BAB II

TINJAUAN PUSTAKA TENTANG DIGITAL FORENSIK, ALAT BUKTI DALAM SISTEM HUKUM PIDANA, dan PROSES PEMBUKTIAN DALAM PERSIDANGAN DI PERADILAN PIDANA

A. Tinjauan Umum Digital Forensik

1. Definisi, Perkembangan dan Ruang Lingkup Digital Forensik

a. Definisi Digital Forensik

Istilah Forensik berasal dari bahasa Latin *forensic* yang berati "dari luar" dan serumpun dengan kata forum yang berati "tempat umum". Dalam kaitan ini, digital forensik dikenal istilah *chain of custody* dan *rules of vidence* yang artinya pemeliharaan dengan meminimalisir kerusakan yang diakibatkan karena investigasi, sehingga, forensik adalah metode investigasi yang digunakan untuk membantu proses penegakan keadilan melalui proses penerapan ilmu (sains) dengan memeriksa dan menganalisis suatu bukti digital yang dapat dipertanggungjawabkan (Hummerson, 2024, hal. 73). Pada hakikatnya digital forensik merupakan ilmu pengetahuan mengenai teknologi komputer terhadap kasus-kasus kejahatan dengan barang bukti elektronik *(computer crime*) guna menemukan bukti untuk kepentingan pembuktian hukum (Totota & Bakhtiar, 2024, hal. 180).

Adapun beberapa pengertian digital forensik berdasarkan pendapat dari pakar forensik digital ialah sebagai berikut:

1) Menurut Eoghan Casey, mendefenisikan digital forensik sebagai karakteristik bukti yang mempunyai kesesuaian dalam mendukung pembuktian fakta dan mengungkap kejadian berdasarkan bukti statistik yang meyakinkan.
2) Menurut Budhisantoso, menjelaskan bahwa digital forensik adalah kombinasi disiplin ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum.
3) Menurut Andi Dharmawan, menjelaskan bahwa digital forensik merupakan hal penting dalam menangani kasus kriminal di era teknologi dengan mengumpulkan, menganalisis, dan menyajikan bukti digital secara akurat dan dapat dipertanggungjawabkan.
4) Menurut Dr. HB Wolfe, mendefinisikan sebagai sebuah seri metodologi dari teknik dan prosedur untuk mengumpulkan bukti, dari peralatan komputer dan alat penyimpanan lainnya dan media digital yang dapat disajikan di pengadilan dalam format yang koheren dan bermakna.

5) Menurut Marcella, digital forensik adalah kegiatan yang terkait dengan pengamanan, identifikasi, pengambilan/penyaringan, dan dokumentasi bukti digital dalam konteks kejahatan komputer.

b. Sejarah dan Perkembangan Digital Forensik

Rizky Aulia Cahyadri dalam bukunya yang berjudul "Apa yang Harus Ditanyakan Kepada Ahli Digital Forensics (2021), hal. 19-23" menjelaskan bahwa:

Digital Forensik bermula dari komputer Forensik yang lahir seiring ditemukannya komputer. Kesadaran akan kejahatan komputer pertama kali mulai muncul pada 1976 di Eropa dan 1977 di Amerika Serikat, meskipun Florida baru menetapkan undang-undang pertama tentang kejahatan komputer pada 1978. Selanjutnya, perhatian internasional terhadap *cybercrime* mulai digagas oleh INTERPOL pada 1979 dan OECD pada 1983 yang merekomendasikan harmonisasi hukum pidana terkait kejahatan komputer.

Perkembangan awal Digital Forensik pada tahun 1980-an disebut sebagai fase *pre-forensics* atau *ad hoc phase* karena masih kekurangan formalitas, protokol, pelatihan, dan peralatan yang memadai. Memasuki pertengahan 1980-an, digital Forensik berkembang ke *structured phase* yang ditandai dengan harmonisasi antara prosedur forensik dengan aturan kejahatan komputer. Meskipun peralatan forensik masih terbatas dan mahal, pembahasan

bukti elektronik mulai dimasukkan dalam konferensi ilmu forensik internasional pada 1999, diikuti dengan penerbitan jurnal khusus bukti elektronik pada 2002. Pada akhir fase ini, *Computer Forensics* berevolusi menjadi *Digital Forensics* karena ruang lingkup analisis meluas dari bukti fisik menjadi berbagai bentuk bukti elektronik yang ditemukan di banyak perangkat seperti telepon seluler, GPS, kamera, jaringan, dan konsol permainan. Pada awal tahun 2000, digital forensik memasuki *enterprise phase* atau *golden age* di mana pengadilan semakin familiar dengan bukti elektronik dan perangkat forensik semakin banyak dikembangkan.

c. Ruang Lingkup Digital Forensik

Digital forensik mencakup sejumlah disiplin ilmu, yang terkait dengan komputer *(host, server)*, jaringan *(network)*, aplikasi (termasuk database) dan perangkat *(digital devices)* (Hummerson, 2024, hal.72-73). Hal tersebut dijelaskan sebagai berikut (Awaka & Alhadiansyah, 2023, hal. 463-464):

1) Forensik komputer ini bergantung pada sistem operasi yang digunakan. Sebagai contoh, kebanyakan pengguna komputer desktop menggunakan sistem operasi *Microsoft Windows*. Oleh karena itu, diperlukan kemampuan untuk melakukan forensik pada komputer yang menggunakan sistem operasi *Microsoft Windows*. Informasi mengenai layanan yang disediakan oleh komputer atau server biasanya tercatat dalam berbagai berkas

log. Sebagai contoh, aktivitas pengguna yang gagal masuk karena salah memasukkan *password* akan tercatat sebagai bagian dari upaya untuk melakukan penerobosan akses dengan cara *brute force password cracking*. Selain itu, aktivitas seperti pengguna memasukkan *flashdisk* ke port USB juga tercatat dan dapat menjadi fokus dalam penyidikan komputer forensik.

2) Forensik jaringan memfokuskan pada data yang diperoleh berdasarkan pengamatan pada jaringan. Sebagai contoh, kita dapat mengamati *traffic* pada server yang diakses oleh seorang pengguna, yang diduga melakukan penerobosan pada server.
3) Forensik aplikasi terkait dengan penggunaan aplikasi tertentu. Aplikasi memiliki fitur untuk meninggalkan jejak sebagai bagian dari fungsi audit. Ada kewajiban bagi aplikasi untuk mencatat berbagai akses sebagai bagian dari fungsi audit ini. Sebagai contoh, penggunaan *email* dapat ditelusuri dengan adanya catatan jejak di *header* dari *email*. Kejadian yang terkait dengan *email* palsu atau *email* kaleng dapat ditelusuri sumbernya dengan menelusuri *header* dari *email*.
4) *Mobile Forensic* berkaitan dengan barang bukti elektronik seperti *handphone* maupun tablet. Pemeriksaan ini terfokus pada informasi digital yang tersimpan di perangkat tersebut, seperti panggilan masuk, panggilan keluar, SMS, email, foto, dan video. Tujuan dari *mobile forensic* adalah untuk

mengidentifikasi komunikasi antara pelaku kejahatan dan menganalisis data yang berkaitan dengan kejahatan yang terjadi.

5) *Image Forensic* berkaitan dengan jenis barang bukti digital berupa file gambar. Jenis digital forensik ini sering dianalisis untuk mengetahui peralatan kamera digital yang digunakan untuk mengambil gambar tersebut dan juga dapat memeriksa waktu pengambilan gambar. Pemeriksaan ini dapat membantu dalam mengidentifikasi asal dan autentisitas gambar digital yang menjadi bukti dalam suatu kasus.

2. Landasan Hukum Digital Forensik

Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik secara eksplisit mengakui informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah di pengadilan dan merupakan perluasan alat bukti sesuai hukum acara di Indonesia sebagaimana diatur dalam Pasal 5 ayat (1) dan (2) UU ITE, asalkan memenuhi syarat dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan yang diatur dalam Pasal 6 UU ITE. Berdasarkan Pasal 5 dan Pasal 6 UU ITE menjadi dasar penting penggunaan digital forensik dalam pembuktian tindak pidana siber dan kasus lain yang melibatkan

bukti digital. Digital forensik berperan dalam mengidentifikasi, mengumpulkan, menganalisis, dan menyajikan bukti digital agar dapat memenuhi syarat sebagai alat bukti yang sah di pengadilan. Proses digital forensik memastikan keaslian, integritas, dan pertanggungjawaban bukti digital sesuai dengan ketentuan UU ITE.

Selanjutnya mengenai keabsahan barang bukti secara eksplisit diatur dalam Peraturan Kepala Kepolisian Negara Republik Indonesia No. 10 Tahun 2009 tentang Tata Cara dan Persyaratan Permintaan Pemeriksaan Teknis Kriminalistik TKP dan Laboratoris Kriminalistik Barang Bukti Kepada Laboratorium Forensik Kepolisian Negara Republik Indonesia Pasal 2 ayat (1) dan ayat (2) yang menyebutkan bahwa, dalam ayat (1) peraturan ini bertujuan sebagai pedoman bagi petugas pelaksana penyidikan di lapangan dalam menangani tempat kejadian perkara dan barang bukti yang akan dimintakan pemeriksaan ke laboratorium forensik Polri. Selanjutnya dalam ayat (2) menyatakan bahwa tujuan permintaan pemeriksaan ke Laboratoium Forensik Polri adalah untuk pembuktian secara ilmiah barang bukti. Ketentuan ini dapat dipahami bahwa keabsahan barang bukti dapat ditentukan melalui hasil pemeriksaan laboratorium forensik.

Standarisasi yang mengatur tata cara pengumpulan dan pengamanan bukti digital yang sering digunakan adalah ISO/IEC 27037:2012 tentang *Guidelines for identification, collection,*

acquisition, and preservation of digital evidence, 2012 yang diadopsi secara identik dalam Standar Nasional Indonesia (SNI) 27037:2014, yakni memberikan panduan mengenai identifikasi, pengumpulan, dan pengamanan bukti digital untuk keperluan forensik. Panduan ini digunakan secara luas oleh penyidik digital untuk memastikan bahwa seluruh proses dilakukan sesuai dengan standar internasional dan dapat diterima di berbagai yurisdiksi (Goodison et al., 2018: Bahri, 2024, hal. 114).

SNI 27037:2014 memberikan penjelasan bahwa terdapat 3 (tiga) prinsip dasar dalam bukti digital, yaitu *relevance* (relevansi), *reliability* (keandalan) dan *sufficiency* (ketercukupan). Penjelasan terhadap 3 (tiga) prinsip dasar tersebut adalah (Putri, 2024, hal. 25-26):

1) *Relevance* (relevansi)

   Harus dapat ditunjukkan bahwa materi yang diperoleh relevan dengan investigasi, yaitu berisi informasi yang berharga dalam membantu investigasi dan ada alasan yang kuat untuk itu.

2) *Reliability* (keandalan)

   Semua proses yang digunakan dalam menangani bukti digital harus dapat diaudit dan dapat diulang. Hasil penerapan proses tersebut harus dapat direproduksi.

3) *Sufficiency* (ketercukupan)

Digital Evidence First Responder (DEFR) harus telah mempertimbangkan bahwa materi yang dikumpulkan cukup untuk memungkinkan dilakukannya penyelidikan yang tepat.

ISO/IEC 17025 tentang *General Requirements for the Competence of Testing and Calibration Laboratori* merupakan pespersyaratan umum untuk kompetensi laboratorium pengujian dan kalibrasi. Di sebagian besar negara, ISO/IEC 17025 merupakan standar yang harus diakreditasi oleh sebagian besar laboratorium sehingga dapat dianggap kompeten secara teknis. Dalam banyak kasus, pemasok dan otoritas regulasi tidak akan menerima hasil pengujian atau kalibrasi dari laboratorium yang tidak terakreditasi. ISO/IEC 17025 awalnya dikenal sebagai ISO/IEC *Guide* 25 dan dikeluarkan oleh ISO/IEC pada tahun 1999. Ada banyak kesamaan dengan standar ISO 9000 , tetapi ISO/IEC 17025 lebih spesifik dalam persyaratan kompetensi dan berlaku langsung pada organisasi yang menghasilkan hasil pengujian dan kalibrasi dengan didasarkan pada prinsip yang lebih teknis. Laboratorium menggunakan ISO/IEC 17025 untuk menerapkan sistem mutu yang ditujukan untuk meningkatkan kemampuan mereka dalam menghasilkan hasil yang valid secara konsisten dengan standar yang berakreditasi (Wikipedia, 2024).

3. Tujuan, Fungsi dan Peranan Digital Forensik dalam Proses Hukum

Berdasarkan Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik *juncto* Kitab Undang-Undang Hukum Acara Pidana (KUHAP), digital forensik bertujuan sebagai salah satu alat bantu penyidik dalam melakukan penyidikan dan penyelidikan (Rachmie, 2020, hal. 108). Digital forensik berfungsi untuk mengumpulkan, memeriksa, dan menyajikan bukti digital. Hasil pengujian forensik digital dari metode ini digunakan untuk mendukung bukti digital sebagai bukti yang sah dan bukti di pengadilan (Abdullah, 2022, hal. 6). Digital forensik akan menentukan keabsahan suatu alat bukti elektronik di persidangan.

Peran digital forensik banyak ditempatkan dalam berbagai keperluan, diantaranya untuk menangani beberapa kasus kriminal yang melibatkan perangkat digital seperti rekonstruksi perkara, upaya pemulihan kerusakan sistem, pemecahan masalah yang melibatkan *hardware* ataupun *software,* dan dalam memahami sistem ataupun berbagai perkara yang melibatkan perangkat digital lainnya. Oleh karena itu, peran digital forensik dalam proses hukum adalah untuk memberikan bukti digital dari suatu aktivitas tertentu atau umum dalam mengungkap berbagai kasus kejahatan. Selain mengidentifikasi bukti langsung sebuah kejahatan, digital forensik dapat digunakan untuk mengkonfirmasi hubungan antara tersangka dan kasus tertentu,

mengkonfirmasi alibi-alibi atau pernyataan pernyataannya, untuk memahami niat mengidentifikasi sumber (misalnya, dalam kasus sengketa hak cipta), atau mengontentikasi dokumen-dokumen (Hummerson, 2024, hal. 71).

Beberapa bukti elektronik, seperti analisis metadata atau rekaman CCTV yang dienkripsi, memerlukan pengetahuan teknis yang mendalam untuk dipahami dan dipresentasikan secara tepat di pengadilan. Hal ini memerlukan keahlian dari pihak yang memproses bukti, seperti ahli forensik digital, untuk menjelaskan bukti tersebut dalam istilah yang dapat dimengerti oleh hakim sehingga Hakim dapat menilai dengan tepat validitas dan relevansi bukti digital yang diajukan

4. Mekanisme Digital Forensik

Bukti digital bersifat sangat mudah diubah atau dihapus, sehingga proses pengumpulannya memerlukan prosedur khusus yang memastikan integritas data terjaga. SNI 27037:2014 memberikan pedoman dalam penanganan bukti digital yang meliputi tahapan: *identification* (identifikasi). *collection* (pengumpulan), *acquisition* (akusisi) dan *preservation* (preservasi). Pengertian dari tahapan-tahapan tersebut adalah (Badan Standardisasi Nasional, 2014):

a) *Identification* (identifikasi), yakni proses yang melibatkan pencarian, rekognisi (identifikasi) dan dokumentasi terhadap bukti digital yang potensial;

b) *Collection* (pengumpulan), yakni proses pengumpulan barang-barang fisik yang mengandung bukti digital yang potensial;
c) *Acquisition* (akusisi), yakni proses untuk menciptakan salinan dari data, hasil dari proses akuisisi adalah salinan dari bukti digital;
d) *Preservation* (preservasi), yakni proses untuk menjaga integritas dan/atau kondisi awal dari bukti digital.

Penanganan bukti digital juga memerlukan ketelitian tinggi dalam memastikan bahwa bukti tersebut tidak direkayasa atau diubah sehingga dapat menjamin validitas bukti digital. Sehingga, dalam pengambilan barang bukti digital ini, diperlukan ahli yang bisa mengambil data digital dengan kompetensi dan relevansi yang jelas terhadap tindakan-tindakannya selama melakukan pemeriksaan dan analisis barang bukti tersebut. Penggunaan *Chain of Custody* yang ketat sangat diperlukan dalam proses pengumpulan bukti digital untuk memastikan keasliannya. Berikut ini adalah beberapa hal yang umumnya dilakukan dalam proses investigasi untuk menjaminkan *CoC,* yaitu (*Chain Of Custody*, 2013):

1) Selalu mendokumentasikan semua kondisi yang terjadi pada barang bukti.
2) Dokumentasi dilengkapi dengan foto dan video untuk menjaminkan bahwa semua proses penanganan barang bukti telah sesuai dengan ketentuan.

3) Selalu memberikan label segel pada barang bukti untuk menjaminkan authonetifikasi barang bukti, demikian juga ketika harus membuka segel prosesnya terdokumentasi dengan baik.
4) Mencatat dalam log setiap individu yang bersinggungan dengan barang bukti.
5) Form untuk dokumentasi dibuat rangkap.

Output dari proses forensik digital tersebut adalah *digital evidence* itu sendiri serta hasil uji forensik digital.

B. Tinjauan Umum Alat Bukti Dalam Sistem Hukum Pidana

1. Definisi Pembuktian

Hukum pembuktian adalah bagian hukum yang termasuk dalam bagian hukum formil atau prosedural, peraturan hukum pembuktian ini harus sesuai dengan makna keadilan di dalamnya sehingga dapat menjadi dasar penerapan dalam menemukan kebenaran materiel dalam suatu persidangan perkara pidana. Sehingga dengan menganalisa hukum pembuktian secara menyeluruh maka digunakan rumusan alat ukur dalam hukum pembuktian yang terdiri atas (R. Soebjakto, 1991: Takariawan, 2021, hal 44):

a) Dasar-dasar pembuktian yang tersimpul dalam pertimbangan keputusan Pengadilan untuk memperoleh fakta-fakta yang benar *(bewijsgronderi)*.

b) Alat bukti yang dapat dipergunakan Hakim untuk mendapatkan gambaran tentang terjadinya perbuatan pidana yang sudah lampau *(bewijsmiddelen)*.
c) Penguraian cara bagaimana menyampaikan alat bukti kepada Hakim disidang Pengadilan *(bewijsvoering)*.
d) Kekuatan pembuktian dari masing-masing alat bukti dalam rangkaian penilaian terbuktinya suatu dakwaan *(bewijskracht)*.
e) Beban pembuktian yang diwajibkan oleh undang-undang untuk membuktikan tentang dakwaan dimuka sidang pengadilan *(bewijslast)*.
f) Bukti minimum yang diperlukan dalam pembuktian untuk meningkatkan keabsahan Hakim *(bewijs minimun)*.

Adapun pengertian pembuktian menurut para ahli, ialah sebagai berikut:

a) M. Yahya Harahap menyatakan bahwa pembuktian adalah ketentuan-ketentuan yang berisi penggarisan dan pedoman tentang cara-cara yang dibenarkan undang-undang membuktikan kesalahan yang didakwakan kepada terdakwa. Pembuktian juga merupakan ketentuan yang mengatur alat-alat bukti yang dibenarkan undang-undang dan boleh dipergunakan hakim membuktikan kesalahan yang didakwakan.
b) R Supomo mengajukan dua gagasan mengenai arti penting pembuktian. Pertama, pembuktian penting sebagai upaya

pembenaran hubungan hukum. Adanya pembuktian dalam memperkuat kesimpulan hakim berbasis pada syarat-syarat bukti yang sah. Olehnya ini disebut dengan pembuktian dalam arti luas. Kedua, pembuktian penting dalam hal apa yang dikemukakan oleh penggugat dibantah oleh tergugat. Hal-hal yang tidak dibantah tidak membutuhkan pembuktian.

c) Eddy O.S. Hiariej merumuskan gagasan tentang arti pentingnya suatu pembuktian sebagai langkah mencari kebenaran atas suatu peristiwa.

d) Martiman Prodjohamidjojo mengemukakan bahwa pembuktian mengandung maksud dan usaha untuk menyatakan kebenaran atas sesuatu peristiwa, sehingga dapat diterima akal terhadap kebenaran peristiwa tersebut.

e) Darwan Prinst berpendapat bahwa pembuktian adalah pembuktian bahwa benar suatu peristiwa pidana telah terjadi dan terdakwalah yang bersalah melakukannya, sehingga harus mempertanggung jawabkannya.

2. Jenis-Jenis Alat Bukti Berdasarkan Pasal 184 Ayat (1) KUHAP

Alat bukti adalah segala sesuatu yang ada hubungannya dengan suatu perbuatan yang dapat dipergunakan sebagai bahan pembuktian dan memberikan keyakinan hakim atas kebenaran adanya suatu tindak pidana yang telah dilakukan oleh terdakwa. Dalam sistem hukum pembuktian di Indonesia, terdapat pengelompokkan alat bukti, yang

membagi alat bukti ke dalam kategori berikut (Mansur & Gultom, 2005, hal. 100-101):

a) *Oral Evidence*, yakni keterangan saksi, keterangan ahli, dan keterangan terdakwa.
b) *Documentary Evidence*, yakni surat dan petunjuk.
c) *Material Evidence*, yakni barang yang digunakan untuk melakukan tindak pidana, barang yang digunakan untuk membantu tindak pidana, barang yang merupakan hasil dari suatu tindak pidana, barang yang diperoleh dari suatu tindak pidana, dan informasi dalam arti khusus.
d) *Electronic Evidence*, yakni pengaturannya tidak melahirkan alat bukti baru, tetapi memperluas cakupan alat bukti yang masuk kategori *documentary evidence*.

Macam-macam alat bukti yang sah yang digunakan untuk membuktikan telah ditentukan pasal 184 ayat (1) KUHAP, yaitu:

a. Keterangan Saksi

Keterangan saksi yang mempunyai nilai sebagai alat bukti ialah keterangan yang sesuai dengan Pasal 1 angka 27 KUHAP, yakni yang saksi dengar sendiri, saksi lihat sendiri,dan saksi alami sendiri serta menyebut alasan dari pengetahuannya itu. Keterangan saksi diatur dalam Pasal 185 KUHAP, yang menyebutkan bahwa: "Keterangan saksi sebagai alat bukti ialah apa yang saksi nyatakan di sidang pengadilan". Keterangan seorang saksi saja tidak cukup

untuk membuktikan bahwa terdakwa bersalah terhadap perbuatan yang didakwakan kepadanya *(unus testis nullus testis).* Keterangan saksi yang dapat dianggap cukup membuktikan kesalahan terdakwa harus memenuhi paling sedikit atau sekurang-kurangnya dengan 2 (dua) alat bukti (Ramdhana dkk., 2024, hal. 146).

Berkenaan dengan sifat *cybercrime* yang *virtual*, maka pembuktian dengan menggunakan keterangan saksi tidak dapat diperoleh secara langsung melainkan hanya dapat berupa hasil pembicaraan atau hanya mendengar dari orang lain, Kesaksian ini dikenal sebagai *testimonium de auditum* atau *hearsay evidence*. Meskipun kesaksian sejenis ini tidak diperkenakan sebagai alat bukti, akan tetapi dalam praktiknya tetap dapat dipergunakan sebagai bahan pertimbangan bagi hakim untuk memperkuat keyakinannya sebelum menjatuhkan putusan melalui hasil interaksi di dalam dunia *cyber*, seperti *chatting* dan *email* antara pengguna internet atau juga dapat melalui keterangan seorang administrator sistem komputer yang telah disertifikasi (Mansur & Gultom, 2005, hal. 116).

b. Keterangan Ahli

Keterangan ahli adalah keterangan yang diberikan oleh seseorang yang memiliki keahlian khusus, yang mengkaji hal-hal yang diperlukan termasuk petunjuk-petunjuk perkara pidana sebagaimana yang dijelaskan dalam Pasal 1 angka 28 KUHAP (Kasidin, 2021, hal. 9). Keterangan ahli diatur dalam Pasal 186 KUHAP yang

menyebutkan bahwa: “Keterangan ahli ialah apa yang seorang ahli nyatakan di sidang pengadilan”. Keterangan ahli dapat juga diberikan pada waktu pemeriksaan oleh penyidik atau penuntut umum yang dituangkan dalam suatu bentuk laporan dan dibuat dengan mengingat sumpah di waktu ia menerima jabatan atau pekerjaan (Zega dkk., 2021, hal. 175). Keterangan ahli didasarkan pada pengetahuan, keahlian, pengalaman, serta penalaran yang dimiliki oleh ahli tersebut.

Keterangan ahli menjadi signifkan penggunaannya jika jaksa mengajukan alat bukti elektronik untuk memberikan suatu penjelasan di dalam persidangan bahwa dokumen/data elektronik yang diajukan adalah sah dan dapat dipertanggungjawabkan secara hukum sehingga dapat memperkuat untuk membuktikan kesalahan pelaku *cybercrime*. Hal ini diperlukan karena terkadang dalam praktiknya, para pelaku *cybercrime* dapat menghapus atau menyembunyikan aksi mereka agar tidak terdeteksi oleh aparat penegak hukum. Peranan seorang ahli dalam *cybercrime* merupakan sesuatu yang tidak bisa ditawar-tawar lagi mengingat pembuktian dengan alat bukti elektronik masih sangat riskan penggunaannya di depan sidang pengadilan. Di sinilah pentingnya kedudukan seorang ahli, yaitu untuk memberikan keyakinan kepada hakim (Mansur & Gultom, 2005, hal. 117).

c. Surat

Aspek fundamental surat sebagai alat bukti diatur pada Pasal 184 ayat (1) huruf c KUHAP. Kemudian secara substansial tentang bukti surat ini ditentukan oleh Pasal 187 KUHAP yang menjelaskan bahwa:

"Surat sebagaimana tersebut pada Pasal 184 ayat (1) huruf c, dibuat atas sumpah jabatan atau dikuatkan dengan sumpah, adalah:

a) Berita acara dan surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat di hadapannya, yang memuat keterangan tentang kejadian atau keadaan yang didengar, dilihat atau yang dialaminya sendiri, disertai dengan alasan yang jelas dan tegas tentang keterangannya itu;
b) Surat yang dibuat menurut ketentuan peraturan perundang-undangan atau surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksana yang menjadi tanggung jawabnya dan yang diperuntukkan bagi pembuktian sesuatu hal atau sesuatu keadaan;
c) Surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai sesuatu hal atau sesuatu keadaan yang diminta secara resmi daripadanya;
d) Surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain."

Jenis alat bukti surat lainnya dapat berupa bukti elektronik yang dapa dicetak atau print out dan surat yang terpampang dalam layar monitor sebuah jaringan komputer. Selama kedua bukti ini dikeluarkan dibuat oleh yang berwenang dan sebuah sistem jaringan komputer tersebut dipat dipercaya, maka surat tersebut memiliki kekuatan pembuktian yang sama dengan alat bukti surat sebagaimana yang ditentukan dalam KUHAP (Mansur & Gultom, 2005, hal. 118).

d. Petunjuk

Berdasarkan Pasal 188 ayat (1) KUHAP menjelaskan bahwa: "Petunjuk adalah perbuatan, kejadian atau keadaan, yang karena persesuaiannya, baik antara yang satu dengan yang lain, maupun dengan tindak pidana itu sendiri, menandakan bahwa telah terjadi suatu tindak pidana dan siapa pelakunya". Petunjuk dapat diperoleh dari Keterangan saksi, Keterangan ahli, Surat dan Keterangan terdakwa sebagaimana yang disebutkan dalam Pasal 188 ayat (2) KUHAP. Selanjutnya dalam Pasal 188 ayat (3) KUHAP menjelaskan tentang penilaian terhadap kekuatan pembuktian dari suatu petunjuk dalam setiap keadaan tertentu dilakukan oleh pemeriksaan hakim dengan dengan cermat dan adil.

Mewujudkan suatu petunjuk dari bukti-bukti yang ditemukan dalam *cybercrime* akan sulit jika hanya mendasarkan pada keterangan saksi, surat, atau keterangan terdakwa saja meskipun hal tersebut

masih mungkin untuk diterapkan oleh hakim untuk memperoleh petunjuk dari alat-alat bukti terebut di persidangan. Akan tetapi, apabila hakim dapat petunjuk yang dujukan di persidangan adalah bukti elektronik yang disertai dengan keterangan ahli, maka petunjuk ini akan bersifat lebih kuat dan memberatkan terdakwa dibandingkan dengan petunjuk-petunjuk lain (Mansur & Gultom, 2005, hal. 119).

e. Keterangan Terdakwa

Berdasarkan Pasal 189 KUHAP dapat disimpulkan bahwa keterangan terdakwa dapat dilakukan di dalam maupun di luar sidang pengadilan. Untuk membuat keterangan terdakwa di persidangan dapat dinilai sebagai alat bukti yang sah, maka harus memuat penjelasan atau jawaban yang dikemukakan terdakwa dalam menjawab setiap pertanyaan, serta perbuatan-perbuatan yang dilakukan, diketahui atau dialami sendiri. Sedangkan, keterangan terdakwa di luar sidang pengadilan hanya dapat digunakan untuk membantu pengadilan menemukan bukti yang ada (Mulyadi, 2007: Kasidin, 2021, hal. 10). Keterangan terdakwa saja tidak cukup untuk membuktikan bahwa ia bersalah melakukan perbuatan yang didakwakan kepadanya, melainkan harus disertai dengan alat bukti yang lain sebagaimana yang dijelaskan lebih lanjut dalam Pasal 189 ayat (4) KUHAP.

Pada praktiknya, perolehan keterangan terdakwa menjadi sesuatu proses yang sulit dilakukan dikarenakan kemampuan/pengetahuan teknologi informasi penyidik yang terbatas, pelaku *cybercrime* yang sulit untuk identifikasi secara pasti, serta kuatnya jaringan diantara sesama pelaku *cybercrime* (Mansur & Gultom, 2005, hal. 119).

Perluasan alat bukti petunjuk selain dari keterangan saksi, surat dan keterangan terdakwa, dapat berupa informasi yang diperoleh secara eleketronik berupa tulisan, suara, gambar, huruf, angka, ataupun yang bentuk lain yang terdapat makna (Budiman, 2021, hal.116).

3. Alat Bukti Elektronik

a. Definisi dan Ruang Lingkup

Alat bukti elektronik adalah Informasi Elektronik dan/atau Dokumen Elektronik yang memenuhi persyaratan formil dan persyaratan materiil yang diatur dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Alat bukti elektronik dalam Pasal 1 Angka 1 Undang-Undang tentang Informasi dan Transaksi Elektronik menjelaskan bahwa informasi elektronik berarti setiap atau kumpulan data elektronik, termasuk namun tidak terbatas pada data tertulis. Audio, gambar, peta, gambar, foto, pertukaran data elektronik (EDI), teks secara

elektronik (email), telegram, teleks, faksimili atau sejenisnya, surat. tanda tangan, angka yang berarti, kode akses, simbol, perforasi mesin, atau hal ini dapat dipahami oleh mereka yang dapat memahaminya.

Alat bukti elektronik secara tegas diatur dalam Pasal 5 Undang-Undang ITE sebagai syarat formil. Suatu asas yang juga dipakai sebagai upaya untuk menelusuri *materiiel waarheid* (kebenaran materiil) sebagaimana dinyatakan oleh Van Bemmelen, bahwa dalam menelusuri kebenaran materiil, maka berlaku suatu asas bahwa keseluruhan proses yang menghantarkan kepada Putusan Hakim, harus secara langsung dihadapkan kepada Hakim dan proses secara keseluruhan diikuti oleh Terdakwa serta harus diusahakan dengan alat bukti yang sempurna. Debra L. Shinder mengemukakan, bahwa terdapat beberapa syarat yang harus dipenuhi agar alat bukti dapat diterima di pengadilan, yaitu pertama, alat bukti harus kompeten *(reliable dan credible)* sehingga terjamin validitasnya. Melalui sistem keamanan informasi yang *certified*, maka integritas konten dalam suatu bukti elektronik (informasi dan/atau dokumen elektronik) menjadi terjamin keautentikannya. Kedua, alat bukti harus relevan (dapat membuktikan fakta dari suatu kasus). Dan ketiga, alat bukti harus material (memperkuat persoalan yang dipertanyakan dalam suatu kasus).

Bukti Elektronik memiliki beberapa ciri-ciri, yaitu (Hummerson, 2024, hal. 55-59):

1) *Integrity.*

   Aspek siber menekankan integritas perlindungan informasi dan modifikasi oleh orang yang tidak berwenang. Oleh karena itu, informasi tidak dapat diubah tanpa izin dari pemilik infomasi.

2) *Availability*

   Bukti elektronik yaitu ketersediaan yang menitikberatkan kepada memberi kepastian untuk pihak yang berwenang agar dapat mengakses informasi ketika dibutuhkan. Hal tersebut didukung dengan adanya pemeliharaan perangkat keras *(Hardware)* sebagai sarana dalam menyimpan dan menampilkan informasi dengan baik. Pasal 16 UU ITE menjelaskan bahwa:

   "Sepanjang tidak ditentukan lain oleh undang undang tersendiri, setiap Penyelenggaraan Sistem Elektronik wajib mengoperasikan sistem elelaronik yang memenuhi persyaratan minimum sebagai berikut:

   a) dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang diterapkan dalam peraturan Perundang-undangan;
   b) dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut, Dapat

beroperasi sesuai dengan prosedur atau penunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;

c) dapat beroperasi sesuai dengan prosedur ataua petunjuk dalam Penyelenggaran Sistem Elektronik tersebut;
d) dilengkapi dengan prosedur atau penunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan
e) memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk".

3) *Authentication*

Eksistensi informasi elektronik dan/atau dokumen elektronik telah diakui sebagai alat bukti yang sah dan merupakan perluasan dari alat bukti dalam Hukum Acara yang berlaku di Indonesia dengan syarat informasi elektronik dan/atau dokumen elektronik tersebut menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Dalam praktiknya, bukti elektronik ditampilkan dengan cara yang berbeda-beda, seperti menghadirkan hasil

cetaknya, sampai menghadirkan perangkat pembawa bukti elektronik tersebut dan menunjukkan data di dalamnya secara langsung. Tidak adanya aturan ini menyebabkan ketidakpastian hukum mengenai bagaimana seharusnya bukti elektronik ditampilkan di persidangan. Sehingga kendala yang terbesar dalam pelaksanaan atau pembuktian alat bukti elektronik di persidangan adalah belum diaturnya alat bukti dan pembuktiannya dalam hukum acara sebagai hukum formal. Pengaturan alat bukti elektronik baru diatur pada hukum materiil.

4) *Confidentiality*

Confidenciality atau kerahasiaan adalah upaya pencegahan bagi mereka yang tidak berkepentingan untuk dapat mencapai informasi. Secara umum dapat disebutkan bahwa kerahasiaan yang mengandung makna bahwa informasi yang tepat hanya dapat terakses oleh mereka yang berhak (dan bukan orang lain).

5) Non-repudiation

Digunakan dalam bidang komputasi, keamanan informasi, dan komunikasi. *Non Repudiation* adalah salah satu dari lima pilar jaminan informasi (IA), yang merupakan praktik pengelolaan risiko terkait informasi dan melindungi sistem informasi, seperti komputer, server, dan jaringan perusahaan. Empat pilar lainnya yaitu integritas, ketersediaan, autentikasi dan kerahasiaan.

b. Syarat Alat Bukti Elektronik

Keabsahan alat bukti didasarkan pada pemenuhan syarat dan ketentuan baik segi formil maupun materiil sehingga alat bukti tersebut dapat dinyatakan sah dan dapat dipergunakan di persidangan. Ketentuan dan persyaratan tersebut adalah untuk menjamin kepastian hukum dan berfungsi sebagai alat penguji dalam menentukan keabsahan alat bukti sehingga hakim yakin dengan fakta-fakta hukum yang dihadirkan melalui alat bukti elektronik.

Menurut Pasal 5 ayat (4) Undang-Undang ITE syarat formil suatu alat bukti, yaitu bahwa informasi atau dokumen elektronik bukanlah dokumen atau surat yang menurut perundang-undangan harus dalam bentuk tertulis. Selain itu, informasi dan/atau dokumen tersebut harus diperoleh dengan cara yang sah. Ketika alat bukti diperoleh dengan cara yang tidak sah, maka alat bukti tersebut dikesampingkan oleh hakim atau dianggap tidak mempunyai nilai pembuktian oleh pengadilan. Sedangkan syarat materiil diatur dalam Pasal 6, Pasal 15, dan Pasal 16 UU ITE, yang pada intinya informasi dan dokumen elektronik harus dapat dijamin keotentikannya, keutuhannya, dan ketersediaannya. Dengan dipenuhinya persyaratan materiil dan juga persyaratan formil maka alat bukti elektronik memiliki nilai yang sama (Putri, 2024, hal. 93).

C. Tinjauan Umum Proses Pembuktian Dalam Persidangan Di Peradilan Pidana

1. Sistem Pembuktian dalam Hukum Acara Pidana Indonesia

Teori pembuktian dalam sistem peradilan pidana merupakan aspek fundamental yang menentukan proses penegakan hukum dan pencapaian keadilan. Pembuktian merujuk pada tindakan memberikan atau menunjukkan bukti, menegakkan suatu kebenaran, menghadirkan saksi, dan memberikan keyakinan. Dalam bahasa Belanda, istilah *"bewijs"* memiliki dua makna yakni, sebagai suatu tindakan yang memberikan kepastian dan sebagai hasil dari tindakan tersebut yang berupa adanya kepastian (Budiman, 2022).

Pembuktian dimulai pada tahap penyidikan, sebagaimana yang dijelaskan dalam Pasal 1 angka 2 KUHAP bahwa: "Penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam Undang-Undang untuk mencari serta mengumpulkan bukti yang terjadi guna menemukan tersangkanya". Sedangkan penyidik diatur dalam Pasal 1 angka 1 KUHAP yang menjelaskan bahwa: "Penyidik adalah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang- undang untuk melakukan penyidikan". Bukti yang telah diperoleh oleh penyidik kemudian dinilai untuk menentukan bukti tersebut telah cukup untuk membuat terang suatu tindak pidana yang terjadi dan dapat digunakan untuk menemukan

tersangkanya. Selanjutnya, pada tahap penuntutan dan persidangan terkait kesesuaian dan hubungan antara alat-alat bukti dan pemenuhan unsur pidana akan diuji (Putri, 2024, hal. 89).

Terdapat empat jenis teori pembuktian, yaitu: sistem positif, *conviction intime*, *conviction raisonnee*, dan sistem negatif (Hamzah:251-25: Soetarna, 2023).

a) *Positief Wettelijk Bewijstheorie* atau Pembuktian berdasarkan undang-undang secara positif yakni mengutamakan kepastian hukum yang hanya berpedoman pada ketentuan undang-undang saja tanpa memerlukan pertimbangan hakim. Teori sudah ditinggalkan karena menyampingkan fungsi hakim (Hawasara dkk., 2022, hal. 591).
b) *Conviction Intime* (Sistem Keyakinan Hakim) yakni berbasis pada keyakinan hakim semata, tidak memerlukan alasan yang logis hanya mengikuti hati nuraninya sehingga Hakim sangat subjektif untuk menentukan seorang terdakwa bersalah atau tidak.
c) *Conviction Raisonee* (Keyakinan Hakim Dengan Alasan Yang Logis) yakni mempertimbangkan aspek rasionalitas, kombinasi antara keyakinan dan penalaran. Hakim harus memiliki keyakinan penuh atas kebenaran perbuatan sebelum menjatuhkan hukuman yang berdasarkan kepada dasar-dasar pembuktian yakni prinsip *beyond reasonable doubt* menuntut hakim untuk memiliki

keyakinan yang didukung dengan bukti kuat atas kebenaran perbuatan terdakwa.

d) Sistem pembuktian dalam KUHAP didasarkan pada prinsip *negatief wettelijk bewijstheorie* (Hawasara dkk., 2022, hal. 592), sebagaimana diatur dalam Pasal 183 KUHAP yang menyatakan bahwa:"Hakim tidak boleh menjatuhkan pidana kepada seorang kecuali apabila sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya".

2. Mekanisme Pemeriksaan Alat Bukti dalam Persidangan Pidana

Hakim bertugas memeriksa alat bukti yang diajukan oleh penuntut umum dalam proses pembuktian. Alat bukti tersebut tentunya merupakan yang relevan dan sah menurut ketentuan peraturan perundang undangan serta memenuhi syarat formil maupun materiil. Alat bukti yang sah menurut sistem peradilan pidana di Indonesia ialah sebagaimana yang ditentukan dalam Pasal 184 Ayat (1) KUHAP yaitu keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan Terdakwa. Namun, dalam KUHAP tidak secara tegas memasukkan bukti elektronik ke dalam jenis-jenis alat bukti, maka dengan mengikuti perkembangan teknologi, upaya perluasan terkait pengaturan tentang alat bukti elektronik ialah dengan mengeluarkan Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor

11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.(Nuarta & Santhi, 2024, hal. 40).

KUHAP telah menganut asas legalitas dan *lex stricta*, namun kedua asas itu bukan berarti tidak dapat dikesampingkan. Asas legalitas *(principle of legality)* menentukan bahwa tidak ada perbuatan yang dilarang dan diancam dengan pidana jika tidak ditentukan terlebih dahulu dalam perundang-undanga yang ditafsirkan dengan memuat syarat, yakni larangan retroaktif, ketentuan pidana harus dirumuskan dalam wujud peraturan tertulis *(lex scripta*); dirumuskan secara jelas *(lex certa)* dan harus ditafsirkan secara ketat, termasuk ke dalamnya larangan penafsiran analogi *(lex stricta)* (Riadi, 2024). Apabila aturan-aturan yang ada di dalam KUHAP tidak lengkap atau tidak sempurna, maka dapat dikesampingkan demi tercapainya tujuan hukum acara pidana, yaitu kebenaran materiil. Hal itu selaras dengan sifat sistem hukum Indonesia yang bersifat terbuka *(open system)*. Apabila hanya didasarkan pada ketentuan KUHAP yang kaku dan bersifat limitatif, maka kebenaran materiil belum tentu dapat tercapai. Praktik demikian hanya dapat mewujudkan keadilan prosedural (kebenaran formal), bukan keadilan substansial (kebenaran materiil) (Nelson dkk., 2022).