LAB 01

THU THẬP DỮ LIỆU VÀ BẰNG CHỨNG

(Data and Evidence Acquisition)

Họ tên và MSSV: Trương Quang Long B2203727

Nhóm học phần: 01

- *Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.*
- *Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết.* Hình minh hoạ chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.

1. Thu thập dữ liệu sử dụng công cụ FTK Imager

1.1. Tạo đĩa mục tiêu chứa dữ liệu cần thu thập (chọn 1.1.1 hoặc 1.1.2)

1.1.1. Sử dụng một ổ đĩa USB. Gắn USB vào máy tính, sao chép một số tập tin bất kỳ vào ổ đĩa.

1.1.2. Xem video hướng dẫn và tạo 01 ổ đĩa ảo 2G trên máy tính. Sau khi tạo xong sao chép một số tập tin bất kỳ vào ổ đĩa.

1.2. Tải và thực thi công cụ USB write protection để ngăn chặn ổ USB bị thay đổi dữ liệu (trong thực tế một thiết bị phần cứng write blocker sẽ được dùng). Sau khi thực thi công cụ, chúng ta có ghi dữ liệu vào được ổ USB không?

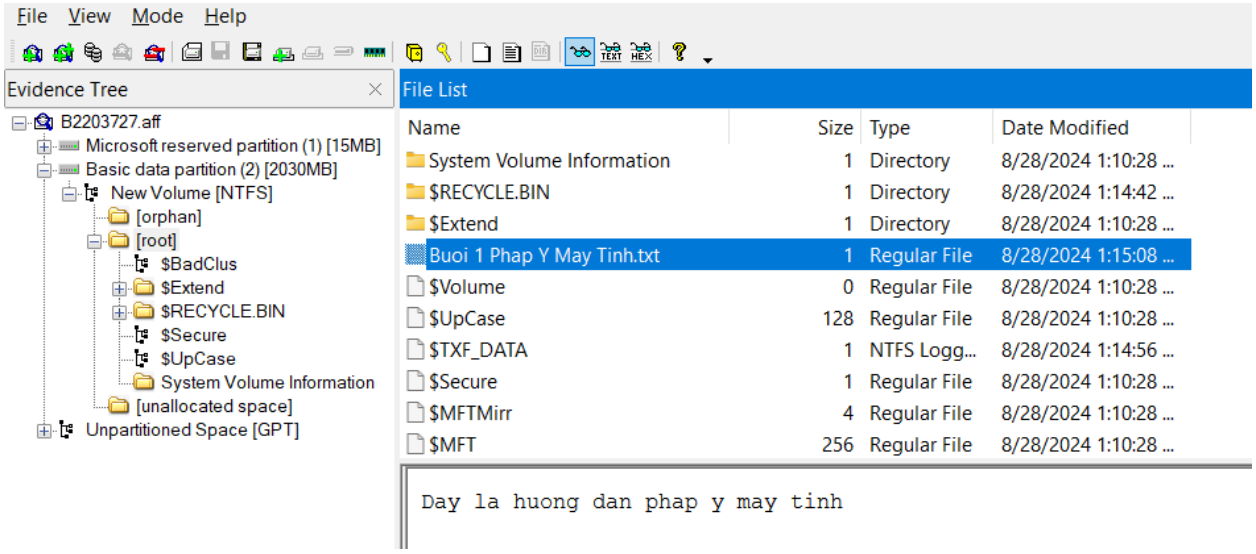
1.3. Tải và cài đặt FTK Imager vào máy tính.

- Nếu cần chạy FTK Imager trực tiếp trên USB, không cần cài đặt lên Windows; thì sao chép toàn bộ thư mục chứa (ví dụ: "C:\Program Files\AccessData\FTK Imager") vào USB, sau đó chạy tập tin “FTK Imager.exe” (không cần thực hiện bước này)

1.4. Thực thi công cụ FTK Imager trên máy tính. Sau đó tiến hành thu thập dữ liệu có trong ổ đĩa ở Câu 1.1.

- Loại tập tin image là AFF; tên tập tin image là <Mã số sinh viên>.
- Kích thước fragment là 1000MB;
- Các thông số khác giữ nguyên theo mặc định.

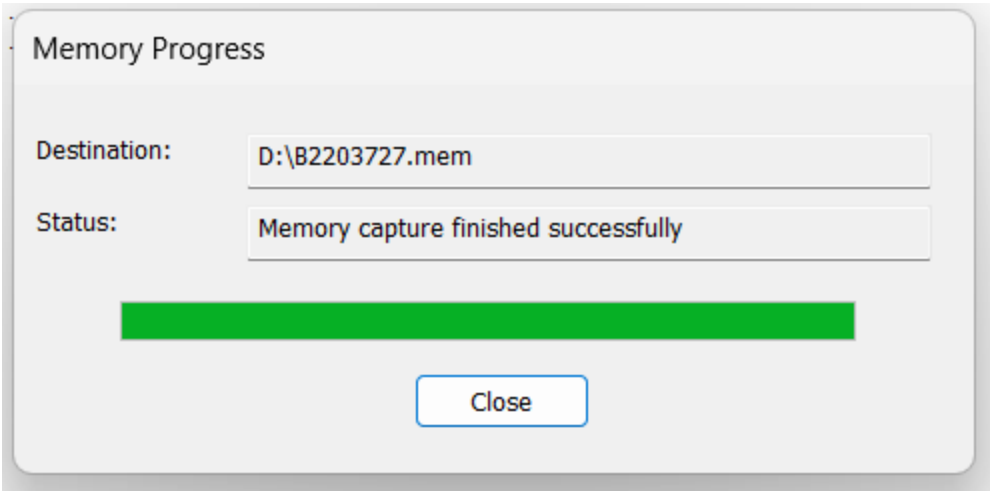
Chụp hình minh họa kết quả thực hiện.



1.5. Sử dụng công cụ FTK để thu thập dữ liệu trên bộ nhớ RAM của máy tính.

- Tên tập tin image là <Mã số sinh viên>.mem

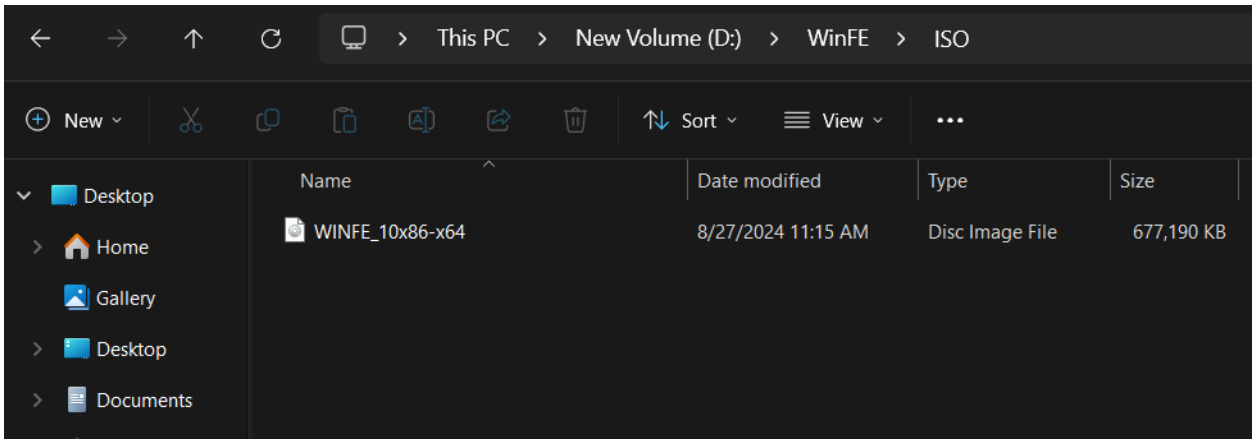
Chụp hình minh họa kết quả thực hiện.



2. Tạo USB thu thập dữ liệu sử dụng WinFE và FTK Imager

- Tải và cài đặt FTK Imager (không cần làm bước này nếu đã thực hiện Câu 1.3)
- Tải WinFE Intel x86/x64; giải nén file vừa tải vào một thư mục (ví dụ: “D:\WinFE”)
- Tải và cài đặt Windows Assessment and Deployment Kit (Windows ADK). Lưu ý lựa chọn phiên bản phù hợp (Win 10/11).
- Sao chép thư mục chứa FTK Imager (ví dụ: "C:\Program Files\AccessData\FTK Imager") vào "D:\WinFE\USB\x86-x64\tools\x64\"
- Tương tự tải WinHex, giải nén và sao chép toàn bộ thư mục “winhex” vào "D:\WinFE\USB\x86-x64\tools\x64\"

- Thực "cmd.exe" với quyền của Administrator. Chuyển tới thư mục chứa WinFE ("D:\WinFE"), thực thi lệnh 'MakeWinFEx64-x86.bat' và 'Makex64-x86-CD.bat' để tạo file ISO khởi động. File ISO tạo ra được chứa trong thư mục "D:\WinFE\ISO".
  Chụp hình minh họa kết quả thực hiện.
- Sử dụng công cụ Ventoy để tạo USB khởi động (không cần thực hiện bước này).



3. Thu thập dữ liệu sử dụng WinFE và FTK Imager

3.1. Tạo máy ảo mục tiêu:

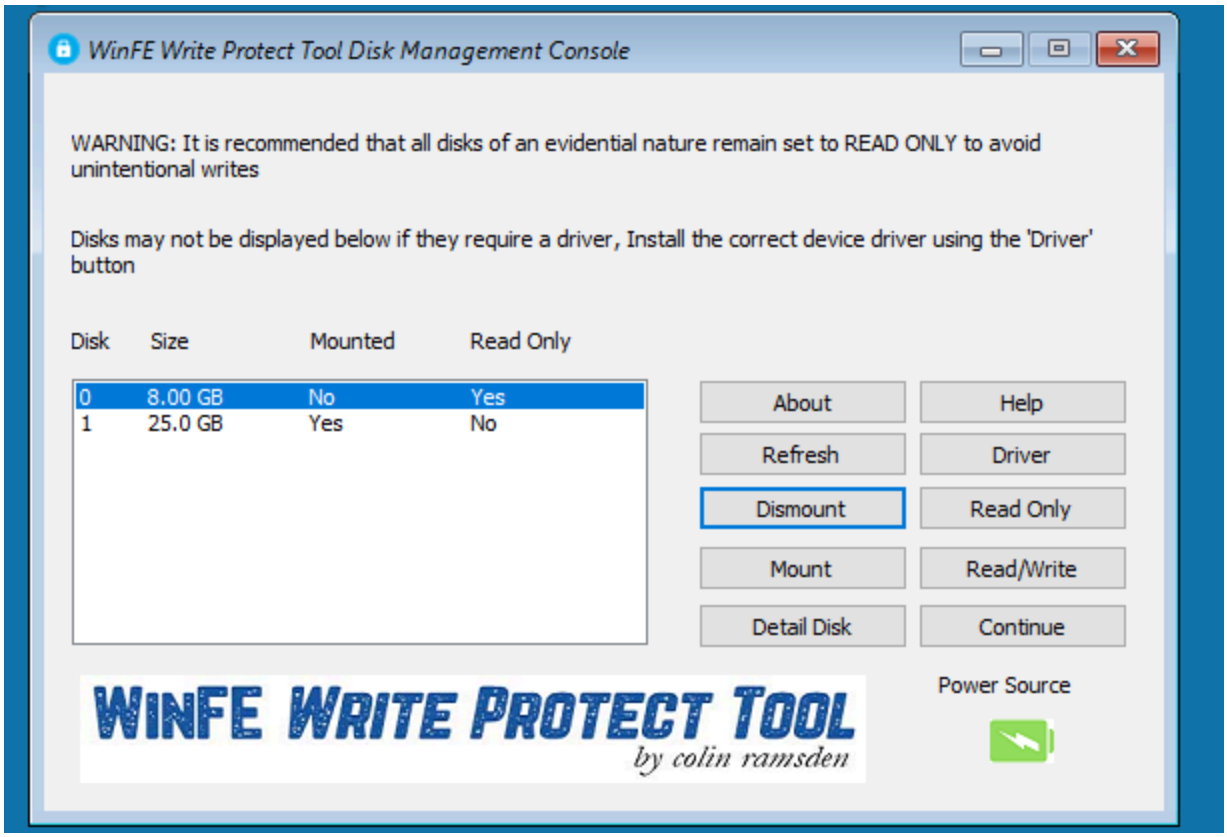
3.1.1. Cài đặt VirtualBox (hoặc phần mềm ảo khác) lên máy tính.

3.1.2. Tải file metasploitable 2, thực thi file để tạo máy ảo Metasploitable trên Virtual Box. Trên máy ảo có một ổ cứng đóng vai trò thiết bị chứa dữ liệu cần thu thập.

3.1.3. Tạo 1 ổ cứng thứ 2 cho máy ảo ở Câu 3.1.2. Ổ cứng này đóng vai trò chứa dữ liệu thu thập được.

3.2. Thêm file ISO WinFE tạo được ở Câu 2 vào ổ CD/DVD của máy ảo. Sau đó khởi động máy ảo. Nhấn F12 và chọn khởi động từ đĩa CD/DVD.

3.3. Ở giao diện của công cụ WinFE Write Protection Tool, chọn Mount + Read/Write cho Disk 0 (20G); Dismount + Read Only cho Disk 1 (8G).
Chụp hình minh họa kết quả thực hiện. Sau đó chọn Continue.



3.4. Tạo ổ đĩa chứa dữ liệu thu thập được:

- Chạy Other tools/Command Prompt; chạy lệnh `diskpart`
- Ở giao diện DISKPART, thực hiện các lệnh sau

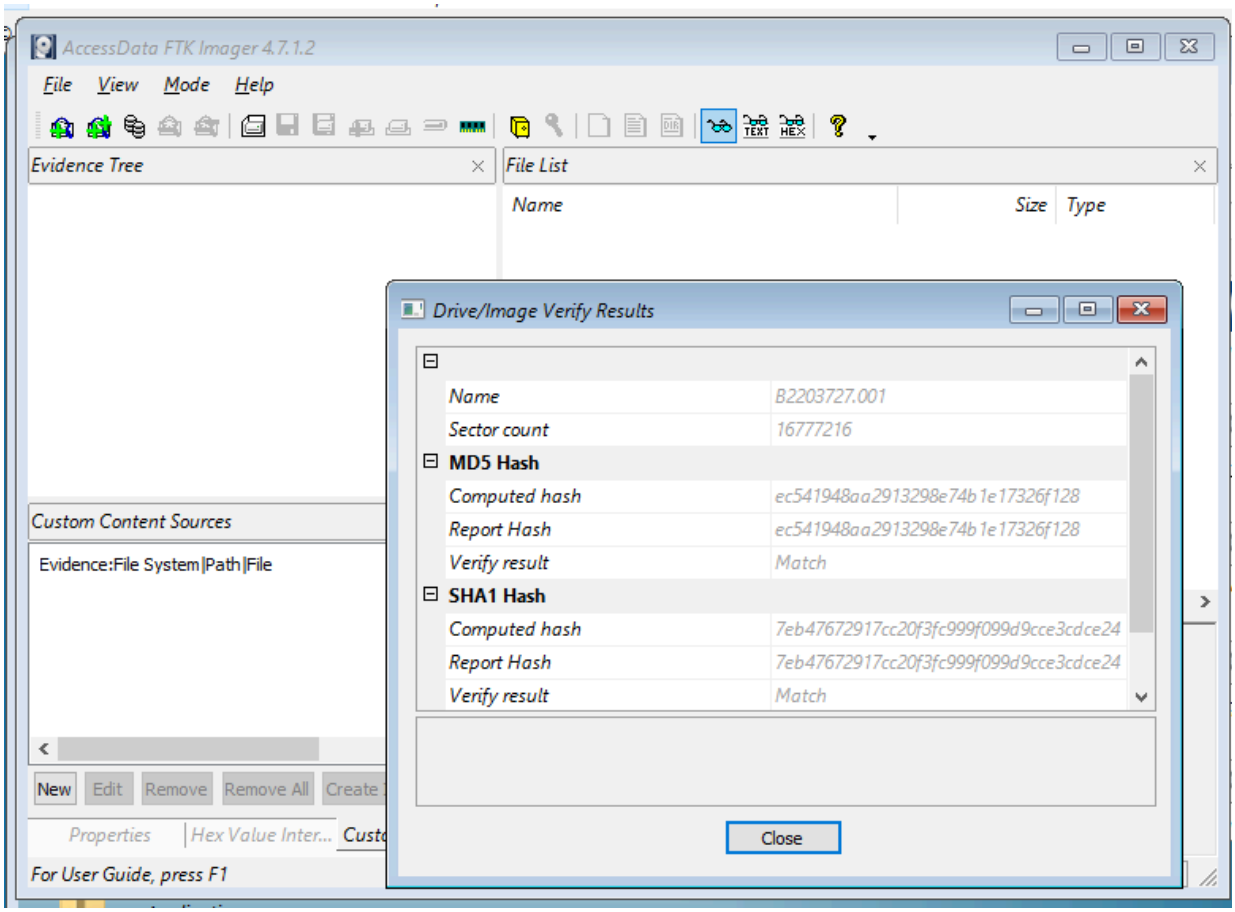
```
list disk
select disk 1
clean
create partition primary
list partition
select partition 1
assign letter=f
```

3.5. Sử dụng công cụ "Other tools/File explorer" để format ổ đĩa vừa tạo (click chuột phải và format).

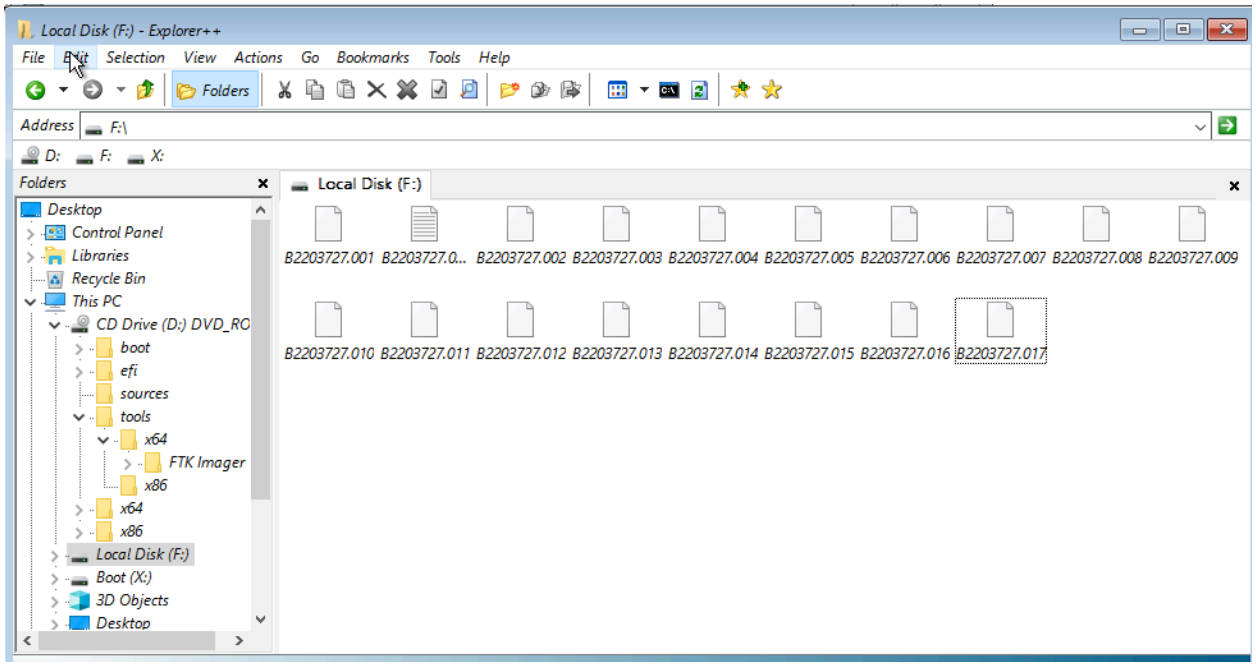
3.6. Sử dụng công cụ FTK để thu thập dữ liệu từ ổ đĩa vật lý Disk 1 và lưu ở ổ đĩa vừa tạo ở Câu 3.5 (ổ đĩa F:\). Công cụ FTK nằm ở đường dẫn: "D:\tools\x64\FTK Imager\FTK Imager.exe"

- Loại tập tin image là RAW (dd); tên tập tin image là <Mã số sinh viên>.
- Kích thước fragment là 500MB;
- Các thông số khác giữ nguyên theo mặc định.

Chụp hình minh họa kết quả thực hiện.



3.7. Sử dụng công cụ Other tools/File explorer mở ổ đĩa F:\
Chụp hình minh họa kết quả thực hiện.



4. Thu thập dữ liệu sử dụng công cụ `dcfldd` trên Kali Linux

4.1. Tải file ISO của Kali Linux_Live.

4.2. Thêm file ISO Kali Linux vào máy ảo ở Câu 3.1. Sau đó khởi động máy ảo. Nhấn F12 và chọn khởi động từ đĩa CD/DVD. Chọn chế độ khởi động "Live system (amd64 forensic mode)".

4.3. Cài đặt công cụ `dcfldd` vào Kali.

```
$sudo apt update
$sudo apt install dcfldd
```

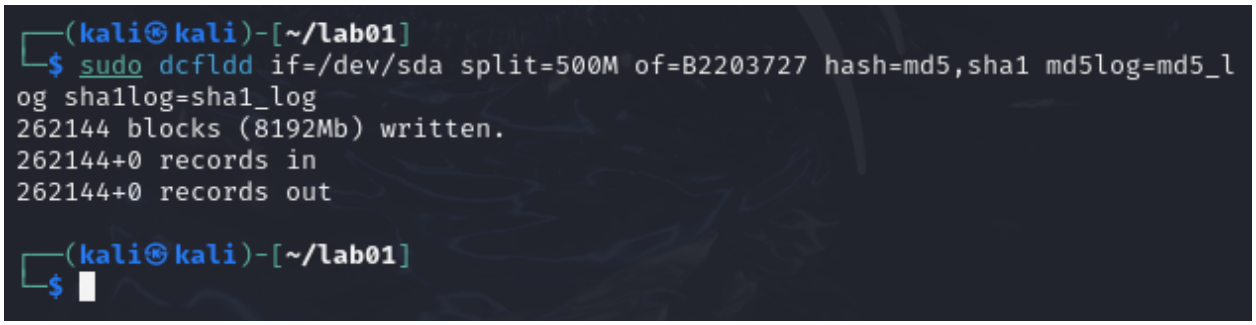
4.4. Tạo thư mục `./data` và mount ổ đĩa `/dev/sdb1` vào thư mục này. Xóa hết dữ liệu đang có trong thư mục. Thư mục này dùng để chứa dữ liệu thu thập được.

```
$sudo mkfs.ext4 /dev/sdb1
$mkdir lab01
$sudo mount /dev/sdb1 ./lab01
$cd lab01
```

4.5. Sử dụng công cụ `dcfldd` để thu thập dữ liệu từ ổ đĩa `/dev/sda`

```
$sudo dcfldd if=/dev/sda split=500M of=<Mã số sinh viên>
hash=md5,sha1 md5log=md5_log sha1log=sha1_log
```

Chụp hình minh họa kết quả thực hiện.



4.6. Tính lại giá trị băm của ổ đĩa `/dev/sda` và so sánh với giá trị băm chứa trong tập tin `md5_log,sha1_log`. Giá trị băm có giống với kết quả của Câu 3.6?

```
$sudo md5sum /dev/sda
$cat md5_log
$sudo sha1sum /dev/sda
$cat sha1_log
```

Chụp hình minh họa kết quả thực hiện.

```
┌──(kali㉿kali)-[~/lab01]
└─$ sudo md5sum /dev/sda
ec541948aa2913298e74b1e17326f128  /dev/sda

┌──(kali㉿kali)-[~/lab01]
└─$ cat md5_log

Total (md5): ec541948aa2913298e74b1e17326f128

┌──(kali㉿kali)-[~/lab01]
└─$ sudo sha1sum /dev/sda
7eb47672917cc20f3fc999f099d9cce3cdce241a  /dev/sda

┌──(kali㉿kali)-[~/lab01]
└─$ cat sha1_log

Total (sha1): 7eb47672917cc20f3fc999f099d9cce3cdce241a
```

4.7. Sử dụng thêm công cụ `Guymager` trên Kali Linux để thu thập dữ liệu.

Chụp hình minh họa kết quả thực hiện.

Devices Misc Help

Rescan

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]
VB0-01f003f6	/dev/sr0	VBOX_CD-ROM	Idle	4.6GB	unknown			
VBd8876e35-be77811b	/dev/sda	VBOX_HARDDISK	Finished - Verified & ok	8.6GB	unknown	0	100%	202.27
VB8b5ee80c-8d64c07c	/dev/sdb	VBOX_HARDDISK	Idle	26.8GB	unknown			
	/dev/loop0	filesystem.squashfs	Idle	4.0GB	unknown			
	/dev/dm-0		Idle	7.5GB	unknown			
	/dev/dm-1		Idle	822.1MB	unknown			

--- Hết ---