Digital Forensics Investigation Models
Sabtu, 23 Maret 2019 | 19:27:07 WIB |

Kuala Lumpur - Forensik digital (bahasa Inggris: Digital forensics) (juga dikenal sebagai ilmu forensik digital) adalah salah satu cabang ilmu forensik, terutama untuk penyelidikan dan penemuan konten perangkat digital, dan seringkali dikaitkan dengan kejahatan komputer. Istilah forensik digital pada awalnya identik dengan forensik komputer tetapi kini telah diperluas untuk menyelidiki semua perangkat yang dapat menyimpan data digital. Forensik digital diperlukan karena biasanya data di perangkat target dikunci, dihapus, atau disembunyikan. Berawal dari bangkitnya revolusi komputasi personal pada akhir 1970-an dan awal 1980-an, disiplin ini berkembang secara alami selama tahun 1990-an, dan baru pada awal abad ke-21 negara-negara secara bertahap membentuk kebijakannya terhadap disiplin ini.

Landasan forensik digital ialah praktik pengumpulan, analisis, dan pelaporan data digital. Investigasi forensik digital memiliki penerapan yang sangat beragam. Penggunaan paling umum adalah untuk mendukung atau menyanggah asumsi kriminal dalam pengadilan pidana atau perdata.

Pesatnya perkembangan dan pemanfaatan teknologi informasi pada berbagaiaktivitas manusia memberi dampak yang positif untuk beberapa aspek kehidupan. Perkembangan teknologi banyak memberikan kemudahan bagi penggunanya, dan menjadikan pekerjaan jauh leih efektif dan efisien. Namun di sisi lain, perkembangan teknologi juga memberikan dampak negative yang tentunya tidak bisa disangkal. Dengan kecanggihan perangkat-perangkat digital sekarang ini, kejahatan dapat dilakukan dengan canggih menggunakan alat-alat yang belum mempunyai fitur teknologi tinggi.

Jika diteliti kebelakang, banyak sekali kasus-kasus yang mencuat dan disadari atau tidak, kebutuhan akan digital forensik dan kemampuan cyber security mulai bermunculnya, seiring dengan kasus-kasus kejahatan khususnya di bidang computer (cyber crime) dan digital forensic, guna mendukung investigasi pada kasus kejahatan.

Dalam menangani kasus kejahatan yang berhubungan dengan teknologi digital, perlu untuk terus membuat berbagai macam terbosan-terobosan dalam menanganinya. Model investigasi harus diperbaharui, mengingat kejahatan dengan memanfaatkan teknologi terus berkembang. Sejak tahun 1984 sampai sekarang banyak penelitian yang membahas mengenai model proses investigasi digital forensik.

Kita akan mencoba melihat beberapa model investigasi forensik digital terutama model Generic Computer Forensic Investigation Model (GCFIM) yang dapat kita lihat pada paper yang judulnya Common Phases Of Computer Forensics Investigation Models yang ditulis oleh Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, dan paper dengan judul A New Digital Investigation Frameworks Comparison Method dengan penulisnya adalah Omrani Takwa, Chibani Rhaimi Belgacem, dan Dallali Adel.

Sebelum kita membahas mengenai model pada kedua paper tersebut, kita mencoba untuk melihat model proses investigasi digital forensik yang terdahulu:

Tahun 1984, Pollite mengusulkan tahapan investigasiyang mana dengan model ini hasil investigasinya bisa dipercaya secara ilmiah dan bisa diterima secara hukum.

Computer Forensic Investigative Process (CFIP)

Adapun tahapan investigasi CFIP sebagai berikut:

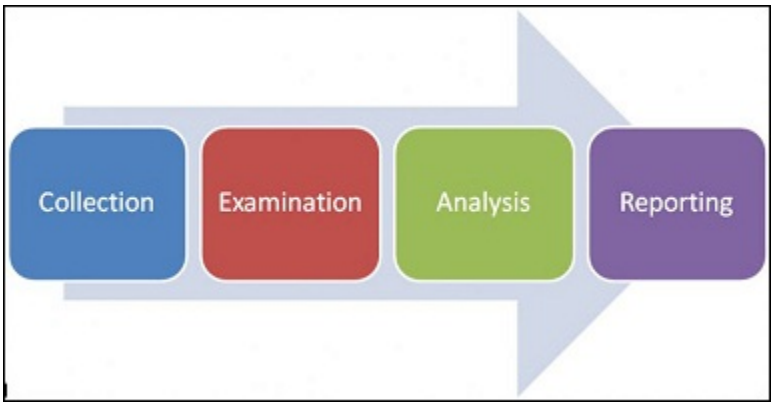
- Acquisition: merupakan tahapan untuk mendapatkan barang bukti sesuai dengan prosedur yang disetujui oleh pihak otoritas.

- Identification: merupakan tahapan identifikasi barang bukti digital yang telah diakusisi sebelumnya.
- Evaluation: merupakan tahap untuk menemukan bukti digital dari barang bukti yang sudah diidentifikasi dan nantinya menjadi barang bukti yang sah di pengadilan.
- Admission: ini merupakan tahap akhir yakni tahap mempresentasikan barang bukti digital di hadapan pengadilan.

Pada tahun 2001, Digital Forensic Research Workshop (DFRWS) merilis Proses Investigasi untuk Ilmu Forensik Digital (A Road Map for Digital Forensic Research, 2001). Gambar di bawah menguraikan tahapan proses penyelidikan ini.

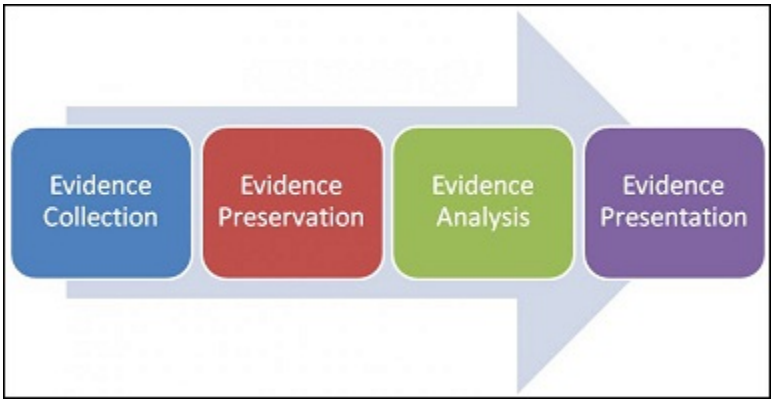
DFRWS Investigative Model

Pada tahun 2006, National Institute of Standards and Technology (NIST) merilis publikasi khusus 800-86 Panduan untuk Mengintegrasikan Teknik Forensik ke dalam Respon Insiden (Kent, Chevalier, Grance, & Dang, 2006). Gambar di bawah menguraikan tahapan proses penyelidikan ini.



DFRWS Investigative Model

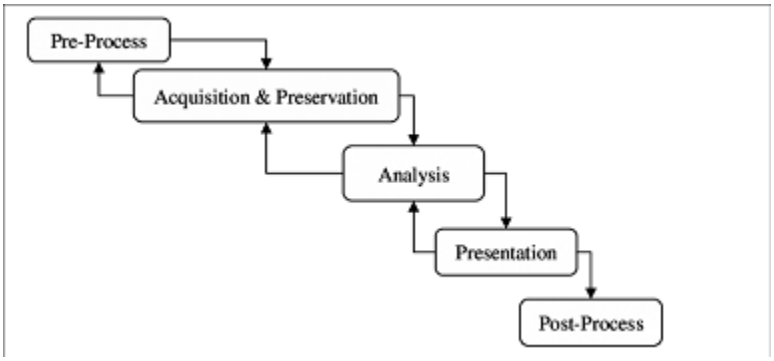
Pada tahun 2009, Elsevier, Inc merilis buku Building a Digital Forensic Laboratory. Buku ini membahas tahapan proses penyelidikan yang ditunjukkan di bawah ini (Jones & Valli, 2009).



DFRWS Investigative Model

Jika kita lihat dengan seksama, maka ada kesamaan pada ke-tiga model investigasi diatas. Sekarang mari kita lihat model yang ada pada paper yang ditulis oleh Yunus Yusoff dkk dan Omrani Takwa dkk.

Tahun 2011, Yunus Yussof, Roslan Ismail dan Zainuddin Hassan mengusulkan model investigasi baru yang disebut dengan model Generic Computer Forensic Investigation Model (GCFIM) dengan tahapan sebagai berikut :

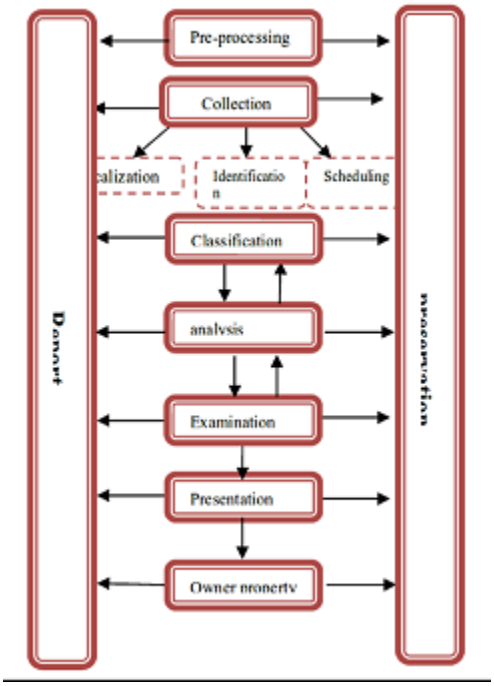


Terdapat 5 tahapan dari model ini, yakni:

- Pre-Process: investigator melakukan hal yang berhubungan dengan pekerjaan sebelum melakukan investigasi, seperti mempersiapkan surat dan dokumen resmi, dan juga mempersiapkan alat-alat yang nantinya akan digunakan.
- Acquisition & Preservation: pada tahap ini, semua data yang relevan diambil, disimpan dan dipersiapkan untuk tahap selanjutnya.
- Analysis: tahapan ini merupakan proses utama dalam penyelidikan komputer forensik, yakni dilakukan analisa pada data yang telah diperoleh pada tahap sebelumnya untuk dilakukan identigikasi sumber kejahatan, motif kejahatan dan pada akhirnya menemukan orang yang bertanggungjawab atas kejahatan tersebut.
- Presentation: setelah melakukan analisa, maka tahapan ini adalah melakukan presentasi terhadap hasil yang sudah didapatkan ke pihak yang berwenang. Tahapan ini penting, mengingat hasil analisa yang ada tidak hanya harus dipresentasikan saja, namun juga harus didukung dengan bukti yang memadai/memenuhi syarat dan dapat diterima. Hasil dari tahap ini adalah untuk membuktikan dan/atau menyangkal dugaan tindak pidana.
- Post-Process: Tahapan ini merupakan tahapan akhir, yang mana bukti digital dan fisik harus dikembalikan kepada pemilik yang sah dan disimpan di tempat yang aman. Investigator meninjau ulang proses investigasi yang telah dilakukan agar dapat digunakan untuk perbaikan proses penyelidikan selanjutnya.

Jika kita perhatikan, pada model GCFIM ini arah panah pada setiap tahapan tergambar bolak balik atau dua arah, artinya bahwa setiap tahapan dapat diulang kembali. Hal ini dapat dilakukan apabila pada saat investigasi terjadi sesuatu yang tidak diinginkan atau masih ada proses yang luput, sehingga investigator dapat mengulang tahapan yang diperlukan tanpa harus mengulang dari tahap pertama.

Sekarang, mari kita lihat model yang diusulkan oleh Omrani Takwa dkk, yang judulnya A New Digital Investigation Frameworks Comparison Method. Model yang disulkan ini diakui bisa menghemat waktu, reusability, dan prosesnya terjaga keamanannya.



Omrani Takwa Model (Malaysia)

Tahapan dari model ini antara lain:

- Pre-processing: tahap ini dilakukan sebagai persiapan dan pengecekan alat software dan hardware yang akan digunakan. Pada tahap ini juga akan diuji kemampuan dan pengalaman penyelidik (investigator), serta anggota penyelidik yang akan diberi otoritas untuk melakukan investigasi agar proses investigasi berjalan lancar. Tahap awal ini investigator akan difasilitasi untuk kebutuhan dalam mendapatkan data yang relevan dan fasiltas yang diperlukan untuk membantu penyelesaian masalah investigasi pada tahap berikutnya.
- Collection

  Localization: merupakan tahap untuk mengidentifikasi data yang relevan yang kemudian dilakukan lokalisasi. Identification: merupakan tahap untuk mengidentifikasi informasi yang tersembunyi. Scheduling: merupakan tahap untuk mengurutkan data berdasarkan prioritas dan kehandalan data.
- Classification: tahap ini data akan dikelompokkan berdasarkan hasil dari proses investigasi sebelumnya dan dibandingkan dengan hasil dari proses investigasi saat ini. Tahap ini diselesaikan menggunakan dengan cara statistik dan teknik fusi data, yang tujuannya adalah untuk memahami kasus kejadian dan mempercepat pemilihan solusi investigasi yang andal.
- Analysis: tahap ini adalah melakukan analisa terhadap data yang sudah dikumpulkan untuk mendapatkan estimasi, kemungkinan, dan hipotesis dari data yang akan berpotensi menjadi barang bukti.
- Examination: tahap ini adalah tahap pengujian keabsahan data, keutuhan data dan keterkaitan data dengan tindak kriminal suatu kasus.
- Presentation: tahap ini adalah tahap presentasi bukti digital kepada pihak yang berwenang dengan menggunakan bahasa yang dapat dipahami dan dipahami oleh orang-orang di persidangan.
- Rapport: tahap ini merupakan tahapan untuk mencari hubungan dari semua hasil investigasi. Hasil dari tahap ini seperti penetapan barang bukti, penjelasan, kebijakan baru dan prosedur investigasi, penutupan kegiatan investigasi.
- Preservation: tahap ini, barang bukti baik yang berupa fisik maupun digital akan dijaga kamanan, dan keutuhannya pada setiap tahapan proses investigasi, sehingga validitas dan integritas barang bukti tetap terjaga.
- Owner property: tahap akhir setelah proses investigasi selesai, semua barang bukti yang disita akan

dikembalikan secara utuh kepada pemiliknya. Utuh maksudnya, keadaan seluruh barang bukti fisik sebelum disita dan setelah disita tetap sama dan keadaan seluruh informasi dan otoritas yang ada pada barang bukti yang disita dikembalikan sepenuhnya kepada pemiliknya sesuai keadaan sebelum dista.

Kesimpulannya, penerapan model investigasi digital forensik setiap tahun berbeda, hal ini tergantung dari tingkat perkembangan zaman, jenis kriminalitas, dan penerapan regulasi yang berbeda pada setiap wilayah. Mengenai relevansi model investigasi GCFIM yang diajukan Yussof tahun 2011, hingga saat ini bisa saja masih relevan diterapkan di Malaysia sebagai objek penelitiannya, namun berbeda halnya dengan Tunisia yang mengembangkan model baru yang dilakukan oleh Omrani Takwa dkk pada tahun 2016. Model terbaru Omrani Takwa akan bisa digunakan di Malaysia jika regulasi, tingkat kemajuan, dan tingkat kriminalitas minimal sudah sama dengan negara tunisia.
