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

 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: <u>http://www.backtrack-linux.org/downloads</u>

Pada komputer di lab. Foreseo, huat folder dengan nama kalia

- 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.
```

```
✓ <u>M</u>D5 147ec4ee8e361937564f4539f1a7b6bd
```

Membuat New Virtual Machine

6. Buka VirtualBox. Click "New"

Settings Start Discard	Oracle VM VirtualBox Manager	🔅 Details 💿 Snapshots
22 (1) Powered Off	📃 General	Preview
Windows 7 (Snapshot 2)	Name: Windows XP S3 Operating System: Windows XP	
BackTrack4R2	System	
Off	Base Memory: 2032 MB	
bb03-32 Powered Off	Disk, Floppy	
wbuntu 11.10	Acceleration: VT-x/AMD-V, Nested Paging	

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

00	Create Virtual Machine
	Name and operating system
	Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.
	Name: Project11
	Type: Linux 🗘 🌮
	Version: Ubuntu 🗘
2	
	Hide Description Go Back Continue

- 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

 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

			9		7	$\langle \rangle$	É		
General	System	Display	Storage	Audio	Network	Ports	Shared	Folders	
		Adapter 1	Adapt	ter 2	Adapter 3	Adap	oter 4		
🗌 En	able Netv	vork Adap	oter						
	Attached	d to: N	AT		*				
	Na	ime:							÷
	Advan	ced							

Project11 - Network

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



- 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

	<< back track 5
	1.557591] sd 2:0:0:0: [sda] Write Protect is off 1.558022] sd 2:0:1:0: [sdb] 204000 512-byte logical blocks: (104 MB/100 MiB)
	1.5500493 sd 2.0:0.0: Isdal write cache: enabled, read cache: enabled, doesn't support pro or run 1.559203] sd 2:0:1:0: Isdal Write Protect is off 1.5610321 sda: unknown partition table
I I	1.561681] sd 2:0:0:0: [sda] Attached SCSI disk 1.564159] sd 2:0:1:0: [sdb] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
[[1.565224] sdb: sdb1 1.565869] sd 2:0:1:0: [sdb] Attached SCSI disk
	1.566343] Freeing unused kernel memory: 704k freed 1.566933] Write protecting the kernel text: 5508k
Loa	1.5574251 Write protecting the kernel read-only data. 2106k ding, please wait
L L	1.581688] udev: starting version 151 1.588426] udevd (83): /proc/83/oom_adj is deprecated, please use /proc/83/oom_score_adj instead. 1.6750661 usb 2-1: new full-semed USB device number 2 using obri bod
i 13	1.883510] input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/usb2/2-1/2-1:1.0/input/inpu
E On	1.885784] generic-usb 0003:80EE:0021.0001: input,hidraw0: USB HID v1.10 Mouse [VirtualBox USB Tablet] usb-0000:00:06.0-1/input0
E	1.886949] usbcore: registered new interface driver usbhid
	1.8869491 usbhid: USB HID core driver 2.4220411 Betimed TSC clockrouwer calibration: 2399 787 MWr
	2.433951 An include 150 Clocksburge Largerton, 255,107 miz.
Lin	ux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux
S	ystem information as of Wed May 1 01:15:04 EDT 2013
S U	ystem load: 0.07 Memory usage: 11% Processes: 68 sage of ∕home: unknown Swap usage: 0%. Users logged in: 1
G	raph this data and manage this system at https://landscape.canonical.com/ tebt:"#
roo	tebt:~#

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.

<pre>root@bt:~# mount</pre>	: /dev/sdal /media/	data		/	
<pre>root@bt:~# df</pre>					
Filesystem	1K-blocks	Used	Available	Use%	Mounted on
aufs	254100	2344	251756	1%	/
none	245196	212	244984	1%	/dev
/dev/sr0	3217866 3	217866	Θ	100%	/cdrom
/dev/loop0	3160960 3	160960	Θ	100%	/rofs
none	254100	8	254092	1%	/dev/shm r
tmpfs	254100	40	254060	1%	/tmp
none 🦳 🦳	254100	44	254056	1%	/var/run
none	254100	► 0	254100	0%	/var/lock
none	254100	Θ	254100	0%	/lib/init/rw
/dev/sdb1	93307	1550	86940	2%	/media/7a16c81b-6583-424
1-a6e3-aa45327a3	69a				
/dev/sda1	487312	4	487308	1%	/media/data
root@bt:~#					▼
none none /dev/sdb1 1-a6e3-aa45327a3 /dev/sda1 root@bt:~#	254100 254100 93307 369a 487312	44 0 0 1550 4	254056 254100 254100 86940 487308	1% 0% 0% 2% 1%	/var/run /var/lock /lib/init/rw /media/7a16c81b-6583-424 /media/data

Menguji Working Partition

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

```
cd /media/data
echo test > foo
ls -1
```

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.)
 1s -1

_			_									
	root@bt:	/med	ia/dat	ta# ls	5-l	-						
	total 23	6916		K		- 1		d		К		
	-rwxr-xr	-x 1	root	root	<u> </u>	5	2013	-02-1	5 13:	13	foo	
	-rwxr-xr	-x 1	root	root	3286	8864	2013	-02-1	5 13:	17	YOURNAME-1-dd	
	-rwxr-xr	-x 1	root	root		48	2013	-02-1	5 13:	17	YOURNAME-1-dd-hash	
	-rwxr-xr	-x 1	root	root	10485	7600	2013	-02-1	5 13:	20	YOURNAME-dc	
	-rwxr-xr	-x 1	root	root		46	2013	-02-1	5 13:	20	YOURNAME-dc-hash	
	-rwxr-xr	-x 1	root	root	10485	7600	2013	-02-1	5 13:	14	YOURNAME - dd	
	-rwxr-xr	-x 1	root	root		46	2013	-02-1	5 13:	14	YOURNAME-dd-hash	
	<pre>root@bt:/media/data#</pre>											
١.												

e. Direktori memperlihatkan dua file acquisition YOURNAME-dd dan YOURNAMEdc. 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).



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