

# Proj 11: Acquisition menggunakan DEFT 7 (20 point)

## Kebutuhan Project

- VirtualBox
- A DEFT 7 ISO file **deft7.2.iso**, sudah tersedia di laboratorium Foresec. Bisa di download dari <http://www.deftlinux.net/>

## Mengumpulkan Files yang dibutuhkan

1. File **deft7.2.iso** tersedia di laboratorium Foresec. Jika mengerjakan di lab. Foresec, sebaiknya kopi file tersebut ke direktori yang kalian buat dan gunakan copy file tersebut. Jika kalian mengerjakannya di rumah dan memiliki akses broadband, file ISO bisa di download di sini: <http://www.deftlinux.net/>
2. Pada komputer di lab. Foresec, buat folder dengan nama kalian. Di dalamnya buat subfolder dengan nama **NAMAKAMU-proj11**.
3. Klik kanan pada link di elearning p10Evidence.zip (file yang sama pada project 10), dan simpan Evidence File ke desktop.

## Memeriksa Nilai Hash dari Evidence File

4. Di jendela Backtrack buka Terminal

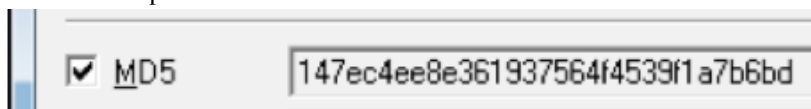
```
cd Desktop
unzip p10Evidence.zip
ls
```

maka akan terlihat ada file **Windows 2000 Professional-sparse.vmdk**

5. Gunakan md5hash untuk memeriksa nilai hash file tersebut

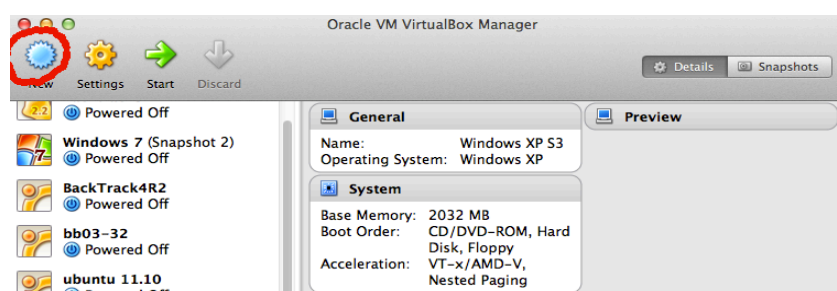
```
md5sum "Windows 2000 Professional-sparse.vmdk"
```

Pastikan nilai MD5 hash sesuai dengan nilai berikut. Membuktikan file yang didownload tidak korup.

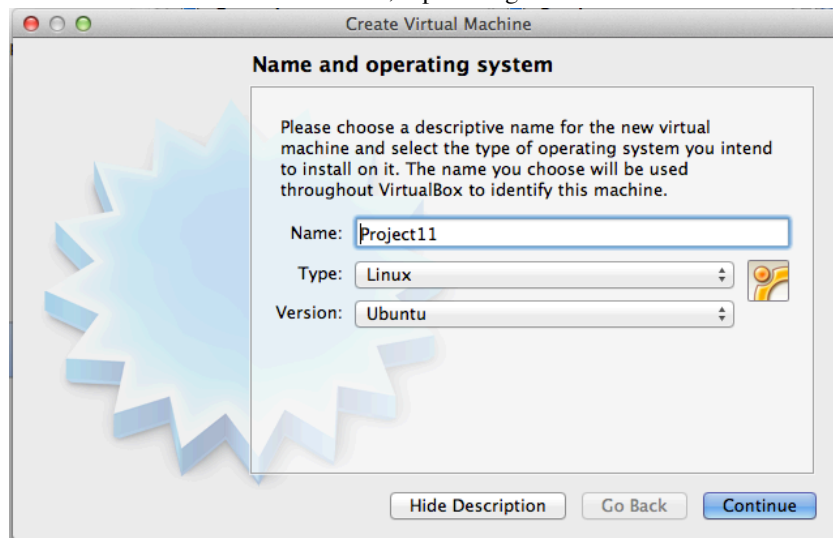


## Membuat New Virtual Machine (Bisa menggunakan Virtual Machine pada Project 10 langsung ke langkah 9 tetapi untuk evidence mounting ulang file yang baru diekstrak karena pada project 10 evidence sudah berubah)

6. Buka VirtualBox. Click "New"



otak “Name and Operating System”, isikan “Name” **Project13**, “Type” pilih **Linux** dan Version “**Ubuntu**”, seperti di gambar:



- c. Pada menu “**Memory Size**”, ketikkan **512 MB**. Kemudian Klik “*Continue*”.
- d. Pada menu “**Hard drive**”, pilih “**Create Virtual Hard drive now**”. Kemudian click “*create*”. Pilih default “**VMDK (Virtual Machine Disk)**”, click “*Continue*” pilih “**Dynamically allocated**”, click “*Continue*”, biarkan ukuran default kemudian click “*create*”. Hardisk ini digunakan untuk menampung hasil bukti evidence.
- e. Maka akan ada VirtualMachine baru dengan nama Project11.

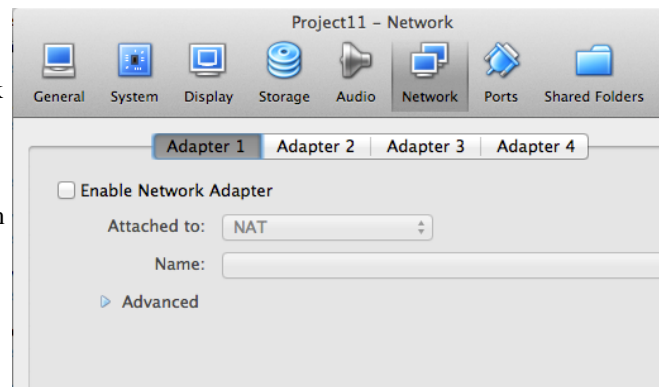
## Mengkoneksikan Evidence Drive

7. Pada VirtualBox pada VirtualMachine Project11, klik kanan kemudian pilih *setting*. Akan muncul jendela menu General.
  - a. Klik pada “**Storage**”, maka akan seperti berikut:
  - b. Pilih “**Add Hardisk**”, icon tanda + dengan latar hd.
  - c. Akan muncul menu, pilih “*choose existing disk*”.
  - d. Arahkan ke file “**Windows 2000 Professional-sparse.vmdk**” pilih, kemudian click Select.

## Disable Jaringan

8. Masih pada menu Seting VirtualBox Project11, click pada icon “**Network**”. Buang tanda centang pada “**Enable Network Adaptor**”, seperti di bawah ini: Click **OK**.

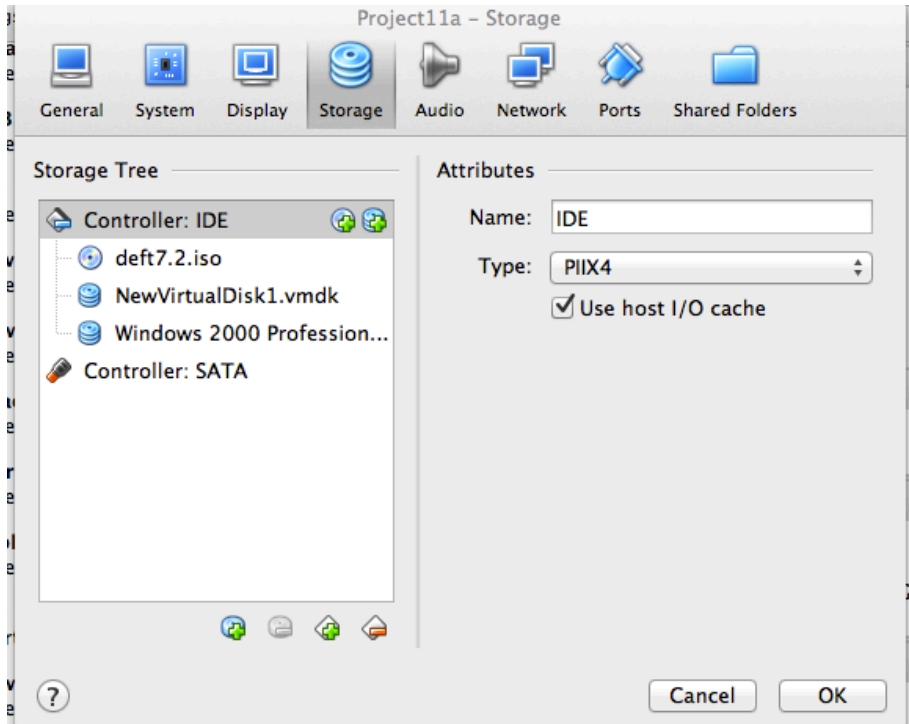
Pada aturan dasar forensic, **WORK IN ISOLATION**—dengan kata lain, jangan terkoneksi ke internet ketika melakukan imaging drives.



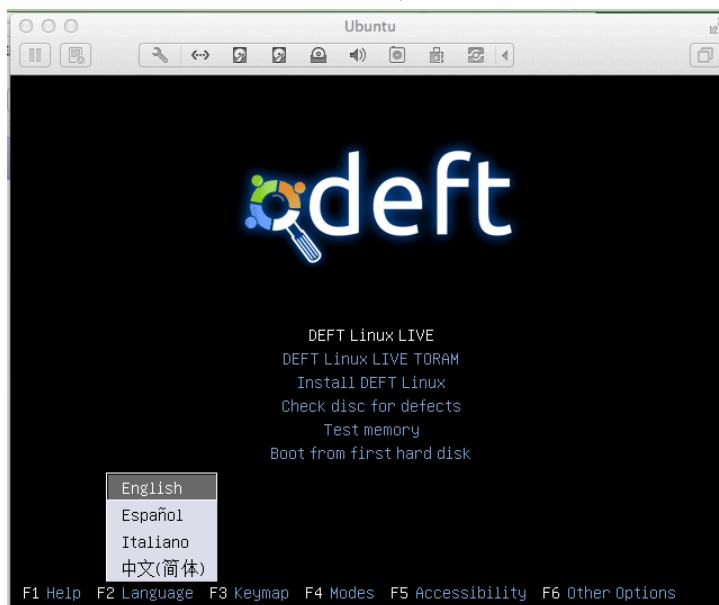
## Booting dari file ISO DEFT 7 dalam Forensics Mode

9. Seperti pada langkah 7, pada menu seting VirtualMachine Project11.
  - a. Klik pada “**Storage**”,
  - b. Pilih “**Add CD/DVD Device**”, icon tanda + dengan latar cd.

- c. Akan muncul menu, pilih “**Choose disk**”.
- d. Arahkan ke file image ISO DEFT7. Maka akan seperti pada gambar.



- e. Kemudian click **OK**.
- f. Kemudian klik Pada icon “System”.
- g. Kemudian rubah urutan “Boot Order”, menjadi CD/DVD ROM yang paling atas dengan mengklik panah ke atas atau ke bawah, sehingga urutan booting menjadi seperti berikut.
- h. Kemudian klik tombol **OK**.
- i. Kemudian jalankan Komputer Virtual Project11
- j. Akan muncul DEFT 7 berjalan seperti pada gambar. Tekan Enter untuk menerima default language **English**. Tekan Enter untuk menerima pilihan default boot selection “**DEFT Linux LIVE**”.



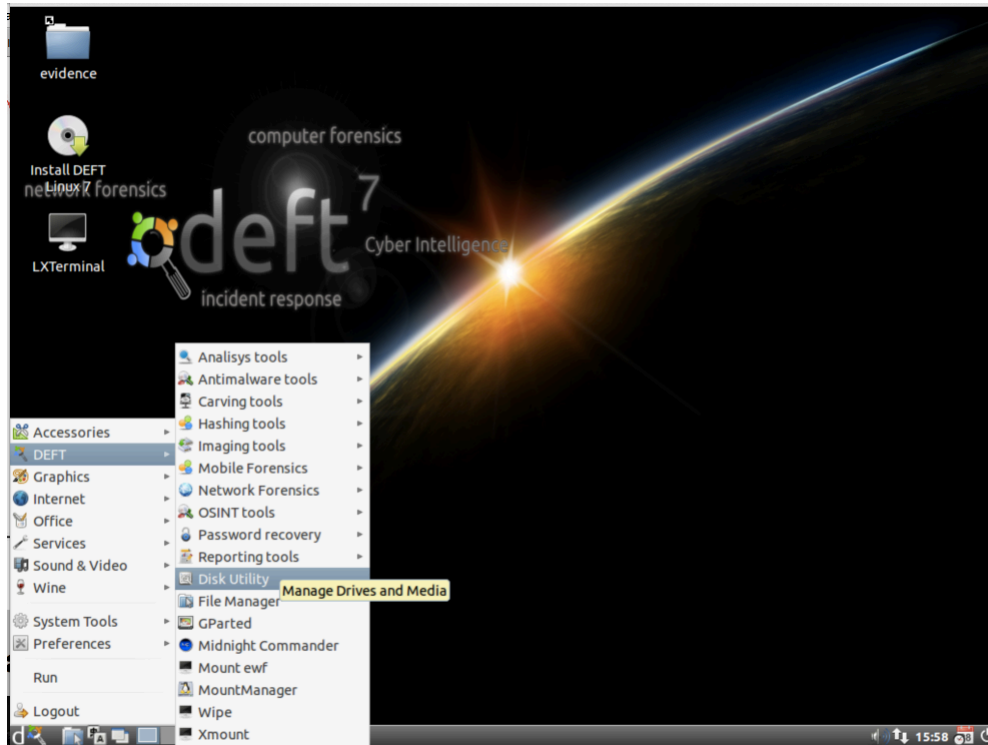
Ketika muncul prompt **deft ~ %**, masukkan perintah berikut diakhiri dengan Enter:

**deft-gui**

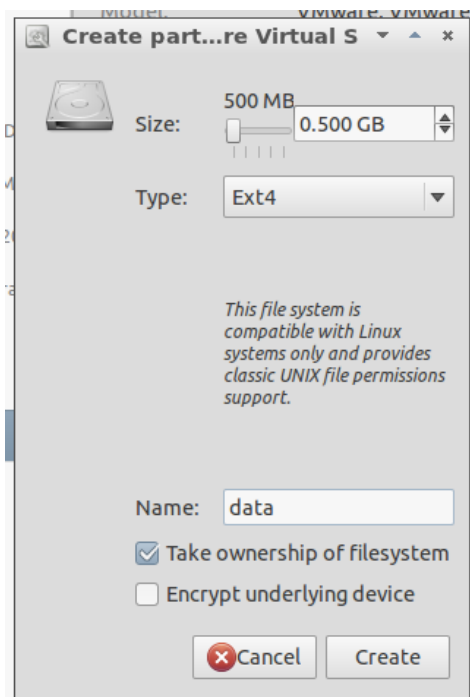
## Menyiapkan Partisi untuk Acquire Data

10. Ketika DEFT 7 berjalan maka akan terlihat tampilan desktop, seperti di bawah ini.

a. Pada kiri bawah, click **d**, **DEFT**, "**Disk Utility**", seperti terlihat di bawah ini:



b. Pada kotak "DEFT - Warning!", click "**I know what I'm doing**".



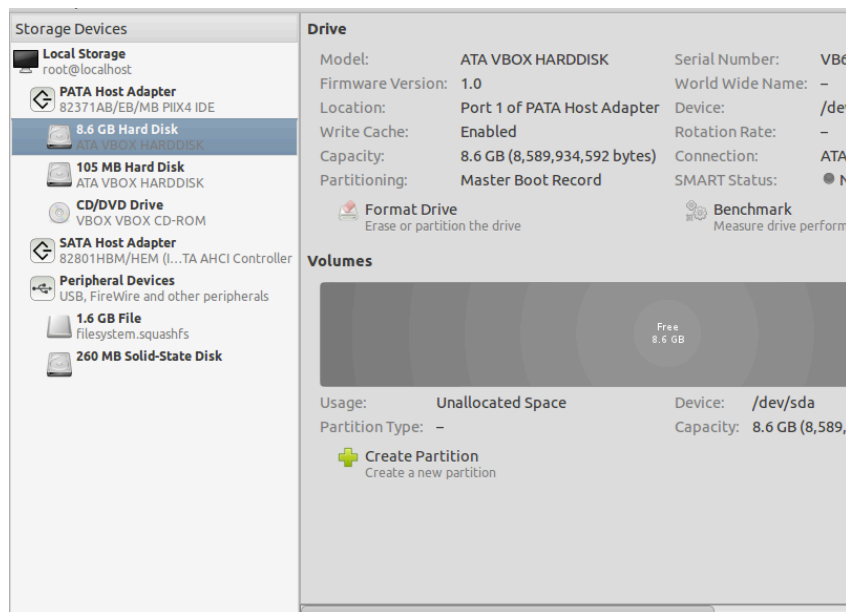
c. Jendela Disk Utility terbuka, seperti gambar.

d. Pada sisi kiri, click "**8 GB Hard Disk**". Disk yang akan kita gunakan untuk meng capture image.

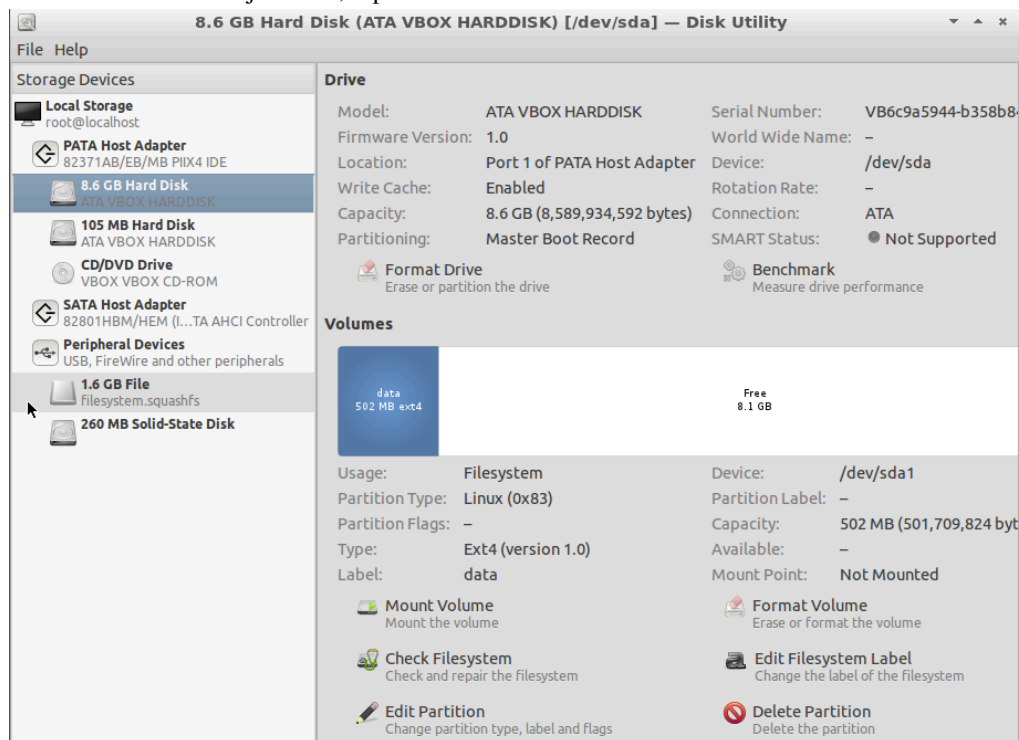
e. Perhatikan di sebelah kanan terdapat drive dengan labelled "Unknown" dan drive ini yang akan kita gunakan and "-", seperti terlihat di bawah ini. (Jika ada partisi dari project sebelumnya di delete dulu, tapi pada proses Forensic sebenarnya pastikan hardisk untuk mengumpulkan evidence dalam keadaan benar-benar kosong misal dengan menggunakan tools clean disk yang menimpa data disk dengan 00 seperti kita gunakan sebelumnya)

f. OS tidak akan bisa meletakkan files ke hardisk tersebut sebelum hardisk tersebut dipartisi.

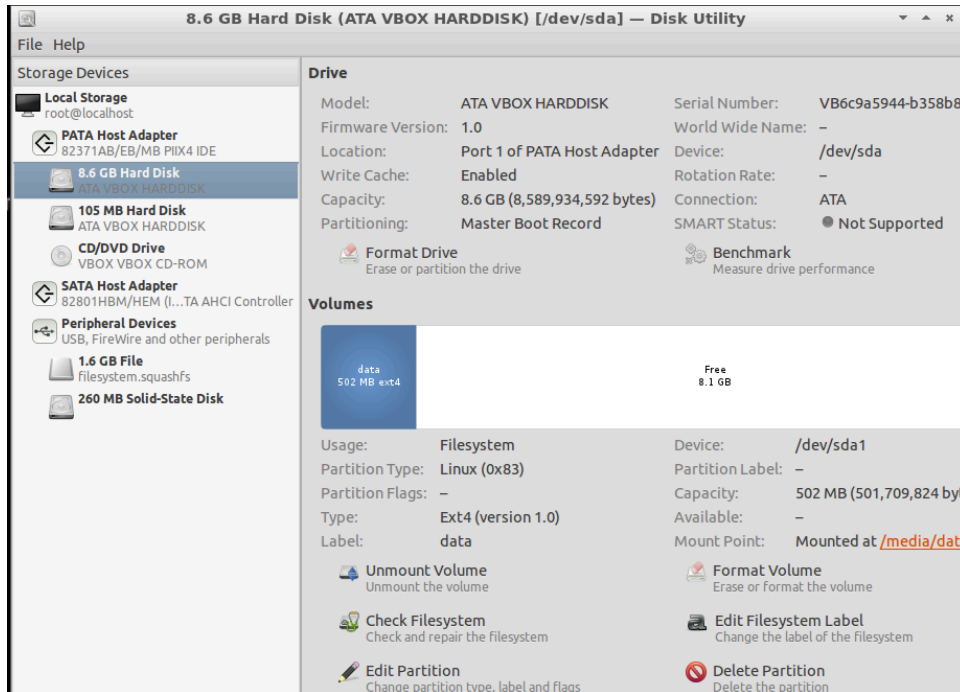
g. Pada panel kanan, click tombol "**Format Drive**".



- h. Kotak popup, menayakan Scheme yang digunakan. Biarkan default selection "**Master Boot Record**" dan click tombol **Format**.
- i. Pada kotak "Are you sure...", click tombol **Format**.
- j. Pada kanan bawah, click tombol "**Create Partition**".
- k. Kotak pops up "Create part...", akan terlihat.
- l. Masukkan ukuran **0.5** dan Name **data**.
- m. Click tombol **Create**.
- n. Pada panel kanan bawah, click partisi **data** yang baru dibuat, maka akan berubah menjadi biru, seperti berikut.



- o. Click tombol "**Mount Volume**".
- p. Sekarang panel kanan bawah akan terlihat sebagai "Mounted at /media/data", seperti berikut.



q. Tutup Disk Utility.

## Acquiring Evidence Drive

11. Pada kiri bawah, click **d**, DEFT, "Imaging Tools", Cyclone, seperti berikut:



a. Jendela LXTerminal terbuka dengan "cyClone" banner, terlihat seperti di gambar.

- b. Dua disks terlihat di tengah jendela. /dev/sdb1 merupakan evidence drive yang akan acquired, dan /dev/sda merupakan partisi "data" yang akan digunakan untuk menyimpan image.

```

cyClone - Tool for cloning disks
ver. 0.0.1

-----

Start time:          2013-05-01 22:11:35

Disk /dev/sda: 8589 MB, 8589934592 bytes
/dev/sda1          63      979964      489951   83   Linux

Disk /dev/sdb: 104 MB, 104857600 bytes
/dev/sdb1          63      64259      32098+   4   FAT16 <
32M

-----

Type the disk name or the partition name
(Ex.: /dev/sda or /dev/sda1):

```

- c. Ketikkan path berikut, akhiri dengan Enter:  
**/dev/sdb**
- d. cyClone akan menanyakan "disk image filename", seperti berikut.

```

LXTerminal
File Edit Tabs Help

-----

cyClone - Tool for cloning disks
ver. 0.0.1

-----

Start time:          2013-05-01 22:11:35

Type the disk image filename with full path
without the extension (Ex.: /media/image_name):

/media/data/YOURNAME-p13a

```

- e. Ketikkan pada path, diakhiri dengan Enter. (ganti YOURNAME dengan nama kalian tanpa spasi).  
**/media/data/YOURNAME-p13a**
- f. Layar berikutnya akan menanyakan format yang digunakan, seperti berikut.

```
LXTerminal
File Edit Tabs Help

cyClone - Tool for cloning disks
ver. 0.0.1

Start time:      2013-02-13 00:55:55

What kind of image format do you want create?
1) RAW (DD - No compression)
2) AFF (Advanced Forensics Format)
3) E01 (EnCase File Format)

3
```

- g. Ketikkan **3** untuk menggunakan "EnCase File Format" (format untuk Expert Witness format), akhiri dengan Enter.
- h. Layar berikutnya akan menanyakan apakah akan dibuat hash hash.
- i. Ketik **y** dan tekan Enter.
- j. Layar berikutnya akan menanyakan apakah akan memverifikasi image.
- k. Ketik **y** dan tekan Enter.
- l. Layar berikutnya akan menanyakan apakah ingin meng-compress image.
- m. Ketik **y** dan tekan Enter.
- n. Layar berikutnya menanyakan jenis compression yang diinginkan.
- o. Ketik **2** dan tekan Enter.
- p. Layar berikutnya menanyakan Case number.
- q. Ketikkan **YOURNAME-p11**, seperti berikut, dan tekan Enter. (Gunakan nama masing-masing tanpa spasi).

```
LXTerminal
File Edit Tabs Help

cyClone - Tool for cloning disks
ver. 0.0.1

Start time:      2013-05-01 22:11:35

Case number:

YOURNAME-p13
```

- r. Layar berikutnya menanyakan deskripsi. Tekan Enter.
- s. Layar berikutnya menanyakan "Evidance number". Tekan Enter.
- t. Layar berikutnya menanyakan "Examiner name". Tekan Enter.



- u. Layar berikutnya menayakan "Notes". Tekan Enter.
- v. Image dibuat. Setelah selesai, akan terlihat pesan yang mengatakan "**Hash of device and image match!**".

```

root:~
File Edit Tabs Help

-----
cyClone - Tool for cloning disks
ver. 0.0.1
-----

Start time:      2013-05-01 22:11:35
End time:        2013-05-01 22:36:07

Hash of device and image match!

The log file was written in '/media/data/YOURNAME-p13a.log'
-----


```

## Melihat Log

12. Pada jendela Terminal window, ketikkan perintah berikut diakhiri dengan Enter:

```
cat /media/data/YOURNAME-p11a.log
```

Akan terlihat MD5 hash yang didapatkan akan sama dengan project sebelumnya, berakhiran dengan "08fd", seperti berikut:



```

The log file was written in '/media/data/YOURNAME-p13a.log'
-----
~ % cat /media/data/YOURNAME-p13a.log
one ver. 0.0.1

Start time:      2013-05-01 22:11:35
End time:        2013-05-01 22:36:07

Input:           /dev/sdb
Output:          /media/data/YOURNAME-p13a

MD5:             9e84766b1998ade5e514c1b8281708fd
SHA1:            0e65a36a74cbb0062c53e5528b82e70e90f9061c

Hash of device and image match!

deft ~ %

```

## Simpan Screen Image

13. Pastikan di layar terdapat tiga item berikut:

- ▲ Output: filename berisi nama kalian
- ▲ MD5 yang berakhiran **08fd**
- ▲ Pesan: "**Hash of device and image match!**"

Tekan PrintScrn untuk mengkopikan seluruh desktop ke clipboard.

**PASTIKAN SUBMIT GAMBAR KESELURUHAN DESKTOP UNTUK POIN MAKSIMAL!**

Simpan dengan nama "**Your Name Proj 13a**". Gunakan nama masing-masing.

## Acquiring Raw Image

14. Sekarang kita ulangi process untuk membuat Raw image yang lain.

- a. Click **d**, **DEFT**, "**Imaging Tools**", **Cyclone**. Masukkan disk name: **/dev/sdb**
- b. Masukkan disk image filename: **/media/data/YOURNAME-p11b**
- c. Pilih format **1** untuk acquire RAW image.
- d. Ketik **y** untuk membuat hash.
- e. Ketik **y** untuk memverifikasi image.
- f. Image dibuat, menggunakan **dcfldd**.
- g. Ketika proses selesai terlihat "**Hash of device and image match!**".


## Melihat Files

15. Pada jendela Terminal, ketikkan perintah berikut, akhiri dengan Enter tiap barisnya.

Catatan perintah terakhir huruf L kecil, bukan angka "1".

```
cd /media/data
cat YOURNAME-p11b.log
ls -l
```

Akan terlihat MD5 hash berakhiran dengan "08fd", dan direktori terdiri dari empat file yang diawali dengan nama kalian seperti berikut ini:



```
deft ~ % cd /media/data
deft /media/data % cat YOURNAME-p13b.log
Cyclone ver. 0.0.1
Start time:      2013-05-01 22:49:11
End time:        2013-05-01 22:52:17

Input:           /dev/sdb
Output:          /media/data/YOURNAME-p13b.dd

MD5:             9e84766b1998ade5e514c1b8281708fd
SHA1:            0e65a36a74cbb0062c53e5528b82e70e90f9061c
SHA256:          af0bd8ffe77bf52b84ca5a123d083b92dec3fd4f4e511104a80f330423
SHA512:          a4a4234fb731054210e7c17d6808a1384825e2b57e93f91c7034005cfd
2b8953924e1e6cca2ba735170f54dc21bb37e5569db0bd66033910a64e1a1df4

Hash of device and image match!

deft /media/data % ls -l
total 103361
drwx----- 2 root root    12288 2013-05-01 22:06 lost+found
-rw-r--r-- 1 root root    967985 2013-05-01 22:36 YOURNAME-p13a.E01
-rw-r--r-- 1 root root      261 2013-05-01 22:36 YOURNAME-p13a.log
-rw-r--r-- 1 root root 104857600 2013-05-01 22:52 YOURNAME-p13b.dd
-rw-r--r-- 1 root root      476 2013-05-01 22:52 YOURNAME-p13b.log
deft /media/data %
```

## Simpan Screen Image

16. Pastikan pada layar terdapat lima items:

- ▲ MD5 yang berakhiran **08fd**
- ▲ Empat file yang diawali dengan nama kalian
- ▲ Tekan PrintScrn untuk mengkopi seluruh desktop ke clipboard.

**PASTIKAN SUBMIT GAMBAR KESELURUHAN DESKTOP UNTUK POIN MAKSIMAL!**

Simpan dengan nama "**Your Name Proj 11b**". Gunakan nama masing-masing.

## Penjelasan Ukuran File

17. Perhatikan kedua images memiliki ukuran file berbeda.

- a. File .dd file merupakan exact duplicate dari original evidence disk, hamper berukuran 104 MB.
- b. File .E01 lebih kecil, kurang dari 1 MB.
- c. Perhatikan kenapa situasinya demikian, dan kirim juga file teks NAMA KAMU\_proj13c.txt (atau bisa juga doc) untuk menjawab pertanyaan berikut.
  1. **Kenapa file .dd dan .E01 memiliki ukuran berbeda?**
  2. **File yang mana yang merupakan evidence image yang tepat untuk digunakan di pengadilan, atautkah keduanya bisa digunakan?**

## Kumpulkan Project

18. Jawab dua pertanyaan tersebut dalam file teks /doc. Kirim melalui elearning.

Kirim juga dua gambar proj11a dan proj11b.

Last Modified: 2-5-2013