GOV-CSIRT INDONESIA

Panduan Pelaksanaan *Technical Workshop*: Akuisisi Data Pada Kegiatan Communication Check Gov-CSIRT

Skenario 1: Akuisisi Data

Tujuan

Skenario 1 dilakukan untuk melakukan kegiatan akuisisi data server pada suatu instansi pemerintah yang terkena suatu insiden.

Persiapan

Terdapat hal-hal yang diperlukan dalam melaksanakan skenario ini, yaitu:

a. Perangkat Laptop atau Komputer masing-masing dengan spesifikasi minimal :
   - Sistem Operasi yang digunakan : Windows atau Linux
   - RAM : 4 GB
   - Aplikasi : FTK Imager versi berapapun

b. Sebuah penyimpanan Flashdisk berukuran maksimal 16 GB untuk kegiatan akuisisi.

Langkah-langkah

Setelah memastikan persyaratan yang dijelaskan dipenuhi, selanjutnya dijelaskan skenario yang akan diselesaikan.

Pada suatu daerah di pemerintah A, terdapat Tim CSIRT yang bertindak sebagai CSIRT yang berwenang pada daerah tersebut. Tim CSIRT mendapatkan sebuah informasi bahwasanya terdapat sebuah insiden siber berupa serangan *web defacement* pada Dinas XYZ. Diketahui bahwa *website* yang terdampak tersebut pada URL http://xyz.go.id, yang berada pada sebuah server ABC. Selanjutnya Tim CSIRT mengirimkan sebuah email notifikasi insiden kepada Dinas XYZ tersebut untuk dapat ditinjaklanjuti. Dinas XYZ menerima email tersebut, menanggapi dan segera mengirimkan permohonan asistensi kepada Tim CSIRT daerah yang ada. Selanjutnya Tim CSIRT daerah, khususnya Ketua Tim CSIRT menanggapi permohonan asistensi tersebut dan melakukan investigasi lebih lanjut dengan tahapan yang akan dijelaskan pada skenario ini.

Pada skenario ini, USB yang telah disiapkan oleh masing-masing peserta diumpamakan sebagai sebuah server dari *website* yang terdampak insiden. Selanjutnya terdapat langkah-langkah yang dilakukan dalam melakukan Skenario 1. Langkah-langkah tersebut adalah sebagai berikut:

a. Tahap Identifikasi

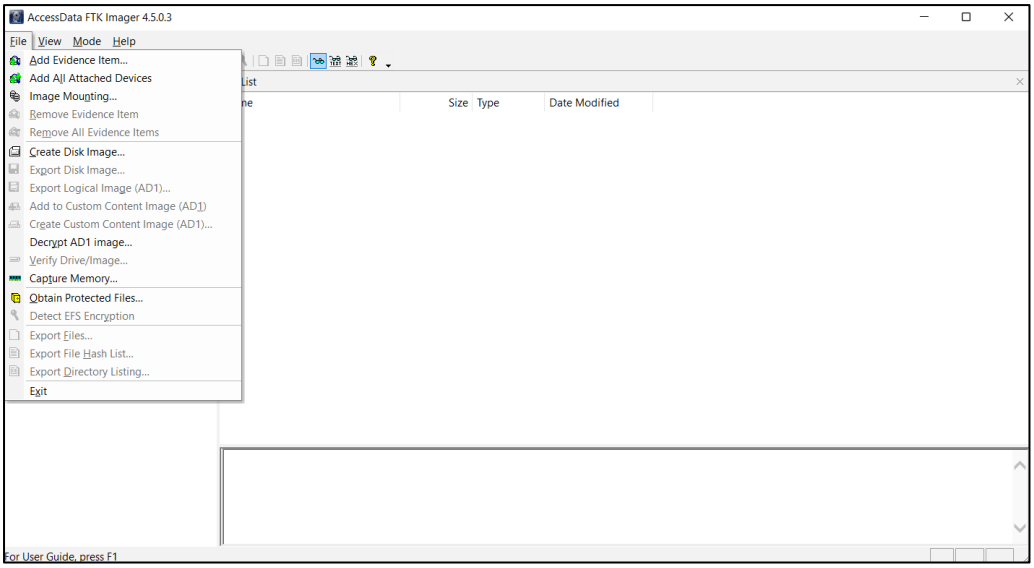
   Pada tahap ini, Anda dan Tim CSIRT anda menuju ke lokasi server terdampak untuk dapat melakukan akuisisi data. Dari hasil akuisisi data tersebut, nantinya akan dicatat beberapa hal yang penting dalam bentuk form pendokumentasian seperti *chain of custody*, seperti :

   - Merk server yang diakuisisi (Dalam skenario ini merk USB)
   - Seri server (Dalam skenario ini seri USB), dan
   - Kapasitas (Ukuran dalam byte)

b. Tahap Akuisisi

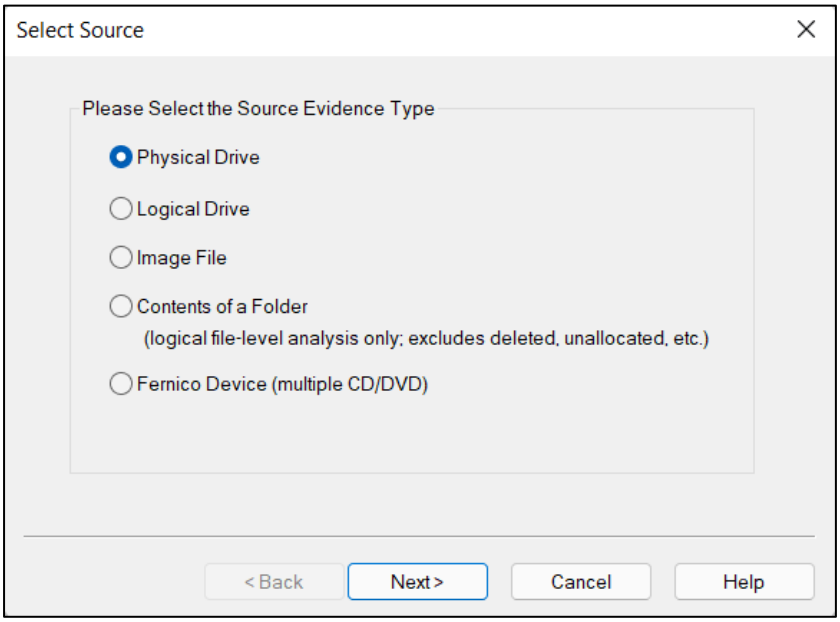
   Pada tahapan akuisisi, kondisi *environment* yang ada menggunakan sistem operasi Windows, sehingga dapat menggunakan aplikasi FTK Imager untuk melakukan akuisisi data. Proses akuisisi dapat dilakukan dengan langkah berikut :

   - Buka Aplikasi FTK Imager dan klik menu bar *File*, kemudian pilih ‘Create Disk Image…’ untuk melakukan tahapan akuisisi.



Gambar 1. Tampilan *Create Disk Image*

- Pilih sumber data barang bukti yang akan dilakukan akuisisi. Karena pada skenario ini kita akan melakukan akuisisi keseluruhan server, maka pilih pada opsi 'Physical Drive'.



Gambar 2. Sumber *evidence* yang akan dibuat

Keterangan :

- *Physical Drive*, akuisisi keseluruhan data pada server
- *Logical Drive*, akuisisi masing-masing partisi yang ada pada server
- *Image File*, akuisisi image data

- *Contents of a folder*, akuisisi pada tahap *logical* (Kecuali *file-file* yang sudah dihapus)

- Selanjutnya lanjutkan proses akuisisi dengan mengisi opsi-opsi yang harus diisi tempat direktori maupun tipe *image file* hingga proses akhir, dan klik ‘Start’ untuk mengakuisisi.

c. Tahap Preservasi

Tahapan ini bertujuan untuk memastikan data yang telah diakuisisi. Hal yang harus dicatat dalam proses ini yaitu :

1. Nama *file* yang telah diakuisisi,
2. Nilai Hash *file* yang telah diakuisisi,
3. Ukuran *file* yang telah diakuisisi, dan
4. Tanggal *file* diakuisisi.