# Praktikum 2
# (Digital Imaging) *dd linux Base*

**Pretest:**

1. Sebutkan definisi dari Digital Imaging!
2. Mengapa perlu dilakukan Digital Imaging pada barang bukti temuan?

**Langkah Praktikum:**

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* disk secara utuh. Dilakukan apabila terindikasi ada folder/file yang telah dihapus, sehingga membutuhkan *recovery* file.
**2. *Logical***
Hanya membuat *image* pada partisinya saja.
Pada postingan kali ini akan dibahas mengenai cara untuk melakukan ***physical imaging*** sebuah **flashdisk**menggunakan *command* Linux. Distro Linux yang digunakan pada praktikum kali ini adalah **Kali Linux**.

**Langkah-langkah:**

1. Tancapkan flashdisk ke komputer.

2. Cek apakah flashdisk sudah terbaca oleh sistem Linux. Cari baris yang mengandung "/dev/sd…"

**# fdisk -l**
**/dev/sdb …**

3. Lakukan proses *imaging* terhadap flashdisk dan langsung lakukan *hashing*. ***Hashing*** adalah metode untuk melakukan ***integrity check***, yaitu membandingkan hasil *imaging* apakah sama persis dengan aslinya.

**# dc3dd if=/dev/sdb of=/root/Desktop/hasil.dd hash=md5**

***Keterangan :***

- *if=/dev/sdb –> media input adalah **/dev/sdb** di mana flashdisk ditancapkan*
- *of=/root/Desktop/hasil.dd –> hasil imaging diletakkan di direktori **/root/Desktop**dengan nama file-nya adalah **hasil.dd** (format raw)*
- *hash=md5 –> algoritma hashing yang digunakan adalah **MD5***

**Cara lain menggunakan DD**
**# sudo dd if=/dev/sdb of=/root/Desktop/hasil.dd bs=512**

**Keterangan :**

- **sudo -> menjalankan perintah dengan permission ROOT**
- **if=/dev/sdb -> media input /dev/sdb dimana flashdisk ditancapkan**
- **of=/root/Desktop/hasil.dd -> hasil imaging diletakan di direktori /root/Desktop/ dengan nama file hasil.dd**
- **bs=512 -> adalah bytes yang ada pada flashdisk**

4. Tunggu sampai selesai. Output di layar akan memberitahukan bahwa proses *imaging* telah berhasil dan menampilkan nilai *hash* MD5-nya.

**c105a26e214939091239f949fd0c9aba (md5)**

5. Lakukan *integrity check*.

**# md5sum /dev/sdb**
**c105a26e214939091239f949fd0c9aba (/dev/sdb)**

atau:

**# md5sum /root/Desktop/hasil.dd**
**c105a26e214939091239f949fd0c9aba (/root/Desktop/hasil.dd)**

6. Cocokkan nilai *hash* MD5 pada md5sum dengan nilai *hash* MD5 pada proses *imaging*. Jika sama, maka hasil *imaging* sudah OK.