

Pertimbangan Hakim Atas Penghadiran Bukti Digital Forensik dalam Perkara Kejahatan *Fraud*

Wahdah Prasetya^{1*}, Puti Priyana²

^{1,2}Fakultas Hukum, Universitas Singaperbangsa Karawang, Indonesia
Jalan HS Ronggowaluyo, Telukjambe Timur, Karawang, Jawa Barat 41361
Correspondence email: wahdahpras@gmail.com

Abstrak. Permasalahan dalam penelitian ini adalah pengaturan hukum digital forensik dalam sistem pembuktian tindak pidana di Indonesia, pertimbangan hakim atas penghadiran bukti digital forensik dalam perkara kejahatan *fraud*. Penelitian ini menggunakan pendekatan yuridis normatif, dengan cara menelaah dan menginterpretasikan hal-hal yang bersifat teoritis yang menyangkut asas, konsepsi, doktrin dan norma hukum yang berkaitan dengan penghadiran bukti digital forensik dalam perkara kejahatan *fraud*. Hasil penelitian menunjukkan bahwa Pengaturan Digital Forensik dalam menganalisis barang bukti digital dalam hal pembuktian tindak pidana tidak secara khusus diatur dalam Kitab Undang-Undang Hukum Acara Pidana (KUHP) karena pengecualian tentang alat bukti elektronik/digital diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) sehingga yang dapat menjadi dasar hukum digital forensik. Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik pada Pasal 5 telah secara jelas menyebutkan bahwa Informasi Elektronik merupakan alat bukti hukum yang sah berupa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya. Maraknya tindak pidana data *fraud* ini, membutuhkan suatu pengaturan hukum yang diharapkan mampu mencegah dan mengurangi tindak pidana tersebut. Oleh karena ini, penting kiranya mengelaborasi pengaturan hukum baik implementasi maupun sanksi pidana terkait data *fraud* di Indonesia.

Kata kunci : Digital forensik, Pembuktian, Kejahatan *fraud*

Abstract. The problems in this research are regulate digital forensic law in proving crime in Indonesia, judges consider the presence of digital forensic evidence in fraud crime. This research uses normative juridical approach, by examining and interpreting matters relating theoretical principles, conceptions, doctrines and legal norms relating to the presence of forensic digital evidence. The result showed that digital Forensic Arrangements in analyzing digital evidence in terms of proving criminal acts are not specifically regulated in the Criminal Procedure Code (KUHP) because exceptions to electronic / digital evidence are regulated in the Information and Electronic Transaction (ITE) Act so that can be a legal basis for digital forensics. Law No. 11 of 2008 on Information and Electronic Transactions on Article 5 has been clearly stated that electronic information is a valid legal evidence in the form of electronic information and / or electronic documents and / or printout. The rise of data fraud requires a legal arrangement that is expected to be able to prevent and reduce these crimes. For this reason, it is important to elaborate legal arrangements for both implementation and criminal sanctions related to data fraud in Indonesia.

Keyword : Digital forensics , Verification, Fraud crime

PENDAHULUAN

Kini lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber atau *cyber law*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*), dan hukum mayantara.¹ Dalam perkembangannya teknologi informasi dan komunikasi menciptakan suatu dunia tersendiri yang sering disebut dunia maya (*cyberspace*) yang menjadi bagian dari berbagai penemuan dibidang teknologi informasi dan komunikasi yang saat ini memungkinkan orang untuk menggunakan jaringan internet melalui komputer pribadi (*personal computer*) atau media elektronik lainnya di manapun.² Dimana teknologi tersebut dapat juga digunakan untuk menciptakan atau menjadi sarana efektif bagi terjadinya perbuatan-perbuatan melawan hukum. Permasalahan hukum yang sering dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian perbuatan hukum yang dilaksanakan melalui sistem elektronik memiliki tingkat kesulitan tersendiri.³ Kecanggihan teknologi komputer disadari telah memberikan kemudahan, terutama dalam membantu pekerjaan manusia. Selain itu, perkembangan teknologi komputer menyebabkan munculnya kejahatan-kejahatan baru, yaitu dengan memanfaatkan komputer sebagai modus operandinya.

¹ Budi Suharyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime), Urgensi Pengaturan dan Celah Hukumnya*, (Jakarta: Rajawali Prers, 2012), hlm.3.

² Sigid Suseno, *Yuridiksi Tindak Pidana Siber*, (Bandung: Refika Aditama, 2012), hlm.1.

³ Budi Suharyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime), Urgensi Pengaturan dan Celah Hukumnya*, (Jakarta: Rajawali Prers, 2012), hlm.3.

Penyalahgunaan komputer dalam perkembangannya menimbulkan persoalan yang sangat rumit, terutama kaitannya dengan proses pembuktian pidana. Penggunaan komputer sebagai media untuk melakukan kejahatan memiliki tingkat kesulitan tersendiri dalam pembuktiannya. Hal ini dikarenakan komputer sebagai media memiliki karakteristik tersendiri atau berbeda dengan kejahatan konvensional yang dilakukan tanpa komputer.⁴ Dalam penanganannya sering membutuhkan forensik, yang merupakan kegiatan untuk melakukan investigasi dan menetapkan fakta yang berhubungan dengan kejadian kriminal dan permasalahan hukum lainnya. Menurut ahli digital forensik Muhammad Nuh Al-Azhar, komputer forensik atau digital forensik merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum, yang dalam hal ini adalah untuk membuktikan kejahatan berteknologi tinggi secara ilmiah sehingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut.⁵ Tindakan kejahatan *fraud* Menurut *Association of Certified Fraud Examiners* (ACFE) tahun 2002, kecurangan adalah tindakan penipuan atau kekeliruan yang dibuat oleh seseorang atau badan yang mengetahui bahwa kekeliruan tersebut dapat mengakibatkan beberapa manfaat tidak baik kepada individu atau entitas atau pihak lain. Rezaee mendefinisikan *fraud* sebagai tindakan melawan hukum, penipuan berencana, dan bermakna ketidakjujuran. *Fraud* dapat terdiri dari berbagai bentuk kejahatan atau tindak pidana kerah putih (*white collar crime*), antara lain pencurian, penggelapan aset, penggelapan informasi, penggelapan kewajiban, penghilangan atau penyembunyian fakta, rekayasa fakta termasuk korupsi. Sedangkan *computer fraud* adalah perbuatan melawan hukum yang dilakukan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Konsep *fraud triangle* pertama kali dikemukakan oleh Donald Cressey. *Fraud triangle theory* sebagai dasar teori utama dalam penelitian ini. Teori *Fraud Triangle Cressey* (1953) dalam Tuanakotta (2007), kecurangan (*fraud*) disebabkan oleh 3 faktor, yaitu (1) Tekanan (*pressure*) adalah motivasi dari individu karyawan untuk bertindak *fraud* dikarenakan adanya tekanan baik keuangan dan non keuangan dari pribadi maupun tekanan dari organisasi, (2) Peluang (*opportunity*) adalah peluang terjadinya *fraud* akibat lemah atau tidaknya efektifitas kontrol sehingga membuka peluang terjadinya *fraud*.

Secara global Indonesia merupakan negara dengan tindak pidana *credit card fraud* tertinggi kedua setelah Ukraina. Kerugian-kerugian akibat *credit card fraud* menjadi penyebab munculnya reaksi negatif dari negara-negara lain dalam transaksi bisnis secara *online*. Data dari kepolisian Republik Indonesia menyebutkan bahwa dari rata-rata 200 kasus *cyber crime* yang ditangani, pada umumnya didominasi oleh *credit card fraud* dengan sasaran luar negeri seperti Amerika Serikat, Australia dan Kanada dengan pelaku berasal dari kota-kota besar seperti Yogyakarta, Bandung, Jakarta, Semarang, Medan dan Riau.⁶ Maraknya tindak pidana *credit/debit card fraud* ini, membutuhkan suatu pengaturan hukum yang diharapkan mampu mencegah dan mengurangi tindak pidana tersebut. Oleh karena ini, penting kiranya mengelaborasi pengaturan hukum baik implementasi maupun sanksi pidana terkait *credit/debit card fraud* di Indonesia. Dengan demikian dalam prakteknya, pembuktian dalam hukum pidana merupakan sesuatu yang sangat vital perannya, mengingat dalam KUHAP (Kitab Undang-Undang Acara Pidana) peran suatu bukti sangat berpengaruh kepada pertimbangan hakim. Setiap kendala yang muncul membuat penegak hukum menjadi bingung untuk menyimpulkan suatu perkara dalam bidang Teknologi Informasi, yang mana bentuk barang bukti berbentuk digital.

METODE

Dalam rangka melakukan sebuah penelitian, metodologi menjadi sesuatu yang mutlak dalam rangka menemukan jawaban dari permasalahan yang diajukan di dalam penelitian. Berdasarkan hal tersebut, maka metode penelitian pada penelitian ini adalah sebagai berikut :

1. Metode Pendekatan

Adapun pendekatan yang digunakan adalah yuridis normatif. Pendekatan dilakukan dengan cara menelaah dan menginterpretasikan hal-hal yang bersifat teoritis yang menyangkut asas, konsepsi, doktrin dan norma hukum yang berkaitan dengan penghadiran bukti digital forensik dalam perkara kejahatan *fraud*.

2. Spesifikasi Penelitian

Penelitian yang penulis lakukan bersifat deskriptif analitis yaitu menggambarkan, menganalisis, menyimpulkan masalah-masalah yang menjadi objek penelitian, yakni penghadiran bukti digital forensik dalam perkara kejahatan *fraud*.

3. Jenis dan Sumber Data

Bahan hukum yang dikaji dan yang dianalisis dalam penelitian ini menggunakan data sekunder, meliputi :

⁴ Maskun, *Kejahatan Siber (Cyber Crime) Suatu Pengantar*, (Makassar: Kencana Prenada Media Group, 2012) (Jakarta: Rajawali Press, 2013), hlm.17.

⁵ Muhammad Nuh Al-Azhar, *Digital Forensic: Panduan Praktis Investigasi Komputer*, (Jakarta: Salemba Infotek, 2012), hlm.19.

⁶ Sigid Suseno. (2012). *Yurisdiksi Tindak Pidana Siber*, (Bandung: Refika Aditama), hlm.29.

- a. Bahan Hukum Primer
Bahan hukum primer merupakan bahan hukum yang mengikat atau yang membuat orang taat pada hukum seperti peraturan perundang-undangan, dan putusan hakim. Bahan hukum primer yang penulis gunakan di dalam penulisan ini.
 - b. Bahan Hukum Sekunder
Bahan hukum sekunder biasanya berupa pendapat hukum / doktrin/ teori-teori yang diperoleh dari literatur hukum, hasil penelitian, artikel ilmiah, maupun website yang terkait dengan penelitian. Bahan hukum sekunder pada dasarnya digunakan untuk memberikan penjelasan terhadap bahan hukum primer. Dengan adanya bahan hukum sekunder maka peneliti akan terbantu untuk memahami/menganalisis bahan hukum primer.
 - c. Bahan Hukum Tersier
Bahan hukum tersier adalah bahan hukum yang mendukung bahan hukum primer dan bahan hukum sekunder dengan memberikan pemahaman dan pengertian atas bahan hukum lainnya. Bahan hukum yang dipergunakan oleh penulis adalah Kamus Besar Bahasa Indonesia dan Kamus Hukum.
4. Teknik Pengumpulan Data
Teknik untuk mengkaji dan mengumpulkan ketiga bahan hukum itu, yaitu menggunakan studi dokumenter. Studi dokumenter merupakan studi yang mengkaji tentang berbagai dokumen, baik yang berkaitan dengan peraturan perundang-undangan maupun dokumen-dokumen yang sudah ada.
5. Analisis Data
Teknis analisis yang digunakan adalah metode analisis normatif kualitatif. Metode secara normatif kualitatif ini berdasarkan bahan hukum primer sebagai hukum positif, kemudian dianalisis secara kualitatif, yaitu dilakukan analisis yang bersifat yuridis.

HASIL DAN PEMBAHASAN

Pengaturan hukum digital forensik dalam sistem pembuktian tindak pidana di Indonesia.

Sistem pembuktian di era teknologi informasi sekarang ini menghadapi tantangan besar yang memerlukan penanganan serius. Pembuktian dalam hukum pidana merupakan sub sistem kebijakan kriminal sebagai *science of response* yang mencakup berbagai disiplin ilmu. Hal ini disebabkan oleh luasnya kuasa dan motif berkembangnya jenis kejahatan yang berbasis teknologi informasi. Penggunaan transaksi elektronik yang tidak menggunakan kertas dalam sistem pembayaran menimbulkan permasalahan khususnya terkait dengan ketentuan pembuktian sebagaimana diatur dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHP). Sedangkan dalam Pasal 186 Kitab Undang-Undang Hukum Perdata disebutkan alat-alat bukti terdiri atas : bukti tulisan, bukti dengan saksi-saksi, persangkaan, pengakuan dan sumpah.⁷

Pembuktian merupakan tahap yang menentukan dalam proses perkara, karena dari hasil pembuktian dapat diketahui benar atau tidaknya suatu dakwaan atau tuntutan tersebut dengan menunjuk pada alat bukti. Alat bukti adalah segala sesuatu yang ada hubungannya dengan suatu perbuatan, dimana dengan alat-alat bukti tersebut, dapat dipergunakan sebagai bahan pembuktian guna menimbulkan keyakinan hakim atas kebenaran adanya suatu tindak pidana yang telah dilakukan terdakwa. Pembuktian sendiri ialah perbuatan membuktikan, membuktikan berarti memberi atau memperlihatkan bukti, melakukan sesuatu sebagai kebenaran, melaksanakan, menandakan, menyaksikan, dan meyakinkan.⁸

Sistem Hukum Pembuktian

Di dalam literatur hukum acara Indonesia dikenal 4 teori sistem pembuktian yaitu :

1. Sistem Pembuktian *Conviction In Time*, pembuktian yang menyandarkan pada keyakinan hakim semata. Keyakinan dapat disimpulkan hakim dari alat-alat bukti yang diperiksanya dalam persidangan dan dapat juga hasil pemeriksaan alat-alat bukti itu diabaikan hakim, dan langsung menarik keyakinan dari keterangan atau pengakuan terdakwa.⁹
2. Sistem Pembuktian *Conviction In Raison*, menurut sistem ini satu putusan tentang bersalah atau tidaknya terdakwa adalah didasarkan kepada motivasi keyakinan yang dituntut oleh dasar-dasar pembuktian, disertai dengan satu kesimpulan yang berdasarkan kepada peraturan-peraturan pembuktian tertentu, dalam hal menentukan keyakinannya itu, hakim bebas secara sadar untuk memilih alasan-alasan menurut pembuktian yang diikutinya.¹⁰

⁷ Dikdik M.Arief Mansur dan Elisatris Gultom., *Cyber Law Aspek Hukum Teknologi Informasi*, (Bandung:Refika Aditama, 2005), Hlm.97.

⁸ Eddy O.S. Hiarij, *Teori & Hukum Pembuktian*, (Jakarta: Erlangga, 2012), Hlm.3.

⁹ Reda Manthovani, *Problematika dan Solusi Penanganan Kejahatan Cyber di Indonesia*, (Jakarta: Malibu, 2006), hlm.38.

¹⁰ Nikolas Simanjuntak, *Acara Pidana Indonesia Dalam Sirkus Hukum*, (Jakarta, Ghalia Indonesia, 2009), hlm. 242.

3. Sistem Pembuktian Positif, pembuktian yang menyandarkan diri pada alat bukti yang telah ditentukan oleh undang-undang. Disebut positif karena jika seorang terdakwa bisa dinyatakan bersalah melakukan tindak pidana hanya didasarkan pada alat bukti yang sah yang disebut dalam undang-undang.
4. Sistem Pembuktian Negatif, di dalam mengambil keputusan tentang salah atau tidaknya seorang terdakwa, Hakim terikat oleh alat bukti yang ditentukan oleh undang-undang dan keyakinan (nurani) hakim sendiri.

Sistem Pembuktian Berdasarkan KUHAP

Dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP) sistem pembuktian diatur dalam Pasal 183 yang berbunyi: “Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwa yang bersalah melakukannya”. Dari bunyi pasal tersebut, dapat dikatakan bahwa KUHAP menganut sistem “pembuktian menurut undang-undang secara negatif”.

Alat Bukti Menurut KUHAP

Unsur Alat bukti yang sah berdasarkan undang-undang secara jelas diatur dalam pasal 184 ayat 1 KUHAP, yaitu :

1. Keterangan Saksi

Pasal 1 angka 27 KUHAP menjelaskan apa itu Keterangan Saksi. Keterangan saksi sebagai alat bukti ialah apa yang saksi nyatakan di sidang pengadilan (pasal 185 ayat (1) KUHAP) dan keterangan saksi yang telah disumpah (pasal 185 ayat (7) KUHAP), dipersamakan dengan keterangan saksi.

Berdasarkan Pasal 1 angka 26 KUHAP dinyatakan “Saksi adalah orang yang dapat memberikan keterangan guna kepentingan penyidikan, penuntutan, dan peradilan tentang perkara pidana yang ia dengar sendiri, ia lihat sendiri, dan ia alami sendiri”. Sementara itu Keterangan Saksi menurut Pasal 1 angka 27 KUHAP, “keterangan saksi adalah salah satu alat bukti dalam perkara pidana yang berupa keterangan dari saksi mengenai suatu peristiwa pidana yang ia dengar sendiri, ia lihat sendiri, dan ia alami sendiri dengan menyebut alasan dari pengetahuannya itu”. Saksi dituntut untuk memberikan keterangan yang sebenarnya atau paling tidak mendekati dari peristiwa yang dia lihat, untuk memberikan pemahaman pada hakim dalam memberikan putusan kepada pelaku tindak pidana.

2. Keterangan Ahli

Pengertian Keterangan Ahli terdapat dalam Pasal 1 butir 28 KUHAP. Dalam proses pembuktian, keterangan-keterangan ahli yang memiliki nilai pembuktian adalah apa yang dinyatakan dalam sidang pengadilan (Pasal 186 KUHAP). Di Dalam Pasal 186 KUHAP menyatakan bahwa “keterangan seorang ahli ialah apa yang seorang ahli nyatakan di sidang pengadilan”. Menurut penjelasan Pasal 186 KUHAP dibuat dengan mengingat sumpah di waktu ia menerima jabatan atau pekerjaan. Merujuk pada ketentuan dalam KUHAP, keahlian dari seorang yang memberikan keterangan ahli tidak hanya berdasarkan pengetahuan yang ia miliki melalui pendidikan formal, namun keahlian itu juga dapat diperoleh berdasarkan pengalamannya.

3. Surat

Surat yang dapat dinilai sebagai alat bukti yang sah adalah yang dibuat atas sumpah jabatan atau yang dikuatkan dengan sumpah (Pasal 187 KUHAP). Menurut Pasal 187 KUHAP, Surat sebagaimana tersebut pada Pasal 184 ayat (1) huruf c, dibuat atas sumpah jabatan atau dikuatkan dengan sumpah, jenis surat yang dimaksud adalah :

- 1) 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.
- 2) Surat yang dibuat menurut ketentuan peraturan perundang-undangan atau surat yang dibuat oleh pejabat mengenal hal yang termasuk dalam tata laksana yang menjadi tanggung jawabnya dan yang diperuntukkan bagi pembuktian sesuatu hal atau sesuatu keadaan.
- 3) Surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai sesuatu hal atau sesuatu keadaan yang diminta secara resmi dan padanya.
- 4) Surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain.

4. Petunjuk

Alat bukti petunjuk adalah perbuatan kejadian atau keadaan yang mempunyai persesuaian antara yang satu dengan yang lain atau dengan tindak pidana itu sendiri, yang menunjukkan adanya suatu tindak dan seseorang sebagai pelakunya (Pasal 188 KUHAP). Alat bukti petunjuk dapat diperoleh melalui saksi, surat dan terdakwa. Pasal 188 KUHAP ayat (1) yang berbunyi “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”. Alat bukti petunjuk merupakan otoritas penuh dan subjektivitas hakim yang memeriksa perkara tersebut. Hakim dalam mengambil kesimpulan tentang pembuktian

sebagai suatu petunjuk haruslah menghubungkan alat bukti yang satu dengan yang lain. Penilaian atas kekuatan pembuktian suatu petunjuk dalam setiap keadaan tertentu dilakukan oleh hakim setelah ia mengadakan pemeriksaan. Syarat-syarat petunjuk sebagai alat bukti harus mempunyai persesuaian satu sama lain atas perbuatan yang terjadi. Selain itu, keadaan-keadaan tersebut berhubungan satu sama lain dengan kejahatan yang terjadi dan berdasarkan pengamatan hakim yang diperoleh dari keterangan saksi, surat dan keterangan terdakwa.

Menurut Adami Chazawi mengungkapkan persyaratan suatu petunjuk adalah sebagai berikut :¹¹

- 1) Adanya perbuatan, kejadian, dan keadaan yang bersesuaian. Perbuatan, Kejadian, dan Keadaan merupakan fakta-fakta yang menunjukkan tentang telah terjadinya tindak pidana, menunjukkan terdakwa yang melakukan dan menunjukkan terdakwa bersalah karena melakukan tindak pidana tersebut.
 - 2) Ada dua persesuaian, yaitu bersesuaian antara masing-masing perbuatan, kejadian, dan keadaan satu sama lain ataupun bersesuaian antara perbuatan, kejadian atau keadaan dengan tindak pidana yang didakwakan.
 - 3) Persesuaian yang demikian itu menandakan atau menunjukkan adanya dua hal, yaitu menunjukkan siapa pelakunya. Unsur ini merupakan kesimpulan bekerjanya proses pembentukan alat bukti petunjuk, yang sekaligus merupakan tujuan dari alat bukti petunjuk.
 - 4) Hanya dapat dibentuk melalui tiga alat bukti, yaitu keterangan saksi, surat dan keterangan terdakwa. Sesuai dengan asas minimum pembuktian seperti pada Pasal 183 KUHAP, selayaknya petunjuk juga dihasilkan dari minimal dua alat bukti yang sah.
5. Keterangan Terdakwa

Keterangan terdakwa ialah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang diketahui sendiri atau alami sendiri (Pasal 189 ayat (1) KUHAP).¹² Penerapan pembuktian perkara pidana yang diatur dalam hukum acara pidana selamanya tetap diperlukan sekalipun terdakwa mengakui tindak pidana yang didakwakan kepadanya. Terdakwa dalam Pasal 1 Butir 15 KUHAP adalah seseorang tersangka yang dituntut, diperiksa, dan diadili di sidang pengadilan. Menurut Pasal 189 ayat (1) KUHAP, “Keterangan terdakwa adalah apa yang terdakwa nyatakan di sidang tentang perbuatan yang dilakukan atau yang ia ketahui sendiri atau ia alami sendiri”. Keterangan terdakwa yang diberikan di luar sidang dapat digunakan untuk membantu menemukan bukti di sidang, asalkan keterangan itu didukung oleh suatu alat bukti yang sah sepanjang mengenai hal yang didakwakan kepadanya. Keterangan terdakwa hanya dapat digunakan terhadap dirinya sendiri, hal ini menunjuk pada Pasal 189 ayat (4) KUHAP “Keterangan terdakwa saja tidak cukup untuk membuktikan bahwa ia bersalah melakukan perbuatan yang didakwakan kepadanya”. Bahwa seorang terdakwa tidak dibebani kewajiban dalam pembuktian, jadi keterangan terdakwa yang sah adalah keterangan dinyatakan di sidang pengadilan.

Alat Bukti Diluar KUHAP

1. Alat bukti dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) Undang-undang yang mengatur mengenai cyberspace yaitu Undang-Undang No. 11 Tahun 2008 Jo Undang-Undang No.19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Di dalam Undang-undang tersebut alat bukti mengalami perluasan yang digunakan sebagai pembuktian dalam mengungkap suatu tindak pidana, yaitu alat bukti elektronik sebagai bukti yang sah secara hukum.

Pasal 5 ayat (1) Undang-Undang ITE sudah mengakomodasi informasi dan dokumen elektronik tersebut sebagai alat bukti hukum yang sah, terlepas dari Pasal 184 KUHAP yang membuat penggolongan alat bukti yang sah, ini dijelaskan di Pasal 5 ayat (2) Undang-Undang ITE. Hal ini juga diperkuat pada pasal 44 huruf (b) bahwa informasi elektronik dan dokumen elektronik merupakan alat bukti lain, selain alat bukti yang sebagaimana dimaksud dalam ketentuan perundang-undangan yang ada.

Berdasarkan Pasal 1 ayat (1) Undang-Undang ITE menjelaskan bahwa Informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, elektronik 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”. Kemudian dalam Pasal 1 ayat (4) menjelaskan bahwa: “Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirim, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tapi 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”.

2. Undang-undang No.20 Tahun 2001 tentang Perubahan Undang-Undang No. 31 Tahun 1999 tentang Tindak Pidana Korupsi. Alat bukti Informasi elektronik terdapat dalam (Pasal 26A).

¹¹ Eddy O.S. Hiariej, *Teori & Hukum Pembuktian*, (Jakarta:Erlangga, 2012), hlm.110.

¹² Ibid, hal.7.

3. Undang-Undang Tindak Pidana Pencucian Uang yang mana dalam pasal 38 jo Pasal 1 butir 7 Undang undang No.15 Tahun 2002 jo Pasal 1 butir 9 Undang- undang No.25 tahun 2003 tentang Tindak Pidana Pencucian Uang mengatur tentang alat bukti berupa informasi elektronik.
4. Undang-Undang No.15 Tahun 2003 tentang Tindak Pidana Terorisme mengatur alat bukti dalam Pasal 27.
5. Undang-Undang No.17 Tahun 2006 Tentang Kepabeanan Dalam penjelasan Pasal 5A ayat (1) dapat juga ditemukan data elektronik sebagai alat bukti.

Sedangkan saksi dalam perkara cybercrime melibatkan orang yang melihat dan menguasai dunia maya yang keterangannya dapat dijadikan pertimbangan hakim dalam mengungkap fakta di persidangan, hal ini diatur dalam Pasal 7 Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang berbunyi “Setiap orang yang menyatakan hak, memperkuat hak yang telah ada, atau menolak hak orang lain berdasarkan adanya Informasi Elektronik dan/atau Dokumen Elektronik harus memastikan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang ada padanya berasal dari sistem Elektronik yang memenuhi syarat berdasarkan peraturan perundang-undangan”. Dalam Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, seorang saksi dapat menggunakan media elektronik untuk memberikan keterangan nya, sehingga tidak harus datang langsung ke pengadilan sehingga bisa melalui media komunikasi berdasarkan pada Pasal 44 Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik menyebutkan “Alat bukti penyidikan penuntutan dan pemeriksaan sidang pengadilan menurut ketentuan undang-undang ini adalah sebagai berikut : alat bukti sebagaimana dimaksud dalam ketentuan perundang-undangan, alat bukti berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3)”.

Alat bukti surat yang dipakai dalam pembuktian cyber crime merupakan alat bukti yang sah sepanjang itu sesuai dengan sistem elektronik yang diatur dalam undang-undang yang mengaturnya, karena alat bukti surat terlebih yang berbentuk digital dapat diubah keasliannya dalam hitungan detik dan tanpa harus memegang barang bukti yang ditunjukan di persidangan. Dengan demikian dapat diketahui bahwa surat merupakan alat bukti yang sah sesuai dengan pasal 5 ayat (1) Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik Serta merujuk pada pertimbangan hakim yang bersangkutan.

Dengan merujuk pada arti kata bukti, yakni sesuatu yang menyatakan kebenaran suatu peristiwa, Penulis berpendapat bahwa arti penting pembuktian adalah mencari kebenaran atas suatu peristiwa. Dalam konteks hukum, arti penting pembuktian adalah mencari kebenaran suatu peristiwa hukum. Peristiwa hukum adalah peristiwa yang mempunyai akibat hukum. Jadi, dapat dimengerti bahwa pembuktian dilihat dari perspektif hukum acara pidana, yakni ketentuan yang membatasi sidang pengadilan dalam usaha mencari dan mempertahankan kebenaran, baik oleh hakim, penuntut umum, terdakwa maupun penasehat hukum, semuanya terikat pada ketentuan dan tata cara, serta penilaian alat bukti yang ada pada Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Peranan digital forensik dalam menganalisis barang bukti digital

Peran digital forensik dalam membantu pembuktian suatu kejahatan secara digital sangatlah penting, namun digital forensik bukan hanya dapat digunakan untuk mengungkap bukti kejahatan digital tapi kejahatan konvensional yang memiliki barang bukti elektronik/digital. Tentunya digital forensik penting untuk menganalisis barang bukti elektronik dari kejahatan komputer dan/atau kejahatan terkait komputer. Kejahatan terkait komputer adalah segala jenis macam kejahatan tradisional seperti pencurian, perampokan, pembunuhan, korupsi, narkoba, dan lain-lain. Sedangkan kejahatan komputer merupakan kejahatan yang menggunakan komputer sebagai alat utama untuk melakukan aksi kejahatannya, misalnya defacement (pengubahan halaman-halaman suatu situs secara ilegal), denial distributed of service (membuat suatu sistem tidak berjalan atau berfungsi sebagaimana mestinya), keylogging (merekam setiap aktivitas pengetikan di keyboard dan aplikasi yang tertampil di layar), identity theft (pencurian data-data penting dari orang-orang yang menjadi target), intrusion (masuk secara ilegal ke dalam suatu sistem), dan lain-lain.¹³

Dalam Digital forensik ada prinsip-prinsip yang harus diikuti, agar menjamin analisis terhadap barang bukti dijamin keasliannya dan dapat diterima dalam persidangan, antara lain:

1. Prinsip dasar pertama

Sebuah media penyimpanan seperti harddisk, floppy disk, dan flashdisk yang merupakan barang bukti harus dijaga keutuhannya sesuai dengan prinsip Chain of custody, ini dimaksudkan agar informasi digital yang tersimpan di media tersebut tetap ada dan terjaga keutuhannya hingga bisa dibawa ke pengadilan, serta bisa dipertanggungjawabkan asal-usulnya, khususnya dari kemungkinan adanya rekayasa data digital.

2. Prinsip kedua

¹³ Muhammad Nuh Al-Azhar, *Digital forensik : Panduan Praktis Investigasi Komputer*, (Jakarta:Salemba Infotek, 2012),hlm.3.

Seorang investigator dan analis forensik yang akan memeriksa dan menganalisis media penyimpanan barang bukti harus memiliki kompetensi yang jelas, baik melalui jalur formal maupun non-formal. Dengan begitu diharapkan bahwa mereka dapat menjelaskan, baik secara teknis maupun praktis alasan-alasan mereka dalam melakukan tindakan-tindakan terhadap media penyimpanan barang bukti.

3. Prinsip Ketiga

Adanya catatan teknis dan praktis terhadap langkah-langkah yang diterapkan terhadap media penyimpanan barang bukti selama pemeriksaan dan analisis berlangsung, sehingga ketika barang bukti tersebut diperiksa oleh pihak ketiga maka seharusnya pihak ketiga tersebut akan mendapatkan hasil yang sama dengan hasil yang telah dilakukan oleh investigator atau analis forensik sebelumnya.

4. Prinsip Keempat

Seseorang yang bertanggung jawab terhadap investigasi kasus maupun pemeriksaan dan analisis barang bukti elektronik harus dapat memastikan bahwa proses yang berlangsung sesuai dengan hukum yang berlaku dan prinsip-prinsip dasar sebelumnya dan dapat diaplikasikan dengan baik. Ini dimaksudkan agar hasil pemeriksaan dan analisis terhadap media penyimpanan barang bukti elektronik yang berupa data digital tidak bertentangan dengan hukum positif yang berlaku sehingga dapat diterima secara teknis dan hukum oleh majelis hakim di persidangan.¹⁴

Menurut Kemmish yang dikutip Asrizal, ada empat tahapan pada proses implementasi digital forensik, yaitu:

1. Identifikasi Bukti Digital

Merupakan tahapan paling awal dalam forensik. Pada tahapan ini dilakukan identifikasi dimana bukti itu berada, dimana bukti itu disimpan, dan bagaimana penyimpanannya untuk mempermudah tahapan selanjutnya. Media digital yang bisa dijadikan sebagai barang bukti mencakup sebuah sistem komputer, media penyimpanan (seperti *flashdisk*, *pen drive*).

2. Penyimpanan Bukti Digital

Termasuk ke tahap yang paling kritis dalam forensik. Pada tahapan ini, bukti digital dapat saja hilang karena penyimpanannya kurang baik. Penyimpanan ini lebih menekankan bahwa bukti digital pada saat ditemukan akan tetap, tidak berubah baik bentuk, isi, makna, dan sebagainya dalam jangka waktu yang lama. ini adalah konsep ideal dari penyimpanan bukti digital.

3. Analisa Bukti Digital

Bukti yang telah didapatkan perlu di-explore kembali ke dalam sejumlah skenario yang berhubungan dengan tindak pengusutan. Termasuk juga pengecekan pada metadata. Kebanyakan file mempunyai metadata yang berisi informasi yang ditambahkan mengenai file tersebut seperti computer name, total edit time, jumlah editing session, dimana dicetak, beberapa kali terjadi penyimpanan, tanggal dan waktu modifikasi. Selanjutnya melakukan *recovery* dengan mengembalikan file dan folder yang terhapus, unformat drive, membuat ulang partisi, mengembalikan password, merekonstruksi ulang halaman web yang pernah dikunjungi, mengembalikan email-email yang terhapus dan seterusnya. Tahapan analisis terbagi dua yaitu analisis media dan analisis aplikasi pada barang bukti yang ada.

Keberadaan barang bukti sangat penting dalam investigasi kasus-kasus computer crime maupun computer-related crime karena dengan barang bukti inilah investigator dan forensic analyst dapat mengungkap kasus-kasus tersebut dengan kronologis yang lengkap, untuk kemudian melacak keberadaan pelaku dan menangkapnya. Oleh karena posisi barang bukti ini sangat strategis, investigator dan forensic analyst harus paham jenis-jenis barang bukti. Diharapkan ketika ia datang ke TKP yang berhubungan dengan kasus computer crime dan computer-related crime, ia dapat mengenali keberadaan barang bukti tersebut untuk kemudian diperiksa dan dianalisa lebih lanjut. Barang bukti elektronik. Barang bukti ini bersifat fisik dan dapat dikenali secara visual, oleh karena itu investigator dan forensic analyst 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 :

- a. Komputer PC, laptop/notebook, netbook, tablet.
- b. Handphone, smartphone.
- c. Flashdisk/thumb drive.
- d. Floppy disk.
- e. Harddisk.
- f. CD/DVD.
- g. Router, switch, hub.

¹⁴ Muhammad Nuh Al-Azhar, *Digital Forensic: Panduan Praktis Investigasi Komputer*, (Jakarta: Salemba Infotek, 2012), hlm.19-24.

- h. Kamera video, cctv.
- i. Kamera digital.
- j. Digital recorder.
- k. Music/video player

4. Presentasi

Adalah proses persidangan dimana bukti digital akan diuji otentifikasi dan korelasinya dengan kasus yang ada. Presentasi disini berupa penunjukan bukti digital yang berhubungan dengan kasus yang disidangkan. Presentasi dilakukan dengan menyajikan dan menguraikan secara detail laporan penyelidikan dengan bukti-bukti yang sudah dianalisa secara mendalam dan dapat dipertanggungjawabkan secara umum di pengadilan. Laporan yang disajikan harus di crosscheck langsung dengan saksi yang ada, baik saksi yang terlibat langsung maupun tidak langsung.¹⁵

Pertimbangan hakim atas penghadiran bukti digital forensik dalam perkara kejahatan *fraud*.

Pertimbangan hakim merupakan salah satu aspek terpenting dalam menentukan terwujudnya nilai dari suatu putusan hakim yang mengandung keadilan (*ex aequo et bono*) dan mengandung kepastian hukum, di samping itu juga mengandung manfaat bagi para pihak yang bersangkutan sehingga pertimbangan hakim ini harus disikapi dengan teliti, baik, dan cermat. Apabila pertimbangan hakim tidak teliti, baik, dan cermat, maka putusan hakim yang berasal dari pertimbangan hakim tersebut akan dibatalkan oleh Pengadilan Tinggi Mahkamah Agung. Dalam pemeriksaan suatu perkara juga memerlukan adanya pembuktian, dimana hasil dari pembuktian itu akan digunakan sebagai bahan pertimbangan dalam memutus perkara. Pembuktian merupakan tahap yang paling penting dalam pemeriksaan di persidangan. Pembuktian bertujuan untuk memperoleh kepastian bahwa suatu peristiwa / fakta yang diajukan itu benar-benar terjadi, guna mendapatkan putusan hakim yang benar dan adil. Hakim tidak dapat menjatuhkan suatu putusan sebelum nyata baginya bahwa peristiwa / fakta tersebut benar-benar terjadi, yakni dibuktikan kebenarannya, sehingga nampak adanya hubungan hukum antara para pihak. Selain itu, pada hakikatnya pertimbangan hakim hendaknya juga memuat tentang hal-hal sebagai berikut :

1. Pokok persoalan dan hal-hal yang diakui atau dalil-dalil yang tidak disangkal.
2. Adanya analisis secara yuridis terhadap putusan segala aspek menyangkut semua fakta/hal-hal yang terbukti dalam persidangan.
3. Adanya semua bagian dari petitum Penggugat harus dipertimbangkan/diadili secara satu demi satu sehingga hakim dapat menarik kesimpulan tentang terbukti/tidaknya dan dapat dikabulkan/tidaknya tuntutan tersebut dalam amar putusan.

Menurut Wiryono Kusumo, Pertimbangan atau yang sering disebut juga *considerans* merupakan dasar putusan Hakim atau argumentasi Hakim dalam memutuskan suatu perkara. Jika argumen hukum itu tidak benar dan tidak sepantasnya, maka orang kemudian dapat menilai bahwa putusan itu tidak benar dan tidak adil. Kemudian menurut Sudikno Mertokusumo, secara sederhana putusan hakim mencakup irah-irah dan kepala putusan, pertimbangan, dan amar. Dari cakupan itu, yang dipandang sebagai dasar putusan adalah pertimbangan. Alasan-alasan yang kuat dalam pertimbangan sebagai dasar putusan membuat putusan sang hakim menjadi objektif dan berwibawa.¹⁶ Sehingga dapat dikatakan dasar pertimbangan merupakan, argumen yang menjadi dasar/bahan untuk menyusun pertimbangan majelis hakim sebelum majelis hakim membuat analisa hukum yang kemudian digunakan untuk menjatuhkan putusan kepada terdakwa, dasar pertimbangan hakim itu sendiri memiliki kedudukan yang penting di dalam suatu putusan yang dibuat oleh hakim sebab semakin baik dan tepat pertimbangan yang digunakan oleh hakim dalam sebuah putusan, akan mencerminkan sejauh mana rasa keadilan yang ada di dalam diri si hakim yang membuat putusan tersebut. Selain itu berkaitan dengan keadilan itu sendiri kedudukan seorang hakim yang memiliki tugas mengadili dan memutus perkara haruslah benar-benar bisa dipercaya, adil dan tidak memihak di dalam mengadili dan memutus suatu perkara. Oleh sebab itu maka, keobyektifan hakim dalam mengadili perkara, tanggung jawab hakim terhadap putusannya, serta kebebasan hakim dalam mengadili dan memutus perkara menjadi faktor-faktor yang perlu diperhatikan juga.

Sebelum diundangkannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, penegakan hukum terhadap tindak pidana *fraud* di Indonesia dilakukan melalui Kitab Undang-Undang Hukum Pidana (KUHP), yaitu pasal 263-276 tentang pemalsuan, pasal 362-367 tentang pencurian, dan pasal 378-395 tentang penipuan. Sejatinya, pasal-pasal ini merupakan antisipasi kejahatan-kejahatan konvensional, dan agak sulit untuk diterapkan pada kejahatan *cyber*.

¹⁵ <http://gajehaje.blogspot.com/2015/11/digital-forensik-tahapan-prosedur.html> Diakses 08 Februari 2021.

¹⁶ Sudikno Mertokusumo, *Mengenal Hukum : Suatu Pengantar*, (Yogyakarta:Liberty, 2005), hlm.22.

Pertimbangan hakim dalam mengungkap fakta di persidangan dengan menggunakan alat bukti digital ialah pada Pasal 5 ayat (1) Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik¹⁷ menjelaskan “Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah”. Untuk mengungkap alat bukti digital maka hakim memerlukan saksi ahli dalam menjelaskan alat bukti tersebut seperti yang tercantum pada Pasal 1 angka 1 dan angka 4 yang menjelaskan “angka 1 : 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, angka 4 : Dokumen Elektronik 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. Majelis Hakim membutuhkan alat bukti digital dalam perkara cyber crime dan peran saksi ahli dalam menguatkan peran kedudukan alat bukti digital tersebut, karena dalam Pasal 1 angka 1 dan angka 4 Undang-Undang No. 11 tahun 2008 menjelaskan bahwa Informasi Elektronik dan Dokumen Elektronik hanya bisa dipahami oleh orang yang mampu memahaminya, orang yang mampu memahaminya berarti mempunyai keahlian dalam bidang Informasi dan Transaksi Elektronik, dalam hal ini disebut saksi ahli. Karena kedudukan alat bukti digital dalam putusan mempengaruhi pertimbangan hakim untuk membuat putusan.

Alat bukti digital adalah Informasi Elektronik dan/atau Dokumen Elektronik yang memenuhi persyaratan formil dan persyaratan materiil yang diatur dalam Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Barang bukti dapat dikatakan alat bukti digital karena berbentuk Informasi Elektronik dan/atau Dokumen Elektronik yang sesuai dengan kriteria Pada Pasal 1 angka 1 dan angka 4 Undang-Undang No. 11 tahun 2008 yang meliputi 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 dan 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, yang dalam putusan diatas merupakan alat bukti yang mempunyai kedudukan untuk menjelaskan suatu tindak *cyber crime* yang mungkin dilakukan oleh tersangka, sehingga alat bukti digital ini memperjelas fakta yang terjadi dengan didukung alat bukti lainnya.

Yang membedakan antara Informasi Elektronik dan Dokumen Elektronik ialah sarana yang dipakai dalam pembuktian alat bukti digital tersebut, sesuai dengan Pasal 1 angka 1, Informasi Elektronik hanya terbatas pada orang yang mampu memahami Informasi yang selanjutnya dapat mengartikan Informasi Elektronik tersebut, sedangkan pada Pasal 1 angka 4 menggunakan sarana komputer dan/atau sistem elektronik untuk menerjemahkan Informasi yang ada dalam Dokumen Elektronik. Yang dimaksud Sistem Elektronik ialah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik (Penjelasan Pasal 1 angka 5 Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik). Dalam Pasal 183 KUHAP “Hakim tidak boleh menjatuhkan pidana kepada seorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwa yang bersalah melakukannya”.

Pengertian Fraud

Bologna et al mendefinisikan kecurangan “*Fraud is criminal deception intended to financially benefit the deceiver*” yaitu kecurangan adalah penipuan kriminal yang bermaksud untuk memberi manfaat keuangan kepada si penipu. Kriminal disini berarti setiap tindakan kesalahan serius yang dilakukan dengan maksud jahat. Dari tindakan jahat tersebut ia memperoleh manfaat dan merugikan korbannya secara finansial. Biasanya kecurangan mencakup tiga langkah yaitu (1) tindakan/*the act*, (2) Penyembunyian/*the concealment* dan (3) konversi/*the conversion*.

Sedangkan Razaee mendefinisikan *fraud* sebagai tindakan melawan hukum, penipuan berencana, dan bermakna ketidakjujuran. *Fraud* dapat terdiri dari berbagai bentuk kejahatan atau tindak pidana kerah putih (*white collar crime*), antara lain pencurian, penggelapan aset, penggelapan informasi, penggelapan kewajiban, penghilangan atau penyembunyian fakta, rekayasa fakta termasuk korupsi.¹⁸

¹⁷ Undang-undang Informasi dan Transaksi Elektronik atau Undang-undang nomor 11 tahun 2008.

¹⁸ Kurnia Kusuma Rachmawati, *Pengaruh Faktor-faktor Dalam Perspektif Fraud*, Skripsi, Semarang, 11 Maret 2014

Computer Fraud adalah perbuatan melawan hukum yang dilakukan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis utama komputer dan jaringan telekomunikasi ini dalam beberapa literatur dan prakteknya dikelompokkan dalam beberapa bentuk, antara lain:

1. *Illegal Access/Akses Tanpa Ijin ke Sistem Komputer*

Dengan sengaja dan tanpa hak melakukan akses secara tidak sah terhadap seluruh atau sebagian sistem komputer, dengan maksud untuk mendapatkan data komputer atau maksud-maksud tidak baik lainnya, atau berkaitan dengan sistem komputer yang dihubungkan dengan sistem komputer lain. Hacking merupakan salah satu dari jenis kejahatan ini yang sangat sering terjadi.

2. *Illegal Contents/Konten Tidak Sah*

Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

3. *Data Forgery/Pemalsuan Data*

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi salah ketik yang pada akhirnya akan menguntungkan pelaku.

4. *Spionase Cyber/Mata-mata*

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized*.

5. *Data Theft/Mencuri Data*

Kegiatan memperoleh data komputer secara tidak sah, baik untuk digunakan sendiri ataupun untuk diberikan kepada orang lain. Identity theft merupakan salah satu dari jenis kejahatan ini yang sering diikuti dengan kejahatan penipuan (*fraud*). Kejahatan ini juga sering diikuti dengan kejahatan data leakage.

6. *Misuse of devices/Menyalahgunakan Peralatan Komputer*

Dengan sengaja dan tanpa hak, memproduksi, menjual, berusaha memperoleh untuk digunakan, diimpor, diedarkan atau cara lain untuk kepentingan itu, peralatan, termasuk program komputer, *password* komputer, kode akses, atau data semacam itu, sehingga seluruh atau sebagian sistem komputer dapat diakses dengan tujuan digunakan untuk melakukan akses tidak sah, intersepsi tidak sah, mengganggu data atau sistem komputer, atau melakukan perbuatan-perbuatan melawan hukum lain.

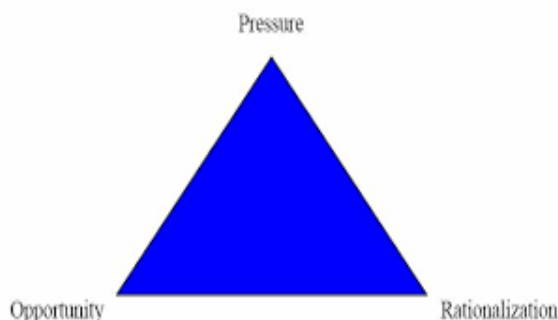
Faktor penyebab kejahatan fraud

Konsep *fraud triangle* pertama kali dikemukakan oleh Donald Cressey. *Fraud triangle theory* sebagai dasar teori utama dalam penelitian ini. Teori *fraud triangle cressey* (1953) dalam Tuanakotta (2007), kecurangan (*fraud*) disebabkan oleh 3 faktor, yaitu (1) Tekanan (*Pressure*) adalah motivasi dari individu karyawan untuk bertindak *fraud* dikarenakan adanya tekanan baik keuangan dan non keuangan dari pribadi maupun tekanan dari organisasi, (2) Peluang (*Opportunity*) adalah peluang terjadinya *fraud* akibat lemah atau tidaknya efektifitas kontrol sehingga membuka peluang terjadinya *fraud*.

Faktor penyebab *fraud* yang disebabkan adanya kelemahan di dalam sistem dimana seseorang mempunyai kuasa atau kemampuan untuk memanfaatkan sehingga perbuatan curang dapat dilakukan, (3) Rasionalisasi (*Rationalization*) adalah *fraud* terjadi karena kondisi nilai-nilai etika lokal yang mendorong (membolehkan) terjadinya *fraud*. Pertimbangan perilaku kecurangan sebagai konsekuensi dari kesenjangan integritas pribadi karyawan atau penalaran moral yang lain. Rasionalisasi terjadi dalam hal seseorang atau sekelompok orang membangun pembenaran atas kecurangan yang dilakukan. Pelaku *fraud* biasanya mencari alasan pembenaran bahwa yang dilakukannya bukan pencurian atau kecurangan.

Fraud atau kecurangan merupakan penipuan yang sengaja dilakukan oleh seseorang atau sekelompok orang sehingga menimbulkan kerugian tanpa disadari oleh pihak yang dirugikan tersebut dan memberikan keuntungan bagi pelaku kecurangan. Kecurangan umumnya terjadi karena tiga hal utama, yaitu adanya tekanan untuk melakukan penyelewengan, adanya kesempatan yang bisa dimanfaatkan serta adanya pembenaran terhadap tindakan tersebut. Pada prinsipnya *fraud* memiliki tiga unsur, yaitu: adanya perbuatan yang melawan hukum (*illegal acts*); dilakukan oleh orang-orang dari dalam dan/atau dari luar organisasi serta dilakukan untuk mendapatkan keuntungan pribadi dan/atau kelompok sementara di lain pihak merugikan pihak lain baik langsung maupun tidak langsung. Soekardi Husodo menyatakan bahwa ada tiga hal yang menyebabkan seseorang melakukan *fraud*, yaitu: *pressure* (tekanan), *opportunity* (kesempatan) dan *rationalization* (pembenaran). Tekanan atau *pressure* umumnya disebabkan karena perilaku individual karyawan yang menyebabkannya melakukan *fraud*. Bisa jadi tekanan itu disebabkan masalah

keuangan (financial pressure) yang dipicu karena gaya hidup yang berlebihan, sikap tamak dan serakah, banyak hutang atau tanggungan dan sebagainya, yang menyebabkan seseorang “terpaksa” melakukan *fraud*.



SIMPULAN

Pengaturan hukum digital forensik dalam sistem pembuktian tindak pidana di Indonesia, pada pembuktian dalam hukum pidana merupakan sub sistem kebijakan kriminal sebagai science of response yang mencakup berbagai disiplin ilmu. Hal ini disebabkan oleh luasnya kuasa dan motif berkembangnya jenis kejahatan yang berbasis teknologi informasi. Penggunaan transaksi elektronik yang tidak menggunakan kertas dalam sistem pembayaran menimbulkan permasalahan khususnya terkait dengan ketentuan pembuktian sebagaimana diatur dalam Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP). Sedangkan dalam Pasal 186 Kitab Undang-Undang Hukum Perdata disebutkan alat-alat bukti terdiri atas : bukti tulisan, bukti dengan saksi-saksi, persangkaan, pengakuan dan sumpah. Menurut Kimmish yang dikutip Asrizal, ada empat tahapan pada proses implementasi digital forensik, yaitu: Identifikasi Bukti Digital, Penyimpanan Bukti Digital, Analisa Bukti Digital, Presentasi. Bukti digital ialah pada Pasal 5 ayat (1) Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik menjelaskan “Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah”. Untuk mengungkap alat bukti digital maka hakim memerlukan saksi ahli dalam menjelaskan alat bukti tersebut seperti yang tercantum pada Pasal 1 angka 1 dan angka 4.

Bologna et al mendefinisikan kecurangan “*Fraud* is criminal deception intended to financially benefit the deceiver” yaitu kecurangan adalah penipuan kriminal yang bermaksud untuk memberi manfaat keuangan kepada si penipu. Kriminal disini berarti setiap tindakan kesalahan serius yang dilakukan dengan maksud jahat. Dari tindakan jahat tersebut ia memperoleh manfaat dan merugikan korbannya secara finansial. Faktor penyebab *fraud* yang disebabkan adanya kelemahan didalam sistem dimana seseorang mempunyai kuasa atau kemampuan untuk memanfaatkan sehingga perbuatan curang dapat dilakukan, (3) Rasionalisasi (*Rationalization*) adalah *fraud* terjadi karena kondisi nilai-nilai etika lokal yang mendorong (membolehkan) terjadinya *fraud*.

DAFTAR PUSTAKA

Buku

- Budi Suharyanto. *Tindak Pidana Teknologi Informasi (Cyber Crime), Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: Rajawali Prers, 2012.
- Sigid Suseno. *Yuridiksi Tindak Pidana Siber*. Bandung: Refika Aditama, 2012.
- Maskun. *Kejahatan Siber (Cyber Crime) Suatu Pengantar*. Makassar: Kencana Prenada Media Group, Jakarta: Rajawali Press, 2012.
- Muhammad Nuh Al-Azhar. *Digital Forensic: Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek, 2012.
- Dikdik M.Arief Mansur. *Elisatris Gultom., Cyber Law Aspek Hukum Teknologi Informasi*. Bandung:Refika Aditama, 2005.
- Reda Manthovani. *Problematika dan Solusi Penanganan Kejahatan Cyber di Indonesia*. Jakarta: Malibu, 2006.
- Nikolas Simanjuntak. *Acara Pidana Indonesia Dalam Sirkus Hukum*. Jakarta:Ghalia Indonesia, 2009.
- Eddy O.S. Hiariej. *Teori & Hukum Pembuktian*. Jakarta:Erlangga, 2012.
- Sudikno Mertokusumo. *Mengenal Hukum : Suatu Pengantar*. Yogyakarta:Liberty, 2005.

Peraturan Perundang-Undang

Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Undang-Undang nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Hasil Penelitian/Tugas Akhir

Kurnia Kusuma Rachmawati, *Pengaruh Faktor-faktor Dalam Perspektif Fraud*, Skripsi, Semarang, 11 Maret 2014.

Internet

<http://gajehaje.blogspot.com/2015/11/digital-forensik-tahapan-prosedur.html>