PRAKTIKUM 2: (DIGITAL IMAGING) FTK IMAGER WINDOWS BASE

Pertemuan ke : 2

Total Alokasi Waktu : 90 menit
- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

Total Skor Penilaian : 100 %
- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

Pemenuhan CPL dan CPMK

CPL-04	Mampu berpikir logis, kritis, sistematis dan inovatif, dan mampu mengambil keputusan secara tepat dibidang keahliannya
CPMK-01	Mahasiswa memahami tahapan investigasi digital forensik

2.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan: (sesuai dengan RPS)
1. Mampu melakukan akuisisi digital evidence dengan tools windows
2. Mampu mengidentifikasi jenis-jenis digital evidence dan autentikasinya

2.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

CPL-04	CPMK-01	Mahasiswa dalam menerapkan Proses akuisisi digital evidence & Analisisi digital evidence md5 sha

2.3. TEORI PENDUKUNG

Seperti telah diketahui bersama, bahwa cara untuk mendapatkan bukti digital adalah dengan melakukan akuisisi barang bukti elektronik. Akuisisi yang dimaksud adalah dengan mengidentifikasi, mengumpulkan, membuat image (imaging) atau menyalin (cloning/copy bit by bit) dan mengamankan barang bukti elektronik.

Untuk proses imaging sendiri dapat dilakukan dengan 2 cara:

1. Physical

   Membuat image dari physical drive yang biasanya berupa hard disk atau flash disk, atau dapat dikatakan drive secara fisik. Jika kapasitas drive adalah 500 GB, maka image yang dihasilkan juga akan memiliki ukuran sebesar 500 GB (kecuali jika dikompres). Jadi proses physical imaging ini akan mengclone hard disk atau flash disk secara fisik, tidak peduli apakah ada isinya atau tidak. Biasanya proses akuisisi ini dilakukan untuk melihat apakah ada file-file yang didelete.
2. Logical

   Membuat image dari logical drive, berupa drive di computer, yaitu biasanya A:, C:, D:, dst. Bisa saja satu harddisk dipartisi menjadi 2 atau lebih logical drive, misalnya C: untuk system dan D: untuk data. Jika membuat image dari logical drive berarti satu drive utuh termasuk bagian yang kosong/tidak ada datanya.

2.4. HARDWARE DAN SOFTWARE

Alat dan bahan yang digunakan dalam praktikum ini yaitu:
1. Komputer.

2. FTK Imager App.
3. Flashdisk (Partisi Hardisk)

2.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-04	CPMK-01	Mengapa seorang investigator digital forensik harus melakukan imaging evidence dengan serangkaian proses investigasi!	50
2.	CPL-04	CPMK-01	Apa perbedaan imaging dengan copy evidence biasa?	50

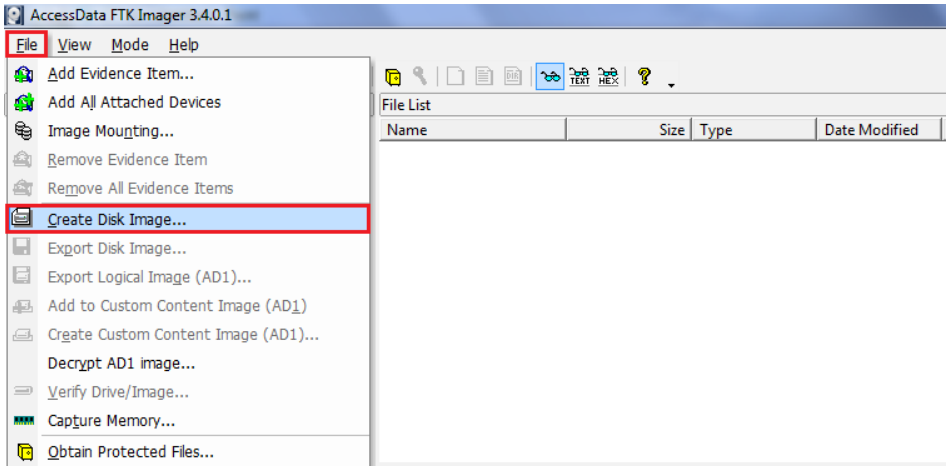
2.6. LANGKAH PRAKTIKUM

Aturan Penilaian (Total Skor: 100):

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-04	CPMK-01	Selesaikan langkah praktikum berikut dengan masing-masing evidence	Screen Shot Hasil praktikum	100

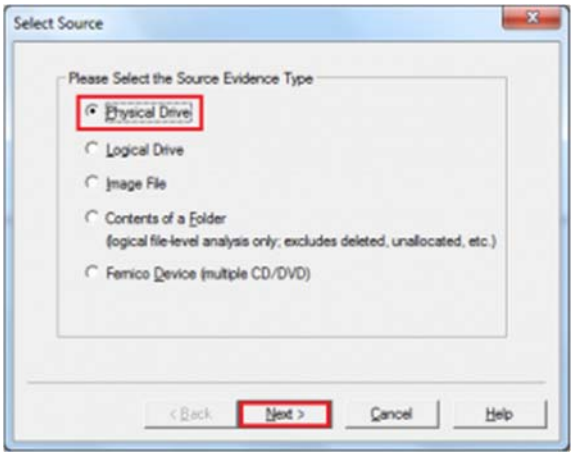
Pada praktikum kali ini akan dibahas mengenai cara untuk melakukan physical imaging sebuah flashdisk menggunakan FTK Imager App.
Ikuti langkah praktikum berikut ini:

1. Download dan *install* aplikasi FTK Imager di link berikut https://bit.ly/2TN9qAD
2. Buka aplikasi FTK Imager yang sudah di-*install*, klik **Start All Programs AccessData FTK Imager**. Dapat pula melalui shortcut di Desktop jika ada.
3. Pilih menu **File Create Disk Image**



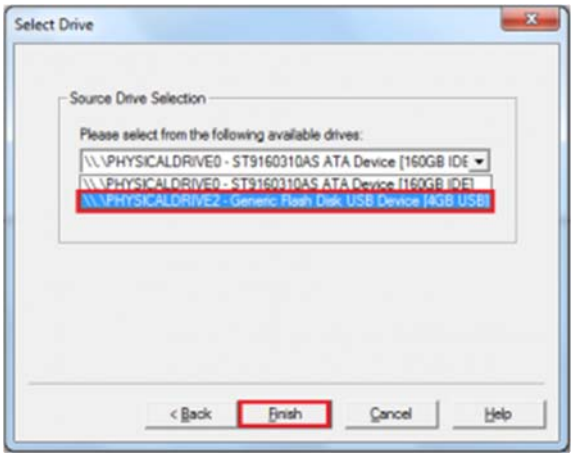
Gambar 2.1 FTK Imager Create Disk Image.

4. Pilih ***Physical Drive***, kemudian klik **Next**.



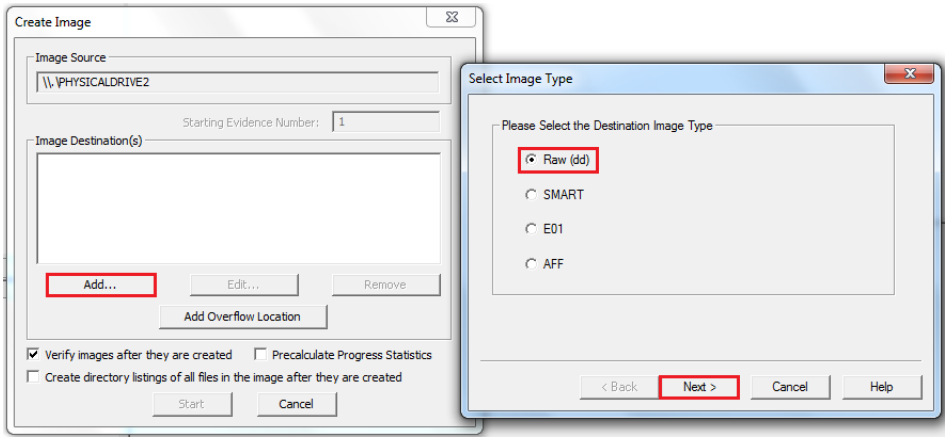
Gambar 2.2 Physical Drive.

5. Pilih *device* yang akan dibuat *physical image*-nya. Dalam hal ini, pilih flashdisk yang tadi sudah terbaca sistem, kemudian klik tombol **Finish**.



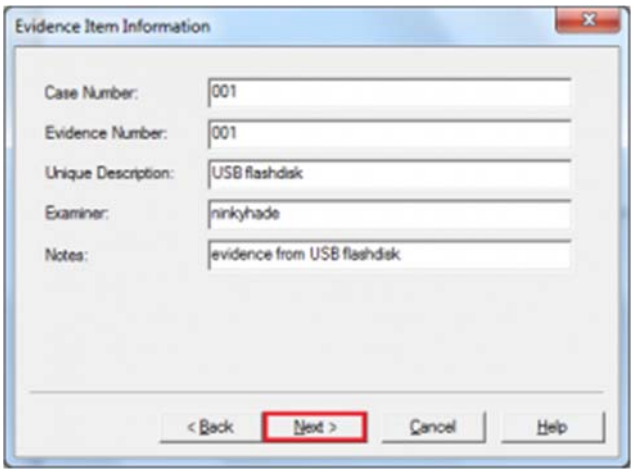
Gambar 2.3 Pilih device yang akan dibuat physical image.

6. Atur setting *destination folder* dengan tombol **Add**. Lalu pilih format **Raw(dd)** agar hasilnya sam a dengan hasil pada praktikum linux yang menggunakan format *raw*. Klik tombol **Next**.



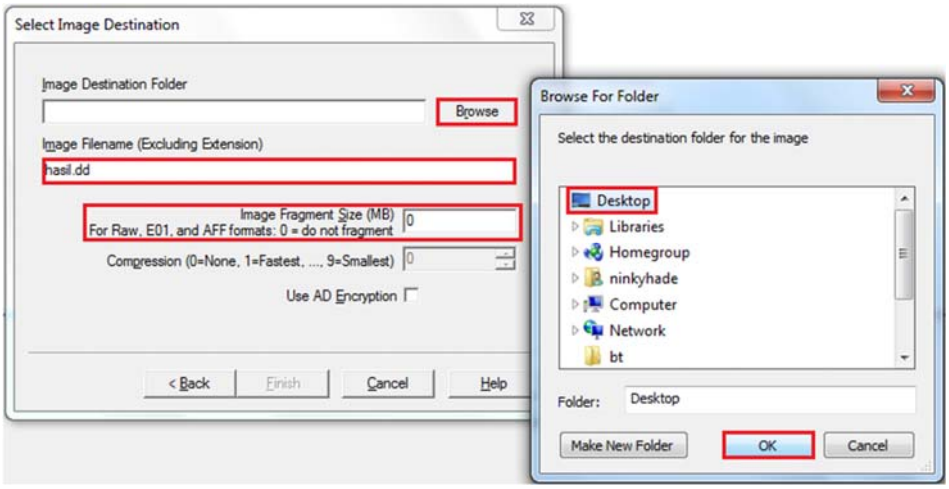
Gambar 2.4 Destination Folder.

7. Isikan informasi tambahan, sesuaikan dengan kondisi praktikan. Klik tombol **Next**.



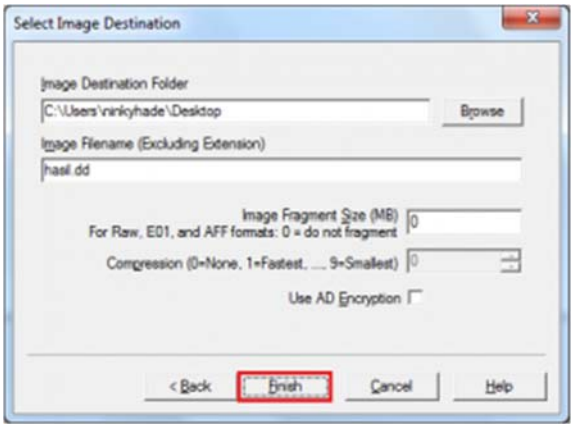
Gambar 2.5 Informasi Tambahan.

8. Pilih *destination folder* dengan klik tombol **Browse**. Pada praktikum kali ini, pilih **Desktop** sebagai *destination folder* agar lebih memudahkan. Klik tombol **OK**.
   Isikan nama file *image* berikut ekstensi file-nya. Pada praktikum kali ini, nama file yang digunakan adalah **hasil.dd**.
   Isikan angkal **0** (nol) pada bagian **Image Fragment Size** agar hasil *imaging* tidak dipecah-pecah menjadi beberapa file.



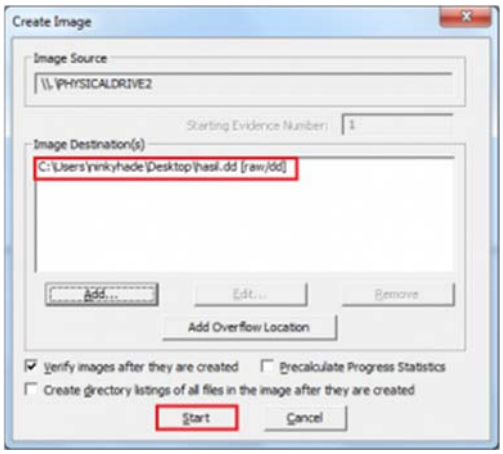
Gambar 2.6 Destination Folder Hasil Capture.

9. Klik tombol **Finish**.



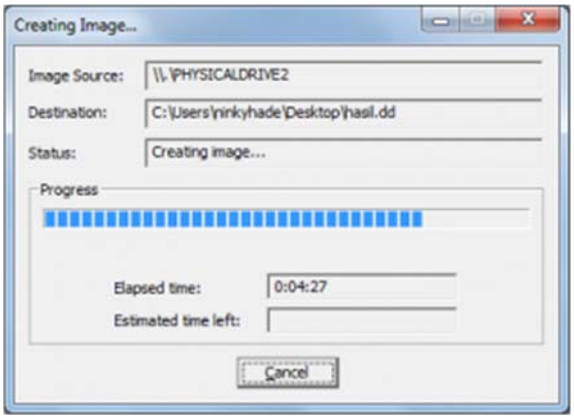
Gambar 2.7 Destination Image

10. Muncul *window* berisi informasi *destination folder*. Klik tombol **Start**.



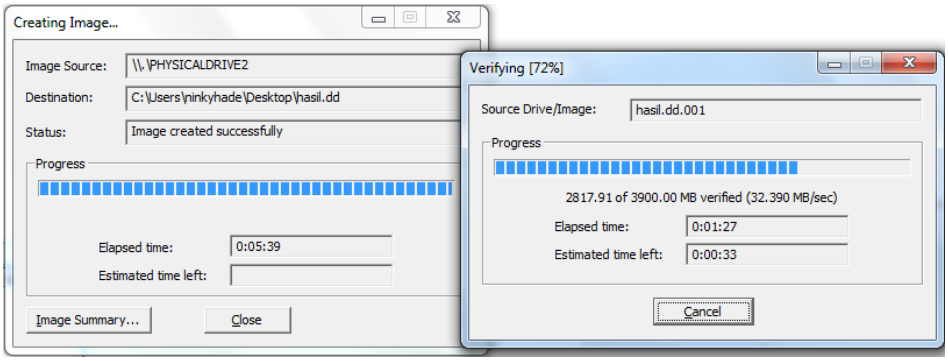
Gambar 2.8 Destination Image Directory.

11. Tunggu *progress*-nya sampai *imaging* selesai.



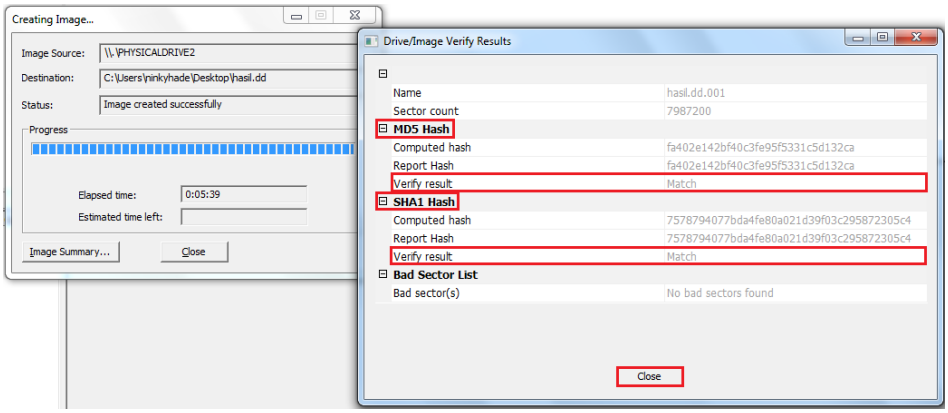
Gambar 2.9 Proses Imaging.

12. Setelah selesai proses *imaging*, akan muncul window verifikasi (*integrity check*) file *image* apakah telah sama persis nilai *hash*-nya dengan yang asli.



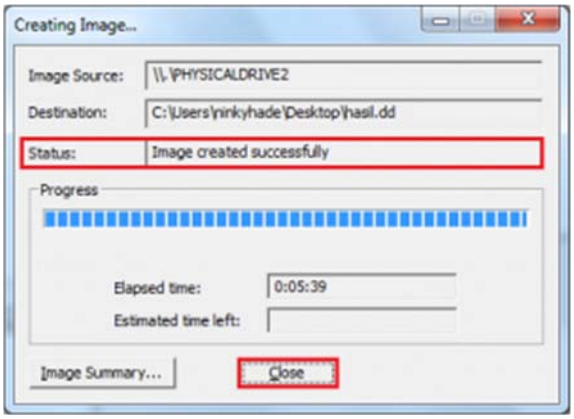
Gambar 2.10 Create & Verifying.

13. Hasil akhir dari verifikasi file adalah muncul *window* yang berisi nilai *hash* dan kecocokan nilai *hash* file *image* dengan aslinya. Amati, jika sudah sesuai lalu klik tombol **Close**.



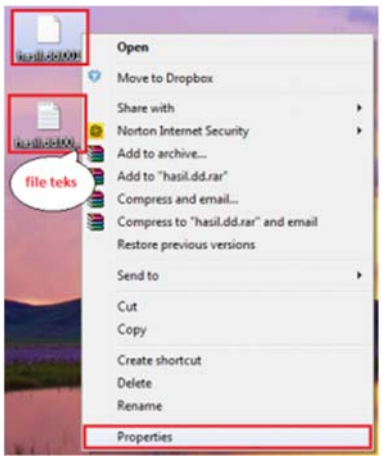
Gambar 2.11 Creating Images & SHA Cek.

14. Akan muncul *window* notifikasi bahwa proses imaging telah berhasil. Klik tombol **close**. Proses *physical imaging* terhadap flashdisk telah berhasil dilakukan.



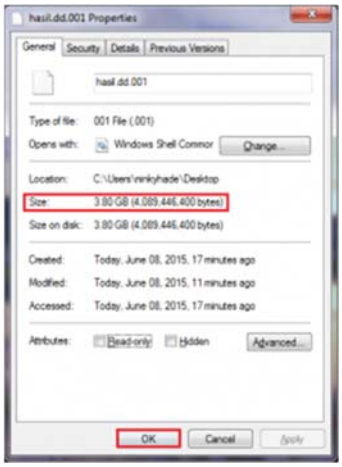
Gambar 2.12 Proses Selesai.

15. Cari file *image* yang disave di *destination folder*-nya.
16. Cek file *image* bernama **hasil.dd**. Akan ada 2 file, yaitu file *image* dan file teks (berisi informasi proses *imaging* dan hasil verifikasi/*integrity check*).
17. Pilih file *image*, klik kanan **Properties** untuk melihat *size* file *image*.



Gambar 2.15 Hasil Imaging Pada Desktop.

18. Akan muncul *window* berupa informasi mengenai *size* dari file *image* **hasil.dd** tersebut. Bandingkan *size* file *image* dengan kapasitas flashdisk yang telah dicek pada awal praktikum.



Gambar 2.16 Size On Disk.

2.7. POST-TEST

Jawablah pertanyaan berikut (**Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-04	CPMK-01	Berikan analisis hasil imaging meliputi komparasi size evidence dan hasil dari nilai Hash!	100

2.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-04	CPMK-01	20%		
2.	Praktik	CPL-04	CPMK-01	30%		
3.	Post-Test	CPL-04	CPMK-01	50%		
					Total Nilai	

LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM

Nama : **NIM :**	**Asisten:** **Paraf Asisten:**	**Tanggal:** **Nilai:**