Registry Export - Encase® Forensic

The following section can be used as a guide to assist in exporting all the hive files which comprise the Windows Registry using Encase® Forensic. In this example, Encase® Forensic is being used to interpret a forensic image of a Windows 7 machine. The following files exist on a Windows 7 machine:

Filename	Occurrences on a typical machine
NTUSER.DAT	One per user account
USRCLASS.DAT	One per user account
SECURITY	One per machine plus backup
SYSTEM	One per machine plus backup
SOFTWARE	One per machine plus backup
SAM	One per machine plus backup
USERDIFF	May or may not exist
DEFAULT	One per machine plus backup
COMPONENTS	One per machine plus backup – Vista/7 only
BCD-TEMPLATE	One per machine plus backup – Vista/7 only
INDEX.DAT **	Many per user based on usage

** INDEX.DAT files store IE cache information and are not part of the Windows Registry. However, if included during a Windows Registry export, Registry Browser can view the IE cache files as well as the registry files, saving time.

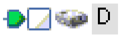
The above list of files should be kept handy when doing an export even after successfully exporting the registry many times.

This guide will work with earlier versions of Windows including Windows NT, Windows 2k, Windows XP and Windows Vista. USRCLASS.DAT first appeared on Windows XP systems, whilst COMPONENTS and BCD-TEMPLATE first appeared on Windows Vista systems. Using the above list will ensure that all necessary files are included in the export.

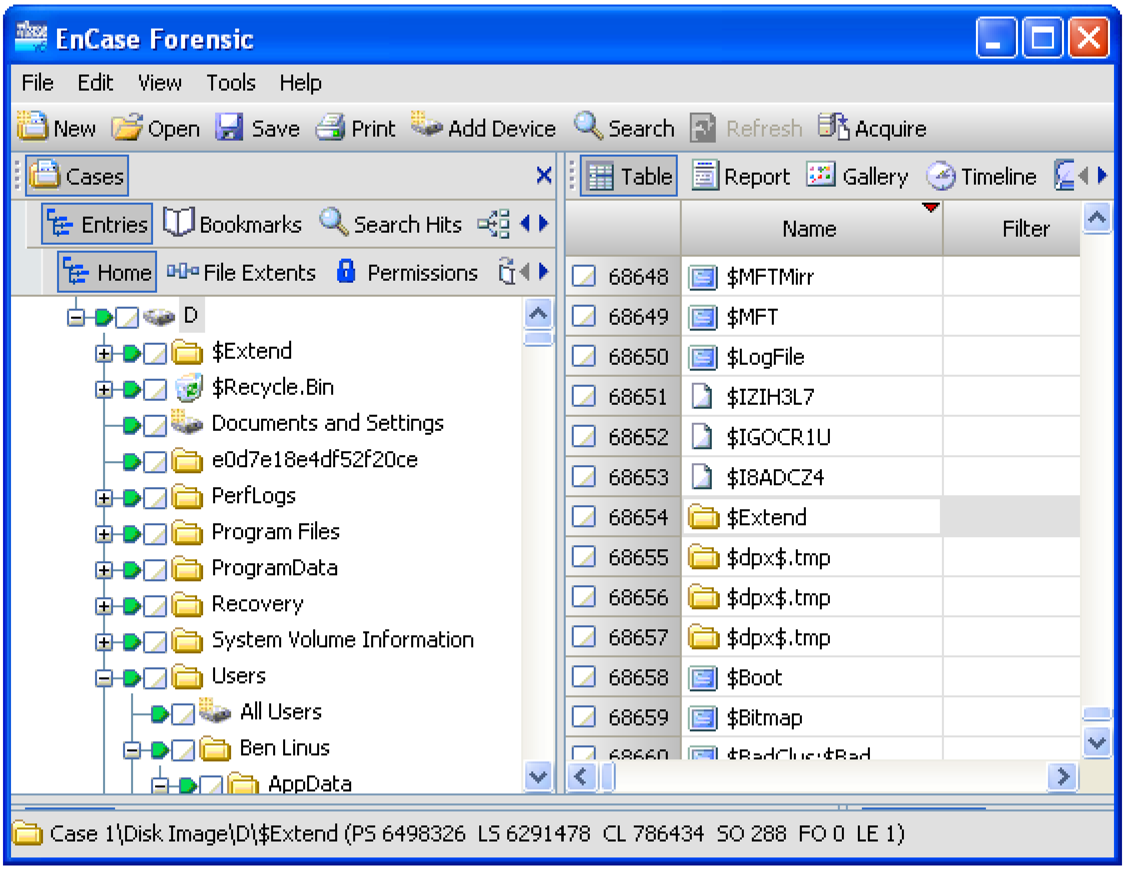
1. Use Encase® Forensic to open your E01, raw image or physical device.

2. Locate the volume which contains the Windows Operating system. On modern machines it will be the second logical volume and will be described by Encase® Forensic as “D”.

3. If this is not a freshly opened case, ensure that there are no files currently tagged as they will be included in the export as well.

4. Click the home plate icon next to the volume containing the operating system and the home plate will become green eg. 

5. All descendant items below the green home plate will also appear green indicating that the table view on the right will contain all the files on the entire “D” volume as pictured below.


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Acquire
Cases
Entries Bookmarks Search Hits
Home File Extents Permissions
Table Report Gallery Timeline
D
$Extend
$Recycle.Bin
Documents and Settings
e0d7e18e4df52f20ce
PerfLogs
Program Files
ProgramData
Recovery
System Volume Information
Users
All Users
Ben Linus
AppData

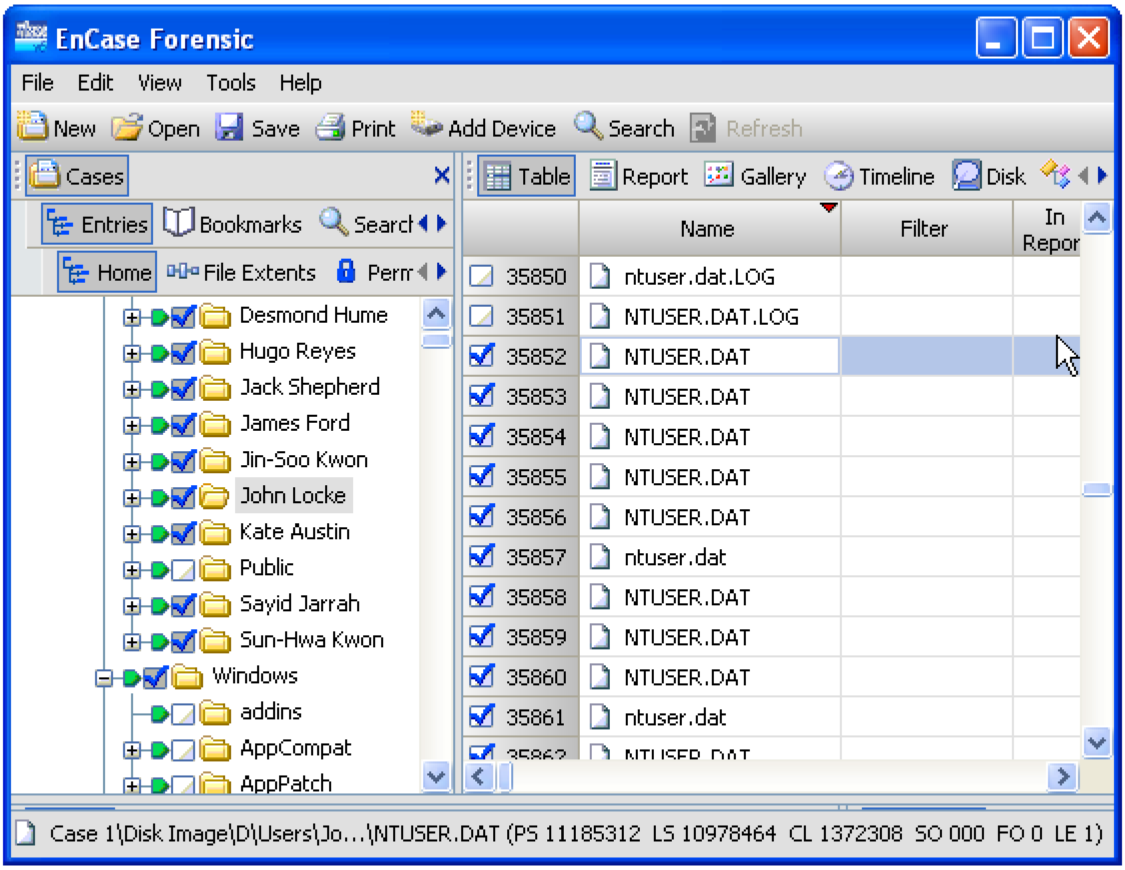
	Name	Filter
68648	$MFTMirr	
68649	$MFT	
68650	$LogFile	
68651	$IZIH3L7	
68652	$IGOCR1U	
68653	$I8ADCZ4	
68654	$Extend	
68655	dpx.tmp	
68656	dpx.tmp	
68657	dpx.tmp	
68658	$Boot	
68659	$Bitmap	
68660	$BadClus:$Bad	

Case 1\Disk Image\D\$Extend (PS 6498326 LS 6291478 CL 786434 SO 288 FO 0 LE 1)

6. Ensure the table view on the right is being sorted by file name. The example above indicates this with the red arrow in the top right corner of the “Name” heading in the table view.

7. Start with the first file on the list, “NTUSER.DAT” and locate it in the table view. There are two ways to do this. The hard way is to use the scroll bar to navigate down alphabetically until you find NTUSER.DAT. The easy way is to ensure the focus is on the table view by selecting the first row in the table and then using the keyboard to type “NTUSER.DAT” without quotes. This technique will jump straight down to the correct location.

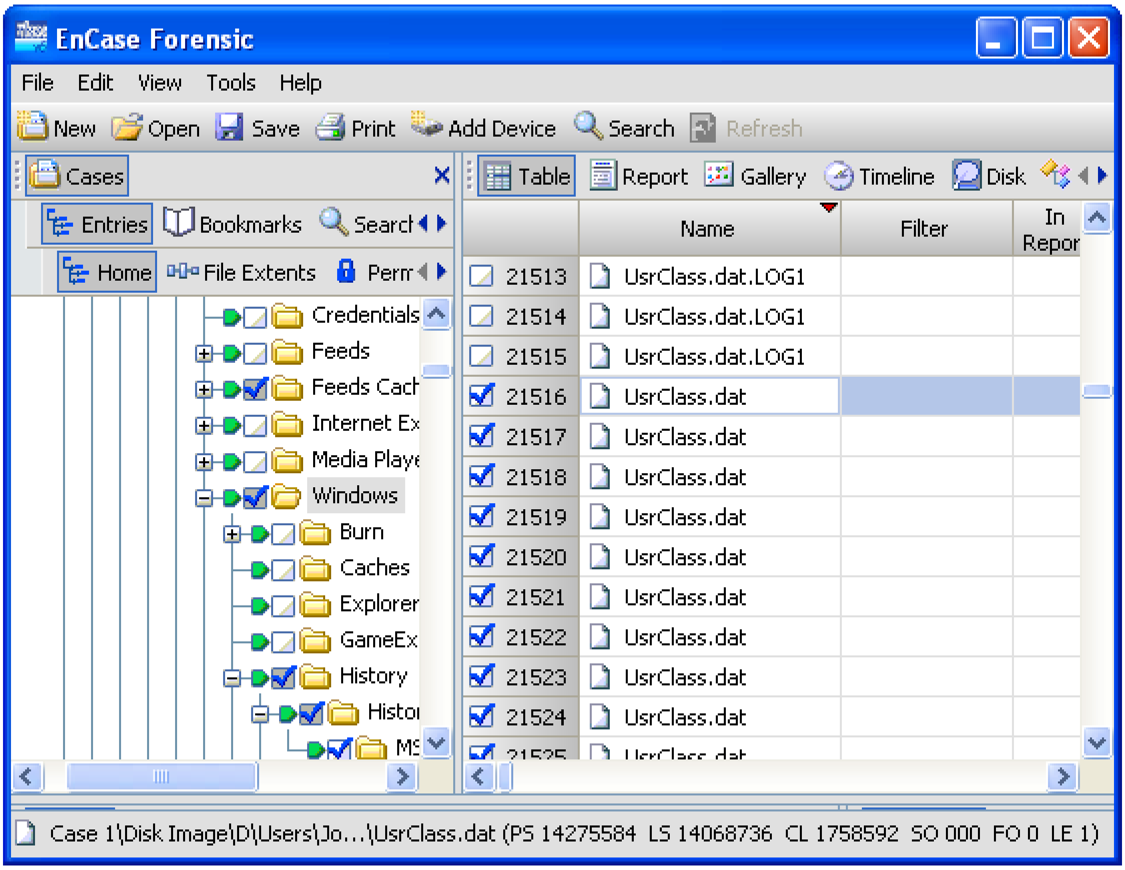
8. Locate all the NTUSER.DAT files and tag them with a blue tick as illustrated below.



		Name	Filter	In Repor
☐	35850	ntuser.dat.LOG		
☐	35851	NTUSER.DAT.LOG		
☑	35852	NTUSER.DAT		
☑	35853	NTUSER.DAT		
☑	35854	NTUSER.DAT		
☑	35855	NTUSER.DAT		
☑	35856	NTUSER.DAT		
☑	35857	ntuser.dat		
☑	35858	NTUSER.DAT		
☑	35859	NTUSER.DAT		
☑	35860	NTUSER.DAT		
☑	35861	ntuser.dat		
☑	35862	NTUSER.DAT		

Case 1\Disk Image\D\Users\Jo...\NTUSER.DAT (PS 11185312 LS 10978464 CL 1372308 SO 000 FO 0 LE 1)

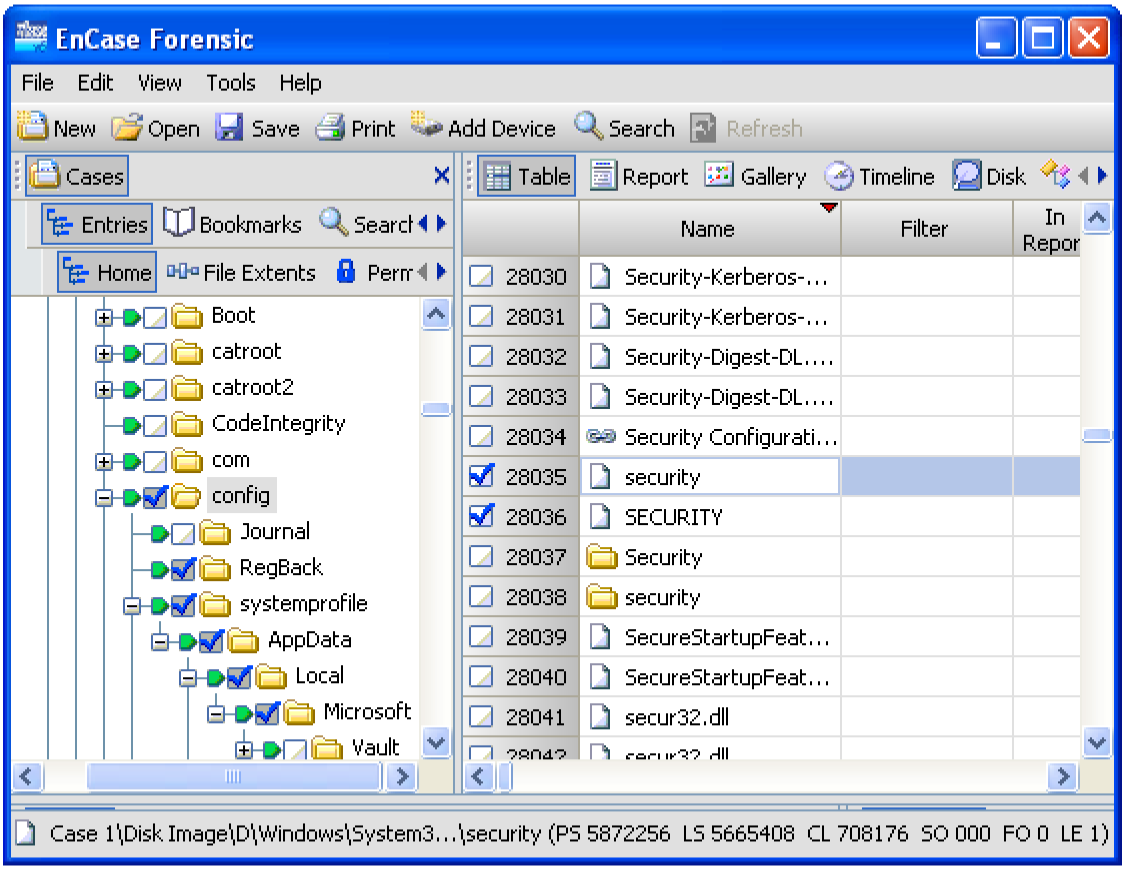
9. Next, repeat the above step with the next file “USRCLASS.DAT” as shown.



		Name	Filter	In Repor
☐	21513	UsrClass.dat.LOG1		
☐	21514	UsrClass.dat.LOG1		
☐	21515	UsrClass.dat.LOG1		
☑	21516	UsrClass.dat		
☑	21517	UsrClass.dat		
☑	21518	UsrClass.dat		
☑	21519	UsrClass.dat		
☑	21520	UsrClass.dat		
☑	21521	UsrClass.dat		
☑	21522	UsrClass.dat		
☑	21523	UsrClass.dat		
☑	21524	UsrClass.dat		
☑	21525	UsrClass.dat		

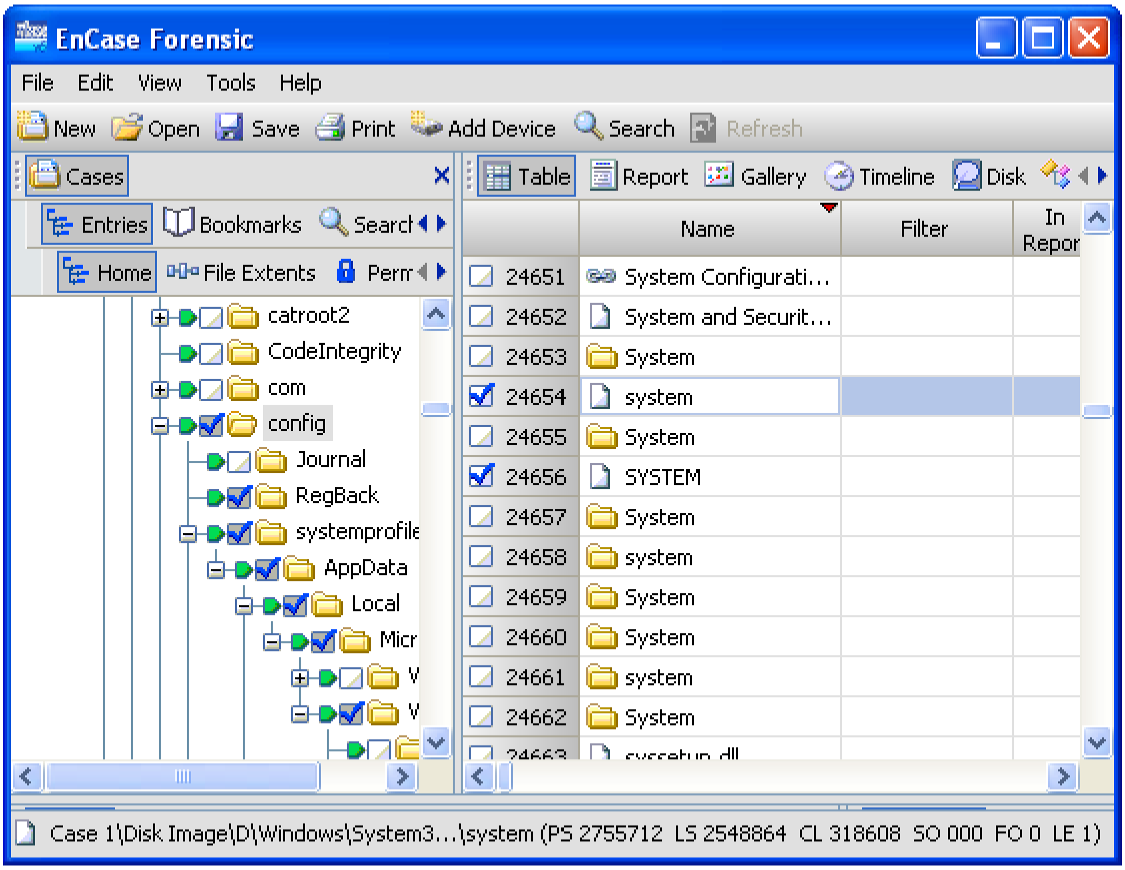
Case 1\Disk Image\D\Users\Jo...\UsrClass.dat (PS 14275584 LS 14068736 CL 1758592 SO 000 FO 0 LE 1)

10. Moving on to the system side of the registry, repeat again for all the remaining files on the list. The examples below show the SECURITY and SYSTEM files. Be careful to tag all instances and note that they may appear in upper or lower case.



		Name	Filter	In Report
□	28030	Security-Kerberos-…		
□	28031	Security-Kerberos-…		
□	28032	Security-Digest-DL.…		
□	28033	Security-Digest-DL.…		
□	28034	Security Configurati…		
☑	28035	security		
☑	28036	SECURITY		
□	28037	Security		
□	28038	security		
□	28039	SecureStartupFeat…		
□	28040	SecureStartupFeat…		
□	28041	secur32.dll		
□	28042	secur32.dll		

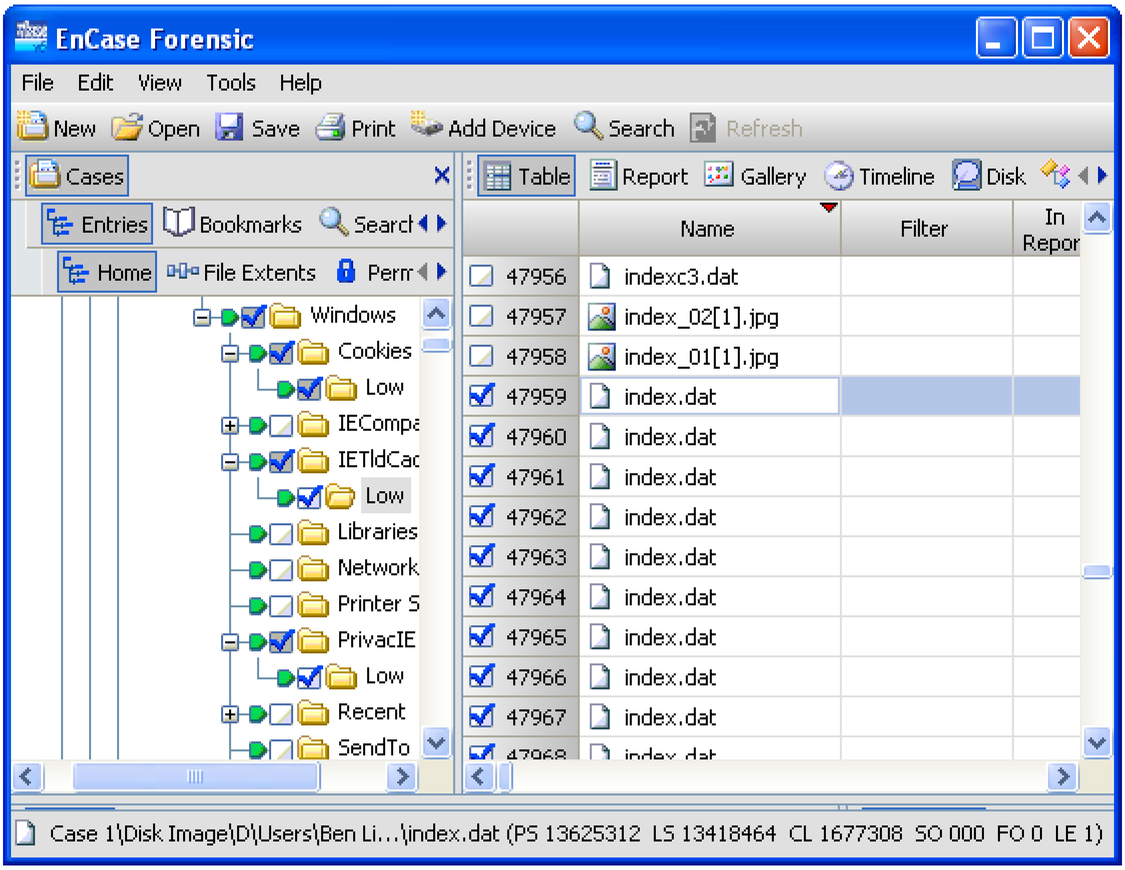
Case 1\Disk Image\D\Windows\System3…\security (PS 5872256 LS 5665408 CL 708176 SO 000 FO 0 LE 1)



		Name	Filter	In Report
□	24651	System Configurati…		
□	24652	System and Securit…		
□	24653	System		
☑	24654	system		
□	24655	System		
☑	24656	SYSTEM		
□	24657	System		
□	24658	system		
□	24659	System		
□	24660	System		
□	24661	system		
□	24662	System		
□	24663	syssetup.dll		

Case 1\Disk Image\D\Windows\System3…\system (PS 2755712 LS 2548864 CL 318608 SO 000 FO 0 LE 1)

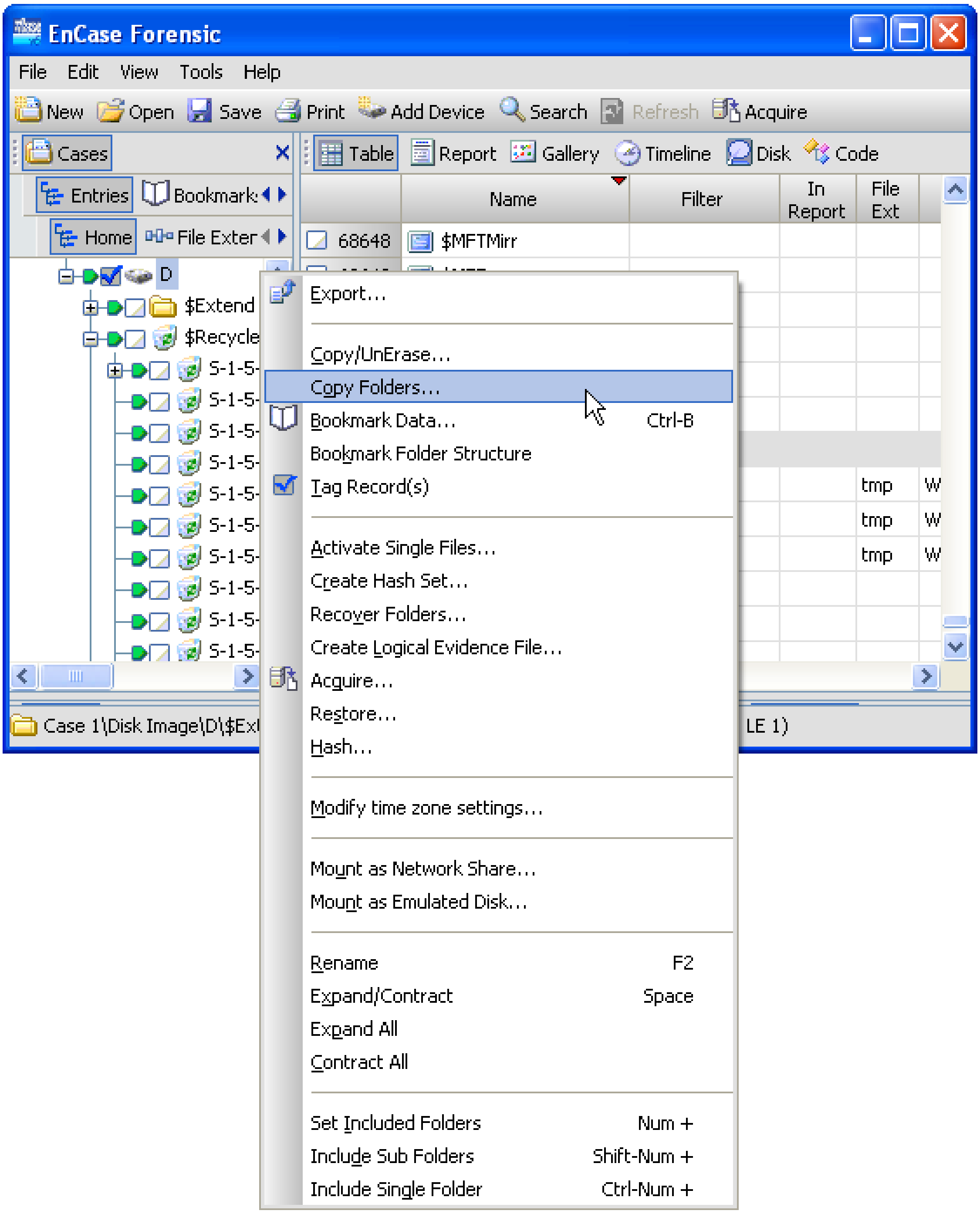
11. Before moving on, it’s a good idea to include the IE cache files named “INDEX.DAT”. This step is completely optional, however, if you were considering examining the IE cache files with a product other than Encase® Forensic, this is a perfect opportunity to export these files as well. Also note that Registry Browser will allow you to view the contents of the INDEX.DAT files. The illustration below shows the INDEX.DAT files being tagged.



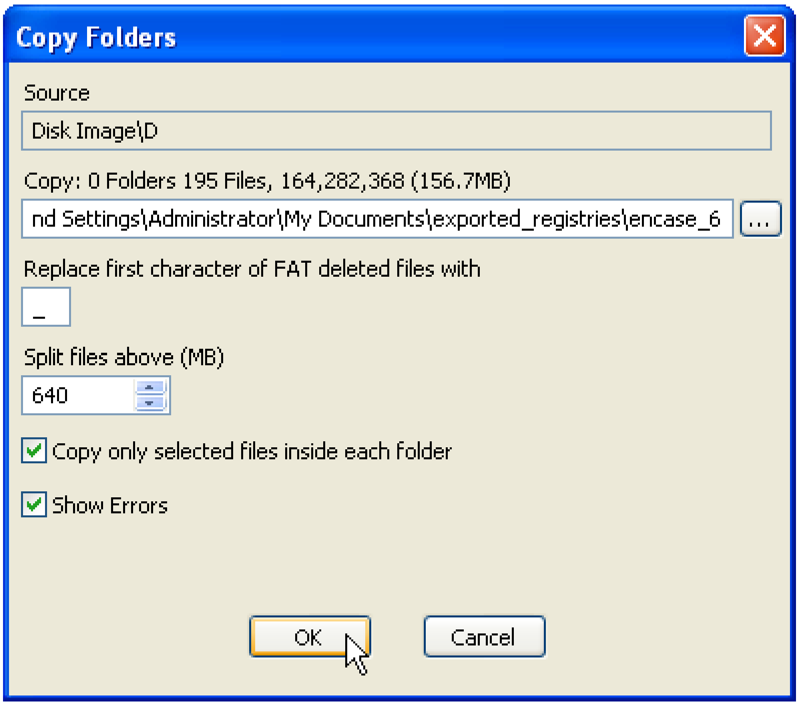
	Name	Filter	In Repor
□ 47956	indexc3.dat		
□ 47957	index_02[1].jpg		
□ 47958	index_01[1].jpg		
☑ 47959	index.dat		
☑ 47960	index.dat		
☑ 47961	index.dat		
☑ 47962	index.dat		
☑ 47963	index.dat		
☑ 47964	index.dat		
☑ 47965	index.dat		
☑ 47966	index.dat		
☑ 47967	index.dat		
☑ 47968	index.dat		

Case 1\Disk Image\D\Users\Ben Li...\index.dat (PS 13625312 LS 13418464 CL 1677308 SO 000 FO 0 LE 1)

12. Now that all the necessary files have been tagged, it's time to export the files. Return to the left pane and scroll back to the top of the tree, so that the "D" volume is again visible. Right click on the "D" volume and the following popup menu will appear. Select "Copy Folders".


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Acquire
Cases
Table Report Gallery Timeline Disk Code
Entries Bookmark
Home File Exter
Name Filter In Report File Ext
68648 $MFTMirr
D
$Extend
$Recycle
S-1-5-
Export...
Copy/UnErase...
Copy Folders...
Bookmark Data... Ctrl-B
Bookmark Folder Structure
Tag Record(s)
Activate Single Files...
Create Hash Set...
Recover Folders...
Create Logical Evidence File...
Acquire...
Restore...
Hash...
Modify time zone settings...
Mount as Network Share...
Mount as Emulated Disk...
Rename F2
Expand/Contract Space
Expand All
Contract All
Set Included Folders Num +
Include Sub Folders Shift-Num +
Include Single Folder Ctrl-Num +
tmp
Case 1\Disk Image\D\$Ext
LE 1)

13. The following dialog box will appear where you can specify a folder where the files should be exported. Ensure the “Copy only selected files inside each folder” option is checked. Click okay to begin the copy.



Copy Folders

Source

Disk Image\D

Copy: 0 Folders 195 Files, 164,282,368 (156.7MB)

nd Settings\Administrator\My Documents\exported_registries\encase_6

Replace first character of FAT deleted files with

_

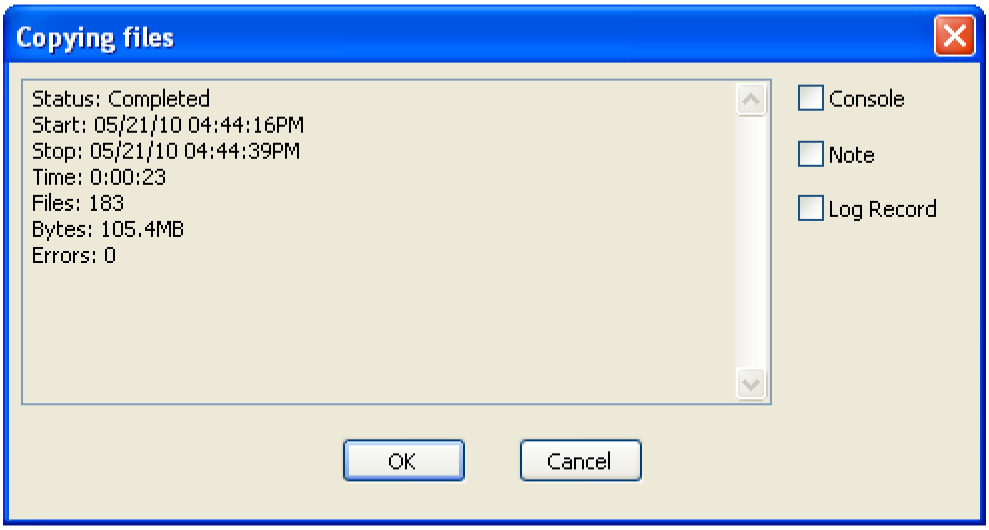
Split files above (MB)

640

☑ Copy only selected files inside each folder

☑ Show Errors

14. Once the export is complete, a dialog will appear stating how many files were exported. (See below). Upon browsing to the folder selected for the export, a folder named after the volume eg. “D” will be visible. Inside this folder will be a Windows folder and a Users folder. These two folders will mirror the original Windows and Users folders except that only the subfolders containing registry files will exist as well as the registry files themselves. This process has successfully created a copy of the Windows Registry whilst maintaining the original directory structure.



Copying files

```
Status: Completed
Start: 05/21/10 04:44:16PM
Stop: 05/21/10 04:44:39PM
Time: 0:00:23
Files: 183
Bytes: 105.4MB
Errors: 0
```

☐ Console

☐ Note

☐ Log Record