Malware lab4

Chen Zhuge IVCM132116

Lab environment:

Linux Mint 17
16GB Samsung USB memory stick(It has been used for over 1 year.)

1. Writing test files into USB memory stick.

File list:

Pdf: Debian 7- System Administration Best Practices.pdf
duhr_Chpt_01.pdf
L1_CloudComputing.pdf
L2_CloudProviders.pdf
learning_bash.pdf
Jpg: 12243713196_14cbfc8aeb_o.jpg
12459622334_f0b284bc07_o.jpg
12487877634_2edf1b5aef_o.jpg
Gif: 377adab44aed2e738b7dbd9d8501a18b86d6faee.gif
292b9c16fdfaaf51a083e0988e5494eef01f7a61.gif
Mp3: Miner Stories.mp3
Avi: LinkGameTest2.avi
ManagementSystem.avi
Pptx: 7.2. Software Engineering II. DevOps_2013.pptx
14 files totally.

As the files are going to have different names after restoration, for the ease of verification, I chose only 14 files in 6 most popular formats, as shown in the figure1.

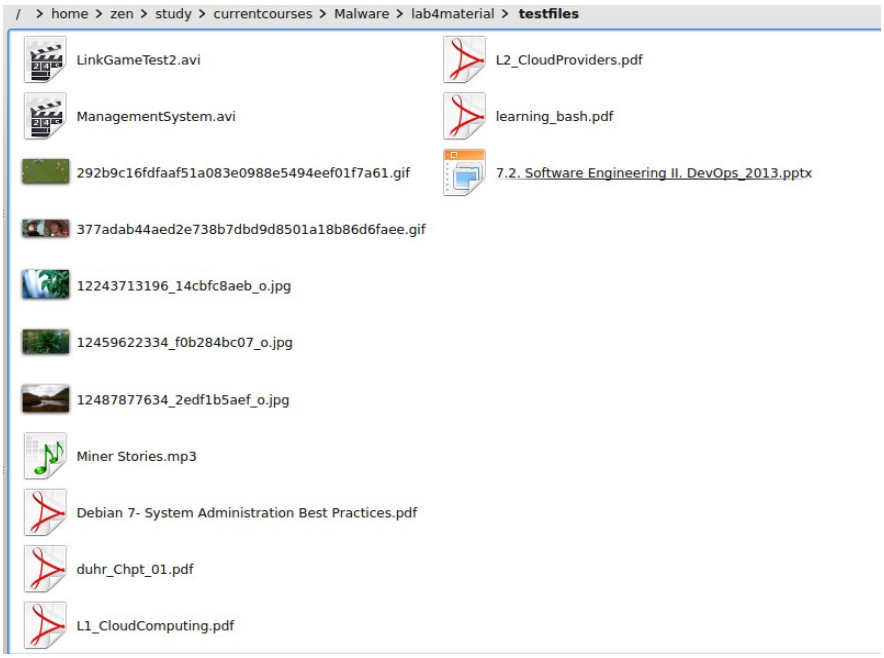

Figure1. Test files snapshot

After these test files were copied to the 16GB Samsung USB memory stick(in root directory), I deleted them, along with some other files that have already existed in the device before this lab.

2. Make image

zen@zen-Inspiron:~ > sudo fdisk -l
[sudo] password for zen:

Disk /dev/sda: 500.1 GB, 500107862016 bytes
255 heads, 63 sectors/track, 60801 cylinders, total 976773168 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0x000d2d5e

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	2048	968638463	484318208	83	Linux
/dev/sda2		968640510	976771071	4065281	5	Extended

Partition 2 does not start on physical sector boundary.

/dev/sda5		968640512	976771071	4065280	82	Linux swap / Solaris

Disk /dev/sdc: 16.1 GB, 16131293184 bytes
255 heads, 63 sectors/track, 1961 cylinders, total 31506432 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xcad4ebea

Device	Boot	Start	End	Blocks	Id	System
/dev/sdc1	*	0	0	0	0	Empty
/dev/sdc4		256	31506431	15753088	c	W95 FAT32 (LBA)

Disk /dev/sdd: 1000.2 GB, 1000170586112 bytes
255 heads, 63 sectors/track, 121597 cylinders, total 1953458176 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x345b142e

Device	Boot	Start	End	Blocks	Id	System
/dev/sdd1		2048	1953458175	976728064	7	HPFS/NTFS/exFAT

zen@zen-Inspiron:~ > sudo dd if=/dev/sdc conv=sync,noerror bs=64K | gzip -c > /tmp/lab4.img.gz
246144+0 records in
246144+0 records out
16131293184 bytes (16 GB) copied, 972,063 s, 16,6 MB/s

Time consumed: about 20 minutes.

3. Restore the image

I Copied the lab4.img.gz from /tmp to ../lab4materials, and extracted it, as a backup.

zen@zen-Inspiron:~/study/currentcourses/Malware/lab4material > sudo kpartx -v -a lab4.img
add map loop0p4 (252:0): 0 31506176 linear /dev/loop0 256

zen@zen-Inspiron:~/study/currentcourses/Malware/lab4material > sudo photorec
PhotoRec 6.14, Data Recovery Utility, July 2013
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

As shown in figure2, in the interface I selected /dev/mapper/loop0p4 as the target to restore.

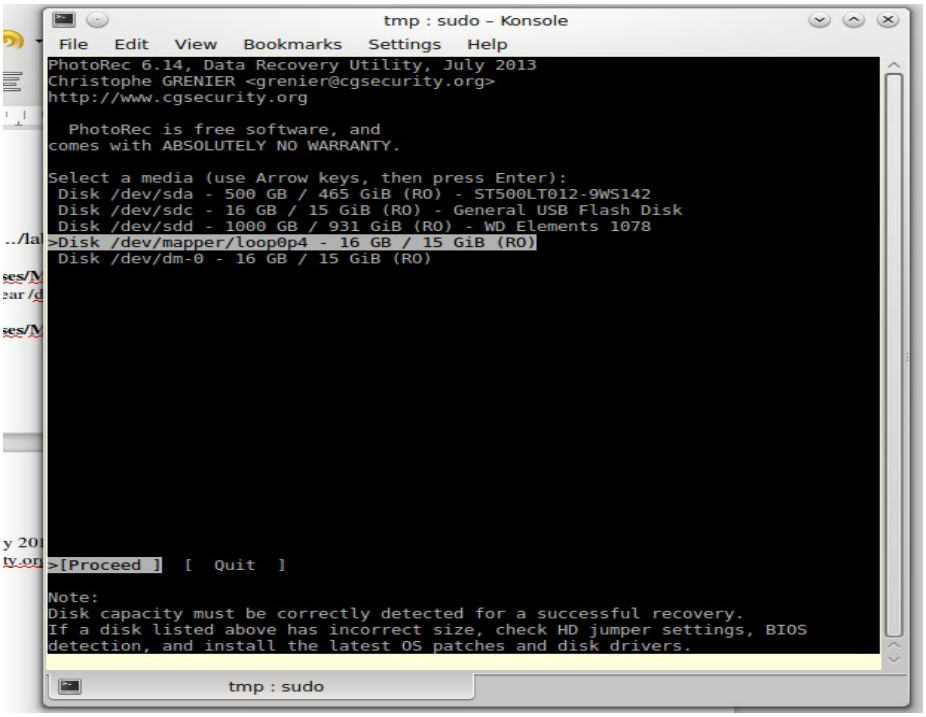

Figure2. Disk selection in Photorec

During the restoration process, I found that many files were being restored, as the USB memory stick has a bit long history, as shown in figure3.

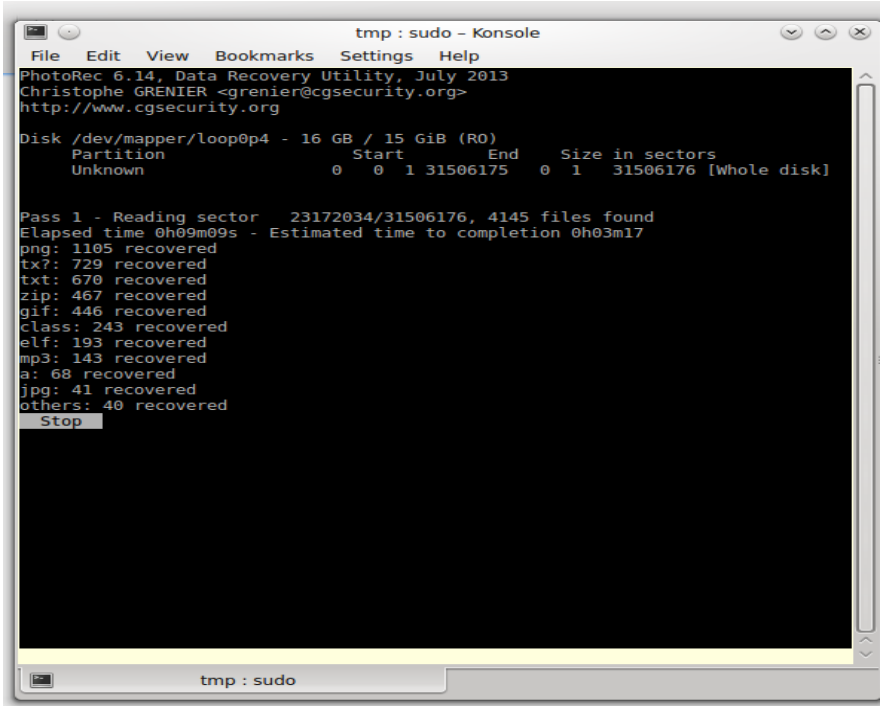

Figure3. Restoration process snapshot

About 10 minutes later, the restoration process has been finished. The output of Photorec is shown as below.

```
PhotoRec 6.14, Data Recovery Utility, July 2013
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/mapper/loop0p4 - 16 GB / 15 GiB (RO)
    Partition                  Start        End    Size in sectors
    Unknown                    0   0  1 31506175   0  1   31506176 [Whole disk]


7706 files saved in /home/zen/tmp/recup_dir directory.
Recovery completed.

You are welcome to donate to support further development and encouragement
http://www.cgsecurity.org/wiki/Donation
```

4. Verification

```
zen@zen-Inspiron:~/tmp > ls
recup_dir.1   recup_dir.12  recup_dir.15  recup_dir.3  recup_dir.6  recup_dir.9
recup_dir.10  recup_dir.13  recup_dir.16  recup_dir.4  recup_dir.7
recup_dir.11  recup_dir.14  recup_dir.2   recup_dir.5  recup_dir.8
```

There are 15 folders generated by Photorec. As the numbers of files are large, I roughly viewed the folders and found some of the files that I copied and deleted in the first step, as shown in figure4.

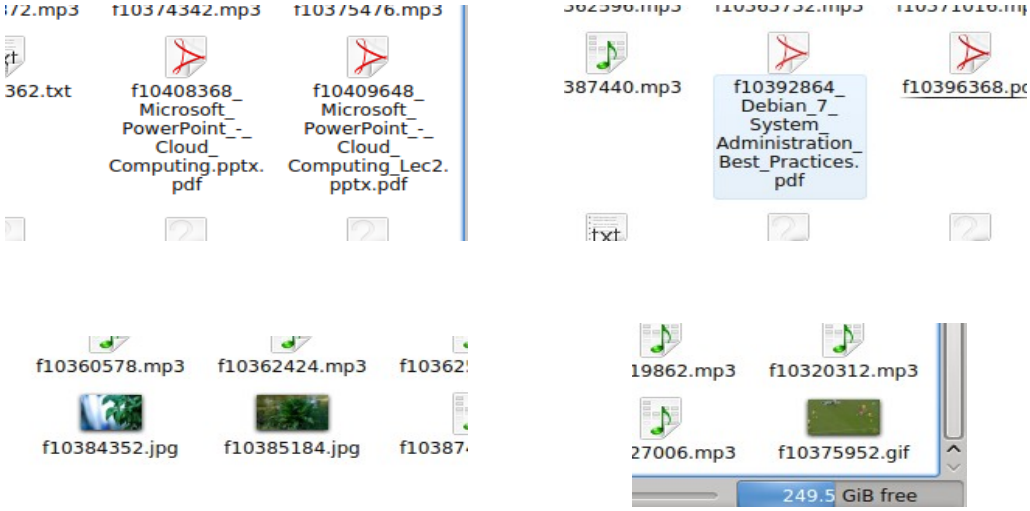

Figure4. Some files that I copied and deleted in the first step

In summary, Photorec is reliable in data restoration. The combination of dd, kpartx and Photorec worked very well in this forensics simulation.

5. Reason of restoring from image rather than from actual drive/card.

Image can provide the same data integrity and processing speed as actual drive/card. Meanwhile, image can also be duplicated whenever as we wish. Therefore, in case of irreversible critical data loss, manipulating image is more preferable than directly manipulating actual drive/card.