PALAR (Pakuan Law Review)
https://journal.unpak.ac.id/index.php/palar

Volume 12, Number 01, January-March 2026, Pages 281-288
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

Reconstruction of Digital Evidence Models in Cybercrime: An Integrative Analysis of Contemporary Criminology and Digital Forensics

Rachmat Alviando[1]; Herlita Eryke[2].

[1,2,] Faculty of Law, Department of Law, University of Bengkulu, Indonesia
E-mail: rachmatalviando2611@gmail.com, herlitaeryke@unib.ac.id.
Manuscripts received : 28/02/2026, Revision and Review : 10/02/2026, Approved 15/03/2026

Abstract

The rapid development of information technology has changed the social and economic landscape, while introducing complex challenges in the form of cybercrime, which is often difficult to handle using conventional legal evidence mechanisms. This study aims to develop and test a conceptual model that links perpetrator criminogenic factors, the application of digital forensics, and regulatory or institutional power with the success of digital evidence in cybercrime cases. To address this issue, a quantitative approach with a correlational design was used, with data collected through a purposive sampling survey of 120 law enforcement practitioners and digital forensic experts in Indonesia. The results show that the application of digital forensics ($\beta = 0.45$, $p < 0.001$) and regulatory strength ($\beta = 0.28$, $p < 0.01$) significantly increase the success of digital evidence, while perpetrator criminogenic factors and complex modus operandi have a negative influence ($\beta = -0.22$, $p < 0.05$). Analysis of these findings suggests that the success of digital evidence is highly dependent on the integration of technical-forensic precision with institutional support to counter the increasing complexity of anti-forensic techniques used by criminals. This study provides a significant scientific contribution by offering a multidimensional model that integrates technical forensic procedures with criminological profiling, thereby enriching the development of the evidence system in modern criminal law. Based on this analysis, it is recommended that law enforcement agencies strengthen the capacity of digital forensic laboratories and harmonize legal regulations to be more adaptive to the dynamic nature of cyber threats and technological advances.

Keywords: Cybercrime; Digital Evidence; Digital Forensics; Contemporary Criminology.

A. Introduction

The rapid development of information and communication technology and increased global internet access have driven socio-economic transformation while also giving rise to new challenges in the form of *cybercrime*, which affects various aspects of modern life[1]. The main problem that arises is the inability of conventional evidence mechanisms to deal with the characteristics of digital evidence, which is easily transferred, manipulated, and often

[1] Afrin Nafish and A. Rengarajan, "The Effects of Technology Evolution on Cybercrime," *International Journal of Innovative Research in Computer and Communication Engineering* 12, no. 02 (February 25, 2024): 1060–66, https://doi.org/10.15680/ijircce.2024.1202056.

Volume 12, Number 01, January-March 2026, Pages 281-288
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

involves cross-border jurisdictions[2]. In Indonesia, the urgency of this issue is evident from a significant spike in cybercrime reports, reaching 8,831 cases in 2022, where digital evidence is central to criminal investigations to reconstruct technology-based criminal events[3]. Despite fluctuating dynamics in subsequent years, cyber threats remain at a serious level that requires strengthening the investigation system and the capacity of officials to ensure the effectiveness of law enforcement amid the vulnerability of the national digital infrastructure[4].

The unpreparedness of the legal system to keep up with the rapid dynamics of technology raises specific issues regarding the validity and reliability of digital evidence in court [5]; [6]; [7]. A particular issue to be addressed in this study is the gap between digital investigation practices and legality standards, where digital forensic infrastructure in Indonesia is not yet uniform and the number of experts is still very limited[8];[9]. In addition, the absence of integrated inter-agency guidelines often results in suboptimal evidence integrity assessment processes, which ultimately threatens the application of the principle of justice in increasingly complex and transnational cybercrime cases. Therefore, a reconstruction of the evidence model is needed that can systematically integrate technical forensic aspects with the applicable legal framework.

International literature shows that advances in digital forensics have been responded to with various innovations such as the integration of artificial intelligence (*AI*) and *machine learning* to analyze digital artifacts and IoT device traces [10];[11]. However, most previous studies are still stuck on the technical focus of data detection and recovery without touching on the need for a comprehensive evidence model. There is a significant research gap where existing studies tend to separate criminological aspects (motives and

[2] Rofila Salsa Billah and Horadin Saragih, "Tantangan Penegakan Hukum Kejahatan Siber Bagi Hakim Dari Aspek Hukum Pembuktian Di Indonesia," *Arus Jurnal Sosial Dan Humaniora* 5, no. 2 (August 15, 2025): 2739–47, https://doi.org/10.57250/ajsh.v5i2.1543.

[3] Muhammad Fadil Fadillah and Trihastuti Yuniati, "Perbandingan Hasil Recovery Tools Mobile Forensic Di Smartphone Android Menggunakan Metode National Institute of Justice (NIJ)," *Cyber Security Dan Forensik Digital* 6, no. 2 (February 1, 2024): 54–61, https://doi.org/10.14421/csecurity.2023.6.2.4172.

[4] Endro Satoto and Faisal Santiago, "Reconstruction of Indonesia's Cyber Law System for Adaptive and Integrated Digital Crime Prevention in the Era of Technological Disruption," *Greenation International Journal of Law and Social Sciences* 3, no. 2 (June 18, 2025): 309–17, https://doi.org/10.38035/gijlss.v3i2.425.

[5] Nurjana Lahangatubun and Andi Muliyono, "Public Trust and the Legal Validity of Electronic Signatures in Indonesia," *JIHK* 7, no. 1 (June 27, 2025): 499–516, https://doi.org/10.46924/jihk.v7i1.311.

[6] Bambang Sujatmiko and Bambang Soesatyo, "The Urgency of Using Electronic Evidence in Trials as an Effort to Answer the Challenges of Law Enforcement in the Digital Era and Social Media Dynamics," *Asian Journal of Social and Humanities* 3, no. 9 (June 20, 2025): 1604–13, https://doi.org/10.59888/ajosh.v3i9.567.

[7] Amelia Sukmasari et al., "Application of Electronic Evidence as Extension of Legal Civil Evidence Divorce Cases in Indonesia," *International Journal of Law, Environment, and Natural Resources* 4, no. 1 (April 5, 2024): 1–14, https://doi.org/10.51749/injurlens.v4i1.95.

[8] Edwin Setiawan and Hartiwiningsih, "Optimizing the Use of Digital Forensics and Information Technology in Proving Criminal Acts of Electronic Document Forgery in Indonesia," *International Journal of Law, Crime and Justice* 2, no. 2 (May 14, 2025): 72–86, https://doi.org/10.62951/ijlcj.v2i2.587.

[9] Feby Thealma and Yova Rudelviani, "Digital Forensic Ethical Data Handling in Indonesia," *The Indonesian Journal of Computer Science* 14, no. 1 (February 7, 2025), https://doi.org/10.33022/ijcs.v14i1.4588.

[10] Mahmoud Basharat, "Machine Learning in IoT and Mobile Device Forensics," *Advances in Digital Crime, Forensics, and Cyber Terrorism Book Series*, December 30, 2024, 115–46, https://doi.org/10.4018/979-8-3373-0857-9.ch005.

[11] Usharani Bhimavarapu, "Deep Learning for Digital Forensics," *Advances in Computational Intelligence and Robotics*, June 24, 2025, 155–70, https://doi.org/10.4018/979-8-3373-0245-4.ch006.

Volume 12, Number 01, January-March 2026, Pages 281-288
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

perpetrator profiles) from technical digital forensics aspects[12];[13]; [14]. The strength of previous research methods lies in their ability to provide in-depth normative analysis of the regulatory framework and description of the role of forensics in law enforcement [15]; [16]. However, their fundamental weakness is the lack of quantitative evaluation that systematically tests the relationship between variables, as well as their failure to clearly position how the interaction between digital evidence quality, expert competence, and perpetrator motivations affects practical evidence effectiveness.

To address these limitations and clearly establish the position of this research within existing scientific literature, this study offers an integrative model of digital evidence that combines contemporary criminological analysis, digital forensic procedures, and institutional regulatory support to increase the effectiveness of evidence in cybercrime cases in Indonesia. This correlational design not only describes the phenomenon but also measures the simultaneous influence of these multidimensional factors. Furthermore, the reconstruction of this digital evidence model is designed to provide clear legal policy implications, offering a foundation for reformulating more adaptive regulations to counteract sophisticated anti-forensic techniques. Ultimately, this research aims to test and develop a reliable conceptual model to improve the success of prosecutions in cybercrime cases in Indonesia.

B. Research Method

This study uses quantitative research with a correlational (non-experimental) design to examine the relationship between predetermined variables. The approach used is an empirical approach that focuses on the legal behavior of practitioners in the field related to digital evidence[17];[18]. The data source in this study is primary data obtained directly from respondents through the distribution of research instruments. The research population includes all law enforcement practitioners and digital forensic experts in Indonesia who have qualifications or experience in handling cybercrime cases.

The data collection technique was conducted through a survey using a closed questionnaire compiled based on a Likert scale to measure the construct of each research variable. Given the scattered population and the need for specific expertise, sampling was carried out using *purposive sampling*, where respondents were selected based on criteria of real experience in investigations or trials involving electronic evidence. Before full data collection was carried out, the research instruments first underwent construct validity

[12] Yidnekachew Worku Kassa, Joshua Isaac James, and Elefelious Getachew Belay, "Intention Recognition for Digital Forensics: A Formal Model," February 11, 2025, https://doi.org/10.20944/preprints202502.0764.v1.

[13] Yidnekachew Worku Kassa, Joshua Isaac James, and Elefelious Getachew Belay, "Intention Recognition for Digital Forensics: A Formal Model," February 11, 2025, https://doi.org/10.20944/preprints202502.0764.v1.

[14] Malinka Ivanova and Svetlin Stefanov, "Digital Forensics Investigation Models: Current State and Analysis," June 20, 2023, https://doi.org/10.23919/splitech58164.2023.10193176.

[15] Achmad Miftah Farid and Novi Nur Indahsari, "Fungsi Hasil Laboratorium Forensik Sebagai Bukti Dalam Tindak Pidana Narkotika," *JURNAL USM LAW REVIEW* 7, no. 3 (December 22, 2024): 1911–11, https://doi.org/10.26623/julr.v7i3.10729.

[16] Ratu Wida and Subhandi Bakhtiar, "Peranan Metode Scientific Crime Investigation Melalui Ilmu Kedokteran Forensik Dalam Proses Pengungkapan Jenazah Di Pondok Gede Permai, Kota Bekasi," *Jurnal Hukum Dan Sosial Politik* 2, no. 4 (November 28, 2024): 123–30, https://doi.org/10.59581/jhsp-widyakarya.v2i4.4294.

[17] Rezza Fauziyah, Agus Raharjo, and Setya Wahyudi, "Efektivitas Penegakan Hukum Tindak Pidana Pemilu Melalui Media Sosial," *Syntax Literate ; Jurnal Ilmiah Indonesia* 10, no. 8 (August 15, 2025): 6642–54, https://doi.org/10.36418/syntax-literate.v10i8.61435.

[18] Teddy Lahati, "EKSISTENSI DAN PERAN ALAT BUKTI ELEKTRONIK DALAM SISTEM PERADILAN DI INDONESIA," *Judex Laguens* 2, no. 1 (March 22, 2024): 97–107, https://doi.org/10.25216/ikahi.2.1.4.2024.97-107.

Volume 12, Number 01, January-March 2026, Pages 281-288
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

testing and internal reliability testing using *Cronbach's alpha* to ensure measurement consistency.

The data analysis technique in this study was carried out in two main stages using statistical software. First, descriptive statistical analysis was used to describe the characteristics of the respondents and the distribution of variable scores through the calculation of means, percentages, and standard deviations. Second, inferential statistical analysis was applied to rigorously test the hypotheses. Specifically, multiple linear regression analysis was selected as the primary analytical tool because it effectively measures the simultaneous and partial influence of multiple independent variables (criminogenic factors, digital forensics application, and regulatory strength) on a single dependent variable (the success of digital evidence).

The hypothesis testing process involved the F-test to assess the overall model's significance and the t-test to evaluate the individual contribution of each predictor at a strict significance level ($p < 0.05$). Furthermore, to fulfill the fundamental objectives of legal research, the statistical outputs from this regression analysis were not merely interpreted mathematically. Instead, the numerical results were synthesized and interpreted contextually within the framework of Indonesian criminal procedural law and contemporary criminological theories. This ensures that the statistical findings directly translate into comprehensive legal policy implications and practical recommendations for law enforcement.

C. Results and Discussion

1. Dynamics of Cybercrime Development in Modern Legal Systems

Based on the analysis of 120 respondents consisting of investigators, prosecutors, judges, and digital forensic experts, the level of readiness and effectiveness of digital evidence in Indonesia is currently in the moderate to good category. The success of digital evidence scored an average of 3.60 (SD=0.68), indicating that although digital evidence is increasingly accepted in court, the process of achieving complete legal certainty still faces significant procedural and technical challenges amidst the rapid evolution of cyber threats. Fluctuations in cyber cases and the continuous adaptation of crime patterns, such as the use of artificial intelligence for document forgery, demand a highly adaptive legal system that can quickly respond to new technological phenomena.

2. The Role of Digital Forensics in the Criminal Evidence System

Digital forensics plays a crucial role in uncovering cybercrimes. The average score for the implementation of digital forensics reached 3.85 (SD=0.62), showing that most practitioners assess the identification, collection, and preservation of evidence as being well-executed according to standard operating procedures. Hypothesis testing through multiple linear regression reveals that the application of digital forensics has the most dominant positive influence ($\beta = 0{,}45, p < 0{,}001$) on the success of evidence in court. This proves that higher-quality forensic operational standards linearly increase the probability of successful digital evidence presentation. The details of the regression parameter testing results are presented in Table 1 below.

Table 1. Results of Regression Analysis of the Influence of Criminogenic, Forensic, and Regulatory Factors

Volume 12, Number 01, January-March 2026, Pages 281-288
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

Independent Variables	Coefficient (β)	Standard Error	t-Statistic	Significance (p)
Application of Digital Forensics	0.45	0.06	7.5	< 0.001
Regulatory/Institutional Strength	0.28	0.08	3.5	< 0.01
Criminogenic Factors of Perpetrators	-0.22	0.07	-3.14	< 0.05
Moderating Effect (Regulation * Forensic)	0.15	0.05	2.17	0.03

3. Analysis of Criminogenic Factors in the Complexity of Cybercrime

The empirical data was further analyzed using contemporary criminology theory to deeply understand the negative impact of the perpetrator's modus operandi on the evidence process. Criminogenic factors and complex modus operandi have a significant negative influence ($\beta = -0{,}22, p < 0{,}05$), severely hindering the legal evidence process. This finding strongly supports the application of neutralization and differential association theories; modern cybercriminals often possess high technical skills acquired from closed communities to minimize their digital footprints and psychologically justify their illegal actions. Because evidence is frequently found in encrypted forms or manipulated using anti-forensic techniques, law enforcement must not solely focus on hardware. Instead, they must deeply analyze the sociological profile and behavioral patterns of cybercriminals to accurately predict and counter evidence removal strategies.

4. The Influence of Regulation and Institutions on Digital Evidence

Technical validity is insufficient without strong formal legal backing. The variables of regulatory strength and institutional capability recorded an average score of 3.40 (SD=0.75), reflecting that legal support and infrastructure urgently need reinforcement. Regression analysis shows institutional strength significantly influences evidence success ($\beta = 0{,}28, p < 0{,}01$). Furthermore, an interaction test revealed a crucial moderating effect: regulatory and institutional capabilities significantly reinforce the positive impact of digital forensics (interaction coefficient ($\beta = 0{,}15, (p < 0{,}03$). Interpreting these statistics from a legal perspective highlights a critical point: technically sound digital evidence may still be deemed inadmissible if seizure procedures and the *chain of custody* violate formal legal corridors. Therefore, continuous synchronization between IT experts and law enforcement officials is mandatory to close legal loopholes frequently exploited by defense attorneys to invalidate electronic evidence.

5. Reconstruction of the Digital Evidence Model in Law Enforcement

Addressing the gap in previous publications, this study successfully constructs an integrative digital evidence model combining criminological profiling, forensic technicalities, and institutional strengthening. This multidimensional model powerfully explains 48% of the variance in digital evidence success ($R^2 = 0{,}48,\ F(3{,}116) = 35{,}2, p < 0{,}001$. The uniqueness of this reconstruction lies in shifting the paradigm from a purely linear-technical approach to a holistic-contextual one, providing empirical evidence that institutional strength acts as a catalyst maximizing forensic potential before judges. The

Volume 12, Number 01, January-March 2026, Pages 281-288
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

legal policy implications of this model are profound. It explicitly demands policy reform to standardize regional digital forensic laboratories to prevent regional disparities in evidence quality. Moreover, human resource capacity building through specialized, continuous training for prosecutors and judges regarding the technical aspects of digital evidence is absolutely necessary to prevent a knowledge gap during the evidentiary process in court.

D. Conclusion and Recommendations

This study concludes that the effectiveness of digital evidence in combating cybercrime in Indonesia is determined by the integration of three main pillars: the quality of digital forensic techniques, the strengthening of institutional regulations, and a deep understanding of the criminogenic factors of perpetrators. The proposed reconstruction model proves that although digital forensic capabilities are a crucial instrument in improving the accuracy of investigations, their success is highly dependent on adaptive regulations as a moderating variable that validates the evidence before the law. Furthermore, the sociological-criminological aspects of perpetrators, particularly their sophisticated anti-forensic techniques, cannot be separated from the formal legal process. Theoretically, this research contributes to the legal literature by shifting the evidence paradigm from a purely technical focus to a holistic-contextual approach that synthesizes contemporary criminology and digital forensics.

Practically, this integrative model provides a concrete foundation for law enforcement agencies to standardize digital forensic laboratories across all regions to ensure the consistency of electronic evidence quality. Policymakers are strongly recommended to conduct dynamic regulatory harmonization to accommodate new types of evidence, such as artificial intelligence artifacts and IoT traces, to minimize legal loopholes in court. Additionally, continuous training for investigators, prosecutors, and judges on the *chain of custody* is highly recommended to ensure data integrity is maintained until a court decision is handed down.

For future academic research, it is highly recommended to expand this study by employing a comparative approach to evaluate digital evidence systems within the legal frameworks of other countries. Moreover, future studies should advance the analysis of digital evidence by examining final court decisions related to cybercrime. Integrating this empirical approach with deeper normative analysis will further strengthen the external validity and theoretical robustness of the developed digital evidence model.

Volume 12, Number 01, January-March 2026, Pages 281-288
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

References

Basharat, Mahmoud . "Machine Learning in IoT and Mobile Device Forensics." *Advances in Digital Crime, Forensics, and Cyber Terrorism Book Series*, December 30, 2024, 115–46. https://doi.org/10.4018/979-8-3373-0857-9.ch005.

Bhimavarapu, Usharani. "Deep Learning for Digital Forensics." *Advances in Computational Intelligence and Robotics*, June 24, 2025, 155–70. https://doi.org/10.4018/979-8-3373-0245-4.ch006.

Billah, Rofila Salsa, and Horadin Saragih. "Tantangan Penegakan Hukum Kejahatan Siber Bagi Hakim Dari Aspek Hukum Pembuktian Di Indonesia." *Arus Jurnal Sosial Dan Humaniora* 5, no. 2 (August 15, 2025): 2739–47. https://doi.org/10.57250/ajsh.v5i2.1543.

Fadillah, Muhammad Fadil, and Trihastuti Yuniati. "Perbandingan Hasil Recovery Tools Mobile Forensic Di Smartphone Android Menggunakan Metode National Institute of Justice (NIJ)." *Cyber Security Dan Forensik Digital* 6, no. 2 (February 1, 2024): 54–61. https://doi.org/10.14421/csecurity.2023.6.2.4172.

Farid, Achmad Miftah, and Novi Nur Indahsari. "Fungsi Hasil Laboratorium Forensik Sebagai Bukti Dalam Tindak Pidana Narkotika." *JURNAL USM LAW REVIEW* 7, no. 3 (December 22, 2024): 1911–11. https://doi.org/10.26623/julr.v7i3.10729.

Fauziyah, Rezza, Agus Raharjo, and Setya Wahyudi. "Efektivitas Penegakan Hukum Tindak Pidana Pemilu Melalui Media Sosial." *Syntax Literate ; Jurnal Ilmiah Indonesia* 10, no. 8 (August 15, 2025): 6642–54. https://doi.org/10.36418/syntax-literate.v10i8.61435.

Fernando, Dennis, Dini Dewi Heniarti, and Chepi Ali Firman Zakaria. "Transformasi Alat Bukti Elektronik Menggunakan Digital Forensik Dalam Pembaharuan Hukum Acara Pidana." *Journal Justiciabelen (JJ)* 5, no. 01 (January 31, 2025): 60. https://doi.org/10.35194/jj.v5i01.5506.

Ivanova, Malinka, and Svetlin Stefanov. "Digital Forensics Investigation Models: Current State and Analysis," June 20, 2023. https://doi.org/10.23919/splitech58164.2023.10193176.

Kassa, Yidnekachew Worku, Joshua Isaac James, and Elefelious Getachew Belay. "Intention Recognition for Digital Forensics: A Formal Model," February 11, 2025. https://doi.org/10.20944/preprints202502.0764.v1.

Lahangatubun, Nurjana , and Andi Muliyono. "Public Trust and the Legal Validity of Electronic Signatures in Indonesia." *JIHK* 7, no. 1 (June 27, 2025): 499–516. https://doi.org/10.46924/jihk.v7i1.311.

Lahati, Teddy. "Eksistensi Dan Peran Alat Bukti Elektronik Dalam Sistem Peradilan Di Indonesia." *Judex Laguens* 2, no. 1 (March 22, 2024): 97–107. https://doi.org/10.25216/ikahi.2.1.4.2024.97-107.

Nafish, Afrin , and A. Rengarajan. "The Effects of Technology Evolution on Cybercrime." *International Journal of Innovative Research in Computer and Communication Engineering* 12, no. 02 (February 25, 2024): 1060–66. https://doi.org/10.15680/ijircce.2024.1202056.

Satoto, Endro, and Faisal Santiago. "Reconstruction of Indonesia's Cyber Law System for Adaptive and Integrated Digital Crime Prevention in the Era of Technological Disruption." *Greenation International Journal of Law and Social Sciences* 3, no. 2 (June 18, 2025): 309–17. https://doi.org/10.38035/gijlss.v3i2.425.

Volume 12, Number 01, January-March 2026, Pages 281-288
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

Setiawan, Edwin, and Hartiwiningsih. "Optimizing the Use of Digital Forensics and Information Technology in Proving Criminal Acts of Electronic Document Forgery in Indonesia." *International Journal of Law, Crime and Justice* 2, no. 2 (May 14, 2025): 72–86. https://doi.org/10.62951/ijlcj.v2i2.587.

Sujatmiko, Bambang, and Bambang Soesatyo. "The Urgency of Using Electronic Evidence in Trials as an Effort to Answer the Challenges of Law Enforcement in the Digital Era and Social Media Dynamics." *Asian Journal of Social and Humanities* 3, no. 9 (June 20, 2025): 1604–13. https://doi.org/10.59888/ajosh.v3i9.567.

Sukmasari, Amelia, Wulanmas Frederik, Merry Elisabeth Kalalo, and Muhammad Herro Soepeno. "Application of Electronic Evidence as Extension of Legal Civil Evidence Divorce Cases in Indonesia." *International Journal of Law, Environment, and Natural Resources* 4, no. 1 (April 5, 2024): 1–14. https://doi.org/10.51749/injurlens.v4i1.95.

Thealma, Feby, and Yova Rudelviani. "Digital Forensic Ethical Data Handling in Indonesia." *The Indonesian Journal of Computer Science* 14, no. 1 (February 7, 2025). https://doi.org/10.33022/ijcs.v14i1.4588.

Wida, Ratu, and Subhandi Bakhtiar. "Peranan Metode Scientific Crime Investigation Melalui Ilmu Kedokteran Forensik Dalam Proses Pengungkapan Jenazah Di Pondok Gede Permai, Kota Bekasi." *Jurnal Hukum Dan Sosial Politik* 2, no. 4 (November 28, 2024): 123–30. https://doi.org/10.59581/jhsp-widyakarya.v2i4.4294