Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

Etika dan Keadilan dalam Penggunaan Bukti Digital Hasil Forensik Siber di Persidangan

Karunia Adi Setiawan[1*], Agus Pramono[2], Sri Yuni Hastuti[3]
[1,3]Fakultas Hukum, Universitas Darul Ulum Islamic Centre Sudirman
[2]Fakultas Hukum, Universitas Wisnuwardhana Malang
[*]Email Korespondensi: adikarunia071@gmail.com

ABSTRAK

Perkembangan teknologi informasi telah mengubah paradigma pembuktian dalam hukum acara pidana, di mana bukti digital kini menjadi instrumen krusial bagi penegak hukum. Namun, sifat bukti digital yang volatil, mudah dimodifikasi, dan tidak berwujud menimbulkan tantangan serius terhadap etika profesi forensik dan keadilan prosedural. Artikel ini bertujuan untuk menganalisis dimensi etika dan keadilan dalam penggunaan bukti digital hasil forensik siber dengan menggunakan perspektif teori keadilan John Rawls serta standar internasional seperti Daubert dan ISO/IEC 27037. Melalui metode penelitian hukum normatif dengan pendekatan konseptual dan perbandingan literatur asing, penelitian ini mengkaji dua topik utama: integrasi standar etika internasional dalam validasi alat forensik dan penguatan prinsip *Equality of Arms* dalam proses ajudikasi digital. Hasil penelitian menunjukkan bahwa keabsahan bukti digital tidak cukup hanya bersandar pada integritas teknis (*hashing*), melainkan harus melalui proses auditabilitas yang transparan untuk mencegah bias algoritmik, terutama dengan hadirnya kecerdasan buatan. Temuan ini menekankan perlunya reformasi hukum acara yang mengakomodasi hak *Digital Habeas Corpus* bagi terdakwa untuk menjamin keseimbangan posisi hukum di hadapan negara. Artikel ini menyimpulkan bahwa keadilan dalam ruang siber hanya dapat dicapai apabila teknologi forensik diposisikan sebagai alat pencari kebenaran objektif, bukan sekadar instrumen pemidanaan.

Kata Kunci: Forensik Siber, Bukti Digital, Keadilan Prosedural, Standar Daubert, UU ITE

1. PENDAHULUAN

Transformasi masyarakat menuju era digital telah membawa implikasi yang mendalam terhadap sistem peradilan pidana di seluruh dunia, termasuk Indonesia. Bukti fisik tradisional yang selama berabad-abad menjadi tulang punggung pembuktian kini mulai tergeser oleh bukti digital yang bersifat intangible dan tersimpan dalam berbagai

perangkat elektronik, mulai dari peladen awan (*cloud servers*) hingga perangkat Internet of Things (IoT) (Ismail & Ariffin, 2025). Dalam konteks ini, forensik siber muncul sebagai disiplin ilmu yang esensial untuk mengidentifikasi, mengamankan, menganalisis, dan mempresentasikan data elektronik agar dapat diterima secara sah di muka persidangan (Aleke & Trigui, 2025). Namun, di balik kecanggihan teknologinya, penggunaan bukti digital membawa kerentanan sistemik yang berkaitan erat dengan etika penanganan data dan keadilan bagi para pihak yang bersengketa (Ferguson et al., 2020).

Urgensitas penelitian ini didasarkan pada fakta bahwa bukti digital memiliki karakteristik unik yang membedakannya dari bukti fisik, yaitu volatilitas dan kemudahan untuk dimanipulasi tanpa meninggalkan jejak yang kasat mata (Lasagni, 2025). Kesalahan kecil dalam prosedur akuisisi atau kegagalan dalam menjaga rantai penjagaan (*chain of custody*) dapat mengakibatkan perubahan bit data yang fatal, sehingga merusak otentisitas bukti tersebut (Tiba, 2025). Fenomena "fundamentalism data" di mana aparat penegak hukum dan hakim cenderung menerima hasil analisis alat forensik secara mutlak tanpa mempertimbangkan margin kesalahan atau bias alat, seringkali menjadi ancaman tersembunyi bagi hak asasi terdakwa (Lasagni, 2025). Ketidaktahuan yudisial terhadap kompleksitas teknis ini menciptakan ketidakseimbangan kekuasaan, di mana negara dengan sumber daya forensik yang masif berhadapan dengan individu yang memiliki keterbatasan akses terhadap teknologi audit tandingan (Filletti, 2026).

Penelitian ini memiliki keunikan karena tidak hanya berfokus pada aspek teknis forensik, tetapi secara mendalam mengintegrasikan teori-teori keadilan global dengan standar teknis internasional. Literasi hukum di Indonesia seringkali masih tertinggal dalam mendiskusikan konsep seperti *Equality of Digital Arms* atau penerapan *Daubert Standard* dalam konteks lokal (Rustamaji et al., 2026). Melalui pemanfaatan literatur asing terbaru (2019-2025), artikel ini mengeksplorasi bagaimana prinsip-prinsip etika universal dari organisasi seperti ACM, IEEE, dan ISFCE dapat diinternalisasi dalam

hukum acara pidana Indonesia, terutama pasca berlakunya Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE (Sukarta et al., 2025).

Signifikansi penelitian ini tercermin dalam upayanya untuk mengisi kekosongan doktriner mengenai batasan etis penggunaan kecerdasan buatan (AI) dalam analisis bukti digital. Dengan semakin maraknya penggunaan alat forensik berbasis AI yang bersifat *"black box",* tantangan terhadap transparansi dan akuntabilitas menjadi semakin nyata (Mandayam, 2025). Laporan ini akan memberikan wawasan mendalam bagi para praktisi hukum dan akademisi mengenai bagaimana membangun kerangka tata kelola bukti digital yang menjunjung tinggi praduga tak bersalah dan hak atas peradilan yang jujur (*fair trial*) (Bhatti, 2026).

Sebagai landasan awal, terdapat setidaknya lima studi relevan yang menjadi titik tolak penelitian ini. Pertama, penelitian oleh Ismail & Ariffin (2025) yang menekankan pentingnya validasi alat forensik sumber terbuka untuk memenuhi standar Daubert di pengadilan. Kedua, studi Ferguson et al., (2020) yang memperkenalkan kerangka kerja PRECEPT untuk menyeimbangkan kebutuhan investigasi dengan hak privasi individu melalui sebelas prinsip etika. Ketiga, analisis dari International Criminal Court (ICC) mengenai tahap-tahap penerimaan bukti digital yang mencakup relevansi, nilai pembuktian, dan efek merugikan (Sangari & Mohammadi, 2025). Keempat, kajian Bhatti (2026) mengenai ancaman sistemik terhadap keadilan prosedural akibat instabilitas informasi digital. Kelima, penelitian Rustamaji et al., (2026) yang menyoroti perlunya penguatan kompetensi teknis hakim di Indonesia dalam memverifikasi metadata dan integritas data elektronik. Dengan menggabungkan temuan-temuan tersebut, artikel ini akan memberikan kontribusi baru bagi pengembangan hukum forensik siber yang berorientasi pada keadilan.

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan multidisipliner yang menggabungkan analisis yuridis-dogmatik dengan konsep-konsep dari ilmu komputer dan etika profesional (Muhaimin, 2020). Pendekatan perundang-undangan (*statute approach*) dilakukan untuk meninjau sinkronisasi antara UU ITE, KUHAP Indonesia, dan instrumen hukum internasional seperti Konvensi Budapest tentang Kejahatan Siber. Pendekatan konseptual (*conceptual approach*) digunakan untuk membedah teori-teori keadilan, termasuk *Theory of Justice* dari John Rawls dan etika deontologis Immanuel Kant, yang kemudian diterapkan pada praktik forensik digital.

Data yang digunakan bersumber dari bahan hukum sekunder yang mencakup literatur asing dari basis data jurnal bereputasi (MDPI, Cambridge Core, Springer, Frontiers) dan dokumen standar internasional (ISO/IEC 27037, NIST SP 800-86). Analisis dilakukan secara deskriptif-analitis dengan membandingkan praktik ajudikasi bukti digital di berbagai yurisdiksi, seperti Amerika Serikat, Uni Eropa, dan Arab Saudi, guna memberikan rekomendasi bagi sistem hukum Indonesia (Rustamaji et al., 2026). Fokus utama analisis terletak pada identifikasi celah antara kapabilitas teknologi forensik dengan perlindungan hak-hak prosedural terdakwa, yang kemudian disintesis menjadi sebuah kerangka kerja tata kelola bukti digital yang etis dan adil.

3. HASIL & PEMBAHASAN

Integritas Teoritis dan Etika Forensik Digital: Melampaui Validasi Teknis melalui Integrasi Standar Internasional

Dalam ranah forensik digital, etika bukan sekadar pelengkap profesi, melainkan fondasi yang menentukan validitas ontologis dari bukti yang dihadirkan di pengadilan. Dasar dari seluruh ilmu forensik, termasuk forensik siber, adalah *Locard's Exchange Principle* yang menyatakan bahwa "setiap kontak meninggalkan jejak" (Palmer, 2016).

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

Dalam dunia fisik, jejak ini mungkin berupa debu atau serat, namun dalam dunia digital, jejak tersebut bermanifestasi dalam bentuk perubahan status magnetik, log transaksi, atau metadata yang seringkali tidak terlihat tanpa alat bantu khusus (Wikipedia, 2026). Tantangan etis pertama muncul ketika investigator menyadari bahwa tindakan pemeriksaan itu sendiri adalah sebuah "kontak" yang berpotensi mengubah bukti asli. Oleh karena itu, prinsip etika fundamental mewajibkan penggunaan prosedur yang menjamin bahwa data asli tetap murni, biasanya melalui pembuatan citra forensik bit-demi-bit (*forensic imaging*) dan penggunaan fungsi *hash* kriptografis sebagai sidik jari digital (Aleke & Trigui, 2025).

Integritas bukti digital secara etis harus diukur melalui kacamata Standar Daubert, sebuah tolok ukur hukum yang berasal dari yurisprudensi Amerika Serikat (1993) untuk menilai reliabilitas bukti ilmiah (Ismail & Ariffin, 2025). Standar ini mengharuskan alat forensik yang digunakan diuji secara ketat, memiliki tingkat kesalahan (*error rate*) yang diketahui, telah melalui tinjauan sejawat (*peer review*), dan diterima secara umum oleh komunitas ilmiah (Ismail & Ariffin, 2025). Secara etis, seorang ahli forensik siber melanggar kewajiban profesionalnya jika ia menggunakan alat atau metode yang belum tervalidasi, karena hal ini dapat menyesatkan hakim dan berujung pada hukuman yang salah (*wrongful conviction*) (Imam, 2017).

Penting untuk dicatat bahwa validasi alat ini menjadi semakin kompleks dengan munculnya alat forensik berbasis kecerdasan buatan (AI). AI menjanjikan kecepatan dalam menganalisis dataset yang masif, namun algoritma AI seringkali bersifat *black box* yang tidak transparan (Mandayam, 2025). Secara etis, penggunaan AI dalam forensik harus mematuhi prinsip akuntabilitas dan *"explainability"* (keterjelasan). Jika seorang investigator tidak dapat menjelaskan bagaimana sebuah algoritma AI menyimpulkan bahwa sebuah file adalah ilegal, maka bukti tersebut secara etis cacat karena tidak dapat diuji silang oleh pihak pembela (Mandayam, 2025). Hal ini selaras dengan kode etik IEEE

dan ACM yang menekankan kewajiban profesional untuk menghindari bahaya dan menghormati privasi serta hak asasi manusia (Association for Computing Machinery, 2018).

Kerangka kerja etika yang lebih komprehensif dapat ditemukan dalam proposal PRECEPT (*Privacy-Respecting EthiCal framEwork*). Kerangka kerja ini mengaplikasikan teori keadilan John Rawls, khususnya prinsip kebebasan dan kesetaraan, ke dalam tahapan investigasi digital (Ferguson et al., 2020). Dalam pandangan Rawlsian, ketidaksetaraan dalam akses terhadap data atau teknologi hanya dapat dibenarkan jika hal tersebut menguntungkan pihak yang paling tidak beruntung atau diperlukan untuk mencegah kerugian yang lebih besar bagi masyarakat (Ferguson et al., 2020). Etika forensik menuntut investigator untuk bertindak berdasarkan *categorical imperative* Kant: bertindaklah hanya berdasarkan aturan yang Anda inginkan menjadi hukum universal (Ferguson et al., 2020). Jika investigator melakukan penyitaan data yang melampaui batas kewenangan tanpa izin yang sah, ia telah melanggar prinsip etika dasar yang menjunjung tinggi supremasi hukum.

Standar internasional ISO/IEC 27037 memberikan pedoman teknis yang bermuatan etis bagi identifikasi, pengumpulan, akuisisi, dan pelestarian bukti digital (Konfirmity Pte Ltd, 2026). Standar ini menekankan pentingnya auditabilitas dan repetibilitas—bahwa ahli lain dengan alat yang sama harus dapat menghasilkan temuan yang identik dari data yang sama (Morić et al., 2026). Tanpa auditabilitas, hasil forensik siber hanyalah klaim otoritatif sepihak yang tidak memiliki dasar keadilan prosedural.

Komponen Etika Forensik Digital	**Instrumen/Teori Pendukung**	**Implikasi Yuridis**
Objektivitas dan Ketidakberpihakan	ISFCE Code of Ethics	Ahli tidak boleh menjadi advokat bagi klien, melainkan bagi kebenaran data (Imam, 2017).

Transparansi Metodologi	Daubert Standard	Metode harus dapat diuji ulang dan tingkat kesalahan harus diungkapkan (Ismail & Ariffin, 2025).
Perlindungan Privasi	Rawls' Theory of Justice	Pengumpulan data harus proporsional dan tidak boleh melanggar hak privasi tanpa dasar hukum (Ferguson et al., 2020).
Akuntabilitas Algoritmik	Explainable AI (XAI)	Hasil analisis AI harus dapat dijelaskan logikanya di persidangan (Mandayam, 2025).
Integritas Data	ISO/IEC 27037	Rantai penjagaan harus terdokumentasi dengan hashing kriptografis di setiap tahap (Bhatti, 2026).

Dalam konteks operasional, ahli forensik seringkali menghadapi dilema antara tekanan untuk memberikan bukti yang cukup bagi penuntutan (*pressure to secure a conviction*) dengan kewajiban etis untuk mengungkapkan bukti yang meringankan (*exculpatory evidence*) (Ferguson et al., 2020). Kode etik DFCB dan ISFCE secara tegas melarang penyembunyian temuan yang dapat mengubah fakta kasus (Digital Forensics Certification Board, 2026). Keadilan dalam forensik digital dimulai dari laboratorium; jika proses di laboratorium sudah bias, maka keadilan di ruang sidang tidak akan pernah tercapai. Oleh karena itu, standarisasi laboratorium forensik nasional yang independen menjadi imperatif etis untuk menjamin bahwa bukti yang diajukan benar-benar representasi jujur dari realitas digital (Setiawan & Hartiwiningsih, 2024).

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

Keadilan Prosedural dan *Equality of Arms* dalam Pembuktian Digital di Persidangan: Tantangan dan Reformasi Hukum di Indonesia

Keadilan prosedural adalah inti dari legitimasi sistem peradilan pidana (Ashalirrohman, 2024). Dalam kasus-kasus yang melibatkan bukti digital, keadilan prosedural seringkali terancam oleh fenomena "digital divide" atau kesenjangan teknologi antara penuntut dan terdakwa (Bhatti, 2026). Prinsip *Equality of Arms* (Kesetaraan Senjata) mengharuskan setiap pihak dalam persidangan memiliki kesempatan yang sama untuk mengajukan kasusnya tanpa ditempatkan pada posisi yang sangat tidak menguntungkan dibandingkan lawannya (Ramos, 2023). Namun, dalam praktiknya, negara memiliki akses hampir tak terbatas terhadap alat forensik mahal dan basis data intelijen siber, sementara terdakwa seringkali kesulitan bahkan untuk mendapatkan salinan data mereka sendiri yang telah disita (Filletti, 2026).

Kasus nyata di Indonesia memberikan ilustrasi yang tajam mengenai pentingnya otentikasi bukti digital. Dalam Putusan Nomor 488/Pid.B/2024/PN Sda, majelis hakim menolak bukti *screenshot* percakapan yang diajukan karena tidak melalui proses verifikasi forensik yang menjamin integritasnya (Tiba, 2025). Keputusan ini menunjukkan pemahaman yudisial bahwa tanpa prosedur forensik (identifikasi, pelestarian, analisis, pelaporan), data digital sangat rentan terhadap rekayasa (Tiba, 2025). Namun, keputusan ini juga menimbulkan pertanyaan tentang keadilan: bagaimana jika terdakwa yang tidak bersalah tidak memiliki biaya untuk menyewa ahli forensik guna membuktikan bahwa *screenshot* tersebut adalah asli? Inilah mengapa konsep *"Equality of Digital Arms"* memerlukan dukungan negara melalui penyediaan ahli forensik bagi pihak pembela atau akses ke laboratorium independen (Filletti, 2026).

Mahkamah Pidana Internasional (ICC) telah mengembangkan model tiga tahap untuk menilai penerimaan bukti digital yang dapat menjadi rujukan bagi reformasi hukum di Indonesia (Sangari & Mohammadi, 2025):

a. Relevansi: Menentukan apakah bukti tersebut memiliki kaitan logis dengan fakta yang diperdebatkan.
b. Nilai Pembuktian (*Probative Value*): Menilai keandalan bukti berdasarkan integritas metadata, sumber, dan rantai penjagaan.
c. Efek Merugikan (*Prejudicial Effect*): Menimbang apakah potensi prasangka yang timbul dari bukti tersebut (misalnya jika diperoleh melalui pelanggaran privasi yang berat) jauh melebihi nilai pembuktiannya.

Di Indonesia, Pasal 5 ayat (1) dan (2) UU ITE telah mengakui informasi elektronik sebagai alat bukti yang sah, namun Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 memberikan batasan penting bahwa bukti elektronik berupa penyadapan hanya sah jika diperoleh dalam rangka penegakan hukum atas permintaan resmi kepolisian atau kejaksaan (Pramata, 2020). Hal ini merupakan perwujudan dari *Exclusionary Rule*, di mana bukti yang diperoleh secara ilegal (*unlawful legal evidence*) harus dikesampingkan oleh hakim untuk melindungi hak asasi manusia (Rustamaji et al., 2026). Namun, seiring dengan berlakunya UU No. 1 Tahun 2024, tantangan baru muncul terkait interpretasi pasal-pasal yang dianggap multitafsir, seperti Pasal 27A dan 28 ayat (2) UU ITE, yang seringkali menggunakan bukti digital sebagai instrumen untuk membatasi kebebasan berpendapat (Sukarta et al., 2025).

Keadilan prosedural juga menuntut adanya transparansi dalam *"Digital Chain of Custody"*. Rantai penjagaan digital tidak hanya mencatat siapa yang memegang perangkat, tetapi juga setiap akses bit-level terhadap data tersebut (Bhatti, 2026). Penggunaan teknologi mutakhir seperti *blockchain* untuk mencatat log aktivitas forensik mulai diusulkan oleh para peneliti internasional untuk memastikan bahwa catatan audit tidak dapat diubah *(immutable),* sehingga memperkuat kepercayaan antara pihak-pihak yang bersengketa (Haji et al., 2026).

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

Perbandingan Standar Admissibility Bukti Digital	**Amerika Serikat (Daubert/FRE)**	**Uni Eropa (ECHR Article 6)**	**Indonesia (UU ITE/KUHAP)**
Kriteria Utama	Reliabilitas Ilmiah & Relevansi (Palmer, 2016).	Fairness & Equality of Arms (Ramos, 2023).	Keabsahan Perolehan & Integritas Sistem (Tiba, 2025).
Peran Hakim	*Gatekeeper* (Penjaga Pintu Ilmu) (Lasagni, 2025).	Pelindung Hak Asasi Prosedural (Filletti, 2026).	Penilai Formal & Materiil Bukti (Rustamaji et al., 2026).
Status Hearsay	Pengecualian untuk Catatan Bisnis/Otomatis (Wang et al., 2024).	Fokus pada Hak Konfrontasi (Filletti, 2026).	Diperlakukan sebagai Bukti Surat/Ahli (Herman et al., 2024).
Kebutuhan Ahli	Mandatori untuk Kesaksian Ilmiah (Ismail & Ariffin, 2025).	Hak atas Akses Ahli Independen (Filletti, 2026).	Bergantung pada Diskresi Hakim/Penyidik (Rustamaji et al., 2026).

Salah satu reformasi krusial yang diusulkan dalam literatur asing adalah legislasi *Digital Habeas Corpus* (Filletti, 2026). Dalam hukum tradisional, *Habeas Corpus* melindungi individu dari penahanan ilegal; dalam era digital, ini berarti melindungi "kehidupan digital" seseorang dari penyitaan tanpa batas tanpa hak akses bagi pemiliknya untuk membela diri. Jika negara menyita seluruh data digital seseorang, negara secara etis dan hukum berkewajiban untuk memberikan salinan yang dapat digunakan oleh terdakwa untuk mencari bukti yang membebaskan dirinya (Filletti, 2026). Tanpa hak ini, persidangan digital hanyalah sebuah formalitas administratif yang menjustifikasi kehendak negara.

Pendidikan yudisial juga menjadi faktor penentu keadilan. Studi di Saudi Arabia menunjukkan bahwa meskipun kesiapan penuntut tinggi, kompetensi hakim dalam mengelola bukti digital seringkali dinilai rendah atau menengah (Aleisa, 2026). Hal serupa juga teridentifikasi dalam riset di Indonesia, di mana terdapat ketidakkonsistenan dalam penerapan prosedur otentikasi antar pengadilan (Vanessa & Firmansyah, 2025). Hakim tidak perlu menjadi ahli komputer, tetapi mereka harus memiliki "literasi digital fungsional" untuk memahami kapan sebuah metadata file terlihat mencurigakan atau kapan sebuah rantai penjagaan dianggap cacat (Rustamaji et al., 2026). Akhirnya, keadilan prosedural dalam siber forensik harus bersandar pada empat pilar: standar hukum yang jelas, integritas forensik yang teruji, rantai penjagaan yang transparan, dan penghormatan mutlak terhadap hak asasi manusia (Bhatti, 2026).

4. KESIMPULAN

Penggunaan bukti digital dalam persidangan merupakan tantangan multidimensional yang menguji ketahanan etika profesi forensik dan prinsip keadilan hukum. Secara teoritis, integrasi standar ilmiah global seperti Daubert dengan kerangka kerja etika PRECEPT yang berbasis pada teori keadilan John Rawls memberikan jalan keluar untuk mengatasi "data fundamentalism" yang sering mengabaikan margin kesalahan teknologi. Etika forensik digital menuntut lebih dari sekadar ketepatan teknis; ia mengharuskan transparansi metodologis, terutama dalam menghadapi algoritma kecerdasan buatan yang bersifat *black box*.

Keadilan prosedural dalam sistem peradilan pidana Indonesia hanya dapat terwujud jika terdapat kesetaraan akses terhadap teknologi forensik. Konsep *Equality of Digital Arms* dan hak *Digital Habeas Corpus* harus mulai diinternalisasi ke dalam hukum acara nasional untuk mencegah ketidakseimbangan kekuasaan antara negara dan individu. Putusan-putusan pengadilan terbaru di Indonesia menunjukkan kesadaran yudisial yang

meningkat akan pentingnya verifikasi forensik, namun inkonsistensi praktis masih tetap ada akibat kesenjangan kompetensi teknis di kalangan hakim.

Sebagai rekomendasi, diperlukan pembentukan standar prosedur operasional nasional yang selaras dengan ISO/IEC 27037 dan penguatan peran laboratorium forensik independen yang dapat diakses oleh pihak pembela. Reformasi hukum juga harus diarahkan pada penguatan peran hakim sebagai *gatekeeper* yang aktif dalam menilai reliabilitas alat forensik, bukan sekadar penerima pasif dari laporan ahli. Dengan menempatkan etika dan keadilan sebagai kompas dalam setiap bit data yang dianalisis, forensik siber akan berfungsi sebagai instrumen pencari kebenaran yang hakiki, yang melindungi yang tidak bersalah sekaligus menghukum yang bersalah berdasarkan bukti yang tak terbantahkan.

5. REFERENSI

Aleisa, N. (2026). The Study of Digital Forensics in KSA: Education, and Prosecution Capabilities: A Needs-Based Analysis. *Electronics*, *15*(2). https://doi.org/10.3390/electronics15020316

Aleke, N. T., & Trigui, M. (2025). Legal and Ethical Challenges in Digital Forensics Investigations. In *Digital Forensics in the Age of AI*. IGI Global Scientific Publishing.

Ashalirrohman, Y. (2024). Asset Forfeiture for the Offense of Illicit Enrichment: Between Eradication and Deterrence. *Lex Journal: Kajian Hukum Dan Keadilan*, *8*(1), 1–12.

Association for Computing Machinery. (2018). *ACM Code of Ethics and Professional Conduct*. https://www.acm.org/code-of-ethics

Bhatti, N. (2026). The Use of Digital Evidence in Criminal Proceedings. *American Journal of Society and Law*, *5*(1), 10–19. https://doi.org/10.54536/ajsl.v5i1.7211

Digital Forensics Certification Board. (2026). *Code of Ethics and Standards of Professional Conduct*. https://dfcb.org/code-of-ethics-and-standards-of-professional-conduct/

Ferguson, R. I., Renaud, K., Wilford, S., & Irons, A. (2020). Precept: a framework for

ethical digital forensics investigations. *Journal of Intellectual Capital*, 1–29. https://doi.org/10.1108/JIC-05-2019-0097

Filletti, S. (2026). Efficiency over Equity: Why the Speed of Digital Investigation Extinguishes Defence Rights. *Malta Journal of Legal Studies*, 1–8. https://brill.com/view/journals/mjls/aop/article-10.1163-30508762-00000008/article-10.1163-30508762-00000008.xml?ebody=pdf-130820

Haji, I. A., Mohammed, S. D., & Mousa, K. M. (2026). Blockchain based chain of custody and digital evidence legality in post conflict prosecutions. *Frontiers Media SA*, *9*. https://doi.org/10.3389/fbloc.2026.1801364

Herman, Handrawan, Haris, O. K., Abdullah, S. A., Rizky, A., & Indah, S. R. (2024). Use of Digital Forensics in Proofing the Criminal Offense of Damage to Good Name in Social Media Based on the Law of Information and Electronic Transactions. *Halu Oleo Legal Research*, *6*(2), 588–603.

Imam, F. (2017). *Computer Forensics: Legal and Ethical Principles*. https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-legal-ethical-principles/

Ismail, I., & Ariffin, K. A. Z. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLoS One*, *20*(9). https://doi.org/10.1371/journal.pone.0331683

Konfirmity Pte Ltd. (2026). *ISO/IEC 27037: Understanding its role in compliance and security (2026)*. https://www.konfirmity.com/glossary/iso-iec-27037

Lasagni, G. (2025). Admissibility of Digital Evidence. In V. Franssen & S. Tosza (Eds.), *The Cambridge Handbook of Digital Evidence in Criminal Investigations* (pp. 126–152). Cambridge University Press.

Mandayam, R. (2025). Ethical Considerations in Digital Forensic. *International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences*, *13*(1), 1–4.

Morić, Z., Dakić, V., & Biškupić, I. O. (2026). An Empirical Assessment of Digital Forensic Process Reliability Using Integrated ISO/IEC 27037 and 27041 Standards. *Journal of Cybersecurity and Privacy*, *6*(2). https://doi.org/10.3390/jcp6020057

Muhaimin. (2020). *Metode Penelitian Hukum*. Mataram University Press.

Palmer, G. (2016). *Locard's Exchange Principle and the Daubert Test*. https://zymitry.com/locards-exchange-principle-daubert-test/

Pramata, A. G. (2020). Analisis Kekuatan dan Nilai Pembuktian Alat Bukti Elektronik Berwujud CCTV (Closed Circuit Television) Pasca Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 dalam Hukum Acara Pidana. *Jurnal Verstek*, *8*(3), 392–400.

Ramos, V. C. (2023). The EPPO and the equality of arms between the prosecutor and the defence. *New Journal of European Criminal Law*, 1–28. https://doi.org/10.1177/20322844231157078

Rustamaji, M., Sitompul, S. M., & Khoiruddin, A. R. (2026). Reforming the Role of Judges in Assessing Evidence Authenticity and Legality: A Comparative Study Using the Exclusionary Rule Approach. *Media Iuris*, *9*(1), 153–180. https://doi.org/10.20473/mi.v9i1.77218

Sangari, ziba N., & Mohammadi, A. (2025). Admissibility of Digital Evidence at the International Criminal Court. *Journal of Criminal Law Research*, *13*(48), 41–84. https://doi.org/10.22054/jclr.2025.81549.2697

Setiawan, E., & Hartiwiningsih. (2024). Pemanfaatan Digital Forensik dan Teknologi Informasi dalam Proses Pembuktian Tindak Pidana Pemalsuan Dokumen Elektronik. *Prosiding APPIHI*. https://prosiding.appihi.or.id/index.php/PROSEMNASHUK/article/download/39/39

Sukarta, D. T. W., Akbar, M. G. G., & Abas, M. (2025). Akibat Hukum Pasca Putusan Mahkamah Konstitusi tentang Kerusuhan dalam Ruang Siber Bukan Sebagai Tindak Pidana (Studi Putusan Nomor 105/PUU-XXII/2024). *Jurnal Ilmu Hukum, Humaniora Dan Politik (JIHHP)*, *6*(1), 306–315.

Tiba, S. K. S. (2025). Implikasi Penolakan Bukti Elektronik Tanpa Verifikasi Digital Forensik: Studi Putusan dan Analisis Yuridis. *Media Hukum Indonesia (MHI)*, *4*(1), 865–868. https://doi.org/10.5281/zenodo.17946561

Vanessa, & Firmansyah, H. (2025). Analysis of the Validity of Electronic Evidence in Criminal Trial Proceedings and the Implementation of Its Admissibility (Judgment Study). *Indonesian Journal of Law and Economics Review*, *20*(4). https://doi.org/10.21070/ijler.v20i4.1395

Wang, X., Wu, Y. C., & Ma, Z. (2024). Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in U.S. judicial processes. *Frontiers Blockchain*, *7*. https://doi.org/10.3389/fbloc.2024.1306058

Wikipedia. (2026). *Locard's exchange principle*. https://en.wikipedia.org/wiki/Locard%27s_exchange_principle