NEXUS RESEARCH PUBLISHING

Nexus of Justitia Law Review
Volume 1, Number 2, 2026
E-ISSN : 3124-0860
Open Access: https://journal.nexuspublishing.co.id/njlr

Digital Forensik dan Penegakan Hukum Siber di Indonesia (Analisis Tantangan dan Reformasi Prosedural)

Ahmad Iqbal [1], Aldi fachriansyah [2], Tavita Adinnia [3] Syarief hidayat [4], Supardi [5]
[1] Fakultas Hukum Universitas Pamulang Serang Banten Indonesia
[2] Fakultas Hukum Universitas Pamulang Serang Banten Indonesia
[3] Fakultas Hukum Universitas Pamulang Serang Banten Indonesia
[4] Fakultas Hukum Universitas Pamulang Serang Banten Indonesia
[5] Fakultas Hukum Universitas Pamulang Serang Banten Indonesia
Correspondence: iqbalahmad3144@gmail.com

iqbalahmad3144@gmail.com[1], auliaAldifachriansyah30@gmail.com[2], tavita240505@gmail.com[3]
syarifsh177@gmail.com[4], supardypardy776@gmail.com[5]

Article Info
Article history:
Received th, 2026
Revised th, 2026
Accepted , 2026

Keyword:
Digital Forensik; Penegakan Hukum Siber; Kekosongan Norma; Reformasi Prosedural; *Chain of Custody*.

ABSTRACT (10 PT)
Perkembangan teknologi keuangan digital telah melahirkan aset kripto (Perkembangan teknologi digital telah mentransformasi lanskap kejahatan global, menjadikan kejahatan siber sebagai ancaman serius bagi keamanan nasional dan stabilitas ekonomi Indonesia. Digital forensik, sebagai instrumen teknis sekaligus yuridis dalam pengungkapan kejahatan siber, menghadapi kompleksitas prosedural yang menghambat efektivitas penegakan hukum. Artikel ini bertujuan menganalisis tantangan normatif dan implementatif dalam penerapan digital forensik di Indonesia serta merumuskan reformasi prosedural yang diperlukan.
Penelitian ini menggunakan metode yuridis-normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Bahan hukum dianalisis secara kualitatif melalui interpretasi gramatikal, sistematis, dan teleologis terhadap peraturan perundang-undangan, putusan pengadilan, serta literatur ilmiah terkini.
Hasil penelitian menunjukkan bahwa meskipun pengakuan hukum terhadap bukti elektronik telah diperkuat melalui Undang-Undang Nomor 1 Tahun 2024 dan KUHAP baru (UU No. 20 Tahun 2025), masih terdapat kekosongan norma dalam standar prosedur digital forensik yang bersifat mengikat. Tantangan utama mencakup ketiadaan standar akuisisi data, mekanisme preservasi, metode analisis forensik, dan rantai penguasaan bukti (chain of custody) yang terstandar. Akibatnya, pembuktian perkara siber sangat bergantung pada interpretasi subjektif aparat dan ahli, berpotensi menimbulkan disparitas putusan dan ketidakpastian hukum. Artikel ini merekomendasikan pembentukan hukum acara digital forensik sebagai *lex specialis*, penguatan akreditasi laboratorium, sertifikasi ahli, serta harmonisasi regulasi sektoral untuk mewujudkan penegakan hukum siber yang akuntabel dan berkeadilan.

© 2026 The Authors. Published by PT Nexus Research Publishing. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)

PENDAHULUAN

Perkembangan teknologi digital yang eksponensial telah mengubah secara fundamental lanskap kehidupan manusia, menghadirkan paradoks antara kemajuan peradaban dan munculnya dimensi kejahatan baru yang melampaui batas-batas yurisdiksi nasional. Transformasi digital yang seharusnya menjadi katalis efisiensi dan konektivitas global justru melahirkan ruang siber yang rentan dieksploitasi oleh aktor-aktor jahat, menjadikan kejahatan siber (*cybercrime*) sebagai ancaman serius bagi keamanan nasional, stabilitas ekonomi, dan perlindungan hak-hak fundamental warga negara (Putra, 2024). Kompleksitas kejahatan siber semakin meningkat seiring dengan penggunaan teknik-teknik canggih

seperti enkripsi, anonimitas, jaringan lintas negara, dan penghapusan data secara sistematis, yang secara signifikan menyulitkan proses pengumpulan dan pembuktian alat bukti elektronik (Irawan, 2025).

Di tengah tantangan tersebut, digital forensik hadir sebagai bidang multidisiplin yang mengintegrasikan teknologi informasi dan ilmu forensik untuk mengidentifikasi, mengamankan, mengekstraksi, dan menganalisis bukti digital guna kepentingan proses peradilan (Sina, 2025). Peran digital forensik tidak sekadar teknis, melainkan substantif dalam menjamin keaslian, keutuhan, dan keterandalan data elektronik, serta menjembatani aspek teknis dan yuridis melalui keterangan ahli di persidangan (Prihatini, Sihombing & Nuraeni, 2026). Keberadaannya menjadi prasyarat mutlak karena bukti digital memiliki karakteristik yang berbeda secara fundamental dari bukti konvensional: bersifat tidak kasat mata (*intangible*), volatil (mudah hilang atau berubah), rentan terhadap manipulasi, dan sangat bergantung pada sistem serta infrastruktur tempat data tersebut disimpan (Setiawan & Hartiwiningsih, 2025). Tanpa proses forensik yang tepat, informasi elektronik berisiko kehilangan nilai pembuktiannya atau bahkan dinyatakan tidak sah di persidangan (Hariyanto & Kusumah, 2026).

Indonesia telah menunjukkan kemajuan dalam pengakuan normatif terhadap bukti elektronik melalui serangkaian pembaruan regulasi. Pengakuan terhadap informasi dan dokumen elektronik sebagai alat bukti yang sah telah ditegaskan melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang secara eksplisit memperluas rezim pembuktian dengan menempatkan bukti elektronik bukan sekadar sebagai pelengkap, melainkan sebagai perluasan alat bukti yang setara secara normatif dengan alat bukti dalam KUHAP (Bukian, Yasmiati & Fathullah, 2026). Reformasi lebih lanjut dilakukan melalui Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP baru), yang mengakui bukti elektronik sebagai alat bukti yang sah dengan syarat dapat diautentikasi dan diperoleh secara sah, serta memperkuat *exclusionary rule* dengan memberikan kewenangan kepada hakim untuk menolak bukti yang tidak autentik atau diperoleh secara melawan hukum (Hariyanto & Kusumah, 2026). Pengakuan normatif ini mencerminkan pergeseran paradigma penting bahwa kebenaran hukum tidak lagi semata-mata dibangun dari bukti fisik, tetapi juga dari data digital yang diperoleh melalui sistem elektronik yang sah (Budhijanto, 2026).

Namun, penguatan normatif ini menghadapi realitas kontradiktif di tingkat implementasi. Meskipun bukti elektronik diakui secara normatif, Indonesia masih menghadapi kesenjangan prosedural yang signifikan dalam kerangka hukum acara pidana (Bukian, Yasmiati & Fathullah, 2026). Aspek-aspek fundamental seperti standar akuisisi data, mekanisme preservasi, metode analisis forensik yang terstandar, serta pengaturan rantai penguasaan bukti (*chain of custody*) masih belum dirumuskan secara tegas dan mengikat dalam peraturan pelaksana (Prihatini, Sihombing & Nuraeni, 2026). Standar Nasional Indonesia (SNI) 27037:2014 yang mengatur pedoman identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital masih bersifat sukarela (*voluntary*) dan tidak memiliki kekuatan mengikat secara hukum, sehingga aparat penegak hukum di lapangan tidak memiliki pedoman prosedural yang baku dan seragam (Putra, 2024). Kekosongan norma (*rechtsvacuum*) ini memiliki implikasi serius, karena tanpa standar prosedural yang jelas, keabsahan bukti elektronik menjadi sangat bergantung pada interpretasi subjektif aparat penegak hukum dan otoritas keilmuan ahli digital forensik (Sina, 2025).

Kondisi ini telah terbukti menimbulkan masalah dalam praktik peradilan. Putusan Pengadilan Negeri Sidoarjo Nomor 488/Pid.B/2024/PN Sda yang menolak bukti elektronik karena ketiadaan standar autentikasi yang jelas menjadi contoh konkret betapa fatalnya konsekuensi dari ketiadaan regulasi prosedural yang komprehensif (Bukian, Yasmiati & Fathullah, 2026). Kasus pemalsuan dokumen elektronik di Pengadilan Tata Usaha Negara Jakarta pada tahun 2022 dan kasus kebocoran data Tokopedia pada tahun 2023 semakin menggambarkan bahwa tanpa prosedur forensik yang terstandar, bukti-bukti digital yang diajukan di persidangan rentan digugat dan bahkan ditolak karena dianggap tidak memenuhi standar ilmiah dan prosedural yang disyaratkan (Setiawan & Hartiwiningsih, 2025). Situasi ini, sebagaimana dianalisis oleh Bukian, Yasmiati dan Fathullah (2026), merupakan bentuk kelalaian negara (*staatsverzuim*) yang melanggar prinsip negara hukum (*rechtsstaat*)

sebagaimana diamanatkan dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Lebih jauh, praktik pembuktian yang sangat bergantung pada interpretasi subjektif berpotensi menimbulkan disparitas putusan antar pengadilan serta mengaburkan kepastian hukum dan perlindungan hak asasi manusia (Hariyanto & Kusumah, 2026).

Tantangan implementatif lainnya menyangkut kapasitas kelembagaan dan sumber daya manusia yang sangat terbatas. Data dari Asosiasi Forensik Digital Indonesia (AFDI) pada tahun 2023 menunjukkan bahwa hanya terdapat 147 ahli forensik digital bersertifikasi di Indonesia, jumlah yang sangat tidak seimbang dengan volume dan kompleksitas kejahatan siber yang terus meningkat setiap tahunnya (Prihatini, Sihombing & Nuraeni, 2026). Dari sisi infrastruktur, laboratorium forensik digital yang memadai masih sangat terbatas, baik dari sisi jumlah, akreditasi, maupun peralatan yang dimiliki, di mana percepatan akreditasi laboratorium-laboratorium forensik sesuai standar internasional ISO/IEC 17025 masih berjalan lambat (Sina, 2025). Keterbatasan ini berdampak pada kecepatan dan kualitas pemeriksaan teknis, sehingga penyidikan berisiko tertunda atau sangat bergantung pada ahli luar yang jumlahnya terbatas, yang pada akhirnya memperlemah posisi penuntut dalam membuktikan kasus kejahatan siber di pengadilan (Irawan, 2025).

Di tingkat yurisdiksi, karakter lintas batas ruang siber menimbulkan hambatan tambahan karena data atau server yang berada di luar negeri mensyaratkan mekanisme *Mutual Legal Assistance* (MLA) atau kerja sama internasional lain yang seringkali lambat karena perbedaan sistem hukum dan kendala diplomatik (Awaluddin, Amsori & Mulyana, 2024). Proses MLA yang panjang ini tidak hanya memperlambat waktu penanganan perkara, tetapi juga melemahkan kontinuitas pembuktian karena bukti digital bersifat volatil dan dapat hilang atau dimanipulasi dalam rentang waktu yang singkat (Putra, 2024). Upaya Indonesia untuk memperkuat ketahanan siber nasional melalui pembentukan Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) merupakan langkah strategis, namun draf RUU tersebut memunculkan kekhawatiran dari masyarakat sipil terkait potensi pengawasan lalu lintas internet yang berlebihan, ancaman terhadap hak privasi, dan pembatasan kebebasan berekspresi (Eu SEE, 2025). Hal ini mengindikasikan bahwa reformasi prosedural di bidang digital forensik harus diseimbangkan dengan perlindungan hak asasi manusia dan prinsip *due process of law*.

Di tengah dinamika ini, konflik dan ketidakharmonisan antar peraturan perundang-undangan semakin memperparah masalah. Terdapat ketegangan antara ketentuan UU ITE dan KUHAP baru dalam hal prosedur penyidikan dan pembuktian, di mana Pasal 43 UU ITE memberikan kewenangan luas kepada penyidik untuk mengakses sistem elektronik dan data digital tanpa batasan prosedural yang eksplisit dalam KUHAP baru (Bukian, Yasmiati & Fathullah, 2026). Konflik regulasi ini menciptakan ketidakpastian hukum bagi aparat penegak hukum di lapangan, yang seringkali dihadapkan pada pilihan sulit ketika harus menentukan prosedur penyidikan digital yang tepat karena tidak ada pedoman tunggal yang mengintegrasikan berbagai ketentuan yang saling tumpang tindih (Hariyanto & Kusumah, 2026). Selain itu, dalam konteks penanganan kejahatan sumber daya alam (SDA) yang memanfaatkan teknologi digital, terdapat konflik antara UU ITE dan undang-undang di bidang kehutanan, pertambangan, dan energi baru terbarukan (EBT), yang semakin menambah kompleksitas penegakan hukum (Ferdyan, 2026; Mahfud, 2021).

Berdasarkan latar belakang tersebut, artikel ini mengajukan pertanyaan penelitian: (1) Bagaimana pengaturan dan implementasi digital forensik dalam penegakan hukum siber di Indonesia? (2) Apa saja tantangan prosedural yang dihadapi dalam penerapan digital forensik di Indonesia? (3) Bagaimana reformasi prosedural yang diperlukan untuk mengoptimalkan peran digital forensik dalam penegakan hukum siber yang berkeadilan? Penelitian ini bertujuan untuk menganalisis secara kritis tantangan normatif dan implementatif dalam penerapan digital forensik di Indonesia, serta merumuskan rekomendasi reformasi prosedural yang komprehensif. Urgensi penelitian ini terletak pada kebutuhan mendesak untuk menjembatani kesenjangan antara pengakuan normatif bukti elektronik dan kebutuhan

akan standar prosedural yang baku, guna mewujudkan penegakan hukum siber yang akuntabel, adil, dan melindungi hak asasi manusia di era digital.

METODOLOGI

Penelitian ini menggunakan metode penelitian hukum normatif (*normative legal research*) dengan pendekatan yuridis-normatif. Metode ini dipilih karena fokus penelitian pada analisis norma hukum positif, asas-asas hukum, dan doktrin hukum yang berkaitan dengan digital forensik dan penegakan hukum siber di Indonesia (Bukian, Yasmiati & Fathullah, 2026). Pendekatan yang digunakan meliputi:

Pendekatan Perundang-undangan (*Statute Approach*) : Pendekatan ini digunakan untuk mengkaji secara mendalam peraturan perundang-undangan yang relevan dengan digital forensik dan penegakan hukum siber, termasuk Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP), Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 jo. Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana, serta peraturan pelaksana lainnya seperti Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2012 tentang Manajemen Penyidikan Tindak Pidana (Hariyanto & Kusumah, 2026). Analisis dilakukan untuk mengidentifikasi pengaturan, kekosongan norma (*rechtsvacuum*), dan ketidakharmonisan antar peraturan (Prihatini, Sihombing & Nuraeni, 2026).

Pendekatan Konseptual (*Conceptual Approach*) : Pendekatan ini digunakan untuk menganalisis konsep-konsep hukum dan doktrin yang relevan, seperti konsep alat bukti, sistem pembuktian, digital forensik, *chain of custody*, dan perlindungan hak asasi manusia dalam konteks penegakan hukum siber (Putra, 2024). Pendekatan ini memungkinkan peneliti untuk mengeksplorasi makna dan implikasi dari konsep-konsep tersebut dalam kerangka hukum Indonesia (Setiawan & Hartiwiningsih, 2025).

Pendekatan Kasus (*Case Approach*) : Pendekatan ini dilakukan dengan mengkaji putusan-putusan pengadilan yang relevan untuk memahami bagaimana bukti digital diperlakukan dalam praktik peradilan di Indonesia (Sina, 2025). Kasus yang dianalisis meliputi Putusan Pengadilan Negeri Sidoarjo Nomor 488/Pid.B/2024/PN Sda yang menolak bukti elektronik karena ketiadaan standar autentikasi, serta kasus pemalsuan dokumen elektronik di Pengadilan Tata Usaha Negara Jakarta pada tahun 2022 dan kasus kebocoran data Tokopedia pada tahun 2023 yang menggambarkan aplikasi praktis digital forensik di pengadilan Indonesia (Bukian, Yasmiati & Fathullah, 2026; Setiawan & Hartiwiningsih, 2025). Analisis kasus ini memberikan gambaran konkret tentang tantangan implementatif dalam pembuktian berbasis bukti digital (Hariyanto & Kusumah, 2026).

Bahan Hukum: Penelitian ini menggunakan tiga jenis bahan hukum. Pertama, bahan hukum primer, yaitu peraturan perundang-undangan dan putusan pengadilan yang memiliki kekuatan mengikat (Prihatini, Sihombing & Nuraeni, 2026). Kedua, bahan hukum sekunder, yaitu literatur hukum, artikel jurnal, buku teks, dan hasil penelitian yang relevan (Awaluddin, Amsori & Mulyana, 2024). Ketiga, bahan hukum tersier, yaitu kamus hukum dan ensiklopedia (Irawan, 2025). Bahan hukum dikumpulkan melalui studi kepustakaan (*library research*) dengan memanfaatkan sumber-sumber yang terbit dalam 7 tahun terakhir untuk memastikan aktualitas dan relevansi (Putra, 2024).

Teknik Analisis: Data dianalisis secara kualitatif menggunakan metode interpretasi hukum. Pertama, interpretasi gramatikal digunakan untuk memahami makna tekstual peraturan (Hariyanto & Kusumah, 2026). Kedua, interpretasi sistematis digunakan untuk memahami hubungan antar peraturan (Bukian, Yasmiati & Fathullah, 2026). Ketiga, interpretasi teleologis digunakan untuk memahami tujuan pembentukan peraturan (Setiawan & Hartiwiningsih, 2025). Analisis dilakukan secara preskriptif untuk memberikan rekomendasi kebijakan berdasarkan temuan penelitian (Sina,

2025). Validitas data dijamin melalui teknik triangulasi sumber, yaitu membandingkan dan mengkonfirmasi temuan dari berbagai sumber bahan hukum (Prihatini, Sihombing & Nuraeni, 2026).

HASIL DAN PEMBAHASAN

1. Pengakuan Normatif Bukti Digital dan Kesenjangan Prosedural

Perkembangan hukum positif Indonesia menunjukkan pengakuan yang semakin kuat terhadap bukti digital sebagai alat bukti yang sah dalam proses peradilan pidana (Prihatini, Sihombing & Nuraeni, 2026). Pengakuan ini diperkuat melalui dua instrumen legislatif utama: pertama, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang secara tegas mengakui informasi elektronik dan/atau dokumen elektronik beserta hasil cetaknya sebagai alat bukti hukum yang sah (Bukian, Yasmiati & Fathullah, 2026); kedua, reformasi KUHAP melalui Undang-Undang Nomor 20 Tahun 2025 yang memperluas rezim pembuktian dengan mengakui bukti elektronik bukan sekadar sebagai pelengkap, melainkan sebagai perluasan alat bukti yang setara secara normatif dengan alat bukti konvensional (Hariyanto & Kusumah, 2026). Pengakuan normatif ini mencerminkan kesadaran legislatif bahwa sistem peradilan pidana modern tidak dapat mengabaikan realitas digital yang telah merasuki hampir seluruh aspek kehidupan manusia (Setiawan & Hartiwiningsih, 2025).

Secara normatif, pengakuan ini menandai pergeseran paradigma penting dalam sistem pembuktian pidana Indonesia, di mana kebenaran hukum tidak lagi semata-mata dibangun dari bukti fisik, tetapi juga dari data digital yang diperoleh melalui sistem elektronik yang sah (Budhijanto, 2026). Pasal 235 ayat (3)-(5) KUHAP baru bahkan memperkuat *exclusionary rule* dengan memberikan kewenangan kepada hakim untuk menolak bukti yang tidak autentik atau diperoleh secara ilegal (Hariyanto & Kusumah, 2026). Pengaturan ini sejalan dengan perkembangan hukum acara pidana di negara-negara maju yang telah lebih dahulu mengakui bukti digital sebagai bagian integral dari sistem pembuktian (Putra, 2024). Namun, kemajuan normatif ini belum diiringi dengan konstruksi hukum acara yang sistematis dan terintegrasi, sehingga menimbulkan kesenjangan yang signifikan antara pengakuan normatif dan realitas implementatif (Sina, 2025).

Temuan penelitian mengungkapkan adanya kesenjangan prosedural yang signifikan dalam tiga lapisan. *Pertama,* kekosongan prosedur (*leemten*) dalam hal akuisisi data, mekanisme preservasi, metode analisis forensik, serta pengaturan rantai penguasaan bukti (*chain of custody*) yang belum dirumuskan secara tegas dan mengikat dalam kerangka hukum acara pidana (Bukian, Yasmiati & Fathullah, 2026). Standar Nasional Indonesia (SNI) 27037:2014 yang mengatur pedoman identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital masih bersifat sukarela (*voluntary*) dan tidak memiliki kekuatan mengikat secara hukum (Putra, 2024). Akibatnya, aparat penegak hukum di lapangan tidak memiliki pedoman prosedural yang baku dan seragam dalam menangani bukti digital (Irawan, 2025). *Kedua,* kekaburan norma (*vage normen*) dalam parameter autentikasi bukti digital sebagaimana diatur dalam Pasal 235 ayat (3) KUHAP baru, yang tidak memberikan pedoman teknis yang jelas bagi aparat penegak hukum di tingkat lapangan (Hariyanto & Kusumah, 2026). Ketidakjelasan parameter autentikasi ini menimbulkan interpretasi yang berbeda-beda di antara aparat penegak hukum, yang pada gilirannya menghasilkan perlakuan yang tidak seragam terhadap bukti digital di berbagai wilayah hukum (Prihatini, Sihombing & Nuraeni, 2026). *Ketiga,* disharmoni antara kewenangan luas yang diberikan oleh Pasal 43 UU ITE dengan ketiadaan pedoman teknis kepolisian yang memadai untuk melaksanakan kewenangan tersebut (Bukian, Yasmiati & Fathullah, 2026). Kewenangan yang luas tanpa diimbangi dengan pedoman operasional yang jelas berpotensi menimbulkan penyalahgunaan wewenang dan pelanggaran hak asasi manusia dalam proses penyidikan (Awaluddin, Amsori & Mulyana, 2024).

Implikasi dari kesenjangan ini sangat serius. Tanpa standar prosedural yang baku, praktik pembuktian perkara siber menjadi sangat bergantung pada interpretasi subjektif aparat penegak hukum dan otoritas keilmuan ahli digital forensik, bukan pada standar prosedural yang seragam (Sina, 2025). Hal ini berpotensi menimbulkan disparitas putusan yang signifikan antar pengadilan, mengaburkan kepastian hukum, dan bahkan dapat melanggar hak-hak tersangka atau terdakwa dalam memperoleh peradilan yang adil (*fair trial*) (Hariyanto & Kusumah, 2026). Lebih lanjut, ketergantungan pada interpretasi subjektif ini bertentangan dengan prinsip kepastian hukum (*rechtszekerheid*) yang merupakan salah satu pilar utama negara hukum (*rechtsstaat*) sebagaimana diamanatkan dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (Bukian, Yasmiati & Fathullah, 2026). Kondisi ini juga menciptakan ketidakadilan prosedural bagi para pihak yang berperkara, karena nasib suatu perkara dapat sangat bergantung pada kebijaksanaan subjektif aparat penegak hukum atau ahli yang menangani kasus tersebut (Putra, 2024).

2. Rantai Penguasaan Bukti (*Chain of Custody*): Pilar Integritas yang Terabaikan

Salah satu temuan paling kritis dalam penelitian ini adalah belum diaturnya secara komprehensif mekanisme rantai penguasaan bukti (*chain of custody*) digital dalam sistem hukum Indonesia (Prihatini, Sihombing & Nuraeni, 2026). *Chain of custody* merupakan rangkaian penguasaan dan pengelolaan bukti sejak ditemukan hingga diajukan di persidangan, yang menentukan validitas dan integritas pembuktian (Setiawan & Hartiwiningsih, 2025). Setiap gangguan terhadap rantai penguasaan ini dapat menurunkan atau bahkan menghilangkan nilai pembuktian bukti digital (Putra, 2024). Dalam konteks bukti fisik konvensional, *chain of custody* telah diatur secara relatif memadai melalui berbagai peraturan dan praktik kepolisian yang mapan (Irawan, 2025). Namun, untuk bukti digital yang memiliki karakteristik berbeda, pengaturan *chain of custody* masih sangat minim dan belum terintegrasi dalam kerangka hukum acara pidana (Sina, 2025).

Karakteristik bukti digital yang bersifat volatil (mudah hilang/berubah), tidak kasat mata, dan rentan terhadap manipulasi menjadikan *chain of custody* sebagai elemen yang lebih krusial dibandingkan dengan bukti fisik konvensional (Awaluddin, Amsori & Mulyana, 2024). Proses forensik digital yang baik menuntut pembuatan *forensic image* menggunakan teknologi *write-blocker* untuk mencegah perubahan data, perhitungan nilai *hash* (kode digital) untuk memverifikasi integritas data, serta dokumentasi *chain of custody* yang lengkap untuk menjamin keaslian dan keabsahan bukti elektronik di persidangan (Putra, 2024). Tanpa pengaturan operasional yang rinci dalam peraturan pelaksana, bukti digital rentan digugat di persidangan sehingga melemahkan posisi penuntut (Hariyanto & Kusumah, 2026). Ketiadaan standar prosedural yang baku dalam *chain of custody* digital menciptakan celah bagi pihak-pihak yang berkepentingan untuk mempertanyakan integritas bukti, yang pada akhirnya dapat menghambat proses peradilan dan mengurangi efektivitas penegakan hukum siber (Prihatini, Sihombing & Nuraeni, 2026).

Putusan Pengadilan Negeri Sidoarjo Nomor 488/Pid.B/2024/PN Sda yang menolak bukti elektronik karena ketiadaan standar autentikasi yang jelas menjadi contoh konkret betapa fatalnya konsekuensi dari ketiadaan regulasi *chain of custody* yang komprehensif (Bukian, Yasmiati & Fathullah, 2026). Kasus ini menunjukkan bahwa meskipun bukti digital diakui secara normatif, tanpa prosedur standar yang menjamin integritas dan keasliannya, bukti tersebut dapat ditolak oleh pengadilan (Setiawan & Hartiwiningsih, 2025). Kasus pemalsuan dokumen elektronik di Pengadilan Tata Usaha Negara Jakarta pada tahun 2022 dan kasus kebocoran data Tokopedia pada tahun 2023 semakin memperkuat temuan ini, di mana bukti-bukti digital yang diajukan di persidangan menghadapi gugatan serius terkait keaslian dan integritasnya karena kurangnya dokumentasi *chain of custody* yang memadai (Setiawan & Hartiwiningsih, 2025). Situasi ini, sebagaimana dianalisis oleh Bukian, Yasmiati dan Fathullah (2026), merupakan bentuk kelalaian negara (*staatsverzuim*) yang melanggar prinsip negara hukum (*rechtsstaat*) sebagaimana diamanatkan dalam Pasal 1 ayat (3) UUD 1945. Kelalaian negara ini tidak hanya merugikan para pihak yang berperkara, tetapi juga mencederai kepercayaan publik terhadap sistem peradilan pidana secara keseluruhan (Hariyanto & Kusumah, 2026).

Penelitian ini juga menemukan bahwa ketiadaan regulasi *chain of custody* yang mengikat menciptakan ketidakpastian hukum dan membuka peluang penyalahgunaan prosedural (Prihatini, Sihombing & Nuraeni, 2026). Dalam praktik, penegak hukum seringkali harus mengandalkan protokol internal kepolisian atau interpretasi ahli yang tidak seragam, yang dapat bervariasi antar wilayah hukum (Irawan, 2025). Kondisi ini diperparah oleh terbatasnya kapasitas laboratorium forensik digital yang terakreditasi dan kekurangan analis forensik yang bersertifikasi, sebagaimana dibahas pada sub-bab berikutnya (Putra, 2024). Akibatnya, kualitas penanganan *chain of custody* sangat bergantung pada kapasitas individu dan institusi yang menangani kasus, yang tidak jarang menghasilkan perlakuan yang tidak adil dan tidak konsisten terhadap para pihak yang berperkara (Sina, 2025). Ketiadaan standar *chain of custody* yang baku juga menghambat upaya penegakan hukum dalam kasus-kasus kejahatan siber yang melibatkan bukti digital dalam jumlah besar dan kompleks, karena setiap bukti digital memerlukan penanganan yang cermat dan terdokumentasi dengan baik untuk menjamin integritasnya di persidangan (Setiawan & Hartiwiningsih, 2025).

3. Kapasitas Kelembagaan dan Sumber Daya Manusia: Hambatan Implementatif

Tantangan implementatif digital forensik di Indonesia tidak hanya bersifat normatif, tetapi juga menyangkut kapasitas kelembagaan dan sumber daya manusia (SDM) yang sangat terbatas (Prihatini, Sihombing & Nuraeni, 2026). Temuan penelitian mengungkapkan bahwa Indonesia masih menghadapi kendala serius dalam hal infrastruktur forensik digital dan kompetensi SDM pendukungnya (Sina, 2025). Keterbatasan ini tidak hanya mempengaruhi kecepatan dan kualitas penanganan perkara siber, tetapi juga menimbulkan keraguan terhadap keandalan hasil analisis forensik yang dihasilkan (Putra, 2024). Dalam sistem peradilan pidana yang mengandalkan bukti ilmiah, kredibilitas temuan forensik sangat bergantung pada kompetensi analis dan kualitas laboratorium tempat analisis dilakukan (Irawan, 2025).

Data dari Asosiasi Forensik Digital Indonesia (AFDI) pada tahun 2023 menunjukkan bahwa hanya terdapat 147 ahli forensik digital bersertifikasi di Indonesia, jumlah yang sangat tidak seimbang dengan volume dan kompleksitas kejahatan siber yang terus meningkat setiap tahunnya (Prihatini, Sihombing & Nuraeni, 2026). Keterbatasan jumlah ahli ini berdampak pada kecepatan dan kualitas pemeriksaan teknis, sehingga penyidikan berisiko tertunda atau sangat bergantung pada ahli luar yang jumlahnya terbatas (Awaluddin, Amsori & Mulyana, 2024). Selain itu, belum adanya sistem sertifikasi yang terstandar dan diakui secara nasional menambah kompleksitas masalah, karena kualitas ahli forensik digital bisa sangat bervariasi tanpa adanya tolok ukur kompetensi yang jelas (Sina, 2025). Ketiadaan standar kompetensi yang baku juga menyulitkan hakim dalam menilai kredibilitas keterangan ahli di persidangan, karena tidak ada acuan objektif untuk mengukur keahlian seorang saksi ahli digital forensik (Setiawan & Hartiwiningsih, 2025). Kondisi ini semakin memperparah ketergantungan pada interpretasi subjektif yang telah diuraikan pada sub-bab sebelumnya.

Dari sisi infrastruktur, laboratorium forensik digital yang memadai masih sangat terbatas, baik dari sisi jumlah, akreditasi, maupun peralatan yang dimiliki (Putra, 2024). Akreditasi laboratorium forensik digital mengacu pada standar internasional ISO/IEC 17025, namun percepatan akreditasi laboratorium-laboratorium forensik di Indonesia masih berjalan lambat (Prihatini, Sihombing & Nuraeni, 2026). Laboratorium yang tidak terakreditasi akan menghasilkan temuan forensik yang secara ilmiah kurang dapat dipertanggungjawabkan dan berpotensi ditolak di persidangan karena tidak memenuhi standar ilmiah yang diakui (Bradley, 2025). Keterbatasan infrastruktur ini juga berdampak pada kemampuan Indonesia untuk menangani kasus-kasus kejahatan siber yang kompleks dan berskala besar, seperti serangan siber terhadap infrastruktur kritikal atau kasus kebocoran data massal yang melibatkan jutaan catatan data pribadi (Irawan, 2025). Tanpa laboratorium yang terakreditasi dan dilengkapi dengan peralatan canggih, analisis forensik terhadap bukti digital dalam jumlah besar menjadi sangat sulit dilakukan, dan hasil analisis yang dihasilkan mungkin tidak memenuhi standar ilmiah yang disyaratkan untuk pembuktian di pengadilan (Setiawan & Hartiwiningsih, 2025).

Temuan ini sejalan dengan penelitian lain yang mengidentifikasi bahwa efektivitas penegakan hukum sangat dipengaruhi oleh kualitas penanganan bukti digital, ketersediaan prosedur forensik terstandar, dan kolaborasi lintas sektor antar lembaga (Awaluddin, Amsori & Mulyana, 2024). Disparitas teknologi, kapasitas kelembagaan yang terbatas, dan kurangnya program pelatihan berkelanjutan secara signifikan mempengaruhi konsistensi dan akurasi hasil penyidikan (Prihatini, Sihombing & Nuraeni, 2026). Hambatan infrastruktur dan SDM ini pada akhirnya memperlemah posisi penuntut dalam membuktikan kasus kejahatan siber di pengadilan, karena bukti-bukti digital yang dikumpulkan mungkin tidak memenuhi standar ilmiah dan prosedural yang disyaratkan (Sina, 2025). Dalam jangka panjang, keterbatasan kapasitas kelembagaan dan SDM ini dapat menghambat upaya Indonesia untuk membangun sistem peradilan pidana yang modern dan efektif dalam menghadapi ancaman kejahatan siber yang semakin kompleks dan canggih (Putra, 2024). Oleh karena itu, penguatan kapasitas kelembagaan dan SDM menjadi prasyarat mutlak bagi reformasi digital forensik di Indonesia.

4. Konflik Regulasi dan Ketidakharmonisan Horizontal

Penelitian ini juga mengidentifikasi adanya konflik dan ketidakharmonisan antar peraturan perundang-undangan yang mengatur digital forensik dan penegakan hukum siber di Indonesia (Bukian, Yasmiati & Fathullah, 2026). Konflik regulasi ini terjadi dalam dua dimensi: pertama, antara UU ITE dengan undang-undang sektoral yang mengatur sumber daya alam dan perlindungan data; kedua, antara UU ITE dan KUHAP baru (Prihatini, Sihombing & Nuraeni, 2026). Ketidakharmonisan horizontal antar regulasi ini tidak hanya menciptakan kebingungan di kalangan aparat penegak hukum, tetapi juga membuka peluang bagi pihak-pihak yang berperkara untuk memanfaatkan celah hukum guna menghindari pertanggungjawaban pidana (Hariyanto & Kusumah, 2026). Dalam sistem hukum yang terintegrasi, harmonisasi antar peraturan merupakan prasyarat penting untuk menjamin kepastian hukum dan efektivitas penegakan hukum (Irawan, 2025).

Dalam konteks penanganan kejahatan sumber daya alam (SDA) yang memanfaatkan teknologi digital, terdapat konflik antara UU ITE dan undang-undang di bidang kehutanan, pertambangan, dan energi baru terbarukan (EBT) (Bukian, Yasmiati & Fathullah, 2026). Konflik ini menciptakan ketidakpastian hukum dan menyulitkan penegak hukum dalam menentukan dasar hukum yang tepat untuk menangani kasus-kasus kejahatan SDA yang melibatkan bukti digital, seperti *GPS tracking illegal logging* atau manipulasi data pertambangan (Mahfud, 2021). Ketiadaan harmonisasi antar regulasi sektoral ini merupakan salah satu faktor yang menyebabkan ketidakefektifan penegakan hukum dalam kasus-kasus kejahatan lingkungan berbasis digital (Ferdyan, 2026). Dalam praktiknya, aparat penegak hukum seringkali dihadapkan pada pilihan sulit antara menerapkan UU ITE atau undang-undang sektoral, yang masing-masing memiliki ketentuan prosedural dan sanksi yang berbeda (Bukian, Yasmiati & Fathullah, 2026). Ketidakpastian ini tidak hanya menghambat proses penegakan hukum, tetapi juga menciptakan celah bagi pelaku kejahatan untuk menghindari pertanggungjawaban pidana dengan memanfaatkan konflik regulasi yang ada (Irawan, 2025).

Selain itu, meskipun KUHAP baru (UU No. 20 Tahun 2025) telah mengakui bukti elektronik secara normatif, masih terdapat ketegangan antara ketentuan KUHAP dan UU ITE dalam hal prosedur penyidikan dan pembuktian (Hariyanto & Kusumah, 2026). Pasal 43 UU ITE memberikan kewenangan yang luas kepada penyidik untuk mengakses sistem elektronik dan data digital, namun KUHAP baru tidak secara eksplisit mengatur batasan-batasan prosedural dalam pelaksanaan kewenangan tersebut (Bukian, Yasmiati & Fathullah, 2026). Hal ini menimbulkan ketidakpastian mengenai apakah prosedur akuisisi data digital dalam UU ITE telah sejalan dengan prinsip-prinsip perlindungan hak asasi manusia dan *due process of law* yang dijamin dalam KUHAP (Prihatini, Sihombing & Nuraeni, 2026). Ketegangan antara kedua regulasi ini juga berpotensi menimbulkan pelanggaran hak-hak tersangka atau terdakwa, karena tidak ada pedoman yang jelas mengenai batasan-batasan kewenangan penyidik dalam mengakses data digital (Setiawan & Hartiwiningsih, 2025). Dalam konteks perlindungan data pribadi, konflik antara UU ITE dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

(UU PDP) semakin memperumit masalah, karena kedua regulasi ini memiliki pendekatan yang berbeda dalam mengatur akses dan penggunaan data pribadi untuk kepentingan penegakan hukum (Awaluddin, Amsori & Mulyana, 2024).

Konflik regulasi ini berimplikasi pada ketidakpastian hukum bagi aparat penegak hukum di lapangan. Penyidik kepolisian di tingkat resor (Polres) seringkali dihadapkan pada pilihan sulit ketika harus menentukan prosedur penyidikan digital yang tepat, karena tidak ada pedoman tunggal yang mengintegrasikan berbagai ketentuan yang saling tumpang tindih (Irawan, 2025). Pada akhirnya, ketidakharmonisan horizontal antar regulasi ini semakin memperparah masalah kekosongan prosedur dan disparitas penanganan perkara siber di berbagai wilayah hukum di Indonesia (Bukian, Yasmiati & Fathullah, 2026). Kondisi ini tidak hanya merugikan para pihak yang berperkara, tetapi juga menurunkan kepercayaan publik terhadap sistem peradilan pidana dalam menangani kejahatan siber (Hariyanto & Kusumah, 2026). Oleh karena itu, harmonisasi regulasi sektoral menjadi salah satu prioritas utama dalam reformasi prosedural digital forensik di Indonesia.

5. Dimensi Lintas Batas dan Kerja Sama Internasional

Karakter kejahatan siber yang melintasi batas-batas yurisdiksi nasional menambahkan dimensi kompleksitas tersendiri dalam penegakan hukum di Indonesia (Putra, 2024). Bukti digital seringkali berada di luar negeri, baik di server yang berlokasi di negara lain atau dikelola oleh penyedia layanan digital asing (Awaluddin, Amsori & Mulyana, 2024). Untuk mengakses dan memperoleh bukti tersebut, Indonesia memerlukan mekanisme *Mutual Legal Assistance* (MLA) atau kerja sama internasional lainnya yang seringkali berjalan lambat karena perbedaan sistem hukum dan kendala diplomatik (Irawan, 2025). Proses MLA yang panjang ini tidak hanya memperlambat waktu penanganan perkara, tetapi juga melemahkan kontinuitas pembuktian karena bukti digital bersifat volatil dan dapat hilang atau dimanipulasi dalam rentang waktu yang singkat (Prihatini, Sihombing & Nuraeni, 2026). Dalam kasus-kasus kejahatan siber yang melibatkan aktor lintas negara, seperti serangan *ransomware* atau pencurian data massal, proses MLA yang lambat dapat menjadi penghalang utama dalam upaya penegakan hukum yang efektif (Setiawan & Hartiwiningsih, 2025).

Upaya Indonesia untuk memperkuat ketahanan siber nasional melalui pembentukan Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) merupakan langkah strategis yang mencakup perlindungan infrastruktur informasi kritikal, penguatan ketahanan siber nasional, dan kerja sama internasional (Kompas.com, 2026). Namun, draf RUU KKS yang saat ini dalam proses pembahasan menimbulkan kekhawatiran dari masyarakat sipil karena dianggap lebih berorientasi pada keamanan negara ketimbang perlindungan hak-hak warga negara, dengan diperkenalkannya konsep "pengkhianatan digital" (*digital treason*) yang ancaman pidananya mencapai 20 tahun penjara (Eu SEE, 2025). Yang lebih kontroversial, RUU KKS memberikan peran investigasi kepada Tentara Nasional Indonesia (TNI) dalam penanganan ancaman siber, yang dikhawatirkan akan mengaburkan batas antara penegakan hukum sipil dan operasi militer, serta berpotensi mengancam hak-hak sipil dan kebebasan demokratis (Kompas.com, 2026). Kekhawatiran ini mencerminkan ketegangan antara kebutuhan keamanan nasional dan perlindungan hak asasi manusia, yang merupakan isu sentral dalam setiap upaya reformasi hukum di bidang siber (Putra, 2024).

Dari perspektif penegakan hukum siber yang efektif, kerja sama internasional menjadi suatu keharusan (Awaluddin, Amsori & Mulyana, 2024). Namun, kerja sama ini harus didasarkan pada prinsip saling menghormati kedaulatan hukum, perlindungan hak asasi manusia, dan standar prosedural yang disepakati bersama (Prihatini, Sihombing & Nuraeni, 2026). Indonesia perlu mendorong percepatan mekanisme MLA dan mengembangkan protokol teknis serta diplomasi siber yang cepat dan terstandarisasi dengan negara-negara mitra (Irawan, 2025). Pembentukan unit koordinasi nasional untuk penegakan hukum siber yang melibatkan kepolisian, kejaksaan, Kementerian Luar Negeri, BSSN, dan penyelenggara sistem elektronik (PSE) menjadi prasyarat operasional untuk menjamin akses

legal sekaligus meminimalkan risiko penyalahgunaan wewenang dalam penanganan kasus lintas batas (Setiawan & Hartiwiningsih, 2025). Selain itu, Indonesia juga perlu aktif dalam forum-forum internasional yang membahas kerja sama penegakan hukum siber, seperti ASEAN, INTERPOL, dan PBB, untuk memastikan bahwa kepentingan nasional terlindungi dalam setiap inisiatif kerja sama internasional di bidang siber (Putra, 2024).

6. Reformasi Prosedural yang Diperlukan

Berdasarkan analisis tantangan-tantangan yang telah diuraikan, penelitian ini merumuskan sejumlah rekomendasi reformasi prosedural yang komprehensif untuk mengoptimalkan peran digital forensik dalam penegakan hukum siber di Indonesia (Prihatini, Sihombing & Nuraeni, 2026). Reformasi ini mencakup aspek normatif, kelembagaan, dan kapasitas SDM yang saling terkait dan perlu diimplementasikan secara terintegrasi (Sina, 2025). Keberhasilan reformasi ini tidak hanya bergantung pada perubahan regulasi, tetapi juga pada komitmen politik, alokasi anggaran, dan perubahan budaya kerja di kalangan aparat penegak hukum (Putra, 2024). Dalam konteks ini, reformasi prosedural harus dipandang sebagai proses jangka panjang yang memerlukan evaluasi dan penyesuaian berkelanjutan sesuai dengan perkembangan teknologi dan dinamika kejahatan siber (Irawan, 2025).

Pertama, pembentukan hukum acara digital forensik yang bersifat *lex specialis*. Kebutuhan mendesak yang teridentifikasi dari penelitian ini adalah perumusan hukum acara digital forensik sebagai *lex specialis* yang secara tegas mengatur prosedur perolehan, pengamanan, analisis, dan penyajian bukti digital (Bukian, Yasmiati & Fathullah, 2026). Pengaturan ini penting untuk mengatasi kekosongan normatif yang selama ini menyebabkan keabsahan bukti elektronik sangat bergantung pada penilaian subjektif aparat penegak hukum dan keterangan ahli (Hariyanto & Kusumah, 2026). Hukum acara khusus ini harus mencakup standar prosedur operasional yang baku untuk setiap tahap digital forensik: identifikasi, pengumpulan, akuisisi, preservasi, analisis, dan presentasi (yang sering dikenal dengan model kerangka kerja forensik digital) dengan mengadopsi standar internasional seperti ISO/IEC 27037 dan menyesuaikannya dengan konteks hukum Indonesia (Putra, 2024). Selain itu, hukum acara ini juga harus mengatur mekanisme pengawasan dan akuntabilitas untuk memastikan bahwa setiap tahapan prosedural dilaksanakan dengan integritas dan sesuai dengan ketentuan yang berlaku (Setiawan & Hartiwiningsih, 2025).

Kedua, pengaturan *chain of custody* bukti digital yang bersifat wajib dan terstandarisasi. Penelitian ini menekankan perlunya pengaturan yang tegas mengenai rantai penguasaan bukti digital yang wajib didokumentasikan dan diverifikasi pada setiap tahap penanganan bukti, untuk menjamin keutuhan, keaslian, dan keterpercayaan data elektronik sepanjang proses peradilan pidana (Prihatini, Sihombing & Nuraeni, 2026). Pengaturan ini harus mencakup kewajiban penggunaan teknologi *write-blocker*, perhitungan dan pencatatan nilai *hash*, serta dokumentasi yang ketat mengenai setiap transfer, penyimpanan, dan akses terhadap bukti digital (Sina, 2025). Dengan adanya rantai penguasaan yang terdokumentasi dengan baik, integritas bukti dapat dipertanggungjawabkan di persidangan (Setiawan & Hartiwiningsih, 2025). Pengaturan *chain of custody* juga harus mencakup sanksi bagi pelanggaran prosedur yang dapat mengancam integritas bukti, serta mekanisme pemulihan jika terjadi pelanggaran (Hariyanto & Kusumah, 2026).

Ketiga, penguatan kapasitas laboratorium forensik digital dan percepatan akreditasi ISO/IEC 17025. Rekomendasi ini menyangkut peningkatan jumlah dan kualitas laboratorium forensik digital di seluruh Indonesia, serta percepatan akreditasi laboratorium-laboratorium tersebut sesuai dengan standar internasional ISO/IEC 17025 untuk menjamin kompetensi teknis dan hasil uji yang sah secara ilmiah (Bradley, 2025). Selain itu, diperlukan program sertifikasi bagi penyidik dan analis digital forensik yang diakui secara nasional untuk memastikan standar profesionalisme global, termasuk adopsi sertifikat internasional seperti CISSP (*Certified Information Systems Security Professional*) atau CISA (*Certified Information Systems Auditor*) untuk penanganan kasus yang melibatkan aktor lintas negara (Prihatini,

Sihombing & Nuraeni, 2026). Penguatan kapasitas ini harus didukung dengan alokasi anggaran yang memadai dan program pelatihan berkelanjutan bagi aparat penegak hukum di semua tingkatan (Irawan, 2025).

Keempat, harmonisasi regulasi sektoral dan koordinasi antar lembaga. Rekomendasi ini menekankan perlunya harmonisasi antara UU ITE, KUHAP baru, dan undang-undang sektoral lainnya untuk menghilangkan konflik dan tumpang tindih kewenangan, serta pembentukan unit koordinasi nasional untuk penegakan hukum siber yang melibatkan kepolisian, kejaksaan, BSSN, Kementerian Komunikasi dan Informatika, dan penyelenggara sistem elektronik (PSE) (Bukian, Yasmiati & Fathullah, 2026). Koordinasi yang efektif akan memastikan penanganan kasus siber yang terintegrasi dan menghindari tumpang tindih atau kelambanan prosedural (Hariyanto & Kusumah, 2026). Harmonisasi regulasi juga harus mencakup penyelarasan antara UU ITE dan UU PDP untuk memastikan bahwa akses terhadap data pribadi untuk kepentingan penegakan hukum dilakukan dengan tetap menghormati hak privasi warga negara (Awaluddin, Amsori & Mulyana, 2024).

Kelima, penguatan perlindungan data pribadi dan hak asasi manusia dalam proses forensik digital. Reformasi prosedural harus menyeimbangkan kebutuhan penegakan hukum dengan perlindungan hak privasi dan data pribadi warga negara (Prihatini, Sihombing & Nuraeni, 2026). Penyelidik harus memiliki dasar hukum yang jelas dan proporsional sebelum meminta akses data pribadi, dengan otorisasi prosedural, batasan waktu, dan dokumentasi akses (*access logs*) untuk menjaga akuntabilitas (Setiawan & Hartiwiningsih, 2025).

Penerapan prinsip *proportionality* dan *necessity* menjadi sangat penting untuk memastikan bahwa intervensi terhadap privasi hanya dilakukan sebatas yang diperlukan untuk kepentingan penegakan hukum (Sina, 2025). Kolaborasi terstruktur antara Kementerian Komunikasi dan Informatika, lembaga perlindungan data, BSSN, aparat penegak hukum, dan PSE menjadi prasyarat operasional untuk menjamin akses legal sekaligus meminimalkan risiko penyalahgunaan wewenang (Awaluddin, Amsori & Mulyana, 2024). Dalam jangka panjang, perlindungan hak asasi manusia dalam proses forensik digital harus menjadi bagian integral dari setiap upaya reformasi hukum di bidang siber, karena penegakan hukum yang efektif tidak boleh mengorbankan hak-hak fundamental warga negara (Putra, 2024).

KESIMPULAN

Penelitian ini menganalisis secara komprehensif tantangan dan reformasi prosedural dalam penerapan digital forensik untuk penegakan hukum siber di Indonesia. Berdasarkan analisis yang telah dilakukan, dapat ditarik beberapa kesimpulan penting.

Pertama, sistem hukum acara pidana Indonesia masih berada dalam fase transisional dalam menghadapi dinamika kejahatan berbasis teknologi yang terus berkembang. Meskipun pengakuan normatif terhadap bukti elektronik telah ditegaskan melalui pembaruan UU ITE (UU No. 1 Tahun 2024) dan KUHAP baru (UU No. 20 Tahun 2025), penguatan normatif tersebut belum sepenuhnya diiringi dengan konstruksi hukum acara yang sistematis dan terintegrasi. Aspek-aspek fundamental seperti standar akuisisi data, mekanisme preservasi, metode analisis forensik, serta pengaturan chain of custody masih belum dirumuskan secara tegas dan mengikat dalam kerangka hukum acara pidana. Kekosongan norma ini memiliki implikasi serius, termasuk penolakan bukti elektronik di persidangan (sebagaimana terjadi dalam Putusan PN Sidoarjo) dan ketidakpastian hukum yang merugikan semua pihak.

Kedua, tantangan implementatif digital forensik di Indonesia bersifat multidimensi, meliputi: (1) terbatasnya jumlah dan kualitas SDM forensik digital (hanya 147 ahli bersertifikasi pada tahun 2023); (2) infrastruktur laboratorium forensik yang terbatas dan belum terakreditasi sesuai ISO/IEC 17025; (3) konflik dan ketidakharmonisan antar regulasi (UU ITE, KUHAP, dan undang-undang sektoral); (4) karakter lintas batas kejahatan siber yang memerlukan mekanisme MLA yang seringkali lambat; serta (5) ketiadaan standar prosedur operasional yang baku untuk penanganan bukti digital. Akibatnya,

praktik pembuktian perkara siber di Indonesia masih sangat bergantung pada interpretasi subjektif aparat penegak hukum dan otoritas keilmuan ahli digital forensik, bukan pada standar prosedural yang seragam, berpotensi menimbulkan disparitas putusan dan mengancam kepastian hukum.

Ketiga, reformasi prosedural yang komprehensif dan terintegrasi menjadi kebutuhan mendesak. Penelitian ini merekomendasikan lima pilar reformasi: (1) pembentukan hukum acara digital forensik sebagai lex specialis yang mengatur secara rinci seluruh tahapan prosedural; (2) pengaturan chain of custody bukti digital yang bersifat wajib dan terstandarisasi; (3) penguatan kapasitas laboratorium forensik digital dan percepatan akreditasi; (4) harmonisasi regulasi sektoral dan koordinasi antar lembaga; serta (5) penguatan perlindungan data pribadi dan hak asasi manusia dalam proses forensik digital. Reformasi ini harus diimplementasikan secara paralel dan berkelanjutan untuk menjembatani kesenjangan antara pengakuan normatif dan realitas implementatif.

Keempat, digital forensik tidak lagi dapat dipandang sekadar sebagai instrumen teknis pendukung, melainkan sebagai elemen sentral dalam sistem pembuktian pidana modern yang memerlukan pengaturan khusus dan komprehensif. Tanpa reformasi prosedural yang memadai, Indonesia akan terus menghadapi kesulitan dalam menegakkan hukum terhadap kejahatan siber yang semakin kompleks, yang pada akhirnya dapat mengancam keamanan nasional, stabilitas ekonomi, dan perlindungan hak-hak warga negara di era digital. Keberhasilan implementasi digital forensik tidak hanya bergantung pada regulasi yang kuat, tetapi juga pada komitmen kolektif untuk mengadopsi praktik terbaik global (global best practices), pengembangan kapasitas kelembagaan, dan penegakan prinsip-prinsip perlindungan hak asasi manusia serta due process of law.

DAFTAR PUSTAKA

A. Peraturan Perundang-undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (Kitab Undang-Undang Hukum Acara Pidana).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Nomor 4843).

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Nomor 5952).

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6958).

Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 170, Tambahan Lembaran Negara Nomor 6839).

Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 14 Tahun 2012 tentang Manajemen Penyidikan Tindak Pidana.

Peraturan Menteri Komunikasi dan Informatika Nomor 7 Tahun 2016 tentang Tata Kelola dan Pengawasan Sistem Elektronik.

Surat Edaran Mahkamah Agung Nomor 1 Tahun 2026 tentang Pedoman Pemberlakuan KUHAP Baru.

Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016.

Putusan Pengadilan Negeri Sidoarjo Nomor 488/Pid.B/2024/PN Sda.

B. Buku dan Artikel Jurnal

Awaluddin, F., Amsori, & Mulyana, M. (2024). Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital. *HUMANIORUM*, 2(1), 14–19.

Bradley, C. (2025). Comprehensive Guide to ISO/IEC 17025 Accreditation Prep for Forensic Labs. *Lab Manager*.

Budhijanto, D. (2026). Digital Evidence di Era AI dan Sistem Pembuktian Terbuka dalam KUHAP Baru. *Hukumonline*.

Bukian, P. K. K. P., Yasmiati, N. L. W., & Fathullah, S. K. R. (2026). Kekosongan Norma Digital Forensik dalam Penanganan Kejahatan Sumber Daya Alam (SDA): Analisis Tanggung Jawab Konstitusional Negara Pasca UU 1/2024. *Aliansi: Jurnal Hukum, Pendidikan dan Sosial Humaniora*, 3(3).

Ferdyan, D. T. (2026). To crack down on illegal logging and comply with EUDR rules, documentation alone is not enough. *World Resources Institute*.

Hariyanto, Y., & Kusumah, H. A. (2026). Kepastian Hukum dan Efektivitas Pembuktian Digital dalam Penyidikan Online Fraud: Analisis Normatif Pasal 235 KUHAP Baru dan Implementasinya di Polres Cimahi. *Mahkamah: Jurnal Riset Ilmu Hukum*, 3(3), 116–125.

Irawan, D. (2025). Tinjauan Yuridis Terhadap Tindak Pidana Siber. *Jurnal Litbang Polri*, 28(2), 138–152.

Mahfud, M. (2021). Satellite Image Data as Environmental Crime Evidence in the Field of Illegal Logging. *Fiat Justisia: Jurnal Ilmu Hukum*, 15(3), 269–286.

Prihatini, L., Sihombing, L. A., & Nuraeni, Y. (2026). Optimizing Digital Forensics for Effective Cybercrime Law Enforcement in Indonesia. *Law Development Journal*, 8(2).

Putra, G. R. A. (2024). Peran Forensik Digital dalam Mengungkap Kejahatan Siber: Tantangan Prosedural dan Kebutuhan Standardisasi di Indonesia. *Adalah: Jurnal Hukum dan Keadilan*, 8(7).

Setiawan, E., & Hartiwiningsih, H. (2025). 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(2), 72–86.

Sina, M. I. (2025). *Fungsional Digital Forensik dalam Tahap Penyidikan Tindak Pidana Cybercrime* [Tesis Magister, Universitas Islam Sultan Agung].

C. Sumber Lain

Eu SEE. (2025, November 23). Draft Cybersecurity and Cyber Resilience Bill signals further militarization of digital space. *Eu SEE*.

Kompas.com. (2026, Juni 30). Draf RUU Keamanan dan Ketahanan Siber di DPR Tertutup dari Publik, Kenapa? *Kompas.com*.