METODOLOGI COMPUTER FORENSIK

Disusun untuk memenuhi tugas ke III, MK. Digital Evidence

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

Fathirma'ruf

13917213

PROGRAM PASCASARJANA TEKNIK INFORMATIKA

FAKULTAS TEKNIK INDUSTRI

UNIVERSITAS ISLAM INDONESIA

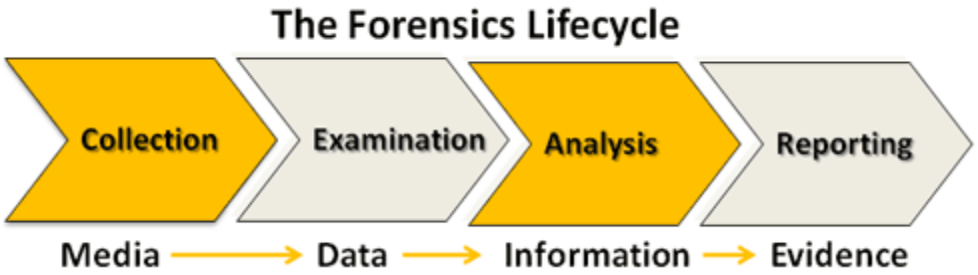
YOGYAKARTA

2014

PEMBAHASAN

Dalam melakukan forensik komputer terdapat beberapa tahapan diantaranya yaitu :

Pengumpulan (Collection), Pengujian (Examination), Analisa (Analysis), Laporan (Reporting). seperti yang digambarkan dalam alur metodologi berikut ini :



Gambar : Tahap-tahap komputer forensik

1. Pengumpulan Data *(Collection)*

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 :

- Identivikasi
- 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*)

2. Pengujian *(Examination)*

Setelah melalui proses pengummpulan 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.

hard 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.

3. Analisa *(Analysis)*

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:

1. Mengidentifikasi user atau orang di luar dari pengguna tetapi yang tidak terlibat secara langsung.
2. Lokasi (melakukan observasi lokasi kejadian)
3. Barang-barang (menentukan barang-barang yang berhubungan dengan kejadian)
4. Kejadian (menelusuri rangkaian kejadian yang terdapat pada TKP)
5. 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. Dokumentasi dan Laporan *(Reporting)*

Repworting adalah tahapan akhir dari proses computer forensic, dalam tahapan ini kita akan merepresentasikan informasi yang merupakan hasik dari proses analisis, banyak factor yang dapat mempengaruhi reporting seperti yang akan dibahas berikut ini :

1. **Alternative Explanations *(penjelasan alternatif)***
   Jika informasi yang mengacu pada suatu kasus dikategorikan tidak lengkap, maka definisi akhir yang diperoleh tidak memadai, dan tidak dapat diandalkan, untuk mengamati kejadian bahkan jika didapati beberaoa oenjelasan lain yang masuk akal akan suatu kejadian, masing-masing informasi yang diperoleh haruslah dipertimbangkan dan diteruskan dalam proses reporting.
   Apa pun yang terjadi, seorang examiner harus tetap menggunakan pendekatan metodikal dalam menentukan untuk menyetujui atau menolak setiap penjelasan perihal duduk perkara yang mungkin untuk diteruskan/diajukan dihadapan pengadilan
2. **Audience Consideration *(pertimbangan audiensi/pengamat)***
   Menyajikan data/informasi pada audiensi sangatlah penting kasus yang melibatkan perundangan membutuhkan laporan detail/spesifik berkenaan dengan informasi yang dikumpulkan, dan duplikasi setiap fakta (evidentiary data) yang diperoleh. Pertimbangan ini beralasan, misalnya saja administrator system ingin melihat lebih jauh *network trafik* secara detail.
3. ***Actionable Information***
   Proses reporting mencakup pula identifikasi actionable information yang diperoleh dari data-data terdahulu, darinnya kita bias mendapatkan ninformasi baru.

Misalnya saja, daftar alamat seseorang dapat dikembangkan lebih lanjut yang kemudian akan mengarahkan pada informasi lain terkait dengan kejadian tindak criminal tersebut.

Keuntungan lain dari actionable information, informasi yang diperoleh akan dapat mungkin dapat digunakan untuk keperluan mendatang, misalnya tujuan pengamanan seperti backdoor yang mungki bias dieksploitasi, maka dibutuhkan penanganan segera. Dalam prosesnya, mungkin didapati mesalah yang harus diperbaiki sesegera mungkin seperti *policy shortcomings* atau *procedural errors* formal review dapat membantu dalam mengidentifikasi dan meningkatkan kualitas.

Daftar Pustaka

Sulianta F, (2014), “Teknik Forensik-cara jitu mengatasi problema computer”.