Chapter Contents

Published: 12-Feb-19 at 13:04:04

Quick Start Guide........................................................................................................................................... 11
Wibu CodeMeter Activation Dongle.............................................................................................................. 11
System Requirements...................................................................................................................................... 11
Download....................................................................................................................................................... 11
Installation...................................................................................................................................................... 12
Forensic Explorer Module Overview ........................................................................................................... 12
Live Boot ....................................................................................................................................................... 14

Chapter 1 - Introduction................................................................................................................................. 15
  1.1 Introducing Forensic Explorer .................................................................................................................. 16
  1.2 Supported file formats............................................................................................................................... 16
  1.3 Supported file systems ............................................................................................................................. 16
  1.4 Key program features .............................................................................................................................. 17

Chapter 2 - 30 Day Evaluation Version ...................................................................................................... 19
  2.1 30 day evaluation version........................................................................................................................ 20
  2.2 Activating the 30-DAY evaluation version ............................................................................................... 20

Chapter 3 - Purchase...................................................................................................................................... 27
  3.1 Purchase .................................................................................................................................................. 28
  3.2 License maintenance ................................................................................................................................. 29

Chapter 4 - Installation.................................................................................................................................. 31
  4.1 System requirements............................................................................................................................... 33
  4.2 Download.............................................................................................................................................. 33
  4.3 Installation.............................................................................................................................................. 33
  4.4 Uninstall Forensic Explorer .................................................................................................................. 38

Chapter 5 - Dongle Activation...................................................................................................................... 39
  5.1 Dongle activation of the purchased version ......................................................................................... 40
Chapter 10 - Evidence Module

10.1 Preview
10.2 New case
10.3 Open an existing case
10.4 Adding evidence
10.5 Evidence Processor
10.6 Adding additional evidence to a case
10.7 Saving a case
10.8 Closing a case

Chapter 11 - File System Module

11.1 File System module
11.2 Toolbar
11.3 Folders view
11.4 Categories view
11.5 File List view
11.6 Other data views
11.7 File System Toolbar
16.5 Examining registry files using scripts ............................................................ 213

Chapter 17 - Bookmarks Module ........................................................................ 215
17.1 Adding Bookmarks ...................................................................................... 216
17.2 Bookmarks Module ...................................................................................... 218
17.3 Identifying Bookmarked files other modules .............................................. 222

Chapter 18 - Reports Module ............................................................................. 223
18.1 Reporting & Bookmarks .............................................................................. 225
18.2 The Reports Module .................................................................................... 226
18.3 Reports Tree ................................................................................................. 227
18.4 Report Editor ................................................................................................. 233
18.5 Creating Reports .......................................................................................... 235

Chapter 19 - Scripts Module .............................................................................. 271
19.1 Scripts Module .............................................................................................. 272
19.2 Managing scripts in the scripts window ....................................................... 278
19.3 Introduction to Scripting .............................................................................. 279
19.4 Startup.Pas .................................................................................................... 282

Chapter 20 – Encryption ...................................................................................... 287
20.1 Encryption .................................................................................................... 288
20.2 Decrypting Supported Encryption Formats ................................................ 290
20.3 Identifying Other Encrypted Files ............................................................... 293

Chapter 21 - Date and Time ............................................................................... 297
21.1 Date and time in computer forensics ............................................................ 298
21.2 FAT, HFS, CDFS file system date and time ................................................ 298
21.3 NTFS, HFS+ file system date and time ........................................................ 298
21.4 Date and time information in the Windows registry ..................................... 298
21.5 Daylight saving time (DST) ......................................................................... 302
21.6 Adjusting Date in Forensic Explorer ............................................................ 302
<table>
<thead>
<tr>
<th>Chapter 27 – Mount Image Pro</th>
<th>371</th>
</tr>
</thead>
<tbody>
<tr>
<td>27.1 Mount Image Pro</td>
<td>372</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 28 – Live Boot</th>
<th>375</th>
</tr>
</thead>
<tbody>
<tr>
<td>28.1 Live Boot</td>
<td>376</td>
</tr>
<tr>
<td>28.2 Requirements</td>
<td>376</td>
</tr>
<tr>
<td>28.3 Compatibility</td>
<td>379</td>
</tr>
<tr>
<td>28.4 Live Boot Working Folder</td>
<td>380</td>
</tr>
<tr>
<td>28.5 How to Live Boot a Forensic Image</td>
<td>380</td>
</tr>
<tr>
<td>28.6 Live Boot and User login Password bypass</td>
<td>386</td>
</tr>
<tr>
<td>28.7 Troubleshooting Live Boot</td>
<td>405</td>
</tr>
<tr>
<td>28.8 Creating A deployable live boot</td>
<td>409</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 29 – Forensic Image Converter</th>
<th>421</th>
</tr>
</thead>
<tbody>
<tr>
<td>29.1 Forensic Image Converter</td>
<td>423</td>
</tr>
<tr>
<td>29.2 Download and Install Forensic Image Converter</td>
<td>423</td>
</tr>
<tr>
<td>29.3 Add Forensic Image Converter to the Windows Path</td>
<td>425</td>
</tr>
<tr>
<td>29.4 Launching the Windows Command Line</td>
<td>429</td>
</tr>
<tr>
<td>29.5 ConvertTOL01.EXE - Usage</td>
<td>429</td>
</tr>
<tr>
<td>29.6 Validation of Conversion</td>
<td>433</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 30 – Working With</th>
<th>435</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.1 iTunes Backups</td>
<td>437</td>
</tr>
<tr>
<td>30.2 Thumbnails</td>
<td>454</td>
</tr>
<tr>
<td>30.3 Jump Lists</td>
<td>458</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 31 - Legal</th>
<th>461</th>
</tr>
</thead>
<tbody>
<tr>
<td>31.1 This User Guide</td>
<td>462</td>
</tr>
<tr>
<td>31.2 Copyright</td>
<td>462</td>
</tr>
<tr>
<td>31.3 License agreement</td>
<td>462</td>
</tr>
<tr>
<td>31.4 License agreement Disclaimer</td>
<td>464</td>
</tr>
</tbody>
</table>
Appendix 1 - Technical Support ................................................................. 465
Appendix 2 - Write Blocking ................................................................. 467
Appendix 3 - File Carving ................................................................. 469
Appendix 4 - Summary of Date and Time ................................................................. 475
Appendix 5 - References ................................................................. 477
Appendix 6 - Definitions ................................................................. 481
Appendix 7 - Sample Script ................................................................. 495
Appendix 8 - Icon Key ................................................................. 497
Appendix 9 – iTunes Backup Files ................................................................. 499
Appendix 10 - Index ................................................................. 503
QUICK START GUIDE

This quick start guide gives a brief introduction to Forensic Explorer. More detailed information is available from:

**User Guide:**  ‘Forensic Explorer User Guide.en.pdf’ is in the installation folder.

C:\Program Files\GetData\Forensic Explorer v4

**Online:**  http://www.forensicexplorer.com/support.php

**By Phone or email:**  USA: +1.844.300.0552 (Pacific Time) or support@getdata.com

WIBU CODEMETER ACTIVATION DONGLE

A Wibu CodeMeter USB activation dongle is shipped with a Forensic Explorer purchase. Each dongle is uniquely identified by a serial number stamped on the USB insert. It contains an activation key for:

- Forensic Explorer;
- Mount Image Pro (http://www.mountimage.com);

**Important:** The dongle is for activation purposes only and cannot be used for USB storage.

SYSTEM REQUIREMENTS

Forensic Explorer and Mount Image Pro are optimized for an Intel® Core i7 with 16GB RAM. Forensic Explorer is a 64bit application which will run Windows 7, 8, 8.1 or 10. Forensic Explorer should be run with local administrator permissions where possible. (Contact support@getdata.com if a 32bit version is required).

DOWNLOAD

**Forensic Explorer:**  The latest version of Forensic Explorer is available for download at: http://www.forensicexplorer.com/download.php. Customers should download and install the Full Version Dongle Only.

**Mount Image Pro:**  Mount Image Pro is required for Live Boot. The latest version of Mount Image Pro is available for download at: http://www.mountimage.com.

**Virtualization Software:**  Oracle VirtualBox (recommended) is free and is available for download at https://www.virtualbox.org;  

Or;  

VMWare Workstation Pro is commercial software available for purchase and download at: https://my.vmware.com/web/vmware/downloads. VMWare Player (free for non-commercial use) may also be used, but has limited functionality (i.e. multiple disks cannot be added to a Live Boot session).

**Important:** VMWare must be activated at the program splash screen on first run.
INSTALLATION

It is recommended that Forensic Explorer and Mount Image Pro be installed and run with local administrator user rights. Run the setup files and follow the installation instructions. To set Forensic Explorer and Mount Image Pro to run as administrator, right click on the desktop icons and select Properties > Compatibility > Run this program as an administrator.

Important: Mount Image Pro installs two system drivers which require a reboot of the forensic workstation. Once installed, run Mount Image Pro and check that the driver status in the information bar at the bottom of the GUI.

FORENSIC EXPLORER MODULE OVERVIEW

Forensic Explorer is made up of modules which are access via tabs at the top of the program GUI. Each module contains a toolbar where analysis functions are launched. Within a module, right click in a data view window to access a drop down menu of available options relevant to that window.

1.1.1 EVIDENCE MODULE

The Evidence module is the default window that appears when Forensic Explorer is run. The Evidence module is where a case is created, opened or previewed and evidence is added. Evidence can be added in the form of a physical device, a forensic image or individual files.

To add a forensic image, select the Add Image button. When evidence is added, the Evidence Processor window enables the investigator to select and run automated processing tasks. This includes a Triage, which sends registry files to the Registry module, automatically bookmarks items of interest and uses this information to populate the Triage report in the Reports module.

For more information on the Evidence module see Chapter 10 of the Forensic Explorer User Guide.

1.1.2 FILE SYSTEM MODULE

The File System module is typically where most the forensic analysis will be conducted. Use the branch plate, filtering, highlight and sorting functions to navigate around the filesystem. Use the various data views, such as gallery, text, hex and display to examine file content. The toolbar menu gives access to programs that assist with automated analysis, including tasks such as folder recovery, file carving, file signature analysis, skin tone analysis and more.

For more information on the File System module see Chapter 11 of the Forensic Explorer User Guide.

1.1.3 KEYWORD SEARCH

The Keyword Search module allows a low-level search across raw case data for user created search expressions. Keywords can be simple text words or more complex search formulas such as Regular Expression (RegEx), and hexadecimal values. User CTRL+N from any module to add a new keyword, or import lists of keywords from the Keyword module, Keyword Management toolbar button.

For more information on the Keyword Search module see Chapter 13 of the Forensic Explorer User Guide.
1.1.4 INDEX SEARCH

The Index Search module uses dTSearch indexing technology to create a real-time keyword searchable index. The index can also be exported and used as a dictionary to break passwords.

For more information on the Index Search module see Chapter 14 of the Forensic Explorer User Guide.

1.1.5 EMAIL MODULE

The email module supports the analysis of Microsoft .PST files. PST files can be passed into the Email module by right clicking on a selected file and using the Send to Module > Email option.

For more information on the Email module see Chapter 15 of the Forensic Explorer User Guide.

1.1.6 REGISTRY MODULE

The Registry module is used to expand and examine Windows registry files. A Windows registry can contain a great deal of information that can be of value to the forensic investigator, including computer and user information. The toolbar buttons automate the process of extracting data from relevant keys.

For more information on the Registry module see Chapter 16 of the Forensic Explorer User Guide.

1.1.7 BOOKMARKS MODULE

Bookmarks are used to identify 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. To create a bookmark, select the item of interest, right click > add bookmark, choose a folder where it will be saved within the Bookmark module and include any comments associated to it.

Important: Forensic Explorer Reports are generated from Bookmarked items.

For more information on the Bookmarks module see Chapter 17 of the Forensic Explorer User Guide.

1.1.8 REPORTS

Reports are generated from bookmarked items. The Report Editor is used to design a report and populate it with data from the specified bookmark folders. Reports can be saved as templates for use in future investigations. Default templates, such as the Triage report, are provided with Forensic Explorer for fast access by the investigator. Any report component can be easily moved or edited from one report to another. Hyperlinks can be associated to a file of interest within a report, with the actual file being exported when it is finalized and created. Reports can be exported as DOC, RTF, PDF, and HTML formats.

For more information on the Reports module see Chapter 18 of the Forensic Explorer User Guide.
1.1.9 SCRIPTS

Forensic Explorer sits on top of a Delphi scripting language. Scripts are written and run in the scripts module, or launched in other modules via toolbar buttons or by other scripts.

For more information on the Scripts module see Chapter 19 of the Forensic Explorer User Guide.

LIVE BOOT

Forensic Explorer Live Boot enables an investigator to boot a forensic image or write-protected physical hard drive containing a Windows, Linux or MAC Operating System.

To Live Boot you need the following software installed:


2. VMWare Workstation or VMware Player, https://my.vmware.com/web/vmware/downloads (Player is free for non-commercial use. Player does not support the addition of additional disks within the virtual machine);

   OR,

   Oracle Virtual Box, https://www.virtualbox.org (Recommended: Live Boot of MAC will work only with VirtualBox).

Ensure that the forensic image file is an image of a bootable file system (Windows, UNIX or MAC) and that it contains a Master Boot Records (booting of logical volumes is not currently supported).

Click the Live Boot button in the File System module and follow the onscreen instructions.

For more information on Live Boot see Chapter 28 of the Forensic Explorer User Guide.
# Chapter 1 - Introduction

## In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 1 - INTRODUCTION</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Introducing Forensic Explorer</td>
<td>16</td>
</tr>
<tr>
<td>1.2 Supported file formats</td>
<td>16</td>
</tr>
<tr>
<td>1.3 Supported file systems</td>
<td>16</td>
</tr>
<tr>
<td>1.4 Key program features</td>
<td>17</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Type</th>
<th>Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple DMG</td>
<td>.DMG</td>
</tr>
<tr>
<td>DD or RAW</td>
<td>.DD, .BIN, .RAW</td>
</tr>
<tr>
<td>EnCase®</td>
<td>.E01, .Ex01, .L01, .Lx01</td>
</tr>
<tr>
<td>Forensic File Format</td>
<td>.AFF</td>
</tr>
<tr>
<td>FTK®</td>
<td>.E01, .AD1</td>
</tr>
<tr>
<td>ISO</td>
<td>.ISO</td>
</tr>
<tr>
<td>Macquisition</td>
<td>.00001</td>
</tr>
<tr>
<td>Microsoft VHD</td>
<td>.VHD</td>
</tr>
<tr>
<td>NUIX</td>
<td>.MFS</td>
</tr>
<tr>
<td>ProDiscover®</td>
<td>.EVE</td>
</tr>
<tr>
<td>Safeback® v2</td>
<td>.001</td>
</tr>
<tr>
<td>SMART</td>
<td>.S01</td>
</tr>
<tr>
<td>VMWare®</td>
<td>.VMD, .VMDK</td>
</tr>
<tr>
<td>Xways Container</td>
<td>.CTR</td>
</tr>
</tbody>
</table>

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 analyze data at a text or hexadecimal level. 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

<table>
<thead>
<tr>
<th>CHAPTER 2 - 30 DAY EVALUATION VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 30 day evaluation version</td>
</tr>
<tr>
<td>2.1.1 Installation</td>
</tr>
<tr>
<td>2.1.2 Limitations</td>
</tr>
<tr>
<td>2.2 Activating the 30-DAY evaluation version</td>
</tr>
<tr>
<td>2.2.1 Online Activation (30 day Evaluation)</td>
</tr>
<tr>
<td>2.2.2 Offline Activation (30 day evaluation)</td>
</tr>
</tbody>
</table>
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):
A successful activation message will display the following screen, as shown in Figure 2 below:

![Figure 2, 30-day evaluation version successful activation message](image)

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](http://www.forensicexplorer.com).
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;
2. Click on the Export button to export and save the license file "GetData.GDActRequest":

3. Using a 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

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

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

<table>
<thead>
<tr>
<th>SECTION</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Purchase</td>
<td>28</td>
</tr>
<tr>
<td>3.1.1</td>
<td>Purchase Online</td>
<td>28</td>
</tr>
<tr>
<td>3.1.2</td>
<td>Purchase Orders</td>
<td>28</td>
</tr>
<tr>
<td>3.1.3</td>
<td>Resellers</td>
<td>28</td>
</tr>
<tr>
<td>3.2</td>
<td>License maintenance</td>
<td>29</td>
</tr>
<tr>
<td>3.2.1</td>
<td>Purchase License Maintenance</td>
<td>29</td>
</tr>
</tbody>
</table>
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:

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

<table>
<thead>
<tr>
<th>CHAPTER 4 - INSTALLATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 System requirements .................................................................</td>
</tr>
<tr>
<td>4.2 Download .........................................................................................</td>
</tr>
<tr>
<td>4.3 Installation .....................................................................................</td>
</tr>
<tr>
<td>4.3.1 Installed files ................................................................................</td>
</tr>
<tr>
<td>4.3.2 Non-English installation ...............................................................</td>
</tr>
<tr>
<td>4.4 Uninstall Forensic Explorer ..............................................................</td>
</tr>
</tbody>
</table>
4.1 SYSTEM REQUIREMENTS

Forensic Explorer minimum recommendations:

- Windows 7 or above;
- Pentium i5 processor or above;
- 16GB RAM;
- Forensic Explorer is 64bit (version 3.5.7.5134 and above).

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

2. A successful install will display the following screen. Click **Finish** to confirm.
3. Run Forensic Explorer from the installed desktop icon:

![Desktop icon](image)

### 4.3.1 INSTALLED FILES

#### PROGRAM PATH

The default Forensic Explorer installation folder is:

```
C:\Program Files\GetData\Forensic Explorer vX\n```

#### WORKING PATH

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

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

- **AppLogs**: Forensic Explorer usage logs.
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.

REGISTRY KEYS

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

To uninstall Forensic Explorer:

- Open the Windows Control Panel and in the Programs section use the Uninstall a program option.

The following window will display:

Figure 15, Uninstall process

A successful removal will show the following message:

Figure 16, Successful un-install

Uninstalling Forensic Explorer removes the installation from the C:\Program Files\ folder (check this folder for residual items such as log files that are not automatically removed and delete them as needed.)

The working path: \My Documents\Forensic Explorer\ where case file data is NOT automatically removed and if it is no longer required can be manually deleted.
Chapter 5 - Dongle Activation

In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 5 - DONGLE ACTIVATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Dongle activation of the purchased version .......................................................... 40</td>
</tr>
<tr>
<td>5.1.1 Successful dongle activation .......................................................... 41</td>
</tr>
<tr>
<td>5.1.2 Troubleshooting Dongle Activation .................................................. 41</td>
</tr>
<tr>
<td>5.2 Activate a Remote Computer .......................................................... 44</td>
</tr>
<tr>
<td>5.3 Applying maintenance updates to your Wibu dongle ........................................ 45</td>
</tr>
</tbody>
</table>
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 17, 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 18 below. Include this number in correspondence with GetData:

Figure 18, 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:

![Forensic Explorer Splash Screen](image)

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 29 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 19 below:
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.

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

The CodeMeter Control Center will open, shown in Figure 21 below:
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 22 below:

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:

2. Run CodeMeter WebAdmin by browsing to http://localhost:22350
3. Select Configuration > Server Configuration from the menu, as shown in Figure 23 below:

Figure 23, CodeMeter WebAdmin

4. In the Network Sever window click Enable 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:


8. Browse to [http://localhost:22350](http://localhost:22350) and select the Configuration tab:

```
Figure 24, Wibu CodeMeter Local Host Configuration
```

9. In the Basic menu click the **add new server** 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, that 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 25 below. The existing Maintenance expiration date is displayed in the Maintenance column:

   ![GetData License Manager](image)
   
   **Figure 25, 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 .......................................................................................................................... 48

6.2 GetData’s Forensic Imager .................................................................................................... 49

6.2.1 Installation ....................................................................................................................... 49

6.2.2 System Requirements ..................................................................................................... 49

6.2.3 Protected Disk Areas - HPA and DCO ......................................................................... 49

6.2.4 Running Forensic Imager ............................................................................................... 50

6.2.5 1. Selecting the source .................................................................................................... 51

6.2.6 2. Selecting the destination ............................................................................................ 52

6.2.7 3. Progress ...................................................................................................................... 56

6.2.8 4. Log file ....................................................................................................................... 57

6.2.9 Bad Sectors and error reporting ..................................................................................... 57
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 26 below is a Tableau USB hardware write block. The source media, an 8 GB Kingston USB drive is attached and ready for acquisition:

Figure 26, 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.

(1)
6.2.4 RUNNING FORENSIC IMAGER

Forensic Imager is 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 27, Forensic Imager below:

![Figure 27, Forensic Imager](image)

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 28, 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)
This is because manufacturers 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 in 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 29 below, is where the parameters for the image file are set, including type, compression, name, location etc.

**Figure 29, 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 originates 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”. 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 30, EnCase® header

![EnCase® header diagram](image)

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 consider 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 later (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.


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.


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

After 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 31 below:

Figure 31, 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:** 3370edc5662703534d3ad539d49b7f0ca86f559b7faa3c4dc7f7290056d039
- **Verify MD5Hash:** 94ED73DA0856F2BAD16C1D6CC320DBFA
- **Verify SHA1Hash:** 3370edc5662703534d3ad539d49b7f0ca86f559b7faa3c4dc7f7290056d039

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

<table>
<thead>
<tr>
<th>CHAPTER 7 - FORENSIC EXPLORER INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 Modules ..................................60</td>
</tr>
<tr>
<td>7.1.1 Undocking and docking modules ....61</td>
</tr>
<tr>
<td>7.2 Module data views ..........................63</td>
</tr>
<tr>
<td>7.2.1 Undocking and docking data views ...63</td>
</tr>
<tr>
<td>7.3 Customizing layouts .......................65</td>
</tr>
<tr>
<td>7.3.1 Save a custom layout ...................65</td>
</tr>
<tr>
<td>7.3.2 Load a custom layout ....................65</td>
</tr>
<tr>
<td>7.3.3 Default layout ..........................65</td>
</tr>
</tbody>
</table>
# 7.1 MODULES

The Forensic Explorer interface is broken down into **modules** which separate the program's 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:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Function</th>
<th>Chapter &amp; Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
<td>Case management.</td>
<td>Chapter 10</td>
</tr>
<tr>
<td>File System</td>
<td>Detailed analysis of file systems added to the case.</td>
<td>Chapter 11</td>
</tr>
<tr>
<td>Artifacts</td>
<td>Artifacts can include browsing history, char, call history, Operating System records, and other potential evidence.</td>
<td>Chapter 12</td>
</tr>
<tr>
<td>Keyword Search</td>
<td>Keyword search raw case data using simple or RegEx keywords.</td>
<td>Chapter 13</td>
</tr>
<tr>
<td>Index Search</td>
<td>Create and search indexed data using dtSearch technology.</td>
<td>Chapter 14</td>
</tr>
<tr>
<td>Email</td>
<td>Examine PST files.</td>
<td>Chapter 15</td>
</tr>
<tr>
<td>Bookmarks</td>
<td>Add investigator bookmarks to document the analysis.</td>
<td>Chapter 17</td>
</tr>
<tr>
<td>Reports</td>
<td>Create reports.</td>
<td>Chapter 18</td>
</tr>
<tr>
<td>Scripts</td>
<td>Program, manage and run scripts against case data.</td>
<td>Chapter 19</td>
</tr>
</tbody>
</table>
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 19.4 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 32 below:

![Figure 32, Un-docking a module](image)

**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 33 below:
Figure 33, Re-dock a module tab

Re-dock by dragging the module back into the top bar.
### 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 34 below:

Figure 34, 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 35 below:
Figure 35, 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 36 below:

Figure 36, 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 bar of the program click on the Forensic Explorer button to open the drop down menu and select Layout > Save Layout, as shown in Figure 37 below:

   Figure 37, Accessing the Layout Options

   ![Forensic Explorer layout options](image)

   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 bar of the program click on the Forensic Explorer button to open the drop down menu and select Layout > Load Layout, as shown in Figure 37.

   2. Select the desired .xml layout file and click the Open button.

7.3.3 DEFAULT LAYOUT

To return to the default layout:

In the top bar of the program click on the Forensic Explorer button to open the drop down menu and select Layout > Default Layout, as shown in Figure 37.
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.

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

*Figure 38, Forensic Explorer processes window*

![Processes List](image)

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 39, 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 40 below:

**Figure 40, Setting Logging and Priority options**

![Screenshot of the 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 41, Access Process Log Files**

![Screenshot of Process Log Access]

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 bottlenecks 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 42, Display of a Reference in Forensic Explorer

![Reference Library](image)

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 43, adding a Reference Library button to the toolbar below:

Figure 43, adding a Reference Library button to the toolbar

![Toolbar](image)

A Reference Library button is then added to the File System module toolbar.
Figure 44, 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 required files:

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

The Fixed References.txt file is populated by GetData.

**WARNING:** The content of this file is replaced upon each new install of Forensic Explorer and should not be used to store personal references.

To remove these references from display, comment the content of the file by starting each line with //, or remove the content and save it as a blank file.

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

The My References.txt file is where the investigator can add personal references. This file will not be modified on installation of a new Forensic Explorer version.

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

Add personal references to the My References.txt file 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},
year={2005},
publisher={Addison-Wesley},
pages={121},
},
```

Additional information about the BiBTex structure can be found at:

- [http://en.wikipedia.org/wiki/BibTeX](http://en.wikipedia.org/wiki/BibTeX), or;
7.6.3 ADDING A REFERENCE TO THE REFERENCE LIBRARY

There are several 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 44 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 45, adding a Reference item

When the Create button is pressed, the information in the window is written into the My 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 “MY REFERENCES.TXT” FILE

The My 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.
The **My References.txt** file is for personal references. This file will not be modified when a new version of Forensic Explorer is installed (the **Fixed References.txt** is populated by GetData and will be replaced on each new install).

### 3. COPY AND PASTE FROM A 3RD PARTY SITE


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 **My 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/](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:

  \[url=\{C:\Program Files\GetData\Forensic Explorer v4\Forensic Explorer User Guide.en.pdf\},\]

- If the file is 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

<table>
<thead>
<tr>
<th>SECTION</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1 Data views summary</td>
<td></td>
<td>75</td>
</tr>
<tr>
<td>8.1.1 Components of a data view</td>
<td></td>
<td>76</td>
</tr>
<tr>
<td>8.1.2 Data views relationships in the File System module</td>
<td></td>
<td>76</td>
</tr>
<tr>
<td>8.2 Tree view</td>
<td></td>
<td>78</td>
</tr>
<tr>
<td>8.2.1 Navigating Tree view</td>
<td></td>
<td>78</td>
</tr>
<tr>
<td>8.2.2 Tree view filter</td>
<td></td>
<td>78</td>
</tr>
<tr>
<td>8.2.3 Branch plate</td>
<td></td>
<td>79</td>
</tr>
<tr>
<td>8.3 List view</td>
<td></td>
<td>81</td>
</tr>
<tr>
<td>8.4 Disk view</td>
<td></td>
<td>82</td>
</tr>
<tr>
<td>8.4.1 Resizing the Disk view display</td>
<td></td>
<td>82</td>
</tr>
<tr>
<td>8.4.2 Color Coded Content</td>
<td></td>
<td>83</td>
</tr>
<tr>
<td>8.4.3 Navigating Disk view</td>
<td></td>
<td>85</td>
</tr>
<tr>
<td>8.4.4 Add Partition</td>
<td></td>
<td>87</td>
</tr>
<tr>
<td>8.4.5 Selecting data in Disk view</td>
<td></td>
<td>88</td>
</tr>
<tr>
<td>8.5 Gallery view</td>
<td></td>
<td>90</td>
</tr>
<tr>
<td>8.5.1 Gallery View Folder Level Filtering</td>
<td></td>
<td>90</td>
</tr>
<tr>
<td>8.5.2 Gallery View – File Level Filtering/Sorting</td>
<td></td>
<td>91</td>
</tr>
<tr>
<td>8.5.3 Caching thumbnails to disk</td>
<td></td>
<td>93</td>
</tr>
<tr>
<td>8.5.4 Increase the number of graphics displayed</td>
<td></td>
<td>93</td>
</tr>
<tr>
<td>8.5.5 Working with data in Gallery view</td>
<td></td>
<td>93</td>
</tr>
<tr>
<td>8.5.6 Blur</td>
<td></td>
<td>94</td>
</tr>
</tbody>
</table>
### 8.1 Data Views Summary

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

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

### 8.1.1 COMPONENTS OF A DATA VIEW

**Figure 46, 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 47, Relationships between data views

Key:

- **Multi relationship.** A selection in one view changes the selection in all other connected views.

- **A single relationship.** A change in the parent view changes the view in the child view.
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 per the module, i.e.:

<table>
<thead>
<tr>
<th>Module</th>
<th>Tree view Name</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System</td>
<td>Folders</td>
<td>Chapter 11</td>
</tr>
<tr>
<td>Keyword Search</td>
<td>Keyword Tree</td>
<td>Chapter 13</td>
</tr>
<tr>
<td>Bookmarks</td>
<td>Bookmark Tree</td>
<td>Chapter 17</td>
</tr>
<tr>
<td>Registry</td>
<td>Registry Tree</td>
<td>Chapter 16</td>
</tr>
</tbody>
</table>

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 48:
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 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.
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 per the module, i.e.:

<table>
<thead>
<tr>
<th>Module</th>
<th>List View Name</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System</td>
<td>File List</td>
<td>Chapter 11</td>
</tr>
<tr>
<td>Keyword Search</td>
<td>Keyword Result List</td>
<td>Chapter 12</td>
</tr>
<tr>
<td>Bookmarks</td>
<td>Bookmarks List</td>
<td>Chapter 17</td>
</tr>
<tr>
<td>Registry</td>
<td>Registry List</td>
<td>Chapter 16</td>
</tr>
</tbody>
</table>

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 50, 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 51, 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:
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](http://en.wikipedia.org/wiki/Web_colors)):

- The start sector of a file
- Currently selected sector
- One type overlays another

<table>
<thead>
<tr>
<th>Color Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔴</td>
<td>MBR/VBR (Red)</td>
</tr>
<tr>
<td>🟤</td>
<td>FAT 1 (DarkViolet)</td>
</tr>
<tr>
<td>💜</td>
<td>FAT 2 (WebViolet)</td>
</tr>
<tr>
<td>🟣</td>
<td>$MFT (DarkViolet)</td>
</tr>
<tr>
<td>🟢</td>
<td>System files (WebTomato)</td>
</tr>
<tr>
<td>🌟</td>
<td>$MFT resident file (the file overlays the $MFT)</td>
</tr>
<tr>
<td>🌃</td>
<td>Folder (Deepskyblue)</td>
</tr>
<tr>
<td>🉐</td>
<td>Allocated File (CornFlowerBlue)</td>
</tr>
<tr>
<td>🅿️</td>
<td>Unallocated space (LtGray)</td>
</tr>
<tr>
<td>🟤</td>
<td>Deleted file (A deleted file overlays unallocated space)</td>
</tr>
<tr>
<td>🔴</td>
<td>Carved file (DarkOrange: Carved file overlays unallocated space)</td>
</tr>
</tbody>
</table>

### 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 19 - 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 53, Right-click Disk View menu links to scripts**

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
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 59 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 pace.

KEYBOARD NAVIGATION

The following commands are available for navigation in Disk view:

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 54, Disk view Goto window

- Select the **Unit** required, Byte, Sector or Cluster

- Select the **Start** position on the disk:
  - Beginning of Device (i.e. go forwards from the first sector)
  - Current Sector
  - End of Device (i.e. go backwards from the last sector)

- Enter the **End** position. This can be entered either as a **Count** of the unit required (byte, sector cluster), or a disk **Sector**.

**GOTO Example**, Figure 55 below:

- The **currently select sector** is 445;

- The **sector to GOTO** is 89, which is -356 from the currently select sector.
8.4.4 ADD PARTITION

It is possible in Forensic Explorer to add an unallocated partition (for example, when a drive has been formatted but the unallocated partition structure is still intact).

To Add Partition:

1. In Disk View, locate the required **Volume Boot Record (VBR)**:

   - **Manually**: Users who are familiar with the VBR format and disk position may use Disk View to find the sector manually;

   *Figure 56, NTFS VBR in HEX view*

   - **File Carve**: To automate the search for Volume Boot Records, File Carve for Operating System volumes, as shown in Figure 57 below:
The file carve will return the position of found VBRs with the file name representing the sector number on the device:

2. In Disk View, click on the sector of the VBR, right click and select Add Partition. The partition will then be added to the File System Folder tree.

8.4.5 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 59 below. This enables other views, such as HEX view to see the selected range;

**Figure 59, 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 60 below;

**Figure 60, 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]

Gallery view is also present in Bookmarks and Email modules. Gallery view is fast ways to thumbnail graphics located in the case.

Figure 61, Gallery view thumbnails

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 GALLERY VIEW FOLDER LEVEL FILTERING

Gallery view content is first controlled by the selection made in the File System module Folder 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, as shown in Figure 62 below.
8.5.2 GALLERY VIEW – FILE LEVEL FILTERING/SORTING

In addition to Folder level filtering described above, the content and sort of Gallery view can also be determined by filters and sorting in the File List. For example, in Figure 63 below, the File List has had a Text Typing filter applied for the word “Cat” which filters out only files containing that word in the file name:
Figure 63, Gallery view filtered or sorted by a File List selection

Any filter or sort applied in the File List will dictate the content of the Gallery view. The result of applying the above filter is shown in Figure 64 below where the Gallery view contains only graphics that match the filter:

Figure 64, Gallery view with a File List filter applied
TIP: To more clearly see File List filters and their effect on Gallery view it can assist if the Gallery view is detached and viewed on a second monitor so that both the File List and Gallery view can be viewed simultaneously.

### 8.5.3 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 Programs 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.

### 8.5.4 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 65, 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).

### 8.5.5 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**.

### 8.5.6  **BLUR**

**Gallery view blur** enables the investigator to blur the content of a graphic both in the Gallery view. Once blurred in the Gallery view, the graphic will also be blurred in Display view and Reports.

The blur is intended to distort the fine detail of a graphic. It is most commonly used in child protection cases where display of a full resolution graphic may not be possible on legal or ethical grounds.

To **blur a graphic**:

1. In the **File System module Gallery view**, use the mouse to select the required picture in the Gallery view (or use the CRTRL, SHIFT and mouse to select multiple graphics).

2. In the Gallery view toolbar, click on the blur button. The graphic will blur both in Gallery and Display view, as shown in Figure 66 below.

To **un-blur a graphic**:

1. In the File System module Gallery view, click on the blurred graphic.

2. In the Gallery view toolbar, click on the un-blur button. The graphic will now display at normal resolution in both Gallery and display view.

*Figure 66, Gallery view blur*

Blur can also be associated with keyboard hotkeys.
8.5.7 CLASSIFICATION KEYS [0-9, -] (HOTKEYS)

In some circumstances the investigator may need to manually classify graphics based on their content. A classification can be added to a graphic using a keyboard shortcut.

To classify a graphic in Gallery View:

1. In Gallery view place a tick in the Classification Keys [0-9, -] checkbox to activate the keyboard keys 0 to 9 and -. A classification legend will also appear to the right of the Gallery view graphics (see Figure 69 below).

2. Right-click in the file list and select Classify > Enable Classification

3. Pressing a keyboard key from 0 to 9 will classify the currently selected according to the keyboard number pressed. (- removes the classification, see below).

4. Visual confirmation of the classification is provided:
   a. In the bottom right hand corner of the information bar of the Gallery view graphic is the classification number.
   b. The background color of the graphic changes according to the classification.
   c. The classification legend will increment with each classified item.
Figure 69, Gallery View classification

d. A Classification column can also be added to the File List view showing the classification number:

Figure 70, File List Classification column

To remove classification from a graphic in Gallery View:

1. In Gallery view place a tick in the Classification Keys [0-9,-] checkbox to activate the keyboard keys 0-9 and -:

2. Select the graphic/s with the mouse.

3. Press the – (minus) button on the keyboard.

4. The classification number is removed.

To remove classification from a group of classified files:

1. Use the SHIFT or CTRL key to select a groups of files.
2. **Press the – (minus) button** on the keyboard.

3. The classification for the entire group is removed.

To remove **all classification**:

1. In the File System module click on the Tools button > Clear Column Content > Classification.

2. Classification will be removed from all items.

### 8.5.8 GALLERY CLASSIFICATION FILE INDEX

When manually classifying graphics it can be beneficial to number the display items in order to keep track of the current position.

To change the information displayed under the graphic in Gallery view:

1. Right click in Gallery view and select **Caption** from the drop down menu.

2. Select an available option: FileName, Index, or Blank.

The **index** option adds a numeric counter to the bottom of the Gallery view image, as shown in Figure 71 below:

**Figure 71, Classification with index numbering**

### 8.5.9 CLASSIFICATION AND BOOKMARK USING HOTKEYS [0-9, -]

**Important:** Classification and Bookmarking are separate functions, i.e. you can classify without bookmarking. Note that:

- A file can have only **one Classification**.
- A file can have **multiple bookmarks**.

The Bookmark checkbox in Gallery view becomes active only when the Classification Keys [0-9] checkbox is check (described in 8.5.7 above).

To **hotkey classify then bookmark** a file from **Gallery view**:

1. Right-click and **Classify > Enable Classification**.

2. Check the **Bookmark** checkbox at the top of the Gallery view.
3. Press a hotkey (0 to 9). The item will be **classified** (given a number according to the key pressed) and **bookmarked** to the bookmark folder designated for that key.

The default path for hotkey bookmarks is *My Bookmarks\Pictures\Classification 01, Classification 02*, etc. The bookmark path and folder can be changed in the **Gallery Classification Options** window. To open the **Gallery Classification Options** window, click on the cog icon in the Gallery view toolbar (shown in Figure 68 above):

**Figure 72, Gallery Classification Options**

- **Base Bookmark folder:** Assigns the bookmark folder where items will be bookmarked.
- **Key 1, Key 2, etc.:** Assigns the keyboard number with a bookmark folder.
- **Blur checkbox:** If checked, the hotkey will blur the item in Gallery view.
- **Bookmark Folder:** Assigns the bookmark folder when the item/s will be bookmarked. If the folder does not exist in the Bookmarks module it will be created.
- **Color:** Sets the color of the category number in the gallery view information bar as described in *Error! Reference source not found. Error! Reference source not found.*.

**To re-classify then bookmark:**

1. Check in the **Classification** and **Bookmark** checkboxes at the top of the Gallery view.
2. Highlight the file that needs reclassification and press the new classification key, i.e. 1 to 10.

3. The classification number in the Gallery view overlay (shown in Error! Reference source not found. Error! Reference source not found.) will update.

4. A new bookmark will be created.

5. **Note:** The original bookmark will **not** be removed from original bookmark folder. It is recommended that at the end of the classification process, add the **Classification** column to the Bookmarks module, and sort by classification, and review and remove any bookmarks that no longer belong in the classification folder.

To **remove a bookmark**:

1. Switch to the **Bookmark module**;

2. Select the required bookmark/s with the mouse.

3. Right click and select **Delete Bookmark\'s** from the drop down menu.
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:

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 17 - 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:

![Carving files from Hex view](image_url)
**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 75, Text view tab

The Text tab shows the highlighted item as ASCII text.

Figure 76, Text view
8.8 INFO

The default location of the Info view is in the bottom data view window, access via the Info tab:

Figure 77, Info view tab

The Info view displays the properties of the currently highlighted file. This includes File System information, such as Created, Modified and Access dates, and information about how the file is displayed by Forensic Explorer, such as checked status and file signature. It is a convenient location to quickly view the entire list of properties for a file.

Figure 78, Info data view
8.9 DISPLAY VIEW

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

Figure 79, Display view tab

The File Display tab uses GetData’s Explorer View technology to display the content of the currently highlighted file:

Figure 80, 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:
The following buttons are displayed for audio and video files

![Image of right-click menu]

**8.9.1 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 82 below:

![Image of 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.
8.10 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 83, 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 were 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 per 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](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 time 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 84, 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.

8.10.1 BYTE PLOT EXAMPLES

Microsoft Word document:

Figure 85 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.

JPG Photograph:

Figure 86 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 86, Byte Plot and Character Distribution of a .jpg file

RTF document:

Figure 87 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 much of the file appears as text.

Figure 87, Byte Plot and Character Distribution of an .rtf file

ZIP file:

Figure 88 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 8.8, Byte Plot and Character Distribution of a .zip file
8.11 FILESYSTEM RECORD VIEW

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

Figure 89, 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 90 below:

Figure 90, Filesystem Record view
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 90 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.
8.12 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. File types support include:

- OLE (.doc, .xls, .ppt);
- Open XML format (Office 2007 .docx, .xlsx, .pptx);
- JPEG;
- ZIP.

Figure 91 below show the metadata of a Microsoft Word .doc file:

* Starting with Microsoft Office 2007, the Office Open XML file format has become the default for Microsoft Office. These file types, e.g. docx, are compressed container files for XML content.

Viewing a docx file in the File Metadata view will show the properties of the compressed file. To view the metadata of the content files it is first necessary to Expand Compound Files so that the metadata for
individual content files can be examined (in docx files, `core.xml` and `app.xml` hold much of the commonly used metadata).

Metadata for both Office and Office 2007 files can be extracted to columns by running the **Extract Metadata to Columns** script (see below) without the need to first expand compound files.

### 8.12.1 EXTRACT METADATA

**EXTRACT METADATA - EVIDENCE PROCESSOR**

The option to **Extract Metadata** can be selected in the **Evidence Processor** when evidence is added to a case:

*Figure 92, Evidence Processor - Extract Metadata*

Selecting the Extract Metadata option gives access to the configuration window where it is possible to select individual metadata types and to bookmark results:
The metadata extraction options are also available from the File System module, Extract Metadata toolbar button, shown below:

**EXTRACT METADATA – ANALYSIS PROGRAMS**
Figure 94, Metadata extraction scripts, File System module, Extract Metadata menu

Manage the visible metadata columns using the **Show/Hide Metadata Columns** menu option under the **Extract Metadata** or **Tools** button.

A separate menu is available under the **File System module, Extract Metadata button** that will bookmark metadata.

Figure 95, File System > Analysis Programs > Bookmark Metadata

**METADATA EXTRACTION SCRIPT**

Either of the methods described above runs the metadata extraction script:

```
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). Bookmarks are added to the Bookmarks module under the **Script Output** folder.
The default location for File Extent view is the bottom data view window, accessed via the File Extent tab:

![File Extent](image)

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 97 below is a fragmented file with three data runs:

![File Extent data view](image)

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

<table>
<thead>
<tr>
<th>CHAPTER 9 - WORKING WITH DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1 Working with data</td>
</tr>
<tr>
<td>9.2 Highlighted and checked items</td>
</tr>
<tr>
<td>9.2.1 Highlighted items</td>
</tr>
<tr>
<td>9.2.2 Checked items</td>
</tr>
<tr>
<td>9.3 Add and edit bookmarks</td>
</tr>
<tr>
<td>9.4 Open with</td>
</tr>
<tr>
<td>9.5 Expand compound file</td>
</tr>
<tr>
<td>9.5.1 To expand compound files</td>
</tr>
<tr>
<td>9.5.2 Identifying Expanded Compound Files</td>
</tr>
<tr>
<td>9.5.3 Filtering compound files</td>
</tr>
<tr>
<td>9.6 Export</td>
</tr>
<tr>
<td>9.6.1 Export Folders and Files</td>
</tr>
<tr>
<td>9.6.2 Export Logical Evidence File (.L01)</td>
</tr>
<tr>
<td>9.6.3 Export Delimited Rows (.csv or .tab)</td>
</tr>
<tr>
<td>9.7 Send to Module</td>
</tr>
<tr>
<td>9.8 Columns</td>
</tr>
<tr>
<td>9.9 Sorting</td>
</tr>
<tr>
<td>9.10 Flags</td>
</tr>
<tr>
<td>9.11 Filtering data</td>
</tr>
<tr>
<td>9.11.1 Date range filter</td>
</tr>
<tr>
<td>9.11.2 Column filter tool</td>
</tr>
</tbody>
</table>
9.11.3 Explorer Tool .................................................................................................................. 137
9.11.4 Folders Filter .................................................................................................................. 137
9.12 Copy rows to clipboard ...................................................................................................... 137
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 accessed by a right-click menu, as shown Figure 98 below:

Figure 98, 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.

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 99, Highlighted items

![Highlighted items](image)

The information bar at the bottom of the list view identifies the number of visible, highlighted and checked items in the File List.

### 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 100 below:
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 17 - 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.

Important: An expanded compound file in Forensic Explorer is currently limited to the first 100MB. To access the entire content the parent compound file must be exported to disk and expanded using tools such as WinZip, WinRAR or 7Zip.

This limitation is being addressed. Contact support@getdata.com for more information.

9.5.1 TO EXPAND COMPOUND FILES:

Compound files are expanded via the script:

Scripts > File System > Expand Compound Files.pas

The script can be executed using the Expand Files button in the File System module toolbar (or via the drop down menu under the File System > Analysis Programs button):

Figure 101, File System toolbar, Expand Compound Files

The script opens the options window shown in Figure 102 below:
To expand an individual compound file using right-click:

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

### 9.5.2 IDENTIFYING EXPANDED COMPOUND FILES

Once a compound file has been expanded the file icon changes to a container which holds the expanded content (like 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.

### 9.5.3 FILTERING COMPOUND FILES

To display only expanded files in the File System module:
In the File System module Folders Filter, select the required filter, for example:

- **Expanded**: Displays all expanded files;
- **Jump List (Windows)**: Shows expanded MS Jump List files;
- **Thumbs.db**: Shows expanded Thumbs.db files; etc.

**Important**: Applying a Folders Filter during the expand process will slow the process due to multiple GUI refresh. It is recommended that the Folders Filter be turned off prior to the expand process.

### 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 103, 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 19 - 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](http://www.guidancesoftware.com)) and .AD1 (Access Data - [www.accessdata.com](http://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:
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.

MD5: If selected, an MD5 is calculated for each file and stored within the L01.

Compression: Sets the level of compression for the image file.

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 105, 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 106, 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.

### 9.7SEND 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 16.2 for more information).

### 9.8COLUMNS

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;

![Column Headers Window](Image)

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 8.12.1 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 108, 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 [column name]” or “Sort Descending [column name]”:

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 and a “1” will indicate that this is the first sorting column. 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 “2” 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 109, 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:
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”.

---

*Copyright GetData Forensics Pty Ltd 2010 - 2019, All rights reserved.*
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 111 below:

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 112 below:
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 19 - 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 113 below.
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:

To modify the time scale, when the magnifying glass with plus sign is displayed (see Figure 114 above) double click to range drill down the scale (e.g. year to day, day to hour, etc.);

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

To close the date range filter, click the icon.

**9.11.2 COLUMN FILTER TOOL**

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

To access the column filter tool:
1. Right click on a List view window;

2. From the drop down menu, select "Column Filter Tool";

3. The text filter then appears above the List view column headings, as shown in Figure 115 below.

To apply a column filter:

1. Type into the filter field above the column heading:
    a. A Requires A-Z characters;
    b. 1 Requires numbers 1 – 9.
    c. Use >, =, or < symbols to list data greater than, equal to or less than the typed number;
    d. D 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 115 below;

Figure 115, Column 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:
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 117 below:

![Figure 117, NOT column filter active](image)

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

![Figure 118, RegEx column filter](image)

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

DOS Mask

File masks consist of any combination of three general symbols types:

- Fixed characters, such as letters, numbers and other characters allowed in file names;
- ? (question-mark character) that stands in for any single character;
- * (asterisk character) that stands in for any number of various characters.

For example, file mask:

?at.jpg Refers to all files with three letters in their name ending with at, and .jpg extension, matching:

cat.jpg
mat.jpg
hat.jpg
rat.jpg

and all other files starting with any character and ending with at.jpg.

*e.jpg Refers to all .jpg files that start with h, end with e and contain any number (including zero) in between, matching:

ashe.jpg
hue.jpg
here.jpg
house.jpg, etc.

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

<table>
<thead>
<tr>
<th>Flags Text Filter Value</th>
<th>Flags shown</th>
</tr>
</thead>
<tbody>
<tr>
<td>=1</td>
<td>Shows column 1 (red)</td>
</tr>
<tr>
<td>=2</td>
<td>Shows column 2 (blue)</td>
</tr>
<tr>
<td>=4</td>
<td>Shows column 3 (yellow)</td>
</tr>
<tr>
<td>=8</td>
<td>Shows column 4 (orange)</td>
</tr>
<tr>
<td>=16</td>
<td>Shows column 5 (green)</td>
</tr>
<tr>
<td>=32</td>
<td>Shows column 6 (pink)</td>
</tr>
<tr>
<td>=64</td>
<td>Shows column 7 (aqua)</td>
</tr>
<tr>
<td>=128</td>
<td>Shows column 8 (brown)</td>
</tr>
</tbody>
</table>

Note: If the equals sign is not used then the results will show the specified color and above.
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 119, Explorer Tool below.

Figure 119, 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 273, 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

<table>
<thead>
<tr>
<th>CHAPTER 10 - EVIDENCE MODULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1  Preview                      ........................................................................................................ 140</td>
</tr>
<tr>
<td>10.2  New case ............................................................. ................................................................ 142</td>
</tr>
<tr>
<td>10.2.1  Managing Investigators .......................................................... ............................................ 143</td>
</tr>
<tr>
<td>10.3  Open an existing case .......................................................... ..................................................... 145</td>
</tr>
<tr>
<td>10.3.1  Recent cases .............................................................. ......................................................... 146</td>
</tr>
<tr>
<td>10.4  Adding evidence .............................................................................................................................. 147</td>
</tr>
<tr>
<td>10.4.1  Adding a Device ......................................................................................................................... 147</td>
</tr>
<tr>
<td>10.4.2  Adding a Remote Device ............................................................. ........................................... 148</td>
</tr>
<tr>
<td>10.4.3  Adding a Forensic image file .......................................................... .......................................... 152</td>
</tr>
<tr>
<td>10.4.4  Adding a registry file ............................................................ ................................................. 152</td>
</tr>
<tr>
<td>10.4.5  Add file ................................................................................................................................. 153</td>
</tr>
<tr>
<td>10.4.6  Add folder .............................................................................................................................. 153</td>
</tr>
<tr>
<td>10.5  Evidence Processor ............................................................. ........................................................... 154</td>
</tr>
<tr>
<td>10.5.1  Processor tasks ......................................................................................................................... 154</td>
</tr>
<tr>
<td>10.5.2  Adjust Time Zone ..................................................................................................................... 158</td>
</tr>
<tr>
<td>10.6  Adding additional evidence to a case ........................................................................................... 158</td>
</tr>
<tr>
<td>10.7  Saving a case ................................................................................................................................. 160</td>
</tr>
<tr>
<td>10.7.1  Auto Save .............................................................................................................................. 160</td>
</tr>
<tr>
<td>10.7.2  Saving or closing a preview .................................................................................................... 161</td>
</tr>
<tr>
<td>10.8  Closing a case .............................................................................................................................. 162</td>
</tr>
</tbody>
</table>
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 120, 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-BA18-6338394721C5]};

- The evidence window in the Evidence module identifies that a preview is in progress with the words “Case: Preview”. The Add Device, Add Image, Add File, Add Folder, Add Group and Remove buttons become active in preparation for adding evidence to the preview, as shown in Figure 121 below:
For information on adding evidence to a preview, see “Adding evidence” on page 147.

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 122, Evidence module, new case button

The “New Case” window will open, as shown in Figure 123 below:

Figure 123, New Case window

**New Case**

- **Case Name**: Case 123
- **Investigator**: Graham Herley
- **Cases Folder**: C:\Users\Owner\Documents\Forensic Explorer\Cases
- **Case Notes**: This is a test case.

**Case Time Zone Settings**

- **TimeZone**: Local Time
- **TimeZone Name**: AUS Eastern Standard Time (-600 mins)
- **Daylight Savings**: AUS Eastern Daylight Time (-660 mins)
- **STD/DLS Bias**: -600 / -660 minutes

**Case Created**: 30-Dec-16 10:40:45 AM

**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.

**Cases Folder** is the location where files for each case are stored.

**Case Notes** are 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 Time Zone Settings** are applied to the entire case. The default is the local time zone. Refer to Chapter 21 for more information about date and time.

**Case Created** identified the date and time that the case is created per 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 35) 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 147.

### 10.2.1 MANAGING INVESTIGATORS

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

![Forensic Explorer drop down menu](image)

Select and edit the investigator as needed:
Figure 125, New Investigator

**Import VCF** is a fast way to import investigator details using the VCard.vcf format.

**Export VCF** export the currently selected investigator to a file in VCard.vcf format.
10.3 OPEN AN EXISTING CASE

To open an existing case,

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

   ![Figure 126, Evidence module, new case button](image)

   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 127 below). Click **Open** to open the case file.

   ![Figure 127, Open Case File](image)

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 128, Select investigator window](image)

   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 129 below:

Figure 129, Evidence module > Cases tab, Open recent cases

<table>
<thead>
<tr>
<th>Case</th>
<th>Details</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>Test Case 3</td>
<td></td>
</tr>
<tr>
<td>Investigator:</td>
<td>Graham Henley</td>
<td></td>
</tr>
<tr>
<td>Created:</td>
<td>06-Jun-12 12:28:11 PM</td>
<td>Less than 1 minute</td>
</tr>
<tr>
<td>Name:</td>
<td>Test Case 2</td>
<td>2 mins</td>
</tr>
<tr>
<td>Investigator:</td>
<td>Graham Henley</td>
<td></td>
</tr>
<tr>
<td>Created:</td>
<td>06-Jun-12 12:25:47 PM</td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td>Test Case 1</td>
<td>3 mins</td>
</tr>
<tr>
<td>Investigator:</td>
<td>Graham Henley</td>
<td></td>
</tr>
<tr>
<td>Created:</td>
<td>06-Jun-12 12:25:00 PM</td>
<td></td>
</tr>
</tbody>
</table>

This is test case 3
10.4 ADDING EVIDENCE

Evidence in Forensic Explorer can be:

- A device (including a remote 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 shown in Figure 130 below:

**Figure 130, 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 manufactures 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 25 - 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 REMOTE 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 AS STAND-ALONE**

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 131, GetData UDP Network Server

Server IP: The IP address of the computer on which the Network Server is running. **IMPORTANT:** When troubleshooting, double check the IP address using CMD line “IPCONFIG” command to ensure the correct machine address;

Server port: The port for communication is 443.

Server Status: 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.

**NETWORK SERVER COMMAND LINE OPTIONS**

The **GetData UDP Network Server** can be deployed from the CMD line on the remote computer with the following switches:

/\Q   Quite Mode (No GUI);

/P:XXXX Specified port number.

**IMPORTANT:** When deployed in **Quite Mode**:

- The **GetData UDP Network Server** will appear as a running process in the Windows Task Manager. The name of the process is the name of the executable (i.e. rename “GetData UDP Network Server” as needed).
• The GetData UDP Network Server can only be terminated by ending the process in the Windows Task Manager.

### DEPLOY THE GETDATA UDP NETWORK SERVER AS A WINDOWS SERVICE

The GetDataNetworkServer can be deployed as a **Windows Service**.

To **install** as a **service**, use the following command line switch:

- `GetDataNetworkServer /install /silent`

To **uninstall** the **service**, use the following switch:

- `GetDataNetworkServer /uninstall /silent`

If a non-default port is required (i.e. a port other than 443) the following key must be added to the registry to specify the port number:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GDStreamService\UDPPort(DWORD) = 443
```

### 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 **Remote** button. The following screen appears:
**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 (default is port 443).

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 133 below:
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 16.2 for more information.

10.4.5 ADD 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.

10.4.6 ADD FOLDER

The add folder button enables the investigator to add a folder full of files to a case (for example, a folder containing Microsoft Word documents). Add Folder will add all files, including subfolders and their contents.

To add a folder 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 Folder button.

3. In the Browse to Folder window, navigate to the required folder and click OK. The Evidence Processing Options window will open. See section 10.5 below. The contents of the selected folder (and subfolders) 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 21 - 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 per the file type.
The Evidence Processor 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 later, the processing window enables the investigator to batch these tasks at the start of the case.

The Evidence Processor window uses the following icons:

- **Parent / Child**: Indicates a parent / child relationship between tasks. A parent task 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.
CUSTOM PROCESSING PROFILES

At the top of the Evidence Processor is a drop down menu and save button that enables the investigator to save and load custom Processing Profiles. Saved profiles are stored as .txml files in the “Documents\Forensic Explorer\Startup” folder. Forensic Explorer will default to the last used task (as stored in the registry).

When a different profile is selected from the drop down menu the following warning message is displayed:

Figure 135, Changing the evidence processing profile

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

The triage process runs scripts that extract data from the File System and Registry files. Items identified are bookmarked and can be seen in the Bookmarks module under the path: My Bookmarks\Triage\Registry. These bookmarks are used to generate the Triage report.

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 136 below):

**Figure 136, Evidence module, Evidence tab, device hash**

A device hash can also be calculated at any time using the Verify Devices script. This script can be run either from the “Analysis Programs” button in the File System module, or directly from the Scripts module. See 22.4 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 after the identification of a file system. For this reason, it is a sub-task of “Search for FileSystems” (as shown in Figure 134 above).

Signature analysis can also be independently run in the File System module. Learn more about signature analysis in Chapter 23.

**File Carve**

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

File carving can only take place after the identification of a file system. For this reason, it is a sub-task of “Search for FileSystems” (as shown in Figure 134 above).

File carving can also be independently run in the File System module. Learn more about file carving in section 24.4.

**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 per the time zone from which the device or forensic image originates.

The default setting is to process the image per **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 to display file date and times per 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 21** for further information.

*Figure 137, 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 138 below:
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 139, Evidence module, save button

Or;

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

Figure 140, Save Case

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

10.7.1 AUTO SAVE

A Forensic Explorer case can be set to auto-save at regular timed intervals. To configure auto-save options, in the Forensic Explorer drop down menu, select Options > Case, as show in Figure 141 below:
Saves are written to the root of the **Case folder**. The current case file is `fe.rsv`.

During the save process a temporary file is written called `~fe.rsv`. On completion of a successful save the temporary file is renamed to `fe.rsv`. Therefore, if a save is not successful, the current case file with be the last successfully written `fe.rsv`.

When a successful auto-save takes place, if the previous saved file was initiated by the user (i.e. by pressing the save button) the file is named `fe.0001.rsv`. If the previous saved file was an auto-save the file is backed up as `fe.0001.auto.rsv`.

### 10.7.2 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 142, Evidence module, Close button

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

Figure 143, 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

<table>
<thead>
<tr>
<th>Chapter 11 - FILE SYSTEM MODULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1  File System module..........................164</td>
</tr>
<tr>
<td>11.2  Toolbar............................................164</td>
</tr>
<tr>
<td>11.3  Folders view....................................164</td>
</tr>
<tr>
<td>11.3.1 Folders icons ..................................165</td>
</tr>
<tr>
<td>11.3.2 ORPHANS ........................................165</td>
</tr>
<tr>
<td>11.4  Categories view.................................166</td>
</tr>
<tr>
<td>11.4.1 Files by Extension..........................166</td>
</tr>
<tr>
<td>11.5  File List view....................................167</td>
</tr>
<tr>
<td>11.5.1 File List icons ...............................167</td>
</tr>
<tr>
<td>11.5.2 File List Metadata Columns .................167</td>
</tr>
<tr>
<td>11.6  Other data views...............................169</td>
</tr>
</tbody>
</table>
11.1 FILE SYSTEM MODULE

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

Figure 144, 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. After this, individual buttons or button groups can be added and removed by running scripts. See Chapter 19 - Scripts Module, for more information on toolbar scripts.

11.3 FOLDERS VIEW

Folders view is 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 145, Folder's 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 24.4 - 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 24.3.2 - NTFS - orphans.
11.4 CATEGORIES VIEW

Categories view is 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 146, 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.

Copyright GetData Forensics Pty Ltd 2010 - 2019, All rights reserved.
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 in the top right hand window of the File System module. File List displays content per the selections make 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:
• 0-5 are normal DOS attributes

• 6-15 are NTFS attributes.

Additional information is available https://msdn.microsoft.com/en-us/library/aa365535(v=VS.85).aspx (Other OS’s are mapped to these when available)

Bit 0:  r - Read only
Bit 1:  h - Hidden
Bit 2:  s - System
Bit 3:  v - Dos Volume
Bit 4:  d - Dos Directory
Bit 5:  a - Archive
Bit 6:  D - Device
Bit 7:  N - Normal
Bit 8:  T - Temporary
Bit 9:  S - Sparse
Bit10:  R - Reparse/Symbolic Link
Bit11:  C - Compressed
Bit12:  O - Offline
Bit13:  I - Not Indexed
Bit14:  E - Encrypted
Bit15> 'X' - Other higher flags (not yet determined), but typically are associated with NTFS system files such as $ObjID etc. that are in the reserved $MFT area, but also can exist on other files.

File Signature: This column receives data after a file signature analysis (see Chapter 23 - 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 8.12.1 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.

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

The File System module Recover Folders and File Carve buttons are used for data recovery. See Chapter 24 for more information.

Figure 147, File System module, Recover Folders and File Carve buttons

11.7.1 SHADOW COPY

The File System module Shadow Copy button is used to add shadow copy volumes to the case. See Chapter 26 for more information.

Figure 148, File System module, Shadow Copy button

11.7.2 CLAM ANTIVIRUS

The Cisco Clam Anti Virus (ClamAV) toolbar button in the File System module enables the forensic investigator to run a virus scan over the case:

Figure 149, File System module, Cisco Clam Anti-Virus

ABOUT CLAMAV


UPDATING THE CLAMAV VIRUS DATABASE (CVD)

ClamAV Virus Database updates are released daily. It is recommended that these files are updated frequently.
CLAMAV VIRUS DATABASE UPDATE BUTTON

To update the ClamAV Virus Database files using the **Update button** (an internet connection is required):

1. Click on the **Options** tab;

2. Select the database path. The default path is `C:\Program Files\GetData\Forensic Explorer v4\ClamAV\database`;

3. Click the **Update** button;

4. A **Command** window will open an commence download of the latest ClamAV database files, as shown in Figure 150, Update of ClamAV database files below:

**Figure 150, Update of ClamAV database files**
5. Exit the Command window.

**CLAMAV VIRUS DATABASE MANUAL UPDATE**

To manually update the ClamAV Virus Database files:

1. Using an internet connected computer, visit the web page: [https://www.clamav.net/downloads](https://www.clamav.net/downloads).
2. In the Virus Database section, download the `main.cvd`, `daily.cvd` and `bytecode.cvd` files.
3. Copy these files into the `C:\Program Files\GetData\Forensic Explorer v4\ClamAV\database` folder.
4. Follow the instructions below to run a scan.

**RUNNING A SCAN**

To run a ClamAV scan of a case:

1. Click the Cisco ClamAv Anti Virus button in the File System module toolbar.
2. Follow the instructions above to update the ClamAV Virus Database files if required.
3. Select the **Source** files to scan: Searchable items, Highlighted items, Checked items;

4. Set the **Scan Options**;

<table>
<thead>
<tr>
<th>Quick Scan</th>
<th>Scans common file types. See: <a href="https://www.clamav.net/documents/how-to-speed-up-clamwin">https://www.clamav.net/documents/how-to-speed-up-clamwin</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan for Potentially Unwanted Applications (PUA)</td>
<td>See: <a href="https://www.clamav.net/documents/potentially-unwanted-applications-pua">https://www.clamav.net/documents/potentially-unwanted-applications-pua</a></td>
</tr>
</tbody>
</table>

5. Select the **Output** options;
Flag infected files with: [Flag Color]  
A flag is added to the File System module

Bookmark infected files  
A bookmark is added to the Bookmarks module under the Virus Scan bookmark folder

Add new column showing infection status  
The Virus Name column is added to the File System and Bookmarks module giving the identified virus name.

6. Click the Scan button to start the scan.

11.7.3 HASHING

The File System module hash buttons are used to hash case file. See Chapter 22 for more information.

Figure 152, File System module, Hash buttons
Chapter 12 – Artifacts Module

In This Chapter

12.1 Artifacts .......................................................................................................................... 177
12.2 Artifacts module ............................................................................................................. 177
12.1 ARTIFACTS

Although widely used in computer forensics, the term Artifact is not well defined. As Vikram et al. discuss, this can result in a “in a lack of standardized reporting, linguistic understanding between professionals” (11).

A broad based definition or an Artifact is ‘an item of digital interest’. In practical terms artifacts can include:

- browsing history;
- call history;
- chat text;
- Operating System records, etc.

The term artifacts is also used to describe the container of the items of digital interest, such as SMS database, a browser history, or a chat history file.

The proliferation of ‘Apps’ has meant that there is more artifact data that ever before, often spread over multiple devices including phones, tablets and computers.

12.2 ARTIFACTS MODULE

The Artifacts module in Forensic Explorer is designed to make artifact records easily accessible by the forensic examiner. Artifacts are extracted using one or more of the following techniques:

1. Extraction of records from SQLite database files (Forensic Explorer does not currently extract deleted records within SQLite files);
2. Extracting of records from Plist or XML format;
3. Carving data from files or unallocated clusters;
4. Other custom extraction.

Artifacts in Forensic Explorer are extracted by scripts. This enables the investigator to examine the exact criteria used to locate the Artifacts. Scripts are located in the path:

```
My Documents\Forensic Explorer v4\Scripts\Artifacts\``
Chapter 13 - Keyword Search Module

In This Chapter

13.1 Keyword search .......................................................... 180

13.2 Keyword management .................................................. 181
  13.2.1 Creating a keyword.................................................. 181
  13.2.2 Edit or delete a keyword.......................................... 183
  13.2.3 Grouping keywords................................................. 184
  13.2.4 Importing keywords............................................... 184
  13.2.5 Running a Keyword Search..................................... 186

13.3 Search results............................................................ 188
  13.3.1 delete a keyword search folder (and keywords)............. 188
  13.3.2 To delete a keyword.............................................. 189
  13.3.3 Note: Why keyword hits differ when compared to EnCase® .................................................. 189

13.4 Keyword result list ..................................................... 190
  13.4.1 Hits.................................................................... 190
  13.4.2 Hit Text................................................................. 190
13.1 KEYWORD SEARCH

The keyword search module is accessed via the “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 154 below:
13.2 KEYWORD MANAGEMENT

13.2.1 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.
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 Expression” (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” (12). 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 ?, +, *, |
**Chapter 13 - Keyword Search Module**

\{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://regexlib.com/](http://regexlib.com/)

**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.

---

**13.2.2 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.

*Copyright GetData Forensics Pty Ltd 2010 - 2019, All rights reserved.*
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.

### 13.2.3 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 156, Add Keyword Group window

![Add Keyword Group window](image)

**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”.

#### 13.2.4 IMPORTING KEYWORDS

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

```plaintext
; Indicates a comment and is ignored in the import
```

*Copyright GetData Forensics Pty Ltd 2010 - 2019, All rights reserved.*
### Keyword Search Module

- **[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:**

```plaintext
; 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:
13.2.5 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 158 below:
Figure 158, New Keyword Search window

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.
13.3 SEARCH RESULTS

The **Keyword Tree** window contains the search results, as shown in Figure 159 below:

![Keyword Tree search results](image)

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.

### 13.3.1 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 160, Delete a keyword search folder

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

13.3.2 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).

13.3.3 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 in the directory entry of the file). If a keyword is 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.
13.4 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 161, Keyword Result List**

![Keyword Result List](image)

13.4.1 HITS

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

13.4.2 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.
13.4.3 HIT OFFSET (FILE, PARTITION, DEVICE)

A keyword search hit has three columns which describe the location of the hit in the evidence, Hit Offset (File), Hit Offset (Partition) and Hit Offset (Device), as shown in Figure 162 below:

Figure 162, Keyword Search Hit Offset

Important

When working with hit offset in Forensic Explorer it is important to remember that that Hex view is file based, that is, Hex view is driven by the selection in the Folder tree, the List View or the Disk View. For example, to view the entire disk in Hex view from physical 0, the evidence file (i.e. the raw device) must be selected in either the Folder tree, or the File list. If any other file is selected, only the content of that files will be shown in HEX view.

Hit Offset (File)

For the file in which the hit was found, Hit Offset (File) is the number of bytes from the beginning of the file to the location of the hit. In the example in Figure 162 above the file offset to the first search hit ‘Graham’ in Turtles.jpg is 2232.

When the first hit in Figure 162 above is selected, Hex view displays the content of the file with the hit highlighted. If the cursor is manually placed at the beginning of the first hit, the Hex view information bar shows:

- Sector: 663820 (xA210C): The sector of the current hit.
- Device Offset: 339876024 (x1448B8): The number of bytes from the beginning of the device (DEMO 7.E01) to the start of the hit.
- File Offset: 2232 (x8B8): The number of bytes from the beginning of Turtles.jpg to the start of the hit.
Hit Offset (Partition)

For the partition in which the hit was found, Hit Offset (Partition) is the number of bytes from the beginning of the partition to the location of the hit. In the example in Figure 162 above the partition offset to the first search hit ‘Graham’ in Turtles.jpg is 339876024.

In order to view the partition Hex view it is necessary to change to the File System module and select the partition in either the Folder tree or the List view.

Figure 164, In this example...

NOTE: In this example:

The forensic image is an acquisition of a partition (e.g. the ‘D:\’ drive was acquired), so evidence file is the entire partition. This is why the Hit Offset (Partition) and Hit Offset (Device) numbers are identical in Figure 162 Figure 162, Keyword Search Hit Offset.

When the evidence file is selected in the File System tree (shown in Figure 165 below), the entire device is shown in the Hex view:
To go to the Hit Offset (Partition):

1. In the File System module Hex view, right click, select GOTO from the drop down menu;

2. Enter the partition offset taken from the Hit Offset (Partition) column in the Keyword Search module (use right-click Copy Cell to copy the partition offset number from the keyword hit), as shown Figure 166 below:

NOTE: You must have the correct file selected:

- Click the Device to Goto from the beginning of the device;
- Click the Partition to Goto from the beginning of the partition;
- Click the File to Goto from the beginning of the file.

Goto takes the Hex view to the entered offset. **Manually click** at the offset to ensure the Hex view information bar refreshes to show:

- Offset: 339876024 (x144218B8): The number of bytes from the beginning of the partition to the Goto location.
13.5 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 14 - Index Search Module

In This Chapter

CHAPTER 14 - INDEX SEARCH MODULE

14.1 Index search ........................................................................................................................................... 196
  14.1.1 Indexed file types .......................................................................................................................... 196
  14.1.2 Index database ............................................................................................................................... 196
  14.1.3 Noise words .................................................................................................................................... 196
14.2 Considerations prior to creating an index ............................................................................................ 196
14.3 Creating an index ..................................................................................................................................... 197
  14.3.1 Index progress .................................................................................................................................. 198
14.4 Searching an index .................................................................................................................................... 199
  14.4.1 Select the search features to use in your search ............................................................................. 200
  14.4.2 Boolean Search ............................................................................................................................... 201
  14.4.3 Words and Phrases ......................................................................................................................... 201
  14.4.4 Wildcards (*, ?, and =) ................................................................................................................ 202
14.5 Search results ....................................................................................................................................... 202
14.6 Index Search Compound Files ............................................................................................................ 203
14.1 INDEX SEARCH

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

Figure 168 - 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.

14.1.1 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

14.1.2 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\DTSерачIndexes\index name\n
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.

14.1.3 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 an 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.

14.2 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;
14.3 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 169 below:
Figure 169, New Index

![New Index](image)

**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.

### 14.3.1 INDEX PROGRESS

An index in progress will show “Running” in the Indexes window, as shown in Figure 170 below:
The progress is also tracked in the program process list, as shown in Figure 171 below:

**Figure 171 - Forensic Explorer process window showing a completed index**

When the indexing process is complete, the index will appear in the “Available Indexes” window, as shown in Figure 172 below:

**Figure 172, Index creation in progress**

14.4 SEARCHING AN INDEX

When the indexing process is complete, the index will appear in the “Available Indexes” window, as shown in Figure 172 below:
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.

14.4.1 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”.

---

*Copyright GetData Forensics Pty Ltd 2010 - 2019, All rights reserved.*
Phonic searching

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

Fuzzy

Fuzzy searching sifts through scanning and typographical errors.

14.4.2 BOOLEAN SEARCH

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

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

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)

14.4.3 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.

### 14.4.4 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:

<table>
<thead>
<tr>
<th>Wildcard Pattern</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>appl*</td>
<td>Would match apple, application, etc.</td>
</tr>
<tr>
<td><em>cipl</em></td>
<td>Would match principle, participle, etc.</td>
</tr>
<tr>
<td>appl?</td>
<td>Would match apply and apple but not apples.</td>
</tr>
<tr>
<td>ap*ed</td>
<td>Would match applied, approved, etc.</td>
</tr>
</tbody>
</table>

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

### 14.5 Search Results

Search results display in the Index Results List view window, as shown in Figure 174 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 173, Navigate index search hits**

<table>
<thead>
<tr>
<th>&lt;&lt;</th>
<th>&lt;</th>
<th>&gt;</th>
<th>&gt;&gt;</th>
<th>Hit 1 of 22</th>
</tr>
</thead>
</table>

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:
14.6 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.

14.7 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 investigator's 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 15 - Email Module

In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 15 - EMAIL MODULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1 Email</td>
</tr>
<tr>
<td>15.2 Email module</td>
</tr>
<tr>
<td>15.3 Microsoft Outlook .PST email</td>
</tr>
<tr>
<td>15.3.1 Add a standalone OUTLOOK.PST file</td>
</tr>
<tr>
<td>15.3.2 Add a .PST file from a Forensic Explorer module</td>
</tr>
<tr>
<td>15.4 Index Search the Email module</td>
</tr>
</tbody>
</table>
15.1 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), all versions;

Note: It is possible to independently index and keyword search email in the Index Search module. Refer to Chapter 14 - Index Search Module, for more information.

15.2 EMAIL MODULE

The Email module is accessed via the “Email” 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.

15.3 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). OST files are NOT currently supported in the email module.
15.3.1 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.

15.3.2 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.

15.4 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 176, 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 in the file system. DTSearch will already index a PST file that is in the file system.
15.5 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 177, Keyword Search module, Run Keyword Search window*
Chapter 16 - Registry Module

In This Chapter

CHAPTER 16 - REGISTRY MODULE

16.1 Registry module .................................................................................................................. 210
  16.1.1 Windows location of registry files ............................................................................... 210

16.2 Adding a REGISTRY FILE to the registry module ............................................................... 210
  16.2.1 Add a standalone registry file .................................................................................... 211
  16.2.2 Add a registry file from a Forensic Explorer module ................................................. 211

16.3 Registry Data Views .......................................................................................................... 211
  16.3.1 Registry Tree ............................................................................................................. 211
  16.3.2 Registry List ............................................................................................................. 212
  16.3.3 Hex, Text and Filesystem Record views ..................................................................... 213

16.4 Deleted registry keys ......................................................................................................... 213

16.5 Examining registry files using scripts ............................................................................... 213
16.1 REGISTRY MODULE

The Registry module is accessed via the “Registry” 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 (13)

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.

16.1.1 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 (13)” 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.

16.2 ADDING A REGISTRY FILE TO THE REGISTRY MODULE

There are two methods to add a Windows registry file to the Forensic Explorer Registry module.
16.2.1 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.

16.2.2 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 16.1.1 - 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 179 below:

![Figure 179, Registry module showing "Sent from"](image)

16.3 REGISTRY DATA VIEWS

16.3.1 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 180 below:
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 78.

16.3.2 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 181 below:

Figure 181, Registry List view
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” (14) 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).

### 16.3.3 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.

### 16.4 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

### 16.5 EXAMINING REGISTRY FILES USING SCRIPTS

A default installation of Forensic Explorer includes a “Parse Registry Keys” button group in the Registry Module toolbar:

*Figure 182, 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:
The *Registry Key Processor.pas* uses a RegEx search to locate the relevant key. The script then process and displays the result per 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 artifact, results from the *Registry Key Processor.pas* should be validated before being relied upon.
Chapter 17 – Bookmarks Module

In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 17 - BOOKMARKS MODULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.1 Adding Bookmarks ................................................................. 216</td>
</tr>
<tr>
<td>17.1.1 Manually add a bookmark .................................................. 216</td>
</tr>
<tr>
<td>17.1.2 Triage bookmarks .............................................................. 217</td>
</tr>
<tr>
<td>17.1.3 Adding Bookmarks from a script .......................................... 217</td>
</tr>
<tr>
<td>17.1.4 Hot key bookmarking .......................................................... 217</td>
</tr>
<tr>
<td>17.2 Bookmarks Module ................................................................. 218</td>
</tr>
<tr>
<td>17.2.1 Bookmarks tree ................................................................. 219</td>
</tr>
<tr>
<td>17.2.2 Bookmarks List ................................................................. 220</td>
</tr>
<tr>
<td>17.2.3 Bookmark Data Views ......................................................... 221</td>
</tr>
<tr>
<td>17.3 Identifying Bookmarked files other modules .............................. 222</td>
</tr>
</tbody>
</table>
17.1 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.

17.1.1 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:

![Add Bookmarks window](image)
Chapter 17 — Bookmarks Module

Source Files: A bookmark action can be performed on a highlighted file/s or checked files.

Select Folder: Folders are used by the investigator to group together bookmarked files of like interest. Folders can be moved using the mouse **drag and drop**.

Folder Comment: A comment about the folder holding the bookmarked files.

File/s Comment: A comment about the file/s being bookmarked.

17.1.2 TRIAGE BOOKMARKS

When evidence is added to a case the option exists in the Evidence Processor (See 10.5) to “Triage” data.

17.1.3 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 Programs 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.

17.1.4 HOT KEY BOOKMARKING

A **hot key** (or: hotkey; hot-key; shortcut key) refers to the use of a keyboard key (or combination of keys) that, when pressed, performs a task more quickly than by using a mouse or other input device. The Forensic Explorer **Gallery view** supports hot key bookmarking.

To activate **hot key bookmarking** in **Gallery view**:

1. Put a tick in the **Category Hot Keys [0-9]** checkbox, as shown in Figure 185 below:
2. The bookmark folder section button is used to select the parent folder where the hot key bookmarks will be added.

3. The number keys 0 to 9 are now the active hot keys.

To add a hot key bookmark:

- **Important**: Ensure that the current mouse focus is on the Gallery View window.

Press a number key on the keyboard. The currently highlighted file is bookmarked to a numbered ‘Category’ subfolder of the selected parent bookmark folder. In the example in Figure 185 above, when the 1 key is pressed the highlighted file 47.JPG is bookmarked to:

```
My Bookmarks\Pictures\Category 01\47.JPG
```

When the 2 key is pressed the currently highlighted file is bookmarked to:

```
My Bookmarks\Pictures\Category 02\[filename.ext]
```

And so on.

### 17.2 BOOKMARKS MODULE

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

Figure 186, 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.

### 17.2.1 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 187 below:

**Figure 187, Bookmark folder tree**

<table>
<thead>
<tr>
<th>Bookmark Name</th>
<th>Comment</th>
<th>Investigator Name</th>
<th>Modif</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Case 31 (0)</td>
<td></td>
<td>Graham Henley</td>
<td>27-Fr</td>
</tr>
<tr>
<td>My Bookmarks (0)</td>
<td></td>
<td>Graham Henley</td>
<td>27-Fr</td>
</tr>
<tr>
<td>Evidence (0)</td>
<td></td>
<td>Graham Henley</td>
<td>27-Fr</td>
</tr>
<tr>
<td>Files (0)</td>
<td></td>
<td>Graham Henley</td>
<td>27-Fr</td>
</tr>
<tr>
<td>Documents (0)</td>
<td></td>
<td>Graham Henley</td>
<td>27-Fr</td>
</tr>
<tr>
<td>Pictures (2)</td>
<td>Important Pictures</td>
<td>Graham Henley</td>
<td>27-Fr</td>
</tr>
<tr>
<td>Email (0)</td>
<td></td>
<td>Graham Henley</td>
<td>27-Fr</td>
</tr>
<tr>
<td>Internet (0)</td>
<td></td>
<td>Graham Henley</td>
<td>27-Fr</td>
</tr>
<tr>
<td>Registry (0)</td>
<td></td>
<td>Graham Henley</td>
<td>27-Fr</td>
</tr>
</tbody>
</table>

**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:
To move a bookmark folder:

**Drag and drop** an existing folder to its required location.

### 17.2.2 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 189, Bookmark list below:

**MANAGE BOOKMARK LIST**

To **add** a bookmark:

See 17.1 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:
2. Click OK to proceed. The file/s is deleted from the Bookmarks module.

To **copy a bookmark to another bookmark folder:**

1. Left click on the bookmarked item;
2. Drag and drop the bookmark to the required folder.

To **move a bookmark from one bookmark folder to another:**

1. Left click on the bookmarked item;
2. Hold down the **SHIFT** key;
3. Drag and drop the bookmarked item to the required folder.

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.

### 17.2.3 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 191 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.
Bookmarked files can be identified in the File System module by:

1. A purple bookmark that overlays the file icon, as shown in Figure 192 below:

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 18 – Reports Module

In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 18 - REPORTS MODULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.1 Reporting &amp; Bookmarks ................................................................. 225</td>
</tr>
<tr>
<td>18.2 The Reports Module ................................................................. 226</td>
</tr>
<tr>
<td>18.3 Reports Tree ............................................................................. 227</td>
</tr>
<tr>
<td>18.3.1 The Triage Report ................................................................. 227</td>
</tr>
<tr>
<td>18.3.2 Changing the default report ......................................................... 229</td>
</tr>
<tr>
<td>18.3.3 Open a new report .................................................................. 229</td>
</tr>
<tr>
<td>18.3.4 Report name, Groups and Sections ........................................ 229</td>
</tr>
<tr>
<td>18.3.5 Rename or Move a Group or Section .......................................... 230</td>
</tr>
<tr>
<td>18.3.6 Print a report ........................................................................ 230</td>
</tr>
<tr>
<td>18.3.7 Export a report as DOC, RTF or PDF ........................................ 230</td>
</tr>
<tr>
<td>18.3.8 Save a report as a template ..................................................... 231</td>
</tr>
<tr>
<td>18.4 Report Editor ............................................................................ 233</td>
</tr>
<tr>
<td>18.4.1 Report Editor - Preview ........................................................ 233</td>
</tr>
<tr>
<td>18.4.2 Report Editor - Edit ............................................................... 234</td>
</tr>
<tr>
<td>18.5 Creating Reports ..................................................................... 235</td>
</tr>
<tr>
<td>18.5.1 Preparation for Report exercises ............................................. 236</td>
</tr>
<tr>
<td>18.5.2 Exercise 1: Report on a single file ........................................... 238</td>
</tr>
<tr>
<td>18.5.3 Exercise 2: Listing bookmarked files in a table ....................... 244</td>
</tr>
<tr>
<td>18.5.4 Exercise 3: Creating a Gallery view report ................................ 251</td>
</tr>
<tr>
<td>18.5.5 Exercise 4 - Nested Tables ..................................................... 257</td>
</tr>
<tr>
<td>18.5.6 Apply a filter to a report table ............................................... 266</td>
</tr>
</tbody>
</table>
18.1 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 193, Modules > Bookmarks > Reports

Bookmarks are either added manually or as the result of running a script (e.g. Triage scripts). For more information about adding bookmarks see Chapter 17 above.

Care should be taken to arrange the bookmark structure effectively to fully maximize the use of report templates discussed in this chapter.
18.2 THE REPORTS MODULE

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

Figure 194, Reports module tab

The Reports module is divided into three main sections (as shown in Figure 195 below):

1. Reports tree
2. Preview window
3. Report Editor window

Figure 195, Reports Module showing the Triage Report

The sections are described in more detail below.
18.3 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.

18.3.1 THE TRIAGE REPORT

RUNNING A TRIAGE

When evidence is added to Forensic Explorer the option exists in the Evidence Processor window to Triage (see “Evidence Processor” on page 154 for more information). The triage process runs scripts that bookmark data in the My Bookmarks\Triage\ folder. The dynamic content of the Triage report is populated from this bookmark. (Note: If the triage option was not selected, or there were no files found, the Triage report will contain blank fields).

A triage can also be run at any time from the Triage button in the File System module:

Figure 196, Triage from File System module

TRIAGE REPORT REPEATING OVER MULTIPLE DEVICES

The Triage report is designed to work for multiple devices in a case by repeating on the “Triage – Bookmark Folder” report section as represented by the green icon in Figure 197 below:
Figure 197, Reports Tree showing the Triage Report

The repeat function is set by right clicking on the required folder and applying the * symbol, as shown in Figure 198:

Figure 198, Iterating a report over multiple devices

**TRIAGE REPORT AND UNIQUE DEVICE NAMES**

The Triage report is also an example where bookmarks are created under unique device names. This is handled in the report by replacing the unique folder name with * in the bookmark path, as shown in Figure 199:
18.3.2 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.

18.3.3 OPEN A NEW REPORT

All new reports are created from a template. Templates are 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 the report is deleted.

18.3.4 REPORT NAME, GROUPS AND SECTIONS

A report consists of the following components:
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 197 below:

18.3.5 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.

18.3.6 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.

18.3.7 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 format;
Figure 200, Export a Report

- Save the file to the desired location.

Note: .docx and .rtf do not currently support the saving of page headers and footers.

**EXPORTING A REPORT WITH HYPERLINKS**

When a report has been created and a field in the report has the option to **Hyperlink to Exported File** checked (see Step 8 – Adding Hyperlinks for the exported report on page 248), a folder called **ReportData** is created to hold the relevant exported files. An example is shown in Figure 201 below where the report and report data has been exported to the Windows Desktop:

Figure 201, A report with hyperlinks exported to the Windows Desktop

18.3.8 SAVE 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 202, Save a Report Template**

   ![Image of Browse For Folder window]

   - Make New Folder
   - OK
   - Cancel

4. Click OK to save the components of the report into the folder.

   Once saved as a template, the report will now be available under the **New** button in the **Reports** tree:

   **Figure 203, Load a report template**

   ![Image of Report Selection window]
18.4 REPORT EDITOR

The Report Editor window has two functions:

1. To **preview** a current report;
2. To **create \ Edit** a report.

To switch between **preview** and **edit**, click on the report section in the tree and;

- Click the **Edit** or **Preview** button in the toolbar, or,
- Right click in the tree and select **Edit** or **Preview** from the drop down menu.

18.4.1 REPORT EDITOR - PREVIEW

The Report Editor Preview (shown in Figure 204 below) displays the content of the currently selected report in the Report tree.

To preview the **report**:

- In the Repot tree, click on the report name;

To preview a **group** or a **section**:

- In the Report tree, click on a group or a section.

(If in edit mode, click the **preview** button at the top of the tree to change to preview.)

Figure 204, Report Editor Preview

**IMPORTANT**: For speed purpose a report Preview is limited by default to **100 records**. This default can be changed by setting the following Registry key:

```
HKEY_CURRENT_USER\SOFTWARE\GetData\ForensicExplorer v4\Configuration\ DWORD ReportPreviewLimit = 100.
```
If the report contains more than limit a message will appear in the Preview information bar with the option to generate a Preview for the entire report, as shown in Figure 205 below:

Figure 205, Limited Preview - Generate Full Report

To cancel the generation of a full report in progress click on the cancel button for this task in the progress bar.

18.4.2 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, click on a report section and click the Edit button at the top of the tree; or
- Right click and select the Edit option from the drop down menu.

When in Edit mode the Report Editor will show the toolbar with the various edit functions:

Figure 206 - Report Editor in Edit Mode
18.5 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.
18.5.1 PREPARATION FOR REPORT EXERCISES

The following exercises are created using the image file Animals.L01 available for download from:

http://download.getdata.com/support/forensic-image-files/Animals.zip

Unzip the download file and use the Animals.L01 file.

STEP 1 – START A CASE AND BOOKMARK FILES

Start a case and add bookmarks:

a. In the Evidence module, create a new case, and add the forensic image Animals.L01.

b. In the Bookmarks module, right click on the Pictures bookmark folder and add two additional sub folders, Cats and Dogs (as shown below).

Figure 207, Bookmarks module

c. In the File System module;

- Branch plate the Cats folder;
- Highlight the 21 JPG files in the Cats folder;
- Right click in the File List view and Add Bookmark. Bookmark the files to the Cats bookmark folder.
d. Repeat the step above to bookmark the 10 dog pictures to the Dogs bookmark folder.

e. Switch to the Bookmarks module. Review the Pictures bookmark folder to ensure that it contains the bookmarked files, as shown in Figure 209 below:

Figure 208, Preparation for report exercises, bookmarking files

Figure 209, Bookmarked files from Animals.101
18.5.2 EXERCISE 1: REPORT ON A SINGLE FILE

OBJECTIVE

The objective of this exercise is to create a report for a single file bookmarked in the My Bookmarks\Pictures\Cats folder. The bookmarked file used in this example is Orange Cat 4.JPG. The finished report will look as follows:

Figure 210, Reporting on a Single Bookmarked File (finished report output)

<table>
<thead>
<tr>
<th>Filename:</th>
<th>Orange Cat 4.JPG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessed:</td>
<td>14-Mar-12 9:37:12 PM</td>
</tr>
<tr>
<td>Created:</td>
<td>17-May-12 2:01:22 PM</td>
</tr>
<tr>
<td>Modified:</td>
<td>14-Mar-12 9:37:12 PM</td>
</tr>
<tr>
<td>Path:</td>
<td>Exercise - Creating Report Templates\Lexar 7G</td>
</tr>
</tbody>
</table>

STEP 1 – PREPARE BOOKMARKS

Follow STEP 1 in 18.5.1 above to prepare a case with bookmarks.

STEP 2 – CREATE A BLANK REPORT

Create a blank report:

a. Switch to the Reports module.

b. In the Reports tree, select New > Blank Report.
STEP 3 – RENAME THE BLANK REPORT

Rename the blank report:

a. In the Reports module, click then hover over the report name to rename the report to **Single Item Report**.

b. Repeat this step to rename the section. The Reports folder tree should now look like this:

    ![Figure 212, Rename the Report and Section](image)

STEP 4 – EDIT THE REPORT

Edit the report:

a. Highlight the **Single Item Report** and click the **Edit** button to open the report in the **Report Editor** window.

    Note that the **Edit** button changes from **Edit** to **Preview** depending on whether the **Report Editor** window is in Preview or Edit mode:
b. In the **Reportable Items** column (shown in Figure 214 below), click on the folder containing the desired bookmark, i.e. **Cats**. Then at the bottom of this column, locate and click on the required file, i.e. **Orange Cat4.JPG**.

c. The fields available for the highlighted file are now shown in the **Available Fields** column to the left (as shown in Figure 214 below).
d. 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 Figure 215 below:
e. Preview the report by clicking on the Preview button at the top of the folder tree. This will show the contents of the field, as shown in Figure 216 below:

![Figure 216, Report Editor - Preview](image)

f. To insert the picture:

- Click on the Edit button to edit the page in the Script Editor;
- Click on the file name Orange Cat 4.JPG in the Reportable Items column (shown in Figure 214 above). The picture will display at the bottom of the Available Fields Column;
- Drag and drop the picture to the required position onto the report, as shown in Figure 217 below:
g. To insert field labels, click on a field then right click and select **Insert Label** from the drop down menu:

![Figure 217, Drag and drop picture onto report](image1)

**Figure 217, Drag and drop picture onto report**

h. Use the format toolbar to add formatting (font, text size, color, etc.). The formatted output is shown in Figure 210 at the start of the exercise.

**SAVE REPORT**

Save the report:

a. Use the save button at the top of the Report Editor window to save the current report. The report is saved with the case.

**SAVE REPORT AS A TEMPLATE**

To make this report available for future cases, the report must be saved as a **Report Template**:

a. Follow the instructions in 18.3.8 above to save the report as a template.
18.5.3 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. The finished report is shown in Figure 219 below:

Figure 219, Exercise 1 – Listing bookmarked files in a table

<table>
<thead>
<tr>
<th>Filename</th>
<th>Created</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>CatsB7_Maebh.JPG</td>
<td>17-May-12 2:01:22 PM</td>
<td>14-Mar-12</td>
</tr>
<tr>
<td>CatsB6_Grendel.JPG</td>
<td>17-May-12 2:01:22 PM</td>
<td>14-Mar-12</td>
</tr>
<tr>
<td>CatsB5_Choco.JPG</td>
<td>17-May-12 2:01:22 PM</td>
<td>14-Mar-12</td>
</tr>
<tr>
<td>CatsB3_CharlieTuna.JPG</td>
<td>17-May-12 2:01:21 PM</td>
<td>14-Mar-12</td>
</tr>
<tr>
<td>CatsB1_Corduroy.JPG</td>
<td>17-May-12 2:01:21 PM</td>
<td>14-Mar-12</td>
</tr>
<tr>
<td>CatsA9_Mnktn.JPG</td>
<td>17-May-12 2:01:21 PM</td>
<td>14-Mar-12</td>
</tr>
<tr>
<td>CatsA8_Gadget.JPG</td>
<td>17-May-12 2:01:21 PM</td>
<td>14-Mar-12</td>
</tr>
<tr>
<td>CatsA7_TomTom.JPG</td>
<td>17-May-12 2:01:21 PM</td>
<td>14-Mar-12</td>
</tr>
<tr>
<td>CatsA5_Starbuck.JPG</td>
<td>17-May-12 2:01:21 PM</td>
<td>14-Mar-12</td>
</tr>
<tr>
<td>CatsA4_Kristaj.JPG</td>
<td>17-May-12 2:01:21 PM</td>
<td>14-Mar-12</td>
</tr>
<tr>
<td>DogsA9_Kode.JPG</td>
<td>17-May-12 2:01:23 PM</td>
<td>14-Mar-12</td>
</tr>
<tr>
<td>DogsA8_Jack-Jack.JPG</td>
<td>17-May-12 2:01:23 PM</td>
<td>14-Mar-12</td>
</tr>
</tbody>
</table>

STEP 1 – PREPARE BOOKMARKS

If not already done, follow STEP 1 in 18.5.1 above to prepare a case with bookmarks.

STEP 2 – CREATE A BLANK REPORT

To create a blank report:

a. Switch to the Reports module.

b. In the Reports tree, select New > Blank Report (as shown in Figure 211 above).

STEP 3 – RENAME THE BLANK REPORT

Rename the report:

a. Click and hover on the report name to rename to List of Pictures Bookmarks.

b. Repeat this step to rename the section, as shown in Figure 220 below:
STEP 4 – ADD A REPEATING TABLE TO THE REPORT

Edit and add a repeating table to the report:

a. In the Reports tree, highlight the report and click on the Edit button to open the report in the Report Editor window.

b. In the Reportable Items column, select the Pictures bookmark folder and drag and drop it onto the blank page, as shown in Figure 221 below:

c. Select to Insert Item as Table for the table to iterate through each bookmarked file:

d. Select the Multiple columns per item column table:
Figure 222, Selecting a List View Table Style

![Column Table]

Multiple columns per Item

The Insert as Table window opens showing the available fields for the Pictures bookmark folder. In this example we will not use fields associated with this bookmark folder. Leave the Selected Fields blank and click OK:

Figure 223, Insert Table Window

![Insert Table Window]

A blank Pictures table will be added to the report, as shown in Figure 224 below:
Figure 224, Pictures bookmarks table

Note that hovering over the Pictures folder with the mouse will show the source bookmark folder for the table (My Bookmarks\Pictures) in the bottom information bar of the Report Editor window.

**STEP 5 - POPULATE THE REPEATING TABLE WITH THE REQUIRED FIELDS**

To populate the table with the required fields:

a. In the Reportable Items column, select the sub bookmark folder containing the files, e.g. **Cats**;

b. In the bottom window, click on a file name within the Cats bookmark folder. The **Available Files** column will now populate. Drag and drop the required files into the table, as shown in Figure 225 below:

Figure 225, Adding fields to a table

f. Format the table as needed and switch to the Preview window to view the result. The table list should look like Figure 219 at the start of this exercise.
STEP 6 - SET THE PROPERTIES OF THE REPEATING TABLE

The properties of the repeating table determine what content will be displayed. To set the properties of the repeating table:

a. Hover the mouse over the table folder, i.e. Pictures. Right click and select Properties:

![Figure 226, Table Properties]

This will open the Bookmark Enumerator Properties window:

![Figure 227, Repeating table properties]

- **Fully Recursive**: The table includes all sub-folders under the Parent Bookmark Folder (i.e. Pictures);
- **Include Items Only**: The table will report on items (files) only.

STEP 7 - PREVIEW THE FINAL REPORT

a. Click on the Preview button to display the report. The report should appear similar to Figure 219 at the beginning of this exercise.

b. Update formatting as needed.

STEP 8 – ADDING HYPERLINKS FOR THE EXPORTED REPORT

In the Report Editor select the field where the link is required, right click and check Hyperlink to Exported File, as shown in Figure 228 below:
Figure 228, inserting a hyperlink for an exported report

When the report Preview tab is selected, a blue hyperlink will appear in the relevant column, as shown in Figure 229 below:

Figure 229, a report with a hyperlink

When the report is exported, a ReportData folder will also be created containing the relevant images which are hyperlinked from the report. See section 18.3.7 above.

SAVE REPORT

Save the report:

a. Use the save button at the top of the Report Editor window to save the current report. The report is saved with the case.
SAVE REPORT AS A TEMPLATE

To make this report available for future cases, the report must be saved as a Report Template:

a. Follow the instructions in 18.3.8 above to save the report as a template for future use.
18.5.4 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 230 below:

Figure 230, creating a Gallery View Report (finished report shown)

**Bookmarked Pictures**

- Cats88_Ta_JPG
  - C: 17-May 12 2:01:22 PM
- Cats89_Minikin_JPG
  - C: 17-May 12 2:01:21 PM
- Cats88_Gadget_JPG
  - C: 17-May 12 2:01:21 PM
- Cats84_Krista
  - C: 17-May 12 2:01:20 PM
- Orange Cat 1 JPG
  - C: 17-May 12 2:01:22 PM
- Orange Cat 2 JPG
  - C: 17-May 12 2:01:23 PM
- Orange Cat 3 JPG
  - C: 17-May 12 2:01:23 PM
- Orange Cat 4 JPG
  - C: 17-May 12 2:01:22 PM
- Dog 5A7_M.jpg
  - C: 17-May 12 2:01:20 PM

**STEP 1 – PREPARE BOOKMARKS**

If not already done, follow **STEP 1** in 18.5.1 above to prepare a case with bookmarks.

**STEP 2 – CREATE A BLANK REPORT**

To create a blank report:

a. Switch to the Reports module.

b. In the Reports tree, select New > Blank Report (as shown in Figure 211 above).

**STEP 3 – RENAME THE BLANK REPORT**

Rename the report:

a. Click and hover on the report name to rename the section to **My Gallery Report - Pictures**.

b. Repeat this step to rename the report section.
STEP 4 – ADD A REPEATING TABLE TO THE REPORT

Edit and add a repeating table to the report:

a. In the Reports tree, highlight the report and click on the Edit button to open the report in the Report Editor window.

b. In the Reportable Items column, select the Pictures bookmark folder and drag and drop it onto the blank page, as shown in Figure 221 above:

Figure 231, Drag and drop folder

\[\text{Insert Item as Table}\]

For the table to iterate through each bookmarked file:

a. In the table selection window, use the Grid Table to display files in the bookmark folder (i.e. pictures) entered horizontally across the screen in the gallery view format:
b. The **Insert as Table** window opens showing the available fields for the **Pictures** bookmark folder:

In this example we will not use fields associated with the folder. Leave the **Selected Fields** blank and click **OK**. The pictures table will be added to the report:
Note that hovering over the **Pictures** folder with the mouse will show the source bookmark folder for the table (My Bookmarks\Pictures) in the bottom information bar of the Report Editor window.

**STEP 5 - POPULATE THE REPEATING TABLE WITH THE REQUIRED FIELDS**

To populate the table with the required fields:

c. In the Reportable Items column, select the sub bookmark folder containing the files, e.g. **Cats**;

d. In the bottom window, click on a file name within the Cats bookmark folder. The **Available Files** column will now populate. Drag and drop the required files into the table, as shown in Figure 225 above:

**Figure 235, Adding fields to a table**

- Format the table as needed and switch to the Preview window to view the result. The table list should look like Figure 219 at the start of this exercise.
STEP 6 - SET THE PROPERTIES OF THE REPEATING TABLE

The properties of the repeating table determine what content will be displayed. To set the properties of the repeating table:

c. Hover the mouse over the table folder, i.e. Pictures. Right click and select Properties:

![Figure 236, Table Properties]

This will open the Bookmark Enumerator Properties window:

![Figure 237, Repeating table properties]

- **Fully Recursive**: The table includes all sub-folders under the Parent Bookmark Folder (i.e. Pictures);
- **Include Items Only**: The table will report on items (files) only.

STEP 7 - PREVIEW THE FINAL REPORT

Preview the final report:

a. Click on the Preview button to display the report. The report should appear similar to Figure 219 at the beginning of this exercise.

b. Update formatting as needed.
STEP 8 – ADDING HYPERLINKS FOR THE EXPORTED REPORT

If hyperlinks are required for an exported report, refer the instructions in the previous exercise.

SAVE REPORT

Save the report:

b. Use the save button at the top of the Report Editor window to save the current report. The report is saved with the case.

SAVE REPORT AS A TEMPLATE

To make this report available for future cases, the report must be saved as a Report Template:

b. Follow the instructions in 18.3.8 above to save the report as a template for future use.
18.5.5 EXERCISE 4 - NESTED TABLES

OBJECTIVE

In this exercise, we will create a list of bookmarked pictures grouped by a sub category, i.e. Cats and Dogs. The finished report looks as follows:

Figure 238, Finished nested table report

The report is created using nested tables. The structure of the tables is described in xx:
STEP 1 – PREPARE BOOKMARKS

If not already done, follow **STEP 1** in **18.5.1** above to prepare a case with bookmarks.

STEP 2 – CREATE A BLANK REPORT

To create a blank report:

a. Switch to the Reports module.

b. In the Reports tree, select **New > Blank Report**.

STEP 3 – RENAME THE BLANK REPORT

Rename the report:

a. Click and hover on the report name to rename the section to **Nested Table Report**.
b. Repeat this step to rename the report section.

**STEP 4 – ADD A REPEATING OUTER TABLE TO THE REPORT**

The purpose of the outer table is to group report results. In this example we wish to group report results by the sub-folders of the Pictures bookmark folder, i.e. Cats and Dogs.

To add the outer table to the report:

a. In the Reports tree, highlight the report and click on the Edit button to open the report in the Report Editor window.

b. In the Reportable Items column, select the Pictures bookmark folder and drag and drop it onto the blank page, as shown in Figure 221 above:

![Drag and drop folder](image)

Figure 240, Drag and drop folder

c. Select to Insert Item as Table:

![Insert As Field...](image)

![Insert items as Table...](image)
d. Use the table type **Multiple columns per Item**;

![Multiple columns per Item](image)

e. Add the **Bookmark Name** field to the report:

![Insert as Table](image)

f. Click OK to add the **Outer Table**.

g. To visually assist in the creation process, rename the Column Header from **Bookmark Name** to **Outer Table** and add space to the table. The table should look as follows:
Table 1, Outer table

STEP 6 - SET THE PROPERTIES OF THE OUTER TABLE

The properties of the repeating table determine what content will be displayed. To set the properties of the repeating table:

a. Hover the mouse over the table folder, i.e. Pictures. Right click and select Properties:

Figure 241, Table Properties

This will open the Bookmark Enumerator Properties window:

Figure 242, Repeating table properties
**Direct Children:** The table will report Parents direct children, i.e. the Cats and Dogs sub-folders.

**Include Items Only:** The table will report only folders (any files in the parent folder will be ignored).

b. Click the Preview button to display the content of the report. It should look like this:

**Table 2, Outer table**

![Table 2, Outer table]

**STEP 5 – ADDING THE NESTED INNER TABLE**

The purpose of the inner table is to display records by group (i.e. a list of all Cats, followed by a list of all Dogs).

To add the inner table:

a. Drag and drop one of the folders required for the inner table, e.g. Cats, to the Report Editor and insert it *inside the outer table*, as shown in Figure 243 below:

![Figure 243 - Nested table. Insert a sub-table.]

*Figure 243 - Nested table. Insert a sub-table.*
c. Select to **Insert Item as Table** and use the table type **Multiple columns per Item**;

![Multiple columns per Item](image)

d. Select the fields to use the in the table. In this exercise use Filename, Created and modified, as shown in **Table field selection** Figure 244 below:

![Insert as Table](image)

Figure 244, Table field selection

e. Click OK to drop the table into the report.

f. The Inner Table will display a “*”, indicating that is operating on the first sub folder, as shown in Figure 245 below (a refresh of the view may be required to see the *).

![Inner Table](image)

g. Right click on the **Pictures\*** folder and display the contents of each sub folder (i.e. Cats & Dogs) by selecting:
Table 3, Open the Properties of the inner table

h. Set the properties of the inner table:

Figure 245 - Setting the attributes of the inner table

Full Recursive: The table will report all items in all subfolders of the parent.
Include Items Only: The table will report only folders (any files in the parent folder will be ignored).

STEP 7 - PREVIEW THE FINAL REPORT

Preview the final report:

c. Click on the Preview button to display the report. The report should appear similar to Figure 238Figure 219 at the beginning of this exercise.

d. Update formatting as needed.

STEP 8 – ADDING HYPERLINKS FOR THE EXPORTED REPORT

If hyperlinks are required for an exported report, refer the instructions in the previous exercise.
SAVE REPORT

Save the report:

c. Use the save button at the top of the Report Editor window to save the current report. The report is saved with the case.

SAVE REPORT AS A TEMPLATE

To make this report available for future cases, the report must be saved as a Report Template:

Follow the instructions in 18.3.8 above to save the report as a template for future use.
18.5.6 APPLY A FILTER TO A REPORT TABLE

It is possible to limit the items shown in a report by applying a filter. The filter can be applied to a wide ranging criteria including: filename, path, file size, maximum number of records to display, etc.

In the examples below, the Nested Table report from the previous exercise is used.

FILTER 1 – FILTER BY BOOKMARK FOLDER (OUTER TABLE)

To display only contents of the Cats folder only, a filter is applied to the outer table:

a. Right click on the Outer Table folder and in the drop-down menu select Properties;

b. Set the Custom Children Filter using the code:

\[
\text{Result} := \text{uppercase(Entry.EntryName)} = '\text{CATS}'
\]

as shown in Figure 246 below:

Figure 246 – Filter a bookmark folder
FILTER 2 – FILTER TABLES USING A FILE NAME

To filter a table report by filename;

a. Remove any prior filters;

b. Right click on the Pictures\* folder (inner table) and in the drop-down menu select Properties;

c. In the Table Iteration Filter enter the filter:

```
Result := (pos('CHARLIE', Uppercase(Entry.EntryName)) > 0)
```

as shown below:

Figure 247, Filter a file name

which gives the following result:
The following RegEx commands could also be used:

//Include filenames names that end with .doc:
Result := (RegExMatch(Entry.EntryName,'\.doc$', false))

//Include filenames that end with .doc, .xls, or .pdf:
Result := (RegExMatch(Entry.EntryName,'(\.doc|\.xls|\.pdf)$', false))

//Include filenames that start with 2 and end with .doc:
Result := (RegExMatch(Entry.EntryName,'^2.*\.doc$', false))

//Include filenames that contain only text and not numbers:
Result := (RegExMatch(Entry.EntryName,'^[^0-9]*$', false))
FILTER 3 – LIMIT THE NUMBER OF RECORDS SHOWN IN A TABLE

It is possible to limit the maximum number of items displayed in a repeating table:

a. Remove any prior filters;

b. Right click on the Pictures\* folder (inner table) and in the drop-down menu select Properties;

c. In the Table Iteration Filter enter the filter:

\[ \text{Result} := (\text{index} < 5) \]

as shown below. This will list the first 5 records in the bookmark folder:

Figure 249, Limit reporting on a bookmark folder to X records
# Chapter 19 – Scripts Module

## In This Chapter

<table>
<thead>
<tr>
<th>19.1</th>
<th>Scripts Module ...........................................................................................................</th>
<th>272</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.1.1</td>
<td>Scripts Window ..................................................................................................</td>
<td>273</td>
</tr>
<tr>
<td>19.1.2</td>
<td>Script Editor window ....................................................................................</td>
<td>276</td>
</tr>
<tr>
<td>19.1.3</td>
<td>Messages Window (Console) ........................................................................</td>
<td>277</td>
</tr>
<tr>
<td>19.2</td>
<td>Managing scripts in the scripts window .........................................................</td>
<td>278</td>
</tr>
<tr>
<td>19.3</td>
<td>Introduction to Scripting ..................................................................................</td>
<td>279</td>
</tr>
<tr>
<td>19.3.1</td>
<td>Programming Comments ...................................................................................</td>
<td>279</td>
</tr>
<tr>
<td>19.3.2</td>
<td>Reserved Words ..................................................................................................</td>
<td>279</td>
</tr>
<tr>
<td>19.3.3</td>
<td>Uses (libraries) ..................................................................................................</td>
<td>280</td>
</tr>
<tr>
<td>19.3.4</td>
<td>Const ..................................................................................................................</td>
<td>280</td>
</tr>
<tr>
<td>19.3.5</td>
<td>Var .....................................................................................................................</td>
<td>280</td>
</tr>
<tr>
<td>19.3.6</td>
<td>Procedures and Functions ................................................................................</td>
<td>281</td>
</tr>
<tr>
<td>19.3.7</td>
<td>Begin and End ....................................................................................................</td>
<td>281</td>
</tr>
<tr>
<td>19.3.8</td>
<td>Errors ................................................................................................................</td>
<td>281</td>
</tr>
</tbody>
</table>
19.1 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 250, Scripts module tab

The scripts module is arranged into three windows: Scripts; Script Editor; and Messages, as shown in Figure 251 below:

Figure 251, Scripts module
19.1.1 SCRIPTS WINDOW

The script window lists available .pas (Pascal) scripts and their attributes.

Figure 252, 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 hash is so that the investigator can validate the authenticity of a GetData script, or a script from a trusted third party.

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 **created, 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 253 below.
for the File System module (filters can be applied in Folders view of other modules, including Email and Registry):

**Figure 253, 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:

```pascal
begin
  filename := uppercase(anEntry.Entryname);
  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 on 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. Colors are assigned using the color reference chart: [http://en.wikipedia.org/wiki/Web_colors](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 19.4 below.
19.1.2 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.

Enter script parameters, e.g. “Parameter One” “Two” “Three” “Four”
19.1.3 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 the command “ConsoleLog(‘Text’)”. See Appendix 7 - Sample Script, for an example.

If a script is run in the Scrips 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).
19.2 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:

   ![Rename File](image)

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.
19.3 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 254, 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.

19.3.1 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}

19.3.2 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
19.3.3 **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

19.3.4 **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.

19.3.5 **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, \( X := 27; \)

### 19.3.6 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 255, 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
```

### 19.3.7 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 **semicolon**. If a command extends over several lines, for example an “If Then Else” statement, generally the semicolon won’t appear until the end of the entire statement.

### 19.3.8 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.
19.4 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;

- Go to the Scripts module;
- At the bottom of the Scripts window (top left hand window) click on the "Startup" folder to show "startup.pas”;
- 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.
19.4.1 MANAGE DISPLAYED 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 256, Startup Modules.pas](image)

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:

   ```pascal
   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 to re-enable the Scripts module).
   ```

19.4.2 CUSTOMIZING TOOLBARS

The content of the toolbar can be changed by the user.
*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, 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 you want logging (in this example, logging is false).

*Button Group – Hex.pas*

Now let’s 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\HWorks32.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, to test the script, we can do this in the scripts module by using the “Parameter” box in the toolbar.

If you type in “File System” (use the quotes when a space is 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 20 – Encryption

In This Chapter

CHAPTER 20 – ENCRYPTION

20.1 Encryption .......................................................................................................................... 288
  20.1.1 Windows NTFS Encrypted files ................................................................................... 288
  20.1.2 Bitlocker Encryption ..................................................................................................... 289
  20.1.3 File Vault 2 .................................................................................................................. 289

20.2 Decrypting Supported Encryption Formats ......................................................................... 290

20.3 Identifying Other Encrypted Files ...................................................................................... 293
  20.3.1 Identifying encrypted files using Entropy ..................................................................... 293
  20.3.2 Identifying Encrypted Files using a third party tool .................................................... 293
20.1 ENCRYPTION

There are many different types of encryption which vary in complexity and effectiveness. Some are easily identified and broken. Some are difficult to identify and impossible to break.

Forensic Explorer currently supports the following types of encryption:

- Windows NTFS encryption;
- BitLocker;
- File Vault 2.

20.1.1 WINDOWS NTFS ENCRYPTED FILES

Forensic Explorer displayed Windows NTFS encrypted (green) and compressed (blue) files using color, the same way as Windows:

Figure 257, Windows 10 file: Compressed (blue), Encrypted (green), Password Protected, and Normal

Windows Encrypted files can be easily filtered in Forensic Explorer by adding the IsEncrypted column to the File List view. IsEncrypted is a Boolean field of Yes or No.

Windows encrypted files can be decrypted in Live Boot by logging into the computer as an authorized user. See Chapter 28 for more detail.
20.1.2 BITLOCKER ENCRYPTION

BitLocker is a full disk encryption feature included with Windows Vista and later. It is designed to protect data by providing encryption for entire volumes. By default it uses the AES encryption algorithm in cipher block chaining (CBC) or XTS mode with a 128-bit or 256-bit key. (https://en.wikipedia.org/wiki/BitLocker, July 2017). For more information see:


During setup of a BitLocker partition a user is provided a recovery key which can be used to access the encrypted partition even if the main key is lost. Microsoft recommend that the recovery key is:

- Saved to a file;
- Printed;
- Stored on a USB flash drive; or
- Saved to a Microsoft account on Windows 8 and 8.1. If you back up the recovery key to your Microsoft account.

A BitLocker Recovery Key file has a default filename in the format:

BitLocker Recovery Key 0C29BEFD-E244-4ADC-B8A0-A6D1DD6588B5.TXT

where the number used in the filename is the identifier (not the actual key). Inside this file is the Bitlocker key:

Figure 259, Content of a Bitlocker Recovery Key file

BitLocker Drive Encryption recovery key
To verify that this is the correct recovery key, compare the start of the following identifier with the identifier value displayed on your PC.

Identifier:

0C29BEFD-E244-4ADC-B8A0-A6D1DD6588B5

If the above identifier matches the one displayed by your PC, then use the following key to unlock your drive.

Recovery Key:

672573-169873-647867-465509-462253-505483-475772-203071

If the above identifier doesn't match the one displayed by your PC, then this isn't the right key to unlock your drive.

Try another recovery key, or refer to http://go.microsoft.com/fwlink/?LinkId=260589 for additional assistance.

20.1.3 FILE VAULT 2

File Vault 2 is a full disk encryption feature included with MAC OS X Lion (released July 2011) or later. See https://support.apple.com/en-au/HT204837 for more information.
20.2 DECRYPTING SUPPORTED ENCRYPTION FORMATS

To decrypt Bitlocker and File Vault 2 drives:

DECRIPTION WHEN ADDING EVIDENCE

When a forensic image containing a supported encryption format is added to Forensic Explorer the investigator will be prompted with the following Bitlocker Credentials window:

Figure 260, Encryption Credentials window (BitLocker shown)

This window will accept either the password (or in the case of Bitlocker, the recovery key or Bitlocker recovery file). Without one of these credentials, the partition cannot be decrypted (click Cancel to bypass the decryption process.

Examples of an encrypted and decrypted partition are shown in the screen shots below:

Figure 261, Encrypted Partition (closed padlock)
DECRYPTION DURING A CASE

To decrypt a partition during a case, right click on the encrypted partition and select Encryption Password, as shown in Figure 263, Decryption during a case:

**IMPORTANT:** Once the partition has been decrypted, it is necessary to process the file system on the partition, shown in Figure 264 below:
Figure 264, Process the decrypted Bitlocker partition
20.3 IDENTIFYING OTHER ENCRYPTED FILES

20.3.1 IDENTIFYING ENCRYPTED FILES USING ENTROPY

The entropy score of a file is an expression of randomness where the more random the data, the higher the score. Encrypted files have a high entropy score.

To calculate file entropy scores in a case:

1. In the File System module click the Analysis Programs button and select Entropy Analysis from the drop down menu.
2. Add the Entropy column to the display.
3. Double click on the column name to sort by Entropy.

It is expected that an encrypted file will have an entropy score of .995 or higher, as shown in Figure 258 above.

The limitations of using entropy to identify encrypted files include:

- Many files, e.g. ZIP, have a naturally high entropy score and false positives may occur.
- Depending on the type of encryption used, a protected file may not have an entropy score above .995, as shown in Figure 258 above with the Microsoft Word Password Protected File.docx.

20.3.2 IDENTIFYING ENCRYPTED FILES USING A THIRD PARTY TOOL

The most well know tool to identify encrypted/password protected files is Passware’s free Encryption Analyzer, available at: https://www.passware.com/encryption-analyzer/.

To identify encrypted files using Passware Encryption Analyzer and Mount Image Pro (provided with Forensic Explorer):

1. Install the latest version of Mount Image Pro from www.mountimage.com (requires a reboot after install to load the mount drivers).
2. Run Mount Image Pro from the desktop icon.
3. Click the Mount button in the GUI toolbar.
4. Click Add Image and add the required image to the Device Selection window:
5. Click the Mount button.

6. Mount the image as File System with the following settings (File System ensures access to all files, including deleted, system and hidden):
7. If additional images are added, it is possible to add to the same drive letter under the **Mount Points** option.

8. Click **OK** to mount the drive.
4. Launch Passware Encryption Analyzer and scan the mounted drive:

Figure 268, Passware Encryption Analyzer
Chapter 21 – Date and Time

In This Chapter

CHAPTER 21 - DATE AND TIME

21.1 Date and time in computer forensics ................................................................. 298
21.2 FAT, HFS, CDFS file system date and time ......................................................... 298
21.3 NTFS, HFS+ file system date and time ................................................................. 298
21.4 Date and time information in the Windows registry ........................................... 298
   21.4.1 Manually examine registry for time zone information .................................. 299
   21.4.2 Extract time zone information using a script ................................................. 301
21.5 Daylight saving time (DST) .................................................................................. 302
21.6 Adjusting Date in Forensic Explorer ..................................................................... 302
   21.6.1 Setting the Time Zone for the Case ............................................................... 303
   21.6.2 Setting the Time Zone for evidence items .................................................... 304
   21.6.3 Synchronizing time zones ............................................................................. 307
21.1 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 8.11 - Filesystem Record view, for more information).

21.2 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.

21.3 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).

To display date and time information in a format relevant to the end user’s location, the UTC time is translated into local time using the computers time zone setting.

21.4 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):
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.

21.4.1 MANUALLY EXAMINE REGISTRY FOR TIME ZONE INFORMATION

Registry files are 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**

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 270 below:
Figure 270, Windows registry:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
Image file: NIST Hacking Case (15)

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.

### 21.4.2 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:
21.5 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**

<table>
<thead>
<tr>
<th></th>
<th>Clocks forward 1 hour</th>
<th>Clocks back 1 hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>1986 - 2006</td>
<td>First Sunday of April</td>
<td>Last Sunday of October</td>
</tr>
<tr>
<td>2007 onward</td>
<td>Second Sunday of March</td>
<td>First Sunday of November</td>
</tr>
</tbody>
</table>

Microsoft released a patch for the NTFS file system to compensate for the 2007 change (See [http://support.microsoft.com/kb/931836](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.

21.6 ADJUSTING DATE IN FORENSIC EXPLORER

In Forensic Explorer, date and time can be adjusted for a:

**Case:** Date and time settings are applied to all evidence items within the case;

or,
Evidence: When case time is not set (i.e. case time is “None”), evidence items, including devices and/or volumes, can be individually set.

IMPORTANT: A case time setting has precedence over evidence time settings.

21.6.1 SETTING THE TIME ZONE FOR THE CASE

Case time zone settings are applied when the case is created in the Evidence module, as shown in Figure 272 below:

Figure 272, Setting a Case Time Zone (Local Time shown)

The default case time zone settings applied by Forensic Explorer is Local Time, i.e. the settings of the forensic examiners computer. If the device or forensic image originates from the same time zone as the forensic analysis computer, then usually no adjustment is required.

To change case time zone settings during a case:

1. In the File System module, right click on the case folder;
2. From the drop down menu select the **Modify time settings** option;

As shown in Figure 273 below:

*Figure 273, Adjusting Case Time Zone Settings*

---

**21.6.2 SETTING THE TIME ZONE FOR EVIDENCE ITEMS**

When examining NTFS or HFS+ file system, to view date and times zones per 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). To cope with evidence items from multiple time zones, it can be necessary to adjust date and time settings for individual evidence items. For example, your **forensics lab** and computer is 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.

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). If the device or forensic image is collected from a different time zone, change the time zone setting to the source location to display file date and times per that location using the **TimeZone** drop down menu shown in Figure 274 below:
IMPORTANT: A **case time setting** has precedence over **evidence time settings** so the case time setting must be set to ‘**None**’ before evidence time settings will take effect.

### TO CHANGE EVIDENCE TIME ZONE SETTINGS DURING A CASE

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:
2. Select the **Time Zone** 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 be displayed next to the device, as shown in Figure 277 below:
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).

### 21.6.3 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.

**IMPORTANT**: A case time setting has precedence over evidence time settings. The case time will be applied to all evidence items irrespective of their individual settings.

**EXAMPLE**

A new case is created with two evidence files:

- The **case time zone setting** is set at None;
- 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 22 - Hash Sets

In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 22 - HASHING</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.1 Hash Values ................................................................. 310</td>
</tr>
<tr>
<td>22.2 Hash Algorithms .............................................................. 310</td>
</tr>
<tr>
<td>22.3 Acquisition Hash ............................................................. 310</td>
</tr>
<tr>
<td>22.4 Verification Hash ............................................................. 310</td>
</tr>
<tr>
<td>22.5 Hashing files in a case ....................................................... 312</td>
</tr>
</tbody>
</table>
22.1 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.

22.2 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 x 10^38”. (EnCase Forensic Version 6.10 User Manual. s.l. : Guidance Software, 2008 (16 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.

22.3 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 280, Acquisition and Verification hashes.

22.4 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 278, Evidence Processor](image)

2. **Calculate the verification hash during a case:**

   a. In the **File System module**, run the “Verify Device Hash” script accessed from the **Hash Files** toolbar button:

   ![Figure 279, Running the Verify Device Hash from the File System module toolbar](image)
The verification hash is written to the evidence module with the acquisition hash, as shown below:

**Figure 280, Acquisition and Verification hashes**

---

### 22.5 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 281, File System module Hash Files button**

2. This opens the Hash Files Options window:
Source

A hash of files will take place in the module that the hash is run. For example, if the button in pressed in the Email module, a hash is calculated for the messages and attachments in that module.

The hash can be calculated or 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 check, 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.
**22.5.1 HASH METHODS**

**CRYPTO HASH METHODS**

A crypto hash is used to determine if two files contain identical data. A cryptographic hash function takes an input (file data) and calculates and returns a fixed-size alphanumeric string called the Hash Value. The common and well-documented formats used in computer forensics are **CRC, MD5, SHA1 and SHA256**.

Historically MD5 has been the mainstay of computer forensics. More recently, due to the possibility of MD5 hash collisions (see: [https://en.wikipedia.org/wiki/MD5](https://en.wikipedia.org/wiki/MD5)) the stronger SHA1 is increasingly used.

**SIMILARITY HASH METHODS**

**DIFFERENTIAL HASH (FIND VISUALLY SIMILAR GRAPHICS)**

A differential hash is a 64 bit number. The hash is created by:

- Grey-scaling a graphic;
- Shrinking the graphic to 9 x 8 in size;
- Setting each bit for the hash to a +/- according to whether the previous pixel is greater or less than the current pixel (hence the differential).

More detailed information on the differential hash process is available here: [http://www.hackerfactor.com/blog/?/archives/432-Looks-Like-It.html](http://www.hackerfactor.com/blog/?/archives/432-Looks-Like-It.html)

A differential hash can be used to locate similar graphics in a case, as shown in the following examples.

**Example 1:**

In the following example 1.JPG is **checked as the source file**. Other variations of this file exist in the case (e.g. 1-blur.bmp, 1-gamma.bmp, etc.), as well as an identical file in a sub-folder also called 1.JPG.
To locate graphics visually similar to 1.JPG:

1. **Differential Hash the files**
   
   In the File System module click on the **Hash Files** button and check the **Differential Hash (graphics only)**. Click OK to run the hash and a **Hash (Differential)** column is created containing the differential hash value.

2. **Run Match Visually Similar Graphics (Differential Hash)**

   A comparison between differential hashes is determined by calculating the **Hamming Distance** (see: [https://en.wikipedia.org/wiki/Hamming_distance](https://en.wikipedia.org/wiki/Hamming_distance)). In the File System module click the **Hash Match** button drop down menu and select **Match Visually Similar Graphics (Differential Hash)**:
3. The following option window will open:

In this example **1.JPG** is checked as the source file. The maximum difference score is set at 10 (no files with a greater score will be included in the result). Clicking **Run** produces the following output:
We can see that each of the 8 files similar to 1.JPG have been identified. The scores range from 0 (the identical file 1.JPG in the sub-folder) to 9 (the pixilated version of the picture).

As the **Bookmark Results** option was selected the matching files were bookmarked and grouped in folders according to their difference score, as shown in Figure 287:

*Figure 287, Bookmark results of Find Similar Graphics (Differential Hash)*
Example 2

A the following digital photo is retouched to blue the outline of the hair:

Figure 288, First edit of digital photograph

The original file is used as the source. Running a **Match Visually Similar Graphics (Differential Hash)** identifies the touched file (Blur_Hair.png) with a 0 score (the highest possible match), as shown below:

Figure 289, FEX search results

The Blur_Hair.png file is edited a second time to add a yellow circle, thus increasing the visual difference between the original and the new file Yellow.png:
Figure 290, Second edit of digital photograph

The original file is used as the source. Running a Match Visually Similar Graphics (Differential Hash) identifies the Yellow.png with a score of 7.

Figure 291, FEX search results

PHOTO DNA

PhotoDNA is a technology developed by Microsoft and improved by Hany Farid of Dartmouth College that computes hash values of images, video and audio files to identify alike images.[1] PhotoDNA is primarily used in the prevention of child pornography, and works by computing a unique hash that represents the image. This hash is computed such that it is resistant to alterations in the image, including resizing and minor color alterations.[1] It works by converting the image to black and white, re-sizing it, breaking it into a grid, and looking at intensity gradients or edges. (https://en.wikipedia.org/wiki/PhotoDNA, October 2017).

GetData Forensics is licensed to distribute Photo DNA to law enforcement agencies solely for the purpose preventing the spread, or investigation targeted to stop the distribution and possession, of child sexual abuse content. Photo DNA files are not shipped with Forensic Explorer, which is why this option may appear to be
disabled in the File System module Hash Files menu. To request the Photo DNA files, please contact support@getdata.com from a law-enforcement email address identifying your status to meet these requirements. Further information will then be provided.

FUZZY HASH (FIND SIMILAR FILES)

A fuzzy hash uses context triggered piecewise hashing to identify almost identical files. (See: Identifying almost identical files using context triggered piecewise hashing, Jesse Kornblum, Digital Investigation, September 2006, Pages 91-97, Elsevier, September 2006). The implementation used in Forensic Explorer is detailed at: https://ssdeep-project.github.io/ssdeep/index.html

IMPORTANT: Fuzzy hash works on digital content. Many programs encode data when a file is written to disk. For example, a small edit and save of the digital photograph in Figure 288 above produces two files with almost entirely different content (shown as red below):

Figure 292, Binary comparison of Original.png and Blur_Hair.png shown in Figure 288 above

Similarly, a Microsoft Word.docx file that is edited with the addition of a single word, when saved will have an almost entirely different digital footprint.

For this reason, a Fuzzy Hash match is useful only for file formats where file encoding does not take place (e.g. the edit of a plain text document).

22.5.2 DUPLICATES

The “Find duplicate files” checkbox (shown in Figure 282 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 Count 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).

The Duplicate Count column has the following meaning:
Chapter 22 - Hash Sets

22.5.3 Filtering a Unique Data Set

A common objective of the investigator is to operate on a unique data set that contains no duplicates. This is usually done for speed purposes, as it can reduce the time needed for a keyword, index or similar search. The Duplicate Index column is used for this purpose.

The Duplicate Index column assigns a count to each duplicate. In below, there are three files with the same MD5 hash. The Duplicate Count column shows 3. The Duplicate Index column assigns 1, 2 and 3 to each file.

IMPORTANT: The Duplicate Count number is assigned per the sequence of the files as they were processed. The number is NOT an indication that one file has any greater relevance than the next.

To locate only unique files a case:

A unique data set consists of all files that have a Duplicate Index that is blank and all files that have a Duplicate Index of 1.

- In the Text Typing filter, this is achieved by <=1

![Figure 293, Identifying duplicate count and duplicate index](image)

22.6 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.

Hash 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.

### 22.6.1 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 22.8.2 below).

The default hash set location is: `[profile]\Documents\Forensic Explorer\HashSets`

### 22.7 DOWNLOAD HASH SETS

Hash Sets for use with Forensic Explorer are available for download from: [http://www.forensicexplorer.com/hashsets.php](http://www.forensicexplorer.com/hashsets.php). Hash sets from other trusted locations can also be used.

### 22.8 CREATING HASH SETS

Before creating a custom hash set, files in a case must be hashed. Follow the instructions in 22.5 above.

#### 22.8.1 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**:
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 22.9- Hash Match, below).

22.8.2 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 295, Flat Hash Set format**

```
# This is a Flat MD5 Hash Set file
# Hash Set Name = My MD5 List 1
# Identified As = Significant
83e05311eab2c2d50c2bc6fa219e6905
a526a99fc34e049360755d9f0450d662
b8bca7ac76f0ade815c5c743866293e0
```

A blank line = end.

**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 296 below .
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 294 above (This executes a script which can be viewed and edited in the Scripts module). The following window appears:
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 296 above.

### 22.9 HASH MATCH

A Hash Match is the process whereby hash values contained in a Hash Set are matched to hash values in a case.

To run a Hash Match:

1. Hash individual files in your case as described in 22.5 above.
2. In the File System module, click the Hash Match icon.

Figure 298, File System module, Hash Match icon

3. The Match Hash window will open:
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 300, Running a Hash Match in a case

<table>
<thead>
<tr>
<th>Hash (MD5)</th>
<th>Hash Set</th>
<th>HashSet Identified As</th>
</tr>
</thead>
<tbody>
<tr>
<td>b6d81b360a3672d80c27430f391532c</td>
<td>GetData [Windows]</td>
<td>good</td>
</tr>
<tr>
<td>4f1ba565d1c4efc927c9fa322685f26eb</td>
<td>GetData [Windows]</td>
<td>good</td>
</tr>
<tr>
<td>b93f3b3d1c3405725be765540d650111f</td>
<td>GetData [Windows]</td>
<td>good</td>
</tr>
<tr>
<td>fafa2e4af3be3b2232748d13e626a1</td>
<td>GetData [Windows]</td>
<td>good</td>
</tr>
<tr>
<td>07e5ced758a1c13c1a0e9c233365f</td>
<td>GetData [Windows]</td>
<td>good</td>
</tr>
<tr>
<td>9e8e6eca3902f3b40099759be3549b5a</td>
<td>GetData [Windows]</td>
<td>good</td>
</tr>
<tr>
<td>cdf80f3a8322550e8e61e6fe2995</td>
<td>GetData [Windows]</td>
<td>good</td>
</tr>
<tr>
<td>ba45c586456a672e033a875e44690eeb</td>
<td>GetData [Windows]</td>
<td>good</td>
</tr>
<tr>
<td>za44c7a5bae4c4867233b67e480684a8</td>
<td>GetData [Windows]</td>
<td>good</td>
</tr>
<tr>
<td>9d377b10c777c4938b3c7263a229e</td>
<td>GetData [Windows]</td>
<td>good</td>
</tr>
<tr>
<td>15988347a31ba4b5d6e89f913db76f</td>
<td>GetData [Windows]</td>
<td>good</td>
</tr>
</tbody>
</table>

An entry in the Hash Set column identifies that the file hash matches a hash in the set.

22.9.1 HASH MATCH WITH MULTIPLE HASH SETS

In the following example two has sets were created:

- **Cats.db3**, Identified as Bad, containing a hash for all 19 files in the Cats folder and its sub folders (including the Orange Cats folder);

- **OrangeCats.db3**, identified as Bad, containing a hash for 4 files in the Orange Cats folder;

As shown in Figure 301 below:
When a **Hash Match** is run using multiple hash sets (either one at a time or simultaneously) :

- the name of each matching hash set is appended to any existing text in the the **Hash Set** column and separated by a comma. For example, in Figure 302 below:
  - the text “**Cats**” identifies a Hash Match for the **Cats.db3** file only;
  - the text “**Cats,OrangeCats**” identifies a Hash Match in both **Cats.db3** and **OrangeCats.db3**;

- the **HashSet Identified As** name for each hash set is appended to existing text in the **HashSet Identified As** column, separated by a comma. For example, in Figure 302 below;
  - the text “**bad**” identifies a Hash Match for one of the hash sets; and
  - the test “**bad,bad**” identifies a match in both of the hash sets.
It can be seen from this example that providing a descriptive name for both the Hash Set Name and the Identified As text can be beneficial.

**Important:** The contents of the HashSet and HashSet Identified As columns are not saved with a case. Each time the case is opened, a new Hash Match must be run to re-populate this data. This is done so that if additional data is added to a case, or hashes are added to or removed from a Hash Set, the changes will be included in the next Hash Match.

---

### 22.10 PROJECT VIC™

“Project VIC is a global partnership that uses advanced technology to fight child sexual exploitation and trafficking. Using new forensic and data analytics tools, Project VIC identifies new victims of abuse and locates perpetrators around the globe. More than 2,500 law enforcement agencies in 40 countries use the technology developed by Project VIC’s partners to rescue child victims, apprehend offenders and secure crime scenes.” ([www.projectvic.org](http://www.projectvic.org), 25 October 17).

Project VIC™ files use a JavaScript Object Notation (JSON) format (see [https://en.wikipedia.org/wiki/JSON](https://en.wikipedia.org/wiki/JSON)).

In some situations an investigator may wish to export Project VIC™ JSON data to be used by a third party application.

**To Export a Project VIC™ JSON file:**

1. Files within the case must have an existing hash value (an MDS hash is mandatory). To has files, follow the instructions in 22.5 above.

2. In the File System module, click on the **Project Vic toolbar button**:

3. The Export JSON VIC File Options window will open:
a) Select to export Hashed or Check Hashed items;

b) Select the Project VIC model supported by the location where the file will be used;

c) In certain situations, in addition to the JSON file, it is beneficial to export the hashed files (for example the JSON file and data files may be imported into a third party application for classification). To export the data files linked to the JSON file, click the Export files and link checkbox.

d) Enter the destination path and JSON file name. Note: If the Export files and link option is checked, ensure there is sufficient space in the destination folder to export the files.
Chapter 23 - File Signature Analysis

In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 23 - FILE SIGNATURE ANALYSIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>23.1 File signature analysis ................. 334</td>
</tr>
<tr>
<td>23.2 Why run file signature analysis? ........... 334</td>
</tr>
<tr>
<td>23.3 Running a file signature analysis .......... 334</td>
</tr>
<tr>
<td>23.4 Examine the results of a file signature analysis .... 336</td>
</tr>
</tbody>
</table>
23.1 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 304, JPEG file signature Figure 304 below, is the beginning of a photo taken with a digital camera. It is identified as a JPEG by the file header ýØýà· (or in Hex: FF D8 FF E0 00).

Figure 304, 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.

23.2 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 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:

- Identify 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;

23.3 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) to open the Signature Analysis Options window shown in Figure 306, Selecting file types for signature analysis, below:
2. Or, right click on a file in the File System module and select Determine File Signature from the drop down menu. This method will determine the File Signature of the currently highlighted file/s and add the result to the File Signature column. If more than 1000 files are highlighted the Signature Analysis Options window shown below will open:

Figure 306, Selecting file types for signature analysis
Find: 
Use this filter to find a specific file type.

Force Determination: 
If the File Signature is already determined this setting will force a re-determination of the signature rather than using the existing value.

Insert new columns at... 
File Signature results are added to the File Signature column of the File System module. The default columns position is 3.

3. 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 19 - Scripts Module, for more information on writing scripts).

23.4 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 306 above; or,

b. No Size: The file does not have a logical or physical size, or the file does not have a run list in the Master File Table.

c. Folder: A folder.

d. Unknown: The file signature could not be matched against the files types contained in the Forensic Explorer signature list.

e. is blank: A signature analysis has not been conducted for this file.

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 307 below:
Figure 307, File System module columns relating to file extension

<table>
<thead>
<tr>
<th>Filename</th>
<th>Extension</th>
<th>File Signature</th>
<th>Extension Msr</th>
</tr>
</thead>
<tbody>
<tr>
<td>apple-pie.XLS</td>
<td>.XLS</td>
<td>JPG</td>
<td>Yes</td>
</tr>
<tr>
<td>apple-and-rhubarb-crumble.DOC</td>
<td>.DOC</td>
<td>JPG</td>
<td>Yes</td>
</tr>
<tr>
<td>Baileys - cheesecakes.PPT</td>
<td>.PPT</td>
<td>JPG</td>
<td>Yes</td>
</tr>
<tr>
<td>Bolognese-sauce.PDF</td>
<td>.PDF</td>
<td>JPG</td>
<td>Yes</td>
</tr>
<tr>
<td>Orange Cats</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CatsB8_TC.JPG</td>
<td>.JPG</td>
<td>JPG</td>
<td>No</td>
</tr>
<tr>
<td>CatsB3_CharlieTuna.JPG</td>
<td>.JPG</td>
<td>JPG</td>
<td>No</td>
</tr>
<tr>
<td>CatsB1_Corduroy.JPG</td>
<td>.JPG</td>
<td>JPG</td>
<td>No</td>
</tr>
</tbody>
</table>
# Chapter 24 - Data Recovery

## In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 24 - DATA RECOVERY</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>24.1 Data Recovery - Overview</td>
<td>340</td>
</tr>
<tr>
<td>24.2 FAT data recovery</td>
<td>341</td>
</tr>
<tr>
<td>24.2.1 FAT - Deleted files</td>
<td>341</td>
</tr>
<tr>
<td>24.2.2 FAT - Recover folders</td>
<td>345</td>
</tr>
<tr>
<td>24.3 NTFS data recovery</td>
<td>348</td>
</tr>
<tr>
<td>24.3.1 NTFS - deleted files</td>
<td>348</td>
</tr>
<tr>
<td>24.3.2 NTFS - orphans</td>
<td>349</td>
</tr>
<tr>
<td>24.3.3 NTFS - Recover Folders</td>
<td>350</td>
</tr>
<tr>
<td>24.4 File carving</td>
<td>351</td>
</tr>
<tr>
<td>24.4.1 Carving advantages and limitations</td>
<td>351</td>
</tr>
<tr>
<td>24.4.2 Forensic Explorer file carving engine</td>
<td>352</td>
</tr>
<tr>
<td>24.4.3 Carving using scripts</td>
<td>355</td>
</tr>
</tbody>
</table>
24.1 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.
24.2 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 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.

24.2.1 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 308 below:

Figure 308, 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 308 above with the deleted file “_UNNY.JPG” (originally called “BUNNY.JPG”) has it first character replaced, but Koala.JPG in the same folder retains its original file name.

The starting character of as 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.

Were a file having both a SFN and a Long File Name (LFN) directory entry, the missing first character of the file name is 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 309 below, the parent folder of the file Koala.JPG is highlighted in Folders view:

Figure 309, Animals folder selected in Folders view

The directory entries for the parent are displayed in Hex view:
The directory entries show:

- That file “ªOALA   .JPG” starts with the 0xE5 deleted file marker.
- It has both a short file name and long file name directory entry.

Koala.JPG is then highlighted and its directory entries are decoded in Filesystem Record view, as show below in Figure 311:

![Figure 311, Decoded directory entry of "Koala.JPG"](image-url)
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:

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 “FileExtent” 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 312, Display view of Koala.JPG

24.2.2 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 313, Recover Folders File System module toolbar icon

This opens the Recover Folders options window:
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, because 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 “Recover Folders X”, as shown below:

---

**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.
Figure 315, Recover Folders results
### 24.3 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 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.

#### 24.3.1 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 4, Allocation status for a file**

<table>
<thead>
<tr>
<th>Flag Value for a file</th>
<th>Hex</th>
<th>Binary</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>00</td>
<td>00000000</td>
<td>Unallocated</td>
</tr>
<tr>
<td></td>
<td>01</td>
<td>00000001</td>
<td>Allocated</td>
</tr>
</tbody>
</table>

**Table 5, Allocation status for a folder**

<table>
<thead>
<tr>
<th>Flag value for a folder</th>
<th>Hex</th>
<th>Binary</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>02</td>
<td>00000010</td>
<td>Unallocated</td>
</tr>
<tr>
<td></td>
<td>03</td>
<td>00000011</td>
<td>Allocated</td>
</tr>
</tbody>
</table>

In Forensic Explorer, the allocation status of a file is shown in Filesystem Record view when the file is highlighted:
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.

### 24.3.2 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 NTFS 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.
24.3.3 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:

This opens the Recover Folders options window:

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.
24.4 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” (17).

An example of a file signature is shown in Figure 319, which is the beginning of a .jpg file in Hex view:

Figure 319, View of .jpg file header

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 unallocated space of a file system and allows the investigator to recover files that have no metadata structures pointing to them”. (2)

24.4.1 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 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.

24.4.2 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 320, File System module, File Carve button

The “File Carving” selection window, shown in Figure 321 will open:
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.
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.

**SOURCE**

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 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 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 per that file type.

**LOGGING AND PRIORITY**

See 7.5 - Process Logging and Priority.

**24.4.3 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 19 - Scripts Module.
Chapter 25 - RAID

In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 25 - RAID</th>
</tr>
</thead>
<tbody>
<tr>
<td>25.1</td>
</tr>
<tr>
<td>25.2</td>
</tr>
<tr>
<td>25.3</td>
</tr>
<tr>
<td>25.3.1</td>
</tr>
<tr>
<td>25.3.2</td>
</tr>
<tr>
<td>25.3.3</td>
</tr>
</tbody>
</table>
25.1 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 to create a small number of large virtual disks out of many 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**.

A RAID 1 drive is added to Forensic Explorer using the Add Device (or Add Image) button in the Evidence module (it is not necessary to use the Add RAID button).

**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.

25.2 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?

### 25.3 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 ![Add RAID](image) button. This opens the RAID configuration window.

#### 25.3.1 HARDWARE RAID, KNOWN CONFIGURATION:

Enter the RAID configuration information:

```plaintext
RAID Configuration
RAID Name: User RAID
Type: Hardware
Format: RAID 5 (Striping with Redundancy)
Stripe size: 64

Raid 5 Options
First Checksum Device: 2
Checksum rotation direction: Left
Uses Asynchronous checksum rotation
```

and follow the instructions to add and test the RAID.

#### 25.3.2 SOFTWARE RAID

If it is a software RAID:

1. Set the "Type" of RAID to "software".

2. A valid software RAID will show with green ticks on the added drives (or image files):
25.3.3 ONCE THE CORRECT RAID LAYOUT IS IDENTIFIED

Once the correct RAID layout has been identified, click **SAVE** and **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 26 – Shadow Copy

In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 26 – SHADOW COPY</th>
</tr>
</thead>
<tbody>
<tr>
<td>26.1 Shadow Copy Introduction ................................................................. 362</td>
</tr>
<tr>
<td>26.1.1 Shadow Copy Configuration by Windows Users ....................................... 362</td>
</tr>
<tr>
<td>26.1.2 When are Shadow Copies created? ......................................................... 365</td>
</tr>
<tr>
<td>26.1.3 Where are Shadow Copies Stored .......................................................... 366</td>
</tr>
<tr>
<td>26.2 Examining Shadow Copies With Forensic Explorer ..................................... 367</td>
</tr>
</tbody>
</table>
26.1 SHADOW COPY INTRODUCTION

The ability of Forensic Explorer to easily access and explore 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)

26.1.1 SHADOW COPY CONFIGURATION BY WINDOWS USERS

Windows VSC controls are access 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 323 below:
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 324 below:
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 325 below:
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.

26.1.2 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. VSCs 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 VSC from the Windows System Properties > System Protection > “Create” button, shown in Figure 323 below.
26.1.3 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).
26.2 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 Copy button in the File System module toolbar:

   ![Shadow Copy button in the File System Toolbar](image)

4. The Forensic Explorer Volume Snapshot Mount window will open and list the available VSCs for the selected volume, as shown in Figure 327 below:

   ![Volume Snapshot Mount Window](image)

   **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 with 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 contain 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 copy 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 Figure 328 below:

*Figure 328, 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 column filter tool (see 9.11.2) can be used, as shown below:
Figure 329, 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 27 - Mount Image Pro

In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 27 – MOUNT IMAGE PRO</th>
</tr>
</thead>
<tbody>
<tr>
<td>27.1 Mount Image Pro ..........</td>
</tr>
<tr>
<td>27.1.1 Install and run Mount Image Pro</td>
</tr>
</tbody>
</table>
27.1 MOUNT IMAGE PRO

You Wibu dongle purchased with Forensic Explorer also contain a license key for Mount Image Pro.

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.

27.1.1 INSTALL AND RUN MOUNT IMAGE PRO

Mount Image Pro is a stand-alone application available for download from www.mountimage.com or http://download.getdata.com/MIP-Setup.exe (Note: To use Live Boot within Forensic Explorer you must have Mount Image Pro v6 or above installed).

Download and run the setup file and follow the onscreen installation instructions.

Run Mount Image Pro 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 shown in Figure 330 below:

**Figure 330, Mount Image Pro GUI**

Mount Image Pro 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.mountimage.com](http://www.mountimage.com) and in the support documentation for the product.
Chapter 28 – Live Boot

In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 28 – LIVE BOOT</th>
</tr>
</thead>
<tbody>
<tr>
<td>28.1 Live Boot .................................................................376</td>
</tr>
<tr>
<td>28.2 Requirements .............................................................376</td>
</tr>
<tr>
<td>28.2.1 FEX - Full Version (Dongle Activated) .........................376</td>
</tr>
<tr>
<td>28.2.2 Mount Image Pro v6 (or above) ..................................376</td>
</tr>
<tr>
<td>28.2.3 Virtualization software ............................................377</td>
</tr>
<tr>
<td>28.3 Compatibility ..............................................................379</td>
</tr>
<tr>
<td>28.4 Live Boot Working Folder .............................................380</td>
</tr>
<tr>
<td>28.5 How to Live Boot a Forensic Image ................................380</td>
</tr>
<tr>
<td>28.6 Live Boot and User login Password bypass .......................386</td>
</tr>
<tr>
<td>28.6.1 Windows User Password Recovery ...............................386</td>
</tr>
<tr>
<td>28.6.2 Windows user Password Bypass ....................................389</td>
</tr>
<tr>
<td>28.6.3 MAC Password Bypass ...............................................395</td>
</tr>
<tr>
<td>28.6.4 MAC Keychain Password .............................................404</td>
</tr>
<tr>
<td>28.7 Troubleshooting Live Boot ...............................................405</td>
</tr>
<tr>
<td>28.8 Creating A deployable live boot ......................................409</td>
</tr>
<tr>
<td>28.8.1 Method 1 (Automated Using a Script) ............................409</td>
</tr>
<tr>
<td>28.8.2 Method 1 (MANUAL method) .......................................413</td>
</tr>
<tr>
<td>28.8.3 Method 2 .................................................................419</td>
</tr>
</tbody>
</table>
28.1 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.

28.2 REQUIREMENTS

Live Boot has the following requirements:

28.2.1 FEX - 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.

28.2.2 MOUNT IMAGE PRO V6 (OR ABOVE)

GetData’s Mount Image Pro is used to mount a forensic image to make it accessible to Live Boot. A purchase of Forensic Explorer includes a license for Mount Image Pro on the same dongle.

The latest version of Mount Image Pro is available at:

- [www.mountimage.com](http://www.mountimage.com);
- [http://download.getdata.com/MountImagePro-Setup.exe](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 331 below;
28.2.3 VIRTUALIZATION SOFTWARE

At least one of the following virtualization tools must be installed:

**VIRTUAL BOX (RECOMMENDED)**

Forensic Explorer 3.5.7.5214 and above supports Live Boot using Oracle Virtual Box. This is Open Source visualization software available for download at [www.virtualbox.org](http://www.virtualbox.org).

**VMWARE**

The following VMWare applications are supported:

- **VMWare workstation** (commercial)

- **VMWare Player** (free for non-commercial use)
  [https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/6_0](https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/6_0).

**IMPORTANT**: Adding additional drives requires VMWare Workstation and will **not work with VMWare Player**. See Figure 332 below. VMWare does **NOT** support booting of MAC system, VirtualBox must be used.

**NOTE**: If you are installing **VMWare Player** you must run VMWare Player and agree to the terms and conditions, shown in Figure 332 below, before running Live Boot:
Figure 332, VMWare Player Terms

![VMware Player 7 Welcome Screen](image)

- **VMWare Player Plus** (Commercial)
  

**INSTALLING VMWARE TOOLS (AFTER BOOTING)**

**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 339 below. If you receive the following VMware error message:

![VMware Error Message](image)

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:

![Virtual Machine Settings]

4. Restart the virtual machine, and click on the Install button to install VMWare Tools.

**USING SHARED FOLDERS IN VMWARE (AFTER BOOTING)**

With shared folders, you can easily share files among virtual machines and the host computer. To use shared folders, you must have the current version of VMware Tools installed in the guest operating system and you must use the Virtual Machine Control Panel to specify which directories are to be shared.

To set up one or more shared folders for a virtual machine, be sure the virtual machine is open in Workstation and click its tab to make it the active virtual machine. Go to Edit > Virtual Machine Settings > Options and click Shared folders (See https://www.vmware.com/support/ws4/doc/running_sharefold_ws.html for additional documentation).

### 28.3 COMPATIBILITY

**Forensic Image Files**

Live Boot requires a forensic image of a physical device that contains a bootable file system (Live boot does not currently support the booting of logically acquired partitions).

**Supported Target Operating Systems**

Live Boot will boot the following Operating Systems:
• Windows 95, 98, XP, Vista, 7, 8, 10 (including GPT partitioned drives);
• Windows Server 2012;
• Linux.
• Macintosh HFS (VirtualBox must be used as the virtualization software).

## 28.4 LIVE BOOT WORKING FOLDER

**IMPORTANT:** Live Boot requires a working folder to store the Mount Image Pro disk cache and working files. Each time a Live Boot session is started a working folder is created in the Live Boot folder of the current case path, in the format:

```
[user]\Documents\Forensic Explorer\Cases\[Case Name]\Live Boot\[Boot Image Name + Date Time stamp]
```

As shown below:

*Figure 335, Current Case folder showing Live Boot working folder*

The data for each Live Boot session is retained to enable the re-open in the virtualization software of a Live Boot session at a specific point in time. If individual sessions are no longer required they can be deleted.

## 28.5 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](http://www.cfreds.nist.gov/Hacking_Case.html)). The image is booted using Virtual Box as the virtualization software.

1. **Check installed software:** Ensure that all required software is installed (as detailed in section 28.2 above).

2. **Start a Forensic Explorer case:** Run Forensic Explorer and start a Preview or Case. Add a forensic image file of a Windows disk to the preview or case. If the original computer had additional data disks, also add the forensic image files of these disks.

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 336, Live Boot Options**

- **Device to Boot**: Select the device to boot from the drop down menu;
- **Detected OS**: The OS found on the Device to Boot;
- **Boot to ISO**: Boot the device using an ISO image (used primarily for password cracking (see below));
**Boot Date/Time:** Defaults to Last Shutdown Time (or if not found the current date time). Edit these setting to adjust to a custom date time, or use the drop down menu below.

**Use Date/Time:** Select the:
- MAC (scans the partition on the physical drive to locate the latest date which is a non-future date);
- Last Shutdown (from the registry);
- Current (system clock of the forensic workstation);

From the drop down menu to change the Boot Date/Time;

**Memory (MB):** Default RAM size has been preselected depending on the Operating System detected. Additional memory can be allocated as required (for more information see: [http://support.theenterprisecloud.com/kb/default.asp?id=344&Lang=1](http://support.theenterprisecloud.com/kb/default.asp?id=344&Lang=1)).

**Bypass Windows Passwords:** This option will blank Windows user passwords. See password cracking below. To bypass Windows 10 passwords see 28.6 below.

**Start Virtual Machine:** Launches the virtual machine automatically.

**Minimize Pending Windows Updates**
- This option will limit Windows updates to only those that have started but are not yet complete. No new updates will be started.

b. Ensure that ‘Hard Disk 1 (Boot)’ contains the required image.

c. To add additional Hard Drives to the virtual machine click on the Extra HDDs tab:
Add additional hard drives:

If the suspect’s computer had additional disks, then these disks can be added to the virtual machine.

**IMPORTANT:** Adding additional drives requires VirtualBox, or VMWare Workstation (will not work with VMWare Player).

First, add the forensic images of the disks to the case, then add the additional disks to Live Boot. It is important that the disks are in the original order. For example, if Disk 1 contained the Windows installation, Disk 2 contained the My Documents folder, Disk 3 was an additional storage disk, and then it is important to keep this disk order so that the My Documents disk functions correctly when running in the virtualization software.

d. Switch from the Boot Options tab to the **VM Settings** tab:
e. Ensure that the paths to the installed virtualization software and Mount Image Pro v6 are correct.

f. Click Launch to proceed with the boot.

g. Information about the boot process is displayed in the process window. The virtualization software will then launch and the forensic image will boot, as shown in Figure 339 below:
**HINT:** In Virtual Box, to switch the mouse between the virtual machine and the desktop, use the **RIGHT CTRL Key** (in VMWare it is the CTRL – ALT keys).
28.6 LIVE BOOT AND USER LOGIN PASSWORD BYPASS

In many cases when Live Boot is used to launch a virtual machine access to the virtual computer will be blocked by a user account login screen. If passwords for the user accounts are unknown, there may be options to either recover or bypass the password.

28.6.1 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.

THIRD PARTY PASSWORD RECOVERY TOOL - 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 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 340 below:
c. Click OK to launch Ophcrack in the virtual machine.

d. Follow the on-screen Ophcrack prompts to commence the password breaking process, as shown in Figure 341 below:
Additional rainbow tables are available online. Click the Ophcrack Tables button to add additional tables (if using the Ophcrack vista/7 LiveCD additional Win7 tables are in the /media/hdc/tables folder). Refer to [http://sourceforge.net/p/ophcrack/wiki/ophcrack%20Howto/](http://sourceforge.net/p/ophcrack/wiki/ophcrack%20Howto/) for additional information.

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.
28.6.2 WINDOWS USER PASSWORD BYPASS

**FORENSIC EXPLORER PASSWORD BY-PASS**

Check the **Attempt to bypass Windows Local User Passwords** checkbox in the Live Boot Options window. Forensic Explorer will attempt to blank Windows user passwords. At the Windows login screen, login with a blank password.

**THIRD PARTY PASSWORD BY-PASS TOOL – PCUNLOCKER**

PCUnlocker from [http://www.top-password.com/reset-windows-password.html](http://www.top-password.com/reset-windows-password.html) is a recommended third party application for Windows user account by-pass (Learn more about PCUnlocker here: [http://www.top-password.com/guide/reset-windows-password.html](http://www.top-password.com/guide/reset-windows-password.html))

GetData has partnered with top-password.com to provide licensing solutions. Please contact [support@getdata.com](mailto:support@getdata.com) for more information.

**PCUNLOCKER - MBR (TRADITIONAL BIOS MODE) USING VIRTUALBOX**

1. In Forensic Explorer click the Live Boot button in the File System module to launch the Live Boot window.

2. In the Forensic Explorer Live Boot window check **Boot to ISO** and enter the path to the **pcunlocker.iso** file (31,370kb, MD5 6DDF065CF9B65F265E4654025FB00C58).

3. Click OK to boot and the Virtual Machine will launch PCUnlocker:
4. Highlight the required user accounts to bypass and select the **Reset Password** button. When the password has been successfully reset the password, column will show `<blank>`.

5. Once the required passwords have been bypassed, it is necessary to eject the virtual CD (the booting ISO image) from the virtual machine. In VirtualBox this is done by selecting **Devices > Optical Drives > Remove disk from virtual drive**, as shown in Figure 343 below (**Hint**: To unlock the mouse from the VirtualBox window, press the right CTRL key).

---

**Figure 342, PCUnlocker Windows’s password bypass**

![PCUnlocker screenshot](image)

**Figure 343, Ejecting a virtual CD (ISO image) in VirtualBox**

![VirtualBox eject CD screenshot](image)
6. Once the CD is ejected, press the **Restart** button in the PCUnlocker window. The virtual machine will then restart and boot into Windows. Bypassed Windows User Account passwords will be blank.

**Important:** The error message “FATAL: No bootable medium found! System halted.” Indicates the disk contains an EFI partition. Follow the instructions below:

*Figure 344, PC Unlocker – “Non-bootable medium found! System halted.”*

---

**PCUNLOCKER - EFI SYSTEM PARTITION USING VIRTUALBOX**

"**UEFI** is short for "Unified Extensible Firmware Interface". It's an advanced interface standard of firmware for operating system compared to legacy BIOS, such as it supports fast PC startup, bootable GPT **hard drive**, larger capacity more than 2T etc. Almost all recent PCs are **EFI/UEFI**. ([http://www.farstone.com/articles/what-is-uefi.php](http://www.farstone.com/articles/what-is-uefi.php)).

To bypass Windows user password on an EFI partition using VirtualBox and PCUnlocker it is necessary to **disable EFI** during the password bypass process. Follow these instructions:

1. Run Forensic Explorer and Live Boot the forensic image with VirtualBox using the default Live Boot settings (do not boot with pcunlocker.iso).

2. At the Windows login screen, shutdown the machine using the standard Windows shutdown procedure as shown in Figure 345 below (Windows must be shutdown correctly to obtain access to system boot settings in VirtualBox):
Forensic Explorer can now be closed as the remaining procedure is done using VirtualBox and PCUnlocker only.

3. Run Oracle VM VirtualBox from the desktop icon. In the left column, select the required virtual machine from the list. From the VirtualBox menu, select Machine > Settings > System to display the window shown in Figure 346 below. Uncheck the Enable EFI (special OSes only) box:

Figure 346, VirtualBox System Settings - Disable EFI
**Important:** If the Enable EFI (special OSes only) is greyed out, it means that the virtual machine is running, or Windows has not shutdown correctly (i.e. the running state of the virtual machine has been saved). Restart the virtual machine and power down using the Windows shutdown procedure.

4. With the virtual machine shutdown, in the virtual machine settings window, click on the Optical Drive hyperlink and select the pcunlocker.iso file, as shown in Figure 347 below:

![Figure 347, Select the PCUnlocker ISO from the VirtualBox settings window](image)

5. Click **Start** to launch the virtual machine and **boot with PCUnlocker**. Follow the PCUnlocker instructions to reset the required Windows user account passwords. Once the passwords have been reset, eject the virtual CD containing the pcunlocker.iso by selecting **Devices > Optical Drives > Remove disk from virtual drive** (as shown in Figure 343 above).

6. Power off the machine by selecting the X button in the top right corner of VirtualBox and select **Power off the machine**.
7. Once the machine is powered down go back to the **Machine > Settings > System** settings and re-check **Enable EFI** (special OSes only).

8. Ensure that in in the virtual machine settings window that the **optical drive** is **empty** (eject the pcunlocker.iso if it is still present).

9. Click **Start** to launch the virtual machine. The machine should now boot to the Windows Desktop with passwords bypassed.

---

**WINDOWS DOMAIN USER ACCOUNT BYPASS**

A Windows domain password cannot be recovered or bypassed because it relies on data stored on a remote (an no longer accessible) remote computer for authentication. In this situation the forensic examiner should attempt to gain access to a local administrator account that can be then used to log into the system and change the required user account authentication method (i.e. remove domain authentication and set the user account to have a known or blank local password).

Forensic Explorer users have also reported success with Forensit's User Profile Wizard 3.12 [https://www.forensit.com/downloads.html](https://www.forensit.com/downloads.html) in converting a domain account to a local account.
28.6.3 MAC PASSWORD BYPASS

SINGLE USER MODE – CREATE ADMINISTRATOR ACCOUNT

A Google search for ‘reset MAC user account’ will return many articles relating to the use of MAC Single-User mode. This is the MAC equivalent of accessing a Windows DOS shell where UNIX commands can be issued prior to startup.

Variations of Single-User password reset instructions exist, which can also vary between version of the MAC OS. In this example we use the following commands:

```
mount -uv /
rm /var/db/.AppleSetupDone
```

By deleting the .AppleSetupDone file the next boot will mimic a first install and prompt for the setup of an Administrator account. All system files, apps, personal data, etc., for any existing user accounts remains intact.

To by-pass a MAC user login using Single-User mode:

1. This procedure works only with Forensic Explorer Version 4. Ensure that Forensic Explorer v4 is installed.

2. Start a new case, add the forensic image (ensure that it is a bootable image that contains a Master Boot Record).

3. Click on the Live Boot button in the Forensic Explorer File System module toolbar to open the Live Boot Options window. The Detect OS should identify the type of MAC OS:

   ![Live Boot Options window showing detected MAC OS](image)

4. Click on the Advanced tab. Place a tick in the checkbox for Start MAC OS X in Single User mode (Virtual Box Only):
5. Click **Launch** to launch the virtual machine. The virtual machine will boot the Single-User mode command interface:

![Live Boot Options window Advanced tab](image)

6. At the command prompt, issue the command: `mount -uv /`

**IMPORTANT:** Manually type the above command (there may be invalid characters if copy and paste is used). There is a SPACE between the v and the forward slash.

![Entering UNIX commands in MAC Single-User mode](image)
7. At the command prompt, issue the command: `rm /var/db/.AppleSetupDone`

**IMPORTANT:** Manually type the above command (there may be invalid characters if copy and paste is used). There is a NO SPACE between the forward slash and the period.

Figure 353, Entering UNIX commands in MAC Single-User mode

```
bash-3.2# rm /var/db/.AppleSetupDone
bash-3.2# 
```

8. At the command prompt, type `exit` (to boot the virtual machine). During the startup process you will be prompted by a number of setup screens:

Figure 354, MAC setup

9. At the **Create a Computer Account** screen, enter your details for a new administrator account:
10. Click through the setup screens to reach the MAC desktop. Once at the desktop click on the **settings** button and then **Users & Groups**:

![Figure 356, MAC Settings button](image)

11. In the Users & Groups window, click on the lock icon in the bottom right hand corner and enter your new user account administrator credentials. This will unlock the ability to change passwords for other user accounts. Once the target account is unlocked, use the **Change Password** button.
12. Log out of your administrator account and log back in via the target account.
THIRD PARTY SOFTWARE – KON-BOOT

It is possible to bypass MAC user passwords with a third party commercial tool called Kon-Boot for Mac OSX (http://www.piotrbania.com/all/kon-boot/). This version includes the ISO image: Konboot.iso (MD5 Hash: 6D148A57181429F42F161387FD7A31B8). The most successful methodology is to use this tool to create a new administrator account through which other account passwords can be changed.

To by-pass a MAC user login with Kon-Boot:

1. Start a new case, add the forensic image (ensure that it is a bootable image that contains a Master Boot Record) and Live Boot the image using the instructions described above using VirtualBox as the virtualization software.
2. Once the MAC has booted to the MAC user login window, close the VirtualBox virtual machine and select to Power off the Machine.
3. Close Forensic Explorer, it is no longer required.

Figure 358, MAC user login window

4. Launch VirtualBox from the desktop icon.
5. The last Live Boot session will show at the bottom of the list in the left hand column:
6. In the VirtualBox Manager information window on the right hand side, under **Storage**, look for **[Optical Drive] Empty**. Right click and select “Choose disk image...”:

7. Select the konboot.iso downloaded earlier.

8. Launch the virtual machine (by pressing on the green start arrow in the VirtualBox manager toolbar) whilst pressing the **ESC** key to enter the virtual machine BIOS. TIP: When the virtual machine boot window first appears, click on it to ensure that it has focus and rapidly press the ESC key on your keyboard).
9. Successful access to the virtual machine BIOS will provide the following menu:

**Figure 361, MAC BIOS**

10. Select the **Boot Manager** menu option and then select to boot using **EFI DVD/CDROM**:

**Figure 362, MAC Boot Manager**

![Figure 363, MAC Kon-Boot user menu](image)

- Scanning all disk drives
- Found handles-6 (Sel.Name=7F64A910)
- Found our drive at index-1 (out of 6)
- MacBookEfi device found, id = 3 (7F620010)
- MacBookEfi device found, id = 4 (7F615E10)
- Found 2 mac devices?
- Installing our driver...
- Please pick your option (0-1):
  - [0] Use bypass feature (no new account)
  - [1] Use the-account feature (login: kon-boot password: kon-boot)

12. The MAC computer will then boot with a Kon-Boot user account displayed

![Figure 364, MAC Kon-Boot 'Other' user account](image)

13. Login via the Other user account, using username kon-boot, password kon-boot. Once logged in, click on the MAC System Preference icon:

![Figure 365, MAC System Preferences icon](image)
14. In the System Preferences select the Users & Groups icon. Click on the required user account, and click the Change Password button to enter new password details:

Figure 366, MAC System Preferences, Users & Groups

15. Log out of the kon-boot user account and then in to the target user account using the new password details.

28.6.4 MAC KEYCHAIN PASSWORD

Since Mac OS 8.6, the Mac has managed passwords with Keychain, Apple's password-management system. Learn more about keychain management here: http://www.macworld.com/article/2013756/how-to-manage-passwords-with-keychain-access.html

Once logged into the target account the password will not match the password of the original login keychain. To create a new key chain, follow these instructions: https://support.apple.com/en-au/HT202860#keychain.
28.7 TROUBLESHOOTING LIVE BOOT

Following the checks below to troubleshoot Live Boot:

Is there a valid Master Boot Record (MBR)?

Does the forensic image have a valid Master Boot Record (MBR)?

To boot a forensic image, it must be an image of a physical drive which contains a valid MBR. Check this in the File System module by selecting the image in the Folders view and viewing its child entries in the File List, as shown in Figure 367 below:

Figure 367, Checking for a valid MBR

Live Boot a NIST control image

Can the Live Boot NIST control image be booted successfully?

- Download and boot the NIST “Hacking Case” EnCase image available at: [http://www.cfreds.nist.gov/Hacking_Case.html](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.

Live Boot Configuration

Is VMWare Player or VMWare Workstation or Virtual Box installed?

- Check Live Boot Options (shown in Figure 338, Live Boot Options above) to confirm the correct path to the virtualization software executable file is visible, i.e.:
  - VMPlayer: C:\Program Files x86\VMware\VMware Player\vmplayer.exe. (If you are using VMPlayer ensure that you have entered your user details into the VMPlayer splash screen);
Is Mount Image Pro v6 installed? (Live Boot is NOT compatible with earlier versions);

- Check Live Boot Options (shown in Figure 338 above) to confirm the correct path to MIPv6:
  - C:\Program Files\GetData\Mount Image Pro v6\MIP.exe.

Mount Image Pro Checks

Mount Image Pro Cache and Virtualization 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 368 below:

  Figure 368, 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.

Is it possible that Mount Image Pro is timing out before the image is mounted?

- In the Forensic Explorer Live Boot window change to the Advanced tab and in the Mount Image Timeout (secs) increase the default setting to 360 seconds.

Copyright GetData Forensics Pty Ltd 2010 - 2019, All rights reserved.
BIOS – Intel Virtualization Technology

The live boot of a 64-bit virtual machine can require Intel Virtualization Technology to be enabled in the forensic workstation bios.

Additional information can be found at:


VMWare Checks

If you are using VMWare as the virtualization software, check the following:

---

**VMWARE PROCESSOR CHECK UTILITY FOR 64-BIT COMPATIBILITY**

Ensure that your forensic workstation can run a 64-bit virtual machine. Download the test utility VMware-guest64check[ver].exe using via the link below:

“When you power on a virtual machine with a 64-bit guest operating system, Workstation performs an internal check: if the host CPU is not a supported 64-bit processor, you cannot power on the virtual machine. VMware also provides this standalone processor check utility, which you can use without Workstation to perform the same check and determine whether your CPU is supported for virtual machines with 64-bit guest operating systems” [http://www.vmware.com/pdf/processor_check.pdf](http://www.vmware.com/pdf/processor_check.pdf), accessed 18 March 2015.

---

**KEYBOARD ISSUES**

VMWare keyboard communication issues can include:

- Slow or unresponsive keyboard;
- Unable to issue commands like CTRL/ALT/DEL

Most keyboard communication issues can be solved by installing VMware Workstation and using the custom setup option to add the Enhanced Keyboard Utility (if VMWare Workstation is already installed, re-run the setup and use the modify/change option). Forensic Explorer Live Boot will use the Enhanced Keyboard Utility if available.
Incompatible Security Software

Live Boot can conflict with specific security programs. Known programs are:

- Bitdefender Total Security 2015 (BSOD relating to trufos.sys);

Live Boot has been tested and is compatible with the following security products:

- ESET NOD;
- McAfee;
- Norton.

Contact technical support

Contact technical support (see Appendix 1 - Technical Support) with the supporting information from the above checks.
28.8 CREATING A DEPLOYABLE LIVE BOOT

A standalone Live Boot session can be created and provided to a third party to boot and review a suspect’s computer without Forensic Explorer. Two different methods are detailed below. In these instructions, the following terminology is used:

- **Forensic Workstation** (the computer used by the forensic examiner);
- **Examination Computer** (the computer used by the investigator running the Live Boot and reviewing the evidence);
- **Suspects Computer** (the computer displayed in the Live Boot session).

In the example below, Virtual Box is used to create a deployable Live Boot of the NIST Hacking Case (http://www.cfreds.nist.gov/Hacking_Case.html).

28.8.1 METHOD 1 (AUTOMATED USING A SCRIPT)

Method 1 requires **Mount Image Pro** be installed on the **Examination Computer**.

**ON THE FORENSIC WORKSTATION**

On the Forensic Workstation:

1. Follow the instructions in Chapter 28 to Live Boot the forensic image. Ensure to by-pass Windows login information and make any other changes needed to the running virtual machine.

2. Once booted, **power off the virtual machine** and **close Virtual Box**.

3. Open the **Mount Image Pro GUI**, click on **the Unmount button** and **Unmount All images**:

   ![Mount Image Pro GUI - Unmount All](image)

   The Mount Image Pro GUI should now be empty of image files.

4. In the File System module, from the Live Boot button drop down menu run the **Virtual Box – Create Live Boot Deploy Folder script** (this runs `Scripts\Live_Boot\Deploy_VirtualBox_Live_Boot.pas`):
5. The following input form will open:

Figure 371, Deployable Live Boot Folder for VirtualBox - Selecting the Live Boot Session folder

6. Select the Case Live Boot Session folder by clicking on the folder search button, navigating to the \Documents\Forensic Explorer\Cases[CaseName]\Live Boot\ folder and select the required Live Boot Session (the folder name identifies the date and time that the Live Boot session was created in Forensic Explorer).

7. **Export** path is automatically filled with the path to the case export folder. This can be modified and the folder written directly to another location.

8. **Boot Image** path is automatically filled with the current path to the booting forensic image.

  **Additional Disks** paths are automatically filled with the current path to the image files for any additional disks that were added when the Live Boot was created in Forensic Explorer.

  **IMPORTANT:** When the Live Boot Session folder is deployed to an Examination Computer the folder must have access to the required forensic images in these paths.
**Network Forensic Image store:** If you access forensic images from a central server (i.e. the same path from both the Forensic Workstation and the Examination computer) then this path can be used in the above fields.

**Stand Alone Examination computer:** If the examination computer is stand alone, then it is necessary to copy the required images to a folder on the computer that matches the paths used above.

9. Click the Run button and the configured Live Boot Session folder is exported to the specified location. The exported folder has the name: `Live Boot Deploy – [Forensic Image Name] [YY-MM-DD HHMMSS]` and includes the following files:

Figure 372, Configured Live Boot Session folder

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIPDisks 16-10-05 150224</td>
<td>05-Oct-16 4:00</td>
</tr>
<tr>
<td>NIST - 4Dell Latitude Cpi-liveboot</td>
<td>05-Oct-16 4:00</td>
</tr>
<tr>
<td>Live Boot Session Launch.bat</td>
<td>05-Oct-16 4:2</td>
</tr>
<tr>
<td>NIST - 4Dell Latitude Cpi.gdcache</td>
<td>05-Oct-16 4:0</td>
</tr>
<tr>
<td>NIST - 4Dell Latitude Cpi-liveboot.vmdk</td>
<td>05-Oct-16 4:0</td>
</tr>
<tr>
<td>READ ME.txt</td>
<td>05-Oct-16 4:2</td>
</tr>
</tbody>
</table>

**READ ME.txt** contains information about the Live Boot session, including the path to the required forensic image files.

**Live Boot Session Launch.bat** is the Windows batch file that is used to launch the Live Boot session.

**ON THE EXMAINATION COMPUTER**

1. Copy the **Live Boot Session folder** created above to the **Examination Computer**. Ensure that the path to the required image files detailed in **READ ME.txt** are valid (if not, re-create a new Live Boot Session folder using valid image paths).

2. Launch the by running the **Live Boot Session Launch.bat** file. A CMD window will open to configure and launch VirtualBox:
VirtualBox will then launch the session:

Figure 374, Deployed VirtualBox Live Boot Session Launch
28.8.2 METHOD 1 (MANUAL METHOD)

Method 1 (Manual) describes how to manually perform the process that is undertaken by the script in the description above.

METHOD 1 (MANUAL): ON THE FORENSIC WORKSTATION

On the Forensic Workstation:

1. Follow the instructions in Chapter 28 to Live Boot the forensic image. Ensure to by-pass Windows login information and make any other changes needed to the running virtual machine.

2. Once booted, power off the virtual machine and close Virtual Box.

3. Open the Mount Image Pro GUI, click on the Unmount button and Unmount All images:

   ![Image of Mount Image Pro GUI](Figure 375, Mount Image Pro - Unmount All)

   The Mount Image Pro GUI should now be empty of image files.

4. Using Windows Explorer open the Live Boot working folder (there is a shortcut to this folder from the Forensic Explorer Folder icon at the very top of the GUI). The working files for the Live Boot session will be contained in a folder that is named after the booted image with a date time stamp, as shown in Figure 376 below:

   ![Image of Live Boot working folder](Figure 376, Live Boot working folder)

   Copy this folder to the Examination Computer (see Step 1 below).
METHOD 1 (MANUAL): ON THE EXAMINATION COMPUTER

On the Examination computer:

1. **Copy the Forensic Explorer Live Boot working folder** (described above) from the Forensic Workstation to the Examination Computer. Error messages relating to missing ‘DiskX’ files can be skipped, as shown in Figure 377 below:

   Figure 377, Error message copying Live Boot sessions

   ![Error message](image1.png)

2. **Copy the forensic image files** to a folder on the Examination Computer (unless they are stored on a central server that is accessible to both the Forensic Workstation and the Examination Computer). In this example, the image files have been copied to a folder on the Examination Computer within the Live Boot working folder, as shown below:

   Figure 378, Examination Computer with Live Boot working folder and forensic image files

   ![Examination computer](image2.png)

3. **Run Mount Image Pro** (as local administrator). It can be run either from the desktop icon, or the Windows System tray. **Important:** If this is the first-time Mount Image Pro has been run on the
Examination Computer a Reboot is required to install the mount drivers. Check that the drives are correctly installed as shown in Figure 379.

4. In the Mount Image Pro GUI, click the Mount button and in the Device Selection window click the Add Image button to add the required image file, as shown below in Figure 380. Once added, highlight the image file and click the Mount button:

Figure 380, mounting an image using the MIP GUI

5. The image must be mounted with the following options:
Figure 381, Mount Image Pro settings when mounting for a deployable Live Boot

<table>
<thead>
<tr>
<th>Mount As:</th>
<th>Disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mount Points:</td>
<td>None (Physical Only)</td>
</tr>
<tr>
<td>Plug-and-Play:</td>
<td>Off</td>
</tr>
<tr>
<td>Access Mode:</td>
<td>Write to Cache</td>
</tr>
<tr>
<td>Sector Size:</td>
<td>512</td>
</tr>
<tr>
<td>Cache Folder:</td>
<td>C:\NIST - 4Dell Latitude CPI.E01</td>
</tr>
</tbody>
</table>

Use the following Settings:

- **Mount As:** Disk
- **Mount Points:** None (Physical Only)
- **Plug and Play:** Off
- **Access Mode:** Write to Cache
- **Cache Folder:** This is the path to the Live Boot working folder on the Examination computer (the cache file with the extension .gdcache is located in this folder).

Click OK to mount the image. Note the Physical Drive Mount Point number, as shown in Figure 382 below:
6. In the Live Boot folder open the .vmdk file in an editor (notepad++ is shown below).

**IMPORTANT:** vmdk files may be hidden files. Check your Windows file display settings to set hidden files to visible.

The PHYSICALDRIVE number in the Mount Image Pro GUI must match the physical drive number in the .vmdk file. If it does not match, edit and save the .vmdk file:

**Figure 383, Match the PHYSICALDRIVE number in the .vmdk with MIP**

7. In the Live Boot folder navigate into the folder ending with `-liveboot` to locate the .vbox file:
8. Open the .vbox file in a text editor (notepad++ is shown in the screenshot below). Ensure that the **HardDisk location tag** points to the correct .vmdk file in the copied Live Boot folder:

![Figure 384, Virtual Box .vbox file](image)

9. Double click the .vbox file to launch the virtual machine.
28.8.3 METHOD 2

Method 2 does not require a Mount Image Pro. It does however require the re-acquisition of the mounted physical drive from the forensic workstation so for this reason is a longer process.

On the Forensic Workstation:

1. Follow the instructions in Chapter 28 to Live Boot the forensic image. Ensure to by-pass Windows login information and make any other changes needed to the running virtual machine. Once booted, power off the virtual machine and close Virtual Box. Leave Mount Image Pro running.

2. In the Mount Image Pro GUI, take note of the physical drive number that was used during the Live Boot.

3. Use your forensic imaging tool (e.g. Forensic Imager, or FTK Imager) to forensically image the physical drive identified in the previous step. Create the image as a single DD file (do not segment). Once the DD image is created, unmount all drives and close Mount Image Pro.

On the Examination Computer:

1. Copy the Forensic Explorer Live Boot working folder from the Forensic Workstation to the Examination Computer.

2. Move the DD image of the physical drive in a location accessible by the Examination Computer.

3. Locate the .vmdk file in the Live Boot folder. Edit the file in notepad and ensure that the PHYSICALDRIVE points to the location of the newly created DD image. For example, in a test case the line was changed from: "RW 9514260 FLAT "\\PHYSICALDRIVE4" to "RW 9514260 FLAT "F:\NIST - Hacking Case\NIST_Live_Boot.001". Save the .vmdk file.

4. In the Live Boot folder navigate into the folder ending with ‘–liveboot’ to locate the .vbox file. Open the .vbox file in a text editor. Ensure that the HardDisk location tag points to the .vmdk file in the Live Boot folder.

5. Double click on the .vbox file to launch the virtual machine. The image will now boot without the need for Forensic Explorer or Mount Image Pro.
Chapter 29 – Forensic Image Converter

In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 29 – FORENSIC IMAGE CONVERTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>29.1  Forensic Image Converter</td>
</tr>
<tr>
<td>29.1.1 Program Features</td>
</tr>
<tr>
<td>29.1.2 Frequently Asked Questions</td>
</tr>
<tr>
<td>29.2  Download and Install Forensic Image Converter</td>
</tr>
<tr>
<td>29.3  Add Forensic Image Converter to the Windows Path</td>
</tr>
<tr>
<td>29.4  Launching the Windows Command Line</td>
</tr>
<tr>
<td>29.5  ConvertTOL01.EXE - Usage</td>
</tr>
<tr>
<td>29.5.1 CONVERTTOL01.EXE - Help</td>
</tr>
<tr>
<td>29.5.2 Example Conversion</td>
</tr>
<tr>
<td>29.6  Validation of Conversion</td>
</tr>
</tbody>
</table>
29.1 FORENSIC IMAGE CONVERTER

Forensic Image Converter is a standalone command line tool that is licensed with Forensic Explorer.

As the name suggest, this tool is used to convert forensic image files from one format to another. Forensic Image Converter currently supports conversion of:

- AD1 to L01
  (Additional conversion formats will be added).

29.1.1 PROGRAM FEATURES

Forensic Image Converter has the following key features:

- MD5 validation of source and destination MD5 hash during the conversion process;
- Set compression level and segment size;
- Batch process multiple input files using wildcards.

29.1.2 FREQUENTLY ASKED QUESTIONS

Doesn’t Forensic Explorer already convert AD1 to L01?

Yes. It is possible to export data that has been added into Forensic Explorer by selecting the required files from the File System module, and using the right-click menu option to export to L01 (For more information see Chapter 9.6.2).

Why would I use Forensic Image Converter?

Forensic Image Converter is most commonly used by agencies that have a need to convert many AD1 files into corresponding L01 files. Forensic Image Converter’s batch processing capability means that this process can be setup and run from a Windows Command Line with a minimum of user configuration.

29.2 DOWNLOAD AND INSTALL FORENSIC IMAGE CONVERTER

Download Forensic Image Converter from:


To install Forensic Image Converter:

1. Run the downloaded setup application (i.e. ForensicImageConverter(vX.X.XXX).exe);
2. Follow the onscreen instructions, as shown below:
Important: Forensic Image Converter is a Command Line Application. At the completion of install the setup will NOT create a desktop icon.

Forensic Image Converter will be installed into the default installation path:

```
C:\Program Files\GetData\Forensic Image Converter vX
```

And will install the default files shown in Figure 387 below:

The command line executable is:

- ConvertToL01.exe
29.3 ADD FORENSIC IMAGE CONVERTER TO THE WINDOWS PATH

Frequent users of Forensic Image Converter may choose to add the program into the Windows Path Environment Variable so that the executable can be run from any command line folder without the need for typing the installation path.

To add Forensic Image to the Windows Path Environment Variable:

1. Open the System Properties window by:
   a. Typing: sysdm.cpl; or
   b. Open the Control Panel, search for system and select the Edit the system environment variables option shown in Figure 388 below:

![Figure 388, Windows 10 Control Panel](image)

In the System Properties window select the Advanced tab then the Environment Variables button, as shown in Figure 389 below:
In the Environment Variables window, in the System Variables box, select Path, then press the Edit button, as shown in Figure 390 below:
In the **Edit environment, variable** window, click the **New** button and add the Forensic Image Converter Path:

```
C:\Program Files\GetData\Forensic Image Converter vX
```

as shown in Figure 391 below.
Once the variable has been added, close any existing command windows. Open a new command window to a folder other than in the installation folder, and type the command line filename `ConvertToL01.exe`. The conversion tool will then launch, as shown in Figure 392 below which has been executed from the folder “C:\”:

![Image of Command Prompt with conversion tool running]

Figure 392, Running ConvertToL01 after changing the Windows Path variable
29.4 LAUNCHING THE WINDOWS COMMAND LINE

**Important**: To avoid Windows permission errors it is recommended to run Forensic Image Converter from a Command Prompt launched with Administrator permissions.

To launch a Windows Command prompt with Administrator permissions:

1. Type **CMD** in the Windows search assistant bar;
2. In the display list, right-click on **Command Prompt Desktop app** and select **Run as administrator**, as shown Figure 393 below:

![Figure 393, Running a Windows Command Prompt with Administrator user rights](image)

29.5 CONVERTTOL01.EXE - USAGE

To convert an AD1 forensic image to a L01 forensic image open a Command Line window and run the ConvertToL01 program located in the default installation folder.

29.5.1 CONVERTTOL01.EXE - HELP

Launch a Windows Command Line window (as described in xx above) and navigate to the Forensic Image Converter installation folder:

```
C:\Program Files\GetData\Forensic Image Converter vX
```

There are two help switches:

- **ConvertToL01 /?**, and,
- **ConvertToL01 /Help**.

The output of these switches is shown below:
29.5.2 EXAMPLE CONVERSION

In the examples below the file TEST.AD1 is in the C:\ folder. Forensic Image Converter has been added to the Windows Path Environment Variable to enable its execution directly from the C:\ folder.

DEFAULT CONVERSION

The command:

- ConvertToL01 TEST.AD1

Is used to create a L01 file of the same name in the same folder:
SPECIFYING INPUT AND OUTPUT FILE PATHS

The command:

- ConvertToL01 “C:\TEST.AD1” “C:\This is a test.L01”

Specifies the input and output paths of the files:
BATCH CONVERSION USING DEFAULT OPTIONS

The command:

- ConvertToL01/*.AD1

Is used to convert all AD1 files in the current folder to L01 files of the same name to the same output folder:

![Command Prompt Output]

C:\>ConvertToL01 *.AD1
Convert to L01 v1.0 - GetData Forensics
Processing 2 files.

+++++++ File 1 +++++++
Input filename: TEST1.AD1
Output filename: TEST1.L01
Segment Size: 2000
Compression: Fast

Found 1524 files in TEST1.AD1
Number of HASH Matches = 0
Number of HASH Mismatches = 0
Number of No HASH files = 1525

+++++++ File 2 +++++++
Input filename: TEST2.AD1
Output filename: TEST2.L01
Segment Size: 2000
Compression: Fast

Found 1524 files in TEST2.AD1
Number of HASH Matches = 0
Number of HASH Mismatches = 0
Number of No HASH files = 1525

C:\>
29.6 VALIDATION OF CONVERSION

An MD5 hash validation is conducted during the conversion process. The sequence is as follows:

1. Forensic Image Converter reads the data in the source file and calculates the hash of each file during the read process;

2. Forensic Image Converter compares the calculated hash against the hash that is stored within the source file;

3. Forensic Image Converter writes each file to the output file and stores within the file the calculated hash.

Any difference between the hash stored in the source file and the calculated hash stored in the output file is reported as a Mismatch.

The Number of No HASH files are those files in the source file that did NOT have a hash value stored (e.g. Folders).

INDEPENDENT VALIDATION

To validate the conversion both source and output files should be added to a forensic tool. Individual file hashes between source and output file should match.
# Chapter 30 – Working with ...

## In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 30 – WORKING WITH ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>30.1</strong></td>
</tr>
<tr>
<td><strong>30.1.1</strong></td>
</tr>
<tr>
<td><strong>30.1.2</strong></td>
</tr>
<tr>
<td><strong>30.1.3</strong></td>
</tr>
<tr>
<td><strong>30.1.4</strong></td>
</tr>
<tr>
<td><strong>30.1.5</strong></td>
</tr>
<tr>
<td><strong>30.1.6</strong></td>
</tr>
<tr>
<td><strong>30.1.7</strong></td>
</tr>
<tr>
<td><strong>30.1.8</strong></td>
</tr>
<tr>
<td><strong>30.1.9</strong></td>
</tr>
<tr>
<td><strong>30.1.10</strong></td>
</tr>
<tr>
<td><strong>30.1.11</strong></td>
</tr>
<tr>
<td><strong>30.1.12</strong></td>
</tr>
<tr>
<td><strong>30.1.13</strong></td>
</tr>
<tr>
<td><strong>30.1.14</strong></td>
</tr>
<tr>
<td><strong>30.1.15</strong></td>
</tr>
<tr>
<td><strong>30.1.16</strong></td>
</tr>
<tr>
<td><strong>30.1.17</strong></td>
</tr>
<tr>
<td><strong>30.1.18</strong></td>
</tr>
<tr>
<td><strong>30.1.19</strong></td>
</tr>
</tbody>
</table>

| **30.2** | Thumbnails | 454 |
| **30.2.1** | Thumbs.db | 454 |
30.2.2 Thumbcache ........................................................................................................454

30.2.3 Forensic Value of Thumbnails ........................................................................454
30.1 ITUNES BACKUPS

iOS backups can be a source of high value information for the forensic investigator, particularly if the original iOS device cannot be located. iOS backups can contain call logs, SMS/MMS/Message history, application data, photos, email, device settings and other such data. This paper describes the processing of iOS device backups with Forensic Explorer software (www.forensicexplorer.com).

30.1.1 ICLOUD BACKUP

Apple’s iTunes software is used to backup an iOS device. In early versions of the iPhone (v 2, 3, 4), iOS backups were made to a computer only. At about the time of the release of the iPhone 5 in 2012, Apple introduced the additional option to backup to Apple iCloud online storage. Combined with other additional iCloud features, such as the ability to share data between different devices and to track, lock, or wipe a device remotely, iCloud accounts have become popular and in 2015 there are a projected 500 million iCloud accounts.

Figure 396, projected iTunes and iCloud usage (Source: http://www.asymco.com/2014/11/15/how-big-is-iCloud (18))

iCloud backups occur when this backup option is selected in iTunes and the device is locked and connected to Wi-Fi and a power source. A default iCloud account has a size limit of 5 GB (as of July 2015, although additional storage space can be purchased from Apple. iCloud accounts are password protected and the online storage is encrypted. Once an iCloud account is lawfully accessed the backup files can be processed using the techniques described below for computer based backups.

30.1.2 ITUNES BACKUP

Apple’s iTunes software is used to backup an iOS device to a computer. The backup can be performed via Wi-Fi or using a USB connection. The iTunes ‘sync’ option enables the end user to automate this process each time the device connects. If the sync option is disabled, then the user must manually initiate the backup process. These options are shown in the iTunes screen shot in Figure 397 below:
### 30.1.3 BACKING UP AN iOS DEVICE FOR THE FIRST TIME

When an iOS device is connected to a computer for the first time and synced (or backed-up) with iTunes, a folder is created using the **Unique Device Identifier (UDID)**, (referred to in this document as a ‘backup folder’.)

**iTunes UDID Backup Folders**

A backup folder is created using information specific to the iOS device. Backup folders are very distinctive as they are **40 hexadecimal characters in length**. When an original device is connected via iTunes the UDID can be found in the phone summary window by clicking on the serial number, as shown in Figure 398 below:

**Figure 398, iTunes options showing the UDID**

For more information on how UDIDs are created, see: [https://www.theiphonewiki.com/wiki/UDID](https://www.theiphonewiki.com/wiki/UDID) (19).

**Full, Incremental and Differential Backups**

When an iOS device is backed up for the first time it is a **full backup**. Subsequent backups are **incremental** where only the data that has changed since the last backup (be it full or incremental) is backed-up.

When an iOS device is updated or restored, an automated backup is initiated as a **differential backup**. A differential backup contains all files that have changed since the last full backup. A differential backup folder is created with the same UDID appended with the date and time of the backup, for example:

- 48be275db912427e61f1a074c6ce0f2c6a2e8920-20150719-170306
30.1.4 ENCRYPTED BACKUPS

iTunes provides the option to encrypt backups (as shown in Figure 397 above). During the backup process the user is prompted to enter a password to encrypt all files in the backup:

Figure 399, iTunes encrypted backup password request

Dealing with encrypted backups is further discussed in section 30.1.15 below.

30.1.5 IOS BACKUP PATHS

The default paths for iTunes backups are:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7/8</td>
<td>C:\Users[username]\AppData\Roaming\Apple Computer\MobileSync\Backup\</td>
</tr>
<tr>
<td>Windows XP</td>
<td>C:\Documents and Settings\username\Application Files\MobileSync\Backup\deviceid\</td>
</tr>
<tr>
<td>MAC OS X</td>
<td>[User HomeDirectory]\Library\Application Support\MobileSync\Backup\</td>
</tr>
</tbody>
</table>
30.1.6 LOCATING APPLE BACKUP FOLDERS WITH FORENSIC EXPLORER

iTunes backup folders can be quickly located in the Forensic Explorer File System module by using the iTunes Backups folders filter, as shown in Figure 400 below:

Figure 400, iTunes Backups filter applied in the File System module (two backup devices shown)

The iTunes Backups filter can be viewed (and edited) in the Scripts module. The filter identifies relevant files by searching file paths containing `\MOBILESYNC\BACKUP\`. 
30.1.7 INSIDE AN ITUNES BACKUP FOLDER

A typical iTunes backup folder contains many files, each with forty-character unique file names and no file extension, as shown in Figure 401 below:

Figure 401, Example content of an iTunes backup folder

The forty-character file names are generated by a SHA1 hash of the file name as it would appear on the iOS device, together with the path and domain name. For example, on the physical iOS device, the file:

HomeDomain-Library/SMS/sms.db, becomes:

3d0d7e5fb2ce288813306e4d4636395e047a3d28, as a backup folder.

Websites such as https://md5hashing.net/hashing/sha1 allow this process to be performed for a file.

Note: When dealing with logical iPhone acquisitions created with tools like Cellebrite, the iOS file names will appear in plain text and will not be SHA1 encoded.

30.1.8 THE IMPORTANCE OF FILE SIGNATURE ANALYSIS

It is important to note that because an iTunes backup file has no extension a File Signature analysis is required to identify the file type. This can affect the data displayed in Forensic Explorer, for example:

- If a Gallery view of an iTunes backup folder is conducted prior to a signature analysis, the gallery will be empty. Once a signature analysis has been conducted the same gallery view will show the thumbnail pictures contained within the backup folder;
- A plist file will only be passed and displayed in the File Metadata view if its signature is known.

This underlines the importance of running a File Signature Analysis early in the case. Figure 402 below shows the same list of files in Figure 401 after a File Signature Analysis has been run:
Figure 402, Example content of an iTunes backup folder after running a file Signature Analysis

<table>
<thead>
<tr>
<th>File List</th>
<th>Gallery View</th>
<th>Risk View</th>
<th>Category Graph</th>
</tr>
</thead>
<tbody>
<tr>
<td>File List</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Filename</th>
<th>Extension</th>
<th>File Signature</th>
<th>Extension Mismatch</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>188ac5cd7f49900e690cde252a78518f3688359681</td>
<td>JPG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>457a000399284460f732159b04eb0e04d/4df9</td>
<td>XML</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>6e5329a007b9a305a9f9a2d6e569b559e0e8</td>
<td>Text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>f2346e2a5f7f1202a599e5e39b50002024b3</td>
<td>XML</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>70811c883535660w9777f776656071ea990b1f0f9d</td>
<td>Plist (Binary)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6f38bea00e3f4f5e492e86325f18e62802ec4b4ce3</td>
<td>Text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0f3e1e4175ec3f3f2d65ebe2d31e996e2016e09597</td>
<td>Text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>fa9b370e8874770e55b012a495e0a2e2633a4a84</td>
<td>PNG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>f52b8b1d7b1e06f6715d6a0477371669f0226e8</td>
<td>JPG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>827b4b909c0a046010229ce6b03089e79e7</td>
<td>JPG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>1d1577de3329f93347220e2b1d1b0e06df7b0d0</td>
<td>JPG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>1e605f4b1436e881dee8123617e86b0994f6e5</td>
<td>XML</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>5a46622114ebd7e7d41e9901c501e93681af0a</td>
<td>XML</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>6e590b4f1518e5575800865e0a98c17959a1d4e5e</td>
<td>JPG</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## 30.1.9 KEY USER FILES IN AN ITUNES BACKUP

The following table lists iTunes backup files that may be of interest to the forensic investigator:

<table>
<thead>
<tr>
<th>Contents</th>
<th>Domain</th>
<th>iOS Path and file name</th>
<th>SHA-1 backup file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calendar</td>
<td>HomeDomain</td>
<td>Library/Calendar/Calendar.sqlitedb</td>
<td>2041457d5fe04d39d0ab481178355df6781e6858</td>
</tr>
<tr>
<td>Call History</td>
<td>WirelessDomain</td>
<td>Library/CallHistory/call_history.db</td>
<td>2b2b0084a1bc3a5ac8c27afdf14afbf42c61a19ca</td>
</tr>
<tr>
<td>Chat – KikChat</td>
<td>AppDomain-com.kik.chat</td>
<td>Documents/kik.sqlite</td>
<td>8e281be6657d4523710d96341b6f86ba89b56df7</td>
</tr>
<tr>
<td>Chat – Line</td>
<td>AppDomain-jp.naver.line</td>
<td>Documents/talk.sqlitedb</td>
<td>53a7099b474f4fb3f2cd006f8e59578d58fb44a</td>
</tr>
<tr>
<td>Chat – MessageMe</td>
<td>AppDomain-com.littleinc.MessageMe</td>
<td>Library/Application Support/MessageMe/MessageMe.sqlitedb</td>
<td>8c625842c0b74efff30d92eece44a1da30d2e8e</td>
</tr>
<tr>
<td>Chat – Skype</td>
<td>AppDomain.skype.skype</td>
<td>Library/Application Support/Skype/[user]/main.db</td>
<td></td>
</tr>
<tr>
<td>Chat – Touch</td>
<td>AppDomain-enflick.ping</td>
<td>Documents/Touch.sqlitedb</td>
<td>b18a30bf72824a7d024a95178ae42d8339f83633</td>
</tr>
<tr>
<td>Chat – Viber</td>
<td>AppDomain-com.viber</td>
<td>Documents/Contacts.data</td>
<td>b39bac0d347adafa17527f97c3a5fa3f726a3a</td>
</tr>
<tr>
<td>Chat – WeChat</td>
<td>AppDomain-com.tencent.xin</td>
<td>Documents/[chat-UDID]/DB/MM.sqlitedb</td>
<td></td>
</tr>
<tr>
<td>Chat - WhatsApp</td>
<td>AppDomain-net.whatsapp.WhatsApp</td>
<td>AppDomain-net.whatsapp.WhatsApp</td>
<td>1b6b187a1b6b9a68b720c79e2c67f472bab09c0</td>
</tr>
<tr>
<td>Contacts</td>
<td>HomeDomain</td>
<td>Library/AddressBook/AddressBook.sqlitedb</td>
<td>31bb7ba8914766d4a0d6df6113c8614be442</td>
</tr>
<tr>
<td>Keyboard</td>
<td>HomeDomain</td>
<td>Library/Keyboard/dynamic-text.dat</td>
<td>Changes with language installed</td>
</tr>
<tr>
<td>Locations</td>
<td>RootDomain</td>
<td>Library/Caches/locationd/consolidated.db</td>
<td>4096c9ec676f2847d283405900e28a7c815386*</td>
</tr>
<tr>
<td>Maps History</td>
<td>HomeDomain</td>
<td>Library/Maps/History.plist</td>
<td>b60c382887d5a562166f0f99f24797e55c12a94e4</td>
</tr>
<tr>
<td>Notes</td>
<td>HomeDomain</td>
<td>Library/Notes/notes.sqlitedb</td>
<td>ca3bc056d4da0bbf88b5fb3be254f3b7147e639c</td>
</tr>
<tr>
<td>Safari History</td>
<td>HomeDomain</td>
<td>Library/Safari/History.plist</td>
<td>1d6740792a2b845f4c5e62204c4906d7f0a8e8ab</td>
</tr>
<tr>
<td>SMS</td>
<td>HomeDomain</td>
<td>Library/SMS/sms.db</td>
<td>3d0df7e5f6b2c83813006e4d463635e047a3d28</td>
</tr>
<tr>
<td>Wifi Networks</td>
<td>SystemPreferencesDomain</td>
<td>SystemConfiguration/com.apple.wifi.plist</td>
<td>ade0340576ee14793e607073bd7e8e409af07a8</td>
</tr>
</tbody>
</table>

Removed from iOS backup (not the device) after iPhone 4.
30.1.10 ITUNES BACKUP CONFIGURATION FILES

In every iTunes backup folder there are four configuration metadata files:

- Info.plist
- Manifest.plist
- Status.plist
- Manifest.mbdb

These files are described in more detail below.

INFO.PLIST

The info.plist file contains device details, including:

- device name
- build version
- IMEI
- phone number
- last backup date
- product version
- product type
- serial number
- sync settings, and
- a list of application names that were installed on the device.

Forensic Explorer fully decodes the info.plist file in the File System module, Metadata data view, as shown in Figure 403 below:
Figure 403, manually examine the content of an iTunes info.plist file

The **status.plist** file contains the details about the backup, including the date, version, backup state, etc. This plist file is decoded using the File Metadata view as described above.

**MANIFEST.PLIST**

The **manifest.plist** file contains third party application details, as well as an additional source of serial, product type, UDID and date information. This plist file is decoded using the File Metadata view as described above.

**MANIFEST.MBDB**

The **manifest.mbdb** binary file contains information about all other files in the backup along with the file sizes and file system structure data. (Note: In older iOS versions, there were two files to perform this task, Manifest.mbdx and Manifest.mbdb). The mbdb file structure is provided in detail at: [http://www.securitylearn.net/tag/manifest-mbdb-format/](http://www.securitylearn.net/tag/manifest-mbdb-format/) (20).

### 30.1.11 PROCESSING ITUNES BACKUPS IN FORENSIC EXPLORER

Forensic Explorer automates processing of iTunes backups to assist the investigator to quickly identify relevant data.

### 30.1.12 STEP 1 - IDENTIFY AND BOOKMARK ITUNES BACKUP FOLDERS

The first step in the process it to locate and bookmark any iTunes backup folders located in the case:

To **identify and bookmark iTunes Backup folders**:

- In the File System module, under the Analysis Programs button, select **iTunes Backups – Identify and Bookmark**, as shown in Figure 404 below:
The **Identify and Bookmark** script automates the following functions:

1. **Locates iTunes backup folders** in the case;

2. **Bookmarks the backup folders** and uses the information contained within the `info.plist` to create a parent folder constructed of *device name, device model and device serial number*, as shown in Figure 406 below:

   ![Bookmarks module, iTunes backup folders](image)

   Click on the bookmarked file to display the bookmark comment containing additional information extracted from the `info.plist` file:
The following iTunes Backup Info was found:
- Build Version = 11D257
- Device Name = Aimee iPhone
- Display Name = Aimee iPhone
- GUID = 5DFA1D9CD6F29408E684F94747754870
- ICCD = 8901260261774999902
- IMEI = 012961004973953
- Last Backup Date = 2015-01-17T21:19:45Z
- Product Name = iPhone 4
- Product Type = iPhone3,1
- Product Version = 7.1.2
- Serial Number = DNRGQ6LNDP0N
- Target Identifier = 46ccc52c5cbd5ec19732d39d49ba7e778b4a2192
- Target Type = Device
- Unique Identifier = 46CC52C5CBD5EC19732D39D49BA7E778B4A2192

3. Performs a **File Signature Analysis of the content of the backup folders**;

4. **Options: Extract domain and backup filename to columns**
   Selecting this option decodes the forty character SHA1 hashed file name and makes information available as separate columns in Forensic Explorer List views, as per Figure 408 below. Adding these names to Forensic Explorer can greatly assist the investigator navigate through backup folders and identify relevant files. An example is shown in Figure 408 below:

**Figure 408, File list of an ITunes Backup with Backup Domain and Backup Name columns added**

a. **Extract Manifest MAC date/times to columns**
   The Manifest.mbdb file contains Created, Modified and Accessed (MAC) date/time stamps in UNIX time format. Selecting this option makes this MAC data available in columns.
30.1.13 STEP 2 - ITUNES BACKUP ANALYZE

The second step in Forensic Explorer is to analyze the contents of the located UDID folders to identify files of interest.

To Analyze and bookmark the content of an iTunes backup folder:

- In the File System module, under the Analysis Programs button, select iTunes Backups – Analyze, as shown in Figure 404 above. This runs a script with the following options:

![Image of Analyze iTunes Backups]

Each of the options in this window runs an individual script located in the Scripts module: Scripts\Files System\iTunes Backup folder. The purpose of these scripts is to bookmark files of interest for easy access by the investigator. A typical output from running these scripts is shown in Figure 410 below:
The bookmark folders are described in more detail at Appendix 9 – iTunes Backup Files, page 499.

### 30.1.14 STEP 3 – EXAMINING ITUNES BACKUP FILE CONTENT

An investigator will usually seek to extract call logs, SMS/MMS/Message history, application data, photos, email, device settings and other such data from individual iOS device applications. This data is often held in one of the following file types:

- SQLite
- Binary Plist
- MBDB
- DAT
- Media files, such as JPG, PNG, TIF, MOV etc.

### 3RD PARTY TOOLS

Historically investigators have exported iOS backup files to examine their content with third party applications, such as:

- [http://sqlitebrowser.org/](http://sqlitebrowser.org/)

Files can be extracted from Forensic Explorer using the right click Extract Files menu option and exporting files to disk. Individual files can also be written to a logical L01 evidence file to be read by other forensic applications.

### FORENSIC EXPLORER DATA VIEWS

Individual iOS device backup files can be examined using Forensic Explorer data views. The following table summarizes the best data views for each file type:
### 30.1.15 Working with Encrypted Backups

iTunes provides the option to encrypt backups (as shown in Figure 397 above). During the backup process the user is prompted to enter a password to encrypt all files in the backup.

This password is stored within the backup itself to enable access to the backup if the physical device is not present. For more information on password storage see Forensic analysis of iPhone Backups, Decrypting Encrypted backups, reference Satish, B. (21) and (22).

### 30.1.16 Identifying Encrypted iTunes Backups

To identify an Encrypted iTunes backup:

1. Run a Signature Analysis on the iTunes backup folders. An encrypted backup will show backup files with no valid file signature; or,

2. Run the **iTunes Backup Analyze** as described 30.1.13 above and select the **Encryption Check** (launching the script `Scripts\File System\iTunes Backup\iTunes Backup Encryption Check.pas`). When an encrypted backup is located it will add a warning folder to the Bookmarks module, as shown Figure 413 below:

---

**Figure 411, Examine iOS backup files with Forensic Explorer data views**

<table>
<thead>
<tr>
<th>File Type</th>
<th>Best Forensic Explorer Data View</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQLite or DB</td>
<td>Display view (shows SQL tables and data rows)</td>
</tr>
<tr>
<td>Binary PList</td>
<td>File Metadata view (decoded Plist) or Display view (XML format)</td>
</tr>
<tr>
<td>MBDB</td>
<td>HEX or Text view</td>
</tr>
<tr>
<td>DAT</td>
<td>HEX or Text view</td>
</tr>
<tr>
<td>JPG, PNG, TIF, MOV etc.</td>
<td>Display view</td>
</tr>
</tbody>
</table>

---

**Figure 412, iTunes encrypted backup password request**

![Set Password]

Enter a password to protect your iPhone backup.

Password: [ ]

Verify Password: [ ]

[Set Password]  [Cancel]

---

**Figure 413, Bookmarks module, possible encrypted backup**

![Bookmarks module, possible encrypted backup]
3. Or, by executing a Live Boot of the suspect’s computer (see Live Boot section 30.1.18 below) and running third party application, e.g. Tenorshare’s iPhone Backup Unlocker (23), to locate encrypted backups.

Figure 414, Encrypted iTunes backup identified by Tenorshare iPhone Backup Unlocker

30.1.17 DECRYPTING AN ITUNES BACKUP

As the password is stored within the iTunes backup, it is susceptible to a password attack by brute-force, or dictionary methods. There are several commercial tools available to decrypt then export files, including:

- Tenorshare’s iPhone Backup Unlocker (6), http://www.tenorshare.com/products/iphone-backup-unlocker.html (password breaking and decryption);
- IPhone Backup Extractor Pro, http://www.iphonebackupextractor.com (24) (used to extract files once password is known).

iTunes backup password breaking and decryption can be:

- Run directly on the suspects computer during a Live Boot session (see Live Boot section 30.1.18 below); or,
- Run on encrypted files exported from the case to the forensic workstation (recommended for faster processing speed).

If a complex password is suspected, it can be beneficial to use Forensic Explorer to create a customized dictionary file using keywords located on the suspect’s computer. This is done in the Index Search module by indexing the device (or part thereof) and exporting the list using the Export Words button.

RE-IMPORTING DECRYPTED BACKUP FILES TO FORENSIC EXPLORER

To add decrypted iTunes backup files to a Forensic Explorer case:

1. Ensure that the path to the backup files contains \MobileSync\Backup\ (required for some Forensic Explorer scripts);
2. Preview the device on which the backup files are located;
3. Check and export the backup files to a L01 file.

Add the L01 file as evidence to the required case.
30.1.18 LIVE BOOT

Forensic Explorer Live Boot enables an investigator to boot a forensic image or write-protected physical hard drive. The investigator can then operate the suspect’s computer in a forensically sound virtual environment.

In iOS device investigations, this gives the investigator the ability to launch iTunes on the suspect’s computer and confirm settings such as:

1. iTunes account names and passwords;
   
   **Figure 415, iTunes account information in a Live Boot session**

   ![iTunes account information](image)

2. Applications, including version number information, in the iTunes library:
   
   **Figure 416, iTunes Library in a Live Boot session**

   ![iTunes Library](image)

30.1.19 SHADOW COPY

Consideration should be given to Shadow copies (Windows Restore Points) present on the suspect’s computer. These Shadow copies may hold historical iTunes backup folders and provide additional information not present in the existing file system.

To identify Shadow copy files, in the File System module, click the **Shadow Copy** button:
Existing Shadow copies will then be displayed in the Shadow Copy options window:

Select and add the Shadow copy to the case (For more information about shadow copies see the Shadow Copy section in the Forensic Explorer user manual). Apply the procedures described in this document to examine the iTunes backup files within the mounted Shadow copy files.
30.2 THUMBNAIDS

30.2.1 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 in the same folder in which the pictures represented by the thumbnails reside.

From Windows Vista, onward, Thumbs.db were largely replaced by Thumbscache (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.

30.2.2 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 per their maximum pixel size, that is:

- thumbcache_32.db
- thumbcache_96.db
- thumbcache_256.db
- thumbcache_1024.db

30.2.3 FORENSIC VALUE OF THUMBNAIDS

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”. (25)

Further suggested references include:


30.2.4 THUMBNAIL IN FORENSIC EXPLORER

For 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 418 below:

**Figure 418, Thumbs.db Display view**

---

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_***db***. A Thumbs.db Folders filter as shown in Figure 419 below:

---

**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_***db***. A Thumbs.db Folders filter as shown in Figure 419 below:
The filter code is accessible in the Scripts Module, in the path:

- Filters\FileSystem\Thumbs.pas
- Filters\FileSystem\Thumbcache.pas

**EXPANDING COMPOUND THUMBNAIL-FILES**

Thumbnail-Files are **Compound** files because they act as containers for content.

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 THUMBNAIL-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 420 below:
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 Programs 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.
30.3 JUMP LISTS

Jump Lists were introduced in Windows 7 to give users quick access to recently accessed application files and actions. Jump Lists appear in both the Windows Start menu and the Windows Task Bar, as shown in Figure 421 and Figure 422 below:

Figure 421, Start Menu, MS Word Automatic Destinations Jump List (Windows 8 shown)

Figure 422, Task bar, MS Word, Automatic Destinations Jump List (Windows 8 shown)

There are two types of Jump Lists:

- **Automatic** (autodest, or *.automaticDestinations-ms) files, created by the Windows Operating System. These files are in the path:

  \[C:\User\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\\[AppID\].automaticDestinations-ms\]

- Custom (custdest, or *.customDestinations-ms) files, created by software applications. The files are in the path:

  \[C:\User\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\[AppID\].customDestinations-ms\]
A list of Jump List AppID's are located on the Forensics Wiki:
http://www.forensicswiki.org/wiki/List_of_Jump_List_IDs

30.3.1 FORENSIC VALUE OF JUMP LISTS

Jump Lists are becoming increasingly prevalent as software vendors increasingly use them in preference to the Windows Registry to store MRU (Most Recently Used) or MFU (Most Frequently Used) lists.

From a forensic examiner’s perspective, Jump Lists can indicate recently used resources, including files, applications and web sites. They can be a reliable indication of a user’s recent behavior.

30.3.2 AUTOMATICDESTINATIONS JUMP LISTS IN FORENSIC EXPLORER

Automaticdestinations Jump List files are in a compressed OLE file format within which are LNK files that hold metadata relevant to the investigator.

AUTOMATED EXTRACTION OF AUTOMATICDESTINATIONS JUMP LIST METADATA

To automatically extract automaticdestinations Jump List metadata:

In the File System module click the Extract Metadata button and run;

- Extract MS Jump List script; or,
- Bookmark MS Jump List LNK.

Metadata from the embedded LNK files is extracted and put into File System module columns. The columns include:

- LNK Target Accessed (UTC)
- LNK Target Drive Type
- LNK Target Local Base Path
- LNK Target Volume Serial

When the Bookmark MS Jump List LNK option is used, relevant LNK metadata is bookmarked by file name, as shown in Figure 423 below:

Figure 423, Bookmarked automaticdestinations Jump List Files
Metadata LNK columns can also be added to the Bookmarks module.

### OLE Compound File Format

**Automaticdestinations** files are in a compound OLE (Object Linking and Embedding) format. To access the content of an automaticdestinations the OLE structure must first be decompressed. This is done in the File System module by:

- Selecting a file, then right-click and select the **Expand Compound File** menu option; or
- Run the **Expand Compound Files.pas** script from the File System module toolbar button or the **Analysis Programs > Expand Compound Files** menu item.

For more information about expanding compound files See 9.5.

**LNK Format**

Once the OLE file is decompressed its internal data streams are exposed. These are very like Windows LNK files and running a Signature Analysis on the files will identify them as such.

To examine the metadata of a file, click on the LNK file and look at the **File System > File Metadata View** to see the embedded metadata fields. These are the fields that are extracted to columns in the automated process.
Chapter 31 - Legal

In This Chapter

<table>
<thead>
<tr>
<th>CHAPTER 31 - LEGAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>31.1  This User Guide ................................................................. 462</td>
</tr>
<tr>
<td>31.2  Copyright .......................................................... 462</td>
</tr>
<tr>
<td>31.3  License agreement ......................................................... 462</td>
</tr>
<tr>
<td>31.4  License agreement Disclaimer ............................................... 464</td>
</tr>
</tbody>
</table>
31.1 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.

31.2 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 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®.

Other company products include:

- Cisco ClamAV® (https://www.clamav.net/).

31.3 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 always 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. If 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


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.
31.4 LICENSE AGREEMENT DISCLAIMER

The software available for downloading 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.

31.4.1 SUPPORT

Documentation:  http://www.forensicexplorer.com/support

Video Tutorials:  http://www.forensicexplorer.com/video

Email Support:  support@getdata.com

Phone Support:

USA:  +1.844.300.0552

x801 - Sales

x802 - Support

x804 - Training (866)

Or;

Sydney, Australia:  +61 (0)2 8208 6053

Hours:  Australian Eastern Standard Time, 9am - 5:30pm Mon - Fri

31.4.2 SECURE POST

GetData Forensics Pty Ltd

P.O. Box 71
Engadine, New South Wales, 2233
Australia

31.4.3 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

The following file types are supported by Forensic Explorers inbuilt file carving component. Refer to Chapter 24 - Data Recovery, for more information:

- Microsoft Office
  - Access Database (.mdb)
  - Microsoft Excel Worksheet (.xls, .xlsx)
  - Microsoft PowerPoint Presentation (.ppt)
  - Microsoft Word Document (.doc, .docx)
  - Open Office Document (.odt)
  - Open Office Spreadsheet (.ods)
  - Outlook Email file (.pst, .pob)
- Camera
  - Canon Raw graphics file (.crw)
  - JPEG Digital Camera file (.jpg, jpeg)
  - Olympus RAW file (.orf)
  - TIFF Graphics file (.tif, .tiff, .tiff, .nef, .arn)
- Music
  - iTunes audio file (.m4a, .m4b, .mp4)
  - MP3 Music file (.mp3, .mp1, .mp2)
  - Musical Instrument Digital Interface file (.mid, .mid)
  - WAVE Multimedia file (.wav)
- Video
  - ASF, WMA, WMV Multimedia file (.asf, .wma, .asx)
  - AVCHD Multimedia file (.mts, .m2ts, .h264)
  - AVI Multimedia file (.avi)
  - MOV Multimedia file (Quicktime) (.mov, .mp4)
  - MPEG Multimedia file (.mpg, .mpeg, .m1v, .vro)
- Internet
  - HTML Documents (.htm, .html, .shtml, .html, .php, .php5, .asp)
  - Internet Explorer URL Cache Index Dat (.dat)
  - Internet Favorites (.url)
  - ShockWave Flash (.swf)
- Graphics
  - 3d Studio Max (.max)
  - Adobe InDesign file (.indd)
  - Adobe Photoshop (.psd)
  - AutoCAD Drawing file (.dwg)
  - AutoCad DX File (.dxf)
  - AutoCad DX File (.hpg, .hp, .hpg, .plt)
  - AutoSketch (.skf)
  - Bentley MicroStation v7 Drawing (.dgn)
  - Bentley MicroStation v8 Drawing (.dgn)
## APPENDIX 4 - SUMMARY OF DATE AND TIME

<table>
<thead>
<tr>
<th>File System Type</th>
<th>FAT</th>
<th>NTFS</th>
<th>exFAT</th>
<th>HFS</th>
<th>HFS+</th>
<th>EXT2/3/4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Type</td>
<td>Local</td>
<td>UTC</td>
<td>Local</td>
<td>Local</td>
<td>UTC</td>
<td>UTC</td>
</tr>
<tr>
<td>Calculation Method</td>
<td>DOS Date &amp; Time.</td>
<td>100ns since 1st Jan 1601.</td>
<td>DOS date &amp; time.</td>
<td>Seconds since midnight 1st Jan 1904.</td>
<td>Seconds since midnight 1st Jan 1904.</td>
<td>Seconds since 1st Jan 1970.</td>
</tr>
<tr>
<td>Modified</td>
<td>Written Time (2 bytes); Written Date (2 bytes); Total=4 bytes.</td>
<td>Written Time; Written Date; Total=8 bytes.</td>
<td>Created Time (2 bytes); Created Date (2 bytes); Created msecs (1 byte); Total=5 bytes.</td>
<td>Content Modified Date &amp; Time. The date and time the file's contents were last changed by extending, truncating, or writing either of the forks. Total=4 bytes.</td>
<td>Content Modified Date &amp; Time. The date and time the file's contents were last changed by extending, truncating, or writing either of the forks. Total=4 bytes.</td>
<td>Last Date &amp; Time that the content was modified. Total=4 bytes.</td>
</tr>
<tr>
<td>Accessed</td>
<td>Accessed Date; Total=2 bytes.</td>
<td>Accessed Time; Accessed Date; Total=8 bytes.</td>
<td>Accessed Time (2 bytes); Accessed Date (2 bytes); Total=4 bytes.</td>
<td>N/A</td>
<td>Last accessed Date &amp; Time. The date and time the file's content was last read. Total=4 bytes.</td>
<td>Access Date &amp; Time. Total=4 bytes.</td>
</tr>
<tr>
<td>Created</td>
<td>Created Time (2 bytes); Created Date (2 bytes); Created msecs (1 byte); Total=5 bytes</td>
<td>Created Time; Accessed Date; Total=8 bytes.</td>
<td>Created Time (2 bytes); Created Date (2 bytes); Created msecs (1 byte); Total=5 bytes.</td>
<td>Created Date &amp; Time. Total=4 bytes.</td>
<td>Created Date &amp; Time. Total=4 bytes.</td>
<td>N/A</td>
</tr>
<tr>
<td>Modified Record</td>
<td>N/A</td>
<td>Modified Time; Modified Date; Total=8 bytes.</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>The last date and time that any field in the file's catalogue record was changed. Total=4 bytes.</td>
</tr>
</tbody>
</table>
Appendix 5 - References

APPENDIX 5 - REFERENCES


23. Tenorshare. iPhone Backup Unlocker. [Online] [Cited: July 26, 2015.]


### 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 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/](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 (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 106.

### Carved (file)

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.

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>| <strong>Case File</strong> | 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. 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. |
| <strong>ClamAV (Clam AntiVirus)</strong> | ClamAV® is an open source (GPL) anti-virus engine. It is free software and can be redistributed and/or modified under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version. GetData Pty Ltd have modified parts of the ClamAV engine to allow Forensic Explorer to scan evidence files. Those modifications, including the source code, are available upon written request to GetData at <a href="mailto:support@getdata.com">support@getdata.com</a>. ClamAV and Clam AntiVirus are trademarks of Cisco Systems, Inc. 2017. |
| <strong>Clear Columns</strong> | In Forensic Explorer additional data can be calculated (e.g. Entropy, MD5 Hash, etc.) or given (e.g. Classification, Flag, Signature, etc.) to an entry. This information is usually displayed in columns in a File List view. In some circumstances it may be beneficial to clear all information from these columns and re-apply the process. To do this, in the File System module, select Tools &gt; Clear Column Content. |
| <strong>Cluster</strong> | 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. |
| <strong>Cluster Boundaries</strong> | 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. 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. |
| <strong>Codepage</strong> | Codepage is another term for character encoding. It consists of a table of values that describes the character set for a language. When a keyword search is conducted in Forensic Explorer, the correct codepage should be selected. |
| <strong>Computer forensics</strong> | 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>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compound File</td>
<td>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.</td>
</tr>
<tr>
<td>Data carve</td>
<td>See file carve.</td>
</tr>
<tr>
<td>Data View</td>
<td>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.</td>
</tr>
<tr>
<td>Deleted File</td>
<td>A deleted file is one which has been marked as deleted by the file system (usually because 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. If 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. 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.</td>
</tr>
<tr>
<td>Delphi Basics©</td>
<td>Delphi Basics© is a documentation package for the Delphi programming language (see <a href="http://www.delphibasics.co.uk/">http://www.delphibasics.co.uk/</a>). 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.</td>
</tr>
<tr>
<td>Device</td>
<td>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.</td>
</tr>
<tr>
<td>Directory</td>
<td>See Root Directory</td>
</tr>
<tr>
<td>Directory Entry (FAT)</td>
<td>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.</td>
</tr>
<tr>
<td>Disk Slack</td>
<td>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.</td>
</tr>
<tr>
<td>Disk view (Forensic Explorer)</td>
<td>A graphical representation in Forensic Explorer of sectors on the examined device. Disk view can be used to:</td>
</tr>
<tr>
<td></td>
<td>• Examine the content of the data in a specific sector/s;</td>
</tr>
</tbody>
</table>
- 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**
Daylight Savings Time

**dtSearch®**
dtSearch® ([www.dtsearch.com](http://www.dtsearch.com)) is third party index search software built into Forensic Explorer and accessed via the Index Search module tab (see Chapter 14 - Index Search Module, for more information).

**Entropy**
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.

**E01**
A forensic file format used to create disk image files. Developed by Guidance Software ([http://www.guidancesoftware.com/](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**
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).

For more information see: [http://www.forensicswiki.org/wiki/FAT](http://www.forensicswiki.org/wiki/FAT)

**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**
File carving is the process of searching for files based on a known content, rather than relying of file system metadata. This usually involves searching for a known header and footer of a specific file type.

Forensic Explorer has built in code to data carve for more than 300 file types.

**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 that 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 106.

**Flag**
In Forensic Explorer, a flag is used to mark a file as relevant. It is a colored 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 and 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.

**Folder**
See Root Directory

**Forensic Image**
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.

Using non-invasive procedures, forensic software is used to create the image file. The image contains all data, including deleted and system files, ad is an exact copy of the original.

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.

**Forensic Integrity**
In computer forensic 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 using 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 later.)

**Fragmented File**
The distribution of a file on a disk so that it's written in non-contiguous clusters.
Free Space
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.

**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.

**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.

GeoTag (Geotagging)
Geotagging is the process of adding geographical identification metadata to files, usually photographs or videos. This data is usually latitude and longitude co-ordinates.

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
“A hard link is the file system representation of a file by which more than one path references a single file in the same volume” Microsoft (26).

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
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.

Hash Sets are often grouped in the forensic community into two groups:

**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.

Hash sets can be created in Forensic Explorer, or downloaded from a trusted source.

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**
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.

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.

**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**
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).

A keyword can be an actual word, but can also be raw data.

Complex keywords are usually created using RegEx expressions.

**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. (27)

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)
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.

Common Logical Evidence File formats are L01, created by EnCase* forensic software (www.guidancesoftware.com) or AD1 by Access Data’s 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 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)
“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”. (28)
Metadata: Metadata is often referred to as “data about data”. Windows metadata can include a file 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 (tab) at the bottom window of Forensic Explorer is used to show all metadata properties for a file.

Metadata from the File Metadata view can be extracted and placed in columns using the Extract Metadata button in the File System module toolbar. See 8.12.1 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 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: 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 affect multi-core speed.

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.

<table>
<thead>
<tr>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ophcrack</td>
<td>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.</td>
</tr>
<tr>
<td>Pane</td>
<td>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 as a Hex view, Text view, Disk view, Console etc.</td>
</tr>
<tr>
<td>Pascal</td>
<td>A programming language used to create scripts in Forensic Explorer. See Module Chapter 19 - Scripts Module.</td>
</tr>
<tr>
<td>Partition</td>
<td>A part of a hard disk that can have an independent file system.</td>
</tr>
<tr>
<td>PCRE (Perl Compatible Regular Expression)</td>
<td>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.</td>
</tr>
<tr>
<td>Pre-processing (a case)</td>
<td>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. Pre-processing options are set in Forensic Explorer when a device or forensic image file is added. See 10.5 for more information.</td>
</tr>
<tr>
<td>Priority</td>
<td>In Forensic Explorer priority refers to the use of threaded multi-core processing. See “Multi-Core Processing”.</td>
</tr>
<tr>
<td>Preview (Evidence Module)</td>
<td>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.</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Independent Disks.</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory, where programs are loaded and computer code is executed. The content of RAM is lost when the computer is turned off.</td>
</tr>
<tr>
<td>RAM Slack</td>
<td>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</td>
</tr>
</tbody>
</table>
could contain data from RAM unrelated to the content of the file. In more recent Operating Systems, RAM slack is filled with zeroes.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record View (Forensic Explorer)</td>
<td>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.</td>
</tr>
<tr>
<td>Recover My Files</td>
<td>Data Recovery Software authored and sold by GetData at <a href="http://www.recovermyfiles.com">www.recovermyfiles.com</a></td>
</tr>
<tr>
<td>Regex (Regular Expression)</td>
<td>A regular expression provides a concise and flexible means to &quot;match&quot; (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” (<a href="http://en.wikipedia.org/wiki/Regex">http://en.wikipedia.org/wiki/Regex</a>).</td>
</tr>
<tr>
<td>Registry</td>
<td>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.</td>
</tr>
<tr>
<td>Ribbon (Toolbar)</td>
<td>The ribbon refers to the Forensic Explorer toolbar and the top of each module. The contents of the toolbar are controlled by scripts.</td>
</tr>
<tr>
<td>Root Directory/Folder</td>
<td>A directory is a container used to organize folders and files into a 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. 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. “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”.</td>
</tr>
<tr>
<td>Script</td>
<td>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.</td>
</tr>
<tr>
<td>Sector</td>
<td>A sector is a specifically sized unit or 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).</td>
</tr>
</tbody>
</table>
### SFN (see also LFN)

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.

### Signature Analysis

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.

### Shadow Copy

“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](https://en.wikipedia.org/wiki/Shadow_Copy).

Forensic Explorer enables investigators to add and examine the content of Shadow Copies. See Chapter 26.

### Skin Tone Analysis

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.

### Slack

See File Slack, Disk Slack, FAT Slack

### Steganography

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity [http://en.wikipedia.org/wiki/Steganography](http://en.wikipedia.org/wiki/Steganography).

### 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

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.

**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.
| **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 30.1 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.

```
program Help_File_Sample_Script_1;

uses
  GUI,  SysUtils;

const
  starting_age = 10;

var
  my_age: integer;

begin
  my_age := starting_age;
  ShowMessage('Your current age is: ' + inttostr(starting_age));
  Progress.Log('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!');
      Progress.Log('Congratulations. You made it from ' + inttostr(starting_age) + ' to: ' + inttostr(my_age));
      end
    else begin
      ShowMessage('Next year you will be: ' + inttostr(my_age));
      Progress.Log('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:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📁</td>
<td>Case</td>
<td>A Forensic Explorer case</td>
</tr>
<tr>
<td>📏</td>
<td>Shadow Copy</td>
<td>A mounted shadow copy volume</td>
</tr>
<tr>
<td>📀</td>
<td>Compound file</td>
<td>A folder holding the contents of an expanded compound file</td>
</tr>
<tr>
<td>📄</td>
<td>Date</td>
<td>Categorize dates - File System &gt; Folders view &gt; Category view</td>
</tr>
<tr>
<td>📆</td>
<td>Device</td>
<td>A physical device, e.g. a hard drive</td>
</tr>
<tr>
<td>📆</td>
<td>Device</td>
<td>A logical device, e.g. C: drive.</td>
</tr>
<tr>
<td>📄</td>
<td>File</td>
<td>A deleted file</td>
</tr>
<tr>
<td>📄</td>
<td>File</td>
<td>A FAT “dot” directory entry</td>
</tr>
<tr>
<td>📄</td>
<td>File</td>
<td>A FAT “double dot” directory entry</td>
</tr>
<tr>
<td>📄</td>
<td>File</td>
<td>A system file</td>
</tr>
<tr>
<td>📄</td>
<td>File</td>
<td>An active file</td>
</tr>
<tr>
<td>📄</td>
<td>File</td>
<td>An alternate data stream</td>
</tr>
<tr>
<td>📂</td>
<td>Folder</td>
<td>A folder holding the results of a Forensic Explorer file carve</td>
</tr>
<tr>
<td>📂</td>
<td>Folder</td>
<td>A deleted folder</td>
</tr>
<tr>
<td>🗑️</td>
<td>Deleted items</td>
<td>Categorize deleted items - File System &gt; Folders view &gt; Category view</td>
</tr>
<tr>
<td>📂</td>
<td>Folder</td>
<td>An active folder</td>
</tr>
<tr>
<td>🏛️</td>
<td>Free space</td>
<td>Free space in partition</td>
</tr>
<tr>
<td>📀</td>
<td>Image</td>
<td>A forensic image file</td>
</tr>
<tr>
<td>📀</td>
<td>Image folder</td>
<td>Select an image from a folder</td>
</tr>
<tr>
<td>🏛️</td>
<td>Navigation</td>
<td>An expandable branch (folder structure)</td>
</tr>
<tr>
<td>🏛️</td>
<td>Navigation</td>
<td>Active branch plate</td>
</tr>
</tbody>
</table>
## Icons in Forensic Explorer

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Inactive branch plate" /></td>
<td>Inactive branch plate</td>
</tr>
<tr>
<td><img src="image" alt="Partition" /></td>
<td>A partition</td>
</tr>
<tr>
<td><img src="image" alt="Partition" /></td>
<td>An active partition</td>
</tr>
<tr>
<td><img src="image" alt="Unallocated" /></td>
<td>Unallocated clusters</td>
</tr>
</tbody>
</table>

**Disk View**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="The start sector of a file" /></td>
<td>The start sector of a file</td>
</tr>
<tr>
<td><img src="image" alt="Currently selected sector" /></td>
<td>Currently selected sector</td>
</tr>
<tr>
<td><img src="image" alt="One type overlays another" /></td>
<td>One type overlays another</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="MBR/VBR" /></td>
<td>MBR/VBR (Red)</td>
</tr>
<tr>
<td><img src="image" alt="FAT 1" /></td>
<td>FAT 1 (Dark Violet)</td>
</tr>
<tr>
<td><img src="image" alt="FAT 2" /></td>
<td>FAT 2 (Web Violet)</td>
</tr>
<tr>
<td><img src="image" alt="$MFT" /></td>
<td>$MFT (Dark Violet)</td>
</tr>
<tr>
<td><img src="image" alt="System files" /></td>
<td>System files (Web Tomato)</td>
</tr>
<tr>
<td><img src="image" alt="File overlays the $MFT" /></td>
<td>$MFT resident file (the file overlays the $MFT)</td>
</tr>
<tr>
<td><img src="image" alt="Folder" /></td>
<td>Folder (Deep Sky Blue)</td>
</tr>
<tr>
<td><img src="image" alt="Allocated File" /></td>
<td>Allocated File (Corn Flower Blue)</td>
</tr>
<tr>
<td><img src="image" alt="Unallocated space" /></td>
<td>Unallocated space (Lt Gray)</td>
</tr>
<tr>
<td><img src="image" alt="Deleted file" /></td>
<td>Deleted file (A deleted file overlays unallocated space)</td>
</tr>
<tr>
<td><img src="image" alt="Carved file" /></td>
<td>Carved file (Dark Orange: Carved file overlays unallocated space)</td>
</tr>
</tbody>
</table>

Icons in Forensic Explorer include those supplied by:

- Silk Icons: [http://www.famfamfam.com/lab/icons/silk/](http://www.famfamfam.com/lab/icons/silk/); and
- [http://www.softicons.com](http://www.softicons.com)
## Appendix 9 – iTunes Backup Files

The following table lists iTunes backup files that may be of interest to the forensic investigator:

<table>
<thead>
<tr>
<th>Contents</th>
<th>Domain</th>
<th>iOS Path and file name</th>
<th>SHA-1 backup file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calendar</td>
<td>HomeDomain</td>
<td>Library/Calendar/Calendar.sqlitedb</td>
<td>2041457d5fe04d39d0b481178355df6781e6858</td>
</tr>
<tr>
<td>Call History</td>
<td>WirelessDomain</td>
<td>Library/CallHistory/call_history.db</td>
<td>2b2b0084a1bc3a5ac8c27afdf14af642c61a19ca</td>
</tr>
<tr>
<td>Chat – KikChat</td>
<td>AppDomain-com.kik.chat</td>
<td>Documents/kik.sqlite</td>
<td>8e281be6657d4523710d96341b6f86ba89b56df7</td>
</tr>
<tr>
<td>Chat – Line</td>
<td>AppDomain-jp.naver.line</td>
<td>Documents/talk.sqlite</td>
<td>53a7099b474f4fbb3f2cd00f8e59578d58fb44a</td>
</tr>
<tr>
<td>Chat – MessageMe</td>
<td>AppDomain-com.littleinc.MessageMe</td>
<td>Library/Application Support/MessageMe/MessageMe.sqlite</td>
<td>8c625842c0b74efff30d92e3e4e4a1d3a2e8e</td>
</tr>
<tr>
<td>Chat – Skype</td>
<td>AppDomain-com.skype.skype</td>
<td>Library/Application Support/Skype/[user]/main.db</td>
<td></td>
</tr>
<tr>
<td>Chat – Touch</td>
<td>AppDomain-com.enflick.ping</td>
<td>Documents/Touch.sqlite</td>
<td>b18a30bf72824a7d024a95178ae42d8339f83633</td>
</tr>
<tr>
<td>Chat – Viber</td>
<td>AppDomain-com.viber</td>
<td>Documents/Contacts.data</td>
<td>b39bac0d347adfa17527f97c3af3df726a3a</td>
</tr>
<tr>
<td>Chat – WeChat</td>
<td>AppDomain-com.tencent.xin</td>
<td>Documents/[chat-UDID]/DB/MM.sqlite</td>
<td></td>
</tr>
<tr>
<td>Chat - WhatsApp</td>
<td>AppDomain-net.whatsapp.WhatsApp</td>
<td>AppDomain-net.whatsapp.WhatsApp</td>
<td>1b6b187a1b60b9ae8b720c79e2c67f472bab09c0</td>
</tr>
<tr>
<td>Contacts</td>
<td>HomeDomain</td>
<td>Library/AddressBook/AddressBook.sqlitedb</td>
<td>31bb78a9147664ba406dbf6113c8b614be442</td>
</tr>
<tr>
<td>Keyboard</td>
<td>HomeDomain</td>
<td>Library/Keyboard/dynamic-text.dat</td>
<td>Changes with language installed</td>
</tr>
<tr>
<td>Locations</td>
<td>RootDomain</td>
<td>Library/Caches/locationd/consolidated.db</td>
<td>4096c9ec676f2847dc28345900e284a7c815836*</td>
</tr>
<tr>
<td>Maps History</td>
<td>HomeDomain</td>
<td>Library/Maps/History.plist</td>
<td>b60c382887dfa562166f099f24797e55c12a94e4</td>
</tr>
<tr>
<td>Notes</td>
<td>HomeDomain</td>
<td>Library/Notes/notes.sqlite</td>
<td>ca3bc056d4da0bbf8bb5fbb3e254f3b7147e639c</td>
</tr>
<tr>
<td>Safari History</td>
<td>HomeDomain</td>
<td>Library/Safari/History.plist</td>
<td>1d6740792a2b845f4c1e6220c4390de7f0afe8ab</td>
</tr>
<tr>
<td>SMS</td>
<td>HomeDomain</td>
<td>Library/SMS/sms.db</td>
<td>3d0d7e5fb2ce288813306e4d4636395e47a3d28</td>
</tr>
<tr>
<td>Wifi Networks</td>
<td>SystemPreferencesDomain</td>
<td>SystemConfiguration/com.apple.wifi.plist</td>
<td>ade0340f576ee14793c607073bd7e8e409af07a8</td>
</tr>
</tbody>
</table>

* Removed from iOS backup (not the device) after iPhone 4
The following table summarizes the results of running the **File System > Analysis Scripts > iTunes Backup > Analyze** scripts:

<table>
<thead>
<tr>
<th>Bookmark Folder</th>
<th>Bookmarked File/s</th>
<th>Description</th>
<th>Best FEX Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Book</td>
<td>AddressBook.sqlite (SQLite) 31bb7ba8914766d4ba0d6d6b6113c8b614be442</td>
<td>Contacts</td>
<td>Display; Phone module; External SQLite viewer.</td>
</tr>
<tr>
<td>Call History</td>
<td>call_history.db (SQLite) 2b2b0084a1bc3a5ac8c27afdf14af42c61a19ca</td>
<td>Last 100 calls.</td>
<td>Display; Phone module; External SQLite viewer.</td>
</tr>
<tr>
<td>Camera Roll</td>
<td>Photos and Movies</td>
<td>Files in the CameraRoll domain.</td>
<td>Display/Gallery</td>
</tr>
<tr>
<td>Domain - JPG</td>
<td>JPG files</td>
<td>JPG files are bookmarked according to the Apple Domain in which they reside. This is very useful for identifying applications that use JPG files (such as chat/messaging apps).</td>
<td>Display/Gallery</td>
</tr>
<tr>
<td>Domain - MOV</td>
<td>MOV files</td>
<td>MOV files are bookmarked according to the Apple Domain in which they reside. This is very useful for identifying applications that use MOV files (such as chat/messaging apps).</td>
<td>Display</td>
</tr>
<tr>
<td>Domain - PNG</td>
<td>PNG files</td>
<td>PNG files are bookmarked according to the Apple Domain in which they reside. This is very useful for identifying applications that use PNG files (such as chat/messaging apps).</td>
<td>Display/Gallery</td>
</tr>
<tr>
<td>Domain - SQLite</td>
<td>SQLite files</td>
<td>SQLite files are bookmarked according to the Apple Domain in which they reside. This is very useful for identifying applications installed on the iOS device that may be of value to the investigator.</td>
<td>Display; External SQLite viewer.</td>
</tr>
<tr>
<td>Keyboard</td>
<td>dynamic-text.dat 0b68edc697a550c9b977b77cd012fa9a0557dfcb</td>
<td>“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.” Morrissey, S. (29) page 150.</td>
<td>Text; Hex.</td>
</tr>
</tbody>
</table>
### Phone Chat Apps

<table>
<thead>
<tr>
<th>App</th>
<th>File Hashes</th>
<th>Description</th>
<th>Display; Phone Apps module; External SQLite viewer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kikchat</td>
<td>8e281be6657d4523710d96341b6f86ba89b56df7534a7099b474f4f3f2cd006f8e59578d58fb44a8c625842c0b749eff30d92eec4e4a1da30d2e8</td>
<td>SQLite files containing communication history from Phone/Chat applications.</td>
<td></td>
</tr>
<tr>
<td>Line</td>
<td>534a7099b474f4f3f2cd006f8e59578d58fb44a8c625842c0b749eff30d92eec4e4a1da30d2e8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MessageMe</td>
<td>N/A (changes with user account)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skype</td>
<td>b18a30bf72824a7d024a95178ae42d8339f83633b39bac0d347adfa172527f97c3a5fa3df726a3a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Touch</td>
<td>N/A (changes with user account)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Viber</td>
<td>1b6b187a1b60b9ae8b720c79e2c67f472bab09c0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WeChat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WhatsApp</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Maps History

<table>
<thead>
<tr>
<th>File</th>
<th>Hashes</th>
<th>Description</th>
<th>Display</th>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>History.plist</td>
<td>b60c382887dfa562166f099f24797e55c12a94e4</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Photo Streams Data

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Description</th>
<th>Display/Gallery</th>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photo Streams Data</td>
<td>Media files</td>
<td>Media streamed to the phone with Apple PhotoStream.</td>
<td></td>
</tr>
</tbody>
</table>

### Recordings

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Description</th>
<th>Display</th>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recordings</td>
<td>Recordings (and configuration files) located in the Media/Recordings/ domain.</td>
<td>Display</td>
<td></td>
</tr>
</tbody>
</table>

### Safari History

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Description</th>
<th>Display</th>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safari History</td>
<td>History.plist ed50eadf14505ef0b433e0c4a380526ad6656d3a</td>
<td>Folders are given page titles. Safari history contains browsing information. This includes the URL, page title, last visited date (converted from MAC absolute date UTC) and visit count.</td>
<td>Display</td>
</tr>
</tbody>
</table>

### SMS Attachments

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Description</th>
<th>Display/Gallery</th>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS Attachments</td>
<td>Media files</td>
<td>File attachments sent by SMS</td>
<td></td>
</tr>
</tbody>
</table>

### WARNING - Backup may be Encrypted -

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Description</th>
<th>N/A</th>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>WARNING</td>
<td>The backup may be encrypted (see 30.1.15 below).</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
| Wifi                 | com.apple.wifi.plist ade0340f576ee14793c607073bd7e8e409af07a8 | 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) | File Metadata |

Copyright GetData Forensics Pty Ltd 2010 - 2019, All rights reserved.
# Appendix 10 - Index

## APPENDIX 10 - INDEX

<table>
<thead>
<tr>
<th>Accessed</th>
<th>Cell phone. See Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date, 168</td>
<td>Checked</td>
</tr>
<tr>
<td>Activation</td>
<td>Count, 120</td>
</tr>
<tr>
<td>Dongle, 39</td>
<td>Items, 120</td>
</tr>
<tr>
<td>Evaluation version offline, 22</td>
<td>Clam</td>
</tr>
<tr>
<td>Evaluation version online, 20</td>
<td>Anti Virus, 170</td>
</tr>
<tr>
<td>AD1 to L01, 423</td>
<td></td>
</tr>
<tr>
<td>Add Partition, 87</td>
<td></td>
</tr>
<tr>
<td>Apple Backups, 437</td>
<td></td>
</tr>
<tr>
<td>Artifact</td>
<td></td>
</tr>
<tr>
<td>Selected, 120</td>
<td></td>
</tr>
<tr>
<td>Artifacts</td>
<td></td>
</tr>
<tr>
<td>Definition, 177</td>
<td></td>
</tr>
<tr>
<td>Module, 177</td>
<td></td>
</tr>
<tr>
<td>ASCII</td>
<td></td>
</tr>
<tr>
<td>Character distribution, 106</td>
<td></td>
</tr>
<tr>
<td>Attributes, 167</td>
<td></td>
</tr>
<tr>
<td>Auto Save, 160</td>
<td></td>
</tr>
<tr>
<td>Bitlocker Encryption, 289</td>
<td></td>
</tr>
<tr>
<td>Blur</td>
<td></td>
</tr>
<tr>
<td>Gallery view, 94</td>
<td></td>
</tr>
<tr>
<td>Bookmarks</td>
<td></td>
</tr>
<tr>
<td>Hotkey, 217</td>
<td></td>
</tr>
<tr>
<td>Module, 218</td>
<td></td>
</tr>
<tr>
<td>Bookmarks Module, 215</td>
<td></td>
</tr>
<tr>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>Index search, 201</td>
<td></td>
</tr>
<tr>
<td>BpB - Bypes per block, 116</td>
<td></td>
</tr>
<tr>
<td>BpS - Bytes per sector, 116</td>
<td></td>
</tr>
<tr>
<td>Branch plate, 79</td>
<td></td>
</tr>
<tr>
<td>Byte Plot, 106</td>
<td></td>
</tr>
<tr>
<td>Examples, 107</td>
<td></td>
</tr>
<tr>
<td>Carve</td>
<td></td>
</tr>
<tr>
<td>About file carving, 351</td>
<td></td>
</tr>
<tr>
<td>Cluster, Sector, Byte, 354</td>
<td></td>
</tr>
<tr>
<td>Disk view icon, 83, 498</td>
<td></td>
</tr>
<tr>
<td>Evidence Processor, 157</td>
<td></td>
</tr>
<tr>
<td>Hex Selection, 100</td>
<td></td>
</tr>
<tr>
<td>Case</td>
<td></td>
</tr>
<tr>
<td>Close, 162</td>
<td></td>
</tr>
<tr>
<td>New, 142</td>
<td></td>
</tr>
<tr>
<td>Open, 145</td>
<td></td>
</tr>
<tr>
<td>Recent, 146</td>
<td></td>
</tr>
<tr>
<td>Save, 160</td>
<td></td>
</tr>
<tr>
<td>Categories, 166</td>
<td></td>
</tr>
</tbody>
</table>

Copyright GetData Forensics Pty Ltd 2010 - 2019, All rights reserved.
Duplicates
- De-duplicate, 320
Email
- Module, 206
- Email Module, 205
Evidence
- Add, 147
Evidence Processor, 154
Explorer Tool, 137
Export
- Delimited rows, 127
- Files, 124
- to L01, 125
- Using a script, 125
Export Word List, 203
Extension, 167
Extract Metadata
- Evidence Processor, 157
File List view, 167
File Name, 167
File signature analysis, 334
File slack
- Definition, 485
- Index search, 198
File System module, 164
File tree
- File System workspace, 164
Filter
- COLUMN filter tool, 133
- File System module, 78
- Scripts, 79, 137, 273
Filtering, 132
Flags
- Apply, 131
- Clear, 132
Flat File Hash set, 324
Forensic Image Converter, 423
Fragmentation
- File (FAT), 341
Full Path, 167
Fuzzy. See Index Search
Fuzzy hash, 320
Gallery View, 90
GUID
- Preview, 140, 161
Hash
- Acquisition hash display, 157
- Flat File Hash Set, 324
- Forensic Imager Acquisition, 54
- Verify (Evidence Processor), 156
- Verify L01, 126
Hash set, 321
Hex view, 100
Hit Offset (Device), 194
Hit Offset (File), 191
Hit Offset (Partition), 192
Hits
- Keyword Result List, 190
Hotkey
- Bookmarking, 217
HPA, 49
Hyperlinks
- Reports, 231, 248, 256, 264
Index Search
- Creating an index, 197
- Module, 196
- Searching an index, 199
Info view, 103
Installation, 33
Investigators
- Add, Edit, Delete, 143
- Is Deleted, 168
- JBOD, 358
- Jump List, 458
- Keyboard Shortcuts
  - Disk View, 84
Keyword
- Add, 181
- Edit or Delete, 183
- Group, 184
- Import, 184
- Regular expression (RegEx), 182
Keyword Search, 180
- Results, 188
- Run, 186
L01
- Export, 125
- Verify, 126
License agreement, 462
List view, 81
Live Boot, 376, 423
- VMWare Workstation Shared Folders, 379
Logical Size, 168
MBR
- Search for known, 156
MD5, 310, See Hash
Metadata
- Extract to columns, 113
- View, 112
Mobile Phone. See Phone
Modified, 168
Module
- Bookmarks, 215
- Email, 205
Evidence, 139
File System, 163
Index Search, 195
Keyword Search, 179
Registry, 209
Reporting, 223
Scripts, 271
Network Server
UDP Network Server, 148
Offset
Keyword Search
File, Partition, Device, 191
Open
Case, 145
Ophcrack, 386
Orphans
NTFS, 349
Path
Case folders, 36
Program, 35
Registry keys, 36
Working, 35
PCUnlocker, 389, 400
Phone
Carve, 354
Phonic. See Index Search
Photo DNA, 319
PhotoDNA, 319
Physical size
Column, 168
Preview
Evidence, 140
Project VIC, 330
Purchase orders, 28
RAID, 358
Hardware, 359
Software, 359
Recover Folders
FAT, 345, 350
NTFS, 350
RegEx
Column filter, 135
Keyword Search, 182
Quick start guide, 135
Registry
Location of registry files, 210
Module, 210
Registry file
Add from File System module, 211
Add standalone, 211
Report
Hyperlinks, 231, 248, 256, 264
Save
Case, 160
Scripting
Data recovery, 355
Scripts
Introduction to scripting, 279
Open, Copy, Rename, Delete, 278
Send to Module, 128
Servelet. Network Server
SHA. See Hash
Shadow Copy, 367
Background, 362
Mount in Forensic Explorer, 367
Shared Folders
VMWare Workstation, 379
Signature Analysis
Evidence processor, 157
Similarity Hash, 314
Sort
Multi column, 129
Persistent, 130
Remove, 130
Single column, 129
Startup.pas
Installation folder, 36
Script, 275
Stemming. See Index Search
Technical support, 465
text view, 102
Thumbeache, 454
Thumbs.db, 454
Time Zone. See Date and Time
tree view, 78, 164
Triage Report, 227
un-blur
Gallery view, 94
Undocking, 61
Uninstall, 38
User Datagram Protocol (UDP), 148
UUID
Apple Backup, 438, 487
VCard
Investigator, 144
VCF
VCard Investigator Details, 144
Verification Hash
Verify Device Hash, 310
Video
Thumbnail viewing, 105
Virtual Box
Live Boot, 377
VMWare
Live Boot, 377
Volume Shadow Copy. See Shadow Copy
VSC or VSC. See Shadow Copy
Wildcards
Index search, 202
Word List, 203