LEX PROGRESSIUM
Organized by Yayasan Pendidikan Dan Pelayanan Kesehatan Rahmat Husada
Email: lexprogressium@gmail.com
Website: https://jurnal.dokterlaw.com/index.php/lexprogressium/index

PERAN DIGITAL FORENSIK DALAM PENEGAKAN HUKUM TERHADAP KEJAHATAN KONVENSIONAL

Article

Author
Tri Yoga Achmad Budianto[1], Sujono[2]

[1]Faculty Of Law, Dirgantara Marsekal Suryadarma University
[2]Faculty Of Law, Dirgantara Marsekal Suryadarma University

Email
triyogaab@gmail.com[1],
sujono@unsurya.ac.id[2]

Data
Submitted:01-08-2024
Revised:01-12-2024
Accepted:20-01-2025

Abstract

Abstract : *The main challenge faced by law enforcement in Indonesia is the need for increased capacity in dealing with the misuse of electronic devices for conventional crimes. This includes the development of skills in digital forensics, increased cooperation between law enforcement agencies, and the formation of stricter regulations related to crimes in the digital realm. This study discusses the legal regulations in Indonesia regarding the use of digital forensics in law enforcement and the implications of legal evidence that arise in the use of digital forensics in law enforcement against conventional crimes. This study is normative juridical. It can be concluded that the regulation (legality) of electronic evidence has been legally clarified in Chapter III concerning Information, Documents, and Electronic Signatures in Articles 5, Article 6, and through reaffirmation in Article 44 of Law Number 28 of 2011 concerning Information and Electronic Transactions. This electronic evidence is very much needed in the Criminal Justice System in order to pass judgment on defendants who are tried in cases of technological crimes by making electronic evidence as valid evidence in criminal trials. Digital forensics in a crime helps to prove a conventional crime case digitally. In accordance with Article 5 paragraph (1) of the Republic of Indonesia Law Number 11 of 2008 Law No. 19 of 2016 concerning Electronic Information and Transactions, electronic information and/or electronic documents and/or printouts are valid legal evidence.*

Keywords *:Digital Forensics, Law Enforcement, Crime, Conventional*

Abstrak : Tantangan utama yang dihadapi oleh penegakan hukum di Indonesia adalah kebutuhan akan peningkatan kapasitas dalam menghadapi penyalahgunaan perangkat elektronik untuk kejahatan konvensional. Hal ini meliputi perkembangan keterampilan dalam digital forensik, peningkatan Kerjasama antara Lembaga penegak hukum, dan pembentukan regulasi yang lebih ketat terkait dengan kejahatan di ranah digital. Penelitian ini membahas pengaturan hukum di Indonesia mengenai penggunaan digital forensik dalam penegakan hukum dan implikasi pembuktian hukum yang muncul dalam penggunaan digital forensik dalam penegakan hukum terhadap kejahatan konvensional. Penelitian ini bersifat yuridis normatif. Dapat disimpulkan, bahwa pengaturan (legalitas) alat bukti elektronik secara sah telah di perjelas di dalam BAB III tentang Informasi, Dokumen, dan Tanda Tangan Elektronik dalam Pasal 5, Pasal 6, dan melalui penegasan kembali di dalam Pasal 44 Undang-

Undang Nomor 28 Tahun 2011 tentang Informasi dan Transaksi Elektronik. Alat bukti elektronik ini sangat dibutuhkan dalam Sistem Peradilan Pidana guna untuk menjatuhkan putusan bagi terdakwa yang di sidangkan dalam kasus kejahatan Teknologi dengan menjadikan alat bukti elektronik sebagai alat bukti yang sah di dalam persidangan peradilan pidana. Digital forensik dalam suatu tindak pidana membantu pembuktian suatu kasus kejahatan konvensional secara digital. Sesuai dengan Pasal 5 ayat (1) Undang-undang Republik Indonesia Nomor 11 Tahun 2008 Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik bahwa Informasi elektronik dan/atau dokumen elektronik dan/atau cetaknya merupakan alat bukti hukum yang sah.
Kata Kunci : Digital Forensik, Penegakan Hukum, Kejahatan, Konvensional

PENDAHULUAN

Globalisasi yang berkembang pesat membawa revolusi digitalisasi teknologi, memengaruhi berbagai aspek kehidupan manusia, termasuk di Indonesia. Kemajuan teknologi informasi telah memberikan manfaat besar, tetapi juga menimbulkan tantangan baru, terutama dalam penegakan hukum terhadap kejahatan konvensional yang kini beralih ke ranah digital. Pemerintah Indonesia telah menetapkan regulasi untuk memastikan pembangunan nasional dapat berjalan selaras dengan perkembangan teknologi, termasuk dalam penanganan kejahatan yang melibatkan perangkat elektronik.[1]

Penyalahgunaan perangkat elektronik menjadi tantangan serius dalam dunia hukum. Teknologi seperti smartphone dan internet sering dimanfaatkan untuk kejahatan seperti pencurian identitas, penipuan, pemerasan online, peredaran konten ilegal, serta kejahatan finansial berbasis internet. Pelaku juga memanfaatkan media sosial sebagai sarana merencanakan kejahatan. Maraknya akses internet juga meningkatkan risiko kejahatan digital terhadap kelompok rentan seperti anak-anak dan remaja.

Dalam menghadapi tantangan ini, digital forensik menjadi elemen penting dalam investigasi dan pembuktian hukum. Digital forensik adalah proses penyelidikan berbasis teknologi yang memungkinkan pengumpulan, analisis, dan validasi bukti digital agar dapat digunakan secara sah di pengadilan. Bukti elektronik dapat berupa catatan aktivitas, pesan teks, atau rekaman transaksi digital.[2] Namun, penerapan digital forensik di Indonesia masih menghadapi kendala, seperti kurangnya tenaga ahli, infrastruktur yang terbatas, serta prosedur

[1] Nurul Aisyah et al., "Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review," *Jurnal Esensi Infokom: Jurnal Esensi Sistem Informasi Dan Sistem Komputer* 6, no. 1 (2022): 22–27.
[2] Andria Andria dan Sekreningsih Nita, "Forensik Digital Sistem Informasi Berbasis Web," *JAMI: Jurnal Ahli Muda Indonesia* 2, no. 2 (2021): 137–149.

hukum yang kompleks. Oleh karena itu, peningkatan kapasitas aparat penegak hukum melalui pelatihan dan kerja sama dengan akademisi serta sektor swasta sangat diperlukan.

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) menjadi dasar hukum utama dalam menangani kejahatan digital. Beberapa pasal dalam UU ITE yang berkaitan dengan digital forensik antara lain:

a) Pasal 5, yang menyatakan bahwa informasi elektronik dan dokumen elektronik dapat dijadikan alat bukti yang sah.
b) Pasal 26, yang mengatur tentang penyalahgunaan sistem elektronik dan menjadi dasar investigasi digital forensik.
c) Pasal 27, yang membahas tanggung jawab penyelenggara sistem elektronik dalam menyimpan informasi.
d) Pasal 28, yang berkaitan dengan validitas transaksi elektronik dalam proses hukum.

Keterkaitan antara kejahatan konvensional dengan digital forensik tampak dalam berbagai kasus kriminal yang menggunakan bukti digital untuk mengungkap kejahatan, seperti pencurian, pembunuhan, korupsi, dan penyalahgunaan narkotika. Perangkat seperti CCTV sering menjadi sumber bukti penting dalam investigasi.[3]

Salah satu contoh penerapan digital forensik di Indonesia adalah kasus pembunuhan anak di Kolam Renang Taman Palem, Jakarta Timur, pada Januari 2024. Awalnya, korban diduga tenggelam, tetapi hasil digital forensik dari rekaman CCTV menunjukkan adanya kejanggalan. Selain itu, analisis terhadap ponsel tersangka oleh tim forensik digital Polri berhasil mengungkap bukti tambahan, seperti riwayat aktivitas dan komunikasi tersangka. Proses pembuktian dalam kasus ini juga menghadapi tantangan dalam menentukan **mens rea**, yaitu niat jahat pelaku dalam hukum pidana.

Kasus ini menegaskan bahwa bukti digital memiliki peran strategis dalam sistem peradilan pidana. Oleh karena itu, diperlukan regulasi yang lebih spesifik mengenai digital forensik agar dapat digunakan secara lebih efektif dalam penegakan hukum di Indonesia.

Berdasarkan uraian latar belakang diatas, maka peneliti tertarik untuk melakukan penelitian dengan mengangkat judul "Peran Digital Forensik Dalam Penegakan Hukum Terhadap Kejahatan Konvensional*"*.

[3] W. Eriani, "Pengaturan Digital Forensik dalam Pembuktian Tindak Pidana Cyber Crime" (Skripsi, Universitas Jambi, 2022).

METODE PENELITIAN

Jenis penelitian yang dipergunakan dalam penelitian ini adalah jenis penelitian hukum yuridis normatif. Pendekatan penelitian hukum yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan *(statute approach),* pendekatan konseptual *(conceptual approach),* dan pendekatan kasus *(case approach).* Jenis Data yang dipergunakan dalam penelitian ini adalah data sekunder. Untuk memperoleh informasi atau data yang diperlukan guna menjawab rumusan masalah penelitian, Peneliti menggunakan metode atau teknik pengumpulan data dengan *library research.* Metode analisis data yang dipergunakan adalah analisis data kualitatif.

HASIL PENELITIAN DAN PEMBAHASAN

1. Pengaturan Hukum Di Indonesia Mengenai Penggunaan Digital Forensik Dalam Penegakan Hukum Terhadap Kejahatan Konvensional

Penggunaan digital forensik dalam penegakan hukum terhadap kejahatan konvensional di Indonesia semakin penting seiring dengan perkembangan teknologi informasi dan komunikasi, terutama di era Revolusi Industri 4.0. Revolusi ini membawa perubahan signifikan dalam tatanan sosial dan ekonomi, termasuk munculnya budaya baru seperti *"human machine communication", "internet of things",* dan *"big data".*[4] Namun, perkembangan ini juga menimbulkan tantangan, seperti meningkatnya angka pengangguran akibat otomatisasi. Oleh karena itu, Polri perlu memanfaatkan teknologi informasi untuk memelihara keamanan dan ketertiban masyarakat (kamtibmas) serta merespons laporan dengan cepat.[5]

Digital forensik adalah metode investigasi yang menggunakan ilmu dan teknologi untuk menganalisis jejak dan bukti digital dalam kasus kejahatan. Bukti digital dapat ditemukan dalam penyimpanan permanen atau sementara, seperti *Solid State Drive* (SSD) atau *flashdisk.* Proses forensik digital memerlukan aplikasi atau tools seperti *FTK Imager* dan *Autopsy* untuk mempermudah analisis dan pemulihan data yang telah dihapus.[6]

Di Indonesia, pengaturan hukum mengenai penggunaan digital forensik diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). UU ITE mengakui informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah,

[4] M. H. Akbar dan I. Riadi, "Analisis Bukti Digital pada Flash Disk Drive Menggunakan Metode Generic Computer Forensic Investigation Model (GCFIM)," 2019, 715–723.
[5] I. Riadi, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute of Justice (NIJ)," vol. 3, no. 1, 2019.
[6] I. Riadi, S. Sunardi, dan A. Hadi, "Analisis Bukti Digital SSD NVMe pada Sistem Operasi Proprietary Menggunakan Metode Static Forensics," no. February 2020, 2019.

sebagaimana diatur dalam Pasal 5 ayat (1). Informasi elektronik mencakup data seperti email, gambar, dan suara, sementara dokumen elektronik adalah informasi yang dibuat, dikirim, atau disimpan dalam bentuk digital. Untuk memastikan keabsahan bukti digital, sistem elektronik yang digunakan harus andal, aman, dan bertanggung jawab.

Dalam proses penyidikan, penyidik dapat menggunakan alat bukti digital seperti *Call Data Record* (CDR) dari provider telekomunikasi atau hasil cloning handphone menggunakan alat seperti *Cellebrite.* Data ini kemudian dianalisis oleh ahli digital forensik untuk dijadikan bukti sah di pengadilan. Ahli forensik harus membuat laporan teknis yang menjelaskan analisis tersebut, yang kemudian dilampirkan sebagai Berita Acara Pemeriksaan (BAP). Laporan ini harus disusun dengan bahasa yang sederhana agar dapat dipahami oleh hakim, jaksa, dan penasihat hukum.

Digital forensik juga memainkan peran penting dalam kasus kejahatan konvensional, seperti pembunuhan berencana. Penyidik dapat menggunakan teknologi tinggi seperti *Alsus Direction Finder* untuk menentukan lokasi pelaku berdasarkan sinyal *handphone, Mapinfo Professional* untuk memetakan lokasi secara *real-time,* dan *i2 Analyst Notebook* untuk menganalisis jaringan komunikasi pelaku. Alat-alat ini membantu penyidik melacak pelaku, membuktikan motif, dan memenuhi unsur-unsur tindak pidana sesuai Pasal 340 KUHP.

Prosedur penyelidikan dan penyidikan dalam kasus pembunuhan berencana melibatkan beberapa tahapan:

1) *Cloning handphone* pelaku menggunakan *Cellebrite* untuk mendapatkan data komunikasi.
2) Menentukan lokasi pelaku menggunakan *Alsus Direction Finder* dan *Mapinfo Professional.*
3) Menganalisis *Call Data Record* (CDR) dari *BTS provider* telekomunikasi menggunakan *software i2 Analyst Notebook* untuk membuat jaringan komunikasi pelaku.
4) Melakukan penangkapan setelah bukti permulaan yang cukup terpenuhi sesuai Pasal 184 KUHAP.

Kegunaan alat dan software dalam penyelidikan meliputi:

1) *Alsus DF:* Menentukan titik koordinat pelaku.
2) *Cellebrite:* Mengkloning handphone untuk mendapatkan bukti digital.
3) *Mapinfo Professional:* Memetakan lokasi pelaku secara real-time.
4) *i2 Analyst Notebook:* Menganalisis jaringan komunikasi dan transfer uang pelaku.

Digital forensik tidak hanya membantu dalam kasus kejahatan siber, tetapi juga dalam kejahatan konvensional seperti pembunuhan. Dengan memanfaatkan teknologi tinggi dan software canggih, penyidik dapat membuktikan unsur-unsur tindak pidana, termasuk motif dan perencanaan pelaku. Hal ini sesuai dengan prinsip pembuktian dalam hukum acara pidana, yang bertujuan untuk mencari kebenaran materiil.

Secara keseluruhan, penggunaan digital forensik dalam penegakan hukum di Indonesia telah diakomodir oleh UU ITE dan KUHAP. Alat bukti digital seperti informasi elektronik dan dokumen elektronik diakui sebagai alat bukti yang sah, asalkan memenuhi persyaratan formil dan materiil. Ahli digital forensik memegang peran krusial dalam menjelaskan dan menganalisis bukti digital agar dapat diterima di pengadilan. Dengan demikian, digital forensik menjadi instrumen penting dalam menghadapi kejahatan di era digital, baik kejahatan siber maupun kejahatan konvensional.

2. Implikasi Pembuktian Hukum Yang Muncul Dalam Penggunaan Digital Forensik Dalam Penegakan Hukum Terhadap Kejahatan Konvensional

Pembuktian merupakan bagian yang sangat strategis dan menjadi inti dalam penyelesaian perkara pidana. Menurut Eddy Hiariej, pembuktian pidana bertujuan untuk mencari kebenaran materiil suatu peristiwa hukum, yaitu kebenaran yang sesungguhnya. Di Indonesia, sistem pembuktian yang dianut adalah *negatief wettelijk bewijstheorie,* di mana hakim harus memperoleh keyakinan berdasarkan alat bukti yang sah dan diatur dalam undang-undang. Hal ini diatur dalam Pasal 183 Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yang menyatakan bahwa hakim harus mendasarkan putusannya pada minimal dua alat bukti yang sah. Sistem pembuktian ini juga menjadi acuan dalam pembuktian perkara pidana di luar KUHAP.[7]

Perkembangan teknologi, khususnya dalam bidang keamanan komputer, telah membawa tantangan baru dalam proses pembuktian, terutama terkait bukti digital. Keaslian dan integritas bukti digital menjadi masalah mendasar, sehingga diperlukan forensik digital untuk memeriksa dan menganalisis bukti digital agar dapat dipercaya. Forensik digital adalah metode investigasi yang menggunakan ilmu pengetahuan dan teknologi untuk menganalisis bukti digital dari sistem elektronik. Hasil dari proses forensik digital ini adalah *digital evidence* (bukti digital) serta laporan hasil uji forensik.

[7] Rachmie, S. "Peranan Ilmu Digital Forensik terhadap Penyidikan Kasus Peretasan Website." *Litigasi* 21 (2020): 104–127.

Bukti digital diakui sebagai alat bukti yang sah di Indonesia berdasarkan Pasal 5 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Namun, ahli forensik digital, Christopher, menekankan bahwa barang bukti asli harus dijaga keutuhannya, tidak seperti dalam kasus medis di mana tubuh korban dapat dibedah. Penyidik memiliki wewenang untuk mengumpulkan bukti sesuai dengan Pasal 2 ayat (1) KUHAP, yang menyatakan bahwa penyidikan adalah serangkaian tindakan untuk mencari dan mengumpulkan bukti serta menemukan tersangka. Dalam kasus kejahatan berbasis teknologi, penerapan ilmu digital forensik menjadi kunci untuk memahami dan membuktikan kasus tersebut.

Untuk menghadapi kejahatan siber yang semakin kompleks dan canggih, diperlukan beberapa langkah strategis, antara lain:

1) Pelatihan digital forensik bagi petugas penegak hukum. Investasi dalam pelatihan dan pengembangan keterampilan digital forensik sangat penting agar petugas penegak hukum dapat mengatasi tantangan kejahatan siber dengan lebih efektif.
2) Kolaborasi multidisipliner antara ahli forensik digital, ahli hukum, dan ahli teknologi informasi. Kerja sama ini memungkinkan analisis forensik yang komprehensif dan mendalam untuk mendukung proses penegakan hukum.
3) Penyediaan teknologi forensik terkini. Menyediakan perangkat dan perangkat lunak forensik terbaru adalah langkah penting untuk memastikan tim forensik memiliki alat yang diperlukan untuk menghadapi kejahatan di ranah digital yang semakin kompleks.[8]

Pasal 5 ayat (3) UU ITE mengatur bahwa informasi atau dokumen elektronik dinyatakan sah jika menggunakan sistem elektronik yang andal, aman, dan bertanggung jawab, serta dapat menampilkan informasi secara utuh. Persyaratan formil alat bukti elektronik diatur dalam Pasal 5 ayat (4) dan Pasal 43 UU ITE, yang meliputi:

1) Informasi atau dokumen elektronik tidak berlaku untuk surat yang menurut undang-undang harus dibuat dalam bentuk tertulis atau akta notariil.
2) Penggeledahan atau penyitaan terhadap sistem elektronik harus dilakukan atas izin ketua pengadilan negeri setempat.
3) Penggeledahan atau penyitaan harus tetap menjaga terpeliharanya kepentingan pelayanan umum.

[8] Nur Laili, Isma, dan Arima Koyimatun. "Kekuatan Pembuktian Alat Bukti Informasi Elektronik pada Dokumen Elektronik serta Hasil Cetaknya dalam Pembuktian Tindak Pidana." *Jurnal Penelitian Hukum* 1, no. 2 (Juli 2014): 112.

Dalam sistem peradilan pidana, alat bukti elektronik memegang peranan penting untuk melindungi masyarakat dan menegakkan hukum. Fungsi sistem peradilan pidana meliputi:[9]

1) Pencegahan kejahatan.
2) Penindakan pelaku tindak pidana dengan memberikan pengertian terhadap pelaku di mana pencegahan tidak efektif.
3) Peninjauan ulang terhadap legalitas ukuran pencegahan dan penindakan.
4) Putusan pengadilan untuk menentukan bersalah atau tidak bersalah terhadap orang yang ditahan.
5) Disposisi yang sesuai terhadap seseorang yang dinyatakan bersalah.
6) Lembaga koreksi oleh alat-alat negara yang disetujui oleh masyarakat terhadap perilaku mereka yang telah melanggar hukum pidana.

Pembuktian dalam hukum acara pidana melibatkan dua unsur penting:

1) Alat bukti yang sah sesuai dengan peraturan perundang-undangan. Para pihak dalam tahapan pembuktian harus menggunakan alat bukti yang sah dan tidak boleh menggunakan alat bukti yang tidak diatur dalam peraturan perundang-undangan.
2) Peraturan pembuktian yang mengatur cara pembuatan, penggunaan, dan kekuatan alat bukti. Alat-alat bukti yang diatur dalam peraturan perundang-undangan dianggap sebagai alat bukti yang sah dan dapat dipergunakan sebagai alat bukti di persidangan.

ALAT BUKTI HUKUM ACARA PERDATA	ALAT BUKTI HUKUM ACARA PIDANA	ALAT BUKTI HUKUM ACARA TUN
Pasal 164 HIR dan 284 Rbg	Pasal 184 KUHAP	Pasal 100 UU PTUN
1. Tulisan atau Surat	1. Keterangan Saksi	1. Surat atau Tulisan
2. Saksi – saksi	2. Keterangan Ahli	2. Keterangan Ahli
3. Persangkaan	3. Surat	3. Keterangan Saksi
4. Pengakuan	4. Petunjuk	4. Pengakuan para pihak
5. Sumpah	5. Keterangan Terdakwa	5. Pengetahuan Hukum

Gambar 5.1 Alat Bukti Hukum Acara Perdata, Pidana dan TUN

Persyaratan materiil dan formil alat bukti elektronik diatur dalam UU ITE. Persyaratan materiil meliputi keandalan sistem elektronik, sedangkan persyaratan formil meliputi larangan penggunaan informasi elektronik untuk surat yang harus dibuat secara tertulis atau akta notariil, serta prosedur penggeledahan dan penyitaan yang harus dilakukan atas izin ketua pengadilan negeri. Pasal 30 UU ITE juga melarang akses tanpa izin ke sistem elektronik orang lain, namun tidak ada mekanisme jelas jika seseorang menolak memberikan akses password.

[9] Edmon Makarim, *Kompilasi Hukum Telematika* (Jakarta: PT Raja Grafindo Persada, 2004), 435.

Dengan demikian, pengembangan forensik digital dan pemahaman tentang alat bukti elektronik menjadi langkah penting dalam menghadapi kejahatan di era digital. Peningkatan kapasitas petugas penegak hukum, kolaborasi antar disiplin ilmu, dan penyediaan teknologi terkini adalah upaya yang diperlukan untuk memastikan keadilan dan keamanan dalam lingkungan digital yang semakin kompleks.

KESIMPULAN

Pengaturan (legalitas) alat bukti elektronik secara sah telah di perjelas di dalam BAB III tentang Informasi, Dokumen, dan Tanda Tangan Elektronik dalam Pasal 5, Pasal 6, dan melalui penegasan kembali di dalam Pasal 44 Undang-Undang Nomor 28 Tahun 2011 tentang Informasi dan Transaksi Elektronik. Alat bukti elektronik ini sangat dibutuhkan dalam Sistem Peradilan Pidana guna untuk menjatuhkan putusan bagi terdakwa yang di sidangkan dalam kasus kejahatan Teknologi dengan menjadikan alat bukti elektronik sebagai alat bukti yang sah di dalam persidangan peradilan pidana. Dan juga pengaturan alat bukti elektronik di dalam UU ITE tersebut di atas, merupakan perluasan dari alat bukti yang sudah di atur dalam KUHAP Pasal 184. Peran *digital forensic* dalam melakukan pengolahan alat bukti merupakan suatu langkah yang diperlukan dalam hal alat bukti elektronik akan dipergunakan sebagai alat bukti dalam persidangan. Seharusnya dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Teknologi dan Informasi memasukkan Pasal mengenai Digital Forensik guna mengolah dokumen elektronik atau barang bukti elektronik agar dapat digunakan sebagai alat bukti elektronik dalam persidangan.

Digital forensik dalam suatu tindak pidana membantu pembuktian suatu kasus kejahatan konvensional secara digital. Sesuai dengan Pasal 5 ayat (1) Undang-undang Republik Indonesia Nomor 11 Tahun 2008 Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik bahwa Informasi elektronik dan/atau dokumen elektronik dan/atau cetaknya merupakan alat bukti hukum yang sah.

SARAN

Diperlukan peningkatan investasi dalam pelatihan dan pengembangan keterampilan digital forensik bagi petugas penegak hukum. Ini akan memungkinkan mereka untuk mengatasi tantangan kompleks kejahatan dengan lebih efektif.

Perlu mendorong kerja sama erat antara ahli forensik digital, ahli hukum, dan ahli teknologi informasi sangat penting. Kolaborasi ini akan memungkinkan analisis forensik yang komprehensif dan mendalam untuk mendukung proses penegakan hukum. Penyediaan

Perlu menyediakan perangkat dan perangkat lunak forensik terbaru adalah langkah penting dalam memastikan tim forensik memiliki alat yang diperlukan untuk menghadapi kejahatan di ranah digital yang semakin kompleks dan canggih.

DAFTAR PUSTAKA

Andria Andria dan Sekreningsih Nita. "Forensik Digital Sistem Informasi Berbasis Web." *JAMI: Jurnal Ahli Muda Indonesia* 2, no. 2 (2021).

Edmon Makarim. *Kompilasi Hukum Telematika.* Jakarta: PT Raja Grafindo Persada, 2004.

I. Riadi, S. Sunardi, dan A. Hadi. "Analisis Bukti Digital SSD NVMe pada Sistem Operasi Proprietary Menggunakan Metode Static Forensics," no. February 2020, 2019.

I. Riadi. "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute of Justice (NIJ)," *Jurnal ...*, vol. 3, no. 1, 2019.

M. H. Akbar dan I. Riadi. "Analisis Bukti Digital pada Flash Disk Drive Menggunakan Metode Generic Computer Forensic Investigation Model (GCFIM)," 2019.

Nur Laili, Isma, dan Arima Koyimatun. "Kekuatan Pembuktian Alat Bukti Informasi Elektronik pada Dokumen Elektronik serta Hasil Cetaknya dalam Pembuktian Tindak Pidana." *Jurnal Penelitian Hukum* 1, no. 2 (Juli 2014).

Nurul Aisyah et al. "Analisa Perkembangan Digital Forensik dalam Penyidikan Cybercrime di Indonesia Secara Systematic Review." *Jurnal Esensi Infokom: Jurnal Esensi Sistem Informasi dan Sistem Komputer* 6, no. 1 (2022).

S. Rachmie. "Peranan Ilmu Digital Forensik terhadap Penyidikan Kasus Peretasan Website." *Litigasi* 21 (2020).

W. Eriani. "Pengaturan Digital Forensik dalam Pembuktian Tindak Pidana Cyber Crime." Skripsi, Universitas Jambi, 2022.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Kitab Undang-Undang Hukum Pidana (KUHP).

Kitab Undang-Undang Hukum Acara Pidana

Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang Nomor 19 tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Undang Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Peraturan Kepala Kepolisian Negara 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

Peraturan Menteri Komunikasi dan Informatika Nomor 7 Tahun 2016 tentang Administrasi Penyidikan dan Penindakan Tindak Pidana di Bidang Teknologi Informasi dan Transaksi Elektronik

Peraturan Presiden Nomor 53 Tahun 2017 Tentang Badan Siber dan Sandi Negara.