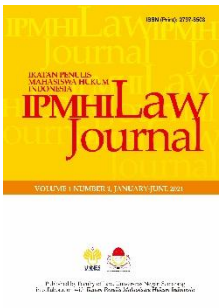
IKATAN PENULIS MAHASISWA HUKUM INDONESIA
LAW JOURNAL



ISSN 2797-8508 (Print)
ISSN 2807-8330 (Online)
VOL. 5 NO. 3, JUNE-DEC (2025)

Riwayat Artikel
History of Article
Diajukan: 12 Desember 2025
Submitted
Direvisi: 25 Desember 2025
Revised
Diterima: 2 Febuari 2026
Accepted

Saran Perujukan
How to cite:
Nugraha, Michael Adi., & Widjayanto, I. (2025). Konsep Lembaga Khusus Pemberian Bantuan Hukum Dalam Hukum Acara Pidana: Studi Komparatif Antara Indonesia Dan Belanda *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal, 5*(3), 209-230. https://doi.org/10.15294/ipmhi.v5i3.44723

OPTIMALISASI DIGITAL FORENSIK: UPAYA PENGUATAN ALAT BUKTI ELEKTRONIK DALAM TINDAK PIDANA SIBER DI INDONESIA

Optimization of Digital Forensics: Efforts to Strengthen Electronic Evidence in Cybercrime in Indonesia

Michael Adi Nugraha ✉, Indung Widjayanto
Fakultas Hukum Universitas Negeri Semarang

✉Email Korespondensi: michaeladi@students.unnes.ac.id

Abstract The rapid development of information technology has significantly increased the complexity of cybercrime, particularly in relation to the collection and verification of electronic evidence. Although Indonesian law has formally recognized electronic evidence through the Criminal Procedure Code and the Law on Information and Electronic Transactions, practical challenges remain in ensuring its admissibility and probative value in court. This study aims to examine the role of digital forensics in strengthening electronic evidence in cybercrime

cases in Indonesia, with a particular focus on the influence of evolving cybercrime modus operandi on evidence collection and verification. This research employs a qualitative approach with an empirical juridical method by combining normative legal analysis and empirical data. Normative analysis focuses on relevant laws and regulations governing electronic evidence and cybercrime, while empirical data were obtained through in-depth interviews with law enforcement officials from the Indonesian National Police. The collected data were analyzed descriptively through data reduction, presentation, and interpretation. The findings indicate that increasingly sophisticated cybercrime techniques—such as encryption, anonymization, cross-border servers, and data deletion—significantly complicate the collection and preservation of electronic evidence. Digital forensics plays a crucial role in addressing these challenges by ensuring data authenticity, integrity, and reliability, as well as by translating technical findings into legally comprehensible expert testimony. However, the effectiveness of digital forensics is highly dependent on proper implementation of standard operating procedures and consistent application of the chain of custody. This study concludes that optimizing digital forensics is essential not only to enhance the technical reliability of electronic evidence but also to strengthen its legal legitimacy within the criminal justice system.

Keywords Cybercrime, Digital Forensics, Electronic Evidence

Abstrak Perkembangan teknologi informasi yang pesat telah mendorong meningkatnya kompleksitas tindak pidana siber, khususnya dalam aspek pengumpulan dan pembuktian alat bukti elektronik. Meskipun hukum positif di Indonesia telah mengakui informasi elektronik dan/atau dokumen elektronik sebagai alat bukti yang sah, penerapannya dalam praktik peradilan masih menghadapi berbagai tantangan, terutama akibat perkembangan modus operandi kejahatan siber yang semakin canggih. Penelitian ini bertujuan untuk menganalisis peran digital forensik dalam memperkuat kedudukan alat bukti elektronik dalam penegakan hukum tindak pidana siber di Indonesia. Penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian yuridis empiris. Jenis Data yang di gunakan adalah Data Primer dan Data Sekunder. Data Primer didapat melalui wawancara dengan Perwira di Bareskrim Polri. Data Sekunder di peroleh melalui studi pustaka terhadap bahan Hukum Primer dan bahan Hukum Sekunder. Data yang diperoleh dianalisis secara kualitatif deskriptif untuk memahami kesesuaian antara pengaturan hukum dan praktik penegakan hukum di lapangan. Hasil penelitian menunjukkan bahwa penggunaan teknik kejahatan siber seperti enkripsi, anonimitas, jaringan lintas negara, dan penghapusan data secara sistematis berdampak signifikan terhadap kesulitan pengumpulan alat bukti elektronik. Digital forensik berperan penting dalam menjamin keaslian, keutuhan, dan keterandalan data elektronik serta menjembatani aspek teknis dan yuridis melalui keterangan ahli. Namun, efektivitas digital forensik sangat bergantung pada penerapan standar operasional prosedur dan konsistensi chain

of custody. Penelitian ini menyimpulkan bahwa optimalisasi digital forensik merupakan faktor krusial dalam memperkuat legitimasi teknis dan yuridis alat bukti elektronik dalam sistem peradilan pidana siber di Indonesia.

Kata kunci *Digital Forensik, Alat Bukti Elektronik, Tindak Pidana Siber*.

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan masyarakat, termasuk dalam bidang hukum. Digitalisasi yang berlangsung secara masif telah menciptakan ruang siber sebagai medium baru bagi aktivitas manusia, baik dalam konteks sosial, ekonomi, maupun pemerintahan. Dalam bidang sosial, media sosial dan aplikasi pesan instan dimanfaatkan sebagai sarana komunikasi, kampanye sosial, serta penggalangan donasi secara daring. Di bidang ekonomi, teknologi mendorong pertumbuhan perdagangan via online, penggunaan dompet digital, dan sistem pembayaran elektronik dalam aktivitas transaksi bisnis. Pada sektor pemerintahan, penerapan *e-government* terlihat melalui layanan administrasi kependudukan daring, pajak elektronik, serta perizinan online yang meningkatkan efisiensi pelayanan publik. Sementara itu, dalam bidang hukum, teknologi diwujudkan melalui penggunaan sistem peradilan elektronik (e-*court*), pengelolaan arsip perkara digital, dan penyelenggaraan persidangan daring. Namun demikian, kemajuan teknologi tersebut juga melahirkan bentuk-bentuk kejahatan baru yang dikenal sebagai tindak pidana siber (*cybercrime*), yang karakteristiknya berbeda secara mendasar dari kejahatan konvensional. Kejahatan siber berkembang dengan tingkat kompleksitas yang tinggi, bersifat lintas batas negara, dilakukan secara anonim, serta sangat bergantung pada pemanfaatan teknologi digital sebagai sarana maupun objek kejahatan. Kondisi ini menimbulkan tantangan serius bagi aparat penegak hukum dalam mengidentifikasi pelaku, menelusuri jejak elektronik, serta mengumpulkan dan membuktikan alat bukti yang sah di hadapan hukum.[1]

Kejahatan siber di Indonesia mencakup berbagai perbuatan melawan hukum, antara lain peretasan sistem elektronik, pencurian dan penyalahgunaan data pribadi, penipuan daring, pemalsuan identitas digital, serta serangan terhadap infrastruktur informasi strategis. Ragam perbuatan tersebut menjadikan tindak pidana siber sebagai tantangan serius bagi sistem hukum pidana, khususnya dalam aspek pembuktian.[2] Perkembangan tindak pidana siber menunjukkan tingkat

[1] Hengki Irawan et al., "Dampak Teknologi Terhadap Strategi Litigasi Dan Bantuan Hukum : Tren Dan Inovasi Di Era Digital" 4 (2024): 4600–4613

[2] Agus Nugroho and An An, "Research Synthesis of Cybercrime Laws and COVID - 19 in Indonesia : Lessons for Developed and Developing Countries," Security Journal 36, no. 4 (2023): 651–70, https://doi.org/10.1057/s41284-022-00357-y.

kompleksitas yang semakin tinggi seiring pesatnya kemajuan teknologi informasi dan komunikasi yang telah merambah hampir seluruh aspek kehidupan masyarakat. Sifat lintas batas negara memungkinkan kejahatan ini dilakukan dari mana saja tanpa terikat yurisdiksi teritorial tertentu, sementara karakter anonim mempermudah pelaku menyamarkan identitas melalui berbagai teknik digital. Ketergantungan yang tinggi terhadap teknologi digital menempatkan teknologi tersebut sebagai sarana, target, sekaligus medium kejahatan, mulai dari penyalahgunaan sistem informasi dan pencurian data hingga serangan terhadap infrastruktur kritis. Kondisi tersebut menimbulkan tantangan signifikan bagi aparat penegak hukum dalam mengidentifikasi pelaku, menelusuri jejak elektronik, serta mengumpulkan dan membuktikan alat bukti elektronik yang sah dan dapat dipertanggungjawabkan di hadapan hukum.[3]

Sistem peradilan pidana menempatkan pembuktian sebagai tahap sentral yang menentukan dapat atau tidaknya seseorang dimintai pertanggungjawaban pidana. Hukum acara pidana Indonesia menganut sistem pembuktian yang mensyaratkan adanya alat bukti yang sah menurut undang-undang serta keyakinan hakim. Pengaturan normatif mengenai alat bukti tercantum dalam Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP) yang pada masa pembentukannya belum mengantisipasi perkembangan teknologi informasi digital secara komprehensif. Pengakuan terhadap alat bukti elektronik selanjutnya diakomodasi melalui Pasal 235 ayat (1) Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana (KUHAP) serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 yang selanjutnya disebut sebagai UU ITE. Undang-undang tersebut menegaskan bahwa informasi elektronik dan/atau dokumen elektronik beserta hasil cetaknya merupakan alat bukti hukum yang sah. Pengakuan normatif tersebut belum sepenuhnya menjamin kekuatan pembuktian alat bukti elektronik dalam praktik peradilan karena masih kerap muncul perdebatan mengenai keaslian, integritas, serta tata cara perolehan bukti elektronik.

UU ITE merupakan instrumen hukum yang dirancang untuk mengakomodasi perkembangan teknologi informasi dalam sistem hukum nasional sekaligus memberikan kepastian hukum terhadap pemanfaatan teknologi digital. Pengaturan dalam undang-undang tersebut menegaskan pengakuan yuridis terhadap informasi elektronik dan/atau dokumen elektronik beserta hasil cetaknya sebagai subjek hukum dan alat bukti yang sah dalam proses peradilan. Perubahan UU ITE dilakukan untuk memperjelas norma, memperkuat perlindungan hukum, serta menyesuaikan ketentuan pidana dengan dinamika pemanfaatan teknologi informasi, sehingga

[3] M Fadilurrahman, Tahta Kurniawan, and Syahrial Shaddiq, "Systematic Literature Review of Disruption Era in Indonesia : The Resistance of Industrial Revolution 4 . 0" 2, no. 1 (2021), https://doi.org/10.18196/jrc.2152.

keberadaannya memiliki peran strategis dalam penegakan hukum tindak pidana siber di Indonesia.[4]

Kasus ransomware yang menimpa Bank Syariah Indonesia (BSI) pada Mei 2023 menggambarkan secara nyata kompleksitas pembuktian digital forensik dalam konteks tindak pidana siber. Kelompok peretas yang mengklaim bertanggung jawab atas serangan tersebut menggunakan varian ransomware LockBit 3.0 yang melumpuhkan layanan perbankan elektronik BSI untuk beberapa hari dan mengklaim telah mencuri sebagian besar data nasabah. Menurut laporan media, gangguan layanan tidak hanya memengaruhi transaksi ATM dan mobile banking, tetapi juga memicu kekhawatiran mengenai keamanan data pribadi jutaan pengguna, yang mencakup informasi sensitif seperti nomor rekening dan data kontak. Hal ini menunjukkan bahwa serangan ransomware dengan teknik enkripsi kuat dan pemanfaatan infrastruktur tersebar dapat menyebabkan bukti digital tersebar dalam bentuk terenkripsi serta jejak digital yang terfragmentasi, sehingga menyulitkan proses identifikasi, ekstraksi, dan analisis oleh tim digital forensik.

Peristiwa tersebut menegaskan bahwa dalam praktik penegakan hukum pidana siber, tantangan utama bukan hanya mengakui keberadaan alat bukti elektronik dalam norma hukum, tetapi juga menangani kompleksitas teknik yang digunakan oleh pelaku, seperti enkripsi tingkat tinggi dan pengoperasian dari luar yurisdiksi, yang secara signifikan memperumit proses pembuktian forensik. Dengan kata lain, bukti elektronik yang jelas secara normatif dapat kehilangan nilai pembuktiannya jika proses *chain of custody*, *integrity*, dan *authenticity* tidak dapat dibuktikan secara meyakinkan di pengadilan.[5]

Penelitian terdahulu yang terdiri dari beberapa penelitian yang penulis ambil sebagai contoh menunjukkan bahwa digital forensik menempati posisi yang semakin strategis dalam pembuktian tindak pidana siber, namun implementasinya masih menghadapi sejumlah persoalan konseptual, teknis, dan kelembagaan. Mursyid dan tim mengungkap adanya kelemahan kebijakan keamanan siber serta tantangan serius dalam implementasi hukum siber di Indonesia.[6] Dahlan dan tim menegaskan peran penting digital forensik dalam mengidentifikasi jejak digital, memulihkan data yang terhapus, serta menjaga integritas barang bukti elektronik agar dapat dipertanggungjawabkan di persidangan.[7] Namun, studi-studi berikutnya juga menyoroti berbagai kendala teknis dan prosedural, seperti lemahnya

---

[4] Irfan Santoso, Alvi Syahrin, and Mahmud Mulyadi, "Kebijakan Hukum Pidana Terhadap Perbuatan Melawan Hukum Dalam UU ITE Pasca Berlakunya Pedoman Implementasi Pasal - Pasal Tertentu UU ITE" 3, no. 4 (2024): 329–35.

[5] Souradip Nath, "Digital Evidence Chain of Custody : Navigating New Realities of Digital Forensics," 2024, 11–20, https://doi.org/10.1109/TPS-ISA62245.2024.00012.

[6] Miftahul Jannah Mursyid, Airlangga Putera, "Rekonstruksi Peran Digital Forensik Dalam Penyidikan Tindak Pidana Siber: Analisis Kritis Terhadap Konstruksi Hukum Pidana Di Indonesia" 6, no. 2 (2025).

[7] Ahmad Dahlan, Norma Sari, and Ahmad Dahlan, "Tantangan Hukum Dan Psikologis Dalam Penegakan Hukum Terhadap Pelecehan Dan Intimidasi Online Di Media Sosial" 5, no. 1 (2025): 16–34.

penerapan chain of custody, belum seragamnya standar operasional prosedur, serta keterbatasan sarana dan sumber daya manusia yang kompeten.[8] Di sisi lain, perkembangan modus operandi kejahatan siber melalui penggunaan enkripsi, anonimitas jaringan, dan perangkat lunak anti-forensik semakin meningkatkan kompleksitas pembuktian elektronik.[9] Perspektif global memperlihatkan bahwa efektivitas digital forensik sangat ditentukan oleh perlindungan integritas data, kejelasan rantai penguasaan alat bukti, dan akuntabilitas proses pemeriksaan.[10] Meskipun demikian, penelitian-penelitian sebelumnya masih memiliki keterbatasan. Kajian yang berorientasi pada aspek hukum cenderung belum mengelaborasi secara mendalam dimensi teknis digital forensik, sementara penelitian yang menitikberatkan pada aspek teknis sering kali tidak dikaitkan secara sistematis dengan prinsip dan mekanisme hukum acara pidana. Akibatnya, terdapat kesenjangan antara pengaturan normatif alat bukti elektronik dan praktik digital forensik dalam penegakan hukum tindak pidana siber.

Urgensi dan signifikansi penelitian ini terletak pada kajian mengenai optimalisasi digital forensik sebagai upaya penguatan alat bukti elektronik dalam tindak pidana siber di Indonesia. Fokus penelitian diarahkan pada analisis pengaruh modus operandi tindak pidana siber terhadap proses pengumpulan alat bukti elektronik. Penelitian ini juga menelaah optimalisasi digital forensik melalui pendekatan integratif antara aspek normatif hukum acara pidana dan praktik digital forensik guna memperkuat kedudukan, keandalan, serta validitas alat bukti elektronik dalam penegakan hukum tindak pidana siber di era digital.

B. Metode

Metode Penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian yuridis empiris. Pendekatan ini dipilih karena penelitian tidak hanya menelaah norma hukum yang tertuang dalam peraturan perundang-undangan (law in books), tetapi juga mengkaji penerapannya dalam praktik penegakan hukum (law in action), khususnya dalam konteks tindak pidana siber. Pendekatan yuridis empiris dilakukan melalui penggabungan antara kajian normatif dan kajian empiris. Kajian normatif difokuskan pada analisis peraturan perundang-undangan yang mengatur pembuktian dan tindak pidana siber, sedangkan kajian empiris diarahkan pada pengumpulan data faktual yang diperoleh dari lapangan guna memahami realitas penerapan hukum oleh aparat penegak hukum.

---

[8] Muhammad Singgih Imam Wibowo, "Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia."

[9] Cheny Berlian, "Dos Attack sebagai Tindak Pidana Siber dalam Pengaturan Hukum di Indonesia," n.d.

[10] Nina Sunde and Itiel E Dror, "Forensic Science International : Digital Investigation A Hierarchy of Expert Performance (HEP) Applied to Digital Forensics : Reliability and Biasability in Digital Forensics Decision Making," Forensic Science International: Digital Investigation 37 (2021): 301175, https://doi.org/10.1016/j.fsidi.2021.301175.

Data primer dalam penelitian ini diperoleh melalui wawancara mendalam dengan narasumber yang memiliki kompetensi dan pengalaman di bidang penegakan hukum tindak pidana siber, yaitu Perwira di Badan Reserse Kriminal (Bareskrim Polri).

Data primer dilengkapi dengan data sekunder yang diperoleh melalui studi kepustakaan terhadap bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer di teliliti melalui peraturan perundang undangan sedangkan bahan hukum sekunder diteliti meliputi buku-buku dan jurnal literatur hukum yang terkait dengan alat bukti elektronik, serta jurnal ilmiah yang relevan dengan objek penelitian. Analisis dilakukan melalui tahapan reduksi data, penyajian data, dan penarikan kesimpulan dengan menelaah serta menafsirkan data hasil wawancara dan bahan hukum yang relevan. Proses analisis ini bertujuan untuk memperoleh gambaran yang komprehensif mengenai kesesuaian antara ketentuan hukum yang berlaku dan praktik pembuktian tindak pidana siber di lapangan.

C. Hasil dan Pembahasan

1. Pengaruh Modus Operandi Tindak Pidana Siber dalam Pengumpulan Alat Buktii Elektronik

Pengaturan alat bukti elektronik dalam sistem perundang-undangan Indonesia tercermin dalam KUHAP dan Undang - Undang diluar KUHAP yaitu UU ITE, beserta Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi. Ketentuan tersebut mengakui informasi elektronik dan/atau dokumen elektronik beserta hasil cetaknya sebagai alat bukti hukum yang sah dalam proses peradilan pidana.[11]

Hasil wawancara dengan narasumber dari Bareskrim Polri menunjukkan bahwa perkembangan modus operandi tindak pidana siber berpengaruh langsung terhadap meningkatnya kompleksitas pengumpulan alat bukti elektronik. Pemanfaatan teknologi enkripsi, penggunaan akun anonim, virtual private network (VPN), serta penghapusan data secara sistematis kerap digunakan pelaku untuk menghilangkan jejak digital. VPN sendiri merupakan jaringan privat virtual yang berfungsi menyamarkan alamat protokol internet (IP address) pengguna dengan cara mengalihkan koneksi melalui server lain, sering kali berada di luar wilayah hukum Indonesia, sehingga identitas dan lokasi asli pelaku menjadi sulit dilacak. Kondisi tersebut menimbulkan kesulitan bagi penyidik dalam mengidentifikasi sumber data, menentukan kepemilikan akun, serta mengamankan alat bukti elektronik secara utuh, autentik, dan dapat dipertanggungjawabkan secara hukum.

Temuan empiris tersebut sejalan dengan ketentuan Pasal 5 ayat (1) dan ayat

[11] Frida Tyas Pramesti Ermadi Satriya Wijaya, "Analisis Bukti Digital Forensik Pada Aplikasi Facebook Messenger Dan Twitter Berbasis Android Menggunakan Proses DFRWS (Studi Kasus: Pencemaran Nama Baik)" 18, no. 1 (2024): 15–28.

(2) UU ITE, yang mengakui informasi elektronik dan/atau dokumen elektronik sebagai alat bukti hukum yang sah. Namun, dalam praktiknya, pengakuan normatif tersebut belum sepenuhnya menjamin kemudahan pembuktian, terutama ketika modus operandi tindak pidana siber menyebabkan alat bukti elektronik menjadi sulit diakses atau terfragmentasi.Selain itu, Pasal 44 Undang-Undang ITE menegaskan bahwa alat bukti dalam tindak pidana siber meliputi alat bukti sebagaimana diatur dalam hukum acara pidana serta alat bukti lain berupa informasi elektronik dan/atau dokumen elektronik. Ketentuan ini memperluas ruang pembuktian, tetapi juga menuntut aparat penegak hukum untuk memiliki pemahaman teknis yang memadai agar proses pengumpulan alat bukti tetap memenuhi prinsip legalitas dan akuntabilitas. Narasumber juga berkata bahwa kegagalan memahami modus operandi pelaku berpotensi menyebabkan loss of evidence, yang pada akhirnya melemahkan proses pembuktian di persidangan. Dengan demikian, pengaruh modus operandi tindak pidana siber terhadap pengumpulan alat bukti elektronik tidak hanya bersifat teknis, tetapi juga berdampak yuridis. Hal ini menunjukkan bahwa efektivitas pembuktian sangat bergantung pada kemampuan penyidik dalam mengintegrasikan pemahaman modus operandi kejahatan siber dengan kerangka hukum pembuktian yang berlaku.

Pengaruh modus operandi tindak pidana siber terhadap pengumpulan alat bukti elektronik Secara teknis berkaitan erat dengan seluruh tahapan operasional penyidikan, mulai dari penanganan awal perkara hingga penyajian alat bukti di persidangan.[12] Tahapan teknis tersebut menuntut ketelitian dan ketepatan langkah penyidik karena alat bukti yang dihadapi tidak lagi berbentuk fisik konvensional, melainkan berupa data elektronik yang bersifat dinamis, mudah berubah, dan rentan terhadap kerusakan. Dalam konteks ini, kesalahan pada satu tahap awal dapat berdampak signifikan terhadap keseluruhan proses pembuktian. Aspek teknis pengumpulan alat bukti elektronik meliputi beberapa tahapan penting, antara lain identifikasi sumber data elektronik, pengamanan tempat kejadian perkara digital, akuisisi data dari perangkat elektronik atau sistem informasi, serta analisis melalui metode digital forensik. Identifikasi sumber data menjadi tahap krusial karena penyidik harus menentukan lokasi dan media penyimpanan data yang relevan dengan peristiwa pidana, baik yang berada pada perangkat pelaku, korban, maupun pihak ketiga. Kesalahan dalam mengidentifikasi sumber data berpotensi menyebabkan terlewatkannya alat bukti penting atau bahkan hilangnya jejak digital yang seharusnya dapat memperkuat pembuktian.[13]

Pengamanan tempat kejadian perkara digital juga memiliki peran yang tidak kalah penting. Berbeda dengan tempat kejadian perkara konvensional, TKP digital

[12] Eka Pratiwi, "Analisis Forensik Digital dalam Mendukung Pengungkapan Tindak Kriminal" 2025, 15097–100.

[13] Zain Arfin Utama, Pandam Bayu, dan Seto Aji, "Ristek: Jurnal Riset, Inovasi dan Teknologi Kabupaten Batang Data Forensik Digital dalam Penyidikan Kejahatan" 10, no. 1 (2025): 116–23.

dapat berupa perangkat elektronik, akun daring, atau sistem jaringan yang sewaktu-waktu dapat diakses, diubah, atau dihapus dari jarak jauh.[14] Oleh karena itu, penyidik dituntut untuk segera melakukan langkah pengamanan guna mencegah perubahan atau penghapusan data. Selanjutnya, proses akuisisi data harus dilakukan dengan metode yang tepat agar keutuhan dan keaslian data tetap terjaga, sebelum kemudian dianalisis melalui proses digital forensik.[15] Dalam praktiknya, kompleksitas modus operandi tindak pidana siber sering kali menjadi hambatan utama dalam proses teknis tersebut. Penggunaan teknologi seperti enkripsi, jaringan privat virtual (VPN), server lintas negara, hingga teknik penghapusan dan penyamaran data menyebabkan alat bukti elektronik menjadi tersebar, terfragmentasi, atau sulit diakses. Kondisi ini tidak hanya menyulitkan penyidik dalam mengumpulkan alat bukti, tetapi juga meningkatkan risiko terjadinya kehilangan alat bukti elektronik sebelum berhasil diamankan secara sah.[16]

Proses teknis pengumpulan alat bukti elektronik Pada prinsipnya telah memiliki standar operasional prosedur (SOP) yang bersifat tertulis, khususnya yang berkaitan dengan digital forensik dan penanganan barang bukti elektronik. SOP tersebut mengatur tahapan penyitaan, pengamanan, pemeriksaan, hingga penyimpanan alat bukti elektronik agar tetap terjaga keutuhan dan keasliannya. Keberadaan SOP ini dimaksudkan untuk memberikan pedoman yang jelas dan seragam bagi penyidik dalam menangani alat bukti elektronik sesuai dengan ketentuan hukum yang berlaku.[17] Namun demikian, efektivitas penerapan SOP sangat bergantung pada pemahaman dan kompetensi penyidik terhadap karakteristik modus operandi tindak pidana siber. SOP yang bersifat umum tidak selalu mampu mengakomodasi variasi teknik kejahatan siber yang terus berkembang. Ketidaktepatan langkah teknis pada tahap awal penanganan perkara, meskipun SOP tersedia secara tertulis, dapat mengakibatkan terjadinya loss of evidence yang bersifat irreversibel. Kehilangan alat bukti elektronik tersebut pada akhirnya tidak hanya berdampak secara teknis, tetapi juga berimplikasi yuridis terhadap kekuatan pembuktian di persidangan. Dengan demikian, pengaruh modus operandi tindak pidana siber terhadap pengumpulan alat bukti elektronik menegaskan pentingnya integrasi antara kepatuhan terhadap SOP dan kemampuan teknis penyidik. Keberhasilan pembuktian tidak hanya ditentukan oleh ketersediaan prosedur tertulis, tetapi juga oleh kecakapan aparat penegak hukum

[14] Fakultas Hukum and Universitas Tarumanagara, "Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.5. No.7 (2024) Tema/Edisi : Hukum Pidana (Bulan Ketujuh) Https://Jhlg.Rewangrencang.Com/" 5, no. 7 (2024): 1–17.

[15] M Ihsan, "Hambatan Dalam Menangani Tindak Pidana Penipuan Melalui Media Sosial (Online) Oleh Siber Dit Reskrimsus Polda Sumsel," 2024.

[16] Hudi Yusuf Nurfitri Fathonah, "Pencegahan dan Tantangan dalam Memerangi Tindak Pidana Siber," no. September (2025): 6303–12.

[17] Linda Safitri, "Etika Profesi Polisi Etika Kepolisian" 1, no. 4 (2024): 230–35.

dalam memahami dan merespons kompleksitas kejahatan siber secara tepat dan profesional.[18]

Dampak Modus Operandi dalam aspek yuridis tindak pidana siber tercermin pada terpenuhinya atau tidak terpenuhinya syarat formil dan materil alat bukti elektronik sebagaimana diatur dalam hukum acara pidana dan Undang-Undang ITE. Kegagalan dalam proses teknis pengumpulan alat bukti berpotensi menimbulkan persoalan yuridis, seperti tidak terjaminnya keaslian (*authenticity*), keutuhan (*integrity*), dan keterkaitan alat bukti dengan perbuatan pidana. Kondisi ini dapat berimplikasi pada lemahnya nilai pembuktian di persidangan, bahkan berujung pada dikesampingkannya alat bukti oleh hakim.[19] Dengan demikian, aspek teknis dan yuridis dalam pembuktian tindak pidana siber merupakan satu kesatuan yang tidak dapat dipisahkan dan harus berjalan secara bersamaan.

Kejahatan siber (*cyber crime*) pada umumnya menghasilkan alat bukti yang bersifat digital dan tidak berwujud fisik, sehingga berbeda dengan alat bukti dalam tindak pidana konvensional.[20] Alat bukti tersebut dapat berupa informasi elektronik dan/atau dokumen elektronik, seperti data log sistem, rekaman aktivitas jaringan, metadata komunikasi, surat elektronik (*e-mail*), pesan instan, rekaman transaksi digital, konten media sosial, rekaman akses akun, hingga hasil forensik dari perangkat elektronik seperti komputer, telepon seluler, dan server. Selain itu, alat bukti elektronik dalam kejahatan siber sering kali bersifat volatile, mudah diubah, dihapus, atau dipindahkan, sehingga memerlukan penanganan khusus melalui prosedur digital forensik agar keaslian, integritas, dan rantai penguasaan (chain of custody) tetap terjaga.[21] Karakteristik alat bukti tersebut menuntut kemampuan teknis penyidik dalam melakukan akuisisi, analisis, dan penyajian bukti elektronik secara tepat agar memiliki kekuatan pembuktian yang sah dan meyakinkan di persidangan.

2. Optimalisasi Digital Forensik dalam Memperkuat Alat Bukti Elektronik

Hasil wawancara dengan narasumber dari Bareskrim Polri menunjukkan bahwa digital forensik menjadi instrumen utama dalam memperkuat kedudukan alat bukti elektronik dalam penegakan hukum tindak pidana siber. Narasumber menegaskan bahwa penerapan digital forensik dilakukan melalui tahapan yang sistematis dan terstandar, mulai dari pengamanan barang bukti, proses akuisisi

[18] Raihan Aprilianto et al., "Implementasi Fungsi Kepolisian Sebagai Pelindung Pengayom Dan Pelayan Masyarakat Dalam Mewujudkan Ketertiban Dan Keamanan Masyarakat" 1, no. 1 (2025): 168–82.
[19] Fadhila Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia" 2, no. 1 (2024): 8–16.
[20] Puti Priyana, "Alat Bukti Informasi Elektronik Tindak Pidana Penipuan Online dalam Perspektif Hukum Acara Pidana di Indonesia," 9, no. 1 (2021).
[21] Husnul Khatimah, "Analisis Hukum Bukti Elektronik Sebagai Alat Bukti Dalam Pemeriksaan Hukum Acara Perdata," n.d., 1–16.

data, analisis forensik, hingga penyajian hasil analisis dalam bentuk keterangan ahli di persidangan.

Standar Operasional Prosedur (SOP) kepolisian dalam penanganan tindak pidana siber Secara normatif tidak berdiri sendiri, melainkan diturunkan dan disusun berdasarkan ketentuan peraturan perundang-undangan serta regulasi internal kepolisian. SOP tersebut berfungsi sebagai instrumen pelaksana dari norma hukum yang bersifat umum agar dapat diterapkan secara konkret dalam praktik penegakan hukum. Dengan demikian, SOP menjadi penghubung antara ketentuan hukum normatif (*law in books*) dengan realitas teknis operasional di lapangan (*law in action*), khususnya dalam penanganan tindak pidana yang berbasis teknologi informasi dan komunikasi.[22] Keberadaan SOP dalam konteks penegakan hukum pidana siber memiliki posisi strategis karena karakteristik kejahatan siber berbeda secara fundamental dengan tindak pidana konvensional. Tindak pidana siber bersifat lintas batas negara, menggunakan sarana elektronik yang kompleks, serta sering kali melibatkan anonimitas pelaku dan distribusi data yang cepat. Oleh karena itu, ketentuan hukum yang bersifat umum memerlukan penjabaran lebih lanjut dalam bentuk SOP agar dapat diimplementasikan secara efektif, terukur, dan dapat dipertanggungjawabkan secara hukum.

Dasar hukum utama yang melandasi penyusunan SOP kepolisian dalam penanganan tindak pidana siber mencakup KUHAP. KUHAP memberikan kerangka hukum formil mengenai kewenangan penyelidikan, penyidikan, penyitaan, dan pembuktian dalam perkara pidana. Ketentuan tersebut menjadi rujukan utama agar setiap tindakan aparat penegak hukum dilakukan berdasarkan prinsip legalitas, akuntabilitas, serta penghormatan terhadap hak asasi manusia. Dalam konteks ini, SOP berfungsi sebagai pedoman teknis agar kewenangan yang diberikan oleh KUHAP dapat dijalankan secara tertib dan konsisten.[23]

Pasal KUHAP yang menjadi dasar dalam legitimasi yuridis Pembuatan SOP ialah Pasal 5 ayat (1) dan ayat (2) KUHAP mengatur kewenangan penyelidik untuk menerima laporan atau pengaduan serta melakukan tindakan awal sebagai dasar SOP penerimaan laporan, sedangkan Pasal 7 ayat (1) KUHAP memberikan dasar agar bisa dilakukan nya suatu penyidikan apabila penyelidikan dirasa cukup . Selain KUHAP ada juga Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia memberikan legitimasi yuridis dan kelembagaan kepada kepolisian untuk menyelenggarakan fungsi penegakan hukum serta menyusun kebijakan internal, termasuk SOP teknis. Ketentuan ini menegaskan bahwa kepolisian tidak hanya berperan sebagai pelaksana hukum, tetapi juga sebagai

[22] Raka Winarko., "Pelanggaran Standar Operasional Pelaksanaan (SOP) dalam Manajemen Penyidikan," 2023.

[23] Vanessa , "Analisis Keabsahan Bukti Elektronik Dalam Pemeriksaan Persidangan Perkara Pidana Dan Implementasi Admisibilitasnya (Studi Putusan)" 20, no. 4 (2025), https://doi.org/10.21070/ijler.v20i4.1395.

institusi yang memiliki kewenangan diskresi terbatas untuk mengatur tata cara pelaksanaan tugasnya sepanjang tidak bertentangan dengan peraturan perundang-undangan. Oleh karena itu, SOP kepolisian memiliki kedudukan yang sah sebagai instrumen administratif-yuridis dalam sistem penegakan hukum pidana. Dalam konteks khusus tindak pidana siber, UU ITE menjadi dasar yuridis utama. Undang-undang ini tidak hanya mengatur jenis-jenis tindak pidana siber, tetapi juga memberikan landasan hukum mengenai kewenangan penyidik serta kedudukan informasi elektronik dan/atau dokumen elektronik sebagai alat bukti hukum yang sah.

Pasal 5 dan Pasal 44 Undang-Undang ITE memperluas rezim pembuktian pidana dengan memasukkan alat bukti elektronik ke dalam sistem pembuktian yang diakui secara hukum. Berdasarkan landasan normatif tersebut, Kepolisian Negara Republik Indonesia menyusun dan mengembangkan berbagai SOP khusus yang mengatur penanganan tindak pidana siber secara lebih rinci dan teknis. SOP tersebut mencakup tahapan penyelidikan, penyidikan, patroli siber, penyitaan dan pengamanan barang bukti elektronik, pengelolaan alat bukti, hingga pelaksanaan forensik digital. SOP-SOP ini disusun untuk menyeragamkan tindakan aparat penegak hukum di lapangan sekaligus meminimalkan potensi kesalahan prosedural yang dapat berdampak pada keabsahan alat bukti.

Salah satu SOP yang memiliki peran penting dalam tahap awal penanganan perkara adalah SOP Patroli Siber yang diterapkan di lingkungan Direktorat Tindak Pidana Siber Bareskrim Polri. SOP ini mengatur alur kegiatan patroli di ruang siber mulai dari dasar hukum pelaksanaan, kualifikasi petugas pelaksana, penggunaan sarana dan prasarana teknologi informasi, hingga mekanisme pendokumentasian dan penanganan hasil patroli sebelum ditingkatkan ke tahap penyidikan. Keberadaan SOP Patroli Siber menunjukkan bahwa penanganan tindak pidana siber tidak hanya bersifat represif, tetapi juga preventif melalui upaya deteksi dini terhadap potensi pelanggaran hukum di ruang digital.Melalui SOP Patroli Siber, proses perolehan informasi elektronik sebagai bahan awal penyelidikan diharapkan dapat dilakukan secara sah, terstruktur, dan dapat dipertanggungjawabkan secara hukum. Informasi elektronik yang diperoleh melalui patroli siber dapat menjadi dasar untuk melakukan penyelidikan lebih lanjut tanpa melanggar prinsip legalitas. Dengan demikian, sejak tahap awal penanganan perkara, aparat penegak hukum telah diarahkan untuk bertindak sesuai prosedur guna menghindari perolehan alat bukti yang cacat secara yuridis.

SOP penanganan tindak pidana siber telah tersedia secara tertulis dan relatif komprehensif, implementasinya dalam praktik masih menghadapi sejumlah kendala. Salah satu permasalahan utama terletak pada ketergantungan efektivitas SOP terhadap kapasitas dan pemahaman penyidik mengenai modus operandi tindak pidana siber yang terus berkembang. Karakteristik kejahatan siber yang dinamis, adaptif, serta memanfaatkan teknologi canggih sering kali melampaui skema yang

telah diantisipasi dalam SOP yang bersifat umum. Kondisi ini menuntut penyidik untuk tidak hanya patuh secara prosedural, tetapi juga memiliki kompetensi teknis yang memadai.

Permasalahan lain muncul pada tahap pengumpulan dan pengelolaan alat bukti elektronik. Secara normatif, SOP digital forensik dan SOP chain of custody telah dirancang untuk menjamin keaslian, keutuhan, dan keterlacakan alat bukti elektronik sejak tahap penyitaan hingga penyajiannya di persidangan. SOP tersebut mengatur secara rinci prosedur penyitaan perangkat elektronik, pengamanan tempat kejadian perkara digital, pencatatan alur penguasaan barang bukti, serta mekanisme penyimpanan yang aman. Namun, dalam praktik, kesalahan teknis pada tahap awal penanganan perkara dapat menyebabkan terjadinya loss of evidence yang bersifat permanen dan sulit dipulihkan.

Kesalahan teknis tersebut tidak hanya berdampak secara operasional, tetapi juga menimbulkan implikasi yuridis yang signifikan. Alat bukti elektronik yang diperoleh atau dikelola tidak sesuai SOP berpotensi dipersoalkan keabsahannya di persidangan, baik dari aspek keaslian data, keutuhan informasi, maupun keterkaitan alat bukti dengan perbuatan pidana yang didakwakan. Dalam kondisi demikian, hakim dapat mengesampingkan alat bukti elektronik tersebut karena dianggap tidak memenuhi syarat formil maupun materil pembuktian.[24] Dalam konteks forensik digital, unit forensik kepolisian, termasuk Digital Forensic Analyst Team (DFAT) Puslabfor Bareskrim Polri, memiliki SOP yang mengatur secara teknis penanganan bukti digital. SOP tersebut mencakup prosedur penerimaan dan penyerahan barang bukti elektronik, pelaksanaan triage forensik untuk menentukan prioritas pemeriksaan, proses akuisisi data, analisis forensik, hingga pelaporan hasil pemeriksaan. Seluruh tahapan tersebut dirancang untuk memastikan bahwa proses forensik digital dilakukan secara sistematis, terdokumentasi dengan baik, serta dapat dipertanggungjawabkan secara ilmiah dan yuridis. Praktik teknisnya, penyidik dan analis forensik digital wajib melakukan proses acquiring dan imaging terhadap bukti elektronik, yaitu penggandaan data secara identik (1:1) guna menjamin bahwa data asli tidak mengalami perubahan selama proses pemeriksaan. Analisis selanjutnya dilakukan terhadap salinan data tersebut dengan menggunakan metode dan perangkat lunak forensik yang sesuai, disertai dengan dokumentasi menyeluruh atas setiap tindakan yang dilakukan. Prosedur ini tidak hanya berlandaskan SOP internal kepolisian, tetapi juga merujuk pada pedoman teknis internasional, seperti panduan ACPO dan standar ISO/IEC 27037, yang dijadikan kerangka acuan dalam pengelolaan bukti digital.

SOP chain of custody memiliki dasar hukum pada prinsip pembuktian pidana yang menuntut keterlacakan dan akuntabilitas alat bukti sejak pertama kali diperoleh hingga diajukan di persidangan. Prinsip ini bersumber dari KUHAP dan

[24] Husnul Khatimah, "Analisis Hukum Bukti Elektronik sebagai Alat Bukti dalam Pemeriksaan Hukum Acara Perdata," n.d., 1–16.

doktrin hukum pembuktian pidana, yang menekankan pentingnya menjaga kontinuitas penguasaan barang bukti. SOP chain of custody berfungsi sebagai instrumen administratif-yuridis untuk memastikan bahwa tidak terjadi manipulasi, penggantian, atau kehilangan alat bukti elektronik selama proses penanganan perkara. Dengan demikian, SOP kepolisian dalam penanganan tindak pidana siber tidak dapat dipahami semata-mata sebagai pedoman administratif, melainkan sebagai instrumen yuridis-teknis yang memiliki peran strategis dalam menentukan sah atau tidaknya alat bukti elektronik. Efektivitas pembuktian dalam perkara tindak pidana siber sangat ditentukan oleh kemampuan aparat penegak hukum dalam mengintegrasikan kepatuhan terhadap SOP tertulis dengan pemahaman teknis yang mendalam mengenai modus operandi kejahatan siber. Oleh karena itu, penguatan kapasitas sumber daya manusia, peningkatan pelatihan teknis, serta pembaruan SOP secara berkelanjutan menjadi kebutuhan mendesak guna menjawab tantangan penegakan hukum pidana di era digital.

Penguatan alat bukti elektronik melalui penerapan digital forensik memiliki kesesuaian dengan ketentuan Pasal 235 ayat (1) KUHAP yang mengatur jenis alat bukti yang sah dalam proses peradilan pidana. Meskipun KUHAP tidak secara eksplisit mencantumkan alat bukti elektronik, perkembangan teknologi informasi menuntut adanya penafsiran yang sistematis dan progresif terhadap ketentuan tersebut. Pengakuan terhadap informasi elektronik dan/atau dokumen elektronik sebagai alat bukti hukum yang sah kemudian ditegaskan dalam UU ITE, sehingga memperluas rezim pembuktian pidana yang sebelumnya bersifat konvensional. Dalam konteks ini, digital forensik berperan strategis sebagai mekanisme penghubung antara alat bukti elektronik dan alat bukti keterangan ahli sebagaimana dikenal dalam Pasal 235 ayat (1) KUHAP. Melalui digital forensik, data elektronik yang bersifat teknis dan kompleks dapat dianalisis secara ilmiah, kemudian diterjemahkan ke dalam bentuk keterangan ahli yang dapat dipahami dan dinilai oleh hakim. Oleh karena itu, hasil pemeriksaan digital forensik tidak berdiri sendiri sebagai data teknis semata, melainkan menjadi bagian integral dari sistem pembuktian hukum pidana.[25]

Digital forensik berfungsi untuk menjamin bahwa alat bukti elektronik yang diajukan dalam persidangan memenuhi syarat keaslian (*authenticity*), keutuhan (*integrity*), dan keterandalan (*reliability*). Melalui metode dan prosedur forensik yang terstandar, penyidik dan analis forensik dapat memastikan bahwa data elektronik yang diperiksa benar-benar berasal dari sumber yang relevan, tidak mengalami perubahan sejak pertama kali diperoleh, serta dapat dipertanggungjawabkan secara ilmiah. Aspek ini menjadi krusial mengingat sifat data elektronik yang mudah diubah, disalin, atau dihapus tanpa meninggalkan jejak yang kasatmata.

[25] Siti Nurul Romadiyah, "' Analisis Jenis -Jenis Alat Bukti dan Kekuatan Bukti Digital dalam Pembuktian Acara Perdata " 4, no. 2 (2021).

Optimalisasi digital forensik dalam penanganan tindak pidana siber juga didukung oleh berbagai regulasi internal kepolisian yang mengatur tata cara penanganan barang bukti digital. Regulasi tersebut mencakup prosedur penyitaan perangkat elektronik, pengamanan tempat kejadian perkara digital, proses akuisisi data, hingga penyimpanan dan pemeriksaan barang bukti elektronik. Salah satu prinsip utama yang ditekankan dalam regulasi internal tersebut adalah penerapan chain of custody, yaitu mekanisme pencatatan dan pengawasan terhadap alur penguasaan barang bukti sejak pertama kali diperoleh hingga diajukan di persidangan. Narasumber dalam penelitian ini menegaskan bahwa dokumentasi pada setiap tahapan penanganan alat bukti elektronik merupakan aspek yang tidak dapat diabaikan. Setiap tindakan terhadap barang bukti digital, mulai dari penyitaan, pemindahan, pemeriksaan, hingga penyimpanan, harus dicatat secara rinci dan sistematis. Dokumentasi tersebut berfungsi sebagai jaminan bahwa proses penanganan alat bukti dilakukan sesuai prosedur dan tidak menimbulkan keraguan mengenai keaslian serta keutuhan data. Tanpa dokumentasi yang memadai, hasil pemeriksaan digital forensik berpotensi dipersoalkan keabsahannya dalam proses persidangan. Lebih jauh, narasumber juga menekankan bahwa kegagalan dalam menjaga chain of custody dapat menurunkan nilai pembuktian alat bukti elektronik, meskipun secara teknis data yang diperoleh valid dan relevan. Dalam praktik peradilan, hakim tidak hanya menilai kebenaran materiil dari suatu alat bukti, tetapi juga menilai apakah alat bukti tersebut diperoleh dan dikelola sesuai dengan ketentuan hukum yang berlaku. Apabila terdapat celah dalam penerapan chain of custody, alat bukti elektronik berpotensi dianggap tidak memenuhi syarat formil pembuktian dan dapat dikesampingkan oleh hakim.Dari perspektif yuridis, kondisi tersebut menunjukkan bahwa kekuatan alat bukti elektronik tidak hanya ditentukan oleh kecanggihan teknologi digital forensik yang digunakan, tetapi juga oleh kepatuhan aparat penegak hukum terhadap prosedur hukum yang mengaturnya. Digital forensik yang dilakukan tanpa memperhatikan aspek prosedural justru dapat melemahkan posisi pembuktian, karena membuka ruang bagi pihak terdakwa untuk mempersoalkan keabsahan alat bukti. Oleh karena itu, optimalisasi digital forensik harus dipahami sebagai upaya yang mencakup dimensi teknis dan yuridis secara simultan.

Digital forensik juga berperan penting dalam menjembatani kesenjangan pemahaman antara aspek teknis teknologi informasi dan aspek hukum pembuktian. Hakim sebagai penentu akhir dalam proses peradilan pidana pada umumnya tidak memiliki latar belakang teknis yang mendalam di bidang teknologi informasi. Melalui keterangan ahli yang didasarkan pada hasil pemeriksaan digital forensik, informasi teknis yang kompleks dapat disajikan dalam bahasa hukum yang lebih sederhana dan sistematis, sehingga memudahkan hakim dalam menilai relevansi dan kekuatan pembuktian alat bukti elektronik. Dengan demikian, optimalisasi digital forensik tidak hanya berfungsi untuk memperkuat alat bukti

elektronik secara teknis, tetapi juga untuk memastikan bahwa alat bukti tersebut memiliki legitimasi yuridis yang kuat dalam proses pembuktian. Sinergi antara ketentuan KUHAP, pengaturan khusus dalam Undang-Undang ITE, serta regulasi internal kepolisian menjadi prasyarat penting bagi terwujudnya pembuktian tindak pidana siber yang efektif dan berkeadilan. Oleh karena itu, peningkatan kapasitas aparat penegak hukum di bidang digital forensik, disertai dengan konsistensi penerapan chain of custody, merupakan faktor kunci dalam memperkuat sistem pembuktian tindak pidana siber di Indonesia.

Optimalisasi digital forensik pada hakikatnya tidak hanya berfungsi untuk memperkuat alat bukti elektronik dari sisi teknis, tetapi juga berperan penting dalam memberikan legitimasi yuridis yang lebih kuat dalam proses pembuktian tindak pidana siber. Dari perspektif teknis, digital forensik memastikan bahwa data elektronik yang diperoleh, dianalisis, dan disajikan telah melalui prosedur ilmiah yang terstandar, sehingga memenuhi prinsip keaslian, keutuhan, dan keterandalan. Hal ini menjadi krusial mengingat karakteristik data elektronik yang sangat rentan terhadap perubahan, penghapusan, maupun manipulasi, baik yang dilakukan secara sengaja maupun tidak disengaja. Tanpa dukungan digital forensik yang tepat, alat bukti elektronik berpotensi kehilangan nilai pembuktiannya meskipun secara substansi relevan dengan peristiwa pidana yang terjadi. Selain memperkuat aspek teknis, digital forensik juga memiliki dimensi yuridis yang tidak kalah penting. Melalui hasil pemeriksaan digital forensik, alat bukti elektronik dapat ditempatkan secara tepat dalam sistem pembuktian hukum pidana, khususnya melalui mekanisme keterangan ahli. Keterangan ahli yang didasarkan pada hasil forensik digital memungkinkan data teknis yang kompleks diterjemahkan ke dalam bahasa hukum yang sistematis dan dapat dipahami oleh hakim. Dengan cara ini, digital forensik berfungsi sebagai penghubung antara perkembangan teknologi informasi dan kerangka normatif pembuktian pidana, sehingga alat bukti elektronik tidak hanya dipandang sebagai data teknis semata, melainkan sebagai alat bukti hukum yang memiliki kekuatan pembuktian.

Optimalisasi digital forensik juga tidak dapat dipisahkan dari kepatuhan terhadap prosedur hukum, terutama dalam penerapan prinsip *chain of custody*.[26] Setiap tahapan penanganan alat bukti elektronik, mulai dari penyitaan, pengamanan, pemeriksaan, hingga penyajian di persidangan, harus dilakukan secara cermat dan terdokumentasi dengan baik. Dokumentasi yang berkesinambungan tersebut berfungsi sebagai jaminan yuridis bahwa alat bukti elektronik tetap terjaga keasliannya dan tidak mengalami perubahan selama proses penanganan perkara. Apabila prinsip chain of custody tidak diterapkan secara konsisten, hasil pemeriksaan digital forensik yang secara teknis valid pun berpotensi kehilangan kekuatan pembuktiannya di hadapan hukum. Dalam konteks

[26] Insan Pribadi, "Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana," n.d., 109–24.

penegakan hukum tindak pidana siber, optimalisasi digital forensik menuntut adanya integrasi yang kuat antara regulasi, prosedur, dan kapasitas sumber daya manusia aparat penegak hukum. Regulasi yang mengakui alat bukti elektronik harus diimplementasikan melalui SOP yang jelas dan aplikatif, serta didukung oleh kemampuan teknis penyidik dan analis forensik dalam memahami serta menerapkan metode digital forensik secara tepat. Tanpa integrasi tersebut, digital forensik berisiko hanya menjadi prosedur formal yang tidak memberikan kontribusi optimal terhadap penguatan pembuktian. Oleh karena itu, optimalisasi digital forensik perlu dipahami sebagai upaya strategis yang bersifat komprehensif, mencakup aspek teknis, prosedural, dan yuridis secara simultan. Penerapan digital forensik yang optimal tidak hanya meningkatkan kualitas dan kredibilitas alat bukti elektronik, tetapi juga memperkuat legitimasi hukum pembuktian tindak pidana siber. Dengan pendekatan demikian, digital forensik berperan sebagai instrumen penting dalam mendukung terwujudnya proses peradilan pidana yang efektif, adil, dan berorientasi pada pencarian kebenaran materiil.

Optimalisasi tersebut tidak hanya dimaknai sebagai peningkatan penggunaan perangkat teknologi forensik semata, melainkan sebagai proses penguatan yang terintegrasi antara aspek teknis, prosedural, dan normatif. Optimalisasi menuntut adanya standardisasi metode pemeriksaan, konsistensi penerapan *chain of custody*, peningkatan kapasitas dan kompetensi sumber daya manusia, serta harmonisasi antara ketentuan KUHAP, Undang-Undang ITE, dan regulasi internal kepolisian. Dengan pendekatan yang komprehensif tersebut, alat bukti elektronik tidak hanya mampu memenuhi prinsip keaslian, keutuhan, dan keterandalan secara ilmiah, tetapi juga memperoleh legitimasi yuridis yang kuat dalam proses pembuktian di persidangan. Oleh karena itu, optimalisasi digital forensik merupakan strategi krusial dalam memastikan bahwa perkembangan teknologi informasi tidak melemahkan sistem pembuktian pidana, melainkan justru memperkuat efektivitas dan kredibilitas penegakan hukum tindak pidana siber di Indonesia.

D. Simpulan

Penelitian ini menyimpulkan bahwa Pengaruh modus operandi tindak pidana siber dalam pengumpulan alat bukti elektronik menunjukkan bahwa karakter kejahatan siber yang dinamis, anonim, dan lintas yurisdiksi secara langsung memengaruhi proses pembuktian. Perkembangan pola kejahatan menuntut penyidik memiliki kemampuan teknis yang adaptif dalam mengamankan, mengekstraksi, dan mengelola data elektronik sejak tahap awal penanganan perkara. Kegagalan dalam menjaga prosedur, khususnya pengamanan barang bukti digital dan penerapan chain of custody, berpotensi melemahkan nilai pembuktian meskipun data yang diperoleh secara teknis valid. Oleh karena itu, SOP penyidikan, koordinasi lintas instansi, serta peningkatan kapasitas sumber daya manusia menjadi faktor penting agar proses pengumpulan alat bukti elektronik tetap

memenuhi prinsip legalitas, akuntabilitas, dan due process of law dalam menghadapi kompleksitas modus operandi kejahatan siber Penelitian ini menegaskan bahwa optimalisasi digital forensik dalam memperkuat alat bukti elektronik tidak dapat dipahami sekadar sebagai instrumen teknis, melainkan sebagai bagian integral dari sistem pembuktian pidana. Integrasi antara kerangka hukum, seperti Pasal 235 ayat (1) KUHAP dan ketentuan UU ITE, memberikan legitimasi terhadap penggunaan alat bukti elektronik, namun kekuatan pembuktiannya sangat bergantung pada pelaksanaan digital forensik yang profesional, terstandar, dan konsisten. Melalui proses forensik digital, data elektronik yang kompleks dapat diterjemahkan ke dalam keterangan ahli yang sistematis sehingga membantu hakim membangun keyakinan berdasarkan alat bukti yang sah. Oleh karena itu, penguatan regulasi, pembaruan SOP secara berkala, peningkatan kompetensi penyidik dan analis forensik, serta kolaborasi dengan penyedia layanan digital menjadi prasyarat utama agar digital forensik mampu memperkuat kedudukan alat bukti elektronik dan mendukung penegakan hukum tindak pidana siber secara efektif serta berorientasi pada kebenaran materiil.

Penulis menyarankan agar optimalisasi digital forensik dalam penguatan alat bukti elektronik dilakukan melalui pendekatan yang komprehensif dengan penguatan regulasi dan standar operasional prosedur yang mengatur pengumpulan, pengamanan, analisis, serta penyajian alat bukti elektronik guna menjamin keaslian, keutuhan, dan keterandalan dalam proses pembuktian pidana; selain itu aparat penegak hukum perlu meningkatkan kapasitas teknis melalui pelatihan berkelanjutan, penyediaan perangkat forensik yang memadai, serta kerja sama dengan tenaga ahli agar mampu menghadapi karakter kejahatan siber yang dinamis dan lintas yurisdiksi; integrasi antara kerangka hukum pembuktian dalam KUHAP dan ketentuan UU ITE dengan praktik digital forensik di lapangan juga perlu diperkuat agar pengakuan normatif terhadap alat bukti elektronik diikuti oleh kekuatan pembuktian yang optimal di persidangan

E. Ucapan Terimakasih

Penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada Bapak Indung Widjayanto, S.H. selaku Dosen Pembimbing yang telah meluangkan waktu, tenaga, dan pikiran dalam memberikan arahan, bimbingan, serta masukan yang konstruktif selama proses penyusunan penelitian ini. Ucapan terima kasih juga penulis sampaikan kepada teman-teman yang senantiasa memberikan dukungan, motivasi, serta bantuan dalam berbagai aspek, baik secara akademis maupun moral, sehingga penelitian ini dapat terselesaikan dengan baik. Tak lupa, penulis mengucapkan terima kasih yang tulus kepada keluarga tercinta yang selalu memberikan doa, dukungan, dan kepercayaan penuh, sehingga penulis dapat menyelesaikan penulisan ini dengan sebaik-baiknya.

F. Pernyataan Konflik Kepentingan

Penulis menegaskan bahwa dalam penyusunan artikel ini tidak terdapat konflik kepentingan yang berpotensi memengaruhi hasil penelitian. Seluruh proses penelitian dan penulisan dilakukan secara independen, tanpa keterlibatan kepentingan pribadi, komersial, finansial, maupun profesional yang dapat memengaruhi objektivitas serta integritas ilmiah dari karya ini.

G. Informasi Pendanaan

Penelitian serta penyusunan artikel ini dilaksanakan secara independen dengan pendanaan mandiri oleh penulis.

H. Referensi

Aprilianto, Raihan, Bangun Raharjo, Gorgonius Patrick, Alviano Reamur, Muhammad Darmasyah Faza, Program Kepolisian, dan Akademi Kepolisian. "Implementasi Fungsi Kepolisian Sebagai Pelindung Pengayom Dan Pelayan Masyarakat Dalam Mewujudkan Ketertiban Dan Keamanan Masyarakat" 1, no. 1 (2025): 168–82.

Berlian, Cheny, and Universitas Muhammadiyah Riau. "Dos Attack Sebagai Tindak Pidana Siber Dalam Pengaturan Hukum di Indonesia," n.d.

Bukti, Analisis, Digital Forensik, Pada Aplikasi, Facebook Messenger, Dan Twitter, and Twitter Android. "Jurnal Media Pratama" 18, no. 1 (2024): 15–28.

Dahlan, Ahmad, Norma Sari, and Ahmad Dahlan. "Tantangan Hukum Dan Psikologis Dalam Penegakan Hukum Terhadap Pelecehan Dan Intimidasi Online Di Media Sosial" 5, no. 1 (2025): 16–34.

Ermadi Satriya Wijaya, Frida Tyas Pramesti. "Analisis Bukti Digital Forensik Pada Aplikasi Facebook Messenger Dan Twitter Berbasis Android Menggunakan Proses DFRWS (Studi Kasus: Pencemaran Nama Baik)" 18, no. 1 (2024): 15–28.

Fadilurrahman, M, Tahta Kurniawan, and Syahrial Shaddiq. "Systematic Literature Review of Disruption Era in Indonesia : The Resistance of Industrial Revolution 4 . 0" 2, no. 1 (2021). https://doi.org/10.18196/jrc.2152.

Hukum, Fakultas, and Universitas Tarumanagara. "Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.5. No.7 (2024) Tema/Edisi : Hukum Pidana (Bulan Ketujuh) Https://Jhlg.Rewangrencang.Com/" 5, no. 7 (2024): 1–17.

Ihsan, M. "Hambatan Dalam Menangani Tindak Pidana Penipuan Melalui Media

Sosial (Online) oleh Siber Dit Reskrimsus Polda Sumsel," 2024.

Irawan, Hengki, Zainudin Hasan, Universitas Bandar Lampung, Hengki Irawan, and Zainudin Hasan. "Dampak Teknologi Terhadap Strategi Litigasi Dan Bantuan Hukum : Tren Dan Inovasi Di Era Digital" 4 (2024): 4600–4613.

Khatimah, Husnul, Sonia Winda Khairani, Dimas Ardiansyah, and Fauziah Lubis. "Analisis Hukum Bukti Elektronik Sebagai Alat Bukti Dalam Pemeriksaan Hukum Acara Perdata," n.d., 1–16.

Muhammad Singgih Imam Wibowo, Akhmad Munawar, dan Hidayatullah Universitas. "Kendala Teknis dan Hukum Dalam Proses Penyidikan Tindak Pidana Siber di Indonesia" 5, no. 7 (2024): 1–15.

Mursyid, Airlangga Putera, Miftahul Jannah. "Rekonstruksi Peran Digital Forensik Dalam Penyidikan Tindak Pidana Siber: Analisis Kritis Terhadap Konstruksi Hukum Pidana Di Indonesia" 6, no. 2 (2025).

Najwa, Fadhila Rahman. "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia" 2, no. 1 (2024): 8–16.

Nath, Souradip. "Digital Evidence Chain of Custody : Navigating New Realities of Digital Forensics," 2024, 11–20. https://doi.org/10.1109/TPS-ISA62245.2024.00012.

Nugroho, Agus, and An An. "Research Synthesis of Cybercrime Laws and COVID - 19 in Indonesia : Lessons for Developed and Developing Countries." Security Journal 36, no. 4 (2023): 651–70. https://doi.org/10.1057/s41284-022-00357-y.

Nurfitri Fathonah, Hudi Yusuf. "Pencegahan dan Tantangan dalam Memerangi Tindak Pidana Siber," . September (2025): 6303–12.

Pratiwi, Eka. "Analisis Forensik Digital dalam Mendukung Pengungkapan Tindak Kriminal Modern " 2025, 15097–10.0.

Pribadi, Insan. "Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana," n.d., 109–24.

Priyana, Puti. "Alat Bukti Informasi Elektronik Tindak Pidana Penipuan Online dalam Perspektif Hukum Acara Pidana di Indonesia" 9, no. 1 (2021).

Romadiyah, Siti Nurul. "' Analisis Jenis -Jenis Alat Bukti Dan Kekuatan Bukti Digital Dalam Pembuktian Acara Perdata '" 4, no. 2 (2021).

Safitri, Linda, Universitas Hasyim Tebuireng Jombang. "Etika profesi Polisi Etika Kepolisian" 1, no. 4 (2024): 230–35.

Sunde, Nina, and Itiel E Dror. "Forensic Science International : Digital Investigation A Hierarchy of Expert Performance (HEP) Applied to Digital Forensics : Reliability and Biasability in Digital Forensics Decision Making." *Forensic Science International: Digital Investigation* 37 (2021): 301175. https://doi.org/10.1016/j.fsidi.2021.301175.

Utama, Zain Arfin, Pandam Bayu, dan Seto Aji. "Ristek: Jurnal Riset, Inovasi Dan Teknologi Kabupaten Batang Data Forensik Digital Dalam Penyidikan Kejahatan" 10, no. 1 (2025): 116–23.

Vanessa. "Analisis Keabsahan Bukti Elektronik Dalam Pemeriksaan Persidangan Perkara Pidana Dan Implementasi Admisibilitasnya (Studi Putusan)" 20, no. 4 (2025). https://doi.org/10.21070/ijler.v20i4.1395

"Teka – Teki Kejanggalan Dalam Kasus Pidana Pembunuhan 'Kopi Sianida.'" Accessed October 2, 2024. https://jurnal.kolibi.org/index.php/kultura/article/view/563/544.

Wijaya, Universitas Kusuma Surabaya Fakultas Hukum Program Studi Hukum. "Terhadap Pelanggaran Standar Operasional Pelaksanaan (SOP) dalam Manajemen Penyidikan," 2023.

I. Biografi Penulis

Michael Adi Nugraha adalah seorang mahasiswa Program Studi Ilmu Hukum Universitas Negeri Semarang. Saat ini ia sedang menempuh pendidikan sarjana dengan minat kajian yang berfokus pada bidang hukum pidana, khususnya yang berkaitan dengan penegakan hukum dan isu-isu hukum kontemporer. Selama masa perkuliahan, penulis aktif dalam berbagai kegiatan kemahasiswaan, antara lain tergabung dalam Badan Eksekutif Mahasiswa Keluarga Mahasiswa Universitas Negeri Semarang (BEM KM UNNES) serta Unit Kegiatan Mahasiswa Lex Scientia. Melalui keterlibatan tersebut, penulis mengembangkan kemampuan akademik, organisasi, dan kepemimpinan. Selain itu, penulis juga aktif dalam kegiatan diskusi dan pengembangan keilmuan hukum sebagai bagian dari upaya memperdalam pemahaman teoritis dan praktis di bidang hukum pidana.

"This Page Intentionally Left Blanks"