin & Asthana, 2024). Similarly, determining its relevance and probative weight is challenging, as digital data is often fragmentary and requires expert interpretation to connect it to the disputed legal facts.

Regulations across various jurisdictions strive to catch up with the rapid pace of technological development (Rahman et al., 2024). In common law systems, particularly in the United States, the Federal Rules of Evidence (FRE) have adopted amendments to accommodate electronic evidence. Rule 901 concerning authentication requirements and Rule 902 concerning evidence that is self-authenticating have become important references. Meanwhile, the Indonesian legal system, which adheres to the civil law tradition, possesses its own positive law framework. Recognition of electronic evidence is explicitly granted in Law Number 11 of 2008 concerning Electronic Information and Transactions (the ITE Law) and its amendments, as well as in criminal and civil procedural law (Aryadi et al., 2024; Mujisulistyo et al., 2024). However, these regulations often remain general and require further elaboration through jurisprudence and technical standards. The philosophical differences between the adversarial common law system and the inquisitorial-elective civil law system also influence how digital evidence is presented, examined, and assessed in court.

The scope of digital evidence is vast, encompassing various forms and sources. Instant messages such as WhatsApp or Telegram conversations have become commonplace evidence in civil cases like contract breaches or criminal cases such as threats and fraud. Email with its metadata can prove employment relationships, agreements, or the dispatch time of important documents. Closed-circuit television (CCTV) recordings are often key evidence in criminal acts like theft, assault, or traffic accidents. Data from blockchain, with its decentralized and difficult-to-manipulate nature, is beginning to be submitted as evidence in financial and digital property disputes. Each type of this digital evidence has distinct technical characteristics, vulnerabilities, and methods of preservation and forensic analysis, all of which legal practitioners must understand to utilize it effectively (Sujatmiko & Soesatyo, 2025).

Therefore, a systematic and comparative study of evidentiary strategies using digital evidence is required. This study must bridge the technical knowledge of digital forensics with the applicable principles of evidence law. Its focus is on analyzing the formal and material

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

requirements that must be met for digital evidence to be considered admissible and to possess probative force in court. Formal requirements concern the procedures for collection, seizure, and presentation in accordance with procedural law. Material requirements concern the substance of the evidence itself; namely, how to prove its authenticity, integrity, and relevance to the case. A comparison with the common law system, which has longer experience and more mature doctrines in this regard, can provide valuable lessons and an evaluative framework for refining digital evidentiary strategies within the Indonesian legal system, both in civil and criminal trials.

The most fundamental first challenge is the misalignment between the speed of digital technological innovation and the pace of legal formation and interpretation. Written regulations, such as the ITE Law, often only provide general recognition of electronic information as admissible evidence, without offering detailed technical guidelines on authentication and integrity standards (Darmawan & Negara, 2023; Sukmasari et al., 2024). This causes legal uncertainty in practice. Judges, prosecutors, and lawyers, whose professional expertise is in law, are forced to assess evidence whose understanding requires technical competence in computers and networks. Meanwhile, digital forensic experts who understand the technical aspects often lack a deep understanding of the legal standards of proof that must be met. This knowledge gap potentially leads to two outcomes: the rejection of actually valid digital evidence due to ignorance, or the admission of digital evidence that is technically and legally flawed.

Another problem lies in the procedures for collecting and presenting digital evidence that satisfy procedural law requirements. In Indonesian criminal procedure law, the seizure of physical evidence is specifically regulated. However, what constitutes a lawful seizure procedure for digital data stored on overseas cloud servers or on personal devices protected by passwords and encryption? The principle of chain of custody, the series of documentation proving that digital evidence has not been altered, tampered with, or falsified from the moment of discovery until its presentation in court, becomes crucial yet difficult to implement perfectly (Dewi et al., 2024). Every file transfer, format conversion, or forensic analysis risks altering the metadata or hash value of the original data. In civil trials, where parties submit evidence, issues such as data storage by third-party intermediaries and privacy consent also become substantial obstacles to obtaining and submitting desired digital evidence.

A further problem relates to the assessment and weighting of evidence by judges. Even after digital evidence is declared formally admissible, the question of its precise probative force remains an area of interpretation. How does a judge assess the reliability of a CCTV recording with low image quality or that may have been edited? How does one test the authenticity of a chat conversation saved as a screenshot, which is extremely easy to falsify? Differences in legal system approaches also influence this. In the adversarial common law system, testing of digital evidence is conducted rigorously through cross-examination of experts and the discovery process (Billah & Saragih, 2025). Meanwhile, in the Indonesian system, judges have a dominant role in examining and assessing evidence. This difference demands different

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

evidentiary strategies and legal arguments, and methods effective in one system are not necessarily directly applicable in the other.

The volume and variety of disputes and criminal acts involving digital elements continue to increase exponentially. Civil cases such as electronic contract disputes, violations of intellectual property rights in the digital world, or defamation through social media have become common occurrences in courts. In the criminal realm, modes of cybercrime, online fraud, hate speech, and online narcotics trafficking are increasingly prevalent (Ali et al., 2024). In all these cases, digital evidence is often the sole or primary evidence that can uncover the truth. Without adequate understanding and digital evidentiary strategies, law enforcement efforts and the achievement of justice will be seriously hindered. Courts risk rendering decisions not based on the best available evidence, or even failing to process cases due to technical difficulties in proof.

The development of new technologies such as artificial intelligence, the Internet of Things (IoT), and blockchain further underscores the need for this study. Data generated by IoT devices, logs from AI-based systems, or transaction records on blockchain represent more complex forms of digital evidence requiring more advanced forensic analysis methods. The legal system must prepare now for the next wave of digital evidence. In-depth academic study is needed to map the characteristics of these new forms of evidence, identify emerging legal challenges, and formulate evidentiary principles that can remain relevant amidst technological change. Without academic anticipation, the justice system will perpetually be in a reactive and lagging position, which may ultimately undermine public trust in the law.

At the global level, there has been some harmonization and standardization effort concerning digital evidence, for instance through conventions like the Budapest Convention on Cybercrime. Indonesia, as part of the international community, needs to adapt and align its digital evidentiary practices with widely recognized standards, while of course considering the specificities of its domestic legal system. Comparative legal study, particularly with common law jurisdictions like the United States which have more established doctrinal and practical developments, provides a critical perspective and a valuable source of learning. Understanding the principles within the Federal Rules of Evidence can aid in interpreting and developing similar provisions in Indonesian law, so that digital evidence is not only valid domestically but can also be recognized in international legal cooperation.

This literature study aims to critically and comparatively analyze evidentiary strategies using digital evidence in civil and criminal trials. Specifically, this research first seeks to delineate and compare the legal construction regarding authentication requirements and integrity assessment of digital evidence within the Indonesian legal framework (especially the ITE Law and procedural law) with the common law system as reflected in the United States Federal Rules of Evidence. Second, this research intends to identify, categorize, and analyze the concurrent technical and legal challenges and opportunities arising from the use of various types of digital evidence such as chat logs, email, CCTV recordings, blockchain data, and metadata in trial proceedings. Third, this research aims to compare evidentiary strategies and

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

the role of judges in assessing digital evidence between the adversarial common law system and the Indonesian legal system, examining the implications for the effectiveness of the search for material truth. Theoretically, this study is expected to contribute to the development of a more systematic and adaptive doctrine of digital evidence law. Practically, the results of this research are expected to serve as a guideline for judges, prosecutors, lawyers, and digital forensic experts in designing and implementing evidentiary strategies that are lawful, reliable, and effective in court.

2. Research Methods

This research is designed as a qualitative literature study that is exploratory, descriptive, and comparative. This study does not involve the collection of primary empirical field data but relies entirely on in-depth analysis of secondary data in the form of existing written sources. The literature study approach was chosen because it aligns with the research objectives of building a comprehensive conceptual understanding, mapping doctrinal developments, and conducting systematic legal comparison of a complex and rapidly evolving legal issue. As explained by John W. Creswell in his book on qualitative research design, literature study research allows the researcher to investigate a problem by delving into various theoretical perspectives and previous findings, thereby enabling the identification of knowledge gaps and the formulation of new syntheses. Thus, this research relies on the strength of analyzing legal and academic texts to produce robust arguments.

The secondary data employed in this study is classified into three principal categories based on its nature and authority. The first category comprises primary legal sources, which encompass applicable statutory regulations. These sources include the Indonesian Criminal Procedure Code (Kitab Undang-Undang Hukum Acara Pidana or KUHAP), the Indonesian Civil Procedure Code (Herziene Inlandsch Reglement/Reglement op de Burgerlijke Rechtsvordering or HIR/RBg), Law Number 11 of 2008 concerning Electronic Information and Transactions (the ITE Law) and its amendments, along with related technical regulations. For comparative analysis, primary legal documents from a common law jurisdiction, specifically the United States Federal Rules of Evidence (FRE), also constitute an object of analysis. The second category consists of secondary legal sources. These include textbooks on the law of evidence, information technology law, and digital forensics; scholarly articles from reputable national and international law journals; and expert commentaries on judicial jurisprudence from both Indonesia and foreign jurisdictions such as the United States and the United Kingdom. The third category is supporting sources. This encompasses publications from professional bodies like the American Academy of Forensic Sciences and technical guidelines from institutions such as the National Institute of Standards and Technology (NIST) concerning digital forensic standards.

The analytical techniques applied are qualitative content analysis and comparative normative legal analysis. Content analysis is utilized to systematically examine written sources in order to identify patterns, themes, key concepts, and the development of arguments regarding digital evidence. This process involves the stages of coding the text, categorizing it based on

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

emergent themes (such as "authentication challenges," "formal requirements," "the judge's role"), and interpreting the data to uncover relationships and meanings behind these categories. Comparative normative legal analysis is conducted using the method of functional comparison, as developed by comparative law scholars. This method entails comparing not only regulatory texts but also the function and application of digital evidence principles in resolving similar legal problems across two distinct legal systems. The entire analytical process is iterative, involving repeated, critical readings and reviews of sources to ensure the consistency, depth, and validity of the findings. This research strives to synthesize findings from diverse sources to construct a coherent analytical narrative, address the research questions, and ultimately provide a meaningful contribution to the development of legal science.

3. Results and Discussion

3.1. The Legal Construction of Digital Evidence Authentication and Integrity: A Comparative Analysis

The legal construction concerning the authentication and integrity of digital evidence within the Indonesian legal system is built upon a multi-layered foundation that combines general procedural law with specialized regulations in information technology. The most fundamental layer is found in the Criminal Procedure Code (KUHAP). Article 184 of the KUHAP enumerates admissible forms of evidence: witness testimony, expert testimony, documents, indicia, and defendant statements. At the time of its drafting, the concept of digital evidence was naturally inconceivable; consequently, its classification requires extensive interpretation. Electronic mail or digital documents are often subsumed under the categories of "documents" or "indicia." However, this analogical interpretation creates uncertainty because it does not explicitly regulate the unique characteristics of digital evidence, such as its volatility and systemic dependency. To fill this lacuna, specialized legislation emerged through Law Number 11 of 2008 concerning Electronic Information and Transactions (the ITE Law). Article 5 Paragraph (1) of the ITE Law constitutes a vital normative leap, stating that Electronic Information and/or Electronic Documents and their printouts are legally admissible evidence (Negara & Darmawan, 2023; Sidabutar et al., 2024). This explicit recognition provides a strong formal foundation, yet simultaneously burdens the system with the obligation to define authentication and integrity parameters for an intangible entity.

Formal authentication requirements within the Indonesian system are principally governed by Article 6 of the ITE Law. This article stipulates that Electronic Information and/or Electronic Documents are deemed authentic provided the information is accessible, displayable, its integrity assured, and it is accountable so as to elucidate a particular circumstance. The phrasing "its integrity assured" and "accountable" constitutes the key formal requirements. The implementation of this integrity assurance is subsequently detailed in implementing regulations. Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE) provides a more operational technical framework. Article 59 of the PP PSTE specifies that authentication of Electronic Information

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

can be accomplished using electronic signatures, electronic time stamps, or other similar accountable technologies. A qualified electronic signature under this regulation is one that utilizes an electronic certificate issued by an accredited Electronic Certification Provider (Penyelenggara Sertifikasi Elektronik or PSrE) (Noor, 2024). Thus, the formal authentication requirement in Indonesia shifts from mere physical proof towards verification relying on a public key infrastructure and a trusted certification authority. Digital evidence accompanied by a valid, qualified electronic signature is considered to have met the preliminary formal authentication requirement.

However, fulfilling these formal requirements is often insufficient or not always possible, particularly for digital evidence generated in everyday interactions, such as chat messages or CCTV recordings, which do not employ certified electronic signatures. It is here that the material requirements for authentication and integrity assessment assume a more significant role. The material requirement no longer resides solely in the technical attributes inherent to the evidence itself but in the trial process of persuading the judge regarding the evidence's origin and integrity. The primary instrument for satisfying this material requirement is the testimony of a digital forensic expert, recognized as admissible evidence under Article 184 of the KUHAP. The digital forensic expert's task is to explain to the judge the data acquisition methodology, the use of write-blockers to prevent modification, the calculation of hash values (such as MD5 or SHA-256) as digital fingerprints, and the analysis of metadata to trace origin and creation time (Dhumillah, 2024). This process is, in essence, the demonstration of digital evidence integrity and provenance through scientific explanation, thereby substituting for or complementing formal authentication via electronic certificates.

The legal construction within the common law system, particularly in the United States under the Federal Rules of Evidence (FRE), is built upon a different philosophy and mechanism, albeit with a similar ultimate objective (Freckelton, 2016). The core rule governing authentication is FRE Rule 901(a). This rule establishes a general requirement: to satisfy the requirement of authenticating an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it to be (Losavio, 2020). This is a relatively low threshold, not absolute certainty, but sufficiency to support a finding. Rule 901(b) provides illustrative examples of authentication methods, many of which are highly relevant for digital evidence, such as testimony from a person with knowledge that an item is what it is claimed to be (b)(1), or identification based on distinctive characteristics of voice, text messages, or email (b)(4 and 5). The FRE approach is more pragmatic and grounded in trial facts, compared to the Indonesian approach which initially emphasizes compliance with normative technical standards like certified electronic signatures (Hardinanto et al., 2023).

The FRE also recognizes the concept of self-authentication through Rule 902. Certain categories of documents, including printouts of data accompanied by a certification from a custodian or other qualified person stating the printout is accurate, can be admitted as evidence without requiring foundational testimony to prove authenticity (Bahri et al., 2024). This concept parallels the idea of certified electronic signatures in Indonesia, but its application in U.S. court practice is more flexible. Furthermore, the assessment of digital

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

evidence integrity and reliability is significantly influenced by FRE Rule 403, which authorizes the judge to exclude evidence if its probative value is substantially outweighed by the danger of unfair prejudice, confusing the issues, or misleading the jury. For digital evidence susceptible to manipulation, judges will rigorously assess whether the storage and presentation methods have preserved its integrity such that its probative value is not outweighed by the risk of misleading.

A fundamental difference is evident in the emphasis placed on the chain of custody. In common law practice, particularly in criminal proceedings, the chain of custody constitutes a critical evidentiary element and is frequently a primary target for defense challenges (O'Sullivan, 2023). Every individual who handles the digital evidence, from the first investigator to the laboratory forensic expert, must be identifiable and accountable for each stage. The absence or weakness in chain of custody documentation can be grounds for the suppression of evidence. Within the Indonesian system, although the concept of chain of custody is acknowledged in investigative guidelines and taught in forensic science, its legal force as an absolute prerequisite for admissibility is not as robust as in common law (Komalasari & Mustafa, 2023). Its assessment more often forms part of the judge's overall consideration regarding the quality of expert testimony and other evidence, rather than serving as a determinative threshold for admissibility.

Another regulation influencing the construction in Indonesia is Law Number 27 of 2022 concerning Personal Data Protection (the PDP Law). This law introduces a new dimension in assessing the validity of digital evidence. Article 65 of the PDP Law regulates that the use of personal data for law enforcement purposes must be conducted in accordance with prevailing laws and regulations. If digital evidence constituting personal data (such as message content, location, or communication history) is obtained through means that violate the provisions of the PDP Law, for instance without a legal basis or valid consent, the legality of obtaining such evidence can be challenged (Manurung & Harefa, 2024). This creates the possibility of excluding unlawfully obtained digital evidence (an exclusionary rule), a concept also developed in common law jurisprudence (for example, through the Fourth Amendment). Thus, the integrity of digital evidence pertains not only to its technical immutability but also to the legality of its acquisition process (Rowe, 2016).

From this comparison, it can be observed that the Indonesian legal system tends to commence from an ideal normative regulation, prioritizing technical standards such as qualified electronic signatures. When this ideal standard is unfulfilled, the system then relies on the material proof pathway through expert testimony to establish authentication and integrity at trial. Conversely, the U.S. common law system focuses directly on judicial proof as the primary arena for establishing authentication, with Rule 901 as its gatekeeper (Plaxton & Sankoff, 2023). The common law system relies more heavily on the adversarial process, where each party strives to prove or disprove the evidence's authenticity through cross-examination of witnesses and experts, while the judge or jury acts as the arbiter and final evaluator (Fernando et al., 2025).

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

Ultimately, both systems must confront the same technical reality and are moving toward a convergence of principles. The Indonesian system is learning to place greater value on the trial proof process and the potential for excluding unlawfully obtained evidence (Setiawan & Hartiwiningsih, 2025). The common law system, on the other hand, also adopts certain technical standards and certifications to enhance efficiency and reliability (Monique et al., 2024). The core of both legal constructions is the recognition that the authority and credibility of digital evidence cannot be taken for granted. That authority must be constructed, either through state-regulated legal and technical infrastructure (such as PSrE in Indonesia) or through rigorous testing in the judicial arena. The choice between a more preventive-normative approach versus a more corrective-adversarial one reflects differing legal traditions; however, their final objective remains identical: to ensure that the digital evidence forming the basis of a legal decision is reliable, intact, and genuinely originates from the claimed source.

3.2. Challenges and Opportunities in Utilizing Various Types of Digital Evidence in Court

The submission and examination of digital evidence in the form of chat conversations and email face dual technical and legal challenges. Technically, both are data that can be easily replicated, modified, or fabricated with simple software. A screenshot of a WhatsApp conversation or a copy of an email can be readily altered before being submitted to court. The legal challenge lies in proving that the submitted evidence truly constitutes the communication that occurred between the disputing parties. This is where the ITE Law plays a crucial role, as Article 5 Paragraph (1) provides legal recognition. However, this recognition is conditional, as elaborated in Article 6, upon the ability to assure integrity and accountability. The strategic opportunity, in fact, lies in the exploitation of attached metadata. Every chat message and email contains ancillary data such as timestamps (send/receive times), sender IP addresses, routing headers, and device identifiers. This metadata, when analyzed by a digital forensic expert, can construct a robust narrative regarding authenticity and chronology, and can identify anomalies indicative of fabrication, thereby transforming the challenge of integrity into an opportunity for deeper, more credible proof (Budianto et al., 2024).

Closed-circuit television (CCTV) recordings offer compelling visual evidence, yet the challenges center on issues of continuity of handling and file integrity (Deviriana et al., 2025). Raw footage from cameras is typically stored in proprietary compressed formats on digital video recording devices. The processes of extraction, format conversion for examination purposes, and storage are highly susceptible to interference that can compromise its integrity. The chain of custody problem becomes crucial here. If it cannot be proven who accessed the recording file from the moment of seizure at the location until its presentation in court, its validity can be undermined by allegations of contamination or tampering (Santosa & Kamali, 2022). The legal framework for this relies not only on the general provisions of the Criminal Procedure Code but also on the internal standards of law enforcement agencies, such as the Indonesian National Police Chief Regulation on Evidence Management Procedures. The emerging strategic opportunity lies in the development of cloud-based storage technologies with immutable access logs and the application of hashing technology directly at the recording device. These

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

innovations can create an automatic, more easily auditable digital chain of custody, thereby strengthening the position of CCTV footage as reliable evidence.

Data from blockchain technology introduces a unique paradigm for digital evidence due to its distributed nature and cryptographic protection from alteration. Its primary challenge stems precisely from its novelty and technical complexity, which complicates understanding for judges and legal parties. The evidence submitted is not the transaction data itself stored on a public blockchain like Bitcoin or Ethereum, but rather a representation or certification of that data. Existing regulations, such as the ITE Law and Government Regulation Number 71 of 2019, do not yet specifically set standards for proving blockchain data. The legal challenge is formulating an authentication method acceptable to the court to prove that a claimed hash indeed refers to a specific transaction within a given blockchain at a specific time. The strategic opportunity, however, is immense. The immutable nature of blockchain means that once data is recorded, it cannot be altered without changing all subsequent blocks, a feat that is computationally near-impossible. This makes it an ideal tool for proving the existence of a document, digital contract, or transaction record at a particular time, which is invaluable in civil disputes concerning intellectual property rights, digital asset ownership, or tracing fund flows in money laundering criminal cases (Hadinoto et al., 2025).

Metadata, or data about data, often constitutes the most overlooked yet most informative form of digital evidence. Its greatest challenge is its invisibility and the requirement for specialized tools and expertise for extraction and interpretation. Within a document file, metadata can store revision history, the name of the original author, the device used, and even geolocation coordinates if the document was a photo taken with a mobile phone. In legal proceedings, overlooking metadata means losing a layer of proof that can confirm or refute testimony. The opportunity lies in its correlative power. Email metadata can trace the server route traversed, proving where an email was actually sent from, not merely the sender's address which can be spoofed. Metadata from photos or videos can prove the time and location of capture, which is crucial in alibi cases. Effective use of metadata requires either an amendment or a progressive interpretation of Article 184 of the Criminal Procedure Code and Article 5 of the ITE Law to explicitly recognize the results of metadata analysis as part of admissible "expert testimony" with independent probative force (Puspita et al., 2025).

In civil trials, a specific challenge arises from the lower standard of proof (prima facie) compared to criminal cases, coupled with constraints related to ownership of and access to digital evidence. One party may hold key digital evidence, such as emails or chat logs, on servers owned by service providers (like Google or Meta) or on personally encrypted devices. The legal process to obtain such evidence can be protracted and complex. Law Number 30 of 1999 concerning Arbitration and Alternative Dispute Resolution, along with Civil Procedure Law, lacks a discovery mechanism as extensive as that in common law systems. A strategic opportunity lies in the early use of digital evidence in mediation or arbitration processes, where formalities can be more flexible. Furthermore, courts can begin to adopt or refer to evolving international practice standards, such as The Sedona Principles, which provide

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

guidance on e-discovery, to resolve cross-border commercial disputes involving large volumes of digital evidence.

In criminal trials, challenges are compounded by the demands of the suspect's human rights and stringent procedural rules. The collection of digital evidence such as mobile phone contents or private communication recordings is highly susceptible to intersecting with privacy rights. Law Number 27 of 2022 concerning Personal Data Protection (the PDP Law) now serves as a significant legal barrier. Article 20 of the PDP Law restricts the processing of personal data, including for law enforcement purposes, which must have a clear legal basis. Investigators who extract data from a suspect's mobile phone without a valid seizure warrant or without observing the principle of proportionality risk violating the PDP Law (Fernando et al., 2025). The challenge is to find a balance between investigative needs and respect for privacy. The opportunity is that the PDP Law compels law enforcement officials to better document the digital evidence acquisition process in accordance with legal procedures, which ultimately strengthens the legality and admissibility of that evidence in court and protects the process from nullification due to procedural violations.

One major challenge with digital evidence, regardless of its form, is ensuring judges and other legal professionals have the capacity and digital literacy to handle it. Since judges are the final arbiters of fact in a case, they need a working grasp of fundamental digital concepts like hashing, metadata, and encryption. This understanding is essential for them to properly evaluate expert witness statements and ask the right questions. Without this literacy, a significant risk exists: judges may uncritically accept inadequate expert testimony or, conversely, reject valid digital evidence due to a lack of understanding. The long-term strategic opportunity lies in reforming legal education and implementing mandatory continuing training programs for prospective and sitting judges. Institutions like the Supreme Court's Judicial Training Center need to integrate modules on information technology law and basic digital forensics into their core curriculum (Poor Mollaei et al., 2024). Such efforts would build judicial confidence in handling digital evidence and lead to more consistent and well-founded jurisprudence.

The greatest underutilized strategic opportunity is leveraging digital evidence to build a preventive and predictive evidentiary system. In civil law, smart contract clauses executed on a blockchain can automatically record and even enforce contractual terms, meaning evidence of default or performance is available objectively and is difficult to dispute. In criminal law, analysis of communication metadata patterns or digital financial transactions can be used to build strong preliminary evidence to support requests for wiretaps or seizures. Regulations like the Government Regulation on the Implementation of Electronic Systems and Transactions have already opened the door for recognizing electronic signatures and time stamps. The opportunity lies in promoting the widespread adoption of these foundational technologies in both the public and private sectors. This would create a digital evidence environment that is inherently more trustworthy, easier to authenticate, and ready for submission to court, thereby transforming the evidentiary landscape from reactive to proactive (Pangabean & Kemala, 2025).

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

3.3. Digital Evidence Strategies: A Comparison of the Judge's Role in Common Law and Indonesian Systems

A comparison of digital evidence strategies between the adversarial common law system and the Indonesian legal system reveals profound philosophical differences concerning how truth is adjudicated and the role of judicial institutions (Fernando et al., 2025). In the common law system, particularly as applied in the United States, evidentiary strategy is built upon the foundation of a pure adversarial process (Fletcher & Sheppard, 2005). Its underlying philosophy is that truth is best revealed through confrontation and rigorous testing between two opposing parties, each with a strong motivation to present its best version of the facts and expose the weaknesses of the opponent. In the context of digital evidence, this strategy is manifested through two main phases: discovery and trial. The discovery phase is governed by extensive procedural rules (such as the Federal Rules of Civil Procedure), which obligate the parties to mutually share relevant information and documents, including electronic data (Rofiqi et al., 2025). During this phase, parties aggressively use document requests, interrogatories, and requests for admission to collect and scrutinize the opponent's digital evidence. The judge in this phase acts as an overseer who ensures the process is fair and resolves disputes regarding the scope of discovery but does not actively engage in evidence gathering.

Once a case proceeds to trial, the strategy shifts to focus on issues of admissibility and probative weight. The governing rules are the Federal Rules of Evidence (FRE). The party seeking to introduce digital evidence (the proponent) must first lay a foundation for its admission by proving authentication as stipulated in Rule 901. This is typically accomplished through witness testimony, which may come from a user familiar with the system, a network administrator, or most commonly, a digital forensic expert (Billah & Saragih, 2025). After the foundational authentication is established, the opposing party (the opponent) has a full opportunity to attack the validity of the evidence through intensive cross-examination of that expert witness, questioning the methodology, tool reliability, or potential for contamination. The judge acts as a gatekeeper, determining whether the admissibility requirements are met based on the arguments presented. FRE Rule 702 and the landmark Daubert v. Merrell Dow Pharmaceuticals decision empower judges to assess whether an expert's methodology is scientifically valid and applicable to the facts of the case. However, once evidence is deemed admissible, the final assessment of its weight and credibility is left entirely to the jury (in certain criminal and civil cases) as the trier of fact. Thus, the evidentiary strategy in common law is a contest of technical and legal argumentation heavily reliant on the skill of attorneys and the credibility of their experts, with the judge serving as a procedural referee and the jury as the ultimate substantive evaluator (Edward & Ojeniyi, 2019).

Conversely, the evidentiary strategy within the Indonesian legal system, which adheres to a civil law tradition with inquisitorial elements, is built upon a different premise (Wisnubroto et al., 2025). Its underlying philosophy positions the judge as an active seeker of material truth. This system places less emphasis on a contest between the parties and more on the judge's duty to uncover the truth. The evidentiary strategy is conceptually more structured and driven

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

by judicial authority. Its normative basis is clear codification. Article 184 of the Criminal Procedure Code (KUHAP) enumerates admissible forms of evidence, and Article 5 of the Electronic Information and Transactions Law (ITE Law) provides specific recognition for electronic evidence (Kholis et al., 2023). However, these regulations are not followed by comprehensive e-discovery procedural rules as in the United States. Consequently, the initial digital evidence collection strategy heavily depends on the initiative and capacity of law enforcement officials (investigators) in criminal cases, or on the parties independently gathering and submitting evidence in civil cases, with the judge retaining the authority to order the presentation of evidence.

The role of the Indonesian judge in evaluating digital evidence is far more active and substantive than that of their common law counterpart who acts as a gatekeeper. Under KUHAP Article 183, a criminal judge may not impose a sentence except based on a minimum of two valid pieces of evidence and their own conviction. The phrase "the judge's conviction" is central. The judge does not merely decide whether evidence may be presented (admissible) but is also obligated to conduct an in-depth assessment of its probative value to reach that conviction. In practice concerning digital evidence, this requires the judge to critically examine the testimony of digital forensic experts presented, whether by the prosecutor or the defense. The judge can, and is often expected, to pose questions directly to the expert to test their understanding and the consistency of their explanation. The judge serves as the primary examiner, not merely a moderator of a debate between prosecution and defense experts. In civil cases, although there is no two-evidence requirement, the judge still possesses broad authority to order an on-site inspection, summon additional experts, or even appoint their own expert (from the court's list of experts) to assist in evaluating complex digital evidence, as regulated in the Civil Procedure Code (HIR/RBg) (Gunarto et al., 2023).

The strategy of the parties within the Indonesian system also differs due to the absence of a comprehensive discovery process and a sharply distinct trial phase. Lawyers in civil cases must submit all digital evidence together with the lawsuit or the answer, or within a timeframe set by the judge. Opportunities to request additional digital evidence from the opposing party during the trial process are more limited (Revanoor, 2022). Therefore, evidentiary strategy is more defensive and anticipatory, focusing on building a strong evidentiary dossier from the outset and relying on the judge's ability to independently discern weaknesses in the opposing party's evidence. Attorneys rely less on destructive cross-examination techniques to nullify the opponent's digital evidence and depend more on their own expert's explanation and written arguments to shape the judge's conviction.

This difference yields varied approaches to handling technical issues such as chain of custody and reliability standards. In the common law system, chain of custody is a primary line of defense invariably attacked by the defense. If this chain is broken or its documentation is poor, the defense will file a motion to suppress the evidence (Monique et al., 2024). The judge will rule on that motion based on the arguments from both sides. In the Indonesian system, lapses in the chain of custody do not automatically render evidence inadmissible. They become one factor among many the judge considers in forming their conviction. The judge may decide that

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

despite imperfect chain of custody documentation, based on hash value analysis and expert testimony, the digital evidence remains reliable. This decision constitutes a substantive consideration regarding the weight of evidence, not a procedural ruling on admissibility.

The impact of this strategic difference on trial outcomes can be significant. The common law system, with its adversarial process and rigorous cross-examination, may be more effective at exposing methodological flaws or bias in a specific expert (Monaco, 2020). However, this system also heavily depends on the resources of the parties; a party with limited resources to hire the best digital forensic expert may lose in this technical contest. The Indonesian system, with an active judge potentially assisted by a court-appointed expert, holds the potential for greater fairness in terms of access to expertise, as the court can appoint a neutral expert. However, this system places a substantial burden on the competency and digital literacy of the individual judge. If a judge lacks sufficient understanding of digital forensics fundamentals, their ability to assess expert credibility and form a proper conviction can be called into question.

In reality, both systems are moving towards a certain convergence in response to the complexity of digital evidence. The common law system, through FRE amendments and court rulings, continues to refine rules on e-discovery and expert testimony, reducing the potential for abuse of the process by more powerful parties. The Indonesian system, through Supreme Court jurisprudence development and outreach, strives to elevate judicial assessment standards and encourage more standardized use of experts. The clearest point of convergence is the recognition that independent technical expertise and accessible explanation are key to evaluating digital evidence in any system. There is still a fundamental difference at play. Under common law, that kind of expert knowledge must withstand the intense pressure of an adversarial trial. In Indonesia, however, a judge evaluates the expertise as part of their own investigation to uncover the factual truth. How a lawyer chooses to present their evidence is still a direct response to this deep-seated contrast in the judge's function, which shifts from being a neutral referee in a legal battle to an active seeker of answers.

Therefore, the ultimate challenge for any legal system is not merely to incorporate digital evidence procedurally, but to cultivate a judiciary and a bar that are both critically engaged with the technical realities of the evidence and consciously aware of the philosophical underpinnings of their own adjudicative role, ensuring that the pursuit of justice is neither obscured by procedural combat nor hampered by a lack of foundational understanding. This dual competence is essential for maintaining the legitimacy of court decisions in the digital age. A failure to build this capacity risks undermining public trust, as verdicts may appear detached from the technological realities that shape modern disputes. Ultimately, the law can only deliver on its core promise of fair and authoritative justice when those who interpret and argue it truly understand the digital proof upon which cases increasingly rest.

4. Conclusion

Based on the comparative analysis conducted, it can be concluded that the legal construction and evidentiary strategies for digital evidence within the Indonesian legal system and the

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

United States common law system are shaped by different legal paradigms, yet both strive to address identical technical challenges. In the Indonesian system, the approach is codificatory and positions the judge as an active seeker of material truth. The validity of digital evidence rests on fulfilling the formal and material requirements stipulated in the ITE Law, its implementing Government Regulation (PP PSTE), and criminal and civil procedural law, with digital forensic expert testimony serving as the judge's primary tool for forming their conviction. Meanwhile, the common law system adheres to a rigorous adversarial strategy, where truth is expected to emerge from the clash of arguments between the parties. The authentication and reliability of digital evidence are tested in depth through an expansive discovery process and cross-examination at trial, with the judge functioning as a procedural referee and gatekeeper of admissibility based on the Federal Rules of Evidence. The fundamental difference lies in the locus of evaluation: in Indonesia, substantive assessment of evidentiary weight resides with the judge; in common law, after passing the judicial gate, substantive assessment is entrusted to the jury. The implications of this comparison are multidimensional. For the development of Indonesian law, these findings indicate that the system's success heavily depends on two pillars: the capacity and digital literacy of judges, and the availability and standardization of digital forensic expertise. Without continuous enhancement of judicial capacity, the risk of error in assessing complex digital evidence will remain high. This implication underscores the necessity of integrating information technology law education into judicial training curricula and mandatory continuing education programs. On the other hand, the common law system faces implications concerning inequality in access to justice, where parties with greater financial resources can dominate the process through superior forensic expertise and complex litigation tactics. For legal practitioners in Indonesia, the strategic implication is the need to adapt evidentiary techniques. Lawyers must develop the ability to present digital evidence and expert testimony in a manner readily comprehensible to judges, and they should be more proactive in requesting the judge to order inspections or summon experts as needed, given the absence of an aggressive discovery mechanism. Based on these conclusions and implications, several constructive suggestions are proposed. First, it is recommended that the Supreme Court and legal education institutions promptly formulate and implement Technical Guidelines or Standard Operating Procedures (SOPs) for the examination and evaluation of digital evidence in courts. These guidelines should detail minimum standards for digital forensic expertise, procedures for its submission and testing, and examples of critical questions judges can pose. Second, for legislators, consideration should be given to amending civil procedural law to introduce a limited and managed e-discovery mechanism, particularly for complex commercial cases, to enhance transparency and efficiency in digital evidence collection without fully adopting the high-cost adversarial model. Third, to encourage positive practical convergence, there is a need for dialogue forums and joint training involving judges, legal practitioners, academics, and digital forensic experts from both legal traditions, to learn from each other's methods and develop internationally recognized standards that can be contextually adopted.

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

5. References

Journals:

Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). *Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in The Digital Era*. https://doi.org/10.71317/rjsa.003.05.0375

Ali, E. M., Dirgantara, F., & Darmawan, D. (2024). Legal Protection of Consumers in Online Transactions: A Case Study of Online Fraud in Indonesia. *International Journal of Service Science, Management, Engineering, and Technology*, *6*(3), 27-38.

Aryadi, D. W., Hardyansah, R., Darmawan, D., Saputra, R., Putra, A. R., Negara, D. S., & Maulani, A. (2024). Prosecution on online gambling based on enforcement of criminal law in Indonesia. *International Journal of Service Science, Management, Engineering, and Technology*, *5*(2), 1-6.

Bahri, S., Zeinudin, Moh., & Munir, M. (2024). *Recognition of Electronic Signatures in Proving Civil Procedure Law in Indonesia*. https://doi.org/10.62951/ijlcj.v1i3.131

Billah, R. S., & Saragih, H. (2025). Tantangan Penegakan Hukum Kejahatan Siber Bagi Hakim dari Aspek Hukum Pembuktian di Indonesia.*Arus Jurnal Sosial Dan Humaniora*. https://doi.org/10.57250/ajsh.v5i2.1543

Billah, R. S., & Saragih, H. (2025). Tantangan Penegakan Hukum Kejahatan Siber Bagi Hakim dari Aspek Hukum Pembuktian di Indonesia.*Arus Jurnal Sosial Dan Humaniora*. https://doi.org/10.57250/ajsh.v5i2.1543

Budianto, A. S., Fransisca, I., & Tedjokusumo, D. D. (2024). Perluasan dari Alat Bukti Tertulis dalam Perspektif Hukum Acara Perdata.*Law, Development and Justice Review*. https://doi.org/10.14710/ldjr.7.2024.124-140

Darmawan, D., & Negara, D. S. (2023). The Application of Restorative Justice in Resolving Speech Cases in the Digital Space: A Normative Analysis of the Electronic Information and Transactions Law and the Criminal Code. Journal of Social Science Studies, 3(1), 295-306.

Deviriana, B. I., Nurdianti, D., Chandra, F. T., Nagib, M., & Danella, X. (2025). Analysis of Whatsapp Chat Usage as Court Evidence.Devotion. https://doi.org/10.59188/devotion.v6i6.25492

Dewi, M. M., Alifia, T. D., & Sitohang, S. (2024). Penggunaan Alat Bukti Elektronik dalam Menyelesaikan Sengketa Hukum Perdata di Indonesia.Mandub. https://doi.org/10.59059/mandub.v2i3.1416

Dhumillah, D. S. R. (2024). The Stand of Electronic Evidence in Cyber Crime Law Enforcement in Indonesia.Eduvest. https://doi.org/10.59188/eduvest.v4i9.1812

Edward, E. O., & Ojeniyi, J. A. (2019, December 1). A Systematic Literature Review on Digital Evidence Admissibility: Methodologies, Challenges and Research Directions. International Conference on Electronics, Computer and Computation. https://doi.org/10.1109/ICECCO48375.2019.9043250

Fernando, D., Heniarti, D. D., & Zakaria, C. A. F. (2025). Transformasi alat bukti elektronik menggunakan digital forensik dalam pembaharuan hukum acara pidana. Journal Justiciabelen. https://doi.org/10.35194/jj.v5i01.5506

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

Fletcher, G. P., & Sheppard, S. (2005). The American Civil Trial in Outline. https://doi.org/10.1093/oso/9780195167221.003.0027

Freckelton, I. (2016). Evidence, Rules of. https://doi.org/10.1016/B978-0-12-800034-2.00168-3

Gunarto, G., Yusri, Y., & Kusriyah, S. (2023). Reconstruction of Evidence Regulations in Civil Jurisdiction Based on Justice Value.Scholars International Journal of Law, Crime and Justice. https://doi.org/10.36348/sijlcj.2023.v06i08.008

Hadinoto, S. H., Setiono, J., & Prisgunanto, I. (2025). Application of Blockchain Technology for Strengthening The Integrity of The Electronic Investigation Management System (E-Mp) in The Indonesian National Police. https://doi.org/10.38035/gijlss.v3i2.487

Hardinanto, A., Arief, B. N., & Setiyono, J. (2023). The Significance of Computer Forensics in Electronic Documents as Evidence in Criminal Law.Jurnal Cakrawala Hukum. https://doi.org/10.26905/idjch.v14i2.10820

Kholis, K. N., Chamim, N., Susanto, J. A., Darmawan, D., & Mubarak, M. (2023). Analyzing Electronic Medical Records: A Comprehensive Exploration of Legal Dimensions within the Framework of Health Law. International Journal of Service Science, Management, Engineering, and Technology, 4(1), 36-42.

Komalasari, R., & Mustafa, C. (2023). Electronic Evidence in The Healthy Justice System: Reimagined.Jurnal Hukum Dan Peradilan. https://doi.org/10.25216/jhp.12.3.2023.547-580

Losavio, M. (2020). Identity and Sufficiency of Digital Evidence. https://doi.org/10.1007/978-3-030-56223-6_2

Manurung, K. H., & Harefa, B. (2024). The Validity of Electronic Evidence and Its Relation to Personal Data Protection.Jurnal Daulat Hukum. https://doi.org/10.30659/jdh.v7i4.41815

Mohsin, K., & Asthana, K. B. (2024). Digital Forensics in Law: Unravelling the Challenges and Advancements.International Journal of Forensic Research. https://doi.org/10.33140/ijfr.05.01.05

Monaco, P. (2020). Scientific Evidence in Civil Courtrooms: A Comparative Perspective. https://doi.org/10.1007/978-3-030-34754-3_6

Monique, C., Yuliati, Y., & Sulistio, F. (2024). Exploring the Role of Digital Forensics in Identifying Cyber Crime in Indonesia's Criminal Procedure Law.Pena Justisia: Media Komunikasi Dan Kajian Hukum (Edisi Elektronik). https://doi.org/10.31941/pj.v23i2.4068

Mujisulistyo, Y. F., Darmawan, D., & Dirgantara, F. (2024). Reconstruction of the Legal Mechanism for Consumer Rights Recovery Regarding Personal Data Leaks in the Financial Technology and E-Commerce Sectors in Indonesia. Journal of Social Science Studies, 4(1), 75-84.

Negara, D. S., & Darmawan, D. (2023). Digital Empowerment: Ensuring Legal Protections for Online Arisan Engagements. Bulletin of Science, Technology and Society, 2(2), 13-19.

Noor, Z. Z. (2024). Proof of the Legal Power of Electronic Certificates Against Criminal Acts of Forgery.Journal of Law, Poliitic and Humanities. https://doi.org/10.38035/jlph.v4i6.846

O'Sullivan, M. (2023). Collection and Chain of Evidence. https://doi.org/10.1016/b978-0-12-

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

823677-2.00184-7

Pangabean, B. A. B., & Kemala, A. P. (2025). Technology Integration in Law Enforcement Efforts in Indonesia: Legal and Regulatory Perspectives.FOCUS. https://doi.org/10.37010/fcs.v6i2.2028

Plaxton, M., & Sankoff, P. (2023). A Gatekeeper Stage for Lay Opinion Evidence. Manitoba Law Journal. https://doi.org/10.29173/mlj1334

Poor Mollaei, A., Salarzaei, A., & Tabatabaei, S. A. H. (2024). A Legal Analysis of the Challenges and Enforcement Mechanisms of Electronic Evidence in the Iranian Judicial System. https://doi.org/10.61838/kman.lsda.3.4.16

Puspita, D., Sari, Muh. I. F., Rahim, Ibnu, Muh., & Rahim, F. (2025). Handling of Crypto Assets as Evidence in Criminal Cases. https://doi.org/10.64843/prolev.v3i1.31

Rahman, A., Darmawan, D., & Saputra, R. (2024). Analysis of Cross-border Payment Regulation and its Impact on Consumers in Indonesia. Bulletin of Science, Technology and Society, 3(2), 23-28.

Revanoor, G. (2022). The Power of Digital Signature Evidence in Indonesian Civil Procedural Law. https://doi.org/10.56128/ljoalr.v1i1.46

Rowe, N. C. (2016). Privacy Concerns with Digital Forensics. https://doi.org/10.4018/978-1-4666-9905-2.CH008

Santosa, D. G. G., & Kamali, K. M. I. (2022). Acquisition and presentation of digital evidence in criminal trial in indonesia. Jurnal Hukum Dan Peradilan. https://doi.org/10.25216/jhp.11.2.2022.195-218

Setiawan, E. M. N., & Hartiwiningsih, H. (2025). Optimizing the use of Digital Forensics and Information Technology in Proving Criminal Acts of Electronic Document Forgery in Indonesia.International Journal of Law, Crime and Justice. https://doi.org/10.62951/ijlcj.v2i2.587

Sidabutar, A., Risdalina, R., & Kumalasari, I. M. (2024). Proof of Criminal Acts in The Field of Information and Electronic Transactions Judging from Law Number. 19 Of 2016 Concerning Information nd Electronic Transactions. https://doi.org/10.51601/ijersc.v5i1.770

Sujatmiko, B., & Soesatyo, B. (2025). The Urgency of Using Electronic Evidence in Trials as an Effort to Answer the Challenges of Law Enforcement in the Digital Era and Social Media Dynamics.Asian Journal of Social and Humanities. https://doi.org/10.59888/ajosh.v3i9.567

Sukmasari, A., Apg Frederik, W., Kalalo, M. E., & Soepeno, M. H. (2024). Application Of Electronic Evidence as Extension of Legal Civil Evidence Divorce Cases in Indonesia.International Journal of Law, Environment and Natural Resources. https://doi.org/10.51749/injurlens.v4i1.95

Wisnubroto, A., Lay, F. R. F., & Soumokil, Y. M. (2025). The Active Judge System in the Adversary Model: Prospects for Its Application in Indonesia.International Journal of Science and Environment. https://doi.org/10.51601/ijse.v5i4.239

Books:

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law

Internet (3rd ed.). Academic Press.

Creswell, J. W. (2009). Research design: Qualitative, quantitative, and mixed methods approaches (3rd ed.). Sage Publications.

Federal Rules of Civil Procedure. (2023). United States Courts.

Federal Rules of Evidence. (2023). United States Courts.

Krippendorff, K. (2013). Content analysis: An introduction to its methodology (3rd ed.). Sage Publications.

Zweigert, K., & Kötz, H. (1998). An introduction to comparative law (3rd ed.). Clarendon Press.

Regulations:

Criminal Procedure Code, Law No. 8 of 1981 (1981). State Gazette of the Republic of Indonesia Number 76 of 1981.

Government Regulation of the Republic of Indonesia Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. (2019). State Gazette of the Republic of Indonesia Number 186 of 2019.

Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions. (2008). State Gazette of the Republic of Indonesia Number 58 of 2008.

Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection. (2022). State Gazette of the Republic of Indonesia Number 144 of 2022.

Law of the Republic of Indonesia Number 30 of 1999 concerning Arbitration and Alternative Dispute Resolution. (1999). State Gazette of the Republic of Indonesia 1999 Number 138.

Regulation of the Chief of the Indonesian National Police concerning Evidence Management. (2020).

The copyright of this document is owned by Jurnal Daulat Hukum and is protected by law