



FORENSICS LAB SERIES

Lab 7: Windows OS Artifact Forensics

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
4: File and Program Activity Analysis	4: Digital Forensics	8: Windows Forensics

Document Version: 2016-08-17

Copyright © 2016 Network Development Group, Inc.
www.netdevgroup.com

NETLAB Academy Edition, NETLAB Professional Edition and NETLAB+ are registered trademarks of Network Development Group, Inc.

Contents

Introduction	3
Objective	3
Pod Topology	4
Lab Settings	5
1 Analyzing Prefetch Files	6
2 Mounting & Exploring Shadow Copies	9

Introduction

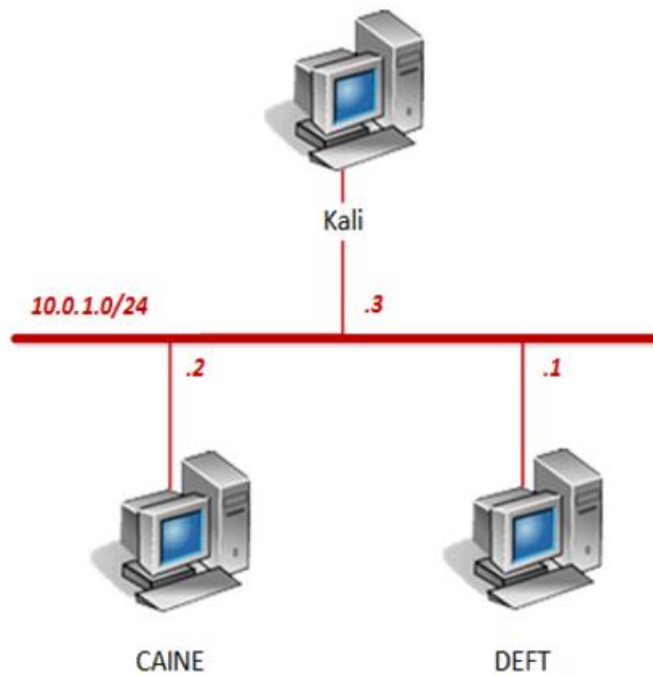
This lab will introduce the concept of performing a forensic examination of a Windows system. The Windows OS artifacts are not in the registry or internet browsing history, instead they will be artifacts left behind by the Windows OS.

Objective

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

1. Analyzing Prefetch Files
2. Mounting & Exploring Shadow Copies

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 Analyzing Prefetch Files

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 tool pane.



3. Using the terminal, navigate to the **/home/caine/Downloads** directory by typing the command below followed by pressing the **Enter** key.

```
cd Downloads/
```

```
caine@Caine01:~$ cd Downloads/
caine@Caine01:~/Downloads$
```

4. List the files in the current directory by entering the command below.

```
ls
```

```
caine@Caine01:~/Downloads$ ls
11-carve-fat                license.txt
12-carve-ext2               lifer-1.0.0
Application.evtx            lifer-1.0.0.tar.gz
bin                          LiME-master
DiskEditor                  Parse-Evtx-1.1.1
DiskEditor.tar.gz           profiles-master
doc                          pynker-master
EvtxParser-current.zip      Security.evtx
Gary Kessler File Signatures System.evtx
lib                          Windows-Prefetch-Parser-master
libvshadow-20160110         wxHexEditor
caine@Caine01:~/Downloads$
```

Notice the *Windows-Prefetch-Parser-master* directory.

5. Navigate into the **/home/caine/Downloads/Windows-Prefetch-Parser-master/windowsprefetch** directory. Enter the command below.

```
cd Windows-Prefetch-Parsers-master/windowsprefetch
```

```
caine@Caine01:~/Downloads$ cd Windows-Prefetch-Parser-master/windowsprefetch
caine@Caine01:~/Downloads/Windows-Prefetch-Parser-master/windowsprefetch$
```

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

```
ls
```

```
caine@Caine01:~/Downloads/Windows-Prefetch-Parser-master/windowsprefetch$ ls
prefetch.py
caine@Caine01:~/Downloads/Windows-Prefetch-Parser-master/windowsprefetch$
```

7. Notice the prefetch.py file. Prefetch files are created by the Windows operating system after an application is run. It tracks how many times an application runs and is used to speed up the loading of the application. Enter the command below to examine a sample prefetch file.

```
./prefetch.py -f /home/caine/Desktop/Prefetch_Files/SOLITAIRE.EXE-906D7E29.pf
```

```
caine@Caine01:~/Downloads/Windows-Prefetch-Parser-master/windowsprefetch$ ./prefetch.py -f /home/caine/Desktop/Prefetch_Files/SOLITAIRE.EXE-906D7E29.pf

=====
SOLITAIRE.EXE-906D7E29.pf
=====

Executable Name: SOLITAIRE.EXE

Run count: 1
Last Executed: 2015-03-24 18:29:07.209940

Volume Information:
  Volume Name: \DEVICE\HARDDISKVOLUME2
  Creation Date: 2015-03-25 11:08:36.956950
  Serial Number: ca0c7a48

Directory Strings:
  \DEVICE\HARDDISKVOLUME2\PROGRAM FILES
  \DEVICE\HARDDISKVOLUME2\PROGRAM FILES\MICROSOFT GAMES
  \DEVICE\HARDDISKVOLUME2\PROGRAM FILES\MICROSOFT GAMES\SOLITAIRE
  \DEVICE\HARDDISKVOLUME2\USERS
  \DEVICE\HARDDISKVOLUME2\USERS\INFORMANT
```

Notice the number of times the program was run, the date it was last run, the directories it was found in, and the resources the application uses.



8. Enter the command below to analyze another prefetch file, but this time a *CMD.exe* file from a Windows 7 system.

```
./prefetch.py -f /home/caine/Desktop/Prefetch_Files/Win7/CMD.EXE-4A81B364.pf
```

```
caine@Caine01:~/Downloads/Windows-Prefetch-Parser-master/windowsprefetch$ ./prefetch.py -f /home/caine/Desktop/Prefetch_Files/Win7/CMD.EXE-4A81B364.pf

=====
CMD.EXE-4A81B364.pf
=====

Executable Name: CMD.EXE

Run count: 2
Last Executed: 2016-01-16 20:26:42.515108

Volume Information:
  Volume Name: \DEVICE\HARDDISKVOLUME2
  Creation Date: 2016-01-16 21:15:18.109374
  Serial Number: 88008c2f

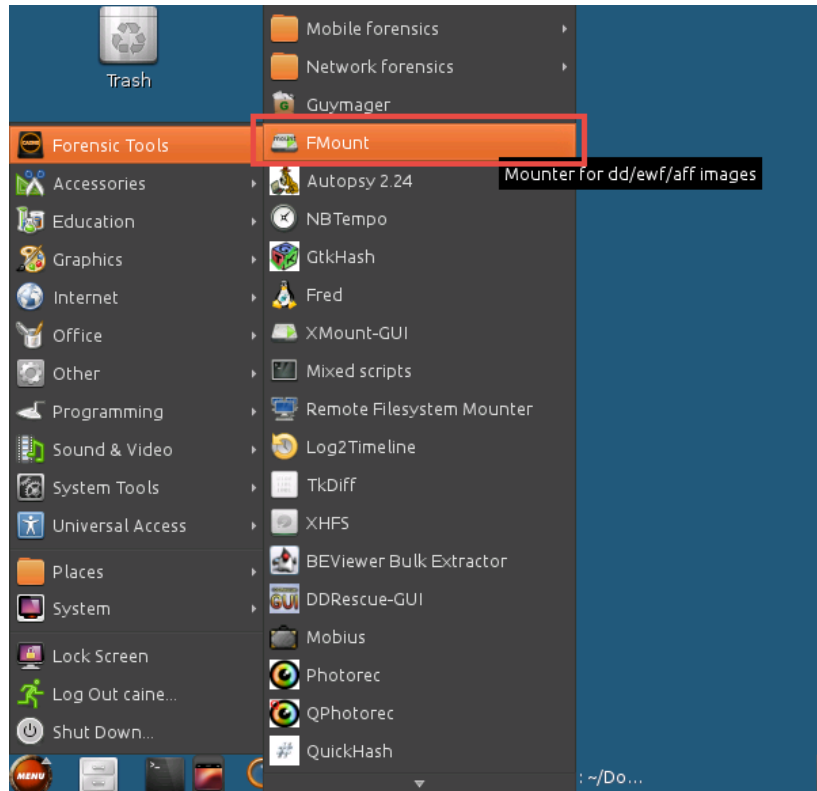
Directory Strings:
  \DEVICE\HARDDISKVOLUME2\WINDOWS
  \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING
  \DEVICE\HARDDISKVOLUME2\WINDOWS\BRANDING\BASEBRD
  \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION
  \DEVICE\HARDDISKVOLUME2\WINDOWS\GLOBALIZATION\SORTING
```

Notice that the *CMD.EXE* file was executed twice and was last run on 2016-01-16.

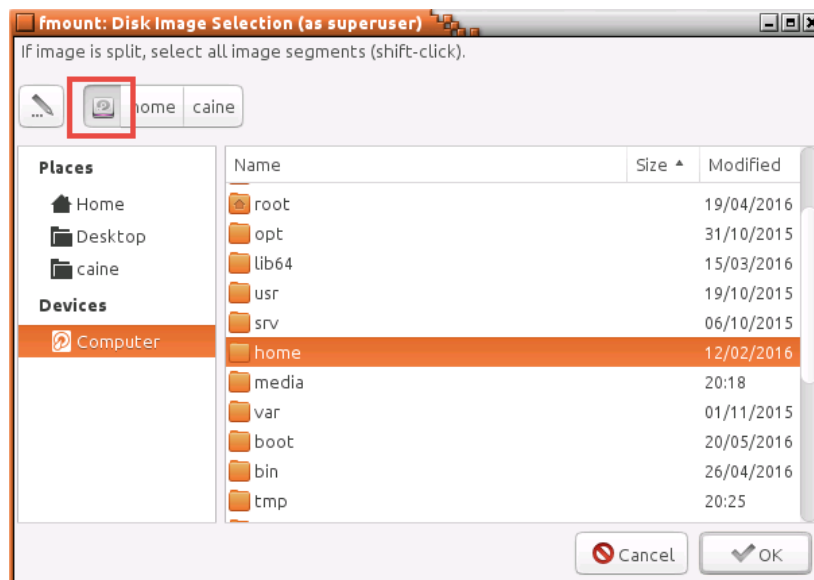
9. Leave the *PC Viewer* open to continue with the next task.

2 Mounting & Exploring Shadow Copies

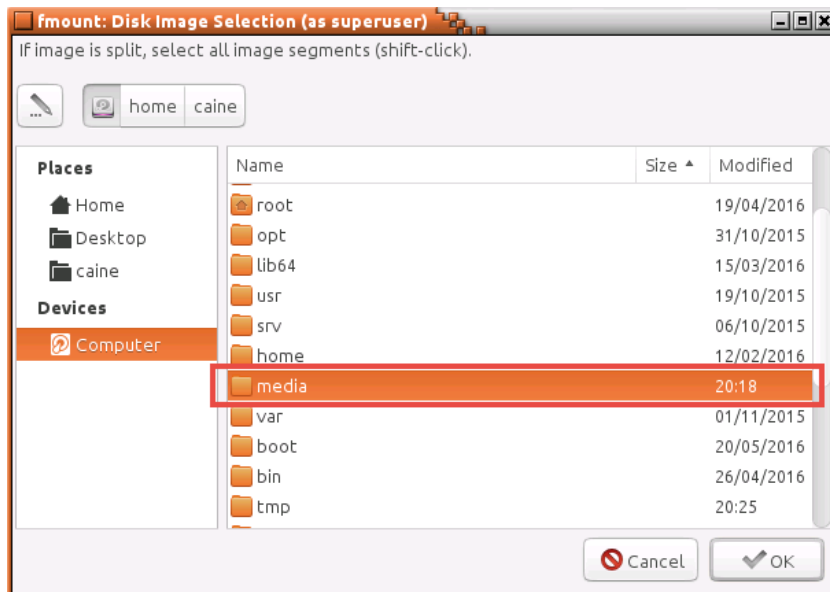
1. Operating systems can be configured to make volume shadow copies, which are snapshots of a volume that can be used to restore previous versions of files. Navigate to **Menu > Forensic Tools > FMount** to use a tool called *FMount* to mount the image and find where they are stored.



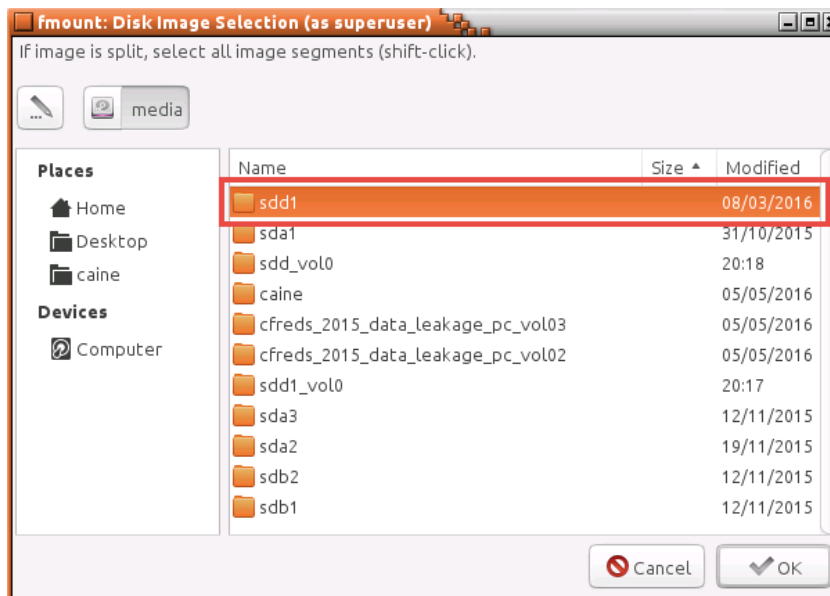
2. In the new *FMount* application window, click on the **HDD** icon.



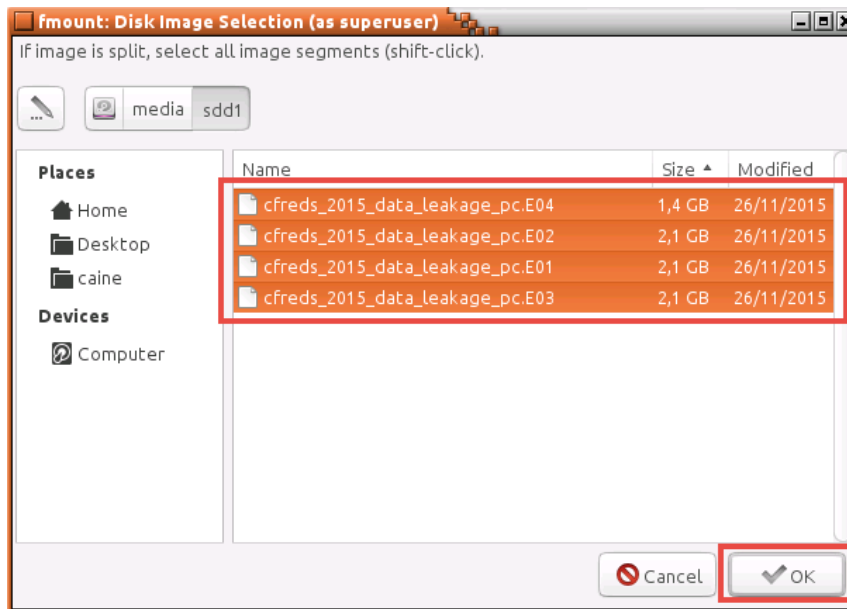
3. Double-click on the **media** folder.



4. Double-click on the **sdd1** folder.



5. Select all four files that begin with “cfreds_2015” and click **OK**.



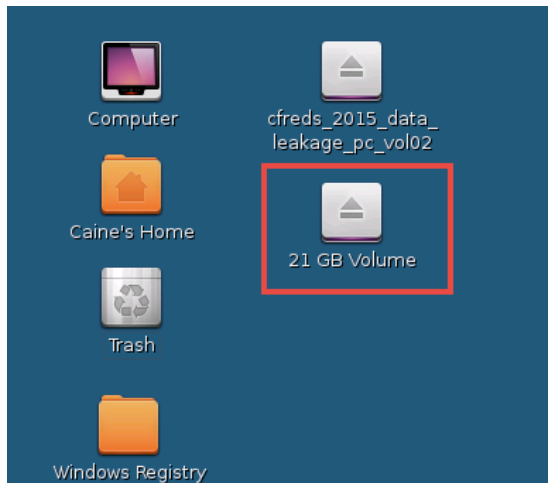
Tip: When attempting to select multiple files, selecting the top file followed by pressing and holding down the **Shift** key, followed by another click, this time on the bottom-most file, will select all files. An alternative would be to press and hold the **CTRL** key followed by clicking each individual file to select them all as well.

6. “Operation succeeded!”, should now be indicated. Click **OK** to close the dialog box.

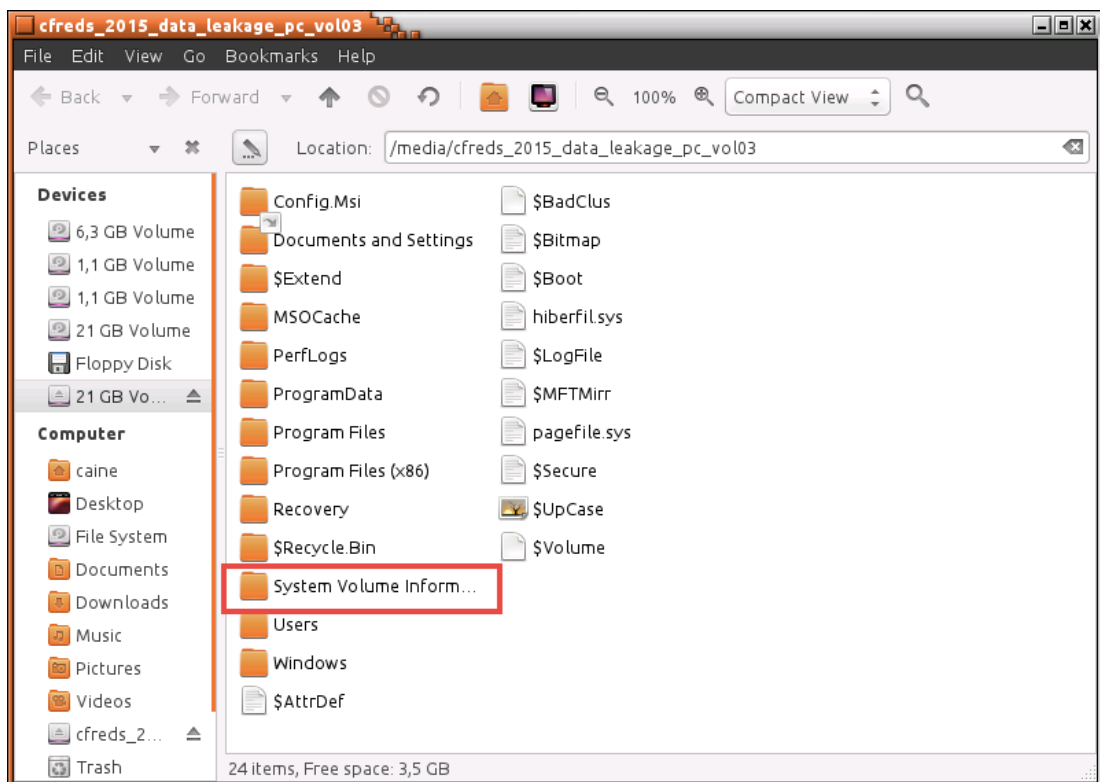




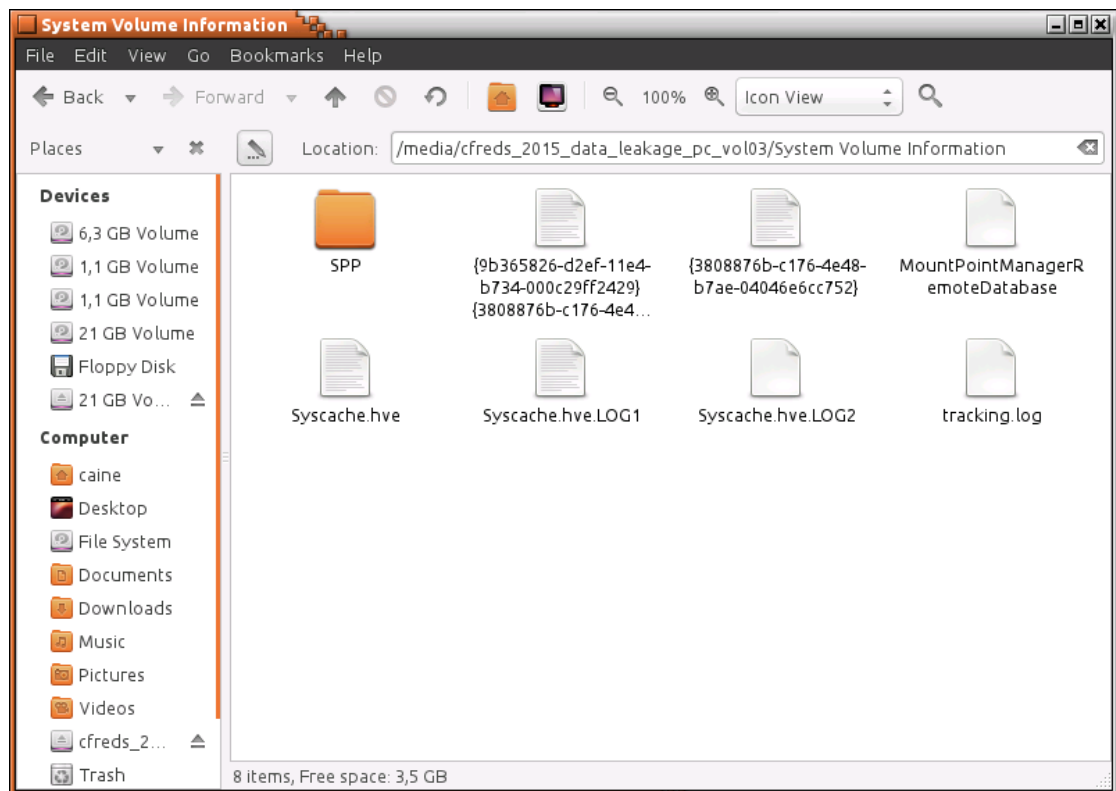
7. Navigate to the **Desktop** and notice two new icons appear. Double-click on the **21 GB Volume** icon.



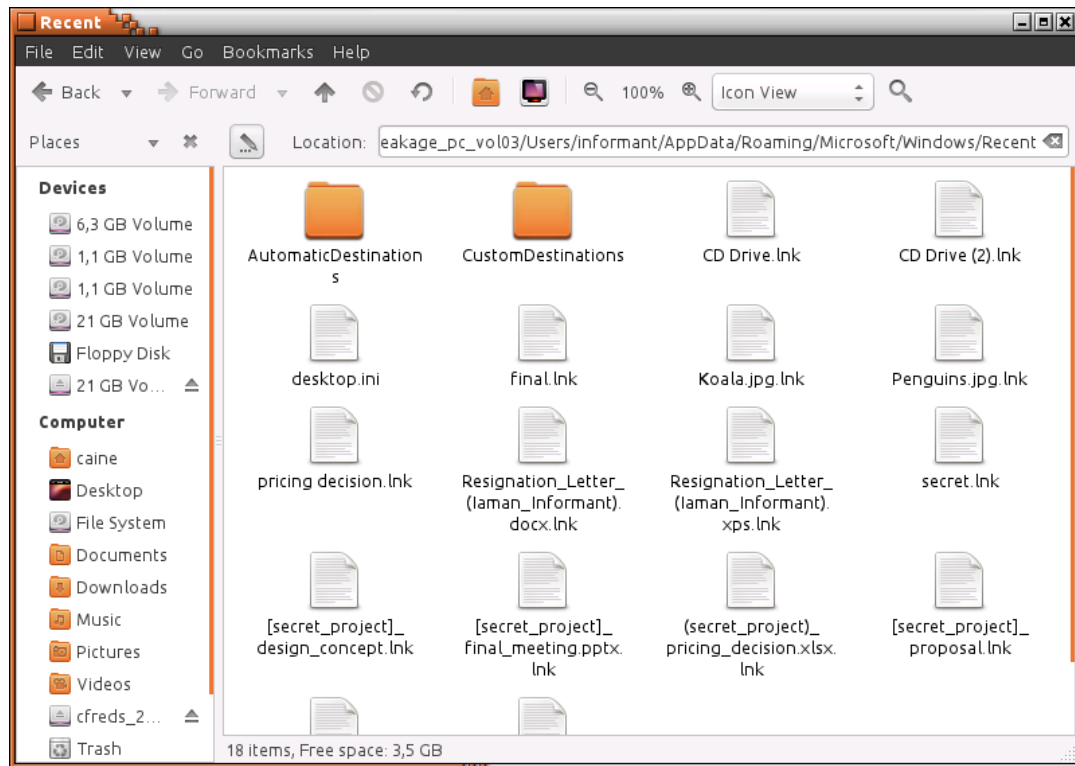
8. This is one of the mounted partitions of the *cfreds* image. Locate and double-click the folder named **System Volume Information**.



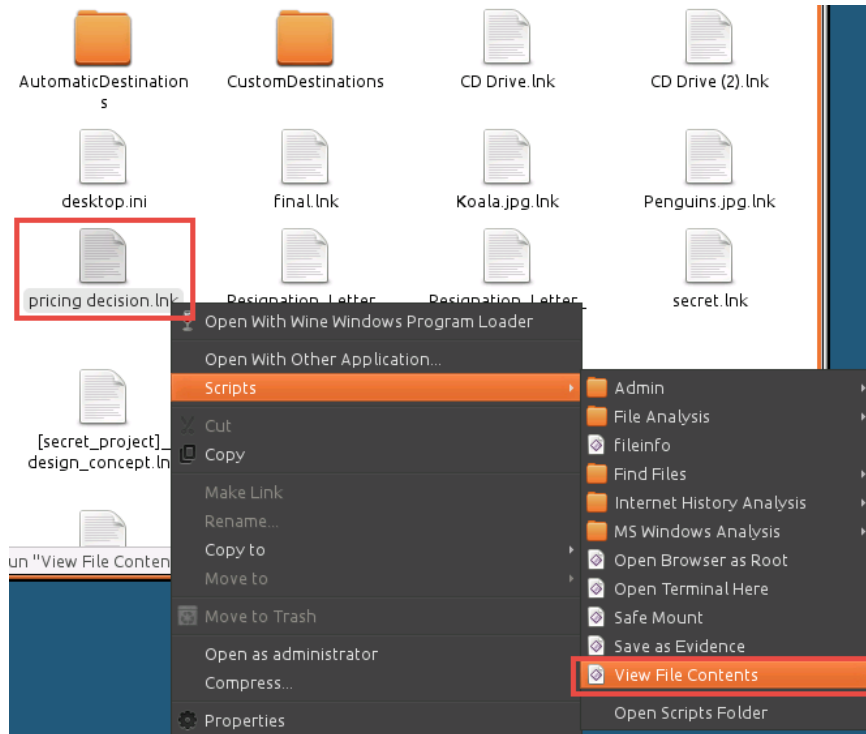
9. Notice the files presented in the *System Volume Information* folder. These are shadow copies that can be exported to a Windows machine and explored for evidence.



10. Using the *File Manager*, navigate to the **/media/cfreds_2015_data_leakage_pc_vol03/Users/informant/AppData/Roaming/Microsoft/Windows/Recent** directory.



11. Another set of useful Windows OS artifact are the Windows shortcuts called “*Ink*” files. They are located in the *Users* home directory under their roaming profile. Notice the *Ink* files in the current directory, right-click on **pricing decision.Ink** and select **Scripts > View File Contents**.



12. Analyze the contents of the file, taking notice of the location and other information concerning the file.

```
File: pricing decision.Ink
FILE CONTENTS: ASCII and Unicode Strings
-----
10.11.11.128
Secret Project Data
pricing decision
\\10.11.11.128\secured_drive\Secret Project Data\pricing decision
\\10.11.11.128\SECURED_DRIVE
Secret Project Data\pricing decision
1SPS0
1SPS:
1SPSSC
\\10.11.11.128\secured_drive
Microsoft Network
Company's Secured Network Drive
SECRET~1
PRICIN~1
\\10.11.11.128\secured_drive\Secret Project Data\pricing decision
1SPS
WmcG
WmcG
```

Remember this is a shortcut to the real file. More information can be brought forth from the *Ink* using a tool called *lifer*.

13. Change focus back to the **terminal** window.
14. Using the terminal, navigate to the **/home/caine/Downloads/lifer-1.0.0** by entering the command below.

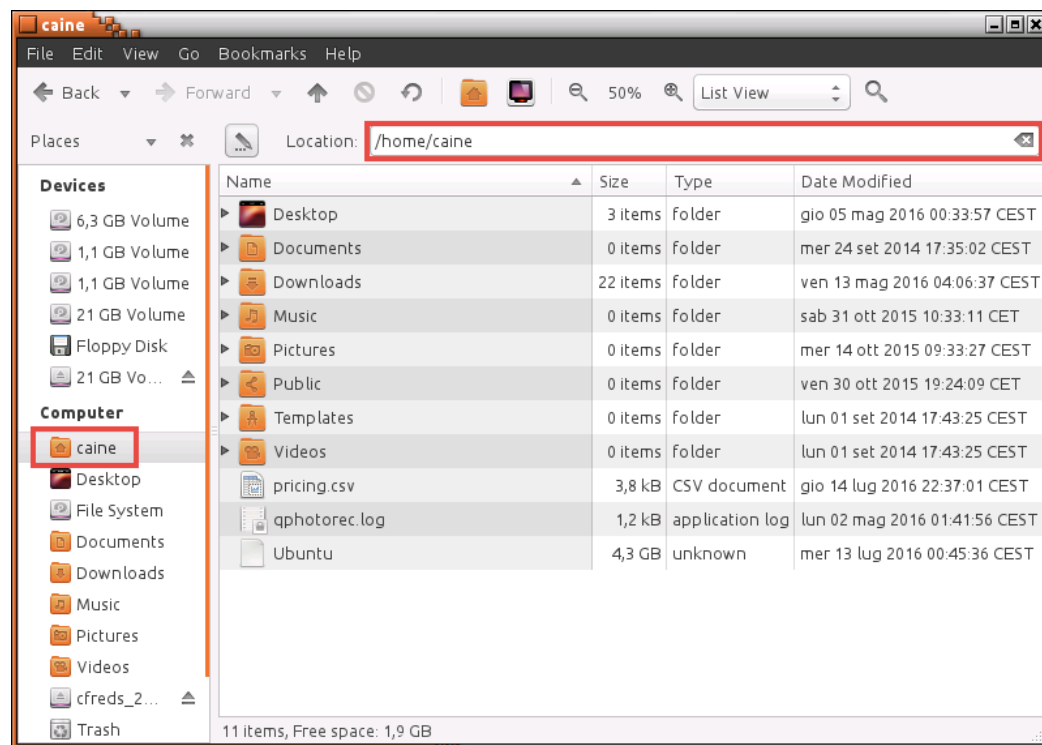
```
cd /home/caine/Downloads/lifer-1.0.0
```

15. Use the *lifer* tool to extract more information on the **pricing decision.lnk** shortcut file. Enter the command below.

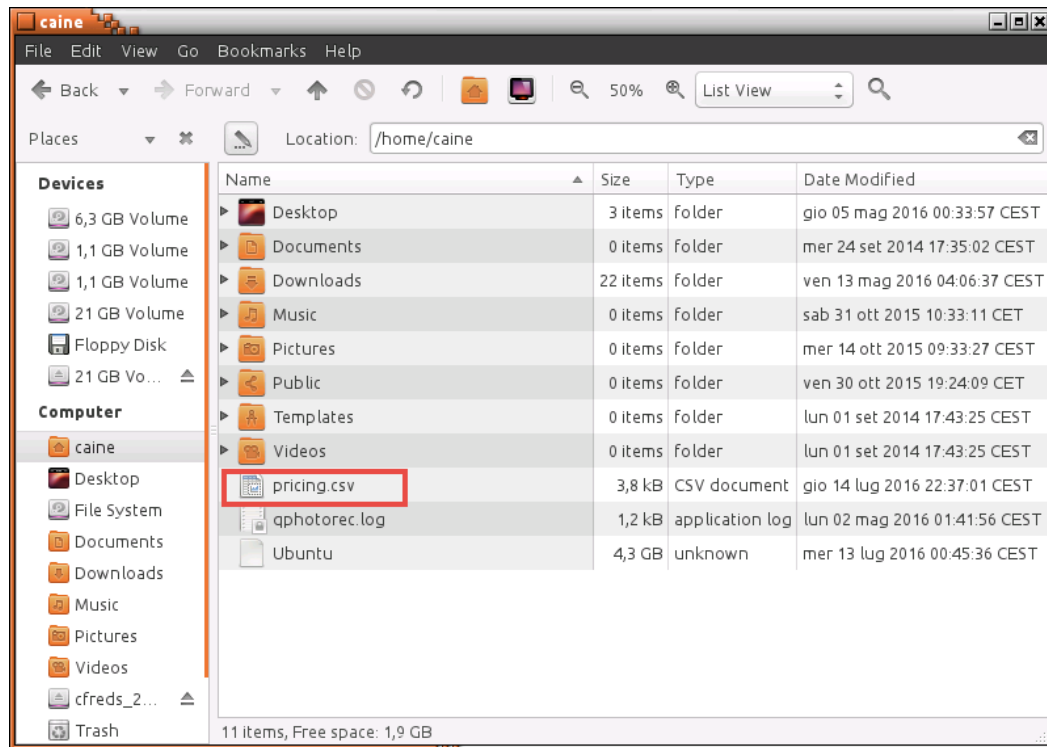
```
lifer -o csv
/media/cfreds_2015_data_leakage_pc_vol03/Users/informant/AppData/Roaming/
Microsoft/Windows/Recent/pricing\ decision.lnk > /home/caine/pricing.csv
```

```
caine@Caine01:~/Downloads/lifer-1.0.0$ lifer -o csv /media/cfreds_2015_data_le
akage_pc_vol03/Users/informant/AppData/Roaming/Microsoft/Windows/Recent/pricin
g\ decision.lnk > /home/caine/pricing.csv
caine@Caine01:~/Downloads/lifer-1.0.0$
```

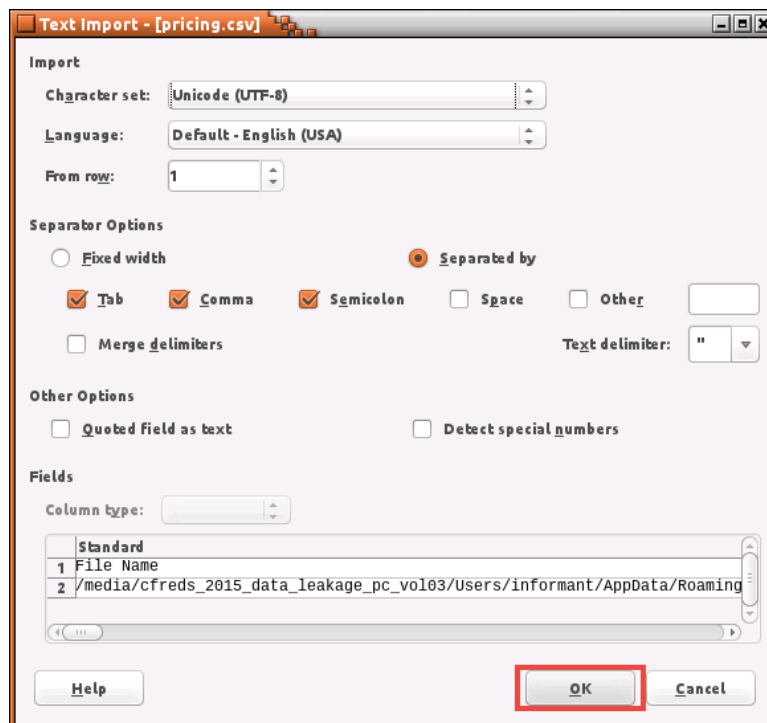
16. Change focus to the **File Manager** application.
17. Using the *File Manager*, navigate to the **/home/caine** directory.



18. Locate and double-click on the **pricing.csv** file in the current directory.

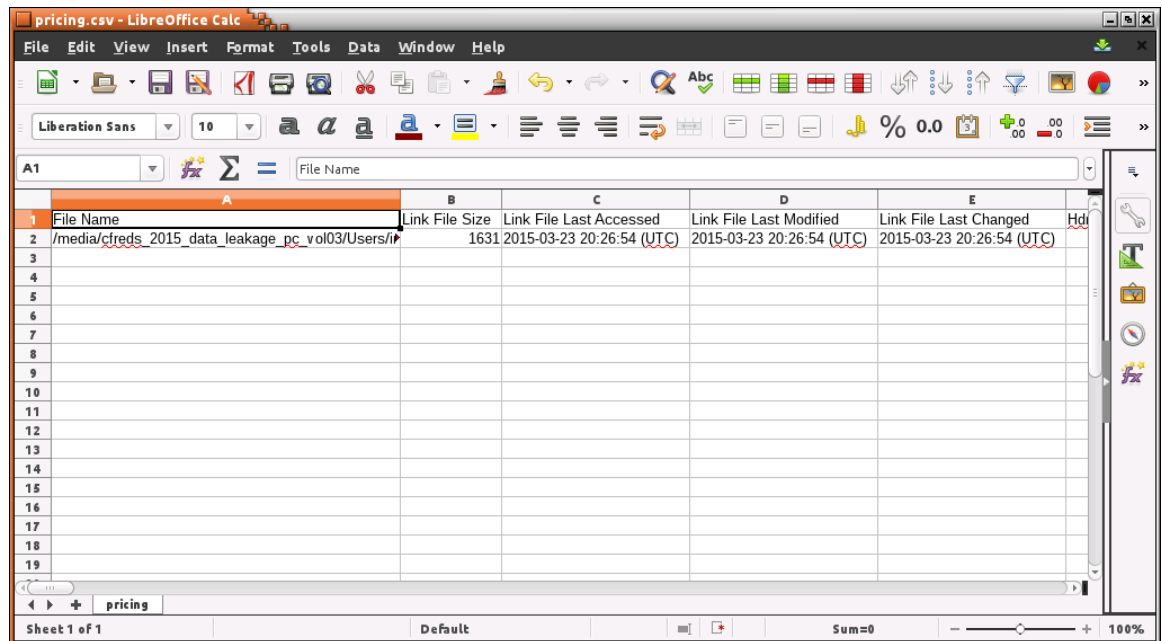


19. Notice the *Test Import* window from LibreOffice. With defaults loaded, click **OK** to continue.





20. Notice the additional information found in the *pricing.csv* file. Identify the File Name path where the *lnk* pointed towards including last modified, last accessed, and last changed (MAC) times.



	A	B	C	D	E
	File Name	Link File Size	Link File Last Accessed	Link File Last Modified	Link File Last Changed
2	/media/cfreds_2015_data_leakage_pc_vol03/Users/irp	1631	2015-03-23 20:26:54 (UTC)	2015-03-23 20:26:54 (UTC)	2015-03-23 20:26:54 (UTC)
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					

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