Sejarah Forensik dan Digital Forensik

Disusun untuk memenuhi tugas ke II, MK. Manajemen Investigasi Tindak Kriminal

(Dosen Pengampu : Yudi Prayudi, S.Si, M.Kom)

Fathirma'ruf

13917213

PROGRAM PASCASARJANA TEKNIK INFORMATIKA

FAKULTAS TEKNIK INDUSTRI

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2014

MATERI

ILMU FORENSIK DAN DIGITAL FORENSIK

1.1. Definisi Forensik

Forensik merupakan sebuah penerapan dari berbagai ilmu pengetahuan yang digunakan untuk menjawab pertanyaan-pertanyaan penting dari sebuah system hokum, yang dalam hal ini berkaitan dengan hokum pidana, penerapan bidang ilmu ini tidak terlepas dari penggunaan metode-metode ilmiah, atau ilmu pengetahuan, aturan-aturan yang dibentuk dari fakta-fakta dari suatu kejadian sebagai bentuk melakukan pengenalan terhadap bukti-bukti fisik.
*Menurut **Dr Edmond Locard.** Istilah Forensik berasal dari bahasa yunani yaitu "Forensis" yang berarti debat atau perdebatan merupakan bidang ilmu pengetahuan yang digunakan untuk membantu proses penegakan keadilan melalui proses penerapan ilmu (sains).*
Sedangkan *menurut beberapa pendapat lain Forensik berasal dari bahasa latin yaitu "Forum" yang berarti tempat/lokasi untuk melakukan transaksi.*
Dalam perkembangan selanjutnya semakin banyak bidang ilmu yang dilibatkan atau dimanfaatkan dalam penyidikan suatu kasus kriminal untuk kepentingan hukum dankeadilan.

Dari beberapa pendapat yang telah dijelaskan diatas maka dapat saya jelaskan pendefinisian terhadap ilmu forensic adalah Ilmu forensik adalah penerapan suatu bidang Ilmu pengetahuan dengan tujuan untuk pengungkapan suatu kasus tertentu demi penetapan hukum dan pelaksanaan hukum dalam sistem peradilan hukum pidana maupun hukum perdata.

Prinsip dasar ilmu forensik dipelopori oleh Dr Edmond Locard. Ia berspekulasi bahwa setiap kontak yang Anda buat dengan orang lain, tempat, atau hasil objek dalam pertukaran materi fisik. Ini dikenal sebagai **Locar exchange principle** . Ini pertukaran materi fisik dapat dapat digunakan untuk membuktikan tidak bersalah seseorang atau bersalah di pengadilan hukum.

Dalam investigasi kriminal yang khas, kejahatan adegan penyelidik, kadang-kadang dikenal sebagai Penyidik Crime Scene (CSI), akan mengumpulkan bukti fisik dari TKP, korban dan / atau tersangka. Ilmuwan forensik kemudian memeriksa bahan yang dikumpulkan untuk memberikan bukti ilmiah untuk membantu dalam penyelidikan polisi dan proses pengadilan. Dengan

demikian, mereka sering bekerja sangat erat dengan pihak kepolisian dalam pengungkapan suatu kasus.

1.2. Sejarah dan penjelasan secara umum dari *Ilmu Forensik*

Sejarah dari ilmu forensik, beberapa dokumentasi tentang ilmu forensik sudah ditemukan sejak ribuan tahun yang lalu. Dua ratus tahun sebelum masehi, Archimedes menggunakan metode apung untuk menentukan sebuah mahkota yang terbuat dari emas adalah benar terbuat dari emas murni (tanpa campuran) atau sudah bercampur dengan perak dengan membandingkan terhadap emas padat. Catatan lain yang menggunakan obat-obatan dan entomology untuk mengungkapkan kasus-kasus criminal ditemukan ada sebuah buku berjudul Xi Yuan Lu, di Cina pada masa Dinasti Song (1248) oleh Song Ci. Cina juga pertama kali menggunakan sidik jari sebagai salah satu otentikasi dokumen bisnis.

Perkembangan terus berlanjut, ilmu forensik mulai digunakan untuk mengungkapkan kasus-kasus kriminal. Sir Francis Galton pada tahun 1892 mendirikan sistem pertama untuk mengklasifikasikan sidik jari. Pada tahun 1896, Sir Edward Henry, mengembangkan system berdasarkan arah, aliran, pola dan karakteristik lain yang terdapat pada sidik jari. Klasifikasi “The Henry” menjadi standar untuk teknik penyelidikan sidik jari pada kriminal di seluruh dunia.

Di tahun 1835, Henry Goddard menjadi orang pertama yang melakukan analisa secara fisik untuk menghubungkan peluru dengan senjata si pembunuh. Perkembangan penyelidikan terhadap peluru menjadi semakin tepat setelah Calvin Goddard membuat mikroskop perbandingan untuk menafsirkan peluru keluar dari selonsong yang mana. Di tahun 1970, tim ilmuwan dari Aerospace Corporation mengembangkan meotde untuk mendekteksi residu bubuk mesiu dengan menggunakan mikroskop elektron.

James Marsh, di tahun 1836, mengembangkan tes kimia untuk mendeteksi arsenik, yang digunakan pada percobaan pembunuhan. Pada tahun 1930, ilmuwan Karl Landsteiner mengklasifikasikan darah manusia ke dalam berbagai kelompok. Penemuan ini membuka jalan bagi penggunaan darah dalam investigasi kriminal. Pengembangan terus dilanjutkan, di pertengahan 1900-an ditemukan cara untuk menganalisa air liur, air mani dan cairan tubuh lainnya serta untuk membuat tes darah yang lebih akurat.

Edmond Locard, seorang profesor di University of Lyons, mendirikan laboratorium kriminal polisi pertama di Perancis pada tahun 1910. Untuk kepeloporannya dalam kriminologi forensik, Locard dikenal sebagai “Sherlock

Holmes Perancis". Sementara itu di Los Angeles pada tahun 1924, Agustus Vollmer mendirikan laboratorium kriminal polisi Amerika. Pada akhir abad ke-20, ilmuwan forensik memiliki banyak alat berteknologi tinggi yang mereka miliki untuk menganalisis bukti dari reaksi berantai polimerase (PCR) untuk analisis DNA, teknik sidik jari dengan kemampuan pencarian dengan komputer.

Ilmu Forensik sekarang tidak lagi hanya berhubungan dengan pembunuhan ataupun bidang kedokteran. Saat ini, ilmu forensik semakin luas, di antaranya adalah:

- Art Forensic
- Computational Forensic
- Digital Forensic
- Forensic Accounting
- Forensic Chemistry
- Forensic DNA Analysis
- Forensic Pathology
- Forensic Video Analysis
- Mobile Device Forensics
- Blood Spatter Analysis
- Forensic Investigation
- Dan sebagainya.

Penggunaan prinsip dan prosedur ilmiah untuk memecahan masalah hukum dikenal sebagai ilmu pengetahuan forensik. Istilah "forensik" dapat menggambarkan sejumlah disiplin ilmiah, di antaranya kimia, toksikologi, psikiatri, patologi, biologi, dan teknik. Oleh karena itu, sangatlah wajar untuk memikirkan ilmu pengetahuan forensik dalam kaitannya dengan ilmu pengetahuan alam, fisika, dan ilmu sosial, pengelompokan besar cabang pengetahuan terkumpul di mana kebenaran dan hukum diperiksa dan dicatat. Ketika ilmu pengetahuan forensik digunakan untuk menyelesaikan masalah hukum, banyak subkelompok menjadi spesialisasi yang dikenal sebagai farmakologi forensik, psikologi forensik, dan lain-lain. Sebenarnya, tiap subspesialisasi ini dapat digunakan dalam pemecahan masalah hukum.

Scientific Method and Law (Hukum dan Metode Ilmiah)
Untuk menentukan sejarah permulaan ilmu pengetahuan forensik, seseorang harus mempertimbangkan evolusi proses hukum di Eropa, terutama Inggris. Penentuan bersalah atau tidak bersalahnya suatu tindak kejahatan dimulai dari peradilan primitif melalui cobaan berat, proses inquisitorial, dan pada akhirnya ajaran dasar yurisprudensi modern, yaitu praduga tak bersalah berdasarkan hukum Anglo-Saxon dan praduga bersalah berdasarkan

Napoleon Code. Metode ilmiah atau penyelidikan rasional menjadi bagian dari proses peradilan pada abad ke-19, dan ilmu pengetahuan forensik berkembang dengan cepat pada abad ke-20. Kemajuan teknologi terus mendorong pertumbuhan ilmu pengetahuan forensik.

Contoh penggunaan awal pengetahuan ilmiah untuk memecahkan masalah tindak pidana mungkin diusahakan paling banyak oleh ahli kimia dan dokter medis. Pembunuhan yang terkenal oleh Jack the Ripper di London pada tahun 1888 memberikan kesempatan untuk pemeriksaan medis terhadap korban dan suatu penafsiran pola luka yang mungkin. Pada bulan Mei 1899, kasus James Maybrick, seorang broker kapas Liverpool, dipusatkan pada peran arsenik sebagai penyebab kematian, pemeriksaan terhadap arsenik telah dilakukan pertama kali di Prancis pada tahun 1839. Fotografi dilaporkan telah digunakan untuk mencatat potret kejahatan di Brussels pada tahun 1840, dan pada tahun 1879, Alphonse Bertillon mulai mengembangkan suatu metode pengidentifikasian melalui serangkaian pengukuran antropometrik. Data ini, terdiri atas 11 sampai 14 pengukuran ciri-ciri fisik, tengkorak, panjang lengan bawah, tinggi, dan lain-lain, yang merupakan dasar suatu pengumpulan kartu pengukuran yang mencatat statistik dari kejahatan yang diketahui, informasi yang dapat digunakan untuk mengidentifikasi seseorang pada waktu setelah itu. Sistem pengukuran Bertillon pada akhirnya diterima oleh banyak lembaga kepolisian di Eropa, Amerika dan lembaga kepolisian yang lain. Meski demikian, kesulitan melakukan pengukuran yang tepat telah membatasi kegunaan metode ini dan terkadang mengakibatkan ketidakadilan.

Pada waktu yang bersamaan, dua orang yang bekerja di negara yang terpisah, William Hershchel di India pada tahun 1877 dan Dr. Henry Fauld di Tokyo pada tahun 1880, meletakkan dasar untuk ilmu pengidentifikasian pribadi melalui sidik jari. Francis Galton menerbitkan buku Fingerprints pada tahun 1892, sementara itu pada tahun 1896 Edward Henry yang juga bekerja di India mengembangkan sistem praktik untuk pengklasifikasian dan pengisian sejumlah sidik jari, suatu metodologi yang telah menghindari Galton. Sistem pengklasifikasian Henry kemudian diterima di semua negara jajahan Inggris dan diperkenalkan ke Amerika pada tahun 1904 saat pameran dunia di St. Louis, Missouri. Sistem klasifikasi dikembangkan dan digunakan di Prancis, Indo-Cina, dan Amerika Selatan. Meski demikian, sistem Henry dengan beberapa perubahan karena file tumbuh lebih besar tiap tahun, adalah sistem yang paling luas digunakan secara internasional.

Tidak sampai penutup abad ke-19, berbagai teknik dan praktik penyelidikan kejahatan ilmiah mendapat perhatian lembaga praktisi umum, administrator kepolisian, dan para ilmuwan. Seorang kontributor penting bagi penyebaran

yang luas informasi ini adalah Arthur Conan Doyle, yang ahli dalam kedokteran, dengan pengecualian patuh dan imajinatif. Kontributor lain adalah Hans Gross, seorang hakim di Graz, Austria dengan keras berpraktik, seksama, dan meluaskan minatnya. Cerita Sherlock Holmes dari Doyle, yang ditulis antara tahun 1887 dan 1917, memancarkan imajinasi penyelidik dan tidak diragukan lagi memberikan kontribusi bagi peningkatan kualitas penyidikan kejahatan yang ada. Bagaimana pun, Hans Grosslah yang mengumpulkan dua volume pengetahuan waktu yang tersedia yang benar-benar dapat diterapkan pada penyelidikan kejahatan dan administrasi peradilan. Bukunya, Handbuch für Untersuchungsrichter (A manual for Examining Magistrates) yang diterbitkan pada tahun 1893, menjadi pertanda bagi permulaan ilmu pengetahuan forensik kontemporer. Pada edisi ketiga (1898) System der Kriminalistick ditambahkan pada judul aslinya. Terjemahan bahasa inggeris Madras (Criminal Investigation) oleh John Adam dan Collyer Adam muncul pada tahun 1907. Edisi berikutnya muncul pada tahun 1962, yang mengandung pencocokan kesaksian agar risalah dasar menjadi berharga.

Berbagai penambahan teknik ilmiah pada cara penyelidikan kejahatan mengalami kemajuan dengan cepat pada abad ke-20. Beberapa yang menjadi sorotan dari kemajuan ini antara lain pengujian benzidine dan hemin pada darah, uji Uhlenhuth pada darah manusia, sistem pengelompokan darah ABO Landsteiner, dan identifikasi faktor rhesus Alexander Weiner. Kasus Stielow memberikan pengaruh yang penting tentang identifikasi senjata api, sementara kontribusi berharga lain diberikan oleh Charless Waite, Phillip O. Gravelle, Max Poser, dan Calvin Goddard yang penting dalam bidang balistik forensik, yang membawa ilmu pengetahuan forensik pada garis terdepan, sebagai hasil dari pekerjaannya dalam memecahkan the St. Valentine's Day Massacre yang terjadi di Chicago, Illinois, pada tahun 1929.

Early Centers of Learning (Pusat Pembelajaran Awal)
Pembangunan laboratorium Scientific Crime Detection Laboratory di Northwestern University Law School di Chicago merupakan usaha pertama yang terkenal untuk menyatukan kelompok ilmuwan forensik dari berbagai bidang ilmu untuk memberikan keahliannya dalam penyelidikan kejahatan dan administrasi peradilan. Sejumlah pemeriksa swasta di negara yang berbeda memelopori pekerjaan pemeriksaan dokumen yang dipermasalahkan, identifikasi sidik jari, pemeriksaan senjata api, mikroskopi, dan serologi forensik.

1.3. Sejarah *Forensik* dan *Digital Forensik* secara umum

1. Francis Galton (1822-1911) : sidik jari;
2. Leone Lattes (1887-1954) : Golongan darah (A,B,AB & O)
3. Calvin Goddard (1891-1955) : senjata dan peluru (Balistik)
4. Albert Osborn (1858-1946) : Document examination
5. Hans Gross (1847-1915) : menerapkan ilmiah dalam investigasi criminal
6. FBI (1932) : Lab.forensik.

1.4. Definisi *Digital Forensik*

Istilah forensik dapat didefinisikan sebagai penerapan ilmu pengetahuan untuk menyelesaikan *masalah hukum. Definisi yang paling popular tentang digital forensik berasal dari definisi komputer forensik yaitu teknik pengumpulan, analisis, dan penyajian barang bukti elektronik untuk digunakan untuk menyelesaikan masalah* hukum dalam persidangan.[1)]

Menurut Ruby Alamsyah digital forensik adalah ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Barang bukti digital merupakan hasil ekstrak dari barang bukti elektronik seperti Personal Komputer, mobilephone, notebook, server, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa.

Menurut Eoghan Casey : "Semua barang bukti informasi atau data baik yang tersimpan maupun yang melintas pada sistem jaringan digital, yang dapat dipertanggungjawabkan di depan pengadilan"

Menurut Scientific Working Group on Digital Evidence : "Informasi yang disimpan atau dikirimkan dalam bentuk digital"

menurut FBI ini berarti ilmu mengenalisis dan mempresentasikan data yang sudah diproses secara elektronik dan disimpa dalam media computer.

Penggunaan metode ilmiah terhadap penjagaan, pengumpulan, validasi, identifikasi, analisis, interpretasi, dokumentasi dan presentasi bukti digital yang berasal dari sumber-sumber digital guna memfasilitasi atau melanjutkan rekontruksi terhadap kejadian tindak pidana (scientific working group on digital evidence, 2007).

Sedangkan menurut Noblett, Digital Forensik adalah ilmu yang berperan untuk mengambil, menjaga, mengembalikan, dan menyajikan data yang telah diproses secara elektronik dan disimpan di media komputer. Jadi dari pengertian diatas dapat disimpulkan bahwa digital forensik merupakan teknik atau cara menangani barang bukti digital untuk diproses dan menghasilkan informasi yang berguna untuk keperluan pengadilan.

Menurut Ruby Alamsyah, digital forensik atau terkadang disebut komputer forensik adalah ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Barang bukti digital tersebut termasuk handphone, notebook, server, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa.

Jumlah kejahatan komputer (computer crime),terutama yang berhubungan dengan sistem informasi, akan terus meningkat karena kejahatan di internet terbagi dalam berbagai versi. Salah satu versi menyebutkan bahwa kejahatan ini terbagi dalam dua jenis, yaitu kejahatan dengan motif intelektual. Biasanya jenis yang pertama ini tidak menimbulkan kerugian dan dilakukan untuk kepuasan pribadi.

Jenis kedua adalah kejahatan dengan motif politik, ekonomi, atau kriminal yang potensial yang dapat menimbulkan kerugian bahkan perang informasi. komputer forensik dapat diartikan sebagai pengumpulan dan analisis data dari berbagai sumber daya komputer yang mencakup sistem komputer, jaringan komputer, jalur komunikasi, dan berbagai media penyimpanan yang layak untuk diajukan dalam sidang pengadilan. Komputer forensik banyak ditempatkan dalam berbagai keperluan, bukan hanya untuk menangani beberapa kasus kriminal yang melibatkan hukum, seperti rekonstruksi perkara insiden keamanan komputer, upaya pemulihan kerusakan sistem, pemecahan masalah yang melibatkan hardware ataupun software, dan dalam memahami sistem atau pun berbagai perangkat digital agar mudah dimengerti. Komputer forensik merupakan ilmu baru yang akan terus berkembang. Ilmu ini didasari oleh beberapa bidang keilmuan lainnya yang sudah ada. Bahkan, komputer forensik pun dapat dispesifikasi lagi menjadi beberapa bagian, seperti Disk Forensik, System Forensik, Network Forensik, dan Internet Forensik. Pengetahuan Disk Forensik sudah terdokumentasi dengan baik dibandingkan dengan bidang forensik lainnya. Beberapa kasus yang dapat dilakukan dengan bantuan ilmu Disk Forensik antara lain mengembalikan file yang terhapus, mendapatkan password, menganalisis File Akses dan System atau Aplikasi Logs, dan sebagainya.

Dari beberapa penjelasan dan pengertian dari bidang ilmu forensik yang telah dijelaskan sebelumnya, maka saya dapat merumuskan bahwa bidang ilmu digital forensic adalah suatu bidang ilmu khusus yang berkaitan dengan bagaimana, mendapatkan, mengolah, dan mempresentasikan data digital dengan berdasarkan aturan-aturan yang dibentuk dari fakta-fakta dari suatu kejadian sebagai bentuk pengenalan terhadap bukti-bukti fisik pada lokasi kejadian, demi kebutuhan penegakan hokum. Bidang ilmu digital forensic ini merupakan turunan dari bidang imu forensic secara umum.

1.5. Penjelasan umum dari bidang ilmu *Digital Forensik*

Tujuan Digital Forensik

Tujuaan dari digital forensik adalah untuk menjelaskan seputar digital artefak yakni sistem komputer, media penyimpanan (harddisk atau CD-ROM), dokumen elektronik (E-mail atau gambar JPEG) atau paket – paket data yang bergerak melalui jaringan komputer.

Barang Bukti Digital Sebagai Alat Bukti Sah

Menurut Pasal 5 UU No. 11/2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menyebutkan bahwa "informasi elektronik dan atau dokumen elektronik dan atau hasil cetaknya merupakan alat bukti hukum yang sah"

Bukti Digital / Elektronik

Menurut Eoghan Casey :"Semua barang bukti informasi atau data baik yang tersimpan maupun yang melintas pada sistem jaringan digital, yang dapat dipertanggungjawabkan di depan pengadilan" Menurut Scientific Working Group on Digital Evidence : "Informasi yang disimpan atau dikirimkan dalam bentuk digital" Contoh barang bukti digital : alamat E-Mail, wordprocessor/spreadsheet files, source code dari perangkat lunak, files bentuk images (JPEG, PNG, dll), web browser bookmarks, cookies serta kalender dan to do list.

Penanganan Barang Bukti Digital

Penanganan barang bukti digital perlu dilakukan secara khusus mengingat barang bukti digital tergolong rapuh sehingga sangat besat kemungkinan terjadinya pencemaran barang bukti digital baik disengaja maupun tidak disengaja. Kesalahan kecil pada penanganan barang bukti dapat membuat barang bukti digital tidak dapat diajukan dipengadilan sebagai alat bukti yang sah dan akurat.

Ahli forensik bisa mengidentifikasikan penyusupan dengan mengetahui apa yang harus dicari, dimana, dan bukti lain yang diperlukan. Informasi harus mencukupi untuk menentukan apakah upaya penegakan hukum harus disertakan. Proteksi barang bukti merupakan suatu hal yang krusial. Barang bukti tidak boleh rusak atau berubah selama tahapan dan proses recovery dan analisis, juga diproteksi dari kerusakan virus dan mekanis/elektromekanis. Proses harus dilakukan secepat mungkin setelah insiden supaya detilnya masih terekam baik oleh mereka yang terlibat. Hal itu bisa dimulai dengan catatan secara kronologis. Misalnya tentang tanggal, jam, dan deskripsi komputer. Bila menganalisa server mungkin akan diperiksa event log. Karena user bisa mengubah waktu dengan mudah, perhatikanlah bagaimana kecocokannya dengan kronologi kejadian. Buka komputer dan lihat apakah ada lebih dari satu hard disk, catat peripheral apa

yang terhubung, termasuk nomor seri hard disk. Beberapa ancaman terhadap barang bukti :

- Virus – Bisa mengakibatkan kerusakan atau perubahan file.
- Prosedur cleanup – Adanya program atau script yang menghapus file saat komputer shutdown atau start up.
- Ancaman eksternal, misal dari lingkungan yang tidak kondusif sehingga merusak data. Seperti tempat yang terlalu panas, dingin, atau lembab.

Prinsip Kerja Forensik Digital

1. Menurut Pavel Gladyshev prinsip kerja dari forensik digital adalah :Pemeliharaan (“Freezing the Crime Scene”) Mengamankan lokasi dengan cara menghentikan atau mencegah setiap aktivitas yang dapat merusak atau menghilangkan barang bukti.
2. Pengumpulan. Menemukan dan mengumpulkan semua barang bukti digital atau hal – hal yang dapat menjadi barang bukti atau informasi apa saja yang masih bersangkutan dengan kasus yang sedang diselidiki.
3. Pemeriksaan. Menganilisis barang bukti yang ada dan mencari data sebanyak – banyaknya yang berhubungan dengan kasus. Tahap ini adalah penentuan apakah pelaku kejahatan bisa tertangkap atau lolos dari jeratan hukum.
4. Analisis. Menyimpulkan bukti – bukti yang dikumpulkan selama proses penyelidikan.

pemeriksaan yang dilakukan oleh petugas yang tidak berpengalaman dan tidak mengerti forensic digital (prosedur forensic digital), hampir dapat dipastikan akan menghasilkan bukti yang tidak hampir pasti menghasilkan bukti yang tidak dapat diterima di pengadilan hukum.

Tantangan Forensik Digital

Dalam mengumpulkan bukti forensik digital, banyak tantangan – tantangan yang harus dihadapi oleh para penyidik seperti :

- Bagaimana menangani kasus yang melibatkan media perangkat digital
- Bagaimana menemukan bukti dari web browser secara forensik suara
- Bagaimana menganalisis bukti dalam segala kondisi berbeda baik secara perangkat maupun system
- Bagaimana melacak dan mendapatkan pelaku (tak menutup kemungkinan si pelaku adalah orang dalam)
- Bagaimana mengidentifikasi dan menyelidiki kasus – kasus seperti spionase korporasi
- Bagaimana melakukan investigasi network logs guna melacak dan mengadili penjahat cyber

Judd Robbins dari "An Explanation of Computer Forensics" mensyaratkan hal berikut:

- Barang bukti tidak rusak atau terpengaruh oleh prosedur yang dipergunakan untuk penyelidikan.
- Tidak terinfeksi virus komputer selama proses analisis.
- Bukti-bukti yang relevan dan ekstraksinya, ditangani dan dilindungi dari kerusakan mekanis atau elektromekanis lebih jauh.
- Penerapan pemeliharaan
- Membatasi dampak pada operasi bisnis
- Semua informasi client yang diperoleh selama eksplorasi forensik dihargai secara etis dan tidak diumumkan.

Beberapa faktor yang tidak berkaitan secara fisik dengan barang bukti :

1. Rangkaian pemeliharaan – Merupakan rekaman penanganan barang bukti dari penyitaan sampai di bawa ke pengadilan. Dokumentasinya harus menyatakan siapa, apa, di mana, kapan, mengapa dan bagaimana. Lebih rinci hal itu akan lebih baik.
2. Batasan waktu bisa sangat krusial pada beberapa penyelidikan. Khususnya kasus yang melibatkan kehidupan manusia. Misalkan saja bila bukti yang ada berkaitan dengan rencana serangan teroris.
3. Informasi yang tidak diumumkan – Informasi yang berkaitan dengan client

Prioritas pengumpulan data harus dilakukan berdasarkan volatilitas :

1. Register, peripheral memori, dan cache
2. Memori (kernel dan fisik)
3. Keadaan jaringan
4. Proses yang sedang berjalan
5. Disk
6. Floppy, media backup
7. CD ROM, printout

Dengan menganalogikan prinsip ketidakpastian Heisenberg yaitu "Melakukan pengujian sekumpulan atau suatu bagian dari sistem akan menimbulkan gangguan pada komponen lainnya. Sehingga akan mustahil untuk melakukan capture keseluruhan sistem pada satu saat saja." Mengumpulkan barang bukti sangat memakan waktu. Banyak barang bukti dalam bentuk terenkripsi atau hidden. Terdapat program yang dipergunakan untuk recovery password dari perusahaan software yang dipercaya. Program untuk mengeksploitasi kelemahan pada beberapa sistem bisa didownload dari internet atau diperoleh dari penegak hukum. File bisa disimpan dengan ekstension yang

menipu atau gambar yang disimpan seperti dokumen teks, misal kasus gambar porno anak-anak yang disimpan dalam nama README.TXT di folder setup.

DAFTAR PUSTAKA

Daniel E Larry, Daniel E Lars, 2011, GPU Computing Gems Emerald Edition, Access Online via Elsevier, British.

Curran, Wm. J., Louis A. McGarry dan Charles Petty. Modern Legal Medicine Psychiatry and Forensic Science. Philadelphia: F.A. Davis, 1980.

Gerber, Samuel M. (ed.). Chemistry and Crime. Washington, DC: American Chemical Society, 1983.

Gonzales, T.A., M. Vance dan M. Klepern. Legal Medicine and Toxicology. New York: D. Appleton, Century, 1937.

Gross, Hans. Criminal Investigations: A Practical Handbook for Magistrates, Police Officers and Lawyers. Diterjemahkan oleh John Adam dan J. Collyer Adam. London: The Specialist Press, 1907.

http://ondigitalforensics.weebly.com/forensic-focus/sejarah-forensik-digital#.VJJ6PsA-Y (diakses pada Tanggal : 17-12-2014 Pukul 10.02 PM)

http://ondigitalforensics.weebly.com/forensic-focus/category/ilmu%20forensik#.VJJ7xsA-Z (diakses pada Tanggal : 17-12-2014 Pukul 09.22 PM)

http://humaspoldametrojaya.blogspot.com/2009/05/forensic-science-ilmu-pengetahuan.html (diakses pada Tanggal : 17-12-2014 Pukul 08.33 PM)

http://coret2ilmiah.blogspot.com/2014/05/history-of-forensic-locard-exchange.html (diakses pada Tanggal : 18-12-2014 Pukul 01.33 AM)

http://www.beasleyallen.com/webfiles/From Frye to Daubert.pdf
http://en.wikipedia.org/wiki/Digital_forensics
http://en.wikipedia.org/wiki/Forensic_science
http://science.howstuffworks.com/forensic-lab-technique1.htm
http://science.howstuffworks.com/locards-exchange-principle.htm
http://science.howstuffworks.com/locards-exchange-principle2.htm
https://viaforensics.com/computer-forensic-ediscovery-glossary/what-is-daubert.html

http://www.forensics-research.com/index.php/computer-forensics/computer-forensics-history/
http://www.law.cornell.edu/wex/daubert_standard
http://www.law.cornell.edu/wex/frye_standard
http://www.law.ua.edu/pubs/lrarticles/Volume 51/Issue 2/McLeod.pdf
http://www.wisegeek.com/what-is-the-frye-standard.htm