

Beyond the Numbers: How Digital Evidence Shapes Anti-Corruption Justice in Indonesia

✉A-F Wishnu Agung Baroto

Institute of Science Tokyo, Japan

Ministry of Finance of the Republic of Indonesia

TADAR Digital Nusantara, Indonesia

ARTICLE INFORMATION

Article History:

Received January 7, 2025

Revised April 15, 2026

Accepted June 3, 2026

DOI:

[10.21532/apfjournal.v11i1.485](https://doi.org/10.21532/apfjournal.v11i1.485)

- A – Research concept and design
- B – Collection and/or assembly of data
- C – Data analysis and interpretation
- D – Writing the article
- E – Critical revision of the article
- F – Final approval of article



Copyright © 2026 Authors. This is an open access article under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

ABSTRACT

Digital evidence has become increasingly important in corruption investigations; however, its quality and utilization vary significantly across Indonesia's judicial system. This study examines how digital evidence influences anti-corruption justice by analyzing institutional capacity, forensic quality, and regional disparities. Using a mixed-methods approach combining quantitative analysis of 1,248 court decisions from 2010–2023 and qualitative document analysis, this study identifies patterns in digital evidence adoption and forensic procedures. The findings reveal a dual-track system in which corruption cases demonstrate substantially higher forensic compliance than other case categories, while significant disparities exist between Jakarta and regional courts. The study argues that legal frameworks alone are insufficient to ensure consistent digital evidence practices, as institutional capacity and resource distribution play critical roles. This research contributes by proposing a reform framework emphasizing tiered standards, regional forensic capacity development, specialized task forces, and procedural improvements.

Keywords: Digital Evidence, Digital Forensics, Corruption Justice, Evidence Quality, Institutional Capacity, Regional Disparities.

How to Cite:

Baroto, W. A. (2026). Beyond the Numbers: How Digital Evidence Shapes Anti-Corruption Justice in Indonesia. *Asia Pacific Fraud Journal*, 11(1), 99-117. <https://doi.org/10.21532/apfjournal.v11i1.485>.

✉Corresponding author :
Email: wishnu.ab@gmail.com

The 2nd Best Paper of Call for Papers Seminar ACFE Indonesia Chapter 2025

Association of Certified Fraud Examiners (ACFE)

Indonesia Chapter

Page. 99-117

1. INTRODUCTION

The digitalization of governance, commerce, and social interaction has fundamentally changed the evidentiary foundations of contemporary legal systems. Communications that were once temporary are now recorded, financial transactions are logged in real time, and administrative decision-making increasingly leaves detailed digital traces. As a result, digital evidence has become indispensable in the investigation and prosecution of complex crimes, including corruption and financial fraud (Casey, 2011; Kerr, 2005).

Legal systems worldwide have responded by formally recognizing electronic information and documents as admissible evidence. Yet, comparative scholarship shows that technological advances often outpace the institutional, technical, and procedural capacities required to ensure evidentiary reliability (Kerr, 2005; Daskal, 2015). Digital evidence presents unique challenges: it is easily altered, highly replicable, and commonly embedded in complex technological systems that require specialized expertise for interpretation. Without robust forensic procedures, such as controlled acquisition, chain-of-custody documentation, technical authentication, and expert validation, digital artifacts risk losing their evidentiary value and may potentially mislead judicial decision-making (International Organization for Standardization, 2012; United Nations Office on Drugs and Crime, 2020).

Indonesia responded by enacting significant legal reforms, most notably Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law) and its subsequent amendments. The Act formally recognizes electronic information and electronic documents as legal evidence and represents a milestone in the recognition of digital evidence within the justice system. At the same time, corruption remains a persistent structural challenge in Indonesia, undermining public trust, distorting public procurement, and weakening institutional

accountability. The establishment of the Corruption Eradication Commission (Komisi Pemberantasan Korupsi, KPK) reflects an institutional commitment to addressing corruption through specialized investigative and prosecutorial capacity.

Within this institutional framework, digital evidence has become a cornerstone of anti-corruption enforcement. In major Indonesian corruption cases, such as the e-KTP bribery case and infrastructure corruption scandals, courts have relied heavily on electronic financial transaction records, lawful wiretap recordings, and electronic communications to establish intent, coordination, and illicit benefits (Wigana & Maryanto, 2020; Sumilat & Ginting, 2023; Ali & Bakhtiar, 2024). These cases illustrate how digital evidence, when supported by expert testimony and appropriate forensic procedures, can complement or substitute traditional forms of evidence in complex corruption schemes.

The utilization of digital evidence in corruption enforcement is not unique to Indonesia. Internationally, several significant corruption prosecutions over the past two decades have depended on electronic communications and digital financial data. Brazil's Operation Lava Jato (Car Wash) relied extensively on email archives, encrypted messaging records, and digital accounting systems to uncover systemic bribery networks involving public officials and private corporations (United Nations Office on Drugs and Crime, 2018). The 1MDB scandal in Malaysia relied on cross-border electronic banking records, which were analyzed and presented by foreign jurisdictions through mutual legal assistance mechanisms (U.S. Department of Justice, 2016; Organisation for Economic Co-operation and Development (OECD), 2019). Similarly, the Siemens global bribery case and the South Korean former president corruption case demonstrate how corporate emails, mobile phone messages, and electronic financial records have become critical in establishing evidence of high-level corruption and

abuse of office (Organisation for Economic Co-operation and Development (OECD), 2019; Transparency International, 2018).

Despite the growing incorporation of digital evidence into judicial proceedings, a critical question remains: whether formal admissibility translates into consistent forensic practices across the legal system. Socio-legal and institutional scholarship emphasizes that evidentiary standards are shaped not only by statutory rules but also by institutional capacity, professional expertise, and resource distribution within legal institutions (Kerr, 2005; Daskal, 2015). Empirical studies across multiple jurisdictions demonstrate that specialized enforcement bodies and courts located in major urban centers are more likely to adopt digital forensic procedures than general courts operating under high caseload pressure and limited technical infrastructure (United Nations Office on Drugs and Crime, 2020; Garrie & Morrissy, 2014).

This institutional differentiation has important implications. Research indicates that when forensic standards vary systematically across institutions or regions, legal outcomes may become dependent on organizational capacity rather than evidentiary merit, raising concerns regarding procedural equality and consistency in adjudication (Daskal, 2015; Organisation for Economic Co-operation and Development (OECD), 2019). In corruption cases, uneven application of digital forensic standards may weaken deterrence and reduce accountability, particularly in jurisdictions with limited investigative and forensic resources.

In the Indonesian context, existing research has primarily focused on doctrinal analysis of the EIT Law or qualitative discussions of anti-corruption enforcement by specialized institutions. While these studies provide important insights into legal frameworks and institutional mandates, they offer limited empirical assessment of how digital evidence is handled in everyday judicial practice across different courts, case categories, and

geographic regions (Sumilat & Ginting, 2023; Sukmasari et al., 2024). There has been limited systematic, decision-based analysis examining whether forensic standards are consistently applied in Indonesian courts or how institutional and regional disparities shape evidentiary quality in practice. This empirical gap limits understanding of how digital evidence operates within Indonesia's broader justice system and motivates the present study.

This study investigates how digital evidence is used and evaluated in Indonesian judicial practice through a systematic analysis of published court decisions issued between 2010 and 2023. Moving beyond doctrinal examination of legal rules, this study adopts an empirical approach to assess both the prevalence and documented quality of digital evidence practices. The study is guided by three research questions:

- a. How has the use of digital evidence in Indonesian court decisions evolved between 2010 and 2023?
- b. How do documented forensic practices, including acquisition, chain of custody, authentication, expert testimony, and source verification, differ across legal domains, particularly between corruption cases and other case categories?
- c. How do institutional type and geographic location shape the documentation and treatment of digital evidence in judicial decisions?

Corresponding to these research questions, this study pursues three objectives. First, it aims to document the evolution of digital evidence usage in Indonesian courts over the examined period. Second, it seeks to compare documented forensic practices across legal domains, with particular attention to differences between corruption cases and other case types. Third, it examines how institutional and geographic variation is reflected in the documentation and treatment of digital evidence in judicial

decisions. Through these objectives, this study contributes to socio-legal scholarship on digital evidence, anti-corruption enforcement, and institutional capacity by providing empirical evidence on how evidentiary practices operate within Indonesia's justice system.

2. LITERATURE REVIEW AND HYPOTHESIS

Digital Evidence and Transformation of Criminal Proof

Digital evidence is defined as information of probative value stored or transmitted in digital form, encompassing electronic communications, transactional logs, metadata, and system records generated through routine social, economic, and administrative activities (Casey, 2011). Digital evidence is inherently intangible, easily altered, and highly dependent on technological systems for its creation and interpretation. These characteristics fundamentally challenge conventional evidentiary doctrines developed primarily for physical artifacts and human testimony.

Legal scholars have long recognized that the emergence of digital evidence requires a reconfiguration of criminal procedure. Kerr (2005) argues that existing procedural safeguards, such as search, seizure, and authentication doctrines, were not designed to address the scale, volatility, and complexity of digital data. Digital evidence frequently exists in multiple identical copies, may be distributed across different jurisdictions, and often requires expert interpretation to establish meaning and reliability.

Consequently, the value of digital evidence is closely tied to the procedures used to collect, preserve, and analyze it. Without proper forensic handling, digital artifacts may be selectively extracted, separated from contextual metadata, or manipulated through technological means that are difficult for courts to detect (Casey, 2011; Carrier & Spafford, 2004). Recent research further reinforces this perspective. Horsman & Sunde (2022) argue that reliability depends on

transparency throughout every stage of the investigative process, rather than solely on admissibility at trial.

International Standards and Best Practices in Digital Forensics

In response to these challenges, international standard-setting bodies have developed frameworks to guide the lifecycle of digital evidence. The ACPO Good Practice Guide (2012) establishes four foundational principles: no action should alter evidence that may be relied upon in court; individuals accessing evidence must be competent; an audit trail must document all processes; and the person responsible must ensure compliance with these principles. These principles extend beyond specific technologies or investigative contexts.

Furthermore, ISO/IEC 27037 provides guidelines for the identification, collection, acquisition, and preservation of digital evidence, emphasizing the protection of data integrity and the prevention of contamination. Complementing this framework, ISO/IEC 27042 addresses the analysis and interpretation of digital evidence by highlighting requirements such as methodological transparency, repeatability, and examiner competence.

At the policy level, the United Nations Office on Drugs and Crime (UNODC) has formulated best practices for handling digital evidence in criminal proceedings. These practices include forensic imaging rather than live examination, cryptographic hash verification to ensure data integrity, comprehensive chain of custody documentation, and the involvement of qualified forensic experts who can explain technical findings to judges and prosecutors (United Nations Office on Drugs and Crime, 2020). Together, these standards reflect a broad consensus that digital evidence is not self-authenticating; rather, its reliability must be demonstrated through documented forensic processes.

Recent scholarship has examined emerging challenges in digital evidence management. Casey (2011) and Casey &

Turnbull (2018) explore the complexities of cloud-based evidence, where data may be distributed across multiple jurisdictions. Garfinkel (2010) and Quick & Choo (2014) examine challenges associated with large-scale digital data processing that require advanced analytical capabilities. Montasari (2016) discusses admissibility challenges across jurisdictions, while Karie & Venter (2015) analyze challenges in mobile device forensics. These studies demonstrate that compliance with international standards requires substantial institutional capacity beyond merely recognizing legal frameworks (Horsman, 2023).

Despite the availability of these standards, empirical research indicates uneven implementation. Garrie & Morrissy (2014) show that even courts in technologically advanced jurisdictions may struggle to assess the technical validity and limitations of digital forensic evidence, resulting in inconsistent evaluation of admissibility and evidentiary weight. Furthermore, Bhat et al. (2021) demonstrate that forensic tools may generate unreliable outputs without independent validation, emphasizing that access to technology alone does not guarantee institutional competence.

Moreover, research in the United Kingdom Tully et al. (2020) indicates that sustainable quality improvement is more strongly associated with accreditation-based standards than with legislative recognition alone. These challenges become more pronounced in legal systems with limited forensic infrastructure, training capacity, and institutional coordination.

Digital Evidence, Corruption, and Complex Financial Crime

Corruption cases represent one of the legal domains in which digital evidence has become particularly significant. Unlike conventional crimes that often rely on physical evidence or eyewitness testimony, modern corruption schemes frequently involve sophisticated financial transactions, electronic communications,

and coordinated actions among multiple actors. As a result, digital evidence has become essential for reconstructing patterns of interaction, tracing financial flows, and establishing the relationships between public officials, intermediaries, and private entities.

International anti-corruption enforcement demonstrates the growing importance of digital evidence. The Organisation for Economic Co-operation and Development (OECD) (2019) reports that successful foreign bribery investigations increasingly depend on electronic communications, financial databases, and cross-border digital records. Similarly, the United Nations Office on Drugs and Crime (2018) highlights that complex corruption cases often require advanced investigative techniques because illicit transactions are frequently concealed through layered financial structures and digital communication channels.

In Indonesia, the Corruption Eradication Commission (KPK) has increasingly relied on digital evidence as part of its investigative strategy. Telephone interception records, electronic financial transactions, and digital communications have played significant roles in several high-profile corruption prosecutions (Wigana & Maryanto, 2020; Sukmasari et al., 2024). However, reliance on digital evidence also introduces procedural challenges, particularly concerning authenticity, integrity, and judicial interpretation.

The relationship between corruption enforcement and digital forensic capacity is therefore reciprocal. High-profile corruption cases often receive greater institutional attention and resources, enabling more sophisticated forensic processes. At the same time, stronger forensic capacity increases the ability of enforcement institutions to detect and prove complex corruption schemes. This relationship suggests that differences in institutional capacity may significantly influence how digital evidence contributes to legal outcomes.

Indonesia's Legal Framework for Digital Evidence

Indonesia's legal framework for digital evidence is grounded in Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law), as amended in 2016 and 2024. The EIT Law formally recognizes electronic information and electronic documents as admissible legal evidence, extending evidentiary recognition beyond traditional written and testimonial forms. Articles 5 and 6 stipulate that electronic evidence is considered valid provided that it can be accessed, displayed, and its integrity is maintained.

However, significant procedural gaps remain. Indonesia's Criminal Procedure Code (KUHAP), enacted long before the digital era, contains no detailed provisions governing the collection, authentication, or preservation of electronic evidence. As a result, courts must rely on general evidentiary principles or judicial discretion when assessing digital evidence (Komalasari & Mustafa, 2023).

Doctrinal and empirical studies indicate substantial variation in judicial practice. Some courts require expert testimony and technical authentication to establish the reliability of digital evidence, while others accept screenshots, printouts, or informal electronic records with minimal scrutiny (Sumilat & Ginting, 2023; Manurung & Harefa, 2024). This inconsistency reflects not only legal ambiguity but also disparities in forensic literacy and institutional support across the judiciary.

Institutional Capacity, Geography, and Evidentiary Quality

Understanding variations in evidentiary quality requires theoretical frameworks that address institutional capacity and resource distribution. Institutional capacity encompasses technical infrastructure, human capital, organizational processes, and supporting resources (Fukuyama, 2013; Grindle, 1997). Human capital itself is stratified. Sunde & Dror (2021)

demonstrate that expert performance in digital forensics is susceptible to cognitive bias and varies depending on training, oversight, and peer-review infrastructure capacity dimensions that are closely associated with institutional resources. Therefore, this conceptualization recognizes that legal standards alone are insufficient; effective implementation requires institutions with the capabilities to execute complex procedures (Halliday & Shaffer, 2015; Trubek & Santos, 2006).

Resource distribution theory examines how limited resources are allocated across competing priorities and geographic areas. In developing contexts, resources typically concentrate in capital cities and major urban centers, creating systematic disparities between well-resourced central institutions and resource-constrained provincial entities (Henderson, 2002; Smoke, 2001). This concentration reflects multiple reinforcing factors, including salary differentials that attract talent to capital cities, political importance that drives disproportionate budget allocations, economies of scale that favor centralized specialized functions, and infrastructure advantages in major urban centers (Ades & Glaeser, 1995).

Organizational priority theory suggests that institutions operating under resource constraints make strategic decisions regarding the quality standards applied to different case types (Lipsky, 2010). Cases receiving organizational priority due to serious legal consequences, public visibility, or international co-operation requirements often receive disproportionate resource allocation, even when formal legal standards apply uniformly. This creates dual-track systems operating under a single legal framework (Gallagher, 2006; Peerenboom, 2002). In the Indonesian context, decentralization and variations in institutional capacity across jurisdictions further intensify these patterns (Buehler, 2010; Butt & Lindsey, 2012).

3. METHODS

Research Design

This study employed a mixed-methods approach combining quantitative analysis of case statistics with qualitative assessment of evidence standards. The research followed a sequential explanatory strategy, where initial quantitative analysis identified systematic patterns in digital evidence utilization, which were subsequently explored through qualitative examination to understand institutional mechanisms, resource constraints, and contextual factors that produced the observed variations.

Data Collection

Data were extracted from Indonesia's Supreme Court database during August–November 2023 (<https://putusan3.mahkamahagung.go.id/>). This database represents the most comprehensive repository of Indonesian court decisions, containing over 8.3 million judgments from all court levels: District Courts (Pengadilan Negeri), High Courts (Pengadilan Tinggi), and the Supreme Court, covering criminal, civil, religious, military, and administrative matters across all provinces.

Cases were identified through systematic keyword searches using Indonesian legal terminology: *forensik digital* (digital forensics) and *bukti digital* (digital evidence). These terms capture cases involving forensic evaluation rather than incidental mention of electronic documents. The temporal scope of 2010–2023 captures digital evidence evolution following the implementation of the 2008 EIT Law. Due to the Supreme Court database's 12–24 month publication lag, 2022–2023 data show incomplete coverage.

The extracted data were then categorized along three dimensions:

- a. Court Type: Religious Courts, Criminal Courts, specialized Corruption Courts, Civil Courts, State Administration Courts, Military Courts.
- b. Geographic Location: Jakarta, major cities (Surabaya, Bandung, Medan,

Semarang), provincial capitals, district/regency areas.

- c. Case Subject Matter: Corruption, EIT Law violations, drugs, tax evasion, general criminal, civil, religious/family, state administration.

Quality Assessment Framework

Digital evidence quality was assessed using five indicators derived from international forensic standards (Association of Chief Police Officers, 2012; International Organization for Standardization, 2012; United Nations Office on Drugs and Crime, 2018). These indicators represent minimum requirements for forensically sound evidence handling rather than ideal-typical best practices, making them appropriate benchmarks for assessing developing-nation contexts where resource constraints affect implementation capacity.

The five quality indicators are as follows. First, forensic acquisition procedures include documentation of write-blocking hardware, forensic imaging software, or other specialized acquisition methods designed to prevent evidence alteration during collection. Second, chain of custody documentation includes documentation of all handlers at each stage, transfer procedures between parties, storage methods and conditions, and integrity verification measures. Third, expert testimony inclusion refers to the presence of qualified forensic experts who provide technical evaluations of digital evidence with documentation of relevant credentials and experience. Fourth, technical authentication methods include hash verification using MD5, SHA-1, or SHA-256 algorithms, metadata analysis, or other comparable verification techniques, establishing evidence integrity. Fifth, source verification includes comparison of presented evidence against original system records, authentication requests sent to service providers, or official institutional confirmations of evidence authenticity.

Each indicator was coded as present (explicitly documented in a court decision), absent (not documented), or unclear (ambiguous documentation). Unclear cases were coded conservatively as absent, potentially underestimating actual forensic quality but ensuring reported findings reflect documented practices verifiable through judicial records. This conservative approach strengthens confidence that identified quality disparities represent genuine differences rather than documentation variations.

Analytical Approach

Analysis employed four complementary techniques. Temporal analysis examined time-series patterns from 2010 to 2023, identifying distinct adoption phases and calculating growth rates across categories. Categorical comparison conducted cross-sectional analysis of quality indicators across case types, calculating percentages documenting each indicator within categories and testing for statistical significance of observed differences. Geographic analysis examined case concentration and quality variation by court location, revealing both volume patterns and systematic quality disparities. Quality pattern assessment identified specific forensic practices present or absent across contexts, revealing concrete manifestations of institutional capacity differences beyond aggregate statistics.

Limitations

Several limitations should be acknowledged. First, reliance on published decisions may introduce selection bias if courts systematically differ in publication practices or if certain case types are overrepresented in published records. However, the Supreme Court database represents the best available source for systematic nationwide analysis. Second, quality assessment depends on what judges documented; actual practices may differ from descriptions in judicial opinions, though documentation itself constitutes an important forensic requirement. Third, 2022–2023 data are incomplete due to

publication lag, potentially affecting temporal trend analysis for recent years. Fourth, the study lacks interview data that could illuminate institutional constraints, resource-allocation decisions, and judicial reasoning behind documented practices. Fifth, single-researcher coding without inter-rater reliability testing may introduce interpretation bias, though the use of concrete observable criteria and conservative coding rules mitigate this concern. Future research incorporating interviews, courtroom observations, and multi-coder reliability checks would strengthen these findings.

4. RESULTS AND DISCUSSION

Results

This section presents findings on digital evidence utilization patterns from 2010 to 2023, examining temporal evolution, categorical quality disparities, geographic distribution, and implementation challenges. The analysis reveals systematic variations in forensic quality across case types and jurisdictions, with significant implications for anti-corruption enforcement effectiveness and justice system equity.

Temporal Evolution of Digital Evidence (2010–2023)

Analysis of 1,248 court decisions reveals growth in the use of digital evidence, increasing from fewer than 50 cases in 2010 to nearly 950 in 2021, reflecting broader digital transformation across Indonesian society and governance. The apparent decline in 2022–2023 reflects incomplete database coverage due to the 12–24-month publication lag rather than an actual reduction in digital evidence use, as shown in Figure 1.

This growth exhibits three distinct phases, each characterized by different adoption dynamics. The Emerging Period (2010–2014) saw fewer than 100 cases annually, primarily concentrated in EIT violations as courts cautiously experimented with the newly established legal framework. The Expansion Period (2015–2018) reached approximately

200 cases by 2018, reflecting steady growth alongside the 2016 EIT Law amendment and increasing institutional familiarity. The Acceleration Period (2019–2021) exceeded 900 cases, showing an acceleration of digital communication and governmental processes. This rapid expansion occurred across multiple case categories simultaneously, raising critical questions about whether forensic quality maintained pace with volume growth.

Amid this explosive overall growth, corruption investigations stand out as a notable exception. These cases maintained relatively stable annual volumes between 30 and 50 throughout the study period, never exceeding 50 cases in any single year. This consistency suggests that institutional capacity to handle forensically sound corruption evidence expanded slowly despite both policy prioritization of anti-corruption efforts and technological advancements enabling more sophisticated evidence collection. This divergence between overall expansion and corruption stagnation sets the stage for understanding the quality disparities examined below.

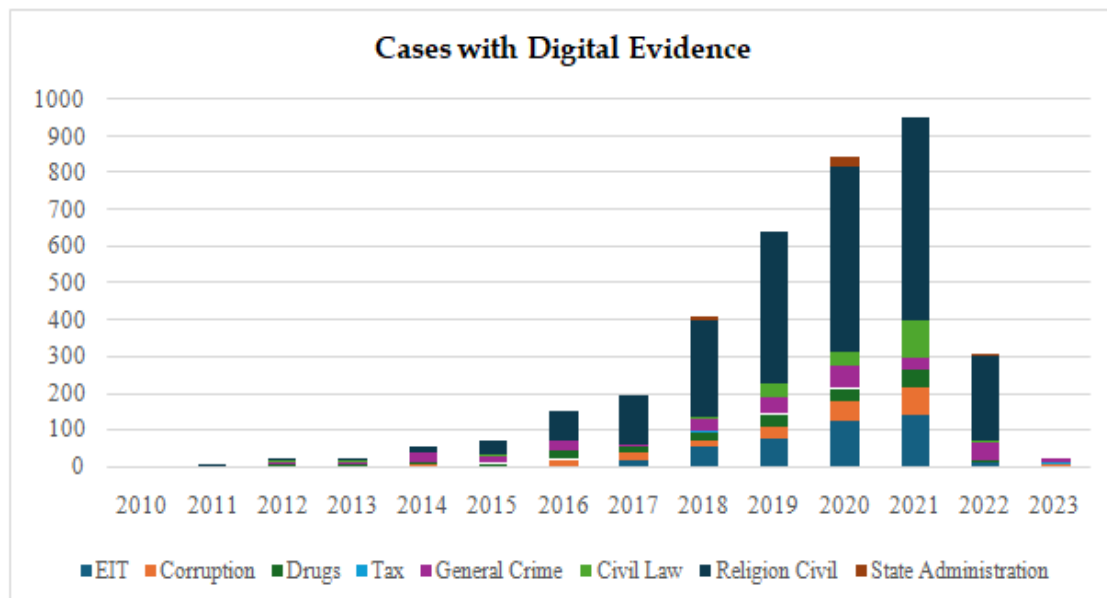
All results reported are based on the dataset of 1,248 court decisions, and descriptive statistics were computed in Microsoft Excel. The percentages refer to the share of decisions within each category that explicitly document the indicated forensic step.

Categorical Distribution and Quality Disparities in Corruption Cases

Cross-sectional analysis reveals systematic variations in quality across case categories, demonstrating a dual-track system in which institutional capacity and organizational priorities determine evidence quality. Table 1 presents comparative quality metrics that reveal stark contrasts, which cannot be attributed to different legal requirements since all cases operate under the same EIT Law provisions.

The disparities are substantial and consistent across all forensic indicators. Corruption cases document chain of custody 83% of the time compared to 19% for EIT cases and only 6% for religious cases, representing a nearly fourteen-fold difference between the highest and lowest

Figure 1. Cases with Digital Evidence by Category (2010-2023)



Source: Processed Data

categories. Similarly, expert testimony appears in 69% of corruption cases, 24% of EIT cases, and 4% of religious matter cases. Technical authentication methods show parallel patterns, with corruption cases demonstrating 71% compliance compared to 16% for EIT cases and just 3% for religious cases. Even the most demanding indicator source verification requiring comparison against original system records appears in 65% of corruption cases, while occurring in only 10% of EIT cases and 1% of religious cases.

These findings reveal two critical insights. First, Indonesian institutions demonstrably can achieve international forensic standards when appropriate conditions exist, such as in corruption cases, which approximate ACPO and ISO guidelines with chain of custody documentation, expert testimony, and technical authentication approaching best practices observed in developed nations. This contradicts narratives suggesting that developing nations inherently lack the capacity for sophisticated forensic procedures. Second, however, this excellence remains concentrated rather than diffused throughout the legal system. The quality-quantity gap, with high standards in limited corruption cases versus low standards in high-volume EIT and religious categories, suggests proper forensic handling has not scaled beyond specialized anti-corruption institutions despite identical legal frameworks ostensibly requiring uniform standards across all digital evidence.

EIT cases constituted the largest category throughout most of the study period, growing from fewer than 10 cases in 2010 to approximately 150 by 2021. As violations explicitly involve electronic information and transactions, these cases should, in theory, receive sophisticated forensic handling given their inherently technical nature. However, quality assessment reveals gaps: only 24% included expert testimony despite the technical nature of the charged offenses; technical authentication methods were used in only 16%; formal forensic acquisition procedures were documented in just 12%; and chain of custody information appeared in only 19%. Most problematically, analysis revealed that 72% of EIT cases relied on simple screenshots or web captures without forensic verification, accepted as primary evidence despite vulnerability to manipulation and absence of authentication.

This pattern creates systemic risk extending beyond individual case outcomes. When courts routinely admit unverified digital evidence in the high-volume EIT category, these permissive standards risk establishing precedents affecting other domains. Judges and prosecutors developing professional practices in EIT matters may carry these lenient approaches into corruption investigations, potentially undermining the higher standards that complex corruption cases require. The normalization of screenshot-based evidence in routine proceedings threatens to erode forensic

Table 1. Forensics Quality Indicators in Each Case

Forensic Quality Indicator	Corruption Cases	EIT Law Cases	Religion Cases
Forensic Acquisition Procedures Referenced	76%	12%	3%
Chain of Custody Documented	83%	19%	6%
Expert Testimony Included	69%	24%	4%
Technical Authentication Described	71%	16%	3%
Verification Against Source Records	65%	10%	1%

Source: Processed Data

rigor precisely when digital evidence's role in high-stakes cases is expanding.

Religious/civil cases showed substantial growth from 2019 to 2021 but demonstrated the lowest forensic standards across all measured indicators. Quality assessment reveals that 94% relied on unverified WhatsApp screenshots as primary evidence, typically presented without technical authentication, expert evaluation, or chain of custody documentation. Only 4% included any expert testimony regarding digital evidence, while technical authentication appeared in just 3% of cases. This prevalence of permissive standards in the highest-volume category raises multiple concerns, compounding the risks identified in EIT cases, establishes baseline judicial expectations that digital evidence requires minimal authentication, and potentially influences standards in other domains, including corruption cases, which require substantially greater rigor.

Geographical Disparities

The categorical disparities documented above interact with pronounced geographic patterns to create what we term digital justice inequality, a systematic variation in forensic capabilities based on location rather than case merits, legal requirements, or defendants' rights. Table 2 presents the geographic distribution, revealing substantial urban concentration. Over 56% of all digital evidence cases are concentrated in Jakarta and major cities, with Jakarta alone handling nearly 30% despite representing approximately 4% of Indonesia's population. For corruption

cases specifically, this concentration is even more pronounced, reaching 47%.

This reflects underlying resource and expertise distribution patterns: Jakarta attracts technical talent through higher salaries and better career opportunities; receives disproportionate budget allocations reflecting political importance; maintains infrastructure supporting sophisticated forensic operations, including reliable electricity and high-speed internet; and, most critically, benefits from the KPK headquarters location, providing direct support unavailable to provincial courts. For corruption investigations specifically, geographic location predicts forensic quality as strongly as case type. Table 3 presents these regional quality variations that cannot be attributed to different legal frameworks since all corruption courts operate under identical legislation.

Jakarta's Corruption Court achieves 85.1% compliance with proper forensic procedures, while regional courts in major cities reach 66.7%, provincial corruption courts demonstrate 41.2%, and other courts handling corruption show only 22.7%. This creates a 62 percentage point gap between Jakarta and other courts, a disparity that fundamentally undermines the principle of equal justice. Provincial prosecutors investigating corruption face difficult choices: send evidence to Jakarta, creating substantial delays while evidence is transported, analyzed, and results returned; attempt analysis with inadequate local resources, risking quality problems that courts may exclude or that defense attorneys may successfully challenge;

Table 2. Geographic Distribution of Cases

Courts Location	Digital Evidence Cases (2010-2021)	Percentage Cases
Jakarta Courts	371	29.73%
Other Major Cities (Surabaya, Semarang, Medan, Bandung)	328	26.28%
Provincial Capitals	367	29.41%
Other Regions	182	14.58%

Source: Processed Data

or strategically avoid digital evidence altogether, leaving corruption schemes involving electronic communications and digital financial transactions unexposed despite potentially strong digital traces of corrupt activity.

This geographic inequality is particularly problematic because much corruption affecting regional development such as infrastructure projects, local procurement, and resource extraction occurs precisely in areas with the weakest forensic capabilities, potentially creating enforcement blind spots that enable sophisticated corrupt actors to operate with reduced detection risks by strategically focusing activities in under resourced jurisdictions.

Implementation Challenges

Beyond the quantitative patterns documented above, qualitative analysis of case records identified specific technical and procedural challenges affecting the utilization of digital evidence. These challenges help explain both why corruption cases remain limited in number despite technological advancement and why quality disparities persist across jurisdictions despite uniform legal frameworks.

Document analysis reveals that 74.3% of corruption cases required evidence from multiple digital platforms, including banking records, messaging applications such as WhatsApp and Telegram, email systems, and electronic document repositories. This multi-platform correlation demands not merely technical ability to extract data from

each individual source, but sophisticated analytical skills to identify connections between data extracted from different sources, establish accurate chronological timelines when different platforms use varying time formats and time zones, and reconstruct complex event sequences from fragmentary digital traces distributed across incompatible systems maintained by different service providers.

Additionally, 81.5% of corruption cases involved financial records that required specialized analysis of complex structures. Modern corruption typically involves shell company networks where funds move through multiple corporate entities to disguise ultimate beneficiaries, layered transactions where corrupt proceeds pass through numerous intermediaries before reaching final recipients, offshore accounts in jurisdictions with banking secrecy protections limiting investigative access, and increasingly cryptocurrency channels used to move corruption proceeds outside traditional banking systems where monitoring mechanisms exist. Analyzing these financial patterns requires specialized capabilities that combine forensic accounting expertise, a deep understanding of international financial systems, familiarity with money laundering techniques, and advanced technical skills to extract and correlate digital financial records from multiple institutions operating under different regulatory regimes.

Procedural inconsistencies compound these technical challenges. Courts apply divergent authentication standards: some courts require sophisticated hash

Table 3. Regional Disparities of Corruption Cases

Court Location	Corruption Cases with Digital Evidence	Cases with Sound Forensic Procedures
Jakarta Corruption Court	87	74 (85.10%)
Regional Corruption Courts in Major Cities	63	42 (66.70%)
Provincial Corruption Courts	51	21 (41.20%)
Other Courts Handling Corruption	22	5 (22.70%)

Source: Processed Data

verification, while others accept simple screenshots without technical verification. Qualified expert availability is severely constrained outside Jakarta, where forensic experts were available in only 28.7% of cases where evidence was challenged, compared to over 80% availability in Jakarta courts. This geographic disparity in access to experts creates systematic disadvantages for provincial corruption investigations. Furthermore, judicial technical knowledge varies substantially across Indonesia's diverse court system, affecting both admissibility decisions and weight assessments. This variation is particularly consequential in corruption cases where digital evidence often plays a central evidentiary role and where sophisticated defendants with access to technical expertise may exploit judicial knowledge limitations to challenge evidence admissibility or credibility.

Discussion

This section interprets the empirical findings through the institutional-capacity lens, comparing results with prior international and Indonesian studies. The analysis is organized around four interrelated arguments: (i) the dual-track system reflects the logic of street-level bureaucracy operating under uneven capacity; (ii) geographic inequality in forensic quality mirrors resource-distribution patterns documented in the urban-primacy literature; (iii) technical complexity imposes capability thresholds that even well-resourced courts struggle to meet; and (iv) the combined evidence supports a tiered reform framework consistent with "good-enough governance" prescriptions for developing states.

Interpreting the Dual-Track System

The finding that identical legislation produces radically different forensic outcomes (83% chain of custody compliance in corruption cases versus 6% in religious cases) is theoretically consistent with institutional capacity scholarship (Grindle, 1997; Fukuyama, 2013) and, more specifically, with Lipsky's (2010)

street-level bureaucracy framework. When formal rules require procedures that implementing agents cannot realistically execute given available resources, those agents develop informal routines that substitute achievable practices for statutory ideals. The EIT Law establishes uniform admissibility in the "law-in-books," but the "law-in-action" is produced by prosecutors, judges, and forensic examiners whose capacity is sharply unequal across Indonesia's judicial architecture.

This pattern is not unique to Indonesia. Comparative studies document similar stratification elsewhere. In Brazil, Operation Lava Jato produced international-standard forensic outputs through a specialized task-force model, while ordinary criminal courts continued to rely on minimally authenticated electronic evidence (United Nations Office on Drugs and Crime, 2018). In cross-border prosecutions under the OECD Anti-Bribery Convention, participating states reported systematically higher forensic quality in high-profile cases than in routine ones, even under identical procedural law (Organisation for Economic Co-operation and Development (OECD), 2019). Garrie & Morrissy (2014) observed comparable stratification in U.S. state courts, though to a lesser extent than the Indonesian evidence indicates. The Indonesian system thus represents a sharper instance of a globally recognized phenomenon rather than a country-specific anomaly.

The theoretical implication is significant. Legal formalism assumes that uniform rules produce uniform outcomes; institutional-capacity theory predicts the opposite unless implementing resources are equalized. The Indonesian data strongly support the latter prediction. Recent Indonesian scholarship corroborates this reading: Sumilat & Ginting (2023) and Manurung & Harefa (2024) document substantial inconsistency in how Indonesian courts assess digital evidence, and Komalasari & Mustafa (2023) attribute much of this inconsistency to the absence of detailed implementing regulations under

the KUHAP, which reflects procedural capacity gaps rather than substantive legal deficiency.

The risk of evidentiary-standard degradation is a further implication of this stratification. When high-volume routine categories normalize minimally authenticated evidence, such as WhatsApp screenshots admitted without hash verification or printouts accepted without expert testimony, the resulting judicial expectations can migrate into high-stakes prosecutions. Horsman & Sunde (2022) describe an analogous dynamic in the United Kingdom, where caseload pressure led to procedural shortcuts that subsequently required regulatory correction. The Indonesian evidence suggests a comparable corrective is needed before routine case norms erode corruption case rigor.

Resource Concentration and Geographic Inequality

The 62 percentage point quality gap between Jakarta's Corruption Court and provincial courts that handle corruption is among the most prominent findings of this study. Because both sets of courts operate under identical legislation and equivalent mandates, the gap cannot be attributed to differences in legal framework; it must reflect resource distribution mechanisms. Henderson (2002) and Smoke (2001) describe the standard pattern in developing states: specialized technical capacity concentrates in capital cities because infrastructure, salaries, career prospects, and political visibility are disproportionately located there. Ades & Glaeser (1995) theorize this urban primacy as a self-reinforcing equilibrium: talent and investment flow to capitals because talent and investment are already there, which closely describes the concentration of Indonesian digital forensic capacity in Jakarta.

This geographic equilibrium matters politically as well as technically. Peerenboom (2002) and Gallagher (2006) document analogous center periphery

disparities in Chinese courts, where formal legal reforms produced capital-city implementation while provincial courts continued to operate under weaker evidentiary norms. Indonesian research on decentralization (Buehler, 2010; Butt & Lindsey, 2012) reaches similar conclusions: post-1998 administrative devolution distributed authority without distributing capacity, producing the "specialized center, under-resourced periphery" pattern the present findings now document for digital evidence specifically.

The anti-corruption consequence is serious. Much of the corruption affecting regional development local procurement fraud, provincial budget manipulation, resource extraction rent seeking generates substantial digital evidence that must be processed precisely where forensic capacity is weakest. Sukmasari et al. (2024) note that provincial investigations of corruption frequently proceed with minimal electronic evidence authentication, creating detection asymmetries that sophisticated actors can exploit. The present findings quantify this risk: corruption investigations outside Jakarta are conducted under forensic conditions that do not meet the standards expected of the same offense within Jakarta.

Technical Complexity and Organizational Priorities

Why do corruption cases receive systematically higher forensic treatment? Lipsky's (2010) analysis of organizational priorities under resource scarcity provides the mechanism. When agencies cannot apply high standards to all cases, they concentrate scarce capability on cases where reputational, political, and international stakes are greatest. The KPK's institutional identity depends on convictions in visible cases; international cooperation under UNCAC and the OECD Anti-Bribery Convention (Organisation for Economic Co-operation and Development (OECD), 2019), demands forensic outputs that satisfy external reviewers; and the reputational penalty for a failed high-

profile prosecution is disproportionately large. These pressures produce exactly the allocation the data show: 76–83% forensic compliance in corruption cases, single-digit compliance elsewhere.

However, the finding that 74% of corruption cases require multi-platform correlation and 82% involve complex financial analysis reveals a capability threshold that priority alone cannot resolve. Prior work identifies this as the “competence ceiling” problem. Sunde & Dror (2021) demonstrate that expert performance in digital forensics is bounded by training, peer review, and cognitive-bias controls infrastructural conditions that many Indonesian provincial courts do not yet possess. Bhat et al., (2021) show that even in jurisdictions with tool access, unvalidated outputs can mislead judicial decision-making, reinforcing that capability is about process, not equipment. Horsman (2023) further argues that examiners facing caseload pressure without institutional support rationally adopt triage strategies that sacrifice evidentiary depth for throughput.

Applied to the Indonesian case, this means that even a well-intentioned provincial court that acquires forensic hardware will not automatically produce Jakarta-quality outputs. The institutional ecosystem certified examiners, peer-review protocols, validated toolchains, and sustained training is the binding constraint, not the equipment. This interpretation is consistent with UK experience documented by Tully et al. (2020): measurable quality improvement followed the introduction of accreditation-backed standards, not the earlier phase of tool deployment alone.

Policy Implications and Reform Framework

The four proposed reforms tiered national standards, regional forensic centers, specialized task forces, and targeted EIT Law amendments follow directly from the theoretical and empirical analysis, and each reform addresses a mechanism

identified in the literature. First, tiered standards operationalize Grindle’s (1997) “good-enough governance” principle: resource-constrained systems improve faster when reform targets are calibrated to achievable implementation capacity rather than to ideal prescriptions. A Tier-1 regime mandating ACPO and ISO/IEC 27037-consistent acquisition, chain-of-custody, authentication, expert testimony, and source verification for corruption and serious financial crime is realistic because it codifies current KPK practice. Tier-2 and Tier-3 floors prevent the evidentiary-degradation pathway discussed in 5.1, while the explicit prohibition on applying lower-tier standards to higher-tier cases addresses the normative-migration risk identified by Horsman & Sunde (2022). Tully et al. (2020) provide empirical support that tiered, accreditation-backed standards produce measurable quality gains.

Second, regional forensic centers in 10–12 strategically distributed locations directly target the resource-distribution mechanism theorized by Henderson (2002), Smoke (2001), and Ades & Glaeser (1995). By relocating capability closer to where corruption is occurring, the reform breaks the self-reinforcing urban primacy equilibrium that concentrates forensic capacity in Jakarta. Mobile expert teams provide a capacity equity mechanism for remote jurisdictions without requiring full laboratory replication, a design consistent with the cost-effectiveness constraints emphasized by Smoke (2001).

Third, specialized task forces combining digital forensics and financial analysis expertise address the capability threshold problem documented in 5.3. The multi-platform correlation and financial-complexity demands identified in 74% and 82% of corruption cases require cross-disciplinary teams that general courts cannot assemble case-by-case. A national registry of certified expert witnesses, aligned with the competence framework of Sunde & Dror (2021), would further reduce the reliability and bias risks that

threaten the quality of expert testimony in current practice.

Fourth, targeted EIT Law amendments specifying concrete authentication, preservation, and verification procedures would close the KUHAP procedural gap identified by Komalasari & Mustafa (2023) and reduce the judicial inconsistency documented by Sumilat & Ginting (2023), Manurung & Harefa (2024), and Sukmasari et al. (2024). Without such amendments, even well funded institutions face the discretion by default problem that makes street level bureaucracy outcomes unpredictable. Taken together, the reform package is coherent with the study's theoretical framework: it addresses legal text, institutional capacity, resource distribution, and organizational incentives as a single system, rather than treating any one dimension as sufficient on its own.

5. CONCLUSION

This study set out to answer three questions about digital evidence in Indonesian courts between 2010 and 2023. The findings are as follows. On RQ1 (temporal evolution), digital evidence usage grew more than tenfold over the period, progressing through three identifiable phases: an emerging phase (2010–2014), an expansion phase (2015–2018), and an acceleration phase (2019–2021). Growth, however, was overwhelmingly concentrated in non-corruption categories; corruption cases remained stable at 30–50 per year, indicating that institutional capacity for forensically sound corruption evidence expanded far more slowly than the underlying digital transformation of Indonesian society.

On RQ2 (categorical quality), forensic practice in Indonesia is sharply stratified. Corruption cases handled by the KPK approximate ACPO and ISO/IEC 27037 standards, achieving 76–83% compliance across core indicators, while EIT (12–24%), religious (3–7%), and civil cases fall far below this level. This pattern constitutes a dual-track system operating under

identical legislation. Lastly, on RQ3 (institutional and geographic variation), Jakarta's Corruption Court reaches 85.1% forensic compliance versus 22.7% in provincial courts, a 62 percentage point gap that cannot be attributed to differences in legal text. Institutional capacity and resource distribution, not legal standards, determine evidentiary quality.

All in all, these findings show that legal reform is necessary but insufficient. The study's four part proposal tiered national standards, regional forensic centers, specialized task forces, and targeted legislative amendments operationalizes an institutional capacity response rather than a framework only one.

For further research, four directions would be beneficial for deeper exploration. First, longitudinal studies tracking reform implementation could assess whether proposed interventions reduce observed disparities or whether institutional path dependencies prevent meaningful change. Second, cross country comparison with other developing jurisdictions would test whether the institutional capacity hypothesis generalizes beyond Indonesia. Third, interview based work with judges, prosecutors, investigators, and defense attorneys could illuminate decision-making processes that documentary analysis cannot capture. Fourth, cost-benefit analysis of the proposed reforms would inform resource allocation by quantifying quality improvements against implementation costs.

REFERENCES

- Ades, A. F., & Glaeser, E. L. (1995). Trade and Circuses: Explaining Urban Giants. *The Quarterly Journal of Economics*, 110(1), 195-227. <https://doi.org/10.2307/2118515>.
- Ali, S., & Bakhtiar, H. S. (2024). Audit Forensik dan Bukti Digital dalam Mengungkap Kasus Korupsi Birokrasi. *Jurnal Akuntansi dan Keuangan*, 15(2), 145-162.

- Association of Chief Police Officers (ACPO). (2012). *ACPO Good Practice Guide for Digital Evidence (Version 5.0)*. National Policing Improvement Agency.
- Bhat, W. A., AlZahrani, A., & Wani, M. A. (2021). Can Computer Forensic Tools be Trusted in Digital Investigations?. *Science & Justice*, 61(2), 198–203.
- Buehler, M. (2010). *Decentralisation and Local Democracy in Indonesia: The Marginalisation of the Public Sphere*. Institute of Southeast Asian Studies.
- Butt, S., & Lindsey, T. (2012). *The Constitution of Indonesia: A Contextual Analysis*. Hart Publishing.
- Carrier, B., & Spafford, E. H. (2004). Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence*, 2(2), 1-20.
- Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.)*. Academic Press.
- Casey, E., & Turnbull, B. (2018). *Digital Evidence on Mobile Devices*. Academic Press.
- Daskal, J. (2015). The Un-Territoriality of Data. *The Yale Law Journal*, 125(2), 326-398.
- Fukuyama, F. (2013). What is Governance?. *Governance*, 26(3), 347-368. <https://doi.org/10.1111/gove.12035>.
- Gallagher, M. E. (2006). Mobilizing the Law in China: “Informed Disenchantment” and the Development of Legal Consciousness. *Law & Society Review*, 40(4), 783-816. <https://doi.org/10.1111/j.1540-5893.2006.00283.x>.
- Garfinkel, S. L. (2010). Digital Forensics Research: The Next 10 years. *Digital Investigation*, 7, S64-S73. <https://doi.org/10.1016/j.diin.2010.05.009>.
- Garrie, D. B., & Morrissy, R. L. (2014). Digital Forensic Evidence in the Courtroom: Understanding Content and Quality. *Northwest Journal of Technology and Intellectual Property*, 12(2), 121-152.
- Grindle, M. S. (1997). *Getting Good Government: Capacity Building in the Public Sectors of Developing Countries*. Harvard Institute for International Development.
- Halliday, T. C., & Shaffer, G. (Eds.). (2015). *Transnational Legal Orders*. Cambridge University Press.
- Henderson, J. V. (2002). Urbanization in Developing Countries. *The World Bank Research Observer*, 17(1), 89-112. <https://doi.org/10.1093/wbro/17.1.89>.
- Horsman, G., & Sunde, N. (2022). Unboxing the Digital Forensic Investigation Process. *Science & Justice*, 62(2), 171–180.
- Horsman, G. (2023). Digital Evidence Strategies for Digital Forensic Science Examinations. *Science & Justice*, 63(1), 116–126.
- International Organization for Standardization. (2012). *ISO/IEC 27037:2012 Information Technology Security Techniques Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. International Organization for Standardization.
- International Organization for Standardization. (2015). *ISO/IEC 27042:2015 Information Technology Security Techniques Guidelines for the Analysis and Interpretation of Digital Evidence*. International Organization for Standardization.

- Karie, N. M., & Venter, H. S. (2015). Taxonomy of Challenges for Digital Forensics. *Journal of Forensic Sciences*, 60(4), 885-893. <https://doi.org/10.1111/1556-4029.12757>
- Kerr, O. S. (2005). Digital Evidence and the New Criminal Procedure. *Columbia Law Review*, 105(1), 279-318.
- Komalasari, R., & Mustafa, A. (2023). Implementasi Undang-Undang Informasi dan Transaksi Elektronik dalam Sistem Peradilan Pidana Indonesia. *Jurnal Hukum Pidana*, 18(3), 234-251.
- Lipsky, M. (2010). *Street-Level Bureaucracy: Dilemmas of the Individual in Public Service (30th Anniversary Expanded Edition)*. Russell Sage Foundation.
- Manurung, K., & Harefa, B. (2024). The Validity of Electronic Evidence and its Relation to Personal Data Protection in the Indonesian Legal System. *International Journal of Cyber Criminology*, 18(1), 45-62.
- Montasari, R. (2016). A Comprehensive Digital Forensic Investigation Process Model. *International Journal of Electronic Security and Digital Forensics*, 8(4), 285-302. <https://doi.org/10.1504/IJESDF.2016.079430>.
- Organisation for Economic Co-operation and Development (OECD). (2019). *Resolving Foreign Bribery Cases with non-Trial Resolutions: Settlements and Non-Trial Agreements by Parties to the Anti-Bribery Convention*. OECD Publishing. <https://doi.org/10.1787/9789264302105-en>.
- Peerenboom, R. (2002). *China's Long March Toward Rule of Law*. Cambridge University Press.
- Quick, D., & Choo, K. K. R. (2014). Big Forensic Data Reduction: Digital Forensic Images and Electronic Evidence. *Cluster Computing*, 17(3), 723-740. <https://doi.org/10.1007/s10586-013-0312-6>.
- Rodden, J. (2004). Comparative Federalism and Decentralization: On Meaning and Measurement. *Comparative Politics*, 36(4), 481-500. <https://doi.org/10.2307/4150172>.
- Smoke, P. (2001). *Fiscal Decentralization in Developing Countries: A Review of Current Concepts and Practice*. United Nations Democracy Fund.
- Sukmasari, A., Frederik, W., Kalalo, M. E., & Soepeno, M. H. (2024). Application of Electronic Evidence in Corruption Crime Investigations in Indonesia. *International Journal of Law and Management*, 66(2), 178-195.
- Sumilat, R. R. I., & Ginting, G. (2023). Legal Study of the Existence of Electronic Evidence in Corruption Eradication Efforts in Indonesia. *Jurnal Hukum dan Pembangunan*, 53(4), 823-841.
- Sunde, N., & Dror, I. E. (2021). A Hierarchy of Expert Performance (HEP) Applied to Digital Forensics: Reliability and Biasability in Digital Forensics Decision Making. *Forensic Science International: Digital Investigation*, 37, 301175.
- Transparency International. (2018). *Corruption Perceptions Index 2018*. Transparency International Secretariat.
- Transparency International. (2023). *Corruption Perceptions Index 2023*. Transparency International Secretariat.
- Trubek, D. M., & Santos, A. (Eds.). (2006). *The New Law and Economic Development: A Critical Appraisal*. Cambridge University Press.
- Tully, G., Cohen, N., Compton, D., Davies, G., Isbell, R., & Watson, T. (2020). Quality Standards for Digital Forensics: Learning from Experience in England & Wales. *Forensic Science International: Digital Investigation*, 32, 200905.

- United Nations Office on Drugs and Crime. (2018). *State of implementation of the United Nations Convention Against Corruption: Criminalization, Law Enforcement and International Cooperation (2nd ed.)*. United Nations.
- United Nations Office on Drugs and Crime. (2020). *Comprehensive Study on Cybercrime (Draft)*. United Nations.
- U.S. Department of Justice. (2016). *United States Seeks to Recover Approximately \$1 Billion Obtained from Corruption Involving Malaysian Sovereign Wealth Fund [Press release]*. U.S. Department of Justice
- Wigana, A., & Maryanto, M. (2020). The Strength of Proof of Telephone Tapping as Electronic Evidence in Corruption Cases. *Jurnal Hukum Ius Quia Iustum*, 27(3), 567-586.