FORENSICS
LAB SERIES

Lab 4: Forensic Acquisition Using Linux Tools

Material in this Lab Aligns to the Following Certification Domains/Objectives		
GIAC Certified Forensics Examiner (GCFE) Domains	Certified Cyber Forensics Professional (CCFP) Objectives	Computer Hacking Forensic Investigator (CHFI) Objectives
3: Evidence Acquisition, Preparation, and Preservation	2: Investigations	9: Data Acquisition and Duplication

Document Version: 2016-08-17

Contents

Introduction 3
Objective 3
Pod Topology 4
Lab Settings 5
1 Configure Disk to be Writeable 6
2 Create dd Image Acquisition 9
3 Create dcfldd Image Acquisition 11

Introduction

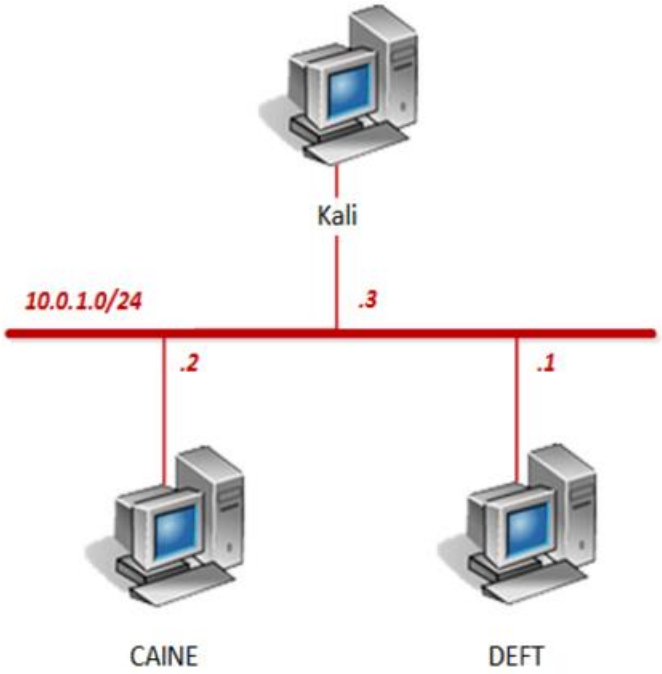
This lab will introduce the task of forensic acquisition using two popular command tools, “dd” (data dump) and “dcfldd” (enhanced version of dd). The lab will acquire two types of partitions and create forensic images for analysis.

Objective

In this lab, you will be conducting forensic practices using various tools. You will be performing the following tasks:

1. Configure Disk to be Writeable
2. Create dd Image Acquisition
3. Create dcfldd Image Acquisition

Pod Topology



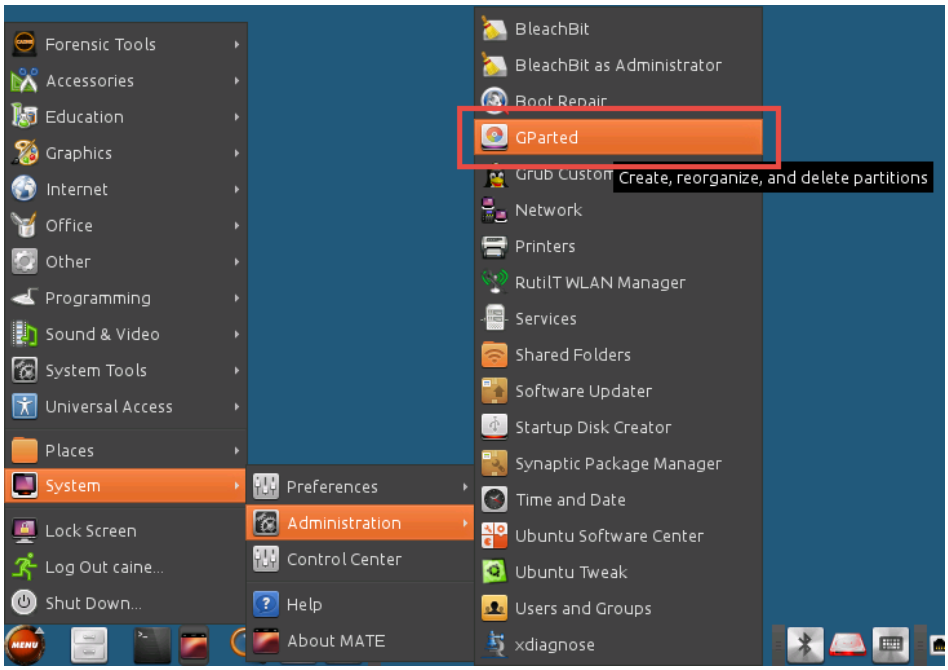
Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

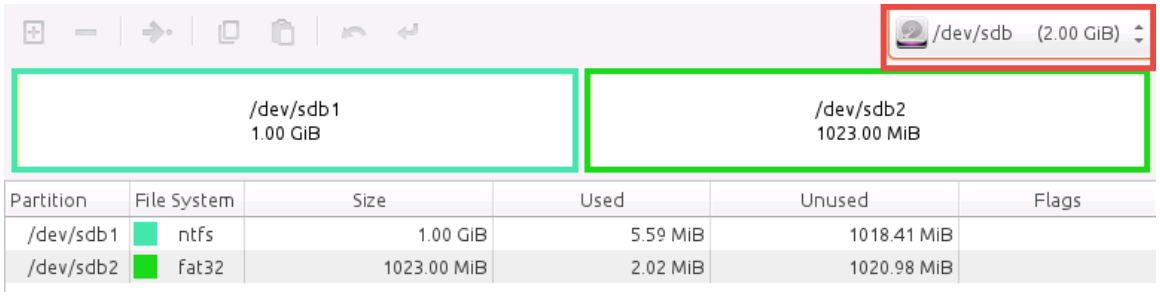
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
DEFT	10.0.1.1	deft	password
CAINE	10.0.1.2	caine	
Kali	10.0.1.3	root	toor

1 Configure Disk to be Writeable

1. Click on the **CAINE** graphic on the *topology page* to open the VM.
2. Open the **GParted** application by navigating to **Start Menu > System > Administration > GParted**.

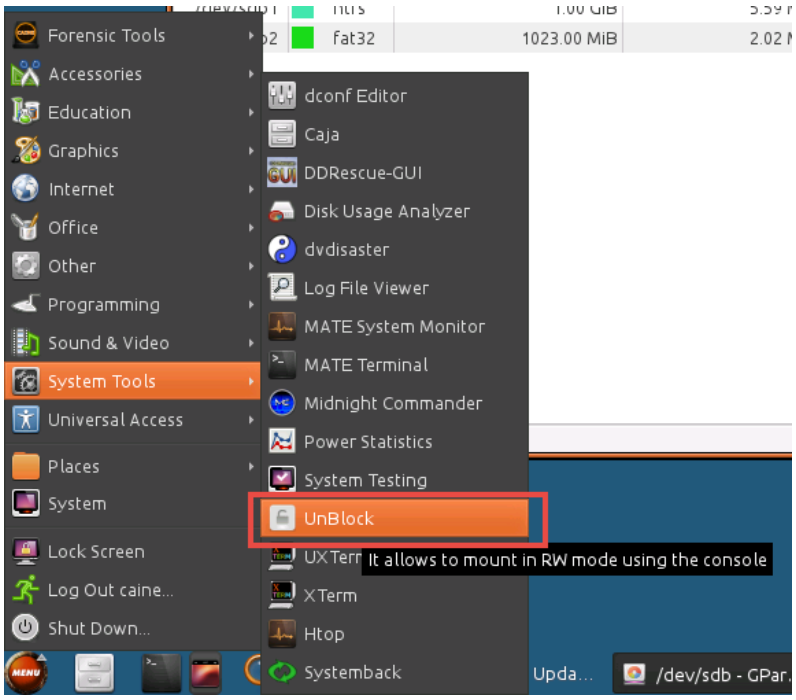


3. Change disk by clicking on the **drop-down menu** located in the top-right corner of the *GParted* application window and select **/dev/sdb (2.00GiB)**.

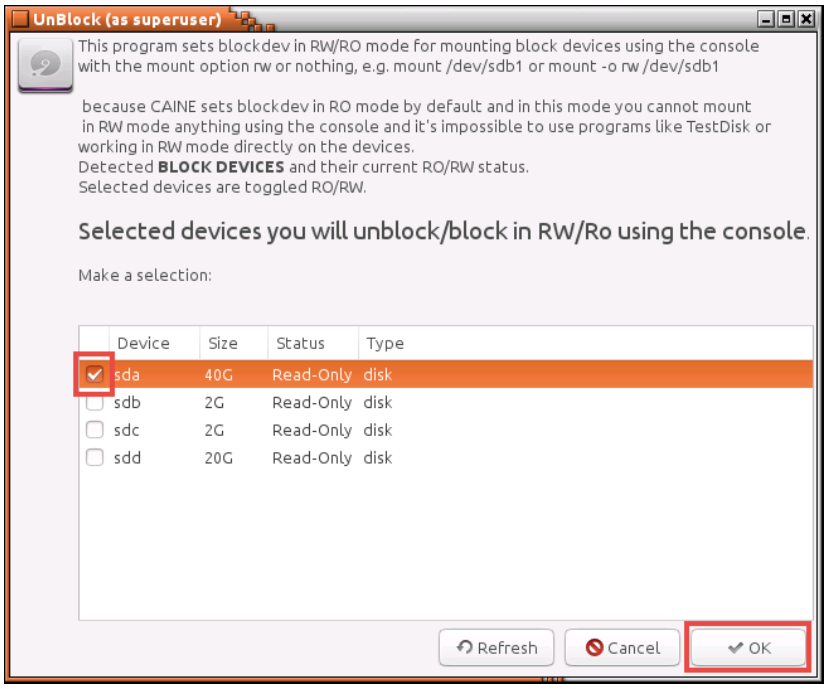


Notice two partitions appear for */dev/sdb*.

4. Before continuing, a verification needs to be made on whether there are write permissions enabled on */dev/sda* to create images. Navigate to **Start Menu > System Tools > UnBlock**.

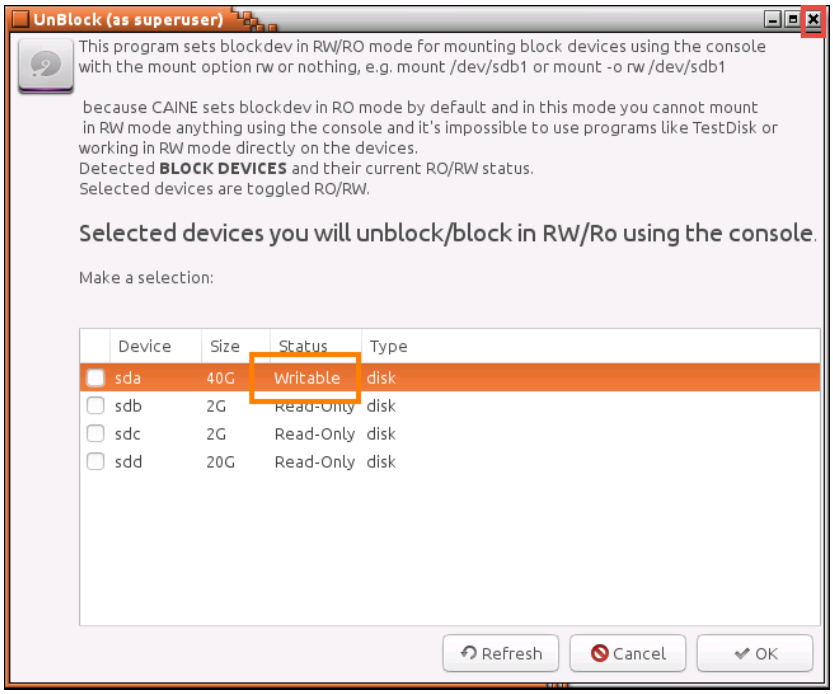


5. A new *UnBlock* application window appears, notice the 4 drives listed. Check the box next to **sda** and click **OK**.



This will make the drive writeable.

6. Notice the *UnBlock* window reappears. Confirm that the *Status* of the *sda* drive now reads *Writeable*. Close the **UnBlock** application window.



2 Create dd Image Acquisition

1. Open a new terminal by clicking on the **MATE Terminal** icon located on the bottom panel.

2. Using the terminal, start by splitting the */dev/sdb1* partition into bytes of 650MB. Type the command below followed by pressing the **Enter** key.

```
sudo dd if=/dev/sdb1 | split -b 650m - ntfsimage_sdb.
```

Notice the cursor will sit for a while with no prompt received back immediately. Allow the program to run for 1-2 minutes.

```
caine@Caine01:~$ sudo dd if=/dev/sdb1 | split -b 650m - ntfsimage_sdb.
2097152+0 records in
2097152+0 records out
1073741824 bytes (1,1 GB) copied, 16,8963 s, 63,5 MB/s
caine@Caine01:~$
```

Breakdown:

if = input file
split = splits the image into bytes of size x

3. Enter the command below to list the files in the current directory.

```
ls -l
```

```
caine@Caine01:~$ ls -l
total 1048620
drwx------  5 caine caine      4096 mag  5 00:33 Desktop
drwx------  2 caine caine      4096 set 24  2014 Documents
drwx------ 16 caine caine      4096 mag 13 04:06 Downloads
drwx------  2 caine caine      4096 ott 31  2015 Music
-rw-rw-r--  1 caine caine 681574400 lug  8 20:19 ntfsimage_sdb.aa
-rw-rw-r--  1 caine caine 392167424 lug  8 20:19 ntfsimage_sdb.ab
drwx------  2 caine caine      4096 ott 14  2015 Pictures
drwx------  2 caine caine      4096 ott 30  2015 Public
-rw-r--r--  1 root  root       1164 mag  2 01:41 qphotorec.log
drwx------  2 caine caine      4096 set  1  2014 Templates
drwx------  2 caine caine      4096 set  1  2014 Videos
caine@Caine01:~$
```

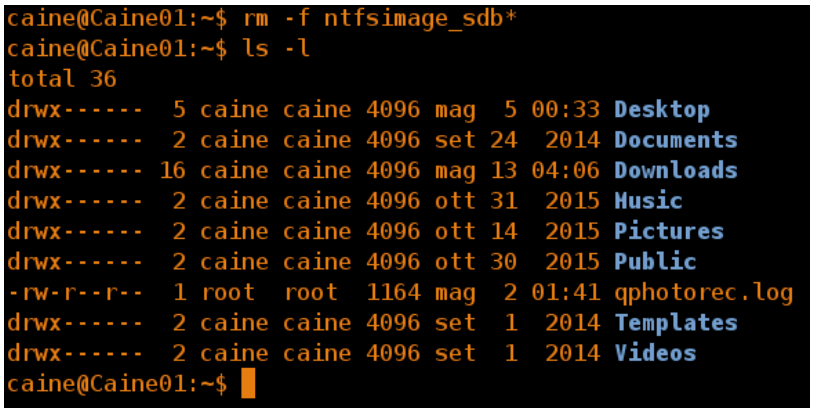
Notice the raw copies of the partition *sdb1* split into 650MB each. The period adds the extension to the end of the filename to show that parts of the image.

4. Make room on the *sda* disk by removing the acquired image from *sdb1*. Enter the command below.

```
rm -f ntfsimage_sdb*
```

5. Confirm that the image has been removed by initiating the command below.

```
ls -l
```



3 Create dcfldd Image Acquisition

1. The dd tool is a tool mostly for system management. With the Defense Computer Forensic Laboratory (dcfldd) tool, it is a tool specifically for forensic acquisition. Using the same terminal, use dcfldd for /dev/sdb2 and add a MD5 hash output to it. Enter the command below.

```
sudo dcfldd if=/dev/sdb2 split=650M of=fat32image hash=md5,sha1
```

```
caine@Caine01:~$ sudo dcfldd if=/dev/sdb2 split=650M of=fat32image hash=md5,sha1
32512 blocks (1016Mb) written.Total (md5): 7a4a24b4eb49fd7d03205475fdab7325
Total (sha1): 7e409c9d235f3d8cdad70e463e2c55e8192e5bce

32736+0 records in
32736+0 records out
caine@Caine01:~$
```

Breakdown:

if = input file
of = output file
split = split image into bytes of size x
hash = hash functions for integrity check

Note: No period necessary with split; dcfldd handles the extension.

2. Enter the command below to list the files in the current directory.

```
ls -l
```

```
caine@Caine01:~$ ls -l
total 1047592
drwx------  5 caine caine      4096 mag  5 00:33 Desktop
drwx------  2 caine caine      4096 set 24  2014 Documents
drwx------ 16 caine caine      4096 mag 13 04:06 Downloads
-rw-r--r--  1 root  root  681574400 lug  8 21:19 fat32image.000
-rw-r--r--  1 root  root  391118848 lug  8 21:19 fat32image.001
drwx------  2 caine caine      4096 ott 31  2015 Music
drwx------  2 caine caine      4096 ott 14  2015 Pictures
drwx------  2 caine caine      4096 ott 30  2015 Public
-rw-r--r--  1 root  root       1164 mag  2 01:41 qphotorec.log
drwx------  2 caine caine      4096 set  1  2014 Templates
drwx------  2 caine caine      4096 set  1  2014 Videos
caine@Caine01:~$
```

Notice the success of forensically acquiring the partition.

3. Close all **PC Viewers** and end the reservation to complete the lab.

