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

Contents

Introduction

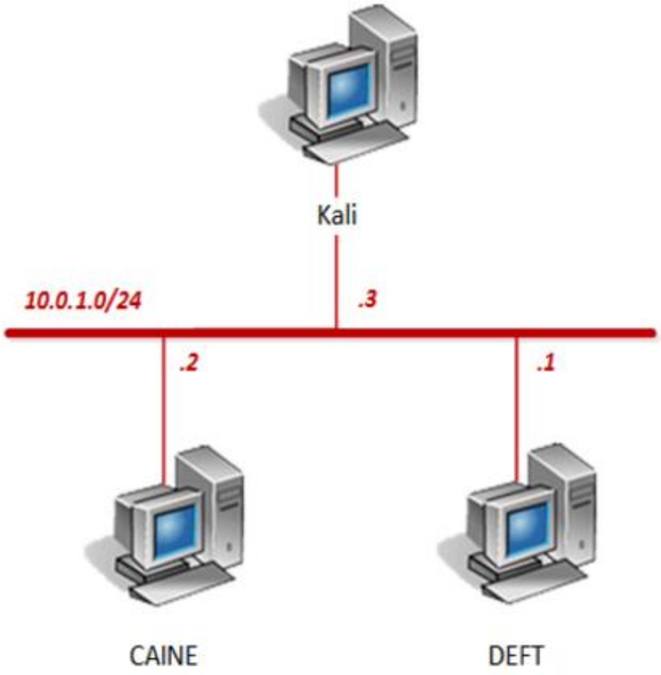
This lab will introduce the concept of performing a forensic examination of a Windows system. The Windows OS artifacts are not in the registry or internet browsing history, instead they will be artifacts left behind by the Windows OS.

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



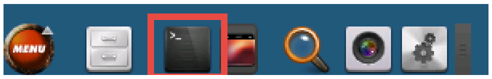
Lab Settings

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

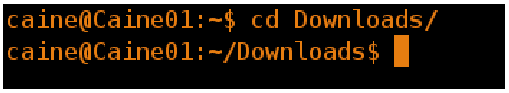
1 Analyzing Prefetch Files

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 he command below followed by pressing the **Enter** key.

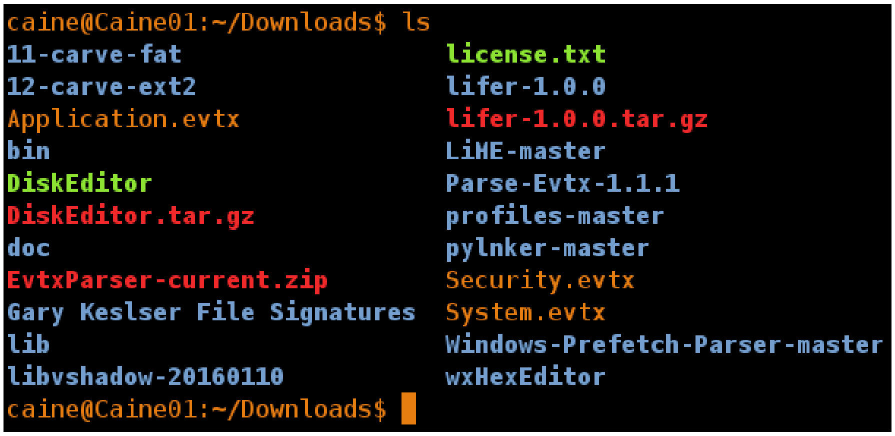
```
cd Downloads/
```



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

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

```
ls
```

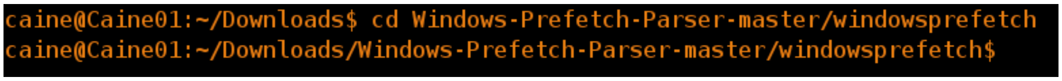


```
caine@Caine01:~/Downloads$ ls
11-carve-fat                  license.txt
12-carve-ext2                 lifer-1.0.0
Application.evtx              lifer-1.0.0.tar.gz
bin                           LiME-master
DiskEditor                    Parse-Evtx-1.1.1
DiskEditor.tar.gz             profiles-master
doc                           pylnker-master
EvtxParser-current.zip        Security.evtx
Gary Keslser 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.

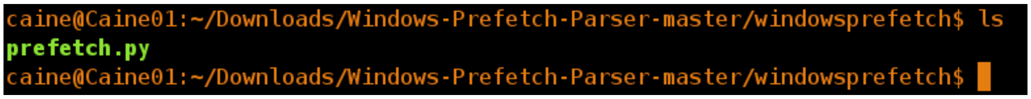
```
cd Windows-Prefetch-Parsers-master/windowsprefetch
```



```
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.

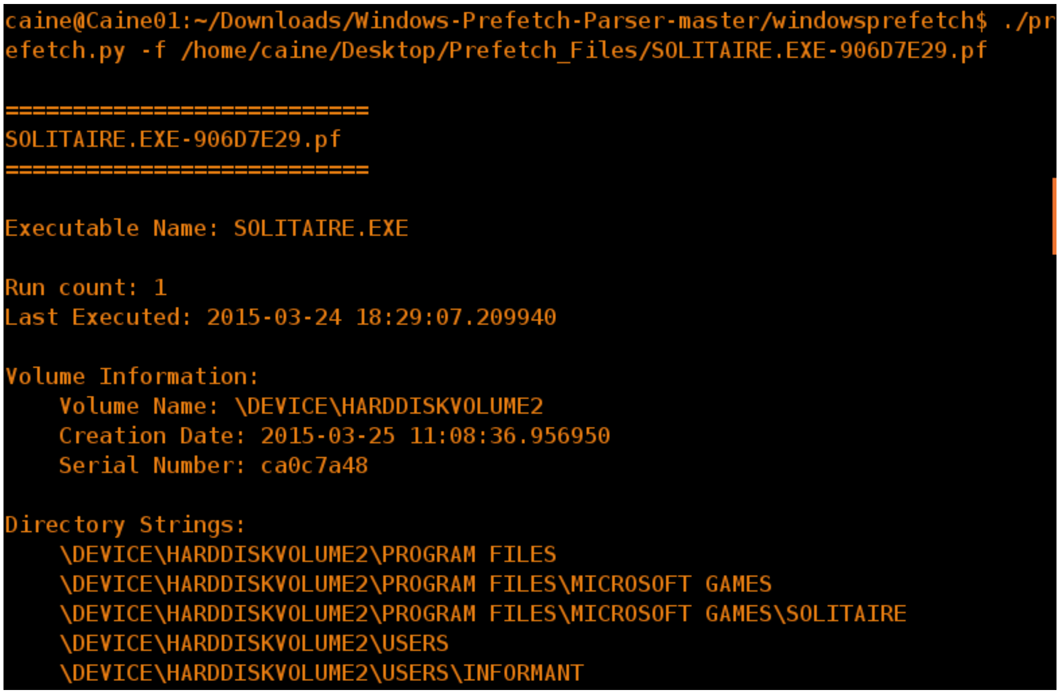
```
ls
```



```
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
```

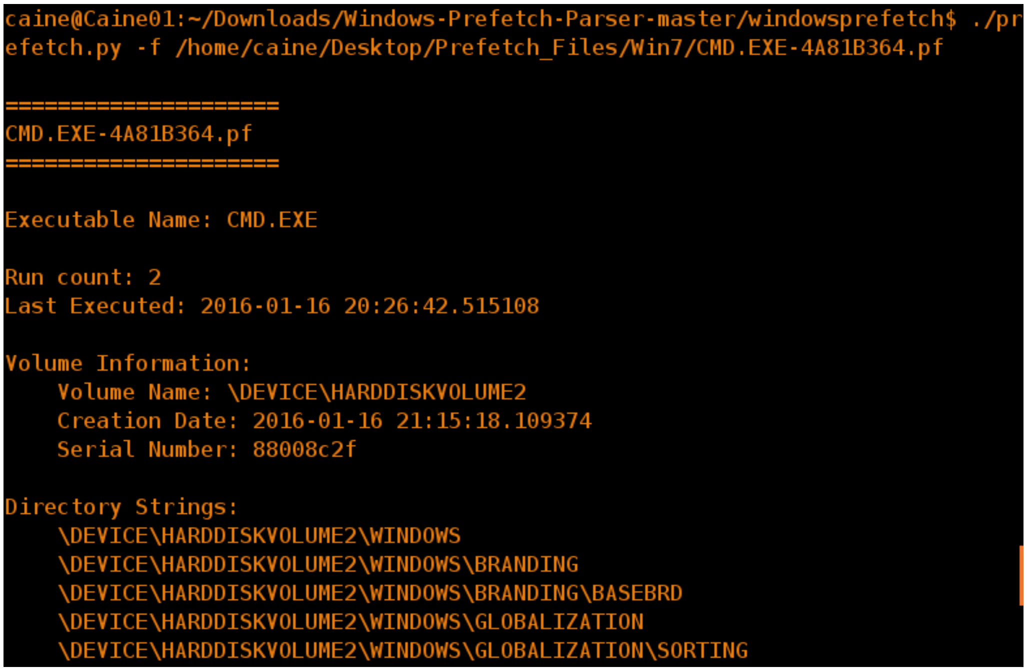


```
caine@Caine01:~/Downloads/Windows-Prefetch-Parser-master/windowsprefetch$ ./pr
efetch.py -f /home/caine/Desktop/Prefetch_Files/SOLITAIRE.EXE-906D7E29.pf

===========================
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
```



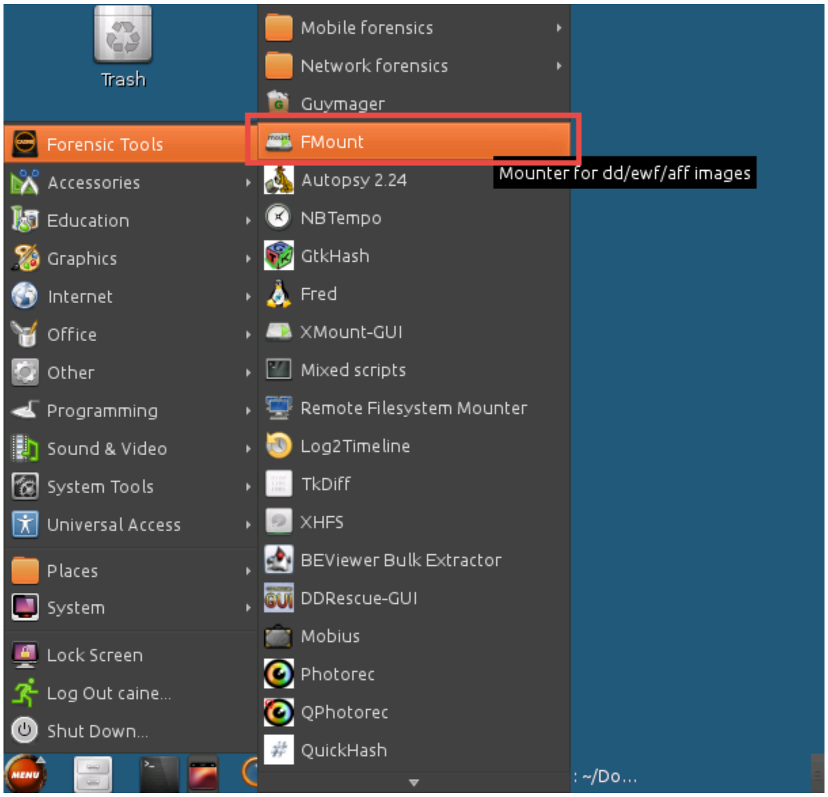
```
caine@Caine01:~/Downloads/Windows-Prefetch-Parser-master/windowsprefetch$ ./pr
efetch.py -f /home/caine/Desktop/Prefetch_Files/Win7/CMD.EXE-4A81B364.pf

=====================
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*.

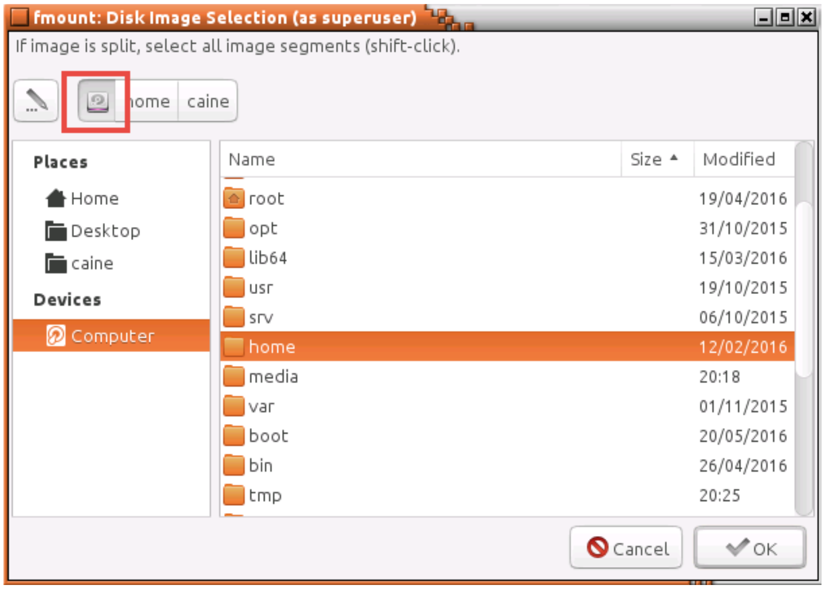
9. Leave the *PC Viewer* open to continue with the next task.

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.



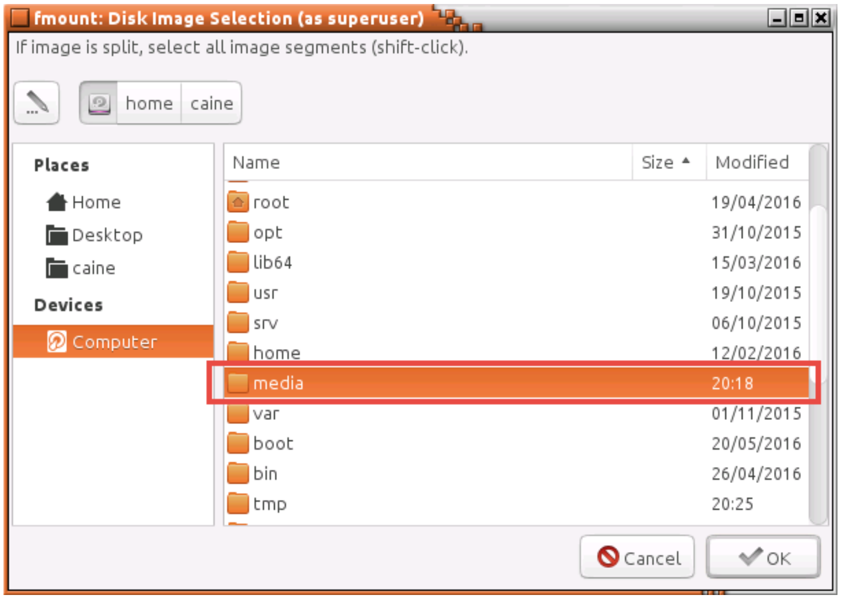
2. In the new *FMount* application window, click on the **HDD** icon.



If image is split, select all image segments (shift-click).

Name	Size	Modified
root		19/04/2016
opt		31/10/2015
lib64		15/03/2016
usr		19/10/2015
srv		06/10/2015
home		12/02/2016
media		20:18
var		01/11/2015
boot		20/05/2016
bin		26/04/2016
tmp		20:25

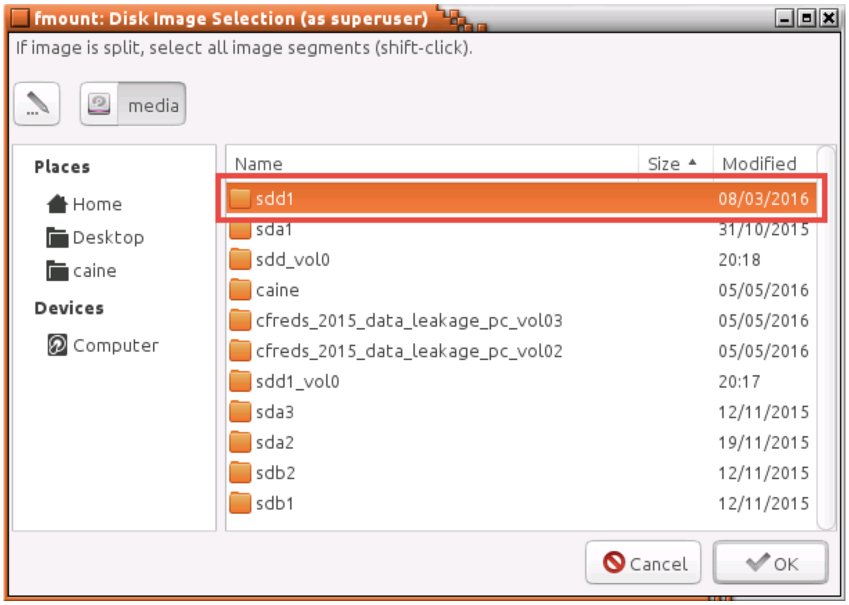
3. Double-click on the **media** folder.



If image is split, select all image segments (shift-click).

Name	Size	Modified
root		19/04/2016
opt		31/10/2015
lib64		15/03/2016
usr		19/10/2015
srv		06/10/2015
home		12/02/2016
media		20:18
var		01/11/2015
boot		20/05/2016
bin		26/04/2016
tmp		20:25

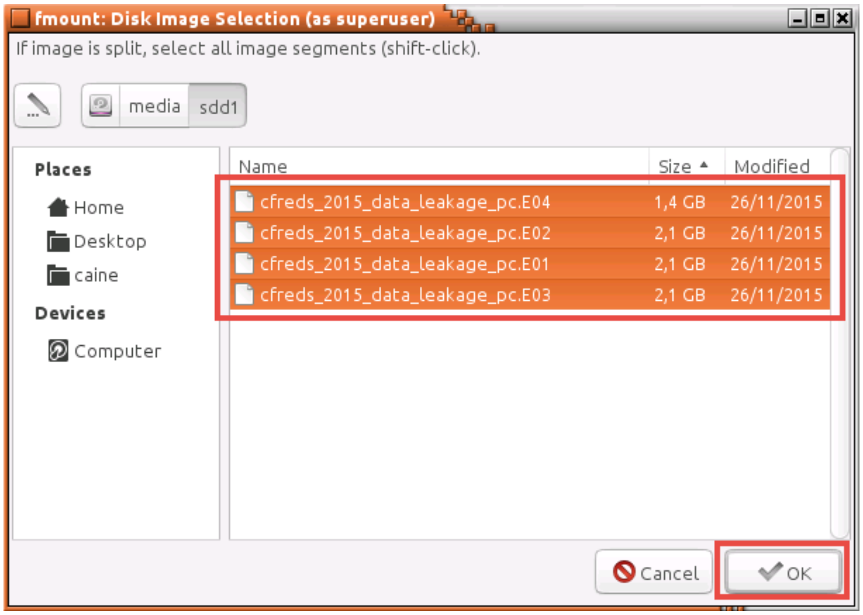
4. Double-click on the **sdd1** folder.



If image is split, select all image segments (shift-click).

Name	Size	Modified
sdd1		08/03/2016
sda1		31/10/2015
sdd_vol0		20:18
caine		05/05/2016
cfreds_2015_data_leakage_pc_vol03		05/05/2016
cfreds_2015_data_leakage_pc_vol02		05/05/2016
sdd1_vol0		20:17
sda3		12/11/2015
sda2		19/11/2015
sdb2		12/11/2015
sdb1		12/11/2015

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



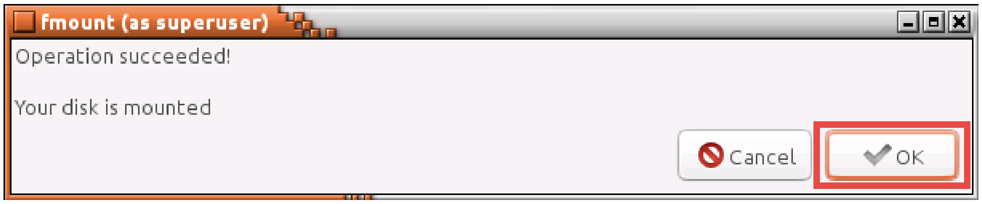
fmount: Disk Image Selection (as superuser)

If image is split, select all image segments (shift-click).

Name	Size	Modified
cfreds_2015_data_leakage_pc.E04	1,4 GB	26/11/2015
cfreds_2015_data_leakage_pc.E02	2,1 GB	26/11/2015
cfreds_2015_data_leakage_pc.E01	2,1 GB	26/11/2015
cfreds_2015_data_leakage_pc.E03	2,1 GB	26/11/2015

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.

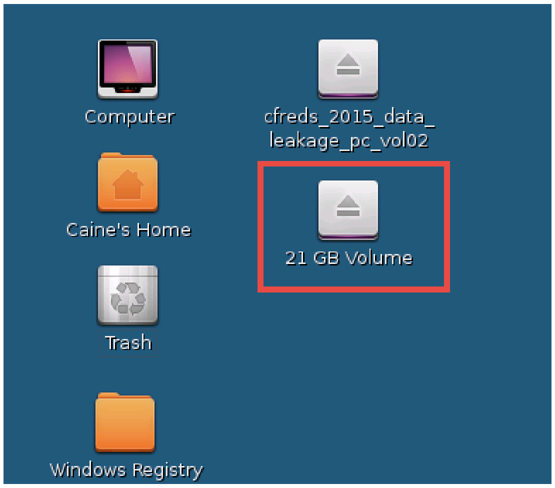


fmount (as superuser)

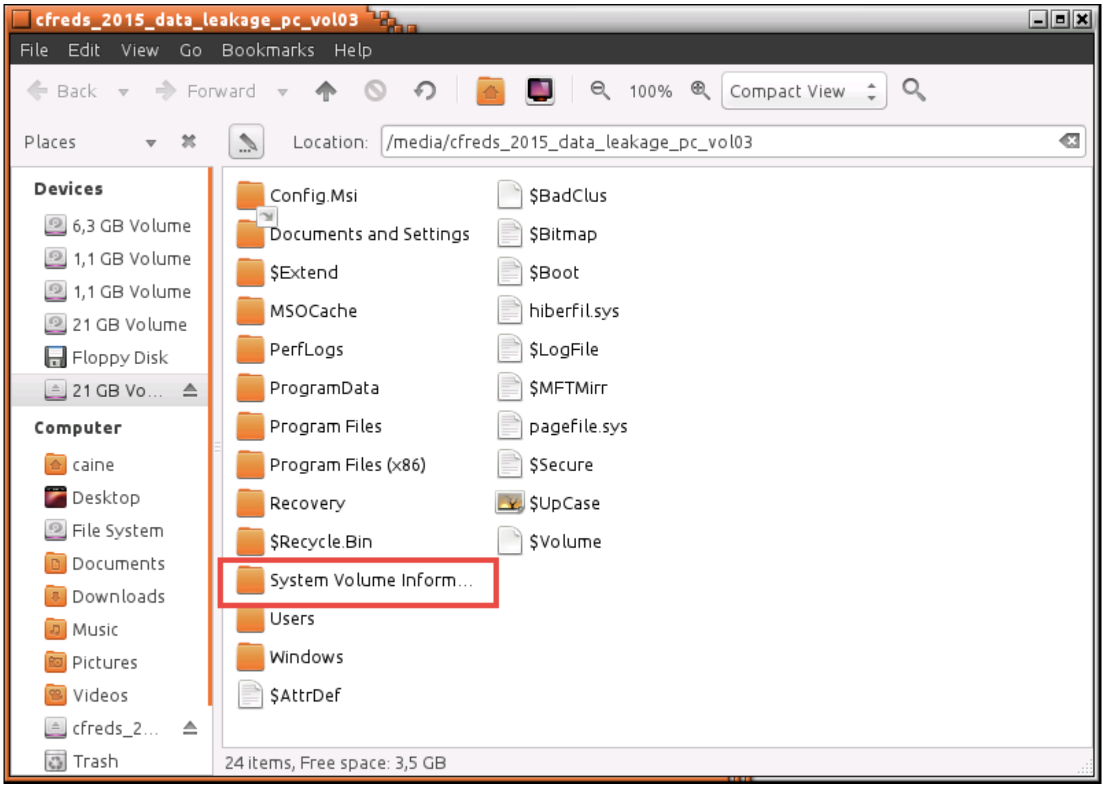
Operation succeeded!

Your disk is mounted

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



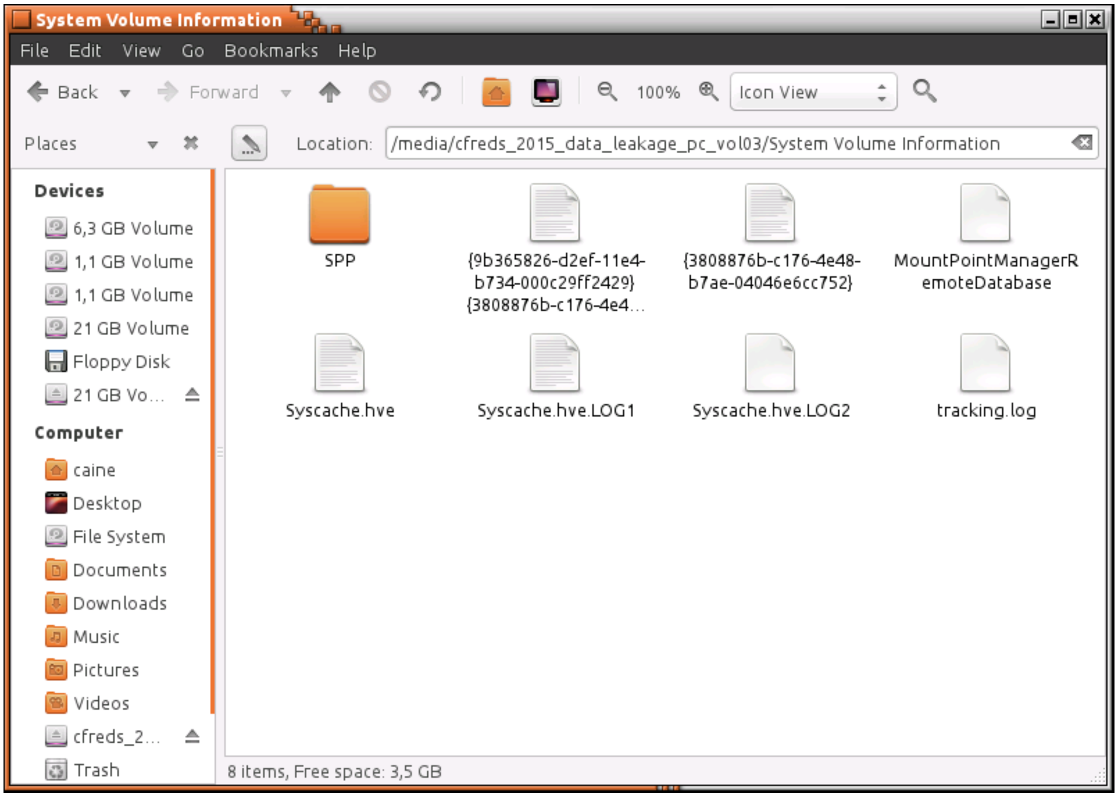
8. This is one of the mounted partitions of the *cfreds* image. Locate and double-click the folder named **System Volume Information**.



Location: /media/cfreds_2015_data_leakage_pc_vol03

24 items, Free space: 3,5 GB

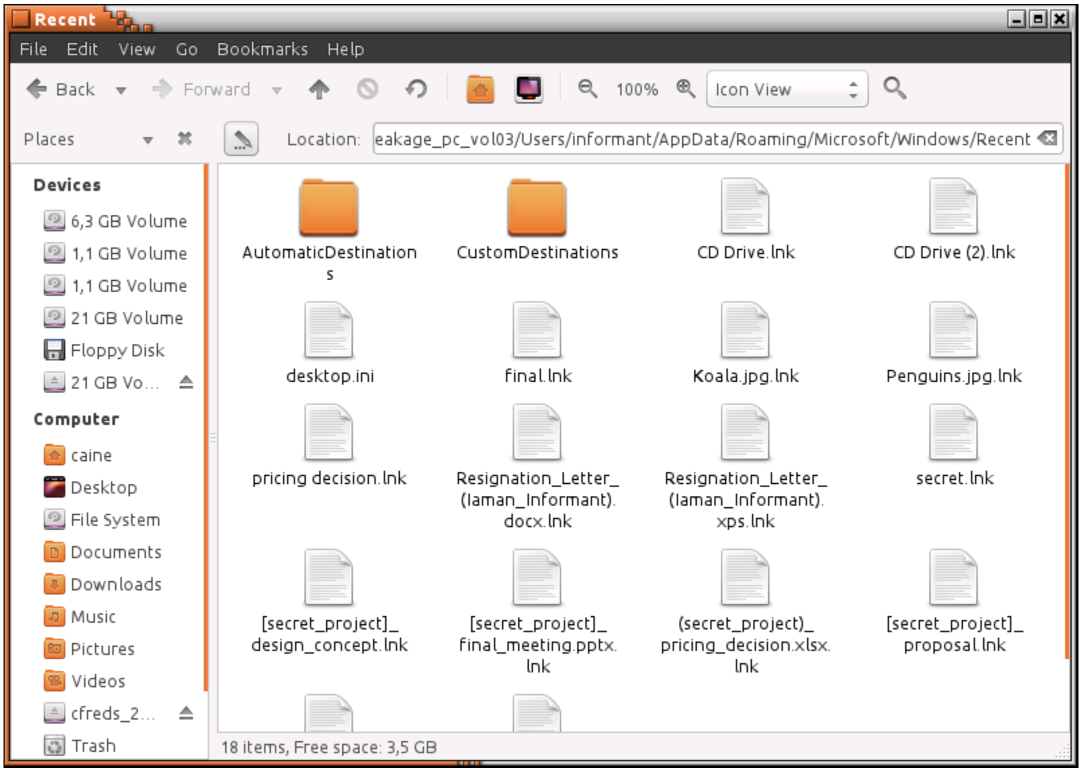
9. Notice the files presented in the *System Volume Information* folder. These are shadow copies that can be exported to a Windows machine and explored for evidence.



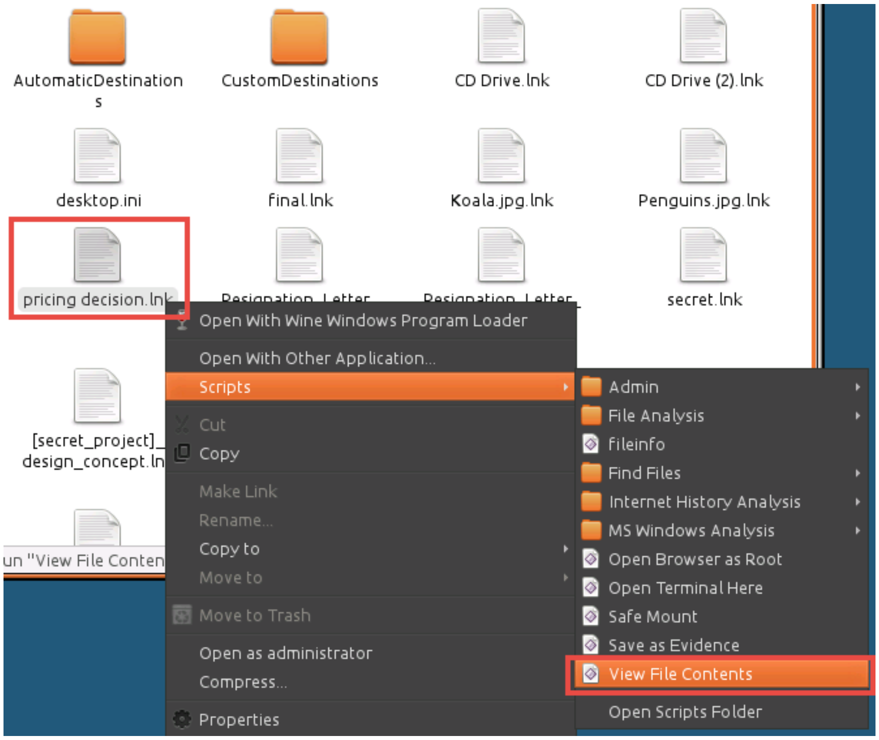
System Volume Information

Location: /media/cfreds_2015_data_leakage_pc_vol03/System Volume Information

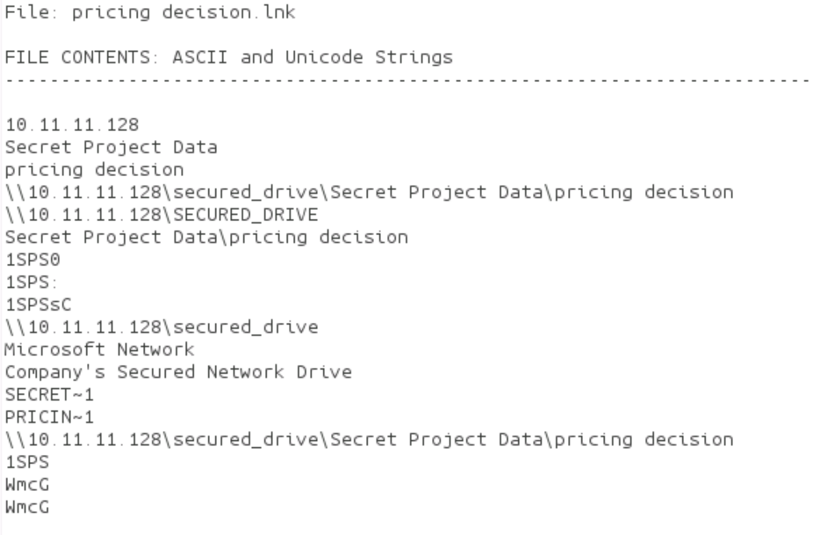
10. Using the *File Manager*, navigate to the **/media/cfreds_2015_data_leakage_pc_vol03/Users/informant/AppData/Roaming/Microsoft/Windows/Recent** directory.


Recent
File Edit View Go Bookmarks Help
Back
Forward
100%
Icon View
Places
Location: eakage_pc_vol03/Users/informant/AppData/Roaming/Microsoft/Windows/Recent
Devices
6,3 GB Volume
1,1 GB Volume
1,1 GB Volume
21 GB Volume
Floppy Disk
21 GB Vo...
Computer
caine
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
cfreds_2...
Trash
AutomaticDestinations
CustomDestinations
CD Drive.lnk
CD Drive (2).lnk
desktop.ini
final.lnk
Koala.jpg.lnk
Penguins.jpg.lnk
pricing decision.lnk
Resignation_Letter_(Iaman_Informant).docx.lnk
Resignation_Letter_(Iaman_Informant).xps.lnk
secret.lnk
[secret_project]_design_concept.lnk
[secret_project]_final_meeting.pptx.lnk
(secret_project)_pricing_decision.xlsx.lnk
[secret_project]_proposal.lnk
18 items, Free space: 3,5 GB

11. Another set of useful Windows OS artifact are the Windows shortcuts called "*lnk"* files. They are located in the *Users* home directory under their roaming profile. Notice the *lnk* files in the current directory, right-click on **pricing decision.lnk** 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.lnk

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
```

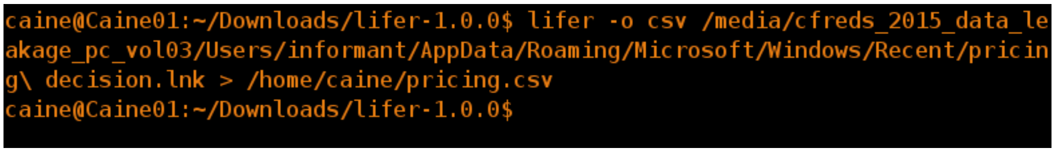
Remember this is a shortcut to the real file. More information can be brought forth from the *lnk* using a tool called *lifer*.

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
```

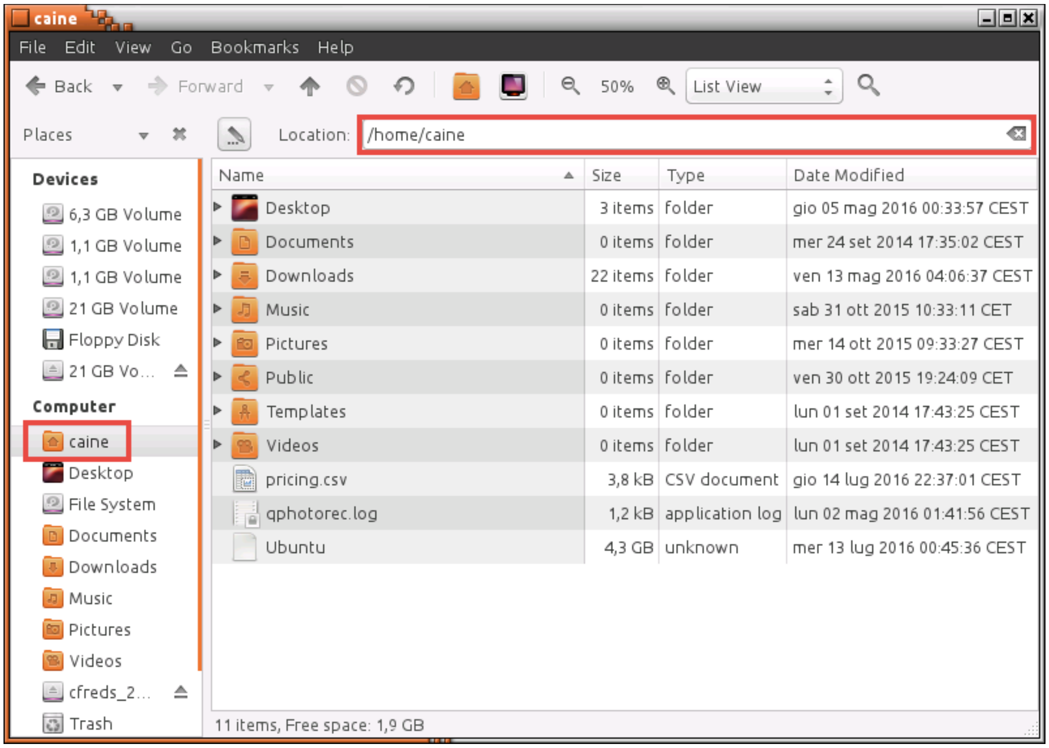
15. Use the *lifer* tool to extract more information on the **pricing decision.lnk** shortcut file. Enter the command below.

```
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.

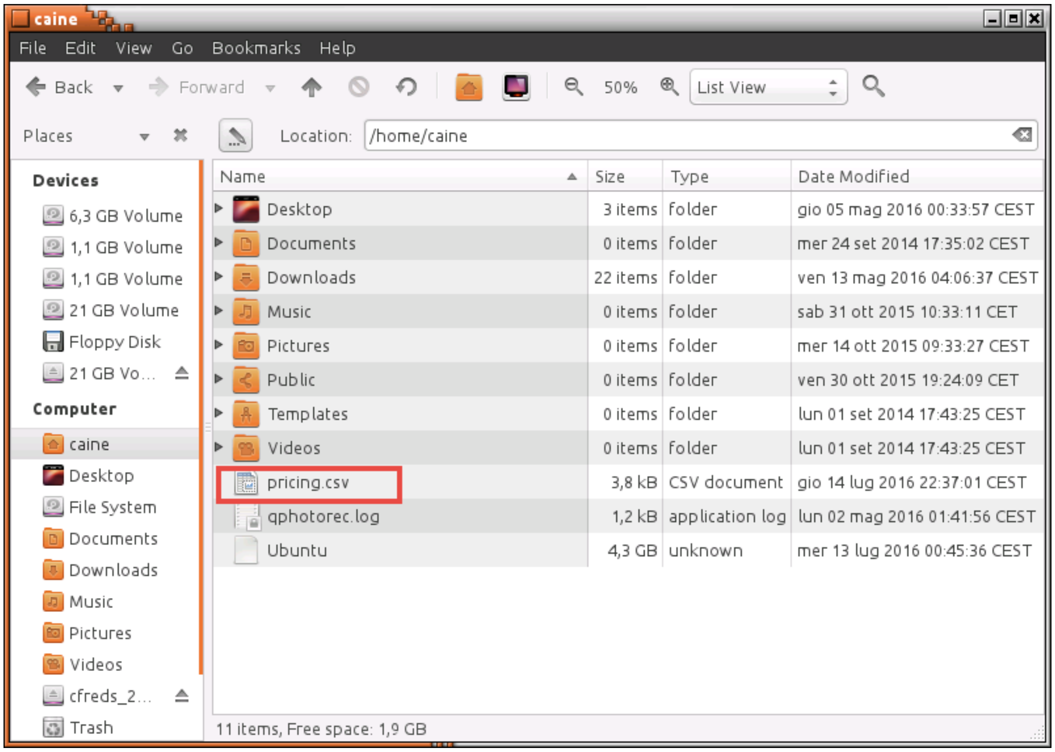


Location: /home/caine

Name	Size	Type	Date Modified
Desktop	3 items	folder	gio 05 mag 2016 00:33:57 CEST
Documents	0 items	folder	mer 24 set 2014 17:35:02 CEST
Downloads	22 items	folder	ven 13 mag 2016 04:06:37 CEST
Music	0 items	folder	sab 31 ott 2015 10:33:11 CET
Pictures	0 items	folder	mer 14 ott 2015 09:33:27 CEST
Public	0 items	folder	ven 30 ott 2015 19:24:09 CET
Templates	0 items	folder	lun 01 set 2014 17:43:25 CEST
Videos	0 items	folder	lun 01 set 2014 17:43:25 CEST
pricing.csv	3,8 kB	CSV document	gio 14 lug 2016 22:37:01 CEST
qphotorec.log	1,2 kB	application log	lun 02 mag 2016 01:41:56 CEST
Ubuntu	4,3 GB	unknown	mer 13 lug 2016 00:45:36 CEST

11 items, Free space: 1,9 GB

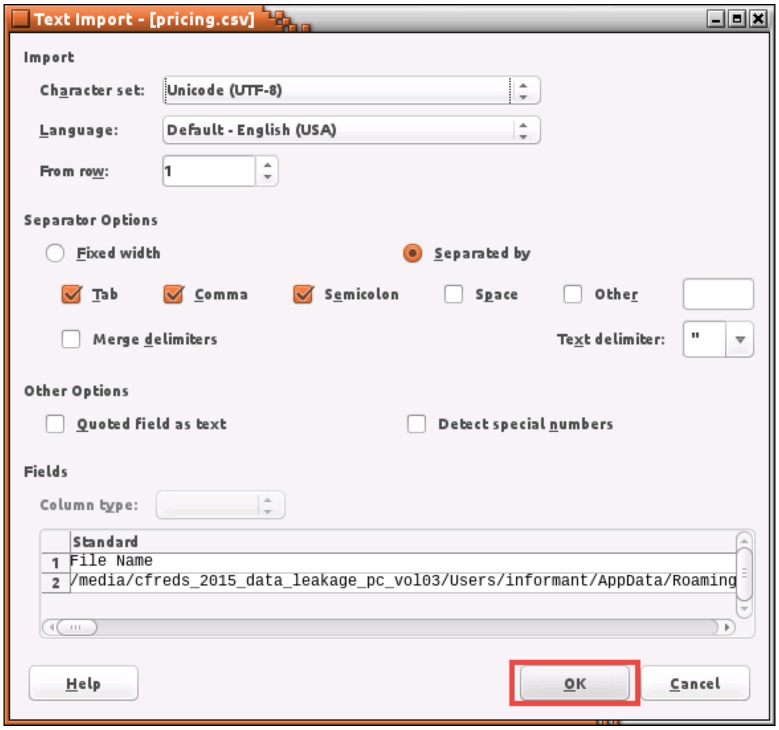
18. Locate and double-click on the **pricing.csv** file in the current directory.



Name	Size	Type	Date Modified
Desktop	3 items	folder	gio 05 mag 2016 00:33:57 CEST
Documents	0 items	folder	mer 24 set 2014 17:35:02 CEST
Downloads	22 items	folder	ven 13 mag 2016 04:06:37 CEST
Music	0 items	folder	sab 31 ott 2015 10:33:11 CET
Pictures	0 items	folder	mer 14 ott 2015 09:33:27 CEST
Public	0 items	folder	ven 30 ott 2015 19:24:09 CET
Templates	0 items	folder	lun 01 set 2014 17:43:25 CEST
Videos	0 items	folder	lun 01 set 2014 17:43:25 CEST
pricing.csv	3,8 kB	CSV document	gio 14 lug 2016 22:37:01 CEST
qphotorec.log	1,2 kB	application log	lun 02 mag 2016 01:41:56 CEST
Ubuntu	4,3 GB	unknown	mer 13 lug 2016 00:45:36 CEST

11 items, Free space: 1,9 GB

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



Import

Character set: Unicode (UTF-8)

Language: Default - English (USA)

From row: 1

Separator Options

○ Fixed width ● Separated by

☑ Tab ☑ Comma ☑ Semicolon □ Space □ Other

□ Merge delimiters Text delimiter: "

Other Options

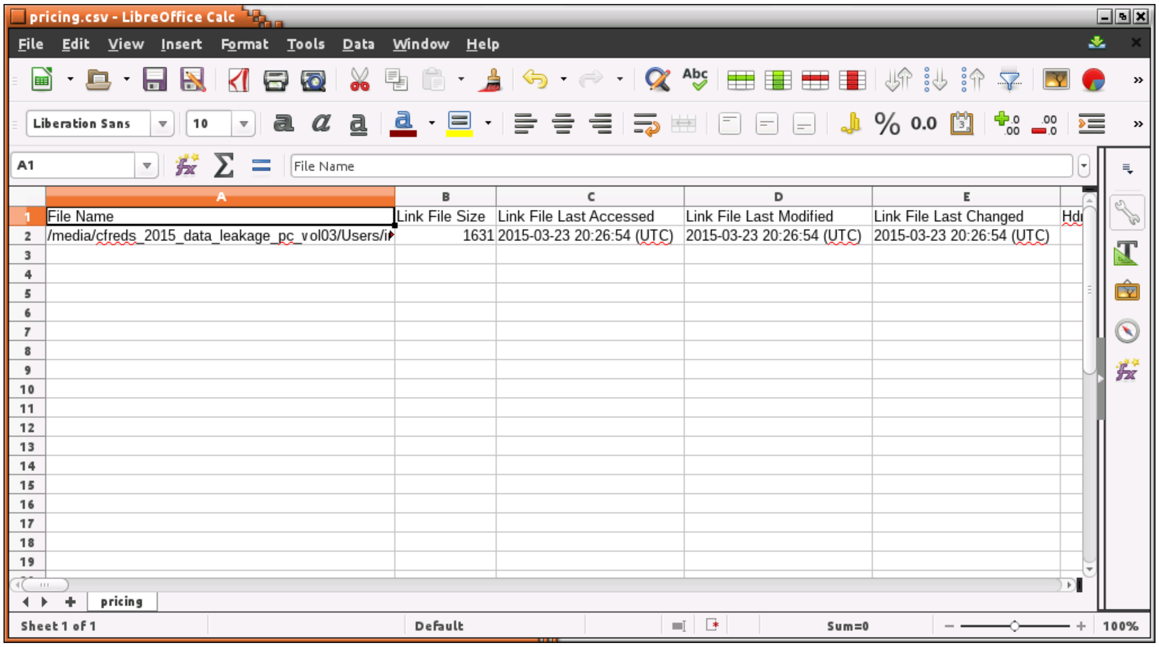
□ Quoted field as text □ Detect special numbers

Fields

Column type:

```
  Standard
1 File Name
2 /media/cfreds_2015_data_leakage_pc_vol03/Users/informant/AppData/Roaming
```

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.



pricing.csv - LibreOffice Calc
File Edit View Insert Format Tools Data Window Help
Liberation Sans
10
A1
File Name
pricing
Sheet 1 of 1
Default
Sum=0
100%

	A	B	C	D	E	
1	File Name	Link File Size	Link File Last Accessed	Link File Last Modified	Link File Last Changed	Hdı
2	/media/cfreds_2015_data_leakage_pc_vol03/Users/i	1631	2015-03-23 20:26:54 (UTC)	2015-03-23 20:26:54 (UTC)	2015-03-23 20:26:54 (UTC)	

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