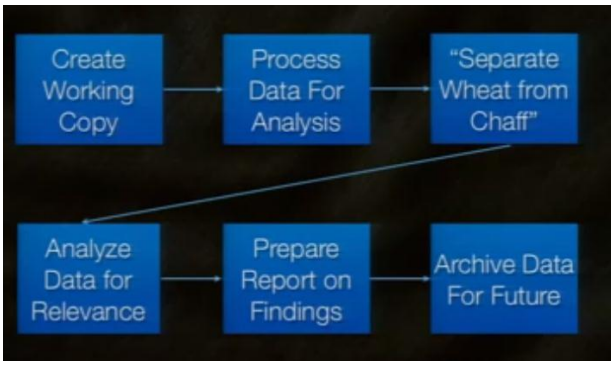
NAMA : FAHRUL ROZI
NIM : 090111813200022
TUGAS KEAMANAN JARINGAN KOMPUTER

Anti-forensics and Anti-Anti-Forensics Attack

Pembicara : Michael Perklin

Terdapat beberapa typical methodology dalam forensic yang pertama yaitu pertama salin (copy) dan kemudian ajukan pertanyaan, pada pengajuan pertaanyaan sesuai dengan typical hukum pelaksanaan. Kemudian dalam metodologi menilai relevansi ,jika perlu salin semua informasi yang didapat dari semua tipe investigasi. Remote analisis dari system yang masih hidup atau sedang menyala , salin hanya bukti yang ditargetkan. Secara dasar target berinteraksi terhadap network dan mesin dari aktivitas tersebut dapat di scan dan kemudian akan dijadikan bukti.

Adapun 6 typical workflow (alur kerja) yaitu :



- Create working copy

  Pada tahap ini yaitu membuat salinan perkerjan yang akan dilakukan untuk investigasi dari target system.
- Process data for analisys

  Kemudian lakukan analisis dari proses data sehingga akan memungkinkan kasus tersebut akan sukses.
- Separate wheat from chaff

  Maksudnya mungkin saja harus melakukan pencocokan informasi yang telah dilakukan dari sebuah kasus.
- Analyze data for relevance

  Menganalisis data sehingga data tersebut agar menjadi relevan
- Prepare report on findings

  Persiapan laporan dalam pencarian , setiap investigasi atau bukti yang telah di dapat buatlah sebuah laporan
- Archive data for future

  Simpan laporan atau jadikan arsip data sehingga dapat diguaka untuk masa yang akan datang ,atau kasus yang bersangkutan.

NAMA : FAHRUL ROZI
NIM : 090111813200022
TUGAS KEAMANAN JARINGAN KOMPUTER

Terdapat 3 teknik anti forensic classic yaitu :

1. HDD Scrubbing / file wiping
   Menyembunyika file dengan cara scrubbing hardisk atau dapat dengan cara oenghapusan file.
2. Encryption
   Dapat dilakukan dengan cara mengencrypsi pada sebuah file
3. Physical Destruction
   Membangun secara fisik.

Dalam anti forensic AF terdapat beberapa teknik yang dapat membingungkan menginvestigasi typical workflow antara lain:

1. AF teknik #1

- Data saturation
  Dalam data saturation terdapat banyak pemilik dalam sebuah LOT media, berhenti untuk membuang perangkat, gunakan setiap device/ wadah untuk potongan kecil dari kejahatan anda, investigator akan pergi kemanapun.
- Mitigating data saturation
  Dalam teknik tersebut adapun cara meringankan dari data saturation yaitu dengan cara proses parallel, gunakan beberapa mesin akuisisi, dapat memanfaatkan hardware dari tersangka.

2. AF teknik #2

- Non-standart RAID
  Tidak adanya RAID yang standar seperti ukuran blok dan parameter lainya, jarang menggukan peraturan , jarang menggunakan hardware RAID
- Mitigating Non-standart RAID
  Untuk meringankan tidak adanya RAID yang standart ini yaitu gunakan boot disc,

3. AF teknik #3

- File signature masking
  File signature dapat diindentifikasi dari file header / footer , dalam sebuah file dapat terdapat kejahatan didalamnya.
- Mitigating File signature masking
  Dapat meringankan dengan cara gunakan hashng fuzzy untuk mengindentifikas file yang mencurugakan.

4. AF teknik #4

- Rendering NSRL useless
  Yang dapat membingungkan tentu saja pelaku dapat memodifikasi file program dari semua system, memodifikasi string didalam file.

- Mitigating Rendering NSRL useless
  Cara menringankannya yaitu dengan cara cari dengan teliti dan jangan memfilter, mengidentifikasi file yang berguna dari pada menghilangkan file yang tidak berguna.

5. AF teknik #5

- Scrambled MAC times
  Maksud dari MAC disini dalah modified, accessed ,created. Secara acak setiap waktu.
- Mitigating Scrambled MAC times
  Mengabaikan tanggal pada semua metadata, mengidentifikasi set dari waktu yang sama.

6. AF teknik #6

- Restricted filename
  Nama file yang dibatasi , bahkan windows 7 pun masih memiliki holdover dari DOS days.
- Mitigating Restricted filename
  Tidak pernah ekport file dengan filename yang asli, selalu mementukan nama yang berbeda.

7. AF teknik #7

- Circular references
  Dalam folder terdapat folder dengan typical yang terbatas 255 karakter pada NTFS.
- Mitigating Circular references
  Untuk meringankannya jangan mengekspor folder untuk menganalisis hanya file itu sendiri.

8. AF teknik #8

- Use lotus notes
  Terdapat masalah dalam file NSF dan file id.
- Mitigating Use lotus notes
  Jangan terpusat ada file gunakan kebiasaan dalam lingkungan sekitar.

9. AF teknik #9

- Hash collisions
  MD5 dan SHA1 hash digunakan untuk mengidentifikasi file dalam laporan, Pencarian untuk file dengan hash akan menghasilkan hasil yang tak terduga
- Mitigating Hash collisions
  Cara meringankan hash collision ini yaitu Menggunakan fungsi hash dengan lebih sedikit collision (SHA1, SHA256, Whirlpool).

10. AF teknik #10

- Dummy HDD

Memiliki PC dengan HDD yang tidak digunakan USB-boot dan mengabaikan HDD untuk penggunaan sehari-hari.

- Mitigating Dummy HDD
  Cara meringankan dummy pada hardisk yaitu Selalu periksa drive USB,biasanya Pagefile pada drive USB dapat menunjukkan lokasi jaringan.