

Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital

Amsori

Sekolah Tinggi Ilmu Hukum IBLAM
amsori07@iblam.ac.id

Fakhri Awaluddin

Sekolah Tinggi Ilmu Hukum IBLAM
fakhriawaluddin@iblam.ac.id

Momon Mulyana

Sekolah Tinggi Ilmu Hukum IBLAM
momonmulyana@iblam.ac.id

Abstract

Significant transformations in human interaction patterns have occurred thanks to advances in science and technology in the field of communication technology. The era of information technology began with the emergence of computer innovation, which initially came in the form of mainframe computers. Advances in information and communication technology have brought major changes to social interaction and human civilization globally. The use of information technology raises cyber law and cyber crime as important issues. Technological developments have commensurate consequences, with benefits in everyday activities but also negative impacts through online fraud and cybercrime. In handling information technology crime cases, digital forensics has an important role, especially in facing evidentiary challenges. Digital forensics includes the analysis of digital traces and has become an integral part of law enforcement in the digital era. The formation of the Indonesian Digital Forensics Association and the Electronic Transaction Information Law confirms the urgency of digital forensics in law enforcement in Indonesia.

Keywords: *transformation, information technology, cybercrime, digital forensics, digital traces*

Abstrak

Transformasi signifikan dalam pola interaksi manusia terjadi berkat kemajuan ilmu pengetahuan dan teknologi di bidang teknologi komunikasi. Era teknologi informasi dimulai dengan munculnya inovasi komputer, yang pada awalnya hadir dalam bentuk mainframe computer. Kemajuan teknologi informasi dan komunikasi membawa perubahan besar dalam interaksi sosial dan peradaban manusia secara global. Penggunaan teknologi informasi memunculkan hukum siber dan kejahatan siber sebagai isu penting. Perkembangan teknologi memiliki konsekuensi sepadan, dengan manfaat dalam aktivitas sehari-hari tetapi juga dampak negatif melalui penipuan daring dan kejahatan siber. Dalam menangani kasus kejahatan teknologi informasi, forensik digital memiliki peran penting, terutama dalam menghadapi tantangan pembuktian. Forensik digital mencakup analisis jejak digital dan menjadi bagian integral dalam penegakan hukum di era digital. Pembentukan Asosiasi Forensik Digital Indonesia dan Undang-Undang Informasi Transaksi Elektronik mengukuhkan urgensi digital forensik dalam penegakan hukum di Indonesia.

Kata kunci: *transformasi, teknologi informasi, kejahatan siber, forensik digital, jejak digital*

PENDAHULUAN

Transformasi signifikan dalam pola interaksi manusia terjadi berkat kemajuan ilmu pengetahuan dan teknologi di bidang teknologi komunikasi. Hal ini memungkinkan komunikasi tanpa batasan geografis dan waktu, membuka jalan menuju era baru dengan perubahan struktur sosial dan nilai-nilai masyarakat, dari yang lokal dan spesifik menjadi global dan universal, serta mempengaruhi nilai-nilai, norma, moral, dan etika. (Rachmie, 2020)

Era teknologi informasi dimulai seiring dengan munculnya inovasi komputer. Awalnya, komputer hadir dalam bentuk mainframe computer pada dekade 1950-an hingga akhir 1970-an. Produsen utama seperti IBM dan The Seven Dwarfs memainkan peran kunci dalam perkembangan mainframe computer (Tatumpe, 2019).

Kemajuan teknologi informasi dan komunikasi membawa perubahan signifikan dalam interaksi sosial dan peradaban manusia secara global. Proliferasi perangkat elektronik seperti ponsel pintar, otomatisasi layanan publik, surat kabar digital, dan perangkat lunak memudahkan komunikasi dan tugas-



tugas sehari-hari, mengintegrasikan teknologi dalam berbagai aspek kehidupan manusia termasuk transaksi keuangan (Eriani, 2022).

Penggunaan teknologi informasi memunculkan sistem hukum baru yang dikenal sebagai hukum siber. Istilah ini merujuk pada bidang hukum terkait penggunaan teknologi informasi, mencakup aktivitas melalui jaringan komputer dan internet. Kejahatan komputer atau kejahatan siber merupakan pelanggaran hukum pidana yang memengaruhi berbagai kalangan, menuntut respons aktif dari lembaga kepolisian untuk menangani kasus-kasus yang melibatkan wilayah yang sangat luas dan tak terbatas (Agus & Riskawati, 2016).

Perkembangan teknologi memberikan konsekuensi sepadan, tergantung pada cara penggunaannya. Keuntungan termasuk kemudahan dalam aktivitas individu atau kelompok, namun dampak negatif muncul ketika teknologi disalahgunakan untuk kejahatan dunia maya. Peningkatan sistem keamanan menjadi penting dalam menghadapi lonjakan kasus cybercrime, memerlukan upaya aktif dalam mengidentifikasi dan mengatasi modus baru dari para pelaku kejahatan dunia maya (Riskiyadi, 2020).

Penipuan daring merupakan salah satu bentuk tindak kejahatan siber yang melibatkan penyampaian informasi, komunikasi, dan/atau transaksi elektronik. Praktik penipuan melalui media sosial semakin meningkat, menuntut kewaspadaan dan tindakan pencegahan, seiring dengan survei yang mengungkapkan peningkatan kasus kejahatan daring di Indonesia (Mirfandaresky, 2022).

Dalam menangani kasus kejahatan yang melibatkan teknologi informasi, diperlukan penerapan forensik. Forensik adalah proses untuk menyelidiki dan memverifikasi fakta terkait kejadian kriminal dan aspek hukum yang terkait. Analisis forensik memiliki peran kunci, terutama jika bukti akan dibawa ke persidangan. Forensik digital, bagian dari bidang forensik, mencakup identifikasi dan investigasi materi atau data dari perangkat digital (Wahyudi, 2022).

Jejak digital adalah fokus dari upaya penyelidikan dalam forensik digital, memperkuat atau melemahkan bukti fisik dalam suatu kasus. Istilah ini awalnya terkait dengan forensik komputer, namun kini mencakup analisis dari semua perangkat penyimpanan data digital. Praktik forensik digital telah berkembang seiring popularitas komputasi pribadi dan era internet (Aisyah et al., 2022).

Dengan terbentuknya Asosiasi Forensik Digital Indonesia (AFDI) oleh Kementerian Komunikasi dan Informatika pada tanggal 17 November 2015, hal ini menandakan bahwa Digital Forensik menjadi bidang ilmu baru dalam dunia komputer. Maraknya kejahatan di bidang komputer dan peningkatan referensi pengetahuan bagi peneliti muda semakin memperkuat urgensi keberadaan Digital Forensik. Undang-undang Informasi Transaksi Elektronik nomor 11 Tahun 2008 mendorong kebutuhan akan ahli komputer forensik untuk mengamankan barang bukti digital, mengikuti standard operational procedure dalam pengambilan bukti-bukti digital, dan memudahkan pemulihan sistem pasca kerusakan (Rosalina & Herli, 2015).

METODE

Studi ini menggunakan pendekatan kualitatif, berfokus pada metode hukum normatif sebagai kerangka kerja utama (Robbani & Yuliana, 2022). Data yang dikumpulkan bersifat deskriptif, termasuk informasi tertulis dan lisan yang diperoleh melalui wawancara serta observasi terhadap perilaku subjek.

Penelitian ini juga mengadopsi metode hukum normatif, berfokus pada interpretasi hukum yang ada, dasar-dasar hukum, kerangka kerja hukum, dan upaya mencari kesesuaian antara berbagai peraturan, baik pada level yang sama maupun berbeda (Putranto & Harvelian, 2023).

Dalam hal penggunaan literatur, komponen ini menjadi elemen krusial dalam penelitian dan ditempatkan sebagai prioritas utama karena sumber informasi melibatkan buku, publikasi ilmiah, dan literatur lainnya. Pendekatan berbasis regulasi dijalankan untuk mengeksplor semua peraturan dan legislasi yang berhubungan dengan isu hukum yang sedang diteliti, terutama yang terkait dengan Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital (Dames Lewansorna et al., 2022).

Selama proses penelitian, sumber rujukan hukum dibedakan menjadi primer dan sekunder. Sumber primer mencakup semua dokumen formal yang diterbitkan oleh institusi pemerintah terkait dan dokumen lain dengan efek mengikat (Irawan, 2020). Sedangkan, sumber sekunder merujuk pada materi hukum dengan keotentikan yang lebih rendah, namun tetap penting sebagai pelengkap sumber primer

(Irawan, 2020). Teknik kajian literatur diadopsi dalam proses pengumpulan data hukum, dengan pendekatan analisis kualitatif digunakan untuk memprosesnya (Dames Lewansorna et al., 2022).

HASIL DAN PEMBAHASAN

Hasil

Selama kurun waktu tiga tahun terakhir, yakni antara tahun 2013, 2014, dan 2015, terdapat laporan sejumlah kasus *Cyber Crime*. Di antara kasus-kasus tersebut, 12 kasus masih dalam tahap penyidikan oleh Polresta Makassar, sementara 22 kasus lainnya berhasil diselesaikan oleh lembaga tersebut. Lebih dari 90% dari total kasus yang dilaporkan berkaitan dengan pencemaran nama baik. Terjadi peningkatan signifikan dalam jumlah kasus *Cyber Crime* terutama pada tahun 2014, yang sebagian besar merupakan kasus pencemaran nama baik. Pada akhir tahun 2015, juga tercatat kasus kejahatan asusila melalui dunia maya (Agus & Riskawati, 2016).

Secara umum, proses penyidikan terhadap kejahatan *Cyber Crime* mirip dengan proses penyidikan kejahatan konvensional lainnya. Namun, perbedaannya terletak pada proses penangkapan pelaku dan koordinasi dengan pihak-pihak terkait. Penanganan tindak kejahatan *Cyber Crime* terlihat sedikit lebih kompleks dibandingkan dengan kejahatan konvensional. Hal ini dikarenakan diperlukan koordinasi dengan beberapa pihak untuk memastikan apakah tindakan tersebut benar-benar merupakan kejahatan pidana atau tidak. Di sisi lain, menetapkan tersangka dalam kasus kejahatan *Cyber Crime* cenderung lebih mudah daripada kejahatan konvensional. Hal ini dapat dilakukan dengan memeriksa barang bukti seperti nomor handphone atau alamat media sosial yang dimiliki oleh pelaku, yang kemudian dapat mengarahkan penyidik kepada pelaku kejahatan yang sebenarnya (Agus & Riskawati, 2016).

Dalam menghadapi kasus *cybercrime* atau kejahatan yang memanfaatkan media elektronik dan digital, pembuktian menjadi tantangan yang kompleks. Penegak hukum di Indonesia seringkali mengalami kesulitan dalam menuntut pelaku *cybercrime* karena kendala dalam memenuhi persyaratan hukum pidana Indonesia. Namun, walaupun penuntutan terhadap pelaku kejahatan digital merupakan hal yang penting, perluasan bukti menjadi solusi yang diperlukan untuk menegakkan hukum. Pada konteks ini, digital forensik sebagai metode ilmiah memegang peranan kunci dalam proses pembuktian perkara pidana, dan kedudukannya dalam hukum pembuktian di Indonesia adalah salah satu parameter yang signifikan. Digital forensik bukanlah alat bukti langsung (*direct evidence*), melainkan sebuah metode yang diterapkan oleh seorang ahli untuk membantu penegak hukum dalam rangka penegakkan hukum (Tatumpu, 2019).

Menurut Feri Sulianta, forensik memiliki makna "membawa ke pengadilan". Istilah forensik merujuk pada suatu proses ilmiah dalam ilmu pengetahuan yang mencakup pengumpulan, analisis, dan penyajian bukti-bukti terkait kasus hukum dalam persidangan. Dalam penanganan tindak pidana yang melibatkan teknologi informasi, investigasi forensik menjadi tahapan yang penting. Forensik adalah kegiatan kajian ilmiah yang dilakukan oleh ahli sesuai dengan bidang keahliannya untuk mengidentifikasi dan menetapkan fakta-fakta yang terkait dengan perkara pidana serta bukti-bukti pendukungnya. Analisis forensik merupakan upaya penyidik yang memiliki kewenangan untuk meminta ahli forensik melakukan kajian ilmiah sebagai langkah kunci dalam mengungkapkan suatu perkara pidana dalam kejahatan komputer, dengan memanfaatkan keahlian digital forensik yang dimiliki oleh ahli tersebut. Salah satu aspek dari ilmu forensik adalah forensik digital, yang melibatkan penemuan hasil investigasi data yang ditemukan di perangkat digital seperti komputer, ponsel, dan sejenisnya. Berbeda dari forensik pada umumnya, forensik digital atau komputer forensik merupakan kegiatan ilmiah dalam mengumpulkan dan menganalisis data dari berbagai sumber daya komputer atau perangkat digital lainnya, termasuk sistem komputer, jaringan komputer, jalur komunikasi fisik maupun non-fisik, serta media penyimpanan data yang dianggap relevan untuk disajikan dalam persidangan sebagai alat bukti pendukung proses penyelesaian perkara pidana. Hal ini menggambarkan bahwa dua disiplin ilmu, yaitu ilmu komputer dan ilmu hukum, bersatu dalam aplikasi forensik digital (Rachmie, 2020).



Christopher, seorang pakar dalam bidang forensik digital, mengungkapkan bahwa dalam konteks dunia digital dan elektronik, bukti asli tidak dapat dianalisis, karena bukti tersebut harus tetap terjaga. Hal ini merupakan perbedaan mendasar dengan melakukan otopsi pada tubuh korban kejahatan. Para pelaku kejahatan dalam ranah kejahatan komputer seringkali berupaya menghilangkan bukti dan menghindari pertanggungjawaban pidana. Mereka seringkali memiliki kecanggihan untuk melindungi diri dan menghancurkan bukti-bukti tersebut. Oleh karena itu, peran utama seorang ahli forensik digital adalah untuk menjaga tegaknya hukum dengan mengamankan bukti-bukti, merekonstruksi kejadian kejahatan, dan memastikan bahwa bukti yang dikumpulkan tersebut dapat bermanfaat dalam proses persidangan (Eriani, 2022).

Pembahasan

Sistem hukum terkait pembuktian adalah salah satu segmen hukum yang telah ada sejak zaman dahulu. Ini disebabkan oleh naluri manusia dan masyarakat, dalam segala keprimitifannya, yang pada dasarnya mempunyai naluri keadilan. Naluri ini akan tersentuh jika terdapat keputusan pengadilan yang menghukum orang yang tidak bersalah, membebaskan orang yang bersalah, atau memberikan kemenangan pada pihak yang sebenarnya tidak berhak dalam suatu persengketaan. Pembuktian mengenai apakah terdakwa benar-benar melakukan tindak pidana yang dituduhkan merupakan elemen kunci dalam proses hukum pidana. Di sini, hak asasi manusia berada dalam bahaya. Oleh karena itu, tujuan dari hukum acara pidana adalah untuk mencari kebenaran materiil, berbeda dengan hukum acara perdata yang lebih memfokuskan pada kebenaran formal (Tatumpe, 2019).

Keterlibatan digital forensik dalam menunjang pembuktian kejahatan di ranah digital memegang peranan yang sangat signifikan. Hal ini melibatkan analisis terhadap barang bukti elektronik terkait kejahatan komputer (*Computer Crime*) maupun kejahatan terkait komputer (*Computer related crime*). Digital forensik merupakan instrumen penting yang membantu penyidik dalam menjalankan tugas penyelidikan dan penyidikan sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang bersinergi dengan Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Implementasi ilmu digital forensik dalam proses penyidikan membutuhkan pemahaman mendalam terhadap teknologi, selain dari aspek hukum yang menjadi bagian rutin dari proses pengadilan pidana. Saat ini, Rancangan KUHAP juga telah memperluas jenis alat bukti untuk memberikan hakim lebih banyak pertimbangan dalam mengambil keputusan. Hal ini tercermin dalam Pasal 175 Ayat (1) Rancangan KUHP, yang mencakup:

- a) Barang bukti
- b) Surat-Surat
- c) Bukti Elektronik
- d) Keterangan seorang ahli
- e) Keterangan seorang saksi
- f) Keterangan seorang terdakwa
- g) Pengamatan hakim (Eriani, 2022).

Penerapan digital forensik sangat krusial dalam membuktikan kasus kejahatan di ranah digital. Sesuai dengan Pasal 5 ayat (1) Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, informasi elektronik dan/atau dokumen elektronik dan/atau cetaknya diakui sebagai alat bukti hukum yang sah. Seorang pakar digital forensik, Christopher, menjelaskan bahwa dalam konteks membuktikan kasus terkait kejahatan digital dan elektronik, bukti asli tidak akan dianalisis karena keasliannya harus tetap terjaga. Hal ini berbeda dengan proses pemeriksaan mayat korban. Dalam konteks ini, penyidik memiliki wewenang yang diatur oleh Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-undang Hukum Acara Pidana, yaitu dijelaskan pada Pasal 2 ayat (1) sebagai serangkaian tindakan penyidik untuk mencari dan mengumpulkan bukti serta menemukan tersangka. Selama proses ini, penyidikan dilakukan oleh pejabat polisi yang memegang kewenangan sesuai dengan kompetensi yang dimilikinya. Apabila kasus yang ditangani melibatkan kejahatan berbasis teknologi informasi, maka penerapan ilmu teknologi informasi menjadi kunci untuk memahami kasus tersebut. Salah satu aspek yang sangat penting dalam proses penegakan hukum adalah penerapan ilmu digital forensik (Rachmie, 2020).

PENUTUP

Dalam era dimana teknologi informasi dan komunikasi mengalami kemajuan pesat, kasus kejahatan di ranah digital menjadi semakin kompleks dan melibatkan berbagai tantangan. Data dan bukti elektronik berperan kunci dalam membuktikan tindak pidana di dunia maya. Dalam konteks ini, digital forensik, sebagai disiplin ilmu yang mengkaji bukti-bukti elektronik dan digital, memainkan peran penting dalam proses penegakan hukum. Digital forensik bukan hanya alat bukti, melainkan juga metode ilmiah yang digunakan oleh ahli forensik digital untuk membantu penyidik dan pengadilan dalam mengungkap dan membuktikan kasus kejahatan di ranah digital. Dalam lingkup ini, menjaga integritas dan otentisitas bukti digital menjadi sangat penting, terutama ketika pelaku kejahatan berupaya menghapus jejak mereka. Tantangan dalam penegakan hukum terhadap kejahatan di ranah digital termasuk kesulitan dalam memenuhi persyaratan hukum pidana yang berlaku di Indonesia. Meskipun demikian, ekspansi jenis bukti dalam hukum pidana dan peran digital forensik memberikan solusi penting untuk memastikan keadilan dalam proses hukum.

Seiring dengan maraknya kejahatan siber, peningkatan pemahaman tentang digital forensik dan peningkatan kemampuan penyidik dan ahli forensik digital menjadi hal yang sangat penting dalam melindungi masyarakat dari ancaman kejahatan di dunia maya. Dengan terus mengembangkan teknik dan standar investigasi forensik digital, kita dapat memastikan bahwa kasus kejahatan di ranah digital dapat ditangani dengan efisien dan adil. Dengan demikian, pemahaman tentang tantangan dan peran digital forensik dalam penegakan hukum terhadap kejahatan di ranah digital adalah langkah penting dalam menjaga keadilan dan keamanan dalam lingkungan digital yang semakin kompleks ini.

Perluasan Pelatihan Digital Forensik: Diperlukan peningkatan investasi dalam pelatihan dan pengembangan keterampilan digital forensik bagi petugas penegak hukum. Ini akan memungkinkan mereka untuk mengatasi tantangan kompleks kejahatan di ranah digital dengan lebih efektif.

Kolaborasi Multidisipliner yang Kuat: Mendorong kerja sama erat antara ahli forensik digital, ahli hukum, dan ahli teknologi informasi sangat penting. Kolaborasi ini akan memungkinkan analisis forensik yang komprehensif dan mendalam untuk mendukung proses penegakan hukum.

Penyediaan Teknologi Forensik Terkini: Menyediakan perangkat dan perangkat lunak forensik terbaru adalah langkah penting dalam memastikan tim forensik memiliki alat yang diperlukan untuk menghadapi kejahatan di ranah digital yang semakin kompleks dan canggih.

DAFTAR PUSTAKA

- Agus, A. A., & Riskawati. (2016). PENANGANAN KASUS CYBER CRIME DI KOTA MAKASSAR (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar). *Jurnal Supremasi*, 11(1).
- Aisyah, N., Syah Putra, A., Valentino, V., Sriyono Prasetyo, B., & Susanti, D. (2022). Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review. *Jurnal Esensi Infokom*, 6(1), 22.
- Dames Lewansorna, Rina, E., Toule, M., & Sopacua, M. (2022). *Pertanggungjawaban Pidana Aparat Kepolisian Yang Melakukan Kekerasan Terhadap Demontran* (Vol. 2, Issue 1).
- Eriani, W. (2022). *PENGATURAN DIGITAL FORENSIK DALAM PEMBUKTIAN TINDAK PIDANA CYBER CRIME*. Universitas Jambi.
- Irawan, V. (2020). ANALISIS YURIDIS TERHADAP PELANGGARAN HAK CIPTA PERMAINAN VIDEO (VIDEO GAMES) BERUPA PEMBAJAKAN SECARA ONLINE. In *Journal of Intellectual Property* (Vol. 3, Issue 2). www.journal.uji.ac.id/JIPRO
- Mirfandaresky, S. (2022). *DIGITAL FORENSIK DALAM PENYIDIKAN TINDAK PIDANA PENIPUAN ONLINE (Studi Kasus di Wilayah Hukum Kepolisian Resor Ponorogo)*. Universitas Islam Malang.
- Putranto, R. D., & Harvelian, A. (2023). Tanggung Jawab Pelaku Usaha dalam Transaksi Elektronik melalui Situs Internet di Tinjau dari Perspektif Hukum Perlindungan Konsumen. *FOCUS*, 4(1), 36–41. <https://doi.org/10.37010/fcs.v4i1.1153>



- Rachmie, S. (2020). PERANAN ILMU DIGITAL FORENSIK TERHADAP PENYIDIKAN KASUS PERETASAN WEBSITE. *LITIGASI*, 21, 104–127. <https://doi.org/10.23969/litigasi.v21i1.2388>
- Riskiyadi, M. (2020). INVESTIGASI FORENSIK TERHADAP BUKTI DIGITAL DALAM MENGUNGKAP CYBERCRIME. *CyberSecurity Dan Forensik Digital*, 3(2), 12–21.
- Robbani, H., & Yuliana, N. (2022). Analysis of Factors Affecting Learning Difficulties during the Covid 19 Pandemic. *FOCUS*, 3(1), 55–58. <https://doi.org/10.37010/fcs.v3i1.537>
- Rosalina, V., & Herli, D. (2015). PENGEMBANGAN MODEL TAHAPAN DIGITAL FORENSIC UNTUK MENDUKUNG SERANG SEBAGAI KOTA BEBAS CYBERCRIME. *Seminar Nasional Riset Terapan*, 12. <http://ftimes.sourceforge.net/FTimes/in>
- Tatumpe, A. (2019). ANALISIS YURIDIS DIGITAL FORENSIK DALAM PEMBUKTIAN TINDAK PIDANA DI INDONESIA. *Scientia De Lex*, 7(1).
- Wahyudi, R. (2022). *Kekuatan Keterangan Saksi Ahli Digital Forensik Dalam Penyidikan Tindak Pidana Di Wilayah Direktorat Reserse Kriminal Umum Kepolisian Daerah Riau*. Universitas Islam Riau.