Anti-Forensics and Anti-Anti-Forensics

Sumber : [https://www.youtube.com/watch?v=1PEOCAxR5Hk]

Pada conference ini membahas beberapa topik, diantaranya :

1. Teknik yang komplek dalam penyelidikan digital-forensik
2. Metodologi untuk mengurangi teknik yang komplek
3. Komplikasi digital lainnya

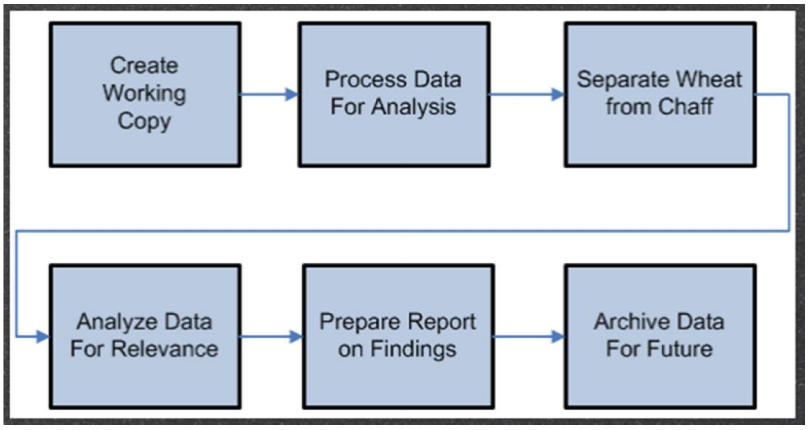
Metodologi khusus yang digunakan adalah :

- *Copy First, Ask Questions Later :* Metode ini biasanya digunakan oleh penegak hukum atau polisi.
- *Assess relevance first, copy if necessary :* Metode ini untuk semua jenis investigasi
- *Remote analysis of live system, copy targeted evidence only :* sedangkan metode yang ketiga ini biasanya digunakan oleh perusahaan yang bermasalah dengan karyawannya ataupun kasus pribadi.

Teknik klasik pada platform forensic yang biasanya orang awam lakukan dan teknik ini sudah jarang digunakan, ialah :

- HDD Scrubbing / File Wiping : menimpa area hardisk berulang kali.
- Encryption : TrueCrypt, PGP, dll
- Physical Destruction

Secara khusus digital forensic memiliki alur kerja. Alur kerja ini dapat memudahkan proses penyelidikan pada kasus-kasus yang ditangani. Dibawah ini merupakan alur kerja pada digital forensic.



- *Create working copy* : Gambar HDD, Copy file dari jarak jauh untuk analisis.
- *Process data for analysis* : File hash, menganalisa signature.
- *Separate wheat from chaff* : NIST atau NSRL, Known File Filter (KFF), Keyword Searches.
- *Analyze data for relevance* : Melihat foto, membaca dokumen, analisa lembar kerja, mengekspor file untuk analisis keaslian file dan Bookmark.
- Prepare report on findings : Meliputi gambar kecil, foto, atau potongan gambar ; Menulis prosedur (Copy / Paste dari kasus serupa untuk mempercepat workload), Melampirkan lampiran, daftar, dll.
- Archive data for future : Gambar disimpan di pusat NAS, rak HDD untuk digunakan di kemudian hari.

Pada alur kerja ada beberapa metode yang dapat mengurangi teknik yang komplek pada digital forensic, diantarnya :

1. Data saturation, hal-hal sederhana yang mengurangi teknik komplek ialah :

- Memiliki banyak media
- Hentikan membuang perangkat
- Menggunakan setiap perangkat / kontainer secara rutin jika memungkinkan.

2. non- standard RAID

- biasanya RAID membagikan pola stripe, ukuran blok dan parameter lainnya
- gunakan hardware RAID controller biasa

3. File signature masking : diidentifikasi oleh beberapa byte pertama, Hal ini memudahkan untuk mencocokan berkas yang palsu.
4. NSRL Scrubbing
5. Scrambled MACE Times
6. Restricted filenames
7. Circular reference : Ketika referensi melingkar dilanjutkan, bisa menyebabkan program untuk memasukkan loop tak terbatas.
8. Broken log files : Membuang karakter di bagian tengah dari rekaman yang akan membingungkan beberapa parser untuk memikirkan entry baru yang telah dimulai
9. Use lotus note : Lotus Notes menggunakan file NSF untuk menahan email, mirip dengan file PST. file ID meliputi user ID dan kunci enkripsi yang dapat dibuka dengan sandi pengguna 2 jam per custodian.
10. Hash collisions
11. Dummy HDD : Menggunakan komputer tanpa hard drive sangat mudah saat ini berkat removable media besar