BAB III
HASIL PENELITIAN DAN PEMBAHASAN

A. Keabsahan Alat Bukti Elektronik Dalam Hukum Nasional

Di Indonesia, sebelumnya belum ada pengaturan yang jelas mengenai sistem hukum pembuktian terkait alat bukti elektronik. Namun, setelah disahkannya UU ITE, yang menekankan bahwa alat bukti elektronik berfungsi sebagai informasi, dokumen elektronik, dan hasil cetakan yang memiliki kekuatan hukum sebagai bukti dalam konferensi, diharapkan undang-undang ini dapat menjawab berbagai hak yang berkaitan dengan hukum, termasuk hukum pembuktian yang berhubungan dengan dunia maya, hukum teknologi dan komunikasi.[37]

Bahwa UU ITE telah mengatur bahwa upaya paksa yang dapat digunakan aparat penegak hukum untuk memperoleh bukti elektronik ialah melalui pengeledahan dan penyitaan sistem elektronik atau melalui intersepsi atau penyadapan. Penyidik menggunakan cara penggeledahan dan penyitaan apabila sudah mengetahui secara jelas sumber bukti elektronik tersebut (lokasi komputer, laptop, USB, server milik tersangka, korban, atau saksi). Sedangkanm berdasarkan batasan-batasan yang diatur dalam perundang-undangan, intersepsi atau penyadapan dapat digunakan oleh aparat penegak hukum sebagai cara mengumpulkan informasi dan keterangan terkait dengan suatu tindak pidana (tersangka, tindak pidana yang dipersangkakan, saksi, lokasi tindak pidana), informasi tersebut dapat dijadikan alat bukti.

Dalam sistem pembuktian di indonesia, keselahan terdakwa ditentukan oleh minimal dua alat bukti yang sah dan ditambah dengan keyakinan hakim. Keabsahan alat bukti didasarkan pada pemenuhi syarat dan ketentuan baik segi formil maupun materiil. Prinsip ini juga berlaku terhadap pengumpulan dan penyajian bukti elektronik baik yang dalam bentuk original maupun hasil cetaknya, yang diperoleh baik melalui penyitaan maupun intersepsi, KUHAP

[37] Munir Fuady, *Teori Hukum Pembuktian Pidana dan Perdata*, (Bandung: PT Citra Aditya, 2012), hlm. 2012.

telah memberikan pengaturan jelas mengenai upaya paksa penggeledahan dan penyitaan secara umum, tetapi belum terhadap Sistem Elektronik.

Salah satu aspek menarik dari penggunaan alat bukti elektronik adalah pemanfaatan teknologi informasi dan internet, yang menjadikannya sebagai topik yang sangat relevan. Selain Indonesia, beberapa negara seperti Singapura, Jepang, China, Chili, dan Australia juga mengakui alat bukti elektronik dalam sistem hukum mereka, di mana data elektronik diakui sebagai bukti yang sah dalam proses persidangan. Pasal 5 ayat (1) UU ITE memberikan dasar hukum yang menyatakan bahwa informasi elektronik dapat menghasilkan dokumen cetak yang berfungsi sebagai perpanjangan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Perluasan ini menunjukkan bahwa alat bukti elektronik menambah jenis alat bukti yang telah diatur sebelumnya dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Lahirnya UU ITE merupakan sedikit kemajuan dalam menyikapi dan menanggulangi maraknya *cyber crime* saat ini, terutama dalam proses penegakan hukumnya/proses beracaranya. Dalam Pasal 1 butir (1) UU ITE, disebutkan 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.

Sedangkan mengenai Dokumen Elektronik sebagaimana disebutkan dalam Pasal 1 butir (4) UU ITE, adalah setiap Informasi Elektronik yang 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.

Dari pengertian mengenai Informasi Elektronik dan Dokumen Elektronik tersebut di atas terlihat perbedaan yang sangat mendasar di antara keduanya, yaitu sebagai berikut:

1. Pada prinsipnya Informasi Elektronik dapat dibedakan tetapi tidak dapat dipisahkan dengan Dokumen Elektronik.
2. Informasi Elektronik ialah data atau kumpulan data dalam berbagai bentuk.
3. Dokumen Elektronik ialah wadah atau "bungkus" dari Informasi Elektronik.
4. Sebagai contoh apabila kita berbicara mengenai file musik dalam bentuk mp3 maka semua informasi atau musik yang keluar dari file tersebut ialah Informasi Elektronik, sedangkan Dokumen Elektronik dari file tersebut ialah mp3.

Tidak semua informasi atau dokumen elektronik dapat dianggap sebagai alat bukti yang sah. Berdasarkan UU ITE, informasi atau dokumen elektronik hanya dapat diakui sebagai alat bukti jika menggunakan sistem elektronik yang memenuhi ketentuan yang ditetapkan dalam undang-undang tersebut. Sistem elektronik tersebut harus andal, aman, dan memenuhi persyaratan minimum, yang meliputi:[38]

a. Kemampuan untuk menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan periode penyimpanan yang ditentukan oleh peraturan yang berlaku;
b. Kemampuan untuk melindungi ketersediaan, integritas, keaslian, kerahasiaan, dan aksesibilitas informasi elektronik dalam pengoperasian sistem elektronik;
c. Kemampuan untuk beroperasi sesuai dengan prosedur atau petunjuk yang ditetapkan untuk sistem elektronik;

[38] Ari Juliano Gema, "*Apakah Dokumen Elektronik Dapat Menjadi Alat Bukti*", http://arijuliano.blogspot.com/2008/04/apakah-dokumen-elektronik-dapat-menjadi.html#, diakses pada tanggal 24 Januari 2025.

d. Dilengkapi dengan prosedur atau petunjuk yang disampaikan dalam bahasa, inf ormasi, atau simbol yang dapat dipahami oleh pihak-pihak yang berkepentingan dalam pengoperasian sistem elektronik
e. Memiliki mekanisme yang berkelanjutan untuk menjaga kesegaran, kejelasan, dan akuntabilitas dari prosedur atau instruksi yang ada.

Oleh karena itu, keabsahan alat bukti yang berupa informasi elektronik dan/atau dokumen elektronik dapat dianggap sebagai perpanjangan dari alat bukti elektronik yang diatur dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Perluasan ini merujuk pada ketentuan yang terdapat dalam Pasal 5 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE):

a. Berfungsi sebagai perluasan alat-alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia;
b. Cakupan alat bukti yang telah diatur di dalam Hukum Acara Pidana diperluas oleh hasil cetak dari informasi;
c. Merupakan alat bukti surat serta alat bukti petunjuk.

Menurut Eddy O.S. Hiariej, Pasal 5 Undang-Undang ITE menyatakan bahwa alat bukti berupa informasi elektronik dan dokumen elektronik, beserta cetakannya, merupakan perluasan dari alat bukti yang diatur dalam Pasal 184 KUHAP. Ia berpendapat bahwa tidak perlu lagi diperdebatkan apakah alat bukti informasi elektronik dan dokumen elektronik serta hasil cetaknya merupakan perpanjangan dari alat bukti surat atau alat bukti indikatif, karena pada dasarnya, alat bukti informasi elektronik dan hasil cetaknya adalah tambahan baru di luar alat bukti yang sudah ada dalam UU ITE. Dengan demikian, alat bukti dalam proses pembuktian perkara pidana saat ini terdiri dari lima jenis yang diatur dalam Pasal 184 KUHAP dan Pasal 5 UU ITE, yaitu: keterangan saksi, keterangan ahli, surat, petunjuk, keterangan terdakwa, serta informasi elektronik dan dokumen elektronik dan/atau hasil cetaknya.[39]

[39] Nur Laili Isma dan Arima Koyimatun, "Kekuatan Pembuktian Alat Bukti Informasi Elektronik Pada Dokumen Elektronik Serta Hasil Cetaknya Dalam Pembuktian Tindak Pidana", Jurnal Penelitan Hukum Volume 1, Nomor 2, Juli 2014, hlm. 112.

Beberapa undang-undang mengklasifikasikan alat bukti elektronik sebagai bagian dari alat bukti indikatif, sementara undang-undang lainnya tidak menganggapnya demikian, melainkan menganggapnya sebagai alat bukti baru yang setara dengan lima jenis alat bukti yang diatur dalam Pasal 184 Kitab Undang-Undang Hukum Pidana (KUHP). Dalam Pasal 44 jo. Pasal 5 Undang-Undang ITE, alat bukti elektronik mencakup istilah "Informasi Elektronik" dan "Dokumen Elektronik". Oleh karena itu, alat bukti elektronik pada dasarnya merujuk pada informasi atau dokumen, yang secara umum dapat disebut sebagai data, bukan sebagai alat.

B. Kedudukan Alat Bukti Digital Dalam Perkara *Cybercrime*

Sebagaimana diketahui bahwa sistem pembuktian dalam hukum acara pidana mengacu kepada Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP). Prinsip pembuktian dalam perkara pidana diatur dalam ketentuan 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 terdakwalah yang bersalah melakukannya".

Dari bunyi ketentuan, dapat dikatakan bahwa keberadaan alat bukti dalam proses persidangan merupakan hal pokok dalam proses peradilan pidana. Oleh karena itu Majelis Hakim harus mendapatkan keyakinan apakah perbuatan pidana yang didakwakan dalam surat dakwaan jaksa penuntut umum kepada terdakwa memiliki dasar hukum yang kuat atau tidak.

Dalam KUHAP secara jelas sudah diatur mengenai apa yang dimaksud dengan alat bukti yang sah, hal mana diatur dalam Pasal 184 KUHAP, yaitu keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Namun demikian KUHAP tidak mendefinisikan secara jelas apa yang dimaksud dengan barang bukti, walaupun istilah barang bukti sering disebut dalam KUHAP.

Meskipun KUHAP tidak menyebutkan secara jelas definisi dari barang bukti, dalam doktrin hukum acara pidana dapat dipahami bahwa yang dimaksud dengan barang bukti itu adalah benda-benda yang dapat dikenakan penyitaan. Hal ini diatur dalam Pasal 39 ayat (1) KUHAP, yang menyatakan bahwa barang bukti itu adalah sebagai berikut:

1. Benda atau tagihan tersangksa atau terdakwa yang seluruhnya atau sebagian diduga diperoleh dari tindakan pidana atau sebagai hasil tindak pidana atau benda yang telah dipergunakan secara langsung untuk melakukan tindak pidana atau untuk mempersiapkannya.
2. Benda yang dipergunakan untuk menghalangi-halangi penyidikan tindak pidana.
3. Benda yang khusus dibuat dan diperuntuhkan melakukan tindak pidana.
4. Benda lain yang mempunyai hubungan langsung dengan tindak pidana yang dilakukan.

Dalam proses pembuktian di persidangan walaupun tidak disebut secara jelas sebagai alat bukti yang sah, barang bukti memiliki kedudukan yang sangat penting. Hal ini terlihat pada Pasal 181 ayat (1) KUHAP yang mengatur kewajiban hakim ketua sidang untuk memperlihatkan semua barang bukti kepada terdakwa dan menanyakan apakah terdakwa mengenal barang-barang bukti tersebut ataukah tidak. Dari hal tersebut dapat dilihat bahwa ini menunjukkan kedudukan barang bukti memiliki fungsi yang penting dalam sistem pembuktian persidangan.

Seiring dengan kemajuan teknologi informasi dan telekomunikasi, alat bukti mengalami perkembangan dengan munculnya alat bukti dalam bentuk informasi elektronik dan/atau dokumen eletronik yang dikenal dengan istilah bukti elektronik

Pengaturan hukum mengenai bukti elektronik dalam Hukum Acara Pidana secara spesifik belum dapat ditemukan dalam KUHAP. Namun, seiring berkembangnya zaman dan berkembangnya tindak pidana, sejalan dengan pendapat Eugen Ehrlich yang menyatakan bahwa dalam membuat undang-

undang hendaklah diperhatikan apa yang hidup dalam masyarakat,[40] dimana pengaturan alat bukti elektronik dinilai penting dalam merespon tumbuhnya modus kejahatan suatu tindak pidana yang dilakukan melalui media elektronik.

Dengan respon yang cukup baik pada tahun 2008 dimana Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan Undang-Undang pertama yang secara khusus mengatur tindak pidana siber di Indonesia. Berdasarkan surat presiden RI.No.R./70/Pres/9/2005 tanggal 5 September 2005, naskah UU ITE secara resmi disampaikan kepada DPR RI kemudian disahkan pada tanggal 21 April 2008. Undang-Undang tersebut dibuat untuk mencegah kejahatan terhadap kasus/perkara siber (*cybercrime*) dan sampai sekarang masih sangat diperlukan (*urgent*) sebagai dasar untuk mengambil sebuah keputusan (*decision maker*) dalam menanggulangi kejahatan siber agar dapat mengetahui modus dan karakteristik pelaku serta modus yang dipergunakan.[41]

Bukti elektronik pertama kali diatur pada tahun 1997 yaitu dalam Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan. Dalam undang-undnag tersebut, tidak disebutkan secara tegas kata bukti elektronik namun dalam Pasal 15 disebutkan bahwa data yang disimpan dalam mikrofilm atau media lainnya dianggap sebagai alat bukti yang sah. Kata elektronik pertama kali dimunculkan pada Undang-Undang Nomor 20 Tahun 2001 yang merupakan perubahan dari Undang-Undang Nomor 31 Tahun 1999 tentang Tindak Pidana Korupsi. Pada Pasal 26 A disebutkan bahwa informasi yang disimpan secara elektronik merupakan alat bukti petunjuk.

Terobosan UU ITE membawa perubahan yang signifikan dalam sistem peradilan, terutama terkait pengakuan alat bukti elektronik. Walaupun didalam KUHAP belum mengaturnya, tetapi UU ITE telah mengizinkan dan melegalkan penggunaan alat bukti elektronik di dalam persidangan.

[40] Efa Laila Fakhriah, Bukti Elektronik dalam Pembuktian Perdata, (Bandung: Alumni, 2009), hlm. 86.
[41] Djanggih, Hardianto, and Nurul Qamar. "Penerapan Teori-Teori Kriminilogi dalam Penanggulangan Kejahatan Siber (Cyber Crime)." *Pandecta Research Law Journal 13*, no. 1 (2018); 10-23 20

Kedudukan alat bukti dalam bentuk informasi elektronik dan dokumen elektronik yang diatur dalam Pasal 5 UU ITE, dalam perkembangan terlihat munculnya pengertian alat bukti elektronik di sembilan (9) undang-undang, diantaranya sebagai berikut:[42]

1. Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan;
2. Undang-Undang Nomor 20 Tahun 2001 tentang Pemberantasan Tindak Pidana Korupsi;
3. Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme;
4. Undang-Undang Nomor 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang;
5. Undang-Undang Nomor 35 Tahun 2009 tentang Narkotika;
6. Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang;
7. Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Pendanaan Terorisme;
8. Undang-Undang Nomor 18 Tahun 2013 tentang Pencegahan dan Pemberantasan Perusakan Hutan;
9. Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

Berdasarkan sembilan (9) undang-undang di atas, terdapat dua pengelompokan tentang alat bukti elektronik, yaitu sebagai berikut:

Pengelompokan pertama, memasukan alat bukti elektronik ke dalam alat bukti yang ada di dalam sistem KUHAP (Pasal 184), yaitu:[43]

a. masuk dalam perluasan alat bukti surat, contoh Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan;
b. masuk dalam perluasan alat bukti petunjuk, contoh Undang-Undang Nomor 20 Tahun 2001 tentang Pemberantasan Tipikor.

[42] Agung Iswanto, "Keabsahan Alat Bukti Elektronik dalam Sistem Peradilan Pidana di Indonesia", E-Journal Pengadilan Militer Utama, hlm. 1.
[43] Harli Siregar dan Sakafa Guraba, ADMISIBILITAS BUKTI ELEKTRONIK DALAM PERSIDANGAN, (Depok: Rajawali Pers, 2023), hlm. 41.

Pengelompokan kedua, memasukkan alat bukti elektronik merupakan alat bukti yang berdiri sendiri, terpisah dari alat bukti yang telah diatur dalam Pasal 184 KUHAP. Contoh: Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme; Undang-Undang Nomor 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang; Undang-Undang Nomor 35 Tahun 2009 tentang Narkotika; Undang-Undang Nomor 8 Tahun 2010 tentang pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang; Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Pendanaan Terorisme, Undang-Undang Nomor 18 Tahun 2013 tentang Pencegahan dan Pemberantasan Perusakan Hutan dan Undang-Undang Nomor 20 Tahun 2014 tentang Hak Cipta.

Berdasarkan ketentuan Pasal 5 ayat (3) UU ITE ditentukan bahwa:

> "Informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam undang-undang ini".

Dari ketentuan tersebut di atas, penggunaan dokumen elektronik sebagai suatu alat bukti yang dianggap sah apabila menggunakan suatu sistem elektronik yang sesuai dengan ketentuan yang berlaku. Hal tersebut sebagaimana diatur dalam Pasal 6 UU ITE, yang menyatakan sebagai berikut:

> "Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, 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".

Disamping itu, dokumen elektronik yang berkedudukannya dapat disetarakan dengan dokumen yang dibuat di atas kertas. Hal ini sebagaimana ditentukan dalam penjelasan umum UU ITE, yang menyatakan bahwa ketentuan tersebut dikecualikan, sebagaimana termaksud di dalam Pasal 5 ayat (4) UU ITE, yang menentukan bahwa ada beberapa jenis dokumen elektronik yang tidak dapat dijadikan alat bukti yang sah apabila terkait dengan

pembuatan surat: surat yang menurut undang-undang harus dibuat dalam bentuk tertulis, dan surat beserta dokumennya yang menurut undang-undang harus dibuat dalam suatu bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Dalam rangka penggunaan dokumen elektronik, maka yang perlu dipahami adalah bahwa UU ITE melarang perbuatan-perbuatan sebagaimana diatur dalam ketentuan Pasal 27 sampai dengan Pasal 37, yang menentukan bahwa jika terjadi penyalahgunaan dalam penggunaan teknologi informasi, terkhusus dokumen elektronik, yang merugikan bagi pihak lain, dapat digugat atau dituntut, baik secara keperdataan maupun kepidanaan. Hal itu sebagaimana ditentukan dalam Pasal 38, Pasal 39, serta Pasal 45 sampai dengan Pasal 52 UU ITE.

C. Standar Penentuan Bukti Elektronik Diterima Sebagai Alat Bukti Dalam Pembuktian Tindak Pidana Penipuan Dengan Modus Sniffing

Secara umum bentuk dari alat bukti elektronik itu adalah berupa informasi elektronik dan dokumen eletronik. Dalam Pasal 1 angka 1 UU ditentukan bahwa informasi elektronik adalah satu atau sekumpulan data elektronik, 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 ditelah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Bukti dalam hukum siber berdasarkan ketentuan umum Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) (Pasal 1 angka 1 s.d angka 6, angka 9, angka 12 s.d 23) adalah:

1. transaksi elektronik;
2. teknologi informasi;
3. dokumen elektronik;
4. sistem elektronik;

5. penyelenggaraan sistem elektronik;
6. agen elektronik;
7. sertifikat elektronik;
8. tanda tangan elektronik;
9. penandatanganan;
10. komputer;
11. kode akses;
12. kontrak elektronik;
13. pengirim;
14. penerima;
15. nama domain.

Alat bukti pada umumnya sering dipergunakan dalam hal pembuktian siber, yaitu informasi elektronik dan dokumen elektronik sebagaimana dijelaskan di dalam Pasal 1 angka 1 jo. Pasal 1 angka 4 UU ITE.

Barang bukti berisfat fisik dan dapat dikenali secara visual, oleh karena itu investigator dan forensik harus sudah memahami untuk kemudian dapat mengenali masing-masing barang bukti elektronik ini ketika sedang melakukan proses *searching* (pencarian) barang bukti di TKP. Jenis-jenis barang bukti elektronik adalah sebagai berikut:[44]

a) Komputer PC. laptop/notebook, netbook, tablet
b) Handphone, smartphone
c) Flashdisk/thumbdrive
d) Floopydisk
e) Harddisk
f) CD/DVD
g) Rounter, switch, hub
h) Kamera video, cctv
i) Kamera digital

[44] Indah Pongantung, "Kedudukan Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana Informasi Dan Transaksi Elektronik Berdasarkan Undang-Undang Nomor 19 Tahun 2016", Lex Crimen Volume 10, Nomor 7, Juni 2021, Halaman 147-156.

j) Digital recorder

k) Music/video player

Bukti digital merujuk pada informasi yang diambil atau dipulihkan dari sumber elektronik. Dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), jenis bukti ini disebut sebagai informasi dan dokumen elektronik. Para ahli forensik perlu mencari dan menganalisis dengan teliti hubungan antara setiap file untuk mengungkap kasus kejahatan yang melibatkan barang bukti elektronik. Berikut adalah beberapa contoh dari bukti digital tersebut:[45]

1. *Logical file* adalah file yang masih ada dan terdaftar dalam sistem file yang sedang berjalan (*running*) pada suatu partisi. Jenis file ini dapat mencakup aplikasi, pustaka, dokumen kantor, log, multimedia, dan lainnya.
2. *Deleted file*, yang juga dikenal sebagai *unallocated cluster*, merujuk pada *cluster* dan sektor penyimpanan yang sebelumnya digunakan untuk file yang telah dihapus dan tidak lagi dialokasikan oleh sistem file. Area ini ditandai sebagai ruang yang dapat digunakan kembali untuk menyimpan file baru. Dengan kata lain, file yang telah dihapus masih berada di *cluster* atau sektor penyimpanannya sampai ditimpa oleh file baru. Jika file yang dihapus belum tertimpa, ada kemungkinan besar untuk melakukan pemulihan secara menyeluruh.
3. *Lost file*, adalah file yang tidak lagi terdaftar dalam di *file system* yang sedang berjalan pada suatu partisi, meskipun file tersebut masih ada di sektor penyimpanan. Situasi ini dapat terjadi, misalnya, ketika flashdisk, harddisk, atau partisi mengalami format ulang, yang menghasilkan sistem file baru, sehingga file yang sebelumnya ada tidak tercatat dalam sistem file yang baru. Proses pemulihan tergantung pada jenis format file yang digunakan.
4. *File slack* adalah area penyimpanan yang terletak di antara End of Cluster (EoC). Ruang ini berpotensi menyimpan informasi penting dari file yang telah dihapus sebelumnya.

[45] *Ibid.*

5. *Long file* adalah file yang merekam aktivitas (*logging*) dari situasi tertentu, seperti log yang dihasilkan oleh sistem operasi, penggunaan internet, browser, aplikasi, *internet traffic*, dan lain-lain.
6. *Encryted file* adalah file yang isinya telah dilindungi dengan algoritma *cryptography* yang rumit, sehingga tidak dapat dibaca atau diakses secara biasa. Satu-satunya cara untuk mengakses atau melihat kembali isi file tersebut adalah dengan mendekripsinya menggunakan algoritma yang sama. Metode ini umum digunakan dalam keamanan informasi digital untuk melindungi data penting. Selain itu, ini juga merupakan salah satu bentuk anti-forensik, yang bertujuan untuk menyulitkan petugas forensik atau penyidik dalam memperoleh informasi terkait jejak tindak pidana.
7. *Stenograph file* dalah file yang menyimpan informasi rahasia yang disisipkan ke dalam file lain, biasanya berupa gambar, video, atau audio. File yang berfungsi sebagai pembawa ini tampak biasa dan tidak mencolok bagi orang lain, tetapi bagi mereka yang memahami metodologinya, file-file ini mengandung makna yang dalam terkait informasi rahasia.
8. *Office file* adalah file yang dihasilkan oleh aplikasi perkantoran seperti *Microsoft Office*, *Open Office*, dan sejenisnya. Jenis file ini umumnya terdiri dari dokumen, spreadsheet, basis data, teks, dan presentasi.
9. *Audio file* adalah file yang menyimpan suara, musik, dan sejenisnya, biasanya dalam format seperti WAV, MP3, dan lainnya. File audio yang berisi rekaman percakapan sering kali menjadi penting dalam penyelidikan, terutama ketika suara dalam file tersebut perlu diperiksa dan dianalisis secara forensik untuk menentukan apakah suara tersebut cocok dengan suara pelaku kejahatan.
10. *Video file* adalah file yang berisi rekaman video yang diambil dari kamera digital, ponsel, handycam, atau CCTV. Ada kemungkinan besar bahwa file video ini menyimpan wajah pelaku kejahatan, sehingga perlu dilakukan analisis mendalam untuk memastikan bahwa individu yang muncul dalam file tersebut adalah pelaku yang dimaksud.

11. *Image file* adalah file digital yang kemungkinan menyimpan informasi penting terkait dengan kamera dan waktu pembuatan (*time stamp*). Data-data ini dikenal dengan istilah *metadata exit* (*exchangeable Image file*). Namun, *metadata exit* ini juga dapat dimanipulasi, sehingga para ahli forensik atau penyelidik perlu berhati-hati saat memeriksa dan menganalisis metadata dari file tersebut.
12. Surat Elektronik, atau yang lebih dikenal dengan istilah email, adalah bentuk komunikasi berbasis sistem elektronik yang memanfaatkan jaringan online untuk pengiriman dan penerimaan. Email memiliki peranan penting dalam penyelidikan, terutama dalam kasus phishing, yaitu kejahatan yang menggunakan email palsu dengan identitas yang tidak benar untuk menipu penerima. Setiap email dilengkapi dengan header yang menyimpan informasi penting mengenai jalur distribusi pengiriman dari pengirim ke penerima. Oleh karena itu, data dalam header sering dianalisis secara mendetail untuk menentukan lokasi pengirim berdasarkan alamat IP. Namun, data dalam header juga rentan terhadap manipulasi, sehingga pemeriksaan header email harus dilakukan dengan cermat dan menyeluruh.
13. *User ID dan password* adalah dua elemen yang diperlukan untuk masuk ke akun secara *online*. Jika salah satu dari keduanya tidak tepat, maka akses ke akun tersebut akan ditolak.
14. *Short Message Service* (*SMS*) adalah layanan yang memungkinkan pengiriman dan penerimaan pesan singkat yang disediakan oleh operator seluler untuk para pelanggannya. SMS, yang dapat berupa pesan masuk, keluar, atau draf, dapat berfungsi sebagai petunjuk dalam penyelidikan untuk mengungkap hubungan antara satu pelaku dengan pelaku lainnya.
15. *Multimedia Massage Service* (*MMS*) adalah layanan yang ditawarkan oleh operator seluler yang memungkinkan pengiriman dan penerimaan pesan multimedia, yang dapat mencakup suara, gambar, atau video.

16. *Call log* adalah catatan yang mencatat semua panggilan yang dilakukan melalui nomor ponsel. Catatan ini mencakup panggilan masuk (*incoming*), panggailan keluar (*outgoing*), dan panggilan yang tak terjawab (*missed*).

Berdasarkan bentuknya, karakteristik alat bukti elektronik berbeda dari alat bukti fisik seperti yang dijelaskan dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Dalam KUHAP, alat bukti memiliki bentuk yang jelas, seperti keterangan saksi, keterangan ahli, dokumen, petunjuk, dan keterangan terdakwa, yang tidak mudah diubah serta dapat dengan mudah dilihat dan didengar. Sementara itu, barang bukti elektronik memiliki ciri khas yang tidak terlihat secara langsung, sangat rentan terhadap perubahan, mudah rusak karena sensitif terhadap waktu, dan dapat dengan mudah dimodifikasi atau dihapus. Selain itu, alat bukti elektronik dapat dipindahkan dengan mudah, dan untuk melihat atau membacanya, diperlukan perangkat tambahan, baik berupa perangkat keras (*hardware*) maupun perangkat lunak (*software*)[46]

Bahwa penentuan bukti elektronik dalam pembuktian tindak pidana penipuan dengan modus *sniffing* agar diterima sebagai alat bukti apabila menggunakan sistem elektronik yang memenuhi persyaratan minimum, sebagaimana dalam Pasal 5 ayat (3) jo. Pasal 6 UU ITE, antara lain:

1. dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan;
2. dapat melindungi ketersedian, keutuhan, keautentikan, kerahasian, dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut;
3. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik tersebut;
4. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik tersebut; dan

[46] Eddy Army, Bukti Elektronik dalam Praktik Peradilan, (Jakarta: Sinar Grafika, 2020), hlm. 107.

5. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Sejatinya ada syarat-syarat yang harus dipenuhi agar bukti elektronik dalam pembuktian tindak pidana penipuan dengan modus *sniffing* memenuhi ketentuan sebagai alat bukti yang sah menurut hukum yaitu dipenuhinya 2 (dua) syarat yaitu sebagai berikut:

1. Dipenuhinya syarat formil sebagaimana diatur di dalam Pasal 5 ayat (4) UU ITE yaitu bahwa Informasi dan Dokumen Elektronik bukanlah dokumen atau surat yang menurut perundang-undangan harus dalam bentuk tertulis.
2. Dipenuhi syarat materiil yaitu sebagaimana diatur di dalam Pasal 6, Pasal 15, dan Pasal 16 UU ITE, yang pada intinya Informasi dan Dokumen Elektronik harus dapat dijamin keotentikannya, keutuhannya, dan ketersediannya.

Yang dimaksud dengan persyaratan materiil ialah ketentuan dan persyaratan yang dimaksudkan untuk menjamin keutuhan data (*integrity*), ketersedian (*availability*), keamanan (*security*), keotentikan (*authenticity*), dan keteraksesan (*accesbility*) informasi dan dokumen elektronik dalam proses pengumpulan dan penyimpanan dalam proses penyidikan dan penuntutan, serta penyampaiannya nanti di sidang pengadilan.

Ditinjau dari sifat alamiahnya, bukti digital sangat tidak konsisten. Maka, bukti digital tidak dapat langsung dijadikan alat bukti untuk proses persidangan sehingga dibutuhkan standar agar bukti digital dapat digunakan sebagai alat bukti di persidangan, yaitu sebagai berikut:[47]

a. Dapat diterima, yaitu data harus mampu diterima dan digunakan demi hukum mulai dari kepentingan penyelidikan sampai dengan kepentingan pengadilan.
b. Asli, yaitu bukti tersebut harus berhubungan dengan kejadian/kasus yang terjadi dan bukan rekayasa.

[47] Dewi Asimah, Menjawab Kendala Pembuktian Dalam Penerapan Alat Bukti Elektronik, *Jurnal Hukum Peratun Volume* 3 Nomor 2 Agustus 2020, hlm. 102.

c. Lengkap, yaitu bukti dapat dikatakan bagus dan lengkap jika di dalamnya terdapat banyak petunjuk yang dapat membantu investigasi.
d. Dapat dipercaya, yaitu bukti dapat mengatakan hal yang terjadi di belakangnya, jika bukti tersebut dapat dipercaya, maka proses investigasi akan lebih mudah dan syarat ini merupakan suatu keharusan.

Suatu alat bukti dalam tindak pidana penipuan dengan modus *sniffing* dapat menjadi alat bukti yang sah di persidangan harus didasarkan sertifikasi, baik mengenai subjek maupun sistemnya. Syarat-syarat mengenai penyelenggara sertifikasi dan penyelenggaraan sistem elektronik diatur dalam Pasal 13 sampai dengan Pasal 16 UU ITE. Proses dan pengelolaan (*processing and treatment*) atas informasi elektronik dan/atau dokumen elektronik sehingga menjadi alat bukti memerlukan ilmu keahlian khusus yang disebut sebagai digital forensik (*digital forensic*).

Digital forensik secara sederhana adalah keseluruhan proses dalam mengambil, memulihkan, menyimpan, memeriksa informasi atau dokumen elektronik yang terdapat dalam sistem elektronik atau media penyimpanan, berdasarkan cara dan dengan alat yang dapat dipertanggungjawabkan secara ilmuah untuk kepentingan pembuktian.

Dalam digital forensik, terdapat tiga entitas yang memiliki peran krusial, yaitu manusia sebagai pelaku yang melakukan aktivitas, barang bukti digital sebagai objek dan aset yang sangat penting, serta proses yang menjadi pedoman yang harus diikuti selama seluruh tahapan penyidikan forensik digital. Pelaksanaan penyidikan harus mengikuti metode ilmiah, yang berarti setiap langkah yang diambil oleh tim penyidik atau lembaga hukum harus berlandaskan pada prinsip-prinsip metode ilmiah. Mengacu pada karakteristik metode ilmiah, proses dalam bidang forensik digital harus mengikuti langkah-langkah yang prosedural dan terstruktur. Proses ini dikenal sebagai investigasi forensik digital, yang diterapkan dalam setiap penyelidikan terhadap barang

bukti digital yang terkait dengan suatu kejadian, untuk menentukan apakah kejadian tersebut merupakan tindakan kriminal atau tidak.[48]

Adapun cabang-cabang dari *digital forensik* antara lain sebagai berikut:

1. Komputer Forensik

   Tujuan dari komputer forensik adalah untuk menjelaskan keadaan sat ini artefak digital, seperti sistem komputer, media penyimpanan atau dokumen elektronik. Disiplin biasanya meliputi komputer, embedded system (perangkat digital dengan daya komputasi dasar dan memori onboard dan statis memori (seperti pen drive USB). Forensik komputer dapat menangani berbagai informasi, mulai dari log (seperti sejarah internet) melalui file yang sebenarnya di drive.

2. Forensik Perangkat Mobile

   Forensik perangkat mobile merupakan cabang sub-forensik digital yang berkaitan dengan pemulihan bukti digital atau data dari perangkat mobile. Ini berbeda dari komputer forensik dalam perangkat mobile akan memiliki sistem komunikasi inbuilt (misalnya GSM) dan biasanya, mekanisme penyimpanan proprietary. Investigasi biasanya fokus pada data sederhana seperti data panggilan dan komunikasi (SMS/email) daripada mendalam pemulihan data yang dihapus. Perangkat mobile juga berguna untuk memberikan informasi lokasi, baik dari gps inbuilt/lokasi pelacakan atau melalui situs sel log, yang melacak perangkat dalam jangkauan mereka.

3. Jaringan Forensik

   Jaringan forensik berkaitan dengan pemantauan dan analisis jaringan komputer lalu lintas, baik lokal dan WAN/internet, untuk tujuan pengum- pulan informasi, pengumpulan bukti, atau deteksi intrusi. Lalu lintas biasanya dicegat pada paket tingkat, dan baik disimpan untuk analisis kemudian atau disaring secara real-time. Tidak seperti

[48] Asep Sudirman, "*Kerangka Kerja Digital Forensic Readiness* pada Sebuah Organinasi", (Studi Kasus: PT Wadira Reka Cipta Bandung)", *Tesis* Program Studi Teknik Informatika Program Magister Fakultas Teknologi Industri Universitas Islam Indonesia, 2019, hlm. 49.

di wilayah-wilayah lain, sistem jaringan data forensik digital umumnya tetap stabil dan jarang mengalami aktivitas login, sehingga bidang ini cenderung bersifat responsif.

4. Forensik Database

   Forensik database merupakan subbidang dari forensik digital yang fokus pada analisis forensik terhadap database serta metadata terkaitnya. Penyelidikan melibatkan pemanfaatan konten database, berkas log, dan data RAM untuk menyusun garis waktu atau mengembalikan informasi penting.

Digital forensik merujuk pada sebuah disiplin ilmu dan teknologi informasi yang memegang peran krusial dalam menangani penyelidikan kasus-kasus kejahatan komputer atau kejahatan yang berkaitan dengan komputer. Istilah kejahatan komputer dan kejahatan terkait komputer mirip satu sama lain, tetapi yang pertama tidak selalu melibatkan perangkat komputer sebagai instrumen utama dalam pelaksanaan tindak pidana, seperti halnya defacement (perubahan halaman situs web secara tidak sah), distributed denial of service (menyebabkan sistem berhenti beroperasi normal akibat banjir data dari banyak komputer yang terinfeksi dan membentuk jaringan bot), keylogging (mencatat setiap input keyboard dan tampilan aplikasi di layar), identity theft (pencurian informasi pribadi dari individu sasaran), intrusion (akses ilegal ke dalam sistem), serta berbagai jenis lainnya. Adapun kejahatan terkait komputer mencakup semua bentuk pelanggaran konvensional, termasuk pencurian, pornografi, perampokan, pembunuhan, korupsi, narkotika, dan sebagainya, di mana dalam kasus tersebut terdapat bukti elektronik seperti ponsel dan komputer yang digunakan oleh pelaku untuk komunikasi atau penyimpanan data yang berhubungan dengan perencanaan, eksekusi, dan hasil tindak kejahatannya.

Agar dapat diakui sebagai alat bukti elektronik, data elektronik harus melewati serangkaian proses yang memenuhi standar ilmiah. Tujuan dari langkah ini adalah untuk memastikan bahwa proses hukum berlangsung secara adil dan tidak melanggar hak asasi manusia, baik bagi tersangka/terdakwa

maupun bagi sumber data elektronik yang digunakan dalam pembuktian suatu kasus pidana (*due process of law*).

Pengumpulan dan pengelolaan data elektronik sangat penting untuk memastikan objektivitas dan validitas alat bukti elektronik. Namun, hingga saat ini, Indonesia belum memiliki peraturan khusus yang berlaku secara umum mengenai hal ini. Praktik yang diterapkan saat ini mengacu pada standar ilmiah yang diakui secara internasional. Misalnya ISO 27037 sebuah panduan standar global yang berkaitan dengan pengelolaan bukti digital, dan dapat diterapkan oleh instansi penegak hukum di Indonesia.

Tujuan pokok dari penerapan ISO 27037 dalam menangani bukti elektronik adalah memastikan integritas serta kelengkapan data bukti digital agar tidak mengalami perubahan atau manipulasi. Standar ini juga menetapkan aturan-aturan fundamental untuk pengaturan bukti elektronik yang harus ditaati oleh petugas pertama, seperti relevansi, keandalan, dan kecukupan. Tambahan pula, proses penanganan bukti elektronik yang dilakukan harus memenuhi syarat-syarat seperti kemampuan diaudit, kemampuan diulangi, kemampuan direproduksi, dan kemampuan dipertanggungjawabkan oleh pemeriksa independen atau pakar lainnya.

Oleh sebab itu, elemen-elemen tersebut wajib diterapkan oleh petugas pertama ketika mengurus bukti elektronik. Pada intinya, langkah-langkah serta aturan dasar untuk menangani bukti elektronik menurut ISO 27037 adalah sebagai berikut:[49]

a. Identifikasi

   Proses pengidentifikasian melibatkan kegiatan mencari, mengenali, serta mencatat bukti-bukti digital. First responder (FR) wajib memutuskan dokumen atau informasi elektronik apa saja yang harus diambil dari alat-alat elektronik yang berkaitan dengan kasus kriminal yang tengah ditangani. Di samping itu, FR perlu berkolaborasi dengan investigator untuk mengatur

[49] D. Sudyana, "instrumen Evaluasi *F*
ramework Investigasi Forensika Digital Menggunakan SNI 27037: 2014", *jiska*, Vol. 1, No. 2, September, hlm. 77.

segala detail teknis seputar penyitaan atau pemeriksaan serta pengambilan barang bukti elektronik (acquisition/collection), sambil memperhitungkan berbagai skenario yang mungkin muncul di lokasi kejadian (Tempat Kejadian Perkara/TKP).

b. Koleksi

Setelah perangkat elektronik yang menyimpan bukti digital penting berhasil ditemukan, first responder (FR) wajib menentukan langkah selanjutnya, yaitu apakah akan melaksanakan pengumpulan (collection) atau mengamankan bukti tersebut melalui tahapan berikutnya. Pengumpulan sendiri adalah bagian dari proses penanganan barang bukti elektronik, di mana alat yang memuat bukti tersebut dipindahkan dari tempat asalnya menuju laboratorium forensik atau area terkontrol lainnya untuk dilakukan ekstraksi dan pemeriksaan mendalam. Dalam fase ini, sangat krusial untuk mencatat setiap langkah yang diambil, serta mengemas perangkat dengan aman sebelum mengangkutnya secara teliti, guna memastikan perangkat tidak rusak dan informasi digital tetap terjaga.

c. Akuisisi

Akuisisi adalah proses penyalinan barang bukti elektronik yang dilakukan di lokasi kejadian. Dalam proses perolehan ini, first responder (FR) yang bertanggung jawab harus memiliki kompetensi dan wewenang untuk menangani barang bukti elektronik. Proses perolehan harus dilakukan dengan mengikuti prosedur pencitraan berkas yang tepat agar hasil hashing barang bukti elektronik tidak berubah. Selanjutnya, dokumentasi mengenai metode dan tindakan akuisisi juga harus dilakukan.

d. Preservasi

Proses preservasi adalah serangkaian langkah yang diambil untuk memastikan bahwa data yang telah ditetapkan sebagai alat bukti elektronik tetap aman dan tidak mengalami kehilangan atau perubahan. Berdasarkan tahapan dan prinsip yang terdapat dalam ISO 27037, terdapat perbedaan dalam penanganan barang bukti elektronik yang diatur dalam Perkap No. 10

Tahun 2009, khususnya dalam menjaga integritas dan keutuhan barang bukti elektronik. Kesenjangan tersebut meliputi beberapa hal sebagai berikut:

1) Pihak Pertama yang Menangani (*First Responder*)

Berdasarkan Peraturan Kepala Polri Nomor 10 Tahun 2009, pemeriksaan yang dilakukan oleh Pusat Laboratorium Forensik Mabes Polri hanya bisa dilaksanakan apabila memenuhi persyaratan formal dan teknis yang telah ditentukan oleh penyidik. Dalam konteks ini, penyidik berkewajiban mengantar perangkat elektronik ke laboratorium forensik untuk menjalani proses pemeriksaan. Akan tetapi, tidak terdapat aturan spesifik mengenai pihak mana yang pertama-tama mengambil barang bukti elektronik tersebut. Hal ini kontras dengan panduan yang tercantum dalam standar ISO 27037, yang menyatakan bahwa individu yang menangani barang bukti elektronik sejak tahap awal harus merupakan seorang pakar yang memiliki otoritas, telah dilatih secara memadai, dan memenuhi standar untuk beroperasi di tempat kejadian dengan tujuan melakukan pengumpulan serta pengambilan barang bukti elektronik, yang disebut sebagai responden pertama. Para pakar tersebut juga diuraikan dalam Penjelasan Pasal 43 ayat (5) huruf h Undang-Undang Informasi dan Transaksi Elektronik, yakni orang-orang yang memiliki kompetensi khusus dalam bidang ITE, baik dari aspek praktis maupun akademis.

2) Dokumentasi

Menurut ISO 27037, first responder diwajibkan untuk mendokumentasikan setiap langkah dalam penanganan bukti elektronik, mulai dari proses identifikasi, pengumpulan, perolehan, hingga pelestarian. Tujuan dari dokumentasi ini adalah agar alat bukti elektronik dapat diaudit oleh pemeriksa independen, majelis hakim, atau ahli dari penasihat hukum terkait metodologi yang digunakan dan tindakan yang diambil, sehingga dapat secara hukum dibuktikan bahwa alat bukti elektronik tersebut tetap utuh. Dokumentasi ini dilakukan melalui foto dan jejak audit, yang mencakup catatan rinci mengenai tindakan yang diambil terhadap barang bukti elektronik. Sementara itu, dalam Perkap No. 10/2009, tidak terdapat

kewajiban untuk mendokumentasikan setiap tindakan forensik, terutama melalui jejak audit.

3) Penggunaan Salinan Bukti Elektronik dalam Analisis (*Working File*)

ISO 27037 mengharuskan proses pemeriksaan, analisis, dan pembuktian bukti elektronik dilakukan dengan menggunakan file kerja, bukan file asli (master copy). Hal ini bertujuan untuk mencegah terjadinya perubahan pada alat bukti elektronik selama proses pemeriksaan atau analisis. Sementara itu, Regulasi yang tertuang dalam Perkap No. 10/2009 belum secara eksplisit mewajibkan pemanfaatan salinan data digital saat proses identifikasi oleh Puslabfor, yang mana hal ini membuka celah risiko modifikasi pada data primer. Mengacu pada hasil evaluasi problematika tersebut serta komparasi dengan standar internasional ISO 27037 mengenai prosedur teknis barang bukti digital, transformasi regulasi terkait pengelolaan bukti elektronik di tanah air menjadi sebuah urgensi. Langkah pembaruan ini sangat krusial guna menjamin orisinalitas serta validitas data elektronik, sekaligus memberikan jaminan keadilan dan ketetapan hukum bagi publik, memastikan vonis didasarkan pada pembuktian yang substantif, mengantisipasi potensi manipulasi bukti oleh oknum otoritas, serta sebagai bentuk implementasi konkret atas mandat Putusan Mahkamah Konstitusi No. 20/PUU-XIV/2016.

Pelaksanaan audit digital forensik pada prinsipnya mensyaratkan kualifikasi khusus yang dibuktikan melalui kepemilikan sertifikasi kompetensi dari institusi pendidikan atau pelatihan yang relevan. Kapasitas sebagai pakar teknologi informasi tidak secara otomatis membuat seseorang memiliki kapabilitas yang valid dalam ranah forensik digital; oleh sebab itu, dalam proses litigasi, rekam jejak akademis di bidang ilmu komputer serta sertifikasi keahlian menjadi prasyarat mutlak yang harus diklarifikasi di awal persidangan. Ketidakhadiran sertifikasi formal dalam bidang digital forensik berimplikasi pada rendahnya kekuatan pembuktian dari keterangan yang diberikan, sehingga kesaksian tersebut sangat layak untuk diabaikan oleh majelis hakim. Kredibilitas seorang saksi ahli di muka persidangan harus

senantiasa bersandar pada lisensi profesional yang diakui. Hingga saat ini, akses untuk memperoleh sertifikasi domestik masih terbatas pada program pelatihan yang diselenggarakan oleh Mabes Polri serta Kementerian Komunikasi dan Informatika (Kemenkominfo), sementara alternatif kualifikasi lainnya hanya dapat ditempuh melalui lembaga pendidikan internasional, khususnya di negara seperti Amerika Serikat atau Inggris.

Di dalam digital forensik terdapat 3 (tiga) tahap dasar yang harus dilakukan oleh orang yang melakukan kegiatan digital forensik. Ketiga tahapan tersebut adalah sebagai berikut:

1. Proteksi Penulisan *(Write Protect),* yang merupakan mekanisme penguncian data pada Informasi maupun Dokumen Elektronik sebelum dimulainya prosedur audit forensik. Implementasi Write Protect menjadi krusial untuk menjamin bahwa data sumber tetap orisinal tanpa adanya modifikasi sedikit pun, baik berupa penyisipan, reduksi, maupun penghapusan informasi selama proses pemeriksaan berlangsung.
2. Pencitraan Forensik *(Forensic Imaging),* yakni sebuah tindakan untuk memproduksi salinan data yang benar-benar serupa dengan sumber aslinya, atau yang sering disebut dengan istilah penggandaan *(cloning)*. Proses ini diterapkan pada data yang telah melalui tahap proteksi penulisan, sehingga menghasilkan berkas identik yang dikenal sebagai Image File. Di lingkungan Kepolisian Republik Indonesia, tata cara teknis mengenai prosedur ini telah diatur secara resmi dalam Peraturan Kapuslabfor Nomor 1 Tahun 2014 terkait Prosedur Operasi Standar (SOP) pelaksanaan *Forensic Imaging*.
3. Verifikasi (*Verifying*), yang merupakan fase evaluasi terhadap *output* dari proses pencitraan forensik guna memastikan bahwa data hasil penggandaan tersebut memiliki konsistensi penuh dengan data primer. Penentuan tingkat keidentikan antara data salinan dengan data asli tersebut divalidasi dengan menganalisis parameter yang terdapat pada *Image File* yang telah dihasilkan.

Berdasarkan rangkaian prosedur di atas, hakim di persidangan memiliki kewenangan untuk menguji saksi ahli terkait detail teknis forensik digital yang diterapkan selama fase penyelidikan maupun penyidikan. Jika ditemukan bahwa tenaga ahli tidak mengimplementasikan ketiga protokol fundamental tersebut, maka testimoni serta hasil kerjanya wajib diabaikan oleh pengadilan. Hal ini dikarenakan pengabaian tahapan standar tersebut menyebabkan integritas *image file* diragukan keidentikannya dengan data primer, mengingat adanya risiko tinggi terjadinya manipulasi data berupa insersi, reduksi, atau penghapusan informasi asli. Lebih lanjut, apabila terungkap bahwa data sumber telah hilang, maka kapasitas ahli harus diuji melalui kemampuannya dalam menjalankan prosedur pemulihan data (*data file recovery*) sebelum ia memulai tiga siklus utama forensik digital yang telah dipaparkan sebelumnya.

Ketikadalam proses peradilan diajukan alat bukti berupa Dokumen atau Informasi Elektronik yang diklaim telah melalui proses digital forensik, namun secara faktual ditemukan ketidaksamaan antara *image file* dengan data sumbernya, maka hakim harus menyatakan alat bukti tersebut tidak memiliki kekuatan hukum dan harus dikesampingkan. Meskipun demikian, berbagai jenis bukti digital seperti surat elektronik (e-mail), log percakapan daring (*chatting*), serta beragam dokumen elektronik lainnya tetap diakui sebagai instrumen pembuktian yang sah di muka persidangan sepanjang prosedur perolehannya valid. Ada beberapa proses atau tahapan untuk menilai apakah suatu alat bukti itu sah secara hukum ataukan tidak.

Bukti elektronik mempunyai tahapan agar dapat dikatakan sebagai alat bukti yang valid, yaitu sebagai berikut:

1. Dokumen Elektronik/alat perekamnya harus sesuai dengan standarisasi yang telah ditentukan.
2. Bukti elektronik tersebut harus dibaca oleh orang yang memang ahlinya.
3. Ahli yang membaca bukti elektronik tersebut harus bersertifikasi.
4. Alat yang digunakan untuk membaca bukti elektronik tersebut sesuai dengan standarisasi untuk pembacaan alat bukti elektronik.
5. Proses pembacaan bukti elektronik itu harus benar.

6. Laboratorium atau tempat fasilitas pembacaan bukti elektronik harus sesuai dengan stadarisasi yang telah ditentukan.