PESHUM : Jurnal Pendidikan, Sosial dan Humaniora
Vol.5, No.5, Agustus 2026

Keabsahan Tindakan *Forensic Imaging* dalam Penyitaan Bukti Digital: Optimalisasi Penegakan Hukum Siber Terhadap Operasional Korporasi

Andry Effendy[1], Ezra Nur Farhan[2], Tri Yulianto Satyadi[3], Subadria[4], Yustinus Stein Siahaan[5]
Program Pascasarjana Magister Ilmu Hukum Universitas Borobudur, Indonesia
E-mail: andry_effendy@borobudur.ac.id[1], farhannurezra@gmail.com[2], triyuliantosatyadi@gmail.com[3], Subadriasubadria@gmail.com[4], yustinusstein85@gmail.com[5]

Article History:
Received: 06 Juli 2026
Revised: 17 Juli 2026
Accepted: 19 Juli 2026

Keywords: *Cyber Law; Chain of Custody; Digital Evidence; Forensic Imaging; Seizure.*

Abstract: *Digital transformation creates challenges in proving cybercrimes, as electronic evidence is volatile and easily modified. Forensic imaging ensures evidence integrity, yet its corporate application often conflicts with operational continuity and trade secrets. This research analyzes the legal validity of forensic imaging in digital seizures to balance coercive measures with corporate data protection. The method is normative juridical, utilizing statutory, conceptual, and case approaches. Results show forensic imaging is legally valid and more proportional than physical seizures, using a cloning (mirroring) method without permanently confiscating devices. Its absolute validity depends on the chain of custody and hash verification. Authority balance is achieved through proportionality and due process of law, manifested in legal (court permission, seizure reports, legal assistance) and technical protections (on-site imaging, write-blockers, data filtering). Compliance with forensic procedures is crucial to prevent harming well-intentioned parties.*

Kata Kunci: Bukti Elektronik; *Chain of Custody*; *Forensic Imaging*; Hukum Siber; Penyitaan.

Abstrak: Tantangan pembuktian pidana siber muncul mengingat bukti elektronik bersifat *volatile* dan mudah dimodifikasi. Prosedur *forensic imaging* hadir menjamin integritas bukti, namun penerapannya pada korporasi kerap berbenturan dengan kelangsungan operasional dan rahasia dagang. Penelitian ini menganalisis keabsahan yuridis *forensic imaging* dalam penyitaan digital guna menyeimbangkan upaya paksa penyidik dengan perlindungan data korporasi. Metode yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Hasilnya menunjukkan *forensic imaging* sah secara hukum dan lebih proporsional dibanding penyitaan fisik karena memakai metode *cloning* (*mirroring*)

tanpa merampas perangkat permanen. Keabsahannya mutlak bergantung pada rantai penguasaan bukti (*chain of custody*) dan verifikasi nilai *hash*. Keseimbangan kewenangan dicapai melalui prinsip *proportionality* dan *due process of law* yang terwujud dalam perlindungan hukum (izin pengadilan, BAP, pendampingan) dan teknis (*on-site imaging*, *write-blocker*, *data filtering*). Kepatuhan prosedur forensik krusial agar tidak merugikan subjek beritikad baik.

PENDAHULUAN

Perkembangan teknologi informasi dan digitalisasi dalam berbagai sektor kehidupan telah menciptakan ekosistem data yang kompleks. Seiring dengan manfaat yang ditawarkan, transformasi digital juga membuka peluang bagi terjadinya tindak pidana yang memanfaatkan medium elektronik. Kejahatan siber, penipuan online, penggelapan data, hingga pelanggaran keamanan informasi menjadi fenomena hukum yang semakin sering dihadapi oleh aparat penegakan hukum di Indonesia. Dalam konteks ini, bukti elektronik menjadi komponen krusial dalam proses pembuktian pidana untuk mengungkap dan menuntut tindak pidana tersebut.

Sifat unik bukti elektronik menciptakan tantangan tersendiri dalam sistem pembuktian Indonesia. Bukti elektronik memiliki karakteristik berbeda dibandingkan bukti konvensional karena bentuknya berupa informasi digital yang dapat direplikasi, dimodifikasi, serta ditransmisikan melalui sistem elektronik.[1] Karakter utama bukti digital terletak pada sifatnya yang *intangible*, mudah direplikasi, mudah dipindahkan, dan secara teknis juga mudah diubah tanpa meninggalkan tanda yang kasatmata bagi pengguna biasa.[2] Kondisi ini menciptakan problematika yuridis: bagaimana aparat penegak hukum dapat mengamankan, mengekstraksi, dan menggunakan bukti elektronik dalam proses persidangan sambil tetap menjamin integritas, autentisitas, dan keasliannya.

Mengatasi permasalahan tersebut, standar digital *forensics* telah berkembang sebagai metode ilmiah untuk mengidentifikasi, mengamankan, mengekstraksi, memelihara, menganalisis, dan mempresentasikan data digital secara dapat dipertanggungjawabkan.[3] Salah satu prosedur krusial dalam digital *forensics* adalah *forensic imaging*, merupakan suatu tindakan untuk mendapatkan data yang identik dari data asal (*cloning*) melalui serangkaian tahapan sistematis. Menurut standar prosedural di lingkungan Polri yang ditetapkan melalui Peraturan Kabareskrim Polri Nomor 1 Tahun 2014, *forensic imaging* harus didahului dengan *write protect* untuk mengunci data asal dari perubahan, dilanjutkan dengan *cloning* untuk mendapatkan *image file*, dan diakhiri dengan *verifying* untuk memastikan keidentikan data *cloning* dengan data asal.[4]

Kehadiran prosedur *forensic imaging* ini seharusnya memberikan solusi terhadap tantangan pembuktian bukti elektronik. Namun, dalam praktik penyidikan di lapangan, implementasi

[1] Sunnah dan Abdul Malik Mufty, "Paradigma Baru Pembuktian Pidana Berbasis Teknologi dalam KUHAP Baru dan Implikasinya terhadap Standar Fair Trial di Indonesia", *Khatulistiwa: Jurnal Pendidikan dan Sosial Humaniora*, Volume 6 Nomor 2, Juni 2026, hlm. 703.

[2] *Ibid.*, hlm. 706.

[3] *Ibid.,* hlm. 707.

[4] H. Santhos Wachjoe P., "Penggunaan Informasi Elektronik dan Dokumen Elektronik Sebagai Alat Bukti Persidangan", *Jurnal Hukum dan Peradilan*, Volume 5 Nomor 1, Maret 2016, hlm. 15.

standar *forensic imaging* masih mengalami hambatan signifikan. Jejak digital memiliki karakter *volatile*, mudah berubah, dan berisiko hilang apabila tidak segera diamankan dengan prosedur yang tepat. Praktik penyidikan di berbagai daerah, termasuk Riau, tidak seluruh penyidik memiliki kompetensi forensik digital yang memadai untuk melakukan *imaging*, analisis *log*, maupun verifikasi *hash value*.[5] Lebih lanjut, efektivitas jejak digital juga terkait erat dengan konsep *chain of custody* atau rantai penguasaan bukti, dimana setiap bukti yang dikumpulkan harus melewati prosedur yang menjamin keaslian dan keutuhan datanya, dan penyidik wajib mendokumentasikan setiap langkah pengambilan, penyimpanan, dan analisis data digital agar bukti tersebut tidak diragukan di persidangan.[6]

Ketegangan antara kebutuhan menjalankan upaya paksa ekstraksi data digital dan perlindungan terhadap integritas bukti ini semakin kompleks ketika prosedur penyitaan diterapkan terhadap korporasi atau badan usaha. Dalam konteks penyidikan *cybercrime* yang menyangkut korporasi, aparat penegak hukum berhadapan dengan dilema: di satu sisi, mereka memiliki kewenangan upaya paksa untuk menyita perangkat atau mengekstraksi data sebagai bukti, di sisi lain, korporasi memiliki hak untuk melindungi keberlangsungan operasional bisnisnya, rahasia dagang, dan aset digital yang tidak terkait dengan tindak pidana yang diselidiki. Penyitaan yang dilakukan tanpa mempertimbangkan aspek proporsionalitas dapat merugikan kepentingan korporasi yang tidak bersalah, mengganggu kontinuitas layanan, dan mengekspos informasi sensitif di luar lingkup tindak pidana yang dikaji.

Mengilustrasikan betapa krusialnya prosedur digital forensik dalam pembuktian pidana, Putusan Nomor 488/Pid.B/2024/PN Sda memberikan preseden yang penting. Dalam perkara tindak pidana penggelapan tersebut, majelis hakim menolak barang bukti elektronik berupa tangkapan layar (*screenshot*) percakapan yang diajukan pihak terdakwa melalui kuasa hukumnya dalam nota pembelaan (pledoi). Penolakan ini bukan karena prosedur *forensic imaging* dilakukan dengan cacat, melainkan karena bukti tersebut sama sekali tidak melalui proses verifikasi digital forensik, sehingga keasliannya tidak dapat dijamin apakah bukti itu telah diubah, direkayasa, atau diedit sebelum diajukan ke hadapan hakim.[7] Putusan ini menegaskan bahwa verifikasi melalui digital forensik merupakan syarat mutlak agar bukti elektronik dapat diterima di persidangan, sekaligus menjadi pengingat bahwa *forensic imaging* (sebagai metode krusial dalam pembuktian digital) tidak dapat digantikan oleh penyerahan bukti elektronik secara mentah tanpa proses autentikasi yang terstandar.

Penelitian ini dimaksudkan untuk menganalisis keabsahan yuridis penerapan standar *forensic imaging* sebagai instrumen penyitaan bukti elektronik dalam sistem hukum acara pidana Indonesia berdasarkan kompleksitas tersebut. Fokus penelitian adalah pada legalitas prosedur, integritas barang bukti, dan mekanisme yang dapat mengoptimalkan penegakan hukum *cybercrime* tanpa mengorbankan kelangsungan operasional atau melanggar hak-hak korporasi. Analisis akan mencakup sinkronisasi antara norma-norma hukum acara pidana, regulasi bukti elektronik, dan prinsip-prinsip *proportionality* dalam upaya paksa, serta menguji apakah *forensic imaging* dapat dipandang sebagai bentuk penyitaan yang lebih proporsional dibandingkan penyitaan fisik perangkat secara keseluruhan.

---

[5] Muhammad Safei, Sandra Dewi, Olivia Anggie Johar, "Implementasi Pada Alat Bukti Jejak Digital Dalam Penegakan Hukum Tindak Pidana Penipuan Online", *Collegium Studiosum Journal*, Vol. 8 No. 2, Desember 2025, hlm. 513.

[6] Muhammad Safei dkk., *op. cit.*, hlm. 504.

[7] Stefania Kandida Sena Tiba, "Implikasi Penolakan Bukti Elektronik Tanpa Verifikasi Digital Forensik: Studi Putusan dan Analisis Yuridis", *Media Hukum Indonesia (MHI)*, Vol. 4, No. 1, Desember 2025, hlm. 866.

Rumusan Masalah

1. Bagaimana keabsahan yuridis penerapan standar *forensic imaging* (kloning *bit-per-bit*) sebagai instrumen penyitaan bukti elektronik yang diakui dalam sistem hukum acara pidana Indonesia guna meminimalisasi kerusakan data dan menjamin integritas barang bukti di persidangan?
2. Bagaimana aparat penegak hukum dapat menyeimbangkan kewenangan upaya paksa ekstraksi data digital dengan upaya pelindungan terhadap kelangsungan operasional serta rahasia dagang korporasi yang dijamin oleh Undang-Undang Perseroan Terbatas dan regulasi lainnya?

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif yang menitikberatkan pada studi kepustakaan dengan memanfaatkan data sekunder sebagai sumber analisis utama.[8] Membedah permasalahan yang dikaji, penelitian ini mengaplikasikan beberapa pendekatan secara komprehensif, yaitu pendekatan yuridis normatif, pendekatan konseptual, pendekatan perundang-undangan (*statute approach*), serta pendekatan kasus (*case approach*). Bahan hukum yang dikumpulkan meliputi bahan hukum primer seperti KUHAP, UU ITE, UUPT, UU Rahasia Dagang, Peraturan Kabareskrim Polri Nomor 1 Tahun 2014, dan Putusan Nomor 488/Pid.B/2024/PN Sda, yang kemudian diperkuat oleh bahan hukum sekunder berupa jurnal maupun literatur akademik terkait. Seluruh data tersebut selanjutnya diolah dan dianalisis menggunakan metode yuridis kualitatif, yakni melalui proses pembacaan, interpretasi, perbandingan doktrin, dan sintesis terhadap norma hukum serta praktik peradilan.[9] Sebagai landasan argumentasi akhir, keseluruhan analisis ini dibingkai oleh kerangka teoritis yang berpijak pada teori pembuktian hukum pidana, teori integritas barang bukti, dan teori *proportionality* dalam upaya paksa penyitaan data digital.

HASIL DAN PEMBAHASAN

Sistem pembuktian pidana Indonesia mengakui berbagai alat bukti sebagaimana diatur dalam Pasal 184 KUHAP, yang mencakup keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Era digitalisasi menghadirkan bukti elektronik yang telah menggeser paradigma pembuktian tradisional, mendorong sistem hukum untuk mengakui dan mengatur bukti yang bersifat *immaterial* dan *volatile*. Bukti elektronik memiliki karakteristik berbeda dibandingkan bukti konvensional karena berbentuk informasi digital yang dapat direplikasi, dimodifikasi, serta ditransmisikan melalui sistem elektronik.[10] Karakteristik ini menciptakan problematika unik: jika bukti konvensional bersifat statis dan dapat diperiksa secara langsung (seperti dokumen fisik atau barang), bukti elektronik sebaliknya bersifat dinamis dan memerlukan mekanisme khusus untuk memastikan keasliannya.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) telah mengakui keabsahan informasi elektronik dan dokumen elektronik sebagai alat bukti. Pasal 5 UU ITE menegaskan bahwa "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah." Pengakuan yuridis ini tidak otomatis menjadikan setiap informasi elektronik sebagai alat bukti yang dapat diterima di

[8] Yulia Audina Sukmawan & Dwi Damayanti, "Metode Penelitian Hukum Normatif dan Empiris sebagai Strategi Penguatan Perspektif Kajian Ilmu Hukum", *Notary Law Journal*, Volume 4 Issue 1, 2025, hlm. 118.

[9] *Ibid.*, hlm. 117.

[10] Sunnah dan Abdul Malik Mufty, *op. cit.*, hlm. 703.

persidangan. Proses validasi, verifikasi, dan pengamanan yang ketat masih diperlukan untuk memastikan integritas dan autentisitas bukti tersebut. Digital *forensics* muncul sebagai fondasi metodologis yang memungkinkan transformasi data digital yang *volatile* dan mudah dimodifikasi menjadi bukti yang dapat dipertanggungjawabkan secara yuridis. Digital *forensics* menyediakan metode ilmiah untuk mengidentifikasi, mengamankan, mengekstraksi, memelihara, menganalisis, dan mempresentasikan data digital secara dapat dipertanggungjawabkan.[11]

Penyitaan sebagaimana diatur dalam Pasal 38-39 KUHAP, adalah tindakan upaya paksa yang dilakukan oleh penyidik untuk menguasai barang bukti yang diduga menjadi alat atau hasil dari tindak pidana. Konteks bukti elektronik menegaskan bahwa penyitaan tidak dapat dilakukan dengan cara konvensional. Tindakan tidak dapat dilakukan dengan memindahkan atau menutup akses terhadap perangkat selamanya, karena hal tersebut akan mengganggu keberlangsungan operasional, terutama jika perangkat tersebut merupakan sistem kritis yang melayani banyak pengguna (seperti server perusahaan).

Forensic imaging yang merupakan prosedur pembuatan tiruan digital (*cloning*) dari data asal menghadirkan alternatif yang lebih proporsional. Melalui *forensic imaging*, penyidik dapat mengamankan dan menganalisis data tanpa perlu menutup atau menonaktifkan perangkat secara permanen. Prosedur ini terdiri dari tiga tahap dasar yang harus dilakukan dengan ketat. Pertama, *write protect*, yang dapat diartikan sebagai mengunci data asal dari informasi elektronik dan/atau dokumen elektronik sebelum melakukan digital forensik. *Write protect* dilakukan agar data asal yang akan dilakukan digital forensik tidak mengalami perubahan, baik itu penambahan, pengurangan maupun penghapusan data. Kedua, *forensic imaging*, yang dapat diartikan sebagai tindakan untuk mendapatkan data yang serupa dari data asal atau dikenal dengan istilah *cloning*. *Forensic imaging* ini dilakukan terhadap data asal yang sudah di *write protect*, dari *forensic imaging* ini akan didapatkan data yang identik dengan data asal yang disebut *image file*. Ketiga, *verifying*, yang dapat diartikan sebagai tahapan untuk menilai hasil dari *forensic imaging*, yaitu data yang di-*clone* harus identik dengan data asal.[12]

Kehadiran Peraturan Kabareskrim Polri Nomor 1 Tahun 2014 Nomor 1 Tahun 2014 tentang *Standar Operating Procedure* (SOP) dalam melakukan *forensic imaging* menunjukkan pengakuan institusional terhadap pentingnya standarisasi prosedur ini. SOP tersebut menetapkan panduan teknis yang harus diikuti oleh penyidik dan forensiker dalam melakukan *forensic imaging* guna memastikan keandalan dan dapat dipertanggungjawabannya hasil *imaging* di persidangan. Perspektif hukum acara pidana menurut analisis penulis mengonseptualisasikan *forensic imaging* sebagai bentuk operasionalisasi penyitaan data digital yang lebih proporsional dibandingkan penyitaan fisik perangkat secara keseluruhan. Hal ini sejalan dengan pandangan bahwa sifat penyitaan bukti elektronik pada dasarnya berbeda dengan penyitaan perangkat biasa, karena penyitaan bukti elektronik bersifat *mirroring* yang menyalin data dari perangkat sehingga pada banyak kasus pemilik data masih dapat mengakses datanya.[13] Justifikasi yuridis *forensic imaging* dalam konteks penyitaan dengan demikian dapat dibangun dari tiga pijakan: (a) pencapaian tujuan penyitaan tanpa mengambilalih fisik perangkat secara permanen, (b) pengurangan dampak negatif terhadap keberlangsungan operasional pihak yang tidak terlibat tindak pidana, (c) penciptaan *audit trail* yang dapat diverifikasi secara independen di persidangan.

Prinsip *chain of custody* (rantai penguasaan bukti) merupakan fondasi krusial dalam

---

[11] *Ibid.*, hlm. 707.

[12] H. Santhos Wachjoe P., *op. cit.*, hlm. 15.

[13] Viona Violeta Marselina Pattipeilohy, Diva A.E. Rombot, dan Syamsia Midu, "Tinjauan Hukum Terhadap Penyitaan Barang Bukti Elektronik Dalam Tindak Pidana Di Bidang Teknologi Informasi Dan Komunikasi", hlm. 10.

pembuktian pidana modern. Konsep ini mensyaratkan bahwa setiap barang bukti yang dikumpulkan harus melewati prosedur yang menjamin keaslian dan keutuhan datanya. Konteks bukti elektronik menunjukkan bahwa efektivitas jejak digital juga terkait erat dengan konsep *chain of custody* atau rantai penguasaan bukti. Hukum pembuktian digital menuntut agar setiap bukti yang dikumpulkan harus melewati prosedur yang menjamin keaslian dan keutuhan datanya. Penyidik wajib mendokumentasikan setiap langkah pengambilan, penyimpanan, dan analisis data digital agar bukti tersebut tidak diragukan di persidangan.

Implementasi *chain of custody* dalam *forensic imaging* memerlukan dokumentasi mendetail pada setiap tahap prosedur: (a) tahap *write protect* harus didokumentasikan siapa yang melakukan, kapan, di mana, dan dengan alat apa, (b) tahap *forensic imaging* harus mencatat identitas *image file* yang dihasilkan, beserta *hash value* yang membuktikan keidentikan antara data asal dan *image file*, (c) tahap *verifying* harus memastikan bahwa *hash value* data asal dan *image file* identik. Praktik penyidikan pasca proses *imaging* selesai mewajibkan penghitungan ulang *hash value* seperti MD5, SHA-1, atau SHA-256 untuk memastikan hasil salinan identik secara *bit-per-bit* dengan barang bukti asli. Seluruh kendala teknis, log proses, dan metode pemulihan juga wajib dicatat dalam berita acara dan dokumentasi *audit trail*.[14] Dokumentasi yang ketat ini bertujuan untuk menciptakan rekam jejak yang dapat diperiksa oleh hakim, pihak lawan, dan ahli di persidangan. Integritas dan autentisitas bukti elektronik dengan demikian dapat diverifikasi secara independen, bukan hanya berdasarkan afirmasi penyidik.

Ketiadaan digital forensik dengan dokumentasi *chain of custody* yang sempurna mengakibatkan suatu dokumen elektronik tidak dapat digunakan sebagai alat bukti karena tidak dapat dijamin kesahihan dari dokumen elektronik tersebut.[15] Kondisi sebaliknya berlaku apabila informasi elektronik dan/atau dokumen elektronik yang diajukan di persidangan merupakan data *image file* yang identik dengan data asal (terbukti melalui verifikasi *hash value* dan dokumentasi *chain of custody* yang lengkap), maka informasi elektronik dan/atau dokumen elektronik tersebut dapat digunakan sebagai alat bukti yang sah untuk membuktikan suatu perkara, baik pidana maupun perdata.[16]

Praktik beserta relevansi prosedur verifikasi digital forensik telah diuji secara nyata di hadapan pengadilan. Putusan Nomor 488/Pid.B/2024/PN Sda memberikan ilustrasi penting tentang bagaimana pengadilan menilai keabsahan bukti elektronik. Perkara tindak pidana penggelapan tersebut memperlihatkan majelis hakim menolak barang bukti elektronik berupa tangkapan layar (*screenshot*) percakapan yang diajukan oleh pihak terdakwa melalui kuasa hukumnya dalam nota pembelaan (pledoi). Penolakan terjadi bukan karena prosedur *forensic imaging* dilakukan secara keliru, melainkan karena bukti tersebut sama sekali tidak melalui proses digital forensik, sehingga pengadilan tidak dapat menjamin keasliannya apakah telah diubah, direkayasa, atau diedit sebelum diajukan ke hadapan hakim.[17] Substansi bukti yang dianggap penting dan berpotensi menunjukkan bahwa terdakwa tidak bersalah, tetap diabaikan majelis hakim yang menyatakan bahwa *screenshot* tersebut tidak dapat dipertimbangkan sebagai alat bukti yang sah.[18]

---

[14] Sangkot Setiawan Lubis, S.H. (IPDA), Wawancara via WhatsApp, 10 Juni 2026, pukul 12.00 WIB.

[15] H. Santhos Wachjoe P., *op. cit.*, hlm. 13.

[16] *Ibid.*, hlm. 16.

[17] Stefania Kandida Sena Tiba, *op. cit.*, hlm. 867.

[18] *Ibid.*

Putusan ini menegaskan prinsip yang telah diakui dalam standar pembuktian pidana: verifikasi digital forensik (termasuk di dalamnya prosedur *forensic imaging*) merupakan syarat mutlak (*conditio sine qua non*) agar bukti elektronik dapat diterima di persidangan. Hal ini selaras dengan doktrin yang dinyatakan oleh H. Santhos Wachjoe P. bahwa ketika *image file* yang diajukan tidak identik dengan data asal, hakim harus mengesampingkan alat bukti tersebut.[19] Putusan 488/2024 bukan hanya menggambarkan konsekuensi ketiadaan *forensic imaging*, tetapi juga secara implisit menegaskan posisi sentral *forensic imaging* sebagai metode autentikasi yang tidak tergantikan dalam sistem pembuktian pidana Indonesia.

Kerangka normatif dan prosedural untuk *forensic imaging* memang sudah terbentuk, namun implementasinya di lapangan masih menghadapi tantangan signifikan. Jejak digital memiliki karakter *volatile*, mudah berubah, dan berisiko hilang apabila tidak segera diamankan dengan prosedur yang tepat. Praktik penyidikan di daerah, termasuk Riau, tidak seluruh penyidik memiliki kompetensi forensik digital yang memadai untuk melakukan *imaging*, analisis *log*, maupun verifikasi *hash value*. Keterbatasan kompetensi ini menciptakan risiko nyata bahwa *forensic imaging* tidak dilakukan dengan benar, sehingga menghasilkan bukti yang tidak dapat diterima di persidangan, seperti ditunjukkan oleh Putusan 488/2024. Mengoptimalkan keabsahan *forensic imaging* dalam praktik penyidikan diperlukan hal-hal berikut: (a) peningkatan kapasitas dan kompetensi penyidik dan forensiker melalui pelatihan berkelanjutan, (b) penyediaan sarana dan prasarana teknis yang memadai di setiap unit penyidikan, (c) pengembangan protokol dan *checklist* yang memudahkan penyidik untuk memastikan setiap tahap prosedur dilakukan dengan benar, (d) kolaborasi yang lebih erat antara penyidik, forensiker, dan penuntut umum dalam memastikan bukti dikumpulkan dan dikelola sesuai standar.

Hukum acara pidana Indonesia mengakui berbagai bentuk upaya paksa yang dapat dilakukan oleh penyidik dalam rangka mengumpulkan bukti. Penyitaan, sebagaimana diatur dalam Pasal 1 angka 16 jo. Pasal 38 KUHAP, adalah tindakan upaya paksa yang dilakukan oleh penyidik untuk menguasai barang bukti yang diduga menjadi alat atau hasil dari tindak pidana. Pasal 1 angka 16 KUHAP mendefinisikan penyitaan, sedangkan Pasal 38 KUHAP mengatur syarat izin dan pelaksanaannya. Konteks elektronik mempertegas ketentuan ini melalui Pasal 43 UU ITE dan praktik digital *forensics* guna menjaga *chain of custody*.[20] Penyitaan dalam konteks bukti elektronik tidak dapat dilakukan dengan memindahkan atau menutup akses terhadap perangkat selamanya, karena hal tersebut akan mengganggu keberlangsungan operasional, terutama jika perangkat tersebut merupakan sistem yang melayani banyak pengguna.

Penyitaan perangkat fisik secara tradisional mengakibatkan hilangnya akses pemilik perangkat terhadap data dan sistem yang digunakan untuk operasional bisnis. Perangkat yang disita berupa server kritis yang melayani layanan penting, seperti sistem pembayaran, *database* pelanggan, atau sistem manajemen, akan mengakibatkan gangguan operasional perusahaan secara signifikan. Hal ini menciptakan dampak yang tidak proporsional terhadap korporasi yang mungkin hanya memiliki hubungan tangensial dengan tindak pidana yang diselidiki. *Forensic imaging* dalam konteks ini menawarkan alternatif yang lebih proporsional. Melakukan *forensic imaging* memungkinkan penyidik mengamankan data tanpa mengganggu keberlangsungan operasional perangkat, namun perlu diperhatikan bahwa tindakan tersebut bukan tanpa batas.

Proses *imaging* itu sendiri memerlukan akses fisik ke perangkat, yang berarti penyidik harus masuk ke lokasi penyimpanan data (*server room*, kantor, dll). Selama proses *imaging* berlangsung, perangkat tersebut harus di-*write protect*, yang berarti aksesnya dibatasi atau

[19] H. Santhos Wachjoe P., *op. cit.*, hlm. 15.

[20] *Ibid.*, hlm. 510.

dimonitor. Durasi proses ini bisa memakan waktu berjam-jam atau bahkan berhari-hari, tergantung pada volume data. Upaya paksa ini masih perlu diimbangi dengan perlindungan terhadap hak-hak korporasi yang tidak bersalah meskipun *forensic imaging* lebih proporsional daripada penyitaan fisik keseluruhan.

Korporasi, sebagai badan hukum, memiliki hak untuk melindungi rahasia dagang dan aset data yang dimilikinya. Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang mendefinisikan rahasia dagang sebagai informasi yang tidak diketahui oleh umum di bidang teknologi dan/atau bisnis, memiliki nilai ekonomis karena tidak diketahuinya oleh umum, dan menjadi objek langkah-langkah yang wajar untuk menjaganya tetap rahasia. Perlindungan ini tidak hanya diberikan terhadap akses ilegal dari pihak lain, tetapi juga terhadap pengungkapan yang tidak perlu atau tidak sengaja. Konteks penyidikan pada saat aparat penegak hukum melakukan *forensic imaging* pada perangkat korporasi, memunculkan risiko bahwa data-data sensitif yang tidak terkait dengan tindak pidana yang diselidiki (seperti formula produk, strategi bisnis, data pelanggan, atau informasi keuangan) dapat terekspos. Paparan awal yang terjadi selama proses *imaging* atau selama penyimpanan *image file* dapat merugikan posisi kompetitif perusahaan, kendatipun data ini akhirnya tidak digunakan sebagai bukti di persidangan.

Hukum korporasi mengkontekstualisasikan bahwa suatu aset data dan informasi rahasia perusahaan tidak semata-mata dilindungi oleh UU Rahasia Dagang. Ketentuan-ketentuan dalam Undang-Undang Perseroan Terbatas (UUPT) yang mengatur kewajiban direksi untuk mengurus dan mengelola perseroan dengan baik secara implisit juga mencakup tanggung jawab untuk melindungi aset data dari pengungkapan yang tidak perlu, termasuk dalam konteks penyidikan pidana yang tidak proporsional. Bukti digital dalam penyelidikan forensik dapat mencakup data sensitif korporasi seperti rencana bisnis, dokumen keuangan, dan informasi lainnya, di mana akses yang tidak terbatas terhadap data tersebut merupakan ancaman nyata terhadap privasi pemilik data.[21] Keseimbangan antara kewenangan upaya paksa penyidik dan perlindungan hak korporasi ini harus dijaga melalui penerapan prinsip *proportionality* dalam setiap tindakan penyitaan.

Prinsip *proportionality* dalam hukum acara pidana mensyaratkan bahwa upaya paksa yang dilakukan harus sesuai dengan kebutuhan penyidikan dan tidak berlebihan. Proporsionalitas dalam konteks penyitaan data digital dapat diukur dari beberapa dimensi, yaitu antara tujuan penyidikan dengan dampak operasional korporasi, volume data yang diakses dengan yang relevan, serta hal teknis durasi maupun penyimpanan *image file*. Penyidik harus mempertimbangkan apakah data yang akan disita benar-benar diperlukan untuk membuktikan tindak pidana yang sedang diselidiki, dan jika data tersebut dapat diperoleh melalui mekanisme lain yang kurang invasif, maka ﷺternatif tersebut harus dipilih terlebih dahulu.

Forensic imaging menghasilkan *image file* yang berisi seluruh isi perangkat atau media penyimpanan yang di-*image*. Semua data di perangkat tersebut (termasuk data yang sama sekali tidak terkait dengan penyidikan) otomatis akan tercakup dalam *image file*. Penjagaan *proportionality* menuntut penyidik untuk membatasi *imaging* hanya pada partisi, folder, atau media penyimpanan yang memungkinkan kemungkinan mengandung data yang relevan dengan penyidikan. Melakukan *forensic imaging* terhadap seluruh sistem operasional perangkat yang berisi data personal karyawan, dokumen keuangan perusahaan, atau informasi bisnis sensitif lainnya akan dianggap tidak proporsional jika hal ini tidak diperlukan.

Proses *forensic imaging* dapat memakan waktu berjam-jam atau berhari-hari sehingga

[21] Feby Thealma dan Yova Ruldeviyani, "Digital Forensic Ethical Data Handling in Indonesia", *The Indonesian Journal of Computer Science*, Vol. 14, Issue 1, February 2025, hlm. 287.

perangkat tidak dapat digunakan dengan normal oleh pemiliknya. Penyidik harus meminimalkan durasi proses *imaging* dan memastikan bahwa proses ini dilakukan dengan efisien. Proses *imaging* harus dilakukan di luar jam operasional perusahaan jika memungkinkan, sehingga dampaknya terhadap bisnis dapat diminimalkan. Penyelesaian *forensic imaging* mewajibkan *image file* yang dihasilkan harus disimpan dengan aman dan akses terhadapnya harus dibatasi hanya kepada personel yang benar-benar memerlukan (penyidik, penuntut umum, hakim, ahli, dan pihak lawan dalam perkara). *Image file* tidak boleh diperbanyak atau didistribusikan secara luas, karena hal ini akan meningkatkan risiko pengungkapan data sensitif. Temuan *image file* yang mengandung data sensitif korporasi yang ternyata tidak relevan dengan penyidikan, mengharuskan penyidik untuk menghapus atau menjauhkan data tersebut dari akses lebih lanjut setelah penyidikan selesai.

Analisis penulis menemukan adanya dua lapisan mekanisme perlindungan yang dapat dan seharusnya diterapkan untuk menjamin bahwa upaya paksa ekstraksi data digital tidak merugikan korporasi secara tidak proporsional, yaitu perlindungan hukum dan perlindungan teknis forensik. Syarat izin pengadilan dan perlindungan kepentingan pelayanan umum menjadi lapisan pertama secara regulasi. Berdasarkan Pasal 43 UU ITE, penyitaan terhadap sistem elektronik yang diduga terkait tindak pidana harus dilakukan atas izin Ketua Pengadilan Negeri setempat, dengan tetap menjaga terpeliharanya kepentingan pelayanan umum.[22] Apabila sistem elektronik korporasi yang menjadi objek penyitaan merupakan infrastruktur layanan (seperti server perbankan atau sistem pembayaran) penyidik tidak dapat memadamkannya secara sepihak. Tindak pidana perpajakan yang melibatkan server bank, apabila mematikan server tersebut akan mengganggu pelayanan publik, merupakan tindakan yang tidak boleh dilakukan.[23]

Hak atas Berita Acara Penyitaan (BAP) yang terperinci merupakan aspek berikutnya. Setiap tindakan eksekusi penyitaan wajib dituangkan dalam BAP, dan pihak korporasi berhak mendapatkan salinannya yang merinci secara persis data, *drive*, atau server apa saja yang disita atau disalin. Mekanisme ini merupakan derivasi dari prinsip transparansi dan akuntabilitas dalam *due process of law* yang dijamin konstitusi.[24] Hak pendampingan penasihat hukum juga diberikan selama proses *forensic imaging* berlangsung. Perwakilan perusahaan dan penasihat hukumnya berhak hadir untuk mengawasi bahwa tindakan penyidik tidak melampaui ruang lingkup surat perintah, misalnya memastikan penyidik tidak mengakses data pribadi karyawan yang tidak relevan. Penyidik memang wajib menjaga kerahasiaan informasi yang tidak relevan dengan tindak pidana yang diselidiki.[25]

Pelaksanaan *on-site imaging* (kloning di tempat) merupakan perlindungan teknis yang pertama. Korporasi yang bersifat kooperatif dan memiliki sistem elektronik sebagai infrastruktur vital, dapat memohon agar penyidik melakukan *imaging* langsung di fasilitas data center perusahaan tanpa mengangkut perangkat keras (*hardware*) aslinya. KPK telah memiliki SOP Forensik Digital yang mengatur pengambilan data dengan metode *forensic image* menggunakan prinsip *read-only* untuk menjaga integritas data, sekaligus mewajibkan pemisahan yang jelas

---

[22] Viona Violeta Marselina Pattipeilohy dkk., *op. cit.*, hlm. 1.

[23] Deya Hazirattul Khudsiyah, Davit Rahmadan, dan Erdianto, "Penegakan Hukum Terhadap Modus Baru Kejahatan Cyber Berupa Rekayasa Informasi Teknologi Pembobolan Rekening Nasabah Melalui Internet Banking", *Jurnal Ilmiah Wahana Pendidikan*, Vol. 11, No. 8.D, Agustus 2025, hlm. 241.

[24] Sunnah dan Abdul Malik Mufty, *op. cit.*, hlm. 714.

[25] Insan Pribadi, "Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana", *LEX Renaissance*, No. 1, Vol. 3, Januari 2018, hlm. 123.

antara data asli (*original data*) dan salinan kerja (*working copy*).[26] Penggunaan *write-blocker* menjadi standar krusial selanjutnya. Penyidik forensik menggunakan *write-blocker* (perangkat keras atau lunak yang memblokir perintah penulisan sehingga data di dalam perangkat asli tidak mengalami perubahan sedikit pun selama proses akuisisi berlangsung, sejalan dengan prinsip *forensically sound*.[27]

Penyaringan atau *filtering* data yang relevan turut diterapkan. Teknik *keyword filtering*, *date filtering*, *file extension filtering*, serta *hash filtering* dan *profiling* pengguna digunakan untuk menyaring data yang benar-benar relevan dengan kasus tanpa menyentuh rahasia dagang atau data keuangan yang tidak terkait.[28] Mekanisme ini secara teknis memungkinkan penyitaan yang lebih tepat sasaran dan tidak melangkah melampaui ruang lingkup penyelidikan. Verifikasi *hash* bertindak sebagai pelindung dari manipulasi pasca-penyitaan. Setelah *imaging* selesai, nilai *hash* (MD5, SHA-1, atau SHA-256) dari salinan harus identik dengan perangkat asli. Mekanisme ini tidak hanya melindungi integritas bukti untuk kepentingan penegakan hukum, tetapi juga melindungi korporasi dari tuduhan bahwa data telah disusupkan atau dimanipulasi oleh penyidik pasca-penyitaan.[29]

Keseimbangan antara penegakan hukum dan perlindungan hak korporasi harus dilihat dalam kerangka prinsip *due process of law* yang menjadi dasar perlindungan hak asasi manusia dalam sistem peradilan pidana.[30] Prinsip ini menuntut bahwa setiap pembatasan terhadap hak individu maupun korporasi harus dilakukan melalui prosedur yang sah, proporsional, dan dapat dipertanggungjawabkan secara hukum. Pasal 28D ayat (1) UUD 1945 menjamin setiap orang atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil serta perlakuan yang sama di hadapan hukum, di mana ketentuan ini relevan bagi korporasi sebagai subjek hukum. *Due process of law* mengandung makna bahwa setiap tindakan negara harus didasarkan pada legalitas norma hukum yang jelas, bukan diskresioner tanpa batas. Transparansi mengharuskan korporasi diberitahu tentang rencana penyitaan beserta alasannya, disertai kesempatan untuk didengar dalam mengajukan keberatan. Pembatasan waktu *forensic imaging* juga harus ditetapkan secara jelas, beriringan dengan akuntabilitas penyidik yang harus dapat dipertanggungjawabkan apabila terjadi pengungkapan data sensitif yang tidak perlu. Pemenuhan prinsip-prinsip *due process* ini menjadikan *forensic imaging* dapat diterapkan sebagai mekanisme penyitaan data digital yang efektif untuk penegakan hukum sekaligus adil bagi korporasi.

KESIMPULAN

Kesimpulan

Pembahasan dan analisis yang telah diuraikan pada bab-bab sebelumnya menghasilkan dua kesimpulan utama. Pertama, penerapan standar *forensic imaging* sebagai instrumen penyitaan bukti elektronik memiliki keabsahan yuridis yang kuat dalam sistem hukum acara pidana Indonesia, berlandaskan pada Pasal 5 dan Pasal 43 UU ITE jo. Pasal 38 KUHAP, serta dioperasionalkan melalui standar teknis Perkapuslabfor Nomor 1 Tahun 2014. Mekanisme ini merupakan bentuk penyitaan yang sah dan proporsional karena bersifat *mirroring*, mengamankan

---

[26] Sacvio Fath Senajaya, Handar Subhandi Bakhtiar, dan Slamet Tri Wahyudi, "Reformulasi Peraturan Digital Forensic Di Dalam Proses Pembuktian Perkara Tindak Pidana Korupsi Di Kejaksaan Agung Republik Indonesia", *Jurnal Kajian Hukum Dan Kebijakan Publik*, Vol. 3, No. 2, Januari-Juni 2026, hlm. 478.

[27] Sangkot Setiawan Lubis, S.H. (IPDA), *loc. cit*

[28] *Ibid.*

[29] *Ibid.*

[30] Sunnah dan Abdul Malik Mufty, *op. cit.*, hlm. 713-714.

bukti tanpa harus merampas fisik perangkat secara permanen. Keabsahan dan daya terima bukti elektronik di persidangan sangat bergantung pada pemenuhan *chain of custody* yang ketat (tahap *write protect*, *cloning*, dan *verifying* dengan nilai *hash*). Putusan Nomor 488/Pid.B/2024/PN Sda menegaskan bahwa prosedur verifikasi digital forensik adalah syarat mutlak (*conditio sine qua non*); kegagalan proses ini akan berakibat pada ditolaknya alat bukti elektronik oleh hakim karena integritas dan keaslian datanya tidak dapat dijamin. Kedua, keseimbangan antara kewenangan aparat penegak hukum dan perlindungan kelangsungan operasional serta rahasia dagang korporasi dapat diwujudkan melalui penerapan prinsip *proportionality* dan *due process of law*. Pelindungan ini dipraktikkan melalui dua lapisan yang saling melengkapi: mekanisme hukum (kewajiban izin pengadilan, pemberian BAP, hak pendampingan penasihat hukum) dan mekanisme teknis forensik (*on-site imaging*, penggunaan *write-blocker*, verifikasi *hash*, serta *data filtering*).

Saran

Kesimpulan di atas melandasi peneliti untuk mengajukan dua saran strategis. Saran pertama ditujukan kepada aparat penegak hukum (penyidik dan laboratorium forensik) agar terus meningkatkan kapasitas, kompetensi teknis, serta pemerataan sarana prasarana *digital forensics* di seluruh wilayah hukum. Standarisasi *forensic imaging* yang menentukan sah tidaknya bukti mengharuskan aparat untuk secara disiplin menjalankan dan mendokumentasikan setiap tahapan *chain of custody* (termasuk verifikasi nilai *hash* MD5/SHA-256) guna meminimalisasi risiko penolakan bukti. Saran kedua ditujukan bagi pembuat kebijakan dan instansi terkait untuk merumuskan regulasi turunan yang lebih komprehensif, tegas, dan spesifik (seperti Peraturan Kapolri atau Peraturan Mahkamah Agung yang diperbarui) mengenai pedoman teknis penyitaan sistem elektronik (*electronic discovery*). Regulasi tersebut perlu mewajibkan prosedur operasional standar terkait *data filtering* dan *on-site imaging* bagi korporasi guna memberikan kepastian hukum dan menghindari kerugian ekonomi atau kebocoran rahasia dagang pihak ketiga yang beritikad baik.

DAFTAR REFERENSI

Khudsiyah, Deya Hazirattul, Davit Rahmadan, dan Erdianto. "Penegakan Hukum Terhadap Modus Baru Kejahatan Cyber Berupa Rekayasa Informasi Teknologi Pembobolan Rekening Nasabah Melalui Internet Banking". Jurnal Ilmiah Wahana Pendidikan, Volume 11, Nomor 8.D, Agustus 2025.

Pattipeilohy, Viona Violeta Marselina, Diva A.E. Rombot, dan Syamsia Midu. "Tinjauan Hukum Terhadap Penyitaan Barang Bukti Elektronik Dalam Tindak Pidana Di Bidang Teknologi Informasi Dan Komunikasi".

Pribadi, Insan. "Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana". LEX Renaissance, Volume 3, Nomor 1, Januari 2018.

Safei, Muhammad, Sandra Dewi, dan Olivia Anggie Johar. "Implementasi Pada Alat Bukti Jejak Digital Dalam Penegakan Hukum Tindak Pidana Penipuan Online". Collegium Studiosum Journal, Volume 8, Nomor 2, Desember 2025.

Senajaya, Sacvio Fath, Handar Subhandi Bakhtiar, dan Slamet Tri Wahyudi. "Reformulasi Peraturan Digital Forensic Di Dalam Proses Pembuktian Perkara Tindak Pidana Korupsi Di Kejaksaan Agung Republik Indonesia". Jurnal Kajian Hukum Dan Kebijakan Publik, Volume 3, Nomor 2, Januari-Juni 2026.

Sukmawan, Yulia Audina dan Dwi Damayanti. "Metode Penelitian Hukum Normatif dan Empiris sebagai Strategi Penguatan Perspektif Kajian Ilmu Hukum". Notary Law Journal, Volume 4, Issue 1, 2025.

Sunnah dan Abdul Malik Mufty. "Paradigma Baru Pembuktian Pidana Berbasis Teknologi dalam KUHAP Baru dan Implikasinya terhadap Standar Fair Trial di Indonesia". Khatulistiwa: Jurnal Pendidikan dan Sosial Humaniora, Volume 6, Nomor 2, Juni 2026.

Thealma, Feby dan Yova Ruldeviyani. "Digital Forensic Ethical Data Handling in Indonesia". The Indonesian Journal of Computer Science, Volume 14, Issue 1, February 2025.

Tiba, Stefania Kandida Sena. "Implikasi Penolakan Bukti Elektronik Tanpa Verifikasi Digital Forensik: Studi Putusan dan Analisis Yuridis". Media Hukum Indonesia (MHI), Volume 4, Nomor 1, Desember 2025.

Wachjoe P., H. Santhos. "Penggunaan Informasi Elektronik dan Dokumen Elektronik Sebagai Alat Bukti Persidangan". Jurnal Hukum dan Peradilan, Volume 5, Nomor 1, Maret 2016.

Wiraguna, Sidi Ahyar. "Eksplorasi Metode Penelitian Dengan Pendekatan Normatif Dan Empiris Dalam Penelitian Hukum Di Indonesia". Lex Jurnalica, Volume 22, Nomor 1, 2025.

Peraturan Perundang-undangan

Kitab Undang-Undang Hukum Acara Pidana (Undang-Undang Nomor 8 Tahun 1981).

Peraturan Kabareskrim Polri Nomor 1 Tahun 2014

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (beserta perubahannya).

Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang.

Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas.

Putusan Pengadilan

Putusan Pengadilan Negeri Sidoarjo Nomor 488/Pid.B/2024/PN Sda.

Wawancara

Lubis, Sangkot Setiawan (IPDA). Wawancara Pribadi (via WhatsApp), 10 Juni 2026, pukul 12.00 WIB.