

## Analisis Kepatuhan Forensik Elektronik dalam Pembuktian Tindak Pidana Siber di Indonesia

### *Electronic Forensic Compliance in Proving Cybercrimes in Indonesia*

Harison Tutu Tumanggor, Hilbertus Sumplisius M. Wau

Fakultas Hukum, Universitas Sumatera Utara, Medan

\*Penulis korespondensi: Harisontumanggor0@gmail.com

Naskah masuk:  
4 Desember 2025  
Review:  
22 April 2026  
Diterima:  
17 Oktober 2026  
Diterbitkan:  
17 Oktober 2026  
Keywords  
Electronic evidence;  
Digital forensics;  
Compliance;  
Authentication;  
Criminal procedure.

**Abstract.** This study formulates parameters for electronic forensic compliance and examines their consequences for proving cybercrimes in Indonesia. It employs doctrinal legal research through statutory, conceptual, and judicial decision analysis, supported by a limited functional comparison with international scholarship. Legal materials are examined through systematic interpretation and prescriptive reasoning. The findings identify four assessment dimensions: lawful acquisition, integrity and authentication, methodological reliability, and meaningful opportunities to challenge evidence. The 2025 Criminal Procedure Code expressly recognizes electronic evidence and requires authentication, making the mere existence of digital files or expert reports insufficient. Hash discrepancies and documentation deficiencies must be evaluated according to their objects, stages, and consequences; neither independently establishes an offender's guilt. The study proposes continuous documentation, task-specific validation, peer review, and adversarial testing as quality safeguards. These measures distinguish evidence that cannot legally be used from evidence requiring a more cautious assessment of probative weight.

Kata Kunci  
Bukti elektronik;  
Forensik digital;  
Kepatuhan;  
Autentikasi; Hukum  
acara pidana.

**Abstrak.** Penelitian ini bertujuan merumuskan parameter kepatuhan forensik elektronik dan akibat hukumnya terhadap pembuktian tindak pidana siber di Indonesia. Penelitian hukum normatif ini menggunakan pendekatan perundang-undangan, konseptual, dan analisis putusan, dengan perbandingan fungsional terbatas terhadap literatur internasional. Bahan hukum dianalisis secara kualitatif melalui penafsiran sistematis dan argumentasi preskriptif. Hasil penelitian menunjukkan bahwa kepatuhan perlu dinilai melalui legalitas perolehan, integritas dan autentikasi, keandalan metode, serta keterbukaan pengujian. KUHAP 2025 mempertegas pengakuan bukti elektronik dan pengujian autentikasi, sehingga penilaian tidak cukup bertumpu pada keberadaan berkas digital atau laporan ahli. Ketidakcocokan nilai hash dan kekurangan dokumentasi harus diperiksa menurut objek, tahap, dan dampaknya; keduanya tidak membuktikan kesalahan pelaku secara mandiri. Penelitian mengusulkan dokumentasi berkesinambungan, validasi berbasis tugas, pemeriksaan sejawat, dan pengujian kontradiktor sebagai perangkat pengendalian mutu. Implikasinya adalah pemisahan yang tegas antara bukti yang tidak dapat digunakan dan bukti yang memerlukan penilaian bobot secara lebih hati-hati.

## 1 Pendahuluan

Pembuktian tindak pidana siber menghadapi hukum acara pidana pada persoalan yang lebih luas daripada penemuan berkas elektronik. Penyidik dapat menemukan percakapan, rekaman, transaksi, atau riwayat akses, tetapi keberadaan data tersebut belum menjawab apakah data diperoleh secara sah, tetap utuh, ditafsirkan dengan benar, dan benar-benar berkaitan dengan orang yang didakwa. Persoalannya terletak pada hubungan antara proses memperoleh pengetahuan teknis dan kewenangan hukum untuk menggunakan pengetahuan itu. Karena itu, keberhasilan pembuktian tidak dapat diukur semata-mata dari banyaknya data yang berhasil diekstraksi. Kualitas hubungan antara sumber data, prosedur pemeriksaan, dan kesimpulan mengenai peristiwa pidana harus dapat diuji oleh para pihak.

Literatur forensik menunjukkan bahwa penambahan kapasitas penyimpanan dan banyaknya perangkat dapat memperpanjang pemeriksaan serta menimbulkan penumpukan pekerjaan. Pengurangan data dan penentuan prioritas menjadi penting, tetapi pilihan tersebut juga menentukan informasi yang terlihat dan informasi yang mungkin terlewat. Dengan demikian, efisiensi pemeriksaan mempunyai dimensi hukum: pemilihan data harus dapat dijelaskan agar informasi yang menguntungkan tersangka tidak diabaikan. Kajian mengenai volume data serta penggabungan data forensik dan informasi sumber terbuka membantu menjelaskan kebutuhan tersebut, tanpa menghilangkan kewajiban memeriksa relevansi setiap informasi terhadap perkara tertentu (Quick & Choo, 2014, 2018).

Dalam konteks Indonesia, persoalan ini memperoleh perkembangan normatif penting setelah berlakunya Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana pada 2 Januari 2026. Pasal 235 ayat (1) huruf f secara tegas memasukkan bukti elektronik dalam jenis alat bukti. Pasal 235 ayat (3) sampai dengan ayat (5) kemudian mensyaratkan autentikasi dan perolehan yang tidak melawan hukum serta memberikan kewenangan penilaian kepada hakim. Oleh sebab itu, pembahasan terkini tidak tepat lagi berangkat dari anggapan bahwa hukum acara umum sama sekali belum mengakui bukti elektronik. Analisis harus beralih pada cara mengoperasionalkan pengakuan tersebut secara bertanggung jawab (Republik Indonesia, 2025).

Pengakuan normatif itu melanjutkan perkembangan melalui Undang-Undang Informasi dan Transaksi Elektronik yang terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024. Akan tetapi, pengakuan terhadap kategori bukti berbeda dari pembuktian autentikasi suatu objek tertentu. Sebuah tangkapan layar dapat memperlihatkan pesan, tetapi belum dengan sendirinya memastikan kelengkapan percakapan, identitas pengirim, atau cara data diperoleh. Begitu pula, kepemilikan perangkat belum tentu menunjukkan siapa pengguna perangkat pada waktu peristiwa terjadi. Perbedaan tersebut penting agar perluasan alat bukti tidak berubah menjadi perluasan asumsi mengenai kesalahan seseorang (Republik Indonesia, 2008, 2016, 2024).

Penelitian terdahulu memberikan landasan yang relevan. Ramiyanto membahas kedudukan bukti elektronik sebagai alat bukti yang berdiri sendiri maupun perluasan alat bukti dalam kerangka hukum sebelum KUHAP 2025. Hartono dan Yuliartini menekankan legalitas perolehan, dukungan pemeriksaan digital, dan kesempatan menyangkal. Medeline dan rekan-rekan menghubungkan forensik digital dengan pembuktian kepemilikan akun dalam perkara

ujaran kebencian. Ketiganya memperlihatkan bahwa pengakuan jenis bukti harus diikuti pemeriksaan terhadap proses dan hubungan bukti dengan subjek hukum. Namun, kerangka historis masing-masing penelitian perlu dibaca sesuai periode hukumnya, bukan langsung diperlakukan sebagai deskripsi hukum yang berlaku sekarang (Hartono & Yulianti, 2020; Medeline et al., 2022; Ramiyanto, 2017).

Literatur internasional memperluas perhatian pada keandalan pemeriksaan. Penelitian tentang keadilan proses menunjukkan risiko ketika teknologi diperlakukan seolah-olah selalu menghasilkan informasi yang benar. Kajian validasi juga membedakan pengujian teknologi, metode, dan penerapannya dalam perkara. Sementara itu, telaah mengenai mutu forensik menegaskan perlunya pengendalian terhadap pekerjaan pemeriksa, termasuk penafsiran dan pelaporan. Sumbangan literatur tersebut bukan menyediakan aturan yang langsung mengikat pengadilan Indonesia, melainkan memperjelas jenis persoalan yang perlu dijawab agar penilaian hukum tidak berhenti pada reputasi perangkat lunak atau sertifikasi pemeriksa (Page et al., 2019; Stoykova, 2021; Stoykova & Franke, 2023).

Kajian nasional mengenai kejahatan teknologi informasi menempatkan penanggulangan kejahatan dalam hubungan dengan perkembangan sistem hukum. Kajian tentang penegakan hukum terhadap peretasan juga menguraikan persoalan kemampuan penyidik, sarana, dan yurisdiksi. Kedua penelitian tersebut menunjukkan bahwa penanggulangan kejahatan memerlukan dukungan kapasitas dan penataan kewenangan secara bersamaan. Namun, pernyataan mengenai kendala harus diperlakukan sesuai ruang lingkup penelitian masing-masing. Penelitian ini tidak mengubahnya menjadi data mutakhir mengenai semua unit penyidikan. Perbedaan antara hasil kajian terdahulu dan temuan penelitian sekarang menjaga argumentasi tetap dapat ditelusuri serta menghindari generalisasi yang tidak mempunyai dasar empiris (Arisandy, 2021; Habibi & Liviani, 2020).

Kesenjangan yang dibahas penelitian ini terletak pada belum terpadunya hubungan antara kewenangan memperoleh bukti, mutu proses forensik, dan konsekuensi penilaian bukti setelah perubahan hukum acara. Pembahasan teknis sering menempatkan nilai hash dan rantai penguasaan sebagai jaminan menyeluruh, sedangkan pembahasan hukum dapat berhenti pada pengakuan formal bukti elektronik. Penelitian ini mempertemukan kedua wilayah tersebut melalui parameter yang mengharuskan pemeriksa menjelaskan kewenangan, identitas objek, proses transformasi, dasar interpretasi, dan kemungkinan pengujian. Kebaruan yang diajukan merupakan konstruksi analitis dan preskriptif, bukan klaim penemuan pertama secara universal atau hasil pengukuran kepatuhan nasional.

Berdasarkan persoalan tersebut, penelitian mengajukan tiga rumusan masalah. Pertama, bagaimana kedudukan dan persyaratan penggunaan bukti elektronik dalam kerangka hukum acara pidana Indonesia setelah KUHAP 2025? Kedua, bagaimana hubungan antara standar teknis forensik, teori sistem hukum, dan penilaian autentikasi serta keandalan bukti? Ketiga, bagaimana akibat ketidakpatuhan dan bentuk pengendalian prosedural yang diperlukan untuk menjaga pembuktian yang adil? Tujuannya ialah menghasilkan parameter penilaian yang dapat digunakan secara berurutan oleh penyidik, pemeriksa, penuntut umum, hakim, dan advokat. Parameter tersebut diharapkan memperjelas alasan menerima, mengesampingkan, atau membatasi bobot suatu bukti.

## **2 Metode Penelitian**

Penelitian ini merupakan penelitian hukum normatif atau doktrinal. Objek kajiannya adalah hubungan antara norma kewenangan, persyaratan bukti, dan prinsip pemeriksaan forensik elektronik. Pendekatan perundang-undangan digunakan untuk membaca KUHAP 2025 bersama UU ITE dalam versi perubahannya, sedangkan KUHAP 1981 ditempatkan sebagai kerangka historis dan aturan yang masih relevan melalui ketentuan peralihan. Pendekatan konseptual digunakan untuk membedakan legalitas, autentikasi, integritas, keandalan, dan bobot pembuktian. Analisis putusan dipusatkan pada Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 karena pertimbangannya menjelaskan hubungan perolehan bukti, penyadapan, dan perlindungan hak.

Bahan hukum primer meliputi undang-undang dan salinan resmi putusan tersebut. Bahan hukum sekunder mencakup buku literatur serta artikel jurnal nasional dan internasional mengenai pembuktian elektronik, validasi, bias pemeriksa, dokumentasi, dan tata kelola forensik. Artikel dalam koleksi bahan hukum penulis digunakan setelah isi dan identitas bibliografinya diperiksa. Penelusuran tambahan dilakukan pada laman penerbit, repositori institusi, dan metadata DOI sampai 17 Oktober 2026. Seleksi didasarkan pada hubungan langsung dengan persoalan penelitian dan keterlacakan sumber. Artikel yang tidak tersedia secara lengkap digunakan sebatas informasi yang dapat diverifikasi pada abstrak atau laman penerbit. Penelitian ini tidak menggunakan prosedur tinjauan sistematis, sehingga tidak mengklaim telah mencakup seluruh publikasi atau menghasilkan pemeringkatan mutu seluruh jurnal.

Analisis dilaksanakan dengan menginventarisasi norma, mengidentifikasi fungsi setiap persyaratan, lalu menghubungkannya dengan risiko pada tahapan penanganan bukti. Penafsiran sistematis digunakan untuk menghindari pembacaan terpisah antara pengakuan jenis bukti dan persyaratan autentikasinya. Perbandingan fungsional terbatas terhadap literatur internasional dipakai untuk menilai kegunaan mekanisme validasi dan pemeriksaan sejawat, bukan untuk memindahkan hukum asing secara langsung. Pembahasan atas putusan pengadilan negeri yang terdapat dalam artikel sekunder dinyatakan sebagai pembacaan melalui sumber tersebut. Penelitian tidak melakukan wawancara, pemeriksaan laboratorium, audit lembaga, atau penghitungan putusan nasional; karena itu, kesimpulannya bersifat normatif dan tidak menyatakan besaran ketidakpatuhan dalam praktik.

## **3 Hasil Penelitian dan Pembahasan**

### **3.1 Kedudukan bukti elektronik dan keberlakuan hukum acara**

Temuan normatif pertama adalah perlunya memisahkan pertanyaan mengenai jenis alat bukti dari pertanyaan mengenai mutu objek yang diajukan. Pasal 242 KUHAP 2025 mencakup informasi elektronik, dokumen elektronik, dan/atau sistem elektronik yang berkaitan dengan tindak pidana. Cakupan tersebut tidak menghapus kebutuhan menunjukkan hubungan antara objek yang diperiksa dan peristiwa yang didakwakan. Penyebutan sebuah perangkat dalam daftar barang bukti belum menjelaskan informasi apa yang diambil darinya. Berkas hasil ekspor juga memerlukan penjelasan mengenai sumber, cara ekstraksi, waktu pemeriksaan, dan keterbatasan hasilnya. Pengakuan kategori merupakan pintu masuk, bukan kesimpulan akhir mengenai fakta pidana (Republik Indonesia, 2025).

KUHAP 1981 tetap perlu dijelaskan secara tepat. Pasal 183 dan Pasal 184 dahulu membentuk kerangka umum pemidanaan dan jenis alat bukti, sedangkan UU ITE beserta perubahannya memberikan pengaturan khusus mengenai informasi dan dokumen elektronik. Penggunaan ketentuan lama dalam penelitian terdahulu dapat dipahami dari waktu terbitnya. Namun, pengulangan pernyataan bahwa KUHAP hanya mengenal lima alat bukti tanpa penjelasan waktu akan menyesatkan pembaca pada 2026. Pasal 361 KUHAP 2025 mengatur beberapa keadaan peralihan berdasarkan tahap penanganan perkara. Dengan demikian, penentuan aturan acara tidak cukup hanya melihat tanggal tindak pidana; tahap penyidikan, penuntutan, dan pemeriksaan pengadilan juga perlu diketahui (Republik Indonesia, 1981, 2025).

Kerangka tersebut mempunyai akibat praktis bagi penyusunan laporan ahli. Laporan sebaiknya menyebut dasar kewenangan tindakan, tahapan perkara, dan objek yang menjadi lingkup pemeriksaan. Pemeriksa tidak perlu mengambil alih tugas hakim menentukan hukum yang berlaku, tetapi harus memberikan fakta prosedural yang memungkinkan penilaian itu. Apabila informasi mengenai tanggal atau dasar penyitaan tidak tersedia, kekurangan tersebut perlu dinyatakan, bukan ditutup dengan pernyataan umum bahwa pemeriksaan telah sesuai prosedur. Kejelasan semacam ini menghindari pencampuran antara kompetensi teknis pemeriksa dan kewenangan yudisial menilai sahnyalah perolehan bukti. Pembagian tanggung jawab justru memperkuat kemampuan setiap pihak menguji persoalan dalam ruang kewenangannya.

Persyaratan dalam UU ITE mengenai aksesibilitas, kemampuan menampilkan informasi, keutuhan, dan pertanggungjawaban harus diterjemahkan menurut karakter objek. Pesan yang hanya tersedia sebagai gambar tidak selalu memuat metadata seperti pesan pada perangkat sumber. Data dari penyedia layanan mungkin memiliki struktur dan penjelasan waktu yang berbeda dari data pada telepon. Oleh sebab itu, autentikasi tidak tepat direduksi menjadi satu teknik yang berlaku untuk semua objek. Parameter yang diperlukan adalah kemampuan menunjukkan asal-usul serta alasan menganggap representasi itu sesuai dengan sumbernya. Analisis Hartono dan Yulianti membantu menempatkan kesempatan menyangkal sebagai bagian dari pemeriksaan tersebut (Hartono & Yulianti, 2020).

Pembedaan juga diperlukan antara keabsahan dan bobot. Keabsahan menyangkut apakah bukti memenuhi persyaratan hukum untuk digunakan, sedangkan bobot menyangkut seberapa jauh bukti itu mendukung suatu proposisi. Bukti autentik dapat mempunyai bobot terbatas apabila hanya membuktikan keberadaan berkas, bukan orang yang membuatnya. Sebaliknya, informasi yang tampak sangat meyakinkan secara isi tetap harus diuji legalitas perolehannya. Dalam kerangka KUHAP 2025, kedua wilayah itu berhubungan tetapi tidak saling menggantikan. Penilaian berurutan diperlukan agar kuatnya isi tidak menutupi persoalan perolehan dan terpenuhinya syarat formal tidak dianggap cukup untuk menyimpulkan kesalahan.

### **3.2 Kerangka sistem hukum dan parameter kepatuhan**

Teori sistem hukum Lawrence M. Friedman digunakan sebagai alat untuk menghubungkan substansi, struktur, dan budaya hukum. Substansi menunjuk pada aturan kewenangan dan persyaratan pembuktian. Struktur mencakup lembaga serta pembagian tugas yang memungkinkan aturan dilaksanakan. Budaya hukum berkaitan dengan orientasi dan

kebiasaan dalam menggunakan aturan tersebut. Perbedaan ini menjelaskan mengapa pembaruan undang-undang perlu diikuti kemampuan lembaga dan kebiasaan mendokumentasikan pekerjaan. Literatur yang membandingkan pandangan Friedman dan Hart juga memperlihatkan pentingnya membaca hukum dalam hubungan dengan konteks sosialnya, meskipun penelitian ini tidak menggunakan teori tersebut sebagai pengganti analisis norma (Ab. Halim et al., 2023; Friedman, 1975).

Dalam penelitian ini, kerangka Friedman dioperasionalkan melalui pertanyaan yang dapat diperiksa. Pada dimensi substansi, pertanyaannya adalah aturan apa yang mengizinkan tindakan dan apa akibat pelanggarannya. Pada dimensi struktur, pertanyaannya adalah siapa yang bertanggung jawab atas akuisisi, pengamanan, analisis, dan penyerahan data. Pada dimensi budaya, pertanyaannya adalah apakah pemeriksa bersedia mencatat keterbatasan, mempertimbangkan penjelasan alternatif, dan menerima pengujian. Penerapan tersebut merupakan pengembangan analitis penulis. Ia tidak dimaksudkan sebagai instrumen statistik untuk menilai seluruh lembaga penegak hukum, melainkan sebagai cara menempatkan kelemahan prosedur pada jenis perbaikan yang sesuai.

Berdasarkan kerangka itu, kepatuhan forensik elektronik dirumuskan dalam empat dimensi. Dimensi pertama adalah legalitas perolehan dan lingkup kewenangan. Dimensi kedua adalah integritas serta autentikasi objek. Dimensi ketiga adalah keandalan metode dan penerapannya. Dimensi keempat adalah keterbukaan terhadap pengujian yang bermakna. Keempatnya harus dibedakan agar keberhasilan satu dimensi tidak dipakai menutupi kegagalan dimensi lain. Sertifikasi tidak menggantikan izin penyitaan; nilai hash tidak menggantikan validasi penafsiran; dan laporan yang rinci tidak menghilangkan kebutuhan memberikan kesempatan kepada pihak lain untuk mengajukan keberatan. Hubungan ini menjadi dasar parameter penilaian yang diusulkan.

Rancangan validasi Stoykova dan Franke membedakan teknologi, metode, dan penerapan sebagai tingkat yang perlu didokumentasikan. Implikasinya, pemeriksaan tidak selesai dengan menyebut nama aplikasi. Teknologi yang sama dapat menghasilkan keluaran berbeda akibat versi, konfigurasi, format data, atau pilihan pemeriksa. Metode yang telah diuji juga dapat diterapkan pada keadaan yang berada di luar ruang pengujiannya. Penelitian ini menggunakan perbedaan tersebut untuk mengusulkan kewajiban penjelasan berlapis: kemampuan alat, alasan pemilihan prosedur, dan kesesuaian prosedur dengan objek perkara. Ketika salah satu lapisan tidak dijelaskan, pihak yang menilai bukti kehilangan dasar untuk menilai ketepatan kesimpulan (Stoykova & Franke, 2023).

Perubahan menuju pemeriksaan yang dapat dipertanggungjawabkan juga memerlukan kehati-hatian terhadap klaim kemajuan teknologi. Casey menempatkan perjalanan forensik digital dalam hubungan dengan risiko ilmiah dan kelembagaan. Dari sudut penelitian ini, pengadaan alat terbaru tidak dengan sendirinya memperbaiki mutu pembuktian apabila beban kerja, pengetahuan pemeriksa, dan mekanisme koreksi tidak berubah. Karena itu, keputusan kelembagaan seharusnya didasarkan pada kebutuhan pemeriksaan yang nyata, bukan sekadar kemampuan mengekstraksi lebih banyak data. Ukuran keberhasilan yang lebih tepat ialah kemampuan menerangkan hubungan antara data, cara memperoleh data, dan kesimpulan yang diajukan (Casey, 2019).

### 3.3 Legalitas perolehan dan analisis putusan

Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 memberikan contoh konkret bahwa persoalan bukti elektronik tidak dapat dipisahkan dari perlindungan hak. Perkara tersebut menguji ketentuan bukti elektronik dalam UU ITE dan UU Pemberantasan Tindak Pidana Korupsi. Dalam pertimbangan paragraf [3.10], Mahkamah menjelaskan kebutuhan memastikan intersepsi dilakukan secara sah dan mencegah penafsiran yang mempersempit pengakuan bukti elektronik secara tidak tepat. Pada paragraf [3.11], perhatian diarahkan pada cara memperoleh serta menyampaikan bukti. Dengan demikian, pusat persoalannya bukan apakah suatu rekaman dapat diputar, melainkan apakah proses yang melahirkan penggunaannya dapat dibenarkan secara hukum (Mahkamah Konstitusi Republik Indonesia, 2016).

Putusan tersebut perlu dibaca bersama antara amar dan pertimbangannya. Rujukan terhadap permintaan aparat penegak hukum berkaitan dengan konstruksi intersepsi yang dibahas Mahkamah. Tidak tepat menyimpulkan bahwa setiap dokumen elektronik yang dibuat warga, termasuk transaksi sehari-hari, otomatis tidak sah karena tidak dibuat atas permintaan aparat. Sebaliknya, juga tidak tepat mengabaikan perlindungan privasi hanya karena informasi memiliki hubungan dengan perkara. Implikasi analitisnya adalah kebutuhan mengidentifikasi terlebih dahulu tindakan yang dilakukan: pengambilan data tersimpan, penyerahan sukarela, penyitaan perangkat, atau intersepsi. Setiap kategori memerlukan pemeriksaan dasar kewenangan yang sesuai, dan tidak boleh disamakan hanya karena hasil akhirnya berbentuk berkas elektronik.

Dalam penyitaan, Pasal 119 KUHAP 2025 mengatur permohonan izin kepada ketua pengadilan negeri. Pasal 120 mengatur keadaan mendesak untuk benda bergerak, dengan kewajiban meminta persetujuan paling lama lima hari kerja. Pasal 121 ayat (3) memberikan akibat ketika izin atau persetujuan ditolak, yakni hasil penyitaan tidak dapat dijadikan alat bukti. Tenggat tersebut harus dibedakan dari kewajiban administratif lain yang juga diatur dalam tahapan penyitaan. Untuk perkara yang tunduk pada KUHAP 1981, dasar pengecualian penyitaan dalam keadaan mendesak diatur dalam Pasal 38 ayat (2) (Republik Indonesia, 1981, 2025).

Kebutuhan menyelamatkan data yang mudah hilang tidak boleh diperlakukan sebagai izin tanpa batas. Alasan mendesak harus berkaitan dengan keadaan konkret dan objek tindakan. Apabila ancamannya berupa penghapusan jarak jauh, laporan perlu menjelaskan indikator ancaman, pilihan yang tersedia, dan alasan tindakan yang dipilih. Sesudah itu, kewajiban hukum yang mengikuti tindakan tetap harus dipenuhi. Cara berpikir ini mempertahankan kemungkinan respons cepat sekaligus memungkinkan kontrol atas penggunaannya. Penilaian proporsional juga harus memperhatikan bahwa sebuah perangkat dapat memuat data pribadi pihak lain yang tidak berkaitan dengan tindak pidana, sehingga keluasaan akses membutuhkan alasan yang dapat diuji.

Perbandingan melalui penelitian Vanessa dan Firmansyah memperlihatkan perbedaan penggunaan forensik dalam dua putusan pengadilan negeri, yaitu Nomor 175/Pid.Sus/2024/PN Jmb dan Nomor 60/Pid.B/2019/PN Drh. Artikel tersebut melaporkan bahwa pengadilan dapat menerima bukti tanpa pemeriksaan forensik mendalam pada satu perkara, sedangkan perkara lain menggunakan hasil laboratorium untuk mendukung pembuktian. Pembahasan ini

digunakan sebagai ilustrasi dari sumber sekunder, bukan sebagai hasil pemeriksaan ulang seluruh berkas putusan oleh penulis. Kegunaannya ialah memperlihatkan bahwa peran forensik perlu dinilai berdasarkan kebutuhan autentikasi dan keberatan dalam perkara, bukan dirumuskan sebagai syarat seragam yang selalu mempunyai akibat identik (Vanessa & Firmansyah, 2025).

Ilustrasi tersebut tidak membenarkan kesimpulan bahwa pemeriksaan forensik boleh ditiadakan tanpa alasan. Hakim tetap memerlukan dasar untuk menilai autentikasi dan legalitas. Persoalannya ialah apakah dasar itu tersedia melalui kombinasi sumber yang dapat diuji, bukan sekadar ada atau tidaknya sebuah dokumen berjudul laporan forensik. Apabila identitas sumber, kelengkapan, atau perubahan data dipersoalkan secara material, kebutuhan pemeriksaan teknis menjadi lebih kuat. Sebaliknya, penerimaan bukti pada satu perkara tidak dapat digeneralisasi sebagai pembenaran semua bukti sejenis. Pembacaan putusan harus mempertahankan perbedaan fakta, keberatan para pihak, serta hukum yang berlaku pada saat penanganannya.

### **3.4 Integritas objek dan batas kemampuan teknik forensik**

ISO/IEC 27037:2012 memberi pedoman identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital. Ruang lingkup itu penting karena standar tersebut tidak sendirian menjawab seluruh masalah analisis maupun penilaian yudisial. Pedoman teknis dapat membantu merancang tindakan yang konsisten, tetapi kewenangan melakukan tindakan tetap bersumber pada hukum yang berlaku. Demikian pula, panduan NIST SP 800-86 disusun dari perspektif teknologi informasi dan respons insiden, bukan sebagai hukum acara pidana Indonesia. Penelitian ini memperlakukan keduanya sebagai rujukan teknis yang perlu disesuaikan dengan tugas serta ketentuan hukum, bukan sebagai norma yang otomatis membatalkan bukti ketika satu teknik tidak digunakan (International Organization for Standardization [ISO] & International Electrotechnical Commission [IEC], 2012; Kent et al., 2006).

Integritas berarti kemampuan menunjukkan bahwa objek tidak mengalami perubahan yang tidak dijelaskan pada rentang penanganan tertentu. Fungsi hash membantu membandingkan representasi bit suatu objek dengan representasi yang telah dicatat. Namun, nilai hash bukan tanda tangan pelaku dan tidak membuktikan kebenaran isi. Berkas yang sejak awal palsu tetap dapat mempunyai nilai hash yang konsisten. Karena itu, nilai hash harus dihubungkan dengan identitas objek, algoritma, waktu penghitungan, dan titik pembanding. Buku Casey mengenai bukti digital menempatkan penanganan bukti dalam keseluruhan penyelidikan; kerangka tersebut mendukung pembacaan hash sebagai bagian dari proses, bukan pengganti penyelidikan (Casey, 2011).

Model proses forensik terintegrasi berusaha mempertemukan tahapan dan istilah yang sebelumnya tersebar dalam berbagai pendekatan. Kajian mengenai arah penelitian forensik juga menekankan perlunya representasi serta pemrosesan data yang lebih terstandar. Bagi penelitian ini, keduanya mendukung kebutuhan kesinambungan antartahap: keputusan pada saat akuisisi harus dapat dikenali akibatnya pada saat analisis dan pelaporan. Standarisasi tidak berarti menyeragamkan seluruh teknik pada semua perangkat. Yang perlu seragam adalah kemampuan menjelaskan tindakan, mempertahankan hubungan dengan sumber, dan

menyatakan batas kesimpulan. Perbedaan metode justru dapat dibenarkan ketika alasan dan konsekuensinya terdokumentasi (Garfinkel, 2010; Kohn et al., 2013).

Ketidakcocokan hash memerlukan pemeriksaan lebih lanjut terhadap objek yang dibandingkan. Salinan identik pada tingkat bit seharusnya menghasilkan nilai sama dengan algoritma yang sama. Akan tetapi, berkas hasil ekspor, data yang dinormalisasi, atau laporan yang menampilkan sebagian informasi tidak selalu identik dengan media sumber secara keseluruhan. Membandingkan dua objek berbeda lalu menyimpulkan manipulasi merupakan kesalahan penalaran. Pemeriksa harus menjelaskan transformasi yang dilakukan dan mempertahankan hubungan antara objek sumber, salinan kerja, serta produk analisis. Untuk pemeriksaan berjalan, pencatatan perubahan yang tidak terhindarkan juga lebih tepat daripada janji bahwa semua data pasti tetap tidak berubah.

Penggunaan write-blocker perlu ditempatkan sesuai sifat media dan metode. Pada pemeriksaan media penyimpanan yang memungkinkan akses baca saja, perlindungan terhadap penulisan merupakan langkah penting untuk mengurangi perubahan. Namun, akuisisi memori aktif, layanan awan, dan sebagian perangkat bergerak mempunyai kondisi berbeda. Pernyataan bahwa write-blocker merupakan syarat yang tidak mengenal pengecualian akan mengabaikan kenyataan teknis tersebut. Yang harus dipertanggungjawabkan adalah alasan pemilihan metode, perubahan yang mungkin ditimbulkan, serta upaya menguranginya. Perbedaan sumber data dan konsekuensi penanganannya sejalan dengan orientasi panduan respons insiden, tanpa menjadikannya kewenangan untuk menyimpang dari hukum (Kent et al., 2006).

Rantai penguasaan bukti mencatat siapa yang menguasai objek, kapan perpindahan terjadi, untuk tujuan apa, dan bagaimana penyimpanan dilakukan. Namun, catatan perpindahan fisik saja belum menjelaskan bagaimana data dipilih serta ditafsirkan. Sebuah media dapat berpindah secara tertib tetapi dianalisis dengan asumsi yang keliru. Penelitian mengenai pemanfaatan blockchain untuk rantai penguasaan menawarkan dukungan integritas dan auditabilitas catatan. Meskipun demikian, pencatatan yang sulit diubah tetap tidak menjamin bahwa informasi awal yang dimasukkan benar. Oleh sebab itu, teknologi pencatatan harus melengkapi pemeriksaan manusia serta tata kelola, bukan menggantikannya (Lone & Mir, 2019).

Pengendalian terhadap media fisik tetap diperlukan sekalipun analisis berpusat pada data. Rancangan manajemen barang bukti dan rantai penguasaan oleh Efendi dan rekan-rekan memperlihatkan kegunaan pencatatan inventaris serta aktivitas penyimpanan. Implikasinya, identitas perangkat, media salinan, dan lokasi penyimpanan tidak boleh dikelola dalam catatan yang tidak dapat dihubungkan. Sebagai contoh analitis, perubahan label tanpa jejak penghubung dapat menyulitkan pembuktian bahwa salinan kerja berasal dari media tertentu. Sistem dokumentasi harus memungkinkan penelusuran itu, termasuk ketika data dipindahkan ke media pengganti untuk menjaga keberlanjutan akses (Efendi et al., 2020).

Pada layanan awan, hubungan antara pengguna dan data dapat tersebar pada beberapa komponen. Log dapat merekam aktivitas aplikasi atau layanan, tetapi identitas akun dan identitas orang harus dibedakan. Penelitian BCFL logging menunjukkan pendekatan untuk memperoleh serta mempertahankan log dalam ekosistem awan. Bagi analisis hukum, pelajarannya ialah kebutuhan mencatat asal log, cara pengambilan, batas akses, dan keadaan penyedia layanan. Penelitian ini tidak menganggap satu rancangan teknologi tertentu sebagai

kewajiban nasional. Setiap penggunaan perlu dinilai terhadap kebutuhan perkara, keterjelasan sumber, serta kemampuan pihak lain memeriksa keluaran yang dipakai (Awuson-David et al., 2021).

### **3.5 Keandalan metode dan pengendalian kesalahan**

Keandalan tidak dapat diasumsikan hanya karena alat dipasarkan untuk kebutuhan forensik. Kajian Horsman mengenai pengujian alat menunjukkan pentingnya memastikan keluaran pemeriksaan dapat diandalkan dan diulang. Dalam praktik penilaian, pernyataan bahwa alat telah digunakan secara luas belum menjawab apakah alat sesuai dengan versi aplikasi atau format yang diperiksa. Pemeriksa perlu menjelaskan fungsi yang diuji, kondisi pengujian, hasil yang diharapkan, serta penyimpangan yang ditemukan. Pengujian berbasis tugas lebih berguna daripada klaim umum bahwa seluruh kemampuan perangkat lunak telah divalidasi. Kesimpulan juga harus dibatasi pada fungsi yang mempunyai dasar pengujian memadai (Horsman, 2019b).

Landasan ilmiah standardisasi perlu dibedakan dari sertifikat kepatuhan organisasi. Literatur mengenai dasar ilmiah akreditasi menghubungkan metode ilmiah dengan kebutuhan penilaian mutu. Penelitian mengenai korpus forensik juga menunjukkan kegunaan data uji yang mempunyai dasar pembandingan untuk menilai kinerja alat. Dari kedua pendekatan ini, penelitian mengusulkan agar kemampuan laboratorium dinilai melalui tugas yang dapat diperagakan, bukan hanya kelengkapan administrasi. Untuk fungsi yang menentukan perkara, data uji perlu cukup mewakili keadaan pemeriksaan. Keberhasilan pada satu contoh tidak dapat dijadikan kesimpulan bahwa alat selalu benar dalam seluruh keadaan (Beckett & Slay, 2011; Garfinkel et al., 2009).

Framework for Reliable Experimental Design memberikan perhatian pada perencanaan penelitian agar penafsiran data tidak dibangun dari percobaan yang tidak terkendali. Dalam konteks perkara, pengujian terhadap artefak yang belum dipahami harus memisahkan data uji dari data perkara dan mencatat variabel yang berpengaruh. Apabila perubahan versi aplikasi dapat mengubah struktur penyimpanan, hasil eksperimen pada versi lama tidak boleh diterapkan tanpa evaluasi. Kewajiban menjelaskan pengujian tersebut berkaitan dengan dasar ilmiah kesimpulan ahli. Pemeriksa bukan hanya menyampaikan apa yang terlihat, tetapi juga alasan menghubungkan tampilan tersebut dengan aktivitas tertentu (Horsman, 2018).

Kerangka VODE menekankan verifikasi atas interpretasi data, sedangkan CODE membahas unsur pengetahuan yang perlu dibagikan agar berguna bagi pemeriksa lain. Kedua pendekatan mempunyai fungsi yang berkaitan: pengetahuan harus diperoleh melalui pengujian, lalu dijelaskan dengan cukup lengkap untuk dievaluasi. Dalam penelitian ini, keduanya mendukung usulan agar laporan membedakan observasi, proses pengujian, interpretasi, dan keterbatasan. Pembagian tersebut membantu hakim melihat titik kesimpulan yang masih memerlukan dukungan. Ia juga memungkinkan pemeriksa berikutnya menguji pengetahuan yang sama tanpa bergantung semata-mata pada pengalaman pribadi penulis laporan (Horsman, 2020a, 2020b).

Model eksperimen forensik digital memperlihatkan pentingnya perencanaan, pelaksanaan, analisis, dan penyebaran hasil secara tertib. Pengembangan ontologi untuk eksperimen juga bertujuan memperjelas unsur yang harus didokumentasikan agar replikasi dapat dilakukan.

Implikasi normatifnya adalah bahwa pernyataan ilmiah perlu disertai jalur pemeriksaan yang terbuka. Tidak semua pengujian harus dituangkan sebagai penelitian besar, tetapi langkah yang menentukan penafsiran bukti tidak boleh dihilangkan dari dokumentasi. Ketika eksperimen sederhana digunakan untuk menyimpulkan asal suatu artefak, keadaan pengujian dan keterbatasannya tetap perlu dijelaskan kepada pihak yang menilai bukti (Oliveira Jr et al., 2020; Silva et al., 2025).

Pemodelan proses internal alat analisis memperlihatkan bahwa kesalahan dapat muncul pada beberapa tahap dan diteruskan ke keluaran akhir. Karena itu, pemeriksaan terhadap laporan akhir saja belum tentu cukup untuk menemukan sumber kesalahan. Apabila data melewati tahap ekstraksi, penguraian, penyaringan, dan penyajian, dokumentasi harus memungkinkan penelusuran kembali ke tahap yang relevan. Penelitian ini mengusulkan penyimpanan hasil antara yang diperlukan bagi pemeriksaan ulang, dengan tetap memperhatikan pembatasan akses. Tujuannya bukan menambah dokumen tanpa kegunaan, melainkan mempertahankan informasi yang menjelaskan bagaimana kesimpulan dibentuk dan di mana kesalahan dapat diperbaiki (Hargreaves et al., 2024).

Kesalahan alat juga perlu dibedakan dari kesalahan penggunaan alat. Sebuah fungsi mungkin bekerja sesuai rancangan, tetapi dipakai pada keadaan yang tidak sesuai atau ditafsirkan melampaui kemampuannya. Sebaliknya, adanya kompetensi pemeriksa tidak meniadakan kemungkinan kesalahan perangkat lunak. Horsman mengingatkan perlunya menentukan secara tepat sumber kegagalan sebelum tindakan korektif dilakukan. Bagi penilaian hukum, pembedaan ini mencegah dua penyederhanaan: menyalahkan alat untuk seluruh kekeliruan dan menganggap seluruh keluaran alat benar karena pemeriksanya berpengalaman. Tanggung jawab harus dihubungkan dengan keputusan serta proses yang dapat diidentifikasi (Horsman, 2022).

### **3.6 Interpretasi fakta dan pengujian kontradiktor**

Data yang autentik masih memerlukan penafsiran. Waktu pada berkas dapat mencerminkan konfigurasi sistem, zona waktu, penyalinan, atau kegiatan aplikasi tertentu. Hubungan antara akun dan orang dapat dipengaruhi akses bersama, penggunaan otomatis, atau kompromi keamanan. Oleh karena itu, ahli perlu merumuskan proposisi yang hendak didukung, kemudian memeriksa apakah data juga konsisten dengan penjelasan alternatif. Pendekatan pembentukan opini evaluatif Casey membantu menempatkan kekuatan bukti sebagai hubungan antara temuan dan hipotesis, bukan pernyataan kepastian tanpa dasar. Penelitian ini tidak mengusulkan angka probabilitas apabila data pendukungnya tidak tersedia (Casey, 2020).

Bias pemeriksa merupakan risiko yang perlu dikelola, bukan tuduhan mengenai niat buruk. Sunde dan Dror mengidentifikasi sumber kesalahan kognitif dalam proses forensik digital. Pengetahuan tentang dugaan pelaku atau arah penyidikan dapat memengaruhi pemilihan dan penafsiran data. Karena itu, informasi kontekstual sebaiknya diberikan sesuai kebutuhan tugas, dan kesimpulan yang menentukan perlu diuji melalui pemeriksaan independen. Pemeriksa juga perlu mencatat data yang tidak mendukung dugaan awal. Kebiasaan tersebut menjaga penyelidikan tetap terbuka terhadap kemungkinan bahwa hubungan teknis yang ditemukan belum cukup untuk menunjukkan kesalahan orang tertentu (Sunde & Dror, 2019).

Telaah sistematis mengenai bias dalam ilmu forensik menunjukkan nilai pengurangan informasi yang tidak diperlukan dan penilaian ulang tanpa mengetahui kesimpulan sebelumnya. Temuan lintas bidang ini tidak dapat dianggap sebagai ukuran prevalensi kesalahan pada laboratorium Indonesia. Namun, ia memberi alasan rasional untuk membangun pengendalian yang tidak bergantung semata-mata pada kehati-hatian individu. Dalam penelitian ini, pembatasan informasi kontekstual, pencatatan hipotesis alternatif, dan pemeriksaan independen diusulkan sebagai bagian tata kelola. Pengendalian tersebut diarahkan pada peningkatan mutu keputusan, bukan pada pembatasan hak pihak berperkara untuk mengetahui dasar kesimpulan ahli (Cooper & Meterko, 2019).

Pemeriksaan sejawat perlu melampaui koreksi tata bahasa laporan. Literatur tentang kebutuhan peer review menguraikan tingkat pemeriksaan yang dapat menyentuh tugas, proses, dan kesimpulan. Rancangan PARS kemudian membedakan fungsi pemberian nasihat selama pekerjaan dan fungsi penelaahan atas hasil. Bagi lembaga yang sumber dayanya terbatas, pembagian tersebut dapat diterapkan secara proporsional dengan mendahulukan temuan yang menentukan atribusi, kronologi, dan autentikasi. Nama penelaah, lingkup yang diperiksa, serta perbedaan pendapat sebaiknya dicatat. Keberadaan tanda tangan kedua tanpa penjelasan lingkup pemeriksaan tidak cukup menggambarkan mutu penelaahan (Horsman & Sunde, 2020; Sunde & Horsman, 2021).

Pengujian kontradiktor mensyaratkan kesempatan nyata untuk memeriksa dasar bukti. Pemberian laporan ringkas tanpa informasi sumber, prosedur, atau keterbatasan dapat menyulitkan advokat mengajukan keberatan yang terarah. Sebaliknya, keterbukaan tidak harus berarti penyebaran seluruh isi perangkat tanpa pembatasan. Pengadilan dapat menata akses yang relevan dengan tetap melindungi data pribadi pihak lain. Posisi yang diusulkan ialah keterbukaan terukur: informasi yang diperlukan untuk menguji kesimpulan harus tersedia dalam bentuk yang dapat dipahami dan diperiksa. Prinsip ini mengikuti perhatian literatur terhadap keadilan proses serta praduga tidak bersalah (Stoykova, 2021).

Dalam perkara berbasis akun, penafsiran harus menghubungkan kepemilikan, penguasaan, dan aktivitas pada waktu yang relevan. Artikel Medeline dan rekan-rekan menunjukkan pentingnya forensik untuk menguji hubungan tersebut dalam perkara ujaran kebencian. Akan tetapi, pengakuan pemilik akun atau nama yang tampil di layar tidak menghapus kebutuhan memeriksa unsur delik dan konteks penggunaan. Penelitian ini mengembangkan perbedaan antara bukti sumber dan bukti aktivitas: perangkat atau akun dapat mengarah pada sumber potensial, sedangkan rangkaian aktivitas memerlukan dukungan waktu, akses, isi, dan keadaan lain yang saling menguatkan. Identitas teknis harus diuji sebelum dipadankan dengan identitas pelaku (Medeline et al., 2022).

### **3.7 Akibat ketidakpatuhan dan tata kelola perbaikan**

Akibat ketidakpatuhan harus ditentukan dari jenis pelanggaran dan norma yang mengaturnya. Dalam KUHAP 2025, bukti yang dinyatakan tidak autentik dan/atau diperoleh secara melawan hukum tidak dapat digunakan dan tidak mempunyai kekuatan pembuktian. Namun, kesimpulan hukum tersebut harus dibedakan dari indikator awal, seperti kolom serah terima yang belum lengkap atau hash yang berbeda pada objek yang belum dipastikan identik. Indikator memerlukan penjelasan dan pengujian; ia tidak otomatis membuktikan seluruh proses melawan hukum. Sebaliknya, kekurangan yang menghalangi pemeriksaan asal-usul

secara material tidak dapat diselesaikan hanya dengan pernyataan pemeriksa bahwa bukti dapat dipercaya (Republik Indonesia, 2025).

Penilaian bertingkat dapat membantu menghubungkan kekurangan dengan tindakan korektif. Apabila masalahnya bersifat administratif dan dapat dijelaskan melalui catatan yang telah ada, kelengkapan perlu diperiksa tanpa membuat catatan seolah-olah ditulis pada waktu sebelumnya. Apabila kekurangan memengaruhi penafsiran, pemeriksaan tambahan atau pembatasan kesimpulan mungkin diperlukan. Apabila menyangkut legalitas perolehan atau autentikasi yang tidak dapat dipertanggungjawabkan, akibat hukumnya mengikuti ketentuan yang berlaku serta penilaian hakim. Pembagian ini merupakan usulan analitis, bukan penciptaan pengecualian baru untuk bukti yang menurut undang-undang tidak dapat digunakan. Perbaikan dokumentasi tidak boleh dipakai melegalkan tindakan secara surut.

Penelitian atas laporan pemeriksaan di Norwegia menunjukkan bahwa dokumentasi yang tidak memadai dapat menghalangi penilaian keandalan. Nilai pembandingnya terletak pada hubungan antara catatan proses dan kemampuan audit, bukan pada anggapan bahwa situasi Indonesia pasti sama. Dari temuan tersebut, penelitian ini mengusulkan pemeriksaan kelengkapan sebelum laporan diserahkan: setiap temuan penting harus dapat ditautkan pada sumber dan langkah yang menghasilkannya. Apabila tautan itu tidak tersedia, keterbatasannya harus dinyatakan secara terbuka. Transparansi mengenai kekurangan lebih berguna bagi penilaian bukti daripada kepastian yang tidak didukung dokumen (Stoykova et al., 2022).

Pengendalian kelembagaan juga perlu mempertimbangkan kapasitas. Survei kebutuhan forensik menempatkan pendidikan, personel, perangkat, komunikasi, dan pembaruan hukum sebagai bidang yang saling berkaitan. Kajian mengenai kematangan organisasi menambahkan hubungan proses, kebijakan, teknologi, serta regulasi. Karena itu, program peningkatan mutu tidak cukup berupa pelatihan penggunaan satu aplikasi. Lembaga perlu memetakan jenis tugas, kecakapan yang diperlukan, distribusi beban kerja, dan mekanisme memperoleh bantuan ahli. Usulan ini tidak didasarkan pada pengukuran jumlah tenaga di Indonesia, melainkan pada kebutuhan fungsional agar kewajiban pemeriksaan dapat dilaksanakan secara konsisten (Ariffin & Ahmad, 2021; Harichandran et al., 2016).

Kesiapan forensik perlu dibangun sebelum perkara muncul. Kajian perbandingan kesiapan forensik menunjukkan hubungan antara kebijakan informasi dan kemampuan mempertahankan bukti. Dalam konteks yang relevan, institusi dapat menata pencatatan waktu, pengamanan log, pembatasan akses, dan prosedur preservasi. Akan tetapi, kesiapan tidak berarti pengumpulan data masyarakat secara tidak terbatas. Dasar kewenangan dan tujuan penggunaan harus tetap jelas. Persiapan yang tepat justru memungkinkan tindakan yang lebih terarah ketika insiden terjadi, sehingga kebutuhan memperoleh bukti tidak selalu direspons dengan penyitaan luas dan penyaringan data yang tidak proporsional (Park et al., 2018).

Strategi pemeriksaan perlu dituangkan sebelum seluruh data diproses. Digital evidence strategy membantu menjelaskan tujuan, prioritas, dan pilihan pemeriksaan. Kerangka DERDS juga memberi perhatian pada pengambilan keputusan investigatif yang dapat dijelaskan. Penelitian ini mengusulkan agar strategi mencatat pertanyaan perkara, sumber yang dipilih, alasan menunda pemeriksaan tertentu, dan kondisi yang mengharuskan perluasan pemeriksaan. Dokumen tersebut dapat diperbarui ketika temuan baru muncul, dengan mempertahankan jejak perubahan. Dengan cara ini, efisiensi tidak dipisahkan dari

pertanggungjawaban dan pemilihan data tidak hanya bergantung pada intuisi pemeriksa (Horsman, 2019a, 2023).

Penelitian kualitatif terhadap pemeriksa di Inggris dan Wales memperlihatkan adanya tuntutan pekerjaan serta hubungan yang tidak selalu mudah antara pemeriksa, penyidik, dan pelaku proses pengadilan. Literatur ini berguna untuk mengingatkan bahwa mutu forensik juga bergantung pada komunikasi mengenai kemampuan dan batas pemeriksaan. Tenggat yang tidak sesuai dengan kompleksitas dapat mendorong kesimpulan terlalu cepat. Karena itu, lembaga perlu menyediakan jalur konsultasi dan eskalasi ketika objek melampaui keahlian pemeriksa atau alat yang tersedia. Pengakuan atas batas kemampuan harus diperlakukan sebagai bagian profesionalitas, bukan kegagalan yang harus disembunyikan (Ng et al., 2024).

Secara operasional, penelitian ini mengusulkan satu paket dokumentasi minimum yang mengikuti siklus bukti. Paket tersebut mencakup dasar tindakan dan lingkupnya, identitas objek, kondisi awal, catatan perpindahan, metode serta konfigurasi, hasil pengujian integritas, dasar interpretasi, keterbatasan, dan hasil penelaahan. Setiap unsur harus terhubung melalui identitas objek yang konsisten. Pengembangan sistem elektronik dapat membantu, tetapi kewajiban dokumentasi tidak perlu menunggu tersedianya teknologi tertentu. Formulir yang jelas dan disiplin penggunaan dapat menjadi tahap awal, selama perubahan tercatat dan pihak yang berwenang dapat memeriksa asal-usul informasi.

Prioritas kebijakan sebaiknya diarahkan pada tindakan yang mengurangi risiko paling menentukan. Pada tahap awal, fokusnya adalah kejelasan kewenangan, pengamanan sumber, dan pencatatan kondisi. Pada tahap analisis, fokusnya adalah validasi fungsi penting serta pengujian penjelasan alternatif. Pada tahap pelaporan, fokusnya adalah keterlacakan kesimpulan dan akses pengujian. Audit internal dapat memilih sampel pekerjaan untuk menemukan pola kekurangan dan memperbaiki prosedur, tanpa mengklaim bahwa audit administratif menggantikan penilaian hakim. Keterhubungan ketiga tahap memungkinkan kesalahan ditemukan lebih awal dan mencegah kekurangan yang sama diteruskan dari satu lembaga kepada lembaga berikutnya.

Usulan ini mempunyai keterbatasan. Penelitian belum menguji kelayakan biaya, durasi, atau kapasitas penerapan pada berbagai wilayah. Analisis putusan tidak merupakan survei seluruh praktik pengadilan, dan ilustrasi putusan negeri dibaca melalui artikel sekunder. Karena itu, penelitian lanjutan perlu menguji parameter melalui pemeriksaan dokumen perkara yang memperoleh izin, wawancara, dan evaluasi laboratorium. Batas tersebut tidak menghilangkan kegunaan normatif parameter yang diajukan, tetapi membatasi jenis kesimpulan yang dapat ditarik. Penelitian ini menunjukkan apa yang perlu dapat dipertanggungjawabkan; penelitian empiris berikutnya diperlukan untuk menilai seberapa jauh persyaratan tersebut dilaksanakan dan hambatan konkretnya.

#### **4 Kesimpulan**

Kedudukan bukti elektronik dalam hukum acara pidana Indonesia telah dipertegas oleh KUHAP 2025, dengan tetap memperhatikan UU ITE dan ketentuan peralihan. Pengakuan jenis bukti tidak menghilangkan persyaratan autentikasi serta perolehan yang tidak melawan hukum. Kepatuhan forensik perlu dinilai melalui empat dimensi yang berkaitan, yaitu legalitas perolehan, integritas dan autentikasi objek, keandalan metode, serta keterbukaan pengujian.

Teori sistem hukum membantu menunjukkan bahwa pemenuhan persyaratan tersebut memerlukan aturan yang jelas, pembagian tanggung jawab, dan kebiasaan mendokumentasikan serta mengoreksi pekerjaan. Bukti teknis tidak boleh digunakan melampaui proposisi yang benar-benar didukungnya.

Ketidakpatuhan harus dinilai menurut jenis, tahap, dan akibatnya. Nilai hash bukan bukti identitas pelaku, kekurangan catatan bukan selalu penolakan otomatis, dan laporan ahli bukan jaminan legalitas perolehan. Apabila hakim menyatakan bukti tidak autentik atau diperoleh secara melawan hukum, akibatnya mengikuti larangan penggunaan dalam KUHAP 2025. Oleh karena itu, direkomendasikan pembakuan dokumentasi minimum, validasi berbasis tugas, pemeriksaan sejawat atas temuan yang menentukan, dan akses pengujian yang terukur. Pelaksanaannya perlu disertai pemetaan kompetensi serta audit mutu. Penguatan tersebut diarahkan untuk menghasilkan pembuktian yang dapat diperiksa dan melindungi semua pihak dari kesimpulan yang tidak mempunyai dasar memadai.

## Daftar Referensi

- Ab. Halim, M. A., Amni, S. Z., & Maulana, M. (2023). Legal system in the perspectives of H.L.A Hart and Lawrence M. Friedman. *Peradaban Journal of Law and Society*, 2(1), 51–61. <https://doi.org/10.59001/pjls.v2i1.83>
- Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. *Computers & Security*, 105, 102237. <https://doi.org/10.1016/j.cose.2021.102237>
- Arisandy, Y. O. (2021). Penegakan hukum terhadap cyber crime hacker. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, 1(3), 162–169. <https://doi.org/10.18196/ijclc.v1i3.11264>
- Awuson-David, K., Al-Hadhrami, T., Alazab, M., Shah, N., & Shalaginov, A. (2021). BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem. *Future Generation Computer Systems*, 122, 1–13. <https://doi.org/10.1016/j.future.2021.03.001>
- Beckett, J., & Slay, J. (2011). Scientific underpinnings and background to standards and accreditation in digital forensics. *Digital Investigation*, 8(2), 114–121. <https://doi.org/10.1016/j.diin.2011.08.001>
- Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd ed.). Academic Press. <https://shop.elsevier.com/books/digital-evidence-and-computer-crime/casey/978-0-08-092148-8>
- Casey, E. (2019). The chequered past and risky future of digital forensics. *Australian Journal of Forensic Sciences*, 51(6), 649–664. <https://doi.org/10.1080/00450618.2018.1554090>
- Casey, E. (2020). Standardization of forming and expressing preliminary evaluative opinions on digital evidence. *Forensic Science International: Digital Investigation*, 32, 200888. <https://doi.org/10.1016/j.fsidi.2019.200888>
- Cooper, G. S., & Meterko, V. (2019). Cognitive bias research in forensic science: A systematic review. *Forensic Science International*, 297, 35–46. <https://doi.org/10.1016/j.forsciint.2019.01.016>
- Efendi, T. F., Rahmadi, R., & Prayudi, Y. (2020). Rancang bangun sistem untuk manajemen barang bukti fisik dan chain of custody (CoC) pada penyimpanan laboratorium forensika digital. *Jurnal Teknologi dan Manajemen Informatika*, 6(2), 53–63. <https://doi.org/10.26905/jtmi.v6i2.4177>
- Friedman, L. M. (1975). *The legal system: A social science perspective*. Russell Sage Foundation. <https://doi.org/10.7758/9781610442282>
- Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7, S64–S73. <https://doi.org/10.1016/j.diin.2010.05.009>

- Garfinkel, S., Farrell, P., Roussev, V., & Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. *Digital Investigation*, 6, S2–S11. <https://doi.org/10.1016/j.diin.2009.06.016>
- Habibi, M. R., & Liviani, I. (2020). Kejahatan teknologi informasi (cyber crime) dan penanggulangannya dalam sistem hukum Indonesia. *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, 23(2), 400–426. <https://doi.org/10.15642/alqanun.2020.23.2.400-426>
- Hargreaves, C., Nelson, A., & Casey, E. (2024). An abstract model for digital forensic analysis tools - A foundation for systematic error mitigation analysis. *Forensic Science International: Digital Investigation*, 48, 301679. <https://doi.org/10.1016/j.fsidi.2023.301679>
- Harichandran, V. S., Breitingner, F., Baggili, I., & Marrington, A. (2016). A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Computers & Security*, 57, 1–13. <https://doi.org/10.1016/j.cose.2015.10.007>
- Hartono, M. S., & Yulianti, N. P. R. (2020). Penggunaan bukti elektronik dalam peradilan pidana. *Jurnal Komunikasi Hukum (JKH)*, 6(1), 281–302. <https://doi.org/10.23887/jkh.v6i1.23607>
- Horsman, G. (2018). Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics. *Computers & Security*, 73, 294–306. <https://doi.org/10.1016/j.cose.2017.11.009>
- Horsman, G. (2019a). Formalising investigative decision making in digital forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework. *Digital Investigation*, 28, 146–151. <https://doi.org/10.1016/j.diin.2019.01.007>
- Horsman, G. (2019b). Tool testing and reliability issues in the field of digital forensics. *Digital Investigation*, 28, 163–175. <https://doi.org/10.1016/j.diin.2019.01.009>
- Horsman, G. (2020a). Part 1: Quality assurance mechanisms for digital forensic investigations: Introducing the Verification of Digital Evidence (VODE) framework. *Forensic Science International: Reports*, 2, 100038. <https://doi.org/10.1016/j.fsir.2019.100038>
- Horsman, G. (2020b). Part 2: Quality assurance mechanisms for digital forensic investigations: Knowledge sharing and the Capsule of Digital Evidence (CODE). *Forensic Science International: Reports*, 2, 100035. <https://doi.org/10.1016/j.fsir.2019.100035>
- Horsman, G. (2022). That tool is rubbish!...or is it?. *Science & Justice*, 62(5), 515–519. <https://doi.org/10.1016/j.scijus.2022.07.006>
- Horsman, G. (2023). Digital evidence strategies for digital forensic science examinations. *Science & Justice*, 63(1), 116–126. <https://doi.org/10.1016/j.scijus.2022.11.004>
- Horsman, G., & Sunde, N. (2020). Part 1: The need for peer review in digital forensics. *Forensic Science International: Digital Investigation*, 35, 301062. <https://doi.org/10.1016/j.fsidi.2020.301062>
- International Organization for Standardization & International Electrotechnical Commission. (2012). *Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence* (ISO/IEC 27037:2012). <https://www.iso.org/standard/44381.html>
- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST SP 800-86). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-86>
- Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model. *Computers & Security*, 38, 103–115. <https://doi.org/10.1016/j.cose.2013.05.001>
- Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digital Investigation*, 28, 44–55. <https://doi.org/10.1016/j.diin.2019.01.002>

- Mahkamah Konstitusi Republik Indonesia. (2016). *Putusan Nomor 20/PUU-XIV/2016* (7 September 2016). [https://www.mkri.id/public/content/persidangan/putusan/20\\_PUU-XIV\\_2016.pdf](https://www.mkri.id/public/content/persidangan/putusan/20_PUU-XIV_2016.pdf)
- Medeline, F., Rusmiati, E., & Ramadhani, R. H. (2022). Forensik Digital dalam Pembuktian Tindak Pidana Ujaran Kebencian di Media Sosial. *PAMPAS: Journal of Criminal Law*, 3(3), 310–325. <https://doi.org/10.22437/pampas.v3i3.19691>
- Ng, M., James, J., & Bull, R. (2024). “What you say in the lab, stays in the lab”: A reflexive thematic analysis of current challenges and future directions of digital forensic investigations in the UK. *Forensic Science International: Digital Investigation*, 51, 301839. <https://doi.org/10.1016/j.fsidi.2024.301839>
- Oliveira Jr, E., Zorzo, A. F., & Neu, C. V. (2020). Towards a conceptual model for promoting digital forensics experiments. *Forensic Science International: Digital Investigation*, 35, 301014. <https://doi.org/10.1016/j.fsidi.2020.301014>
- Page, H., Horsman, G., Sarna, A., & Foster, J. (2019). A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn?. *Science & Justice*, 59(1), 83–92. <https://doi.org/10.1016/j.scijus.2018.09.006>
- Park, S., Akatyev, N., Jang, Y., Hwang, J., Kim, D., Yu, W., Shin, H., Han, C., & Kim, J. (2018). A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement. *Digital Investigation*, 24, S93–S100. <https://doi.org/10.1016/j.diin.2018.01.012>
- Quick, D., & Choo, K. K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*, 11(4), 273–294. <https://doi.org/10.1016/j.diin.2014.09.002>
- Quick, D., & Choo, K. K. R. (2018). Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix. *Future Generation Computer Systems*, 78, 558–567. <https://doi.org/10.1016/j.future.2016.12.032>
- Ramiyanto. (2017). Bukti elektronik sebagai alat bukti yang sah dalam hukum acara pidana. *Jurnal Hukum dan Peradilan*, 6(3), 463–486. <https://doi.org/10.25216/jhp.6.3.2017.463-486>
- Republik Indonesia. (1981). *Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana*. Lembaran Negara Republik Indonesia Tahun 1981 Nomor 76, Tambahan Lembaran Negara Nomor 3209. <https://www.jdih.kemenkeu.go.id/api/download/fullText/1981/8TAHUN~1981UU.HTM>
- Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. <https://peraturan.bpk.go.id/Details/37589/uu-no-11-tahun2008>
- Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. <https://peraturan.bpk.go.id/Details/37582/uu-no19-tahun-2016>
- Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. <https://peraturan.bpk.go.id/Details/274494/>
- Republik Indonesia. (2025). *Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana*. <https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025>
- Silva, T. J., Mazur, A. H. B., Oliveira Jr, E., Zorzo, A. F., & Barcellos, M. P. (2025). An ontology for promoting controlled experimentation in digital forensics. *Forensic Science International: Digital Investigation*, 52, 301845. <https://doi.org/10.1016/j.fsidi.2024.301845>
- Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*, 42, 105575. <https://doi.org/10.1016/j.clsr.2021.105575>

- Stoykova, R., Andersen, S., Franke, K., & Axelsson, S. (2022). Reliability assessment of digital forensic investigations in the Norwegian police. *Forensic Science International: Digital Investigation*, 40, 301351. <https://doi.org/10.1016/j.fsidi.2022.301351>
- Stoykova, R., & Franke, K. (2023). Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations. *Forensic Science International: Digital Investigation*, 45, 301554. <https://doi.org/10.1016/j.fsidi.2023.301554>
- Sunde, N., & Dror, I. E. (2019). Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital Investigation*, 29, 101–108. <https://doi.org/10.1016/j.diin.2019.03.011>
- Sunde, N., & Horsman, G. (2021). Part 2: The Phase-oriented Advice and Review Structure (PARS) for digital forensic investigations. *Forensic Science International: Digital Investigation*, 36, 301074. <https://doi.org/10.1016/j.fsidi.2020.301074>
- Vanessa, V., & 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>