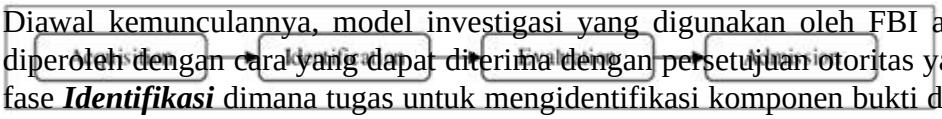
Common Phases of Computer Forensics Investigation Models
Rabu, 1 Februari 2017 | 03:34:42 WIB |

Melanjutkan tulisan sebelumnya (baca : Membangun Integrated Digital Forensics Investigation Framework (IDFIF) Menggunakan Metode Sequential Logic), yang membahas model investigasi yang dipublikasikan researchgate.com. Kali ini penulis akan memberikan sedikit perbandingan lain dalam model investigasi yang di kemukakan oleh Yunus Yusoff, Roslan Ismail and Zainuddin Hassan dalam jurnal internasional Vol 3, No. 3 Juni 2011.

Dalam penjelasannya, dikatakan bahwa dalam proses investigasi haruslah menggunakan langkah-langkah yang tepat, bila ada salah satu langkah saja dilewati maka kesimpulan investigasi tidak akan berpengaruh apapun dalam memecahkan suatu kasus kejahatan komputer, karena tidak dapat dijadikan bukti didalam persidangan ataupun pengadilan. Sejak tahun 1984, model investigasi telah digunakan oleh Laboratorium FBI. Seiring makin meningkatkannya kejahatan komputer maka model investigasi pun ikut "bermetamorfosa" menjadi model-model lain sesuai dengan kebutuhan dan modus operandinya.

Karena banyaknya model investigasi tersebutlah, maka sering menimbulkan masalah lain dikarenakan tidak ada model standard yang dapat digunakan oleh para investigator.



Diawal kemunculannya, model investigasi yang digunakan oleh FBI adalah melakukan ***akuisisi***, bukti yang diperoleh dengan cara yang dapat diterima dengan persetujuan otoritas yang berwenang . Setelah itu diikuti oleh fase ***Identifikasi*** dimana tugas untuk mengidentifikasi komponen bukti digital yang diperoleh dan mengubahnya menjadi format dipahami oleh manusia. Tahap ***evaluasi*** terdiri dari tugas untuk menentukan apakah komponen diidentifikasi di fase sebelumnya, memang relevan dengan kasus yang sedang diselidiki dan dapat dianggap sebagai bukti yang sah. Dan pada tahap akhir, ***penerimaan***, bukti yang diperoleh dibawa ke pengadilan untuk dipresentasikan.

Perkembangan fase model investigasi

Untuk mengidentifikasi model secara umum, maka diurutkan sesuai dengan tahunnya, sebagaimana terlihat dalam tabel berikut :

Setelah proses penyelidikan diidentifikasi, langkah berikutnya adalah mengekstrak semua fase dalam setiap proses penyelidikan. Fase diekstraksi kemudian diklasifikasikan sesuai dengan nomor ID. Fase dengan tugas serupa dikelompokkan bersama. Hasilnya ditampilkan dalam berikut :

Berdasarkan daftar tersebut terlihat jelas bahwa sejumlah fase saling tumpang tindih satu sama lain. Tindakan yang diambil dengan memeprtimbangkan tugas yang dilakukan di masing-masing fase, dan tidak hanya mengandalkan penamaan yang sebenarnya, kita dapat mengamati bahwa fase dapat dikelompokkan menjadi 5 kelompok generik yaitu, pra-proses, akuisisi & pelestarian, analisis, presentasi dan pasca-proses. Tabel dibawah menunjukkan bagaimana fase dikelompokkan ke dalam pengelompokan generik masing-masing.

Dalam tabel tersebut terlihat bagaimana langkah-langkah seorang investigator dalam melakukan tindakan sesuai dengan kategori atapun klasifikasi tindakan yang ada.

Berdasarkan penelitian dari model investigasi lainnya, masing-masing fase mereka dianjurkan juga dapat ditempatkan dalam satu fase generik di atas. Maka berdasarkan hal tersebut diusulkan model investigasi baru yang dikenal dengan **Generic Computer Forensic Investigation Model (GCFIM)**.

Dalam model GCFIM, ada 5 (lima) langkah yang harus di jalankan oleh seorang investigator, dimana langkah-langkah ini tidak boleh terlewati agar hasil kesimpulan dari investigasi ini menjadi valid dan dapat diterima oleh pengadilan. Adapun langkah-langkah tersebut adalah :

1. Pre-Process

Tugas-tugas yang dilaksanakan dalam fase ini berhubungan dengan semua pekerjaan yang harus dilakukan sebelum dimulainya proses investigasi dan pengumpulan data secara resmi.

2. Acquisition dan Preservation

Fase pengumpulan, pengamanan, dan penyimpanan data sehingga dapat digunakan pada fase berikutnya.

3. Analysis

Fase ini adalah fase utama dari proses investigasi forensik komputer dan merefleksikan fokus dari kebanyakan model investigasi yang telah diamati, yaitu analisis terhadap data yang telah didapatkan untuk mengidentifikasi sumber kejahatan dan menemukan pelaku kejahatan tersebut.

4. Presentation

Temuan-temuan dalam fase analisis didokumetasikan dan dipresentasikan kepada pihak yang berwenang. Fase ini merupakan fase yang penting karena tidak hanya bertujuan membuat pihak berwenang paham akan apa yang dipresentasikan, tetapi juga harus didukung oleh bukti yang kuat dan dapat diterima. Tujuan utama dari fase ini adalah untuk membuktikan kebenaran dari kasus kejahatan komputer.

5. Post-Proces

Fase ini berhubungan dengan akhir dari sebuah proses investigasi. Barang bukti fisik dan digital harus dikembalikan kepada pihak yang berwenang untuk menyimpannya. Peninjauan terhadap proses investigasi harus dilakukan agar ada pembelajaran yang dapat diambil dan bisa meningkatkan performa investigasi pada masa yang akan datang.

Dari gambar model investigasi yang penulis sampaikan, dapat terlihat langkah-langkah seorang investigator dalam mengungkap sebuah kasus. Bila tahap pertama sudah dilakukan, maka investigator dapat melanjutkan ke tahap berikutnya, dan apabila dalam tahap ini menemukan informasi ataupun membutuhkan data tambahan lainnya, maka seorang investigator dapat kembali ketahap sebelumnya. Hal ini untuk memastikan bahwa tahap ini sudah dipastikan valid dan dapat dilanjutkan ke tahap selanjutnya.

Semakin banyaknya model investigasi yang disusun, maka semakin banyak pilihan yang dapat digunakan oleh para investigator dalam mengungkap kasus kejahatan komputer. Dan dari model yang ada, dapat disesuaikan dengan kebutuhan dan modus dari kejahatan itu sendiri.

Sumber :

- Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. International Journal of Computer Science & Information Technology (IJCSIT), 3(3)
- M. Kohn, J. H. P. Eloff, & M. S. Olivier, (2006) “Framework for a Digital Forensic Investigation”, in Proceedings of the ISSA 2006 from Insight to Foresight Conference, Sandton, South Africa.
- E. S. Pilli, R. C. Joshi, & R. Niyogi, (2010) “Network Forensic frameworks: Survey and research challenges,” Digital Investigation, Vol. 7, pp. 14-27
