



FORENSIC EXPLORER

User Manual

Published: 6-Apr-25 at 17:26:20



Chapter Contents

Published: 6-Apr-25 at 17:25:28

Quick Start Guide	11
Wibu CodeMeter Activation Dongle.....	11
System Requirements.....	11
Download.....	11
Installation.....	12
Forensic Explorer Module Overview.....	12
Live Boot.....	14
1.2 Introducing Forensic Explorer.....	16
1.3 Supported file formats.....	16
1.4 Supported file systems.....	16
1.5 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	25
3.1 Purchase.....	26
3.2 License maintenance.....	27
Chapter 4 - Installation	29
4.1 System requirements.....	31
4.2 Download.....	31
4.3 Installation.....	31
4.4 Uninstall Forensic Explorer.....	41
Chapter 5 - Dongle Activation	43
5.1 Dongle activation of the purchased version.....	44
5.2 GetData License Manager.....	47

5.3	Wibu CodeMeter Runtime for Windows User	49
5.4	Network Licensing	51
5.5	Applying maintenance updates to your Wibu dongle	55
Chapter 6 - Forensic Acquisition		57
6.1	Write block	58
6.2	GetData's Forensic Imager.....	59
Chapter 7 - Forensic Explorer Interface		69
7.1	Modules	70
7.2	Module data views	72
7.3	Customizing layouts.....	74
7.4	Task Processes List.....	75
7.5	Process Logging and Priority.....	76
7.6	Reference Library.....	77
Chapter 8 - Data Views.....		81
8.1	Data views summary.....	83
8.2	Tree view	86
8.3	List view	89
8.4	Disk view	89
8.5	Gallery view	97
8.6	Category Graph.....	108
8.7	Hex view	108
8.8	Text view.....	109
8.9	Info.....	110
8.10	Display view	110
8.11	Byte Plot and Character Distribution	113
8.12	Filesystem Record view	117
8.13	File Metadata.....	118
8.14	File Extent	126

8.15	Permissions.....	127
Chapter 9 - Working With Data		131
9.1	Working with data	133
9.2	Highlighted and checked items.....	133
9.3	Bookmarks (Add or Edit).....	137
9.4	Columns	137
9.5	Open and Open with.....	139
9.6	Expand compound file	140
9.7	Export.....	142
9.8	OCR (Optical Character Recognition).....	148
9.9	Send to Module	151
9.10	Sorting.....	151
9.11	Flags	154
9.12	Filtering data	155
9.13	Copy rows to clipboard.....	163
Chapter 10 - Evidence Module.....		165
10.1	Preview	167
10.2	New case.....	168
10.3	Open an existing case	171
10.4	Adding evidence	172
10.5	Evidence Processor	182
10.6	Adding additional evidence to a case	187
10.7	Saving a case.....	188
10.8	Closing a case.....	190
Chapter 11 - File System Module		192
11.1	File System module.....	193
11.2	Toolbar.....	193
11.3	Folders view	193

11.4	Categories view.....	196
11.5	File List view.....	197
11.6	Other data views.....	200
11.7	File System Toolbar.....	201
Chapter 12 – Artifacts Module		208
	Artifacts	209
12.1	Artifacts module	209
Chapter 13 - Keyword Search Module.....		213
13.1	Keyword search	214
13.2	Keyword management	216
13.3	Search results.....	222
13.4	Keyword result list	224
13.5	Keyword search data views	227
Chapter 14 - Index Search Module.....		229
14.1	Index search.....	230
14.2	Considerations prior to creating an index	231
14.3	Creating an index.....	231
14.4	Searching an index.....	235
14.5	Search results.....	237
14.6	Index Search Compound Files.....	238
14.7	Export Word List	238
14.8	Index Search Logging	239
Chapter 15 - Email Module.....		241
15.1	Email	242
15.2	Email module	242
15.3	Microsoft Outlook .PST email	242
15.4	Index Search the Email module	243
15.5	keyword Search the Email module	244

Chapter 16 - Registry Module	245
16.1 Registry module.....	246
16.2 Adding a REGISTRY FILE to the registry module	247
16.3 Registry Data Views	248
16.4 Deleted registry keys	250
16.5 Examining registry files using scripts	250
Chapter 17 - Bookmarks Module	253
17.1 Adding Bookmarks.....	254
17.2 Bookmarks Module.....	256
17.3 Identifying Bookmarked files other modules	259
Chapter 18 - Reports	261
18.1 MS Word - Quick Reports	263
18.2 The Reports Module	266
18.3 Reports Tree	268
18.4 Report Editor	275
18.5 Creating Reports	277
Chapter 19 - Scripts Module	309
19.1 Scripts Module.....	310
19.2 Managing scripts in the scripts window	317
19.3 Introduction to Scripting.....	318
19.4 Startup.Pas.....	321
Chapter 20 – Encryption	323
20.1 Encryption.....	324
20.2 Decrypting Supported Encryption Formats	326
20.3 Identifying Other Encrypted Files	330
20.4 Decrypted Password Protected Archives (Zip, 7Z).....	334
Chapter 21 - Date and Time	335
21.1 Date and time in computer forensics	336

21.2	FAT, HFS, CDFS file system date and time	336
21.3	NTFS, HFS+ file system date and time	336
21.4	Date and time information in the Windows registry.....	337
21.5	Daylight saving time (DST)	340
21.6	Adjusting Date in Forensic Explorer.....	341
Chapter 22 - Hashing.....		347
22.1	Hash Values	348
22.2	Hash Algorithms.....	348
22.3	Acquisition Hash	348
22.4	Verification Hash.....	348
22.5	Hashing files in a case	351
22.6	Hash sets.....	360
22.7	Download Hash Sets	361
22.8	Creating hash sets.....	361
22.9	Hash Match.....	365
22.10	Project VIC™	370
Chapter 23 - File Signature Analysis.....		375
23.1	File signature analysis.....	376
23.2	Why run file signature analysis?.....	376
23.3	Running a file signature analysis.....	377
23.4	Examine the results of a file signature analysis	378
Chapter 24 - Data Recovery.....		381
24.1	Data Recovery - Overview	382
24.2	FAT data recovery	383
24.3	NTFS data recovery.....	389
24.4	File carving.....	392
Chapter 25 - RAID		401
25.1	RAID - Introduction	402

25.2	Preparation	402
25.3	Adding a RAID to a case	403
Chapter 26 – Shadow Copy		407
26.1	Shadow Copy Introduction	408
26.2	Examining Shadow Copies With Forensic Explorer	412
Chapter 27 – Mount Image Pro		415
27.1	Mount Image Pro	416
Chapter 28 – Live Boot		418
28.1	Live Boot	419
28.2	Requirements	419
28.3	Compatibility	422
28.4	Live Boot Working Folder	423
28.5	Live Boot on Windows 11 Forensic Workstations	424
28.6	How to Live Boot a Forensic Image	426
28.7	Live Boot and User login Password bypass	431
28.8	Troubleshooting Live Boot	448
28.9	Creating A deployable live boot	452
Chapter 29 – Forensic Image Converter		463
29.1	Forensic Image Converter	464
29.2	Download and Install Forensic Image Converter	464
29.3	Add Forensic Image Converter to the Windows Path	466
29.4	Launching the Windows Command Line	468
29.5	ConvertTOL01.EXE - Usage	469
29.6	Validation of Conversion	473
Chapter 30 – Working With		475
30.1	iTunes Backups	477
30.2	Thumbnails	493
30.3	Video Key Frames (keyframes)	496

30.4	Jump Lists.....	498
30.5	Utilizing 3 rd Party Tools in Forensic Explorer	501
Chapter 31 – FEX Viewer		507
31.1	FEX Viewer	509
31.2	FEX Viewer Case.....	510
31.3	FEX Portable Case	511
Chapter 32 – FEX Automated Analysis		513
32.1	Automated Analysis.....	515
32.2	Graphics Analysis	516
32.3	Face Recognition.....	519
Chapter 33 - Legal		525
33.1	This User Guide.....	526
33.2	Copyright	526
33.3	License agreement.....	527
Appendix 1 - Technical Support		531
Appendix 2 - Write Blocking		533
Appendix 3 - File Carving		535
Appendix 4 - Summary of Date and Time		543
Appendix 5 - References.....		545
Appendix 6 - Definitions.....		549
Appendix 7 - Sample Script.....		563
Appendix 8 - Icon Key.....		565
Appendix 9 – iTunes Backup Files		567
Appendix 10 - Index		571

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:** <https://getdataforensics.com/>
- 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.

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 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: <https://getdataforensics.com/product/forensic-explorer-fex/download/>. Customers should download and install the **Full Version Dongle Only**.

Forensic Explorer Debug: The Forensic Explorer **debug version** contains a error reporting component that can assist technical support staff to isolate an issue. It is available on the **Other download links** section of the above page.

Mount Image Pro: Mount Image Pro is **required for Live Boot**. The latest version of Mount Image Pro is available for download at: <https://getdataforensics.com/product/mount-image-pro/download/>.

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 ddownload 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 is in the information bar at the bottom of the GUI.

FORENSIC EXPLORER MODULE OVERVIEW

Forensic Explorer is made up of modules which are accessed 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 the 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 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 of 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 a variety of email formats, including:

- .EDB Microsoft Exchange
- .EML Email Message format
- .MBOX Mailbox format
- .MSG Microsoft Message file
- .OST Microsoft Offline Storage Table
- .PST Microsoft Personal Storage Table

These 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:

1. Mount Image Pro (MIP). A Forensic Explorer dongle comes with a license of MIP. MIP can be downloaded from www.mountimage.com.
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 [APFS not supported at this time]) 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

1.2 INTRODUCING FORENSIC EXPLORER

Forensic Explorer is a computer forensics software program written by GetData Forensics Pty Ltd (<https://getdataforensics.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.

1.3 SUPPORTED FILE FORMATS

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

- DD or RAW;
- EnCase® .E01;

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

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

1.4 SUPPORTED FILE SYSTEMS

Forensic Explorer supports analysis of:

- Windows FAT12/16/32, exFAT, NTFS,
- Macintosh HFS, HFS+ (no journal processing), APFS (decryption and Live Boot not currently supported)

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

1.5 KEY PROGRAM FEATURES

Key Forensic Explorer features include:

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

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

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

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

Fully Threaded: Run different analysis functions in separate threads.

Data Views: Powerful data views including:

- **File List:** Sort and multi sort files by attribute, including, extension, signature, hash, path and created, accessed and modified dates.
- **Category Views:** Show files by extension, date etc.
- **Disk:** Navigate a disk and its structure via a graphical view. Zoom in and out to graphically map disk usage.
- **Gallery:** Thumbnail photos and image files.
- **Display:** Display more than 300 file types. Zoom, rotate, copy, search.
- **Filesystem Record:** Easily access and interpret FAT and NTFS records.
- **Text and Hexadecimal:** Access and analyse data at a text or hexadecimal 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

CHAPTER 2 - 30 DAY EVALUATION VERSION

2.1	30 day evaluation version.....	20
2.1.1	Installation	20
2.1.2	Limitations.....	20
2.2	Activating the 30-DAY evaluation version	20
2.2.1	Online Activation (30 day Evaluation).....	20
2.2.2	Offline Activation (30 day evaluation)	22

2.1 30 DAY EVALUATION VERSION

To request a 30-day evaluation version of Forensic Explorer, visit <https://getdataforensics.com/> 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 in 30 days.

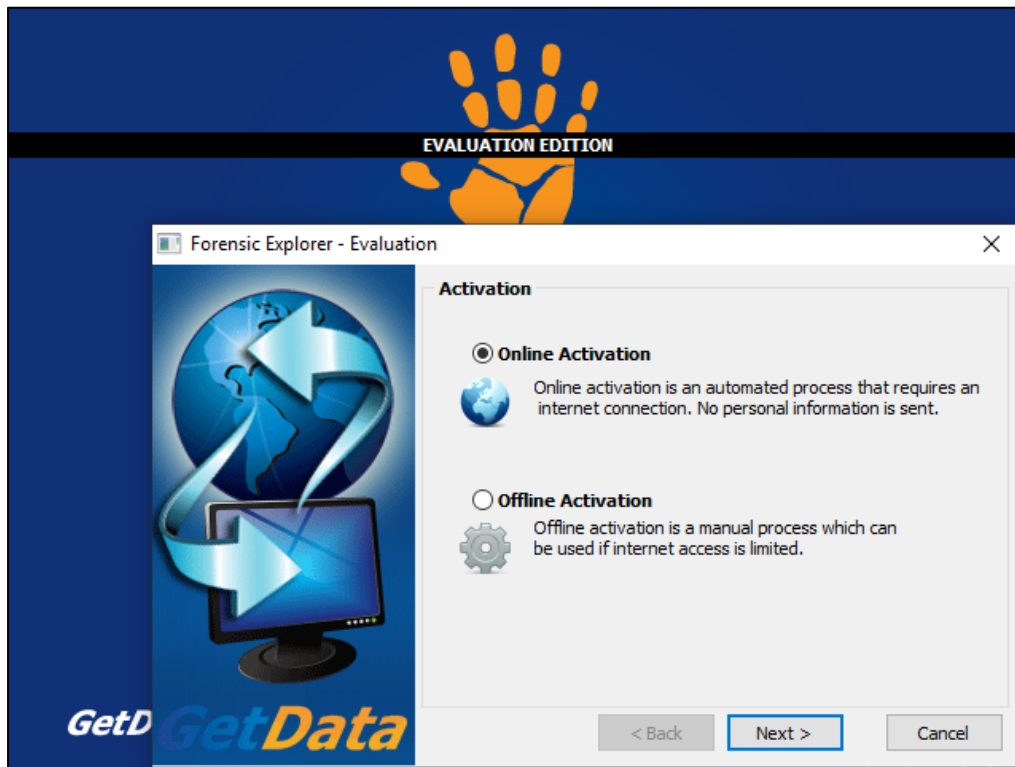
2.2 ACTIVATING THE 30-DAY EVALUATION VERSION

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

2.2.1 ONLINE ACTIVATION (30 DAY EVALUATION)

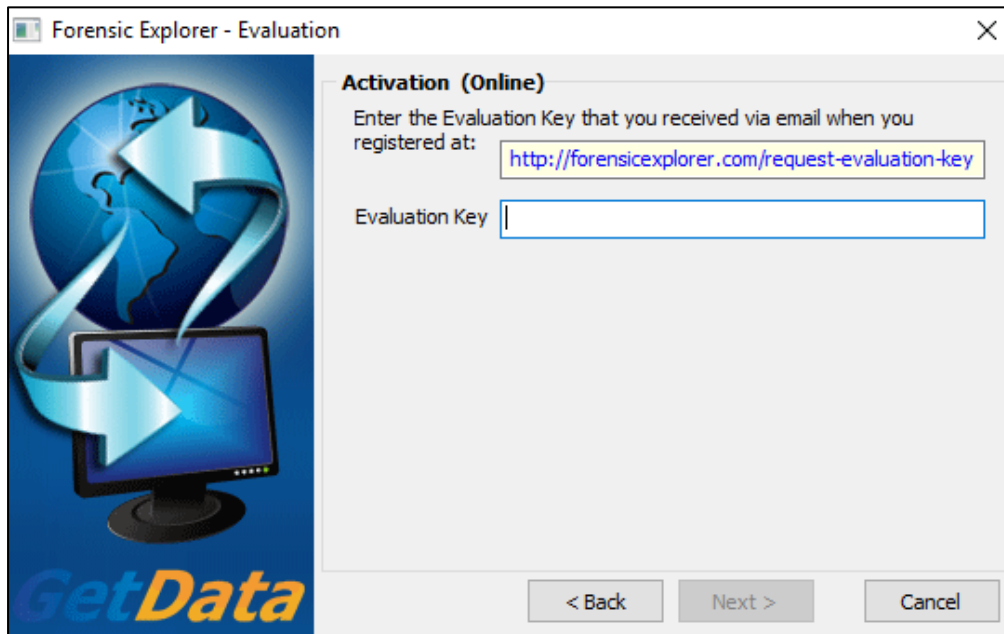
If your computer is connected to the internet, enter the 30 day evaluation version key into the field provided and click Next (as shown in Figure 1 below):

Figure 1: Online activation, 30-day trial version



An evaluation key input message will display the following screen, as shown in Figure 2 below:

Figure 2: 30-day evaluation key input activation message



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

Figure 3: 30-day evaluation version splash screen



2.2.2 OFFLINE ACTIVATION (30 DAY EVALUATION)

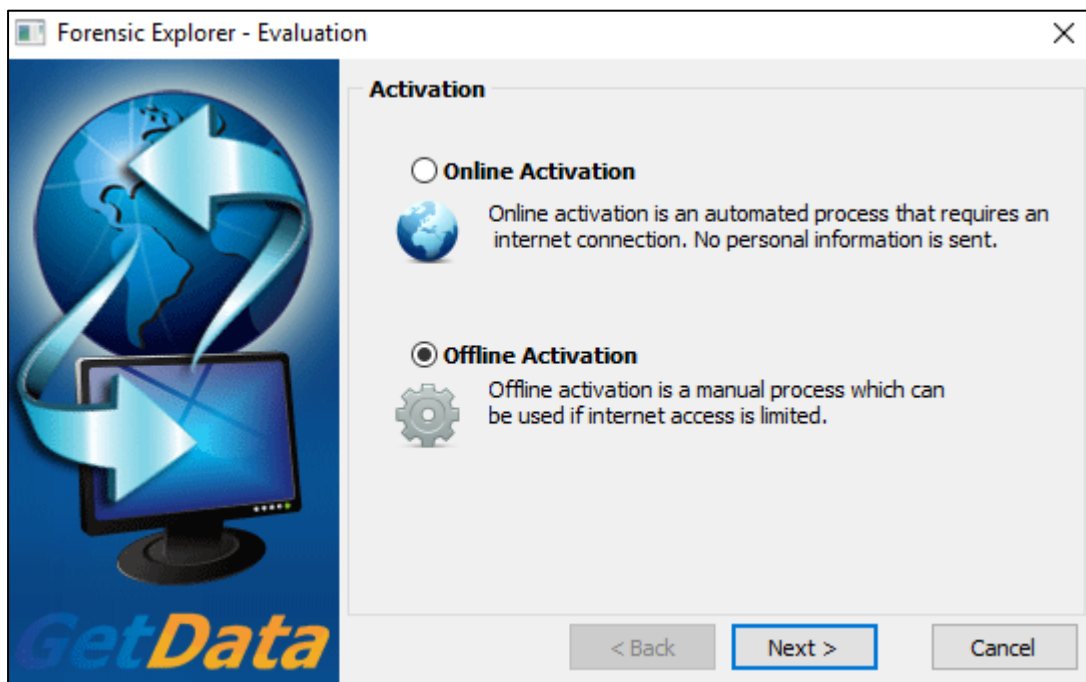
Where the computer on which the software is being installed is not connected to the internet, a separate internet connected computer can be used to activate. The activation process involves:

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

To activate an offline computer:

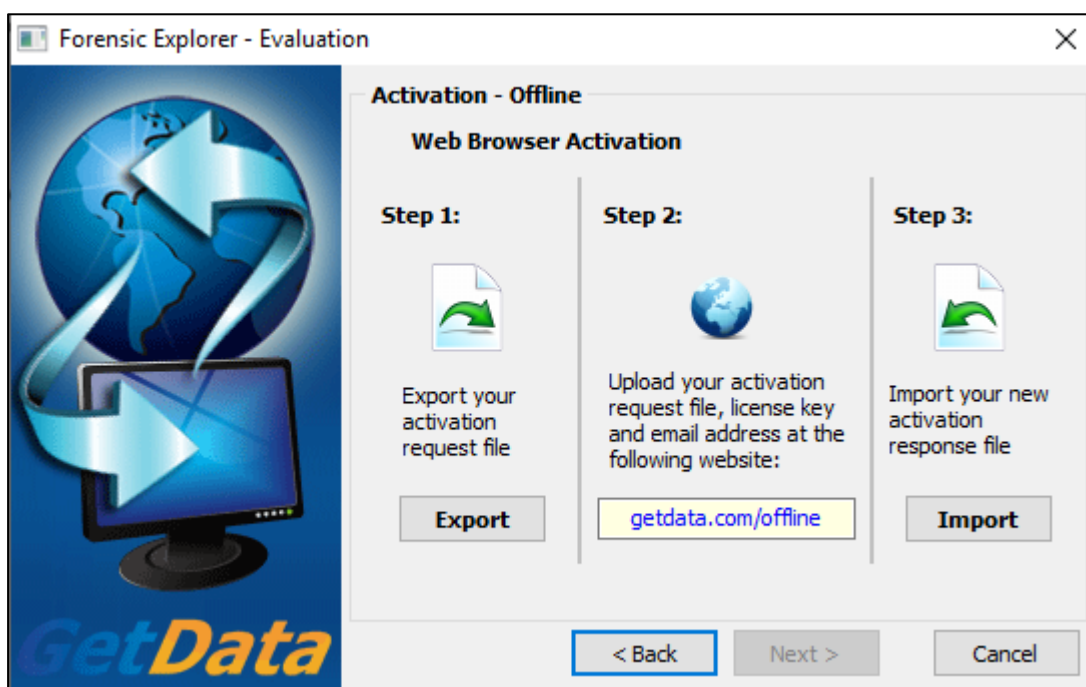
1. Click the Offline Activation button and click Next;

Figure 4: Activation wizard



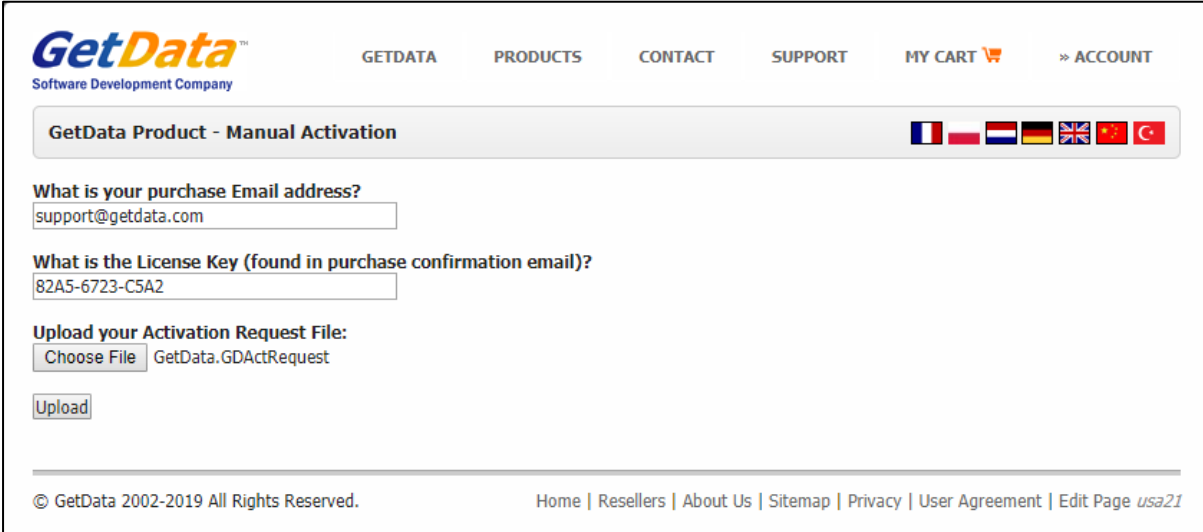
2. Click on the Export button to export and save the license file "GetData.GDActRequest":

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





3. Using a web browser on any internet connected computer, go to <http://getdata.com/offline> (or <http://support.getdata.com/offline-wibu.php>) and enter the required details:

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



GetData™
Software Development Company

GETDATA PRODUCTS CONTACT SUPPORT MY CART  » ACCOUNT

GetData Product - Manual Activation 

What is your purchase Email address?

What is the License Key (found in purchase confirmation email)?

Upload your Activation Request File:
 GetData.GDActRequest

© GetData 2002-2019 All Rights Reserved. Home | Resellers | About Us | Sitemap | Privacy | User Agreement | Edit Page usa21

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



GetData Product - Manual Activation

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

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.--

Chapter 3 - Purchase

In This Chapter

CHAPTER 3 - PURCHASE

3.1	Purchase	26
3.1.1	Purchase Online	26
3.1.2	Purchase Orders	26
3.1.3	Resellers	26
3.2	License maintenance	27
3.2.1	Purchase License Maintenance	27

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 <https://getdataforensics.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 support@getdata.com

Or via your forensic reseller.

GetData fulfil purchase orders in accordance with the laws of the State of New South Wales and the Commonwealth of Australia and any dispute relating a purchase order shall be governed by these laws, without regard to any other Country or State choice of law rules. This supersedes all prior proposals, negotiations, representations, agreements and understandings between the parties, including those contained in any confidentiality agreements, and all terms and conditions contained in any Customer-provided purchase orders, and constitutes the complete and exclusive agreement between Customer and Company regarding the subject matter hereof. Any reference to a purchase order or similar documentation on an invoice or other acceptance thereof is solely for Customer's convenience in record keeping, and no such reference or the provision of Services to Customer shall be deemed an acknowledgement of or agreement to any terms or conditions associated with any such purchase order or other provided documentation. Any such associated terms and conditions shall be of no force and effect and do not apply to and have no effect.

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 8 below:

Figure 8: Forensic Explorer splash screen showing maintenance date



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

3.2.1 PURCHASE LICENSE MAINTENANCE

To purchase additional Forensic Explorer maintenance online:

1. Visit the following web page: <https://getdataforensics.com/>
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 section 5.5.

Chapter 4 - Installation

In This Chapter

CHAPTER 4 - INSTALLATION

4.1	System requirements.....	31
4.2	Download.....	31
4.3	Installation.....	31
4.3.1	Check for Updates.....	33
4.3.2	Installed files.....	35
4.3.3	Dark Mode.....	39
4.3.4	Non-English installation.....	39
4.3.5	Command Line Tool.....	40
4.4	Uninstall Forensic Explorer.....	41

4.1 SYSTEM REQUIREMENTS

Forensic Explorer minimum recommendations:

- Windows 10 or above.
- Pentium i7 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:

Download the **full version** of Forensic Explorer from <https://getdataforensics.com/product/forensic-explorer-fex/download/>.

30-day evaluation version:

Download the **evaluation** version from: <https://getdataforensics.com/product/forensic-explorer-fex/download/>

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

4.3 INSTALLATION

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

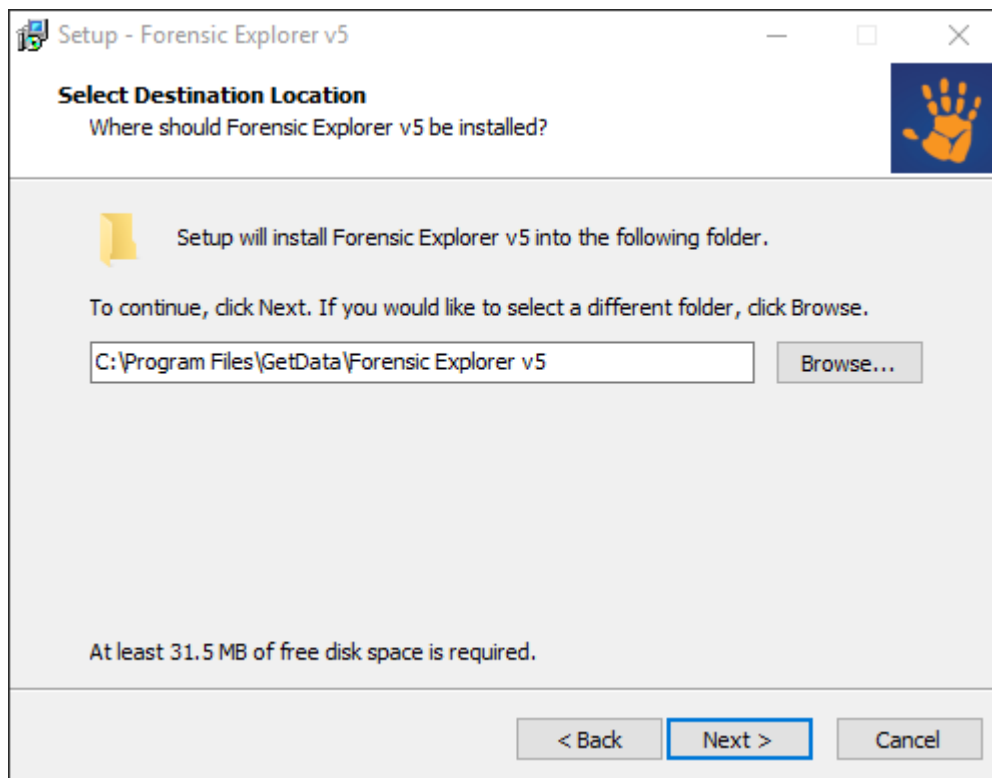
To install Forensic Explorer:

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

The following windows will appear during the installation process:

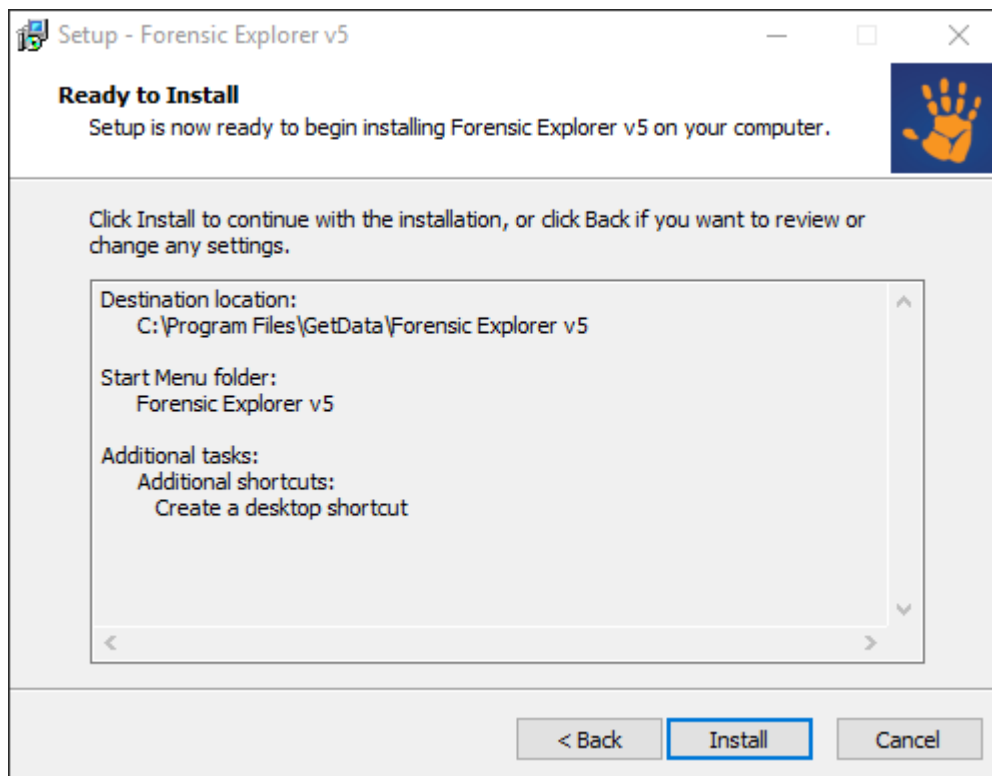
1. Forensic Explorer License agreement. Answer the question and click **Next**.
2. Select the installation language. Click **Next**.
3. Enter the correct installation path or accept the default path (e.g., **C:\Program Files\GetData\Forensic Explorer vX**) and click **Next**;

Figure 9: Selecting the installation folder



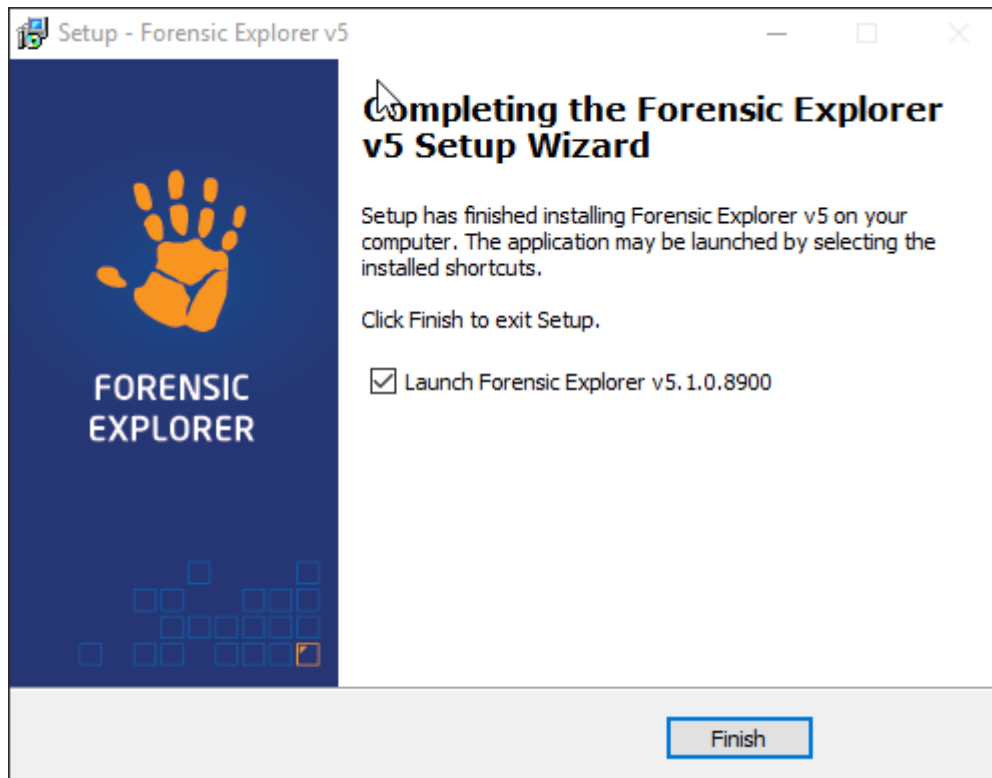
1. Follow the setup instructions and confirm the setup summary by clicking the **Install** button.

Figure 10: Finalize installation



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

Figure 11: Finish installation



3. Run Forensic Explorer from the installed desktop icon:

Figure 12: Desktop icon



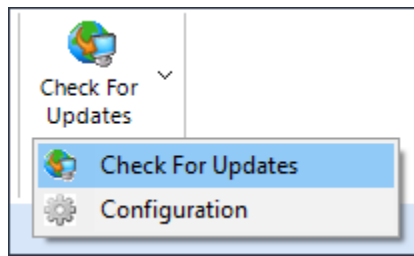
4.3.1 CHECK FOR UPDATES

Forensic Explorer updates and change log are located at <https://getdataforensics.com/product/forensic-explorer-fex/download/>

To check for updates from Forensic Explorer:

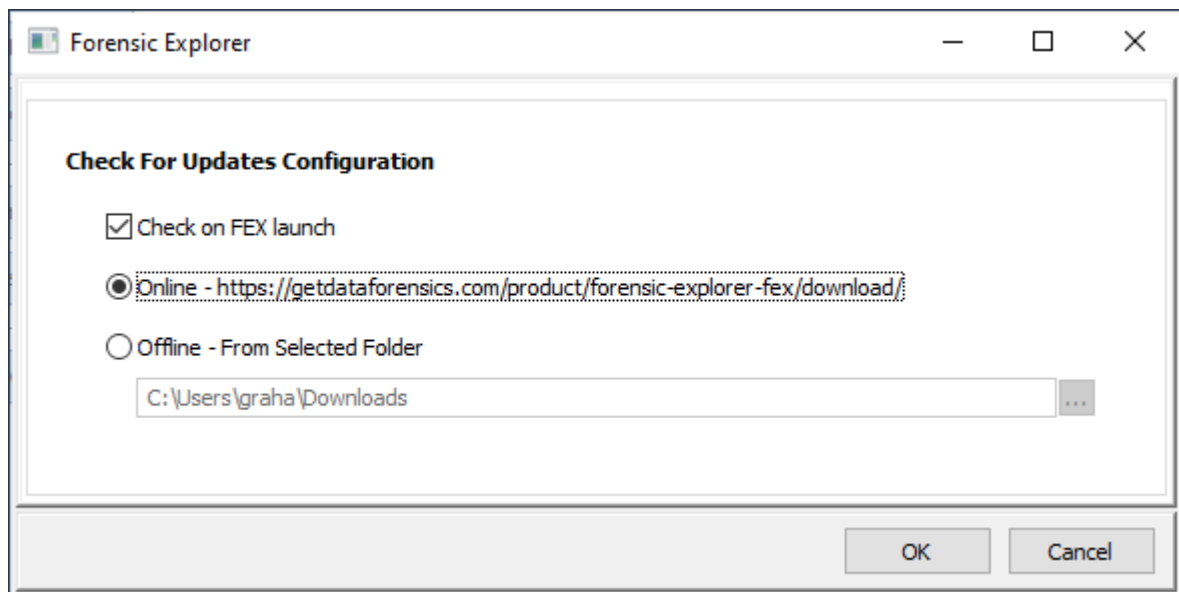
1. Run the software and go to the **Evidence** module.
2. On the toolbar, click the **Check for Updates** button:

Figure 13: Evidence module tool bar, Check for Updates



3. The **Configuration** option in the menu enables the following options:

Figure 14: Check for Updates Configuration

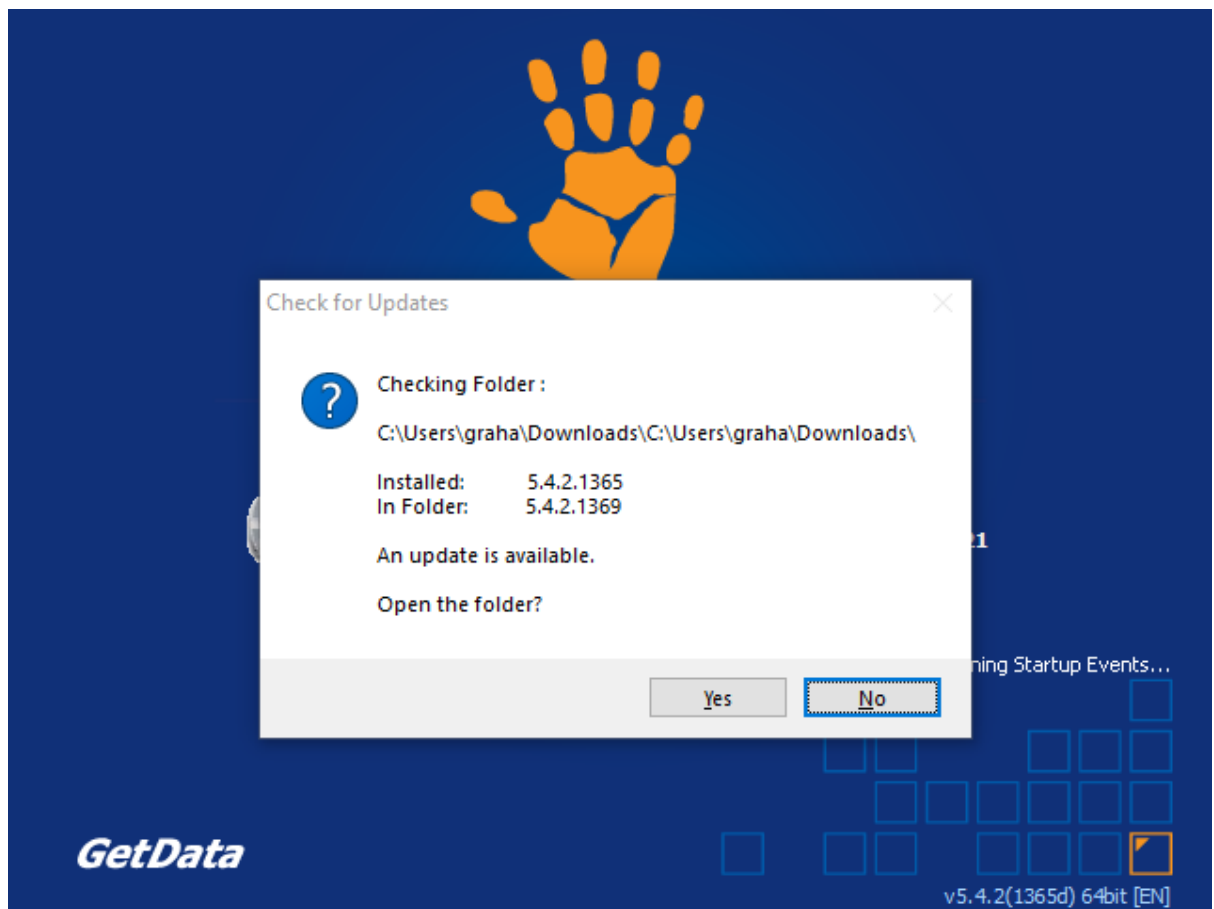


Check on FEX Launch: This checkbox will enable the check when Forensic Explorer is launched from the desktop icon. The check takes place during the period when the program splash screen is displayed.

Online: When the **Online** radio button is selected, a comparison is made between the currently running version number and the version number available at the Forensic Explorer download page: <https://getdataforensics.com/product/forensic-explorer-fex/download/>. If the version on the web page is more recent, an option to go to the web pages is provided.

Offline – From Selected Folder: For security purposes, many forensic workstations are air-gapped from the internet. The offline option can be used to check for updates in a specified folder (either locally or a network folder). If a version exists in the specified folder that is more recent than the running version, a message is displayed to open this folder (the most recent version is shown in the message window):

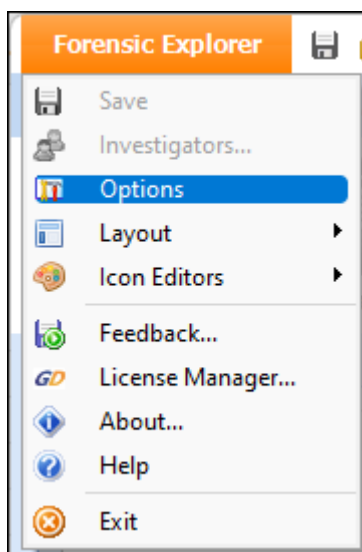
Figure 15: Check for Updates (Check on Launch is selected)



4.3.2 INSTALLED FILES

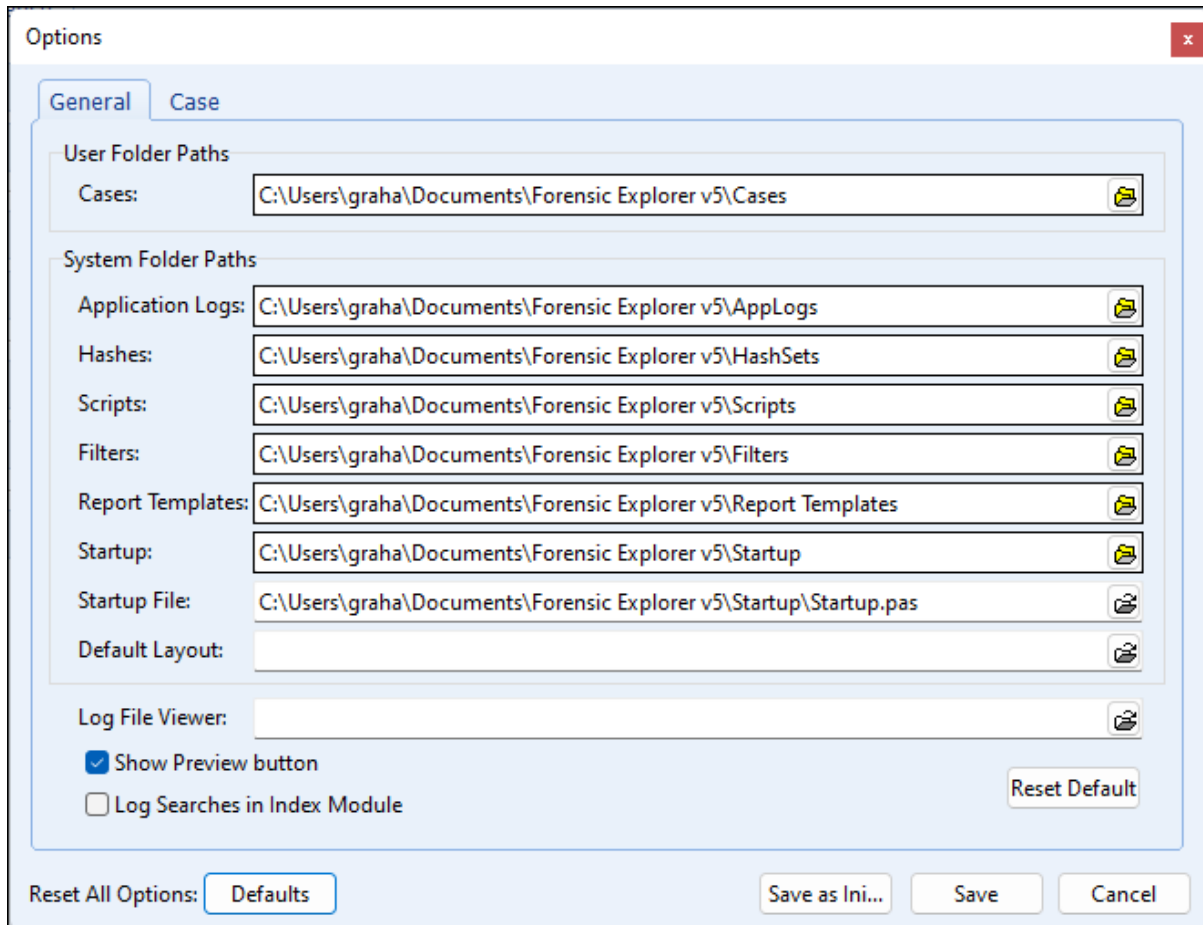
Folder paths are managed via the **Forensic Explorer > Options** menu:

Figure 16: Forensic Explorer menu



The **Options** window provides access to **user and system folder paths**.

Figure 17: Forensic Explorer > Options



PROGRAM PATH





The default Forensic Explorer installation folder is:


C:\Program Files\GetData\Forensic Explorer vX

WORKING PATH

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

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







 AppLogs	Forensic Explorer usage logs.
 Bookmark Templates	Bookmark templates folder.
 Cases	Contains the investigator created case folders.
 Databases	Holds case database files use to store case data, investigator names, etc.

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

CASE FILE FOLDER

The following folders are created within each case folder:

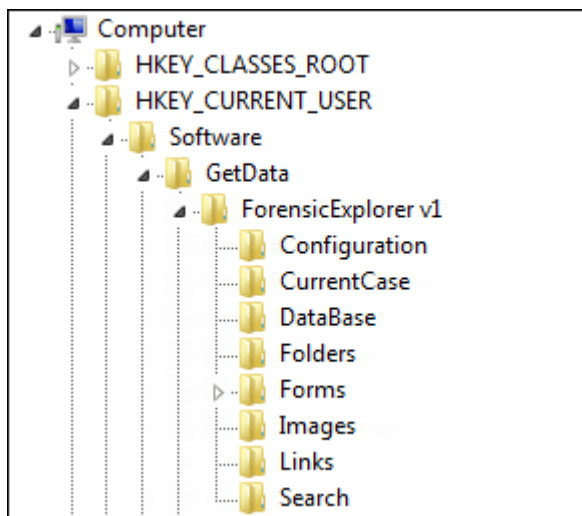
C:\Users\[user folder]\Documents\Forensic Explorer\Cases\[Case Name]

 Attached Evidence	External files (photos, documents etc.) attached to the case.
 DTSearchIndexes	DT Search keyword indexes.
 Expanded	Stores expanded compound files (e.g., ZIP) in BatesNumber.L01 format.
 Exported	File export folder.
 Logs	Program audit logs.
 Reports	Reports folder.
CaseName.FEX	Case file.

REGISTRY KEYS

At the time of installation Forensic Explorer registry keys, including user and system folder path details, are written to the HKEY_CURRENT_USER as shown in Figure 18 below:

Figure 18: Forensic Explorer registry keys

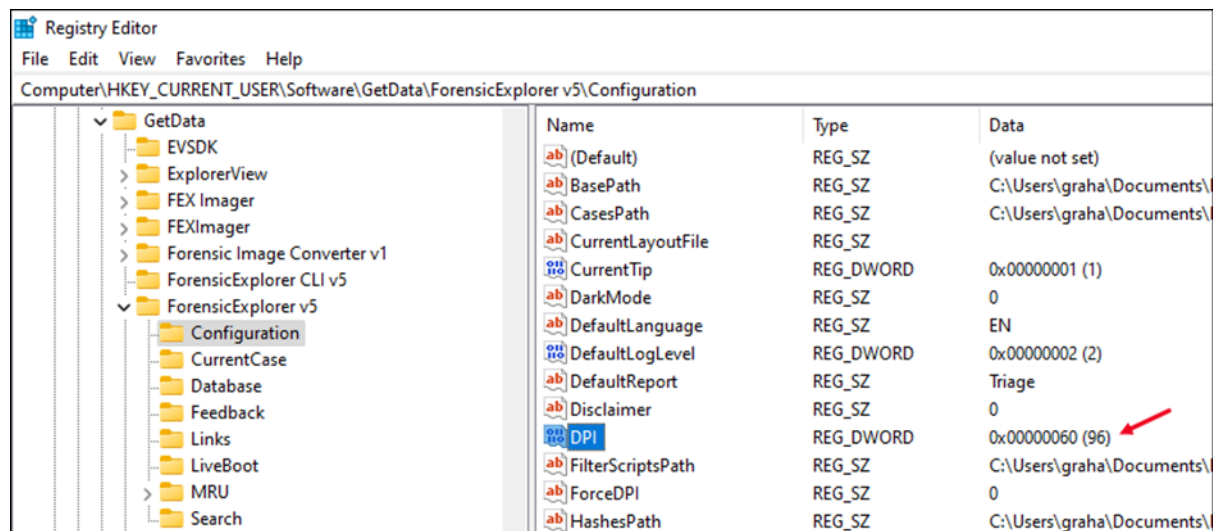


PROBLEMATIC SCREEN RESOLUTION (DPI)

In some circumstances where a non-standard monitor resolution is used (for example, running Forensic Explorer through a data projector) resolution issues may appear in the Reports module or when creating PDFs.

It is possible to manually override the resolution setting by editing the DPI value in the ForensicExplorer v5 > Configuration > DPI registry key. This can also be set using the FEX_CommandLine5.ini file described below.

Figure 19: Manually set display resolution (DPI)



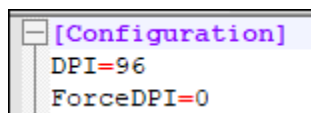
FORENSIC EXPLROER.INI

From Forensic Explorer versions 5.4.8(2771) the **Options** window contains a **Save as Ini** button (shown in Figure 17 above). This button is used to create a **ForensicExplorer.ini** text file with the current configuration settings. Paths within this file can be manually edited as desired.

When Forensic Explorer is launched it first checks for the presence of **ForensicExplroer.ini** in the installation folder (i.e., the folder containing ForensicExplorer.exe). If **ForensicExplorer.ini** is present, its settings are used, otherwise it reads the settings from the registry.

To manually set the display resolution (described above) add the following values to the .ini file and adjust the DPI number as desired.

Figure 20: Manually setting the display resolution (DPI).



4.3.3 DARK MODE

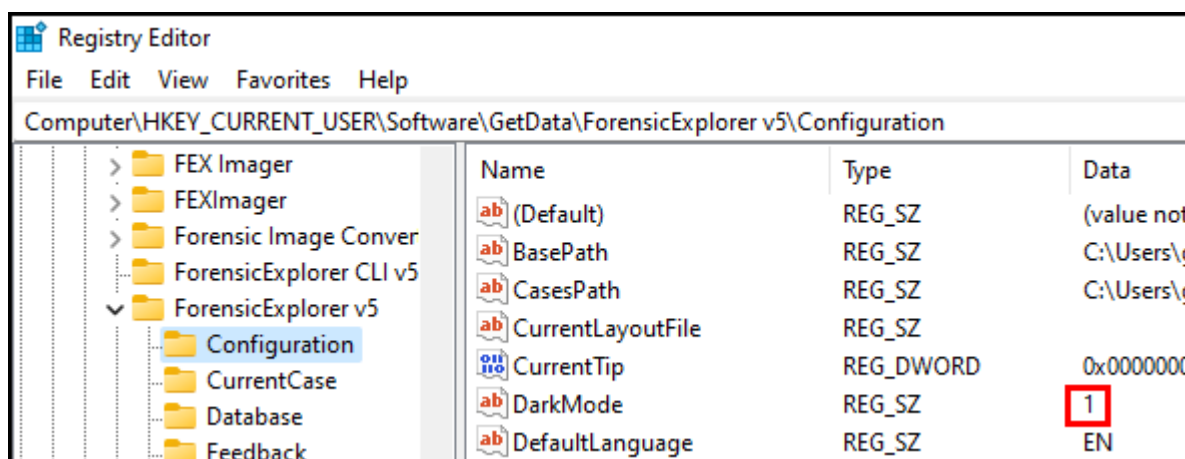
Dark mode changes display to a dark background using a dark theme or color inversion.

Note: Dark mode is work-in-progress and will be improved over multiple version releases. Please contact support@getdata.com for specific dark mode issues.

Activating dark mode requires a registry edit to: **HKEY_CURRENT_USER\Software\GetData\Forensic Explorer v5\Configuration\DarkMode**.

1. Close Forensic Explorer.
2. Run Windows RegEdit and select the above key.
 - a. For dark mode set **Value data** to 1.
 - b. For light mode set **Value data** to 0.
3. Launch Forensic Explorer.

Figure 21: Set dark mode in the registry



4.3.4 NON-ENGLISH INSTALLATION

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

- Chinese (Simplified)
- French
- 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 v5\Configuration\DefaultLanguage

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

BOOKMARK FOLDER TRANSLATION

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

4.3.5 COMMAND LINE TOOL

Forensic Explorer v5 introduces the FEX CLI as stand-alone Command Line tool. The FEX CLI can be launched from USB for triage, run at a workstation level, or expanded to operate at an enterprise level virtual environment spawning multiple simultaneous processing instances.

The FEX CLI can automate all standard forensic processing tasks, including signature analysis, hash verification, hash match, file carve, registry triage, metadata extraction etc.

FEX CLI is licensed separately from the Forensic Explorer GUI. Contact sales@getdata.com for more information.

```

C:\> Create New Case From File (fex_cli_launcher.py): Test 1 - "C:\Users\Owner\Desktop\FEX_CLI_64bit_(v5.1.0.8845)\bin64\FEX_Comm...
Investigator:      Investigator (CLI)
Investigator GUID: {D7DEB64C-45C5-49FA-8802-A719CA134A7B}
Working Directory: C:\Users\Owner\Desktop\FEX_CLI_64bit_(v5.1.0.8845)\cases\
Creating New Case: Test 1
Process XML:      C:\Users\Owner\Desktop\FEX_CLI_64bit_(v5.1.0.8845)\txml\txml_examples\6_multiple_tasks.xml
-----+-----+-----+-----+-----+
Task                |Description                |%   |Time   |State
-----+-----+-----+-----+-----+
Search for Known ISO Tracks |Devices 1, ISO/DVD tracks 0|100 |00:00:00|Complete
Search for Known MBRs      |Devices 1, MBRs 1, Partitions 4|100 |00:00:00|Complete
Search for FileSystems     |Files and folders 198435    |100 |00:00:05|Complete
Signature Analysis        |Processed 198443 of 198443  |100 |00:00:24|Complete
Triage - Registry         |Processing complete         |64  |00:00:34|Complete
Triage - SAM User Accounts|Processing complete         |100 |00:00:05|Complete
Triage - File System      |Processing complete         |100 |00:00:54|Complete
Triage Report             |Initializing: Wiping Tools  |100 |00:00:03|Complete
Filter                    |Filter "cli_filter_by_type_graphics_video.pas"|100 |00:00:08|Running
Hash Files                 |Processed 2.61 GB of 3.90 GB|71  |00:00:06|Running

```

4.4 UNINSTALL FORENSIC EXPLORER

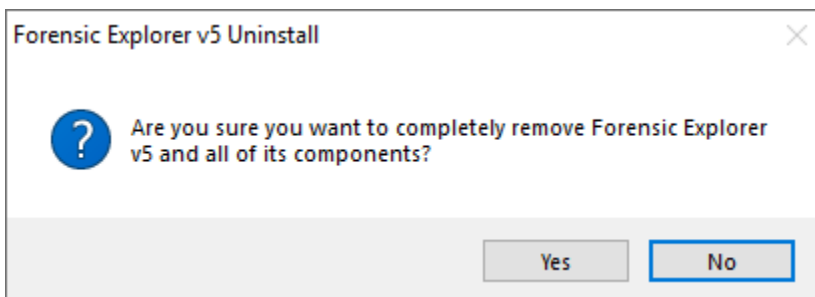
IMPORTANT: Ensure that you have a separate and secure backup of all evidence and case files before you make installation modifications.

To uninstall Forensic Explorer:

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

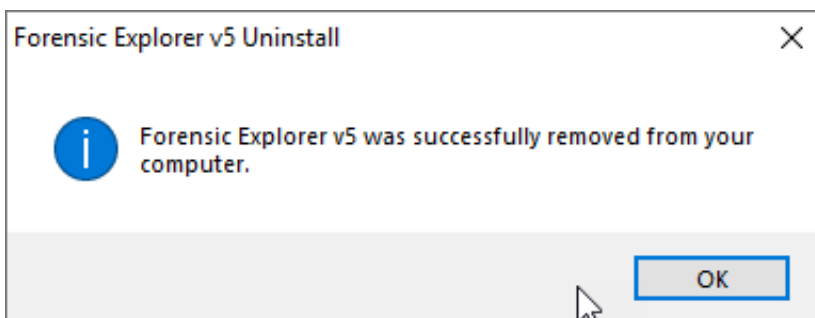
The following window will display:

Figure 22: Uninstall process



A successful removal will show the following message:

Figure 23: 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 deletes them as needed.)

The working path: **\My Documents\Forensic Explorer vX** 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

CHAPTER 5 - DONGLE ACTIVATION

5.1	Dongle activation of the purchased version	44
5.1.1	Successful dongle activation	45
5.1.2	Troubleshooting Dongle Activation	45
5.2	GetData License Manager.....	47
5.3	Wibu CodeMeter Runtime for Windows User.....	49
5.4	Network Licensing	51
5.4.1	Configure a Network dongle with multiple licenses	51
5.4.2	Setup the Server.....	52
5.4.3	Setting up the client (forensic workstation).....	53
5.5	Applying maintenance updates to your Wibu dongle	55

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 24: 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 25 below. Include this number in correspondence with GetData:

Figure 25: 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).

Chapter 5 - Dongle Activation

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

5.1.1 SUCCESSFUL DONGLE ACTIVATION

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



The splash screen identifies:

1. The name, or company name, of the registered owner.
2. The date upon which the current maintenance license expires for that dongle (see page 27 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 26 below:

Figure 26: Dongle not found error message



To troubleshoot dongle activation:

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

If you are still not able to activate Forensic Explorer:

1. Run the GetData LicenseManager.exe from the Forensic Explorer installation folder, or available for download here: <http://download.getdata.com/support/LicenseManager.exe> (LicenseManager is described in more detail below).
2. Download and install **Wibu CodeMeter Runtime** for Windows (described below): <https://www.wibu.com/support/user/downloads-user-software.html>.

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

- Your dongle ID number.
- A screenshot of the GetData License Manager.

Chapter 5 - Dongle Activation

- A screenshot of the CodeMeter Control Center.

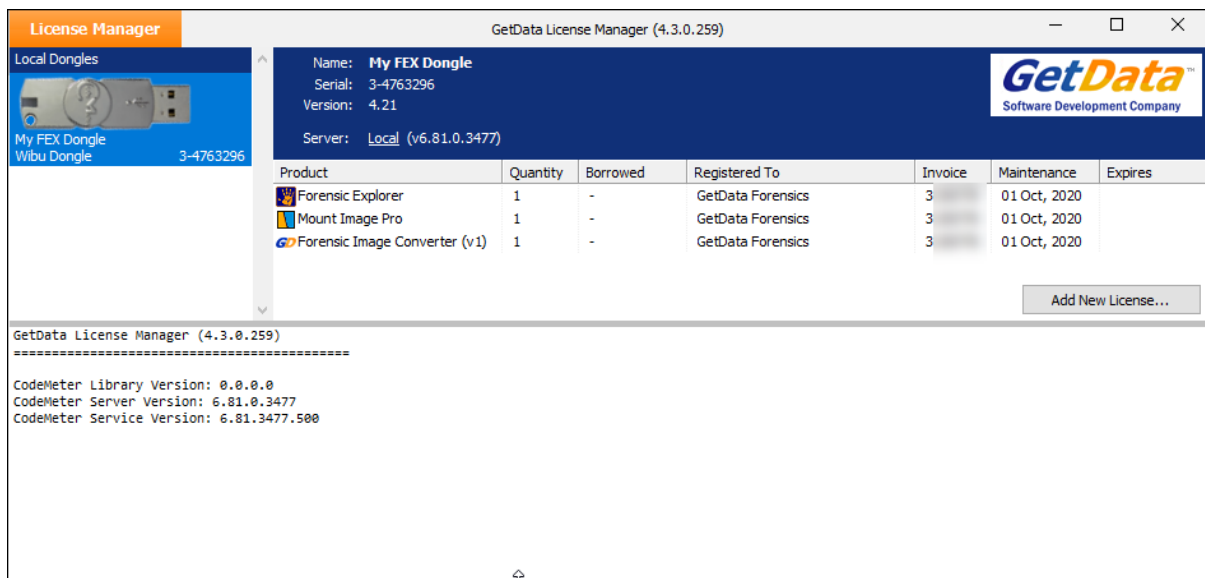
We will then contact you with further instructions.

5.2 GETDATA LICENSE MANAGER

GetData License Manager is a stand-alone executable that is used to provide information about and manage activation. The LicenseManager.exe is in the Forensic Explorer installation folder or is available for download from: <http://download.getdata.com/support/LicenseManager.exe>

The License Manager gives information about licenses including software maintenance dates. It is used to program dongles and apply maintenance updates (see 5.5 below).

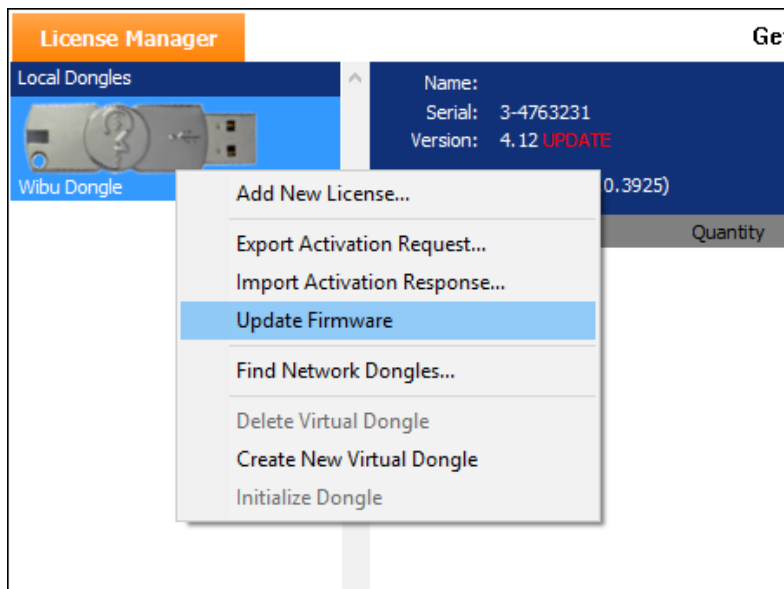
Figure 27: GetData License Manager



UPDATE DONGLE FIRMWARE FROM GEDATA LICENSE MANAGER

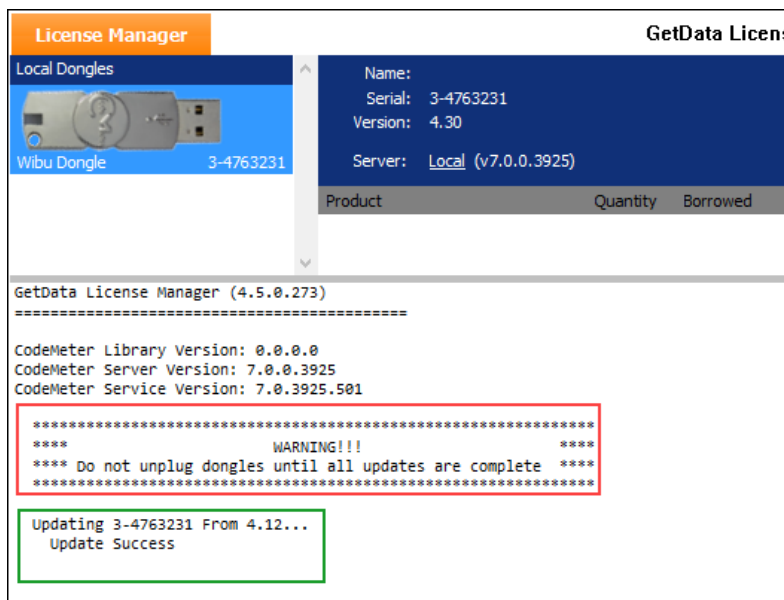
Wibu CodeMeter dongle firmware should be updated from time to time. If the firmware is out of date a red **UPDATE** will display in the GetData **License Manager** next to the version number. Right click on the dongle and select **Update Firmware** from the drop-down menu, as shown in Figure 28 below:

Figure 28, Update Wibu Firmware from GetData License Manager



IMPORTANT: Do not remove the Wibu dongle from the computer during the firmware update. Remove only once the **Update Success** message shown in Figure 29 below is received:

Figure 29, Successful Wibu Firmware Update



5.3 WIBU CODEMETER RUNTIME FOR WINDOWS USER

Wibu CodeMeter Runtime is the management tool for the Wibu Codemeter activation system. Download it here: <https://www.wibu.com/support/user/downloads-user-software.html>

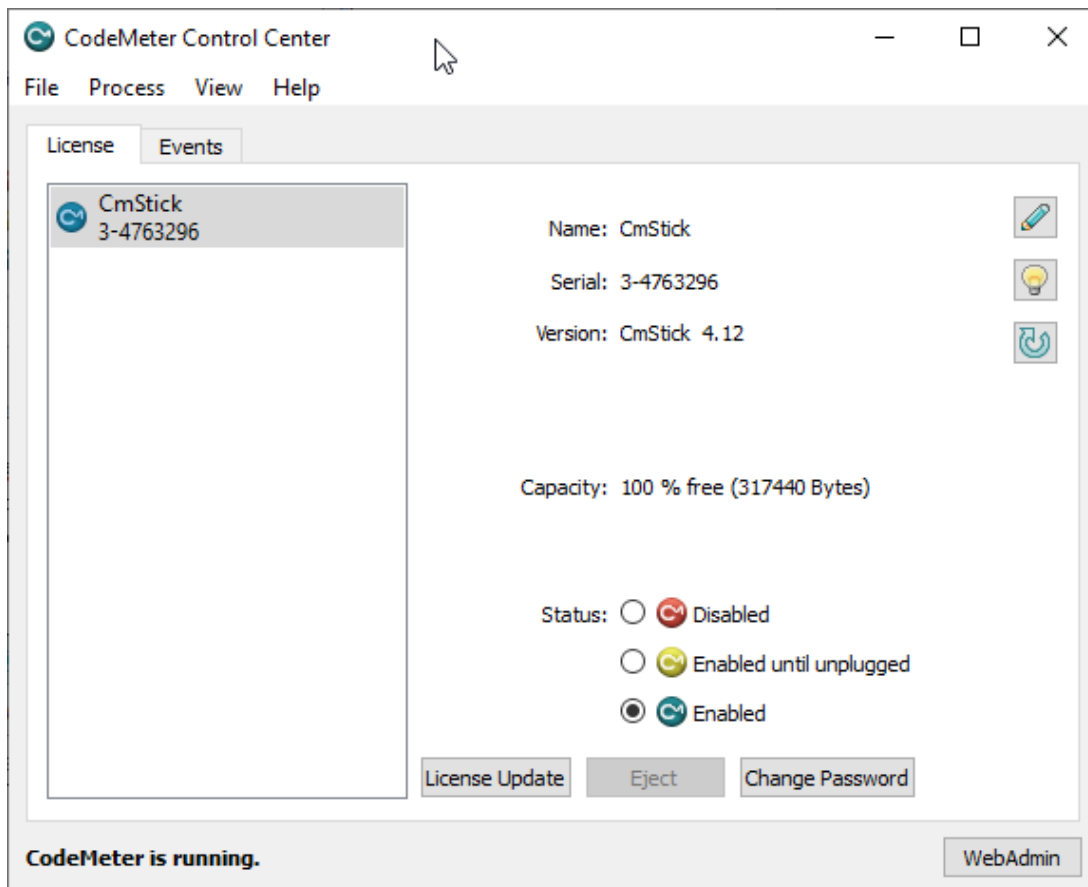
When Wibu CodeMeter Runtime is successfully installed, insert your Forensic Explorer Wibu dongle. Double click on the Wibu icon in the Windows task bar, or launch “Codemeter Control Center”:

Figure 30: Wibu CodeMeter Windows task bar icon



The CodeMeter Control Center will open, shown in Figure 31 below. Note that the dongle serial number shown in the CodeMeter Control Center is the same as that which is engraved on the dongle as shown in Figure 25 above:

Figure 31: Wibu CodeMeter Control Center



Confirm that:

1. Your dongle (**CmStick**) is identified by the CodeMeter Control Center.

2. **CodeMeter** is running (this is the Windows Service responsible for activation).
3. The **Status** is **Enabled**.

RENAME WIBU CODEMETER DONGLE


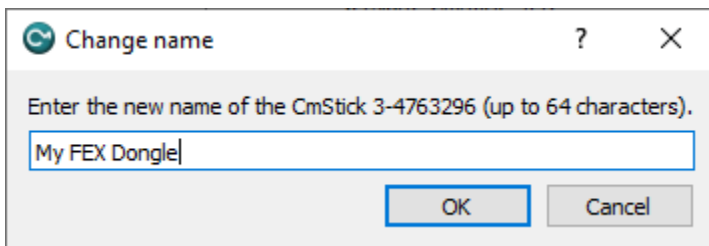
The CmStick can be given a custom name by clicking on the edit button: 

Figure 32: Creating a custom name for the Wibu dongle



UPDATE DONGLE FIRMWARE USING CODEMETER FOR WINDOWS USER


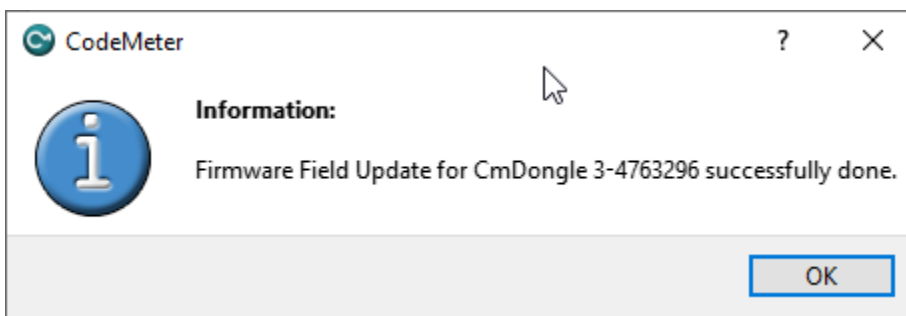
Wibu CodeMeter dongle firmware should be updated from time to time. Click on the update button 

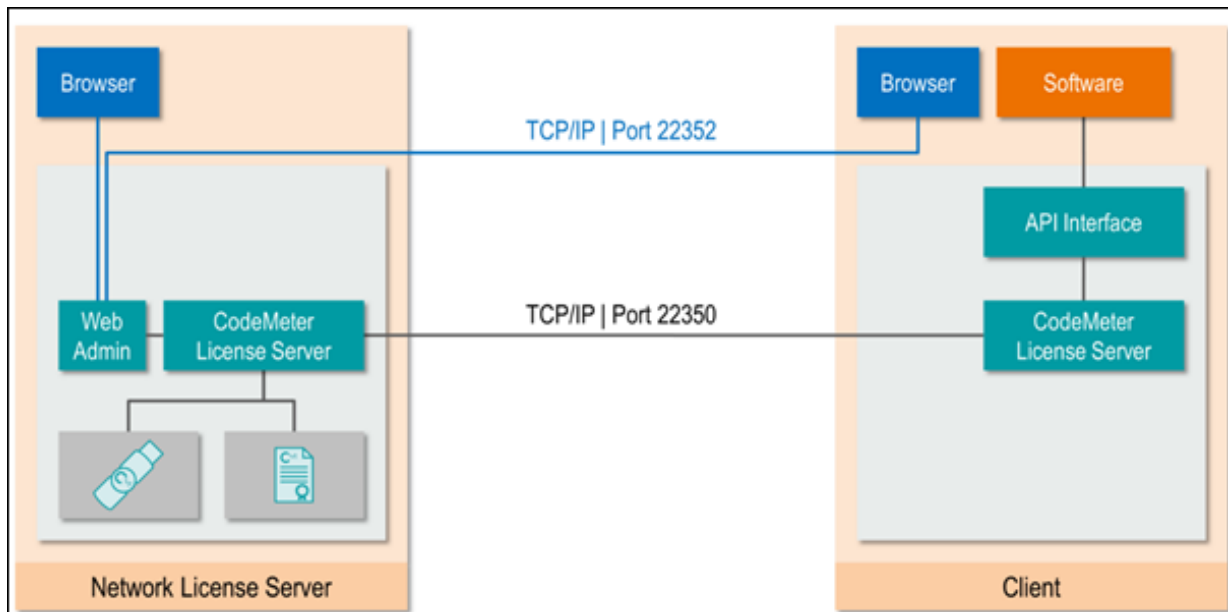
Figure 33: Wibu CodeMeter - Update firmware



5.4 NETWORK LICENSING

Wibu CodeMeter allows for network license activation. For example, a single dongle can contain 20 licenses which allows 20 remote computers to activate. More information is available here: <https://www.wibu.com/products/codemeter/network-license-server.html>

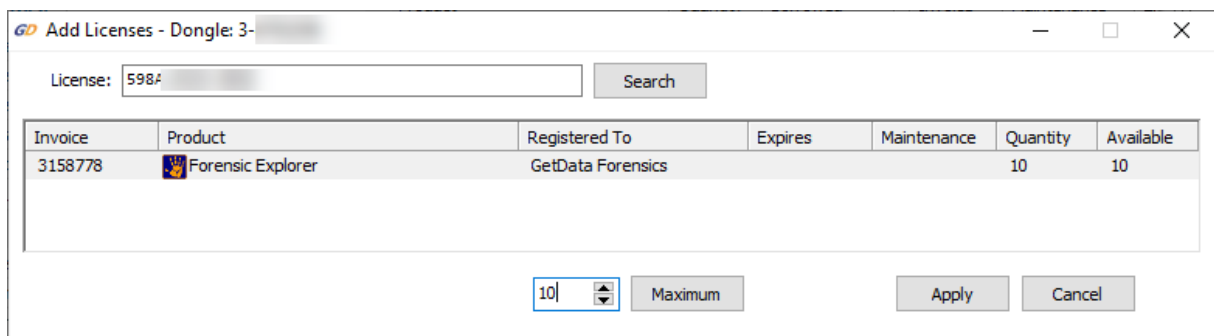
Figure 34: Wibu CodeMeter network activation



5.4.1 CONFIGURE A NETWORK DONGLE WITH MULTIPLE LICENSES

When a network license is purchased from GetData the supplied dongle is pre-configured with the required number of licenses. However, it is possible for the end-user to program a dongle with the required number of licenses using the GetData License Manager (described in 5.2 above) and using the license number selection at the bottom of the add license screen.

Figure 35: GetData License Manager - Creating a network dongle

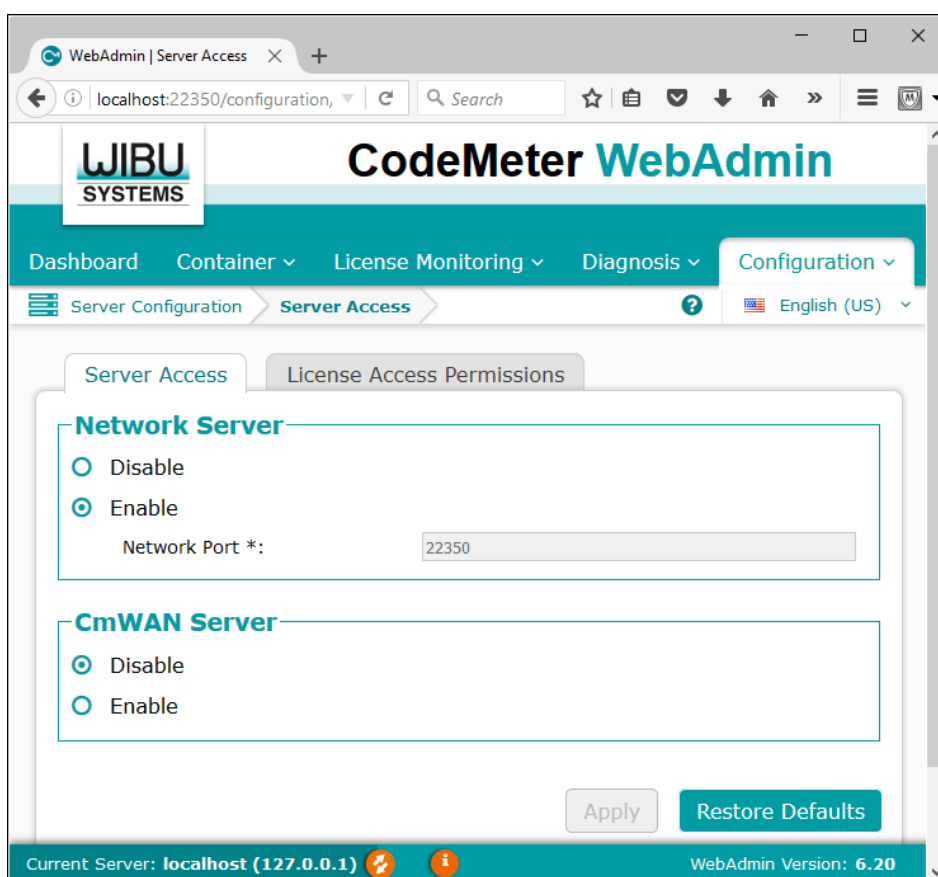


5.4.2 SETUP THE SERVER

On the **computer to be used as the Network Server**:

1. Download the latest **CodeMeter Runtime for Windows User** from <http://download.getdata.com/CodeMeterRuntime.exe> (case sensitive)
2. Run **CodeMeter WebAdmin** from the button in Codemeter Control Center (shown in Figure 31 above) or by browsing to <http://localhost:22350>
3. Select **Configuration > Server Configuration** from the menu, as shown in Figure 36 below:

Figure 36: CodeMeter WebAdmin



4. In the **Network Server** 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 **Process > Stop CodeMeter Service**.

- c. Then **Start CodeMeter Service**.

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

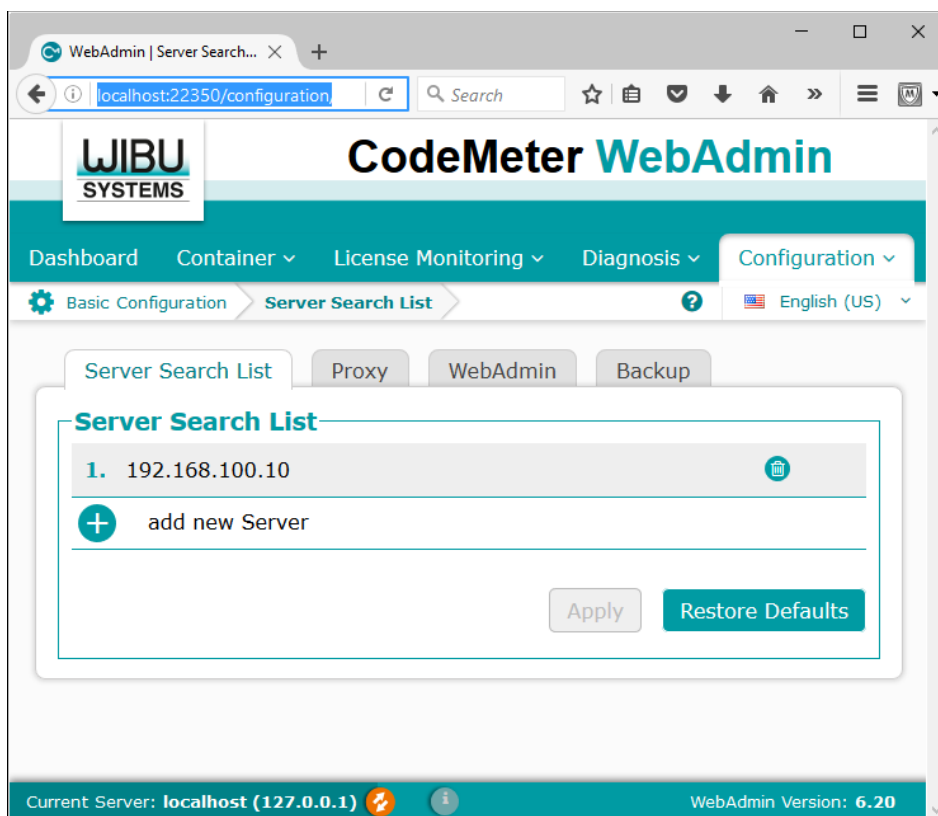
```
HKEY_LOCAL_MACHINE\SOFTWARE\WIBU-SYSTEMS\CodeMeter\Server\CurrentVersion  
IsNetworkServer=1
```

5.4.3 SETTING UP THE CLIENT (FORENSIC WORKSTATION)

On the **client computer**:

1. Install Forensic Explorer full dongle version. **Close** Forensic Explorer.
2. Browse to <http://localhost:22350> and select the **Configuration** tab:

Figure 37: Wibu CodeMeter Local Host Configuration



3. In the **Basic** menu click the **add new server** button and add the IP address of **Network Server** and press **Apply**.
4. 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:

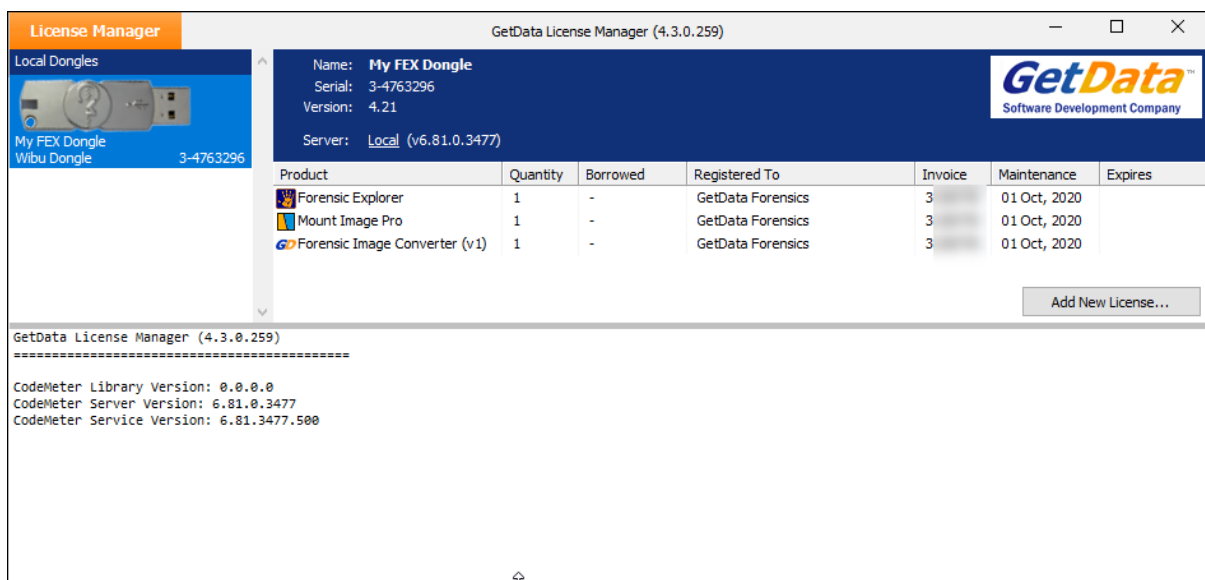
HKEY_LOCAL_MACHINE\SOFTWARE\WIBU-
SYSTEMS\CodeMeter\Server\CurrentVersion\ServerSearchList\Server1
Address=192.168.100.10

5.5 APPLYING MAINTENANCE UPDATES TO YOUR WIBU DONGLE

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

1. Remove any other Wibu dongles that you may have for other products (e.g., EnCase, FTK, etc.).
2. On a computer that has **internet access**, insert your **Forensic Explorer Wibu dongle** into a USB port.
3. Run the **GetData License Manager** located in the installation folder of Forensic Explorer. The default location is: **C:\Program Files\GetData\Forensic Explorer vX\LicenseManager.exe**
4. The GetData License Manager will **detect your Wibu dongle**, as shown in Figure 38 below. The existing Maintenance expiration date is displayed in the Maintenance column:

Figure 38: GetData License Manager



5. **Do NOT delete any existing licenses from the dongle.**
6. **Click on Forensic Explorer** in the **Product** list and press the **Add New License** button.
7. In the **Add Licenses** window, enter the **License** key that you received with your maintenance renewal order. Press the **Search** key.
8. Select the renewal from the available product list. Then click the **Apply** button.
9. Return to the main screen of the License Manager. The dongle should now show the updated 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	58
6.2	GetData's Forensic Imager.....	59
6.2.1	Installation	59
6.2.2	System Requirements	59
6.2.3	Protected Disk Areas - HPA and DCO	59
6.2.4	Running Forensic Imager.....	60
6.2.5	Selecting the source.....	60
6.2.6	Hash or Acquire.....	63
6.2.7	Selecting the destination	63
6.2.8	3. Progress.....	66
6.2.9	4. Log file.....	68
6.2.10	Bad Sectors and error reporting	68

6.1 WRITE BLOCK

IMPORTANT:

An accepted principle 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 39 below is a Tableau USB hardware write block. The source media, an 8 GB Kingston USB drive is attached and ready for acquisition:

Figure 39: Tableau USB write block with USB as the source drive



6.2 GETDATA'S FORENSIC IMAGER

In May 2020 GetData released an update to 'Forensic Imager'. It was renamed to **FEX Imager v2** and is supplied in the Forensic Explorer installation folder as **FEXImager.exe**.

FEX 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")
- E01 (EnCase®) [Version 6 format]
- L01 (EnCase®) (when **Folders and Files** are acquired).

6.2.1 INSTALLATION

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

C:\Program Files\GetData\Forensic Explorer v5\ForensicImager.exe

6.2.2 SYSTEM REQUIREMENTS

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

FEX Imager requires the following minimum specification:

- Windows 7 or above.
- 32 and 64bit compatible.
- I7 processor.
- 8 GB RAM.

FEX 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)

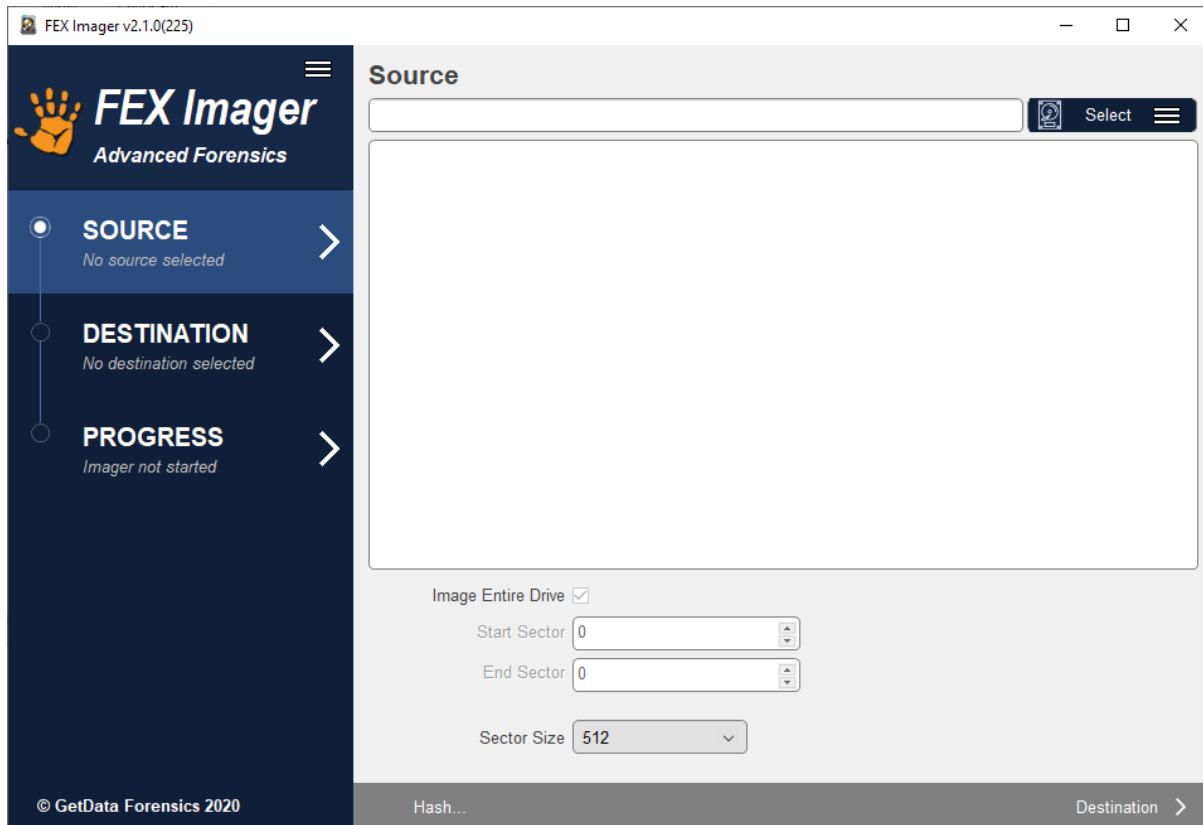
The HPA and DCO are two areas of a hard drive that are not normally visible to an operating system or an end user. The HPA is most used for booting and diagnostic utilities. For example, some computer manufacturers use the area to contain a preloaded OS for installation and recovery purposes. The DCO *"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. **FEX Imager** does **not** currently support the acquisition of HPA or DCO areas.

6.2.4 RUNNING FORENSIC IMAGER

FEX Imager is in the Forensic Explorer installation folder as a stand-alone executable. When **FEX Imager** is run, the investigator is presented with the **Source** window:

Figure 40: Forensic Imager



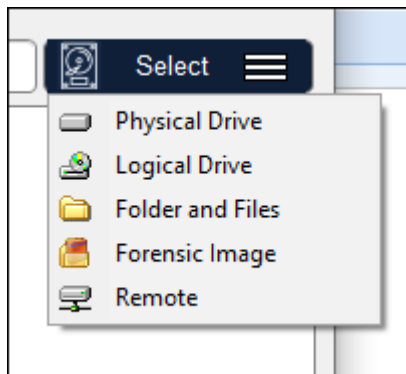
6.2.5 SELECTING THE SOURCE

The **source** describes the data to be acquired. The source can be:

- A **physical drive** (i.e., a physical hard disk)
- A **logical drive** (i.e., a partition such as C:\ or D:\)
- A **folder** or **files** located on a partition
- An existing **Forensic Image** (i.e., an **E01** or **DD** image file)
- A remote drive accessed using the Forensic Explorer servlet.

To **select the source**, click on the **Select** button drop-down menu:

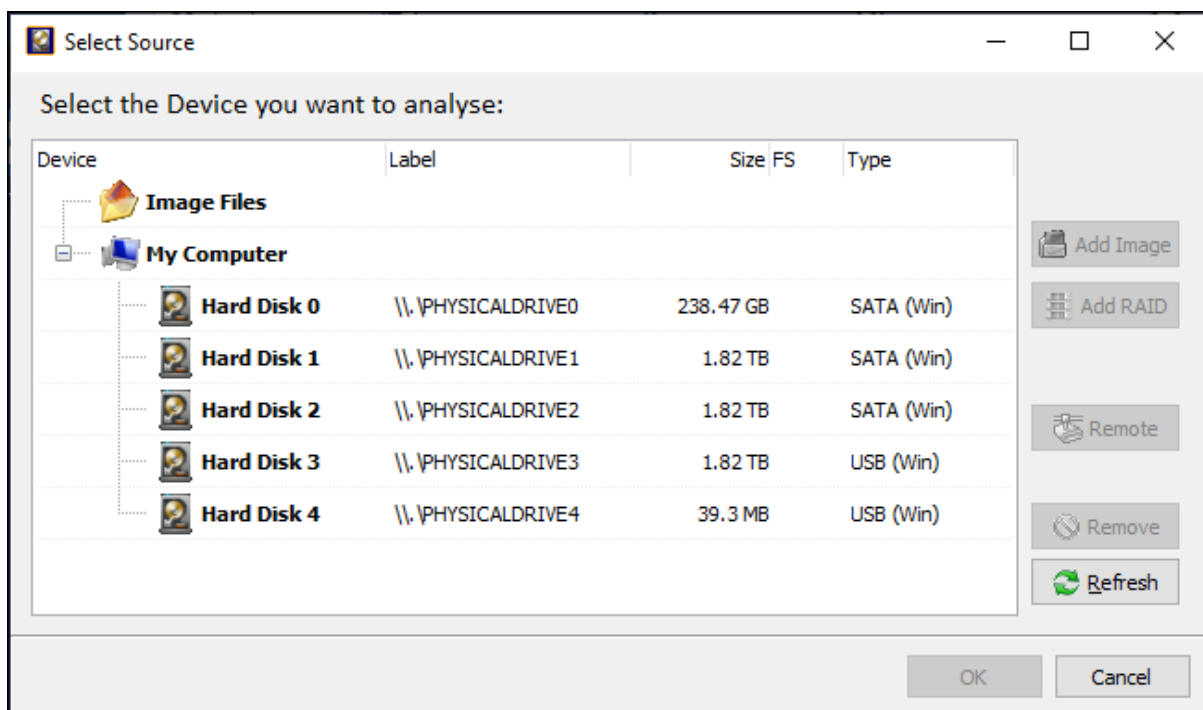
Figure 41, FEX Imager Select source



The **Select** option chosen will determine what is shown in the **Select Source** window. Figure 42 below shows the result of selecting the **Physical Drive** option.

NOTE: If physical drives are not displayed in this window, it is usually because FEX Imager was **not launched as administrator**, and it does not have sufficient privileges to access the physical drives. Re-launch FEX Imager by right-clicking on the icon and **run as administrator**.

Figure 42: Forensic Imager - selecting the source device (Verify or Hash option shown)



The device selection window includes the following information:

Label: Physical drives are listed with their Windows device number. Logical drives display the drive label (if no label is present then "{no label}" is used). Image files show the path to the image.

Size: The size column contains the size of the physical or logical device, or the size of the image file.

(Note that the reported size of a drive is usually smaller than the size printed on the drive label. This is because 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, HFS, APFS.

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 will forensically image a physical device. Imaging the physical device gives access to the content of the entire media, for example, the space between partitions. Carrier, 2005, observes: *“The rule of thumb is to acquire data at the lowest layer that we think there will be evidence. For most cases, an investigator will acquire every sector of a disk”*. (2 p. 48)

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

Figure 43, Select FEX Imager start and end sectors

The screenshot shows a window with a checkbox labeled 'Image Entire Drive' which is checked. Below it are two input fields: 'Start Sector' and 'End Sector', both containing the value '0'. Each input field has a small up/down arrow on its right side.

When a source device is selected the source selection window will populate with the device information:

Figure 44. FEX Image source drive information

The screenshot shows a window titled 'Source' with a text box containing '\\.\PHYSICALDRIVE0'. Below this is a list of properties for the selected source:

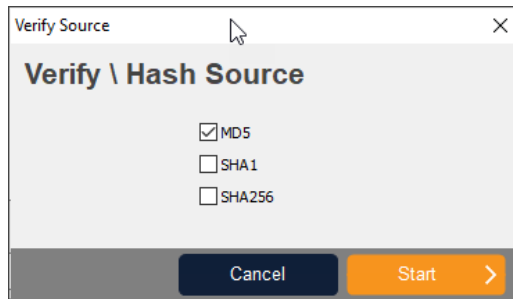
Source Name	\\.\PHYSICALDRIVE0
Description	Hard Disk 0
Serial No	141997403308
Product ID	SanDisk SD6SB1M256G1002
Product Rev.	X231600
Size	238.47 GB
Sectors	500118192
Sector Size	512 bytes

6.2.6 HASH OR ACQUIRE

Once a source is selected, two options become available at the bottom of the **Source** window:

Hash: Hash is selected when the users wishes only to calculate a hash for the device (for example, to verify the hash of an existing forensic image file).

Figure 45: Verify\Hash

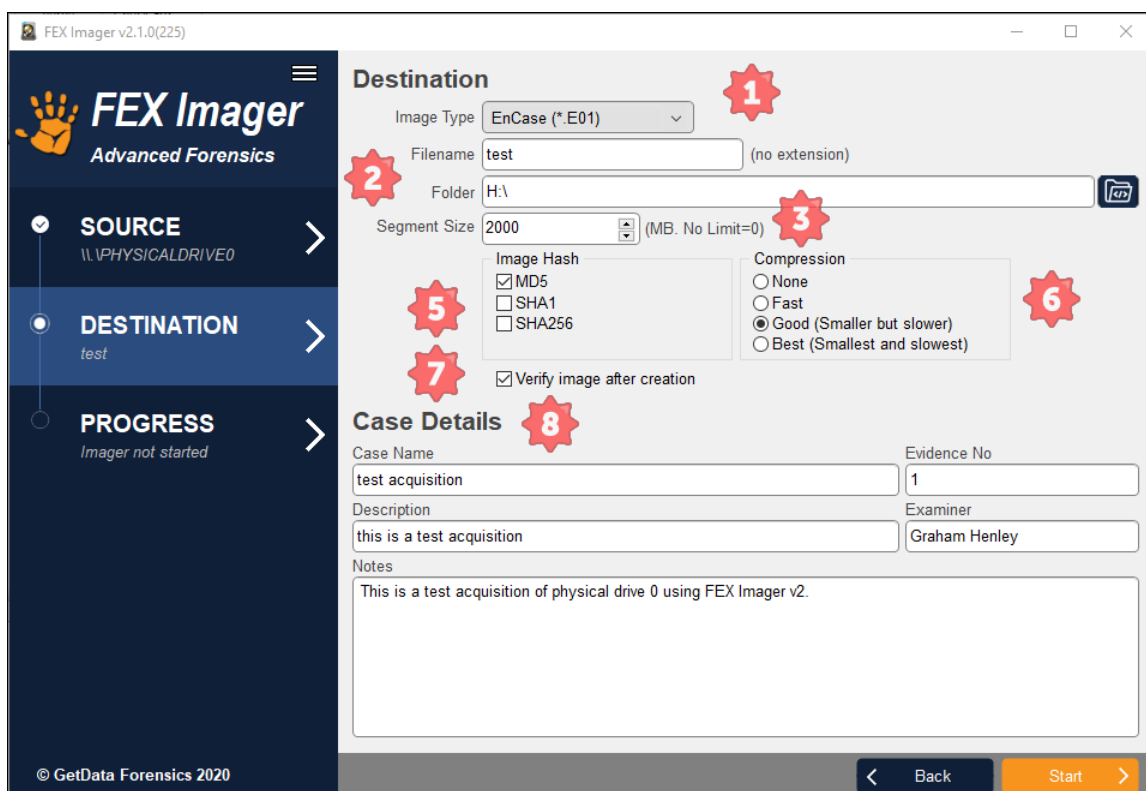


Destination: The **Destination** button is selected to acquire a forensic image. It is described in more detail below.

6.2.7 SELECTING THE DESTINATION

The image destination screen, shown in Figure 46 below, is where the parameters for the image file are set, including type, compression, name, location etc.

Figure 46: Setting destination options



1. IMAGE TYPE

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

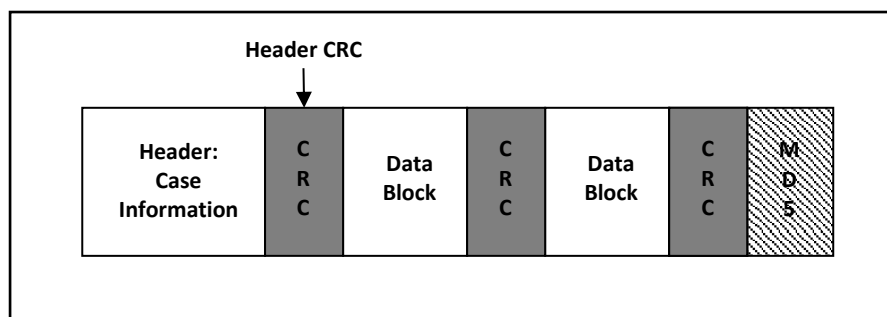
DD / RAW:

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.

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 47: EnCase® header



Source: (3)

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 investigator's forensic workstation. Click on the folder icon to browse for the destination folder.

5. HASH OPTIONS

Calculates an MD5, SHA1 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". (4).

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. (5) (6)

SHA-256:

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

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

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 investigator's 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.

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.

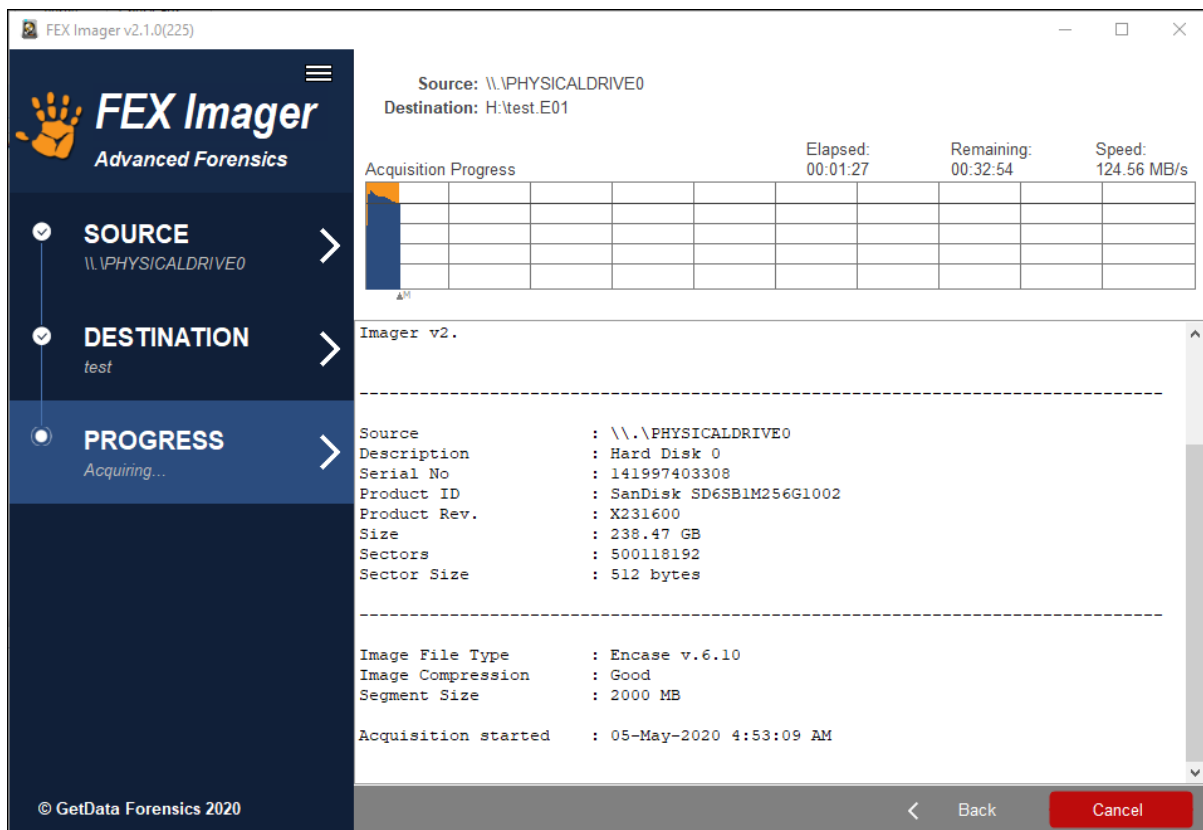
8. DETAILS

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.

6.2.8 3. PROGRESS

The progress screen displays source information (the drive being acquired) and destination information (location where the forensic image files are being written). Progress information, including elapsed time, time remaining, and transfer speed is displayed. The progress window is shown in Figure 48 below:

Figure 48: Forensic Imager Progress screen



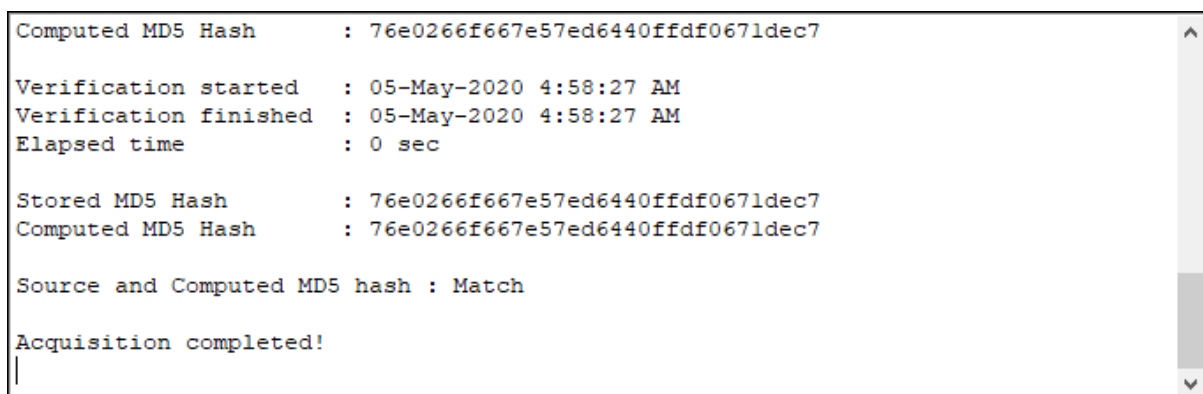
The bottom half of the progress window provides summary information about the acquisition process, including hash information.

If the **E01** image format was selected the **acquisition hash** is stored within the forensic image. If the **verify image after creation** option was selected in the FEX Imager Destination window, the progress window will include a comparison between the:

Stored [Hash Type]: A hash of the data taken during the acquisition and stored in the E01; and

Computed Hash: A hash of the data in the created forensic image file.

Figure 49, FEX Image Progress window hash information



Note that if the **DD** image format is selected a hash value is not stored within the DD image file.

6.2.9 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:

6.2.10 BAD SECTORS AND ERROR REPORTING

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

Chapter 7 - Forensic Explorer Interface











In This Chapter

CHAPTER 7 - FORENSIC EXPLORER INTERFACE

7.1	Modules	70
7.1.1	Undocking and docking modules	70
7.2	Module data views	72
7.2.1	Undocking and docking data views	72
7.3	Customizing layouts	74
7.3.1	Save a custom layout	74
7.3.2	Load a custom layout	74
7.3.3	Default layout	74

7.1 MODULES

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

Tab	Function	Chapter
 Evidence	Case management.	Chapter 10
 File System	Detailed analysis of file systems added to the case.	Chapter 11
 Artifacts	Artifacts can include browsing history, char, call history, Operating System records, and other potential evidence.	Chapter 12
 Keyword Search	Keyword search raw case data using simple or RegEx keywords.	Chapter 13
 Index Search	Create and search indexed data using dtSearch technology.	Chapter 14
 Email	Examine PST files.	Chapter 15
 Registry	View and analyze registry files.	Chapter 16
 Bookmarks	Add investigator bookmarks to document the analysis.	Chapter 17
 Reports	Create reports.	Chapter 18
 Scripts	Program, manage and run scripts against case data.	Chapter 19

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.

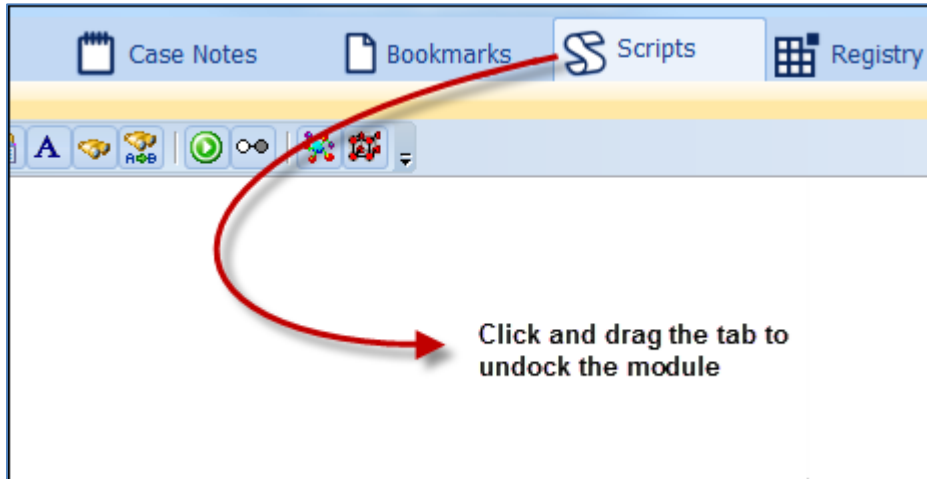
7.1.1 UNDOCKING AND DOCKING MODULES

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:

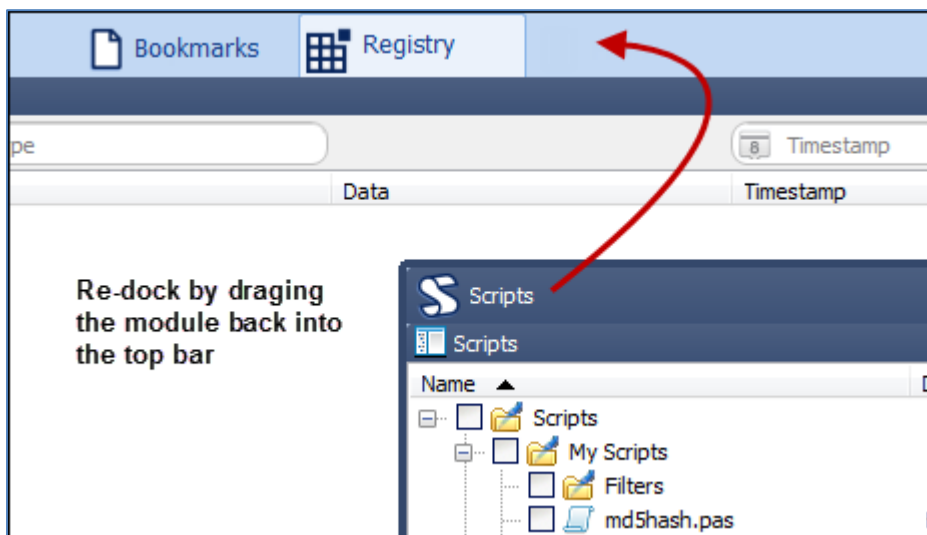
1. Select the module tab with the mouse.
2. Hold down the mouse and drag the module tab free of the bar, as shown in Figure 50 below:

Figure 50: Un-docking a module

**To dock a module:**

1. Select the top bar of the module window.
2. Drag and drop the module back into the module tab menu bar, as shown in Figure 51 below:

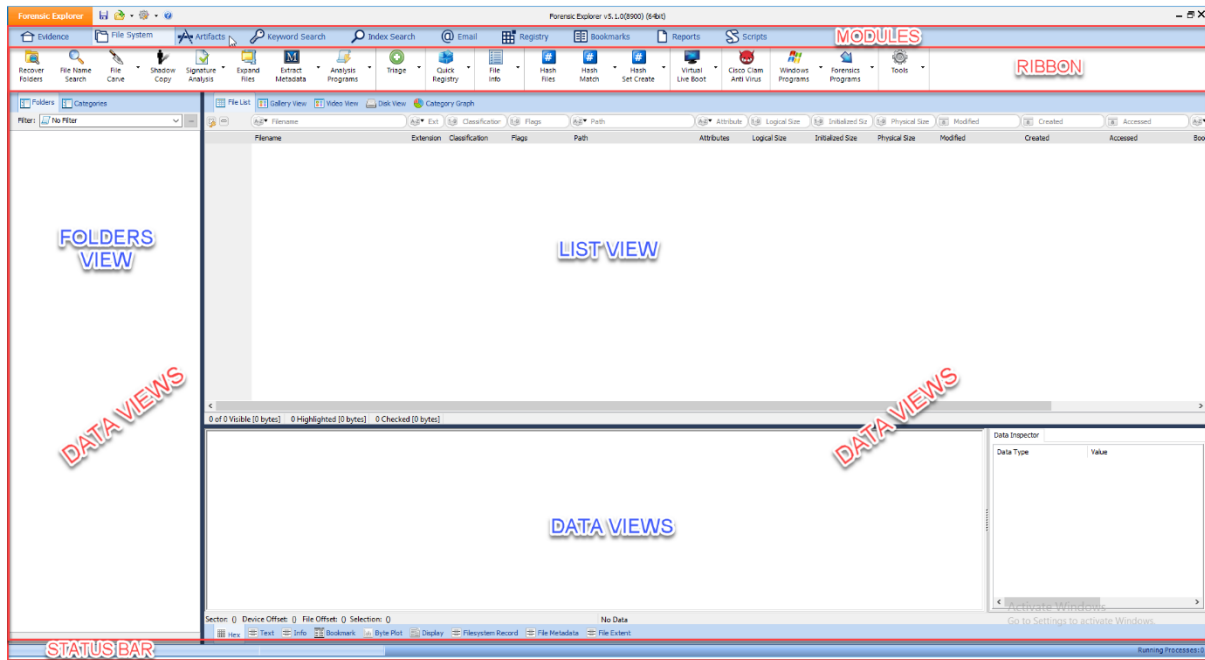
Figure 51: Re-dock a module tab



7.2 MODULE DATA VIEWS

Within each module are one or more “**data views**” which display the data in the case. Data views occupy the three lower panes of the Forensic Explorer module. They operate in a similar fashion to the layout to Microsoft’s Windows Explorer, with a tree (top left), list (top right) and display (bottom) window, as show in Figure 52 below:


Figure 52: 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”**.

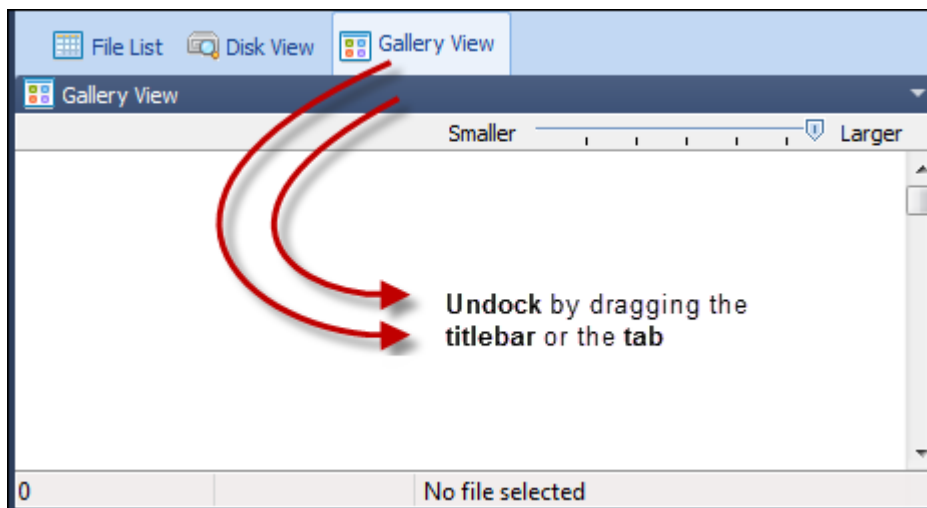
7.2.1 UNDOCKING AND DOCKING DATA VIEWS

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 53 below:

Figure 53: Undocking a view using drag and drop

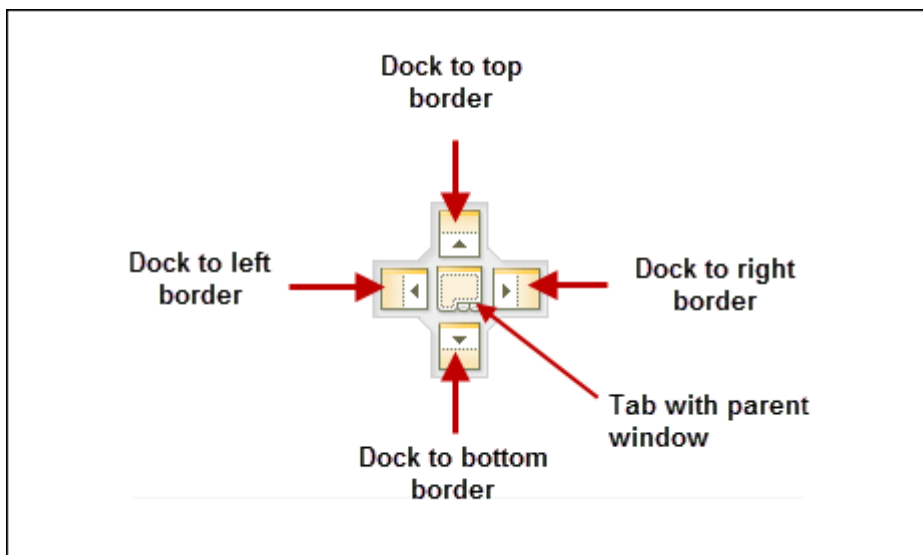


To **dock a data view**:

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 54 below:

Figure 54: Dock positioning arrows



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



7.3 CUSTOMIZING LAYOUTS

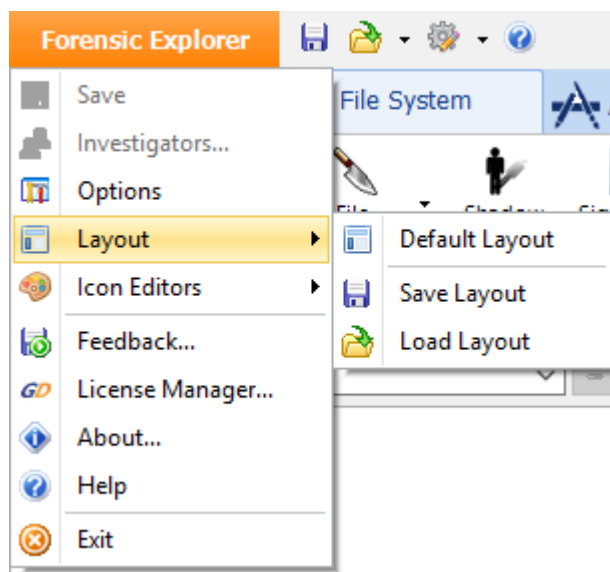
The **position** of modules and data views can be **saved to a file** at any time. This allows the investigator to customize a module for different types of investigations. For example, the module layout for an investigation involving graphics may be different to fraud investigations involving documents.

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 55 below:

Figure 55: Accessing the Layout Options



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 55.
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 55.

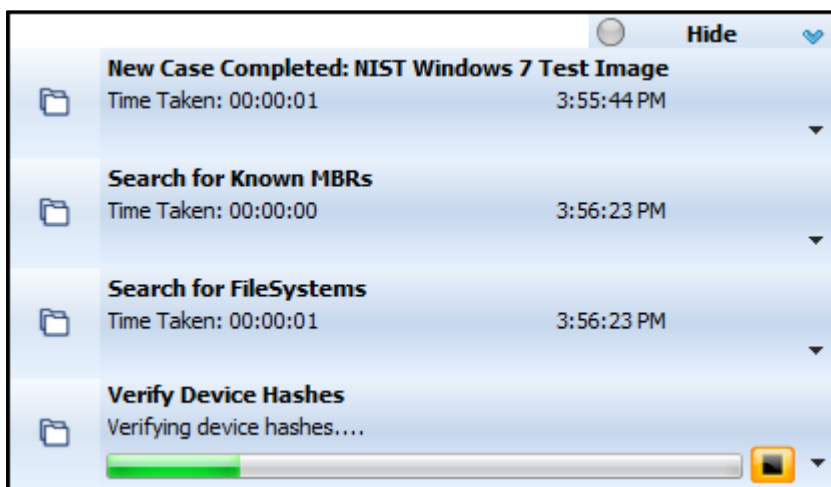
7.4 TASK PROCESSES LIST

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:

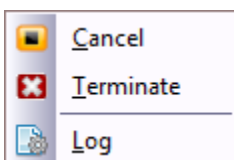
Figure 56: Forensic Explorer processes window



The purpose of the list is to:

- **Visually show** the progress of running processes.
- **Identify processes which have completed**, their duration and the time completed.
- **Cancel** the 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 57: 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 58 below:

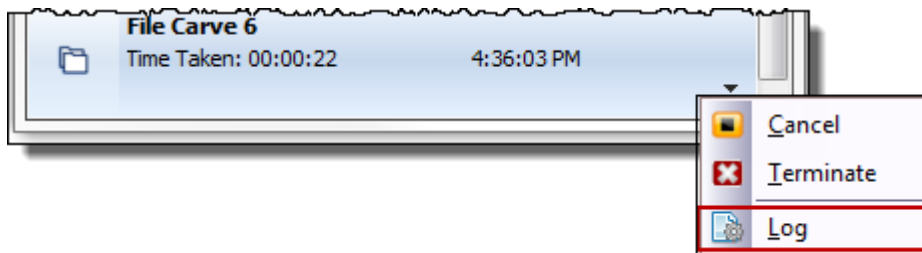
Figure 58: Setting Logging and Priority options



7.5.1 LOGGING

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

Figure 59: Access Process Log Files



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

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

7.5.2 PRIORITY

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

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

Priority settings are:

- **Minimum** 1 thread.
- **Normal** 0.5 times the number of processors
- **High** 1.0 times the number of processors (-1 to stop overload)
- **Maximum** 2.0 times the number of processors in Maximum priority - 2 (2 to stop overload)

7.6 REFERENCE LIBRARY

The purpose of the Reference Library is to put personal reference resources within easy reach of the investigator from Forensic Explorer interface.

In Forensic Explorer v5.4.8.2587 and above the Reference Library is uses a third-party application called Zotero, <https://www.zotero.org>. Zotero is:

- Free.
- Imports from other reference managers.
- Single click extensions are available for most browsers.
- Works on-line or off-line.

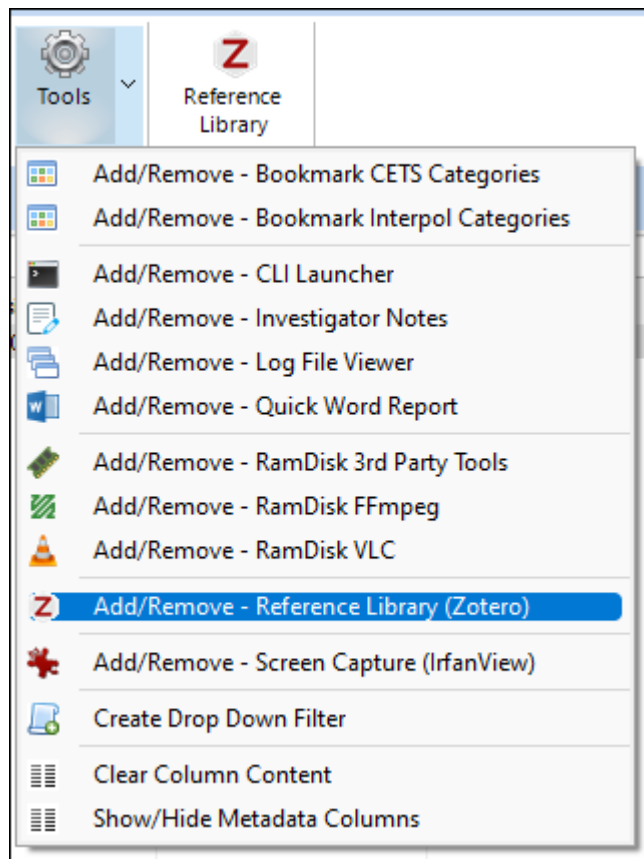
7.6.1 TO INSTALL ZOTERO

Download Zotero from <https://www.zotero.org> and follow the on-screen default installation steps.

To Add a Zotero toolbar button to Forensic Explorer:

1. In the **File System** module, select **Tools > Add/Remove – Reference Library (Zotero)**.

Figure 60: Add Reference Library Zotero button



2. Select the modules to add the Zotero toolbar button.

7.6.2 IMPORTING ZOTERO REFERENCE INFORMATION

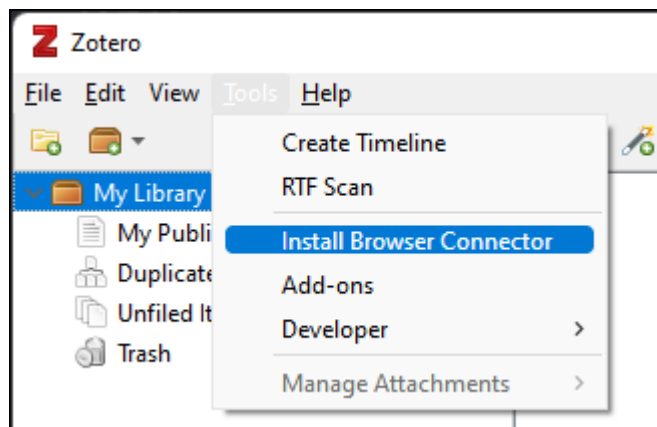
BROWSER CONNECTOR

References can be added directly to Zotero whilst web browsing using a **browser connector**. To install a browser connector:

In Zotero

1. Select Tools > Install Browser Connector > Install

Figure 61: Zotero Browser Connector



IMPORTING REFERENCES

It is possible to import existing references to Zotero from other reference managers.

A default set of references is provided with Forensic Explorer. The import file is located in:

... \Documents\Forensic Explorer v5\Reference Library\FEX References.rdf

To import default Forensic Explorer references:

1. In Zotero, select **File > Import** and navigate to the above **FEX References.rdf** file.
2. Selecting the option to **Place imported collections into a new collection** will create a **new collection folder** for the import (see Figure 63 below). This enables the Forensic Explorer user to manage different reference collections.

Figure 62: Import reference collection to Zotero

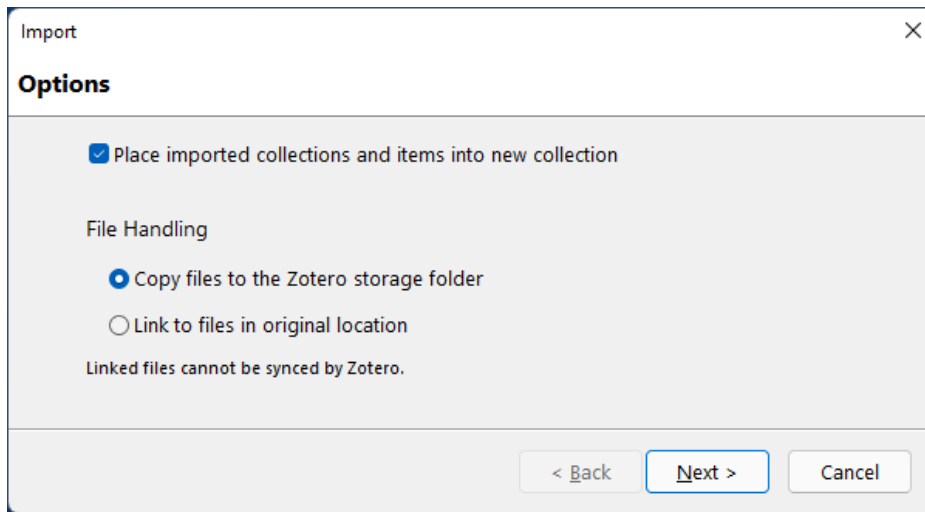
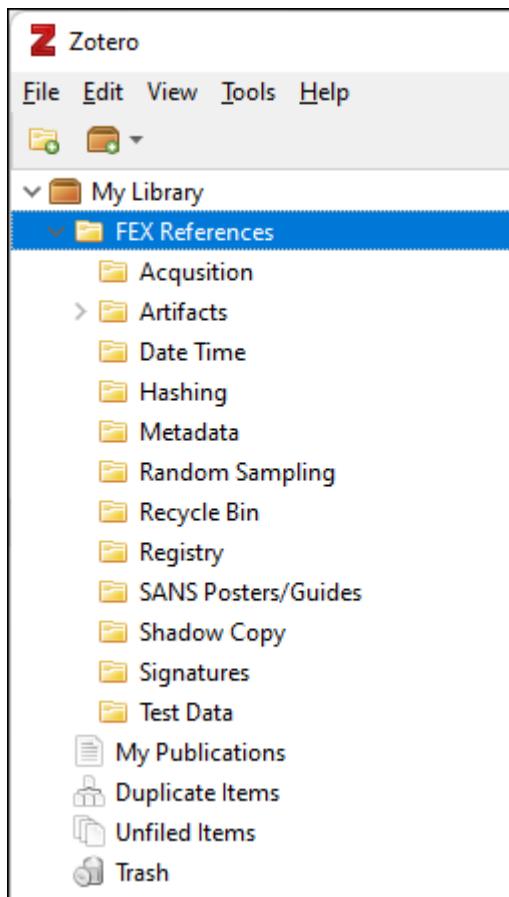


Figure 63: Creating a new Zotero collection folder



For additional information on using Zotero visit: <https://www.zotero.org/support>.

Chapter 8 - Data Views

In This Chapter


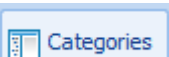
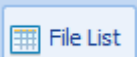

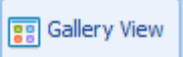
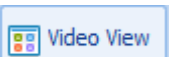

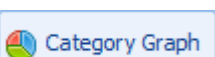
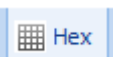
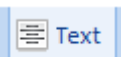
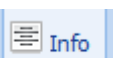


CHAPTER 8 - DATA VIEWS

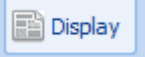
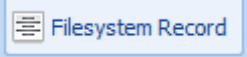

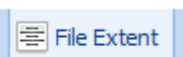
8.1	Data views summary.....	83
8.1.1	Components of a data view	84
8.1.2	Data views relationships in the File System module.....	84
8.2	Tree view	86
8.2.1	Navigating Tree view.....	86
8.2.2	Tree view filter	87
8.2.3	Branch plate	88
8.3	List view	89
8.4	Disk view	89
8.4.1	Resizing the Disk view display	90
8.4.2	Color Coded Content.....	90
8.4.3	Navigating Disk view	92
8.4.4	Add Partition	94
8.4.5	Selecting data in Disk view.....	96
8.5	Gallery view	97
8.5.1	Display View – HEIC, HEIV	98
8.5.2	Gallery View Folder Level Filtering.....	98
8.5.3	Gallery View – File Level Filtering/Sorting	99
8.5.4	Caching thumbnails to disk	100
8.5.5	Increase the number of graphics displayed	101
8.5.6	Working with data in Gallery view	101

8.5.7	Blur	101
8.5.8	Classification Keys [0-9, -] (Hotkeys)	102
8.5.9	Gallery Classification File Index	104
8.5.10	Classification and Bookmark using hotKeys [0-9, -]	104
8.5.11	Custom Classification Type	106
8.6	Category Graph	108
8.7	Hex view	108
8.8	Text view	109
8.9	Info	110
8.10	Display view	110
8.10.1	Display View – HEIC, HEIV	112
8.10.2	Video View and Thumbnails	112
8.11	Byte Plot and Character Distribution	113
8.11.1	Byte Plot examples	114
8.12	Filesystem Record view	117
8.13	File Metadata	118
8.13.1	Extract Metadata	120
8.13.2	XMP Metadata	124
8.13.3	File Info	125
8.14	File Extent	126

8.1 DATA VIEWS SUMMARY

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

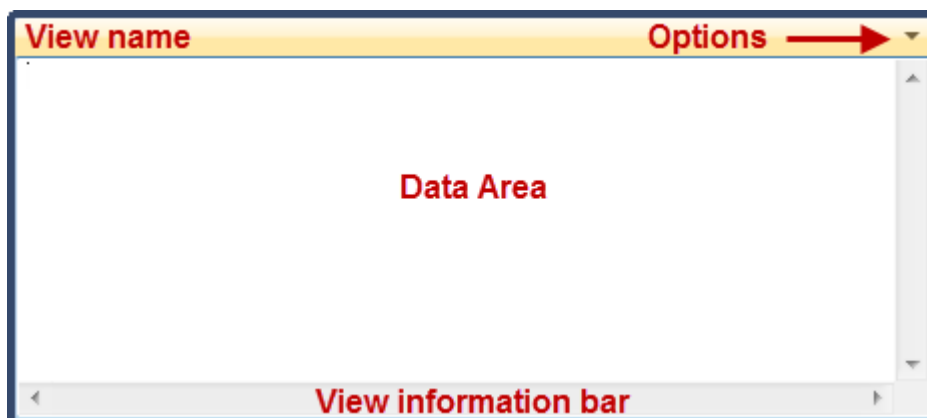
Data View Tabs	Function
 Folders	Shows the folder structure of the examined device.
 Categories	Separates items into categories, including files by extension, files by modified date and flagged files.
 File List	Lists individual items and displays their metadata in columns.
 Disk View	A graphical display of the sectors which make up the examined device.
 Gallery View	A thumbnail presentation of the graphics files.
 Video View	Shows time segment video thumbnails and individual video playback.
 Disk View	A graphical display of the sectors which make up the examined device.
 Category Graph	A graphical display items in "Categories".
 Hex	Hexadecimal view of the currently highlighted item. Automatic interpretation of user selected data.
 Text	Text view of the currently highlighted file.
 Info	Property item information, value and type.
 Bookmark	Shows the bookmark details associated with the item.
 Byte Plot	A graphical representation of byte level data within the currently highlighted file.

 Display	Content display of currently highlighted file. Displays of 300 + different file types including video and audio.
 Filesystem Record	Displays information contained in the MFT record or FAT entry for the currently highlighted file.
 File Metadata	A breakdown of files metadata components.
 File Extent	Details the start, end and length of each data run on the disk.

These views are described in more detail below.

8.1.1 COMPONENTS OF A DATA VIEW

Figure 64: 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:

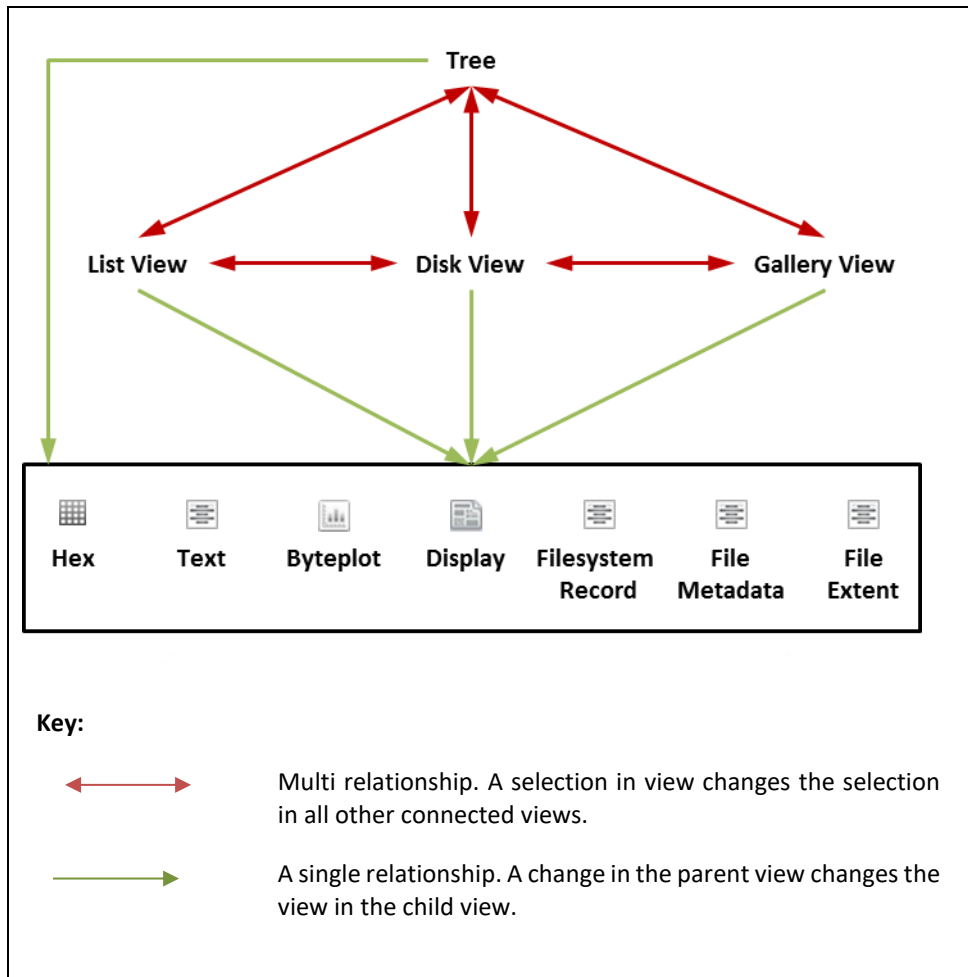
- The full path to the currently highlighted item.
- The currently selected physical sector.

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 65: Relationships between data views



8.2 TREE VIEW

A Tree view is a hierarchical display of items (e.g., devices, partitions, folders, registry key folders, keywords etc.). Like Microsoft's Windows Explorer, the Tree view is most 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.:

Module	Tree view Name	More Information
File System	Folders	Chapter 11
Keyword Search	Keyword Tree	Chapter 13
Bookmarks	Bookmark Tree	Chapter 17
Registry	Registry Tree	Chapter 16

8.2.1 NAVIGATING TREE VIEW

To **navigate** Tree view:



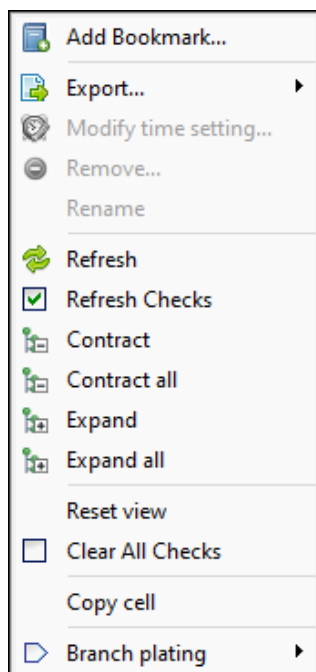
- Use the **keyboard arrow keys** to traverse, expand and contract the tree.
- **Double click a Folder** to drill down into its sub folders; or
- **Click the  and  symbols** to expand and contract the tree hierarchy; or
- **Right click options:**

Figure 66: File System, Folders – right-click options.

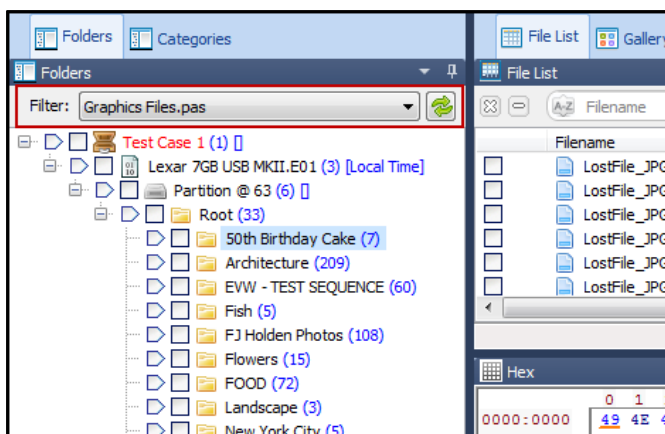


Add Bookmark:	Bookmarks the current highlighted item (folder).
Export:	Options to export the item/s from the tree.
Modify time setting:	Modify evidence time settings during a case.
Remove:	Remove user added items (expand, carve, etc.).
Refresh:	Refresh the current view.
Refresh Checks:	Refresh the checkmarks.
Expand:	Expand the currently highlighted folder.
Expand All:	Expand all folders.
Contract:	Contract the current branch.
Contract All:	Contract all branches.
Reset view:	Remove: branch plate, checks, folders filter, and contracts all.
Clear All Checks:	Removes all checks (checked items count will be zero).
Copy Cell:	Copies the text of the currently highlighted item.
Branch plating:	Turns branch plating on or off (off makes the tree like Windows Explorer).

8.2.2 TREE VIEW FILTER

Some Tree views contain a filter drop-down menu, as shown in Figure 67:

Figure 67: Tree view filter





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

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

8.2.3 BRANCH PLATE

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

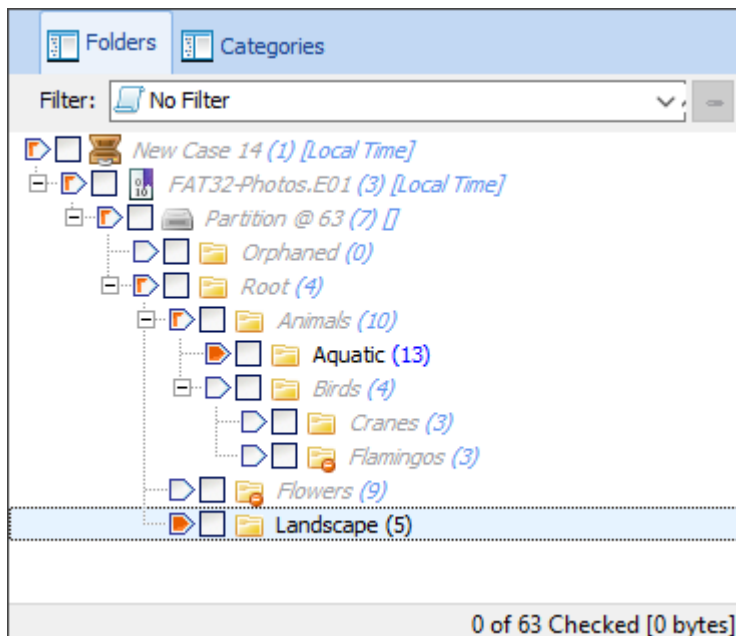
To **branch plate**, click the required plate with the mouse.

- When the plate turns orange,  it is active.
- A semi-filled branch plate,  indicates that a sub-folder of that branch has been plated.

To **plate multiple branches**:

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

Figure 68: File System module, Folder’s view, branch plate with “Aquatic” and “Landscape” folders plated



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

The blue number in brackets, e.g. (13) 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.:

Module	List View Name	More Information
File System	File List	Chapter 11
Keyword Search	Keyword Result List	Chapter 12
Bookmarks	Bookmarks List	Chapter 17
Registry	Registry List	Chapter 16

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 69: Disk View tab



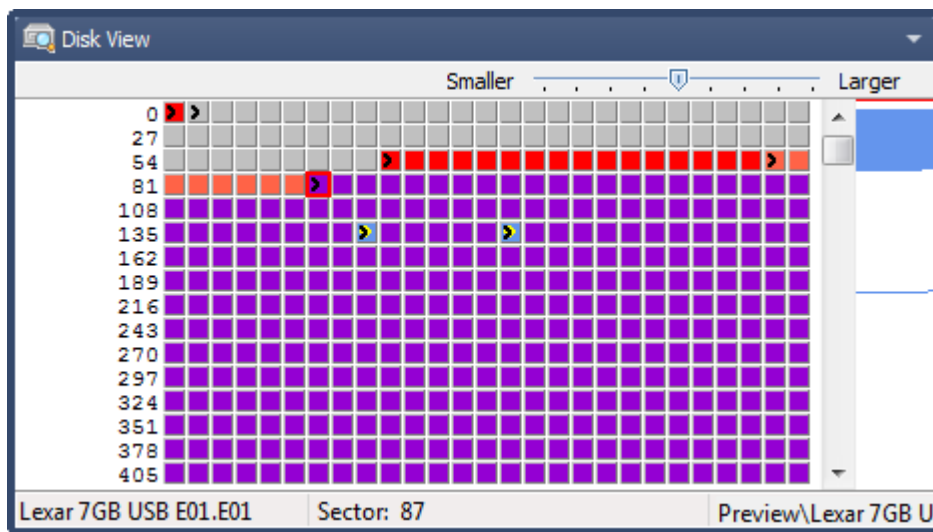
Disk view is a graphical display of the sectors which make up the examined device. Disk view can be used to:

- 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 70: Disk view



8.4.1 RESIZING THE DISK VIEW DISPLAY

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

Figure 71: Disk view scale bar









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

8.4.2 COLOR CODED CONTENT

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

- > The start sector of a file
 - Currently selected sector
 - ☀ One type overlay another
-
- ▣ MBR/VBR (Red)
 - ▣ FAT 1 (DarkViolet)
 - ▣ FAT 2 (WebViolet)
 - ▣ \$MFT (DarkViolet)
 - ▣ System files (WebTomato)

-  \$MFT resident file (the file overlays the \$MFT)
-  Folder (Deepskyblue)
-  Allocated File (CornFlowerBlue)
-  Unallocated space (LtGray)
-  Deleted file (A deleted file overlays unallocated space)
-  Carved file (DarkOrange: Carved file overlays unallocated space)

CUSTOM DISK VIEW COLORS

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

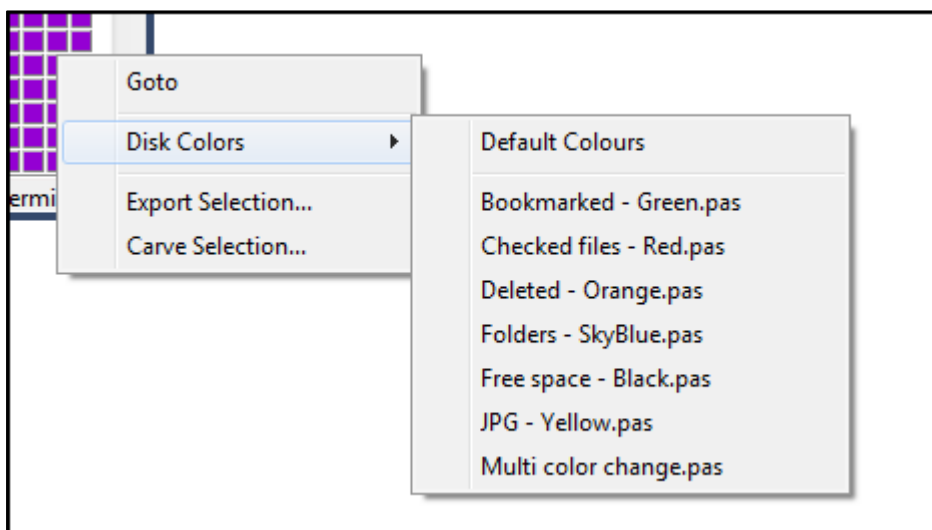
- show a file type, e.g., JPGs as a specific color; or
- change the color of a file type over a certain size to a specific color; or
- show a specific file, e.g., “sample.txt” as a specific color.

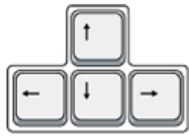
Custom Disk view colors are defined using Forensic Explorer scripts located in the “Scripts > Disk View” folder. (Learn more about scripting in Chapter 19 - Scripts Module).

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 72: Right-click Disk View menu links to scripts





Navigate sectors using the **arrow keys**

To reset Disk view colors to default.

Right click in the Disk view window.



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

Select **Disk Colors > Default Colors**.



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
P	Previous file
Ctrl P	Previous different type
S	System
U	Unallocated

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 78 below) is a map to allocated space on the examined device. Use the vertical scroll bar to quickly navigate to the colored section which identifies allocated disk space.

KEYBOARD NAVIGATION

The following commands are available for navigation in Disk view:

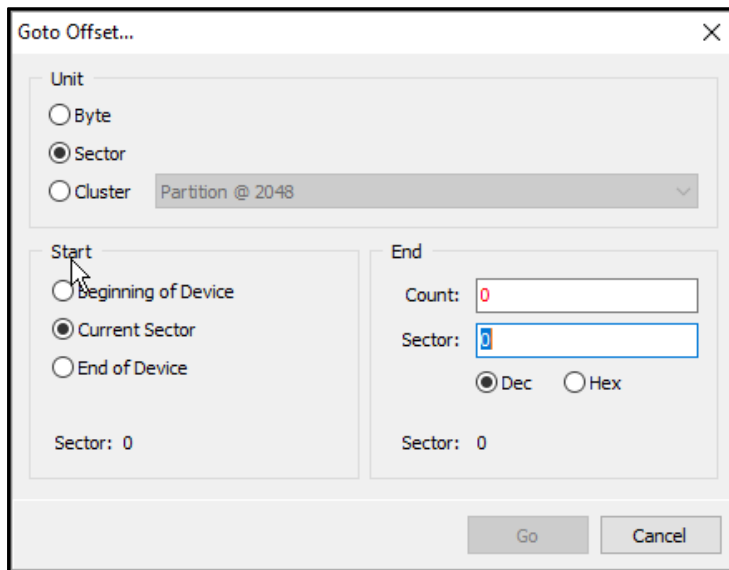
DISK VIEW GOTO

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

To open and use the Goto Offset window:

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

Figure 73: Disk view Goto Offset window

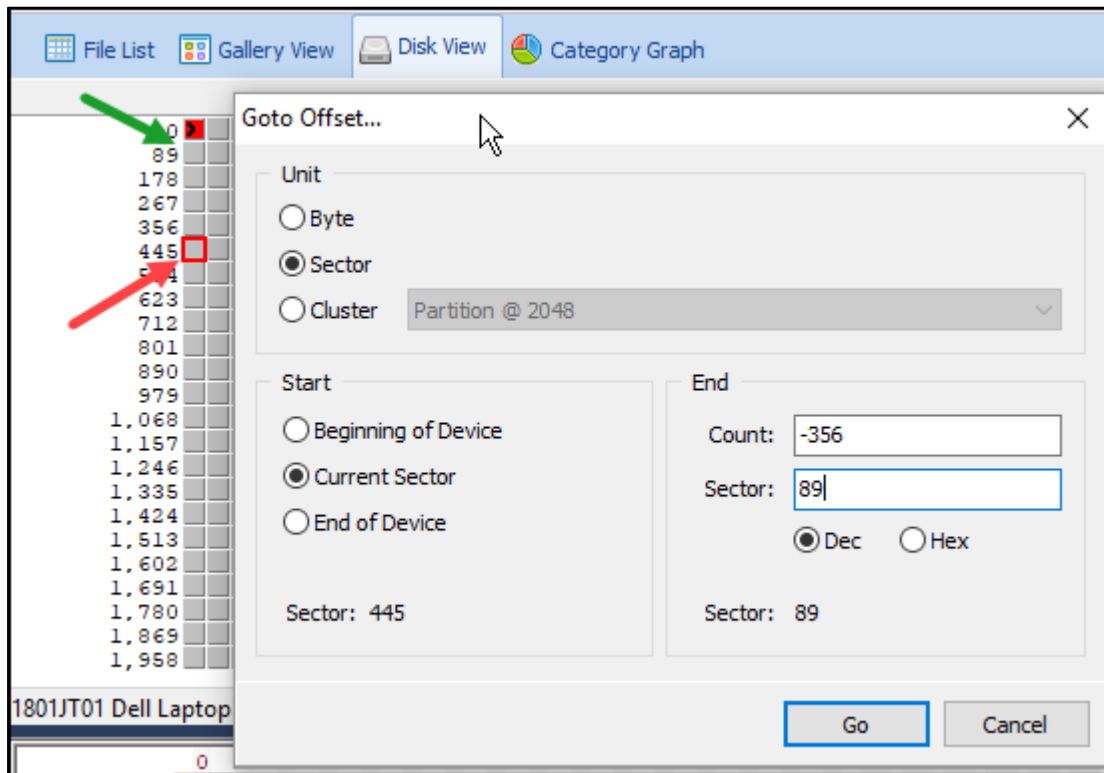


- Select the **Unit** required, Byte, Sector or Cluster
- Select the **Start** position on the disk:
 - Beginning of Device (i.e., go forwards from the first sector)
 - Current Sector
 - End of Device (i.e., go backwards from the last sector)
- Enter the **End** position. This can be entered either as a **Count** of the unit required (byte, sector cluster), or a disk **Sector**.

GOTO Example, Figure 74 below:

- The **currently selected sector** is 445.
- The **sector to GOTO** is 89, which is -356 from the currently selected sector.

Figure 74: GOTO Example



8.4.4 ADD PARTITION

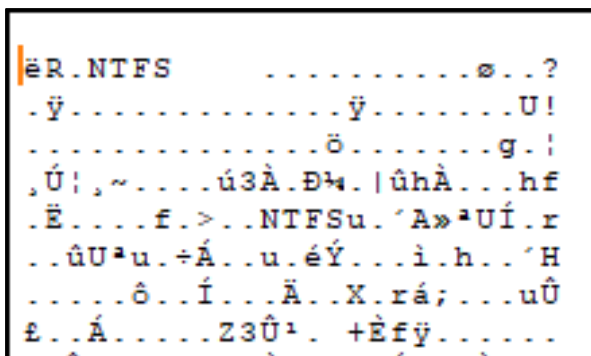
It is possible in Forensic Explorer to add an unallocated partition (for example, when a drive has been formatted but the unallocated partition structure is still intact).

To Add Partition:

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

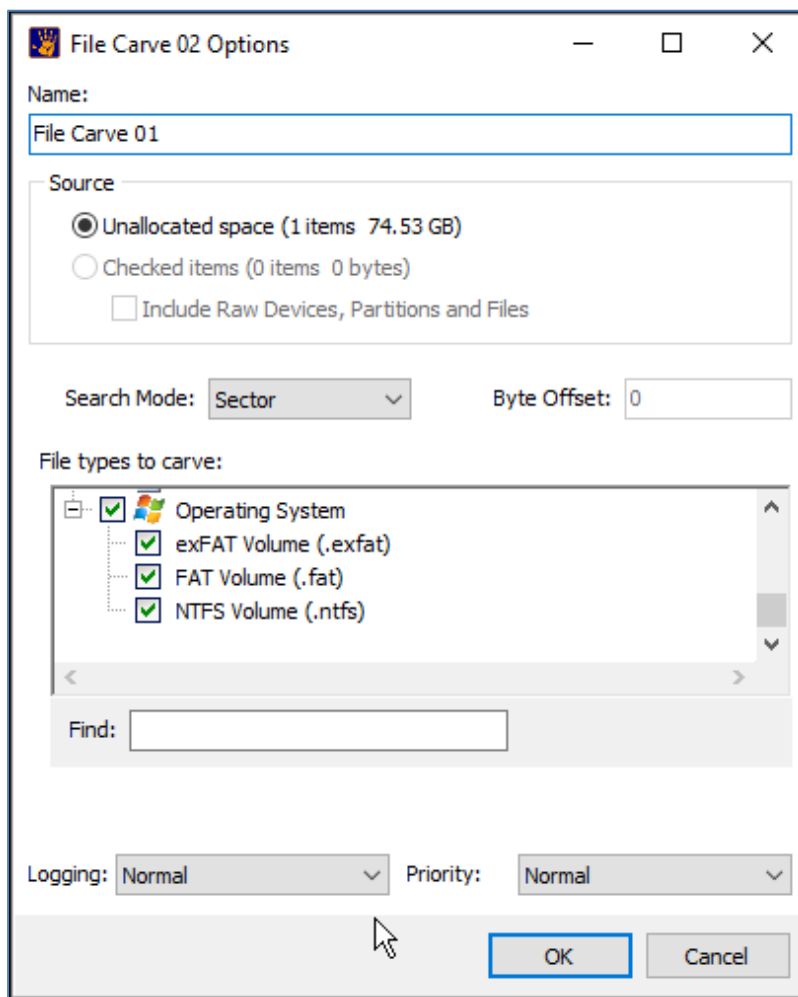
Manually: Users who are familiar with the VBR format and disk position may use Disk View to find the sector manually.

Figure 75: 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 76 below:

Figure 76: File Carve for Volume Boot Record (VBR)



The file carve will return the position of found VBRs with the file name representing the sector number on the device:

Figure 77: File Carve results for Operating System Volumes

	Filename	Extension
<input type="checkbox"/>	1 Carved_NTFS_2048.ntfs	ntfs
<input type="checkbox"/>	2 Carved_NTFS_2384.ntfs	ntfs
<input checked="" type="checkbox"/>	3 Carved_NTFS_206847.ntfs	ntfs
<input type="checkbox"/>	4 Carved_NTFS_206848.ntfs	ntfs
<input type="checkbox"/>	5 Carved_FAT_538667.fat	fat
<input type="checkbox"/>	6 Carved_FAT_538668.fat	fat

- 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

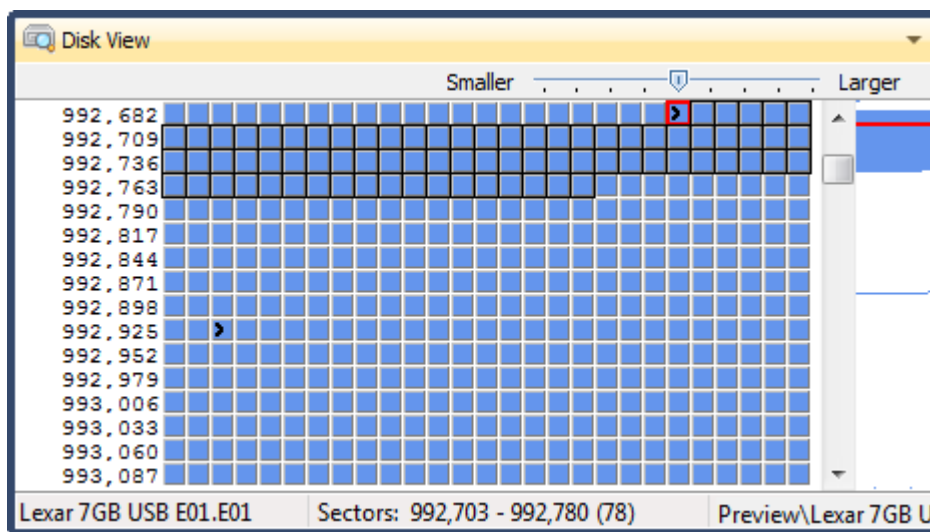
To select a **sector**:

- 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 78 below. This enables other views, such as HEX View, to see the selected range.

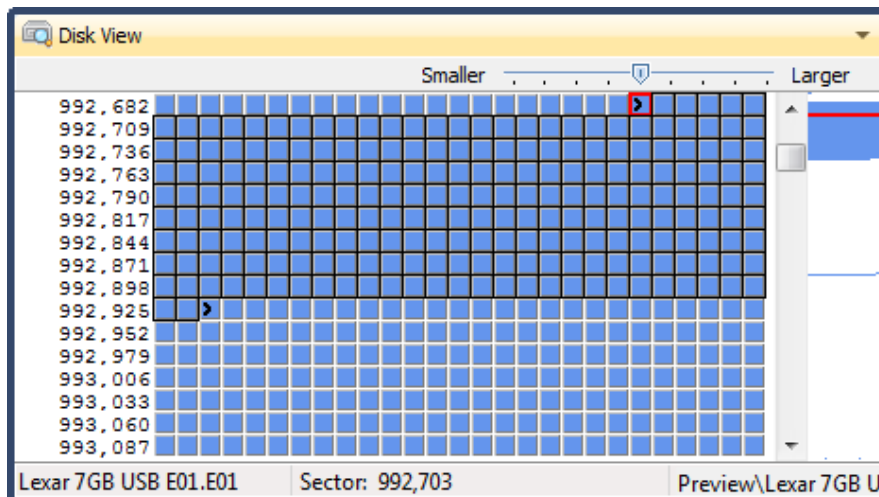
Figure 78: Selecting a range of sector in Disk view



To select a **file**:

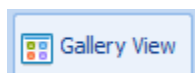
- Double click on a sector. All sectors used by the file will be identified.
- The name of the selected file is displayed in the status bar at the bottom of the Disk view window, as shown in Figure 79 below.

Figure 79: A selected file in Disk view



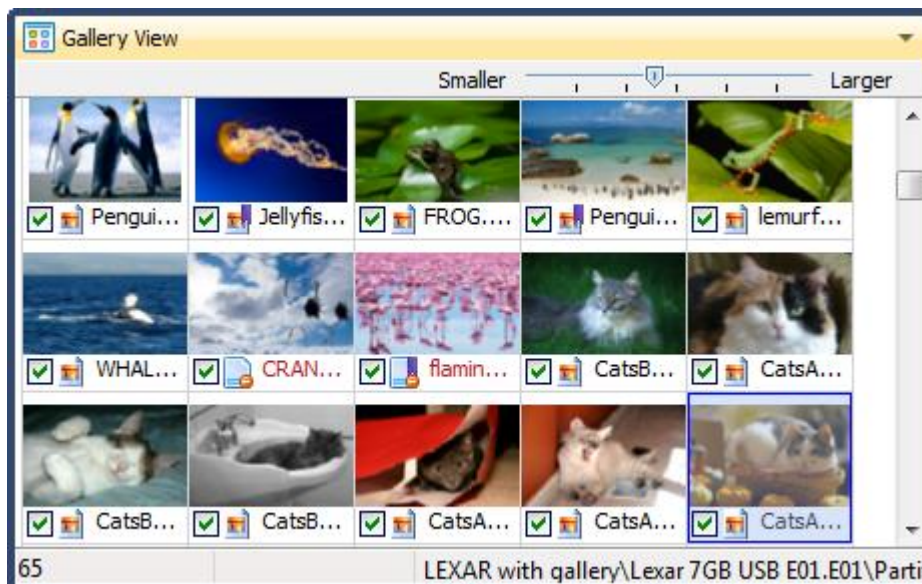
8.5 GALLERY VIEW

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



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

Figure 80: 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 DISPLAY VIEW – HEIC, HEIV

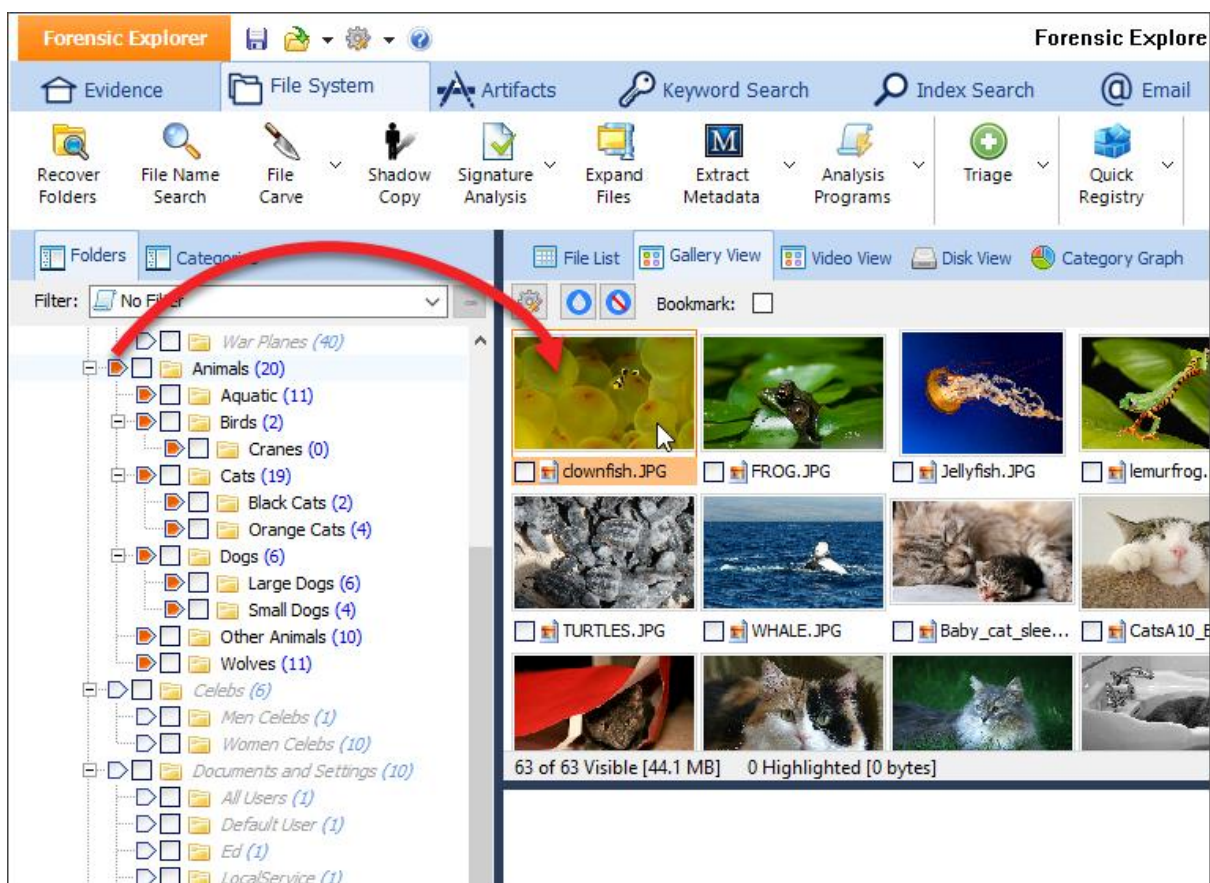
To preview HEIC or HEIV files in the Forensic Explorer Gallery View or Display View the following Microsoft extensions must be installed on the forensic workstation:

- High Efficiency Image File Format (HEIC): Microsoft Image Extensions, <https://apps.microsoft.com/store/detail/heif-image-extensions/9PMMSR1CGPWG?hl=en-us&gl=US>
- High Efficiency Video Coding (HEVC): Microsoft Extensions Package, <https://apps.microsoft.com/store/detail/hevc-video-extensions/9NMZLZ57R3T7?hl=en-us&gl=US>
- Or a non-Microsoft equivalent such as: <https://www.copytrans.net/copytransheic/>

8.5.2 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 81 below.

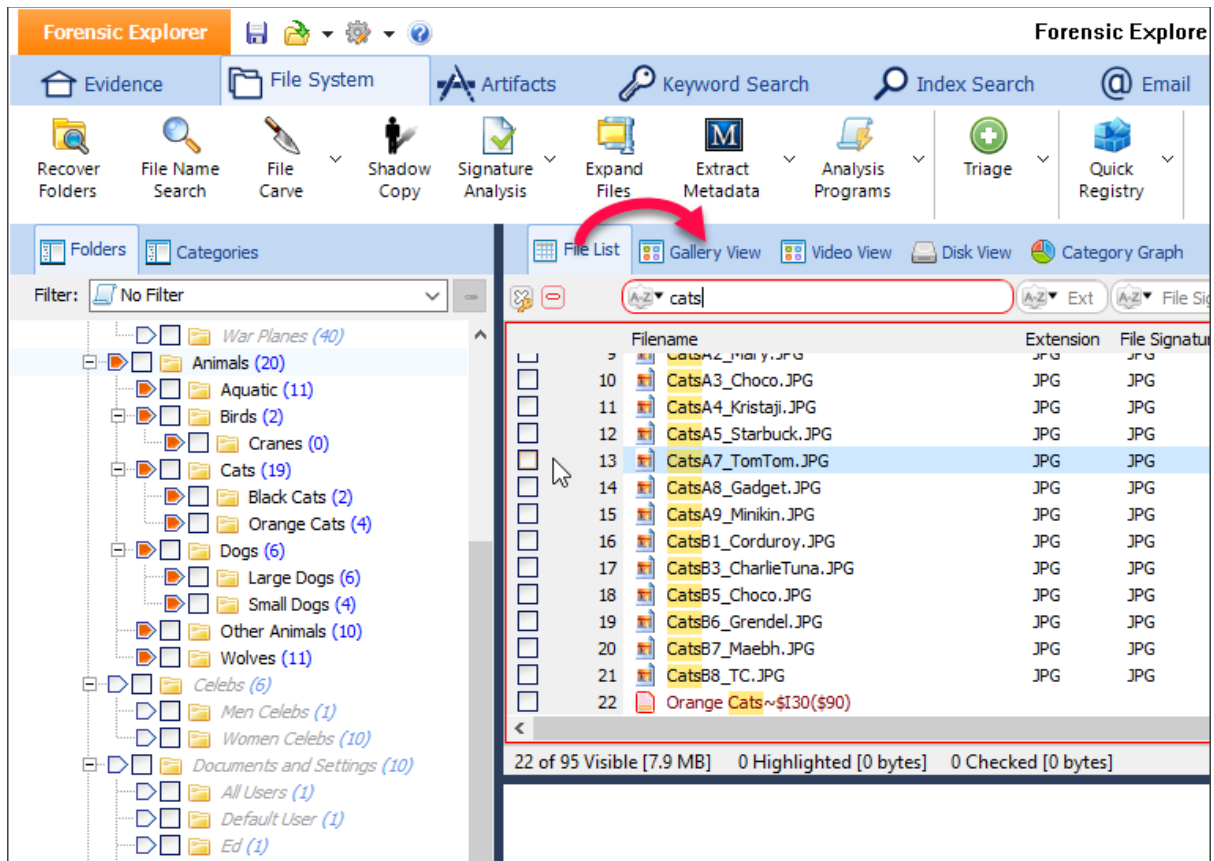
Figure 81: Gallery view as determined by a folder/branch-plate selection



8.5.3 GALLERY VIEW – FILE LEVEL FILTERING/SORTING

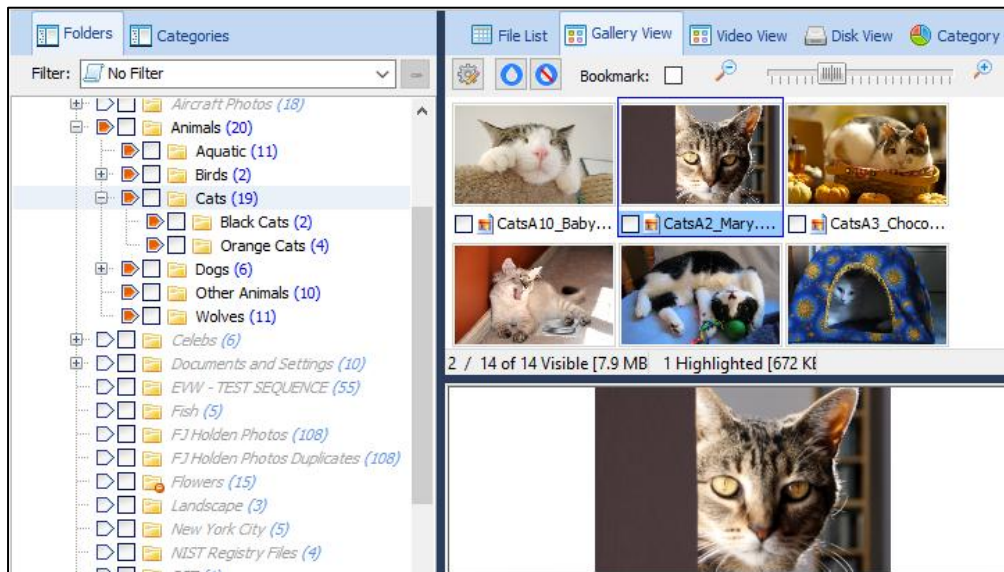
In addition to Folder level filtering described above, the content and sort of Gallery view can also be determined by filters and sorting in the **File List**. For example, in Figure 82 below, the File List has had a **Text Typing filter** applied for the word “Cat” which filters out only files containing that word in the file name:

Figure 82: 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 83 below where the Gallery view contains only graphics that match the filter:

Figure 83: Gallery view with a File List filter applied



TIP: To see File List filters and their effect more clearly 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.

8.5.4 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:

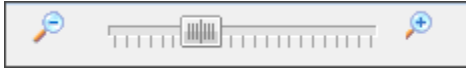
1. When adding evidence:
 - a. When an evidence item is added to a preview or a case, there is an opportunity in the Evidence Processor window (see 10.5) to “Cache Thumbnails”.
2. During a case:
 - a. Select or branch plate the required folders in the File System module.
 - b. Right click in the gallery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

The cache progress will show in the processes window.

8.5.5 INCREASE THE NUMBER OF GRAPHICS DISPLAYED

The size and number of graphics displayed is controlled by moving the slide-bar or by clicking the – or + button graphics.

Figure 84: 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).

8.5.6 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**.

8.5.7 BLUR

Gallery view blur enables the investigator to blur the content of a graphic 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.

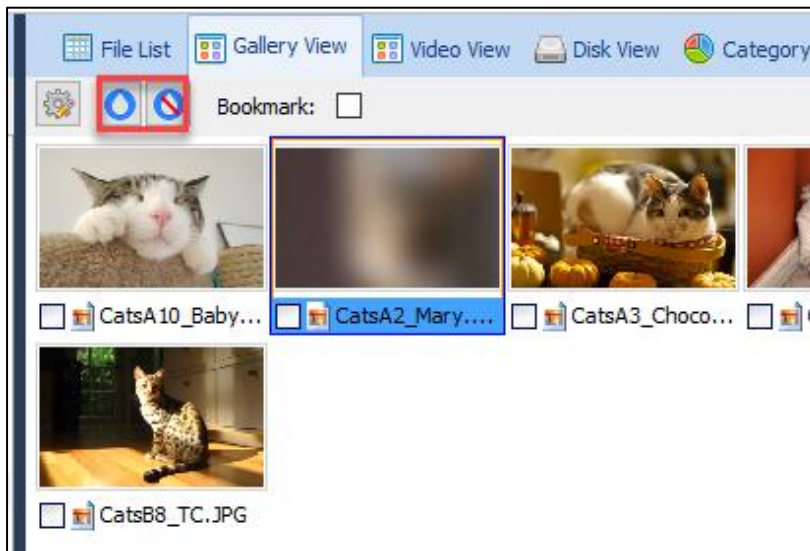
To **blur a graphic**:

1. In the **File System module Gallery view**, use the mouse to select the required picture in the Gallery view (or use the CTRL, 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 85 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 85: Gallery view blur



Blur can also be associated with keyboard hotkeys.

8.5.8 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** right-click and select **Classify > Enable Classification**. A classification legend will also appear to the right of the Gallery view graphics (see Figure 88 below).

Figure 86: Enable classification

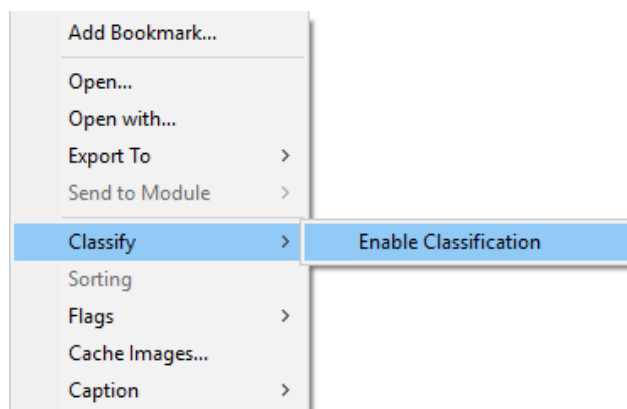
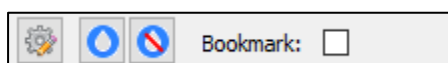


Figure 87: Gallery view toolbar options



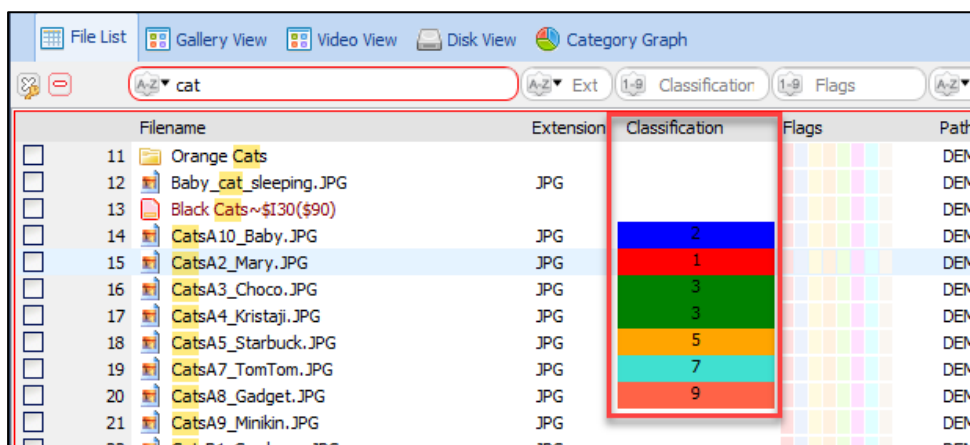
2. Pressing a keyboard key from 0 to 9 will classify the currently graphic item selected according to the keyboard number pressed. (- removes the classification, see below).
3. Visual confirmation of the classification is provided:
 - a. In the **bottom right-hand corner** of the **information bar** 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 88: Gallery View classification



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

Figure 89: File List Classification column



To **remove classification** from a graphic in **Gallery View**:

1. Select the graphic/s with the mouse.
2. **Press the – (minus) button** on the keyboard.
3. The classification number is removed.

To remove classification from a **group of classified files**:

1. Use the **SHIFT** or **CTRL** key to select a group 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 (File List view), click on the Tools button > Clear Column Content > select Classification > Run, or right-click on the column header and select Clear Column from the menu.
2. Classification will be removed from all items.

8.5.9 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 90 below:

Figure 90: Classification with index numbering



8.5.10 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**.

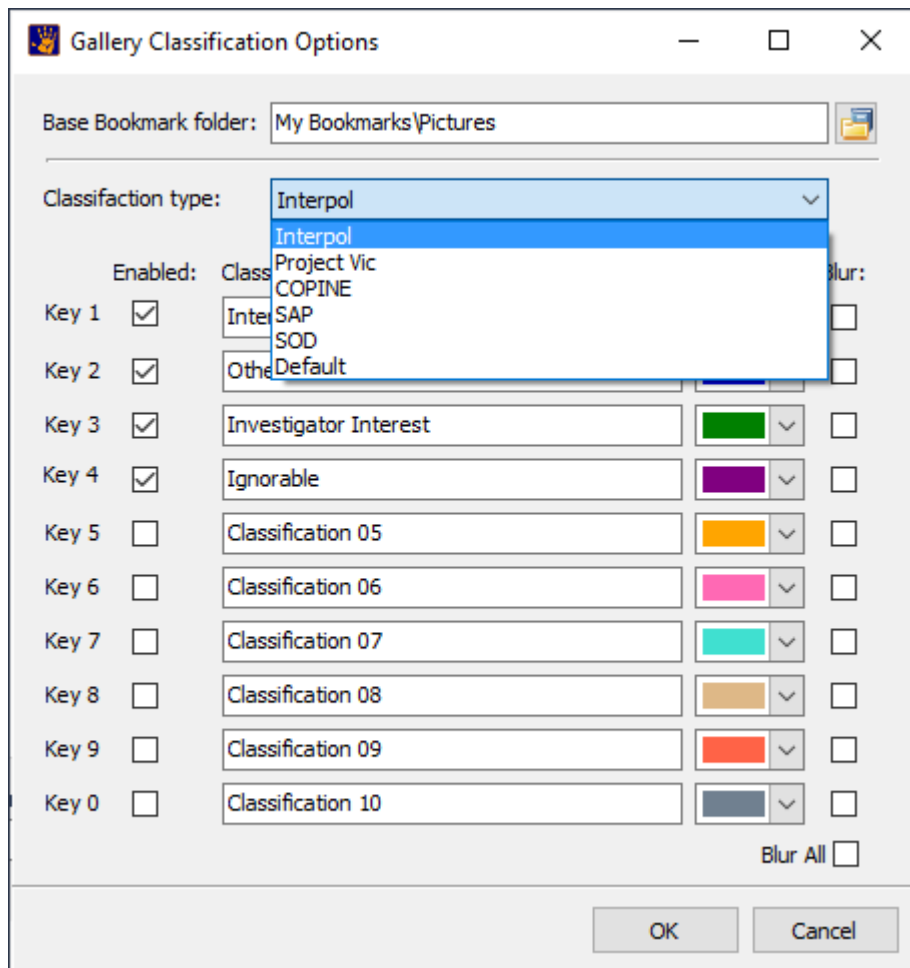
To **hotkey classify then bookmark** a file from **Gallery view**:

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

4. Figure 87 above).

Figure 91: Gallery Classification Options



Base Bookmark folder: Assigns the bookmark folder where items will be bookmarked.

Classification type: There are a number of different classification systems in use, including: Interpol Baseline; Project Vic; COPINE; SAP; and SOD.

In recent years Interpol Baseline has increased in popularity as it offers a simplified 4 category system. For an overview refer to: https://www.sentencingcouncil.qld.gov.au/_data/assets/pdf_file/0017/531503/cem-final-report-july-2017.pdf.

To create a custom classification type, refer to the following section.

Enabled:	The enabled checkbox makes the key active.
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 via Gallery Classification Options > use the drop-down color selection menu.

To re-classify then bookmark:

1. Check in the **Bookmark** checkbox 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 Figure 69) 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 on the Filename in Bookmarked Items List and select **Delete Bookmark\s** from the drop-down menu.

8.5.11 CUSTOM CLASSIFICATION TYPE

The **Default** classification system access from the **Classifications Options** window shown in Figure 91 above can be customise by creating and placing a **DefaultClassification.ini** file in the Forensic Explorer **Startup folder** (My Documents\Forensic Explorer vX\Startup\).

The text in Figure 92 below can be used to create the **DefaultClassification.ini** file. It sets the first 4 classification categories and associated color:

Figure 92: DefaultClassification.ini

```
[Classification 01]
Bookmark=CAM - Real Child Pre-Pubescent <13yo
Color=255
Blur=0
HotKeyEnabled=1

[Classification 02]
Bookmark=CAM - Other Illegal Content, Child <18yo
Color=26367
Blur=0
HotKeyEnabled=1

[Classification 03]
Bookmark=Investigative Interest
Color=65535
Blur=0
HotKeyEnabled=1

[Classification 04]
Bookmark=Ignorable
Color=32768
Blur=0
HotKeyEnabled=1

[Classification 05]
Bookmark=Classification 05
Color=42495
Blur=0
HotKeyEnabled=0

[Classification 06]
Bookmark=Classification 06
Color=11823615
Blur=0
HotKeyEnabled=0

[Classification 07]
Bookmark=Classification 07
Color=13688896
Blur=0
HotKeyEnabled=0

[Classification 08]
Bookmark=Classification 08
Color=8894686
Blur=0
HotKeyEnabled=0

[Classification 09]
Bookmark=Classification 09
Color=4678655
Blur=0
HotKeyEnabled=0

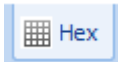
[Classification 10]
Bookmark=Classification 10
Color=9470064
Blur=0
HotKeyEnabled=0
```

8.6 CATEGORY GRAPH

This section is currently being updated.

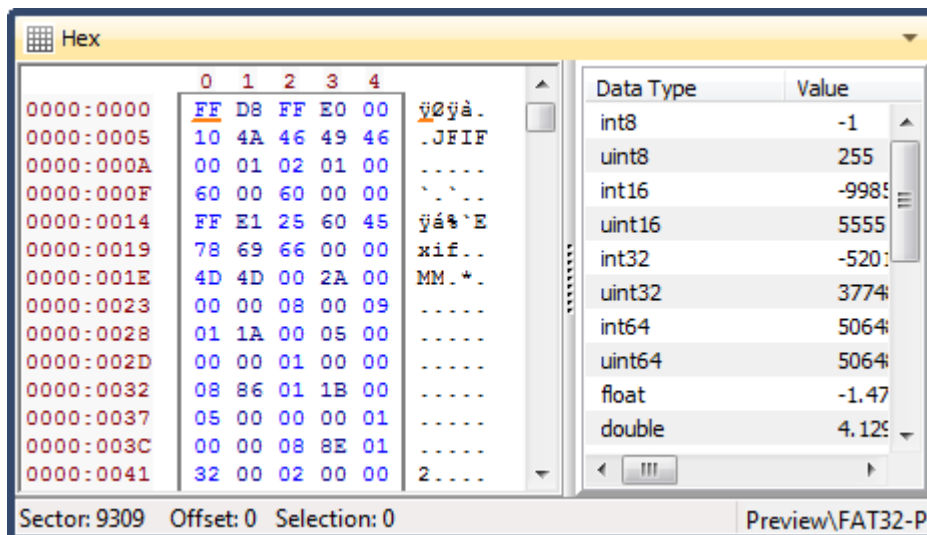
8.7 HEX VIEW

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



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

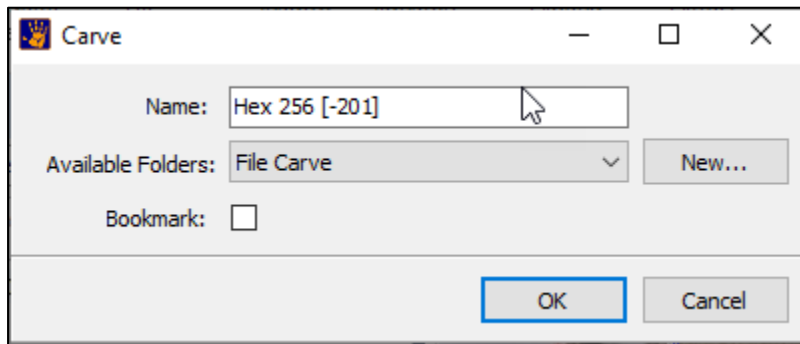
Figure 93: Hex view and data inspector



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

- **Add bookmark:** Highlight a selection of Hex and bookmark 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:

Figure 94: Carving files from Hex view



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

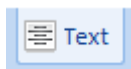
Available Folders: This is the folder name in File System Folders view which will hold the carved file. A new folder can be added as required.

Bookmark: Adds the carved file to the Bookmarks module.

8.8 TEXT VIEW

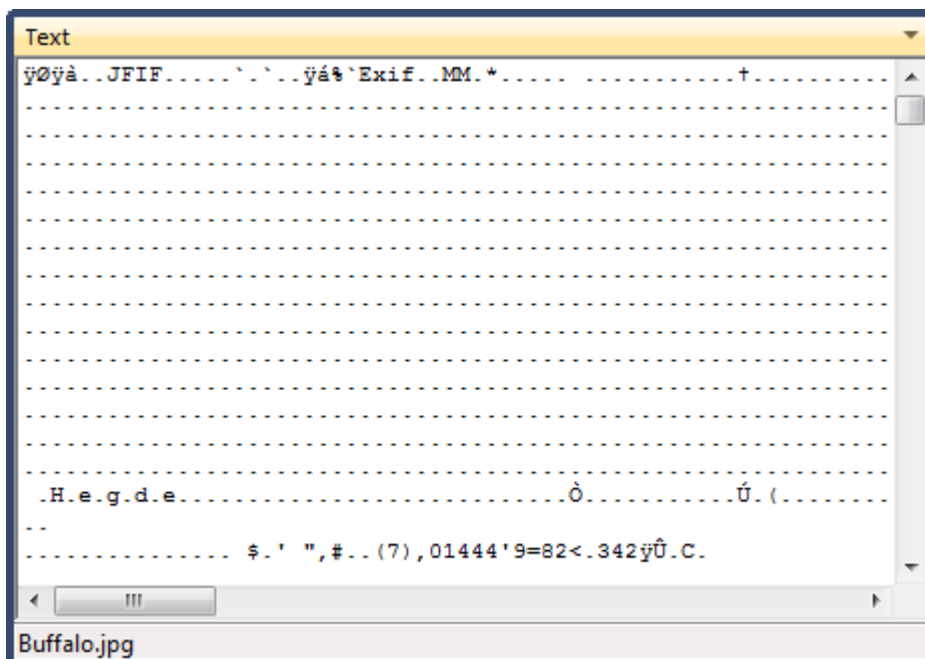
The default location for the Text view window is the bottom data view window, accessed via the Text tab:

Figure 95: Text view tab



The Text tab shows the highlighted item as ASCII text.

Figure 96: Text view



8.9 INFO

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

Figure 97: 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.

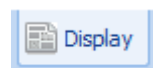
Figure 98: Info data view

Property	Value	Raw Value	Type
Item Information			
Accessed	28-Jan-14 11:21:36 AM	28-Jan-14 11:21:36 AM	Date
Attributes	---I-----a-----	---I-----a-----	UString
BIAS Time	0	0	Int64
Bates #	301,354	301354	Integer
Bookmark Folder			Binary
Bookmarked	False	False	Boolean
Byte Start	12,403,867,648	12403867648	Int64
Created	28-Jan-14 11:21:36 AM	28-Jan-14 11:21:36 AM	Date
Data Size	12,288	12288	Int64
Directory Level	14	14	Integer
Extension	jpg	jpg	UString
Extension Mismatch			Binary
File Category			Binary
File Signature			Binary
Filename	stor-9225_top_ten_1...	stor-9225_top_ten_14...	UString
Flags	0	0	Integer
HashSet			Binary
HashSet Category			Binary
HashSet Identified...			Binary
Intact Size	0	0	Int64
IsChecked	False	False	Boolean
IsCompressed	False	False	Boolean
IsDeleted	False	False	Boolean

8.10 DISPLAY VIEW

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

Figure 99: Display view tab



The File Display tab uses GetData's **Explorer View** technology to display the content of the currently highlighted file (see HEIC and HEIV below):

Figure 100: Display view

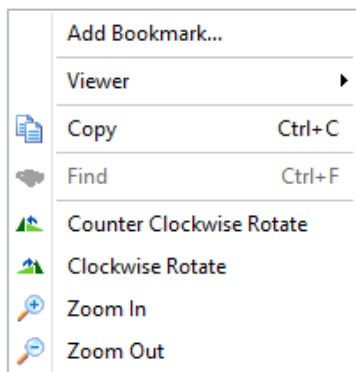


Note that the file Display tab is NOT intended as an exact render of how the file would have appeared to the end user. If this is the objective, it is best achieved by exporting the file and opening it with the same application available to the end user.

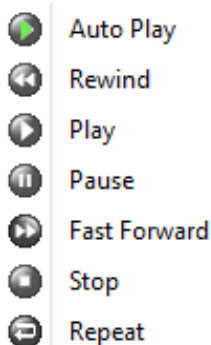
If a file type is selected where a display is not available, or the file is corrupt, an error message will display in this window. The display view will default to Hex or Text view.

Right click on the image to display the options menu:

Figure 101: Display view right-click menu



The following buttons are displayed for audio and video files.



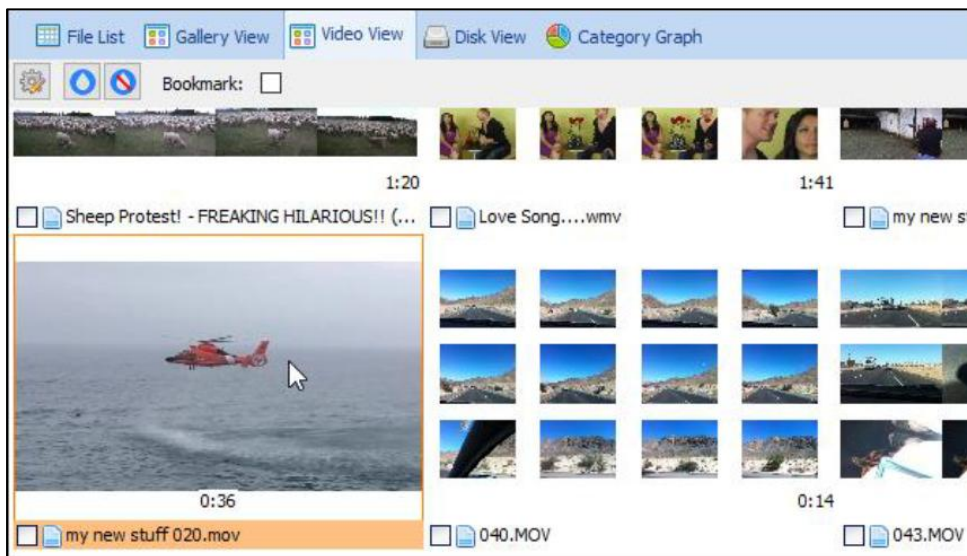
8.10.1 DISPLAY VIEW – HEIC, HEIV

To preview HEIC or HEIV files in the Forensic Explorer Gallery View or Display View the following Microsoft extensions must be installed on the forensic workstation:

- High Efficiency Image File Format (HEIC): Microsoft Image Extensions, <https://apps.microsoft.com/store/detail/heif-image-extensions/9PMMSR1CGPWG?hl=en-us&gl=US>
- High Efficiency Video Coding (HEVC): Microsoft Extensions Package, <https://apps.microsoft.com/store/detail/hevc-video-extensions/9NMZLZ57R3T7?hl=en-us&gl=US>
- Or a non-Microsoft equivalent such as: <https://www.copytrans.net/copytransheic/>

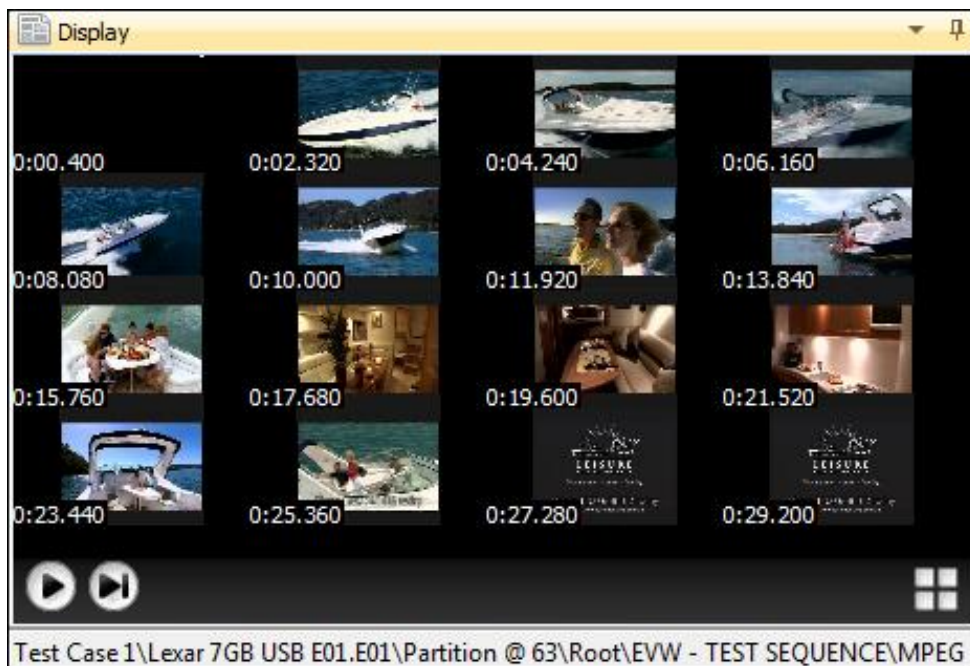
8.10.2 VIDEO VIEW AND THUMBNAILS

The Video view tab shows time segment video thumbnails. Individual videos can be played in this view by drawing the mouse across the thumbnail. The zoom slide bar has been increased to enhance viewing.



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 102 below:

Figure 102: 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.

8.11 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 103: 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”. (7 pp. S3-S12)

Byte Plot is emerging as a future means of file type analysis by binary content or “fileprint” (8).

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

Character Distribution

A character distribution bar graph is used in conjunction with Byte Plot and displays the distribution of ASCII characters 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> (9)). The extended ASCII character set comprises codes 0–256, where codes.

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

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

Color Coding

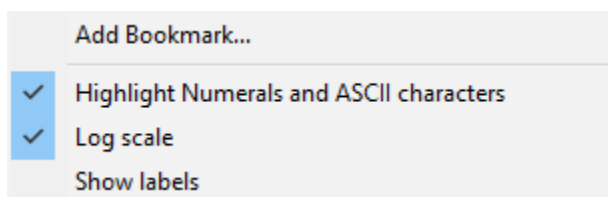
In the Byte Plot data view, ASCII characters are color coded, where:

- Blue** - Non-printable / extended characters
- Red** - Numbers (0 - 9)
- Yellow** - Text (**a to z** and **A to Z**)

Display Options

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

Figure 104: 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.

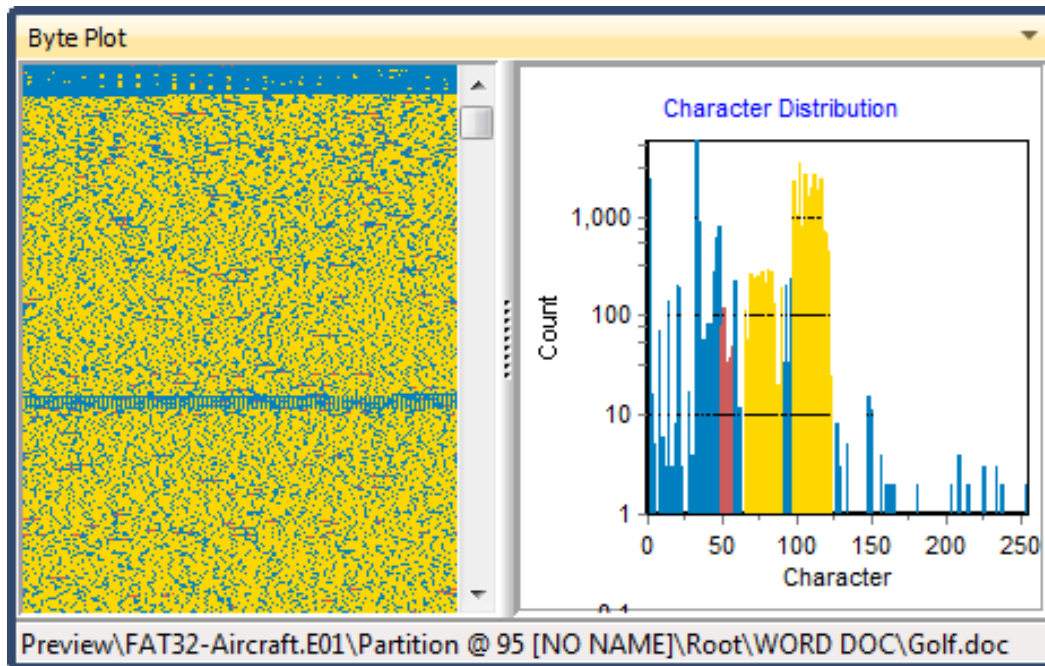
8.11.1 BYTE PLOT EXAMPLES

Microsoft Word document:

Figure 105 shows a Byte Plot and Character Distribution for the Microsoft Word file “Golf.doc”. The visualization is consistent with a Word document, where.

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

Figure 105: Byte Plot and Character Distribution of a .doc file



JPG Photograph:

Figure 106 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 106: Byte Plot and Character Distribution of a .jpg file

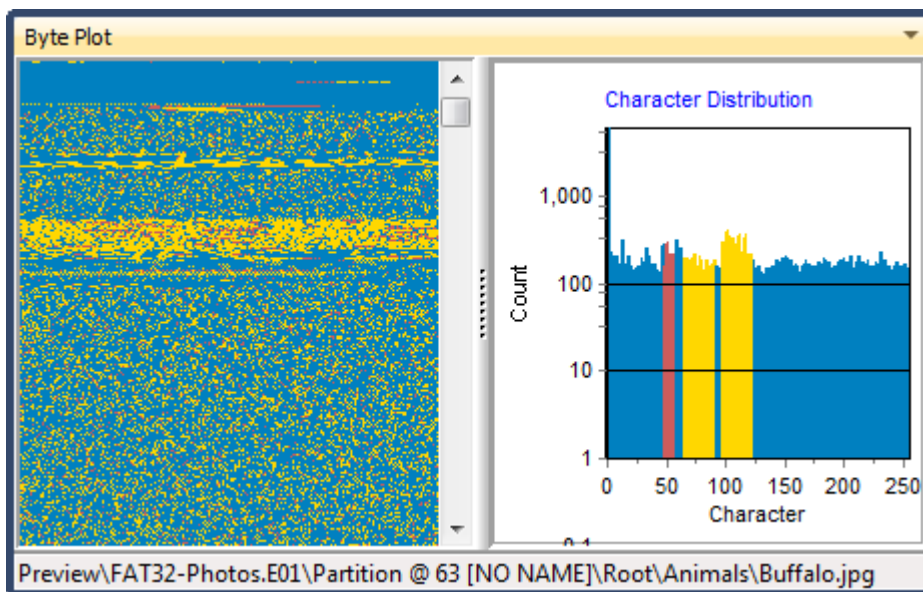
**RTF document:**

Figure 107 shows a Byte Plot and Character Distribution for an RTF document. The visualization is consistent with an RTF file where there is no defined file header and much of the file appears as text.

Figure 107: Byte Plot and Character Distribution of an .rtf file

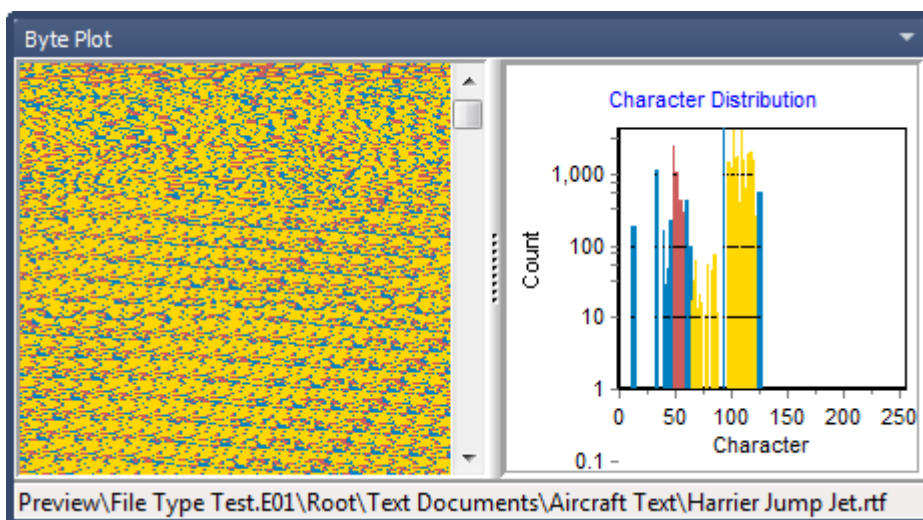
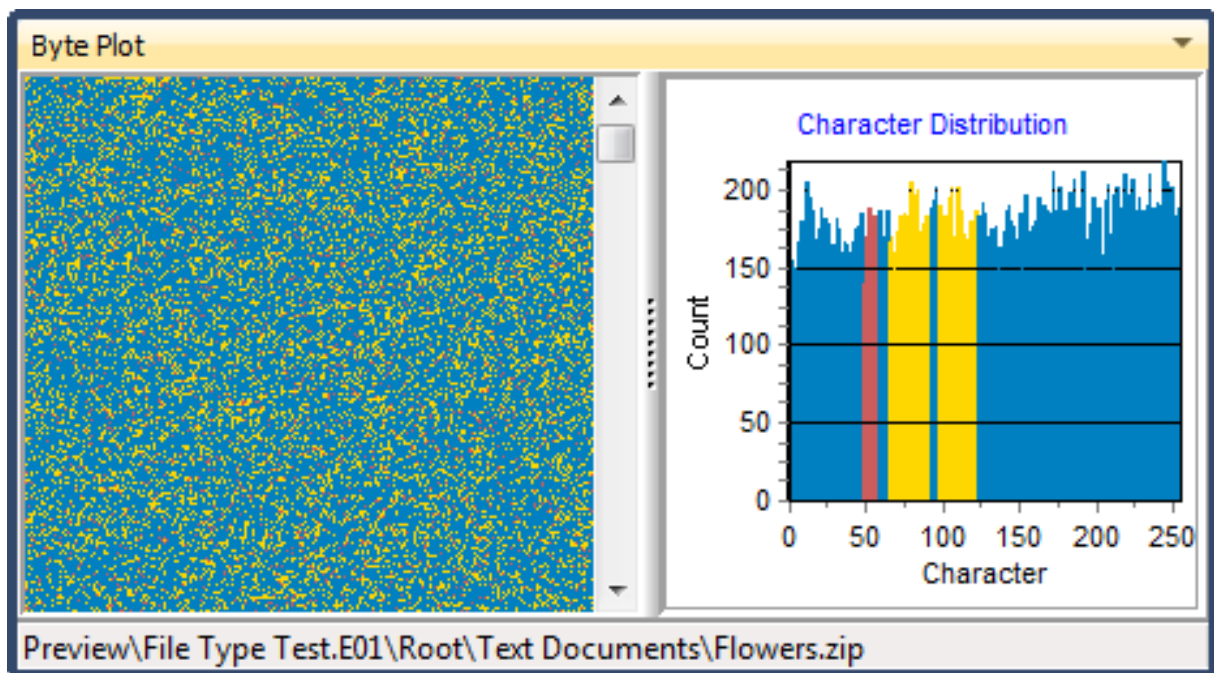
**ZIP file:**

Figure 108 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.

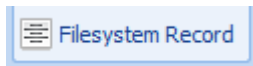
Figure 108: Byte Plot and Character Distribution of a .zip file



8.12 FILESYSTEM RECORD VIEW

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

Figure 109: Filesystem Record tab



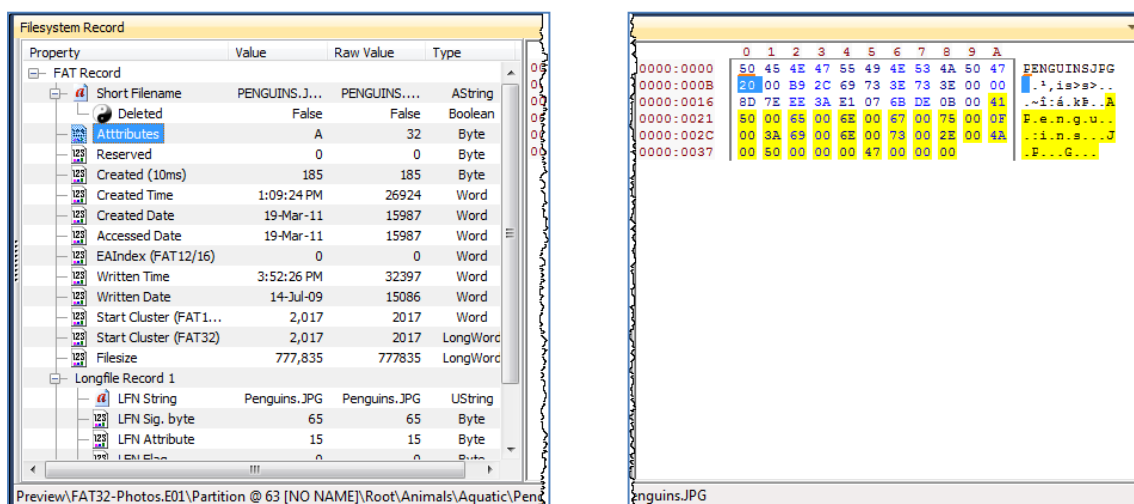
Filesystem Record view decodes and displays the full attributes of highlighted item, including FAT, MFT, HFS file system records and Windows registry entries.

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 110 below:

Figure 110: 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 110 above shows the records for the file “Penguins.JPG”. Clicking on the “Attributes” property on 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.

8.13 FILE METADATA

Metadata is loosely defined as “data about data”. Essentially it is information within a file which further describes 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 support includes:

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

- JPEG.
- ZIP.

Figure 111 below show the metadata of a Microsoft Word .doc file:

Figure 111: Metadata view of a Microsoft Word .doc file

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

- 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).

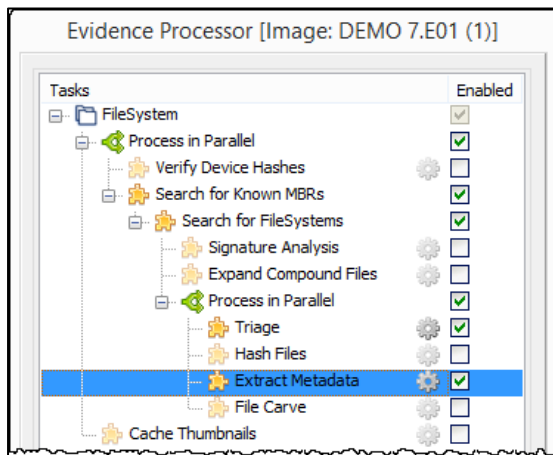
Metadata for both Office and Office 2007 files can be extracted to columns by running the **Extract Metadata to Columns** script (see below) without the need to first expand compound files.

8.13.1 EXTRACT METADATA

EXTRACT METADATA - EVIDENCE PROCESSOR

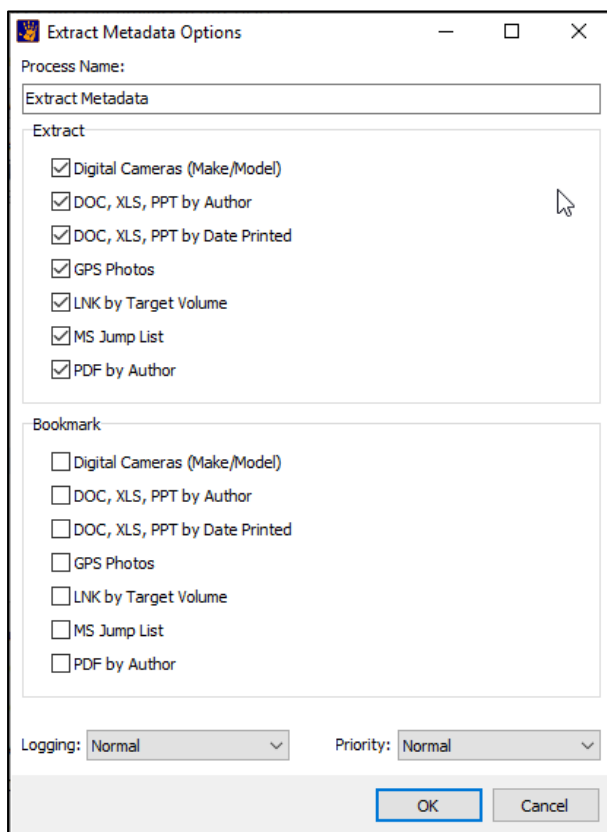
The option to **Extract Metadata** can be selected in the **Evidence Processor** when evidence is added to a case:

Figure 112: 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:

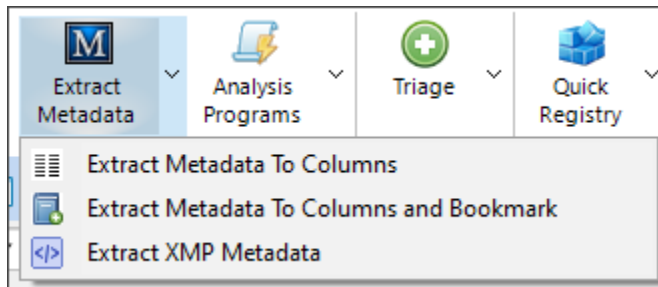
Figure 113: Extract Metadata Options



EXTRACT METADATA – ANALYSIS PROGRAMS

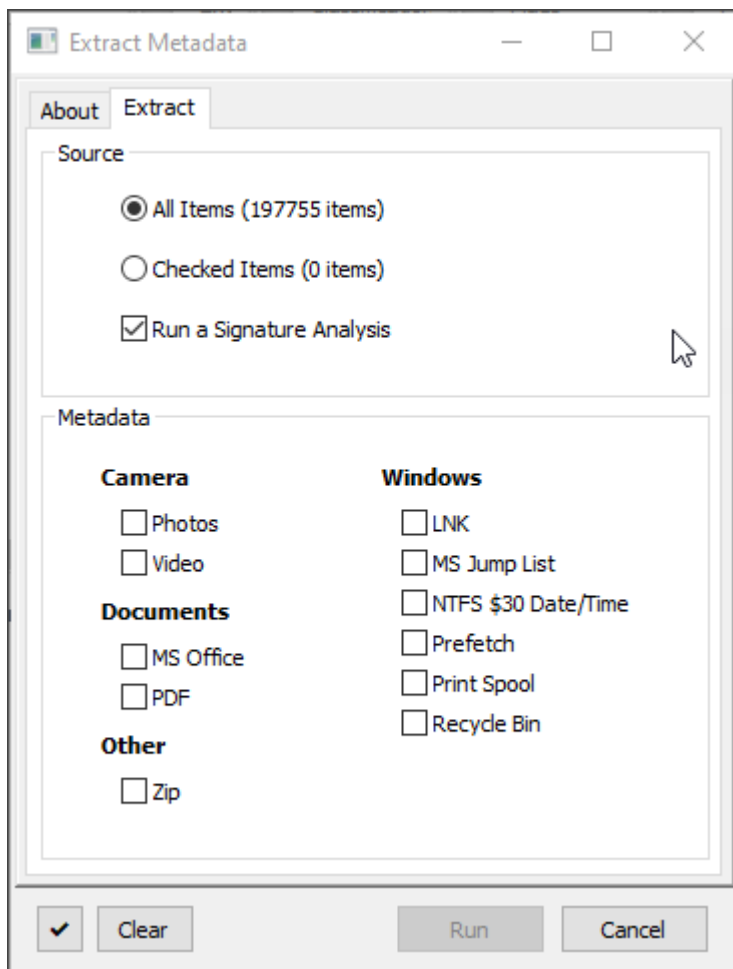
The metadata extraction options are also available from the **File System module, Extract Metadata** toolbar button, shown below:

Figure 114: Metadata extraction scripts, File System module, Extract Metadata menu



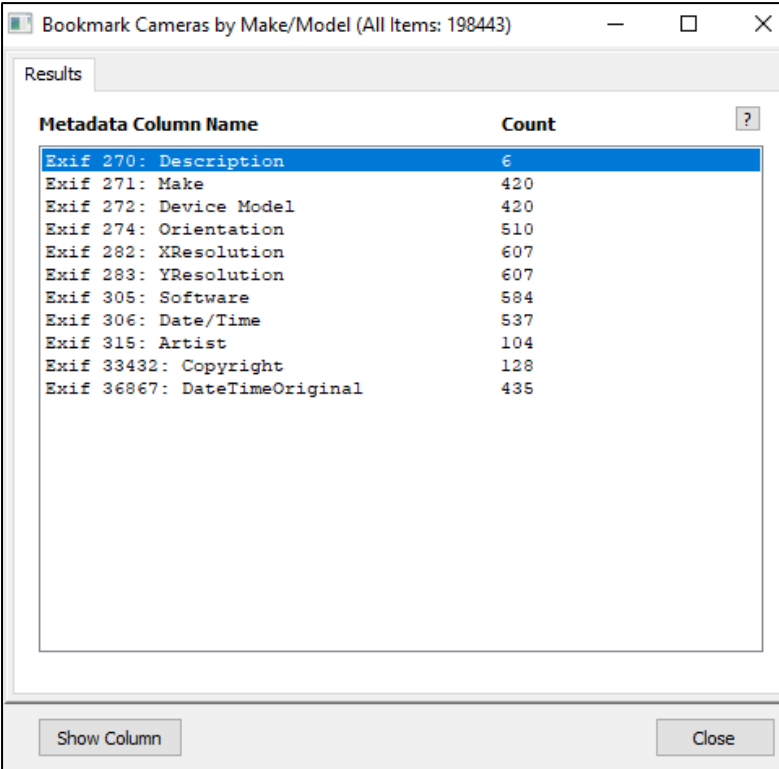
The **Extract Metadata to Columns** menu item opens the following window:

Figure 115: Extract Metadata to Columns



Select the types of metadata to extract and select the **Run** button.

At the completion of the metadata extraction the following window will appear which summarizes the result. Click on specific column names and click the **Show Column** button to add that column to the File System module (or manually add the column in the module using the right click columns menu option, see 9.4 - Columns):

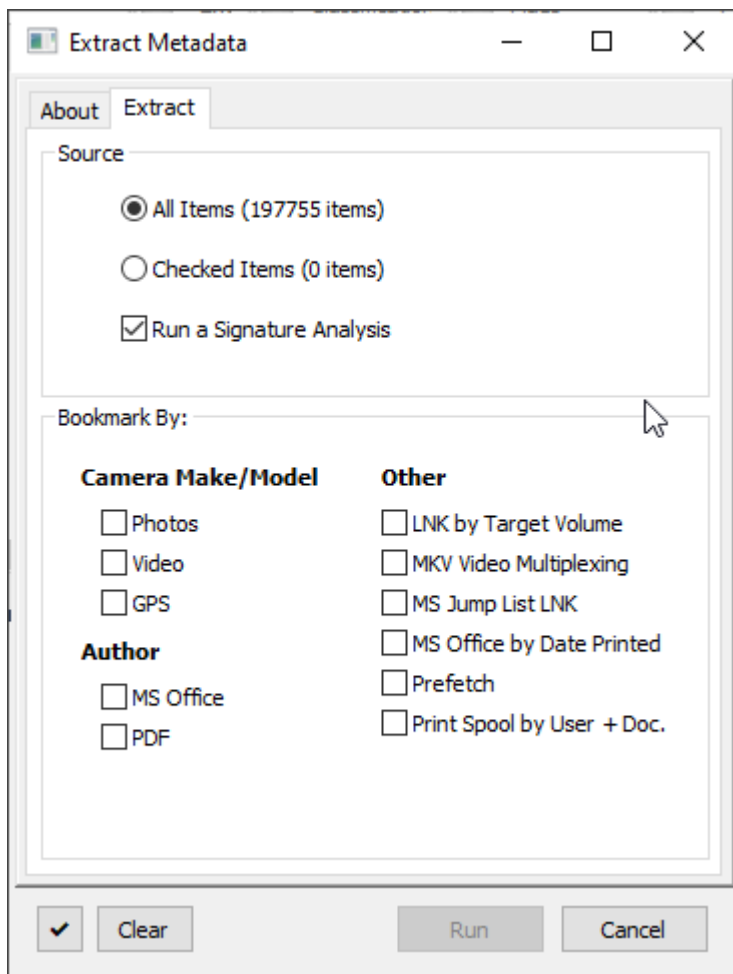


Metadata Column Name	Count
Exif 270: Description	6
Exif 271: Make	420
Exif 272: Device Model	420
Exif 274: Orientation	510
Exif 282: XResolution	607
Exif 283: YResolution	607
Exif 305: Software	584
Exif 306: Date/Time	537
Exif 315: Artist	104
Exif 33432: Copyright	128
Exif 36867: DateTimeOriginal	435

EXTRACT METADATA TO COLUMNS AND BOOKMARK

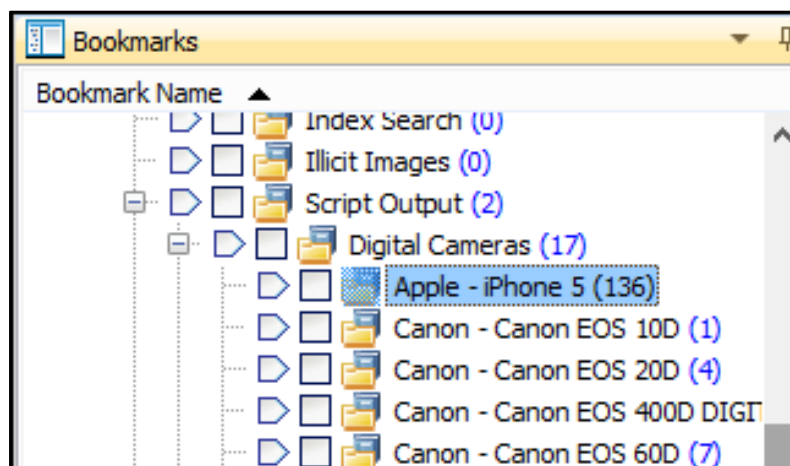
The **Extract Metadata to Columns and Bookmark** will also extract metadata data to columns and bookmark results by the selected criteria shown in Figure 116 below:

Figure 116: File System > Analysis Programs > Bookmark Metadata



Bookmarks are added to the Bookmarks module under the **Script Output** folder. The output of **Bookmark by Camera Make/Model** is shown in Figure 117 below:

Figure 117: Bookmarks by Metadata



8.13.2 XMP METADATA

The Extensible Metadata Platform (XMP) is: *an ISO standard, originally created by Adobe Systems Inc., for the creation, processing and interchange of standardized and custom metadata for digital documents and data sets* (source: https://en.wikipedia.org/wiki/Extensible_Metadata_Platform Accessed 01 September 2020).

XMP metadata can usually be found in documents that have been edited with Adobe products, including Adobe Photoshop. XMP metadata can be important for forensic investigators as it can provide additional information including edit date and time and software used.

XMP metadata for a camera file can be seen in **HEX** or **Text** views in the following format:

Figure 118: XMP Metadata shown in the Text data view for file 001.jpg

```
.....ÿl,http://ns.adobe.com/xap/1.0/.<?xpacket begin='ï»¿' id='
M0MpCehiHzreSzNTczkc9d'?>..<x:xmpmeta xmlns:x="adobe:ns:meta/"><rdf:RDF xmlns:rdf="http://w
.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31
33d75182f1b" xmlns:xmp="http://ns.adobe.com/xap/1.0/"><xmp:CreatorTool>Microsoft Windows Ph
o Viewer 6.1.7600.16385</xmp:CreatorTool></rdf:Description><rdf:Description xmlns:Microsoft
oto="http://ns.microsoft.com/photo/1.0/"><MicrosoftPhoto:DateAcquired>2016-12-20T05:40:50.4
</MicrosoftPhoto:DateAcquired></rdf:Description></rdf:RDF></x:xmpmeta>..
```

The File System module > **Metadata** > **Extract XMP Metadata** option enables the forensic investigator to scan a case and identify those files which contain XMP metadata. Click on the file in the left-hand column to display the XMP metadata in the right-hand side:

Figure 119: XMP Metadata for file 001.jpg

The screenshot shows a window titled "Embedded XMP Metadata" with a "Results" tab. On the left, there is a list of files with a search bar and a filter field. The file "001.JPG" is selected. On the right, the "XMP Metadata Preview" section displays the following information:

Filename:	001.JPG
Bates#:	172638
File Size:	1.09mb (1147307 bytes)
File System Created:	28-May-12 6:13:27 AM
File System Modified:	28-May-12 6:13:27 AM
XMP starts at File Offset:	11101

Below this, the XMP metadata is shown in a structured format:

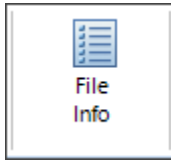
```
x:xmpmeta
rdf:RDF
rdf:Description
photoshop:DateCreated 2012-05-27T13:13:27
xmp:CreateDate 2012-05-27T13:13:27
xmp:ModifyDate 2012-05-28T10:41:04
xmp:CreatorTool QuickTime 7.6.6
MicrosoftPhoto:DateAcquired 2016-01-18T16:24:06.733
```

At the bottom of the window, there are buttons for "Bookmark", "Copy to Clipboard", "Export All XMP", and "Close". A status bar at the bottom indicates "Showing files containing XMP metadata: 713 of 713".

8.13.3 FILE INFO

Another way to view file information, including Metadata and XMP metadata is to use the **File Info** button in the File System module:

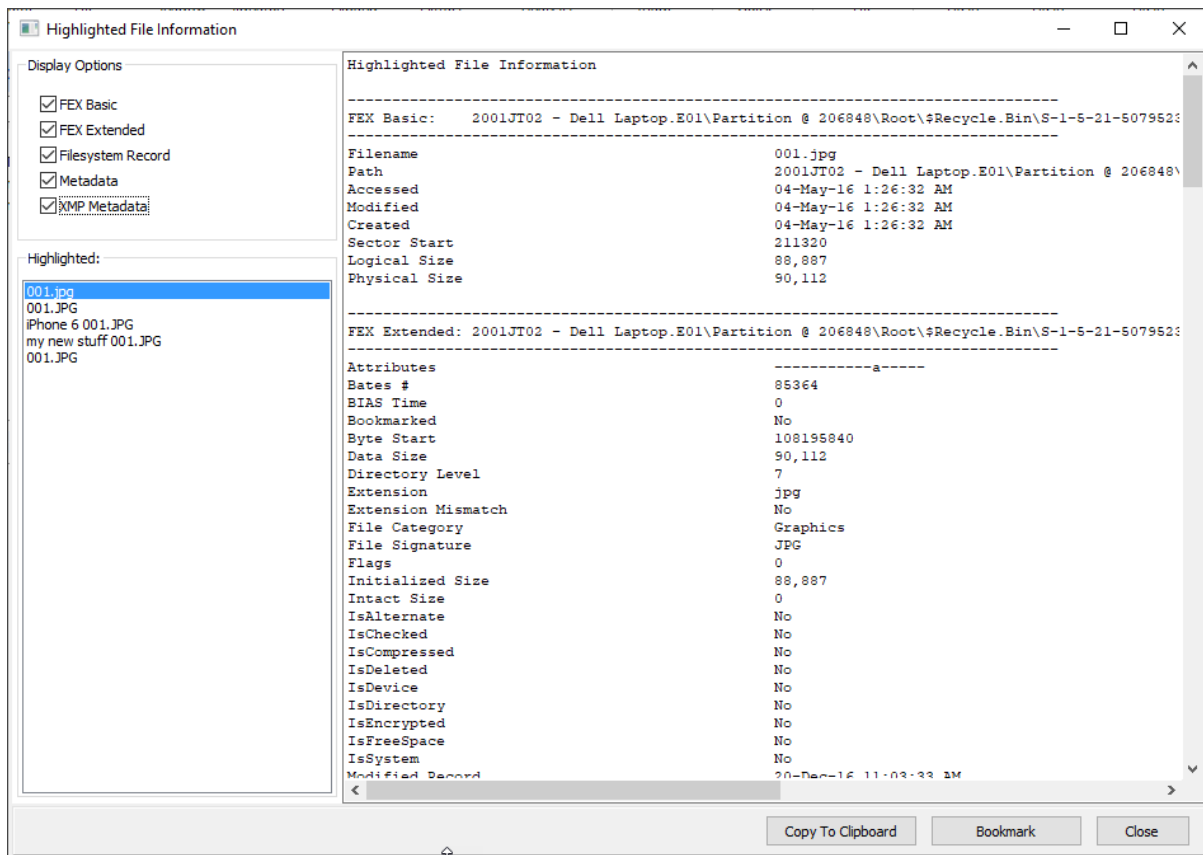
Figure 120: File System module File Info button



The File Info button works with highlighted files and provides options to view:

1. Basis Forensic Explorer fields (including Created, Modified, Accessed).
2. Extended Forensic Explorer fields (including signature and hash information).
3. Filesystem Record fields (as shown in the Filesystem Record data view tab).
4. Metadata (as shown in the Metadata data view tab).
5. XMP metadata (as described above).

Figure 121: File System module File Info button



8.14 FILE EXTENT

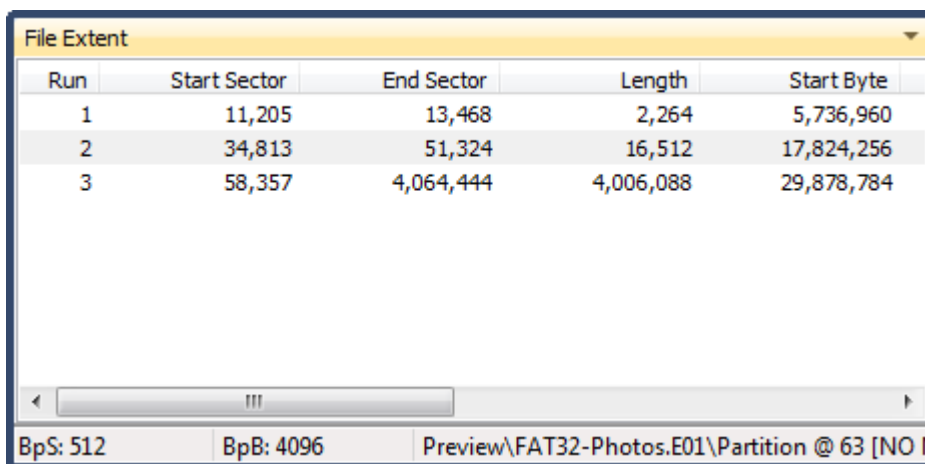
The default location for File Extent view is the bottom data view window, accessed via the File Extent tab:



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

The file shown in Figure 122 below is a fragmented file with three data runs:

Figure 122: File Extent data view

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

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

BpS: 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.

8.15 PERMISSIONS

Each user account on a Windows NTFS formatted computer is assigned a unique number called a security identifier (SID). Actions that take place on the computer can be associated with a specific SID. In more detail:

“In the context of the Microsoft Windows NT line of operating systems, a Security Identifier (commonly abbreviated SID) is a unique, immutable identifier of a user, user group, or other security principal. A security principal has a single SID for life (in a given domain), and all properties of the principal, including its name, are associated with the SID. This design allows a principal to be renamed (for example, from “Jane Smith” to “Jane Jones”) without affecting the security attributes of objects that refer to the principal.” https://en.wikipedia.org/wiki/Security_Identifier, accessed 20 April 2020.

There is a large volume of computer forensics literature relating to the use of a SID to track user behaviors, particularly in relation to identifying a user-account responsible for deleting files found in the Windows Recycle Bin.

In Forensic Explorer, to identify the SID associated with a file on an NTFS file system:

1. In the **File System** module, click on the file in question.
2. Switch to the **Permissions** tab in the bottom data views.
3. The **User SID** and **Group SID** is displayed in the information window, as shown in Figure 123 below (the abbreviated User SID for Marijuana_2011.jpg is **1000**):

Figure 123, Permissions

The screenshot shows the Forensic Explorer interface. At the top, there are view options: File List, Gallery View, Video View, Disk View, and Category Graph. Below that is a search bar containing 'A-Z Marijuana_2011.jpg' and 'A-Z jpg'. The main area displays a table with columns: Filename, Extension, Classification, and Flags. The first row shows '1 Marijuana_2011.jpg' with extension 'jpg'. Below the table, there is a summary bar: '1 of 197754 Visible [446 KB] 1 Highlighted [446 KB] 0 Checked [0 bytes] 2001JT02 - Dell Laptop.E0'. The bottom section is a table with columns: Name, ID, and Property. It lists the User SID (S-1-5-21-507952373-705505546-3123652967-1000), Group SID (S-1-5-21-507952373-705505546-3123652967-513), and a Discretionary ACL with four entries: -Basic ACE (S-1-5-80-2375682873-768044350-3534595160-1005545...), -Basic ACE (S-1-5-18), -Basic ACE (S-1-5-32-544), and -Basic ACE (S-1-5-21-507952373-705505546-3123652967-1000). The bottom toolbar includes tabs for Hex, Text, Info, Bookmark, Byte Plot, Display, Permissions, and Filesystem.

Name	ID	Property
User SID	S-1-5-21-507952373-705505546-3123652967-1000	
Group SID	S-1-5-21-507952373-705505546-3123652967-513	Domain Users
Discretionary ACL		
-Basic ACE	S-1-5-80-2375682873-768044350-3534595160-1005545...	
-Basic ACE	S-1-5-18	Local System
-Basic ACE	S-1-5-32-544	Administrators
-Basic ACE	S-1-5-21-507952373-705505546-3123652967-1000	

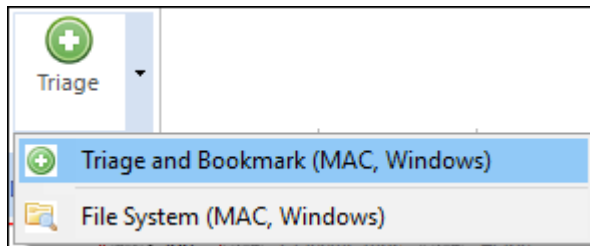
8.15.1 ASSOCIATING A SID TO A USER ACCOUNT

The process of connecting a SID to a specific user account name involves examining data in the Windows Registry.

THE FORENSIC EXPLORER TRIAGE REPORT

In Forensic Explorer if a **Triage** has been run (see 18.3.1):

Figure 124, Running a Triage.



The SID/User Account association is made in the **Reports** module, **Triage** report, in the section titled **User Accounts (SAM parsed data)**. In the example shown below information parsed from the Windows SAM registry file identifies that User ID **1000** is associated with the account of **John Thomas Hamilton**:

Figure 125, Extract from the Triage Report, User Accounts (SAM parsed data)

```

User Name:                John Thomas Hamilton
User ID:                  1000($03E8)
Account Created:         14-Jan-2015 21:55:06 [UTC]
Account Last Modified:   29-Dec-2019 21:47:11 [UTC]
Account Expires:         {Never}
Account Type:             ($0000)
Account Status:          Password not required
                        Normal user account
                        Password does not expire

Number Logins:           100
Last Login:              29-Dec-2019 21:47:04 [UTC]
Password Last Set:       29-Dec-2019 21:47:04 [UTC]
Password Hint:           0tBilbo1234
Last Password Fail:      29-Dec-2019 21:45:27 [UTC]
Invalid Password Count:  0
Country Code:            0 (Default)
~~~~~
Source: 2001JT02 - Dell Laptop.E01\Partition @
206848\Root\Windows\System32\config\SAM\SAM\Domains\Account\Users\000003E8

```

PROFILEIMAGEPATH - SOFTWARE HIVE REGISTRY KEY

A manual method of linking a SID with a user account is by examining the values of the **HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList** registry key. For a more detail on this process see:

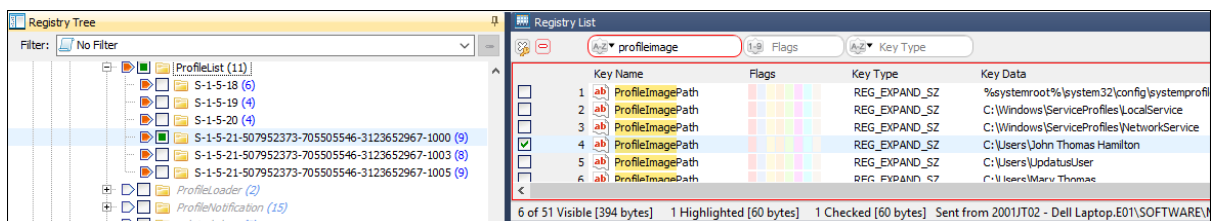
- International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012, DOI : 10.5121/ijnsa.2012.4209 121, FORENSIC ANALYSIS OF WINDOWS REGISTRY AGAINST INTRUSION, 5.3. Forensic Evidence from Security Identifiers, Haoyang Xie, Keyu Jiang, Xiaohong Yuan, Hongbiao Zeng;

- Mastering Windows Network Forensics and Investigation, Steven Anson, Steve Bunting, John Wiley & Sons, 2 Apr 2007, page 234, Registry Evidence.

To examine the Profile **ProfileImagePath** in Forensic Explorer:

1. In the **File System** module, locate the ...**Windows\System32\Config\SOFTWARE** registry file.
2. Right click and select **Send to Module > Registry** from the drop-down menu to send this file to the Registry module.
3. In the **Registry** module, filter for the **SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList** registry key.
4. Identify the SID in question and then examine the data in the **ProfileImagePath** subkey. The **Key Data** will list the path to the user's profile and display the username, as shown in Figure 126 below:

Figure 126, ProfileImagePath registry key



Chapter 9 - Working with data

In This Chapter

CHAPTER 9 - WORKING WITH DATA

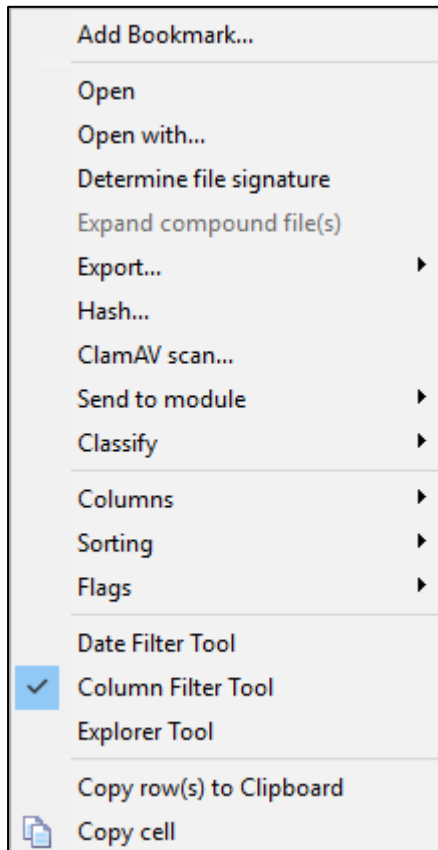
9.1	Working with data	133
9.2	Highlighted and checked items.....	133
9.2.1	Highlighted items	133
9.2.2	Highlight Item in Moule	134
9.2.3	Checked items.....	136
9.3	Bookmarks (Add or Edit).....	137
9.4	Columns	137
9.5	Open and Open with.....	139
9.6	Expand compound file	140
9.6.1	To expand compound files:.....	140
9.6.2	Identifying Expanded Compound Files.....	142
9.6.3	Filtering compound files	142
9.7	Export.....	142
9.7.1	Export Folders and Files	142
9.7.2	Export Logical Evidence File (.LO1)	144
9.7.3	Export Delimited Rows (.csv or .tab).....	147
9.8	OCR (Optical Character Recognition).....	148
9.9	Send to Module	151
9.10	Sorting.....	151

9.11	Flags	154
9.12	Filtering data	155
9.12.1	Date range filter	155
9.12.2	Column filter tool	157
9.12.3	Column Selection	161
9.12.4	Explorer Tool	162
9.12.5	Folders Filter	163
9.13	Copy rows to clipboard	163

9.1 WORKING WITH DATA

Forensic Explorer modules and data views share common functions used to view, analyze, and manage case content. These functions are either performed directly within the view, or are access by a right-click menu, as shown Figure 127 below:

Figure 127: 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 of 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:

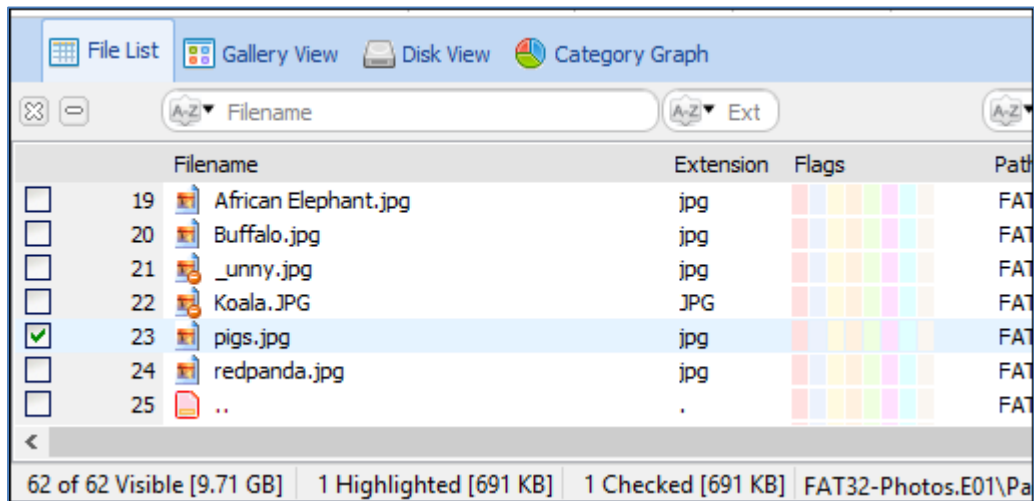
1. Highlight the first file with the mouse and then press and hold the Shift key.

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 128: Highlighted items



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

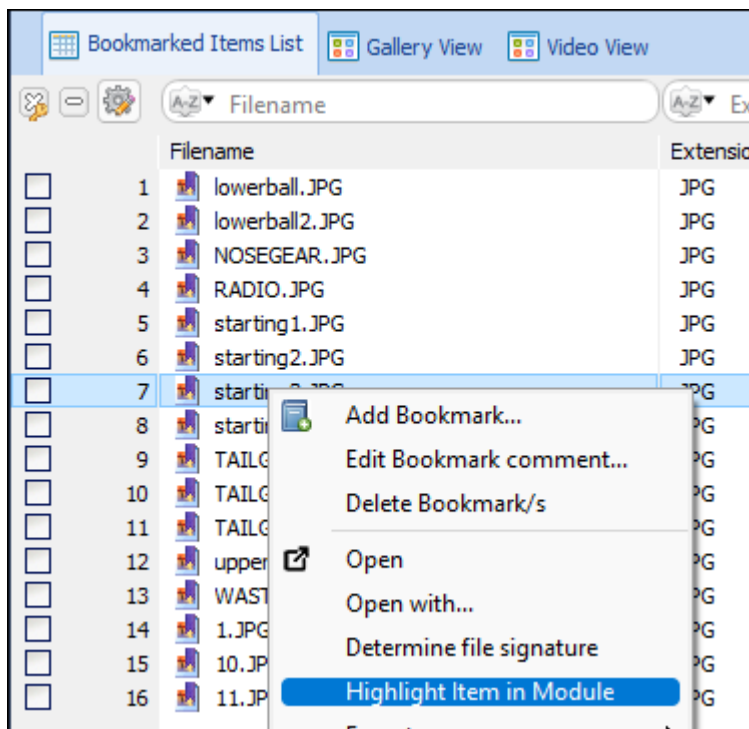
9.2.2 HIGHLIGHT ITEM IN MOULE

In certain modules (Bookmarks, Keyword Search, Index) there is a right-click menu option to **Highlight Item in Module**. The purpose of this it to take the user back to the item in the source module. For example:

In the **Bookmarks module**:

1. Highlight a bookmarked item.
2. Right-click and select **Highlight Item in Module** from the drop-down menu.

Figure 129: Bookmark module right-click Highlight Item in Module



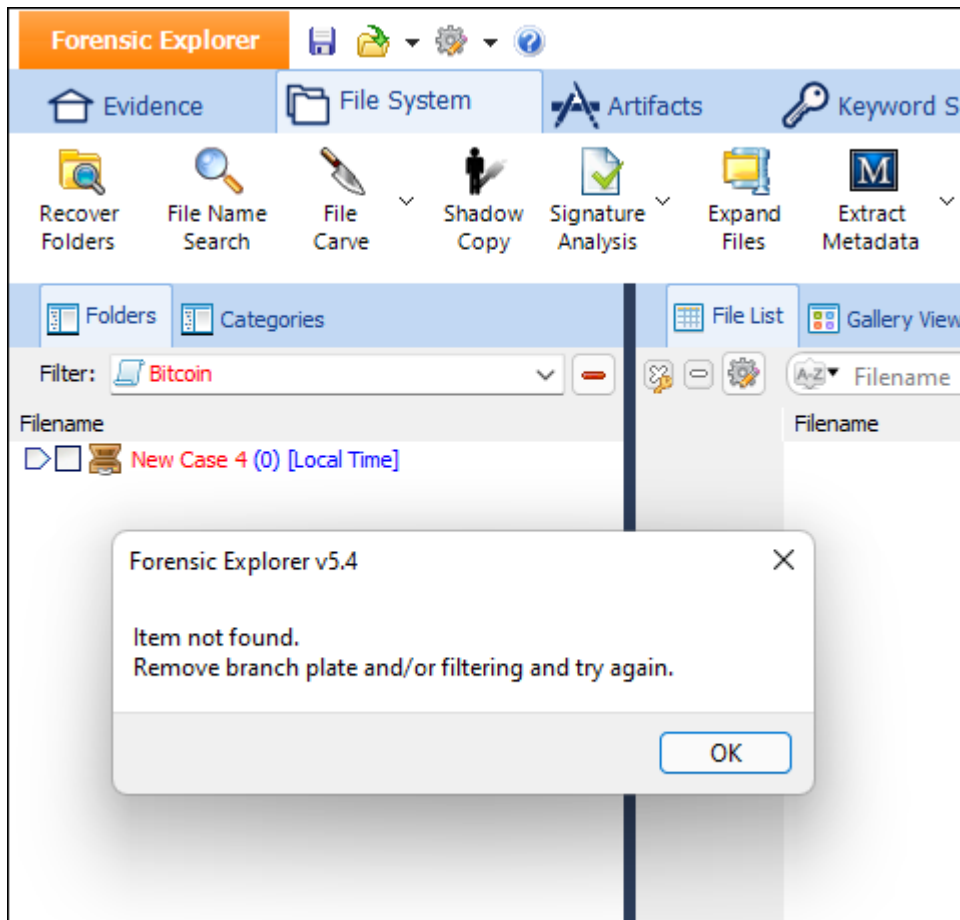
Forensic Explorer will then jump to the **File System module** (the source module of the bookmark) and highlight this item.

NOTE: There may be a situation where the source module has a branch plate or filter which excludes the subject item from view. If this is the case the following message will appear:

Item not found. Remove branch plate and/or filtering and try again.

Resent the branch plate and/or filter and try again.

Figure 130: Highlight Item in Module



9.2.3 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.

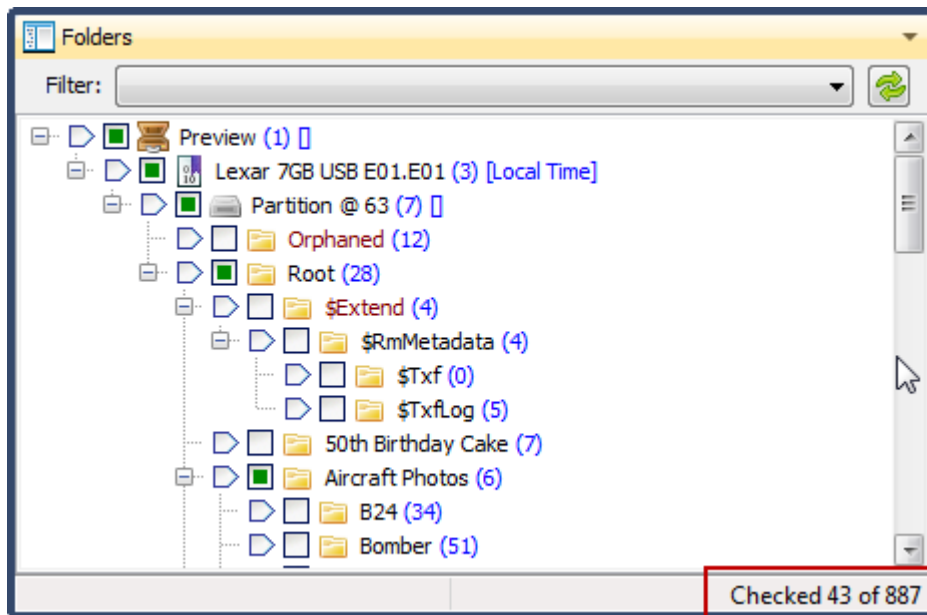
To check **multiple items**:

1. Follow the instructions 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 131 below:

Figure 131: Checked item count in Folders view.



9.3 BOOKMARKS (ADD OR EDIT)

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.**

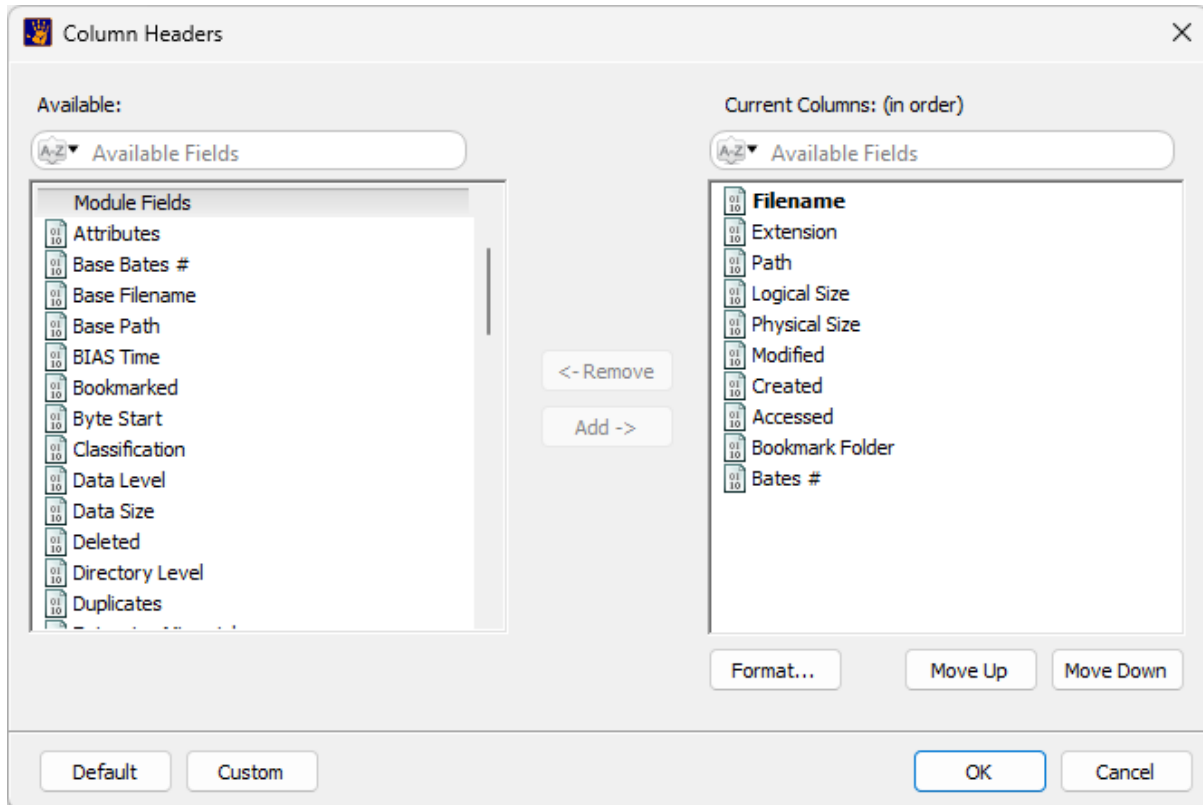
This will open the Add Bookmark window. See **Chapter 17 - Bookmarks Module**, for more information on adding and editing bookmarks.

9.4 COLUMNS

To add columns or remove columns in a list view:

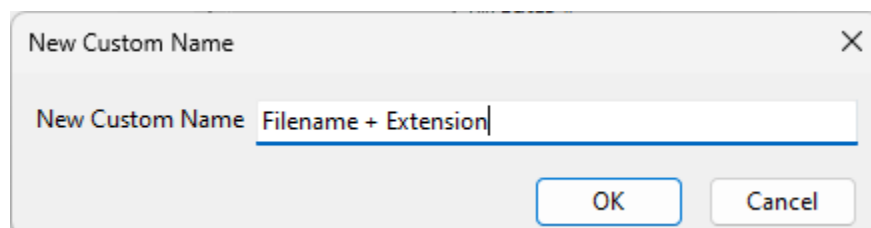
1. **Right click** on the List view and select **Columns > Edit Columns** from the drop-down menu. The Column Headers window will open.

Figure 132: Column Headers



2. **Add** available columns to the current columns and **Move Up** or **Move Down** for the required position (position can also be controlled by dragging and dropping column titles once they are added). **Remove** unwanted columns with the remove button.
3. **Default:** Returns to the default column selection (shown above).
4. **Custom:** Enables the user to save custom column layouts.
 - a. Change **Current Columns** to the require layout.
 - b. In the **Column Headers** window select **Custom > Save...**
 - c. Enter the name for the **Custom Columns:**

Figure 133: Create custom columns.



Custom column layouts are saved as XML files in the following folder:

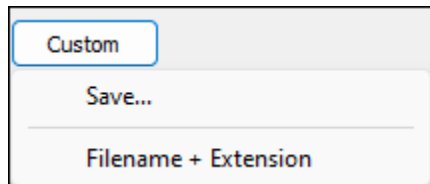
\Documents\Forensic Explorer v5\Startup\Custom Columns\FileSystem-Filename + Extension.xml

Custom columns are specific to each module and are automatically prefixed with the module name.

5. Custom columns are accessed from:

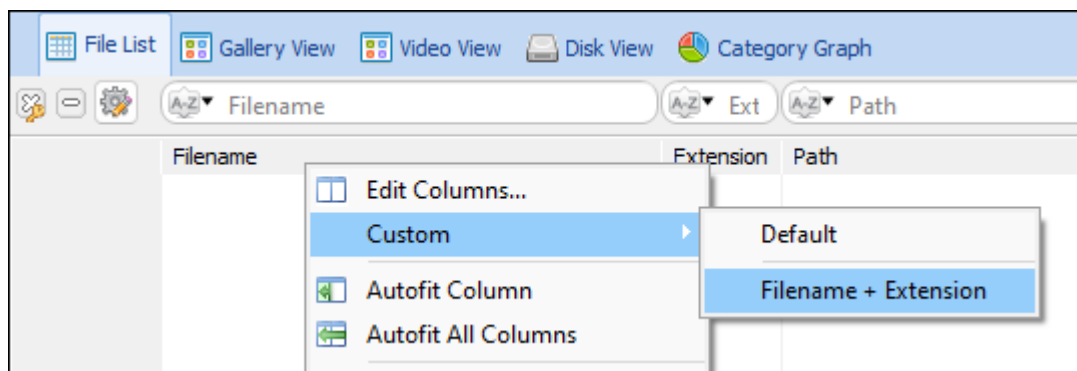
a. The **Custom** button:

Figure 134: Access custom columns.



b. The right-click **File List** menu:

Figure 135: Access custom columns.



Clear columns:

- Columns that have been populated by a user driven process such as **Extract Metadata**, **Skin Tone**, etc. can be cleared:
 - Right-click on the column header and select **Clear Column** from the menu. The clear process will be applied to that column only. Or,
 - In the **File System** module, select **Tools > Clear Columns**. Select the columns to be cleared in the GUI and run.

9.5 OPEN AND OPEN WITH

The **Open** and **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:

- 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.

9.6 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.

An investigator should be selective about the compound files that are expanded. Expanding all compound files could rapidly increase the volume of data in a case.

Typically, user-created 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.

There are two ways to expand compound files:

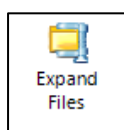
1. Using the **Expand Files toolbar button**.
2. Using the **right-click, expand files** menu option.

9.6.1 TO EXPAND COMPOUND FILES:

TOOLBAR BUTTON

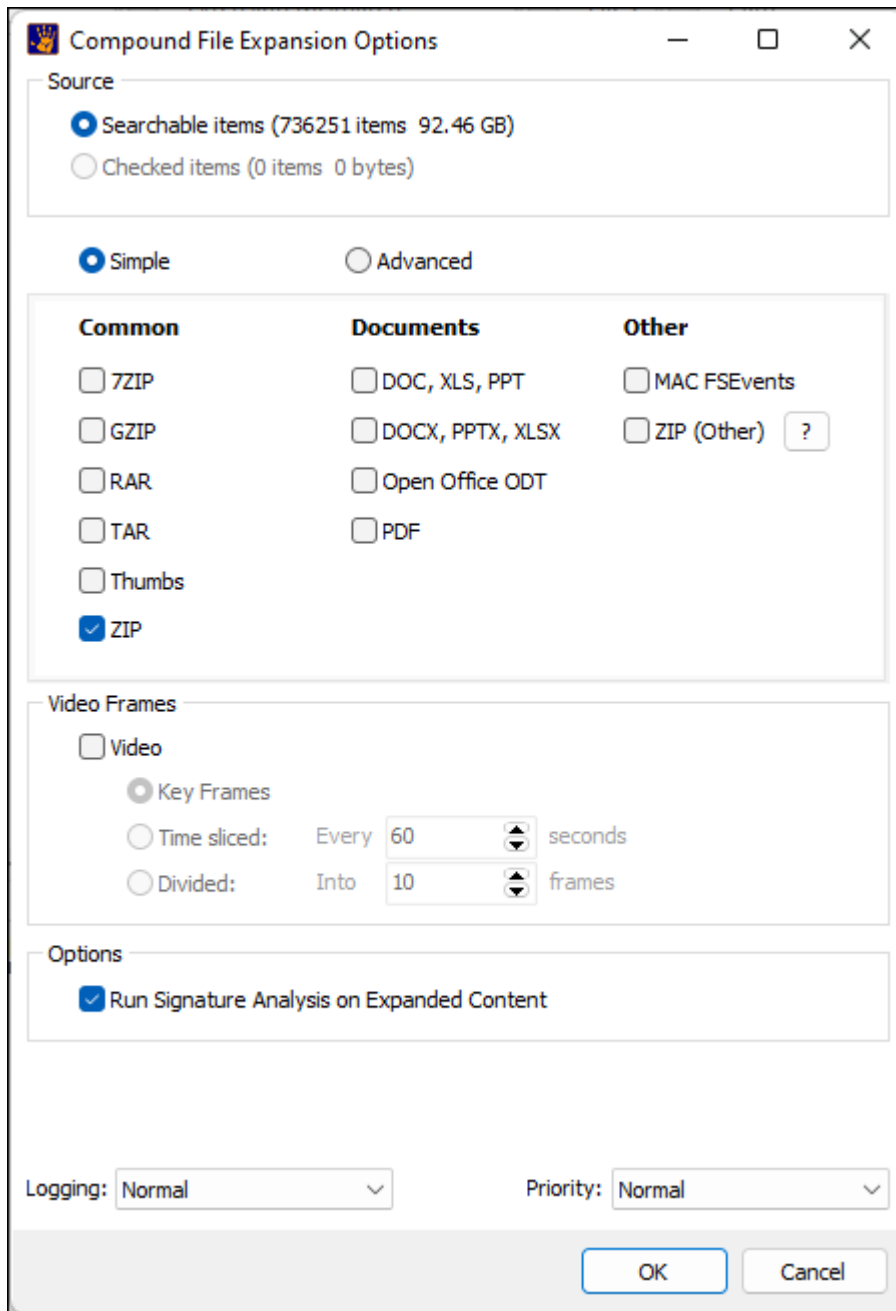
To expand files using the toolbar button, click the button:

Figure 136: File System toolbar, Expand Compound Files



The following options window shown in Figure 137 below:

Figure 137: Expand Compound Files



RIGHT-CLICK MENU

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(s)** from the drop-down menu.

7-Zip files are now decompressed into individual Logical Evidence files (L01) and exported to the Cases\[Case Name]\Expanded folder (this process is seamless to the user). Each L01 is identified by the Bates number of the

originating file. Reading expanded content from L01 considerably speeds up random access to compound data in Forensic Explorer.

9.6.2 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.

9.6.3 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:
 - a. **Expanded:** Displays all expanded files.
 - b. **Jump List (Windows):** Shows expanded MS Jump List files.
 - c. **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.

9.7 EXPORT

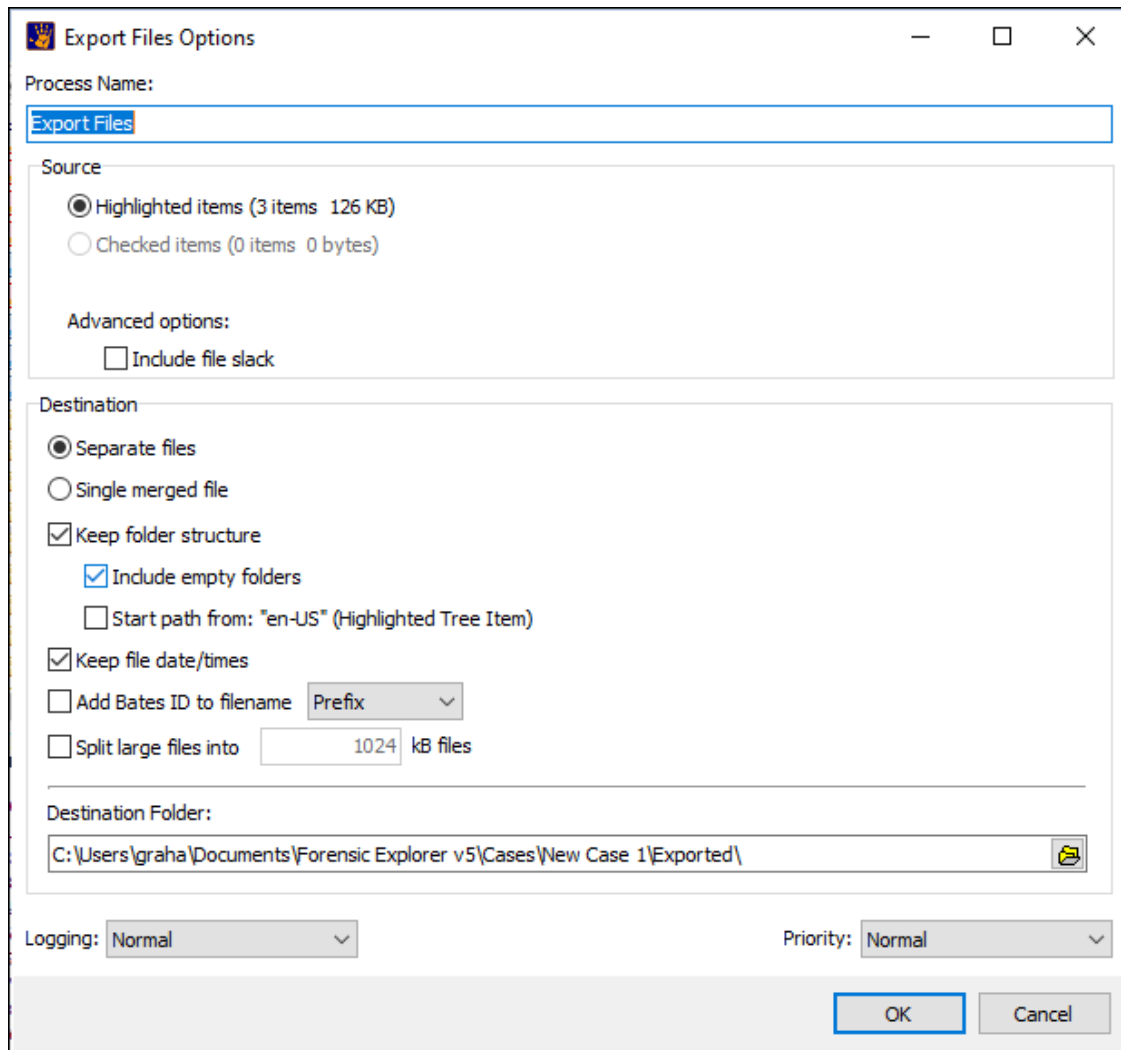
9.7.1 EXPORT FOLDERS AND FILES

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 138: Export files window

**Source:**

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

Include File Slack

- File Slack is 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 that may not relate to the actual file being exported.

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 their full path structure. If not checked all files will be written directly into the export folder.
 - **Include Empty Folders:** Includes empty folders with the export.

- **Start path from:** This option is active when the right-click: **Export > Folders and files** is run from the folder tree. Selecting this option will start the save path from a selected folder. For example, when the **right-click** is executed on the **Cat Pictures** folder:

[Case Name]\Partition @ 2048\Root\My Pictures\Cat Pictures\cat_pic1.jpg

[Case Name]\Partition @ 2048\Root\My Pictures\Cat Pictures\cat_pic2.jpg

the export path will start from 'Cat Pictures'.

- **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.

9.7.2 EXPORT LOGICAL EVIDENCE FILE (.L01)

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

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

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

To export files to an .L01 file:

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

Figure 139: Export to Logical Evidence File (.L01)

Export Files to L01 Options

Process Name:
Export Files to L01

Source

Highlighted items (22 items 344 KB)
 Checked items (0 items 0 bytes)

Advanced options:

Include file slack
 Folder data (FAT Folder Records; Empty Folders, Expanded)

Destination

Case Name: Test Case 1

Evidence Number:

Unique Description:

Examiner: GetData Forensics

Notes:

Image type: Encase® (*.L01) File Segment Size (MB): 2000

File Entry Hashes
 MD5

Compression
 None
 Good (Smaller but slower)
 Best (Smallest and slowest)

Use OS safe filenames
 Start path from: Unavailable - No Highlighted Tree Item

Destination Folder:
C:\Users\graha\Documents\Forensic Explorer v5\Cases\Test Case 1\Exported\

Destination File:
ExportFiles.L01

Logging: Normal Priority: Normal

OK Cancel

Include file slack: File Slack is 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 that may not relate to the actual file being exported.

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.

File Entry Hashes: MD5: If selected, an MD5 is calculated for each file and stored within the L01. At a future time, a new hash of the file in the L01 can be compared to the acquisition hash to determine that the data has not changed.

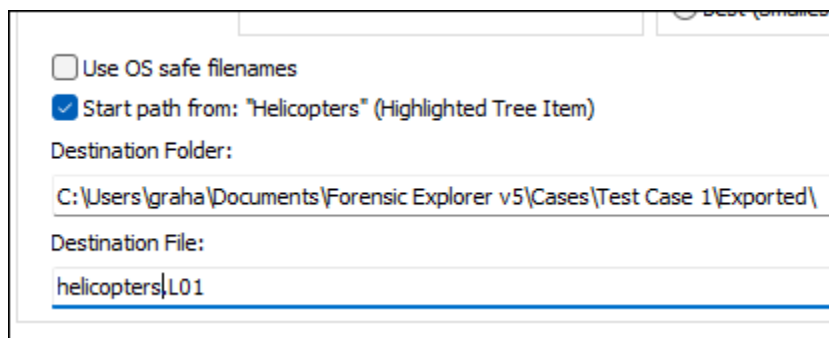
Compression: Sets the level of compression for the image file.

Use OS safe filenames: This option is used to ensure that filenames within the L01 are safe in cross-platform use (e.g., Linux to Windows). When this option is checked:

- Characters: #0 .. #31, ':', '\', '/', '?', '>', '<', '*', '|', '"' are replaced by space.
- Blank spaces at the end of filenames are trimmed.

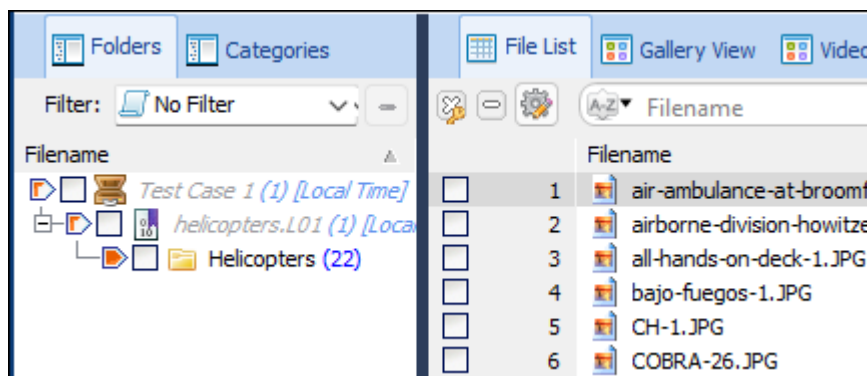
Start path from: This option allows for the shortening of the file path within the L01. The option is only available from the right-click menu in the Folder tree. In the example below, the **Helicopters** folder is selected in the tree:

Figure 140: Start path from



The root folder of the L01 is the selected folder:

Figure 141: Start path from (root folder)



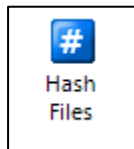
VALIDATING .L01 FILES

To validate an .L01 files in Forensic Explorer

1. **Add the .L01 file** to a case, or a preview:

2. Add the **File Acquisition Hash (MD5)** column to the list view of the File System module (refer to paragraph 9.4 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 142: Hash Files button in the File System module toolbar



4. Compare the **Hash (MD5)** to the **File Acquisition Hash (MD5)**. The acquisition hash and the recalculated hash should be identical, as shown in

Figure 143: Comparing Hash (MD5) to File Acquisition Hash (MD5) in a L01

Filename	Hash (MD5)	File Acquisition Hash (MD5)
1 air-ambulance-at-broomfield-...	d1868c1bea256ad5003f04a631d94...	d1868c1bea256ad5003f04a631d94...
2 airborne-division-howitzer-1....	00d6bbbcf2a6c720def64d51ea968...	00d6bbbcf2a6c720def64d51ea968...
3 all-hands-on-deck-1.JPG	b807f2913f56c1f1232df45041bf7f78	b807f2913f56c1f1232df45041bf7f78
4 bajo-fuegos-1.JPG	fb415999b42aa83095cf7cb9573cae56	fb415999b42aa83095cf7cb9573cae56
5 CH-1.JPG	ac68bb9639b7b519e762812d99063...	ac68bb9639b7b519e762812d99063...
6 COBRA-26.JPG	8e3bc057814e3a3d355ce83b7eb62...	8e3bc057814e3a3d355ce83b7eb62...
7 EH-1.JPG	ca3368833cb536b7fa83f8cc0c6ecada	ca3368833cb536b7fa83f8cc0c6ecada
8 eurocopter-ec-1.JPG	32e529da2e625b427fd43e645f506...	32e529da2e625b427fd43e645f506...
9 helicopter-bell-v-1.JPG	a3b561115cd07342be95954b0dd15...	a3b561115cd07342be95954b0dd15...
10 helicopter-ecureuil-as-1.JPG	8672de7362749f5b4c8a49fce9852...	8672de7362749f5b4c8a49fce9852...
11 helicopter-hh-1.JPG	742d7504e9670bebab5186df2cc70...	742d7504e9670bebab5186df2cc70...
12 helicopter-landing-1.JPG	615e4fab08c72315ccaf6a18de9de356	615e4fab08c72315ccaf6a18de9de356
13 helicopter-mi-1.JPG	0fb7a4caff2074d89beb7846c07a991b	0fb7a4caff2074d89beb7846c07a991b
14 helicopters-mh-1.JPG	1a128db68b02b36c36f37544bbfaa...	1a128db68b02b36c36f37544bbfaa...
15 helicopters-mi-1.JPG	75208903e216ea9777cb46ce4c13e...	75208903e216ea9777cb46ce4c13e...
16 heli-waterfall-australia-1.JPG	721271cd477a1afd6a4403edd1747...	721271cd477a1afd6a4403edd1747...
17 large-as-life-1.JPG	392ed65ccd756b3a16805c93193c8...	392ed65ccd756b3a16805c93193c8...
18 light-helicopter-1.JPG	ecfa544fc8e81b5feff248f9f197747d	ecfa544fc8e81b5feff248f9f197747d
19 MI-1.JPG	095ea7fad6e833b3d2fda5d5690af...	095ea7fad6e833b3d2fda5d5690af...
20 military-helicopter.JPG	2d5b2401f073d9f726a83e19943f1abf	2d5b2401f073d9f726a83e19943f1abf
21 puma-helicopter-1.JPG	9da6c650ba8bfc240782fc07bf7b965f	9da6c650ba8bfc240782fc07bf7b965f
22 tornado-3.JPG	958ae4c1c001d5bd06df7239446c2...	958ae4c1c001d5bd06df7239446c2...

9.7.3 EXPORT DELIMITED ROWS (.CSV OR .TAB)

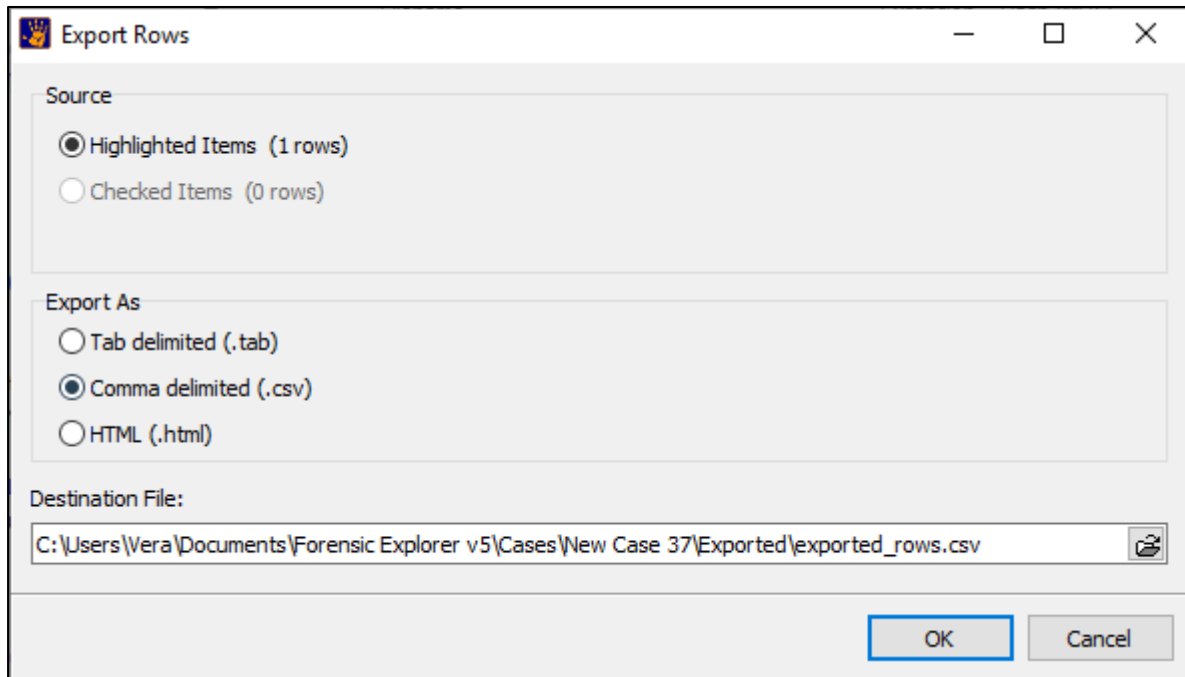
The export delimited rows function is used to copy list view data into a format suitable for import into a spreadsheet or similar program.

To **export delimited rows**:

1. **Highlight** or **check** the required files.
2. **Right click** and select “**Export > Export Rows (tab, csv, html)...**” from the drop-down menu.

The following window will appear:

Figure 144: 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.

9.8 OCR (OPTICAL CHARACTER RECOGNITION)

Optical character recognition (OCR) is the automated conversion of images of typed, handwritten or printed text into computer text. Once in computer text the content can be keyword searched, indexed, etc.

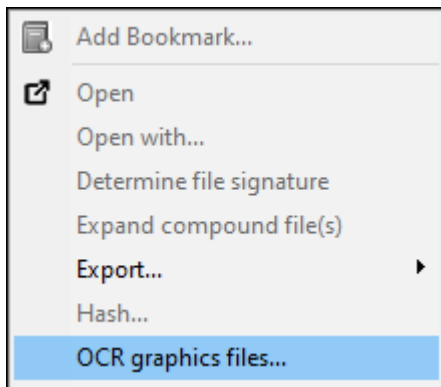
Forensic Explorer uses the **Tesseract Open-Source OCR Engine** (<https://tesseract-ocr.github.io/>).

Important: In Forensic Explorer, OCR operates on **graphics** files. However, other file types with embedded graphics (such as **PDF**, **DOC**, and **DOCX**) can also be processed if the **files are expanded** (right-click, expand compound files) to expose the internal graphics.

To apply OCR in Forensic Explorer:

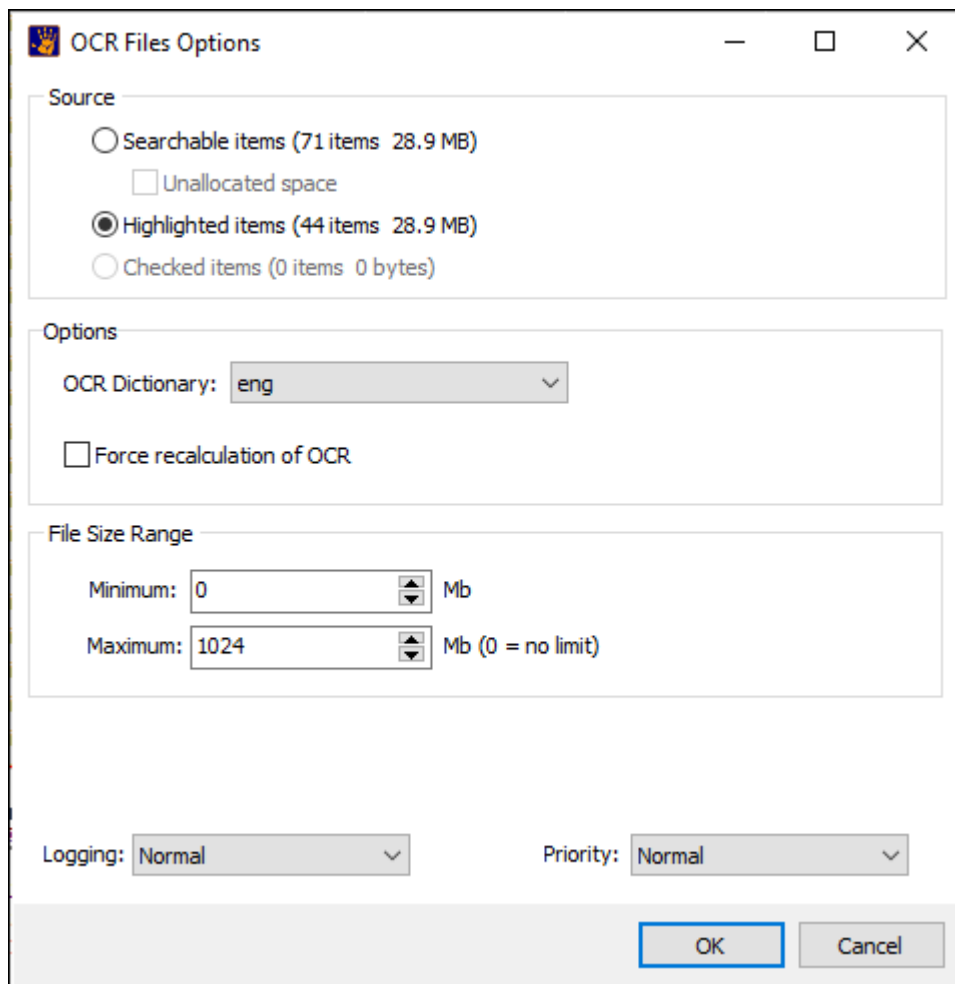
1. Select the graphics to be examined. As OCR is a resource intensive process it can be faster to work with Highlighted or Checked items rather than processing all Searchable items.
2. In the File System module > File List > Right-click menu, select **OCR**:

Figure 145: File System right-click menu option, OCR (Graphics)



3. Select the required options in the OCR File Options window:

Figure 146: OCR File Options

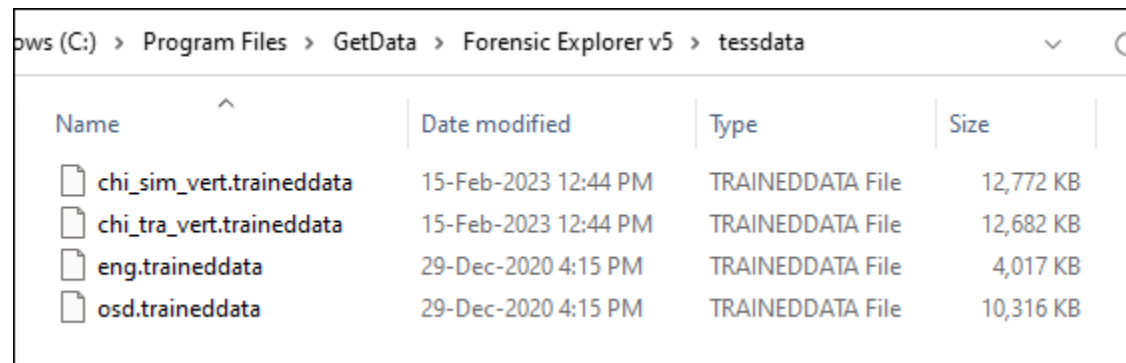


OCR Dictionary: Select the required OCR language (English is selected by default).

Support for additional languages is achieved by adding Tesseract **.traineddata** language files (available from: https://github.com/tesseract-ocr/tessdata_best).

The required language files are added to the **tessdata** folder in the Forensic Explorer installation folder. Once added they will appear in the **OCR Dictionary** drop-down menu.

Figure 147: Tesseract .traineddata language files (English and Chinese shown).



The screenshot shows a Windows File Explorer window with the address bar set to 'C:\Program Files\GetData\Forensic Explorer v5\tessdata'. The file list contains the following items:

Name	Date modified	Type	Size
chi_sim_vert.traineddata	15-Feb-2023 12:44 PM	TRAINEDDATA File	12,772 KB
chi_tra_vert.traineddata	15-Feb-2023 12:44 PM	TRAINEDDATA File	12,682 KB
eng.traineddata	29-Dec-2020 4:15 PM	TRAINEDDATA File	4,017 KB
osd.traineddata	29-Dec-2020 4:15 PM	TRAINEDDATA File	10,316 KB

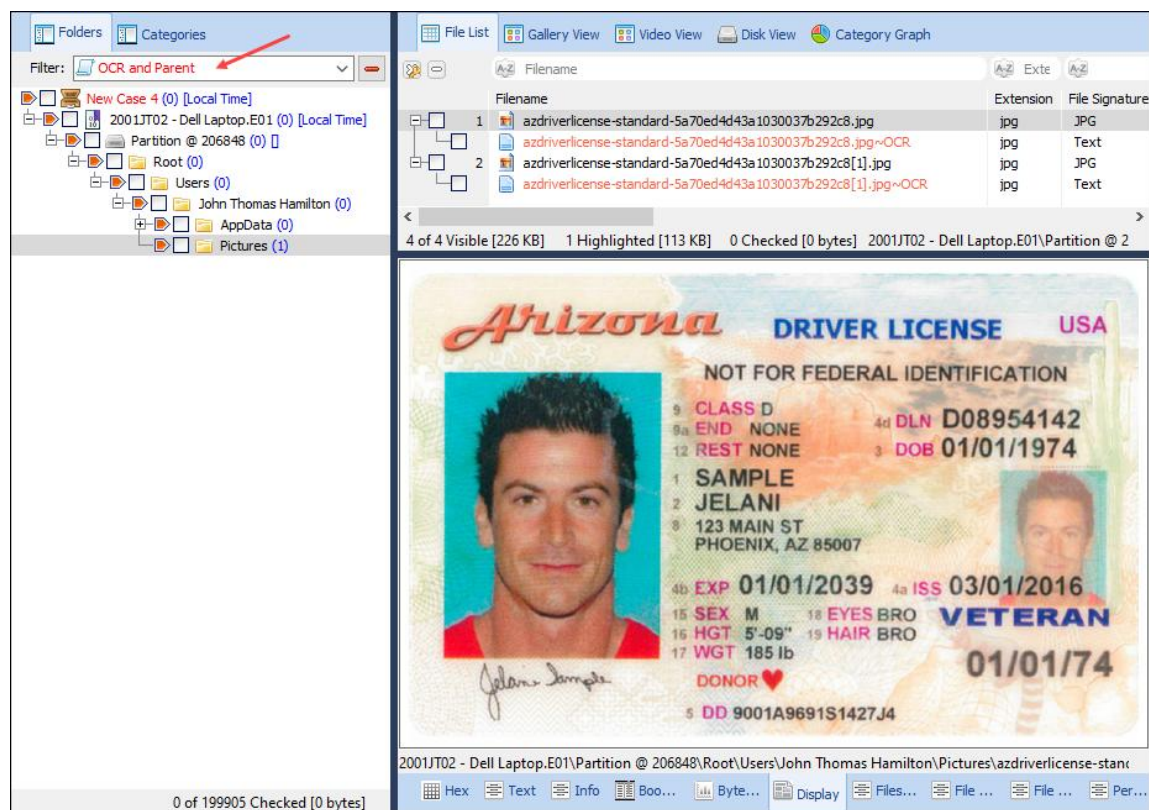
If a graphic contains OCR text, then:

- An **alternate data stream** is created as a child of the file.
- The alternate data stream has the same name as the parent with **~OCR** appended.

IMPORTANT: ~OCR results are added to the Forensic Explorer GUI. If a **branch plate** is active, it will be necessary to **re-branch plate** to see then newly added ~OCR files.

An example of Forensic Explorer OCR output is shown in Figure 148 and Figure 149 below:

Figure 148: A graphic file to which OCR has been applied.



The screenshot shows the Forensic Explorer GUI with a filter set to 'OCR and Parent'. The file list displays the following files:

Filename	Extension	File Signature
1 azdriverlicense-standard-5a70ed4d43a1030037b292c8.jpg	jpg	JPG
2 azdriverlicense-standard-5a70ed4d43a1030037b292c8.jpg~OCR	jpg	Text
azdriverlicense-standard-5a70ed4d43a1030037b292c8[1].jpg	jpg	JPG
azdriverlicense-standard-5a70ed4d43a1030037b292c8[1].jpg~OCR	jpg	Text

The main preview area shows an Arizona Driver License for 'SAMPLE JELANI'. The OCR results are displayed as follows:

Arizona DRIVER LICENSE USA
 NOT FOR FEDERAL IDENTIFICATION

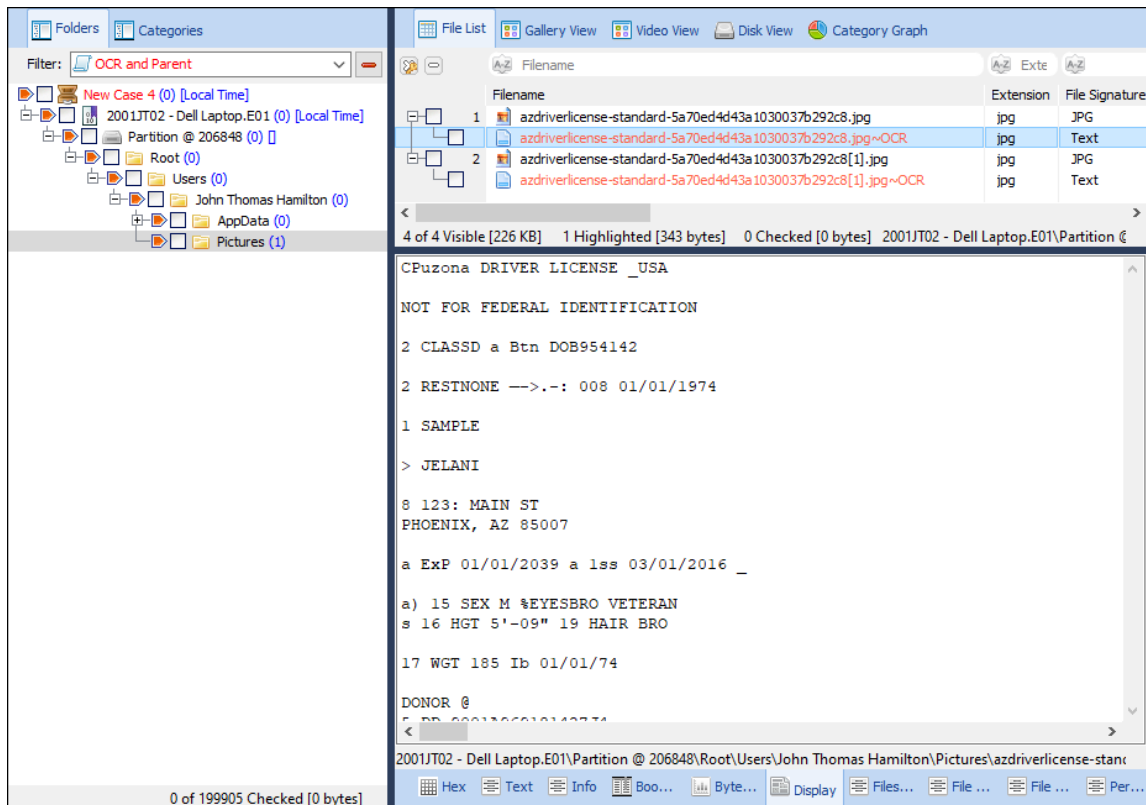
9 CLASS D 4d DLN D08954142
 9a END NONE 3 DOB 01/01/1974
 12 REST NONE

1 SAMPLE
 2 JELANI
 8 123 MAIN ST
 PHOENIX, AZ 85007

4b EXP 01/01/2039 4a ISS 03/01/2016
 15 SEX M 18 EYES BRO VETERAN
 16 HGT 5'-09" 19 HAIR BRO
 17 WGT 185 lb
 5 DD 9001A9691S1427J4

01/01/74

Figure 149: The resulting [filename]~.jpg~OCR output



9.9 SEND TO MODULE

Send to Module is a method of passing specific files from one module to another. For example, a Windows registry file can be highlighted in the list view of the File System module and passed to the Registry module for processing (see 16.2 for more information).

9.10 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 150: Single column sort



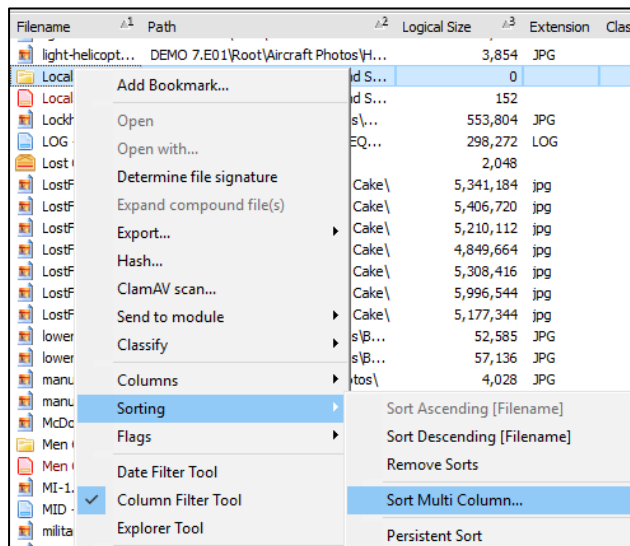
The same single column sort result can be achieved by right clicking on the column and in the drop-down menu select "Sort Ascending [column name]" or "Sort Descending [column name]".

Ascending column sort is denoted by an upward arrow:

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

1. **Double click on the first column heading**, e.g., “Filename”.
2. **Hold down the SHIFT key** on the keyboard.
3. **Double click on the second column heading**, e.g. A “1” will appear for “Filename” and “Path” a “2” to indicate that it is the second column in the sort.
4. Continue to add columns to the sort by following steps 2 to 3 above. (Maximum of 5 columns)

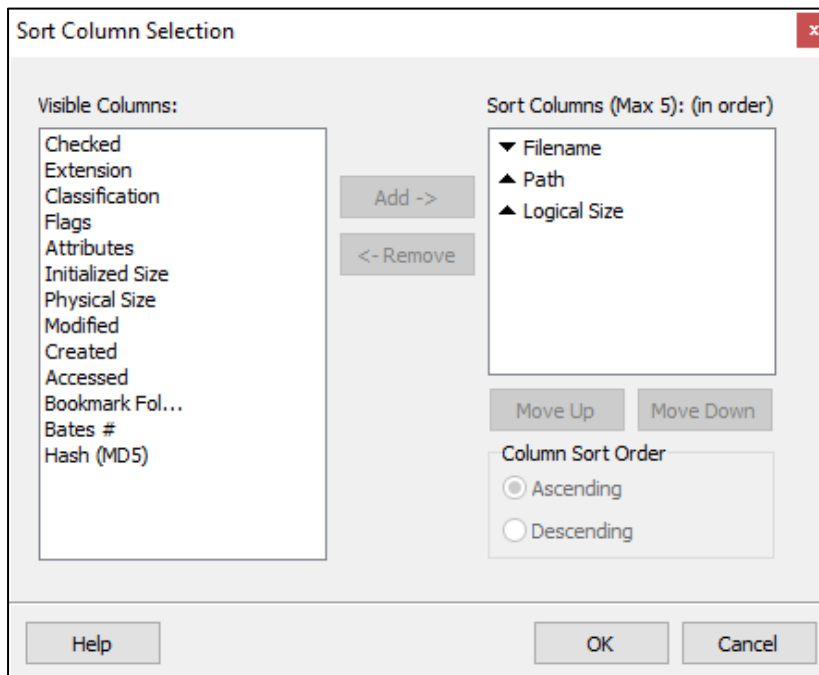
Figure 151: Sort multiple columns by Filename, then Full Path, then Logical Size



A multi column sort can also be achieved by right clicking within the column on a filename:

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

Figure 152: Multi column selection window



Visible columns are shown in the left-hand window:

1. Select the required sort columns.
2. Add the required sort columns to the right-hand window.
3. Use the “Move Up” and “Move Down” buttons to set the order on which to sort the columns.
4. Choose Column Sort Order of “Ascending” or “Descending”.
5. Click the “OK” button to apply the sort.

Persistent Sort:

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

To remove a multi column sort:

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

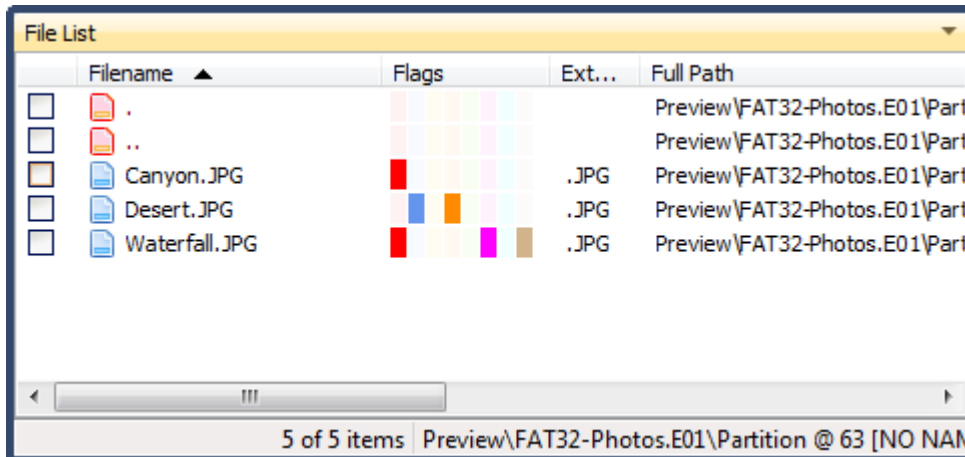
To remove all sorting,

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

9.11 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 153 below:

Figure 153: Flagged items

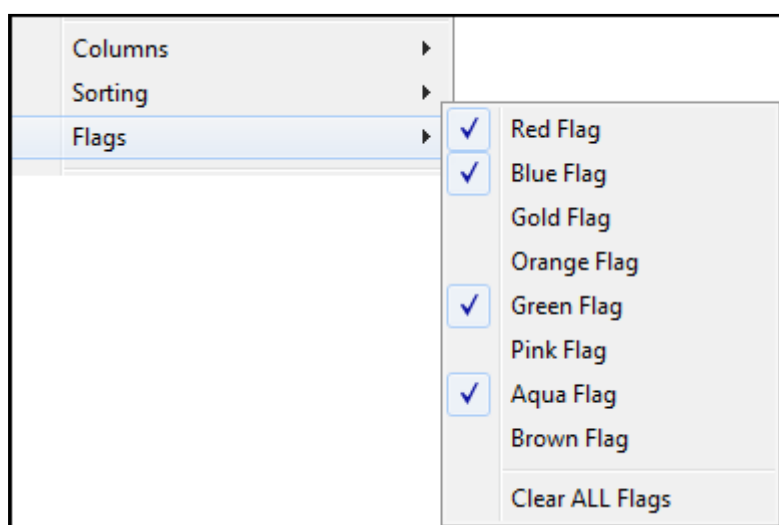


To apply a flag:

1. **Highlight an item** in a List view.
2. **Double click the opaque flag color** in the flag column (if the flag column is not visible add the column - see paragraph 9.4 - Columns); **or**,

Right click and use the “**Add Flag**” menu to place a selection tick next to the required flags, as shown in Figure 154 below:

Figure 154: Right click “Flags” menu option.

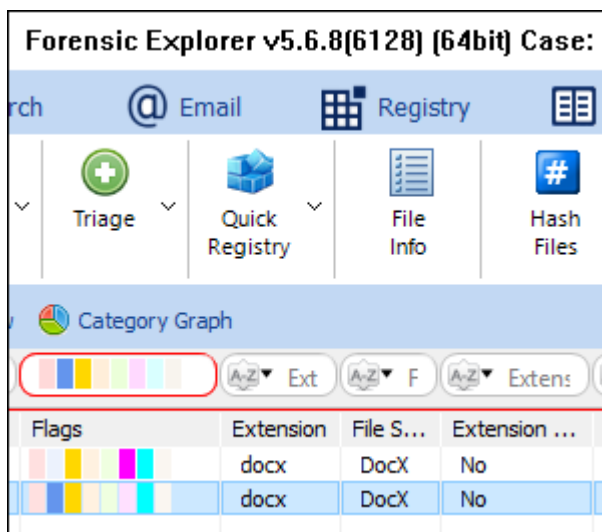


To apply flags simultaneously to multiple items:

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

To **filter flags** (version 5.6.8(6128) and above), use a single click to highlight the flag color in the column header:

Figure 155: Filter 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.

9.12 FILTERING DATA

9.12.1 DATE RANGE FILTER

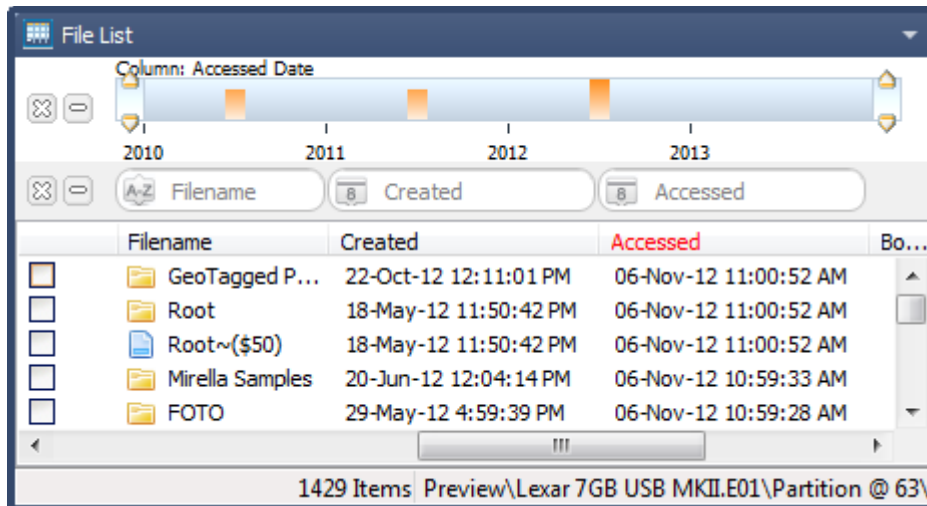
The **Date Range filter tool** is applied to the items displayed in a list view and allows filtering by Created, Modified, and Accessed dates.

To access the **Date Range filter tool**:


1. Right click on a List view window.
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 156 below.

Figure 156: Date filter tool



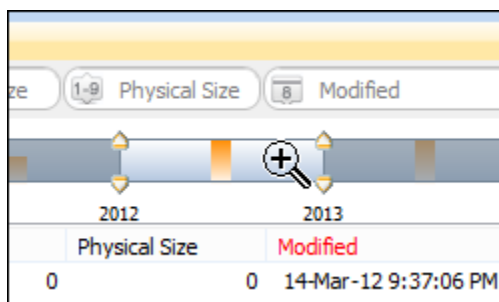
The applied filter column is displayed in red (e.g., “Accessed”).

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

To apply a date filter:

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

Figure 157: Application of date range sliders



To **modify the time scale**, when the magnifying glass with plus sign is displayed (see Figure 157 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.

9.12.2 COLUMN FILTER TOOL

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




A lock has been placed on the 'X' icon of the Column Filter Tool to stop accidental removal.

Additional options of Blank and Not Blank have been added to the drop-down menu. This assists where a column is not fully populated with data, e.g., metadata.

To access the **column filter tool**:

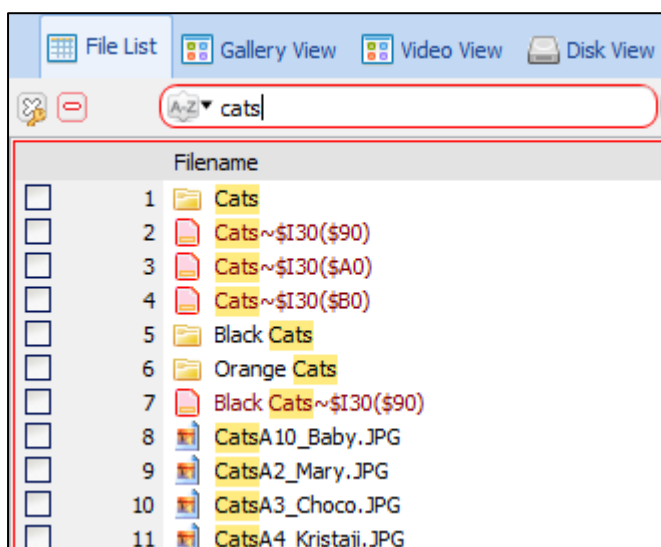
1. Right click on a List view window.
2. From the drop-down menu, select "Column Filter Tool":
3. The text filter then appears above the List view column headings, as shown in Figure 158 below.

To **apply a column filter**:

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


When the filter is applied, the outline of the filter box/s turns red in color, as shown in Figure 158 below.

Figure 158: 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.

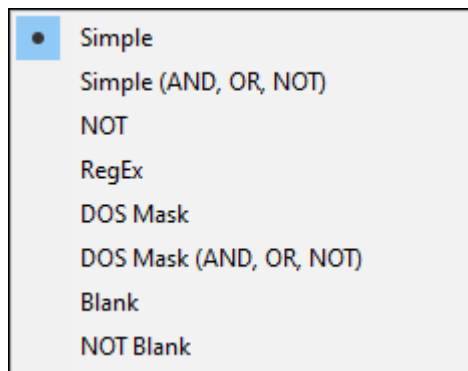
A lock has been placed on the 'X' icon of the Column Filter Tool to stop accidental removal.

Additional options of **Blank** and **Not Blank** have been added to the drop-down menu. This assists where a column is not fully populated with data, e.g., metadata.

COLUMN FILTER: SIMPLE

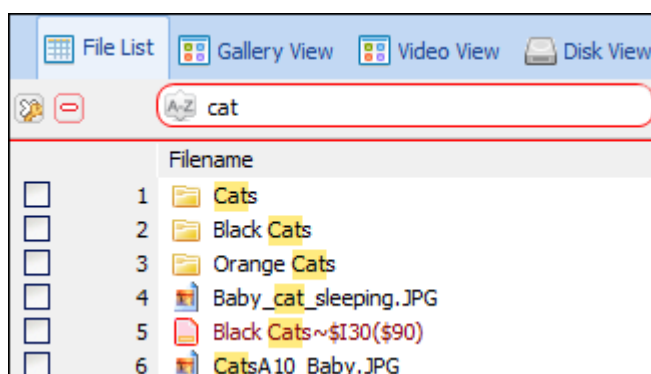
Simple returns the exact text entered:

Figure 159: Text filter search options



Exact text match finds all items containing the entered text:

Figure 160: Simple search for items containing 'cat'

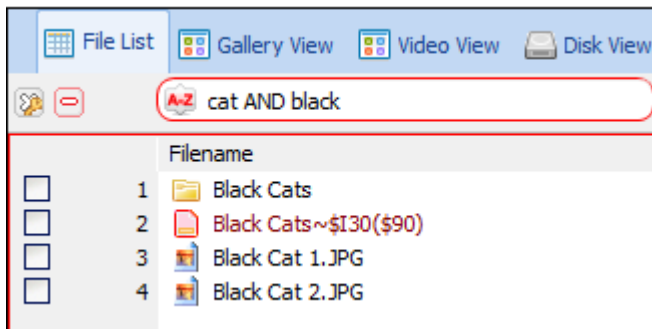


In Forensic Explorer version 5.4.8.2036 and above the addition option of **Simple (AND, OR, NOT)** is added as an additional search option. This adds Boolean search logic to a Simple search. The Boolean operators are **OR, AND, NOT, ()**. For example:

The simple search '**cat AND black**' returns:

- All items that contain the word 'cat', AND
- All items that contain the word 'black'.

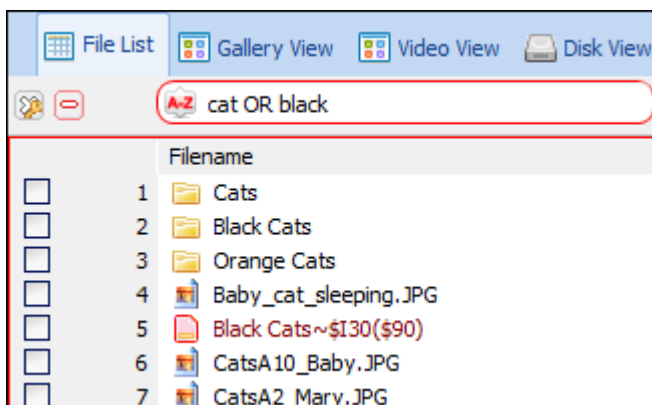
Figure 161: Simple with AND



The simple search '**cat OR black**' returns:

- All items that contain the word 'cat', OR
- All items that contain the word 'black'.

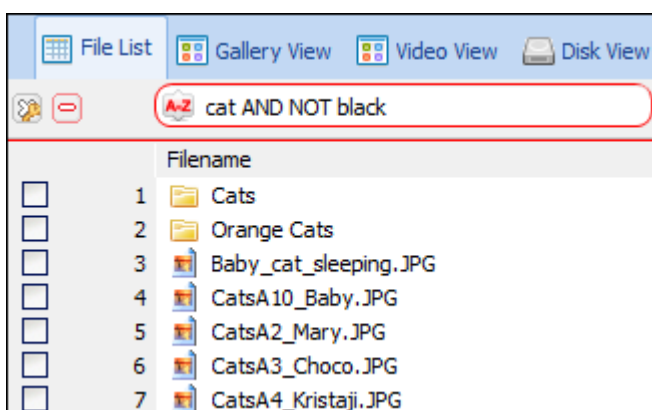
Figure 162: Simple with OR



The simple search '**cat AND NOT black**' returns:

- All items that contain the word 'cat'.
- **AND NOT** items that contain the word 'black'.

Figure 163: Simple AND NOT



For more complex joining of the operators use brackets. For example:

(cat OR dog) AND NOT (black OR orange)

COLUMN FILTER: 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 164 below:

Figure 164: NOT column filter active



COLUMN FILTER: REGEX

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

Figure 165: RegEx column filter



RegEx quick start guide:

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

COLUMN FILTER: DOS MASK

File masks consist of any combination of three general symbol 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.

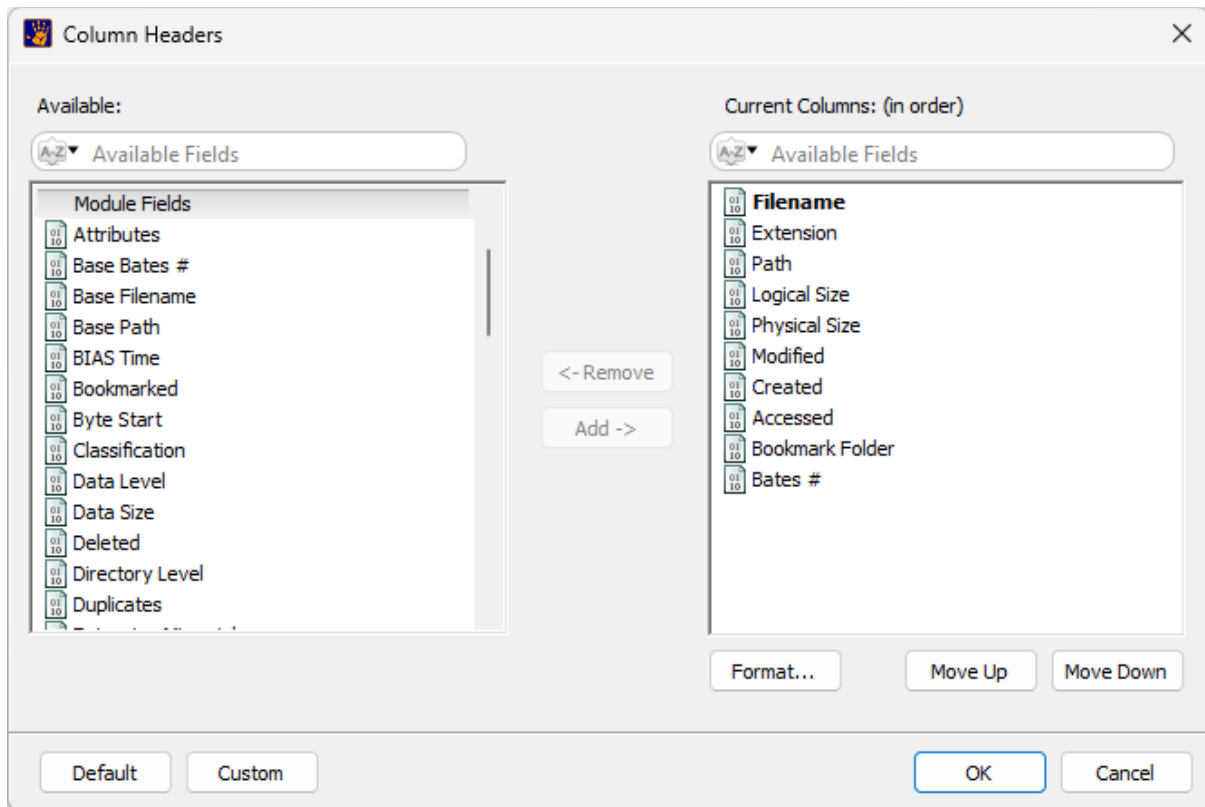
***e.jpg** Refers to all .jpg files that start with h, end with e, and contain any number (including zero) in between, matching:

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

DOS Mask (AND, OR, NOT) adds Boolean logic **OR, AND, NOT, ()** to DOS Mask statements. See 'Simple (AND, OR, NOT)' above.

9.12.3 COLUMN SELECTION

Manage columns (see Custom Columns for more detail):



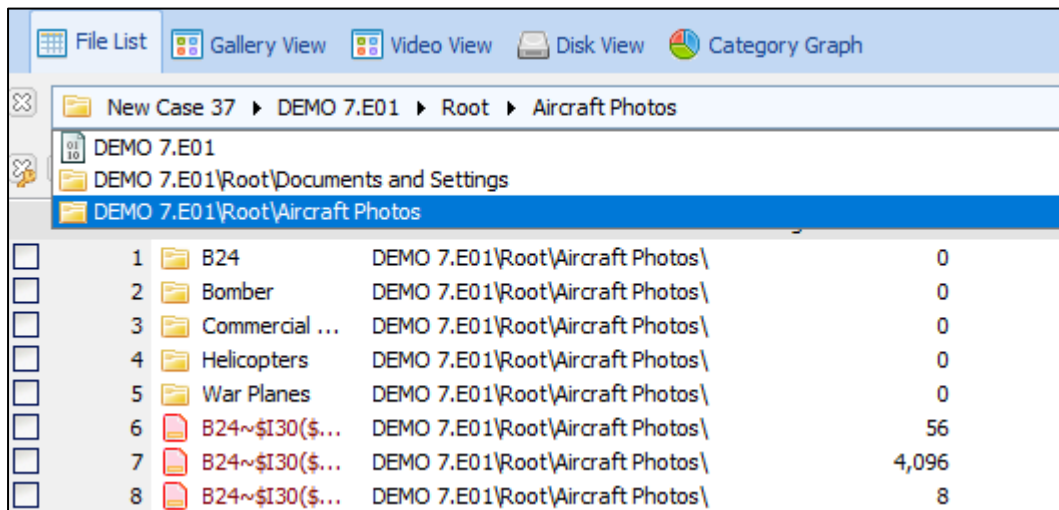
9.12.4 EXPLORER TOOL

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 166: Explorer Tool below.

Figure 166: 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.

9.12.5 FOLDERS FILTER

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

9.13 COPY ROWS TO CLIPBOARD

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

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

Chapter 10 - Evidence Module

In This Chapter

CHAPTER 10 - EVIDENCE MODULE

10.1	Preview	167
10.2	New case.....	168
10.2.1	Managing Investigators	170
10.3	Open an existing case	171
10.3.1	Recent cases	172
10.4	Adding evidence	172
10.4.1	Adding a Device	173
10.4.2	Adding a Remote Device.....	174
10.4.3	Adding a Forensic image	177
10.4.4	Adding a corrupt forensic image	179
10.4.5	Adding a registry file	180
10.4.6	Add file.....	180
10.4.7	Add folder	180
10.4.8	Credentials.....	180
10.5	Evidence Processor	182
10.5.1	Processor tasks	182
10.5.2	Adjust Time Zone	186
10.6	Adding additional evidence to a case	187
10.7	Saving a case.....	188
10.7.1	Auto Save.....	189
10.7.2	Saving or closing a preview.....	190

10.8 Closing a case.....190

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 file**:

- 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 needs only be set once.

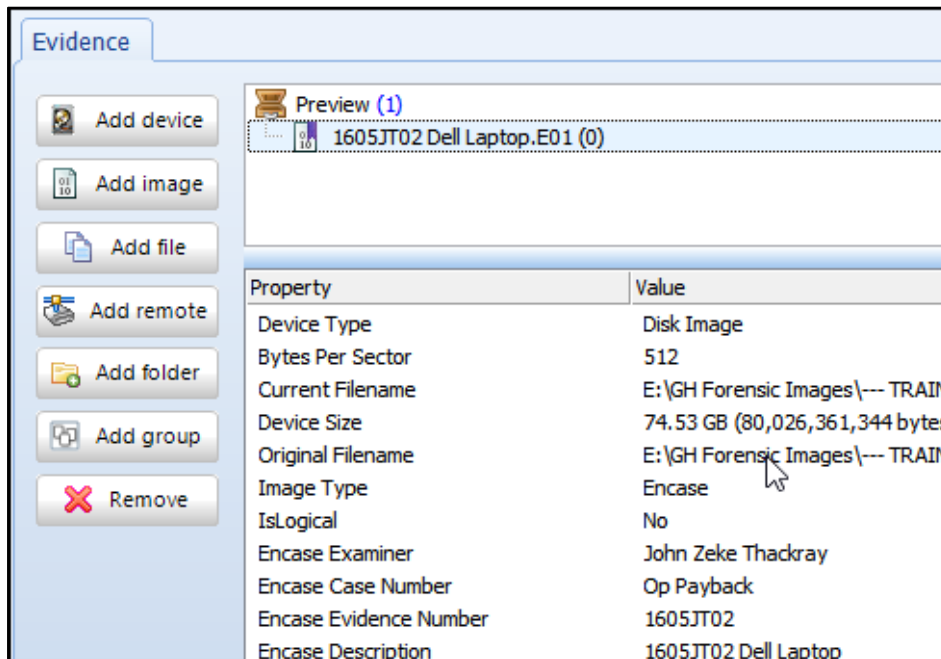
Figure 167: Preview button in the Evidence module



When the preview button is clicked:

- A unique preview working folder is created using a Global Unique Identifier (GUID) in the following path: **C:\Users\Graham\Documents\Forensic Explorer\Previews\{GUID [e.g., 8709A41C-38B6-4F9E-BA18-633B394721C5]}**.
- The evidence window in the Evidence module identifies that a preview is in progress with the words **"Case: Preview"**. The Add 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 168 below:

Figure 168: Evidence Tree in the Evidence module identifying a “Preview.”



For information on adding evidence to a preview, see “10.4 Adding a Device”.

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 169: Evidence module, new case button



New Case

The “New Case” window will open, as shown in Figure 170 below:

Figure 170: New Case window

The screenshot shows a 'New Case' dialog box with the following fields and controls:

- Case Name:** Case 123
- Investigator:** Graham Henley (dropdown), with 'New...' and 'Edit...' buttons.
- Cases Folder:** C:\Users\Owner\Documents\Forensic Explorer\Cases (text field with folder icon)
- Case Notes:** This is a test case. (text area)
- Case Time Zone Settings:**
 - Time Zone:** Local Time (dropdown)
 - Time Zone Name:** AUS Eastern Standard Time (-600 mins) (text field)
 - Daylight Savings:** AUS Eastern Daylight Time (-660 mins) (text field)
 - STD/DLS Bias:** -600 / -660 minutes (text fields)
- Case Created:** 30-Dec-16 10:40:45 AM (text field)
- Buttons:** OK, Cancel

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.

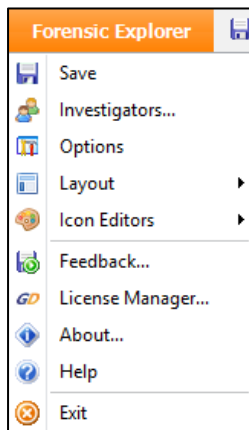
Case Created identified the date and time that the case is created per the local system clock.

Click **OK** in the **New Case** window to create the case. Working folders for the case are written (see “Working Path” page 36) 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 172.

10.2.1 MANAGING INVESTIGATORS

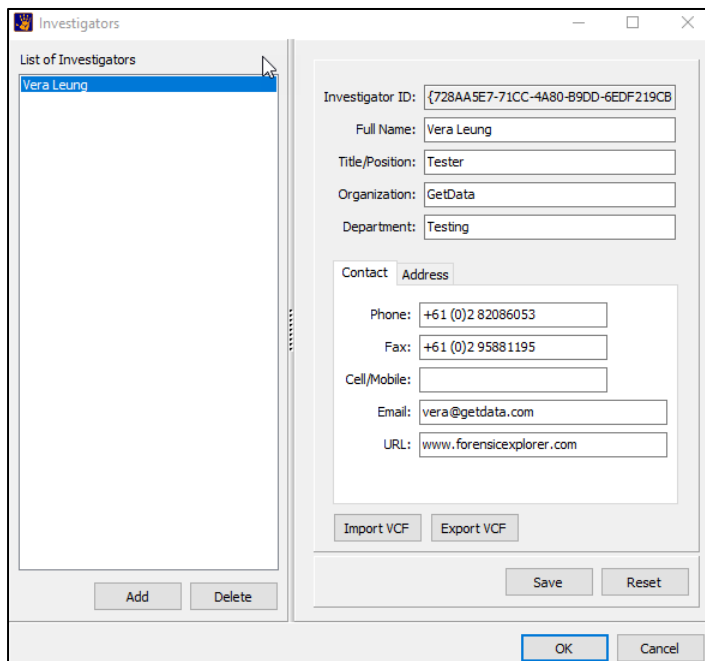
To **add**, **edit** or **delete** an investigator, select “Investigators” from the Forensic Explorer drop-down menu:

Figure 171: Forensic Explorer drop-down menu.



Select and edit the investigator as needed:

Figure 172: 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,

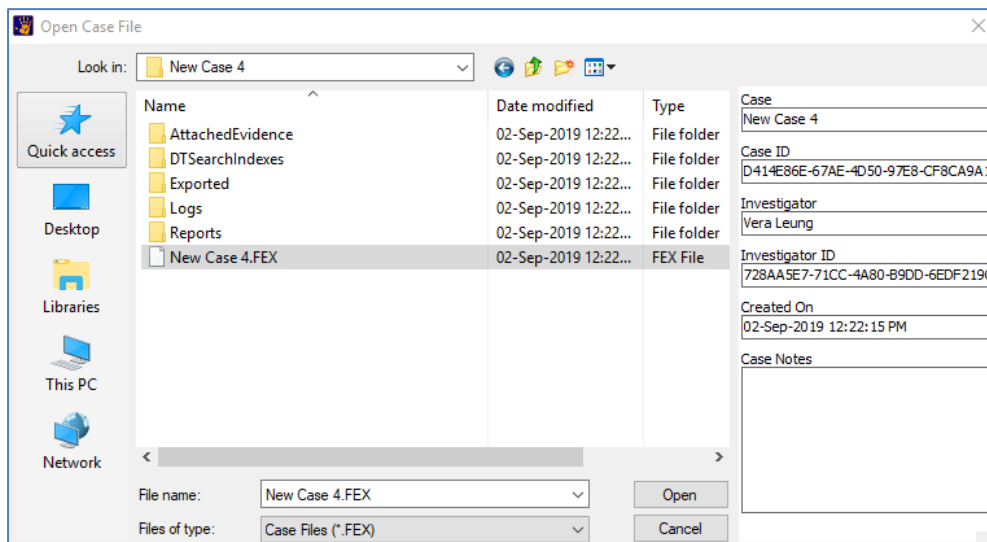
1. Click the **Open** button in the **Evidence module**:

Figure 173: Evidence module, new case button



This will open the “Open Case File” window. When a **.case** file is highlighted the meta-data for that case is displayed on the right-hand side of the Open Case File window (shown in Figure 174 below). Click **Open** to open the case file.

Figure 174: Open Case File



2. The **Select Investigator** window opens so that the person who is about to 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 175, Select investigator window.



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

10.3.1 RECENT CASES

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

When a recent case is highlighted in the Recent Cases list, the “case description” entered when the case was created will be displayed in the description field, as shown in Figure 176 below:

Figure 176: Evidence module > Case’s tab, Open recent cases



The screenshot shows the 'Recent Cases' tab in the Evidence module. It contains two main sections: a list of recent cases and a detailed view of the selected case.

Case	Details	Age
Name:	New Case 44	
Investigator:	Vera Leung	Less than
Created:	16-Sep-2019 11:35:01 AM	1 minute
Name:	New Case 43	
Investigator:	Vera Leung	33 mins
Created:	16-Sep-2019 11:02:17 AM	

Property	Value
Case Name	New Case 44
Case Path	C:\Users\Vera\Documents\Forensic...
Investigator	Vera Leung
Created	16-Sep-2019 11:35:01 AM
Age	Less than 1 minute
Case Notes	This is a test case

10.4 ADDING EVIDENCE

Evidence in Forensic Explorer can be:

- A device (including a remote device).
- A forensic image.
- A registry file.
- A file.

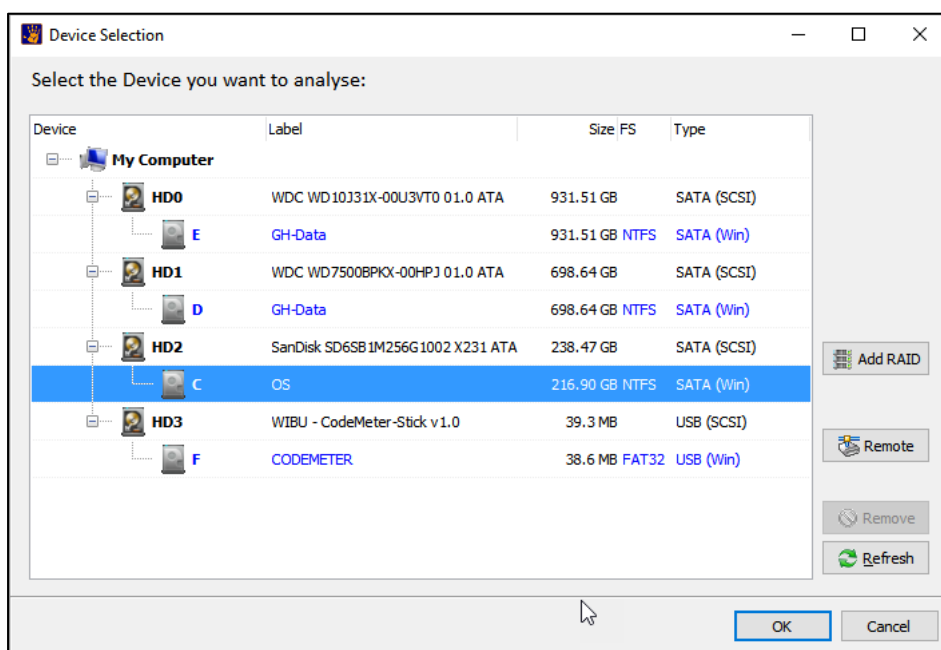
10.4.1 ADDING A DEVICE

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 show in Figure 177 below:

Figure 177: Device Selection window



The Device Selection window includes the following information:

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

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

1. **Highlight** the required physical or logical device and click **OK**, or.

- 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.

Click OK to add the device. The **Evidence Processing Options** window will open. See 0 - Credentials are case specific. If credentials are used between cases, the Import and Export buttons can be used to save and load them for each case.

- Evidence Processor, below.

10.4.2 ADDING A REMOTE DEVICE

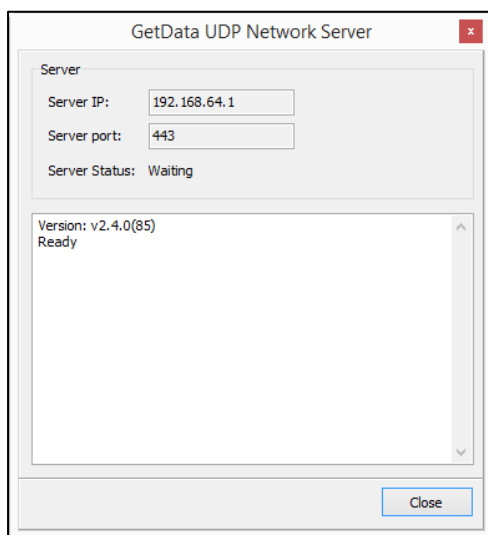
Forensic Explorer has the capability to examine remote devices across a network using the UDP protocol (User Datagram Protocol is one of the core members of the Internet Protocol Suite).

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 178: 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.

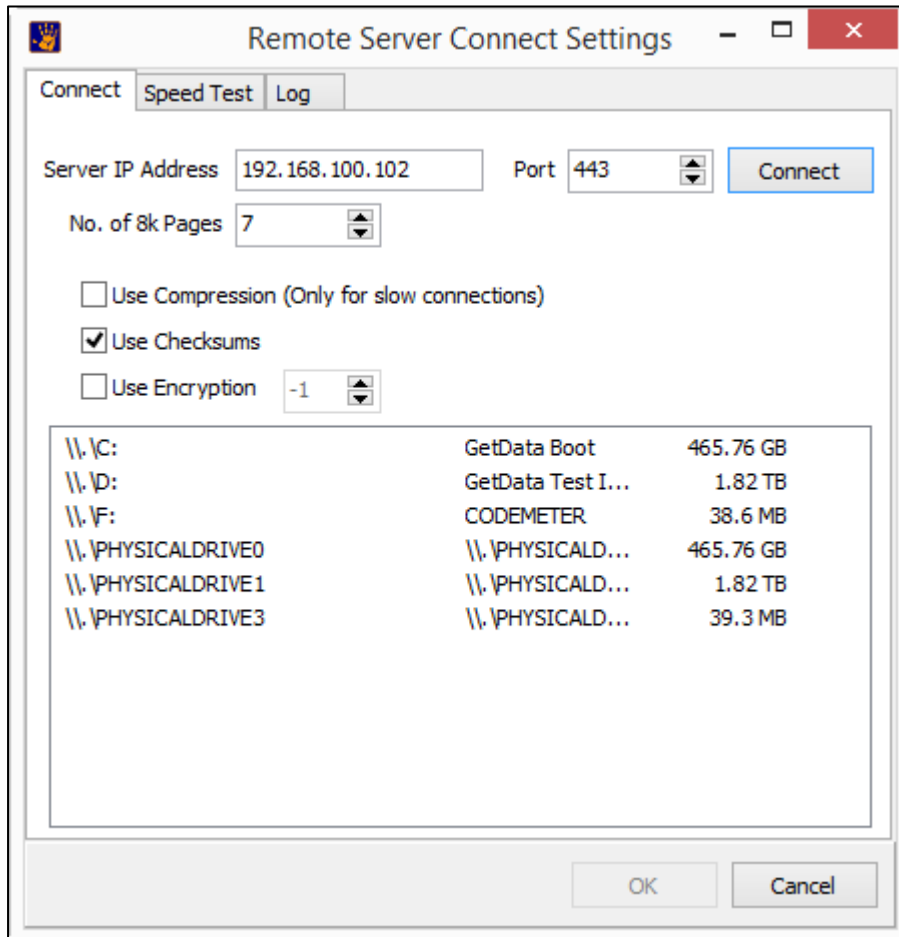
If a non-default port is required (i.e., a port other than 443) the following key must be added to the registry to specify the port number:

```
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:

Figure 179: Forensic Explorer Remote Server Connect Settings



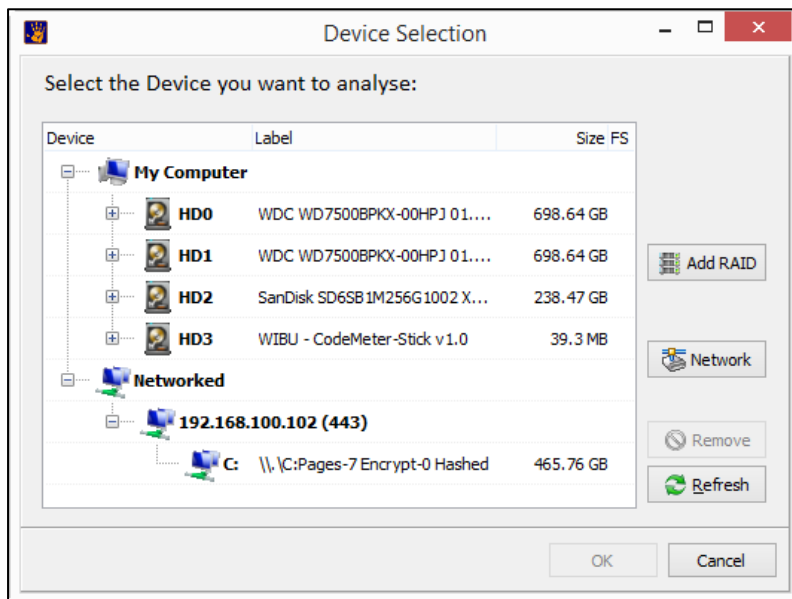
Server IP Address: Enter the IP address of the remote computer as displayed in the **Server IP** field of the GetData UDP Network Server.

Port: Ensure the Port number uses the same port as the GetData UDP Network Server (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 180 below:

Figure 180: Device Selection window showing a UDP connected network device.



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

10.4.3 ADDING A FORENSIC IMAGE

To add an image file to a case:

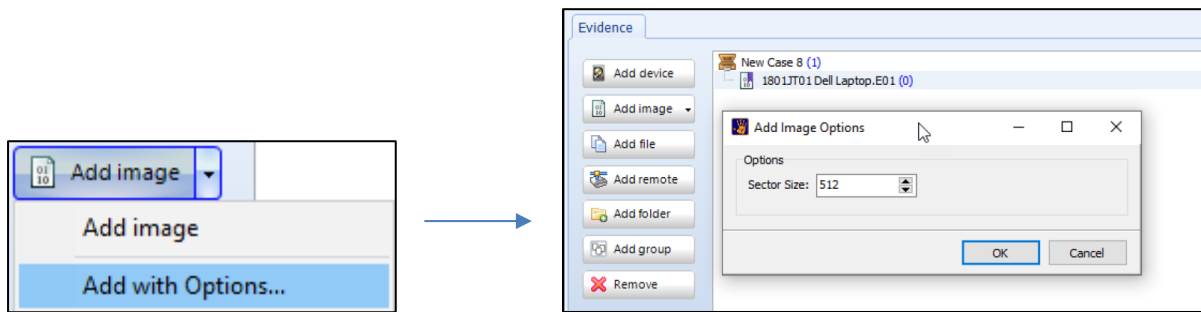
1. Create a preview (see 10.1), a new case (see 10.2), or open an existing case (see 10.3);
2. In the Evidence module, click the **Add Image** button. (If the Add Image button is inactive, click on the case name in the evidence window to activate the buttons).

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 0 below.

A manual sector size adjustment in the Evidence module allows users when adding evidence to manually cater for Advanced Format Drives (512e) with 4096-byte physical sectors which report as 512-byte logical sectors.

This is achieved by selecting **Add with Options** in the drop-down menu in **Add image**:



ADD WITH OPTIONS

There are three common hard drive types that a forensic examiner may encounter:

1. "512" with 512-byte physical sectors reporting as 512-byte logical sectors.
2. "Advanced Format Drives (512e)" with 4096-byte physical sectors which report as 512-byte logical sectors.
3. "4K native" with 4096-byte physical sectors which report as 4096 physical sectors.

How a hard drive is recognized can depend on the third-party device through which it was accessed (e.g., USB hub, write blocker, forensic image hardware). For example, some third-party devices may recognize 512e drives as 512:

"Many host computer hardware and software components assume the hard drive is configured around 512-byte sector boundaries. This includes a broad range of items including chipsets, operating systems, database engines, hard drive partitioning and imaging tools, backup and file system utilities as well as a small fraction of other software applications. In order to maintain compatibility with legacy computing components, many hard disk drive suppliers support Advanced Format technologies on the recording media coupled with 512-byte conversion firmware. Hard drives configured with 4096-byte physical sectors with 512-byte firmware are referred to as Advanced Format 512e, or 512 emulation drives." (https://en.wikipedia.org/wiki/Advanced_Format, accessed 1 August 2019).

"The translation of the 4096-byte physical format to a virtual 512-byte increment is transparent to the entity accessing the hard disk drive. Read and write commands are issued to Advanced Format drives in the same format as legacy drives. However, during the reading process, the Advanced Format hard drive loads the entire 4096-byte sector containing the requested 512-byte data into memory located on the drive. The emulation firmware extracts and re-formats the specific data into a 512-byte chunk before sending the data to the host. The entire process typically occurs with little or no degradation in performance." (https://en.wikipedia.org/wiki/Advanced_Format, accessed 1 August 2019).

In the case where a 512e drive is mis-identified during acquisition, to load the forensic image into FEX it will be necessary to adjust the sector size to correctly parse the file system.

More reading:

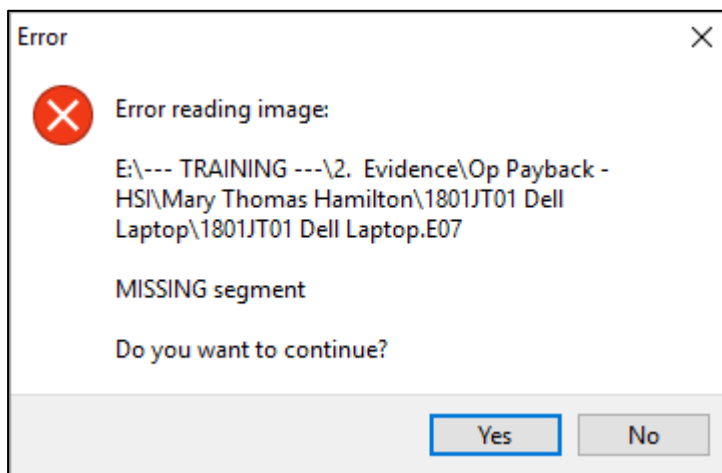
https://en.wikipedia.org/wiki/Advanced_Format

<https://digital-forensics.sans.org/blog/2010/07/28/windows-7-mbr-advanced-format-drives-e512>

10.4.4 ADDING A CORRUPT FORENSIC IMAGE

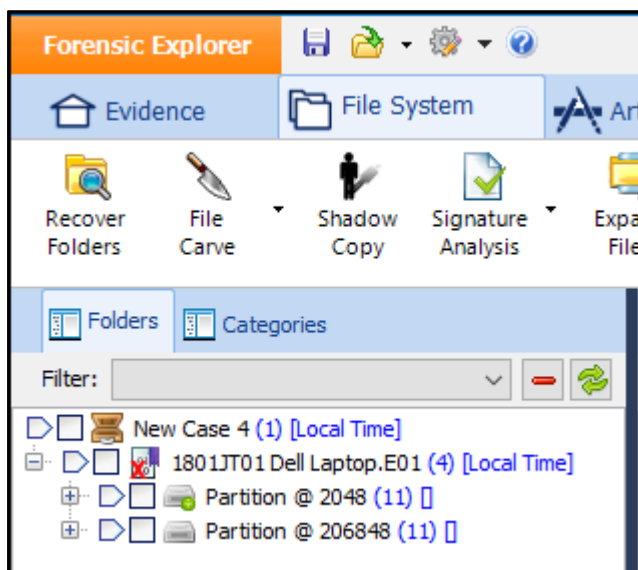
1. During the add image process a validity test for .E01 and .EX01 files is conducted to determine if:
 - a. the image set is complete (i.e., all segments are present); and
 - b. that the image has a valid structure (IMPORTANT: This is validation test only and does NOT replace the need to hash verify).
2. If an error is detected a message box will display:

Figure 181: Invalid image (missing segment)



Clicking the **Yes** button will continue to add the corrupt image. Any missing or corrupt data is replaced by zeros. A corrupt image that has been added to Forensic Explorer is identified by a red X on the image icon, as shown in Figure 182: Icon showing a corrupt image has been added to Forensic below:

Figure 182: Icon showing a corrupt image has been added to Forensic Explorer.



10.4.5 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.

10.4.6 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.

10.4.7 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:

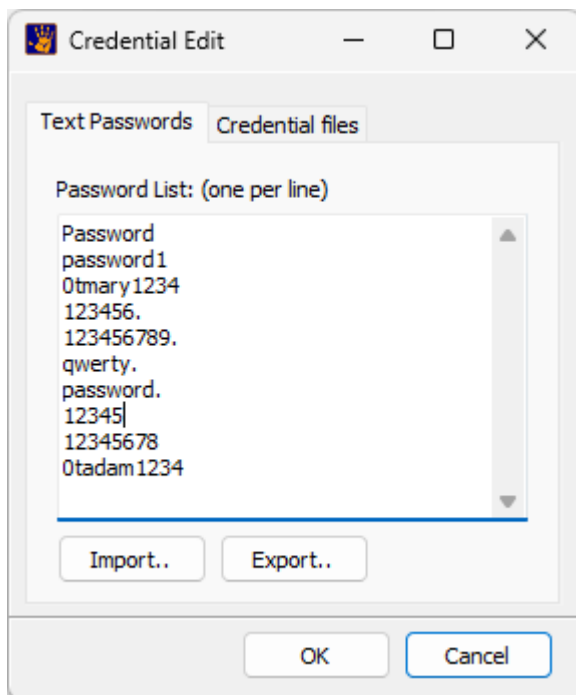
1. Create a preview (see 10.1), a new case (see 10.2), or open an existing case (see 10.3).
2. In the Evidence module, click the **Add Folder** button.
3. In the **Browse to Folder** window, navigate to the required folder and click OK. The Evidence Processing Options window will open. See section 10.5 below. The contents of the selected folder (and subfolders) will be added to the File System module.

10.4.8 CREDENTIALS

The **Credentials** button is a repository for case **BitLocker** and **APFS** passwords and/or credential files. If an encrypted drive is detected Forensic Explorer will cycle through this list to locate the valid password.

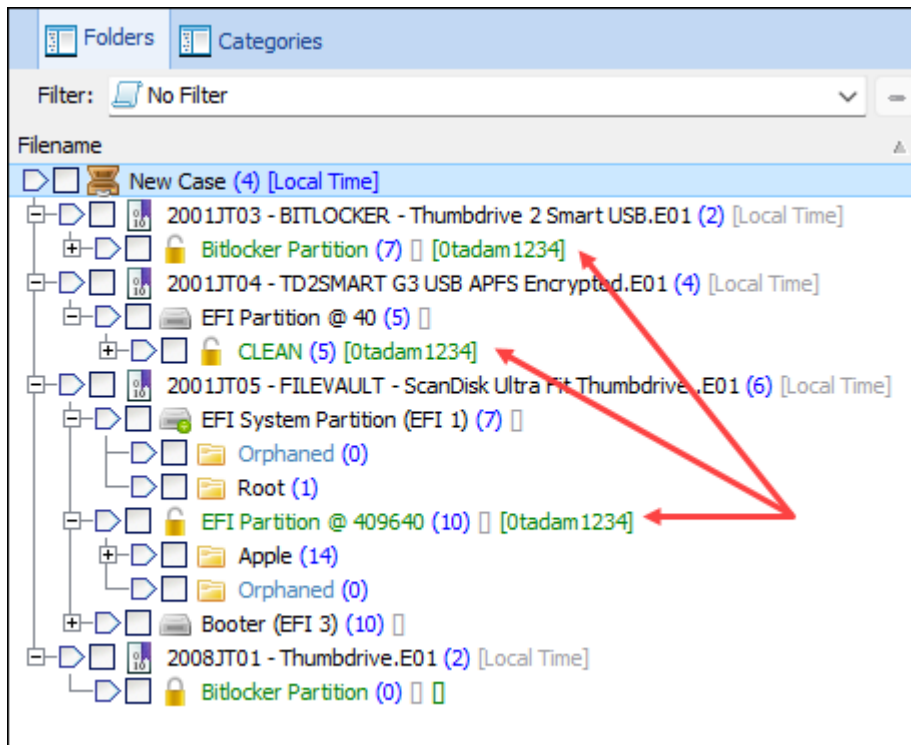
Important: This functionality is not intended for password cracking. Windows will force a delay between password attempts. For speed purposes, it is recommended that no more than **20 passwords** be added to this list.

Figure 183: Credentials Edit.



When an encrypted partition has been accessed using a password, the password is displayed in the tree view, as shown in Figure 184 below .

Figure 184: Encryption Password.



Credentials are case specific. If credentials are used between cases, the Import and Export buttons can be used to save and load them for each case.

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:

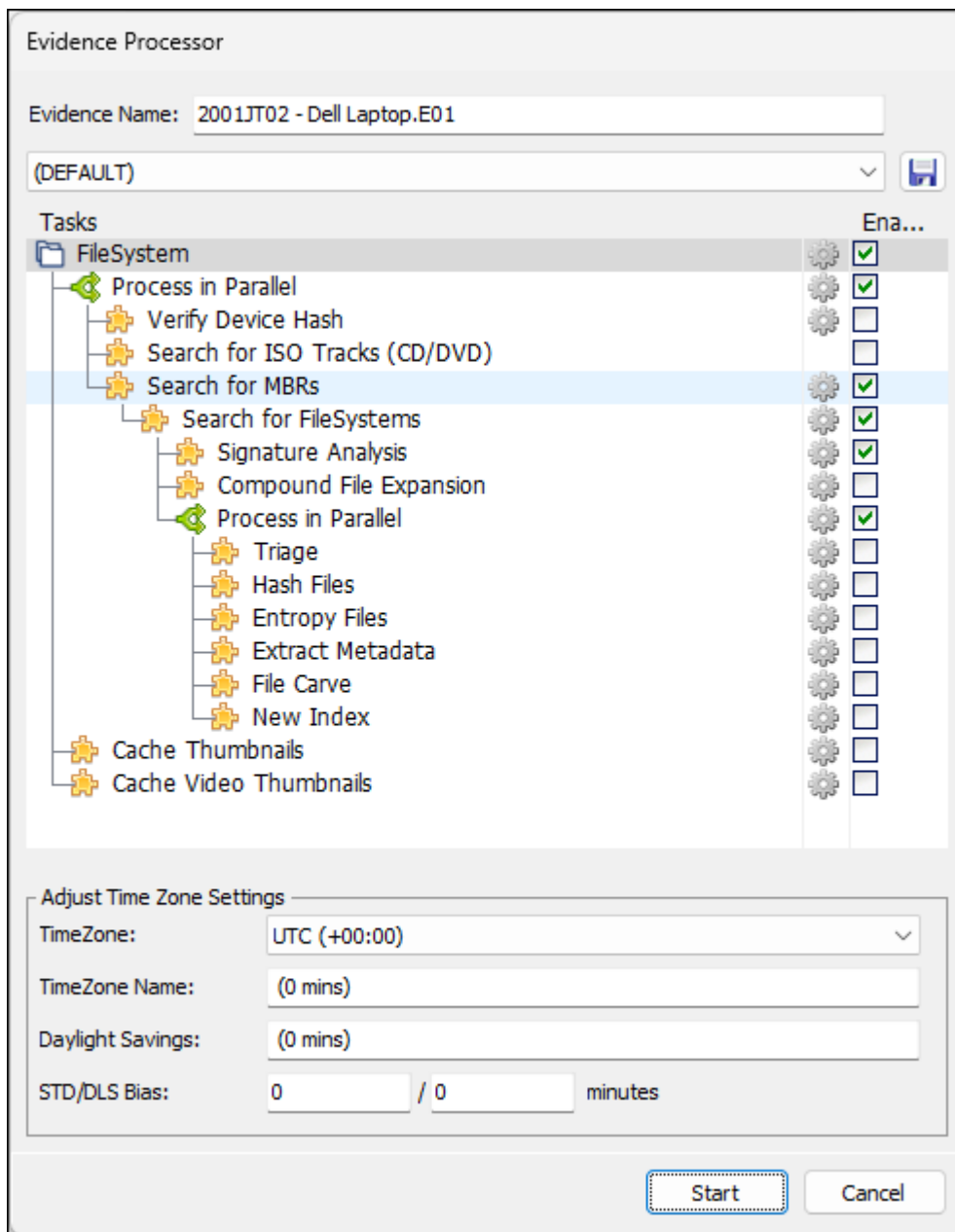
2. To enable the forensic investigator to modify dates and times in the evidence relative to the time zone in which the evidence is situated or was acquired.

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.

Figure 185: Evidence Processing Options (showing options for a forensic image or device)



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 tasks must be completed before a child task can commence.
-  **Process in Parallel:** Identifies that the tasks listed in the immediate sub folder will process concurrently in separate threads.



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



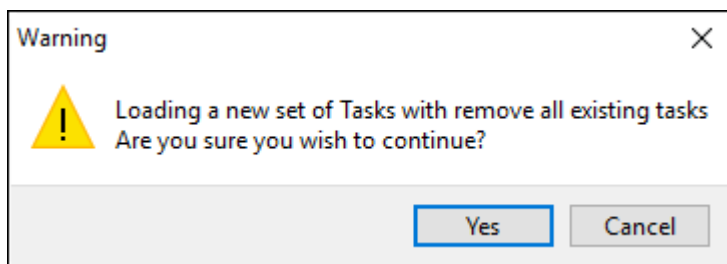
Task options: Identifies those settings for the task must be configured if it is enabled.

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 .xml 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 186: 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 image 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 187 below):

Figure 187: Evidence module, Evidence tab, device hash

Description	LEXAR USB
Notes	This is an EnCase 7 E01 image of a 7gb lexar usb test disk
Acquiring Programm	7.3.1.203
OS Version	Windows 7
Acquired Date	17-May-12 2:25:55 PM
System Date	17-May-12 2:25:51 PM
Compression	Unknown
Password	0
Encase Hash(MD5)	0F88EB0647FF39C1598D76948344BC8B
Hash(MD5)	0F88EB0647FF39C1598D76948344BC8B
Hash(SHA1)	626786505244CCBBBD8FD1C52876A0EC5E105EAF
Hash(SHA256)	C92810E9DB12D4CFDF5FD389F28D4F0DB685E76438C6B...

Acquisition Hash

Verification 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 185 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 185 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.

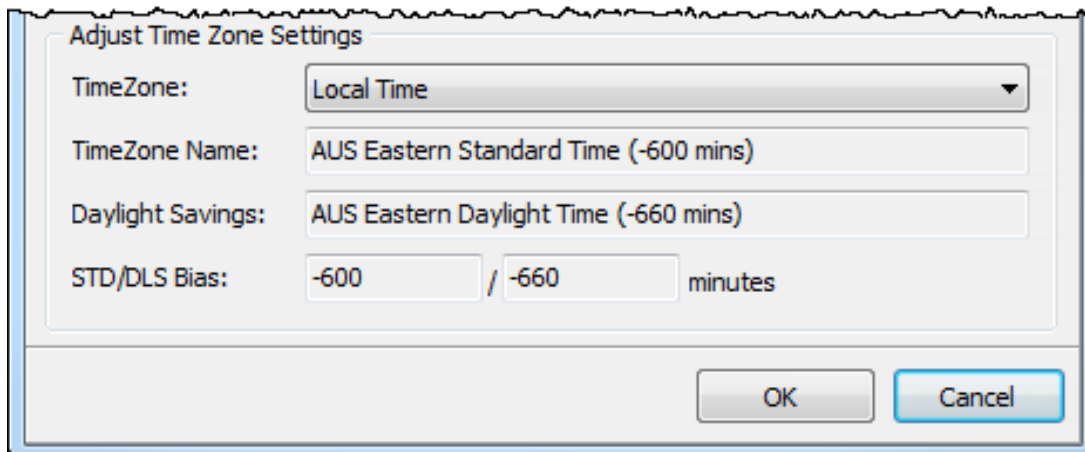
10.5.2 ADJUST TIME ZONE

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 in Coordinated Universal Time (UTC). 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.

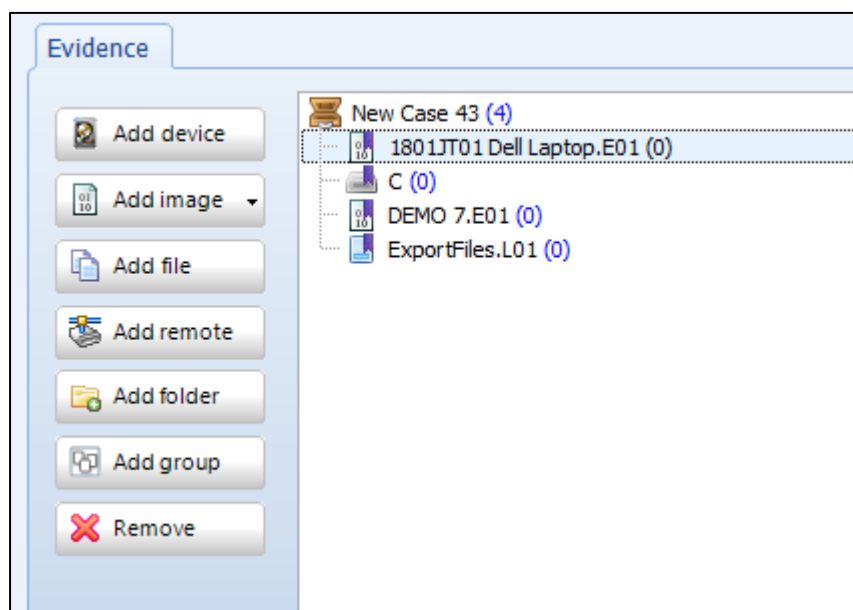
Figure 188: Adjust time zone information when adding evidence.



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 189 below:

Figure 189: Evidence module, Evidence list



To add an additional device, image, or file:

1. Click on the case name (e.g., “Case: New Case 43” 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**:

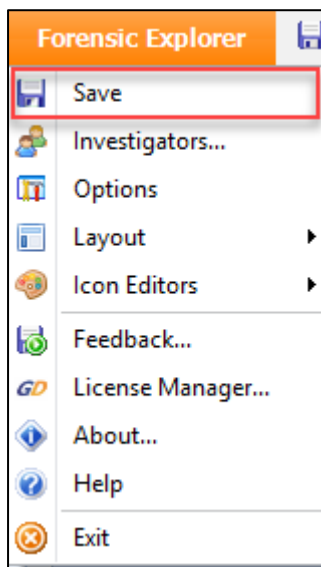
Figure 190: Evidence module, save button.



Or:

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

Figure 191: Save Case.

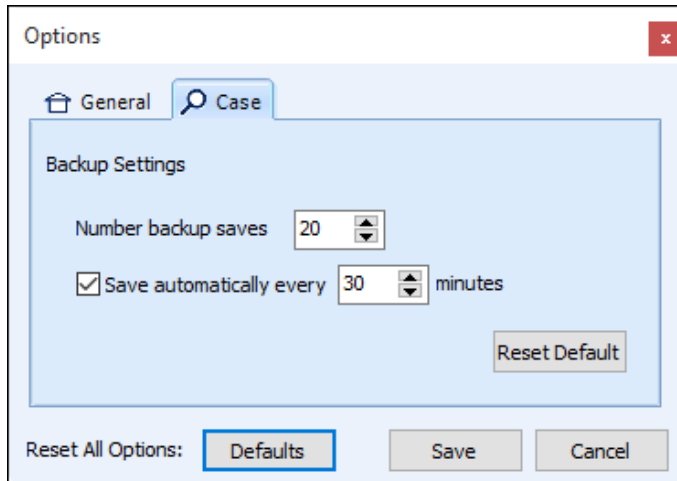


A case should be saved frequently to ensure that any changes from the last save are not lost.

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 192 below:

Figure 192: Setting auto-save options.



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 will be the last successfully written **fe.rsv**.

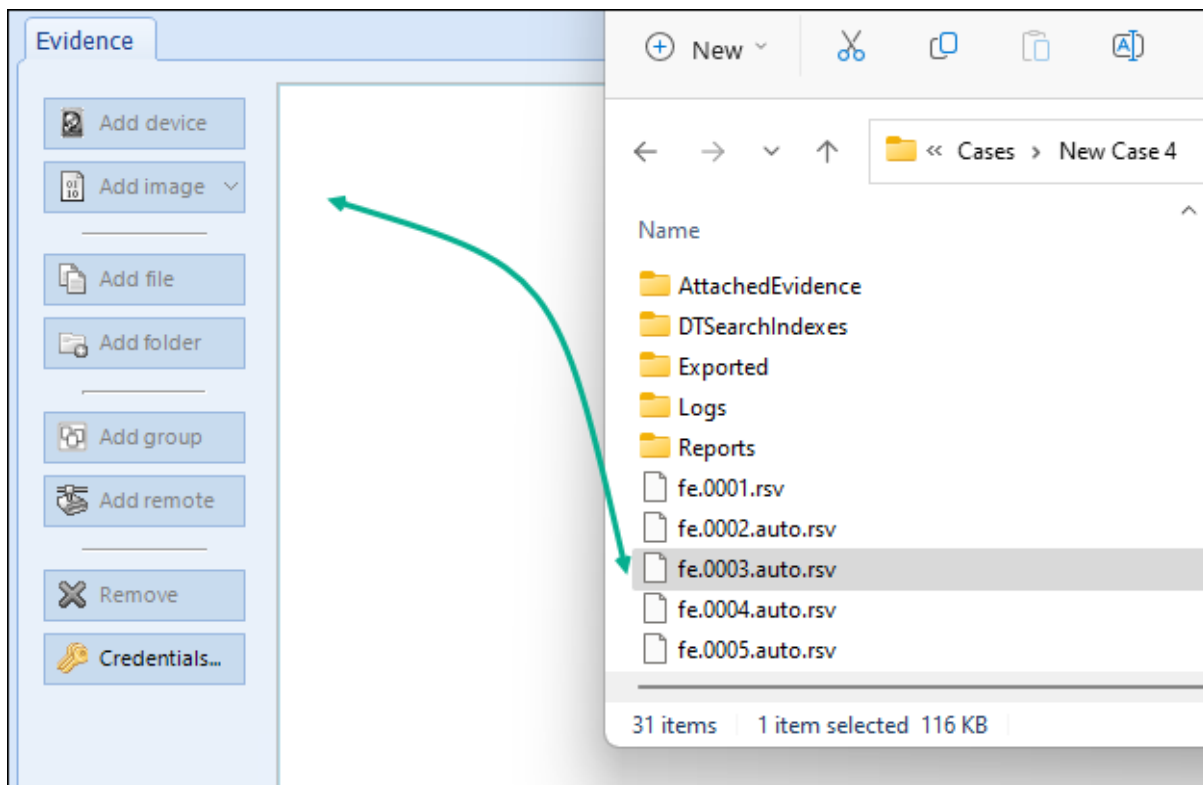
When a successful auto-save takes place, if the previously saved file was initiated by the user (i.e., by pressing the save button) the file is named **fe.0001.rsv**. If the previous saved file was an auto-save the file is backed up as **fe.0001.auto.rsv**.

LOADING A PREVIOUS SAVE

There may be a situation where the investigator needs to load a previous save. To do this:

1. If a case is running, save the current case and consider taking a backup of the current case using the cog icon menu option at the top of the Forensic Explorer window.
2. Close the current case (see 10.8 below).
3. Open the cases folder in Windows Explorer (the default location is `..\Documents\Forensic Explorer v5\Cases\[Case Name]`) and list the **fe.rsv** files described above. Sort by the Windows date/time properties to determine the date and time of the previous saves.
4. Drag and drop the selected **.rsv** file into the top right-hand window of the Forensic Explorer Evidence module. Follow the prompts and the case will open.

Figure 193: Drag and drop a .rsv file to load a previous save.



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

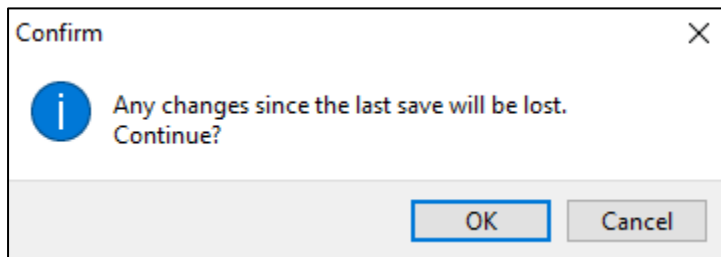
To **close** a preview or a case use the **Close** button in the **Evidence module**:

Figure 194: Evidence module, Close button



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

Figure 195: 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.

Chapter 11 - File System module

In This Chapter

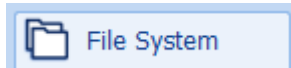
CHAPTER 11 - FILE SYSTEM MODULE

11.1	File System module.....	193
11.2	Toolbar.....	193
11.3	Folders view.....	193
11.3.1	Folders icons.....	194
11.3.2	Orphans.....	195
11.3.3	Filter.....	195
11.3.4	Create drop-down filter.....	195
11.4	Categories view.....	196
11.4.1	Files by Extension.....	196
11.5	File List view.....	197
11.5.1	File List icons.....	197
11.5.2	File List Colors.....	197
11.5.3	File List Metadata Columns.....	198
11.6	Other data views.....	200

11.1 FILE SYSTEM MODULE

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

Figure 196: 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.

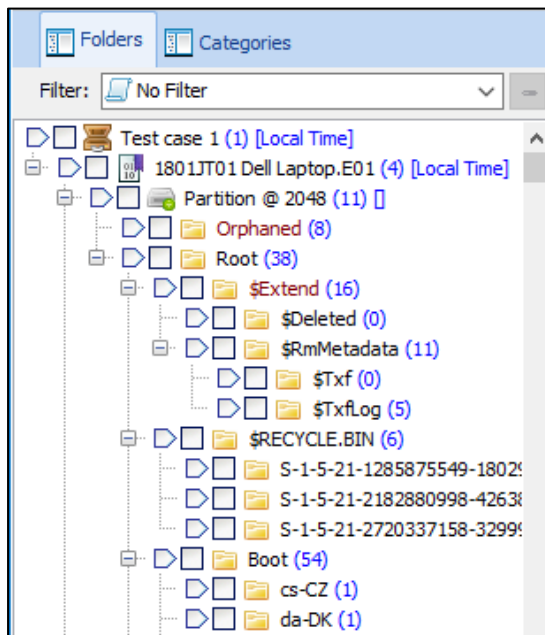
11.3 FOLDERS VIEW

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 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 197: Folders View



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

11.3.1 FOLDERS ICONS

The following icons are used in Folders view:

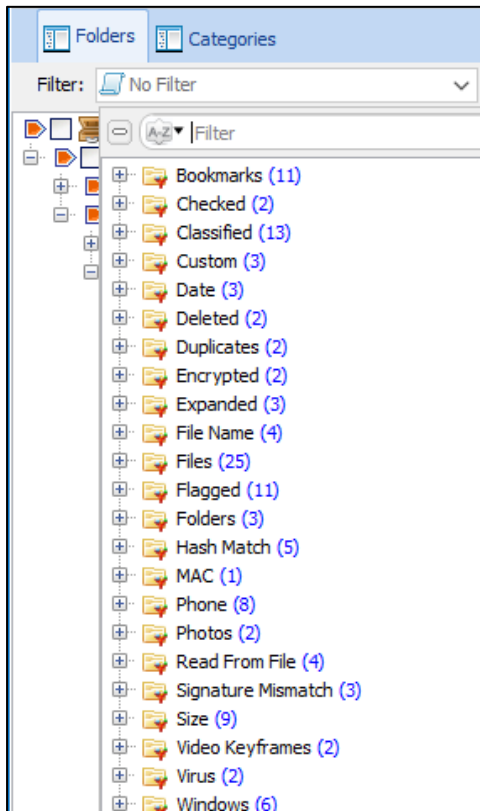
-  “Preview” (indicating a case has not yet been saved) or Case name
-  A device, e.g., a hard drive or camera card
-  A forensic image (the purple flag indicates a bookmark)
-  A corrupt forensic image (the purple flag indicates a bookmark)
-  Boot partition
-  Partition
-  An expandable branch (folder 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 "24.3.2 - NTFS - orphans".

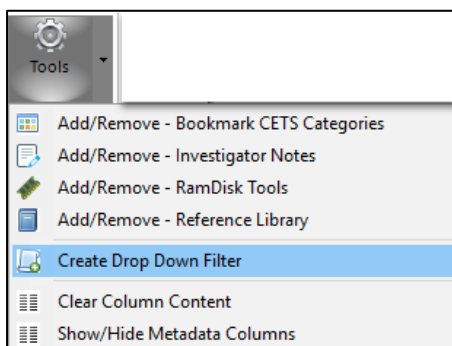
11.3.3 FILTER

The drop-down filter at the top of the folder tree has a number of available filters. A search bar enables fast access via filter name:



11.3.4 CREATE DROP-DOWN FILTER

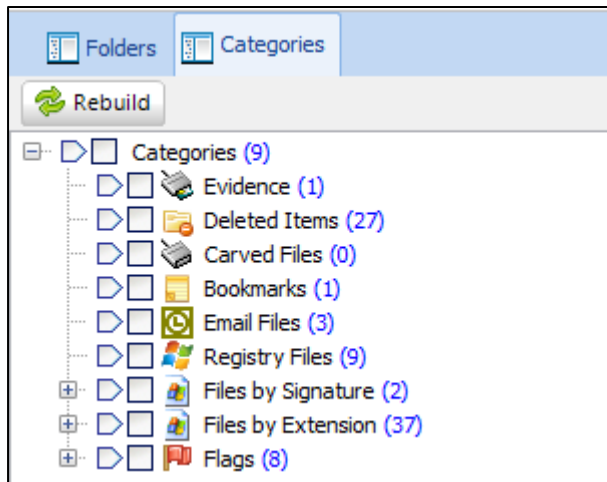
A Create Drop-down Filter script enables custom filters to be added within File System > Tools > Create Drop-down Filter:



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 198: Categories view



Note:

1. 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.
2. 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. Use the “Rebuild” button or right click inside the category view window.
2. Select “Rebuild” from the drop-down menu.

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

11.4.1 FILES BY EXTENSION

Files without extension

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











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

11.5 FILE LIST VIEW

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

11.5.1 FILE LIST ICONS

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

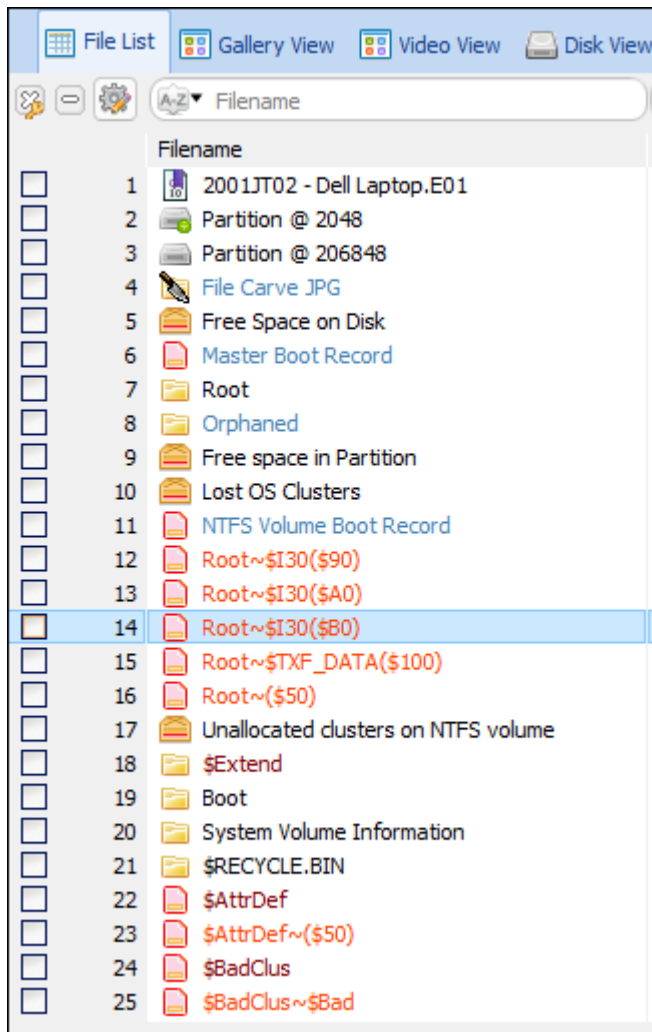
-  Free space on disk
-  Free space in partition
-  Unallocated clusters on NTFS volume
-  An active file
-  An active folder
-  A deleted file
-  A deleted folder
-  A system file
-  A FAT "dot" directory entry
-  A FAT "double dot" directory entry

11.5.2 FILE LIST COLORS

The File List uses the following color to identify specific items (an example is shown in Figure 199 below):

Item:	Black
Operating System Compressed:	Blue
Encrypted:	Green
Expanded:	Purple
Alternate:	WebOrangeRed
System Files:	Maroon
Items displayed by FEX:	SteelBlue

Figure 199: File List colors



11.5.3 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 was 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: <ul style="list-style-type: none"> • 0-5 are normal DOS attributes. • 6-15 are NTFS attributes.

Additional information is available <https://msdn.microsoft.com/en-us/library/aa365535%28v=VS.85%29.aspx> (Other OSs 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


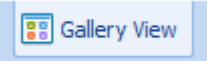
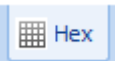
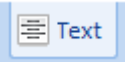
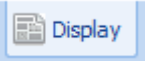
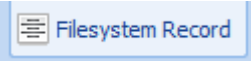
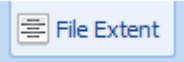


Bit15> 'X' - Other higher flags (not yet determined), but typically are associated with NTFS system files such as \$ObjID etc. that are in the reserved \$MFT area, but also can exist on other files.

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 into columns. See 8.13.1 for more information.

11.6 OTHER DATA VIEWS

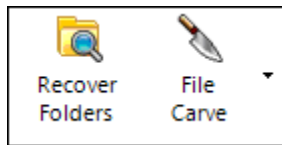
Other data views used in the Files System module includes those summarized in the table below. For more detailed information on each view, see Chapter 8 - Data Views.

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

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 200: 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 201: 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 202: File System module, Cisco Clam Anti-Virus



ABOUT CLAMAV

In 2013, Cisco System acquired the rights to ClamAV (https://en.wikipedia.org/wiki/Clam_AntiVirus, Accessed November 2017). "ClamAV® is an open source (GPL) anti-virus engine used in a variety of situations including email scanning, web scanning, and end point security. It provides a number of utilities including a flexible and scalable multi-threaded daemon, a command line scanner and an advanced tool for automatic database updates". (<https://www.clamav.net/about>, Accessed November 2017). ClamAV documentation is available at <https://www.clamav.net/documents/clam-antivirus-user-manual>.

UPDATING THE CLAMAV VIRUS DATABASE (CVD)

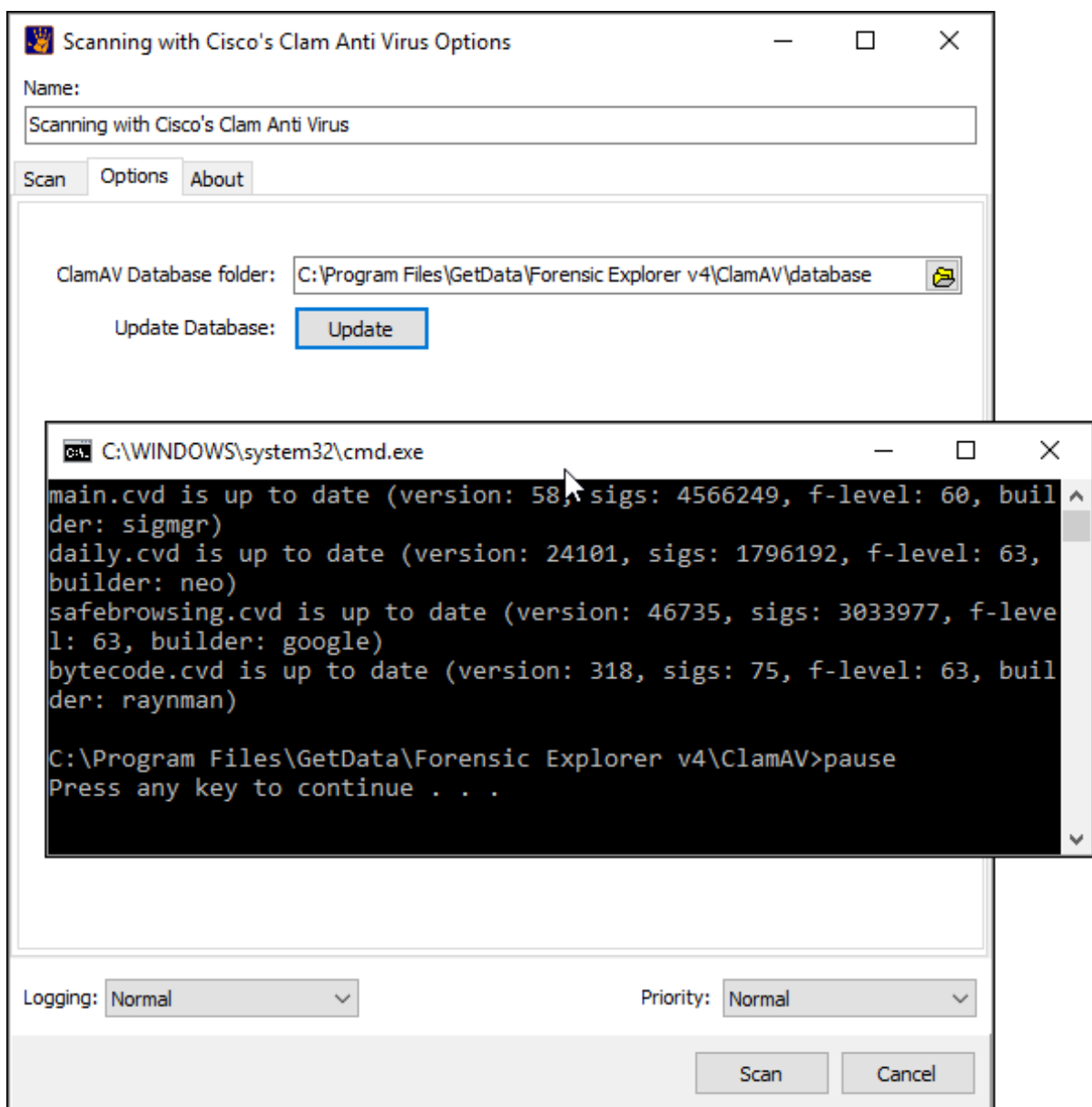
ClamAV Virus Database updates are released daily. It is recommended that these files are updated frequently.

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 and commence download of the latest ClamAV database files, as shown in Figure 203: Update of ClamAV database files below:

Figure 203: Update of ClamAV database files



5. Exit the Command window.

CLAMAV VIRUS DATABASE MANUAL UPDATE

To manually update the ClamAV Virus Database files:

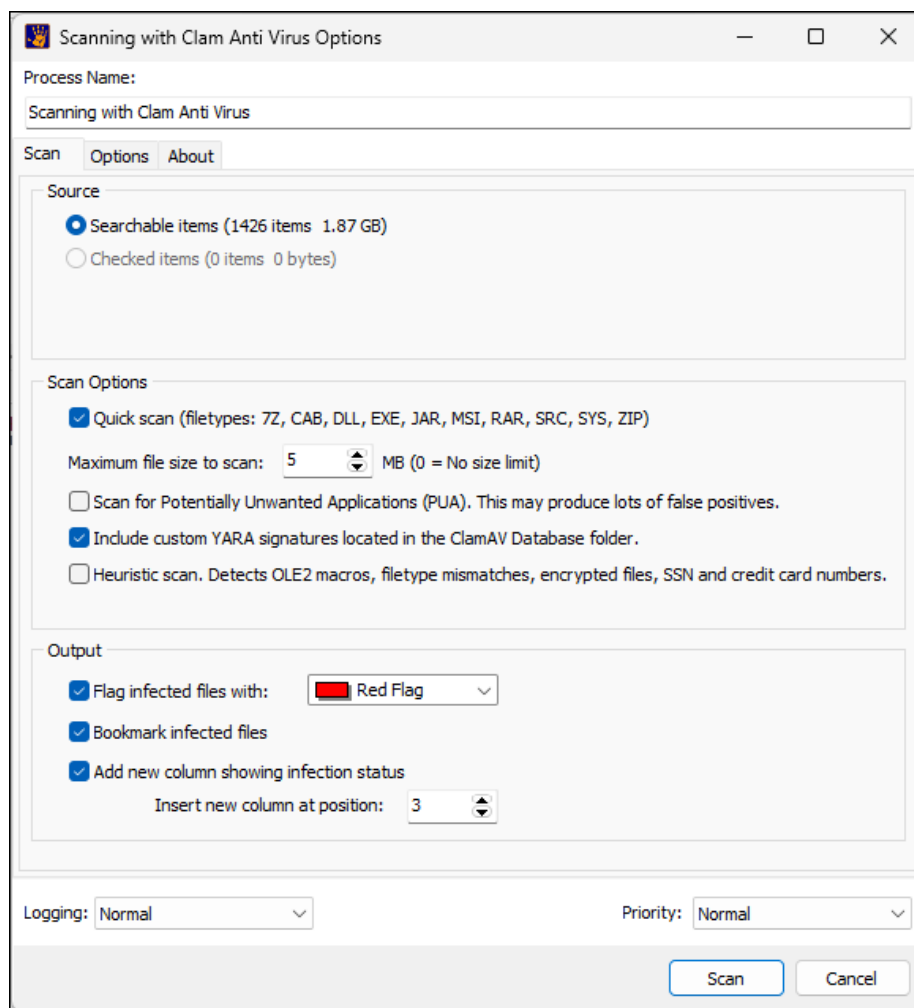
1. Using an internet connected computer, visit the web page: <https://www.clamav.net/downloads>.
2. In the **Virus Database** section, download the **main.cvd**, **daily.cvd** and **bytecode.cvd** files.
3. Copy these files into the **C:\Program Files\GetData\Forensic Explorer v4\ClamAV\database** folder.
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.

Figure 204: ClamAV Virus Scan



3. Select the **Source** files to scan: Searchable items, Highlighted items, Checked items.
4. Set the **Scan Options**.

Quick Scan	Scans common file types. See: https://www.clamav.net/documents/on-access-scanning
Scan for Potentially Unwanted Applications (PUA)	See: https://www.clamav.net/documents/potentially-unwanted-applications-pua
Include custom YARA signatures located in the ClamAV Database folder.	See Custom Yara Signatures below.

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.

YARA SIGNATURES IN CLAM ANTIVIRUS

In Forensic Explorer 5.6.8(4934) Yara has been moved to its own independent function. Please see the section titled Yara Rules below.

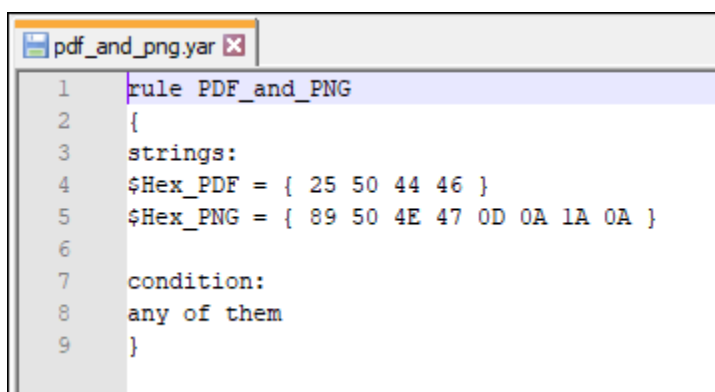
11.7.3 YARA RULES

YARA rules are a powerful and flexible way to identify and classify malware or other types of suspicious files based on specific characteristics or patterns. YARA (Yet Another Recursive Acronym) is an open-source tool primarily used in cybersecurity for malware research and detection.

Yara is “a rule-based approach to create descriptions of malware families based on regular expression, textual or binary patterns. A description is essentially a YARA rule name, where these rules consist of sets of strings and a boolean expression”. (https://en.wikipedia.org/wiki/YARA_-_May_2020).

The following demonstrates the structure of a **sample yara** rule to match against **PDF and PNG files** in a Forensic Explorer case:

Figure 205: Sample yara file (Source: <https://support.phishingtackle.com/hc/en-gb/articles/4410170814609-YARA-Rule-Examples>).



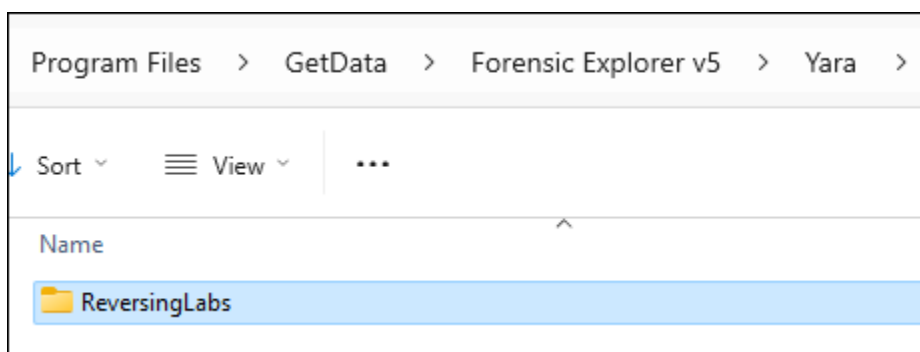
```
1 rule PDF_and_PNG
2 {
3   strings:
4   $Hex_PDF = { 25 50 44 46 }
5   $Hex_PNG = { 89 50 4E 47 0D 0A 1A 0A }
6
7   condition:
8   any of them
9 }
```

Forensic Explorer contains a default selection of open source Yara Rules from **ReversingLabs** (see: <https://www.reversinglabs.com/products/open-source-yara-rules> or [GitHub - reversinglabs/reversinglabs-yara-rules: ReversingLabs YARA Rules](https://github.com/reversinglabs/reversinglabs-yara-rules)).

Yara rules are located by default in the Forensic Explorer installation folder:

...\\Program Files\\GetData\\Forensic Explorer v5\\Yara

Figure 206: FEX Yara folder



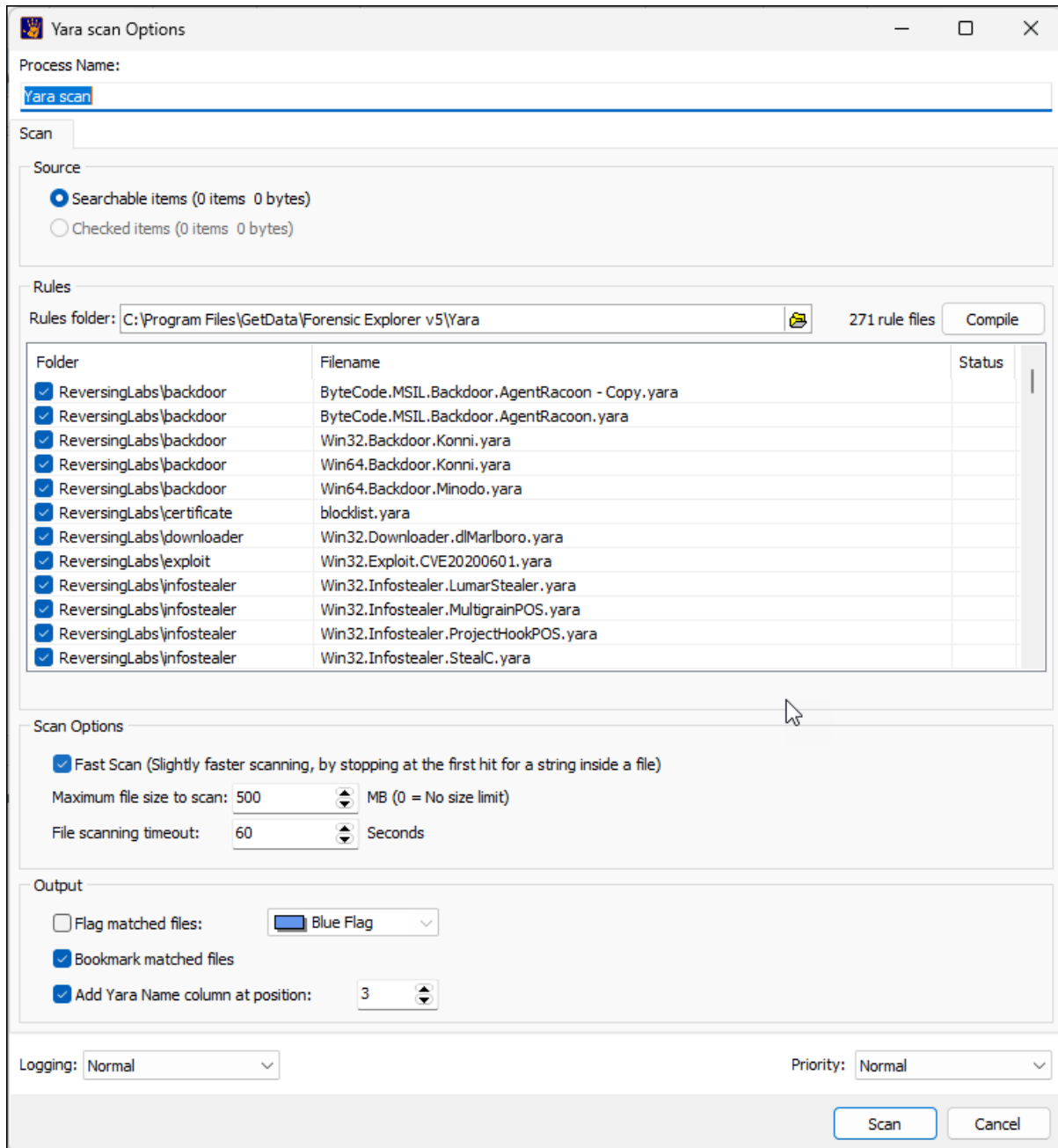
To launch Yara Rules, click on the button in the File System or Email module toolbars.

Figure 207: Yara Rules toolbar button



The Yara scan Options window will appear:

Figure 208: Yara Rules

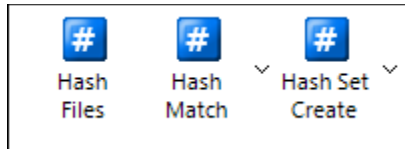


When a file is matched by a Yara rule the matching rule name is written to the **Yara Name** column. The file will also be bookmarked and flag if those settings are active in the Yara scan Options window.

11.7.4 HASHING

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

Figure 209: File System module, Hash buttons



Chapter 12 – Artifacts Module

In This Chapter

CHAPTER 12 – ARTIFACTS MODULE

Artifacts	209
12.1 Artifacts module	209

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”* (10).

A broad-based definition of 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 are 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 than ever before, often spread over multiple devices including phones, tablets and computers.

12.1 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:

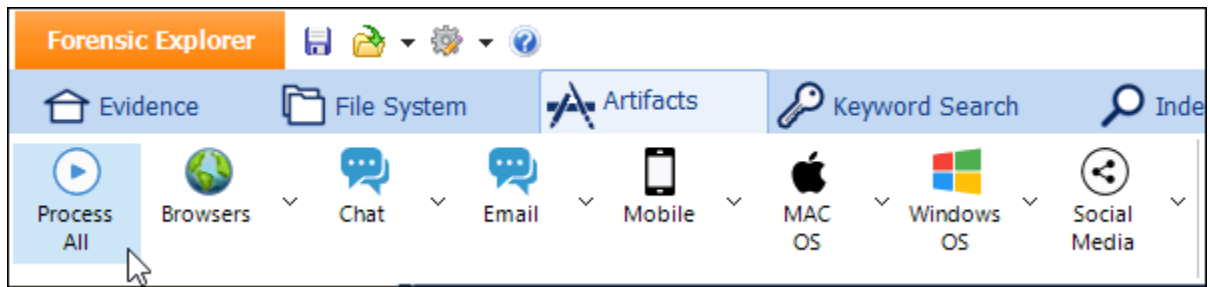
1. Extraction of records from SQLite database files (Forensic Explorer does not currently extract deleted records within SQLite files).
2. Extracting of records from Plist or XML format.
3. Carving data from files or unallocated clusters.
4. Other custom extraction.

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:

C:\Users\user profile\Documents\Forensic Explorer v5\Scripts\Scripts.en\Artifacts

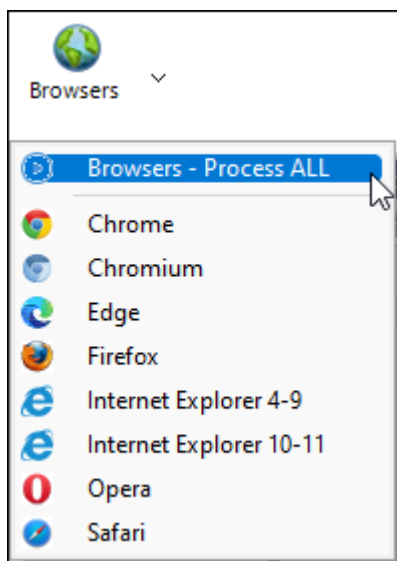
The **Process All** button will run scripts for: Browsers, Chat, Email, Mobile, MAC OS, Windows OS, and Social Media, as shown in Figure 210 below.

Figure 210: Artifacts, Process All button



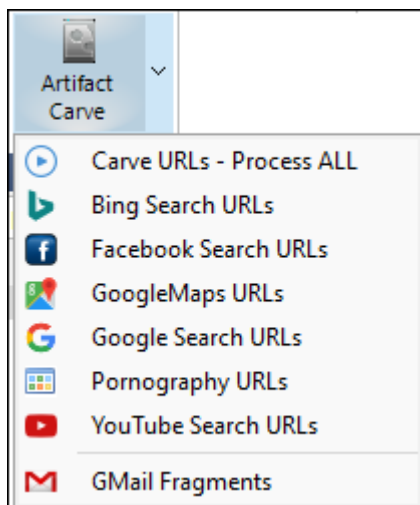
A group of artifact scripts can be run by selecting the **Process All** option for the group, or individual items can be selected from the drop-down menu for each group:

Figure 211: Grouped Artifacts



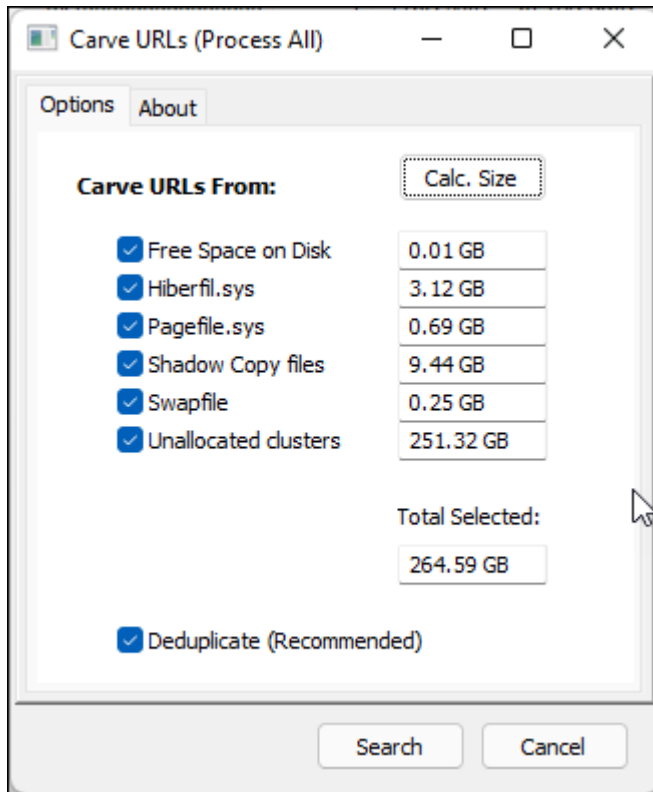
A stand-alone **Artifact Carve** script is available to carve URLs etc. from specific files:

Figure 212: Artifact Carve



When launched, **Artifact Carve** provides a second selection window where the carve source is selected, including carving from **Hiberfil.sys**, **Pagefile.sys**, **Swap file**, and **unallocated clusters**. The **Calc. Size** button can be used to identify the volume of these sources. The length of the search will be determined by the size and the content of the source files.

Figure 213: Artifacts module, Artifact Carve.

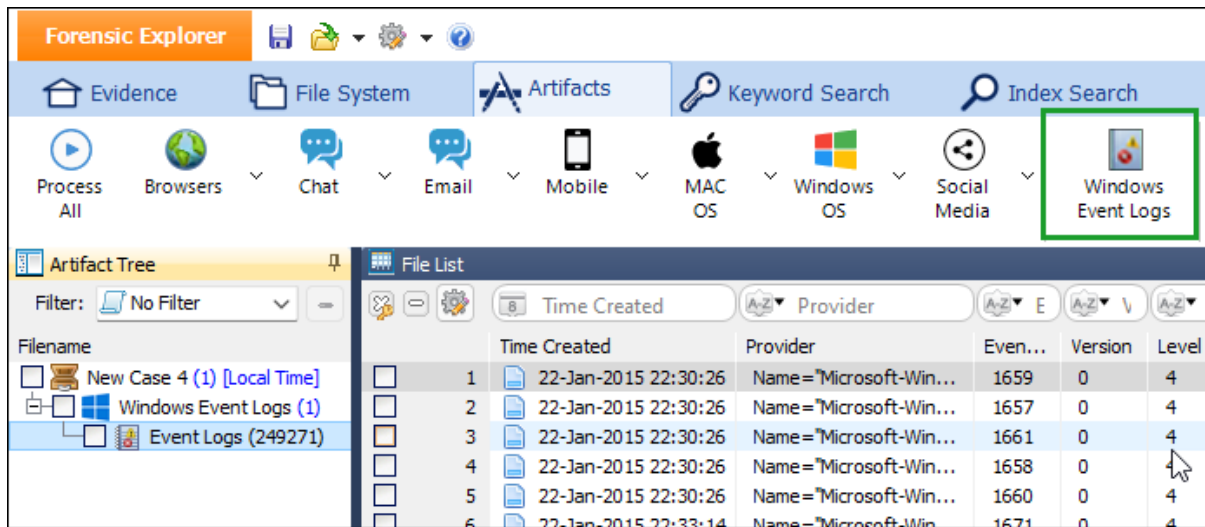


12.1.1 WINDOWS EVENT LOGS (.EVTX)

From Forensic Explorer v5.4.8(2686) onward (April 2022) Windows Event Log files (.evtx) can be processed in the Artifacts module. Click on the Windows Event Logs button in the Artifacts module toolbar to extract event log data from the current case.

Once extract it is possible to use filters, keyword searches, etc. to search for significant records. Records found can be exported using the right-click export options.

Figure 214: Windows Event Logs (.evtx)



Chapter 13 - Keyword Search Module

In This Chapter

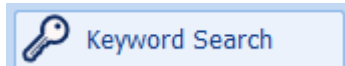
CHAPTER 13 - KEYWORD SEARCH MODULE

13.1	Keyword search	214
13.2	Keyword management	216
13.2.1	Creating a keyword	216
13.2.2	Edit or delete a keyword.....	218
13.2.3	Grouping keywords.....	218
13.2.4	Importing keywords.....	219
13.2.5	Running a Keyword Search	220
13.3	Search results.....	222
13.3.1	Delete a keyword search folder (and keywords)	222
13.3.2	To delete a key word	223
13.3.3	Note: Why keyword hits differ when compared to EnCase®	223
13.4	Keyword result list	224
13.4.1	Hits.....	224
13.4.2	Hit Text	224

13.1 KEYWORD SEARCH

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

Figure 215: 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:

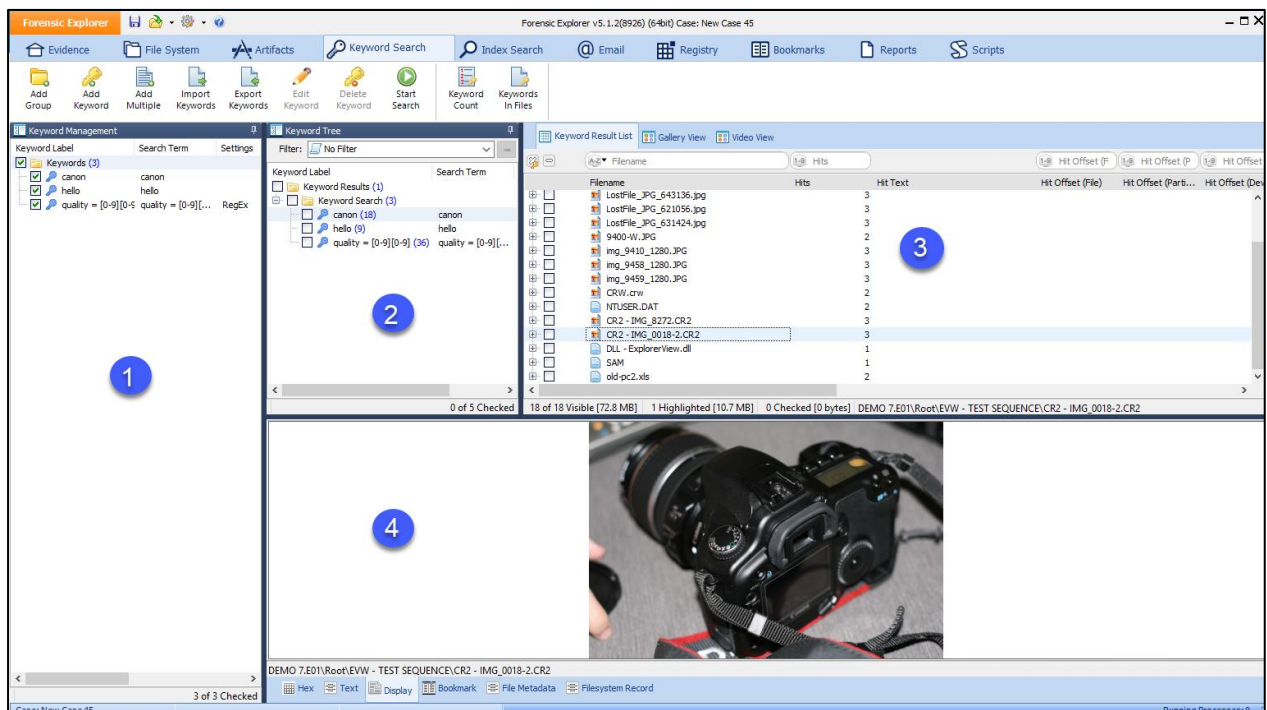
- A keyword search can be time intensive. The volume of data being searched, the number of keywords, and the speed of the computer hardware on which the search is run will influence the duration of the search.
- Each new keyword, or set of keywords, requires a new search. Because a search can be time 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 216 below:

Figure 216: Keyword Search module



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).




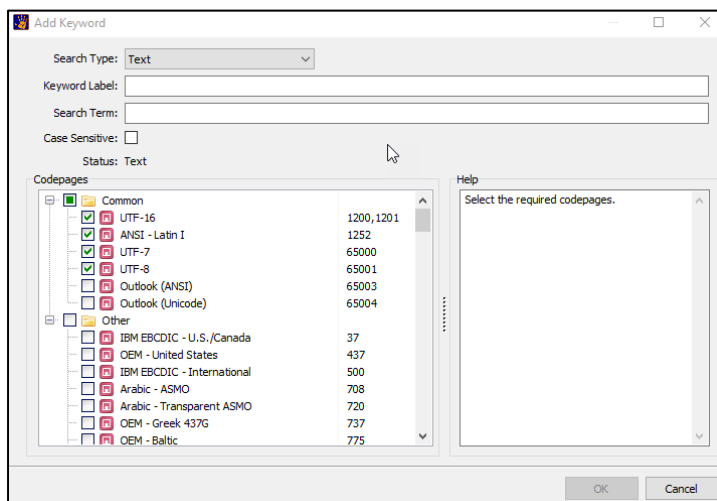
- Click on the **Add Keyword** button  in the module toolbar (if the Keyword icon is inactive, highlight the “Keywords” folder in the “Keyword Name” window); or,
- **Right-click** in the Keyword Management window and select “**Add Keyword**”; or,
- Using the **keyboard**, select the “**CTRL**” and “**N**” key.

Figure 217: Add keyword.



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

Text:

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

Regular Expression (PCRE)

A “Regular 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*” (11). GREP is often misinterpreted as RegEx. GREP is a Linux/Unix program that is a RegEx search utility.

Basic RegEx functions include:

\wFFFF	Unicode character
\xFF	Hex character
.	Any character
\d	Any number [0-9]
?	Repeat zero or one time
+	Repeat at least once
[a-z]	a through z
[A-Z]	A through Z
*	Repeat zero+ times
[XYZ]	Either X, Y, or Z
[^XYZ]	Neither X nor Y nor Z
\[Literal character
(ab)	Group ab together for ?, +, *,
{m,n}	Repeat m to n times
a b	Either a or b

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

For more RegEx examples, see:

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

Hexadecimal

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

Keyword Name

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

Search Expression

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


Case Sensitive

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


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

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

To delete a keyword:

1. **Highlight** the keyword with the mouse.
 - a. Click the **Delete Keyword** button  ; 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** button  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 218: Add Keyword Group window



The image shows a dialog box titled "Add keyword group". It has a close button (X) in the top right corner. Below the title bar is a text input field with the label "Keyword Group:". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

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(s)".

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:

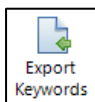
;	Indicates a comment and is ignored in the import
[Folder]	Creates a folder to group subsequent keywords
Keyword	To add a simple list of words, one keyword is placed on each line of the text file. Blank lines are ignored.
	To add additional parameters to the word, use the following format: Keyword Name,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

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

Sample Keywords.txt file:

<pre>; This is a list of digital cameras 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",</pre>
--

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.

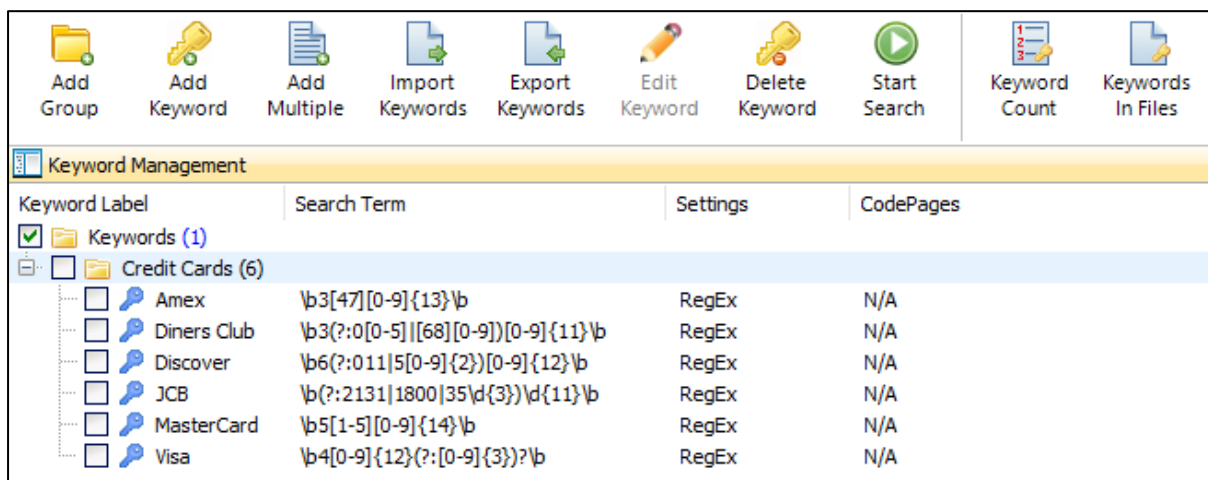
To **import** a keyword text file:



1. In the module toolbar, click on the **Import Keywords** button
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 “Credit Card.txt file” is shown below:

Figure 219: Keyword Management after the import of the above Credit Card.txt file



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 Search 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 220 below:

Figure 220: New Keyword Search window

Keyword Search 2 Options

Process Name:

Source

Module:

Searchable Items (198430 items, 62.01 GB)

Unallocated space

Checked items (0 items 0 bytes)

Include Raw Devices, Partitions and Files

Additional Options:

File slack

Limits

Maximum hits per keyword, per file: (Max = 65536)

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

Logging:

Priority:

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 (cannot exceed 65536 per file) and the total number of hits.

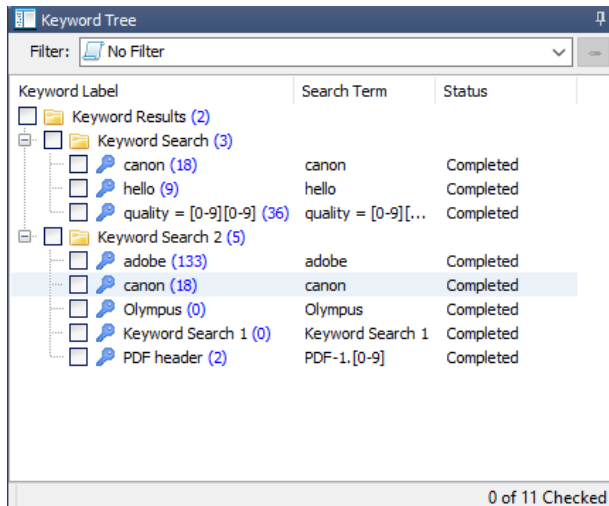
3. Click **OK** to commence the search.

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 221 below:

Figure 221: Keyword Tree search results



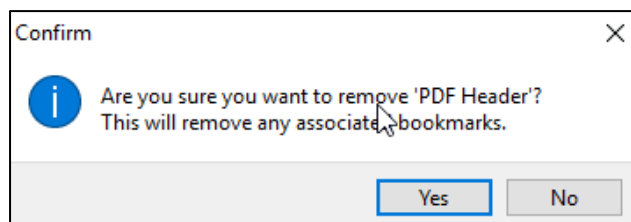
The **Keyword Results** folder at the root of the tree holds a folder for each search. The default search names are “Keyword Search 1”, “...2” etc.:

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

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 222: 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 223: Keyword Result List


Filename	Hits	Hit Text	Hit Offset
LostFile_JPG_580416.jpg	3		
LostFile_JPG_590848.jpg	3		
LostFile_JPG_601408.jpg	3		
LostFile_JPG_611584.jpg	3		
LostFile_JPG_621056.jpg	3		
LostFile_JPG_643136.jpg	3		
LostFile_JPG_631424.jpg	3		
9400-W.JPG	2		
img_9410_1280.JPG	3		
img_9458_1280.JPG	3		
img_9459_1280.JPG	3		
CRW.crw	2	1/2 5.úQ...^.....Canon.Canon Pow 2/2 ^.....Canon.Canon PowerShot	
NTUSER.DAT	2	1/2N9é...100CANON..(.....í. 2/2 p....1.0.0.C.A.N.O.N.....	
CR2 - IMG_8272.CR2	3		
CR2 - IMG_0018-2.CR2	3		
DLL - ExplorerView.dll	1		
SAM	1		

18 of 18 Visible [72.8 MB] | 1 Highlighted [2.4 MB] | 0 Checked [0 bytes] | DEMO 7.E01\Root\EVW - TEST SEQUENCE\CRW.crw

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 224 below:

Figure 224: Keyword Search Hit Offset

Filename	Hits	Hit Text	Hit Offset (File)	Hit Offset (Partition)	Hit Offset (Device)	Extension
LostFile_JPG_580416.jpg	3					jpg
	1/3	df# .Canon .Ca	158	281485470	281485470	
	2/3	non .Canon EC	164	281485476	281485476	
LostFile_JPG_590848.jpg	3					jpg
	1/3	df# .Canon .Ca	158	286826654	286826654	
	2/3	non .Canon EC	164	286826660	286826660	
LostFile_JPG_601408.jpg	3					jpg
	3/3Canon EC	1566	281486878	281486878	
	3/3Canon EC	1566	286828062	286828062	
LostFile_JPG_611584.jpg	3				jpg	
LostFile_JPG_621056.jpg	3				jpg	

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 those 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 224 above the file offset to the first search hit 'Canon' in LostFile_JPG_580416.jpg is **158**.

When the first hit in Figure 224 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: 549776 (x86390): The sector of the current hit.
- Device Offset: 281485470 (x10C7209E): The number of bytes from the beginning of the device (DEMO 7.E01) to the start of the hit.
- File Offset: 158 (x9E): The number of bytes from the beginning of LostFile_JPG_580416.jpg to the start of the hit.

Figure 225: Example of Hit Offset (Device) and Hit Offset (File)

The screenshot shows a hex editor window with the following information bar: Sector: 549776 (x86390) Device Offset: 281485470 (x10C7209E) File Offset: 158 (x9E) DEMO 7.E01\Root\50th Birthday Cake\LostFile_JPG_580416.jpg. The hex data shows the word 'Canon' highlighted in yellow, with the hex values 43 61 62 6F 65 00 43 61 62 6F 65 00.

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 224 above the partition offset to the first search hit 'Canon' in LostFile_JPG_580416.jpg is **281485470**.

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**.

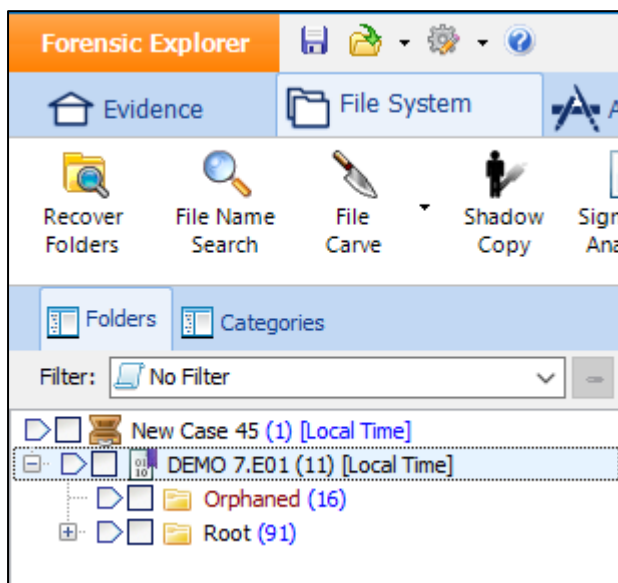
Figure 226: In this example...

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 224 Figure 224: Keyword Search Hit Offset.

When the evidence file is selected in the File System tree (shown in Figure 227 below), the entire device is shown in the Hex view:

Figure 227: Selection of the device in the File System tree view



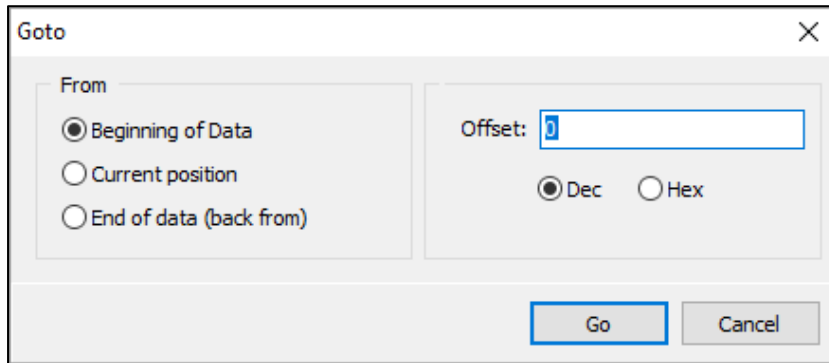
To go to the Hit Offset (Partition):

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 228 below:

Figure 228: Hex view Goto

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.

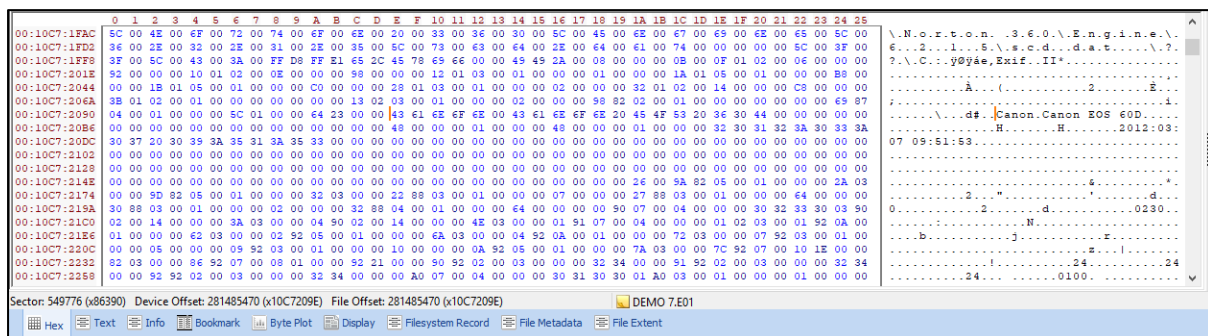


Goto takes the Hex view to the entered offset.

Manually click at the offset to ensure the **Hex view information bar refreshes** to show:

- Offset: 281485470 (x10C7209E): The number of bytes from the beginning of the partition to the Goto location.

Figure 229: Example of Hit Offset (Partition)



Note: In this example the select partition is also the device and the selected file (see Figure 226 above for more information).

Hit Offset (Device)

For the device in which the hit was found, Hit Offset (Device) is the number of bytes from the beginning of the device to the location of the hit. In the example in Figure 224 above the disk offset to the first search hit 'Canon' in LostFile_JPG_580416.jpg is **281485470**.

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

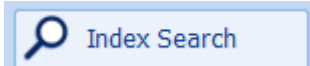
CHAPTER 14 - INDEX SEARCH MODULE

14.1	Index search.....	230
14.1.1	Indexed file types.....	230
14.1.2	Index database.....	230
14.1.3	Noise words	230
14.2	Considerations prior to creating an index	231
14.3	Creating an index	231
14.3.1	Index progress	233
14.3.2	Delete an index.....	234
14.4	Searching an index.....	235
14.4.1	Select the search features to use in your search.....	236
14.4.2	Boolean Search	236
14.4.3	Words and Phrases	237
14.4.4	Wildcards (*, ?, and =)	237
14.5	Search results.....	237
14.6	Index Search Compound Files.....	238

14.1 INDEX SEARCH

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

Figure 230: Index Search module tab



An Index Search creates and 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, fast keyword searches can be performed on those files.

IMPORTANT – Sharing a DTSearch Index:

A DTSearch index requires each file in a case to be **uniquely identified**. In Forensic Explorer this is achieved using an items **Bates ID**. This means that the index alone is **NOT** transferable to another user, as evidence and processes maybe be conducted in a different sequence by that user, resulting in a different bates number sequence.

To share a DTSearch index, **the entire case** must be provided to the third party.

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:\Users\user profile\Documents\Forensic Explorer v5\Cases\case name\DTSearchIndexes\index name

A keyword index is usually about one fourth the size of the original documents, although this may vary 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 v5\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;
- A “file carve” for specific file types (see 24.4 - File carving).
- Decompress or decrypt any compound files not supported by dtSearch®.

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**

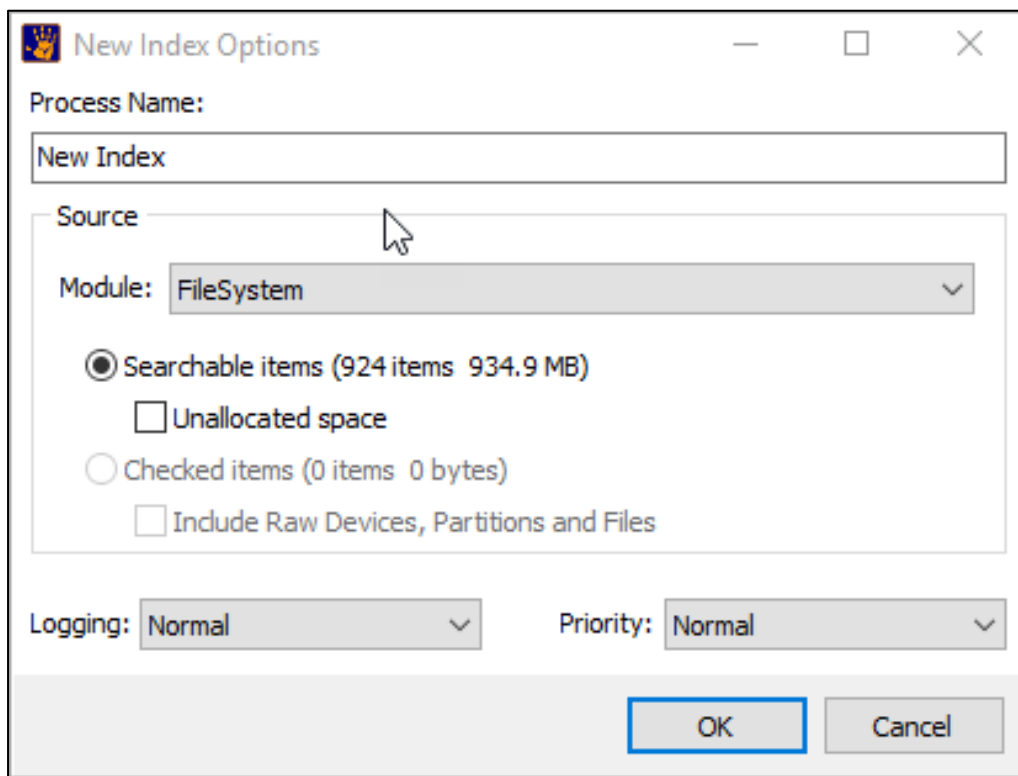
Switch to the required module tab; File System, Email or Registry, and select the required files, then switch to the Index Search module;

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 231 below:

Figure 231: New Index



Process 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.

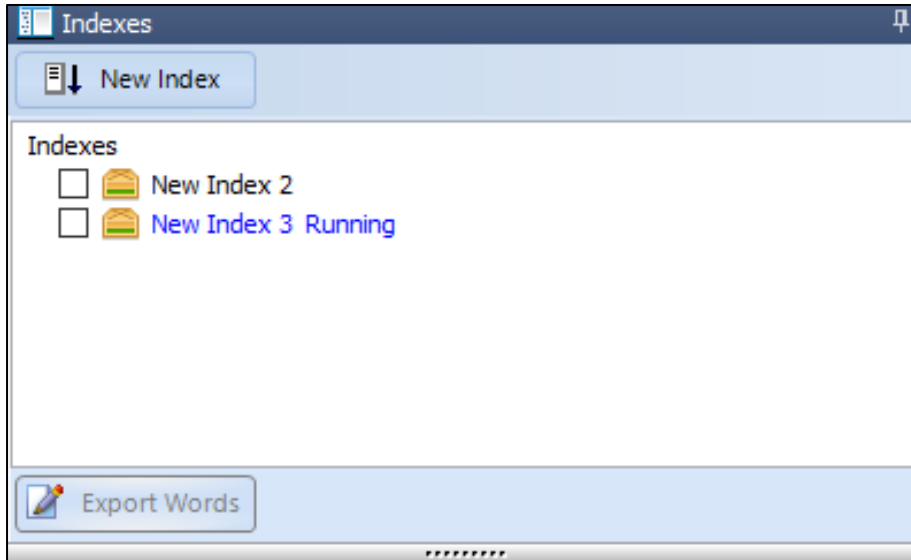
File slack: Determines whether the file slack of each file will be excluded from the index.

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

14.3.1 INDEX PROGRESS

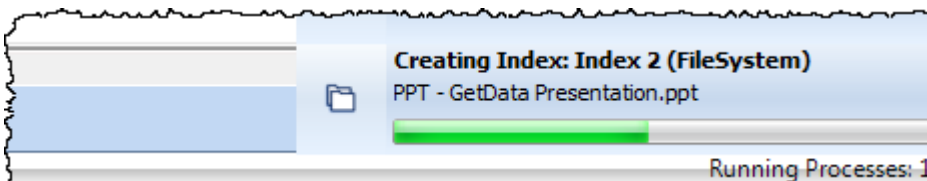
An index in progress will show “Running” in the Indexes window, as shown in Figure 232 below:

Figure 232: Index creation in progress



The progress is also tracked in the program process list, as shown in Figure 233 below:

Figure 233: Forensic Explorer process window showing a completed index

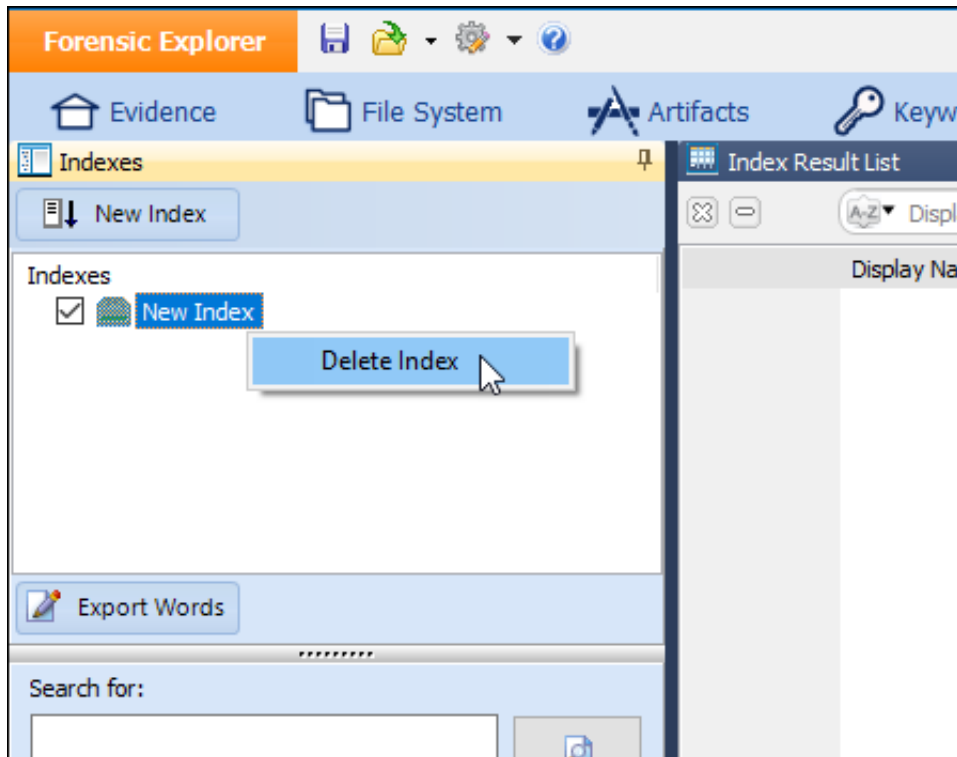


14.3.2 DELETE AN INDEX

Important: Deleting an index is a permanent operation. A deleted index cannot be recovered.

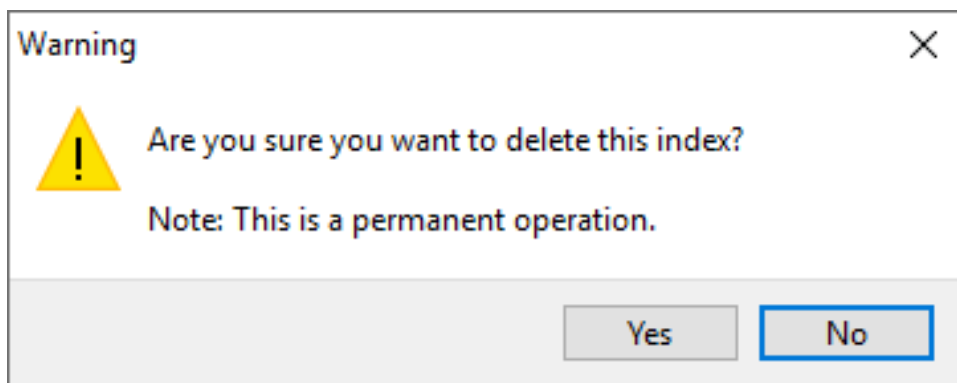
To **delete an index**, check the required index, then right click on the index name, and select **Delete Index** from the drop-down menu:

Figure 234: Delete Index



A warning message will appear. Clicking **Yes** will permanently delete the index.

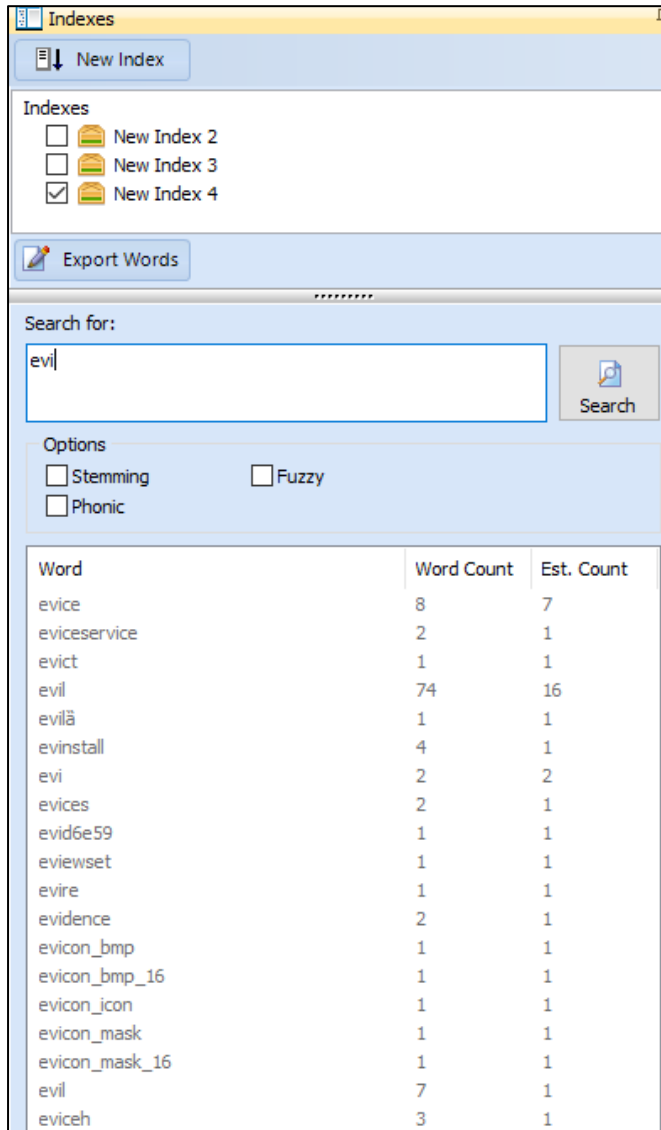
Figure 235: Delete Index confirmation



14.4 SEARCHING AN INDEX

When the indexing process is complete, the index will appear in the “Available Indexes” window, as shown in Figure 236 below:

Figure 236: Index search



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

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

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

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

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

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

Phonic searching

Find 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, OR, that indicate a relationship between them. For example:

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

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

(apple and pear) or (name contains smith)

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:

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

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

14.5 SEARCH RESULTS

Search results display in the *Index Results* List view window, as shown in Figure 238 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:

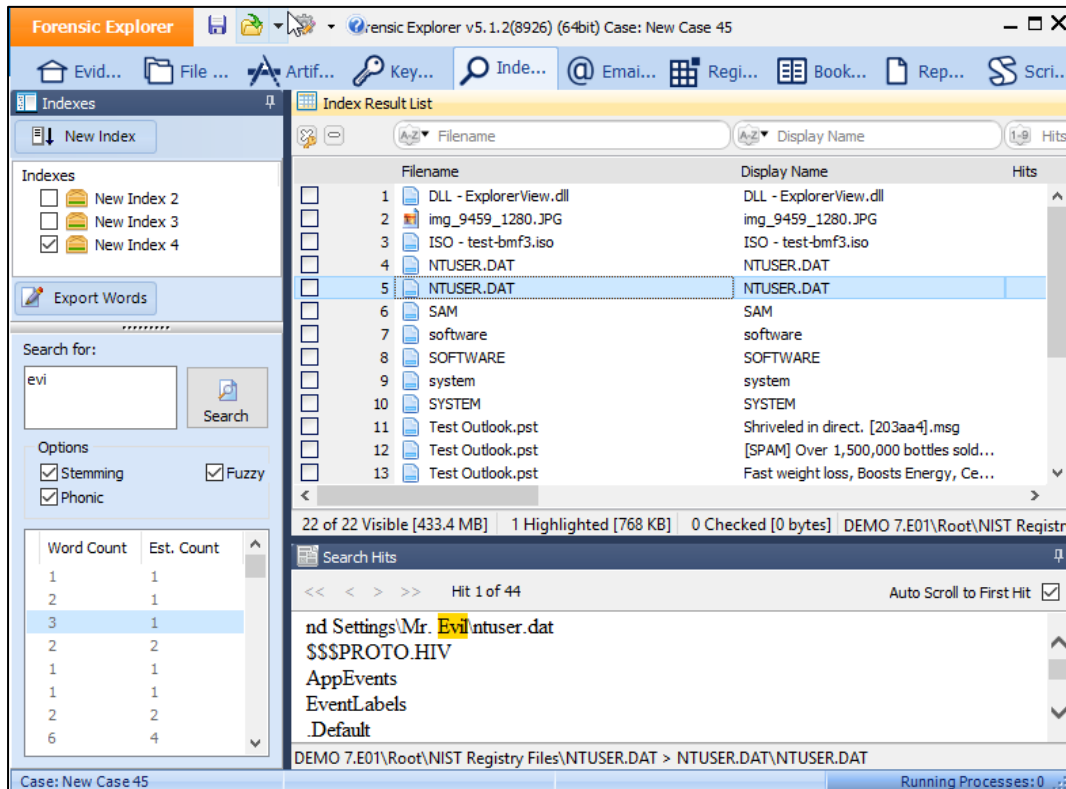
Figure 237: Navigate index search hits



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

Search hits are highlighted in yellow, as shown below:

Figure 238: Index search results



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:

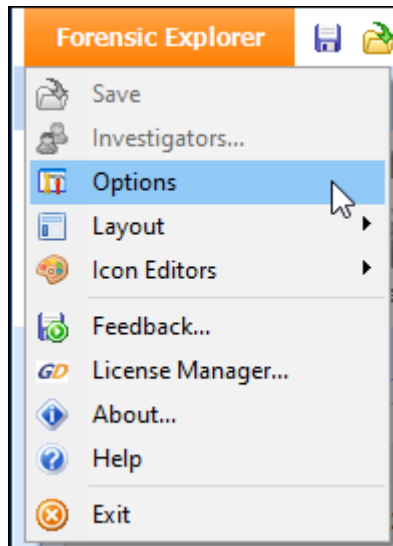
1. In the Index Search Module, Indexes window, check the required index;
2. Click on the **Export Words** button;
3. Select the name and location of the exported .csv file.

14.8 INDEX SEARCH LOGGING

In some instances, a forensic examiner may wish to log the index searches conducted.

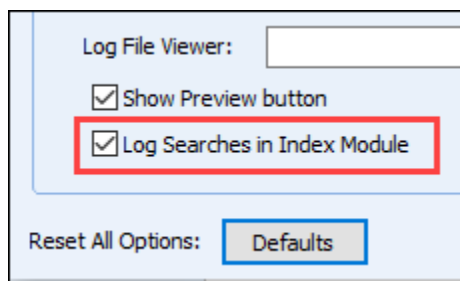
To export the indexed word list:

1. Click on the Orange Forensic Explorer button and select **Options**.



2. Tick the **Log Searches in Index Module** checkbox (note that this setting is remembered for future cases).

Figure 239: Log Searches in Index Module



3. Index Search history is written to the file:
...\\Documents\\Forensic Explorer v5\\Cases\\[CaseName]\\Logs\\Index Search Results.csv
4. and is recorded in the following format:

Figure 240: Sample Search Log

	A	B	C	D	E	F	G	H	I	J
1	Date	Time	Index Name	Search Term	Stemming	Fuzzy	Phonic	Files	Hits	Investigator
2	30-Mar-21	14:13:13	New Index	cat	FALSE	FALSE	FALSE	21	163	Graham Henley
3	30-Mar-21	14:13:17	New Index	dog	FALSE	FALSE	FALSE	8	161	Graham Henley
4	30-Mar-21	14:13:23	New Index	kangaroo	FALSE	FALSE	FALSE	1	1	Graham Henley
5	30-Mar-21	14:13:37	New Index	donket	FALSE	FALSE	FALSE	0	0	Graham Henley
6	30-Mar-21	14:13:43	New Index	donkey	FALSE	FALSE	FALSE	0	0	Graham Henley
7										

Chapter 15 - Email Module

In This Chapter

CHAPTER 15 - EMAIL MODULE

15.1	Email	242
15.2	Email module	242
15.3	Microsoft Outlook .PST email	242
15.3.1	Add a standalone Outlook.PST file	243
15.3.2	Add a .PST file from a Forensic Explorer module.....	243
15.4	Index Search the Email module	243

15.1 EMAIL

Email analysis is a key component of computer forensics. The Forensic Explorer **Email module** supports a variety of email formats, including::

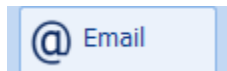
- .EDB Microsoft Exchange
- .EML Email Message format
- .MBOX Mailbox format
- .MSG Microsoft Message file
- .OST Microsoft Offline Storage Table
- .PST Microsoft Personal Storage Table

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.

Figure 241: Email module tab



The Email module is broken down into three panes:

1. **Email Tree**

Holds the folder structure of the email file.

2. **Email List**

Lists individual messages and their metadata. Available columns include.

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

3. **Data Views**

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

15.3 MICROSOFT OUTLOOK .PST EMAIL

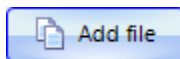
The Microsoft Outlook email client is available as part of the Microsoft Office suite. Microsoft refers to it as a “personal information manager” as it has additional functions to email, including calendar, contacts, and notes.

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)**.

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 module > Email**” in the drop-down menu. The content of the .PST file will then be populated in the Email module.

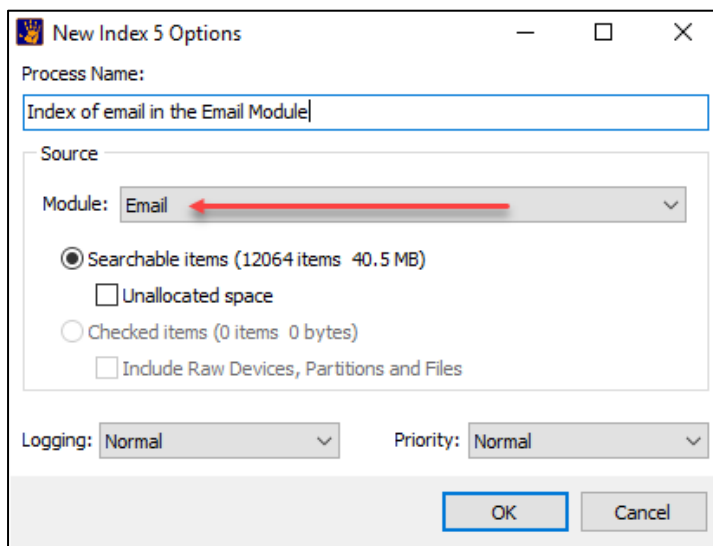
15.4 INDEX SEARCH THE EMAIL MODULE

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 242: Index Search module, New Index window

**Important:**

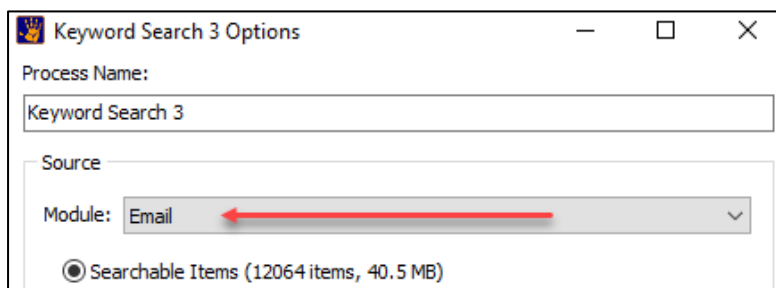
Creating an index of the content of the Email module is **NOT** the same as indexing a PST file that is in the file system. DTSearch will already index a PST file that is in the file system.

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 243: Keyword Search module, Run Keyword Search window



Chapter 16 - Registry Module

In This Chapter

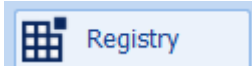
CHAPTER 16 - REGISTRY MODULE

16.1	Registry module	246
16.1.1	Windows location of registry files	246
16.2	Adding a REGISTRY FILE to the registry module	247
16.2.1	Add a standalone registry file	247
16.2.2	Add a registry file from a Forensic Explorer module	247
16.3	Registry Data Views	248
16.3.1	Registry Tree	248
16.3.2	Registry List	249
16.3.3	Hex, TEXT, and Filesystem Record views	249
16.4	Deleted registry keys	250
16.5	Examining registry files using scripts	250

16.1 REGISTRY MODULE

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

Figure 244: Registry module tab



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

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

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

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 (12)” for detailed information.

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

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

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

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

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

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

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**.

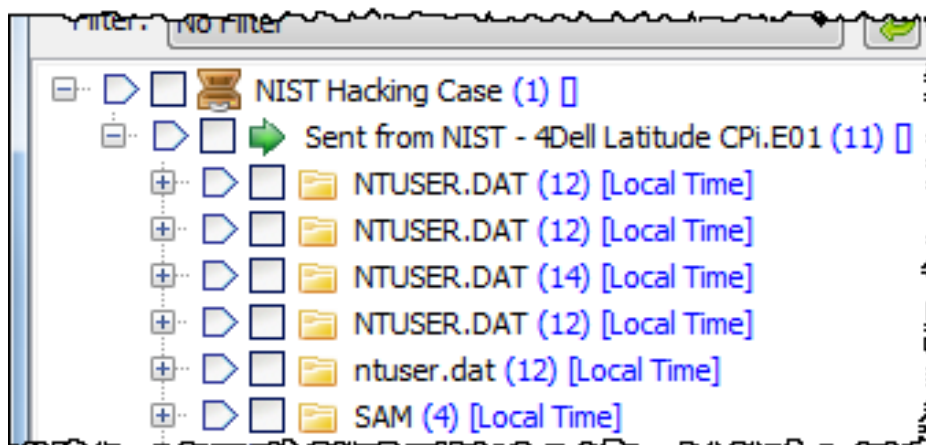
16.2.2 ADD A REGISTRY FILE FROM A FORENSIC EXPLORER MODULE

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 module > Registry**” 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 245 below:

Figure 245: Registry module showing "Sent from"

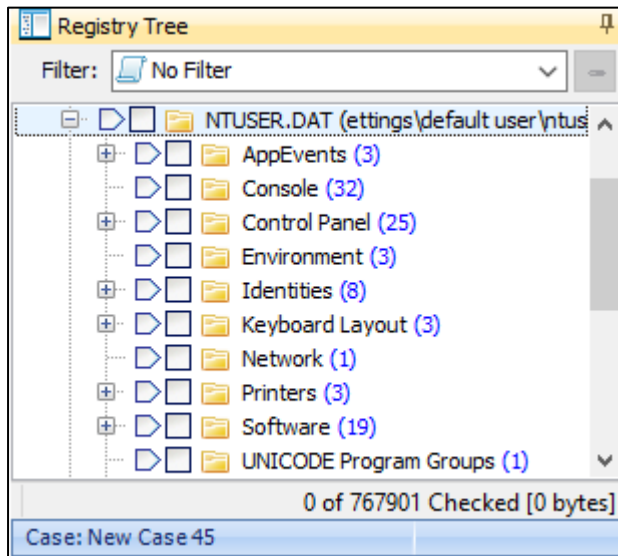


16.3 REGISTRY DATA VIEWS

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 246 below:

Figure 246: Registry Tree, showing folders in NTUSER.DAT



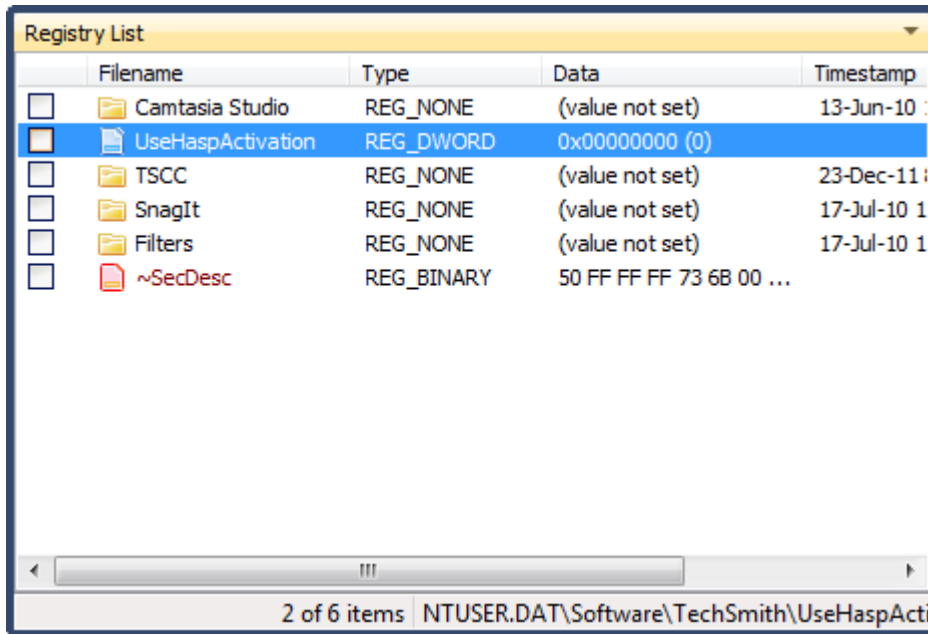
The blue number in brackets, e.g., “(2)” shows the number of items inside the folder (but does not count the contents of sub folders).

For information, see [8.2.1 Navigating Tree views](#), including branch plating.

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 247 below:

Figure 247: Registry List view



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

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

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

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

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



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

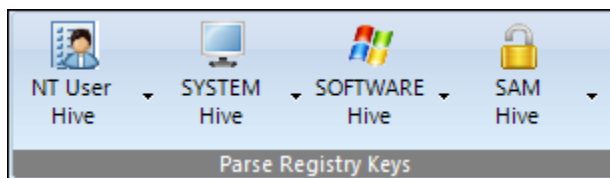
When a registry file is read by Forensic Explorer, the unallocated space within the registry file is parsed for deleted registry keys. These keys are placed into the “Deleted Keys” Folder, marked with the following icons:

-  Deleted key
-  Deleted folder

16.5 EXAMINING REGISTRY FILES USING SCRIPTS

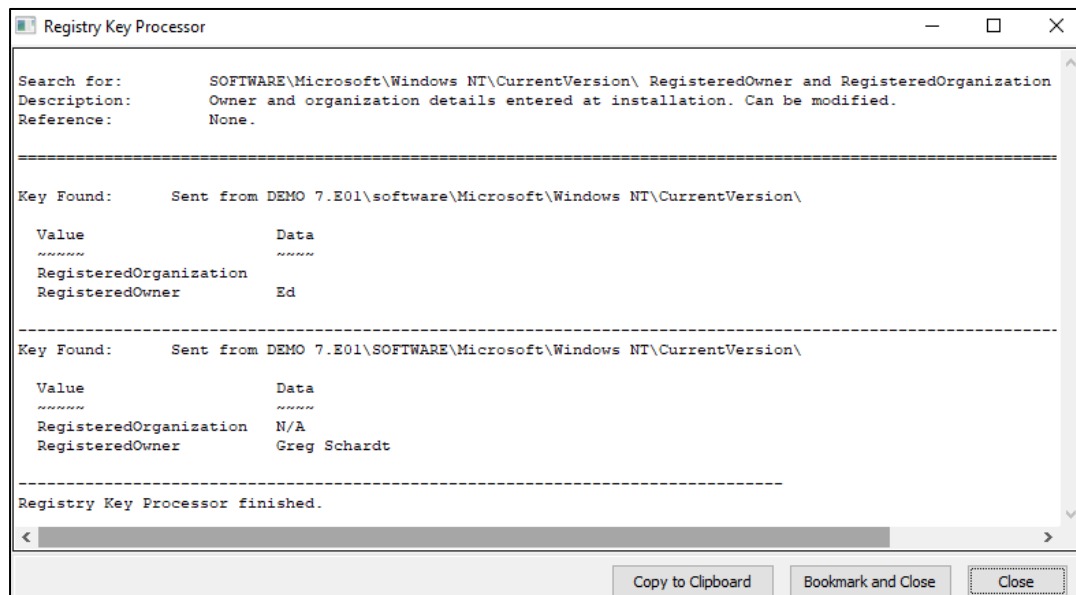
A default installation of Forensic Explorer includes a “Parse Registry Keys” button group in the Registry Module toolbar:

Figure 248: Registry Module, Parse Registry Keys



Each of the drop-down links in the button group passes a variable to the *Scripts/Registry/Registry Key Processor.pas* script to scan (and in some cases interpret) data of interest from specific keys. For example, selecting the “SOFTWARE > Registered Owner\Organization” button returns:

Figure 249: Registry Key Processor



The *Registry Key Processor.pas* uses a RegEx search to locate the relevant key. The script then processes and displays the result per its type (and any unique processing that the specific key requires).

IMPORTANT

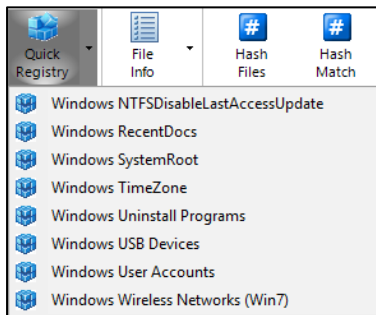
It is important to note that automated registry key analysis is a developing field based largely on individual forensic practitioner research. Limited registry documentation relevant to pertinent keys is made available by Microsoft.

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.

16.5.1 QUICK REGISTRY

A Quick Registry button in the File System module toolbar gives users fast access to important registry Artifacts. This natively reads registry files without the need to add data to the Registry module.



Chapter 17 – Bookmarks Module

In This Chapter

CHAPTER 17 - BOOKMARKS MODULE

17.1	Adding Bookmarks	254
17.1.1	Manually add a bookmark	254
17.1.2	Triage bookmarks	255
17.1.3	Adding Bookmarks from a script	255
17.1.4	Create custom bookmark folders	255
17.2	Bookmarks Module.....	256
17.2.1	Bookmarks tree.....	256
17.2.2	Bookmarks List.....	257
17.2.3	Bookmark Data Views.....	259
17.3	Identifying Bookmarked files other modules	259

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.

A toolbar has been added to the Bookmarks module. This enables faster access to scripts specific to that module.

IMPORTANT: Forensic Explorer Reports are generated from Bookmarked items.

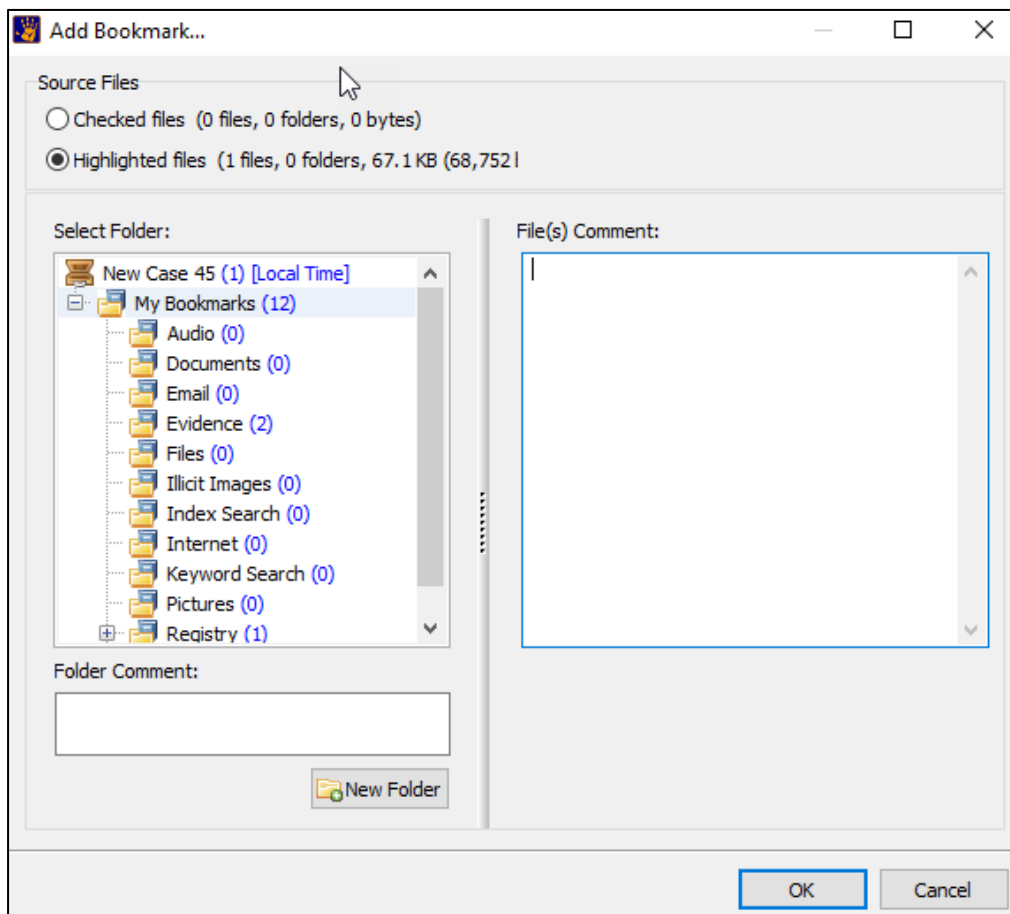
17.1.1 MANUALLY ADD A BOOKMARK

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:

Figure 250: Add Bookmarks window



- 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**.
- The **right click** drop-down menu or the **New Folder** button enables the investigator to add or delete a folder.
- 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 0) to “Triage” data.

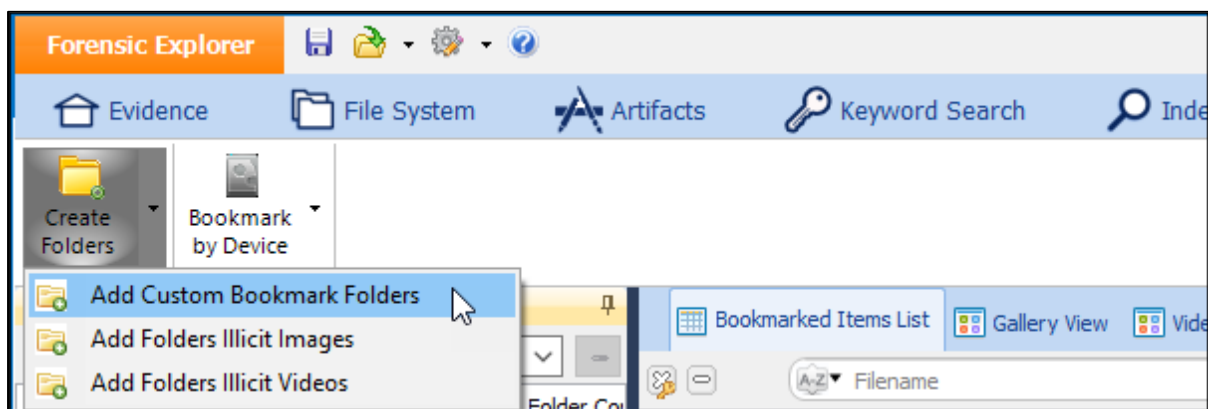
17.1.3 ADDING BOOKMARKS FROM A SCRIPT

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 CREATE CUSTOM BOOKMARK FOLDERS

A script has been added to create custom bookmark folders. Templates can be created and loaded to quickly create bookmark folders for each case:

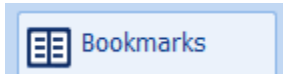
Figure 251: Bookmarks toolbar



17.2 BOOKMARKS MODULE

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

Figure 252: 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

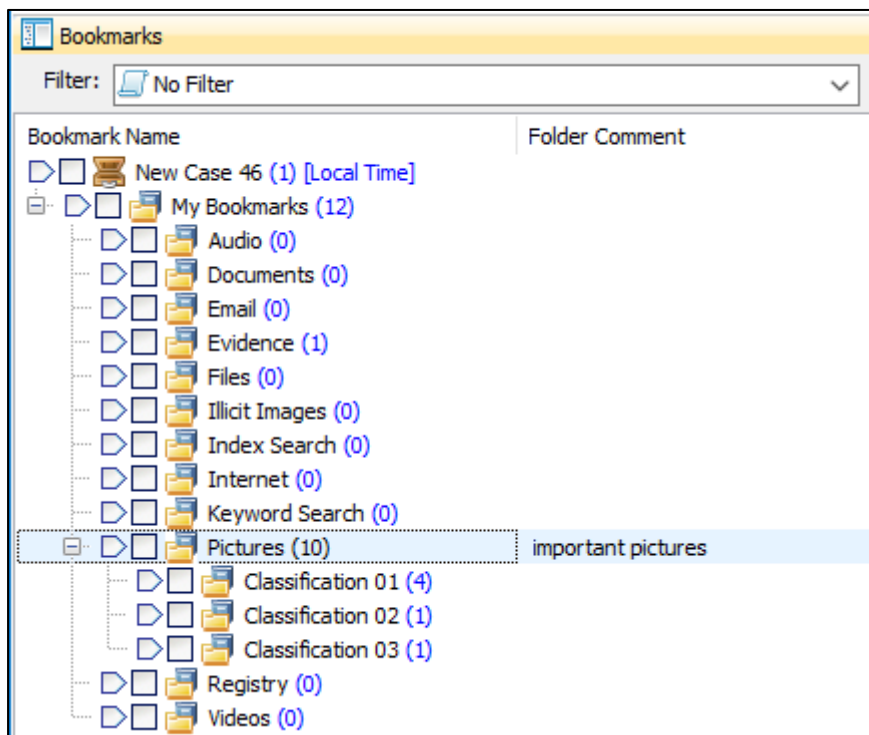
The Bookmark tree displays:



Bookmark folders: used by the investigator to group together bookmarked files of a similar nature.

An example is shown in Figure 253 below:

Figure 253: Bookmark folder tree



MANAGE BOOKMARK FOLDERS

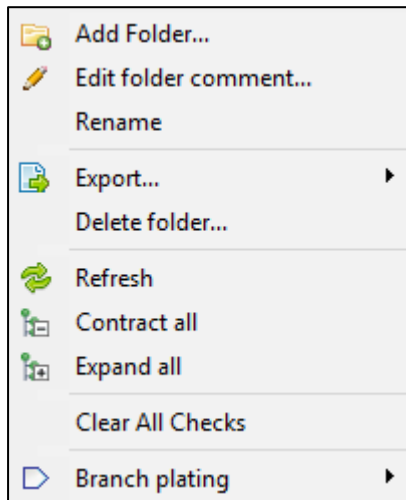
To **add** a bookmark folder:

Right click and select **Add Folder** from the drop-down menu.

To **delete** a bookmark folder and its contents:

Right click and select **Delete folder** from the drop-down menu:

Figure 254: Manage Bookmark folders



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 255: Bookmark list below:

Figure 255: Bookmark list

 A screenshot of the 'Bookmarked Items List' interface. It shows a table with columns for Filename, Classification, Flags, Path, and Data Size. The table contains four rows of data. The interface also shows navigation buttons for 'Gallery View' and 'Video View', and search filters for 'Filename', 'Classification', 'Flags', 'Path', and 'Data Size'.

	Filename	Classification	Flags	Path	Data Size
<input type="checkbox"/>	1 90 min 2.docx			DEMO 7.E01\Root\	28,672
<input type="checkbox"/>	2 DOC.doc			DEMO 7.E01\Root\EVW - TEST SEQ...	2,883,584
<input type="checkbox"/>	3 DOCX - Office 2007 Word Document.docx			DEMO 7.E01\Root\EVW - TEST SEQ...	65,536
<input type="checkbox"/>	4 old-pc1.doc			DEMO 7.E01\Root\Signature Test\	12,288

MANAGE BOOKMARK LIST

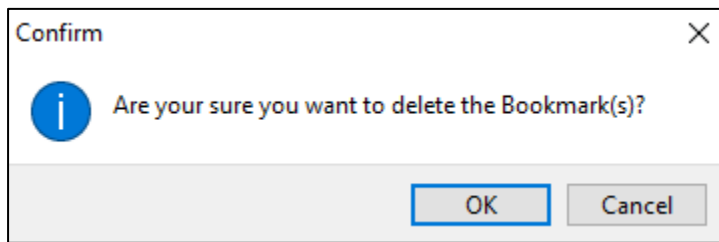
To **add** a bookmark:

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:

Figure 256: Delete bookmark/s confirmation



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 comments will be updated for each of the bookmarks.

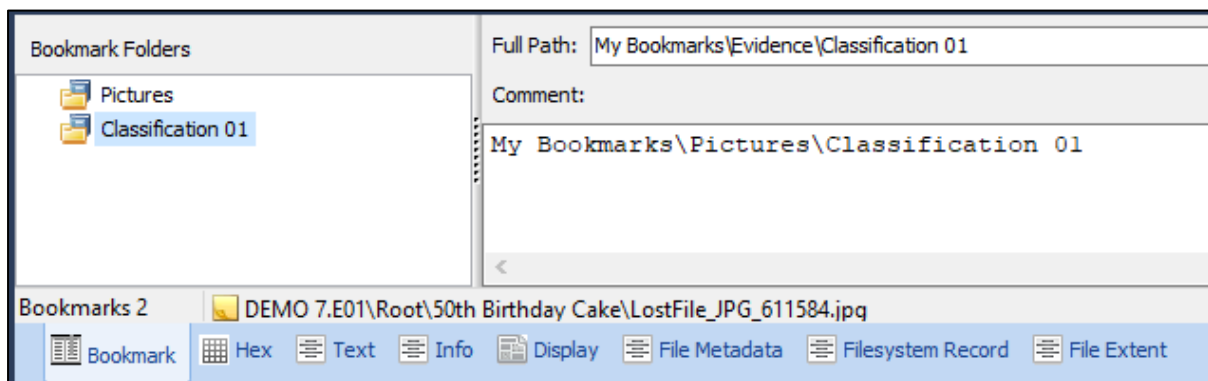
17.2.3 BOOKMARK DATA VIEWS

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, Hex, Text, Info, Display, File Metadata, Filesystem Record, and File Extent.

The **Bookmark data view**, shown in Figure 257 below, is visible in all modules. It enables the investigator to determine the Bookmark folder/s into which a file has been placed.

Right click on the view and select “**Edit bookmark comment...**” from the drop-down menu to edit a comment.

Figure 257: Bookmark data view

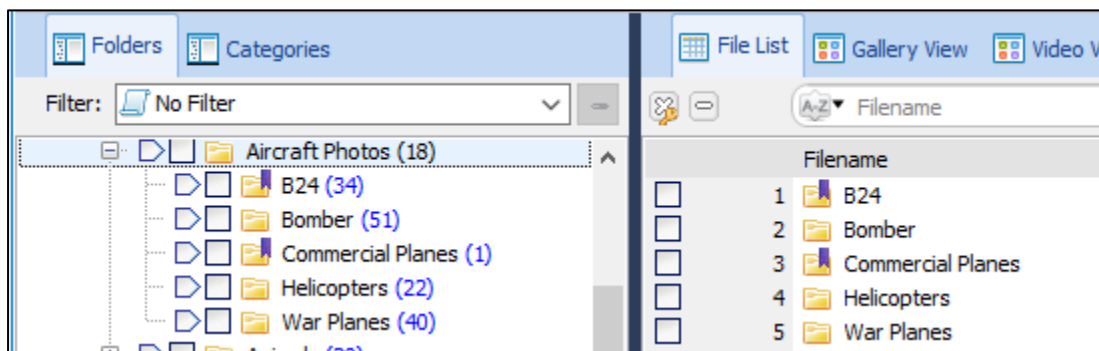


17.3 IDENTIFYING BOOKMARKED FILES OTHER MODULES

Bookmarked files can be identified in the File System module by:

1. A purple bookmark that overlays the file icon, as shown in Figure 258 below:

Figure 258: Bookmarked files in the File System module



2. The bookmark folder name is shown in the Bookmark Folder column (if a file has been bookmarked in multiple folders the column contains each folder name separated by a comma).

Chapter 18 – Reports

In This Chapter

CHAPTER 18 - REPORTS

18.1	MS Word - Quick Reports	263
18.2	The Reports Module	266
18.3	Reports Tree	268
18.3.1	The Triage Report	268
18.3.2	Changing the default report	270
18.3.3	Open a new report.....	270
18.3.4	Report name, Groups and Sections	271
18.3.5	Rename or Move a Group or Section	271
18.3.6	Print a report	271
18.3.7	Export a report as DOC, RTF, or PDF.....	272
18.3.8	Save a report as a template.....	273
18.4	Report Editor	275
18.4.1	Report Editor - Preview	275
18.4.2	Report Editor - Edit	276
18.5	Creating Reports	277
18.5.1	Preparation for Report exercises.....	277
18.5.2	Exercise 1: Report on a single file	279
18.5.3	Exercise 2: Listing bookmarked files in a table	284
18.5.4	Exercise 3: Creating a Gallery view report.....	291

18.5.5	Exercise 4 - Nested Tables	297
18.5.6	Apply a filter to a report table	305

18.1 MS WORD - QUICK REPORTS

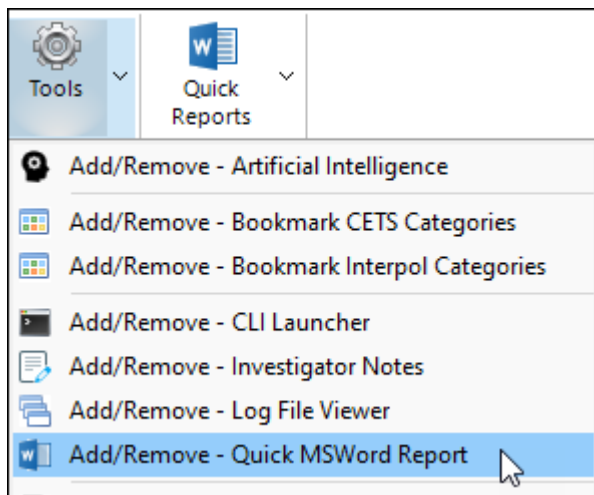
Forensic Explorer **Quick Reports** is a methodology to quickly generate a **Microsoft Word report** on **bookmarked items**.

The **requirement** for Quick Reports is:

- Microsoft Word 2016 or above.
- Microsoft Word must be fully licensed.

Quick Reports is launched from the toolbar icon of Forensic Explorer modules. If the **Quick Reports** button is not visible in a module toolbar, add it to the module using the **File System > Tools > Add/Remove – Quick MSWord Report** menu item.

Figure 259: File System > Tools > Add/Remove – Quick MSWord Report.



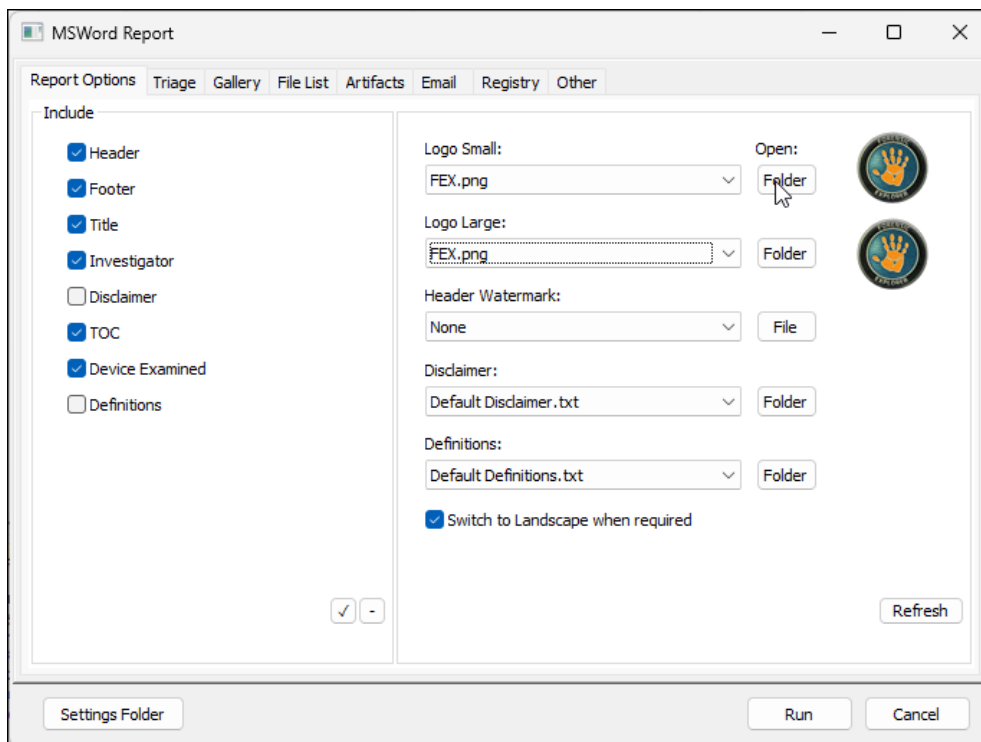
The advantage of using **Quick Reports** is that enables **bookmarked items** to be quickly imported into a Microsoft Word format. This gives the investigator flexibility to use Microsoft features such as:

- Report Sections.
- Table of Contents.
- Styles.

To **launch Quick Reports**:

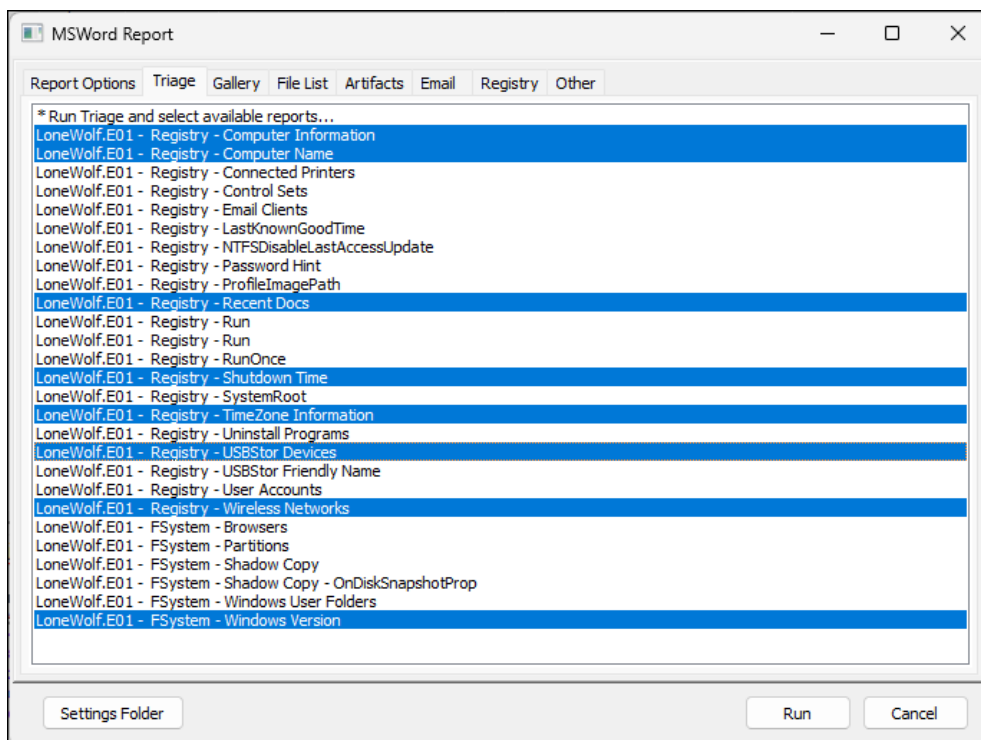
1. Click on the Quick Reports toolbar icon.
2. The Quick Reports script will open in the **Report Options** tab (on first run).

Figure 260: Quick Reports > Report Options.



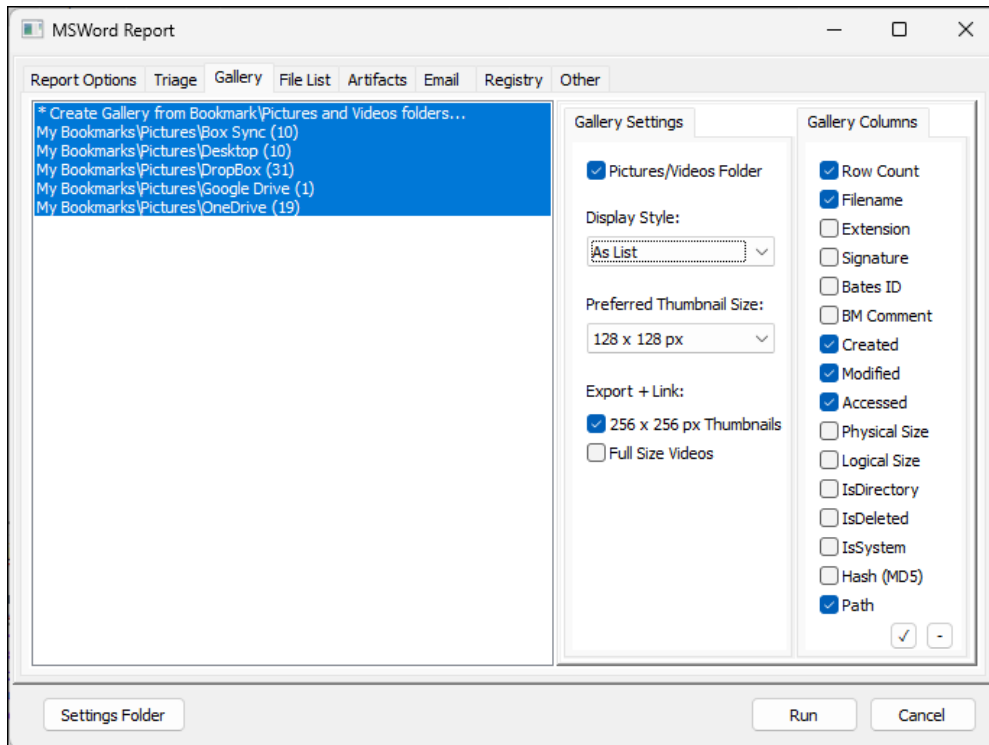
The **Report Options** tab is used to configure the various document options, including header and footer, title page. Customization is possible by saving graphics and text files to the **Settings Folder**. The additional tabs, **Triage**, Gallery, File List, Artifacts, Email, Registry, and Other, source report data from specific bookmark folders. Use the **SHIFT** or **CTRL** key to select the bookmark folders to include in the report:

Figure 261: Triage, selected bookmark folders to include.



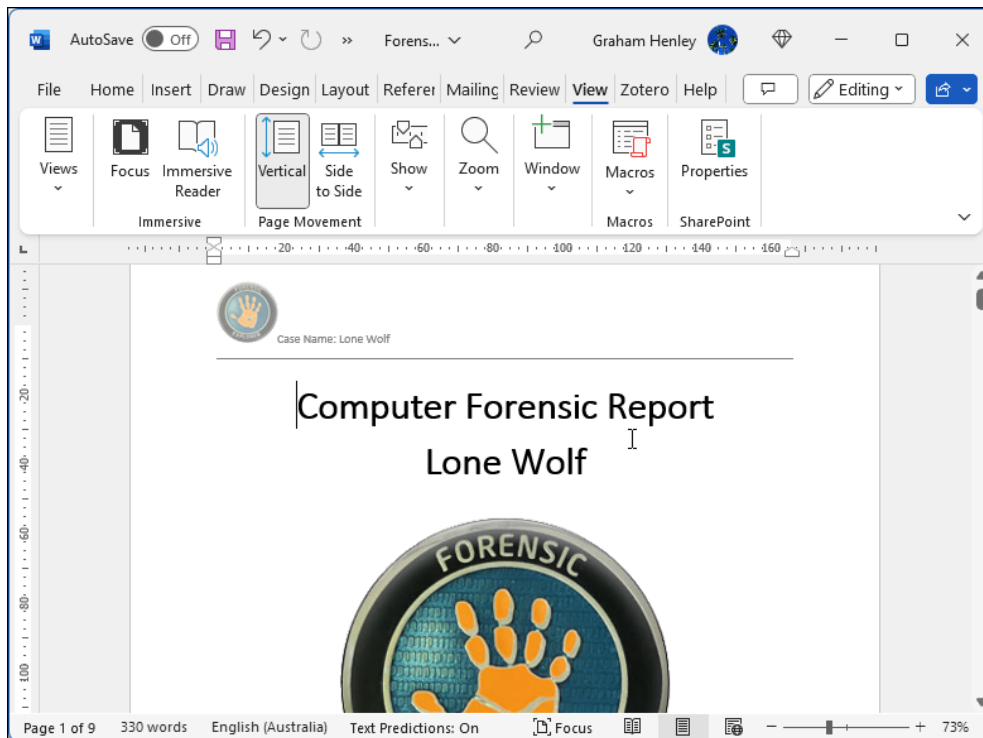
Where additional settings or columns are available, make the applicable selection:

Figure 262: Selecting Quick Report settings and columns.



When the required selections have been made, press the **Run** button to launch Microsoft Word. Once Word has launched, the investigator can customize and save the document as needed.

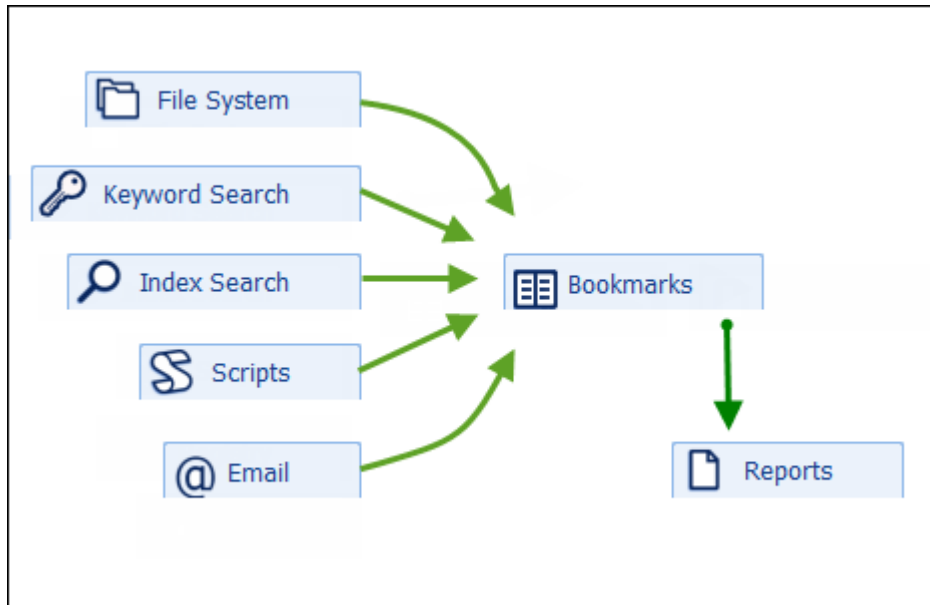
Figure 263: Quick Reports, Microsoft Word.



18.2 THE REPORTS MODULE

The purpose of the Reports Module is to assist in the generation of a report that documents 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 264: Modules > Bookmarks > Reports

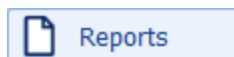


Bookmarks are either added manually or as the result of running a script (e.g., Triage scripts). For more information about adding bookmarks see Chapter 17 above.

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

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

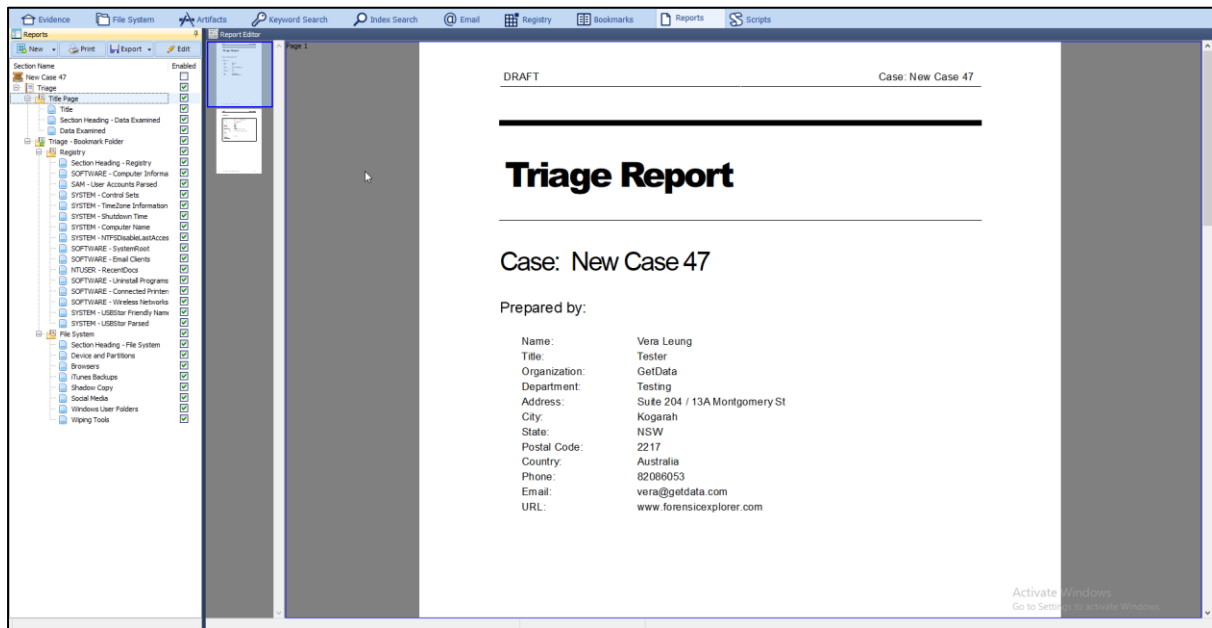
Figure 265: Reports module tab



The Reports module is divided into three main sections (as shown in Figure 266 below):

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

Figure 266: 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

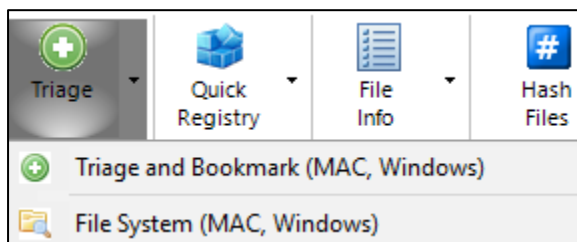
RUNNING A TRIAGE

When evidence is added to Forensic Explorer the option exists in the **Evidence Processor** window to **Triage** (see “10.5 Credentials are case specific. If credentials are used between cases, the Import and Export buttons can be used to save and load them for each case.

Evidence Processor” 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 icon** in the File System module:

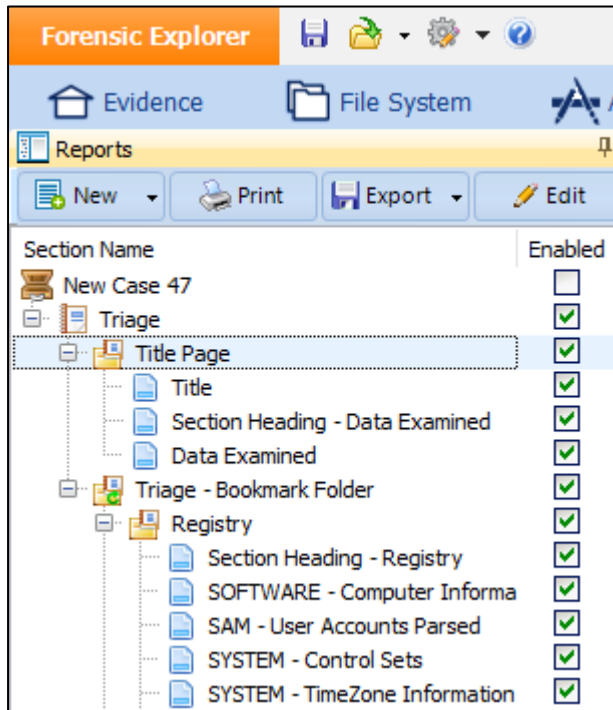
Figure 267: Triage from File System module



TRIAGE REPORT REPEATING OVER MULTIPLE DEVICES

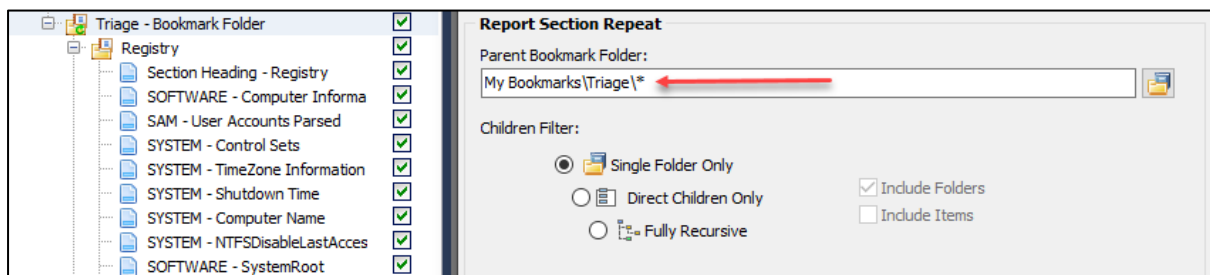
The **Triage** report is designed to work for multiple devices in a case by repeating on the “**Triage – Bookmark Folder**” report section as represented by the green icon in Figure 268 below:

Figure 268: Reports Tree showing the Triage Report



The repeat function is set by right clicking on the required folder > Properties... and applying the * symbol, as shown in Figure 269:

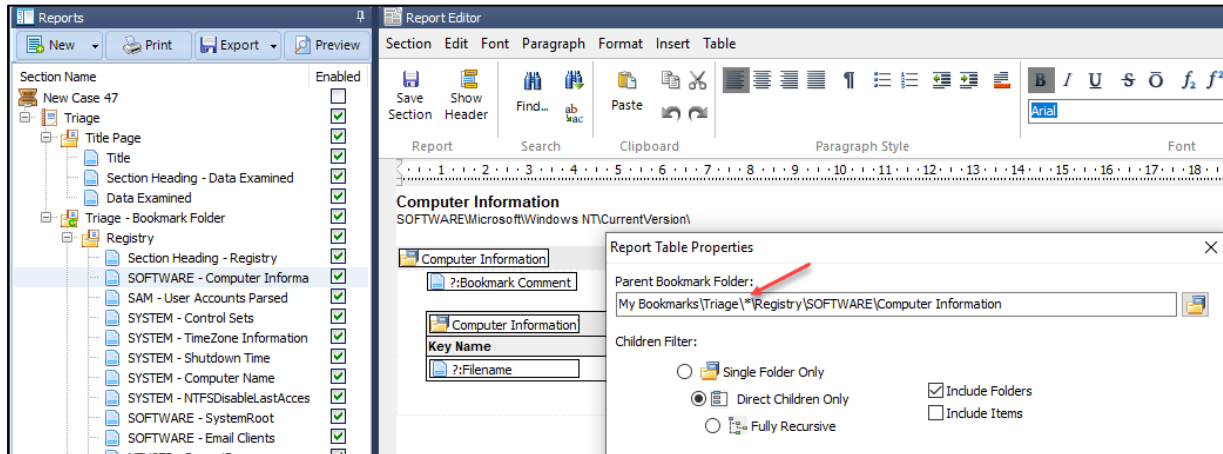
Figure 269: Iterating a report over multiple devices



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 270:

Figure 270: Triage report, handling unique device names



Learn more about creating reports in 18.5 Creating Reports.

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:



Report Name:

Click on the report name to preview the entire contents of the report in the preview window.

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 the 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 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.



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 268 above.

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:

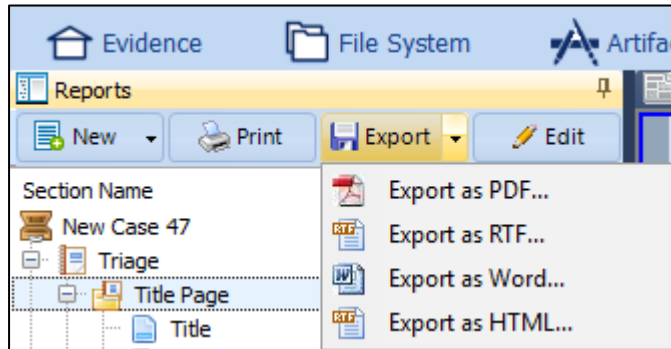
- Click on the report name, or a section in the report, and click the print button. The Windows print dialogue will open.

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** button and select the desired format;

Figure 271: Export a Report



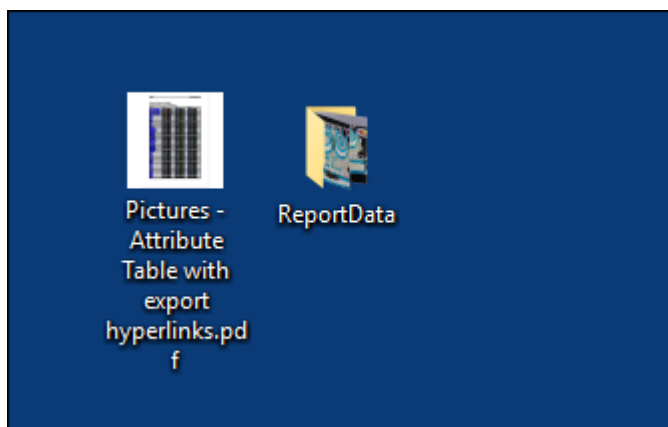
- Save the file to the desired location.

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), a folder called **ReportData** is created to hold the relevant exported files. An example is shown in Figure 272 below where the report and report data has been exported to the Windows Desktop:

Figure 272: A report with hyperlinks exported to the Windows Desktop



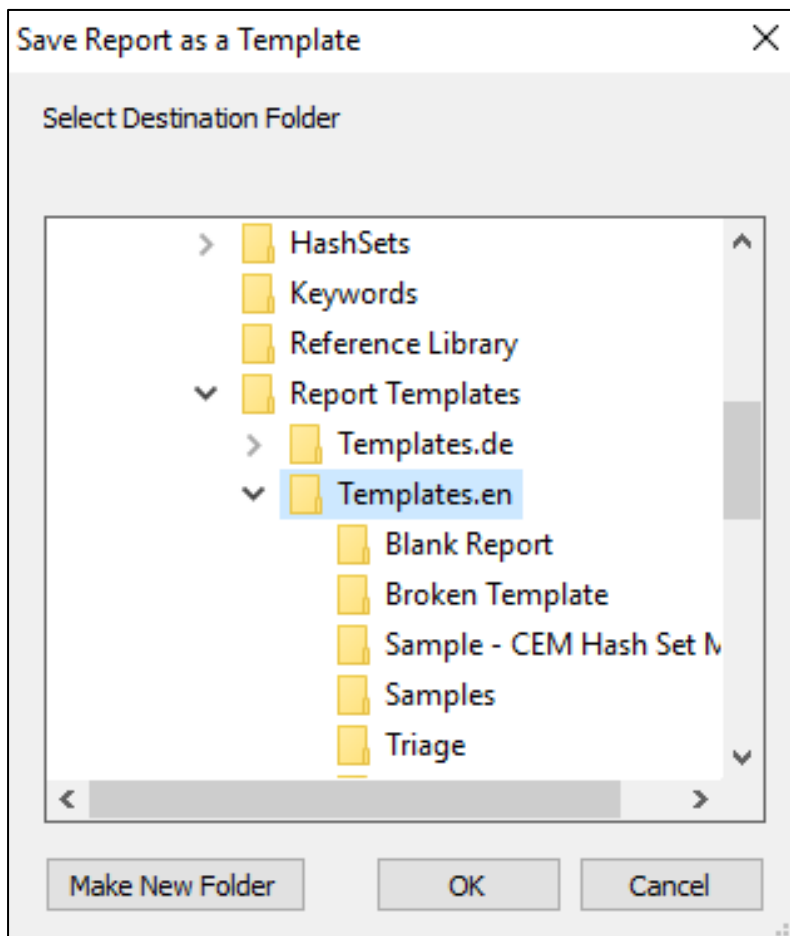
18.3.8 SAVE A REPORT AS A TEMPLATE

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:

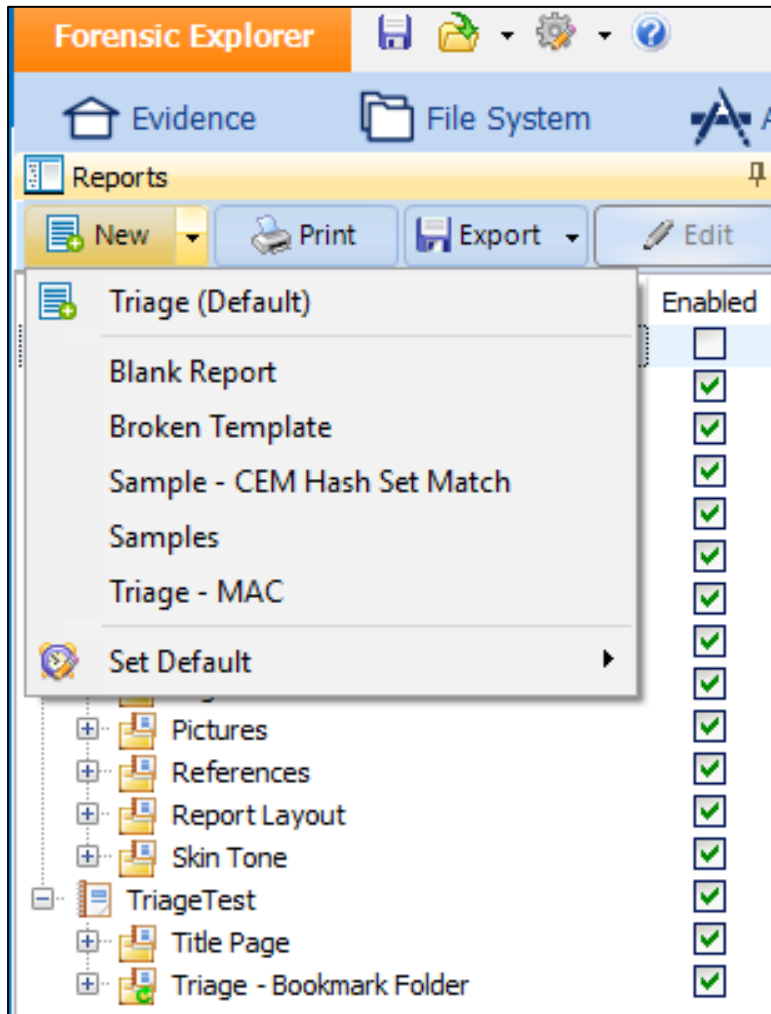
Figure 273: Save a Report Template



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 274: Load a report template



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 275 below) displays the content of the currently selected report in the Report tree.

To preview the **report**:

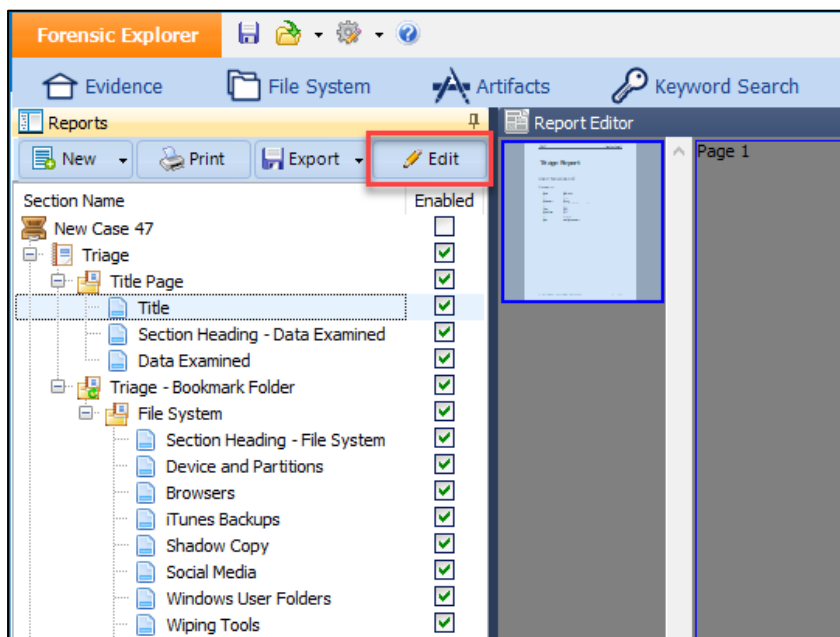
- In the Report tree, click on the report name;

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

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

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

Figure 275: Report Editor Preview

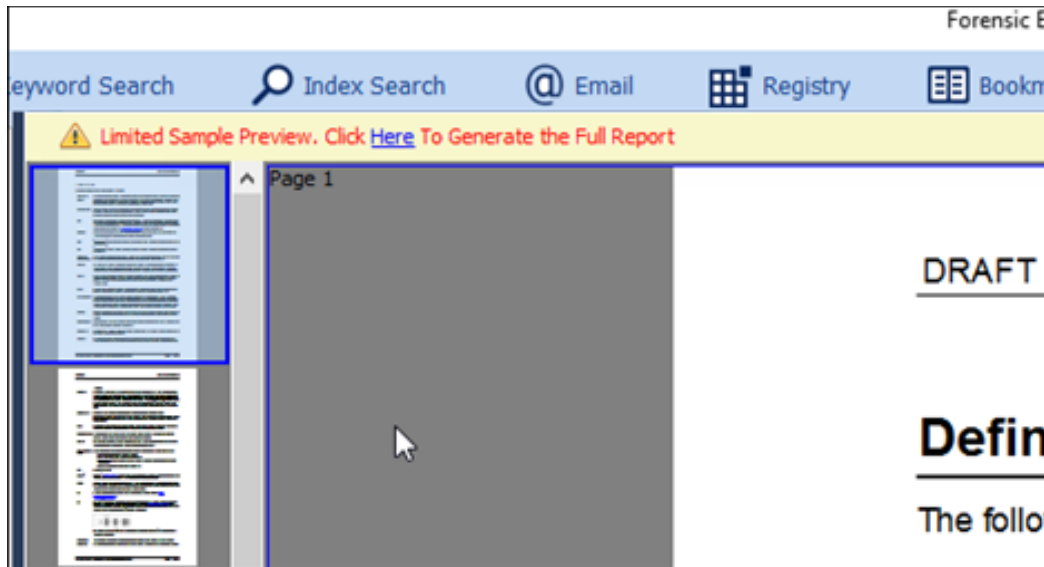


IMPORTANT: For speed purpose a report Preview is limited by default to **100 records**. This default can be changed by setting the following Registry key:

```
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 276 below:

Figure 276: 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

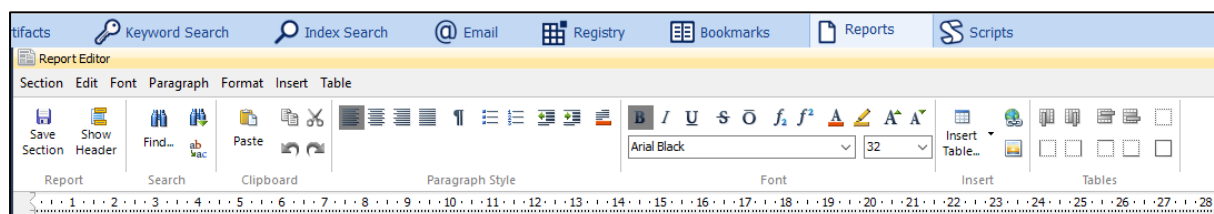
The Report Editor Edit window gives access to edit an existing report, or to design a new report.

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 277: 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 repeatedly.

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/AnimalsL01.zip>

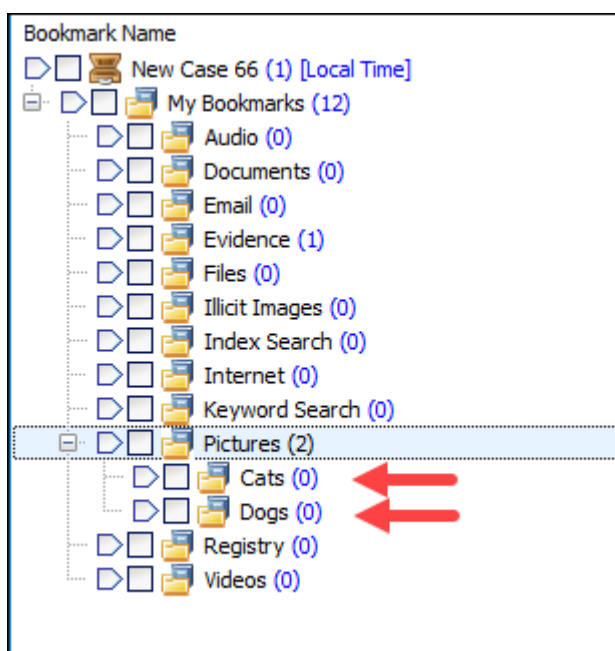
Unzip the download file and use the Animals.L01 file.

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 278: 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.

Figure 279: Preparation for report exercises, bookmarking files

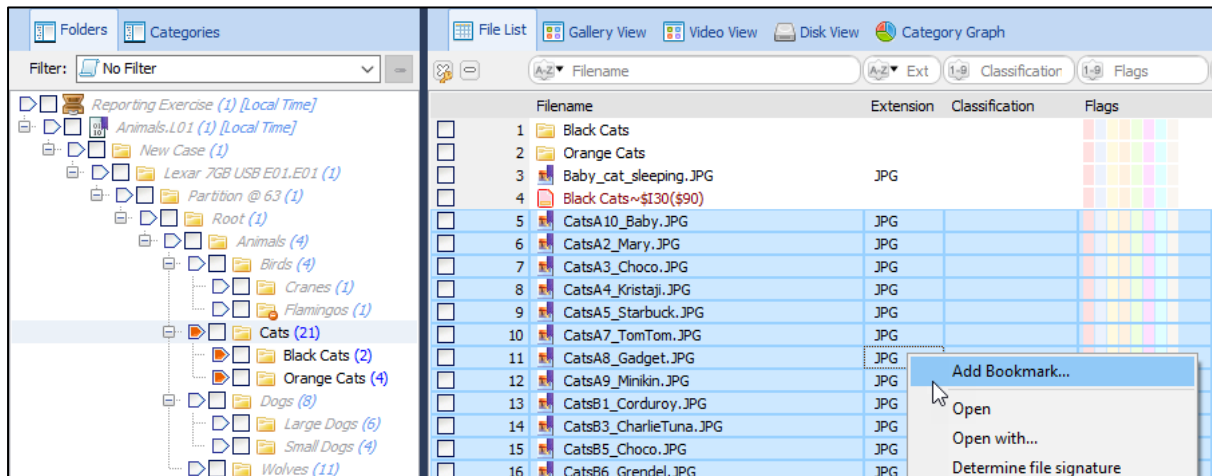
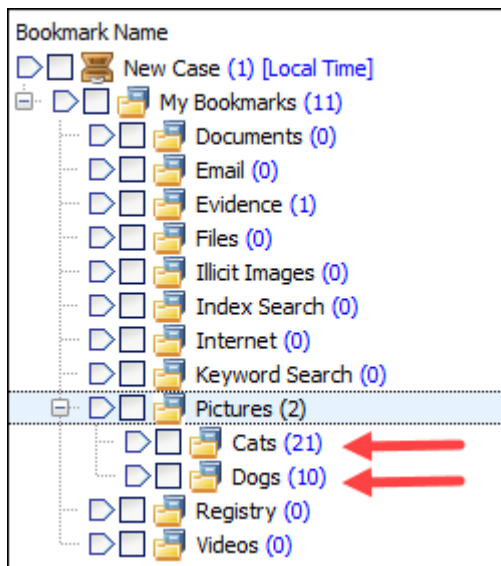
d. Repeat the step above to bookmark the 10 dog pictures to the **Dogs** bookmark folder.e. Switch to the **Bookmarks** module. Review the **Pictures bookmark folder** to ensure that it contains the bookmarked files, as shown in Figure 280 below:

Figure 280: Bookmarked files from Animals.L01

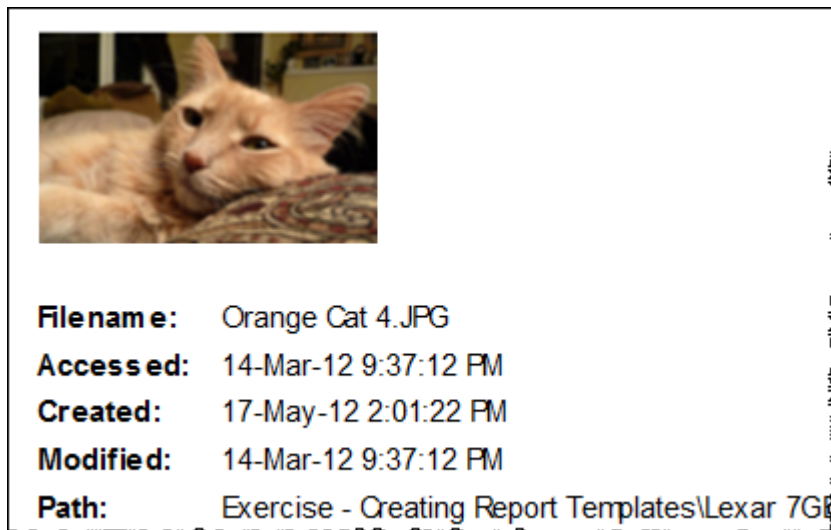


18.5.2 EXERCISE 1: REPORT ON A SINGLE FILE

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 281: Reporting on a Single Bookmarked File (finished report output)



STEP 1 – PREPARE BOOKMARKS

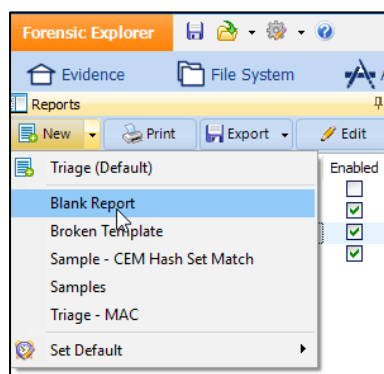
Follow **STEP 1** in **18.5.1** above to prepare a case with bookmarks.

STEP 2 – CREATE A BLANK REPORT

Create a blank report:

- Switch to the Reports module.
- In the Reports tree, select **New > Blank Report**.

Figure 282: Creating a blank report

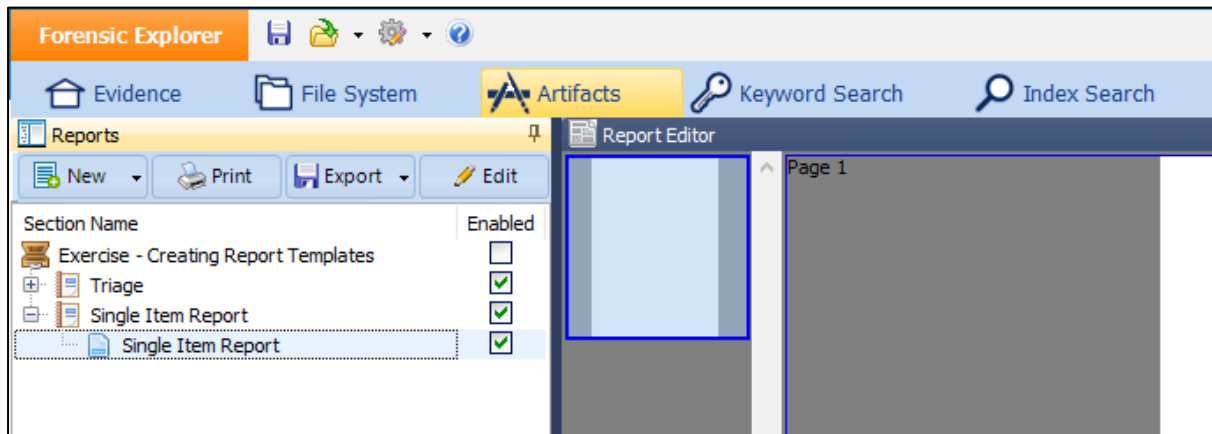


STEP 3 – RENAME THE BLANK REPORT

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 283: Rename the Report and Section



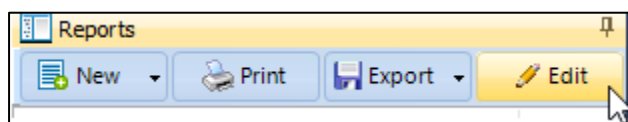
STEP 4 – EDIT THE REPORT

Edit the report:

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

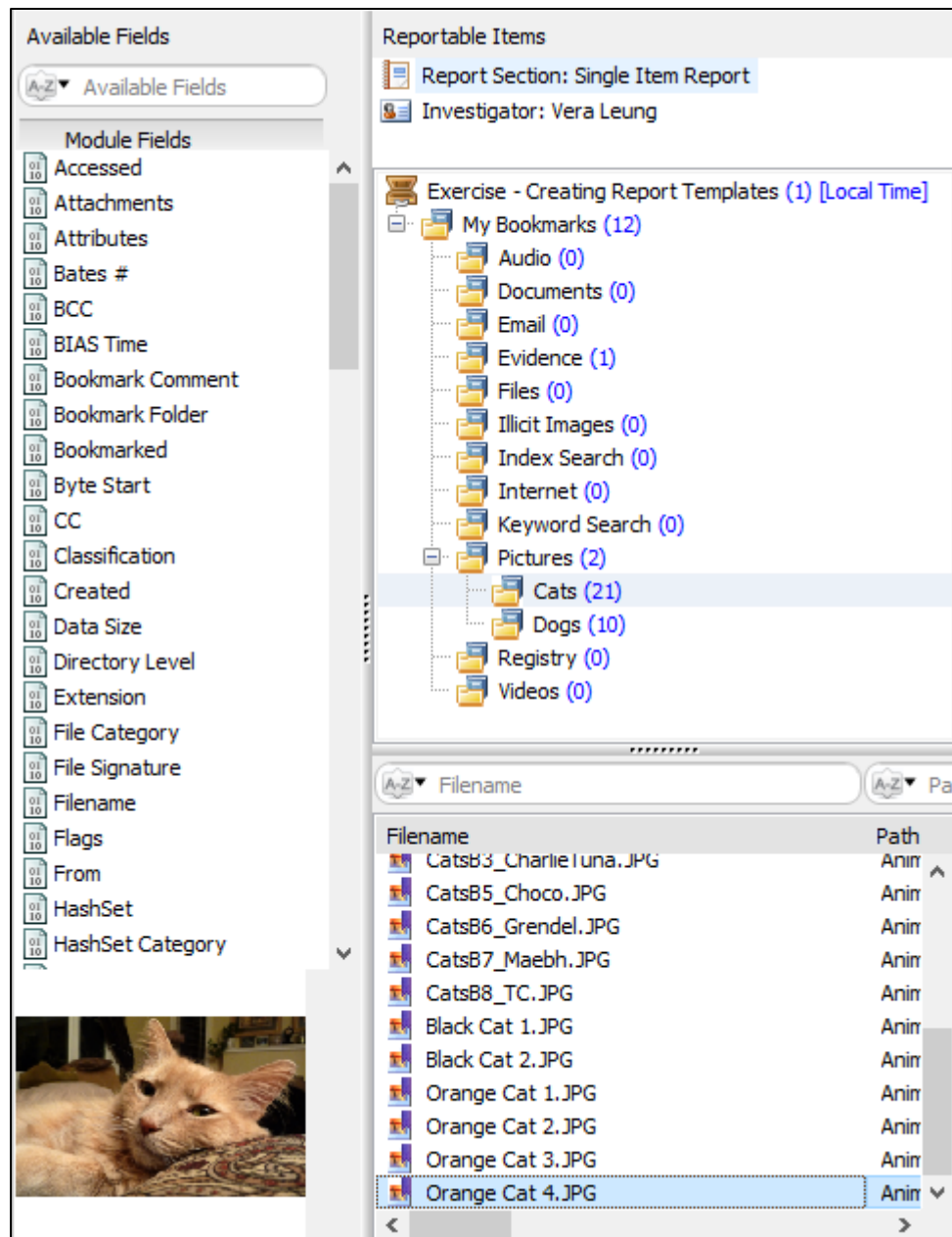
Note that the **Edit** button changes from **Edit** to **Preview** depending on whether the **Report Editor** window is in Preview or Edit mode:

Figure 284: Edit/Preview button



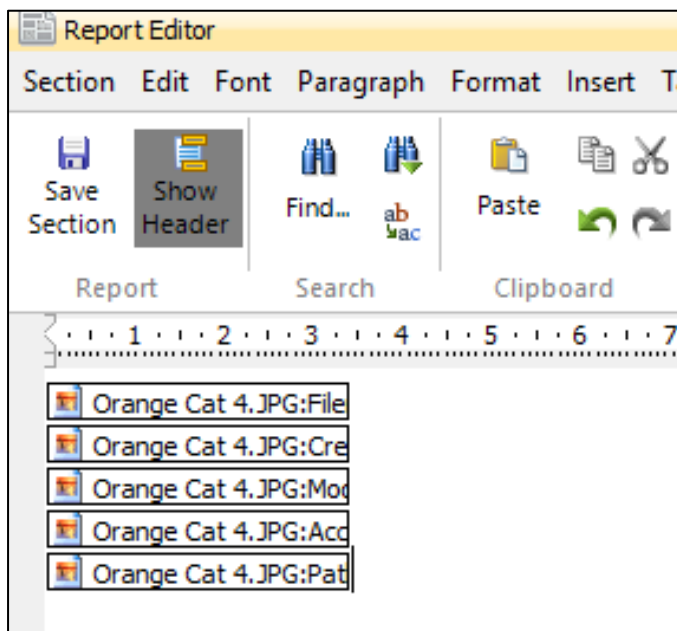
- b. In the **Reportable Items** column (shown in Figure 285 below), click on the folder containing the desired bookmark, i.e., **Cats**. Then at the bottom of this column, locate and click on the required file, i.e., **Orange Cat4.JPG**.
- c. The fields available for the highlighted file are now shown in the **Available Fields** column to the left (as shown in Figure 285 below).

Figure 285: Selecting a Bookmarked File and its Fields



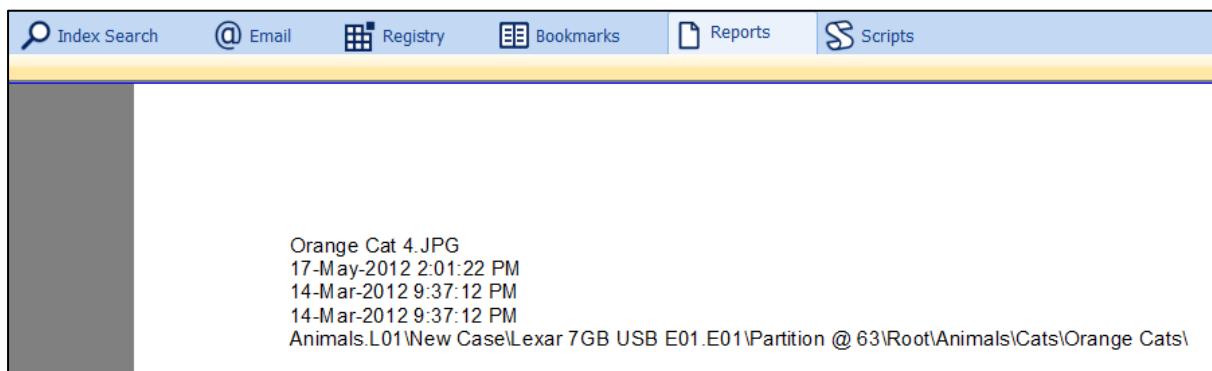
- d. Select the required fields with the mouse (use the CTRL key to select a group) and **drag and drop** the fields for the file onto the Report Editor window. In this example, we are using the fields: Filename; Created; Modified; Accessed; and Path. Organize the fields into a vertical list, as shown in Figure 286 below:

Figure 286: Report Editor Showing Fields



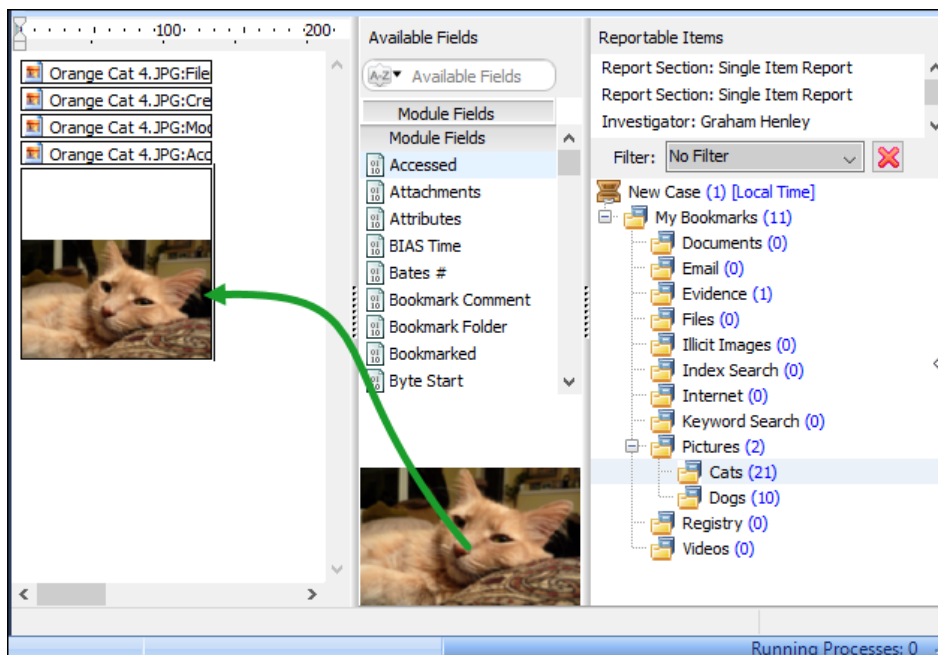
- e. Preview the report by clicking on the **Preview** button at the top of the folder tree. This will show the contents of the field, as shown in Figure 287 below:

Figure 287: Report Editor - Preview



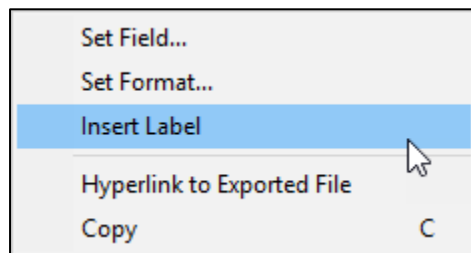
- f. To insert the picture:
- Click on the **Edit** button to edit the page in the Script Editor;
 - Click on the file name **Orange Cat 4.JPG** in the **Reportable Items** column (shown in Figure 285 above). The picture will display at the bottom of the **Available Fields** Column;
 - Drag and drop the picture to the required position onto the report, as shown in Figure 288 below:

Figure 288: Drag and drop picture onto report



- g. To insert field labels, click on a field then right click and select **Insert Label** from the drop-down menu:

Figure 289: Insert default label for report field



- h. Use the format toolbar to add formatting (font, text size, color, etc.). The formatted output is shown in Figure 281 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 290 below:

Figure 290: Exercise 2 – Listing bookmarked files in a table

Filename	Created	Modified
CatsB7_Maebh.JPG	17-May-12 2:01:22 PM	14-Mar-12
CatsB6_Grendel.JPG	17-May-12 2:01:22 PM	14-Mar-12
CatsB5_Choco.JPG	17-May-12 2:01:22 PM	14-Mar-12
CatsB3_CharlieTuna.JPG	17-May-12 2:01:21 PM	14-Mar-12
CatsB1_Corduroy.JPG	17-May-12 2:01:21 PM	14-Mar-12
CatsA9_Minikin.JPG	17-May-12 2:01:21 PM	14-Mar-12
CatsA8_Gadget.JPG	17-May-12 2:01:21 PM	14-Mar-12
CatsA7_TomTom.JPG	17-May-12 2:01:21 PM	14-Mar-12
CatsA5_Starbuck.JPG	17-May-12 2:01:21 PM	14-Mar-12
CatsA4_Kristaji.JPG	17-May-12 2:01:21 PM	14-Mar-12
DogsA9_Kodie.JPG	17-May-12 2:01:23 PM	14-Mar-12
DogsA8_Jack-Jack.JPG	17-May-12 2:01:23 PM	14-Mar-12

STEP 1 – 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:

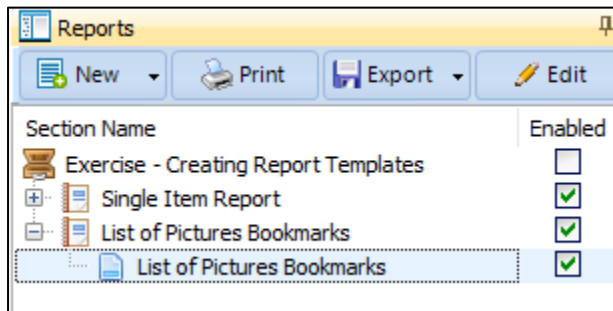
- Switch to the Reports module.
- In the Reports tree, select **New > Blank Report** (as shown in Figure 282 above).

STEP 3 – RENAME THE BLANK REPORT

Rename the report:

- a. Click and hover on the report name to rename it to **List of Pictures Bookmarks**.
- b. Repeat this step to rename the section, as shown in Figure 291 below:

Figure 291: Renaming the report

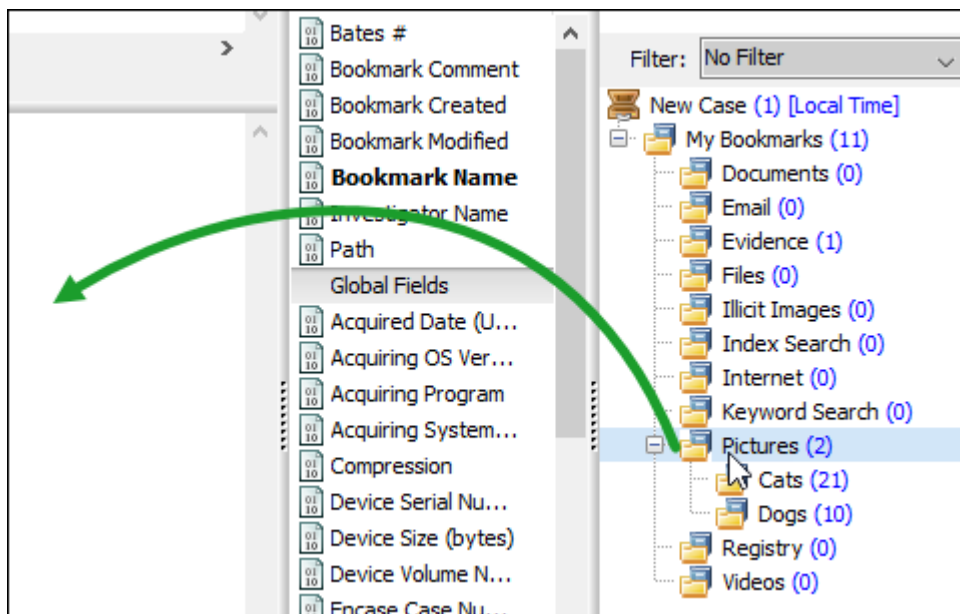


STEP 4 – ADD A REPEATING TABLE TO THE REPORT

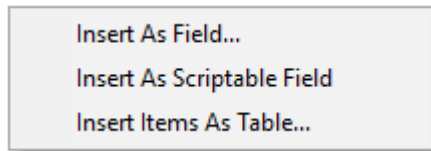
Edit and add a repeating table to the report:

- 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 292 below:

Figure 292: Drag and drop folder

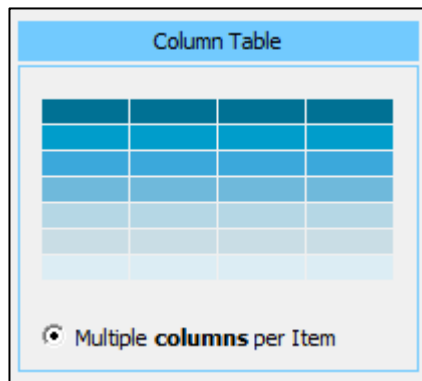


- c. Select to **Insert Item as Table** for the table to iterate through each bookmarked file:



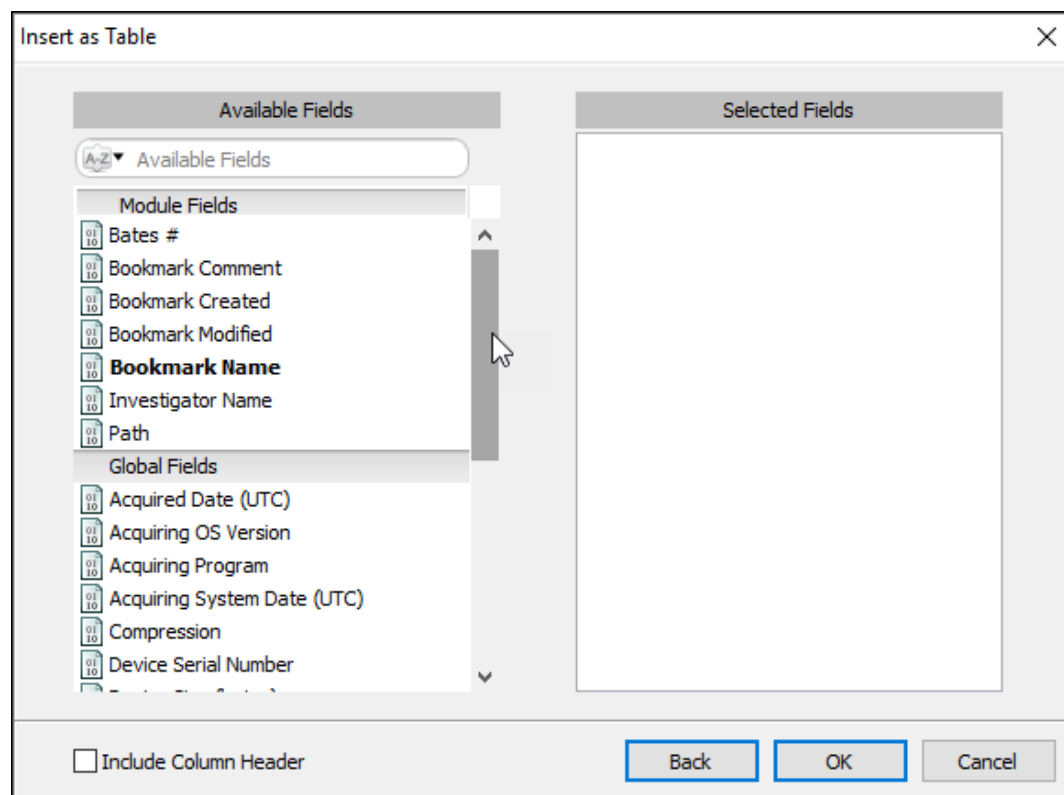
- d. Select the **Multiple columns per item** column table:

Figure 293: Selecting a List View Table Style



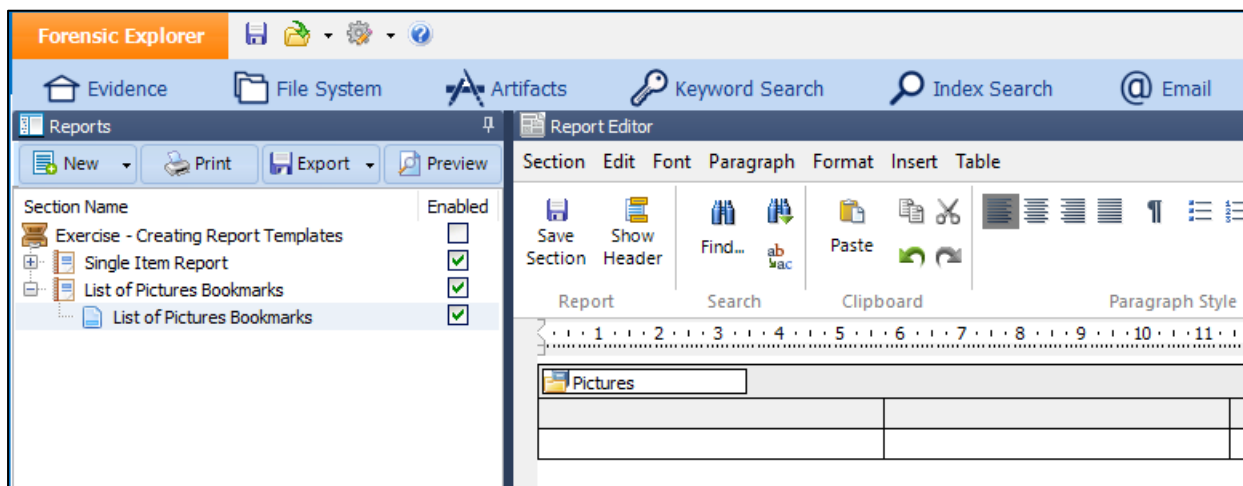
- e. The **Insert as Table** window opens showing the available fields for the **Pictures** bookmark folder. In this example we will not use fields associated with this bookmark folder. Leave the **Selected Fields** blank and click OK:

Figure 294: Insert Table Window



A blank **Pictures** table will be added to the report, as shown in Figure 295 below:

Figure 295: Pictures bookmarks table



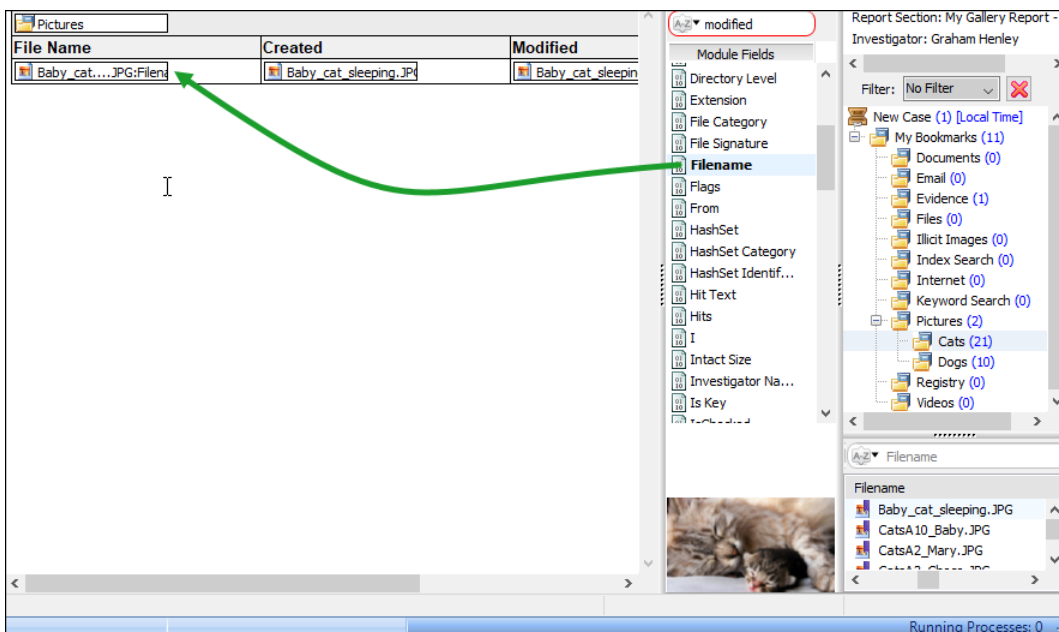
Note that hovering over the Pictures folder with the mouse will show the source bookmark folder for the table (My Bookmarks\Pictures) in the bottom information bar of the Report Editor window.

STEP 5 - POPULATE THE REPEATING TABLE WITH THE REQUIRED FIELDS

To populate the table with the required fields:

- In the Reportable Items column, select the sub bookmark folder containing the files, e.g., **Cats**;
- 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 296 below:

Figure 296: Adding fields to a table



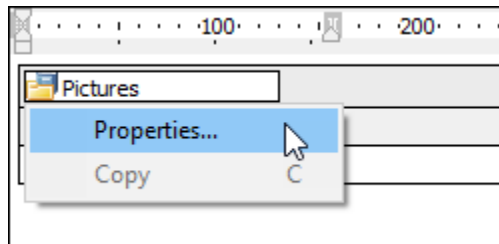
- Format the table as needed and switch to the Preview window to view the result. The table list should look like Figure 290 at the start of this exercise.

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:

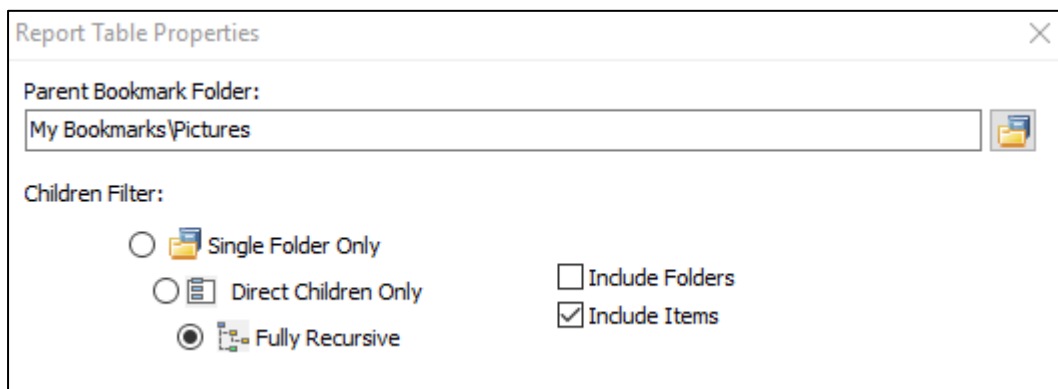
- a. Hover the mouse over the table folder, i.e., **Pictures**. Right click and select **Properties**:

Figure 297: Table Properties



This will open the **Report Table Properties** window:

Figure 298: 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.

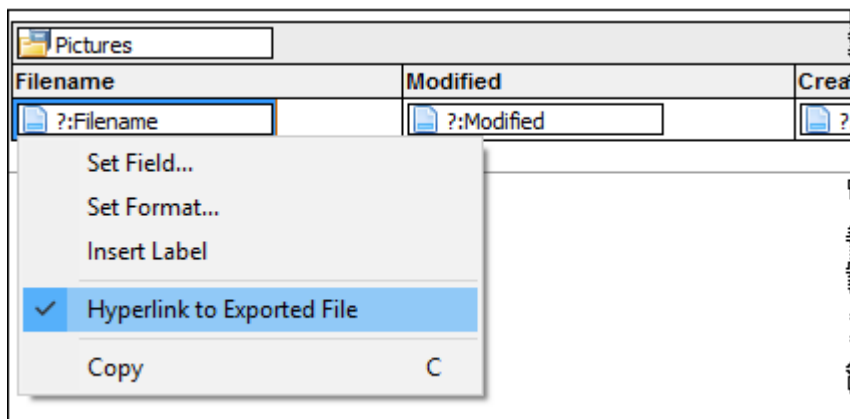
STEP 7 - PREVIEW THE FINAL REPORT

- a. Click on the **Preview** button to display the report. The report should appear like Figure 290 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 299 below:

Figure 299, 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 300 below:

Figure 300: a report with a hyperlink

Filename	Modified	Created
CatsA10_Baby.JPG	14-Mar-12 9:37:11 PM	11-Aug-14 11:09:28
CatsA2_Mary.JPG	14-Mar-12 9:37:11 PM	11-Aug-14 11:09:28
CatsA3_Choco.JPG	14-Mar-12 9:37:12 PM	11-Aug-14 11:09:28
CatsA4_Kristaji.JPG	14-Mar-12 9:37:12 PM	11-Aug-14 11:09:28
CatsA5_Starbuck.JPG	14-Mar-12 9:37:12 PM	11-Aug-14 11:09:28
CatsA7_TomTom.JPG	14-Mar-12 9:37:12 PM	11-Aug-14 11:09:28
CatsA8_Gadget.JPG	14-Mar-12 9:37:12 PM	11-Aug-14 11:09:28
CatsA9_Minikin.JPG	14-Mar-12 9:37:12 PM	11-Aug-14 11:09:28
CatsB1_Corduroy.JPG	14-Mar-12 9:37:12 PM	11-Aug-14 11:09:28
CatsB3_CharlieTuna.JPG	14-Mar-12 9:37:12 PM	11-Aug-14 11:09:28
CatsB5_Choco.JPG	14-Mar-12 9:37:12 PM	11-Aug-14 11:09:28
CatsB6_Grendel.JPG	14-Mar-12 9:37:12 PM	11-Aug-14 11:09:28
CatsB7_Maebh.JPG	14-Mar-12 9:37:12 PM	11-Aug-14 11:09:28
CatsB8_TC.JPG	14-Mar-12 9:37:12 PM	11-Aug-14 11:09:28
DogsA10_Maddie.JPG	14-Mar-12 9:37:12 PM	11-Aug-14 11:09:28
DogsA1_GretaGarbo.JPG	14-Mar-12 9:37:12 PM	11-Aug-14 11:09:28
DogsA4_Brady.JPG	14-Mar-12 9:37:13 PM	11-Aug-14 11:09:28
DogsA6_Shay.JPG	14-Mar-12 9:37:13 PM	11-Aug-14 11:09:28
DogsA7_Moka.JPG	14-Mar-12 9:37:13 PM	11-Aug-14 11:09:28
DogsA9_Kodie.JPG	14-Mar-12 9:37:13 PM	11-Aug-14 11:09:28

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:

- 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**:

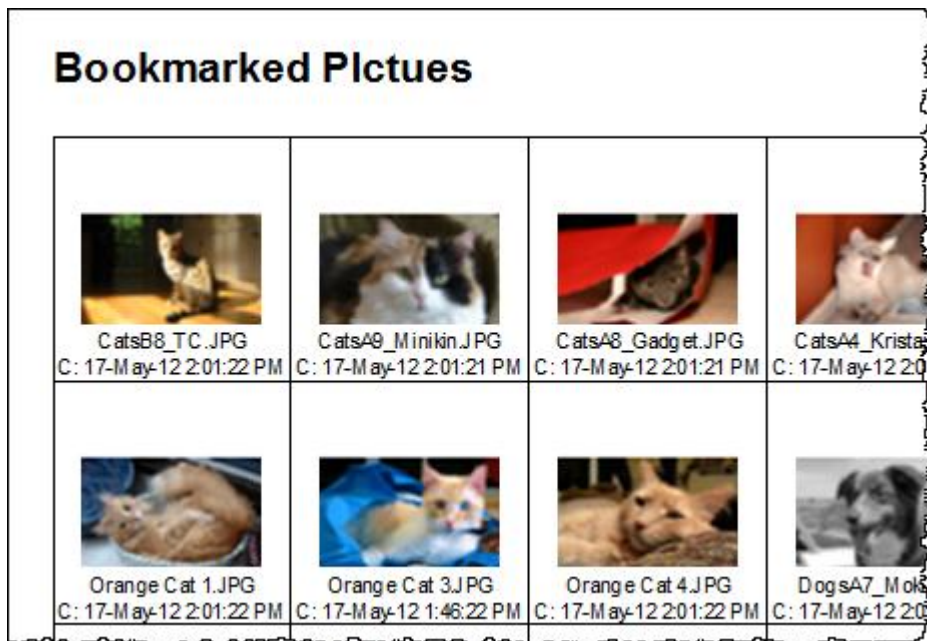
- a. Follow the instructions in 18.3.8 above to save the report as a template for future use.

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 301 below:

Figure 301: creating a Gallery View Report (finished report shown)



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:

- Switch to the Reports module.
- In the Reports tree, select **New > Blank Report** (as shown in Figure 282 above).

STEP 3 – RENAME THE BLANK REPORT

Rename the report:

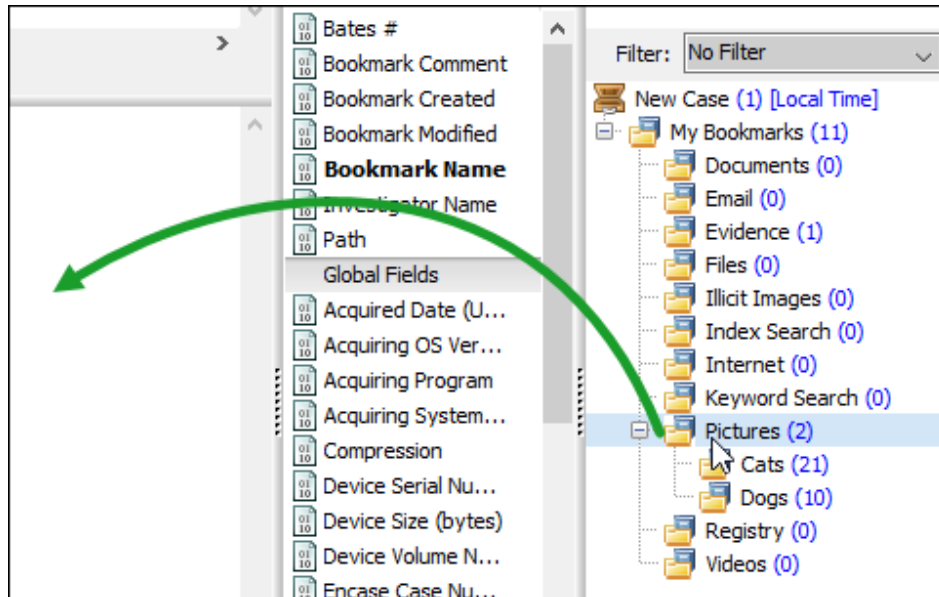
- Click and hover on the report name to rename the section to **My Gallery Report - Pictures**.
- Repeat this step to rename the report section.

STEP 4 – ADD A REPEATING TABLE TO THE REPORT

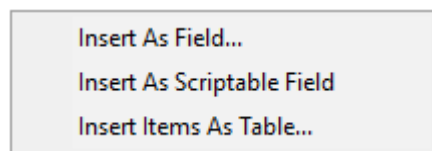
Edit and add a repeating table to the report:

- 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 292 above:

Figure 302: Drag and drop folder

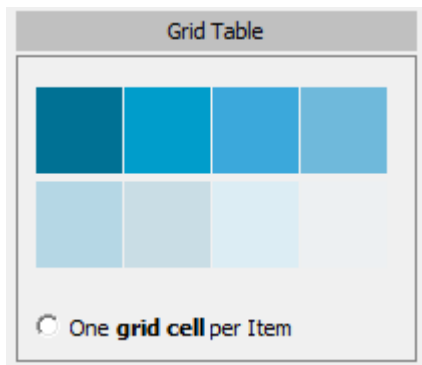


- c. Select to **Insert Item as Table** for the table to iterate through each bookmarked file:



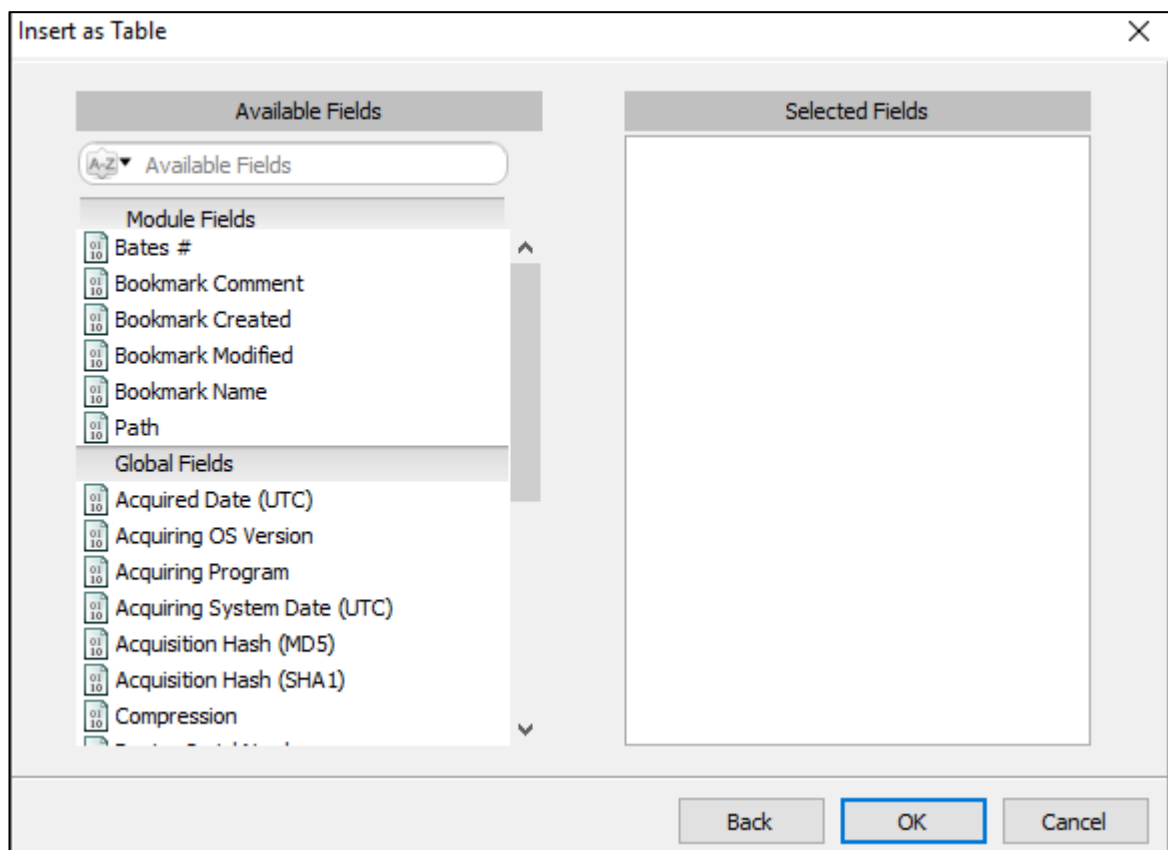
- d. In the table selection window, use the **Grid Table** so that pictures are entered horizontally across the screen in the gallery view format:

Figure 303: Selecting a Gallery View Table Style



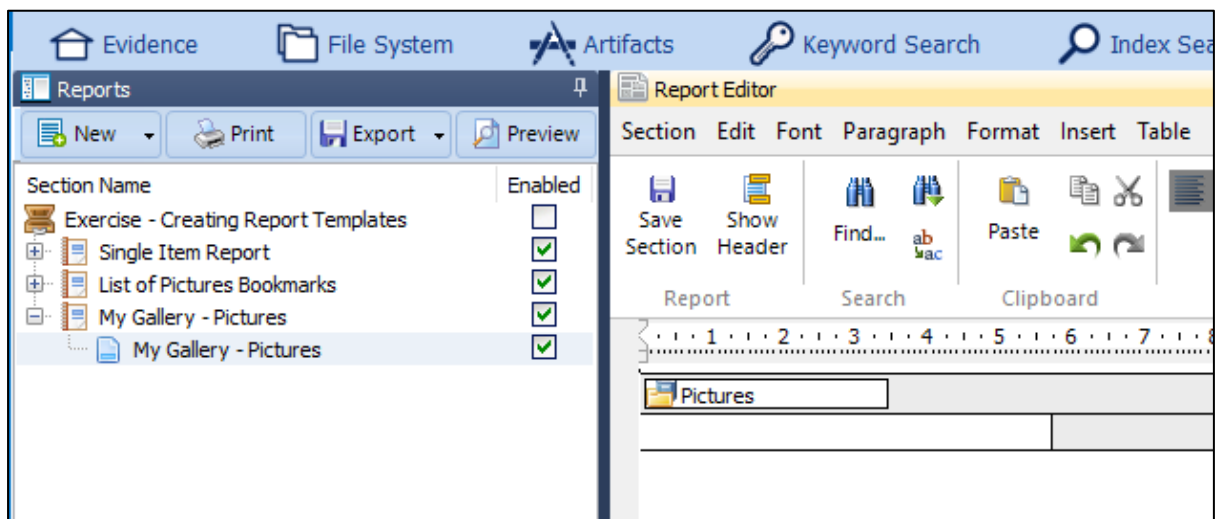
- e. The **Insert as Table** window opens showing the available fields for the **Pictures** bookmark folder:

Figure 304: Insert as Table



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:

Figure 305: Pictures table



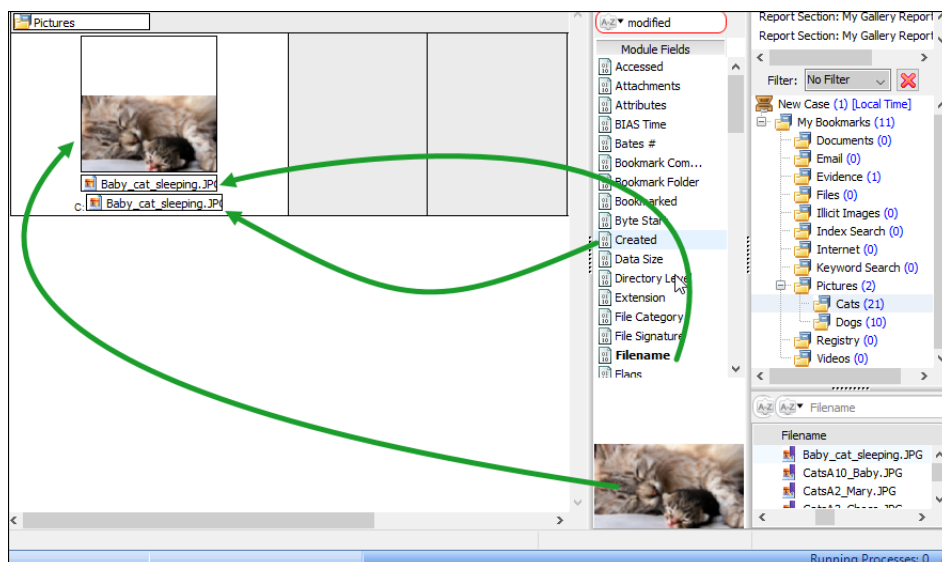
Note that hovering over the **Pictures** folder with the mouse will show the source bookmark folder for the table (My Bookmarks\Pictures) in the bottom information bar of the Report Editor window.

STEP 5 - POPULATE THE REPEATING TABLE WITH THE REQUIRED FIELDS

To populate the table with the required fields:

- In the Reportable Items column, select the sub bookmark folder containing the files, e.g., **Cats**;
- 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 296 above:

Figure 306: Adding fields to a table



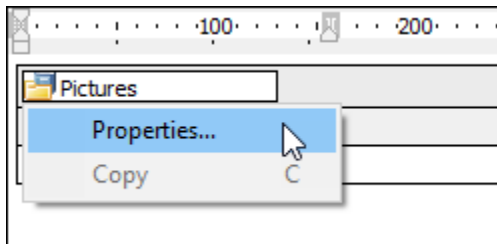
- Format the table as needed and switch to the Preview window to view the result. The table list should look like Figure 290 at the start of this exercise.

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:

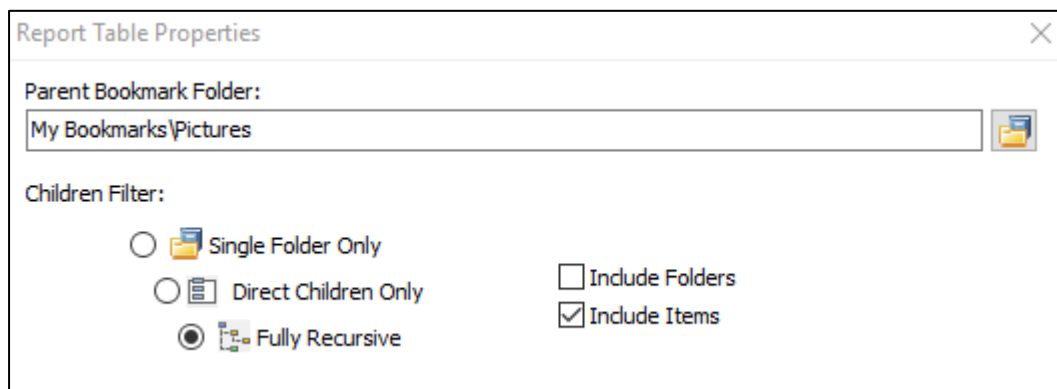
- a. Hover the mouse over the table folder, i.e., **Pictures**. Right click and select **Properties**:

Figure 307: Table Properties



This will open the **Report Table Properties** window:

Figure 308: 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 like Figure 290 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 to the instructions in the previous 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 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 subcategory, i.e., Cats and Dogs. The finished report looks as follows:

Figure 309: Finished nested table report

Outer Table		
Cats		
Filename	Created	Modified
Baby_cat_sleeping.JPG	17-May-12 2:01:20 PM	14-Mar-
Black Cat 1.JPG	17-May-12 2:01:21 PM	14-Mar-
Black Cat 2.JPG	17-May-12 2:01:21 PM	14-Mar-
CatsA10_Baby.JPG	17-May-12 2:01:21 PM	14-Mar-
CatsA2_Mary.JPG	17-May-12 2:01:21 PM	14-Mar-
CatsA3_Choco.JPG	17-May-12 2:01:21 PM	14-Mar-
CatsA4_Kristaji.JPG	17-May-12 2:01:21 PM	14-Mar-
CatsA5_Starbuck.JPG	17-May-12 2:01:21 PM	14-Mar-
CatsA7_TomTom.JPG	17-May-12 2:01:21 PM	14-Mar-
CatsA8_Gadget.JPG	17-May-12 2:01:21 PM	14-Mar-
CatsA9_Minikin.JPG	17-May-12 2:01:21 PM	14-Mar-
CatsB1_Corduroy.JPG	17-May-12 2:01:21 PM	14-Mar-
CatsB3_CharlieTuna.JPG	17-May-12 2:01:21 PM	14-Mar-
CatsB5_Choco.JPG	17-May-12 2:01:22 PM	14-Mar-
CatsB6_Grendel.JPG	17-May-12 2:01:22 PM	14-Mar-
CatsB7_Maebh.JPG	17-May-12 2:01:22 PM	14-Mar-
CatsB8_TC.JPG	17-May-12 2:01:22 PM	14-Mar-
Orange Cat 1.JPG	17-May-12 2:01:22 PM	14-Mar-
Orange Cat 2.JPG	17-May-12 2:01:22 PM	14-Mar-
Orange Cat 3.JPG	17-May-12 2:01:22 PM	14-Mar-
Orange Cat 4.JPG	17-May-12 2:01:22 PM	14-Mar-
Dogs		
Filename	Created	Modified
DogsA10_Maddie.JPG	17-May-12 2:01:22 PM	14-Mar-
DogsA1_GretaGarbo.JPG	17-May-12 2:01:23 PM	14-Mar-

The report is created using nested tables. The structure of the tables is described below:

Figure 310: Layout of a Nested Table

Pictures (bookmark folder)

This is the Outer table

Cats	
<i>This is the Inner table</i>	
File Name	Created Date
CAT1.JPG (Folder 1, Record 1)	Created Date
CAT2.JPG (Folder 1, Record 2)	Created Date
CAT3.JPG (Folder 1, Record 3)	Created Date

Dogs	
File Name	Created Date
DOG1.JPG (Folder 2, Record 1)	Created Date
DOG2.JPG (Folder 2, Record 1)	Created Date
DOG3.JPG (Folder 2, Record 1)	Created Date

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.

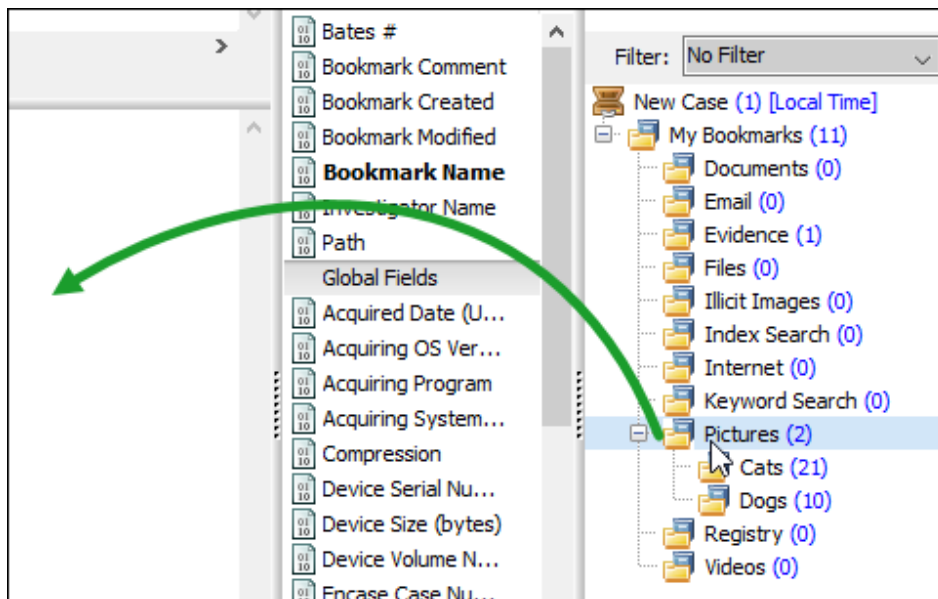
STEP 4 – ADD A REPEATING OUTER TABLE TO THE REPORT

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.

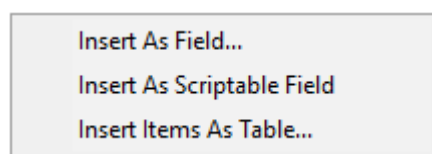
To **add** the **outer table** to the report:

- 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 292 above:

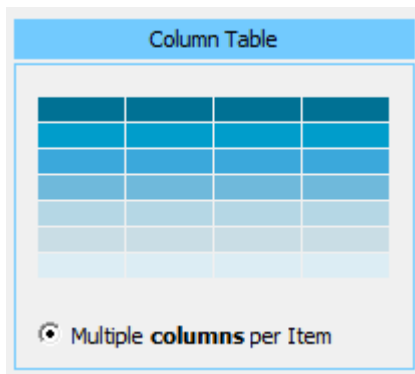
Figure 311: Drag and drop folder



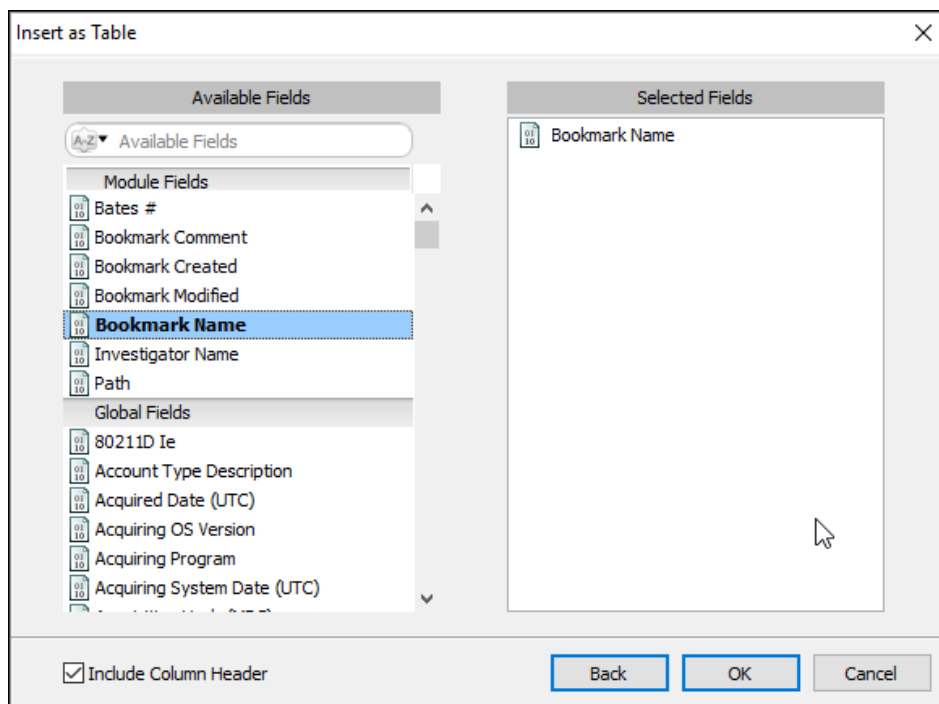
- c. Select to **Insert Item as Table**:



- d. Use the table type **Multiple columns per Item**;

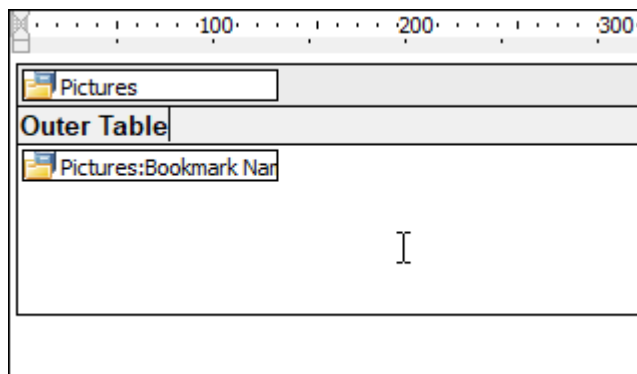


- e. Add the **Bookmark Name** field to the report:



- 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

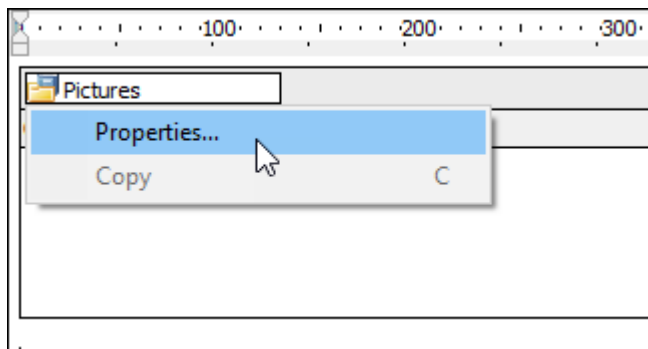


STEP 6 - SET THE PROPERTIES OF THE OUTER TABLE

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

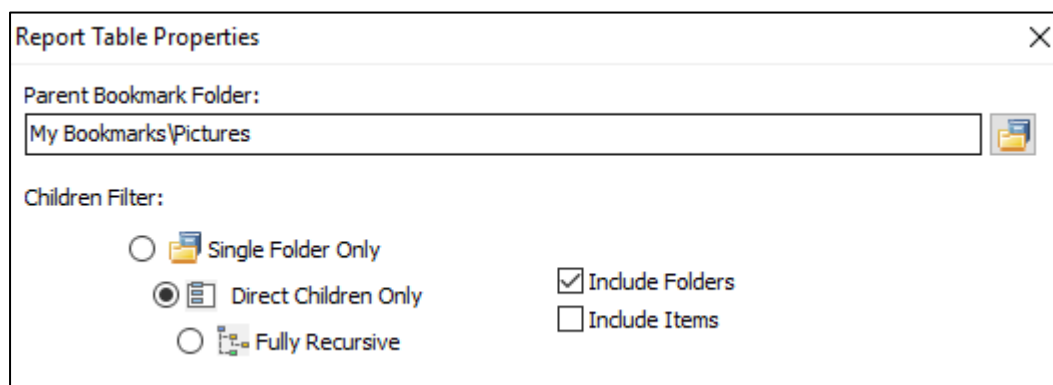
- Hover the mouse over the table folder, i.e., **Pictures**. Right click and select **Properties**:

Figure 312: Table Properties



This will open the **Bookmark Enumerator Properties** window:

Figure 313: 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

Outer Table
Cats
Dogs

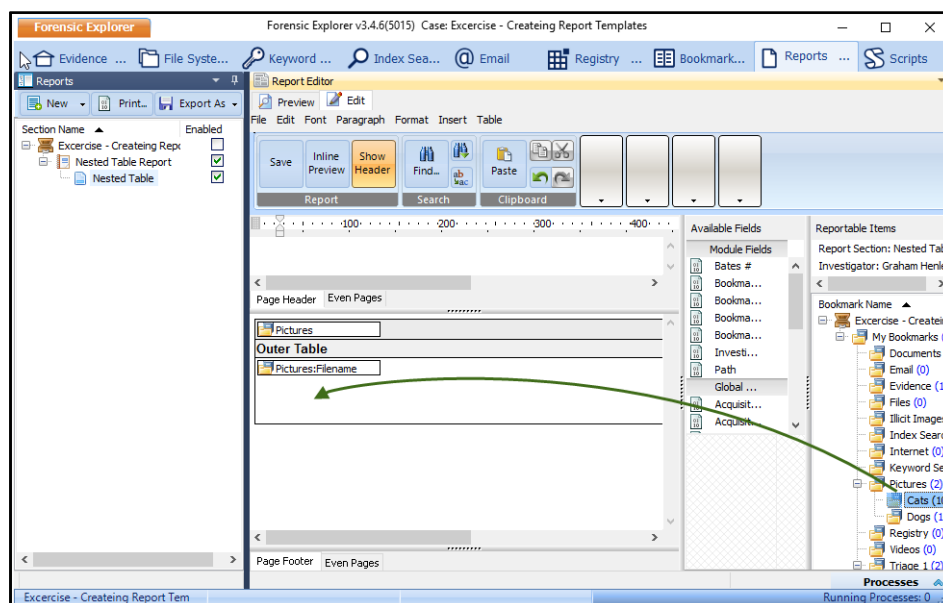
STEP 5 – ADDING THE NESTED INNER TABLE

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).

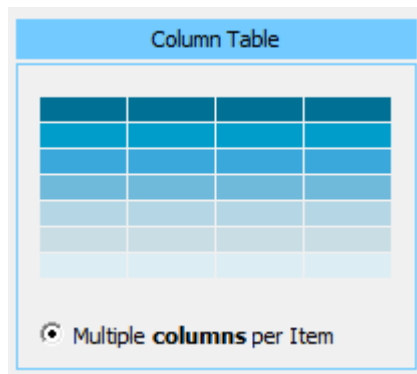
To add the inner table:

- 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 314 below:

Figure 314: Nested table. Insert a sub-table.

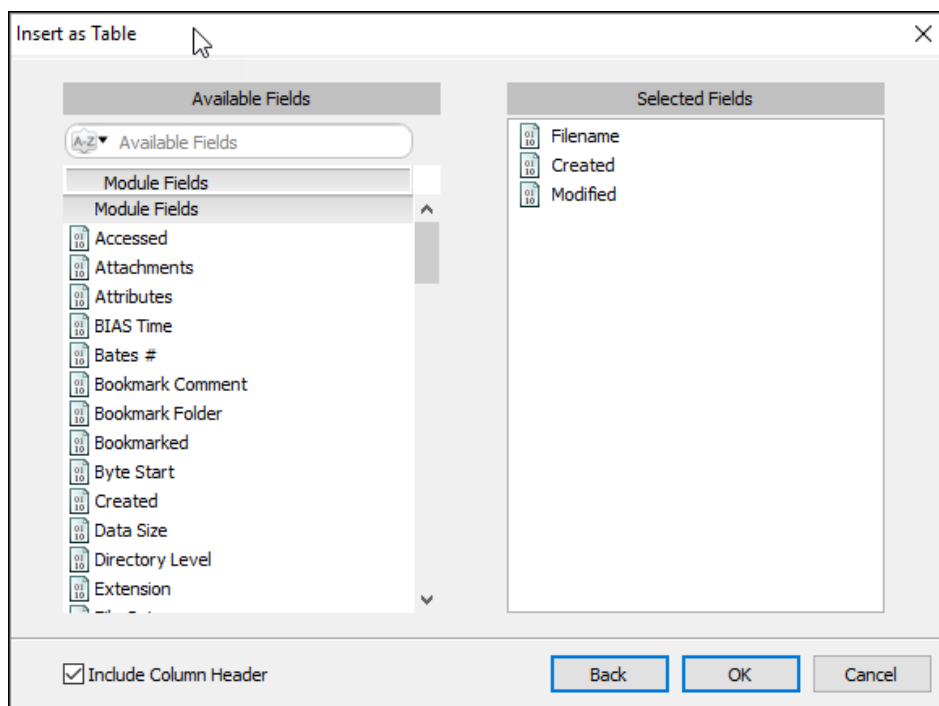


- c. Select to **Insert Item as Table** and use the table type **Multiple columns per Item**;



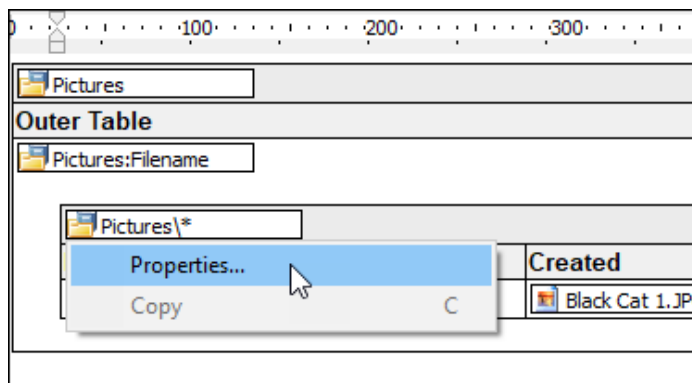
- d. Select the fields to use in the table. In this exercise use Filename, Created and modified, as shown in Table field selection Figure 315 below:

Figure 315: Table field selection



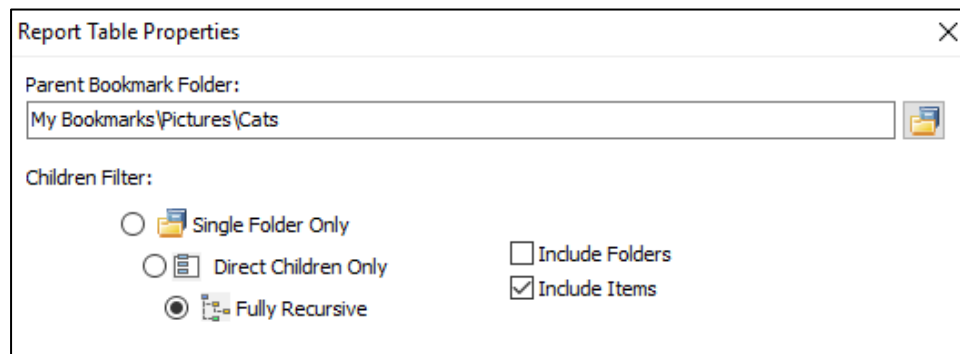
- e. Click OK to drop the table into the report.
- f. The Inner Table will display a “*”, indicating that is operating on the first sub folder, as shown in Figure 316 below (a refresh of the view may be required to see the *).
- g. Right click on the **Pictures*** folder and display the contents of each sub folder (i.e., Cats & Dogs) by selecting:

Table 3: Open the Properties of the inner table



- h. Set the properties of the of the inner table:

Figure 316: 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:

- Click on the **Preview** button to display the report. The report should appear like Figure 309Figure 290 at the beginning of this exercise.
- Update formatting as needed.

STEP 8 – ADDING HYPERLINKS FOR THE EXPORTED REPORT

If hyperlinks are required for an exported report, refer to the instructions in the previous 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**:

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 criterion 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.

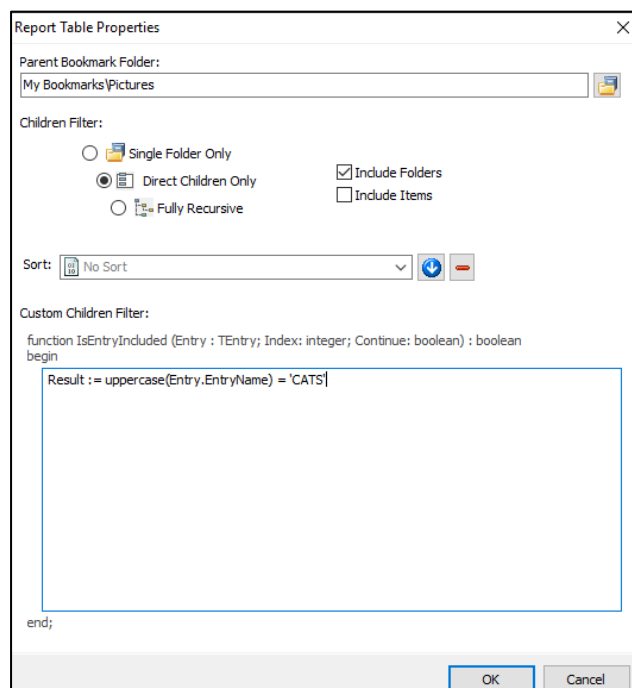
FILTER 1 – FILTER BY BOOKMARK FOLDER (OUTER TABLE)

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:

Result := uppercase(Entry.EntryName) = 'CATS' as shown in Figure 317 below:

Figure 317: Filter a bookmark folder



FILTER 2 – FILTER TABLES USING A FILE NAME

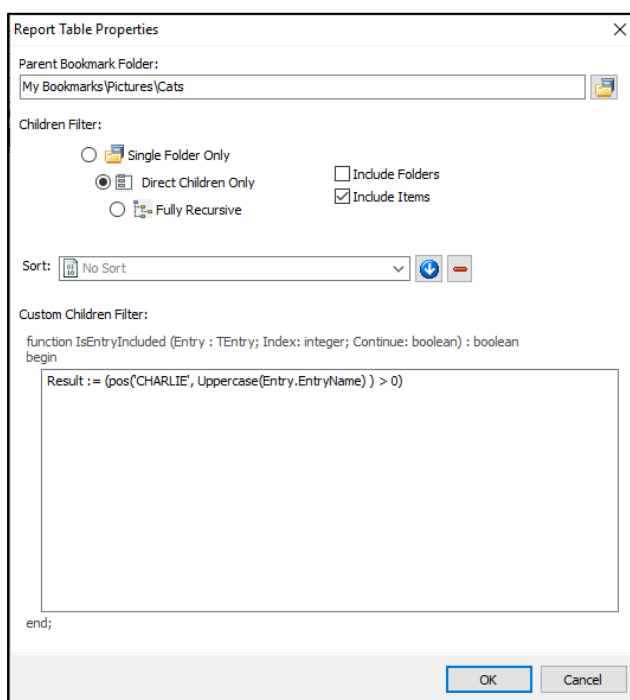
To filter a table report by filename;

- 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 318: Filter a file name



which gives the following result:

Figure 319: Results of filtering on the inner table

Outer Table	
Cats	
File Name	Created
CatsB3_CharlieTuna.JPG	17-May-12 2:01
Dogs	
File Name	Created

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))
```

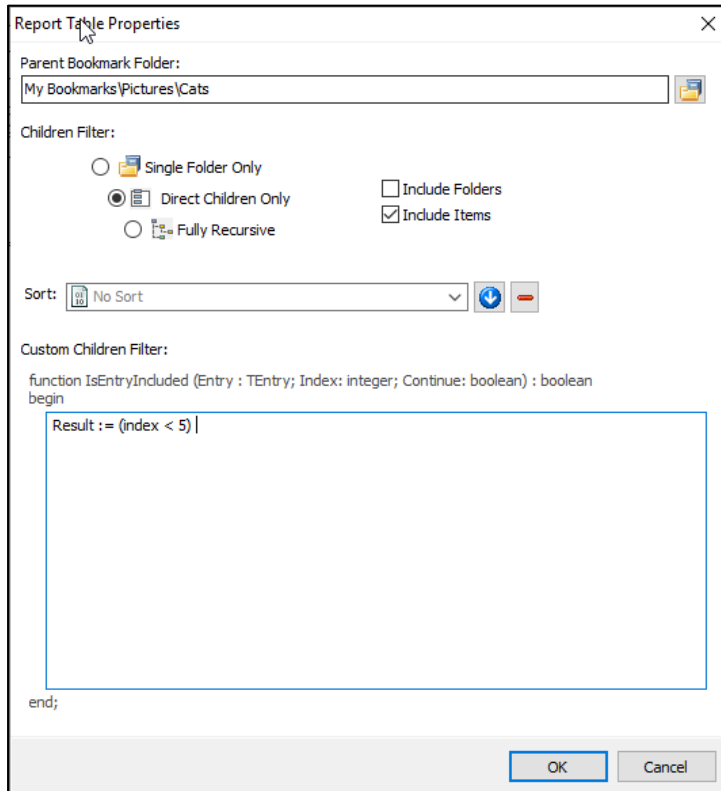
FILTER 3 – LIMIT THE NUMBER OF RECORDS SHOWN IN A TABLE

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

- Remove any prior filters;
- Right click on the **Pictures*** folder (inner table) and in the drop-down menu select **Properties**;
- In the Table Iteration Filter enter the filter:

Result := (index < 5) as shown below. This will list the first 5 records in the bookmark folder:

Figure 320: Limit reporting on a bookmark folder to X records



Chapter 19 – Scripts Module

In This Chapter

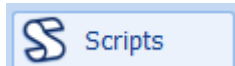
CHAPTER 19 - SCRIPTS MODULE

19.1	Scripts Module.....	310
19.1.1	Script Installation.....	310
19.1.2	Backup scripts.....	311
19.1.3	Scripts Window.....	312
19.1.4	Script Editor window.....	315
19.1.5	Messages Window (Console).....	316
19.2	Managing scripts in the scripts window.....	317
19.3	Introduction to Scripting.....	318
19.3.1	Programming Comments.....	318
19.3.2	Reserved Words.....	318
19.3.3	Uses (libraries).....	319
19.3.4	Const.....	319
19.3.5	Var.....	319
19.3.6	Procedures and Functions.....	320
19.3.7	Begin and End.....	320
19.3.8	Errors.....	320

19.1 SCRIPTS MODULE

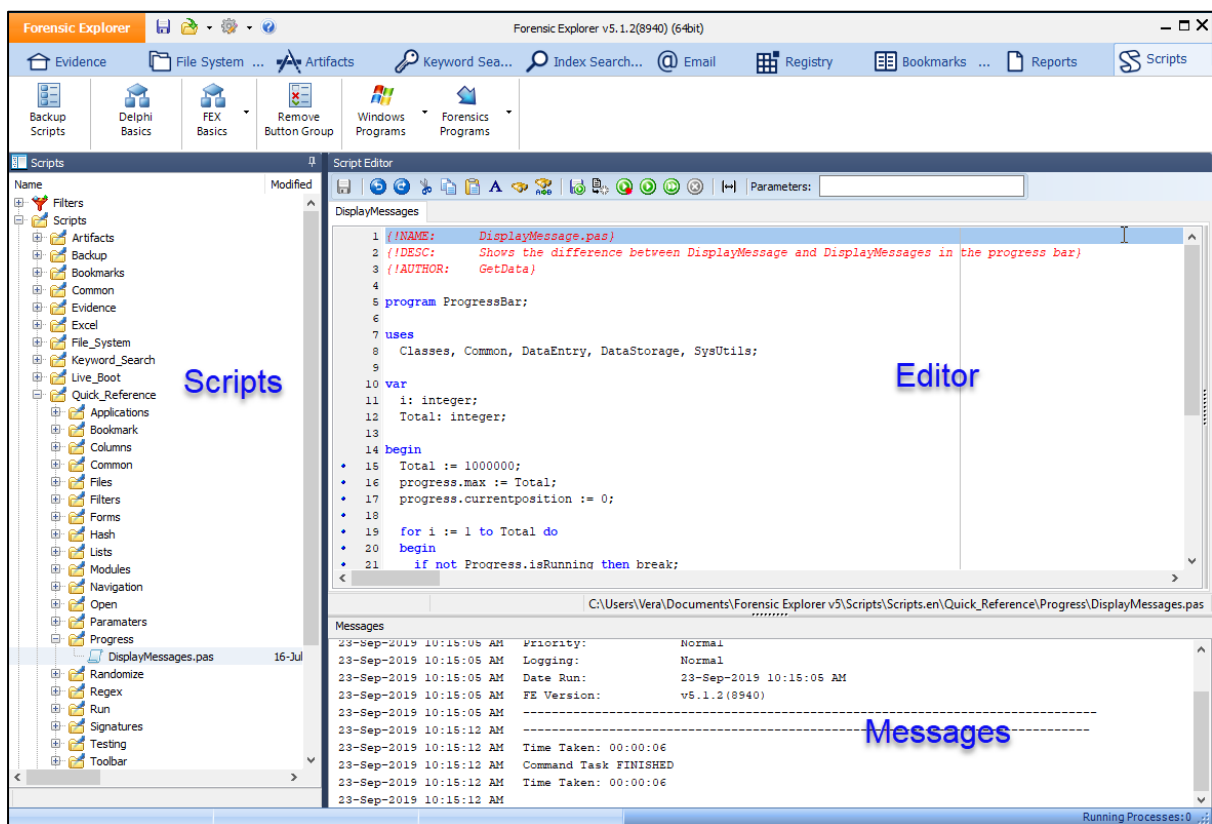
Forensic Explorer utilizes Pascal as its scripting language. Scripts are written and run in the scripts module or launched in other modules via toolbar buttons or by other scripts. The Scripts module is accessed via the scripts tab:

Figure 321: Scripts module tab



The scripts module is arranged into three windows: **Scripts**; **Script Editor**; and **Messages**, as shown in Figure 322 below:

Figure 322: Scripts module



19.1.1 SCRIPT INSTALLATION

Forensic Explorer is installed with a number of default scripts in the paths:

- `..\Documents\Forensic Explorer v5\Scripts\Scripts.en\`
- `..\Documents\Forensic Explorer v5\Filters\Filters.en\`

Scripts are separated into sub-folders based on their function.

19.1.2 BACKUP SCRIPTS

When editing scripts, it can be useful to take a periodic backup of an individual script, or the entire scripts folder. This is achieved with the **Backup Scripts** button in the Scripts module toolbar.

Figure 323: Scripts module, Backup Scripts.

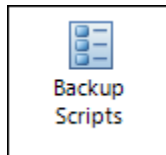
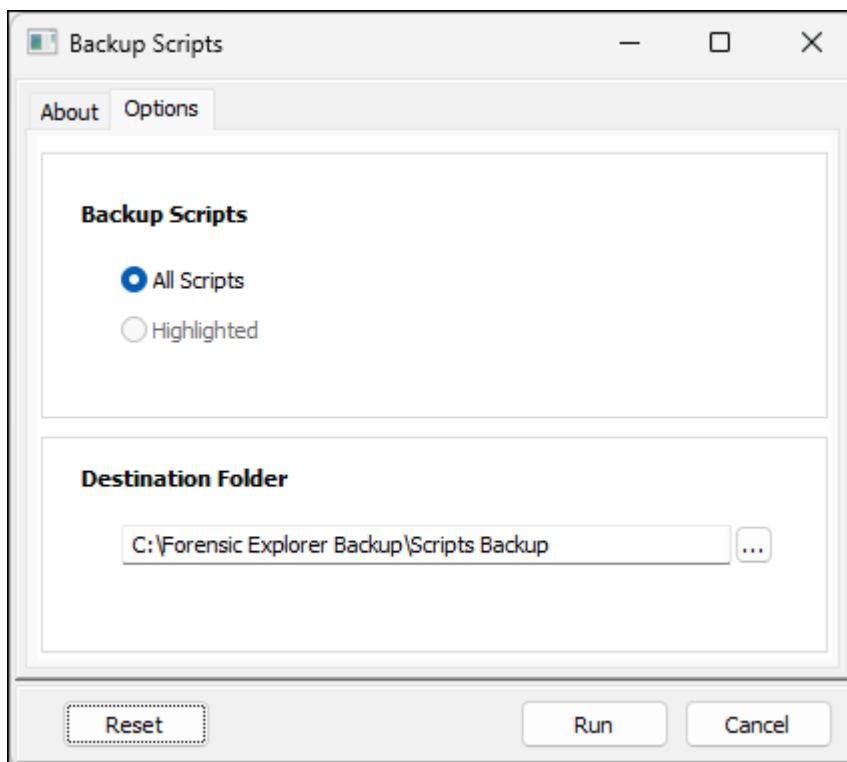


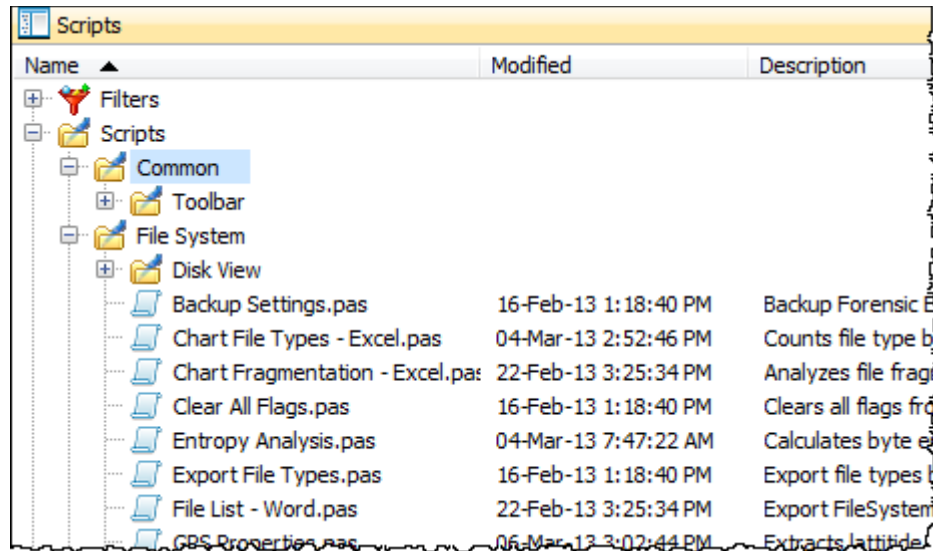
Figure 324: Backup Scripts.



19.1.3 SCRIPTS WINDOW

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

Figure 325: Scripts Windows showing .pas file attributes



Script Attributes

The Scripts window lists the attributes of each script:

Name: The script name is auto generated from the “script.pas” file name.

Description and Author: These attributes are auto generated from the comments at the start of the script.

Modified and Created: Script dates are auto generated from the Windows date and time stamps of the .pas file.

Hash (SHA256): A SHA256 hash is calculated for each script. The hash is updated each time the Scripts window is refreshed. To manually refresh the Scripts window, **right click** in the Scripts window and select **Refresh** option from the drop-down menu.

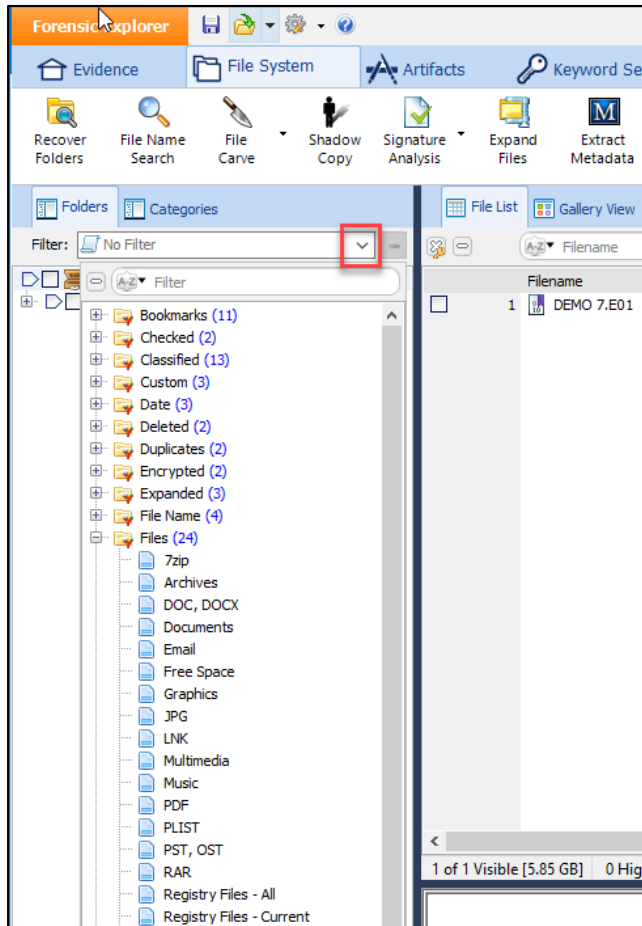
The purpose of the SHA256 has is so that the investigator can validate the authenticity of a GetData script, or a script from a trusted third party.

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

Figure 326: Tree view filter (File System Folders view)



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.

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

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 ExplorerVx\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.

19.1.4 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.
-  Compile and save binary format.
-  Compile current script.
-  Break point a script.
-  (Save and) Run script as a single thread.
-  Run a threaded script.
-  Cancel the execution of the script.
-  Add/Remove comment lines (Ctrl + Q)

Parameters:

Enter script parameters, e.g., "Parameter One" "Two" "Three" "Four".

19.1.5 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 date and time reference using a using the command “`ConsoleLog('Text')`”. See Appendix 7 - Sample Script, for an example.

If a script is run in the Scripts module, the output will appear in the Messages window. However, if a script is executed in another module (run from a toolbar button or a link) the output is written to the log file for that module. Access the log for a module via the “Processes” log (see 7.4 - Task Processes List, for more information).

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 **Scripts > New (.pas)**
2. Enter the name of the new script in the popup **New (Scripts)** 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**.

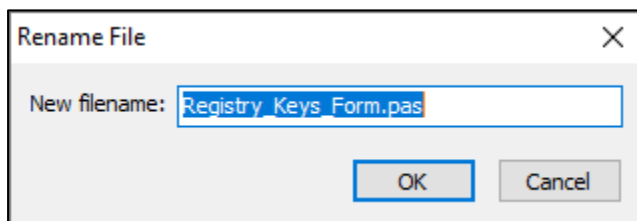
To copy a script:

1. Right click on the script in the **Scripts window**.
2. Select **Scripts > 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 **Scripts > Rename** from the drop-down menu. Edit the file name in the **Rename File** window:



Note: If the renamed file does not appear, **right click in the Scripts window**, and use the **Refresh** option to refresh the display. If the renamed file still does not appear, check to see that it has been renamed with the .pas extension.

To delete a script:

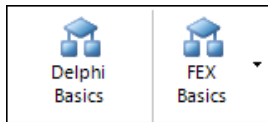
1. Highlight the script in the **Scripts window**.
2. Right click and select **Scripts > Delete** from the drop-down menu.

A confirmation window will appear to confirm that the delete is required.

19.3 INTRODUCTION TO SCRIPTING

Forensic Explorer is installed with “**Delphi Basics**”© reference documentation. It is installed in the path: “C:\Program Files\GetData\Forensic Explorer v5\Delphi Basics\” and accessible by the “Delphi Basics” help button in the Script module toolbar (shown below):

Figure 327: Scripts Module toolbar, Delphi Basics, FEX 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.

FEX Basics can be used to quickly create a working example of FEX specific code. Includes additional templates to quickly create a working GUI script template.

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	in	label	mod
nil	not	of	or	packed	procedure
program	record	repeat	set	then	to
type	until	var	while	With	uses

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 328: 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 **semi-colon**. If a command extends over several lines, for example an “If Then Else” statement, generally the semi colon won’t appear until the end of the entire statement.

19.3.8 ERRORS

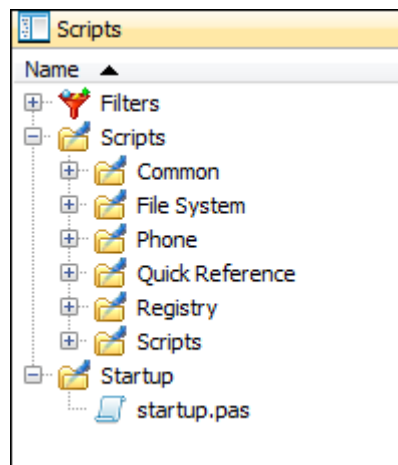
Errors in a script are reported in the Messages (console) window. Usually, the message will provide the line number of the code where the error appears. Double click on the line number to go directly to the problem line.

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:

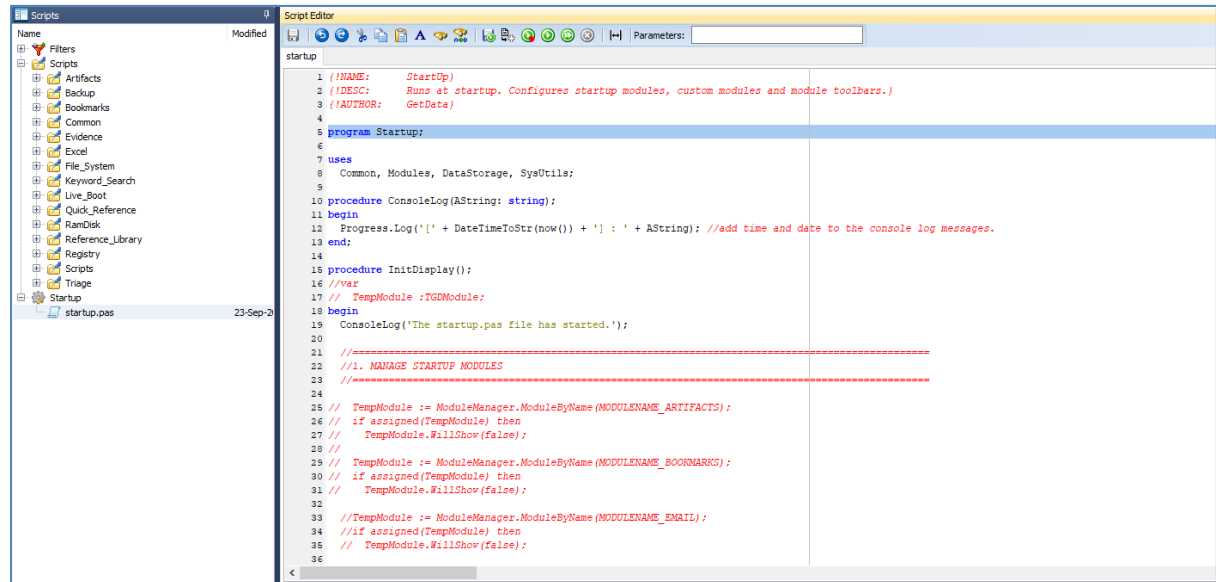
- Manage displayed modules (turn modules on/off at startup using the 'Startup Modules.pas' script.
- Startup with custom modules (see "Phone Module").
- Add button groups and buttons to module toolbars.

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 STARTUP 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.

Figure 329: Startup.pas



The method which can be used is to hard code the modules provided in the default startup.pas script. Example code to hide the Registry Module is shown below:

```
tempModule := ModuleManager.ModuleByName('Registry');
if assigned(tempModule) then
tempModule.WillShow(false);
```

Note: If the Scripts module is hidden with this technique, it will be necessary to edit the script using Windows Notepad (or other such program to re-enable the Scripts module).

Chapter 20 – Encryption

In This Chapter

CHAPTER 20 – ENCRYPTION

20.1	Encryption.....	324
20.1.1	Windows NTFS Encrypted files	324
20.1.2	APPLE AFPS encryption.....	324
20.1.3	Bitlocker Encryption.....	325
20.1.4	File Vault 2	326
20.2	Decrypting Supported Encryption Formats	326
20.3	Identifying Other Encrypted Files	330
20.3.1	Identifying encrypted files using Entropy	330
20.3.2	Identifying Encrypted Files using a THIRD-PARTY tool	330

20.1 ENCRYPTION

There are many different types of encryptions 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 encryptions:

- 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 330: Windows 10 file: Compressed (blue), Encrypted (green), Password Protected, and Normal

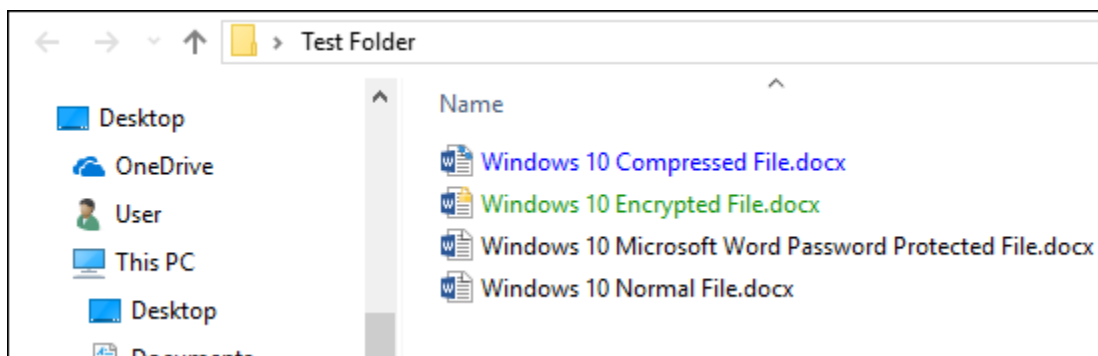


Figure 331: Windows 10 file: Compressed (blue), Encrypted (green), Password Protected, and Normal

Filename	Extension	Entropy
1 Windows 10 Compressed File.docx	docx	0.7226
2 Windows 10 Normal File.docx	docx	0.7422
3 Windows 10 Microsoft Word Password Protected File.docx	docx	0.8722
4 Windows 10 Encrypted File.docx	docx	0.9983

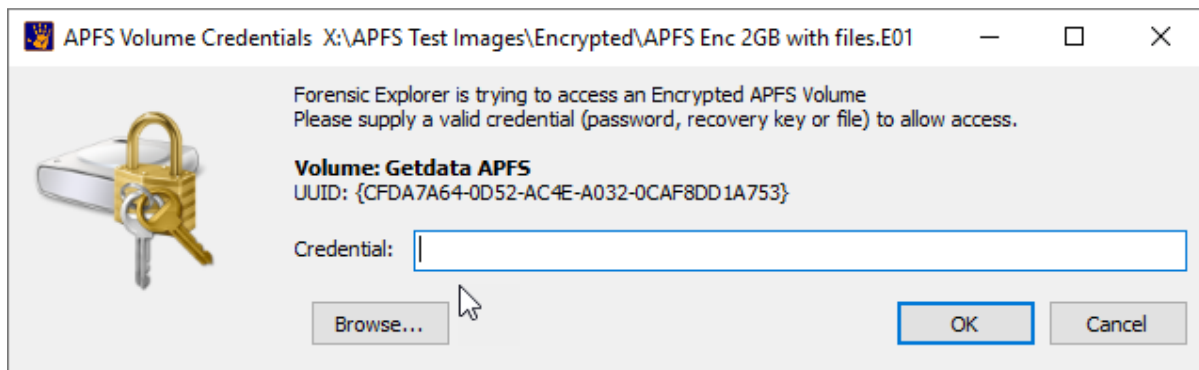
Windows Encrypted files can be easily filtered in Forensic Explorer by adding the **IsEncrypted** column to the **File List** view. IsEncrypted is a Boolean field of Yes or No.

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 APPLE AFPS ENCRYPTION

Support has been added for MAC APFS encryption. A prompt will show for credentials when an image is added.

APFS encryption prompt on add image:



20.1.3 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:

BitLocker frequently asked questions (FAQ) (<https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-frequently-asked-questions>, July 2017).

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 332: 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.

20.1.4 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

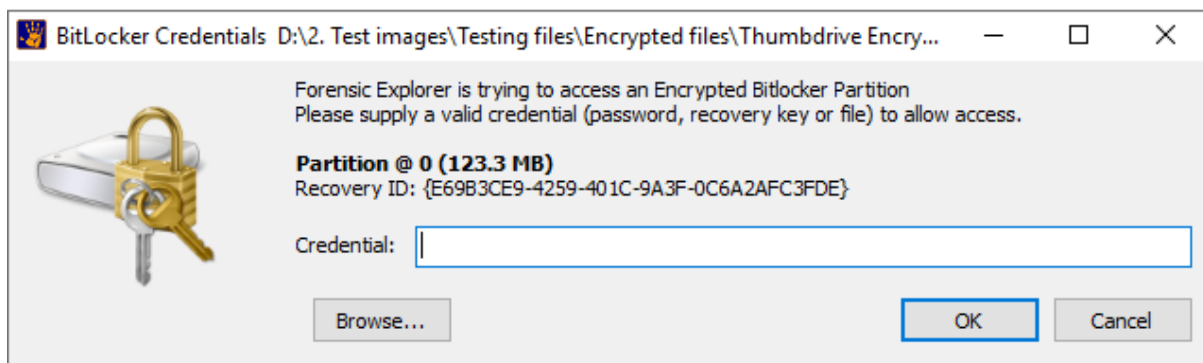
To decrypt BitLocker and File Vault 2 drives:

DECRYPTION WHEN ADDING EVIDENCE

IMPORTANT: BitLocker decryption requires the **forensic workstation to be running Windows 10** (or above).

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 333: 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 334: Encrypted Partition (closed padlock)

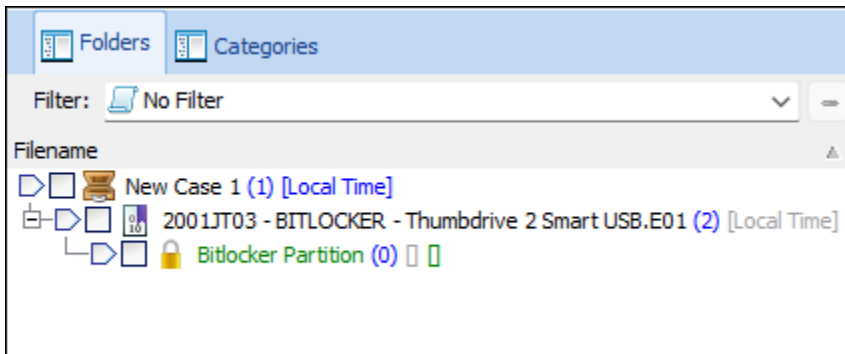
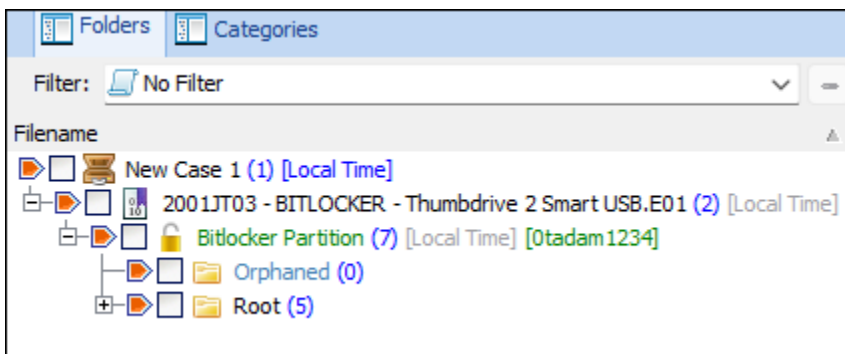


Figure 335: Decrypted Partition (open padlock)

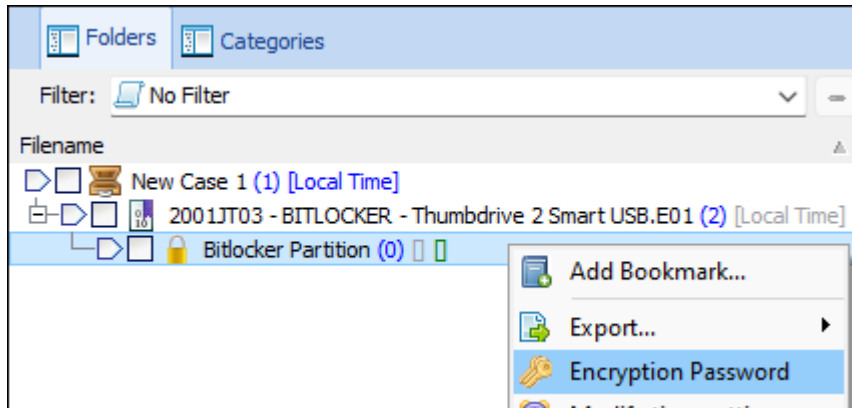


DECRYPTION DURING A CASE

To decrypt a partition during a case:

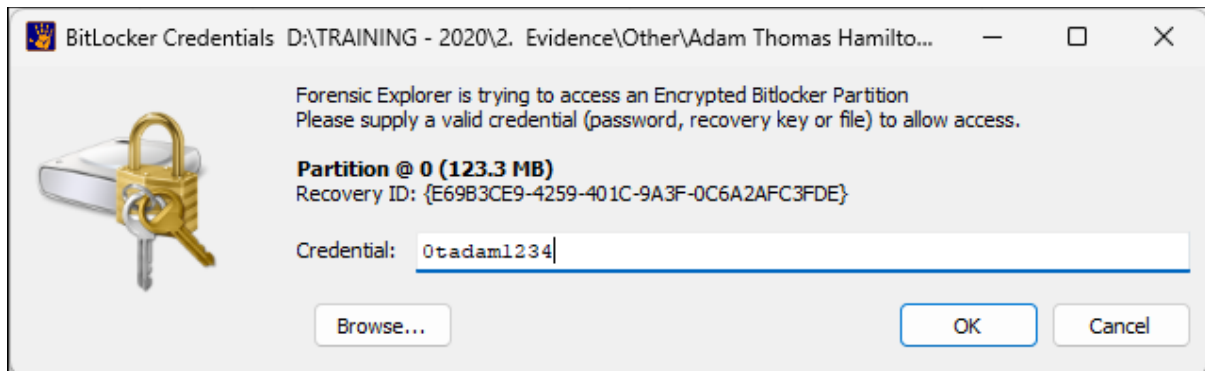
1. Right click on the encrypted partition and select **Encryption Password**, as shown in Figure 336:
Decryption during a case:

Figure 336: Decryption during a case



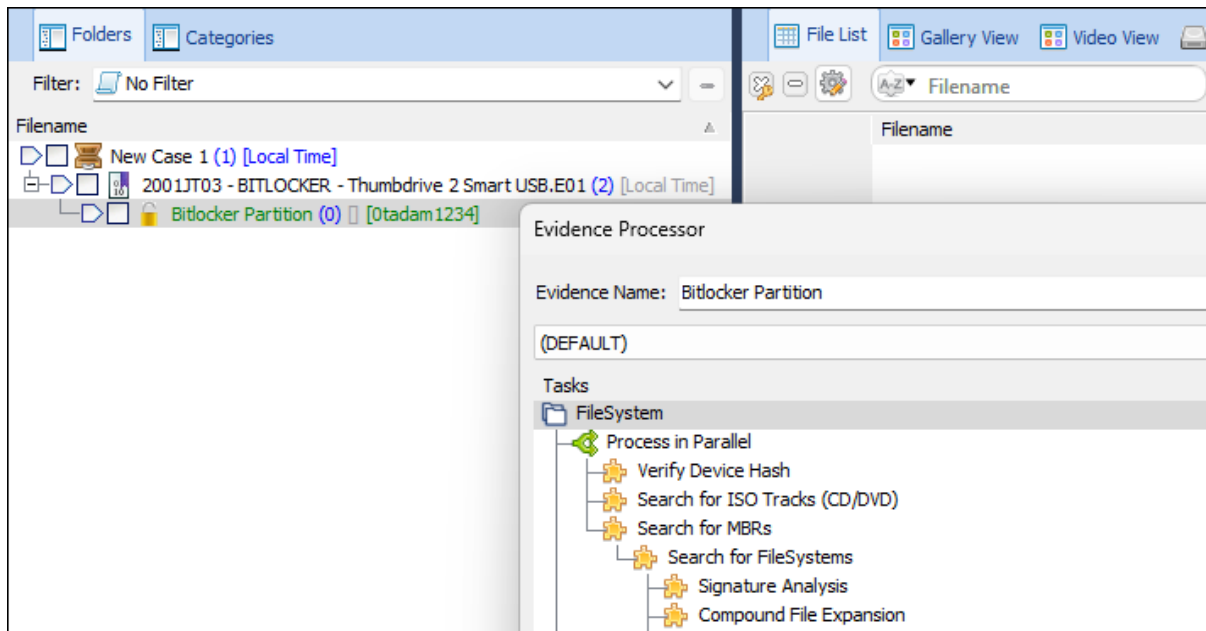
2. Enter the Bitlocker credentials:

Figure 337: Encryption password prompt.



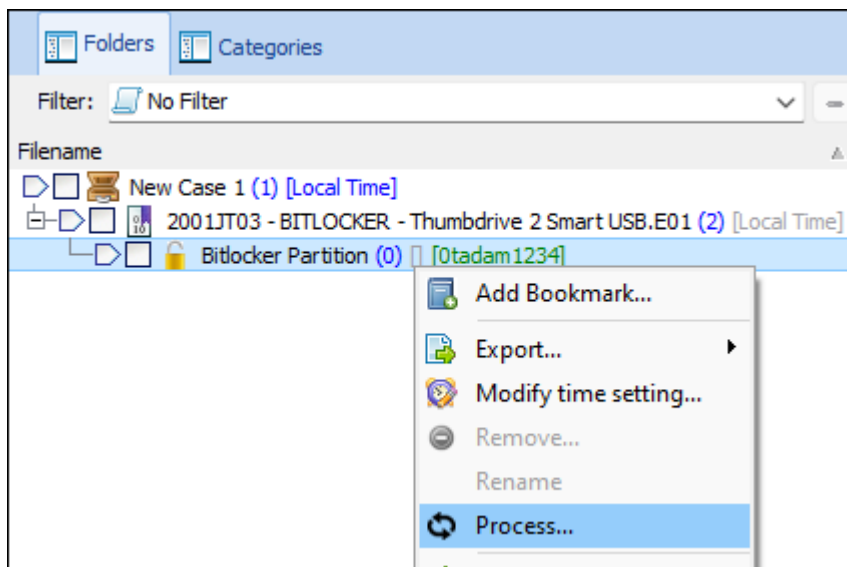
3. If the Bitlocker password has been accepted, the password will appear next to the encrypted partition in the **Folders view** and the **Evidence Processor** window will open:

Figure 338: Process the decrypted Bitlocker partition.



Note that if a Bitlocker partition has been added but not processed (i.e., the **Cancel** option was selected in the **Evidence Processor** window above), it is possible to right-click and **process** the partition during the case:

Figure 339: Process a decrypted Bitlocker partition during a case.



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 331 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 331 above with the **Microsoft Word Password Protected File.docx**.

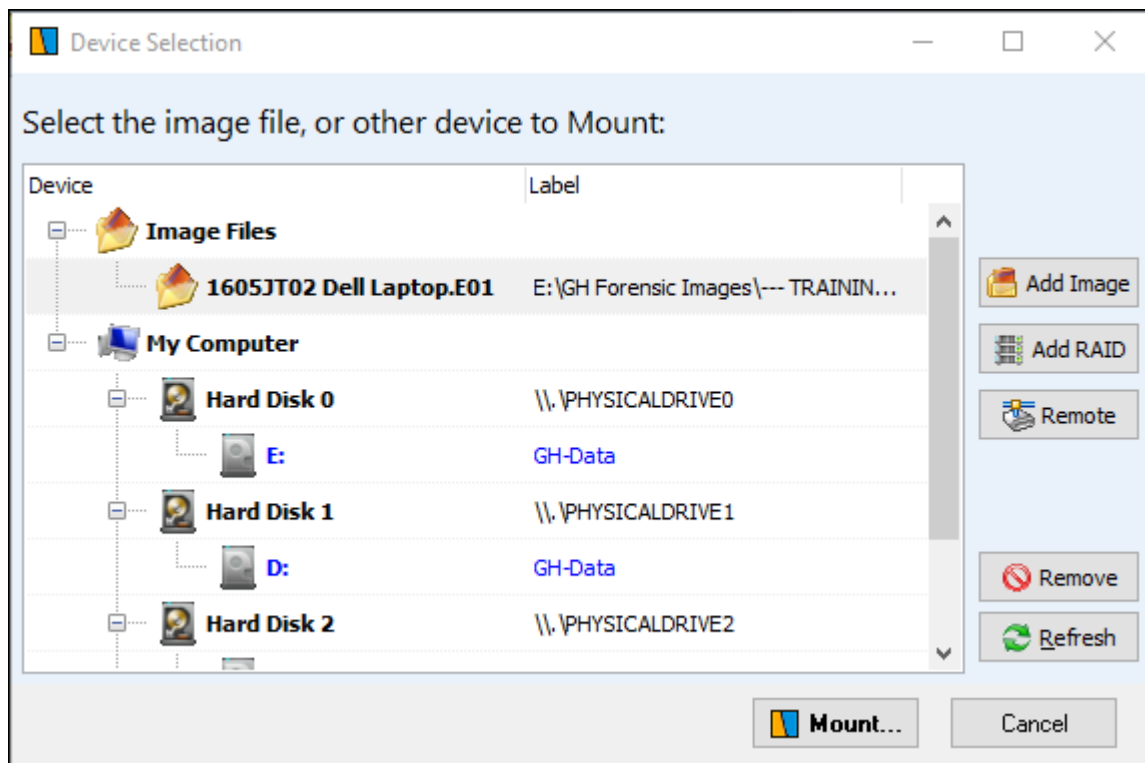
20.3.2 IDENTIFYING ENCRYPTED FILES USING A THIRD-PARTY TOOL

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:

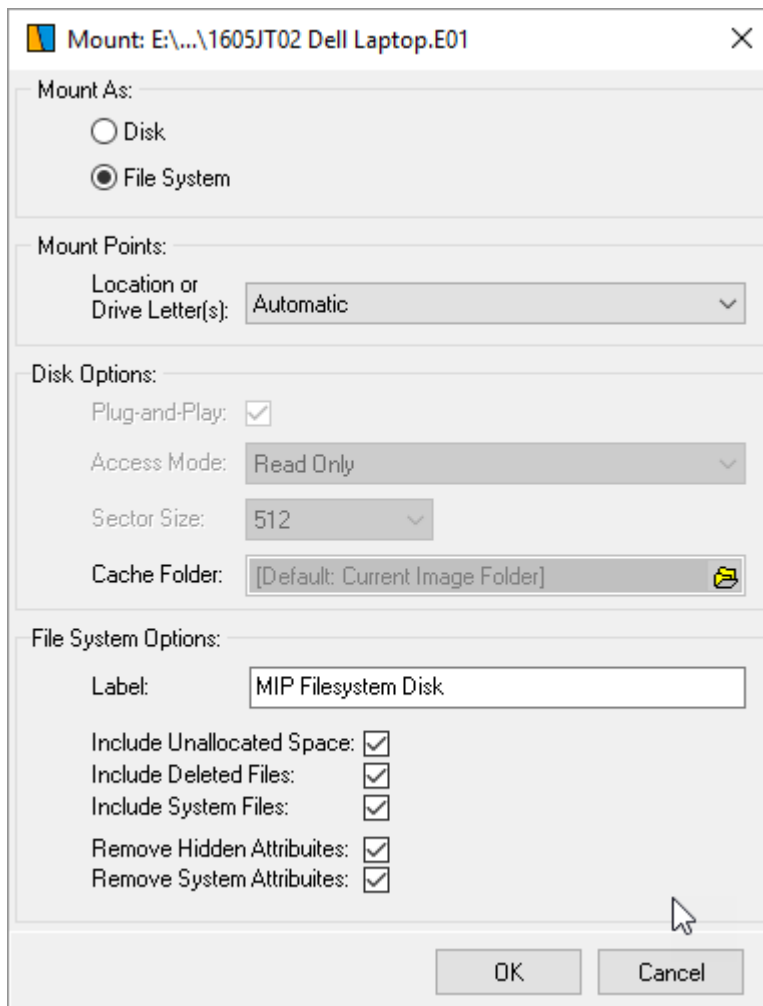
Figure 340: Mount Image Pro Device Selection window



5. Click the **Mount** button.

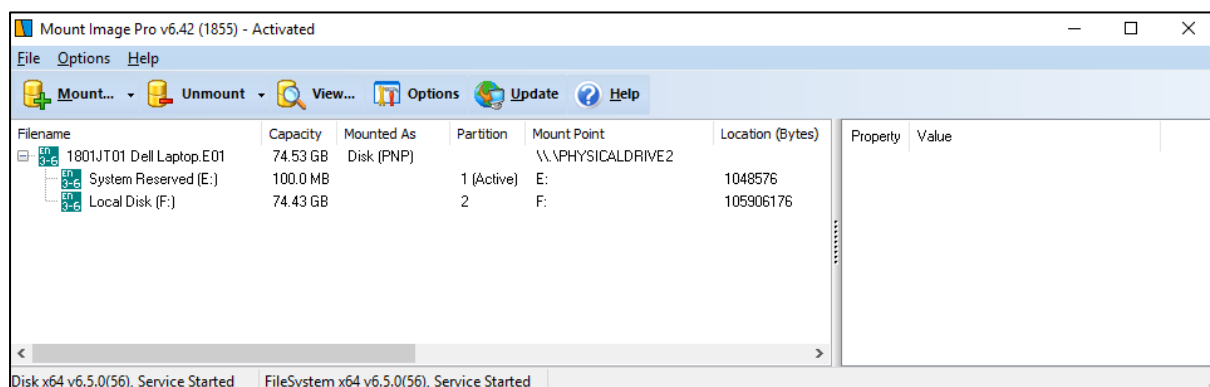
- Mount the image as **File System** with the following settings (File System ensures access to all files, including deleted, system and hidden):

Figure 341: Mount Settings



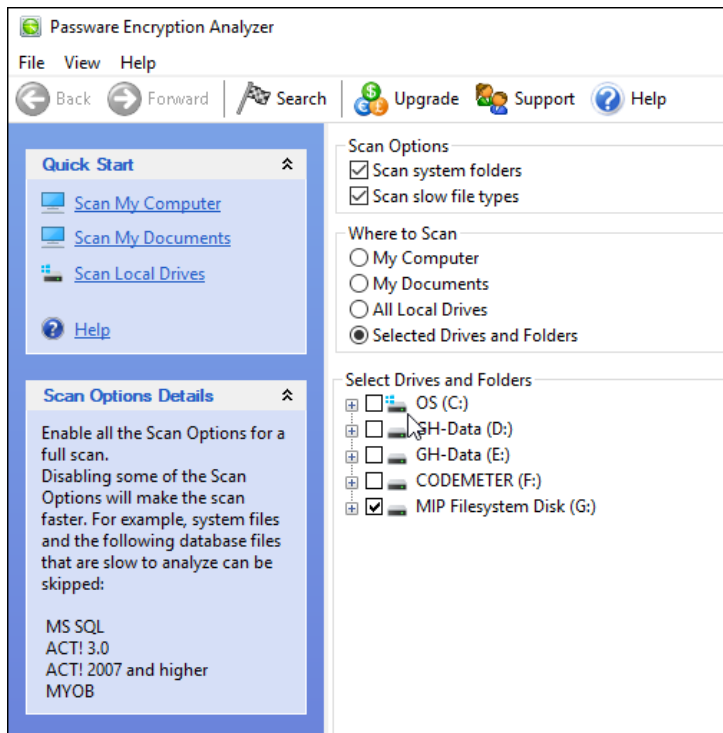
- If additional images are added, it is possible to add to the same drive letter under the **Mount Points** option.
- Click **OK** to mount the drive.

Figure 342: Mount Image Pro GUI showing mounted File System drive



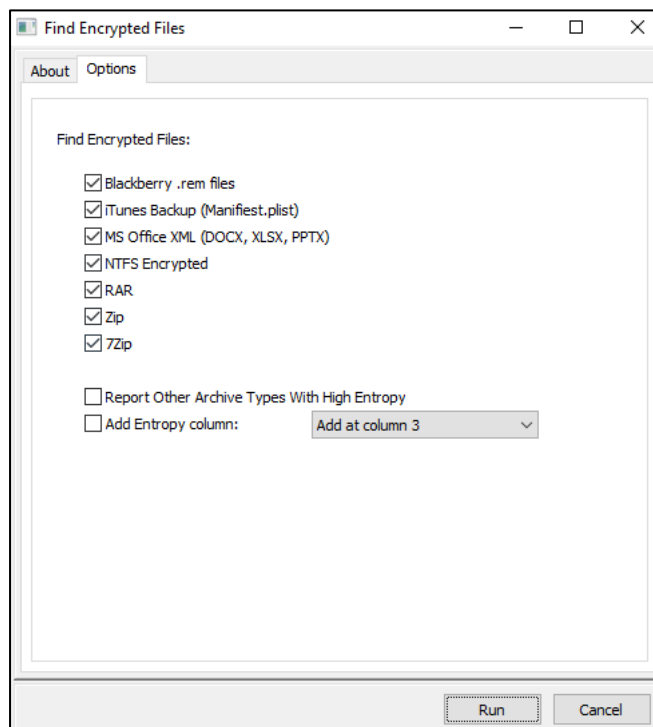
9. Launch Passware Encryption Analyzer and scan the mounted drive:

Figure 343: Passware Encryption Analyzer



20.3.3 ENCRYPTED FILE DETECTION

Encrypted files can now be detected by the File System > Analysis Programs > Encrypted Files script:

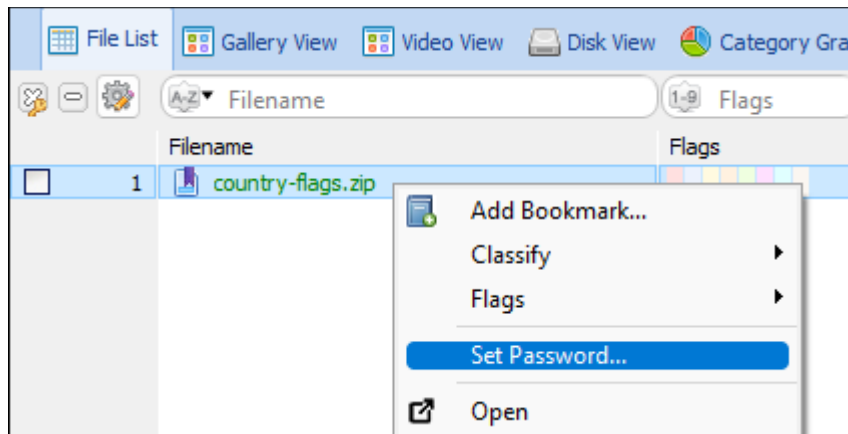


20.4 DECRYPTED PASSWORD PROTECTED ARCHIVES (ZIP, 7Z)

To decrypt a password protected archive file (e.g., ZIP, 7z) in the **File System** module:

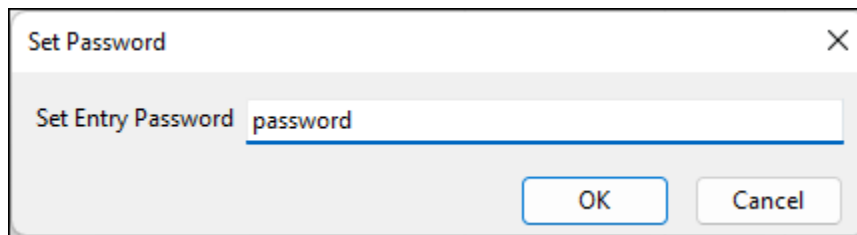
1. Locate the **encrypted file** using the method described above.
2. Right-click on the file and select **Set Password** from the menu:

Figure 344: Setting a password for a file in the File System module



3. **Enter the password** and click **OK**. This password is attached to the file and saved with the case:

Figure 345: Enter file password



4. Right-click and **Expand compound files(s)**. If a password is stored with the file, it will be used in the expand process to decrypt the content.

Chapter 21 – Date and Time

In This Chapter

CHAPTER 21 - DATE AND TIME

21.1	Date and time in computer forensics	336
21.2	FAT, HFS, CDFS file system date and time	336
21.3	NTFS, HFS+ file system date and time	336
21.4	Date and time information in the Windows registry.....	337
21.4.1	Manually examine registry for time zone information.....	337
21.4.2	Extract time zone information	340
21.5	Daylight saving time (DST)	340
21.6	Adjusting Date in Forensic Explorer.....	341
21.6.1	Setting the Time Zone for the Case	341
21.6.2	Setting the Time Zone for individual evidence items	342
21.6.3	Synchronizing time zones	344
21.6.4	What time zone is being applied?	346

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 an 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 8.12 - 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.

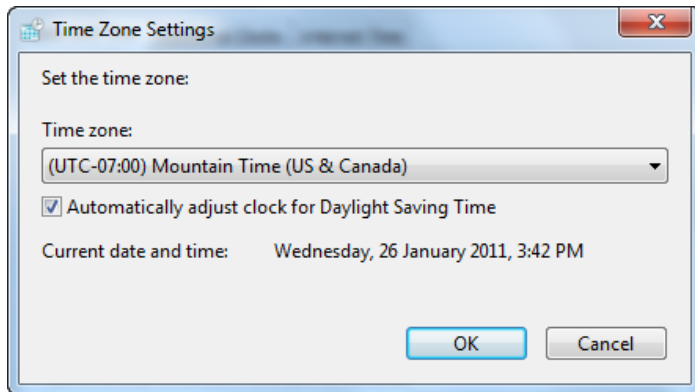
21.3 NTFS, HFS+ FILE SYSTEM DATE AND TIME

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 computer's 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):

Figure 346: Windows 7 time zone settings



For Windows 10, time zone settings can be found in Settings > Time & Language > Date & Time > Time zone drop-down menu.

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, 7 and 10: **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.)

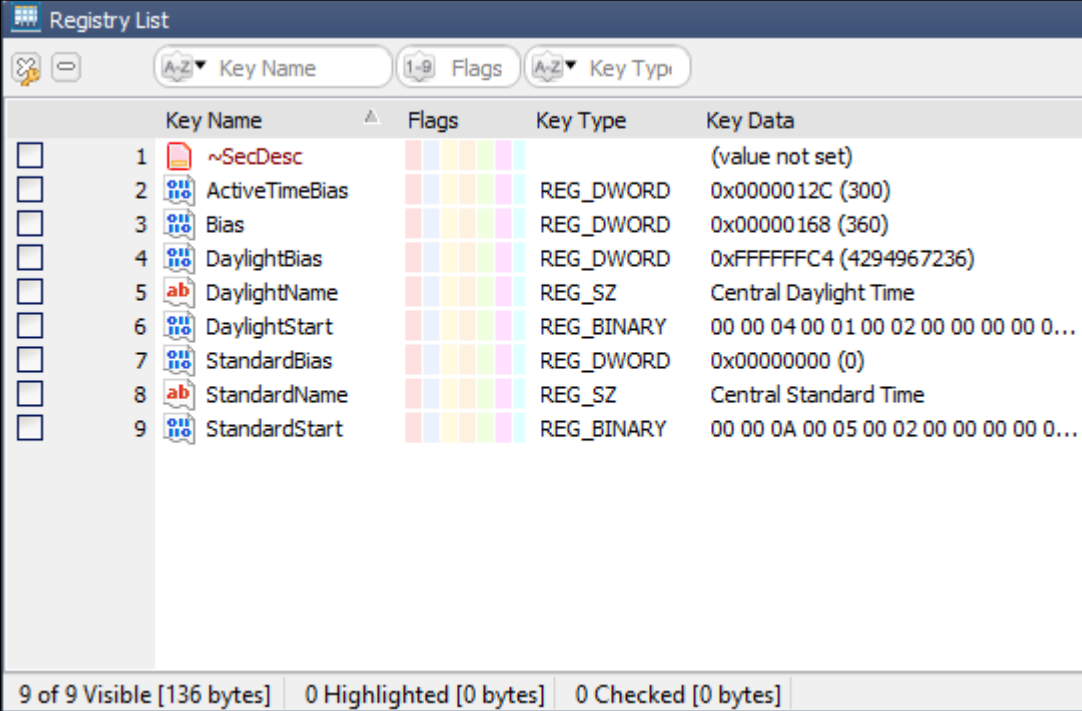
REGISTRY - TIME ZONE INFORMATION

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 347 below:

Figure 347: Windows registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
Image file: NIST Hacking Case (14)



	Key Name	Flags	Key Type	Key Data
<input type="checkbox"/>	1 ~SecDesc			(value not set)
<input type="checkbox"/>	2 ActiveTimeBias		REG_DWORD	0x0000012C (300)
<input type="checkbox"/>	3 Bias		REG_DWORD	0x00000168 (360)
<input type="checkbox"/>	4 DaylightBias		REG_DWORD	0xFFFFF4 (4294967236)
<input type="checkbox"/>	5 DaylightName		REG_SZ	Central Daylight Time
<input type="checkbox"/>	6 DaylightStart		REG_BINARY	00 00 04 00 01 00 02 00 00 00 00 0...
<input type="checkbox"/>	7 StandardBias		REG_DWORD	0x00000000 (0)
<input type="checkbox"/>	8 StandardName		REG_SZ	Central Standard Time
<input type="checkbox"/>	9 StandardStart		REG_BINARY	00 00 0A 00 05 00 02 00 00 00 00 0...

9 of 9 Visible [136 bytes] 0 Highlighted [0 bytes] 0 Checked [0 bytes]

The information in the registry includes:

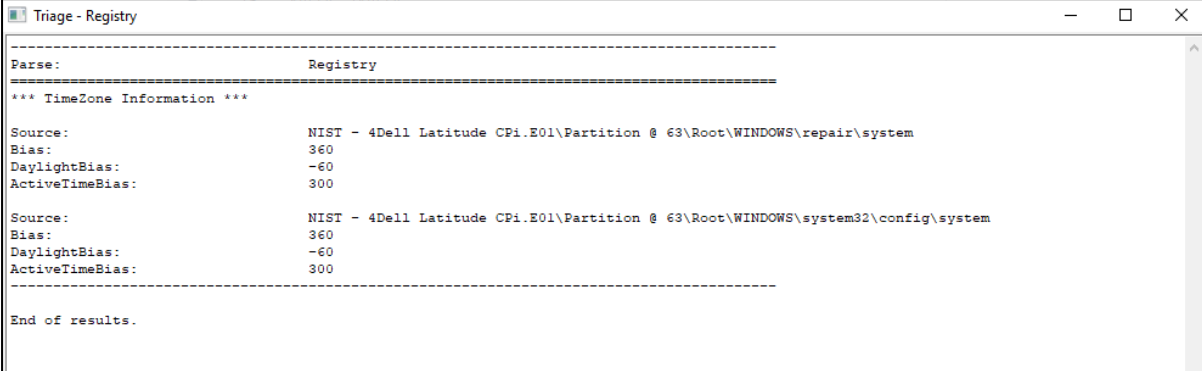
- ActiveTimeBias:** The number of minutes offset from UTC for the current system time.
- Bias:** The number of minutes offset from UTC for the current time zone setting.
- DaylightBias:** The number of minutes offset from UTC for the current time zone when daylight saving is in effect.
- DaylightName:** 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

Registry information, including Windows date and time settings, is also available in Forensic Explorer by using the toolbar shortcut **Quick Registry > Windows TimeZone** located in the File System module.

The Windows TimeZone script decodes the registry keys and provides output in the following format:

Figure 348: NIST Hacking Case (14) output.



```

-----
Parse: Registry
-----
*** TimeZone Information ***
Source: NIST - 4Dell Latitude CPl.E01\Partition @ 63\Root\WINDOWS\repair\system
Bias: 360
DaylightBias: -60
ActiveTimeBias: 300
Source: NIST - 4Dell Latitude CPl.E01\Partition @ 63\Root\WINDOWS\system32\config\system
Bias: 360
DaylightBias: -60
ActiveTimeBias: 300
-----
End of results.

```

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 make 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 an additional four weeks:

United States DST

	Clocks forward 1 hour	Clocks back 1 hour
1986 - 2006	First Sunday of April	Last Sunday of October
2007 onward	Second Sunday of March	First Sunday of November

Microsoft released a patch for the NTFS file system to compensate for the 2007 change (See <https://support.microsoft.com/en-gb/help/932955/how-to-handle-dates-and-times-that-include-dst> 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:

1. **The Entire Case:** Date and time settings are applied to all evidence items within the case.
2. **Individual Evidence Items:** When case time is **Not Set**, evidence items can be individually set.

21.6.1 SETTING THE TIME ZONE FOR THE CASE

IMPORTANT: A **case time setting** has **precedence** over **evidence time settings**. If case time is set all settings will be disabled (i.e. greyed out).

Case time zone settings are applied when the case is created in the Evidence module, as shown in Figure 349 below:

Figure 349: Setting a Case Time Zone (Local Time shown)

The screenshot shows the 'New Case' dialog box with the following details:

- Case Name:** NIST Hacking Case
- Investigator:** Graham Henley (with 'New...' and 'Edit...' buttons)
- Cases Folder:** C:\Users\Owner\Documents\Forensic Explorer\Cases
- Case Summary:** (Empty text area)
- Case Time Zone Settings (Expanded):**
 - 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:** 15-Dec-15 8:32:16 PM

Buttons for 'OK' and 'Cancel' are visible at the bottom right.

TO CHANGE CASE TIME ZONE SETTINGS DURING A CASE

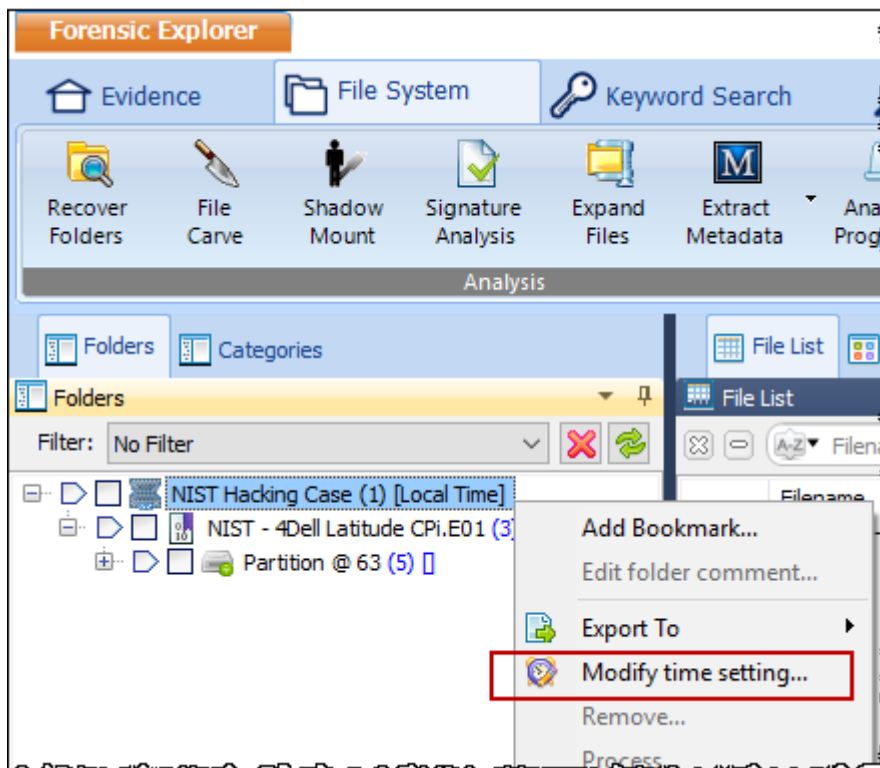
To **change case time zone settings** during a case:

1. In the File System module, right click on the case folder.

- From the drop-down menu select the **Modify time settings** option.

As shown in Figure 350 below:

Figure 350: Adjusting Case Time Zone Settings



21.6.2 SETTING THE TIME ZONE FOR INDIVIDUAL EVIDENCE ITEMS

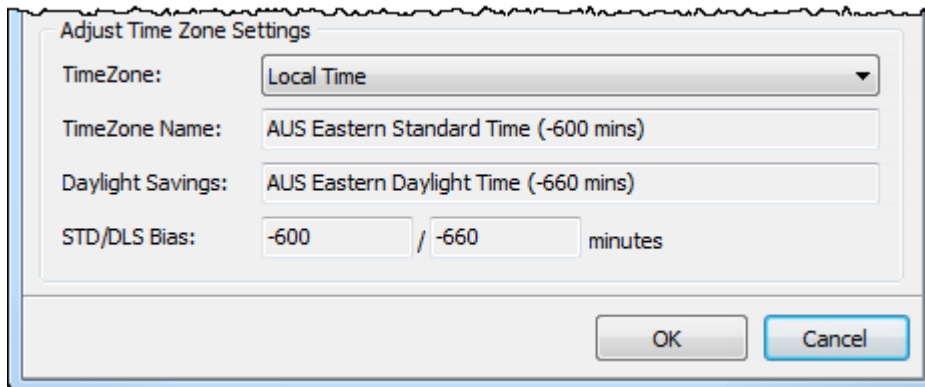
When examining NTFS or HFS+ file system, to view date and times zones per the location of the subject computer, it is necessary to set date and time settings to that location (given that time settings were confirmed to be accurate at the time of acquisition).

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 are 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 351 below:

Figure 351: Adjust time zone information when adding evidence.



IMPORTANT: A **case time setting** has precedence over **evidence time settings** so the case time setting must be **Not Set** 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:

Figure 352: Adjust time zone settings for an evidence item.

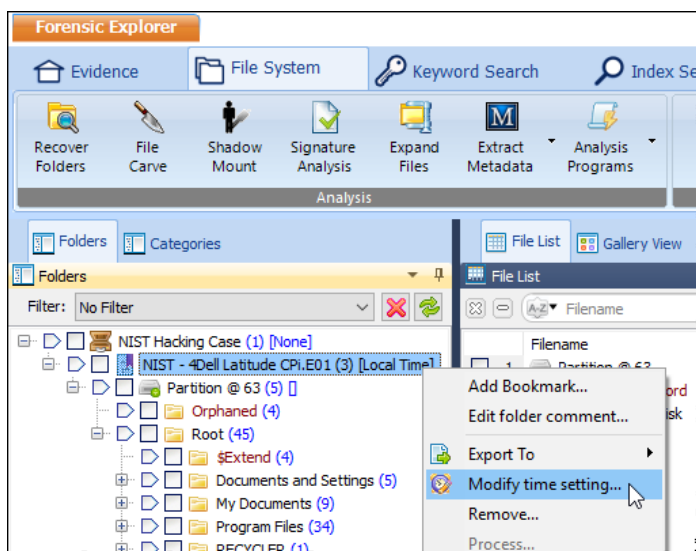
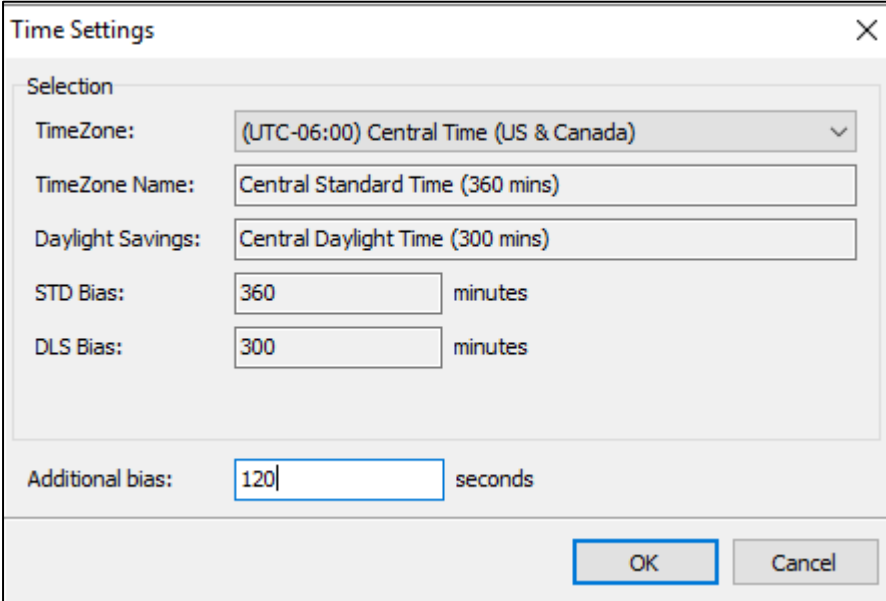
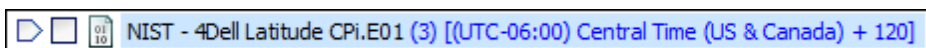


Figure 353: Time settings



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 354 below:

Figure 354: adjusted time zone information



4. Date and time information in the File System > File List will now be adjusted (Note: It may be necessary to refresh the File List display to show this adjustment).

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 **Not Set**.
- 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:

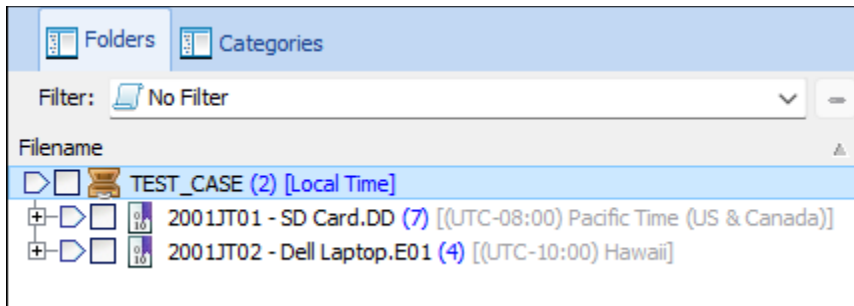
- The New York computer has a file creation time of 11AM.
- The Los Angeles computer has a file creation time of 11AM.

21.6.4 WHAT TIME ZONE IS BEING APPLIED?

In Forensic Explorer v5.4.8.2930 and above, the time-zone/s currently being applied is identified by the **blue highlight color**. In the example below:

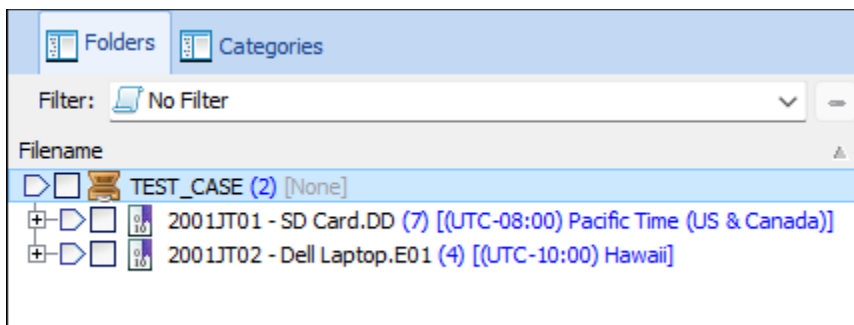
1. **Case [Local Time]** is applied to all evidence items in the case (note that time-zones for individual evidence items are greyed out):

Figure 355: Case time settings are applied to all (shown in blue)



2. When case time is set to **[Not Set]** (greyed out), individual evidence items settings are applied (i.e., **Pacific Time (US & Canada)** and **Hawaii**, as identified by the blue highlight color):

Figure 356: Individual evidence time settings are applied (shown in blue)



Chapter 22 - Hash Sets

In This Chapter

CHAPTER 22 - HASHING

22.1	Hash Values	348
22.2	Hash Algorithms.....	348
22.3	Acquisition Hash	348
22.4	Verification Hash.....	348
22.5	Hashing files in a case	351

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 3.40282×10^{38} ”. (EnCase Forensic Version 6.10 User Manual. s.l. : Guidance Software, 2008 (15 p. 12)).

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

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

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

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 359: Acquisition and Verification hashes.

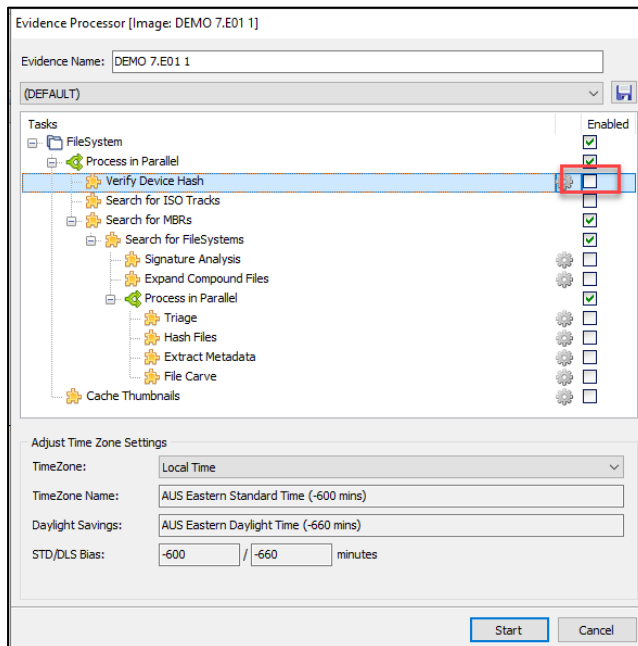
22.4 VERIFICATION HASH

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:

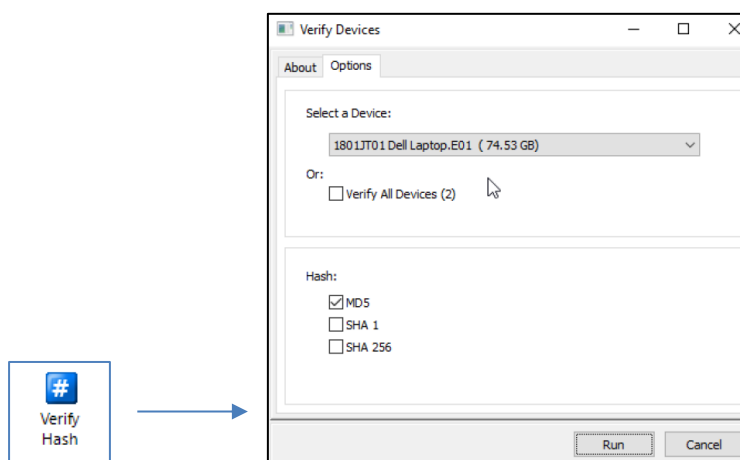
1. Calculate the verification hash **when adding evidence to the case**:
 - a. In the **Evidence Module**, start a case or preview or open an existing case.
 - b. Click the **Add Device, Add Image** or **Add File** button to add evidence to the case.
 - c. In the Evidence Processor window, place a check in the “Verify Device Hash” box and select the hash you would like to process. Click **OK > Start** to proceed with the evidence processing.

Figure 357: Evidence Processor



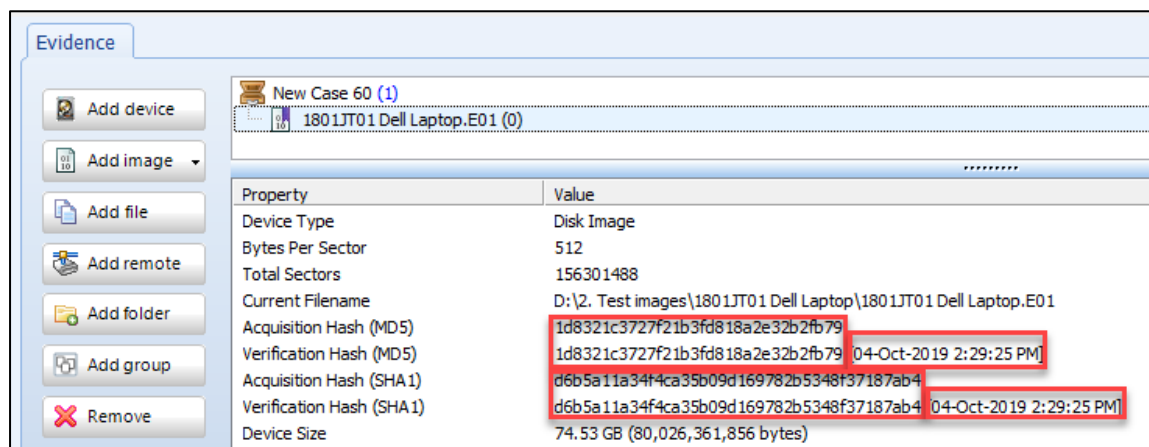
2. Calculate the verification hash during a case:
 - a. In the Evidence module, run the **Verify Device Hash** script accessed from the **Verify Hash** toolbar button which allows for multiple image verification in a single pass:

Figure 358: Verify device hash from the Evidence module toolbar.



The verification hash is written to the evidence module with the acquisition hash and is possible to know the last date and time the image was verified, as shown below:

Figure 359: Acquisition and Verification hashes, last validation date/time



Property	Value
Device Type	Disk Image
Bytes Per Sector	512
Total Sectors	156301488
Current Filename	D:\2. Test images\1801JT01 Dell Laptop\1801JT01 Dell Laptop.E01
Acquisition Hash (MD5)	1d8321c3727f21b3fd818a2e32b2fb79
Verification Hash (MD5)	1d8321c3727f21b3fd818a2e32b2fb79 [04-Oct-2019 2:29:25 PM]
Acquisition Hash (SHA1)	d6b5a11a34f4ca35b09d169782b5348f37187ab4
Verification Hash (SHA1)	d6b5a11a34f4ca35b09d169782b5348f37187ab4 [04-Oct-2019 2:29:25 PM]
Device Size	74.53 GB (80,026,361,856 bytes)

Verification of Logical Image Files (.L01, .LX01, .AD1)

A **logical** forensic image is a collection of individual files written to a logical forensic container such as a .L01 or .LX01 (EnCase format by Guidance Software) or .AD1 (FTK format by Access Data).

When a logical image is created, individual file hashes can be created on acquisition. This means that at a future time, individual file hashes can be recalculated and compared their acquisition hash to determine that file data is unchanged.

Forensic Explorer will calculate an overall verification hash for the entire logical evidence file and display this value in the Evidence module. However, this calculation is unique to Forensic Explorer. If the logical image is provided to a third party, **Forensic Explorer must be used to recalculate the verification hash.**

To provide a simple mechanism whereby a logical image file can be verified by a third party who does not have access to Forensic Explorer, a hash of the logical image segments can be used.

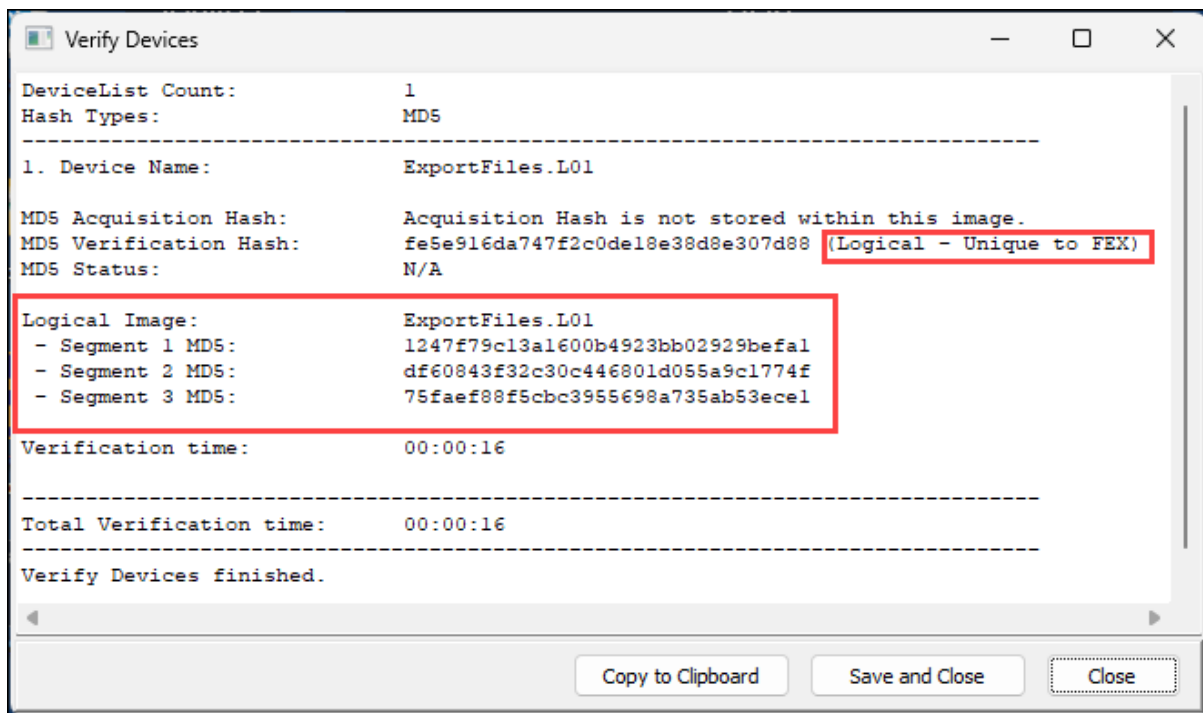
In the example shown in Figure 361 below, a logical image file called **ExportFiles.L01** has been created. The image is made up of three segments, ExportFiles.L01, ExportFiles.L02, ExportFiles.L03. When verified in Forensic Explorer using the Evidence module **Verify Hash** button:

Figure 360: Evidence module, Verify Hash



a MD5, SHA1, or SHA256 hash value will be created for each image segment. Any third-party hashing tool can be used to verify the hash of the image files.

Figure 361: Hash of logical image segments.

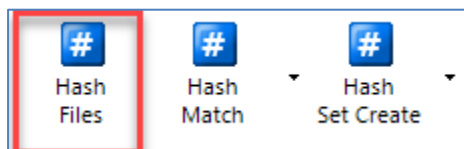


22.5 HASHING FILES IN A CASE

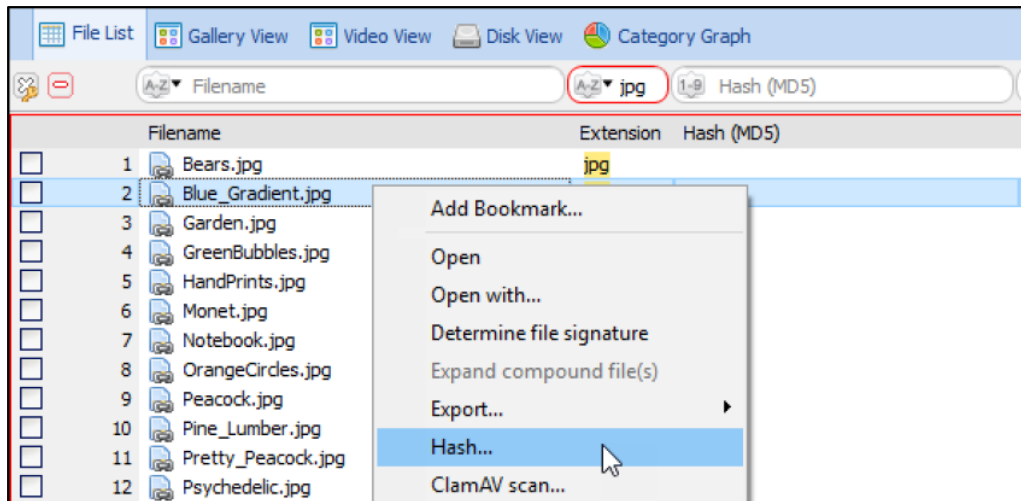
To calculate hash values for individual files in a case:

1. In the **File System module**, click the required Hash button:

Figure 362: File System module Hash Files button

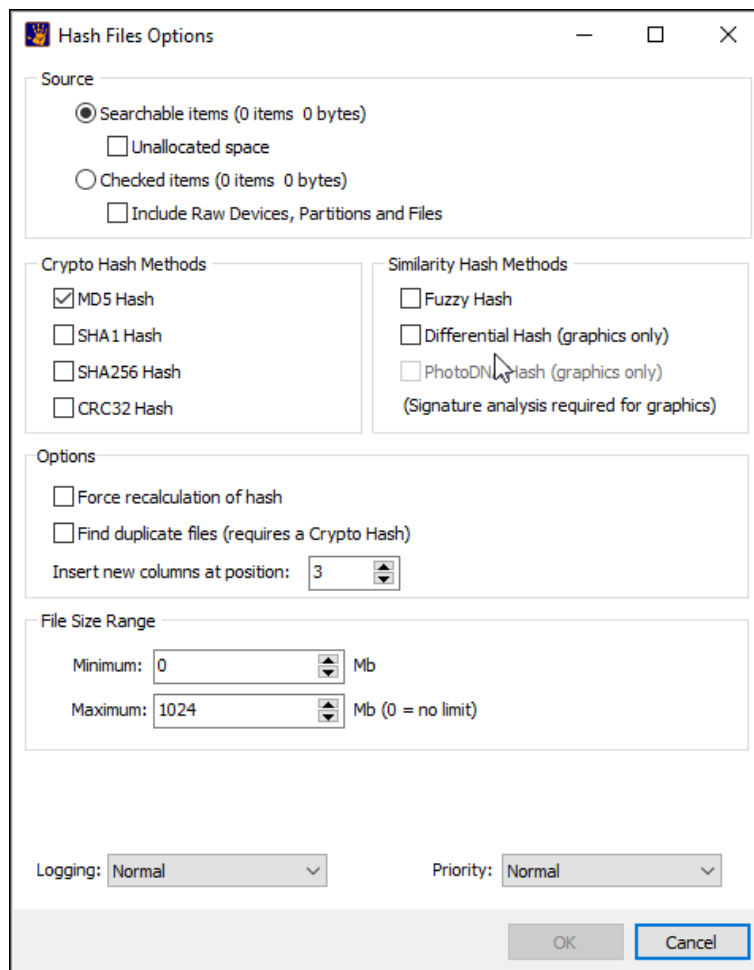


Or alternatively, right click on a file in the File List and select "Hash..." from the drop-down menu.



2. This opens the Hash Files Options window:

Figure 363: 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 is pressed in the Email module, a hash is calculated for the messages and attachments in that module.

The hash can be calculated on all searchable items or checked items. **Include Raw Devices and Partitions** will additionally search those items as stand-alone files (Warning: This will increase the time required).

Hash Methods: Select the type/s of hash to be used.

Force Recalculation: When checked, all hashes will be recalculated. (When unchecked a hash will be calculated for only those items that do not have a hash.)

Duplicates: See below.

File Size Range: Ignore files that do not fall within the range (0,0 = hash all files).

Logging & Priority: See 7.5 – Logging and Priority.

The results of a file hash are written in the Hash column of the File System module.

If the Hash column is not visible, learn how to add columns to the File System module in chapter 9.4 - Columns.

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 **CRC32, 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>) 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:

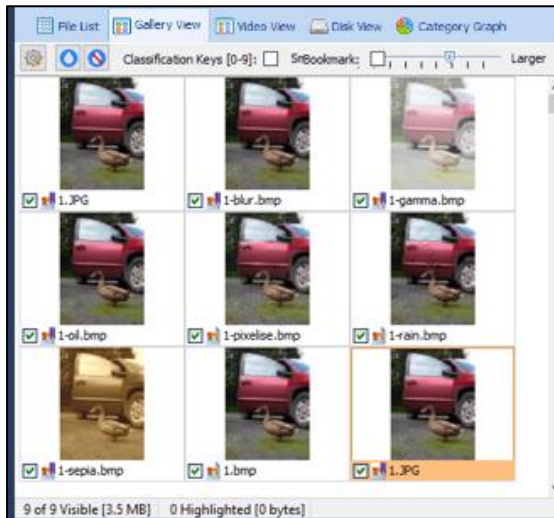
<http://www.hackerfactor.com/blog/?/archives/432-Looks-Like-It.html>

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.

Figure 364: Example of locating similar graphics using differential hash.



To locate graphics visually like 1.JPG.

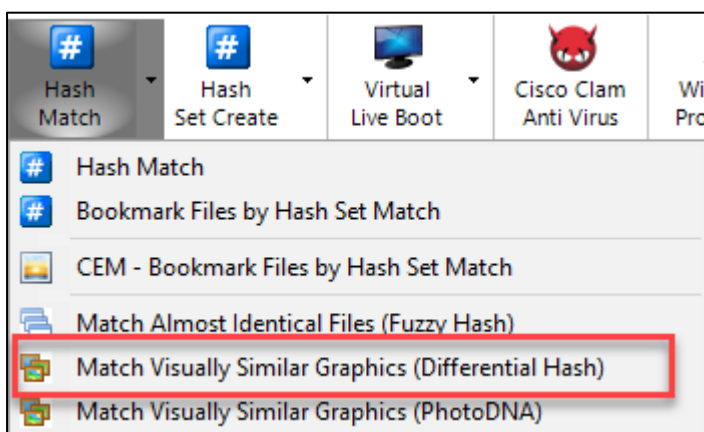
1. Differential Hash the files

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)

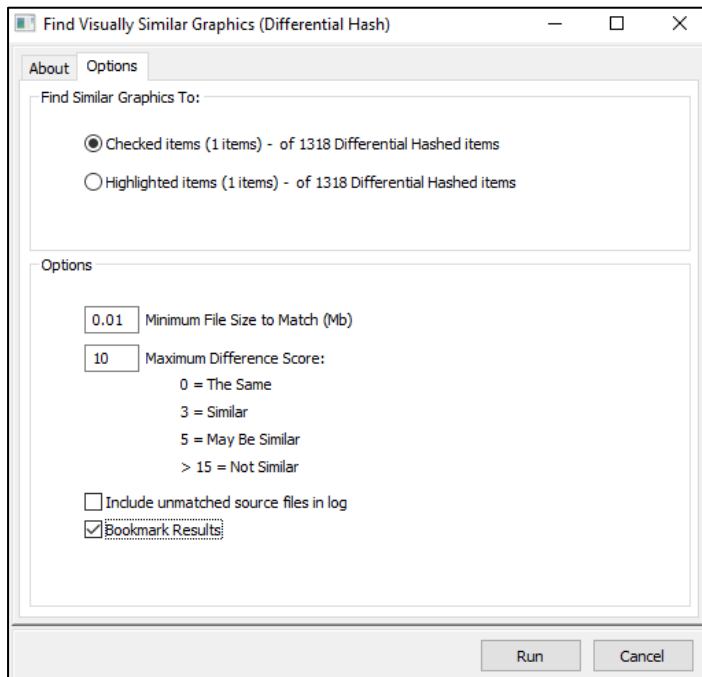
A comparison between differential hashes is determined by calculating the **Hamming Distance** (see: https://en.wikipedia.org/wiki/Hamming_distance). In the File System module click the **Hash Match** button drop-down menu and select **Match Visually Similar Graphics (Differential Hash)**:

Figure 365: Hash Match drop-down menu



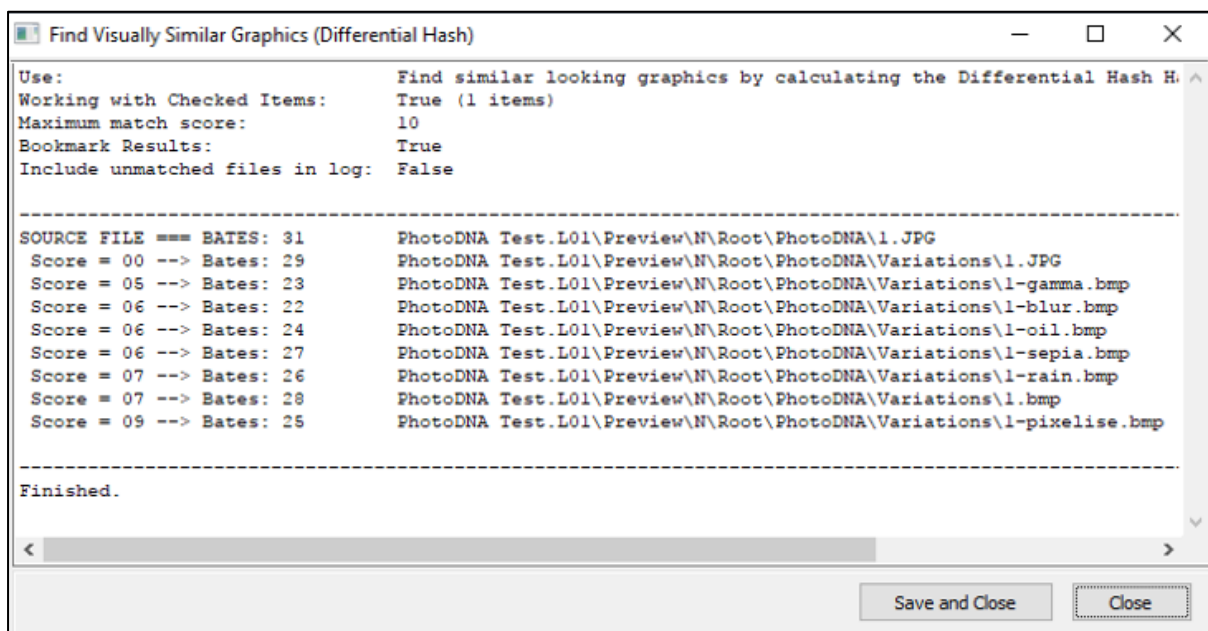
3. The following option window will open:

Figure 366: Find Similar Graphics (Differential Hash)



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:

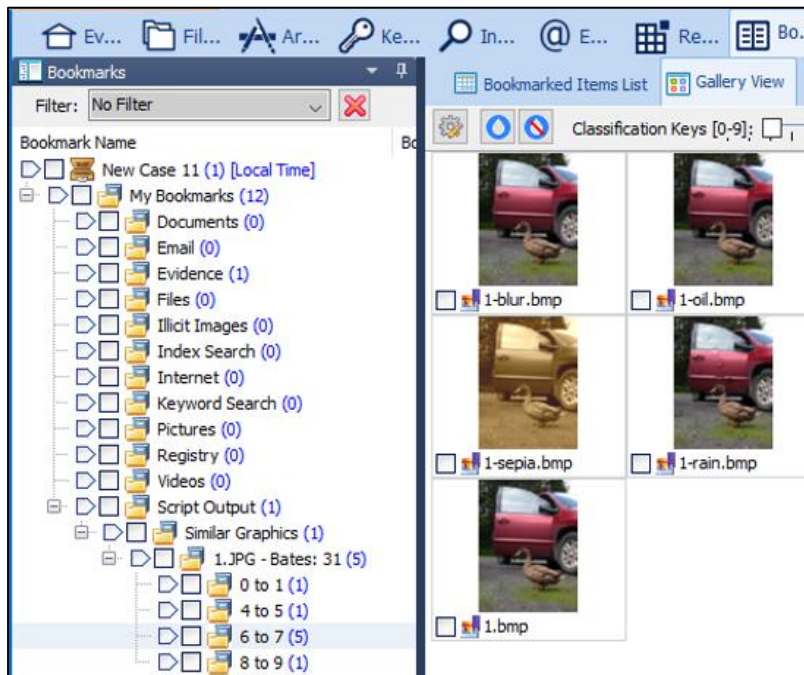
Figure 367: Results of Find Similar Graphics (Differential Hash)



We can see that each of the 8 files like 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 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 368:

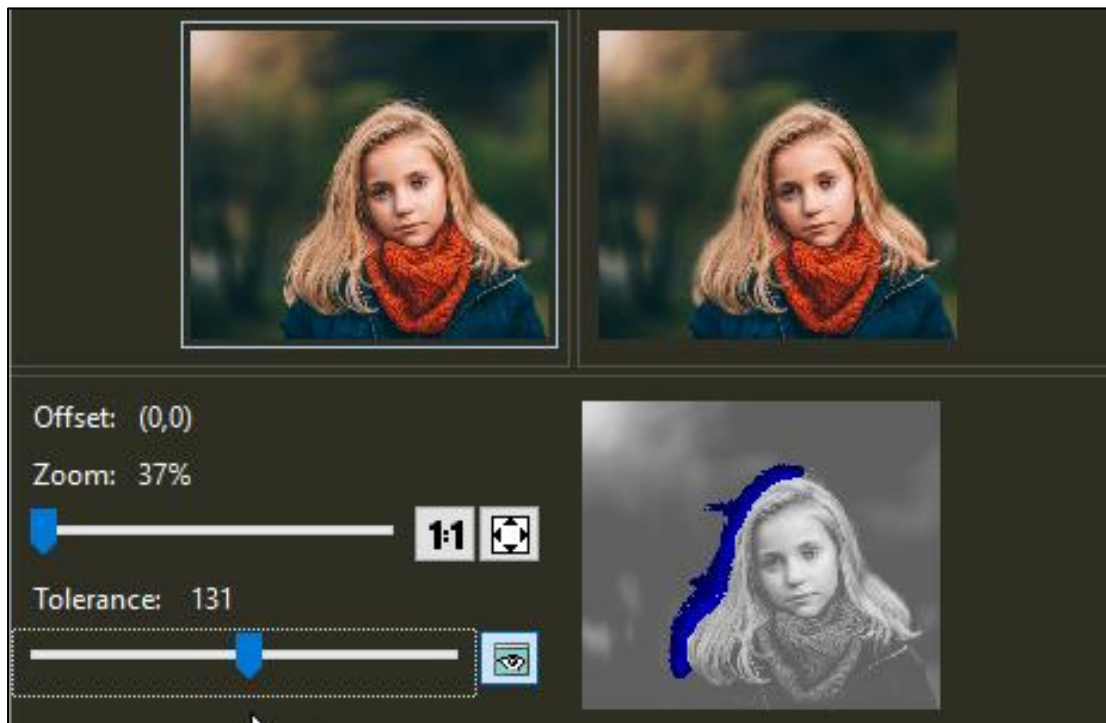
Figure 368: Bookmark results of Find Similar Graphics (Differential Hash)



Example 2

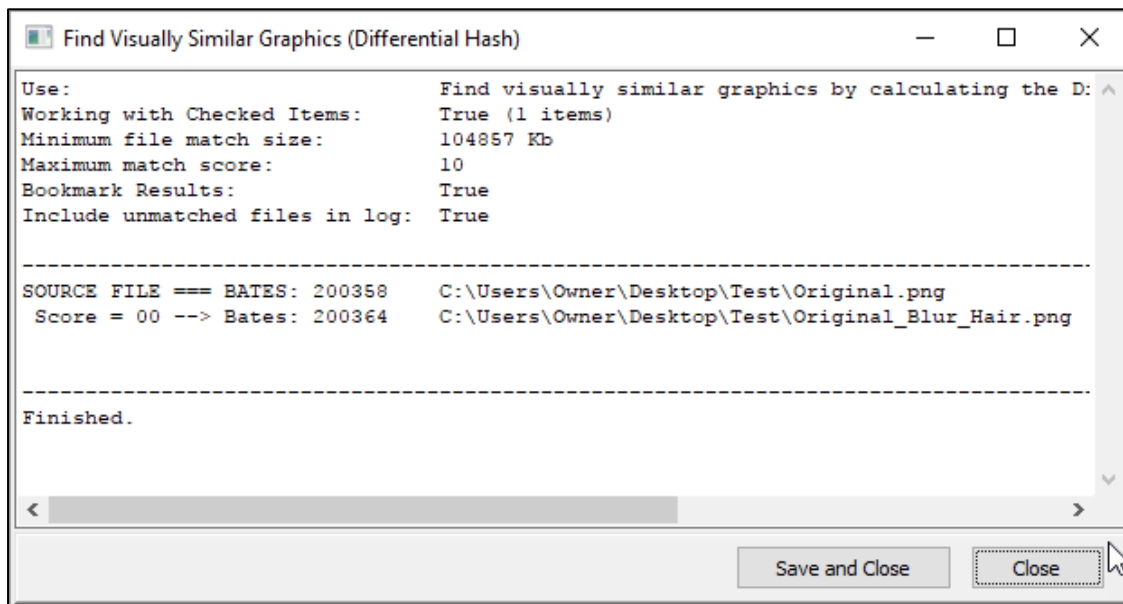
The following digital photo is retouched to blue the outline of the hair:

Figure 369: 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 370: 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 371: 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 372: FEX search results

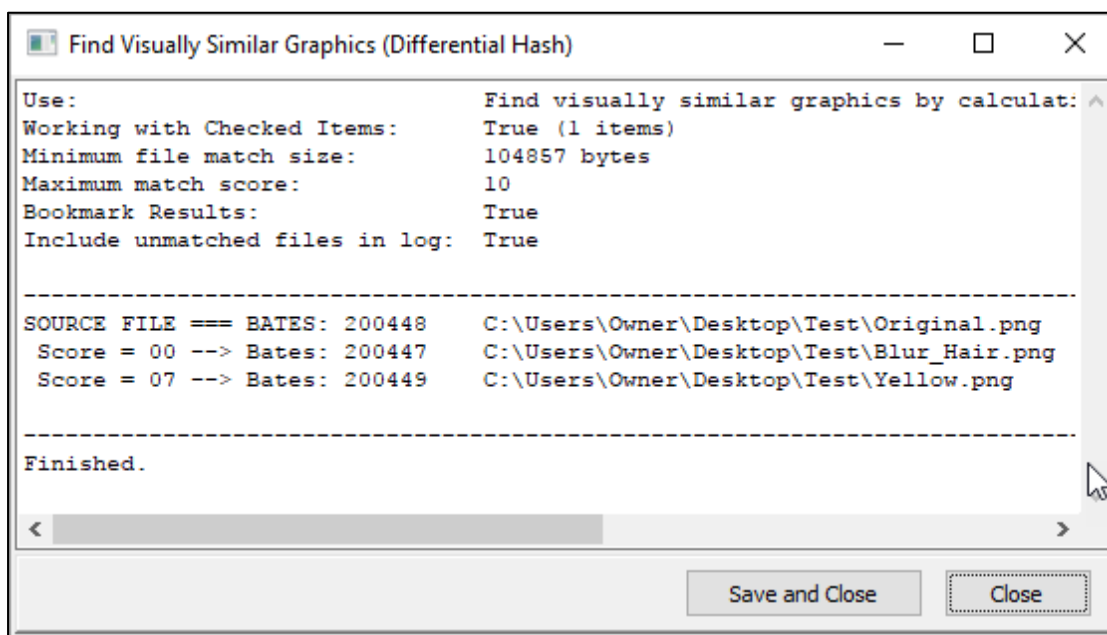


PHOTO DNA

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).

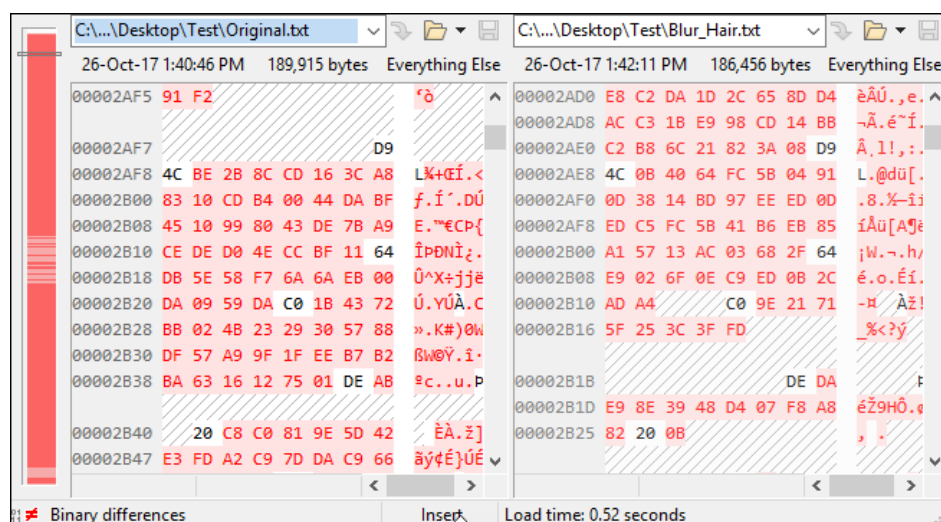
GetData Forensics is licensed to distribute Photo DNA to law enforcement agencies solely for the purpose of preventing the spread, or investigation targeted to stop the distribution and possession, of child sexual abuse content. Photo DNA files are not shipped with Forensic Explorer, which is why this 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 369 above produces two files with almost entirely different content (shown as red below):

Figure 373: Binary comparison of Original.png and Blur_Hair.png shown in Figure 369 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 363 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 Duplicates Index and **Duplicates Count** is created in the **File System > File List** view (to learn how to add this column to the File System > File List, see 9.4).

The **Duplicate Count** column has the following meaning:

- A count of 2 means that two files with identical MD5 hashes have been located (one of which is that file). A count of 3 means that three files with identical MD5 hashes have been located (one of which is that file). Etc.

IMPORTANT CONSIDERATIONS:

- Duplicates are matched by MD5 hash value. **To identify all duplicates a MD5 hash of all files must have been run.**
- Be aware of adding new files to the File System module from a process like a file carve, recover folders, or expand compound files. These new files will need to be hashed.

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 four files with the same MD5 hash. The **Duplicate Count** column shows 4. The **Duplicate Index** column assigns 1, 2, 3 and 4 to each file.

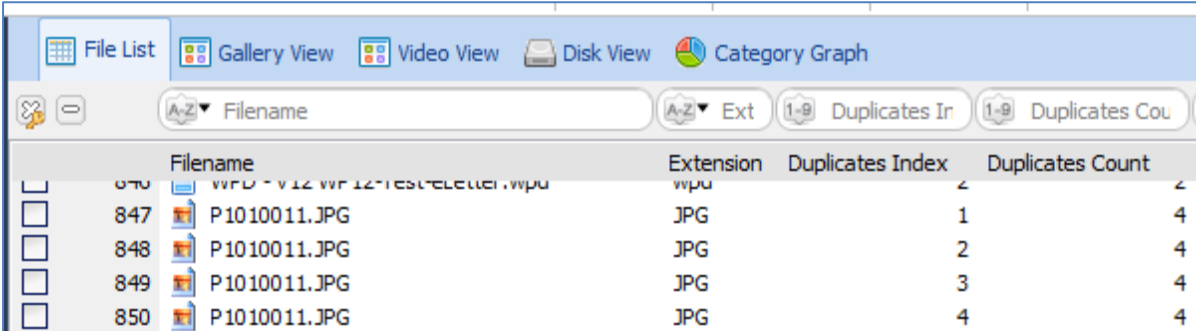
IMPORTANT: The Duplicate Count number is assigned per the sequence of the files as they were processed. The number is NOT an indication that one file has any greater relevance than the next.

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 374: Identifying duplicate count and duplicate index.



Filename	Extension	Duplicates Index	Duplicates Count
847 P1010011.JPG	JPG	1	4
848 P1010011.JPG	JPG	2	4
849 P1010011.JPG	JPG	3	4
850 P1010011.JPG	JPG	4	4

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 listed at <https://getdataforensics.com/hash-sets/> and are available for download by contacting support@getdata.com. Hash sets from other trusted locations can also be used.

22.8 CREATING HASH SETS

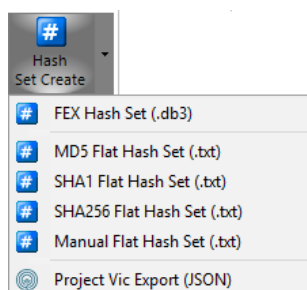
Before creating a custom hash set, files in a case must be hashed. Follow the instructions in 22.5 above.

22.8.1 FORENSIC EXPLORER HASH SET

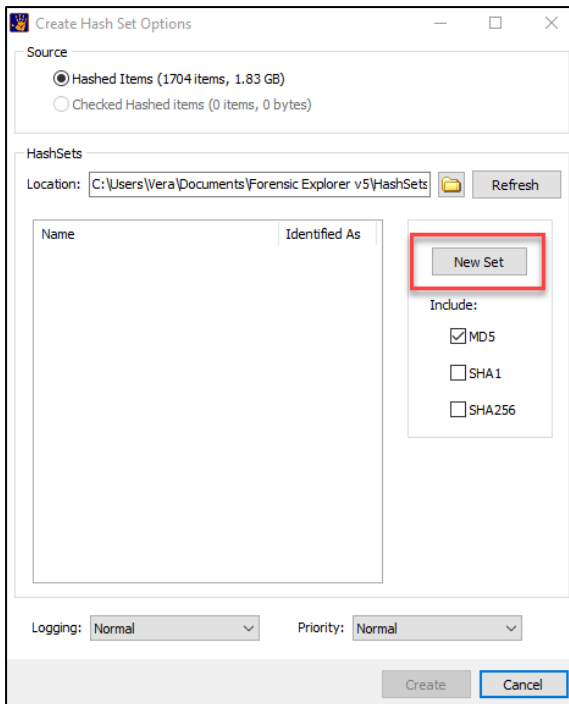
To create a new **Forensic Explorer Hash Set**:

1. Click the “Hash Set Create” button in the File System module toolbar and select **FEX Hash Set**:

Figure 375: Create Hash Set



The following window will display:



2. Click the **New Set** button. Check the type of hash/s to be used in the set (MD5, SHA1, and SHA256). A new hash set will be added to the list.
3. Rename the new hash set and right click to rename the “Identified As” text. Click Save to save the Hash Set. The new hash 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 to give meaning to Forensic Explorer column data:

Figure 376: Flat Hash Set format

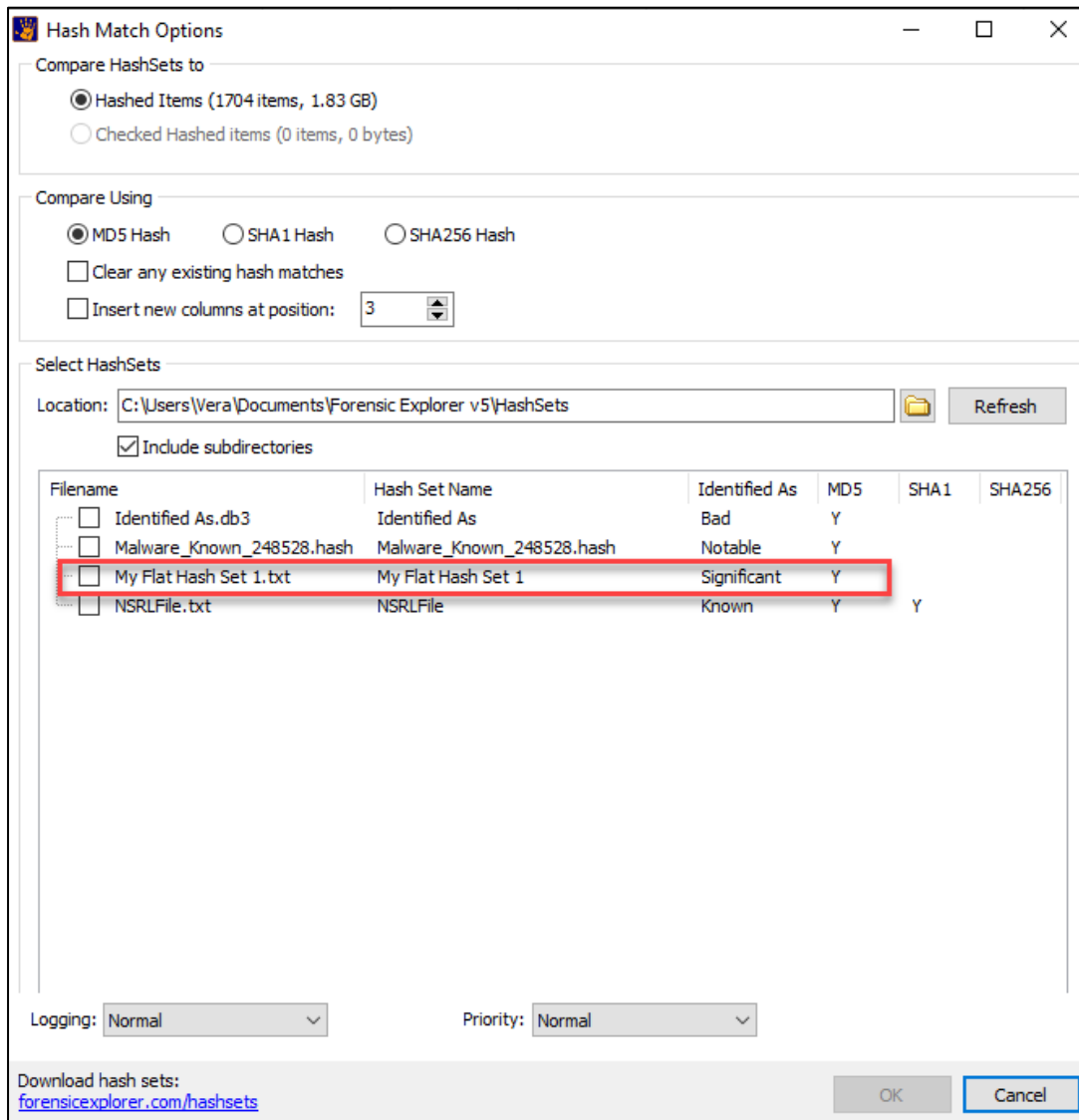
# This is a Flat MD5 Hash Set file	This is a comment
# Hash Set Name = My MD5 List 1	'HashSet' column text
# Identified As = Significant	'HashSet Identified As' column text
83e05311eab2c2d50c2bc6fa219e6905	The list of hash values
a526a95fc34e049360755d9f0450d662	
b8bca7ac76f0ade815c5c743866293e0	
	A blank line = end.

TO MANUALLY CREATE AND USE A FLAT HASH SET

To **manually add** the **Flat Hash Set** file to Forensic Explorer:

1. Place the correctly formatted Flat Hash Set in the Forensic Explorer hash set folder:
[profile]\Documents\Forensic Explorer\HashSets.
2. Click on the **Hash Match** button in the File System module toolbar to open the **Match Hash Files Options** window.
3. The Flat Hash Set should appear in the list of available sets, as shown in Figure 377 below.

Figure 377: Flat Hash Set



TO CREATE AND USE A FLAT HASH SET FROM A CASE

To create a Flat Hash Set, select the required format, MD5, SHA1 or SHA256 from the **Create Hash Set** button drop-down menu as shown in Figure 375 above (This executes a script which can be viewed and edited in the Scripts module). The following window appears:

Figure 378: Create Flat File Hash Set from Case

The screenshot shows a dialog box titled "MD5 - Create Flat Hash Set from Case". It has two tabs: "About" and "Options". Under the "Options" tab, there are two radio buttons under "Source": "All File System items (1859 items)" (selected) and "Checked File System items (0 items)". Below this is the "Destination File" section, which includes: "Hash Set Folder:" with a text box containing "C:\Users\Vera\Documents\Forensic Explorer v5\HashSets\" and a browse button "..."; "File Name:" with a text box containing "Flat Hash Set"; a checked checkbox "Include Comment in Header" with "File Comment:" (text box: "Flat Hash Set created by Forensic Explorer 27-Sep-2019 2:09:54 PM") and "Case Name:" (text box: "New Case 52"); and another checked checkbox "Specify Column Text in Header" with "HashSet:" (text box: "Flat Hash Set") and "Identified As:" (dropdown menu: "Known"). At the bottom right are "Create" and "Cancel" buttons.

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 377 above.

22.9 HASH MATCH

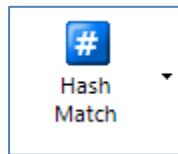
A Hash Match is the process whereby hash values contained in a Hash Set are matched to hash values in a case.

To run a Hash Match:

1. Hash individual files in your case as described in 22.5 above.

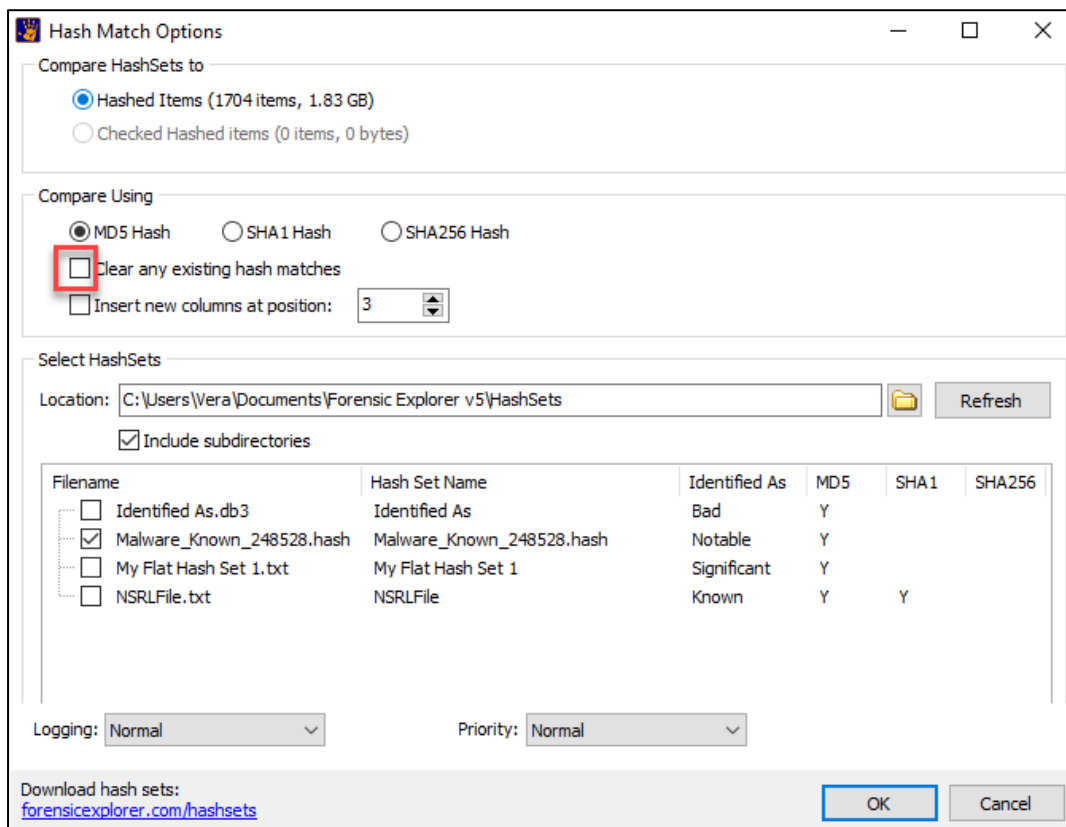
- In the File System module, click the **Hash Match** icon > Hash Match.

Figure 379: File System module, Hash Match icon



- The Match Hash window will open:

Figure 380: Match Hash window



- 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 381: Running a Hash Match in a case.

Hash (MD5)	HashSet ▼	HashSet Identified As
b6d81b360a5672d80c27430f39153e2c	GetData [Windows]	good
f1c9645dbc14efddc7d8a322685f26eb	GetData [Windows]	good
bdf3bf1da3405725be763540d6601144	GetData [Windows]	good
fafa5efeaf3cbe3b23b2748d13e629a1	GetData [Windows]	good
076e3caed758a1c18c91a0e9cae3368f	GetData [Windows]	good
9aebbac92e6bf3b4009f79be3549b5a	GetData [Windows]	good
cdf80f35aba322d5d0e6b6f6fe0b2995	GetData [Windows]	good
ba45c8f60456a672e003a875e469d0eb	GetData [Windows]	good
5a44c7ba5bbe4ec867233d67e4806848	GetData [Windows]	good
9d377b10ce778c4938b3c7e2c63a229a	GetData [Windows]	good
15988347a31ba4fb6dce89f1931db7bf	GetData [Windows]	good
3e80abdf74d921066de10fb05aaa553f	GetData [Windows]	good
2b04df3ecc1d94afddff082d139c6f15	GetData [Windows]	good
9b1afac7447e4b7c1c98702e261be2e	GetData [Windows]	good
b44a59383b3123a747d139bd0e71d2df	GetData [Windows]	good

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

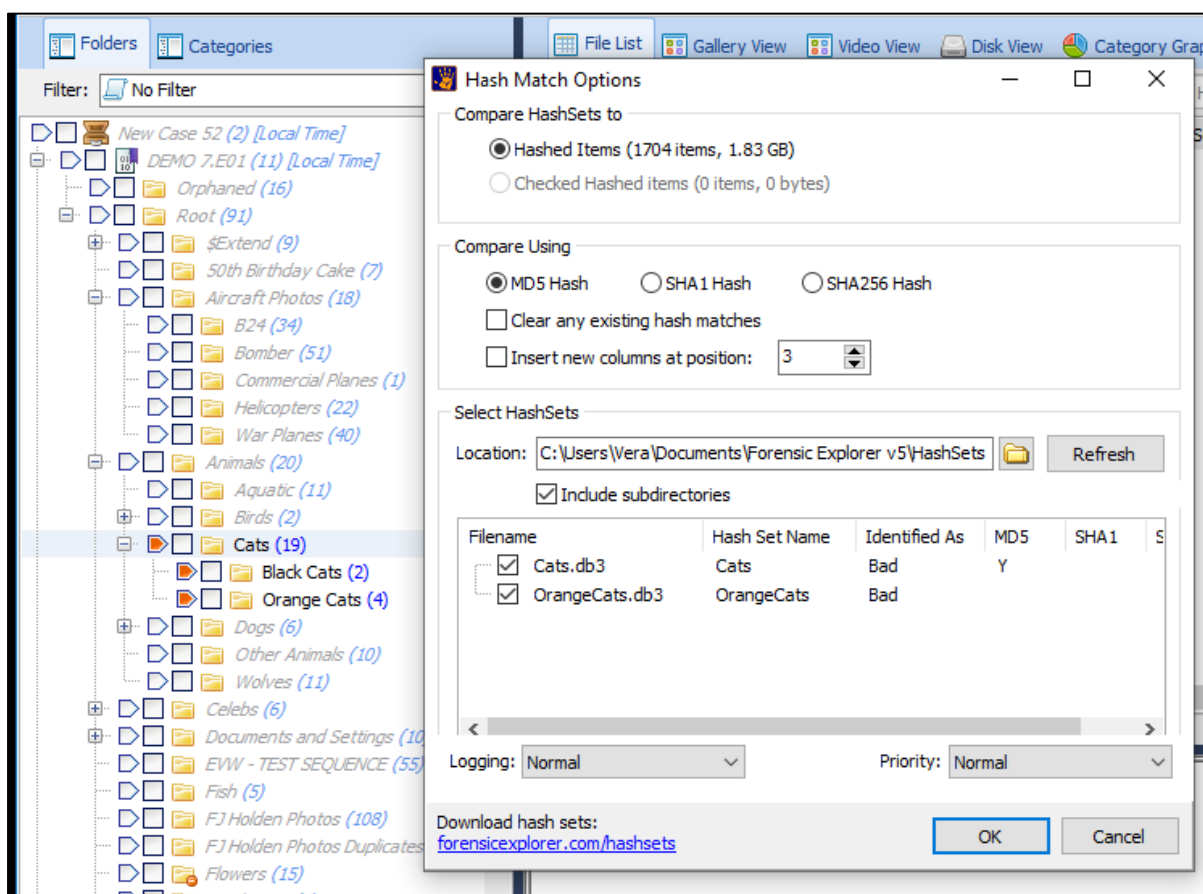
22.9.1 HASH MATCH WITH MULTIPLE HASH SETS

In the following example two hash 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**, contains a hash for **4 files** in the **Orange Cats** folder.

As shown in Figure 382 below:

Figure 382: Hash Match with multiple hash sets



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 **Hash Set** column and separated by a comma. For example, in Figure 383 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 383 below;
 - the text **"bad"** identifies a Hash Match for one of the hash sets; and

- the test “**bad,bad**” identifies a match in both hash sets.

Figure 383: Hash Match using multiple hash sets.

Filename	Ex...	HashSet	HashSet Identified As	Hash (MD5)
1 Orange Cat 1.JPG	JPG	Cats,OrangeCats	Bad,Bad	df95058a18c2715
2 Orange Cat 2.JPG	JPG	Cats,OrangeCats	Bad,Bad	93d1492cc81de6c
3 Orange Cat 3.JPG	JPG	Cats,OrangeCats	Bad,Bad	6da41b620b54cc8
4 Orange Cat 4.JPG	JPG	Cats,OrangeCats	Bad,Bad	4fa22addaf20fc7
5 Baby_cat_sleeping...	JPG	Cats	Bad	36f49dbcb43efe5
6 Black Cats~\$130(\$90)		Cats	Bad	a366487ad4bd06i
7 CatsA10_Baby.JPG	JPG	Cats	Bad	01bf9f0a41df45ai
8 CatsA2_Mary.JPG	JPG	Cats	Bad	4f3e99434df20e0
9 CatsA3_Choco.JPG	JPG	Cats	Bad	bfdfec997fd14dfc
10 CatsA4_Kristaji.JPG	JPG	Cats	Bad	524adf4a69aaf0c
11 CatsA5_Starbuck.JPG	JPG	Cats	Bad	4c945991b63ad9c

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.

22.9.2 NSRL HASH SETS

Forensic Explorer v5 now works directly with NSRL hash sets. Place NSRL hash sets into the Hash Sets folder and they will be directly available under the Hash Match button. It is recommended that SHA1 be used to match against NSRL hash sets as they are pre-sorted by SHA1, and it significantly improves the RAM load speed of large sets.

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, 25 October 17).

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

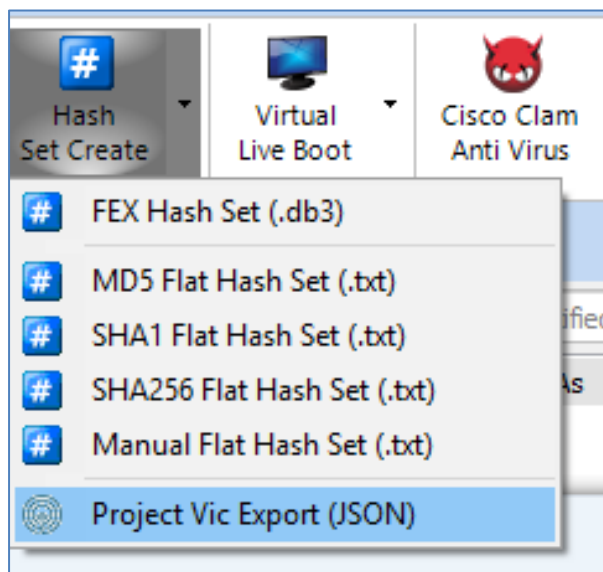
22.10.1 EXPORT PROJECT VIC

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 MD5 hash is mandatory). To hash files, follow the instructions in 22.5 above.
2. In the File System module, click on **Hash Set Create > Project Vic Export (JSON)**:

Figure 384: Project Vic Export as JSON



3. The **Export JSON VIC File Options** window will open:

Figure 385: Export Project VIC™ JSON file

Export JSON VIC File Options

Process Name:
Export JSON VIC File

Source

Module: FileSystem

Hashed Items (1704 items, 1.82 GB)
 Checked Hashed items (4 items, 3.0 MB)

Destination

File type: Project VIC model 1.3

Export: Do Not Export
Do Not Export
Export with unique FileName
Export with hash FileName
Export with hash FileName and Extension

Sort:

Destination Folder:
C:\Users\Vera\Documents\Forensic Explorer v5\Cases\New Case 52\Exported\

Destination File:
ExportProjVic.json

Logging: Normal

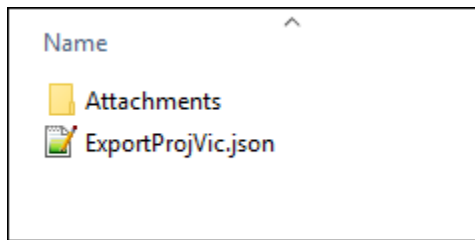
Priority: Normal

OK Cancel

- 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). Choose an option for the export.
- 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.

The export to Project Vic will result in the following in a **ExportProjVic.json** file and an accompanying **Attachments** folder. The json file holds the metadata and links to the actual exported files in the attachments folder (json file and the folder need to stay together as they are linked).

Figure 386 - Export to Project Vic - Output



22.10.2 IMPORT PROJECT VIC .JSON WITH ATTACHMENTS (FROM 3RD PARTY TOOL)

To import Project Vic evidence into Forensics Explorer from a third-party product (e.g., Griffey):

1. In the Evidence module, start a **new case**.
2. Click the **Add Image** button and select the **.JSON** file (e.g., as shown in Figure 386 above). Note that the **JSON file must be accompanied by the Attachments folder (containing the files) in the same directory**.

The contents of the **Attachments folder** will then be visible within Forensic Explorer.

22.10.3 PROJECT VIC .JSON – HASH MATCH

To hash match using Project Vic json:

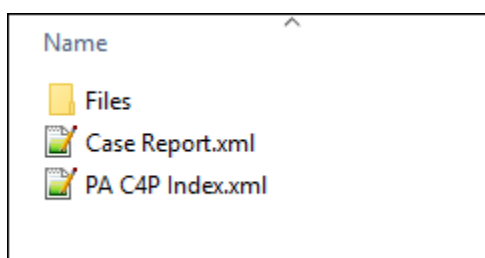
1. Add the .JSON file to the Hash Sets folder: `..\Documents\Forensic Explorer v5\HashSets\`
2. In the File System module, click on the **Hash Match** button. The JSON files will appear in the list of available hash sets in the **Hash Match Options** window.
3. **Check** the required file and click **OK** to run the Hash Match.

IMPORTANT: Files in the case must **already be hashed** with the relevant type of hash (e.g., MD5) in order for a match to take place.

22.10.4 IMPORT C4ALL

Similar to Project Vic (described above) some programs like **Cellebrite** export data in to a **C4All** format. The C4All format uses an **XML** file to store the metadata which points to files contained in a **Files** folder:

Figure 387 - C4ALL Data from Cellebrite



To import C4All data into Forensics Explorer:

1. In the Evidence module, start a new case.
2. Click the **Add Image** button and select the ...**index.xml** file (this file must be accompanied by the **Files** folder containing the data).

Note that in the example shown in Figure 387 above the structure of the filename is:

PA = Cellebrite Physical Analyzer

C4 = Short for C4All

P = Photos (this may be replaced by M for a movie specific export).

Chapter 23 - File Signature Analysis

In This Chapter

CHAPTER 23 - FILE SIGNATURE ANALYSIS

23.1	File signature analysis	376
23.2	Why run file signature analysis?	376
23.3	Running a file signature analysis.....	377
23.4	Examine the results of a file signature analysis	378

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 388: JPEG file signature below, is the beginning of a photo taken with a digital camera. It is identified as a JPEG by the file header `ÿØÿà` (or in Hex: FF D8 FF E0 00).

Figure 388: JPEG file signature

```
ÿØÿà. .JFIF.....'.'...ÿá:4Exif..MM.*.....
.....ž.....
.....°.(.....1...../
...Ä.2.....ò.....#i.....
Ã¥.....Ð..&>ËÖ.....@...'...'NPanasonic.DM
C-TZ15.....'.....'.....Microsoft Window
s Photo Gallery 6.0.6001.18000..2009:07:
19 15:39:02..#,#,š.....°,.....,^"
.....^'.....0221.....
```

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 it gives the investigator 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:

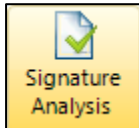
- Identify files for which the file extension does not match the file signature. These files may have been deliberately manipulated to hide data.
- Empower other components of Forensics Explorer, such as the Categories view, to see files based on file signature, rather than extension.

23.3 RUNNING A FILE SIGNATURE ANALYSIS

To run a file signature analysis in Forensic Explorer:

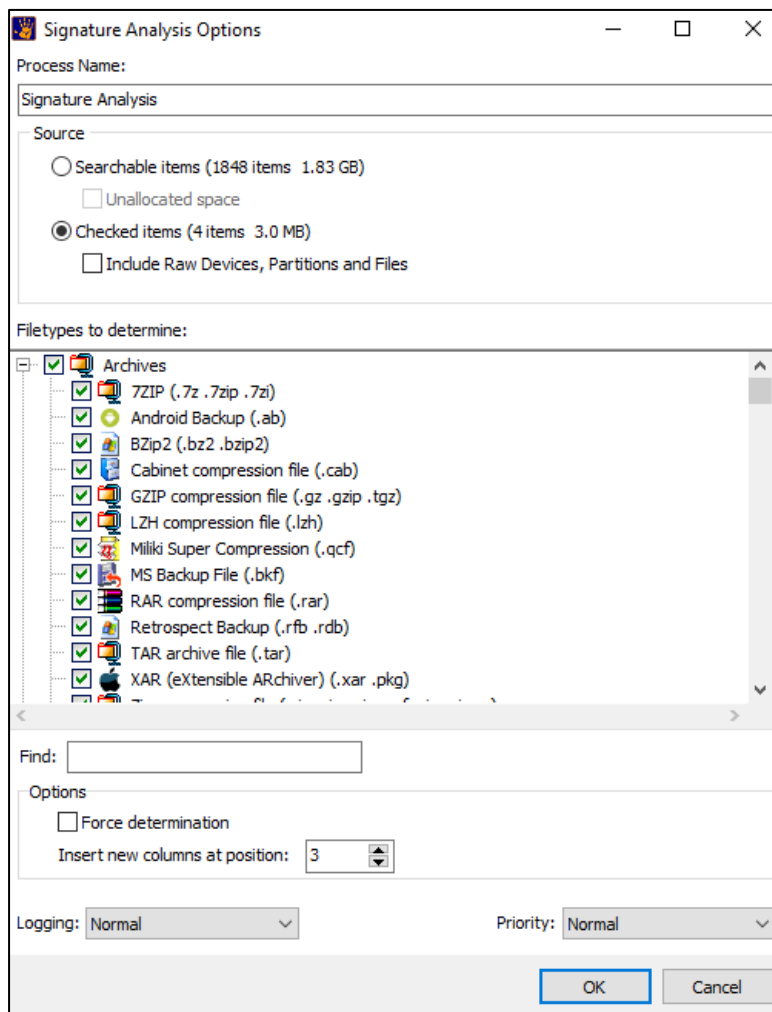
1. Click on the **Signature Analysis** button in the File System toolbar (shown below) to open the **Signature Analysis Options** window shown in Figure 390: Selecting file types for signature , below:

Figure 389: Signature Analysis button in the File System module toolbar



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 390: 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:

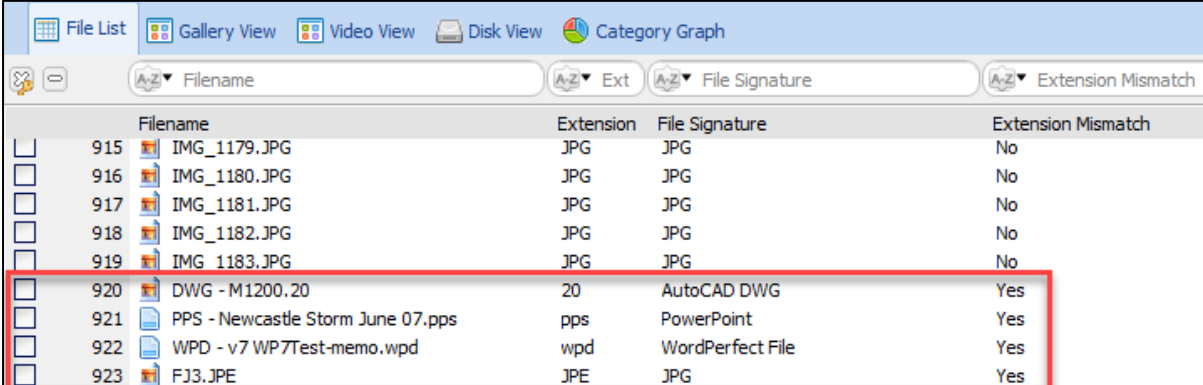
- shows an extension:** This means that it has been successfully identified as a file type contained within the Forensic Explorer signature list, shown in Figure 390 above; or,
- No Size:** The file does not have a logical or physical size, or the file does not have a run list in the Master File Table.
- Folder:** A folder.
- Unknown:** The file signature could not be matched against the file types contained in the Forensic Explorer signature list.
- 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 391 below:

Figure 391: File System module columns relating to file extension.



	Filename	Extension	File Signature	Extension Mismatch
<input type="checkbox"/>	915 IMG_1179.JPG	JPG	JPG	No
<input type="checkbox"/>	916 IMG_1180.JPG	JPG	JPG	No
<input type="checkbox"/>	917 IMG_1181.JPG	JPG	JPG	No
<input type="checkbox"/>	918 IMG_1182.JPG	JPG	JPG	No
<input type="checkbox"/>	919 IMG_1183.JPG	JPG	JPG	No
<input type="checkbox"/>	920 DWG - M1200.20	20	AutoCAD DWG	Yes
<input type="checkbox"/>	921 PPS - Newcastle Storm June 07.pps	pps	PowerPoint	Yes
<input type="checkbox"/>	922 WPD - v7 WP7Test-memo.wpd	wpd	WordPerfect File	Yes
<input type="checkbox"/>	923 FJ3.JPE	JPE	JPG	Yes

Chapter 24 - Data Recovery

In This Chapter

CHAPTER 24 - DATA RECOVERY

24.1	Data Recovery - Overview	382
24.2	FAT data recovery	383
24.2.1	FAT - Deleted files	383
24.2.2	FAT - Recover folders	387
24.3	NTFS data recovery	389
24.3.1	NTFS - deleted files	389
24.3.2	NTFS - orphans	390
24.3.3	NTFS - Recover Folders	391
24.4	File carving	392
24.4.1	Carving advantages and limitations	392
24.4.2	Forensic Explorer file carving engine	394
24.4.3	Carving using scripts	398
24.4.4	Merge Carved Data	398

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.

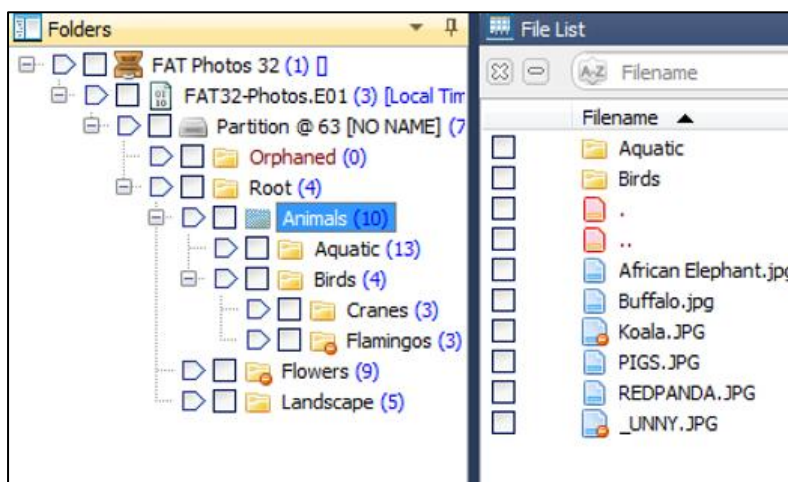
24.2.1 FAT - DELETED FILES

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 392 below:

Figure 392: 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 of a file's 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 392 above with the deleted file “_UNNNY.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 a Short File Name (SFN) is overwritten when a file is deleted by the 0xE5 marker. For display purposes, Forensic Explorer replaces the first character with an underscore.

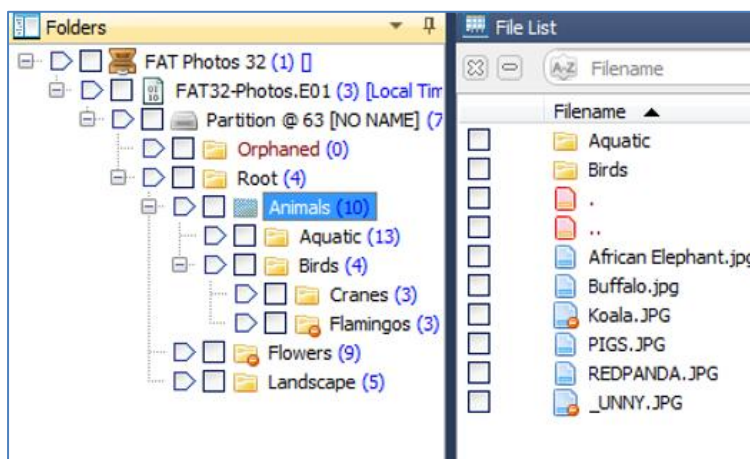
Where a file having both a SFN and a Long File Name (LFN) directory entry, the missing first character of the file name is in the LFN and is used by Forensic Explorer to display the full original file name.

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 393 below, the parent folder of the file Koala.JPG is highlighted in Folders view:

Figure 393: Animals folder selected in Folders view.



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

Figure 394: Animals directory showing 32-byte directory entries.

16	17	18	19	1A	1B	1C	1D	1E	1F	
2B	69	73	3E	03	00	00	00	00	00	...*is>s>..+is>.....
2B	69	73	3E	00	00	00	00	00	00*is>s>..+is>.....
FF	FF	FF	FF	00	00	FF	FF	FF	FF	Ba.n.t...j...ip.g...ÿÿÿÿÿÿ.ÿÿÿÿ
6C	00	65	00	00	00	70	00	68	00	.A.f.r.i.c...ia.n. .E.l.e...p.h.
FD	96	EE	3A	04	00	EC	E2	09	00	AFRICA~1JPG ..*is>s>..ý.í:..iâ..
70	00	67	00	00	00	00	FF	FF	FF	AB.u.f.f.a...íl.o...j.p.g....ÿÿ
0B	58	8D	39	A3	00	A9	C1	0E	00	BUFFALC JPG .N*is>s>...X.9f.@Á..
65	B3	59	3E	90	01	AA	B3	05	00	¿UNNNY JPG ..*is>s>..e*Y>..*^..
00	00	FF	FF	00	00	FF	FF	FF	FF	¿K.o.a.l.a...x...J.P.G...ÿÿ.ÿÿÿÿ
8D	0E	EF	3A	EC	01	1F	EA	0B	00	¿CALA JPG ..*is>s>...i:i..â..
4A	B3	59	3E	AB	02	F8	CC	0A	00	PIGS JPG ..+is>s>..J*Y>«.æí..
96	70	77	3C	58	03	F8	9E	0F	00	REDPANDA.JPG .Z+is>s>...pw<X.æ...
FF	FF	FF	FF	00	00	FF	FF	FF	FF	AA.q.u.a.t...xi.c...ÿÿÿÿÿÿ.ÿÿÿÿ
E4	53	73	3E	52	04	00	00	00	00	AQUATIC ...c+is>s>..âSs>R.....
FF	FF	FF	FF	00	00	FF	FF	FF	FF	AB.i.r.d.s...z...ÿÿÿÿÿÿÿÿÿ.ÿÿÿÿ
24	5E	73	3E	15	0D	00	00	00	00	BIRDS ...F.is>s>..\$^s>.....

The directory entries show:

- That file “_OALA .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 395:

Figure 395: Decoded directory entry of "Koala.JPG"

Property	Value	Raw Value	Type
FAT Record (4,111,136)			
Short Filename	1 → _OALA .JPG	_OALA .JPG	AString
Deleted	True	True	Boolean
Attributes	A	32	Byte
Reserved	0	0	Byte
Created (10ms)	156	156	Byte
Created Time	1:09:20 PM	26922	Word
Created Date	19-Mar-11	15987	Word
Accessed Date	19-Mar-11	15987	Word
EAIIndex (FAT12/16)	0	0	Word
Written Time	1:52:26 AM	3725	Word
Written Date	15-Jul-09	15087	Word
Start Cluster (FAT12/16)	492	492	Word
Start Cluster (FAT32)	2 → 492	492	LongWord
Filesize	3 → 780,831	780831	LongWord
Longfile Record 1			
LFN String	4 → Koala.JPG	Koala.JPG	UString
LFN Sig. byte	229	229	Byte
LFN Attribute	15	15	Byte
LFN Flag	0	0	Byte
LFN Checksum	215	215	Byte
LFN FirstCluster	0	0	Word

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:

Filesystem Record				
Property	Value	Raw Value	Type	
[-] FAT32 VBR Record (32,256)				
JMP Instructions	EB 58 90		Binary	
OEM name	MSDOS5.0	MSDOS5.0	AString	
Bytes per sector	512	512	Word	
Sectors per cluster	8	8	Byte	
Reserved sectors	34	34	Word	
Number of FAT's	2	2	Byte	
Number of root entries ...	0	0	Word	
Number of sectors (16 bit)	0	0	Word	
Media	248	248	Byte	
Sectors per FAT	0	0	Word	
Sectors per track	63	63	Word	
Heads	255	255	Word	
Hidden sectors	63	63	LongWord	
Number of sectors (32 bit)	4,064,382	4064382	LongWord	

To determine the number of clusters used by Koala.JPG, the calculation is:

- File size: 780,832 bytes / 512 bytes per sector = 1525.06 sectors
- 1525 sectors / 8 sectors per cluster = 190.63 clusters

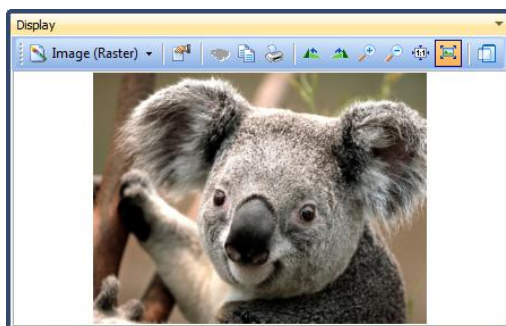
The number of clusters that can be attributed to Koala.JPG is 191. The file therefore starts at cluster 492 and finishes at the end of cluster 682.

To see this information in Forensic Explorer, switch to the "File Extent" view which details the byte, sector, and cluster positions of the file:

Cluster Start: 492
 Cluster End: 682
 Cluster Length: 191
 Sector Start: 11941
 Sector End: 13468
 Sector Length: 1528

Highlighting the sectors in disk view reveals the following picture:

Figure 396: Display view of Koala.JPG

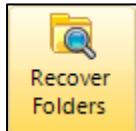


24.2.2 FAT - RECOVER FOLDERS

“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 397: Recover Folders File System module toolbar icon.



This opens the **Recover Folders** options window:

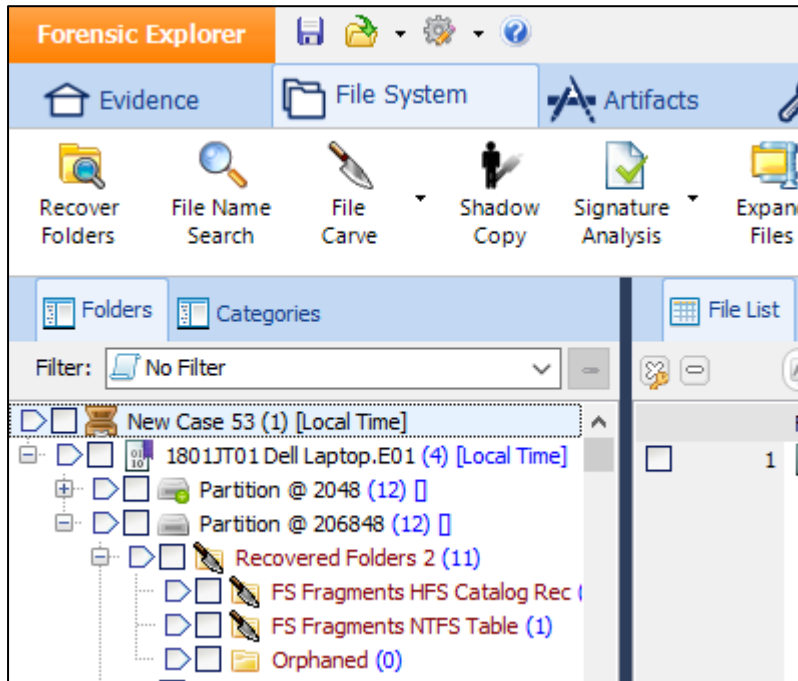
Figure 398: Recover Folders options

Name:	Enter the folder name which will hold the recovered folders in the Folders view of the File System module.
Source:	A Recover Folders search must be run on an existing partition . Select the partition from the drop-down menu.
File Systems:	Select the type of File System records for which to search.
Keep Filesystem fragments:	Fragments are the carved MFT, FAT, etc records that are used to rebuild the folder and file structure. Once the file structure is rebuilt and displayed, the fragments are no longer required. If this option is checked the carved items are displayed in a sub-folder called FS Fragments (as shown in Figure 399). If the option is not checked the fragments are not added.
Logging & Priority:	See 7.5 – Logging and Priority.

When the “Recover Folders” command is executed on a FAT partition in Forensic Explorer, the program searches unallocated clusters for the “dot, double dot” directory entry signature 0x2E and 0x2E2E as well as LFN and SFN directory entry structures.

The “Double Dot” is used to locate the parent folder and traverse up the directory tree. Eventually, 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:

Figure 399: 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 Table 1 and Table 2 below:

Table 1: Allocation status for a file

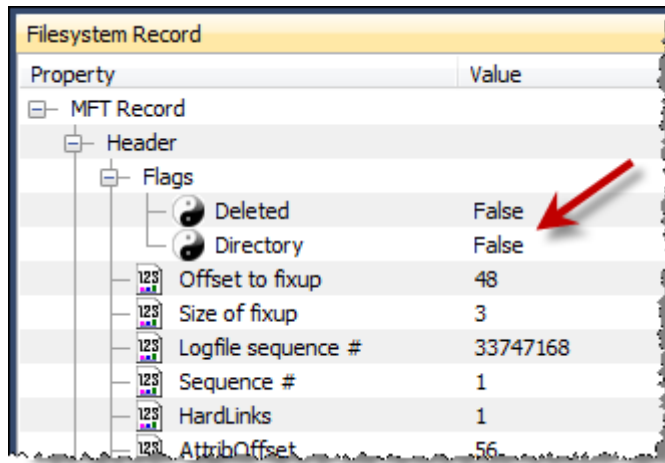
Flag Value for a file		
Hex	Binary	Status
00	00000000	Unallocated
01	00000001	Allocated

Table 2: Allocation status for a folder

Flag value for a folder		
Hex	Binary	Status
02	00000010	Unallocated
03	00000011	Allocated

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

Figure 400: Forensic Explorer Record view showing decoded MFT allocation status (an allocated file)



When the MFT record is marked as unallocated, both the MFT record, and clusters used to store the data (for non-resident files) become available to store new data. However, importantly:

- the file attributes within the unallocated MFT record remain intact;
- the data for the file remains untouched.

When new data is written to the MFT record or the clusters holding the data, the possibility for successful recovery of the deleted file is diminished.

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.

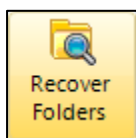
- CHILD-FOLDER-1 and its content are available, but Forensic Explorer cannot determine where in the tree structure it belongs. The Orphans folder is created by Forensic Explorer to hold CHILD-FOLDER-1 and its content.

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.**

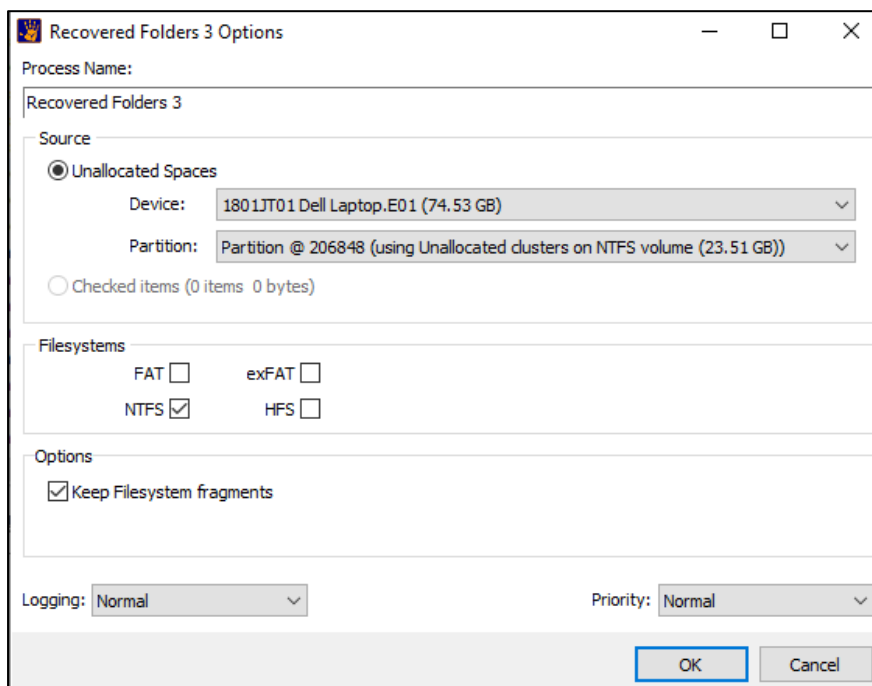
To run a **Recover Folders** search, click the **Recover Folders** toolbar icon in the File System module:

Figure 401: Recover Folders File System module toolbar icon.



This opens the **Recover Folders** options window:

Figure 402: Recover Folders options.



When the “Recover Folders” command is executed on a NTFS partition in Forensic Explorer, the program searches unallocated clusters for MFT records.

The process is identical to that described in “NTFS Orphans” above. The only difference is that instead of working with files in existing MFT records, the MFT records themselves are recovered from unallocated space.

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” (16).

An example of a file signature is shown in Figure 403, which is the beginning of a .jpg file in Hex view:

Figure 403: View of .jpg file header

```

ÿØÿà..JFIF.....'..'ÿá:4Exif..MM.*.....
.....ž.....".....
.....°.(.....1...../
...À.2.....ò.....#i.....
Ä¥.....ð...&>EÒ.....@...'...'N Panasonic.DM
C-TZ15.....'.....'.....Microsoft Window
s Photo Gallery 6.0.6001.18000..2009:07:
19 15:39:02..#,š.....°,.....,^"
.....^'.....0221.....
  
```

The object of the carving exercise is to identify and extract (carve) the file based on this signature information alone. Carrier (2005) describes File carving as:

“...a process where a chunk of data is searched for signatures that correspond to the start and end of known file types. The result of this analysis process is a collection of files that contain one of the signatures. This is commonly performed on the 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 under FAT, NTFS, HFT, EXT2 or other file systems and can be data carved accordingly. File carving is also an 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:

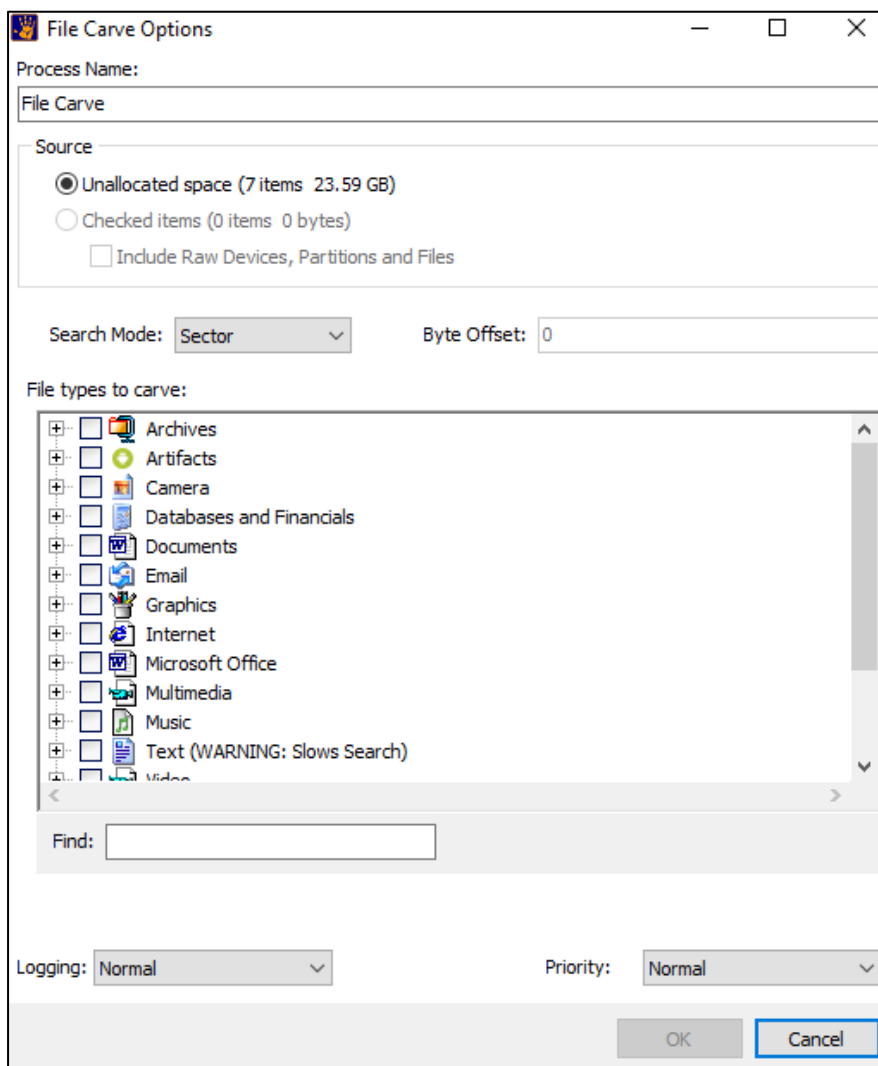
1. Switch to the File System module;
2. Click the File Carve button on the ribbon;

Figure 404: File System module, File Carve button



The “File Carving” selection window, shown in Figure 405 will open:

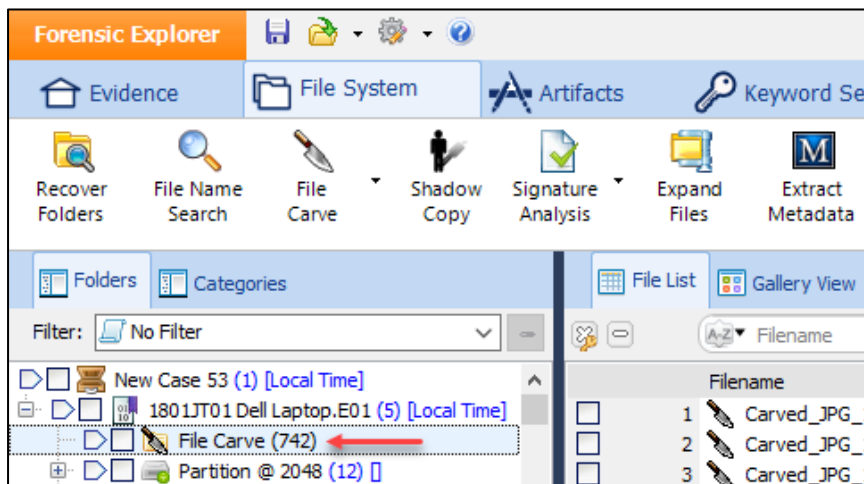
Figure 405: File carving file signature selection window



CARVE NAME

The carve name is the name of the folder which holds the carve results. This folder is displayed in Folders view of the File System module. The default name, "File Carve" can be edited during setup of the search.

Figure 406: File Carve results.



SOURCE

A File Carve is usually run on unallocated space. However, it is possible to carve on a specific file, such as the Windows page file, or a backup file, by first checking the file in the File System module and then selecting to carve the checked items.

CARVE SEARCH MODE:

Cluster based file carving

In a cluster-based file system like FAT or NTFS a new file must start in a new cluster. It follows then that the file signature appears near a cluster boundary. Carving speed is therefore achieved by searching for file signatures only near cluster boundaries.

Sector based file carving (recommended)

It is recommended to perform a lower-level search for sector-aligned file signatures. This search may recover additional files, for example files from a previous volume which had a different cluster layout and is no longer aligned to current cluster boundaries.

NOTE: Carving in sector mode will increase the length of the search.

File Carve > 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.

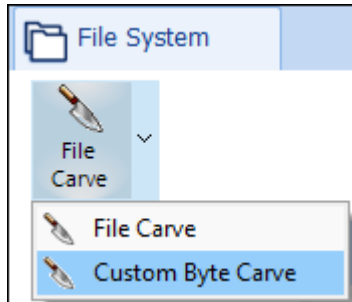
NOTE: Carving in byte mode will greatly increase the length of the search.

CUSTOM BYTE CARVE

Custom Byte Carve is an alternative method to file carve at a byte level. Custom Byte Carve is a script, and uses RegEx as its means of traversing data.

Launch Custom Byte Carve from the drop down menu of the File System module > File Carve > button:

Figure 407: Custom Byte Carve.

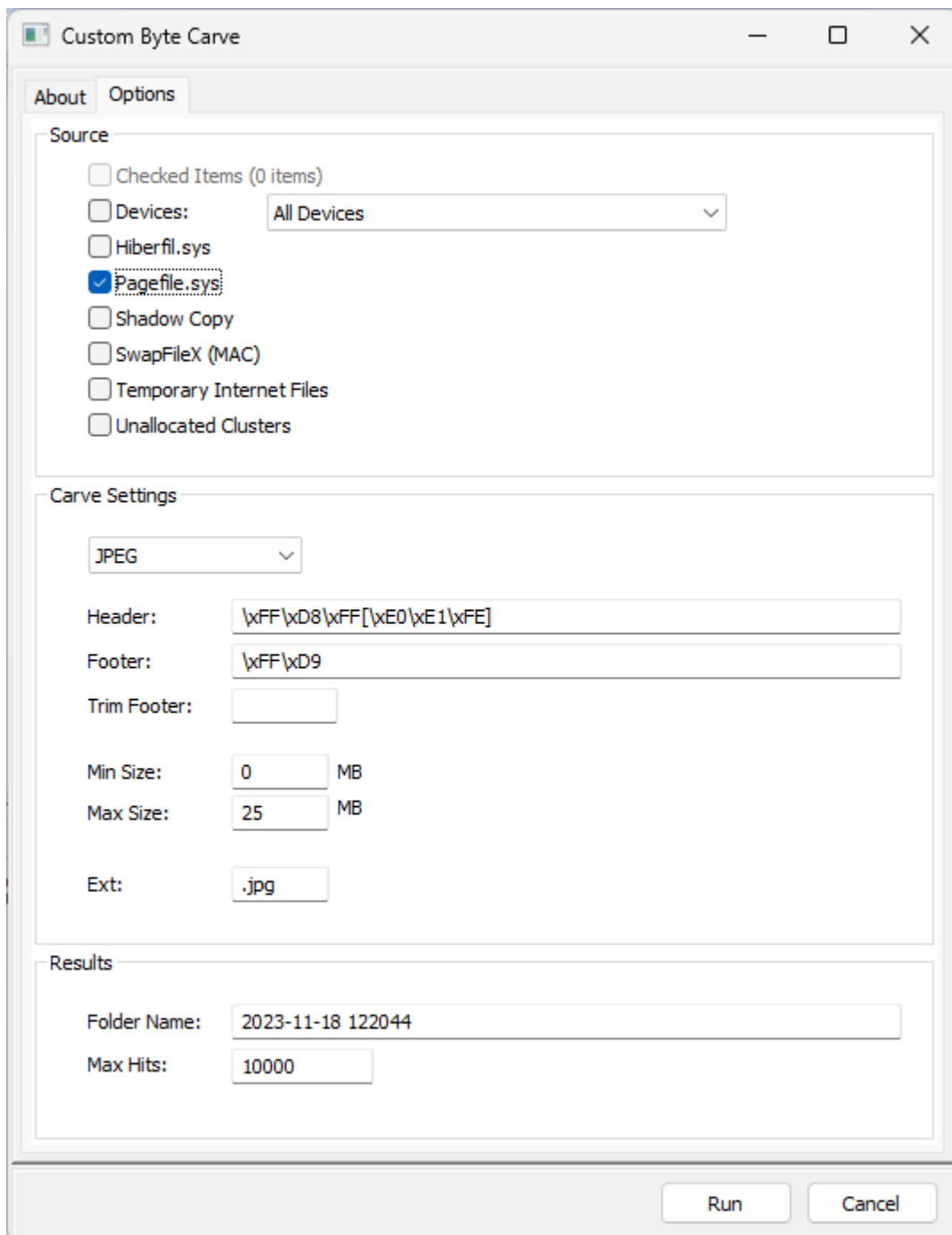


Custom Byte Carve is useful for searching sequential data file such as:

- Hiberfil,
- Pagefile,
- Swap file.

The primary advantage is that users can enter custom header, footer and size information, as show in Figure 408 below.

Figure 408: Custom Byte Carve.



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.

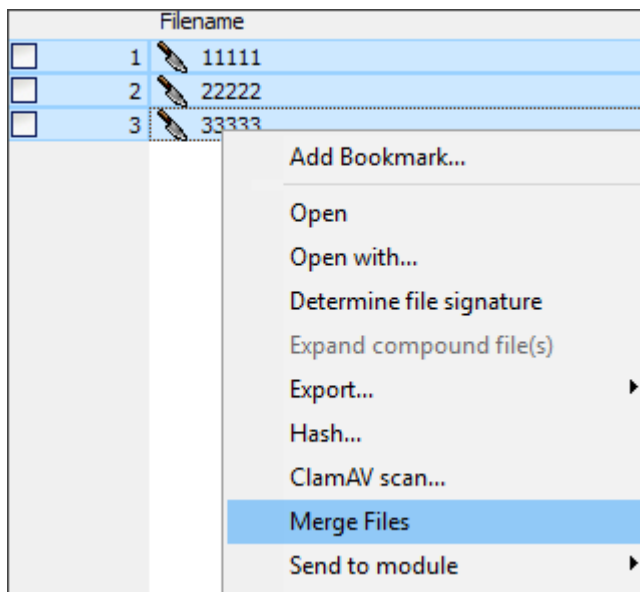
24.4.4 MERGE CARVED DATA

In some circumstances, e.g., carving a fragmented file, it may be necessary to join individual fragments of carved data to make a single file.

To **merge** or **join** files:

1. Select the carved files.
2. Right-click and select Merge Files from the drop-down menu.

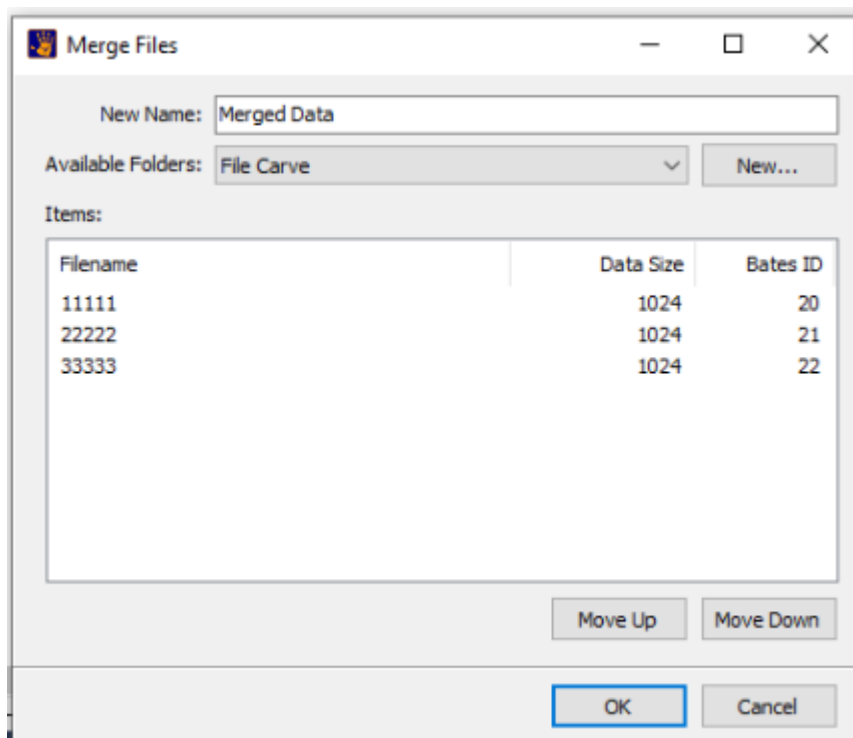
Figure 409: Merge files



In the **Merge Files** window:

1. Adjust the sequence of fragments as needed using the **Move Up** and **Move Down** buttons.
2. Enter a **New Name** to describe the new created file.
3. Click **OK to add** the file to the File System module.

Figure 410: Merge files



Chapter 25 - RAID

In This Chapter

CHAPTER 25 - RAID

25.1	RAID - Introduction	402
25.2	Preparation	402
25.3	Adding a RAID to a case	403
25.3.1	Hardware RAID, known configuration:	403
25.3.2	Software RAID.....	405
25.3.3	Once the correct RAID layout is identified	405

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

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.

RAID 6

RAID 6 is like RAID 5 but parity data is written to two drives. That means it requires at least 4 drives and can withstand 2 drives failing simultaneously.

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);

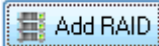
- What is the RAID format, JBOD, RAID 0, 1, 5, other? (Are the drives in the raid identical in size and capacity? This information may be obtained from the system administrator or setup documentation).
- What is the RAID stripe size? (This information may be determined from the RAID controller)
- How many physical disks make up the RAID?
- What is the sequence of the physical disks in the RAID? (Noting or photographing 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:

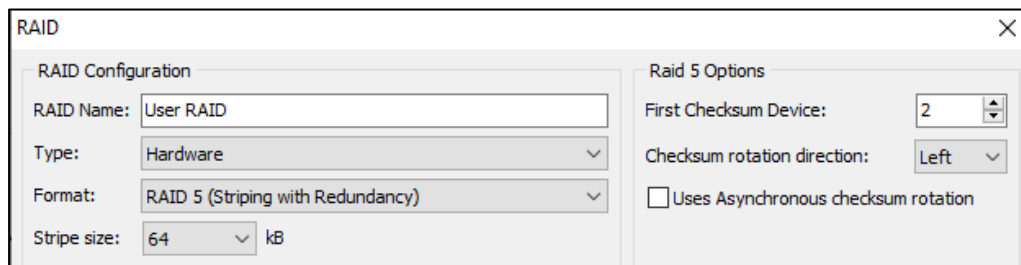
1. Physical disks (Note: When using physical disks, a hardware write blocking device is recommended to preserve forensic integrity);
2. Forensic Image Files; or,
3. A combination of both physical disks and forensic image files.

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  button. This opens the RAID configuration window.

25.3.1 HARDWARE RAID, KNOWN CONFIGURATION:

Enter the RAID configuration information:

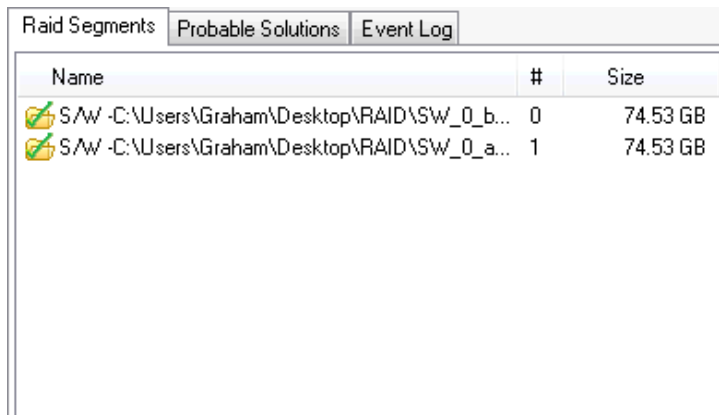


and follow the instructions to add and test the RAID.



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):



The screenshot shows a window titled "Raid Segments" with three tabs: "Raid Segments", "Probable Solutions", and "Event Log". The "Raid Segments" tab is active, displaying a table with the following data:

Name	#	Size
 S/W -C:\Users\Graham\Desktop\RAID\SW_0_b...	0	74.53 GB
 S/W -C:\Users\Graham\Desktop\RAID\SW_0_a...	1	74.53 GB

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

CHAPTER 26 – SHADOW COPY

26.1	Shadow Copy Introduction	408
26.1.1	Shadow Copy Configuration by Windows Users.....	408
26.1.2	When are Shadow Copies created?	410
26.1.3	Where are Shadow Copies STORED?	411
26.2	Examining Shadow Copies With Forensic Explorer	412

26.1 SHADOW COPY INTRODUCTION

The ability of Forensic Explorer to easily access and explorer Volume Shadow Copies (VSCs) offers the forensics investigator the ability to examine data at different time snapshots in a forensic examination. A Shadow Copy is essentially a differential backup of the contents of a drive. By examining a Shadow Copy it can be possible to view previous versions of a file, a directory, or a volume.

Prior to Windows Vista, “Restore Points” were a relatively simple snapshot of critical Windows system files. In Windows Vista and beyond, the Volume Shadow Copy Service (VSS) takes a snapshot of all files on the volume that has changed, including user files.

VSS is present on:

- Windows Server 2003
- Windows Vista (all versions)
- Windows Server 2008
- Windows 7 (all versions)

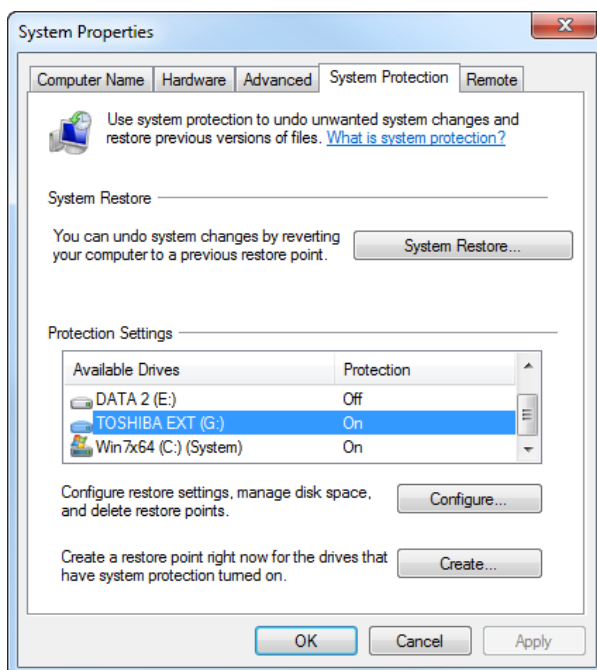
26.1.1 SHADOW COPY CONFIGURATION BY WINDOWS USERS

Windows VSC controls are access via:

“Control Panel\All Control Panel Items\System\System Protection”.

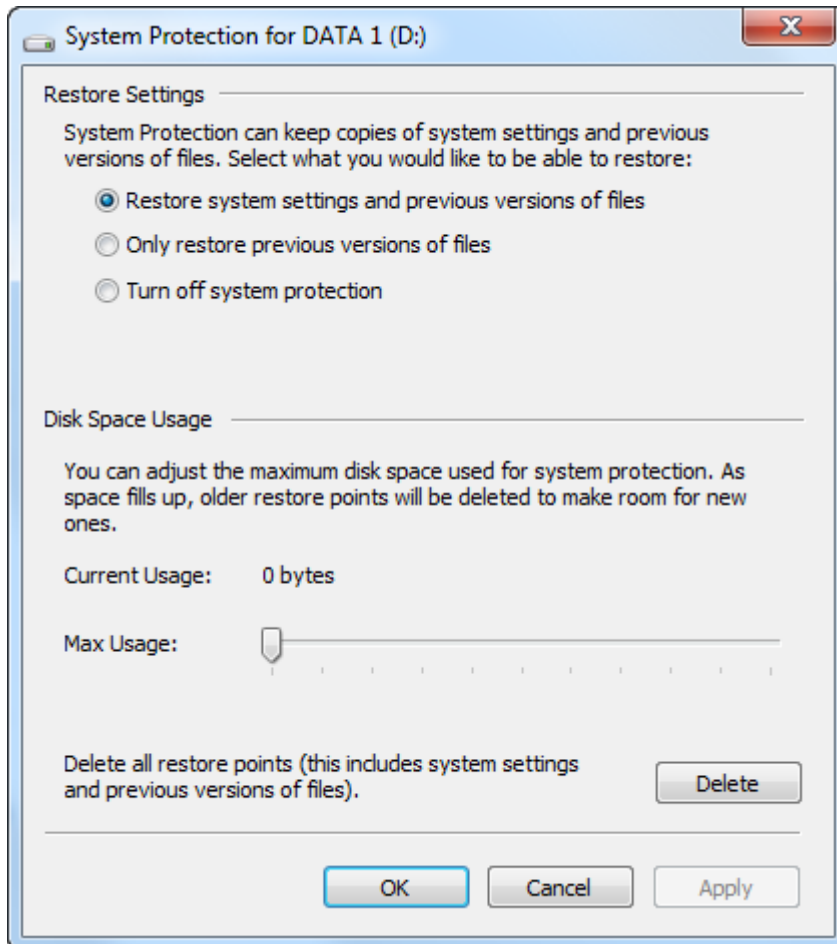
VSC is activated on an NTFS drive by turning on the Protections Settings in the System Properties windows. Shadow Copies can be created on local or removable media. The System Properties window (Win 7) is shown in Figure 411 below:

Figure 411: System Properties, Protection Settings



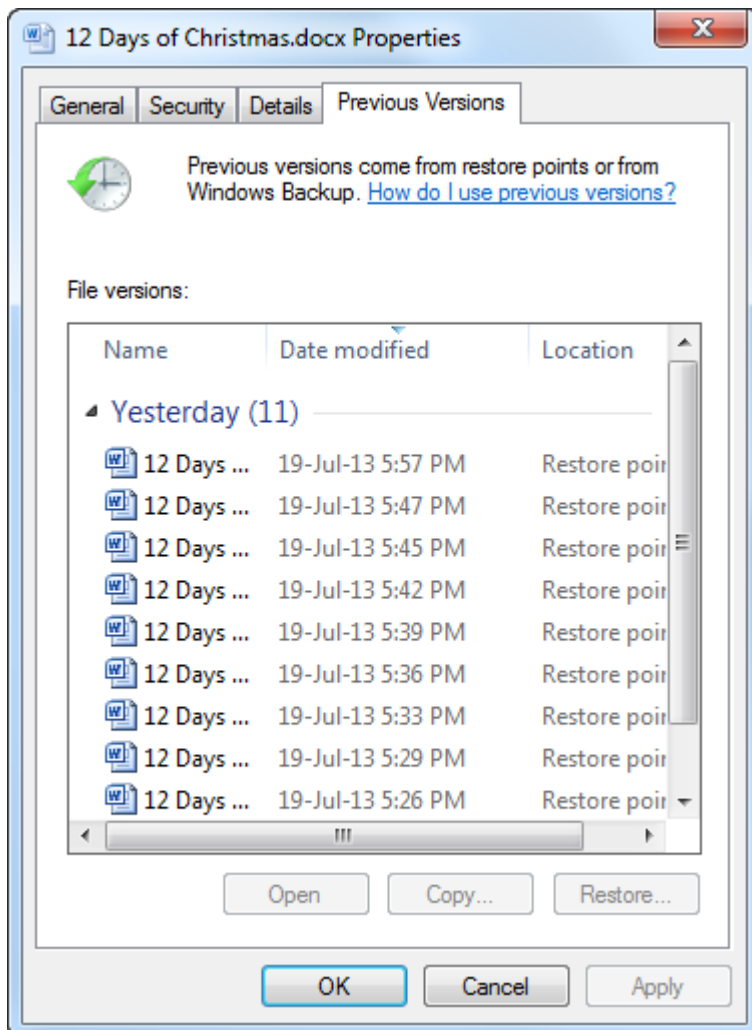
The configure button gives access to further settings. The lowest setting is to “**Only restore previous versions of files**”, with the option to “**Restore system settings and previous version of files**”. This is shown in Figure 412 below:

Figure 412: System Protection Settings



When VSC is active on a volume, a Windows user can right click on any file in Windows, select the **Properties** options for that file, and then access the **Previous Versions** tab, shown in Figure 413 below:

Figure 413: Windows file properties, Previous Versions



It is the ability to extract previous file versions which is of clear value to the investigator. It is possible, for example, that even though a file has been deleted and erased from the current file system (with no trace of the file in unallocated clusters), that a version of the file prior to its deletion could be contained within a VSC on the system.

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 411 above.

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;

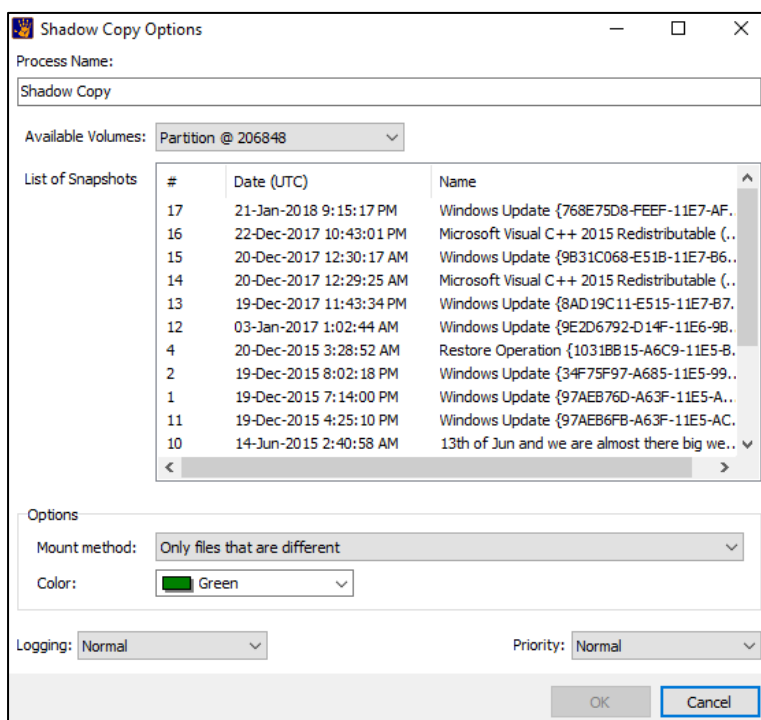
1. In the Forensic Explorer Evidence module, start a preview, a new case, or load an existing case;
2. Switch to the File System module to view the files in the case;
3. Click on the **Shadow Copy button** in the **File System module toolbar**:

Figure 414: Shadow Copy button in the File System Toolbar



4. The Forensic Explorer Volume Snapshot Mount window will open and list the available VSCs for the selected volume, as show in Figure 415 below:

Figure 415: Volume Snapshot Mount Window



Available Volumes:

Enables another volume and its shadow copies to be accessed.

Mount Method:

Only files that are different displays only those files in the VSC which are different from those listed in the current file system. This saves the investigator cluttering with the File System module with duplicate identical files from the VSC.


Each Shadow Copy catalog contains a list of cluster changes. The 'difference' is a comparison between the cluster changes in the Shadow Copy catalog versus the information supplied by the current MFT. A 'difference' does not necessarily mean that a file shown in the Shadow Copy has different content. It may just mean that a file is now located in different clusters in the current MFT, even though both files have the same MD5 hash.

All Files mounts the entire Shadow Copy.

Color:

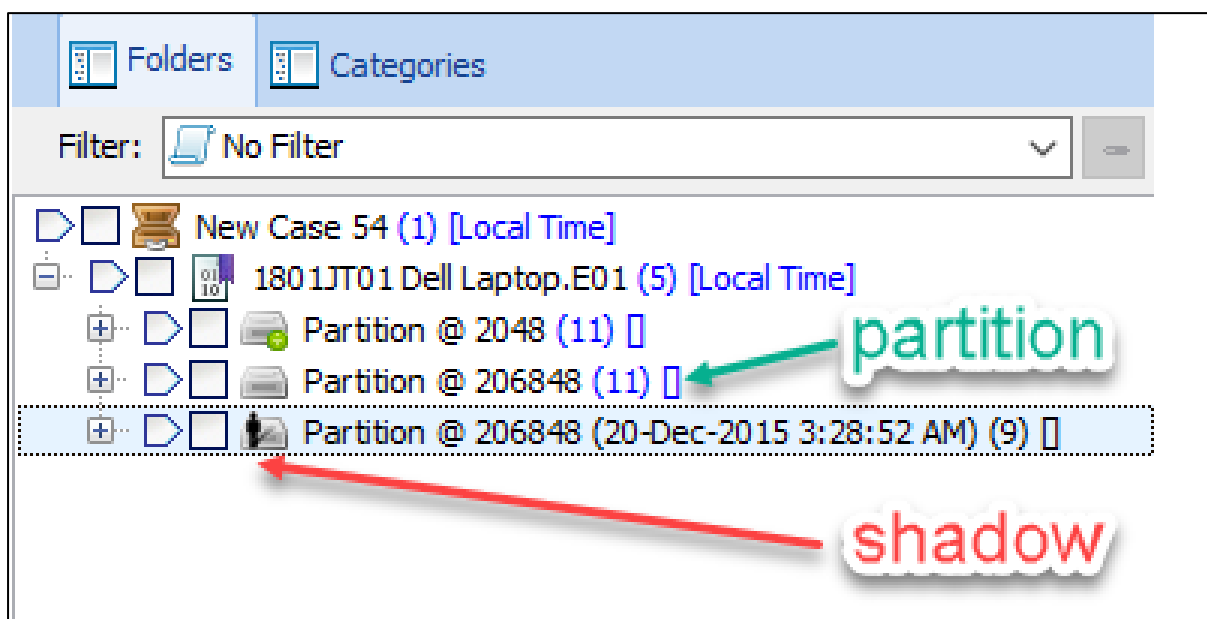
Assigns a color to the mounted VSS. If a color is selected, a new column is created in the File System module called "VSS". The columns contains the selected color to identify the origin of the file.

- 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 416 below:

Figure 416: File System module showing a mounted shadow copy



When a VSS has been added to the File System module, four new columns become available:

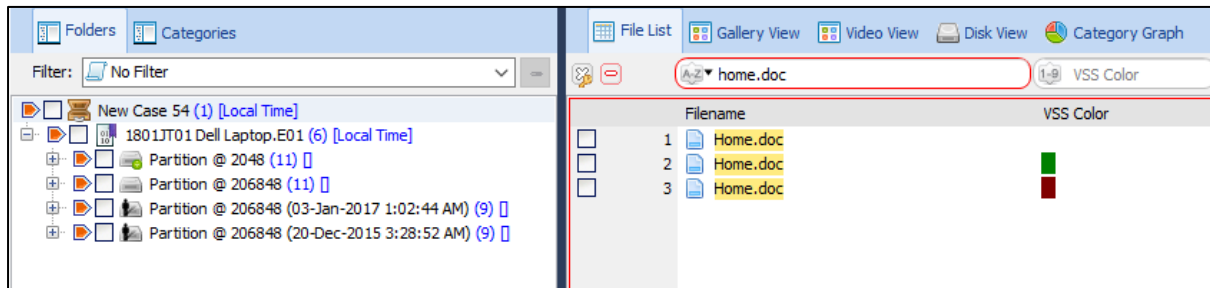
- VSS Color** – Contains the color assigned to the shadow copy volume during the mount process (if a color has been assigned, this column is automatically added to the File System module at position 2);

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 9.12.5), the Branch Plate (see 8.2.3), and the column filter tool (see 9.12.2) can be used, as shown below:

Figure 417: 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

CHAPTER 27 – MOUNT IMAGE PRO

27.1	Mount Image Pro	416
27.1.1	Install and run Mount Image Pro	416

27.1 MOUNT IMAGE PRO

Your Wibu dongle purchased with Forensic Explorer also contains 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 read 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/eMIP-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:

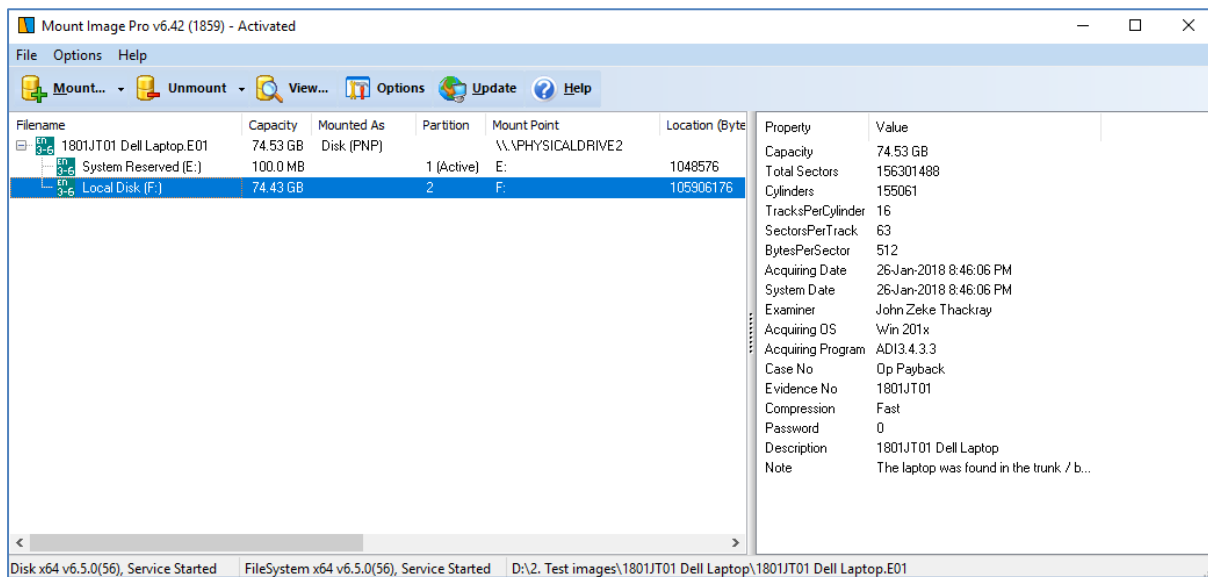
The Mount Disk option is used to Mount an image file and display the physical disk and / or partitions as if the physical drive were connected to the local computer. Windows is responsible for reading the file system and displaying the files.

Mount File System:

The Mount Filesystem button mounts the selected image or disk and uses the Mount Image Pro Version 6 Filesystem Driver (not Microsoft windows) to display the file system. This allows additional information to be displayed within the mounted image, including deleted files and Windows system files.

The Mount Image Pro GUI displays the image details and the assigned drive letter, as show in Figure 418 below:

Figure 418: 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 and in the support documentation for the product.

Chapter 28 – Live Boot

In This Chapter

CHAPTER 28 – LIVE BOOT

28.9.3	Method 2	462
--------	----------------	-----

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 an effective means 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)

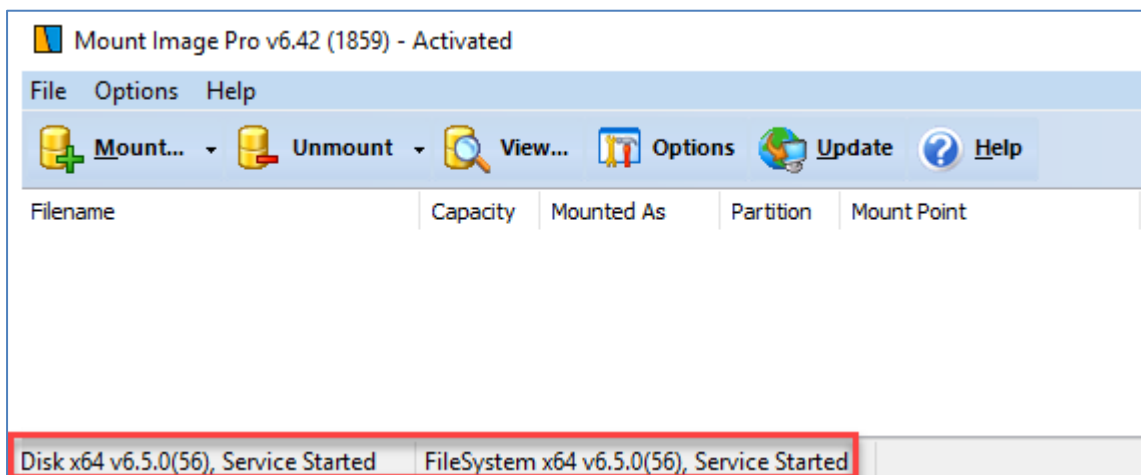
GetData's Mount Image Pro is used to mount a forensic image to make it accessible to Live Boot. A purchase of Forensic Explorer includes a license for Mount Image Pro on the same dongle.

The latest version of Mount Image Pro is available at:

- www.mountimage.com; or,
- <http://download.getdata.com/eMIP-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 419 below;

Figure 419: MIP driver status



28.2.3 VIRTUALIZATION SOFTWARE

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

VIRTUAL BOX (RECCOMENDED)

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.

VMWARE

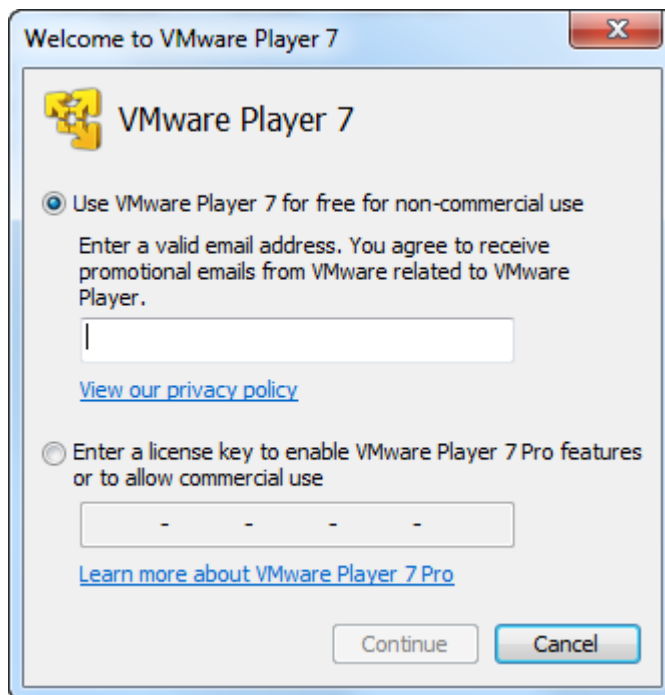
The following VMWare applications are supported:

- **VMWare workstation** (commercial)
<http://www.vmware.com/products/workstation/>; or,
- **VMWare Player** (free for non-commercial use)
https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/7_0%7CP LAYER-714%7Cproduct_downloads

IMPORTANT: Adding additional drives requires VMWare Workstation and will **not work with VMWare Player**. See Figure 420 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 420 below, before running Live Boot:

Figure 420: VMWare Player Terms



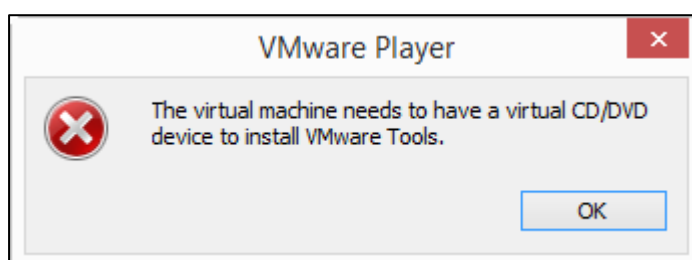
- **VMWare Player Plus** (Commercial)
<http://www.vmware.com/products/player/>.

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. If you receive the following VMware error message:

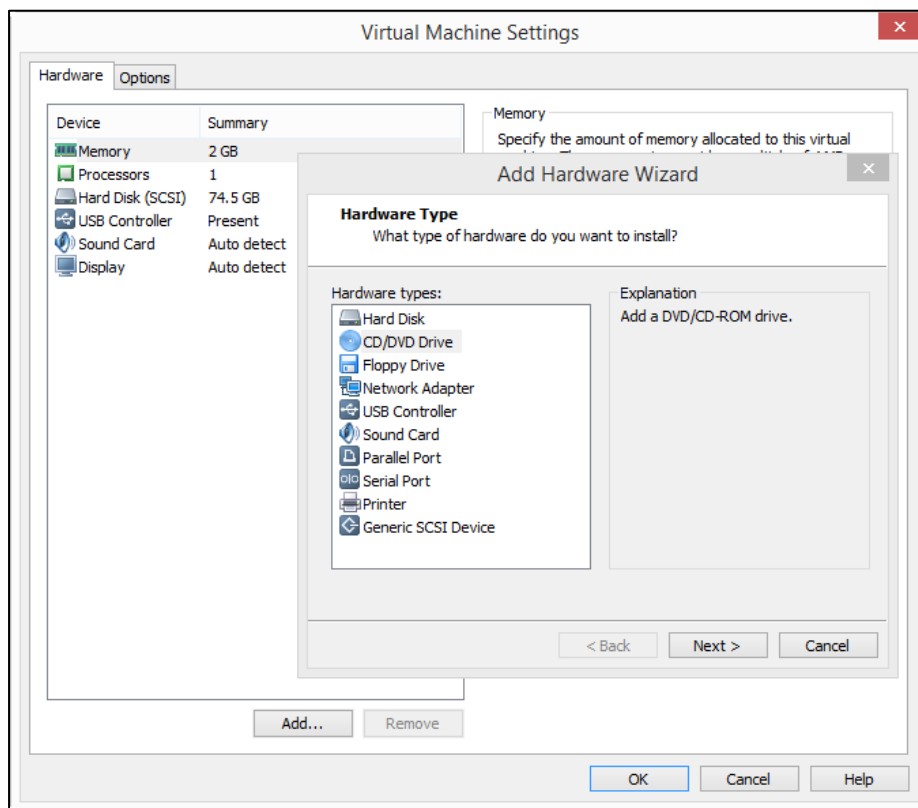
Figure 421: VMWare Tools virtual CD/DVD error



To **enable** the **virtual CD/DVD**:

1. Shut down Windows virtual machine inside the VMWare window;
2. In VMWare window, select the required VMWare session, right click, and select **settings**. The Virtual Machine Settings window will open.
3. Click **Add** to add a virtual device and select **CD/DVD Drive** from the Hardware Type menu:

Figure 422: Virtual Machine Settings



- 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 & <https://docs.vmware.com/en/VMware-Workstation-Pro/15.0/com.vmware.ws.using.doc/GUID-AACE0935-4B43-43BA-A935-FC71ABA17803.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, 11 (including GPT partitioned drives);

- Windows Server 2012;
- Linux.
- Macintosh HFS (VirtualBox must be used as the virtualization software).

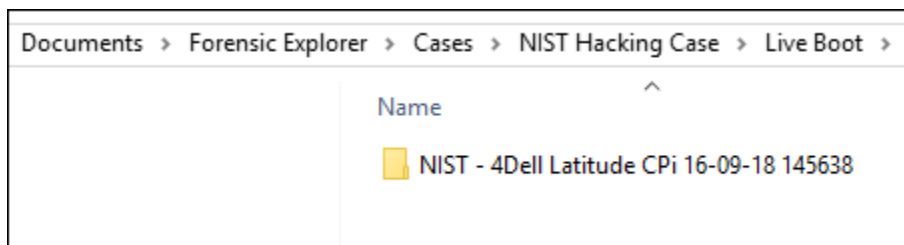
28.4 LIVE BOOT WORKING FOLDER

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 423: 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 LIVE BOOT ON WINDOWS 11 FORENSIC WORKSTATIONS

Changes by Microsoft between Windows 10 and 11 means that there are additional configuration steps required to optimize Live Boot when running a Windows 11 forensic workstation. The following configuration steps are suggested, particularly when attempting to Live Boot to boot **MAC** devices.

1. Turn off Windows Features:

- Virtual Machine Platform.
- Windows Hypervisor Platform.

Figure 424: Windows Features.

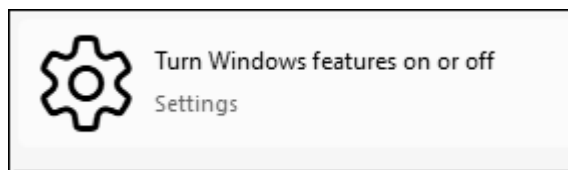
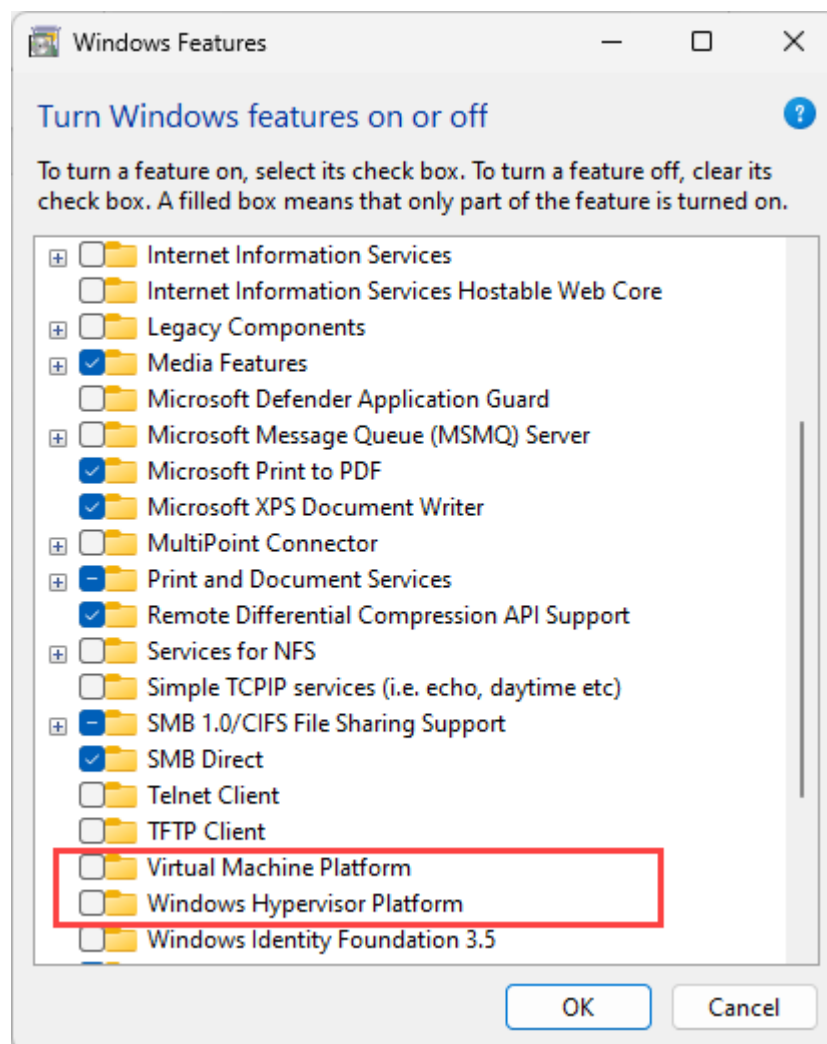


Figure 425: Windows Features.



2. Turn off Core isolation.

Figure 426: Windows Core isolation.

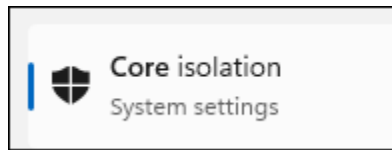
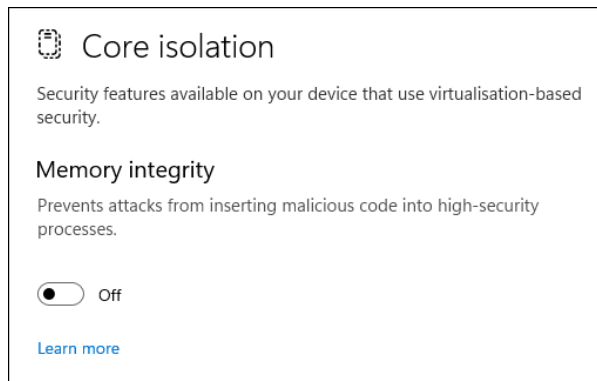


Figure 427: Core Isolation.

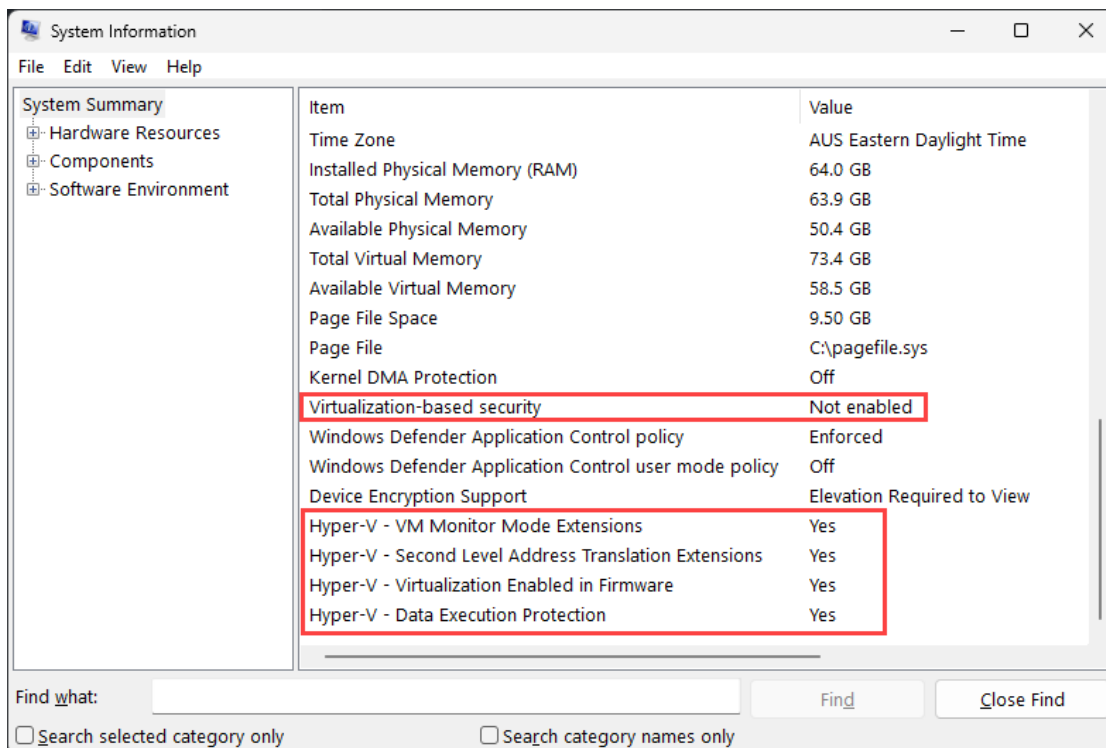


3. Disable Hyper-V in boot configuration using the BCDEdit tool. From an elevated command prompt type:

- **Bcdedit /set hypervisorlaunchtype off**

An optimized Windows 11 forensic workstation will have the following settings in the **System Information** window:

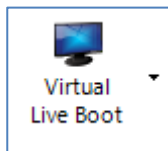
Figure 428: Windows 11 Live Boot optimization.



28.6 HOW TO LIVE BOOT A FORENSIC IMAGE

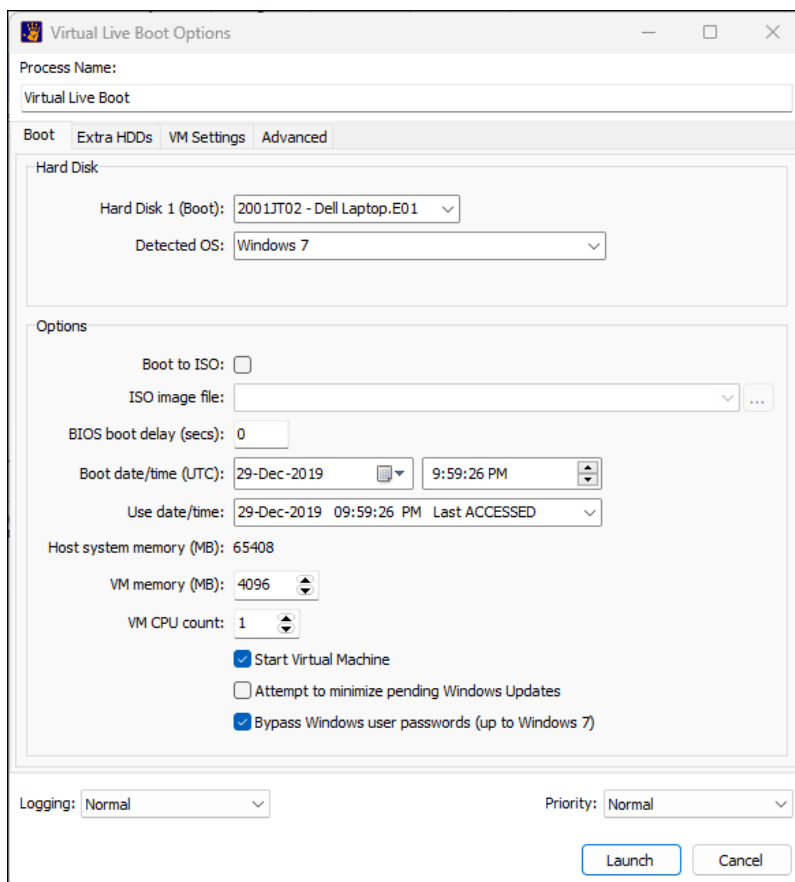
The following steps describe how to use Live Boot to boot a forensic image. In this example an E01 file from the 'NIST Hacking Case' is used (http://www.cfreds.nist.gov/Hacking_Case.html). The image is booted using **Virtual Box** as the virtualization software.

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 Virtual Live Boot button in the toolbar:



The Live Boot Options window will display:

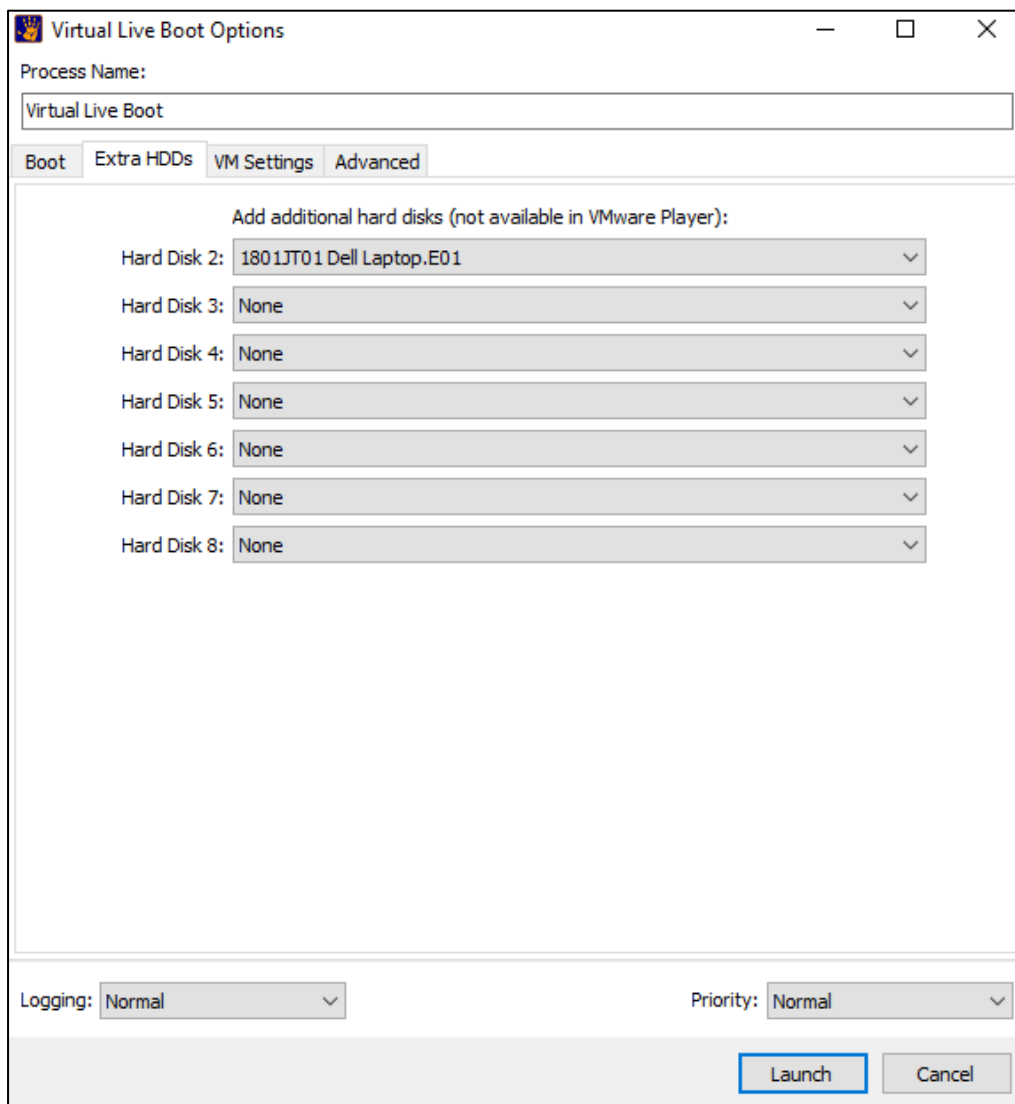
Figure 429: Live Boot Options



Hard Disk 1:	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 settings to adjust to a custom date time or use the drop-down menu below.
Use Date/Time:	Select the: <ul style="list-style-type: none">• 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;
Host system memory (MB):	The amount of RAM on the VM host.
VM 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).
VM CPU count:	The CPUs per virtual machine. Windows 11 computers require a minimum of 2.
Start Virtual Machine:	Launches the virtual machine automatically.
Bypass Windows user Passwords:	This option will blank Windows user passwords. See password cracking below. To bypass Windows 10 passwords, see 28.7 below.
Attempt to 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:

Figure 430: Add additional hard drives to a Live Boot



Add additional hard disks:

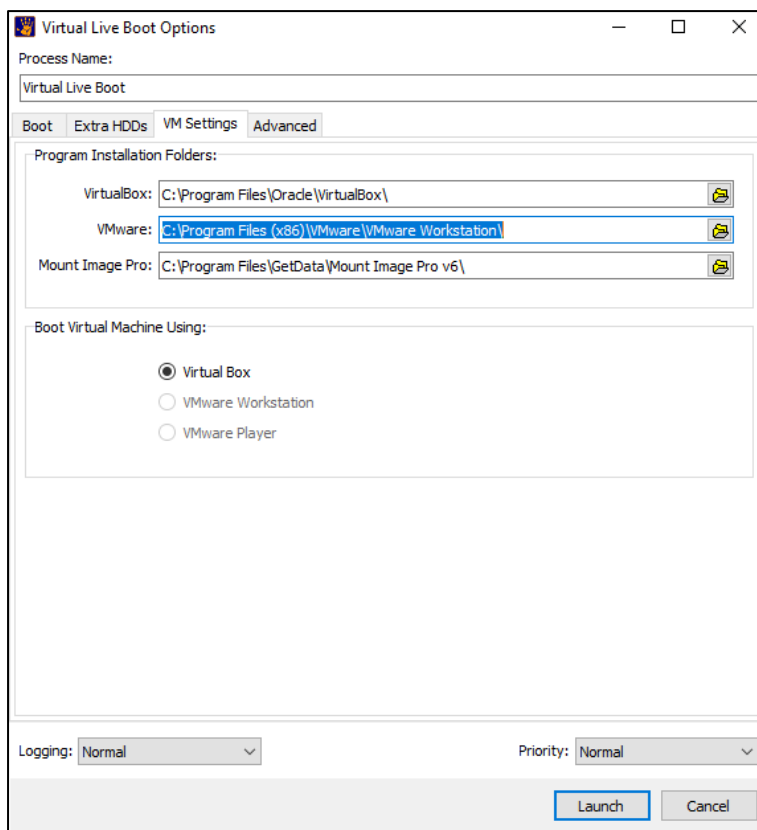
If the suspects computer had additional disks, then these disks can be added to the virtual machine.

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.

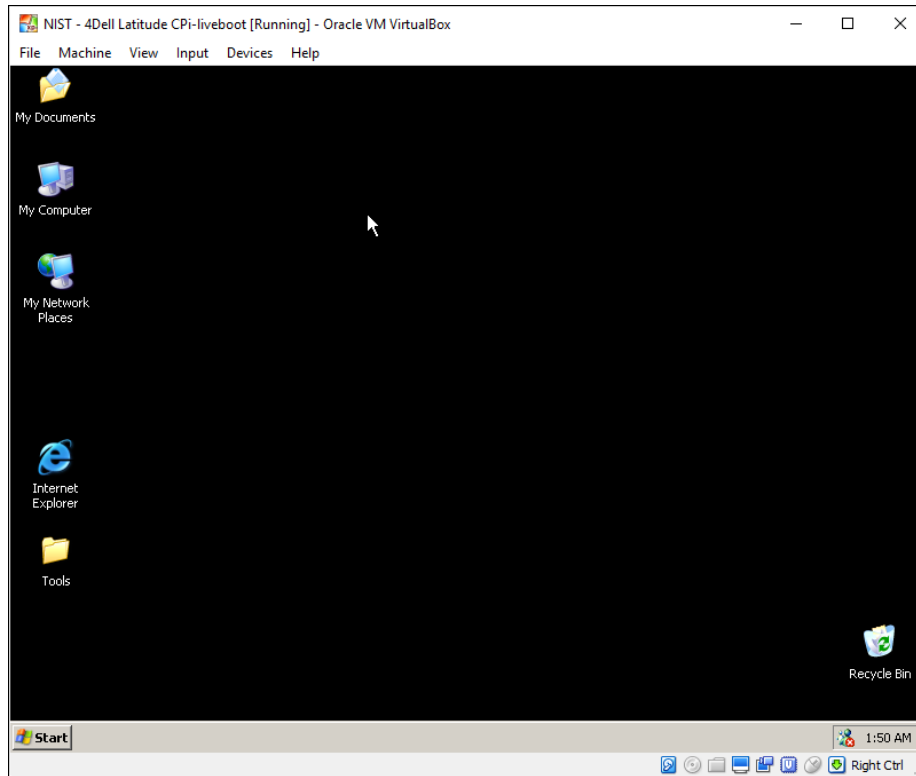
- d. Switch from the Boot Options tab to the **VM Settings** tab:

Figure 431: Live Boot Options



- 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 432 below:

Figure 432, Live Boot using Virtual Box



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).

28.7 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.

28.7.1 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.

WINDOWS NTLM HASHES

An NTLM hash is the cryptographic format in which user passwords are stored on Windows systems. To break an NTLM hash, various programs can be used, such as Ophcrack, John the Ripper, and Hashcat. These programs are capable of performing dictionary attacks, brute-force attacks, and other techniques to crack the hashes and reveal passwords.

NTLM hashes can be extracted in Forensic Explorer using: **File System > Analysis Programs > NTLM Hash Extract**:

- This script requires the ImDisk ramdisk to be installed (ImDisk installation files is located in: C:\Program Files\GetData\Forensic Explorer v5\3rd_Party_Tools\ImDisk\imdiskinst.exe).
- The script executes the GetData's **ntlm_hash.exe** located in the Forensic Explorer installation folder.

Figure 433: File System > Analysis Programs > GetData NTLM Hash Extract.

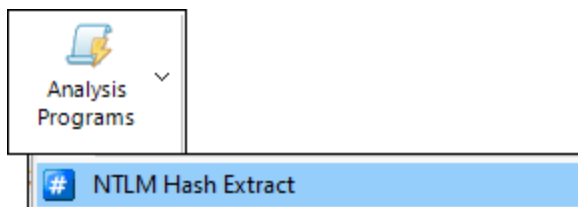
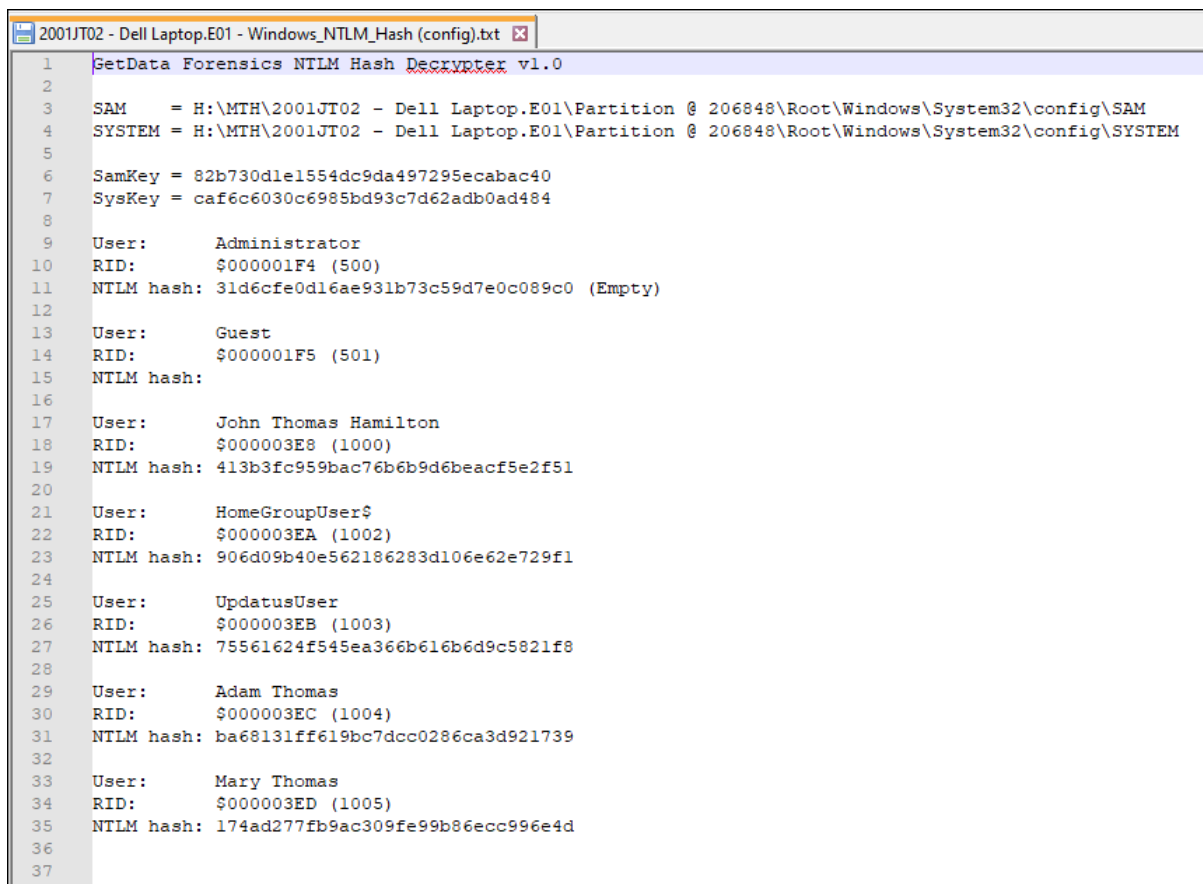


Figure 434: Figure 425: GetData NTLM Hash Extract output.



```

1  GetData Forensics NTLM Hash Decrypter v1.0
2
3  SAM    = H:\MTH\2001JT02 - Dell Laptop.E01\Partition @ 206848\Root\Windows\System32\config\SAM
4  SYSTEM = H:\MTH\2001JT02 - Dell Laptop.E01\Partition @ 206848\Root\Windows\System32\config\SYSTEM
5
6  SamKey = 82b730d1e1554dc9da497295ecabac40
7  SysKey = caf6c6030c6985bd93c7d62adb0ad484
8
9  User:      Administrator
10 RID:       $000001F4 (500)
11 NTLM hash: 31d6cfe0d16ae931b73c59d7e0c089c0 (Empty)
12
13 User:      Guest
14 RID:       $000001F5 (501)
15 NTLM hash:
16
17 User:      John Thomas Hamilton
18 RID:       $000003E8 (1000)
19 NTLM hash: 413b3fc959bac76b6b9d6beacf5e2f51
20
21 User:      HomeGroupUser$
22 RID:       $000003EA (1002)
23 NTLM hash: 906d09b40e562186283d106e62e729f1
24
25 User:      UpdatusUser
26 RID:       $000003EB (1003)
27 NTLM hash: 75561624f545ea366b616b6d9c5821f8
28
29 User:      Adam Thomas
30 RID:       $000003EC (1004)
31 NTLM hash: ba68131ff619bc7dcc0286ca3d921739
32
33 User:      Mary Thomas
34 RID:       $000003ED (1005)
35 NTLM hash: 174ad277fb9ac309fe99b86ecc996e4d
36
37

```

THIRD PARTY PASSWORD RECOVERY TOOLS - OPHCRACK

Ophcrack is a free open-source program that recovers Windows passwords by processing NTLM 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.

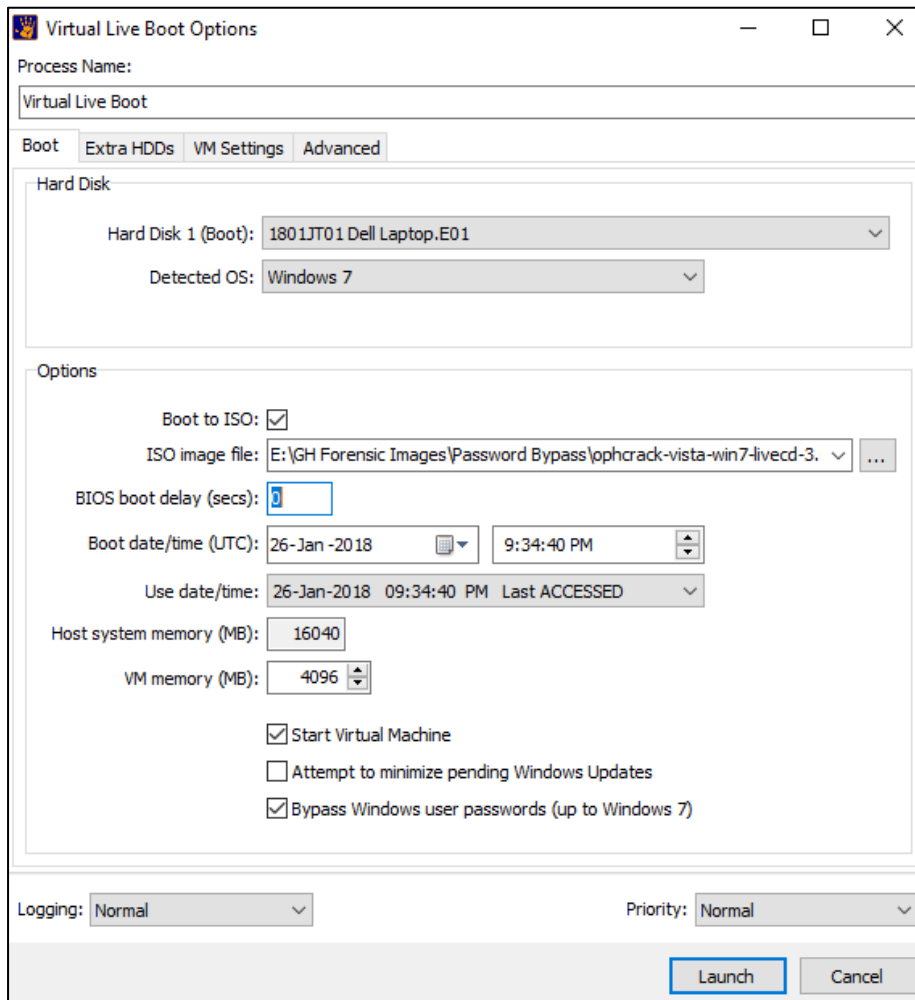
Ophcrack ISO image files are available for download from <http://Ophcrack.sourceforge.net/download.php>. These include:

- 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:

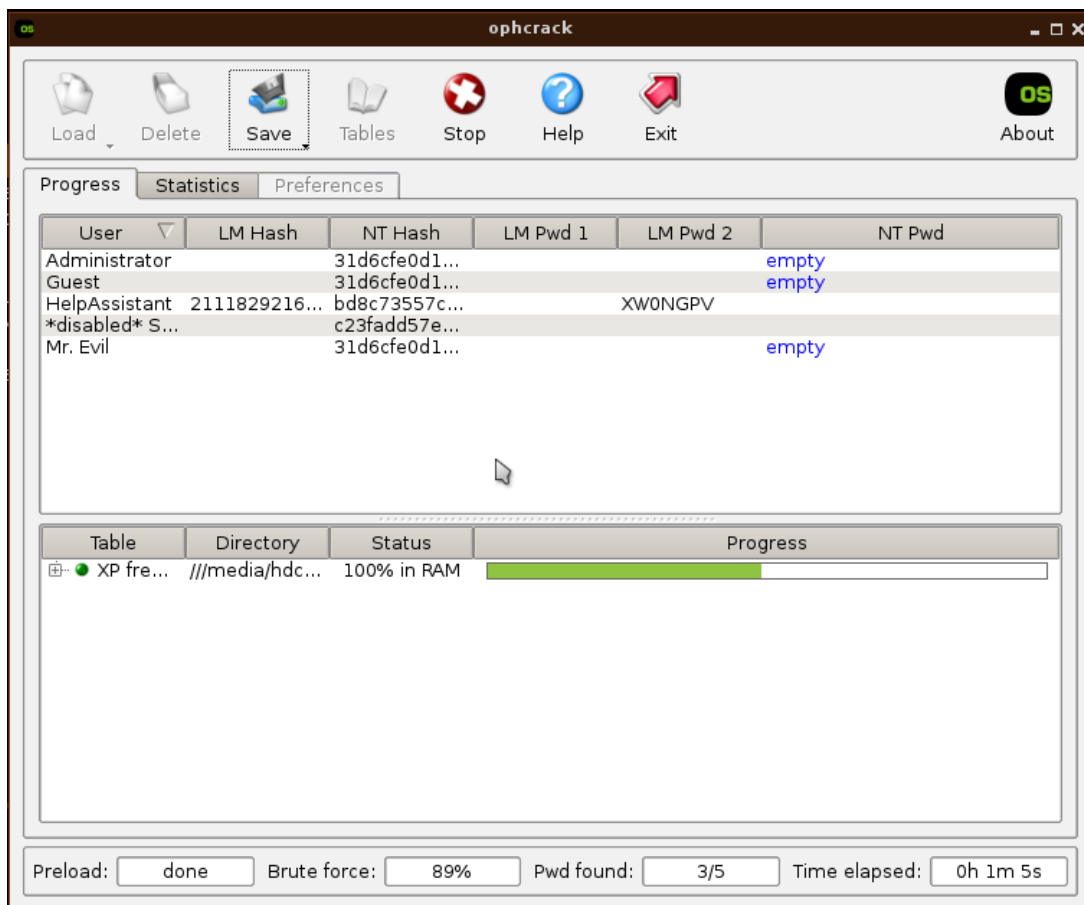
- Follow the instructions provided above to mount the image file and run Live Boot.
- In the Boot Options tab, check 'Boot to ISO' and select the relevant Ophcrack ISO image, as shown in Figure 435 below:

Figure 435: Live Boot ISO



- 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 436 below:

Figure 436: Ophcrack Password Breaking



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/> 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.

28.7.2 WINDOWS USER PASSWORD BYPASS

FORENSIC EXPLORER PASSWORD BY-PASS

Check the **Bypass Windows 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

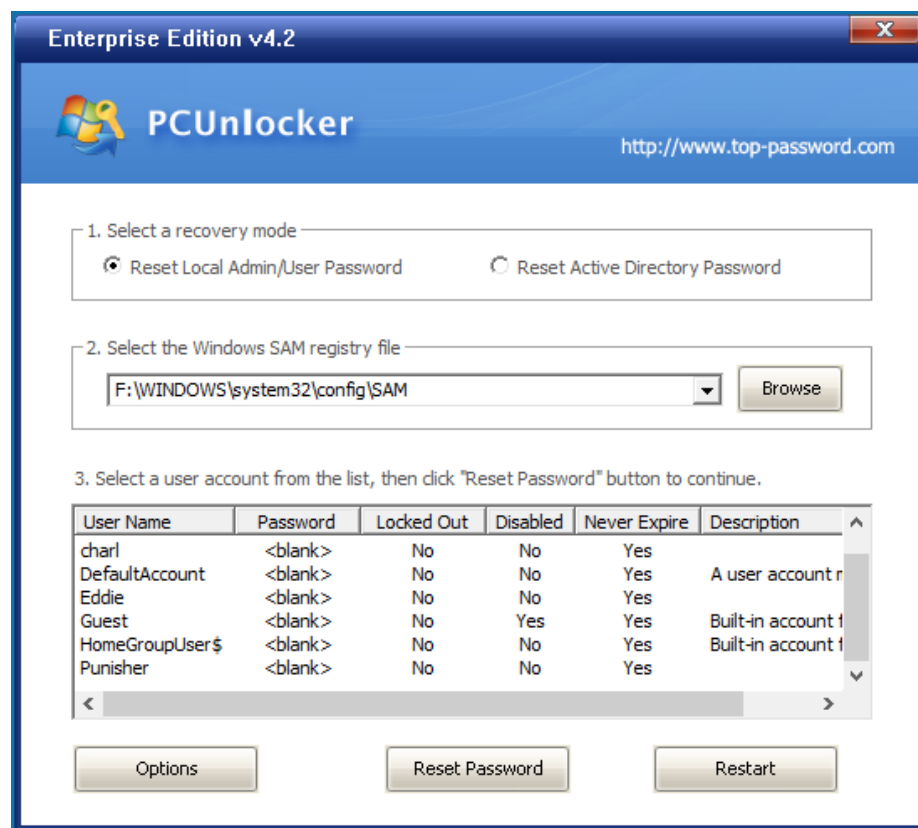
PCUnlocker from <http://www.top-password.com/reset-windows-password.html> is a recommended third party application for Windows user account by-pass (Learn more about PCUnlocker here: <http://www.top-password.com/guide/reset-windows-password.html>)

GetData has partnered with top-password.com to provide licensing solutions. Please contact support@getdata.com for more information.

PCUNLOCKER - MBR (TRADITIONAL BIOS MODE) USING VIRTUALBOX

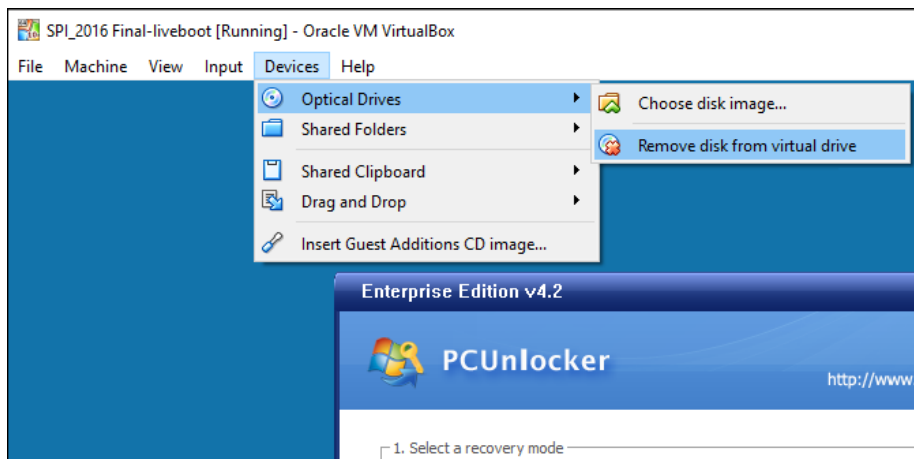
1. In Forensic Explorer click the Live Boot button in the File System module to launch the Live Boot window.
2. In the Forensic Explorer Live Boot window check **Boot to ISO** and enter the path to the **pcunlocker.iso** file (31,370kb, MD5 6DDF065CF9B65F265E4654025FB00C58).
3. Click OK to boot and the Virtual Machine will launch PCUnlocker:

Figure 437: PCUnlocker Windows's password bypass



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 Virtual Box this is done by selecting **Devices > Optical Drives > Remove disk from virtual drive**, as shown in Figure 438 below (**Hint:** To unlock the mouse from the VirtualBox window, press the right CTRL key).

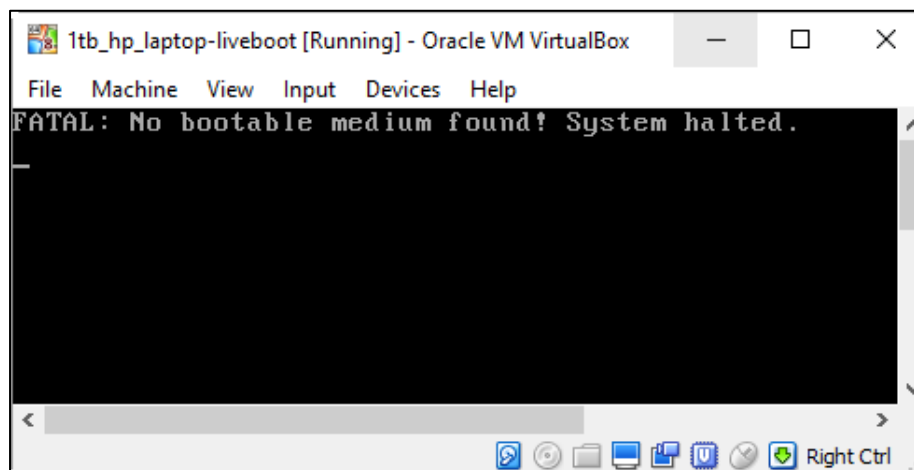
Figure 438: Ejecting a virtual CD (ISO image) in VirtualBox.



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 439: PC Unlocker – “Non-bootable medium found! System halted.”



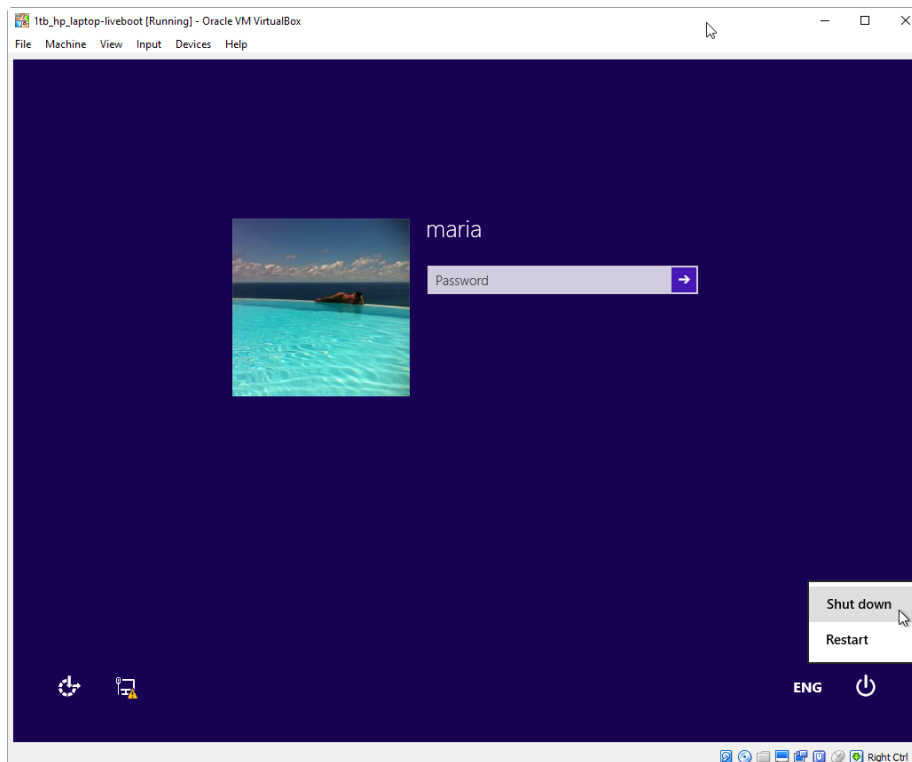
PCUNLOCKER - EFI SYSTEM PARTITION USING VIRTUALBOX

*“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”.*

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 440 below (Windows must be shutdown correctly to obtain access to system boot settings in VirtualBox):

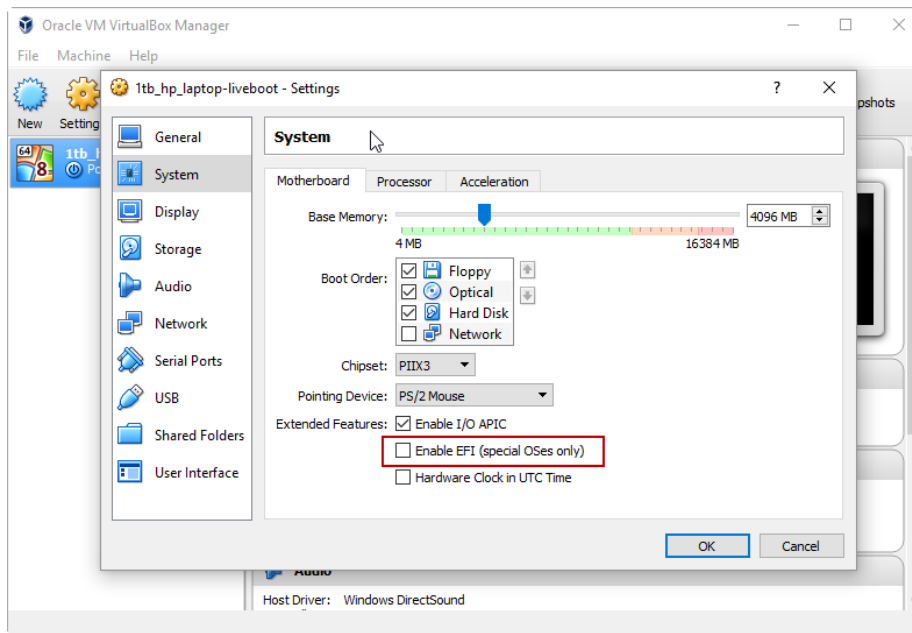
Figure 440: Windows Shutdown in VirtualBox



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 441 below. **Uncheck the Enable EFI (special OSeS only) box**:

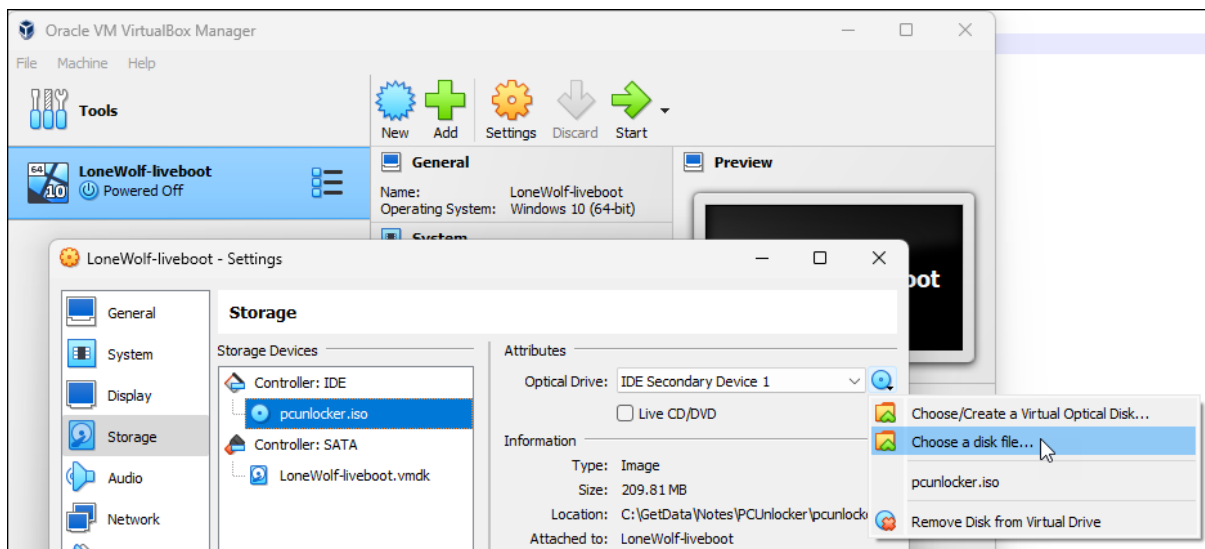
Figure 441: VirtualBox System Settings - Disable EFI



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, select Settings > Storage > click on the **Optical Drive** and select the **pcunlocker.iso** file, as shown in Figure 442 below:

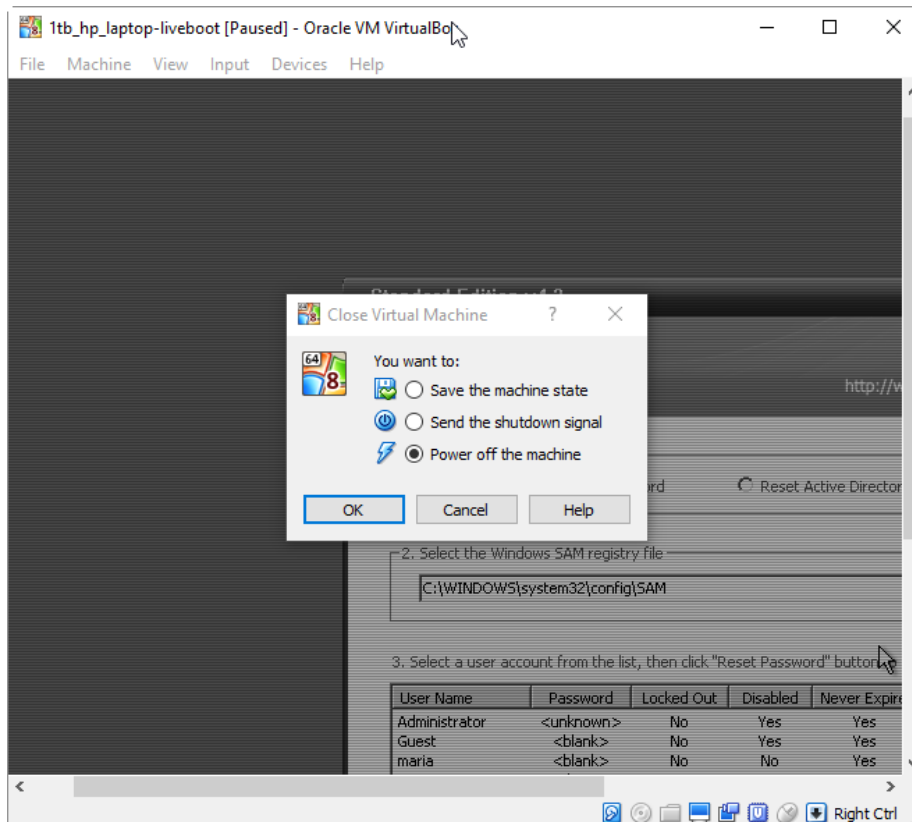
Figure 442: Select the PCUnlocker ISO from the VirtualBox settings window.



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 438 above).

6. Power off the machine by selecting the **X** button in the top right corner of VirtualBox and select **Power off the machine**.

Figure 443: Power off virtual machine in VirtualBox



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 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 computer (no longer accessible) 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 a known or blank local password).

Forensic Explorer users have also reported success with Forensit's User Profile Wizard 3.16 <https://www.forensit.com/downloads.html> in converting a domain account to a local account.

28.7.3 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 versions of the MAC OS. In this example we use the following commands:

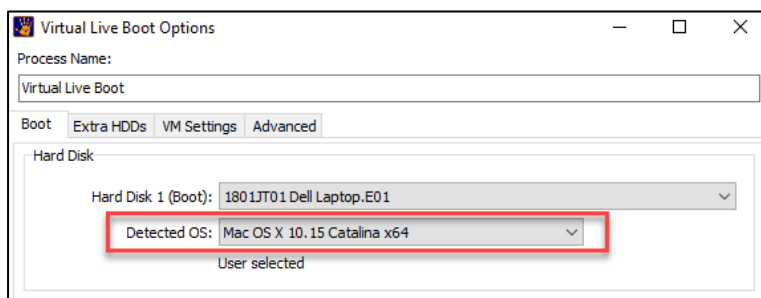
```
mount -uv /  
rm /var/db/.AppleSetupDone
```

By deleting the .AppleSetupDone file the next boot will mimic the first install and prompt for the setup of an Administrator account. All system files, apps, personal data, etc., for any existing user accounts remain intact.

To by-pass a MAC user login using Single-User mode:

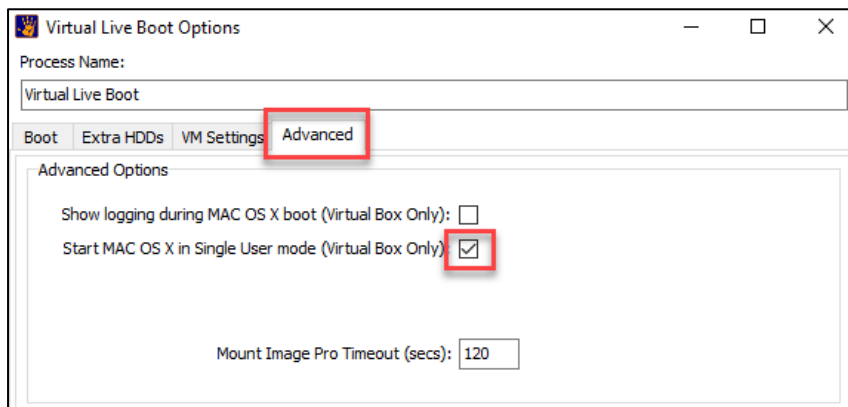
1. This procedure works only with Forensic Explorer Version 4 and above. Ensure that Forensic Explorer v4 or above is installed.
2. Start a new case, add the forensic image (ensure that it is a bootable image that contains a Master Boot Record).
3. Click on the Live Boot button in the Forensic Explorer File System module toolbar to open the **Live Boot Options** window. The **Detect OS** should identify the type of MAC OS:

Figure 444: Live Boot Options window showing detected MAC OS



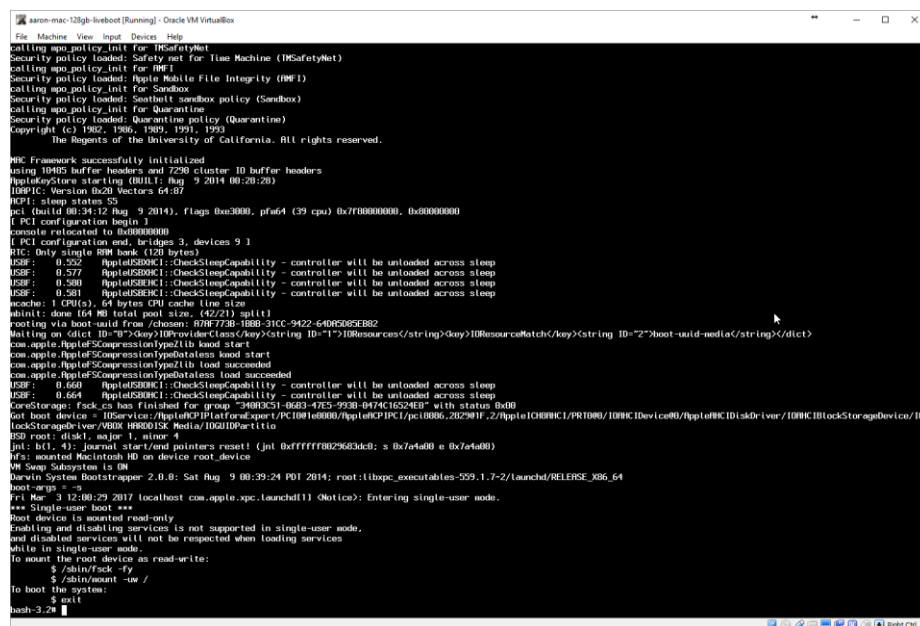
- Click on the **Advanced** tab. Place a tick in the checkbox for **Start MAC OS X in Single User mode (Virtual Box Only)**:

Figure 445: Live Boot Options window Advanced tab



- Click **Launch** to launch the virtual machine. The virtual machine will boot the Single-User mode command interface:

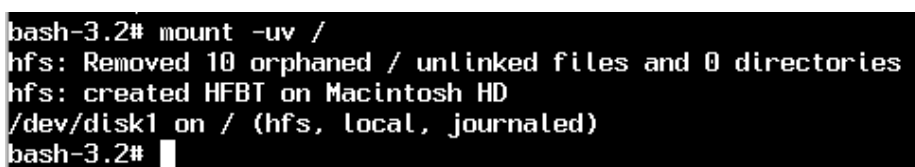
Figure 446: Launch of VirtualBox virtual machine in MAC Single-User mode.



- 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.

Figure 447: Entering UNIX commands in MAC Single-User mode



7. At the command prompt, issue the command: `rm /var/db/.AppleSetupDone`

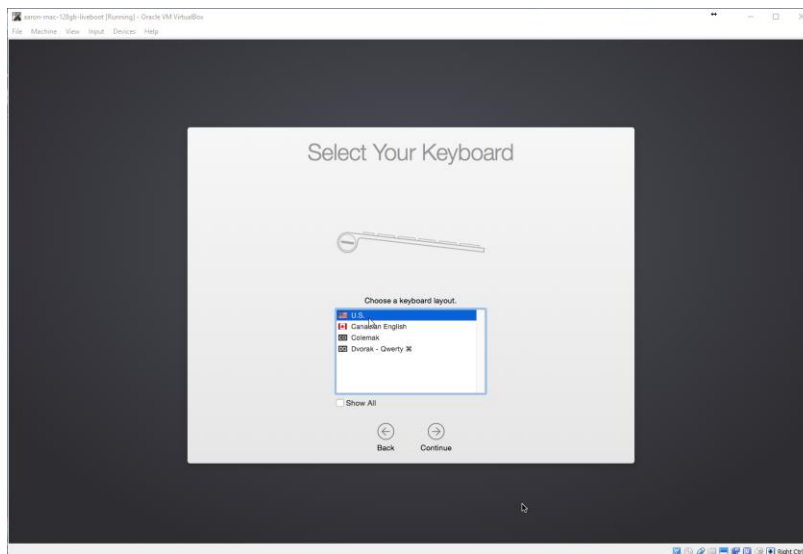
IMPORTANT: Manually type the above command (there may be invalid characters if copy and paste is used). There is NO SPACE between the forward slash and the period.

Figure 448: Entering UNIX commands in MAC Single-User mode.

```
bash-3.2# rm /var/db/.AppleSetupDone
bash-3.2#
```

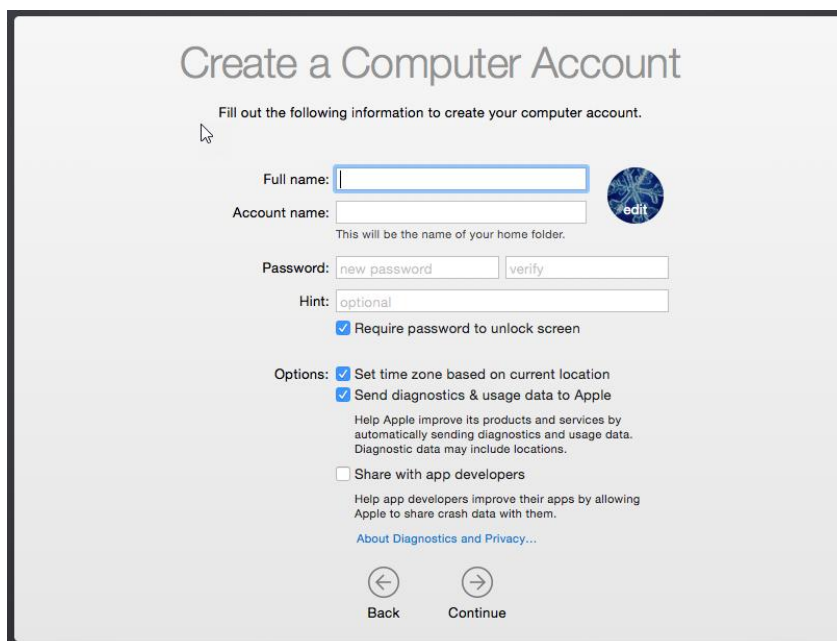
8. At the command prompt, type `exit` (to boot the virtual machine). During the startup process you will be prompted by several setup screens:

Figure 449: MAC setup



9. At the **Create a Computer Account** screen, enter your details for a new administrator account:

Figure 450: Create MAC administrator user account.



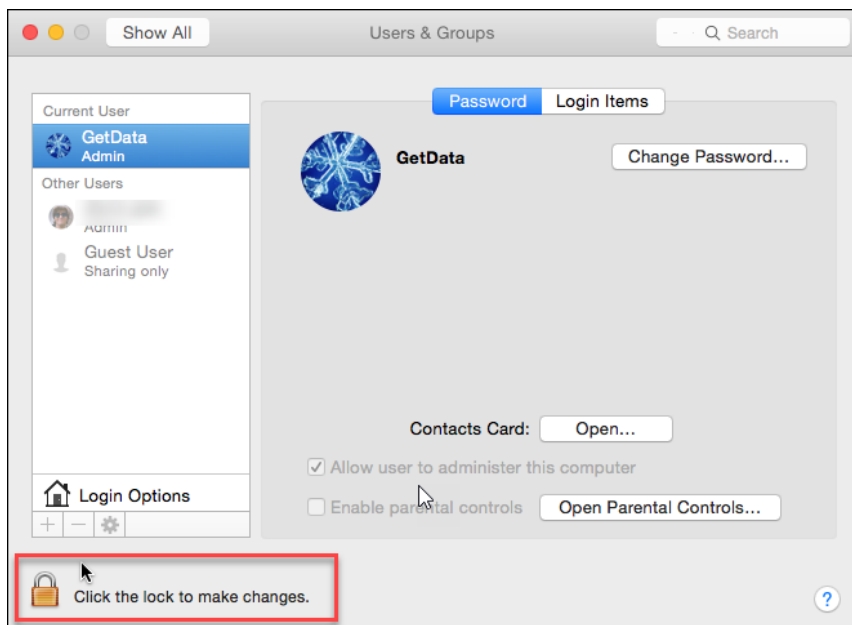
10. Click through the setup screens to reach the MAC desktop. Once at the desktop click on the **settings button** and then **Users & Groups**:

Figure 451: MAC Settings button



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.

Figure 452: Edit user accounts in MAC Users & Groups



12. Log out of your administrator account and log back in via the target account.

THIRD PARTY SOFTWARE – KON-BOOT

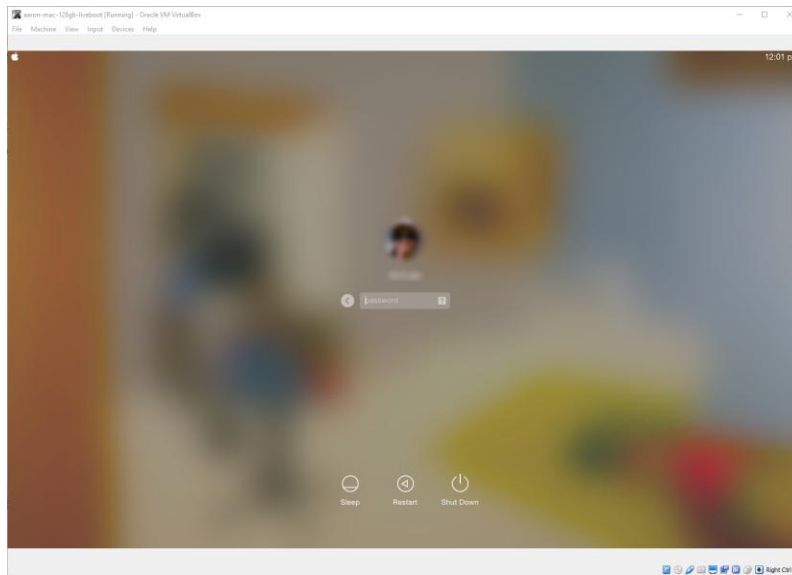
It is possible to bypass MAC user passwords with a third-party commercial tool called **Kon-Boot for Mac OSX** (<http://www.piotrbania.com/all/kon-boot/>). This version includes the ISO image: **Konboot.iso** (MD5 Hash: 6D148A57181429F42F161387FD7A31B8). The most successful methodology is to use this 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 **Power off the Machine**.

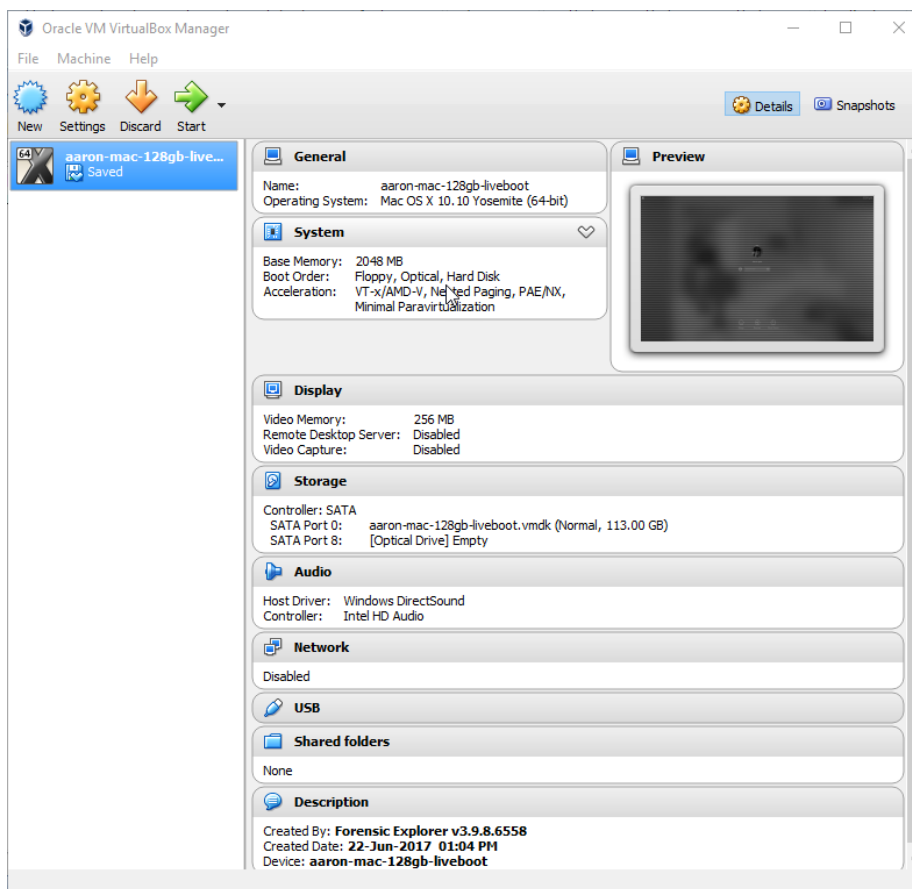
3. Close Forensic Explorer, it is no longer required.

Figure 453: MAC user login window



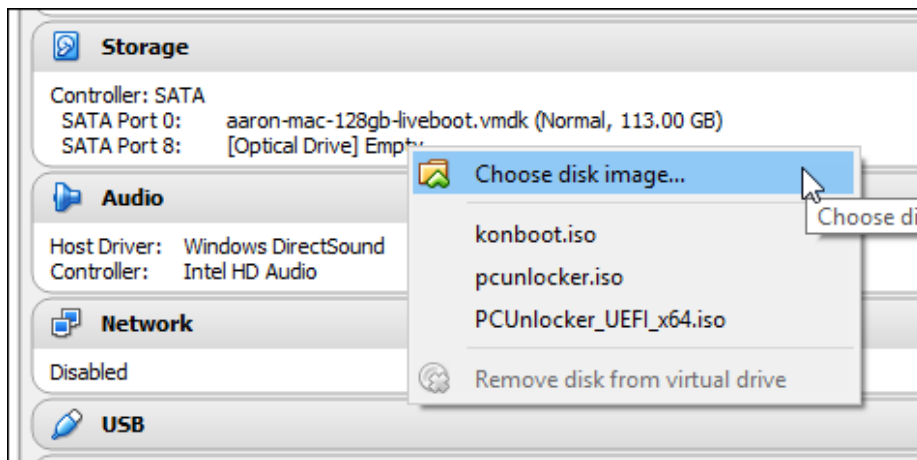
4. Launch VirtualBox from the desktop icon.
5. The last Live Boot session will show at the bottom of the list in the left-hand column:

Figure 454: VirtualBox GUI



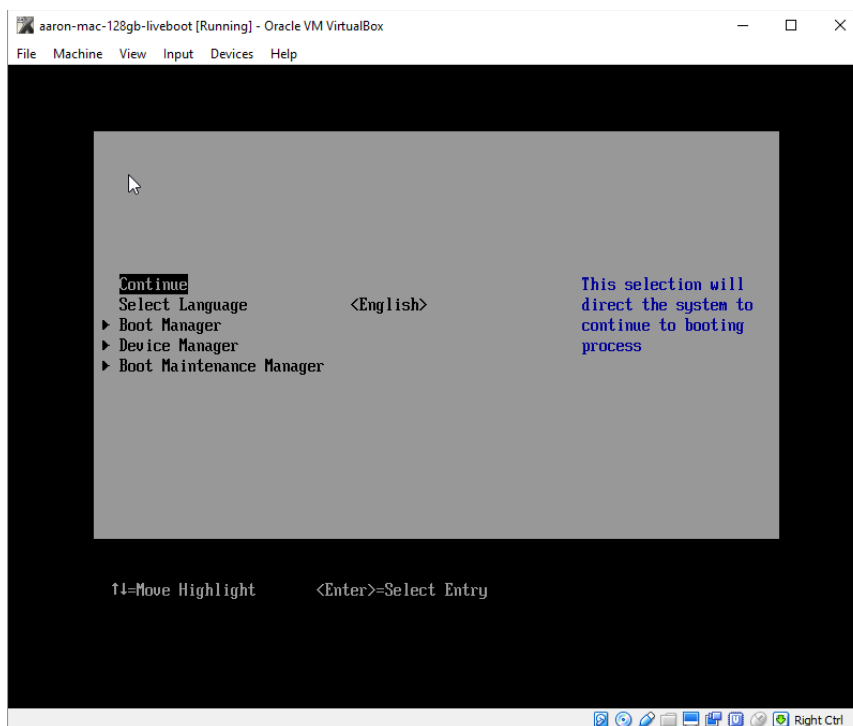
- In the VirtualBox Manger information window on the right-hand side, under **Storage**, look for **[Optical Drive] Empty**. Right click and select “Choose disk image...”:

Figure 455: VirtualBox Optical Drive



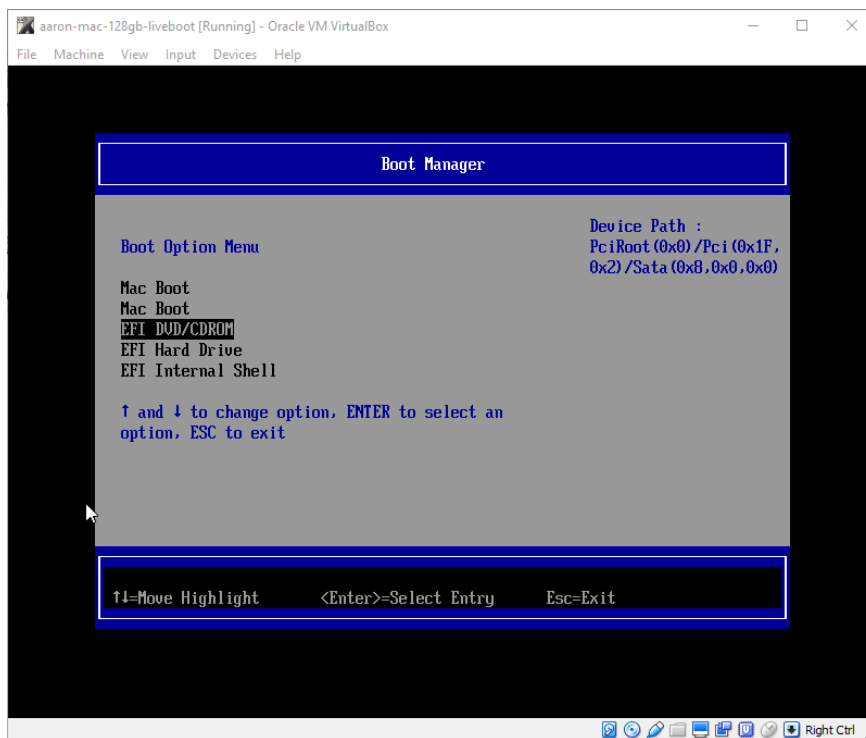
- Select the konboot.iso downloaded earlier.
- Launch the virtual machine (by pressing on the green start arrow in the VirtualBox manager toolbar) whilst pressing the **ESC** key to enter the virtual machine BIOS. TIP: When the virtual machine boot window first appears, click on it to ensure that it has focus and rapidly press the ESC key on your keyboard).
- Successful access to the virtual machine BIOS will provide the following menu:

Figure 456: MAC BIOS



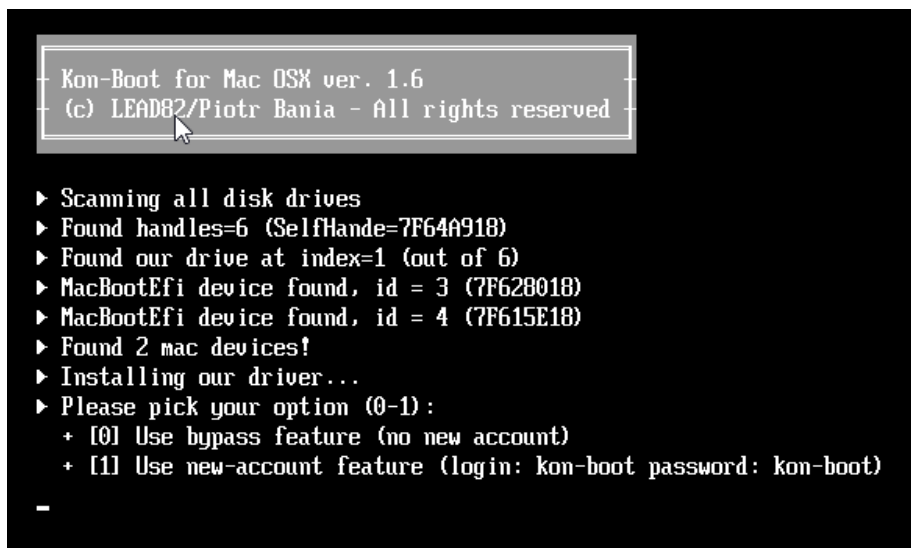
- Select the **Boot Manager** menu option and then select to boot using **EFI DVD/CDROM**:

Figure 457: MAC Boot Manager



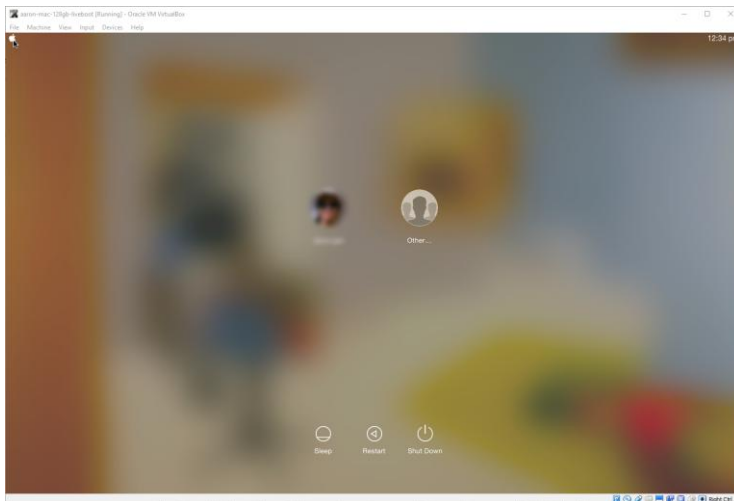
11. The Kon-Boot menu will appear. Use option [1] Use new-account feature (login: kon-boot password: kon-boot):

Figure 458: MAC Kon-Boot user menu



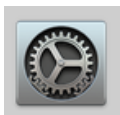
12. The MAC computer will then boot with a Kon-Boot user account displayed.

Figure 459: MAC Kon-Boot 'Other' user account



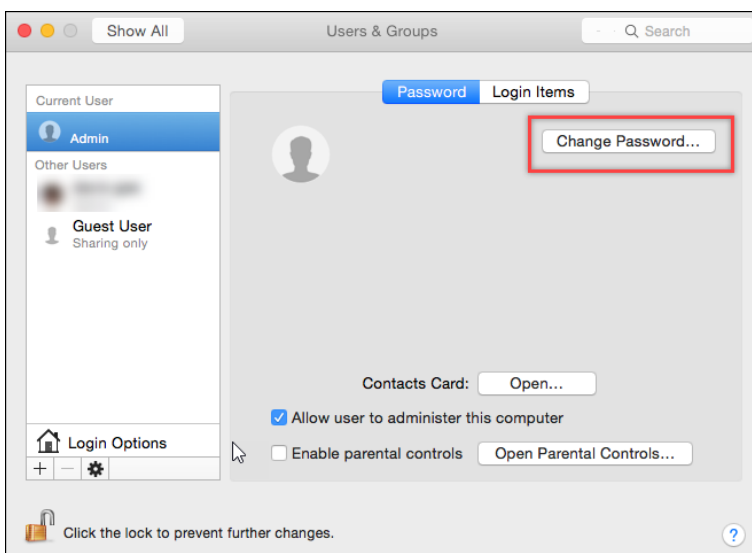
13. Login via the **Other** user account, using username **kon-boot**, password **kon-boot**. Once logged in, click on the MAC System Preference icon:

Figure 460: MAC System Preferences icon



14. In the **System Preferences** select the **Users & Groups** icon. Select on the required user account, and click the **Change Password** button to enter new password details:

Figure 461: MAC System Preferences, Users & Groups



15. Log out of the kon-boot user account and then into the target user account using the new password details.

28.7.4 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>.

28.8 TROUBLESHOOTING LIVE BOOT

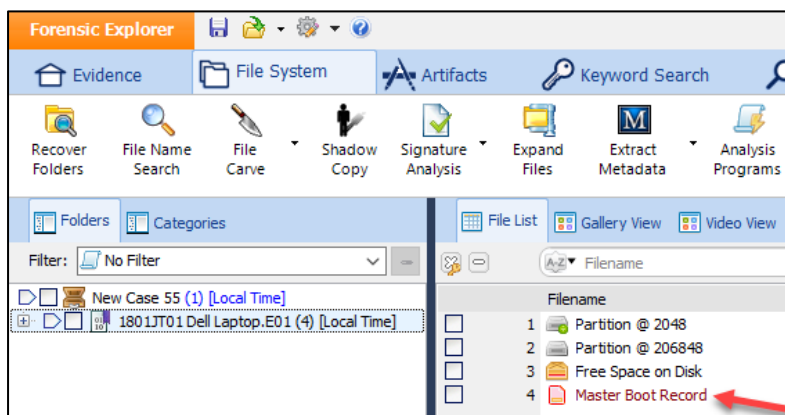
Following the checks below to troubleshoot Live Boot:

28.8.1 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 462 below:

Figure 462: Checking for a valid MBR.



28.8.2 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. 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**.

28.8.3 LIVE BOOT CONFIGURATION

Is VMWare Player or VMWare Workstation or Virtual Box installed?

- Check Live Boot Options (shown in Figure 431: 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);
 - **VMWorkstation:** C:\Program Files (x86)\VMware\VMware Workstation
 - **Virtual Box:** C:\Program Files\Oracle\VirtualBox\...

Is Mount Image Pro v6 installed? (Live Boot is **NOT** compatible with earlier versions);

- Check Live Boot Options (shown in Figure 431 above) to confirm the correct path to MIP:
 - C:\Program Files\GetData\Mount Image Pro vX\MIP.exe.

28.8.4 MOUNT IMAGE PRO CHECKS

Mount Image Pro Cache and Virtualization Files

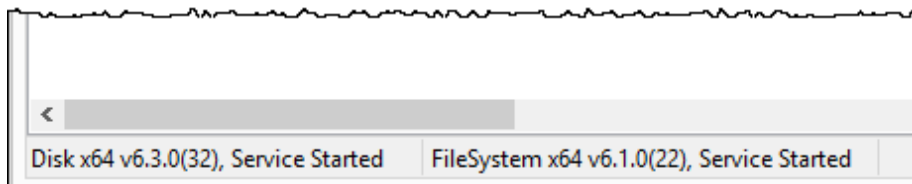
- Locate and delete the Live Boot working folder and then try again. The Live Boot working folder is in the following path:

[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 463 below:

Figure 463: 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.

28.8.5 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:

- http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003944
- <https://www.hardwaresecrets.com/everything-you-need-to-know-about-the-intel-virtualization-technology/>

28.8.6 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, accessed 18 March 2015).

KEYBOARD ISSUES

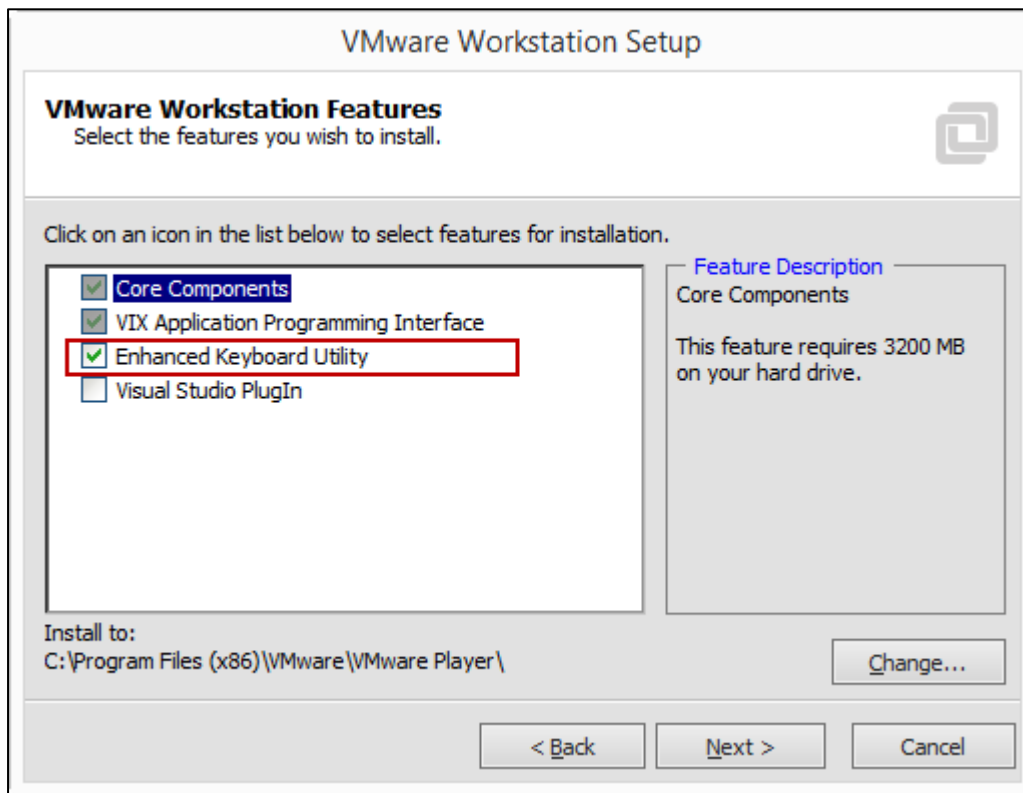
VMWare keyboard communication issues can include:

- 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.

Figure 464: VMWare Workstation Enhanced Keyboard Utility



28.8.7 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.

28.8.8 CONTACT TECHNICAL SUPPORT

Contact technical support (see Appendix 1 - Technical Support) with the supporting information from the above checks.

28.9 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).

28.9.1 METHOD 1 (AUTOMATED USING A SCRIPT)

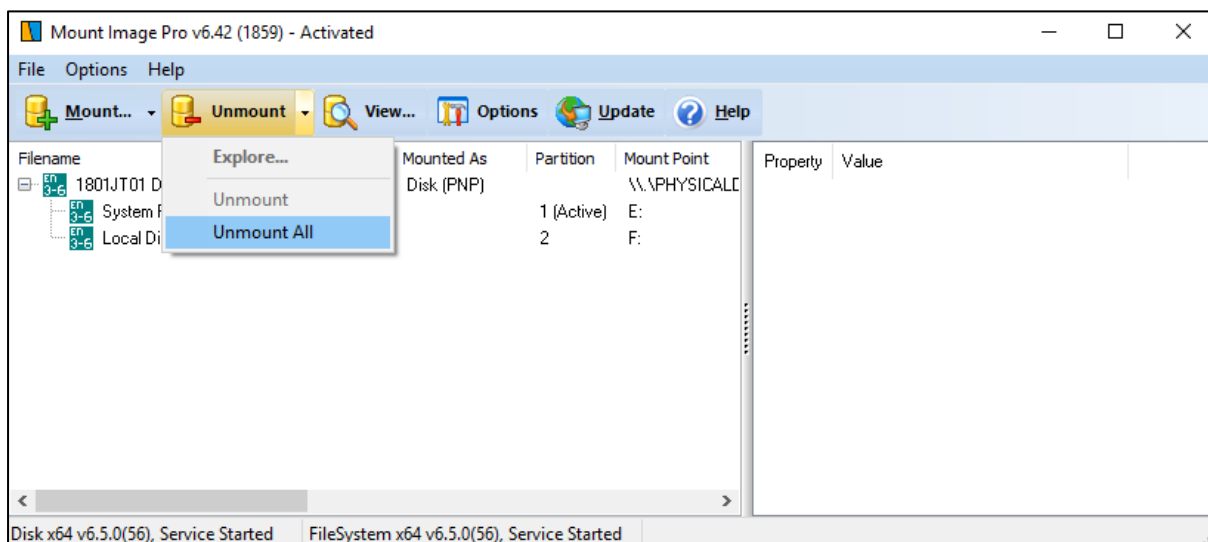
Method 1 requires **Mount Image Pro** to be installed on the **Examination Computer**.

ON THE FORENSIC WORKSTATION

On the Forensic Workstation:

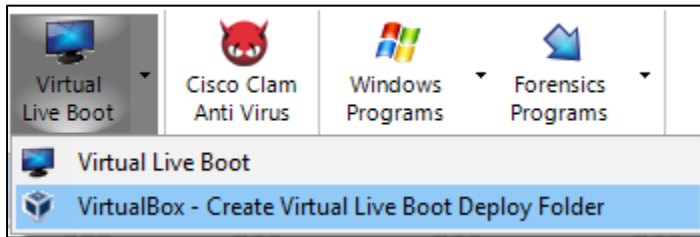
1. Follow the instructions in **Chapter 28 to Live Boot the forensic image**. Ensure to bypass Windows login information and make any other changes needed to the running virtual machine.
2. Once booted, **power off the virtual machine** and **close Virtual Box**.
3. Open the **Mount Image Pro GUI**, click on **the Unmount button** and **Unmount All images**:

Figure 465: Mount Image Pro - Unmount All



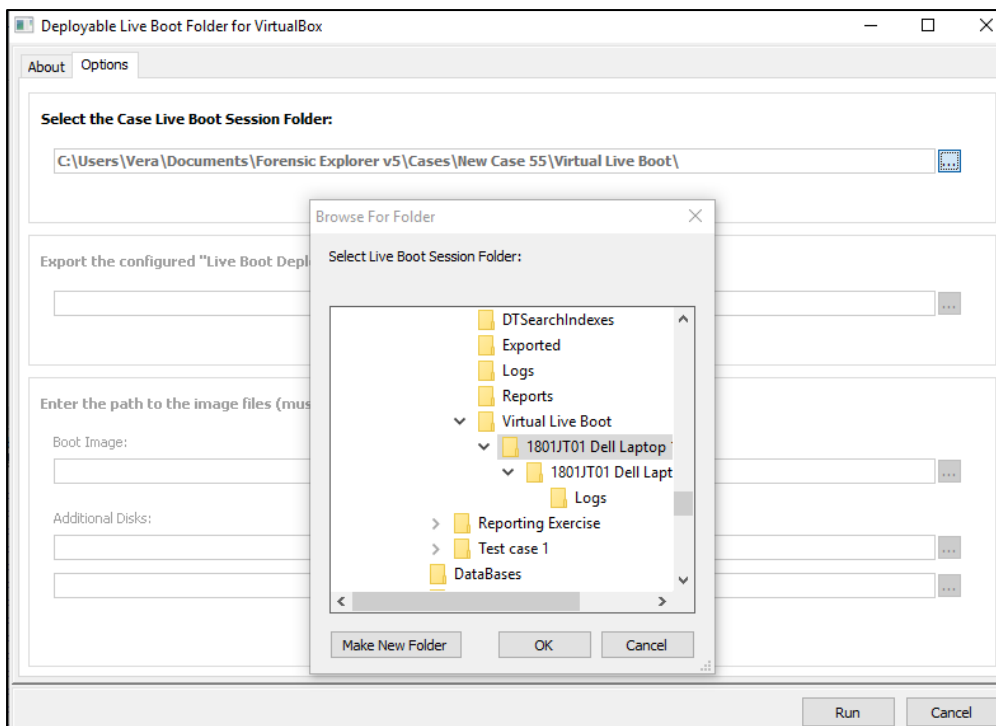
The Mount Image Pro GUI should now be empty of image files.


- 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**):



- The following input form will open:

Figure 466: Deployable Live Boot Folder for VirtualBox - Selecting the Live Boot Session folder.



- Select the Case Live Boot Session folder by clicking on the  folder search button, navigating to the **\Documents\Forensic Explorer vX\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).
- The 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.
- 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.

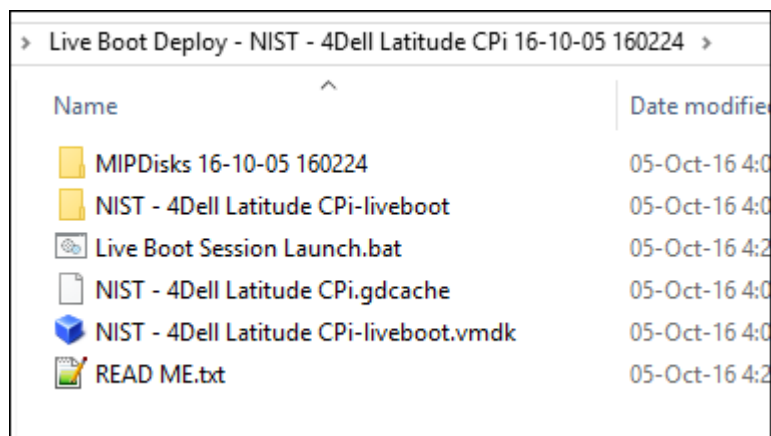
IMPORTANT: When the Live Boot Session folder is deployed to an Examination Computer the folder must have access to the required forensic images in these paths.

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 467: Configured Live Boot Session folder

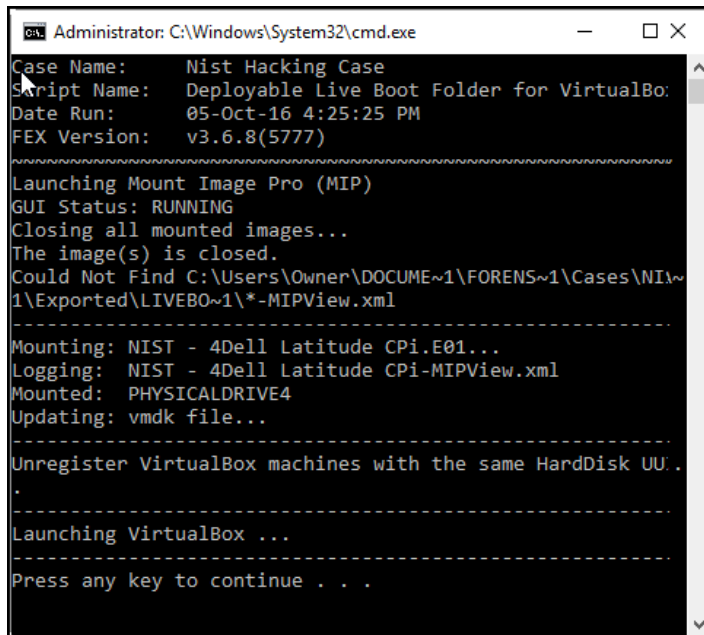


READ ME.txt contains information about the Live Boot session, including the path to the required forensic image files.

Live Boot Session Launch.bat is the Windows batch file that is used to launch the Live Boot session.

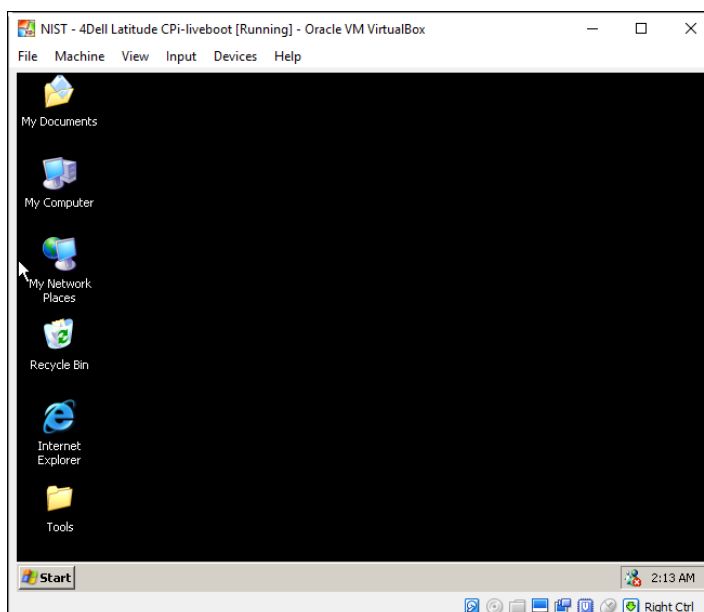
ON THE EXAMINATION COMPUTER

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 by running the **Live Boot Session Launch.bat** file. A CMD window will open to configure and launch VirtualBox:

Figure 468: Launching a VirtualBox Live Boot deploy.

```
Administrator: C:\Windows\System32\cmd.exe
Case Name:      Nist Hacking Case
Script Name:    Deployable Live Boot Folder for VirtualBo
Date Run:      05-Oct-16 4:25:25 PM
FEX Version:    v3.6.8(5777)
~~~~~
Launching Mount Image Pro (MIP)
GUI Status: RUNNING
Closing all mounted images...
The image(s) is closed.
Could Not Find C:\Users\Owner\DOCUME~1\FORENS~1\Cases\WI~
1\Exported\LIVEBO~1\*-MIPView.xml
-----
Mounting: NIST - 4Dell Latitude CPi.E01...
Logging: NIST - 4Dell Latitude CPi-MIPView.xml
Mounted: PHYSICALDRIVE4
Updating: vmdk file...
-----
Unregister VirtualBox machines with the same HardDisk UU.
.
-----
Launching VirtualBox ...
-----
Press any key to continue . . .
```

VirtualBox will then launch the session:

Figure 469: Deployed VirtualBox Live Boot Session Launch

28.9.2 METHOD 1 (MANUAL METHOD)

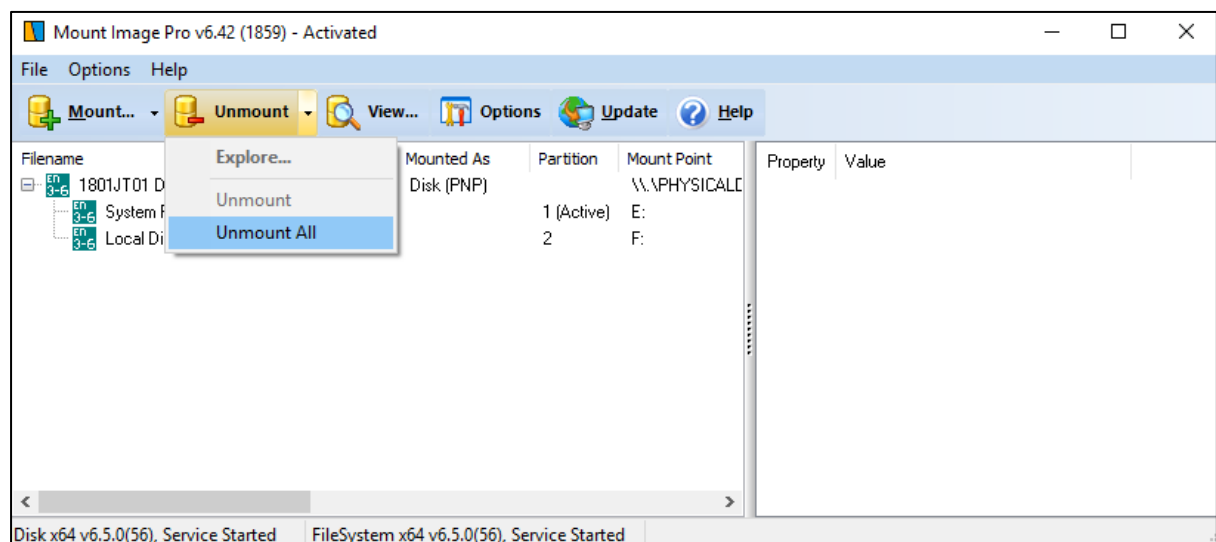
Method 1 (Manual) describes how to manually perform the process that is undertaken by the script in the description above.

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 bypass 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**:

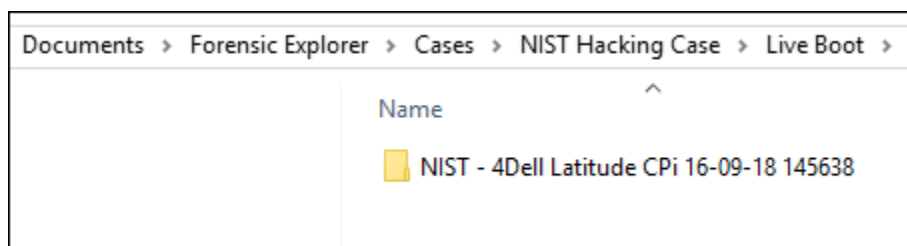
Figure 470: Mount Image Pro - Unmount All



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 471 below:

Figure 471: Live Boot working folder.

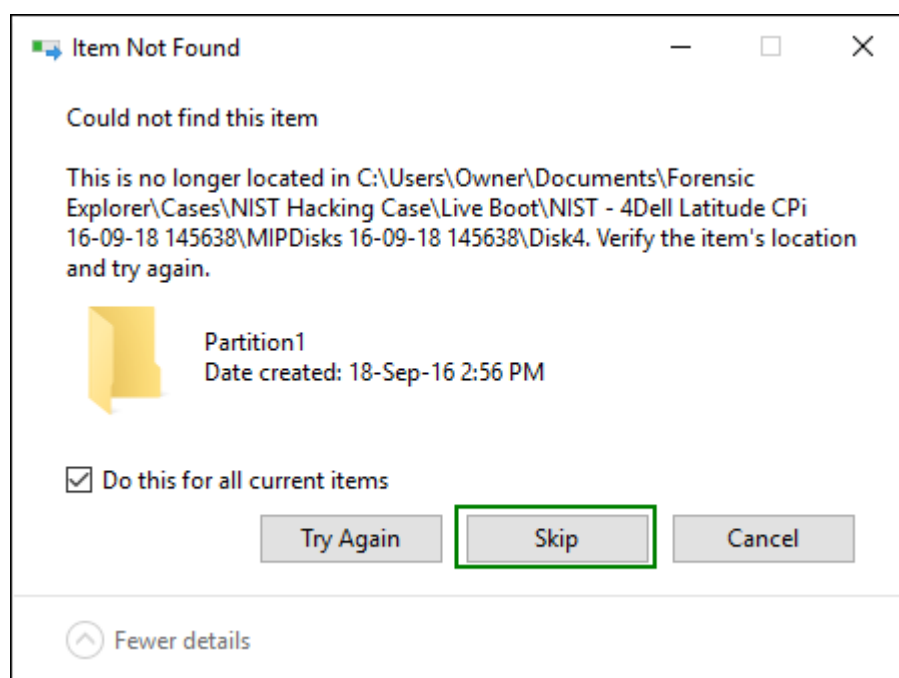


Copy this folder to the **Examination Computer** (see Step 1 below).

METHOD 1 (MANUAL): ON THE EXAMINATION COMPUTER**On the Examination computer:**

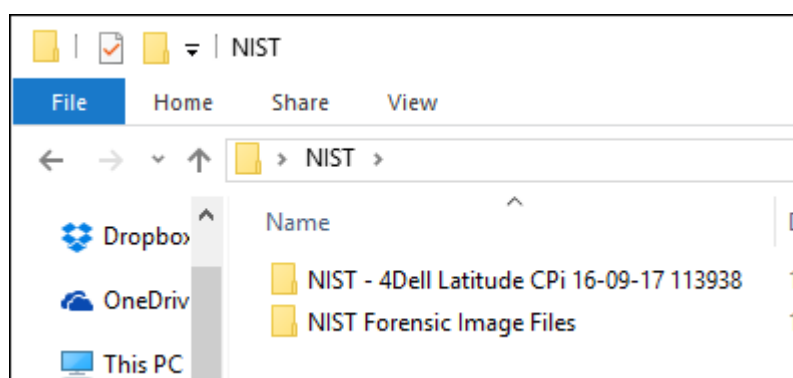
1. **Copy the Forensic Explorer Live Boot working folder** (described above) from the **Forensic Workstation** to the **Examination Computer**. Error messages relating to missing 'DiskX' files can be skipped, as shown in Figure 472 below:

Figure 472: Error message copying Live Boot sessions.



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 473: Examination Computer with Live Boot working folder and forensic image files

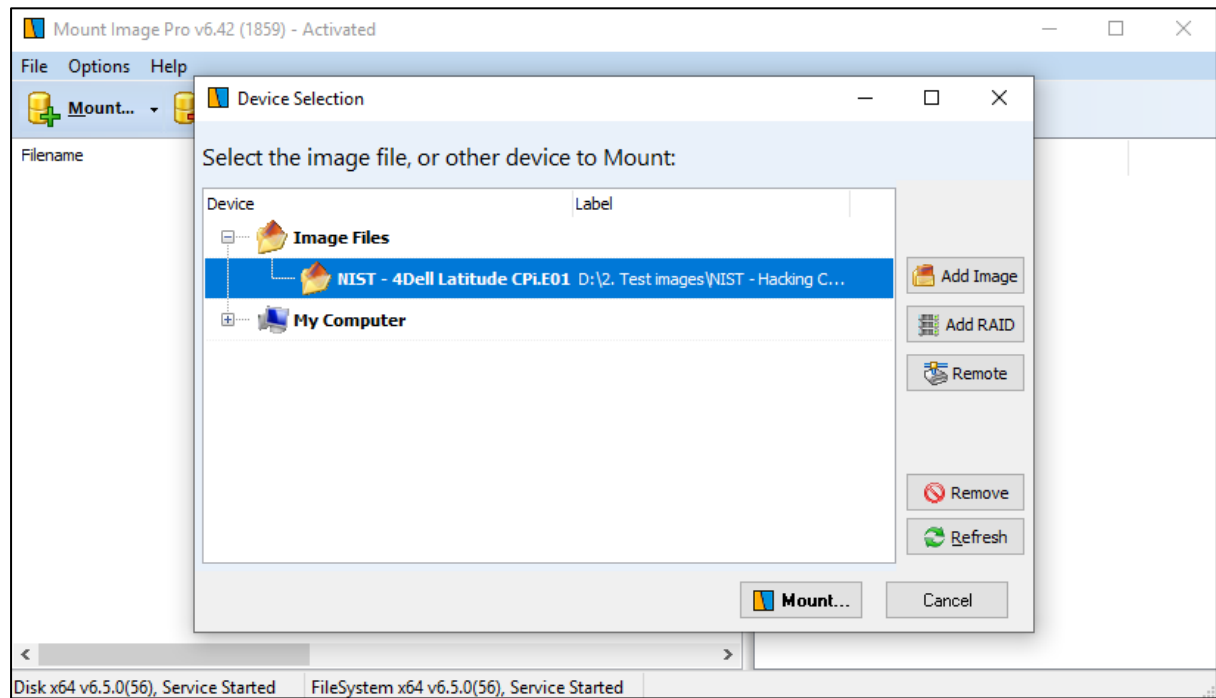


3. **Run Mount Image Pro (as local administrator)**. It can be run either from the desktop icon, or the Windows System tray. **Important:** If this is the first time Mount Image Pro has been run on the **Examination Computer**

a **Reboot** is required to install the mount drivers. Check that the drives are correctly installed as shown in Figure 474.

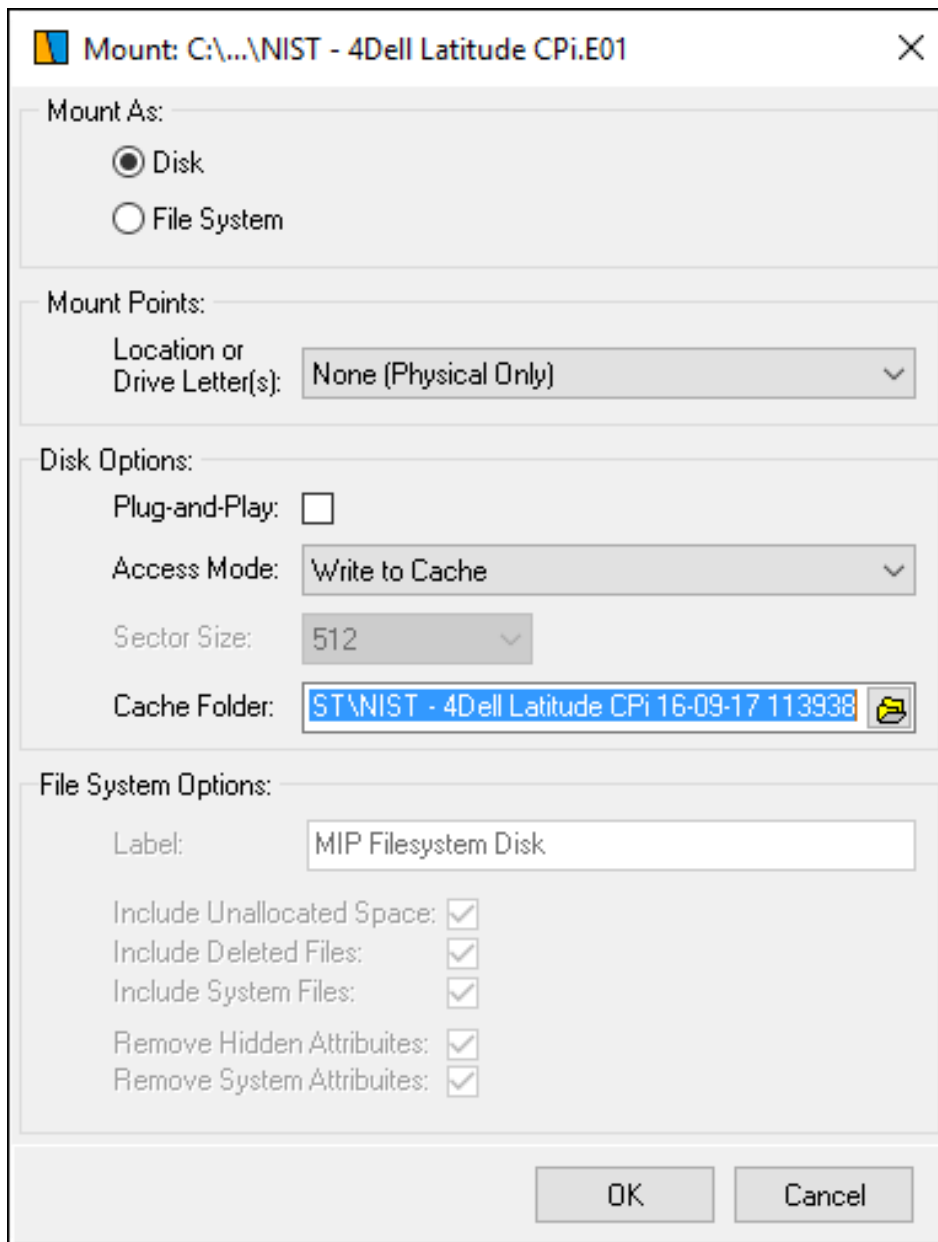
4. In the Mount Image Pro GUI, click the **Mount** button and in the **Device Selection** window click the **Add Image** button to add the required image file, as shown below in Figure 475. Once added, highlight the image file, and click the **Mount** button:

Figure 475: mounting an image using the MIP GUI



5. The image must be mounted with the following options:

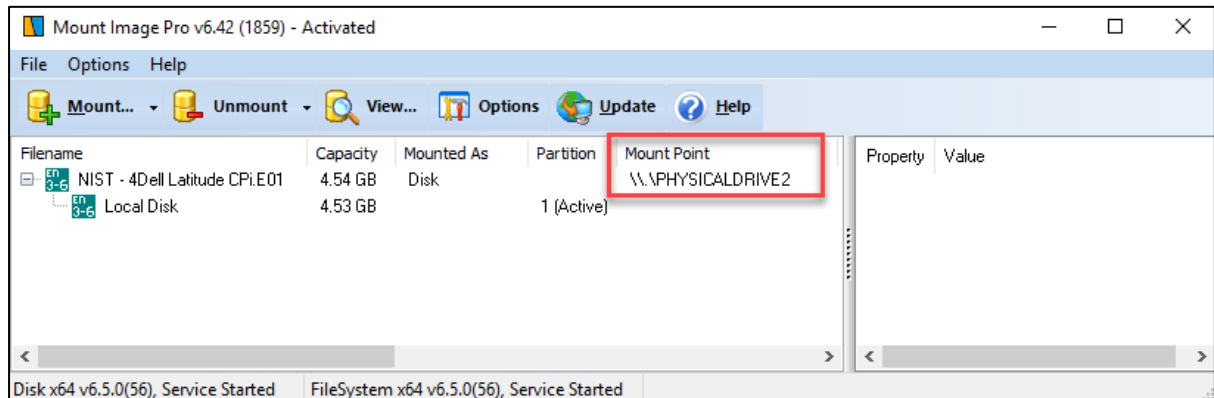
Figure 476: Mount Image Pro settings when mounting for a deployable Live Boot



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 in this folder).

Click OK to mount the image. Note the Physical Drive Mount Point number, as shown in Figure 477 below:

Figure 477: Mounted Physical Device showing Physical Drive Mount Point number.

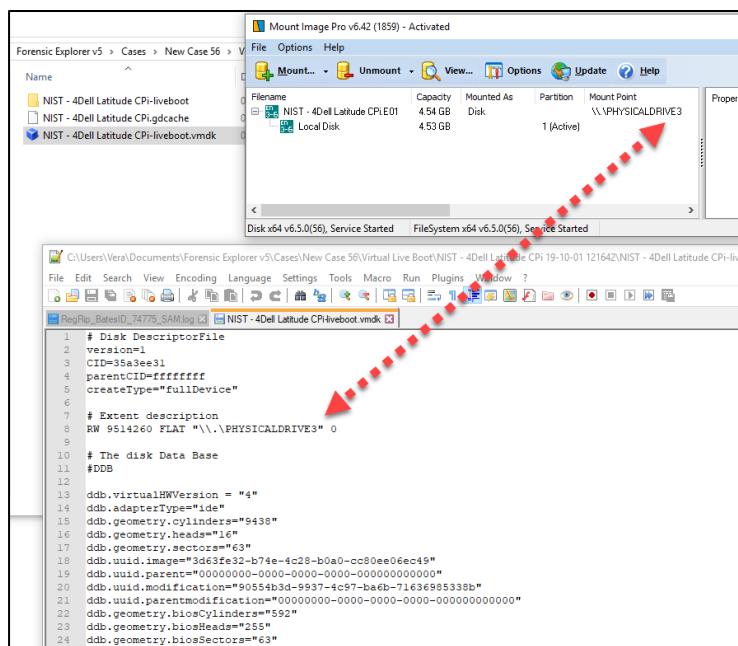


- In the **Live Boot** folder open the **.vmdk** file in an editor (notepad++ is shown below).

IMPORTANT: vmdk files may be **hidden files**. Check your Windows file display settings to set hidden files to be visible.

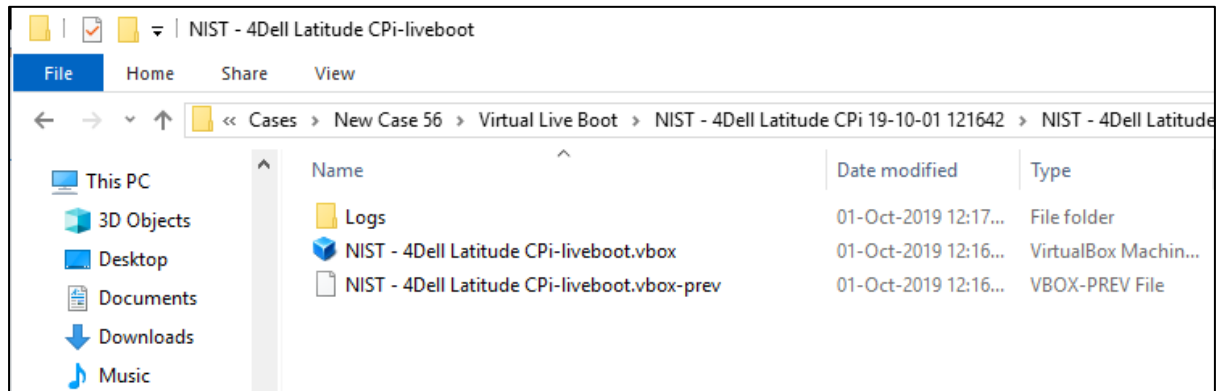
The **PHYSICALDRIVE** number in the **Mount Image Pro GUI** must match the physical drive number in the **.vmdk** file. If it does not match, edit, and save the **.vmdk** file:

Figure 478: Match the PHYSICALDRIVE number in the .vmdk with MIP



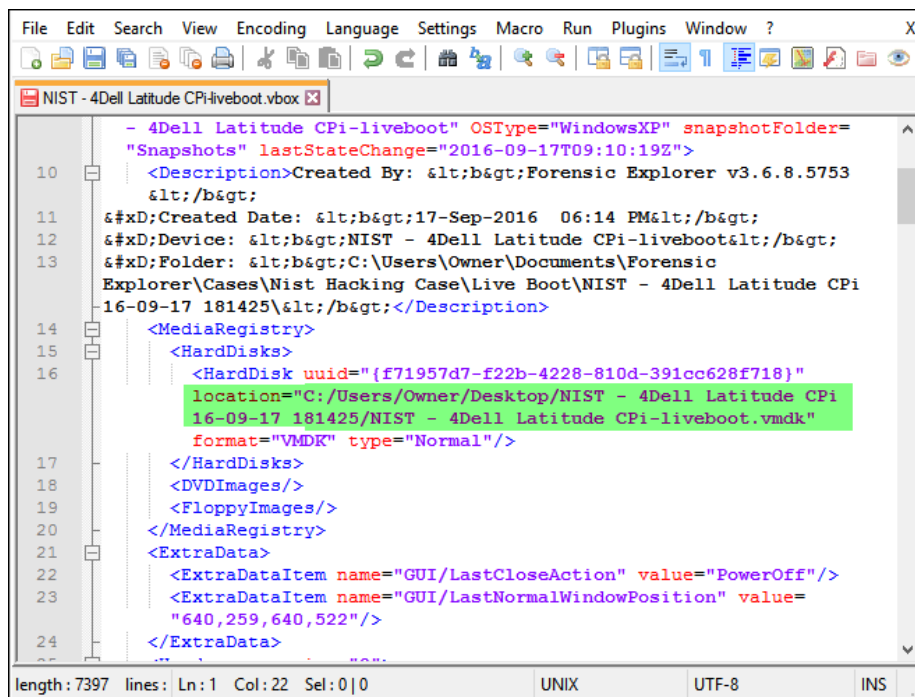
7. In the **Live Boot folder** navigate into the folder ending with **–liveboot** to locate the **.vbox** file:

Figure 479: Virtual Box .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 480: Edit the HardDisk location path in the .vbox file.



9. **Double click** the **.vbox** file to launch the virtual machine.

28.9.3 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 bypass 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

CHAPTER 29 – FORENSIC IMAGE CONVERTER

29.1	Forensic Image Converter	464
29.1.1	Program Features	464
29.1.2	Frequently Asked Questions	464
29.2	Download and Install Forensic Image Converter	464
29.3	Add Forensic Image Converter to the Windows Path	466
29.4	Launching the Windows Command Line	468
29.5	ConvertTOL01.EXE - Usage	469
29.5.1	CONVERTTOL01.EXE - Help	469
29.5.2	Example Conversion	470
29.6	Validation of Conversion	473

29.1 FORENSIC IMAGE CONVERTER

Forensic Image Converter is a **standalone command line tool** that is licensed with Forensic Explorer.

As the name suggests, 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 9.7.2).

Why would I use Forensic Image Converter?

Forensic Image Converter is most 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.

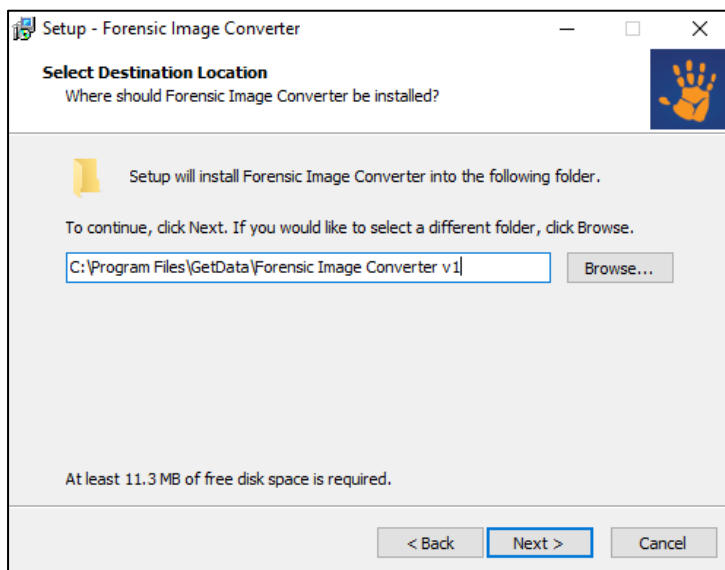
29.2 DOWNLOAD AND INSTALL FORENSIC IMAGE CONVERTER

Contact support@getdata.com for a download link for **Forensic Image Converter**.

To **install Forensic Image Converter**:

1. Run the downloaded setup application (i.e., ForensicImageConverter(vX.X.X.XX).exe;
2. Follow the onscreen instructions, as shown below:

Figure 481: Forensic Image Converter Setup



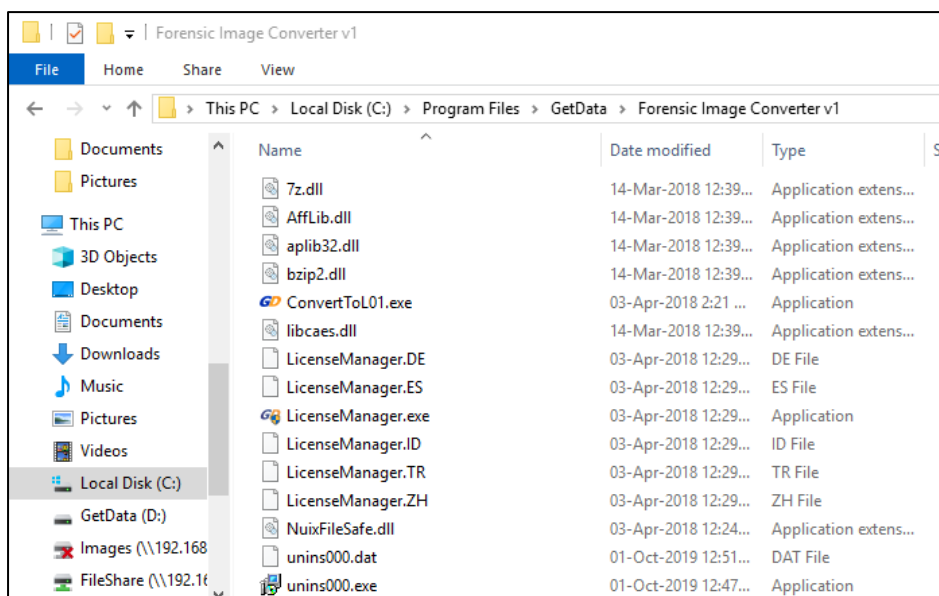
Important: Forensic Image Converter is a **Command Line Application**. At the completion of install the setup will **NOT** create a desktop icon.

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 482 below:

Figure 482: Forensic Image Converter default installation path installed files.



The command line executable is:

- **ConvertToL01.exe**

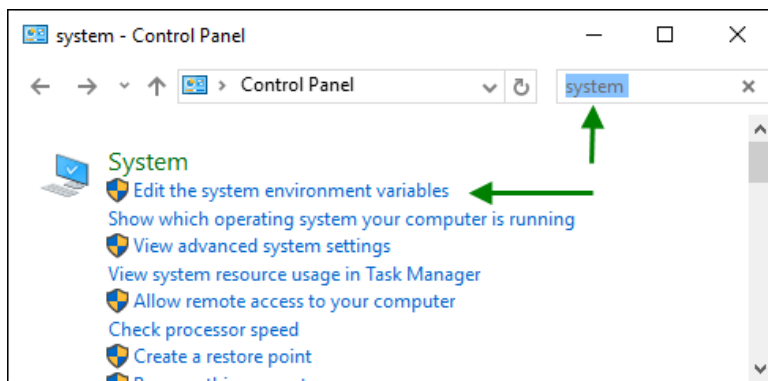
29.3 ADD FORENSIC IMAGE CONVERTER TO THE WINDOWS PATH

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:

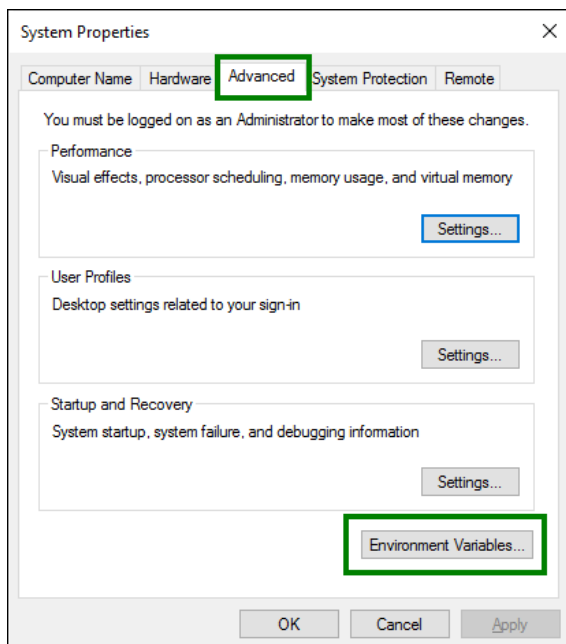
1. Open the **System Properties** window by:
 - a. Typing: **sysdm.cpl**; or
 - b. Open the Control Panel, search for **system** and select the **Edit the system environment variables** option shown in Figure 483 below:

Figure 483: Windows 10 Control Panel



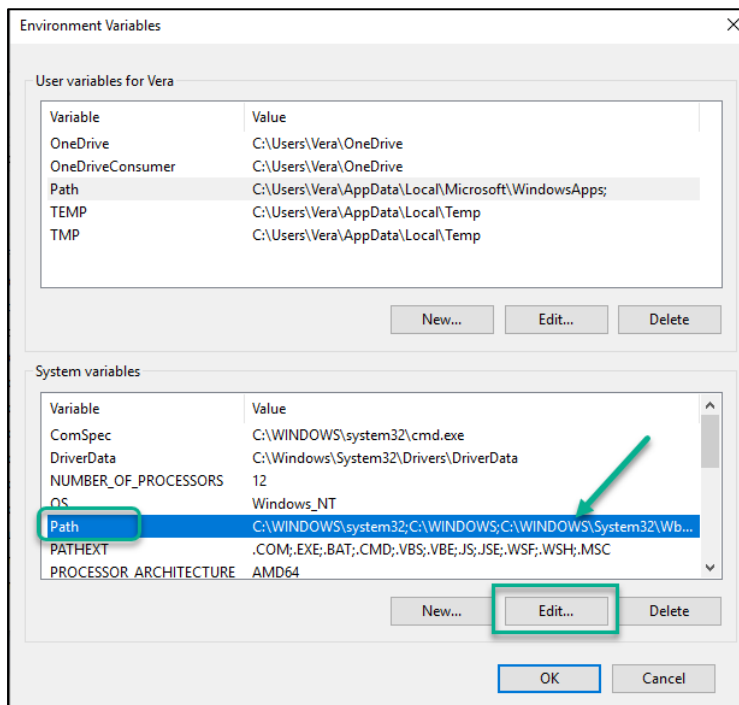
In the System Properties window select the **Advanced** tab then the **Environment Variables** button, as shown in Figure 484 below:

Figure 484: System Properties (Windows 10 shown)



In the **Environment Variables** window, in the **System Variables** box, select **Path**, then press the **Edit** button, as shown in Figure 485 below:

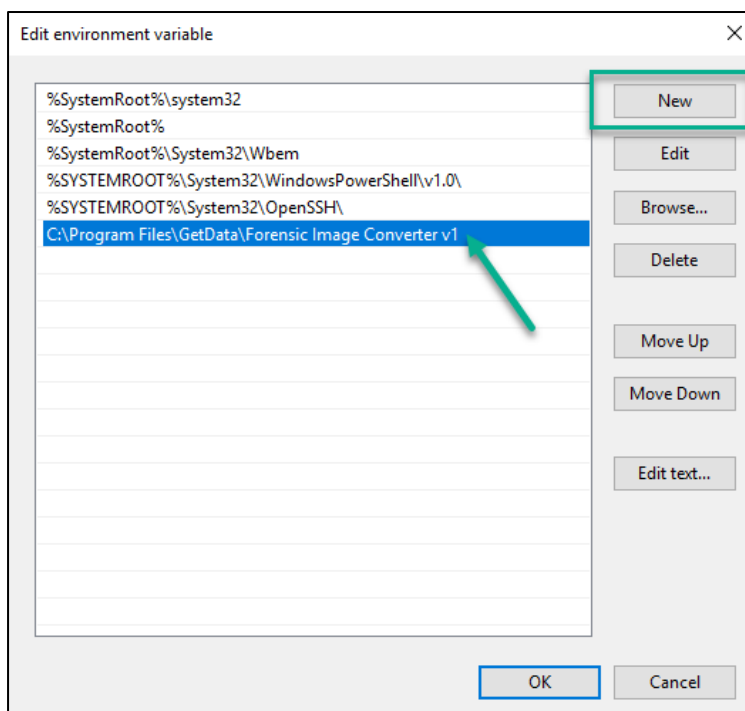
Figure 485: Edit the Windows Path System Variable (Windows 10 shown)



In the **Edit environment, variable** window, click the **new** button and add the Forensic Image Converter Path:

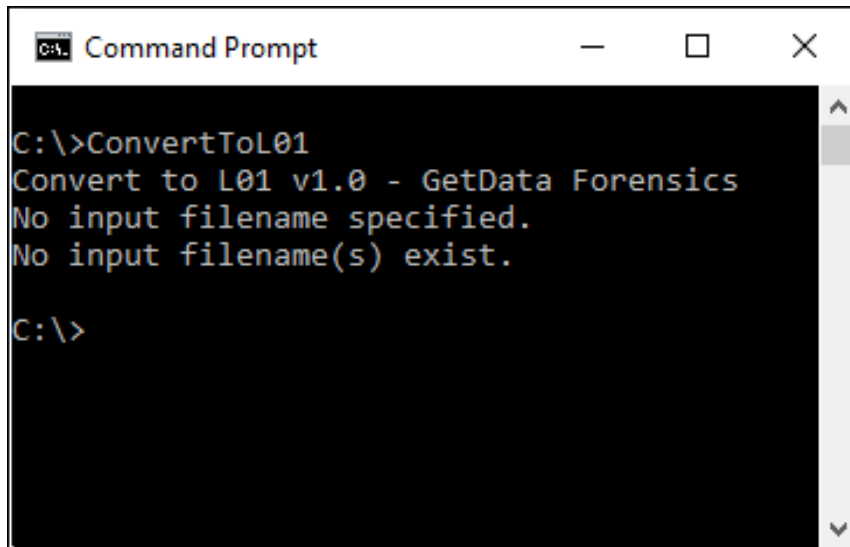
C:\Program Files\GetData\Forensic Image Converter vX as shown in Figure 486 below.

Figure 486: Adding the Forensic Image Converter path to the Environment variables



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 487 below which has been executed from the folder "C:\":

Figure 487: Running ConvertToL01 after changing the Windows Path variable.



```
C:\>ConvertToL01
Convert to L01 v1.0 - GetData Forensics
No input filename specified.
No input filename(s) exist.

C:\>
```

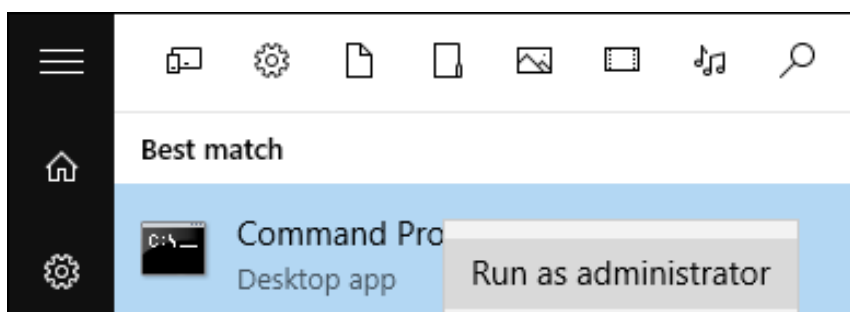
29.4 LAUNCHING THE WINDOWS COMMAND LINE

Important: To avoid Windows permissions 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 488 below:

Figure 488: Running a Windows Command Prompt with Administrator user rights



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:

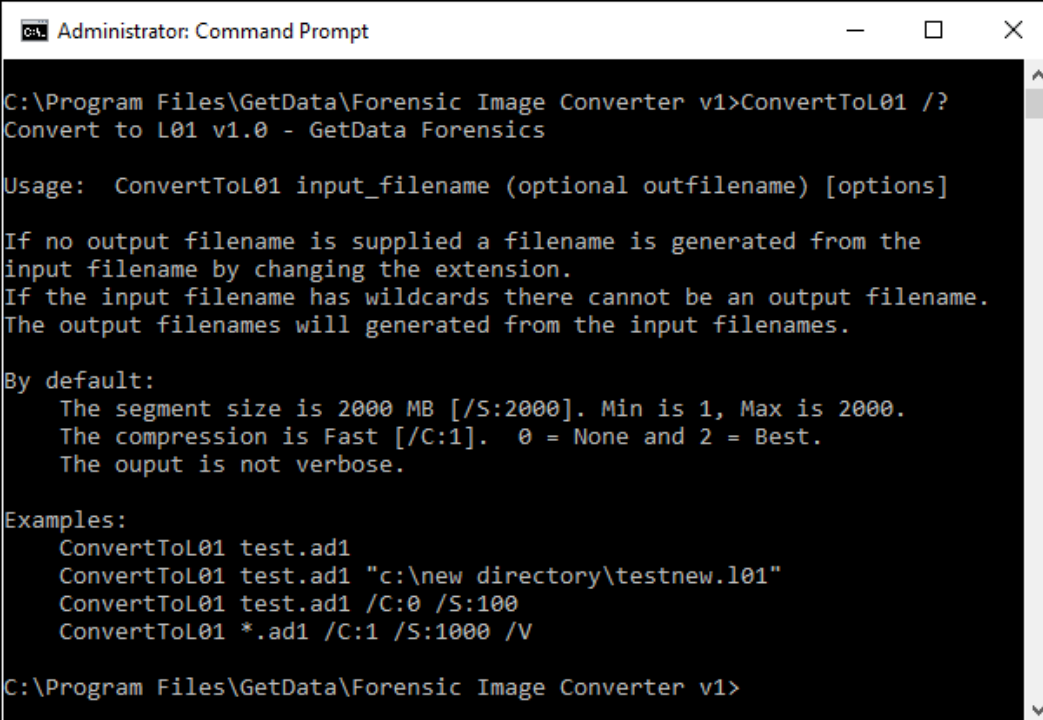
```
C:\Program Files\GetData\Forensic Image Converter vX
```

There are two help switches:

- **ConvertToL01 /?;** and,
- **ConvertToL01 /Help.**

The output of these switches is shown below:

Figure 489: ConvertToL01 /? - Switch



```
Administrator: Command Prompt
C:\Program Files\GetData\Forensic Image Converter v1>ConvertToL01 /?
Convert to L01 v1.0 - GetData Forensics

Usage:  ConvertToL01 input_filename (optional outfilename) [options]

If no output filename is supplied a filename is generated from the
input filename by changing the extension.
If the input filename has wildcards there cannot be an output filename.
The output filenames will generated from the input filenames.

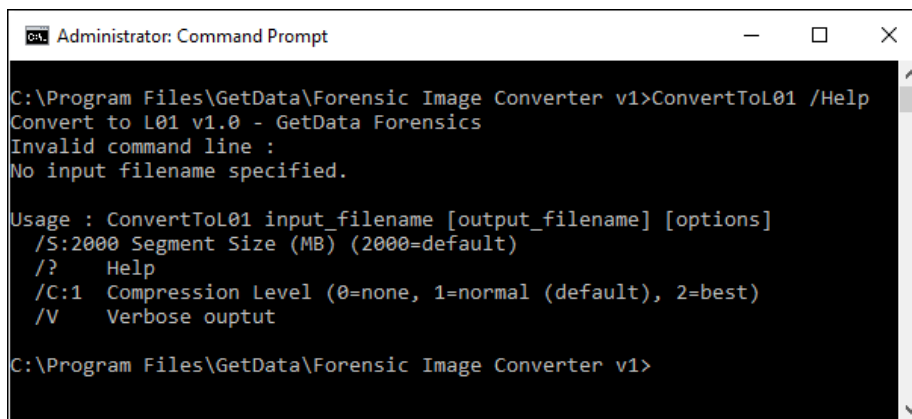
By default:
  The segment size is 2000 MB [/S:2000]. Min is 1, Max is 2000.
  The compression is Fast [/C:1]. 0 = None and 2 = Best.
  The ouput is not verbose.

Examples:
  ConvertToL01 test.ad1
  ConvertToL01 test.ad1 "c:\new directory\testnew.l01"
  ConvertToL01 test.ad1 /C:0 /S:100
  ConvertToL01 *.ad1 /C:1 /S:1000 /V

C:\Program Files\GetData\Forensic Image Converter v1>
```

The /? Switch gives general usage information and examples.

Figure 490: ConvertToL01 /help - Switch



```
Administrator: Command Prompt
C:\Program Files\GetData\Forensic Image Converter v1>ConvertToL01 /Help
Convert to L01 v1.0 - GetData Forensics
Invalid command line :
No input filename specified.

Usage : ConvertToL01 input_filename [output_filename] [options]
/S:2000 Segment Size (MB) (2000=default)
/? Help
/C:1 Compression Level (0=none, 1=normal (default), 2=best)
/V Verbose output
C:\Program Files\GetData\Forensic Image Converter v1>
```

The **/help** switch gives specific information relating to program command line switches.

29.5.2 EXAMPLE CONVERSION

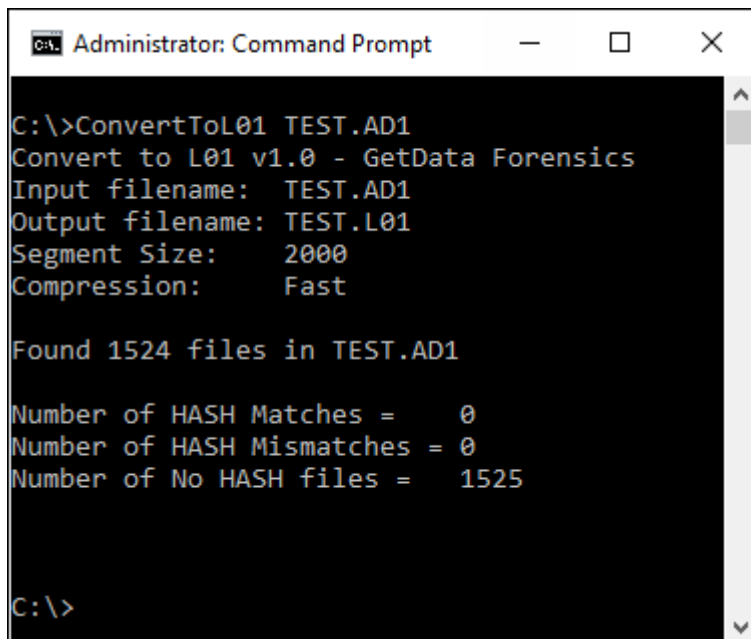
In the examples below the file TEST.AD1 is in the C:\ folder. Forensic Image Converter has been added to the Windows Path Environment Variable to enable its execution directly from the C:\ folder.

DEFAULT CONVERSION

The command:

- **ConvertToL01 TEST.AD1**

Is used to create a **L01** file of the same name in the same folder:



```
Administrator: Command Prompt
C:\>ConvertToL01 TEST.AD1
Convert to L01 v1.0 - GetData Forensics
Input filename: TEST.AD1
Output filename: TEST.L01
Segment Size: 2000
Compression: Fast

Found 1524 files in TEST.AD1

Number of HASH Matches = 0
Number of HASH Mismatches = 0
Number of No HASH files = 1525

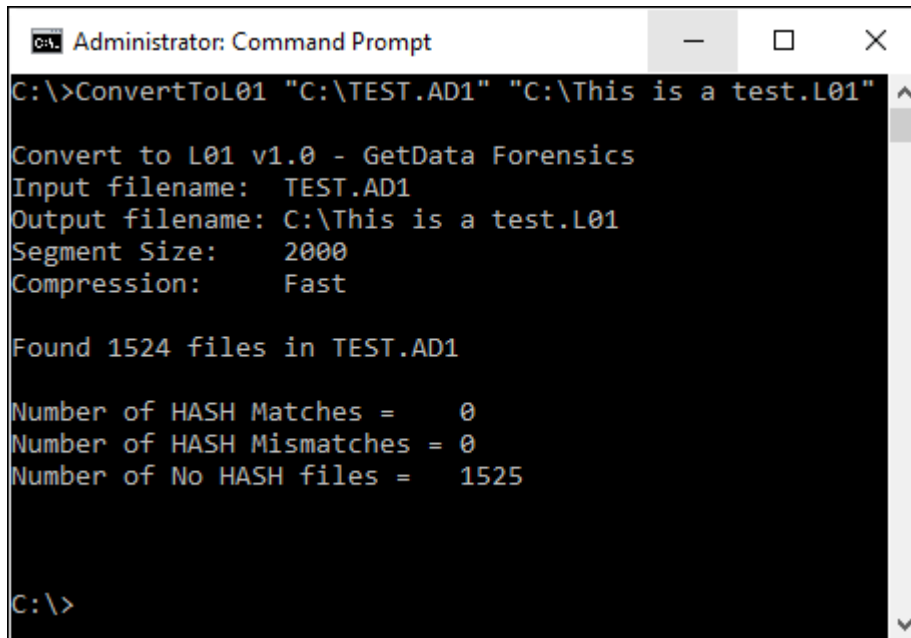
C:\>
```

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:



```
Administrator: Command Prompt
C:\>ConvertToL01 "C:\TEST.AD1" "C:\This is a test.L01"
Convert to L01 v1.0 - GetData Forensics
Input filename: TEST.AD1
Output filename: C:\This is a test.L01
Segment Size: 2000
Compression: Fast

Found 1524 files in TEST.AD1

Number of HASH Matches = 0
Number of HASH Mismatches = 0
Number of No HASH files = 1525

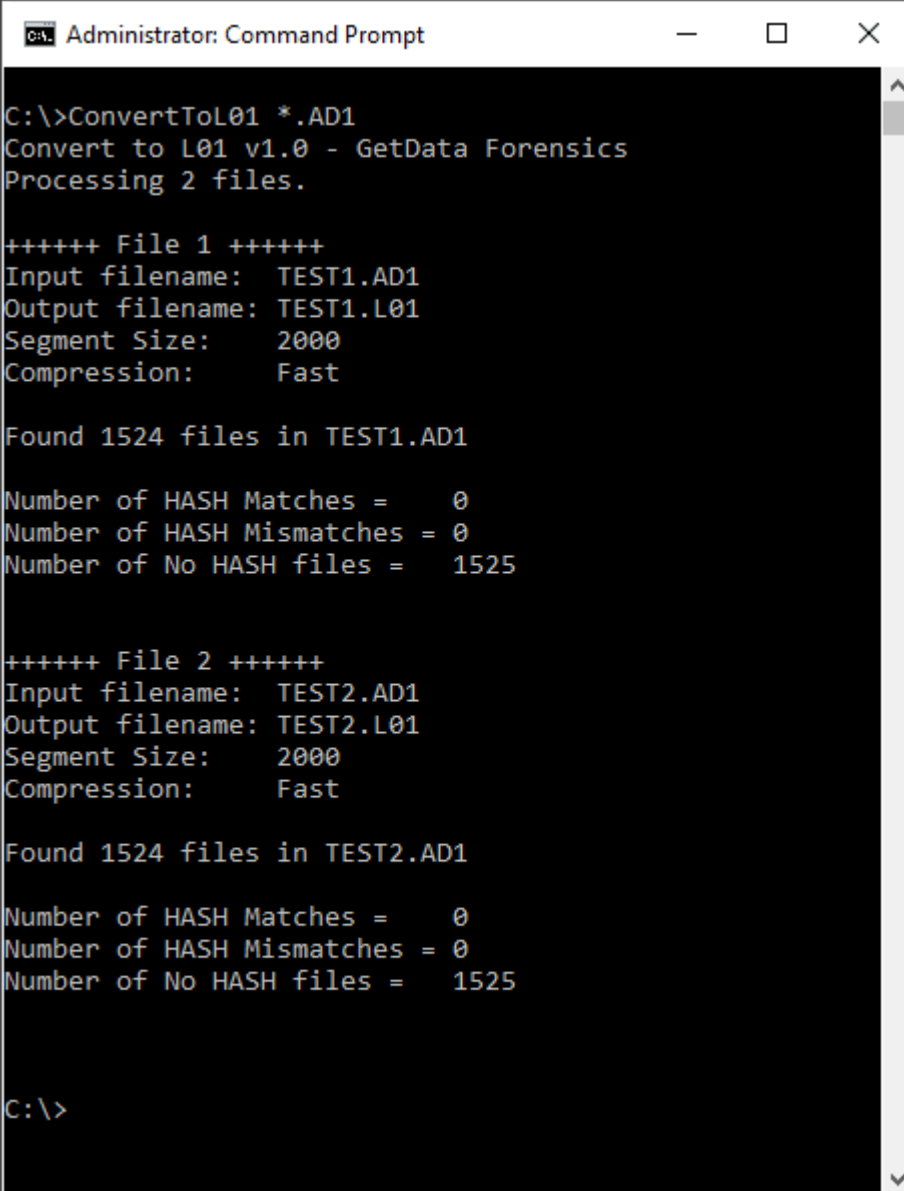
C:\>
```

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:



```
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

CHAPTER 30 – WORKING WITH ...

30.1	iTunes Backups	477
30.1.1	iCloud Backup	477
30.1.2	iTunes Backup	477
30.1.3	Backing up an iOS device for the first time.....	478
30.1.4	Encrypted Backups.....	479
30.1.5	iOS Backup Paths	479
30.1.6	Locating Apple Backup Folders with Forensic Explorer	480
30.1.7	Inside an iTunes Backup Folder	480
30.1.8	The importance of File Signature Analysis.....	481
30.1.9	Key User files in an iTunes Backup.....	482
30.1.10	iTunes Backup Configuration Files	483
30.1.11	Processing iTunes Backups in Forensic Explorer.....	484
30.1.12	Step 1 - Identify and Bookmark iTunes Backup folders	484
30.1.13	Step 2 - iTunes Backup Analyze	487
30.1.14	Step 3 – Examining iTunes backup file content	488
30.1.15	Working with Encrypted Backups.....	489
30.1.16	Identifying Encrypted iTunes Backups	489
30.1.17	Decrypting an iTunes Backup.....	490
30.1.18	Live Boot	491
30.1.19	Shadow Copy	492
30.2	Thumbnails	493
30.2.1	Thumbs.db	493

30.2.2	Thumbcache	493
30.2.3	Forensic Value of Thumbnails.....	493

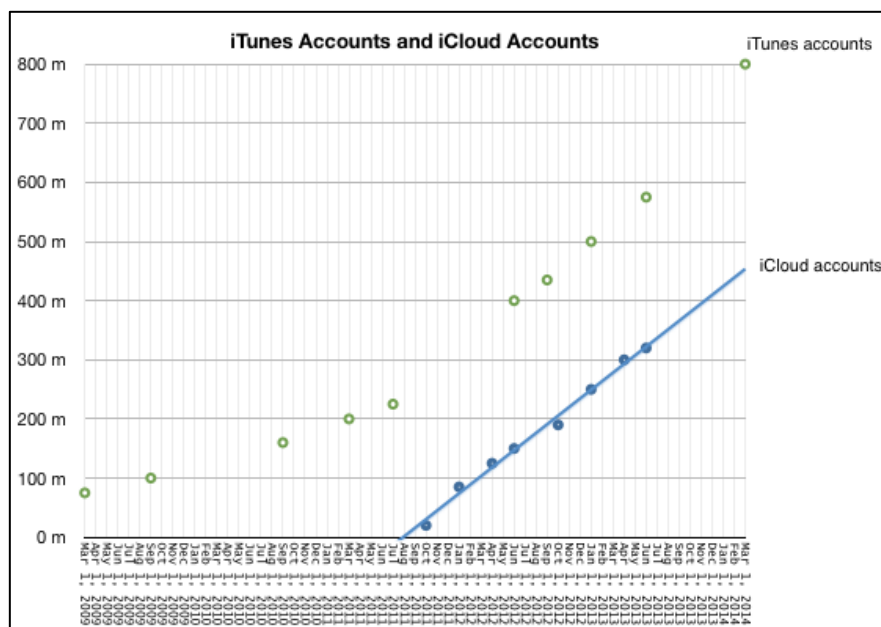
30.1 ITUNES BACKUPS

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 (<https://getdataforensics.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 491: projected iTunes and iCloud usage (Source: <http://www.asymco.com/2014/11/15/how-big-is-iCloud> (17))

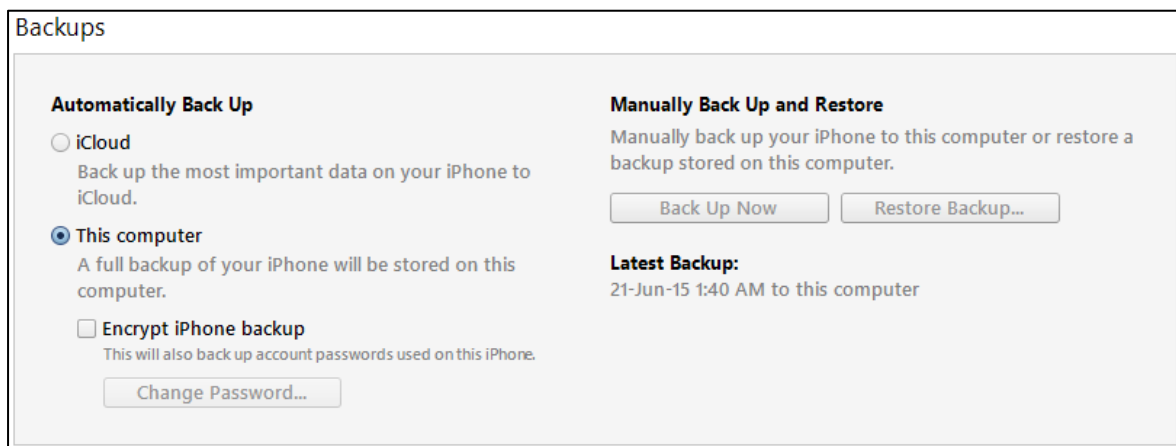


iCloud backups occur when the backup option is selected in iTunes and the device is locked and connected to Wi-Fi and a power source. A default iCloud account has a size limit of 5 GB (as of July 2015,), although additional storage space can be purchased from Apple. iCloud accounts are password protected 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 screenshot in Figure 492 below:

Figure 492: iTunes backup options



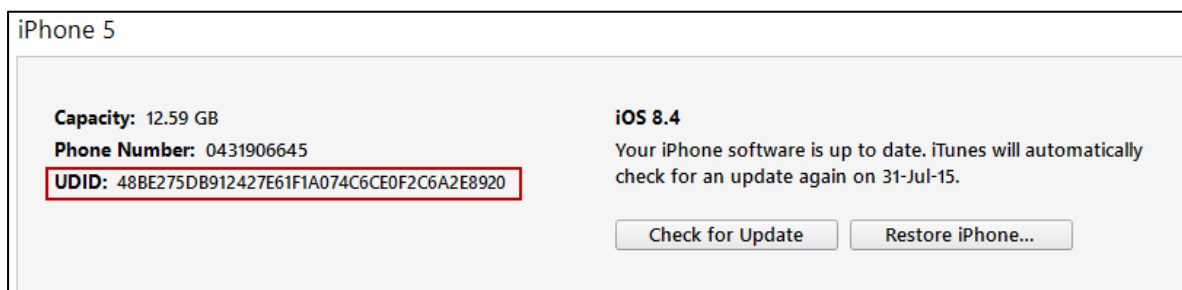
30.1.3 BACKING UP AN IOS DEVICE FOR THE FIRST TIME

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 493 below:

Figure 493: iTunes options showing the UDID.



For more information on how UDIDs are created, see: <https://www.theiphonewiki.com/wiki/UDID> (18).

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.

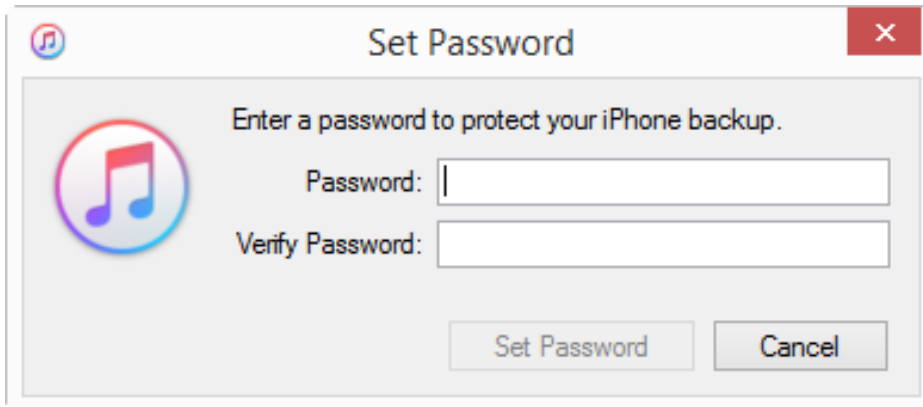
When an iOS device is updated or restored, an automated backup is initiated as a **differential** backup. A differential backup contains all files that have changed since the last full backup. A differential backup folder is created with the same UDID appended with the date and time of the backup, for example:

- 48be275db912427e61f1a074c6ce0f2c6a2e8920-20150719-170306

30.1.4 ENCRYPTED BACKUPS

iTunes provides the option to encrypt backups (as shown in Figure 492 above). During the backup process the user is prompted to enter a password to encrypt all files in the backup:

Figure 494: iTunes encrypted backup password request.



Dealing with encrypted backups is further discussed in section 30.1.15 below.

30.1.5 IOS BACKUP PATHS

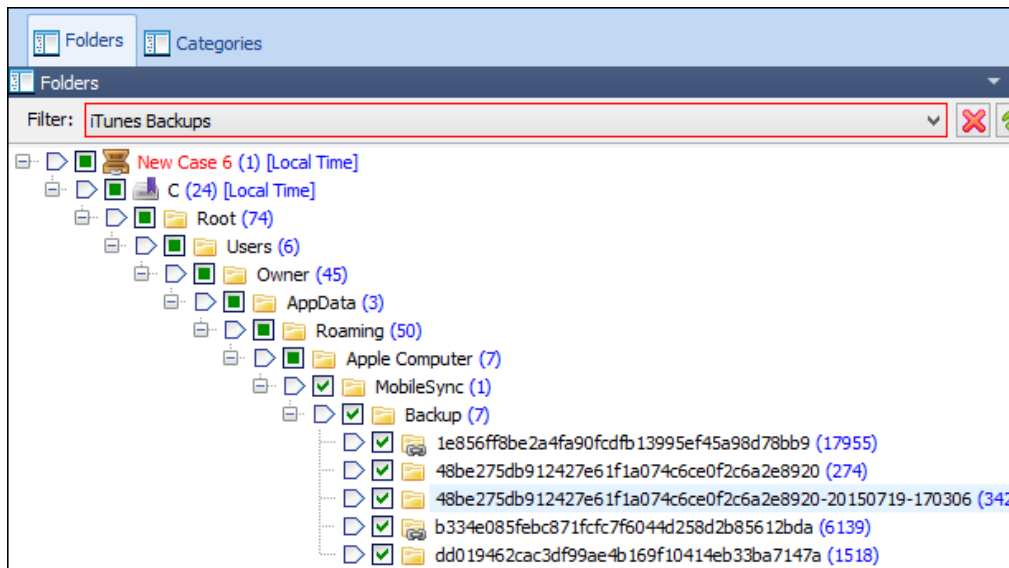
The default paths for iTunes backups are:

Windows 7/8	C:\Users\[username]\AppData\Roaming\Apple Computer\MobileSync\Backup\
Windows XP	C:\Documents and Settings\username\Application Files\MobileSync\Backup\deviceid\
MAC OS X	[User HomeDirectory]\Library\Application Support\MobileSync\Backup\

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 495 below:

Figure 495: 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 496 below:

Figure 496: Example content of an iTunes backup folder

Filename	Extension	File Signature	Extension Mismatch
1 48be275db912427e61f1a074c6ce0f2c6a2...		Folder	
2 000cae3437db21095a85771716e6874f92c...			
3 00dbce3b26b839ef95789e710e9fbc06669...			
4 0119a2aee440a806c87794c56b2f10df585...			
5 012707a2ae34d77a28b16a9e443b780ea4...			
6 012707a2ae34d77a28b16a9e443b780ea4...			
7 01722562244dfdfcb81470a609a52b8a2ab...			
8 02080c751f0cd98738a2e9ccf7c133f01978...			
9 023660cf4f4a29dd36f30ff3de4bfc0f621e7...			
10 02436361e7199aeb9c0b95ce48e6c5ca217...			
11 027cd714eccfd83268ad662cd4f679f0aa5a...			
12 02d2181fb1f29f3cd78b75bd28c295585eb0...			
13 02dcc29d169dda989f3402fe07d8b6526d6f...			
14 02ddf9f5e2ae205dcdc58ba025773368790...			
15 0354ef572fa6f5f20370be41aa816bd69cb2...			

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 497 below shows the same list of files in Figure 496 after a File Signature Analysis has been run:

Figure 497: Example content of an iTunes backup folder after running a file Signature Analysis

Filename	Extension	File Signature	Extension Mismatch
1 48be275db912427e61f1a074c6ce0f2c6a2...		Folder	
2 000cae3437db21095a85771716e6874f92c...		Plist (Binary)	
3 00dbce3b26b839ef95789e710e9fbc06669...		Plist (Binary)	
4 0119a2aee440a806c87794c56b2f10df585...		Unknown	
5 012707a2ae34d77a28b16a9e443b780ea4...		Plist (Binary)	
6 012707a2ae34d77a28b16a9e443b780ea4...		Plist (Binary)	
7 01722562244dfdfcb81470a609a52b8a2ab...		Text	
8 02080c751f0cd98738a2e9ccf7c133f01978...		Plist (Binary)	
9 023660cf4f4a29dd36f30ff3de4bfc0f621e7...		JPG	
10 02436361e7199aeb9c0b95ce48e6c5ca217...		SQLite	
11 027cd714eccfd83268ad662cd4f679f0aa5a...		JPG	
12 02d2181fb1f29f3cd78b75bd28c295585eb0...		Plist (Binary)	
13 02dcc29d169dda989f3402fe07d8b6526d6f...		XML	
14 02ddf9f5e2ae205dcdc58ba025773368790...		Unknown	
15 0354ef572fa6f5f20370be41aa816bd69cb2...		Plist (Binary)	

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:

Contents	Domain	iOS Path and file name	SHA-1 backup file name
Calendar	HomeDomain	Library/Calendar/Calendar.sqlitedb	2041457d5fe04d39d0ab481178355df6781e6858
Call History	WirelessDomain	Library/CallHistory/call_history.db	2b2b0084a1bc3a5ac8c27afdf14afb42c61a19ca
Chat – KikChat	AppDomain-com.kik.chat	Documents/kik.sqlite	8e281be6657d4523710d96341b6f86ba89b56df7
Chat – Line	AppDomain-jp.naver.line	Documents/talk.sqlite	534a7099b474f4fb3f2cd006f8e59578d58fb44a
Chat – MessageMe	AppDomain-com.littleinc.MessageMe	Library/Application Support/MessageMe/MessageMe.sqlite	8c625842c0b74fefff30d92eece44a1da30d2e8e
Chat – Skype	AppDomain-com.skype.skype	Library/Application Support/Skype/[user]/main.db	
Chat – Touch	AppDomain-com.enflick.ping	Documents/Touch.sqlite	b18a30bf72824a7d024a95178ae42d8339f83633
Chat – Viber	AppDomain-com.viber	Documents/Contacts.data	b39bac0d347adfaf172527f97c3a5fa3df726a3a
Chat – WeChat	AppDomain-com.tencent.xin	Documents/[chat-UDID]/DB/MM.sqlite	
Chat - WhatsApp	AppDomain-net.whatsapp.WhatsApp	AppDomain-net.whatsapp.WhatsApp	1b6b187a1b60b9ae8b720c79e2c67f472bab09c0
Contacts	HomeDomain	Library/AddressBook/AddressBook.sqlitedb	31bb7ba8914766d4ba40d6dfb6113c8b614be442
Keyboard	HomeDomain	Library/Keyboard/dynamic-text.dat	Changes with language installed
Locations	RootDomain	Library/Caches/locationd/consolidated.db	4096c9ec676f2847dc283405900e284a7c815836*
Maps History	HomeDomain	Library/Maps/History.plist	b60c382887dfa562166f099f24797e55c12a94e4
Notes	HomeDomain	Library/Notes/notes.sqlite	ca3bc056d4da0bbf88b5fb3be254f3b7147e639c
Safari History	HomeDomain	Library/Safari/History.plist	1d6740792a2b845f4c1e6220c43906d7f0afe8ab
SMS	HomeDomain	Library/SMS/sms.db	3d0d7e5fb2ce288813306e4d4636395e047a3d28
Wifi Networks	SystemPreferencesDomain	SystemConfiguration/com.apple.wifi.plist	ade0340f576ee14793c607073bd7e8e409af07a8

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.

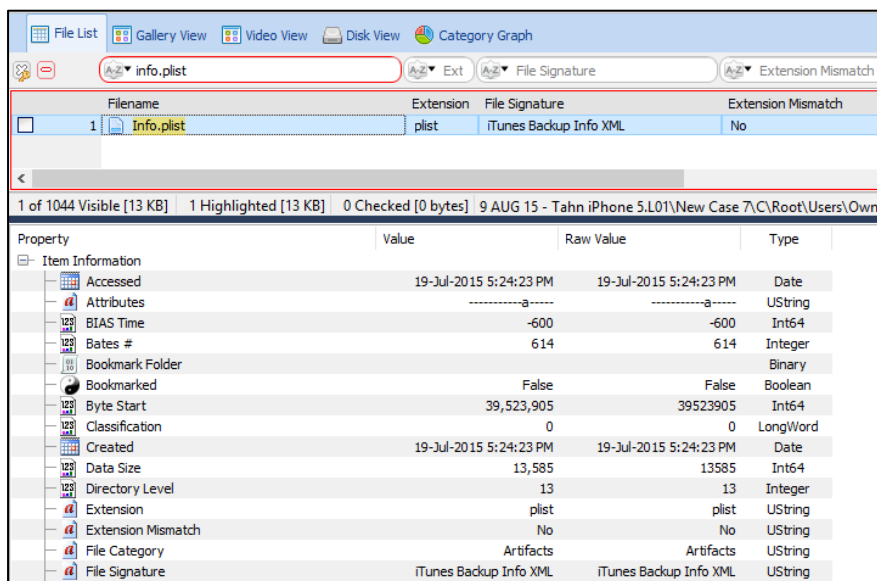
INFO.PLIST

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 498 below:

Figure 498: Manually examine the content of an iTunes info.plist file



The screenshot shows the Forensic Explorer interface with the 'File System' module selected. The 'Metadata' data view is active, displaying the properties of the selected file 'Info.plist'. The file is located at '9 AUG 15 - Tahn iPhone 5.L01\New Case 7\C\Root\Users\Ownr'. The metadata table below shows various properties and their values.

Property	Value	Raw Value	Type
Item Information			
Accessed	19-Jul-2015 5:24:23 PM	19-Jul-2015 5:24:23 PM	Date
Attributes	-----a-----	-----a-----	UString
BIAS Time	-600	-600	Int64
Bates #	614	614	Integer
Bookmark Folder			Binary
Bookmarked	False	False	Boolean
Byte Start	39,523,905	39523905	Int64
Classification	0	0	LongWord
Created	19-Jul-2015 5:24:23 PM	19-Jul-2015 5:24:23 PM	Date
Data Size	13,585	13585	Int64
Directory Level	13	13	Integer
Extension	plist	plist	UString
Extension Mismatch	No	No	UString
File Category	Artifacts	Artifacts	UString
File Signature	iTunes Backup Info XML	iTunes Backup Info XML	UString

STATUS.PLIST

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/> (19).

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 is 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 499 below:

Figure 499: iTunes Backups - Identify and Bookmark

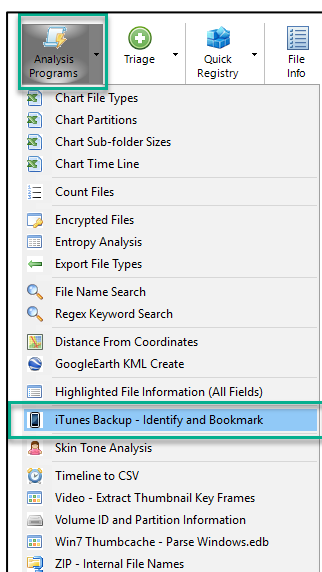
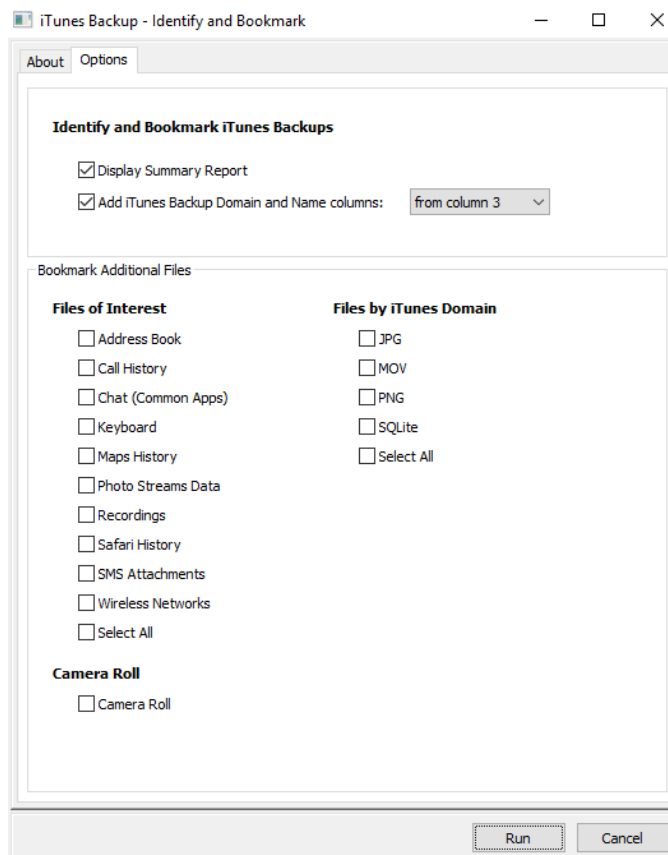


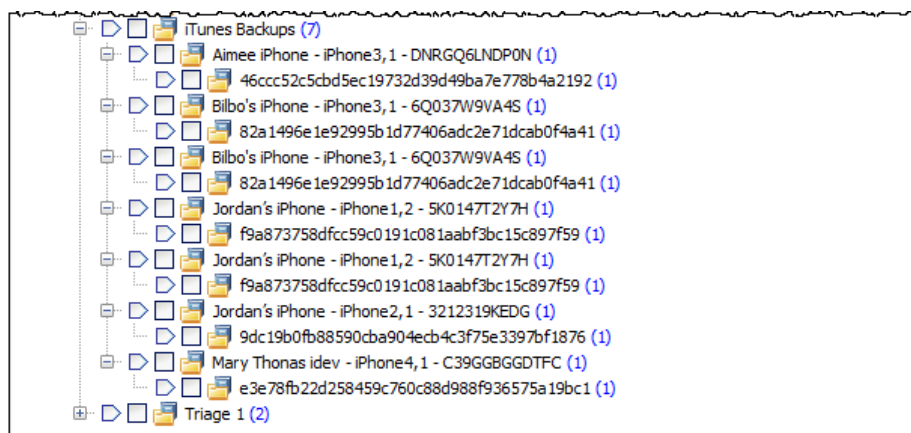
Figure 500: iTunes Identify and Bookmark Options window.



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 501 below:

Figure 501: Bookmarks module, iTunes backup folders



Click on the bookmarked file to display the bookmark comment containing additional information extracted from the info.plist file:

Figure 502: Info.plist bookmark comment for Aimee iPhone

```

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 = 46CCC52C5CBD5EC19732D39D49BA7E778B4A2192

```

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 503 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 503 below:

Figure 503: File list of an iTunes Backup with Backup Domain and Backup Name columns added.

Filename	Extension	File Signature	iTunes Backup Domain	iTunes Backup Name
1 48be275db912427e61f1a074c6ce0f2c6a2...	Folder			
2 000cae3437db21095a85771716e6874f92c...	Plist (Binary)		HomeDomain	Library/SpringBoard/PushStore/com....
3 00dbce3b26b839ef95789e710e9fbc06669...	Plist (Binary)		AppDomain-com.kik.chat	Documents/AddressBook/bloomStor...
4 0119a2aee440a806c87794c56b2f10df585...	Unknown		AppDomain-com.firsttouch.score	Documents/rcd_60_2.dat
5 012707a2ae34d77a28b16a9e443b780ea4...	Plist (Binary)		HomeDomain	Library/Preferences/com.apple.Tele...
6 012707a2ae34d77a28b16a9e443b780ea4...	Plist (Binary)		HomeDomain	Library/Preferences/com.apple.Tele...
7 01722562244dfdfcb81470a609a52b8a2ab...	Text		AppDomain-tv.twitch	Library/Application Support/IN/Onlin...
8 02080c751f0cd98738a2e9ccf7c133f01978...	Plist (Binary)		HomeDomain	Library/Preferences/com.apple.ids.s...
9 023660cf4f4a29dd36f30ff3de4bfc0f621e7...	JPG		CameraRollDomain	Media/PhotoData/Thumbnails/V2/DC...
10 02436361e7199aeb9c0b95ce48e6c5ca217...	SQLite		AppDomain-com.skype.skype	Library/Application Support/Skype/t...
11 027cd714eccfd83268ad662cd4f679f0aa5a...	JPG		CameraRollDomain	Media/PhotoData/Thumbnails/V2/DC...
12 02d2181fb1f29f3cd78b75bd28c295585eb0...	Plist (Binary)		HomeDomain	Library/Preferences/com.apple.ids.s...
13 02dcc29d169dda989f3402fe07d8b6526d6f...	XML		HomeDomain	Library/Preferences/com.apple.secu...

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.

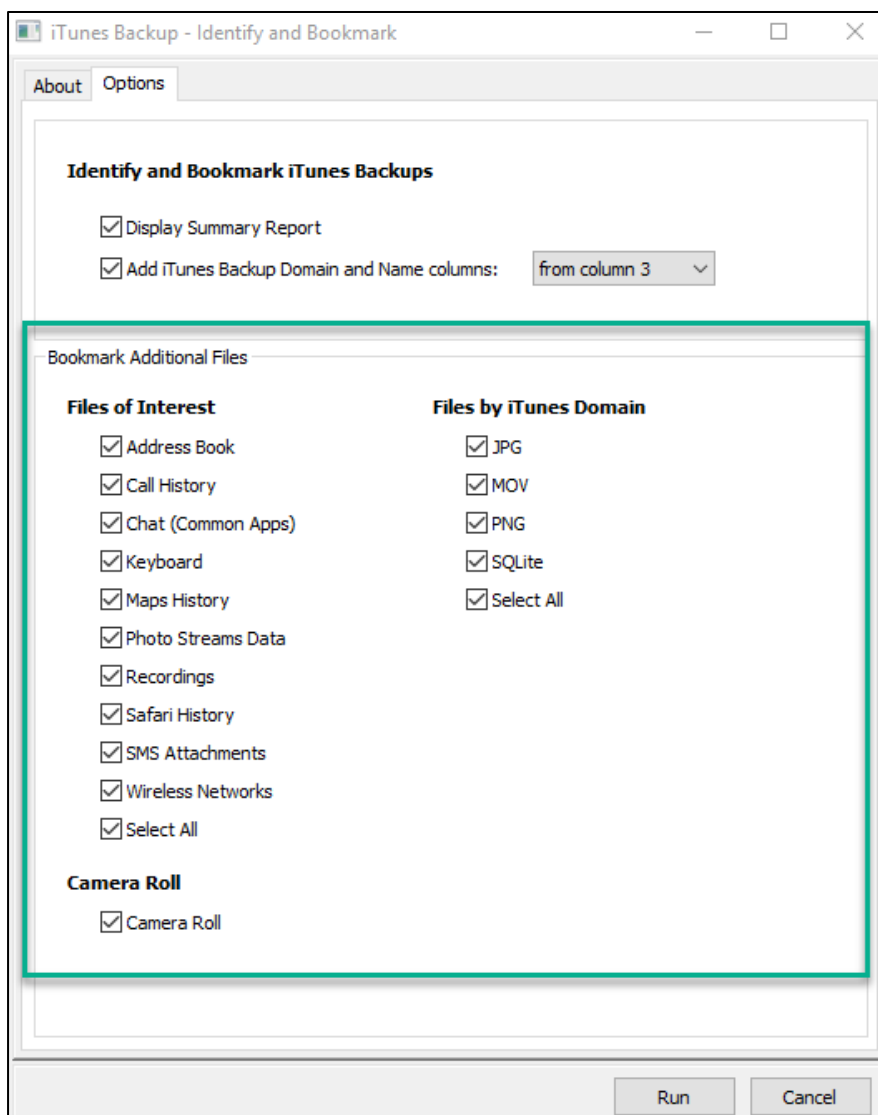
30.1.13 STEP 2 - ITUNES BACKUP ANALYZE

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**:

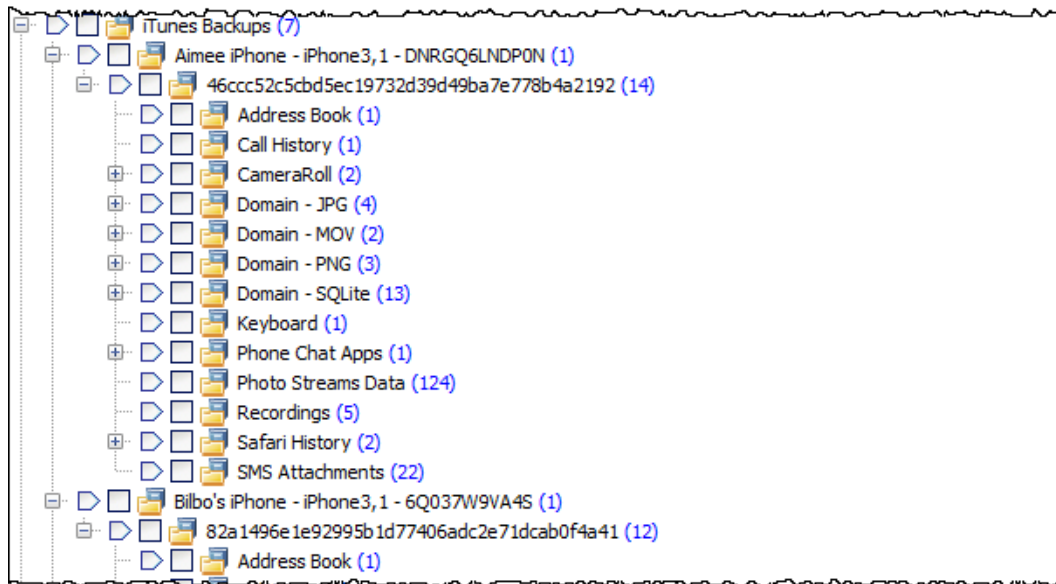
- In the **File System module**, under the **Analysis Programs** button, select **iTunes Backup – Identify and Bookmark**, as shown in Figure 499 above. Select the Files of Interest, files by iTunes Domain and/or Camera Roll in Bookmark Additional Files in below Figure 417:

Figure 504: iTunes Backups – files of interest, by iTunes Domain, camera roll



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 505 below:

Figure 505: Bookmarks module showing output from Analyze iTunes Backups scripts.



The bookmark folders are described in more detail at Appendix 9 – iTunes Backup Files.

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.

Historically investigators have exported iOS backup files to examine their content with third party applications, such as:

- <http://www.sqliteexpert.com/>
- <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:

Figure 506: Examine iOS backup files with Forensic Explorer data views.

File Type	Best Forensic Explorer Data View
SQLite or DB	Display view (shows SQL tables and data rows)
Binary PList	File Metadata view (decoded Plist) or Display view (XML format)
MBDB	HEX or Text view
DAT	HEX or Text view
JPG, PNG, TIF, MOV etc.	Display view

30.1.15 WORKING WITH ENCRYPTED BACKUPS

iTunes provides the option to encrypt backups (as shown in Figure 492 above). During the backup process the user is prompted to enter a password to encrypt all files in the backup.

Figure 507: iTunes encrypted backup password request.



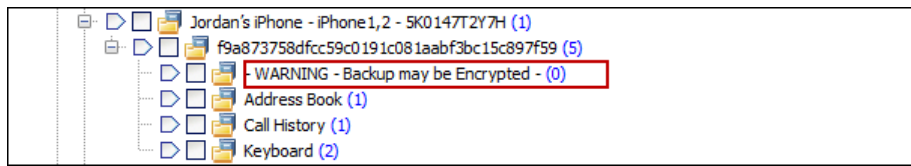
This password is stored within the backup itself to enable access to the backup if the physical device is not present. For more information on password storage see *Forensic Analysis of iPhone Backups, Decrypting Encrypted backups*, reference Satish, B. (20) and (21).

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 508 below:

Figure 508: 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 (22), to locate encrypted backups.

Figure 509: Encrypted iTunes backup identified by Tenorshare iPhone Backup Unlocker

Name	Backup Time	Serial Number
Jordan's iPhone	2015-01-15 18:14:05	3212319KEDG
Mary Thomas idev	2015-01-15 16:59:58	C39GGBGGDTFC
JTH Mistrust iPhone	2015-01-15 19:08:17	82830Z7KY7H
Jordan's iPhone	2015-01-15 17:05:41	5K0147T2Y7H

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> (23) (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.

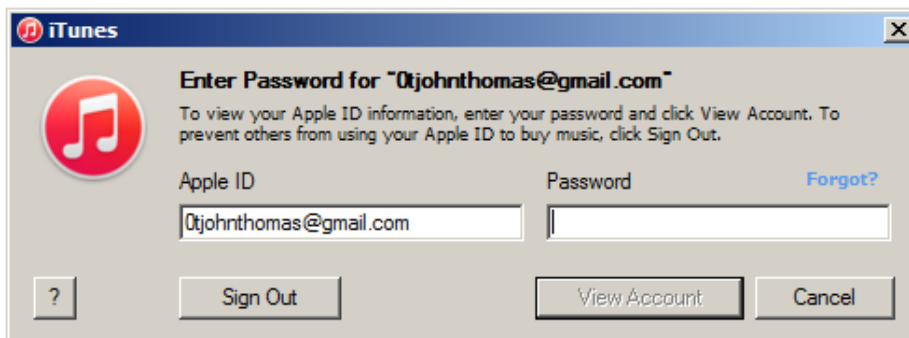
30.1.18 LIVE BOOT

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:

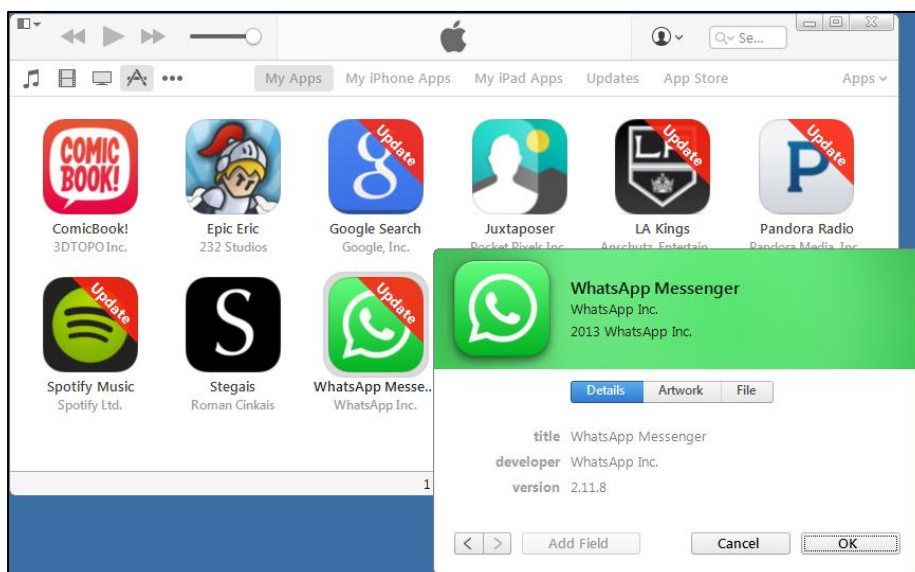
1. iTunes account names and passwords.

Figure 510: iTunes account information in a Live Boot session



2. Applications, including version number information, in the iTunes library:

Figure 511: iTunes Library in a Live Boot session



30.1.19 SHADOW COPY

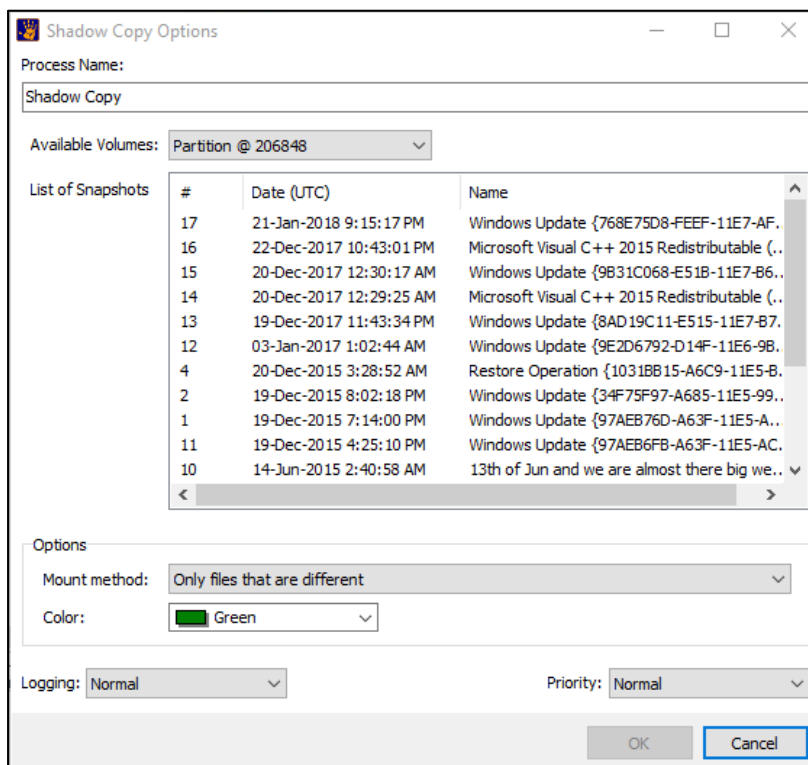
Consideration should be given to Shadow copies (Windows Restore Points) present on the suspect's computer. These Shadow copies may hold historical iTunes backup folders and provide additional information not present in the existing file system.

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:

Figure 512: Shadow Copy options



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 THUMBNAILS

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 Thumbcache (described below). However, it is still possible to locate Thumbs.db files in more recent Microsoft operating systems which are created when viewing remote or mapped drives in Windows Explorer.

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 THUMBNAILS

As Parsonage (2012) observes, “A large proportion of computer users have no knowledge of the presence of Windows thumbnail databases so that whilst they might delete incriminating pictures the evidence of their illicit activity often remains in the thumbnail databases”. (24)

Further suggested references:

- Larson, Troy. Windows 7 Thumbnail Cache. Slideshare. [Online] October 2010 <http://www.slideshare.net/ctin/windows-7-forensics-thumbnaildtr4>
- Hurlbut, Dustin. Thumbs DB Files Forensic Issues. [Online] September 2014 https://ad-pdf.s3.amazonaws.com/wp.Thumbs_DB_Files.en_us.pdf

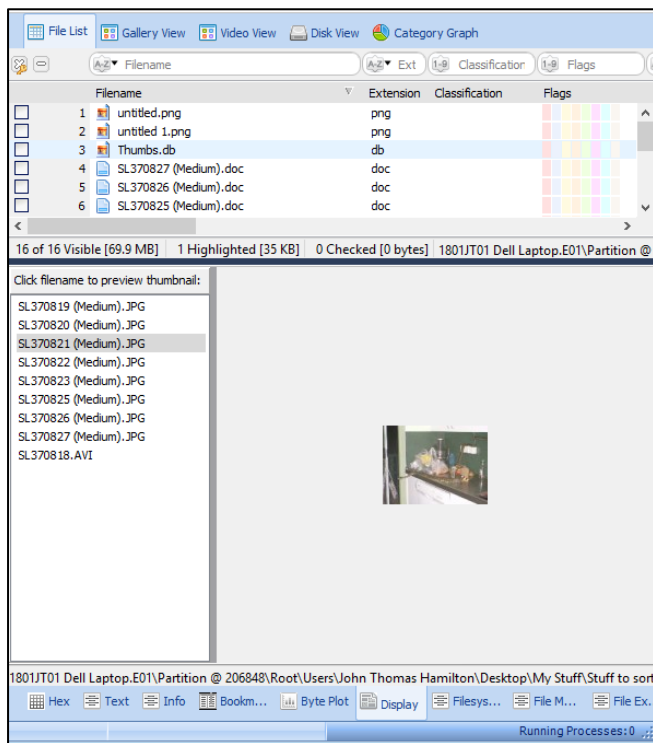
30.2.4 THUMBNAIL IN FORENSIC EXPLORER

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 513 below:

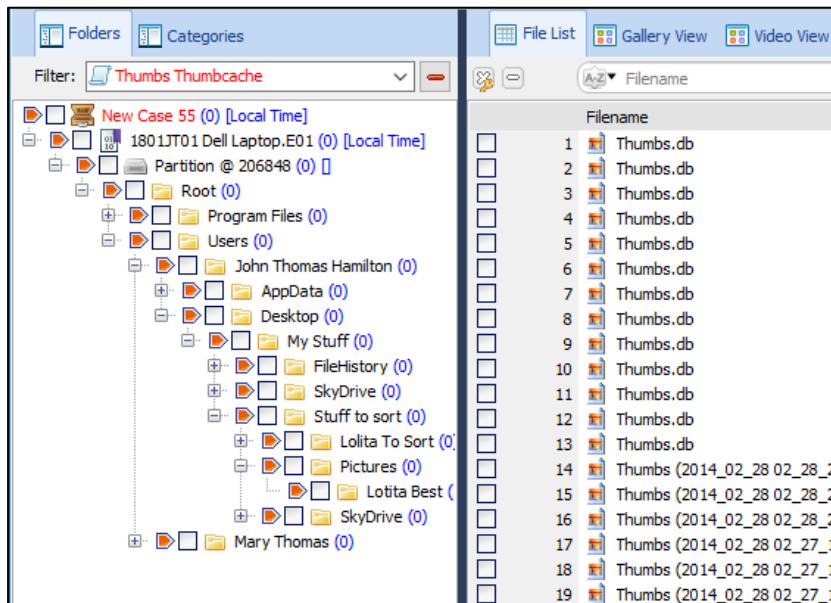
Figure 513: Thumbs.db Display view



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 Thumbscache_XXX.db. A Thumbs.db Folders filter as shown in Figure 514 below:

Figure 514: Folders Thumbs Thumbcache filter applied in the File System module.



The filter code is accessible in the Scripts Module, in the path:

- `Filters\FileSystem\Thumbcache.WindowsEDB.pas`

EXPANDING COMPOUND THUMBNAI-FILES

Thumbnail-Files are **Compound** files because they act as containers for content.

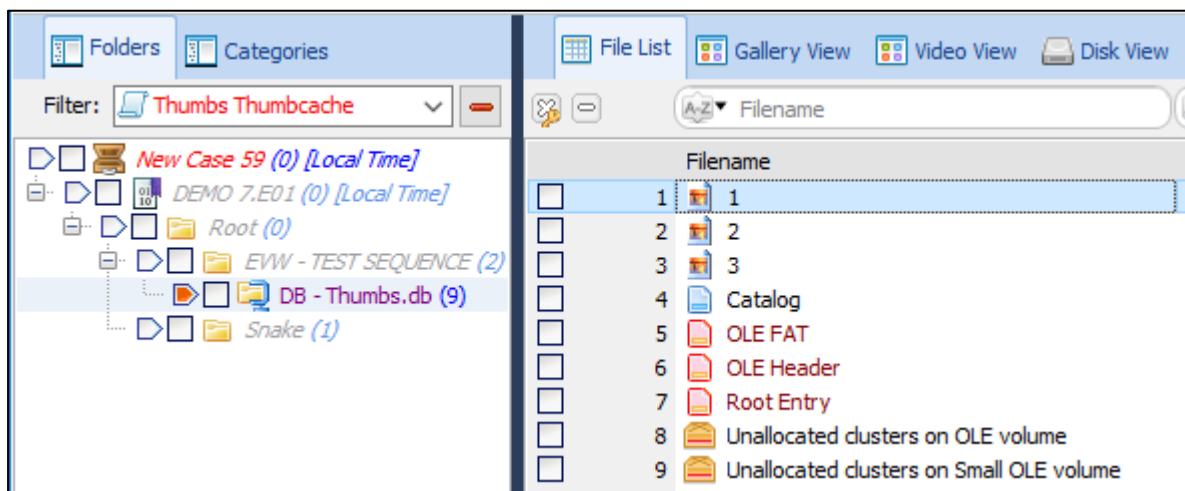
To work with compound files, it is first necessary to identify them as such by running a **Signature Analysis** (a Signature Analysis can be run at any time in the File System module by clicking the Signature Analysis toolbar button). A correctly identified Thumbnail-File will show “**Thumbnail**” or “**ThumbCache**” in the File Signature column when a signature analysis is complete.

EXPAND A SINGLE THUMBNAI-FILE

To **expand a single compound Thumbnail-File**:

1. Run a Signature Analysis (if not already done);
2. Right click on the Thumbnail-File and select **Expand Compound File** from the drop-down menu (if this menu option is not active, run a Signature Analysis).
3. Once expanded, the icon of the Thumbnail-File file will change to the compound file icon. Click on the Thumbnail-File to show the files it contains, as shown in Figure 515 below:

Figure 515: Expanded Thumbs.db file.



EXPAND MULTIPLE THUMBNAIL-FILES

It can be advantageous to expand multiple compound Thumbnail-Files files.

To **expand multiple Thumbnail-Files**:

1. In the File System module, select **Expand Files** icon;

IMPORTANT: For speed purposes, before running the script, turn off any running Folders filter.
2. Select the **Thumbs** 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.

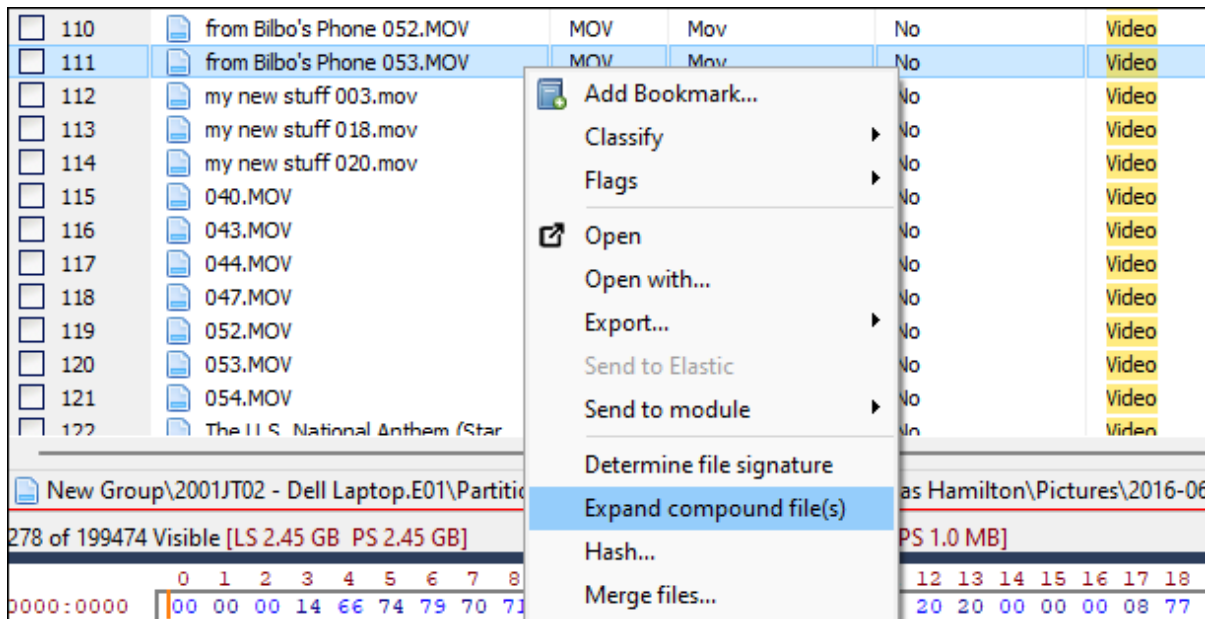
30.3 VIDEO KEY FRAMES (KEYFRAMES)

In animation and filmmaking, a key frame (or keyframe) is a drawing or shot that defines the starting and ending points of a smooth transition. These are called frames because their position in time is measured in frames on a strip of film or on a digital video editing timeline. (https://en.wikipedia.org/wiki/Key_frame, Accessed June 2023). Many software programs have the ability to extract keyframes as a method to represent the visual content of an entire file.

In Forensic Explorer, video keyframes are extracted using:

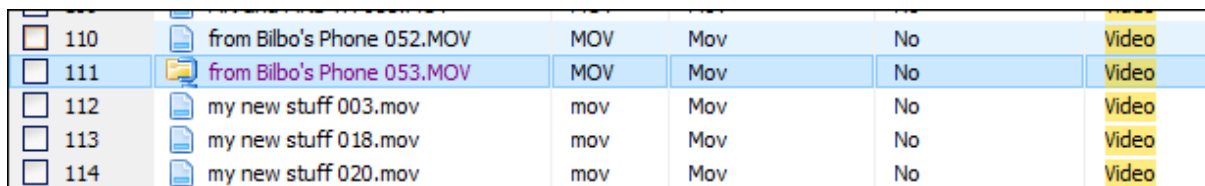
1. The right-click **Expand compound file(s)** menu option.
2. Or the **Expand Files** icon in the toolbar.

Figure 516: Video keyframes, right-click Expand compound files(s).



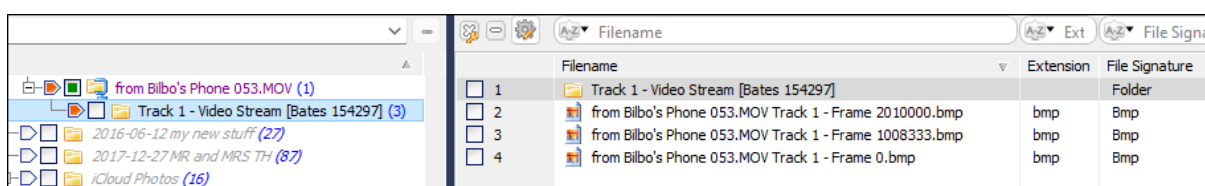
An expanded file will change the icon and color in the **File List** to represent that it is now a container with children (the keyframes).

Figure 517: Video keyframe, expanded file.



A new folder is created in the **Folder Tree** to contain the extracted keyframes as **bmp** files.

Figure 518: Video keyframes.



A similar technique is used to extract **time sliced video frames**, available when running **Expand Files** from the icon the toolbar.

Figure 519: Video keyframes, time slice.



30.4 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 520 and Figure 521 below :

Figure 520: Start Menu, MS Word Automatic Destinations Jump List (Windows 8 shown)

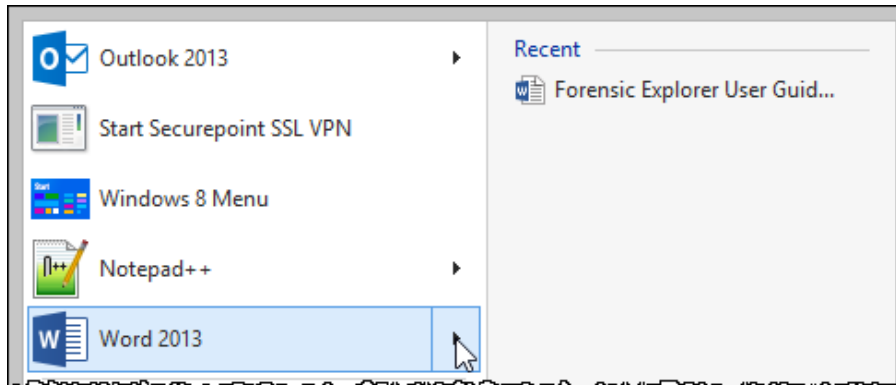
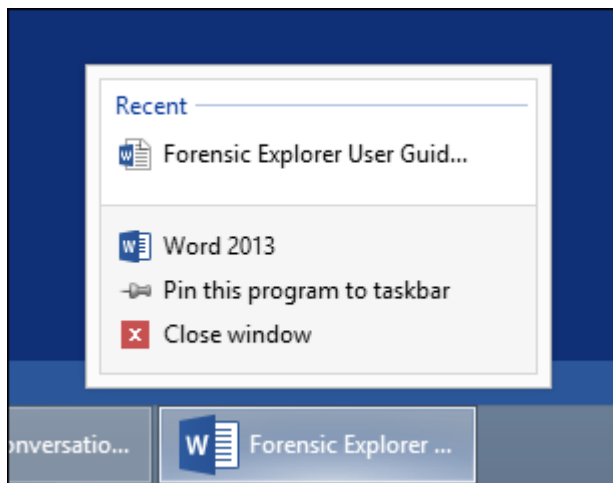


Figure 521: Task bar, MS Word, Automatic Destinations Jump List (Windows 8 shown)



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:\Users\%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:\Users\%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

30.4.1 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 examiners 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.

30.4.2 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;

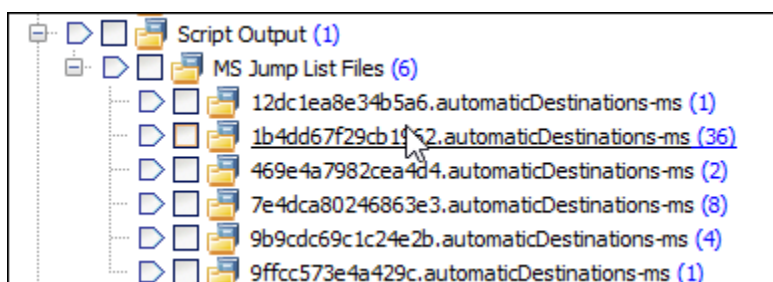
- **Extract MS Jump List** script; or,
- **Bookmark MS Jump List LNK.**

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 522 below:

Figure 522: Bookmarked automaticDestinations Jump List Files



Metadata LNK columns can also be added to the Bookmarks module.

MANUALLY VIEW AUTOMATICDESTINATIONS JUMP LIST METADATA

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 **Expand Files** menu item.

For more information about expanding compound files See 9.6.

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 > Extract Metadata > Extract All Metadata to Columns** to see the embedded metadata fields. These are the fields that are extracted to columns in the automated process.

30.5 UTILIZING 3RD PARTY TOOLS IN FORENSIC EXPLORER

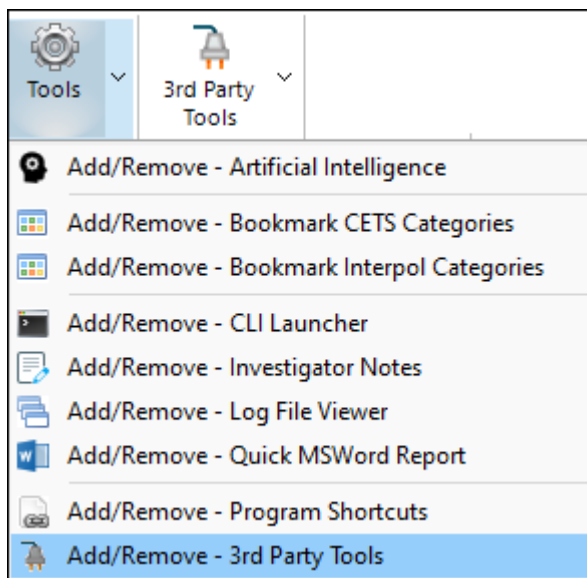
There are many well regarded stand-alone software applications that can be used in computer forensics investigations to process specific artifacts. It is important, where possible, to use multiple tools to corroborate analysis results. In Forensic Explorer, this can be achieved by running **3rd Party Tools**.

30.5.1 ADDING THE 3RD PARTY TOOLS BUTTON TO FORENSIC EXPLORER TOOLBARS

To add 3rd Party Tools to the Forensic Explorer interface:

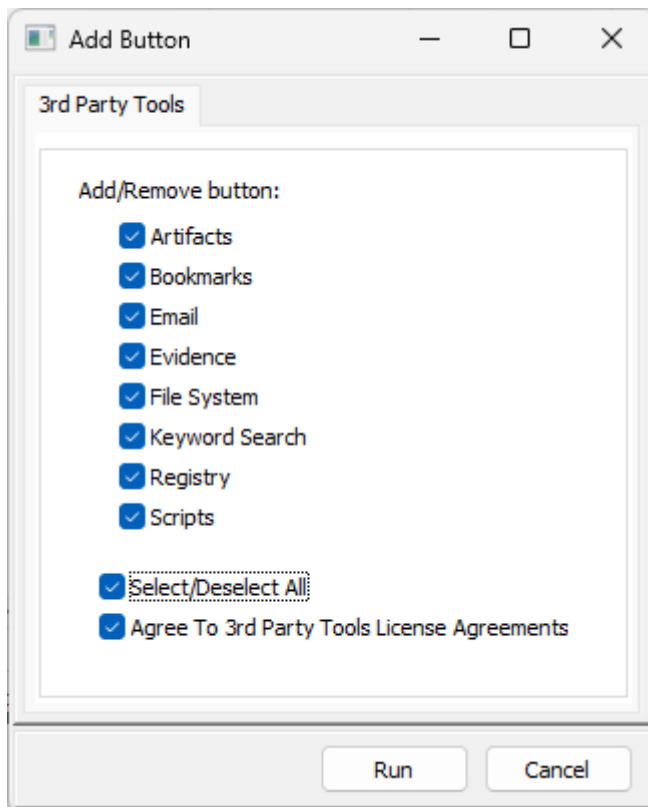
1. Click on the Tools icon in the File System module.
2. Select **Add/Remove – 3rd Party Tools** from the drop-down menu.

Figure 523: Add in the 3rd Party Tools button to the toolbar.



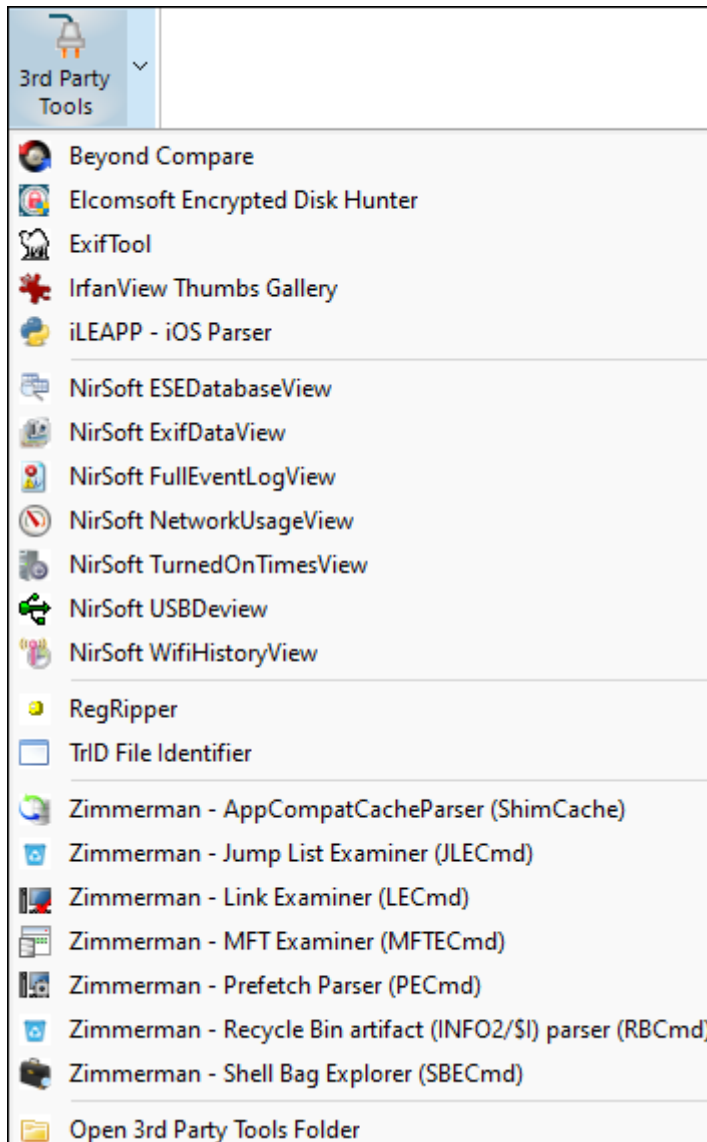
3. Select the Forensic Explorer modules where the 3rd Party Tools button will be displayed.

Figure 524: Select the modules to show the toolbar button.



4. Once the 3rd Party Tools button is added, individual programs are selected from the drop-down menu.

Figure 525: 3rd Party Tools menu.



30.5.2 CONFIGURING 3RD PARTY TOOLS

3rd Party Tools are not distributed with Forensic Explorer. Each tool is independent of Forensic Explorer and has its own license agreement and terms and conditions. By running 3rd Party Tools in Forensic Explorer, the user is accepting and license of the program author.

3RD PARTY TOOLS APPLICATION FOLDER

Individual tools must be downloaded and setup in the Forensic Explorer 3rd Party Tools installation folder, in their respective sub folders.

C:\Program Files\GetData\Forensic Explorer v5\3rd_Party_Tools

IMDISK (RAMDISK)

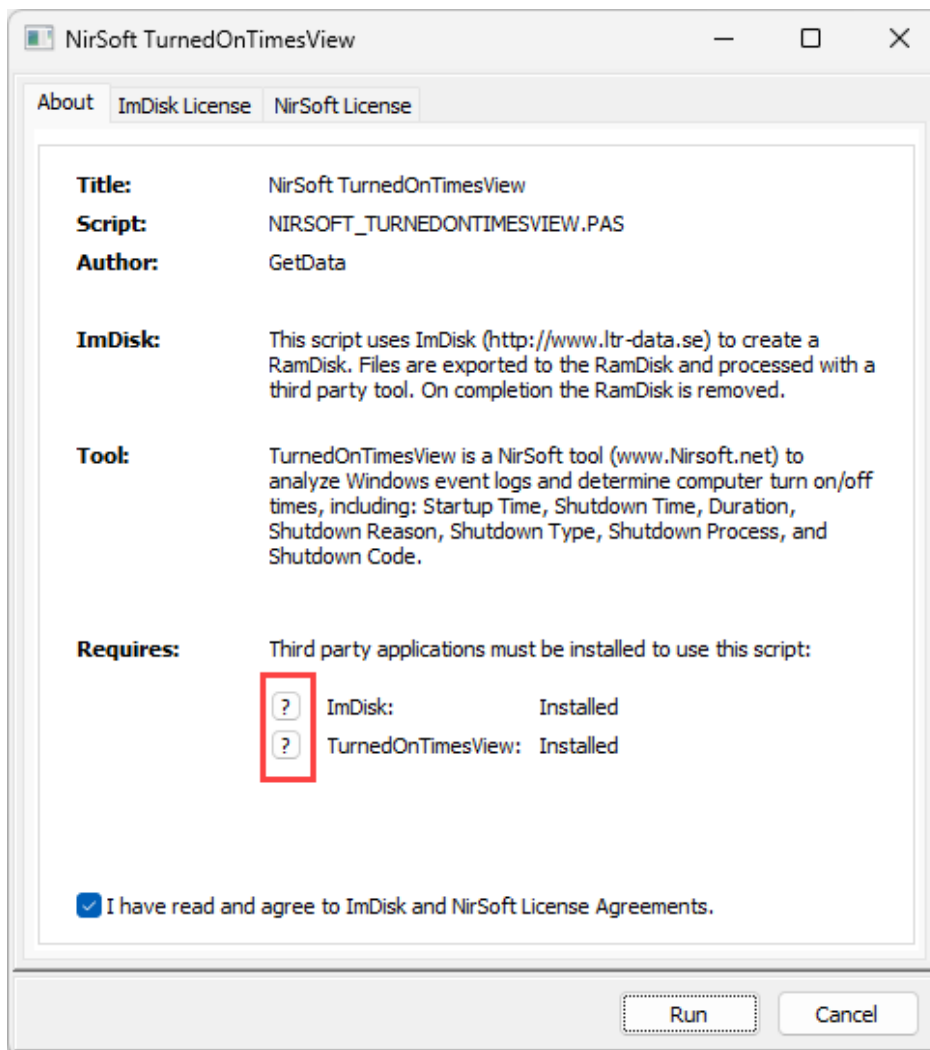
In most cases, the bridge between Forensic Explorer and the 3rd Party Tool is a RAM Disk. Forensic explorer uses ImDisk, a free Virtual Disk Driver created by Olof Lagerkvist. A RAM Disk is a block of random-access memory that a computer's software treats as if it were a disk drive. When a 3rd Party Tool is run in Forensic Explorer:

1. A Forensic Explorer script:
 - a. Locates relevant files in the case.
 - b. Creates a RAM Disk and exports the relevant files to the RAM Disk.
 - c. Executes the 3rd Party Application and directs it to process the files on the RAM Disk.
 - d. Closes the RAM Disk.

30.5.3 LAUNCHING 3RD PARTY TOOLS

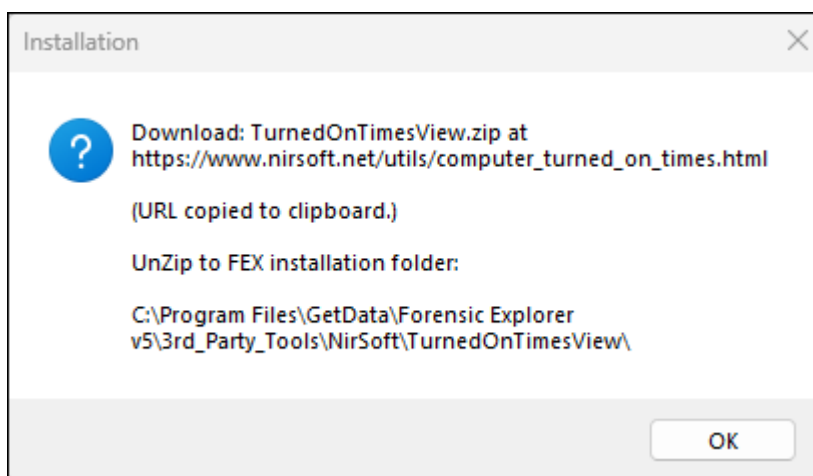
When a 3rd Party Tool is launched in Forensic Explorer, the following window will appear:

Figure 526: NirsoftTurnedOnTimesView



This identifies if ImDisk and the 3rd Party Tool are installed. Additional information is available by clicking on the help button, which gives specific download information:

Figure 527: 3rd Party Tool configuration information.



30.5.4 3RD PARTY TOOL RESULT

3rd Party Tool results depend on the application used. Some tools run the GUI of the application, and results are saved using that application. Other tools pipe output to text or csv files, which are saved in the Forensic Explorer case.

Chapter 31 – FEX Viewer

In This Chapter

CHAPTER 31 – FEX VIEWER

31.1	FEX Viewer	509
31.1.1	FEX Viewer System Requirements	509
31.1.2	FEX Viewer Download and installation	509

31.1 FEX VIEWER

FEX Viewer is a free program that allows a third party to open and review a Forensic Explorer Case (created by Forensic Explorer, CLI, or Triage). It is intended to be used by case officers, other investigators, prosecutors, etc. without the need to tie up a Forensic Explorer license.

FEX Viewer is a **simplified version of Forensic Explorer**. It is intended that a forensic investigator will have **prepared the FEX Viewer case** by running relevant processing, such as signature analysis, triage, metadata extraction, carving, keyword search, artifact extraction etc.

FEX Viewer enables the reviewing party to:

- Open and review an existing FEX case including bookmarks and search results.
- Run new keyword searches.
- Search existing, or create new DTSearch indexes.
- Create new bookmarks and reports.
- Save new results to the case.

31.1.1 FEX VIEWER SYSTEM REQUIREMENTS

FEX Viewer is a stand-alone program. It does **not require Forensic Explorer** to be installed on the same computer.

FEX Viewer is a 64-bit app. Minimum recommended system requirements are: i7, 16 GB RAM, Windows 11.

31.1.2 FEX VIEWER DOWNLOAD AND INSTALLATION

Download FEX Viewer at <https://getdataforensics.com/product/fex-viewer/>. Follow the on-screen installation steps. **No product activation is required.**

The default **program installation folder** is: *C:\Program Files\GetData\Forensic Explorer Viewer v5*

The default **working folder** is: *C:\Users\[username]\Documents\Forensic Explorer Viewer v5*

31.1.3 FEX VIEWER USAGE

There are two different methods to deploy FEX Viewer to examine case data:

1. **A FEX Viewer Case**

An entire Forensic Explorer case (including all source forensic image files) is provided to the third party to be opened and examined in FEX Viewer.

2. **A FEX Viewer Portable Case**

A selection of data (e.g. checks or books) is provided to the third party. It can be opened by FEX Viewer, or an embedded and self contained 'portable' version of FEX Viewer.

31.2 FEX VIEWER CASE

A FEX Viewer case is where an entire Forensic Explorer case (including all source forensic image files) is provided to the third party to be opened and examined using an installed FEX Viewer.

31.2.1 PREPARING A FEX VIEWER CASE IN FORENSIC EXPLORER

This section is currently being updated.

31.3 FEX PORTABLE CASE

A Forensic Explorer Portable Case is where the forensic investigator prepares a selection of files (e.g. checks or bookmarks) to be provided to the third party. The case can either be opened by an installed FEX Viewer, or, FEX Viewer can be embedded within the case so that it operates as a fully self contained 'portable' case that can be launched independently from USB media without the need for any other software.

31.3.1 PREPARING A PORTABLE CASE IN FORENSIC EXPLORER

A portable case is created for selected items.

Items can be selected by **Category**:

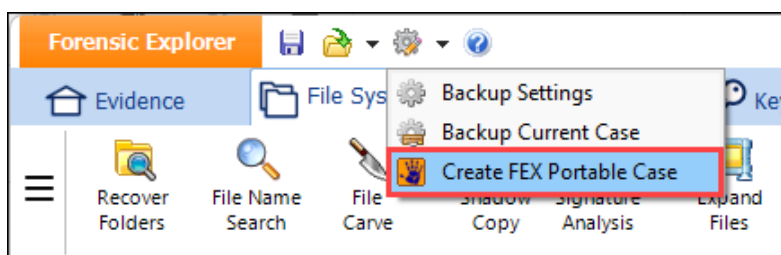
- Artifacts
- Bookmarks
- Documents
- Emails & Attachments
- Graphics
- Videos & Multimedia

Or by **checked items** in Forensic Explorer **modules**:

- Artifacts
- Bookmarks
- Email
- File System
- Keyword Hits
- Registry

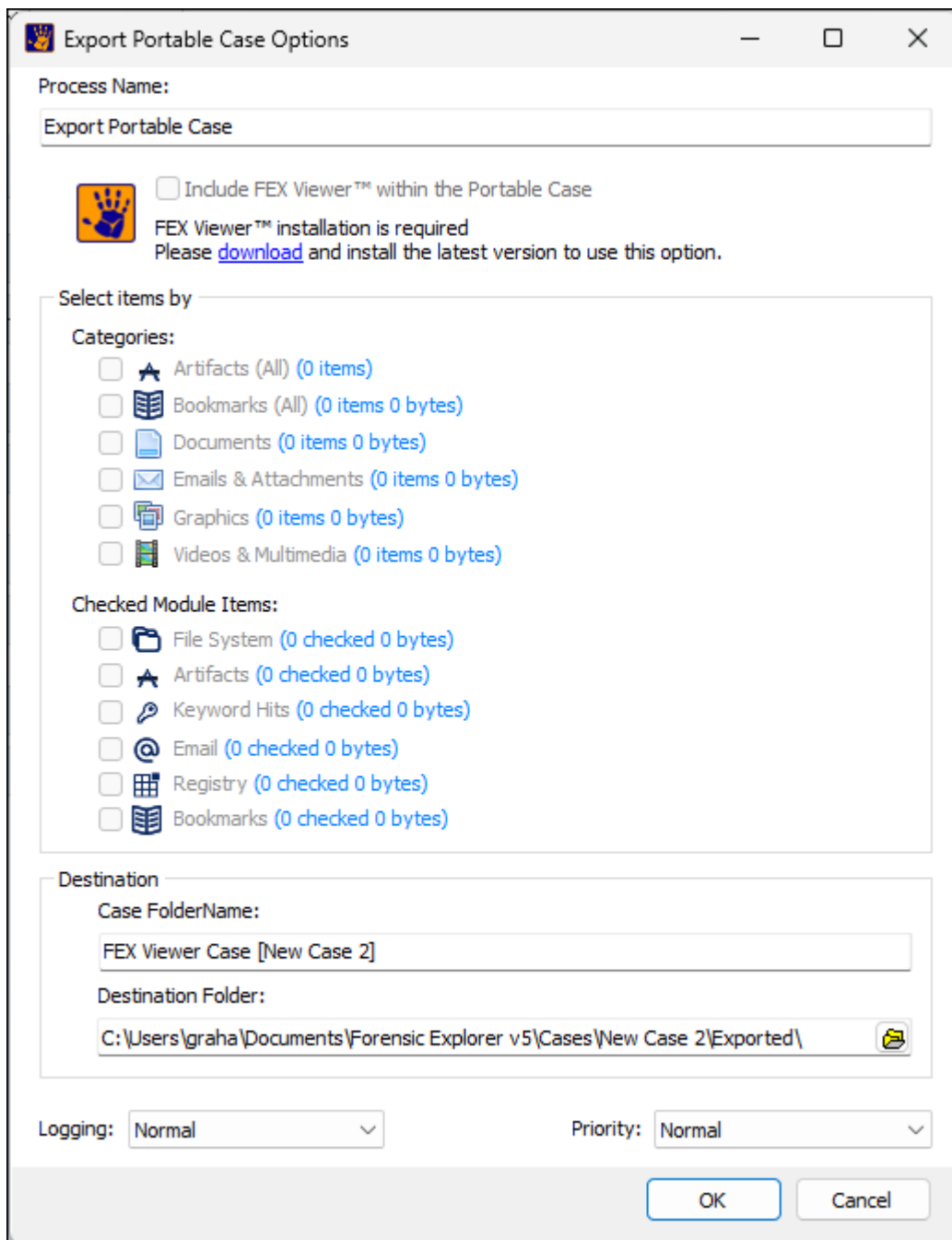
Once items are checked, select the global cog button at the top of Forensic Explorer > **Create FEX Portable Case**:

Figure 528: Create Portable Case



. The following window will display:

Figure 529: Export Portable Case Options



This section of the manual is currently being updated. Check back soon.

Chapter 32 – FEX Automated Analysis

In This Chapter

CHAPTER 32 – FEX AUTOMATED ANALYSIS

32.1	Automated Analysis.....	515
32.2	Graphics Analysis	516
32.2.1	Graphics Analysis – Bookmark	518
32.3	Face Recognition.....	519
32.3.1	Ramdisk (ImDisk virtual disk driver for Windows).....	520
32.3.2	Processing.....	521

32.1 AUTOMATED ANALYSIS

IMPORTANT:

GetData Forensics products include software to assist in the automated analysis and investigation of digital content, including graphics files. It is important to note that while software algorithms strive to accurately predict the content of files, there are inherent limitations and uncertainties associated with such predictions.

The accuracy of predictions may be influenced by various factors, including but not limited to the complexity of the graphics file, the presence of encryption or compression, and the quality of the data being analyzed. Additionally, advancements in technology and changes in file formats may impact the performance of algorithms over time.

Users should exercise caution and consider predictions as supplementary information rather than conclusive evidence. It is crucial to rely on a combination of insights, traditional forensic methodologies, and expert analysis to make informed decisions in the context of digital investigations.

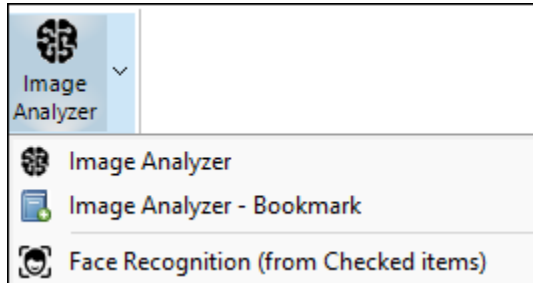
GetData Forensics cannot guarantee the absolute accuracy of predictions, and users should interpret results with awareness of the inherent uncertainties in automated analysis. Our tools are designed to aid professionals in their investigative processes, and users are encouraged to exercise due diligence and critical judgment when interpreting the results generated by our software.

By using GetData Forensics tools, users acknowledge and accept the inherent limitations of automation software in predicting the content of graphics files and agree to use the information provided by our tools responsibly and in conjunction with other investigative techniques.

32.2 GRAPHICS ANALYSIS

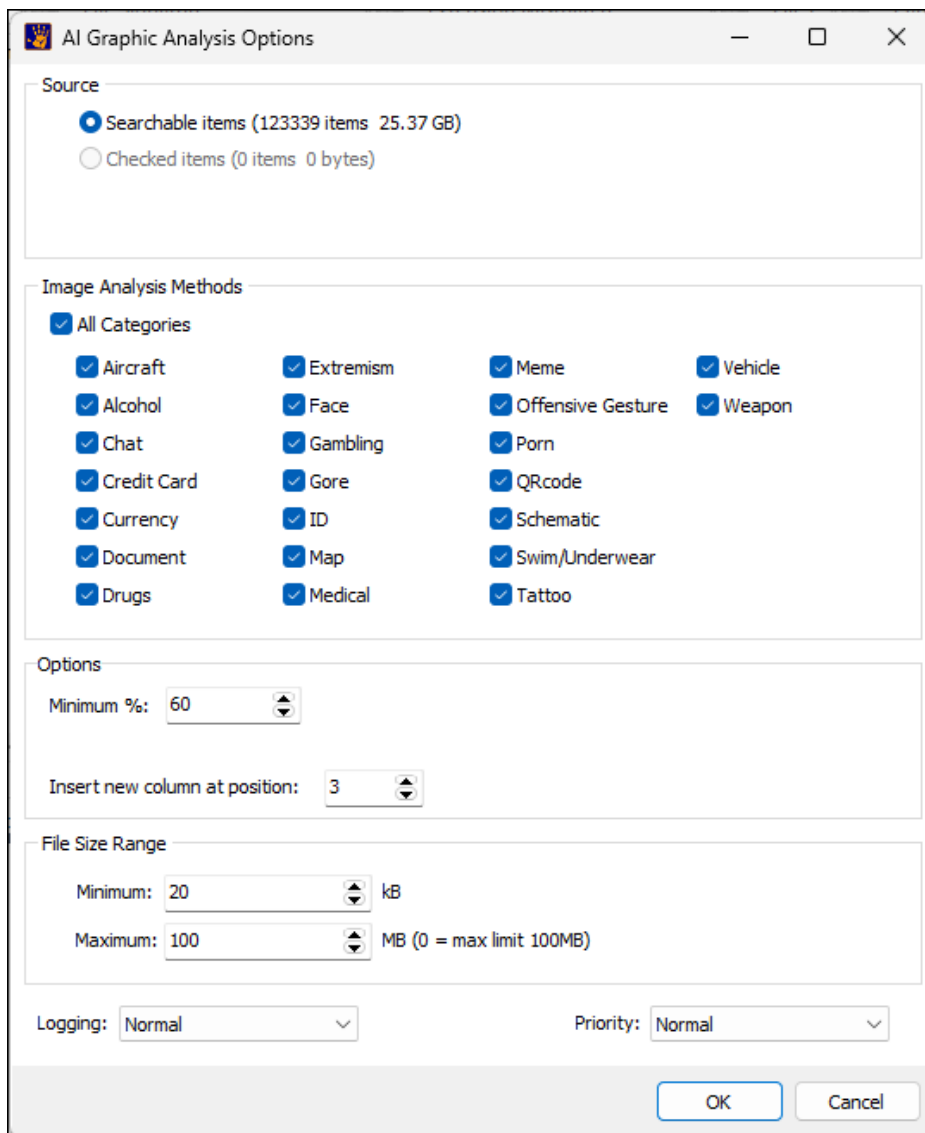
Graphics Analysis can be run from the File System and Email modules from the Graphics Analysis button:

Figure 530: Graphics Analysis



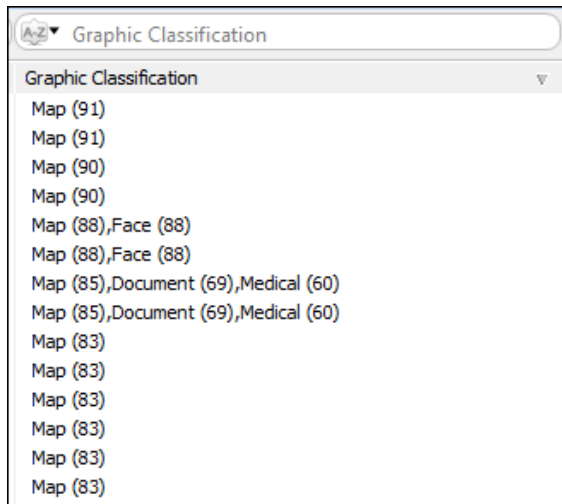
Selecting **Graphics Analysis** from the menu will present the following window:

Figure 531: Graphics Analysis



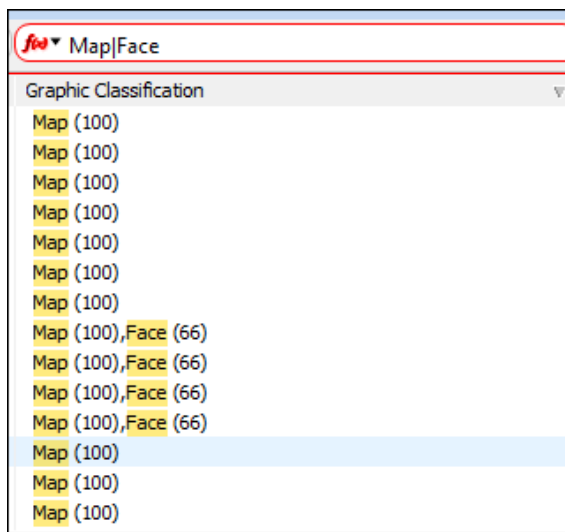
Graphics will be analyzed according to the checked categories. A classification score (above the threshold set in the Options > Minimum field), will be written to the **Graphic Classification** column. If a graphic matches multiple categories, additional categories are appended to the column.

Figure 532: Graphics Analysis > Graphic Classification column score



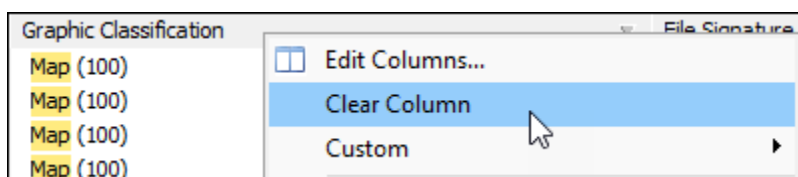
Filter the **Graphic Classification** using the various filter options available (Regex shown below – Tip: Use ChatGPT to easily create more complex regex statements):

Figure 533: Graphics Classification regex filter



To **clear** the **Graphics Classification** column, right-click in the column header and **Clear Column**:

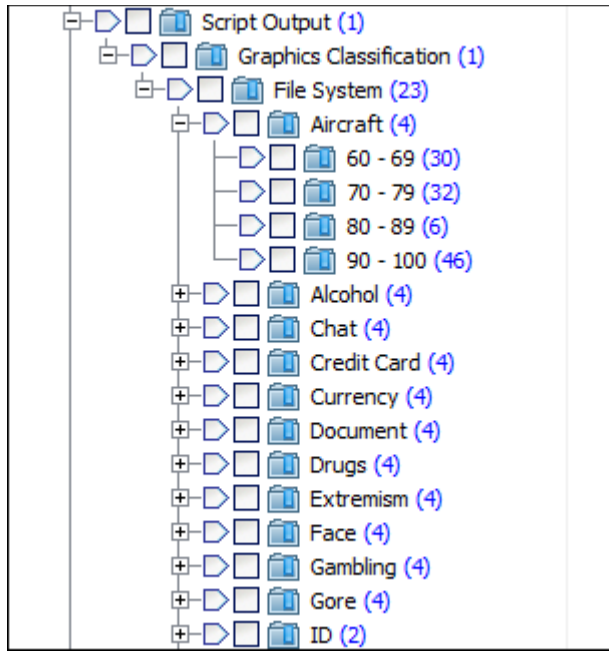
Figure 534: Clear Column



32.2.1 GRAPHICS ANALYSIS – BOOKMARK

The **Graphics Analysis– Bookmark** menu item (shown in Figure 530 above) will bookmark graphics classifications based on the information in the **Graphics Classification** column. Bookmarks will be in increments of 10 according to the classification score:

Figure 535: Graphics Analysis – Bookmark of the Graphics Classification column



32.3 FACE RECOGNITION

Face recognition is the process of machine one face against another.

Face Recognition is performed in **Forensic Explorer** using a stand-alone command line executable, FEX-AI.exe. FEX-AI.exe is powered by **TensorFlow**, a free and open-source software library for machine learning. TensorFlow was developed by the Google Brain team for internal Google use in research and production. (<https://en.wikipedia.org/wiki/TensorFlow>, accessed December 2022).

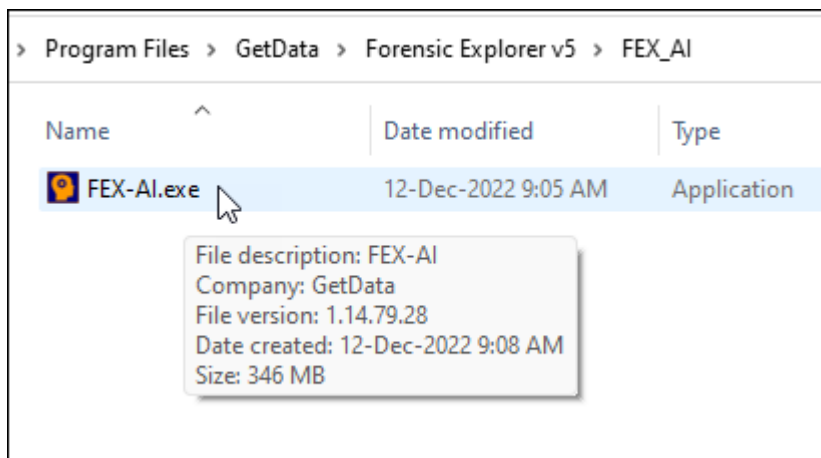
In machine learning, a **model** is a function with learnable parameters that maps an input to an output. The optimal parameters are obtained by training the model on data. A well-trained model will provide an accurate mapping from the input to the desired output. (https://www.tensorflow.org/js/guide/models_and_layers, accessed December 2022). Unless otherwise stated the models used by Forensic Explorer are licensed under Apache 2.0.

FEX-AI.exe was introduced in version 5.5.8.3386 and above and is included with a standard installation in the default folder path:

C:\Program Files\GetData\Forensic Explorer v5\FEX_AI

Launching FEX-AI.exe from the executable will provide version number information, as shown in Figure 536 below:

Figure 536: FEX-AI.exe Installation Path



32.3.1 RAMDISK (IMDISK VIRTUAL DISK DRIVER FOR WINDOWS)

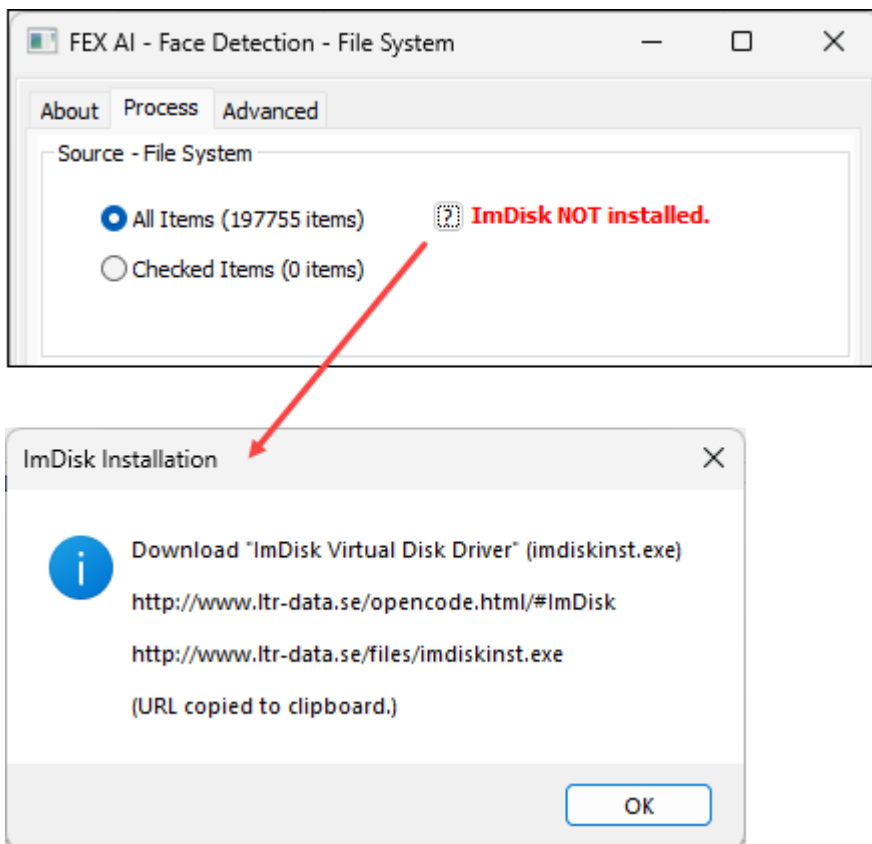
FEX-AI.exe uses a third-party RAM disk program **ImDisk** (a virtual disk driver for Windows) to export and process files. You must agree to the ImDisk license agreements to use this software.

Website: <http://www.ltr-data.se/opencode.html/#ImDisk> or
<https://sourceforge.net/projects/imdisk-toolkit>

Installation: <http://www.ltr-data.se/files/imdiskinst.exe>

If ImDisk is not installed the following message will appear:

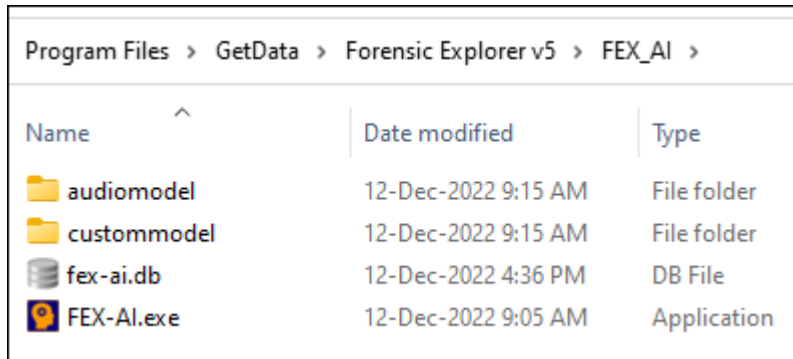
Figure 537: ImDisk not installed.



32.3.2 PROCESSING

FEX-AI.exe creates and updates a **sqlite database**. This database is in the same folder as fex-ai.exe, i.e.:
C:\Program Files\GetData\Forensic Explorer v5\FEX_AI\fex-ai.db

Figure 538: SQLite database, fex-ai.db.



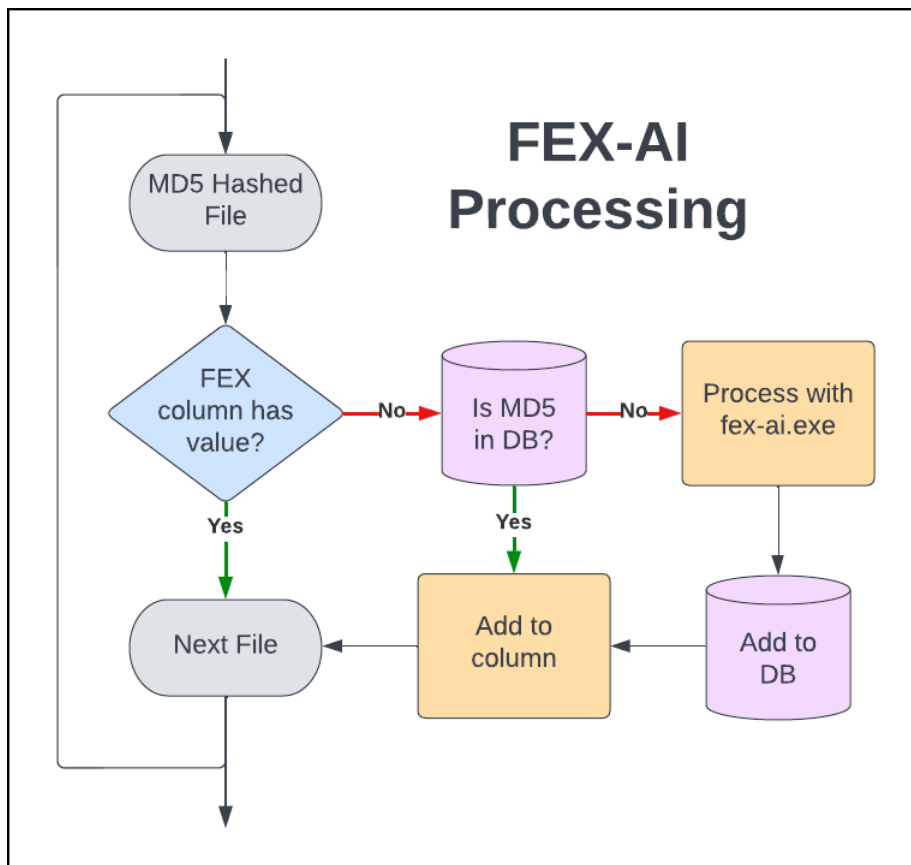
Name	Date modified	Type
audiomodel	12-Dec-2022 9:15 AM	File folder
custommodel	12-Dec-2022 9:15 AM	File folder
fex-ai.db	12-Dec-2022 4:36 PM	DB File
FEX-AI.exe	12-Dec-2022 9:05 AM	Application

The primary functions of the database are:

1. Improve processing speed.
2. To enable information transfer between cases.

FEX automated analysis processing is summarized as follows:

Figure 539: FEX-AI.EXE processing overview.



Database information is accessible from the **Advanced** tab, including:

- The number of unique files (by MD5) in the database.
- The number of unique files processed for data types (faces, license plates, objects, weapons).
- The number of unique files where those data types have been found.

Open Database Folder:	A shortcut to the database folder.
Open Database:	Opens the database in an associated application (e.g., DB Browser for SQLite).
Backup Database:	Copies the database to a sub-folder titled with the date/time of the backup.
Show CMD Window:	Makes the fex-ai.exe processing window visible to the end user.
Clear Column:	Clears the associate column data.

Face Recognition is used to identify pictures containing specific individuals.

IMPORTANT: Face recognition compares a **checked picture** with **each other picture in the case**. Adding multiple source files can **extend processing time**. Consider the following:

- Keep checked source files to a minimum.
- Run Face Detection first (faster) so that files with no faces can be ignored.
- Use quality checked source files with a single clear image.
- Custom name source files by individually adding them to the case.

Figure 540: Face Recognition showing checked source file.

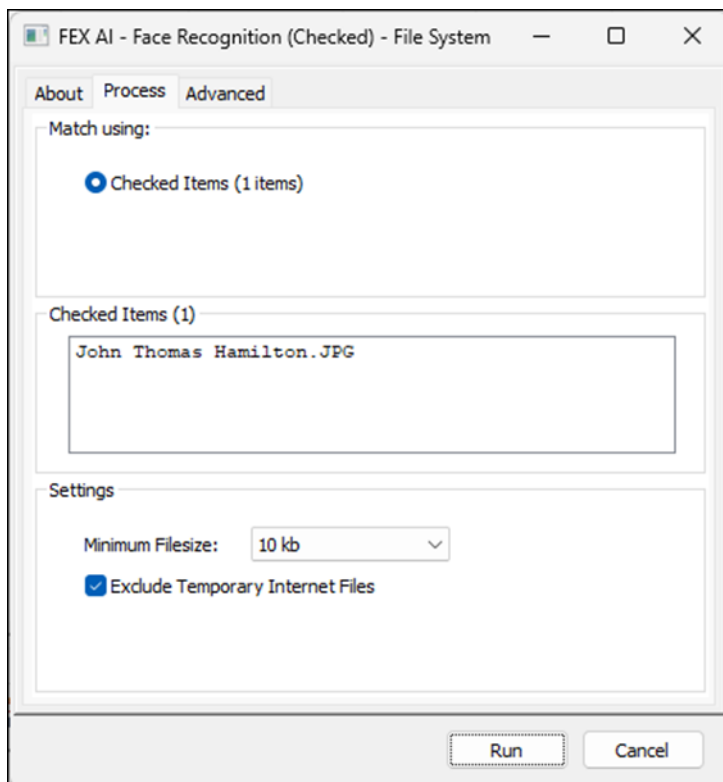
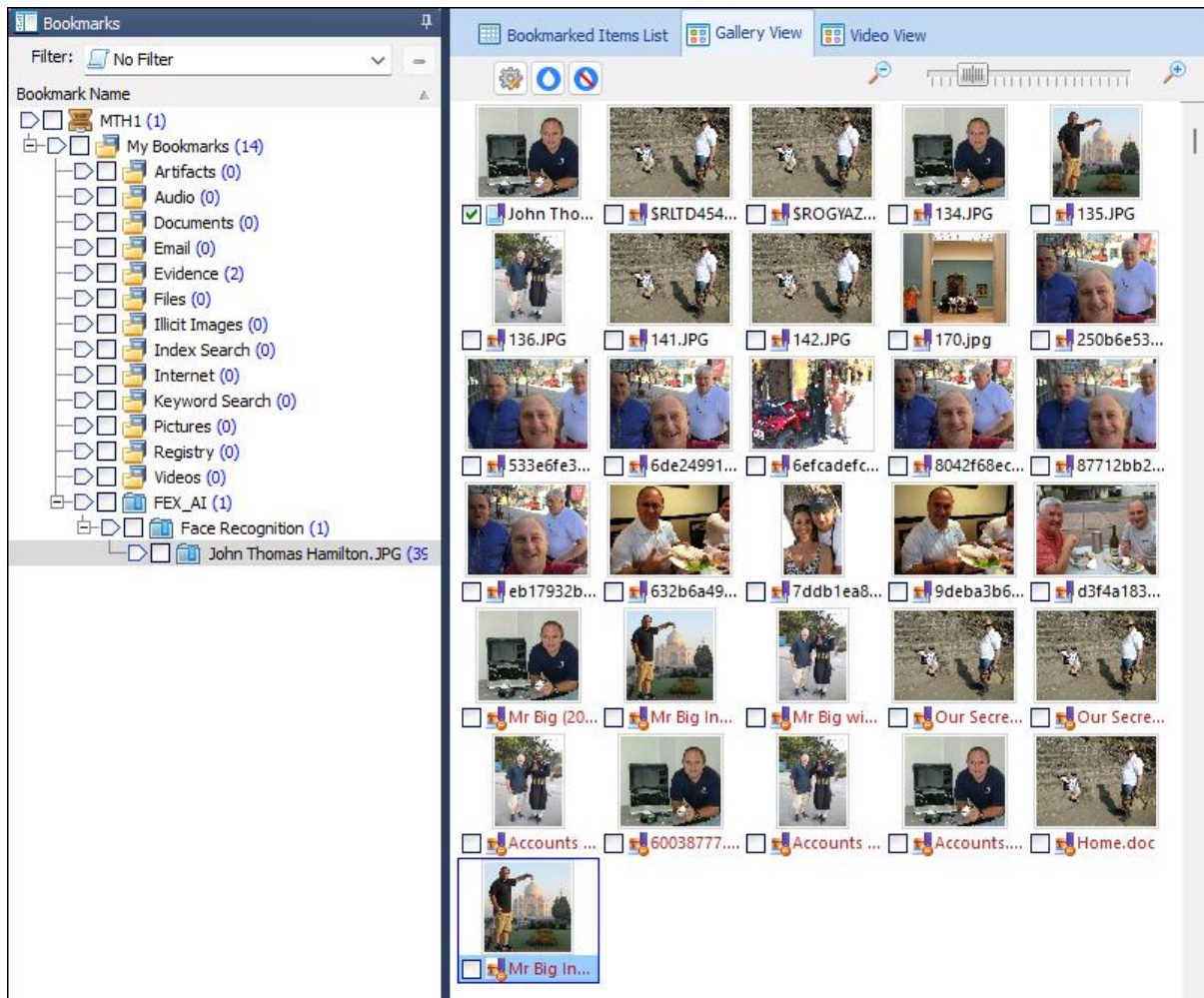


Figure 541: Output of Face Detection in Bookmarks module.



Chapter 31 - Legal

In This Chapter

CHAPTER 33 - LEGAL

33.1	This User Guide.....	526
33.2	Copyright	526
33.3	License agreement.....	527

33.1 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, <https://getdataforensics.com/> for the latest version of the software and documentation.

33.2 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/>).

33.3 LICENSE AGREEMENT

GetData® Forensics Pty Ltd (“GetData”) – ACN: 143458039

IMPORTANT – END USER LICENSE AGREEMENT

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT (“AGREEMENT”) CAREFULLY BEFORE USING FORENSIC EXPLORER (“the SOFTWARE”). BY USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND TO THE TERMS AND CONDITIONS OF THIS LICENSE SET OUT BELOW. IF YOU DO NOT AGREE TO BE BOUND BY THE TERMS AND CONDITIONS SET OUT BELOW, DO NOT INSTALL AND/OR USE THE SOFTWARE. PLEASE TERMINATE INSTALLATION IMMEDIATELY AND DO NOT USE THE SOFTWARE.

1. Software Covered by This License

- 1.1. This license agreement applies only to the version of the Forensic Explorer software package with which this agreement is included. Different license terms may apply to other software packages from GetData and license terms for later versions of Forensic Explorer may also be changed.

2. General

- 2.1. GetData is and remains the exclusive owner of the Software. You acknowledge that copyright in the Software remains at all times with GetData.
- 2.2. The Software and any other materials included under this license, are licensed, not sold to you by GetData for use only under the terms of this Agreement.
- 2.3. GetData or its licensors own the Software, including all materials included with this package. GetData owns the names and marks of ‘GetData,’ and ‘Forensic Explorer’ under copyright, trademark and intellectual property laws and all other applicable laws.

3. Permitted License Uses and Restrictions

- 3.1. Subject to the terms and conditions of this License, a single License of the Software permits you to run a single Licensed instance of the Software. Where multiple Licenses have been purchased, the License permits you to run concurrent instances of the Software equal to the number of Licenses purchased.
- 3.2. You are solely responsible for the protection of your data, your systems and your hardware used in connection with the Software. GetData will not be liable for any loss or damage suffered from the use of the Software.
- 3.3. You and others are not permitted to copy (except as expressly permitted by this Agreement), decompile, reverse engineer, disassemble, attempt to derive the source code of, decrypt, modify (except to the extent allowed in the documentation accompanying this Agreement) or remove or alter any proprietary legends contained in the Software.
- 3.4. You are not permitted to share the product activation information provided to you for this Software with other users.
- 3.5. You may not publicly display the Software or provide instruction or training for compensation in any form without the express written permission of GetData.
- 3.6. GetData reserves the right to check any and all license details at any time in any reasonable manner.
- 3.7. GetData may from time-to-time revise or update the Software and may make such revisions or updates available to you subject to payment of the applicable license fee.

3.8. The Software is protected under United States law and international law and international conventions and treaties. You may not rent, lease, lend, sell, redistribute, or sublicense the Software without the express written permission of GetData.

3.9. If you purchase a site license, there will be terms and conditions listed in the appendix of the site license.

4. Disclaimer of Warranty

4.1. To the extent not prohibited by applicable law, by using the Software, you expressly agree that all risks associated with performance and quality of the Software is solely held by you. GetData shall not be liable for any direct, indirect, special or consequential damages arising out of the use or inability to use the software, even if GetData has been advised of the possibility of such damages.

4.2. To the extent not prohibited by applicable law, the Software is made available by GetData 'As Is' and 'With all Faults,' GetData or any GetData authorised representative does not make any representations or warranties of any kind, either expressly or implied concerning the quality, safety, accuracy 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.

4.3. GetData or any GetData authorised representative makes no representations or warranties as to the truth, accuracy or completeness of any information, statements or materials concerning the Software.

4.4. No oral or written information or advice given by GetData or a GetData authorised representative shall create a warranty. Should the Software prove defective, you assume the entire cost of all necessary servicing, repair or correction. Some jurisdictions do not allow the exclusion of implied warranties or limitations on applicable statutory rights of a consumer, the above exclusions and limitations may not apply to you.

5. Limitation of Liability

5.1. To the extent not prohibited by applicable law, in no event will GetData, its officers, employees, affiliates, subsidiaries or parent organisation be liable for any direct, indirect, special, incidental, exemplary, consequential or punitive damages whatsoever relating to the use of the Software.

5.2. Any and all data obtained from the use of the Software becomes the user's sole responsibility and liability.

5.3. Any and all data obtained from the use of the Software in any civil or criminal jurisdiction that results in wrongful conviction, erroneous charges, misrepresentation of data or death or any other civil or tortious wrong against a person, company, corporation or any other entity, GetData shall bear no liability for any death, wrongful conviction or any other civil or tortious wrong against a person, company, corporation or any other entity.

5.4. Any and all data obtained from the use of the Software is the sole responsibility of the user. In the event the user misconstrues, misinterprets or misunderstands the data and causes it to be used in any and all civil or criminal jurisdictions, GetData shall bear no liability.

5.5. In no event will GetData's liability to you, whether in contract, tort (including negligence) or otherwise, exceed the amount paid by you for the License under this Agreement.

5.6. In the event that a company bearing the name of GetData operating as a separate legal entity, leases the Software to you, and you misconstrue, misinterpret or misunderstand the data that results in any wrongful conviction, erroneous charges, misrepresentation of data, death or any other civil or tortious wrong against a person, corporation or any other entity, GetData ACN: 143458039 shall bear no liability to you, the liability shall be borne by whatever company bearing the name of GetData operating as a separate legal entity.

6. Applicable Law

- 6.1. This Agreement and any dispute relating to the Software or to this Agreement shall be governed by the laws of the State of New South Wales and the Commonwealth of Australia, without regard to any other Country or State choice of law rules.
- 6.2. You agree and consent that jurisdiction and proper venue for all claims, actions and proceedings of any kind relating to GetData or the matters in this Agreement shall be exclusively in Courts located in NSW, Australia. If any part or provision of this Agreement is held to be unenforceable for any purpose, including but not limited to public policy grounds, then you agree that the remainder of the Agreement shall be fully enforceable as if the unenforced part or provision never existed. There are no third-party beneficiaries, or any promises, obligations or representations made by GetData therein.

7. Export

- 7.1. You acknowledge that the Software is subject to Australian export jurisdiction. You agree to comply with all applicable international and national laws that apply to the Software including destination restrictions issued by GetData.

8. Termination

- 8.1. This Agreement is effective on the date you receive the Software and remains effective until terminated. If you fail to comply with any and all terms set out above, your rights under this Agreement will terminate immediately without notice from GetData. GetData may terminate this Agreement immediately should any part of the Software become or in GetData's reasonable opinion likely to become the subject of a claim of intellectual property infringement or trade secret misappropriation. Upon termination, you will cease use of and destroy all copies of the Software under your control and confirm compliance in writing to GetData.

9. Entire Agreement

- 9.1. This Agreement constitutes the entire Agreement between you and GetData relating to the Forensic Explorer Software herein. This Agreement supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgement or other communication between the parties relating to its subject matter during the term of this Agreement. No modification, amendment or addendum to this Agreement will be binding, unless it is set out in writing and signed by an authorised representative of each party.

10. Translations

- 10.1. This agreement is translated into other languages. It is the English version which is the language that will be controlling in all respects. No version of this agreement other than English shall be binding or have any effect.

Appendix 1 - Technical Support

APPENDIX 1 - TECHNICAL SUPPORT

GetData Forensics Pty Ltd has its headquarters in Sydney, New South Wales, Australia.

33.3.1 SUPPORT

Documentation: <https://getdataforensics.com/>

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

33.3.2 SECURE POST

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

33.3.3 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 (AEST), 9am - 5:30pm Mon - Fri

Appendix 2 - Write Blocking

APPENDIX 2 - WRITE BLOCKING

IMPORTANT:

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

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

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

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

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

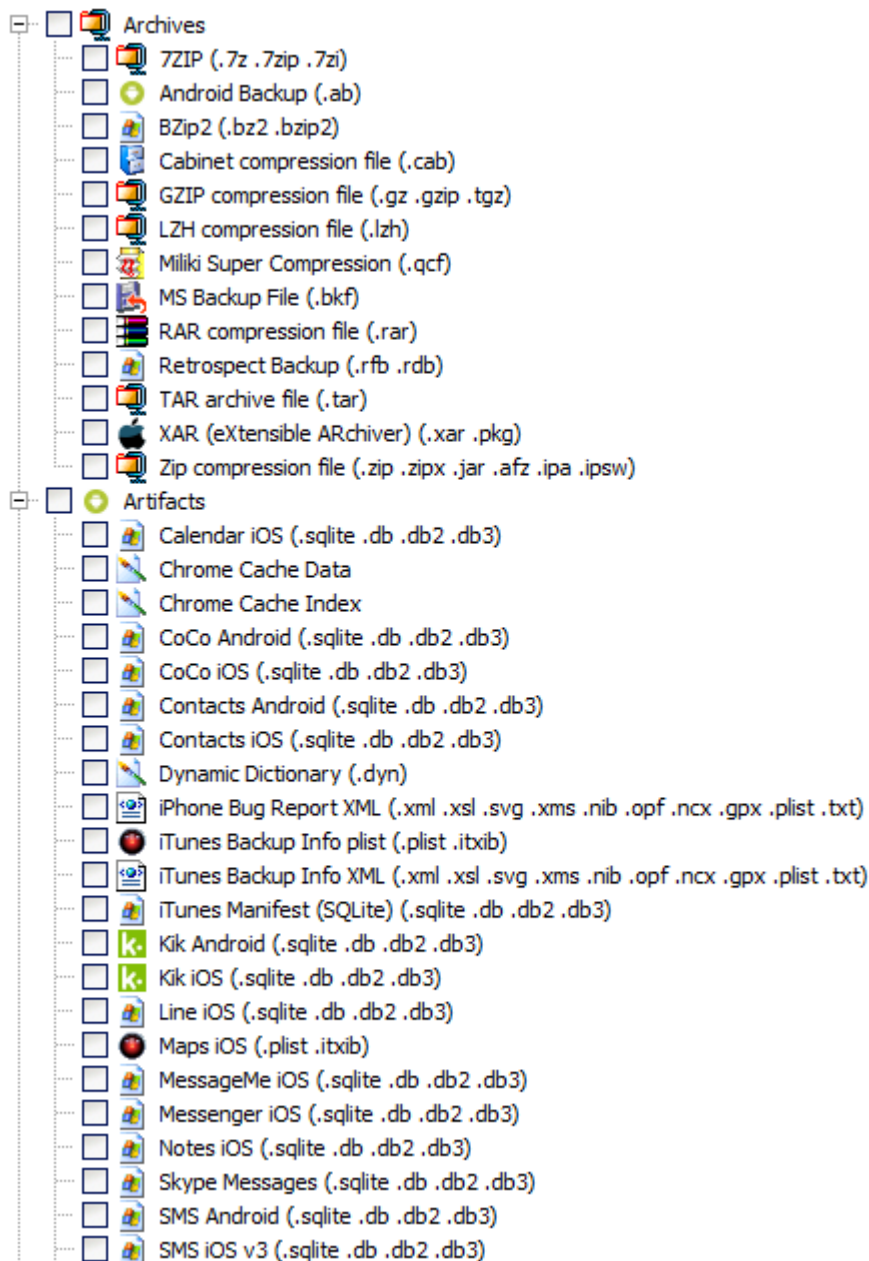
Tableau USB write block with USB as the source drive.

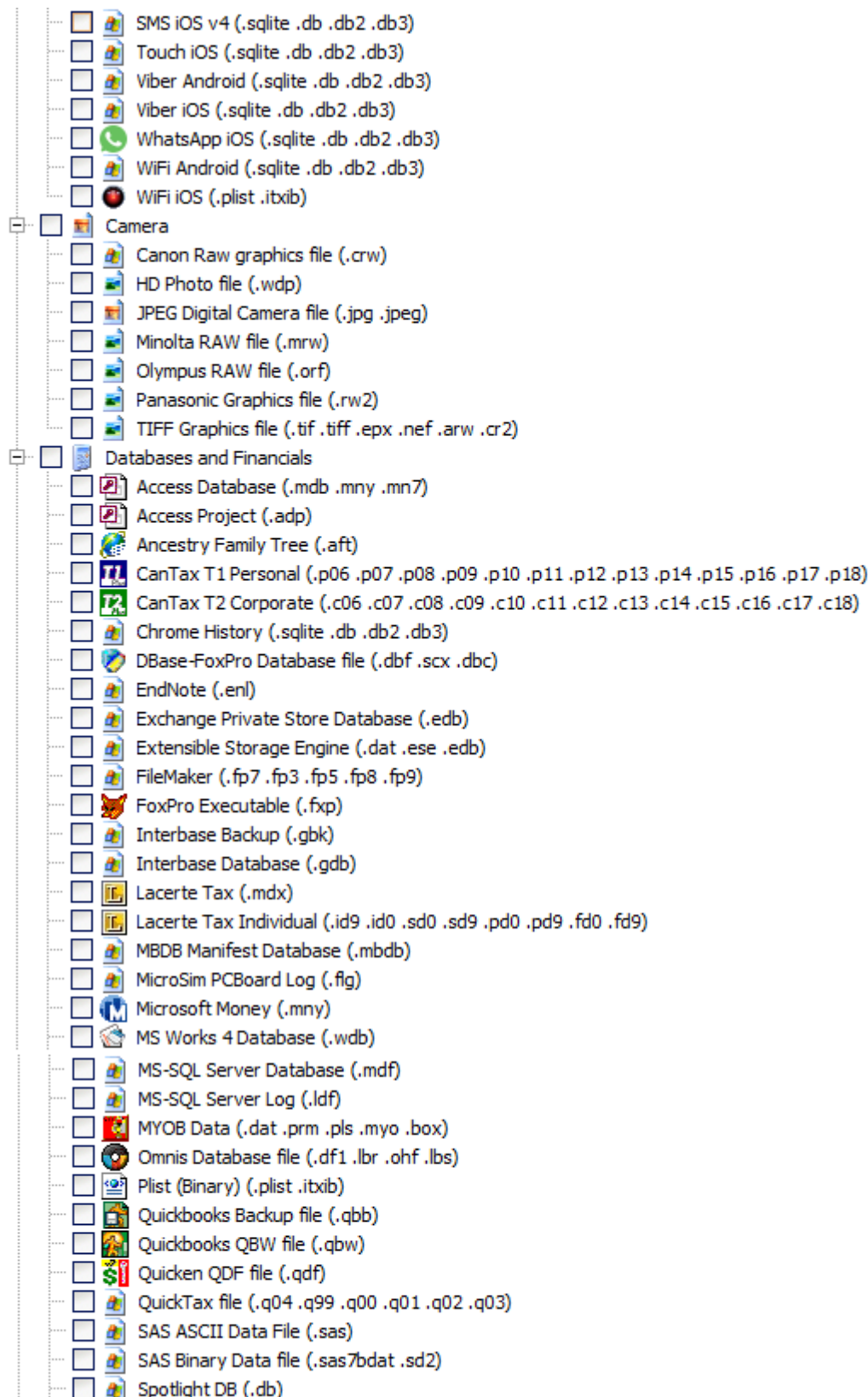





















































Appendix 3 - File Carving

















































APPENDIX 3 - FILE CARVING


















































The following file types are supported by Forensic Explorers inbuilt file carving component. Refer to Chapter 24 - Data Recovery, for more information:



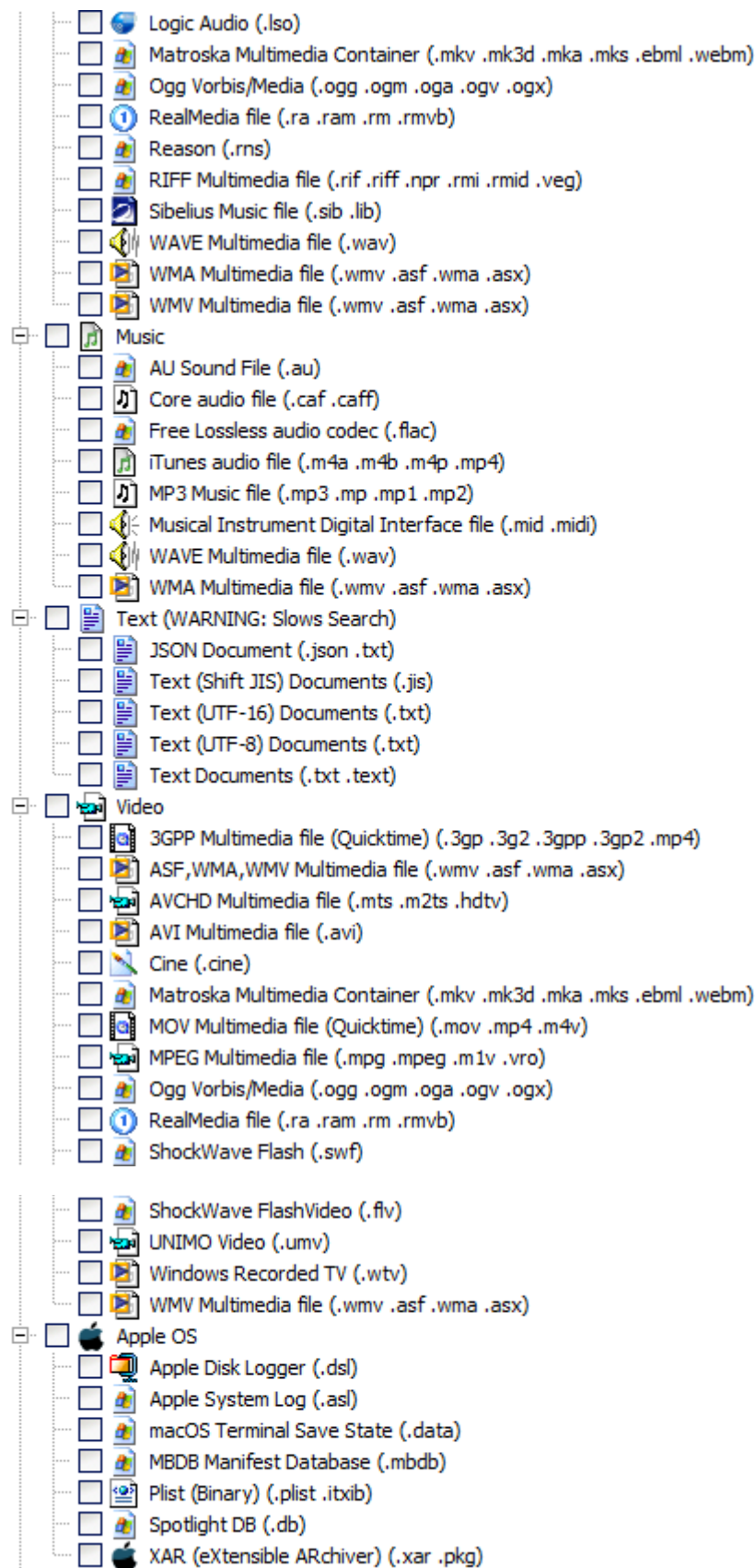


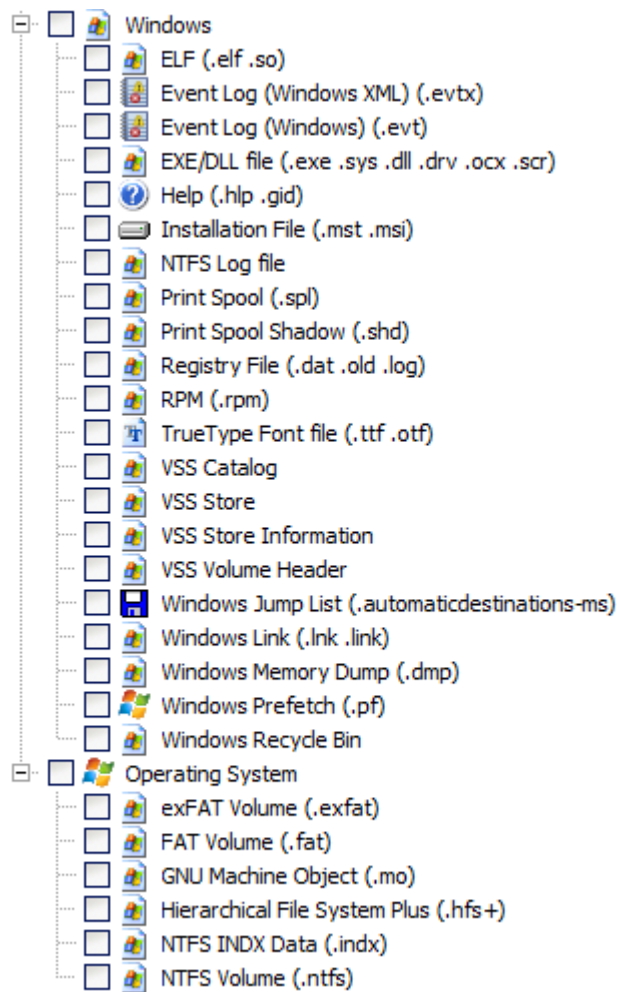
-  SPSS (.sav)
-  SQLite - open source SQL database engine (.sqlite .db .db2 .db3)
-  SQLite SHM (.shm .db-shm .sqlite-shm)
-  SQLite WAL (.wal .db-wal .sqlite-wal)
-  TaxAct (.ta5)
-  TaxCut file (2000-3) (.t00 .t01 .t02 .t03)
-  TurboTax file (.tax)
-  Web Browser Cache Database (.edb)
-  Windows Live Contacts Database (.edb)
-  Windows Search Database (.edb)
-  Documents
 -  Adobe PageMaker (.pmd .p65)
 -  Adobe Premier Project (.ppj)
 -  Adobe Type 1 Font (.ptb)
 -  Apple Document (.pages .numbers .keynote)
 -  Avery DesignPro (.zdp)
 -  Blackberry Encrypted file (.rem)
 -  Casio Disk Title (.ctw)
 -  CoolPage (.cpg)
 -  Corel Presentation File (.shw)
 -  Crystal Reports (.rpt)
 -  Diablo2 Save (.d2s)
 -  Efax file (.efx)
 -  Electronic Publication (.epub)
 -  Family TreeMaker (.ftw)
 -  FamilySearch file (.paf)
 -  Final Draft (.fdr .fdt)
 -  Final Fantasy 7 (.ff7)
 -  Fudemane Greeting Card (.fwa)
 -  Fudeou (.fzd)
 -  Hangul Document (.hwp)
 -  HotDocs (.hfd)
 -  I3F Fax (.i3f)
 -  Ichitaro Document (.jtd)
 -  InteractWeb Reports (.rpt)
 -  Label Mighty (.jlb)
-  Lotus 123 (.wk3 .wk1 .wk2 .wk4 .wks .fm3 .wb1 .123)
-  Lotus WordPro file (.lwp)
-  Mapsource 2 file (.mps)
-  Microsoft Encrypted File (.)
-  Microsoft Excel Worksheet (.xls .xla .xlt)
-  Microsoft Excel Worksheet - XLSX (.xlsx)
-  Microsoft OneNote file (.one)
-  Microsoft PowerPoint Presentation (.ppt)
-  Microsoft PowerPoint Presentation - PPTX (.pptx)
-  Microsoft Project (.mpp)
-  Microsoft Publisher Document (.pub .puz)
-  Microsoft Visio Drawing (.vsd .vss .vst)
-  Microsoft Word Document (.doc .dot .asd)
-  Microsoft Word Document - DocX (.docx)
-  Microsoft Write/WordPad (.wri)

-  MS RSS Feed (.feed-ms)
-  MS Works 4 Document (.wps)
-  MS Works Spreadsheet (.wks)
-  NASCAR Racing 2003 (.sim)
-  OLE Document (eg. MS Office) (.)
-  Open Office Document (.odt)
-  Open Office Spreadsheet (.ods)
-  Open XML Paper Document (.xps .oxps)
-  PDF document (.pdf .ai)
-  QuattroPro 7 File (.qpw)
-  Rich Text Document (.rtf)
-  SureThing CD Labeler (.dsn .std)
-  Uyp (.udf .usf)
-  VI data (.vi)
-  WordPerfect 6 to 10 (.wpd .wcm .wpt .wpg)
-  WordPerfect Documents and Graphics v8 (.wpg)
-  XML Documents (.xml .xsl .svg .xms .nib .opf .ncx .gpx .plist .txt)
-  Email
 -  Exchange Private Store Database (.edb)
 -  Generic Email (.eml .mht .mbx .txt)
 -  Lotus Notes (.nsf)
 -  Mime Email (.eml .mht .mbx .txt)
 -  Mime File (.eml .mht .mbx .txt)
 -  Offline Outlook Email file (.ost)
 -  Outlook Address file (.wab)
 -  Outlook Email file (.pst)
 -  Outlook Express Email file (.dbx)
 -  Outlook MSG (.msg)
 -  Outlook NK2 (.nk2)
 -  Personal Address Book (.pab)
 -  Usenet Item (.eml .mht .mbx .txt)
 -  Web Browser Cache Database (.edb)
-  Graphics
 -  3D Studio (.3ds)
 -  3d Studio Max (.max)
 -  Adobe Indesign file (.indd)
-  Adobe Photoshop (.psd)
-  AutoCAD Drawing file (.dwg)
-  AutoCad DX File (.dxf)
-  AutoCad DX File (.hpgl .hp .hpg .plt)
-  AutoSketch (.skf)
-  Bentley Microstation v7 Drawing (.dgn)
-  Bentley MicroStation v8 Drawing (.dgn)
-  Bitmap (.bmp)
-  Canon Raw graphics file (.crw)
-  COREL Draw file (.cdr)
-  DesignCAD file (.dcd)
-  DICOM (.dcm .dicom)

-  Encapsulated Postscript file (.eps .epsf .epsi)
-  Enhanced Metafile (.emf)
-  FormZ Document (.fmz .fzb)
-  Freehand 10 (.fh10 .fh11)
-  Freehand 7 to 9 (.fh9 .fh7 .fh8)
-  Fuji Camera Raw (.raf)
-  GIF graphics file (.gif)
-  GIS ShapeFiles (.shp)
-  GUE Map file (.gue .gmp)
-  HD Photo file (.wdp)
-  High Efficiency Image Format (.heic .heif)
-  ICO File (.ico .cur)
-  JBig2 (.jb2)
-  JPEG 2000 (.jp2 .j2k .jpx .j2c)
-  JPEG Digital Camera file (.jpg .jpeg)
-  Lightwave object (.lwo)
-  Lightwave scene (.lws)
-  MapSource 1 file (.gdb)
-  Maya 3D file (.mb)
-  Microsoft Photodraw (.mix)
-  Microsoft Visio Drawing (.vsd .vss .vst)
-  Minolta RAW file (.mrw)
-  Olympus RAW file (.orf)
-  Paintbrush file (.pcx)
-  PaintShop Pro (.psp)
-  Panasonic Graphics file (.rw2)
-  PaperPort (.max)
-  PNG Graphics file (.png .jng .mng)
-  Portable Graphics Map (.ppm .pgm .pbm)
-  PrintMaster (.hcr .biz)
-  QuarkXPress file (.qxp .qxd .qxb .qxl .qpt)
-  QuickCAD (.cad)
-  Sigma X3F Raw (.x3f)
-  SmartDraw file (.sdr .sdt)
-  SwishMax (.swi)
-  Targa (.tga .exttga .icb .vda .vst)
-  Thumbnail Cache (.db)
-  Thumbnail file (.db)
-  Thumbnail Index (.db)
-  TIFF Graphics file (.tif .tiff .epx .nef .arw .cr2)
-  TurboCAD for Windows (.tcw)
-  Visi CAD (.wkf)
-  Windows Metafile (.wmf)
-  XARA Graphic file (.xar)
-  Internet
-  Bit Torrent (.torrent)
-  Chrome Autofill (.sqlite .db .db2 .db3)
-  Chrome Cache Data
-  Chrome Cache Index

- Chrome Favicons (.sqlite .db .db2 .db3)
- Chrome History (.sqlite .db .db2 .db3)
- Chrome Logins (.sqlite .db .db2 .db3)
- Chrome Shortcuts (.sqlite .db .db2 .db3)
- Chrome Topsites (.sqlite .db .db2 .db3)
- Firefox Cookies (.sqlite .db .db2 .db3)
- Firefox Form History (.sqlite .db .db2 .db3)
- Firefox History (.sqlite .db .db2 .db3)
- HTML Documents (.htm .html .shtml .phtml .php .php5 .asp .txt)
- Internet Explorer v4-9 History (.dat)
- Internet Favorites (.url)
- Safari Bookmarks (.sqlite .db .db2 .db3)
- Safari Cache (.sqlite .db .db2 .db3)
- Safari Cookie (.binarycookies)
- Safari History (.safari-history)
- Safari Recent Searches (.plist .itxib)
- Usenet Item (.eml .mht .mbx .txt)
- Web Open Font (.woff)
- Yahoo Messenger (.dat)
- Microsoft Office
 - Access Database (.mdb .mny .mn7)
 - Microsoft Encrypted File (.)
 - Microsoft Excel Worksheet (.xls .xla .xlt)
 - Microsoft Excel Worksheet - XLSX (.xlsx)
 - Microsoft PowerPoint Presentation (.ppt)
 - Microsoft PowerPoint Presentation - PPTX (.pptx)
 - Microsoft Word Document (.doc .dot .asd)
 - Microsoft Word Document - DocX (.docx)
 - Offline Outlook Email file (.ost)
 - Open Office Document (.odt)
 - Open Office Spreadsheet (.ods)
 - Open XML Paper Document (.xps .oxps)
 - Outlook Email file (.pst)
 - Outlook NK2 (.nk2)
 - Personal Address Book (.pab)
- Multimedia
 - 3GPP Multimedia file (Quicktime) (.3gp .3g2 .3gpp .3gp2 .mp4)
 - Adaptive MultiRate Audio (.amr)
 - ASF,WMA,WMV Multimedia file (.wmv .asf .wma .asx)
 - Audio Interchange file format (.aif .aiff)
 - CakeWalk Pro (.cwp)
 - Digital Speech File (.dss)
 - Digital Voice File (.dvf .msv)
 - DS_Store (.ds_store)
 - Finale Music file (.mus .fan)
 - Flash (.fla)
 - Fruity Loops file (.flp)
 - High Efficiency Image Format (.heic .heif)
 - Jet Voice File (.sc4)
 - Kaydara FBX Binary (.fbx)





Appendix 4 - Date and Time

APPENDIX 4 - SUMMARY OF DATE AND TIME						
File System Type	FAT	NTFS	exFAT	HFS	HFS+	EXT2/3/4
Time Type	Local	UTC	Local	Local	UTC	UTC
Source	FAT record of the file in the directory data. (32 bytes)	\$10 Standard attribute in the MFT record of the file.	\$85 exFAT record of the file in the directory data. (32 bytes)	The files HFS record in the Catalogue file. (70 bytes)	The files HFS record in the catalogue file. (88 bytes)	The files inode record.
Calculation Method	DOS Date & Time.	100ns since 1 st Jan 1601.	DOS date & time.	Seconds since midnight 1 st Jan 1904.	Seconds since midnight 1 st Jan 1904.	Seconds since 1 st Jan 1970.
Modified	Written Time (2 bytes); Written Date (2 bytes). Total=4 bytes.	Written Time. Written Date. Total=8 bytes.	Created Time (2 bytes). Created Date (2 bytes). Created msec (1 byte); Total=5 bytes.	Content Modified Date & Time. The date and time the file's contents were last changed by extending, truncating, or writing either of the forks. Total=4 bytes.	Content Modified Date & Time. The date and time the file's contents were last changed by extending, truncating, or writing either of the forks. Total=4 bytes.	Last Date & Time that the content was modified. Total=4 bytes.
Accessed	Accessed Date. Total=2 bytes.	Accessed Time. Accessed Date. Total=8 bytes.	Accessed Time (2 bytes). Accessed Date (2 bytes). Total=4 bytes.	N/A	Last accessed Date & Time. The date and time the file's content were last read. Total=4 bytes.	Access Date & Time. Total=4 bytes.
Created	Created Time (2 bytes). Created Date (2 bytes). Created msec (1 byte). Total=5 bytes	Created Time. Accessed Date. Total=8 bytes.	Created Time (2 bytes). Created Date (2 bytes). Created msec (1 byte); Total=5 bytes.	Created Date & Time. Total=4 bytes.	Created Date & Time. Total=4 bytes.	N/A
Modified Record	N/A	Modified Time. Modified Date. Total=8 bytes.	N/A	N/A	The last date and time that any field in the file's catalogue record was changed. Total=4 bytes.	Modification Date & Time of the file record (the "Change" time). Total=4 bytes.

Appendix 5 - References

APPENDIX 5 - REFERENCES

1. **Hidden Disk Areas: HPA and DCO.** Gupta, Mayank R., Hoeschele, Michael D. and Rogers, Marcus K. Fall 2006, Volume 5, Issue 1, International Journal of Digital Evidence.
2. **Carrier, Brian.** *File System Forensic Analysis*. s.l. : Addison Wesley Professional, 2005.
3. **Bunting, Steve and Wei, William.** *The Official EnCE EnCase Certified Examiner Study Guide*. Indianapolis IN : Wiley Publishing, Inc., 2006.
4. **United States Computer Emergency Readiness Team.** US-CERT Vulnerability Note VU#836068. *US-CERT: United States Computer Emergency Readiness Team*. [Online] [Cited: March 5, 2011.] <http://www.kb.cert.org/vuls/id/836068>.
5. **Xiaoyun Wang, Yiqun Lisa Yin, Hongbo Yu.** *Collision Search Attacks on SHA1*. 2005.
6. **Merritt, Rick.** Chinese researchers compromise SHA-1 hashing algorithm. *EE Times*. [Online] 2 16, 2005. [Cited: May 4, 2100.] <http://www.eetimes.com/electronics-news/4051745/Chinese-researchers-compromise-SHA-1-hashing-algorithm>.
7. *Automated mapping of large binary objects using primitive fragment type classification.* **Conti, Gregory, et al.** 2010, Digital Investigation, Vol. 7S, pp. S3-S12.
8. *Fileprints: Identifying file types by n-gram analysis.* **W. Li, K. Wang, S. Stolfo and B. Herzog.** West Point, NY : s.n., June, 2005. 6th IEEE Information Assurance Workshop.
9. **Injosoftware AB.** ASCII Code - The extended ASCII table. <http://www.injosoftware.se/>. [Online] <http://www.ascii-code.com/>.
10. *CuFA: A more formal definition for digital forensic artifacts.* **Vikram, S, et al.** s.l. : <http://www.sciencedirect.com/science/article/pii/S1742287616300366>, 2016, Vol. 18.
11. **Wikipedia.** Regular Expression. [Online] en.wikipedia.org/wiki/Regular_expression.
12. **Microsoft.** Windows registry information for advanced users. *Article ID: 256986 - Revision: 12.3*. [Online] February 4, 2008. [Cited: August 19, 2011.] <http://support.microsoft.com/kb/256986>.
13. **Wikipedia.** Windows Registry. *Wikipedia - List of standard registry value types*. [Online] [Cited: December 27, 2011.] http://en.wikipedia.org/wiki/Windows_Registry.
14. **NIST.** Hacking Case. *NIST Hacking Case*. [Online] [Cited: Dec 03, 2012.] http://www.cfreds.nist.gov/Hacking_Case.html.
15. **Guidance Software Inc.** *EnCase Forensic Version 6.10 User Manual*. s.l. : Guidance Software, 2008.
16. **Magic number (programming).** *Wikipedia*. [Online] [http://en.wikipedia.org/wiki/Magic_number_\(programming\)](http://en.wikipedia.org/wiki/Magic_number_(programming)).

-
17. Asymco. How big is iCloud. [Online] November 15, 2014. [Cited: July 26, 2015.] <http://www.asymco.com/2014/11/15/how-big-is-icloud/>.
 18. wiki, The Phone. [Online] [Cited: June 26, 2015.] <https://www.theiphonewiki.com/wiki/UDID>.
 19. iPhone backup – mbdb file structure. [Online] <http://www.securitylearn.net/tag/manifest-mbdb-format/>.
 20. Satish. iPhone Forensics – Analysis of iOS 5 backups : Part2. *Security Learn*. [Online] 2012. [Cited: June 13, 2014.] <http://www.securitylearn.net/2012/05/30/iphone-forensics-analysis-of-ios-5-backups-part2/>.
 21. B, Satish. Forensic analysis of iPhone backups. [Online] [Cited: June 26, 2015.] <https://www.exploit-db.com/docs/19767.pdf>.
 22. Tenorshare. *iPhone Backup Unlocker*. [Online] [Cited: July 26, 2015.] <http://www.tenorshare.com/products/iphone-backup-unlocker.html>.
 23. Reincubate. Where are all the files in an iPhone Backup. *iPhone Backup Extractor*. [Online] [Cited: July 27, 2015.] <http://www.iphonebackupextractor.com/blog/2012/apr/23/what-are-all-files-iphone-backup/>.
 24. Parsonage, Harry. Under My Thumbs. [Online] 2012. [Cited: September 1, 2014.] <http://computerforensics.parsonage.co.uk/downloads/UnderMyThumbs.pdf>.
 25. Microsoft. [MS-SHLLINK]: Shell Link (.LNK) Binary File Format. *MSDN*. [Online] 2014. [Cited: Oct 23, 2014.] <http://msdn.microsoft.com/en-us/library/dd871305.aspx>.
 26. Microsoft MSDN. <http://msdn.microsoft.com/en-us/library>. [Online] <http://msdn.microsoft.com/en-us/library/cc231989%28PROT.13%29.aspx>.
 27. Morrissey, Sean. *iOS Forensic Analysis for iPhone, iPad and iPod touch*. s.l. : apress, 2010.
 28. Forensiks Wiki. Forensics Wiki. *AFF*. [Online] [Cited: Mar 29, 2011.] <http://www.forensicswiki.org/wiki/AFF>.
 29. *The Windows Registry as a forensic resource*. Carvey, Harlan. 3, September 2005, Pages 201-205 , Digital Investigation, Vol. 2, pp. 201-205.
 30. *Time and date issues in forensic computing--a case study*. Boyd, Chris and Foster, Pete. 1, February 2004, Digital Investigation, Vol. 1, pp. 18-23.
 31. Jones, Keith J, Bejtlich, Richard and Rose, Curtis W. *Real Digital Forensics Computer Security and Incident Response*. s.l. : Addison-Wesley, 2006.
 32. Mederios, Jason. *NTFS Forensics: A Programmers View of Raw Filesystem Data Extraction*. s.l. : Grayscale Research, 2008.
 33. Russon, Richard. Linux NTFS Project: NTFS Documentation. *Sourceforge.net*. [Online] 1996 - 2004. [Cited: March 16, 2011.] <http://sourceforge.net/projects/linux-ntfs/files/NTFS%20Documentation/>.
 34. MBR is damaged - www.NTFS.com. *NTFS.com*. [Online] <http://www.ntfs.com/mbr-damaged.htm>.
 35. Microsoft. *Microsoft Extensible Firmware Initiative FAT32 File System Specification. FAT: General Overview of On-Disk Format*. s.l. : Microsoft, 2000.
-

-
36. Stoffregen, Paul. Understanding FAT32 Filesystems. *PJRC*. [Online] Feb 24, 2005. [Cited: March 18, 2011.] <http://www.pjrc.com/tech/8051/ide/fat32.html>.
 37. Microsoft. Detailed Explanation of FAT Boot Sector. *support.microsoft.com*. [Online] Article ID: 140418 - Last Review: December 6, 2003 - Revision: 3.0, December 6, 2003. <http://support.microsoft.com/kb/140418>.
 38. —. Windows and GPT FAQ. *Microsoft Developers Network (MSDN)*. [Online] July 2008. <http://msdn.microsoft.com/en-us/windows/hardware/gg463525.aspx>.
 39. —. Basic Storage Versus Dynamic Storage in Windows XP. *Microsoft Support*. [Online] December 1, 2007. [Cited: March 23, 2011.] <http://support.microsoft.com/kb/314343>.
 40. National Institute of Standards and Technology. CFTT Project Overview. *Computer Forensics Tool Testing Program*. [Online] [Cited: March 28, 2011.] http://www.cftt.nist.gov/disk_imaging.htm.
 41. Wikipedia - Host Protected Area. http://en.wikipedia.org/wiki/Host_protected_area. [Online] [Cited: Mar 29, 2011.] http://en.wikipedia.org/wiki/Host_protected_area.
 42. Apple Computer, Inc. Technical Note TN2166 - Secrets of the GPT. *developer.apple.com*. [Online] 11 6, 2006. [Cited: April 5, 2011.] http://developer.apple.com/library/mac/#technotes/tn2166/_index.html.
 43. Apple Inc. *Inside Macintosh: Files*. Reading, Massachusetts : Addison-Wesley, August 1992.
 44. Apple, Inc. HFS Plus Volume Format - Technical Note TN1150. *developer.apple.com*. [Online] March 5, 2004. [Cited: April 6, 2011.] <http://developer.apple.com/library/mac/#technotes/tn/tn1150.html>.
 45. Wikipedia: Extent (file systems). Extent (file systems). *Wikipedia: Extent (file systems)*. [Online] [Cited: 4 6, 2011.] [http://en.wikipedia.org/wiki/Extent_\(file_systems\)](http://en.wikipedia.org/wiki/Extent_(file_systems)).
 46. Aomei Technology, Co., Ltd. What is a Dynamic Disk? *Dynamic Disk*. [Online] 2009. [Cited: April 13, 2011.] <http://www.dynamic-disk.com/what-is-dynamic-disk.html>.
 47. Lewis, Don L. The Hash Algorithm Dilemma—Hash Value Collisions. *Forensic Magazine*. [Online] 2009. [Cited: May 2011, 4.] <http://www.forensicmag.com/article/hash-algorithm-dilemma%E2%80%93hash-value-collisions?page=0,0>.
 48. *An Empirical Analysis of Disk Sector Hashes for Data Carving*. Yoginder Singh Dandass, Nathan Joseph Necaie, Sherry Reede Thomas. 2008, *Journal of Digital Forensic Practice*, Vol. 2, pp. 95-104.
 49. Farmer, Derrick J. and Burlington, Vermont. Windows registry quick reference. *A Windows Registry Quick Reference: For the Everyday Examiner*. [Online] [Cited: Oct 12, 2012.] <http://www.forensicfocus.com/downloads/windows-registry-quick-reference.pdf>.
 50. Wong, Lih Wern. Forensic Analysis of the Windows Registry. *ForensicFocus.com*. [Online] School of Computer and Information Science, Edith Cowan University. [Cited: Oct 12, 2012.] <http://www.forensicfocus.com/Content/pid=73/page=1/>.
 51. Harrington, Michael. Seek and You Shall Find: Using Regular Expressions for Fast, Accurate Mobile Device Data Searches. <http://www.dfinews.com>. [Online] [Cited: Oct 29, 12.] <http://www.dfinews.com/article/seek-and-you-shall-find-using-regular-expressions-fast-accurate-mobile-device-data-searches?page=0,0>.
-

52. Access Data Inc. Registry Quick Find Chart. *Access Data*. [Online] 2005. [Cited: August 19, 2011.] <https://ad-pdf.s3.amazonaws.com/Registry%20Quick%20Find%20Chart%20%207-22-08.pdf>.
53. B, Satish. iPhone Forensics – Analysis of iOS 5 backups : Part2. *Security Learn*. [Online] 2012. [Cited: June 13, 2014.] <http://www.securitylearn.net/2012/05/30/iphone-forensics-analysis-of-ios-5-backups-part2/>.
54. iPhone-Backup-Analyzer. *GitHub*. [Online] [Cited: June 18, 2014.] <https://github.com/PicciMario/iPhone-Backup-Analyzer/blob/master/mdbdbdecoding.py#L53>.
55. Microsoft. Hard Links and Junctions. [Online] [Cited: June 14, 2014.] <http://msdn.microsoft.com/en-us/library/windows/desktop/aa365006%28v=vs.85%29.aspx>.

Appendix 6 - Definitions

APPENDIX 6 - DEFINITIONS

Alternate Data Stream	An Alternate Data Stream (ADS) is a feature of the NTFS file system. ADS were originally included in Windows NT for compatibility with Macintosh HFS file systems resource fork and a data fork. The ADS provides a means to allow programmers to add additional metadata to be stored for a file, without adding this data directly to the file. The additional data is attached as a stream which is not normally visible to the user.
ANSI character set	The ANSI character set was that standard character encoding for English versions of Microsoft Windows, including Windows 95 and NT. The ANSI format stores only the 128 ASCII characters and 128 extended characters, using 1 byte per character. Not all the Unicode characters are supported.
ASCII	The American Standard Code for Information Interchange (ASCII) is a 7-bit character encoding scheme that allows text to be transmitted between electronic devices in a consistent way. The ASCII character set comprises codes 0–127, within which codes 0–31 and 127 are non-printing control characters. The addition of Codes 128–255 make up the Extended ASCII character set (see http://www.ascii-code.com/ for more information) (9).
Bookmarks	Forensic Explorer enables any item (file, folder, keyword, search hit etc.), or sections of items, to be marked and listed in the Bookmarks module. Bookmarks are used to note items of interest.
BpB	“Bytes per Block”. Used in the Forensic Explorer File Extent tab to display the number of Bytes per Block (cluster) for the highlighted file.
BpS	“Bytes per Sector”. Used in the Forensic Explorer File Extent tab to display the number of Bytes per Sector for the highlighted file.
Byte Plot view (Forensic Explorer)	A view in Forensic Explorer which includes for a selected file: A graphical representation of a binary file; A Character Distribution graph representing the frequency that each ASCII character is displayed in the file. See “Byte Plot and Character Distribution” page 113.
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 are only stored with the file system record, a carved file does not retain its original file or folder name.

Case File	<p>A case file is the store of investigational activities for an individual case in Forensic Explorer. The case file records the location of the examined devices and holds the results of searching, sorting, bookmarks, reports etc.</p> <p>A case file is designed to build over time as a record of an investigation, in the same way as would a paper based file in a traditional matter.</p>
ClamAV (Clam AntiVirus)	<p>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.</p> <p>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 support@getdata.com. ClamAV and Clam AntiVirus are trademarks of Cisco Systems, Inc. 2017.</p>
Clear Columns	<p>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 > Clear Column Content. To clear an individual column, right-click on the column header and select Clear Column from the menu.</p>
Cluster	<p>A cluster is the smallest logical unit of disk storage space on a hard drive that can be addressed by the computers Operating System. A single computer file can be stored in one or more clusters depending on its size.</p>
Cluster Boundaries	<p>A cluster boundary refers to the start or the end position of a cluster (a group of sectors). If a file is fragmented (stored in non-contiguous clusters), the fragmentation happens at the cluster boundary, as there is no smaller unit of storage space that can be addressed by a computer.</p> <p>Examining data at cluster boundaries can be an important technique to improve the speed of some search routines. For example, when file carving for file headers, it is faster to search the cluster boundary (i.e., the beginning of a cluster) rather than a sector-by-sector search of the drive.</p>
Codepage	<p>Codepage is another term for character encoding. It consists of a table of values that describes the character set for a language. When a keyword search is conducted in Forensic Explorer, the correct codepage should be selected.</p>
Computer forensics	<p>Computer forensics is the use of specialized techniques for recovery, authentication, and analysis of electronic data with a view to presenting evidence in a court of law.</p>

Compound File	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 Error! Reference source not found. 9.6 - Expand compound file.
Data carve	See file carve.
Data View	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.
Deleted File	<p>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.</p> <p>In some cases, the file system record itself can be overwritten and destroyed. If this is the case the file can only be recovered by “file carving” (see 22.4- File carving). Because file and folder information are only stored with the file system record, a carved file does not retain its original file or folder name.</p>
Delphi Basics©	Delphi Basics© is a documentation package for the Delphi programming language (see http://www.delphibasics.co.uk/). Delphi Basics© is installed with and licensed for use only with Forensic Explorer. Delphi Basics© is provided as a reference guide only. Not all commands/features in the documentation are available in Forensic Explorer.
Device	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.
Directory	See Root Directory
Directory Entry (FAT)	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.
Disk Slack	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.
Disk view (Forensic Explorer)	<p>A graphical representation in Forensic Explorer of sectors on the examined device. Disk view can be used to:</p> <ul style="list-style-type: none">• Examine the content of the data in a specific sector/s;• Quickly navigate to a desired sector position on the device;

	<ul style="list-style-type: none">• 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) 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	<p><i>The concept of information entropy was introduced by Claude Shannon in his 1948 paper "A Mathematical Theory of Communication". It is also referred to as Shannon entropy (https://en.wikipedia.org/wiki/Entropy_(information_theory)).</i></p> <p>Entropy is an expression of disorder or randomness. It is used in computer forensics to measure the randomness of data. For example, a compressed file will have a high entropy score. A text file will not. An entropy score is included in Forensic Explorer the Byte Plot data view of the File System module.</p>
E01	A forensic file format used to create disk image files. Developed by Guidance Software (http://www.guidancesoftware.com/)
Evidence Items	Items of evidence that have been added to the case, such as forensic image files, email files, registry files etc.
Explorer View	File display technology written by GetData and used in the Forensic Explorer File Display tab to show the contents of more than 300 different file types.
FAT	<p>FAT (File Allocation Table) is the file system that pre-dates NTFS. Once popular on Windows 95, 98 and XP, it is now primarily used on memory cards, USB drives, flash memory etc. due to its simplicity and compatibility between Operating Systems (e.g., Windows and MAC).</p> <p>For more information see: http://www.forensicswiki.org/wiki/FAT</p>
FAT Slack	The unused space in the last cluster of the FAT where the logical size of the FAT does not fill the complete cluster.
Files carve	<p>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.</p> <p>Forensic Explorer has built in code to data carve for more than 300 file types.</p>
File Signature	The header component of a file which has unique identifiers that assigns it to a type, e.g., a jpeg. Most common file types have a signature set by the International Organization for Standardization (ISO). Identifying a file by its

	signature is a more accurate method of assessment 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” (8). See “Byte Plot and Character Distribution” page 113.
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 an item and double clicking the opaque flag color in the flag column, or by using the right click “Add Flag” menu. Flags can also be applied by running Forensic Explorer scripts.
Folder	See Root Directory
Forensic Image	<p>A “forensic image” is a file (or set of files), used to preserve an exact “bit-for-bit” copy of data residing on electronic media.</p> <p>Using non-invasive procedures, forensic software is used to create the image file. The image contains all data, including deleted and system files, and is an exact copy of the original.</p> <p>Most forensic imaging software integrates additional information into the image file at the time of acquisition. This can include descriptive details entered by the examiner, as well as the output of mathematical calculations, an “acquisition hash”, which can be later used to validate the integrity of the image. The forensic image file acts as a digital evidence container that can be verified and accepted by courts.</p>
Forensic Integrity	In computer forensics the term “forensic integrity” commonly refers to the ability to preserve the evidence being examined so that it is not altered by the investigator or the investigative process. This enables a third party to conduct an independent examination of the evidence on an identical data set. Forensic integrity is usually achieved 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	<p>Free space: Space on the disk that does not form part of any partition but is available for future allocation.</p> <p>(Free space can also exist as sectors between the MBR and the first partition, and space at the end of the disk that was not used in any partition).</p> <p>Free space in Partition: Space inside the partition that is not used by a volume (this is usually a small section of space at the end of a partition). If there is no volume, then this is the entire partition.</p> <p>Also see Unallocated Clusters: Available volume storage not yet used to store files.</p>
GeoTag (Geotagging)	<p>Geotagging is the process of adding geographical identification metadata to files, usually photographs or videos. This data is usually latitude and longitude coordinates.</p>
GREP	<p>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.</p>
Hard Link	<p>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.</p>
Hash	<p>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.</p>
Hash Set	<p>A Hash Sets is a store of mathematical calculations (hash values - usually created by the MD5 algorithm) for a specific group of files. The hash values are a “digital fingerprint” which can then be used to identify a file and either include or exclude the file from a data set.</p> <p>Hash Sets are often grouped in the forensic community into two groups:</p> <p>Good Hash Sets: Operating System files, program installation files, etc.; and Bad Hash Sets: virus files, malware, Trojans, child pornography, Steganography tools, hacking tools etc.</p> <p>Hash sets can be created in Forensic Explorer or downloaded from a trusted source.</p>
Hex	<p>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.</p>

Image File	See Forensic Image.
Index Search	An Index Search is the process of creating a database of search words in the case so that after the index is created an instant search is possible. Forensic Explorer uses the third-party application dtSearch® (www.dtsearch.com) for this process.
INFO2	<p>Windows automatically keeps an index of what files were deleted including the date and time of the deletion. The index is held in a hidden file in the Recycle Bin called INFO2.</p> <p>When the Recycle Bin is emptied, the INFO2 file is deleted. Recovery and analysis of deleted INFO2 files can provide important information about files that were once located on the computer.</p>
Investigator	In this user guide “Investigator” is used to describe the computer forensics examiner, i.e., the user of Forensic Explorer. The investigator is responsible for creating and developing the case file.
Initialized Size	In Microsoft NTFS the logical size of a file can represent additional disk space for future operations. For performance purposes the file initialized size enables Windows to load only the actual required data.
Item	In Forensic Explorer, the term “item” is a generic term used to describe a piece of data. The data could be a file, folder, partition, metadata entry, FAT, MFT, unallocated clusters, or other such data that can be isolated and examined.
iTunes Backup	iTunes Backups are created by iTunes. When an Apple device (iPhone, iPad, iPod) is connected to a computer for the first time and synced with iTunes, a folder is created using the unique device ID (UUID). These iTunes Backup folders are very distinctive, in that they are 40 hexadecimal characters long. iTunes Backups can be processed with Forensic Explorer.
Keyword	<p>A keyword is a string of data created by the forensic examiner so that the case can be searched for instances of that data (a keyword search).</p> <p>A keyword can be an actual word but can also be raw data.</p> <p>Complex keywords are usually created using RegEx expressions.</p>
Video Key Frame (Keyframe)	<p><i>In animation and filmmaking, a key frame (or keyframe) is a drawing or shot that defines the starting and ending points of a smooth transition. These are called frames because their position in time is measured in frames on a strip of film or on a digital video editing timeline. (https://en.wikipedia.org/wiki/Key_frame, Accessed June 2023).</i></p> <p>Many software programs have the ability to extract keyframes as a method to represent the visual content of the entire file. A similar method is to time slice a video, where frames are extracted at set intervals.</p>

	In Forensic Explorer, keyframes and time slicing is performed using Expand Compound File(s) .
LEF	See Logical Evidence File
LFN (also see SFN)	Long File Name refers to a 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. (25)
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 or VirtualBox.
Logical Evidence File (LEF)	<p>A Logical Evidence File is a forensic image containing specific files, rather than the traditional image of an entire volume or physical disk. They are usually created during a preview where an investigator identifies file-based evidence worthy of preservation, when an image of the entire volume or device is not warranted.</p> <p>Common Logical Evidence File formats are L01, created by EnCase® forensic software (www.guidancesoftware.com) or AD1 by Access Data's Forensic Tool Kit® (www.accessdata.com).</p> <p>Forensic Explorer enables files in a case to be exported to a logical evidence file (LEF) in .L01 format (see 9.7.2 for more information).</p>
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 [type] volume.

Master boot record (MBR, Boot Sector)	The very first sector on a hard drive. It contains the startup information for the computer and the partition table, detailing how the computer is organized.
Master File Table (MFT)	<i>“On an NTFS volume, the MFT is a relational database that consists of rows of file records and columns of file attributes. It contains at least one entry for every file on an NTFS volume, including the MFT itself. The MFT stores the information required to retrieve files from the NTFS partition”. (26)</i>
Metadata	<p>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.</p> <p>The File Metadata view (tab) at the bottom window of Forensic Explorer is used to show all metadata properties for a file.</p> <p>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 8.13.1 for more information.</p>
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 to add and browse registry files.
Mount Image Pro (MIP)	A computer forensics software tool written and sold by GetData (www.mountimage.com) which enable the mounting of forensic image files as a drive letter on a Windows computer system. MIP is sold with Forensic Explorer. It is installed as a separate program but can be run from a shortcut in the Forensic Explorer toolbar.
MRU	Most Recently Used (MRU) is a term used to describe a list of the most recently opened files by an application. Many Windows applications store MRU lists as a way of allowing fast and consistent access to most recently used files. Most MRU lists are stored in the Windows registry.
Multi-core processing	<p>A multi-core processor is a single computing component with two or more processors ("cores"). Each core is responsible for reading and processing program instructions. A multi-core process should be faster than the same process run on a single core. However, users are encouraged to test their workstations as different hardware configurations can affect multi-core speed.</p> <p>Forensic Explorer provides the option to use multi core processing in File Carving, Hashing and Keyword Search. The option is set using the “Priority” options, where Minimum is single core, and Normal, High and Maximum are multi-core.</p>
NTFS	The Windows New Technology File System (NTFS) superseded FAT. It was released with Windows NT and subsequently Windows 2000, Windows XP,

	<p>Windows Server 2003, Windows Server 2008, Windows Vista, and Windows 7. It uses a Master File Table (MFT) to store the information required to retrieve files from the NTFS partition.</p>
NTLM Hash	<p>An NTLM hash is the cryptographic format in which user passwords are stored on Windows systems. NTLM hashes can be extracted in Forensic Explorer using File System > Tools > 3rd Party Tools > GetData NTLM Hash Extract.</p> <p>To break an NTLM hash, various programs can be used, such as John the Ripper and Hashcat. These programs are capable of performing dictionary attacks, brute-force attacks, and other techniques to crack the hashes and reveal passwords.</p>
Ophcrack	<p>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.</p>
Pane	<p>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, <i>Console</i> etc.</p>
Pascal	<p>A programming language used to create scripts in Forensic Explorer. See Module Chapter 19 - Scripts Module.</p>
Partition	<p>A part of a hard disk that can have an independent file system.</p>
PCRE (Perl Compatible Regular Expression)	<p>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.</p>
Portable Case (FEX)	<p>A Forensic Explorer Portable Case is where the forensic investigator prepares a selection of files (e.g. checks or books) to be provided to the third party. The case can either be opened by an installed FEX Viewer, or, FEX Viewer can be embedded within the case so that it operates as a fully self contained 'portable' case that can be launched independently from USB media without the need for any other software.</p>
Pre-processing (a case)	<p>Pre-processing describes the setup of a case so that core analysis functions are automatically run prior to investigator review. Core analysis functions can include hashing, carving and signature analysis.</p> <p>Pre-processing options are set in Forensic Explorer when a device or forensic image file is added. See 0 for more information.</p>
Priority	<p>In Forensic Explorer priority refers to the use of threaded multi-core processing. See "Multi-Core Processing".</p>

Preview (Evidence Module)	The Preview button in the Evidence module enables an investigator to quickly add a device or forensic image to Forensic Explorer without first having to go through the steps to create a new case. The investigator can choose to save a preview to a case, or if not, when the preview is closed, no data is saved.
RAID	Redundant Array of Independent Disks.
RAM	Random Access Memory, where programs are loaded, and computer code is executed. The content of RAM is lost when the computer is turned off.
RAM Slack	RAM slack is the data between the end of the logical file and the rest of that sector. For example, a sector is written as a block of 512 bytes, so if the last sector contains only 100 bytes, the remaining 412 bytes is padded with RAM slack. In older Operating Systems, e.g., Windows 95, RAM slack could contain data from RAM unrelated to the content of the file. In more recent Operating Systems, RAM slack is filled with zeroes.
Record View (Forensic Explorer)	Record View displays information directly from the FAT or MFT record. It provides more complete details for a file than the limited information displayed in File List view.
Recover My Files	Data Recovery Software authored and sold by GetData at www.recovermyfiles.com
Regex (Regular Expression)	A regular expression provides a concise and flexible means to "match" (specify and recognize) strings of text, such as particular characters, words, or patterns of characters. "The concept of regular expressions was first popularized by utilities provided by Unix distributions, in particular the editor ED and the filter grep q" (http://en.wikipedia.org/wiki/Regex).
Registry	The Windows Registry is a hierarchical database that stores configuration settings and options for the Microsoft Windows operating systems. For the computer forensics examiner, it can be a wealth of information on all aspects of the computer and its use, including hardware, applications, and user configuration.
Ribbon (Toolbar)	The ribbon refers to the Forensic Explorer toolbar and the top of each module. The contents of the toolbar are controlled by scripts.
Root Directory/Folder	<p>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.</p> <p>A directory that is below the root is called a subdirectory. A directory above a subdirectory is called its parent directory. The root is the parent of all directories.</p>

	<p>“Directory” was a more common term when DOS use was prolific (The “DIR” command is used in DOS to list the contents of a directory). Directories are now more commonly referred to as “Folders”.</p>
Script	<p>A script is a computer program written to perform a specific task. Forensic Explorer has a scripts module which allows the investigator to write Pascal language scripts.</p>
Sector	<p>A sector is a specifically sized unit 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).</p>
SFN (see also LFN)	<p>Short File Name refers to a file or a folder on a FAT file system that has a file name that can be stored in the 8.3 file name format (8 name characters with 3 characters for the extension). The name and metadata for a SFN file can be stored within a standard FAT directory entry.</p>
Signature Analysis	<p>Signature analysis compares a files header with its extension. A mismatch may justify closer examination. Identifying a file by its signature is a more accurate method of classification than using the file extension (e.g. .jpg), as the extension can easily be altered.</p>
Shadow Copy	<p>“Shadow Copy” (also known as Volume Snapshot Service, Volume Shadow Copy Service, VSC or VSS), is a technology included in Microsoft Windows that allows taking manual or automatic backup copies or snapshots of data, even if it has a lock, on a specific volume at a specific point in time over regular intervals” (https://en.wikipedia.org/wiki/Shadow_Copy). Forensic Explorer enables investigators to add and examine the content of Shadow Copies. See Chapter 26.</p>
Skin Tone Analysis	<p>Skin tone analysis is the automated detection of skin tone colors in graphics files. It is often used to identify pornographic pictures on a suspect’s computer. In Forensic Explorer, skin tone analysis is run using a script.</p>
Slack	<p>See File Slack, Disk Slack, FAT Slack.</p>
Steganography	<p>Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity (Definition from: http://en.wikipedia.org/wiki/Steganography).</p>
Tesseract Open-Source OCR Engine	<p><i>Tesseract</i> (https://tesseract-ocr.github.io/) is an optical character recognition engine for various operating systems. It is free software, released under the Apache License. Originally developed by Hewlett-Packard as proprietary software in the 1980s, it was released as open source in 2005 and development</p>

has been sponsored by Google since 2006.

Definition from: ([https://en.wikipedia.org/wiki/Tesseract_\(software\)](https://en.wikipedia.org/wiki/Tesseract_(software))).

User Datagram Protocol (UDP)	UDP is one of the core members of the Internet Protocol Suite (the protocols used for the Internet). Forensic Explorer can use UDP to access remote drives.
Unallocated Clusters	<p>Unallocated clusters (also referred to as unallocated space) are the available clusters not yet allocated to file storage by a volume.</p> <p>Unallocated clusters can be a valuable source of evidence in a computer forensics examination because they can contain deleted files or remnants of deleted files created by the Operating System and / or computer users.</p> <p>In Forensic Explorer the display format is: Unallocated clusters on [type] volume. For NTFS, this is calculated using the \$BITMAP record, for FAT this is calculated from the FAT Table.</p>
Unicode	Unicode is an international standard for processing and displaying all types of text. Unicode provides a unique number for every character for all languages on all platforms.
UUID	An Apple device (iPhone, iPad or iPod Touch) has a Unique Device Identifier (UDID). It is a sequence of 40 letters and numbers. When a backup of the device is made to a PC, the backup files for the device are stored in the UUID folder. See chapter 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.

```
{!NAME:      Help File - Sample Script 1.pas}
{!DESC:      Counts years to 21 }
{!INFO:      Shows basic Pascal programming elements }
{!AUTHOR:    GetData}
{!VERSION:   v1.00}

program Help_File_Sample_Script_1;

uses
  GUI, SysUtils;

const
  starting_age = 10;

var
  my_age: integer;







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:

Icon	Category	Description
	Case	A Forensic Explorer case
	Shadow Copy	A mounted shadow copy volume
	Compound file	A folder holding the contents of an expanded compound file
	Date	Categorize dates - File System > Folders view > Category view
	Device	A physical device, e.g., a hard drive
	Device	A logical device, e.g., C: drive.
	File	A deleted file
	File	A FAT “dot” directory entry
	File	A FAT “double dot” directory entry
	File	A system file
	File	An active file
	File	An alternate data stream
	File	Windows hard link (http://en.wikipedia.org/wiki/Hard_link)
	Folder	A folder holding the results of a Forensic Explorer file carve
	Folder	A deleted folder
	Deleted items	Categorize deleted items - File System > Folders view > Category view
	Folder	An active folder
	Free space	Free space in partition
	Image	A forensic image file
	Image	A corrupt forensic image (see Add Image)
	Image folder	Select an image from a folder
	Navigation	An expandable branch (folder structure)

	Navigation	Active branch plate
	Navigation	Inactive branch plate
	Navigation	A child branch plate is active
	Partition	A partition
	Partition	An active partition
	Unallocated	Unallocated clusters

Disk View

	The start sector of a file
	Currently selected sector
	One type of file overlay another

	MBR/VBR (Red)
	FAT 1 (Dark Violet)
	FAT 2 (Web Violet)
	\$MFT (Dark Violet)
	System files (Web Tomato)
	\$MFT resident file (the file overlays the \$MFT)
	Folder (Deep Sky Blue)
	Allocated File (Corn Flower Blue)
	Unallocated space (Lt Gray)
	Deleted file (A deleted file overlays unallocated space)
	Carved file (Dark Orange: Carved file overlays unallocated space)

Icons in Forensic Explorer include those supplied by:

- Silk Icons: <http://www.famfamfam.com/lab/icons/silk/>
- <http://www.softicons.com>
- <https://icons8.com>

Appendix 9 – iTunes Backup Files

APPENDIX 9 – ITUNES BACKUP FILES

The following table lists iTunes backup files that may be of interest to the forensic investigator:

Contents	Domain	iOS Path and file name	SHA-1 backup file name
Calendar	HomeDomain	Library/Calendar/Calendar.sqlitedb	2041457d5fe04d39d0ab481178355df6781e6858
Call History	WirelessDomain	Library/CallHistory/call_history.db	2b2b0084a1bc3a5ac8c27afdf14afb42c61a19ca
Chat – KikChat	AppDomain-com.kik.chat	Documents/kik.sqlite	8e281be6657d4523710d96341b6f86ba89b56df7
Chat – Line	AppDomain-jp.naver.line	Documents/talk.sqlite	534a7099b474f4fb3f2cd006f8e59578d58fb44a
Chat – MessageMe	AppDomain-com.littleinc.MessageMe	Library/Application Support/MessageMe/MessageMe.sqlite	8c625842c0b74fefff30d92eece44a1da30d2e8e
Chat – Skype	AppDomain-com.skype.skype	Library/Application Support/Skype/[user]/main.db	
Chat – Touch	AppDomain-com.enflick.ping	Documents/Touch.sqlite	b18a30bf72824a7d024a95178ae42d8339f83633
Chat – Viber	AppDomain-com.viber	Documents/Contacts.data	b39bac0d347adfaf172527f97c3a5fa3df726a3a
Chat – WeChat	AppDomain-com.tencent.xin	Documents/[chat-UDID]/DB/MM.sqlite	
Chat - WhatsApp	AppDomain-net.whatsapp.WhatsApp	AppDomain-net.whatsapp.WhatsApp	1b6b187a1b60b9ae8b720c79e2c67f472bab09c0
Contacts	HomeDomain	Library/AddressBook/AddressBook.sqlitedb	31bb7ba8914766d4ba40d6dfb6113c8b614be442
Keyboard	HomeDomain	Library/Keyboard/dynamic-text.dat	Changes with language installed
Locations	RootDomain	Library/Caches/locationd/consolidated.db	4096c9ec676f2847dc283405900e284a7c815836*
Maps History	HomeDomain	Library/Maps/History.plist	b60c382887dfa562166f099f24797e55c12a94e4
Notes	HomeDomain	Library/Notes/notes.sqlite	ca3bc056d4da0bbf88b5fb3be254f3b7147e639c
Safari History	HomeDomain	Library/Safari/History.plist	1d6740792a2b845f4c1e6220c43906d7f0afe8ab
SMS	HomeDomain	Library/SMS/sms.db	3d0d7e5fb2ce288813306e4d4636395e047a3d28
Wifi Networks	SystemPreferencesDomain	SystemConfiguration/com.apple.wifi.plist	ade0340f576ee14793c607073bd7e8e409af07a8

* 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:

Bookmark Folder	Bookmarked File/s	Description	Best FEX Viewer
Address Book	AddressBook.sqlitedb (SQLite) 31bb7ba8914766d4ba40d6dfb6113c8b614be442	Contacts	Display. Phone module. External SQLite viewer.
Call History	call_history.db (SQLite) 2b2b0084a1bc3a5ac8c27afdf14afb42c61a19ca	Last 100 calls.	Display. Phone module. External SQLite viewer.
Camera Roll	Photos and Movies	Files in the CameraRoll domain.	Display/Gallery
Domain - JPG	JPG files	JPG files are bookmarked according to the Apple Domain in which they reside. This is especially useful for identifying applications that use JPG files (such as chat/messaging apps).	Display/Gallery
Domain - MOV	MOV files	MOV files are bookmarked according to the Apple Domain in which they reside. This is especially useful for identifying applications that use MOV files (such as chat/messaging apps).	Display.
Domain - PNG	PNG files	PNG files are bookmarked according to the Apple Domain in which they reside. This is especially useful for identifying applications that use PNG files (such as chat/messaging apps).	Display/Gallery
Domain - SQLite	SQLite files	SQLite files are bookmarked according to the Apple Domain in which they reside. This is especially useful for identifying applications installed on the iOS device that may be of value to the investigator.	Display. External SQLite viewer.
Keyboard	dynamic-text.dat 0b68edc697a550c9b977b77cd012fa9a0557dfcb	“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.” <i>Morrissey, S. (27) page 150.</i>	Text. Hex.

<p>Phone Chat Apps</p> <ul style="list-style-type: none"> - Kikchat - Line - MessageMe - Skype - Touch - Viber - WeChat - WhatsApp 	<p>8e281be6657d4523710d96341b6f86ba89b56df7 534a7099b474f4fb3f2cd006f8e59578d58fb44a 8c625842c0b74fefff30d92eece44a1da30d2e8e N/A (changes with user account) b18a30bf72824a7d024a95178ae42d8339f83633 b39bac0d347adfaf172527f97c3a5fa3df726a3a N/A (changes with user account) 1b6b187a1b60b9ae8b720c79e2c67f472bab09c0</p>	<p>SQLite files containing communication history from Phone/Chat applications.</p>	<p>Display. Phone Apps module. External SQLite viewer.</p>
<p>Maps History</p>	<p>History.plist b60c382887dfa562166f099f24797e55c12a94e4</p>	<p>“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” <i>Morrissey, S. (27) page 155</i>. This can include GPS co-ordinates and names of locations.</p>	<p>File Metadata</p>
<p>Photo Streams Data</p>	<p>Media files</p>	<p>Media streamed to the phone with Apple PhotoStream.</p>	<p>Display/Gallery</p>
<p>Recordings</p>	<p>Audio files</p>	<p>Recordings (and configuration files) located in the Media/Recordings/ domain.</p>	<p>Display.</p>
<p>Safari History</p>	<p>History.plist ed50eadf14505ef0b433e0c4a380526ad6656d3a</p>	<p>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.</p>	<p>File Metadata</p>
<p>SMS Attachments</p>	<p>Media files</p>	<p>File attachments sent by SMS</p>	<p>Display/Gallery</p>
<p>WARNING -Backup may be Encrypted -</p>	<p>N/A</p>	<p>The backup may be encrypted (see 30.1.15 below).</p>	<p>N/A</p>

Wifi	com.apple.wifi.plist ade0340f576ee14793c607073bd7e8e409af07a8	List of Wi-Fi networks that the device joined (or auto joined). Information includes: <ul style="list-style-type: none">• 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
------	--	---	---------------

Appendix 10 - Index

APPENDIX 10 - INDEX

- Accessed
 - Date, 199
- Activation
 - Dongle, 43
 - Evaluation version offline, 22
 - Evaluation version online, 20
- AD1 to L01, 464
- Add Partition, 94
- Add with Options
 - Add Image, 178
- Apple Backups, 477
- Artifact
 - Selected, 136
- Artifacts
 - Definition, 209
 - Module, 209
- ASCII
 - Character distribution, 114
- Attributes, 198
- Auto Save, 189
- Bitlocker Encryption, 325
- Blur
 - Gallery view, 101
- Bookmarks
 - Module, 256
- Bookmarks Module, 253
- Boolean
 - Index search, 236
- BpB - Bytes per block, 126
- BpS - Bytes per sector, 126
- Branch plate, 88
- Byte Plot, 113
 - Examples, 114
- Carve
 - About file carving, 392
 - Cluster, Sector, Byte, 395
 - Disk view icon, 91, 566
 - Evidence Processor, 186
 - Hex Selection, 108
- Case
 - Close, 190
 - New, 168
 - Open, 171
 - Recent, 172
 - Save, 188
- Categories, 196
- Cell phone. *See* Phone
- Checked
 - Count, 136
 - Items, 136
- Clam
 - Anti Virus, 201
- Classification, 102
 - Custom, 106
 - Remove classification, 104
- Close
 - Case, 190
- Columns
 - Add, 137
- Compound file
 - Expand, 140
- Copy
 - Rows to clipboard, 163
- Copyright, 526
- Created, 199
- Credentials
 - Evidence module, 180
- Crypto Hash, 353
- Data fragment, 383, 389
- Data Views
 - Summary, 83
- Data-store, 232
- Date and Time
 - Adjust for Case, 344
 - Adjust for evidence, 342
 - Adjust in Evidence Processor, 186
 - Daylight Saving (DST), 340
 - Overview, 336
 - Registry Time Zone setting, 337
- Date range filter
 - Filter - Date Range, 155
- Deleted Files
 - FAT, 383
 - NTFS, 389
- Delphi Basics, 318
- Differential Hash, 353
- Disk view, 89
 - Custom color script, 314
 - Custom colors, 91
- Display view, 110

-
- docking, 70
 - Dongle. *See* Activation
 - DOS Mask, 160
 - Duplicates
 - De-duplicate, 359
 - Email
 - Module, 242
 - Email Module, 241
 - Evidence
 - Add, 172
 - Evidence Processor, 182
 - Explorer Tool, 162
 - Export
 - Delimited rows, 147
 - Files, 142
 - to L01, 144
 - Using a script, 144
 - Export Word List, 238
 - Extension, 198
 - Extract Metadata
 - Evidence Processor, 186
 - File Info
 - Button, 125
 - File List view, 197
 - File Name, 198
 - File signature analysis, 376
 - File slack
 - Definition, 553
 - Index search, 232
 - File System module, 193
 - File tree
 - File System workspace, 193
 - Filter
 - COLUMN filter tool, 157
 - File System module, 87
 - Scripts, 87, 163, 313
 - filter flags**, 155
 - Filtering, 155
 - Flags
 - Apply, 154
 - Clear, 155
 - Flat File Hash set, 362
 - Forensic Image Converter, 464
 - Fragmentation
 - File (FAT), 383
 - Full Path, 198
 - Fuzzy. *See* Index Search
 - Fuzzy hash, 358
 - Gallery View, 97
 - GUID
 - Preview, 167, 190
 - Hash
 - Acquisition hash display, 185
 - Flat File Hash Set, 362
 - Forensic Imager Acquisition, 65
 - Verify (Evidence Processor), 185
 - Verify L01, 146
 - Hash set, 360
 - Hex view, 108
 - Hit Offset (Device), 227
 - Hit Offset (File), 225
 - Hit Offset (Partition), 226
 - Hits
 - Keyword Result List, 224
 - HPA, 59
 - Hyperlinks
 - Reports, 272, 288, 296, 304
 - Icon Key, 565
 - Index Search
 - Creating an index, 231
 - Logging, 239
 - Module, 230
 - Searching an index, 235
 - Info view, 110
 - information.
 - test, 242
 - Installation, 31
 - Investigators
 - Add, Edit, Delete, 170
 - Is Deleted, 199
 - JBOD, 402
 - Jump List, 498
 - Keyboard Shortcuts
 - Disk View, 92
 - Keyword
 - Add, 216
 - Edit or Delete, 218
 - Group, 218
 - Import, 219
 - Regular expression (RegEx), 216
 - Keyword Search, 214
 - Results, 222
 - Run, 220
 - L01
 - Export, 144
 - Verify, 146
 - Language
 - FEX GUI Languages, 40
 - License agreement, 527
 - License Manager
 - GetData License Manager, 47
 - List view, 89
 - Live Boot, 419, 464
 - VMWare Workstation Shared Folders, 422
 - Logical Size, 199
 - MBR
-

-
- Search for known, 184
 - MD5, 348, *See* Hash
 - Metadata
 - Extract to columns, 120
 - View, 118
 - Mobile Phone. *See* Phone
 - Modified, 199
 - Module
 - Bookmarks, 253
 - Email, 241
 - Evidence, 165
 - File System, 192
 - Index Search, 229
 - Keyword Search, 213
 - Registry, 245
 - Reporting, 261
 - Scripts, 309
 - Network Licensing. *See* Licensing
 - Network Server
 - UDP Network Server, 174
 - OCR, 148
 - Offset
 - Keyword Search
 - File, Partition, Device, 224
 - Open
 - Case, 171
 - Ophcrack, 432
 - Orphans
 - NTFS, 390
 - Path
 - Case folders, 37
 - Program, 36
 - Registry keys, 37, 38
 - Working, 36
 - PCUnlocker, 435, 443
 - Phone
 - Carve, 395
 - Phonic. *See* Index Search
 - Photo DNA, 358
 - PhotoDNA*, 358
 - Physical size
 - Column, 199
 - Portable Case, 511
 - Preview
 - Evidence, 167
 - Project VIC, 370
 - Purchase orders, 26
 - RAID, 402
 - Hardware, 403
 - Software, 405
 - Recover Folders
 - FAT, 387, 391
 - NTFS, 391
 - Recover Partition. *See* Add Partition
 - RegEx
 - Column filter, 160
 - Keyword Search, 216
 - Quick start guide, 160
 - Registry
 - Location of registry files, 246
 - Module, 246
 - Registry file
 - Add from File System module, 247
 - Add standalone, 247
 - Report
 - Hyperlinks, 272, 288, 296, 304
 - Save
 - Case, 188
 - Scripting
 - Data recovery, 398
 - Scripts
 - Introduction to scripting, 318
 - Open, Copy, Rename, Delete, 317
 - Send to Module, 151
 - Servelet. *Network Server*
 - SHA. *See* Hash
 - Shadow Copy, 412
 - Background, 408
 - Mount in Forensic Explorer, 412
 - Shared Folders
 - VMWare Workstation, 422
 - Signature Analysis
 - Evidence processor, 186
 - Similarity Hash, 353
 - Sort
 - Multi column, 152
 - Persistent, 153
 - Remove, 153
 - Single column, 151
 - Startup.pas
 - Installation folder, 37
 - Script, 314
 - Stemming. *See* Index Search
 - Technical support, 531
 - Text view, 109
 - Thumbcache, 493
 - Thumbs.db, 493
 - Time Zone. *See* Date and Time
 - Tree view, 86, 193
 - Triage Report, 268
 - un-blur
 - Gallery view, 101
 - Undelete Partition. *Add Partition*
 - Undocking, 70
 - Uninstall, 41
 - User Datagram Protocol (UDP), 174
 - UUID
 - Apple Backup, 478, 555
-

VCARD
 Investigator, 170

VCF
 VCard Investigator Details, 170

Verification Hash
 Verify Device Hash, 348

Video
 Thumbnail viewing, 112

Virtual Box
 Live Boot, 420

VMWare
 Live Boot, 420

Volume Shadow Copy. *See* Shadow Copy

VSC or VSC. *See* Shadow Copy

Wibu CodeMeter Control Center, 49

Wildcards
 Index search, 237

Windows Event Log
 .evtx, 211

Word List, 238

XMP Metadata, 124