PERAHU (Penerangan Hukum)
Jurnal Ilmu Hukum
P-ISSN: 2338-333X | E-ISSN: 2775-1104
Fakultas Hukum Universitas Kapuas Sintang
Volume 12 Nomor 2, September 2024

PERAHU (Penerangan Hukum)
JURNAL ILMU HUKUM
Journal homepage: http://jurnal.unka.ac.id/index.php/Perahu
Journal email: jurnalperahu@unka.ac.id

MENINJAU ILMU DIGITAL FORENSIK TERHADAP BUKTI ELEKTRONIK DALAM TINDAK PIDANA INFORMASI DAN TRANSAKSI ELEKTRONIK

Herdino Fajar Gemilang[1*], Handar Subhandi Bakhtiar[2]

[1*] Herdino Fajar Gemilang; Fakultas Hukum, Universitas Pembangunan Nasional "Veteran" Jakarta, Jalan RS. Fatmawati Raya, Pd. Labu, Kec. Cilandak, Kota Depok, Jawa Barat, Indonesia, Email: herdinofjr@gmail.com
[2] Handar Subhandi Bakhtiar; Fakultas Hukum, Universitas Pembangunan Nasional "Veteran" Jakarta, Jalan RS. Fatmawati Raya, Pd. Labu, Kec. Cilandak, Kota Depok, Jawa Barat, Indonesia, Email: handar_subhandi@yahoo.com

INFO ARTIKEL

Riwayat Artikel
Diterima: 20 November 2023
Direvisi: -
Diterima: 20 November 2023
Diterbitkan: September 2024

Keywords:
Digital Forensics; Legality; Electronic Evidence.

DOI:
https://doi.org/10.51826/perahu.v12i2

Abstract

The focus of this research aims to assess the application of digital forensic science by investigators to support the identification of a case, swiftly and accurately locating evidence, and revealing the reasons and motivations behind the actions taken by the perpetrator. The research method employed in this article is normative legal research, employing a case approach and a conceptual approach method. The Indonesian Code of Criminal Procedure (KUHAP) does not explicitly regulate the admissibility of electronic evidence, which is related to the principle of legality stating that Law No. 11 of 2008 on Information and Electronic Transactions (ITE) in Article 54, paragraph (1) allows electronic data to be used as admissible evidence. The legality of electronic evidence is also addressed in the ITE Law in Chapter III concerning Information, Documents, and Electronic Signatures, as well as the explanations in Article 44 and Article 5 of the ITE Law. Referring to the rules of evidence provided in the KUHAP, there must be a means of examination for electronic evidence to establish its admissibility in court, similar to other forms of evidence, involving both formal and substantive requirements.

PENDAHULUAN

Di era masifnya perkembangan digitalisasi, teknologi informasi menjadi hal yang tidak dapat dipisahkan dari masyarakat. Perkembangan teknologi informasi saat ini telah mempengaruhi dimensi komunikasi serta interaksi antar masyarakat, sehingga tidak memiliki batas ruang (*borderless*) dan waktu (Satria., 2019). Masifnya perkembangan teknologi ini juga didasari oleh tuntutan globalisasi. Hal ini dapat terlihat jelas bagaimana teknologi telah merubah peradaban dalam hal berkomunikasi dan mendapatkan informasi. Namun, sebagai salah satu inovasi yang memudahkan manusia, disatu sisi teknologi telah melahirkan masalah baru serta sekaligus menjadi sarana yang menstimulasi terjadinya perbuatan melawan hukum (Manope, 2017). Mengutip pendapat J.E Sahetapy, ia mengatakan bahwasanya kejahatan itu memiliki keterkaitan erat dengan budaya. Dalam hal ini memiliki makna bahwa semakin modernya suatu budaya, maka pola kejahatan pun menjadi semakin modern (Pribadi, 2018).

Salah satu kejahatan yang lahir akibat masifnya penggunaan teknologi adalah *cyber crime* (Medeline, 2022). Istilah ini dipergunakan untuk kejahatan yang selazimnya melalui jaringan komputer. Tindak pidana cyber crime tidak sesederhana yang diketahui, khususnya dalam proses penegakan hukumnya, mulai dari pengaturannya, hingga pengadilan mana yang berwenang untuk mengadili perkara tersebut. Tindak pidana cyber crime selain diatur dalam KUHP, diatur juga dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, selanjutnya disebut UU ITE (Zuhdy, 2020). Adapun macam-macam *cyber crime* yang berkembang di masyarakat diantaranya: pemalsuan data, penipuan, pencurian data, provokasi, pornografi, perjudian online, pembajakan hak cipta dan lain-lain (Pribadi, 2018).

Di sisi lain, pentingnya digital forensik dalam membuktikan kasus di dunia maya yang memiliki ciri khasnya sendiri dapat diakui. Ini disebabkan oleh karakteristik alami teknologi komputer yang memungkinkan pelaku kejahatan untuk menyembunyikan tindakannya. Oleh karena itu, salah satu langkah untuk mengungkap kejahatan komputer melibatkan pengujian sistem dengan peran seorang penyidik, bukan sebagai pengguna biasa. Kejahatan komputer (cyber crime) menjadi tantangan yang perlu diatasi melalui pendekatan ini (Tri, 2010).

Tanpa mengenal batasan geografis, kegiatan ini dapat dilakukan baik dari dekat maupun dari ribuan kilometer jauhnya dengan hasil yang serupa. Pelaku kejahatan umumnya lebih canggih daripada penegak hukum, dengan cara melindungi diri dan

menghancurkan barang bukti. Oleh karena itu, tugas ahli digital forensik adalah untuk menjaga keamanan barang bukti, merekonstruksi kejahatan, dan memastikan bahwa bukti yang terkumpul dapat digunakan secara efektif di pengadilan. Dalam konteks pengadilan hukum pidana, mencari kebenaran materiil merupakan tujuan utama. Oleh karena itu, proses pembuktian dalam kasus pidana dimulai pada tahap penyelidikan untuk menemukan indikasi kejahatan dan menentukan apakah penyidikan diperlukan. Melalui tindakan penyidik yang mencari barang bukti, pada tahap ini, pembuktian sudah terjadi untuk menetapkan suatu kejadian pidana dan mengidentifikasi tersangka (Prayudi & Afrianto, 2007).

Modernisasi dalam paradigma teknologi menjadi alat yang dipergunakan oleh penegak hukum untuk menjalankan tugasnya. Kemajuan teknologi saat ini telah membantu para aparat penegak hukum dalam menyelesaikan berbagai kasus, khususnya dalam tahap pembuktian (Satria., 2019). Secara yuridis penggunaan bukti elektronik sudah dikenal dalam sistem hukum pidana Indonesia, walaupun masih menjadi hal yang tergolong baru. Salah satu pilar hukum yang menjadi dasar hal tersebut adalah Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, (Undang-Undang, 2016).

Bertalian dengan alat bukti, pada Pasal 5 UU ITE diatur sebagai berikut: (1) Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah; (2) Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia; (3) Informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan (Hartono & Yuliartini, 2020). Sementara itu, apabila kita melihat ketentuan Pasal 1 UU ITE angka 1 menyatakan bahwa informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy, atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang telah diolah, yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya (Hartono & Yuliartini, 2020). Selanjutnya pada angka 4 menyatakan bahwa dokumen elektronik adalah setiap informasi elektronik dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya, yang dapat dilihat ditampilkan dan/atau didengar, melalui komputer atau sistem elektronik, termasuk

tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya (Hartono & Yuliartini, 2020).

Dalam penanganan kasus atau perkara-perkara melalui jaringan internet, khususnya pada proses pembuktian, dalam hal ini peran digital forensik sangat dibutuhkan. Berdasarkan hakikatnya pembuktian merupakan salah satu proses pengungkapan peristiwa melalui penyajian alat-alat bukti menurut hukum. Dalam dunia peradilan, alat bukti elektronik itu penting dan sah sebagaimana merupakan perluasan dari alat bukti dalam Hukum Acara yang berlaku di Indonesia (Asimah, 2020). Oleh karena itu, kasus kejahatan digital, digital forensik menjadi pemeran utama untuk melakukan analisis keabsahan barang bukti digital tersebut.

Namun, jika menelisik lebih dalam secara yuridis Kitab Undang-Undang Hukum Acara Pidana (KUHAP) Indonesia tidak mengatur mengenai bukti elektronik. Meskipun, pada praktik peradilan pidana terdapat beberapa undang-undang khusus serta instrumen hukum yang telah dikeluarkan oleh Mahkamah Agung yang melandasi penggunaan bukti elektronik. Di dalam undang-undang khusus telah ditentukan, bahwa bukti elektronik dapat digunakan untuk pembuktian perkara pidana, baik di tingkat penyidikan, penuntutan maupun penetapan di pengadilan (Ramiyanto, 2017).

Berkaca bahwa hukum acara itu memiliki sifat yang mengingat terhadap pihak yang menggunakannya khususnya bagi hakim, maka pengaturan mengenai alat bukti elektronik yang belum terakomodasi di dalamnya, memungkinkan hakim akan kesulitan dalam penyelesaian perkara apabila para pihak mengajukan alat bukti dokumen-dokumen digital. Oleh karena masalah tersebut peneliti mengangkat rumusan masalah ialah: Bagaimana bentuk legalitas pembuktian forensik digital dalam tindak pidana informasi dan transaksi elektronik dan bagaimana peranan ilmu forensik digital dalam pengungkapan perkara tindak pidana informasi dan transaksi elektronik.

METODE PENELITIAN

Ada beberapa metode yang umumnya dipergunakan dalam suatu penelitian hukum. Melalui metode metode tersebut peneliti akan memperoleh informasi dan jawaban dari permasalahan yang diangkat. Oleh karena itu, untuk menjawab rumusan masalah diatas, peneliti akan menggunakan jenis penelitian hukum normatif (*normative law research*). Dalam

perkembangannya istilah hukum normatif juga dikenal dengan istilah penelitian hukum doktrinal (Sutra, 2022).

Pada hakikatnya penelitian hukum normatif berfokus kepada pengkajian hukum sebagai norma atau kaidah yang hidup dan berlaku di masyarakat. Berkaca dari pandangan Soerjono Soekanto, penelitian hukum normatif merupakan penelitian dengan menggunakan bahan pustaka atau data-data sekunder (Sutra, 2022). Mengutip pendapat Peter Mahmud Marzuki, penelitian normatif merupakan proses guna menemukan aturan hukum.

Penggunaan metode tersebut dalam penelitian ini dilatarbelakangi oleh kesesuain teori dengan metode penelitian yang memang dibutuhkan oleh peneliti. Khususnya yang terdapat dalam Undang-Undang tentang Informasi dan Transaksi Elektronik. Khususnya untuk melihat bagaimana legalitas dari ilmu digital forensik dalam menangani kasus pidana informasi dan transaksi elektronik itu sendiri.

HASIL DAN PEMBAHASAAN

1. Bentuk Legalitas Pembuktian Forensik Digital Dalam Tindak Pidana Informasi dan Transaksi Elektronik

Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang selanjutnya disebut UU ITE memberikan dasar hukum mengenai kekuatan hukum alat bukti elektronik dan syarat formal dan meteriil alat bukti elektronik agar dapat diterima di persidangan. Secara sederhana, Alat Bukti Elektronik ialah Informasi Elektronik dan/atau Dokumen Elektronik yang memenuhi prasyarat formal dan prasyarat materiil yang diatur dalam UU ITE yang digunakan untuk keperluan pembuktian di persidangan (Arifiyadi & Sitompul, 2015).

Asas legalitas berarti menuntut adanya ketentuan peraturan perundang-undangan ditetapkan terlebih dahulu dengan sah. Setelah itu perbuatan yang dilakukan oleh manusia yang terbukti memenuhi unsur-unsur tindak pidana dapat dijatuhi pidana. Dengan demikian dalam asas ini terseimpul bahwa peraturan perundang-undangan tidak dapat diberlakukan surut/mundur (retroaktif), agar hal ini menjadi jaminan kepastian hukum (Kartanegara, 1976).

UU ITE juga menganut asas legalitas (sebagai asas fundamental dalam hukum pidana), yaitu sebagaimana tampak dalam Pasal 54 ayat (1) bahwa undang-undang ini mulai berlaku pada tanggal diundangkannya. Artinya, ketentan pidana yang ada dalam UU ITE akan dilaksanakan setelah diberlakukannya sejak tanggal 21 Aprli 2008 (Widodo, 2013).

Agar Informasi dan Dokumen Elektronik dapat dijadikan alat bukti hukum yang sah, UU ITE mengatur bahwa adanya syarat formal dan syarat materiil yang harus dipenuhi. Syarat formal diatur dalam Pasal 5 ayat (4) UU ITE, yaitu bahwa Informasi atau Dokumen Elektronik bukanlah dokumen atau surat yang menurut perundangundangan harus dalam bentuk tertulis. Sedangkan syarat materiil diatur dalam Pasal 6, Pasal 15, dan Pasal 16 UU ITE, yang pada intinya Informasi dan Dokumen Elektronik harus dapat dijamin keautentikannya, keutuhannya, dan ketersediaannya. Untuk menjamin terpenuhinya persyaratan materiil yang dimaksud, dalam banyak hal dibutuhkan digital forensik (Arifiyadi & Sitompul, 2015).

Sebagai alat bukti dalam perkara pidana, kita perlu merujuk pada ketentuan dalam UU ITE. Hal ini diatur dalam Pasal 5 UU ITE sebagai berikut (Sitompul, 2012) :

1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.
3) Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.
4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:
   a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan
   b. surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Dari ketentuan Ayat Pasal 5 ayat (2) UU ITE dapat diketahui bahwa alat bukti Infomasi dan Dokumen Elektronik bukanlah alat bukti yang lain dan terpisah dengan alat-alat bukti dalam Pasal 184 KUHAP, melainkan sebagai perluasan dari alat bukti yang ada dalam Pasal 184 tersebut. Akan tetapi UU ITE tidak menjelaskan perluasan dari alat bukti yang mana diantara 5 alat bukti dalam Pasal 184 KUHAP tersebut (Chazawi & Ferdian, 2015).

Persyaratan materil alat bukti elektronik diatur dalam pasal 5 ayat (3) UU ITE, yaitu Informasi atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam UU ITE. Lebih lanjut, Sistem Elektronik diatur

dalam Pasal 15 s.d. 16 UU ITE dan dari kedua pasal ini, dapat diperoleh persayratan lebih rinci, yaitu bahwa Sistem Elektronik (Sitompul, 2012):

1. Andal, aman, dan bertanggungjawab.
2. Dapat menampilkan kembali Informasi atau Dokumen Elektronik secara utuh.
3. Dapat melindungi ketersediaan, keutuham, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik.
4. Dilengkapi dengan prosedur atau petunjuk dan dapat beroperasi sesuai prosedur atau petunjuk yang telah ditetapkan tersebut.

Sedangkan persyaratan formil alat bukti elektronik diatur dalam Pasal 5 ayat (4) dan Pasal 43 UU ITE, yaitu (Sitompul, 2012):

1. Informasi atau Dokumen Elektronik tersebut bukanlah:
   a. Surat yang menurut UU harus dbuat dalam bentuk tertulis.
   b. Surat beserta dokumennya yang menurut undang-undang harus dibuat dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta.
2. Penggeledahan atau penyitaan terhadap Sistem Elektronik harus dilakukan atas izin ketua pengadilan negeri setempat.
3. Pengggeledahan atau penyitaan dan tetap menjaga terpeliharanya kepentingan pelayanan umum.

Association of Chief Police Officers (ACPO) memberikan empat prinsip dalam penanganan alat bukti elektronik, yaitu (*Good Practice Guiede for Computer-Based Electronic Evidence*, n.d.):

1. Semua penanganan terhadap alat bukti elektronik (yaitu data yang diperoleh dari komputer atau media penyimpanan, atau alat dan perangkat elektronik lain) yang dilakukan oleh aparat penegak hukum tidak boleh mengakibatkan adanya perubahan atau kerusakan terhadap data agar dapat diterima di pengadilan.
2. Dalam keadaan-keadaan dimana seseorang harus mengakses data original yang terdapat dalam komputer atau media penyimpanan orang yang dimaksud harus memiliki kompetensi untuk melakukannya, dan harus mampu memberikan penjelasan mengenai relevansi tindakannya terhadap data dan akibat dari perbuatannya itu.
3. Bahwa harus ada prosedur dan proses yang jelas yang diterapkan untuk mengumpulkan dan menganalisa alat bukti elektronik. Prosedur yang dimaksud memuat penanganan alat bukti elektronik mulai dari penemuan barang bukti yang

mengandung alat bukti elektronik, pembungkusan barang bukti, pemeriksaan, analisa dan pelaporan.

4. Harus ada pihak atau pejabat yang bertanggungjawab untuk memastikan pelaksanaan kegiatan agar sesuai dengan peraturan perundang-undangan serta keseluruhan proses dan prosedur yang dimaksud.

Hal lain yang perlu diperhatikan dalam pengumpulan barang bukti yang menyimpan alat bukti elektronik ialah bahwa ada begitu banyak jenis alat dan media yang menyimpan informasi. Mengingat ada begitu banyak jenis media penyimpanan informasi dan teknologi, penanganannya pun memiliki karakteristik masing-masing. Secara umum digital forensik dibagi menjadi (Al-Azhar, 2012):

a. Komputer forensik, yaitu forensik yang dilakukan terhadap komputer, laptop, atau hardisk dan media penyimpanan sejenis.
b. Mobile forensik, yaitu forensik yang dilakukan terhadap telepon genggam.
c. Network forensik, yaitu forensik yang dilakukan terhadap jaringan komputer.
d. Audio forensik, yaitu forensik yang dilakukan terhadap suara.
e. Image forensik, yaitu forensik yang dilakukan terhadap gambar.
f. Video forensik, yaitu forensik yang dilakukan terhadap video dan CCTV.

Berdasarkan prinsip ACPO yang telah disebutkan di atas. Prinsip digital forensik terbagi menjadi tiga tahap, yaitu (US Department of Justice, 2004): pengambilan (acquisition), pemeriksaan dan analisa, serta dokumen dan presentasi. Mengenai pengambilan, mengingat sifatnya yang tidak dapat diubah, dirusak, atau dihilangkan apabila tidak ditangani dengan tepat, pengambilan informasi atau dokumen elektronik harus dilakukan dengan menjaga dan melindngi keutuhan atau integritasnya.

2. Peranan Ilmu Forensik Digital Dalam Pengungkapan Perkara Tindak Pidana Informasi dan Transaksi Elektronik

Diperlukan penerapan ilmu digital forensik ini untuk mengungkap fakta atau bukti yang berkaitan dengan kasus agar menjadi terang dan jelasnya suatu tindak pidana didalam persidangan. Dalam melakukan investigasi melalui digital forensik ada berbagai macam aplikasi sebagai analisis bantu yang beredar di pasar internet mulai dari aplikasi yang gratis maupun aplikasi yang berbayar, diantaranya yang terkenal yaitu Encase, Acces Data FTK, Belkasoft, Autopsy dan lain sebagainya untuk dapat melakukan pencarian alat bukti dalam proses penegakan hukum (Sari Rizki, 2018).

Digital forensik merupakan bagian ilmu forensik yang digunakan untuk penyelidikan dan penyidikan dalam investigasi materi (data) yang dan penemuan konten perangkat digital. Para Ahli mengatakan digital forensik adalah suatu 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. Feri Sulianta mengatakan forensik memilki arti "membawa ke pengadilan". Istilah Forensik adalah suatu proses ilmiah dari ilmu pengetahuan dalam mengumpulkan, menganalisa, dan menghadirkan bukti-bukti dalam persidangan terkait adanya suatu kasus hukum (Sari Rizki, 2018).

Digital forensik merupakan salah satu sarana untuk membantu penyidik dalam kewenangannya melakukan penyelidikan dan penyidikan yang diatur dalam Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo Kitab Undang-undang Hukum Acara Pidana (KUHAP). Untuk dapat melakukan penerapan ilmu digital forensik dalam proses penyidikan perlu pemahaman yang lebih dalam mengenai ilmu teknologi selain dari pada ilmu hukum yang biasa diterapkan dalam proses pengadilan pidana. Penerapan ilmu digital forensik dibagi menjadi 4 (empat) yaitu (Raharjo, 2013):

1. Forensik Komputer yaitu penyidikan yang dilakukan terkait dengan data dan/atau aplikasi yang berada pada komputer tersebut yang didalamnya tercatat dalam berbagai berkas log;
2. Forensik Jaringan/Internet yaitu penyidikan yang dilakukan kepada data yang diperoleh berdasarkan pengamatan di jaringan;
3. Forensik Aplikasi yaitu penyidikan yang dilakukan dengan penggunaan aplikasi tertentu. Aplikasi tersebut memiliki fungsi audit karena aplikasi tersebut terdapat fitur untuk meninggalkan jejak suatu perangkat;
4. Forensik Perangkat yaitu penyidikan dengan tujuan untuk mendapatkan serta mengumpulkan data dan jejak kegiatan-kegiatan tertentu dalam suatu perangkat digital.

Untuk terciptanya penerapan ilmu digital forensik yang komprehensif diperlukan 3 (tiga) komponen terangkai yang harus dipenuhi untuk penerapan ilmu yang berkualitas. Ketiga komponen tersebut yaitu (Ruci Meiyanti, 2015):

1. Manusia (People), faktor kualitas manusia yang berpengaruh dalam proses penerapan ilmu digital forensik. Kualitas yang dibutuhkan tidak hanya mampu menggunakan computer namun diperlukan keahlian ilmu pengetahuan khusus dan pengalaman untuk dapat melakukan proses analisa menggunakan ilmu digital forensik;
2. Peralatan (Equipment), perlunya beberapa perangkat/alat untuk menunjang proses identifikasi menggunakan digital forensik untuk mendapatkan petunjuk guna menerangkan suatu perkara;
3. Aturan (Protocol), dalam komponen aturan diperlukan pemahaman secara mendalam dari sisi ilmu hukum dan pengetahuan lain seperti pengetahuan teknologi informasi untuk menunjang penerapan ilmu dapat menjadi berkualitas dan dengan aturan pula dibutuhkan untuk proses menggali, mendapatkan, menganalisis, dan akhirnya menyajikan dalam bentuk laporan yang akurat.

Dalam melakukan proses investigasi kejahatan dalam teknologi informasi dapat dilakukan melalui metodologi forensik yang dibagi menjadi 2 (dua) kegiatan yaitu (Rosalina et al., 2016):

1. Search & Seizure. Investigator harus terjun langsung melakukan identifikasi, analisa bukti-bukti serta dapat melakukan penyitaan terhadap bukti-bukti untuk membantu proses penyidikan lebih lanjut sesuai dengan aturan hukum yang berlaku;
2. Pencarian Informasi dapat dilakukan oleh investigator melalui aktivitas yang tercatat dalam perangkat digital ataupun investigator dapat melakukan penyitaan media penyimpanan data untuk membantu proses penyidikan lebih lanjut.

Digital forensik akan sangat membantu dalam proses pembuktian suatu kasus kejahatan secara digital. Berdasarkan Pasal 5 ayat (1) Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik bahwa Informasi elektronik dan/atau dokumen elektronik dan/atau cetaknya merupakan alat bukti hukum yang sah. Ahli digital forensik, Christopher mengungkapkan dalam proses pembuktian suatu perkara terkait dengan kejahatan digital dan elektronik bukti yang asli tidak dianalisis, karena bukti tersebut harus tetap dijaga keasliannya, hal itu berbeda dengan membedah tubuh korban (Kumala, n.d.).

Pada pelaksanaannya penyidikan dilakukan oleh pejabat polisi yang diberikan kewenangan oleh Undang-undang untuk melakukan penyidikan sesuai dengan kompetensi yang penyidik miliki. Apabila kasus yang ditangani oleh penyidik tersebut merupakan

kejahatan yang menggunakan teknologi informasi maka proses penyelidikan dan penyidikan memerlukan penerapan ilmu teknologi informasi untuk dapat menerangkan suatu perkara tersebut, salah satunya menggunakan penerapan ilmu digital forensik sangat penting bagi proses penegakan hukum.

KESIMPULAN

Pengaturan (legalitas) alat bukti elektronik secara sah telah di perjelas di dalam BAB III tentang Informasi, Dokumen, dan Tanda Tangan Elektronik dalam Pasal 5, Pasal 6, dan melalui penegasan kembali di dalam Pasal 44 Undang-Undang Nomor 28 Tahun 2011 tentang Informasi dan Transaksi Elektronik. Alat bukti elektronik ini sangat dibutuhkan dalam Sistem Peradilan Pidana guna untuk menjatuhkan putusan bagi terdakwa yang di sidangkan dalam kasus kejahatan Teknologi dengan menjadikan alat bukti elektronik sebagai alat bukti yang sah di dalam persidangan peradilan pidana. Dan juga pengaturan alat bukti elektronik di dalam UU ITE tersebut di atas, Serta peran digital forensik dalam melakukan pengolahan alat bukti merupakan suatu langkah yang diperlukan dalam hal alat bukti elektronik akan dipergunakan sebagai alat bukti dalam persidangan.

Forensik digital merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi data digital yang ditemukan pada perangkat digital untuk kepentingan pembuktian hukum. Dalam hal melakukan proses penyelidikan dan penyidikan harus dapat mengkualifikasikan jenis tindak pidana dengan metode teknologi apa yang digunakan, hal ini mempengaruhi dalam proses investigasi yang dilakukan melalui macam-macam ilmu digital forensik.

DAFTAR PUTAKA

Al-Azhar, M. N. (2012). *Digital Forensic Panduan Praktis Investigasi Komputer*. 25–26.

Arifiyadi, T., & Sitompul, J. (2015). *Gadgetmu, Harimaumu*. Lentera Hati.

Asimah, D. (2020). *Menjawab Kendala Pembuktian Dalam Penerapan Alat Bukti Elektronik*. *3*(2), 99.

Chazawi, A., & Ferdian, A. (2015). *Tindak pidana informasi & transaksi elektronik: penyerangan terhadap kepentingan hukum pemanfaatan teknologi informasi dan transaksi elektronik: UU no. 11 tahun 2008 Tentang Informasi & Transaksi Elektronik*. Media nusa creative.

Good Practice Guiede for Computer-Based Electronic Evidence. (n.d.). 4.

Hartono, M. S., & Yuliartini, N. P. R. (2020). Penggunaan Bukti Elektronik Dalam Peradilan Pidana. *Jurnal Komunikasi Hukum*, *6*(1).

Kartanegara, S. (1976). *Hukum Pidana*. Balai Lektur Mahasiswa.

Kumala, D. N. K. R. (n.d.). *Digital Forensik Dalam Kasus Pembunuhan*. Balipost.Com. Diakses pada 03 Oktober 2023 melalui http://balipost.com.html.

Manope, I. J. (2017). Kekuatan Alat Bukti Surat Elektronik Dalam Pemeriksaan Perkara Pidana. *Lex Cri Men*, *VI*(2), 108.

Medeline, F. (2022). *Forensik Digital dalam Pembuktian Tindak Pidana Ujaran Kebencian di Media Sosial*. *3*(3), 311.

Prayudi, Y., & Afrianto, D. S. (2007). Antisipasi Cyber Crime menggunakan Teknik Komputer Forensik. *Universitas Islam Indonesia, Yogyakarta*.

Pribadi, I. (2018). *Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana*. *3*(1), 111.

Raharjo, B. (2013). Sekilas Mengenai Forensik Digital. *Jurnal Sosioteknologi*, *12*.

Ramiyanto. (2017). Bukti Elektronik Sebagai Alat Bukti Yang Sah Dalam Hukum Acara Pidana. *Jurnal Fakultas Hukum Universitas Sjakhyakirti Palembang*, 472.

Rosalina, V., Suhendarsah, A., & Natsir, M. (2016). Analisis Data Recovery Menggunakan Software Forensic: Winhex And X-Ways Forensic. *Jurnal Prosisko*, *3*(1).

Ruci Meiyanti, dan I. (2015). Perkembangan Digital Forensik. *Jurnal Kajian Ilmial UBJ*, *15*(2).

Sari Rizki, N. (2018). Analisis Digital Forensic Dalam Mengungkapkan Tindak Kejahatan Cyber Pada Tahap Pembuktian. *Jurnal Ilmu Mahasiswa*, *2*(4).

Satria., A. (2019). *Penggunaan Digital Forensik Dalam Pembuktian Tindak Pidana Pencemaran Nama Baik Melalui Media Sosial*. Repository Unair.

Sitompul, J. (2012). *Cyberspace Cybercrime Cyberlaw Tinjauan Aspek Hukum Pidana*. Tata Nusa Jakarta.

Sutra, H. (2022). *Lensa Penelitian Hukum: Esai Deskriptif tentang Metodologi Penelitian Hukum*. *2*, 295.

Tri, A. (2010). *Cyber Crime dalam Perspektif Hukum Pidana*. Surakarta: UMS.

US Department of Justice. (2004). *Forensic Examination of Digital Evidence: Guide for Law Enforcement*.

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

Zuhdy, P. dan M. (2020). Penegakan Hukum oleh Aparat Penyidik Cyber Crime dalam Kejahatan Dunia Maya (Cyber Crime) di Wilayah Hukum Polda DIY. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, *1*(2), 80.

Perundang-Undangan

Undang-Undang. (2016). *Undang-undang No 19 Tahun 2016 Tentang Perubahan atas Undang-undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*.