Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 2, 2026
DOI: https://doi.org/10.61104/alz.v4i2.4827

Kedudukan Hukum Sistem Elektronik dalam *Digital Forensik* Berdasarkan Undang-Undang Nomor 1 Tahun 2023 tentang KUHP

Yevi Mulyana Erawan[1], Novayandra Arinurdin[2], Edy Santoso[3], Dhanang Widijawan[4]
Magister Ilmu Hukum Universitas Langlangbuana, Bandung, Indonesia[1-3]
Email Korespondensi: yevimulyanae@gmail.com

Article received: 01 Januari 2026, Review process: 12 Januari 2026
Article Accepted: 22 Februari 2026, Article published: 01 Maret 2026

ABSTRACT
The development of information technology has brought fundamental changes in the character and modus operandi of criminal acts, especially cyber crimes that make electronic systems as means and objects of crime. This condition has a direct impact on criminal law enforcement practices, especially in the use of digital evidence and the application of digital forensic examinations as part of the evidentiary process. Law Number 1 of 2023 concerning the Criminal Code (New Criminal Code) establishes a new material criminal legal framework, but it has not explicitly regulated the legal position of electronic systems and the results of digital forensic examinations as evidence in cybercrime cases. This article aims to analyze the legal position of electronic systems in forensic digital examination of cyber crimes based on the New Criminal Code, as well as its relationship with the recognition of electronic evidence in other laws and regulations, especially the Electronic Information and Transaction Law. The research method used is normative juridical with a regulatory approach and a conceptual approach. The results of the study show that the New Criminal Code provides a normative space for technology-based criminal law enforcement, but the recognition and legal position of electronic systems in forensic digital examinations are still highly dependent on special arrangements regarding electronic evidence and the provisions of criminal procedural law. Therefore, harmonization of regulations is needed to ensure legal certainty and the effectiveness of proving cybercrimes in the digital era.
Keywords: *New Criminal Code, Digital Forensics, Cybercrime.*

ABSTRAK
Perkembangan teknologi informasi telah membawa perubahan mendasar dalam karakter dan modus operandi tindak pidana, khususnya tindak pidana siber yang menjadikan sistem elektronik sebagai sarana maupun objek kejahatan. Kondisi tersebut berdampak langsung pada praktik penegakan hukum pidana, terutama dalam penggunaan bukti digital dan penerapan pemeriksaan digital forensik sebagai bagian dari proses pembuktian. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Baru) menetapkan kerangka hukum pidana materiil yang baru, namun belum mengatur secara eksplisit mengenai kedudukan hukum sistem elektronik dan hasil pemeriksaan digital forensik sebagai alat bukti dalam perkara pidana siber. Artikel ini bertujuan untuk menganalisis kedudukan hukum sistem elektronik dalam pemeriksaan digital forensik terhadap tindak pidana siber berdasarkan KUHP Baru, serta keterkaitannya dengan pengakuan alat bukti elektronik dalam peraturan perundang-undangan lainnya, khususnya

Undang-Undang Informasi dan Transaksi Elektronik. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan peraturan perundang-undangan dan pendekatan konseptual. Hasil penelitian menunjukkan bahwa KUHP Baru memberikan ruang normatif bagi penegakan hukum pidana berbasis teknologi, namun pengakuan dan kedudukan hukum sistem elektronik dalam pemeriksaan digital forensik masih sangat bergantung pada pengaturan khusus mengenai alat bukti elektronik dan ketentuan hukum acara pidana. Oleh karena itu, diperlukan harmonisasi pengaturan guna menjamin kepastian hukum dan efektivitas pembuktian tindak pidana siber di era digital.
Kata Kunci: *KUHP Baru, Digital Forensik, Tindak Pidana Siber*

PENDAHULUAN

Teknologi digital telah menjadi bagian yang tidak terpisahkan dari kehidupan modern (Apdillah et al., 2022). Hampir setiap aktivitas sosial, ekonomi, dan bahkan hukum kini memanfaatkan sistem elektronik dan teknologi informasi. Transformasi ini membawa banyak kemudahan, namun juga membuka celah bagi munculnya berbagai bentuk kejahatan baru yang dikenal dengan istilah *cybercrime*. Kejahatan siber ini bukan sekadar pelanggaran hukum konvensional yang dilakukan secara online, tetapi juga menimbulkan tantangan baru dalam hal bukti dan pembuktian di pengadilan.

Kejahatan berbasis teknologi dapat mencakup berbagai tindakan, mulai dari penipuan digital, penggelapan elektronik, peretasan sistem, hingga penyebaran konten ilegal secara online (Setiawan, 2024). Dalam banyak kasus, jejak digital menjadi bukti utama yang dapat digunakan untuk mengungkap fakta hukum. Namun, bukti digital ini berbeda dengan bukti fisik tradisional karena sifatnya yang mudah dimanipulasi, tersebar dalam jaringan, dan sering memerlukan keahlian khusus untuk diekstraksi serta dianalisis.

Di sinilah peran *digital forensic* menjadi sangat penting. *Digital forensic* merupakan disiplin yang berkaitan dengan identifikasi, pengumpulan, pelestarian, analisis, dan penyajian bukti digital agar dapat digunakan secara sah dalam proses hukum (Mursyid et al., 2025). Proses ini tidak hanya menekankan aspek teknis, tetapi juga memperhatikan prosedur hukum agar hasil analisis dapat diterima oleh pengadilan. Dengan kata lain, *digital forensic* menjadi jembatan antara dunia teknologi dan hukum.

Namun, dari perspektif hukum materiil Indonesia, UU Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Baru) belum secara spesifik memuat ketentuan mengenai sistem elektronik atau *digital forensic*. KUHP Baru lebih menekankan pada jenis-jenis tindak pidana, ancaman hukuman, dan asas pidana secara umum (Kholik & Zulfaidah, 2025). Hal ini menimbulkan pertanyaan tentang bagaimana kedudukan hukum sistem elektronik dalam proses pembuktian tindak pidana berbasis teknologi (Hasnawati & Safrin, 2023).

Ketiadaan regulasi eksplisit dalam KUHP Baru terkait sistem elektronik dan *digital forensic* membuat aparat penegak hukum harus merujuk pada regulasi lain yang mengatur alat bukti elektronik. Salah satu regulasi utama adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang secara normatif mengakui informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah

dalam hukum pidana (Kholik & Sulastri, 2025). UU ITE menjadi payung hukum yang menguatkan posisi bukti digital di pengadilan, memberikan landasan bagi penggunaan *digital forensic*.

UU ITE menjelaskan bahwa dokumen elektronik dan hasil cetaknya memiliki kekuatan hukum yang setara dengan alat bukti tradisional seperti dokumen fisik, keterangan saksi, dan keterangan ahli. Dengan demikian, *digital forensic* tidak hanya bersifat teknis, tetapi juga memiliki relevansi hukum yang kuat, asalkan proses pengumpulannya memenuhi standar autentikasi, integritas, dan *chain of custody*. Hal ini penting agar bukti elektronik tidak ditolak oleh pengadilan.

Meskipun pengakuan bukti elektronik dalam UU ITE telah memberikan kepastian hukum, praktik di lapangan tetap menghadapi tantangan. Pertama, diperlukan kompetensi khusus dari penyidik untuk mengumpulkan dan menganalisis data digital. Kedua, perangkat hukum lain seperti KUHAP perlu menyesuaikan prosedur pembuktian agar bukti digital dapat diterima secara sah. Ketiga, masih ada ketidakpastian mengenai bagaimana KUHP Baru mengakomodir tindak pidana yang secara spesifik menggunakan sistem elektronik sebagai sarana atau objek kejahatan.

Dalam konteks global, banyak negara telah memasukkan aturan *digital forensic* dan bukti elektronik ke dalam sistem hukum pidana mereka secara eksplisit. Hal ini menunjukkan pentingnya harmonisasi antara hukum materiil dan hukum acara pidana. Indonesia, dengan KUHP Baru dan UU ITE, berada di jalur yang sama, tetapi masih memerlukan pedoman teknis yang lebih rinci agar *digital forensic* dapat diterapkan secara efektif (Bakhtiar et al., 2025).

Beberapa pakar menekankan bahwa *digital forensic* bukan sekadar alat teknis, tetapi merupakan bagian dari strategi penegakan hukum yang lebih luas. Dengan kemampuan untuk mengungkap fakta hukum secara akurat, *digital forensic* membantu mengurangi kesalahan dalam proses peradilan, memperkuat bukti, dan mempercepat penegakan hukum. Oleh karena itu, peran *digital forensic* sangat relevan dalam tindak pidana berbasis teknologi yang terus berkembang.

Selain itu, sistem elektronik juga menjadi sumber data yang sangat kaya, mulai dari log server, metadata, hingga transaksi digital. Data ini bisa digunakan untuk membangun kronologi peristiwa, memverifikasi keterangan saksi, dan mengidentifikasi pelaku kejahatan. Namun, untuk menjadikan data ini sah sebagai bukti hukum, prosedur pengumpulan dan analisis harus mengikuti standar hukum dan etika yang berlaku.

Tantangan lain adalah sinkronisasi antara KUHP Baru dan hukum acara pidana terbaru (KUHAP 2025). KUHAP mengatur mekanisme pembuktian, termasuk penerimaan bukti elektronik di pengadilan. Agar *digital forensic* dapat diterima sebagai alat bukti yang sah, prosedur teknis pengumpulan data harus sesuai dengan ketentuan hukum acara, seperti persyaratan autentikasi dan perlindungan integritas bukti.

Dengan demikian, kedudukan hukum sistem elektronik dalam *digital forensic* bukan hanya masalah teknis, tetapi juga masalah normatif yang melibatkan harmonisasi beberapa regulasi. KUHP Baru memberikan landasan untuk tindak pidana berbasis teknologi, UU ITE mengatur alat bukti elektronik, dan KUHAP

menetapkan prosedur pembuktian. Ketiganya perlu dipahami secara menyeluruh oleh aparat penegak hukum.

Sejumlah penelitian menunjukkan bahwa pengakuan alat bukti elektronik meningkatkan efektivitas penegakan hukum dalam kasus kejahatan siber. *Digital forensic* memungkinkan aparat hukum mengungkap fakta yang sebelumnya sulit diakses dengan metode konvensional. Dengan demikian, *digital forensic* menjadi instrumen strategis dalam mendukung prinsip keadilan dan kepastian hukum. Meski begitu, masih diperlukan regulasi pendukung yang lebih jelas terkait standar *digital forensic*, termasuk sertifikasi alat dan personel, metodologi analisis, dan pedoman pelaporan. Regulasi semacam ini akan meminimalkan risiko penolakan bukti di pengadilan dan memperkuat legitimasi *digital forensic* sebagai alat pembuktian hukum.

Dalam konteks Indonesia, tantangan ini semakin penting karena kejahatan siber terus meningkat, baik dari segi volume maupun kompleksitas. Penegakan hukum yang efektif membutuhkan pemahaman mendalam tentang teknologi, prosedur hukum, dan metode forensik digital yang sesuai standar internasional. Selain itu, *digital forensic* juga membantu mencegah pelanggaran hukum yang lebih besar dengan membangun bukti yang akurat dan dapat diandalkan. Bukti elektronik yang sah dapat memutus rantai kejahatan digital dan memberikan efek jera bagi pelaku.

Kehadiran *digital forensic* juga memunculkan diskusi etis dan legal mengenai privasi, hak atas data, dan batasan pengawasan elektronik. Hal ini menunjukkan bahwa hukum pidana modern harus mampu menyeimbangkan kepentingan penegakan hukum dengan perlindungan hak individu.

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam pola kejahatan, khususnya melalui munculnya berbagai bentuk tindak pidana siber yang menjadikan sistem elektronik sebagai sarana, objek, maupun target kejahatan. Dalam konteks ini, sistem elektronik tidak lagi sekadar alat bantu, melainkan memiliki kedudukan strategis dalam pembuktian tindak pidana melalui pemeriksaan digital forensik. Kehadiran Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Baru) mempertegas perluasan ruang lingkup perbuatan pidana yang berkaitan dengan teknologi informasi, sehingga menuntut kejelasan mengenai kedudukan hukum sistem elektronik dalam proses penegakan hukum pidana.

Oleh karena itu, penelitian mengenai kedudukan hukum sistem elektronik dalam pemeriksaan digital forensik menjadi penting untuk dikaji secara mendalam, khususnya dalam kerangka penerapan KUHP Baru. Penelitian ini menelaah pengakuan hukum terhadap sistem elektronik dan hasil pemeriksaan digital forensik sebagai alat bukti, mekanisme serta prosedur penggunaannya dalam proses penyidikan hingga persidangan, serta berbagai tantangan normatif dan praktis yang dihadapi dalam implementasinya di pengadilan.

Lebih lanjut, kajian ini bertujuan memberikan pemahaman yang komprehensif mengenai keterkaitan antara KUHP Baru, Undang-Undang Informasi dan Transaksi Elektronik, serta praktik digital forensik dalam sistem pembuktian hukum pidana. Dengan demikian, penelitian ini diharapkan mampu merumuskan

rekomendasi yang konstruktif guna meningkatkan efektivitas penegakan hukum pidana terhadap tindak pidana siber di era digital.

Berdasarkan kajian literatur, pengakuan terhadap sistem elektronik dan informasi elektronik sebagai alat bukti telah mengalami perkembangan signifikan dalam sistem hukum pidana Indonesia. Undang-Undang Informasi dan Transaksi Elektronik memberikan dasar normatif bahwa informasi elektronik dan/atau dokumen elektronik beserta hasil cetaknya merupakan alat bukti hukum yang sah, sepanjang memenuhi persyaratan keandalan sistem dan keabsahan proses perolehannya. Hal ini menjadi landasan penting bagi penggunaan hasil pemeriksaan digital forensik dalam mengungkap tindak pidana siber.

Penelitian yang dilakukan oleh Edmon Makarim menegaskan bahwa kekuatan pembuktian bukti elektronik sangat bergantung pada terpenuhinya prinsip keotentikan, integritas, dan ketersediaan data elektronik, yang hanya dapat dibuktikan melalui mekanisme digital forensik yang akuntabel. Menurutnya, sistem elektronik harus dipahami sebagai entitas hukum yang memiliki konsekuensi yuridis, baik sebagai sarana kejahatan maupun sebagai objek pembuktian dalam proses peradilan pidana.

Selain itu, kajian oleh Barda Nawawi Arief menekankan bahwa pembaruan hukum pidana, termasuk melalui KUHP Baru, harus mampu merespons perkembangan kejahatan berbasis teknologi dengan menyesuaikan konsep pertanggungjawaban pidana dan sistem pembuktian. Dalam konteks ini, penguatan kedudukan sistem elektronik dan hasil pemeriksaan digital forensik menjadi bagian dari modernisasi hukum pidana untuk menjamin efektivitas penegakan hukum dan kepastian hukum.

Sementara itu, penelitian oleh Sigid Suseno menunjukkan bahwa praktik digital forensik di Indonesia masih menghadapi berbagai tantangan, antara lain keterbatasan regulasi teknis, perbedaan standar pemeriksaan, serta kapasitas aparat penegak hukum dalam memahami bukti elektronik. Kondisi tersebut berpotensi menimbulkan perbedaan penilaian hakim terhadap kekuatan pembuktian hasil digital forensik di persidangan.

Dengan demikian, kajian literatur menunjukkan bahwa meskipun sistem elektronik dan digital forensik telah memperoleh pengakuan normatif, masih diperlukan harmonisasi pengaturan antara KUHP Baru, UU ITE, dan hukum acara pidana agar kedudukan hukum sistem elektronik dalam pemeriksaan digital forensik memiliki kepastian, konsistensi, dan daya guna dalam penanganan tindak pidana siber.

METODE

Penelitian ini merupakan penelitian hukum normatif dengan pendekatan kepustakaan (*library research*) (Soekanto, 2001), karena objek kajiannya berupa norma hukum dan konsep yang mengatur Kedudukan Hukum Sistem Elektronik dalam *Digital Forensik* Berdasarkan Undang-Undang Nomor 1 Tahun 2023 tentang KUHP. Pendekatan yang digunakan meliputi pendekatan peraturan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan peraturan perundang-undangan digunakan untuk menganalisis pengaturan sistem

elektronik dan alat bukti elektronik dalam KUHP Baru, Undang-Undang Informasi dan Transaksi Elektronik, serta hukum acara pidana. Sementara itu, pendekatan konseptual digunakan untuk mengkaji konsep digital forensik, sistem elektronik, dan pembuktian pidana dalam perspektif hukum pidana modern. Bahan hukum terdiri atas bahan hukum primer berupa peraturan perundang-undangan terkait, dan bahan hukum sekunder berupa buku, jurnal ilmiah, serta artikel akademik yang relevan. Analisis bahan hukum dilakukan secara kualitatif dengan metode deskriptif-analitis untuk menelaah keterkaitan antarregulasi dan menarik kesimpulan preskriptif mengenai kedudukan hukum sistem elektronik dalam pembuktian tindak pidana siber.

HASIL DAN PEMBAHASAN

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Baru) memberikan landasan yang lebih progresif dan memperkuat posisi sistem elektronik beserta dokumen elektronik sebagai alat bukti yang sah dalam pemeriksaan tindak pidana siber. Dalam konteks hukum acara pidana, hasil pemeriksaan digital forensik terhadap sistem elektronik seperti data biner, *log file, email,* atau catatan transaksi berkedudukan setara dengan alat bukti konvensional (Anam, 2022). Penggunaan digital forensik dalam kerangka KUHP 2023 menjadi fondasi sentral untuk menjamin integritas, otentikasi, dan rantai penahanan (*chain of custody*) bukti digital yang rentan berubah.

Lebih lanjut, sistem elektronik dalam pemeriksaan forensik digital tidak hanya berfungsi sebagai "barang bukti" fisik (perangkat keras), tetapi berkedudukan sebagai "alat bukti" yang sah, yaitu perluasan dari jenis alat bukti surat dan keterangan ahli sebagaimana diatur dalam Pasal 184 KUHAP, yang kini disempurnakan dalam kodifikasi baru untuk mengakomodasi kejahatan berbasis teknologi. Oleh karena itu, prosedur digital forensik yang memenuhi standar ilmiah dan hukum (melalui metode autentikasi dan integritas data) menjadikan sistem elektronik sebagai bukti utama yang diakui dalam pembuktian modern untuk mengungkapkan tindak pidana siber.

Dalam sistem hukum pidana Indonesia, validitas bukti elektronik termasuk hasil *digital forensic* perlu dirujuk pada kerangka hukum yang lebih luas daripada sekadar Kitab Undang-Undang Hukum Pidana (KUHP). KUHP Baru (UU No. 1 Tahun 2023) memberikan landasan normatif terhadap delik pidana, tetapi tidak secara spesifik memuat definisi atau ketentuan rinci tentang sistem elektronik maupun *digital forensic* sebagai alat bukti (Djibu et al., 2025). Hal ini menunjukkan bahwa KUHP Baru lebih berfungsi sebagai pengatur materi delik, sedangkan mekanisme pembuktian, termasuk kehadiran bukti elektronik, sering kali diatur dalam undang-undang lain dan hukum acara pidana.

Salah satu regulasi yang paling relevan adalah *Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)* yang secara tegas mengakui informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah dalam proses pemeriksaan perkara pidana. Ketentuan UU ITE mempertegas bahwa bukti yang diperoleh melalui sistem elektronik memiliki kekuatan hukum setara dengan alat bukti lain jika memenuhi persyaratan autentikasi, integritas data, dan relevansi terhadap fakta hukum yang

dibuktikan (Hasnawati & Safrin, 2023). Hal ini menjadi landasan hukum yang kuat bagi penerimaan bukti digital yang diperoleh melalui *digital forensic* dalam praktik peradilan.

Berbeda dengan KUHP Baru, UU ITE memiliki fokus normatif yang lebih spesifik terhadap alat bukti elektronik. Menurut Hasnawati dan Safrin, kedudukan alat bukti elektronik dalam pembuktian tindak pidana di Indonesia telah diatur dalam UU ITE dan memberi kepastian bahwa data digital dapat digunakan sebagai alat bukti, asalkan sesuai dengan standar teknik pembuktian yang berlaku. Kekhususan ini menunjukkan bahwa sistem hukum Indonesia telah mengakui sifat unik dari bukti digital dan kebutuhan untuk mengakomodasi jenis bukti baru yang dihasilkan oleh sistem elektronik.

Dalam praktiknya, aparat penegak hukum dan peradilan di Indonesia mengevaluasi bukti digital melalui pendekatan yang mempertimbangkan aspek teknis dan hukum. Misalnya, *digital forensic* dituntut untuk menjaga agar data yang diambil dari sistem elektronik tetap orisinal dan tidak mengalami perubahan (*unaltered*). Ketentuan mengenai *chain of custody* yang jelas sangat penting untuk memastikan bahwa bukti digital yang disajikan di pengadilan tidak kehilangan integritasnya sejak awal pengambilan hingga saat pembuktian. Ini menjadi salah satu prasyarat yang harus dipenuhi agar bukti digital diterima sebagai bukti yang sah.

Walaupun KUHP Baru tidak memuat definisi istilah "sistem elektronik" dan "*digital forensic*", asas umum dalam hukum pidana tetap berlaku, yaitu kepastian hukum (*legal certainty*) dan asas legalitas (*nullum crimen sine lege*). Kedua asas ini mendorong interpretasi hukum yang menempatkan sistem elektronik sebagai bagian integral dari pembuktian kejahatan yang terjadi di ruang siber, sepanjang didukung oleh aturan lain yang lebih spesifik. Dalam hal ini, UU ITE serta hukum acara pidana menjadi penopang penting untuk kedudukan hukum bukti digital.

Dalam kajian internasional, studi yuridis menunjukkan bahwa peran *digital forensic* dalam proses peradilan pidana global semakin diakui, dan pengakuan tersebut memperkuat urgensi pembentukan aturan yang lebih rinci terkait pembuktian digital. Di beberapa sistem hukum lain, bukti digital sering diperlakukan sebagai alat bukti yang memiliki syarat admissibility tersendiri, termasuk kriteria validitas, keterkaitan, dan keandalan teknis. Model-model seperti ini dapat menjadi referensi untuk meningkatkan kerangka hukum di Indonesia dalam memadukan KUHP Baru dengan aturan pembuktian digital yang lebih komprehensif (Hardinanto et al., 2023).

Sejalan dengan itu, integrasi *digital forensic* dalam proses pembuktian pidana memicu kebutuhan untuk memperkuat kapasitas aparat hukum baik penyidik, penuntut umum, maupun hakim dalam memahami karakteristik bukti elektronik. Tanpa pemahaman yang memadai, ada risiko bahwa bukti digital yang sebenarnya kuat secara teknis justru diabaikan atau dinilai kurang relevan karena persoalan prosedural.

Selain itu, masih terdapat tantangan normatif lain yang perlu diperhatikan, seperti harmonisasi antara KUHP Baru, UU ITE, dan hukum acara pidana (misalnya KUHAP yang baru diberlakukan) (Kholik et al., 2025). Ketidakharmonisan

antarregulasi ini dapat menciptakan kekosongan hukum (*legal lacuna*) yang membingungkan penerapan hukum di tingkat penyidikan dan peradilan (Kholik et al., 2026). Oleh karena itu, sinkronisasi aturan dan pedoman teknis khusus tentang bukti digital dan *digital forensic* menjadi kebutuhan mendesak.

Banyak akademisi menekankan bahwa *digital forensic* tidak hanya sekadar alat bantu teknis, tetapi merupakan bagian dari proses pembuktian modern yang harus diakui secara hukum secara lebih eksplisit. Bukti digital yang dihasilkan lewat *digital forensic* sering kali menjadi bukti kunci dalam kasus kejahatan siber, seperti penipuan elektronik, peretasan sistem, dan pencurian data, sehingga ketentuan hukum yang mengaturnya harus memiliki dasar yang kuat dan jelas di ranah hukum pidana.

Dalam konteks KUHP Baru, meskipun tidak terdapat pasal yang secara tegas mengatur *digital forensic*, prinsip umum pembuktian tetap membuka ruang bagi bukti digital selama memenuhi kriteria sah alat bukti sesuai dengan ketentuan hukum lain yang berlaku. Hal ini berarti sistem elektronik dan bukti hasil *digital forensic* diakui dalam praktik peradilan sepanjang didukung oleh pengaturan lain seperti UU ITE dan hukum acara pidana (Romadhoni et al., 2025).

Dengan demikian, kedudukan hukum sistem elektronik dalam *digital forensic* berada pada posisi yang terintegrasi namun tidak tersendiri dalam KUHP Baru: KUHP Baru memberi ruang normatif untuk tindak pidana teknologi, sementara bukti digital dan hasil *digital forensic* diatur melalui peraturan lain yang lebih khusus. Pendekatan ini masih perlu didukung oleh harmonisasi aturan dan pemahaman aparat hukum untuk menjamin efektivitas pembuktian pidana di era digital.

Sistem elektronik kini memiliki kedudukan yang signifikan dalam proses peradilan pidana modern karena teknologi digital semakin banyak digunakan dalam interaksi manusia sehari-hari. Secara historis, bukti dalam hukum pidana berasal dari barang bukti fisik, saksi, atau dokumen tertulis; namun dengan berkembangnya teknologi informasi, bukti digital menjadi instrumen penting dalam mengungkap fakta hukum. Di Indonesia, pengakuan hukum terhadap sistem elektronik sebagai sumber bukti tidak berdiri sendiri dalam KUHP Baru (UU No. 1 Tahun 2023), tetapi secara eksplisit diberikan melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). UU ITE menetapkan bahwa "informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya" merupakan bukti yang sah di muka pengadilan, sehingga memberikan legitimasi bagi penggunaan bukti yang berasal dari sistem elektronik (Abdullah et al., 2023).

Pengakuan hukum ini penting karena bukti digital yang dihasilkan melalui berbagai perangkat teknologi seperti pesan elektronik, log jaringan, metadata, atau file digital lain berbeda karakter dengan bukti konvensional. Bukti digital mudah berubah bentuk, tersebar pada berbagai lokasi penyimpanan, dan memerlukan penanganan khusus agar tidak kehilangan integritasnya. Oleh karena itu, metode *digital forensic* dipandang sebagai proses ilmiah yang sistematis dalam mengidentifikasi, menyelamatkan, mengumpulkan, menganalisis, dan menyajikan bukti digital yang berasal dari sistem elektronik, sehingga tetap dapat diterima dan dihargai secara hukum.

Dalam kajian hukum Indonesia, *digital forensic* bukan hanya prosedur teknis tetapi juga memiliki substansi hukum karena menjadi prasyarat agar bukti digital yang ditemukan dapat dianggap sah. Penelitian menunjukkan bahwa melalui *digital forensic*, autentikasi, integritas, dan relevansi bukti dapat dipastikan sehingga data digital tidak hanya dipandang sebagai indikasi semata tetapi juga alat bukti yang dapat memengaruhi putusan hakim (Hardinanto et al., 2023). Hal ini semakin memperkuat posisi bukti elektronik di ranah pembuktian pidana, meskipun KUHP Baru tidak secara eksplisit mengatur metode ini.

Secara yuridis, pengakuan sistem elektronik dan *digital forensic* berakar pada interpretasi undang-undang yang saling melengkapi. UU ITE memberikan dasar normatif bagi bukti elektronik, sementara hukum acara pidana termasuk pasal terkait penerimaan alat bukti dalam KUHAP menjadi mekanisme operasional untuk menguji keabsahan bukti tersebut di persidangan. Meski ada perbedaan ketentuan antara hukum pidana materiil (KUHP Baru) dan hukum acara, pengakuan hukum terhadap *digital forensic* mencerminkan perkembangan sistem hukum yang responsif terhadap perubahan teknologi.

Peranan *digital forensic* dalam memperkuat bukti elektronik juga dibahas dalam literatur hukum yang lebih luas, yang menegaskan bahwa prosedur standar *digital forensic* membantu pengadilan dalam memastikan bahwa bukti yang diajukan memang berasal dari sistem elektronik yang autentik, bebas dari kontaminasi, dan dapat dijadikan dasar keputusan yang adil. Di tingkat praktik, bukti digital hasil *digital forensic* telah diterima dalam berbagai putusan perkara cybercrime, menunjukkan bahwa secara nyata sistem peradilan menghargai bukti elektronik yang diproses secara profesional (Hidayatullah et al., 2026).

Pengakuan hukum terhadap *digital forensic* tidak hanya tampak dalam aturan formal, tetapi juga memperlihatkan tren global di mana negara lain, seperti di Malaysia, telah mengintegrasikan prinsip-prinsip *digital forensic* dalam sistem pembuktian mereka. Studi internasional menegaskan bahwa *digital forensic* memperkuat kualitas bukti elektronik dengan memastikan keaslian, integritas, dan nilai probatifnya, sehingga mendukung prinsip keadilan dan kepastian hukum dalam pengadilan (Alias et al., 2025). Meskipun konteks yurisdiksi berbeda, prinsip ini memberikan gambaran bahwa *digital forensic* diakui secara luas sebagai bagian dari sistem pembuktian modern yang efektif.

Tingkat pengakuan hukum ini juga menimbulkan tuntutan terhadap kemampuan aparat hukum untuk memahami dan menerapkan *digital forensic* secara tepat. Kualitas implementasi menjadi kunci agar bukti elektronik yang dihasilkan dari sistem elektronik tidak hanya diakui di tingkat norma, tetapi juga dapat dipertanggungjawabkan secara substansial di depan persidangan.

Namun, tetap ada tantangan dalam penerapan *digital forensic* sebagai alat bukti, termasuk kebutuhan akan standar prosedur yang jelas, pembentukan pedoman teknis, dan peningkatan kapabilitas sumber daya manusia yang menangani bukti digital. Dengan kondisi ini, pengakuan hukum terhadap sistem elektronik dan *digital forensic* harus dilihat sebagai proses yang masih berkembang, namun telah menegaskan keberadaannya dalam kerangka hukum Indonesia (Zulfaidah et al., 2026).

Secara keseluruhan, pengakuan hukum terhadap sistem elektronik dan *digital forensic* menunjukkan bahwa bukti digital bukan sekadar fakta teknis, tetapi juga memiliki kedudukan hukum yang kuat apabila prosedurnya dilakukan sesuai dengan standar normatif dan hukum acara yang berlaku.

Penggunaan sistem elektronik dan *digital forensic* dalam proses hukum pidana tidak bersifat sembarangan, melainkan mengikuti prosedur yang telah diakui baik secara hukum maupun praktik forensik. Prosedur ini penting untuk memastikan bahwa bukti digital yang diperoleh sah, valid, dan dapat diterima di pengadilan.

Secara garis besar, prosedur penggunaan *digital forensic* mencakup (Liu, 2007) :

1. Identifikasi Bukti Digital

Langkah pertama adalah identifikasi jenis bukti digital yang relevan dengan tindak pidana. Sistem elektronik yang berbeda mulai dari komputer, ponsel, server, hingga media penyimpanan cloud dapat menyimpan informasi berbeda. Identifikasi ini menentukan metode pengumpulan yang tepat dan mencegah hilangnya data kritis. Misalnya, log transaksi elektronik dapat digunakan sebagai bukti dalam kasus penipuan digital, sedangkan metadata file dapat digunakan untuk membuktikan keaslian dokumen elektronik.

2. Pengamanan dan Pelestarian Bukti

Setelah identifikasi, bukti digital harus diamankan agar integritasnya terjaga. *Digital forensic* menekankan perlunya prosedur *chain of custody*, yakni dokumentasi yang memastikan setiap langkah penanganan bukti dicatat secara lengkap dan akurat. Tujuannya adalah mencegah kontaminasi atau manipulasi data sehingga bukti tetap sah untuk dipresentasikan di pengadilan. Pengamanan bukti digital sering dilakukan dengan menyalin data menggunakan metode *forensic imaging* yang menghasilkan salinan identik tanpa merusak data asli.

3. Pengumpulan Bukti

Pengumpulan bukti digital dilakukan sesuai dengan prosedur hukum yang berlaku, termasuk izin penyidik dan persetujuan hakim jika diperlukan. Dalam konteks Indonesia, prosedur pengumpulan bukti elektronik harus mengacu pada UU ITE dan KUHAP, agar bukti yang diperoleh tidak batal demi hukum. Metode pengumpulan meliputi ekstraksi data dari perangkat elektronik, pengambilan snapshot sistem, serta pengunduhan file yang relevan dengan tindak pidana yang sedang diselidiki.

4. Analisis Bukti Digital

Analisis bukti merupakan tahap inti dari *digital forensic*. Di sini, penyidik atau ahli *digital forensic* menelaah data untuk menemukan jejak tindak pidana, pola aktivitas, atau bukti keterlibatan tersangka. Analisis ini harus dilakukan dengan standar ilmiah dan terdokumentasi dengan jelas. Misalnya, pemeriksaan log transaksi online harus menunjukkan korelasi waktu, identitas pengguna, dan aktivitas digital yang relevan.

5. Dokumentasi dan Pelaporan

Setiap langkah penggunaan *digital forensic* harus terdokumentasi secara lengkap. Laporan *digital forensic* menjadi dokumen hukum yang menyertai bukti elektronik di persidangan. Laporan ini memuat metode pengambilan data, analisis

yang dilakukan, serta kesimpulan sementara mengenai relevansi bukti terhadap tindak pidana. Dokumentasi yang lengkap memastikan bahwa bukti digital dapat diuji kembali jika diperlukan oleh pihak pengadilan atau ahli lain.

6. Presentasi Bukti di Pengadilan

Bukti yang telah dianalisis disajikan di persidangan oleh penyidik atau ahli *digital forensic*. Presentasi harus menjelaskan bagaimana data diperoleh, proses analisis, dan kesimpulan yang relevan secara hukum. Pihak pengadilan kemudian menilai sah atau tidaknya bukti berdasarkan integritas data, relevansi, dan kepatuhan terhadap prosedur hukum.

Secara keseluruhan, prosedur penggunaan sistem elektronik dan *digital forensic* menekankan prinsip autentikasi, integritas, relevansi, dan transparansi**.** Prosedur ini menggabungkan standar teknis dan hukum untuk memastikan bahwa bukti digital memiliki kekuatan hukum yang sama dengan bukti konvensional. Implementasi prosedur yang konsisten juga memperkuat kredibilitas aparat hukum dan kepercayaan publik terhadap penegakan hukum berbasis teknologi.

Meskipun sistem elektronik dan *digital forensic* telah diakui secara hukum, implementasinya di pengadilan masih menghadapi berbagai tantangan signifikan. Tantangan ini bersifat normatif, teknis, dan prosedural**,** yang memengaruhi sejauh mana bukti digital dapat diterima dan digunakan secara efektif dalam proses peradilan pidana, tantangan antara lain (El-Latif et al., 2024):

1. Kekosongan dan Ambiguitas Hukum

Salah satu tantangan utama adalah ketidakjelasan pengaturan KUHP Baru terkait bukti digital. KUHP Baru (UU No. 1 Tahun 2023) tidak secara eksplisit mengatur prosedur *digital forensic* maupun validitas sistem elektronik sebagai alat bukti. Hal ini menuntut hakim, jaksa, dan penyidik untuk merujuk pada UU ITE atau hukum acara pidana (KUHAP), sehingga menimbulkan potensi perbedaan interpretasi di berbagai pengadilan. Kekosongan hukum ini dapat menyebabkan inkonsistensi dalam penerimaan bukti digital, misalnya dalam kasus peretasan atau penipuan elektronik.

2. Kompetensi Aparat Hukum

Tantangan kedua terkait dengan kompetensi teknis aparat hukum**.** Penyidik, penuntut umum, dan hakim seringkali memiliki pemahaman terbatas mengenai karakteristik bukti digital dan prosedur *digital forensic*. Akibatnya, bukti digital yang sebenarnya kuat secara teknis dapat dianggap tidak sah karena prosedur pengumpulan atau analisisnya dianggap kurang memenuhi standar hukum. Keterbatasan ini menuntut pelatihan khusus agar aparat hukum mampu menilai keaslian, integritas, dan relevansi bukti digital secara tepat.

3. Kompleksitas Bukti Digital

Bukti digital memiliki sifat kompleks dan mudah dimanipulasi**.** Data yang tersebar di berbagai perangkat atau server, enkripsi, dan log yang sulit diakses menjadi hambatan dalam membuktikan keterkaitan antara bukti dan tersangka. Dalam banyak kasus, proses *digital forensic* harus melibatkan ahli bersertifikat untuk memastikan integritas bukti dan menghindari tuduhan manipulasi. Hal ini menambah biaya dan waktu dalam proses peradilan.

4. Standar Prosedur yang Belum Merata

Di pengadilan, belum semua prosedur *digital forensic* diatur secara baku atau seragam. Ketidakteraturan ini dapat menimbulkan perbedaan praktik antarpenyidik atau antarpengadilan. Misalnya, penggunaan *forensic imaging*, dokumentasi *chain of custody*, dan metode analisis bukti digital tidak selalu konsisten. Ketidakseragaman ini berpotensi melemahkan kredibilitas bukti digital di mata hakim.

5. Tantangan Etis dan Privasi

Selain aspek teknis dan hukum, pengumpulan bukti digital juga menghadapi tantangan etis dan privasi. Data digital sering kali memuat informasi pribadi yang sensitif. Penyadapan atau ekstraksi data elektronik harus dilakukan sesuai hukum dan etika, agar tidak melanggar hak privasi warga negara. Di pengadilan, pertentangan antara kebutuhan pembuktian dan hak privasi sering menjadi isu yang kompleks.

6. Perbedaan Pemahaman antara Pengadilan Nasional dan Standar Internasional

Di tingkat internasional, prosedur *digital forensic* sering mengacu pada standar internasional yang ketat terkait keabsahan bukti digital. Perbedaan ini dapat menimbulkan kesenjangan antara praktik di Indonesia dan praktik internasional, khususnya dalam kasus lintas batas negara atau tindak pidana siber yang melibatkan server asing. Harmonisasi standar prosedur *digital forensic* menjadi tantangan penting agar bukti digital yang dihasilkan tetap dapat diterima secara internasional.

SIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana telah membuka ruang bagi penegakan hukum pidana yang responsif terhadap perkembangan teknologi informasi, termasuk tindak pidana siber. Namun demikian, KUHP Baru belum mengatur secara eksplisit mengenai kedudukan hukum sistem elektronik dan hasil pemeriksaan digital forensik sebagai alat bukti dalam pembuktian pidana. Kedudukan hukum sistem elektronik dalam pemeriksaan digital forensik terhadap tindak pidana siber masih bertumpu pada pengaturan khusus dalam Undang-Undang Informasi dan Transaksi Elektronik serta ketentuan hukum acara pidana. Oleh karena itu, hasil pemeriksaan digital forensik hanya memiliki kekuatan pembuktian sepanjang memenuhi prinsip keotentikan, integritas, dan keandalan sistem elektronik. Dengan demikian, diperlukan harmonisasi pengaturan antara KUHP Baru, Undang-Undang Informasi dan Transaksi Elektronik, dan hukum acara pidana guna memberikan kepastian hukum serta meningkatkan efektivitas pembuktian tindak pidana siber di era digital.

DAFTAR RUJUKAN

Abdullah, R. A. F., Mayasari, A., & Mirzana, H. A. (2023). Digital Forensic Urgence in Analyzing Electronic Evidence for Evidence of Criminal Actions in Information and Electronic Transactions. *Journal of Development Research*, *7*(2), 264–271. https://doi.org/10.28926/jdr.v7i2.238

Alias, M. A. A., Ismail, W. A. F. W., Baharuddin, A. S., Hashim, H., & Ibrahim, T. M. F. H. T. (2025). DIGITAL FORENSICS AND THE ADMISSIBILITY OF ELECTRONIC EVIDENCE IN MALAYSIAN SYARIAH COURTS: TOWARDS A STANDARDISED LEGAL FRAMEWORK. *LexForensica: Journal of Forensic Justice and Socio-Legal Research*, *2*(1), 84–91. https://doi.org/10.33102/6grx4619

Anam, M. K. (2022). *Eksistensi Perundang-Undangan Terhadap Digital Forensik Dalam Sistem Pembuktian Pidana*. https://dspace.uii.ac.id/handle/123456789/40791

Apdillah, D., Zebua, R. B., Idham, M., & Anhar, I. (2022). TEKNOLOGI DIGITAL DI DALAM KEHIDUPAN MASYARAKAT. *Selodang Mayang: Jurnal Ilmiah Badan Perencanaan Pembangunan Daerah Kabupaten Indragiri Hilir*, *8*(2), 101–107. https://doi.org/10.47521/selodangmayang.v8i2.247

Bakhtiar, Handar Subhandi, Ilyas, A., Kholiq, A., & Bakhtiar, Handina Sulastrina. (2025). The utilisation of scientific crime investigation methods and forensic evidence in the criminal investigation process in Indonesia. *Egyptian Journal of Forensic Sciences*, *15*(1), 39. https://doi.org/10.1186/s41935-025-00456-y

Djibu, M. A., Ismail, D. E., & Mustika, W. (2025). Implikasi Pengaturan Ilmu Forensik dalam KUHP lama dan Baru terhadap Kepastian dan Keadilan Hukum Pidana Anak. *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, *3*(5), 8004–8019. https://doi.org/10.61104/alz.v3i5.2475

El-Latif, A. A. A., Tawalbeh, L., Mohanty, M., Gupta, B. B., & Psannis, K. E. (2024). *Digital Forensics and Cyber Crime Investigation: Recent Advances and Future Directions*. CRC Press.

Hardinanto, A., Arief, B. N., & Setiyono, J. (2023). The Significance of Computer Forensics in Electronic Documents as Evidence in Criminal Law. *Jurnal Cakrawala Hukum*, *14*(2), 155–166. https://doi.org/10.26905/idjch.v14i2.10820

Hasnawati, H., & Safrin, M. (2023). Kedudukan Alat Bukti Elektronik dalam Pembuktian Tindak Pidana. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, *5*(2), 1207–1214. https://doi.org/10.37680/almanhaj.v5i2.2878

Hidayatullah, R. F., Yusuf, M., & Hermawan. (2026). Pengalaman Praktisi Digital Forensik dalam Penerapan Chain of Custody Bukti Digital di Indonesia. *INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer*, *1*(03). https://portalpublikasi.com/index.php/inomatec/article/view/980

Kholik, M. A., Islam, M. H., Saepullah, U., & Ridwan, A. H. (2025). POSITIVISME HUKUM SEBAGAI DASAR PENJATUHAN PIDANA: ANALISIS PUTUSAN NOMOR 11/PID.B/2025/PN CKR TENTANG TINDAK PIDANA TURUT SERTA MELAKUKAN PEMBUNUHAN BERENCANA. *Jurnal Media Akademik (JMA)*, *3*(12), 1–20. https://doi.org/10.62281/fh4ch693

Kholik, M. A., & Sulastri, D. (2025). Social Engineering Through Criminal Law: The Effectiveness of the ITE Law in Shaping Digital Communication in Indonesia. *Ius Poenale*, *6*(2), 101–112. https://doi.org/10.25041/ip.v6i2.4741

Kholik, M. A., & Zulfaidah, R. (2025). Pergeseran Fungsi Hukum Pidana dalam Sistem Ketatanegaraan Indonesia: Dari Ultimum Remedium ke Political Control. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, *3*(4), 4078–4091. https://doi.org/10.62976/ijijel.v3i4.1670

Kholik, M. A., Zulfaidah, R., & Hakim, S. M. F. (2026). Konstitusionalitas Penerapan Sanksi Pidana terhadap Kebijakan Publik yang Berimplikasi Pidana. *Interdisciplinary Explorations in Research Journal*, *4*(1), 71–88. https://doi.org/10.62976/ierj.v4i1.1709

Liu, J. (2007). Computer Forensics: Principles and Practices. *The Journal of Digital Forensics, Security and Law: JDFSL*, *2*(3), 57.

Mursyid, M., Putera, A., & Jannah, M. (2025). Rekonstruksi Peran Digital Forensik Dalam Penyidikan Tindak Pidana Siber: Analisis Kritis Terhadap Konstruksi Hukum Pidana di Indonesia. *Jurnal Tana Mana*, *6*(2), 289–296. https://doi.org/10.33648/jtm.v6i2.1194

Romadhoni, K., Rosidin, U., Kholik, M. A., & Alifi, A. (2025). Urgensi Pembaharuan Hukum melalui Pendekatan Ius Constitutum dan Ius Constituendum pada Tindak Pidana dalam Kegiatan Bisnis di Indonesia. *AL-MUTSLA*, *7*(2), 678–711. https://doi.org/10.46870/jstain.v7i2.1953

Setiawan, D. A. (2024). STRATEGI PENANGGULANGAN KEJAHATAN EKONOMI BERBASIS TEKNOLOGI: STUDI KOMPARATIF ANTARA INDONESIA, AMERIKA, DAN EROPA. *Masalah-Masalah Hukum*, *53*(1), 78–89. https://doi.org/10.14710/mmh.53.1.2024.78-89

Soekanto, S. (2001). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Raja Grafindo Persada.

Zulfaidah, R., Kholik, M. A., & Maulana, A. (2026). Harmonisasi Sanksi Administratif dan Sanksi Pidana Terhadap Pejabat Publik yang Terlibat Konflik Kepentingan (Conflict of Interest) dalam Pengadaan Barang dan Jasa. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, *4*(1), 838–849. https://doi.org/10.62976/ijijel.v4i1.1716

