OPEN ACCESS

ISAR Journal of Arts, Humanities and Social Sciences

Volume 3, Issue 8, 2025 | pp: 68-73.

Abbriviate Title- ISAR J Arts Humanit Soc Sci

ISSN *(Online)*- 2583-9691

https://isarpublisher.com/journal/isarjahss

Forensics in Cyber Law Enforcement: Roles, Techniques, and Ethical Imperatives

Ni Putu Suci Meinarni[1*], I Putu Agus Eka Darma Udayana[2], Aniek Suryanti Kusuma[3]

[1,2,3]Institut Bisnis & Teknologi Indonesia, Bali, Indonesia.

***Corresponding Author**
Ni Putu Suci Meinarni

Institut Bisnis & Teknologi Indonesia, Bali, Indonesia.

Article History
Received: 03.07.2025
Accepted: 11.08.2025
Published: 27.08.2025

Abstract: In today's hyper-connected digital era, cybercrime has emerged as a critical threat that not only inflicts losses on individuals but also endangers social stability, economic resilience, and national security. The rising intensity and sophistication of cyberattacks demand adaptive legal mechanisms, particularly through the application of digital forensics. This paper highlights the strategic role of IT forensics in cyber law enforcement by integrating technical expertise with professional ethics to ensure the validity of digital evidence while safeguarding human rights in judicial processes. Using a normative juridical and literature-based approach, the study explores the practical functions of digital forensics, regulatory challenges in Indonesia, and the urgent need for ethical standards in handling electronic evidence. The findings reveal that professionalism and ethical compliance are essential foundations for building a trustworthy and accountable digital justice system. This study contributes to the development of legal policy, the formulation of interdisciplinary curricula in law and technology, and the professionalization of law enforcement agencies in the cyber domain.

Keywords: Digital Forensics; Professional Ethics; Cyber Law; Digital Evidence; Law Enforcement.

Cite this article:

Meinarni, N. P. S., Udayana, I. P. A. E. D., Kusuma, A. S., (2025). Forensics in Cyber Law Enforcement: Roles, Techniques, and Ethical Imperatives. *ISAR Journal of Arts, Humanities and Social Sciences*, *3*(8), 68-73.

Introduction:

The rapid advancement of information and communication technology has transformed virtually every aspect of human life, from education and commerce to governance and social interaction. However, this transformation has also given rise to a new landscape of crime that is often difficult to trace and prosecute cybercrime. Unlike conventional crimes that usually leave tangible evidence, cybercrime frequently produces digital traces that are invisible, volatile, and easily manipulated. This unique characteristic necessitates the development of innovative approaches in law enforcement, particularly through digital or IT forensics.

Cybercrime in Indonesia has grown in both scope and impact in line with the country's significant increase in internet usage. According to the 2023 *We Are Social* report, there were over 213 million internet users in Indonesia, marking a 5.44% increase compared to the previous year (We Are Social, 2023) , Such growth, while offering opportunities for digital inclusion and economic innovation, has also intensified risks related to data breaches, hacking, online fraud, and malware distribution. Without a robust legal and technical framework, law enforcement agencies risk falling behind in responding to these challenges, leaving society increasingly vulnerable to cyber threats.

IT forensics (or digital forensics) has emerged as a vital discipline in bridging this gap. It refers to the systematic investigation of digital data using specialized tools and techniques to detect, collect, analyze, and preserve electronic evidence for legal purposes (Dasmen et al., 2024). Beyond technical processes, digital forensics requires strict adherence to legal standards and professional ethics to ensure that evidence is admissible in court and that fundamental human rights, such as the right to privacy, are not violated (Firdonsyah et al., 2023). The principle of *chain of custody*, for instance, is central to maintaining the integrity of evidence throughout the stages of collection, preservation, and presentation in judicial proceedings (Prayudi et al., 2020; Mustafa, 2024).

The urgency of digital forensic development in Indonesia is reflected in several high-profile cases that have drawn public attention. One widely discussed example was the misuse of digital access by an IT analyst in a government institution, who exploited forensic privileges for personal gain. Such incidents underscore that digital forensics is not merely about technical capacity but also about upholding professional integrity and ethical conduct. The handling of sensitive personal or organizational data must comply with established principles of law and human rights to prevent abuse and maintain public trust (Surahman, 2024).

Previous studies reinforce the strategic role of IT forensics in supporting legal enforcement. (Manggala et al., 2024), for example, examined its role in proving fraudulent online investment schemes, concluding that forensic techniques were indispensable in presenting admissible evidence in court. Similarly, Ginting et al. (2024) and Rifqi et al. (2023) applied the National Institute of Standards and Technology (NIST) forensic model in cases involving sexual harassment and WhatsApp-based cybercrimes, demonstrating how structured methodologies simplify the recovery and verification of deleted or hidden data. These works illustrate the necessity of standardized frameworks to enhance both efficiency and reliability in digital investigations.

Nevertheless, challenges remain, particularly in Indonesia, where the regulatory landscape often lags behind technological developments. While the *Information and Electronic Transactions Law* (UU ITE) recognizes digital evidence as legally valid, its practical enforcement is constrained by the absence of comprehensive technical guidelines and a lack of harmonization with international standards such as ISO/IEC 27037 and the ACPO principles (Veronika & Simanjuntak, 2022).(Horsman, 2020). Furthermore, gaps in human resource capacity, limited inter-agency coordination, and the absence of a universally accepted ethical code for forensic practitioners hinder effective law enforcement.

Another pressing issue lies in the ethical dimension of forensic practices. In the era of big data and ubiquitous surveillance, the line between legitimate investigation and privacy infringement can become blurred. As Firdonsyah et al. (2023) highlight in their systematic review, forensic investigators often face risks of overstepping boundaries when digital evidence is collected without proper oversight. The Supervision-Based Digital Forensics Framework (SUFREE) proposed by these scholars emphasizes the importance of embedding ethical supervision at every stage of the forensic process to safeguard both evidentiary integrity and civil liberties.

The stakes are even higher when digital forensics intersects with cases of national or global significance. Cybercrime is increasingly transnational, with perpetrators, victims, and digital evidence spread across multiple jurisdictions. The National Cyber and Crypto Agency of Indonesia (BSSN) reported over 500 million cyber incidents in 2023, a stark increase from 232 million in 2018 (Masyhar et al., 2023). Such numbers highlight the need for international collaboration, not only among governments but also with private technology companies that control critical data infrastructures. Instruments such as the Budapest Convention on Cybercrime and the recently endorsed UN Convention Against Cybercrime (2024) provide essential frameworks for harmonizing laws, facilitating evidence sharing, and ensuring human rights protection in digital investigations (Yunani & Ilmih, 2024).

IT forensics plays a dual role: first, as a technical enabler that equips law enforcement with the tools to trace and verify digital footprints; and second, as a normative discipline that integrates law, ethics, and technology into a coherent practice of justice. The Indonesian experience demonstrates that without this dual integration, forensic evidence risks being either technically unreliable or legally inadmissible. Worse, it may be misused in ways that undermine civil liberties. Thus, developing a credible and ethical forensic ecosystem is not merely a technical necessity but a democratic imperative.

This paper seeks to examine comprehensively the strategic role of digital forensics in strengthening cyber law enforcement, with a particular focus on Indonesia's regulatory and ethical landscape. The study employs a literature-based, normative juridical approach to evaluate current practices, identify gaps, and propose future directions. The discussion is organized into several key areas: definitions and techniques of digital forensics, the challenges of applying professional ethics, the legal validity of electronic evidence, reporting mechanisms for cybercrime, the role of professional codes of conduct, inter-agency and international collaboration, and illustrative case studies. Digital forensics at the intersection of technology, law, and ethics, this study aims to contribute to the discourse on building a more responsive, transparent, and accountable justice system in the digital age. In doing so, it highlights not only the opportunities but also the profound responsibilities that come with integrating forensic science into cyber law enforcement.

Research Methodology

This study adopts a literature-based research design combined with a normative juridical approach to explore the role of digital forensics in cyber law enforcement. The literature review method enables the researchers to synthesize and evaluate concepts, theories, and regulatory frameworks related to digital forensics from a wide range of secondary sources, including academic publications, national regulations, and judicial rulings. According to (Mustika, R., & Hidayat, 2022) , this approach is particularly effective for building a systematic theoretical understanding when primary data collection is not feasible. Emphasis was placed on selecting sources that are credible, recent, and relevant, such as the *Information and Electronic Transactions Law* (UU ITE), ISO/IEC 27037 standards on evidence handling, and scholarly reviews on digital forensic methodologies (Mustika, R., & Hidayat, 2022)

Data analysis was conducted through content analysis, a qualitative technique that identifies recurring themes, patterns of argumentation, and conceptual interrelations within the selected literature. This analytical process allowed the researchers to construct a conceptual framework for understanding both the strategic role and the challenges of IT forensics in Indonesia. By mapping regulatory gaps, ethical dilemmas, and technical practices, the study provides insights into how digital forensics can be better integrated into legal systems to ensure both evidentiary reliability and the protection of human rights. As Casino et al. (2022) note, such integrative approaches are vital in advancing the discipline, ensuring that digital forensic practices remain not only technically sound but also legally robust and ethically accountable (Casino et al., 2022)**.**

Findings and Discussions:

The Foundations and Techniques of Digital Forensics

Digital forensics, often referred to as computer forensics, is the scientific process of investigating, collecting, preserving, and analyzing electronic data for use in legal proceedings. Unlike conventional forensic investigations, which typically involve physical evidence, digital forensics focuses on intangible and volatile data such as system logs, metadata, deleted files, and encrypted communication. As (Dasmen et al., 2024)explain, digital forensics employs specialized tools and methodologies to retrieve traces of criminal activity from devices and networks, ensuring that the extracted data can withstand legal scrutiny in court.

Menururt (Gusti Ayu Gita Dharma Vahini Mahiratna et al., 2022) Digital forensik adalah proses dalam pemeriksaan bukti elektronik yang di mana dalam proses ini para penegak hukum akan mengambil, memulihkan, menyimpan dan memeriksa informasi atau dokumen elektronik yang terdapat dalam penyimpanan elektronik atau sistem elektronik yang akan dapat dipertanggungjawabkan untuk pembuktian. Tujuan dari digital forensik adalah memulihkan semua data yang hilang atau yang telah direkayasa dan penghapusan data atau file.

The scope of digital forensics encompasses multiple domains, each serving a specific investigative purpose. **Computer forensics** investigates operating systems, storage devices, and file structures, including the recovery of deleted documents and internet history (Yang et al., 2023). **Network forensics** monitors and analyzes traffic flows to detect intrusions, denial-of-service attacks, and unauthorized data transfers in real time. **Database forensics** focuses on examining database records, transaction logs, and temporary memory to identify anomalies and user activities. **Mobile device forensics** has become increasingly relevant, with smartphones and tablets often containing critical evidence in the form of call histories, text messages, GPS data, and social media interactions (Sutikno, 2024). Together, these branches form a comprehensive ecosystem that allows investigators to reconstruct digital events and establish accountability.

The methodologies applied in digital forensics typically follow a structured cycle, including **collection, examination, analysis, and reporting** (Haris et al., 2024) (Rifqi et al., 2023). The **collection phase** involves identifying and securing digital evidence while preserving its integrity. The **examination phase** processes raw data, extracting relevant information through forensic tools. The **analysis phase** interprets the data to answer investigative questions, such as identifying perpetrators or reconstructing timelines. Finally, the **reporting phase** presents findings in a transparent and legally defensible manner, detailing the techniques used and providing recommendations for future prevention (Ginting et al., 2024) (Terhadap & Konvensional, 2025). These steps are reinforced by international standards such as ISO/IEC 27037 and ACPO guidelines, which stress the importance of maintaining the original state of digital evidence and ensuring examiner competency.

The effectiveness of these techniques is demonstrated in several studies. For example, (Ginting et al., 2024) successfully reconstructed deleted WhatsApp messages in a sexual harassment case by applying the NIST forensic methodology, proving that even seemingly inaccessible data can be retrieved and used as valid evidence. Similarly, Manggala et al. (2024) highlighted the role of forensic analysis in prosecuting fraudulent online investment schemes, where digital traces were critical to confirming the perpetrator's activities. These cases underscore that digital forensics is not merely a technical exercise but a pivotal component of modern law enforcement, providing courts with reliable evidence to adjudicate increasingly sophisticated cybercrimes.

The foundational techniques of digital forensics combine scientific rigor with legal accountability. By encompassing diverse domains such as computer, network, mobile, and database forensics, the discipline equips investigators with tools to detect, reconstruct, and validate digital evidence. However, the effectiveness of these foundations depends not only on technological sophistication but also on adherence to legal standards and professional ethics, which will be further explored in the next section.

Ethical and Legal Challenges in Digital Forensics

While digital forensics offers indispensable tools for cyber law enforcement, its implementation is fraught with ethical and legal complexities. One of the foremost challenges is the **potential misuse of authority** by investigators who have access to highly sensitive data. (Firdonsyah et al., 2023)warn that without proper oversight, forensic practitioners may overstep their mandate, collecting or disclosing personal information unrelated to the case. This risk is amplified in the digital age, where vast volumes of private data are easily accessible. To mitigate such risks, the Supervision-Based Digital Forensics Framework (SUFREE) has been proposed, emphasizing the need for ethical oversight at each stage of investigation from evidence acquisition to reporting so as to ensure accountability, objectivity, and the protection of individual rights.

Another ethical dilemma lies in the **balance between privacy and security**. The forensic process often involves handling data that belong to private citizens or organizations, such as emails, social media accounts, or financial records. When mishandled, such evidence can result in privacy violations, leading not only to the loss of public trust but also to legal liability for investigators. (Surahman, 2024) notes that in an era characterized by "post-truth" narratives and widespread data manipulation, safeguarding privacy through strong ethical frameworks is as critical as securing evidence itself. This highlights the need for a professional code of ethics specifically designed for digital forensic practitioners. In Indonesia, steps have been taken toward drafting such a code, though implementation remains uneven (Mustafa, 2024).

From a legal perspective, the **principle of legality** plays a vital role in determining the admissibility of digital evidence. According to (Maharani et al., 2024) , all forensic activities must be conducted in strict compliance with applicable laws such as the *Electronic Information and Transactions Law (UU ITE)* and the *Criminal Procedure Code (KUHAP)*. These regulations provide the formal foundation for recognizing electronic evidence in court. However, gaps remain in terms of technical guidance, as the UU ITE does not comprehensively address the practical processes of evidence acquisition and preservation. This gap often creates uncertainty for both investigators and judges in determining whether evidence has been lawfully obtained.

To address this issue, international standards such as **ISO/IEC 27037** and the **ACPO guidelines** have been referenced as benchmarks. These standards emphasize the preservation of original data, examiner competence, and proper audit trails as prerequisites for maintaining evidentiary integrity (Aldiansyah, 2023). Yet, their application in Indonesia has been inconsistent, partly due to the lack of harmonized national technical regulations. This inconsistency can undermine the credibility of digital forensics in judicial proceedings, particularly when evidence is challenged by defense counsel.

Case studies further illustrate these challenges. In the high-profile hacking of activist Ravio Patra's social media account, (Anggraeni & Salsabila, 2024) pointed out that questions over the **validity of digital evidence** and the **legality of the arrest** cast doubt on the fairness of the legal process. Similarly, the unauthorized disclosure of patients' medical records during the COVID-19 pandemic

violated both privacy rights and medical confidentiality, breaching multiple laws and ethical (Materi et al., 2022) These examples underscore that ethical lapses and weak legal safeguards can compromise not only individual rights but also the overall legitimacy of the justice system. The ethical and legal challenges in digital forensics revolve around three interrelated issues: the risk of data misuse by investigators, the tension between privacy rights and law enforcement needs, and the uneven application of legal standards for electronic evidence. Addressing these challenges requires the establishment of clear professional codes of conduct, harmonized national regulations aligned with international standards, and effective oversight mechanisms. Without these safeguards, the potential of digital forensics to strengthen justice may be overshadowed by risks of abuse and public distrust (Masyhar et al., 2023)(Yunani & Ilmih, 2024).

Collaborative Roles and International Perspectives

The complexity of cybercrime often exceeds the investigative capacity of individual law enforcement agencies. Limited resources, specialized technical requirements, and the cross-border nature of cyber offenses necessitate **collaboration across institutions and jurisdictions**. In Indonesia, collaboration between digital forensic experts, the police, and judicial institutions has proven essential for strengthening legal processes. Al-Husaini et al. (2020) describe the Collaborative Digital Forensic Investigations Model (CDFIR) as a framework that integrates law enforcement agencies and forensic laboratories through unified platforms and standardized procedures, ensuring that investigations are both efficient and legally defensible. Within such collaborations, forensic specialists contribute technical expertise in data recovery and evidence authentication, while police and legal institutions manage criminal investigation, prosecution, and adjudication (Hukum et al., 2025)

Beyond national collaboration, the **transnational nature of cybercrime** demands robust international cooperation. Cybercriminals often operate across multiple jurisdictions, making it difficult to trace perpetrators or secure digital evidence without cross-border assistance. The Indonesian National Cyber and Crypto Agency (BSSN) recorded a dramatic surge in cyber incidents from 232 million in 2018 to over 500 million in 2023, underscoring the urgent need for international coordination (Masyhar et al., 2023). INTERPOL has played a pivotal role in this domain, facilitating data sharing, providing intelligence support, and coordinating global responses to cyber threats. Meanwhile, instruments such as the *Budapest Convention on Cybercrime* and the newly endorsed *UN Convention Against Cybercrime (2024)* serve as legal backbones for harmonizing national laws and establishing shared standards for evidence handling (Yunani & Ilmih, 2024).

The private sector also plays a crucial role in international collaboration. Global technology companies often hold critical user data that may serve as evidence in cybercrime cases. Cooperation with these entities can provide law enforcement agencies with timely access to data, though such partnerships raise questions of jurisdictional authority and privacy rights. (Setya & Suganda, 2022) argue that blockchain-based solutions may offer innovative mechanisms for ensuring transparency and maintaining audit trails in digital investigations, thus fostering greater trust among stakeholders across different legal systems.

Case studies demonstrate how weak collaboration or fragmented international frameworks can hinder justice. For instance, delayed cross-border data requests have often resulted in the loss of volatile digital evidence, while differences in national legal systems can create disputes over jurisdiction and admissibility. By contrast, harmonized regulations and coordinated operations have led to successful takedowns of international cybercriminal networks. This highlights that collaboration is not only a matter of resource sharing but also a means of enhancing legitimacy and ensuring consistent legal protection for victims across borders.

In conclusion, effective cyber law enforcement requires a **multi-level collaborative approach**: national cooperation among law enforcement agencies and forensic laboratories, regional and global collaboration through organizations such as INTERPOL, and partnerships with private technology providers. Strengthening these collaborative mechanisms, while ensuring adherence to legal standards and ethical safeguards, is crucial for addressing the borderless nature of cybercrime. Indonesia's participation in international conventions and its efforts to integrate forensic practices with global standards represent important steps toward building a more resilient and trustworthy cyber justice ecosystem (Sa'diyah & Ihsan, 2023) (Al-Husaini et al., 2020)(Hukum et al., 2025).

Conclusion:

Digital forensics has become an indispensable pillar of modern cyber law enforcement, providing the technical means to uncover, preserve, and present electronic evidence while simultaneously demanding adherence to legal standards and ethical accountability. The findings of this study emphasize that the effectiveness of digital forensics does not lie solely in advanced tools and methodologies but also in the professionalism, integrity, and cross-sector collaboration of its practitioners. Indonesia's experience demonstrates that without clear ethical guidelines, harmonized regulations, and international cooperation, digital evidence risks being unreliable or even misused, undermining both justice and public trust. Therefore, strengthening regulatory frameworks, embedding ethical codes of conduct, and fostering collaboration among law enforcement, forensic experts, policymakers, and global partners are critical steps toward building a resilient and trustworthy digital justice ecosystem in the face of increasingly sophisticated cybercrime.

Bibliography

1. Aldiansyah, R. (2023). *Etika Profesi Teknologi Informasi: Pelanggaran Keamanan Data*. *June*, 4–9.
2. Al-Husaini, Y., Al-Khateeb, H., Warren, M., Pan, L., & Epiphaniou, G. (2020). Collaborative Digital Forensic Investigations Model for Law Enforcement. *Security and Organization within IoT and Smart Cities*, 157–180. https://doi.org/10.1201/9781003018636-9
3. Anggraeni, D. R., & Salsabila, M. (2024). Analisis Yuridis Peran Digital Forensik Dalam Pembuktian Tindak Pidana di Indonesia. *Media Hukum Indonesia (MHI)*, *2*(2), 593–600.
4. Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews. *IEEE Access*, *10*, 25464–25493. https://doi.org/10.1109/ACCESS.2022.3154059

5. Dasmen, R. N., Pratama, M. R., Yasir, H., & Budiman, A. (2024). Analisis Forensik Digital Pada Kasus Cyberbullying Dengan Metode National Institute of Standard and Technology Sp 800-86. *Jurnal Ilmiah Informatika*, *12*(01), 68–73. https://doi.org/10.33884/jif.v12i01.8344
6. Fatmah, N., & Indrayani, R. (2022). Analisis forensik digital pada Solid State Drive fungsi TRIM menggunakan tools Autopsy dan OSForensics. *Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD*, *5*(2), 185–192. https://ojs.trigunadharma.ac.id/index.php/jsk/index
7. Fahrudin, Aziz dan Gufron Zaida Muflih. (2025). Analisis Forensik Digital pada pesan Whatsapp yang terenkripsi dengan pretty good privacy (PGP) menggunakan framework DFRWS. Jurnal Mahasiswa Teknik Informatika, Vol. 9 No. 1, Februari 2025.
8. Firdonsyah, A., Purwanto, P., & Riadi, I. (2023). Framework for Digital Forensic Ethical Violations: A Systematic Literature Review. *E3S Web of Conferences*, *448*, 1–10. https://doi.org/10.1051/e3sconf/202344801003
9. Ginting, J. A., Setiawan, H., Andry, J. F., & Ngurah Suryantara, I. G. (2024). Rekonstruksi Dan Investigasi Digital Forensik Pada Aplikasi Whatsapp Dengan Metode Nist : Kasus Pelecehan Seksual. *Infotech: Journal of Technology Information*, *10*(1), 71–76. https://doi.org/10.37365/jti.v10i1.249
10. Gusti Ayu Gita Dharma Vahini Mahiratna, Dewi, A. A. S. L., & Wirawan, K. A. (2022). Kekuatan Alat Bukti Media Sosial Dalam Perkara Tindak Pidana Judi Online. *Jurnal Preferensi Hukum*, *4*(1), 2746–5039.
11. Haris, O. K., Abdullah, S. A., Rizky, A., Indah, S. R., & others. (2024). Penggunaan Digital Forensik dalam Pembuktian Tindak Pidana Pencemaran Nama Baik di Media Sosial Berdasarkan UU ITE. *Halu Oleo Legal Research*, *6*(2), 588–603.
12. Horsman, G. (2020). ACPO principles for digital evidence: Time for an update? *Forensic Science International: Reports*, *2*(February), 100076. https://doi.org/10.1016/j.fsir.2020.100076
13. Hukum, S., Judijanto, L., & Nugroho, B. (2025). *Regulasi Keamanan Siber dan Penegakan Hukum terhadap Cybercrime di Indonesia*. *3*(3), 118–124. https://doi.org/10.58812/shh.v3.i03
14. Julian, D., & Sutabri, T. (2023). Analisa kinerja aplikasi digital forensik Autopsy untuk pengembalian data menggunakan metode NIST SP 800-86. *Jurnal Informatika Terpadu*, *9*(2), 136–142. https://journal.nurulfikri.ac.id/index.php/JIT
15. Kazaure, A. A., Jantan, A., & Yusoff, M. N. (2023). Digital Forensics Investigation Approaches in Mitigating Cybercrimes: A Review. *Journal of Information Science Theory and Practice*, *11*(4), 14–39. https://doi.org/10.1633/JISTaP.2023.11.4.2
16. Maharani, N., Lamminar, A., Christiansen, N., & Rafidah, A. R. (2024). *Media Hukum Indonesia (MHI) Validitas Bukti Digital dan Legalitas Penangkapan Pada Kasus Peretasan Akun Media Sosial Ravio Patra Media Hukum Indonesia (MHI)*. *2*(3), 75–81.
17. Manggala, B. S., Putri, A., Suzeeta, N. S., Nabila Zalfa, V. C., Marpaung, I. H., Natalia, A. A., & Nugroho. (2024). *Analisis Yuridis Peran Digital Forensik Dalam Pembuktian Kasus Penipuan Berkedok Investasi Online (Studi Kasus Doni Salmanan)*. *01*(2), 295–301.
18. Masyhar, A., Utari, I. S., Usman, & Sabri, A. Z. S. A. (2023). Legal Challenges of Combating International Cyberterrorism: The NCB Interpol Indonesia and Global Cooperation. *Legality: Jurnal Ilmiah Hukum*, *31*(2), 344–366. https://doi.org/10.22219/ljih.v31i2.29668
19. Materi, P., Gerak, S., Keguruan, F., & Ilmu, D. A. N. (2022). *Dewi Retno Puspitasari*.
20. Marcellino, S., Seta, H. B., & Widi, W. (2023). Analisis forensik digital recovery data smartphone pada kasus penghapusan berkas menggunakan metode National Institute of Justice (NIJ). *JURNAL INFORMATIK*, *19*(2), 141–156.
21. Mustafa, C. (2024). Integritas Chain of Custody Pada Pemeriksaan Bukti Digital. *Judex Laguens*, *2*(1), 75–96.
22. Mustika, R., & Hidayat, A. (2022). *Digital forensik dan penegakan hukum: Perspektif teknologi dan hukum. Jakarta: Prenada Media*.
23. Permana, Lutfi Aldri et al.(2023). Analisis Forensik Keaslian gambar menggunakan Autopsy, Jurnal and Robotics, Vol. 1. No: 2 Desember 2023, hal 39-45.
24. Ratul, M. H. A., Mollajafari, S., & Wynn, M. (2024). Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution. *Sustainability (Switzerland)*, *16*(24). https://doi.org/10.3390/su162410885
25. Rifqi, M., Ismail, S. J. I., Rizal, M. F., Studi, P., Teknologi, D., & Telkom, U. (2023). Analisis Forensik Untuk Penanganan Cyber Crime Pada Aplikasi Whatsapp Menggunakan Metode National Institute of Standard and Technology (Nist Sp 800-86). *E-Proceeding of Applied Science*, *9*(6), 3017–3022.
26. Riadi, Imam et al.(2021). Forensik Mobile pada Layanan Media Sosial Linkedin. Jurnal JISKA, Vol. 6, No. 1 Januari 2021, Pp 9-20.
27. Sa'diyah, D., & Ihsan, A. Y. (2023). Pertanggungjawaban Pidana Dokter yang Membuka Rahasia Rekam Medis Pasien Covid-19 (Studi Kasus Dokter Jane S.P Rad) History Abstrak. *Jurnal Hukum*, *2*(2), 65–73.
28. Setya, A., & Suganda, A. (2022). Design of Digital Evidence Collection Framework in Social Media Using SNI 27037: 2014. *JUITA: Jurnal Informatika*, *10*(1), 127. https://doi.org/10.30595/juita.v10i1.13149
29. Surahman, S. (2024). Post Truth: Ethics and Digital Security. *Journal of Law, Social Science and Humanities*, *2*(1), 53–60.
30. Sutikno, T. (2024). Mobile forensics tools and techniques for digital crime investigation: a comprehensive review. *International Journal of Informatics and Communication*

Technology, *13*(2), 321–332. https://doi.org/10.11591/ijict.v13i2.pp321-332

31. Terhadap, H., & Konvensional, K. (2025). *Lex progressium*. *2*(1), 1–8.
32. Utami, Dyah Syaza et al. (2021). Analisis Live Forensik pada Whatsapp Web untuk pembuktian kasus penipuan transaksi elektronik. Jurnal CyberSecurity dan Forensik Digital, Vol. 4, No 1, Mei 2021, hlm 24-32.
33. Veronika, V., & Simanjuntak, B. H. (2022). Implementasi Iso 27037 Dalam Pemeriksaan Investigatif Dengan Teknik Forensik Digital Untuk Memperoleh Bukti Audit Di Badan Pemeriksa Keuangan (Bpk). *Jurnal Magister Akuntansi Trisakti*, *9*(2), 89–104. https://doi.org/10.25105/jmat.v9i2.13343
34. We Are Social. (2023). Digital 2023 Indonesia. *We Are Social*, 125. https://wearesocial.com/wp-content/uploads/2023/03/Digital-2023-Indonesia.pdf
35. Yang, L., Moubayed, A., Shami, A., Boukhtouta, A., Heidari, P., Preda, S., Brunner, R., Migault, D., & Larabi, A. (2023). Forensic Data Analytics for Anomaly Detection in Evolving Networks. *Innovations in Digital Forensics*, 99–138. https://doi.org/10.1142/9789811273209_0004
36. Yunani, F. A., & Ilmih, A. A. (2024). *Kajian Yuridis Kejahatan Lintas Negara Berkaitan Dengan Perlindungan Data Pribadi*. *2*(3), 586–592.