

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 8 Tahun 2026
ISSN 3025-0919 (media online)
Hal 2161-2172

Pengelolaan Bukti Digital dalam Forensik Teknologi Informasi: Kajian Literatur atas Empat Elemen Kunci, Chain of Custody, dan Rules of Evidence

Muhammad Hamizan[1], Muhammad Faiz Akmaly[2], Muhammad Raihan Arifin[3], Rifqi Dwiyantoro[4], Muhammad Yunus Rangkuti[5*]

[1,2,3,4,5] Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Indonesia
Email: [1]mhmdhmzn31@gmail.com, [2]futaliga23@gmail.com, [3]raihanarifin0501@gmail.com, [4]rifqidwiyantoro3@gmail.com, [5*]dosen03156@unpam.ac.id
(*: corresponding author)

Abstrak–Pemanfaatan teknologi informasi diikuti oleh kejahatan yang meninggalkan jejak digital, sehingga pengelolaan bukti digital menjadi bagian penting dalam pembuktian. Artikel ini mengkaji konsep forensik teknologi informasi, karakteristik bukti digital, empat elemen kunci forensik, *chain of custody*, dan *rules of evidence*, serta relevansinya bagi penanganan kejahatan digital di Indonesia. Metode yang digunakan adalah kajian literatur konseptual dengan analisis komparatif dokumen terhadap materi ajar Pertemuan V "IT Forensik", standar dan pedoman teknis (NIST, ISO/IEC, dan IETF), literatur akademik, serta peraturan dan putusan tentang pembuktian elektronik. Sumber dipilih secara purposif dan kajian ini tidak mengklaim kelengkapan literatur. Hasil kajian menunjukkan bahwa empat elemen kunci dalam materi ajar sejalan dengan model tahapan dalam literatur, tetapi memerlukan tiga penyempurnaan: pembedaan penyimpanan, pelestarian, dan *chain of custody*; pemisahan unsur andal dan dapat dipercaya sebagaimana dalam RFC 3227 yang merinci lima properti bukti; serta penambahan dimensi teknis berupa verifikasi integritas data beserta batasnya. Kajian ini menyintesis lima tahap pengelolaan bukti digital yang dikaitkan dengan persyaratan *rules of evidence*. Menurut literatur yang dikaji, pengakuan bukti elektronik dalam UU ITE belum disertai standar *chain of custody* bukti digital yang baku dan mengikat secara nasional, sedangkan peraturan Kepolisian memuat ketentuan administratif pengelolaan barang bukti; apakah KUHAP baru mengubah keadaan itu belum diuji. Pengelolaan bukti digital yang tertib dan terdokumentasi dapat memperkuat peluang bukti diterima dalam proses hukum. Kerangka yang diusulkan bersifat konseptual dan perlu diuji pada penelitian lanjutan.

Kata kunci: forensik teknologi informasi; bukti digital; chain of custody; rules of evidence; pembuktian elektronik

Abstract–*Information technology use is accompanied by crimes that leave digital traces, making digital evidence management important to proof. This article examines the concept of information technology forensics, the characteristics of digital evidence, the four key elements of forensics, chain of custody, and rules of evidence, and their relevance to handling digital crime in Indonesia. It is a conceptual literature review with comparative document analysis of a lecture module on IT forensics, technical standards and guidelines (NIST, ISO/IEC, and IETF), academic literature, and Indonesian regulations and court decisions on electronic evidence. Sources were selected purposively, and the review does not claim to be exhaustive. The module's four key elements align with process models in the literature but need three refinements: distinguishing storage, preservation, and chain of custody; separating the reliable and believable properties, as RFC 3227 does when it lists five properties of evidence; and adding a technical dimension of integrity verification together with its limits. The article synthesizes five stages of digital evidence management linked to the rules-of-evidence requirements. According to the literature reviewed, recognition of electronic evidence in the Electronic Information and Transactions Law has not come with a nationally binding standard chain of custody for digital evidence, although police regulations contain administrative evidence-management provisions; whether the new Criminal Procedure Code changes this was not tested. Orderly, documented management can strengthen the likelihood that digital evidence is accepted in legal proceedings. The proposed framework is conceptual and requires further testing.*

Keywords: *information technology forensics; digital evidence; chain of custody; rules of evidence; electronic evidence*

1. PENDAHULUAN

Perkembangan teknologi informasi (TI) telah memindahkan sebagian besar aktivitas pemerintahan, ekonomi, dan sosial ke ruang siber. Pemanfaatan TI ini diikuti oleh kejahatan yang

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 8 Tahun 2026
ISSN 3025-0919 (media online)
Hal 2161-2172

menjadikan sistem elektronik sebagai sarana maupun sasaran. Badan Siber dan Sandi Negara (BSSN) mencatat 330.527.636 anomali trafik di Indonesia sepanjang 2024 (Nurhakim, 2025, laman 2; Samsul dkk., 2025, hlm. 6). Angka ini menunjukkan volume anomali trafik yang terdeteksi, bukan jumlah insiden, serangan yang berhasil, atau tindak pidana. Istilah dalam sumber sekunder pun belum seragam: Samsul dkk. (2025), misalnya, menyebut puncak bulanan Desember 2024 sebagai insiden tanpa menjelaskan hubungannya dengan anomali trafik. Angka tersebut karena itu dibaca sebatas gambaran skala aktivitas mencurigakan yang harus dihadapi organisasi dan aparat penegak hukum.

Kejahatan yang melibatkan sistem elektronik pada umumnya meninggalkan jejak berupa data. Jejak itu baru bernilai hukum apabila ditemukan, diamankan, dan disajikan dengan cara yang dapat dipertanggungjawabkan. Bukti digital rentan karena dapat berubah atau hilang akibat tindakan yang tidak disengaja. Pedoman pengumpulan bukti yang diterbitkan Internet Engineering Task Force (IETF) menyatakan bahwa bukti terlalu mudah dirusak, sekalipun tanpa kesengajaan (Brezinski & Killalea, 2002, §2.2). Karena itu, forensik TI dapat menjadi sarana penting pembuktian. McKemmish (1999) mendefinisikan forensik komputer sebagai proses mengidentifikasi, memelihara, menganalisis, dan menyajikan bukti digital dengan cara yang dapat diterima secara hukum.

Materi ajar Pertemuan V "IT Forensik" (Universitas Pamulang, t.t.) memperkenalkan fondasi konseptual bidang ini: pengertian forensik TI, bukti digital, empat elemen kunci forensik, manajemen bukti melalui *chain of custody* dan *rules of evidence*, serta metodologi *search and seizure*. Materi tersebut bersifat pengantar dan menyatakan bahwa forensik TI masih jarang digunakan oleh pihak berwajib di Indonesia. Pernyataan itu tidak disertai data pendukung dan perlu dikontekstualkan dengan perkembangan hukum pembuktian.

Pasal 5 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), sebagaimana diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024, menetapkan informasi elektronik dan/atau dokumen elektronik sebagai alat bukti hukum yang sah (Republik Indonesia, 2024). Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 menyatakan frasa informasi elektronik dan/atau dokumen elektronik dalam Pasal 5 ayat (1) dan ayat (2) UU ITE tidak mempunyai kekuatan hukum mengikat sepanjang tidak dimaknai khususnya sebagai alat bukti dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang (Mahkamah Konstitusi Republik Indonesia, 2016; lihat juga Heryogi dkk., 2017). Selanjutnya, Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP baru) (Republik Indonesia, 2025), yang menurut sumber sekunder berlaku sejak 2 Januari 2026, memasukkan bukti elektronik sebagai salah satu jenis alat bukti (Nugraha, 2026).

Perkembangan tersebut memunculkan tiga persoalan. Pertama, konsep dalam materi ajar belum dibandingkan dengan pedoman yang diakui secara internasional, yaitu ISO/IEC 27037:2012, NIST SP 800-86, dan RFC 3227. Kedua, kajian hukum nasional yang ditelaah melaporkan bahwa persyaratan substantif keterimaan bukti digital belum jelas dan bahwa standar *chain of custody* bukti digital yang baku dan mengikat secara nasional belum ada (Putra, 2024; Sembiring & Lasube, 2026), sehingga *chain of custody* dan *rules of evidence* dibaca sebagai penghubung praktik forensik dan hukum pembuktian, bukan sekadar konsep teknis. Ketiga, kapasitas investigator dan ahli forensik digital dilaporkan masih menjadi kendala (Putra, 2024; Sembiring & Lasube, 2026).

Berdasarkan persoalan tersebut, rumusan masalah penelitian ini adalah sebagai berikut.

1. Bagaimana konsep, ruang lingkup, dan karakteristik forensik TI serta bukti digital?
2. Bagaimana empat elemen kunci forensik TI, *chain of custody*, dan *rules of evidence* membentuk kerangka pengelolaan bukti digital, dan sejauh mana kerangka itu selaras dengan pedoman internasional?
3. Bagaimana metodologi *search and seizure* dan pencarian informasi dijalankan, serta apa tantangan yang dihadapi investigator?
4. Apa relevansi dan implikasi kerangka tersebut bagi penanganan kejahatan digital di Indonesia?

Tujuan penelitian ini adalah menjawab keempat pertanyaan tersebut melalui kajian literatur konseptual.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 8 Tahun 2026
ISSN 3025-0919 (media online)
Hal 2161-2172

Kontribusi artikel ini bersifat konseptual. Secara akademik, artikel ini memetakan secara terpisah konsep dari materi ajar dan pengembangan dari literatur eksternal sebagai landasan penelitian lanjutan. Secara praktis, artikel ini menawarkan kerangka pengelolaan bukti digital sebagai bahan rujukan awal bagi mahasiswa, praktisi TI, dan pihak lain yang berkepentingan dengan pembuktian. Kerangka itu tidak diuji secara empiris.

2. METODE PENELITIAN

2.1 Jenis dan Pendekatan Penelitian

Penelitian ini merupakan kajian literatur konseptual dengan analisis komparatif dokumen, berpendekatan kualitatif deskriptif. Pendekatannya mengacu pada ragam tinjauan integratif (*integrative literature review*) yang dibedakan Snyder (2019) dari tinjauan sistematis dan semi-sistematis, yaitu pendekatan yang menilai, mengkritisi, dan menyintesis literatur untuk membangun kerangka konseptual dan yang pada umumnya tidak memakai penelusuran sistematis. Snyder (2019) juga mensyaratkan seleksi sumber yang transparan, sehingga kriteria dan keterbatasan seleksi diuraikan pada Bagian 3.3 dan 3.5. Pendekatan ini dipilih karena objek kajian tersebar pada materi ajar, standar teknis, buku akademik, dan peraturan dari dua disiplin, yakni teknologi informasi dan hukum. Kajian ini tidak menerapkan protokol tinjauan sistematis dan tidak mengklaim kelengkapan literatur.

Penelitian ini tidak melibatkan eksperimen, wawancara, survei, maupun pengujian laboratorium. Seluruh temuan bersifat konseptual-analitis dan tidak dimaksudkan untuk digeneralisasi secara statistik.

2.2 Sumber Data

Data penelitian berupa dokumen tertulis yang dikelompokkan menjadi enam kategori sebagaimana ditunjukkan pada Tabel 2.

Tabel 2. Kategori sumber data dan perannya dalam analisis

Kategori	Sumber	Peran dalam analisis	Jenis sumber
Materi inti	Materi ajar Pertemuan V "IT Forensik" (Universitas Pamulang, t.t.)	Kerangka dasar: definisi, bukti digital, empat elemen kunci, manajemen bukti, metodologi	Bahan ajar
Standar dan pedoman teknis	RFC 3227 (Brezinski & Killalea, 2002); NIST SP 800-86 (Kent dkk., 2006); ISO/IEC 27037:2012; ISO/IEC 27042:2015	Pembanding dan penguat prosedur forensik	Standar dan pedoman
Literatur akademik	McKemmish (1999); Reith dkk. (2002); Ó Ciardhuáin (2004); Carrier dan Spafford (2006); Casey (2011); Snyder (2019); DFRWS (2001)	Landasan teori, model tahapan, dan metodologi kajian	Jurnal, laporan, buku, laman konferensi
Peraturan dan putusan	UU 8/1981 (KUHAP lama); UU 1/2024; UU 20/2025; Putusan MK 20/PUU-XIV/2016; Peraturan Kepala Kepolisian (Perkap) 10/2009 dan 10/2010	Konteks hukum pembuktian di Indonesia	Hukum primer (UU 20/2025 dikaji lewat sumber sekunder)
Literatur hukum nasional	Heryogi dkk. (2017); Putra (2024); Sembiring dan Lasube (2026)	Pembanding kondisi hukum dan praktik	Jurnal
Sumber pendukung nonakademik	Nugraha (2026); Giovani (2026); Nurhakim (2025); Samsul dkk. (2025)	Perkembangan terkini dan data ancaman	Klinik hukum, opini, berita, laporan analisis anggaran

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 8 Tahun 2026
ISSN 3025-0919 (media online)
Hal 2161-2172

2.3 Teknik Pengumpulan Data

Sumber dipilih secara purposif dalam enam kelompok sebagaimana Tabel 2, yang berpangkal pada materi ajar sebagai kerangka dasar. Penelusuran dilakukan secara daring pada situs atau basis data yang benar-benar dipakai dengan kata kunci pada rentang tanggal akses. Standar, peraturan, putusan, artikel jurnal, dan buku dipakai sebagai dasar klaim. Tulisan opini, klinik hukum, dan berita dipakai sebagai sumber pendukung nonakademik; klaim hukum yang bersandar padanya diperiksa terhadap teks primer atau dinyatakan sebagai pendapat penulis tulisan tersebut.

Sumber dimasukkan apabila (1) relevan dengan bukti digital, forensik teknologi informasi, atau pembuktian elektronik; (2) identitas bibliografisnya dapat diverifikasi; (3) berupa standar, peraturan, putusan, buku, artikel jurnal, laporan lembaga, atau tulisan nonakademik yang diberi status pendukung; dan (4) berbahasa Indonesia atau Inggris. Sumber dikeluarkan apabila tidak memiliki penulis atau penerbit yang jelas atau tidak dapat diakses. Relevansi dinilai dari kesesuaian sumber dengan salah satu tema analisis pada Bagian 3.4. Mutu dinilai dari jenis sumber (primer, akademik, atau nonakademik) dan dari kemungkinan mencocokkan klaim yang dikutip dengan teks aslinya.

2.4 Teknik Analisis Data

Analisis dilakukan dalam tiga langkah. Pertama, konsep dalam materi ajar dikelompokkan ke dalam tema: konsep dasar, bukti digital, empat elemen kunci, manajemen bukti, dan metodologi investigasi. Kedua, setiap tema dibandingkan dengan standar dan literatur eksternal untuk melihat kesesuaian, perbedaan, dan celah. Ketiga, hasil perbandingan disintesis secara kritis menjadi kerangka pengelolaan bukti digital beserta implikasinya bagi konteks Indonesia. Agar keterlacakan terjaga, bagian Hasil dan Pembahasan menandai gagasan dari materi ajar dan gagasan dari literatur eksternal, dan setiap klaim hukum dibedakan menjadi ketentuan tertulis, putusan, atau pendapat penulis sumber.

2.5 Keterbatasan

Kajian ini tidak memuat data kasus empiris, dan ketentuan hukum dapat berubah. Penelusuran tidak sistematis sehingga sumber yang relevan mungkin terlewat. Isi ISO/IEC 27037 dan ISO/IEC 27042 dianalisis dari abstrak dan cakupan, atau teks lengkap, dan ketentuan UU 20/2025 dari teks resmi atau sumber sekunder. Status berlaku dan perubahan Perkap 10/2009 dan 10/2010 belum dikonfirmasi pada sumber resmi. Sebagian rujukan hukum berupa opini, dan kerangka yang diusulkan belum divalidasi oleh praktisi. Temuan karena itu perlu diuji melalui studi kasus atau wawancara dengan praktisi forensik digital.

3. ANALISA DAN PEMBAHASAN

Pembahasan disusun mengikuti rumusan masalah. Pada setiap subbagian, gagasan yang berasal dari materi ajar, pengembangan dari literatur eksternal, dan analisis penulis ditandai secara eksplisit.

3.1 Konsep Dasar dan Ruang Lingkup IT Forensik

Materi ajar. Modul memosisikan forensik TI sebagai perluasan dari forensik komputer. Cakupannya meliputi telepon seluler, kamera digital, dan kartu pintar, sehingga forensik TI tidak identik dengan komputer atau internet. Modul juga mencatat bahwa di Indonesia forensik komputer biasanya dilakukan tanpa memeriksa isi komputer, padahal bukti akan lebih banyak ditemukan jika isinya diidentifikasi.

Pengembangan literatur. Cakupan lintas perangkat ini dikukuhkan oleh ISO/IEC 27037:2012 (Bagian 2.2). NIST menambahkan bahwa forensik disajikan dari sudut pandang TI, bukan penegakan hukum, sehingga penggunaannya mencakup pemecahan masalah operasional dan pemulihan sistem (Kent dkk., 2006).

Analisis penulis. Definisi Parra (2002, dalam materi ajar) dan McKemmish (1999) sama-sama mengikat proses teknis pada syarat hukum, sehingga keberhasilan forensik TI diukur dari apakah hasilnya dapat dipakai dalam proses hukum, bukan dari kecanggihan alat. Karena NIST mengakui kegunaan forensik di luar proses pidana (Kent dkk., 2006), definisi dalam materi ajar

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 8 Tahun 2026
ISSN 3025-0919 (media online)
Hal 2161-2172

bersifat yuridis-sentris. Ruang lingkup forensik TI karena itu sebaiknya dibedakan menjadi forensik untuk pembuktian hukum dan forensik untuk kepentingan operasional organisasi.

3.2 Jenis dan Karakteristik Bukti Digital

Materi ajar. Bukti digital dibedakan menjadi bukti riil dan bukti abstrak yang harus diolah lebih dahulu; contohnya telah disebut pada Bagian 2.2.

Pengembangan literatur. RFC 3227 menegaskan bahwa bukti terlalu mudah dirusak tanpa disengaja (§2.2) dan menganjurkan agar salinan tingkat bit dari media dibuat (Brezinski & Killalea, 2002). Dalam konteks hukum Indonesia, Putra (2024) menyatakan bahwa konsep "asli" menjadi problematik karena salinan digital sering identik bit demi bit dengan sumbernya, sehingga fokus bergeser ke *chain of custody*.

Analisis penulis. Karakteristik bukti digital dan implikasinya bagi pengelolaan dirangkum pada Tabel 3.

Tabel 3. Karakteristik bukti digital dan implikasinya bagi pengelolaan

Karakteristik	Implikasi bagi pengelolaan	Dasar
Mudah berubah atau hilang	Pengumpulan dari data yang paling mudah hilang; tindakan pemeriksa dicatat	Brezinski & Killalea (2002, §2.1, §2.2); McKemmish (1999)
Dapat disalin identik	Keaslian dibuktikan melalui integritas dan catatan penguasaan, bukan melalui "benda asli"	Putra (2024)
Sering berbentuk abstrak	Perlu pengolahan dan interpretasi oleh pihak yang kompeten	Materi ajar; ISO/IEC (2015)
Tersebar pada banyak jenis perangkat	Prosedur harus mencakup ponsel, kamera, dan jaringan, bukan hanya komputer	ISO/IEC (2012)

3.3 Empat Elemen Kunci: Tahapan dan Analisis Kritis

Identifikasi. Materi ajar menempatkan identifikasi sebagai tahap paling awal, yaitu menentukan lokasi bukti, tempat penyimpanannya, dan caranya. ISO/IEC 27037:2012 juga menempatkan identifikasi sebagai aktivitas pertama, berdampingan dengan pengumpulan, akuisisi, dan pelestarian (ISO/IEC, 2012). Dalam pembacaan penulis, identifikasi adalah keputusan tentang apa yang relevan, sehingga bergantung pada kompetensi dan otorisasi. Casey (2011) memasukkan otorisasi sebagai bagian dari penanganan tempat kejadian perkara digital.

Penyimpanan dan pelestarian. Materi ajar menyebut tahap ini paling kritis karena bukti harus tetap tidak berubah bentuk, isi, dan maknanya dalam jangka lama. Isinya sebenarnya mencakup dua hal yang berbeda. Pertama, pelestarian (*preservation*), yakni tindakan menjaga bukti agar tidak berubah; di sini RFC 3227 menambahkan bahwa pengumpulan didahulukan sebelum analisis dan bahwa salinan tingkat bit perlu dibuat (Brezinski & Killalea, 2002). Kedua, penyimpanan dalam arti tempat dan kondisi bukti disimpan. *Chain of custody* berbeda dari keduanya: ia adalah catatan yang menunjukkan bagaimana penguasaan dan penanganan bukti terjaga (Brezinski & Killalea, 2002, §4.1). Tumpang tindih antara "penyimpanan" dan *chain of custody* dalam materi ajar sebagian bersumber dari terjemahan *preservation* menjadi "penyimpanan". ISO/IEC 27037 memisahkan pengumpulan, akuisisi, dan pelestarian sebagai aktivitas tersendiri (ISO/IEC, 2012), sehingga pemisahan serupa dapat memperjelas kerangka dalam materi ajar.

Analisis. Materi ajar mencakup pengambilan, pemrosesan, dan interpretasi bukti dengan skema yang bergantung pada kasus. NIST memisahkan pemeriksaan dan analisis (Kent dkk., 2006), dan ISO/IEC 27042:2015 secara khusus mengatur analisis dan interpretasi bukti digital (ISO/IEC, 2015). Pembedaan itu penting karena interpretasi adalah titik tempat kesimpulan dibentuk, sehingga memerlukan metode yang dapat diuji. Carrier dan Spafford (2006) menyebut persyaratan ketelitian ilmiah dari luar investigasi, dengan kriteria Daubert sebagai contoh.

Presentasi. Materi ajar menggambarkan presentasi sebagai proses persidangan yang menguji otentikasi bukti dan korelasinya dengan kasus. Giovani (2026) berpendapat bahwa keterangan ahli forensik digital penting untuk autentikasi bukti elektronik dan bahwa KUHAP baru belum

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 8 Tahun 2026
ISSN 3025-0919 (media online)
Hal 2161-2172

menyediakan kriteria bagi hakim untuk menilai mutu metode ahli; pendapat itu belum diuji terhadap teks resmi UU 20/2025. Definisi presentasi dalam materi ajar tampak terlalu sempit, karena laporan hasil forensik juga dipakai di luar persidangan, misalnya dalam penanganan insiden oleh organisasi (Kent dkk., 2006).

Tabel 4 membandingkan empat elemen materi ajar dengan model tahapan dalam literatur. Empat elemen tersebut merupakan ringkasan dari model yang lebih rinci.

Tabel 4. Perbandingan tahapan forensik dalam materi ajar dan model dalam literatur

Sumber	Tahapan	Jumlah
Materi ajar	Identifikasi, penyimpanan, analisis, presentasi	4
McKemmish (1999)	Mengidentifikasi, memelihara (*preservation*), menganalisis, menyajikan	4
Kent dkk. (2006)	Pengumpulan, pemeriksaan, analisis, pelaporan	4
Model DFRWS (Palmer, 2001, dalam Ó Ciardhuáin, 2004)	Identifikasi, pelestarian, pengumpulan, pemeriksaan, analisis, presentasi, keputusan	7
Reith dkk. (2002)	Identifikasi, persiapan, strategi pendekatan, pelestarian, pengumpulan, pemeriksaan, analisis, presentasi, pengembalian bukti	9

3.4 Penerapan Chain of Custody dalam Pengelolaan Bukti

Materi ajar. Modul menyebut empat cara menjaga bukti: catatan lengkap keluar-masuk bukti dari penyimpanan, penyimpanan di tempat aman, akses terbatas, dan pencatatan pihak yang dapat mengakses. Tujuannya agar bukti tetap asli dan tetap sama seperti saat ditemukan ketika persidangan digelar.

Pengembangan literatur. RFC 3227 §4.1 mengharuskan pengelola bukti dapat menjelaskan bagaimana bukti ditemukan, ditangani, dan apa saja yang terjadi padanya. Yang didokumentasikan mencakup di mana, kapan, dan oleh siapa bukti ditemukan, dikumpulkan, ditangani, atau diperiksa; siapa menguasai bukti pada periode tertentu dan bagaimana bukti disimpan; serta kapan dan bagaimana penguasaan berpindah (Brezinski & Killalea, 2002). Dalam literatur hukum Indonesia, Putra (2024) dan Sembiring dan Lasube (2026) melaporkan bahwa standar *chain of custody* bukti digital yang baku dan mengikat secara nasional belum ada. Putra (2024) juga menyimpulkan bahwa kekuatan bukti dalam putusan pengadilan sering bergantung pada pembuktian integritas dan keaslian, bukan pada standar normatif yang jelas. Giovani (2026) menyatakan bahwa jika rantai penguasaan tidak dapat ditunjukkan secara utuh, hakim dapat mengurangi bobot bukti elektronik atau mengesampingkannya.

Peraturan Kepolisian. Pernyataan bahwa standar baku belum ada perlu dibaca bersama dua peraturan Kepolisian. Peraturan Kepala Kepolisian Nomor 10 Tahun 2009 tentang tata cara dan persyaratan permintaan pemeriksaan teknis kriminalistik tempat kejadian perkara dan laboratoris kriminalistik barang bukti kepada Laboratorium Forensik Polri (Perkap 10/2009) memuat prinsip keaslian, yaitu barang bukti dijaga keasliannya dari tempat kejadian perkara sampai diterima di Laboratorium Forensik (Pasal 3), serta persyaratan formal dan teknis permintaan pemeriksaan barang bukti elektronik, telekomunikasi, dan komputer, termasuk pengemasan dan penyegelan (Pasal 17–21; Republik Indonesia, 2009). Peraturan Kepala Kepolisian Nomor 10 Tahun 2010 tentang tata cara pengelolaan barang bukti di lingkungan Polri (Perkap 10/2010) mengatur penerimaan dan pencatatan dalam buku register, pengeluaran dengan berita acara, dan pengawasan melalui buku kontrol (Pasal 8, 12, 15, 17, dan 27; Republik Indonesia, 2010), dan tidak memuat kata "elektronik", "digital", maupun "komputer". Pada pasal yang ditelaah, ketentuan yang merinci pencatatan rantai penguasaan bukti digital tidak ditemukan. Penelusuran belum mencakup peraturan lembaga penegak hukum lain, prosedur operasional internal, maupun standar nasional lain.

Analisis penulis. Empat cara dalam materi ajar bersifat administratif. Pada bukti digital, penjagaan juga memerlukan dimensi teknis, yaitu verifikasi bahwa isi data tidak berubah. NIST SP 800-86 §3.1.2 menyebut pemakaian *message digest* untuk memverifikasi integritas salinan data (Kent dkk., 2006), dan RFC 3227 §3.2 menganjurkan, bila memungkinkan, pembuatan *checksum* dan penandatanganan kriptografis atas bukti karena hal itu dapat memudahkan penjagaan rantai

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 8 Tahun 2026
ISSN 3025-0919 (media online)
Hal 2161-2172

bukti (Brezinski & Killalea, 2002). Giovani (2026) menanyakan apakah nilai hash data sama sejak penyitaan hingga persidangan dan apakah setiap perpindahan bukti tercatat, sebagai dua dari enam pertanyaan untuk menilai keterangan ahli.

Hash perlu dipahami batasnya. Nilai hash menunjukkan bahwa salinan identik dengan data yang di-hash pada saat itu. Hash tidak menunjukkan bahwa isi data benar, bahwa data belum berubah sebelum di-hash, atau bahwa bukti diperoleh secara sah. Verifikasi hash karena itu melengkapi, dan tidak menggantikan, pencatatan penguasaan bukti. Pemilihan algoritma hash yang memadai berada di luar cakupan artikel ini. Berdasarkan sintesis tersebut, penulis mengusulkan unsur pencatatan pada Tabel 5.

Tabel 5. Usulan unsur pencatatan chain of custody untuk bukti digital

Unsur	Isi catatan	Dasar
Identitas dan asal bukti	Jenis perangkat atau data, lokasi ditemukan, dan waktu ditemukan	Materi ajar; Brezinski & Killalea (2002, §4.1)
Penangan	Siapa yang mengakses atau memindahkan bukti	Brezinski & Killalea (2002, §4.1); Putra (2024)
Waktu dan tempat	Kapan dan di mana setiap perpindahan terjadi	Brezinski & Killalea (2002, §4.1); Putra (2024)
Tujuan tindakan	Alasan akses atau pemrosesan	Putra (2024); McKemmish (1999)
Integritas data	Nilai hash pada saat pengumpulan dan pada setiap pemeriksaan, dengan batas hash dicatat	Kent dkk. (2006, §3.1.2); Brezinski & Killalea (2002, §3.2)
Penyimpanan dan akses	Tempat penyimpanan, pembatasan akses, dan daftar pihak berwenang	Materi ajar; Brezinski & Killalea (2002, §4.1)

Unsur dalam tabel tersebut merupakan usulan penulis berdasarkan sintesis sumber dan belum diuji pada kasus nyata.

3.5 Persyaratan Rules of Evidence

Materi ajar menyebut empat persyaratan, sedangkan RFC 3227 §2.4 merinci lima properti bukti komputer (Brezinski & Killalea, 2002). Subbagian ini membahas keempat persyaratan dalam materi ajar dan memisahkan unsur andal dari unsur dapat dipercaya sebagaimana dalam RFC.

Dapat diterima (*admissible*). Materi ajar menyatakan bahwa bukti harus dapat diterima dan digunakan demi hukum, mulai dari penyidikan hingga pengadilan. RFC 3227 §2.4 merumuskannya sebagai kesesuaian bukti dengan aturan hukum tertentu sebelum disampaikan kepada pengadilan (Brezinski & Killalea, 2002). Pasal 5 UU ITE menetapkan informasi elektronik dan/atau dokumen elektronik sebagai alat bukti hukum yang sah, dan Penjelasan Pasal 5 ayat (2) UU 1/2024 mensyaratkan bahwa hasil intersepsi atau penyadapan dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi lain yang kewenangannya ditetapkan berdasarkan undang-undang (Republik Indonesia, 2024), rumusan yang serupa dengan amar Putusan MK 20/PUU-XIV/2016 (Mahkamah Konstitusi Republik Indonesia, 2016). Giovani (2026) menyatakan, tanpa menyebut nomor pasal, bahwa KUHAP baru mewajibkan setiap alat bukti dapat dibuktikan autentikasinya dan diperoleh secara tidak melawan hukum; pernyataan itu belum diperiksa terhadap teks UU 20/2025. Dengan demikian, keterimaan bukti digital di Indonesia tampak bergantung pada legalitas cara memperoleh bukti dan kemampuan membuktikan autentikasinya, sedangkan Putra (2024) menilai persyaratan substantif keterimaan masih belum jelas.

Asli (*authentic*). Materi ajar mensyaratkan bukti berhubungan dengan kejadian dan bukan rekayasa. RFC 3227 §2.4 menyatakan bahwa bukti harus dapat dikaitkan secara positif dengan insiden (Brezinski & Killalea, 2002). Penulis membaca persyaratan ini berlapis: hubungan bukti dengan kasus (relevansi) dan ketiadaan rekayasa (integritas). Lapis kedua dapat didukung melalui *chain of custody* dan verifikasi hash, dengan batas hash sebagaimana diuraikan pada Bagian 4.4, sedangkan penilaian akhirnya sering memerlukan keterangan ahli forensik digital (Giovani, 2026).

Lengkap (*complete*). Materi ajar memandang bukti lengkap jika memuat banyak petunjuk yang membantu investigasi. RFC 3227 §2.4 mensyaratkan bukti menceritakan keseluruhan kisah dan bukan hanya satu perspektif, dan §2 mengarahkan pengumpul bukti agar menangkap gambaran

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 8 Tahun 2026
ISSN 3025-0919 (media online)
Hal 2161-2172

sistem seakurat mungkin (Brezinski & Killalea, 2002). Kelengkapan karena itu juga dapat dimaknai sebagai cakupan konteks yang memadai agar interpretasi tidak parsial.

Andal (*reliable*) dan dapat dipercaya (*believable*). Materi ajar menggabungkan keduanya sebagai "dapat dipercaya dan andal". Menurut RFC 3227 §2.4, bukti andal bila cara pengumpulan dan penanganannya tidak menimbulkan keraguan atas keaslian dan kebenarannya, dan dapat dipercaya bila mudah dipercaya dan dipahami oleh pengadilan (Brezinski & Killalea, 2002). Pembedaan ini membantu merumuskan indikator masing-masing. Dalam pembacaan penulis, unsur andal dapat diperiksa melalui metode pengumpulan yang terbuka dan dapat diulang (Brezinski & Killalea, 2002, §3.1) serta catatan penanganan yang utuh, sedangkan unsur dapat dipercaya diperiksa melalui kejelasan penyajian bagi pengadil fakta. Carrier dan Spafford (2006) menyebut kriteria Daubert sebagai contoh persyaratan ketelitian ilmiah, dan Giovani (2026) mengajukan enam pertanyaan untuk menilai keterangan ahli, yakni kompetensi, metode perolehan, integritas, standar dan replikasi, batas kesimpulan ahli, dan rantai penguasaan.

3.6 Metodologi Search and Seizure dan Pencarian Informasi

Materi ajar. Modul menempatkan investigator sebagai pihak yang berwenang menyita bukti dalam koridor hukum, dengan pencarian informasi dalam tiga tahap sebagaimana diuraikan pada Bagian 2.5.

Pengembangan literatur. Casey (2011) membahas penanganan tempat kejadian perkara digital, termasuk pelestarian data yang mudah hilang (*volatile data*). RFC 3227 §2.1 mengurutkan pengumpulan dari register dan cache, tabel sistem dan memori, berkas sementara, dan disk, hingga data pencatatan jarak jauh (*remote logging*), konfigurasi fisik, dan media arsip. Pedoman itu juga menganjurkan agar sistem tidak dimatikan sebelum pengumpulan bukti selesai dan mengingatkan bahwa memutus sambungan jaringan dapat memicu mekanisme *deadman switch* yang menghapus bukti (Brezinski & Killalea, 2002, §2.2). Prosedur nasional berbeda pendekatan: Perkap 10/2009 Pasal 21 ayat (1) huruf b mengarahkan pencabutan kabel input komputer dari sumber arus listrik sebelum komputer dimatikan secara kasar (*shut down*), sedangkan Pasal 20 ayat (2) huruf a mengakui bahwa bukti komputer bersifat mudah hilang atau berubah (*volatile*) (Republik Indonesia, 2009).

Analisis penulis. Urutan tiga tahap dalam materi ajar perlu dibaca dengan hati-hati. Jika penyitaan media penyimpanan dilakukan sebelum data volatil diamankan, bukti yang paling mudah hilang berisiko tidak tercatat. Namun RFC 3227 §2.2 menganjurkan agar pengumpulan bukti selesai sebelum sistem dimatikan, sedangkan Perkap 10/2009 Pasal 21 ayat (1) huruf b mengarahkan pencabutan kabel input komputer. Pilihan tindakan perlu menimbang risiko hilangnya data volatil dan prosedur yang berlaku bagi penyidik; kajian ini tidak menilai mana yang lebih tepat. Pada perangkat yang masih menyala, pengamanan data volatil dan penelusuran log perlu dipertimbangkan menurut urutan volatilitas. Kewenangan penyitaan menurut hukum acara tidak ditelaah rinci dan dicatat sebagai keterbatasan.

3.7 Tantangan Investigator dalam Menangani Kejahatan Berbasis Teknologi

Materi ajar. Modul menyatakan bahwa tahapan pencarian informasi tampak mudah, tetapi sulit dilakukan di lapangan. Investigator yang biasa menangani kasus kriminal non-teknis cenderung terburu-buru mengambil barang bukti, sehingga barang bukti penting kadang ditinggalkan, padahal celah yang banyak tersedia pada media komputer menuntut investigator lebih cakap dan teliti.

Pengembangan literatur. Literatur memperkuat temuan itu. Reith dkk. (2002) mengidentifikasi kurangnya standardisasi forensik digital sebagai masalah. Sembiring dan Lasube (2026) melaporkan keterbatasan tenaga ahli forensik digital dan disparitas pemahaman hakim terhadap teknologi digital, dan Putra (2024) menyebut disparitas kapasitas penegak hukum. Giovani (2026) mengulang temuan keterbatasan ahli bersertifikasi dengan merujuk Sembiring dan Lasube (2026), lalu menambahkan pendapatnya bahwa KUHAP baru belum menyediakan kriteria bagi hakim untuk menilai mutu metode ahli.

Analisis penulis. Tantangan tersebut dapat dikelompokkan menjadi empat dimensi, sebagaimana Tabel 6.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 8 Tahun 2026
ISSN 3025-0919 (media online)
Hal 2161-2172

Tabel 6. Dimensi tantangan penanganan bukti digital

Dimensi	Wujud tantangan	Sumber
Kompetensi	Investigator terburu-buru; ahli bersertifikasi terbatas dan tidak merata	Materi ajar; Sembiring & Lasube (2026); Giovani (2026)
Standar prosedur	Standar *chain of custody* bukti digital yang baku dan mengikat secara nasional belum ada; standardisasi forensik kurang	Putra (2024); Sembiring & Lasube (2026); Reith dkk. (2002)
Penilaian di pengadilan	Pemahaman hakim berbeda-beda (Sembiring & Lasube, 2026); kriteria menilai mutu metode ahli belum tersedia menurut Giovani (2026)	Sembiring & Lasube (2026); Giovani (2026)
Kerangka hukum	Persyaratan substantif keterimaan bukti belum jelas	Putra (2024)

Dalam pembacaan penulis, keempat dimensi ini saling bergantung. Standar prosedur yang baik tidak berguna tanpa investigator yang mampu menerapkannya, dan investigator yang kompeten tetap menghadapi ketidakpastian jika hakim tidak memiliki kriteria untuk menilai hasil kerjanya.

3.8 Relevansi IT Forensik bagi Penanganan Kejahatan Digital di Indonesia

Kerangka hukum pembuktian Indonesia berkembang cukup jauh. KUHAP lama (UU 8/1981) mengenal lima alat bukti dalam Pasal 184 ayat (1), yaitu keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa, dan tidak menyebut bukti elektronik (Republik Indonesia, 1981). Pengakuan bukti elektronik datang dari UU ITE (Republik Indonesia, 2024), dengan syarat pemaknaan dari Putusan MK 20/PUU-XIV/2016 (Bagian 1.1). Menurut Nugraha (2026), KUHAP baru memasukkan bukti elektronik sebagai jenis alat bukti pada Pasal 235 ayat (1) dan memaknainya pada Pasal 242 sebagai informasi elektronik, dokumen elektronik, dan/atau sistem elektronik yang berkaitan dengan tindak pidana. Rujukan pasal ini bersumber dari tulisan sekunder tersebut dan belum dicocokkan dengan teks resmi UU 20/2025.

Dalam pembacaan penulis, pernyataan materi ajar bahwa forensik TI jarang digunakan perlu dibaca sebagai gambaran kondisi umum, bukan kesimpulan tentang kebutuhan saat ini. Menurut Giovani (2026), autentikasi dan perolehan bukti yang sah kini menjadi syarat penggunaan alat bukti, sehingga kebutuhan akan forensik TI dapat dibaca menguat. Pengakuan normatif belum sama dengan standar prosedural: Putra (2024) dan Sembiring dan Lasube (2026) menunjukkan celah pada aspek *chain of custody*, sedangkan kajian ini belum menguji apakah KUHAP baru mengubah keadaan tersebut.

Kepolisian memiliki regulasi internal yang relevan, yaitu Perkap 10/2009 dan Perkap 10/2010 (Republik Indonesia, 2009, 2010), yang pasalnya diuraikan pada Bagian 4.4 dan 4.6. Keduanya mengatur pengelolaan barang bukti secara administratif, dan Perkap 10/2009 memuat ketentuan pengamanan komputer, tetapi pada pasal yang ditelaah tidak ditemukan prosedur *chain of custody* bukti digital yang dirinci. Status berlaku dan perubahan keduanya belum dikonfirmasi pada sumber resmi.

Angka anomali trafik BSSN pada Bagian 1.1 tidak menunjukkan jumlah insiden, serangan yang berhasil, atau tindak pidana, sehingga tidak dipakai untuk menaksir kebutuhan penanganan bukti; kebutuhan itu perlu dinilai dari data kasus yang tidak tersedia dalam kajian ini. Berdasarkan uraian di atas, penulis menarik empat implikasi: (1) kebutuhan akan prosedur operasional *chain of custody* yang dirinci khusus bagi bukti digital, selain ketentuan administratif yang telah ada; (2) kebutuhan akan kriteria penilaian keterangan ahli, apabila pendapat Giovani (2026) bahwa kriteria itu belum tersedia terbukti pada teks resmi UU 20/2025; (3) peningkatan kompetensi investigator dan pemahaman hakim; dan (4) manfaat menjadikan ISO/IEC 27037 sebagai rujukan prosedur, sebagaimana diusulkan Giovani (2026). Keempatnya merupakan usulan penulis dan bukan ketentuan hukum.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 8 Tahun 2026
ISSN 3025-0919 (media online)
Hal 2161-2172

3.9 Sintesis: Kerangka Pengelolaan Bukti Digital

Hasil pembahasan disintesis menjadi kerangka pengelolaan bukti digital pada Tabel 7, yang menghubungkan lima tahap pengelolaan dengan properti rules of evidence yang dilindungi pada tiap tahap. Kerangka ini merupakan sintesis konseptual penulis dan belum diuji secara empiris.

Tabel 7. Kerangka sintesis pengelolaan bukti digital

Tahap	Tujuan	Praktik kunci	Properti yang dilindungi	Rujukan
Identifikasi dan otorisasi	Menentukan sumber bukti dan dasar kewenangan	Identifikasi lintas perangkat; memastikan otorisasi	Dapat diterima; lengkap	Materi ajar; ISO/IEC (2012)
Pengumpulan dan pelestarian	Mengamankan bukti tanpa mengubahnya	Urutan volatilitas dengan menimbang prosedur penyidik; salinan tingkat bit; pengumpulan sebelum analisis; pencatatan nilai hash beserta batasnya	Asli; andal	Brezinski & Killalea (2002); Kent dkk. (2006); Republik Indonesia (2009)
Penyimpanan dan chain of custody	Menjaga bukti tetap sama dan penguasaannya tercatat hingga persidangan	Catatan keluar-masuk; akses terbatas; unsur pada Tabel 5	Asli; dapat diterima	Materi ajar; Brezinski & Killalea (2002, §4.1); Putra (2024)
Analisis dan interpretasi	Menafsirkan bukti dengan metode yang dapat diuji	Pemisahan pemeriksaan dan analisis; dokumentasi metode; pembatasan kesimpulan	Andal; lengkap	Kent dkk. (2006); ISO/IEC (2015); Giovani (2026)
Presentasi dan pelaporan	Menyajikan bukti agar dapat diuji autentikasi dan korelasinya	Laporan terdokumentasi; keterangan ahli	Dapat dipercaya; dapat diterima	Materi ajar; Giovani (2026)

4. KESIMPULAN

Penelitian ini menjawab empat tujuan yang dirumuskan pada bagian pendahuluan.

Pertama, forensik TI adalah proses mengidentifikasi, memelihara, menganalisis, dan menyajikan bukti digital dengan cara yang dapat diterima secara hukum, dan cakupannya melampaui komputer hingga ponsel, kamera, dan jaringan. Bukti digital mudah berubah, dapat disalin identik, sering berbentuk abstrak, dan tersebar pada banyak perangkat, dan karakteristik itu memengaruhi cara pengelolaannya. Definisi dalam materi ajar bersifat yuridis-sentris, sehingga perlu dilengkapi pengakuan atas kegunaan forensik untuk kepentingan operasional organisasi.

Kedua, empat elemen kunci dalam materi ajar sejalan dengan model tahapan dalam literatur dan standar, tetapi memerlukan tiga penyempurnaan: penyimpanan, pelestarian, dan *chain of custody* perlu dibedakan; properti andal dan dapat dipercaya perlu dipisahkan sebagaimana dalam RFC 3227 §2.4; dan *chain of custody* perlu dilengkapi verifikasi integritas data beserta batasnya. Hasil sintesisnya berupa kerangka lima tahap pengelolaan bukti digital yang dikaitkan dengan properti *rules of evidence* (Tabel 7).

Ketiga, metodologi *search and seizure* dan pencarian informasi perlu mempertimbangkan urutan volatilitas agar data yang paling mudah hilang tidak terabaikan, dengan tetap menimbang prosedur yang berlaku bagi penyidik, misalnya Perkap 10/2009 Pasal 21 yang berbeda pendekatan dari RFC 3227 §2.2. Tantangan investigator mencakup kompetensi, standar prosedur, penilaian di pengadilan, dan kerangka hukum yang saling bergantung.

Keempat, UU ITE telah mengakui bukti elektronik, dan menurut sumber sekunder KUHAP baru memasukkannya sebagai jenis alat bukti. Menurut literatur yang dikaji, pengakuan itu belum

disertai standar *chain of custody* bukti digital yang baku dan mengikat secara nasional, sedangkan peraturan Kepolisian memuat ketentuan administratif pengelolaan barang bukti. Menurut Giovani (2026), KUHAP baru juga belum menyediakan kriteria penilaian keterangan ahli; pendapat ini belum diuji terhadap teks resmi UU 20/2025. Pengelolaan bukti digital yang tertib, terdokumentasi, dan dapat diverifikasi dapat memperkuat peluang bukti diterima dan dipercaya dalam proses hukum, meskipun penilaian akhir berada pada pengadil fakta. Nilai suatu bukti digital dipengaruhi bukan hanya oleh isinya, melainkan juga oleh cara bukti itu dikelola.

Penelitian ini memiliki keterbatasan karena bersifat konseptual, tidak menggunakan data kasus, dan tidak menelaah teks resmi UU 20/2025 secara langsung. Penelitian berikutnya dapat dilakukan dengan:

1. menganalisis putusan pengadilan yang memuat bukti digital setelah KUHAP baru berlaku;
2. mewawancarai praktisi forensik digital, penyidik, dan hakim untuk menguji kerangka pada Tabel 7;
3. menelaah teks resmi UU 20/2025 serta peraturan kepolisian dan peraturan lembaga penegak hukum lain tentang pemeriksaan dan pengelolaan barang bukti terhadap ISO/IEC 27037 dan ISO/IEC 27042; dan
4. menguji unsur pencatatan *chain of custody* pada Tabel 5 melalui simulasi di laboratorium forensik digital.

REFERENCES

Brezinski, D., & Killalea, T. (2002). *Guidelines for evidence collection and archiving* (RFC 3227; BCP 55). Internet Engineering Task Force. https://www.rfc-editor.org/info/rfc3227

Carrier, B. D., & Spafford, E. H. (2006). Categories of digital investigation analysis techniques based on the computer history model. *Digital Investigation, 3*(Suppl.), S121–S130. https://doi.org/10.1016/j.diin.2006.06.011

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd ed.). Academic Press.

Digital Forensic Research Workshop. (2001). *DFRWS USA 2001*. https://dfrws.org/conferences/dfrws-usa-2001/

Giovani. (2026, 7 November). Keterangan ahli digital forensik dalam autentikasi bukti elektronik di KUHAP baru. *Dandapala*. https://www.dandapala.com/article/detail/keterangan-ahli-digital-forensik-dalam-autentikasi-bukti-elektronik-di-kuhap-baru

Heryogi, A., Ruba'i, M., & Sugiri, B. (2017). Fungsi bukti elektronik dalam hukum acara pidana pasca Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016. *Jurnal Ilmiah Pendidikan Pancasila dan Kewarganegaraan, 2*(1). https://doi.org/10.17977/um019v2i12017p007

ISO/IEC. (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

ISO/IEC. (2015). *Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence* (ISO/IEC 27042:2015). https://www.iso.org/standard/44406.html

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

Mahkamah Konstitusi Republik Indonesia. (2016). *Putusan Nomor 20/PUU-XIV/2016* [Putusan diucapkan 7 September 2016]. https://s.mkri.id/public/content/persidangan/putusan/20_PUU-XIV_2016.pdf

McKemmish, R. (1999). *What is forensic computing?* (Trends & Issues in Crime and Criminal Justice No. 118). Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2020-05/tandi118.pdf

Nugraha, M. R. (2026, 6 Januari). Dasar hukum alat bukti elektronik dalam KUHAP. *Hukumonline*. https://www.hukumonline.com/klinik/a/dasar-hukum-alat-bukti-elektronik-dalam-kuhap-cl5461/

Nurhakim, F. (2025, 26 Agustus). BSSN: Phising modus yang banyak ditemui, warga diminta waspada. *Bloomberg Technoz*. https://www.bloombergtechnoz.com/detail-news/81920/bssn-phising-modus-yang-banyak-ditemui-warga-diminta-waspada

Ó Ciardhuáin, S. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence, 3*(1).

Putra, G. R. A. (2024). Kedudukan bukti digital dalam sistem peradilan pidana Indonesia: Rekonsepsi pengaturan dan penguatan chain of custody di era cyber-enabled crime. *Buletin Adalah, 8*(7), 1–16. https://doi.org/10.15408/adalah.v8i7.51879

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence, 1*(3).



JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 8 Tahun 2026
ISSN 3025-0919 (media online)
Hal 2161-2172

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://peraturan.bpk.go.id/Details/47041/uu-no-8-tahun-1981

Republik Indonesia. (2009). *Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 10 Tahun 2009 tentang Tata cara dan persyaratan permintaan pemeriksaan teknis kriminalistik tempat kejadian perkara dan laboratoris kriminalistik barang bukti kepada Laboratorium Forensik Kepolisian Negara Republik Indonesia* (Berita Negara Republik Indonesia Tahun 2009 Nomor 311). https://peraturan.go.id/files/bn311-2009.pdf

Republik Indonesia. (2010). *Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 10 Tahun 2010 tentang Tata cara pengelolaan barang bukti di lingkungan Kepolisian Negara Republik Indonesia* (Berita Negara Republik Indonesia Tahun 2010 Nomor 204). https://peraturan.go.id/files/bn204-2010.pdf

Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik* (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1). https://jdih.komdigi.go.id/index.php/produk_hukum/view/id/884/t/undangundang+nomor+1+tahun+2024

Republik Indonesia. (2025). *Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana* (Lembaran Negara Republik Indonesia Tahun 2025 Nomor 188). https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025

Samsul, I., Sirait, R. A., Aida, A. N., & Iskandar, L. (2025, Juni). *Analisis pagu indikatif Badan Siber dan Sandi Negara*. Badan Keahlian Dewan Perwakilan Rakyat Republik Indonesia. https://berkas.dpr.go.id/pa3kn/analisis-apbn/public-file/analisis-apbn-public-106.pdf

Sembiring, E. S. B., & Lasube, Y. M. (2026). Kekuatan pembuktian alat bukti elektronik dalam perkara pidana di Indonesia. *Lex Technologia: Jurnal Hukum dan Masyarakat Digital, 1*(1), 27–37. https://ejournalfish.unima.ac.id/index.php/lextechnologia/id/article/download/59/44/214

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Universitas Pamulang. (t.t.). *Pertemuan V: IT forensik* [Etika Profesi].