PENGANTAR FORENSIK TEKNOLOGI INFORMASI

“ Tahapan Komputer Forensik ”

Oleh : Farhat, ST, MMSI, MSc

{ Diolah dari berbagai Sumber }

1. DEFINISI FORENSIK

Secara bahasa Kata forensik berasal dari bahasa Yunani *Forensis* yang artinya debat atau perdebatan. Sedangkan menurut istilah forensik ialah salah satu bidang ilmu pengetahuan yang digunakan untuk membantu menegakkan proses keadilan melalui proses penerapan ilmu atau sains.

2. DEFINISI KOMPUTER FORENSIK

Komputer forensik adalah penyelidikan dan analisis komputer untuk menentukan potensi bukti legal Bertahun-tahun yang lalu, kebanyakan bukti dikumpulkan pada kertas. Saat ini, kebanyakan bukti bertempat pada komputer, membuatnya lebih rapuh, karena sifat alaminya Data elektronik bisa muncul dalam bentuk dokumen, informasi keuangan, e-mail, job schedule, log, atau transkripsi voice-mail. (Tawarruq, Usaha, & Syariah, 2015)□

Komputer forensik (kadang dikenal sebagai ilmu komputer forensik) adalah cabang dari ilmu forensik digital yang berkaitan dengan bukti yang ditemukan di komputer dan media penyimpanan digital. Tujuan dari komputer forensik adalah untuk memeriksa media digital dengan tujuan mengidentifikasi, melestarikan, memulihkan, menganalisis dan menyajikan fakta dan opini tentang informasi digital.

Meskipun paling sering dikaitkan dengan penyelidikan dari berbagai kejahatan komputer, komputer forensik juga dapat digunakan dalam proses sipil. Disiplin ilmu yang melibatkan teknik yang sama dan prinsip-prinsip untuk pemulihan data, tetapi dengan pedoman tambahan dan praktek yang dirancang untuk membuat hukum jejak audit.

Bukti dari investigasi forensik komputer biasanya tunduk pada pedoman dan praktik dari bukti digital lain yang sama. Ini telah digunakan dalam sejumlah kasus besar dan diterima secara luas di sistem pengadilan AS dan Eropa.

3. PEMODELAN FORENSIK

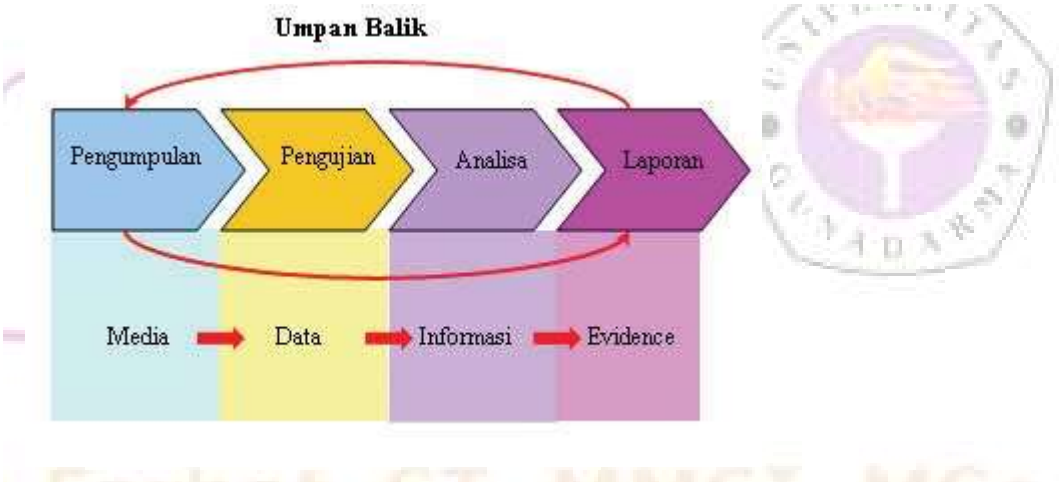
Model forensik melibatkan tiga komponen terangkai yang dikelola sedemikian rupa¬ hingga menjadi sebuah tujuan akhir dengan segala kelayakan dan hasil yang berkualitas. Ketiga komponen tersebut adalah:

- Manusia (People), diperlukan kualifikasi¬ untuk mencapai manusia yang berkua¬litas. Memang mudah untuk belajar komputer forensik, tetapi untuk menjadi¬ ahlinya, dibutuhkan lebih dari sekadar pengetahuan dan pengalaman.

- Peralatan (Equipment), diperlukan sejumlah perangkat atau alat yang tepat untuk mendapatkan sejumlah bukti (evidence) yang dapat dipercaya dan bukan¬ sekadar bukti palsu.
- 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.

4. TAHAPAN KOMPUTER FORENSIK

Tahapan pada Komputer Forensik Ada empat fase dalam komputer forensik, antara lain Empat tahapan dalam komputer forensik.



4.1 Pengumpulan Data

Pengumpulan data bertujuan untuk mengidentifikasi berbagai sumber daya yang dianggap penting dan bagaimana semua data dapat terhimpun dengan baik. Pengumpulan data adalah langkah pertama dalam melakukan proses forensik untuk mengidentifikasi sumber-sumber yang dianggap potensial untuk dijadikan bukti, dan menjelaskan langkah-langkah yang dibutuhkan dalam mengumpulkan data, Pengumpulan data dalam hal ini mencakup beberapa aktifitas seperti berikut :

- Identifikasi
- Penamaan (Labeling)
- Perekaman (Recording)
- Mendapatkan data

Data yang didapatkan haruslah dapat diandalkan dan relevan terhadap kasus yang sedang ditangani, data menjadi barang yang sangat berharga dan merupakan type data yang gampang rapuh, maka dari itu digunakan serangkaian prosedur dalam melakukan penanganan terhadapnya demi menjaga integritas data, setelah melalui proses identifikasi sumber data, langkah selanjutnya tentu mendapatkan data tersebut, ada tiga langkah yang dapat dilakukan dalam mendapatkan data tersebut yaitu:

- Membuat perencanaan untuk mendapatkan data (*develop a plan to acquire data*)
- Mendapatkan data (*Acquire the data*)
- Analisa Integritas data (*Verify the integrity of the data*)

4.2 Pengujian

Setelah melalui proses pengumpulan data, langkah selanjutnya yaitu dengan melakukan pengujian mencakup didalamnya menilai dan melakukan ekstraksi kepingan informasi yang relevan dari data-data yang dikumpulkan, tahapan ini melibatkan *bypassing* atau meminimalisasi fitur-fitur sistem operasi dan sistem aplikasi yang akan mengaburkan data , seperti kompresi, enkripsi dan akses mekanisme kontrol. H*ard drive* berisi ribuan bahkan jutaan file, untuk mengidentifikasi data didalamnya akan sangat menyita waktu dan perhatian serta akan sangat melelahkan, filtrasi akan mengeliminir sebagian data yang tidak dibutuhkan, misalnya data log minggu lalu yang terdiri dari jutaan record dan didapati hanya ratusan record saja yang dinilai penting untuk pemeriksaan lebih lanjut. ada banyak peralatan dan teknik yang digunakan untuk melakukan eliminasi terhadap tumpukan data, pencarian data berbasis teks dan berbagai pola tertentu dapat digunakan untuk mengidentifikasi ketepatan suatu data, seperti pencarian terhadap dokumen yang berhubungan dengan seseorang atau pokok permasalahan tertentu, atau mengidentifikasi pada e-mail log entries untuk mendapatkan email/dan alamat email yang dapat mengarahkan kepada pencerahan kasus. terdapat banyak tool yang dapat digunakan dalam pengujian ini, misalnya software yang mampu menentukan secara akurat jenis file yang berisi karakteristik tertentu, mungkin dapat berupa file teks, grafik, audio, atau berbagai file kompresi lainnya, pengetahuan menyeluruh akan jenis dan type file dapat dijadikan acuan dalam menyingkirkan file yang dianggap tidak memiliki kelayakan/nilai lebih.

4.3 Analisis

Analisis dapat dilakukan dengan menggunakan pendekatan sejumlah metode. Untuk memberikan kesimpulan yang berkualitas harus didasarkan pada ketersediaan sejumlah data atau bahkan sebaliknya, dengan menyimpulkan bahwa “tidak ada kesimpulan”. Hal tersebut sangat dimungkinankan. Tugas

analisis ini mencakup berbagai kegiatan, seperti identifikasi user atau orang di luar pengguna yang terlibat secara tidak langsung, lokasi, perangkat, kejadiaan, dan mempertimbangkan bagaimana semua komponen tersebut saling terhubung hingga mendapat kesimpulan akhir.

Setelah melalui tahapan ekstraksi informasi, Examiner (team forensik) akan melakukan analisa untuk merumuskan kesimpulan dalam menggambarkan data. Analisa dimaksud adalah mengambil pendekatan metodis dalam menghasilkan kesimpulan yang berkualitas berdasarkan pada ketersediaan data atau bahkan sebaliknya, dengan menyimpulkan bahwa tidak terdapat kesimpulan/hasil yang diperoleh, dan hal tersebut mungkin saja akan terjadi ketika menghadapi situasi real di lapangan. Tugas examiner mencakup kegiatan seperti:

- Mengidentifikasi user atau orang di luar dari pengguna tetapi yang tidak terlibat secara langsung.
- Lokasi (melakukan observasi lokasi kejadian)
- Barang-barang (menentukan barang-barang yang berhubungan dengan kejadian)
- Kejadian (menelusuri rangkaian kejadian yang terdapat pada TKP)
- Menentukan atau mempertimbangkan bagaimana komponen-komponen yang terelasi antara satu sama lainnya, sehingga memungkinkan examiner akan mendapatkan kesimpulan.

Misalnya saja, *Network Intrusion Detection System (IDS) log,* yang mungkin memiliki link ke banyak host, *the host audit logs* mungkin berisi banyak link dari aktivitas user dengan account pengguna, dan *thost* IDS log menjadi history dari aktifitas dan aksi yang dilakukan oleh user.

4.4 Dokumentasi dan Laporan

Ada beberapa faktor yang mempengaruhi hasil dokumentasi dan laporan, seperti:

- Alternative Explanations (Penjelasan Alternatif) Berbagai penjelasan yang akurat seharusnya dapat menjadi sebuah pertimbangan untuk diteruskan dalam proses reporting. Seorang analis seharusnya mampu menggunakan sebuah pendekatan berupa metode yang menyetujui atau menolak setiap penjelasan sebuah perkara yang diajukan.
- Audience Consideration (Pertimbangan Penilik) Menghadirkan data atau informasi keseluruh audience sangat berguna. Kasus yang melibatkan sejumlah aturan sangat membutuhkan laporan secara spesifik berkenaan dengan informasi yang dikumpulkan. Selain itu, dibutuhkan pula copy dari setiap fakta (evidentiary data) yang diperoleh. Hal ini dapat menjadi sebuah pertimbangan yang sangat beralasan. Contohnya, jika seorang Administrator Sistem sebuah

jaringan sangat memungkinkan untuk mendapatkan dan melihat lebih dalam sebuah network traffic dengan informasi yang lebih detail.

- Actionable Information Proses dokumentasi dan laporan mencakup pula tentang identifikasi actionable information yang didapat dari kumpulan sejumlah data terdahulu. Dengan bantuan data-data tersebut, Anda juga bisa mendapatkan dan mengambil berbagai informasi terbaru. Dunia teknologi informasi yang berkembang sedemikian cepat sungguh diluar dugaan, tetapi perkembangan ini diikuti pula dengan kejahatan teknologi informasi. Dan karena kejahatan ini pula menyebabkan banyak orang harus membayar mahal untuk mencegahnya dan menaati hukum yang ada.

5. TIP UMUM FORENSIK

Beberapa tip umum dalam menangani dan menganalisa evidence secara umum untuk menjaga keutuhan atau integritas serta kelayakan data. Berikt tip-tipnya :

- Jangan terlebih dahulu menyalakan komputer untuk alasan apapun.
- Hubungi agen yang bersangkutan untuk melakukan analisa secepatnya, keuntungan berimbang didapatkan dengan mempertimbangkan sisi efisiensi, waktu yang terbatas, dan kebutuhan investigasi.
- Lekatkan atau tandai “evidence tape” melingkupi power supply dan disk drives.
- Memiliki surat perintah atau izin sangatlah penting dan ditujukan untuk memberikan kuasa guna melakukan analisa terhadap komputer dan data di dalamnya.
- Laporan petugas atau polisi, pernyataan tertulis yang sah ataupun ringkasan kasus menjadi kebutuhan yang melegalkan untuk “examiner”.
- Buat daftar kata-kata yang dibutuhkan dalam melakukan pencarian, ada baiknya disimpan dalam media ringkas semisal *floppy disk* dengan ukuran file yang kecil (misalnya: *.txt). Gunakan kata-kata yang unik dan bukannya umum.
- Lupakan kata tepat waktu dalam komputer forensik, ini karena anda menelusuri hutan data sewaktu mengeksplorasi.
- Konsistensilah terhadap kasus dan identifikasi kepentingan, misalnya saja jika menyangkut transaksi obat terlarang dan narkoba, tentu anda tidak menanyakan informasi untuk keperluan pengujian dalam kasus pornografi anak.

- Jika ada beberapa orang yang mungkin menggunakan komputer atau dialokasikan di ruang komputer, indikasi terhadapnya perlu dilakukan. Ini mencakup siapa, atau atribut lain yang berkaitan dengan komputer, seperti password.
- Mengindikasikan apakah komputer diintegrasikan dalam jaringan komputer atau tidak. Dapatkan informasi sebanyak dan selengkap mungkin mencakup beberapa hal lainnya, seperti :
    - Jenis komputer dan jumlah komputer, termasuk pula sistem operasi yang digunakan.
    - Jenis softaware jaringan komputer, karakteristik jaringan, dan lokasi server.
    - Aktivitas jaringan yang berlangsung dan jenis koneksi, berikut sumbernya.
- Mengindikasikan apakah terdapat *encryption* atau *password protection*.
- Mengindikasi skill komputer user yang komputernya diambil untuk keperluan forensik.
- Tidak selamanya monitor dan peripheral ataupun perangkat lain harus disertakan, umumnya komputer dan media penyimpanan sudah cukup guna keperluan forensik.

6. **TIP PEMULA FORENSIK**

Bagi user pemula yang mungkin baru dengan istilah foresnsik dan ternyata mendapati adanya kasus-kasus yang membutuhkan penanganan forensic. Beberapa yang layak diperhatikan :

- Investigasi sederhana mungkin dapat dilakukan untuk mengalamati evidence.
- Hubungi organisasi/pihak yang berwenang dalam mengambil keputusan
- Amankan lokasi, akan lebih baik jangan ada yang berada didaerah atau meja kerja.
- Minimalisi interupsi terhadap lokasi, misalnya biarkan computer apa adanya. Jika computer dalam keadaan menyala, maka biarkan menyala atau dalam keadaan mati, maka biarkan seperti itu. Penanganan lebih lanjut diserahkan oleh professional investigator.
- Jangan menjalankan program apapun pada computer yang dimaksud.
- Jangan membiarkan user lain mengotak atik computer, termasuk manajer anda atau bahkan pemiliknya.
- Kumpulkan dan dokumentasikan sumber data lainnya, misalnya CD backup, tape backup, dan log-log file.
- Barang-barang non computer yang memang dapat dijadikan evidence hendaknya diamankan, misalnya: notes, buku, dan berbagai peralatam kantor lainnya.
- Mulailah dokumentasi chain of custody, dengan mencatat setiap evidence dan milik evidence yan adalah milik seseorang atau perusahaan. Lengkapi data-datanya seperti dimana, kapan, dan siapa

yang menemukan evidence, serta siapa yang melakukan pemeriksaan terhadap evidence, wakyu dan jam hendaknya dicatat.

DAFTAR PUSTAKA

[1] Sulianta, Fery. 2008. Komputer Forensik. Jakarta : PT Elex Media Komputindo.

[2] http://www.academia.edu/7018519/Makalah_forensik

[3] https://dokumen.tips/documents/makalah-forensik.html

[4] http://www.academia.edu/7018519/Makalah_forensik

[5] http://dunia-digital.com/komputer-forensik/

[6] http://www.ferisulianta.com/2009/01/komputer-forensik.html

[7] http://idsirtii.or.id/doc/IDSIRTII-Artikel-ForensikKomputer.pdf

[8]https://www.slideshare.net/Hafiz312/m05-metode-komputer-forensik69799528