



FORENSIC EXPLORER

User Manual

Published: 12-Mar-15 at 09:36:51



Chapter Contents

Published: 12-Mar-15 at 09:36:48

Chapter 1 - Introduction.....	11
1.1 Introducing Forensic Explorer	12
1.2 Supported file formats	12
1.3 Supported file systems	12
1.4 Key program features	13
Chapter 2 - 30 Day Evaluation Version	15
2.1 30 day evaluation version.....	16
2.2 Activating the 30 day evaluation version	16
Chapter 3 - Purchase	23
3.1 Purchase	24
3.2 License maintenance	25
Chapter 4 - Installation	27
4.1 System requirements	29
4.2 Download	29
4.3 Installation	29
4.4 Uninstall Forensic Explorer	34
Chapter 5 - Dongle Activation.....	35
5.1 Dongle activation of the purchased version.....	36
5.2 Activate a Remote Computer	40
5.3 Applying maintenance updates to your Wibu dongle.....	42
Chapter 6 - Forensic Acquisition	43
6.1 Write block	44
6.2 GetData's Forensic Imager	45
Chapter 7 - Forensic Explorer Interface	55
7.1 Modules.....	56

7.2	Module data views	59
7.3	Customizing layouts.....	61
7.4	Task Processes List	62
7.5	Process Logging and Priority.....	63
7.6	Reference Library.....	64
Chapter 8 - Data Views.....		69
8.1	Data views summary.....	71
8.2	Tree view	74
8.3	List view	77
8.4	Disk view	78
8.5	Gallery view	84
8.6	Hex view	86
8.7	Text view.....	88
8.8	Display view	89
8.9	Byte Plot and Character Distribution	91
8.10	Filesystem Record view	96
8.11	File Metadata.....	98
8.12	File Extent	100
Chapter 9 - Working with data		101
9.1	Working with data	102
9.2	Highlighted and checked items.....	102
9.3	Add and edit bookmarks.....	104
9.4	Open with	104
9.5	Expand compound file	105
9.6	Export.....	105
9.7	Send to Module	110
9.8	Columns	110
9.9	Sorting.....	111

9.10	Flags.....	113
9.11	Filtering Data	114
9.12	Copy rows to clipboard.....	119
Chapter 10 - Evidence Module.....		121
10.1	Preview	122
10.2	New case	124
10.3	Open an existing case	127
10.4	Adding evidence	129
10.5	Evidence Processor	135
10.6	Adding additional evidence to a case	139
10.7	Saving a case.....	140
10.8	Closing a case	141
Chapter 11 - File System Module		143
11.1	File System module	144
11.2	Toolbar	144
11.3	Folders view.....	144
11.4	Categories view	146
11.5	File List view	147
11.6	Other data views	149
Chapter 12 - Keyword Search Module.....		151
12.1	Keyword search	152
12.2	Keyword management	153
12.3	Search results	160
12.4	Keyword result list	162
12.5	Keyword search data views	163
Chapter 13 - Index Search Module.....		165
13.1	Index search	166
13.2	Considerations prior to creating an index	167

13.3	Creating an index	167
13.4	Searching an index	169
13.5	Search results.....	172
13.6	Index Search Compound Files.....	173
13.7	Export Word List	173
Chapter 14 - Email Module.....		175
14.1	Email	176
14.2	Email module	176
14.3	Microsoft Outlook .PST email	176
14.4	Index Search the Email module	177
14.5	keyword Search the Email module	178
Chapter 15 - Registry Module.....		179
15.1	Registry module	180
15.2	Adding a REGISTRY FILE to the registry module	181
15.3	Registry Data Views	182
15.4	Deleted registry keys	183
15.5	Examining registry files using scripts	184
Chapter 16 - Bookmarks Module		187
16.1	Adding Bookmarks	188
16.2	Bookmarks Module.....	190
16.3	Identifying Bookmarked files other modules	193
Chapter 17 - Reports Module		194
17.1	Reporting & Bookmarks.....	195
17.2	The Reports Module	196
17.3	ReportS Tree	197
17.4	Report Editor	201
17.5	Creating Reports	203

Chapter 18 - Scripts Module	215
18.1 Scripts Module.....	216
18.2 Managing scripts in the scripts window	222
18.3 Introduction to Scripting	223
18.4 Startup.Pas	227
Chapter 19 – Custom Modules	231
19.1 About Custom Modules.....	232
19.2 Browser History Module.....	232
19.3 Phone Module	232
Chapter 20 - Date and Time	235
20.1 Date and time in computer forensics	236
20.2 FAT, HFS, CDFS file system date and time	236
20.3 NTFS, HFS+ file system date and time	236
20.4 Date and time information in the Windows registry.....	236
20.5 Daylight saving time (DST)	240
20.6 Adjusting Date in Forensic Explorer	241
Chapter 21 - Hashing.....	245
21.1 Hash Values	246
21.2 Hash Algorithms	246
21.3 Acquisition Hash	246
21.4 Verification Hash	247
21.5 Hashing files in a case.....	248
21.6 Hash sets	251
21.7 Download Hash Sets.....	252
21.8 Creating hash sets	252
21.9 Apply a Hash Set in a Case.....	256
Chapter 22 - File Signature Analysis	259
22.1 File signature analysis.....	260

22.2	Why run file signature analysis?	260
22.3	Running a file signature analysis.....	260
22.4	Examine the results of a file signature analysis	262
Chapter 23 - Data Recovery		263
23.1	DATA Recovery - Overview	264
23.2	FAT data recovery	265
23.3	NTFS data recovery	272
23.4	File carving	276
Chapter 24 - RAID		281
24.1	RAID - Introduction	282
24.2	Preparation	282
24.3	Adding a RAID to a case	283
Chapter 25 – Shadow Copy		287
25.1	Shadow Copy Introduction	288
25.2	Examining Shadow Copies With Forensic Explorer	293
Chapter 26 – Mount Image Pro		297
26.1	Mount Image Pro	298
Chapter 27 – Live Boot		301
27.1	Live Boot	302
27.2	Requirements	302
27.3	Compatibility	304
27.4	Live Boot Working Folder	304
27.5	How to Live Boot a Forensic Image.....	305
27.6	Live Boot and Windows User Passwords	310
27.7	TroubleShooting Live Boot	313
Chapter 28 – Working With		315
28.1	iTunes Backups	316
28.2	Thumbnails	326

28.3	Thumbnail in Forensic Explorer	327
Chapter 29 - Legal		331
29.1	This User Guide.....	332
29.2	Copyright	332
29.3	License agreement	332
29.4	Disclaimer	334
Appendix 1 - Technical Support		335
Appendix 2 - Write Blocking		337
Appendix 3 - File carving		339
Appendix 4 - Summary of Date and Time		345
Appendix 5 - References.....		347
Appendix 6 - Definitions		351
Appendix 7 - Sample Script.....		363
Appendix 8 - Icon Key.....		365
Appendix 9 - Index		367

Chapter 1 - Introduction

In This Chapter

CHAPTER 1 - INTRODUCTION

1.1	Introducing Forensic Explorer	12
1.2	Supported file formats	12
1.3	Supported file systems	12
1.4	Key program features	13

1.1 INTRODUCING FORENSIC EXPLORER

Forensic Explorer is a computer forensics software program written by GetData Forensics Pty Ltd (www.forensicexplorer.com). Forensic Explorer is a tool for the analysis and presentation of electronic evidence. Primary users of this software are those involved in civil or criminal investigations.

Forensic Explorer combines a flexible graphic user interface (GUI) with advanced sorting, filtering, searching, previewing and scripting technology. It enables investigators to:

- Access and examine all available data, including hidden and system files, deleted files, file and disk slack and unallocated clusters;
- Automate complex investigational tasks;
- Document a case and produce detailed reports; and,
- Provide other parties with a simple to use tool to easily review evidence.

1.2 SUPPORTED FILE FORMATS

Forensic Explorer supports the **acquisition** of the following file formats:

- DD or RAW;
- EnCase® .E01;
- Forensic File Format .AFF

Forensics Explorer supports the **analysis** of the following file formats:

Type	Extension
Apple DMG	.DMG
DD or RAW	.DD, .BIN, .RAW
EnCase®	.E01, .Ex01, .L01, .Lx01
Forensic File Format	.AFF
FTK®	.E01, .AD1
ISO	.ISO
Microsoft VHD	.VHD
NUIX	.MFS
ProDiscover®	.EVE
Safeback® v2	.001
SMART	.S01
VMWare®	.VMD, .VMDK
Xways Container	.CTR

1.3 SUPPORTED FILE SYSTEMS

Forensic Explorer supports analysis of:

- Windows FAT12/16/32, exFAT, NTFS,

- Macintosh HFS, HFS+ (no journal processing)
- EXT 2/3/4 (no journal processing)
- CD/DVD ISO, UDF
- Hardware and Software RAID: JBOD, RAID 0, RAID 5

1.4 KEY PROGRAM FEATURES

Key Forensic Explorer features include:

Fully Customizable Interface: The forensic explorer interface has been designed for flexibility. Drag, drop and detach windows for a customized module. Save and load module configurations to suit investigative needs.

International Language Support: Forensic Explorer supports Unicode. Investigators can search and view data in native language format.

Complete Data Access: Access all areas of physical or imaged media at a file, text, or hex level. View and analyze system files, file and disk slack, swap files, print files, boot records, partitions, file allocation tables, unallocated clusters, etc.

Powerful Pascal Scripting language: Automate analysis using a provided script library, or write your own analysis scripts.

Fully Threaded: Run different analysis functions in separate threads.

Data Views: Powerful data views including:

- **File List:** Sort and multi sort files by attribute, including, extension, signature, hash, path and created, accessed and modified dates.
- **Category Views:** Show files by extension, date etc.
- **Disk:** Navigate a disk and its structure via a graphical view. Zoom in and out to graphically map disk usage.
- **Gallery:** Thumbnail photos and image files.
- **Display:** Display more than 300 file types. Zoom, rotate, copy, search.
- **Filesystem Record:** Easily access and interpret FAT and NTFS records.
- **Text and Hexadecimal:** Access and analyse data at a text or hexadecimal. Automatically decode values with the **data inspector**.
- **File Extent:** Quickly locate files on disk with start and end sector runs.
- **Byte Plot and Character Distribution:** Examine individual files using Byte Plot graphs and ASCII Character Distribution.
- **File Metadata:** Examine metadata properties within files.

RAID Support: Work with physical or forensically imaged RAID media, including software and hardware RAID, JBOD, RAID 0 and RAID 5.

Hashing: Apply hash sets to a case to identify or exclude known files. Hash individual files for analysis.

Keyword search: Sector level keyword search of entire media using RegEx expressions.

Keyword index: Built in DTSearch index and keyword search technology.

Bookmarks and Reporting: Add bookmarks to identify evidence and include bookmarks in a custom report builder.

Data Recovery and Carving: Recover folders and files. Use an inbuilt file carving tool to carve more than 300 known file types or script your own.

File Signature Analysis: Validate the signature against file extension.

Export to LEF: Export a subset of files in a case to a LEF (Logical Evidence File).

Chapter 2 - 30 Day Evaluation Version

In This Chapter

CHAPTER 2 - 30 DAY EVALUATION VERSION

2.1	30 day evaluation version.....	16
2.1.1	Installation	16
2.1.2	Limitations	16
2.2	Activating the 30 day evaluation version	16
2.2.1	Online Activation (30 DAY Evaluation).....	16
2.2.2	Offline Activation (30 day evaluation)	18

2.1 30 DAY EVALUATION VERSION

To request a 30 day evaluation version of Forensic Explorer, visit <http://www.forensicexplorer.com/request-evaluation-key.php> and complete the online registration form. **Download instructions** and an **evaluation version software activation key** and will be sent to your email address.

Note: It is not possible to activate the evaluation version in Virtual Machine.

2.1.1 INSTALLATION

The Forensic Explorer 30 day evaluation version is a standalone program. It has:

- A separate installation file: “**ForensicExplorer-Evaluation-Setup.exe**” and;
- Is installed in its own path “**C:\Program Files\GetData\Forensic Explorer Evaluation vX**”.

The evaluation version is marked as “Evaluation” in the status bar at the bottom of the Evidence Module and in the program “About” tab.

2.1.2 LIMITATIONS

The 30 day evaluation version has the following limitations:

- Does not allow the saving of case files;
- Does not allow the exporting of files from a case; and,
- Will expire after 30 days.

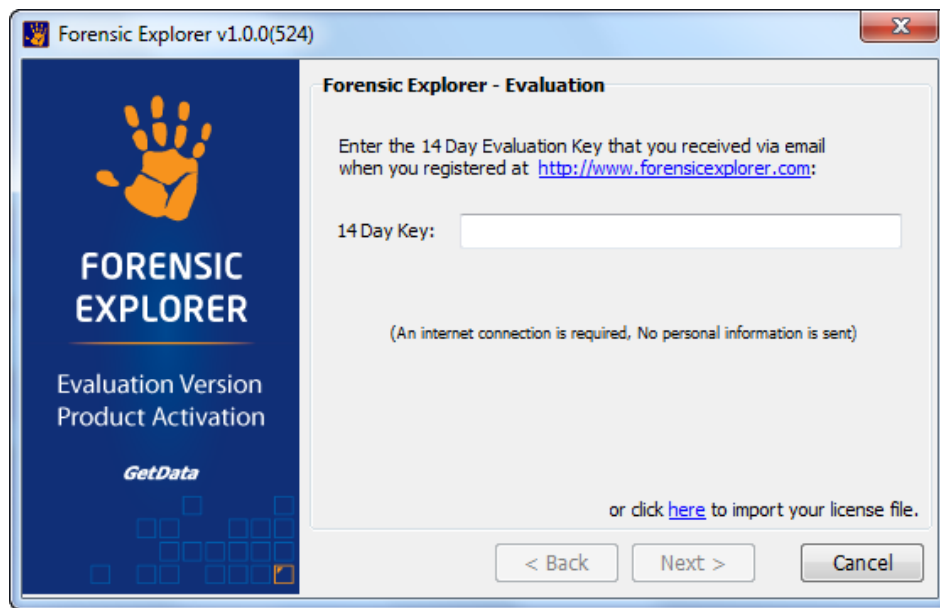
2.2 ACTIVATING THE 30 DAY EVALUATION VERSION

The 30 day evaluation version is activated by a **software key** only (a purchased version is activated by dongle only).

2.2.1 ONLINE ACTIVATION (30 DAY EVALUATION)

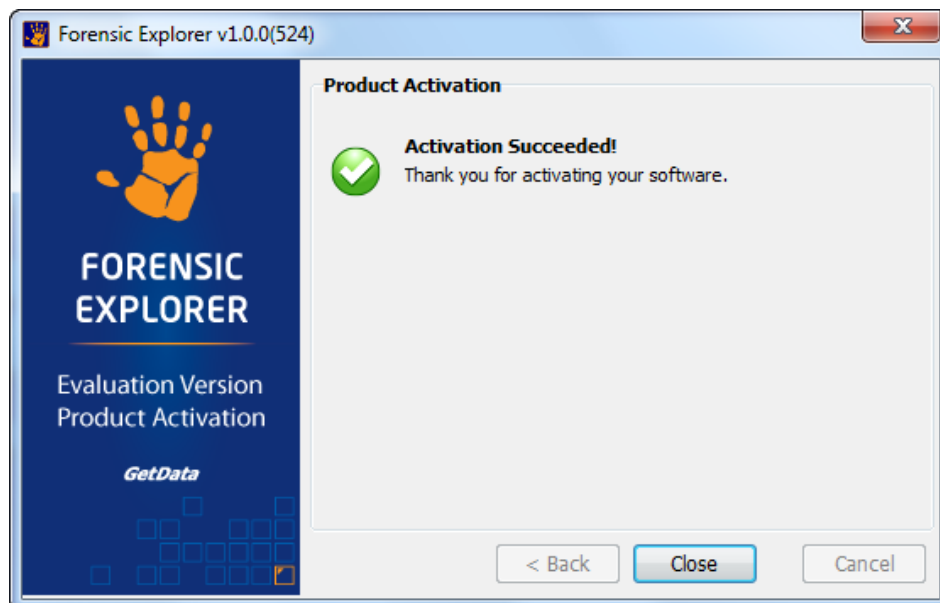
If your computer is connected to the internet, enter the 30 day evaluation version key into the field provided and click Next (as shown in Figure 1 below):

Figure 1, Online activation, 30 day trial version



A successful activation message will display the following screen, as shown in Figure 2 below:

Figure 2, 30 day evaluation version successful activation message



Once the 30 day evaluation version is activated, the number of evaluation days remaining is shown on the program splash screen (see Figure 3 below). Click on the "Continue Evaluation" button to use the software, or the "Buy Online" button to visit the purchase page at www.forensicexplorer.com.

Figure 3, 30 day evaluation version splash screen



2.2.2.2 OFFLINE ACTIVATION (30 DAY EVALUATION)

Where the computer on which the software is being installed is not connected to the internet, a separate internet connected computer can be used to activate. The activation process involves:

- Exporting a license file from the software;
- Uploading the license file, together with your purchase email address and license key at a web site (using any internet connected computer);
- Downloading the validated license file and importing it back into the software.

To activate an offline computer:

1. Click the Offline Activation button and click Next;

Figure 4, Activation wizard



2. Click on the Export button to export and save the license file "GetData.GDActRequest":

Figure 5, Offline activation (evaluation version), export of license file



3. Using an web browser on any internet connected computer, go to "http://getdata.com/offline" (or https://secure.getdata.com/key/key-activation-wibu-offline.php) and enter the required details:

Figure 6, Offline activation (evaluation version), upload of license file and activation details

GetData Product - Manual Activation

What is your purchase Email address?
support@getdata.com

What is the License Key (found in purchase confirmation email)?
82A5-6723-CSA2

Upload your Activation Request File?
C:\Users\Graham\Downloads\GetData.GDActRequest

GetData - Secure Home | Resellers | About Us | Member Login | Sitemap | Merchandise
Copyright © GetData 2012 All Rights Reserved

Click the Upload button to send the details to the activation server:

The details are validated by the activation server and the file "GetData.GDActResponse" is returned to you.

Figure 7, Offline activation (evaluation version), download of license file

here to begin the download manually.' The footer is the same as Figure 6."/>

GetData Product - Manual Activation

Your activation response file will begin to automatically download shortly.
Click [here](#) to begin the download manually.

GetData - Secure Home | Resellers | About Us | Member Login | Sitemap | Merchandise
Copyright © GetData 2012 All Rights Reserved

Save "GetData.GDActResponse" and take it back to the offline computer on which you will be activating the software.

Once the "GetData.GDActResponse" file is back on the offline computer, click the Import button to import the file into the software. The software is now activated:

Figure 8, Successful software key activation of 30 day evaluation version



Chapter 3 - Purchase

In This Chapter

CHAPTER 3 - PURCHASE

3.1	Purchase	24
3.1.1	Purchase Online	24
3.1.2	Purchase Orders.....	24
3.1.3	Resellers.....	24
3.2	License maintenance	25
3.2.1	Purchase License Maintenance	25

3.1 PURCHASE

Forensic Explorer is dongle activated only. A dongle is provided for each license purchased.

Forensic Explorer is available for purchase online, via purchase order, or via forensic software resellers.

3.1.1 PURCHASE ONLINE

Forensic Explorer can be purchased online at <http://www.forensicexplorer.com> by following the purchase links. Please see the purchase page for pricing, volume discounts and software bundle options.

3.1.2 PURCHASE ORDERS

Purchase Orders can be placed by Government and Corporate entities by contacting GetData head office:

GetData Pty Ltd
Suite 204, 13A Montgomery Street
Kogarah,
New South Wales, 2217
Australia
Ph: +61 2 82086053
Fax: +61 2 95881195
Email: sales@getdata.com

Or by secure post:

GetData Forensics Pty Ltd
P.O. Box 71
Engadine, New South Wales, 2233
Australia

Or via your forensic reseller.

3.1.3 RESELLERS

For a list of approved resellers, please contact GetData via: sales@getdata.com or via the contact details above.

3.2 LICENSE MAINTENANCE

A Forensic Explorer license purchase **includes 12 months maintenance** giving access to updates and support.

When the **maintenance for a dongle has expired**, Forensic Explorer will continue to work, however you may only use the latest available version prior to the expiration of your maintenance period.

The expiration date for the maintenance of a dongle is displayed in the program splash screen, shown in Figure 9 below:

Figure 9, Forensic Explorer splash screen showing maintenance date



When the maintenance is nearing the expiration date an email is sent to the purchaser with the option to renew.

3.2.1 PURCHASE LICENSE MAINTENANCE

To purchase additional Forensic Explorer maintenance online:

1. Visit the following web page: <http://www.forensicexplorer.com/buy-forensic-explorer.php>
2. Select the option to purchase maintenance renewal for existing Forensic Explorer dongles.
3. Complete the checkout process.

Forensic Explorer maintenance is sold in increments of 1 year. A purchase of two years maintenance can be used to extend a single dongles maintenance by two years.

To apply the maintenance update to your dongle, and follow the instructions in 5.3 - Applying maintenance updates to your Wibu dongle.

Chapter 4 - Installation

In This Chapter

CHAPTER 4 - INSTALLATION

4.1	System requirements	29
4.2	Download	29
4.3	Installation	29
4.3.1	Installed files	31
4.3.2	Non English installation	33
4.4	Uninstall Forensic Explorer	34

4.1 SYSTEM REQUIREMENTS

Forensic Explorer requires:

- Windows XP, 2003, Vista, Win 7, 2008;
- Pentium IV 1.4 GHz or faster processor;
- 1GB RAM;
- 32bit and 64bit compatible.

When processing large volumes of electronic evidence a high specification forensic workstation is recommended.

4.2 DOWNLOAD

Full purchased version:

Your email received at the time of purchase will contain download instructions for the software.

30 day evaluation version:

See Chapter 2 - 30 Day Evaluation Version, for further information on the evaluation version.

4.3 INSTALLATION

IMPORTANT: Ensure that you have a separate and secure backup of case files before you make installation modifications.

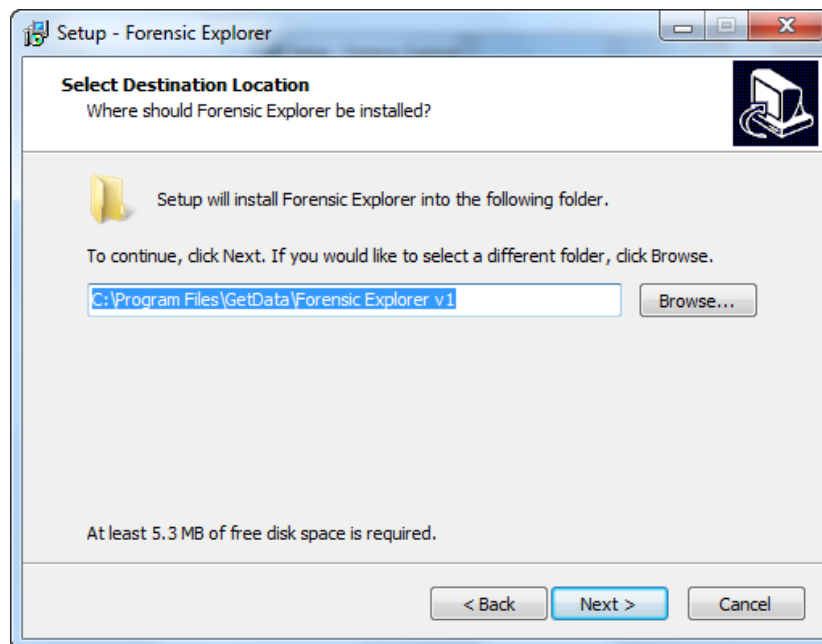
To install Forensic Explorer:

- Run the installation file **ForensicExplorer-Setup.exe** (or ForensicExplorer-Evaluation-Setup.exe if you are installing the 30 day evaluation version).
- Follow the setup instructions.

The following windows will appear during the installation process:

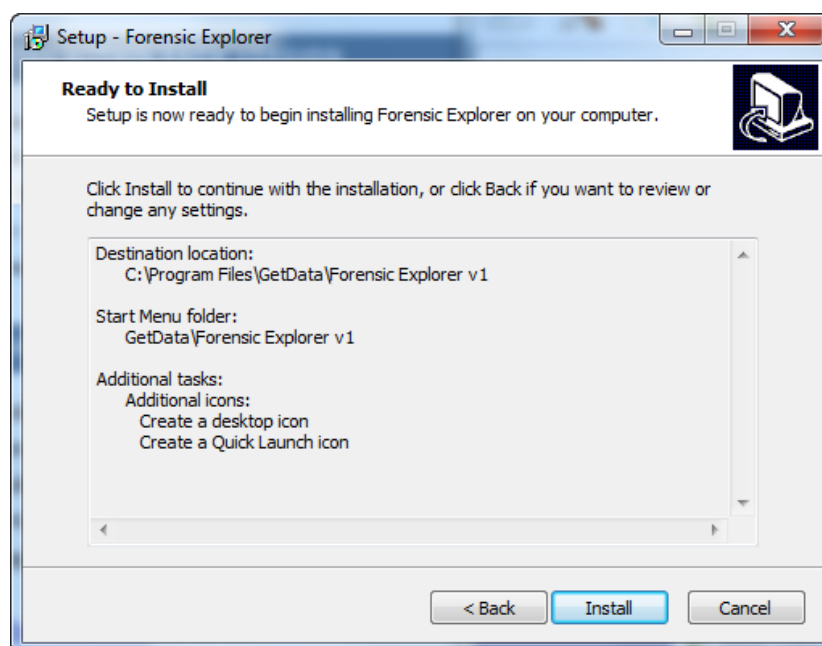
1. Forensic Explorer License agreement. Answer the question and click **Next**;
2. Select the installation language. Click **Next**.
3. Enter the correct installation path or accept the default path (e.g. **C:\Program Files\GetData\Forensic Explorer vX**) and click **Next**;

Figure 10, Selecting the installation folder



1. Follow the setup instructions and confirm the setup summary by clicking the **Install** button;

Figure 11, Finalize installation



2. A successful install will display the following screen. Click **Finish** to confirm.

Figure 12, Finish installation



3. Run Forensic Explorer from the installed desktop icon:

Figure 13, Desktop icon



4.3.1 INSTALLED FILES

PROGRAM PATH

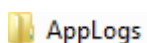
The default Forensic Explorer installation folder is:

C:\Program Files\GetData\Forensic Explorer vX









WORKING PATH

The working path for a case is in the user profile documents folder;

C:\Users\[user folder]\Documents\Forensic Explorer







Forensic Explorer usage logs.

 Cases	Contains the investigator created case folders.
 Databases	Holds case database files use to store case data, investigator names, etc.
 Filters	Filters are created in the Scripts module and used in the Folder view of the File System module. See 8.2.2 - Tree view filter, for more information.
 Hash Sets	Holds the database files used to store hash set information.
 Keywords	This folder is used to store sample keyword search import lists. They can be imported in the Keyword Search module.
 Previews	A device or image can be previewed without fist creating a case. A unique preview working folder is created within this folder using a Global Unique Identifier (GUID, e.g. 8709A41C-38B6-4F9E-BA18-633B394721C5).
 Scripts	Holds Forensic Explorer scripts (created and/or used in the Scripts module). “.pas” are un-compiled. “.bin” are compiled.
 Startup	Holds the “startup.pas” script used to store button positions etc. (see the chapter on Scripts for further information).

CASE FILE FOLDER

The following folders are created within each case folder:

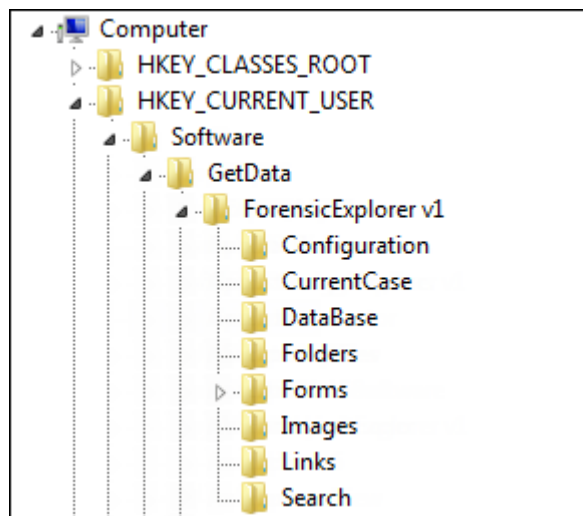
C:\Users\[user folder]\Documents\Forensic Explorer\Cases\[Case Name]

 Attached Evidence	External files (photos, documents etc.) attached to the case.
 DTSearchIndexes	DT Search keyword indexes.
 Exported	File export folder
 Logs	Program audit logs.
CaseName.FEX	Case file.

REGISTRY KEYS

At the time of installation Forensic Explorer registry keys are written to the HKEY_CURRENT_USER as shown in Figure 14 below:

Figure 14, Forensic Explorer registry keys



4.3.2 NON ENGLISH INSTALLATION

The Forensic Explorer GUI has been translated into the following languages:

- Chinese (Simplified)
- German
- Indonesian (Bahasa)
- Spanish
- Turkish

During the installation process, select the desired language:

IMPORTANT: It is recommended that a case be conducted in a single GUI language. Changing language mid case may affect modules which rely on path and field names, such as Scripts and Reports.

STARTUP LANGUAGE

The **startup language** is controlled by the registry setting:

`HKCU\Software\GetData\ForensicExplorer v2\Configuration\DefaultLanguage`

Where the key is set to: EN (default), DE, ID, ES, ZH, TR for the required language.

BOOKMARK FOLDER TRANSLATION

Bookmark folder translations can be managed by using the “bookmark folder translations.txt” file located in the install folder. Currently the translations operate on the first level bookmark folder only.

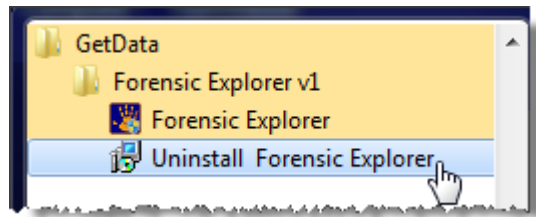
4.4 UNINSTALL FORENSIC EXPLORER

IMPORTANT: Ensure that you have a separate and secure backup of all evidence and case files before you make installation modifications.

There are two methods to start the uninstall process;

1. Select “Uninstall Forensic Explorer” in the Windows Start menu:

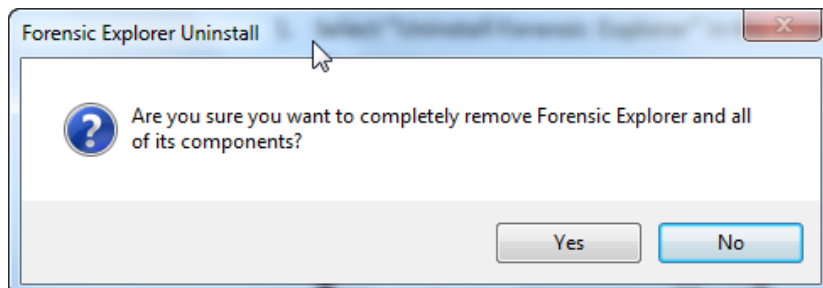
Figure 15, Uninstall from the Windows start menu



2. Or, open the Windows Control Panel and in the “Programs” section use the “Uninstall option.

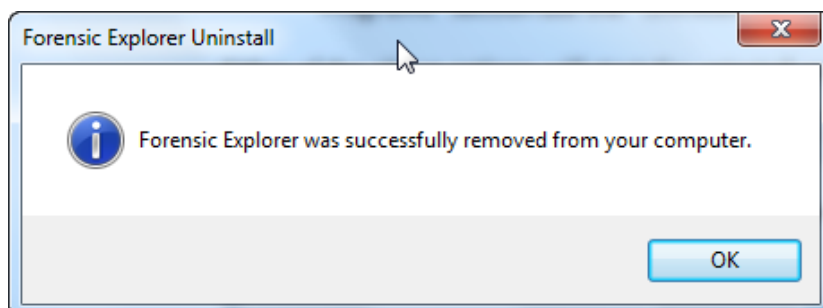
Either of the above options will start the uninstall process:

Figure 16, Uninstall process



A successful removal will show the following message:

Figure 17, Successful un-install



Chapter 5 - Dongle Activation

In This Chapter

CHAPTER 5 - DONGLE ACTIVATION

5.1	Dongle activation of the purchased version.....	36
5.1.1	Successful dongle activation	37
5.1.2	Troubleshooting Dongle Activation	37
5.2	Activate a Remote Computer	40
5.3	Applying maintenance updates to your Wibu dongle	42

5.1 DONGLE ACTIVATION OF THE PURCHASED VERSION

Forensic Explorer is activated using a **Wibu** (www.wibu.com) **USB hardware dongle** which is delivered to you by courier following your purchase (see Chapter 3 - Purchase, for more information on purchasing Forensic Explorer).

Figure 18, Wibu USB hardware activation dongle



Your Wibu dongle has a unique identification number inscribed on the part of the dongle that is inserted into the USB port, as shown in Figure 19 below. Include this number in correspondence with GetData:

Figure 19, Unique Wibu dongle identification number



The Wibu dongle is **driverless** and requires no special installation.

To run Forensic Explorer:

1. Ensure you have installed the **full version of Forensic Explorer** using the link provided in your purchase confirmation email (the dongle will not activate the evaluation version. See Chapter 2 - 30 Day Evaluation Version, for more information on the evaluation version);

2. **Insert your Wibu dongle** into a USB port on your forensic workstation. **Wait up to 30 seconds** to ensure your forensic workstation has the time to detect that the dongle has been inserted;
3. **Run forensic Explorer from the desktop icon.**

5.1.1 SUCCESSFUL DONGLE ACTIVATION

When the dongle is successfully installed, the following screen will display on startup of the application:



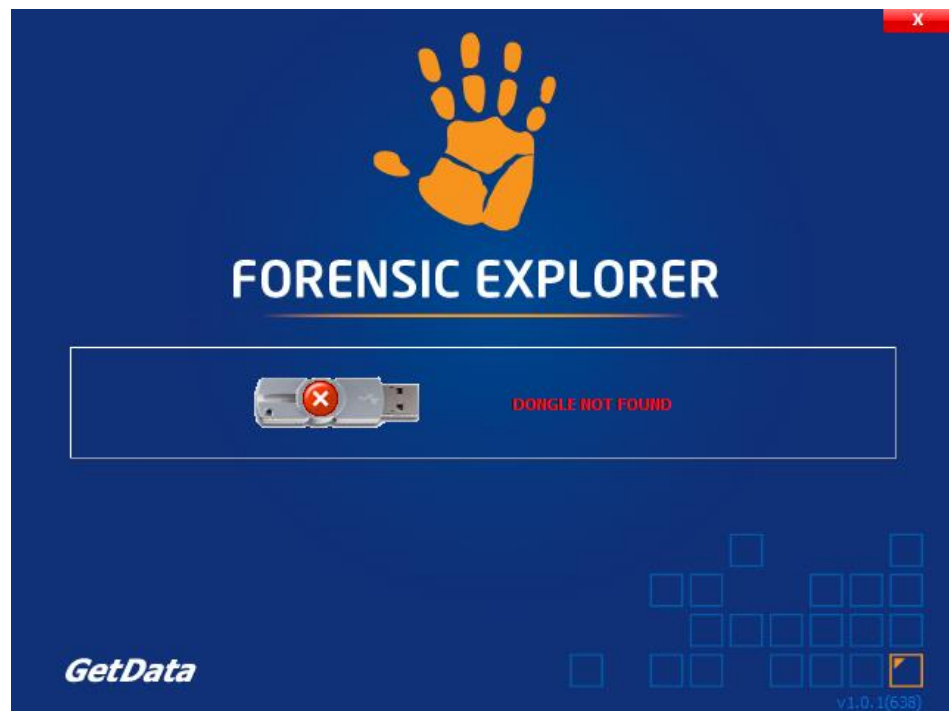
The splash screen identifies:

1. The name, or company name, of the registered owner;
2. The date upon which the current maintenance license expires for that dongle (see page 25 for information on purchasing).

5.1.2 TROUBLESHOOTING DONGLE ACTIVATION

If the Wibu dongle is not detected on application startup, the splash screen will display "DONGLE NOT FOUND", as shown in Figure 20 below:

Figure 20, Dongle not found error message



To troubleshoot dongle activation:

1. Press the “x” button to close the splash window
2. Remove and re-insert the Wibu dongle;
3. Ensure that your forensic workstation has sufficient time to detect that new hardware has been inserted. Wait for the Windows USB device message to show that new hardware has been recognized.
4. Re-run the software from the desktop icon.

WIBU CODEMETER RUNTIME FOR WINDOWS USER

If you are still unable to activate Forensic Explorer, download the **Wibu CodeMeter Runtime** for Windows: <http://www.wibu.com/downloads-user-software.html>

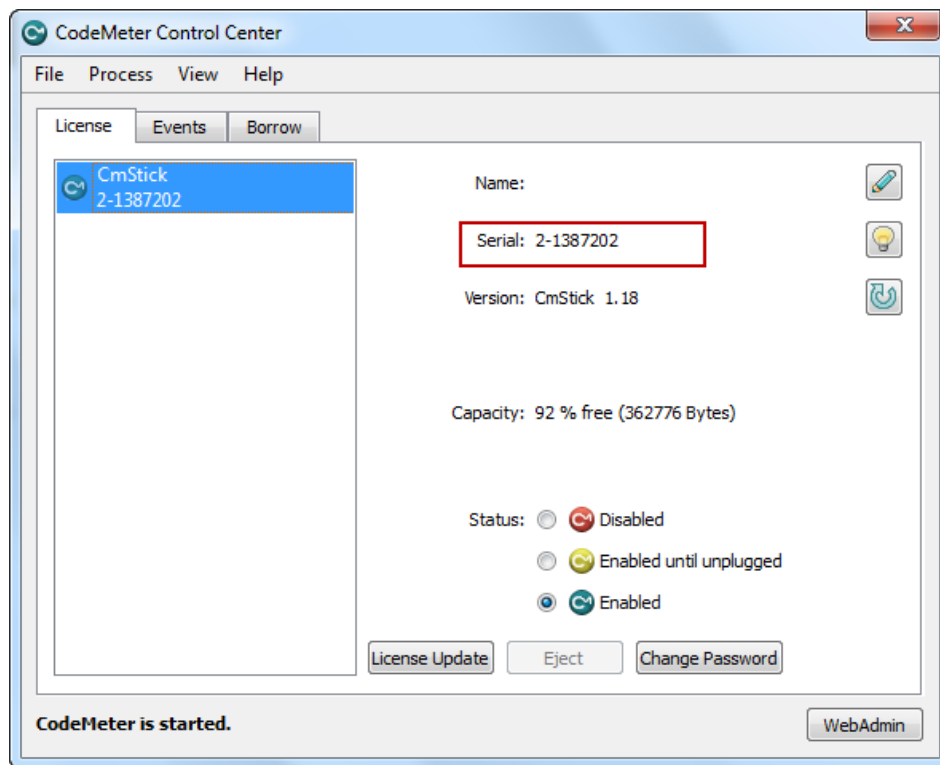
When Wibu CodeMeter software is successfully installed, insert your Forensic Explorer Wibu dongle. Double click on the Wibu icon in the Windows task bar:

Figure 21, Wibu CodeMeter Windows task bar icon



The CodeMeter Control Center will open, shown in Figure 22 below:

Figure 22, Wibu CodeMeter Control Center



Confirm that your **CmStick** is identified by the CodeMeter Control Center and that it has an **Enabled** status. Click on **Web Admin** button, which will open your web browser. In the **Web Admin** page, select **Content > Licenses**. Confirm that your Wibu dongle contains Forensic Explorer activation, as shown in Figure 23 below:

Figure 23, Wibu web admin

101712 GetData Pty Ltd			
Product Code	Name	Unit Counter	Expiration Time
51	Forensic Explorer	n/a	n/a

Contact us via support@getdata.com (see Appendix 1 - Technical Support for full contact details) and provide:

1. Your dongle ID number;
2. A screenshot of the CodeMeter Control Center;
3. A screenshot of the Wibu Web Admin page.

We will then contact you with further instructions.

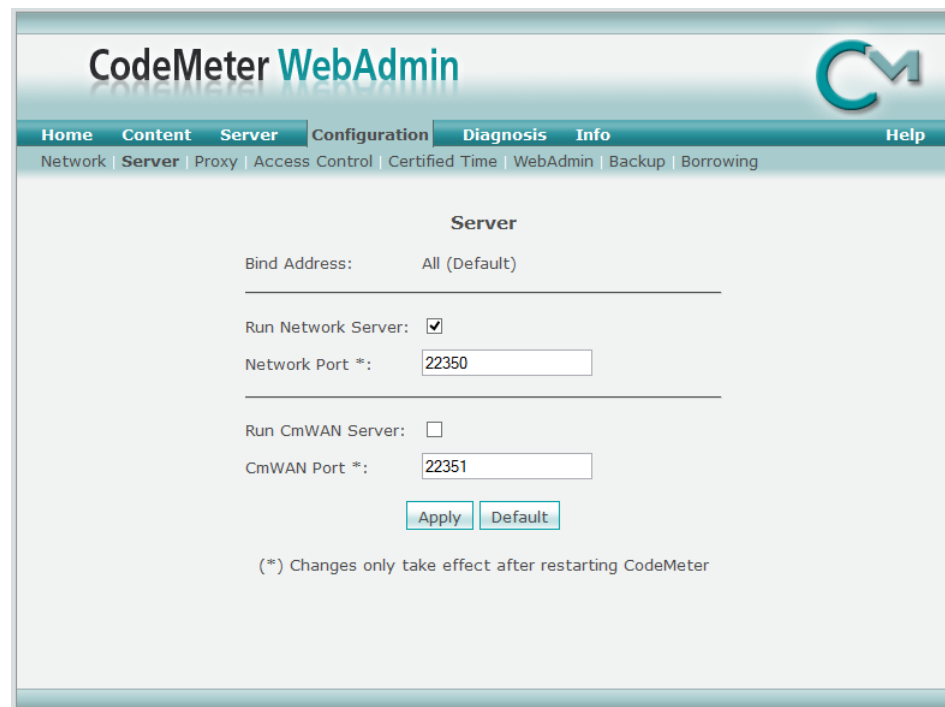
5.2 ACTIVATE A REMOTE COMPUTER

The Wibu Codemeter activation system enables you to use your local dongle to activate a remote internet connected computer:

On the **local computer** with the Forensic Explorer Codemeter dongle is inserted run the **Network Server**:

1. Download the latest **Codemeter Runtime for Windows User** from <http://www.wibu.com/downloads-user-software.html>
2. Run **CodeMeter WebAdmin** by browsing to <http://localhost:22350/ConfigServer.html>.
3. Select **Configuration > Server** from the menu, as shown in Figure 24 below:

Figure 24, CodeMeter WebAdmin



4. In the **Sever** window heck **Run Network Server** and press the **Apply** button.
5. Ensure that the selected **Network Port** 22350 is not blocked by your firewall.
6. Restart the CodeMeter Service.
 - a. Run the **CodeMeter Control Center** by clicking the CodeMeter icon in the Windows Task tray;
 - b. Select **Processes > Stop CodeMeter Service**;
 - c. Then **Start CodeMeter Service**.

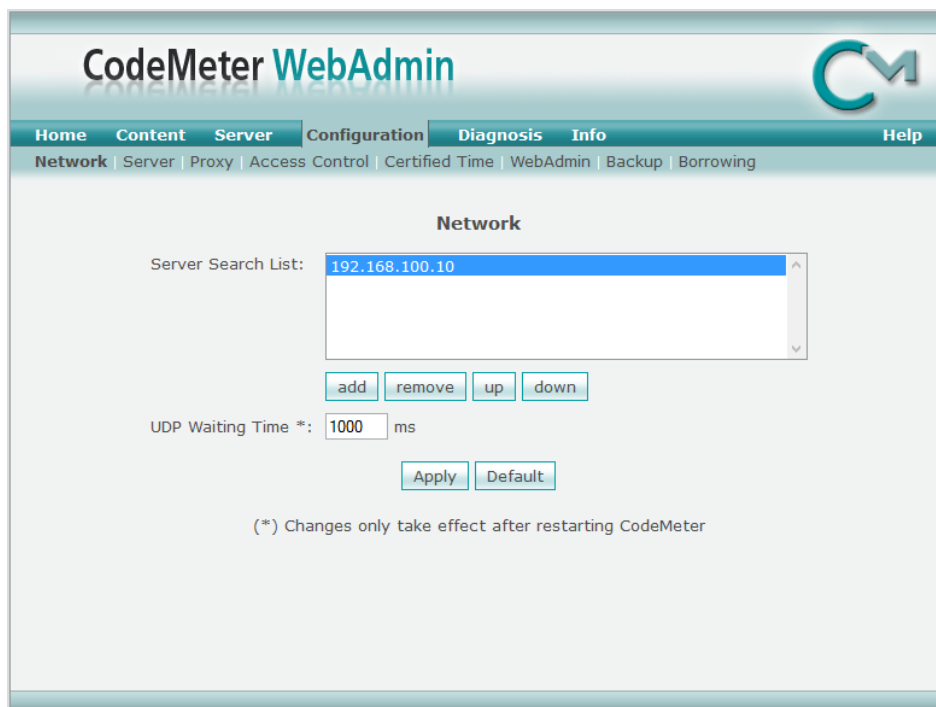
The Wibu CodeMeter Network Server can also be configured using the following registry setting:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WIBU-  
SYSTEMS\CodeMeter\Server\CurrentVersion  
IsNetworkServer=1
```

On the **client computer**:

7. Install Forensic Explorer full dongle version. **Close** Forensic Explorer.
8. Browse to <http://localhost:22350/Configuration.html>:

Figure 25, Wibu CodeMeter Local Host Configuration



9. Click the **add** button and add the IP address of **Network Server** and press **Apply**.
10. Start Forensic Explorer. It should detect the remote dongle license and activate.

The client computer can also be configured using the following registry key setting:

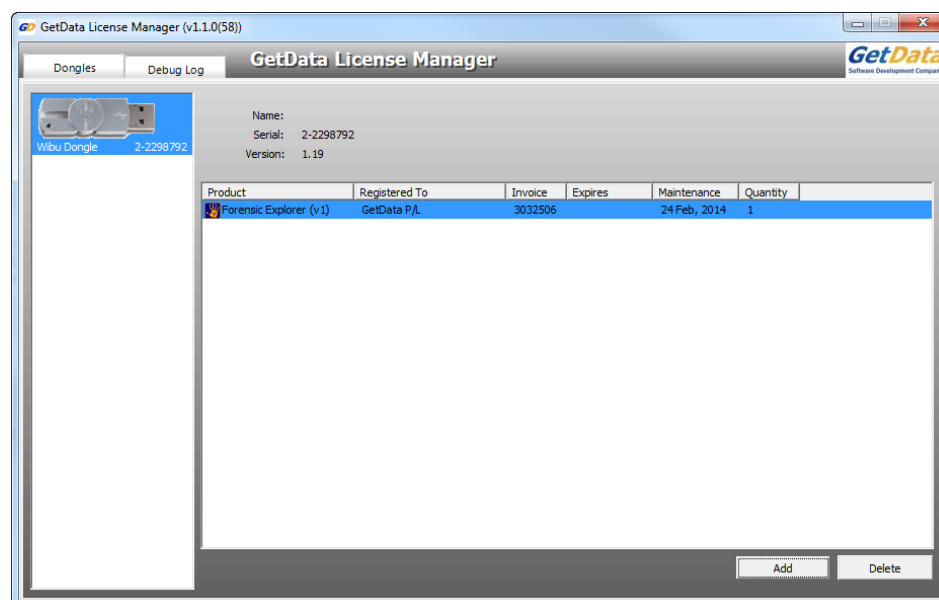
```
HKEY_LOCAL_MACHINE\SOFTWARE\WIBU-  
SYSTEMS\CodeMeter\Server\CurrentVersion\ServerSearchList\Server1  
Address=192.168.100.10
```

5.3 APPLYING MAINTENANCE UPDATES TO YOUR WIBU DONGLE

Once a maintenance update has been purchased, to update maintenance on your Wibu dongle:

1. On a computer which has **internet access**, insert your **Wibu dongle** into a USB port. Remove any other Wibu dongles that you may have for other products.
2. Run the **GetData License Manager** located in the installation folder of Forensic Explorer. The default location is: **C:\Program Files\GetData\Forensic Explorer vx\License Manager.exe**
3. The GetData License Manager will **detect your Wibu dongle**, as shown in Figure 26 below. The existing Maintenance expiration date is displayed in the Maintenance column:

Figure 26, GetData License Manager



4. Select **"Forensic Explorer"** from the product list and press the **ADD button**.
5. In the **Add Licenses** window, enter the **"License"** key that you received with your renewal order. Press the **Search** key.
6. Select the renewal from the available product list. Then click the **Apply** button.
7. Return to the main screen of the License Manager. Click the refresh button to display the new maintenance date.

For further assistance in applying maintenance updates to your Forensic Explorer dongle, please contact support@getdata.com (see Appendix 1 - Technical Support for full contact details).

Chapter 6 - Forensic Acquisition

In This Chapter

CHAPTER 6 - FORENSIC ACQUISITION

6.1	Write block	44
6.2	GetData's Forensic Imager	45
6.2.1	Installation	45
6.2.2	System Requirements	45
6.2.3	Protected Disk Areas - HPA and DCO.....	45
6.2.4	Running Forensic Imager	46
6.2.5	1. Selecting the source.....	47
6.2.6	2. Selecting the destination	48
6.2.7	3. Progress	53
6.2.8	4. Log file.....	53
6.2.9	Bad Sectors and error reporting	54

6.1 WRITE BLOCK

IMPORTANT:

An accepted principal of computer forensics is that, wherever possible, source data to be analyzed in an investigation should not be altered by the investigator.

If physical media such as a hard drive, usb drive, camera card etc. is a potential source of evidence, it is recommended that when the storage media is connected to a forensics workstation it is done so using a Forensic write block device.

A Forensic write blocker is usually a physical hardware device (a write blocker) which sits between the target media and the investigators workstation. It ensures that it is not possible for the investigator to inadvertently change the content of the examined device.

There are a wide variety of forensic write blocking devices commercially available. Investigators are encouraged to become familiar with their selected device, its capabilities and its limitations.

Shown in Figure 27 below is a Tableau USB hardware write block. The source media, an 8 GB Kingston USB drive is attached and ready for acquisition:

Figure 27, Tableau USB write block with USB as the source drive



6.2 GETDATA'S FORENSIC IMAGER

Installed with Forensic Explorer is the standalone forensic imaging tool “**Forensic Imager**”. Forensic Imager is a Windows based program that will acquire a forensic image into one of the following common forensic file formats (described in more detail later in this chapter):

- DD /RAW (Linux “Disk Dump”)
- AFF (Advanced Forensic Format)
- E01 (EnCase®) [Version 6 format]

6.2.1 INSTALLATION

Forensic Imager is installed with Forensic Explorer into its installation folder:

C:\Program Files\GetData\Forensic Explorer v1\ForensicImager.exe

6.2.2 SYSTEM REQUIREMENTS

Forensic Imager should be **run as local Administrator** to ensure that sufficient access rights are available for access to devices.

Forensic Imager requires the following minimum specification:

- Windows 7 or above;
- 32 and 64bit compatible;
- Pentium IV 1.4 GHz or faster processor;
- 1GB RAM.

Forensic Imager does NOT support DOS acquisition. If acquisition from a DOS boot disk is required alternative forensic acquisition software should be used.

6.2.3 PROTECTED DISK AREAS - HPA AND DCO

Host Protected Area (HPA) and Device Configuration Overlay (DCO)

The HPA and DCO are two areas of a hard drive that are not normally visible to an operating system or an end user. The HPA is most commonly used by booting and diagnostic utilities. For example, some computer manufacturer's use the area to contain a preloaded OS for install and recovery purposes. The DCO “allows system vendors to purchase HDDs from different manufacturers with potentially different sizes, and then configure all HDDs to have the same number of sectors. An example of this would be using DCO to make an 80 Gigabyte HDD appear as a 60 Gigabyte HDD to both the OS and the BIOS” (1)

Whilst the HPA and DCO are hidden, it is technically possible for a user to access these areas and store/hide data. Forensic Imager does **not** currently support the acquisition of HPA or DCO areas.

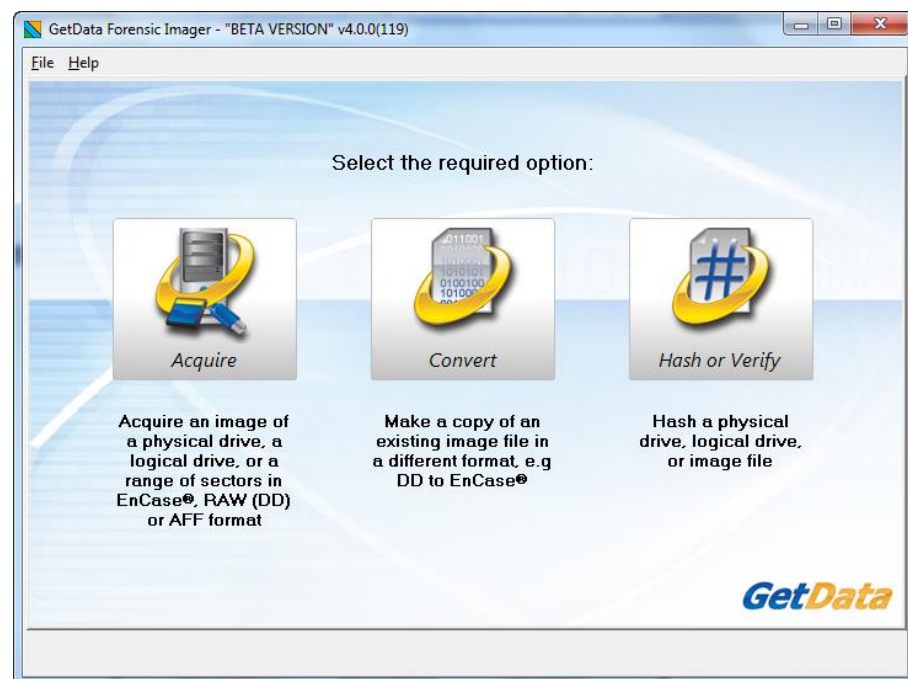
6.2.4 RUNNING FORENSIC IMAGER

Forensic Imager is located in the Forensic Explorer installation folder as a stand-alone executable. When Forensic Imager is run the investigator is presented with 3 options:

- Acquire:** The acquire option is used to take a forensic image (an exact copy) of the target media into an image file on the investigators workstation;
- Convert:** The convert option is used to copy an existing image file from one image format to another, e.g. DD to E01;
- Hash or verify** The hash or verify option is used to calculate a hash value for a device or an existing image file.

As shown in Figure 28, Forensic Imager below:

Figure 28, Forensic Imager



When “Acquire” or “Convert” is selected, the subsequent work flow is:

1. Select source;
2. Select destination options;
3. Create the image;

4. Display and save event log.

When “Hash or Verify” is selected, the subsequent work flow is:

1. Select source;
2. Verify;
3. Display and save event log.

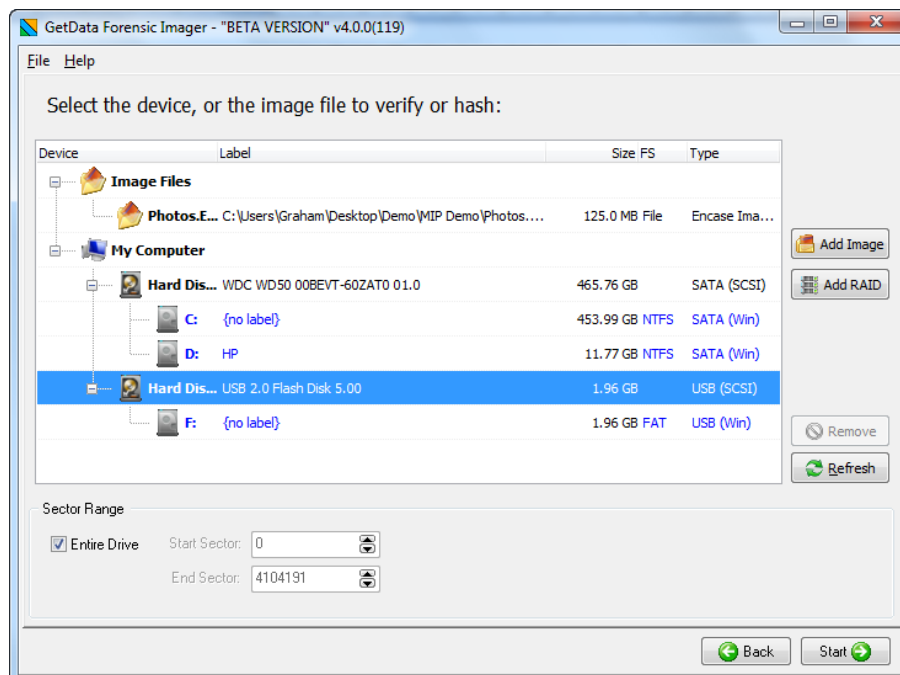
The workflow is discussed in more detail below:

6.2.5 1. SELECTING THE SOURCE

When the “Acquire”, “Convert” or “Hash or Verify” button is selected, the source selection screen is displayed enabling selection of the source media:

- When “**Acquire**” is selected, the source window shows the available physical devices (hard drives, USB drives, camera cards, etc.) and logical devices (partitions or volumes on the physical devices, e.g. "C:" drive) attached to the forensic workstation.
- When “**Convert**” is selected, the source window allows the selection of the source image file. Click the “Add Image” button to add the required image file to the selection list.
- When the “**Hash or Verify**” button is selected, the source window allows the selection of either a physical or logical drive, or an image file.

Figure 29, Forensic Imager - selecting the source device (Hash or Verify option shown)



The device selection window includes the following information:

Label:	Physical drives are listed with their Windows device number. Logical drives display the drive label (if no label is present then "{no label}" is used). Image files show the path to the image.
Size:	The size column contains the size of the physical or logical device, or the size of the image file. (Note that the reported size of a drive is usually smaller than the size printed on the drive label. This is because manufactures report the size in a decimal number of bytes while the Operating System reports the size in 1,024 chunks for each KB).
FS:	The File System on the drive, e.g. FAT, NTFS or HFS;
Type:	Describes the way in which the drive is connected to the computer. An image file will show the type of image (e.g. EnCase® or RAW).

Acquisition of physical vs. logical device

In most situations, pending compliance with any overriding case specific legal requirements, an investigator is most likely to select an image a physical device. Imaging the physical device gives access to the content of the entire media, for example, the space between partitions. Carrier, 2005, observes: *"The rule of thumb is to acquire data at the lowest layer that we think there will be evidence. For most cases, an investigator will acquire every sector of a disk"*. (2 p. 48)

In specific circumstances, an investigator may need to acquire a range of sectors from the device. In this case, start and end sector information is entered in the sector range fields at the bottom of the source selection window.

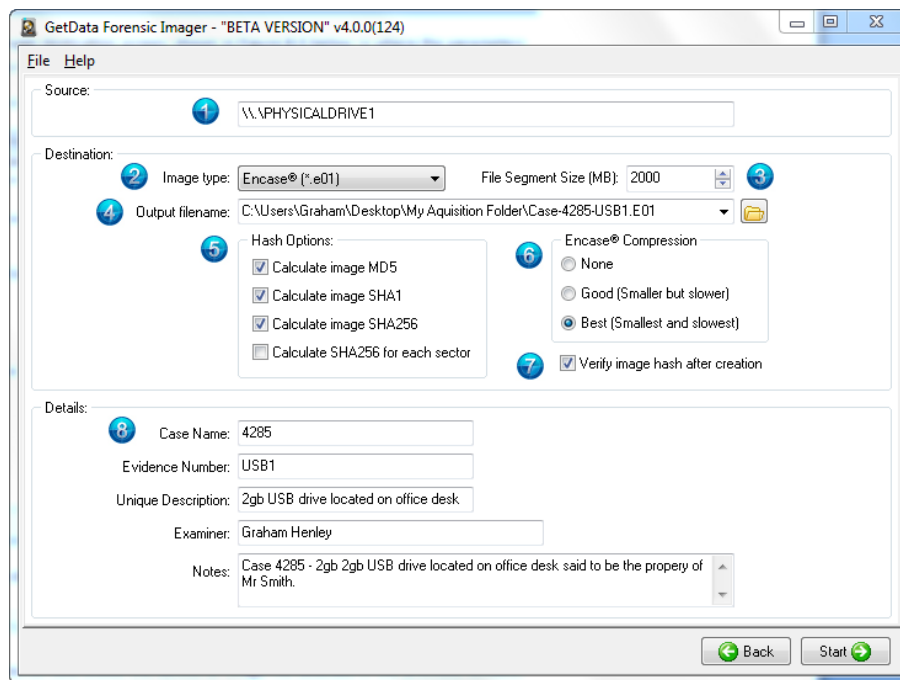
To select the source:

1. **Highlight** the required **device** or **image file** using the mouse;
2. Click the **"Next"** button is clicked to proceed to the destination window.

6.2.6 2. SELECTING THE DESTINATION

The image destination screen, shown in Figure 30 below, is where the parameters for the image file are set, including type, compression, name, location etc.

Figure 30, Setting destination options



1. SOURCE

The source field shows the device or image file selected in the previous window. This source field cannot be edited here. Select the back button if a change to the source is required.

2. IMAGE TYPE

The investigator has the choice of creating the forensic image in one of the following forensic file formats:

DD / RAW:

The DD / RAW format originate from the UNIX command line environment. A DD /RAW image is created from blocks of data read from the input source and written directly into the image file. The simplicity of a DD image makes it possible to compare the imaged data to the source, but the format lacks some of the features found in more modern formats, including error correction and compression.

Advanced Forensic Format (AFF):

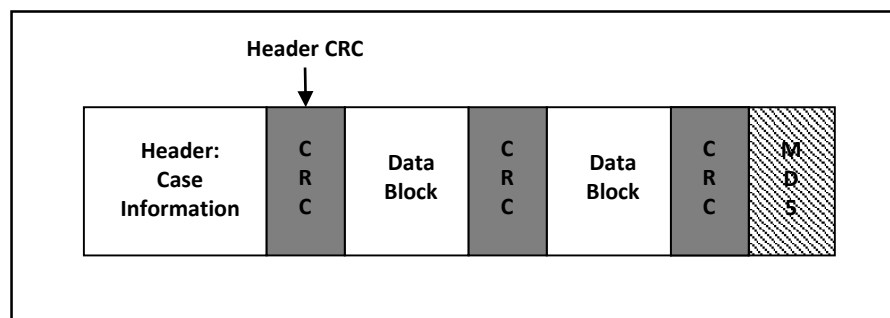
AFF is “an extensible open format for the storage of disk images and related forensic metadata. It was developed by Simson Garfinkel and Basis Technology”. (3). Refer to <http://afflib.org/> for further information.

EnCase®.E01

The EnCase® E01 evidence file format was created by Guidance Software Inc. It is widely accepted in the forensic community as the image file standard. Further

information is available at www.guidancesoftware.com. The structure of the EnCase®.E01 format allows for case and validation information (CRC and MD5) to be stored within the image file. The structure of the EnCase® file format is shown below:

Figure 31, EnCase® header



Source: (4)

3. FILE SEGMENT SIZE

Sets the segment size of the created forensic image file:

This setting enables the forensic image file to be broken into segments of a specific size. Setting an image segment size is primarily used when the forensic image files will later be stored on fixed length media such as CD or DVD.

For the EnCase®.E01 image format, Forensic Imager uses the EnCase® v6 standard and is not limited to a 2 GB segment size. However, if an investigator plans to use larger file segments they should give consideration to the limitations (RAM etc.) of the systems on which the image files will be processed.

4. OUTPUT FILENAME

Sets the destination path and file name for the image file:

The output file name is the name of the forensic image file that will be written to the investigators forensic workstation. Click on the folder icon to browse for the destination folder.

5. HASH OPTIONS

Calculates an MD5 and/or SHA256 acquisition hash of the imaged data:

A hash value is a mathematical calculation that is used for identification, verification, and authentication of file data. A hash calculated by Forensic Imager during the acquisition of a device (the “acquisition hash”) enables the investigator, by recalculating the hash at a later time (the “verification hash”), to confirm the authenticity of the image file, i.e. that the file has not changed. Any change to the acquired image will result in a change to the hash value.

Calculation of HASH values during the acquisition process requires CPU time and will increase the duration of an acquisition. However, it is recommended, in line with accepted best forensic practice, that an acquisition hash is always included when acquiring data of potential evidentiary value. It is also recommended that the investigator regularly recalculate the verification hash during the investigation to confirm the authenticity of the image.

Forensic Imager has three independent hash calculation options, MD5, SHA1 and SHA256. The investigator should select the hash option/s which best suits:

MD5 (Message-Digest algorithm 5):

MD5 is a widely used cryptographic algorithm designed in 1991 by RSA (Ron Rivest, Adi Shamir and Len Alderman). It is a 128-bit hash value that uniquely identifies a file or stream of data. It has been extensively used in computer forensics since the late 1990's.

In 1996 cryptanalytic research identified a weakness in the MD5 algorithm. In 2008 the United States Computer Emergency Readiness Team (USCERT) released vulnerability Note VU#836068 stating that the MD5 hash:

"...should be considered cryptographically broken and unsuitable for further use". (5).

SHA1

In 1995 the Federal Information Processing Standards published the SHA1 hash specification which was adopted in favor of MD5 by some forensic tools. However, in February of 2005 it was announced that a theoretical weakness had been identified in SHA1, which suggests its use in this field may be short lived. (6) (7)

SHA-256:

From 2011, SHA-256 is expected to become the new hash verification standard in computer forensics. SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, and SHA-512) designed by the National Security Agency (NSA), and published by the USA National Institute of Standards and Technology.

For more detailed information on hashing and how the strength of a hash value applies to the forensic investigator suggested reading includes: *"The Hash Algorithm Dilemma—Hash Value Collisions"*, Lewis, 2009, *Forensic Magazine*, www.forensicmag.com.

Sector Hashing

The fourth option in the hash section is **"Calculate SHA-256 for each sector"**. When this option is selected a separate SHA-256 hash for each individual sector of the target device is created and stored in the same folder as the image file.

Like the more commonly used “file hash”, a sector hash can be used to:

- Reduce the volume of a data set by excluding known and trusted sectors from the case. For example, the hash of a blank sector can be used as the identifier to eliminate the need to search all blank sectors in the case; or
- To locate fragments of known files. data in a case. For example, an investigator may search for a fragment of a known document or image file and positively identify the existence (or partial existence) of that file on a disk even if only one sector of that file remains on the disk.

For more information on sector hashing, refer to Yoginder Singh Dandass; Nathan Joseph Nécasse; Sherry Reede Thomas, *An Empirical Analysis of Disk Sector Hashes for File carving*, Journal of Digital Forensic Practice, Volume 2, Number 2, 2008, 95-104.

6. ENCASE® COMPRESSION

Sets the compression level for the EnCase® forensic image file

The EnCase®.E01 file format supports compression of the image file during the acquisition process. Compressing a forensic image file during the acquisition process takes longer, but the file size of the forensic image on the investigators workstation will be smaller. The amount of compression achieved will depend upon the data being imaged. For example, with already compressed data such as music or video, little additional compression will be achieved.

AFF and DD/RAW image formats do not support compression.

7. VERIFY IMAGE HASH AFTER CREATION

During the acquisition of a device the “source” hash (MD5 and/or SHA1 and/or SHA256 as per the investigator selection) is calculated as the data is read from the source disk. Once the acquisition is complete, the source hash is reported in the event log in the format:

Source MD5Hash: 94ED73DA0856F2BAD16C1D6CC320DBFA

For EnCase®.E01 files the MD5 acquisition hash is embedded within the header of the image file.

When the “Verify image hash after creation” box is selected, at the completion of writing the image file Forensic Imager reads the file from the forensic workstation and recalculates the hash. The verification hash is reported in the event log in the format:

Verify MD5Hash: 94ED73DA0856F2BAD16C1D6CC320DBFA

At the conclusion of the verification process a comparison is made between the source and verification hash. An exact image of the source disk to the image file should result in a “match”:

MD5 acquisition and verification hash: Match

Should the acquisition and verification hash not match, it is an indication that a problem has occurred and the device should be re-acquired.

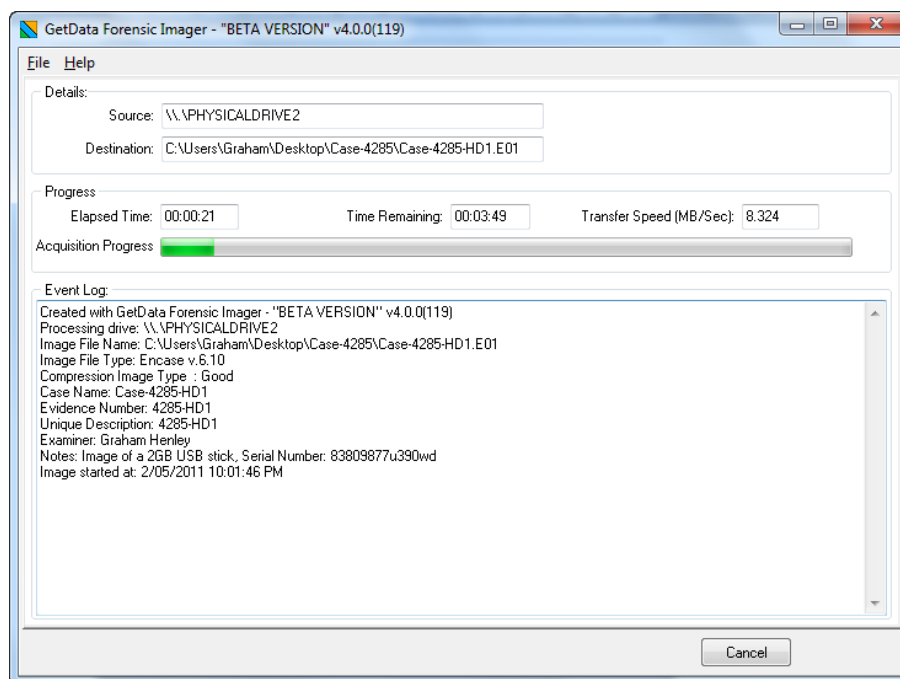
8. DETAILS

For EnCase®.E01 files, information entered into the “Details” field are written into the image file header and stored with the image. DD/RAW and AFF files do not store this information as part of the image, however they are still required to be entered as for all formats the information is included in the Forensic Imager event log.

6.2.7 3. PROGRESS

The progress screen displays source information (the drive being acquired) and destination information (location where the forensic image files is being written). Progress information, including elapsed time, time remaining and transfer speed is displayed. The progress window is shown in Figure 32 below:

Figure 32, Forensic Imager Progress screen



The event log provides feedback to the investigator during the image process.

6.2.8 4. LOG FILE

The event log for each acquisition is automatically saved to the same folder as the image file/s. A typical event log contains the following type of information:

Created with GetData Forensic Imager - v4.0.0(124)

Processing drive: \\.\PHYSICALDRIVE1

Image File Name: C:\Users\Graham\Desktop\My Acquisition Folder\Case-4285-USB1.E01

Image File Type: Encase v.6.10
Compression Image Type: Best
Case Name: 4285
Evidence Number: USB1
Unique Description: 2 GB USB drive located on office desk
Examiner: Graham Henley
Notes: Case 4285 - 2 GB USB drive
Image started at: 4/05/2011 11:45:50 PM
Image finished at: 4/05/2011 11:50:25 PM
Elapsed time: 00:04:34
GUID: {D6BF98CA-F3EA-4BBD-88A9-C5E5B07D8600}
Actual Source MD5Hash: 94ED73DA0856F2BAD16C1D6CC320DBFA
Source SHA1Hash: d11d009c71c089dfcdb3dabad4c4014078c15183
Source SHA256Hash:
3370edc5662703534d3ad539d49bcc7f0ca86f559b7faa3c4dc7f7290056d039
Verify MD5Hash: 94ED73DA0856F2BAD16C1D6CC320DBFA
Verify SHA1Hash: d11d009c71c089dfcdb3dabad4c4014078c15183
Verify SHA256Hash:
3370edc5662703534d3ad539d49bcc7f0ca86f559b7faa3c4dc7f7290056d039
Acquisition completed!
MD5 acquisition and verification hash: Match
SHA1 acquisition and verification hash: Match
SHA256 acquisition and verification hash: Match

6.2.9 BAD SECTORS AND ERROR REPORTING

Disk errors can occur during the image process due to a problem with the entire drive or a problem isolated to specific sectors. If a bad sector is identified, Forensic Imager writes 0's for the data that cannot be read and logs the location of bad sectors in the event log as they are found.

Chapter 7 - Forensic Explorer Interface










In This Chapter

CHAPTER 7 - FORENSIC EXPLORER INTERFACE

7.1	Modules.....	56
7.1.1	Undocking and docking modules	57
7.2	Module data views	59
7.2.1	Undocking and docking data views.....	59
7.3	Customizing layouts.....	61
7.3.1	Save a custom layout	61
7.3.2	Load a custom layout.....	61
7.3.3	Default layout	61

7.1 MODULES

The Forensic Explorer interface is broken down in to a number of **modules** which separate the programs primary functions. Each module is accessed by a tab at the top of the main program screen. The functions of the module are summarized in the following table. More information about each tab can be found by referring to the module specific chapter:

Tab	Function	Chapter & Page
 Home	Case management.	Chapter 10
 File System	Detailed analysis of file systems added to the case.	Chapter 11
 Keyword Search	Keyword search raw case data using simple or RegEx keywords.	Chapter 12
 Index Search	Create and search indexed data using dtSearch technology.	Chapter 13
 Email	Examine PST files.	Chapter 14
 Bookmarks	Add investigator bookmarks to document the analysis.	Chapter 16
 Reports	Create reports.	Chapter 17
 Scripts	Program, manage and run scripts against case data.	Chapter 18
 Registry	View and analyze registry files.	Chapter 15

- Custom Modules:** It is possible to create a custom module. See 18.6 - Custom Modules, for more information.
- Hide Modules at Startup:** It is possible to hide specific modules at program startup. This can be useful when you are providing Forensic Explorer to a non-technical investigator and wish only to show certain modules, such as Index Search and Bookmarks. See 18.4 for more information.

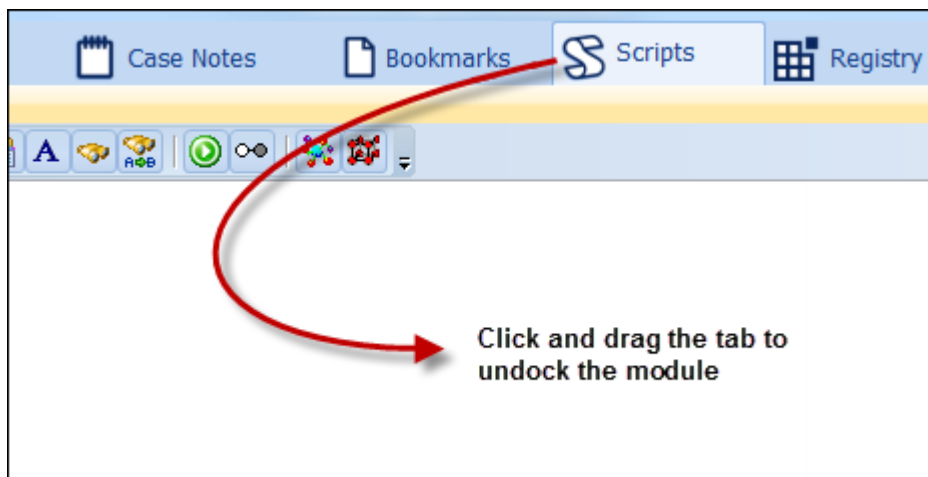
7.1.1 UNDOCKING AND DOCKING MODULES

Forensic Explorer has been designed for use on forensic workstations with **multiple monitors**. Module tabs can be undocked from the main program window and moved across multiple screens.

To undock a module:

1. Select the module tab with the mouse;
2. Hold down the mouse and drag the module tab free of the bar, as shown in Figure 33 below:

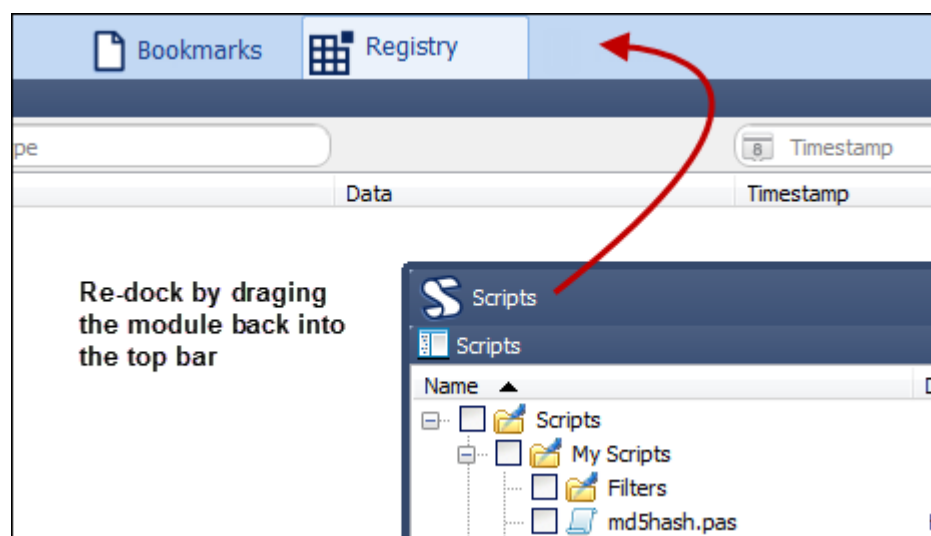
Figure 33, Un-docking a module



To dock a module:

1. Select the top bar of the module window;
2. Drag and drop the module back into the module tab menu bar, as shown in Figure 34 below:

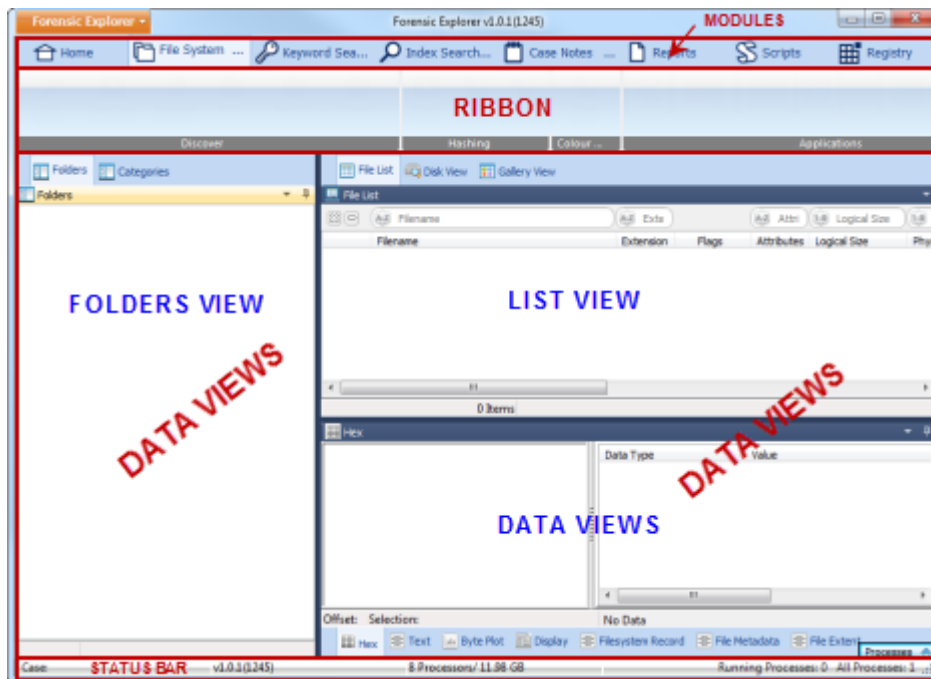
Figure 34, Re-dock a module tab



7.2 MODULE DATA VIEWS

Within each module are one or more “**data views**” which display the data in the case. Data views occupy the three lower panes of the Forensic Explorer module. They operate in a similar fashion to the layout to Microsoft’s Windows Explorer, with a tree (top left), list (top right) and display (bottom) window, as show in Figure 35 below:


Figure 35, Forensic Explorer module layout



Data views are conduits to the examined data. Each data view is designed to expose the investigator to specific information, whether it is lists of file attributes, displaying photos or graphics, detailing file metadata, or dealing with data at a sector or hex level. Data views also contain the tools that are used to display, sort, decode, search, filter, export and report.

More information about each data view is provided in **Chapter 8, “Data Views”**.

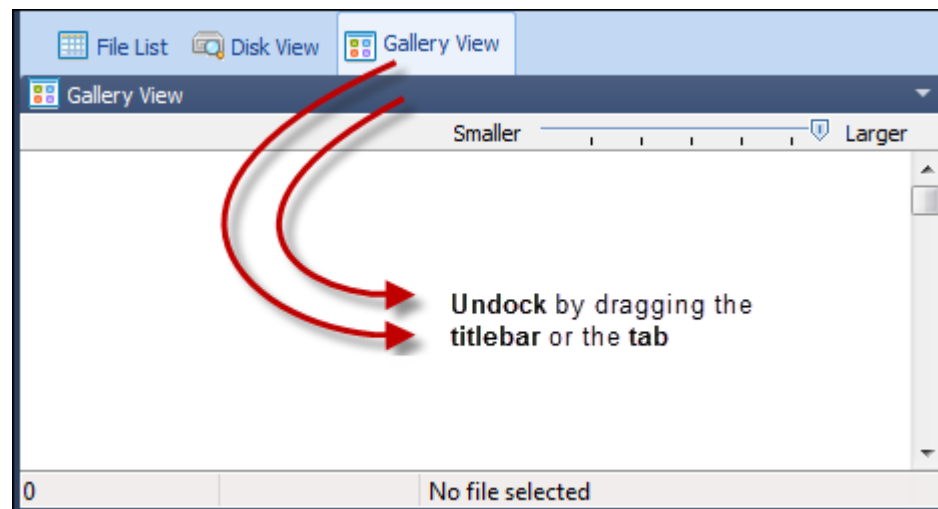
7.2.1 UNDOCKING AND DOCKING DATA VIEWS

Any data view window showing this icon  can be undocked and used as a standalone window.

To undock a data view:

1. Click on the title bar or the data view tab;
2. Hold down the mouse and drag it away from its position, as shown in Figure 36 below:

Figure 36, Undocking a view using drag and drop



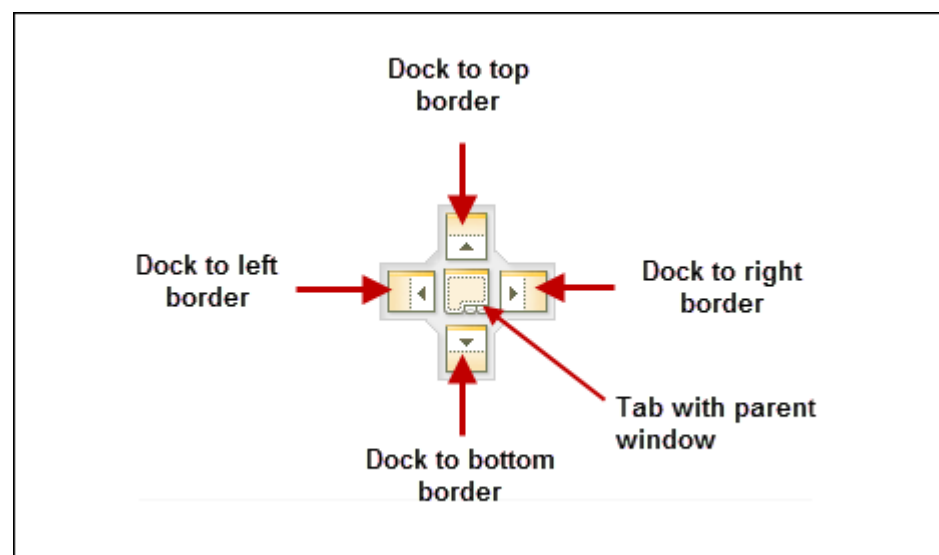
To **dock a data view**:

A data view can only be **re-docked to its parent module**. For example, the File List data view can only be re-docked inside the File System module. It can however be docked to **any position** inside its parent module, including inside another data view.

To dock a data view:

- Click on the data view header and **drag and drop** the header into **next to the other data view tabs** in the required position; or,
- Drag and drop the data view over the **required position arrow** as detailed in Figure 37 below:

Figure 37, Dock positioning arrows



Use the outside position arrows to dock to the larger pane:



7.3 CUSTOMIZING LAYOUTS

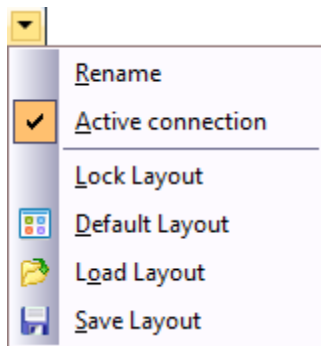
The **position** of modules and data views can be **saved to a file** at any time. This allows the investigator to customize a module for different types of investigations. For example, the module layout for an investigation involving graphics may be different to fraud investigations involving documents.

7.3.1 SAVE A CUSTOM LAYOUT

To **save a custom layout**:

1. In the top right hand corner of any data view, **click on the options drop down arrow** and select **"Save Layout"**:

Figure 38, Layout menu



2. Enter the **name of the .xml layout file** and click the **Save** button.


7.3.2 LOAD A CUSTOM LAYOUT

To **load a custom layout**:

1. In the top right hand corner of any data view, click on the options **drop down arrow** and select **"Load Layout"** (as shown in Figure 38 above);
2. Select the desired .xml layout file and click the **Open** button.

7.3.3 DEFAULT LAYOUT

To **return to the default layout**:

1. In the top right hand corner of any data view, click on the options drop down arrow  and select **Default Layout** (as shown in Figure 38 above).

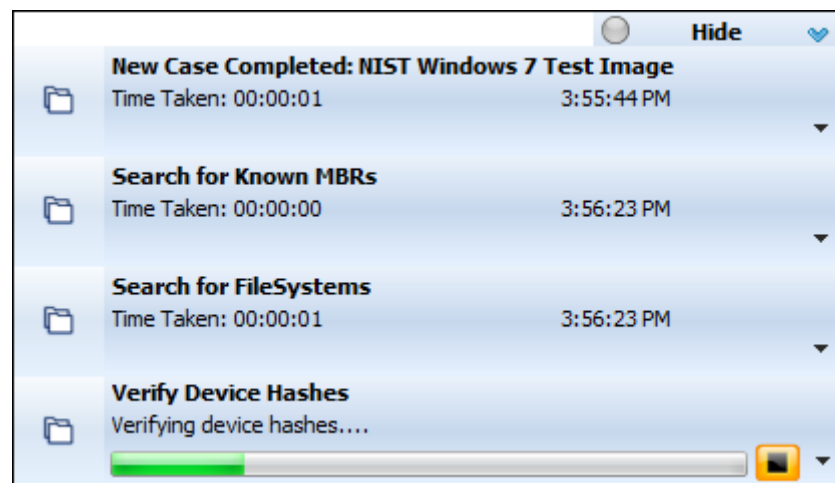
7.4 TASK PROCESSES LIST

In a Forensic Explorer case numerous processing tasks will be performed on the evidence. This includes:

- **administrative tasks:** such as creating and saving case files;
- **processing tasks:** such as reading and displaying a file system; and
- **investigations tasks:** such as signature analysis, file hashing, file carving, running scripts, create indexes etc.

Processes are tracked in the **processes list**, accessed from any Forensic Explorer Module in the bottom right hand corner of the main program screen:

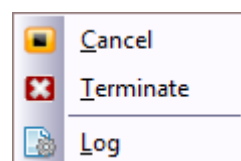
Figure 39, Forensic Explorer processes window



The purpose of the list is to:

- **Visually show** the progress of running processes;
- **Identify processes which have completed**, their duration and the time completed;
- **Cancel** a running process. The cancel button terminates a thread gracefully.
- **Terminate** a thread that not responding to the cancel process:
- Allow access to process **logging** (see 7.5 below).

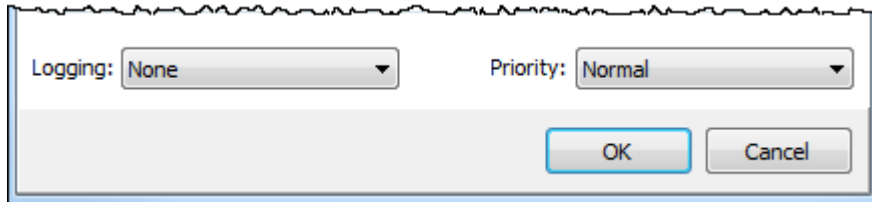
Figure 40, Accessing Process Cancel and Terminate options via the Processes window drop down menu



7.5 PROCESS LOGGING AND PRIORITY

When a task is run in Forensic Explorer the investigator can set Logging and Priority options, as shown in Figure 41 below:

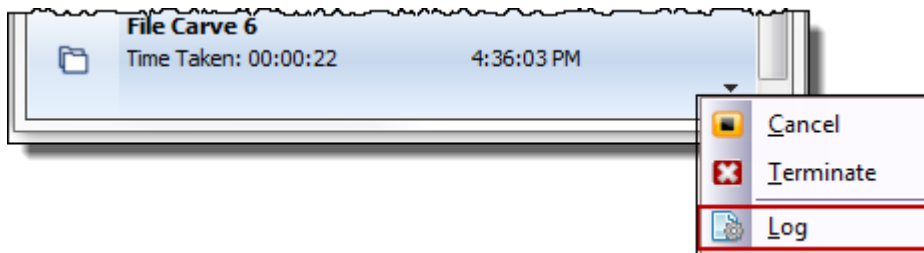
Figure 41, Setting Logging and Priority options



7.5.1 LOGGING

The “Logging” setting determines the detail of case process logging. Case log files are accessed by clicking the drop down arrow for the process in the process list (Note: If logging is set to “None” then the link to the log file will be greyed out):

Figure 42, Access Process Log Files



Case log files are stored in the path: “[User]\Documents\Forensic Explorer\[Case Name]\Logs\”.

Application log files are stored in the path: “[User]\Documents\Forensic Explorer\AppLogs\”.

7.5.2 PRIORITY

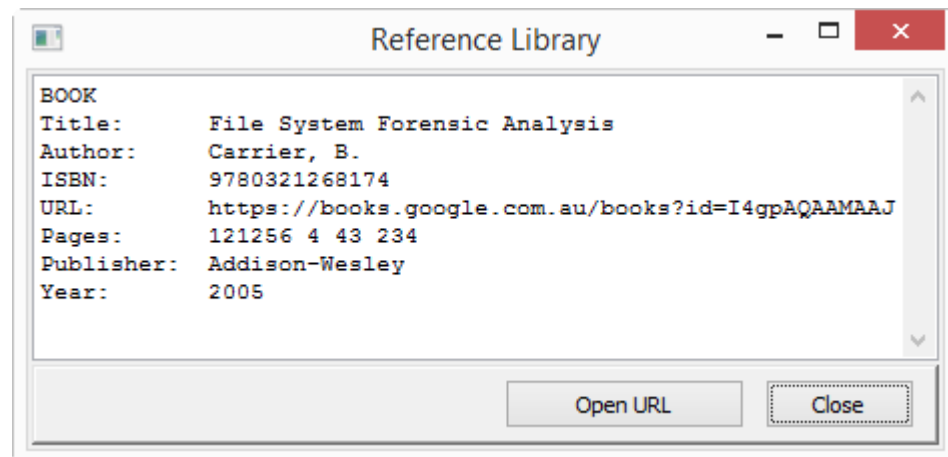
The priority setting is used to determine the number of computer processors allocated to the task. “Low Priority” is allocated a single processing core. “Normal” and above are allocated multi-processing cores (if available).

Important: The speed of multi-core process is influenced by computer hardware. With insufficient hardware resources multi-core can lead to data bottlenecking and be slower than single core process. It is recommended that users test the speed of their hardware to ensure maximum processing speed.

7.6 REFERENCE LIBRARY

The purpose of the Reference Library is to put personal reference resources within easy reach of the investigator from within the Forensic Explorer interface. Reference information can be citation information only, or a link to an online resource or a local file.

Figure 43, Display of a Reference in Forensic Explorer

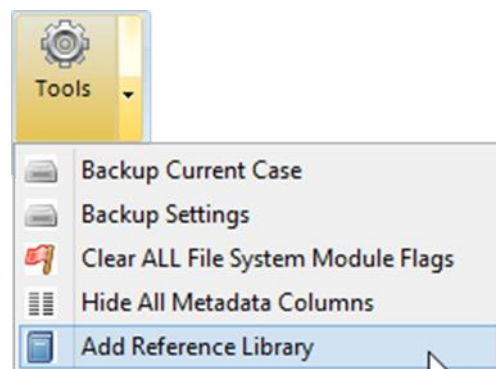


7.6.1 ADDING A REFERENCE LIBRARY TOOLBAR BUTTON

To add the Reference Library toolbar button:

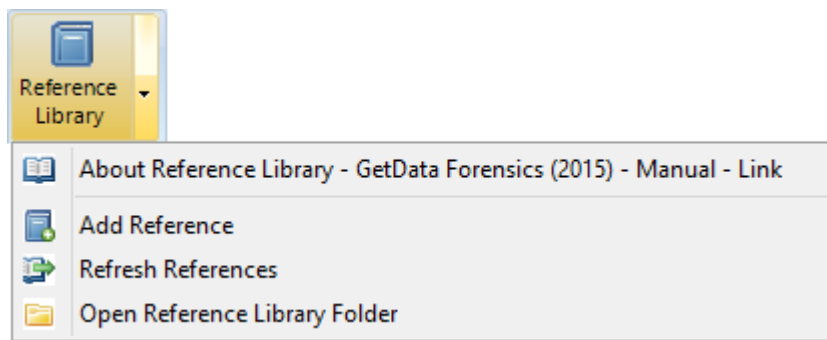
- Select File System Module > Tools > Add Reference Library, as shown in Figure 44, adding a Reference Library button to the toolbar below:

Figure 44, adding a Reference Library button to the toolbar



A Reference Library button is then added to the File System module toolbar. By default, the drop down menu is populated with a sample reference item (this guide):

Figure 45, Reference Library default listing



The reference is listed in the format: Title – Author (Year) – Type (if the reference has a link, a **Link** is added.

7.6.2 REFERENCE LIBRARY ITEMS

Reference items displayed in the drop down menu are dynamically generated by the content of the file:

[User]\Forensic Explorer\Reference Library\References.txt

Access to this folder and file using the **Open Reference Library Folder** menu option.

References.txt is in **BiBTeX** format. BiBTeX is a common citation format used by many popular citation programs and websites, including sites such as Google Books. A BiBTeX record has the following format (where @ indicates the start of the reference and }, indicates the end of the reference):

```
@book{carrier2005file,  
  title={File System Forensic Analysis},  
  author={Carrier, B.},  
  isbn={9780321268174},  
  url={https://books.google.com.au/books?id=l4gpAQAAMAAJ},  
  year={2005},  
  publisher={Addison-Wesley},  
  pages={121},  
},
```

Additional information about the BiBTeX structure can be found at:

- <http://en.wikipedia.org/wiki/BibTeX>, or;
- <https://www.cs.arizona.edu/~collberg/Teaching/07.231/BibTeX/bibtex.html>


7.6.3 ADDING A REFERENCE TO THE REFERENCE LIBRARY

There are a number of ways to manage the items listed in the Reference Library menu:

1. ADD REFERENCE VIA THE DROP DOWN MENU OPTION

The **Reference Library > Add Reference** menu option, shown in Figure 45 above, opens the **Add a Reference** window. The window is completed information known about the reference source, with Title being the only required field:

Figure 46, adding a Reference item



When the Create button is pressed, the information in the window is written into the References.txt file in the BiBTeX format. Click the **Refresh References** button in the drop down menu to show the new reference in the drop down menu.

2. MANUALLY EDIT THE REFERENCES.TXT FILE

The References.txt file can be manually edited. It is usually most effective to copy and paste a previous entry as a template and then update it with the new reference information. Be sure to use the BiBTeX schema.

3. COPY AND PASTE FROM A 3RD PARTY SITE

Visit a site like Google Books (for example:
<https://books.google.com.au/books?id=I4gpAQAAMAAJ>):

1. Select a reference item and look for the option to Export Citation (usually at the bottom of the reference description page) where BiBTeX is one of the citation formats offered.
2. Download and open the BiBTeX file in notepad.
3. Copy and paste the BiBTeX citation into the References.txt file and save the change.
4. Click the Refresh References button in the Reference Library toolbar.
5. The reference will now be listed in the Reference Library drop down menu.

Other third party sites, such as <https://www.citethisforme.com/> enable the management of a complete citation list. The entire list can be exported in BiBTeX format and added to Forensic Explorer using the procedure described above.

7.6.4 LINKING A REFERENCE TO A WEBSITE OR LOCAL FILE

A BiBTeX entry can include a url statement which is used to link to a web page or a local file.

- A link to a **web site**, will included a BiBTeX url in the format:

url={http://en.wikipedia.org/wiki/Computer_forensics},

- A link to a **local file** will include a BiBTeX url in the format:

url={C:\Program Files (x86)\GetData\Forensic Explorer v3\Forensic Explorer User Guide.en.pdf},

- If the file is located in the **[User]\Forensic Explorer\Reference Library\ folder**, only the file name is required, e.g.

url={About Reference Library.rtf},

Chapter 8 - Data Views

In This Chapter


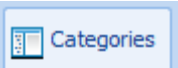
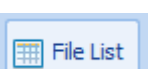
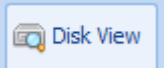
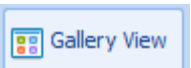

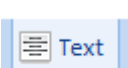
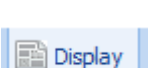

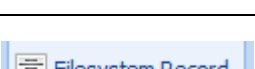
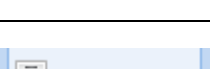
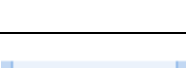
CHAPTER 8 - DATA VIEWS


8.1	Data views summary	71
8.1.1	Components of a data view	72
8.1.2	data views relationships in the file system module	72
8.2	Tree view	74
8.2.1	Navigating Tree view	74
8.2.2	Tree view filter	74
8.2.3	Branch plate	75
8.3	List view	77
8.4	Disk view	78
8.4.1	Resizing the Disk view display	79
8.4.2	Color Coded Content	79
8.4.3	Navigating Disk view	80
8.4.4	Selecting data in Disk view	82
8.5	Gallery view	84
8.5.1	Caching thumbnails to disk	84
8.5.2	Increase the number of graphics displayed	85
8.5.3	Working with data in Gallery view	85
8.6	Hex view	86
8.7	Text view	88
8.8	Display view	89
8.8.1	Video Thumbnails	90
8.9	Byte Plot and Character Distribution	91
8.9.1	Byte Plot examples	92

8.10	Filesystem Record view	96
8.11	File Metadata.....	98
8.11.1	Extract Metadata to File List Columns	98
8.12	File Extent	100

8.1 DATA VIEWS SUMMARY

Each of the Forensic Explorer module tabs contains one or more of the following data views:

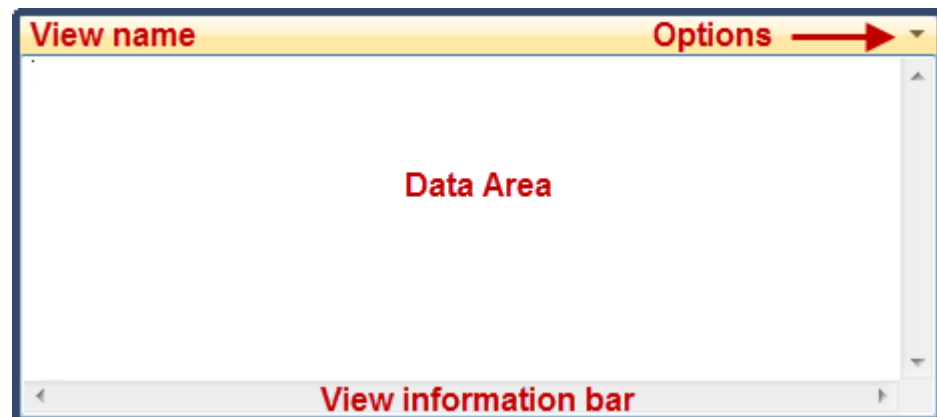
Data View Tabs	Function
 Folders	Shows the folder structure of the examined device.
 Categories	Separates artifacts into categories, including files by extension, files by modified date and flagged files.
 File List	Lists individual items and displays their metadata in columns.
 Disk View	A graphical display of the sectors which make up the examined device.
 Gallery View	A thumbnail presentation of the graphics files.
 Hex	Hexadecimal view of the currently highlighted item. Automatic interpretation of user selected data.
 Text	Text view of the currently highlighted file.
 Display	Content display of currently highlighted file. Displays of 300 + different file types including video and audio.
 Byte Plot	A graphical representation of byte level data within the currently highlighted file.
 Filesystem Record	Displays information contained in the MFT record or FAT entry for the currently highlighted file.
 File Metadata	A breakdown of files metadata components.
 File Extent	Details the start, end and length of each data run on the disk.

	Shows the bookmark details associated with the item.
---	--

These views are described in more detail below.

8.1.1 COMPONENTS OF A DATA VIEW

Figure 47, Data view layout



View Name: The view name describes the function of the view, e.g. “Hex” displays a hexadecimal view of the currently highlighted item. The options button ▼ provides the option to rename a view with a custom name.

Data Area: The data area of the view is where the content of the highlighted item is displayed to the investigator.

View information bar: The information bar at the bottom of a view. It provides details on the data currently displayed in that view. It is an important navigational reference. The information bar can contain information such as:

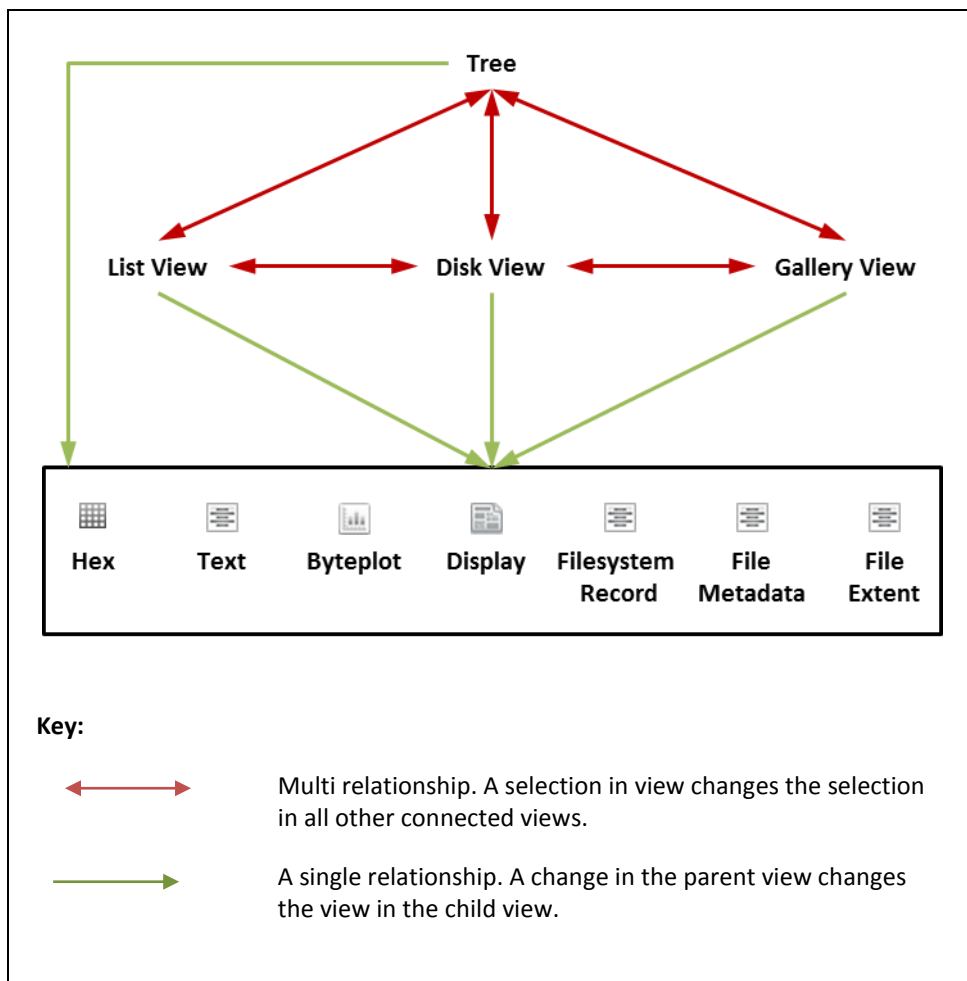
- The full path to the currently highlighted item;
- The currently selected physical sector.

8.1.2 DATA VIEWS RELATIONSHIPS IN THE FILE SYSTEM MODULE

Forensic Explorer data views within a module co-exist in linked relationships. In simplest terms, when a file is highlighted in one view, the other views also change to show that data.

Note: Data views between different modules are **NOT** linked. For example, the Hex data view in the File System module acts independently from the Hex data view in the Keyword Search module.

Figure 48, Relationships between data views



8.2 TREE VIEW



A Tree view is a hierarchical display of items (e.g. devices, partitions, folders, registry key folders, keywords etc.). Like Microsoft's Windows Explorer, the Tree view is most commonly used to select a folder, causing the contents of the folder to be displayed in the adjacent List view.

The default position for a Tree view is in the top left window. The actual name of the Tree view changes according to the module, i.e.:

Module	Tree view Name	More Information
File System	Folders	Chapter 11
Keyword Search	Keyword Tree	Chapter 12
Bookmarks	Bookmark Tree	Chapter 16
Registry	Registry Tree	Chapter 15

8.2.1 NAVIGATING TREE VIEW

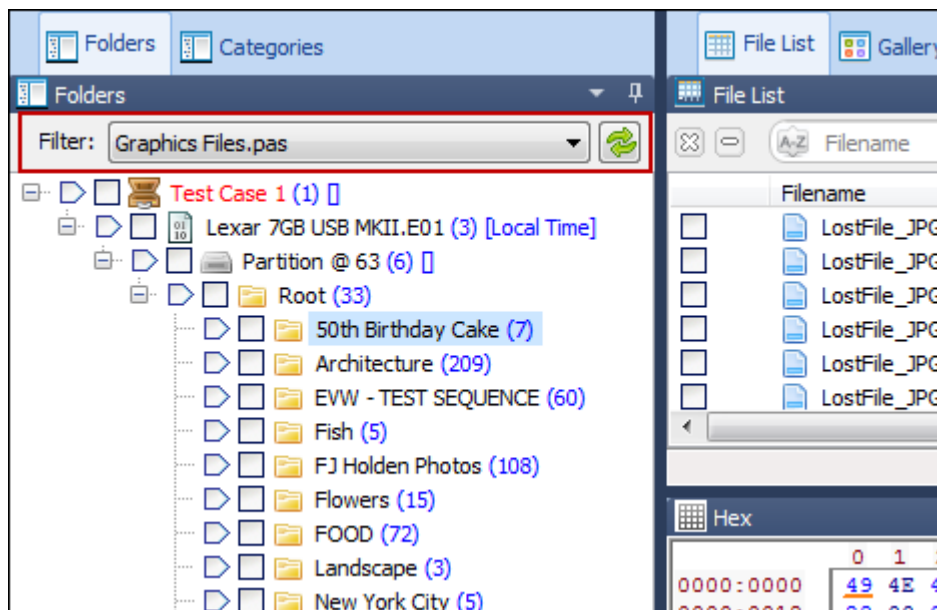
To **navigate** Tree view:

- Use the **keyboard arrow keys** to traverse, expand and contract the tree;
- **Double click a Folder** to drill down into its sub folders; or
- **Click the  and  symbols** to expand and contract the tree hierarchy; or
- **Right click** and use **"Expand All"** to expand the currently highlighted folder, or **"Expand All"** to expand all folders; use **"Contract"** to contract the currently highlighted folder, or **"Contract All"** to contract all folders.

8.2.2 TREE VIEW FILTER

Some Tree views contain a filter drop down menu, as shown in Figure 49:

Figure 49, Tree view filter




A tree view filter is used to display only the folders which match set criteria. For example, applying the “Graphics Files.pas” filter will show only folders containing graphics files. The File list view in the right hand window will also only show the applied filter criteria.

Tree view filters are created using scripts. For more information on creating a Tree view filter, see 0- Filters.

8.2.3 BRANCH PLATE

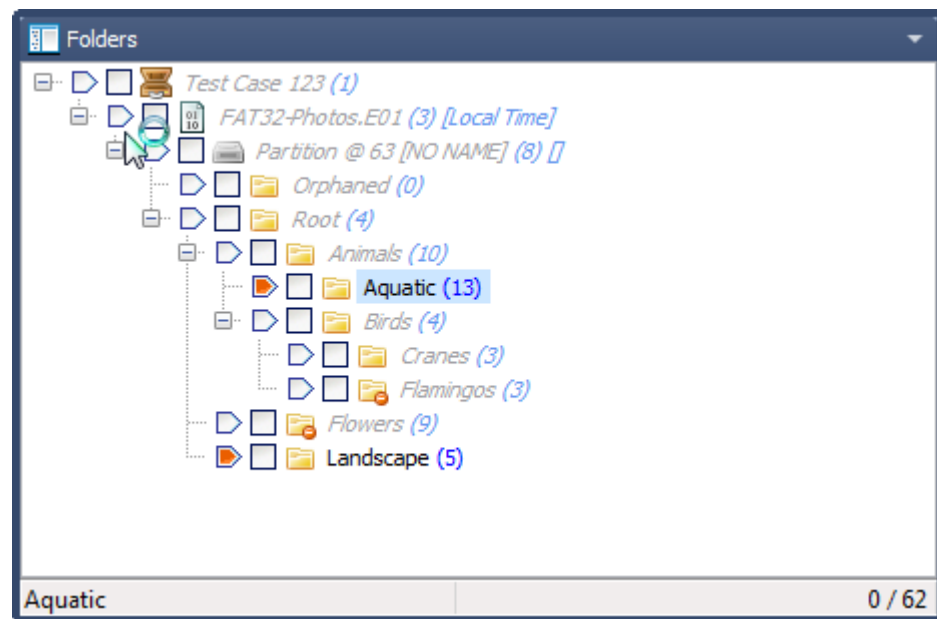
One of the most powerful features of Tree view is the “branch plate”. When a branch plate is selected, all items beneath that plate are displayed as a single list in List view. For example, this action can be used to display the contents of a folder and all of its sub folders and files.

To **branch plate**, click the required plate with the mouse. When the plate turns orange,  it is active.

To **plate multiple branches**;

1. Click the first required plate with the mouse;
2. Hold down the CTRL key and click the other required plates.

Figure 50, File System module, Folders view, branch plate with “Aquatic” and “Landscape” folders plated



Plated folders are displayed in **normal font**. The non-plated folders are in **grey italic**.

The blue number in brackets, e.g. “**(2)**” counts the number of items inside the folder (but does not count the contents of sub folders).

To **turn off the branch plate**:

- Right click in the **File System** module **Folders View**, or in the like tree view of other modules (plating operated independently in each module), and select **Branch Plating > Branch Plate Off**. When branch plating is turned off the tree works in a similar fashion to Windows Explorer.

8.3 LIST VIEW

A List view displays individual items (e.g. files) and their metadata (e.g. file name, size, modified date, created date, etc.) in a table format.

The default position for a List view is in the top right window. The actual name of the List view changes according to the module, i.e.:

Module	List View Name	More Information
File System	File List	Chapter 11
Keyword Search	Keyword Result List	Chapter 12
Bookmarks	Bookmarks List	Chapter 16
Registry	Registry List	Chapter 15

List view allows items (such as: files, notes, keyword search results and registry entries) to be sorted, highlighted, checked, flagged, opened and exported. For more information, see Chapter 9 - Working with data.

8.4 DISK VIEW

The default location for Disk view is the top right hand window of the File System module, accessed via the Disk View tab:

Figure 51, Disk View tab



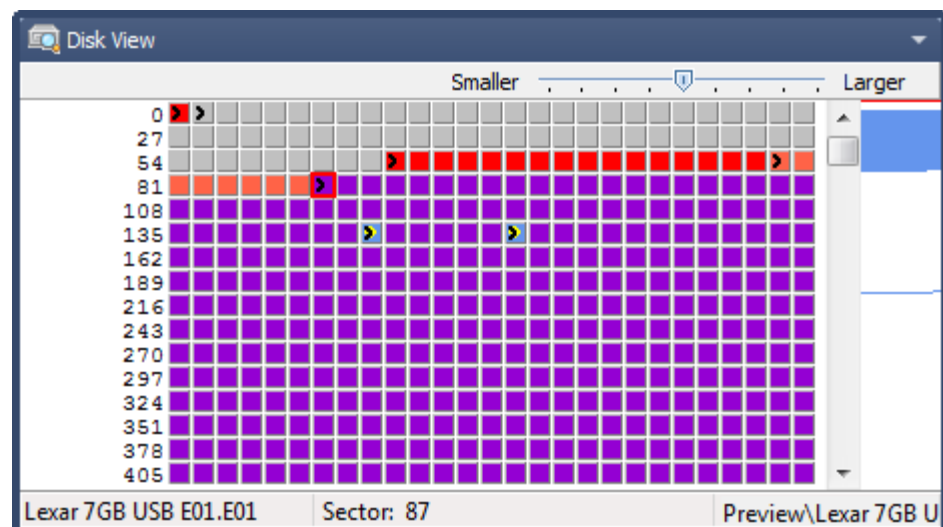
Disk view is a graphical display of the sectors which make up the examined device. Disk view can be used to:

- Obtain a **graphical overview of items** which make up the device (e.g. MBR, VBR, FAT, MFT, files, deleted files, unallocated clusters etc.).
- Quickly **navigate to a desired sector** on the device (see “Navigating Disk view” below);
- **Select sectors for examination** in other Forensic Explorer views (e.g. Hex view, Text view etc.). The selection can include a single sector, a range of sectors, or an entire item.

To open Disk view:

- Open a case or preview evidence;
- Go to the File System module;
- In the left pane, **select the device** (or an item in the file system of the device) to view;
- In the right pane, **select the Disk View tab**

Figure 52, Disk view



8.4.1 RESIZING THE DISK VIEW DISPLAY

The number of sectors shown in Disk view can be dynamically adjusted using the slider bar:














Figure 53, Disk view scale bar



Large scale can be used for examining small groups of individual sectors. Small scale can provide a graphical representation of the data structure on the disk and can also be used to quickly identify content (see 8.4.2 - Color Coded Content below).

8.4.2 COLOR CODED CONTENT

Disk view opens with the following default color coding representing the content of sectors (color coding sourced from http://en.wikipedia.org/wiki/Web_colors):

- > The start sector of a file
 -  Currently selected sector
 -  One type overlays another
-
-  MBR/VBR (Red)
 -  FAT 1 (DarkViolet)
 -  FAT 2 (WebViolet)
 -  \$MFT (DarkViolet)
 -  System files (WebTomato)
 -  \$MFT resident file (the file overlays the \$MFT)
 -  Folder (DeepSkyBlue)
 -  Allocated File (CornFlowerBlue)
 -  Unallocated space (LtGray)
 -  Deleted file (A deleted file overlays unallocated space)
 -  Carved file (DarkOrange: Carved file overlays unallocated space)

CUSTOM DISK VIEW COLORS

Disk view colors can be customized. For example, it is possible to:

- show a file type, e.g. JPGs as a specific color; or

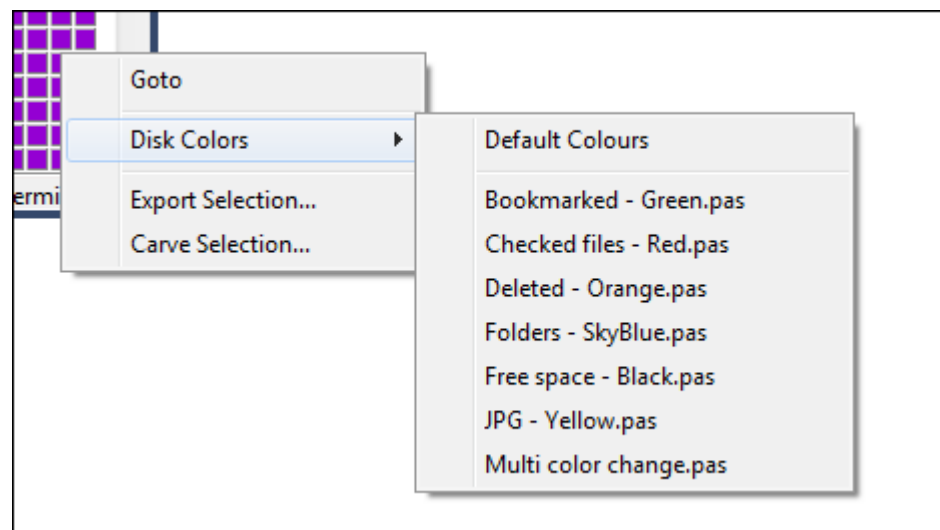
- change the color of a file type over a certain size to a specific color; or
- show a specific file, e.g. “sample.txt” as a specific color.

Custom Disk view colors are defined using Forensic Explorer scripts located in the “Scripts > Disk View” folder. (Learn more about scripting in Chapter 18 - Scripts Module).

To **change Disk view colors** using a script:

1. **Right click** in the Disk view window;
2. Select “**Disk Colors**” from the drop down menu;
3. Select the **required Disk view colors script**.

Figure 54, Right-click Disk View menu links to scripts



To reset Disk view colors to default;

1. **Right click** in the Disk view window;
2. Select **Disk Colors > Default Colors**.

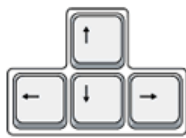
8.4.3 NAVIGATING DISK VIEW

DISK VIEW MAP

The vertical bar on the right hand side of the disk view window (shown in Figure 56 below) is a map to allocated space on the examined device. Use the vertical scroll bar to quickly navigate to the colored section which identifies allocated disk space.

KEYBOARD NAVIGATION

The following commands are available for navigation in Disk view:



Navigate sectors using the **arrow keys**



First and last sectors are reached using the **home** and **end keys**:



Pages of sectors can be scrolled using the **Page Up** or **Page Down** keys.

Mouse Scroll

Scroll by row using the mouse. Hold down the SHIFT key to scroll by page.

Or use the following keyboard shortcuts to go to:

D	Next deleted file
E	Entry
F	Free Space
N	Next File
Ctrl N	Next different type
P	Previous file
Ctrl P	Previous different type
S	System
U	Unallocated

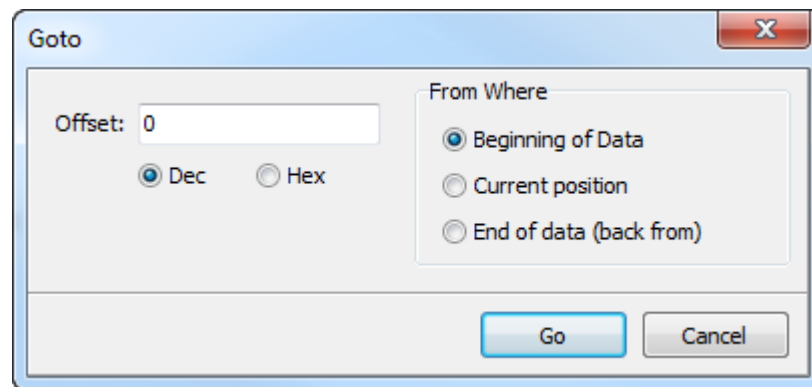
DISK VIEW GOTO

Disk view has a Goto command that allows the investigator to quickly jump to the desired sector.

To open and use the Goto window:

- Right mouse click in the Disk view;
- The following window will appear;

Figure 55, Disk view Goto window



- In the “Offset field, enter the required sector, then press the Go button.

8.4.4 SELECTING DATA IN DISK VIEW

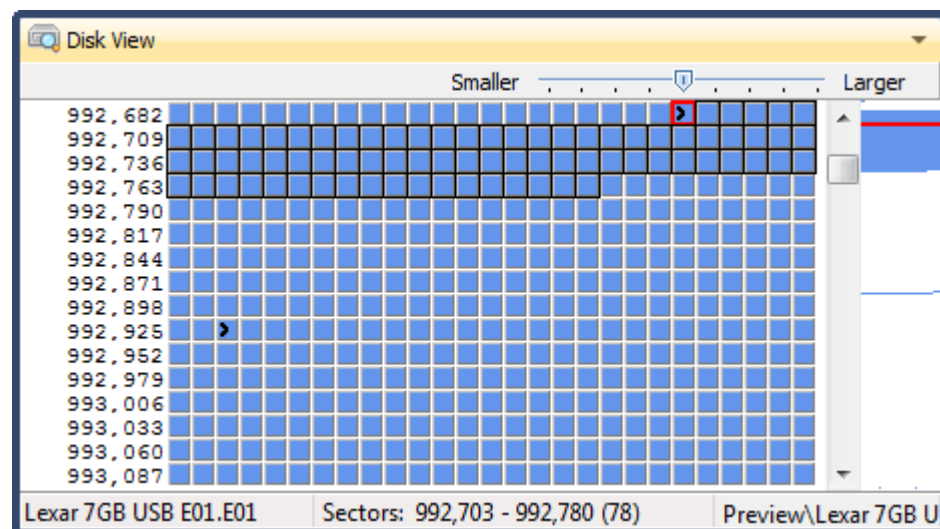
To select a **sector**:

- Click on a sector with the mouse. The selected sector will be marked with a red border.

To select a **range of sectors**:

- Click on a sector with the mouse;
- Hold down the mouse key and drag the mouse over the required range of sectors. The range of sectors will show as selected, as see Figure 56 below. This enables other views, such as HEX view to see the selected range;

Figure 56, Selecting a range of sector in Disk view

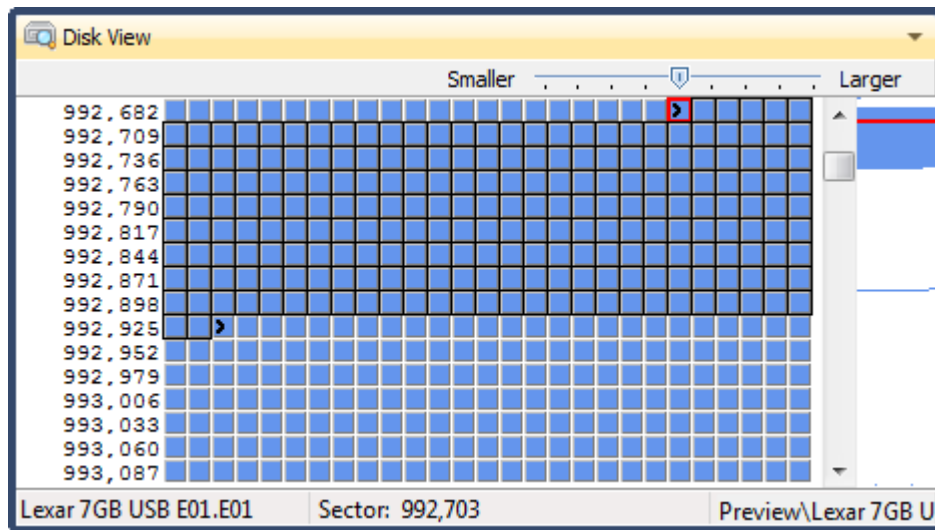


To select a **file**:

- Double click a sector. All sectors used by the file will be identified;

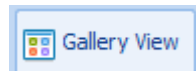
- The name of the selected file is displayed in the status bar at the bottom of the Disk view window, as shown in Figure 57 below;

Figure 57, A selected file in Disk view



8.5 GALLERY VIEW

The default location for Gallery view is the top data view window of the File System module, accessed via the Gallery View tab:



Gallery view is fast ways to thumbnail graphics located in the case.

Figure 58, Gallery view thumbnails



Graphics displayed in Gallery view are determined by the **selection made in the Tree view**. If a single folder is highlighted, the graphics inside that folder will be displayed. When the branch plate option is used (see paragraph 8.2.3 - Branch plate) all graphics in the plated path will be displayed.

The **default setting for Gallery view** is to display **Jpeg, Bmp and Png** file types.

The file icon at the bottom of the thumbnail is a visual identifier of the status of the file (e.g. bookmarked, deleted, carved, etc.).

8.5.1 CACHING THUMBNAILS TO DISK

When a thumbnail is displayed it is written to the disk cache file:

... \User\Documents\Forensic Explorer\Cases\[Case Name]\thumb.cache

When changing between Gallery view folders, Forensic Explorer first checks the cache file to determine if the graphic has previously been displayed. If so, the cached graphic is used.

In some situations it may be advantageous to cache all available images. For example, if running the "Skin Tone Analysis" script (from File System module > Analysis Scripts

button > Skin Tone Analysis) the script will run 50% faster when reading images from the cache.

To cache all thumbnails to disk:

1. When adding evidence:
 - a. When an evidence item is added to a preview or a case, there is an opportunity in the Evidence Processor window (see 10.5) to “Cache Thumbnails”.
2. During a case:
 - a. Select or branch plate the required folders in the File System module.
 - b. Right click in the gallery view window and select “Cache All Images”.

The cache progress will show in the processes window.

8.5.2 INCREASE THE NUMBER OF GRAPHICS DISPLAYED

The size and number of graphics displayed is controlled by moving the slide-bar in the footer of this window from small to large.

Figure 59, Gallery view scale bar



The Gallery view tab can also be detached from the File List view pane and re-sized displayed as a standalone window (see 7.3.1- Save a custom layout, for more information).

8.5.3 WORKING WITH DATA IN GALLERY VIEW

Graphics in Gallery view can be **highlighted**, **checked**, **flagged**, **exported**, **bookmarked** and **opened** with an external application. These commands are access by the right click display menu. For more information on these actions, see Chapter 9 - Working with data.

To **highlight a continuous group of multiple files** in Gallery view, hold down the **SHIFT** key whilst selection files with the mouse.

To **highlight a non-contiguous group of multiple files** in Gallery view, use the **CTRL** key when selecting files with the mouse.

To **check** highlighted files, press the **space bar**.

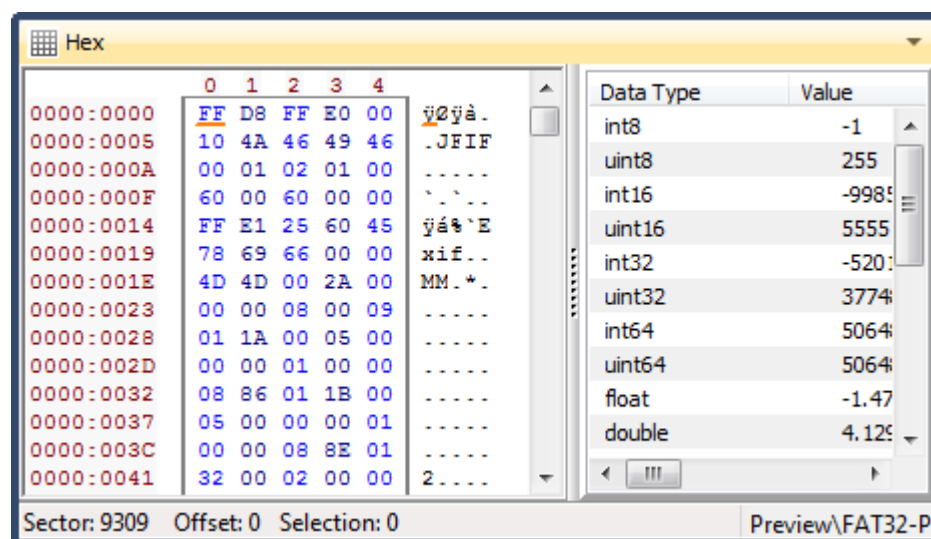
8.6 HEX VIEW

The default location of the Hex view window is the bottom data view window, accessed via the Hex tab:



Hex view shows a hexadecimal/ASCII view of the currently highlighted item. The slide bar to the right of the hex/ASCII windows separates the data inspector. Data highlighted in hex view is automatically analyzed in the data inspector to determine its type:

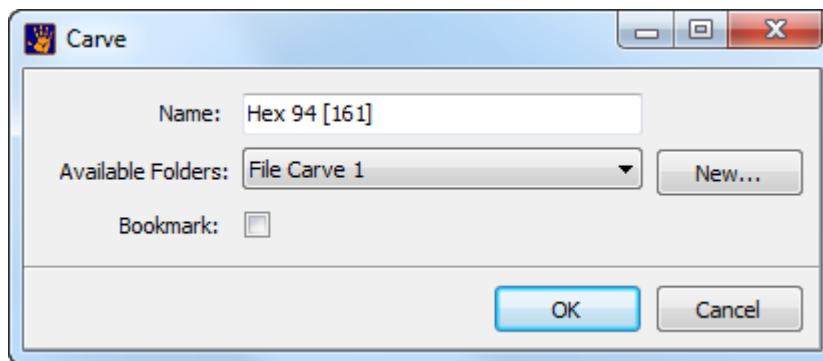
Figure 60, Hex view and data inspector



The **right-click menu** in the **Hex view** provides options to select and copy Hex. It also allows investigators to:

- **Add bookmark:** Highlight a selection of Hex and bookmarked it. See Chapter 16 - Bookmarks Module, for more information.
- **Carve Selection:** Highlight a selection of Hex and carve this data and add it to the File System module as a file. When this option is selected, the following window appears:

Figure 61, Carving files from Hex view



Name: The default name is the Hex Offset and the length of the selection in bytes. The default name can be edited.

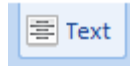
Available Folders: This is the folder name in File System Folders view which will hold the carved file. A new folder can be added as required.

Bookmark: Adds the carved file to the Bookmarks module.

8.7 TEXT VIEW

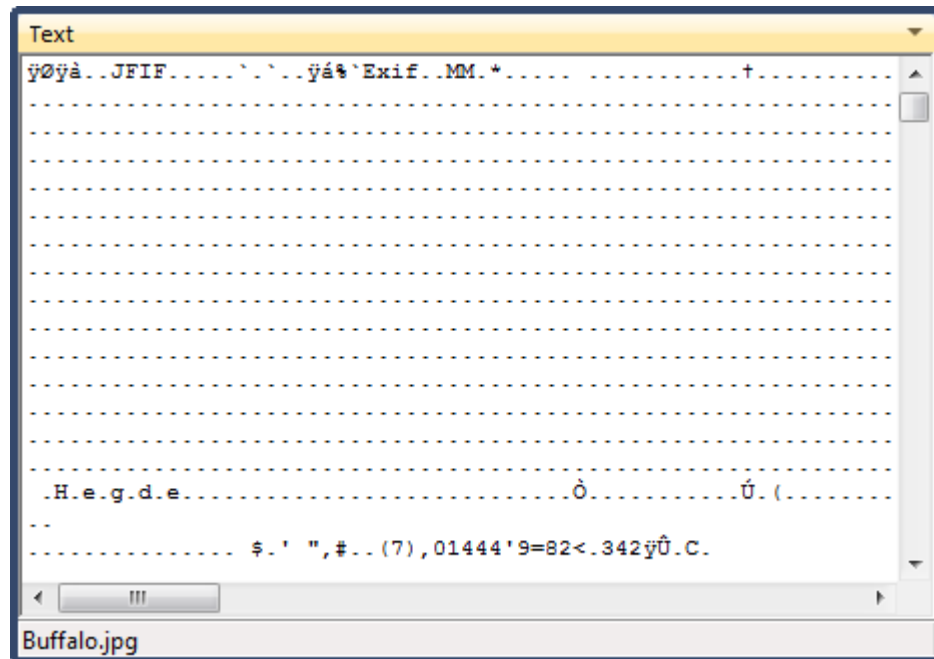
The default location for the Text view window is the bottom data view window, accessed via the Text tab:

Figure 62, Text view tab



The Text tab shows the highlighted item as ASCII text.

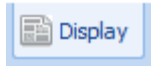
Figure 63, Text view



8.8 DISPLAY VIEW

The default location of the *Display* view window is the bottom data view window, accessed via the Display tab:

Figure 64, Display view tab



The File Display tab uses GetData's **Explorer View** technology to display the content of hundreds of different file types:

Figure 65, Display view

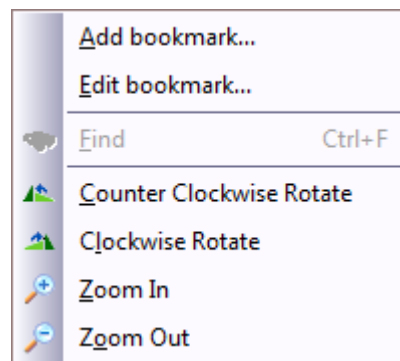


Note that the file Display tab is NOT intended as an exact render of how the file would have appeared to the end user. If this is the objective, it is best achieved by exporting the file and opening it with the same application available to the end user.

If a file type is selected where a display is not available, or the file is corrupt, an error message will display in this window. The display view will default to Hex or Text view.

Right click on the image to display the options menu:

Figure 66, Display view right-click menu



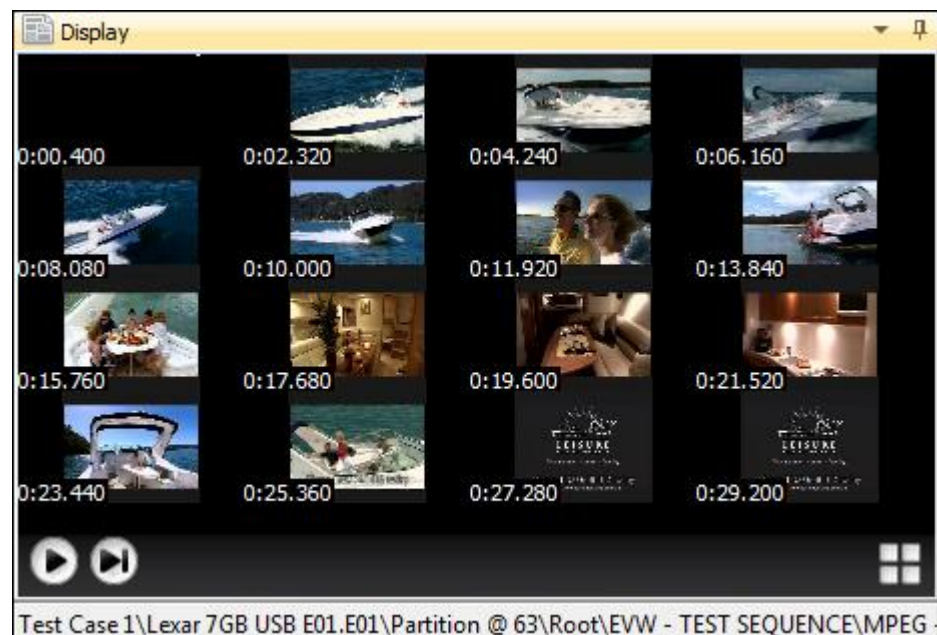
The following buttons are displayed for audio and video files



8.8.1 VIDEO THUMBNAILS

When viewing a video, it is possible to thumbnail the video by click on the thumbnail icon in the bottom right hand corner of the display window, as shown in Figure 67 below:

Figure 67, Video Thumbnails



To **jog** image thumbnails, click on the jog button.

To play all thumbnails, click on the play button.

To play in full screen from a specific thumbnail, double click the thumbnail.

8.9 BYTE PLOT AND CHARACTER DISTRIBUTION

The default location for the Byte Plot window is the bottom data view window, accessed via the Byte Plot tab:

Figure 68, Byte Plot tab



Byte Plot

Byte Plot is a graphical representation of byte level data within the currently highlighted file. It is a visual means to gauge the consistency or regularity of a file. In a Byte Plot;

“...each byte in the binary object is sequentially mapped to a pixel. The plotting of byte values in the object starts at the top left of the image. Subsequent byte values in the object are plotted from left to right, wrapping at the end of each horizontal row”. (8 pp. S3-S12)

Byte Plot is emerging as a future means of file type analysis by binary content or “fileprint” (9).

In the status bar of the Byte Plot data view is an **entropy** score for the displayed data. The entropy score is an expression of randomness where the more random the data, the higher the score. For example, a compressed zip file will have a higher entropy score than a text document.

Character Distribution

A character distribution bar graph is used in conjunction with Byte Plot and displays the distribution of ASCII characters according to the currently displayed segment of file. ASCII is a 7-bit character encoding scheme that allows text to be transmitted between electronic devices in a consistent way (See <http://www.ascii-code.com> (10)). The extended ASCII character set comprises codes 0–256, where codes;

- **0 - 31** are non-printing control characters
- **32 - 127** are printable characters; of which:
 - **48 - 57** are numbers 0 - 9;
 - **65 - 90** are A - Z; and
 - **97 - 122** are a - z.
- **128 - 256** are extended characters

The Character Distribution **X-axis** represents ASCII character codes 0-256. The **Y-axis** represents the number of times each ASCII code appears in the current view. Like Byte Plot, Character Distribution gives a visual interpretation of file content.

Color Coding

In the Byte Plot data view, ASCII characters are color coded, where:

Blue - Non printable / extended characters

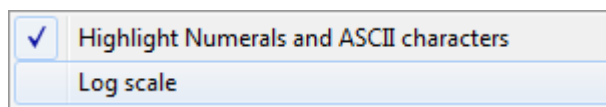
Red - Numbers (0 - 9)

Yellow - Text (a to z and A to Z)

Display Options

To change display options, **right click** on the Character Distribution graph to display the drop down options menu:

Figure 69, Byte Plot right click display options menu



To change **Byte Plot to grayscale**, de-select “Highlight Numerals and ASCII characters”.

To change the **scale of Character Distribution**, select Log scale.

8.9.1 BYTE PLOT EXAMPLES

Microsoft Word document:

Figure 70 shows a Byte Plot and Character Distribution for the Microsoft Word file “Golf.doc”. The visualization is consistent with a Word document, where;

- Non printable ASCII characters (blue) are prominent in the header of the file;
- Text characters predominantly (yellow) follow the header.

Figure 70, Byte Plot and Character Distribution of a .doc file

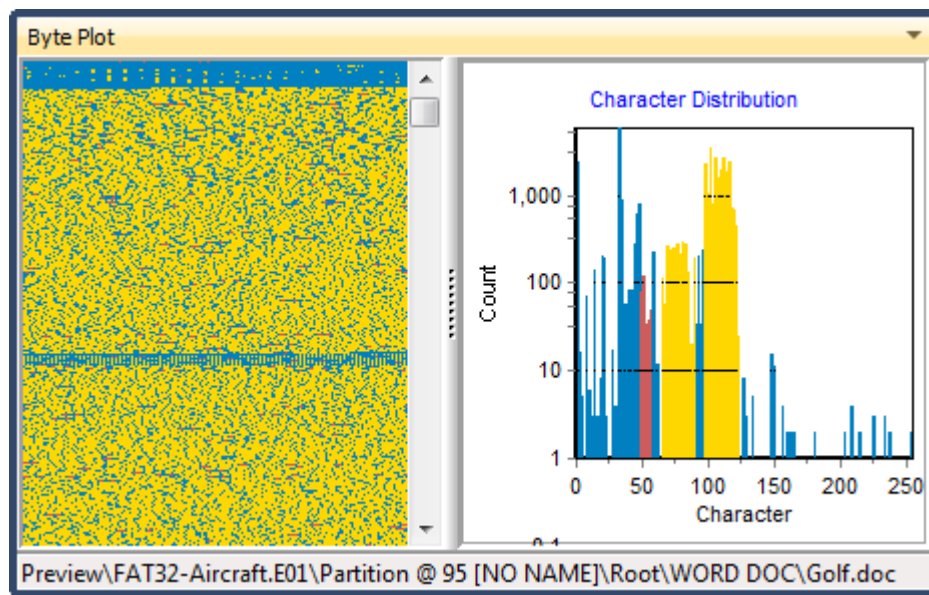
**JPG Photograph:**

Figure 71 shows a Byte Plot and Character Distribution for a JPG digital photograph. The visualization is consistent with a JPG file where;

- Non printable ASCII characters (blue) are prominent in the header of the file;
- JPG metadata text (yellow) follow the header;
- The body of the JPG shows regular compressed data.

Figure 71, Byte Plot and Character Distribution of a .jpg file

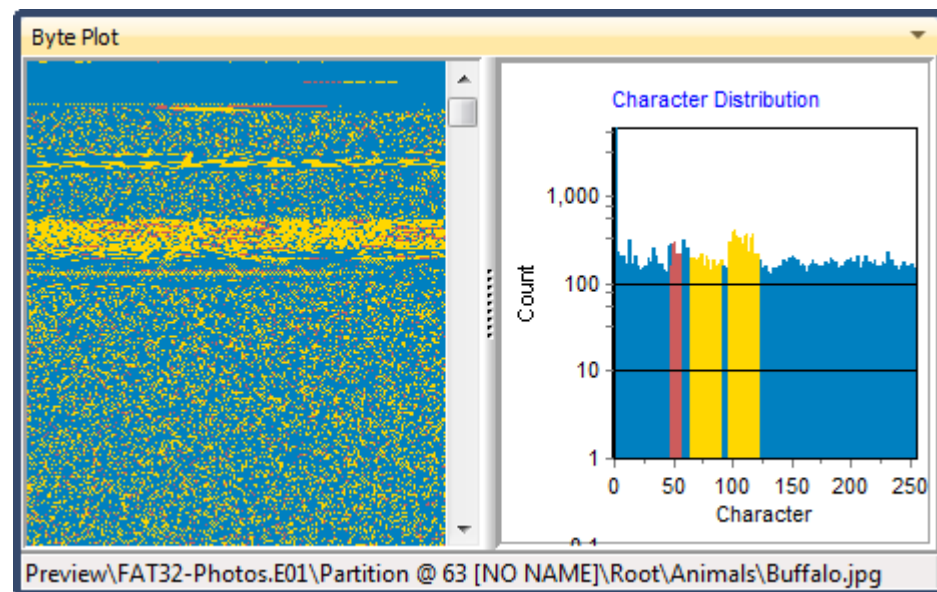
**RTF document:**

Figure 72 shows a Byte Plot and Character Distribution for a RTF document. The visualization is consistent with a RTF file where there is no defined file header and the majority of the file appears as text.

Figure 72, Byte Plot and Character Distribution of an .rtf file

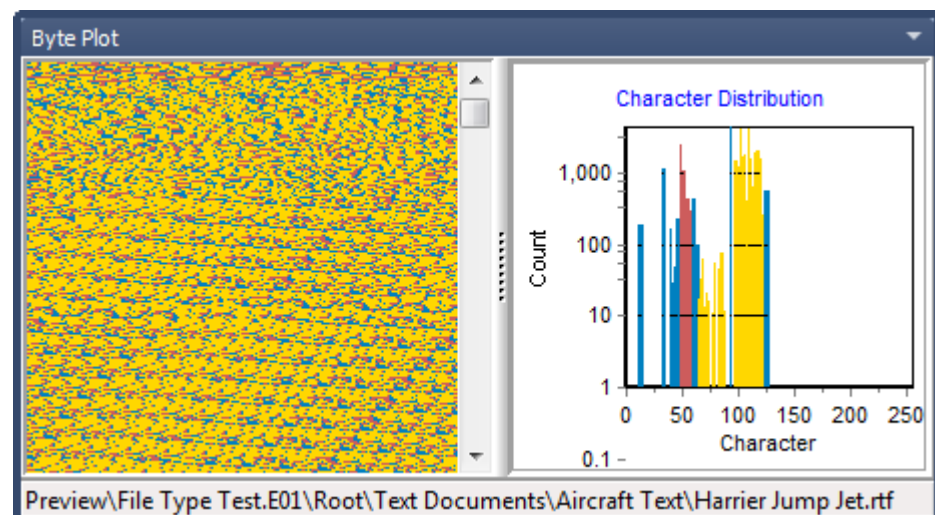
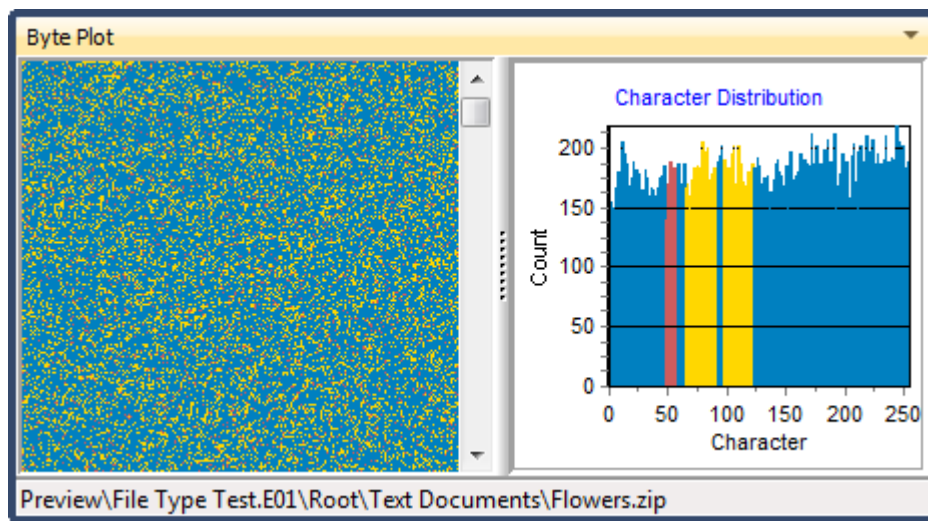
**ZIP file:**

Figure 73 shows a Byte Plot and Character Distribution for a ZIP document. The visualization is consistent with a ZIP file where;

- There is even distribution of the ASCII character set typical of compressed data.

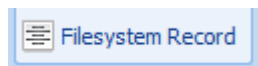
Figure 73, Byte Plot and Character Distribution of a .zip file



8.10 FILESYSTEM RECORD VIEW

The default location for the Filesystem Record view is the bottom data view window of the File System module:

Figure 74, Filesystem Record tab



Filesystem Record view decodes and displays the full attributes of highlighted item, including FAT, MFT, HFS file system records and Windows registry entries.

To **display** the **Filesystem Record view** for a file:

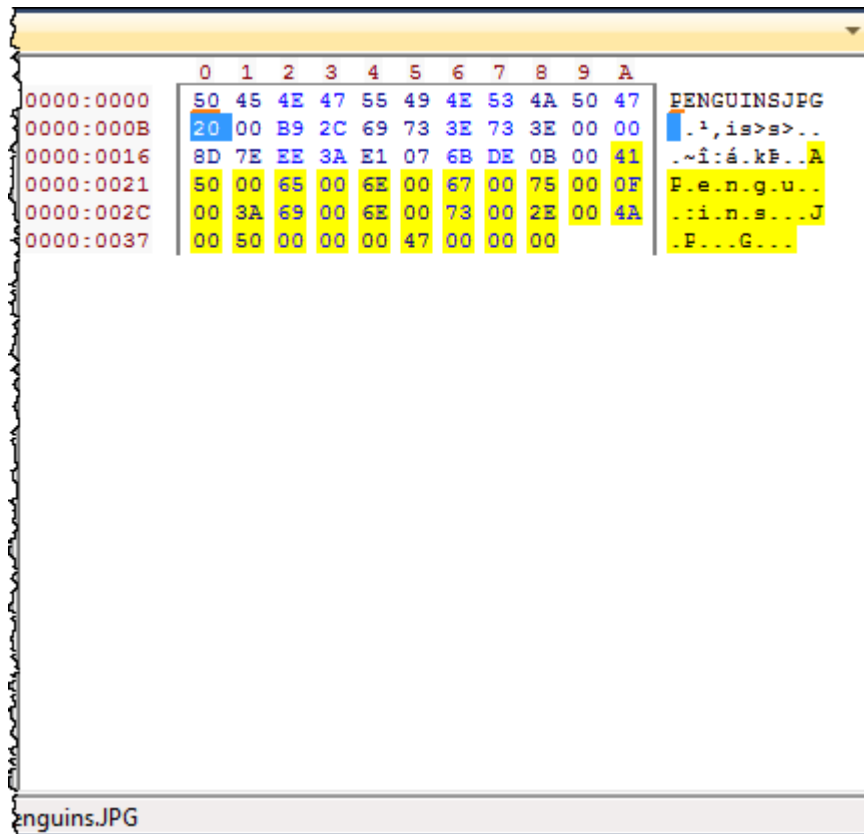
1. **Highlight** a file in **File List view**;
2. Select the **Filesystem Record** view tab in the bottom window.

The details of the highlighted file are then displayed. A Filesystem Record view of a highlighted file on a FAT file system is shown in Figure 75 below:

Figure 75, Filesystem Record view

Property	Value	Raw Value	Type
FAT Record			
Short Filename	PENGUINS.J...	PENGUINS....	AString
Deleted	False	False	Boolean
Attributes	A	32	Byte
Reserved	0	0	Byte
Created (10ms)	185	185	Byte
Created Time	1:09:24 PM	26924	Word
Created Date	19-Mar-11	15987	Word
Accessed Date	19-Mar-11	15987	Word
EAIndex (FAT12/16)	0	0	Word
Written Time	3:52:26 PM	32397	Word
Written Date	14-Jul-09	15086	Word
Start Cluster (FAT1...)	2,017	2017	Word
Start Cluster (FAT32)	2,017	2017	LongWord
Filesize	777,835	777835	LongWord
Longfile Record 1			
LFN String	Penguins.JPG	Penguins.JPG	UString
LFN Sig. byte	65	65	Byte
LFN Attribute	15	15	Byte
LFN File	0	0	Byte

Preview\FAT32-Photos.E01\Partition @ 63 [NO NAME]\Root\Animals\Aquatic\Peng



The Filesystem Record view shows:

Value: The value of the property entry as interpreted by Forensic Explorer.

Raw Value: The raw data as read from the file system record or registry entry.

Type: The type of data read from the file system record or registry entry.

The **adjacent window** displays the raw data from which the individual records have been decoded.

Figure 75 above shows the records for the file “Penguins.JPG”. Clicking on the “Attributes” property in the left highlights (in blue) the raw byte on the right from which the attribute data is decoded.

The yellow highlighting differentiates the section of the FAT directory entry which is dedicated to the long file name data.

8.11 FILE METADATA

Metadata is loosely defined as “data about data”. Essentially it is information within a file which further described the content or the layout of the file.













An example of Metadata is found in Microsoft Word documents where additional information is stored by word, including:

- Author;
- Subject;
- Title; etc.

The File Metadata view breaks down and displays the metadata values for specific file types. Currently supported are OLE (.doc, .xls, .ppt), ZIP and JPEG.

Figure 76 below show the metadata of a Microsoft Word document:

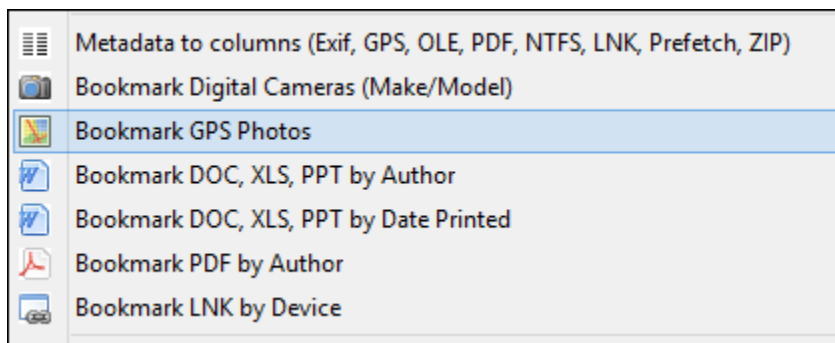
Figure 76, Metadata view of a Microsoft Word document

File Metadata				
Property	Value	Raw Value	Type	
OLE Data				
OLE Header				
OLE Summary				
 Author	LT	LT	UString	
 Subject			Binary	
 Title	Accounting Data	Accounting Data	UString	
 Created (UTC)	13-Jul-06 4:39:00 AM	13-Jul-06 4:39:00 AM	Date	
 Modified (UTC)	13-Jul-06 4:43:00 AM	13-Jul-06 4:43:00 AM	Date	
 Edit Time	2 mins	2	Integer	
 PageCode	1,252	1252	LongWord	
 Keywords			Binary	
 Comments			Binary	
 Last Saved	LT	LT	UString	
 Pages	1	1	LongWord	
 Words	92	92	LongWord	

8.11.1 EXTRACT METADATA TO FILE LIST COLUMNS

It is possible to extract metadata and make it available in a column in a list view. This is done from the **File System module, Analysis Scripts button**, shown below:

Figure 77, Metadata extraction scripts, File System module, Analysis Scripts button

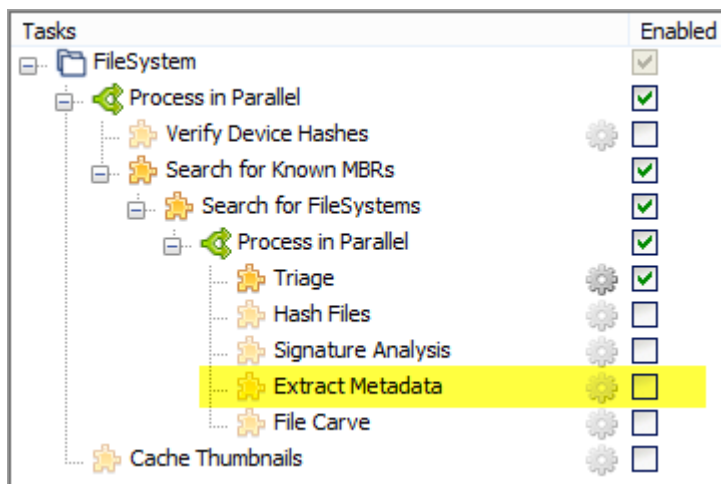


The script used to extract metadata is located in the Scripts module in the path: **\Scripts\File System\Metadata to Columns\Extract Metadata.pas** When run, columns are available to be added in the File System module. Learn how to add a column in section 9.8 - Columns.

EXTRACTING METADATA IN THE EVIDENCE PROCESSOR

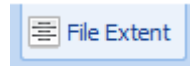
It is also possible to launch metadata extraction (and bookmarking) from the Evidence Processor when adding evidence to a case, as shown below:

Figure 78, Extract Metadata to Columns when adding evidence to a case



8.12 FILE EXTENT

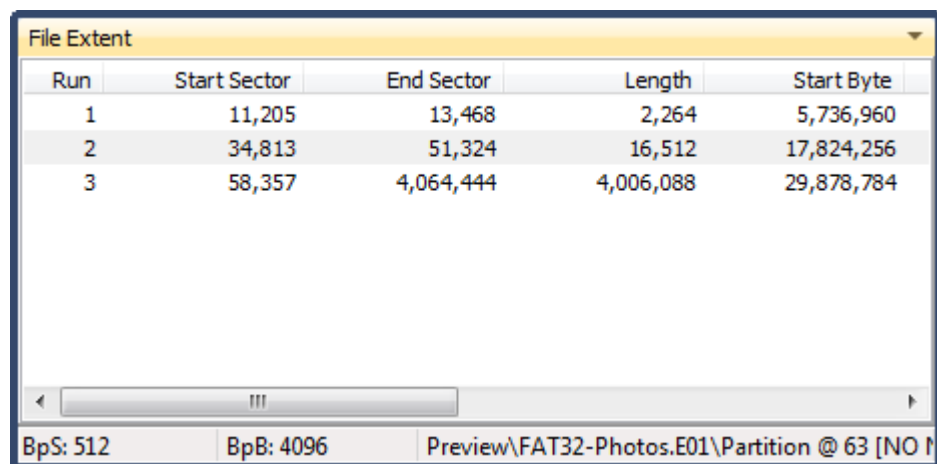
The default location for File Extent view is the bottom data view window, accessed via the File Extent tab:



The File Extent view identifies the location of the highlighted item on the disk. It details the start, end and length of each data run for the item, giving the relevant sector, byte and cluster location.

The file shown in Figure 79 below is a fragmented file with three data runs:

Figure 79, File Extent data view

A screenshot of the 'File Extent' window. It features a table with five columns: 'Run', 'Start Sector', 'End Sector', 'Length', and 'Start Byte'. The table contains three rows of data. Below the table is a scrollbar and a status bar with three fields: 'BpS: 512', 'BpB: 4096', and 'Preview\FAT32-Photos.E01\Partition @ 63 [NO I...]'.

Run	Start Sector	End Sector	Length	Start Byte
1	11,205	13,468	2,264	5,736,960
2	34,813	51,324	16,512	17,824,256
3	58,357	4,064,444	4,006,088	29,878,784

BpS: 512 BpB: 4096 Preview\FAT32-Photos.E01\Partition @ 63 [NO I...]

BpS: Bytes per Sector

BpB: Bytes per Block (cluster).

Using the information displayed in the File *Extent* view it is possible to switch to Disk view and quickly locate the start or end sector of each data run.

Chapter 9 - Working with data

In This Chapter

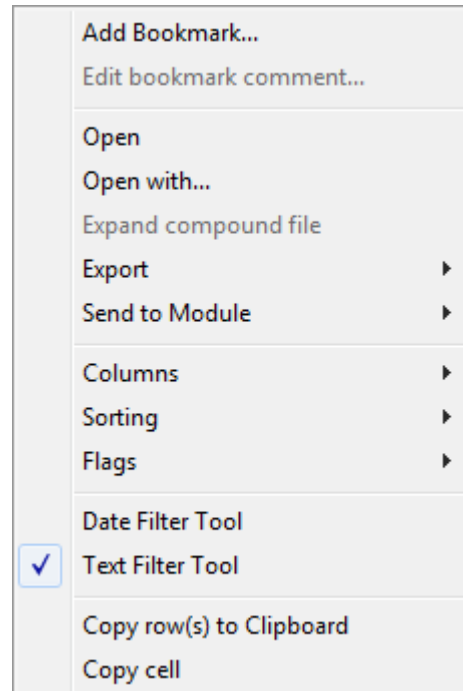
CHAPTER 9 - WORKING WITH DATA

9.1	Working with data	102
9.2	Highlighted and checked items	102
9.2.1	Highlighted items.....	102
9.2.2	Checked items.....	103
9.3	Add and edit bookmarks	104
9.4	Open with	104
9.5	Expand compound file.....	105
9.6	Export	105
9.6.1	Export Folders and Files	105
9.6.2	Export Logical Evidence File (.L01)	107
9.6.3	Export Delimited Rows (.csv or .tab).....	109
9.7	Send to Module	110
9.8	Columns.....	110
9.9	Sorting	111
9.10	Flags.....	113
9.11	Filtering Data	114
9.11.1	Date range filter	114
9.11.2	Text filter tool	115
9.11.3	Explorer Tool	118
9.11.4	Folders Filter.....	119
9.12	Copy rows to clipboard.....	119

9.1 WORKING WITH DATA

Forensic Explorer modules and data views share common functions used to view, analyze and manage case content. These functions are either performed directly within the view, or are access by a right-click menu, as shown Figure 80 below:

Figure 80, Right-click menu in the File System list view



9.2 HIGHLIGHTED AND CHECKED ITEMS

In Forensic Explorer actions are performed on “items”. An item is an addressable piece of data. An item can be a device (e.g. physical drive, logical drive or image file), a file, folder, partition, metadata entry, FAT, MFT, VBR, MBR, unallocated clusters, directory entry, or other such data.

In order to perform an action on an item it is usually either first “**highlighted**” or “**checked**” (or both). An action on a highlighted file is independent to an action on a checked file.

9.2.1 HIGHLIGHTED ITEMS

A highlighted item is one that has been selected with the mouse and the item **has changed color**. It is possible to highlight one or more items.

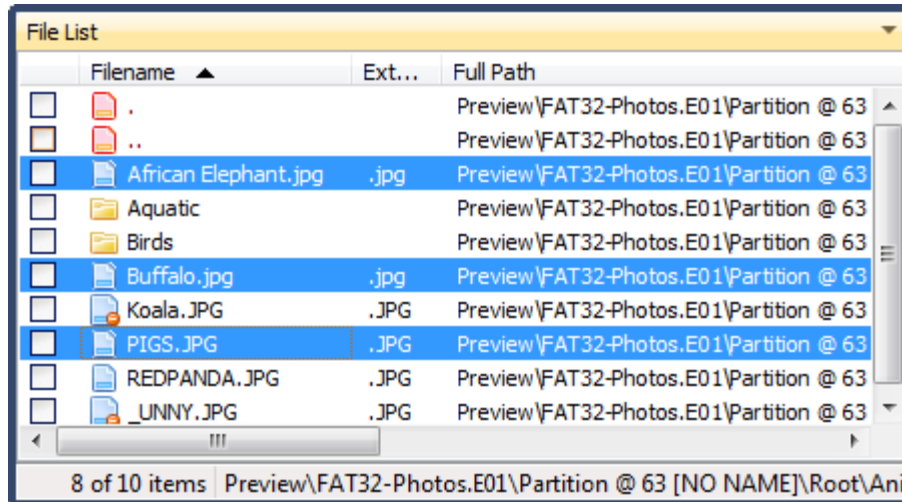
To highlight multiple consecutive items:

1. Highlight the first file with the mouse and then press and hold the Shift key;
2. While holding the Shift key down click the last file. This will highlight all the files in-between the first and last file.

To highlight multiple not consecutive items:

1. Highlight the first required file with the mouse and then hold the Ctrl key;
2. While holding down the Ctrl key, highlight each of the other required files.

Figure 81, Highlighted items

**9.2.2 CHECKED ITEMS**

A checked item is one which has been a tick in its selection box:

- ☒ User checked item;
- ☐ A folder in which not all items inside that folder (or its sub-folders) have been checked.

To check an **individual item**, use the mouse to place a tick in the selection box.

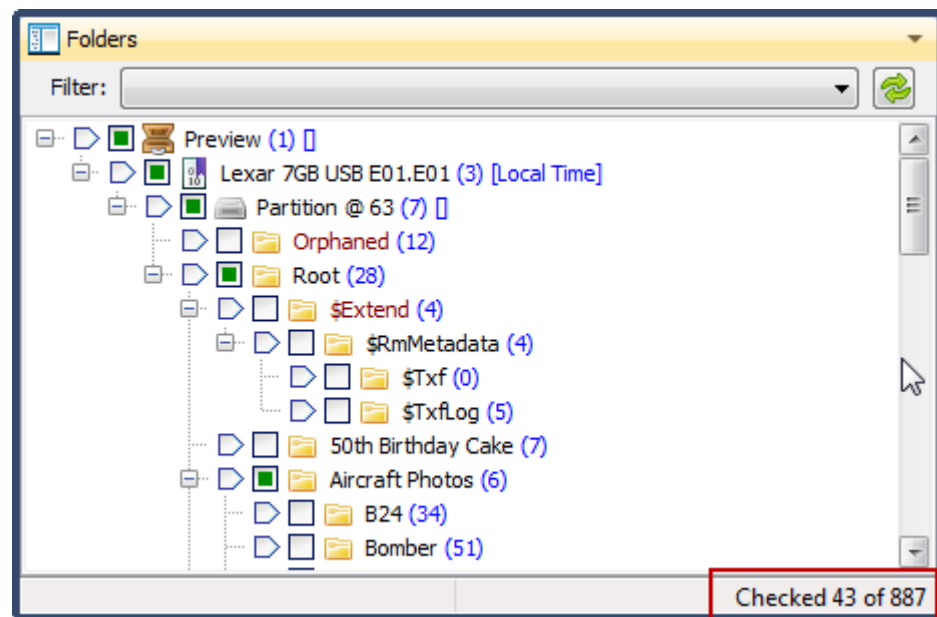
To check **multiple items**:

1. Follow the instruction above to highlight multiple files;
2. Then press the **Space Bar** to turn the check ticks on, or off.

COUNTING CHECKED ITEMS

It is useful in many situations to quickly identify how many items are currently checked. This information is provided in the status bar of a Folders view, as shown in Figure 82 below:

Figure 82, Checked item count in Folders view



9.3 ADD AND EDIT BOOKMARKS

Forensic Explorer enables any item (file, folder, keyword, search hit etc.), or sections of items, to be marked and listed in the Bookmarks module. Bookmarks are used to note items of interest. Bookmarked items in a list view can be identified by a “yes” entry in the “Bookmarked” column.

To **add a bookmark**:

- **Right-click in the data view** and **select Add Bookmark** from the **drop down menu**.

This will open the Add Bookmark window. See **Chapter 16 - Bookmarks Module**, for more information on adding and editing bookmarks.

9.4 OPEN WITH

The **Open With** command uses the standard Windows Open With function to open a file from a list view using an **external application** (such as Windows Paint, or Microsoft Word) using the standard Windows . To use Open With:

1. **Highlight** the required file;
2. **Right-click** and select **Open With** from the text menu.

If the highlighted file is not already associated with a program, the Windows Open With window will display and allow the file type to be associated.

The file to be opened is copied to the case “Temp” folder: “**\My Documents\Forensic Explorer\Cases\[Case Name]\Temp**” and then opened by the external application.

9.5 EXPAND COMPOUND FILE

A compound file is a file that is a container for other files or data. A simple example is ZIP compressed file.

Typically compound files should be expanded early in a case to enable Forensic Explorer full access to the content. This should be performed prior to a keyword or index search so that they may include the expanded data.



Forensic Explorer currently supports the expansion of the following compound files:

- ZIP (Note: Decompressed Zip files are read into RAM. A size limit of 100mb is set. Files over 100mb will not be decompressed).
- OLE (DOC, XLS, PPT, ODT)

To **expand a compound file**:

1. **Highlight** the file in the list view;
2. **Right-click** and select **Expand Compound File** from the drop down menu.

The file changes to a container which holds the expanded content (similar to a folder). For example:

-  "HLA_IT_University_HI-RES_Photos_EXTERIORS.ZIP" is the original file;
-  "HLA_IT_University_HI-RES_Photos_EXTERIORS.ZIP" is the container for the expanded content.

To **expand all compound files in a case**:

1. In the File System module, click on the Analysis Scripts drop down button in the toolbar and run the "Expand Compound Files" script.

To **display only expanded files in the File System module**

1. In the File System module Folders Filter, select the "Expand Compound Files" to show only these files.

9.6 EXPORT

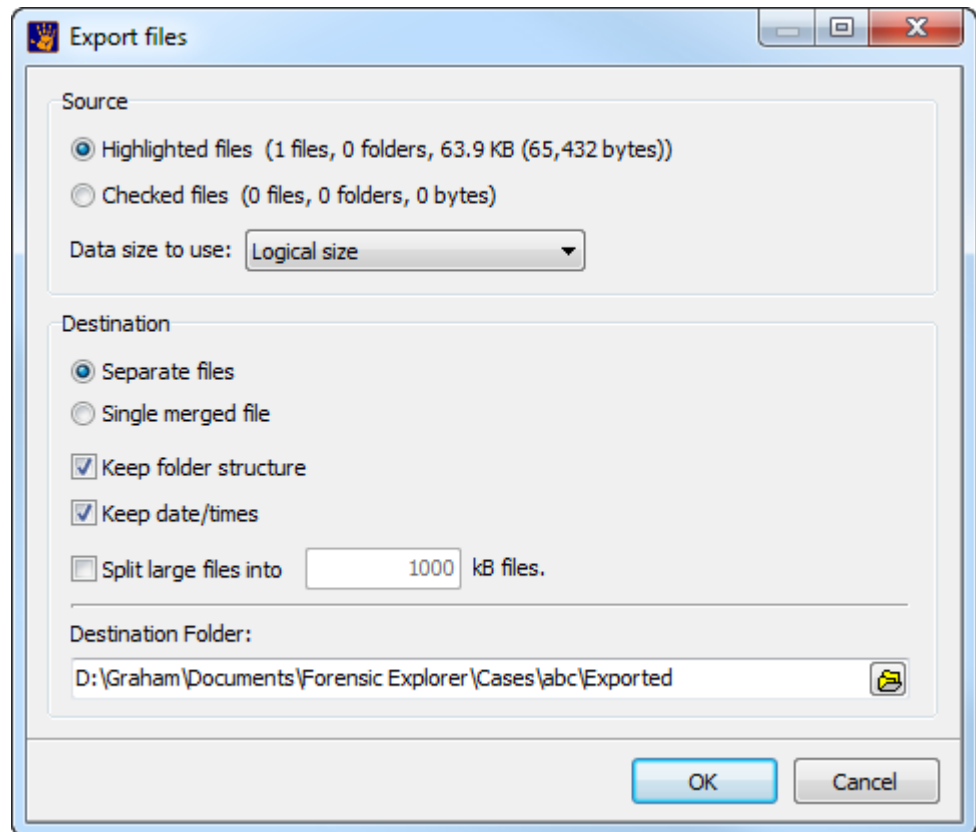
9.6.1 EXPORT FOLDERS AND FILES

The export Folders and Files function is used to copy files from the case to the local disk.

To **export folders and files**:

1. **Highlight** or **check** the required items;
2. **Right click** and select “**Export > Folders and files...**” from the drop down menu;
3. The following Export Files window will then open;

Figure 83, Export files window



Source:

- Files can be exported with their logical or physical size.

Destination:

- **Separate files:** The exported files may be saved individually or as a single merged file.
- **Keep folder structure:** Will determine whether the exported files are saved with the complete path information from the case, or if they are saved into the root level of the selected location.
- **Keep date/times:** Specifies whether the date and times of the exported files will retain their metadata as displayed by Forensic Explorer, or whether dates and times will reflect the creation of the exported files.
- **Split large files:** Large files can be split into designated sizes.

- **Destination folder:** The destination folder specifies the location where the files will be saved. The default location is the “Exported” folder in the case path.

EXPORT FOLDERS AND FILES USING A SCRIPT

One of the default scripts provided with Forensic Explorer is **Scripts\File System\Export File Types.pas**. This script will export files by type (extension) and can be edited as required. For more information about scripts, see Chapter 18 - Scripts Module.

9.6.2 EXPORT LOGICAL EVIDENCE FILE (.L01)

A Logical Evidence File (LEF) is a forensic image containing selected individual files, rather than the image of an entire partition or physical device. LEF's are usually created when:

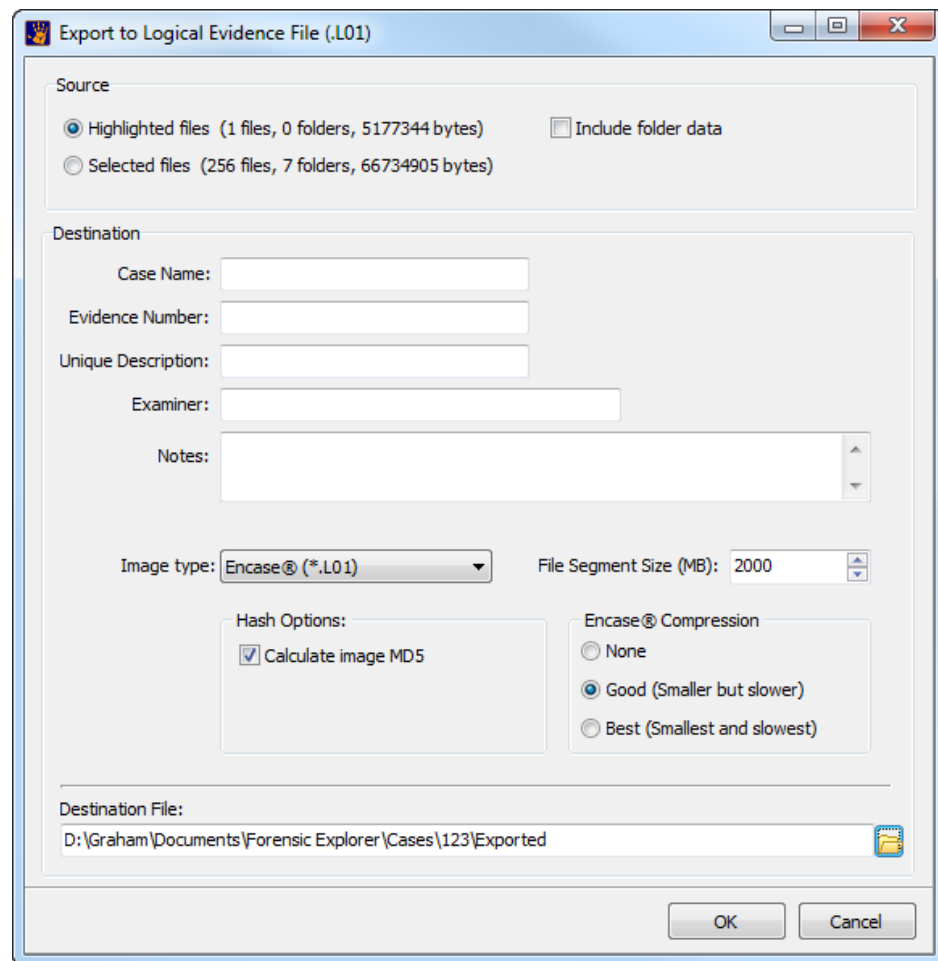
1. A device is previewed and evidence worthy of preservation is identified, but an image of the entire partition or device is not warranted; or
2. When a subset of a files from an existing forensic image is be provided to a third party.

Common LEF formats are .L01 (Guidance Software - www.guidancesoftware.com) and .AD1 (Access Data - www.accessdata.com). Forensic Explorer will read both L01 and AD1 formats and can export files to .L01 format.

To export files to an .L01 file:

1. **Select** or **highlight** the required file/s;
2. **Right click** and select **Export > Logical evidence file (.L01)** from the drop down menu. The following window will appear:

Figure 84, Export to Logical Evidence File (.L01)



Include folder data: If selected, the folder is treated as a file and its content included in the image. This may not be desirable, as the folder data can contain information about other files that have not been selected to be part of the L01 content. If this option is disabled, the image will contain only the folder name.

Calculate image MD5: If selected, an MD5 hash for the entire L01 file is calculated and stored within the file.

Note: Individual files within the LEF are automatically MD5 hashed and each value is stored.

VALIDATING .L01 FILES

To validate an .L01 files in Forensic Explorer

1. **Add the .L01 file** to a case, or a preview:
2. Add the **“L01 Hash” column** to the list view of the File System module (refer to paragraph 9.8 for information on adding a column). This column shows the MD5 hashes created at the time of acquisition and stored within the .L01 file;

3. Use the **Hash Files** button to calculate the current MD5 hash for each file:

Figure 85, Hash Files button in the File System module toolbar



4. Add the **"MD5 hash" column** to the File System module, List view.
5. **Compare the L01 Hash MD5 Hash** results. The acquisition hash and the recalculated hash should be identical.

9.6.3 EXPORT DELIMITED ROWS (.CSV OR .TAB)

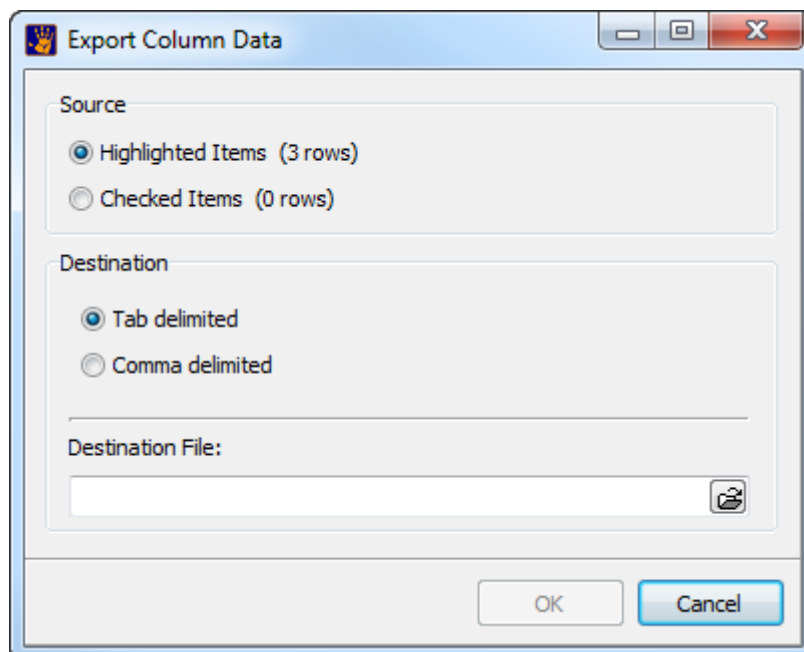
The export delimited rows function is used to copy list view data into a format suitable for import into a spread-sheet or similar program.

To **export delimited rows**:

1. **Highlight** or **check** the required files;
2. **Right click** and select **"Export > Delimited rows (.csv or .tab)"** from the drop down menu;

The following window will appear:

Figure 86, Export delimited rows



Select the source and whether the file is to be TAB or comma delimited. Enter the name of the destination file and click OK to proceed with the export. Only currently visible columns will be exported.

9.7 SEND TO MODULE

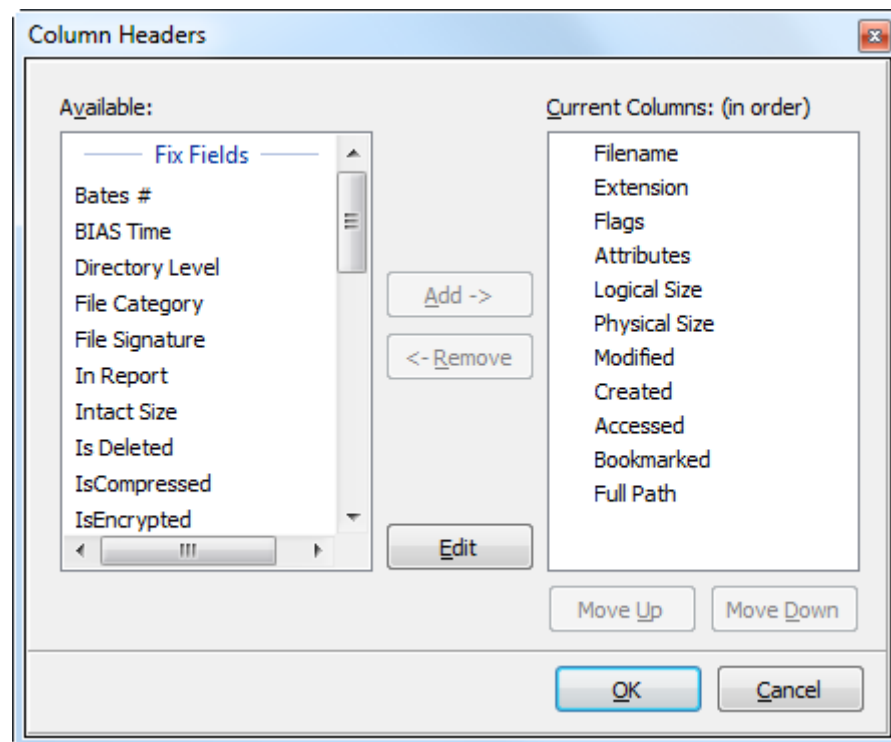
Send to Module is a method of passing specific files from one module to another. For example, a Windows registry file can be highlighted in the list view of the File System module and passed to the Registry module for processing (see 15.2 for more information).

9.8 COLUMNS

To **add columns** or **remove columns** in a list view:

1. **Right click** on the List view and select **Columns > Edit Columns** from the drop down menu. The Column Headers window will open;

Figure 87, Column Headers



2. **Add** available columns to the current columns and **Move Up** or **Move Down** for the required position (position can also be controlled by dragging and dropping column titles once they are added). **Remove** unwanted columns with the remove button.

It is possible to add columns using a script. An example of this is where the metadata properties from a Microsoft Word document, e.g. Author, Title etc. are extracted and placed in to columns. See 8.11.1 for more information.

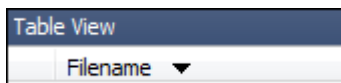
9.9 SORTING

Sorting is conducted in a List view where the attributes of a file, email, Bookmark, keyword search etc. are displayed in the relevant columns.

To sort by a **single column**:

1. Double click on the column heading, e.g. "Filename". An arrow will appear showing the direction of the sort.
2. Double click again on the column heading to reverse the sort:

Figure 88, Single column sort

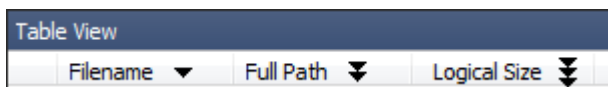


The same single column sort result can be achieved by right clicking on the column and in the drop down menu select "Sorting > Sort Ascending [columnname]" or "Sort Descending [columnname]":

To sort by **multiple columns** using the CTRL key:

1. **Double click on the first column heading**, e.g. "Filename". An arrow will appear showing the direction of the sort. Double click again on the column heading to reverse the sort;
2. **Hold down the SHIFT key** on the keyboard;
3. **Double click on the second column heading**, e.g. "Filename". A double arrow will appear to indicate that it is the second column in the sort.
4. Continue to add columns to the sort by following steps 1 to 3 above.

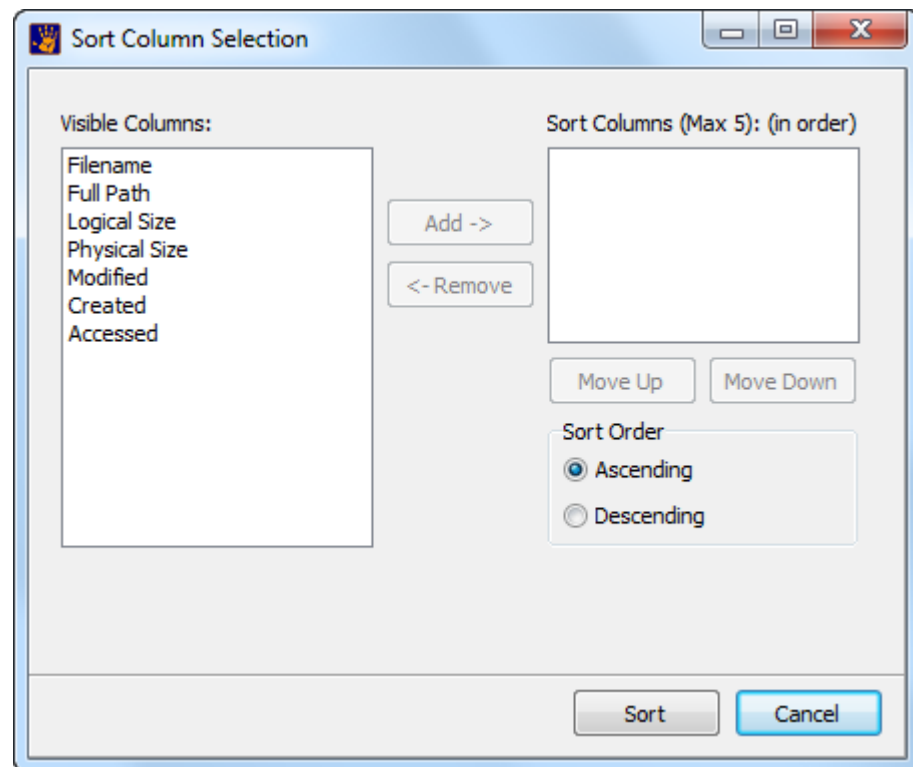
Figure 89, Sort by Filename, then Full Path, then Logical Size



A multi column sort can also be achieved by right clicking on the column heading:

1. Select the "Sorting > Sort Multi Column..." menu item, shown below:

Figure 90, Multi column selection window



Visible columns are shown in the left hand window:

1. Select the required sort columns;
2. Add the required sort columns to the right hand window;
3. Use the “Move Up” and “Move Down” buttons to set the order on which to sort the columns;
4. Click the “Sort” button to apply the sort.

Persistent Sort:

- A **persistent sort** (right-click > Sorting > Persistent Sort) maintains the current sort when switching between data views.

To remove a multi column sort:

- Release the SHIFT key and double click on a column heading to return to a single column sort.

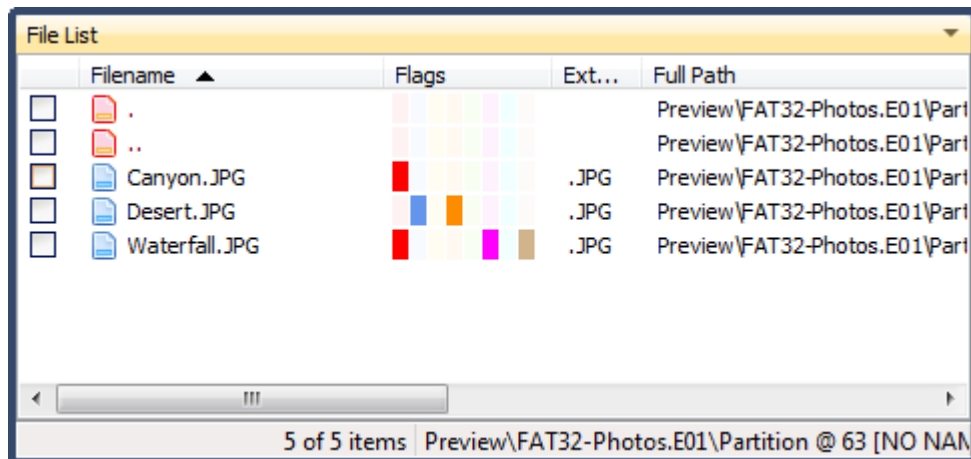
To remove all sorting,

- Right click and from the drop down menu select “Sorting > Remove Sorts”.

9.10 FLAGS

In Forensic Explorer a flag is a colored box applied in a List view in the “Flag” column to mark a file. Eight colored flags are available for use. A single item can be flagged one or more times. Flagged files are shown in Figure 91 below:

Figure 91, Flagged items

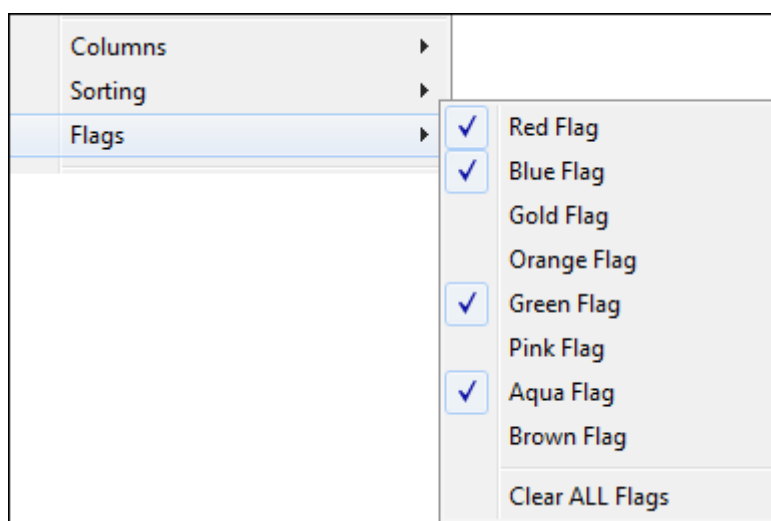


To apply a flag:

1. **Highlight an item** in a List view;
2. **Double click the opaque flag color** in the flag column (if the flag column is not visible add the column - see paragraph 9.8 - Columns); **or**,

Right click and use the “**Add Flag**” menu to place a selection tick next to the required flags, as shown in Figure 92 below:

Figure 92, Right click “Flags” menu option



To apply flags simultaneously to multiple items:

1. In the list view, **highlight multiple items** by holding down the SHIFT or CTRL key and selecting the required items with the mouse;
2. Right click and use the **Flags menu** option;
3. **Select** the required flags.

To clear flags:

1. Double click on the flag; or
2. Highlight the required items, right click and use the **Flags > Clear Flags** menu option; or
3. One of the default scripts provided with Forensic Explorer is “/Scripts/File System/Clear All Flags.pas”, which will programmatically remove all flags.

Scripting Flags

Flags can also be applied by running Forensic Explorer scripts. See the Chapter 18 - Scripts Module, for more information.

9.11 FILTERING DATA

9.11.1 DATE RANGE FILTER

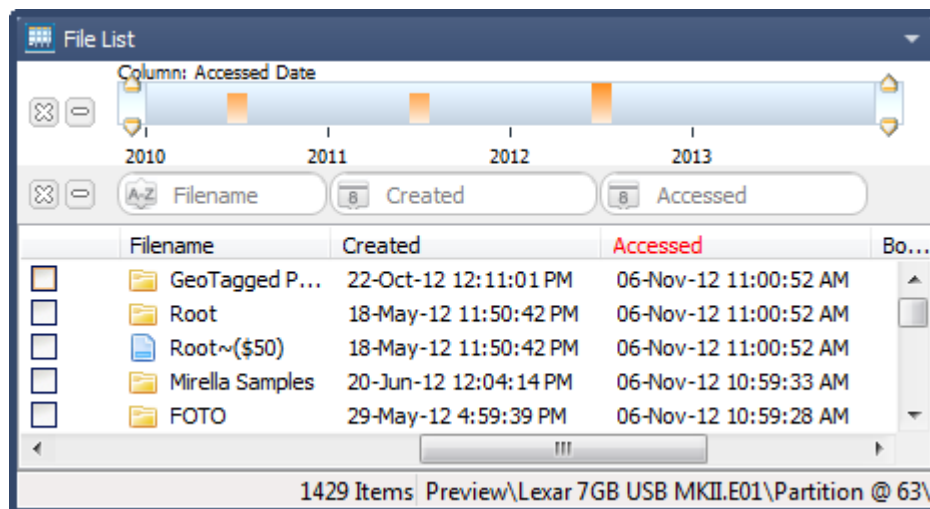
The **Date Range filter tool** is applied to the items displayed in a list view and allows filtering by Created, Modified, and Accessed dates.

To access the Date Range filter tool:


1. Right click on the File list view column headings;
2. From the drop down menu, select “Date Filter Tool”:

The Date Range filter tool then appears above the List view column headings, as shown in Figure 93 below.

Figure 93, Date filter tool



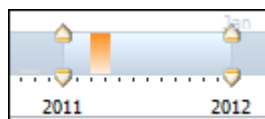
The applied filter column is displayed in red (e.g. “Accessed”).

To change filter criteria, click on the date icon  in the Modified, Created, or Access columns and select the “Show Date Range Tool” for that column.

To apply a date filter:

Select and drag the slide bar pointers at either end of the date range to the required position on the date range bar. As the date range is narrowed, the filter is applied to the list view. In the example below, the filter is set to show only files with a date between 2011 and 2012:

Figure 94, Application of date range sliders



To **modify the time scale**, double click at either end of the date range.

To **clear the date range filter**, click on the  icon.

To **close the date range filter**, click the  icon.

9.11.2 TEXT FILTER TOOL




The **text filter tool** is applied in a list view and allows instant text filtering on column data.

To access the **text filter tool**:

1. Right click on a List view window;
2. From the drop down menu, select “Text Filter Tool”:

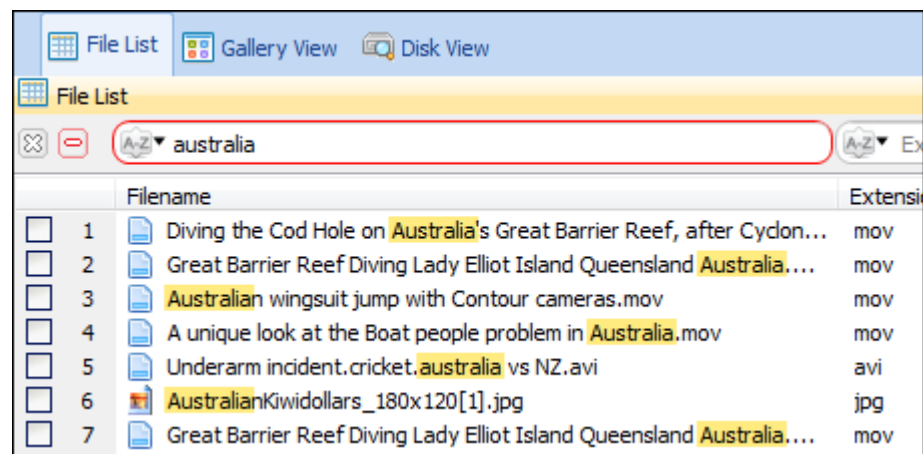
3. The text filter then appears above the List view column headings, as shown in Figure 95 below.

To **apply a text filter**:

1. Type into the filter field above the column heading:
 - i.  Requires A-Z characters;
 - ii.  Requires numbers 1 – 9.
Use >, =, or < symbols to list data greater than, equal to or less than the typed number;
 - iii.  Requires a date format (click for auto selection calendar).
2. As text is typed into the field the displayed content updates based upon the typed criteria.


When the filter is applied, the outline of the filter box/s turns red in color, as shown in Figure 95 below;

Figure 95, Text filter tool



To **apply multiple column text filters**: Enter the filter criteria into the field above each column heading. Multiple text filters are joined with the “and” operator.

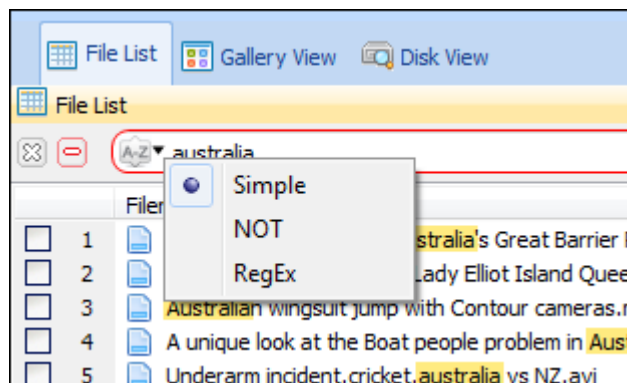
To **clear a text filter**: Remove the text from the filter.

To **clear all filters**: Press the  icon.

To **close the text filter**, click the  icon.

To change search options, click the ▼ icon:

Figure 96, Text filter search options



Simple: Filters for text entered.

NOT: Displays any value which does NOT match text entered. When the NOT column filter is active, the A-Z icon turns black, as shown in Figure 97 below:

Figure 97, NOT column filter active



RegEx: Regular expression search. When the RegEx column filter is active the icon changes to a formula, as shown in xx below:

Figure 98, RegEx column filter



RegEx quick start guide:

abc...	Letters
123...	Digits
\d	any Digit
.	any Character
\.	Period
[abc]	Only a, b, or c
[^abc]	Not a, b, nor c
[a-z]	Characters a to z
[0-9]	Numbers 0 to 9
{m}	m Repetitions
{m,n}	m to n Repetitions
*	Zero or more repetitions
+	One or more repetitions
?	Optional
\s	any Whitespace
^...\$	Starts and ends
()	capture Group
(a(bc))	capture Sub group
(.*)	capture Variable content
(a b)	Match's a or b
\w	any Alphanumeric character

\W	any Non-alphanumeric character
\d	any Digit
\D	any Non-digit character
\s	any Whitespace
\S	any Non-whitespace character

Note: The **Flag Column** is currently a binary search (it will be upgraded in a future version):

Flags Text Filter Value	Flags shown
1	Shows column 1 (red) onward
2	Shows column 2 (blue) onward
4	Shows column 3 (yellow) onward
8	Shows column 4 (orange) onward
16	Shows column 5 (green) onward
32	Shows column 6 (pink) onward
64	Shows column 7 (aqua) onward
128	Shows column 8 (brown) onward

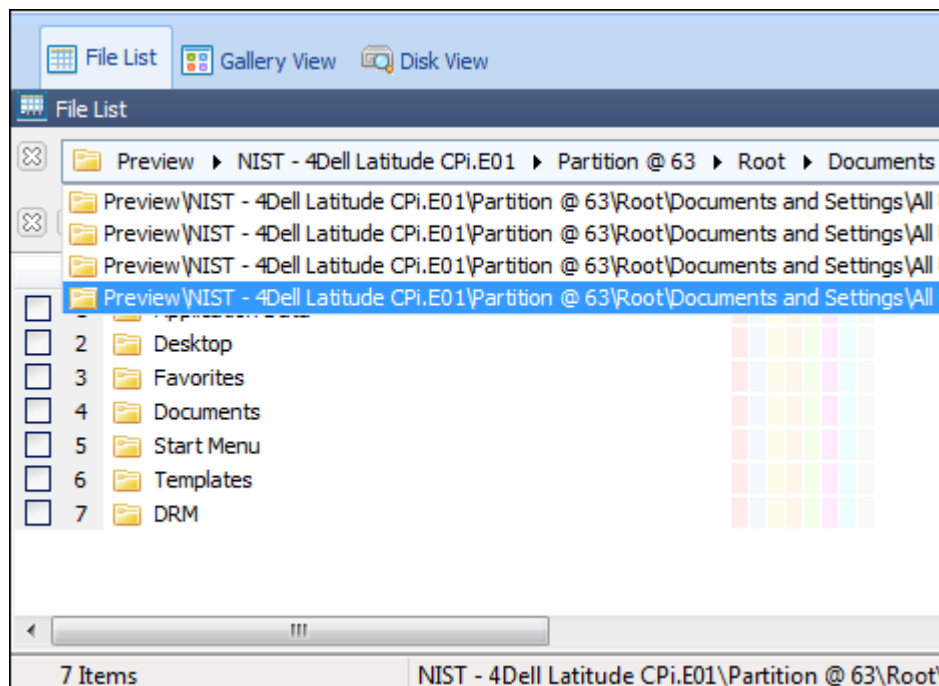
9.11.3 EXPLORER TOOL

The **Explorer Tool** is applied in a list view and allows navigation of the file system in a similar fashion to Windows Explorer.

To access the Explorer tool:

1. Right click on a List view window;
2. From the drop down menu, select "Explorer Tool":
3. The Explorer Tool then appears above the List view column headings, as shown in Figure 99, Explorer Tool below.

Figure 99, Explorer Tool



- Click on a folder in the path to jump to that folder in the List view.
- Use the drop down menu to jump to a recent path.

9.11.4 FOLDERS FILTER

Folders filters are applied using scripts. See Filters, page 218, for more information.

9.12 COPY ROWS TO CLIPBOARD

“Copy Row(s) to Clipboard” is a function specific to a List view. It allows the text in the List view table to be copied and pasted directly into an external program like Microsoft Excel. To copy rows to clipboard:

1. **Highlight the required rows** in the List view;
2. **Right click** and select “**Copy Row(s) to Clipboard**” from the drop down menu.

Chapter 10 - Evidence Module

In This Chapter

CHAPTER 10 - EVIDENCE MODULE

10.1	Preview	122
10.2	New case	124
10.2.1	Managing Investigators	125
10.3	Open an existing case	127
10.3.1	Recent cases	128
10.4	Adding evidence	129
10.4.1	Adding a Device	129
10.4.2	Adding a Network Device	130
10.4.3	Adding a Forensic image file	133
10.4.4	Adding a registry file	133
10.4.5	Adding a file	134
10.5	Evidence Processor	135
10.5.1	Processor tasks	135
10.5.2	Adjust Time Zone	138
10.6	Adding additional evidence to a case	139
10.7	Saving a case	140
10.7.1	Saving or closing a preview	140
10.8	Closing a case	141

10.1 PREVIEW

IMPORTANT: When working with physical devices, accepted forensic procedure dictates the use of a write block. Refer to Appendix 2 - Write Blocking, for more information.

Forensic Explorer allows the investigator to **preview** a **device, image** or **registry file** without first creating a case.

To **preview** a **device, image** or **registry files**:

- Click the **Preview** button in the **Evidence module**:

NOTE - v2.3.6.3518: From version v2.3.6.3518, the Evidence module **Preview** button is no longer displayed by default. To display the preview button, in the **Forensic Explorer drop down menu**, select **Options >** and check **Show Preview button**. The option is stored in a registry key and need only be set once.

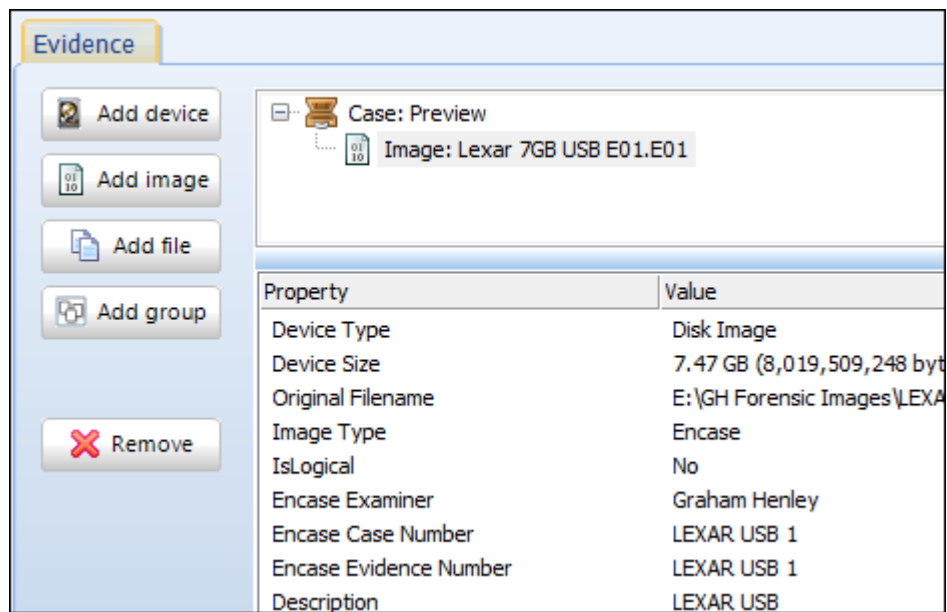
Figure 100, Preview button in the Evidence module



When the preview button is clicked;

- A unique preview working folder is created using a Global Unique Identifier (GUID) in the following path: **C:\Users\Graham\Documents\Forensic Explorer\Previews\{GUID [e.g. 8709A41C-38B6-4F9E-BA18-633B394721C5]}**;
- The evidence window in the Evidence module identifies that a preview is in progress with the words “**Case: Preview**”. The Add Group, Device, Image, File, Remove buttons become active in preparation for adding evidence to the preview, as shown in Figure 101 below:

Figure 101, Evidence Tree in the Evidence module identifying a "Preview"



For information on adding evidence to a preview, see "Adding evidence" on page 129.

A **preview can be saved as a case** at any time by selecting the **Save** button in the **Evidence module** or using the "**Forensic Explorer > Save Case**" drop-down menu item.

When a preview is saved information in the preview GUID folder is transferred to a case folder (see the "New Case" section below) and the GUID folder is deleted.

10.2 NEW CASE

To create a **new case**:

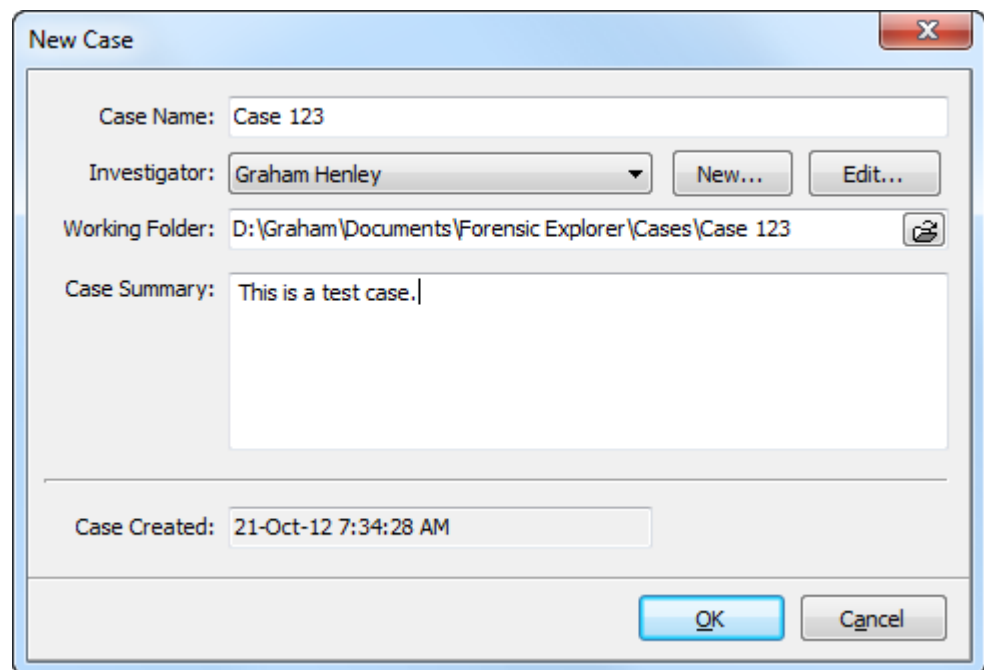
1. Click the **New** button in the **Evidence module**:

Figure 102, Evidence module, new case button



The "New Case" window will open, as shown in Figure 103 below:

Figure 103, New Case window

A screenshot of the "New Case" dialog box. The window has a title bar with "New Case" and a close button. Inside, there are several fields: "Case Name" with the value "Case 123", "Investigator" with a dropdown menu showing "Graham Henley" and buttons "New..." and "Edit...", "Working Folder" with the path "D:\Graham\Documents\Forensic Explorer\Cases\Case 123" and a folder icon button, and "Case Summary" with a text area containing "This is a test case.". At the bottom, there is a "Case Created" field showing "21-Oct-12 7:34:28 AM" and "OK" and "Cancel" buttons.

Enter the relevant case details:

Case Name requires a unique name is automatically used to create the case folder in the working path.

Investigator can be selected from the drop down list, or click the **New** button to create a new investigator. Forensic Explorer records activity in a case by assigning each investigator a **unique investigator ID** (GUID). Investigator details are **stored in the case file** and will be transferred with the case file if it is moved from one analysis computer to another. Investigators details are also saved into a **local database** to ensure that they are automatically available in the drop down list for future cases. The default location for this database is: C:\Users\[profile]\Documents\Forensic Explorer\DataBases\LocalInvestigator.rsv. To **add**, **edit** or **delete** an investigator, see 10.2.1 - Managing Investigators, below.

Working Folder is the location of the files for the case. Edit this location if required.

Case Description is used to briefly summarize the case. This information is used in other parts of the program, such as in the “Recent Case” section of the Evidence module.

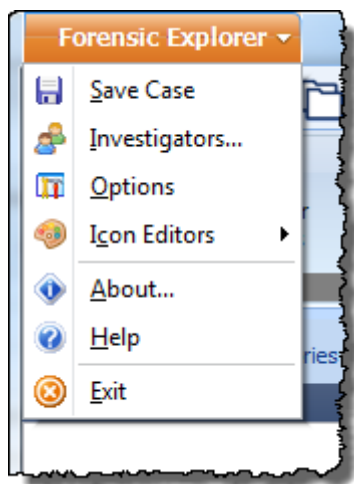
Case Created identified the date and time that the case is created according to the local system clock.

Click **OK** in the **New Case** window to create the case. Working folders for the case are written (see “Working Path” page 31) and the new case is saved for the first time. The **Processes** window will confirm when this process is complete. Evidence can now be added to the case. See “Add evidence to a case” on page 129.

10.2.1 MANAGING INVESTIGATORS

To **add**, **edit** or **delete** an investigator, select “Investigators” from the Forensic Explorer drop down menu:

Figure 104, Forensic Explorer drop down menu



Select and edit the investigator as needed:

Figure 105, New Investigator

The screenshot shows a window titled "Investigators" with a list of investigators on the left and a form for adding a new investigator on the right. The list on the left contains "John Smith" and "Graham Henley", with "Graham Henley" selected. The form on the right has fields for "Investigator ID", "Full Name", "Title/Position", "Organization", and "Department". Below these is a tabbed section with "Contact" and "Address" tabs. The "Contact" tab is active, showing fields for "Phone", "Fax", "Cell/Mobile", "Email", and "URL". At the bottom of the window are "Add", "Delete", "Save", "Reset", "OK", and "Cancel" buttons.

Field	Value
Investigator ID	{1957C8C6-BDEA-44C7-8650-88609D8E662D}
Full Name	Graham Henley
Title/Position	Director
Organization	GetData
Department	Support
Phone	+61 (0)2 82086053
Fax	+61 (0)2 9588 1195
Cell/Mobile	61 414697579
Email	support@getdata.com
URL	www.getdata.com

10.3 OPEN AN EXISTING CASE

To open an existing case,

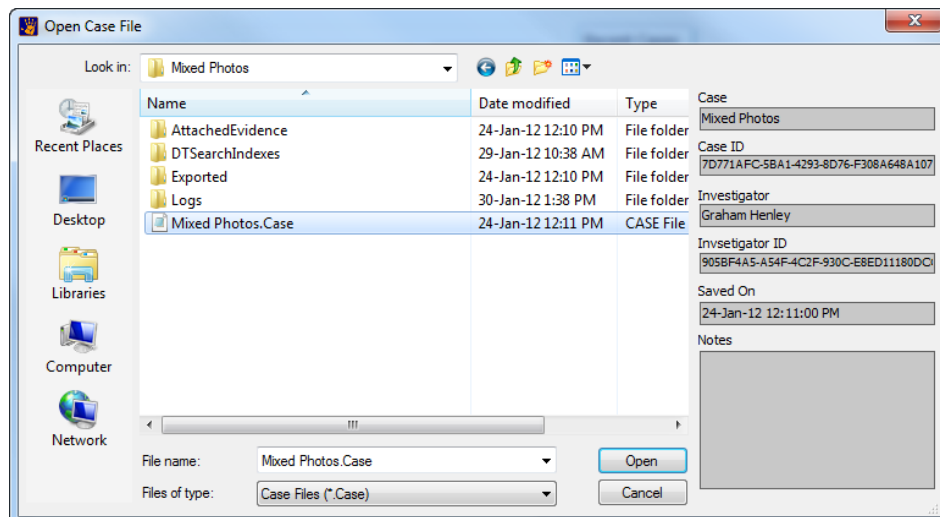
1. Click the **Open** button in the **Evidence module**:

Figure 106, Evidence module, new case button



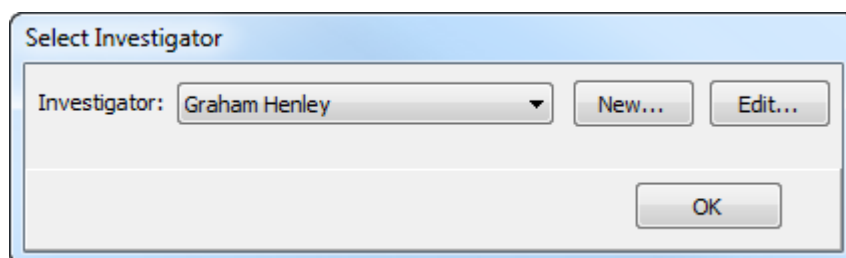
This will open the “Open Case File” window. When a **.case** file is highlighted the meta-data for that case is displayed on the right hand side of the Open Case File window (shown in Figure 107 below). Click **Open** to open the case file.

Figure 107, Open Case File



2. The **Select Investigator** window opens so that the person who is about work on the case can be identified. Select your name from the drop down list. Click **Edit** to preview and change your details if required. If your name does not appear in the drop down list, click “**New...**” to create a new investigator. Click **OK** to continue.

Figure 108, Select investigator window



The evidence in the case will then populate and display in the “Evidence” window of the Evidence module.

10.3.1 RECENT CASES

Recent cases can quickly be opened by selecting the case name from the “**Recent Cases**” list on the **Evidence module**.

When a recent case is highlighted in the Recent Cases list, the “case description” entered when the case was created will be displayed in the description field, as shown in Figure 109 below:

Figure 109, Evidence module > Cases tab, Open recent cases

Recent Cases		
Case	Details	Age
Name:	Test Case 3	
Investigator:	Graham Henley	Less than
Created:	06-Jun-12 12:28:11 PM	1 minute
Name:	Test Case 2	
Investigator:	Graham Henley	2 mins
Created:	06-Jun-12 12:25:47 PM	
Name:	Test Case 1	
Investigator:	Graham Henley	3 mins
Created:	06-Jun-12 12:25:00 PM	

Case Summary		
This is test case 3		

10.4 ADDING EVIDENCE

Evidence in Forensic Explorer can be:

- A device;
- A forensic image;
- A registry file;
- A file;

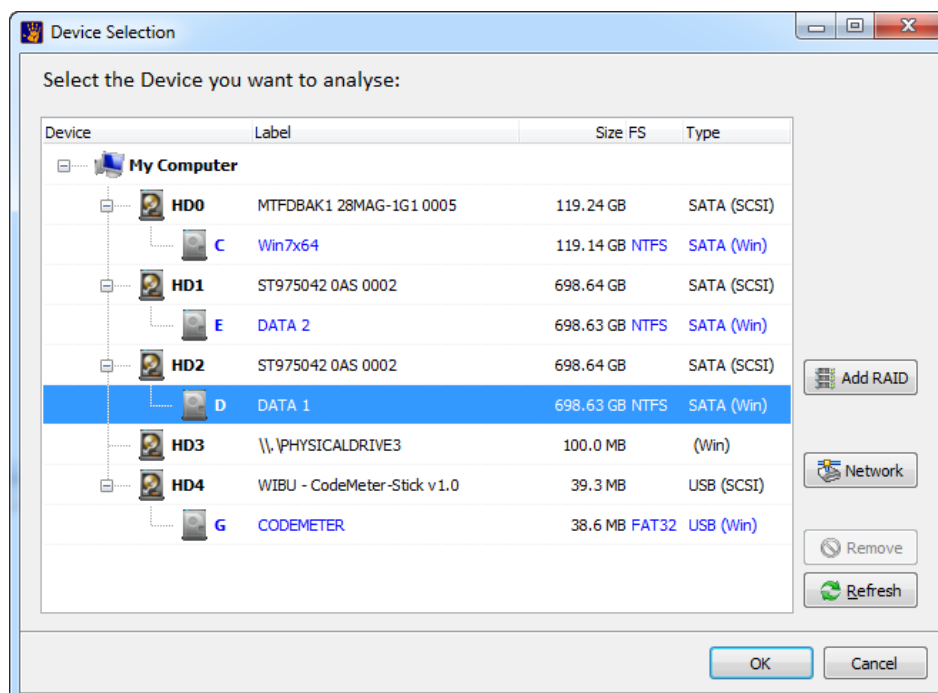
10.4.1 ADDING A DEVICE

IMPORTANT: When working with physical devices or active files, accepted forensic procedure dictates the use of a write block. Refer to Appendix 2 - Write Blocking, for more information.

To **add a device**:

1. Create a preview (see 10.1), a new case (see 10.2), or open an existing case (see 10.3);
2. In the **Evidence module**, click the “**Add Device**” button. (If the Add Device is inactive, click on the case name in the evidence window to activate the buttons). This will open the **Device Selection** window show in Figure 110 below:

Figure 110, Device Selection window



The Device Selection window includes the following information:

- Label:** Physical drives are listed with their Windows device number. Logical drives display the drive label (if no label is present then "{no label}" is used).
- Size:** The size column contains the size of the physical or logical device. Note that the actual size of the drive is usually smaller than what the drive is labeled. Drive manufacturers usually round up the drive capacity, so a 453.99 GB drive in this screen may be sold as 500GB.
- FS:** The File System on the drive, e.g. FAT, NTFS or HFS;
- Type:** Describes the way in which the drive is connected to the computer.

To add a **physical** or **logical** device:

1. **Highlight** the required physical or logical device and click **OK**, or;
2. To add a RAID, click the **Add Raid** button to access the RAID selection window. (Refer to Chapter 24 - RAID, for more information about examining RAID devices).

Troubleshooting: If the drive is not listed, check for basic connection issues (cables / power etc.). Check Windows Disk Management to ensure the device is being correctly recognized. Press the **refresh** button to refresh the Device Selection window.

3. Click OK to add the device. The **Evidence Processing Options** window will open. See 10.5 - Evidence Processor, below.

10.4.2 ADDING A NETWORK DEVICE

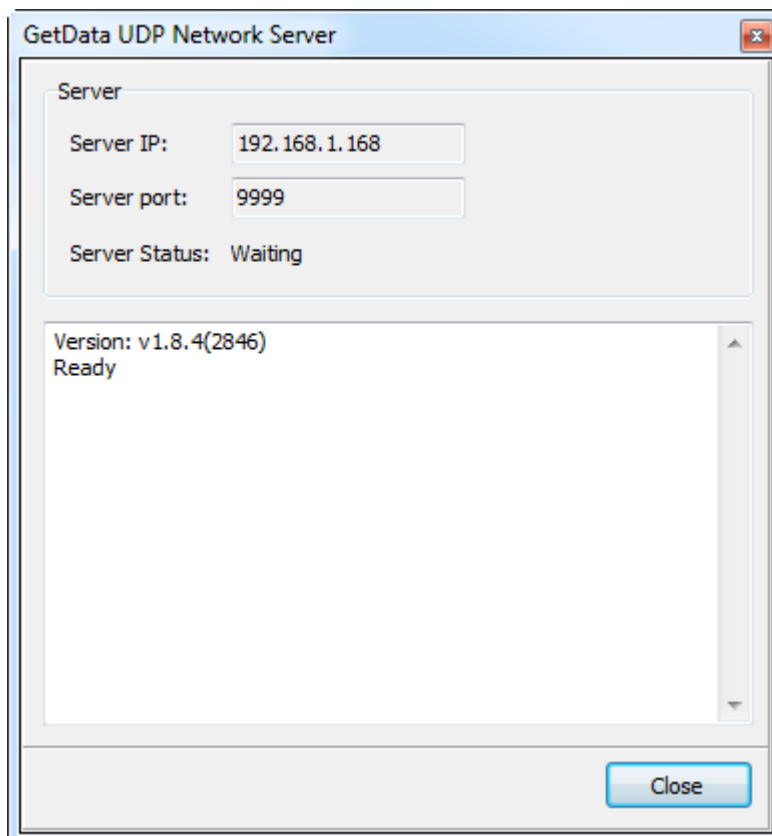
Forensic Explorer has the capability to examine remote devices across a network using the UDP protocol (User Datagram Protocol is one of the core members of the Internet Protocol Suite).

DEPLOY THE GETDATA UDP NETWORK SERVER

To examine a network device it is necessary to deploy and run the **GetData UDP Network Server**, GetDataNetworkServer.exe on the remote computer. This file can be found in the Forensic Explorer installation folder.

When the GetData UDP Network Server is deployed and run, the following screen appears:

Figure 111, GetData UDP Network Server



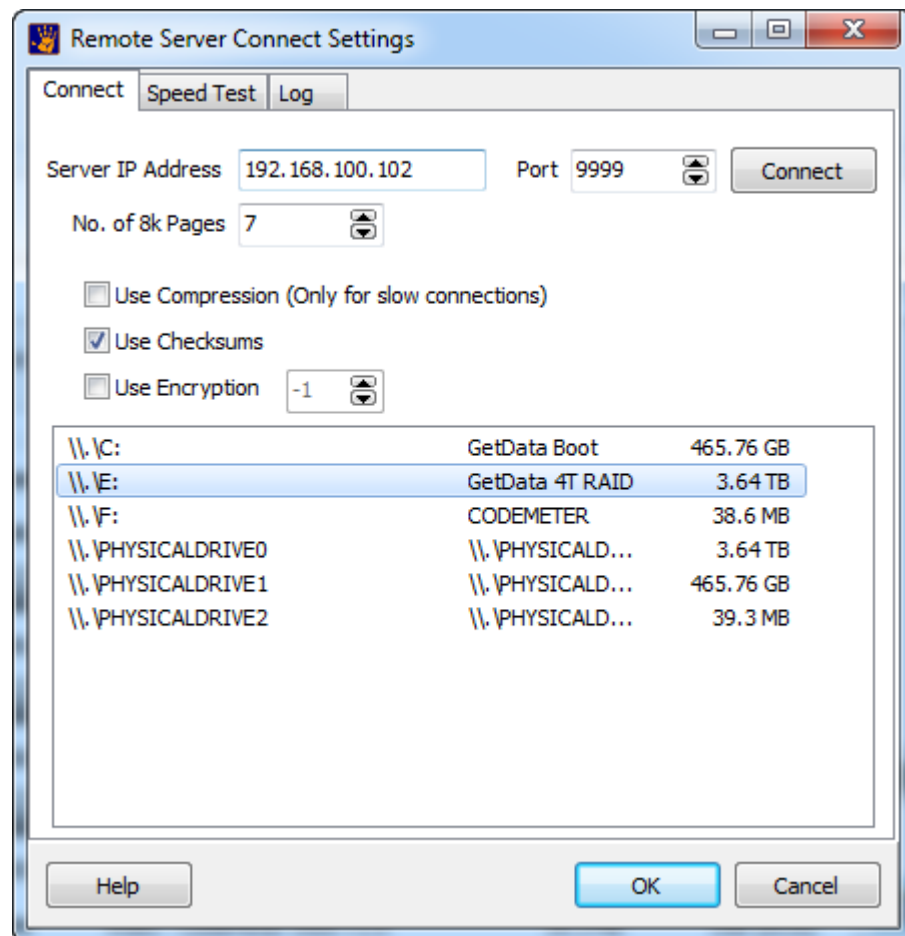
The server enters "waiting" mode for the connection from Forensic Explorer.

Note: It may be necessary to configure firewall settings on the remote computer to enable remote access to the GetData UDP Network Server.

CONNECTING TO THE GETDATA UDP NETWORK SERVER

To connect to the GetData UDP Network Server, follow "Adding a Device" in paragraph 10.4.1 above. In the Device Selection window, click on the **Network** button. The following screen appears:

Figure 112, Forensic Explorer Remote Server Connect Settings



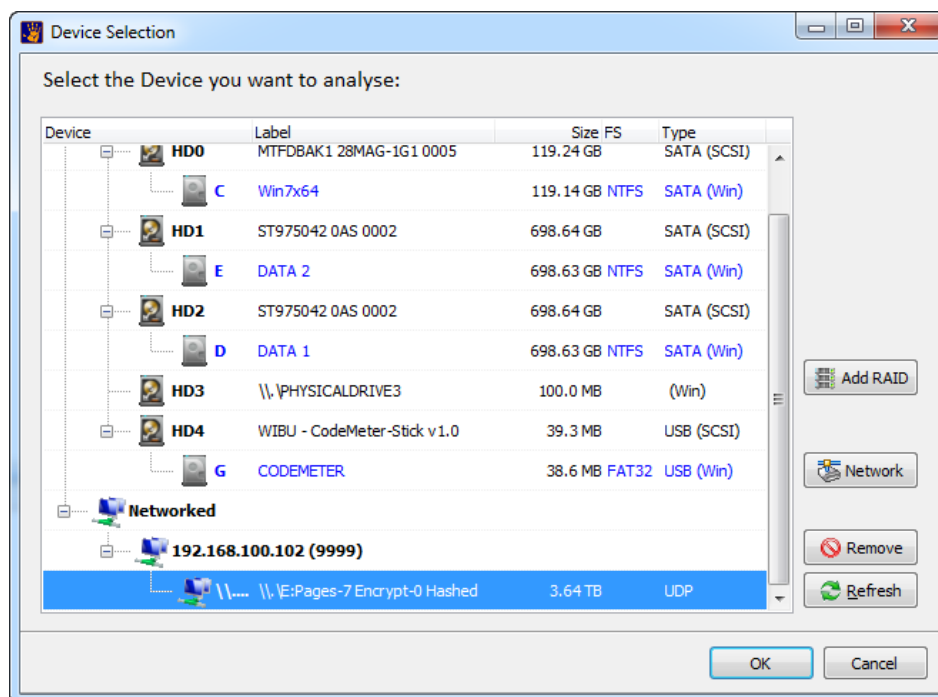
Server IP Address: Enter the IP address of the remote computer as displayed in the **Server IP** field of the GetData UDP Network Server.

Port: Ensure the Port number uses the same port as the GetData UDP Network Server.

Click the **Connect** button to view the available physical and logical devices on the remote computer. **Select** the required device and click **OK**.

The selected device should now appear under the **Networked** section of the Device Selection window, as shown in Figure 113 below:

Figure 113, Device Selection window showing a UDP connected network device



Click **OK** to begin processing of the drive.

10.4.3 ADDING A FORENSIC IMAGE FILE

To **add an image file to a case**:

1. Create a preview (see 10.1), a new case (see 10.2), or open an existing case (see 10.3);
2. In the Evidence module, click the **"Add Image"** button. (If the Add Image button is inactive, click on the case name in the evidence window to activate the buttons).

Note: Due to the low level processing requirements of most forensic investigations (e.g. sector level keyword searches, indexing, etc.) it is recommended that image files be located on a high speed device, such as a local hard drive (minimum USB2 speed).

3. Click OK to add the forensic image. The **Evidence Processing Options** window will open. See section 10.5 below.

10.4.4 ADDING A REGISTRY FILE

To **add a registry file** to a new **case**:

1. Create a preview (see 10.1), a new case (see 10.2), or open an existing case (see 10.3);

2. In the **Evidence module**, click the “**Add File**” button. (If the Add File button is inactive, click on the case name in the evidence window to activate the buttons). This will open the add file window.
3. **Select the registry file** and click **OK**. The Evidence Processing Options window will open. See section 10.5 below.

Note: A registry file can also be added from the File System module. **Locate the registry file, right-click** and select **Send to > Registry** from the drop down menu. See 15.2 for more information.

10.4.5 ADDING A FILE

To add a **file** to a case:

1. Create a preview (see 10.1), a new case (see 10.2), or open an existing case (see 10.3);
2. In the Evidence module, click the “**Add File**” button. (If the Add File button is inactive, click on the case name in the evidence window to activate the buttons).
3. Click OK to add the file. The Evidence Processing Options window will open. See section 10.5 below. The file will be added to the File System module.

10.5 EVIDENCE PROCESSOR

The **Evidence Processor** window opens when evidence (a device, image or file) is added in the Evidence module. The **Evidence Processor** window has two functions:

1. To configure the processing options that will **automatically** take place when the evidence is added;

Note: Evidence processing tasks, such as file carving, do not have to be automatically run. They can be individually run later in the case.

and;

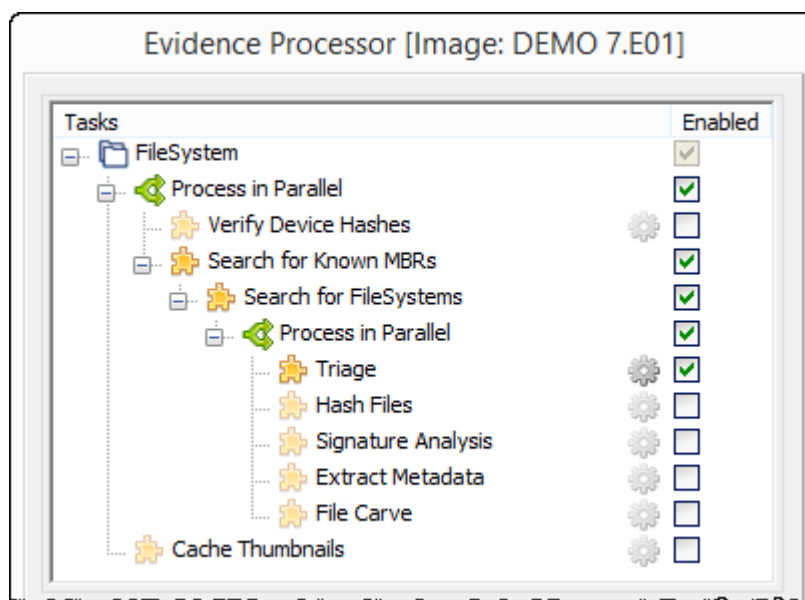
2. To enable the forensic investigator to modify dates and times in the evidence relative to the time zone in which the evidence is situated or was acquired.

Note: Time zone settings can be configured or adjusted later in the case from the File System module. See Chapter 20 - Date and Time, for more information.

10.5.1 PROCESSOR TASKS

Forensic Explorer determines the type of evidence added (e.g. device, forensic image, registry file, or other file) and displays a default tasks list according to the file type.

Figure 114, Evidence Processing Options (showing options for a forensic image or device)



The Tasks window enables the investigator to configure specific tasks (such as hashing, signature analysis and file carving) that will automatically take place when evidence is added. Whilst it is possible to perform these functions independently at a later time, the processing window enables the investigator to batch these tasks at the start of the case.

The task window uses the following icons:



Parent / Child: Indicates a parent / child relationship between tasks. A parent tasks must be completed before a child task can commence.



Process in Parallel: Identifies that the tasks listed in the immediate sub folder will process concurrently in separate threads.



A task: Indicates a task that can be enabled or disabled.



Task options: Identifies that settings for the task must be configured if it is enabled.

DEFAULT TASKS

The default settings in the Evidence Processing window when adding a device or an image file is to read and display existing file systems. :

Search for Known MBRs

A Master Boot Record (MBR) is the very first sector on a hard drive. It contains the startup information for the computer and the partition table, detailing how the computer is organized.

Search for File Systems

Once an MBR is identified, Forensic Explorer then locates and identifies known file systems (i.e. FAT, NTFS, and HFS). The file and folder structure can then be read and populated in the File System module.

If these default tasks are not enabled, the device or forensic image file will be loaded as raw data with no file or folder structure.

OTHER TASKS

Triage Registry

Triage Registry is an inbuilt function of Forensic Explorer to automatically detect and process Windows registry files. The process is divided into two parts:

1. Detect registry files in a Windows file system and automatically send those files to the Registry module; then
2. Process the registry files in the Registry module to identify and bookmark common items of interest. This includes registry keys such as: registered owner; default Windows user name, Windows product ID and name, OS installation date, etc.

Items identified are bookmarked and can be seen in the Bookmarks module under the path: **My Bookmarks\Triage\Registry**. These bookmarks are used to automatically generate reports.

Verify Device Hashes

The “verify device hashes” task calculates a hash/s (MD5, SHA1, or SHA256) for the added device or forensic image.

If the forensic was created with EnCase®, the calculated hash/s can be compared with the acquisition hash stored within the forensic image to show that it has not been altered. The result of the hash is written into the evidence tab of the Evidence module (as shown in Figure 115 below):

Figure 115, Evidence module, Evidence tab, device hash

Description	LEXAR USB
Notes	This is an EnCase 7 E01 image of a 7gb lexar usb test disk
Acquiring Programm	7.3.1.203
OS Version	Windows 7
Acquired Date	17-May-12 2:25:55 PM
System Date	17-May-12 2:25:51 PM
Compression	Unknown
Password	0
Encase Hash(MD5)	0F88EB0647FF39C1598D76948344BC8B
Hash(MD5)	0F88EB0647FF39C1598D76948344BC8B
Hash(SHA1)	626786505244CCBBBD8FD1C52876A0EC5E105EAF
Hash(SHA256)	C92810E9DB12D4CFDF5FD3B9F28D4F0DB685E76438C6B...

A device hash can also be calculated at any time using the **Verify Devices** script. This script can be run either from the “Analysis Scripts” button in the File System module, or directly from the Scripts module. See 21.4 for more information.

Signature Analysis

Signature analysis is the process of identifying a file by its header rather than by other means. For example, identifying a file by its signature is a more accurate method of classification than using the file extension (e.g. .jpg), as the extension can easily be altered.

The signature analysis task can only take place subsequent to the identification of a file system. For this reason, it is a sub-task of “Search for FileSystems” (as shown in Figure 114 above).

Signature analysis can also be independently run in the File System module. Learn more about signature analysis in Chapter 22.

File Carve

File carving is the identification and extraction of file types from unallocated clusters using file signatures.

File carving can only take place subsequent to the identification of a file system. For this reason, it is a sub-task of “Search for FileSystems” (as shown in Figure 114 above).

File carving can also be independently run in the File System module. Learn more about file carving in section 23.4.

Extract Metadata

Extract Metadata is used to collect internal file data and make the information available in columns. For example, for a digital photo, metadata can include camera Make and Model, and the GPS coordinates of the photo.

The Extract Metadata option runs a script located in the Scripts module in the path \File System\Metadata to columns\Extract Metadata.pas. Once the data has been extracted, the metadata columns can be added to a list view.

PROCESSES LIST

When tasks are run in Forensic Explorer its progress is detailed in the “Processes” list. This list is accessed globally from any Forensic Explorer Module by clicking on the “Processes” tab in the bottom right hand corner of the main program screen.

10.5.2 ADJUST TIME ZONE

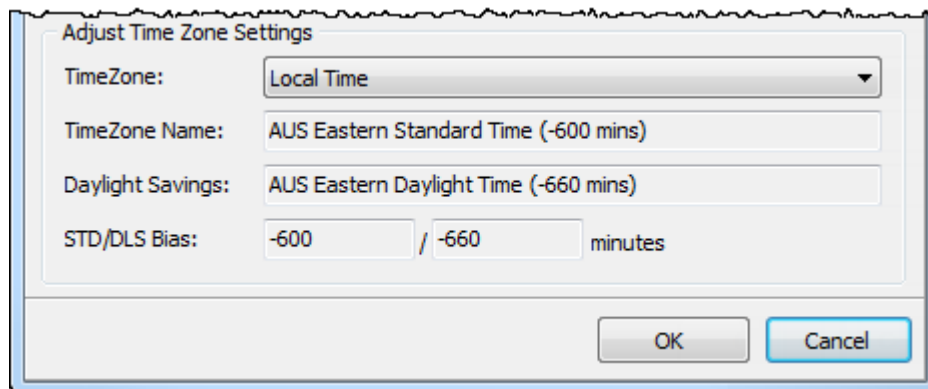
File date and times can be adjusted for each piece of evidence as it is added to a case. File date and times are adjusted according to the time zone from which the device or forensic image originates.

The default setting is to process the image according to **Local Time**, that is, the time zone setting on the forensic analysis computer. If the device or forensic image originates from the same time zone as the forensic analysis computer, then usually no adjustment is required.

If the device or forensic image is collected from a different time zone, change the Time Zone setting to the source location in order to display file date and times according to that location.

Note: Dealing with date and time issues in computer forensics is complex. Additional date and time adjustments can be made from the File System module once the evidence has been added. Refer to **Chapter 20** for further information.

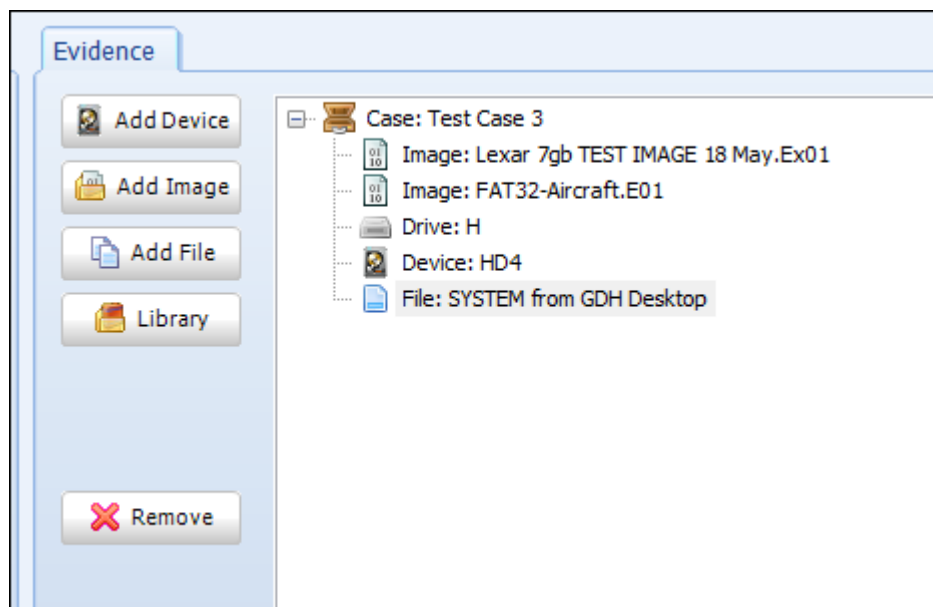
Figure 116, Adjust time zone information when adding evidence



10.6 ADDING ADDITIONAL EVIDENCE TO A CASE

Once added, a device, image, or registry file will appear in the “Evidence” field of the Evidence module, as shown in Figure 117 below:

Figure 117, Evidence module, Evidence list



To add an additional device, image or file:

1. Click on the case name (e.g. “Case: Test Case 3” above) to activate the add buttons;
2. Repeat the process described above.

10.7 SAVING A CASE

To **save** a preview, or save changes to an open case, click the **Save** button in the **Evidence module**:

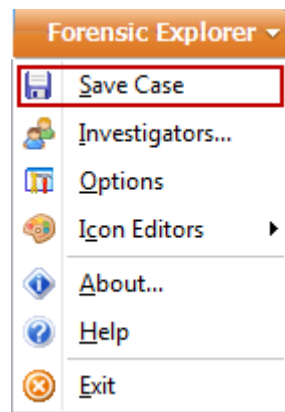
Figure 118, Evidence module, save button



Or;

In the Forensic Explorer drop down menu, select "Save Case":

Figure 119, Save Case



A case should be saved frequently to ensure that any changes since the last save are not lost.

10.7.1 SAVING OR CLOSING A PREVIEW

Each preview is assigned a unique working folder using a Global Unique Identifier (GUID) in the following path:

```
C:\Users\Graham\Documents\Forensic Explorer\Previews\{GUID - e.g.  
8709A41C-38B6-4F9E-BA18-633B394721C5}
```

When the investigator has finished the preview, analysis conducted during the preview may be:

1. **Saved as a new case** (see "saving a case" below). When a preview is saved the contents of the GUID working folder is transferred into the new case folder and the GUID folder is destroyed.
2. **Closed and not saved** (see "closing a case" below). When the case is closed and not saved, or when Forensic Explorer is opened or closed, the preview GUID folder is destroyed.

10.8 CLOSING A CASE

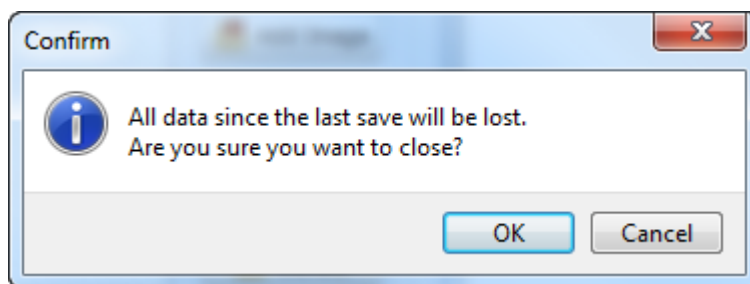
To **close** a preview or a case use the **Close** button in the **Evidence module**:

Figure 120, Evidence module, Close button



Case changes are NOT saved on close. If there are unsaved changes the following confirmation message box will appear:

Figure 121, Close confirmation message



Click OK to close without saving.

To save changes, click the Cancel button, return to the Evidence Module and use the Save button. The Reverse

Chapter 11 - File System Module

In This Chapter

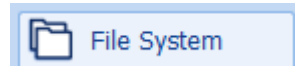
CHAPTER 11 - FILE SYSTEM MODULE

11.1	File System module	144
11.2	Toolbar	144
11.3	Folders view.....	144
11.3.1	Folders icons.....	145
11.3.2	ORPHANS.....	145
11.4	Categories view	146
11.4.1	Files by Extension	147
11.5	File List view	147
11.5.1	File List icons.....	147
11.5.2	File List Metadata Columns	147
11.6	Other data views	149

11.1 FILE SYSTEM MODULE

The File System module is accessed via the “File System” tab:

Figure 122, File System module tab



The File System module is the primary Forensic Explorer window where actions such as **highlighting, selecting, sorting, filtering, flagging, exporting** and **opening** occur.

For more information on these actions, see Chapter 9 - Working with data.

11.2 TOOLBAR

At the top of the File System module is the ribbon. The ribbon is a toolbar to hold buttons that perform functions of the program, such as hashing, data recovery or running scripts. It can also be used to create shortcuts to external programs.

The content of the ribbon in File System view is populated at startup by the **startup.pas script**. Subsequent to this, individual buttons or button groups can be added and removed by running scripts. See Chapter 18 - Scripts Module, for more information on toolbar scripts.

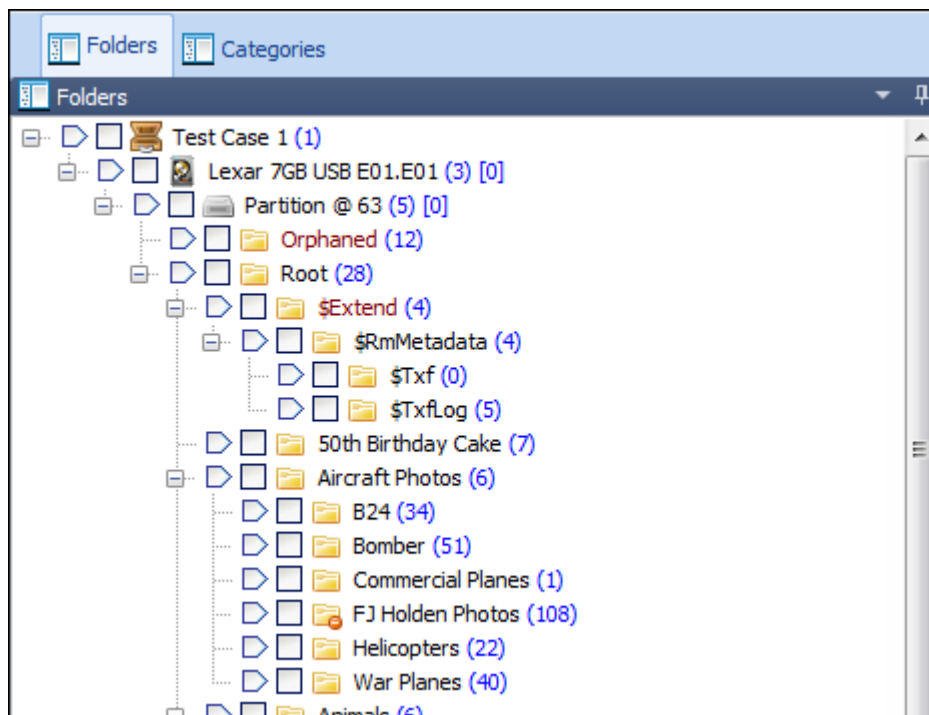
11.3 FOLDERS VIEW

Folders view is located in the top left hand window of the **File System module**.

The Folders view is a hierarchical display of items (e.g. devices, partitions, folders, etc.). Like Microsoft's Windows Explorer, the Folders view is most commonly used to select a folder, causing the contents of the folder to be displayed in the adjacent List view (described further below).

At the top of Folders view is the case name which acts as the root container for all other data. The case is the root of the tree from which all other data in the tree may be explored.









Figure 123, Folders View



Note: The blue number in brackets, e.g. “(2)” counts the number of items inside the folder (but does not count the contents of sub folders).

11.3.1 FOLDERS ICONS

The following icons are used in Folders view:

-  “Preview” (indicating a case has not yet been saved) or Case name
-  A device, e.g. a hard drive or camera card
-  Boot partition
-  Partition
-  An expandable branch (folder structure)
-  An active folder
-  A deleted folder
-  Folders containing the results of a file carve. For more information about file carving see chapter 23.4 - File carving.

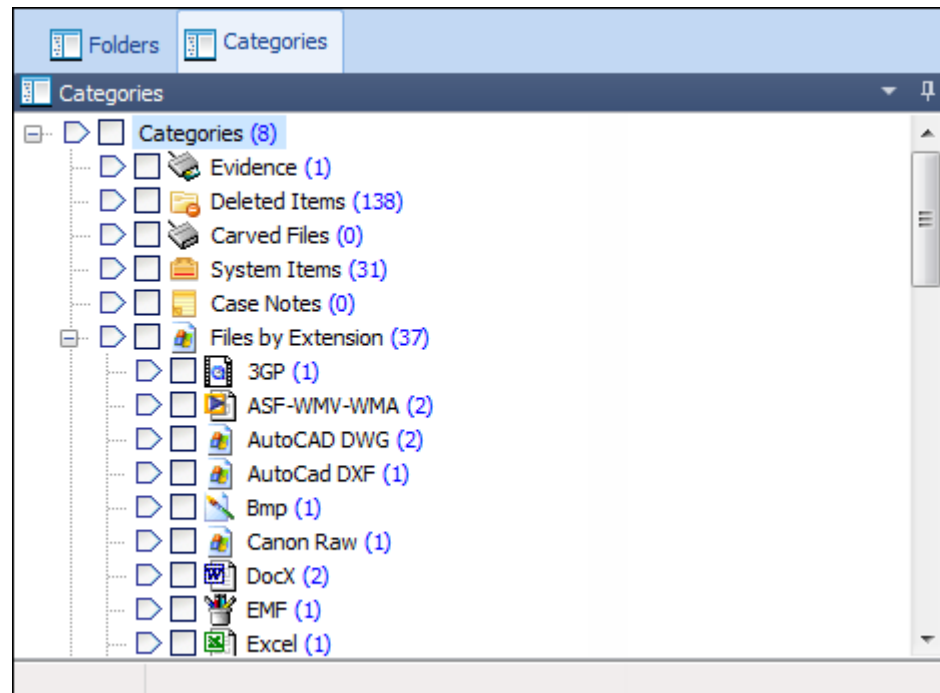
11.3.2 ORPHANS

One of the folders displayed in Folders view is ‘Orphaned’. Orphans are deleted folders and files for which the original parent folder is unknown. For more information on orphaned files see page 23.3.2 - NTFS - orphans.

11.4 CATEGORIES VIEW

Categories view is located in the in the top left hand window of the File System module next to the Folders view Tab. The **Category** view displays items **grouped by criteria**. The following category views are available:

Figure 124, Categories view



Note:

3. A **single file may appear in multiple categories**. For example, a **deleted JPEG** will appear under the categories “Files by Extension > JPEG”, “Deleted”, “Modified Date”, and any other category folder for which it meets the criteria.
4. Categorization of items takes place when a case is opened. If **case meta-data is created by the investigator**, e.g. files are hashed, skin tone analysis is run, flags are added etc. it is necessary to “rebuild categories” before these items will appear in their respective categories.

To re-categorize:

1. Right click inside the category view window;
2. Select “Rebuild categories” from the drop down menu.

The new case metadata should now appear in the respective categories.

11.4.1 FILES BY EXTENSION

Files without extension

Files without extensions will not appear in the **Files By Extension** Category unless a File Signature Analysis has been run and the categories rebuilt.











Once a Signature Analysis has been run, if it is a recognized signature, files without an extension will be placed in their relevant category (after a category rebuild) based on the file type identified in the file header.

11.5 FILE LIST VIEW

File List is located in the top right hand window of the **File System module**. File List displays content according to the selections made in Folders view (described above). File List view presents the metadata for each item (including file name, extension, full path, etc.) in a table format. It allows items (such as: devices, partitions and files) and their metadata to be sorted, highlighted, checked, flagged, opened and exported. For more information on these functions, see Chapter 9 - Working with data.

11.5.1 FILE LIST ICONS

The following icons are used in File List view to describe items:

- | | |
|---|-------------------------------------|
|  | Free space on disk |
|  | Free space in partition |
|  | Unallocated clusters on NTFS volume |
|  | An active file |
|  | An active folder |
|  | A deleted file |
|  | A deleted folder |
|  | A system file |
|  | A FAT "dot" directory entry |
|  | A FAT "double dot" directory entry |

11.5.2 FILE LIST METADATA COLUMNS


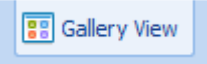

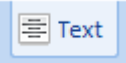

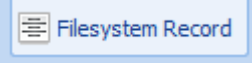

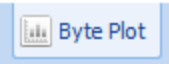
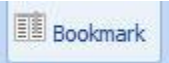
File metadata is displayed in columns. These columns include:

File Name:	The name of the item (system file, partition etc.) or the name of the file.
Extension:	The suffix to the file name, for example .jpg, which indicates the file format. This column reports the given file extension only and does not validate it as correct.
Flags:	A colored flag added by the investigator to mark a file.
Full Path:	Displays the location of the file. The case name examined device name is included in the path.
Attributes:	File attribute settings: R = Read only A = Archive S = System file H = Hidden file
File Signature:	This column receives data after a file signature analysis (see Chapter 22 - File Signature Analysis). If the column contains an extension it means that the file signature has been identified.
Logical Size:	The size of the file in bytes.
Physical Size:	The total size of the clusters occupied by the file.
Modified:	The date and time that a file was opened, edited, and saved.
Created:	The date and time a file was created in its current storage location (not necessarily the original creation date of the file itself).
Accessed:	The date and time a file was last accessed. Note that automated activities, such as a virus scanner, may cause the last accessed date of a file to be updated.
Bookmark Folder	A folder into which a bookmarked file is placed in the Bookmarks Module.
Is Deleted:	True or false to indicate whether a file is deleted.

It is possible to add columns using a script. An example of this is where the metadata values from a Microsoft Word document, e.g. Author, Title etc. are extracted and placed in to columns. See 8.11.1 for more information.

11.6 OTHER DATA VIEWS

Other data views used in the Files System module includes those summarized in the table below. For more detailed information on each view, see Chapter 8 - Data Views.

Data View	Summary of Function
 Disk View	A graphical display of the sectors which make up the examined device.
 Gallery View	A thumbnail presentation of the graphics files.
 Hex	A hexadecimal view of the currently highlighted data. Hex view includes a <i>Data Inspector</i> window where a highlighted block of Hex is dynamically decoded.
 Text	A Text view of the currently highlighted file.
 Display	A preview of the currently highlighted file.
 Filesystem Record	Displays information contained in the MFT record or FAT entry for the currently highlighted file.
 File Extent	Identifies the location of the highlighted file on the disk. It details the start, end and length of each data run on the disk.
 Byte Plot	A graphical representation of byte level data within the currently highlighted file.
 Bookmark	View bookmark information for the item.

Chapter 12 - Keyword Search Module

In This Chapter

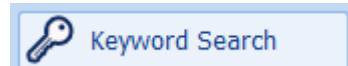
CHAPTER 12 - KEYWORD SEARCH MODULE

12.1	Keyword search	152
12.2	Keyword management	153
12.2.1	Creating a keyword.....	153
12.2.2	Edit or delete a keyword	155
12.2.3	Grouping keywords	156
12.2.4	Importing keywords	157
12.2.5	Running a Keyword Search	158
12.3	Search results	160
12.3.1	delete a keyword search folder (and keywords)	160
12.3.2	To delete a key word	161
12.3.3	Note: Why keyword hits differ when compared to EnCase®	161
12.4	Keyword result list	162
12.4.1	Hits.....	162
12.4.2	Hit Text	162

12.1 KEYWORD SEARCH

The keyword search module is accessed via the “Keyword Search” tab.

Figure 125, Keyword Search tab



A **keyword** is a user created search expression. A keyword can be a simple text, a more complex “Regular Expression” (RegEx), or hexadecimal. A **keyword search** is a search for that data.

Advantages of a Keyword Search:

- A keyword search can be performed on all data in a case, including unused disk space, unallocated clusters and system files;
- A keyword search can locate byte level fragments of data;
- Text translations allow the investigator to search for keywords in different languages.

Disadvantages of a Keyword Search:

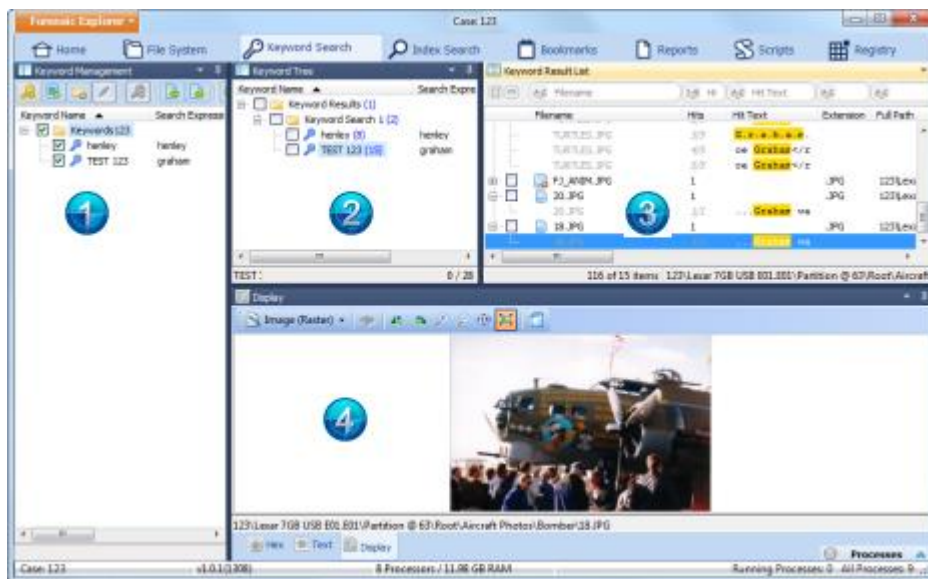
- A keyword search can be time intensive. The volume of data being searched, the number of keywords, and the speed of the computer hardware on which the search is run will influence the duration of the search.
- Each new keyword, or set of keywords, requires a new search. Because a search can be time intensive, keyword lists need to be carefully constructed to ensure to locate relevant data and limit false hits.
- When data is not in raw text format, for example a compressed file, keywords will not be located.

The keyword search module is broken down into the following four sections:

1. **Keyword Management:** Used to create and manage keywords and keyword groups;
2. **Keyword Tree:** List the search results for each keyword, including the number keyword hits;
3. **Keyword Result List:** Lists the files containing the keyword hits and previews the text around the keyword;
4. **Data Views:** Displays the file in which the keyword hit/s was found.

As shown in Figure 126 below:

Figure 126, Keyword Search module



12.2 KEYWORD MANAGEMENT

12.2.1 CREATING A KEYWORD

To create a keyword:


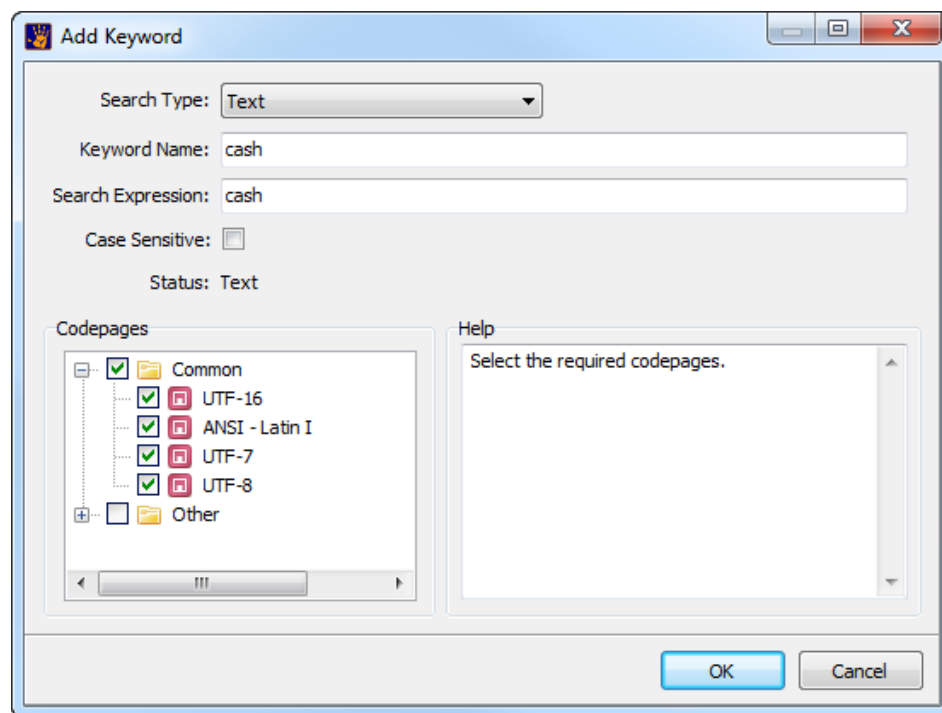
1. Preview, create, or open an existing case and click on the “**Keyword Search**” module tab;
2. To open the **Add Keyword** window (shown in Figure 12-3 below);
 - Click on the “**Add Keyword**” icon  in the “Keyword Management” (if the Keyword icon is inactive, highlight the “Keywords” folder in the “Keyword Name” window) ; or,
 - **Right-click** in the Keyword Management window and select “**Add Keyword**”; or,
 - Using the **keyboard**, select the “**CTRL**” and “**N**” key.

Figure 127, Add keyword



The **Search Type** drop down menu is used to identify the type of search:

Text:

A text search translates the entered keyword into the character encoding of the selected code-page formats. The default selection, UTF7, 8, 16 and ANSI will locate English and other non-complex languages in standard and Unicode format. When searching complex languages, such as Arabic, select the additional code-pages as required.

Regular Expression (PCRE)

A “Regular Expresssion” (RegEx, or Perl Compatible Regular Expression) is a *“concise and flexible means for “matching” (specifying and recognizing) strings text, such as particular characters, words, or patterns of characters”* (11). GREP is often misinterpreted as RegEx. GREP is a Linux/Unix program that is a RegEx search utility.

Basic RegEx functions include:

\wFFFF	Unicode character
\xFF	Hex character
.	Any character
#	Any number [0-9]
?	Repeat zero or one time
+	Repeat at least once
[A-Z]	A through Z
*	Repeat zero+ times
[XYZ]	Either X, Y, or Z
[^XYZ]	Neither X nor Y nor Z

\[Literal character
(ab)	Group ab together for ?, +, *,
{m,n}	Repeat m to n times
a b	Either a or b

Sample RegEx expressions can be loaded from the: "Forensic Explorer\Keywords" folder under the user profile.

For more RegEx examples, see:

- http://en.wikipedia.org/wiki/Regular_expression
- <http://regexlib.com/>
- <http://www.regular-expressions.info/reference.html>

Hexadecimal

The hexadecimal option allows hexadecimal values to be typed directly into the search window without formatting. Valid hex characters are 0-9, A-F, and space. For example, the keyword "cow" can be typed directly into this field as "636F77".

Keyword Name

Keyword Name is used to describe the search term (the Keyword Name is NOT the search term). For example, when searching for a credit card number with a RegEx expression: 45643#####, the Keyword Name can be "Visa Cards".

Search Expression

The "Search Expressions" field is where the keyword is entered.

Case Sensitive


If Case Sensitive is checked, the keyword search will match the exact case used in the search expression field.

The "Status" field provides real time feedback on the validity of the search expression entered. Once the keyword is entered, press the OK button to add the keyword to the Keyword Management list.


12.2.2 EDIT OR DELETE A KEYWORD

To edit a keyword:

1. **Highlight** the keyword with the mouse, then;
 - a. **Double click** on the keyword; or

- b. Select the **edit button**  from the toolbar; or
 - c. Right click and select **Edit Keyword** from the drop down menu.
 2. In the **Edit Keyword window** make the appropriate edit and click **OK** to save the changes. The adjusted keyword should now appear in the Keyword Management list.

To delete a keyword:

1. **Highlight** the keyword with the mouse;
 - a. Click the **keyword delete icon** ; or,
 - b. Right-click on the highlighted keyword and select “delete keyword” from the drop down menu);
2. Click **OK** to confirm the deletion.

See also deleting a keyword group below.

12.2.3 GROUPING KEYWORDS

Keywords can be grouped in the Keyword Management window.

To create a keyword group:


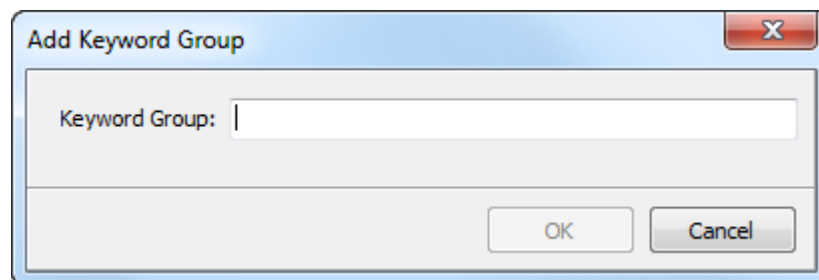
1. Click on the **add group icon**  to open the Add Keyword Group window (or right click in Keyword Management and in the drop down menu select “Add Group”);
2. Type the keyword group name and click **OK**.

Figure 128, Add Keyword Group window



To rename a group:

1. Double click on the group name to open the edit window. Edit the group name and click OK to save changes.

To **delete a group**:

1. Right click on the group folder icon and from the drop down menu select "Delete Keyword".

12.2.4 IMPORTING KEYWORDS

A list of keywords can be imported from a text file. To **prepare** a keyword text file, use the following formatting:

;	Indicates a comment and is ignored in the import
[Folder]	Creates a folder to group subsequent keywords
Keyword	To add a simple list of words, one keyword is placed on each line of the text file. Blank lines are ignored.
	To add additional parameters to the word, use the following format:
	Keyword Name, Search Expression,"CaseSensitive,Regex"


In the example below, two folders "Camera Types" and "PDF Header" are created. The Camera Types group contains a case sensitive keyword. The PDF Header group contains a case sensitive RegEx.

Sample Keywords.txt file:

```
; This is a list of digital camera related keywords

[Camera Types]
adobe,adobe,,"1200,1201,1252,65000,65001"
canon,canon,,"1200,1201,1252,65000,65001"
Olympus,Olympus,CaseSensitive,"1200,1201,1252,65000,65001"

[PDF Header]
PDF header,PDF-1.[0-9],,"CaseSensitive,Regex",
```

A fast way to learn the correct formatting is to add several groups and keywords by hand, then use the export button  to export the list. Then edit the list with additional requirements, and import the file using the instructions below.

To **import** a keyword text file;

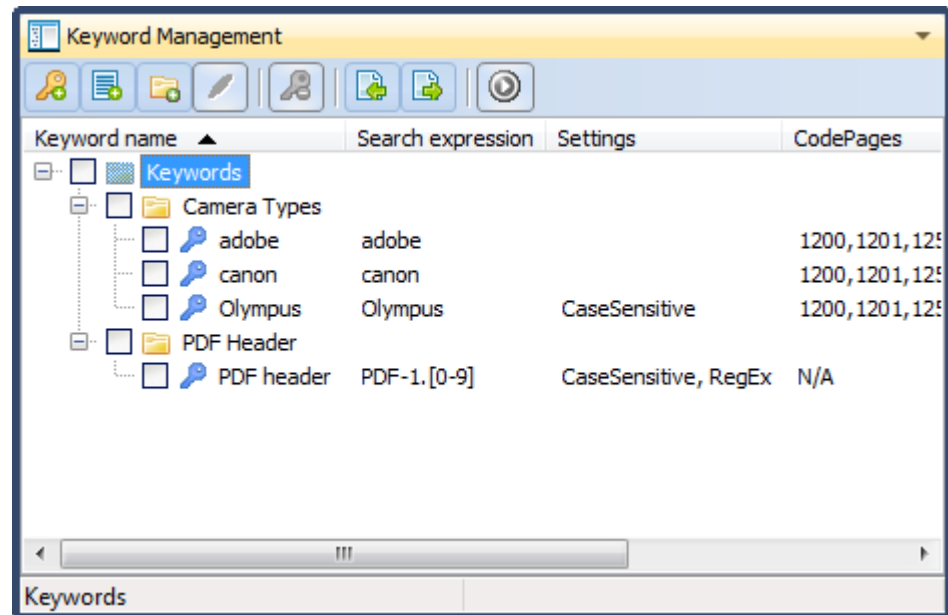
1. In the Keyword Management window click on the **Import Keyword List** icon



2. Browse to the required keyword text file, select the file and click "Open".

The keywords in the file will then populate the Keyword Management window. The result of importing the above “*Sample keyword.txt file*” is shown below:

Figure 129, Keyword Management after the import of the above keyword.txt file



12.2.5 RUNNING A KEYWORD SEARCH

To **run** a keyword search;


1. In the Keyword Management window, **select the keyword/s** to search by placing a **tick in the box** next to the required keyword/s;
2. **Click the green start button**  (or right click in the Keyword Management window and in the drop down menu select “Start Keyword Search”). This will open the “New Keyword Search” window shown in Figure 130 below:

Figure 130, New Keyword Search window

New Keyword Search

Name:

Items to search:

Data:

☒ All items (1424 items)

☐ Selected items (0 items)

Include:

☐ Unallocated space (5.95 GB)

☒ File slack (2.6 MB)

Total items to be searched (1424 items 1.52 GB)

Limits

Maximum hits per keyword, per file: (Blank = unrestricted)

Stop when total search hits reach: (Blank = unrestricted)

Keyword search name: This is the name of the search that will be shown in the Keyword Tree window. The keywords selected for this search and the number of hits per keyword will be displayed under the keyword search name.

Data: Select the data upon which the search is to be carried out, e.g. data from the File System or the Registry modules;

Include: Search either all items, or only those which have been checked;

Limits: Limitations can be set for the maximum number of hits per keyword per file, and the total number of hits.

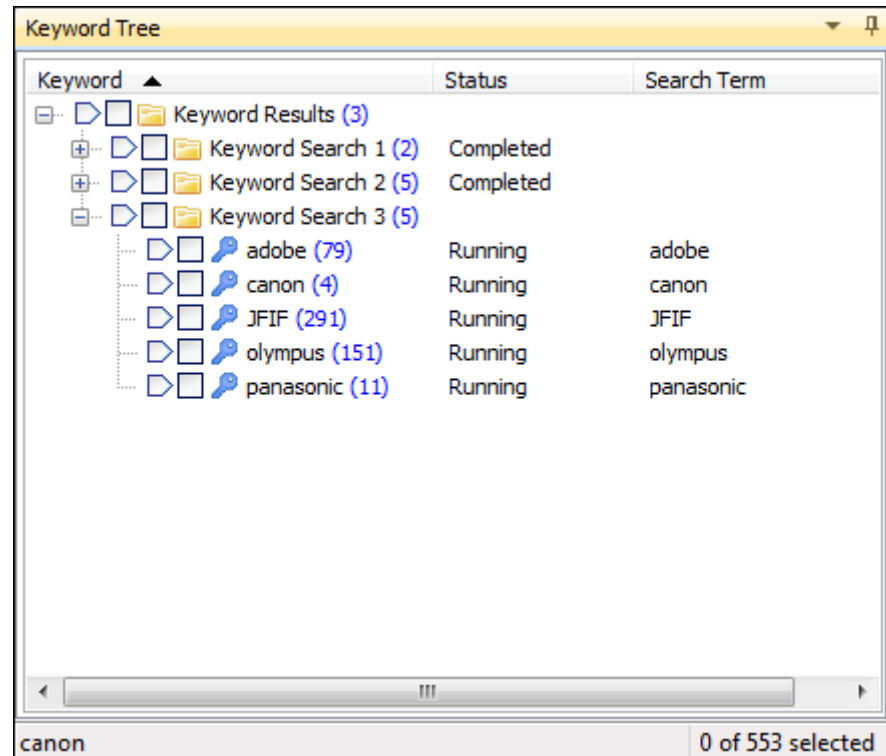
3. Click **OK** to commence the search.

Each search runs in its own thread, so multiple keyword searches can be executed at any one time. The **processes** window tracks the status of the search.

12.3 SEARCH RESULTS

The **Keyword Tree** window contains the search results, as shown in Figure 131 below:

Figure 131, Keyword Tree search results



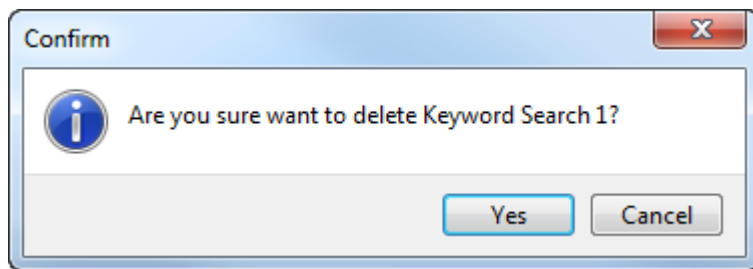
The **Keyword Results** folder at the root of the tree holds a folder for each search. The default search names are “Keyword Search 1”, “...2” etc.:

- Inside the search folder are the **keywords** for each search;
- **Blue brackets**, e.g. (10), next to a keyword identify the number of files in the case in which the keyword has been found;
- The **Status** column indicates if the search for a keyword is **running** or if it is **completed**.
- The **Search Term** column shows the formatting of the keyword string. It also identifies any search parameters, such as case sensitivity, or Unicode.

12.3.1 DELETE A KEYWORD SEARCH FOLDER (AND KEYWORDS)

To delete a keyword search folder, right click on the keyword folder and select “Delete” from the drop down menu. A confirmation message will appear:

Figure 132, Delete a keywords search folder



Upon confirmation, all search results within that keyword search folder will be deleted.

12.3.2 TO DELETE A KEY WORD

To delete a keyword:

1. Right click on the keyword;
2. Select **Deleted Keyword/s** from the drop down menu.

The same procedure is used to delete a keyword group (a folder containing multiple keywords).

12.3.3 NOTE: WHY KEYWORD HITS DIFFER WHEN COMPARED TO ENCASE®

A difference in the number of keyword hits can occur between Forensic Explorer and EnCase® (v7). This is due to the way each program deals with deleted files. For Example:

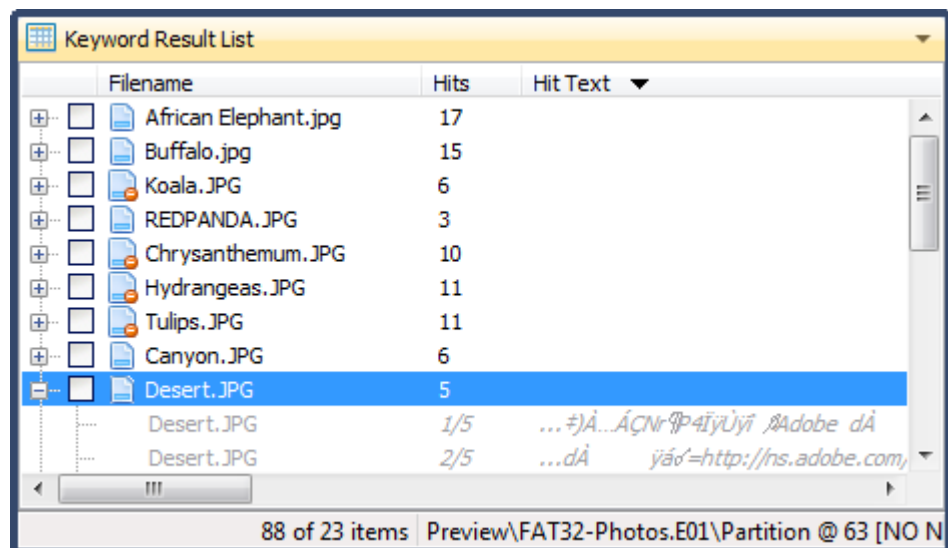
On a Fat32 system, EnCase® treats a deleted file as having 1 allocated cluster (the starting cluster is located in the directory entry of the file). If a keyword is located in this first cluster, the 'hit' is attributed to that file. Subsequent hits in the remaining clusters are identified as belonging to unallocated space.

On the same Fat32 system, Forensic Explorer identifies any search hit within the group of clusters attributed to a deleted file to belong to that file, and the file name appears in the Keyword Result List. In addition to this, as the space occupied by a deleted file is treated by the Windows Operating System as unallocated clusters, Forensic Explorer also attributes the same search hits to unallocated clusters.

12.4 KEYWORD RESULT LIST

When a keyword is highlighted, or a group of keywords is branch plated in the Keyword Tree any files which contain the keyword/s are displayed in the **Keyword Result List** window.


Figure 133, Keyword Result List



12.4.1 HITS

The Keyword Result List includes the “**Hits**” column which identifies the number of times the keyword/s has been found within a file.

12.4.2 HIT TEXT

Each file listed in the Keyword Result List has an expansion cross . Click on the expansion cross to preview the “Hit Text” of each keyword in the file. The Hit Text consists of **20 characters before and after the keyword hit**. It is designed as a quick reference guide to identify hits that require further investigation.

12.5 KEYWORD SEARCH DATA VIEWS

When a file is highlighted in the Keyword Results list, the content of the file is displayed in data views at the bottom of the screen. The data views available to the Keyword Search Module are Hex, Text and Display. Learn more in Chapter 8 - Data Views.

Chapter 13 - Index Search Module

In This Chapter

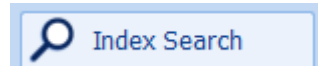
CHAPTER 13 - INDEX SEARCH MODULE

13.1	Index search	166
13.1.1	Indexed file types	166
13.1.2	Index database	166
13.1.3	Noise words	166
13.2	Considerations prior to creating an index	167
13.3	Creating an index	167
13.3.1	Index progress	168
13.4	Searching an index	169
13.4.1	Select the search features to use in your search	170
13.4.2	Boolean Search	171
13.4.3	Words and Phrases	172
13.4.4	Wildcards (*, ?, and =)	172
13.5	Search results	172
13.6	Index Search Compound Files	173

13.1 INDEX SEARCH

The Index Search module is accessed via the “Index Search” tab.

Figure 134 - Index Search module tab



An Index Search creates then uses a database that stores the location of words in the evidence. Forensic Explorer uses inbuilt dtSearch® technology for this purpose (for more information see <http://dtsearch.com/>). Once an index is built for a group of files very fast keyword searches can be performed on those files.

13.1.1 INDEXED FILE TYPES

For a list of the file formats supported by dtSearch® see "What file formats does dtSearch support" at <http://support.dtsearch.com>.
<http://support.dtsearch.com/dts0103.htm#Formats>

13.1.2 INDEX DATABASE

A keyword index is stored as part of a Forensic Explorer case. The default path is:

C:\Program Files\Forensic Explorer vX\Cases\case name\DTSearchIndexes\index name\

A keyword index is usually about one fourth the size of the original documents, although this may vary considerably depending on the number and kinds of documents in the index. The forensic investigator should make sure there is ample disk space available when creating an index.

13.1.3 NOISE WORDS

A noise word is a word such as “the” or “if” that is so common that it is not useful in searches. To save time, noise words are not indexed and are ignored in index searches.

To modify the list of words defined as noise words, edit the file:

C:\Program Files\GetData\Forensic Explorer v1\noise.dat

The noise word list does not have a particular order, and can include wildcard characters such as * and ?. However, noise words may not begin with wildcard characters.

When an index is created, the index will store its own copy of the noise word list. Changes made to the noise word list will be reflected in future indexes, but will not affect existing indexes.

13.2 CONSIDERATIONS PRIOR TO CREATING AN INDEX

Prior to creating an index it may be advantageous to recover any available data from the case and expose the data as files to the index process. For this reason the forensic investigator should consider first running:

- A Recover Folders search;
- A “file carve” for specific file types (see 23.4 - File carving).
- Decompress or decrypt any compound files not supported by dtSearch®.

13.3 CREATING AN INDEX

To **create an index**:

Open a case, or preview or start a new case and add evidence.

To **index checked files**

Switch to the required module tab; File System, Email or Registry, and select the required files, then switch to the Index Search module;

Or;

to **index the entire case**

Go directly to the Index Search module.

In the Index Search module, click on the “**New Index**” button. The New Index window will display, as shown in Figure 135 below:

Figure 135, New Index

New Index

Name:

Items to index:

Module:

☒ Searchable items (1 items)

☐ Checked items (0 items)

Include:

☐ Unallocated space (70.3 MB)

☐ File slack (0 bytes)

Total items to be indexed (1 items 0 bytes)

Name: The name given to the index. Each index must be given a unique name.

Items to Index: The module, e.g. File System, Email or Registry, from which the index will be generated (each module must be indexed separately).

Searchable items (x items): This selection will index all items in the selected module.

Checked items: The items which have been checked in the selected module.

Include: **Unallocated Space:** Determines whether unallocated space will be included in the index.

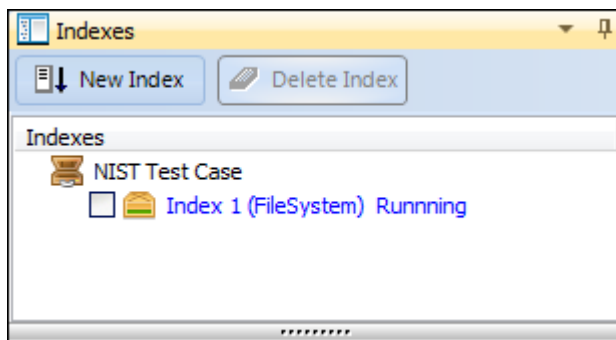
File slack: Determines whether the file slack of each file will be excluded from the index.

Click **OK** to start the index process.

13.3.1 INDEX PROGRESS

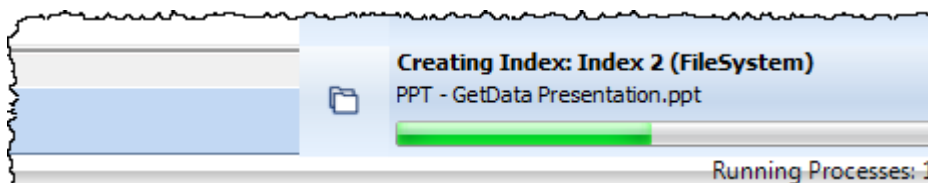
An index in progress will show “Running” in the Indexes window, as shown in Figure 136 below:

Figure 136, Index creation in progress



The progress is also tracked in the program process list, as shown in Figure 137 below:

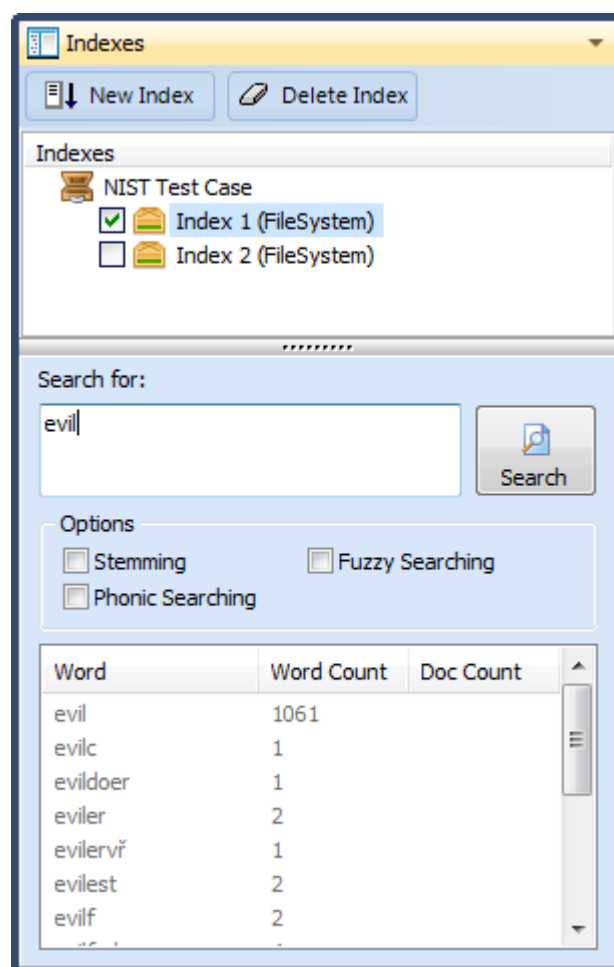
Figure 137 - Forensic Explorer process window showing a completed index



13.4 SEARCHING AN INDEX

When the indexing process is complete, the index will appear in the "Available Indexes" window, as shown in Figure 138 below:

Figure 138, Index search



Select the required index by placing a tick in the box next to the index name.

Type the search term into the “**Search for**” window. As the search term is typed, a list of index words is dynamically displayed showing:

1. The words in the index which match the typed criteria;
2. The number of times the word appears in the index (“Word Count”); and,
3. The number of documents in the index in which the word appears.

An alternate word can be selected from the displayed list by double clicking the required word.

13.4.1 SELECT THE SEARCH FEATURES TO USE IN YOUR SEARCH.

The following options can be included in the search, by selecting the relevant check box:

Stemming

Searches other grammatical forms of the words in your search request. For example, with stemming enabled a search for “apply” would also find “applies”.

Phonic searching

Finds words that sound similar to words in your request, like Smith and Smythe.

Fuzzy

Fuzzy searching sifts through scanning and typographical errors.

13.4.2 BOOLEAN SEARCH

A group of words or phrases linked by connectors such as AND and OR that indicate a relationship between them. For example:

Search Request	Meaning
apple and pear	both words must be present
apple or pear	either word can be present
apple w/5 pear	apple must occur within 5 words of pear
apple not w/12 pear	pear apple must occur, but not within 12 words of pear
apple and not pear	only apple must be present
apple w/5 xfirstword	apple must occur in the first five words
apple w/5 xlastword	apple must occur in the last five words

If you use more than one connector (and, or, contains, etc.), you should use parentheses to indicate precisely what you want to search for. For example,
(apple and pear) or (name contains smith)

13.4.3 WORDS AND PHRASES

For a more complex search which uses a phrase, use quotation marks around it, like this:

apple w/5 "my fruit salad"

If a phrase contains a noise word, dtSearch will skip over the noise word when searching for it. For example, a search for statue of liberty would retrieve any document containing the word statue, any intervening word, and the word liberty.

13.4.4 WILDCARDS (*, ?, AND =)

A search word can contain the wildcard characters:

- ? Matches any character
- = Matches any single digit
- * Matches any number of characters

The wildcard characters can be in any position in a word. For example:

appl*	Would match apple, application, etc.
cipl	Would match principle, participle, etc.
appl?	Would match apply and apple but not apples.
ap*ed	Would match applied, approved, etc.

Note: Use of the * wildcard character near the beginning of a word will slow searching.

13.5 SEARCH RESULTS

Search results display in the *Index Results* List view window, as shown in Figure 140 below. Select the relevant file in the Index Result List and the indexed content will display the Search Hits preview window.

Use the marker arrows to jump between highlighted hits:

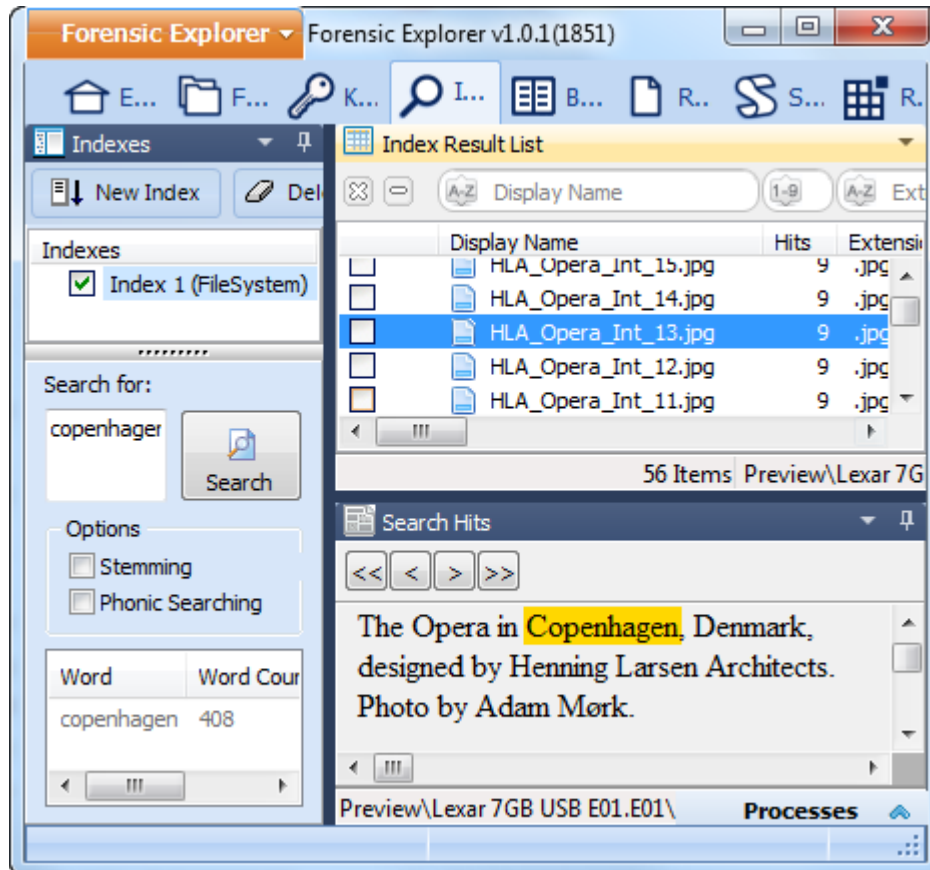
Figure 139, Navigate index search hits



Use the “Auto Scroll to First Hit” check box to automatically scroll to the first keyword hit in the Search Hits window.

Search hits are highlighted in yellow, as shown below:

Figure 140, Index search results



13.6 INDEX SEARCH COMPOUND FILES

DTSearch will index compound files, including PST and ZIP and display individual keyword hits within the messages and files.

It is also possible to add a compound file directly as evidence (use the **Add File** button in the Evidence module) and index its content.

13.7 EXPORT WORD LIST

The **Export Words** button (implemented in v2.3.6.3531 and above) is used to export the list of indexed words to a .csv file on the investigators computer. The list can then be used for password breaking or other purposes.

To export the indexed word list:

1. In the Index Search Module, Indexes window, check the required index;
2. Click on the **Export Words** button;

3. Select the name and location of the exported .csv file.

Chapter 14 - Email Module

In This Chapter

CHAPTER 14 - EMAIL MODULE

14.1	Email	176
14.2	Email module.....	176
14.3	Microsoft Outlook .PST email	176
14.3.1	Add a standalone oUTLOOK.PST file.....	177
14.3.2	Add a .PST file from a Forensic Explorer module	177
14.4	Index Search the Email module	177

14.1 EMAIL

Email analysis is an important component of computer forensics. The Forensic Explorer **Email module** currently supports examination of the following email formats:

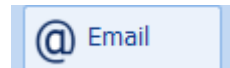
- **Microsoft Outlook** (.PST and .OST), all versions;

Note: It is possible to independently index and keyword search email in the **Index Search** module. Refer to Chapter 13 - Index Search Module, for more information.

14.2 EMAIL MODULE

The Email module is accessed via the “Email” tab.

Figure 141, Email module tab



The Email module is broken down into three panes:

1. **Email Tree**

Holds the folder structure of the email file;

2. **Email List**

Lists individual messages and their metadata. Available columns include;

- I (importance);
- Subject;
- Sent From, etc.

3. **Data Views**

Displays message content and additional properties. The **Property Viewer** contains Outlook MAPI (Microsoft Application Programming Interface) properties associated with each message.

14.3 MICROSOFT OUTLOOK .PST EMAIL

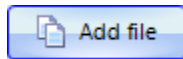
The Microsoft Outlook email client is available as part of the Microsoft Office suite. Microsoft refers to it as a “personal information manager” as it has additional functions to email, including calendar, contacts and notes.

When running on a typical home computer Outlook stores mail on the local hard disk in an **Outlook Data File (.PST)** file. In a business environment Outlook can be configured to interact with a mail server (usually Microsoft Exchange). In this case a local copy of the data may be held in an **Offline Data File (.OST)**.

14.3.1 ADD A STANDALONE OUTLOOK.PST FILE

To add a **stand-alone** Microsoft Outlook .PST file to the Email module:

1. In the Evidence module, start a new case or preview;
2. In the **Evidence module** click the “**Add File**” button.



3. **Select the .PST file** to add. Click “**Open**”. The .PST file will then be added to the case. Forensic Explorer will detect that it is a .PST file and add the content to the **Email module**.

14.3.2 ADD A .PST FILE FROM A FORENSIC EXPLORER MODULE

Add a **.PST file from within an existing case** to the **Email module**:

1. Locate the relevant .PST file in a module;
2. **Right click** on the **.PST file** and select “**Send to Email Module**” in the drop down menu. The content of the .PST file will then be populated in the Email module.

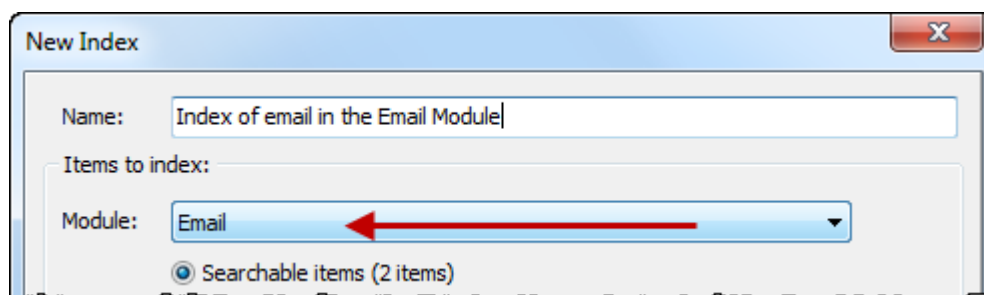
14.4 INDEX SEARCH THE EMAIL MODULE

Data that has been added to the Email module can be independently **indexed** or **keyword searched**.

To **index** the content of the **Email** module;

1. In the **Index Search** module, create a **new index**;
2. In the **New Index** window, select **Email** as the target module.

Figure 142, Index Search module, New Index window



Important:

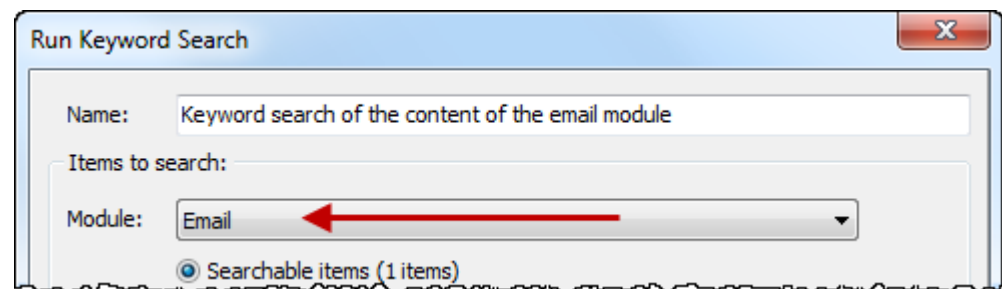
Creating an index of the content of the Email module is **NOT** the same as indexing a PST file that is located in the file system. DTSearch will already index a PST file that is located in the file system.

14.5 KEYWORD SEARCH THE EMAIL MODULE

To **keyword search** the content of the **Email** module;

1. In the **Keyword Search** module, start a keyword search;
2. In the **Run Keyword Search** window, select **Email** as the target module.

Figure 143, Keyword Search module, Run Keyword Search window



Chapter 15 - Registry Module

In This Chapter

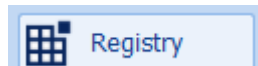
CHAPTER 15 - REGISTRY MODULE

15.1	Registry module.....	180
15.1.1	Windows location of registry files	180
15.2	Adding a REGISTRY FILE to the registry module	181
15.2.1	Add a standalone registry file	181
15.2.2	Add a registry file from a Forensic Explorer module	181
15.3	Registry Data Views	182
15.3.1	Registry Tree.....	182
15.3.2	Registry List	182
15.3.3	Hex, Text and Filesystem Record views.....	183
15.4	Deleted registry keys	183
15.5	Examining registry files using scripts	184

15.1 REGISTRY MODULE

The Registry module is accessed via the “Registry” tab:

Figure 144, Registry module tab



The Registry module is used to expand and examine Windows registry files. A Windows registry contains a great deal of information that can be of value to the forensic investigator.

“The Registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can create, property sheet settings for folders and application icons, what hardware exists on the system, and the ports that are being used.” Windows registry information for advanced users (12)

Unlike the Microsoft Windows registry editor, which is restricted to the current systems registry, Forensic Explorer allows the forensic investigator to examine registry files from any computer.

15.1.1 WINDOWS LOCATION OF REGISTRY FILES

The Windows Registry is physically stored in several files. The number of files, their name and location, will vary depending on the version of Windows in use. See <http://support.microsoft.com/kb/256986> “Windows registry information for advanced users (12)” for detailed information.

In most cases the forensic investigator will target the following Windows registry files:

Windows 95, 98, and ME operating systems have two registry files, located in the **C:\Windows folder and or Windows\profiles\user profile** folder:

- **system.dat**, and
- **user.dat**.

Windows NT based operating systems separate system registry data into four files, located in the **C:\Windows\system32\config** folder:

- **security**;
- **software**;
- **SAM**; and
- **System**.

User settings are stored in a separate file called **ntuser.dat** inside the user path.

15.2 ADDING A REGISTRY FILE TO THE REGISTRY MODULE

There are two methods to add a Windows registry file to the Forensic Explorer Registry module.

15.2.1 ADD A STANDALONE REGISTRY FILE

To add a **stand-alone registry** file to a case:

4. In the Evidence module, start a new case or preview;
5. In the **Evidence module** click the “**Add File**” button.
6. **Select the registry file** to add. Click “**Open**”. The registry file will then be added to the case. Forensic Explorer will detect that it is a registry file and add the content to the **Registry module**.

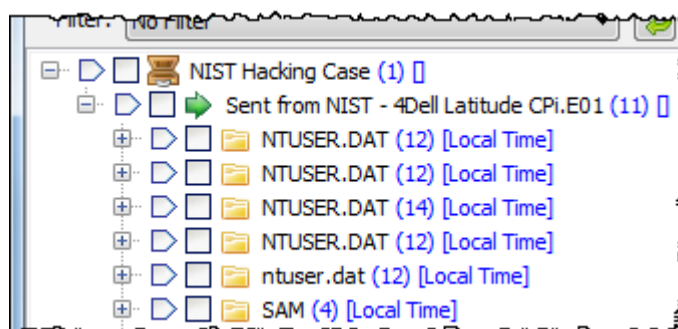
15.2.2 ADD A REGISTRY FILE FROM A FORENSIC EXPLORER MODULE

Add a **registry file from within an existing case** to the **registry module**:

3. Locate the relevant registry file in the File System module (use the locations described in 15.1.1 - Windows location of registry files, above);
4. **Right click** on the **registry file** and select “**Send to Registry Module**” in the drop down menu. The content of the registry file will then be populated in the registry module.

Registry files will be grouped by the originating device. Groups are identified by the “Sent From [device name]” folder, as shown in Figure 145 below:

Figure 145, Registry module showing "Sent from"

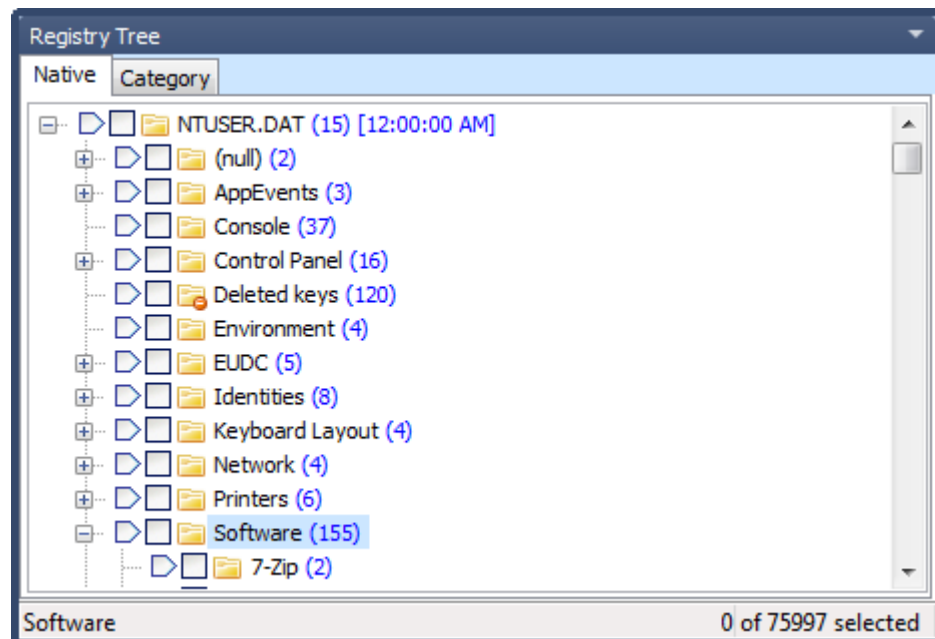


15.3 REGISTRY DATA VIEWS

15.3.1 REGISTRY TREE

The **Registry Tree** in the top left window of the Registry module lists the folders that contain registry keys, as shown in Figure 146 below:

Figure 146, Registry Tree, showing folders in NTUSER.DAT



The blue number in brackets, e.g. "(2)" shows the number of items inside the folder (but does not count the contents of sub folders).

For information on **navigating Tree views**, including branch plating, see page 74.

15.3.2 REGISTRY LIST

When a folder is highlighted in the *Registry Tree*, the contents of that folder are displayed in the *Registry List*, as shown in Figure 147 below:

Figure 147, Registry List view

Filename	Type	Data	Timestamp
Camtasia Studio	REG_NONE	(value not set)	13-Jun-10
UseHaspActivation	REG_DWORD	0x00000000 (0)	
TSCC	REG_NONE	(value not set)	23-Dec-11
SnagIt	REG_NONE	(value not set)	17-Jul-10
Filters	REG_NONE	(value not set)	17-Jul-10
~SecDesc	REG_BINARY	50 FF FF FF 73 6B 00 ...	

2 of 6 items NTUSER.DAT\Software\TechSmith\UseHaspActi

The following default columns are displayed in *Registry List* view:

Filename:	Gives the name of the registry item.
Type:	Describes the type of data held. See “List of standard registry value types” (13) for more information.
Data	The value stored.
Timestamp	The date attributed to the registry folder.
Physical Size	The physical storage size of the entry.

The Registry List view makes the standard analysis tools available from the right click menu. This includes: **Bookmarks** (See Chapter 14 - Bookmarks) and **sort** and **filter** (See Chapter 9 - Working with data).

15.3.3 HEX, TEXT AND FILESYSTEM RECORD VIEWS

Hex and Text data views are provided in the Registry module to give access to the raw data of the registry entry.

The Filesystem Records view decodes the entry and maps the decoded parts to the raw entry data.

15.4 DELETED REGISTRY KEYS

When a registry file is read by Forensic Explorer, the unallocated space within the registry file is parsed for deleted registry keys. These keys are placed into the “Deleted Keys” Folder, marked with the following icons:



Deleted key

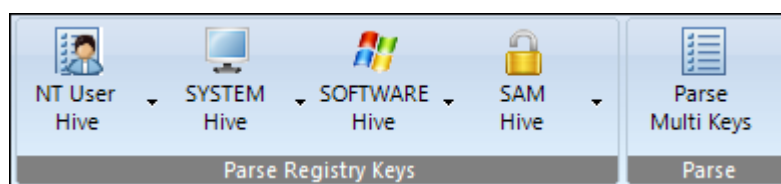


Deleted folder

15.5 EXAMINING REGISTRY FILES USING SCRIPTS

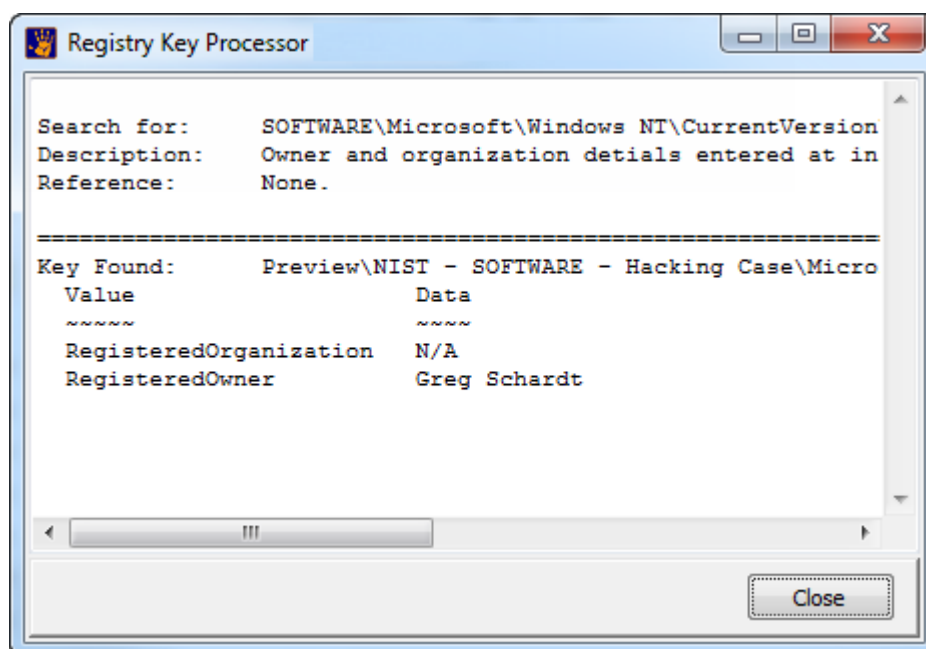
A default installation of Forensic Explorer includes a “Parse Registry Keys” button group in the Registry Module toolbar:

Figure 148, Registry Module, Parse Registry Keys



Each of the drop-down links in the button group passes a variable to the **Scripts/Registry/Registry Key Processor.pas** script to scan (and in some cases interpret) data of interest from specific keys. For example, selecting the “SOFTWARE > Registered Owner\Organization” button returns:

Figure 149, Registry Key Processor



The **Registry Key Processor.pas** uses a RegEx search to locate the relevant key. The script then process and displays the result according to its type (and any unique processing that the specific key requires).

IMPORTANT

It is important to note that automated registry key analysis is a developing field based largely on individual forensic practitioner research. Limited registry documentation relevant to pertinent keys is made available by Microsoft.

Also note that registry content is largely the result of user behaviour and that registry structure will change between Windows versions. The **Registry Key Processor.pas** script has been developed on sample registry hives and there is no guarantee that other hives will be parsed accurately.

As with the analysis of any Windows artefact, results from the **Registry Key Processor.pas** should be validated before being relied upon.

Chapter 16 – Bookmarks Module

In This Chapter

CHAPTER 16 - BOOKMARKS MODULE

16.1	Adding Bookmarks.....	188
16.1.1	Manually add a bookmark.....	188
16.1.2	Automated Triage bookmarks.....	189
16.1.3	Adding Bookmarks from a script.....	189
16.2	Bookmarks Module.....	190
16.2.1	Bookmarks tree.....	190
16.2.2	Bookmarks List.....	191
16.2.3	Bookmark Data Views.....	192
16.3	Identifying Bookmarked files other modules.....	193

16.1 ADDING BOOKMARKS

Bookmarks are used to annotate items of interest. Forensic Explorer enables almost any item (e.g. file, folder, keyword, search hit, etc.), or a selection from an item (e.g. a fragment of text from a file or unallocated clusters), to be bookmarked and listed in the Bookmarks module.

IMPORTANT: Forensic Explorer Reports are generated from Bookmarked items.

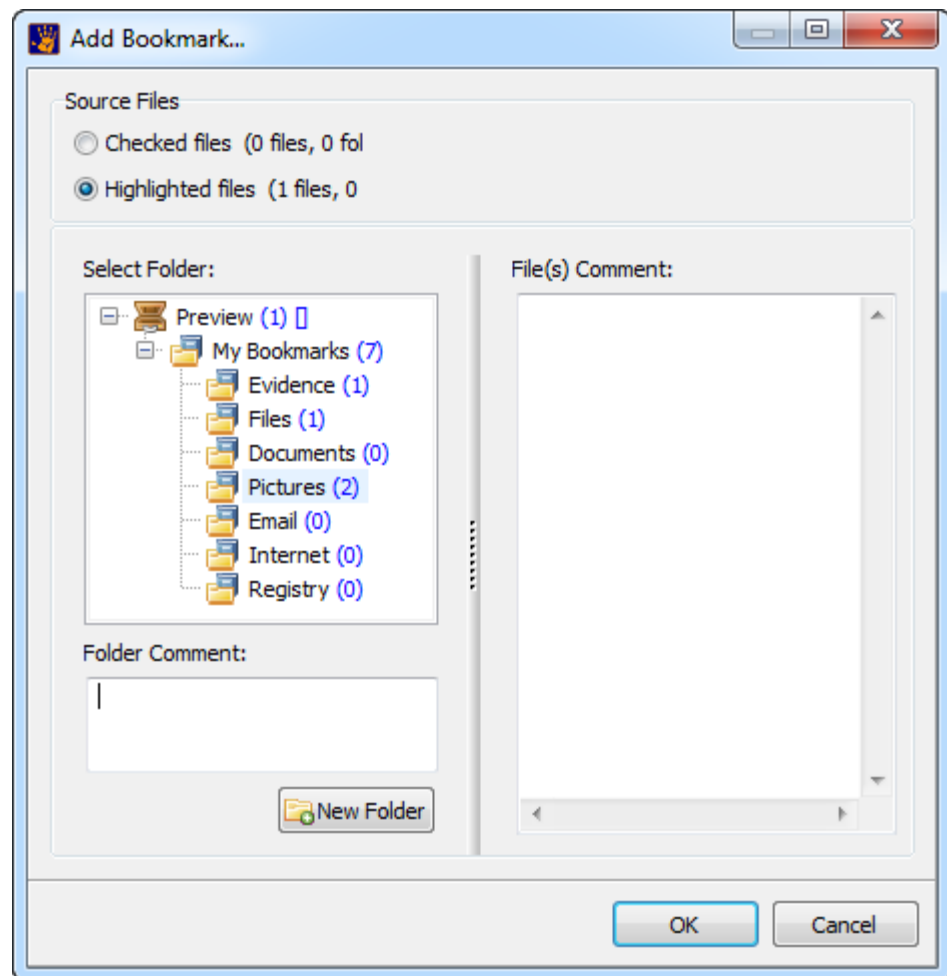
16.1.1 MANUALLY ADD A BOOKMARK

To manually add a bookmark:

- In a **Tree**, **List**, or **Gallery** view, **right click** on the required file/s and select “**Add Bookmark**” from the drop down menu; or,
- In a **Hex** or **Text** view, **highlight the required data** with the mouse, **right click** and select “**Add Bookmark**” from the drop down menu.

This will open the “Add Bookmarks” window, shown below:

Figure 150, Add Bookmarks window



Source Files:	A bookmark action can be performed on a highlighted file/s or checked files.
Select Folder:	<p>Folders are used by the investigator to group together bookmarked files of like interest. Folders can be moved using the mouse drag and drop.</p> <p>The right click drop down menu or the New Folder button enables the investigator to add or delete a folder.</p>
Folder Comment:	A comment about the folder holding the boomarked files.
File/s Comment:	A comment about the file/s being bookmarked.

16.1.2 AUTOMATED TRIAGE BOOKMARKS

When evidence is added to a case the option exists in the Evidence Processor (See 10.5) to “Triage” data.

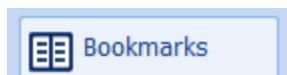
16.1.3 ADDING BOOKMARKS FROM A SCRIPT

Many of the scripts supplied with Forensic Explorer have the option to bookmark search results, (for example, **Discover PDF Files by Author**, located under the Analysis Scripts button in the File System module). The default folder for script bookmarks is: **My Bookmarks\Script Output**. A user who writes or modifies a script can select or create a bookmark folder of their choice.

16.2 BOOKMARKS MODULE

The Bookmarks module is accessed via the “Bookmarks” tab:

Figure 151, Bookmarks module tab



The bookmarks module provides a single location where items of interest are gathered together. The bookmarks module is divided into three areas;

1. Bookmarks tree;
2. Bookmark List;
3. Bookmark data views,

which are described in more details below.

16.2.1 BOOKMARKS TREE

The Bookmark tree displays:



Bookmark folders: used by the investigator to group together bookmarked files of a similar nature.

An example is shown in Figure 152 below:

Figure 152, Bookmark folder tree

Bookmarks			
Bookmark Name	Comment	Investigator Name	Modified
Test Case 31 (0)			
My Bookmarks (0)		Graham Henley	27-Feb
Evidence (0)		Graham Henley	27-Feb
Files (0)		Graham Henley	27-Feb
Documents (0)		Graham Henley	27-Feb
Pictures (2)	Important Pictures	Graham Henley	27-Feb
Email (0)		Graham Henley	27-Feb
Internet (0)		Graham Henley	27-Feb
Registry (0)		Graham Henley	27-Feb

MANAGE BOOKMARK FOLDERS

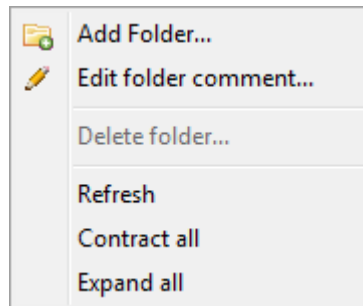
To add a bookmark folder:

Right click and select **Add Folder** from the drop down menu.

To **delete** a bookmark folder and its contents:

Right click and select **Delete folder** from the drop down menu:

Figure 153, Manage Bookmark folders



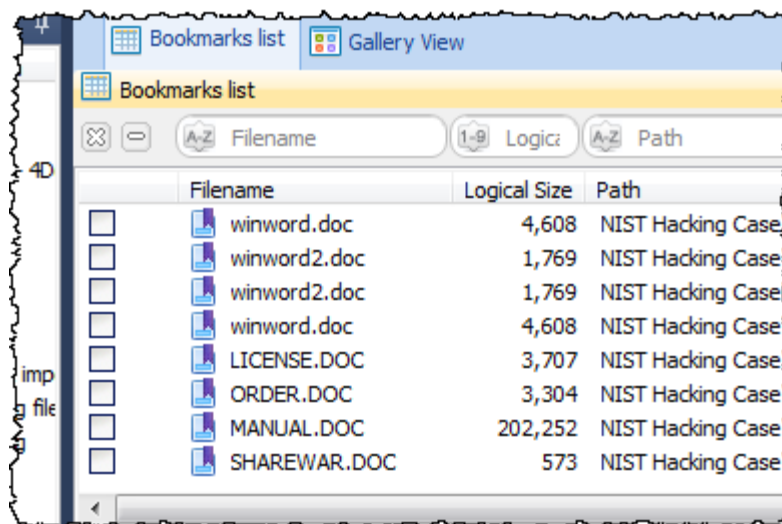
To **move** a bookmark folder:

Drag and drop an existing folder to its required location.

16.2.2 BOOKMARKS LIST

The Bookmarks List is a list view of the bookmarked items (files or data). Bookmarked files are identified by a bookmark icon that overlays the file icon, as shown in Figure 154, Bookmark list below:

Figure 154, Bookmark list



MANAGE BOOKMARK LIST

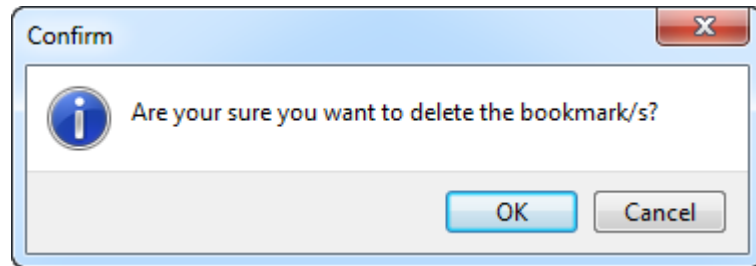
To **add** a bookmark:

See 16.1 Adding Bookmarks, above.

To **delete** a bookmark:

1. In the **Bookmarked Items List**, highlight the required file/s, **right click** and select **Delete Bookmark/s** from the drop down menu. The following confirmation window will appear:

Figure 155, Delete bookmark/s confirmation



2. Click OK to proceed. The file/s is deleted from the Bookmarks module.

To edit a bookmark comment:

1. Right click on the bookmark or a file in the Bookmarks List and from the drop down menu select **Edit bookmark comment**.
2. The **Edit Bookmark** window will open where the comment text can be updated.

To edit multiple bookmark comments:

1. **Highlight multiple bookmarked** files using the mouse and the SHIFT or CTRL key;
2. Right click and select **Edit Bookmark Comment** from the drop down menu;
3. The **Edit Bookmark** window will open. Edit the first bookmark and click **OK**. The comment will be updated for each of the bookmarks.

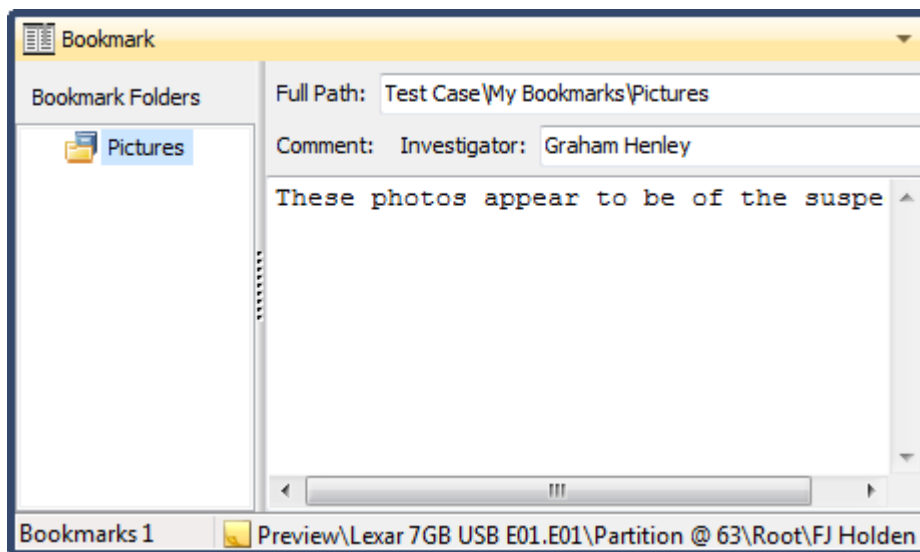
16.2.3 BOOKMARK DATA VIEWS

Data views enable the investigator to examine the item (device, folder, file, email message or registry key) that has been bookmarked. The data Views available in the Bookmarks module are: Bookmark, Gallery, Hex, Text, Display, Filesystem Record, and File Extent.

The **Bookmark data view**, shown in Figure 156 below, is visible in all modules. It enables the investigator to determine the Bookmark folder/s into which a file has been placed.

Right click on the view and select **"Edit bookmark comment..."** from the drop down menu to edit a comment.

Figure 156, Bookmark data view

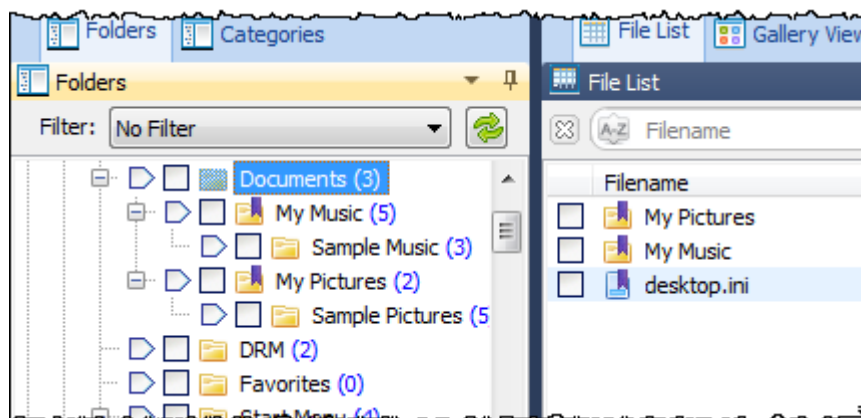


16.3 IDENTIFYING BOOKMARKED FILES OTHER MODULES

Bookmarked files can be identified in the File System module by:

1. A purple bookmark that overlays the file icon, as shown in Figure 157 below:

Figure 157, Bookmarked files in the File System module



2. The bookmark folder name is shown in the Bookmark Folder column (if a file has been bookmarked in multiple folders the column contains each folder name separated by a comma).

Chapter 17 – Reports Module

In This Chapter

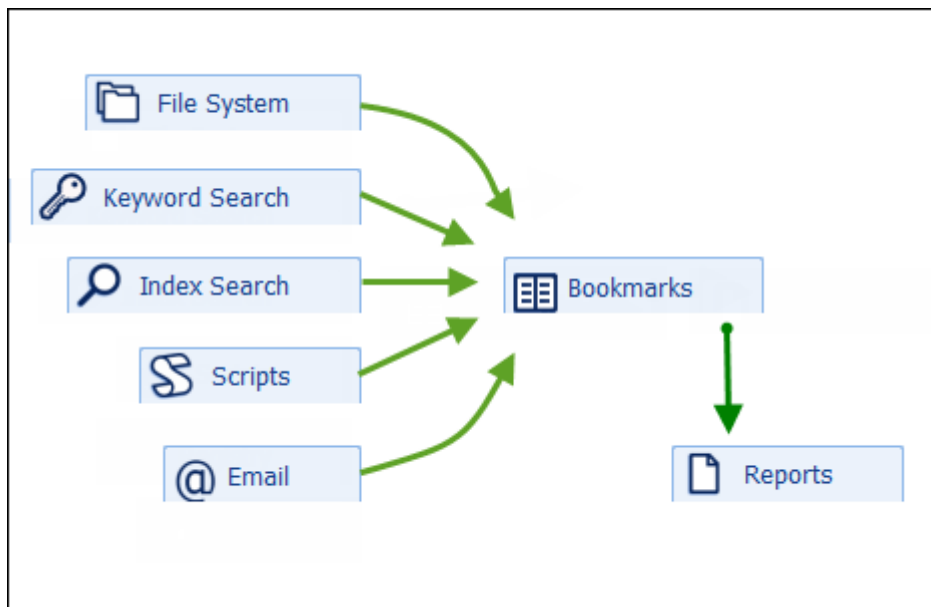
CHAPTER 17 - REPORTS MODULE

17.1	Reporting & Bookmarks
17.2	The Reports Module
17.3	ReportS Tree
17.3.1	The Default Report.....
17.3.2	Report name, Groups and Sections
17.3.3	Rename or Move a Group or Section.....
17.3.4	Print a report.....
17.3.5	Export a report as DOC, RTF or PDF
17.3.6	Export a report as a template
17.4	Report Editor.....
17.4.1	Report Editor Preview
17.4.2	Report Editor - EDIT
17.5	Creating Reports
17.5.1	Report exercises.....
	Exercise 1: Report on a single file
	Exercise 2: Listing bookmarked files in a table.....
	Exercise 3: Creating a GallEry view report

17.1 REPORTING & BOOKMARKS

The purpose of the Reports Module is to assist in the generation of a report that documents the forensic analysis. The Reports module is based on the use of templates that can be re-used across multiple investigations. A report template can be automatically populated with bookmarked items.

Figure 158, Modules > Bookmarks > Reports



Bookmarks are added manually, as the result of an automated triage, or as the output of a script. For more information about adding bookmarks see Chapter 16 above.

Care should be taken to arrange the bookmark structure effectively to fully maximize the use of report templates discussed in this chapter.

17.2 THE REPORTS MODULE

The Reports module is accessed via the “Reports” tab:

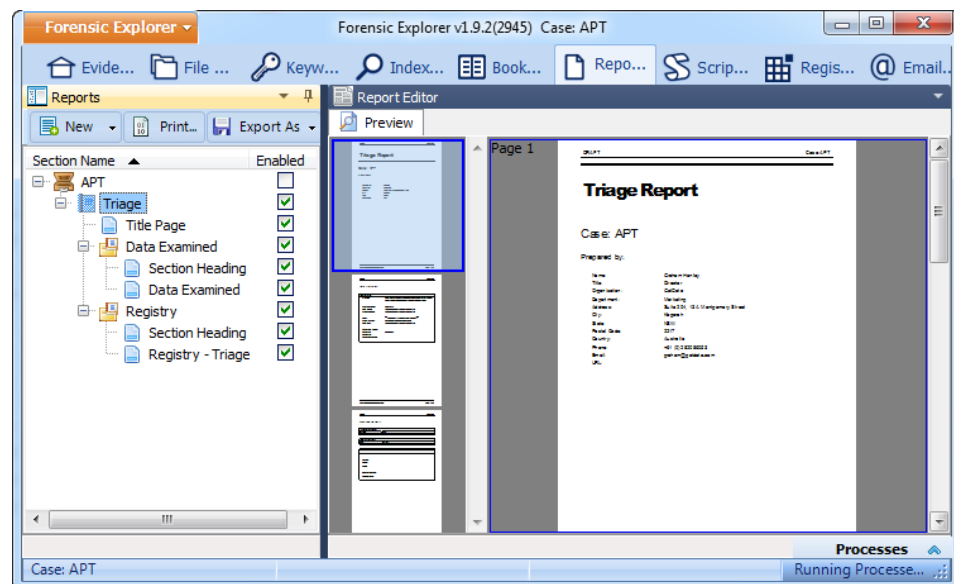
Figure 159, Reports module tab



The Reports module is divided into three main sections (as shown in Figure 160 below):

1. Reports tree
2. Preview window
3. Report Editor window

Figure 160, Reports Module showing the Triage Report



The sections are described in more detail below.

17.3 REPORTS TREE

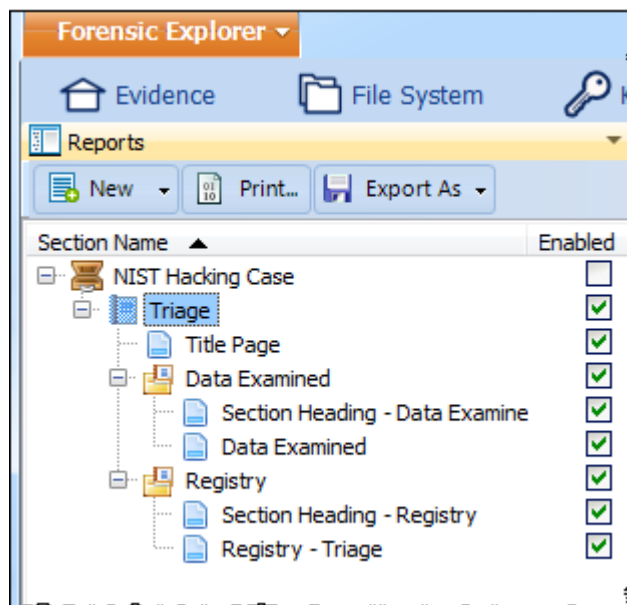
The Reports tree is the location where reports are managed. This includes:

- Loading a new report from a template;
- Printing or exporting a report as PDF, DOC or RTF;
- Deleting a report;
- Renaming reports;
- Rearranging sections of a report
- Exporting an edited report (or section of a report) as a new template.

17.3.1 THE DEFAULT REPORT

When Forensic Explorer is run for the first time and a new case or preview or is commenced and evidence added, the Reports module displays by default **Triage Report** (as shown in Figure 160 above). The dynamic content of the Triage report is obtained from the bookmarked files in the Bookmarks module under the **My Bookmarks\Triage** folder¹.

Figure 161, Reports Tree showing the Triage Report



¹ Triage bookmarks were created when the evidence was added to the case and the "Triage" option was run from the evidence processing window (see "Evidence Processor" on page 123 for more information). If the triage option was not selected, or there were no bookmarks found, the Triage report will contain blank fields.

CHANGING THE DEFAULT REPORT

To use a different report as default:

1. In the Reports tree, click the **New** button and select **Set Default** from the drop down menu;
2. Choose the desired report from the list. Any new case will now show the selected report as the default.

OPEN A NEW REPORT

All new reports are created from a template. Templates are located in the *...[profile]/My Documents/Forensic Explorer/Reports/Templates* folder. These templates are accessible for any case.

To **open a new report**;

1. Click on the **New** button in toolbar;
2. **Select** the desired report from the drop down menu.

The report is loaded from a template and added to the Report tree (click on the report name to preview its content). Once a report has been added to a case it becomes part of that case. It will remain with the case until such time as the report is deleted.

17.3.2 REPORT NAME, GROUPS AND SECTIONS

A report consists of the following components:



Report Name:

Click on the report name to preview the entire contents of the report in the preview window (see 0 below).

Note that it is possible to have more than one report open and visible in the Report tree.



Report Section:

A report section is used to compartmentalize content of the report. Click on a section to display its contents in the preview window (see 0 below). By using multiple sections additional control can be gained over how the final report is displayed (see Enabled checkbox below).



A group of sections:

A group is used to arrange like sections. Grouping also gives additional control on how the final report will be displayed. Click on the group to display the entire group content in the preview window (see 0 below).

**Enabled checkbox:**

The enabled checkbox determines if the sections or group will appear in a preview, print or export.

The Reports tree for the Triage report is shown in Figure 161 below:

17.3.3 RENAME OR MOVE A GROUP OR SECTION

To **rename** a report, group or a section:

- Using the mouse, click then hover on the name. Then type the new name in the edit window.

To **move** a group or section:

- Click on the group or section with the mouse and drag and drop the group or section to the desired location.

All rename or move options are automatically saved to the case.

17.3.4 PRINT A REPORT

To print a report:

- Click on the report name, or a section in the report, and click the print button. The Windows print dialogue will open.

17.3.5 EXPORT A REPORT AS DOC, RTF OR PDF

To export a report as a .doc, .rtf or .pdf:

- Click on the **Export As** button and select the desired formation;
- Save the file to the desired location.

Note: .docx and .rtf do not currently support the saving of page headers and footers.

17.3.6 EXPORT A REPORT AS A TEMPLATE

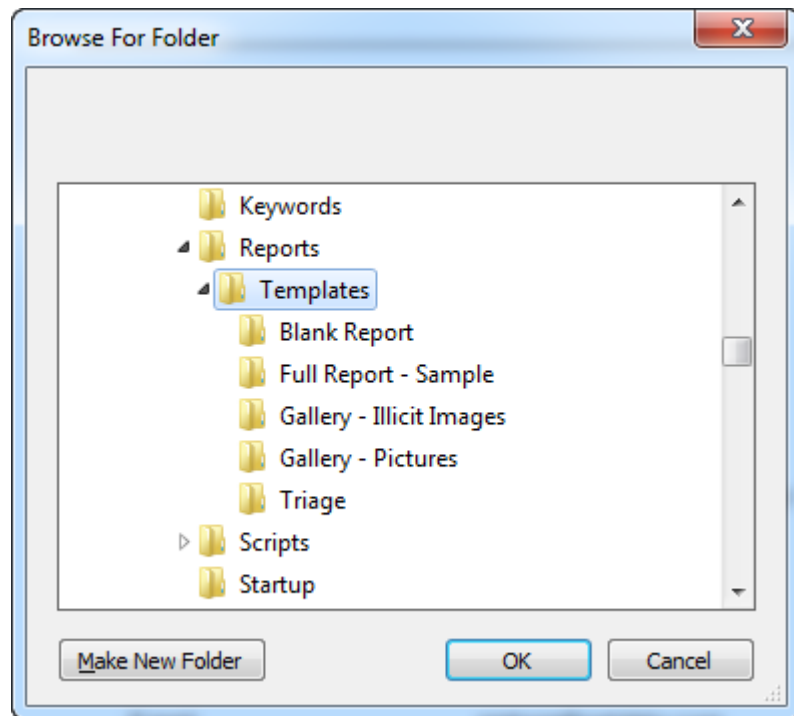
If a report has been changed, or a new report has been created, it may be beneficial to save it as a template so that it can be re-used in future investigations.

To **save a report as a template**:

1. In the Report tree, click on the name of the report;
2. Right click and in the drop down menu select **Save As Report Template**.

3. Browse to the required folder, or use the **Make New Folder** button to create a new destination:

Figure 162, Save a Report Template



4. Click OK to save the components of the report into the folder.

17.4 REPORT EDITOR

17.4.1 REPORT EDITOR PREVIEW

The Report Editor Preview (shown in Figure 163 below) displays the content of the currently selected report in the Report tree.

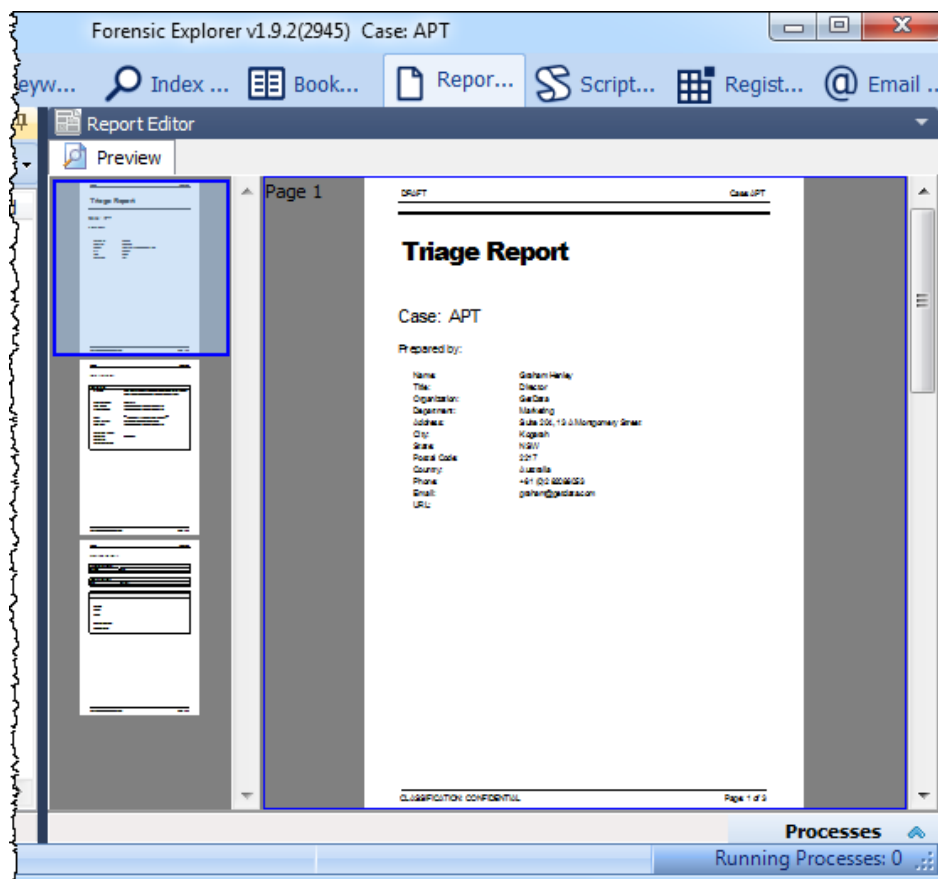
To preview the **entire report**:

- In the Report tree, click on the report name;

To preview a **group** or a **section**:

- In the Report tree, click on a group or a section.

Figure 163, Report Editor Preview



17.4.2 REPORT EDITOR - EDIT

The Report Editor Edit window gives access to edit an existing report, or to design a new report.

To **open** the report **Edit** window;

- In the Report tree, **double click** on a section;

- The **Edit** tab then appears in the Report Editor next to the Preview tab.

17.5 CREATING REPORTS

Whilst the Forensic Explorer Reports module can be effectively used to create one off reports on a case by case basis, the power of the module comes from the ability to design, use, and then re-use automated report templates in future cases.

As described in the sections above, Forensic Explorer reports are created from bookmarked items. A methodical approach to bookmark structure will ensure that report templates can be used again and again.

Forensic Explorer can report on a single bookmarked item and its attributes, or iterate through a list of bookmarked files and their attributes. The following exercises provide examples of how to design basic report templates.

17.5.1 REPORT EXERCISES

In order to work through the exercises below it is necessary to have a basic understanding of how to create a case, add evidence and bookmark files.

To prepare for the exercises:

STEP 1 – START A CASE AND BOOKMARK FILES

- a. In the evidence module, create a new case, adding a forensic image that contains JPG files.
- b. In the File System module, select a group of JPG files, right click and “Add Bookmark.
- c. In the Add Bookmark window, add the files to the Pictures bookmark folder.
- d. Switch to the Bookmarks module.
- e. Review the Pictures bookmark folder to ensure that it contains the bookmarked files.

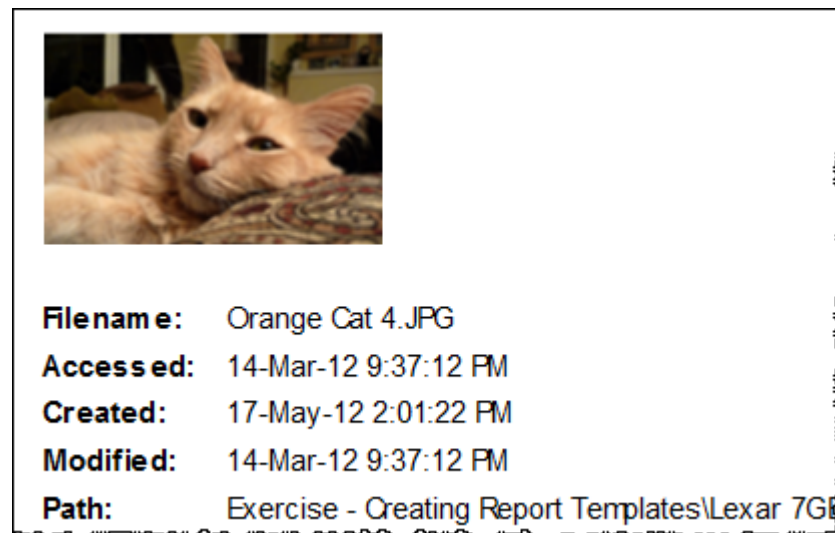
STEP 2 – CREATE A NEW BLANK REPORT

- a. Switch to the Reports module.
- b. In the Reports tree, select **New > Blank Report**. Exercise 1: Reporting on a single bookmarked item

EXERCISE 1: REPORT ON A SINGLE FILE**OBJECTIVE**

In this exercise create a report on a single file bookmarked in the **My Bookmarks\Pictures** folder. The example here is “Orange Cat 4.JPG”:

Figure 164, Reporting on a Single Bookmarked File (finished report output)

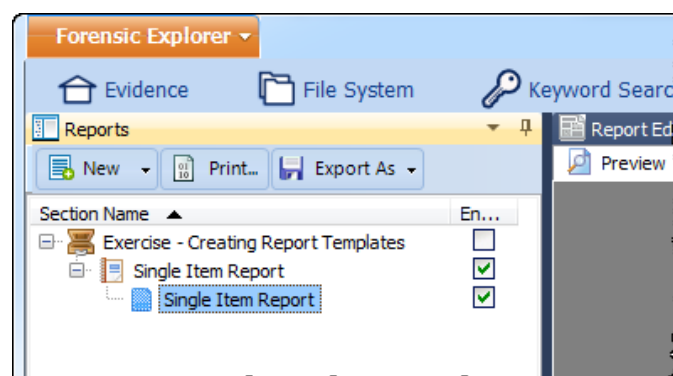
**STEP 1 & 2**

Follow STEPS 1 and 2 in 17.5.1 above to prepare a case with bookmarks.

STEP 3 – RENAME THE BLANK REPORT

- In the Reports module, click then hover over the report name to rename the section to “Single Item Report”.
- Repeat this step to rename the section. The Reports folder tree should now look like this:

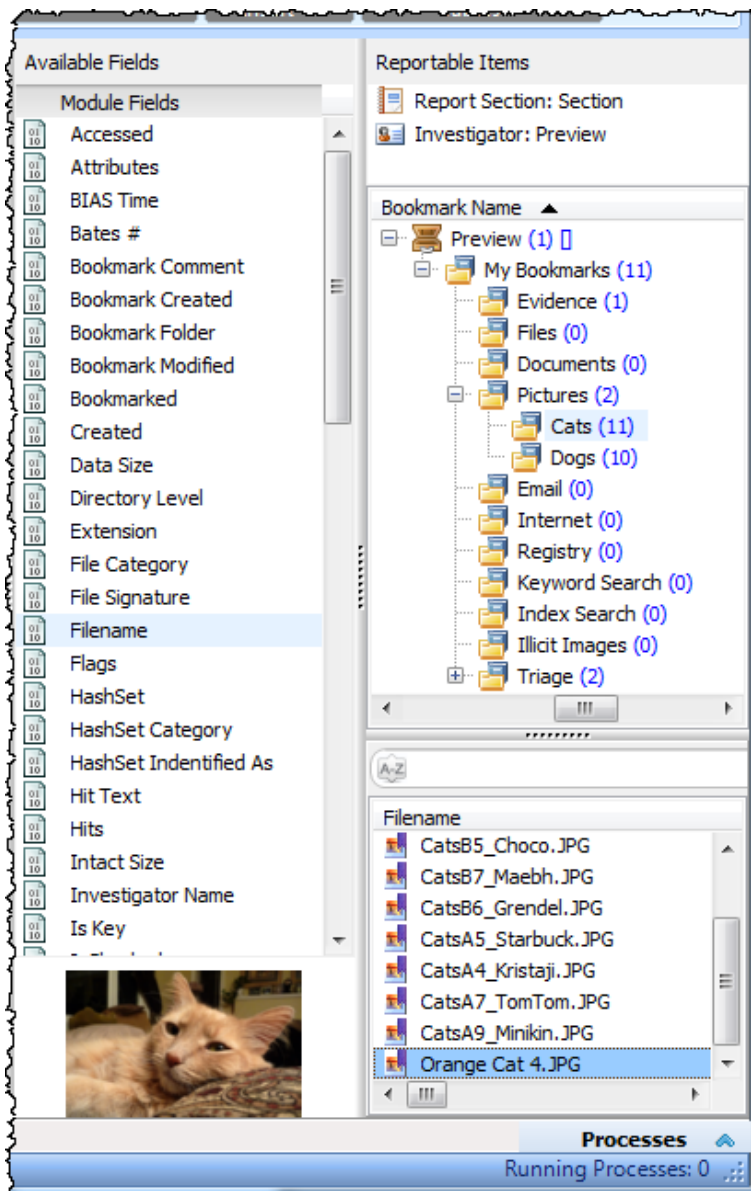
Figure 165, Rename the Report and Section



STEP 4 – EDIT THE REPORT

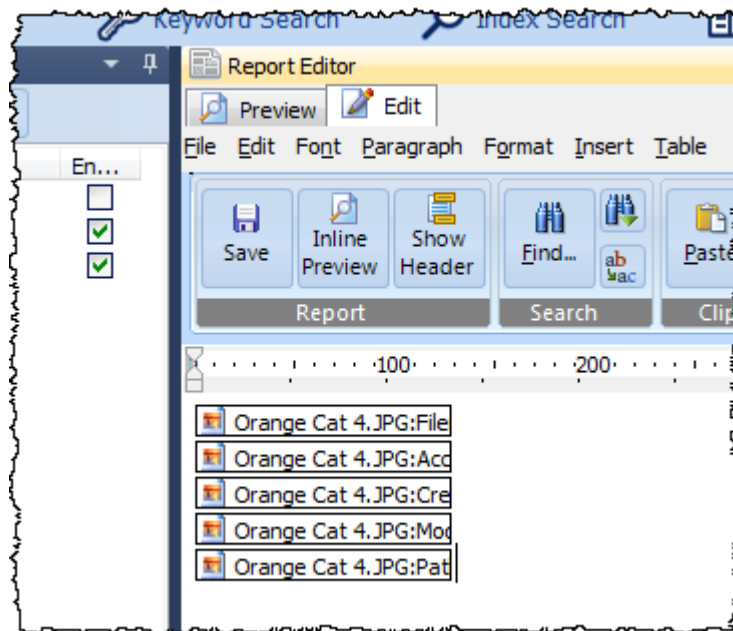
- c. Double click on the report section “Single Item Report” to open the report Editor Tab.
- d. In the **Reportable Items** column (shown in Figure 166 below), click on the folder containing the desired bookmark. Then located and click on the required file (in this example, Orange Cat4.JPG) in the “Filename” section.
- e. The fields available for the selected file are now shown in the “Available Fields” column to the left (as shown in Figure 166 below).

Figure 166, Selecting a Bookmarked File and its Fields



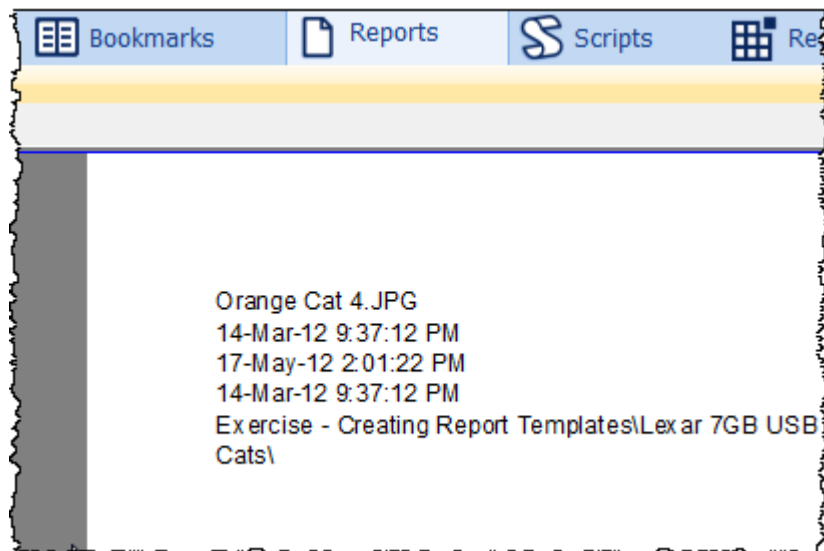
- f. Select the required fields with the mouse (use the CTRL key to select a group) and drag and drop the fields for the file onto the Report Editor window. In this example we are using the fields: Filename; Created; Modified; Accessed; and Path. Organize the fields into a vertical list, as shown in (shown in Figure 167 above) below:

Figure 167, Report Editor Showing Fields



- g. Switch to the Report Editor Preview tab to see the field names in the report.

Figure 168, Report Editor Showing Report



- h. To insert the picture, go back to the Editor window and click on the file name (Orange Cat 4.JPG) in the Reportable Items > Filename section shown in Figure 166 above. The selected picture will display at the bottom of the field list. Drag and drop the picture onto the report.

- i. Format the report as desired by inserting labels, font options etc. Layout can be achieved by using standard table with hidden borders. The formatted output is shown in Figure 164 above.

EXERCISE 2: LISTING BOOKMARKED FILES IN A TABLE

OBJECTIVE

The object of this exercise is to show the contents of a bookmark folder as a list in a table, as follows:

Figure 169, Exercise 1 - Objective

Filename	Created	Modified
CatsB7_Maebh.JPG	17-May-12 2:01:22 PM	14-Mar-12
CatsB6_Grendel.JPG	17-May-12 2:01:22 PM	14-Mar-12
CatsB5_Choco.JPG	17-May-12 2:01:22 PM	14-Mar-12
CatsB3_CharlieTuna.JPG	17-May-12 2:01:21 PM	14-Mar-12
CatsB1_Corduroy.JPG	17-May-12 2:01:21 PM	14-Mar-12
CatsA9_Minikin.JPG	17-May-12 2:01:21 PM	14-Mar-12
CatsA8_Gadget.JPG	17-May-12 2:01:21 PM	14-Mar-12
CatsA7_TomTom.JPG	17-May-12 2:01:21 PM	14-Mar-12
CatsA5_Starbuck.JPG	17-May-12 2:01:21 PM	14-Mar-12
CatsA4_Kristaji.JPG	17-May-12 2:01:21 PM	14-Mar-12
DogsA9_Kodie.JPG	17-May-12 2:01:23 PM	14-Mar-12
DogsA8_Jack-Jack.JPG	17-May-12 2:01:23 PM	14-Mar-12

STEP 1 & 2

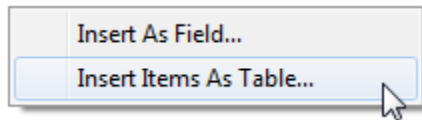
Follow STEPS 1 and 2 in 17.5.1 above to prepare a case with bookmarks.

STEP 3 – RENAME THE BLANK REPORT

- Click and hover on the report name to rename the section to “My Gallery Report - Pictures”.
- Repeat this step to rename the report section.

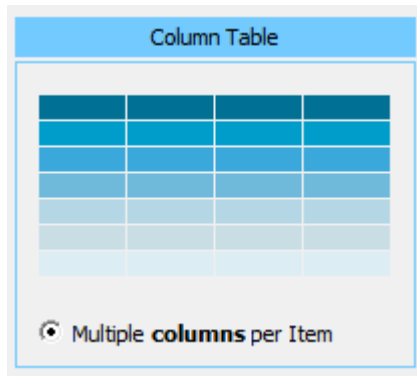
STEP 4 – EDIT THE REPORT

- Double click on the report section “My Gallery Report - Pictures” to open the Report editor.
- In the Bookmark Name column, select the “Pictures” bookmark folder and drag and drop it onto the blank page.
- Select to “Insert Item as Table” in order for the table to iterate through each bookmarked file:



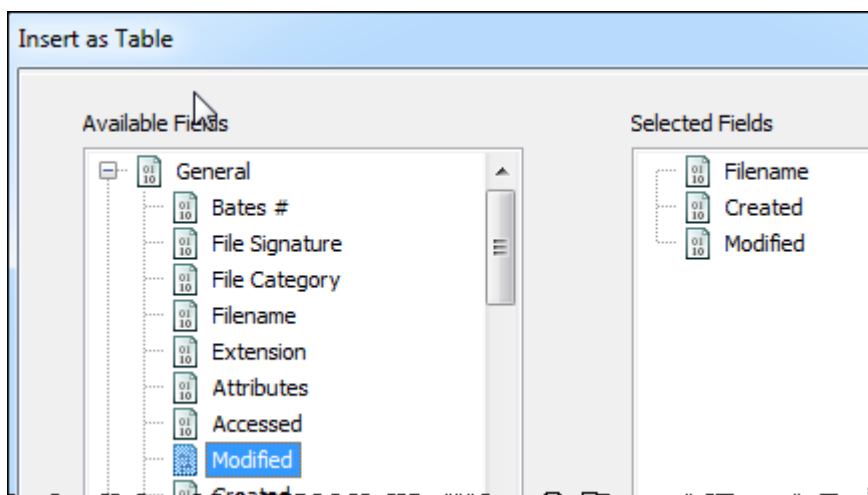
- d. Select the “Multiple columns per item” table which lists records vertically:

Figure 170, Selecting a List View Table Style



- e. Double click to select the fields for each column in the table:

Figure 171, Adding Fields to the Table



The table is now inserted into the Report Editor as follows:

Pictures		
Filename	Created	Modified
CatsB7_Maebh.JPG:Fi	CatsB7_Maebh.JPG:Cr	CatsB7_Maebh.JPG:M

- f. Switch to the Preview window to view the result. The table list should look like Figure 169 above.

EXERCISE 3: CREATING A GALLERY VIEW REPORT

OBJECTIVE

The objective of this exercise is to produce a gallery view of bookmarked items in the **My Bookmarks\Pictures** folder, as shown in Figure 172 below. The report will then be saved as a template for future use.

Figure 172, Creating a Gallery View Report (finished report shown)



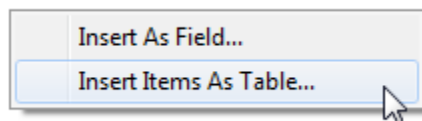
Follow **STEPS 1 and 2** in 17.5.1 above to prepare a case with bookmarks.

STEP 3 – RENAME THE BLANK REPORT

- c. Click and hover on the report name to rename the section to “My Gallery Report - Pictures”.
- d. Repeat this step to rename the report section.

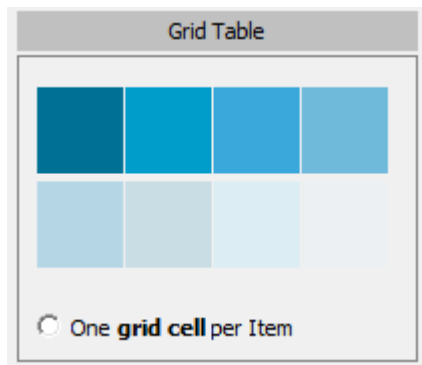
STEP 4 – EDIT THE REPORT

- g. Double click on the report section “My Gallery Report - Pictures” to open the Report editor.
- h. In the Bookmark Name column, select the “Pictures” bookmark folder and drag and drop it onto the blank page.
- i. Select to “Insert Item as Table” in order for the table to iterate through each bookmarked file:



- j. In the table selection window, use the “Grid Table” to that files in the bookmark folder (i.e. pictures) are entered horizontally across the screen in the gallery view format:

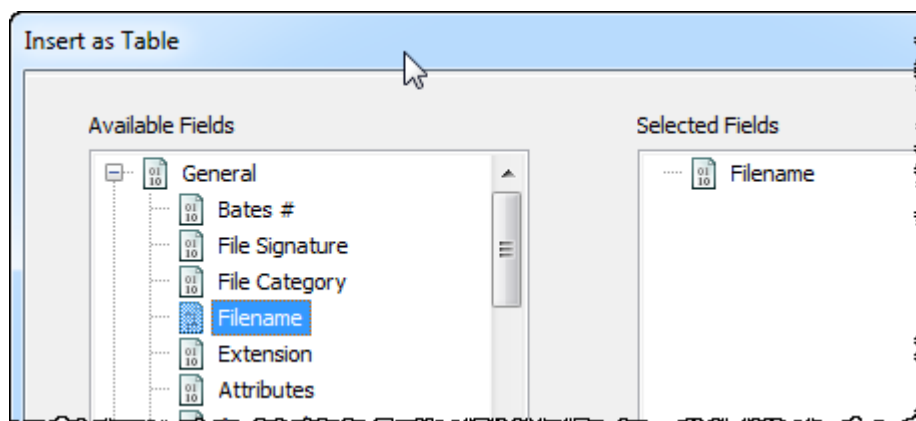
Figure 173, Selecting a Gallery View Table Style



(The direction of the repeating records is indicated by the color shading).

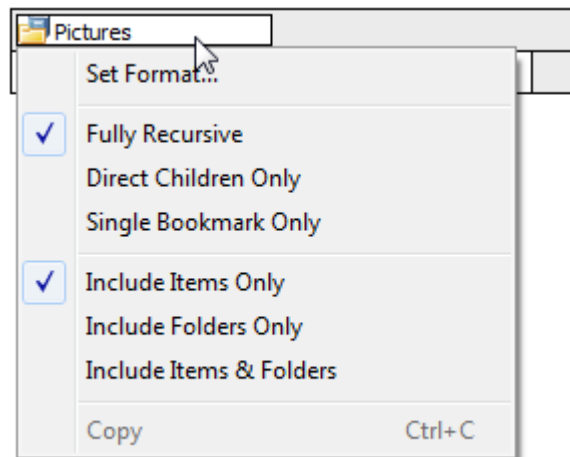
- k. Double click to select the **Filename** field to add to the report:

Figure 174, Select table fields



Click OK to proceed and the table will be inserted into the report.

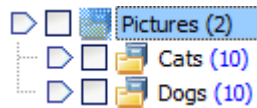
- l. Right click on the pictures folder to confirm the levels on which the table will operate. Fully Recursive and Include Items Only will operate on all files in all subfolders:



- m. Click on the **Preview** tab of the Report editor to preview the report. The Filename will be repeated in the table across the page, as shown below:
- n. In the Reportable Items > Filename window, select a file and drag and drop it into the first cell of the table. Select to insert field as Graphic. The picture will now display in the first cell of the table. Use the formatting tools (alignment, font etc.) to adjust as necessary. Add a title if required.

17.5.2 NESTED TABLES

More complex reports where records are group by folders require nested tables. For example, to group the following bookmark structure by first level folders (Cats and Dogs):



a nested table is required. Figure 175 below describes the layout:

Figure 175, Layout of a Nested Table

PICTURES (Root Folder)

CATS (Group by bookmark folder 1 at level 1)

File Name	Created Date
CAT1.JPG (Folder 1, Record 1)	Created Date
CAT2.JPG (Folder 1, Record 2)	Created Date
CAT3.JPG (Folder 1, Record 3)	Created Date

DOGS (Group by bookmark folder 2 at level 1)

File Name	Created Date
DOG1.JPG (Folder 2, Record 1)	Created Date
DOG2.JPG (Folder 2, Record 1)	Created Date
DOG3.JPG (Folder 2, Record 1)	Created Date

Chapter 18 – Scripts Module

In This Chapter

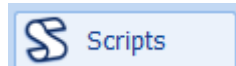
CHAPTER 18 - SCRIPTS MODULE

18.1	Scripts Module.....	216
18.1.1	Scripts Window.....	217
18.1.2	Script Editor window	220
18.1.3	Messages Window (Console)	221
18.2	Managing scripts in the scripts window	222
18.3	Introduction to Scripting	223
18.3.1	Programming Comments.....	223
18.3.2	Reserved Words	223
18.3.3	Uses (libraries).....	224
18.3.4	Const.....	224
18.3.5	Var	225
18.3.6	Procedures and Functions	225
18.3.7	Begin and End.....	225
18.3.8	Errors	226

18.1 SCRIPTS MODULE

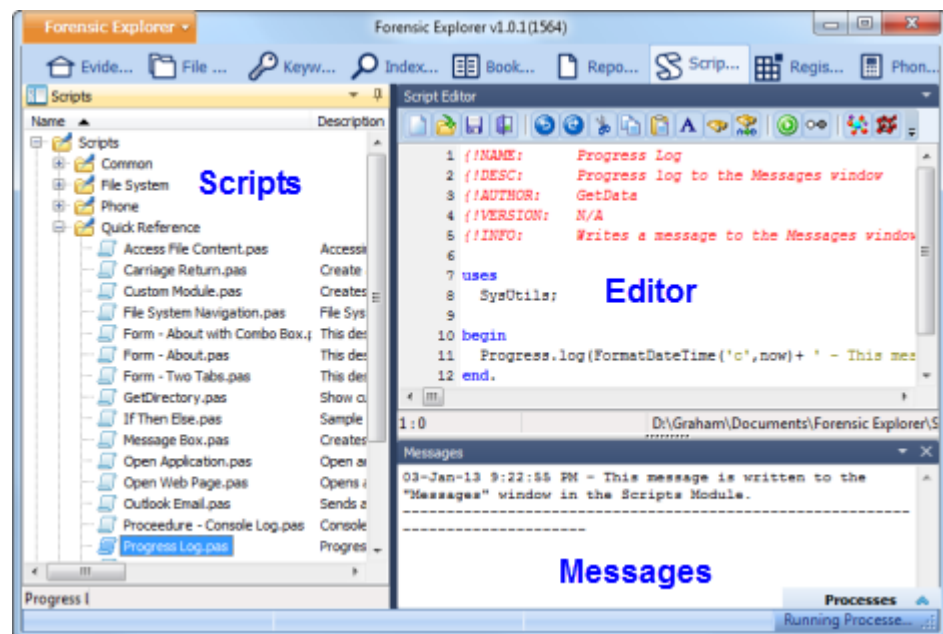
Forensic Explorer utilizes Pascal as its scripting language. Scripts are written and run in the scripts module, or launched in other modules via toolbar buttons or by other scripts. The Scripts module is accessed via the scripts tab:

Figure 176, Scripts module tab



The scripts module is arranged into three windows: **Scripts**; **Script Editor**; and **Messages**, as shown in Figure 177 below:

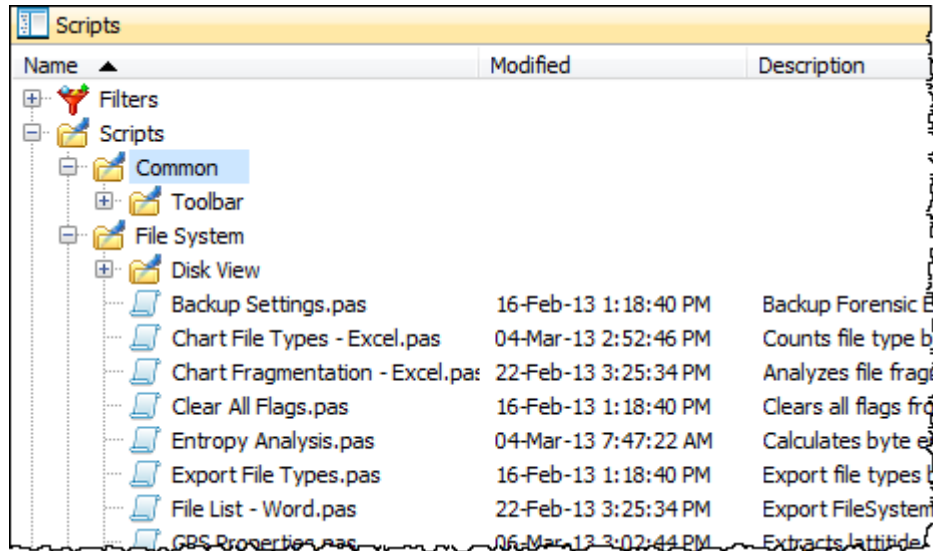
Figure 177, Scripts module



18.1.1 SCRIPTS WINDOW

The script window lists available .pas (Pascal) scripts and their attributes.

Figure 178, Scripts Windows showing .pas file attributes



Script Attributes

The Scripts window lists the attributes of each script:

Name: The script name is auto-generated from the “script.pas” file name.

Description and Author: These attributes are auto-generated from the comments at the start of the script.

Modified and Created: Script dates are auto-generated from the Windows date and time stamps of the .pas file.

Hash (SHA256): A SHA256 hash is calculated for each script. The hash is updated each time the Scripts window is refreshed. To manually refresh the Scripts window, **right click** in the Scripts window and select **Refresh** option from the drop down menu.

The purpose of the SHA256 has is so that the investigator can validate the authenticity of a GetData script, or a script from a trusted third party. GetData script hashes are published at <http://www.forensicexplorer.com/scripts.php>. If an installed script differs from the hash published on the web page it means that the content of the script has changed.

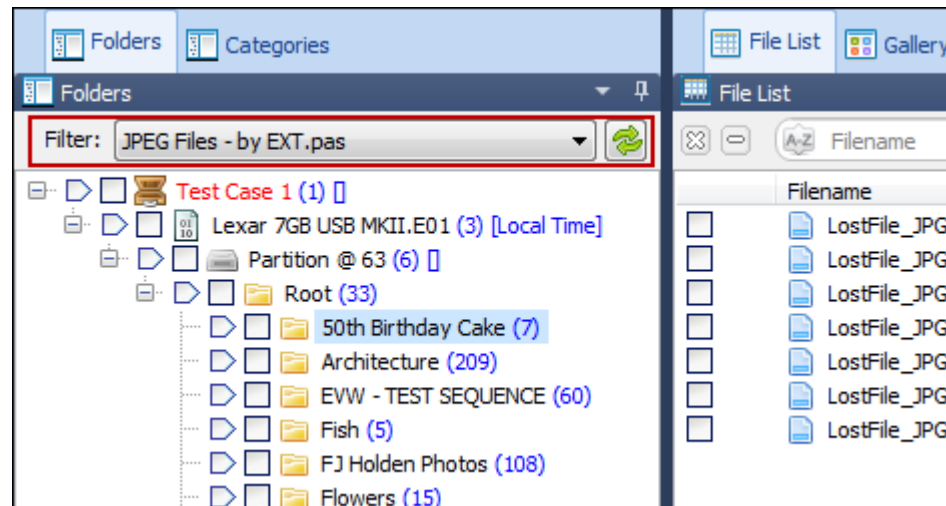
Forensic Explorer is installed with a number of default scripts in the **\Users\[user folder]\Documents\Forensic Explorer** path. Scripts are separated into folders, depending on their function. These include Filters, Scripts and Startup, as described below.

The scripts window is where scripts are **create, copied, renamed** and **deleted**.

FILTERS

Filters are scripts which perform the specific task of filtering displayed results to show only files specified in the filter criteria. The filter scripts are listed in the drop down bar of a Folders view, as shown in Figure 179 below for the File System module (filters can be applied in Folders view of other modules, including Email and Registry):

Figure 179, Tree view filter (File System Folders view)



The **JPEG Files by EXT.pas** filter is shown below. A result of “1” is used to display content. A result of “-1” is used to hide content:

```
begin
  filename := uppercase(anEntry.Entrypname);
  fileext := extractfileext(filename); // tests for specific extension
  if (fileext = '.JPG') then
    Result := 1; // 1 = display, -1 = hide
  end;
```

The filter can easily be modified to add additional file types.

SCRIPTS

Default scripts are separated into subfolders depending the module in which they are used or their function.

SCRIPTS\COMMON\

The **Scripts\Common** folder is used to hold scripts that are frequently called by other scripts.

The **Scripts\Common\Toolbar** folder contains the scripts used to manage the default toolbar button navigation system provided with Forensic Explorer:

- The default **Startup.pas** file (described above) initiates the creation of toolbars and buttons by calling scripts in the Common\Toolbar\ folder;
- Toolbar buttons are then managed by the Scripts\Common\Toolbar Manager.pas.

SCRIPTS\FILE SYSTEM\

The **Scripts\File System** folder contains default scripts which used in the File System module. This includes Hashing, Exporting and Skin Tone Analysis.

Sub-folders include:

Scripts\File System\Disk view

The “..\FileSystem\Disk View\” sub-folder contains scripts used to change block color in the Disk View window of the File System module. Colours are assigned using the color reference chart:

http://en.wikipedia.org/wiki/Web_colors

SCRIPTS\REGISTRY\

The **Scripts\Registry** folder contains default scripts used to extract information from registry keys. The processing script is “Registry Key Processor.pas”.

SCRIPTS\SCRIPTS\

Scripts\Scripts contains default scripts used in the Scripts module.

STARTUP

The Startup folder contains the script **startup.pas** (..\User Profile\Documents\Forensic Explorer\Startup\startup.pas”).

The purpose of **startup.pas** script is to automatically run when Forensic Explorer is launched and configure the interface. It can be individually configured by the investigator. For more information, see 18.4 below.

18.1.2 SCRIPT EDITOR WINDOW

A .pas file selected in the Script window will display its content in the Script Editor. A script can be opened directly from the editor, or a new script created in the editor. The functions of the editor are primarily controlled by the toolbar at the top of the Script Editor window. The button functions are as follows:



Save an existing script (a script is also saved when it is run). This button is only active when a script has been modified but not saved.



Undo last.



Redo last.



Cut text.



Copy text.



Paste from clipboard.



Change font.



Search for text.



Replace text.



(Save and) Run script as a single thread.



Run a threaded script.



Break point a script.



Compile current script.



Cancel the execution of the script.

Parameters:

Enter script parameters, e.g. "Parameter One" "Two" "Three" "Four"

18.1.3 MESSAGES WINDOW (CONSOLE)

The Messages window (also referred to as the “**console**”), is used to display compiler error messages or script output.

A console message is written with the “`Process.log(“Text”)`” command. In the default scripts provided with Forensic Explorer the log output is often formatted with a “procedure” (see below) to include a data and time reference using a using the command “`ConsoleLog(“Text”)`”. See Appendix 7 - Sample Script, for an example.

If a script is run in the Scripts module, the output will appear in the Messages window. However, if a script is executed in another module (run from a toolbar button or a link) the output is written to the log file for that module. Access the log for a module via the “Processes” log (see 7.4 - Task Processes List, for more information).

18.2 MANAGING SCRIPTS IN THE SCRIPTS WINDOW

To **open** a script;

Double click on the **script name** in the **Scripts window**. This will display the script in its own tab in the **Script Editor** window.

To **create** a script;

1. **Right Click** in the **Scripts window** and select **File > New Script**.
2. Enter the name of the new script in the popup New Script window.
3. The script will then appear in alphabetical order in the Scripts window. Double click to display the content of the new script in a tab in the Script Editor.

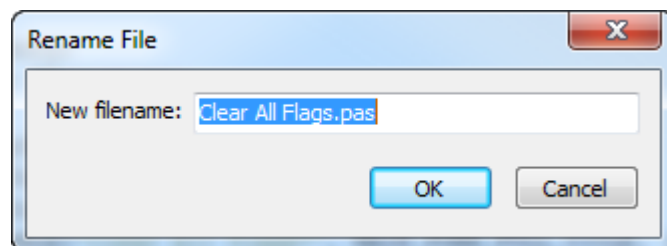
To **copy** a script;

1. Right click on the script in the Scripts window;
2. Select **File > Copy** from the drop down menu.

The highlighted script will be copied. A new script of the same name will appear in the Scripts window with the added file name text “_0001.pas”. Then use the re-name function to rename this file.

To **rename** a script;

1. Highlight the script in the Scripts window;
2. Right click and select **File > Rename** from the drop down menu. Edit the file name in the Rename File window:



Note: If the renamed file does not appear, **right click in the Scripts window** and use the **Refresh** option to refresh the display. If the renamed file still does not appear, check to see that it has been renamed with the .pas extension.

To **delete** a script;

1. Highlight the script in the Scripts window;
2. Right click and select **File > Delete** from the drop down menu.

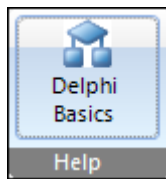
A confirmation window will appear to confirm that the delete is required.

18.3 INTRODUCTION TO SCRIPTING

This section is an introduction to Forensic Explorer scripting only. More technical scripting documentation is available at <http://www.forensicexplorer.com>.

Forensic Explorer is installed with “**Delphi Basics**”© reference documentation. It is installed in the path: “C:\Program Files\GetData\Forensic Explorer v1\Delphi Basics\” and accessible by the “Delphi Basics” help button in the Script module toolbar (shown below):

Figure 180, Scripts Module toolbar, Delphi Basics scripting documentation



The Delphi language is a set of object-oriented extensions to standard Pascal and has become the most popular commercial Pascal implementation (see http://en.wikipedia.org/wiki/Comparison_of_Pascal_and_Delphi for more information). **Delphi Basics**© is provided as a reference guide only. Not all commands/features in the documentation are available in Forensic Explorer. Delphi Basics© is licensed for use from <http://www.delphibasics.co.uk/> and may only be used with Forensic Explorer.

A typical Forensic Explorer script contains the elements described in the paragraphs below.

18.3.1 PROGRAMMING COMMENTS

It is good programming practice to include comments within a script. Comments help anyone reading the script understand the authors intention. Comments are shown in the Script Editor window in red. To insert a comment:

- `//` The forward slash marks are used for a single line comment
- `{` The right and left brackets are used for a comment that can be written over multiple lines `}`

18.3.2 RESERVED WORDS

A Forensic Explorer script starts with the word '**Program**' (although it is not explicitly required) and ends with '**End.**' (A period after an “End” identifies the end of the program). These are examples of “**Reserved Words**”, set aside for special use and which cannot be used for any other purpose. Reserved words are shown in blue in the Script Editor window. Following is a list of reserved words in Forensic Explorer:

and array begin case const

div	do	downto	else	end
file	for	function	goto	if
in	label	mod	nil	not
of	or	packed	procedure	program
record	repeat	set	then	to
type	until	var	while	With
uses				

18.3.3 USES (LIBRARIES)

‘Uses’ enables a script to call on a library of additional code. For example, the “GUI” library in the example above enables the scripter to use “MessageBox”, which constructs a displayed window without the need to write extensive code. Forensic Explorer has the following code libraries:

- ByteStream
- Classes
- Common
- DataEntry
- DataStorage
- DataStreams
- Graphics
- GUI
- Math
- MetaData
- RawRegistry
- System
- SysUtils

Further information about user libraries is provided at <http://www.forensicexplorer.com/scripts.php>

18.3.4 CONST

A constant declares a value that cannot be changed during script execution. It is often used so that the constant can be easily edited (outside of program execution) and thus updated at multiple reference points in the script. An example is provided in Appendix 7 - Sample Script, where “starting age” is declared as a constant and referenced multiple times.

18.3.5 VAR

The variable block starts after the "**var**" reserved word and continues until the next reserved word is reached. A variable stores a value that can be changed during the execution of a script. Each variable must be a unique, non-reserved name, followed by a declaration of its type, for example:

- Integer = a whole number, positive or negative;
- Real = a decimal number (e.g. 12.987)
- Boolean = true / false
- String = Character

Once a variable is declared, it can be assigned a value in the script ":", for example, X := 27;

18.3.6 PROCEDURES AND FUNCTIONS

A procedure is a set of instructions to be executed, with no return value. A function is a procedure with a return value.

A commonly used procedure, "ConsoleLog", is used in Appendix 7 - Sample Script. The procedure formats the Progress.log command (writing a message to the messages window) to include the date and time:

Figure 181, Procedure "ConsoleLog"

```
procedure ConsoleLog(AString: string);  
begin  
  Progress.Log([' + DateTimeToStr(now) + ' ] : ' + AString);  
end;
```

The procedure is called with the line:

```
ConsoleLog ('Here is the message');
```

And the resulting output is:

```
[17-Jan-13 1:47:22 PM] : Here is the message
```

18.3.7 BEGIN AND END

The main part of the script appears between the two reserved words, "begin", marking the start of the code, and "end." (with a period) marking the end.

A script is broken down into a series of commands. A general rule is that a command must end with a **semi-colon**. If a command extends over several lines, for example an

“If Then Else” statement, generally the semi colon won’t appear until the end of the entire statement.

18.3.8 ERRORS

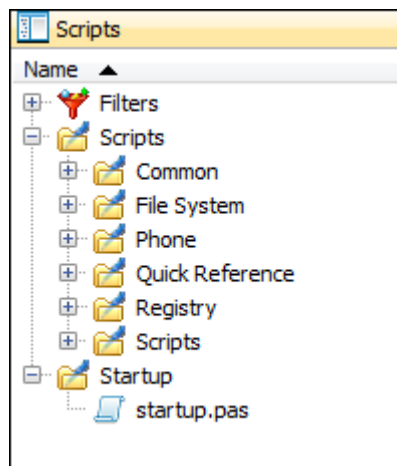
Errors in a script are reported in the Messages (console) window. Usually the message will provide the line number of the code where the error appears. Double click on the line number to go directly to the problem line.

18.4 STARTUP.PAS

The startup.pas script, “...\\[User Profile]\\Documents\\Forensic Explorer\\Startup\\startup.pas” runs when Forensic Explorer is launched.

To **view** the **startup.pas** script;

1. Go to the Scripts module;
2. At the bottom of the Scripts window (top left hand window) click on the "Startup" folder to show "startup.pas";



3. Double click on "startup.pas" to open and display its content in the Script Editor (right hand window).

Startup.pas can be used to:

- Manage displayed modules (turn modules on/off at startup using the 'Startup Modules.pas' script;
- Startup with custom modules (see "Phone Module");
- Add button groups and buttons to module toolbars.

These features in the startup.pas file can be activated by removing the **// slash marks are used to comment out the code**.

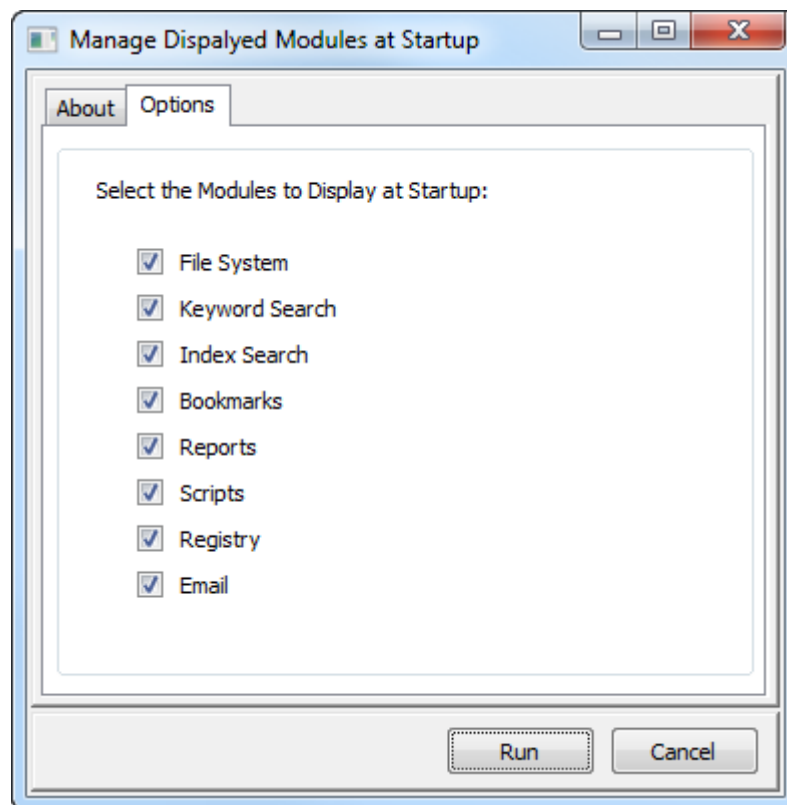
18.4.1 MANAGE DIPLAYED MODULES

In certain situations a computer forensics investigator may choose not to start Forensic Explorer with all modules visible. For example, when a case is to be reviewed by a third party, the forensic investigator may choose only to display relevant modules, such as Keyword Search and Bookmarks.

There are two methods to manage startup modules provided in the default startup.pas script:

1. The first method is to use startup.pas to run another script, "Scripts/Common/Startup Modules.pas". This script launches a form during startup that enables the user to select the modules to be displayed;

Figure 182, Startup Modules.pas



2. The second method is to hard code the modules to be hidden into the startup.pas script. Example code to hide the Registry Module is shown below:

```
tempModule := ModuleManager.ModuleByName('Registry');  
if assigned(tempmodule) then  
tempModule.WillShow(false);
```

Note: If the Scripts module is hidden with this technique it will be necessary to edit the script using Windows Notepad (or other such program in order to re-enable the Scripts module).

18.4.2 CUSTOM MODULE - PHONE MODULE

See Chapter 19.

18.4.3 CUSTOMIZING TOOLBARS

The contents of the toolbar is your own space. You can customize it as you see fit.

Startup.pas

The toolbar buttons are created on startup by the "startup.pas" script. If startup.pas is blank, there will be no toolbars at all.

It is possible to add buttons by placing code directly into startup.pas. However, in order to keep startup.pas uncluttered, it is used to create toolbars by calling other scripts. If you look at startup.pas you will see the use of the "RunScript" command in lines like:

```
RunScript(gScriptsDir+'Common\Toolbar\Button Group - Hex.pas','File System',false);
```

The "RunScript" command has 3 parameters:

1. The path of the script that you wish to run (in this example, the script to run is ; gScriptsDir+'Common\Toolbar\Button Group - Hex.pas');
2. The module where you want the script to be run (in this example it is the "File System" module);
3. Whether or not you want logging (in this example, logging is false).

Button Group – Hex.pas

Now let's take a look at the "Button Group – Hex.pas" script. In the scripts module, navigate to the "Scripts\Common\Toolbar" folder and double click on "Button Group – Hex.pas" to open it in the Script Editor. Once you have it open in the editor, you will see the following 4 lines midway through the script:

```
ToolBar := Module.AddToolBar('Hex'); // Creates the button group and puts the  
name of the button group at the bottom
```

```
ToolBar.AddButton('Hex v6', 'C:\Program Files\BreakPoint Software\Hex  
Workshop v6\HWork32.exe', "", -1, 64, 64, BTNS_SHOWCAPTION); //adds and  
names the button
```


```
ToolBar.AddButton('UltraEdit', 'C:\Program Files\IDM Computer  
Solutions\UltraEdit\Uedit32.exe', "", -1, 64, 64, BTNS_SHOWCAPTION); //adds  
and names the button
```

```
ToolBar.AddButton('UltraEdit', 'C:\Program Files (x86)\IDM Computer  
Solutions\UltraEdit\Uedit32.exe', "", -1, 64, 64, BTNS_SHOWCAPTION); //adds  
and names the button
```

You can see that the first line creates the button group, and the next three lines point to different types of HEX editors that may be installed on your system. Remember that if the file does not exist, the code will be ignored and the button not added (Note that because we run this as a default menu button we need to include two options for 'Ultra Edit' to cover both the 32 and 64 bit version installation path).

To add a link to your own program, make a copy of one of these lines and then edit it. Change the name of the button, put and put in the correct path on your machine. Once you have edited the script, press the save button in the Scrip Editor window to save you changes.

Running Your Script

A script is run in single thread mode by pressing the green play button , or in multi thread mode by pressing the green fast forward button in in the Script Editor toolbar.

However, running a button group script here is not going to work, because it needs to know the parameter for the module where you want the button to appear (remember this information is passed to the script at startup by the line in startup.pas).

You could close and restart Forensic Explorer to show the button. Or, in order to test the script, we can do this in the scripts module by using the "Parameter" box in the toolbar.

Parameters:

If you type in "File System" (use the quotes when a space is located in the module name) in the parameters box and then run the script, the button will appear in the File System module. If you type in Scripts, the button will appear in the Scripts module. If there is an error in the script the messages will be displayed in the messages window at the bottom of the Scripts module.

If you want to remove a button group without restarting, run the "Toolbar - Delete Button Group Form.pas" in the Quick Reference folder.

You can then of course start experimenting. You can create your own script in "Scripts\Toolbar\My Custom Button Group.pas", fill it with your own buttons, and call it using the startup.pas script so it is there each time you start the program. If you are feeling brave, you can edit the Toolbar Manager.pas so that you can open and close it on the fly.

Chapter 19 – Custom Modules

In This Chapter

CHAPTER 19 – CUSTOM MODULES

19.1	About Custom Modules.....	232
19.2	Browser History Module.....	232
19.3	Phone Module	232
19.3.1	iPhone.....	232
19.3.2	Nokia PM	233

19.1 ABOUT CUSTOM MODULES

The flexibility of Forensic Explorer means that a custom module can be created and populated with data entirely from scripts.

19.2 BROWSER HISTORY MODULE

The **Browser History module** is a custom module created from script. Browser History scripts are located in the **Scripts module** at the path:

Scripts\Internet\Browser History\.

Browser history scripts include:

- **Module - Browser History Create.pas** that creates the module;
- Individual scripts, such as **History - Process Chrome.pas**, that extract browser history from relevant files and populate the module with data.

A number of browser store data in an SQLite database format. For example the Chrome browser stores history data in the SQLite **history** file. This data is extracted and populated into module using an SQL statement.

19.3 PHONE MODULE

The **Phone module** is a custom module created from script. The Phone module is created by the script:

Scripts\Phone\Phone Moudle Create.pas

19.3.1 IPHONE

The scripts folder: *Scripts\Phone\iPhone* contains scripts specific to the extraction of data from iPhone devices and iTunes backups.

IPhones commonly store data in one of the following formats:

- As standard media files, e.g. JPG, PNG
- Plist;
- XML;
- SQLite.

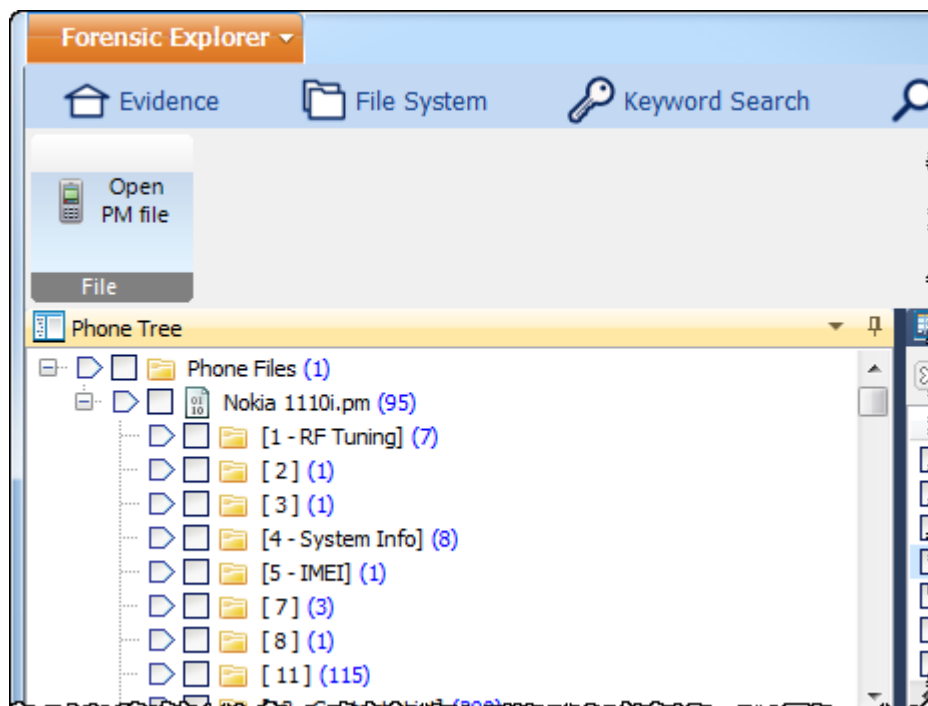
Each script is designed to extract the intended data and populate the Phone module. There are however a great many files within an iPhone that may be relevant to and investigation. If the required script does not existing by default, the following scripts can be used as templates for the different types of extraction:

- **SQLite: iPhone – Facebook.pas** - This script extracts Facebook data from the SQLite file fbsyncstore.db.
- **Images: iPhone - Images.pas** - This script adds iPhone graphics files (e.g. JPG, PNG) from the File System to the Phone module.
- **Plist: iPhone – Wifi Networks.pas** - This script adds a list of Wi-Fi networks and SSID information to the Phone module.
- **XML: - iPhone – iTunes Info.pas** - This script collects iphone user information and adds it to the Phone module.

19.3.2 NOKIA PM

The “..\Scripts\Phone\Phone PM.pas” script opens, reads, and adds a selected Nokia PM phone image file to the module. It then parses the files to extract information from the image, as shown in Figure 183 below:

Figure 183, Custom Phone module - parsing a Nokia PM file



Chapter 20 – Date and Time

In This Chapter

CHAPTER 20 - DATE AND TIME

20.1	Date and time in computer forensics	236
20.2	FAT, HFS, CDFS file system date and time	236
20.3	NTFS, HFS+ file system date and time	236
20.4	Date and time information in the Windows registry	236
20.4.1	Manually examine registry for time zone information.....	237
20.4.2	Extract time zone information using a script.....	239
20.5	Daylight saving time (DST)	240
20.6	Adjusting Date in Forensic Explorer	241
20.6.1	Adjusting the date and time when adding evidence	241
20.6.2	Adjusting evidence date and time during a case	242
20.6.3	Synchronizing time zones	243

20.1 DATE AND TIME IN COMPUTER FORENSICS

Timestamps are often important in a computer forensics examination. The investigator should have a clear understanding of the subject before making critical conclusions.

When date and time is in issue, the following verified information should be at hand:

- The time zone where the computer or device was operating when it was acquired;
- The time of the computer BIOS clock compared with a verified time source (e.g. a recorded time service) for that location.

It is the file system in use which determines whether Modified, Accessed and Created (MAC) times are stored in local time or Coordinated Universal Time (UTC). Appendix 4 - Summary of Date and Time, is a summary table of file system date and time, including the location of the source data interpreted by Forensic Explorer.

Date and time attributes of individual files can be examined using the Filesystem Record view of the File System module (see 8.10 - Filesystem Record view, for more information).

20.2 FAT, HFS, CDFS FILE SYSTEM DATE AND TIME

FAT, HFS and CDFS store local date and time as per on the BIOS clock. There is no time zone adjustment. For example:

- A file stored at 11am is stored in the file system as 11am.

When Forensic Explorer opens this file, the default file time will display as 11am.

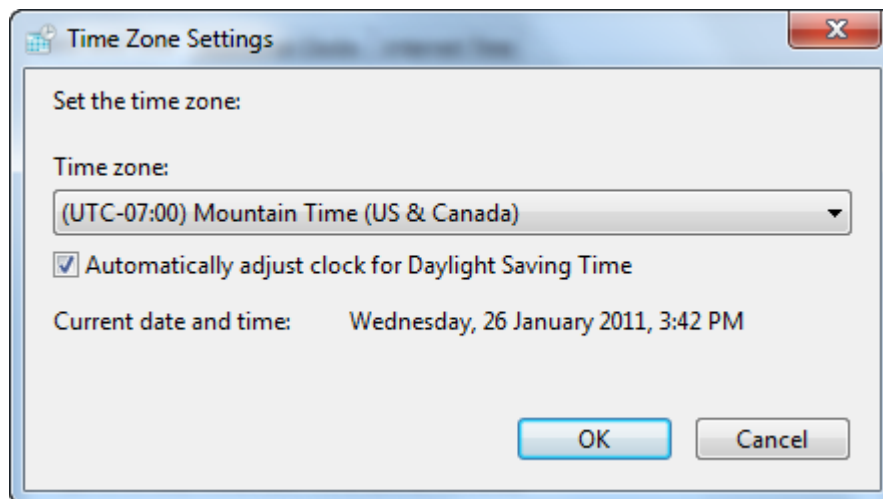
20.3 NTFS, HFS+ FILE SYSTEM DATE AND TIME

NTFS and HFS+ file systems store date and time in Coordinated Universal Time (UTC), which in practical terms, when fractions of a second are not important, can be considered equivalent to Greenwich Mean Time (GMT). In order to display date and time information in a format relevant to the end users location, the UTC time is translated into local time using the computers time zone setting.

20.4 DATE AND TIME INFORMATION IN THE WINDOWS REGISTRY

Windows time zone settings are held in the Windows registry. They are set during install and can be modified at any time via the Time Zone Setting options of the control panel (shown below):

Figure 184, Windows 7 time zone settings



As the time zone may be incorrectly configured or deliberately altered, it is necessary for the investigator to determine these settings so that the correct time zone offset for the case can be made.

20.4.1 MANUALLY EXAMINE REGISTRY FOR TIME ZONE INFORMATION

Registry files are located in the following path:

- Windows NT/2000: **C:\Winnt\System32\config**
- Windows XP/Vista and 7: **C:\Windows\System32\config**

This path contains the five hive files:

- **SAM** (Security Accounts Manager);
- **SECURITY** (Security information);
- **SOFTWARE** (Software information);
- **SYSTEM** (Hardware information); and,
- **DEFAULT** (Default user settings).

(Note that each file has a corresponding repair file in case of corruption. Be sure to examine the active registry files.)

To examine a registry file in Forensic Explorer the file must be first added to the Registry module.

To add a **stand-alone registry file**:

1. In the **Evidence module**, commence a **case** or a **preview**;

2. Click on the **Add File** button and select the file. Forensic Explorer identifies a registry file by its file signature. The **Evidence Options** window displays with the option to add the hive to the Registry module. Click **OK** to proceed.

To add a **registry file** from **within an existing case or preview**;

1. Locate the registry file in the file list view of the **File System module**;
2. Right-click on the registry file and select the **Send to Module > Registry** option from the drop down menu.

REGISTRY - CURRENT CONTROL SET

In order to locate relevant date and time information in the registry it is first necessary to determine the “current control set”. This identifies the last system configuration booted by the computer.

CurrentControlSet is identified using registry file:

- Registry file: **C:\Windows\System32\config\SYSTEM**

And registry key:

- **\Select\Current**

The key **Current** is a pointer to the current control set. A Dword hex value of “01 00 00 00” identifies the current control set to be:

- **\ControlSet001**

(Note: A typical Windows installation contains at least two control sets.)

REGISTRY - TIME ZONE INFORMATION

Once the current control set is identified, Time Zone information can then be identified in the **SYSTEM registry file** under key:

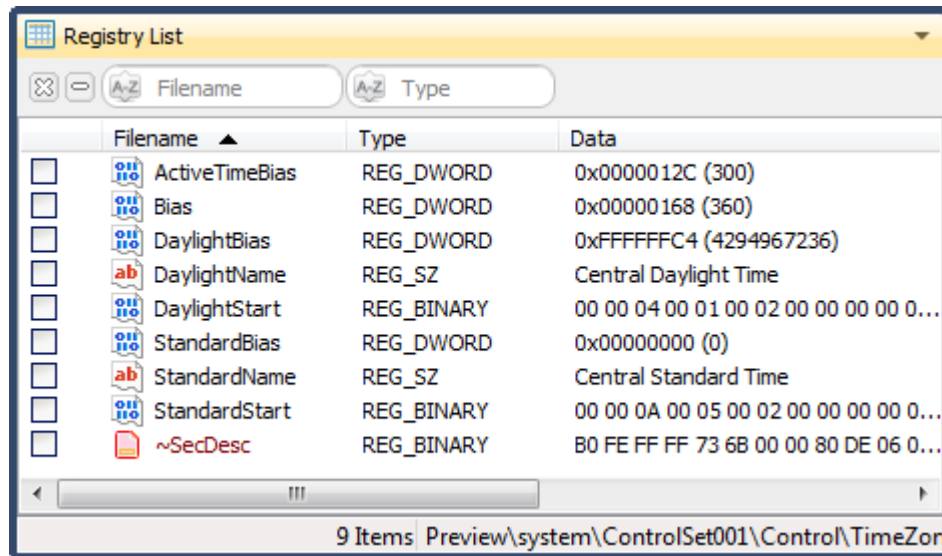
- **\CurrentControlSet\Control\TimeZoneInformation**

As shown in the Forensic Explorer Registry module in Figure 185 below:

Figure 185, Windows registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Image file: NIST Hacking Case (14)



The information in the registry includes:

- ActiveTimeBias:** The number of minutes offset from UTC for the current system time.
- Bias:** The number of minutes offset from UTC for the current time zone setting.
- DaylightBias:** The number of minutes offset from UTC for the current time zone when daylight saving is in effect.
- DaylightName:** The name of the time zone (daylight saving);
- DaylightStart:** The date and time daylight saving starts;
- StandardBias:** The number of minutes offset from GMT when standard time is in effect.
- StandardName:** The name of the time zone (standard time);
- StandardStart:** The date and time when Standard time starts.

20.4.2 EXTRACT TIME ZONE INFORMATION USING A SCRIPT

Registry information, including Windows date and time settings, is also available in Forensic Explorer by running the **Registry Analyzer** script. This script is provided with a default install of Forensic Explorer in the folder:

\User\My Documents\Forensic Explorer\ Scripts\Registry\Registry Analyzer.pas

The Registry Analyzer script can be run directly from the Scripts module, or using the toolbar shortcut **Quick Scripts > Registry Analyzer** located in the File System module.

The Registry Analyzer script decodes the registry keys and provides output in the following format:

Figure 186, NIST Hacking Case (14) Registry Analyzer script output

```
\ControlSet001\Control\TimeZoneInformation\ActiveTimeBias = 300
\ControlSet001\Control\TimeZoneInformation\Bias = 360
\ControlSet001\Control\TimeZoneInformation\DaylightBias = -60
\ControlSet001\Control\TimeZoneInformation\DaylightName = Central Daylight Time
\ControlSet001\Control\TimeZoneInformation\StandardBias = 0
\ControlSet001\Control\TimeZoneInformation\StandardName = Central Standard Time
```

20.5 DAYLIGHT SAVING TIME (DST)

Daylight saving time (DST), involves the advancing of clocks (usually by 1 hour) to add more daylight in the evenings at the expense of less daylight in the mornings. Depending on where you are in the world, it can be implemented on a country, region or state by state basis. Generally DST is a practice that is undertaken in summer months (when there is more daylight is available), meaning that it is implemented at different times in the Northern and Southern hemispheres.

Forensic Explorer automatically adjusts the times for DST based upon when the date occurred. The investigator does not need to made additional changes.

DST - UNITED STATES OF AMERICA

In the United States, the days of the year when DST time changes were made (i.e. clocks put forward and the put back) were first regulated in 1986. In 2007, the Energy Policy Act extended these dates by and additional four weeks:

United States DST

	Clocks forward 1 hour	Clocks back 1 hour
1986 - 2006	First Sunday of April	Last Sunday of October
2007 onward	Second Sunday of March	First Sunday of November

Microsoft released a patch for the NTFS file system to compensate for the 2007 change (See <http://support.microsoft.com/kb/931836> for further information). If the examiners forensic workstation is patched, Forensic Explorer will convert the dates in the additional four week period to have the new daylight savings time applied.

Caution: This will apply to all date and times in this four week period, even those in 2006 and prior.

20.6 ADJUSTING DATE IN FORENSIC EXPLORER

The default date and time settings applied by Forensic Explorer are those of the examiners computer.

When examining NTFS or HFS+ file system, in order to view date and times zones according to the location of the subject computer, it is necessary to set date and time settings to that location (given that time settings were confirmed to be accurate at the time of acquisition).

For example, your **forensics lab** and computer is located in **Texas USA**:

- Evidence1.E01 is from New York. Adjust the Time Zone to USA EST to show New York time;
- Evidence2.E01 comes from Los Angeles. Adjust the Time Zone to USA PST to show Los Angeles time.

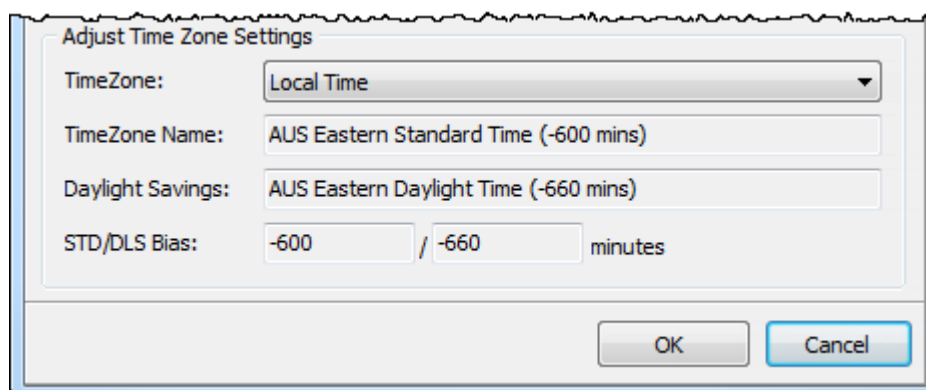
20.6.1 ADJUSTING THE DATE AND TIME WHEN ADDING EVIDENCE

File date and times can be adjusted for each piece of evidence as it is added to a case. For information on adding evidence to a case, see section 10.4 - Adding evidence.

The default Forensic Explorer setting is to process the image according to local time, that is, the time zone setting on the forensic analysis computer. If the device or forensic image originates from the same time zone as the forensic analysis computer, then usually no adjustment is required.

If the device or forensic image is collected from a different time zone, change the time zone setting to the source location in order to display file date and times according to that location using the **TimeZone** drop down menu shown in Figure 187 below:

Figure 187, Adjust time zone information when adding evidence



20.6.2 ADJUSTING EVIDENCE DATE AND TIME DURING A CASE

Time zone settings in a case are displayed in the File System module, Folders view, next to the device or image. In Figure 188 below, the “NIST – 4Dell Latitude CPi.E01” is currently set at “[Local Time]”.

Date and time settings can be adjusted whilst a case is in progress. Settings can be applied to a **device** as well as **volumes** on a device (for example if a drive has an NTFS and FAT partition, date and time adjustments can be made for each).

To adjust date and time settings on a device;

1. In File System, Folders view, **right click** on the **device** or a **partition** and select “**Modify Time Setting...**” from the drop down menu, which opens the Times Settings window, as shown below:

Figure 188, Adjust time zone settings

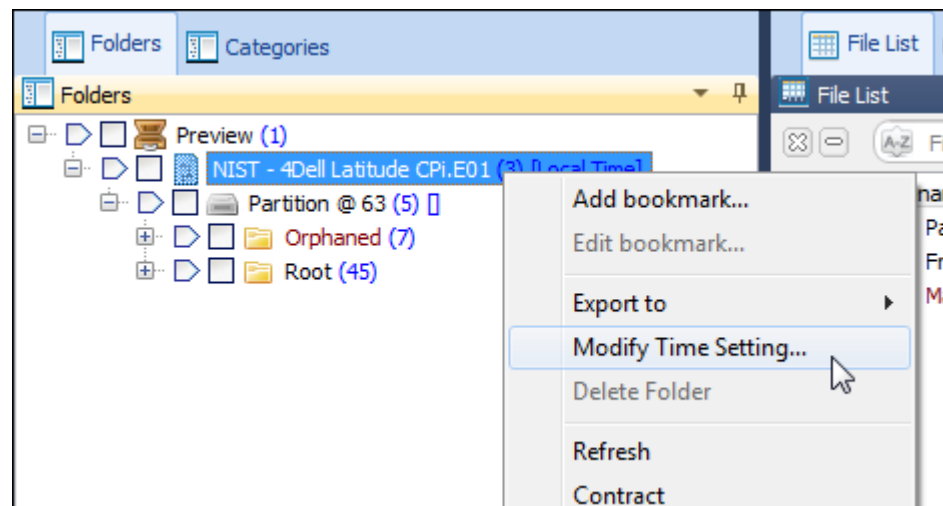
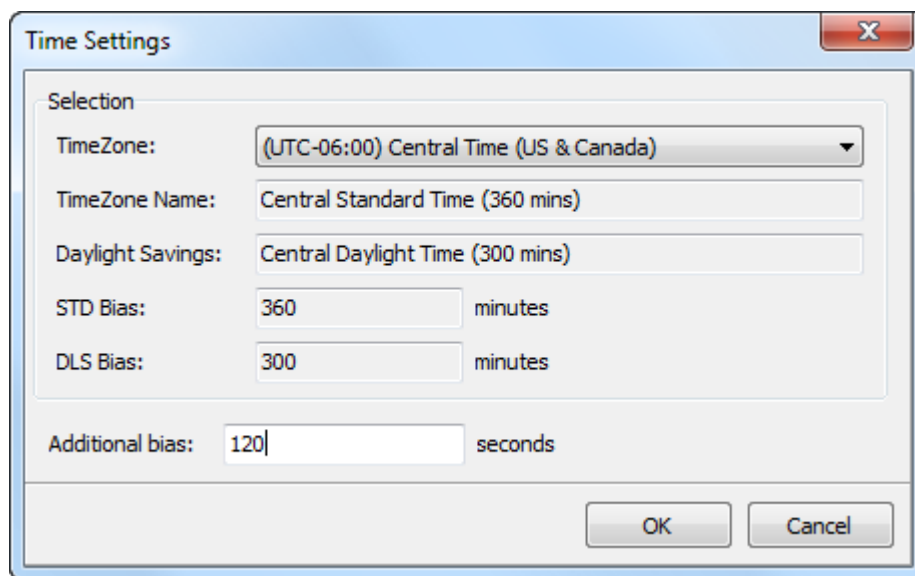
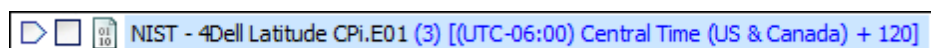


Figure 189, Time settings



2. Select the **TimeZone** relevant to the evidence. The **Additional Bias** field is used to make **minor adjustments in seconds** (for example when the system bios clock is not correctly synced with a known time source).
3. Click **OK** to save these settings. New time zone information will displayed next to the device, as shown in Figure 190 below:

Figure 190, adjusted time zone information



4. Date and time information in the File System > File List will now be adjusted (Note: It may be necessary to refresh the File List display to show this adjustment).

20.6.3 SYNCHRONIZING TIME ZONES

In a case involving multiple computers from different geographic locations, it may be advantageous for the investigator to synchronize time zones.

To synchronize time zones;

1. In the **File System** module, **right click on the case icon**;
2. Select **modify time setting** from the drop down menu, and apply the time to the case.

A **case time setting** has precedence over **evidence time settings**.

EXAMPLE

A new case is created with two evidence files:

- Evidence1.E01 is from New York. The **evidence time zone setting has been adjusted to** USA EST to show New York time;
- Evidence2.E01 is from Los Angeles. The **evidence Time Zone setting has been adjusted** to USA PST to show Los Angeles time.

The suspect in New York created a file at **11 AM** and immediately sent it to the suspect in Los Angeles.

With evidence time adjusted:

- The New York computer has a file creation time of 11AM.
- The Los Angeles computer has a file creation time of 8AM (three hours earlier).

A **Case** time setting of **New York** is then applied to the entire case:

- The New York computer has a file creation time of 11AM.
- The Los Angeles computer has a file creation time of 11AM.

Chapter 21 - Hash Sets

In This Chapter

CHAPTER 21 - HASHING

21.1	Hash Values	246
21.2	Hash Algorithms	246
21.3	Acquisition Hash	246
21.4	Verification Hash	247
21.5	Hashing files in a case	248

21.1 HASH VALUES

A hash value is the numeric result of a mathematical calculation to uniquely identify a file or stream of data. A hash is often referred to as a “digital fingerprint”, as a strong hash algorithm essentially rules out different data from having the same hash value.

21.2 HASH ALGORITHMS

MD5 (Message-Digest algorithm 5) is a publicly available and widely used cryptographic algorithm designed in 1991 by RSA (Ron Rivest, Adi Shamir and Len Alderman). MD5 is the most well-known hash algorithm in computer forensics largely through its implementation by Guidance Software in its EnCase® .E01 forensic acquisition file format:

“The MD5 algorithm uses a 128-bit value. This raises the possibility of two files having the same value to one in 3.40282×10^{38} ”. (EnCase Forensic Version 6.10 User Manual. s.l. : Guidance Software, 2008 (15 p. 12)).

In 1996 cryptanalytic research identified a weakness in the MD5 algorithm. In 2008 the United States Computer Emergency Readiness Team (USCERT) released vulnerability Note VU#836068 stating that the MD5 hash:

“...should be considered cryptographically broken and unsuitable for further use”. (5)

SHA-2 is expected to become the new hash verification standard in computer forensics. SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, and SHA-512) designed by the National Security Agency (NSA), and published by the USA National Institute of Standards and Technology.

21.3 ACQUISITION HASH

In computer forensics, an “**acquisition hash**” is calculated by forensic imaging software during the acquisition of a physical or logical device. It represents the digital fingerprint at the time the image was taken. It is recommended, in line with accepted best forensic practice, that an acquisition hash is always included when acquiring data of potential evidentiary value.

In EnCase® .E01 and Ex01 image file formats, the acquisition hash is written into the image header. In other formats, such as with a DD image, a hash value is usually written into an associated text file.

To **display an acquisition hash** in Forensic Explorer:

1. In the Evidence module, **create or open a case**;
2. In the Evidence module, in the Evidence tab, **click on the image** file to display the file properties, including the Acquisition hash value, as shown in Figure 193, Acquisition and Verification hashes.

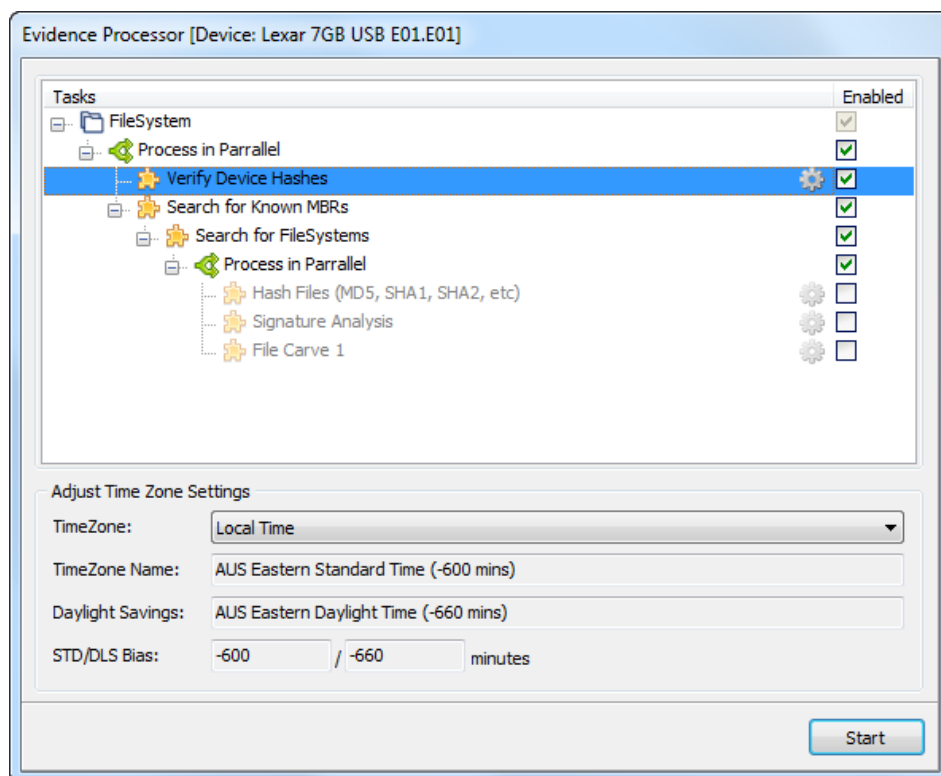
21.4 VERIFICATION HASH

A “verification hash” is a recalculation of the hash for a forensic image file. It enables the investigator to compare the acquisition hash with the verification hash to confirm the validity of the image file, i.e. if the hashes are identical; the image has not changed since acquisition.

There are two methods to calculate verification hash in Forensic Explorer:

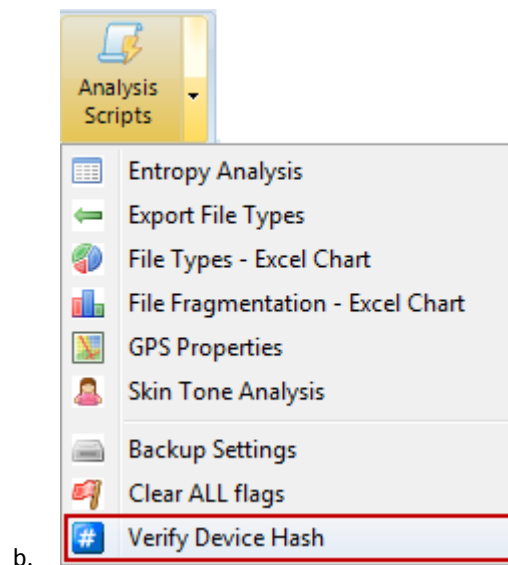
1. Calculate the verification hash **when adding evidence to the case**:
 - a. In the **Evidence Module**, start a case or preview or open an existing case.
 - b. Click the **Add Device**, **Add Image** or **Add File** button to add evidence to the case.
 - c. In the Evidence Processor window, place a check in the “Verify Device Hashes” box. Click **Start** to proceed with the evidence processing.

Figure 191, Evidence Processor



2. Calculate the verification hash during a case:
 - a. In the File System module, run the “Verify Device Hash” script accessed from the **Analysis Scripts** drop down menu:

Figure 192, Running the Verify Device Hash from the File System module toolbar

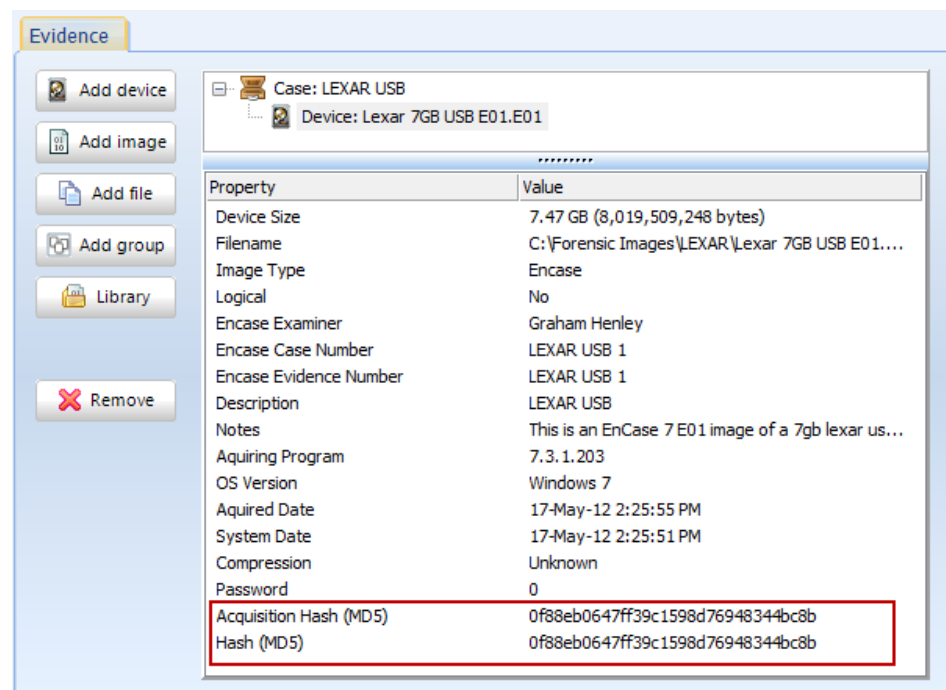


b.

Or alternately run this script from the Scripts module.

The verification hash is written to the evidence module with the acquisition hash, as shown below:

Figure 193, Acquisition and Verification hashes



21.5 HASHING FILES IN A CASE

To calculate hash values for individual files in a case:

1. In the **File System module**, click the required Hash button:

Figure 194, File System module Hash Files button



2. This opens the Hash Files Options window:

Figure 195, Hash Files Options window

A screenshot of the 'Hash Files Options' dialog box. The window has a title bar with a small icon, the text 'Hash Files Options', and standard window controls (minimize, maximize, close). The main area is divided into several sections: 'Source' with three radio buttons ('Searchable items (0 items 0 bytes)' is selected, 'Unallocated space', and 'Checked items (0 items 0 bytes)') and a checkbox 'Include Raw Devices, Partitions and Files'; 'Hash Methods' with four checkboxes ('MD5 Hash' is checked, 'SHA1 Hash', 'SHA256 Hash', and 'CRC32 Hash' are unchecked); 'Options' with two checkboxes ('Force recalculation of hash' and 'Find duplicate files', both unchecked); 'File Size Range' with 'Minimum' set to 0 Mb and 'Maximum' set to 100 Mb (0 = no limit); 'Logging' set to 'Normal' and 'Priority' set to 'Normal'. At the bottom right are 'OK' and 'Cancel' buttons.**Source**

A hash of files will take place in the module that the hash is run. For example, if the button is pressed in the Email module, a hash is calculated for the messages and attachments in that module.

The hash can be calculated on all searchable items, or checked items. **Include raw Devices and Partitions** will

additionally search those items as stand-alone files
(Warning: This will increase the time required);

Hash Methods:	Select the type/s of hash to be used;
Force Recalculation:	When checked, all hashes will be recalculated. (When unchecked a hash will be calculated for only those items that do not have a hash.
Duplicates:	See below.
File Size Range:	Ignore files that do not fall within the range (0,0 = hash all files);
Logging & Priority:	See 7.5 – Logging and Priority.

The results of a file hash are written to the Hash column of the File System module.

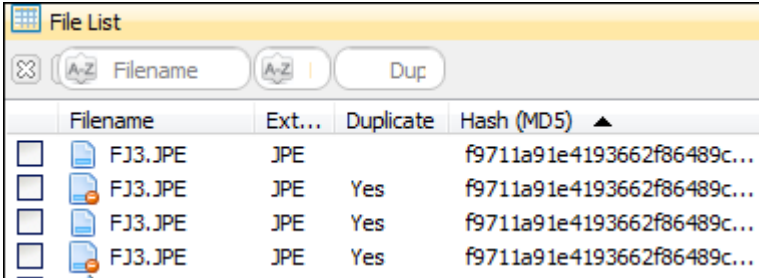
If the Hash column is not visible, learn how to add columns to the File System module in chapter 9.8 - Columns.

21.5.1 DUPLICATES

The “Find duplicate files” checkbox (shown in Figure 195 above) is used to identify files that have identical hash values. In addition to this benefit, a principal reason for identifying duplicates is that it enables the investigator the opportunity to “de-duplicate” a case. This potentially improves case processing time in that it allows the forensic investigator to work with unique files only.

When the “Find duplicate files” option is checked, a **new column** titled “**Duplicate**” is created in the **File System > File List** view (to learn how to add this column to the File System > File List, see 9.8). If the column contains the text “**Yes**”, it means that during the hash process a file with an identical hash value has already been located (the entry in the Duplicate column for the first file found with a unique hash remains blank).

Figure 196, Identifying duplicate files



Filename	Ext...	Duplicate	Hash (MD5)
FJ3.JPE	JPE		f9711a91e4193662f86489c...
FJ3.JPE	JPE	Yes	f9711a91e4193662f86489c...
FJ3.JPE	JPE	Yes	f9711a91e4193662f86489c...
FJ3.JPE	JPE	Yes	f9711a91e4193662f86489c...

A “Hash Method” must be selected before “Find duplicate files” can be used. If multiple hash methods are selected during the hash process, for example MD5, SHA1 and SHA256, the duplicate hash comparison is made using the strongest hash, in this example, SHA256.

To locate only unique files a case (or inversely, to locate only files that are duplicates), it is necessary to apply a filter. For example, a “Text Typing filter (see 9.11.2) or a Folders Filter (see 9.11.4) can be used. Once the de-duplicated list is shown, the unique items can be checked and then subsequent operations performed on checked files only.

21.6 HASH SETS

A Hash Set is a store of hash values for a specific group of files. The hash values are a “digital fingerprint” which can then be used to identify a file and either include or exclude the file from future analysis.

Has Sets are often grouped in the forensic community into:

Good Hash Sets: Operating System files, program installation files, etc. (these are also often referred to as “**Known**” files); and

Bad Hash Sets: virus files, malware, Trojans, child pornography, steganography tools, hacking tools etc. (these are often referred to as “**Notable**” files).

Hash Sets have two essential uses:

1. **To reduce the size of a data set and speed up an investigation:** A Hash Set that eliminates known operating system and program installation files, allows the examiner to quickly focus on electronic files created by the user and which are likely to be the subject of the investigation.
2. **To quickly identify specific files relevant to a case:** If the investigator is attempting to locate the presence of a group of known files, applying their hash value to the case will quickly and positively identify them in the data set.

21.6.1 SUPPORTED HASH SET FORMATS

Forensic Explorer supports the following types of Hash Sets:

.db3 or .edb3	The Forensic Explorer Hash Set (SQLite database format. The .edb3 is the extension is for an encrypted file from a third party supplier, e.g. www.hashsets.com);
.hash	EnCase 6 format (no conversion is necessary);
Flat Hash Set	A list of hash values in a text file (a Flat Hash Set must have a file extension of .txt, md5, .sha1 or .sha256. See 21.8.2 below).

The default hash set location is: *[profile]\Documents\Forensic Explorer\HashSets*

21.7 DOWNLOAD HASH SETS

Hash Sets for use with Forensic Explorer are available for download from:

<http://www.forensicexplorer.com/hashsets.php>. Hash sets from other trusted locations can also be used.

21.8 CREATING HASH SETS

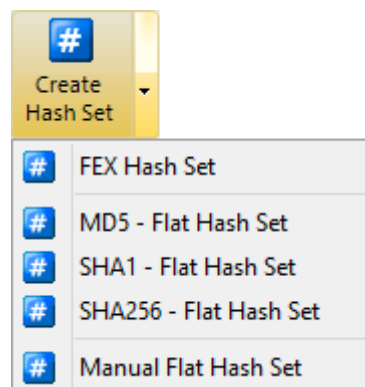
Before creating a custom hash set, files in a case must be hashed. Follow the instructions in 21.5 above.

21.8.1 FORENSIC EXPLORER HASH SET

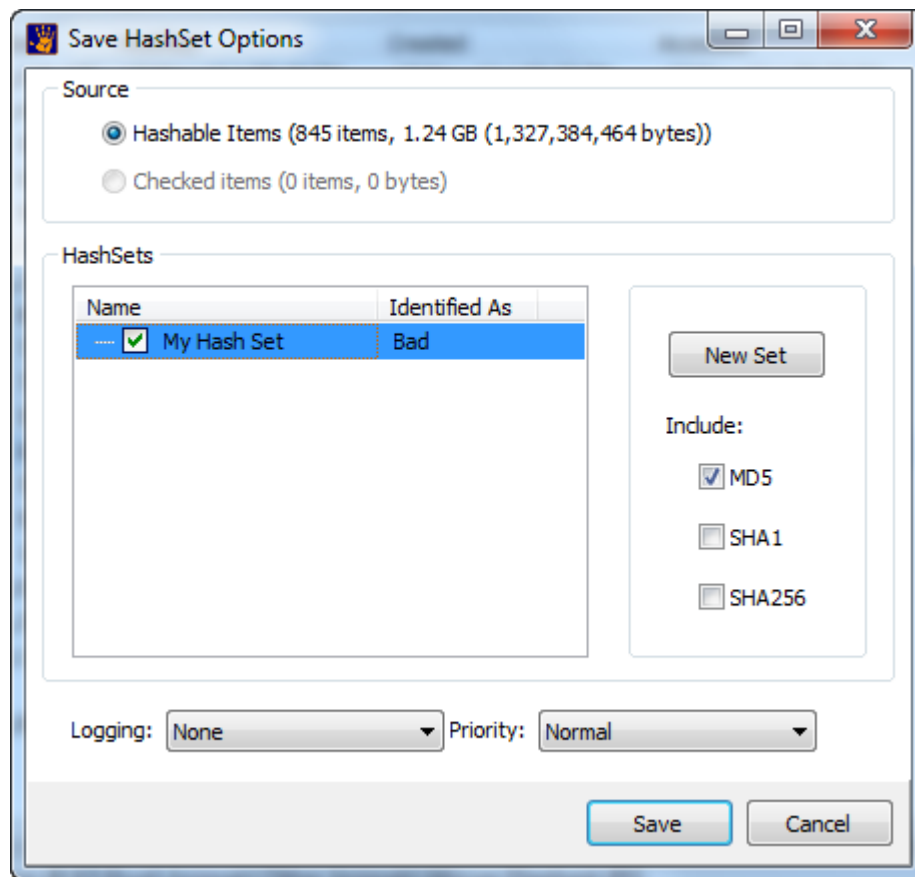
To create a new **Forensic Explorer Hash Set**:

1. Click the “Create Hash Set” button in the File System module toolbar and select **FEX Hash Set**:

Figure 197, Create Hash Set



The following window will display:



2. Click the **New Set** button. Check the type of hash/s to be used in the set (MD5, SHA1, and SHA256). A new hash set will be added to the list;
3. Rename the new hash set and right click to rename the "Identified As" text. Click Save to save the Hash Set. The new has set is created and saved to disk in the current hash set location (default location is: "[User]\Documents\Forensic Explorer\HashSets\").

Files with the extension .db3 are hash sets created by Forensic Explorer. Files with the extension .edb3 are encrypted files that have been acquired from a third party source and provided for use with Forensic Explorer.

4. The new hash set is now available when the Hash Match button is pressed (refer to 21.9- Apply a Hash Set in a Case, below).

21.8.2 FLAT FILE HASH SETS

A Flat File Hash set must:

- Be a plain text file in **ANSI** format;
- Have an extension of **.txt**, **md5**, **.sha1** or **.sha256** (If the .txt extension is used Forensic Explorer will determine the type);
- **NO blank lines**. A blank line identifies the end of the list.

The following file format can be used in order to give meaning to Forensic Explorer column data:

Figure 198, Flat Hash Set format

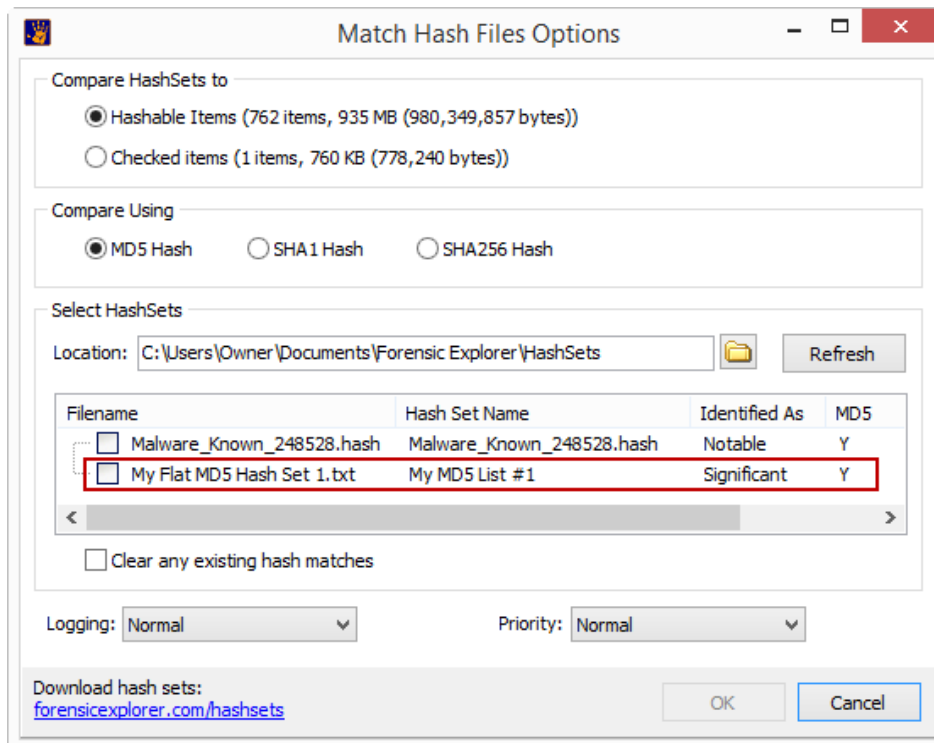
# This is a Flat MD5 Hash Set file	This is a comment
# Hash Set Name = My MD5 List 1	'HashSet' column text
# Identified As = Significant	'HashSet Identified As' column text
83e05311eab2c2d50c2bc6fa219e6905	The list of hash values
a526a95fc34e049360755d9f0450d662	
b8bca7ac76f0ade815c5c743866293e0	
	A blank line = end.

TO MANUALLY CREATE AND USE A FLAT HASH SET

To **manually add** the **Flat Hash Set** file to Forensic Explorer:

1. Place the correctly formatted Flat Hash Set in the Forensic Explorer hash set folder: **[profile]\Documents\Forensic Explorer\HashSets**;
2. Click on the **Hash Match** button in the File System module toolbar to open the **Match Hash Files Options** window;
3. The Flat Hash Set should appear in the list of available sets, as shown in Figure 199 below .

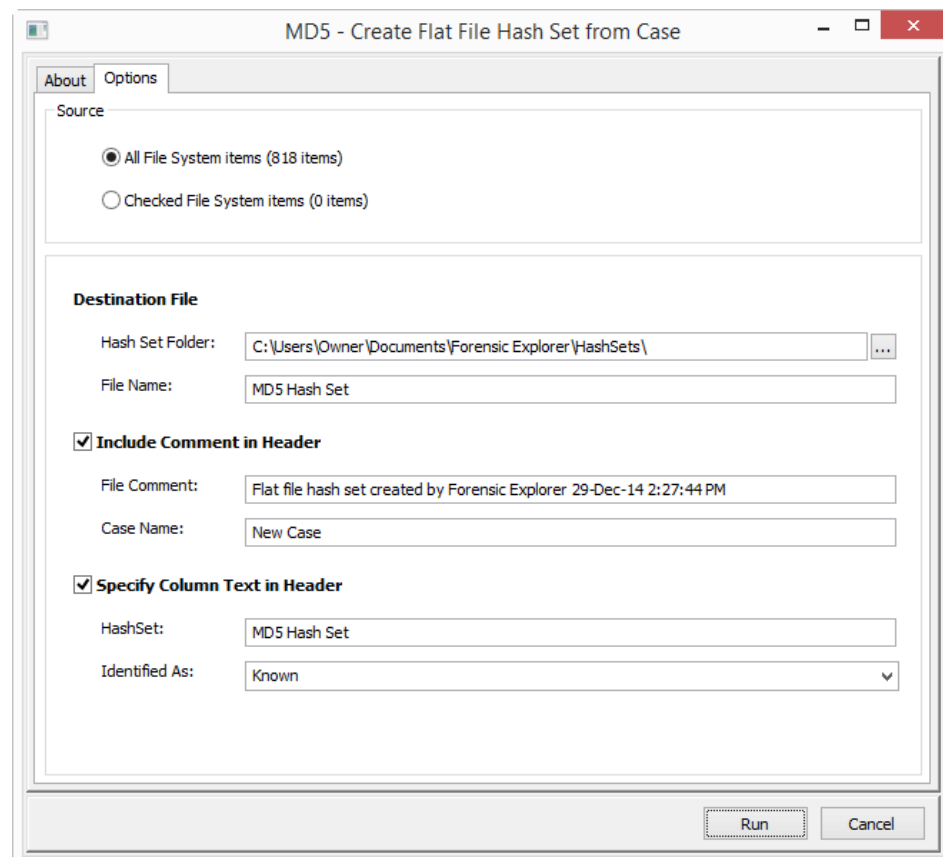
Figure 199, Flat Hash Set



TO CREATE AND USE A FLAT HASH SET FROM A CASE

To create a Flat Hash Set, select the required format, MD5, SHA1 or SHA256 from the **Create Hash Set** button drop down menu as shown in Figure 197 above (This executes a script which can be viewed and edited in the Scripts module). The following window appears:

Figure 200, Create Flat File Hash Set from Case



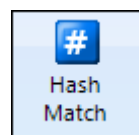
The Flat File Hash set is then created with the specified options and written to the **[profile]\Documents\Forensic Explorer\HashSets** folder. The hash set appears and is available for use in the Hash Set window shown in Figure 199 above.

21.9 APPLY A HASH SET IN A CASE

To apply a hash set in a case:

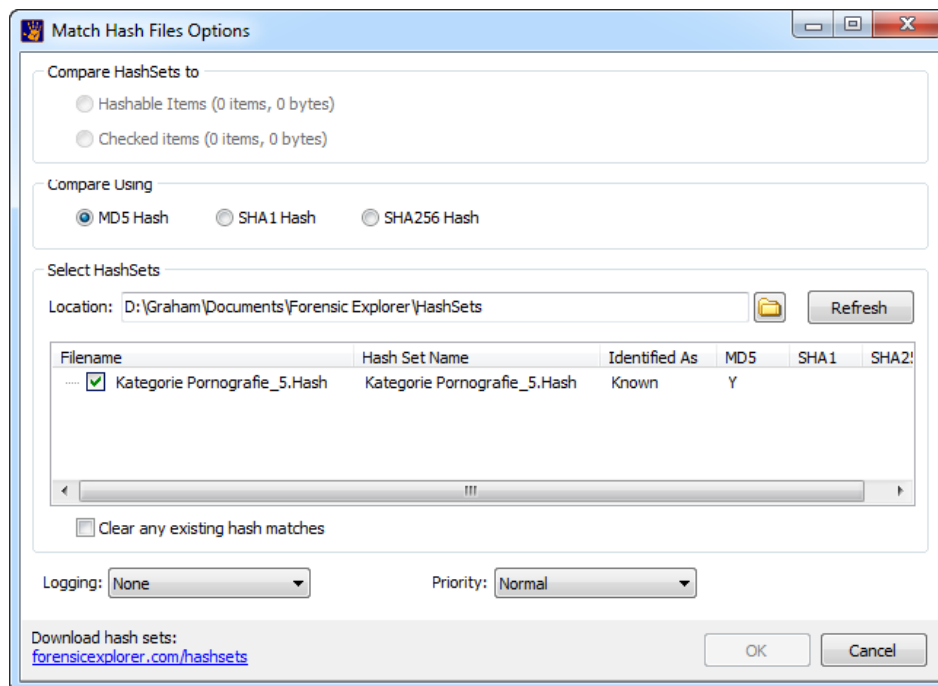
1. Hash individual files in your case as described in 21.5 above.
2. In the File System module, click the **Hash Match** icon.

Figure 201, File System module, Hash Match icon



3. The Match Hash window will open:

Figure 202, Match Hash window



4. Select the hash set to use by placing a tick in its box:

File Name: The name of the hash file;

Hash Set Name: The name given to the hash set read from the header of the file. If the Hash Set Name is blank, the File Name is used.

Identified as: Describes the classification given to the hash set when it was created.

Hash Type: The types of hashes contained in the file are marked in the remaining columns using "Y".

5. **Clear any existing hash matches:**

- a. When "Clear any existing hash matches" is checked:
Existing has values in the "Hash Set" and "Hash Set Identified As" columns will be cleared before then new values are written into the columns.
- b. When "Clear any existing hash matches" is not checked:
The new values of the hash comparison will populate the "Hash Set"

and “Hash Set Identified As” columns. They will overwrite any existing values. However, existing values in those columns which are not overwritten will remain.

6. Click OK to proceed with the hash match.

Once a Hash Match has been run, two columns will be created in the Forensic Explorer File System module, “Hash Set” and “Hash Set Identified As”:

Figure 203, Running a Hash Match in a case

Hash (MD5)	HashSet ▼	HashSet Identified As
b6d81b360a5672d80c27430f39153e2c	GetData [Windows]	good
f1c9645dbc14efddc7d8a322685f26eb	GetData [Windows]	good
bdf3bf1da3405725be763540d6601144	GetData [Windows]	good
fafa5efeaf3cbe3b23b2748d13e629a1	GetData [Windows]	good
076e3caed758a1c18c91a0e9cae3368f	GetData [Windows]	good
9aebbac92e6bf3b4009f79be3549b5a	GetData [Windows]	good
cdf80f35aba322d5d0e6b6f6fe0b2995	GetData [Windows]	good
ba45c8f60456a672e003a875e469d0eb	GetData [Windows]	good
5a44c7ba5bbe4ec867233d67e4806848	GetData [Windows]	good
9d377b10ce778c4938b3c7e2c63a229a	GetData [Windows]	good
15988347a31ba4fb6dce89f1931db7bf	GetData [Windows]	good
3e80abdf74d921066de10fb05aaa553f	GetData [Windows]	good
2b04df3ecc1d94afddff082d139c6f15	GetData [Windows]	good
9b1afacf7447e4b7c1c98702e261be2e	GetData [Windows]	good
b44a59383b3123a747d139bd0e71d2df	GetData [Windows]	good

An entry in the Hash Set column identifies that the file hash matches a hash in the set.

Chapter 22 - File Signature Analysis

In This Chapter

CHAPTER 22 - FILE SIGNATURE ANALYSIS

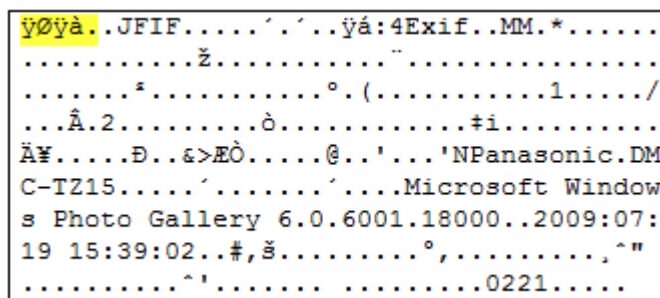
22.1	File signature analysis.....	260
22.2	Why run file signature analysis?.....	260
22.3	Running a file signature analysis	260
22.4	Examine the results of a file signature analysis.....	262

22.1 FILE SIGNATURE ANALYSIS

Signature analysis is the process of identifying a file by its header rather than by other means (such as the file extension). The International Organization for Standardization (ISO) has published standards for the structure of many file types. The standards include a “file signature”, a recognizable header which usually precedes the file data and assigns a file to a specific type, e.g. a jpeg.

For example, shown Figure 204, JPEG file signature Figure 204 below, is the beginning of a photo taken with a digital camera. It is identified as a JPEG by the file header `ÿØÿà` (or in Hex: FF D8 FF E0 00).

Figure 204, JPEG file signature



Identifying a file by its signature is a more accurate method of classification than using the file extension (e.g. .jpg), as the extension can easily be altered.

22.2 WHY RUN FILE SIGNATURE ANALYSIS?

File signatures are an important part of the examination process because gives the investigator a confidence that they are seeing files for what they actually are. It is recommended that a File Signature analysis is one of the first steps performed by the investigator in each new case.

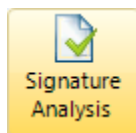
A file signature analysis with Forensic Explorer will:

- Flag files for which the file extension does not match the file signature. These files may have been deliberately manipulated to hide data;
- Empower other components of Forensics Explorer, such as the Categories view, to see files based on file signature, rather than extension;

22.3 RUNNING A FILE SIGNATURE ANALYSIS

To run a file signature analysis in Forensic Explorer:

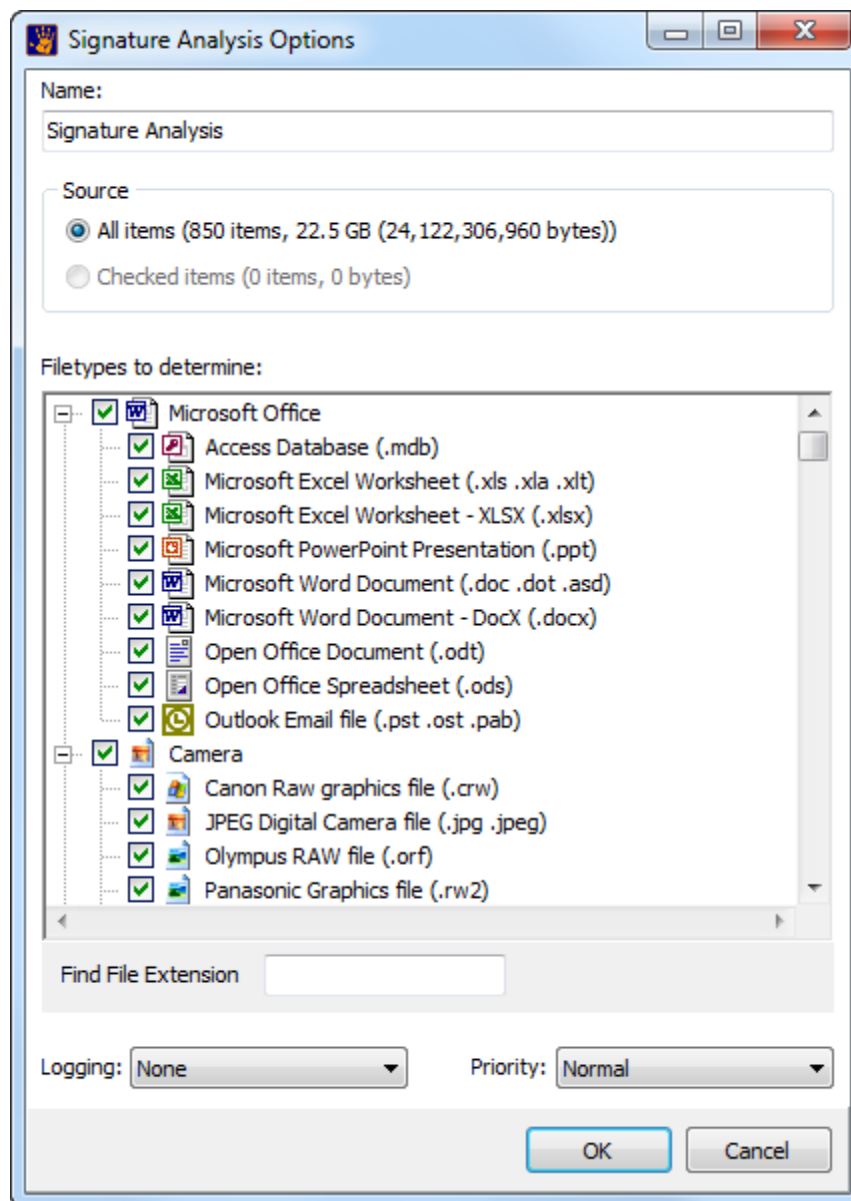
1. Click on the “Signature Analysis” button in the File System toolbar (shown below):



Select the file types for which a signature analysis is to be conducted.

Note that the speed of the analysis is affected by the number of file types selected. File signatures are inbuilt into Forensic Explorer and cannot be added. A custom file signature can be created using a script. See Chapter 18 - Scripts Module, for more information on writing scripts.

Figure 205, Selecting file types for signature analysis



Logging & Priority: See 7.5 – Logging and Priority.

22.4 EXAMINE THE RESULTS OF A FILE SIGNATURE ANALYSIS

There are three columns which relate to file signatures:

1. Extension

The Extension column lists the files given extension (i.e. the extension given with the file name).

2. File Signature

The File Signature column is the result of the analysis of the file header. After a File Signature Analysis has been conducted for a file, the column either:

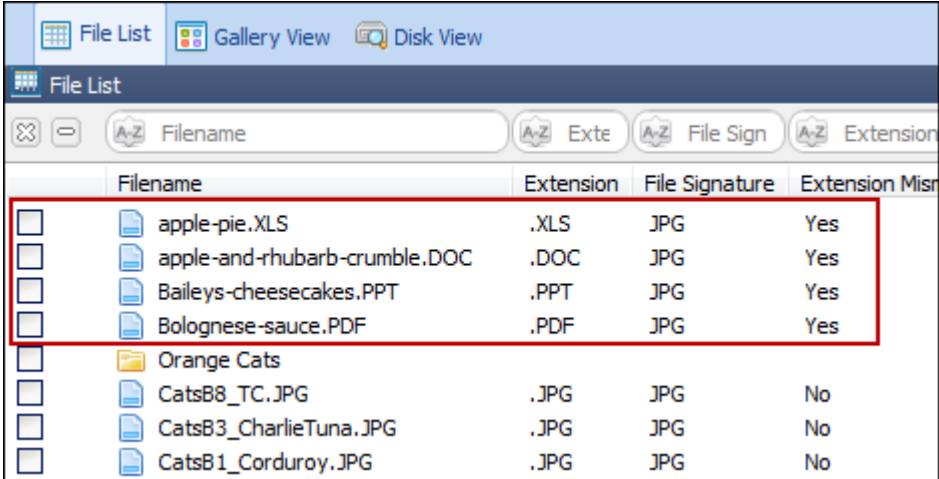
- a. **shows an extension:** This means that it has been successfully identified as a file type contained within the Forensic Explorer signature list, shown in Figure 205 above; or,
- b. **is blank:** This means that the file signature could not be matched against the files types contained in the Forensic Explorer signature list.

3. Extension Mismatch

The Extension Mismatch column alerts the forensic investigator to any files where the identified signature does not match the current extension. These files are worthy of closer examination to determine the underlying reason.

Results of a file signature analysis are shown in Figure 206 below:

Figure 206, File System module columns relating to file extension



	Filename	Extension	File Signature	Extension Mismatch
<input type="checkbox"/>	apple-pie.XLS	.XLS	JPG	Yes
<input type="checkbox"/>	apple-and-rhubarb-crumble.DOC	.DOC	JPG	Yes
<input type="checkbox"/>	Baileys-cheesecakes.PPT	.PPT	JPG	Yes
<input type="checkbox"/>	Bolognese-sauce.PDF	.PDF	JPG	Yes
<input type="checkbox"/>	Orange Cats			
<input type="checkbox"/>	CatsB8_TC.JPG	.JPG	JPG	No
<input type="checkbox"/>	CatsB3_CharlieTuna.JPG	.JPG	JPG	No
<input type="checkbox"/>	CatsB1_Corduroy.JPG	.JPG	JPG	No

Chapter 23 - Data Recovery

In This Chapter

CHAPTER 23 - DATA RECOVERY

23.1	DATA Recovery - Overview	264
23.2	FAT data recovery.....	265
23.2.1	FAT - Deleted files.....	265
23.2.2	FAT - Recover folders.....	269
23.3	NTFS data recovery.....	272
23.3.1	NTFS - deleted files	272
23.3.2	NTFS - orphans	273
23.3.3	NTFS - Recover Folders	274
23.4	File carving.....	276
23.4.1	Carving advantages and limitations.....	276
23.4.2	Forensic Explorer file carving engine.....	277
23.4.3	Carving using scripts	280

23.1 DATA RECOVERY - OVERVIEW

An essential part of computer forensics is the ability to recover evidence from deleted data. Forensic Explorer automates the following data recovery procedures:

1. Recovery of **deleted files** within the existing file system;
2. Recovery of **orphaned** folders in the existing file system;
3. **Recovery of folders** from unallocated clusters;
4. **File carving** from unallocated clusters.

It is important for the forensic investigator to understand the methodology behind the recovery automation and to be able to validate recovery results manually. This chapter sets out to provide a description of the tools for automation and the methodology to validate search results.

It should be noted that the success of data recovery will depend on many factors, including such things as;

- Subsequent disk activity which may have overwritten and corrupted data;
- The level of file fragmentation and the extent to which it can be tracked.

An investigator should always critically examine data recovery results before drawing conclusions.

23.2 FAT DATA RECOVERY

When a file is from a FAT file system, the content of the file remains available for recovery from those newly unallocated clusters. The original data will remain in each cluster up until such time as it is used to store new data and the previous content overwritten. If only a percentage of clusters are reused, then partial recovery, or the recovery of a data fragment, may still be possible. If all clusters are re-used, all original content is overwritten and destroyed.

23.2.1 FAT - DELETED FILES

Forensic Explorer automatically displays deleted files and folders in Folders view and File List view. They are marked with the following icons:



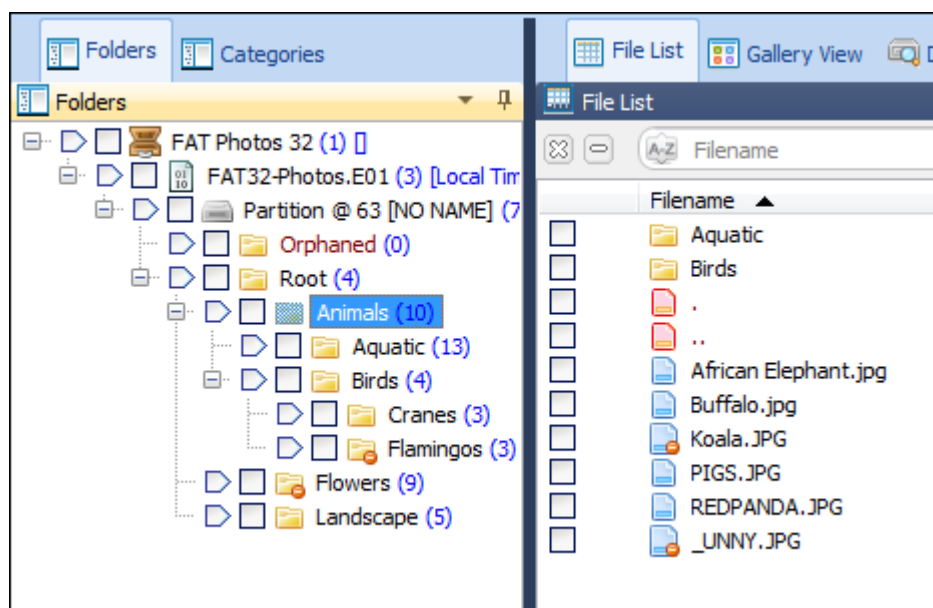
Deleted file



Deleted folder

An example is shown in Figure 207 below:

Figure 207, Deleted folders and files in File System module Folder view and File List view



FAT - IDENTIFYING DELETED FILES

In a FAT file system Forensic Explorer identifies deleted files by locating the **0xE5** marker in the first byte a files directory entry.

When a file is deleted on a FAT system its entries in the FAT table are reset. At this point, as far as the FAT is concerned, a deleted file no longer occupies physical space on the disk.

Importantly, the directory entry for a deleted FAT file retains the attributes for the starting cluster and the logical file size. Forensic Explorer uses the logical file size to calculate the total clusters used by the file.

FAT - FILENAMES OF DELETED FILES

Some deleted files will display in File List view of Forensic Explorer with an underscore as the first character, whilst other deleted files retain their original name. An example is shown in Figure 207 above with the deleted file “_UNNY.JPG” (originally called “BUNNY.JPG”) has its first character replaced, but Koala.JPG in the same folder retains its original file name.

The starting character of a Short File Name (SFN) is overwritten when a file is deleted by the 0xE5 marker. For display purposes, Forensic Explorer replaces the first character with an underscore.

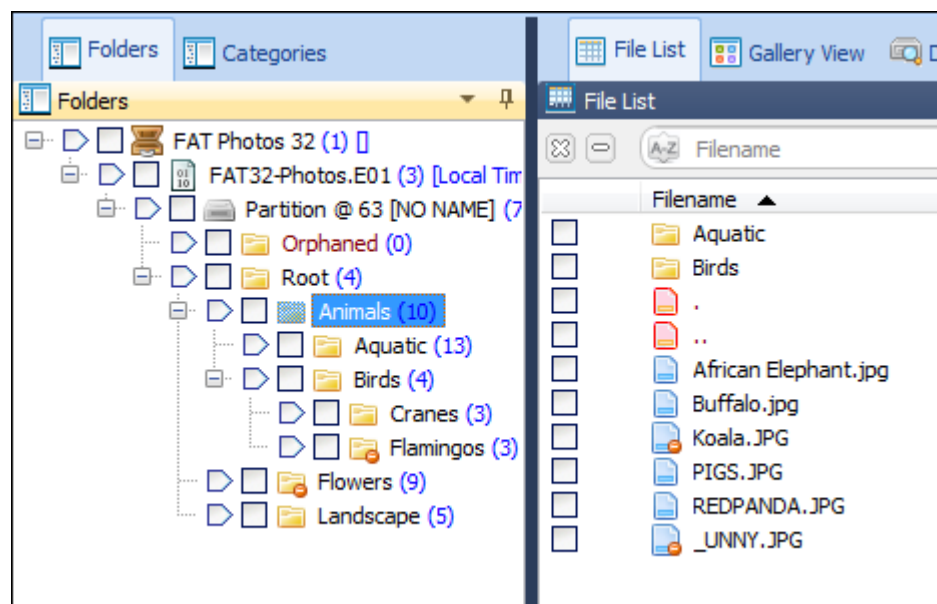
Where a file has both a SFN and a Long File Name (LFN) directory entry, the missing first character of the file name is located in the LFN and is used by Forensic Explorer to display the full original file name.

FAT - LOCATING DATA FOR A DELETED FILE ON DISK

The following example details the methodology used by Forensic Explorer to identify and locate deleted files on a FAT formatted disk.

In Figure 208 below, the parent folder of the file Koala.JPG is highlighted in Folders view:

Figure 208, Animals folder selected in Folders view



The directory entries for the parent are displayed in Hex view:

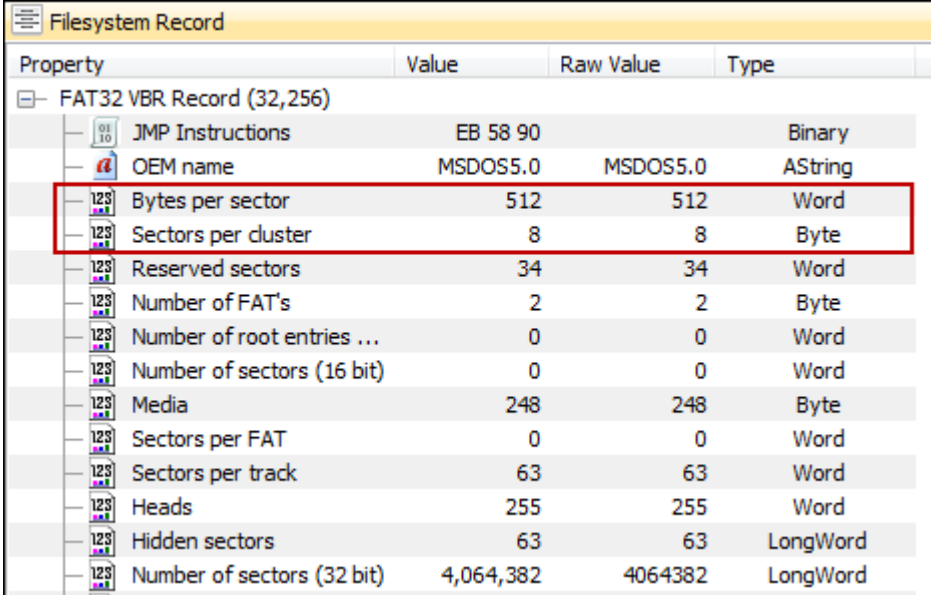
The following information is observed:

1. The short filename is “_OALA.JPG”
2. The starting cluster is 492;
3. The file size is “780831” bytes;
4. The long file name is “Koala.JPG”

To manually calculate the number of clusters used by Koala.JPG, the following additional disk information is needed:

1. Bytes per sector; and
2. Sectors per cluster.

This information is available by decoding the Volume Boot Record (VBR) with Filesystem Record view:



Property	Value	Raw Value	Type
FAT32 VBR Record (32,256)			
JMP Instructions	EB 58 90		Binary
OEM name	MSDOS5.0	MSDOS5.0	AString
Bytes per sector	512	512	Word
Sectors per cluster	8	8	Byte
Reserved sectors	34	34	Word
Number of FAT's	2	2	Byte
Number of root entries ...	0	0	Word
Number of sectors (16 bit)	0	0	Word
Media	248	248	Byte
Sectors per FAT	0	0	Word
Sectors per track	63	63	Word
Heads	255	255	Word
Hidden sectors	63	63	LongWord
Number of sectors (32 bit)	4,064,382	4064382	LongWord

To determine the number of clusters used by Koala.JPG, the calculation is:

- File size: 780,832 bytes / 512 bytes per sector = 1525.06 sectors
- 1525 sectors / 8 sectors per cluster = 190.63 clusters

The number of clusters that can be attributed to Koala.JPG is 191. The file therefore starts at cluster 492 and finishes at the end of cluster 682.

To see this information in Forensic Explorer, switch to the “File Extent” view which details the byte, sector and cluster positions of the file:

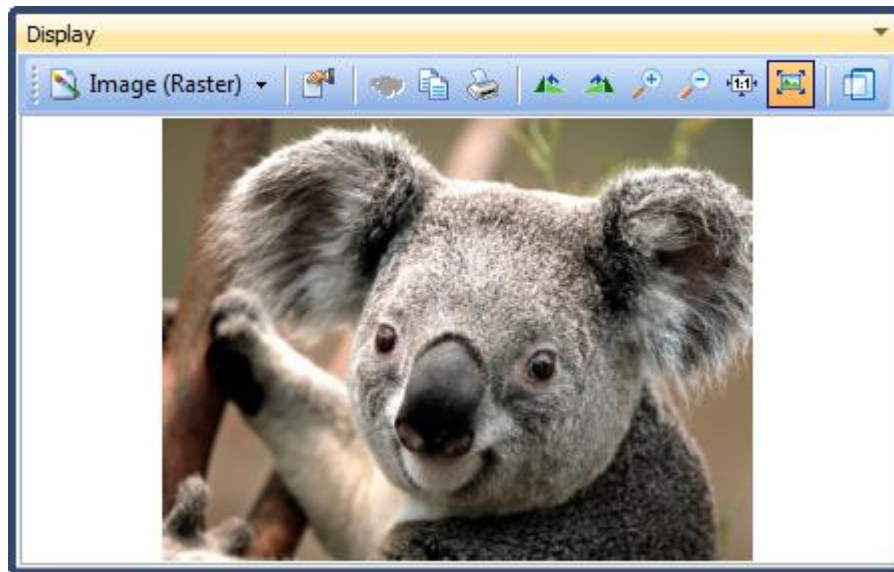
Cluster Start: 492

Cluster End: 682

Cluster Length: 191
Sector Start 11941
Sector End 13468
Sector Length 1528

Highlighting the sectors in disk view reveals the following picture:

Figure 211, Display view of Koala.JPG

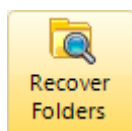


23.2.2 FAT - RECOVER FOLDERS

“Recover Folders” is a method of searching unallocated clusters to find deleted or missing folders and their content. Recover Folders will often locate multilevel folder and sub folder structures and make them visible to the investigator within the File System module. **For this reason it is recommended that a Recover Folders search be one of the first tasks undertaken by an investigator in a new case.**

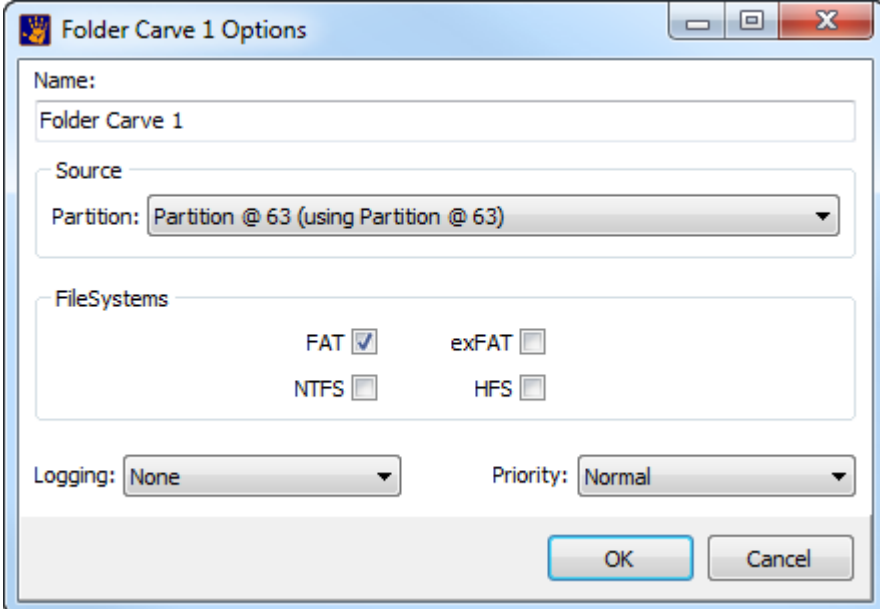
To run a **Recover Folders** search, click the **Recover Folders** toolbar icon in the File System module:

Figure 212, Recover Folders File System module toolbar icon



This opens the **Folder Carve** options window:

Figure 213, Recover Folders options

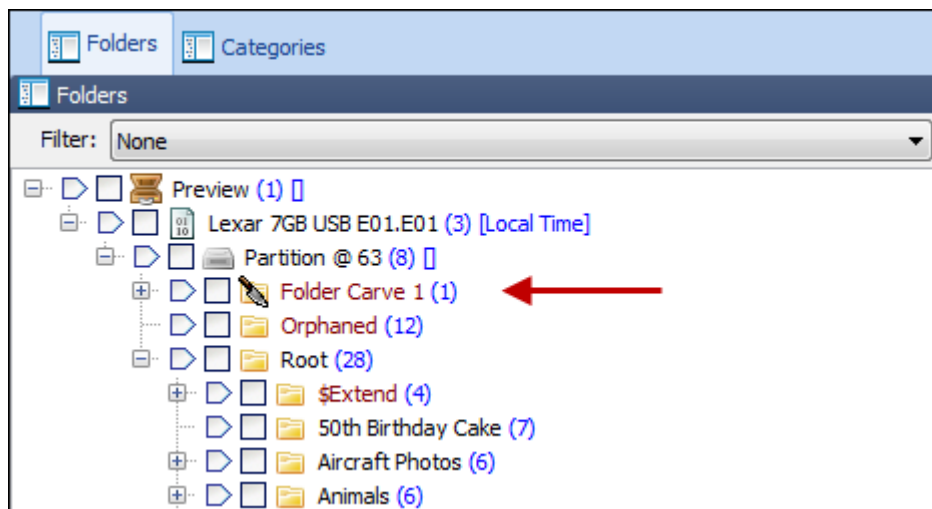


Name:	Enter the folder name which will hold the recovered folders in the Folders view of the File System module.
Source:	A Recover Folders search must be run on an existing partition . Select the partition from the drop down menu.
File Systems:	Select the type of File System records for which to search.
Logging & Priority:	See 7.5 – Logging and Priority.

When the “Recover Folders” command is executed on a FAT partition in Forensic Explorer, the program searches unallocated clusters for the “dot, double dot” directory entry signature 0x2E and 0x2E2E as well as LFN and SFN directory entry structures.

The “Double Dot” is used to locate the parent folder and traverse up the directory tree. Eventually, by reason of the fact that located folders are not part of the existing file system, a parent folder will not be found. Forensic Explorer appends the results in a folder in File System module Folders view using the generic name “Folder Carve X”, as shown below:

Figure 214, Recover Folders results



23.3 NTFS DATA RECOVERY

When a file is deleted in a NTFS file system, the data content of the file remains available for recovery from the newly unallocated clusters. The original data will remain in each cluster up until such time as it is used to store new data and the previous content overwritten.

If only a percentage of clusters are reused, then partial recovery, or the recovery of a “data fragment”, may still be possible. If all clusters are re-used, all original content is overwritten and destroyed.

23.3.1 NTFS - DELETED FILES

Each file and folder on an NTFS drive has an “allocation status” set by a flag in the Master File Table (MFT) record header. The flag identifies whether it is an “allocated” (active) file, or “unallocated” (deleted). To display deleted files, Forensic Explorer reads the MFT to find “unallocated entries”.

Allocation status flag values are shown in the tables Table 1 and Table 2 below:

Table 1, Allocation status for a file

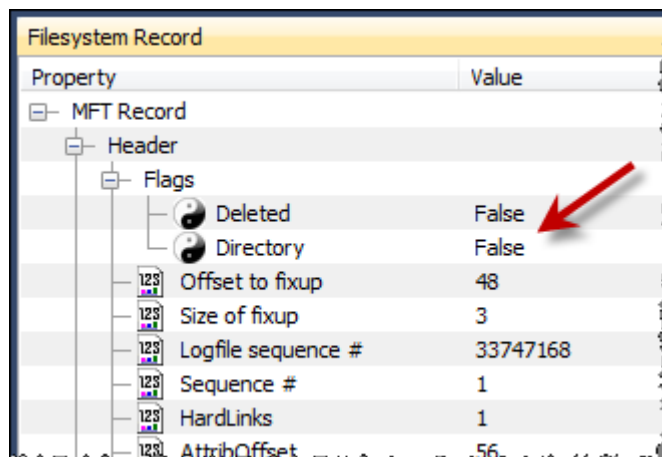
Flag Value for a file		
Hex	Binary	Status
00	00000000	Unallocated
01	00000001	Allocated

Table 2, Allocation status for a folder

Flag value for a folder		
Hex	Binary	Status
02	00000010	Unallocated
03	00000011	Allocated

In Forensic Explorer, the allocation status of a file is shown in Filesystem Record view when the file is highlighted:

Figure 215, Forensic Explorer Record view showing decoded MFT allocation status (an allocated file)



When the MFT record is marked as unallocated, both the MFT record and clusters used to store the data (for non-resident files) become available to store new data. However, importantly:

- the file attributes within the unallocated MFT record remain intact;
- the data for the file remains untouched.

When new data is written to the MFT record or the clusters holding the data, the possibility for successful recovery of the deleted file is diminished.

23.3.2 NTFS - ORPHANS

In Folders view a folder is created by Forensic Explorer called “Orphans”. Orphans are deleted folders and files for which the original parent folder is unknown.

From the investigators perspective, an orphaned file can be treated in an investigation the same way as any other deleted file. The only difference is that it is longer possible to determine the location of the file or folder within the directory structure prior to deletion.

An example of how NTF folders and file can become orphaned is as follows:

1. A folder on an NTFS drive, “PARENT-1” is deleted by the user. At this point PARENT-1 and its content, “CHILD-FOLDER-1”, are deleted files.
2. The user then saves a new file. The MFT record for PARENT-1 is re-used to store information for the new file. The MFT information for PARENT-1 is now overwritten and destroyed.
3. The computer is then forensically imaged and examined.
4. Forensic Explorer reads the file system and CHILD-FOLDER-1 is located. Forensic Explorer then tries to trace the parent folder, but determines that

the MFT record for the parent folder has been re-used by another file and the original information for the parent is no longer available.

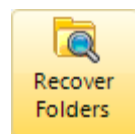
5. CHILD-FOLDER-1 and its content are available, but Forensic Explorer cannot determine where in the tree structure it belongs. The Orphans folder is created by Forensic Explorer to hold CHILD-FOLDER-1 and its content.

23.3.3 NTFS - RECOVER FOLDERS

“Recover Folders” is a method of searching unallocated clusters to find deleted or missing folders and their content. Recover Folders will often locate multilevel folder and sub folder structures and make them visible to the investigator within the Forensic Explorer module. **For this reason it is recommended that a Recover Folders search be one of the first tasks undertaken by an investigator in a new case.**

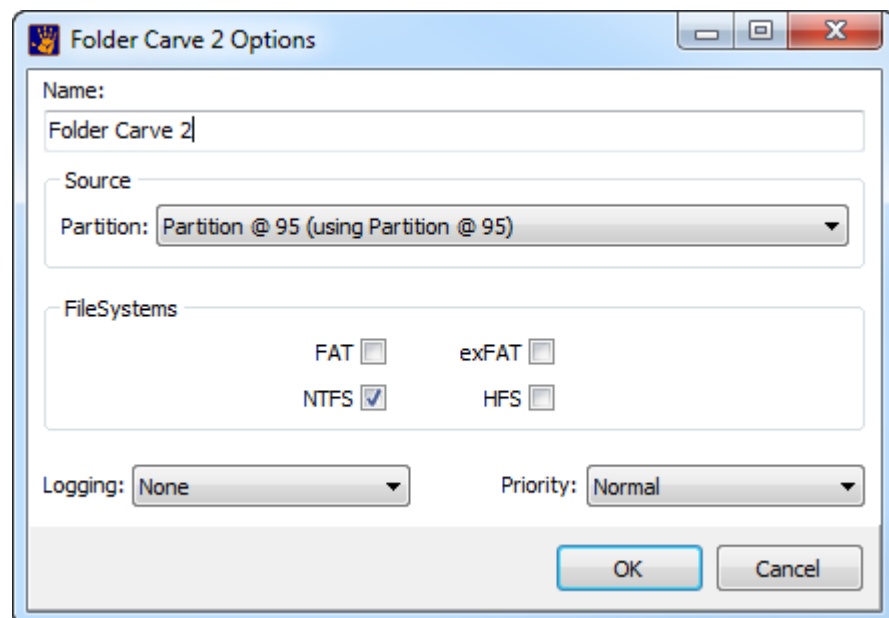
To run a **Recover Folders** search, click the **Recover Folders** toolbar icon in the File System module:

Figure 216, Recover Folders File System module toolbar icon



This opens the **Folder Carve** options window:

Figure 217, Recover Folders options



When the “Recover Folders” command is executed on a NTFS partition in Forensic Explorer, the program searches unallocated clusters for MFT records.

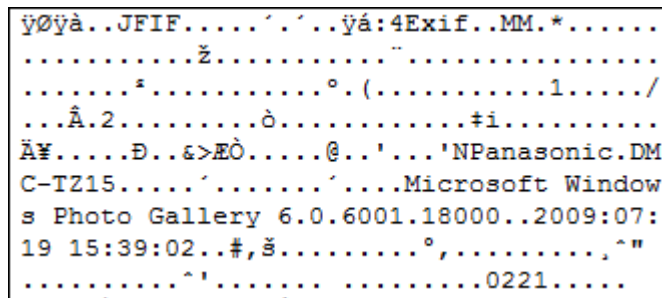
The process is identical to that described in “NTFS Orphans” above. The only difference is that instead of working with files in existing MFT records, the MFT records themselves are recovered from unallocated space.

23.4 FILE CARVING

File carving is a well-known computer forensics term used to describe the identification and extraction of file types from unallocated clusters using file signatures. A file signature, also commonly referred to as a magic number, is “a constant numerical or text value used to identify a file format or protocol” (16).

An example of a file signature is shown in Figure 218, which is the beginning of a .jpg file in Hex view:

Figure 218, View of .jpg file header



```

ÿØÿà..JFIF.....'..'ÿá:4Exif..MM.*.....
.....Ž.....".....
.....*.....°.(.....1...../
...Â.2.....ò.....#i.....
Ä¥.....Ð..&>EÒ.....@...'...'NPanasonic.DM
C-TZ15.....'.....'.....Microsoft Window
s Photo Gallery 6.0.6001.18000..2009:07:
19 15:39:02...#,š.....°,.....,^"
.....^'.....0221.....
  
```

The object of the carving exercise is to identify and extract (carve) the file based on this signature information alone. Carrier (2005) describes File carving as:

“...a process where a chunk of data is searched for signatures that correspond to the start and end of known file types. The result of this analysis process is a collection of files that contain one of the signatures. This is commonly performed on the unallocate space of a file system and allows the investigator to recover files that hav no metadata structures pointing to them”. (2)

23.4.1 CARVING ADVANTAGES AND LIMITATIONS

File carving has both advantages and limitations. These include:

File system independent

File carving is essentially file system independent. A file type will exhibit the same file signature and structure on under FAT, NTFS, HFT, EXT2 or other file systems and can be data carved accordingly. File carving is also effective method of recovery when the file system is corrupt or destroyed.

Time Required:

A drawback of file carving is that it can take a considerable amount of time to process a large drive. The lower the level of search (i.e. cluster v's sector v's byte), and the greater the number of file signatures searched for simultaneously, the longer the search.

False Positives:

File carving always brings with it the risk of false positives, where identified file signatures are not true identifiers for the start of a file. Searching at the lower levels of sector and byte may increase the number of false positives because it removes the validation requirement that the signatures must start near cluster boundaries.

Data Fragmentation:

Without file system records, it is difficult to track a fragmented files. File carving relies on the information contained in the file structure and to a lesser extent it's on disk layout.

No Original File Names

As file names are stored only as part of the file system, data carved files cannot be recovered with their original name.

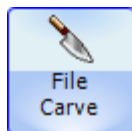
23.4.2 FORENSIC EXPLORER FILE CARVING ENGINE

Forensic Explorer has an inbuilt file carving engine capable of carving more than 300 file types.

To run a file carve using the Forensic Explorer file carving engine:

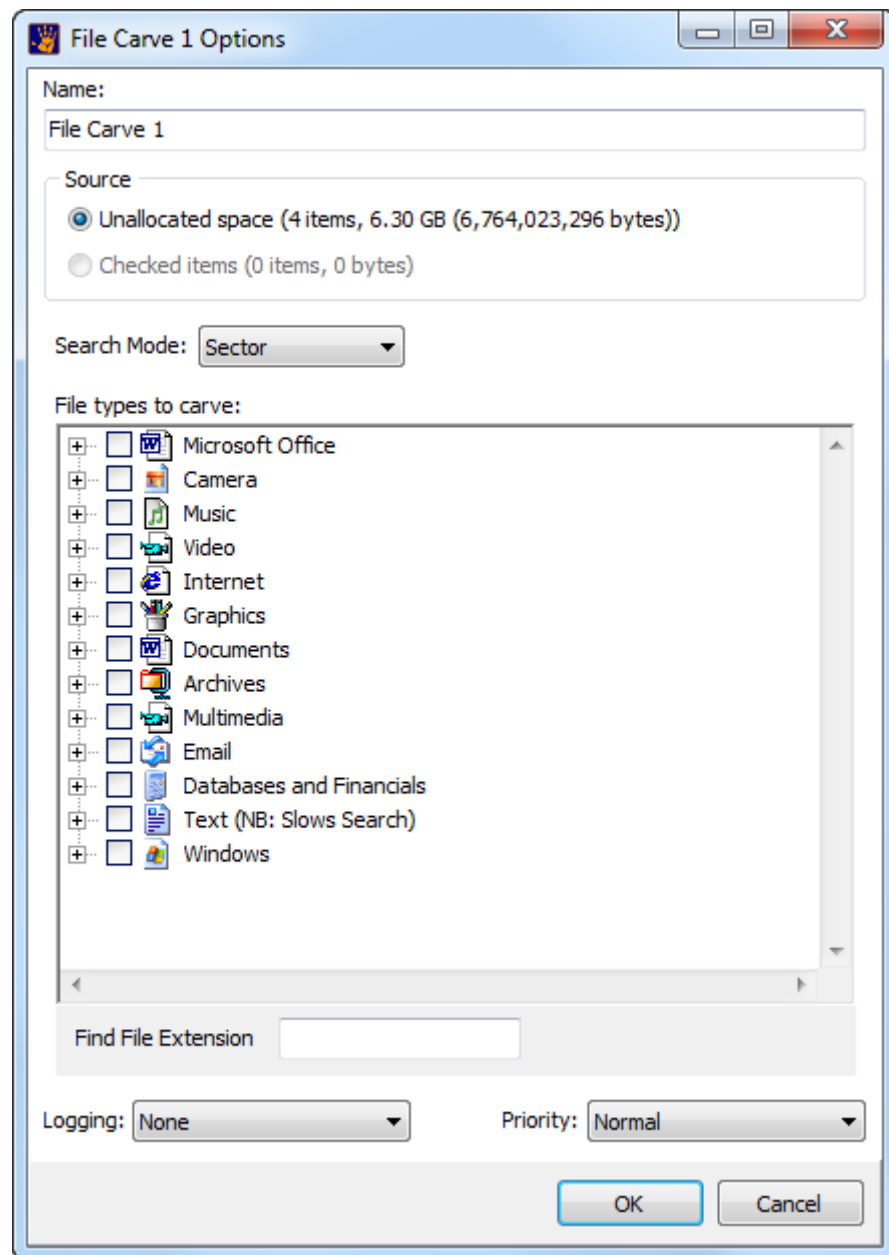
1. Switch to the File System module;
2. Click the File Carve button on the ribbon;

Figure 219, File System module, File Carve button



The "File Carving" selection window, shown in Figure 220 will open:

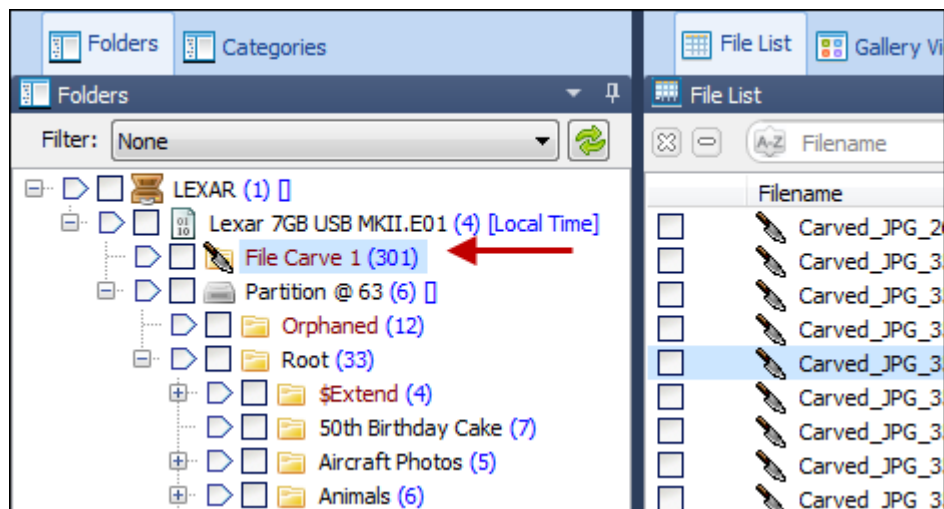
Figure 220, File carving file signature selection window



CARVE NAME

The carve name is the name of the folder which holds the carve results. This folder is displayed in Folders view of the File System module. The default name, "Carve 1" can be edited during setup of the search.

Figure 221, File Carve results



SOURCE

A File Carve is usually run on unallocated space. However it is possible to carve on a specific file, such as the Windows page file, or a backup file, by first checking the file in the File System module and then selecting to carve the checked items.

CARVE SEARCH MODE:

Cluster based file carving

In a cluster based file system like FAT or NTFS a new file must start in a new cluster. It follows then that the file signature appears near a cluster boundary. Carving speed is therefore achieved by searching for file signatures only near cluster boundaries.

Sector based file carving (recommended)

It is recommended to perform a lower level search for sector-aligned file signatures. This search may recover additional files, for example files from a previous volume which had a different cluster layout and is no longer aligned to current cluster boundaries.

NOTE: Carving in sector mode will increase the length of the search.

Byte based file carving

In certain situations it is necessary to data carve at a byte by byte level. This will locate additional files where the file signature is neither aligned with a cluster or sector boundary.

Sector carving is used to recover files from mobile/cell phone image files.

NOTE: Carving in byte mode will greatly increase the length of the search.

SELECTING FILE TYPES TO CARVE

Select the required **file signatures** by placing a tick in the selection box and click **OK** to begin the search.

NOTE: It is recommended that in order to maintain search speed, **no more than 10 file signatures be selected at one time.**

CARVE PROGRESS

The progress of the data carve is shown in the processes window. To stop a data carve click the stop button in this window.

DEFAULT SIZE ALLOCATION

When a file signature of a selected file is located, Forensic Explorer will analyze the file structure in an attempt to locate the end of the file. If the file end is not found, but sufficient information is found within the file to suggest it will at minimum be partially recovered, it is assigned a pre-determined default file size according to that file type.

LOGGING AND PRIORITY

See 7.5 - Process Logging and Priority.

23.4.3 CARVING USING SCRIPTS

The second file carving method available in Forensic Explorer is to use a custom file carving script. An investigator may use, modify or write a script to suit their data recovery needs.

For more information on scripts, please refer to Chapter 18 - Scripts Module.

Chapter 24 - RAID

In This Chapter

CHAPTER 24 - RAID

24.1	RAID - Introduction.....	282
24.2	Preparation.....	282
24.3	Adding a RAID to a case.....	283
24.3.1	Hardware RAID, known configuration:.....	284
24.3.2	Software RAID	285
24.3.3	Once the correct RAID layout is identified	285

24.1 RAID - INTRODUCTION

Forensic Explorer supports the analysis of the following types of RAID:

JBOD

JBOD (Just a Bunch of Disks) is a term to describe the grouping of odd-sized drives into one larger useful drive. For example, a JBOD could combine 3 GB, 15 GB, 5.5 GB, and 12 GB drives into a logical drive at 35.5 GB, which is often more useful than the individual drives separately.

RAID 0

A RAID 0 (also known as a stripe set or striped volume) splits data evenly across two or more disks (striped) with no parity information for redundancy. It is important to note that RAID 0 was not one of the original RAID levels and provides no data redundancy. RAID 0 is normally used to increase performance, although it can also be used as a way to create a small number of large virtual disks out of a large number of small physical ones.

A RAID 0 can be created with disks of differing sizes, but the storage space added to the array by each disk is limited to the size of the smallest disk. For example, if a 120 GB disk is striped together with a 100 GB disk, the size of the array will be 200 GB.

RAID 1

RAID 1 is a mirrored set with parity. Typically, it consists of two physical drives, one being an exact copy of the other. The RAID Array continues to operate so long as at least one drive is functioning. Using RAID 1 with a separate controller for each disk is sometimes called *duplexing*.

RAID 5

A RAID 5 uses block - level striping with parity data distributed across all member disks. Distributed parity means that if a single drive fails the array is not destroyed. Upon a drive failure, any subsequent drive reads can be calculated from the distributed parity of the functioning drives. A single drive failure in the set will result in reduced performance of the entire set until the failed drive has been replaced and rebuilt.

24.2 PREPARATION

When dealing with RAID drives, care should be taken in the forensic acquisition phase to document as much information as possible as to the RAID configuration.

Successful RAID setup in Forensic Explorer will be assisted by knowledge of the following:

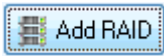
- Is it a hardware or software RAID? (A hardware RAID usually has a separate RAID controller card);
- What is the RAID format, JBOD, RAID 0, 1, 5, other? (Are the drives in the raid identical in size and capacity? This information may be obtained from the system administrator or setup documentation).
- What is the RAID stripe size? (this information may be determined from the RAID controller)
- How many physical disks make up the RAID?
- What is the sequence of the physical disks in the RAID? (Noting or photograph the RAID controller port numbers may assist to determine drive sequence).
- Is the RAID complete and functioning? Are there missing drives?

24.3 ADDING A RAID TO A CASE

A RAID can be constructed and added to Forensic Explorer using:

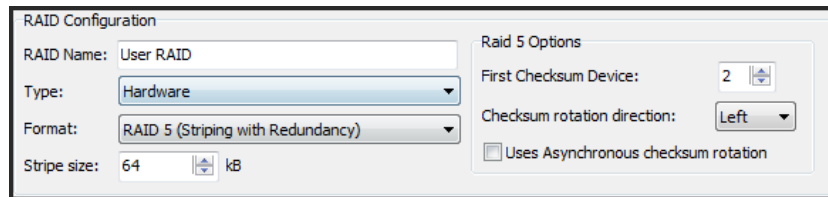
1. Physical disks (Note: When using physical disks a hardware write blocking device is recommended to preserve forensic integrity);
2. Forensic Image Files; or,
3. A combination of both physical disks and forensic image files.

To add a RAID drive to a case:

1. Click the button to add a device to the current case.
2. In the Device Selection window, click on the  button. This opens the RAID configuration window.

24.3.1 HARDWARE RAID, KNOWN CONFIGURATION:

Enter the RAID configuration information:



and follow the instructions to add and test the RAID:

HARDWARE RAID, UNKNOWN CONFIGURATION:

If you do NOT know the parameters of your hardware RAID drive, Forensic Explorer will attempt to identify the way in which the RAID was configured. To do this:

1. Set the RAID type to "**hardware**";
2. **Add the drives (or image files) in the correct sequence**, or, if the correct sequence is unknown, add them in the order that is believe to be most correct;
3. Click on the "**Find Layout**" button to find a suggested configuration. A suggested configuration is indicated by a **green tick** next to each added drive.

Important:

A suggested configuration is based on the information available from the drives. However, due to the complexity of a RAID structure, there may be more than one configuration that returns this result. A suggested configuration should be tested by adding the image to the case to determine if individual files can be accessed and previewed.

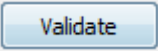
**If Find Layout did not return a suggested configuration, or,
The suggested configuration did not result in a successful recovery;**



If the Find Layout button did not return green ticks for each added drive, or the continued recovery from a suggested configuration did not work, try the following:

1. click on the "Probable Solutions" tab to view suggested configurations for the RAID;
2. change the "stripe size", RAID Options and drive sequence as suggested;
3. click the "Test Layout" button to test the modified configuration;
4. add the RAID drive to the case.

24.3.2 SOFTWARE RAID

If it is a software RAID:

1. Set the "Type" of RAID to "software".
2. Press  to confirm a valid software RAID. A valid software RAID will show with green ticks on the added drives (or image files):

Raid Segments			Probable Solutions	Event Log
Name	#	Size		
 S/W -C:\Users\Graham\Desktop\RAID\SW_0_b...	0	74.53 GB		
 S/W -C:\Users\Graham\Desktop\RAID\SW_0_a...	1	74.53 GB		

24.3.3 ONCE THE CORRECT RAID LAYOUT IS IDENTIFIED

Once the correct RAID layout has been identified, click **OK** to add the configured RAID drive to the Device Selection window.



Select the **RAID drive** and click **OK** to add the drive to the case.

Once the RAID drive is added, select and preview individual files to ensure that the RAID drive is correctly configured and access to all files in the RAID has been achieved.

Chapter 25 – Shadow Copy

In This Chapter

CHAPTER 25 – SHADOW COPY

25.1	Shadow Copy Introduction	288
25.1.1	Shadow Copy Configuration by WindowsUsers	288
25.1.2	When are Shadow Copies created?.....	291
25.1.3	Where are Shadow Copies Stored.....	292
25.2	Examining Shadow Copies With Forensic Explorer	293

25.1 SHADOW COPY INTRODUCTION

The ability of Forensic Explorer to easily access and explorer Volume Shadow Copies (VSCs) offers the forensics investigator the ability to examine data at different time snapshots in a forensic examination. A Shadow Copy is essentially a differential backup of the contents of a drive. By examining a Shadow Copy it can be possible to view previous versions of a file, a directory, or a volume.

Prior to Windows Vista, “Restore Points” were a relatively simple snapshot of critical Windows system files. In Windows Vista and beyond, the Volume Shadow Copy Service (VSS) takes a snapshot of all files on the volume that has changed, including user files.

VSS is present on:

- Windows Server 2003
- Windows Vista (all versions)
- Windows Server 2008
- Windows 7 (all versions)

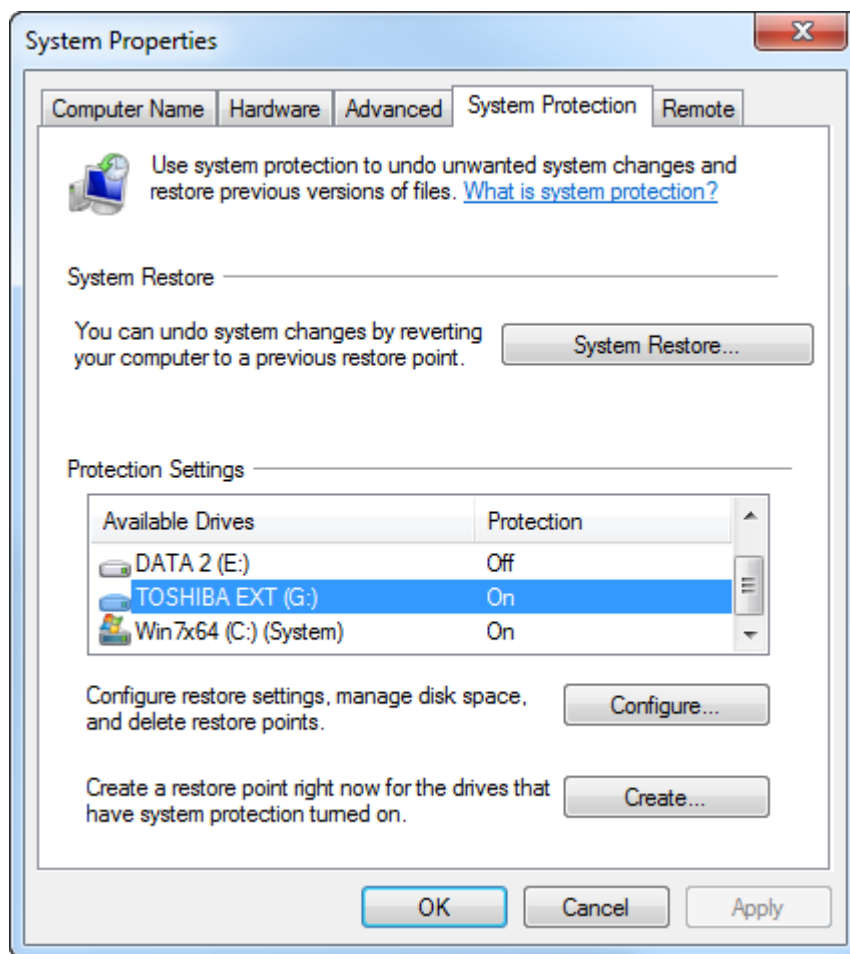
25.1.1 SHADOW COPY CONFIGURATION BY WINDOWSUSERS

Windows VSC controls are accessed via:

“Control Panel\All Control Panel Items\System\System Protection”.

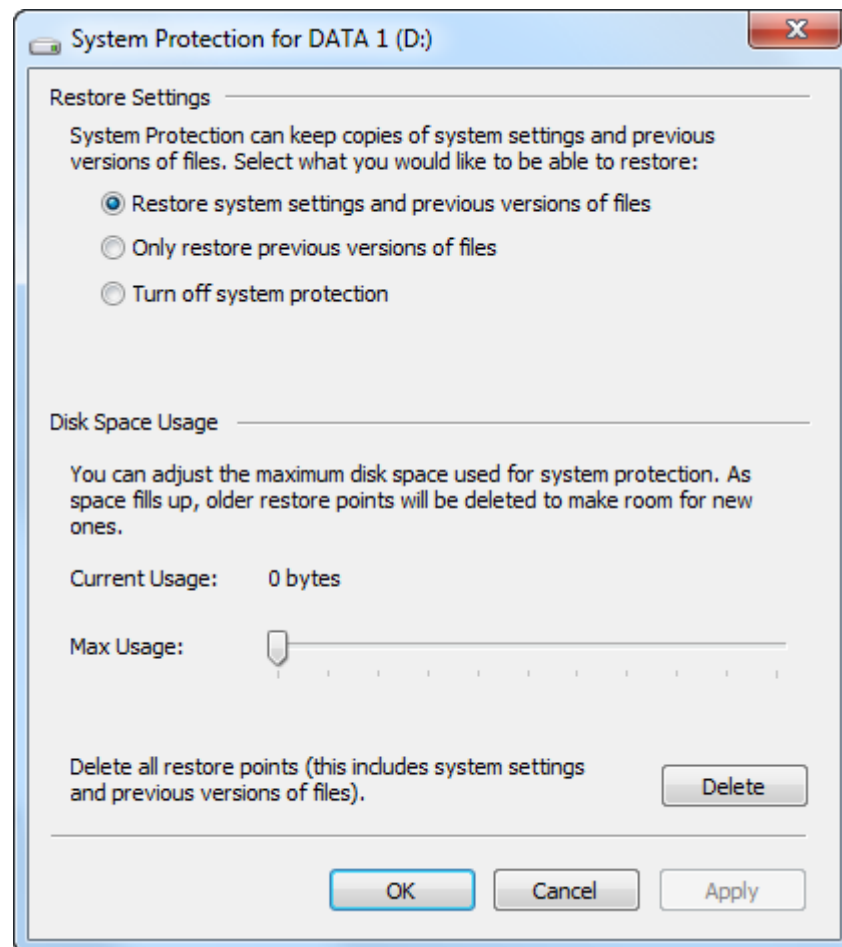
VSC is activated on an NTFS drive by turning on the Protections Settings in the System Properties windows. Shadow Copies can be created on local or removable media. The System Properties window (Win 7) is shown in Figure 222 below:

Figure 222, System Properties, Protection Settings



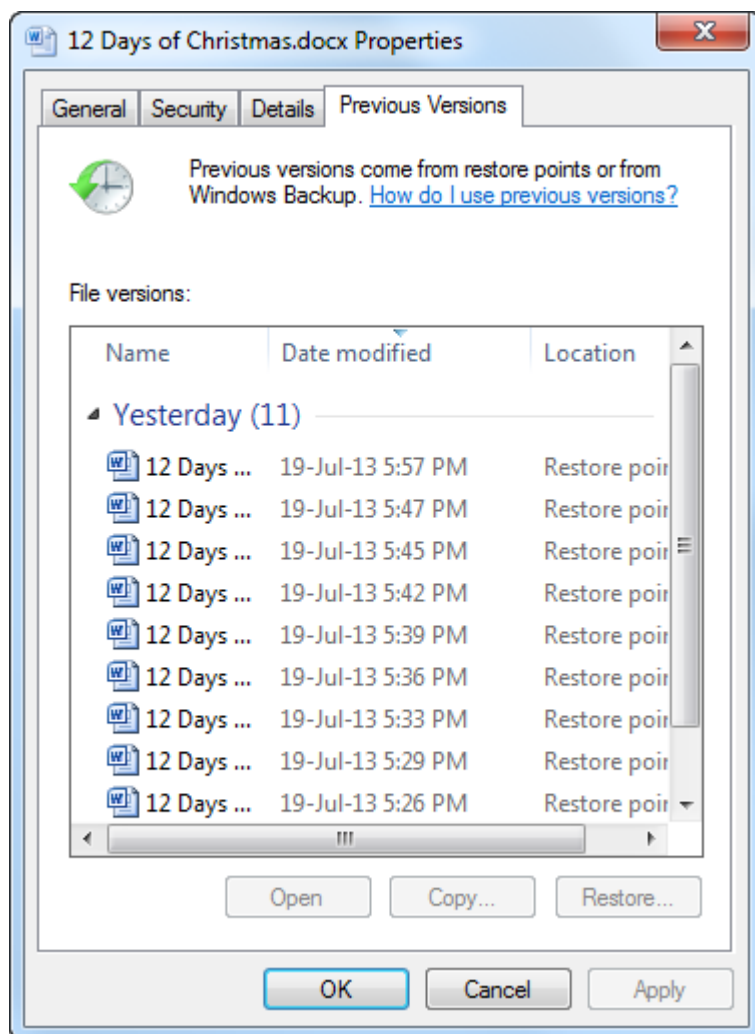
The configure button gives access to further settings. The lowest setting is to “**Only restore previous versions of files**”, with the option to “**Restore system settings and previous version of files**”. This is shown in Figure 223 below:

Figure 223, System Protection Settings



When VSC is active on a volume, a Windows user can right click on any file in Windows, select the **Properties** options for that file, and then access the **Previous Versions** tab, shown in Figure 224 below:

Figure 224, Windows file properties, Previous Versions



It is the ability to extract previous file versions which is of clear value to the investigator. It is possible, for example, that even though a file has been deleted and erased from the current file system (with no trace of the file in unallocated clusters), that a version of the file prior to its deletion could be contained within a VSC on the system.

25.1.2 WHEN ARE SHADOW COPIES CREATED?

The frequency of VSC creation will depend on the Operating System installed. Typically they are automatically created daily in Vista, and weekly in Windows 7. VFCs can also be automatically created prior to significant Windows Operating System events, such as the installation of new software, including Windows updates.

In addition to this, many commercial applications such as registry optimization software offer the ability to create a system restore point (for backup purposes) prior to making disk changes. An end user can also manually create a VFC from the

Windows System Properties > System Protection > “Create” button, shown in Figure 222 below.

25.1.3 WHERE ARE SHADOW COPIES STORED

Shadow Copies are stored in the hidden folder “**Partition\Root\System Volume Information**” on the volume on which the “Protection Settings” are enabled.

The “**System Volume Information**” folder contains:

- a **VSS Catalog** file called {3808876b-c176-4e48-b7ae-04046e6cc752} , a unique identifier specific to VSS;
- **VSS Store** files (the files which contain the actual shadow copy data) which have names like:

{c678aea6-f000-11e2-93bf-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}.

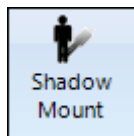
(Note that the VSS identifier is attached to the Store name in the second set of braces).

25.2 EXAMINING SHADOW COPIES WITH FORENSIC EXPLORER

To **mount a Volume Shadow Copy (VSC)** in Forensic Explorer;

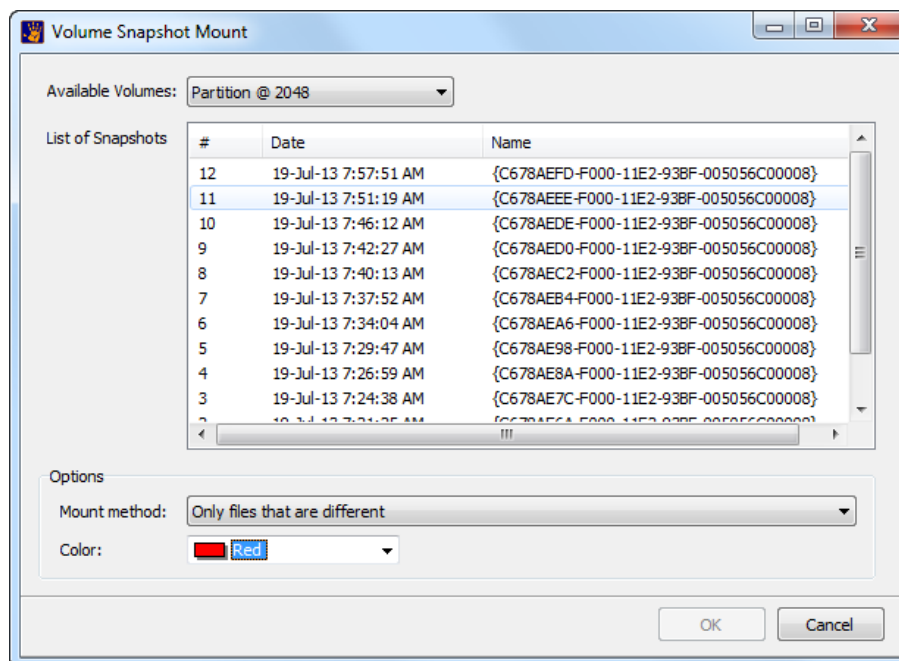
1. In the Forensic Explorer Evidence module, start a preview, a new case, or load an existing case;
2. Switch to the File System module to view the files in the case;
3. Click on the **Shadow Mount** button in the **File System module toolbar**:

Figure 225, Shadow Mount button in the File System Toolbar



4. The Forensic Explorer Volume Snapshot Mount window will open and list the available VSCs for the selected volume, as shown in Figure 226 below:

Figure 226, Volume Snapshot Mount Window



Available Volumes:

Enables another volume and its shadow copies to be accessed.

Mount Method:


Only files that are different displays only those files in the VSC which are different from that listed in the current file system. This saves the investigator cluttering the File System module with duplicate identical files from the VSC.

All Files mounts the entire Shadow Copy.

Color:

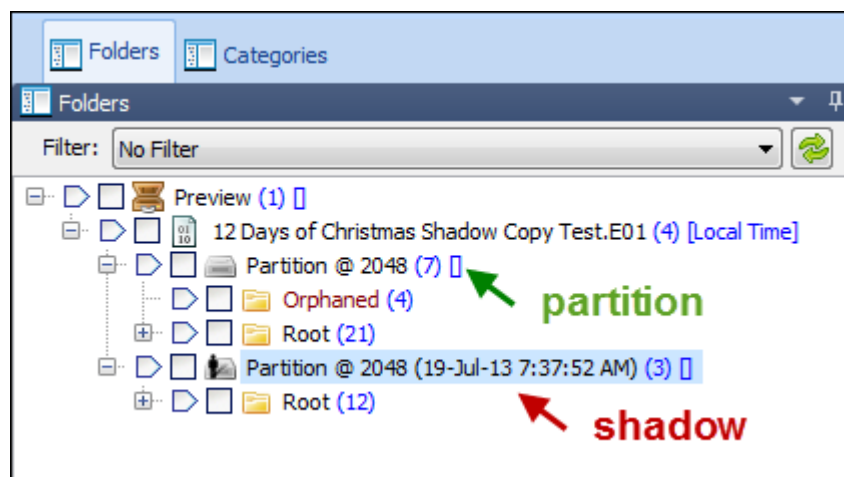
Assigns a color to the mounted VSS. If a color is selected, a new column is created in the File System module called "VSS". The columns contains the selected color to identify the origin of the file.

5. In the Volume Snapshot Mount window, **click on the required snapshot** (identified by the date created) and click **OK**. The Shadow Copy is then processed (the process status is shown in the process window in the bottom right hand corner of Forensic Explorer) and the VSC files added to the File System module.

 Added VSC volumes are identified by the shadow mount icon in the Folders window of the File System module.

The VSC volume name includes the date and time of the snapshot, as shown in below Figure 227 below:

Figure 227, File System module showing a mounted shadow copy



When a VSS has been added to the File System module, four new columns become available:

- **VSS** – Contains the color assigned to the shadow copy volume during the mount process (if a color has been assigned, this column is automatically added to the File System module at position 2);

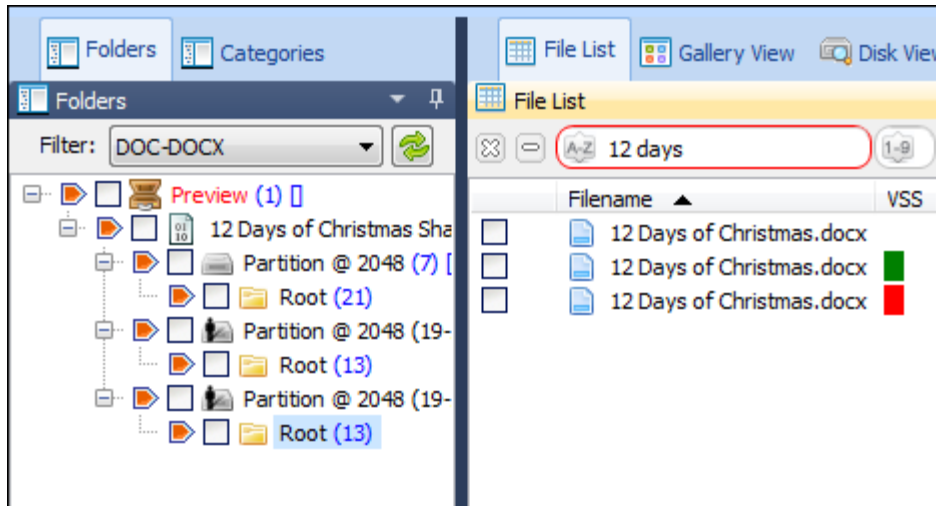
The following columns can be manually added (Right Click > Columns > Edit Columns);

- **VSS Date** – The date of creation of the VSS;
- **VSS GUID** – The Windows GUID assigned to the VSS, e.g. {C678AE98-F000-11E2-93BF-005056C00008}

- **VSS ID** – The VSS snapshot ID.

To best examine different version of a single file a combination of the Folders Filter (see 9.11.4), the Branch Plate (see 8.2.3), and the text filter tool (see 9.11.2) can be used, as shown below:

Figure 228, Filtering Different Versions of the same file – shows original and two VSS versions (green and red)



Once a VSC is mounted in the File System module, it is possible to operate on it like as you would a normal volume, including keyword search, indexing etc.

Chapter 26 - Mount Image Pro

In This Chapter

CHAPTER 26 – MOUNT IMAGE PRO

26.1	Mount Image Pro.....	298
26.1.1	Install and run Mount Image Pro.....	298

26.1 MOUNT IMAGE PRO

You Wibu dongle purchased with Forensic Explorer also contain a license key for **Mount Image Pro v5**.

Mount Image Pro is software used to 'mount' forensic image files as a drive letter or physical drive on your forensic workstation. This allows users to:

- Browse the contents of an image file in programs such as Windows Explorer;
- Run third party applications, such as virus scanners, spyware scanners, cache analyzers etc. over the mounted evidence files;
- Run third party programs on the physical drive, such as Virtual Forensic Computing (www.virtualforensiccomputing.com), used to boot an image of a Windows file system in a virtual environment.

Once an image is mounted, these actions are ready only and "forensically secure", as the contents of the image file will not be changed.

26.1.1 INSTALL AND RUN MOUNT IMAGE PRO

Mount Image Pro v5 is a stand-alone application available for download from www.mountimage.com or <http://download.getdata.com/MIP-Setup.exe> (**Note:** Your Forensic Explorer dongle will NOT activate Mount Image Pro versions prior to version 5).

Download and run the setup file and follow the onscreen installation instructions.

Run Mount Image Pro v5 from the desktop icon. Ensure that the dongle is inserted to activate the product (when activated the red "buy online" button will not show in the program tool bar).

To mount an image file;

1. Click the mount button in the program toolbar;
2. In the "Drive Selection" window, select the image file or physical device to mount (If the image file is not listed, click the "Add Image" button and select and add the image to the available devices list). Then click the Mount Disk, or Mount File System button.

Mount Disk:

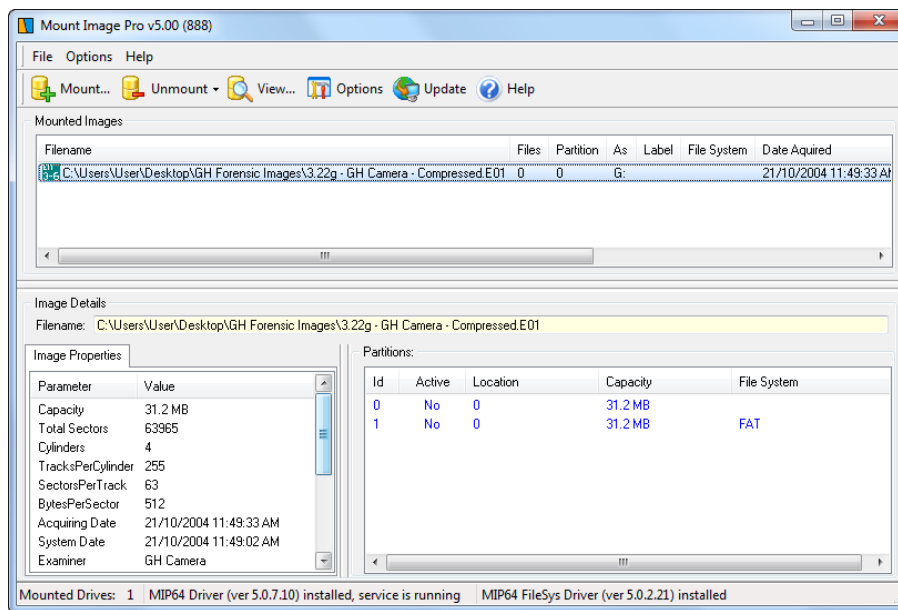
The Mount Disk option is used to Mount an image file and display the physical disk and / or partitions as if the physical drive were connected to the local computer. Windows is responsible for reading the file system and displaying the files.

Mount File System:

The Mount Filesystem button mounts the selected image or disk and uses the Mount Image Pro Version 5 Filesystem Driver (not Microsoft windows) to display the file system. This allows additional information to be displayed within the mounted image, including deleted files and Windows system files.

The Mount Image Pro GUI displays the image details and the assigned drive letter, as show in Figure 229 below:

Figure 229, Mount Image Pro v5 GUI



Mount Image Pro v5 has numerous other features, including:

- Mount as read only or simulate disk writes
- Mount the physical drives into Windows disk management
- Mount from the command line
- Mount logical image files from created by EnCase® and FTK.

These features are more fully described at www.mountiamge.com and in the support documentation for the product.

Chapter 27 – Live Boot

In This Chapter

CHAPTER 27 – LIVE BOOT

27.1	Live Boot	302
27.2	Requirements	302
27.3	Compatibility	304
27.4	Live Boot Working Folder	304
27.5	How to Live Boot a Forensic Image	305
27.5.1	Installing VMWare Tools	308
27.6	Live Boot and Windows User Passwords.....	310
27.6.1	Windows User Password Recovery	310

27.1 LIVE BOOT

Forensic Explorer **Live Boot** enables an investigator to boot a forensic image or write-protected physical hard drive containing a Windows Operating System. The investigator can then operate the computer in a forensically sound virtual environment.

Utilizing Live Boot as part of a forensic examination can give insight into computer use that may not be as readily evident when examining file system records alone. For example, viewing the desktop, icon layout, menus, and running installed software, is a fast and effective way to quickly profile computer use.

Live Boot also offers a compelling means of presenting digital evidence to a client, prosecutor, or court. To demonstrate a live running computer can be effective mean of conveying complex evidence in a way that is easily understood.

27.2 REQUIREMENTS

Live Boot has the following requirements:

Forensic Explorer Full Version (Dongle Activated)

Live Boot requires a full dongle version of Forensic Explorer. Live Boot will not run in the Forensic Explorer evaluation edition.

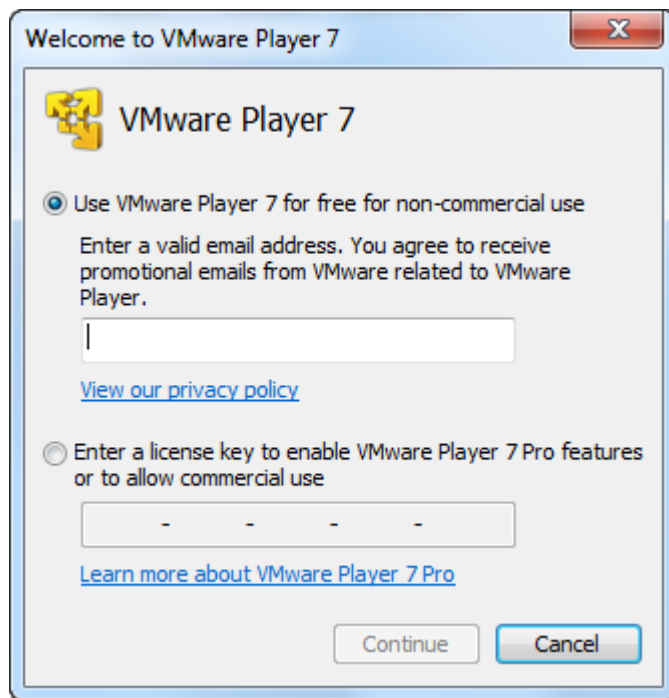
VMWare Workstation or VMWare Player

One of the following VMWare products must be installed:

- **VMWare workstation**
<http://www.vmware.com/products/workstation/>; or,
- **VMWare Player** (free for non-commercial use)
https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/6_0.

NOTE: If you are installing **VMWare Player** (for non-commercial use) you must run VMWare Player and agree to the terms and conditions, shown below, before running Live Boot:

Figure 230, VMWare Player Terms



- **VMWare Player Plus**
<http://www.vmware.com/products/player/>.

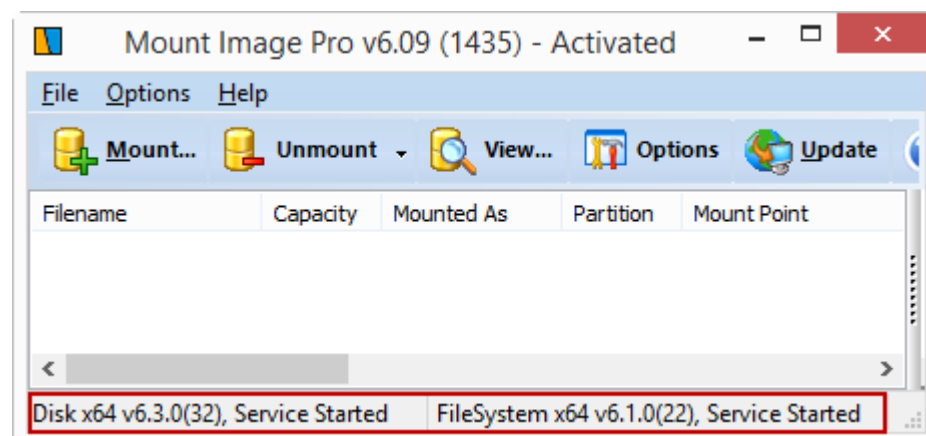
Mount Image Pro v6

GetData's Mount Image Pro is used to mount a forensic image to make it accessible to Live Boot and VMWare. A purchase of Forensic Explorer includes a license for Mount Image Pro. The latest version of Mount Image Pro is available at:

- www.mountimage.com; or,
- <http://download.getdata.com/MountImagePro-Setup.exe>

NOTE: When installing Mount Image Pro v6 for the first time, a reboot is required. Ensure that when Mount Image Pro starts, both the Disk and FileSystem drivers show a 'Service Started' status, as shown Figure 231, below;

Figure 231, Mount Image Pro v6 driver status



27.3 COMPATIBILITY

Forensic Image Files

Live Boot requires a forensic image of a physical device that contains a bootable file system (Live boot does not support the booting of logically acquired partitions).

Supported Target Operating Systems

Live Boot will boot the following Operating Systems:

- Windows 95;
- Windows 98;
- Windows XP;
- Windows Vista;
- Windows 7;
- Windows 8 (including GPT partitioned drives).

NOT currently supported:

- Macintosh HFS.

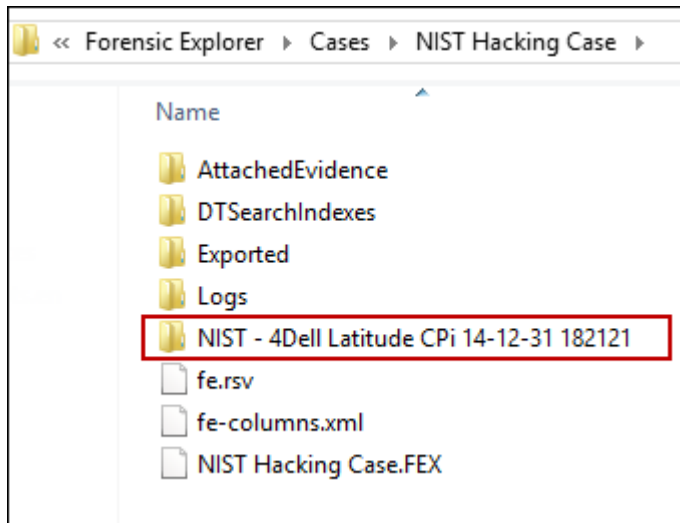
27.4 LIVE BOOT WORKING FOLDER

IMPORTANT: Live Boot requires a working folder to store the Mount Image Pro disk cache and VMWare working files. Each time a Live Boot VMWare session is started a working folder is created in the root of the current case path, in the format:

[user]\Documents\Forensic Explorer\Cases\[Case Name]\[Boot Image Name + Date Time stamp]

As shown below:

Figure 232, Current Case folder showing Live Boot working folder



The data for each Live Boot session is retained to enable the re-open in VMWare of a Live Boot session at a specific point in time. If individual sessions are no longer required they can be deleted.

27.5 HOW TO LIVE BOOT A FORENSIC IMAGE

The following steps describe how to use Live Boot to boot a forensic image. In this example an E01 file from the 'NIST Hacking Case' is used (http://www.cfreds.nist.gov/Hacking_Case.html).

1. Check installed software

Ensure that all required software is installed (as detailed in section 27.2 above).

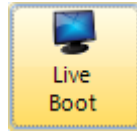
2. Start a Forensic Explorer case

- a. Run Forensic Explorer and start a Preview or Case.

Add a forensic image file of a Windows disk to the preview or case.

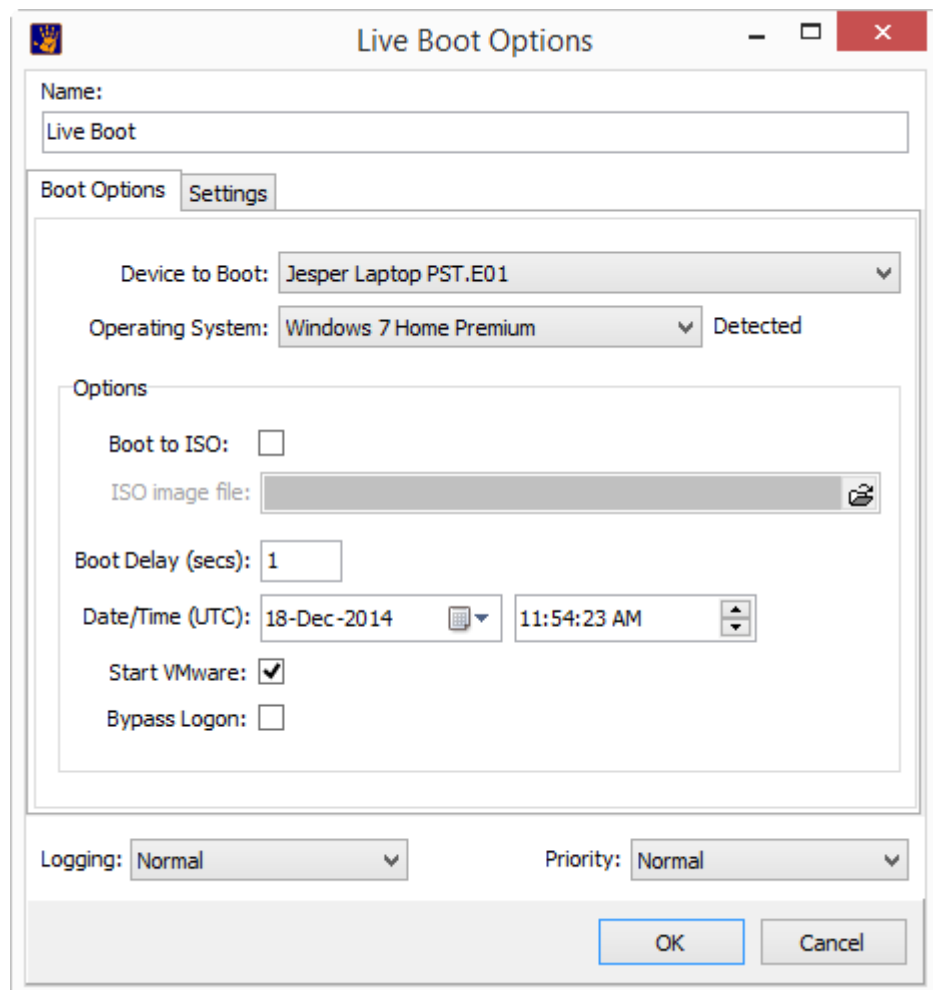
3. Run Live Boot

- a. To run Live Boot, In the Forensic Explorer File System module click on the Live Boot button in the toolbar:



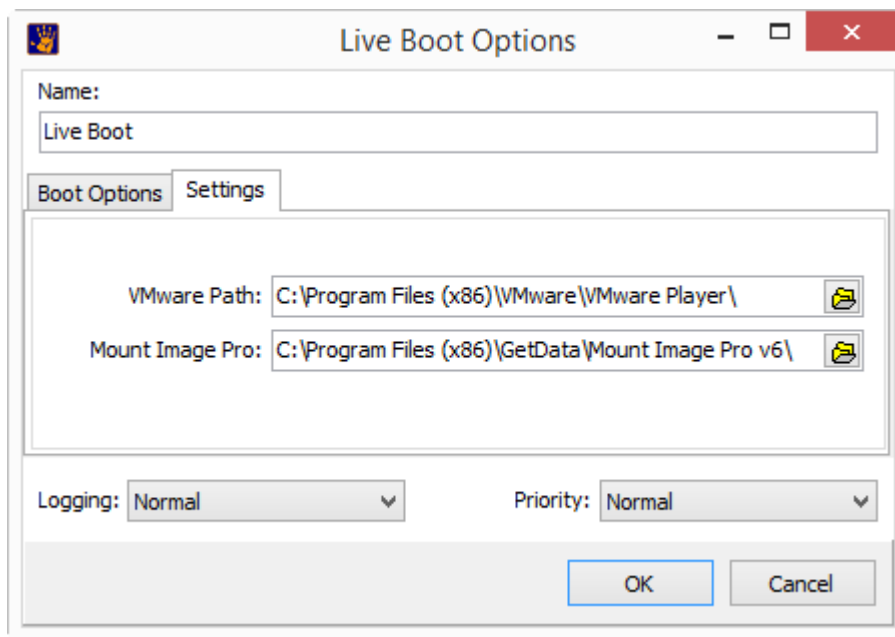
The Live Boot Options window will display:

Figure 233, Live Boot Options



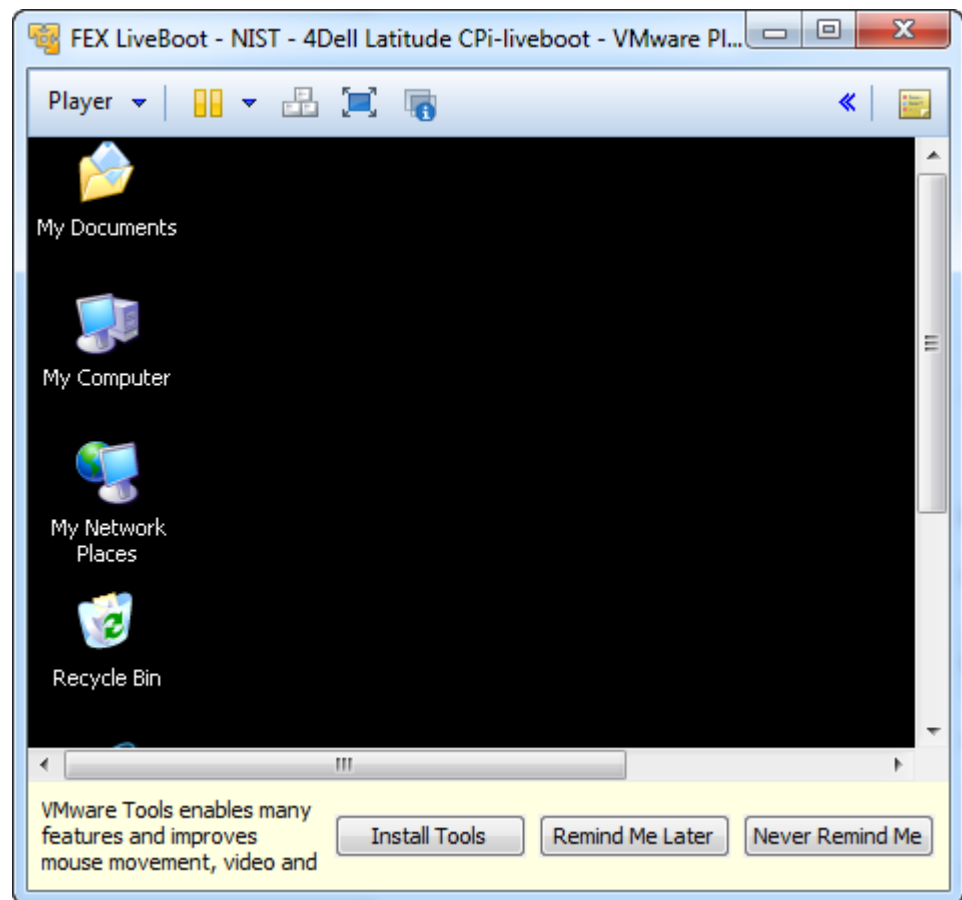
- b. Ensure that '**Device to Boot**' contains the required image.
- c. Switch from the Boot Options tab to the **Settings** tab:

Figure 234, Live Boot Options



- d. Ensure that the paths to **VMWare** and **Mount Image Pro v6** are correct.
- e. Click **OK** to proceed with the boot.
- f. Information about the boot process is displayed in the process window. The VMWare GUI will then launch and the forensic image will boot, as shown in Figure 235 below:

Figure 235, Live Boot VMWare Screen



To switch the mouse between the virtual machine and the desktop, use the **CTRL – ALT** keys. A quick start guide for virtual machines is available at:

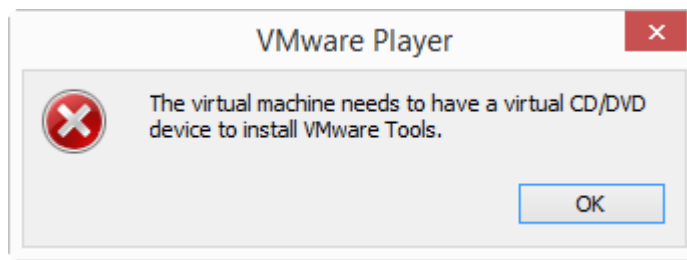
<http://www.vmware.com/pdf/desktop/ws10-getting-started.pdf>

27.5.1 INSTALLING VMWARE TOOLS

VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system. It also improves management of the virtual machine by allowing such options as the transfer of data into or out of the virtual machine.

To install VMware Tools, click on the **Install Tools** button shown in Figure 235 above. If you receive the following VMware error message::

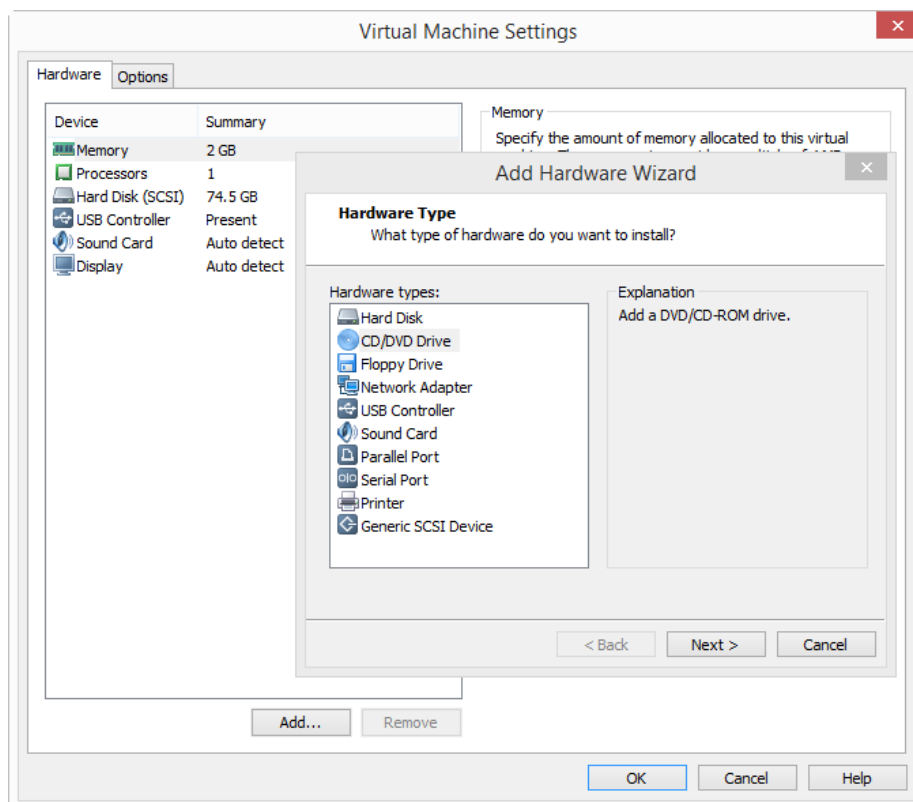
Figure 236, VMWare Tools virtual CD/DVD error



To **enable** the **virtual CD/DVD**:

1. Shut down Windows virtual machine inside the VMWare window;
2. In VMWare window, select the required VMWare session, right click and select **settings**. The Virtual Machine Settings window will open.
3. Click **Add** to add a virtual device and select **CD/DVD Drive** from the Hardware Type menu:

Figure 237, Virtual Machine Settings



4. Restart the virtual machine, and click on the **Install** button to install VMWare Tools.

27.6 LIVE BOOT AND WINDOWS USER PASSWORDS

In many cases when Windows starts in Live Boot access to the virtual computer will be blocked by the Windows user account login screen. If passwords for the user accounts are unknown, there are two options:

1. Password recovery; or
2. Password bypass.

Described in more detail below.

27.6.1 WINDOWS USER PASSWORD RECOVERY

The advantages of password recovery are:

1. A known password may be of evidentiary value to a case. For example, a unique password may tie an individual to a computer.
2. A known password may assist in other avenues of investigation. For example, the password may be used in the decryption user files.

The disadvantages of password recovery are:

1. Password recovery requires the use of third-party software.
2. Password recovery can be resource and time intensive.
3. Strong passwords may not be recovered.

OPHCRACK

Ophcrack is a free open source program that recovers Windows passwords by processing LM hashes through rainbow tables (see <http://en.wikipedia.org/wiki/Ophcrack>). Ophcrack can be used to recover passwords from Win XP, Vista, Win7 and Win8 operating systems.

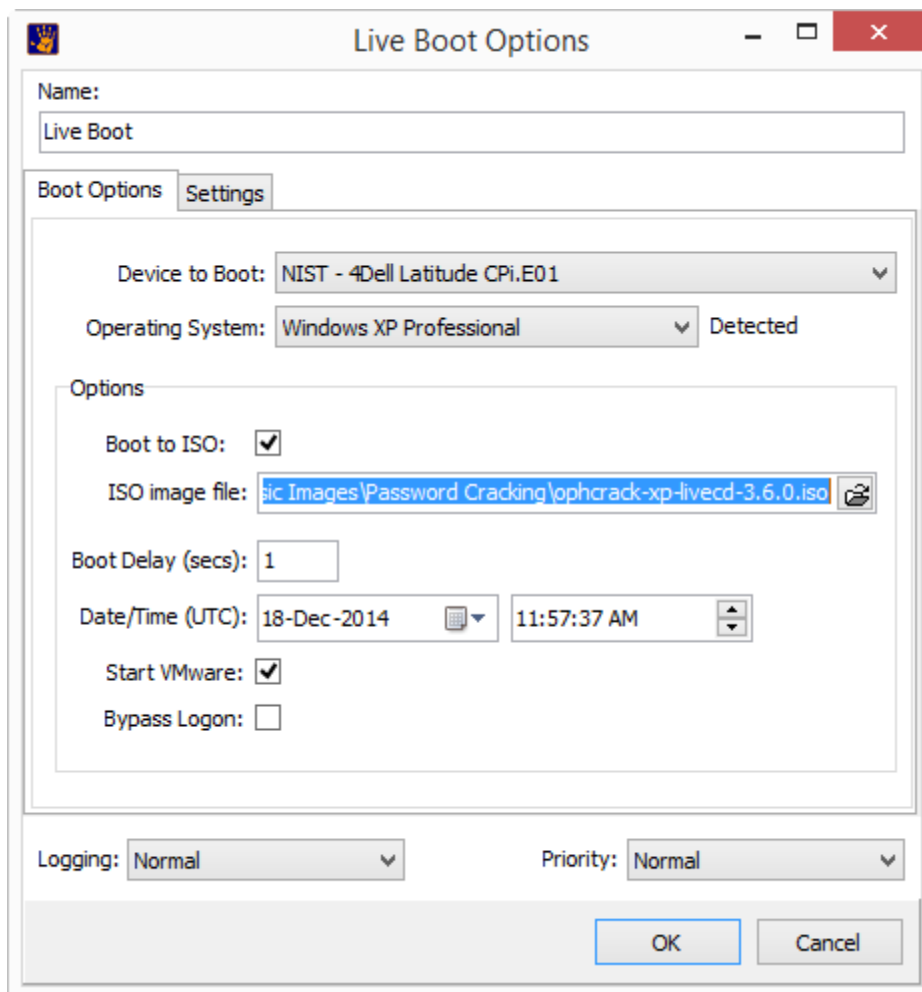
Ophcrack ISO image files are available for download from <http://Ophcrack.sourceforge.net/download.php>. These include:

- Ophcrack-xp-livecd-3.6.0.iso (for LM hashes of Windows XP and earlier);
- Ophcrack-vista-livecd-3.6.0.iso (for NT hashes of Windows Vista and 7).

To recover a password with Ophcrack:

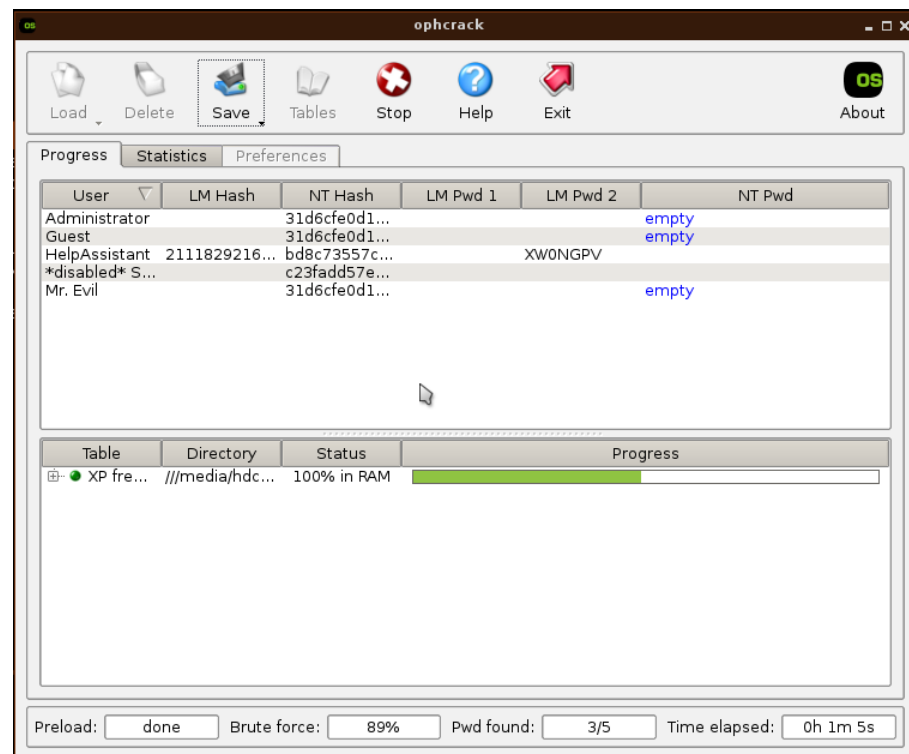
- a. Follow the instructions provided in 0 above to mount the image file and run Live Boot.
- b. In the Boot Options tab, check 'Boot to ISO' and select the relevant Ophcrack ISO image, as shown in Figure 238 below:

Figure 238, Live Boot ISO



- c. Click OK to launch Ophcrack in VMWare.
- d. Follow the on-screen Ophcrack prompts to commence the password breaking process, as shown in Figure 239 below:

Figure 239, Ophcrack Password Breaking



Once the required password is recovered, close the virtual machine and re-launch Live Boot without the ISO boot option checked. When presented with the Windows login screen, enter the recovered password to proceed.

27.6.2 WINDOWS USER PASSWORD BYPASS

Password bypass patches the forensic image in VMware to blank user passwords. Select the **Bypass Logon** checkbox in the Live Boot Options window. At the Windows login screen, login with a blank password.

27.7 TROUBLESHOOTING LIVE BOOT

Following the checks below to troubleshoot Live Boot:

27.7.1 LIVE BOOT A NIST CONTROL IMAGE

Can you Live Boot a NIST control image successfully?

- Download and boot the NIST “Hacking Case” EnCase image available at: http://www.cfreds.nist.gov/Hacking_Case.html. This image boots to Windows XP. A successful boot will assist you to determine if the error relates to the **configuration of Live Boot** or the **image that you attempting to boot**.

27.7.2 LIVE BOOT CONFIGURATION

Is VMWare Player or VMWare Workstation installed?

- Check Live Boot Options (shown in Figure 234, Live Boot Options above) to confirm the correct path to the VMWare executable file (64bit paths are shown below):
 - **VMPlayer:** C:\Program Files (x86)\VMware\VMware Player\vmplayer.exe; OR
 - **VMWorkstation:** C:\Program Files (x86)\...

Is Mount Image Pro v6 installed? (Live Boot is not compatible with earlier versions);

- Check Live Boot Options (shown in Figure 234 above) to confirm the correct path to MIPv6:
 - C:\Program Files (x86)\GetData\Mount Image Pro v6\MIP.exe (64bit path shown).

27.7.3 MOUNT IMAGE PRO CHECKS

Mount Image Pro Cache and VMWare Files

- Locate and delete the Live Boot working folder and then try again. The Live Boot working folder is in the following path:

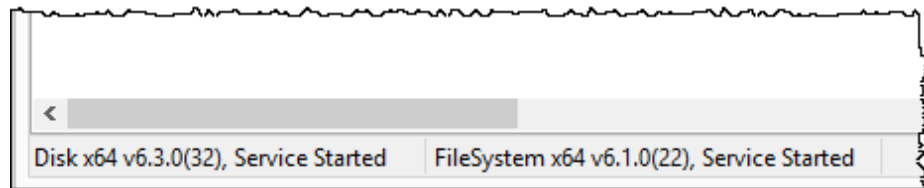
[user]\Documents\Forensic Explorer\Cases\[Case Name]\[Boot Image Name + Date Time stamp].

Does the Image mount independently in Mount Image Pro v6?

- Run Mount Image Pro v6 as a stand-alone program;
 - Ensure that Mount Image Pro is activated;

- Ensure that Mount image Pro drivers are correctly installed, as shown in Figure 240 below:

Figure 240, Mount Image Pro drivers



- Manually mount the required image in Mount Image Pro using: Mount Disk; PNP; Write to Cache. Confirm that the image mounts successfully.

Does the image that you are trying to boot contain a valid Windows File System?

- In the Forensic Explorer File System module, examine the file and folder structure to confirm that the image has a valid bootable Windows file system. Check that this folder is also accessible in the mounted image.
- NOTE: Live Boot does not currently support Windows 8 GPT.

27.7.4 CONTACT TECHNICAL SUPPORT

Contact technical support (see Appendix 1 - Technical Support) with the supporting information from the above checks.

Chapter 28 – Working with ...

In This Chapter

CHAPTER 28 – WORKING WITH ...

28.1	iTunes Backups	316
28.1.1	Locating Apple UUID Backup Folders	316
28.1.2	iTunes Backups - Identify and Bookmark	317
28.1.3	Manually Examining iTunes Backup Files	320
28.1.4	iTunes Backups – Analyze (Scripts).....	321
28.2	Thumbnails	326
28.2.1	Thumbs.db.....	326
28.2.2	Thumbcache	326
28.2.3	Forensic Value of Thumbnails	326

28.1 ITUNES BACKUPS

When an Apple device (iPhone, iPad, iPod) is connected to a computer for the first time and synced with iTunes, a folder is created using the unique device ID (**UUID**). These iTunes Backup folders are very distinctive, in that they are **40 hexadecimal characters long**. The default folder locations are:

Figure 241, iTunes Backup paths

Windows 7	C:\Users\[username]\AppData\Roaming\Apple Computer\MobileSync\Backup\
Windows XP	C:\Documents and Settings\username\Application Files\MobileSync\Backup\deviceid
MAC OS X	[User HomeDirectory]/Library/Application Support/MobileSync/Backup

iTunes Backup UUID folders can contain high value information for the forensic investigator, particularly if the original device itself cannot be located. Each time an Apple device is synced with a computer, the UUID backup folder will store configuration information, address book data, SMS database, call records, the camera photo cache, and other types of personal data.

Apple device analysis is well documented. Suggested reference material includes:

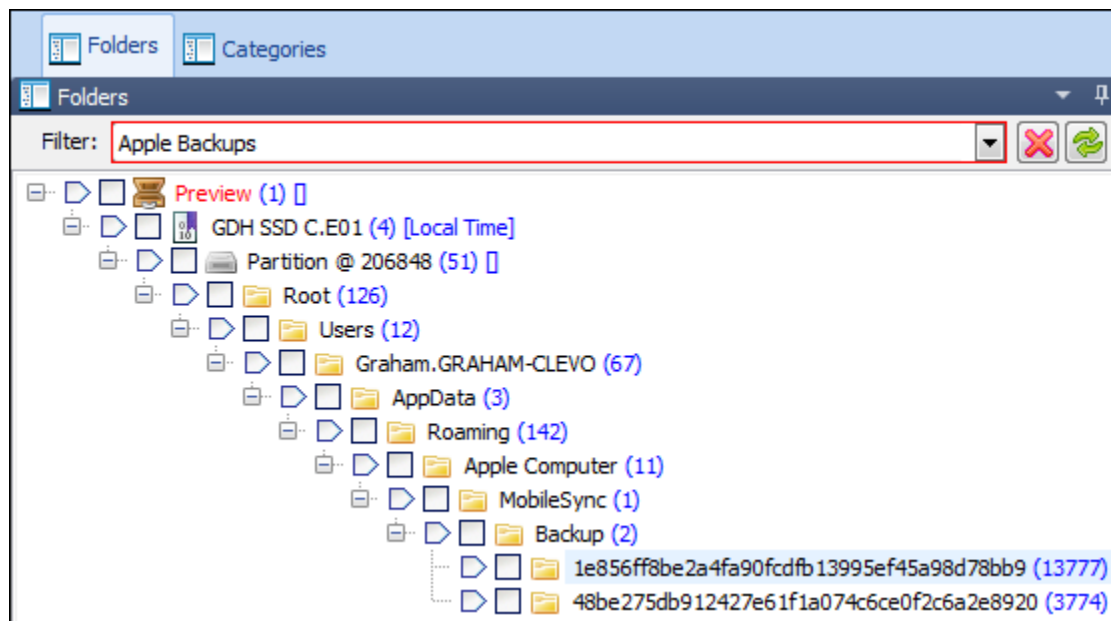
- iOS Forensic Analysis for iPhone, iPad and iPod Touch, Sean Morrissey, 2010, Apress;
- iPhone Forensics, 1st Edition, Jonathan Zdziarski, 2008, O'Reilly Media Inc.

This section is provided only as a guide to process iTunes Backup files with Forensic Explorer and is not a complete IOS analysis resource.

28.1.1 LOCATING APPLE UUID BACKUP FOLDERS

iTunes Backup UUID folders can be located in the Forensic Explorer File System module by using the “Apple Backups” folders filter, as shown in Figure 242 below:

Figure 242, iTunes Backups filter applied in the File System module (two backup devices shown)



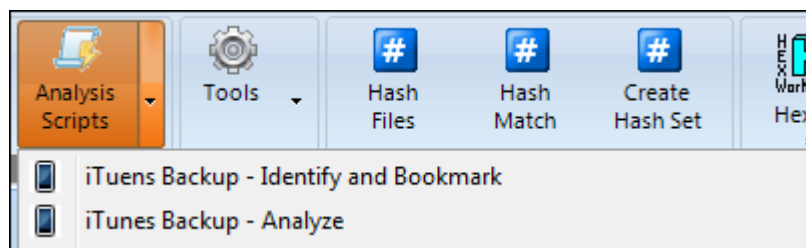
28.1.2 ITUNES BACKUPS - IDENTIFY AND BOOKMARK

The first step to analyze iTunes Backups in Forensic Explorer is to identify and bookmark the UUID folders.

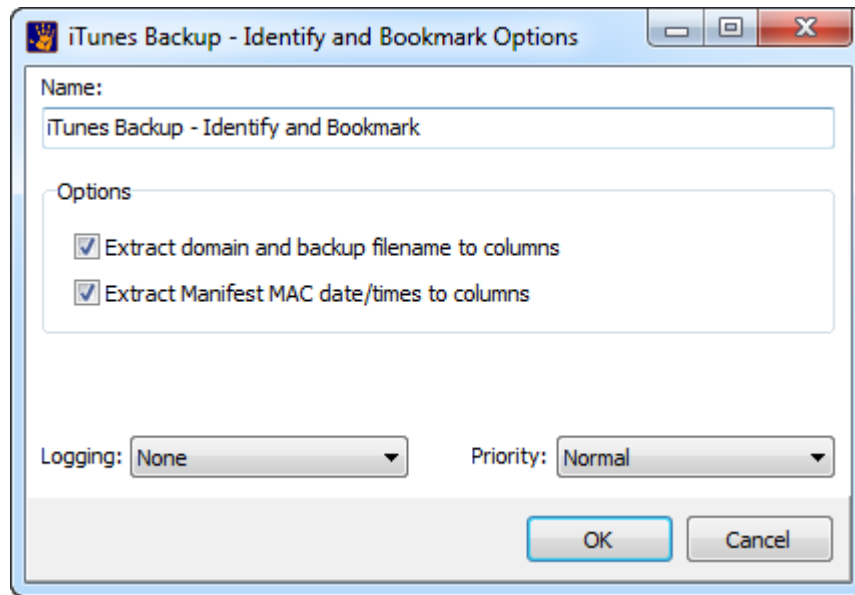
To **identify and bookmark iTunes Backup UUID folders**:

- In the **File System** module, under the **Analysis Scripts** button, select **iTunes Backups – Identify and Bookmark**, as shown in Figure 243 below:

Figure 243, iTunes Backups - Identify and Bookmark



The following window is displayed:

**Options:****Extract domain and backup filename to columns**

Like the parent folder, file names within each Apple device UUID backup folder can also be 40 decimal character hex encoded. The file names are SHA1 hash values of the original domain and file path on the device.

Selecting this option makes the decoded information available as separate columns in Forensic Explorer List views. Adding these names to Forensic Explorer can greatly assist the investigator navigate through backup folders and identify relevant files.

Extract Manifest MAC date/times to columns

The Manifest.mbdb file contained within an Apple UUID backup folder contains information about all other files in the backup. This includes Created Modified and Accessed (MAC) date/time stamps in UNIX time format (UTC) (17) (18) (19).

Selecting this option makes this MAC data available in columns: Note: Independent date/time testing is recommended to determine how MAC dates are effected on the examined device.

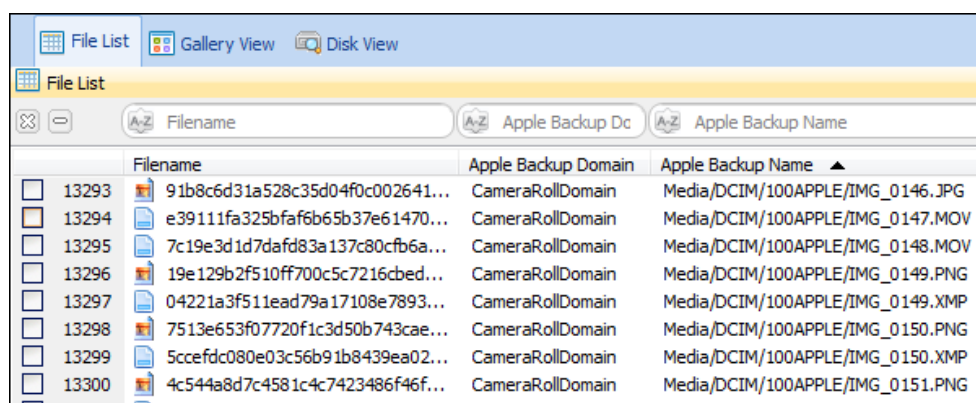
To add column data to list views:

1. **Right click** in a Forensic Explorer List view;
2. Select **Columns > Edit Columns**;
3. Add the:
 - iTunes Backup Domain

- iTunes Backup Name
- iTunes Backup Accessed (UTC)
- iTunes Backup Created (UTC)
- iTunes Backup Modified (UTC)

Columns to the view. An example of Domain and Name columns is shown in figure 219 below:

Figure 244, File list of an iTunes Backup with Backup Domain and Backup Name columns added



	Filename	Apple Backup Domain	Apple Backup Name
13293	91b8c6d31a528c35d04f0c002641...	CameraRollDomain	Media/DCIM/100APPLE/IMG_0146.JPG
13294	e39111fa325bfaf6b65b37e61470...	CameraRollDomain	Media/DCIM/100APPLE/IMG_0147.MOV
13295	7c19e3d1d7dafd83a137c80cfb6a...	CameraRollDomain	Media/DCIM/100APPLE/IMG_0148.MOV
13296	19e129b2f510ff700c5c7216cbcd...	CameraRollDomain	Media/DCIM/100APPLE/IMG_0149.PNG
13297	04221a3f511ead79a17108e7893...	CameraRollDomain	Media/DCIM/100APPLE/IMG_0149.XMP
13298	7513e653f07720f1c3d50b743cae...	CameraRollDomain	Media/DCIM/100APPLE/IMG_0150.PNG
13299	5ccefdc080e03c56b91b8439ea02...	CameraRollDomain	Media/DCIM/100APPLE/IMG_0150.XMP
13300	4c544a8d7c4581c4c7423486f46f...	CameraRollDomain	Media/DCIM/100APPLE/IMG_0151.PNG

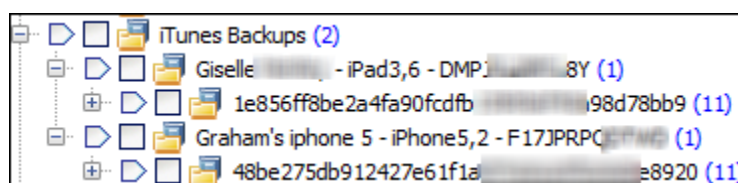
File Signature Analysis

When launched, an automatic and important part of the identification process is a file signature analysis of the Apple UUID backup folder content. This accurately identifies pictures, movies, sqlite files, plists, and other important files.

BOOKMARKED DATA

“iTunes Backups – Identify and Bookmark” bookmarks iTunes Backup UUID folders. For ease of identification each UUID folder is placed in a parent folder constructed using “**Device Name - Device Type - Device serial number**” from its **Info.plist** file. An example is shown in Figure 245 below:

Figure 245, Bookmarks module, iTunes Backup UUID folders



Additional summary information is provided in the bookmark comment of the file, for example:

Figure 246, Info.plist bookmark comment

The following iTunes Backup Info was found:
Build Version = 11D201

```

Device Name = Bill's iphone 5
Display Name = Bill's iphone 5
GUID = C33F23C95555099AD4921C8DC6D500E
ICCD = 8961029455559007627
IMEI = 01340900555590
Last Backup Date = 2014-05-01T06:43:21Z
Product Name = iPhone 5
Product Type = iPhone5,2
Product Version = 7.1.1
Serial Number = F55555PQDTWD
Target Identifier = 48be275db91255551f1a074c6ce0f2c6a2e8920
Target Type = Device
Unique Identifier = 48BE275DB915555561F1A074C6CE0F2C6A2E8920

```

28.1.3 MANUALLY EXAMINING ITUNES BACKUP FILES

The forensic value of individual iTunes Backup files is well documented (See: iOS Forensic Analysis for iPhone, iPad and iPod Touch [Sean Morrissey, 2010, Apress]). Key files are summarized in the following table:

Figure 247, Key iTunes Backup files for the forensic investigator

Type	Artifact	Summary
Address book	AddressBook.sqlitedb	Contacts
Call History	Call_History.db	Call history data
Keyboard	Dynamic-Text.dat	Keyboard input
Maps	/Library/Maps/History.plist	Map bookmarks Map directions Map route history
Safari	/Library/Safari/History.plist	Bookmarks Internet History Web pages
Wireless Networks	/SystemConfiguration/com.apple.wifi.plist	SSID BSSID Joined Dates

Due to the varied content of an iTunes Backup UUID folder, different Forensic Explorer data views are needed to best view each file type. The following table summarizes the recommended data views:

Figure 248, Recommended Forensic Explorer data views for iTunes Backup file types

File Type	Forensic Explorer data view
Media files (JPG, PNG, MOV)	Display view or Gallery view
XML	Display view

SQLite or DB	Display view
Binary PList	File Metadata view
MBDB	HEX or Text view
DAT	HEX or Text view

An example of the detail contained within the **com.apple.wifi.plist** file and shown in the Forensic Explorer File Metadata view is shown in Figure 249 below (detailing wireless network information for the Virgin Airlines Coolangatta airport lounge):

Figure 249, com.apple.wifi.plist in File Metadata viewer

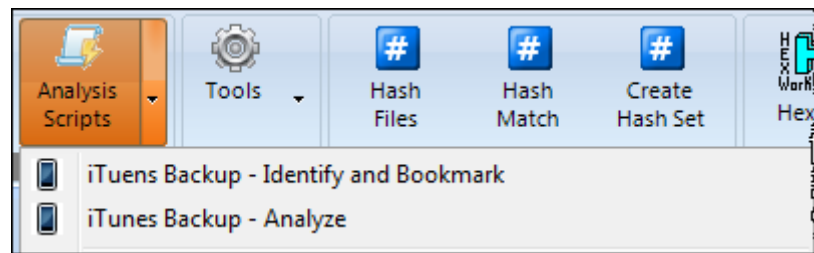
File Metadata				
Strength	0.753836512565613	0.753836512565613	Double	
SSID	Q29vbGFuZ2F0dGEgVml...	Q29vbGFuZ2F0dGEgVml...	UString	
CHANNEL	6	6	Int64	
CHANNEL_FLAGS	8	8	Int64	
isWPA	0	0	Int64	
lastAutoJoined	12-Jul-12 1:41:32 AM	12-Jul-12 1:41:32 AM	Date	
BSSID	c4:a:cb:a5:74:a0	c4:a:cb:a5:74:a0	UString	
authMode	0	0	Int64	
lastJoined	12-Jul-12 1:19:32 AM	12-Jul-12 1:19:32 AM	Date	
NOISE	0	0	Int64	
networkChannelListKey				
1				
CHANNEL	1	1	Int64	
CHANNEL_FLAGS	8	8	Int64	
6				
CHANNEL	6	6	Int64	
CHANNEL_FLAGS	8	8	Int64	
enabled	True	True	Boolean	
AGE	643	643	Int64	
ScaledRSSI	0.753836512565613	0.753836512565613	Double	
AP_MODE	2	2	Int64	
ScaledRate	1	1	Double	
WEPKeyLen	0	0	Int64	
RATES				
isValid	True	True	Boolean	
ASSOC_FLAGS	1	1	Int64	
SSID_STR	Coolangatta Virgin Lounge	Coolangatta Virgin Lounge	UString	
BEACON_INT	10	10	Int64	
RSSI	-65	-65	Int64	

28.1.4 ITUNES BACKUPS – ANALYZE (SCRIPTS)

Scripts provided with Forensic Explorer can be used to extract and bookmark specific data from iTunes Backup files. Bookmarked data is available to the Reports module.

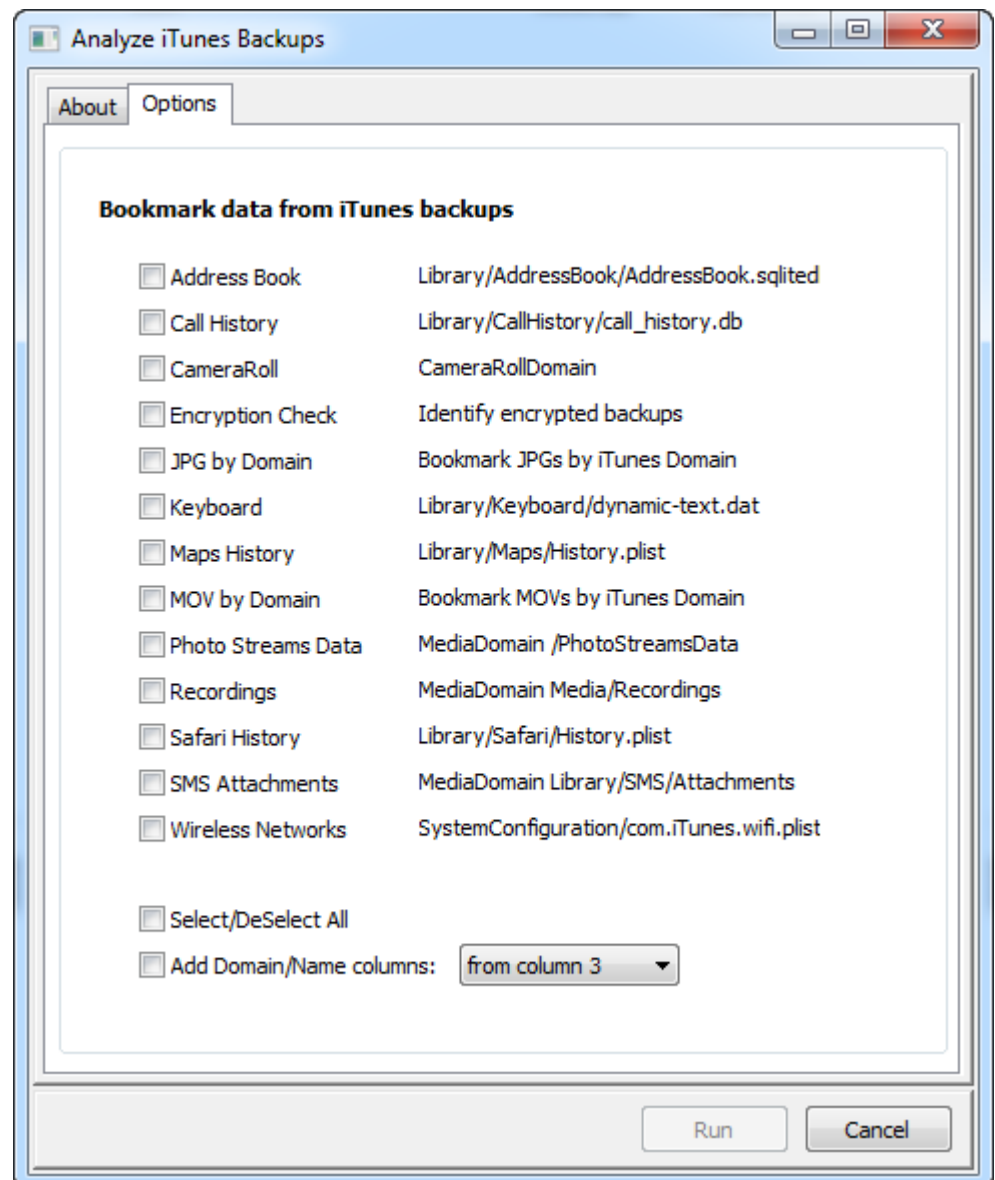
Provided iTunes Backup scripts are executed via the **File System module > Analysis Scripts > iTunes Backups – Analyze** button, shown in Figure 250 below:

Figure 250, iTunes Backups - Identify and Bookmark



This script opens the following the window:

Figure 251, iTunes Backups - Analyze



This window is itself a script, located in the Scripts Module > File System > iTunes Backups folder. It is used to execute additional scripts also located in that folder. Existing scripts are summarized as follows:

ADDRESS BOOK

Source iTunes Backup File:

31bb7ba8914766d4ba40d6dfb6113c8b614be442
Library/AddressBook/AddressBook.sqlitedb

Description

List of contacts in a sqlite database.

Output

The script bookmarks the Address Book sqlite database file. View the contents of the database in Display view.

CAMERA ROLL

Source iTunes Backup File:

JPG and MOV files in the CameraRoll domain are identified by a file signature analysis.

Output

Files are bookmarked under the CameraRoll folder of the relevant iTunes Backup UUID folder.

JPG BY DOMAIN

Source iTunes Backup File:

All JPG files are identified by a file signature analysis.

Output

Files are bookmarked according to the Apple Domain in which they reside. This is very useful for identifying applications that use image files such as kik messenger (kik.com).

KEYBOARD HISTORY

Source iTunes Backup File:

Library/Keyboard/dynamic-text.dat

Note that the path (and the subsequent UUID) will change with language settings. For example, Library/Keyboard/en_AU-dynamic-text.dat is the

Australian language file. This script identifies and bookmarks files by using the unique text “dynamic-text.dat”.

Description

“This file is sometimes referred to as a key logger for the iPhone, which is mostly true. Words get populated in this database by the user from keyboard inputs from numerous applications on the iPhone. Since this is a dynamic file, the data continues to grow.” (iOS Forensic Analysis for iPhone, iPad and iPod touch - Sean Morrissey, 2010, Apress, pp 150.) (20).

Output

Search query strings are bookmarked under the Address Book folder of the relevant iTunes Backup UUID folder. View the content of this file in Hex or Text data views.

MAPS HISTORY

Source iTunes Backup File:

b60c382887dfa562166f099f24797e55c12a94e4
/Library/Maps/History.plist

Description

“The History.plist file located in the Maps directory will give you a list of previous searches using the Maps app, as well as routes that were generated”(iOS Forensic Analysis for iPhone, iPad and iPod touch - Sean Morrissey, 2010, Apress, pp 155.) (20). This can include GPS co-ordinates and names of locations.

Output

Search query strings are bookmarked under the Maps History folder of the relevant iTunes Backup UUID folder. Manually review the File Metadata view of the file for more detailed content.

SAFARI HISTORY

Source iTunes Backup File:

1d6740792a2b845f4c1e6220c43906d7f0afe8ab
HomeDomain Library/Safari/History.plist

And;

ed50eadf14505ef0b433e0c4a380526ad6656d3a
AppDomain-com.apple.mobilesafari Library/Safari/History.plist

Description

Safari history contains browsing information. This includes the URL, page title, last visited date (converted from MAC absolute date UTC) and visit count.

Output

Page titles are bookmarked under the Safari History folder of the relevant iTunes Backup UUID folder. Manually review the file in File Metadata view for more detailed information.

WIRELESS NETWORKS

Source iTunes Backup File:

ade0340f576ee14793c607073bd7e8e409af07a8
SystemPreferencesDomain SystemConfiguration/com.apple.wifi.plist

Description

List of Wi-Fi networks that the device joined (or auto joined). Information includes:

- SSID (Service Set Identifier is used to uniquely identify any given wireless network) and;
- BSSID (Basic Service Set Identifier is a unique address that identifies the access point/router that creates the wireless network).
- Date/Time of last connection (UTC)

Output

The script bookmarks individual Wi-Fi network information under the Wifi bookmarks folder of the iTunes Backup UUID folder. Key data is summarized in bookmark comment. Note that date and times are converted from UTC.

28.2 THUMBNAILS

28.2.1 THUMBS.DB

In Windows operating systems up to and including Windows XP, a **Thumbs.db** file is created to store picture thumbnails that are used for display in Windows Explorer. The Thumbs.db is located in the same folder in which the pictures represented by the thumbnails reside.

From Windows Vista onward, Thumbs.db were largely replaced by Thumbcache (described below). However, it is still possible to locate Thumbs.db files in more recent Microsoft operating systems which are created when viewing remote or mapped drives in Windows Explorer.

28.2.2 THUMBCACHE

Beginning with Windows Vista, a “Thumbcache” database is created and stored under a user’s profile in the path:

C:\Users\{UserName}\AppData\Local\Microsoft\Windows\Explorer

The files containing the thumbnails are named according to their maximum pixel size, that is:

thumbcache_32.db

thumbcache_96.db

thumbcache_256.db

thumbcache_1024.db

28.2.3 FORENSIC VALUE OF THUMBNAILS

As Parsonage (2012) observes, “A large proportion of computer users have no knowledge of the presence of Windows thumbnail databases so that whilst they might delete incriminating pictures the evidence of their illicit activity often remains in the thumbnail databases”. (21)

Further suggested references include:

- Larson, Troy. Windows 7 Thumbnail Cache. Slideshare. [Online] October 2010 <http://www.slideshare.net/ctin/windows-7-forensics-thumbnaildtr4>
- Hurlbut, Dustin. Thumbs DB Files Forensic Issues. [Online] September 2014 https://ad-pdf.s3.amazonaws.com/wp.Thumbs_DB_Files.en_us.pdf

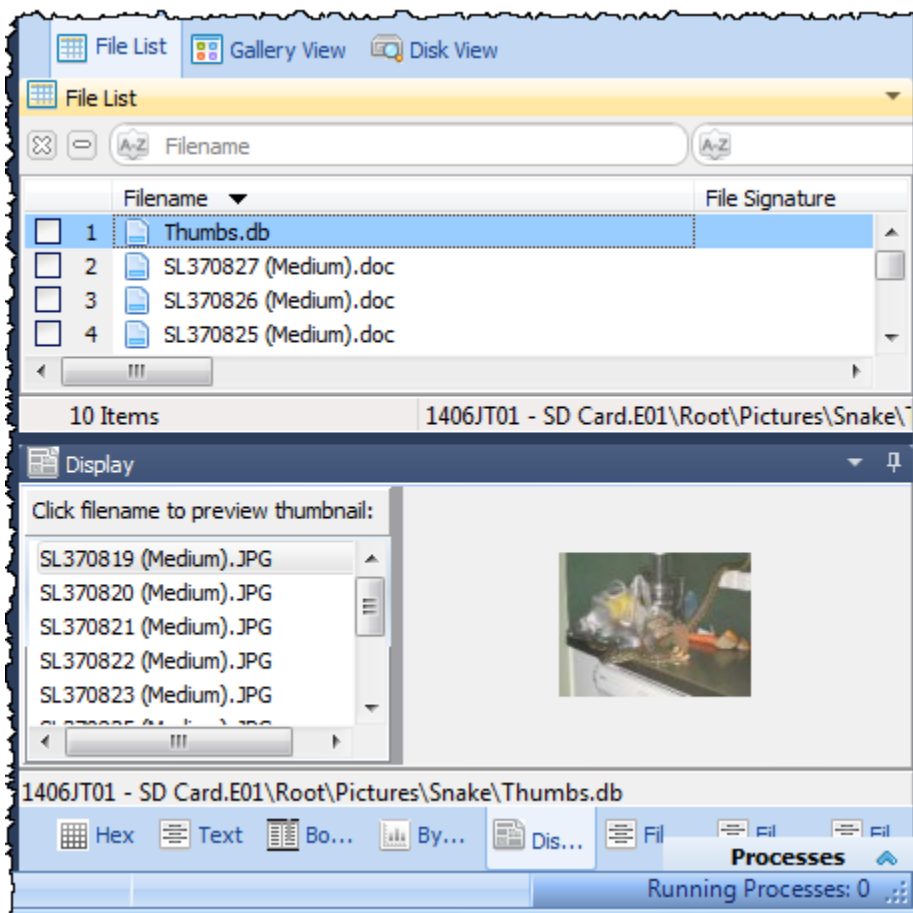
28.3 THUMBNAIL IN FORENSIC EXPLORER

For the purpose of this section, the term “**Thumbnail-Files**” is used to describe both Thumbs.db and Thumbcache_xxx.db files.

Like any other file types, Thumbnail-Files can be sorted, filtered, bookmarked, etc. in the modules of Forensic Explorer.

A **Thumbs.db** file can be previewed directly in the Forensic Explorer Display view. The content of each image can be displayed by clicking the image name in the left of the Display view, as shown in Figure 252 below:

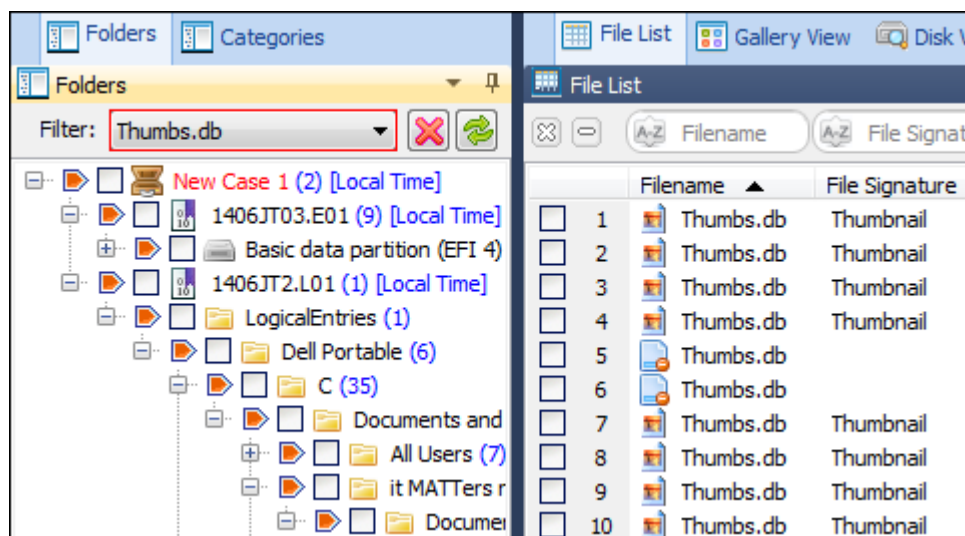
Figure 252, Thumbs.db Display view



28.3.1 THUMBNAIL-FILES FOLDERS FILTER

A fast way to view all Thumbnail-Files in a case is to branch plate all files in the case, and then apply a folders filter. A separate folders filter is available for Thumbs.db and Thumbcache_xxx.db. A Thumbs.db Folders filter as shown in Figure 253 below:

Figure 253, Folders Thumbs.db filter applied in the File System module



The filter code is accessible in the Scripts Module, in the path:

- *Filters\FileSystem\Thumbs.pas*
- *Filters\FileSystem\Thumbcache.pas*

28.3.2 EXPANDING COMPOUND THUMBNAI-FILES

Thumbnail-Files are considered to be **Compound** files because they act as containers for content.

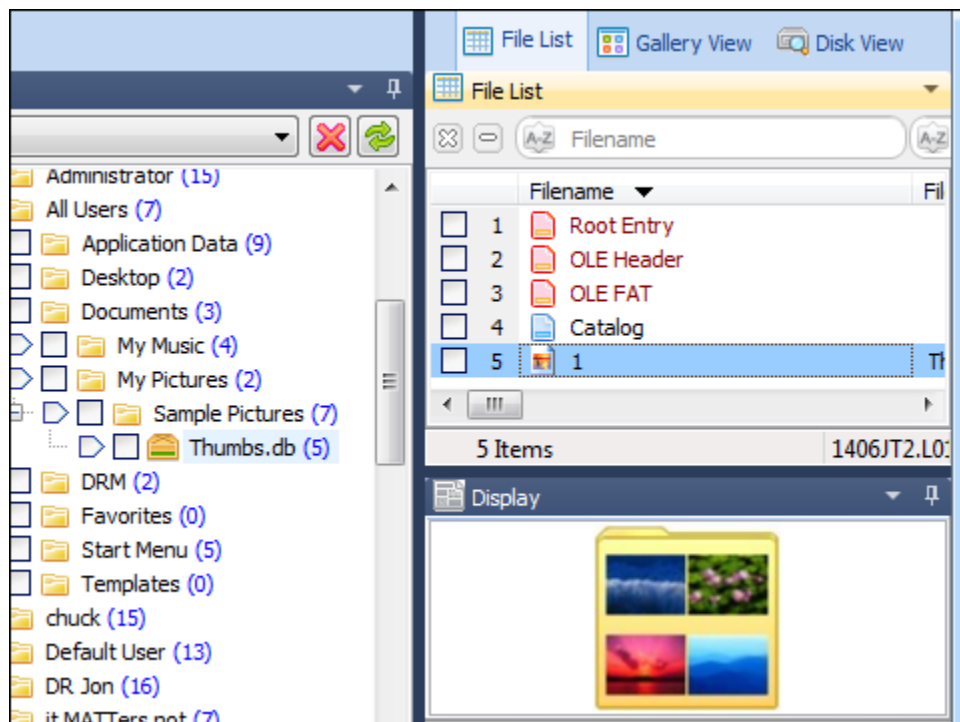
In order to work with compound files it is first necessary to identify them as such by running a **Signature Analysis** (a Signature Analysis can be run at any time in the File System module by clicking the Signature Analysis toolbar button). A correctly identified Thumbnail-File will show “**Thumbnail**” or “**ThumbCache**” in the File Signature column when a signature analysis is complete.

EXPAND A SINGLE THUMBNAI-FILE

To **expand a single compound Thumbnail-File**:

1. Run a Signature Analysis (if not already done);
2. Right click on the Thumbnail-File and select **Expand Compound File** from the drop down menu (if this menu option is not active, run a Signature Analysis).
3. Once expanded, the icon of the Thumbnail-File file will change to the compound file icon. Click on the Thumbnail-File to show the files it contains, as shown in Figure 254 below:

Figure 254, Expanded Thumbs.db file



EXPAND MULTIPLE THUMBNAIL-FILES

It can be advantageous to expand multiple compound Thumbnail-Files files

To **expand multiple Thumbnail-Files**:

1. In the File System module, select the Analysis Scripts button, run the **Expand Compound Files script**;

IMPORTANT: For speed purposes, before running the script, turn off any running Folders filter.

2. Select the **Thumbs/ThumbCache** checkbox and run the script.
3. All Thumbnail-Files in the case will then be expanded.
4. Use the branch plate and then filter with the File Signature column to display only Thumbnail-Files in the list view.

Chapter 29 - Legal

In This Chapter

CHAPTER 29 - LEGAL

29.1	This User Guide.....	332
29.2	Copyright	332
29.3	License agreement	332
29.4	Disclaimer	334

29.1 THIS USER GUIDE

This user guide is provided for information purposes only. All information provided in this user guide is subject to change without notice.

Please check the website, www.forensicexplorer.com for the latest version of the software and documentation.

29.2 COPYRIGHT

This user guide and its content is © copyright of GetData Forensics Pty Ltd. All rights reserved.

Any redistribution or reproduction of part or all of the contents in any form is prohibited without the express written permission of GetData Forensics Pty Ltd.

Products and corporate names appearing in this user guide may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation into the owners' benefit, without intent to infringe.

Specific trademark owners who are well established in the field of computer forensics software and whose products and terminology have become synonymous with forensics include:

Guidance Software (www.guidancesoftware.com), EnCase®;

Access Data (www.accessdata.com), Forensic Tool Kit® (FTK®);

Xways forensics (<http://www.winhex.com>), X-ways forensics®.

29.3 LICENSE AGREEMENT

GetData Forensics Pty Ltd ACN 143458039 ("GetData") is the developer of the software program Forensic Explorer. Permission to use Forensic Explorer and / or its documentation (the "Software") is conditional upon you agreeing to the terms set out below. By installing or otherwise using the Software you agree to be bound by the terms of this agreement. If you do not wish to accept the terms, do not install or use the Software.

GetData is and remains the exclusive owner of the Software. You acknowledge that copyright in the Software remains at all times with GetData. Unauthorized copying or modification of the Software will entitle GetData to immediately terminate this Agreement.

A single license of the software permits you to use the Software on a single computer. In the event that you have purchased multiple licenses, you may install and use the Software concurrently on multiple computers equivalent to the number of licenses that you have purchased. Unless you have purchased multiple licenses, this license does not permit you to load or use the Software on a network server or similar device which permits access by multiple computers.

You are not permitted to share the product activation information provided to you for this Software with other users.

GetData shall have the right to check license details at any time in any reasonable manner.

GetData may from time to time revise or update the software and may make such revisions or updates available subject to payment of the applicable license fee.

You may not publicly display the Software or provide instruction or training for compensation in any form without the express written permission of GetData.

The Software is protected under United States law and international law and international conventions and treaties. You may not rent, lease, sublicense, assign or otherwise transfer use of the Software to others without the express written permission of GetData. Doing so will entitle GetData to immediately terminate this Agreement.

Except to the extent applicable law specifically prohibits such restrictions, you may not reverse engineer, reverse compile, disassemble or otherwise modify the Software in any way.

You are solely responsible for protecting yourself, your data, your systems and your hardware used in connection with the Software. GetData will not be liable for any damages suffered from the use of the Software.

BY USING THE SOFTWARE, YOU EXPRESSLY AGREE THAT ALL RISKS ASSOCIATED WITH THE PERFORMANCE AND QUALITY OF THE SOFTWARE IS ASSUMED SOLELY BY YOU. YOU ACKNOWLEDGE AND AGREE THAT YOU HAVE EXERCISED YOUR INDEPENDENT JUDGEMENT IN ACQUIRING THE SOFTWARE.

TO THE EXTENT PERMITTED BY LAW, GETDATA SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF GETDATA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOFTWARE IS MADE AVAILABLE BY GETDATA "AS IS" AND "WITH ALL FAULTS". TO THE EXTENT PERMITTED BY LAW, GETDATA DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, CONCERNING THE QUALITY, SAFETY OR SUITABILITY OF THE SOFTWARE, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OR THAT THE SOFTWARE IS ERROR FREE.

IF ANY CONDITION OR WARRANTY IS IMPLIED INTO THIS AGREEMENT UNDER ANY APPLICABLE LEGISLATION CANNOT BE EXCLUDED, OR IF NOTWITHSTANDING THE EXCLUSION OF LIABILITY ABOVE GETDATA IS OTHERWISE LIABLE TO YOU, THEN TO THE EXTENT PERMITTED BY LAW THE LIABILITY OF GETDATA FOR BREACH OF THE CONDITION OR WARRANTY WILL BE LIMITED TO ONE OR MORE OF THE FOLLOWING AS DETERMINED BY GETDATA IN ITS ABSOLUTE DISCRETION:

(i) IN THE CASE OF GOODS, (A) THE REPLACEMENT OR SUPPLY OF EQUIVALENT GOODS OR THE REPAIR OF THE GOODS; OR (B) THE PAYMENT OF THE COST OF REPLACING

THE GOODS, ACQUIRING EQUIVALENT GOODS, OR HAVING THE GOODS REPAIRED;
AND

(ii) IN THE CASE OF SERVICES, THE SUPPLYING OF THE SERVICES AGAIN OR THE
PAYMENT OF THE COST OF HAVING THE SERVICES SUPPLIED AGAIN.

This agreement cannot be changed or altered except by a written document signed by you and GetData. This agreement is governed by the laws in force in New South Wales, Australia. Each party irrevocably and unconditionally submits to the non-exclusive jurisdiction of the courts of New South Wales, Australia.

29.4 DISCLAIMER

The software available for down loading through Internet sites and published by GetData Forensics Pty Ltd ("GetData") is provided pursuant to this license agreement. GetData encourages you to know the possible risks involved in the download and use of the Software from the Internet. You are solely responsible for protecting yourself, your data, your systems and your hardware used in connection with this software. GetData will not be liable for any damages suffered from the use of the Software.

BY USING THIS SOFTWARE, YOU EXPRESSLY AGREE THAT ALL RISKS ASSOCIATED WITH THE PERFORMANCE AND QUALITY OF THE SOFTWARE IS ASSUMED SOLELY BY YOU. GETDATA SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF GETDATA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOFTWARE IS MADE AVAILABLE BY GETDATA "AS IS"; AND "WITH ALL FAULTS" GETDATA DOES NOT MAKE ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, CONCERNING THE QUALITY, SAFETY OR SUITABILITY OF THE SOFTWARE, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. FURTHER, GETDATA MAKES NO REPRESENTATIONS OR WARRANTIES AS TO THE TRUTH, ACCURACY OR COMPLETENESS OF ANY INFORMATION, STATEMENTS OR MATERIALS CONCERNING THE SOFTWARE THAT IS CONTAINED IN GETDATA'S SOFTWARE DOWNLOAD SITE. IN NO EVENT WILL GETDATA BE LIABLE FOR ANY INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES HOWEVER THEY MAY ARISE AND EVEN IF GETDATA HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Appendix 1 - Technical Support

APPENDIX 1 - TECHNICAL SUPPORT

GetData Forensics Pty Ltd has its headquarters in Sydney, New South Wales, Australia.

SUPPORT

Documentation: <http://www.forensicexplorer.com/support>

Video Tutorials: <http://www.forensicexplorer.com/video>

Email Support: support@getdata.com

Phone Support: USA: (866) 723-7329 callback service

Or;

Sydney, Australia: +61 (0)2 8208 6053

Hours: Australian Eastern Standard Time, 9am - 5:30pm Mon - Fri

SECURE POST

GetData Forensics Pty Ltd
P.O. Box 71
Engadine, New South Wales, 2233
Australia

HEAD OFFICE

GetData Forensics Pty Ltd
Suite 204, 13A Montgomery Street
Kogarah, New South Wales, 2217
Australia

Phone: +61 (0)2 82086053

Fax: +61 (0)2 95881195

Hours: Australian Eastern Standard Time, 9am - 5:30pm Mon - Fri

Appendix 2 - Write Blocking

APPENDIX 2 - WRITE BLOCKING

IMPORTANT:

An accepted principal of computer forensics is that, wherever possible, source data to be analyzed in an investigation should not be altered by the investigator.

If physical media such as a hard drive, USB drive, camera card etc. is a potential source of evidence, it is recommended that when the media is connected to a forensics workstation it is done so using a write block device.

A write block is usually a physical hardware device (a write blocker) which sits between the target media and the investigators workstation. It ensures that it is not possible for the investigator to inadvertently change the content of the examined device and maintain “forensic integrity”.

There are a wide variety of forensic write blocking devices commercially available. Investigators are encouraged to become familiar with their selected device, its capabilities and its limitations.

Shown below is a Tableau USB hardware write block. The source media, an 8 GB Kingston USB drive is attached and ready for acquisition or analysis:

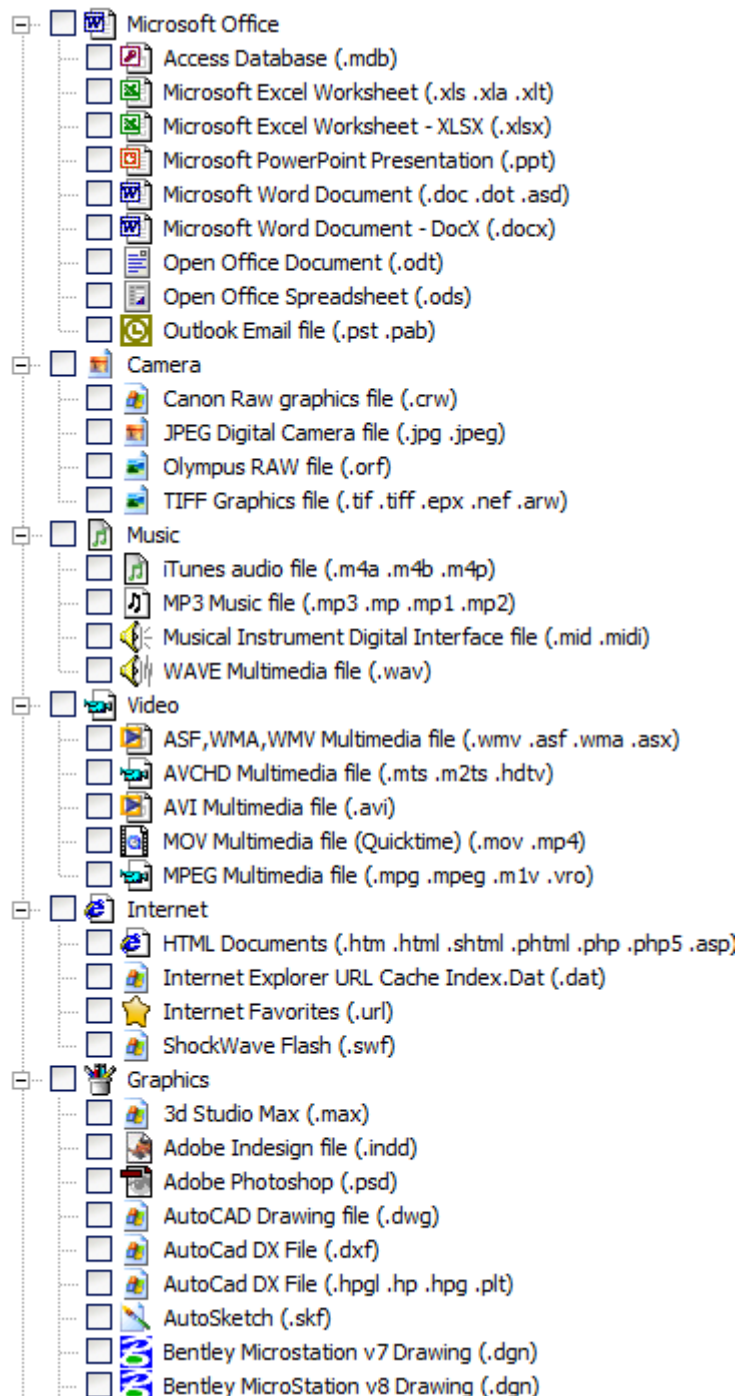
Tableau USB write block with USB as the source drive

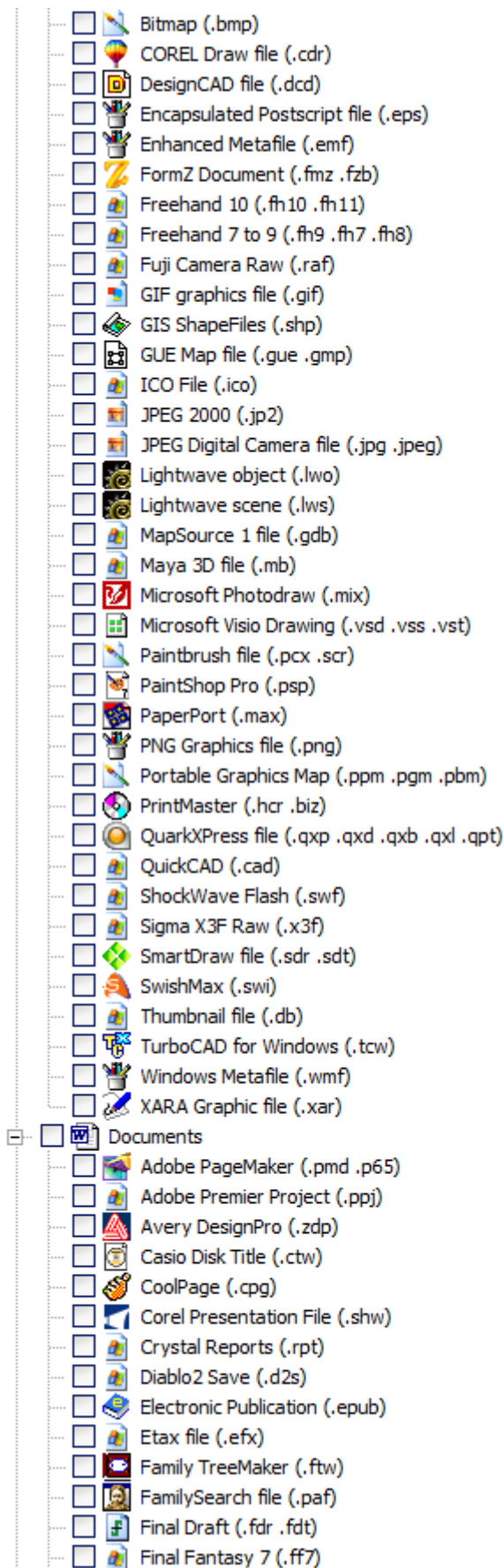


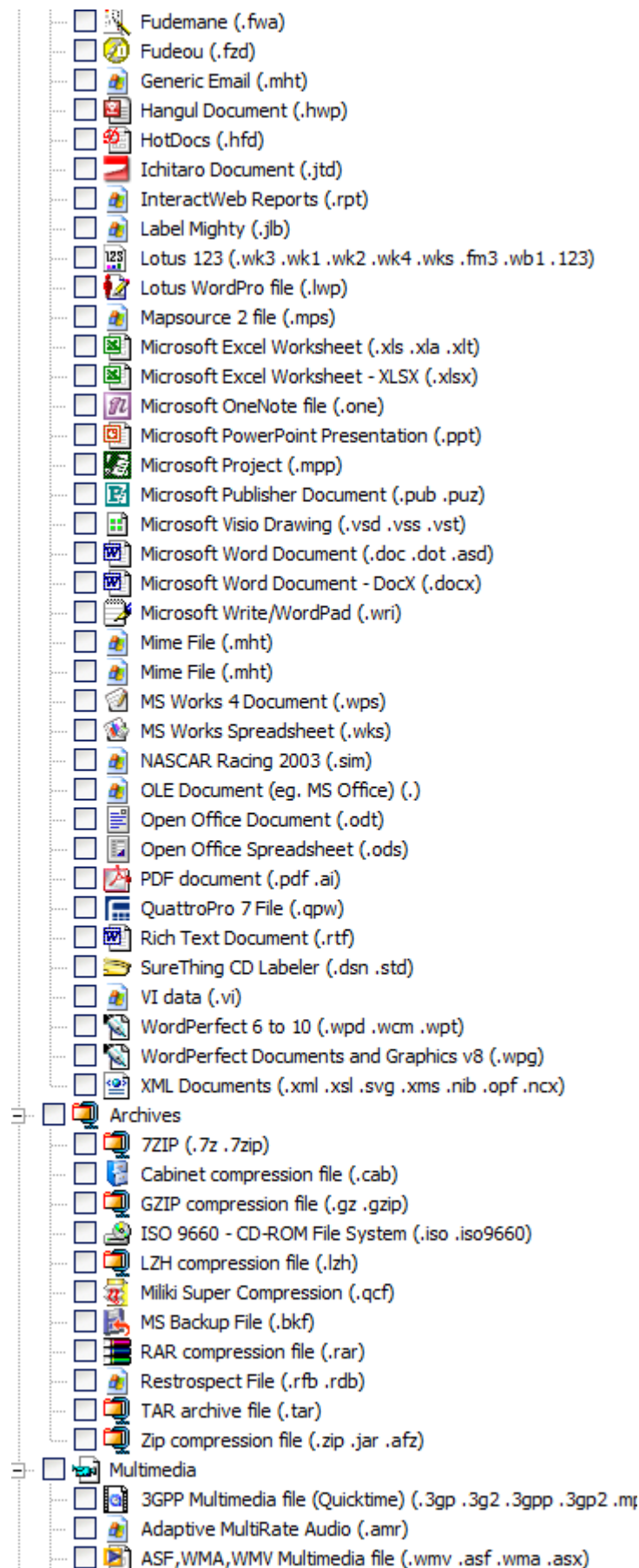
Appendix 3 - File Carving

APPENDIX 3 - FILE CARVING

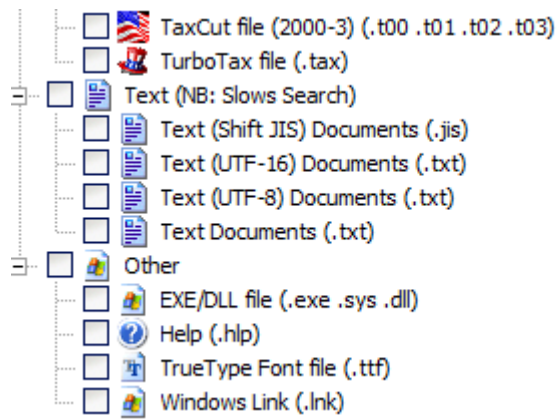
The following file types are supported by Forensic Explorers inbuilt file carving component. Refer to Chapter 23 - Data Recovery, for more information:







Copyright GetData Forensics Pty Ltd 2010 - 2015. All rights reserved.



Appendix 4 - Date and Time

APPENDIX 4 - SUMMARY OF DATE AND TIME						
File System Type	FAT	NTFS	exFAT	HFS	HFS+	EXT2/3/4
Time Type	Local	UTC	Local	Local	UTC	UTC
Source	FAT record of the file in the directory data. (32 bytes)	\$10 Standard attribute in the MFT record of the file.	\$85 exFAT record of the file in the directory data. (32 bytes)	The files HFS record in the Catalog file. (70 bytes)	The files HFS record in the Catalog file. (88 bytes)	The files inode record.
Calculation Method	DOS Date & Time.	100ns since 1 st Jan 1601.	DOS date & time.	Seconds since midnight 1 st Jan 1904.	Seconds since midnight 1 st Jan 1904.	Seconds since 1 st Jan 1970.
Modified	Written Time (2 bytes); Written Date (2 bytes); Total=4 bytes.	Written Time; Written Date; Total=8 bytes.	Created Time (2 bytes); Created Date (2 bytes); Created msecs (1 byte); Total=5 bytes.	Content Modified Date & Time. The date and time the file's contents were last changed by extending, truncating, or writing either of the forks. Total=4 bytes.	Content Modified Date & Time. The date and time the file's contents were last changed by extending, truncating, or writing either of the forks. Total=4 bytes.	Last Date & Time that the content was modified. Total=4 bytes.
Accessed	Accessed Date; Total=2 bytes.	Accessed Time; Accessed Date; Total=8 bytes.	Accessed Time (2 bytes); Accessed Date (2 bytes); Total=4 bytes.	N/A	Last accessed Date & Time. The date and time the file's content was last read. Total=4 bytes.	Access Date & Time. Total=4 bytes.
Created	Created Time (2 bytes); Created Date (2 bytes); Created msecs (1 byte); Total=5 bytes	Created Time; Accessed Date; Total=8 bytes.	Created Time (2 bytes); Created Date (2 bytes); Created msecs (1 byte); Total=5 bytes.	Created Date & Time. Total=4 bytes.	Created Date & Time. Total=4 bytes.	N/A
Modified Record	N/A	Modified Time; Modified Date; Total=8 bytes.	N/A	N/A	The last date and time that any field in the file's catalog record was changed. Total=4 bytes.	Modification Date & Time of the file record (the "Change" time). Total=4 bytes.

Appendix 5 - References

APPENDIX 5 - REFERENCES

1. *Hidden Disk Areas: HPA and DCO*. **Gupta, Mayank R., Hoeschele, Michael D. and Rogers, Marcus K.** Fall 2006, Volume 5, Issue 1, International Journal of Digital Evidence.
2. **Carrier, Brian.** *File System Forensic Analysis*. s.l. : Addison Wesley Professional, 2005.
3. **Forensiks Wiki.** Forensics Wiki. *AFF*. [Online] [Cited: Mar 29, 2011.] <http://www.forensicswiki.org/wiki/AFF>.
4. **Bunting, Steve and Wei, William.** *The Official EnCE EnCase Certified Examiner Study Guide*. Indianapolis IN : Wiley Publishing, Inc., 2006.
5. **United States Computer Emergency Readiness Team.** US-CERT Vulnerability Note VU#836068. *US-CERT: United States Computer Emergency Readiness Team*. [Online] [Cited: March 5, 2011.] <http://www.kb.cert.org/vuls/id/836068>.
6. **Xiaoyun Wang, Yiqun Lisa Yin, Hongbo Yu.** *Collision Search Attacks on SHA1*. 2005.
7. **Merritt, Rick.** Chinese researchers compromise SHA-1 hashing algorithm. *EE Times*. [Online] 2 16, 2005. [Cited: May 4, 2100.] <http://www.eetimes.com/electronics-news/4051745/Chinese-researchers-compromise-SHA-1-hashing-algorithm>.
8. *Automated mapping of large binary objects using primitive fragment type classification*. **Conti, Gregory, et al.** 2010, Digital Investigation, Vol. 7S, pp. S3-S12.
9. *Fileprints: Identifying file types by n-gram analysis*. **W. Li, K. Wang, S. Stolfo and B. Herzog.** West Point, NY : s.n., June, 2005. 6th IEEE Information Assurance Workshop.
10. **Injosoft AB.** ASCII Code - The extended ASCII table. <http://www.injosoft.se/>. [Online] <http://www.ascii-code.com/>.
11. **Wikipedia.** Regular Expression. [Online] en.wikipedia.org/wiki/Regular_expression.
12. **Microsoft.** Windows registry information for advanced users. *Article ID: 256986 - Revision: 12.3*. [Online] February 4, 2008. [Cited: August 19, 2011.] <http://support.microsoft.com/kb/256986>.
13. **Wikipedia.** Windows Registry. *Wikipedia - List of standard registry value types*. [Online] [Cited: December 27, 2011.] http://en.wikipedia.org/wiki/Windows_Registry.
14. **NIST.** Hacking Case. *NIST Hacking Case*. [Online] [Cited: Dec 03, 2012.] http://www.cfreds.nist.gov/Hacking_Case.html.
15. **Guidance Software Inc.** *EnCase Forensic Version 6.10 User Manual*. s.l. : Guidance Software, 2008.
16. **Magic number (programming).** *Wikipedia*. [Online] [http://en.wikipedia.org/wiki/Magic_number_\(programming\)](http://en.wikipedia.org/wiki/Magic_number_(programming)).

-
17. B, Satish. iPhone Forensics – Analysis of iOS 5 backups : Part2. *Security Learn*. [Online] 2012. [Cited: June 13, 2014.] <http://www.securitylearn.net/2012/05/30/iphone-forensics-analysis-of-ios-5-backups-part2/>.
 18. iPhone backup – mbdb file structure. [Online] <http://www.securitylearn.net/tag/manifest-mbdb-format/>.
 19. iPhone-Backup-Analyzer. *GitHub*. [Online] [Cited: June 18, 2014.] <https://github.com/PicciMario/iPhone-Backup-Analyzer/blob/master/mbdbdecoding.py#L53>.
 20. Morrissey, Sean. *iOS Forensic Analysis for iPhone, iPad and iPod touch*. s.l. : apress, 2010.
 21. Parsonage, Harry. Under My Thumbs. [Online] 2012. [Cited: September 1, 2014.] <http://computerforensics.parsonage.co.uk/downloads/UnderMyThumbs.pdf>.
 22. Microsoft. Hard Links and Junctions. [Online] [Cited: June 14, 2014.] <http://msdn.microsoft.com/en-us/library/windows/desktop/aa365006%28v=vs.85%29.aspx>.
 23. —. [MS-SHLLINK]: Shell Link (.LNK) Binary File Format. *MSDN*. [Online] 2014. [Cited: Oct 23, 2014.] <http://msdn.microsoft.com/en-us/library/dd871305.aspx>.
 24. Microsoft MSDN. <http://msdn.microsoft.com/en-us/library>. [Online] <http://msdn.microsoft.com/en-us/library/cc231989%28PROT.13%29.aspx>.
 25. *The Windows Registry as a forensic resource*. Carvey, Harlan. 3, September 2005, Pages 201-205 , Digital Investigation, Vol. 2, pp. 201-205.
 26. *Time and date issues in forensic computing--a case study*. Boyd, Chris and Foster, Pete. 1, February 2004, Digital Investigation, Vol. 1, pp. 18-23.
 27. Jones, Keith J, Bejtlich, Richard and Rose, Curtis W. *Real Digital Forensics Computer Security and Incident Response*. s.l. : Addison-Wesley, 2006.
 28. Mederios, Jason. *NTFS Forensics: A Programmers View of Raw Filesystem Data Extraction*. s.l. : Grayscale Research, 2008.
 29. Russon, Richard. Linux NTFS Project: NTFS Documentation. *Sourceforge.net*. [Online] 1996 - 2004. [Cited: March 16, 2011.] <http://sourceforge.net/projects/linux-ntfs/files/NTFS%20Documentation/>.
 30. MBR is damaged - www.NTFS.com. *NTFS.com*. [Online] <http://www.ntfs.com/mbr-damaged.htm>.
 31. Microsoft. *Microsoft Extensible Firmware Initiative FAT32 File System Specification. FAT: General Overview of On-Disk Format*. s.l. : Microsoft, 2000.
 32. Stoffregen, Paul. Understanding FAT32 Filesystems. *PJRC*. [Online] Feb 24, 2005. [Cited: March 18, 2011.] <http://www.pjrc.com/tech/8051/ide/fat32.html>.
 33. Microsoft. Detailed Explanation of FAT Boot Sector. *support.microsoft.com*. [Online] Article ID: 140418 - Last Review: December 6, 2003 - Revision: 3.0, December 6, 2003. <http://support.microsoft.com/kb/140418>.
 34. —. Windows and GPT FAQ. *Microsoft Developers Network (MSDN)*. [Online] July 2008. <http://msdn.microsoft.com/en-us/windows/hardware/gg463525.aspx>.
-

-
35. —. Basic Storage Versus Dynamic Storage in Windows XP. *Microsoft Support*. [Online] December 1, 2007. [Cited: March 23, 2011.] <http://support.microsoft.com/kb/314343>.
36. National Institute of Standards and Technology. CFTT Project Overview. *Computer Forensics Tool Testing Program*. [Online] [Cited: March 28, 2011.] http://www.cftt.nist.gov/disk_imaging.htm.
37. Wikipedia - Host Protected Area. http://en.wikipedia.org/wiki/Host_protected_area. [Online] [Cited: Mar 29, 2011.] http://en.wikipedia.org/wiki/Host_protected_area.
38. Apple Computer, Inc. Technical Note TN2166 - Secrets of the GPT. *developer.apple.com*. [Online] 11 6, 2006. [Cited: April 5, 2011.] http://developer.apple.com/library/mac/#technotes/tn2166/_index.html.
39. Apple Inc. *Inside Macintosh: Files*. Reading, Massachusetts : Addison-Wesley, August 1992.
40. Apple, Inc. HFS Plus Volume Format - Technical Note TN1150. *developer.apple.com*. [Online] March 5, 2004. [Cited: April 6, 2011.] <http://developer.apple.com/library/mac/#technotes/tn/tn1150.html>.
41. Wikipedia: Extent (file systems). Extent (file systems). *Wikipedia: Extent (file systems)*. [Online] [Cited: 4 6, 2011.] [http://en.wikipedia.org/wiki/Extent_\(file_systems\)](http://en.wikipedia.org/wiki/Extent_(file_systems)).
42. Aomei Technology, Co., Ltd. What is a Dynamic Disk? *Dynamic Disk*. [Online] 2009. [Cited: April 13, 2011.] <http://www.dynamic-disk.com/what-is-dynamic-disk.html>.
43. Lewis, Don L. The Hash Algorithm Dilemma—Hash Value Collisions. *Forensic Magazine*. [Online] 2009. [Cited: May 2011, 4.] <http://www.forensicmag.com/article/hash-algorithm-dilemma%E2%80%93hash-value-collisions?page=0,0>.
44. *An Empirical Analysis of Disk Sector Hashes for Data Carving*. Yoginder Singh Dandass, Nathan Joseph Necaie, Sherry Reede Thomas. 2008, Journal of Digital Forensic Practice, Vol. 2, pp. 95-104.
45. Farmer, Derrick J. and Burlington, Vermont. Windows registry quick reference. *A Windows Registry Quick Reference: For the Everyday Examiner*. [Online] [Cited: Oct 12, 2012.] <http://www.forensicrofocus.com/downloads/windows-registry-quick-reference.pdf>.
46. Wong, Lih Wern. Forensic Analysis of the Windows Registry. *ForensicFocus.com*. [Online] School of Computer and Information Science, Edith Cowan University. [Cited: Oct 12, 2012.] <http://www.forensicrofocus.com/Content/pid=73/page=1/>.
47. Harrington, Michael. Seek and You Shall Find: Using Regular Expressions for Fast, Accurate Mobile Device Data Searches. <http://www.dfinews.com>. [Online] [Cited: Oct 29, 12.] <http://www.dfinews.com/article/seek-and-you-shall-find-using-regular-expressions-fast-accurate-mobile-device-data-searches?page=0,0>.
48. Access Data Inc. Registry Quick Find Chart. *Access Data*. [Online] 2005. [Cited: August 19, 2011.] <https://ad-pdf.s3.amazonaws.com/Registry%20Quick%20Find%20Chart%20%207-22-08.pdf>.
-

Appendix 6 - Definitions

APPENDIX 6 - DEFINITIONS

Alternate Data Stream	An Alternate Data Stream (ADS) is a feature of the NTFS file system. ADS were originally included in Windows NT for compatibility with Macintosh HFS file systems resource fork and a data fork. The ADS provides a means to allow programmers to add additional metadata to be stored for a file, without adding this data directly to the file. The additional data is attached as a stream which is not normally visible to the user.
ANSI character set	The ANSI character set was that standard character encoding for English versions of Microsoft Windows, including Windows 95 and NT. The ANSI format stores only the 128 ASCII characters and 128 extended characters, using 1 byte per character. Not all of the Unicode characters are supported.
ASCII	The American Standard Code for Information Interchange (ASCII) is a 7-bit character encoding scheme that allows text to be transmitted between electronic devices in a consistent way. The ASCII character set comprises codes 0–127, within which codes 0–31 and 127 are non-printing control characters. The addition of Codes 128–255 make up the Extended ASCII character set (see http://www.ascii-code.com/ for more information) (10).
Bookmarks	Forensic Explorer enables any item (file, folder, keyword, search hit etc.), or sections of items, to be marked and listed in the Bookmarks module. Bookmarks are used to note items of interest.
BpB	“Bytes per Block”. Used in the Forensic Explorer File Extent tab to display the number of Bytes per Block (cluster) for the highlighted file.
BpS	“Bytes per Sector”. Used in the Forensic Explorer File Extent tab to display the number of Bytes per Sector for the highlighted file.
Byte Plot view (Forensic Explorer)	A view in Forensic Explorer which includes for a selected file: A graphical representation of a binary file; A Character Distribution graph representing the frequency that each ASCII character is displayed in the file. See “Byte Plot and Character Distribution” page 91.
Carved (file)	<p>Files located by “file carving” with Forensic Explorer are displayed as “Carved_ [filetype].ext. This is because a file system record for these files no longer exists so they are in effect lost to the file system.</p> <p>Because file and folder information is only stored with the file system record, a carved file does not retain its original file or folder name.</p>

Case File	<p>A case file is the store of investigational activities for an individual case in Forensic Explorer. The case file records the location of the examined devices and holds the results of searching, sorting, bookmarks, reports etc.</p> <p>A case file is designed to build over time as a record of an investigation, in the same way as would a paper based file in a traditional matter.</p>
Cluster	<p>A cluster is the smallest logical unit of disk storage space on a hard drive that can be addressed by the computers Operating System. A single computer file can be stored in one or more clusters depending on its size.</p>
Cluster Boundaries	<p>A cluster boundary refers to the start or the end position of a cluster (a group of sectors). If a file is fragmented (stored in non-contiguous clusters), the fragmentation happens at the cluster boundary, as there is no smaller unit of storage space that can be addressed by a computer.</p> <p>Examining data at cluster boundaries can be an important technique to improve the speed of some search routines. For example when file carving for file headers, it is faster to search the cluster boundary (i.e. the beginning of a cluster) rather than a sector by sector search of the drive.</p>
Codepage	<p>Codepage is another term for character encoding. It consists of a table of values that describes the character set for a particular language. When a keyword search is conducted in Forensic Explorer, the correct codepage should be selected.</p>
Computer forensics	<p>Computer forensics is the use of specialized techniques for recovery, authentication, and analysis of electronic data with a view to presenting evidence in a court of law.</p>
Compound File	<p>A compound file is a file that is a container for other files or data, such as a .Zip or .Pst (Microsoft Outlook mail file). See Chapter 19.5 - Expand compound file.</p>
Data carve	<p>See file carve.</p>
Data View	<p>A data view describes the different methods available in Forensic Explorer to examine evidence. For example a single file may be examined in the Hex, Text or Display data views, with each view giving a different perspective on its content.</p>
Deleted File	<p>A deleted file is one which has been marked as deleted by the file system (usually as a result of being sent to and emptied from with Recycle Bin). A deleted file can be recovered by reading the file system record for the file, then reading and restoring the file data. As long as the data for the file is intact (i.e. the space once occupied by the file has not been used to store new data) the recovered file will be valid.</p>

	<p>In some cases the file system record itself can be overwritten and destroyed. If this is the case the file can only be recovered by “file carving” (see 22.4- File carving). Because file and folder information is only stored with the file system record, a carved file does not retain its original file or folder name.</p>
Delphi Basics©	<p>Delphi Basics© is a documentation package for the Delphi programming language (see http://www.delphibasics.co.uk/). Delphi Basics© is installed with and licensed for use only with Forensic Explorer. Delphi Basics© is provided as a reference guide only. Not all commands/features in the documentation are available in Forensic Explorer.</p>
Device	<p>A device refers to the electronic media being examined. It usually refers to a physical device, such as a hard drive, camera card etc., but can also mean the forensic image of a device in DD, E01 or other formats.</p>
Directory	<p>See Root Directory</p>
Directory Entry (FAT)	<p>A component of the FAT file system. Each file or folder on a FAT partition has a 32 byte directory entry which contains its name, starting cluster, length and other metadata and attributes.</p>
Disk Slack	<p>The area between the end of a partition and the end of the disk. It is usually considered to be blank, but can hold remnants of previous disk configurations or could be used to purposely hide data.</p>
Disk view (Forensic Explorer)	<p>A graphical representation in Forensic Explorer of sectors on the examined device. Disk view can be used to:</p> <ul style="list-style-type: none">• Examine the content of the data in a specific sector/s;• Quickly navigate to a desired sector position on the device;• Obtain a graphical overview of the file types which make up the drive and where they are position on the examined media;• Identify the location and fragmentation of individual files.
DST	<p>Daylight Savings Time</p>
dtSearch®	<p>dtSearch® (www.dtsearch.com) is third party index search software built into Forensic Explorer and accessed via the Index Search module tab (see Chapter 13 - Index Search Module, for more information).</p>
Entropy	<p>Entropy is an expression of disorder or randomness. It is used in computer forensics to measure the randomness of data. For example, a compressed file will have a high entropy score. A text file will not. An entropy score is included in Forensic Explorer the Byte Plot data view of the File System module.</p>

E01	A forensic file format used to create disk image files. Developed by Guidance Software (http://www.guidancesoftware.com/)
Evidence Items	Items of evidence that have been added to the case, such as forensic image files, email files, registry files etc.
Explorer View	File display technology written by GetData and used in the Forensic Explorer File Display tab to show the contents of more than 300 different file types.
FAT	<p>FAT (File Allocation Table) is the file system that pre-dates NTFS. Once popular on Windows 95, 98 and XP, it is now primarily used on memory cards, usb drives, flash memory etc. due to its simplicity and compatibility between Operating Systems (e.g. Windows and MAC).</p> <p>For more information see: http://www.forensicswiki.org/wiki/FAT</p>
FAT Slack	The unused space in the last cluster of the FAT where the logical size of the FAT does not fill the complete cluster.
File carve	<p>File carving is the process of searching for files based on a known content, rather than relying on file system metadata. This usually involves searching for a known header and footer of a specific file type.</p> <p>Forensic Explorer has built in code to data carve for more than 300 file types.</p>
File Signature	The header component of a file which has unique identifiers that assigns it to a type, e.g. a jpeg. Most common file types have a signature set by the International Organization for Standardization (ISO). Identifying a file by its signature is a more accurate method of assessment than using the file extension, which can easily be altered.
File Slack	The unused space in the last cluster of a file where the logical size of the file does not fill the complete cluster. The file slack can contain fragments of old data previously stored in that cluster.
File system	The organization of files into a structure accessible by the Operating System. The most common types of file systems used by Windows are FAT and NTFS. Others include EXT (Linux) and HFS (MAC).
Fileprint	A byte level graphical representation of a file content that may “serve as a distinct representation of all members of a single type of file” (9). See “Byte Plot and Character Distribution” page 91.
Flag	In Forensic Explorer a flag is used to mark a file as relevant. It is a colored

	<p>box (flag) that is applied to a List view when the “Flag” column is displayed. Eight colored flags are available for use. Flags are applied by highlighting an item and double clicking the opaque flag color in the flag column, or by using the right click “Add Flag” menu. Flags can also be applied by running Forensic Explorer scripts.</p>
Folder	See Root Directory
Forensic Image	<p>A "forensic image is a file (or set of files), used to preserve an exact "bit-for-bit" copy of data residing on electronic media.</p> <p>Using non-invasive procedures, forensic software is used to create the image file. The image contains all data, including deleted and system files, and is an exact copy of the original.</p> <p>Most forensic imaging software integrates additional information into the image file at the time of acquisition. This can include descriptive details entered by the examiner, as well as the output of mathematical calculations, an "acquisition hash", which can be later used to validate the integrity of the image. The forensic image file acts as a digital evidence container that can be verified and accepted by courts.</p>
Forensic Integrity	<p>In computer forensics the term “forensic integrity” commonly refers to the ability to preserve the evidence being examined so that it is not altered by the investigator or the investigative process. This enables a third party to conduct an independent examination of the evidence on an identical data set. Forensic integrity is usually achieved through the use of write blocking devices (to protect original media from being changed) and the forensic image process (the acquisition of an identical copy which can be re-verified at a later date.)</p>
Fragmented File	<p>The distribution of a file on a disk so that it's written in non-contiguous clusters.</p>
Free Space	<p>Free space is often used to describe unallocated clusters, the available disk storage space that is not allocated to file storage by a volume. Free space can however also refer to the unused area of a disk.</p> <p>Free space in Partition: Space inside the partition that is not used by a volume (this is usually a small section of space at the end of a partition). If there is no volume then this is the entire partition.</p> <p>Free space on Disk: Space on the disk that does not form part of any partition but is available for future allocation. Usually consists of some sectors between the MBR and the first partition, and space at the end of the disk that was not used in any partition.</p>
GeoTag (Geotagging)	<p>Geotagging is the process of adding geographical identification metadata to files, usually photographs or videos. This data is usually latitude and longitude co-ordinates.</p>

GREP	Stands for Generalized Regular Expression Parser. Originally a command line text search utility in UNIX it is now an acronym to describe the format of a search. It uses a concise but flexible structure to match strings of text, including characters, words, or patterns of characters. Forensic Explorer utilizes PCRE (Perl Compatible Regular Expressions) for keyword searching, of which GREP is a subset.
Hard Link	<i>"A hard link</i> is the file system representation of a file by which more than one path references a single file in the same volume" Microsoft (22).
Hash	A Hash is a mathematical calculation to generate a unique value for specific data. The chances of two files that contain different data having the same hash value are exceedingly small. The most common hash algorithms in use are MD5, SHA1 and SHA256.
Hash Set	<p>A Hash Sets is a store of mathematical calculations (hash values - usually created by the MD5 algorithm) for a specific group of files. The hash values are a "digital fingerprint" which can then be used to identify a file and either include or exclude the file from a data set.</p> <p>Hash Sets are often grouped in the forensic community into two groups:</p> <p>Good Hash Sets: Operating System files, program installation files, etc.; and Bad Hash Sets: virus files, malware, Trojans, child pornography, Steganography tools, hacking tools etc.</p> <p>Hash sets can be created in Forensic Explorer, or downloaded from a trusted source.</p>
Hex	Hexadecimal is a base 16 numbering system. It contains the sixteen sequential numbers 0-9 and then uses the letters A-F. In computing, a single hexadecimal number represents the content of 4 bits. It is usually expressed as sets of two hexadecimal numbers, such as "4B", which gives the content of 8 bits, i.e. 1 byte.
Image File	See Forensic Image.
Index Search	An Index Search is the process of creating a database of search words in the case so that after the index is created an instant search is possible. Forensic Explorer uses the third party application dtSearch® (www.dtsearch.com) for this process.
INFO2	<p>Windows automatically keeps an index of what files were deleted including the date and time of the deletion. The index is held in a hidden file in the Recycle Bin called INFO2.</p> <p>When the Recycle Bin is emptied, the INFO2 file is deleted. Recovery and analysis of deleted INFO2 files can provide important information about files that were once located on the computer.</p>

Investigator	In this user guide “Investigator” is used to describe the computer forensics examiner, i.e. the user of Forensic Explorer. The investigator is responsible for creating and developing the case file.
Item	In Forensic Explorer the term “item” is a generic term used to describe a piece of data. The data could be a file, folder, partition, metadata entry, FAT, MFT, unallocated clusters, or other such data that can be isolated and examined.
iTunes Backup	iTunes Backups are created by iTunes. When an Apple device (iPhone, iPad, iPod) is connected to a computer for the first time and synced with iTunes, a folder is created using the unique device ID (UUID). These iTunes Backup folders are very distinctive, in that they are 40 hexadecimal characters long. iTunes Backups can be processed with Forensic Explorer.
Keyword	<p>A keyword is a string of data created by the forensic examiner so that the case can be searched for instances of that data (a keyword search).</p> <p>A keyword can be an actual word, but can also be raw data.</p> <p>Complex keywords are usually created using RegEx expressions.</p>
LEF	See Logical Evidence File
LFN (also see SFN)	Long File Name refers to file or folder on a FAT file system which has a name greater than 8 characters and 3 for the file extension (or one which contains special characters). The storage of the additional file name information makes it necessary for Windows to create an additional LFN directory entry (or entries) to hold the extra information.
Link Files	Link files (.lnk) are Microsoft Windows shortcut files. Link files have their own metadata and can provide valuable information about files stored on the computer. (23)
Live Boot	‘Live Boot’ is a component of Forensic Explorer that enables an investigator to boot a forensic image or write protected physical hard drive. The investigator can then operate the computer in a real time, forensically sound, virtual environment. The boot process is achieved through and integration of Mount Image Pro and VMWare.
Logical Evidence File (LEF)	<p>A Logical Evidence File is a forensic image containing specific files, rather than the traditional image of an entire volume or physical disk. They are usually created during a preview where an investigator identifies file based evidence worthy of preservation, when an image of the entire volume or device is not warranted.</p> <p>Common Logical Evidence File formats are L01, created by EnCase® forensic software (www.guidancesoftware.com) or AD1 by Access Data’s</p>

	Forensic Tool Kit ® (www.accessdata.com).
	Forensic Explorer enables files in a case to be exported to a logical evidence file (LEF) in .L01 format (see 9.6.2 for more information).
Logical file space	The actual amount of space occupied by a file on a hard drive. It may differ from the physical file size, because the file may not completely fill the total number of clusters allocated for its storage. The part of the last cluster which is not completely filled is called the file slack.
Lost OS Clusters	Clusters in a volume that have no file data. For NTFS this is calculated from accumulating all clusters associated with all the files in the MFT (including the Unallocated clusters as that was derived from the \$BITMAP record), then working out the space left over. For NTFS this is space that the OS might not be able to allocate without a check disk or equivalent. For normal uncorrupted NTFS this would be non-existent or small. For FAT typically this is non-existent, as the FAT table is used both in cluster allocation of files and the working out of Unallocated clusters on X volume.
Master boot record (MBR, Boot Sector)	The very first sector on a hard drive. It contains the startup information for the computer and the partition table, detailing how the computer is organized.
Master File Table (MFT)	<i>"On an NTFS volume, the MFT is a relational database that consists of rows of file records and columns of file attributes. It contains at least one entry for every file on an NTFS volume, including the MFT itself. The MFT stores the information required to retrieve files from the NTFS partition". (24))</i>
Metadata	Metadata is often referred to as "data about data". Windows metadata can include a files create, last accessed and modified dates, as shown in File List view of Forensic Explorer. File metadata includes information such as camera make and model in a JPEG, or author name in Microsoft Word. The File Metadata view in Forensic Explorer is used to show the metadata in a file. Metadata can also be extracted by a script and added to a column. See 8.11.1 for more information.
Module	Refers to the horizontal tabs (Evidence, File System, Keyword Search, Index Search, Bookmarks, Reports, Scripts, Email, and Registry) at the top of the Forensic Explorer main program window. Each module tab is used to access a particular function of the program, for example, the Registry module enables the investigator add and browse registry files.
Mount Image Pro (MIP)	A computer forensics software tool written and sold by GetData (www.mountimage.com) which enable the mounting of forensic image files as a drive letter on a Windows computer system. MIP is sold with Forensic Explorer. It is installed as a separate program but can be run from a shortcut in the Forensic Explorer toolbar.

MRU	Most Recently Used (MRU) is a term used to describe a list of the most recently opened files by an application. Many Windows applications store MRU lists as a way of allowing fast and consistent access to most recently used files. Most MRU lists are stored in the Windows registry.
Multi-core processing	<p>A multi-core processor is a single computing component with two or more processors ("cores"). Each core is responsible for reading and processing program instructions. A multi-core process should be faster than the same process run on a single core. However users are encouraged to test their workstations as different hardware configurations can effect multi-core speed.</p> <p>Forensic Explorer provides the option to use multi core processing in File Carving, Hashing and Keyword Search. The option is set using the "Priority" options, where "Low" is single core, and Normal, High and Critical are multi-core.</p>
NTFS	The Windows New Technology File System (NTFS) superseded FAT. It was released with Windows NT and subsequently Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista, and Windows 7. It uses a Master File Table (MFT) to store the information required to retrieve files from the NTFS partition.
Ophcrack	Ophcrack is a free open source program that recovers Windows passwords by processing LM hashes through rainbow tables. Ophcrack ISO images can be used with Forensic Explorer Live Boot.
Pane	An area of the Forensic Explorer module. The Forensic Explorer module is broken down into three panes, Folders view, File List view and File Display. A pane can contain multiple different windows, such a Hex view, Text view, Disk view, <i>Console</i> etc.
Pascal	A programming language used to create scripts in Forensic Explorer. See Module Chapter 18 - Scripts Module.
Partition	A part of a hard disk that can have an independent file system.
PCRE (Perl Compatible Regular Expression)	Perl Compatible Regular Expressions (PCRE) is a regular expression (RegEx) library. The PCRE library is incorporated into a number of prominent open source programs, such as the Apache HTTP Server and PHP language. RegEx expressions can be used to keyword search evidence in Forensic Explorer.
Pre-processing (a case)	<p>Pre-processing describes the setup of a case so that core analysis functions are automatically run prior to investigator review. Core analysis functions can include hashing, carving and signature analysis.</p> <p>Pre-processing options are set in Forensic Explorer when a device or</p>

	forensic image file is added. See 10.5 for more information.
Priority	In Forensic Explorer priority refers to the use of threaded multi-core processing. See "Multi-Core Processing".
Preview (Evidence Module)	The Preview button in the Evidence module enables an investigator to quickly add a device or forensic image to Forensic Explorer without first having to go through the steps to create a new case. The investigator can choose to save a preview to a case, or if not, when the preview is closed, no data is saved.
RAID	Redundant Array of Independent Disks.
RAM	Random Access Memory, where programs are loaded and computer code is executed. The content of RAM is lost when the computer is turned off.
RAM Slack	RAM slack is the data between the end of the logical file and the rest of that sector. For example, a sector is written as a block of 512 bytes, so if the last sector contains only 100 bytes, the remaining 412 bytes is padded with RAM slack. In older Operating Systems, e.g. Windows 95, RAM slack could contain data from RAM unrelated to the content of the file. In more recent Operating Systems, RAM slack is filled with zeroes.
Record View (Forensic Explorer)	Record View displays information directly from the FAT or MFT record. It provides more complete details for a file than the limited information displayed in File List view.
Recover My Files	Data Recovery Software authored and sold by GetData at www.recovermyfiles.com
Regex (Regular Expression)	A regular expression provides a concise and flexible means to "match" (specify and recognize) strings of text, such as particular characters, words, or patterns of characters. "The concept of regular expressions was first popularized by utilities provided by Unix distributions, in particular the editor ED and the filter grep q" (http://en.wikipedia.org/wiki/Regex).
Registry	The Windows Registry is a hierarchical database that stores configuration settings and options for the Microsoft Windows operating systems. For the computer forensics examiner it can be a wealth of information on all aspects of the computer and its use, including hardware, applications, and user configuration.
Ribbon (Toolbar)	The ribbon refers to the Forensic Explorer toolbar and the top of each module. The contents of the toolbar are controlled by scripts.
Root Directory/Folder	A directory is a container used to organize folders and files into a

	<p>hierarchical structure. The root (also referred as the root folder or root directory) is the first level folder of the hierarchy. It is analogous to the root of a tree, from which the trunk and branches arise.</p> <p>A directory that is below the root is called a subdirectory. A directory above a subdirectory is called its parent directory. The root is the parent of all directories.</p> <p>“Directory” was a more common term when DOS use was prolific (The “DIR” command is used in DOS to list the contents of a directory). Directories are now more commonly referred to as “Folders”.</p>
Script	<p>A script is a computer program written to perform a specific task. Forensic Explorer has a scripts module which allows the investigator to write Pascal language scripts.</p>
Sector	<p>A sector is a specifically sized unit of storage on a hard disk. A sector on a hard disk usually contains 512 bytes. A group of sectors forms a cluster, which is the lowest level of storage space which can be addressed by an Operating System (e.g. Windows).</p>
SFN (see also LFN)	<p>Short File Name refers to a file or a folder on a FAT file system that has a file name that can be stored in the 8.3 file name format (8 name characters with 3 characters for the extension). The name and metadata for a SFN file can be stored within a standard FAT directory entry.</p>
Signature Analysis	<p>Signature analysis compares a file's header with its extension. A mismatch may justify closer examination. Identifying a file by its signature is a more accurate method of classification than using the file extension (e.g. .jpg), as the extension can easily be altered.</p>
Shadow Copy	<p>“Shadow Copy” (also known as Volume Snapshot Service, Volume Shadow Copy Service, VSC or VSS), is a technology included in Microsoft Windows that allows taking manual or automatic backup copies or snapshots of data, even if it has a lock, on a specific volume at a specific point in time over regular intervals” (https://en.wikipedia.org/wiki/Shadow_Copy). Forensic Explorer enables investigators to add and examine the content of Shadow Copies. See Chapter 25.</p>
Skin Tone Analysis	<p>Skin tone analysis is the automated detection of skin tone colors in graphics files. It is often used to identify pornographic pictures on a suspect's computer. In Forensic Explorer, skin tone analysis is run using a script.</p>
Slack	<p>See File Slack, Disk Slack, FAT Slack</p>
Steganography	<p>Steganography is the art and science of writing hidden messages in such a</p>

	<p>way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity (Definition from: http://en.wikipedia.org/wiki/Steganography)</p>
User Datagram Protocol (UDP)	UDP is one of the core members of the Internet Protocol Suite (the protocols used for the Internet). Forensic Explorer can use UDP to access remote drives.
Unallocated Clusters	<p>Unallocated clusters (also referred to as unallocated space or free space) are the available disk storage space that is not allocated to file storage by a volume. Unallocated clusters can be a valuable source of evidence in a computer forensics examination because they can contain deleted files or remnants of deleted files created by the Operating System and / or computer users.</p> <p>Unallocated clusters on X volume: Space inside the X volume that is available to the File System for future file storage. For NTFS this is calculated from the \$BITMAP record, for FAT this is calculated from the FAT Table.</p>
Unicode	Unicode is an international standard for processing and displaying all types of text. Unicode provides a unique number for every character for all languages on all platforms.
UUID	An Apple device (iPhone, iPad or iPod Touch) has a Unique Device Identifier (UDID). It is a sequence of 40 letters and numbers. When a backup of the device is made to a PC, the backup files for the device are stored in the UUID folder. See chapter 28.1 for more information.
Volume	A collection of addressable sectors that are used to store data. The sectors give the appearance of being consecutive, but a volume may span more than one partition or drive.
Word List	A list of words exported from an index in the Index Search module. The word list can be used for password breaking or other purposes.
Write Block	A hardware device or software program that prevents writing to an examined device. A write block is designed to maintain the 'forensic integrity' of an examined device by demonstrating that changes to the content of the device were not possible.
VSC or VSS	Volume Shadow Copy, or Volume Shadow Service: - See "Shadow Copy"

Appendix 7 - Sample Script

APPENDIX 7 - SAMPLE SCRIPT

Sample script showing some of the common features of Delphi / Pascal scripting. A fully commented version is provided in the Quick Reference folder in the Script Module.

```
{!NAME:      Help File - Sample Script 1.pas}
{!DESC:      Counts years to 21 }
{!INFO:      Shows basic Pascal programming elements }
{!AUTHOR:    GetData}
{!VERSION:   v1.00}

program Help_File_Sample_Script_1;

uses
  GUI, SysUtils;

const
  starting_age = 10;

var
  my_age: integer;

procedure ConsoleLog(AString: string);
begin
  Progress.Log([' + DateTimeToStr(now) + ']: ' + AString);
end;

begin
  my_age := starting_age;
  ShowMessage('Your current age is: ' + inttostr(starting_age));
  ConsoleLog ('Your current age is: ' + inttostr(starting_age));
  if my_age > 21 then ShowMessage('You are already older than 21' + #13#10 + 'The program will now end');
  while my_age < 21 do
  begin
    my_age := my_age + 1;
    if my_age = 21 then
    begin
      ShowMessage('WOW, happy 21st!');
      ConsoleLog ('Congratulations. You made it from '+inttostr(starting_age)+' to: ' + inttostr(my_age));
    end
  end
  else
  begin
    ShowMessage('Next year you will be: ' + inttostr(my_age));
    ConsoleLog ('Next year you will be: ' + inttostr(my_age));
  end;
end;

end.
```


Appendix 8 - Icon Key

APPENDIX 8 - ICON KEY

Forensic Explorer icons sorted by Category:

Icon	Category	Description
	Case	A Forensic Explorer case
	Shadow Copy	A mounted shadow copy volume
	Compound file	A folder holding the contents of an expanded compound file
	Date	Categorize dates - File System > Folders view > Category view
	Device	A physical device, e.g. a hard drive
	Device	A logical device, e.g. C: drive.
	File	A deleted file
	File	A FAT “dot” directory entry
	File	A FAT “double dot” directory entry
	File	A system file
	File	An active file
	File	An alternate data stream
	File	Windows hard link (http://en.wikipedia.org/wiki/Hard_link)
	Folder	A folder holding the results of a Forensic Explorer file carve
	Folder	A deleted folder
	Deleted items	Categorize deleted items - File System > Folders view > Category view
	Folder	An active folder
	Free space	Free space in partition
	Image	A forensic image file
	Image folder	Select an image from a folder
	Navigation	An expandable branch (folder structure)
	Navigation	Active branch plate

	Navigation	Inactive branch plate
	Partition	A partition
	Partition	An active partition
	Unallocated	Unallocated clusters

Disk View

	The start sector of a file
	Currently selected sector
	One type overlays another

	MBR/VBR (Red)
	FAT 1 (Dark Violet)
	FAT 2 (Web Violet)
	\$MFT (Dark Violet)
	System files (Web Tomato)
	\$MFT resident file (the file overlays the \$MFT)
	Folder (Deep Sky Blue)
	Allocated File (Corn Flower Blue)
	Unallocated space (Lt Gray)
	Deleted file (A deleted file overlays unallocated space)
	Carved file (Dark Orange: Carved file overlays unallocated space)

Icons in Forensic Explorer include those supplied by:

- Silk Icons: <http://www.famfamfam.com/lab/icons/silk/>; and
- <http://www.softicons.com>

Appendix 9 - Index

APPENDIX 9 - INDEX

- Accessed
 - Date, 148
- Activation
 - Dongle, 35
 - Evaluation version offline, 18
 - Evaluation version online, 16
- Apple Backups, 316
- Artifact
 - Count, 103
 - Selected, 103
- ASCII
 - Character distribution, 91
- Attributes, 148
- Bookmarks
 - Module, 190
- Bookmarks Module, 187
- Boolean
 - Index search, 171
- BpB - Bytes per block, 100
- BpS - Bytes per sector, 100
- Branch plate, 75
- Byte Plot, 91
 - Examples, 92
- Carve
 - About file carving, 276
 - Cluster, Sector, Byte, 279
 - Disk view icon, 79, 366
 - Evidence Processor, 137
 - Hex Selection, 86
- Case
 - Close, 141
 - New, 124
 - Open, 127
 - Recent, 128
 - Save, 140
- Categories, 146
- Cell phone. *See* Phone
- Close
 - Case, 141
- Columns
 - Add, 110
- Compound file
 - Expand, 105
- Copy
 - Rows to clipboard, 119
- Copyright, 332
- Created, 148
- Data fragment, 265, 272
- Data Views
 - Summary, 71
- Data-store, 168
- Date and Time
 - Adjust for Case, 243
 - Adjust for evidence, 241
 - Adjust in Evidence Processor, 138
 - Daylight Saving (DST), 240
 - Overview, 236
 - Registry Time Zone setting, 236
- Date range filter
 - Filter - Date Range, 114
- Deleted Files
 - FAT, 265
 - NTFS, 272
- Delphi Basics, 223
- Disclaimer, 334
- Disk view, 78
 - Custom color script, 219
 - Custom colors, 79
- Display view, 89
- Dongle. *See* Activation
- Duplicates
 - De-duplicate, 250
- Email
 - Module, 176
- Email Module, 175
- Evidence
 - Add, 129
- Explorer Tool, 118
- Export
 - Delimited rows, 109
 - Files, 105
 - to L01, 107
 - Using a script, 107
- Export Word List, 173
- Extension, 148
- Extract Metadata**
 - Evidence Processor, 138
- File List view, 147
- File Name, 148
- File signature analysis, 260

-
- File slack
 - Definition, 354
 - Index search, 168
 - File System module, 144
 - File tree
 - File System workspace, 144
 - Filter
 - File System module, 74
 - Scripts, 75, 119, 218
 - Text filter tool, 115
 - Filtering, 114
 - Flags
 - Apply, 113
 - Clear, 114
 - Flat File Hash set, 253
 - Fragmentation
 - File (FAT), 266
 - Full Path, 148
 - Fuzzy. *See* Index Search
 - Gallery View, 84
 - GUID
 - Preview, 122, 140
 - Hash
 - Acquisition hash display, 137
 - Flat File Hash Set, 253
 - Forensic Imager Acquisition, 50
 - Verify (Evidence Processor), 137
 - Verify L01, 108
 - Hash set, 251
 - Hex view, 86
 - Hits
 - Keyword Result List, 162
 - HPA, 45
 - Index Search
 - Creating an index, 167
 - Module, 166
 - Searching an index, 169
 - information.
 - test, 176
 - Installation, 29
 - Investigators
 - Add, Edit, Delete, 125
 - Is Deleted, 148
 - JBOD, 282
 - Keyword
 - Add, 153
 - Edit or Delete, 155
 - Group, 156
 - Import, 157
 - Regular expression (RegEx), 154
 - Keyword Search, 152
 - Results, 160
 - Run, 158
 - L01
 - Export, 107
 - Verify, 108
 - License agreement, 332
 - List view, 77
 - Live Boot, 302
 - Logical Size, 148
 - MBR
 - Search for known, 136
 - MD5, 246, *See* Hash
 - Metadata
 - Extract to columns, 98
 - View, 98
 - Mobile Phone. *See* Phone
 - Modified, 148
 - Module
 - Bookmarks, 187
 - Email, 175
 - Evidence, 121
 - File System, 143
 - Index Search, 165
 - Keyword Search, 151
 - Registry, 179
 - Reporting, 194
 - Scripts, 215
 - Open
 - Case, 127
 - Orphans
 - NTFS, 273
 - Path
 - Case folders, 32
 - Program, 31
 - Registry keys, 32
 - Working, 31
 - Phone
 - Carve, 279
 - Phone Module
 - Create custom module, 229
 - Phonic. *See* Index Search
 - Physical size
 - Column, 148
 - Preview
 - Evidence, 122
 - Purchase orders, 24
 - RAID, 282
 - Hardware, 284
 - Software, 285
 - Recover Folders
 - FAT, 269, 274
 - NTFS, 274
 - RegEx
 - Column filter, 117
 - Keyword Search, 154
-

-
- Quick start guide, 117
 - Registry
 - Location of registry files, 180
 - Module, 180
 - Registry file
 - Add from File System module, 181
 - Add standalone, 181
 - Save
 - Case, 140
 - Scripting
 - Data recovery, 280
 - Scripts
 - Introduction to scripting, 223
 - Open, Copy, Rename, Delete, 222
 - Send to Module, 110
 - SHA. *See* Hash
 - Shadow Copy
 - Background, 288
 - Mount in Forensic Explorer, 293
 - Signature Analysis
 - Evidence processor, 137
 - Sort
 - Multi column, 111
 - Persistent, 112
 - Remove, 112
 - Single column, 111
 - Startup.pas
 - Installation folder, 32
 - Script, 219
 - Stemming. *See* Index Search
 - Technical support, 335
 - Text view, 88
 - Thumbcache, 326
 - Thumbs.db, 326
 - Time Zone. *See* Date and Time
 - Tree view, 74, 144
 - Uninstall, 34
 - User Datagram Protocol (UDP), 130
 - UUID
 - Apple Backup, 316, 357
 - Video
 - Thumbnail viewing, 90
 - Volume Shadow Copy. *See* Shadow Copy
 - VSC or VSC. *See* Shadow Copy
 - Wildcards
 - Index search, 172
 - Word List, 173
-