Forensic Explorer v5

Release Notes

Published: 10-Oct-19 at 12:48:02

Availability:

Forensic Explorer v5 is available to all users with **current maintenance**. There are no additional costs or requirements.

Installation:

Forensic Explorer v5 has a separate **installation** and **working** folder. It is possible to have both v4 and v5 installed on the same computer.

Important:

Forensic Explorer v5 can open a v4 case. However, once saved in v5, the case will no longer be backward compatible to v4. For this reason it is recommended that users make a working copy of any v4 case prior to opening with v5.

This Document:

This document is intended only as a summary of changes between Forensic Explorer v4 and v5. It is not an exhaustive list. Numerous additional updates have been made for speed and stability.

1.1 CONTENTS

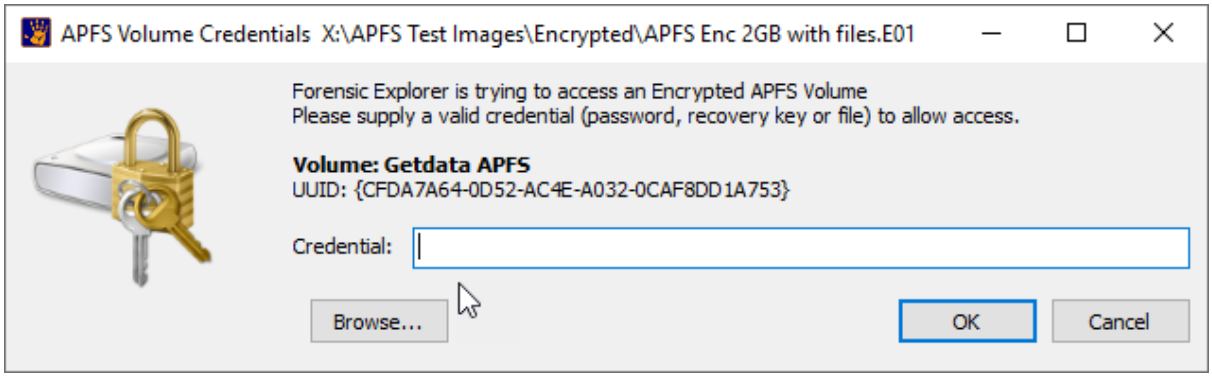
1. STARTUP AND CASE LOAD TIME

Once installed for the first time, Forensic Explorer v5 has a significantly faster startup time through the program splash screen. This is achieved primarily by pre-compiling scripts and filters to .bin files on first install. Case load time is also significantly faster.

2. APPLE AFPS ENCRYPTION

Support has been added for MAC APFS encryption. A prompt will show for credentials when an image or physical disk is added.

Figure 1: APFS encryption prompt on add image



3. BOOKMARKS

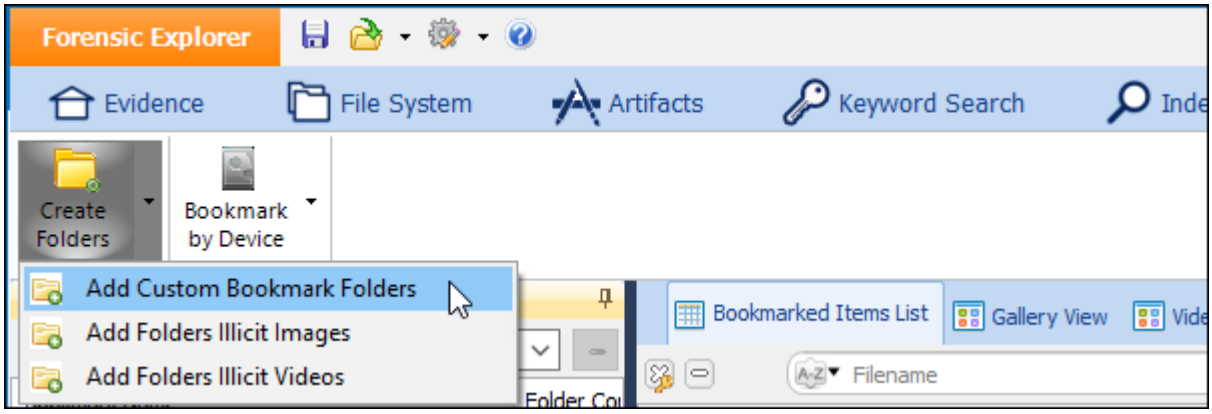
3.1 BOOMARKS TOOLBAR

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

3.2 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 2: Bookmarks toolbar

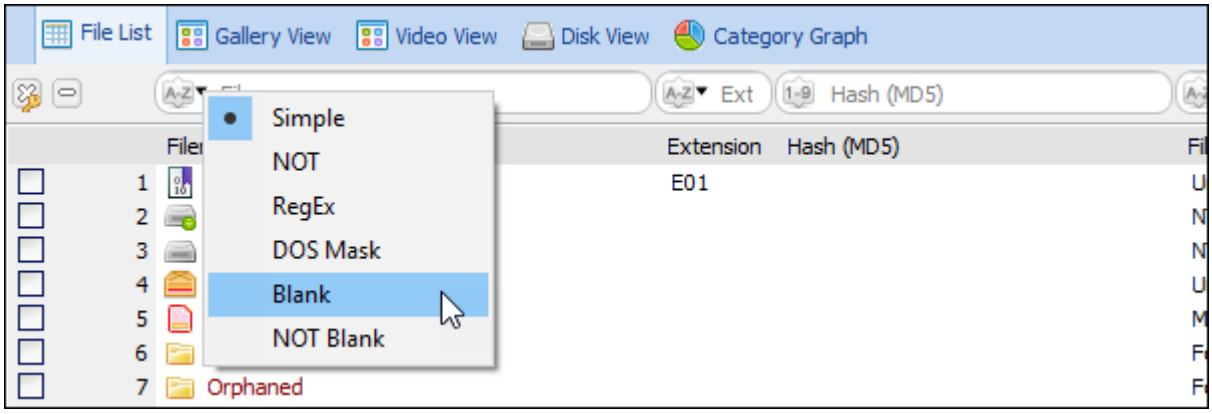


4. COLUMN FILTER TOOL

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.

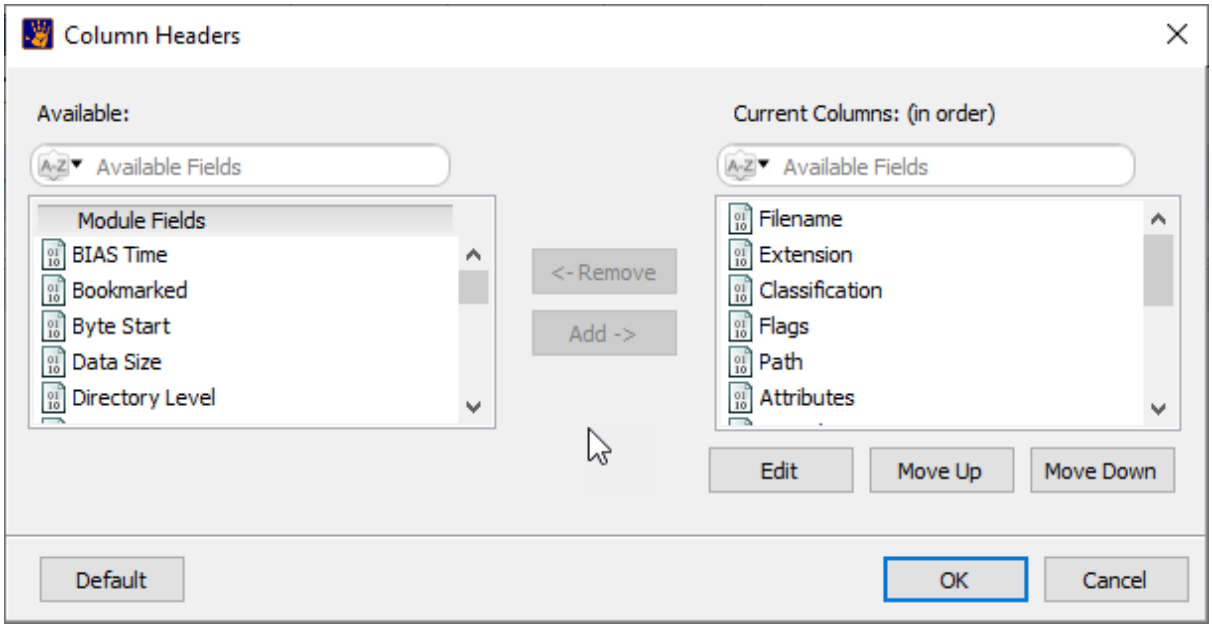
Figure 3: Column Filter Tool



5. COLUMN SELECTION

The File List column selection tool has been improved to enable column name filtering and more flexible management options. A Default button has been added to quickly return to default column layout.

Figure 4: File List Edit Columns



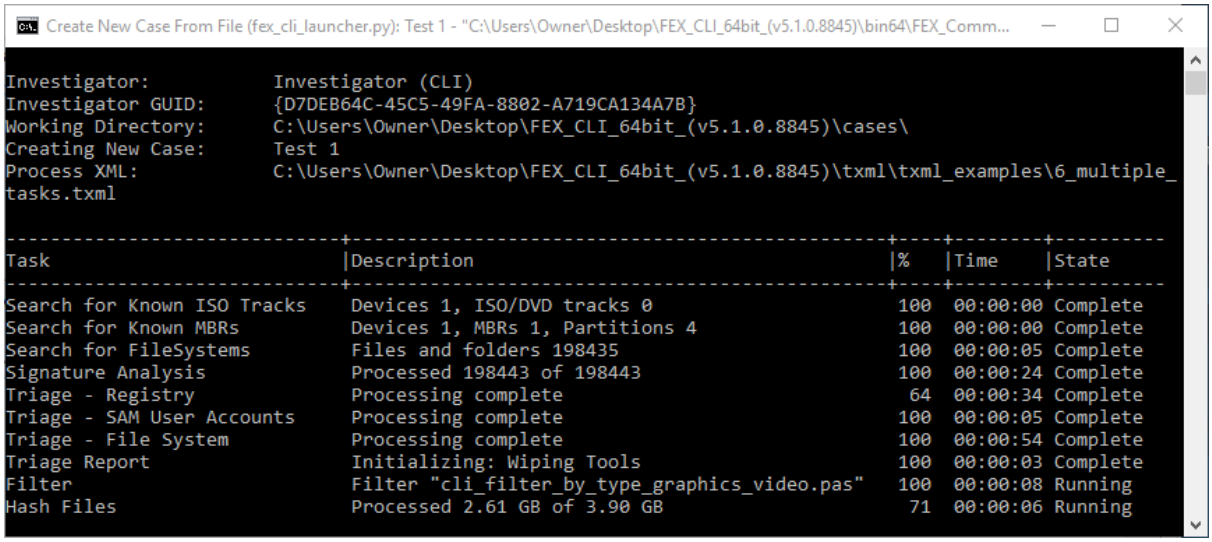
6. COMMAND LINE

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.

Figure 5: FEX CLI

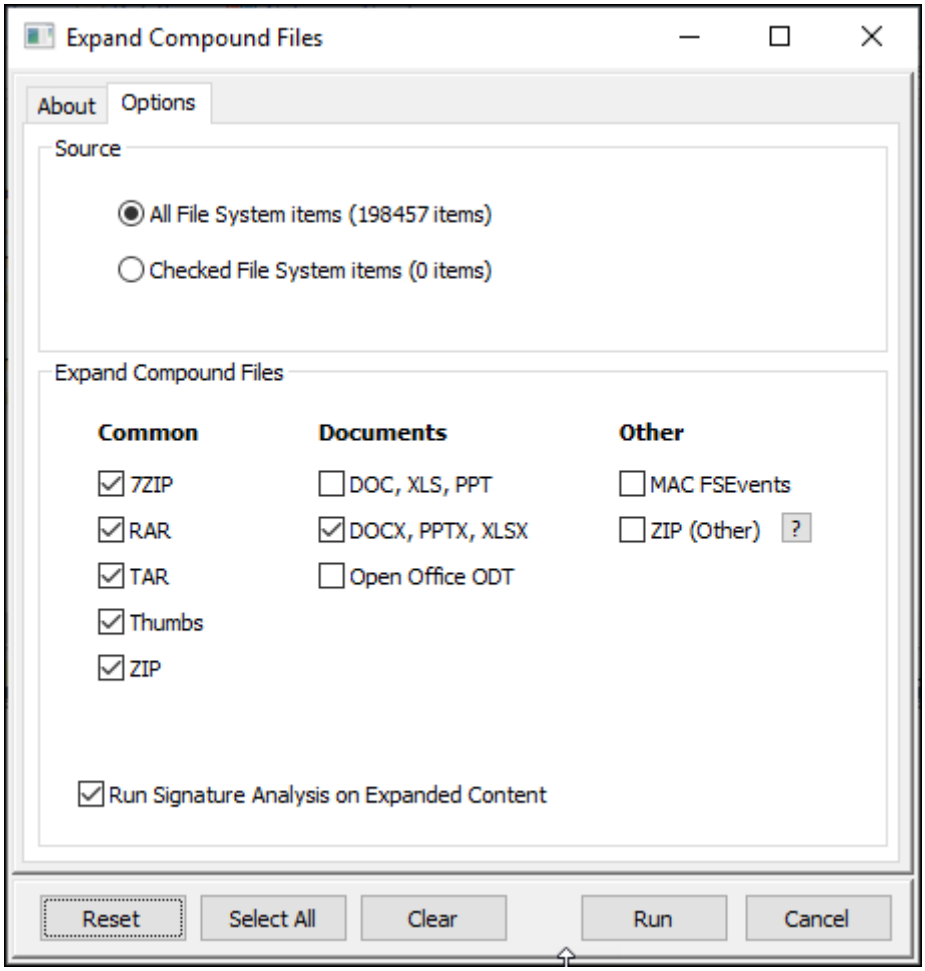


7. COMPOUND FILES

7.1 7-ZIP

Additional support has been added for the processing of 7-Zip compressed files. 7-Zip has been added to the File System module Expand Files button:

Figure 6: File System module, Expand Compound Files



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.

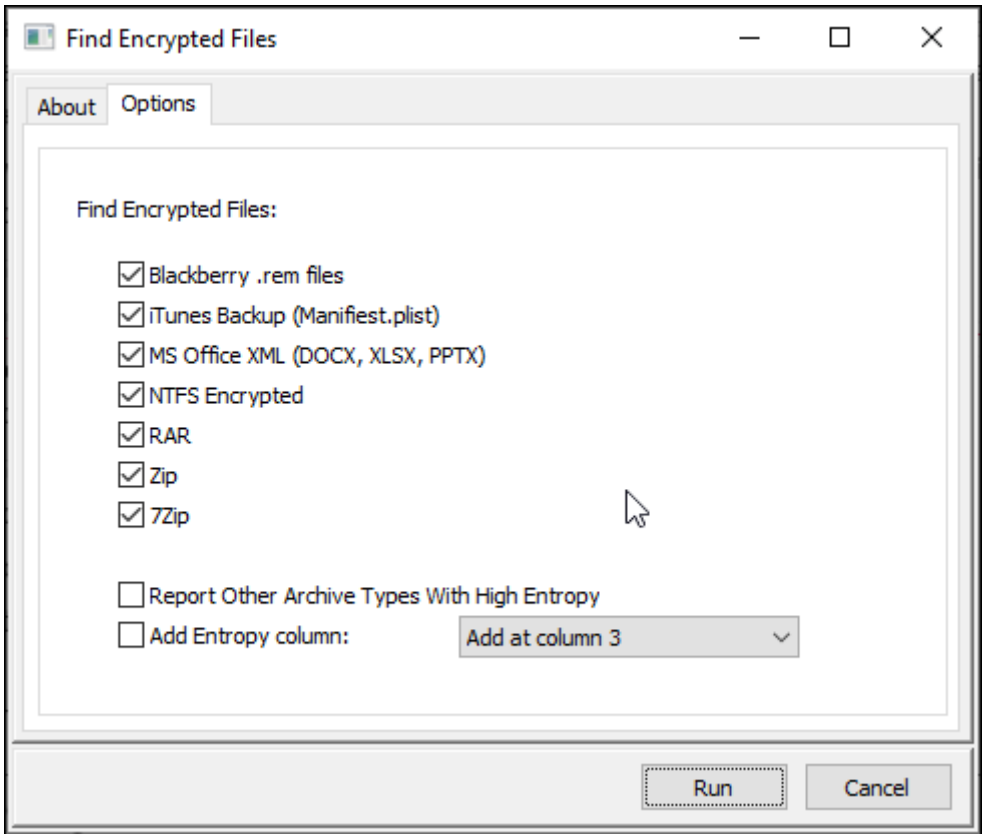
8. EMAIL MODULE

Microsoft PST and OST email formats have been updated allowing for significant improvements in processing speed.

9. ENCRYPTED FILE DETECTION

Encrypted 7-Zip files are now detected by the File System > Analysis Programs > Encrypted Files script:

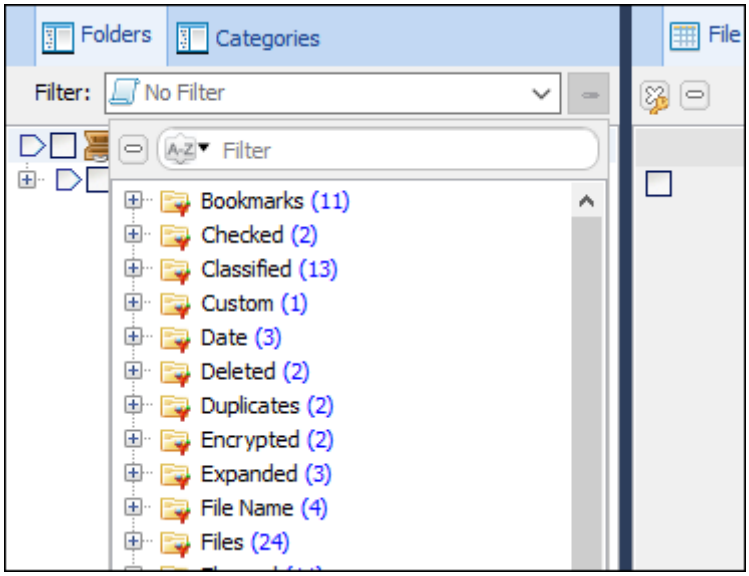
Figure 7: Find encrypted 7z files



10. FILTER

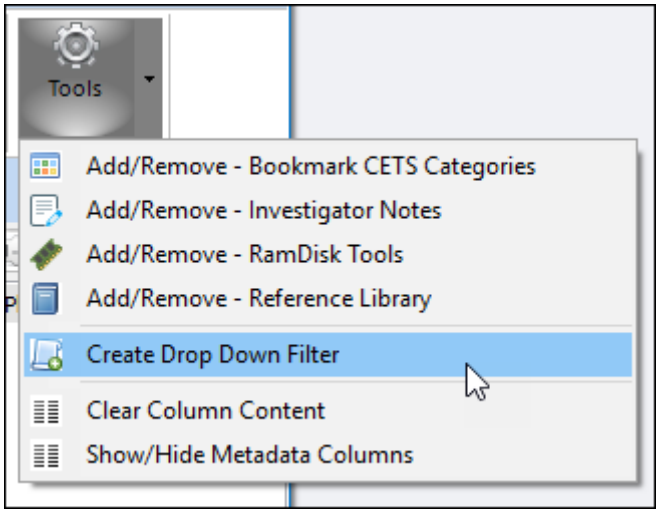
The drop down filter at the top of the folder tree has been updated to expand the number of available filters. A search bar enables fast access via filter name.

Figure 8: Redesigned Folders filter



A Create Drop Down Filter script enables custom filters to be added.

Figure 9: File System > Tools > Create Drop Down Filter



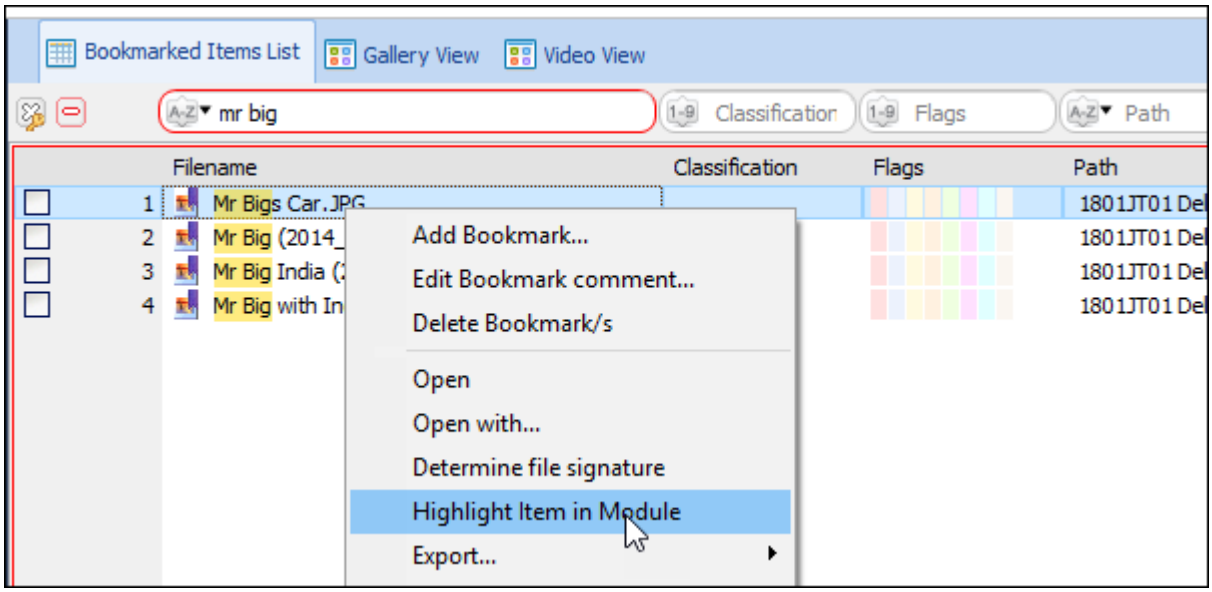
11. HASH SETS - NSRL

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.

12. HIGHLIGHT ITEM IN MODULE

Improved the functionality of Highlight Item in Module to switch between modules.

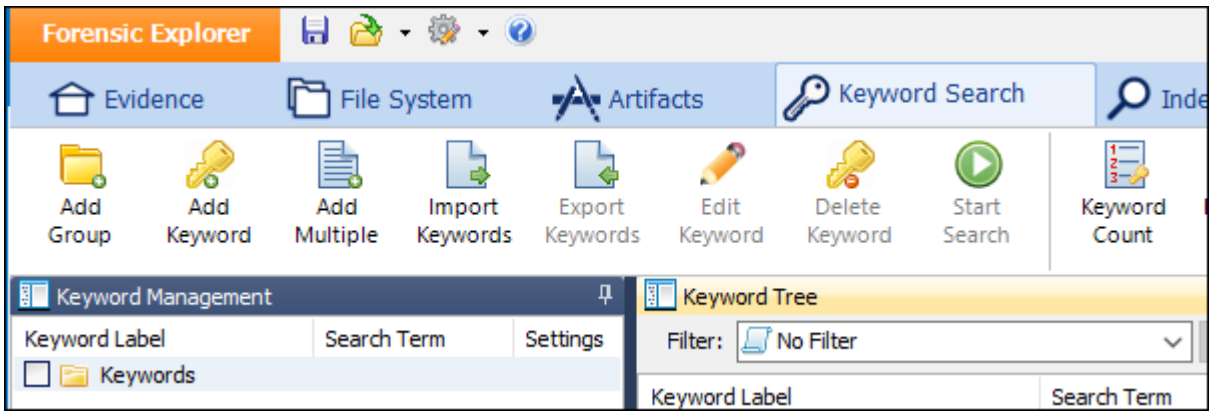
Figure 10: Highlight Item in Module



13. KEYWORD SEARCH

Keyword search buttons have been moved to the module toolbar.

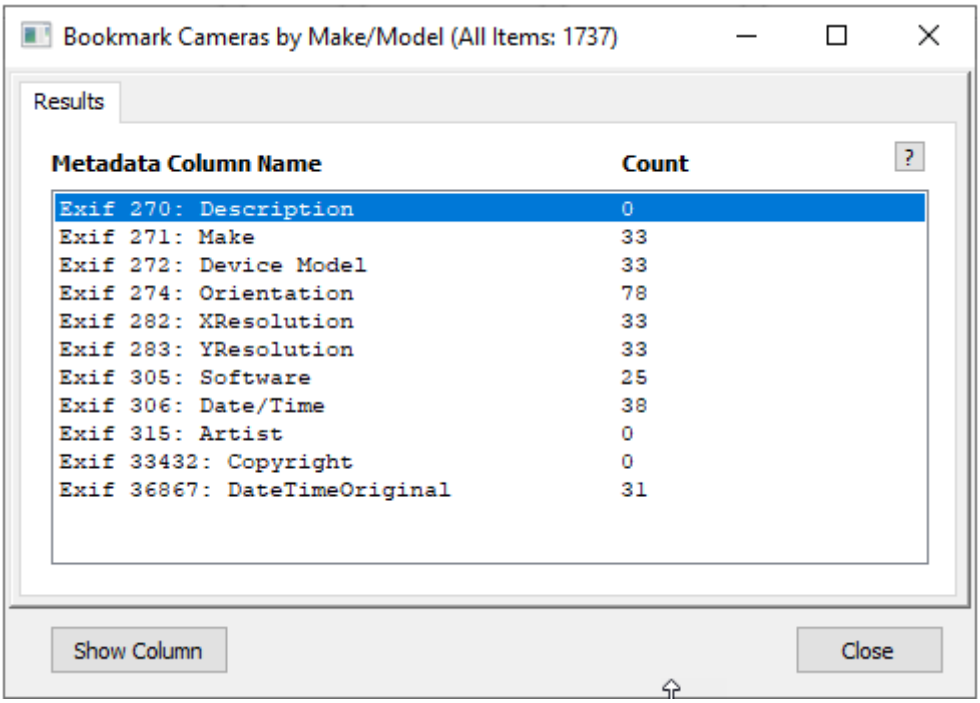
Figure 11: Keyword search module



14. METADATA

The File System module Extract Metadata script has been updated with a GUI to simplify the process and enable columns to be selected and added from the results window.

Figure 12: Extract Metadata



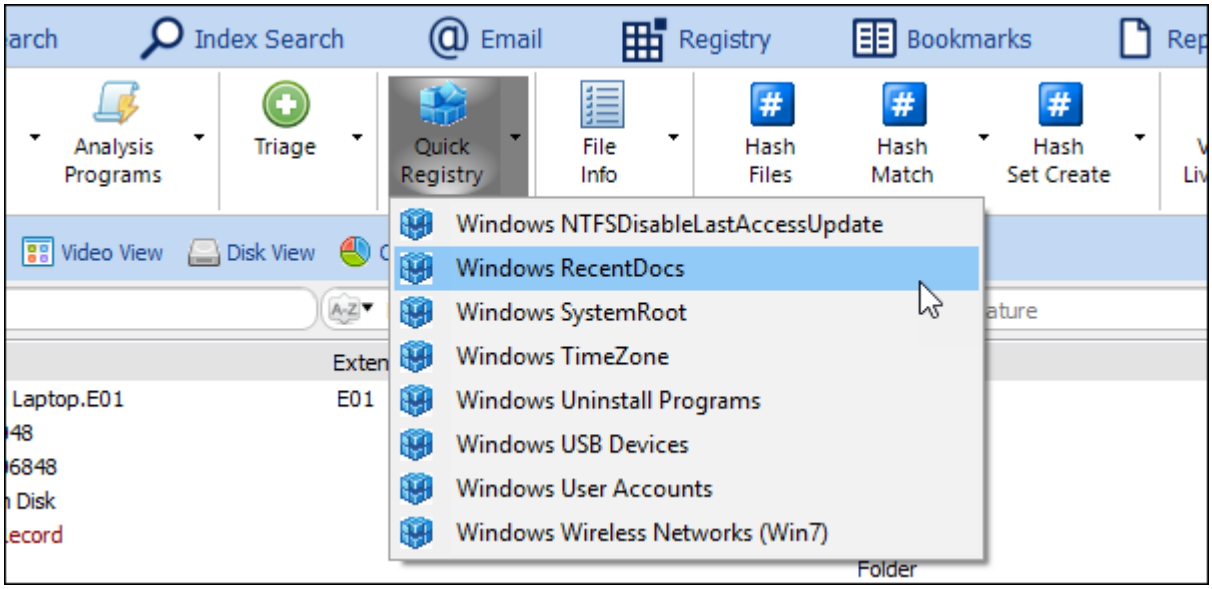
15. PROGRESS WINDOW

The progress window now clears between cases.

16. REGISTRY

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

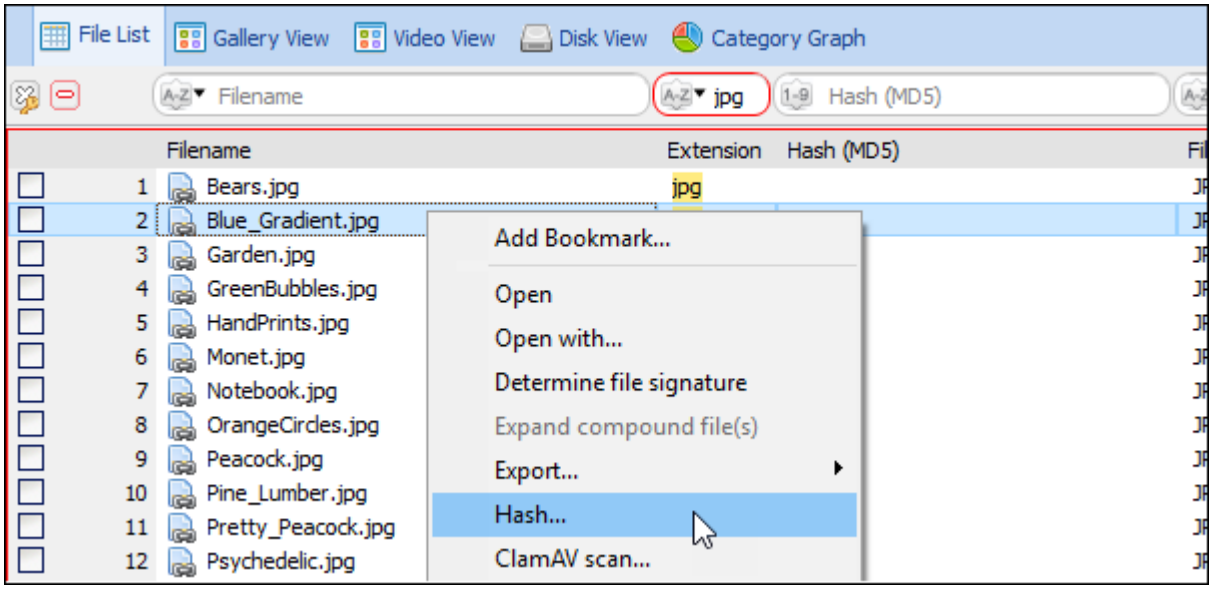
Figure 13: File System module Quick Registry



17. RIGHT-CLICK MENU OPTIONS

Right-click menu options have been enhanced with Hash and ClamAV options.

Figure 14: Hash from File List right click menu

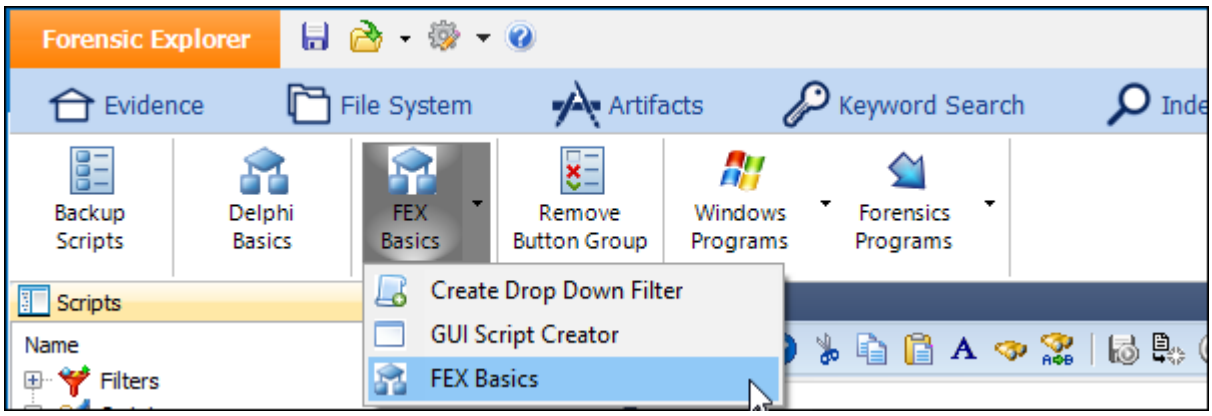


18. SCRIPTING

Added scripts, including:

- FEX Basics: Quickly create a working example of FEX specific code.
- GUI Script Creator: Quickly create a working GUI script template.

Figure 15: FEX Basics

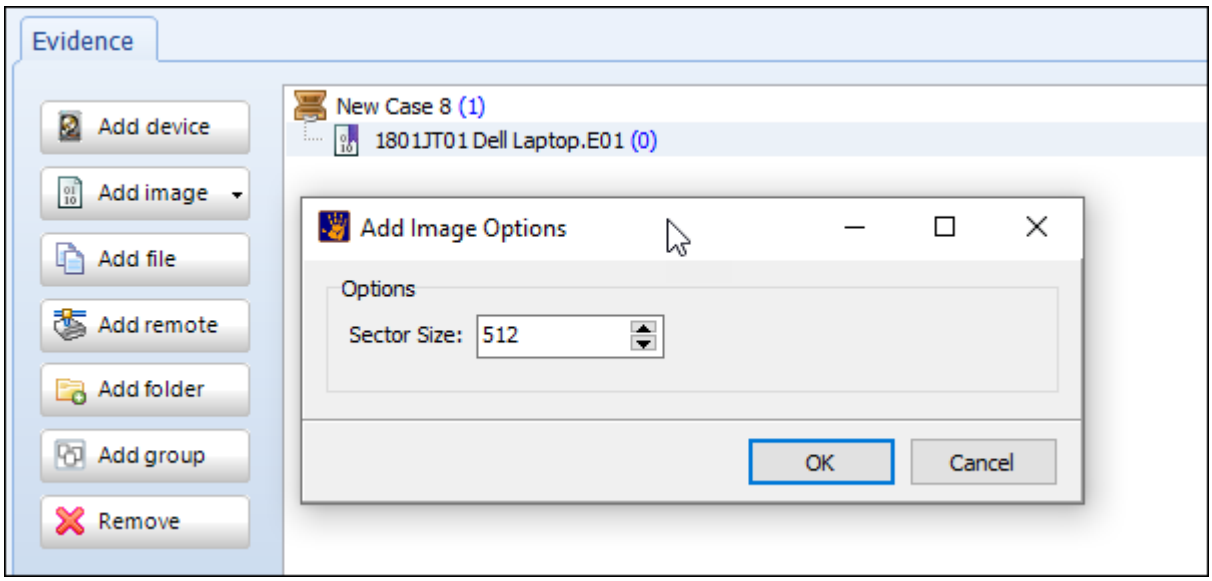


- Parse ESE to CSV (File System > Analysis Programs).
- Windows 7 Thumbcache – Parse Windows.edb (File System > Analysis Programs).

19. SECTOR SIZE ADJUSTMENT

A manual sector size adjustment has been added to the Evidence module. This 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.

Figure 16: Evidence module, add evidence sector size adjustment



20. SIGNATURES, PROPERTIES, METADATA

Updated file types for signature analysis and file carving. Added new signatures including:

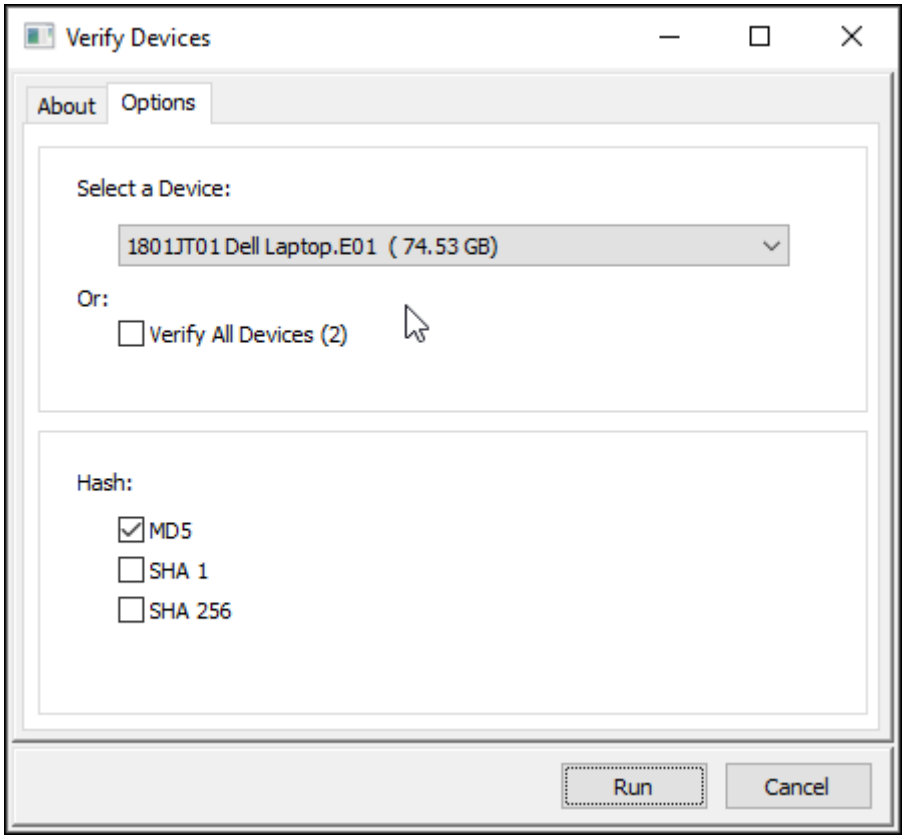
- Adobe Type 1 Font
- Apple Document
- Blackberry Encrypted file
- NTFS Log file
- Visi CAD
- Web Browser Cache Database

Added additional file properties for RTF, ORF, RW2, LNK, BZIP etc.

21. VERIFICATION

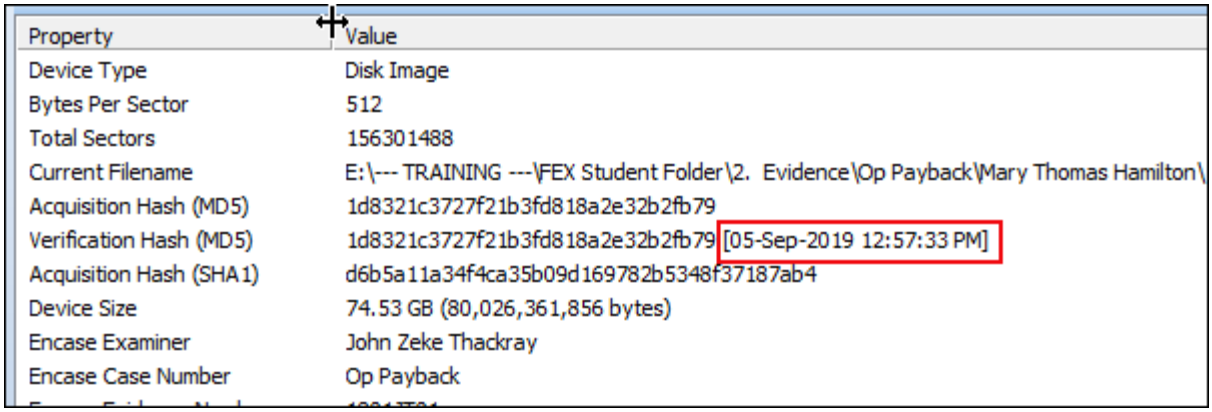
The Evidence module Verify Devices script has been updated to increase verification speed and allow for multiple image verification in a single pass.

Figure 17: Evidence module, Verify Devices



The verification hash is written to the Evidence module information window so that it is possible to know the last date and time the image was verified.

Figure 18: Evidence module, last validation date/time



22. VIDEO VIEW

A Video view tab has been added showing time segment video thumbnails. Individual videos can be played in this view by sliding the mouse across the thumbnail (right for forward play, left for reverse play). The zoom slide bar has been increased to enhance viewing.

Figure 19: Video View