Forensics: mounting a partition from a raw image by using Kali Linux

by Alexandre Borges

This document explains how to mount a partition from a raw image by using Kali Linux

Date: January/2015
Revision: 1.0

Today I received a very simple question about how to mount a partition (not a whole disk) from a raw image created by FTK Imager (http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.3.0) by using Kali Linux. Therefore, it follows a straight step-by-step procedure:

1. First, it is necessary to know what are the partition inside of the image:

   ```
   root@hacker:~# mmls /mnt/hgfs/Desktop/win7.001

   DOS Partition Table
   Offset Sector: 0
   Units are in 512-byte sectors
   Slot          Start          End          Length       Description
   00:  Meta     0000000000     0000000000   0000000001   Primary Table (#0)
   01:  -----    0000000000     0000002047   0000002048   Unallocated
   02:  00:00    0000002048     0000206847   0000204800   NTFS (0x07)
   03:  00:01    0000206848     0083884031   0083677184   NTFS (0x07)
   04:  -----    0083884032     0083886079   0000002048   Unallocated
   ```

2. We are interested in mounting the image three and it has as offset the value: **0000206848**. Nonetheless, this offset value is represented as sectors (each sector has 512 bytes), so we have to calculate the number of bytes as being **0000206848** x 512 bytes = **105906176**. Therefore, to mount this partition, execute the following command to create a device (/dev/loop0) associated to our raw image:

   ```
   root@hacker:~# losetup -r -o 105906176 /dev/loop0 /mnt/hgfs/Desktop/win7.001
   ```

3. To verify if everything is OK until now, check if the first sector represents the boot information from our image. Execute:

   ```
   root@hacker:~# dd if=/dev/loop0 bs=512 count=1 | file –

   1+0 records in
   ```

```
1+0 records out
512 bytes (512 B) copied, 0.000292556 s, 1.8 MB/s
/dev/stdin: x86 boot sector, code offset 0x52, OEM-ID "NTFS    ", sectors/cluster 8,
reserved sectors 0, Media descriptor 0xf8, heads 255, hidden sectors 206848, dos < 4.0
BootSector (0x80)
```

4. Now it is time to mount the image (as read only, sure):

   ```
   root@hacker:~# mount -o ro /dev/loop0 /img/
   root@hacker:~# ls /img

   7f6100f431c6bff2452e25540380c83e  pagefile.sys  ProgramData    Program Files
   (x86)  $Recycle.Bin            Users
   Documents and Settings         PerfLogs      Program Files  Recovery           System Volume
   Information  Windows
   ```

5. To undo our job we have to unmount the partition and remove the device associated to the raw image, execute:

   ```
   root@hacker:~# umount /img
   root@hacker:~# losetup -d /dev/loop0
   ```

As we can realize, it was very easy and quick. I hope you have liked it.

Have a nice day.

Alexandre Borges

(LinkedIn: http://www.linkedin.com/in/aleborges)