Hard drive data acquisition and analysis

Introduction

In this practice you will perform data acquisition by using AccessData FTK Imager, dd and dc3dd, where the first tool is a commercial software and the rest two are open source applications.

By the end of this lab you will be able to

- Use a data acquisition application to acquire images in a forensic sound manner
- Compare the advantages and disadvantages of various image acquisition tools
- Perform initial analysis by using Imager

Task 1: Data acquisition (in Windows)

This is individual exercise.

- Find a USB drive on the work bench in the middle of the lab
- Logon to Windows OS and locate the AccessData FTK imager via start button -> all Programs -> AccessData -> FTKImager

If you know (or you think you know) how to use FTK Imager, please go ahead.

Otherwise, follow the instructions below:

1. Launch the AccessData FTK imager application
2. Go to File Create Disc Image,
3. In the popup window, choose the "Physical Drive" option and click on "Next"
    - Have an explore on other options when you have time
4. Select the correct USB drive that need to be imaged and click "Finish"
5. In the new popup window, click on "Add" and Select Raw(dd) for the Destination Image Type
    - Please note that this needs to be repeated for other image formatting as well i.e. SMART, E01 and AFF
6. For the Evidence Item Information, complete as much and accurate as you can; and then click on "Next"
7. Choose a Destination Folder (better to put on E drive) and give a meaningful image filename
8. Regarding the "image fragment size", "compression", and "use AD Encryption" options, [use them and find out what they do] and Click "Finish".
9. Click finish
10. Once the image is created, note down the MD5, and SHA1 hash values.
11. Compare your results from step 10 with another person's and discuss the difference.

12. Note down the difference between dd, SMART, E01 and AFF formats and discuss the pros and cons of these formats

    - ***Both E01 and SMART formats contain the hash value of the image with them but not the dd and AFF formats; personally I prefer E01 and SMART formats as I do not need to carry a***

separate file for the image hash (e.g. another layer of protection for the integrity). However, dd format is compatible with most of the forensic software if not all.

- *Apart from dd, the other three formats allow additional options for the image, including compression (so easier for storage and transportation) and encryption (another layer of security)*

13. Note down the functionalities of "image fragment size", "compression", and "AD encryption" options and discuss their relevance with digital forensic investigations
    - *Image fragment size allows the image to be separated into smaller file sizes, allowing easier transportation*
    - *Compression can be used to reduce the size of an original image; hence smaller storage is required. By default, the comparison level 6 is chosen (from 0-9) due to the compromise between amount of time that requires for carrying out the compression and size of the final file.*
    - *AD encryption can be used to encrypt the image file, providing another layer of security.*

Task 2: Data acquisition and compression (in Linux)

This is individual exercise.

Logon to Linux OS and use the following cmds to complete the imaging process

sudo fdisk -l [this allows you to locate the USB drive]

dd [this allows you to create an image from the USB drive]

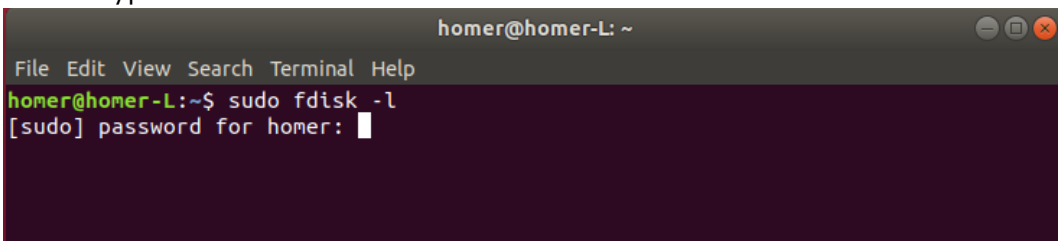
dc3dd [you need to install this program first; then you can use it to image a drive]

gzip [this allows you to compress a file]

If you know (or you think you know) how to use these commands, please go ahead.

Otherwise, follow the instructions below:

1. Type "sudo fdisk -l" in the terminal



2. Locate the USB drive 120MB (this could be 128MB) if not sure please do ask the lecturer!!!

```
homer@homer-L: ~
File  Edit  View  Search  Terminal  Help

Disk /dev/sdb: 120 MiB, 125829120 bytes, 245760 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
Disklabel type: dos
Disk identifier: 0x6f20736b

Device     Boot      Start        End    Sectors   Size Id Type
/dev/sdb1         778135908 1919645538 1141509631 544.3G 72 unknown
/dev/sdb2         168689522 2104717761 1936028240 923.2G 65 Novell Netware 386
/dev/sdb3        1869881465 3805909656 1936028192 923.2G 79 unknown
/dev/sdb4                 0 3637226495 3637226496   1.7T  d unknown

Partition table entries are not in disk order.
homer@homer-L:~$
```

3. Then use "sudo dd if=[location of the USB drive] of=[the destination of outputfile with extension of .img]" to create the image

```
homer@homer-L: ~
File  Edit  View  Search  Terminal  Help
Disk identifier: 0x6f20736b

Device     Boot      Start        End    Sectors   Size Id Type
/dev/sdb1         778135908 1919645538 1141509631 544.3G 72 unknown
/dev/sdb2         168689522 2104717761 1936028240 923.2G 65 Novell Netware 386
/dev/sdb3        1869881465 3805909656 1936028192 923.2G 79 unknown
/dev/sdb4                 0 3637226495 3637226496   1.7T  d unknown

Partition table entries are not in disk order.
homer@homer-L:~$ dd if=/dev/sdb of=/home/homer/Desktop/test.img
dd: failed to open '/dev/sdb': Permission denied
homer@homer-L:~$ sudo dd if=/dev/sdb of=/home/homer/Desktop/test.img
245760+0 records in
245760+0 records out
125829120 bytes (126 MB, 120 MiB) copied, 37.0659 s, 3.4 MB/s
homer@homer-L:~$
```

4. Use the "dc3dd" method to create an image; you may have to use the following command to install the dc3dd program

```
homer@homer-L: ~/Desktop
e  Edit  View  Search  Terminal  Help
ier@homer-L:~/Desktop$ sudo apt-get install dc3dd
```

5. Once dc3dd is installed, image the USB drive by using the dc3dd tool as shown below

```
homer@homer-L: ~/Desktop
File  Edit  View  Search  Terminal  Help
homer@homer-L:~/Desktop$ sudo dc3dd if=/dev/sdb of=/home/homer/Desktop/dc3ddtest
.img

dc3dd 7.2.646 started at 2018-09-26 14:19:54 +0100
compiled options:
command line: dc3dd if=/dev/sdb of=/home/homer/Desktop/dc3ddtest.img
device size: 245760 sectors (probed),      125,829,120 bytes
sector size: 512 bytes (probed)
   32473088 bytes ( 31 M ) copied ( 26% ),   16 s, 1.9 M/s
```

```
homer@homer-L: ~/Desktop
File  Edit  View  Search  Terminal  Help
homer@homer-L:~/Desktop$ sudo dc3dd if=/dev/sdb of=/home/homer/Desktop/dc3ddtest
.img

dc3dd 7.2.646 started at 2018-09-26 14:19:54 +0100
compiled options:
command line: dc3dd if=/dev/sdb of=/home/homer/Desktop/dc3ddtest.img
device size: 245760 sectors (probed),      125,829,120 bytes
sector size: 512 bytes (probed)
   125829120 bytes ( 120 M ) copied ( 100% ),   63 s, 1.9 M/s

input results for device `/dev/sdb':
   245760 sectors in
   0 bad sectors replaced by zeros

output results for file `/home/homer/Desktop/dc3ddtest.img':
   245760 sectors out

dc3dd completed at 2018-09-26 14:20:56 +0100

homer@homer-L:~/Desktop$ ls -l
total 245764
-rw-r--r-- 1 root root 125829120 Sep 26 14:20 dc3ddtest.img
-rw-r--r-- 1 root root 125829120 Sep 26 14:11 test.img
homer@homer-L:~/Desktop$
```

6. Use gzip to compress the image file

```
homer@homer-L: ~/Desktop
File  Edit  View  Search  Terminal  Help
homer@homer-L:~/Desktop$ ls -l
total 245764
-rw-r--r-- 1 homer homer 125829120 Sep 26 14:20 dc3ddtest.img
-rw-r--r-- 1 root  root  125829120 Sep 26 14:11 test.img
homer@homer-L:~/Desktop$ gzip dc3ddtest.img
homer@homer-L:~/Desktop$ ls -l
total 147604
-rw-r--r-- 1 homer homer  25310264 Sep 26 14:20 dc3ddtest.img.gz
-rw-r--r-- 1 root  root  125829120 Sep 26 14:11 test.img
homer@homer-L:~/Desktop$
```

Task 3: Discuss the pros and cons of the above imaging tools

Talk to the person next to you and discuss the pros and cons of the used forensic imaging tools.

- ***Imager is a commercial application which is proved to be used in real life scenarios. Also it provides a number of utilities such as encryption, compression and calculating the hash value of the image; and support various formats.***
- ***While dd and dc3dd are open source applications, they are relatively easy to use; dc3dd is better than dd as it shows the progress of the imaging process. Both of them do not offer any additional functionalities other than creating the raw image.***