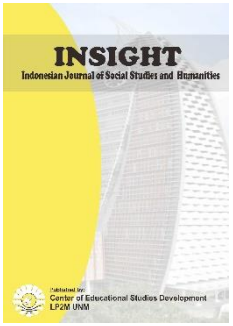
# Forensik Digital dan Pembuktian Siber: Menakar Keabsahan Bukti Elektronik dalam Sistem Peradilan Pidana




**Heri Tahir[1], Ririn Nurfaathirany Heri[2]**
Universitas Negeri Makassar, Indonesia[1,2]
Email: heri.tahir@unm.ac.id[1]

**Abstrak.** Perkembangan teknologi informasi telah mendorong transformasi kejahatan dari bentuk konvensional menuju tindak pidana berbasis digital yang bersifat virtual, lintas yurisdiksi, dan sulit dibuktikan. Secara normatif (*das sollen*), sistem hukum pidana di Indonesia menghendaki adanya kepastian hukum dan efektivitas pembuktian terhadap setiap tindak pidana, termasuk kejahatan siber, melalui pengakuan alat bukti elektronik sebagaimana diatur dalam Pasal 5 dan Pasal 6 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Namun dalam praktiknya (*das sein*), proses pembuktian tindak pidana siber menghadapi berbagai tantangan, seperti karakter bukti digital yang mudah dimodifikasi, bersifat volatil, tersebar lintas negara, serta sulitnya mengidentifikasi pelaku anonim dalam ruang siber. Penelitian ini merupakan penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Bahan hukum diperoleh melalui studi pustaka terhadap peraturan perundang-undangan, putusan pengadilan, jurnal ilmiah, dan literatur terkait cybercrime serta digital forensics, yang dianalisis secara deskriptif kualitatif. Hasil penelitian menunjukkan bahwa alat bukti elektronik memiliki kedudukan yang sah dan mandiri dalam sistem pembuktian pidana di Indonesia, yang diperkuat oleh Putusan Mahkamah Konstitusi. Keabsahan bukti digital sangat ditentukan oleh penerapan *Chain of Custody*, proses akuisisi forensik, penggunaan *write-blocker*, serta verifikasi integritas melalui nilai hash. Selain itu, ahli forensik digital memegang peran penting dalam menjelaskan validitas dan reliabilitas alat bukti elektronik di persidangan. Penelitian ini menyimpulkan bahwa pembuktian tindak pidana siber memerlukan adaptasi hukum acara pidana, penguatan kapasitas digital forensics, serta harmonisasi regulasi guna menjamin kepastian hukum dan efektivitas penegakan hukum di era digital.

**Kata Kunci :** Cybercrime; Bukti Elektronik; Digital Forensics; Chain of Custody; Pembuktian Digital; UU ITE.

## PENDAHULUAN

Transformasi digital telah menjadi pedang bermata dua bagi peradaban manusia. Di satu sisi, ia mendorong inovasi dan efisiensi di hampir semua sektor kehidupan. Di sisi lain, ia membuka pintu bagi bentuk-bentuk baru deviantasi dan kriminalitas yang memanfaatkan teknologi sebagai alat utama[1]. Perkembangan kejahatan dari bentuk-bentuk konvensional yang mengandalkan kontak fisik menjadi kejahatan digital yang bersifat virtual dan nirbatas merupakan sebuah fenomena transformatif yang menantang asumsi-asumsi dasar dalam hukum pidana dan kriminologi. Kejahatan tidak lagi terbatas pada ruang dan waktu yang konkret. Pergeseran ini bukan sekadar perubahan medium, melainkan perubahan fundamental dalam sifat, skala, dan kecepatan kejahatan. Sebuah tindak pidana pencurian data, misalnya, dapat mengakibatkan kerugian yang jauh lebih besar dan menimpa jutaan korban secara simultan, sesuatu yang mustahil dilakukan oleh pencuri konvensional[2]. Fenomena ini memaksa masyarakat dan negara untuk memikirkan kembali konsep keamanan, privasi, dan kedaulatan dalam sebuah dunia yang semakin terhubung.

Evolusi kejahatan menuju ranah digital dapat dipahami melalui tiga tahapan utama. Tahap pertama adalah ketika komputer digunakan sebagai *alat bantu* untuk melakukan kejahatan konvensional. Sebagai contoh, seorang akuntan menggunakan program *spreadsheet* untuk memanipulasi laporan keuangan dan menggelapkan dana perusahaan. Pada tahap ini, esensi kejahahatan tetaplah konvensional (penggelapan), namun teknologi mempermudah pelaksanaannya[3]. Sistem hukum pidana yang ada masih relatif mampu menangani jenis kejahatan ini karena unsur-unsur deliknya tidak berubah secara fundamental.

Tahap kedua adalah saat komputer dan jaringan menjadi *target* dari kejahatan. Inilah titik awal dari apa yang kita kenal sebagai *cybercrime* dalam arti sempit. Tindakan seperti *hacking* untuk mengakses sistem secara ilegal, penyebaran virus untuk merusak data, atau serangan *Denial of Service* (DoS) untuk melumpuhkan sebuah situs web adalah contohnya. Kejahatan jenis ini tidak memiliki padanan yang sama persis di dunia fisik dan secara spesifik menargetkan integritas, kerahasiaan, dan ketersediaan sistem komputer[4]. Munculnya kejahatan ini mendorong lahirnya peraturan-peraturan hukum baru yang secara khusus mengkriminalisasi tindakan-tindakan tersebut. Tahap ketiga, yang paling relevan saat ini, adalah ketika ruang siber menjadi *lingkungan* atau *ekosistem* tempat berbagai jenis kejahatan terjadi. Ruang siber menjadi tempat pertemuan antara pelaku dan korban, pasar untuk barang dan jasa ilegal, serta

---

[1] Wall, D. S. (2019). The social epistemology of cybercrime. In L. Gelsthorpe & R. Morgan (Eds.), *The Oxford handbook of criminology*. Oxford University Press.

[2] Smrithy, S., Doreen, R., & Rene, R. (2023). A censorious interpretation of cyber theft and its footprints. *i-manager's Journal on Information Technology*, *12*(1), 18-24. https://doi.org/10.26634/jit.12.1.19394

[3] Holt, T. J., & Bossler, A. M. (2020). Cybercrime and digital forensics: An introduction. Routledge.

[4] Mirzakarimova, D. (2025). TYPES OF CYBERCRIMES AND THEIR CHARACTERISTICS. *Criminology and Criminal Justice*, *5*(2).

platform untuk melakukan penipuan, eksploitasi, dan penyebaran ideologi berbahaya[5]. Pada tahap ini, batas antara kejahatan konvensional dan kejahatan siber menjadi semakin kabur. Misalnya, perdagangan manusia kini banyak difasilitasi melalui media sosial, di mana ruang siber menjadi medium utama yang memungkinkan kejahatan konvensional tersebut terjadi dalam skala yang lebih luas dan tersembunyi.

Serangan *ransomware* WannaCry pada tahun 2017 menginfeksi lebih dari 200.000 komputer di 150 negara dalam satu hari, melumpuhkan sistem layanan kesehatan di Inggris (NHS), perusahaan telekomunikasi di Spanyol, dan berbagai institusi vital lainnya. Kasus ini menjadi contoh nyata bagaimana sebuah kejahatan siber dapat terjadi dalam skala global, melintasi yurisdiksi, dan menyebabkan dampak fisik yang nyata (melumpuhkan layanan rumah sakit) hanya melalui penyebaran kode berbahaya. Ini menunjukkan transformasi dari kejahatan yang bersifat lokal menjadi ancaman global yang terkoordinasi. Transformasi kejahatan menuntut adanya sistem klasifikasi baru yang lebih sesuai dengan realitas digital. Secara umum, kejahatan di era digital dapat diklasifikasikan ke dalam tiga kategori besar.

Pembuktian dalam tindak pidana siber merupakan aspek paling krusial dalam penegakan hukum di era digital karena keberhasilannya sangat bergantung pada kemampuan mengidentifikasi, memperoleh, dan memverifikasi bukti digital sebagai alat bukti utama di pengadilan. Bukti digital dapat berupa setiap informasi yang memiliki nilai pembuktian dan disimpan atau ditransmisikan dalam format elektronik, seperti email, metadata, log aktivitas sistem, percakapan digital, hingga data jaringan internet. Di Indonesia, keabsahan alat bukti elektronik telah memperoleh landasan hukum melalui Pasal 5 dan Pasal 6 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang menegaskan bahwa informasi elektronik dan dokumen elektronik merupakan alat bukti hukum yang sah sebagai perluasan alat bukti dalam KUHAP, serta diperkuat melalui Putusan Mahkamah Konstitusi yang menempatkan bukti elektronik sebagai alat bukti mandiri dalam sistem pembuktian pidana. Namun demikian, karakteristik bukti digital yang bersifat nonfisik, mudah dimodifikasi, dan sangat bergantung pada sistem teknologi menimbulkan tantangan serius dalam proses pembuktian.

Secara forensik, bukti digital dibedakan menjadi data volatil, yaitu data sementara yang tersimpan dalam RAM dan harus diamankan melalui *live acquisition*, serta data non-volatil yang tersimpan permanen pada media penyimpanan dan umumnya diperoleh melalui *static acquisition*. Dalam praktiknya, keabsahan bukti digital sangat ditentukan oleh penerapan *Chain of Custody* atau rantai penjagaan bukti, yaitu proses dokumentasi kronologis yang memastikan otentisitas, integritas, dan reliabilitas alat bukti sejak ditemukan di tempat kejadian perkara digital hingga diajukan di persidangan. Proses akuisisi forensik dilakukan melalui pembuatan *forensic image* secara bit-demi-bit menggunakan *write-blocker* untuk mencegah perubahan data asli, kemudian diverifikasi menggunakan nilai hash seperti MD5 atau SHA-256 guna

[5] Zhou, Y., Tiwari, M., Bernot, A., & Lin, K. (2024). Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality. *Asian Journal of Criminology*. https://doi.org/10.1007/s11417-024-09436-y

menjamin integritas bukti. Meski demikian, pembuktian tindak pidana siber masih menghadapi berbagai hambatan, antara lain sifat bukti yang mudah hilang (*volatility*), kesulitan memperoleh data lintas yurisdiksi negara, serta kompleksitas mengidentifikasi pelaku yang beroperasi secara anonim di ruang siber. Dalam kondisi tersebut, ahli forensik digital memegang peranan yang sangat penting sebagai pihak yang mampu menerjemahkan temuan teknis menjadi keterangan ilmiah yang dapat dipahami oleh aparat penegak hukum dan majelis hakim, sehingga kualifikasi, objektivitas, dan kemampuan komunikasi ahli menjadi faktor penentu dalam membangun keyakinan hakim terhadap validitas alat bukti digital dalam proses peradilan pidana.

Berdasarkan uraian tersebut, proses pembuktian dalam tindak pidana siber tidak lagi dapat disamakan dengan pembuktian konvensional karena karakteristik alat bukti digital yang bersifat nonfisik, mudah berubah, serta tersebar dalam ruang siber lintas yurisdiksi. Kondisi ini menuntut adanya mekanisme pembuktian yang mampu menjamin keaslian, integritas, dan validitas alat bukti elektronik agar dapat diterima dalam proses peradilan pidana. Selain itu, perkembangan teknologi informasi juga memunculkan tantangan baru bagi aparat penegak hukum dalam melakukan identifikasi pelaku, pengamanan barang bukti digital, hingga penerapan digital forensics dalam proses penyidikan dan pembuktian di persidangan. Oleh karena itu, diperlukan kajian yang komprehensif mengenai kedudukan alat bukti elektronik dan mekanisme pembuktian tindak pidana siber dalam sistem hukum pidana Indonesia. Berdasarkan latar belakang tersebut, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana kedudukan dan kekuatan alat bukti elektronik dalam proses pembuktian tindak pidana di ruang digital menurut hukum pidana Indonesia?
2. Bagaimana mekanisme dan tantangan pembuktian tindak pidana siber dalam menjamin keaslian, integritas, dan validitas alat bukti digital?

## METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (*normative legal research*) yang mengkaji norma hukum, asas hukum, dan peraturan perundang-undangan terkait proses pembuktian dalam ruang digital. Fokus penelitian diarahkan pada kedudukan alat bukti elektronik, mekanisme pembuktian tindak pidana siber, serta tantangan penegakan hukum dalam sistem peradilan pidana di Indonesia.

Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan dilakukan dengan menelaah KUHAP, KUHP, serta Undang-Undang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024. Pendekatan konseptual digunakan untuk memahami konsep alat bukti elektronik, digital forensics, dan cybercrime, sedangkan pendekatan kasus dilakukan melalui kajian terhadap putusan pengadilan dan praktik pembuktian tindak pidana siber.

Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier yang diperoleh melalui studi pustaka (*library research*). Seluruh bahan hukum dianalisis secara deskriptif kualitatif guna memperoleh pemahaman mengenai efektivitas sistem pembuktian dalam menghadapi perkembangan kejahatan digital di era teknologi informasi.

## HASIL DAN PEMBAHASAN

Dari perspektif hukum pidana, suatu perbuatan dapat dikategorikan sebagai *cybercrime* apabila memenuhi unsur-unsur yang dirumuskan dalam undang-undang pidana. Definisi ini berpegang teguh pada asas legalitas, yang menyatakan bahwa tidak ada perbuatan yang dapat dipidana kecuali atas kekuatan aturan pidana dalam perundang-undangan yang telah ada sebelum perbuatan dilakukan. Dengan demikian, hukum pidana mendefinisikan *cybercrime* secara enumeratif, yaitu dengan mendaftar satu per satu perbuatan apa saja yang dilarang, seperti yang tercantum dalam Bab VII UU ITE (Perbuatan yang Dilarang).

Meskipun jenisnya beragam, sebagian besar tindak pidana siber memiliki beberapa unsur esensial yang membedakannya dari kejahatan konvensional. Unsur pertama adalah adanya penggunaan atau eksploitasi teknologi informasi. Komputer atau jaringan tidak hanya menjadi alat, tetapi seringkali menjadi bagian tak terpisahkan dari *corpus delicti* atau tubuh kejahatan itu sendiri[6]. Tanpa adanya komponen digital ini, perbuatan tersebut mungkin tidak dapat terjadi atau akan memiliki bentuk yang sama sekali berbeda.

Unsur kedua adalah sifat non-fisik (*intangible*) dari objek kejahatan dan kerugian yang ditimbulkan. Dalam banyak kasus, yang dicuri atau dirusak bukanlah benda berwujud, melainkan data, informasi, reputasi, atau kepercayaan. Kerugian yang timbul seringkali bersifat finansial atau ekonomi, namun dapat pula berupa kerugian non-materiil seperti kerusakan citra atau trauma psikologis[7]. Hal ini menimbulkan tantangan dalam proses pembuktian dan penghitungan ganti rugi di pengadilan.

Unsur ketiga yang krusial adalah unsur kesengajaan (*mens rea*) dan perbuatan melawan hukum (*actus reus*) dalam konteks digital. Pembuktian niat jahat pelaku di ruang siber seringkali lebih sulit, karena pelaku dapat berdalih melakukan "uji coba keamanan" atau "ketidaksengajaan". Selain itu, konsep "melawan hukum" atau "tanpa hak" juga memerlukan interpretasi baru, misalnya dalam menentukan apakah mengakses sebuah *database* publik dengan linkcara yang tidak biasa sudah dapat dianggap sebagai akses ilegal atau belum [8].

### 1. Jenis Bukti Digital

kita mengetahui beragam modus kejahatan siber dan tiba pada sebuah persimpangan krusial: bagaimana kejahatan-kejahatan tak berwujud tersebut

[6] Al-Faraji, N. (2025). The legal framework of cybercrime and the obstacles to proving it. *International Journal of Criminal, Common and Statutory Law*, *5*(1a), 113.

[7] Lee, S., Kang, I., & Kim, H. (2023). Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes?. *Technology in Society*, 74, 102361.

[8] Situmorang, V. H. (2020). Kebijakan Kriminal Penanggulangan Kejahatan Dunia Maya (Cyber Crime) di Indonesia. *Jurnal Hukum & Pembangunan*, 49(4), 846-866.

dibuktikan di hadapan hukum? Sebuah dakwaan, sekuat apapun narasinya, akan runtuh tanpa didasari oleh alat bukti yang sah dan meyakinkan. Di dunia siber, alat bukti ini tidak lagi berupa sidik jari di gagang pintu atau selongsong peluru di lantai, melainkan jejak-jejak digital yang tak kasat mata, rapuh, dan tersebar di berbagai penjuru dunia. Bab ini akan membedah dunia pembuktian digital yang menjadi tulang punggung penegakan hukum siber.

Konsep "bukti" dalam hukum pidana secara tradisional terikat pada sifat fisik dan stabilitasnya. Sebaliknya, bukti digital memiliki karakteristik yang bertolak belakang. Ia bersifat non-fisik (*intangible*), mudah dimodifikasi atau dihancurkan tanpa meninggalkan jejak yang jelas, dan seringkali sangat volatil, dapat lenyap seketika hanya dengan mematikan sebuah perangkat. Sifat-sifat inilah yang menantang asumsi-asumsi dasar dalam hukum acara pidana dan menuntut lahirnya sebuah disiplin ilmu baru: forensik digital.

Pengakuan hukum terhadap bukti elektronik merupakan revolusi senyap dalam sistem peradilan. Di Indonesia, Undang-Undang ITE menjadi pionir yang secara tegas menyatakan bahwa informasi dan dokumen elektronik merupakan alat bukti hukum yang sah. Namun, pengakuan ini barulah langkah awal. Pertanyaan yang lebih rumit menyusul: bagaimana memastikan bahwa serangkaian bit dan byte yang disajikan di pengadilan adalah bukti yang otentik, tidak diubah sejak ditemukan, dan benar-benar relevan dengan perkara yang disidangkan?

Jawaban atas pertanyaan tersebut terletak pada sebuah proses yang sangat teliti dan metodis yang dikenal sebagai *Chain of Custody* atau Rantai Penjagaan Bukti. Proses ini adalah jantung dari integritas forensik digital. Ia adalah dokumentasi tanpa putus yang mencatat setiap tangan yang menyentuh dan setiap tindakan yang dilakukan terhadap barang bukti, dari sejak ia ditemukan di tempat kejadian perkara digital hingga disajikan di hadapan majelis hakim. Tanpa rantai penjagaan yang kokoh, nilai pembuktian dari sebuah data digital dapat dengan mudah dipatahkan. metode untuk "mengamankan" jejak digital tersebut. Proses akuisisi forensik, baik yang dilakukan pada sistem yang masih menyala (*live*) maupun yang sudah mati (*static*), memiliki teknik dan implikasinya masing-masing. Pemilihan metode yang tepat menjadi kunci untuk dapat mengumpulkan sebanyak mungkin bukti yang relevan tanpa merusak atau mengkontaminasi bukti aslinya.

Perjalanan dari jejak digital menjadi putusan pengadilan tidaklah mulus. Berbagai tantangan menghadang di setiap langkah, mulai dari sifat bukti yang mudah hilang, kerumitan mendapatkan bukti dari yurisdiksi negara lain, hingga kelihaian pelaku dalam menyamarkan identitas mereka di balik lapisan anonimitas. Di tengah kompleksitas inilah, peran seorang ahli forensik digital menjadi sangat vital, bertindak sebagai penerjemah yang menjelaskan makna dari data-data teknis yang rumit kepada para praktisi hukum. Bukti digital, atau bukti elektronik, dapat didefinisikan sebagai setiap informasi yang memiliki nilai pembuktian yang disimpan atau ditransmisikan dalam format digital[9] Ruang lingkupnya sangat luas, mencakup segala sesuatu mulai

[9] Casey, E. (2021). The challenge of cross-border access to electronic evidence. *Digital Investigation*, *38*, 101-110.

dari file dokumen di *hard drive*, email di server, *log* aktivitas jaringan, riwayat penelusuran internet, data lokasi dari ponsel, hingga metadata yang tersembunyi di dalam sebuah file gambar. Pada dasarnya, hampir setiap interaksi dengan teknologi modern berpotensi menghasilkan bukti digital.

Memahami jenis-jenis bukti digital dan dasar hukum yang mengaturnya adalah fondasi bagi setiap praktisi hukum di era digital. Tanpa pengakuan eksplisit dari undang-undang, semua jejak digital ini tidak akan memiliki nilai di mata pengadilan. Di Indonesia, UU ITE menjadi terobosan legislatif yang memberikan landasan hukum yang kuat bagi penggunaan bukti elektronik, yang kemudian diperkuat oleh berbagai putusan yudisial dan harmonisasi dengan hukum acara pidana yang ada. Pengakuan ini membuka pintu bagi penegakan hukum untuk menjerat kejahatan yang sebelumnya sulit atau bahkan mustahil untuk dibuktikan.

Bukti digital dapat diibaratkan seperti jejak kaki di berbagai jenis permukaan. Ada jejak di lumpur basah (data volatil) yang akan hilang seketika saat hujan turun atau matahari bersinar terik. Ada pula jejak yang membatu menjadi fosil (data non-volatil) yang bisa bertahan ribuan tahun jika tidak dirusak. Seorang penyelidik harus tahu jenis jejak apa yang ia hadapi. Untuk jejak di lumpur, ia harus segera mendokumentasikannya sebelum hilang. Untuk fosil, ia harus menggali dengan hati-hati agar tidak merusaknya. Undang-undang adalah pengakuan bahwa jejak-jejak ini, baik yang sementara maupun yang permanen, dapat diterima sebagai penunjuk arah kebenaran di pengadilan.

Secara forensik, bukti digital umumnya diklasifikasikan ke dalam dua kategori besar berdasarkan tingkat persistensinya: data volatil dan data non-volatil. Data volatil (*volatile data*) adalah data yang bersifat sementara dan akan hilang jika sumber daya listrik ke perangkat tersebut dimatikan. Sumber utama data volatil adalah *Random Access Memory* (RAM). RAM berisi informasi yang sangat berharga bagi penyelidik, seperti proses yang sedang berjalan, koneksi jaringan yang aktif, kata sandi yang tersimpan sementara, dan kunci enkripsi [10]. Karena sifatnya yang mudah hilang, pengumpulan data volatil menjadi prioritas utama dan harus dilakukan saat sistem masih dalam keadaan menyala (*live acquisition*).

Sebaliknya, data non-volatil (*non-volatile data*) adalah data yang tersimpan secara permanen pada media penyimpanan dan tidak akan hilang meskipun perangkat dimatikan. Ini adalah jenis bukti digital yang paling umum dikenal, mencakup file, dokumen, gambar, dan video yang tersimpan di *hard disk drive* (HDD), *solid-state drive* (SSD), *flash drive*, atau media penyimpanan lainnya. Data ini juga mencakup informasi yang "dihapus" oleh pengguna, yang seringkali masih dapat dipulihkan dari ruang disk yang belum terisi kembali (*unallocated space*) menggunakan perangkat lunak forensik. Pengumpulan data non-volatil biasanya dilakukan setelah sistem dimatikan (*static acquisition*) untuk menjaga integritasnya.

Selain kedua kategori utama tersebut, bukti digital juga dapat ditemukan di lokasi lain, seperti di jaringan (*network logs*, data paket) atau di *cloud* (data yang tersimpan

[10] Ricci, C. (2021). Volatile data analysis in digital forensics: a review. *Journal of Forensic Sciences*, *66*(4), 1187-1199.

di server jarak jauh milik penyedia layanan seperti Google atau Amazon). Klasifikasi ini sangat penting karena ia menentukan urutan prioritas dan metode yang harus digunakan oleh tim forensik saat mengamankan tempat kejadian perkara digital. Kesalahan dalam menangani data volatil dapat menyebabkan hilangnya bukti yang tidak akan pernah bisa dipulihkan kembali.

Landasan hukum utama yang mengakui keabsahan bukti elektronik di Indonesia adalah Pasal 5 ayat (1) Undang-Undang ITE. Pasal ini secara tegas menyatakan bahwa "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah". Pasal 5 ayat (2) lebih lanjut menyatakan bahwa alat bukti tersebut merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. Ini adalah sebuah pernyataan revolusioner yang secara formal memasukkan bukti digital ke dalam sistem pembuktian nasional.

Pasal 6 UU ITE memberikan syarat formil, yaitu bahwa informasi atau dokumen elektronik dianggap sah "sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan". Syarat-syarat ini, aksesibilitas, keterbacaan, integritas, dan akuntabilitas, menjadi standar yang harus dipenuhi oleh penuntut umum saat menyajikan bukti digital di persidangan.

Kedudukan bukti elektronik ini semakin diperkuat oleh Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016. Putusan ini menafsirkan bahwa frasa "perluasan alat bukti" dalam UU ITE berarti bukti elektronik diakui sebagai jenis alat bukti baru yang berdiri sendiri, di samping lima alat bukti yang telah diatur dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yaitu keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Putusan ini menghilangkan keraguan dan perdebatan mengenai apakah bukti elektronik hanya dianggap sebagai "petunjuk" atau memiliki kekuatan pembuktian yang setara dengan alat bukti lainnya.

Agar dapat diterima oleh pengadilan (*admissibility*) dan dipercaya oleh hakim (*reliability*), bukti digital harus memenuhi beberapa standar kualitas minimum. Standar pertama adalah keaslian (*authenticity*). Penuntut harus dapat menunjukkan bahwa bukti yang disajikan adalah benar-benar bukti yang sama dengan yang ditemukan di TKP digital dan berasal dari sumber yang diklaim. Ini seringkali dibuktikan melalui keterangan ahli dan dokumentasi *chain of custody*.

Standar kedua adalah integritas (*integrity*). Harus ada jaminan bahwa bukti tersebut tidak mengalami perubahan, penambahan, atau pengurangan sejak diamankan. Dalam forensik digital, integritas ini dijamin secara matematis menggunakan fungsi *hash* (seperti MD5 atau SHA-256). Nilai *hash* dari bukti asli dihitung saat pertama kali diamankan. Nilai ini harus sama persis dengan nilai *hash* dari salinan kerja yang dianalisis dan disajikan di pengadilan. Perbedaan sekecil apapun pada nilai *hash* mengindikasikan bahwa bukti tersebut telah berubah dan integritasnya diragukan.

Standar ketiga adalah reliabilitas. Ini berkaitan dengan keandalan dari proses dan peralatan yang digunakan untuk mengumpulkan dan menganalisis bukti. Metode yang digunakan harus sesuai dengan praktik terbaik yang diakui secara ilmiah dan

internasional, seperti yang diuraikan dalam standar ISO/IEC 27037 (*Guidelines for identification, collection, acquisition, and preservation of digital evidence*). Ahli forensik harus dapat menjelaskan dan mempertahankan metodologinya di bawah pemeriksaan silang di pengadilan untuk menunjukkan bahwa hasilnya dapat diandalkan.

**2. Chain of Custody (Rantai Penjagaan Bukti)**

*Chain of Custody* secara formal didefinisikan sebagai dokumentasi kronologis yang menunjukkan alur penjagaan, penguasaan, pengendalian, pemindahan, analisis, dan disposisi dari barang bukti fisik atau elektronik. Dokumentasi ini harus mencatat secara detail siapa yang memegang bukti, kapan, di mana, dan untuk tujuan apa, dari saat bukti tersebut pertama kali diamankan hingga saat tidak lagi dibutuhkan. Tujuannya adalah untuk menjawab pertanyaan-pertanyaan fundamental yang akan diajukan di pengadilan: Di mana bukti ini ditemukan? Bagaimana ia dikumpulkan? Siapa saja yang telah menanganinya? Dan bagaimana kita tahu bahwa ini adalah bukti yang asli?

Tujuan utama dari proses ini adalah untuk menjaga tiga pilar kualitas bukti: otentisitas, integritas, dan reliabilitas. Otentisitas dipastikan dengan menunjukkan bahwa bukti tersebut benar-benar berasal dari sumber yang diklaim. Integritas dijamin dengan membuktikan bahwa bukti tersebut tidak mengalami perubahan yang tidak sah. Reliabilitas dibangun dengan menunjukkan bahwa proses penanganan bukti dilakukan sesuai dengan prosedur standar yang dapat diandalkan[11]

Kegagalan dalam menjaga *Chain of Custody* dapat berakibat fatal bagi sebuah kasus. Jika ada "mata rantai" yang hilang dalam dokumentasi, misalnya, ada periode waktu di mana tidak jelas siapa yang memegang bukti atau apa yang dilakukan terhadapnya, maka integritas bukti tersebut menjadi cacat. Hal ini akan membuka celah bagi pembela untuk berargumen bahwa bukti tersebut tidak dapat dipercaya, dan hakim mungkin memutuskan untuk menolak bukti tersebut (*inadmissible*), yang bisa menyebabkan seluruh kasus menjadi goyah atau bahkan dibatalkan.

Langkah pertama dalam *Chain of Custody* adalah identifikasi dan pengamanan bukti. Setelah perangkat yang berpotensi mengandung bukti (seperti laptop, ponsel, atau server) diidentifikasi, langkah selanjutnya adalah membuat salinan forensik yang identik. Prosedur standar melarang keras penyelidik untuk bekerja langsung pada barang bukti asli. Semua analisis harus dilakukan pada salinan kerja (*working copy*) untuk mencegah perubahan yang tidak disengaja pada bukti aslinya[12]. Untuk membuat salinan, digunakan perangkat keras yang disebut *write-blocker*. Perangkat ini dipasang di antara barang bukti asli (misalnya, *hard disk*) dan komputer forensik, dan secara fisik mencegah komputer untuk menulis data apa pun ke bukti asli, sehingga menjaga keutuhannya. Proses penyalinan ini menciptakan sebuah *forensic image* atau citra forensik, yang merupakan salinan bit-demi-bit dari seluruh isi media penyimpanan, termasuk ruang yang kosong dan file yang telah dihapus. Setelah citra forensik dibuat, langkah yang paling krusial adalah menghitung nilai *hash* dari kedua

[11] Wardani, D. K., & Asrori, A. (2019). Urgensi Menjaga Integritas Barang Bukti Digital d

[12] Budi, I. S. (2021). Penerapan Standar Operasional Prosedur Chain of Custody dalam Penanganan Barang Bukti Digital Forensik. *Jurnal Ilmu Kepolisian*, *15*(3), 189-201.

media: bukti asli dan citra forensik. Nilai *hash* (misalnya, SHA-256) ini berfungsi sebagai sidik jari digital yang unik. Jika kedua nilai *hash* tersebut identik, maka ini membuktikan secara matematis bahwa salinan tersebut adalah replika yang sempurna dari aslinya. Nilai *hash* asli ini kemudian dicatat dalam formulir *Chain of Custody* dan akan digunakan sebagai titik referensi untuk verifikasi integritas di setiap tahap selanjutnya.

Dokumentasi adalah nyawa dari *Chain of Custody*. Setiap tindakan yang terkait dengan barang bukti harus dicatat dalam formulir atau log *Chain of Custody*. Informasi yang harus dicatat meliputi: deskripsi detail dari barang bukti, tanggal dan waktu pengamanan, lokasi penemuan, nama dan tanda tangan petugas yang mengamankan, serta nilai *hash* awal. Setiap kali bukti tersebut dipindahkan atau diserahkan kepada orang lain (misalnya, dari penyidik lapangan ke analis forensik di laboratorium), baik penerima maupun pemberi harus menandatangani formulir tersebut, mencatat tanggal dan waktu serah terima. Dengan cara ini, tercipta jejak audit yang jelas dan tidak terputus. Jika bukti disimpan dalam lemari penyimpanan bukti, log akses ke lemari tersebut juga menjadi bagian dari dokumentasi.

Selama proses analisis, analis forensik juga harus mendokumentasikan semua langkah yang diambilnya dalam sebuah catatan kasus (*case notes*). Catatan ini harus merinci perangkat lunak apa yang digunakan, perintah apa yang dijalankan, dan temuan apa yang dihasilkan. Transparansi ini penting agar pihak lain (misalnya, ahli forensik dari pihak pembela) dapat mereplikasi dan memverifikasi proses analisis tersebut. Di akhir proses, semua dokumentasi ini, formulir *Chain of Custody*, catatan kasus, dan laporan akhir, menjadi satu paket yang mendukung keabsahan bukti di pengadilan.

## KESIMPULAN

Transformasi kejahatan menuju ruang digital telah mengubah pola pembuktian dalam sistem peradilan pidana modern. Alat bukti elektronik kini menjadi instrumen utama dalam mengungkap tindak pidana siber, baik dalam bentuk data digital, metadata, log aktivitas sistem, maupun informasi elektronik lainnya. Di Indonesia, kedudukan alat bukti elektronik telah memperoleh legitimasi hukum melalui Pasal 5 dan Pasal 6 UU ITE serta diperkuat oleh Putusan Mahkamah Konstitusi yang menempatkan bukti elektronik sebagai alat bukti yang sah dan mandiri dalam sistem pembuktian pidana.

Proses pembuktian tindak pidana siber memiliki karakteristik yang berbeda dengan pembuktian konvensional karena bukti digital bersifat nonfisik, mudah dimodifikasi, mudah hilang, dan seringkali berada dalam ruang lintas yurisdiksi. Oleh karena itu, penerapan *Chain of Custody*, proses akuisisi forensik, penggunaan *write-blocker*, dan verifikasi integritas melalui nilai hash menjadi aspek yang sangat penting dalam menjamin otentisitas, integritas, dan reliabilitas alat bukti digital.

Selain itu, keberhasilan pembuktian tindak pidana siber sangat bergantung pada kemampuan aparat penegak hukum dan ahli forensik digital dalam mengidentifikasi, mengamankan, menganalisis, dan menjelaskan bukti elektronik di hadapan pengadilan. Dengan demikian, diperlukan penguatan kapasitas digital forensics,

pembaruan hukum acara pidana, serta harmonisasi regulasi agar sistem pembuktian di Indonesia mampu menjawab tantangan perkembangan cybercrime di era transformasi digital.

## DAFTAR PUSTAKA

Al-Faraji, N. (2025). The Legal Framework of Cybercrime and the Obstacles to Proving It. *International Journal of Criminal, Common and Statutory Law*, 5(1a), 113.

Astuti, S. I. (2019). Tinjauan Yuridis Perilaku Cyberbullying di Kalangan Remaja Dihubungkan dengan Undang-Undang Nomor 19 Tahun 2016. *Jurnal Wawasan Yuridika*, 3(2), 249–266.

Budi, I. S. (2021). Penerapan Standar Operasional Prosedur Chain of Custody dalam Penanganan Barang Bukti Digital Forensik. *Jurnal Ilmu Kepolisian*, 15(3), 189–201.

Casey, E. (2021). The Challenge of Cross-Border Access to Electronic Evidence. *Digital Investigation*, 38, 101–110.

Febriani, A. (2021). Perlindungan Hukum Terhadap Korban Cyberbullying dalam Perspektif Hukum Pidana Indonesia. *Jurnal Pembangunan Hukum Indonesia*, 3(1), 108–122.

Holt, T. J., & Bossler, A. M. (2020). *Cybercrime and Digital Forensics: An Introduction*. Routledge.

Ispriyarso, B., & Setya, W. (2020). The Limitation of Hate Speech Based on SARA in Indonesia: A Criminal Law Perspective. *Journal of Indonesian Legal Studies*, 5(2), 349–376.

Lee, S., Kang, I., & Kim, H. (2023). Understanding Cybercrime from a Criminal's Perspective: Why and How Suspects Commit Cybercrimes?. *Technology in Society*, 74, 102361.

Mirzakarimova, D. (2025). Types of Cybercrimes and Their Characteristics. *Criminology and Criminal Justice*, 5(2).

Miquic, A., & Brewer, G. (2023). Organized Cybercrime: A Systematic Review. *Trauma, Violence, & Abuse*, 25(2).

Ricci, C. (2021). Volatile Data Analysis in Digital Forensics: A Review. *Journal of Forensic Sciences*, 66(4), 1187–1199.

Saragih, H. Y., & Simarmata, J. (2021). Penegakan Hukum Pidana Ujaran Kebencian (*Hate Speech*) Berdasarkan Pasal 28 Ayat (2) UU ITE. *Jurnal Ilmiah Penegakan Hukum*, 8(1), 1–13.

Sari, I. P., & Wijaya, A. (2020). Penerapan Pasal 27 Ayat (3) UU ITE Terkait Pencemaran Nama Baik Pasca Putusan Mahkamah Konstitusi. *Jurnal Kertha Wicaksana*, 14(2), 101–110.

Situmorang, V. H. (2020). Kebijakan Kriminal Penanggulangan Kejahatan Dunia Maya (*Cyber Crime*) di Indonesia. *Jurnal Hukum & Pembangunan*, 49(4), 846–866.

Sitorus, L. (2022). Karakteristik Kejahatan Siber Lintas Negara dan Penegakan Hukumnya di Indonesia. *Lex Librum: Jurnal Ilmu Hukum*, 8(2), 115–128.

Smrithy, S., Doreen, R., & Rene, R. (2023). A Censorious Interpretation of Cyber Theft and Its Footprints. *i-manager's Journal on Information Technology*, 12(1), 18–24. https://doi.org/10.26634/jit.12.1.19394

Wardani, D. K., & Asrori, A. (2019). Urgensi Menjaga Integritas Barang Bukti Digital.

Wall, D. S. (2019). The Social Epistemology of Cybercrime. In L. Gelsthorpe & R. Morgan (Eds.), *The Oxford Handbook of Criminology*. Oxford University Press.

Zhou, Y., Tiwari, M., Bernot, A., & Lin, K. (2024). Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality. *Asian Journal of Criminology*. https://doi.org/10.1007/s11417-024-09436-y

**Peraturan Perundang-Undangan**

Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 tentang Pengujian Undang-Undang Informasi dan Transaksi Elektronik.

Surat Keputusan Bersama Menteri Komunikasi dan Informatika, Jaksa Agung, dan Kepala Kepolisian Negara Republik Indonesia tentang Pedoman Implementasi atas Pasal Tertentu dalam Undang-Undang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, khususnya Pasal 45 ayat (4) dan Pasal 45 ayat (5).