Investigation Models : Membangun Integrated Digital Forensics Investigation Framework (IDFIF) Menggunakan Metode Sequential Logic
Rabu, 21 Desember 2016 | 15:15:20 WIB |

Menulis itu sesuatu banget, dari mulai mata melek sampe mata terpejam yang ada setumpuk paper dan buku-buku yang membuat kepala “kram”. Karena sudah mau deadline, tidak usah basa basi, kita langsung ke TKP.

By the way, untuk hari ini “menu” yang akan penulis berikan adalah tentang model investigasi yang berjudul, “Membangun Integrated Digital Forensics Investigation Framework (IDFIF) Menggunakan Metode Sequential Logic” yang pernah di publikasikan oleh Yeni Dwi Rahayu dan Yudi Prayudi tahun 2014.

Dalam uraiannya dikatakan bahwa, model investigasi yang digunakan saat ini belum memiliki standard baku yang diterapkan. Dalam proses investigasi selalu menggunakan tahapan yang berbeda-beda. Hal ini dapat mengakibatkan pembuktian yang dihasilkan sulit diukur dan dibandingkan. Pengukuran dan perbandingan akan muncul ketika salah satu pihak tidak puas atas hasil pembuktian pihak yang lain. DFIF yang telah banyak berkembang tentu memiliki tujuan masing-masing. Dengan banyaknya model investigasi yang ada, itu hanya membuat masalah baru. Oleh karena itu perlu adanya DFIF standart yang dapat mengakomodir DFIF yang telah hadir sebelumnya.

Metode Sequential Logic dikatakan dalam publikasinya dapat menjadi solusi dalam proses investigasi. Metode ini memiliki keterikatan atas latar belakang masukan terhadap keluarannya. Selain itu, metode ini memiliki karakteristik yang dapat merekam histori dari masukan, sehingga dapat diasumsikan metode tersebut dapat melihat urutan DFIF sebelumnya untuk membentuk DFIF yang baru. DFIF yang dihasilkan dalam penelitian ini disebut sebagai Integrated Digital Forensics Investigation Framework (IDFIF) dikarenakan telah memperhitungkan DFIF sebelumnya. DFIF yang telah ada sebelumnya dapat di akomodir IDFIF dengan menggunakan Metode Sequential Logic.

Sebelum dibahas mengenai metode sequential logic, agar informasinya utuh dan tidak membingungkan para netizen, penulis akan memberikan gambaran secara umum mengenai phase-phase dari model investigasi framework yang digunakan.

1. Computer Forensic Investigative Process (1984)

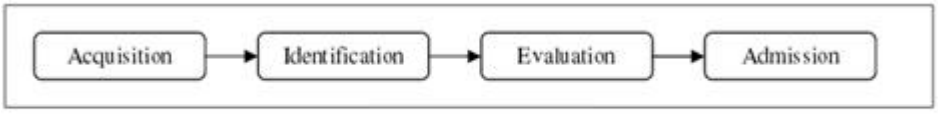


Figure 1: Computer Forensic Investigative Process

2. DFRWS Investigative Model (2001)

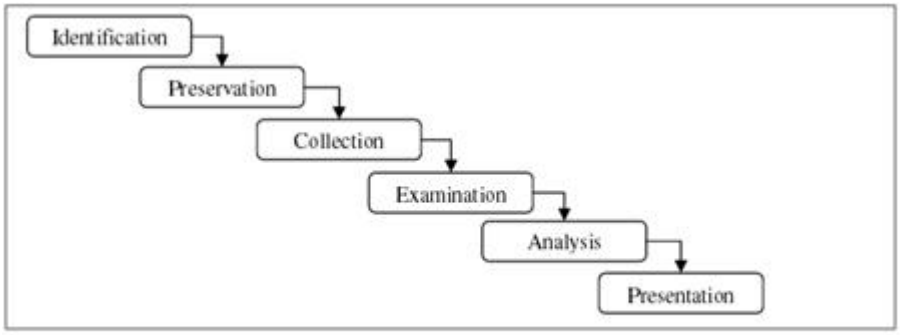


Figure2: DFRWS Investigative Model

3. Abstract Digital Forensics Model (ADFM) (2002)

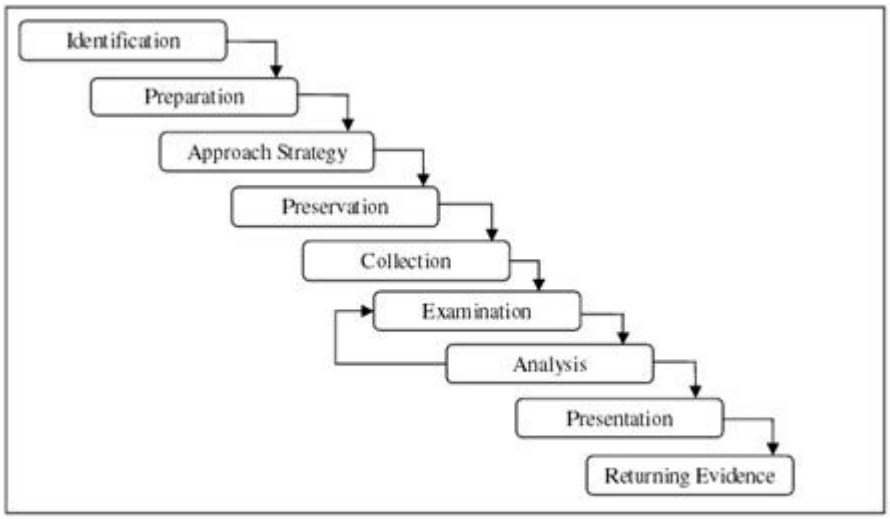


Figure 3: Abstract Digital Forensics Model

4. Integrated Digital Investigation Process (IDIP) (2003)

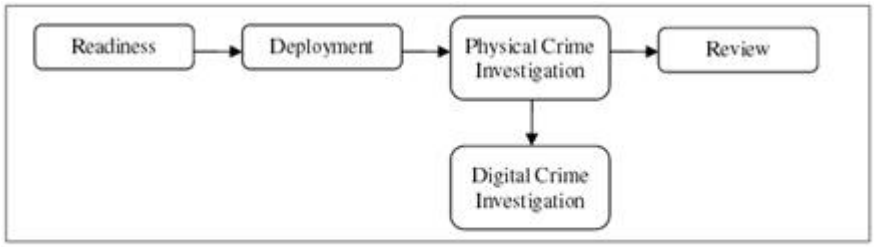


Figure 4: Integrated Digital Investigation Process

5. Enhanced Digital Investigation Process Model (EDIP) (2004)

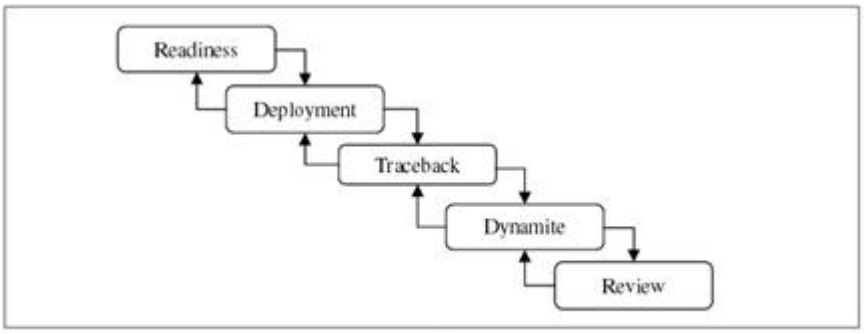


Figure 5: Enhanced Digital Investigation Process Model

6. Computer Forensics Field Triage Process Model (CFFTPM) (2006)

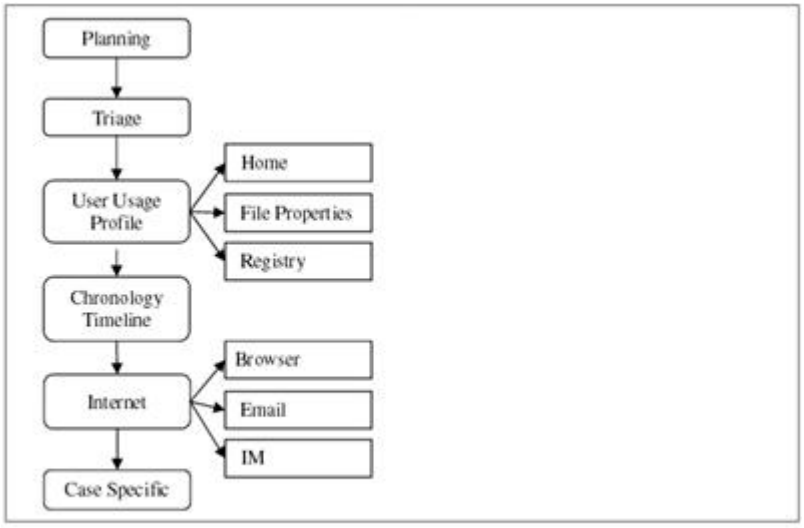


Figure 6: Computer Forensics Field Triage Process Model

7. Digital Forensic Model based on Malaysian Investigation Process (DFMMIP) (2009)

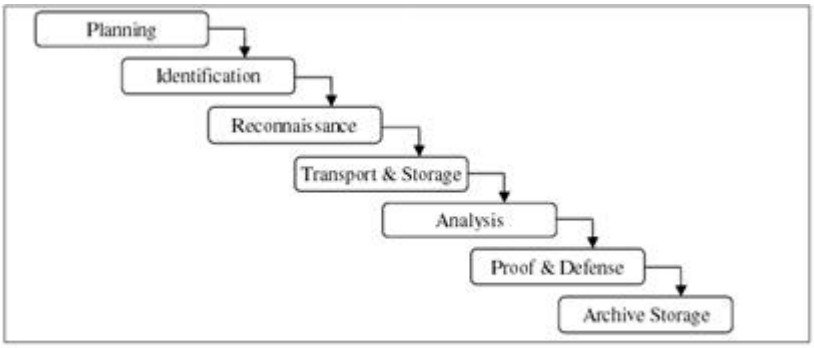


Figure 7: DFMMIP model

8. Generic Computer Forensics Investigation Model (2014)

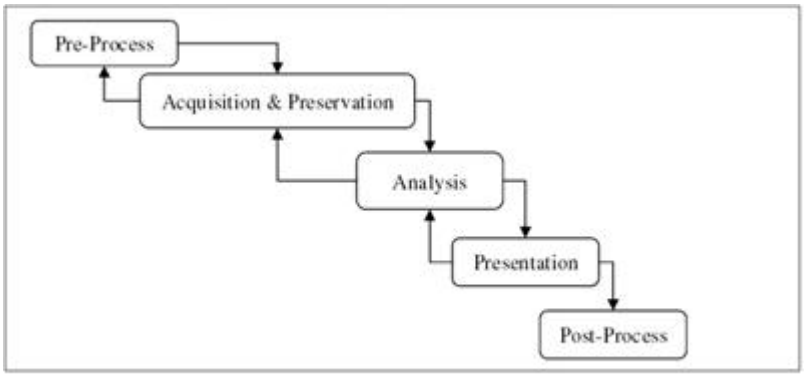
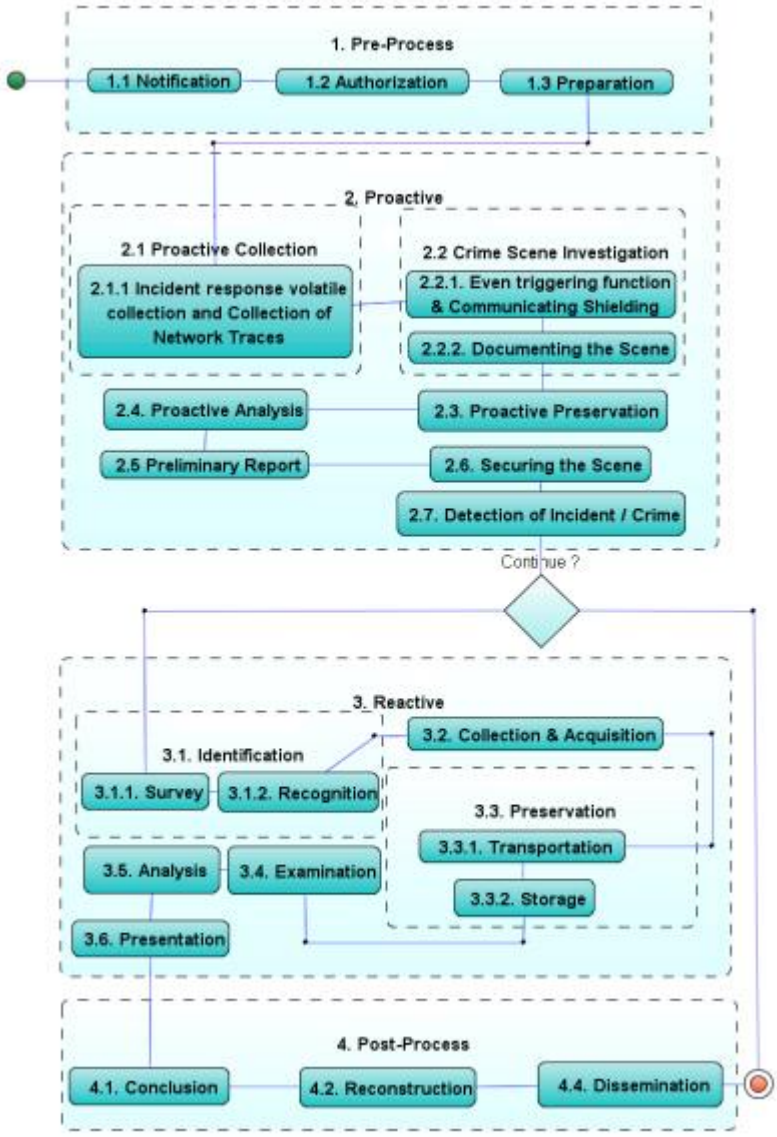


Figure 8 : Generic Computer Forensic Investigation Model (GCFIM)

9. Integrated Digital Forensics Investigation Framework (2014)



Pada phase terakhir ini, penulis akan mengulas tuntas, bagaimana framework ini bekerja dalam suatu model investigasi yang bersumber dari publikasi dalam researchgate.com

IDFIF ini terbagi menjadi empat tahapan yakni ***Pre-Process, Proactive, Reactive dan Post-Process.***

1. Pre-Process

Merupakan tahapan permulaan yang meliputi Notification yakni pemberitahuan pelaksanaan investigasi ataupun melaporkan adanya kejahatan kepada penegak hukum. Authorization merupakan tahapan mendapatkan hak akses terhadap barang bukti dan status hukum proses penyelidikan. Yang terkhir dari tahap ini adalah preparation yakni tahap persiapan yang meliputi ketersediaan alat, personil dan berbagai hal kebutuhan penyelidikan.

2. Proactive

Dalam tahapan Proactive terdapat tujuh tahapan pendukung yakni :

a. *Proactive Collecction* merupakan tindakan cepat mengumpulkan barang bukti di tempat kejadian perkara. Tahapan ini termasuk Incident response volatile collection and Collection of Network Traces. Incident response volatile collection sendiri merupakan mekanisme penyelmatan dan pengumpulan barang bukti, terutama yang bersifat volatile. Sedangkan Collection of Network Traces adalah mekanisme pengumpulan barang bukti dan melacak rute sampai ke sumber barang bukti yang berada dalam jaringan. Tahapan ini juga memperhitungan keberlangsungan sistem dalam pelakasanaan pengumpulan barang buktinya.
b. *Crime Scene Investigation* sendiri terdiri dari tiga tahapan pokok yakni Even triggering function & Communicating Shielding dan Documenting the Scene. Tujuan pokok dari tahapan ini adalah mengolah tempat kejadian perkara, mencari sumber pemicu kejadian, mencari sambungan komunikasi atau jaringan dan mendokumentasikan tempat kejadian dengan mengambil gambar setiap detail TKP.
c. *Proactive preservation* ini adalah tahapan untuk meyimpan data/kegiatan yang mencurigakan melalui metode hashing.
d. *Proactive Analysis* adalah tahapan live analysis terhadap barang temuan dan membangun hipotesa awal dari sebuah kejadian.
e. *Preliminary Report*, merupakan pembuatan laporan awal atas kegiatan penyelidikan proaktif yang telah dilakukan.
f. Securing the Scene di tahap ini dilakukan sebuah mekanisme untuk mengamankan TKP dan melindungi integritas barang bukti.
g. *Detection of Incident / Crime*, di tahap ini adalah tahap untuk memastikan bahwa telah terjadi pelanggaran hukum berdasarkan premilinary report yang telah dibuat. Dari tahapan ini diputuskan penyelidikan cukup kuat untuk dilanjutkan atau tidak.

3. Reactive

Merupakan tahapan penyelidikan secara tradisional meliputi Identification, Collection & Acquisition, Preservation, Examination, Analysis dan Presentation.

4. Post-Process

Merupakan tahap penutup investigasi. Tahapan ini mengolah barang bukti yang telah digunakan sebelumnya. Tahapan ini meliputi mengebalikan barang bukti pada pemiliknya, menyimpan barang bukti di tempat yang aman dan melakukan review pada investigasi yang telah dilaksanakan sebagai perbaikan pada penyelidikan berikutnya.

Dari penjelasan yang penulis uraikan, dapat ditarik kesimpulan bahwa, Integrasi model investigasi dengan Metode Sequential Logic dapat digunakan sebagai salah satu alternatif dalam proses investigasi yang sudah ada. Karakteristik yang dimiliki melalui metode ini dapat merekam histori dari masukan, sehingga dapat diasumsikan metode tersebut dapat melihat urutan DFIF sebelumnya untuk membentuk DFIF yang baru.

Sehingga semua proses investigasi tidak menimbulkan masalah baru.

Sumber :

- Phases Of A Forensic Investigation Information Technology Essay
- Comparative Digital Forensic Model
- Common Phases of Computer Forensics Investigation Models
- N. L. Beebe & J. G. Clark, (2004) “A Hierarchical, Objective-Based Framework for the Digital Investigations Process”, in Proceeding of Digital Forensic Research Workshop (DFRWS), Baltimore, Maryland.
- 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

All is about imagination - Endang Kurniawan
Sumber : https://endangkurniawan.com/article-investigation-models-membangun-integrated-digital-forensics-investigation-framework-idfif-menggunakan-metode-sequential-logic.html