Project 10: Static Acquisition dengan BackTrack (20 Points)

Kebutuhan Project

- VirtualBox
- File BT5R3-GNOME-32.iso, sudah tersedia di lab. Foresec, bisa Backtrack versi yang lain.

Mengumpulkan Files yang Dibutuhkan

1. File BT5R3-GNOME-32.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.backtrack-linux.org/downloads
2. Pada komputer di lab. Foresec, buat folder dengan nama kalian. Di dalamnya buat subfolder dengan nama **NAMAKAMU-proj10**.
3. Klik kanan pada link di elearning p10Evidence.zip, dan simpan Evidence File ke desktop.

Memeriksa Nilai Hash dari Evidence File

4. Di jendela Backtrack buka Terminal

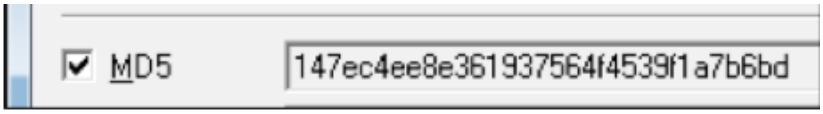
   ```
   cd Desktop
   unzip p10Evidence.zip
   ls
   ```

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

5. Gunakan md5hash untuk memeriksa nilai hash file tersebut

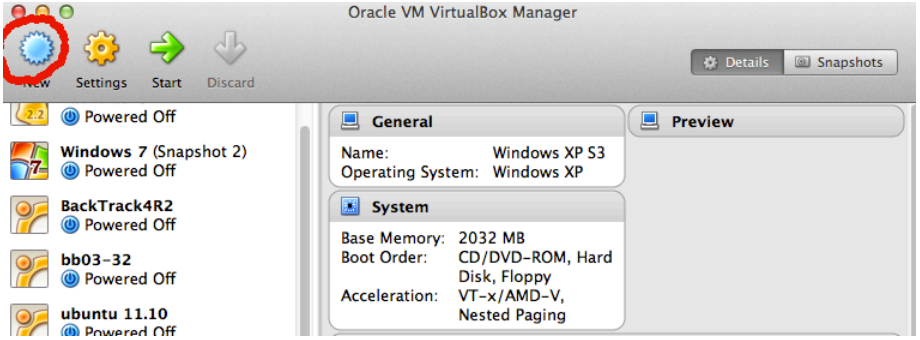
   ```
   md5sum "Windows 2000 Professional-sparse.vmdk"
   ```

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

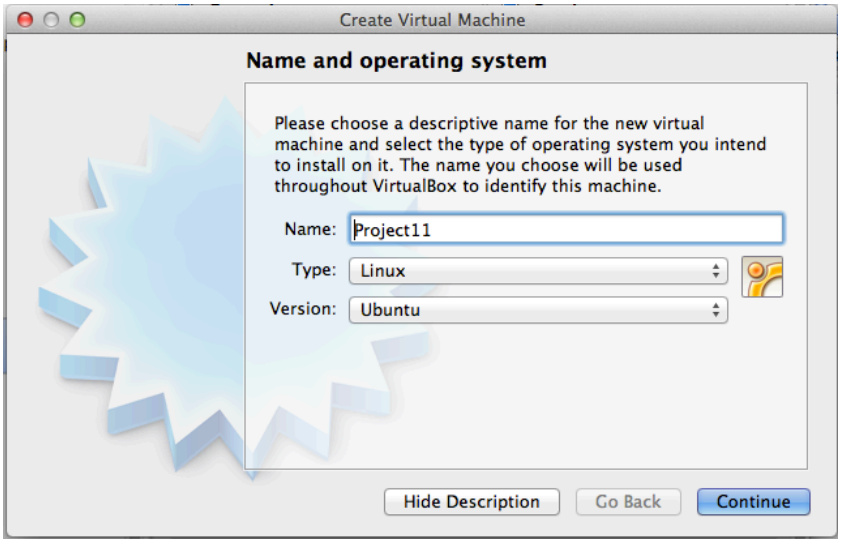


Membuat New Virtual Machine

6. Buka VirtualBox. Click **"New"**



a. Pada kotak "**Name and Operating System",** isikan "Name" **Project11, "**Type" pilih **Linux** dan Version **"Ubuntu'**, seperti di gambar:



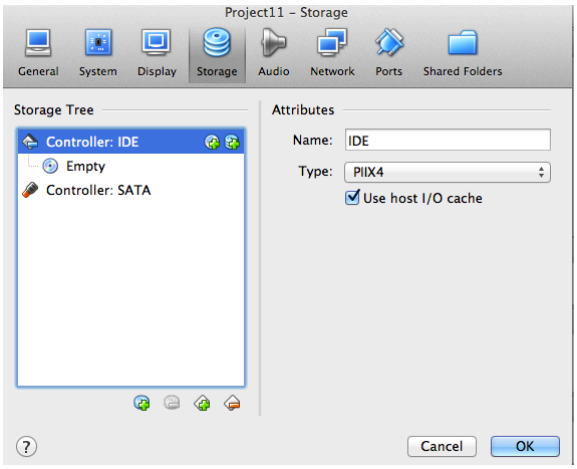
b. Klik **"***Continue"***.**

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 **"Dynamicaly 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.

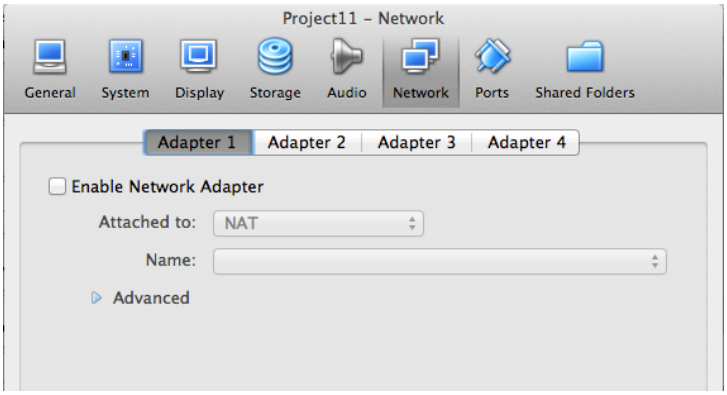
   a. Klik pada **"Storage"** , maka akan seperti berikut:

   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 Project10, click pada icon **"Network".** Buang tanda centang pada **"Enable Network Adaptor"**, seperti di bawah ini:

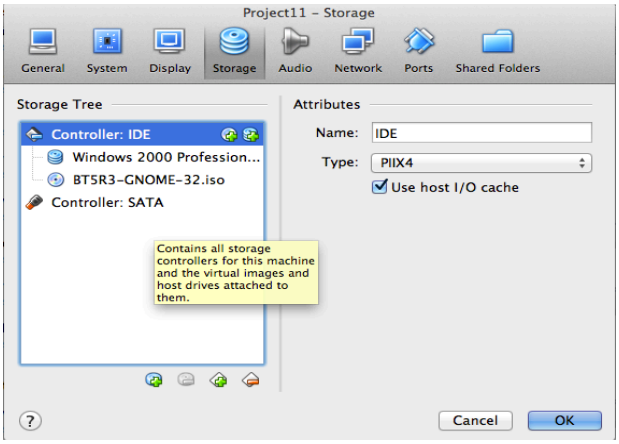
Click **OK.**

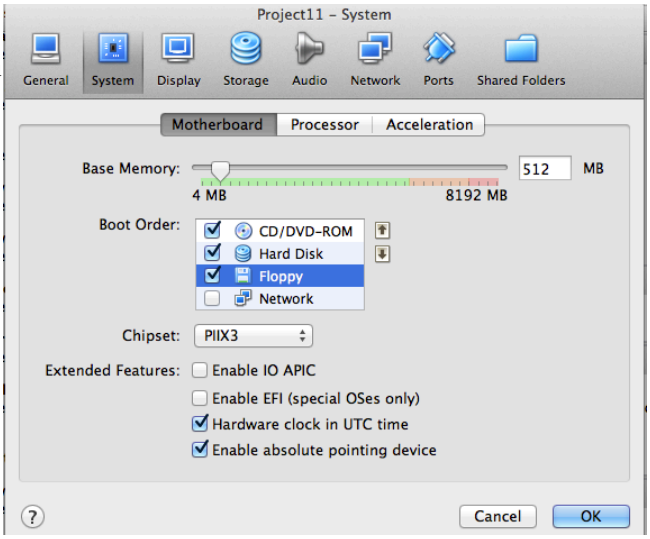
Pada aturan dasar forensic, WORK

IN ISOLATION—dengan kata lain, jangan terkoneksi ke internet ketika melakukan imaging drives.

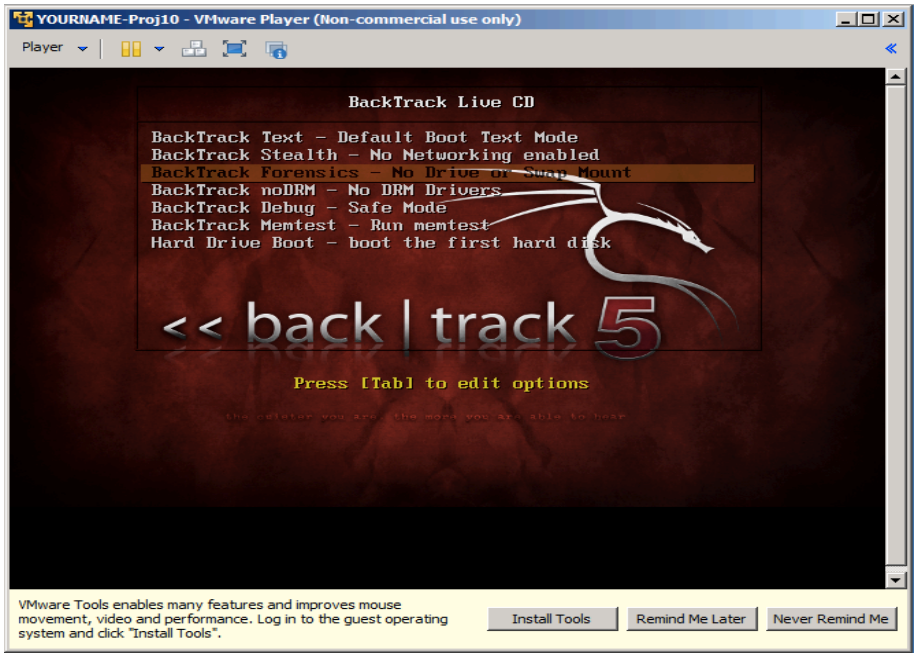
Booting dari file ISO BackTrack dalam Forensics Mode

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 Backtrack5R3. 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 tombok **OK**.
   i. Kemudian jalankan Komputer Virtual Project10
   j. Akan muncul tanda prompt yang bertuliskan **boot:**. Tekan Enter.
   k. BackTrack akan berjalan, seperti berikut.





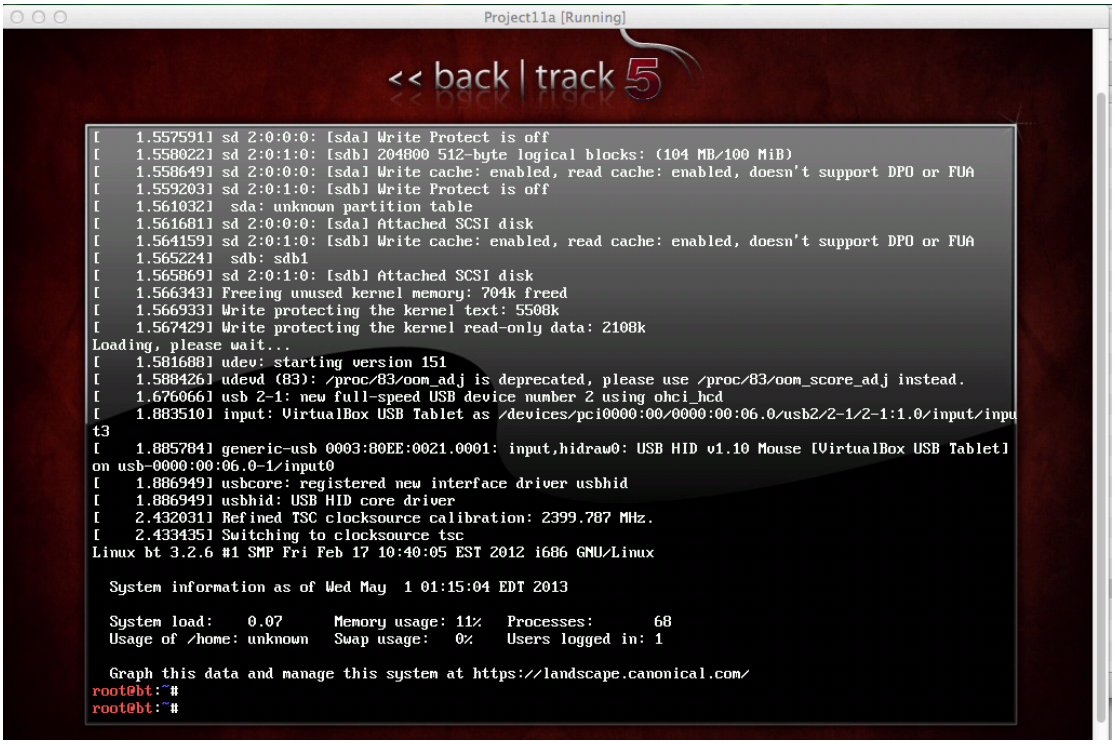
10. Gunakan panah ke atas dan ke bawah untuk memilih "**Backtrack Forensics**" seperti terlihat di atas.
    a. Tekan tombol Enter untuk memulai BackTrack.



b. Perhatikan hardisk yang terkoneksi terbaca sebagai sda/sdb, pada contoh /dev/sda merupakan hardisk baru kosong yang berukuran 8 G, dan /dev/sdb hardisk windows 2000 yang berukuran 104 M. **(Jangan salah saat mengenali hardisk evidence)**

c. Ketika muncul prompt **root@bt:~#**, masukkan perintah berikut diakhiri dengan Enter key:

```
startx
```



BackTrack Desktop

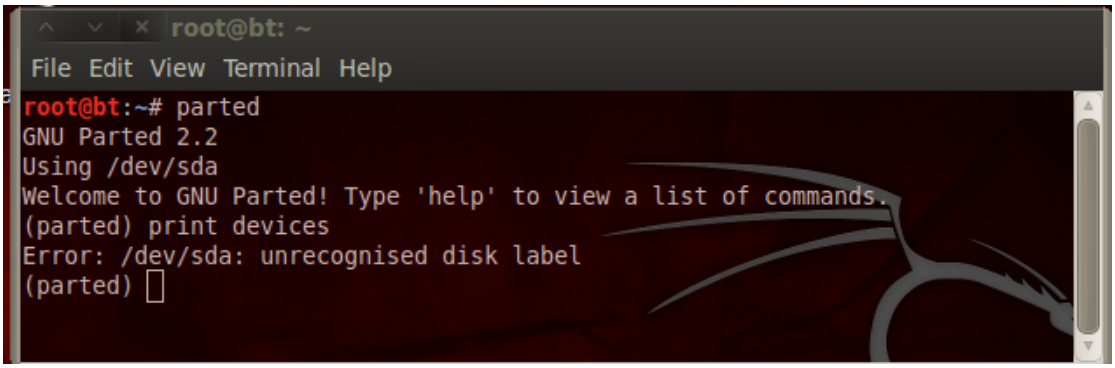
11. Ketika desktop muncul, akan terlihat tampilan seperti pada gambar.

a. Pada sisi kiri atas, click icon kotak kecil pada jendela Terminal.

Mengidentifikasi Drives dengan parted

12. Pada jendela Terminal, masukkan perintah berikut, tekan Enter setiap baris:

```
parted
print devices
```



a. Daftar drive yang di-attached, seperti terlihat di atas.
b. Jika keluar pesan error seperti di atas, tidak bermasalah. Hal tersebut dikarenakan hardisk berukuran 8 G yang dibuat belum ada partisi table.
c. Hard drive yang kosong tersebut (ukuran tergantung pada saat dibuat) merupakan hard drive /dev/sda yang masih kosong untuk mengumpulkan barang bukti.

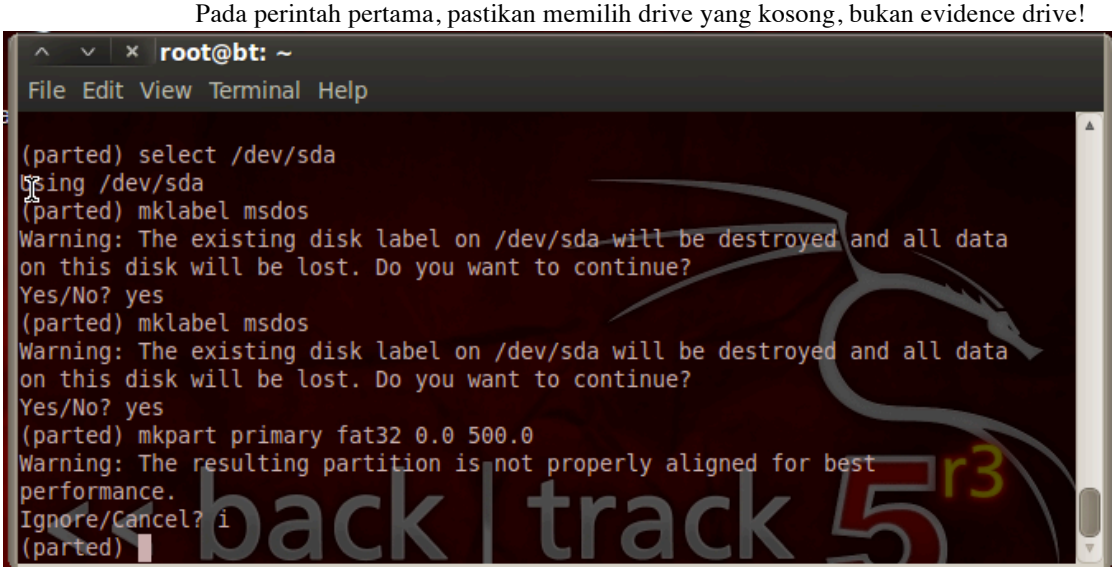
Format Empty Drive

13. Untuk menggunakan drive yang kosong tersebut untuk memeriksa image evidence drive. Sebelumnya harddisk tersebut terlebih dahulu diformat.

a. Pada Terminal window, ketikkan perintah berikut, diikuti dengan enter tiap barisnya.

```
select /dev/sda
mklabel msdos
mkpartfs primary fat32 0.0 500.0
```

Perintah tersebut membuat partisi pada drive kosong tersebut dengan ukuran 500 MB.
Pada perintah pertama, pastikan memilih drive yang kosong, bukan evidence drive!

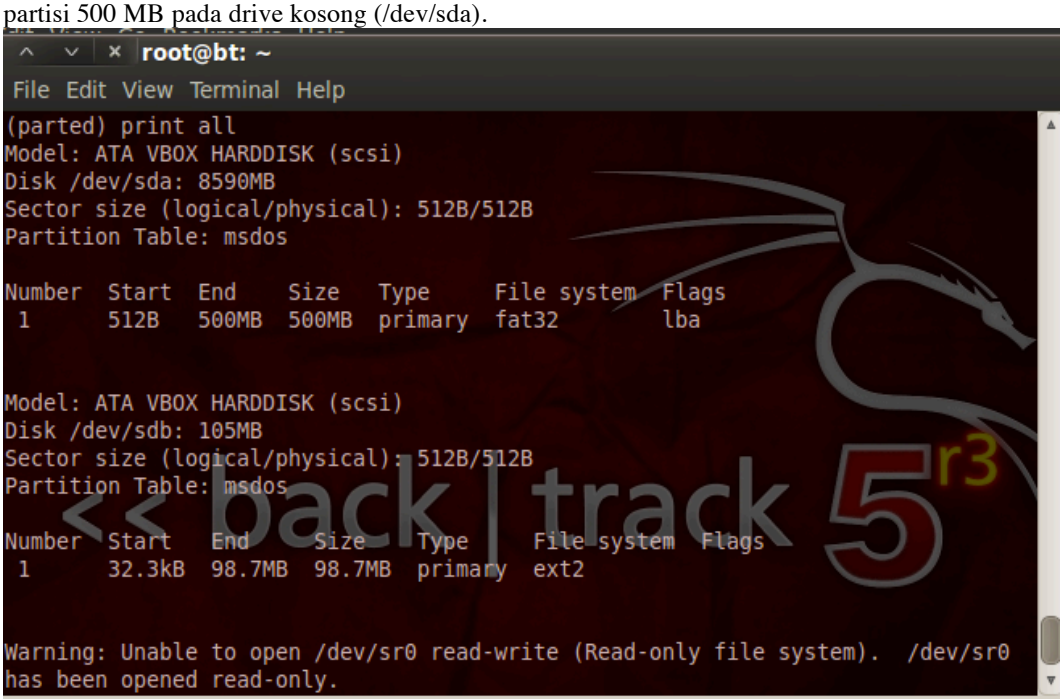


b. Pesan akan muncul, yang mengatakan: "The resulting partition is not properly aligned for best performance". Ketikan **i** dan tekan Enter, uuntuk mengabaikan pesan.
c. Pada jendela Terminal, pada bagian (parted) prompt, masukkan perintah berikut diikuti Enter:

```
print all
```

Maka akan terlihat semua partisi yang ada seperti pada gambar.

Maka akan terlihat partisi sebesar 98.78 MB pada evidence drive (/dev/sdb), dan partisi 500 MB pada drive kosong (/dev/sda).



d. Pada jendela Terminal, pada (parted) prompt, masukkan perintah berikut diikuti Enter:

```
quit
```

Perintah ini menutup parted dan kembali ke normal Linux bash prompt.

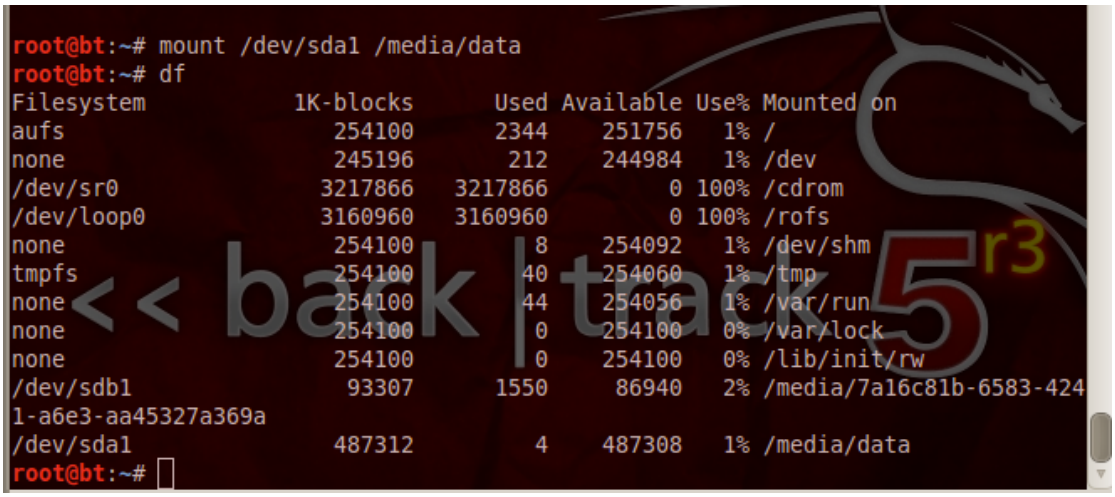
Mounting Partisi

14. Lakukan mounting (gandeng) pada partisi yang baru.

a. Pada jendela Terminal, pada # prompt, masukkan perintah berikut, dan tekan Enter tiap barisnya:

```
mkdir /media/data
mount /dev/sda1 /media/data
df
```

b. Pada baris terakhir terlihat volume baru dengan filesystem /dev/sdb1 yang digandeng pada /media/data, seperti terlihat di bawah ini.



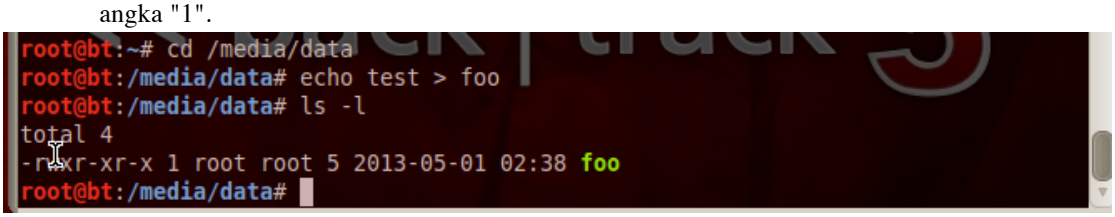
Menguji Working Partition

15. Pada jendela Terminal, ketikkan perintah berikut, diikuti dengan Enter setiap barisnya.

```
cd /media/data
echo test > foo
ls -l
```

Perintah tersebut merubah direktori kerja ke drive kosong, membuat file kecil bernama foo pada direktori tersebut, dan menampilkan file direktori.

Perhatikan perintah terakhir keduanya merupkan karakter huruf "L" kecil – bukan karakter angka "1".



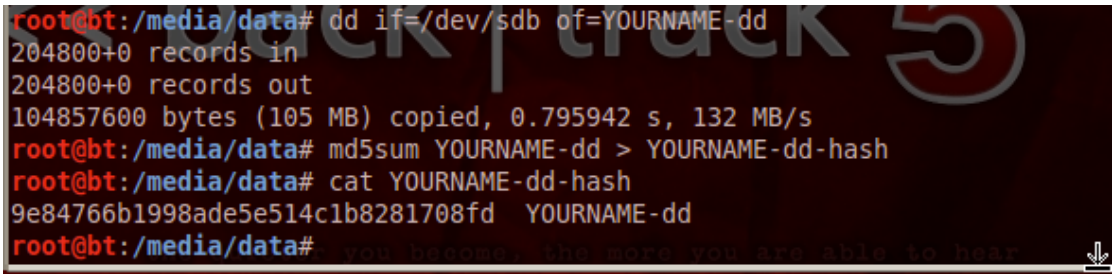
Direktori memperlihatkan file foo, seperti terlihat di atas.

Partisi kosong tersebut siap digunakan.

Acquiring Image Disk Evidence dengan dd

16. Pada jendela Terminal, ketikkan perintah berikut, tekan Enter setiap barisnya.
    a. Perintah dd mengkopi data dari evidence drive ke file bernama **YOURNAME-dd**. (Ganti YOURNAME dengan nama sendiri).
    b. Perintah md5sum menghitung nilai md5 hash dan menyimpannya pada file bernama **YOURNAME-dd-hash**.
    c. Perintah cat menampilkan isi file hash **YOURNAME-dd-hash**.

```
dd if=/dev/sdb of=YOURNAME-dd
md5sum YOURNAME-dd > YOURNAME-dd-hash
cat YOURNAME-dd-hash
```



d. Nilai hash harus sama dengan image yang terlihat di atas.

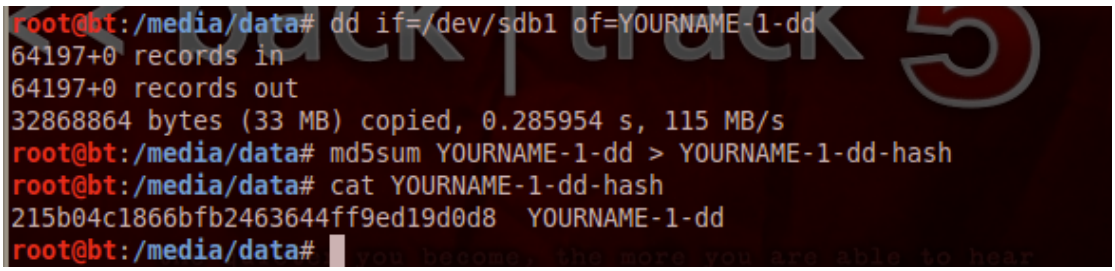
Membandingkan Nilai Hash dengan Nilai Hashcalc

17. Hash tersebut tidak sama dengan nilai MD5 hash yang kita hitung sebelumnya dari VMware hard disk file. Tidak masalah, karena VMware hard disk format tidak sesederhana dd hard drive. Vmware menambahkan headers, rollback data, dan lain-lain, seperti dijelaskan di sini: http://www.vmware.com/app/vmdk/?src=vmdk

Acquiring Image dari Satu Partisi dengan dd

18. Kita juga bisa meng-capture hanya partisi dari drive, yang bisa berisi semua data yang kita inginkan saja, atau bisa juga semua data yang ada untuk di kumpulkan.
    a. Pada jendela Terminal, ketikkan perintah berikut, diikuti dengan Enter tiap barisnya.

```
dd if=/dev/sdb1 of=YOURNAME-1-dd
md5sum YOURNAME-1-dd > YOURNAME-1-dd-hash
cat YOURNAME-1-dd-hash
```

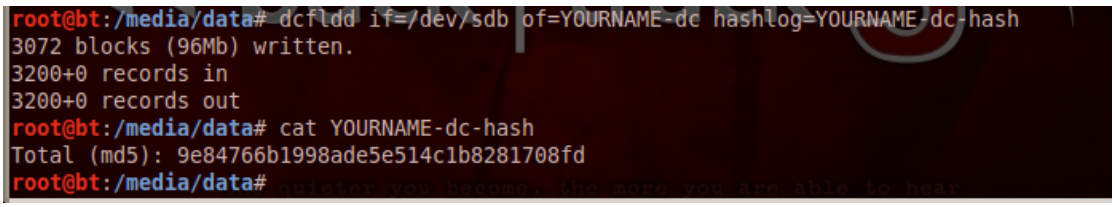


b. Nilai hash seharusnya seperti pada gambar di atas. Hash tidak sama dengan sebelumnya, karena image ini hanya untuk satu partisi bukan seluruh drive.

Acquiring Image dari Keseluruhan Evidence Disk dengan dcfldd

19. Dcfldd merupakan versi pengembangan dd yang dikembangkan oleh U.S. Department of Defense Computer Forensics Lab. Secara default sudah ada di BackTrack.
    a. Pada jendela Terminal, ketikkan perintah berikut diikuti dengan Enter tiap barisnya.

```
dcfldd if=/dev/sdb of=YOURNAME-dc hashlog=YOURNAME-dc-hash
cat YOURNAME-dc-hash
```

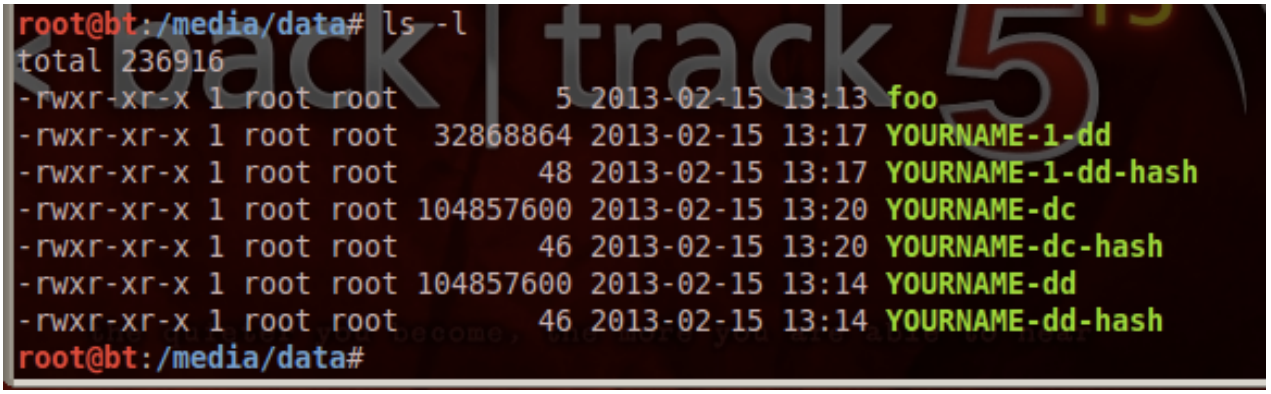


b. Perhatikan tampilannya lebih baik dibandingkan dd – tools ini memperlihatkan jumlah running count of blocks yang ditulis untuk memastikan pada saat pengkopian tidak terjadi crashed.

c. Nilai hash seharusnya sama dengan nilai hash yang dihitung sebelumnya dengan perintah dd.

d. Pada jendela Terminal window, ketikkan perintah berikut diikuti dengan tombol Enter. (Perintah ini berisi dua karakter L kecil, bukan angka.)

```
ls -l
```



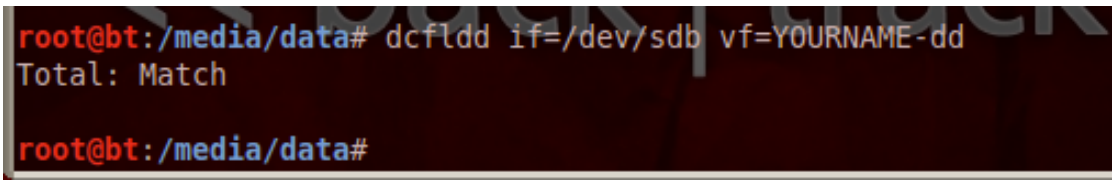
e. Direktori memperlihatkan dua file acquisition YOURNAME-dd dan YOURNAME-dc. Ukurannya sama. Sebenarnya file tersebut indentik, karena nilai md5 hash-nya sama.

Gunakan dcfldd untuk Memverifikasi Image

20. Pada jendela Terminal, ketikkan perintah berikut, diikuti dengan Enter:

```
dcfldd if=/dev/sdb vf=YOURNAME-dd
```

a. Bandingkan Nilai vf value points untuk image yang dibuat dengan if file (partisi atau disk yang dikopi).



b. Hasilnya memperlihatkan "Total: Match", seperti terlihat di bawah ini.

Simpan Screen Image

21. Pastikan terlihat "**Total: Match**", seperti di atas.

a. Tekan **Ctrl+Alt** untuk mengaktifkan mouse dari Virtual Machine.

b. Tekan PrintScrn key untuk mengkopi seluruh desktop ke clipboard.

SUBMIT KESELURUHAN DESKTOP UNTUK MENDAPATKAN POIN MAKSIMAL!

c. Simpan dengan nama file "**NamaKamu_Proj10**".

Menguji Effects Error

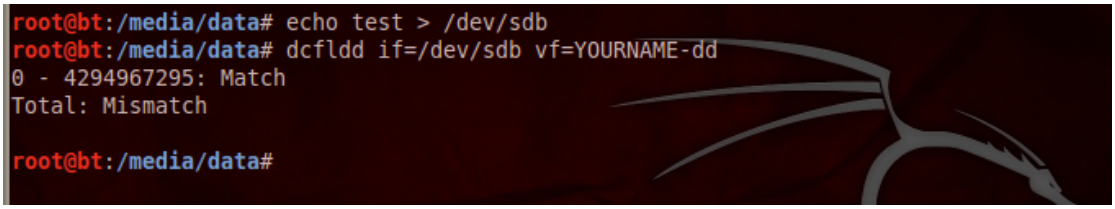
22. Apa yang terjadi jika terjadi terjadi kesalahan perintah, dan penulisan pada evidence drive?

a. Pada jendela Terminal, ketikkan perintah berikut, diikuti dengan Enter key:

`echo test > /dev/sdb`

Apakah evidence tersebut korup? Untuk melihatnya, bisa dijalankan perintah berikut:

`dcfldd if=/dev/sdb vf=proj10-dd`



b. Seperti terlihat, file tidak matching dengan drive. Terlihat evidence (barang bukti) sudah diganti! Jadi meskipun teknik ini bekerja, akan tetapi tidak sebaik jika kita menggunakan hardware write-blocker.

Mengumpulkan Project

23. Kumpul melalui elearning.

Last Modified: 1-5-2013 pm