FORENSICS
LAB SERIES

Lab 2: Exploring the Linux File System

Document Version: 2016-08-17

Material in this Lab Aligns to the Following Certification Domains/Objectives	
Certified Cyber Forensics Professional (CCFP) Objectives	Computer Hacking Forensic Investigator (CHFI) Objectives
4: Digital Forensics	7: Understanding Hard Disks and File Systems

Contents

Introduction

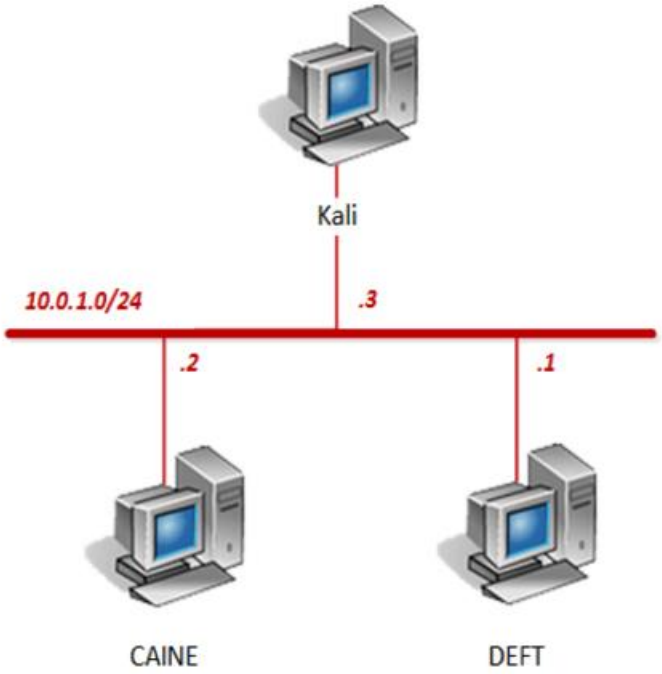
This lab will explore the Linux file system in detail. The ability to understand how data is stored and organized is a valuable skill for the forensic examiner.

Objective

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

1. Exploring Linux Data Structure with iNodes

Pod Topology



Lab Settings

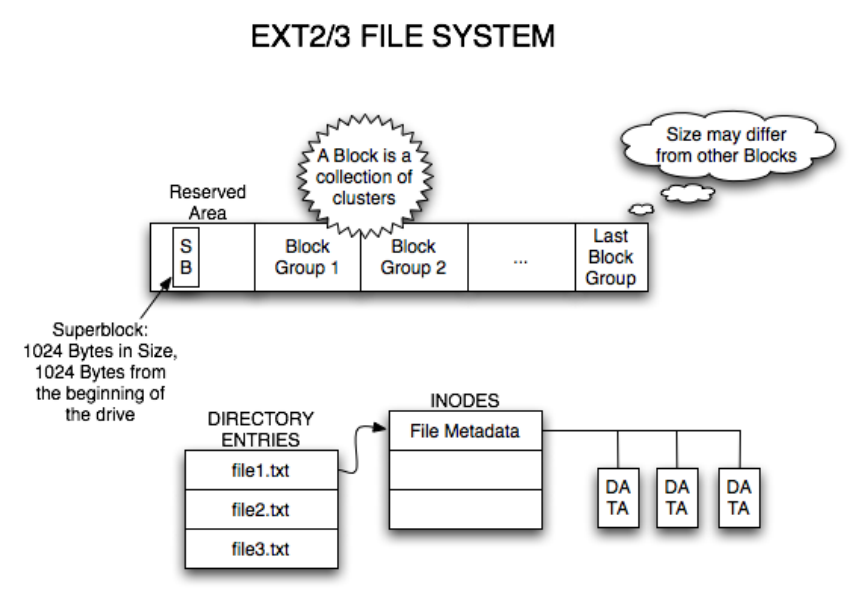
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

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 Exploring Linux Data Structure with iNodes

1. Click on the **CAINE** graphic on the *topology page* to open the VM.
2. Open a new terminal by clicking on the **MATE Terminal** icon located on the bottom panel.

The *Linux* file system contains *inodes*, *blocks*, and *superblocks*. As a reference, see the diagram below.



3. Using the terminal, start with by analyzing with the *inode* by typing the command below followed by pressing **Enter**. The *inode* contains metadata about a specified file.

```
ls -ia
```

```
caine@Caine01:~$ ls -ia
129794 .                205964 .ICEauthority    131109 .themes
129793 ..               130243 .icons           131110 .thumbnails
205989 .bash_history    130244 .java            131114 .tkcvs
129798 .bash_logout     130259 .kde             131115 .tkcvs-picklists
129799 .bashrc          130290 .local           129795 .TrueCrypt
129800 .cache           130659 .mobiusft        131139 Videos
129859 .compiz          131019 .mozilla         672071 .wine
129862 .config          131137 Music            131116 .wireshark
348842 .cpan            131138 Pictures         151304 .wxHexEditor
130157 .dbus            796810 .pip             131119 .x11vnc.log.caine:5900
131132 Desktop          671737 .PlayOnLinux     131120 .x11vnc.log.caine:5980
130159 .dmrc            131099 .profile         205960 .Xauthority
131136 Documents        131135 Public           129797 .Xdefaults
131133 Downloads        131100 .pureadminrc     131392 .xinputrc
130160 .dvdisaster      131101 .putty           129856 .xsession-errors
130161 .fred            131104 .python_history  129854 .xsession-errors.old
130164 .gconf           144558 qphotorec.log    131121 .zenmap
130195 .gimp-2.8        131105 .remmina         131128 .zuluCrypt
130235 .gksu.lock       131107 .save_dir        131131 .zuluCrypt-socket
130236 .gnupg           131108 .ssh
130241 .gstreamer-0.10  131134 Templates
caine@Caine01:~$
```

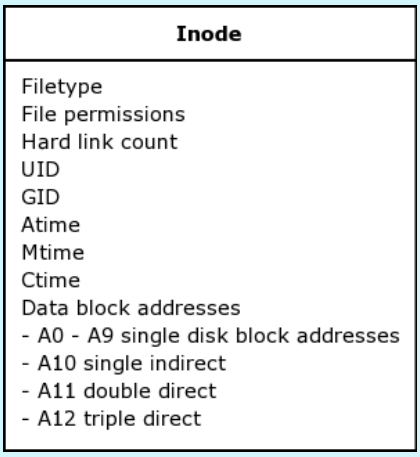
Notice the *inode* numbers for all the files that are both visible and hidden along with the directories.

4. Using the terminal, analyze the metadata for the **.bashrc** hidden file by entering the command below.

```
stat .bashrc
```

```
caine@Caine01:~$ stat .bashrc
  File: '.bashrc'
  Size: 3637            Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 129799      Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 1000/   caine)   Gid: ( 1000/   caine)
Access: 2016-06-09 14:41:57.408080152 +0200
Modify: 2014-09-01 17:08:26.000000000 +0200
Change: 2015-11-12 15:45:29.030177017 +0100
 Birth: -
caine@Caine01:~$
```


As a reference, the image below highlights the basic structure of metadata. Analyze the metadata presented from the *.bashrc* file.

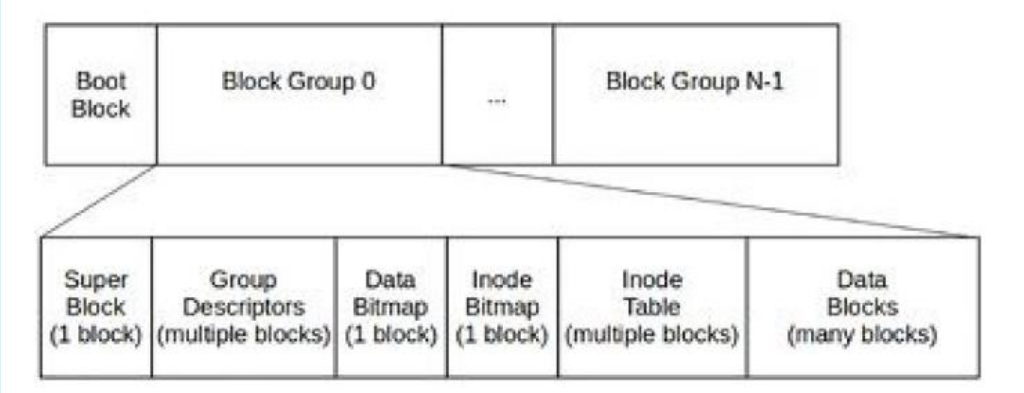


5. *Tune2fs* is an application that allows a system administrator to change various tunable parameters on a specified file system. Enter the *tune2fs* command below to look at the overall file system of the Linux system.

```
sudo tune2fs -l /dev/sda1 | more
```

```
tune2fs 1.42.9 (4-Feb-2014)
Filesystem volume name:   SB@
Last mounted on:          /
Filesystem UUID:          2517b2fe-5d46-4d0c-8cd3-d592a930490e
Filesystem magic number:  0xEF53
Filesystem revision #:    1 (dynamic)
Filesystem features:      has_journal ext_attr resize_inode dir_index filetype n
eeds_recovery extent flex_bg sparse_super large_file huge_file uninit_bg dir_nli
nk extra_isize
Filesystem flags:         signed_directory_hash
Default mount options:    user_xattr acl
Filesystem state:         clean
Errors behavior:          Continue
Filesystem OS type:       Linux
Inode count:              1906320
Block count:              7674880
Reserved block count:     331442
Free blocks:              1769564
Free inodes:              1441147
First block:              0
Block size:               4096
Fragment size:            4096
Reserved GDT blocks:      623
--More--
```


Using the "l" option allows a user to view the contents of the "Superblock", which contains information about the file system. Notice the inode counts, block counts, free blocks, and free inodes among additional information. Refer to the diagram below to get a perspective on the information presented.



6. Use the **spacebar** to navigate down a page or the **down arrow** to navigate to a new line and analyze the information. Navigate all the way down to receive your prompt back.
7. Enter the command below to identify the overall *inode* usage.

```
df -i
```

```
caine@Caine01:~$ df -i
Filesystem      Inodes  IUsed   IFree IUse% Mounted on
udev            501152    592  500560    1% /dev
tmpfs           505175    589  504586    1% /run
/dev/sda1      1906320 465188 1441132   25% /
none            505175      2  505173    1% /sys/fs/cgroup
none            505175      7  505168    1% /run/lock
none            505175      4  505171    1% /run/shm
none            505175     20  505155    1% /run/user
caine@Caine01:~$
```

Notice that there is only 25% of the total *inodes* used.

2 Exploring Nodes with Disk Editor

1. Navigate to the **/home/caine/Downloads** directory by entering the command below.

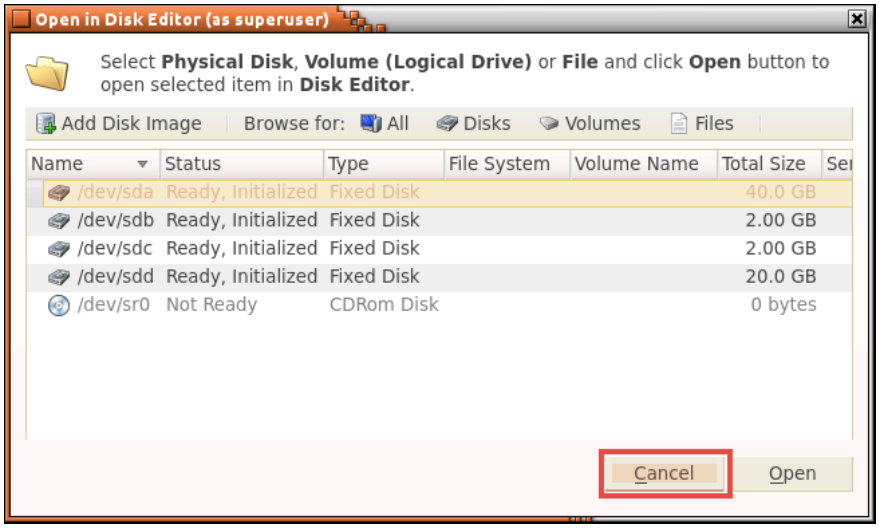
```
cd Downloads/
```

2. Analyze a bit deeper using another tool called *DiskEditor*. Enter the command below.

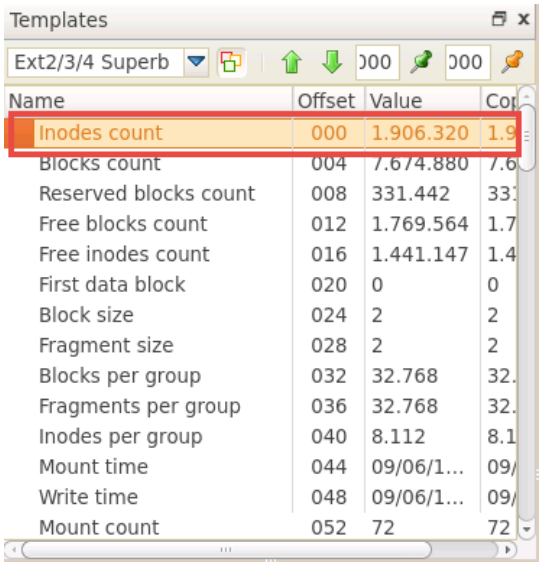
```
./DiskEditor
```

3. Notice a new *DiskEditor* window appear. Using the *Getting Started* wizard, click on the **Open Disk** icon.

4. In the *Open in DiskEditor* window, click the **Cancel** button.



5. Using the hex view in *DiskEditor*, explore the file system. Click on the **Inodes count** entry in the left pane, underneath the *Name* column.



Notice the tool highlights the value in the hex window based on what was highlighted in the left pane. When compared to the inode count reported by tune2fs, the inodes count is the same value. Using *DiskEditor* has its advantages so that it is now possible to traverse the file system easily and visually see where the various sizes and counts come from.

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

