



Rethinking Cybercrime Investigation: A Systematic Review of Digital Forensic Capacities and Cross-Jurisdictional Realities

Anorboev Amiriddin Ulugbek ugli^{1*}, Sulhani², Asmaa Assassi³, Elemegious Mugamba⁴

¹The Institute of Legislation and Legal Policy Republic of Uzbekistan-Uzbekistan,

²Universitas Tazkia-Indonesia,

³Faculty of Law and Political Science, University of Médéa-Algeria,

⁴Autonomous University of Barcelona- Barcelona, Spain

*Corresponding Author: a.anorboyev786@mail.ru

ABSTRACT

This study explores the institutional transformation of digital forensics and the cross-jurisdictional dynamics of modern cybercrime investigations using a Systematic Literature Review (SLR) design. Guided by the PRISMA 2020 framework, this paper synthesizes 34 peer-reviewed journal articles harvested from the Scopus database spanning the years 2020 to 2026. The findings comprehensively map the literature into seven core thematic areas: cloud and distributed forensics, mobile and IoT forensics, blockchain-backed evidence authentication, legal admissibility and cybercrime legislation, artificial intelligence and automated threat/evidence analysis, cybercriminalistics and cognitive mapping, and pedagogical problem-based learning. The results indicate that modern investigations require advanced computational architectures (such as automated triage, machine learning, and blockchain ledgers) to manage big digital evidence, while simultaneously confronting severe structural challenges, including technical anti-forensic techniques, opaque AI decision-making, and fragmented cross-border legal frameworks. The study concludes that strengthening digital forensic ecosystems necessitates harmonized international laws, explainable AI integration, proactive public-private collaboration, and specialized multidisciplinary education. Theoretically, this study enriches the conceptual framework of cyber governance; practically, it provides policymakers and law enforcement agencies with actionable strategies to enhance investigative efficacy and judicial reliability across diverse global jurisdictions.

ABSTRAK

Penelitian ini mengeksplorasi transformasi kelembagaan forensik digital dan dinamika lintas yurisdiksi dalam investigasi kejahatan siber modern dengan menggunakan desain *Systematic Literature Review* (SLR). Berpedoman pada kerangka PRISMA 2020, makalah ini mensintesis 34 artikel jurnal *peer-reviewed* yang dihimpun dari *database* Scopus dari tahun 2020 hingga 2026. Temuan penelitian ini memetakan literatur secara komprehensif ke dalam tujuh area tematik utama: forensik awan dan terdistribusi, forensik seluler dan IoT, autentikasi barang bukti berbasis *blockchain*, penerimaan hukum dan legislasi kejahatan siber, kecerdasan buatan (AI) serta analisis ancaman/bukti otomatis, kriminalisasi siber dan pemetaan kognitif, serta pembelajaran berbasis masalah di bidang pedagogis. Hasil penelitian menunjukkan bahwa investigasi modern memerlukan arsitektur komputasi tingkat lanjut (seperti triase otomatis, pembelajaran mesin, dan buku besar *blockchain*) untuk mengelola bukti digital berskala besar, sekaligus menghadapi tantangan struktural yang berat, termasuk teknik anti-forensik teknis, pengambilan keputusan AI yang tidak transparan (*black-box*), serta kerangka hukum lintas batas yang terfragmentasi. Studi ini menyimpulkan bahwa penguatan ekosistem

ARTICLE INFO

Article History:

Submitted/Received 3 Oct 2025

First Revised 8 Sep 2026

Accepted 14 Sep 2026

First Available online 22 Sep 2026

Publication Date 22 Sep 2026

Keyword:

Cybercrime, Digital Forensics, Forensic Expertise, Cyber Investigation, Systematic Literature Review

Kata Kunci:

Kejahatan Siber, Forensik Digital, Keahlian Forensik, Investigasi Siber, Tinjauan Literatur Sistematis



forensik digital memerlukan harmonisasi hukum internasional, integrasi AI yang dapat dijelaskan (*Explainable AI*), kolaborasi proaktif publik-swasta, serta pendidikan multidisiplin yang terspesialisasi. Secara teoretis, studi ini memperkaya kerangka konseptual tata kelola siber (*cyber governance*); secara praktis, penelitian ini memberikan strategi yang dapat ditindaklanjuti oleh pembuat kebijakan dan penegak hukum untuk meningkatkan efektivitas investigasi dan keandalan yudisial di berbagai yurisdiksi global.

INTRODUCTION

The rapid convergence of advanced information and communication technologies, particularly artificial intelligence, distributed ledgers, and distributed cloud computing systems, has substantially altered patterns of transnational criminal conduct (Bhagat et al., 2026). These technologies provide significant economic value, but they also offer malicious actors powerful instruments to execute coordinated, anonymous, and technically resilient offenses across international borders (Prasad et al., 2025). Cybercrimes have developed from simple, opportunistic acts into organized computational operations, including sophisticated ransomware syndicates, large-scale financial fraud, and covert operations across dark web environments (Prasetyo et al., 2024; Broadhurst et al., 2014). Consequently, law enforcement authorities and judicial institutions encounter severe operational bottlenecks. Conventional investigative procedures cannot adequately locate, secure, and verify electronic evidence that is volatile, geographically dispersed, and subject to distinct legal boundaries (Casey, 2019). This operational reality demands a fundamental transition in which digital forensic practice serves as an essential foundation of the contemporary criminal justice system.

At the conceptual level, cybercrime investigation and forensic expertise operate within an interdependent relationship governed by scientific principles and procedural jurisprudence. Cybercrime involves illicit actions where information systems serve as the target, instrument, or medium of criminal conduct (Ho & Luong, 2022; Ho et al., 2024). Forensic expertise, on the other hand, represents the systematic application of specialized technical knowledge to identify, isolate, extract, and interpret electronic traces into legally admissible facts (Morey et al., 2026). However, traditional forensic methodologies are increasingly strained by the volume, velocity, and architectural complexity of contemporary digital records. Standard post-mortem disk acquisition and manual analysis can no longer address the extreme scale of big digital evidence and advanced cryptographic protection (Lusetti et al., 2020; Dweib & Abu-amara, 2026). Because digital evidence can be easily manipulated or erased, investigative procedures must rigorously maintain an unbroken chain of custody while satisfying demanding statutory standards of judicial admissibility, including the Daubert threshold and international guidelines established under ISO/IEC 27037 (Nath et al., 2024; Ndubuisi, 2023).

To respond to these systemic problems, governments worldwide have begun modernizing their institutional forensic capacities through distinct statutory and operational mechanisms. Advanced legal systems, including those in North America and Western Europe, have committed significant public resources toward automated forensic triage platforms, algorithmic parsing of application artifacts, and statutory mechanisms for cross-border data transfer, such as the United States CLOUD Act and European Union digital evidence directives (Khan et al., 2024; Track, 2025). At the same time, emerging and transitional economies in regions such as Central Asia, Eastern Europe, Latin America, and Southeast Asia are undertaking structural judicial reforms. These initiatives include enacting comprehensive procedural rules for seizing digital assets, introducing technical standards for tracking



crypto-wallet transactions, and establishing dedicated national training bodies to resolve persistent shortages of qualified digital investigators (Valjarevic, 2012; Lusetti et al., 2020).

Despite these widespread global initiatives, academic scholarship in this field remains structurally fragmented across technological, procedural, and jurisdictional lines. Although machine learning models and automated classification tools can accelerate pattern detection across complex evidence sets, these systems often function without transparent decision pathways, which complicates judicial validation, auditability, and expert testimony during trial cross-examination (Hermosilla et al., 2025; Datta et al., 2026). Furthermore, a pronounced gap persists between rapidly evolving technical capabilities and relatively static statutory provisions. While emerging frameworks using distributed ledgers can securely preserve evidence logs, their practical interoperability across jurisdictions with distinct evidentiary standards remains largely untested (Prakash & Sadawarti, 2022; Abu-alhaija, 2020; Hanif, 2025). Compounding these challenges, existing scholarly inquiries are predominantly bifurcated between evaluations of advanced computational methods in well-funded Western jurisdictions and isolated, descriptive case analyses from individual developing nations that lack comparative integration within a broader global framework (Valjarevic, 2012; Casey, 2019).

As a result, contemporary scholarship lacks a consolidated, evidence-based assessment of how digitalized forensic practices influence investigative speed, data integrity, and courtroom admissibility across institutions with differing levels of technical and legal maturity. This fragmentation limits the formulation of cohesive policies, operational benchmarks, and practical standards for cross-border judicial cooperation. To address this knowledge gap, this study conducts a Systematic Literature Review using the guidelines established by Kitchenham & Charters (2007) and the PRISMA framework (Page et al., 2021) with two primary objectives: first, to systematically synthesize the core thematic landscape of modern digital forensics and cybercrime investigation; and second, to formulate strategic policy and research directions for enhancing institutional capacity, cross-jurisdictional cooperation, and judicial reliability. This analysis constructs an integrated conceptual foundation through an exhaustive assessment of empirical and doctrinal studies across global jurisdictions; this review investigates the dominant technical architectures driving forensic transformation, evaluates the procedural and evidentiary barriers encountered in judicial proceedings, and analyzes the structural variations in institutional capacity between developed and developing legal frameworks. This analysis constructs an integrated conceptual foundation to guide policymakers, legal authorities, and forensic practitioners working to enhance the efficacy of modern cybercrime investigations.

LITERATURE REVIEW

Cybercrime Dynamics and the Imperative of Digital Forensic Expertise

Cybercrime constitutes unlawful activity wherein computing infrastructure, algorithmic architectures, or digital communication networks serve as the primary instrument, target, or operating environment of an offense (Chen et al., 2023; Rakha, 2023). Unlike conventional territorial offenses, modern cybercrimes frequently exploit decentralized protocols, multi-layered anonymization networks, and distributed hosting systems to conceal perpetrator identities and fragment evidentiary trails across multiple sovereign territories (Broadhurst et al., 2014). Contemporary cyber threats have evolved into professionalized computational operations, including distributed ransomware operations, algorithmic financial manipulation, and automated credential exploitation (Baftiu et al., 2026; Abdullah et al., 2025). The geographic dispersion and extreme volatility of digital traces pose severe operational dilemmas for statutory criminal justice systems. Successfully identifying and prosecuting malicious



actors requires moving beyond localized investigative policing toward structured, scientifically validated investigative methodologies capable of identifying, preserving, and reconstructing electronic evidence across heterogeneous environments (Casey, 2019).

Within this operational reality, forensic expertise serves as an institutional and procedural mechanism designed to evaluate scientific facts for judicial scrutiny. Digital forensics specifically governs the identification, acquisition, recovery, analysis, and formal presentation of electronic data to establish objective facts that satisfy strict legal standards of courtroom admissibility (Yeboah-Ofori & Brown, 2020; Ismail et al., 2025). Because digital traces are easily overwritten, intentionally altered, or compromised during extraction, forensic practitioners must anchor each stage of inquiry to established legal doctrines and international technical benchmarks, such as the Daubert admissibility framework and ISO/IEC 27037 standards (Baier et al., 2024). Forensic expertise therefore functions as the indispensable evidentiary bridge that translates complex, volatile computational artifacts into verifiable and legally robust evidence capable of sustaining statutory burdens of proof.

Digital Forensic Modernization and Cross-Jurisdictional Realities

The transformation of forensic capacity increasingly depends on adopting advanced computational architectures to manage the velocity, volume, and cryptographic complexity of modern evidence. Contemporary forensic workflows frequently incorporate automated triage systems, machine learning-driven artifact parsing, and unified evidentiary databases to mitigate the acute pressures of the forensic data deluge (Wu & Du, 2026; Salih & Ibrahim, 2023). In technologically advanced jurisdictions across North America and Western Europe, substantive capital has been directed toward centralized digital evidence repositories, cloud-native investigative architectures, and bilateral frameworks designed to streamline extraterritorial evidence requests, such as the United States CLOUD Act and European cross-border digital evidence directives (Marandici et. al., 2022; Hossain, 2023). At the same time, emerging and transitional economies across Central Asia, Eastern Europe, Latin America, and Southeast Asia are undertaking targeted judicial and procedural reforms. These initiatives include updating criminal procedural rules to formalize electronic evidence seizure, standardizing analytical methods for tracking distributed crypto-wallet transactions, and establishing dedicated national training facilities to mitigate severe shortages of forensic investigators.

Despite widespread institutional investment, the development of forensic capacity reveals profound structural fractures across technological, legal, and regional lines. At the technical level, investigators are persistently challenged by sophisticated anti-forensic techniques, zero-access encryption protocols, and non-linear data distributions across multi-tenant cloud architectures (Casey, 2019). Furthermore, while automated tools and artificial intelligence models accelerate pattern recognition, their internal decision-making processes often lack algorithmic explainability, raising acute evidentiary questions regarding auditability, methodological validation, and judicial credibility during adversarial courtroom proceedings (Mugamba, 2026). These technical vulnerabilities are magnified by stark cross-jurisdictional asymmetries. Divergent statutory definitions of digital privacy, conflicting warrant requirements for extraterritorial data retrieval, and prolonged diplomatic channels create friction that frequently derails cross-border prosecutions (Baftiu et al., 2026; Shahid et al., 2023). These procedural obstacles are exacerbated by an unequal global distribution of forensic expertise, leaving transitional and developing jurisdictions structurally disadvantaged against advanced cyber adversaries (Dunsin et al., 2024). While past scholarly literature has examined individual technical extraction tools (Baftiu et al., 2026; Ho et al., 2024), procedural doctrines (Shevchuk et al., 2025), or investigator training needs (Krupa et al., 2026) in isolation, there remains an acute lack of an integrated, evidence-



based synthesis that evaluates how institutional capacities and cross-jurisdictional realities jointly dictate the efficacy of modern cybercrime investigations.

RESEARCH METHODOLOGY

This study employs a Systematic Literature Review design to evaluate the institutional transformation of digital forensics and the cross-jurisdictional dynamics of modern cybercrime investigation. The review framework strictly observes the methodological procedures established by Kitchenham & Charters (2007) alongside the Preferred Reporting Items for Systematic Reviews and Meta-Analyses statement (Page et al., 2021). Applying these standardized procedural controls guarantees an auditable, transparent, and replicable selection sequence while substantially reducing subjective researcher bias.

Primary bibliographic records were harvested from the Scopus database, selected for its comprehensive indexing of peer-reviewed journals across social sciences, management, and technical disciplines. The retrieval strategy integrated Boolean logic applied across document titles, abstracts, and author keywords using the following parameters: ("cybercrime" OR "cyber-crime") AND ("investigat") AND ("digital forensic*" OR "forensic expertise"). This baseline automated query yielded an unrefined total of 527 publications. To align the review with organizational, managerial, and institutional perspectives, an initial subject area filter was applied targeting business, management, accounting, and social science domains. Because specialized literature addressing digital forensics and investigative capacities is predominantly indexed under the broader social sciences category rather than isolated commercial domains, the resulting 178 records were successfully consolidated within the social science classification. Limiting the document type strictly to peer-reviewed journal articles, thereby excluding book chapters, conference proceedings, notes, and industry editorials, further reduced the dataset to 51 articles. Language screening subsequently removed two non-English publications, leaving 49 candidate articles for full-text retrieval and eligibility appraisal.

During the full-text evaluation phase, 15 publications were eliminated from the final synthesis based on accessibility and thematic screening. Eleven articles could not be retrieved due to permanent institutional repository restrictions and full-text access barriers. The remaining documents were subjected to substantive eligibility assessment, leading to the exclusion of three articles whose thematic focus diverged from the investigative scope of the study, specifically concerning peripheral internal corporate compliance without addressing criminal procedural mechanics or digital forensic workflows. Following these exclusions, exactly 34 peer-reviewed journal articles satisfied all procedural criteria and constituted the final analytic corpus for qualitative thematic synthesis (Braun & Clarke, 2006).

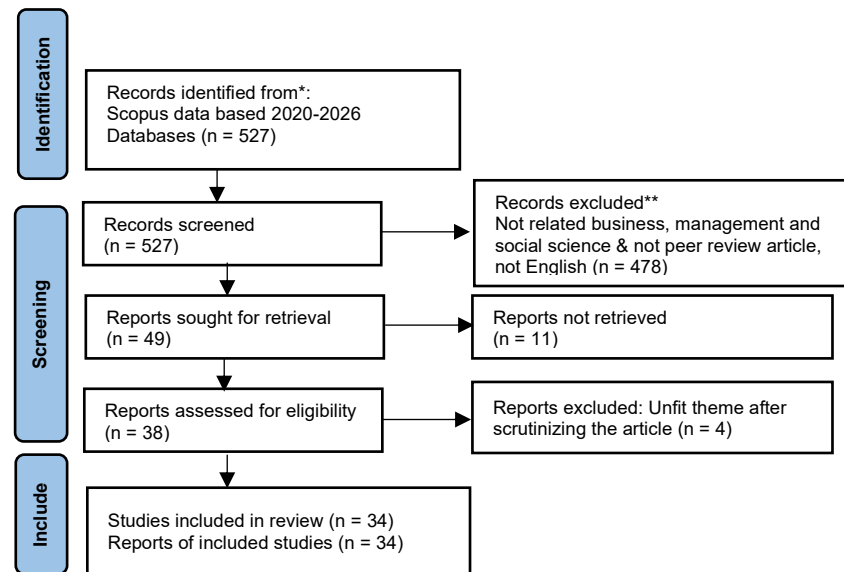


Figure 1: PRISMA Diagram

RESULT AND DISCUSSION

The reviewed corpus comprises thirty-four scholarly publications spanning 2020 to 2026, reflecting an active timeline of recent research. Specifically, the temporal distribution includes four papers published in 2020; Oh et al., (2020), Tok et al. (2020), Khanuja & Adane (2020), and Schreuders et al. (2020), four papers in 2021; Hegarty & Taylor (2021), Prayudi et al. (2021), and Cabrero-holgueras & Pastrana, (2021) and Zhang et al. (2021), four papers in 2022; Gruber et al. (2022), James (2022), Padalka & Doctus (2022) and Singh et al. (2022). Furthermore, the collection incorporates eight papers published in 2023; Ngo & Le-khac (2023), Nasreen & Mir (2023), Kazaure et al. (2023), Khan et al. (2023), Kim et al. (2023), Rakha (2023), Kumar et al. (2023) and Tok & Chattopadhyay (2023), five papers in 2024; Saniyazova et al. (2024), Dunsin et al. (2024), Baier et al. (2024), Moreb et al. (2024), and Venkatesh et al. (2024), four papers in 2025; Shevchuk et al. (2025), Slimi & Chichti, (2025), Stone & Vaidyan (2025), Tok et al. (2025), and five papers in 2026; Apsimet et al. (2026) Fisher et al., (2026), Heitmann & Johnsen (2026), Nujumudeen et al. (2026) and Tippe et al. (2026). These studies are hosted in esteemed peer-reviewed venues such as Forensic Science International: Digital Investigation, Computers & Security, IEEE Access, International Journal of Electronic Security and Digital Forensics, and various international law and management journals such as Mexican Law Review, The Law, State and Telecommunications Review and Global Journal of Flexible Systems Management.

Geographically, the research contexts encompass diverse country settings including India, Kazakhstan, Germany, South Korea, the United Kingdom, the United States, Malaysia, Nigeria, Pakistan, Ireland, Palestine, Ukraine, Indonesia, Uzbekistan, Tunisia, and Singapore. The corresponding industry and operational settings span law enforcement and national security agencies, cloud and fog computing infrastructures, financial institutions and banking sectors, higher education and academic institutions, smart city and IoT ecosystems, and transnational migration and underground cybercrime networks.



Methodologically and theoretically, the research areas represented in this collection are multifaceted, addressing cloud and distributed forensics, mobile and IoT app forensics, blockchain-backed evidence authentication, legal admissibility and cybercrime legislation, artificial intelligence and automated threat/evidence analysis, cybercriminalistics and cognitive mapping, smart city threat modeling, and pedagogical problem-based learning. Across these domains, authors draw upon foundational and specialized theories such as containment and social bonding theories, the criminalistic cycle and cybercrime execution stacks, Dempster-Shafer theory, routine activity theory, the Integrated Cyber Investigation Process (ICIP) framework, design science research methodology, and organizational elements models.

To address these complex security and investigative challenges, the studies employ a diverse spectrum of research methods and analytical techniques. Qualitative investigations including doctrinal legal analysis, abductive thematic frameworks, and expert interviews are utilized to evaluate procedural gaps and regulatory policies. Quantitative and econometric methodologies, such as multiple linear regressions, ANOVA, and variance inflation factor (VIF) analyses, are implemented to model macroeconomic correlations between cybercrime and irregular migration. Computational and experimental approaches leverage machine learning classification, neural networks, secure vectorization, and similarity/fuzzy hashing variants like FbHash-E, alongside design science.

Synthesizing the Core Thematic Landscape of Digital Forensics and Cybercrime Investigation

The landscape of digital forensics and cybercrime investigation has experienced a profound evolution, driven by the rapid expansion of digital technologies, interconnected architectures, and emerging threat vectors. To synthesize the contributions of the thirty-four reviewed papers, the literature can be effectively classified into seven core thematic categories. As organizational data migrates to elastic and decentralized environments, traditional forensic models have proven insufficient. Researchers have addressed the complexities of cloud and distributed architectures by developing advanced security and investigation frameworks. For instance, Nasreen & Mir (2023) introduced the Distributed Key Cipher Policy Elliptic Curve Cryptography (DK-CP-ECC) algorithm combined with an Adaptive Neuro-Fuzzy Inference System to secure cloud forensic investigations. Similarly, Hegarty & Taylor (2021) formulated a specialized forensic framework tailored to fog computing environments, bridging the gap between cloud infrastructure and edge sensor networks. Complementing these technical models, Khan et al. (2023) and Kumar et al. (2023) explored the broader paradigms of cloud forensics, addressing issues of multi-tenancy, service level agreements (SLAs), and distributed data acquisition.

Simultaneously, the proliferation of smart devices and mobile platforms has expanded the boundaries of digital evidence. Moreb et al. (2024) designed a comprehensive Mobile Forensics Investigation Process Framework (MFIPF) to standardize evidence handling across Android and iOS ecosystems. In the realm of the Internet of Things (IoT), Kim et al. (2023) developed a service-interconnectivity-based framework (SIUFF) to uncover hidden associations and data sharing among smart devices. Furthermore, Tok et al. (2025) established foundational evidence classification and correlation tools, such as the STITCHER framework, to help investigators navigate the heterogeneity of IoT environments. Zhang et al. (2021) reinforced this domain by employing a design science approach to create a rigorous forensic framework for Android mobile applications.

To secure the chain of custody and ensure the non-repudiation of digital evidence, recent scholarship has increasingly turned to distributed ledger technology. Nujumudeen et al. (2026) proposed an adaptive blockchain framework utilizing a lightweight Proof-of-Authority (PoA) consensus



mechanism and dynamic cryptography to authenticate forensic evidence in resource-constrained environments. By anchoring cryptographic hashes on-chain while storing bulky evidence off-chain, these blockchain-enabled paradigms protect investigative logs from tampering and satisfy stringent legal admissibility standards across multiple jurisdictions.

However, the technical dimensions of digital forensics are inextricably linked to legal and procedural standards. Apsimet et al. (2026) analyzed the challenges of admitting digital evidence in pretrial fraud investigations, drawing lessons for legal systems such as Kazakhstan from international practice. Rakha (2023) explored the broader legal bottlenecks and the acute lack of standardization hindering evidence admissibility in court, while Saniyazova et al. examined the emergence of digital forensics within the Kazakh legal environment. Padalka & Doctus (2022) contributed an institutional perspective from Ukraine, detailing the critical role of state-accredited forensic technical support in countering national cyber threats.

Facing massive volumes of digital data, manual examination is no longer viable, prompting the integration of artificial intelligence (AI) and machine learning (ML). Dunsin et al. (2024) provided a comprehensive systematic review detailing the transformative role of AI and ML across the digital forensics and incident response lifecycle. In specialized analytical domains, Khanuja & Adane, (2020) introduced a database forensics model utilizing the Dempster-Shafer theory of evidence to detect illegal financial transactions and money laundering patterns. Furthermore, Singh et al. (2022) improved similarity hashing through an efficient Bloom-filter-based version of FbHash (FbHash-E) to rapidly filter cybercrime artifacts, while Stone & Vaidyan (2025) investigated the reliability, transparency, and confidence levels associated with AI-generated forensic evidence.

Understanding the operational tactics of cybercriminals also requires structured investigative reasoning and threat modeling. Gruber et al. (2022) introduced the concept of cognitive maps to bridge the gap between abstract process models and concrete botnet investigations. Cabrero-holgueras & Pastrana (2021) developed a scalable methodology using multi-feature similarity (MultFS) metrics to identify related accounts across underground hacking forums. To address smart city security, Tok & Chattopadhyay (2023) formulated a standardized definition of Smart City Infrastructure (SCI) and integrated STRIDE threat modeling to identify vulnerabilities, crimes, and evidence requirements, a work expanded through the Smart City Ontological Paradigm Expression (SCOPE) by Tok et al. (2025). Additionally, Heitmann & Johnsen (2026) analyzed the landmark LockerGoga ransomware attack on Norsk Hydro through the Integrated Cyber Investigation Process (ICIP) framework, Slimi & Chichti (2025) explored the macroeconomic intersection of cybercrime and irregular migration, and Tippe et al. engineered containerized simulation scenarios for investigating Tor Onion Services.

Finally, bridging the skills gap in cybersecurity requires innovative educational frameworks. Fisher et al. (2026) emphasized the importance of early engagement by introducing high school students to open-source forensic tools like Autopsy and Sleuth Kit. Schreuders, et al. (2020) conducted a large-scale needs assessment within a UK police force to evaluate training, communication, and resource gaps across the cyber-investigation lifecycle. Lastly, Venkatesh et al., (2024) presented problem-based learning (PBL) strategies utilizing the DIGIT framework to align engineering education with real-world digital forensics investigations, while Kazaure et al. (2023) provided a comprehensive review of forensic investigation approaches and training requirements to mitigate persistent cybercrimes.

Strategic Policy and Research Directions for Future Cyber Forensics

Based on the comprehensive synthesis of the thirty-four reviewed papers across the seven core thematic areas, the future landscape of digital forensics and cybercrime investigation demands a



paradigm shift. As technology evolves, ranging from distributed cloud-fog ecosystems and automated artificial intelligence to quantum threats and smart city infrastructures, traditional reactive investigative methods are increasingly inadequate. To bridge the gap between technical innovation, evidentiary reliability, and legal frameworks, future research and policy directions must focus on the following key areas:

Governments and international bodies must establish unified, cross-jurisdictional standards for digital evidence collection, preservation, and admissibility. As demonstrated by legal studies, divergent national laws and the absence of standardized protocols severely impede the prosecution of transnational cybercrime. Policymakers should champion international treaties (such as expanding the reach and adoption of the Budapest Convention) and mandate standardized metadata formats (such as UCO/CASE and ISO/IEC 27037/27043) to ensure evidence is legally defensible across borders. To support this, future technical research should focus on developing open-source, vendor-neutral middleware and interoperable case management schemas (similar to the Ontological Knowledge Map or SCOPE framework) that seamlessly ingest disparate artifacts from cloud, fog, and mobile platforms without losing evidentiary provenance or violating data privacy regulations like the GDPR (Ngo & Le-khac, 2023; Tok & Chattopadhyay, 2023).

Legal systems must also update their rules of evidence and criminal procedures to accommodate AI-driven forensic findings. Because courts require transparency and interpretability, regulatory bodies should formulate guidelines that govern the use of machine learning in investigations. These policies must mandate that any AI tool utilized for pattern recognition, evidence triage, or threat attribution provide explainable outputs to satisfy the Daubert standard or equivalent judicial reliability thresholds. In parallel, researchers must prioritize the development of Explainable AI (XAI) models within digital forensics. Future work should move away from opaque black-box machine learning algorithms and focus on robust, interpretable verification models, combined with automated confidence metrics, to quantify the accuracy and validity of AI-generated digital evidence.

Furthermore, law enforcement agencies and private sector enterprises must shift from a reactive posture to a proactive collaborative model. Policymakers should incentivize or mandate cross-organizational investigative readiness, establishing pre-incident agreements, secure communication channels, and pre-defined information-sharing protocols (such as harmonized translation layers between TLP and law enforcement handling codes) between CSIRTs, private incident responders, and police units. To facilitate this, research should explore real-time, secure information-sharing architectures such as privacy-preserving blockchain ledgers for chain-of-custody tracking that allow private corporations to share telemetry and threat intelligence with law enforcement instantaneously without compromising commercial confidentiality or user privacy rights.

Legal frameworks must also address the reality of modern criminal infrastructure such as Tor Onion Services, encrypted darknet markets, and distributed botnets where traditional physical imaging is impossible. Legislators need to provide clear, regulated legal pathways for authorized remote active engagement and Network Investigative Techniques (NITs) that balance effective law enforcement oversight with strict constitutional privacy safeguards. Correspondingly, academic and technical research must expand beyond static file analysis to investigate active, hypothesis-driven forensic methodologies. This includes building standardized, containerized simulation environments (like DarkMarket) for training practitioners in live network tracing, as well as developing forensically sound, immutable logging tools for active remote acquisition (Tippe et al., 2026).



Finally, educational institutions and law enforcement academies must overhaul their curricula to combat the persistent global cybersecurity skills gap and technical illiteracy across the justice system. Policymakers should fund specialized degree tracks in cybercriminalistics and mandate continuous professional development and certification for investigators, prosecutors, and judges. To achieve this, future pedagogical research must evaluate and scale active learning methodologies such as Problem-Based Learning (PBL) and experiential frameworks (the DIGIT framework or live simulation testbeds) to ensure that future professionals possess both deep technical proficiency and rigorous legal fluency. Longitudinal studies are ultimately needed to track how practical, interdisciplinary training impacts career readiness and successful courtroom prosecutions.

CONCLUSION

The landscape of modern cybercrime investigation has undergone a fundamental paradigm shift, wherein the digitalization of forensic expertise is no longer merely a complementary instrument but a core pillar of global cybersecurity governance. Based on a comprehensive synthesis of 34 selected articles spanning 2020 to 2026, current literature is effectively classified into seven primary thematic pillars ranging from cloud and fog computing, mobile and IoT forensics, and blockchain-based authentication to artificial intelligence integration and pedagogical frameworks. The findings indicate that while the adoption of cutting-edge technologies, such as machine learning and distributed ledger systems, drastically accelerates big data reduction and safeguards the integrity of the chain of custody, investigative efforts continue to be hampered by severe structural hurdles. These include advanced anti-forensic techniques, opaque AI decision-making models (the black-box problem), and inconsistent legal admissibility standards across diverse cross-border jurisdictions.

Nevertheless, this study acknowledges several limitations that should be addressed in future research. First, constraining the bibliographic search primarily to the Scopus database with specific language criteria may have excluded valuable insights from alternative repositories and grey literature published by international law enforcement agencies. Second, relying on a systematic literature review design emphasizes secondary and theoretical synthesis, lacking direct empirical validation of digital forensic tools within active operational environments. Third, the macro-level synthesis does not fully capture the nuanced micro-level institutional and infrastructural constraints unique to developing or transitional economies.

In response to these challenges and limitations, strengthening the digital forensic ecosystem moving forward requires synchronized and strategic interventions. Governments and international bodies are urged to advance cross-jurisdictional legal harmonization through expanded adoption of frameworks like the Budapest Convention and update judicial evidentiary standards to accommodate transparent, scientifically verifiable AI-driven findings (Explainable AI). Operationally, law enforcement agencies and private sector enterprises must transition from a reactive stance to a collaborative proactive model of investigative readiness, supported by secure, real-time threat intelligence sharing architectures. Finally, academic institutions and law enforcement academies must overhaul their educational curricula by integrating active problem-based learning and simulated virtual testbeds to bridge the persistent global cybersecurity skills gap, ensuring that future investigations seamlessly balance technological innovation with rigorous legal accountability.



REFERENCES

- Abdullah, M., Nawaz, M. M., Saleem, B., Zahra, M., Ashfaq, E., & Muhammad, Z. (2025). Evolution Cybercrime Key Trends , Cybersecurity Threats , and Mitigation Strategies from Historical Data. *Analytics*, 25(4), 1–44.
- Abu-alhaija, M. (2020). Cyber security: between challenges and prospects. *ICIC International*, 11(11), 1019–1028. <https://doi.org/10.24507/icicelb.11.11.1019>
- Apsimet, N. Y. A. B. K. A. Z. A. M. (2026). Challenges of using digital evidence in pretrial investigations of online fraud : lessons for Kazakhstan from international practice. *IDP Revista de Internet Derecho y Política*, 44(44).
- Baftiu, N., Sofiu, E., Pachemska, T., & Atanasova, A. (2026). A Technical Analysis of Modern Ransomware Operations and Defense Mechanisms. *SAR Journal*, 9(1), 67–74. <https://doi.org/10.18421/SAR91>
- Baier, D., Basse, A., Hilgert, J., & Lambertz, M. (2024). Forensic Science International : Digital Investigation TLS key material identification and extraction in memory: Current state and future challenges. *Forensic Science International: Digital Investigation*, 49(S), 301766. <https://doi.org/10.1016/j.fsidi.2024.301766>
- Bhagat, H. V., Kaur, P., Kaur, A., Kriti & Singh, M., J. (2026). *Artificial Intelligence in Cybersecurity and Risk Management*. Deep Science Publishing. <https://doi.org/10.70593/978-93-7185-561->
- Braun, V., Clarke, V., Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101.
- Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and Cyber crime : An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*, 8(1), 1–20.
- Cabrero-holgueras, J., & Pastrana, S. (2021). TC 11 Briefing Papers A Methodology For Large-Scale Identification of Related Accounts in Underground Forums. *Computers & Security*, 111. <https://doi.org/10.1016/j.cose.2021.102489>
- Casey, E. (2019). The chequered past and risky future of digital forensics The chequered past and risky future of digital forensics. *Australian Journal of Forensic Sciences*, 00(00), 1–16. <https://doi.org/10.1080/00450618.2019.1554090>
- Chen, S., Hao, M., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*. <https://doi.org/10.1057/s41599-023-01560-x>
- Crime, U. N. O. on D. and. (2024). *Transnational Organized Crime in the Pacific : Expansion , Challenges and Impact October 2024*. October.
- Datta, S., Chakraborty, R., Bhattacharjee, R., & Kumar, A. (2026). Review article A review of artificial intelligence in materials screening: Data , models , and applications in forensic science. *Next Materials*, 13(July), 102756. <https://doi.org/10.1016/j.nxmte.2026.102756>
- Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). Forensic Science International : Digital Investigation 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(January), 301675. <https://doi.org/10.1016/j.fsidi.2023.301675>
- Dweib, A., & Abu-amara, F. (2026). Toward Secure and Scalable Digital Evidence Preservation : A Blockchain-Driven Framework. *Blockchains*, 1–21.
- Fisher, T., Weber, C., Burruss, G., & Fisk, N. (2026). Digital Detectives in the Making : Introducing



- Data Security Through Forensic Challenges Digital Detectives in the Making: Introducing Data. *Journal of Criminal Justice Education*, 37(2), 275–293. <https://doi.org/10.1080/10511253.2026.2625781>
- Gruber, J., Voigt, L. L., Benenson, Z., & Freiling, F. C. (2022). Forensic Science International : Digital Investigation Foundations of cybercriminalistics: From general process models to case-specific concretizations in cybercrime investigations. *Forensic Science International: Digital Investigation*, 43, 301438. <https://doi.org/10.1016/j.fsidi.2022.301438>
- Hanif, N. (2025). Blockchain-Based Chain of Custody in Digital Forensics : Ensuring Integrity and Legal Admissibility of Evidence. *FORSEC: Forensic and Security Journal*, 1(1), 34–41.
- Hegarty, R., & Taylor, M. (2021). Digital evidence in fog computing systems. *Computer Law & Security Review*, 41, 105576. <https://doi.org/10.1016/j.clsr.2021.105576>
- Heitmann, O., & Johnsen, J. W. (2026). Cybercrime investigations in practice: Insights from the LockerGoga ransomware attack on Norsk Hydro. *Forensic Science International: Digital Investigation*, 49, 1–10. <https://doi.org/10.1016/j.fsidi.2026.302111>
- Hermosilla, P., & Berríos, S. H. A.-C. (2025). Explainable AI for Forensic Analysis : A Comparative Study of SHAP and LIME in Intrusion Detection Models. *Applied Science*, 15, 1–29.
- Ho, H., Gilmour, J., Mazerolle, L., & Ko, R. (2024). Utilizing cyberplace managers to prevent and control cybercrimes: a vignette experimental study. *Security Journal*, 37(1), 129–152. <https://doi.org/10.1057/s41284-023-00371-8>
- Ho, H. T. N., & Luong, H. T. (2022). Research trends in cybercrime victimization during 2010–2020: A bibliometric analysis. *SN Social Sciences*, 2(1), Artikel 4. Springer International Publishing. <https://doi.org/10.1007/s43545-021-00305-4>
- Hossain, B. (2023). Digital Evidence in Foreign Jurisdiction and Quality of. *ELCOP Journal on Human Rights*, 1(October), 143–159.
- Ismail, I., Akram, K., & Ariffin, Z. (2025). The admissibility of digital evidence from open-source forensic tools : Development. *PLoS ONE*, 20(9), 1–26. <https://doi.org/10.1371/journal.pone.0331683>
- James, J. E. (2022). High tech cybercrime unit : A partnership between a local county and a university. *Issues in Information Systems*, 23(4), 46–55.
- K. Venkatesh; R. Rajasubramanian; T. Manikumar; Mohideen, A. B. (2024). Unravelling Digital Crime Scenes : Pedagogical Strategies in Digital Forensics. *Journal of Engineering Education Transformations*, 38, 146–152.
- Kazaure, A. A. (2023). Digital Forensics Investigation Approaches in Mitigating Cybercrimes : A Review. *Journal of Information Science Theory and Practice*, 11(4), 14–39.
- Khan, S. H., Zakir, M. H., Tayyab, A., & Ibrahim, S. (2024). The Role of International Law in Addressing Transnational Organized Crime. *Journal of Asian Development Studies*, 13(1), 283–294.
- Khan, A. A., Shaikh, A. A., Laghari, A. A., & Rind, M. M. (2023). Cloud forensics and digital ledger investigation: A new era of forensics investigation. *International Journal of Electronic Security and Digital Forensics*, 15(1), 1–19. <https://doi.org/10.1504/IJESDF.2023.127745>
- Khanuja, H., & Adane, D. (2020). Monitor and detect suspicious transactions with database forensics and Dempster-Shafer theory of evidence. *International Journal of Electronic Security and Digital Forensics*, 12(2), 154–173. <https://doi.org/10.1504/IJESDF.2020.106302>
- Kim, J., Park, J., & Lee, S. (2023). Forensic Science International : Digital Investigation An improved



- IoT forensic model to identify interconnectivity between things. *Forensic Science International: Digital Investigation*, 44, 301499. <https://doi.org/10.1016/j.fsidi.2022.301499>
- Kitchenham, B. and Charters, S. (2007). *Guidelines for Performing Systematic Literature Reviews in Software Engineering, Technical Report EBSE 2007-001*.
- Krupa, J. M., Holt, T. J., Fisher, T., Mcnealey, R. L., Holt, K., Holt, T. J., Fisher, T., Mcnealey, R. L., & Holt, K. (2026). Cybercrime and Cyber Investigations : Development of a Training Curriculum for Law Enforcement Personnel Cybercrime and Cyber Investigations : Development of a. *Journal of Criminal Justice Education*, 37(2), 232–255. <https://doi.org/10.1080/10511253.2025.2596018>
- Kumar, R., Kakade, K. S., Priscilla, M., & Krishna, B. V. S. (2023). An effective digital forensic paradigm for cloud computing criminal investigation. *Int. J. Electronic Security and Digital Forensics*, 15(6), 655–664.
- Lusetti, M., Salsi, L., & Dallatana, A. (2020). Forensic Science International : Digital Investigation A blockchain based solution for the custody of digital fi les in forensic medicine. *Forensic Science International: Digital Investigation*, 35, 301017. <https://doi.org/10.1016/j.fsidi.2020.301017>
- Marandici, O., & Iordan, C. (2022). Transnational Gathering Of Electronic Evidences : Challenges And Perspectives In The European Union Și Perspective În Uniunea. *Revista I Nstitutului N Ațional Al J Ustiției*, 3(6 2), 54–60.
- Moreb, M., Salah, S., & Amro, B. (2024). A Novel Framework for Mobile Forensics Investigation Process. *International Journalof Computing and Digital Systems*, 135(1), 125–135.
- Morey, K. B., Thakare, V. J., Pawade, V. S., & Mahajan, V. B. (2026). File System Forensics : A Comparative Analysis across Operating Systems. *International Journal of Scientific Research in Science and Technology*.
- Mugamba, E. (2026). Digital Due Process in the Age of Algorithms : Redesigning Fairness in Criminal Justice Decision Systems in Uganda. *International Journal of Law: "Law and World*, 12(1), 75–80.
- Nasreen, S., & Mir, A. H. (2023). Enhancing Cloud Forensic Investigation System in Distributed Cloud Computing Using DK-CP-ECC Algorithm and EK-ANFIS. *Journal of Mobile Multimedia*, 19, 679–706. <https://doi.org/10.13052/jmm1550-4646.1933>
- Nath, S. K. S. B. G.-J. A. (2024). Digital Evidence Chain of Custody : Navigating New Realities of Digital Forensics. *IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications*, 11–20. <https://doi.org/10.1109/TPS-ISA62245.2024.00012>
- Ndubuisi, A. F. (2023). The impact of international cybersecurity treaties on domestic cybercrime control and national critical infrastructure protection. *World Journal of Advanced Research and Reviews*, 20(03), 2285–2304.
- Ngo, H. Q., & Le-khac, N. (2023). Forensic Science International : Digital Investigation Ontology-based case study management towards bridging training and actual investigation gaps in digital forensics. *Forensic Science International: Digital Investigation*, 47(September), 301621. <https://doi.org/10.1016/j.fsidi.2023.301621>
- Nujumudeen, F., Mubarak, D. M. N., & Hussain, T. (2026). Adaptive blockchain framework for reliable authentication and preservation of digital forensic evidence. *Discover Computing*, 29.
- Oh, D. Bin, Park, K. H., & Kim, H. K. (2020). De-Wipimization: Detection of data wiping traces for investigating NTFS file system. *Computers & Security*, 99, 102034. <https://doi.org/10.1016/j.cose.2020.102034>
- Padalka, A., & Doctus, M. (2022). Forensic and technical criminalistics support in cybercrime



- investigation: countering cyber threats in Ukraine. *Colombian Journal of Military and Strategic Studies*, 20(38).
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-wilson, E., McDonald, S., Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews Systematic reviews and Meta-Analyses. *CCBY Open Access Research Methods & Reporting*. <https://doi.org/10.1136/bmj.n71>
- Prakash, F., & Sadawarti, H. (2022). Blockchain-Based Chain Of Custody : A Secure Digital Evidence Framework For Digital Forensics Investigation. *Applied Innovative Research*, 3(1), 108–112.
- Prasad, N. A. D. W. F. (2025). Computers & Security A survey of cyber threat attribution : Challenges , techniques , and future directions. *Computers & Security*, 157(August), 104606. <https://doi.org/10.1016/j.cose.2025.104606>
- Prasetyo, F., Putra, E., Anggreni, S., Sugi, A., Mufidah, K., & Febriani, Y. R. (2024). Analysis of Cyber Attacks on Network Security. *Jurnal Informasi Dan Teknologi*, 6, 4–7. <https://doi.org/10.60083/jidt.v6i2.569>
- Prayudi, Y., Islam, U., Mada, G., Ashari, A., & Priyambodo, T. K. (2021). The Framework to Support the Digital Evidence Handling : A Case Study of Procedures for the Management of Evidence in Indonesia. *Journal of Cases on Information Technology*, 22(3), 51–71. <https://doi.org/10.4018/JCIT.2020070104>
- Rakha, N. A. (2023). Cybercrime and the Law : Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican Law Review*, XVI(June 2024), 23–54.
- Salih, K. M. M., & Ibrahim, N. B. (2023). Digital forensic tools: A literature review. *Journal of Education and Science*, 32(1), 109–124. <https://doi.org/10.33899/edusj.2023.137420.1304>
- Saniyazova, Y., Mediyev, R., Saitova, E., Utegenova, G., & Kzykhoyayeva, A. (2024). Advancing Forensic Science in Kazakhstan : The Emergence and Impact of Digital Forensics in Cybercrime Investigation. *The Law, State and Telecommunications Review*, 16(2), 48–68.
- Schreuders, ZC; Cockcroft, TW; Butterfield, EM; Elliott, JR and Soobhany, A., & Shan-A-Khuda, M. (2020). Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force. *International Journal of Cyber Criminology*, 14(June), 316–340. <https://doi.org/10.5281/zenodo.3757271>
- Shahid, H., Joshi, M., & Kaya, M. (2024). Cross-border data flows and conflict of laws: A multi-layered framework for digital trade regulation. *Legal Studies in Digital Age*, 2(1), 53–68.
- Shevchuk, V., Bululukov, O., Chorny, H., Tyshchenko, O., & Baranchuk, V. (2025). Latest Criminalistic Tools and Technologies in the Investigation of Cybercrimes : International and Ukrainian Experience. *The Law, State and Telecommunications Review*, 17(1), 207–235.
- Singh, M., Khunteta, A., Ghosh, M., & Chang, D. (2022). Forensic Science International : Digital Investigation FbHash-E : A time and memory efficient version of FbHash similarity hashing algorithm. *Forensic Science International: Digital Investigation*, 41, 301375. <https://doi.org/10.1016/j.fsidi.2022.301375>
- Slimi, H., & Chichti, J. (2025). The Nexus Between Cybercrime and Irregular Migration in the Age of Cyberspace : Implications for Geographic Flexibility and Mobility Management. *Global Journal of Flexible Systems Management*. <https://doi.org/10.1007/s40171-025-00474-8>
- Stone, M. R. V. V. (2025). Confidence Levels of Artificial Intelligence Generated Evidence in



- Cybercrime Investigations - A Survey Confidence Levels of Artificial Intelligence. *Security Journal*, 39(3), 0–31.
- Tippe, P., Spiekermann, D., & Tippe, A. (2026). From dockets to Docker: Engineering realistic forensic scenarios for Onion Service investigations. *Forensic Science International: Digital Investigation*, 57(S), 302125. <https://doi.org/10.1016/j.fsidi.2026.302125>
- Tok, Y. C., & Chattopadhyay, S. (2023). Identifying threats, cybercrime and digital forensic opportunities in Smart City Infrastructure via threat modeling. *Forensic Science International: Digital Investigation*, 45, 301540. <https://doi.org/10.1016/j.fsidi.2023.301540>
- Tok, Y. C., Zheng, D. Y., & Chattopadhyay, S. (2025). A Smart City Infrastructure ontology for threats, cybercrime, and digital forensic investigation. *Forensic Science International: Digital Investigation*, 52(February), 301883. <https://doi.org/10.1016/j.fsidi.2025.301883>
- Tok, Y. C., Wang, C., & Chattopadhyay, S. (2020). STITCHER : Correlating digital forensic evidence on internet-of-things devices. *Forensic Science International: Digital Investigation*, 35, 301071. <https://doi.org/10.1016/j.fsidi.2020.301071>
- Track, S. (2025). *G20 ACWG 2025 Report on Impact of Technical Assistance , Capacity-Building and Knowledge Sharing Initiatives for Asset Recovery* (Issue October).
- Valjarevic, A. (2012). Harmonised Digital Forensic Investigation Process Model. *Information Security for South Africa*.
- Wu, Y., & Du, Y. (2026). AI-driven transformation in forensic medicine education : applications , pedagogical shifts , and future challenges. *Frontiers in Medicine*, January, 1–11. <https://doi.org/10.3389/fmed.2026.1732967>
- Yeboah-Ofori, A. (2020). Digital forensics investigation jurisprudence: Issues of admissibility of digital evidence. *Forensic Legal & Investigative Sciences*, 6(1), 1–8. <https://doi.org/10.24966/FLIS-733X/100045>
- Zhang, X., Liu, C. Z., Choo, K. R., & Alvarado, J. A. (2021). A design science approach to developing an integrated mobile app forensic framework. *Computers & Security*, 105, 102226. <https://doi.org/10.1016/j.cose.2021.102226>