PERKEMBANGAN DIGITAL FORENSIK SAAT INI DAN MENDATANG

Ruci Meiyanti[1], Ismaniah[2].

Dosen Prodi Teknik Informatika, Fakultas Teknik, Universitas Bhayangkara Jakarta Raya

Abstrak - Ilmu forensik adalah ilmu yang digunakan untuk tujuan hukum, bersifat tidak memihak yang merupakan bukti ilmiah untuk digunakan dalam kepentingan peradilan dan penyelidikan. Digital forensik atau sering disebut juga sebagai komputer forensik adalah salah satu cabang dari ilmu forensik yang berkaitan dengan bukti legal yang masih terdapat pada sebuah atau lebih komputer dan media penyimpanan digital lainnya sebagai bukti-bukti digital yang digunakan dalam kejahatan komputer dan dunia maya. Seorang Pakar digital forensik harus benar-benar terlatih dan berpengalaman dalam menggunakan cara untuk mengumpulkan semua data-data yang diperlukan sehingga bisa dijadikan bukti legal yang semuanya sudah diatur dalam undang-undang informasi dan transaksi elektronik. Dengan pesatnya perkembangan teknologi dewasa ini dalam informatika da komunikasi yang dapat digunakan untuk aktifitas kejahatan di dunia maya maka dapat diupayakan peralatan investigasi dan aplikasi-aplikasi yang dapat digunakan di dunia sekuriti dan berguna untuk digital forensik pada saat ini dan mendatang.

Kata kunci : digital forensik, sekuriti, kejahatan dunia maya, bukti digital

Abstraction - Forensic science is the science used to purpose in law and no have take sides that evidence science to used in a court and investigation. Digital forensic or computer forensic is one of forensic science relative with legal evidence in one or more computers and others digital storage medias as an digital evidence used cyber or computer crime. A digital forensic expert must trained and have experience to collect data needed so that become a legal evidence managing in law of the information and electronic transaction. Recently developing high tech in informatics and telecommunication that used in cyber crime, the investigation tools and applications can use in security world and useful digital forensic now and future.

Keyword: digital forensic, security, cyber crime, digital evidence

I. PENDAHULUAN

Pemeriksaan suatu perkara di dalam suatu proses peradilan bertujuan untuk mencari kebenaran materiil (nyata) terhadap perkara tersebut. Hal ini dapat dilihat dari adanya berbagai usaha yang dilakukan oleh aparat penegak hukum dalam memperoleh bukti-bukti yang dibutuhkan untuk mengungkap suatu perkara baik pada tahap pemeriksaan pendahuluan seperti penyidikan dan penuntutan maupun pada tahap persidangan perkara tersebut, hal itu diklasifikasikan kedalam ilmu forensik. Ilmu forensik telah didefinisikan sebagai ilmu yang digunakan untuk tujuan hukum, bersifat tidak memihak yang merupakan bukti ilmiah untuk digunakan dalam kepentingan peradilan dan penyelidikan.

Digital forensik atau sering disebut komputer forensik adalah ilmu yang menganalisa barang bukti digital sehingga dapat dipertanggungjawabkan di pengadilan. Barang bukti digital dapat berupa *mobilephone, notebook, server*, alat teknologi apapun yang mempunyai media penyimpanan dan dapat dianalisa. Digital forensik merupakan ilmu baru yang terus berkembang.

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". Walau demikian tidak sembarang informasi elektronik atau dokumen elektronik dapat dijadikan alat bukti yang sah. Menurut UU ITE, suatu informasi elektronik atau dokumen elektronik dinyatakan sah untuk dijadikan alat bukti apabila menggunakan sistem elektronik yang sesuai dengan ketentuan yang diatur dalam UU ITE.

II. PENGERTIAN ILMU FORENSIK

Forensik merupakan cabang ilmu dari kriminalistik, yang agak berbeda dengan kriminologi. Walaupun begitu, keduanya mempunyai ruang lingkup yang sama yaitu membahas soal kejahatan. Forensik dipakai untuk membantu penyidikan dalam suatu kasus kejahatan. Hasil analisa forensik tersebut nantinya akan digunakan untuk membantu penyajian data atau bukti dalam pemeriksaan di pengadilan.

Kata "forensik" berasal dari bahasa Yunani yaitu "Forensis" yang berarti debat atau perdebatan. Istilah forensik dapat mempunyai arti yaitu bidang ilmu pengetahuan yang digunakan untuk membantu proses penegakan keadilan melalui proses penerapan sains. Ada lima hal dasar yang diketahui dalam daur hidup forensik (Dahake,2012) yaitu :

1. Preparasi (Informasi dari penyidik dan saksi)
2. Pengumpulan (Mengumpulkan data)
3. Pemeriksaan
4. Penganalisaan (Menganalisa dan menarik benang merah dari data-data yang telah dikumpulkan)
5. Pelaporan (Mengambil keputusan/ kesimpulan)

Ilmu forensik dibutuhkan karena dalam suatu peristiwa kejahatan dapat memiliki bukti-bukti kejahatan selain saksi hidup, yaitu bukti-bukti fisik yang biasa disebut "saksi diam" atau *silent witness*. *Silent witness* ini bisa mengindikasikan informasi yang sama dengan keterangan seorang saksi hidup. *Silent witness* atau bukti fisik bisa memiliki berbagai bentuk, misalnya selongsong peluru, jejak sepatu, bagian tubuh manusia, tanda tangan, dan lainnya. Bukti-bukti fisik ini tentu tidak akan dengan sendirinya menceritakan apa yang mereka alami layaknya saksi hidup.

Diperlukan ilmu forensik untuk "mengetahui" isi yang tersembunyi di dalam bukti fisik tersebut kemudian dijelaskan dalam laporan analisa forensik. Forensik terus berkembang

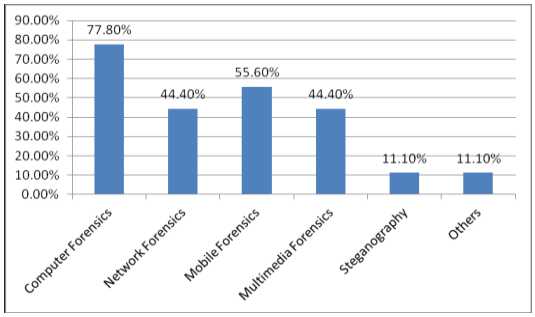
menyangkut subjek forensik, proses, metodologi, hingga meluas kebidang lain. Salah satunya, muncul istilah komputer forensik atau digital forensik seiring dengan perkembangan perangkat teknologi informatika dan komunikasi.

III. DIGITAL FORENSIK

Digital Forensik atau dalam bahasa Indonesia disebut sebagai komputer forensik menurut wikipedia adalah salah satu cabang dari ilmu forensik yang berkaitan dengan bukti legal yang masih terdapat pada sebuah komputer atau lebih dan media penyimpanan digital. Digital Forensik bisa dikatakan sebagai metodologi ilmiah dalam pengembangan sistem untuk mengidentifikasi, mencari, mendapatkan kembali, dan menganalisis barang bukti dari komputer, media penyimpanan komputer dan perangkat elektronik lainnya serta mempresentasikan hasil penemuan tersebut sesuai dengan standar yang telah ditetapkan oleh pengadilan. Penggunaan metodologi ilmiah diperlukan terhadap penjagaan, pengumpulan, validasi, identifikasi, analisis, interpretasi, dokumentasi dan presentasi bukti digital yang berasal dari sumber-sumber digital guna memfasilitasi atau melanjutkan rekontruksi pada kejadian tindak pidana.

Digital forensik dapat juga 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. Digital forensik banyak ditempatkan dalam berbagai keperluan, diantaranya untuk menangani beberapa kasus kriminal yang melibatkan hukum, seperti rekonstruksi perkara, upaya pemulihan kerusakan sistem, pemecahan masalah yang melibatkan hardware ataupun software, dan dalam memahami sistem ataupun berbagai perkara yang melibatkan perangkat digital.

Digital forensik dapat dispesifikasi lagi menjadi beberapa bagian, seperti Disk Forensik, System Forensik, Network Forensik, dan Internet Forensik. Seiring dengan perkembangan teknologi komputer dan mobile telepon maka pengembangan terhadap bagian yang dinvestigasi dalam digital forensik menjadi bertambah seperti yang terlihat pada gambar berikut ini.



Gambar 2.1 Kasus yang dikembangkan dalam investigasi digital forensik. Sumber: IJCSDF 2(2): 52, Digital forensic trends and future.

Dalam suatu model digital forensik melibatkan tiga komponen terangkai yang dikelola sedemikian rupa sehingga menjadi sebuah tujuan akhir dengan segala kelayakan serta hasil yang berkualitas. Ketiga komponen tersebut adalah:

1. Manusia *(People)*, diperlukan kualifikasi untuk mencapai manusia yang berkualitas. Memang mudah untuk belajar komputer forensik, tetapi untuk menjadi ahlinya, dibutuhkan lebih dari sekadar pengetahuan dan pengalaman.

2. Peralatan *(Equipment)*, diperlukan sejumlah perangkat atau alat yang tepat untuk mendapatkan sejumlah bukti yang dapat dipercaya dan bukan sekadar bukti palsu.
3. Aturan *(Protocol)*, diperlukan dalam menggali,mendapatkan, menganalisis, dan akhirnya menyajikan dalam bentuk laporan yang akurat. Dalam komponen aturan, diperlukan pemahaman yang baik dalam segi hukum dan etika, kalau perlu dalam menyelesaikan sebuah kasus perlu melibatkan peran konsultasi yang mencakup pengetahuan akan teknologi informasi dan ilmu hukum tentunya.

IV. PERANGKAT DAN TEKNIK DIGITAL FORENSIK

Pada Teknik digital forensik data disimpan atau ditransfer dengan standard sistem IT, dihubungkan ke berbagai perangkat dan jaringannya lalu ke *personal digital assistants (PDAs)* dan berbagai media elektronik lainnya. Kemudian dilakukan pemeriksaan dan analisa data dari data yang sudah dikumpulkan. Teknik digital forensik digunakan untuk berbagai tujuan diantaranya untuk mendukung investigasi tindak kriminal, menganalisa, meninjau dan memulihkan kerusakan sistem itu sendiri. Berbagai perangkat dapat digunakan untuk digital forensik dengan kegunaan untuk pemecahan code dan pemulihan password, mengumpulkan file dan image file, menganalisa GUI dan program digital forensik, meningkatkan efisiensi, privasi dan kegunaan perangkat tersebut.

V. BUKTI DIGITAL

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". 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,* kalender, *to do list*, dan lainnya.

Penanganan barang bukti digital perlu dilakukan secara khusus mengingat barang bukti digital tergolong rapuh sehingga sangat besar 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.

Dalam UU ITE diatur bahwa informasi elektronik/dokumen elektronik dan atau hasil cetaknya (bukti digital) merupakan alat bukti hukum yang sah, dan merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Menurut UU ITE, suatu informasi elektronik atau dokumen elektronik dinyatakan sah untuk dijadikan alat bukti apabila menggunakan sistem elektronik yang sesuai dengan ketentuan yang diatur dalam UU ITE, yaitu sistem elektronik yang andal dan aman, serta memenuhi persyaratan minimum yaitu sebagai berikut:

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 ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut

3. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik, dilengkapi dengan prosedur atau petunjuk yang dipresentasikan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dalam penyelenggaraan sistem elektronik
4. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Sejumlah rangka kerja dalam proses pembuktian dengan menggunakan digital forensik (Inikpi, 2011) terdiri dari 9 komponen:

1. *Identification*: mengenal & mengamati suatu perkara serta menntukan jenis perkaranya. Komponen ini yang paling penting karena mempengaruhi langkah-langkah selanjutnya untuk penentuan jenis forensik.

2. P*reparation*: melibatkan tools, tehnik, mencari barang bukti, memonitor serta mengelolanya.

3. *Approach strategy*: memformulasikan prosedur dan pendekatan yang digunakan untuk memaksimalisasikan pengumpulan bukti-bukti dan meminimalisasikan pengaruhnya terhadap korban.

4. *preservation*: meliputi pengamanan, pengasingan dan penjagaan terhadap bukti-bukti secara materiil dan digital.

5. *collection*: mencatat dan mengumpulkan bukti-bukti sesuai dengan standard dan prosedur yang diterima.

6. *Examination*: Memeriksa pencarian yang sistematik dari bukti-bukti yang berhubungan dengan tersangka kriminal, fokus pada pengidentifikasian dan penentuan lokasi bukti yang potensial.

7. A*nalysis*: menganalisis hasil dari bukti-bukti yang telah diperiksa.

8. *Presentation*: mengambil kesimpulan dari apa yang telang dirangkum dan dijelaskan.

9. *Returning Evidence*: mengembalikan kepada pemiliknya baik bukti-bukti berupa materiil dan digital.

VI. PERKEMBANGAN DIGITAL FORENSIK

Metodologi investigasi digital forensik dewasa ini adalah dengan penggunaan neural networks dan database pola pengenalan (*pattern recognition*) yang digunakan untuk penganalisaan objek. Suatu proses investigasi dapat dibagi menjadi 4 tahapan yaitu: *recognation, identification, individualization, dan reconstruction.* Maka pada setiap tahapan inilah ditempatkan sistem cerdas yang menghasilkan informasi dari hasil analisa kegiatan investigasi tersebut. Informasi yang besar disimpan dalam bentuk digital.

Ada 3 bentuk data yang penting yang terlibat dalam proses investigasi saat ini yaitu data preparasi (*generation*), *data warehouse* dan *data mining*. Tujuan dari *data mining* ini adalah menemukan hubungan yang berarti dalam data item, siapa pemilik data tersebut dan memvalidasi kehandalan dari pemrosesan data awal. Tentunya dalam investigasi digital forensik ini menggunakan berbagai macam perangkat elektronik yang mendukung penguatan pembuktiannya.

Berdasarkan penelitian dari berbagai topik jurnal mengenai digital forensik yang telah dilakukan maka untuk saat ini implementasi digital forensik mengarah pada penggunaan multimedia seperti teknik perekayasaan gambar; jaringan komputer seperti perekayasaan transaksi melalui *mobile* aplikasi dalam kasus pencucian uang, pencurian uang dan lainnya.

Ada beberapa peralatan investigasi yang digunakan dalam digital forensik dewasa ini (Dezfoli, 2013) yaitu:

1. *Digital Media Exploitation Kit (MEK)* yaitu mengambil data dari *hard drive* PC sehingga dapat diketahui siapa yang telah menggunakan komputer yang tidak sesuai dengan otoritasnya.
2. Pencarian kata kunci, hal ini sering terjadi dan dapat menimbulkan bahaya dalam kesalahan menganalisa kata kunci yang dilakukan dalam berbagai bahasa yang dapat digunakan dalam komputer yang menggunakan Unicode sebagai standard *encoding* yang meliputi 16 bahasa dunia yang terdiri dari 12 bahasa eropa, beberapa bahasa timur tengah dan asia yang dipelopori oleh *Rosette Core Library for Unicode.*
3. Perluasan format penyimpanan data atau sering disebut dengan *Advanced Forensic Format (AFF)* dimana dapat dilakukan tindak kejahatan dengan menyembunyikan atau menghapus data yang terdapat didalam tempat penyimpanan data.
4. Dalam *Cloud computing system* investigasi forensik menjadi lebih kompleks lagi karena menyangkut otoritas dengan pemeriksaan enkripsi data sebelum dan sesudah data dihantarkan ke jaringan publik.
5. Dan sebagainya.

Dari berbagai kecanggihan peralatan komputer yang dapat digunakan untuk tindak kriminal maka sudah saatnya untuk meningkatkan laboratorium forensik dengan kecanggihan teknologi yang dapat melakukan pengolahan gambar yang dapat digunakan untuk investigasi forensik, *database* dengan teknologi yang lebih luas dalam pemanfaatan beragam data seperti *neural networks and pattern recognition databases*, dan dapat menelusuri bukti-bukti yang lebih luas dengan menggunakan keamanan *password* dan *bar code* yang dapat terintegrasi dengan bukti-bukti di pengadilan. Untuk saat ini dan masa mendatang mobile aplikasi juga dapat dikembangkan untuk membantu kegiatan identifikasi, akuisisi dan pengamanan terhadap bukti-bukti digital pada suatu tindak kejahatan.

VII. KESIMPULAN

Digital forensik digunakan untuk membantu investigasi (pemeriksaan) yang merupakan bukti-bukti dari suatu tindak kejahatan yang menggunakan perangkat teknologi informasi yang senantiasa berkembang dengan cepat. Fungsi dari digital forensik adalah untuk melindungi kerahasiaan pribadi, mendukung pemeriksaan yang jelas dan aturan pemrosesan dalam pemanfaatan teknologi informasi. Perkembangan

digital forensik seharusnya terus senantiasa dilakukan seiring dengan perkembangan teknologi canggih di dunia informatika dan komputer karena tindak kriminal akan selalu mencari celah yang dapat dimanfaatkan untuk terjadinya tindak kejahatan komputer atau kejahatan di dunia maya.

DAFTAR PUSTAKA

[1]. Cosic, Jasmin, et al, "Chain of Digital Evidence" Based Model of Digital Forensic Investigation Process, International Journal of Computer Science and Information Security (IJCSIS), Vol 9 No.8, 2011.

[2]. Dahake, Sandhya, et al, A Study of Digital Forensic: Process and Tools, National Conference on Innovative Paradigms in Engineering & Technology (NCIPET-2012) Proceedings published by International Journal of Computer Applications® (IJCA).

[3]. Dezfoli, farhood Norouzizadeh, et al, Digital Forensic Trends and Future, International journal of Cyber Security nad Digital Forensic (IJCSDF) 2(2):48-76, The Society of Digital Information and Wireless Communication, 2013, ISSN 2305-0012.

[4]. Gupta, Pankaj, et al, Review Research Paper Digital Forensics - A Technological Revolution in Forensic, Journal Indian Acad Forensic Med. April-June 2011, Vol. 33, No. 2, ISSN 0971-0973.

[5]. Inikpi O. Ademu, et al, A New approach of Digital Forensic Model for Digital Forensic Investigation" , International Journal of Advanced Computer Science and Applications (IJACSA), Vol 2 No.12, 2011.

[6]. Kumar, Kailash, et al, Identification of User Ownership in Digital Forensic using Data Mining Technique, International Journal of Computer Applications (0975-8887) volume 50 – No.4, July 2012.

[7]. Selamat, Siti Rahayu, et al, A Forensic Tracebility Index in Digital Forensic Investigation, Journal of Information Security, pp: 19-32, Universiti Teknikal Malaysia Melaka, 2013.