IMPLEMENTASI DIGITAL FORENSICS DALAM PEMBUKTIAN TINDAK PIDANA *CYBER CRIME* DI PENGADILAN NEGERI MEDAN

Irvan Saputra[1], Andi Maysarah[2]

Hukum, Fakultas Hukum, Universitas Dharmawangsa,Medan, Indonesia

Email: andimaysarah@dharmawangsa.ac.id

ABSTRAK – Perkembangan teknologi informasi yang pesat telah melahirkan fenomena kejahatan siber *(cyber crime)* yang memerlukan pendekatan khusus dalam sistem pembuktian hukum pidana. Penelitian ini bertujuan untuk menganalisis implementasi digital forensics dalam pembuktian tindak pidana *cyber crime* di Pengadilan Negeri Medan. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan studi kasus. Data dikumpulkan melalui studi kepustakaan dan analisis putusan pengadilan. Hasil penelitian menunjukkan bahwa digital forensics memainkan peran krusial dalam pembuktian *cyber crime* melalui tahapan identifikasi, preservasi, analisis, dan pelaporan bukti elektronik. Pengadilan Negeri Medan telah mengakui keabsahan alat bukti elektronik sebagaimana diatur dalam UU ITE, namun masih menghadapi tantangan dalam hal kompetensi aparat penegak hukum, standarisasi prosedur, dan integritas *chain of custody*. Penelitian ini menyimpulkan bahwa implementasi digital forensics di Pengadilan Negeri Medan telah sejalan dengan ketentuan hukum positif Indonesia, meskipun masih diperlukan peningkatan kapasitas sumber daya manusia dan infrastruktur laboratorium forensik digital.

Kata Kunci : Digital Forensics, *Cyber Crime*, Alat Bukti Elektronik, Pembuktian, Pengadilan Negeri Medan

ABSTRACT *- The rapid development of information technology has given rise to the phenomenon of cyber crime, which requires a specific approach in the criminal law evidence system. This research aims to analyze the implementation of digital forensics in proving cyber crime offenses at the Medan District Court. The research method employed is normative juridical with a case study approach. Data was collected through literature study and analysis of court decisions. The research findings indicate that digital forensics plays a crucial role in proving cyber crime through the stages of identification, preservation, analysis, and reporting of electronic evidence. The Medan District Court has recognized the validity of electronic evidence as regulated in the ITE Law, but still faces challenges regarding law enforcement personnel competence, procedural standardization, and chain of custody integrity. This research concludes that the implementation of digital forensics at the Medan District Court has been in accordance with Indonesian positive law provisions, although improvement in human resource capacity and digital forensic laboratory infrastructure is still required.*

Keyword : *Digital Forensics, Cyber Crime, Electronic Evidence, Evidence, Medan District Court*

PENDAHULUAN

Revolusi teknologi informasi dan komunikasi telah mengubah lanskap kehidupan masyarakat secara fundamental. Kemudahan akses internet dan perangkat digital memberikan manfaat signifikan dalam berbagai aspek kehidupan, namun di sisi lain melahirkan fenomena

kejahatan baru yang dikenal sebagai *cyber crime* atau kejahatan siber(Gultom, 2005). Kejahatan siber merupakan perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer dan jaringan internet sebagai alat atau sasaran kejahatan(Suhariyanto, 2012).

Indonesia sebagai negara dengan jumlah pengguna internet terbesar di Asia Tenggara menghadapi tantangan serius dalam menangani kejahatan siber. Data menunjukkan peningkatan kasus *cyber crime* yang signifikan, mulai dari penipuan online (*phishing*), peretasan (*hacking*), pencemaran nama baik di media sosial, penyebaran konten ilegal, hingga ujaran kebencian (*hate speech*) berbasis Suku, Agama, Ras, dan Antar Golongan (SARA)(Permatasari, 2018).

Karakteristik khusus kejahatan siber yang bersifat *borderless*, *anonymous*, dan meninggalkan jejak digital yang mudah dihapus atau dimanipulasi, menuntut pendekatan pembuktian yang berbeda dengan tindak pidana konvensional(Hermansyah, 2014). Dalam konteks inilah, digital forensics menjadi instrumen vital dalam mengungkap, mengumpulkan, dan menganalisis bukti elektronik untuk kepentingan proses peradilan(Salsabila, 2024).

Digital forensics atau forensik digital adalah cabang ilmu forensik yang menitikberatkan pada identifikasi, pengumpulan, pemrosesan, analisis, dan pelaporan data yang tersimpan secara elektronik dengan tujuan untuk menemukan fakta-fakta dalam investigasi kejahatan atau perkara hukum(Interpol.int, n.d.). Keberadaan ilmu digital forensics menjadi jembatan antara bukti elektronik yang bersifat volatil dan kompleks dengan sistem pembuktian hukum pidana yang memerlukan tingkat kepastian mendekati seratus persen (*beyond reasonable doubt*) untuk memenuhi kebenaran materiil(Miller, 2005).

Dalam sistem hukum Indonesia, Kitab Undang-Undang Hukum Acara Pidana (KUHAP) telah mengatur alat bukti yang sah sebagaimana tercantum dalam Pasal 184 ayat (1), yaitu: keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Namun, ketentuan KUHAP yang disusun pada tahun 1981 belum mengakomodasi perkembangan teknologi digital yang berkembang pesat setelahnya. Untuk mengisi kekosongan hukum tersebut, diundangkanlah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 (UU ITE), yang secara eksplisit mengakui informasi elektronik dan/atau dokumen elektronik sebagai alat bukti yang sah.

Pasal 5 ayat (1) UU ITE menyatakan bahwa “Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah”. Ketentuan ini diperjelas dalam ayat (2) yang menyatakan bahwa alat bukti elektronik merupakan perluasan

alat bukti yang sesuai dengan hukum acara yang berlaku di Indonesia(Medan, n.d.). Dengan demikian, alat bukti elektronik memiliki kedudukan yang setara dengan alat bukti konvensional dalam proses pembuktian di pengadilan.

Pengadilan Negeri Medan sebagai salah satu pengadilan negeri besar di Indonesia yang memiliki wilayah hukum meliputi 21 kecamatan dengan luas kurang lebih 26.510 km² di Provinsi Sumatera Utara, telah menangani berbagai kasus cyber crime dengan menggunakan alat bukti elektronik. Salah satu kasus landmark adalah Putusan Pengadilan Negeri Medan Nomor 3168/Pid.Sus/2018/PN.Mdn tertanggal 23 Mei 2019 terkait tindak pidana ujaran kebencian yang menggunakan bukti digital berupa *screenshot* Facebook sebagai alat bukti utama.

Implementasi digital forensics dalam pembuktian tindak pidana *cyber crime* di Pengadilan Negeri Medan menarik untuk dikaji mengingat masih adanya berbagai tantangan dalam praktik, antara lain: keterbatasan kompetensi aparat penegak hukum dalam memahami teknologi digital, minimnya laboratorium forensik digital yang memadai, belum terstandarnya prosedur pengumpulan dan analisis bukti elektronik, serta persoalan autentikasi dan integritas alat bukti elektronik yang rentan manipulasi(I Made Dwi Krisnanda, 2021).

Berdasarkan latar belakang tersebut, penelitian ini difokuskan pada analisis implementasi digital forensics dalam pembuktian tindak pidana *cyber crime* di Pengadilan Negeri Medan, dengan rumusan masalah:

1 Bagaimana implementasi digital forensics dalam pembuktian tindak pidana *cyber crime* di Pengadilan Negeri Medan?
2 Apa saja kendala yang dihadapi dalam penerapan digital forensics sebagai alat bukti di Pengadilann Negeri Medan?
3 Seberapa jauh kesiapan aparat penegak hukum dalam menerapkan digital forensics dalam pembuktian *cyber crime*?

KAJIAN TEORI

1 Teori Pembuktian Hukum Pidana

Pembuktian merupakan tahapan paling krusial dalam proses peradilan pidana karena menentukan apakah seseorang dapat dipidana atau tidak(Hiariej, 2012). Sistem pembuktian yang dianut dalam hukum acara pidana Indonesia adalah sistem pembuktian negatif menurut undang-undang (*negatief wettelijk bewijstheorie*), sebagaimana diatur dalam Pasal 183 KUHAP yang menyatakan bahwa hakim tidak boleh menjatuhkan pidana kepada seseorang

kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya(Harahap, 2009).

Menurut M. Yahya Harahap, sistem pembuktian negatif menurut undang-undang menggabungkan dua unsur, yaitu:

a. Pembuktian harus dilakukan menurut cara dan dengan alat-alat bukti yang sah menurut undang-undang; dan
b. Keyakinan hakim yang didasarkan pada cara dan alat bukti yang sah tersebut.

Sistem ini bertujuan untuk menegakkan kebenaran materiil (*materiil waarheid*), bukan sekadar kebenaran formal, sehingga hakim memiliki kebebasan menilai kekuatan pembuktian sepanjang dilakukan berdasarkan cara yang ditentukan undang-undang.

Dalam perkara pidana, tingkat kepastian pembuktian yang diperlukan adalah *beyond reasonable doubt* atau hingga tidak ada lagi keraguan yang beralasan, yang berbeda dengan perkara perdata yang hanya memerlukan tingkat kepastian *more likely than not* atau lebih dari 50%. Hal ini sejalan dengan asas praduga tak bersalah (*presumption of innocence*) dan prinsip *in dubio pro reo* yang memberikan perlindungan maksimal terhadap hak asasi tersangka/terdakwa.

2 Konsep Digital Forensics

Digital forensics atau forensik digital didefinisikan oleh International *Organization on Computer Evidence* (IOCE) sebagai ilmu yang menggunakan teknik yang teruji dan terbukti untuk mengumpulkan, menganalisis, dan menyajikan bukti digital dalam proses hukum. Menurut Interpol, digital forensics adalah proses identifikasi, preservasi, analisis, dan dokumentasi bukti digital untuk keperluan investigasi kejahatan atau litigasi perdata.

Para ahli memberikan definisi yang beragam namun substansial sama. Agarwal et al. mendefinisikan digital forensics sebagai rangkaian metodologi yang terdiri dari teknik dan prosedur untuk mencari dan mengumpulkan bukti-bukti berbasis entitas maupun piranti digital sebagai alat bukti yang sah di pengadilan(A. Agarwal, 2011). Sementara Kent et al. dari National Institute of Standards and Technology (NIST) menyatakan bahwa digital forensics adalah penerapan ilmu pengetahuan dan teknologi untuk mengidentifikasi, mengumpulkan, menganalisis, dan memeriksa informasi digital sambil mempertahankan integritas informasi dan menjaga rantai pembuktian yang ketat.

Dari berbagai definisi tersebut, dapat disimpulkan bahwa digital forensics memiliki beberapa karakteristik esensial, yaitu:

(1) Bersifat ilmiah dan menggunakan metode yang terstandar;

(2) Bertujuan untuk menemukan kebenaran fakta digital;

(3) Hasil analisisnya dapat dipertanggungjawabkan di pengadilan; dan

(4) Harus menjaga integritas bukti sepanjang proses investigasi.

Terdapat beberapa kerangka kerja (*framework*) dalam digital forensics yang digunakan secara internasional. Salah satu yang paling banyak diadopsi adalah NIST SP 800-86 (Guide to Integrating Forensic Techniques into Incident Response) yang dikembangkan oleh National Institute of Standards and Technology Amerika Serikat. Framework NIST membagi proses digital forensics menjadi empat tahapan utama:

a. ***Collection*** **(Pengumpulan)**

Tahap ini meliputi identifikasi, pelabelan, pencatatan, dan pengumpulan data dari sumber yang relevan dengan mengikuti prosedur yang menjaga integritas data. Pada tahap ini, investigator harus memastikan bahwa bukti digital tidak mengalami perubahan atau kerusakan.

b. ***Examination*** **(Pemeriksaan)**

Tahap pemrosesan data yang dikumpulkan secara forensik dengan menggunakan kombinasi metode otomatis dan manual, untuk menilai dan mengekstrak data yang relevan dengan kebutuhan investigasi, sambil mempertahankan integritas data.

c. ***Analysis*** **(Analisis)**

Tahap menganalisis hasil pemeriksaan dengan menggunakan metode dan teknik yang diakui secara ilmiah untuk mendapatkan informasi yang berguna dan menjawab pertanyaan-pertanyaan yang menjadi dasar pengumpulan dan pemeriksaan.

d. ***Reporting*** **(Pelaporan)**

Tahap pelaporan hasil proses forensik yang mencakup deskripsi tindakan yang dilakukan, penjelasan tentang alat dan prosedur yang dipilih, penentuan tindakan lain yang perlu dilakukan, dan rekomendasi untuk perbaikan kebijakan, prosedur, alat, dan aspek lain dari proses forensik.

Kerangka kerja lain yang juga dikenal adalah model forensik digital yang dikembangkan oleh Baryamureeba dan Tushabe yang meliputi:

(1) Readiness;

(2) Deployment;

(3) Physical Investigation;

(4) Digital Forensics Investigation;

(5) Review; dan

(6) Post Investigation.

3 Alat Bukti Elektronik dalam Hukum Positif Indonesia

Sebelum berlakunya UU ITE, alat bukti yang sah dalam hukum acara pidana Indonesia hanya terbatas pada lima jenis sebagaimana diatur dalam Pasal 184 ayat (1) KUHAP. Keterbatasan ini menimbulkan permasalahan dalam mengakomodasi bukti elektronik yang mulai marak digunakan dalam berbagai kasus pidana.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memberikan landasan hukum bagi penggunaan bukti elektronik. Pasal 5 UU ITE secara tegas menyatakan keabsahan informasi elektronik dan/atau dokumen elektronik sebagai alat bukti hukum yang sah.

Namun, tidak semua informasi elektronik dapat dijadikan alat bukti. Terdapat syarat formil dan materiil yang harus dipenuhi. Syarat formil diatur dalam Pasal 5 ayat (4) yang menyatakan bahwa informasi elektronik tidak berlaku untuk surat yang menurut undang-undang harus dibuat dalam bentuk tertulis dan surat beserta dokumennya yang harus dibuat dalam bentuk akta notariil.

Adapun syarat materiil diatur dalam Pasal 6 UU ITE yang mensyaratkan bahwa informasi elektronik dan/atau dokumen elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan. Selain itu, Pasal 15 dan Pasal 16 UU ITE mengatur tanggung jawab penyelenggara sistem elektronik dalam menjamin integritas dan keamanan data elektronik.

Mahkamah Konstitusi melalui Putusan Nomor 20/PUU-XIV/2016 telah memberikan penafsiran konstitusional terhadap alat bukti elektronik, dengan menegaskan bahwa informasi elektronik dan/atau dokumen elektronik yang diperoleh secara tidak sah tidak dapat dijadikan alat bukti yang sah di pengadilan. Putusan ini memperkuat prinsip bahwa proses pengumpulan bukti elektronik harus mengikuti prosedur hukum yang benar (*due process of law*) dan menghormati hak asasi manusia, khususnya hak atas privasi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis empiris, yaitu pendekatan yang menggabungkan studi hukum normatif dengan penelitian lapangan untuk memahami bagaimana digital forensics diterapkan dalam pembuktian tindak pidana *cyber crime* di

Pengadilan Negeri Medan. Metode ini dipilih untuk memperoleh gambaran yang lebih komprehensif mengenai implementasi penerapan forensik digital dalam sistem peradilan pidana.(Subekti, 2019)

HASIL DAN PEMBAHASAN

A. Implementasi digital forensics dalam pembuktian tindak pidana *cyber crime* di Pengadilan Negeri Medan

Digital forensics merupakan cabang ilmu forensik yang berkaitan dengan identifikasi, pengumpulan, analisis, dan pelaporan bukti digital yang diperoleh dari perangkat elektronik untuk kepentingan penegakan hukum(Hamzah, 2014). Dalam konteks hukum Indonesia, digital forensics memiliki kedudukan penting sebagai alat bukti dalam pembuktian tindak pidana cyber crime sebagaimana diatur dalam 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 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 2019).

Pasal 5 ayat (1) UU ITE menegaskan bahwa "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah." Ketentuan ini memberikan landasan yuridis yang kuat bagi penggunaan bukti digital dalam proses peradilan. Lebih lanjut, Pasal 44 UU ITE mengatur bahwa alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagaimana diatur dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik.

Implementasi digital forensics di Pengadilan Negeri Medan mengikuti prosedur standar yang berlaku dalam sistem peradilan pidana Indonesia. Proses ini dimulai dari tahap penyidikan oleh kepolisian, khususnya melalui unit *Cyber Crime* Polda Sumatera Utara, yang memiliki kewenangan untuk melakukan penanganan kasus-kasus kejahatan siber.(Makarim, 2012)

Dalam praktiknya, penyidik melakukan pengumpulan barang bukti digital melalui proses yang dikenal dengan istilah *"chain of custody"* atau rantai pengamanan barang bukti. Proses ini sangat krusial untuk memastikan integritas bukti digital tetap terjaga dari saat pengumpulan hingga pemeriksaan di persidangan(Gultom, 2015). Tahapan *chain of custody*

meliputi identifikasi, pengumpulan, akuisisi, preservasi, analisis, dan presentasi bukti digital di pengadilan.(Sitompul, 2012)

Di Pengadilan Negeri Medan, bukti digital yang sering diajukan dalam kasus *cyber crime* antara lain meliputi log akses sistem komputer, rekaman komunikasi elektronik seperti email dan pesan instan, tangkapan layar (screenshot) dari media sosial, metadata file, serta data dari server dan perangkat penyimpanan.(Ramli, 2013) Bukti-bukti ini harus melalui proses verifikasi dan validasi oleh ahli digital forensics untuk dapat diterima sebagai alat bukti yang sah.

Hakim dalam memeriksa bukti digital menggunakan prinsip pembuktian sebagaimana diatur dalam KUHAP, namun dengan mempertimbangkan karakteristik khusus bukti elektronik. Menurut Pasal 184 KUHAP, alat bukti yang sah terdiri dari keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa.(Undang-Undang Tentang Hukum Acara Pidana, UU No. 8 Tahun 1981, 1981) Bukti digital dapat masuk dalam kategori "surat" atau didukung oleh "keterangan ahli" yang menjelaskan autentisitas dan relevansi bukti tersebut.

Pengadilan Negeri Medan telah menangani berbagai jenis kasus *cyber crime* yang memerlukan pembuktian melalui digital forensics, di antaranya adalah kasus pencemaran nama baik melalui media sosial sebagaimana diatur dalam Pasal 27 ayat (3) UU ITE, kasus penipuan online yang melanggar Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE, serta kasus penyebaran konten ilegal lainnya.(Maskun, 2013)

Dalam kasus pencemaran nama baik, bukti digital yang digunakan biasanya berupa *screenshot* percakapan, metadata posting media sosial, dan laporan analisis dari ahli digital forensics yang membuktikan bahwa konten tersebut benar-benar diunggah oleh terdakwa.(Widodo, 2013) Untuk kasus penipuan online, bukti yang diajukan mencakup rekaman transaksi elektronik, log komunikasi antara pelaku dan korban, serta data rekening bank yang digunakan dalam transaksi.(Suseno, 2012)

Implementasi digital forensics di Pengadilan Negeri Medan mengacu pada standar internasional dan praktik terbaik dalam forensik digital. Penyidik dan ahli forensik digital menggunakan tools dan software yang telah terstandarisasi untuk memastikan bukti yang dikumpulkan dapat dipertanggungjawabkan secara ilmiah dan hukum.(Suhariyanto, 2013)

Prosedur standar yang diterapkan meliputi dokumentasi lengkap terhadap setiap tahap penanganan bukti, penggunaan metode write-blocking untuk mencegah perubahan data asli, pembuatan hash value untuk verifikasi integritas data, serta penyimpanan bukti dalam kondisi yang aman dan terkontrol. Semua proses ini didokumentasikan dalam berita

acara pemeriksaan yang kemudian menjadi bagian dari berkas perkara yang diajukan ke pengadilan.(Raharjo, 2012)

B. Kendala Yang Dihadapi Dalam Penerapan Digital Forensics Sebagai Alat Bukti Di Pengadilan Negeri Medan

1. Kendala Teknis dan Teknologi

Salah satu kendala utama dalam penerapan digital forensics adalah keterbatasan sarana dan prasarana teknologi yang dimiliki oleh aparat penegak hukum. Perkembangan teknologi informasi yang sangat cepat seringkali tidak diimbangi dengan pembaruan peralatan forensik yang digunakan oleh penyidik(Labib, 2010). Hal ini menyebabkan kesulitan dalam mengakses dan menganalisis bukti digital yang menggunakan teknologi atau enkripsi terbaru.

Kendala teknis lainnya adalah volatilitas data digital yang dapat dengan mudah hilang, berubah, atau rusak jika tidak ditangani dengan prosedur yang tepat(Kurde, 2011). Berbeda dengan bukti fisik konvensional, bukti digital sangat rentan terhadap manipulasi dan kerusakan, baik disengaja maupun tidak disengaja. Misalnya, data dalam *Random Access Memory* (RAM) akan hilang ketika komputer dimatikan, sementara data dalam hard disk dapat dengan mudah dihapus atau dimodifikasi.(Purwoleksono, 2014)

Masalah enkripsi juga menjadi tantangan tersendiri. Banyak pelaku *cyber crime* menggunakan enkripsi tingkat tinggi untuk menyembunyikan jejak digital mereka, sehingga penyidik menghadapi kesulitan dalam mengakses data yang dibutuhkan sebagai bukti.(Brenner, 2010) Teknologi seperti *end-to-end encryption* pada aplikasi komunikasi membuat proses intersepsi dan analisis komunikasi digital menjadi hampir tidak mungkin dilakukan tanpa kerjasama dari penyedia layanan.

2. Kendala Regulasi dan Hukum

Meskipun Indonesia telah memiliki UU ITE yang mengatur tentang bukti elektronik, namun masih terdapat beberapa kekosongan hukum dan ketidakjelasan dalam regulasi yang berkaitan dengan digital forensics.(Mukantardjo, 2015) Misalnya, belum ada regulasi yang secara spesifik dan detail mengatur tentang standar prosedur baku dalam penanganan bukti digital, sertifikasi untuk ahli digital forensics, maupun akreditasi untuk laboratorium forensik digital.(Wardhana, 2015)

Permasalahan yurisdiksi juga menjadi kendala dalam kasus *cyber crime* yang bersifat transnasional. Kejahatan siber seringkali melibatkan pelaku, korban, atau server yang berada

di negara yang berbeda, sehingga menimbulkan kompleksitas dalam hal penerapan hukum dan pengumpulan bukti. Perbedaan sistem hukum dan kurangnya kerjasama internasional yang efektif menyulitkan penyidik dalam mendapatkan bukti digital yang tersimpan di server luar negeri.

Kendala hukum lainnya adalah terkait dengan isu privasi dan perlindungan data pribadi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan batasan-batasan tertentu dalam pengumpulan dan penggunaan data pribadi, yang dapat berbenturan dengan kepentingan penegakan hukum dalam pengumpulan bukti digital.(Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, n.d.) Penyidik harus dapat menyeimbangkan antara kebutuhan investigasi dengan penghormatan terhadap hak privasi individu.

3. Kendala Prosedural dan Administratif

Dalam praktiknya, seringkali terjadi kesalahan prosedural dalam penanganan bukti digital yang dapat mengakibatkan bukti tersebut tidak dapat diterima di pengadilan. Kesalahan yang umum terjadi antara lain adalah tidak dilakukannya dokumentasi yang lengkap terhadap proses pengumpulan bukti, terputusnya *chain of custody*, atau tidak digunakannya metode yang dapat dipertanggungjawabkan secara ilmiah dalam analisis bukti.(Hafrida, 2012)

Koordinasi antar instansi penegak hukum juga menjadi kendala. Penanganan kasus *cyber crime* seringkali melibatkan berbagai instansi seperti kepolisian, kejaksaan, dan lembaga lainnya. Kurangnya koordinasi dan standarisasi prosedur antar instansi dapat menyebabkan inkonsistensi dalam penanganan bukti digital.

Keterbatasan waktu dalam proses penanganan bukti digital juga menjadi masalah. Analisis forensik digital yang komprehensif memerlukan waktu yang tidak sedikit, sementara proses peradilan pidana memiliki batasan waktu yang ketat sebagaimana diatur dalam KUHAP.(Harahap, 2012) Tekanan waktu ini dapat mengakibatkan analisis yang dilakukan tidak optimal atau terburu-buru, sehingga berpotensi menghasilkan kesimpulan yang kurang akurat.

C. Kesiapan Aparat Penegak Hukum Dalam Menerapkan Digital Forensics Dalam Pembuktian *Cyber Crime*

1 Kesiapan Institusional

Dari sisi kelembagaan, Indonesia telah melakukan berbagai upaya untuk meningkatkan kesiapan dalam menangani *cyber crime*. Kepolisian Republik Indonesia telah membentuk unit khusus *cyber crime* di tingkat Mabes Polri maupun di tingkat Polda, termasuk Polda Sumatera Utara yang wilayah hukumnya mencakup Medan. Unit-unit ini dilengkapi dengan laboratorium forensik digital, meskipun dengan tingkat kelengkapan yang masih bervariasi.

Kejaksaan Agung juga telah membentuk Jaksa Agung Muda Bidang Tindak Pidana Khusus yang salah satu fokusnya adalah penanganan *cyber crime*. Di beberapa kejaksaan tinggi dan kejaksaan negeri, telah dibentuk tim khusus yang menangani kasus-kasus teknologi informasi. Namun demikian, infrastruktur dan sumber daya yang tersedia masih belum merata di seluruh Indonesia, dengan konsentrasi yang lebih baik di kota-kota besar.

Mahkamah Agung telah menerbitkan beberapa peraturan dan pedoman terkait pemeriksaan perkara *cyber crime*, termasuk pedoman dalam menilai bukti elektronik. Namun, implementasi di tingkat pengadilan negeri masih menghadapi berbagai tantangan terkait pemahaman dan kapasitas hakim dalam memeriksa kasus-kasus yang melibatkan teknologi tinggi.

2. Kesiapan Sumber Daya Manusia

Peningkatan kapasitas SDM aparat penegak hukum dalam bidang digital forensics telah menjadi prioritas beberapa tahun terakhir. Kepolisian RI secara rutin menyelenggarakan pelatihan digital forensics bagi anggotanya, baik melalui pelatihan internal maupun kerjasama dengan lembaga internasional.(Wibisono, 2016) Beberapa penyidik telah mendapatkan sertifikasi internasional dalam bidang digital forensics seperti *Certified Computer Examiner* (CCE) atau *Certified Forensic Computer Examiner* (CFCE).

Kejaksaan dan peradilan juga telah menyelenggarakan berbagai program pelatihan dan bimbingan teknis terkait penanganan kasus *cyber crime.* Mahkamah Agung bekerjasama dengan berbagai universitas dan lembaga internasional untuk memberikan pelatihan kepada hakim tentang teknologi informasi dan bukti digital.(Waluyo, 2011) Namun, cakupan pelatihan ini masih terbatas dan belum menjangkau seluruh aparat penegak hukum di Indonesia.

Meskipun demikian, masih terdapat kesenjangan yang signifikan antara kebutuhan dan ketersediaan SDM yang kompeten. Jumlah penyidik yang memiliki keahlian khusus dalam digital forensics masih jauh dari ideal jika dibandingkan dengan jumlah kasus *cyber crime* yang terus meningkat setiap tahunnya. Demikian pula dengan jaksa dan hakim yang

memiliki pemahaman mendalam tentang teknologi informasi dan digital forensics masih sangat terbatas.

3. Kesiapan Sarana dan Prasarana

Dari aspek sarana dan prasarana, terdapat perbedaan yang cukup signifikan antara laboratorium forensik digital di tingkat pusat dengan yang ada di daerah. Laboratorium forensik digital Polri di Mabes Polri dilengkapi dengan peralatan yang cukup canggih dan mutakhir, termasuk berbagai tools forensik komersial yang berlisensi. Namun, untuk tingkat Polda, terutama di daerah, masih banyak yang memiliki keterbatasan dalam hal peralatan dan *tools* forensik.

Beberapa kendala dalam hal sarana dan prasarana antara lain adalah tingginya biaya pengadaan dan pemeliharaan tools forensik profesional, keterbatasan anggaran untuk pembaruan teknologi, serta kurangnya dukungan teknis untuk pengoperasian dan maintenance peralatan forensik yang kompleks. Akibatnya, tidak jarang penyidik harus menggunakan tools forensik yang sudah usang atau bahkan menggunakan *software open source* yang kemampuannya terbatas.

Di sisi lain, beberapa instansi penegak hukum telah mulai mengembangkan kerjasama dengan universitas dan lembaga riset untuk pengembangan *tools* forensik digital yang lebih terjangkau dan sesuai dengan kebutuhan lokal. Inisiatif ini diharapkan dapat mengurangi ketergantungan pada produk komersial yang mahal dan meningkatkan kapasitas nasional dalam bidang digital forensics.

4. Kesiapan dari Aspek Kerjasama dan Koordinasi

Penanganan *cyber crime* yang efektif memerlukan kerjasama dan koordinasi yang baik, baik antar instansi dalam negeri maupun dengan pihak internasional. Di tingkat nasional, telah dibentuk berbagai forum koordinasi antar lembaga penegak hukum untuk penanganan *cyber crime*, meskipun efektivitasnya masih perlu ditingkatkan.

Kerjasama internasional juga menjadi aspek penting mengingat sifat *cyber crime* yang sering bersifat lintas negara. Indonesia telah menjadi anggota berbagai organisasi internasional yang fokus pada penanggulangan *cyber crime*, seperti INTERPOL dan ASEAN *Cyber Crime Working Group*.(Atmasasmita, 2006) Melalui kerjasama ini, aparat penegak hukum Indonesia dapat memperoleh bantuan dalam bentuk pertukaran informasi, pelatihan, maupun mutual *legal assistance* dalam penanganan kasus.

Namun, masih terdapat kendala dalam implementasi kerjasama internasional, terutama terkait dengan perbedaan sistem hukum, lamanya proses birokrasi dalam permintaan

bantuan hukum, serta ketiadaan perjanjian kerjasama dengan beberapa negara yang menjadi basis operasi pelaku *cyber crime*. Hal ini menyebabkan banyak kasus *cyber crime* yang sulit diselesaikan karena pelaku atau bukti berada di luar yurisdiksi Indonesia.

Secara keseluruhan, kesiapan aparat penegak hukum Indonesia dalam menerapkan digital forensics untuk pembuktian *cyber crime* dapat dikatakan masih dalam tahap pengembangan. Terdapat kemajuan yang signifikan dalam beberapa tahun terakhir, terutama dalam hal pembentukan unit khusus, peningkatan kapasitas SDM, dan pengadaan sarana prasarana. Namun, masih banyak pekerjaan rumah yang harus diselesaikan untuk mencapai tingkat kesiapan yang ideal.

Beberapa kekuatan yang dimiliki antara lain adalah adanya payung hukum yang cukup memadai melalui UU ITE dan peraturan pelaksanaannya, komitmen institusional untuk meningkatkan kapasitas penanganan *cyber crime*, serta semakin meningkatnya kesadaran akan pentingnya digital forensics dalam penegakan hukum. Di sisi lain, kelemahan yang masih ada adalah keterbatasan SDM yang kompeten, kesenjangan sarana prasarana antara pusat dan daerah, serta kurangnya koordinasi dan standardisasi prosedur.

Untuk meningkatkan kesiapan, diperlukan upaya sistematis dan berkelanjutan dalam beberapa aspek. Pertama, peningkatan kualitas dan kuantitas SDM melalui program pendidikan dan pelatihan yang terstruktur dan berkelanjutan. Kedua, pengadaan dan pembaruan sarana prasarana forensik digital secara merata di seluruh Indonesia. Ketiga, pengembangan standar operasional prosedur yang baku dan terstandarisasi untuk penanganan bukti digital. Keempat, penguatan kerjasama dan koordinasi antar instansi serta dengan pihak internasional.

SIMPULAN

Berdasarkan hasil penelitian dan pembahasan mengenai implementasi digital forensics dalam pembuktian tindak pidana *cyber crime* di Pengadilan Negeri Medan, dapat disimpulkan beberapa hal sebagai berikut:

1. Implementasi digital forensics di Pengadilan Negeri Medan telah berjalan sesuai dengan kerangka hukum positif Indonesia, khususnya UU ITE yang memberikan landasan yuridis bagi penggunaan bukti elektronik. Proses pembuktian mengikuti tahapan standar digital forensics yang meliputi identifikasi, preservasi, analisis, dan pelaporan bukti digital, dengan menerapkan prinsip *chain of custody* untuk menjaga integritas bukti dari tahap penyidikan hingga pemeriksaan di persidangan.

2. Terdapat berbagai kendala signifikan dalam penerapan digital forensics sebagai alat bukti, yang dapat dikategorikan dalam tiga aspek utama:
   a. Kendala teknis-teknologi, berupa keterbatasan sarana prasarana, volatilitas data digital, dan tantangan enkripsi;
   b. Kendala regulasi-hukum, mencakup kekosongan hukum dalam standar prosedur baku, kompleksitas yurisdiksi transnasional, dan ketegangan antara kepentingan penegakan hukum dengan perlindungan privasi; serta
   c. Kendala prosedural-administratif, meliputi kesalahan penanganan bukti, lemahnya koordinasi antar instansi, dan keterbatasan waktu dalam proses peradilan.
3. Kesiapan aparat penegak hukum dalam menerapkan digital forensics masih berada dalam tahap pengembangan. Meskipun telah terdapat kemajuan dalam pembentukan unit khusus *cyber crime*, peningkatan kapasitas SDM melalui pelatihan dan sertifikasi, serta pengadaan laboratorium forensik digital, namun masih terdapat kesenjangan signifikan antara kebutuhan dan ketersediaan sumber daya. Disparitas kemampuan antara aparat di tingkat pusat dan daerah, keterbatasan jumlah personel yang kompeten, serta belum meratanya infrastruktur forensik digital menjadi tantangan yang harus diatasi.

DAFTAR PUSTAKA

A. Agarwal, D. (2011). "Systematic Digital Forensic Investigation Model",. *International Journal of Computer Science and Security*, *5*(1), 118.

Atmasasmita, R. (2006). *Pengantar Hukum Pidana Internasional*. Refika Aditama,.

Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*.

Gultom, D. M. A. M. dan E. (2005). *Cyber Law: Aspek Hukum Teknologi Informasi*. Refika Aditama,.

Gultom, D. M. A. M. dan E. (2015). *Cyber Law: Aspek Hukum Teknologi Informasi*. Refika Aditama.

Hafrida. (2012). "Kebijakan Hukum Pidana Terhadap Penanganan Cyber Crime di Indonesia",. *Jurnal Hukum Respublica*, *12*(1), 112.

Hamzah, A. (2014). *Hukum Acara Pidana Indonesia*. Sinar Grafika.

Harahap, M. Y. (2009). *Pembahasan Permasalahan dan Penerapan KUHAP*. Sinar Grafika.

Harahap, M. Y. (2012). *Pembahasan Permasalahan dan Penerapan KUHAP: Penyidikan dan Penuntutan, Edisi Kedua*. Sinar Grafika.

Hermansyah. (2014). *Hukum Perbankan Nasional Indonesia*. Kencana.

Hiariej, E. O. S. (2012). *Teori & Hukum Pembuktian*. Erlangga.

I Made Dwi Krisnanda, D. (2021). "Analisis Yuridis Bukti Digital dalam Pembuktian Perkara Tindak Pidana Ujaran Kebencian",. *RNLJ*, *3*(2), 100–101.

Interpol.int. (n.d.). *"Digital Forensics."* Retrieved January 10, 2026, from https://www.interpol.int/How-we-work/Innovation/Digital-forensics

Kurde, N. A. (2011). "Telaah Kritis terhadap Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)." *Jurnal Hukum Ius Quia Iustum*, *18*(4), 458.

Labib, A. W. dan M. (2010). *Kejahatan Mayantara (Cybercrime)*. PT Refika Aditama,.

Makarim, E. (2012). *"Penyelesaian Sengketa dalam Teknologi Informasi dan Transaksi Elektronik", dalam Hukum Telematika: Suatu Pengantar*. RajaGrafindo Persada,.

Maskun. (2013). *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Kencana Prenada Media Group,.

Medan, P. N. (n.d.). *"Sejarah Pengadilan",*. Pengadilan Negeri Medan.

Miller, D. W. M. dan C. G. (2005). "On Evidence, Medical and Legal",. *Journal of American Physicians and Surgeons*, *10*(3), 29.

Mukantardjo, R. S. (2015). "Digital Forensik dalam Pembuktian Perkara Cyber Crime." *Jurnal Hukum Dan Pembangunan*, *45*(3), 345.

Permatasari, G. A. M. G. (2018). "Tinjauan Yuridis Mengenai Pengaturan dan Pertanggungjawaban Pidana Terhadap Tindak Pidana Ujaran Kebencian di Media Sosial",. *Journal Ilmu Hukum*, *7*(3), 4.

Purwoleksono, D. E. (2014). *Hukum Pidana*.

Raharjo, A. (2012). *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. PT Citra Aditya Bakti,.

Ramli, A. M. (2013). *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*. Refika Aditama.

Salsabila, D. R. A. dan M. (2024). "Analisis Yuridis Peran Digital Forensik dalam Pembuktian Tindak Pidana di Indonesia",. *Media Hukum Indonesia*, *2*(2), 593.

Sitompul, J. (2012). *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Tatanusa.

Subekti. (2019). *Metodologi Penelitian Hukum*. Prenadamedia Group.

Suhariyanto, B. (2012). *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi dan Pengaturan Celah Hukumnya*. RajaGrafindo Persada,.

Suhariyanto, B. (2013). *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. PT RajaGrafindo Persada.

Suseno, S. (2012). *Yurisdiksi Tindak Pidana Siber*. PT Refika Aditama,.

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, (2019).

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Undang-Undang Tentang Hukum Acara Pidana, UU No. 8 Tahun 1981, (1981).

Waluyo, B. (2011). *Viktimologi: Perlindungan Korban dan Saksi*. Sinar Grafika.

Wardhana, M. (2015). "Penegakan Hukum Terhadap Cybercrime di Indonesia",. *Jurnal Ilmu Hukum Legal Opinion*, *3*(2), 78.

Wibisono, Y. (2016). "Kapasitas Aparat Penegak Hukum dalam Menangani Kasus Cybercrime." *Jurnal Mimbar Hukum, 28*(1), 89.

Widodo. (2013). *Aspek Hukum Pidana Kejahatan Mayantara*. Aswaja Pressindo,.