ISSN: 2338 4638

Volume 8 Nomor 7 (2024)

'ADALAH

Buletin Hukum & Keadilan

Peran Forensik Digital dalam Mengungkap Kejahatan Siber: Tantangan Prosedural dan Kebutuhan Standardisasi di Indonesia

Gilang Rizki Aji Putra*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v8i7.1880

Abstract:

Digital forensics is a multidisciplinary field that integrates information technology and forensic science to identify, secure, extract, and analyze digital evidence for judicial proceedings. This article examines the vital role of digital forensics in uncovering cybercrime in Indonesia, analyzing its legal foundations and identifying procedural and institutional challenges affecting its effectiveness. Using normative legal research with statutory, conceptual, and case study approaches, the study finds that digital forensics serves as a crucial mechanism for transforming volatile digital traces into admissible evidence that satisfies chain of custody requirements. The Electronic Information and Transactions Law (ITE Law) and relevant Supreme Court jurisprudence provide a legal basis for the acceptance of digital evidence. However, implementation faces significant obstacles, including fragmented procedural standards, limited expert personnel, regional disparities in laboratory infrastructure, and the absence of uniform national guidelines. The article concludes that strengthening standardization, certification, and institutional capacity is essential.

Keywords: Digital Forensics, Cybercrime, Chain of Custody, Electronic Information and Transactions Law (ITE Law), Digital Evidence.

* Peneliti pada Pusat Studi Konstitusi dan legislasi Nasional (Poskolegnas), Universitas Islam Negeri Syarif Hidayatullah Jakarta. Email: gilang.rizkiajiputra19@uinjkt.ac.id.

A. PENDAHULUAN

Kejahatan siber merupakan salah satu bentuk kriminalitas yang tumbuh paling pesat di abad ke-21. Keunikannya terletak pada karakteristiknya yang sepenuhnya terjadi di ruang virtual: tidak mengenal batas teritorial, berlangsung dalam kecepatan milidetik, dan meninggalkan jejak yang tidak kasat mata. Mulai dari peretasan, penipuan digital, hingga spionase siber, bukti fisik klasik seperti sidik jari atau bekas darah tidak lagi ditemukan. Sebagai gantinya, tersangka meninggalkan jejak digital berupa log server, metadata, nilai hash, atau potongan kode berbahaya. Dalam konteks inilah forensik digital menjelma sebagai pendekatan investigasi yang tidak dapat diabaikan. Ia adalah jembatan yang menjadikan data biner yang abstrak menjadi fakta hukum yang dapat dipahami dalam persidangan (Casey, 2011).

Indonesia, melalui UU ITE dan perubahannya, telah secara progresif mengakui informasi dan dokumen elektronik sebagai alat bukti yang sah. Namun, pengakuan normatif saja tidak cukup. Bukti digital mudah rusak, berubah, atau dihapus dalam hitungan detik. Tanpa penanganan yang tepat, potensi pembuktian yang dimilikinya lenyap sebelum sempat diajukan ke pengadilan. Di sinilah urgensi forensik digital: ia menyediakan metode ilmiah untuk mengamankan, mengawetkan, dan menganalisis bukti digital tanpa mengubah integritasnya, sekaligus mendokumentasikan setiap

langkah dalam rantai penguasaan (*chain of custody*). Tantangan yang dihadapi Indonesia tidak sederhana. Jumlah penyidik dan analis forensik digital masih sangat minim dibandingkan dengan volume kejahatan siber yang terus naik. Lebih dari itu, standar operasional prosedur (SOP) yang baku dan seragam untuk seluruh institusi penegak hukum belum tersedia, sehingga akurasi dan kredibilitas bukti digital kerap dipertanyakan di persidangan (Santoso, 2023). Rumusan masalah artikel ini adalah: Pertama, apa peran forensik digital dalam membangun bukti yang sah dan meyakinkan dalam pengungkapan kejahatan siber? Kedua, apa kendala utama penerapannya di Indonesia dan bagaimana solusi untuk mengatasinya? Tujuannya untuk menegaskan posisi sentral forensik digital dalam rantai peradilan pidana siber dan merekomendasikan langkah-langkah strategis pengembangannya.

B. FORENSIK DIGITAL SEBAGAI ILMU DAN METODE OTENTIKASI

Forensik digital didefinisikan sebagai penerapan prinsip-prinsip ilmu pengetahuan untuk mengidentifikasi, mengumpulkan, memelihara, menganalisis, dan melaporkan bukti digital dari sumber-sumber elektronik guna kepentingan investigasi dan proses peradilan (Casey, 2011). Berbeda dengan forensik konvensional yang objeknya bersifat fisik dan statis, forensik digital bekerja pada objek yang bersifat volatil, mudah

dimodifikasi, dan bergantung penuh pada perangkat keras maupun lunak. Oleh karena itu, metodologi forensik digital mensyaratkan prinsip-prinsip mendasar yang ketat. Pertama, prinsip integritas: setiap tindakan yang dilakukan terhadap bukti digital tidak boleh mengubah data asli. Kedua, prinsip *auditability*: setiap langkah harus terdokumentasi secara rinci sehingga dapat direplikasi dan diuji oleh pihak lain. Ketiga, prinsip kompetensi: pemeriksaan harus dilakukan oleh personel terlatih dengan menggunakan peralatan yang tepat. Keempat, prinsip chain of custody yang merupakan jantung forensik digital, yaitu rangkaian kronologis yang mendokumentasikan siapa yang mengakses bukti, kapan, di mana, menggunakan apa, dan untuk tujuan apa.

Dalam konteks hukum pidana Indonesia, bukti digital yang dihasilkan dari forensik digital tunduk pada ketentuan Pasal 184 KUHAP dan Pasal 5 UU ITE. Untuk dapat diterima sebagai alat bukti sah, bukti digital harus memenuhi syarat formil dan materiil. Syarat formil berkaitan dengan cara perolehan dan prosedur penanganannya; di sinilah *chain of custody* berfungsi. Syarat materiil berkaitan dengan isi dan relevansinya dengan perkara. Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 menegaskan bahwa penilaian terhadap keabsahan alat bukti elektronik harus dilakukan dengan cermat, termasuk memastikan integritasnya. Dengan demikian, peran forensik digital secara

teoretis adalah untuk mengonversi bukti mentah (*raw evidence*) menjadi bukti yang terautentikasi secara ilmiah dan dapat diandalkan dalam proses pembuktian (Brenner, 2022). Tanpa forensik digital, bukti elektronik hanyalah sekumpulan bit yang tidak memiliki nilai pembuktian karena tidak dapat diverifikasi keasliannya.

C. PERAN MULTIDIMENSI FORENSIK DIGITAL DALAM PENGUNGKAPAN KEJAHATAN SIBER

1. Identifikasi dan Preservasi Jejak Digital yang Cepat Lenyap

Peran pertama dan paling fundamental dari forensik digital adalah menghentikan risiko hilangnya data. Dalam kejahatan siber, pelaku seringkali menggunakan teknik anti-forensik seperti enkripsi, penghapusan log, atau perintah remote wipe. Forensik digital dengan prosedur l*ive forensics* (akuisisi data dari sistem yang sedang berjalan) dan *dead forensics* (akuisisi dari media penyimpanan yang telah dimatikan) mampu mengamankan data sebelum dihancurkan. Misalnya, pada kasus serangan ransomware, analisis forensik terhadap memori volatil (*RAM dump*) seringkali menjadi satu-satunya cara untuk menemukan *decryption key* atau melacak alamat *command and control server* pelaku sebelum terputus (Prasetyo, 2024). Tanpa keahlian ini, penyidik akan tiba di lokasi dan hanya menemukan sistem yang telah mati tanpa jejak.

Di Indonesia, Badan Siber dan Sandi Negara (BSSN) serta Pusat Laboratorium Forensik (*Puslabfor*) Polri kerap mengerahkan tim untuk melakukan incident response yang didalamnya tercakup langkah first responder forensik. Keberadaan mereka menentukan apakah bukti awal dapat diamankan atau tidak. Sayangnya, jangkauan tim ini masih terbatas di pulau Jawa dan kota-kota besar, sementara insiden siber dapat terjadi di seluruh pelosok negeri.

2. Analisis dan Rekonstruksi Peristiwa Pidana

Setelah bukti diamankan, peran forensik digital berlanjut pada analisis. Di sinilah data mentah seperti log file, timestamp, registry entries, dan *network* packet disusun menjadi kronologi kejadian yang runtut. Forensik digital mampu merekonstruksi perbuatan pelaku: kapan ia pertama kali masuk ke sistem, file apa yang diakses, apa yang diubah, dan ke mana data dikirim. Kemampuan rekonstruksi ini sangat krusial untuk membangun actus reus dan mens rea, serta untuk membantah alibi.

Sebagai contoh, dalam kasus penipuan digital berkedok investasi, analisis forensik terhadap server platform investasi bodong dapat mengungkap bahwa grafik keuntungan yang tampil di layar korban hanyalah simulasi yang dikendalikan oleh admin, bukan data pasar riil. Temuan ini menjadi dasar untuk mengubah konstruksi hukum dari

wanprestasi perdata menjadi penipuan pidana. Forensik digital juga dapat melacak aliran dana digital melalui analisis blockchain pada kasus yang melibatkan mata uang kripto, yang sebelumnya dianggap mustahil dilacak oleh aparat konvensional (Kusumawardhani, 2024).

3. Mendukung Proses Pembuktian di Persidangan

Peran ketiga adalah menjembatani dunia teknis dengan dunia hukum. Analis forensik digital bertindak sebagai saksi ahli yang menjelaskan kepada hakim dan jaksa tentang temuan teknis dengan bahasa yang dapat dipahami. Mereka menerjemahkan hash value, IP address, dan malware signature menjadi fakta hukum. Kredibilitas seorang ahli forensik digital seringkali menentukan diterima atau ditolaknya bukti digital. Dalam perkara peretasan situs pemerintah oleh kelompok "Bjorka", hasil forensik dari BSSN menjadi bukti kunci untuk mengidentifikasi jenis serangan dan celah keamanan yang dieksploitasi, meskipun identitas pelaku tetap sulit terungkap karena penggunaan teknik anonimisasi berlapis (BSSN, 2023).

UU ITE Pasal 44 menegaskan bahwa alat bukti penyidikan, penuntutan, dan pemeriksaan di persidangan meliputi informasi elektronik dan/atau dokumen elektronik. Forensik digital memberikan jaminan bahwa bukti yang diajukan benar-benar telah melalui prosedur ilmiah, sehingga memenuhi syarat "keadaan yang diketahui oleh hakim" dan

bukan sekadar asumsi. Putusan Mahkamah Agung Nomor 661 K/Pid.Sus/2019 menekankan pentingnya analisis forensik untuk mengonfirmasi keaslian alat bukti digital, dan tanpa itu, bukti tersebut hanya bernilai sebagai petunjuk belaka.

D. FORENSIK DIGITAL DALAM PRAKTIK DI INDONESIA

Pengungkapan Serangan Ransomware terhadap Pusat Data Nasional (2024)

Pada Juni 2024, Pusat Data Nasional Sementara (PDNS) mengalami serangan ransomware yang melumpuhkan berbagai layanan publik. Tim forensik digital dari BSSN, Polri, dan TNI dikerahkan untuk melakukan investigasi. Langkah pertama yang diambil adalah mengisolasi sistem yang terinfeksi untuk mencegah penyebaran, kemudian melakukan imaging forensik terhadap server yang terkena dampak. Analisis forensik mengidentifikasi bahwa *ransomware* yang digunakan adalah varian Brain Cipher, yang diduga terkait dengan kelompok peretas asing. Tim forensik mampu mengekstrak sampel malware, menganalisis command and control infrastructure-nya, serta melacak jejak komunikasi ke beberapa alamat IP di luar negeri. Meskipun pelaku belum tertangkap, laporan forensik ini menjadi dasar bagi pemerintah untuk mengambil langkah diplomatik dan memperkuat keamanan siber nasional. Kasus ini menunjukkan bahwa forensik digital tidak hanya berfungsi represif, tetapi juga preventif-strategis

dalam memberikan informasi intelijen untuk pertahanan negara (Nugroho, 2024).

Investigasi Kebocoran Data Pengguna E-commerce (2022)

Pada tahun 2022, sebuah *platform e-commerce* besar mengalami dugaan kebocoran data jutaan pengguna. Forensik digital berperan penting dalam menginvestigasi apakah kebocoran benar terjadi, dari celah mana data keluar, dan siapa yang mengaksesnya. Tim forensik melakukan analisis terhadap log server, database access records, dan firewall logs. Hasilnya, diketahui bahwa terjadi akses tidak sah melalui *Application Programming Interface* (API) yang tidak diamankan dengan baik. Forensik digital juga mampu mengidentifikasi digital fingerprints pelaku berupa alamat IP dan tools yang digunakan untuk mengeksfiltrasi data. Temuan ini memperkuat laporan ke kepolisian dan menjadi dasar bagi pengenaan sanksi administratif terhadap perusahaan oleh Kominfo karena kelalaian menjaga data pribadi. Kasus ini menegaskan peran forensik digital dalam menegakkan akuntabilitas, tidak hanya kepada individu pelaku, tetapi juga kepada korporasi (Wibisono, 2023).

Kegagalan Forensik karena *Chain of Custody* yang Terputus

Sebagai antitesis, sebuah kasus penipuan daring yang ditangani oleh kepolisian daerah

berujung pada pembebasan terdakwa karena bukti digital tidak diterima pengadilan. Penyidik setempat menyita laptop tersangka dan membukanya sendiri tanpa kehadiran saksi atau perekaman forensik. Mereka kemudian menemukan bukti percakapan WhatsApp yang memberatkan dan mencetaknya. Di persidangan, penasihat hukum berhasil meyakinkan hakim bahwa bukti percakapan tersebut tidak dapat dijamin keasliannya karena *chain of custody* telah terputus; siapa pun bisa saja menyunting isi percakapan sebelum dicetak. Hakim menyatakan bukti tersebut tidak memenuhi syarat formil sebagai alat bukti digital yang sah. Kasus ini menjadi pelajaran mahal bahwa forensik digital bukan sekadar mengkopi data, melainkan serangkaian prosedur ketat yang harus dipenuhi, dan kegagalan sekecil apa pun dapat menghancurkan seluruh kasus (Santoso, 2023).

E. TANTANGAN FUNDAMENTAL DAN UPAYA PENGUATAN FORENSIK DIGITAL DI INDONESIA

Berdasarkan analisis dan studi kasus, terdapat beberapa tantangan fundamental. Pertama, fragmentasi dan ketiadaan standardisasi. Saat ini, Polri memiliki Puslabfor, BSSN memiliki Tim *Computer Security Incident Response Team* (CSIRT), Kominfo memiliki pengawas, dan lembaga lain kadang memiliki unit forensik sendiri-sendiri. Masing-masing memiliki SOP internal yang belum tentu selaras. Ketiadaan pedoman nasional yang seragam tentang tahapan akuisisi, analisis, dan

pelaporan forensik digital mengakibatkan disparitas kualitas dan kredibilitas bukti. Satu laporan forensik dari Polri bisa dinilai sempurna, sementara laporan dari konsultan swasta yang menggunakan metode berbeda bisa dianggap cacat. Ini menciptakan ketidakpastian hukum.

Kedua, krisis sumber daya manusia. Jumlah examiner forensik digital yang bersertifikasi internasional (seperti *Certified Forensic Computer Examiner* atau *Certified Ethical Hacker*) di Indonesia masih sangat kurang untuk melayani ribuan kasus siber per tahun. Banyak penyidik yang mendapat pelatihan dasar, namun tidak memiliki pengalaman dan pendampingan berkelanjutan. Akibatnya, kualitas investigasi forensik di daerah tertinggal jauh dari pusat.

Ketiga, infrastruktur yang timpang. Laboratorium forensik digital yang ideal harus memiliki perangkat *write blocker*, perangkat lunak forensik berlisensi (seperti EnCase, FTK, atau Cellebrite), serta clean room untuk mencegah kontaminasi data. Alat-alat ini mahal dan hanya tersedia di institusi tertentu. Keempat, perkembangan teknologi yang selalu selangkah lebih maju. Enkripsi *end-to-end*, *cloud computing*, *Internet of Things* (IoT), dan *artificial intelligence* adalah medan baru yang belum sepenuhnya dikuasai oleh para pemeriksa forensik. Diperlukan riset dan pengembangan berkelanjutan agar forensik digital tidak kedaluwarsa.

Untuk mengatasi tantangan-tantangan itu, langkah strategis harus segera diambil. Pertama, pemerintah bersama lembaga penegak hukum perlu menerbitkan Standar Nasional Indonesia (SNI) atau Peraturan Bersama tentang Pedoman Umum Forensik Digital. Pedoman ini harus mencakup seluruh fase: persiapan, akuisisi, preservasi, analisis, dan pelaporan, dengan mengacu pada standar internasional seperti ISO/IEC 27037. Kedua, perlu dibentuk Indonesia Digital Forensics Center of Excellence yang bertugas melakukan riset, pelatihan, dan sertifikasi berkelanjutan bagi para pemeriksa forensik dari seluruh institusi. Ketiga, pembangunan laboratorium forensik digital yang memadai harus diprioritaskan tidak hanya di ibu kota, tetapi di setiap ibu kota provinsi. Keempat, revisi KUHAP harus segera mengadopsi ketentuan tentang bukti elektronik secara lebih komprehensif dan menegaskan kedudukan forensik digital sebagai prosedur baku dalam penanganan bukti elektronik.

F. KESIMPULAN

Peran forensik digital dalam mengungkap kejahatan siber adalah mutlak dan tidak tergantikan. Ia berfungsi sebagai tulang punggung yang mengonversi data digital yang abstrak menjadi alat bukti yang konkret, ilmiah, dan kredibel di persidangan. Melalui kemampuannya dalam mengidentifikasi, mengawetkan, menganalisis, dan mempresentasikan bukti, forensik digital menjadi instrumen utama untuk membangun kebenaran

materiil di dunia maya. Menjawab rumusan masalah, peran ini mencakup menjadi penjaga integritas bukti, penyusun rekonstruksi peristiwa kejahatan, dan penyedia dasar bagi keyakinan hakim. Namun, efektivitasnya di Indonesia masih dibelenggu oleh ketidakseragaman standar, minimnya personel ahli, dan keterbatasan infrastruktur.

Rekomendasi yang diajukan adalah: pertama, segera menerbitkan pedoman nasional forensik digital yang terstandarisasi dan mengikat seluruh institusi penegak hukum; kedua, mengintensifkan program pendidikan dan sertifikasi forensik digital bagi penyidik, jaksa, dan hakim melalui kerjasama dengan perguruan tinggi dan lembaga internasional; ketiga, membangun laboratorium forensik digital terakreditasi di setiap Polda dan Kejaksaan Tinggi; dan keempat, merevisi KUHAP secara komprehensif agar kerangka hukum acara pidana tanggap terhadap era digital. Hanya dengan profesionalisme forensik digital yang kokoh, keadilan di ruang siber dapat ditegakkan tanpa keraguan.

REFERENSI:

Brenner, S. W. (2022). Cybercrime: Criminal Threats from Cyberspace (2nd ed.). Praeger.

BSSN. (2023). Lanskap Keamanan Siber Indonesia 2023. Jakarta: Badan Siber dan Sandi Negara.

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.

Kusumawardhani, A. (2024). Rekonsepsi Chain of Custody dalam Bukti Digital di Indonesia. Jurnal Hukum Siber, 6(1), 15–32.

Nugroho, A. (2024). Serangan Ransomware terhadap Infrastruktur Publik: Pembelajaran dari Kasus PDNS. Jurnal Ketahanan Informasi, 5(2), 88–105.

Prasetyo, B. (2024). Analisis Forensik Digital dalam Pembuktian Tindak Pidana Siber. Jurnal Hukum dan Masyarakat, 16(1), 88–107.

Putusan Mahkamah Agung Nomor 661 K/Pid.Sus/2019.

Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016.

Santoso, L. (2023). Chain of Custody Bukti Digital dalam Sistem Peradilan Pidana Indonesia. Jurnal Yudisial, 16(3), 301–322. https://doi.org/10.29123/jy.v16i3.542

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).

Wibisono, A. (2023). Kebocoran Data dan Tanggung Jawab Korporasi Digital. Jurnal Pelindungan Data Pribadi, 2(2), 101–118.