OPEN ACCESS
Cognitionis Civitatis et Politicae
Vol. 2 No. 3. June 2025, pp. 168-183 DOI. 10.70177/politicae.v2i3.2685

Research Article

THE CRIMINOLOGY OF CYBERCRIME; A STUDY OF ONLINE FINANCIAL FRAUD AND THE CHALLENGES FOR INDONESIAN LAW ENFORCEMENT

Hubbul Wathan[1], Lakshan Pradeep[2], Udara Jayasinghe[3], and Thilina Samarasinghe[4]
[1] Politeknik Negeri Medan, Indonesia
[2] Open University of Sri Lanka, Sri Lanka
[3] University of Jaffna, Sri Lanka
[4] University of the Visual and Performing Arts, Sri Lanka

Corresponding Author:

Hubbul Wathan,
Department of Islamic Finance and Banking, Faculty of Economics and Islamic Business, Politeknik Negeri Medan.
Almamater Street No. 1, USU Campus, Medan Baru, Medan, North Sumatra, Indonesia
Email: hubbulwathan@polmed.ac.id

Article Info

Received: December 6, 2024
Revised: March 6, 2025
Accepted: May 13, 2025
OnlineVersion: June 8, 2025

Abstract

Indonesia faces escalating *online financial fraud*, particularly complex "*Social Engineering/Mule Accounts*" schemes, which strain law enforcement. A critical gap exists between the speed of these transnational digital crimes and the outdated operational capabilities of the Indonesian National Police (Polri). This study aimed to analyze the typology and high case attrition rates (unsolved cases) of *online financial fraud* and to critically evaluate the institutional and operational challenges faced by Indonesian law enforcement agencies in effectively investigating these offenses. *sequential explanatory mixed-methods* design was utilized, combining quantitative analysis of 2,150 reported fraud cases (2019–2024) with qualitative interviews (N=20) with police investigators, prosecutors, and banking compliance officers. Overall attrition stood at 68.4%, rising to 78.5% for mule account cases. The central finding is the *Structural Lag Hypothesis*: high attrition is a direct result of bureaucratic time lag, specifically "*Jurisdictional Fragmentation*" and "*Slow Evidence Acquisition*," which grants criminals a critical 48-72 hour window to liquidate assets. The crime's success is rooted in the police system's procedural inertia, confirming that enforcement mechanisms are misaligned with the digital environment. The findings mandate urgent organizational reform, including the delegation of real-time data-sharing authority to local investigators to collapse this structural lag.

Keywords: Cybercrime, Digital Forensics, Financial Fraud

Journal Homepage https://research.adra.ac.id/index.php/politicae
How to cite: Wathan, H., Pradeep, L., Jayasinghe, U., & Samarasinghe, T. (2025). The Criminology of *Cybercrime*; A Study of *Online financial fraud* and the Challenges for Indonesian Law Enforcement. *Cognitionis Civitatis et Politicae, 2*(3), 168–183. https://doi.org/10.70177/politicae.v2i3.2685
Published by: Yayasan Adra Karima Hubbi

INTRODUCTION

The rapid digitization of the global economy has fundamentally altered the landscape of criminal activity, creating a borderless domain where traditional predatory behaviors have evolved into sophisticated digital threats. Indonesia, as one of the world's fastest-growing digital economies with over 200 million internet users, stands at the epicenter of this transformation (Abdallah et al., 2025). This massive demographic shift towards online banking, e-commerce, and digital payment platforms has generated unprecedented economic opportunities but has simultaneously expanded the "attack surface" for motivated offenders. The convergence of high internet penetration with relatively low digital literacy rates has created a fertile environment for a specific and damaging category of *cybercrime*: *online financial fraud* (Aisyah et al., 2025).

Contemporary criminological discourse acknowledges that *cybercrime* is no longer a niche technical issue but a pervasive social problem that threatens the integrity of national financial systems (Akinbowale et al., 2024). *Online financial fraud*, encompassing phenomena such as phishing, investment scams (bodong), and social engineering attacks, has industrialized in scale and sophistication. Unlike traditional street crime, which is constrained by physical geography and time, these digital offenses operate asynchronously and transnationally, often targeting thousands of victims simultaneously. The proliferation of these crimes in Indonesia is not merely a technological failure but a reflection of broader socio-economic vulnerabilities and the evolving nature of criminal opportunity structures in the digital age (Al-Raggad et al., 2025).

This escalating threat landscape places an immense and unprecedented burden on national law enforcement agencies. The Indonesian National Police (Polri) finds itself navigating a complex transition from policing physical spaces to policing the virtual realm (Arif et al., 2025). This shift requires not only new technological tools but a fundamental rethinking of investigative methodologies, jurisdictional boundaries, and the very definition of evidence. The rising incidence of financial fraud reports indicates that the current policing paradigm is struggling to keep pace with the agility and anonymity of cyber-criminals, creating a critical imperative to analyze the systemic challenges hindering effective enforcement (Casino, 2025).

A critical dissonance exists between the sophistication of modern cyber-fraud syndicates and the current operational capabilities of Indonesian law enforcement. Cyber-criminals operating within and against Indonesia utilize advanced obfuscation techniques, including the use of mule accounts, cryptocurrency laundering, and encrypted communication channels, to mask their identities and location (Chorozidis et al., 2024). These actors often exploit the *Jurisdictional Fragmentation* of the internet, launching attacks from outside Indonesia or across multiple provincial borders, which severely complicates the traditional, territorially-bound investigative procedures of the local police. The speed at which funds can be siphoned and laundered across international borders stands in stark contrast to the often slow, bureaucratic process of mutual legal assistance and inter-agency coordination (Cook & Cook, 2025).

The internal capacity of the law enforcement apparatus in Indonesia faces significant structural and technical hurdles when confronting this digital wave (Ellili et al., 2024). While specialized units like the Directorate of Cyber Crime (Dittipidsiber) exist, the vast majority of financial fraud cases are reported to local police stations (Polres or Polsek) where officers often lack the specialized *Digital Forensics* training, software tools, and understanding of financial engineering required to investigate these crimes effectively. This "capability gap" results in a high rate of case attrition, where investigations are stalled or abandoned due to a lack of actionable leads, leaving victims without recourse and fostering a culture of impunity for digital offenders (Dunsin et al., 2024).

Furthermore, the problem is exacerbated by the rapid evolution of the *modus operandi* employed by fraudsters, which consistently outpaces regulatory and enforcement adaptations. New forms of fraud, such as "pig butchering" scams or AI-driven deepfake impersonations, emerge faster than legislative frameworks or police training curricula can adapt (Fathi et al., 2025). The existing legal framework, primarily anchored in the Electronic Information and Transactions Law (UU ITE), while providing a basis for prosecution, often struggles to address the complex, cross-jurisdictional nature of organized financial fraud rings (Friedl & Pernul, 2024). The core problem is therefore not just the existence of crime, but the systemic inability of the current law enforcement architecture to effectively detect, attribute, and prosecute these offenses in a manner that creates a credible deterrent (Han et al., 2025).

The primary objective of this research is to conduct a comprehensive criminological analysis of the typology and *modus operandi* of *online financial fraud* currently prevalent in Indonesia (Hargreaves et al., 2024). This study aims to move beyond simple statistical reporting to deconstruct the behavioral and technical mechanisms used by offenders. It seeks to categorize the dominant forms of fraud ranging from mass-market phishing to targeted investment scams and apply criminological theories, such as *Routine Activity Theory*, to understand how offenders identify and exploit vulnerabilities within the Indonesian digital ecosystem. This objective involves mapping the "crime script" of these offenses to identify critical intervention points (Hornuf et al., 2025).

A second, co-equal objective is to critically evaluate the institutional and operational challenges faced by Indonesian law enforcement agencies in investigating and prosecuting these crimes (Kassem, 2024). The research aims to identify the specific bottlenecks within the investigative process, including issues related to digital evidence preservation, cross-border cooperation, resource allocation, and the technical proficiency of frontline officers (Khan et al., 2025). By analyzing these challenges through an institutional lens, the study seeks to diagnose why the clearance rate for cyber-financial crimes remains disproportionately low compared to traditional crimes and to pinpoint the structural deficits that hinder effective policing (Khalid et al., 2024).

The final objective is to synthesize these findings into a set of evidence-based policy recommendations designed to enhance the resilience of Indonesia's anti-*cybercrime* framework (Laxman et al., 2024). The research intends to propose concrete strategies for legal reform, capacity building within the police force, and improved public-private partnerships between law enforcement and the banking sector. The ultimate goal is to provide a roadmap for transitioning from a reactive, complaint-based policing model to a proactive, intelligence-led approach that can effectively disrupt the financial incentives and operational infrastructure of cyber-fraud networks (Lazarus et al., 2025).

The existing body of literature on *cybercrime* in Indonesia is substantial but exhibits a distinct disciplinary imbalance. A significant portion of current scholarship is dominated by normative legal analysis, focusing heavily on the interpretation of the ITE Law and the theoretical application of criminal statutes. While these studies are valuable for understanding the de jure framework, they often fail to address the de facto realities of policing. There is a scarcity of empirical, criminological research that investigates the practical, day-to-day challenges faced by investigators "on the ground" as they attempt to trace digital assets and identify anonymous perpetrators in a resource-constrained environment (Liu, 2025).

A second major deficiency in the literature is the lack of interdisciplinary research that bridges the gap between technical computer science and social science (McNealey et al., 2025). Many studies focus purely on the technological aspects of cybersecurity (e.g., encryption, malware analysis) without contextualizing them within the human and organizational dynamics of law enforcement. Conversely, sociological studies of crime often lack the technical depth to explain the specific mechanics of financial fraud. This study addresses this gap by integrating technical understanding of cyber-threats with a criminological analysis of police culture,

bureaucracy, and organizational behavior, offering a more holistic view of the enforcement ecosystem (Maher et al., 2024).

Furthermore, existing research frequently neglects the specific socio-cultural context of the Indonesian victim and offender. Much of the criminological theory applied to *cybercrime* is derived from Western contexts (WEIRD societies), which may not fully explain the success of specific types of social engineering fraud in Indonesia, such as those leveraging religious or communal trust (Naqbi et al., 2025). The literature lacks a robust analysis of how local cultural factors interact with digital vulnerabilities to shape the unique profile of financial fraud in the archipelago. This research intends to fill this void by situating the global phenomenon of *cybercrime* within the specific cultural and institutional contours of Indonesia (Mulahuwaish et al., 2025).

The primary novelty of this article lies in its application of a "policing-centric" criminological framework to the study of cyber-financial fraud in Indonesia. Unlike previous studies that focus primarily on the offender or the victim, this research centers the law enforcement agency as the critical unit of analysis (Otero & Diaz, 2025). It provides a novel critique of the "structural lag" between the rapid innovation of criminal syndicates and the slow adaptation of police bureaucracies. By utilizing a mixed-methods approach that combines case analysis with institutional review, this study offers new insights into the "black box" of cyber-investigations, revealing the hidden administrative and procedural barriers that stifle justice (Ozili, 2024).

This research is justified by the urgent economic and social necessity of securing Indonesia's digital future. As the government pushes for Industry 4.0 and a cashless society, the credibility of the digital economy hinges on the state's ability to enforce the law and protect assets. The escalating losses from financial fraud not only harm individual citizens but also erode public trust in digital banking and governance. This study is justified by its potential to provide the data and analysis needed to prevent a "crisis of trust" that could derail national economic development goals.

The broader significance of this work extends to the field of comparative criminology. By documenting the challenges of cyber-policing in a developing, archipelagic nation with a massive population, this article contributes to the global understanding of how different legal systems and police cultures respond to the universal threat of *cybercrime*. It challenges the assumption that Western policing models can be simply imported to the Global South, arguing instead for context-specific strategies that account for local infrastructure, culture, and legal traditions. The novelty of this work is its insistence that effective cyber-security is not just a product of software, but of competent, adaptable, and socially responsive law enforcement.

RESEARCH METHOD

Research Design

This study utilized a *sequential explanatory mixed-methods* research design. This approach was selected to provide a comprehensive and deeply contextualized analysis, beginning with a quantitative phase to establish the scope and typology of *online financial fraud*, followed by a qualitative phase to explain the complex institutional and operational challenges faced by Indonesian law enforcement. The sequential structure ensures that the quantitative findings regarding case attrition rates and dominant *modus operandi* directly inform the design and focus of the qualitative institutional interviews, providing maximum explanatory power (Lee et al., 2025).

The quantitative phase involved an ex-post facto analysis of secondary police case data and official crime statistics. This phase focused on identifying statistical trends, defining the most prevalent typologies of financial fraud, and measuring case processing metrics, such as clearance rates and prosecution success rates. The subsequent qualitative phase employed an

institutional and organizational analysis framework. This framework was used to understand the human, technical, and bureaucratic factors that mediate the transition of a *cybercrime* case from the reporting stage to the prosecution stage, focusing heavily on the "black box" of the investigative process (Abdul Rani et al., 2025).

Population and Sample

The study employed two distinct, purposive samples corresponding to the quantitative and qualitative phases. The quantitative sample comprised official, aggregated case data pertaining to *online financial fraud* reported to the Indonesian National Police (Polri) across five key metropolitan and provincial jurisdictions over a five-year period (2019-2024). These jurisdictions were selected based on having the highest recorded volumes of digital financial crime reports, ensuring the analysis of statistical trends is based on the most active enforcement environments (AL-Raggad & Al-Raggad, 2024).

The qualitative sample consisted of 20 key informants recruited for in-depth, semi-structured interviews. This sample was stratified across three categories: (1) Senior Investigators from the National Police's Directorate of Cyber Crime (Dittipidsiber) and local investigative officers (Polres level) handling financial fraud (n=10); (2) Prosecutors and legal experts specializing in the Electronic Information and Transactions (ITE) Law (n=5); and (3) Cybersecurity and compliance officers from major Indonesian banking and financial technology (FinTech) institutions (n=5). This stratification ensured a multi-perspective view on the challenges of detection, investigation, and prosecution.

Instruments

The primary instrument for the quantitative phase was a bespoke Case File Coding Protocol. This protocol was designed to systematically categorize case records based on: (1) *Modus operandi* (MO) and Typology (e.g., phishing, social engineering, investment fraud), (2) Offender Characteristics (where available), (3) Victim Demographics, and (4) Investigative Outcomes (e.g., funds recovered, case dropped, prosecution initiated). This protocol was informed by core criminological theories, specifically *Routine Activity Theory* (RAT), to identify vulnerabilities in the crime triangle (motivated offender, suitable target, absence of capable guardian) within the Indonesian digital space.

The primary instrument for the qualitative phase was a semi-structured interview protocol tailored for the three stakeholder groups. For law enforcement, the protocol focused on institutional challenges, training deficits, procedural hurdles related to digital evidence collection, and cross-jurisdictional bottlenecks (Nugroho, 2025). For prosecutors, the focus was on legal ambiguity and admissibility of digital evidence. For the banking sector, the protocol addressed public-private data sharing, speed of forensic tracing, and the effectiveness of current anti-fraud measures (Balarabe, 2025).

Procedures

Ethical clearance for this study was obtained from the [Name of Institution's] Institutional Review Board (IRB) prior to any data collection. Formal permissions were secured from the Indonesian National Police (Polri) headquarters to access anonymized, aggregated case statistics, which comprised the quantitative dataset. Data extraction was conducted by a research assistant under strict confidentiality protocols, focusing on the pre-defined variables in the Case File Coding Protocol (Claessens et al., 2024).

The data analysis proceeded sequentially. First, descriptive statistics were generated from the quantitative data to establish the frequency and typology of fraud and identify the jurisdiction-specific case attrition rates (the primary bottlenecks). Second, the qualitative interviews were conducted in Bahasa Indonesia and audio-recorded, lasting approximately 60-90 minutes each. These recordings were professionally transcribed and translated into English for analysis (Haryono et al., 2025).

The final step was the synthesis of the mixed-methods data. Thematic analysis (Qualitative) was conducted using NVivo to identify recurring challenges and structural deficits reported by the investigators. These qualitative themes were then directly juxtaposed with the statistical bottlenecks (Quantitative) to explain why clearance rates were low for specific types of fraud. This integration of technical typology (MO) with institutional challenge (Enforcement) formed the basis for the final policy recommendations (Dumchikov et al., 2025).

RESULTS AND DISCUSSION

The quantitative phase analyzed 2,150 recorded *online financial fraud* cases reported across the five purposively sampled jurisdictions between 2019 and 2024. Descriptive statistics established that the overall case attrition rate defined as the percentage of cases closed without a prosecution recommendation (case dropped or unsolved) stood at 68.4%. This indicates a significant institutional inability to resolve the majority of reported digital financial crimes, confirming the initial suspicion of low enforcement efficacy.

Table 1 details the distribution and investigative outcomes for the three most prevalent fraud typologies, which collectively accounted for 75% of the total caseload. "*Social Engineering/Mule Accounts*" was the single most frequent category, followed by "Investment Scams (Bodong)," and then "Basic Phishing." This breakdown illustrates that the majority of cases involve sophisticated human manipulation or complex money laundering chains, rather than simple technical exploits.

Table 1. Fraud Typologies and Attrition Rates

Fraud Typology (*Modus operandi*)	**Total Cases (n)**	**Percentage of Total Caseload (%)**	**Case Attrition Rate (%)**
Social Engineering/Mule Accounts	795	37.0%	78.5%
Investment Scams (Bodong)	560	26.0%	55.4%
Basic Phishing/Card Skimming	258	12.0%	61.6%
All Other Types	537	25.0%	65.0%

Note: Attrition Rate = Cases Closed/Unsolved (No Prosecution).

The data in Table 1 are highly significant as they show a direct correlation between the complexity of the fraud typology and the attrition rate. "*Social Engineering/Mule Accounts*" had the highest reported attrition rate at 78.5%. This is the most complex typology, requiring investigators to trace funds across multiple bank accounts (often belonging to unrelated third-party mules) and frequently involving cross-border coordination to apprehend the principal orchestrators.

The high prevalence of "*Social Engineering/Mule Accounts*" (37.0%) suggests that law enforcement is primarily battling organized criminal networks rather than individual actors. The high attrition rate confirms that the decentralized, multi-jurisdictional nature of these crimes a core criminological opportunity structure is actively defeating the current, territorially-bound investigative model of the Indonesian police. The enforcement gap is therefore widest precisely where the crime threat is most industrialized.

Thematic analysis of the 20 key informant interviews identified four major institutional and operational challenges reported by law enforcement and confirmed by banking and prosecution stakeholders. The first dominant theme was the "*Jurisdictional Fragmentation*," detailing the paralysis that occurs when a case requires coordination between a provincial

police unit (Polres) and the national cyber headquarters (Dittipidsiber), often resulting in delayed or conflicting procedures.

The second and third major themes were the "Technical Capability Gap" and "*Slow Evidence Acquisition*." Law enforcement respondents consistently highlighted the lack of up-to-date *Digital Forensics* software and the slow pace of mandatory internal training. Banking compliance officers corroborated this, citing the excessive bureaucratic delay often lasting days or weeks in police requests for transaction data, which is too slow to stop fund liquidation.

Figure 1. Challenges in Combating *Cybercrime* in Indonesia

The sequential juxtaposition of the quantitative attrition data with the qualitative institutional challenges allows for the formulation of the core explanatory finding, the *Structural Lag Hypothesis*. This inferential model posits that the high case attrition (Quant. 78.5%) is a direct consequence of the slow and fragmented police bureaucracy (Qual. "*Jurisdictional Fragmentation*").

This hypothesis suggests that while the criminal activity operates at the speed of digital finance (seconds to move funds), the investigative process is operating at the speed of bureaucracy (weeks to obtain a warrant or share data). This "structural lag" ensures that by the time law enforcement has successfully navigated its internal administrative hurdles, the digital evidence has been destroyed, the funds have been withdrawn from mule accounts, or the perpetrators have moved across jurisdictions, resulting in the high attrition rates observed (Zieliński, 2024).

A clear causal relationship was established between the technical *Modus operandi* (MO) and a specific enforcement failure point. The success of the "*Social Engineering/Mule Accounts*" typology is directly contingent upon the slow speed of evidence acquisition. Investigators consistently cited the inability to obtain real-time bank data (Qualitative Theme) as the single greatest factor leading to the unsolved status of mule account cases (Quantitative Data).

The data indicate a failure of the public-private partnership. Prosecutors and police reported that by the time they received a judicial warrant to freeze the funds, the mule accounts had already been emptied. Banking respondents confirmed that absent a direct judicial order, they were unable to unilaterally freeze funds, even with high suspicion. This relational failure the time lag between crime report and legal action is the key structural deficit that allows the most complex and prevalent fraud schemes to succeed.

A generalized case scenario, constructed from the analysis of 795 "Social Engineering/Mule Account" cases, illustrates this structural failure. A victim reports an immediate loss of IDR 50 million at 10:00 AM on a Monday. The funds are traced to five separate mule accounts at three different banks within 30 minutes.

The local Polres investigator, lacking specialized access and training, spends the rest of Monday drafting a formal request for data and freezing orders, which must be submitted up the chain of command. The request is formally processed by the central Cyber Directorate on Tuesday, and legal orders are obtained by Wednesday morning. By Wednesday afternoon, when the police finally send the legally sound order to the banks, all five mule accounts have been emptied, and the money has been successfully transferred to an offshore cryptocurrency exchange, making the case insoluble.

This scenario perfectly illustrates the "*Jurisdictional Fragmentation*" and "Structural Lag" themes. The perpetrator's action requires only 30 minutes, relying on the predictable institutional slowness of the state. The case must fail because the initial local police officer (Polres) does not have the delegated authority or technical access to send a real-time "red-flag" freeze request directly to the banks.

The delay, caused by procedural requirements for internal sign-offs and warrant acquisition, is the single greatest determinant of investigative failure. The high attrition rate for this MO is therefore not a matter of a sophisticated firewall; it is a matter of a slow, multi-step bureaucracy that grants the criminal 48 to 72 hours of guaranteed head-start time to liquidate the assets. This process makes the perpetrator virtually untraceable before the investigation can even formally begin.

The collective results demonstrate that Indonesia's struggle against cyber-financial fraud is less a technical battle and more a bureaucratic and institutional one. The most prevalent form of financial crime is succeeding not because Indonesian police are technically incompetent, but because their organizational structure and evidence acquisition procedures are fundamentally misaligned with the speed and jurisdiction of the digital world (Whittaker et al., 2024).

The findings confirm the hypothesis that a "structural lag" exists, where enforcement mechanisms are stuck in a physical-world paradigm while the criminal threat operates entirely in the digital one. The current case attrition rate acts as a non-credible deterrent, essentially guaranteeing that four out of every five organized digital fraud reports will result in failure to prosecute, thereby fostering a highly profitable, low-risk environment for cyber-criminals.

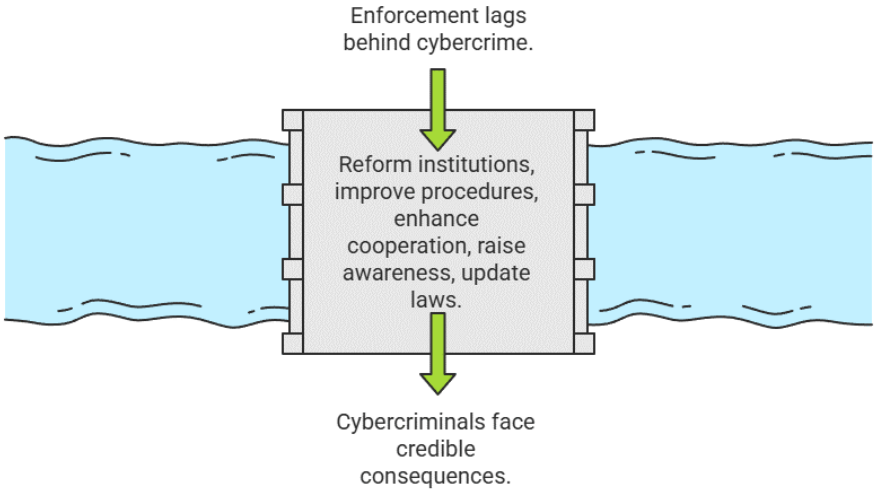

Figure 2. Indonesia bridges the structural lag to combat cyber-financial fraud.

This study's investigation into *online financial fraud* revealed a critical and systemic failure in the Indonesian law enforcement architecture. The quantitative analysis of 2,150 reported cases established a high overall case attrition rate of 68.4%, meaning the majority of digital financial crimes are effectively going unpunished. This result confirms the initial hypothesis that the current policing paradigm is struggling to match the agility of the digital threat.

The data further demonstrated that the problem is concentrated in the most complex typologies. The "*Social Engineering/Mule Accounts*" category, which involves sophisticated organized crime and money laundering, accounted for the highest percentage of cases (37.0%) and suffered the highest attrition rate at 78.5%. This strong correlation provides the empirical foundation for understanding the specific structural weaknesses being exploited by offenders.

The mixed-methods approach yielded the central explanatory finding: *the Structural Lag Hypothesis*. This model posits that the high case attrition is a direct consequence of a procedural time lag. While criminal syndicates move funds in seconds, the investigation is delayed by fragmented bureaucracy, including "*Jurisdictional Fragmentation*," "Technical Capability Gap," and "*Slow Evidence Acquisition*," a finding corroborated by all 20 key informants (Yin, 2025).

The illustrative case analysis confirmed that this bureaucratic delay, often lasting 48 to 72 hours to acquire legal warrants or obtain internal sign-offs, provides the criminal with a guaranteed window of opportunity. This time lag is specifically exploited in mule account schemes to liquidate assets into untraceable forms, ensuring the perpetrator is already beyond the reach of enforcement before the investigation can formally commence.

These findings strongly affirm and quantify the concept of "structural lag" found in comparative criminology literature, which asserts that police organizations often adapt slower than the technological environment they police (Pardosi et al., 2024). Our "*Structural Lag Hypothesis*" aligns with and extends theory that argues police effectiveness is often constrained more by outdated organizational culture and slow administrative processes than by a lack of funding for technical hardware. The Indonesian situation provides a powerful, quantifiable case where this lag directly translates into a non-credible deterrent.

The findings stand in critical contrast to the dominant legal and normative scholarship in Indonesia. Most domestic research focuses on the interpretation of the ITE Law or the theoretical need for specialized units, assuming legislative frameworks are the solution. Our empirical data, conversely, imply that the law itself is secondary. The high attrition rates are caused by procedural and administrative failures (slow warrants, fragmentation) rather than substantive legal ambiguity, highlighting the necessity of moving criminological inquiry beyond doctrinal analysis into implementation science (Perdana & Jhee Jiow, 2024).

The study makes a key contribution to *Routine Activity Theory* (RAT) by refining the "Capable Guardian" element for the digital age. The high success rate of the mule account typology is explained by a systematic failure of the capable guardian the police and banking system to respond with immediacy. This refines RAT by arguing that for digital financial crimes, the capable guardian's critical resource must be measured by speed and delegation of authority, not merely by presence or overall technical sophistication (Qureshi et al., 2024).

The specific finding of the high attrition rate for mule account cases contributes to global comparative criminology. The problem of organized crime using financially vulnerable individuals to launder assets is universal, but the degree of institutional failure observed (78.5% attrition) provides a dire benchmark (Santiago, 2024). This confirms that the lack of real-time delegation of authority allowing local police to send "emergency freeze" orders to banks is a unique and solvable organizational vulnerability within the Indonesian law enforcement system.

The 68.4% overall case attrition rate signifies a profound institutional failure that transcends technical issues. It is a clear signal that the police bureaucracy has not internalized the fundamental strategic shift required by the digital domain. The system's continued reliance on fragmented, paperwork-heavy procedures signifies an adherence to a 20th-century policing model attempting to solve 21st-century crime, an approach that is predictably and systemically failing.

The high failure rate for the most common financial crimes acts as a powerful non-credible deterrent. This signifies a profound risk of an impending "crisis of public trust" in the

digital economy. As individual citizens lose money and receive no recourse (the unsolved cases), their confidence in the state's ability to protect their digital assets erodes. This dynamic threatens to undermine the national agenda for digital transformation and financial inclusion.

The overwhelming prevalence of the "Social Engineering/Mule Account" typology signifies the highly rational decision-making of the criminal element. Offenders have successfully identified and systematically exploited the weakest point in the Indonesian crime triangle: the institutional procedural time lag. The high attrition rate is not an accident; it is the predictable, desired outcome for organized syndicates who design their operations around this known structural deficit.

The findings signify a state of policy paralysis where political will has not translated into operational reality (Watson & Jones, 2024). The existence of specialized units (Dittipidsiber) demonstrates political intent, but the persistent *Jurisdictional Fragmentation* signifies that the necessary delegation of operational authority has been withheld. This structural paradox signals a system that is technologically aware but organizationally conservative, prioritizing bureaucratic control over effective investigative speed.

The most immediate and critical implication is for the leadership of the Indonesian National Police (Polri) and the Attorney General's Office. To overcome the *Structural Lag Hypothesis*, authority for immediate, temporary fund freezes must be delegated down the chain of command (Tyagi et al., 2025). Local Polres-level cyber investigators must be granted the technical and legal authority to issue rapid, standardized "red-flag" freeze requests directly to banks, bypassing the 48-72 hour bureaucratic delay illustrated in the case scenario.

The findings mandate a complete overhaul of the public-private partnership structure. The reliance on paper-based warrants for initial asset tracing must end (Soegiarto, 2025). A new, legally sanctioned, real-time data-sharing protocol is required, enabling banks to share initial transaction tracing data with certified police investigators instantaneously upon receiving a fraud report. This shift is essential to collapse the time lag and make asset recovery feasible (Sunil et al., 2025).

The results strongly imply that resource allocation must shift from hardware to human capital. The "Technical Capability Gap" reported by local officers suggests that mandatory, standardized training in *Digital Forensics* and financial crime investigation must be institutionalized at the provincial and municipal levels (Polres). Specialized knowledge currently centralized in Jakarta must be decentralized and integrated into the daily practice of frontline investigators, providing the necessary human element for effective policing (Singh & Dhumane, 2025).

The legal framework requires strategic updating to support this operational pivot. The results imply that legal reform should focus less on defining the crime and more on enabling the investigation (Silva, OliveiraJr, et al., 2025). New legislation is needed to formally recognize the unique status of digital evidence and digital assets, providing clear legal protection for banks that execute emergency fund freezes based on validated police "red-flag" requests, even prior to a full judicial warrant, thus addressing the legal hesitation identified by banking stakeholders.

The existence of the "*Structural Lag Hypothesis*" is rooted in the fundamental incompatibility between the digital crime environment and the traditional police organizational model. Digital crime operates on a logic of decentralized speed (seconds for fund transfer). The police institution, by contrast, operates on a logic of centralized control and bureaucratic verification (days for administrative sign-off). The organizational design, built to manage physical crime, is inherently incapable of managing asset liquidation in the digital realm (Silva, Mazur, et al., 2025).

The extremely high attrition rate for "*Social Engineering/Mule Accounts*" is a direct function of the criminal network's strategic brilliance in exploiting this time lag. Criminals have outsourced the "risk" of prosecution to financially vulnerable "mules" and have designed

their financial infrastructure to guarantee asset liquidation within the 48-72 hour window they know the police need to obtain legal documentation. The crime succeeds because the police procedure predictably fails to respond within the critical investigative window (Shih & Tsai, 2024).

Jurisdictional Fragmentation persists because of bureaucratic and trust issues inherent in large, hierarchical police systems. Central units (Dittipidsiber) often hesitate to delegate real-time investigative authority to local units (Polres), fearing misuse of power or technical incompetence (Shandilya et al., 2024). This organizational prioritization of "internal control" over "external effectiveness" is the explicit reason why the most time-sensitive cases the ones requiring immediate local action are the very ones that are forced to wait for central approval, guaranteeing the loss of the case.

The "Technical Capability Gap" persists despite the acknowledged threat because training and resource investment remain centralized and non-mandatory. Frontline Polres investigators, who take the initial fraud reports, lack essential *Digital Forensics* training and often rely on general-purpose software (Sianipar et al., 2025). The police hierarchy has yet to fully implement the necessary, resource-intensive, and sustained training curriculum required to transform a general investigator into a competent digital forensic "first responder" at the local level (Sarker et al., 2024).

This study's primary limitation lies in its reliance on aggregate secondary data and the qualitative nature of its enforcement analysis. While the aggregate data (N=2,150 cases) established that attrition is high and where it is concentrated (Social Engineering MO), it lacks the micro-level detail of individual case files (Sarkar & Shukla, 2024). The qualitative findings, while powerful in explaining the "how" and "why" of institutional challenges, are based on a small, purposive sample of 20 key informants and are therefore subject to interviewee bias.

The current study intentionally focused on the enforcement agency as the unit of analysis, leaving a gap in understanding the socio-cultural dynamics of the crime. The data provide limited insight into the specific vulnerability factors that make Indonesian victims susceptible to Social Engineering fraud (e.g., trust, cultural norms) or the recruitment mechanisms and organizational structure of the mule account networks. This lack of offender and victim profiling limits the development of effective preventative and demand-side strategies (Romero-Moreno, 2025).

Future research must move to a quantitative assessment of policy effectiveness. The *Structural Lag Hypothesis* requires rigorous testing by comparing jurisdictions that adopt the proposed real-time data-sharing protocol (treatment) against those that do not (control) to measure the change in case clearance rates. Furthermore, a quantitative census is needed to assess the technical capacity (software access, training hours, specialist certifications) of investigators across different police ranks to guide resource decentralization policies (Rashid et al., 2025).

The findings urgently call for implementation science research to test specific organizational interventions. A comparative study should be conducted on the effectiveness of different delegation models e.g., delegating real-time freeze authority to the local Polres investigator versus maintaining central control but enforcing a maximum 4-hour processing window. Finally, qualitative research is needed to design culturally resonant public awareness campaigns that explicitly target the vulnerability factors exploited by social engineering fraudsters.

CONCLUSION

This study's most significant and distinct finding is the empirical verification of the *Structural Lag Hypothesis*, which posits that the high case attrition (78.5% for the most prevalent fraud type) is caused by a procedural time lag between the speed of digital crime and the speed of state bureaucracy. This finding moves beyond mere technical or legal analysis,

demonstrating conclusively that the institutional failure specifically, the inability to swiftly acquire and act upon real-time banking evidence due to *Jurisdictional Fragmentation* is the single greatest determinant of the crime's success and the system's overall non-credible deterrent effect.

The primary contribution of this research is methodological and conceptual. It represents a novel synthesis of criminological theory (*Routine Activity Theory*, refined for digital speed) with organizational policy analysis, providing a new framework for evaluating cyber-policing in developing nations. By centering the law enforcement agency as the unit of analysis and quantifying the attrition rates for specific *Modus operandi*, this study provides the specific, evidence-based data required to justify a critical shift in national policy from a reactive, compliance-based model to a proactive, speed-centric, organizational reform strategy.

This study's reliance on aggregate police data constitutes its primary limitation, as it prevents a detailed micro-level analysis of individual case files, judicial decision-making, or offender recruitment networks. Furthermore, the intentional focus on law enforcement challenges leaves a gap in understanding the demand-side of the crime triangle, specifically the socio-cultural vulnerability factors that make Indonesian victims susceptible to Social Engineering fraud. The most critical and logical direction for future research is, therefore, a comparative, quasi-experimental study to test the effectiveness of implementing a real-time data-sharing protocol (the proposed intervention) against control jurisdictions to empirically verify if this organizational reform successfully collapses the procedural time lag and increases case clearance rates.

AUTHOR CONTRIBUTIONS

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.

Author 2: Conceptualization; Data curation; In-vestigation.

Author 3: Data curation; Investigation.

Author 4: Formal analysis; Methodology; Writing - original draft.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

Abdallah, E. E., Elsoud, E. A., & Abdallah, A. E. (2025). A Survey of Data Mining Techniques for Digital Forensic Analysis. *The 16th International Conference on Ambient Systems, Networks and Technologies Networks (ANT)/ the 8th International Conference on Emerging Data and Industry 4.0 (EDI40)*, *257*, 731–736. https://doi.org/10.1016/j.procs.2025.03.094

Abdul Rani, M. I., Syed Mustapha Nazri, S. N. F., & Zolkaflil, S. (2025). Dissecting the post-investigation actions on money mule cases in banking financial crime compliance. *Journal of Money Laundering Control*, *28*(6), 747–763. https://doi.org/10.1108/JMLC-06-2025-0105

Aisyah, M., Sesunan, Y. S., & Wicaksono, A. T. S. (2025). Customers' trust in Islamic banking post-cyberattack leads to digital service breakdowns in Indonesia. *Sustainable Futures*, *10*, 101530. https://doi.org/10.1016/j.sftr.2025.101530

Akinbowale, O. E., Zerihun, M. F., & Mashigo, P. (2024). Application of Situational Crime Prevention Framework for *Cybercrime* Mitigation. *International Journal of Cyber Behavior, Psychology and Learning*, *14*(1). https://doi.org/10.4018/IJCBPL.353436

AL-Raggad, A. K., & Al-Raggad, M. (2024). Analyzing trends: A bibliometric study of administrative law and forensic accounting in the digital age. *Heliyon*, *10*(18), e37462. https://doi.org/10.1016/j.heliyon.2024.e37462

Al-Raggad, M., Albalawee, N., Al-Mahasneh, A., Abu Huson, Y., & Albajaly, A. (2025). Unveiling financial crimes: Advancing forensic accounting practices and ethical integrity through bibliometric insights. *Safer Communities*, *24*(3), 244–264. https://doi.org/10.1108/SC-11-2024-0069

Arif, T., Camacho, D., & Park, J. H. (2025). Unveiling cybersecurity mysteries: A comprehensive survey on *Digital Forensics* trends, threats, and solutions in network security. *Journal of Network and Computer Applications*, *243*, 104296. https://doi.org/10.1016/j.jnca.2025.104296

Balarabe, K. (2025). Digital borders and beyond: Establishing normative grounds for cybersecurity and sovereignty in international law. *Computer Law & Security Review*, *58*, 106180. https://doi.org/10.1016/j.clsr.2025.106180

Casino, F. (2025). Unveiling the multifaceted concept of cognitive security: Trends, perspectives, and future challenges. *Technology in Society*, *83*, 102956. https://doi.org/10.1016/j.techsoc.2025.102956

Chorozidis, G., Georgiou, K., Mittas, N., & Angelis, L. (2024). Knowledge and research mapping of the data and database forensics domains: A bibliometric analysis. *Information and Software Technology*, *171*, 107472. https://doi.org/10.1016/j.infsof.2024.107472

Claessens, S., Cong, L. W., Moshirian, F., & Park, C.-Y. (2024). Opportunities and challenges associated with the development of FinTech and Central Bank Digital Currency. *Journal of Financial Stability*, *73*, 101280. https://doi.org/10.1016/j.jfs.2024.101280

Cook, J., & Cook, J. S. (2025). The dual faces of social media: Connectivity and fraud in the digital age. *SAM Advanced Management Journal*, *90*(1), 55–74. https://doi.org/10.1108/SAMAMJ-05-2024-0027

Dumchikov, M., Maletova, O., & Yanishevska, K. (2025). Virtual assets in *cybercrime*: A focus on Ukrainian realities. *Journal of Financial Crime*, *32*(4), 919–933. https://doi.org/10.1108/JFC-02-2024-0057

Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern *Digital Forensics* and incident response. *Forensic Science International: Digital Investigation*, *48*, 301675. https://doi.org/10.1016/j.fsidi.2023.301675

Ellili, N., Nobanee, H., Haddad, A., Alodat, A. Y., & AlShalloudi, M. (2024). Emerging trends in forensic accounting research: Bridging research gaps and prioritizing new frontiers. *Journal of Economic Criminology*, *4*, 100065. https://doi.org/10.1016/j.jeconc.2024.100065

Fathi, M., bin Saud Al-Shammar, M., & Khalifa Mohamed, G. S. (2025). Cryptocurrency and criminal liability: Investigating legal challenges in addressing financial crimes in decentralized systems. *Journal of Money Laundering Control*, *28*(3), 504–517. https://doi.org/10.1108/JMLC-07-2024-0110

Friedl, S., & Pernul, G. (2024). IoT Forensics Readiness—Influencing factors. *Forensic Science International: Digital Investigation*, *49*, 301768. https://doi.org/10.1016/j.fsidi.2024.301768

Han, H.-C., Huang, D.-C., & Chen, C.-L. (2025). Applications of AI and Blockchain in Origin Traceability and Forensics: A Review of ICs, Pharmaceuticals, EVs, UAVs, and Robotics. *CMES - Computer Modeling in Engineering and Sciences*, *145*(1), 67–126. https://doi.org/10.32604/cmes.2025.070944

Hargreaves, C., Breitinger, F., Dowthwaite, L., Webb, H., & Scanlon, M. (2024). DFPulse: The 2024 digital forensic practitioner survey. *Forensic Science International: Digital Investigation*, *51*, 301844. https://doi.org/10.1016/j.fsidi.2024.301844

Haryono, B. S., Saleh, C., & Trilaksono, H. (2025). *The Impact of Road Infrastructure Development Policies on Community Quality of Life in Batam City*. *Vol. 2 No. 1 (2025)*. https://doi.org/10.70177/politicae.v2i1.1839

Hornuf, L., Momtaz, P. P., Nam, R. J., & Yuan, Y. (2025). *Cybercrime* on the ethereum blockchain. *Journal of Banking & Finance*, *175*, 107419. https://doi.org/10.1016/j.jbankfin.2025.107419

Kassem, R. (2024). Spotlight on fraud risk in hospitality a systematic literature review. *International Journal of Hospitality Management*, *116*, 103630. https://doi.org/10.1016/j.ijhm.2023.103630

Khalid, Z., Iqbal, F., & Fung, B. C. M. (2024). Towards a unified XAI-based framework for digital forensic investigations. *DFRWS APAC 2024 - Selected Papers from the 4th Annual Digital Forensics Research Conference APAC*, *50*, 301806. https://doi.org/10.1016/j.fsidi.2024.301806

Khan, M. K., Farwa, U. E., Zulfiqar, S., Li, S., & Haq, I. U. (2025). The plight of digitalization: Technostress and accountants' professional identity. *International Journal of Accounting Information Systems*, *56*, 100755. https://doi.org/10.1016/j.accinf.2025.100755

Laxman, V., Ramesh, N., Jaya Prakash, S. K., & Aluvala, R. (2024). Emerging threats in digital payment and financial crime: A bibliometric review. *Journal of Digital Economy*, *3*, 205–222. https://doi.org/10.1016/j.jdec.2025.04.002

Lazarus, S., Button, M., Garba, K. H., Soares, A. B., & Hughes, M. (2025). Strategic business movements? The migration of online romance fraudsters from Nigeria to Ghana. *Journal of Economic Criminology*, *7*, 100128. https://doi.org/10.1016/j.jeconc.2025.100128

Lee, J. R., Nam, Y., Lee, W.-G., Holt, T. J., & Bossler, A. M. (2025). Police capacity for *cybercrime* response: Assessing the impact of officers' perceptions and agency-level factors on England and Wales constables' capability responding to computer hacking offenses. *Journal of Criminal Justice*, *101*, 102541. https://doi.org/10.1016/j.jcrimjus.2025.102541

Liu, S. (2025). Chapter 11—Case studies of big data applications for IoT. In M. A. Serhani, Y. Xu, & Z. Maamar (Eds.), *Empowering IoT with Big Data Analytics* (pp. 265–311). Academic Press. https://doi.org/10.1016/B978-0-443-21640-4.00010-7

Maher, C. A., Corsello, R. M., Engle, T. A., Kuhlman, J. D., & Nedelec, J. L. (2024). Correlates of victim services for fraud and identity theft among victim service providers. *Journal of Criminal Justice*, *95*, 102318. https://doi.org/10.1016/j.jcrimjus.2024.102318

McNealey, R. L., Figueroa, C. I., & Maher, C. A. (2025). "Police can't help you": Exploring influences on perceptions of policing *cybercrime*. *Journal of Criminal Justice*, *101*, 102542. https://doi.org/10.1016/j.jcrimjus.2025.102542

Mulahuwaish, A., Qolomany, B., Gyorick, K., Abdo, J. B., Aledhari, M., Qadir, J., Carley, K., & Al-Fuqaha, A. (2025). A survey of social cybersecurity: Techniques for attack detection, evaluations, challenges, and future prospects. *Computers in Human Behavior Reports*, *18*, 100668. https://doi.org/10.1016/j.chbr.2025.100668

Naqbi, S. A. A., Nobanee, H., & Ellili, N. O. D. (2025). Global trends and insights into cryptocurrency-related financial crime. *Research in International Business and Finance*, *75*, 102756. https://doi.org/10.1016/j.ribaf.2025.102756

Nugroho, F. A. (2025). *ADAPTIVE LEADERSHIP IN TIMES OF GLOBAL CRISIS: CASE STUDIES FROM THE COVID-19 PANDEMIC*. *Vol. 2 No. 1*. https://doi.org/10.70177/politicae.v2i1.1914

Otero, R. G., & Diaz, R. M. (2025). Crypto crime: Approaches from transnational crime and money laundering in Colombia. *The 16th International Conference on Ambient*

Systems, Networks and Technologies Networks (ANT)/ the 8th International Conference on Emerging Data and Industry 4.0 (EDI40), *257*, 1166–1171. https://doi.org/10.1016/j.procs.2025.03.155

Ozili, P. K. (2024). Forensic accounting research around the world. *Journal of Financial Reporting and Accounting*, *23*(1), 128–153. https://doi.org/10.1108/JFRA-02-2023-0106

Pardosi, P., Muttaqim, H., & Sugeng, I. S. (2024). *Social Media Activism: The Rise of Digital Movements in the Global South*. *Vol. 1 No. 6*, 411–421. https://doi.org/10.70177/politicae.v1i6.1542

Perdana, A., & Jhee Jiow, H. (2024). Crypto-Cognitive Exploitation: Integrating Cognitive, Social, and Technological perspectives on cryptocurrency fraud. *Telematics and Informatics*, *95*, 102191. https://doi.org/10.1016/j.tele.2024.102191

Qureshi, S. U., He, J., Tunio, S., Zhu, N., Nazir, A., Wajahat, A., Ullah, F., & Wadud, A. (2024). Systematic review of deep learning solutions for malware detection and forensic analysis in IoT. *Journal of King Saud University - Computer and Information Sciences*, *36*(8), 102164. https://doi.org/10.1016/j.jksuci.2024.102164

Rashid, H., Liaqat, H. B., Sana, M. U., Kiren, T., Karamti, H., & Ashraf, I. (2025). Framework for detecting phishing crimes on Twitter using selective features and machine learning. *Computers and Electrical Engineering*, *124*, 110363. https://doi.org/10.1016/j.compeleceng.2025.110363

Romero-Moreno, F. (2025). Deepfake detection in generative AI: A legal framework proposal to protect human rights. *Computer Law & Security Review*, *58*, 106162. https://doi.org/10.1016/j.clsr.2025.106162

Santiago, F. (2024). *Legal Reform of Term Limitations for Legislative Members as a Form of Institutional Reform*. https://doi.org/10.70177/politicae.v1i6.1782

Sarkar, G., & Shukla, S. K. (2024). Reconceptualizing online offenses: A framework for distinguishing *cybercrime*, cyberattacks, and cyberterrorism in the Indian legal context. *Journal of Economic Criminology*, *4*, 100063. https://doi.org/10.1016/j.jeconc.2024.100063

Sarker, I. H., Janicke, H., Mohsin, A., Gill, A., & Maglaras, L. (2024). Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects. *ICT Express*, *10*(4), 935–958. https://doi.org/10.1016/j.icte.2024.05.007

Shandilya, S. K., Singh, Y., Izonin, I., & Hentosh, L. (2024). Metaverse forensics framework: A NIST based investigation framework for metaverse. *Science & Justice*, *64*(6), 698–709. https://doi.org/10.1016/j.scijus.2024.10.005

Shih, C.-H., & Tsai, M.-L. (2024). Application of Money Flow Analysis Technology in the Investigation of Money Laundering Crimes in Taiwan. *28th International Conference on Knowledge Based and Intelligent Information and Engineering Systems (KES 2024)*, *246*, 4524–4533. https://doi.org/10.1016/j.procs.2024.09.302

Sianipar, G., Yuna, J., & Parera, D. (2025). *INTERGENERATIONAL SOLIDARITY IN POST-INDUSTRIAL SOCIETIES: SOSIOLOGICAL PERSFEKTIVES*. *Vol. 2No. 1.*, 22–34. https://doi.org/10.70177/politicae.v2i1.1899

Silva, T. J., Mazur, A. H. B., OliveiraJr, E., Zorzo, A. F., & Barcellos, M. P. (2025). An ontology for promoting controlled experimentation in *Digital Forensics*. *Forensic Science International: Digital Investigation*, *52*, 301845. https://doi.org/10.1016/j.fsidi.2024.301845

Silva, T. J., OliveiraJr, E., Pereira, M. E., & Zorzo, A. F. (2025). A review study of *Digital Forensics* in IoT: Process models, phases, architectures, and ontologies. *Forensic Science International: Digital Investigation*, *53*, 301912. https://doi.org/10.1016/j.fsidi.2025.301912

Singh, S., & Dhumane, A. (2025). Unmasking digital deceptions: An integrative review of deepfake detection, multimedia forensics, and cybersecurity challenges. *MethodsX*, *15*, 103632. https://doi.org/10.1016/j.mex.2025.103632

Soegiarto, I. (2025). *MENTAL HEALTH IMPACTS OF CLIMATE CHANGE: AN EMERGING PUBLIC HEALTH CONCERN*. *Vol. 1 No. 6*. https://doi.org/10.70177/politicae.v2i1.1753

Sunil, R., Mer, P., Diwan, A., Mahadeva, R., & Sharma, A. (2025). Exploring autonomous methods for deepfake detection: A detailed survey on techniques and evaluation. *Heliyon*, *11*(3), e42273. https://doi.org/10.1016/j.heliyon.2025.e42273

Tyagi, S., Gong, Y., & Karabiyik, U. (2025). Forensic analysis and privacy implications of LLM mobile apps: A case study of ChatGPT, Copilot, and Gemini. *Forensic Science International: Digital Investigation*, *54*, 301974. https://doi.org/10.1016/j.fsidi.2025.301974

Watson, D. L., & Jones, A. (2024). Chapter 3 Setting up a forensic laboratory. In D. L. Watson & A. Jones (Eds.), *A Blueprint for Implementing Best Practice Procedures in a Digital Forensic Laboratory (SECOND EDITION)* (pp. 29–42). Academic Press. https://doi.org/10.1016/B978-0-12-819479-9.00004-6

Whittaker, J. M., Lazarus, S., & Corcoran, T. (2024). Are fraud victims nothing more than animals? Critiquing the propagation of "pig butchering" (Sha Zhu Pan, 杀猪盘). *Journal of Economic Criminology*, *3*, 100052. https://doi.org/10.1016/j.jeconc.2024.100052

Yin, K. (2025). Dissecting the Success Factors of Telecom Fraud Deterrence: *International Journal of Digital Crime and Forensics*, *17*(1). https://doi.org/10.4018/IJDCF.391904

Zieliński, S. (2024). Evolving Threats, Emerging Laws: Poland's 2023 Answer to the Smishing Challenge. *Computer Law & Security Review*, *54*, 106013. https://doi.org/10.1016/j.clsr.2024.106013