OSForensics

OSForensics

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: June 2017

Table of Contents

1 Introduction and Overview

PassMark OSForensics is a powerful, comprehensive forensics tool for discovering, identifying and managing digital evidence that is found in computer systems and digital storage devices. OSForensics is organized into a collection of modules for simplifying the task of analyzing the vast amounts of data on live systems and storage media with a simple, easy-to-use modular interface. Such modules include a File Name Search module which can identify evidence material by file name in seconds, as well as more sophisticated module such as a Deleted File Search module for identifying harder to locate digital evidence artifacts.

For a summary of the included modules and functionality, see the Features page.

2 How to Purchase OSForensics

Price

US Dollars: $899 (single user)

Purchase Online Here

Discounts apply when ordering 5 or more copies at once.

What happens when you order

After the order is processed, a License Key will be returned (via E-Mail). This Key is then entered with the User Name into the initial window. At this point the program then changes permanently into the full licensed version.

What you get when you license the software

- 6 Months Free Email and Phone Support in addition to normal forum support.

  http://www.passmark.com/about/contact_us.htm

- Free minor upgrades & bug fixes as they become available

  http://www.osforensics.com/download.html

- The removal of the initial startup window.

Unlocked advanced features

- Search for alternate file streams.
- Sort found files by image color.
- Use multiple processor cores to speed up decryption.
- Customize system information gathering.
- Import / Export Hash Sets
- Maximum of 3 cases limitation is removed
- Maximum of 10 items per case limitation is removed
- Maximum of 10 recent activity items allowable to be exported is removed.
- Maximum of 2,500 files and emails allowable to be indexed is removed.
- Maximum of 250 index search results limitation is removed.
- Maximum of 5 login details per browser limitation is removed.
- Restore multiple deleted files at once.
- View NTFS $I30 directory entries.
- Watermark in web browser screen capture is removed.
- Bootable without an operating system.

Confidentiality

All personal details supplied when placing an order will be strictly confidential. Online orders will only be accepted over a secure, encrypted connection.

Multi-user & Site Licenses

Please contact us for details if you require multi-user or site licensing for your organization.

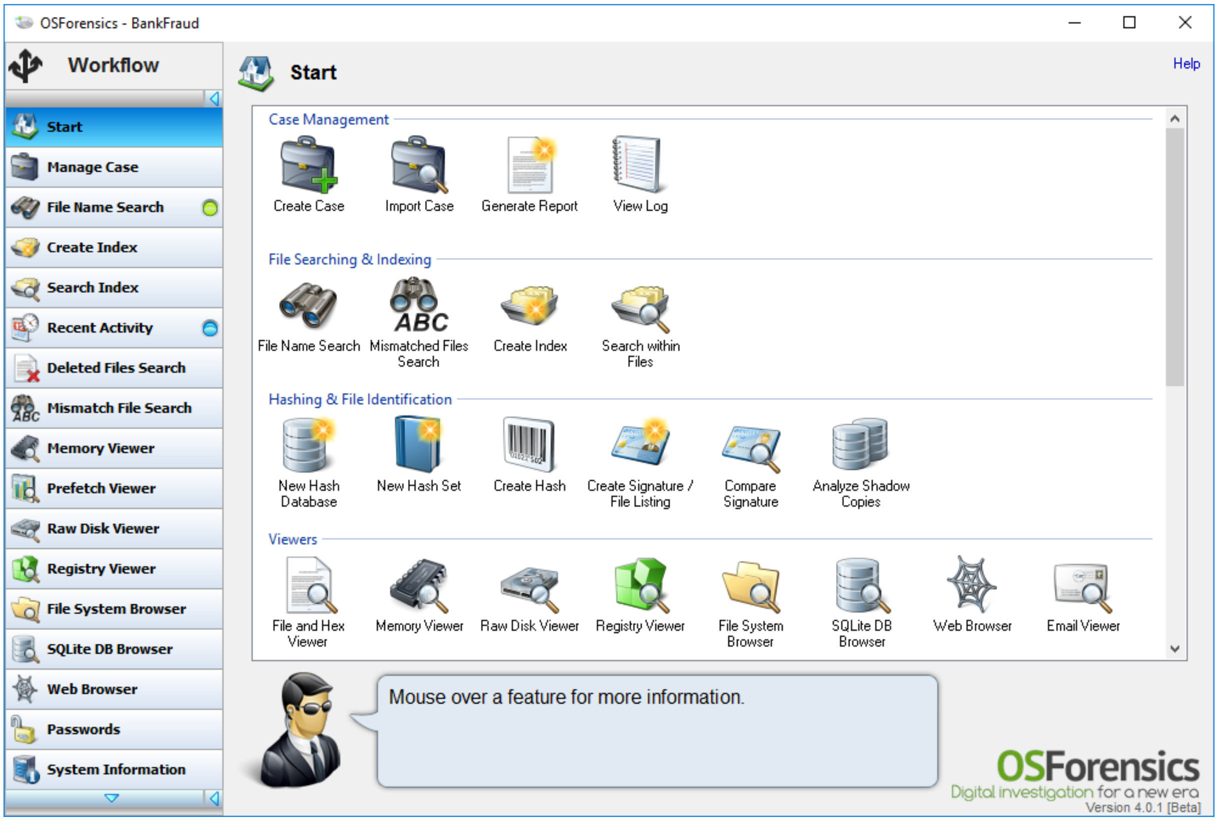
Questions & more information

If you have any questions we would be happy to hear about them. Contact

sales@passmark.com

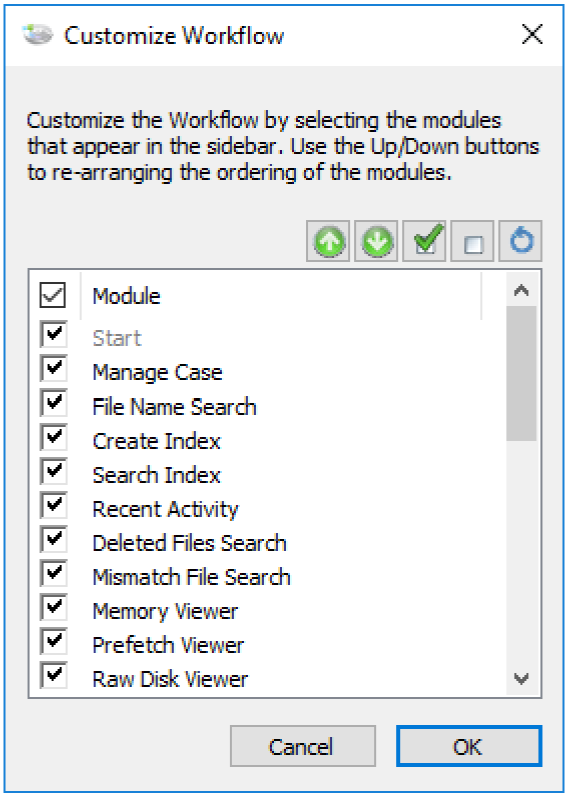
3 Navigating OSForensics

OSForensics is organized into multiple feature modules for discovering, identifying and managing digital forensics artifacts.



Mouse over a feature for more information.

The Workflow navigation buttons on the left side of the window allows the investigator to switch between multiple modules simultaneously, allowing forensic analysis operations to be performed in parallel. The order of the navigation buttons in the Workflow can be customized to reflect the chronological order of the organization's forensic workflow. The workflow order can by customized by right-clicking any navigation button and selecting 'Customize Workflow'. Alternatively, there is a 'Customize Workflow' icon under the 'Housekeeping' group in the Start Window.



Customize Workflow

Customize the Workflow by selecting the modules that appear in the sidebar. Use the Up/Down buttons to re-arranging the ordering of the modules.

☑ Module
☑ Start
☑ Manage Case
☑ File Name Search
☑ Create Index
☑ Search Index
☑ Recent Activity
☑ Deleted Files Search
☑ Mismatch File Search
☑ Memory Viewer
☑ Prefetch Viewer
☑ Raw Disk Viewer

In addition to the Workflow navigation buttons, all modules can be accessed via the Start Window when OSForensics starts up.

The start window contains a brief description of each feature on mouse over. A green pulsating light appearing next to the sidebar button means that the module is currently performing a task. A blue light means that a task has been completed.

4 Features

OSForensics contains a collection of modules for searching, collecting, analyzing and recovering digital artifacts that can be used as legal evidence in court. The main features of OSForensics are outlined as follows.

Case Management

This module is used to aggregate results from all the other modules into a single location, a Case, allowing for later analysis of the findings as a whole and reporting on findings.

File Name Search

This module allows for searching for files/directories via its filename.

Indexing

Indexing allows for full text searching within the contents of a file. Also capable of searching within email archives and pulling text out of unallocated disk sectors.

Recent Activity

This module allows an investigator to scan the system for evidence of recent activity, such as accessed websites, USB drives, wireless networks, and recent downloads.

Deleted Files Search

Search for and recover files that have been recently deleted from the hard drive.

Mismatch Search

Finds files that have a file extension that is different from what the contents of the file suggests. Eg. A .jpeg file renamed to a .txt file.

Memory Viewer

The memory viewer allows an investigator to collect and analyze digital evidence in volatile memory storage. Due to the non-persistent nature of memory, some digital evidence may only be available on a live system.

Prefetch Viewer

The Prefetch viewer displays the information stored by the operating system's Prefetcher, which includes when and how often an application is run.

Raw Disk Viewer

The raw disk viewer displays the raw sector-by-sector contents of a disk. Data hidden in the sectors outside the file system can be identified and analyzed with this module.

Registry Viewer

The registry viewer allows Windows Registry Hives, including the live system where files can be locked / in use, to be opened and viewed within OSForensics.

File System Browser

The file system browser displays all devices added to a case in a hierarchical fashion, similar to Windows Explorer. Unlike Explorer, additional information specific to forensics analysis are displayed.

SQLite Database Browser

The SQLite database browser displays the contents of SQLite database files in an organized manner, allowing for ease of navigation and searching.

Web Browser

The web browser provides a basic web viewer with forensics capabilities. This includes the ability to save screen captures of web pages and add them to the currently opened case.

Passwords

Recover and decrypt passwords from various sources.

System Information

The detailed information about the system's core components can be viewed and exported.

Verify/Create Hash

Create hashes (SHA1, MD5, CRC32) of files or entire hard disk.

Hash Sets

A hash set is a tool to quickly identify known safe or known suspected files to reduce the need for further time-consuming analysis.

Signatures

Signatures are snapshots of a system's directory structure at different points in time. Signatures can be compared in order to identify files that have been added, deleted and changed.

Drive Preparation

Drive Preparation allows byte pattern verification tests to be performed on fixed and removable drives attached to the system.

Forensic Imaging

Save a bit-by-bit copy of a disk into an image file. Restore an image file back to the disk. Create a logical image of files/directories of interest.

Internal Viewer

The internal file viewer allows previewing of most common file formats from within OSForensics without needing to open an external application.

Email Viewer

The e-mail viewer provides a simple interface for browsing and analyzing e-mail messages with forensics capabilities.

Thumbnail Cache Viewer

The thumbnail cache viewer extracts the thumbnail images stored in Windows' thumbnail cache files for viewing. Thumbnail cache files may contain evidence of images that have been deleted on the system.

ESE Database Viewer

The ESE database viewer displays the tables and records contained within ESE database files. Various Microsoft applications including Windows Search and Microsoft Exchange Server store data with potential forensics value in the ESE database file format.

$UsnJrnl Viewer

The $UsnJrnl viewer parses and displays the log records stored in the NTFS $UsnJrnl volume change journal. This information is useful for identifying suspect files (eg. malware) that no longer exist in the file system or $MFT.

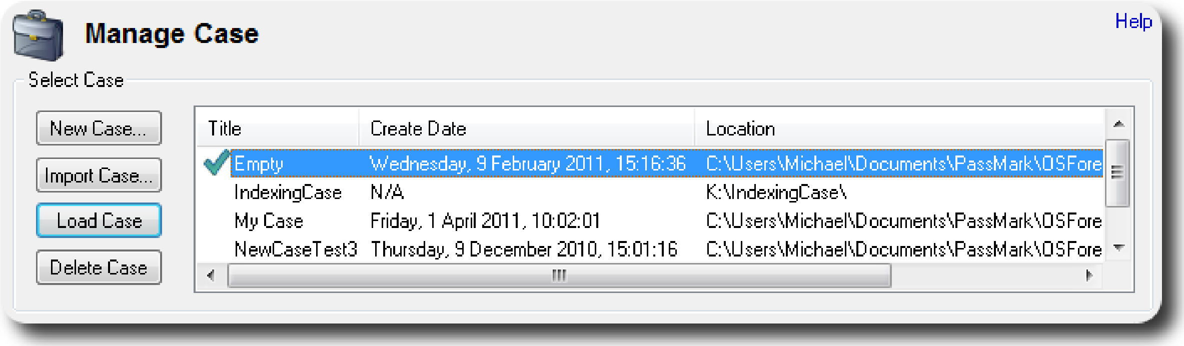
Plist Viewer

View the contents of Plist (property list) files which are commonly used by OSX and iOS to store settings and properties.

4.1 Case Management

In the case management window can be used to create and manage cases. Cases are used to group together findings from other functions into a single location that can be exported or saved for later analysis.

A new case must be created, or a previous case loaded, before it is possible to add items to a case from the other functions.



Title	Create Date	Location
✓ Empty	Wednesday, 9 February 2011, 15:16:36	C:\Users\Michael\Documents\PassMark\OSFore
IndexingCase	N/A	K:\IndexingCase\
My Case	Friday, 1 April 2011, 10:02:01	C:\Users\Michael\Documents\PassMark\OSFore
NewCaseTest3	Thursday, 9 December 2010, 15:01:16	C:\Users\Michael\Documents\PassMark\OSFore

New Case
Clicking the new case button will allow you to generate a new empty case in which to collect data into. A case must have a name, and may have an associated investigator although this is not required.

By default a case is created as in the OSForensics folder situated in the user's My Documents folder. On creation a sub folder will be created in the target location that will contain the case, there is no need to select an empty folder.

The timezone selection when creating a new case is used to change the display of times to match a preferred timezone, internally where possible all times are stored in UTC. Note that daylight saving time is not automatically accounted for.

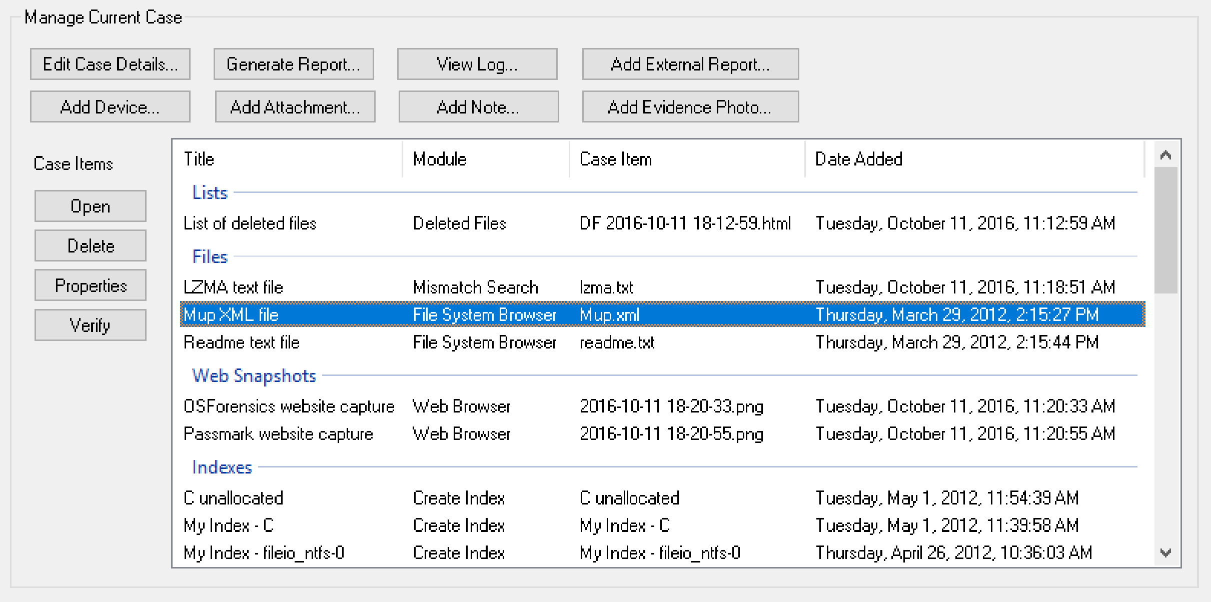
Import Case
Add a case to the list that is not in the default case folder and load it.

Load Case
Loads the currently selected case from the list. You can also simply double click in the list to perform the same action.

Delete Case
Deletes the currently selected case. The user is given the option to backup the case data to a specified location before deleting.

Case Manager

Once a case is created/opened, the contents of the case can be managed from this window. All Case items are displayed in the list, grouped by the Case item type.



Title	Module	Case Item	Date Added
Lists			
List of deleted files	Deleted Files	DF 2016-10-11 18-12-59.html	Tuesday, October 11, 2016, 11:12:59 AM
Files			
LZMA text file	Mismatch Search	lzma.txt	Tuesday, October 11, 2016, 11:18:51 AM
Mup XML file	File System Browser	Mup.xml	Thursday, March 29, 2012, 2:15:27 PM
Readme text file	File System Browser	readme.txt	Thursday, March 29, 2012, 2:15:44 PM
Web Snapshots			
OSForensics website capture	Web Browser	2016-10-11 18-20-33.png	Tuesday, October 11, 2016, 11:20:33 AM
Passmark website capture	Web Browser	2016-10-11 18-20-55.png	Tuesday, October 11, 2016, 11:20:55 AM
Indexes			
C unallocated	Create Index	C unallocated	Tuesday, May 1, 2012, 11:54:39 AM
My Index - C	Create Index	My Index - C	Tuesday, May 1, 2012, 11:39:58 AM
My Index - fileio_ntfs-0	Create Index	My Index - fileio_ntfs-0	Thursday, April 26, 2012, 10:36:03 AM

Manage Current Case

Edit Case Details
Edit the properties (eg. name, investigator, time zone, logging options) of the case.

Generate Report
Creates a HTML report of the contents of the case. OSForensics has a number of built-in templates to choose from, which is fully customizable. You can also create your own custom template.

View Log
If logging is enabled for the case, opens the log viewer for viewing the log entries.

Add External Report
Add a report (eg. HTML, PDF) generated from an external tool to the case.

Add Device
Add a storage device to the case for analysis.

Add Attachment
Add a generic file to the case as an attachment.

Add Note
Add a note to the case as a text file.

Add Evidence Photo
Add an evidence photo (eg. hard disk) to the case.

Case Items

Open
Opens the currently selected case item.

Delete
Deletes the currently selected case item.

Properties
Show the properties for the currently selected case item, properties window also allows editing the comments for this item.

Verify
Calculates the SHA1, SHA256 and MD5 hashes for the file and compares them to the stored values.

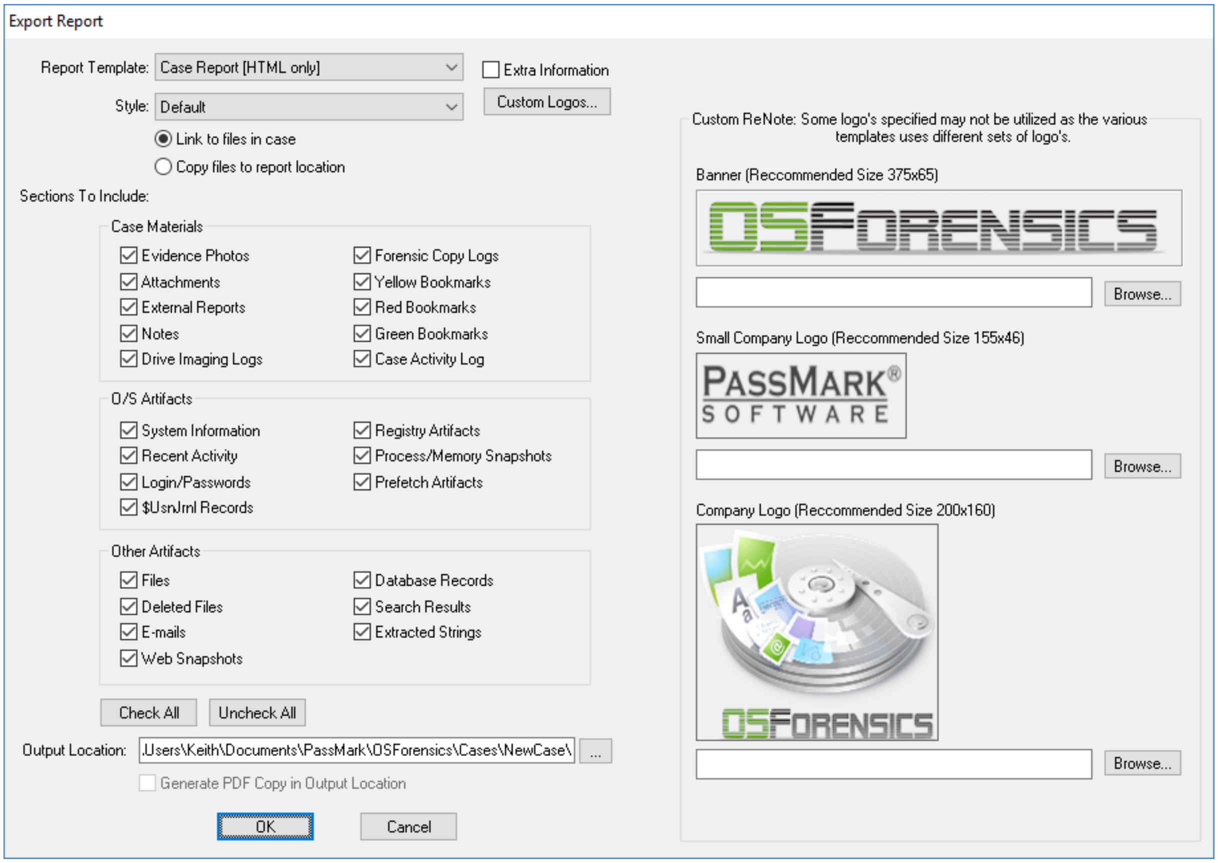
4.1.1 Customizing Report Appearances

OSForensics generates reports as HTML web pages, which allows the style, layout and appearance to be modified with any web authoring application of your choice (or you can directly edit the HTML and CSS). Customizable elements include fonts, colors, and page layout.

Reports are generated using the fully customizable report templates included in the OSForensics install. The report templates can be found in the OSForensics Program Data folder.

There are several pre-installed report templates corresponding to a report type, which are stored as separate folders containing a set of template files. At the very minimum, a single HTML file, report.html, must exist in each folder which serves as the index page that OSForensics shall use to create the report. In addition, some templates also contain a set of additional HTML files corresponding to each section of the report (eg. files.html, deleted-files.html, notes.html). These files are required in order to generate working links to the corresponding sections via the report.html file.

You can include images (for company logos, headers or footers), CSS files, or JS files. All files in the folder will be copied across and included with the generated report.



Export Report

Report Template: Case Report [HTML only]
☐ Extra Information
Style: Default
● Link to files in case
○ Copy files to report location

Sections To Include:

Case Materials
☑ Evidence Photos ☑ Forensic Copy Logs
☑ Attachments ☑ Yellow Bookmarks
☑ External Reports ☑ Red Bookmarks
☑ Notes ☑ Green Bookmarks
☑ Drive Imaging Logs ☑ Case Activity Log

O/S Artifacts
☑ System Information ☑ Registry Artifacts
☑ Recent Activity ☑ Process/Memory Snapshots
☑ Login/Passwords ☑ Prefetch Artifacts
☑ $UsnJrnl Records

Other Artifacts
☑ Files ☑ Database Records
☑ Deleted Files ☑ Search Results
☑ E-mails ☑ Extracted Strings
☑ Web Snapshots

Output Location: .Users\Keith\Documents\PassMark\OSForensics\Cases\NewCase\
☐ Generate PDF Copy in Output Location

Custom ReNote: Some logo's specified may not be utilized as the various templates uses different sets of logo's.
Banner (Reccommended Size 375x65)
Small Company Logo (Reccommended Size 155x46)
Company Logo (Reccommended Size 200x160)

Report Template
List of report templates found in the Program Data folder that shall be used to generate the report.

Style
List of stylesheets available for the selected report template. Multiple styles can exist for each report and each CSS file in the report's folder will be listed as an available style. When creating the report, OSForensics will replace the HTML comment tag "<!--OSF_CSS_NAME-->" with the selected style name.

Link to files in case
Hyperlinks to case items in the report shall link directly to the files stored in the Case directory

Copy files to report location
Files stored in the Case shall be copied to the report folder. Hyperlinks to case items in the report shall link to the newly copied Case files in the report directory.

Extra Information
If checked, extra details such as MD5/SHA-1/SHA-256 hash values for each Case item shall be included in the report.

Custom Logos... *(Pro only)*
Organization-specific logos and banners can be specified here to include in the report

Sections to Include
Specify the sections to include/exclude in the report. Each section corresponds to a specific category of items added to the case.

Output Location
Specify the location where the report files shall be generated.

Generate PDF Copy in Output Location
If supported by the report template, specifies whether a copy of the report shall be generated in PDF format in the output location.

Editing HTML Template Files

The report templates can be found in the OSForensics Program Data folder, which is typically located in the following location:

```
   C:\ProgramData\PassMark\OSForensics\ReportTemplates\ (Vista and newer)

   C:\Documents and Settings\All Users\Application Data\PassMark
\OSForensics\ReportTemplates\ (XP)
```

NOTE: *All HTML template files must be saved in UTF-8 encoding (character set).*

The template HTML files are fully editable and are used to generate the final report files. OSForensics shall scan the template files for specific tags that correspond to a certain Case element, and replace it with the appropriate content. The following table summarizes the HTML comment tags that are recognized by OSForensics and replaced accordingly.

<!--OSF_CSS_NAME-->	This will be replaced with a reference to the selected style sheet.

<!--OSF_CASE_TITLE-->	This is the Case Name.
<!--OSF_CASE_INVESTIGATOR-->	This is the Investigator of the case.
<!--OSF_CASE_ORGANIZATION-->	This is the Organization details from the case.
<!--OSF_CASE_CONTACTDETAILS-->	This is the Contact details from the case.
<!--OSF_CASE_CUSTOMFIELD1_NAME-->	This is the name of the first custom field, if defined in the case.
<!--OSF_CASE_CUSTOMFIELD1_VALUE-->	This is the value of the first custom field, if defined in the case.
<!--OSF_CASE_CUSTOMFIELD2_NAME-->	This is the name of the second custom field, if defined in the case.
<!--OSF_CASE_CUSTOMFIELD2_VALUE-->	This is the value of the second custom field, if defined in the case.
<!--OSF_CASE_TIMEZONE-->	This is the Timezone from the case.
<!--OSF_CASE_DEFAULTDRIVE-->	This is the default drive selected in the case
<!--OSF_CASE_CASEFOLDER-->	This is the where the OSForensics case file is saved
<!--OSF_CASE_CASEDATE-->	This is the date that the case was created
<!--OSF_CASE_CASESHORTDATE-->	This is the date that the case was generated without timezone information .
<!--OSF_CASE_REPORTDATE-->	This is the date that the report was generated.
<!--OSF_CASE_REPORTSHORTDATE-->	This is the date the report was generated without timezone information .
<!--OSF_CASE_EVIDENCEIMAGES-->	This table contains all evidence images added to the case
<!--OSF_CASE_ATTACHMENTSTABLE-->	This table contains all attachments added to the case.
<!--OSF_CASE_NOTESTABLE-->	This table contains all notes added to the case.
<!--OSF_CASE_BOOKMARKSGREEN-->	This table contains all green bookmarks added to the case.
<!--OSF_CASE_BOOKMARKSYELLOW-->	This table contains all yellow bookmarks added to the case.
<!--OSF_CASE_BOOKMARKSRED-->	This table contains all red bookmarks added to the case.

<!--OSF_CASE_ACQUIREDIMAGES-->	This table contains the logs of images acquired using the Drive Imaging module that have been added to the case.
<!--OSF_CASE_FORENSICSCOPY-->	This table contains the logs of forensic copy operations that have been added to the case.
<!--OSF_CASE_EXTERNALREPORTS-->	This table contains all external reports that been added to the case.
<!--OSF_CASE_SYSINFO-->	This table contains all System Information reports that have been added to the case.
<!--OSF_CASE_RECENT-->	This table contains all Recent Activity scan results that have been added to the case.
<!--OSF_CASE_FILESEARCH-->	This table contains all File Name Search results that have been added to the case.
<!--OSF_CASE_DELETEDFILESEARCH-->	This table contains all Deleted File Search results that have been added to the case.
<!--OSF_CASE_INDEXSEARCH-->	This table contains all Index Search results that have been added to the case.
<!--OSF_CASE_MISMATCHSEARCH-->	This table contains all Mismatch Search results that have been added to the case.
<!--OSF_CASE_PREFETCH-->	This table contains all Prefetch Viewer lists that have been added to the case.
<!--OSF_CASE_PASSWORDS-->	This table contains all Password retrieval scan results that have been added to the case.
<!--OSF_CASE_FILESTABLE-->	This table contains all files added to the case.
<!--OSF_CASE_UNDELETETABLE-->	This table contains all deleted files added to the case.
<!--OSF_CASE_EMAILS-->	This table contains all e-mails that have been added to the case.
<!--OSF_CASE_WEBSNAPSHOTS-->	This table contains all web snapshots that have been added to the case.
<!--OSF_CASE_REGISTRY-->	This table contains all registry keys that have been added to the case.
<!--OSF_CASE_ESEDBRECORDS-->	This table contains all ESEDB database records that have been added to the case.
<!--OSF_CASE_SQLITERECORDS-->	This table contains all SQLite database records that have been added to the case.
<!--OSF_CASE_THUMBDBRECORDS-->	This table contains all Thumbnail Cache database records that have been added to the case.
<!--OSF_CASE_PROCSNAPSHOTS-->	This table contains all process snapshots that have been added to the case.
<!--OSF_CASE_MEMORYDUMP-->	This table contains all memory dumps that have been added to the case.

<!--OSF_CASE_STRINGLIST-->	This table contains all string lists extracted from the internal viewer that have been added to the case.
<!--OSF_CASE_PLISTRECORDS-->	This table contains all p-list properties and values that have been added to the case.
<!--OSF_CASE_NAVIGATION-->	This is where the navigation links to the different sections of the report shall be placed
<!--OSF_CASE_FOOTER-->	This is where the report footer shall be placed
<!--OSF_CASE_LOGO-->	This is where the company logo shall be placed
<!--OSF_CASE_LOGO_BANNER-->	This is where the banner logo shall be placed
<!--OSF_CASE_LOGO_COMPANY-->	This is where the small company logo shall be placed

Editing CSS (Cascading Style Sheets) Files

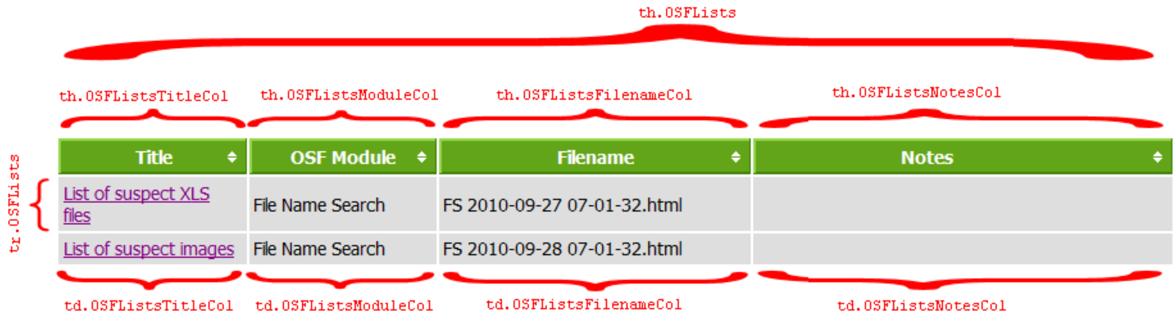
The fonts, colors and general appearance of the page, and in particular the tables in the report, are defined by CSS. If you are not familiar with CSS, you can take a look at the default templates supplied with OSForensics as reference (or simply make a copy of it, and modify it as you see fit).

Most of the CSS would be depending on the template file used and the markup of the HTML you place in the template.

However, the table for the items and the files are hard-coded but you can style them by their multiple class names.

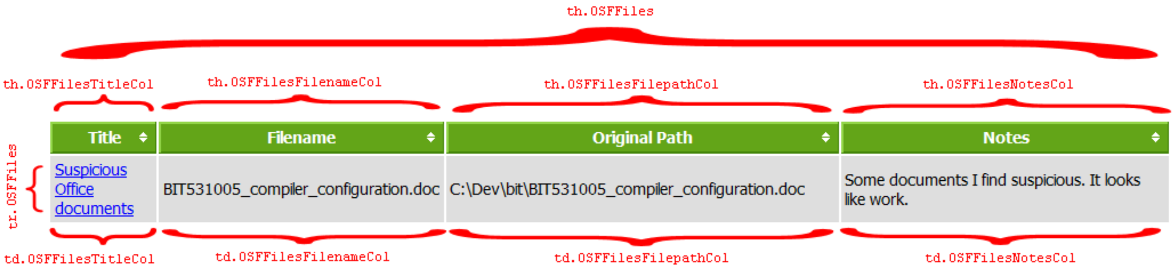
Below is a reference example of the report table with the corresponding CSS class names in red and the {} braces indicate the sections of the table that they span.

Lists table



Title	OSF Module	Filename	Notes
List of suspect XLS files	File Name Search	FS 2010-09-27 07-01-32.html	
List of suspect images	File Name Search	FS 2010-09-28 07-01-32.html	

Files table

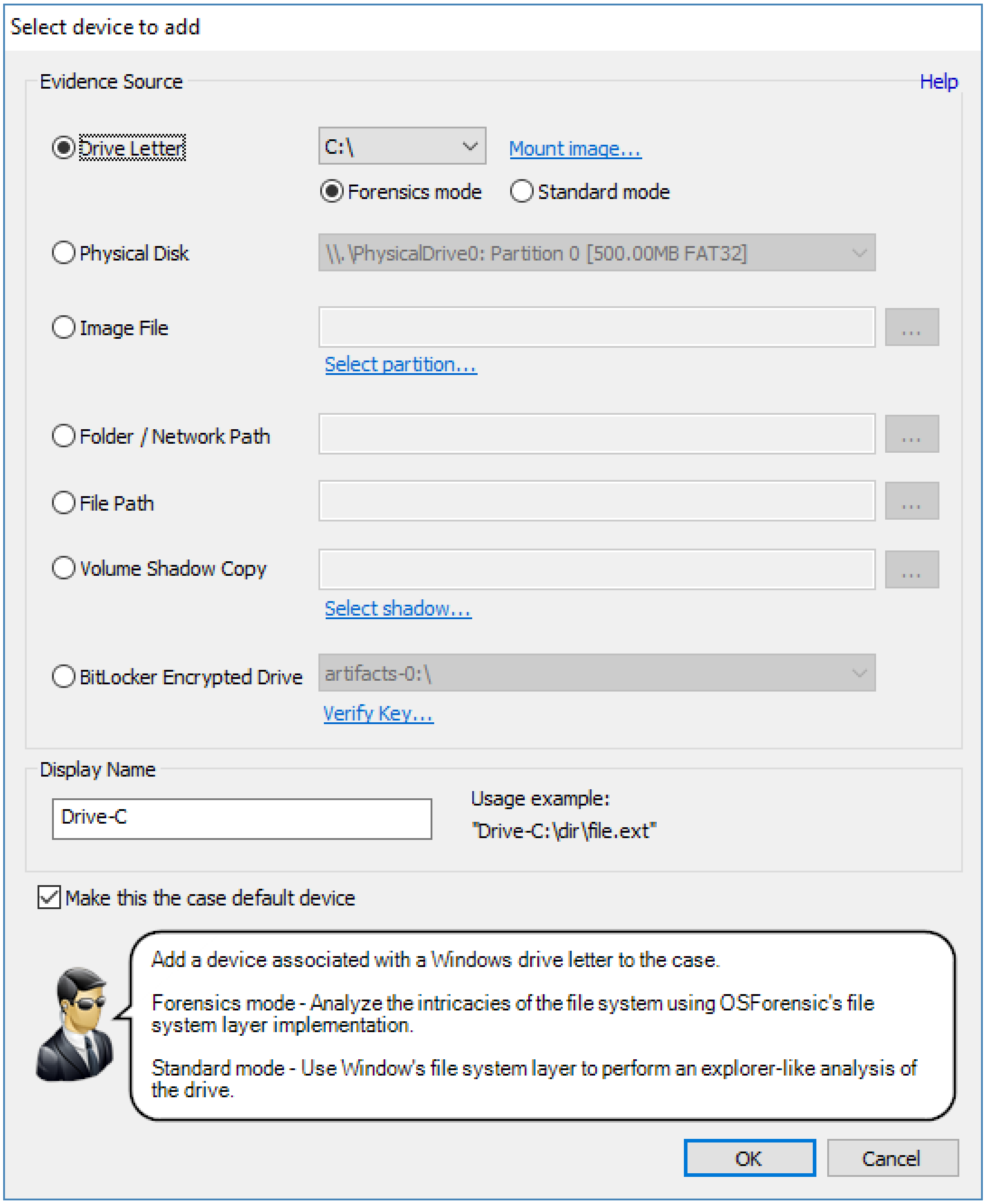


Title	Filename	Original Path	Notes
Suspicious Office documents	BIT531005_compiler_configuration.doc	C:\Dev\bit\BIT531005_compiler_configuration.doc	Some documents I find suspicious. It looks like work.

The other tables follow a similar naming convention.

4.1.2 Add Device

An investigator can specify storage devices to associate with a case. Once the device is added to the case, it can be accessed across all OSForensics functionality via a user-defined display name (similar to a drive letter in Windows).



Select device to add

Evidence Source

● Drive Letter: C:\ — Mount image...

● Forensics mode ○ Standard mode

○ Physical Disk: \\.\PhysicalDrive0: Partition 0 [500.00MB FAT32]

○ Image File — Select partition...

○ Folder / Network Path

○ File Path

○ Volume Shadow Copy — Select shadow...

○ BitLocker Encrypted Drive: artifacts-0:\ — Verify Key...

Display Name: Drive-C

Usage example: "Drive-C:\dir\file.ext"

☑ Make this the case default device

Add a device associated with a Windows drive letter to the case.

Forensics mode - Analyze the intricacies of the file system using OSForensic's file system layer implementation.

Standard mode - Use Window's file system layer to perform an explorer-like analysis of the drive.

Evidence Source

The user chooses from the following types of devices to add to the case.

Drive Letter

Add a device associated with a Windows drive letter to the case. The 'Mount Image' link opens OSFMount for mounting image files to a drive letter.

Forensics mode - The file system is accessed via OSForensic's own file system layer, bypassing normal Window file management mechanisms. This allows for deeper analysis of file system objects (eg. NTFS metafiles), bypassing permissions, and ability to see files not visible in Windows (eg. rootkit files). However, operations on the drive are slower.

Standard mode - The file system is accessed via Windows file system layer (ie. explorer-like access to files). This mode is quicker but does not have the same depth of access as in Forensics mode.

Physical Disk
Add a physical disk partition attached to the system containing a valid file system to the case. This allows access to partitions that are normally inaccessible in Windows such as hidden, unnamed or unsupported (Linux/Mac) partitions. Physical disk partitions are accessed in Forensics mode since they are not normally accessible in Windows.

Image File
Add an image file containing a valid file system to the case. The image file can contain a single volume or multiple partitions under a supported partition scheme. Only a single partition can be added as a device at one time via 'Select Partition'. Image files are accessed in Forensics mode since they are not normally accessible in Windows. *See Supported Image Formats for a list of image file formats that are supported.*

Folder / Network Path
Add a folder or network path to the case. Folder/network paths are accessed in Standard mode (ie. Windows file system layer) since the physical medium of such paths are not accessible.

File Path
Add a single file path to the case. File paths are accessed in Standard mode (ie. Windows file system layer) since the physical medium of such paths are not accessible.

Volume Shadow Copy
Add a Volume Shadow Copy for a supported NTFS volume. Shadow copies are backup copies of data on a specific volume at a specific point in time. Shadow Copies are accessed in Forensic mode since they are not normally accessible in Windows. See Support for Volume Shadow Copy for more information.

BitLocker Encrypted Drive
Add an existing Case Device that is BitLocker encrypted to access the drive in decrypted, raw form. See Support for BitLocker Encrypted Drives for more information.

Display Name
The user specifies a unique display name to assign to the device. The name must be 2-32 characters long, and must not contain any special characters. Once the device has successfully been added, its display name can be used to reference the device using the following syntax:

<display_name>:

Eg. dell-pc-vista:

Make this the case default device
When checked, the mounted device is set to the case's default device when successfully mounted.

4.1.2.1 Supported Image Formats

The following is a list of image formats supported by OSForensics when adding an image file to a case:

- Raw Image (.IMG, .DD)
- Raw CD Image (.ISO, .BIN)

- Split Raw Image (.00n)
- Advanced Forensics Format* (.AFF, .AFD, .AFM)
- VMWare Image (.VMDK)
- EnCase Image (.E01, .Ex01)
- EnCase Logical Image (.L01, .Lx01)
- SMART Image (.S01)
- VHD Image (.VHD)

*The supported version of Advanced Forensics Format is AFFv3 with zlib compression support. Encryption and signatures are not supported.

4.1.2.2 Supported File Systems

The following is a list of file systems supported by OSForensics when adding a device to the case in Forensics mode:

- NTFS (Windows) *
- FAT16/FAT32 (DOS/Windows)
- exFAT (Windows)
- Ext2/Ext3/Ext4 (Linux/Android)**
- HFS+/HFSX (Mac/iPhone/iPad)

* NTFS Compression is supported. Windows 10 'CompactOS' (ie. 'System Compression') is supported for the XPRESS compression format. LZX compression is not yet supported.

**In some of the more popular Linux distributions (eg. Fedora, Gentoo, Ubuntu), the Logical Volume Manager (LVM) manages the volumes in the system. This allows for a single, continuous volume to be backed by one or more physical disk partitions for ease of management. However, when the physical disks are imaged, the partitions appear as an 'LVM partitions' containing metadata regarding how the partitions are arranged into the single volume. OSForensics is unable to rearrange the partitions back into the single volume. To resolve this issue, an image of the volume must be created under Linux so that the operating system handles the complexity of the LVM layer. This resulting image can then be added to the case as it appears to OSForensics as a standard Linux volume.

4.1.2.3 Supported Partitioning Schemes

The following is a list of partitioning schemes supported by OSForensics when adding a device to the case:

- Master Boot Record (MBR)
- GUID Partition Table (GPT)
- Apple Partition Map (APM)

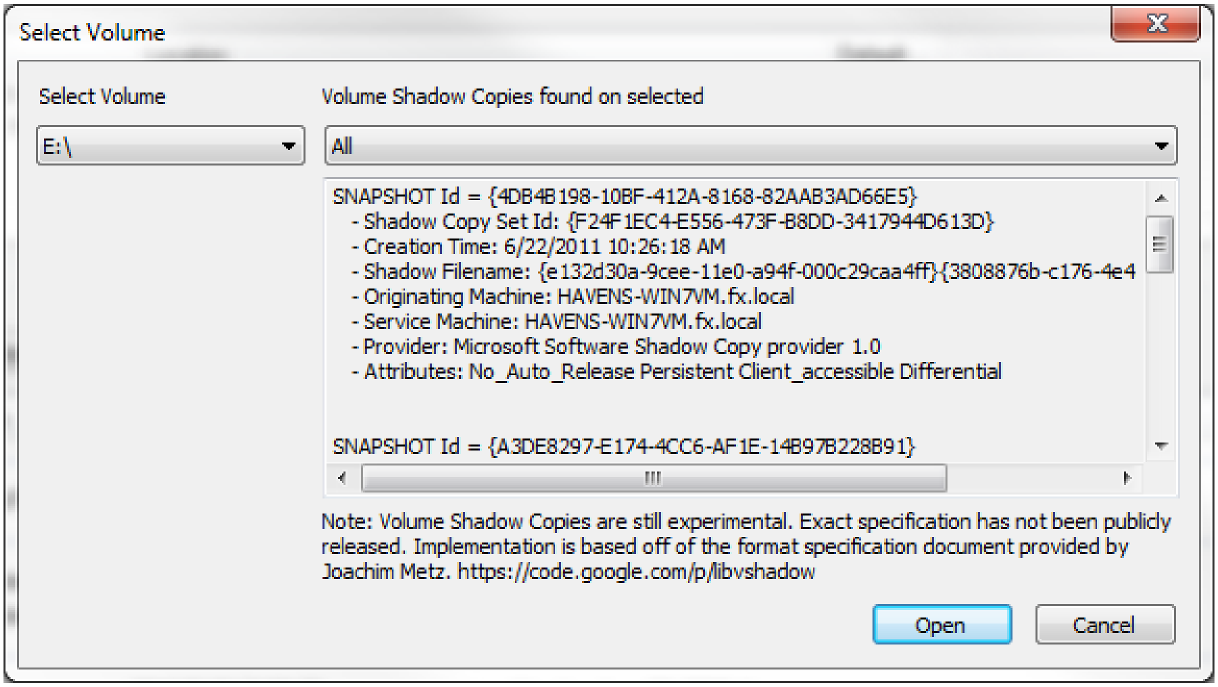
4.1.2.4 Support for Volume Shadow Copy

Background

The Volume Shadow Copy Service is a backup technology from Microsoft used in Windows XP and later operating systems. It is a mechanism for creating consistent point in time copies of data know as shadow copies. Shadow copy technology requires the file system to be NTFS. Shadow copies are stored on the volume and can be used to reconstruct the volume to a previous point in time.

Usage

Shadow Copies can be added to the case and used in various OSForensics modules. Shadow copies are loaded on first use. The time to load a shadow copy is dependent on the number of shadow copies existing on the volume and the size of the copies themselves. This means for larger drives, the time to load can be quite substantial. Shadow copies changes are stacked, in the sense to access the oldest shadow copy, the more recent shadow copies must first be applied to the volume. To decrease the time needed to access shadow copies, OSForensics can cache up to 10 volume's set of shadow data in memory (i.e. if drive E:\ has 4 shadow copies, the entire set will count as one toward the 10 limit).



Select Volume

Select Volume: E:\

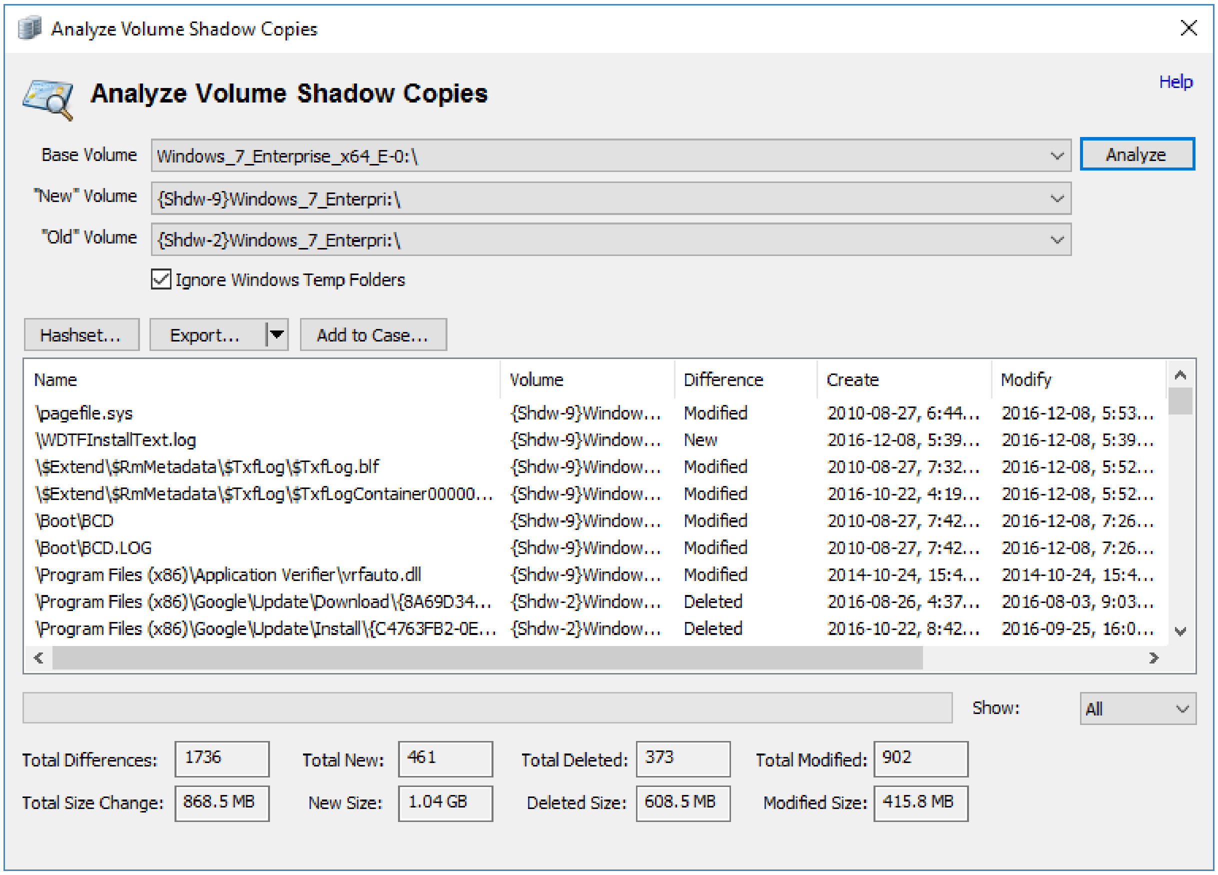
Volume Shadow Copies found on selected: All

```
SNAPSHOT Id = {4DB4B198-10BF-412A-8168-82AAB3AD66E5}
   - Shadow Copy Set Id: {F24F1EC4-E556-473F-B8DD-3417944D613D}
   - Creation Time: 6/22/2011 10:26:18 AM
   - Shadow Filename: {e132d30a-9cee-11e0-a94f-000c29caa4ff}{3808876b-c176-4e4
   - Originating Machine: HAVENS-WIN7VM.fx.local
   - Service Machine: HAVENS-WIN7VM.fx.local
   - Provider: Microsoft Software Shadow Copy provider 1.0
   - Attributes: No_Auto_Release Persistent Client_accessible Differential


SNAPSHOT Id = {A3DE8297-E174-4CC6-AF1E-14B97B228B91}
```

Note: Volume Shadow Copies are still experimental. Exact specification has not been publicly released. Implementation is based off of the format specification document provided by Joachim Metz. https://code.google.com/p/libvshadow

Analyze Volume Shadow Copies

OSForensics provides a tool to find changes in files and directories between two shadow copies of a single volume. By comparing the signature between two shadow copies, files that have been created, deleted or modified can be determined within the period of when the snapshots were taken.



Base Volume: Windows_7_Enterprise_x64_E-0:\

"New" Volume: {Shdw-9}Windows_7_Enterpri:\

"Old" Volume: {Shdw-2}Windows_7_Enterpri:\

☑ Ignore Windows Temp Folders

Name	Volume	Difference	Create	Modify
\pagefile.sys	{Shdw-9}Window...	Modified	2010-08-27, 6:44...	2016-12-08, 5:53...
\WDTFInstallText.log	{Shdw-9}Window...	New	2016-12-08, 5:39...	2016-12-08, 5:39...
\$Extend\$RmMetadata\$TxfLog\$TxfLog.blf	{Shdw-9}Window...	Modified	2010-08-27, 7:32...	2016-12-08, 5:52...
\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000...	{Shdw-9}Window...	Modified	2016-10-22, 4:19...	2016-12-08, 5:52...
\Boot\BCD	{Shdw-9}Window...	Modified	2010-08-27, 7:42...	2016-12-08, 7:26...
\Boot\BCD.LOG	{Shdw-9}Window...	Modified	2010-08-27, 7:42...	2016-12-08, 7:26...
\Program Files (x86)\Application Verifier\vrfauto.dll	{Shdw-9}Window...	Modified	2014-10-24, 15:4...	2014-10-24, 15:4...
\Program Files (x86)\Google\Update\Download\{8A69D34...	{Shdw-2}Window...	Deleted	2016-08-26, 4:37...	2016-08-03, 9:03...
\Program Files (x86)\Google\Update\Install\{C4763FB2-0E...	{Shdw-2}Window...	Deleted	2016-10-22, 8:42...	2016-09-25, 16:0...

Show: All

Total Differences:	1736	Total New:	461	Total Deleted:	373	Total Modified:	902
Total Size Change:	868.5 MB	New Size:	1.04 GB	Deleted Size:	608.5 MB	Modified Size:	415.8 MB

Hashset
Create a hashset that includes all files in the comparison result.

Export
Export the comparison results to a text, CSV or HTML file

Add to Case
Add the comparison results to case as an CSV or HTML file

File System Browser

The File System Browser can display multiple shadow copy versions of a file alongside the most current version. See Shadow Copies for details on its usage.

Implementation & Limitation

The specification of the Volume Shadow Copy has not been publicly released by Microsoft. Implementation for Volume shadow copies is based on the work of Joachim Metz's document Volume Shadow Snapshot (VSS)[1].

[1] libvshadow - Library and tools to support the Volume Shadow Snapshot (VSS) format. Version 0.0.10. Obtained on March 6, 2013

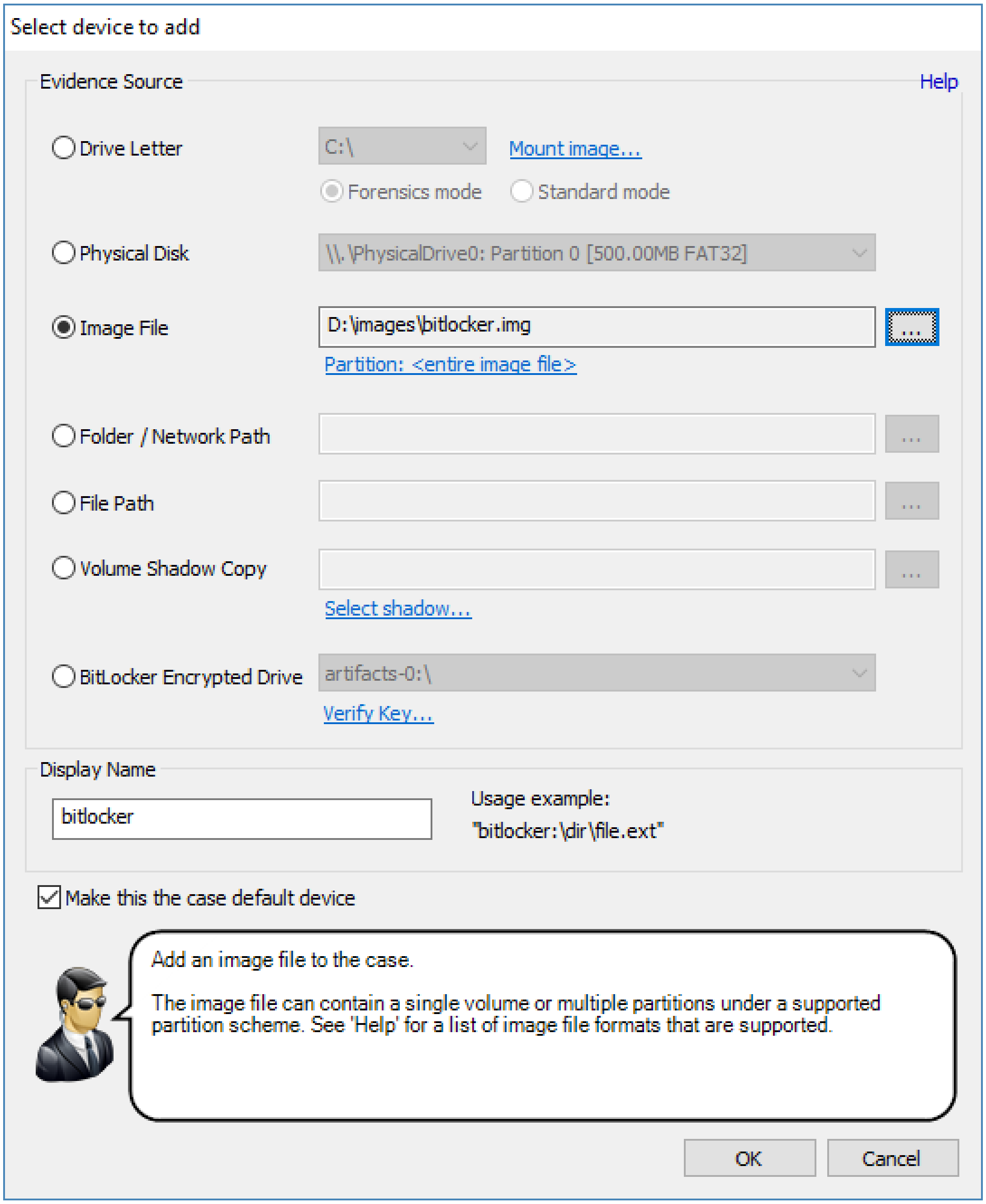
4.1.2.5 Support for BitLocker Encrypted Drives

OSForensics is capable of accessing images or drives that are encrypted using BitLocker, provided that a valid key is specified. The following key protectors are supported:

- Password
- Recovery Key *(eg. 531135-570372-522236-480007-142241-640487-244519-333049)*
- Startup Key File *(.bek file)*

Usage

To add a BitLocker encrypted drive to the case, the image file or disk must first be added in his encrypted form. For example, an Encase image file of a BitLocker encrypted drive, *bitlocker.e01*, is first added to the case.



Select device to add

Evidence Source

○ Drive Letter — C:\ — Mount image...

● Forensics mode ○ Standard mode

○ Physical Disk — \\.\PhysicalDrive0: Partition 0 [500.00MB FAT32]

● Image File — D:\images\bitlocker.img

Partition: <entire image file>

○ Folder / Network Path

○ File Path

○ Volume Shadow Copy

Select shadow...

○ BitLocker Encrypted Drive — artifacts-0:\

Verify Key...

Display Name: bitlocker

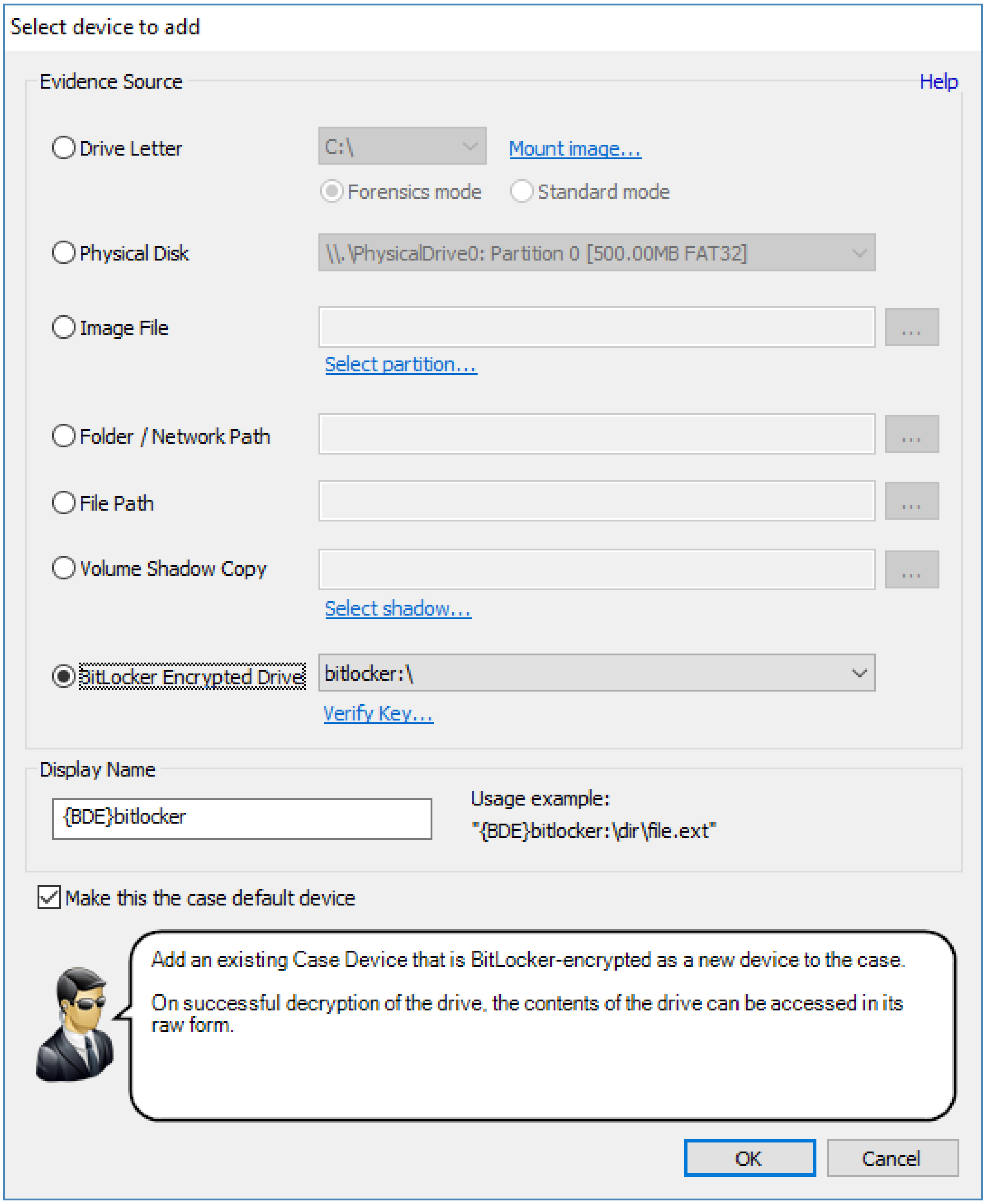
Usage example:
"bitlocker:\dir\file.ext"

☑ Make this the case default device

Add an image file to the case.

The image file can contain a single volume or multiple partitions under a supported partition scheme. See 'Help' for a list of image file formats that are supported.

Because the image file is encrypted, performing forensic analysis on this device is not very useful. To access the drive in decrypted form, a "BitLocker Drive" device must be added to the case on top of the image file device. Open the Add Device dialog and select 'BitLocker Encrypted Drive'. Select the previously added image file device from the drop down list.



Select device to add

Evidence Source

○ Drive Letter C:\

● Forensics mode ○ Standard mode

○ Physical Disk \\.\PhysicalDrive0: Partition 0 [500.00MB FAT32]

○ Image File

○ Folder / Network Path

○ File Path

○ Volume Shadow Copy

● BitLocker Encrypted Drive bitlocker:\

Display Name

{BDE}bitlocker

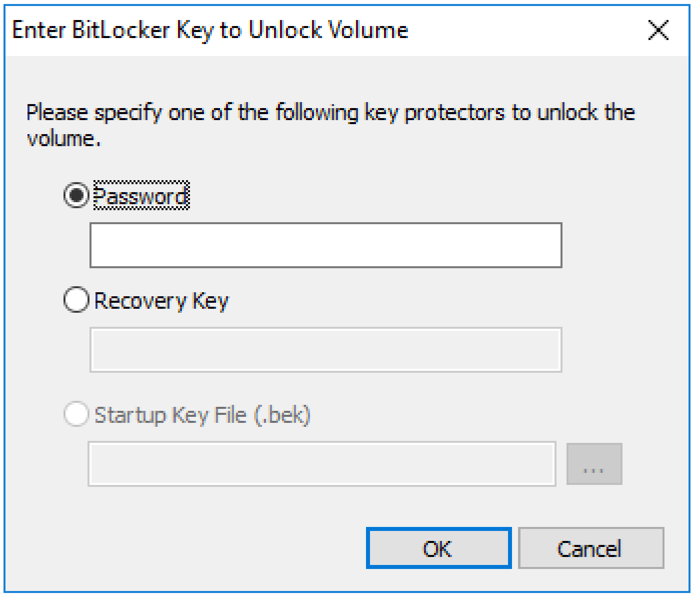
Usage example:
"{BDE}bitlocker:\dir\file.ext"

☑ Make this the case default device

Add an existing Case Device that is BitLocker-encrypted as a new device to the case.

On successful decryption of the drive, the contents of the drive can be accessed in its raw form.

To verify whether the drive can be decrypted, click on 'Verify Key...' to specify the key needed to unlock the drive. Select one of the key protectors to use and enter the corresponding key for the drive. Unsupported key protectors are disabled.



Enter BitLocker Key to Unlock Volume

Please specify one of the following key protectors to unlock the volume.

● Password

○ Recovery Key

○ Startup Key File (.bek)

Upon successful key verification, click OK in the Add Device dialog to add the device to case. After entering the key one more time, the device should be accessible via any OSForensics module in decrypted form.

4.1.3 Case Activity Log

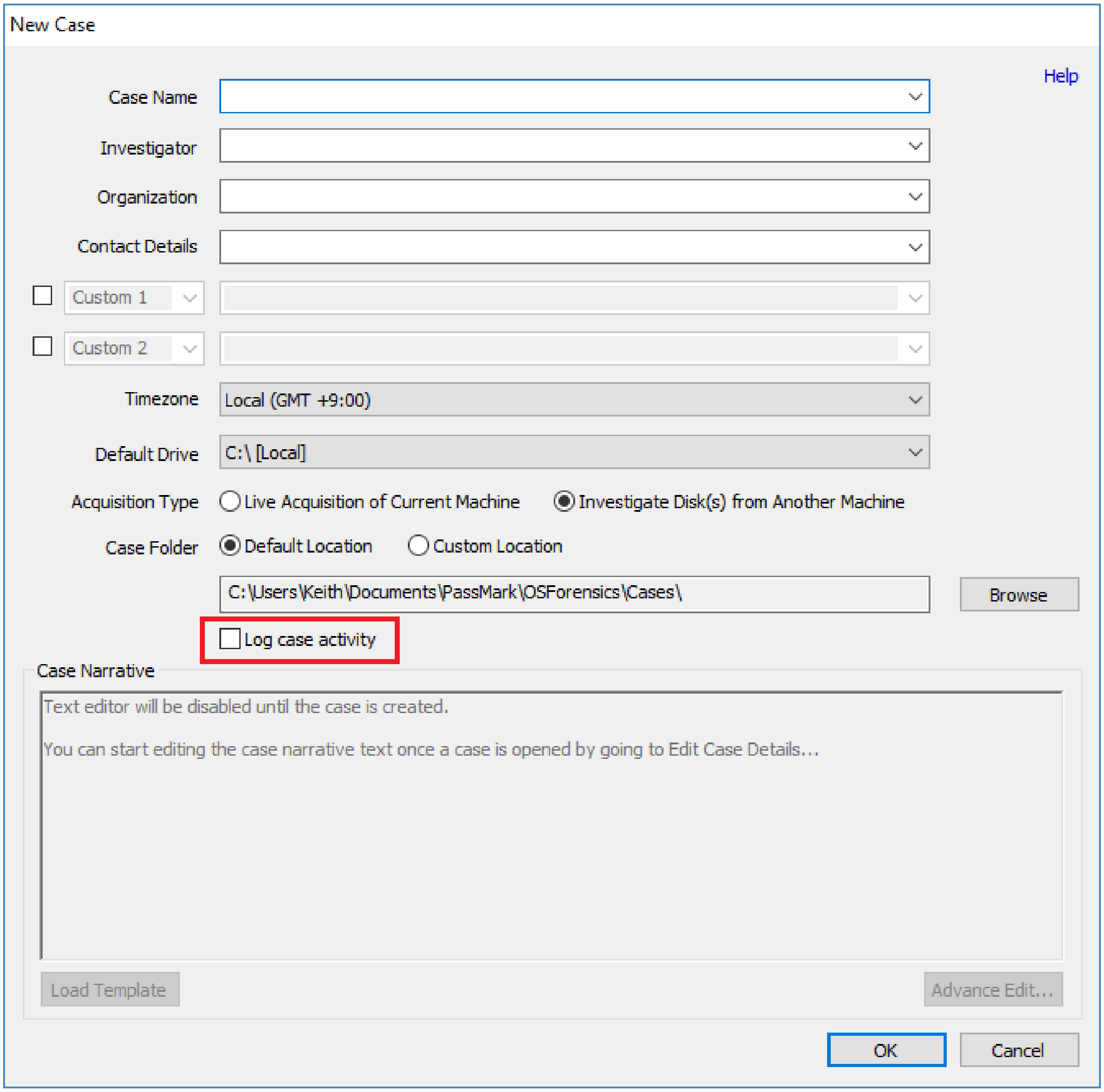
When performing forensic investigations, it is important to maintain an audit trail of the exact activities carried out during the course of the investigation for several purposes including the following:

- Debriefing of a completed investigation
- Auditing the activities of an investigation to determine whether proper procedures and protocols were followed
- Educating and evaluating of investigators in training

OSForensics provides the option to specify whether activities performed in the case should be automatically logged to a tamper-resistant log file on disk, producing a trace of all actions performed during the investigation.

Enable/Disable Logging

Logging can be enabled/disabled when creating a case for the first time or when editing an existing case in the Case Management window



New Case

Case Name

Investigator

Organization

Contact Details

□ Custom 1

□ Custom 2

Timezone: Local (GMT +9:00)

Default Drive: C:\ [Local]

Acquisition Type: ○ Live Acquisition of Current Machine ● Investigate Disk(s) from Another Machine

Case Folder: ● Default Location ○ Custom Location

C:\Users\Keith\Documents\PassMark\OSForensics\Cases\

□ Log case activity

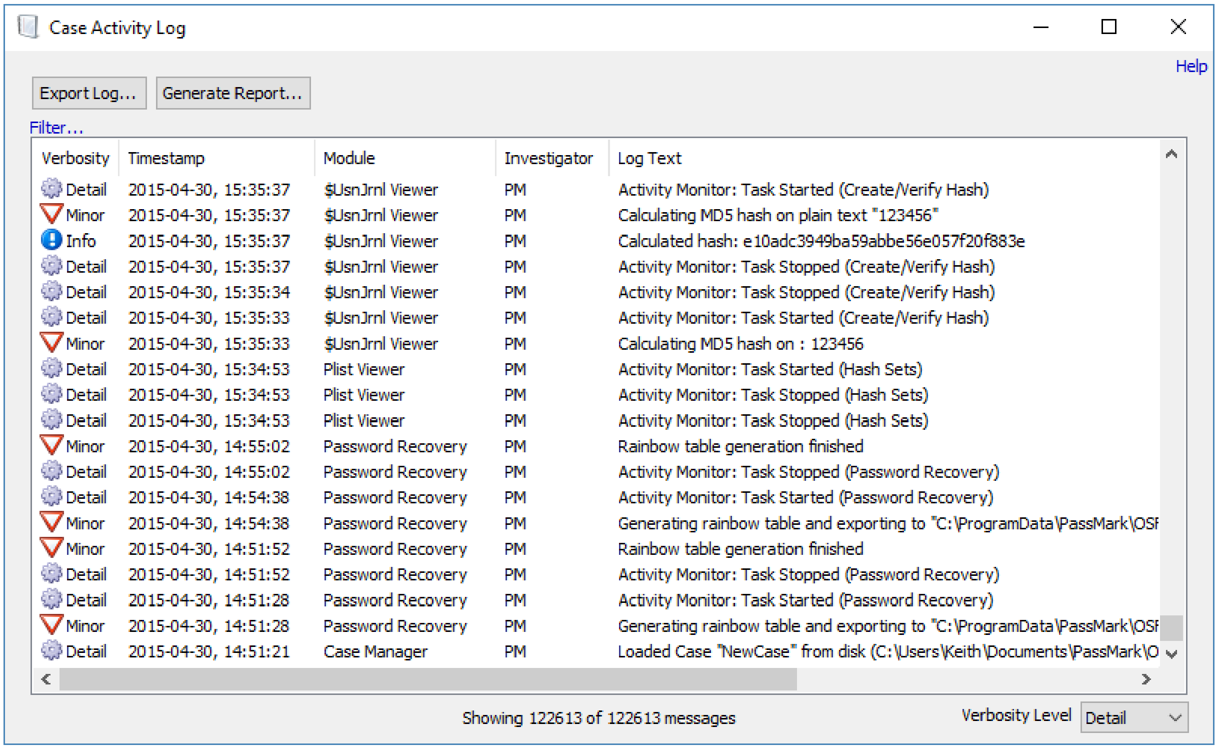
Case Narrative

Text editor will be disabled until the case is created.

You can start editing the case narrative text once a case is opened by going to Edit Case Details...

Viewing the Log

Once logging is enabled, the log can be viewed by clicking the "View Log" button in the Case Management window, as well as the "View Log" icon in the "Case Management" group under the Start tab.



Verbosity	Timestamp	Module	Investigator	Log Text
Detail	2015-04-30, 15:35:37	$UsnJrnl Viewer	PM	Activity Monitor: Task Started (Create/Verify Hash)
Minor	2015-04-30, 15:35:37	$UsnJrnl Viewer	PM	Calculating MD5 hash on plain text "123456"
Info	2015-04-30, 15:35:37	$UsnJrnl Viewer	PM	Calculated hash: e10adc3949ba59abbe56e057f20f883e
Detail	2015-04-30, 15:35:37	$UsnJrnl Viewer	PM	Activity Monitor: Task Stopped (Create/Verify Hash)
Detail	2015-04-30, 15:35:34	$UsnJrnl Viewer	PM	Activity Monitor: Task Stopped (Create/Verify Hash)
Detail	2015-04-30, 15:35:33	$UsnJrnl Viewer	PM	Activity Monitor: Task Started (Create/Verify Hash)
Minor	2015-04-30, 15:35:33	$UsnJrnl Viewer	PM	Calculating MD5 hash on : 123456
Detail	2015-04-30, 15:34:53	Plist Viewer	PM	Activity Monitor: Task Started (Hash Sets)
Detail	2015-04-30, 15:34:53	Plist Viewer	PM	Activity Monitor: Task Stopped (Hash Sets)
Detail	2015-04-30, 15:34:53	Plist Viewer	PM	Activity Monitor: Task Stopped (Hash Sets)
Minor	2015-04-30, 14:55:02	Password Recovery	PM	Rainbow table generation finished
Detail	2015-04-30, 14:55:02	Password Recovery	PM	Activity Monitor: Task Stopped (Password Recovery)
Detail	2015-04-30, 14:54:38	Password Recovery	PM	Activity Monitor: Task Started (Password Recovery)
Minor	2015-04-30, 14:54:38	Password Recovery	PM	Generating rainbow table and exporting to "C:\ProgramData\PassMark\OSF
Minor	2015-04-30, 14:51:52	Password Recovery	PM	Rainbow table generation finished
Detail	2015-04-30, 14:51:52	Password Recovery	PM	Activity Monitor: Task Stopped (Password Recovery)
Detail	2015-04-30, 14:51:28	Password Recovery	PM	Activity Monitor: Task Started (Password Recovery)
Minor	2015-04-30, 14:51:28	Password Recovery	PM	Generating rainbow table and exporting to "C:\ProgramData\PassMark\OSF
Detail	2015-04-30, 14:51:21	Case Manager	PM	Loaded Case "NewCase" from disk (C:\Users\Keith\Documents\PassMark\O

Showing 122613 of 122613 messages

Verbosity Level: Detail

The log window displays a list of log entries ordered chronologically. The verbosity of the displayed log entries can be changed by selecting one of the following verbosity levels, from lowest to highest:

- **Major** - *Includes all major activity related to the case itself, such as when it is first created.*
- **Minor** - *Includes start/completion of all significant forensics activity, such as file name searching, index creation, deleted file searching, etc.*
- **Info** - *Includes all supplemental forensics activity performed, such as exporting results to disk, adding files to case, etc.*
- **Detail** - *Includes details of the subtasks that are being executed internally while major forensics operations are being performed.*

Selecting a verbosity level will include all log entries marked with the specified verbosity level and lower. For example, selecting 'Minor' will include all log entries that are marked as 'Major' or 'Minor'.

Filter...
Clicking on the "Filter" link allows the investigator to filter the log entries by module.

Export Log...
Export the log to a text or CSV file

Generate Report...
Generate an HTML or PDF report of the log

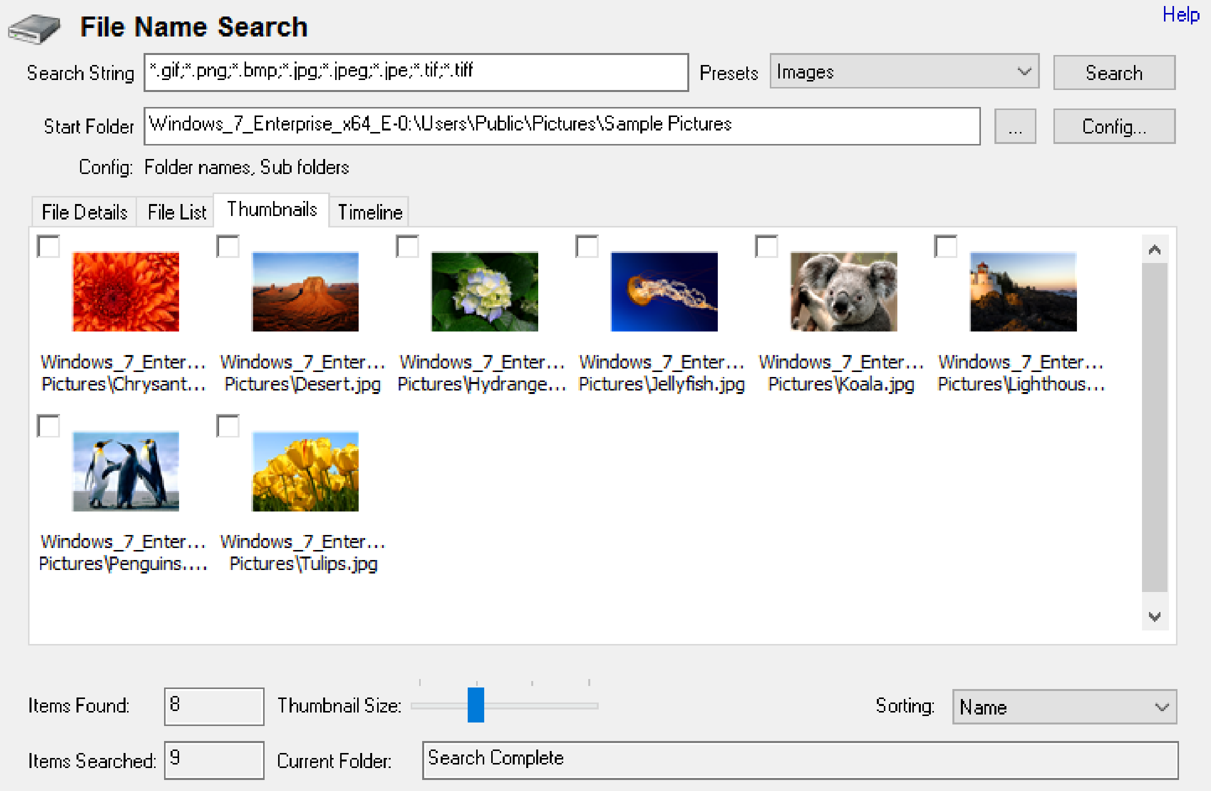
Tamper-resistant Log File

To maintain the integrity of a case's recorded history, the log file has built-in security mechanisms for verifying whether or not it has been tampered with. The log file itself is stored in an encrypted format and can only be viewed when the case is opened within OSForensics; it cannot be viewed as-is using a text viewer like Notepad or when another case is opened in OSForensics. In order to prevent log entries from being inserted, removed, or re-ordered, each log entry is encrypted using a key linked to previous log entries. This key is destroyed immediately after the log entry is written. In addition, several layers of integrity checks (ie. hash chains) are computed for each log entry that serves to verify the integrity of all previous log entries.

Note: The security mechanisms in place cannot prevent a user from corrupting or deleting the log file; it can only detect whether or not the contents of the log file have been compromised. Once the log file has been tampered with, the contents may or may not be recoverable. That is why it is always a good idea to make periodic backups of your case files.

4.2 File Name Search

The File Name Search Module can be used to search for names of files and folders that match the specified search pattern.



File Name Search

Search String: *.gif;*.png;*.bmp;*.jpg;*.jpeg;*.jpe;*.tif;*.tiff

Presets: Images

Start Folder: Windows_7_Enterprise_x64_E-0:\Users\Public\Pictures\Sample Pictures

Config: Folder names, Sub folders

Items Found: 8

Items Searched: 9

Sorting: Name

Current Folder: Search Complete

Help
Search
...
Config...
File Details
File List
Thumbnails
Timeline
Windows_7_Enter... Pictures\Chrysant...
Windows_7_Enter... Pictures\Desert.jpg
Windows_7_Enter... Pictures\Hydrange...
Windows_7_Enter... Pictures\Jellyfish.jpg
Windows_7_Enter... Pictures\Koala.jpg
Windows_7_Enter... Pictures\Lighthous...
Windows_7_Enter... Pictures\Penguins....
Windows_7_Enter... Pictures\Tulips.jpg
Thumbnail Size:

Basic Usage

A basic search simply involves entering a search string and location. Any files or folders that contain the search string within their name will be displayed in the search results. For instance, searching for "File" will match "file.txt", "test.file" or "MyFile.doc". The basic search is case insensitive.

Presets

You can select one of the preset search options to quickly locate files of certain file type (eg. image files or office documents). These presets can be customized by altering the FileNameSearchPresets.txt file in the OSForensics program data folder (generally C:\ProgramData\PassMark\OSForensics). Each entry requires 3 lines in this file, a name, a search string and a line representing the configuration options that can be set. This file needs to be opened and saved in Unicode format.

Multiple Searches
To run multiple different searches at once by separating the terms with the ';' character.

Wildcards
You can use '*' or '?' as wildcards within the search string.

'*' represents any number of characters
'?' represents a single character

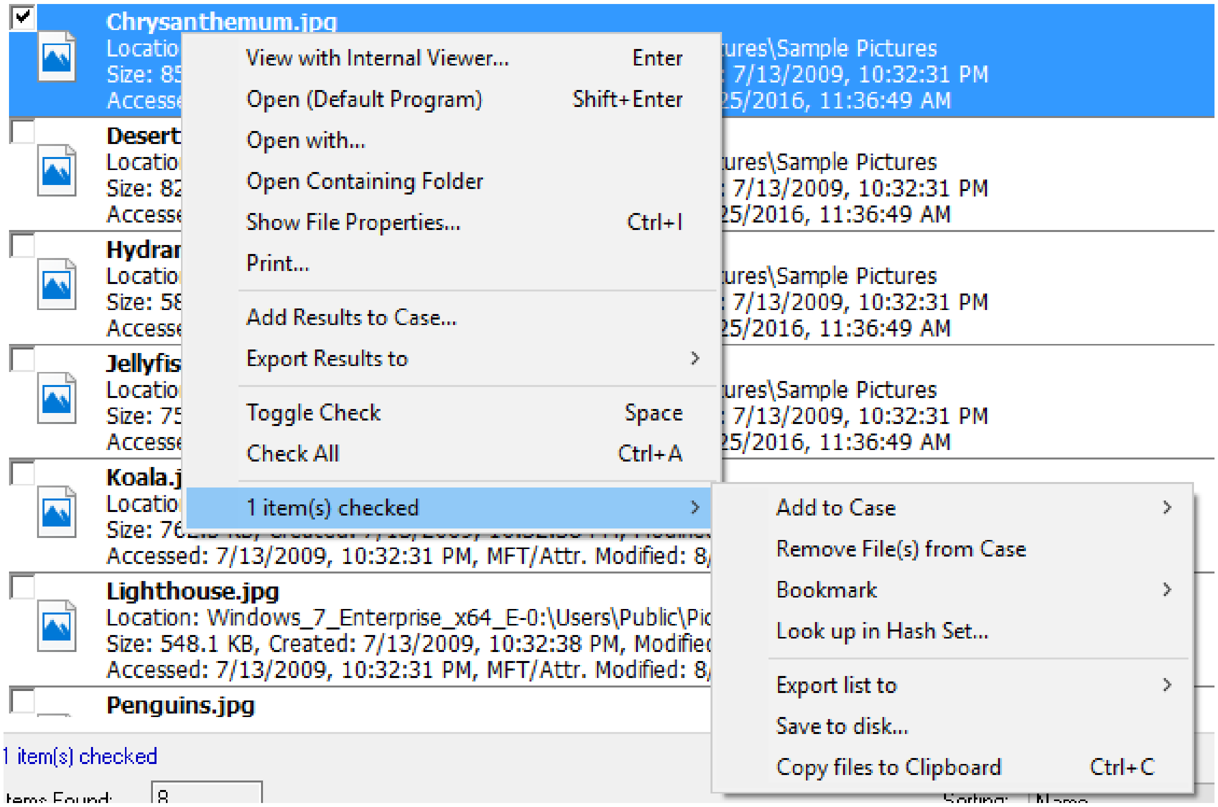
If a wildcard is entered anywhere in the search field, wildcard matching is enabled on all search terms. When wildcard matching is enabled, you will need to explicitly add '*' to the start and end of the search term if you are trying match a word that may appear in the middle of a filename.

More Advanced Options

By clicking the "Config..." button you will be taken to the File Name Search Configuration window where more advanced options can be selected.

Results

The results of the search are displayed in one of several views, along with a summary of the number of items searched/found. Right-clicking a file opens the following context menu.



View with Interval Viewer
Opens the file with OSForensics Viewer to perform a more thorough analysis

Open (Default Program)
Open the file with the default program

Open With...
Allows the user to select the program to open the file

Open Containing Folder
Opens the folder than contains the file

Show File Properties
Opens the file with OSForensics Viewer in File Info mode.

Print...
Print the file (if applicable)

Add Results to Case...
Add the list of results as an HTML or CSV file to case

Export Results to
Export the list of results to a TXT, CSV or HTML file

Toggle Check
Toggle the check state of the selected item.

Check All
Check all the items in the list.

n Item(s) checked

> **Add to Case**
> Add the checked file(s) or list of checked file(s) to the case
>
> **Remove File(s) from Case**
> Remove the checked file(s) from the case
>
> **Bookmark**
>
> > **Green**
> > Add/remove selected path from the list of Green bookmarks. *Keyboard shortcut: Ctrl+G*
> >
> > **Yellow**
> > Add/remove selected path from the list of Yellow bookmarks. *Keyboard shortcut: Ctrl+Y*
> >
> > **Red**
> > Add/remove selected path from the list of Red bookmarks. *Keyboard shortcut: Ctrl+R*
>
> **Look up in Hash Set**
> Verify whether the checked file(s) are contained in a hash set in the active database. See Hash Set Lookup.
>
> **Export list to**
> Export the list of checked file(s) to a TXT, CSV or HTML file

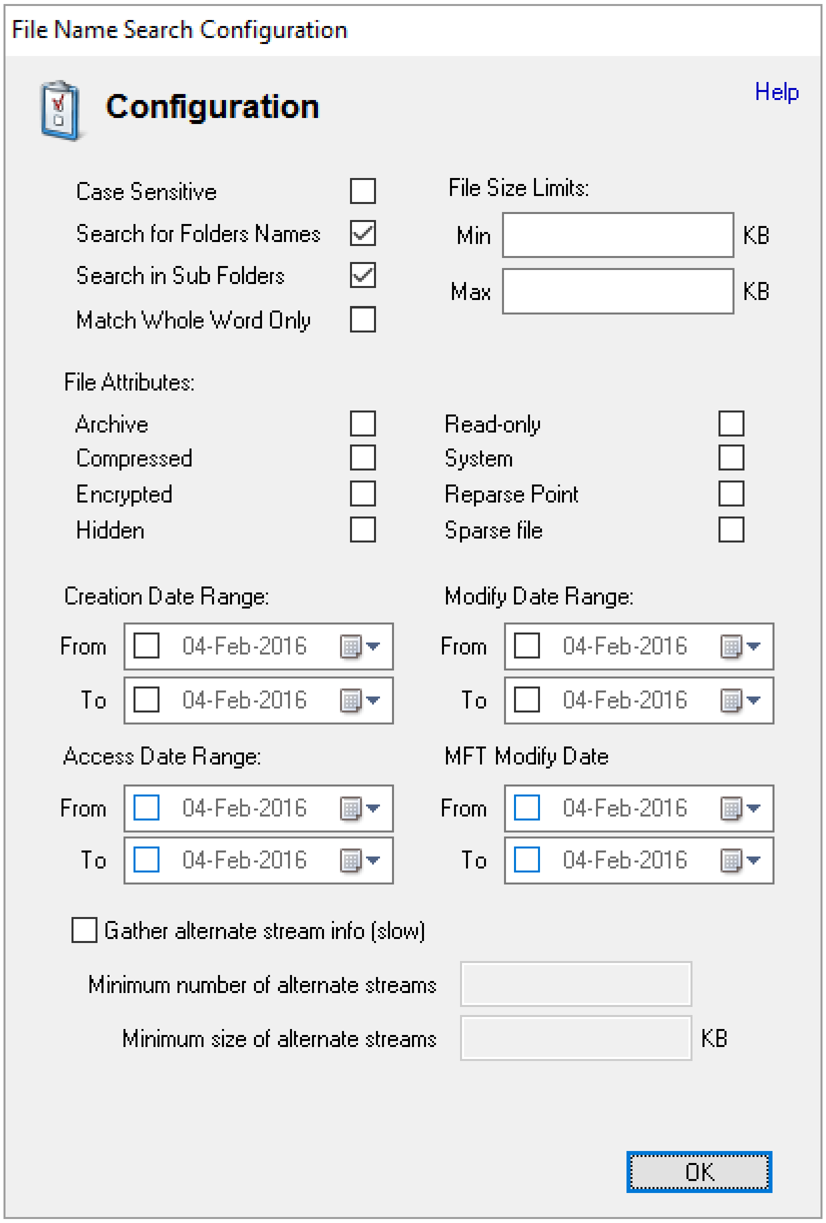
Save to disk...
Save the checked file(s) to a location on disk.

Copy File(s) to Clipboard
Copy the checked file(s) to clipboard. Once copied to the clipboard, the file(s) can be pasted to any other application that supports it (eg. Windows Explorer).

Note: In some cases, copy and pasting files to an explorer window may fail without an error message when "preparing to copy". This may happen if the file has already been deleted (eg a temp file) or if Windows Explorer does not have permissions to access the files (eg restricted system files and folders). In these cases, it is better to use the "Add to case" function.

4.2.1 File Name Search Configuration

The File Name Search Configuration Window allows for setting advanced options for the File Name Search. This window can be accessed by clicking on the "Config..." button in the main File Name Search window.



File Name Search Configuration

Configuration

Help

Case Sensitive □
Search for Folders Names ☑
Search in Sub Folders ☑
Match Whole Word Only □

File Size Limits:
Min ____ KB
Max ____ KB

File Attributes:

Archive	□	Read-only	□
Compressed	□	System	□
Encrypted	□	Reparse Point	□
Hidden	□	Sparse file	□

Creation Date Range:		Modify Date Range:	
From	□ 04-Feb-2016	From	□ 04-Feb-2016
To	□ 04-Feb-2016	To	□ 04-Feb-2016
Access Date Range:		**MFT Modify Date**	
From	□ 04-Feb-2016	From	□ 04-Feb-2016
To	□ 04-Feb-2016	To	□ 04-Feb-2016

□ Gather alternate stream info (slow)

Minimum number of alternate streams ____

Minimum size of alternate streams ____ KB

Case Sensitive

If checked, searches will be case sensitive. This option is disabled by default.

Search for Folder Names

If checked, folder names will also be included in searches, not just filenames. This option is enabled by default.

Search in Sub Folders

If checked, sub folders will also be included in searches, not just the files in the start directory. This option is enabled by default

Match Whole Word Only

If checked, results only include whether the search string is matched as a discreet word in the file name. In addition to spaces, the following characters are used as breaking characters around a word "_-.()[] ". For instance, searching for "Test" with this option enabled would return files like "_Test.txt", "A(Test).jpg", "This is a Test.docx" and "file.test". But it would not return "testing.txt", "testimony.pdf" or "contest.zip".

This option is disabled by default. This option has no effect on wildcard searches.

File Size Limits
Allows the user to specify file size limits for search results. The user may enter either a minimum, maximum, both or neither. The only restriction is that the maximum must be larger than the minimum.

File Attributes
Filters the search results based on the file system attributes that are checked.

Archive
A file or directory that is an archive file or directory, which is typically marked for the purpose of backup or removal.

Compressed
For a file, the data is compressed. For a directory, newly created files and subdirectories shall also be compressed.

Encrypted
For a file, the data is encrypted. For a directory, newly created files and subdirectories shall also be encrypted.

Hidden
A file or directory that is hidden, and are typically not shown in a directory listing.

Read-only
A file that cannot be written on or deleted. This attribute does not have any meaning for directories.

System
A file or directory that is used by the operating system.

Reparse Point
A file or directory that has a reparse point, which is typically used as a symbolic link.

Sparse file
A file that is a sparse file (eg. data is mostly zeros)

Creation Date Range
Allows the user to specify the creation date range for the search results.

Modify Date Range
Allows the user to specify the modify date range for the search results.

Access Date Range
Allows the user to specify the access date range for the search results.

MFT Modify Date Range
Allows the user to specify the MFT modify date range for the search results (if applicable).

Gather alternate stream info
Selecting this option will gather information about alternate NTFS data streams within a file. Turning this on will slow down the search slightly.

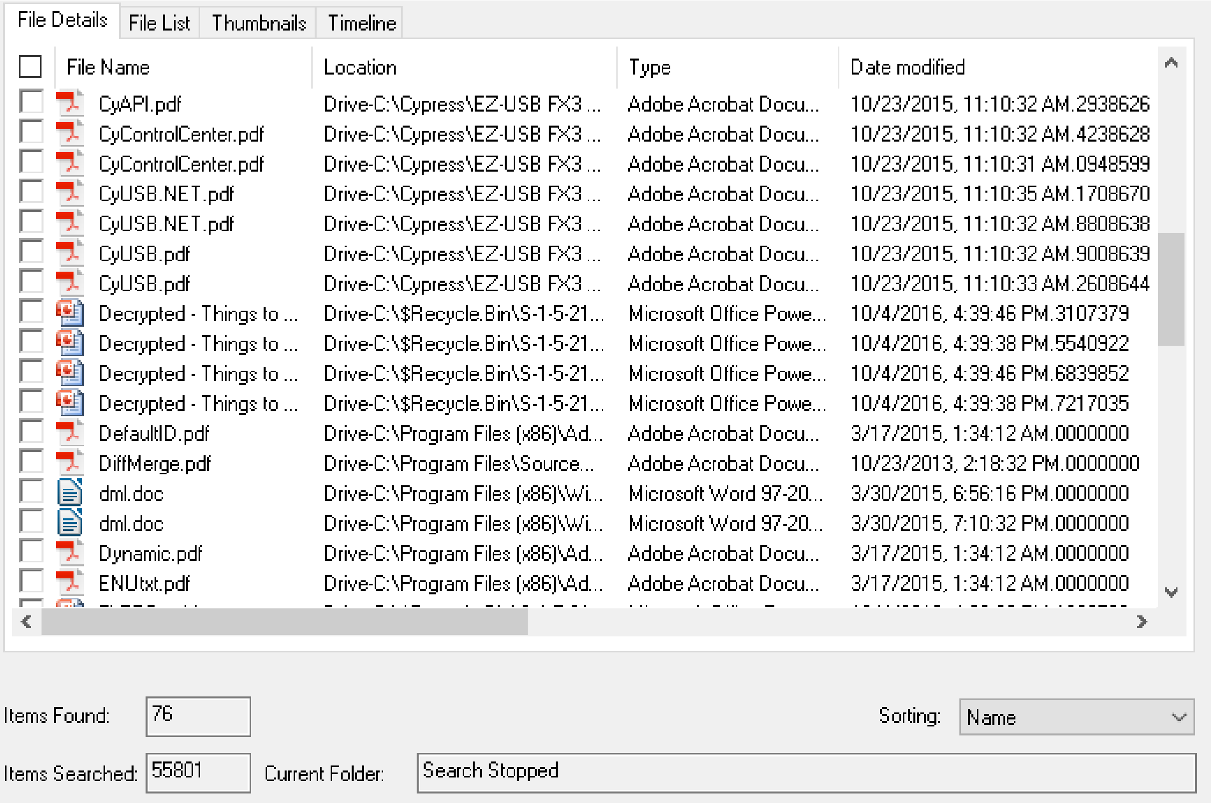
Minimum number of alternate stream
A file must have at least this many alternate data streams to be included.

Minimum size of alternate streams
The total combined size of all alternate data streams must be at least this much for the file to be included.

4.2.2 File Name Search Results View

The user may view the file name search results in one of several views.

File Details View



□ File Name	Location	Type	Date modified
□ CyAPI.pdf	Drive-C:\Cypress\EZ-USB FX3 ...	Adobe Acrobat Docu...	10/23/2015, 11:10:32 AM.2938626
□ CyControlCenter.pdf	Drive-C:\Cypress\EZ-USB FX3 ...	Adobe Acrobat Docu...	10/23/2015, 11:10:32 AM.4238628
□ CyControlCenter.pdf	Drive-C:\Cypress\EZ-USB FX3 ...	Adobe Acrobat Docu...	10/23/2015, 11:10:31 AM.0948599
□ CyUSB.NET.pdf	Drive-C:\Cypress\EZ-USB FX3 ...	Adobe Acrobat Docu...	10/23/2015, 11:10:35 AM.1708670
□ CyUSB.NET.pdf	Drive-C:\Cypress\EZ-USB FX3 ...	Adobe Acrobat Docu...	10/23/2015, 11:10:32 AM.8808638
□ CyUSB.pdf	Drive-C:\Cypress\EZ-USB FX3 ...	Adobe Acrobat Docu...	10/23/2015, 11:10:32 AM.9008639
□ CyUSB.pdf	Drive-C:\Cypress\EZ-USB FX3 ...	Adobe Acrobat Docu...	10/23/2015, 11:10:33 AM.2608644
□ Decrypted - Things to ...	Drive-C:\$Recycle.Bin\S-1-5-21...	Microsoft Office Powe...	10/4/2016, 4:39:46 PM.3107379
□ Decrypted - Things to ...	Drive-C:\$Recycle.Bin\S-1-5-21...	Microsoft Office Powe...	10/4/2016, 4:39:38 PM.5540922
□ Decrypted - Things to ...	Drive-C:\$Recycle.Bin\S-1-5-21...	Microsoft Office Powe...	10/4/2016, 4:39:46 PM.6839852
□ Decrypted - Things to ...	Drive-C:\$Recycle.Bin\S-1-5-21...	Microsoft Office Powe...	10/4/2016, 4:39:38 PM.7217035
□ DefaultID.pdf	Drive-C:\Program Files (x86)\Ad...	Adobe Acrobat Docu...	3/17/2015, 1:34:12 AM.0000000
□ DiffMerge.pdf	Drive-C:\Program Files\Source...	Adobe Acrobat Docu...	10/23/2013, 2:18:32 PM.0000000
□ dml.doc	Drive-C:\Program Files (x86)\Wi...	Microsoft Word 97-20...	3/30/2015, 6:56:16 PM.0000000
□ dml.doc	Drive-C:\Program Files (x86)\Wi...	Microsoft Word 97-20...	3/30/2015, 7:10:32 PM.0000000
□ Dynamic.pdf	Drive-C:\Program Files (x86)\Ad...	Adobe Acrobat Docu...	3/17/2015, 1:34:12 AM.0000000
□ ENUtxt.pdf	Drive-C:\Program Files (x86)\Ad...	Adobe Acrobat Docu...	3/17/2015, 1:34:12 AM.0000000

Items Found: 76

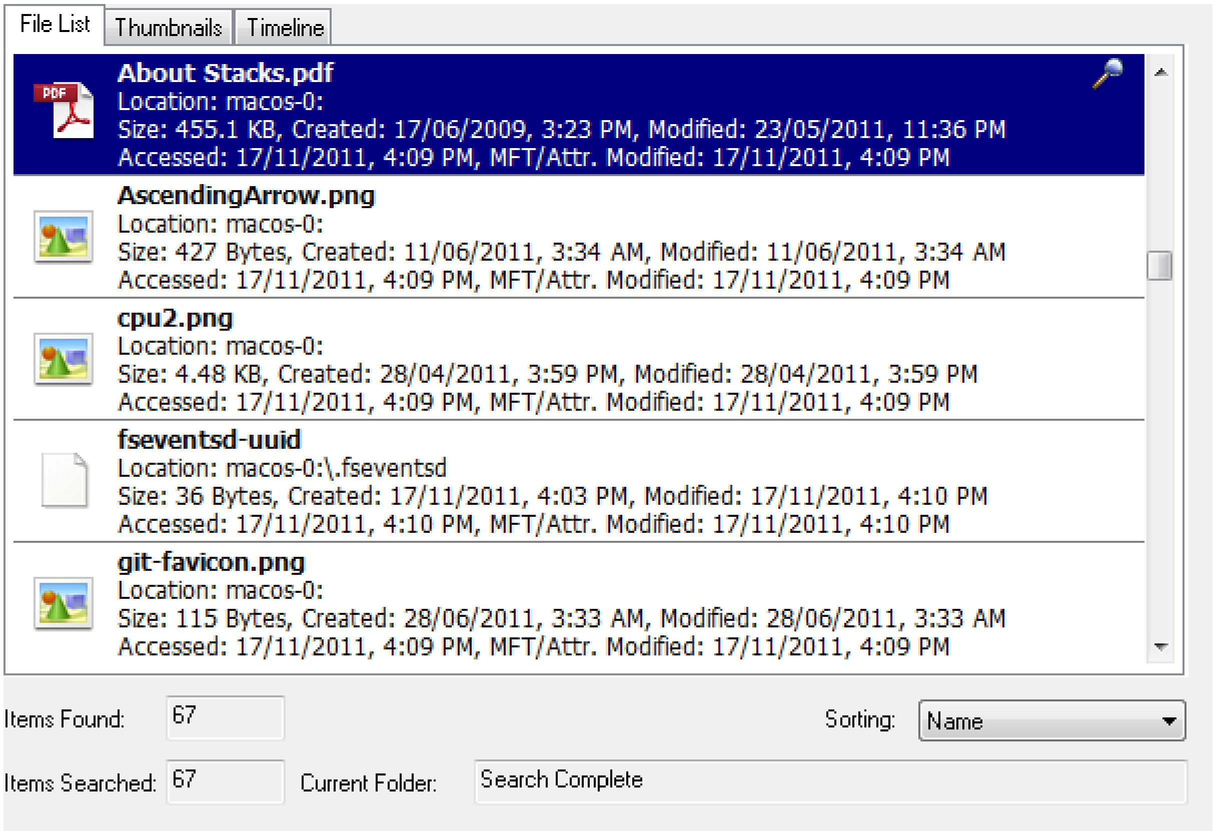
Sorting: Name

Items Searched: 55801

Current Folder: Search Stopped

The File Details View displays the search result in a table format, listing the file names along with relevant attributes and metadata.

File List View



About Stacks.pdf
Location: macos-0:
Size: 455.1 KB, Created: 17/06/2009, 3:23 PM, Modified: 23/05/2011, 11:36 PM
Accessed: 17/11/2011, 4:09 PM, MFT/Attr. Modified: 17/11/2011, 4:09 PM

AscendingArrow.png
Location: macos-0:
Size: 427 Bytes, Created: 11/06/2011, 3:34 AM, Modified: 11/06/2011, 3:34 AM
Accessed: 17/11/2011, 4:09 PM, MFT/Attr. Modified: 17/11/2011, 4:09 PM

cpu2.png
Location: macos-0:
Size: 4.48 KB, Created: 28/04/2011, 3:59 PM, Modified: 28/04/2011, 3:59 PM
Accessed: 17/11/2011, 4:09 PM, MFT/Attr. Modified: 17/11/2011, 4:09 PM

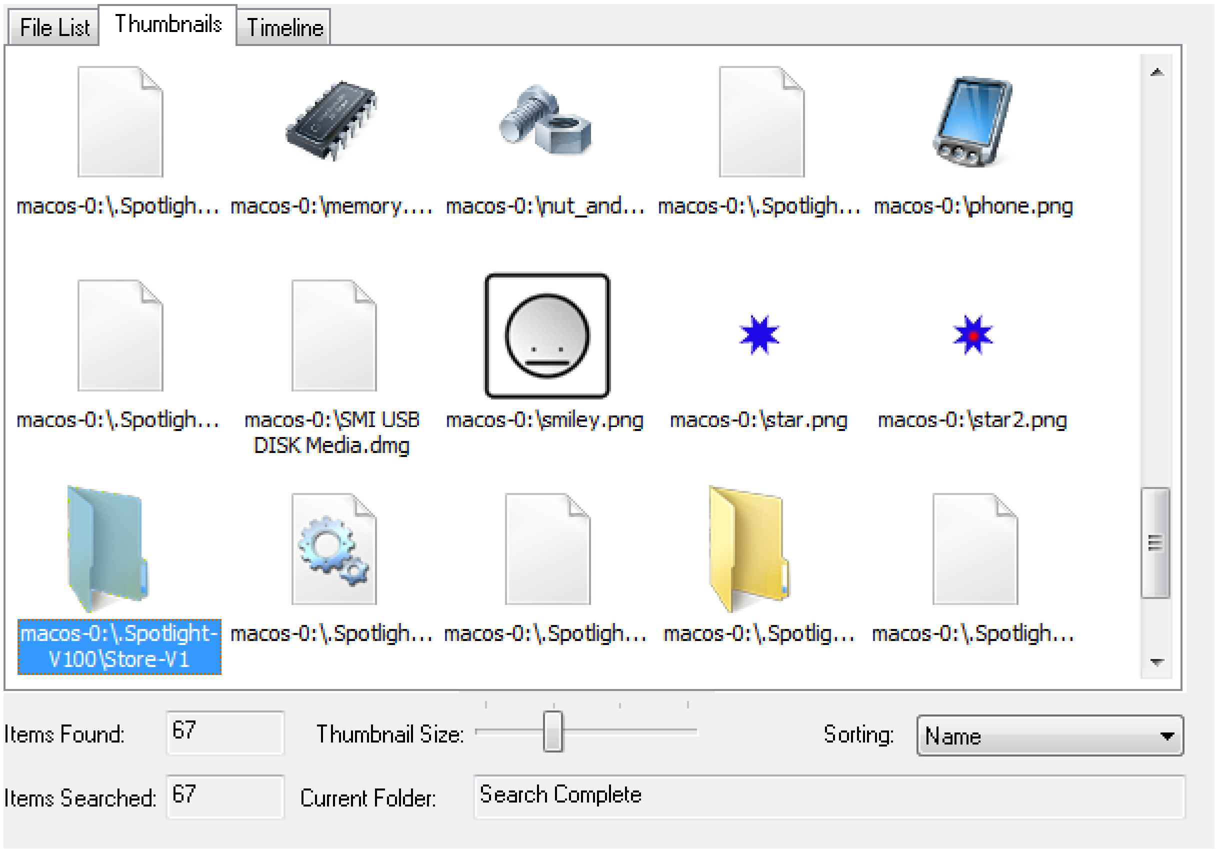
fseventsd-uuid
Location: macos-0:\.fseventsd
Size: 36 Bytes, Created: 17/11/2011, 4:03 PM, Modified: 17/11/2011, 4:10 PM
Accessed: 17/11/2011, 4:10 PM, MFT/Attr. Modified: 17/11/2011, 4:10 PM

git-favicon.png
Location: macos-0:
Size: 115 Bytes, Created: 28/06/2011, 3:33 AM, Modified: 28/06/2011, 3:33 AM
Accessed: 17/11/2011, 4:09 PM, MFT/Attr. Modified: 17/11/2011, 4:09 PM

Items Found: 67
Sorting: Name
Items Searched: 67
Current Folder: Search Complete

The File List View displays the search result as a list of file names, along with the corresponding metadata and icon. The results are sorted according to the criteria selected in the Sorting combo box.

Thumbnails View



Items Found: 67

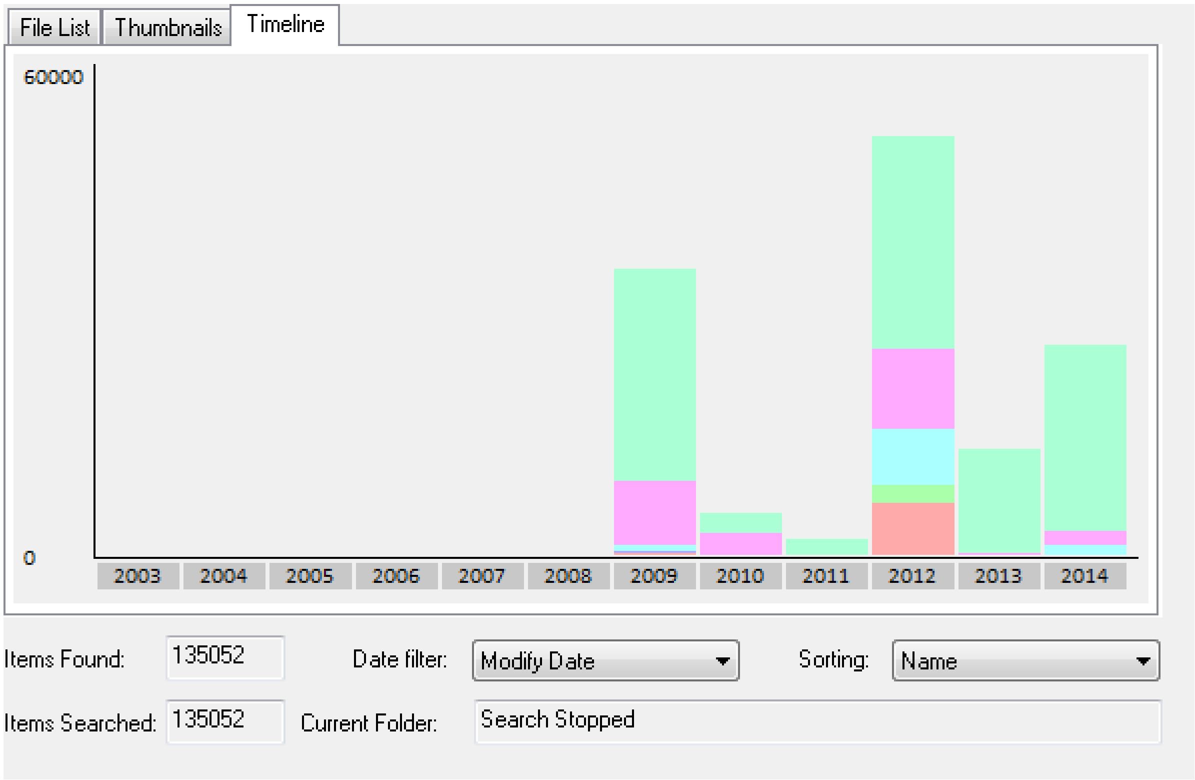
Items Searched: 67

Sorting: Name

Current Folder: Search Complete

The Thumbnails View displays the search result as a list of thumbnails as well as with its file path. This view is useful when searching for media files, allowing the user to quickly browse through the thumbnail images. Similar to the File List View, the results can be sorted via the Sorting combo box. The size of the thumbnails can be adjusted using the Thumbnail Size slider bar.

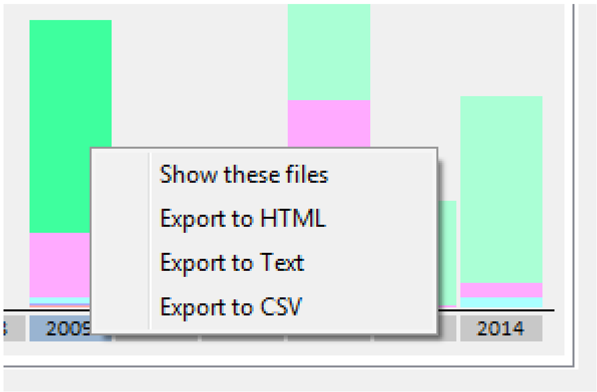
Timeline View



Items Found: 135052 Date filter: Modify Date Sorting: Name

Items Searched: 135052 Current Folder: Search Stopped

The Timeline View displays an interactive bar graph providing the user with a visual view of the distribution of files with respect to the date of the files. This view is useful for identifying date ranges where significant file activity has occurred. The granularity of the scale can be adjusted by clicking on the bar graphs to zoom in or the '-' button on the top-right corner to zoom out. Each bar is colour-coded by file type. Right-clicking a bar section brings up the following menu:



Show these files
Filter the results to show only those that belong to the selected time bar

Export to HTML
Export the results contained in the highlighted bar to HTML

Export to Text
Export the results contained in the highlighted bar to text

Export to CSV
Export the results contained in the highlighted bar to CSV

4.3 Indexing

Indexing allows you to search within the content of many files at once. Unlike the other search modules which only inspect filenames and other surface criteria, indexing allows you to perform deep searches inside the content of PDF documents, Word files, E-mails, image meta data and much more.

In order to do this, you must first create an index for the set of files you wish to examine. This is a thorough process which scans and analyzes the files and builds an index (consider it to be a more sophisticated version of what you would find in the back of a book), which can then be used to perform searches on.

The following modules are used to perform index-based searches.

Create Index
Module that performs the initial index generation required for an index-based search

Search Index
Module that performs an index-based search using the index files created via the Create Index module.

4.3.1 Create Index

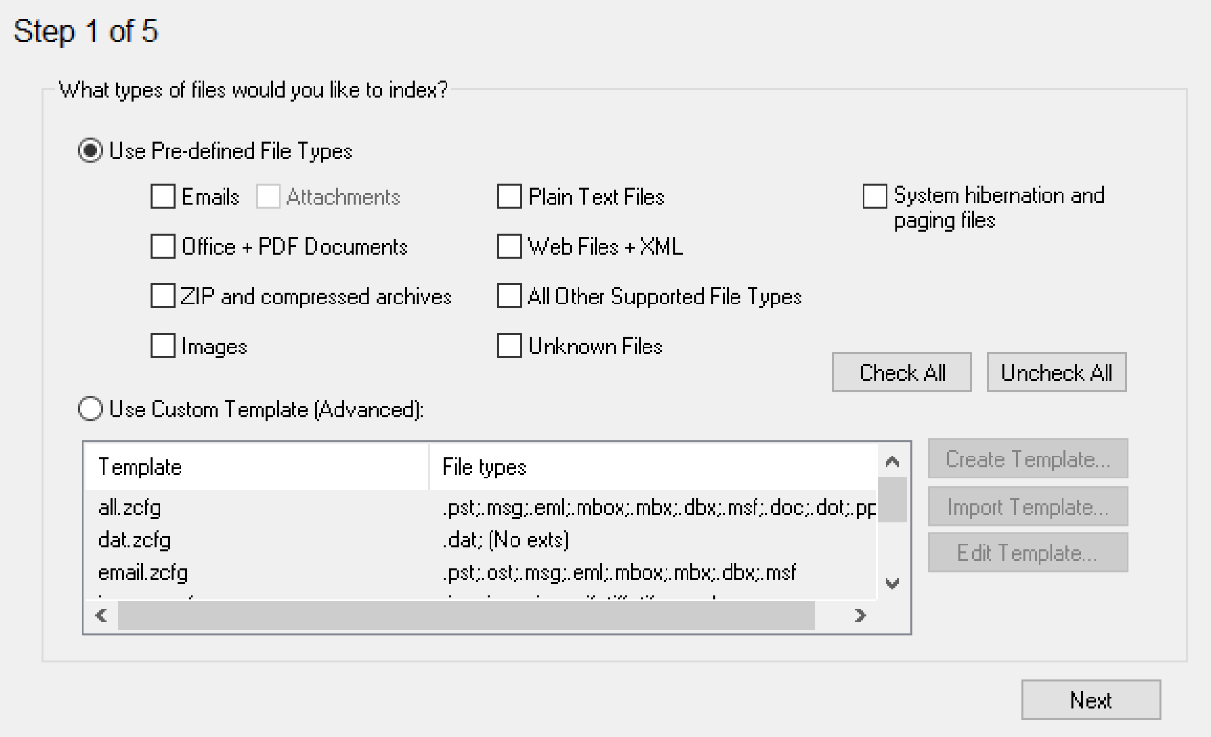
Creating an index allows the investigator to perform lighting fast, content-based searches across the entire drive or section of the drive. This process involves scanning the content of files and emails on the hard drive, and then constructing an index of the words found.

TIP: 64-bit OSForensics is highly recommended when indexing large sets of data.

If you are having problems with the indexing not completing properly or having a lot of errors see this page for common causes and solutions.

The indexing process is presented as a wizard.

Step 1: Select File Types to Index



Step 1 of 5

What types of files would you like to index?

● Use Pre-defined File Types

□ Emails □ Attachments	□ Plain Text Files	□ System hibernation and paging files
□ Office + PDF Documents	□ Web Files + XML	
□ ZIP and compressed archives	□ All Other Supported File Types	
□ Images	□ Unknown Files	

○ Use Custom Template (Advanced):

Template	File types
all.zcfg	.pst;.msg;.eml;.mbox;.mbx;.dbx;.msf;.doc;.dot;.pp
dat.zcfg	.dat; (No exts)
email.zcfg	.pst;.ost;.msg;.eml;.mbox;.mbx;.dbx;.msf

In this step you must select what kind of files you wish to index. You can select between a predefined set of file types or you can specify more advanced indexing options via templates. In general, the more file types that are selected, the longer and more resource consuming the indexing process will take.

E-mails
Scan e-mail files found on the disk. Supports pst, msg, eml, mbox and dbx files.

Attachments
Scan all attachment documents found in email messages.

Office + PDF Documents
Scan Microsoft Office documents, OpenOffice documents and PDF files.

Zip Files
Scan zip archives for files that match the other selected types. As such you should select other file types along with this option as zip files are merely containers and don't contain much interesting information in and of themselves.

Images
Scan image files for metadata information. Supported types are jpeg, gif, tiff, png and bmp.

Plain Text Files
Scan plain text files and rich text documents.

Web Files + XML
Scan HTML web pages and documents including PHP, Perl, JavaScript, CGI, ASP/ASPX, and Shockwave Flash files.

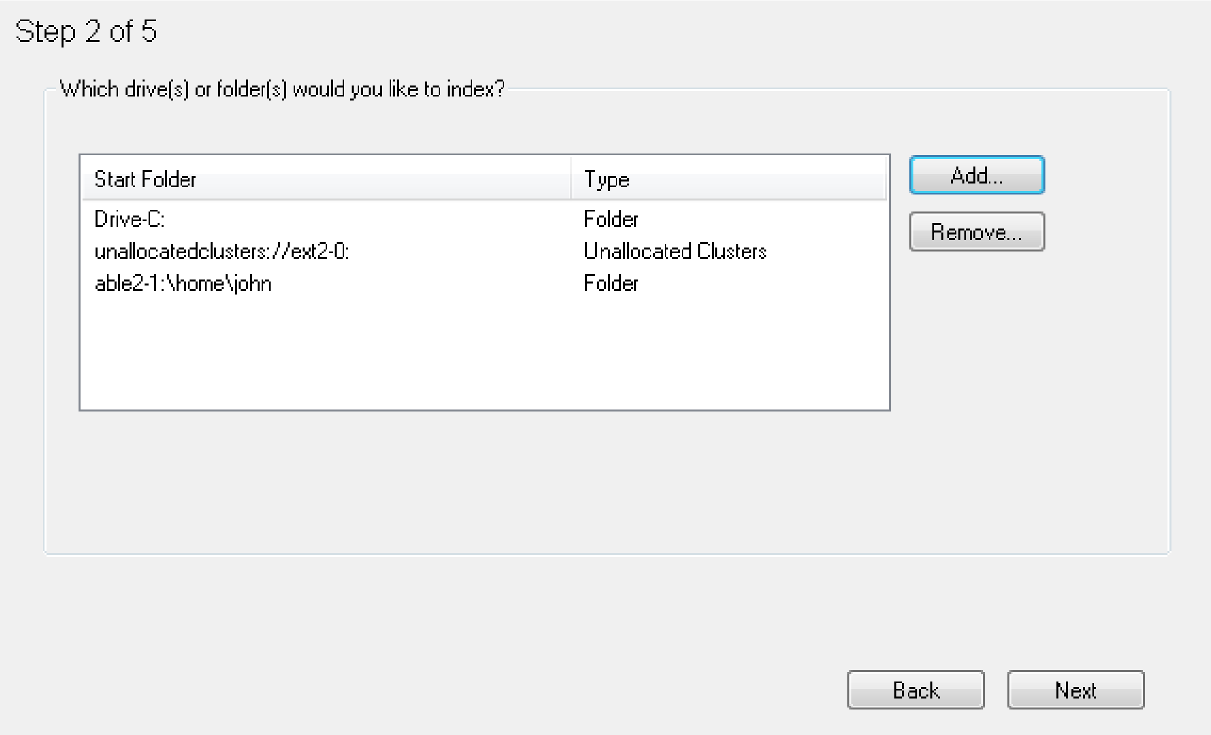
All Other Supported File Types

Scan all other supported types of files supported by the indexing process. This includes the following file types: .nfo, .dat, .wpd, .mp3, .dwf, .torrent, .mht, .avi, .wmv, .mpg, .mpeg, .rmv, .rmvb, .flv, .mov, .qt, .exe, .dgn, .wma, .tar, .gz, .cab, .rar, .psd

Unknown Files
Scan files whose type cannot be determined by their extension or have no extension at all. The indexing process will attempt to identify what kind of file it is dealing with. This option can somewhat increase indexing time as a far greater number of files will be scanned.

System hibernation and paging files
Scan system hibernation file (hiberfile.sys) and system page files (pagefile.sys). Text strings will be extracted from these system files, which are typically very large. This option will significantly increase indexing time and indexed data. We advise a separate index for these files.

Step 2: Location and Advanced Options

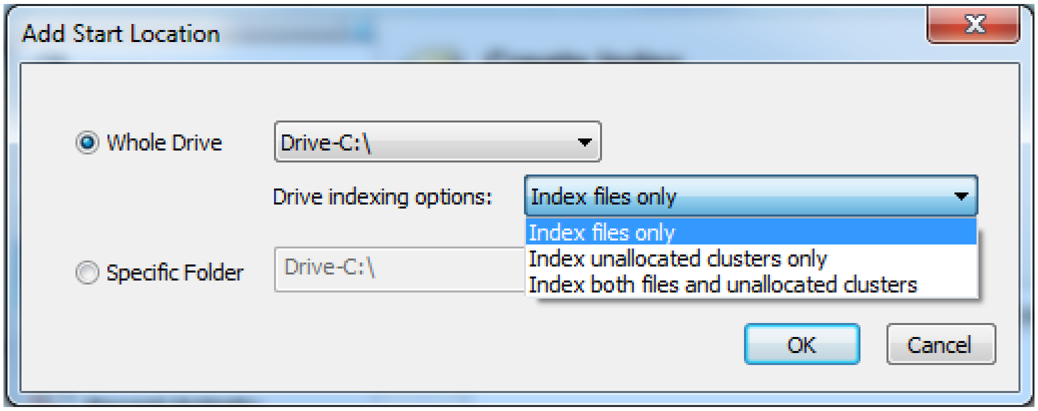


Step 2 of 5

Which drive(s) or folder(s) would you like to index?

Start Folder	Type
Drive-C:	Folder
unallocatedclusters://ext2-0:	Unallocated Clusters
able2-1:\home\john	Folder

In this step, you will specify start directories where OSForensics will scan for files to index. Click the 'Add' button to specify the start location you want to add to the list:



● Whole Drive: Drive-C:\

Drive indexing options: Index files only

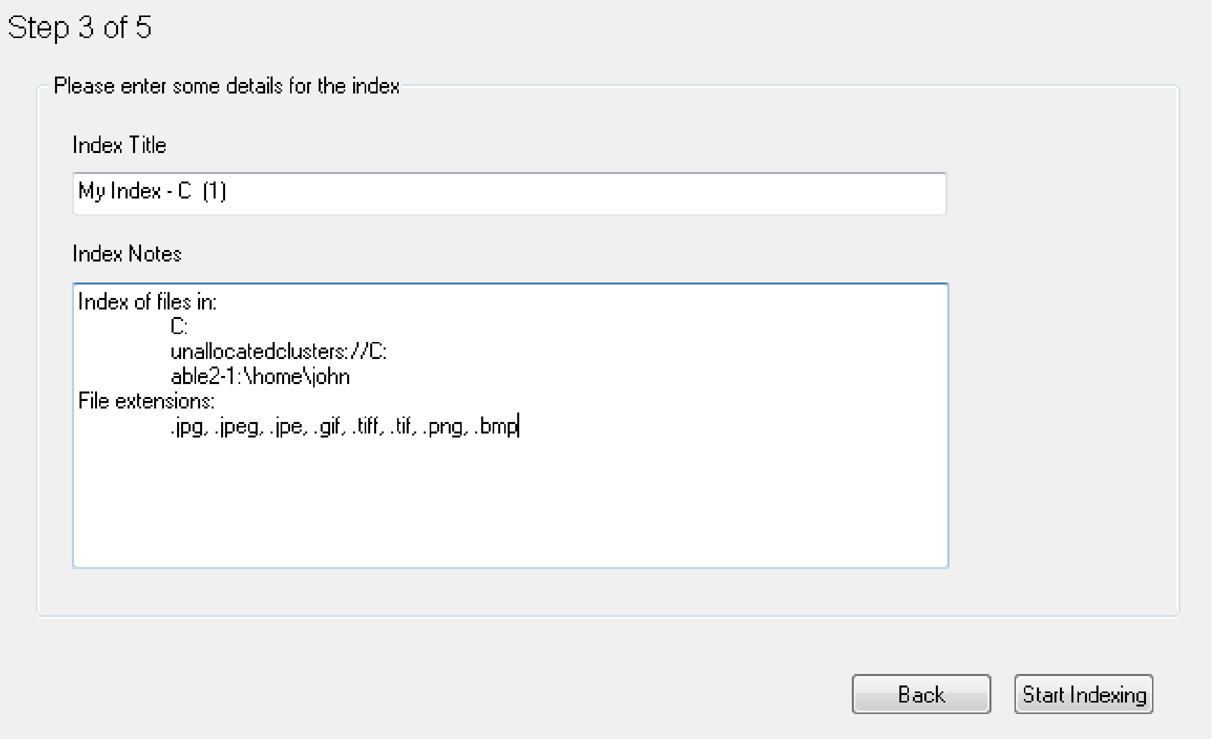
- Index files only
- Index unallocated clusters only
- Index both files and unallocated clusters

○ Specific Folder: Drive-C:\

You may specify an entire drive, or a specific directory (eg. "My Documents" folder) to index. For Whole Drives, you have the option to scan the drive's unallocated clusters as well. However, this will greatly increase the indexing time and resource requirements. Indexing of unallocated clusters is available for all supported file systems.

If you choose to index unallocated clusters, then the file types you have selected are ignored for the data found in the unallocated clusters. In a sense there are no files in unallocated clusters. Any data found in unallocated clusters is treated the same. The strings are extracted and added to the index. Even if, for example, a fragment of data in unallocated clusters was once part of an .doc file, it still isn't processed like an Word document. Only string extraction is done.

Step 3: Case Details



Please enter some details for the index

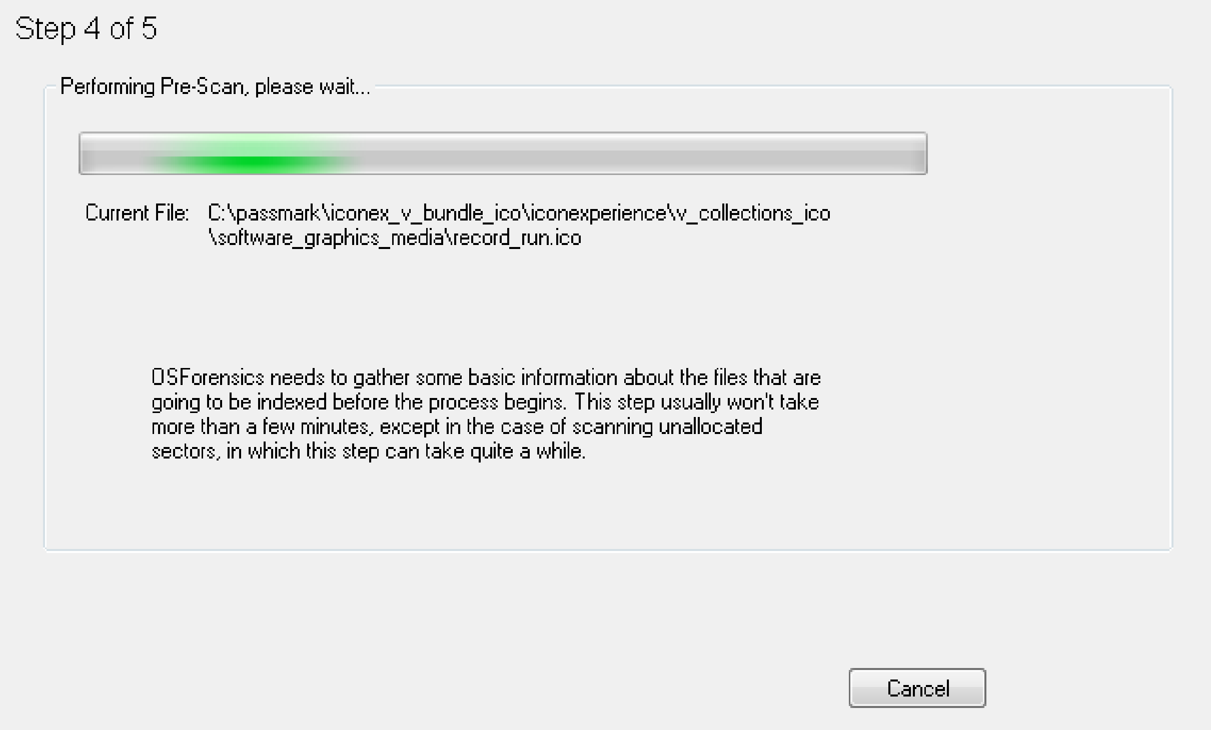
Index Title: My Index - C (1)

Index Notes:

```
Index of files in:
        C:
        unallocatedclusters://C:
        able2-1:\home\john
File extensions:
        .jpg, .jpeg, .jpe, .gif, .tiff, .tif, .png, .bmp
```

In this step, you will need to enter details for this index to be added to the case. If you do not have a case open, you will be prompted to create/open one before moving to the next step. This step allows you to specify a title and notes for your index that will be stored in the case.

Step 4: Pre Scan



Step 4 of 5

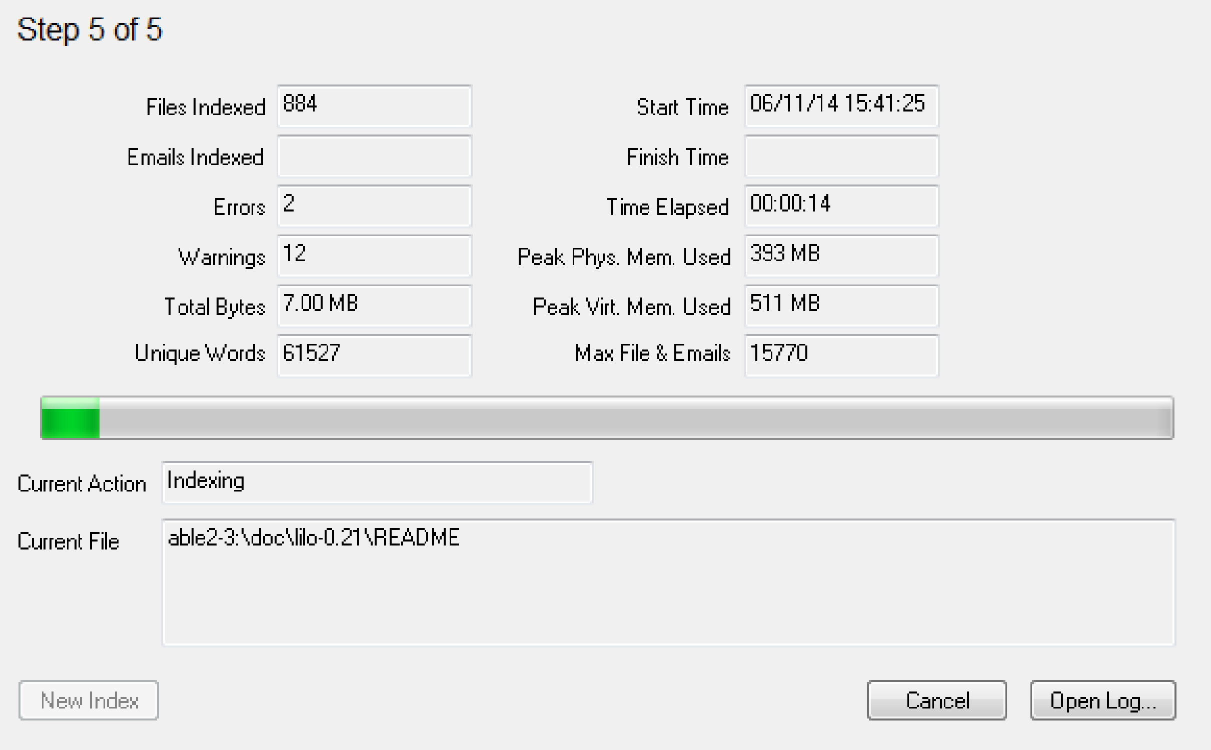
Performing Pre-Scan, please wait...

Current File: C:\passmark\iconex_v_bundle_ico\iconexperience\v_collections_ico \software_graphics_media\record_run.ico

OSForensics needs to gather some basic information about the files that are going to be indexed before the process begins. This step usually won't take more than a few minutes, except in the case of scanning unallocated sectors, in which this step can take quite a while.

During this stage, OSForensics will conduct a preliminary scan of the location and files you have specified in order to set limits for the indexing process. If you have manually set these limits in the advanced indexing options, then this step will be skipped. Barring any errors in this step, it will immediately move on to the final stage where indexing begins.

Step 5: Indexing



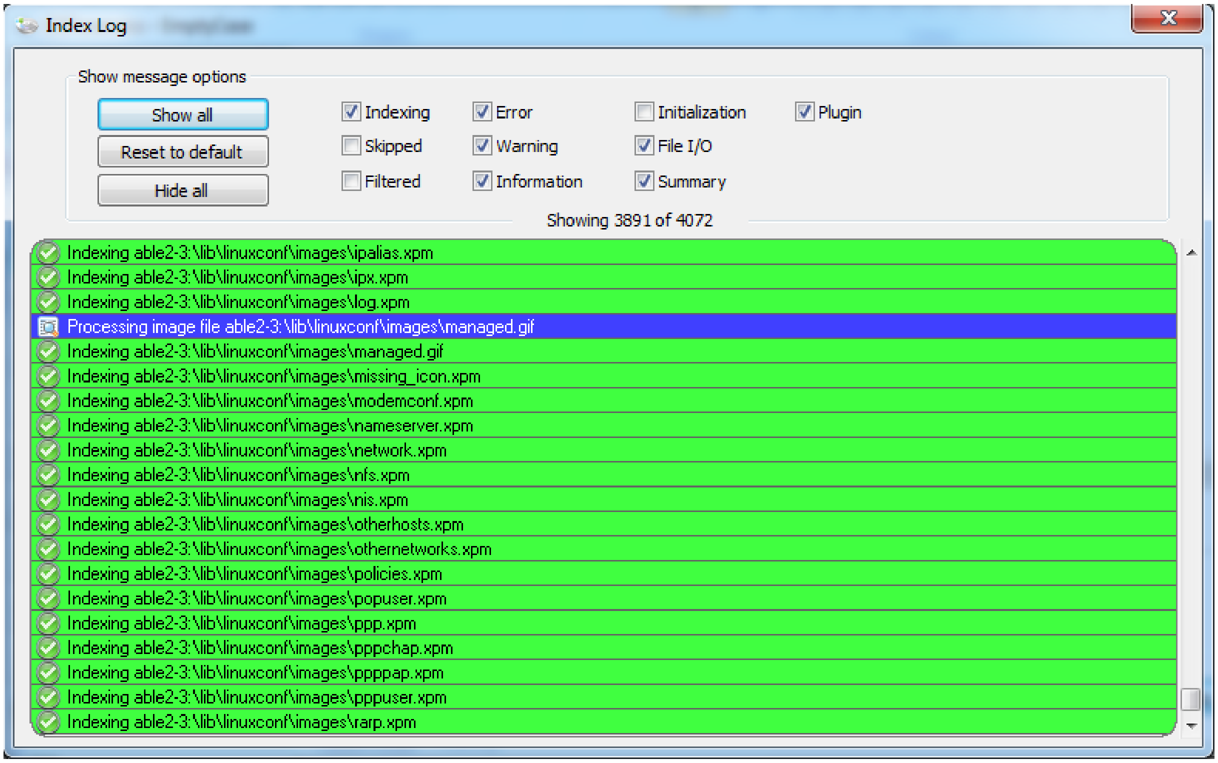
Step 5 of 5

Files Indexed	884	Start Time	06/11/14 15:41:25
Emails Indexed		Finish Time	
Errors	2	Time Elapsed	00:00:14
Warnings	12	Peak Phys. Mem. Used	393 MB
Total Bytes	7.00 MB	Peak Virt. Mem. Used	511 MB
Unique Words	61527	Max File & Emails	15770

Current Action: Indexing

Current File: able2-3:\doc\lilo-0.21\README

The index is now being created. This process can take quite a long time depending on the options selected. To view the log in real-time while indexing is being performed, click on 'Open Log...' to bring up a log window as shown below.



Show message options

☑ Indexing ☑ Error ☐ Initialization ☑ Plugin
☐ Skipped ☑ Warning ☑ File I/O
☐ Filtered ☑ Information ☑ Summary

Showing 3891 of 4072

```
Indexing able2-3:\lib\linuxconf\images\ipalias.xpm
Indexing able2-3:\lib\linuxconf\images\ipx.xpm
Indexing able2-3:\lib\linuxconf\images\log.xpm
Processing image file able2-3:\lib\linuxconf\images\managed.gif
Indexing able2-3:\lib\linuxconf\images\managed.gif
Indexing able2-3:\lib\linuxconf\images\missing_icon.xpm
Indexing able2-3:\lib\linuxconf\images\modemconf.xpm
Indexing able2-3:\lib\linuxconf\images\nameserver.xpm
Indexing able2-3:\lib\linuxconf\images\network.xpm
Indexing able2-3:\lib\linuxconf\images\nfs.xpm
Indexing able2-3:\lib\linuxconf\images\nis.xpm
Indexing able2-3:\lib\linuxconf\images\otherhosts.xpm
Indexing able2-3:\lib\linuxconf\images\othernetworks.xpm
Indexing able2-3:\lib\linuxconf\images\policies.xpm
Indexing able2-3:\lib\linuxconf\images\popuser.xpm
Indexing able2-3:\lib\linuxconf\images\ppp.xpm
Indexing able2-3:\lib\linuxconf\images\pppchap.xpm
Indexing able2-3:\lib\linuxconf\images\ppppap.xpm
Indexing able2-3:\lib\linuxconf\images\pppuser.xpm
Indexing able2-3:\lib\linuxconf\images\rarp.xpm
```

The log entries can be filtered according to the message type.

At the end of the indexing process, if no critical errors occurred, you will now be able to search against the index via the search index module.

Additional Information:

See the following pages for more detailed information about the specifics of some of the data gathering.
Advanced Indexer Options
Indexing Problems and Solutions

4.3.1.1 Indexing Problems and Solutions

The indexing process fails due to not enough memory

Indexing uses a lot a memory, especially for large file sets. If indexing a large number of files it is highly recommended to use the 64-bit version of OSForensics if possible which has far higher memory capacity (also a machine with lots of physical memory will help). If this is not possible, or you are still encountering errors even with this, there are a few other things you can try.

Don't index unallocated sectors, this is a highly intensive operation.

Breaking up the index into several smaller indexes. For example, one for emails, one for office documents or an index for the "Program Files" directory and an index for the "Users" directory. This will mean that each index will need to be searched separately however it will allow you to overcome the limitations of the indexing process.

Reducing the maximum file size indexed in the advanced indexing options can also greatly reduce the amount of memory needed. 99% of files indexed will probably be less then 1MB, however if the pre-scan detects a single 1GB file the indexing process will use that much extra memory. By excluding a few very big files you can greatly reduce the memory requirements.

The log file shows a lot of errors about files being locked

If you are indexing an active system drive (the drive windows is running from) this is quite common as many programs and windows itself will be using the files on the drive making them inaccessable. Usually these files are system files without much interesting text in them and this should not be a problem.

The log file says the max number of pages was reached

During the pre-scan step OSForensics tries to detect the number of files that will be included in the index and sets this as the maximum the indexing process will scan. Because the pre-scan is a rough and fast scan it may sometimes get this wrong. If this is the case you should try indexing again by setting the maximum pages manually in the advanced options.

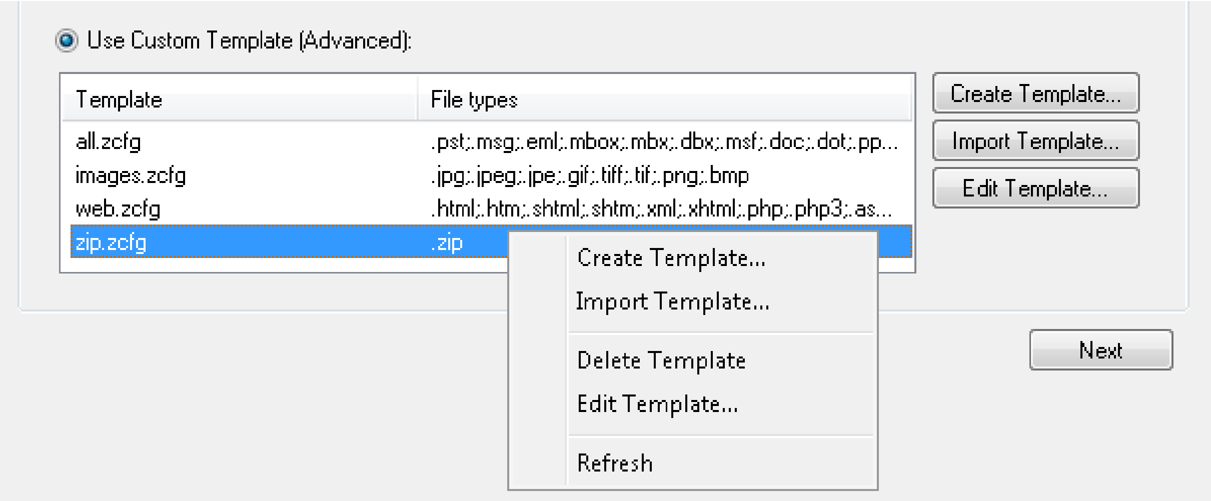
Limits on recursive indexing

When indexing archive files like ZIP, there is a limit to the number of recursions that can take place. For example, when a ZIP file contains a ZIP file, this requires a recursive indexing. OSF is currently designed to index up to 16 levels of recursion in archive files.

For e-mails containing attachments (which may themselves be another e-mail containing yet another attachment), OSF will successfully index recursively until the URL is too long to return meaningfully as a search result. There is no fixed depth limit for recursively indexing e-mail attachments.

4.3.1.2 Indexing Templates

Templates allow the user to specify advanced indexing options in cases where the predefined options are insufficient for an investigator's analysis needs. To use templates, select the 'Use Custom Template' button from Step 1 of the index creation procedure.



● Use Custom Template (Advanced):

Template	File types
all.zcfg	.pst;.msg;.eml;.mbox;.mbx;.dbx;.msf;.doc;.dot;.pp...
images.zcfg	.jpg;.jpeg;.jpe;.gif;.tiff;.tif;.png;.bmp
web.zcfg	.html;.htm;.shtml;.shtm;.xml;.xhtml;.php;.php3;.as...
zip.zcfg	.zip

Create Template

To create a new template, click the 'Create Template' button or right-click menu option. You will be prompted to specify a set of file types to be scanned as part of the indexing process via the Advanced Indexing Options window. Once the settings have been finalized, you will be prompted to specify a name for the template file.

Import Template

A template can be imported from an existing .zcfg file, which can be an existing template or a Zoom configuration file. Once the file is selected, the settings are propagated to the Advanced Indexing Options window where the template can be further refined.

Delete Template

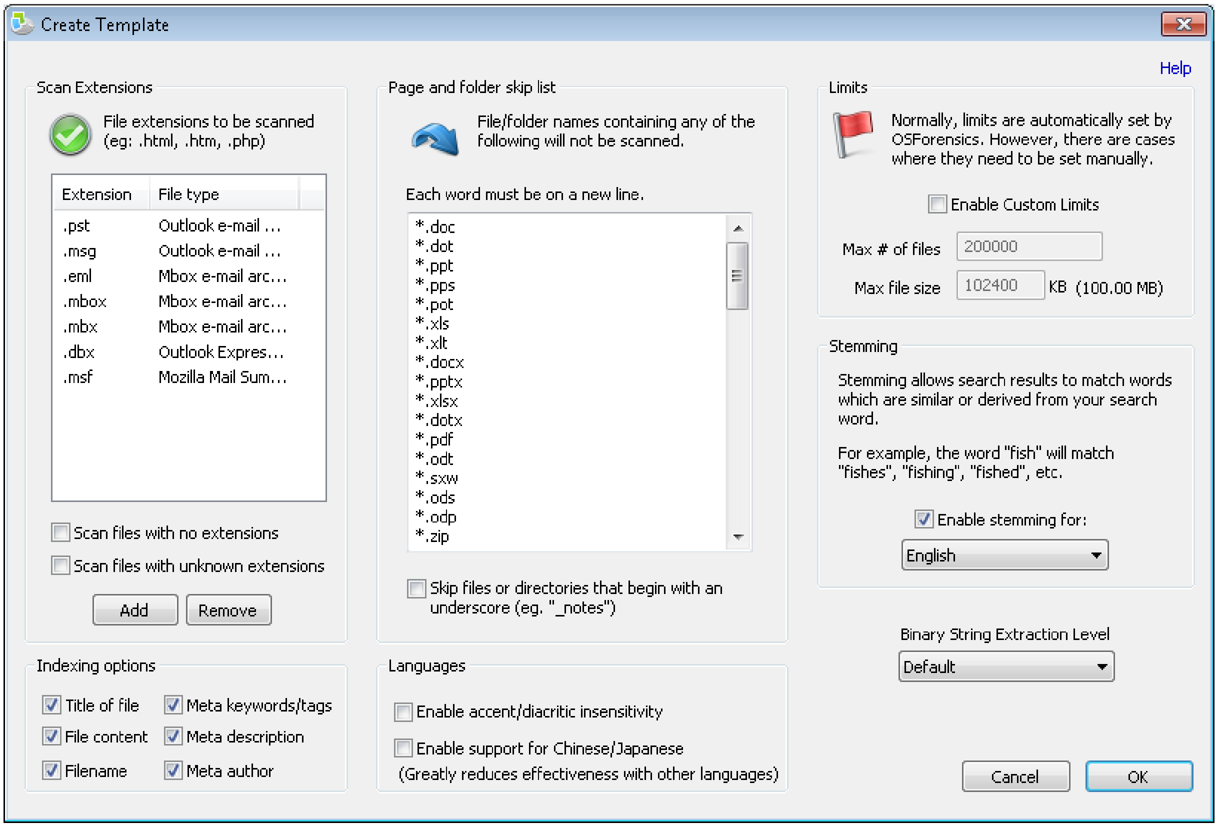
Deletes the template file from OSForensics

Edit Template

Opens the Advanced Indexing Options window where the existing template can be modified.

4.3.1.2.1 Advanced Indexing Options

The Indexer Advanced Options allows users to configure various indexing parameters. This window can be accessed when Creating or Editing a template.



Create Template

Help

Scan Extensions

File extensions to be scanned (eg: .html, .htm, .php)

Extension	File type
.pst	Outlook e-mail ...
.msg	Outlook e-mail ...
.eml	Mbox e-mail arc...
.mbox	Mbox e-mail arc...
.mbx	Mbox e-mail arc...
.dbx	Outlook Expres...
.msf	Mozilla Mail Sum...

□ Scan files with no extensions

□ Scan files with unknown extensions

Add Remove

Page and folder skip list

File/folder names containing any of the following will not be scanned.

Each word must be on a new line.

```
*.doc
*.dot
*.ppt
*.pps
*.pot
*.xls
*.xlt
*.docx
*.pptx
*.xlsx
*.dotx
*.pdf
*.odt
*.sxw
*.ods
*.odp
*.zip
```

□ Skip files or directories that begin with an underscore (eg. "_notes")

Limits

Normally, limits are automatically set by OSForensics. However, there are cases where they need to be set manually.

□ Enable Custom Limits

Max # of files: 200000

Max file size: 102400 KB (100.00 MB)

Stemming

Stemming allows search results to match words which are similar or derived from your search word.

For example, the word "fish" will match "fishes", "fishing", "fished", etc.

☑ Enable stemming for: English

Binary String Extraction Level: Default

Indexing options

☑ Title of file ☑ Meta keywords/tags

☑ File content ☑ Meta description

☑ Filename ☑ Meta author

Languages

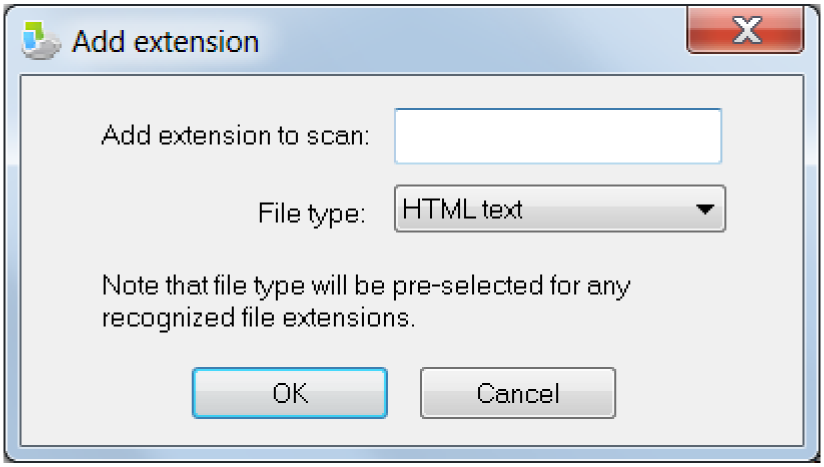
□ Enable accent/diacritic insensitivity

□ Enable support for Chinese/Japanese (Greatly reduces effectiveness with other languages)

Cancel OK

Scan Extensions

The list of file types whose contents will be scanned are configured here. Typical file extensions are added to the list by default. To add a new file extension, click the 'Add' button.



Add extension

Add extension to scan:

File type: HTML text

Note that file type will be pre-selected for any recognized file extensions.

OK Cancel

The user must specify the file extension and the associated file type to include the new file extension in the indexing process. To remove a file extension, click the 'Remove' button

Scan files with no extension
If checked, files without an extension are included in the indexing process

Scan files with unknown extension
If checked, files not included in the list are included in the indexing process

Page and folder skip list

Pages and folders containing particular words can be excluded from the scan by adding the words to the list. Note that the folder the created index files are written to is also automatically added so that the indexing process does not index the files it is creating. This folder is a sub folder of the currently active case folder.

Skip files or directories that begin with an underscore when indexing offline
If checked, files or directories that begin with an underscore will be excluded from the scan when indexing offline

Limits

Limits allow users to manually configure indexing limits, which may need to be done in special cases. To enable custom limits, check the 'Enable Custom Limits' checkbox.

Max. files to index
Maximum number of files to scan and include in the index

Max. file size indexed
Maximum file size that can be indexed, This limit does not apply directly to containers such are zip and mail files (but does apply to the files extracted from within them).

Stemming

Stemming refers to similar words that derived from search terms. For example, searches for "fish" would return results for "fishing", "fishes", and "fished". To enable stemming, check the 'Enable stemming for:' checkbox and select a language.

Accent/diacritic insensitivity

This will map all occurrences of accented characters to their non-accented equivalent (eg. ó, ò, ô, etc. will all be treated as “o”). With this enabled, a user can enter the search word “cliché” and it will find all occurrences of the word on your website spelt as either “cliché” or “cliche".

Unallocated

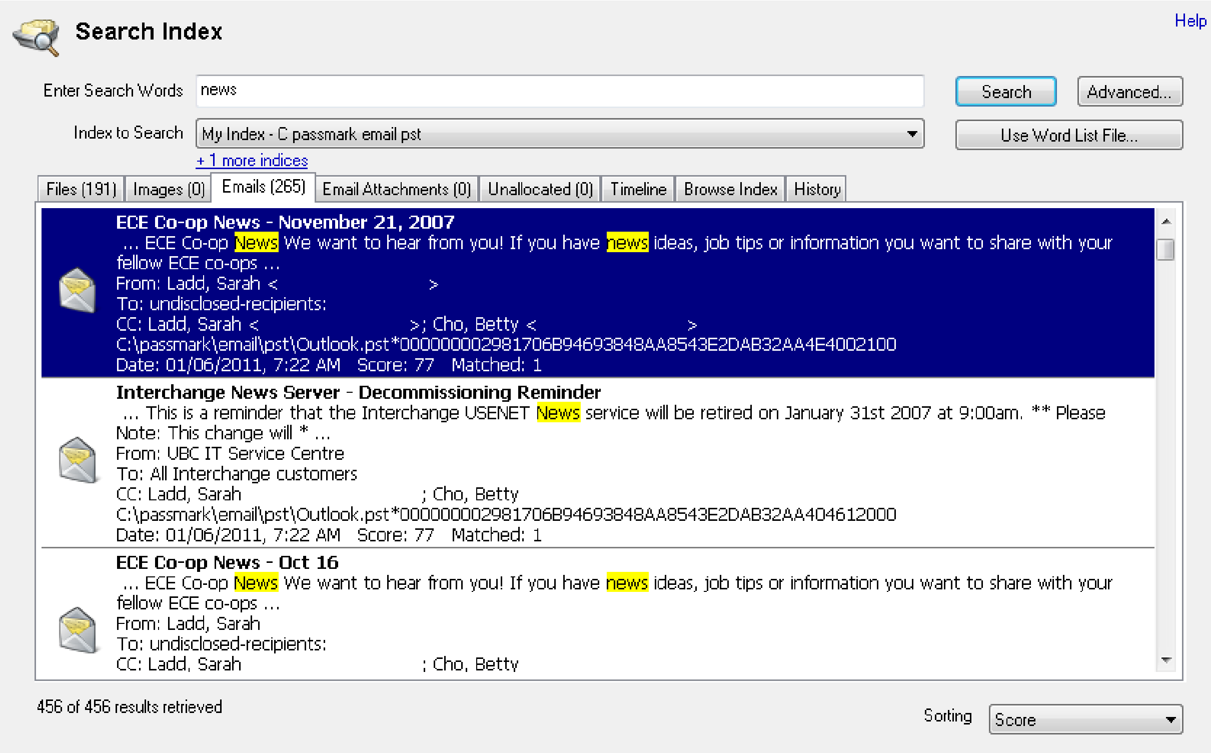
Allows for indexing of text found in unallocated sectors of the hard disk.

Binary String Extraction Level

When trying to get words out of binary data the indexing process has to make a decision as to what is a word and what is just random data. Changing this option will determine how lenient/strict the indexer is when making this decision. Generally leaving this on default, the most strict option, is recommended as this will aggressively remove nonsense data a keep the index to a more manageable size. The Code Words setting is useful if you are trying to find things like passwords missed by the default option. The Extreme option will pull out a lot of data, much of which will be nonsense, in most cases this option will not be needed.

4.3.2 Search Index

The Search Index module performs the actual search using the index generated via the Create Index module. Unlike the File Name Search, the contents of the file are searched (as opposed to just the filename) for the user-specified search words.



Enter Search Words: news

Index to Search: My Index - C passmark email pst

ECE Co-op News - November 21, 2007
... ECE Co-op News We want to hear from you! If you have news ideas, job tips or information you want to share with your fellow ECE co-ops ...
From: Ladd, Sarah < >
To: undisclosed-recipients:
CC: Ladd, Sarah < >; Cho, Betty < >
C:\passmark\email\pst\Outlook.pst*000000002981706B94693848AA8543E2DAB32AA4E4002100
Date: 01/06/2011, 7:22 AM Score: 77 Matched: 1

Interchange News Server - Decommissioning Reminder
... This is a reminder that the Interchange USENET News service will be retired on January 31st 2007 at 9:00am. ** Please Note: This change will * ...
From: UBC IT Service Centre
To: All Interchange customers
CC: Ladd, Sarah ; Cho, Betty
C:\passmark\email\pst\Outlook.pst*000000002981706B94693848AA8543E2DAB32AA404612000
Date: 01/06/2011, 7:22 AM Score: 77 Matched: 1

ECE Co-op News - Oct 16
... ECE Co-op News We want to hear from you! If you have news ideas, job tips or information you want to share with your fellow ECE co-ops ...
From: Ladd, Sarah
To: undisclosed-recipients:
CC: Ladd, Sarah ; Cho, Betty

456 of 456 results retrieved

Sorting: Score

Usage

To perform a search, first select an index or multiple indices to search. Multiple indices can be specified by clicking the '...more...' link under the drop-down box. Next, simply enter one or several words and click search. More advanced searching criteria is detailed below.

Search Criteria

Any or All Search Words
You can select to search for either any or all of the entered words from the Advanced Search Options (accessed by clicking on the 'Advanced' button).

Wildcards
You can use wildcard characters '*' and '?' in your search terms to search for multiple words and return larger set of results. An asterisk character ('*') in a search term represents any number of characters, while a question mark ('?') represents any single character.

This allows you to perform advanced searches such as "zoom*" which would return all pages containing words beginning with "zoom". Similarly, "z??m" would return all pages containing four letter words beginning with 'z' and ending with 'm'. Also, "*car*" would be a search for any words containing the word "car".

Exact phrase

An exact phrase search returns results where the phrase of words are found, in the same order that they are specified. For example, an exact phrase search for the words "green tea" would only return results where the phrase 'green tea' appears. It would not return pages where the words 'green' and 'tea' are found separately, or in a different order such as, 'tea green'.

To specify an exact phrase search term, you need to enclose the words that form the phrase using double quotation marks. You can also combine the use of exact phrase searches with normal search terms and wildcard search terms within a single search query (eg. "green tea" japan*). Note however, that wildcards within exact phrases (eg. "green te*") are not supported.

Exclusion/negative searches
You can precede a search term with a hyphen character to exclude that search term from being included in your search results. For example, a search for "cat -dog" would return all pages containing the word "cat" but not the word "dog".

Use Word List File

A Word List File allows the user to specify a file containing a list of terms to search for in the currently selected index. This effectively performs a bulk search on the list of terms automatically. Results from the bulk search will appear in the History View from where they can be opened and viewed.

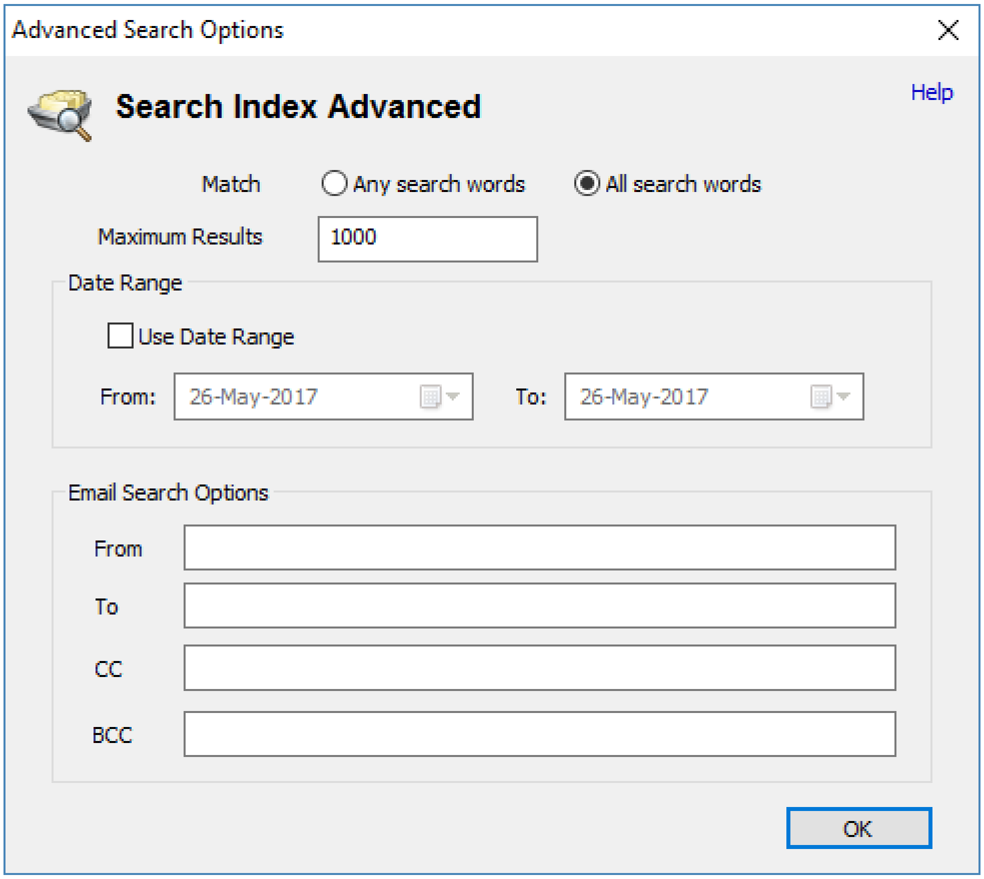
The word list file should place each search on a new line. Lines starting with # are comment lines and will not be searched. A double # at the beginning of a line can be used if you actually need the search term to start with a #. Example search word lists have been provided and will appear in the default directory when selecting a file. For easy access it is recommended you put your own search word list files in this same directory.

Results

The results of the index search are displayed in the tabbed view, organized into file types. See Index Search Results View for more details.

4.3.2.1 Advanced Search Index Options

The Advanced Search Options Window allows users to configure various search parameters. This window can be accessed by clicking on the "Advanced" button in the main Search Index window.



Advanced Search Options

Search Index Advanced

Match ○ Any search words ● All search words

Maximum Results 1000

Date Range

□ Use Date Range

From: 26-May-2017 To: 26-May-2017

Email Search Options

From

To

CC

BCC

Match
The user can select whether the results will match any of the words or all of the words in the search string

Maximum Results
Specifies the maximum number of results to display

Date Range
If 'Use Date Range' is checked, allows the user to filter the results to include only files within the specified date range.

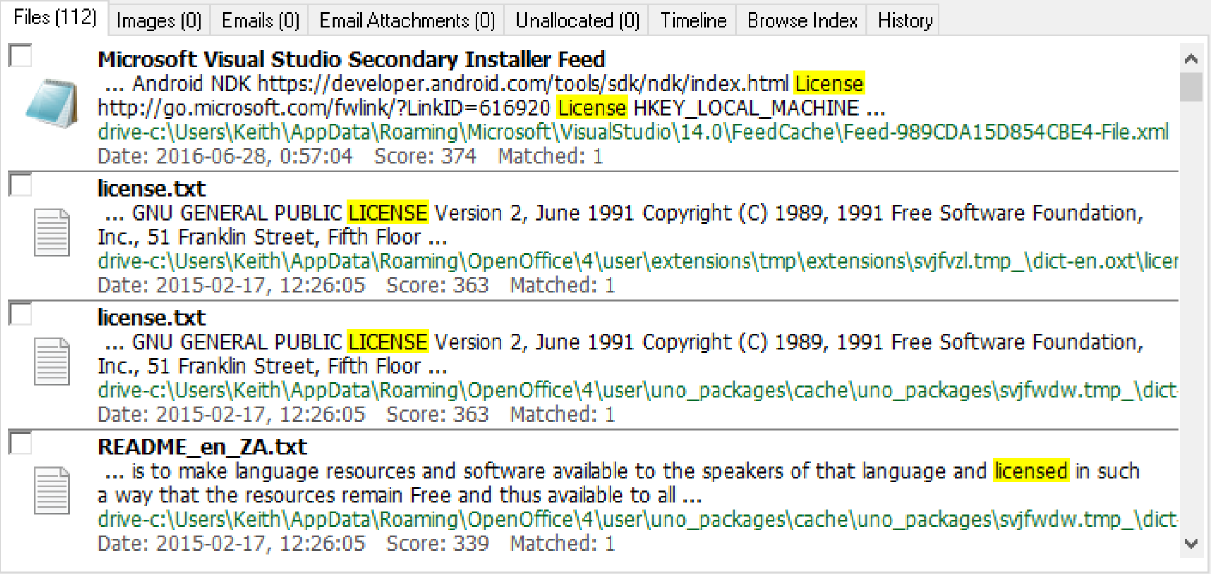
Email Search Options
Allows the user to filter the e-mail search results to those matching the 'From', 'To' and 'CC' fields

4.3.2.2 Index Search Results View

After an index search is performed, the results are displayed in the Results View. The results are organized into several views, depending on the file type.

Types of Views

Files View



□ **Microsoft Visual Studio Secondary Installer Feed**
... Android NDK https://developer.android.com/tools/sdk/ndk/index.html License http://go.microsoft.com/fwlink/?LinkID=616920 License HKEY_LOCAL_MACHINE ...
drive-c:\Users\Keith\AppData\Roaming\Microsoft\VisualStudio\14.0\FeedCache\Feed-989CDA15D854CBE4-File.xml
Date: 2016-06-28, 0:57:04 Score: 374 Matched: 1

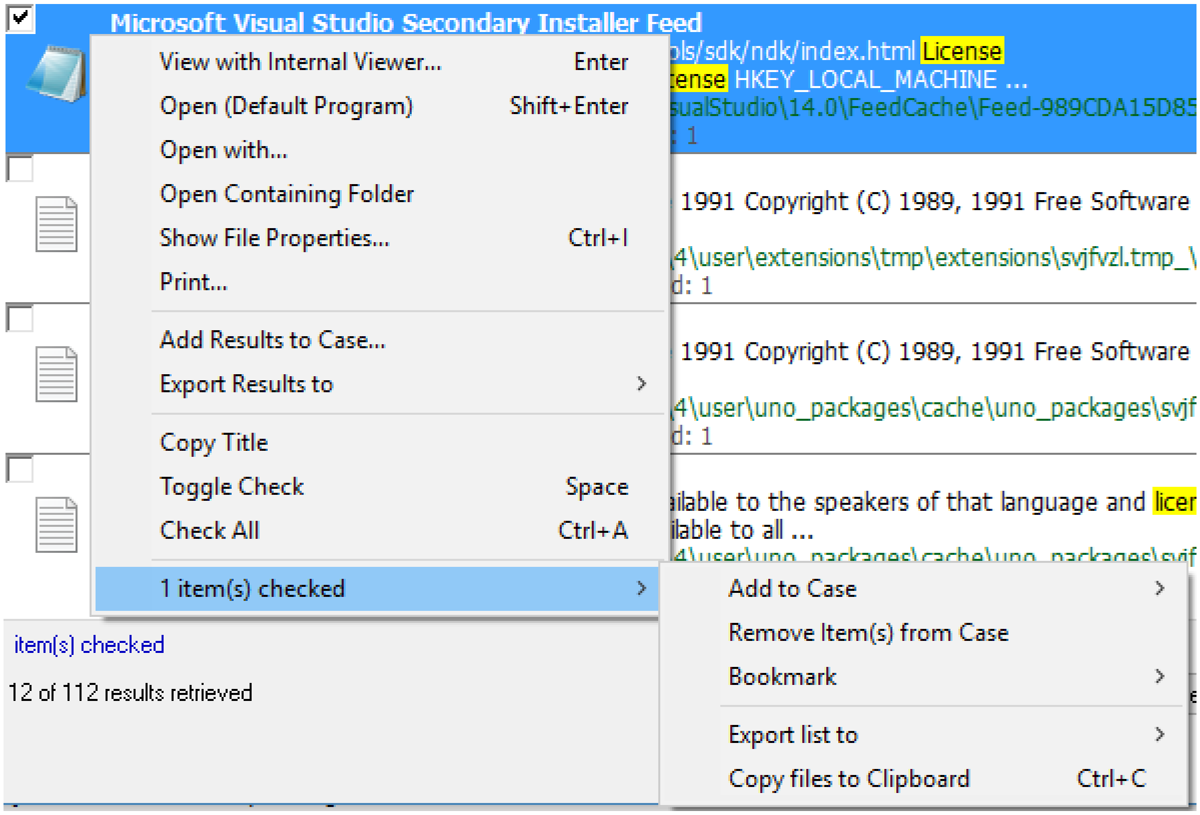
□ **license.txt**
... GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor ...
drive-c:\Users\Keith\AppData\Roaming\OpenOffice\4\user\extensions\tmp\extensions\svjfvzl.tmp_\dict-en.oxt\licer
Date: 2015-02-17, 12:26:05 Score: 363 Matched: 1

□ **license.txt**
... GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor ...
drive-c:\Users\Keith\AppData\Roaming\OpenOffice\4\user\uno_packages\cache\uno_packages\svjfwdw.tmp_\dict
Date: 2015-02-17, 12:26:05 Score: 363 Matched: 1

□ **README_en_ZA.txt**
... is to make language resources and software available to the speakers of that language and licensed in such a way that the resources remain Free and thus available to all ...
drive-c:\Users\Keith\AppData\Roaming\OpenOffice\4\user\uno_packages\cache\uno_packages\svjfwdw.tmp_\dict
Date: 2015-02-17, 12:26:05 Score: 339 Matched: 1

The File View displays the search results as a list of file names, along with its corresponding metadata, icon, score and the number matched. The score ranks the relevancy of the search string with the file.The results are sorted according to the criteria selected in the Sorting combo box.

Right-clicking a file opens the following context menu. Certain actions may or may not be available depending on the current results tab.



View with Interval Viewer

Opens the file with OSForensics Viewer to perform a more thorough analysis

Open (Default Program)
Open the file with the default program.

Open With...
Allows the user to select the program to open the file

Open Containing Folder
Opens the folder than contains the file

Show File Properties
Opens the file with OSForensics Viewer in File Info mode.

Print...
Print the file (if applicable)

Add Results to Case...
Add the list of results as an HTML or CSV file to case

Export Results to
Export the list of results to a TXT, CSV or HTML file

Copy Title
Copy the title to clipboard

Toggle Check
Toggle the check state of the selected item.

Check All
Check all the items in the list.

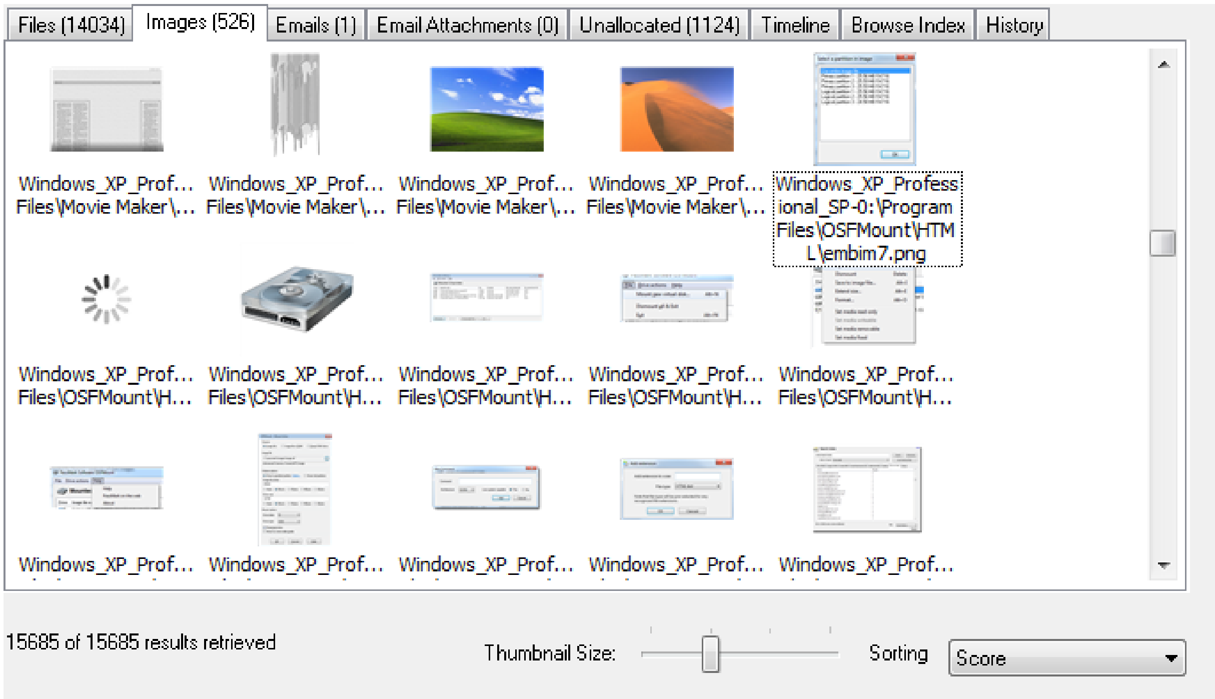
n Item(s) checked

> **Add to Case**
> Add the checked file(s) or list of checked file(s) to the case
>
> **Remove Item(s) from Case**
> Remove the checked file(s) from the case
>
> **Bookmark**
>
> > **Green**
> > Add/remove selected path from the list of Green bookmarks. *Keyboard shortcut: Ctrl+G*
> >
> > **Yellow**
> > Add/remove selected path from the list of Yellow bookmarks. *Keyboard shortcut: Ctrl+Y*
> >
> > **Red**
> > Add/remove selected path from the list of Red bookmarks. *Keyboard shortcut: Ctrl+R*
>
> **Export list to**
> Export the list of checked file(s) to a TXT, CSV or HTML file

Copy File(s) to Clipboard
Copy the checked file(s) to clipboard. Once copied to the clipboard, the file(s) can be pasted to any other application that supports it (eg. Windows Explorer).

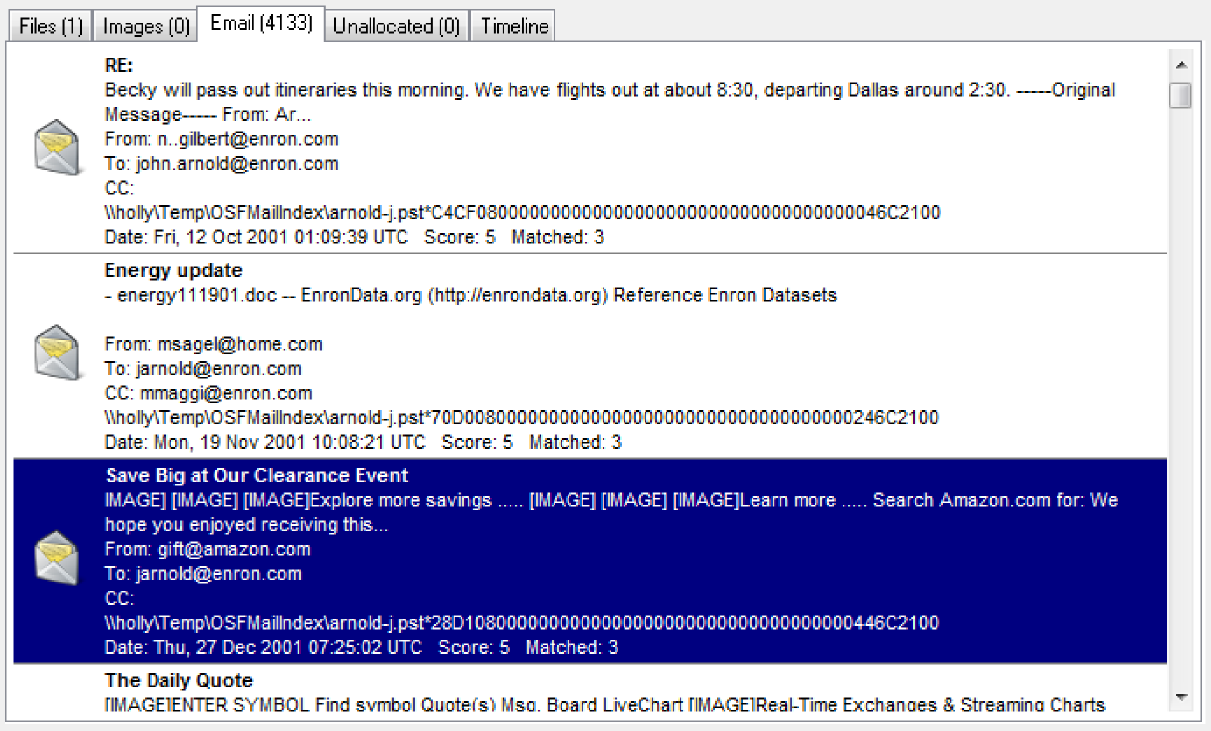
Note: In some cases, copy and pasting files to an explorer window may fail without an error message when "preparing to copy". This may happen if the file has already been deleted (eg a temp file) or if Windows Explorer does not have permissions to access the files (eg restricted system files and folders). In these cases, it is better to use the "Add to case" function.

Images View


Files (14034)
Images (526)
Emails (1)
Email Attachments (0)
Unallocated (1124)
Timeline
Browse Index
History
Windows_XP_Prof... Files\Movie Maker\...
Windows_XP_Professional_SP-0:\Program Files\OSFMount\HTML\embim7.png
Windows_XP_Prof... Files\OSFMount\H...
15685 of 15685 results retrieved
Thumbnail Size:
Sorting
Score

The Images View displays only the search results that contain images as a list of thumbnails. This view is useful when the search results contain media files, allowing the user to quickly browse through the thumbnail images. Similar to the File View, the results can be sorted via the Sorting combo box. The size of the thumbnails can be adjusted using the Thumbnail Size slider bar.

Email View



RE:
Becky will pass out itineraries this morning. We have flights out at about 8:30, departing Dallas around 2:30. -----Original Message----- From: Ar...
From: n..gilbert@enron.com
To: john.arnold@enron.com
CC:
\\holly\Temp\OSFMailIndex\arnold-j.pst*C4CF080000000000000000000000000000000046C2100
Date: Fri, 12 Oct 2001 01:09:39 UTC Score: 5 Matched: 3

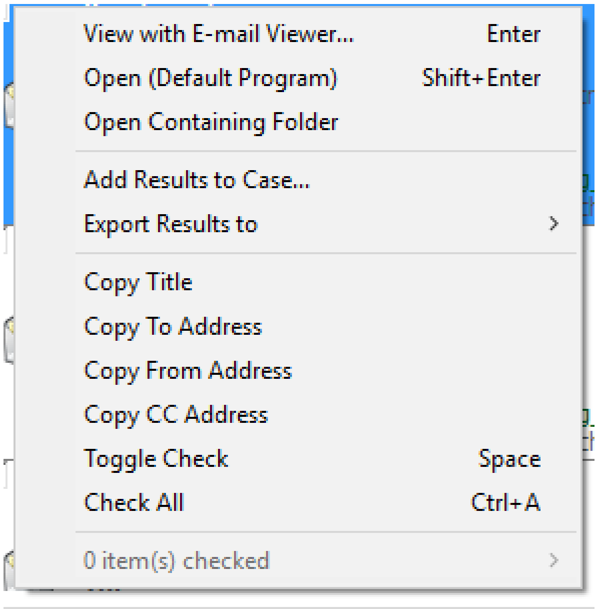
Energy update
- energy111901.doc -- EnronData.org (http://enrondata.org) Reference Enron Datasets

From: msagel@home.com
To: jarnold@enron.com
CC: mmaggi@enron.com
\\holly\Temp\OSFMailIndex\arnold-j.pst*70D0080000000000000000000000000000246C2100
Date: Mon, 19 Nov 2001 10:08:21 UTC Score: 5 Matched: 3

Save Big at Our Clearance Event
IMAGE] [IMAGE] [IMAGE]Explore more savings ..... [IMAGE] [IMAGE] [IMAGE]Learn more ..... Search Amazon.com for: We hope you enjoyed receiving this...
From: gift@amazon.com
To: jarnold@enron.com
CC:
\\holly\Temp\OSFMailIndex\arnold-j.pst*28D1080000000000000000000000000000446C2100
Date: Thu, 27 Dec 2001 07:25:02 UTC Score: 5 Matched: 3

The Daily Quote
[IMAGE]ENTER SYMBOL Find symbol Quote(s) Msg. Board LiveChart [IMAGE]Real-Time Exchanges & Streaming Charts

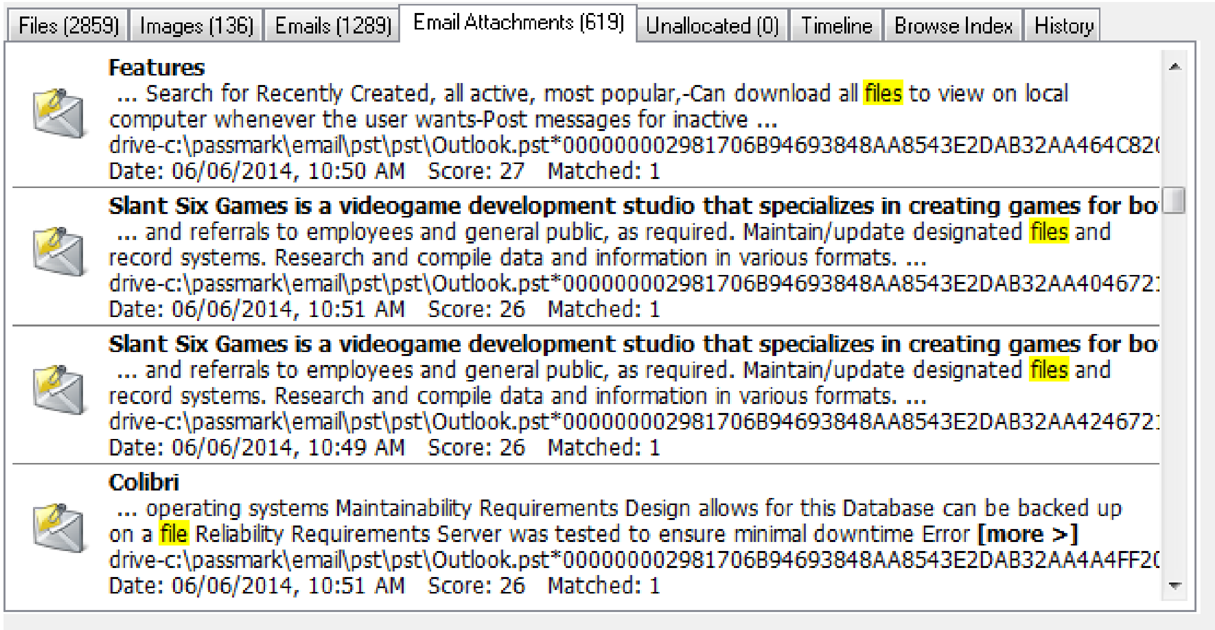
The Email View displays a list of e-mail results. This view displays results containing specific e-mail metadata, such as a preview of the message body, and various e-mail header fields (eg. From, To, CC). Double clicking on an e-mail opens the E-mail Viewer window. Right-clicking an e-mail opens the following context menu:



Copy To / From / CC Address

For emails you can copy any of the addresses associated with it.

Email Attachments View



Features
... Search for Recently Created, all active, most popular,-Can download all files to view on local computer whenever the user wants-Post messages for inactive ...
drive-c:\passmark\email\pst\pst\Outlook.pst*00000002981706B94693848AA8543E2DAB32AA464C82
Date: 06/06/2014, 10:50 AM Score: 27 Matched: 1

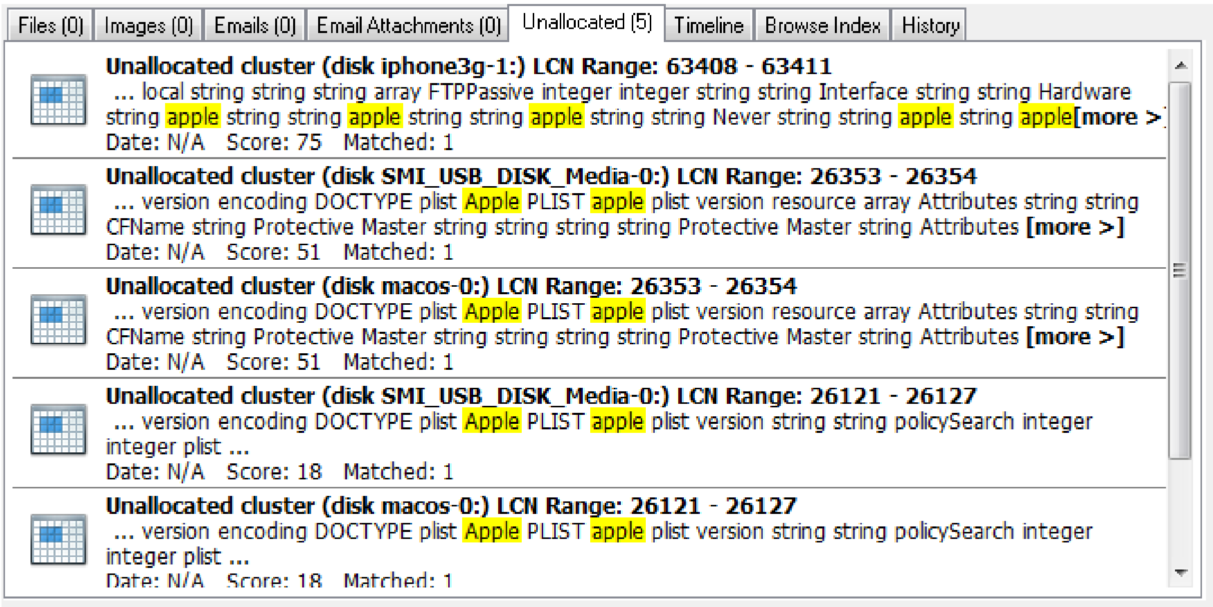
Slant Six Games is a videogame development studio that specializes in creating games for bo
... and referrals to employees and general public, as required. Maintain/update designated files and record systems. Research and compile data and information in various formats. ...
drive-c:\passmark\email\pst\pst\Outlook.pst*00000002981706B94693848AA8543E2DAB32AA404672
Date: 06/06/2014, 10:51 AM Score: 26 Matched: 1

Slant Six Games is a videogame development studio that specializes in creating games for bo
... and referrals to employees and general public, as required. Maintain/update designated files and record systems. Research and compile data and information in various formats. ...
drive-c:\passmark\email\pst\pst\Outlook.pst*00000002981706B94693848AA8543E2DAB32AA424672
Date: 06/06/2014, 10:49 AM Score: 26 Matched: 1

Colibri
... operating systems Maintainability Requirements Design allows for this Database can be backed up on a file Reliability Requirements Server was tested to ensure minimal downtime Error **[more >]**
drive-c:\passmark\email\pst\pst\Outlook.pst*00000002981706B94693848AA8543E2DAB32AA4A4FF2
Date: 06/06/2014, 10:51 AM Score: 26 Matched: 1

The Email Attachments View displays a list of attachment files that were found within e-mails. Double clicking on an e-mail opens the E-mail Viewer window.

Unallocated View



Unallocated cluster (disk iphone3g-1:) LCN Range: 63408 - 63411
... local string string string array FTPPassive integer integer string string Interface string string Hardware string apple string string apple string string apple string string Never string string apple string apple**[more >]**
Date: N/A Score: 75 Matched: 1

Unallocated cluster (disk SMI_USB_DISK_Media-0:) LCN Range: 26353 - 26354
... version encoding DOCTYPE plist Apple PLIST apple plist version resource array Attributes string string CFName string Protective Master string string string string Protective Master string Attributes **[more >]**
Date: N/A Score: 51 Matched: 1

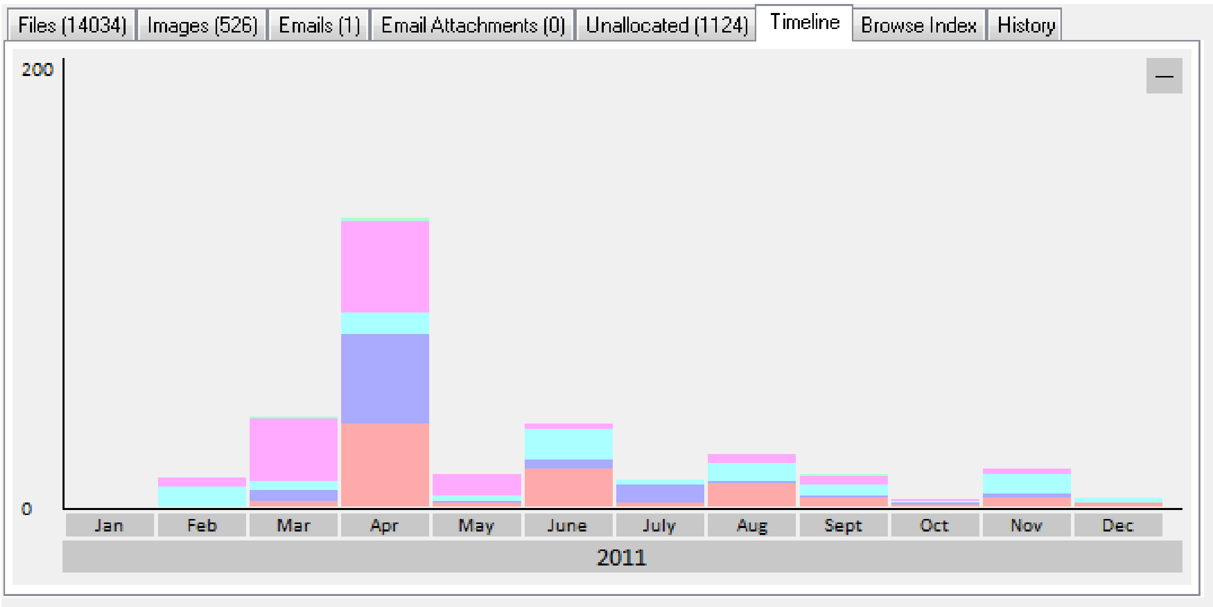
Unallocated cluster (disk macos-0:) LCN Range: 26353 - 26354
... version encoding DOCTYPE plist Apple PLIST apple plist version resource array Attributes string string CFName string Protective Master string string string string Protective Master string Attributes **[more >]**
Date: N/A Score: 51 Matched: 1

Unallocated cluster (disk SMI_USB_DISK_Media-0:) LCN Range: 26121 - 26127
... version encoding DOCTYPE plist Apple PLIST apple plist version string string policySearch integer integer plist ...
Date: N/A Score: 18 Matched: 1

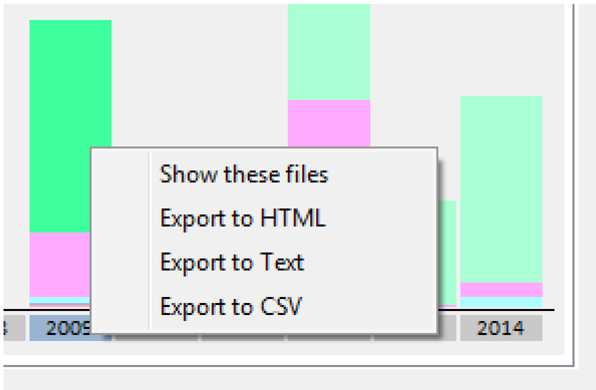
Unallocated cluster (disk macos-0:) LCN Range: 26121 - 26127
... version encoding DOCTYPE plist Apple PLIST apple plist version string string policySearch integer integer plist ...
Date: N/A Score: 18 Matched: 1

The Unallocated View displays a list of unallocated cluster (free clusters not allocated to any file) results. The results contain the LCN range, along with any contained text if applicable. Double clicking on a cluster range opens the Internal Viewer.

Timeline View



The Timeline View displays an interactive bar graph providing the user with a visual view of the distribution of the search results with respect to the modified dates of the files. The granularity of the scale can be adjusted by clicking on the bar graphs to zoom in or the '-' button on the top-right corner to zoom out. Right-clicking a bar section brings up the following menu:



Show these files
Filter the search results to show only those that belong to the selected time bar

Export to HTML
Export the results contained in the highlighted bar to HTML

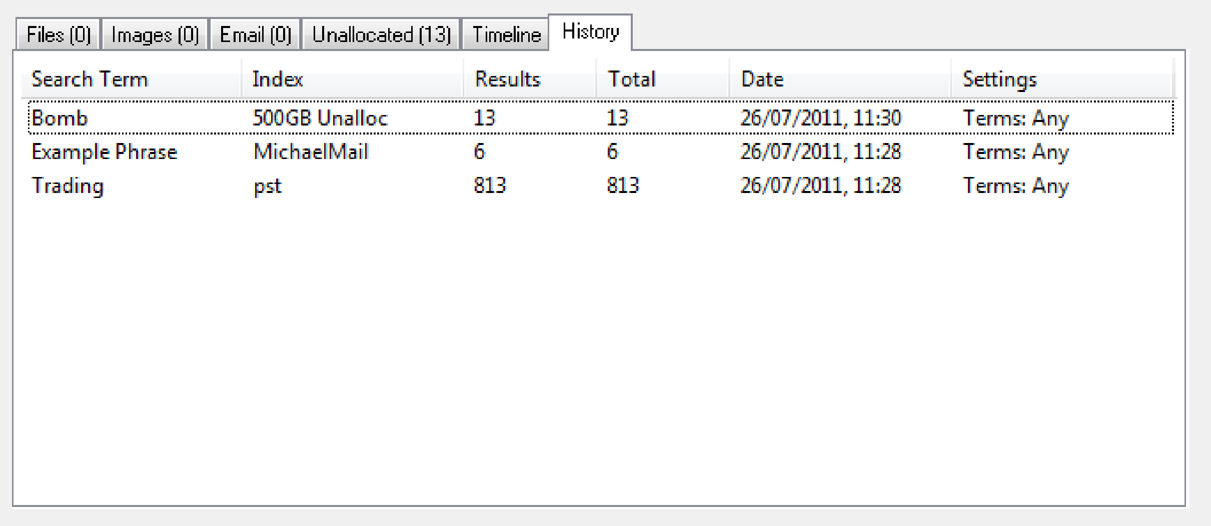
Export to Text
Export the results contained in the highlighted bar to text

Export to CSV
Export the results contained in the highlighted bar to CSV

Browse Index View

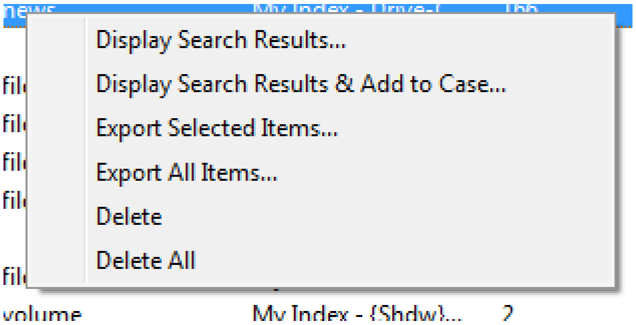
The Browse Index View shows the list of words, text and strings found when the index was created. For more information, see Browse Index.

History View



Search Term	Index	Results	Total	Date	Settings
Bomb	500GB Unalloc	13	13	26/07/2011, 11:30	Terms: Any
Example Phrase	MichaelMail	6	6	26/07/2011, 11:28	Terms: Any
Trading	pst	813	813	26/07/2011, 11:28	Terms: Any

The History View keeps a history of all index searches performed for the case. This allows previous searches to be logged so that they can be repeated if necessary. Loading previous search results from history is much faster than doing the searches again. Additionally, when the user performs a search using a Word List, the results are displayed in the History View. Right-clicking a previous search brings up the following menu:


Display Search Results...
Display Search Results & Add to Case...
Export Selected Items...
Export All Items...
Delete
Delete All

Display Search Results

Display the results of the selected previous search

Search For Selected Items & Add To Case

Display the results of the selected previous search(es), and add all files contained in the results to case

Export Selected Items...

Export the list of selected history items to a CSV file.

Export All Items...

Export the entire list of history items to a CSV file.

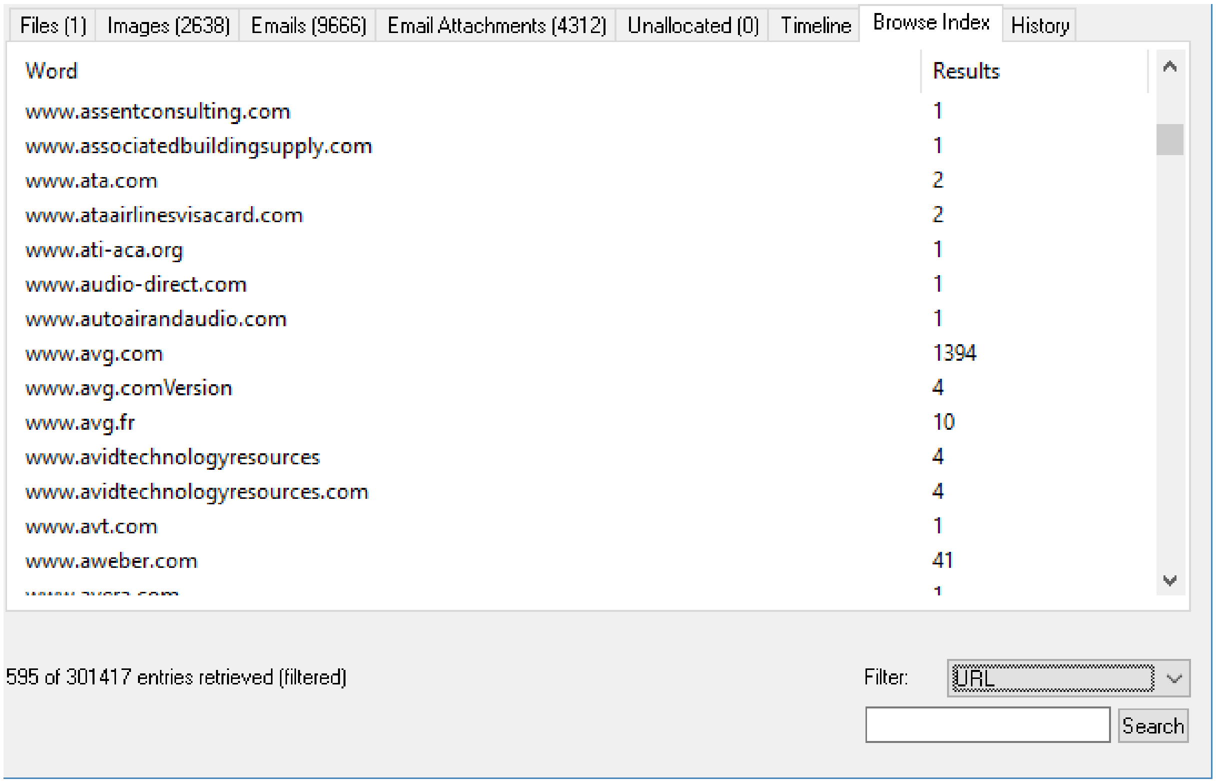
Delete

Delete the selected history item(s)

Delete All
Delete all history items in the list

4.3.2.3 Browse Index

The "Browse Index" tab allows the investigator to examine the actual index itself, which is a list of words, text and strings found when the index was created. It will list all the words in alphabetically ascending order. The main purpose of analyzing the index contents is to look for recognizable strings such as e-mail addresses, phone numbers, credit card numbers, IP addresses and more.



Word	Results
www.assentconsulting.com	1
www.associatedbuildingsupply.com	1
www.ata.com	2
www.ataairlinesvisacard.com	2
www.ati-aca.org	1
www.audio-direct.com	1
www.autoairandaudio.com	1
www.avg.com	1394
www.avg.comVersion	4
www.avg.fr	10
www.avidtechnologyresources	4
www.avidtechnologyresources.com	4
www.avt.com	1
www.aweber.com	41

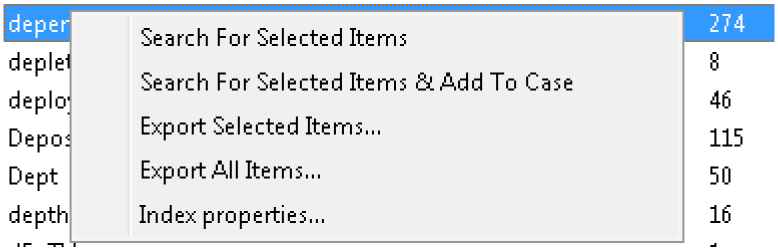
595 of 301417 entries retrieved (filtered)

Filter: URL

Usage

Right-click Menu

Right-clicking an index word opens the following context menu. Certain actions may or may not be available depending on the current results tab.



Search For Selected Items
Performs the search on the selected item(s) and save the results in History View.

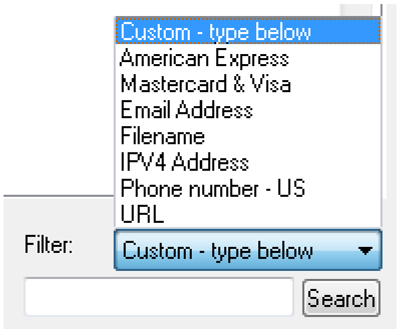
Search For Selected Items & Add To Case
Performs the search on the selected item(s), save the results in History View and add the results to case.

Export Selected Items...
Export the list of selected items to a CSV file.

Export All Items...
Export the entire list of words to a CSV file.

Index properties...
Shows the details of the index including number of files indexed, total size and number of unique words.

Filtering Index Strings



Regular expressions are used to filter the list of strings. There are several pre-configured regular expressions that can be selected in the Filter drop-down box. The user may also specify their own regular expressions in the search box.

Predefined Regular Expressions

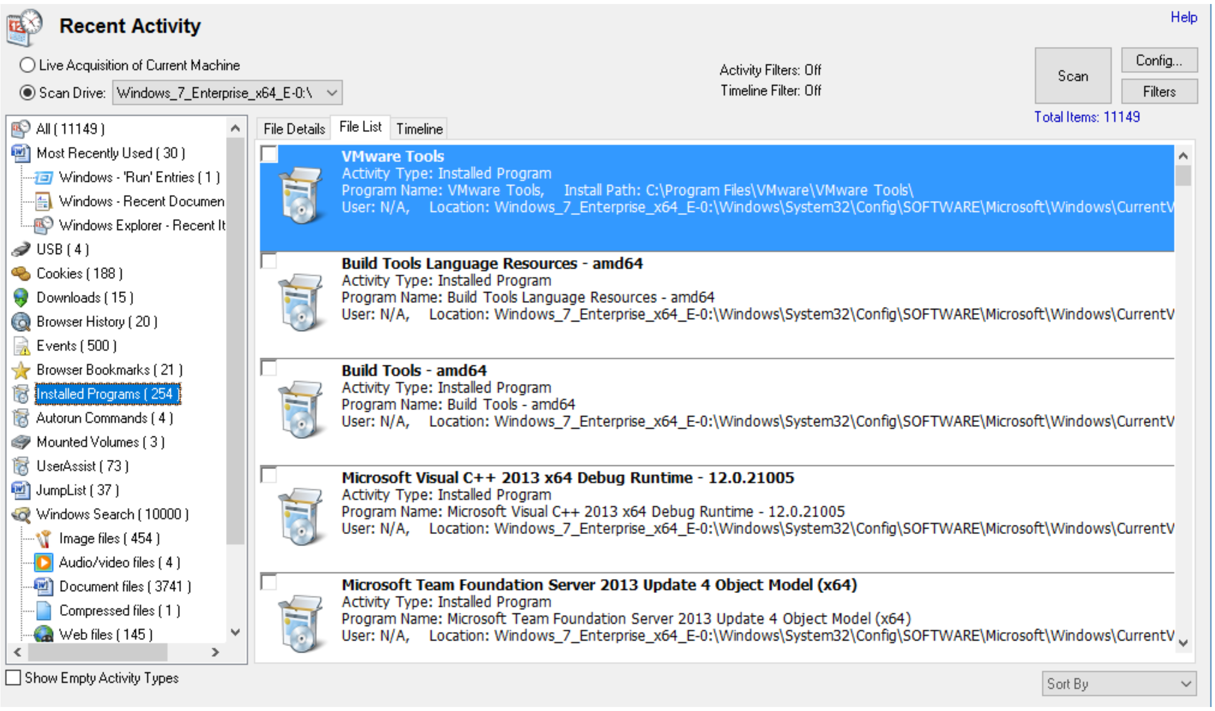
Predefined regular expressions can be selected using the drop-down box. The source of the actual regular expressions used can be found in the "RegularExpressions.txt" file in the OSForensics program data directory (ProgramData\PassMark\OSForensics). These have been collected from various sources and are kept as simple as possible while still returning fairly accurate results, please note these will not be 100% accurate in all situations.

User-Specified Regular Expressions

The investigator can specify their own regular expression pattern to filter the list of strings. For example, to search for any entry containing the word "test", select the Custom option from the drop down list, type "test" and then click the search button. To find only entries that begin with the word "test" use "^test", the "^" character is used to indicate the pattern match must start at the beginning of the found word. For a basic overview of regular expressions, see Regular Expressions.

4.4 Recent Activity

The Recent Activity module scans the system for evidence of recent activity, such as accessed websites, installed programs, USB drives, wireless networks, and recent downloads. This is especially useful for identifying trends and patterns of the user, and any material that had been accessed recently.



○ Live Acquisition of Current Machine
● Scan Drive: Windows_7_Enterprise_x64_E-0:\

Activity Filters: Off
Timeline Filter: Off

Total Items: 11149

☐ Show Empty Activity Types

VMware Tools
Activity Type: Installed Program
Program Name: VMware Tools, Install Path: C:\Program Files\VMware\VMware Tools\
User: N/A, Location: Windows_7_Enterprise_x64_E-0:\Windows\System32\Config\SOFTWARE\Microsoft\Windows\CurrentV

Build Tools Language Resources - amd64
Activity Type: Installed Program
Program Name: Build Tools Language Resources - amd64
User: N/A, Location: Windows_7_Enterprise_x64_E-0:\Windows\System32\Config\SOFTWARE\Microsoft\Windows\CurrentV

Build Tools - amd64
Activity Type: Installed Program
Program Name: Build Tools - amd64
User: N/A, Location: Windows_7_Enterprise_x64_E-0:\Windows\System32\Config\SOFTWARE\Microsoft\Windows\CurrentV

Microsoft Visual C++ 2013 x64 Debug Runtime - 12.0.21005
Activity Type: Installed Program
Program Name: Microsoft Visual C++ 2013 x64 Debug Runtime - 12.0.21005
User: N/A, Location: Windows_7_Enterprise_x64_E-0:\Windows\System32\Config\SOFTWARE\Microsoft\Windows\CurrentV

Microsoft Team Foundation Server 2013 Update 4 Object Model (x64)
Activity Type: Installed Program
Program Name: Microsoft Team Foundation Server 2013 Update 4 Object Model (x64)
User: N/A, Location: Windows_7_Enterprise_x64_E-0:\Windows\System32\Config\SOFTWARE\Microsoft\Windows\CurrentV

A scan for recent activity can be initiated by simply pressing the Scan button. The following settings are available to the user:

Live Acquisition of Current Machine
Recent activity is gathered from the currently running operating system.

Scan Drive
Gather the recent activity from a particular drive, useful when live acquisition are not possible and a drive image is being dealt with. This particular scan may not be able to gather as much information as a live acquisition. By default, OSForensics will search for known Windows directories to scan registry files. However, if you have some standalone registry files you can place them in the root directory of a drive (eg a USB thumb drive) and select this drive to be scanned.

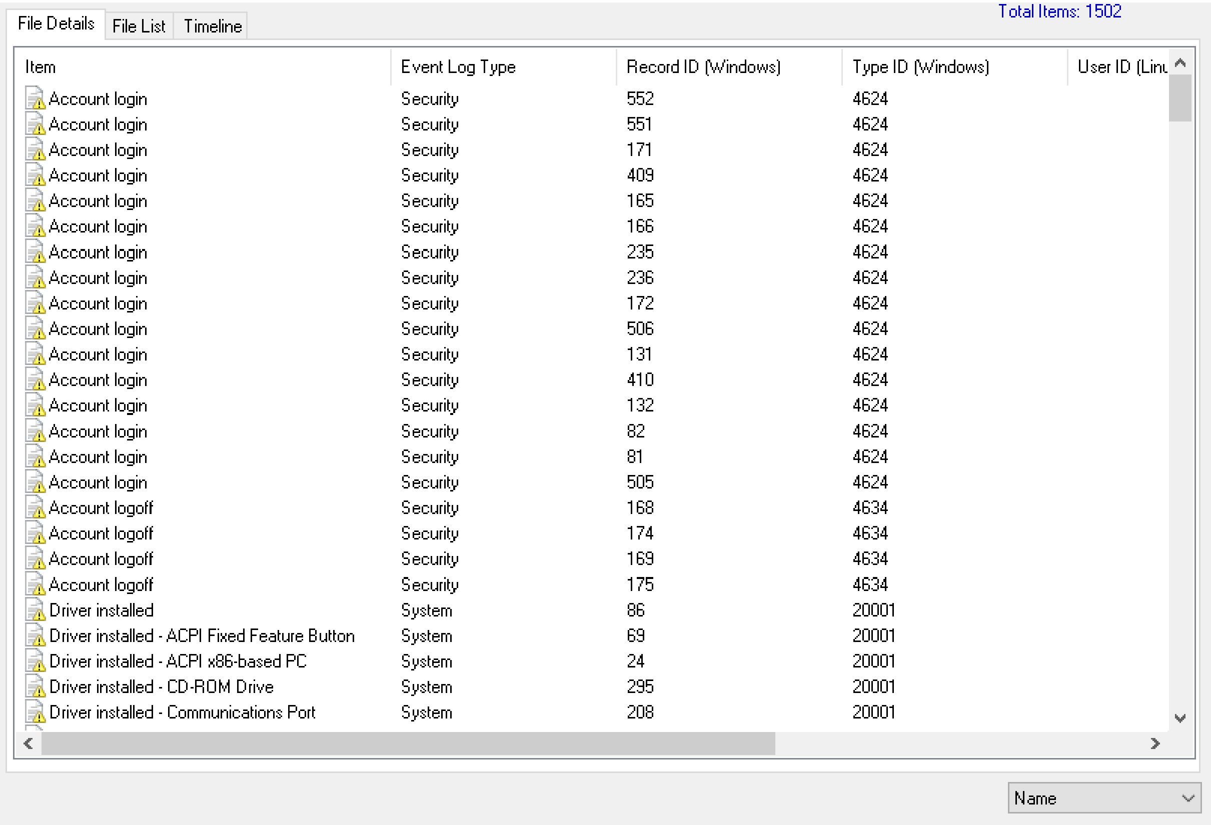
More Scan Options

By clicking the "Config..." button you will be taken to the Recent Activity Configuration window where more advanced options can be selected.

Activity Filters

By clicking the "Filter" button you will be taken to the Recent Activity Filters window where you can further refine what activity types are displayed.

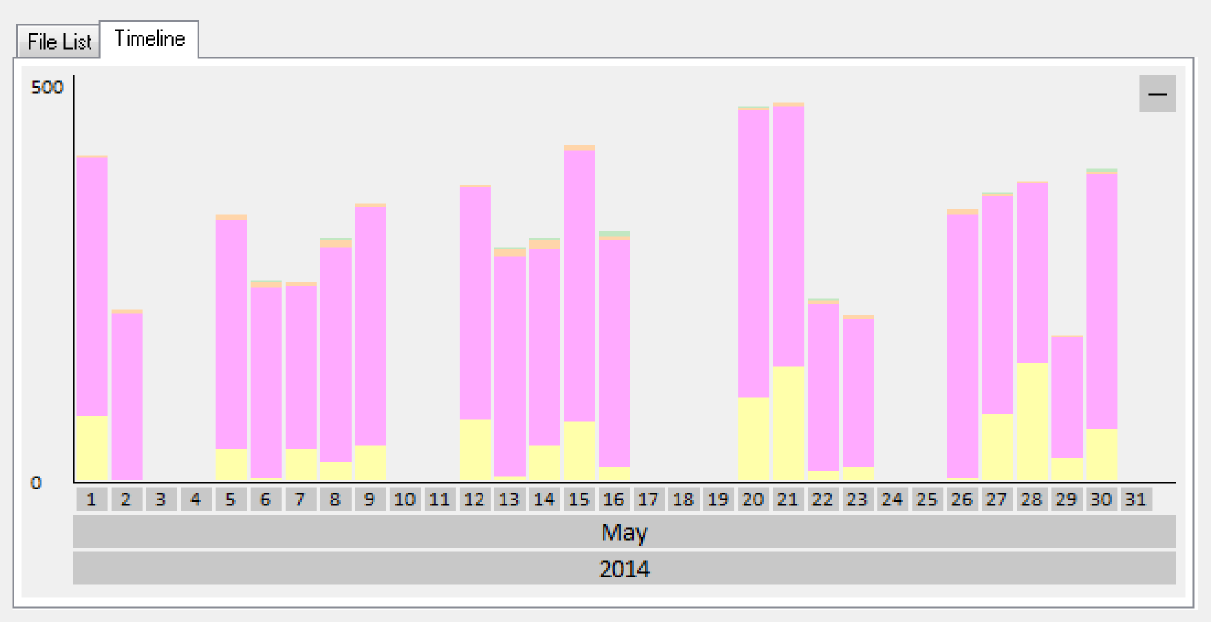
File Details View



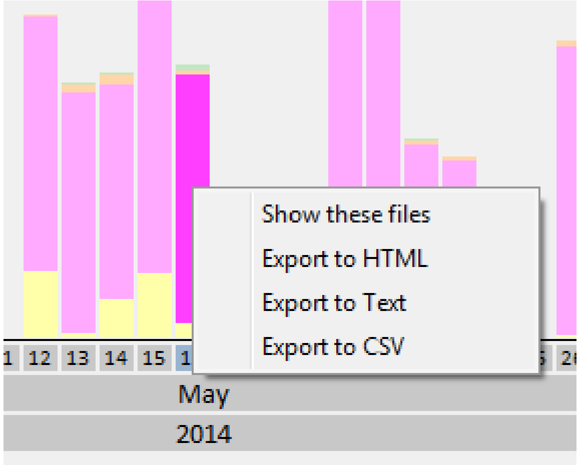
Item	Event Log Type	Record ID (Windows)	Type ID (Windows)	User ID (Linu
Account login	Security	552	4624	
Account login	Security	551	4624	
Account login	Security	171	4624	
Account login	Security	409	4624	
Account login	Security	165	4624	
Account login	Security	166	4624	
Account login	Security	235	4624	
Account login	Security	236	4624	
Account login	Security	172	4624	
Account login	Security	506	4624	
Account login	Security	131	4624	
Account login	Security	410	4624	
Account login	Security	132	4624	
Account login	Security	82	4624	
Account login	Security	81	4624	
Account login	Security	505	4624	
Account logoff	Security	168	4634	
Account logoff	Security	174	4634	
Account logoff	Security	169	4634	
Account logoff	Security	175	4634	
Driver installed	System	86	20001	
Driver installed - ACPI Fixed Feature Button	System	69	20001	
Driver installed - ACPI x86-based PC	System	24	20001	
Driver installed - CD-ROM Drive	System	295	20001	
Driver installed - Communications Port	System	208	20001	

The File Details View displays the same recent activity of the system as the File List View except presented in a table format. This view is useful for quickly identifying, locating and sorting activities of interest. Each entry is coded by the type of activity and can be identified by the icon displayed at the beginning of the row.

Timeline View



The Timeline View displays an interactive bar graph providing the user with a time-based view of recent activity on the system. This view is useful for identifying trends where significant activity has occurred. Each bar is colour-coded by the type of activity. Right-clicking a bar sections brings up the following menu:



Show these files
Filter the results according to the corresponding activity type and date/time

Export to HTML
Export the results contained in the highlighted bar to HTML

Export to Text
Export the results contained in the highlighted bar to text

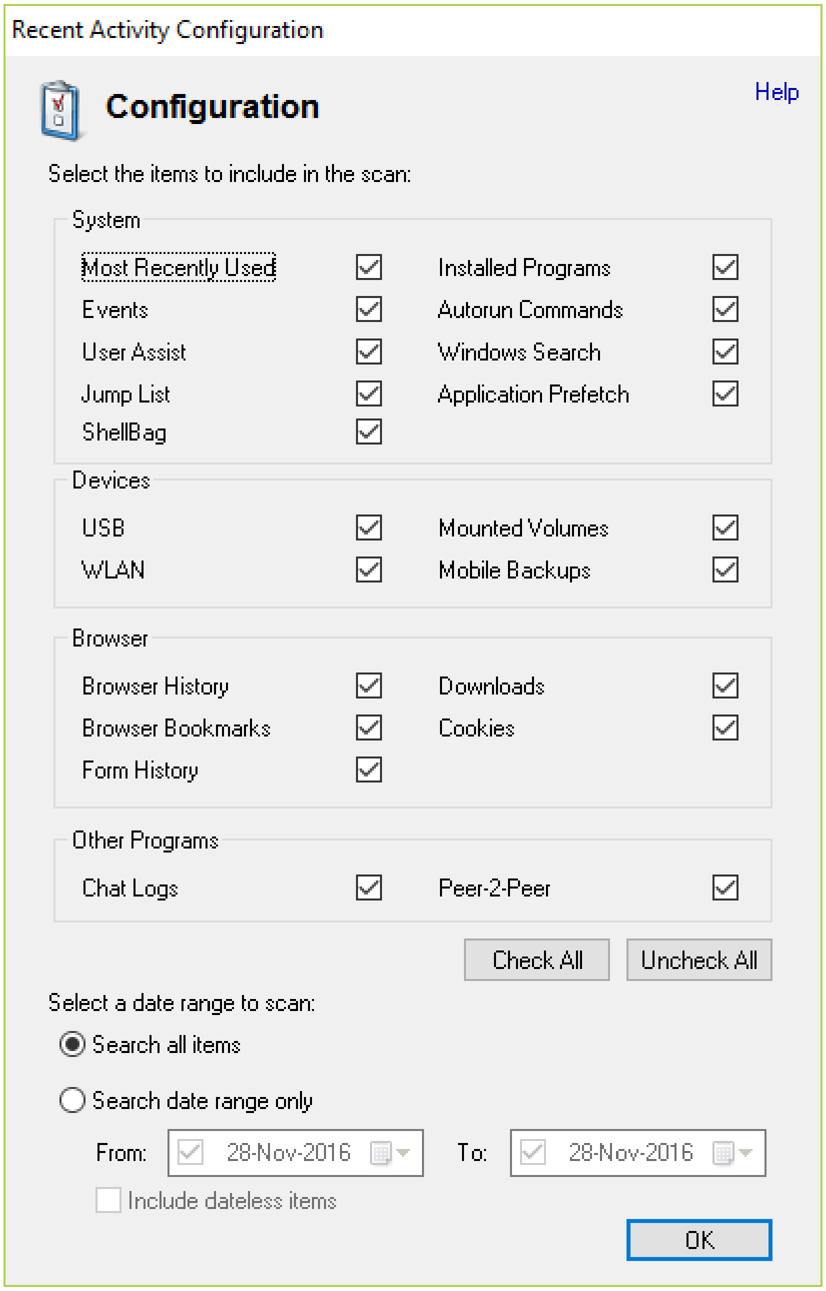
Export to CSV
Export the results contained in the highlighted bar to CSV

Additional Information

See the following pages for more detailed information about the specifics of some of the data gathering.
Web Browser Activity
Registry Activity
Windows Event Log
Windows Jump Lists
Windows Search
Chat Logs
Peer-2-Peer
Windows Prefetch
OSX Activity

4.4.1 Recent Activity Configuration

The Recent Activity Configuration Window allows the user to configure the Recent Activity scan options. This window can be accessed by clicking on the "Config..." button in the main Recent Activity window.



Recent Activity Configuration

Configuration

Select the items to include in the scan:

System

Most Recently Used	☑	Installed Programs	☑
Events	☑	Autorun Commands	☑
User Assist	☑	Windows Search	☑
Jump List	☑	Application Prefetch	☑
ShellBag	☑		

Devices

USB	☑	Mounted Volumes	☑
WLAN	☑	Mobile Backups	☑

Browser

Browser History	☑	Downloads	☑
Browser Bookmarks	☑	Cookies	☑
Form History	☑		

Other Programs

Chat Logs	☑	Peer-2-Peer	☑

Select a date range to scan:

● Search all items

○ Search date range only

From: ☑ 28-Nov-2016 To: ☑ 28-Nov-2016

□ Include dateless items

Most Recently Used (MRU)
If checked, enables scanning for Most Recently Used (MRU) items. See Registry Activity for details about MRU.

Events
If checked, enables scanning for event logs from the operating system . See Windows Event Log for details about Windows events.

UserAssist
If checked, enables scanning for UserAssist items. See Registry Activity for details about UserAssist.

Jump List

If checked, enables scanning for Jump List items. See Windows Jump List for more details.

Installed Programs
If checked, enables scanning for programs installed on the operating system. See Registry Activity for details about installed programs.

Autorun Commands
If checked, enables scanning for Autorun commands. See Registry Activity for details about Autorun commands.

Windows Search
If checked, enables scanning for items in the Windows Search database. See Windows Search for more details

Application Prefetch
If checked, enables scanning for Prefetch information. See Prefetch Viewer for details about information stored by the Prefetcher .

USB
If checked, enables scanning for USB devices that have been connected to the system. See Registry Activity for details about connected USB devices.

WLAN
If checked, enables scanning for wireless networks that the computed has connected to. See Registry Activity for details about wireless connections.

Mounted Volumes
If checked, enables scanning for volumes that have been mounted by the operating system. See Registry Activity for details about mounted volumes.

Mobile Backups
If checked, enables scanning for iOS backups that may have been stored on the system.

Browser History
If checked, enables scanning for browser URL history. See Web Browser Activity for details about supported web browsers.

Browser Bookmarks
If checked, enables scanning for browser bookmarks. See Web Browser Activity for details about supported web browsers.

Form History
If checked, enables scanning for browser form history. See Web Browser Activity for details about supported web browsers.

Downloads
If checked, enables scanning for files downloaded via the browser . See Web Browser Activity for details about supported web browsers.

Cookies
If checked, enables scanning for cookies stored by the browser . See Web Browser Activity for details about supported web browsers.

Chat Logs

If checked, enables scanning for chat logs from MSN Messenger, AIM, Yahoo Messenger, ICQ, Skype, Miranda IM, and Pidgin.

Peer-2-Peer
If checked, enables scanning for artifacts from BitTorrent/uTorrent resume.dat file and .torrent files in the user's download folder. Artifacts from Ares Galaxy ShareH.dat file are retrieved. Emule known.met, server.met, StoredSearches.met and cancelled.met files. Will look for files with .nzb extension in the download folder along with installation of popular Usenet program SABnzbd. Also, registry search information from Shareaza. Additional results may be obtained from running the Peer-2-Peer preset from File Name Search.

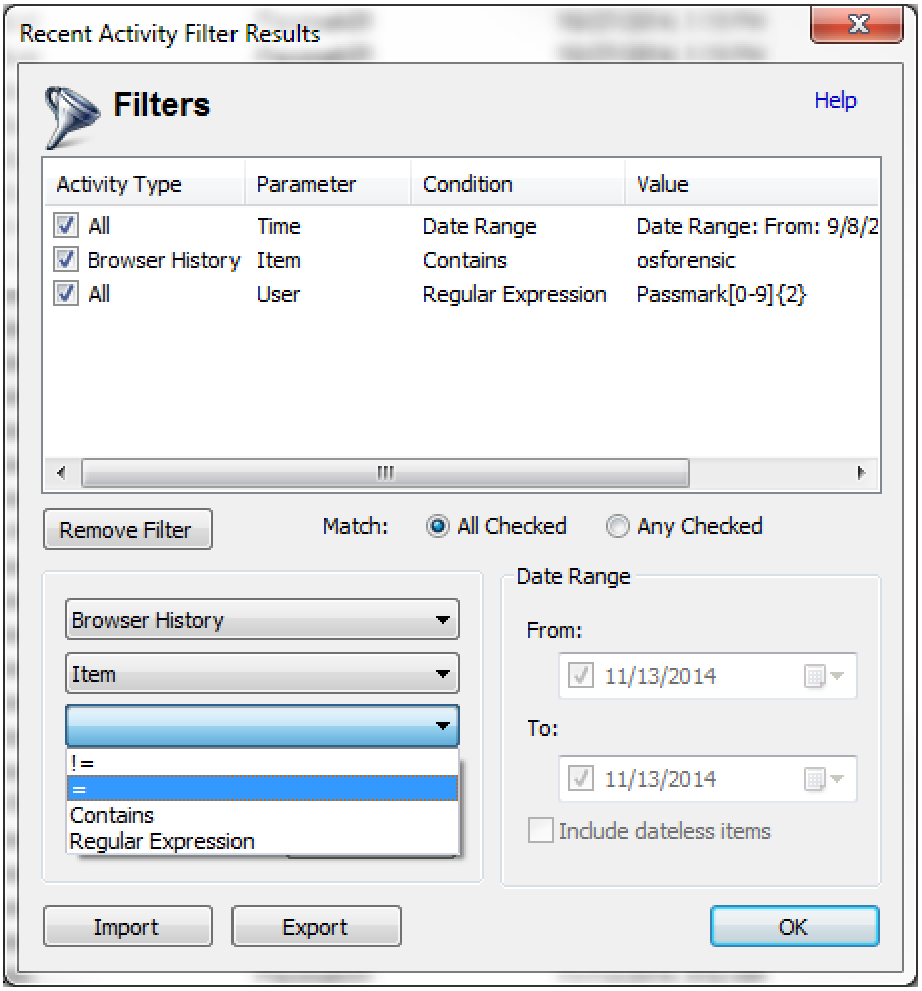
Search all items
Searches all items for recent activity.

Search date ranges only
Allows the user to specify a particular access date range for the search results.

Include dateless items
If checked, will include items without an access date.

4.4.2 Recent Activity Filters

The Recent Activity Filters Window allows the user to add filters to narrow down the results from a Recent Activity scan. This window can be accessed by clicking on the "Filters" button in the main Recent Activity window.



Activity Type	Parameter	Condition	Value
☑ All	Time	Date Range	Date Range: From: 9/8/2
☑ Browser History	Item	Contains	osforensic
☑ All	User	Regular Expression	Passmark[0-9]{2}

Match: ● All Checked ○ Any Checked

Browser History

Item

Date Range

From: ☑ 11/13/2014

To: ☑ 11/13/2014

□ Include dateless items

The top list will show which filters have been added and which are enabled. Filters with the check mark will be **enabled**. To temporarily disable a filter you can uncheck the item in the list. To no longer have the filter available, you can use the **Remove Filter** button.

About Filters
There are two types of filters: one that affects all activity types and ones that are activity type specific. If the "Activity Type" is set to "All", it will be applied to all activities. If the filter is set to a specific type, e.g. "Browser History", then the filter will only be used to filter those activity types.

Match:
If set to "All Checked", then for the activity to be displayed in the list it must match every enabled "All" filters and every enabled activity specific filters for its type. If set to "Any Checked" then for the activity to be displayed in the list it must match at least one of the enabled "All" filters or one of the enabled activity specific filters for its type.

Import & Export
These buttons let you save and load existing filters for future use.

Adding Filters

There are three drop down boxes.The top dropdown box is for the Activity Type and will contain the available activity type filters and an All type. The second dropdown box is the Parameter to filter for that activity. The third dropdown is the condition upon which to match. Depending on your selection, the

Parameter and Condition dropdowns will be auto-populated to aid you in adding filter. Depending on the Parameter type you will be given different conditions to use. Parameter types are:

	Equal (=)	Not Equal (!=)	Less Than (<)	Less Than or Equal (<=)	Greater Than (>)	Greater Than or Equal (>=)	Contains	Regular Expression	Date Range
Text	Yes	Yes	No	No	No	No	Yes	Yes	No
Number	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No
Date	Yes	Yes	No	No	No	No	No	No	Yes
User	Yes	Yes	No	No	No	No	No	Yes	No
Choice	Yes	Yes	No	No	No	No	No	No	No
Filesize	No	No	Yes	Yes	Yes	Yes	No	No	No

Equal - For text, the string must match exactly (case insensitive). For Number the number must match exactly. For Date, the day must match. For Choice the selected choice must equal.
Not Equal - See "Equal" above, except in this case it must not match.
Less Than - For number and file size, must be less than this number or size.
Less Than or Equal - For number and file size, must be less than or equal to this number or size.
Greater Than - For number and file size, must be greater than this number or size.
Greater Than or Equal - For number and file size, must be greater than or equal to this number or size.
Contains - For text only. The text must contain this string (case insensitive).
Regular Expression - Case insensitive. See Regular Expressions for more details.
Date Range - Date must be within these dates. If "Include dateless items" is checked, then any activity without a proper date will be a match.

4.4.3 Web Browser Activity

OSForensics scans known locations for web browser profiles and their related history and cache files to detect cookies, bookmarks, visited URL history, downloads, form history and saved login and password form fields where available.

Below is a table that shows which features are supported for web browsers and their different versions.

Browser	Versions	URL History	Cookies	Downloads	Form History
Chrome	8+	Yes	Yes	Yes	Yes
Internet Explorer	6	Yes	Yes	No	No
Internet Explorer	7,8,9,10+	Yes	Yes	No	No
FireFox	2	Yes	Yes	Yes	No
FireFox	3,4+	Yes	Yes	Yes	Yes
Safari	4	Yes	Yes	Yes	No
Opera	20+	Yes	Yes	Yes	Yes
Opera	10	Yes	Yes	No	No
Opera	9	Yes	Yes	No	No

4.4.4 Registry Activity

By default OSForensics will search for known Windows directories to scan for registry files, however if you have some standalone registry files you can place them in the root directory of a drive (eg a USB thumb drive at G:) and select this drive to be scanned. OSForensics will scan the following registry files for recent activity:

- SOFTWARE
- SYSTEM
- NTUSER.dat

Most Recently Used Lists (MRU)

OSForensics checks several known registry locations that store MRU data, this includes locations for Microsoft Office, Microsoft Wordpad, Microsoft Paint, Microsoft Media Player, Windows search, recent documents, connected network drives and the Windows Run command. In addition, OSF will also check the user's Recent Items directory. The Recent Items access is very useful to view the recently opened files from a local computer or network location. [1]

AutoRun Entrires

Programs that are run automatically when Windows starts or a user log in are retrieved from the registry,

Mounted Volumes

Volume IDs are collected from the system registry and matched to the and drive letters they were associated with.

Installed Programs

Programs that have been installed are retrieved from the system and user registry files

Connected USB devices

USB devices that have been connected to the computer, this includes USB memory sticks, portable hard drives and other external USB devices like CD-Rom drives. A manufacturer name, product ID, serial number and the last connection date should be displayed for each device.

Wireless Network Connections (WLAN)

The MAC address of any wireless networks connected to using the Windows Zero Config service (default Windows wireless connection manager) **(Windows XP only). On Vista and newer** the registry and known locations on disk are checked for XML profiles of networks. The Creation/Modified dates represent the file times of the XML profile, or if it was purely a registry entry the last key write time.

UserAssist Entrys

The UserAssist key from the regsitry contains programs and links that are opened frequently.

Shellbag entries

Shellbag entries are recovered from the user specific registry files NTUSER.DAT and USRCLASS.DAT. OSForensics will attempt to recover dates and names of items where available. Currently more information will be exported into CSV format than is displayed due to screen limitations. Items that are identified only by a GUID will attempt to be named using a lookup list with the GUID appended to the name in '{ }'.

[1] The Recent Items folder (previously called Recent Documents in Windows XP) is used by Windows to record what documents have been opened (the default location is typically is "C:\Users\%UserName%

\AppData\Roaming\Microsoft\Windows\Recent"). The files in this directory are actually shortcut (.lnk) files. As these are shortcuts, they may no longer work if the file have been moved or deleted since it was originally created. Also of note, is when using "Scan Drive" option and choosing an added OSForensics' device, links may point to local and network locations that may not be available on the current machine.

4.4.5 Windows Event Log

OSForensics will scan the Windows logs for the following events;

Security Log Events

- 4624 - Account login
- 4625 - Failed login attempt
- 4634 - Account logoff
- 4723 - Password change attempted
- 4724 - Password reset attempted
- 4740 - User account locked
- 4767 - User account unlocked

System Log Events

- 19 - Windows update success
- 20 - Windows update failure
- 1074 - Shutdown
- 6009 - System boot
- 20001 - Driver installed

Application Log Events

- 11707 - Product installed
- 11708 - Product install failed

The feature can only be used when running **Windows Vista** or **Windows 7**.

4.4.6 Windows Jump Lists

Jumps lists are a feature introduced to Windows 7 that allow fast access to programs and favorites as well as functioning as a most recently used list for some programs (see the Micorosoft page on jump lists for more information on how they function.

Jump lists come in two formats, automatic which are created by Windows and custom which are created when a user interacts with the program such as pinning an item to the list. OSForensics is currently retrieving information from the "Destlist" section of the automatic jump lists and all the entries from the custom jump lists.

The information presented by OSForensics includes;

- filename, path and any command line arguments stored (where available)
- system name (where available)
- the item ID (where the item appears in the jump list file
- last access date
- location of jumplist file item was retrieved from

4.4.7 Shellbag

Shellbag entries keep a record of size, position, icon and views of a folder when accessed via Windows Explorer. This information can be used to see what folders have been accessed in Explorer.

The information presented by OSForensics includes;
- Folder name and disk path
- Location in the registry file (registry bag path) entry was retrieved from
- last access date of folder
- creation and modified date for the entry in the registry file

4.4.8 Windows Search

Windows Search is a desktop indexer that has been integrated and enabled by default in Windows operating systems since Vista. Windows (Desktop) Search can also be optionally installed on Windows XP and Windows 2003. During its normal operating, Window Search runs in the background, creating a full-text index of the files on the computer. This index allows for fast searching of filenames and file contents matching the specified search term.

In a forensics point of view, the index database can contain valuable artifacts that an be useful for mapping user activity during any given time frame. In particular, a forensics investigator can obtain valuable forensics information from the analysis of the index database, such as:

- File activity at any given point in time (such as installed programs and modified documents)
- Files contained in disks that are damaged or no longer exist (such as external disks)
- Plain text data from indexed files such as documents and e-mails
- Plain text data from encrypted files

Because Windows Search is enabled by default, the index database acts as a digital footprint of the system activity. The typical user is likely to be unaware of the indexing operation taking place in the background.

4.4.9 Chat Logs

OSForensics will search for chat logs from these programs:

- Microsoft Chat
- AIM
- Yahoo
- ICQ
- Skype
- Miranda
- Pidgin

4.4.10 Peer-2-Peer

OSForensics will search for Peer-2-Peer artifacts from these programs:

- BitTorrent
- Ares
- EMule
- Usenet
- Shareaza

4.4.11 Prefetch Items

The Prefetcher is an operating system component that improves the performance of the system by pre-caching applications and its associated files into RAM, reducing disk access. In order to determine the applications that are used most frequently, the Prefetcher collects application usage details such as the number of times the application has been executed, the last run time, and any files that the application uses when it is running.

In a forensics point of view, application usage patterns (eg. "Cleaner" software used recently) and files that have been opened (eg. documents) recently can be uncovered.

4.4.12 OSX Activity

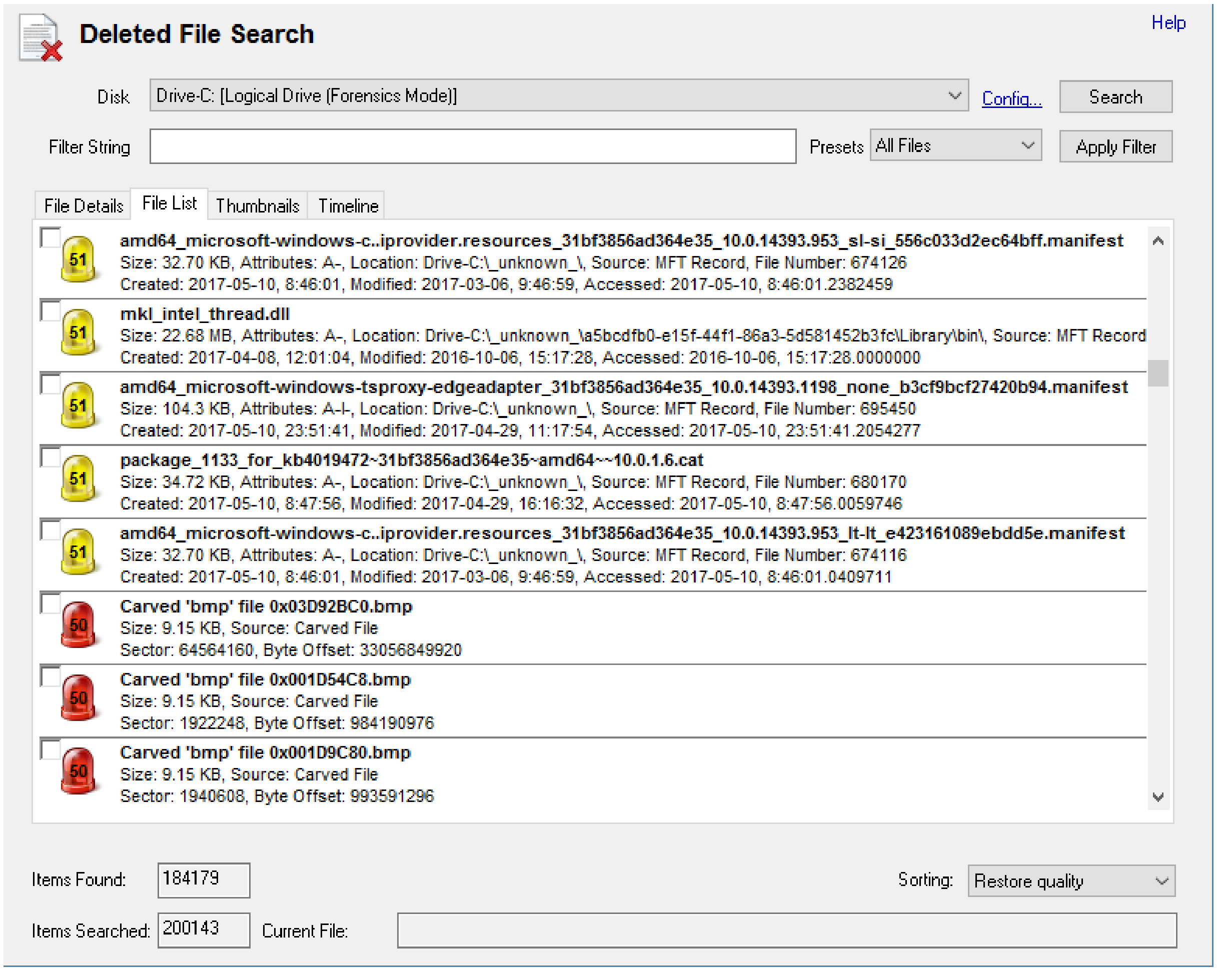
OSForensics Recent Activity module will scan for OSX specific artifacts if it detects that the drive to be searched is formatted as a HFS file-system.

Most Recently Used - Search for recent items,documents, media and network connection in various property list (.plist) files.
Installed Programs - List the applications found in the Applications directory and sub-directories.
AutoRun - Search for log in activity items.
Events - Parse logs for Shutdown and CD/DVD disc burning events.
USB - List connection of iOS devices.
Mounted Volumes
WiFi - Show previous connections WiFi.
Mobile Backups - List backups from iOS devices.

In addition to the OSX specific artifacts, browser artifacts from Safari, Chrome and Firefox are searched for. Including History, Bookmark, Download and Cookie data.

4.5 Deleted Files Search

The Deleted Files Search Module can be used to recover files deleted from the file system (ie. deleted file no longer in recycling bin). This is especially useful for recovering files that the user may have attempted to destroy.



Disk: Drive-C: [Logical Drive (Forensics Mode)]

Filter String:

Presets: All Files

51 **amd64_microsoft-windows-c..iprovider.resources_31bf3856ad364e35_10.0.14393.953_sl-si_556c033d2ec64bff.manifest**
Size: 32.70 KB, Attributes: A-, Location: Drive-C:_unknown_\, Source: MFT Record, File Number: 674126
Created: 2017-05-10, 8:46:01, Modified: 2017-03-06, 9:46:59, Accessed: 2017-05-10, 8:46:01.2382459

51 **mkl_intel_thread.dll**
Size: 22.68 MB, Attributes: A-, Location: Drive-C:_unknown_\a5bcdfb0-e15f-44f1-86a3-5d581452b3fc\Library\bin\, Source: MFT Record
Created: 2017-04-08, 12:01:04, Modified: 2016-10-06, 15:17:28, Accessed: 2016-10-06, 15:17:28.0000000

51 **amd64_microsoft-windows-tsproxy-edgeadapter_31bf3856ad364e35_10.0.14393.1198_none_b3cf9bcf27420b94.manifest**
Size: 104.3 KB, Attributes: A-I-, Location: Drive-C:_unknown_\, Source: MFT Record, File Number: 695450
Created: 2017-05-10, 23:51:41, Modified: 2017-04-29, 11:17:54, Accessed: 2017-05-10, 23:51:41.2054277

51 **package_1133_for_kb4019472~31bf3856ad364e35~amd64~~10.0.1.6.cat**
Size: 34.72 KB, Attributes: A-, Location: Drive-C:_unknown_\, Source: MFT Record, File Number: 680170
Created: 2017-05-10, 8:47:56, Modified: 2017-04-29, 16:16:32, Accessed: 2017-05-10, 8:47:56.0059746

51 **amd64_microsoft-windows-c..iprovider.resources_31bf3856ad364e35_10.0.14393.953_lt-lt_e423161089ebdd5e.manifest**
Size: 32.70 KB, Attributes: A-, Location: Drive-C:_unknown_\, Source: MFT Record, File Number: 674116
Created: 2017-05-10, 8:46:01, Modified: 2017-03-06, 9:46:59, Accessed: 2017-05-10, 8:46:01.0409711

50 **Carved 'bmp' file 0x03D92BC0.bmp**
Size: 9.15 KB, Source: Carved File
Sector: 64564160, Byte Offset: 33056849920

50 **Carved 'bmp' file 0x001D54C8.bmp**
Size: 9.15 KB, Source: Carved File
Sector: 1922248, Byte Offset: 984190976

50 **Carved 'bmp' file 0x001D9C80.bmp**
Size: 9.15 KB, Source: Carved File
Sector: 1940608, Byte Offset: 993591296

Items Found: 184179

Sorting: Restore quality

Items Searched: 200143

Current File:

Basic Usage

A basic deleted file search simply involves entering a search string and selecting a physical disk. OSForensics will scan through the selected disk for traces of deleted files that contain the search string within their name. The basic search is case insensitive.

Presets
You can select one of the preset search options to quickly locate image files or office documents.

Multiple Searches
To run multiple different searches at once by separating the terms with the ';' character.

Wildcards
You can use '*' or '?' as wildcards within the search string.

'*' represents any number of characters
'?' represents a single character

If a wildcard is entered anywhere in the search field, wildcard matching is enabled on all search terms. When wildcard matching is enabled, you will need to explicitly add '*' to the start and end of the search term if you are trying match a word that may appear in the middle of a filename. '*' to the start and end of the term if you are trying match a word that may appear in the middle of a filename.

More Advanced Options

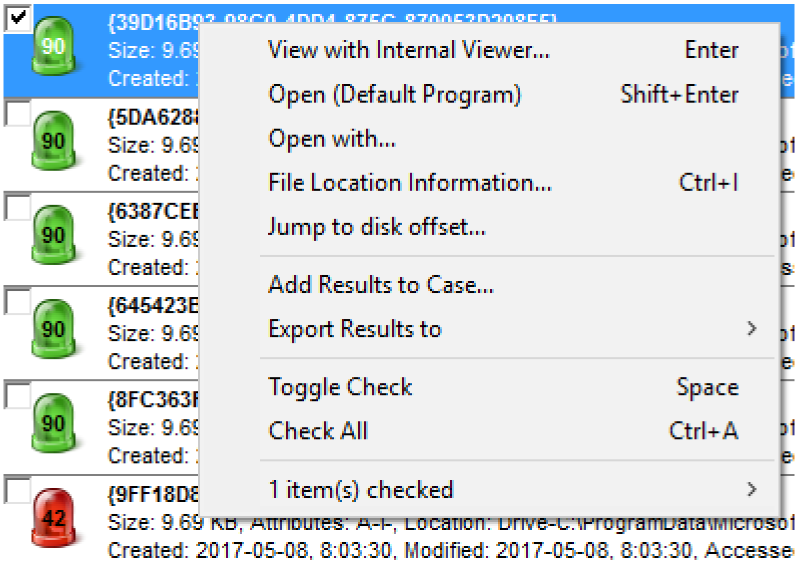
By clicking the "Config..." button you will be taken to the Deleted Files Search Configuration window where more advanced options can be selected.

Results

The results of the search are displayed in one of several views, along with a summary of the number of items searched/found. The File List view contains a list of file names, along with the corresponding metadata and a quality indicator between 0-100. A value close to 100 means that the deleted file is largely in tact, with only a few missing clusters of data. The results are sorted according to the criteria selected in the Sorting combo box.

Naming Convention for Carved Files
For carved files, the naming convention is as follows: "Carved '**[type]**' file **[sector location in HEX]**.**[extension]**" e.g. "Carved 'jpg' file 0x0003FA22.jpg".

Right-Click Menu
Right-clicking a deleted file will open a context menu of options available on the selected file. Not all options may be available for carved files.


View with Internal Viewer... Enter
Open (Default Program) Shift+Enter
Open with...
File Location Information... Ctrl+I
Jump to disk offset...
Add Results to Case...
Export Results to
Toggle Check Space
Check All Ctrl+A
1 item(s) checked
90
90
90
90
90
42
Size: 9.69 KB, Attributes: A-I-, Location: Drive-C:\ProgramData\Microsof
Created: 2017-05-08, 8:03:30, Modified: 2017-05-08, 8:03:30, Accesse

View with Internal Viewer
Opens the deleted file with OSForensics Viewer to perform a more thorough analysis

Open (Default Program)
Open the deleted file with the default program

Open With
Allows the user to select the program to open the deleted file

File Location Information
Opens a graphical display of the location of the file clusters on the physical disk.

Jump to disk offset...
Opens the Raw Disk Viewer tab and jumps to the first cluster of the selected deleted file

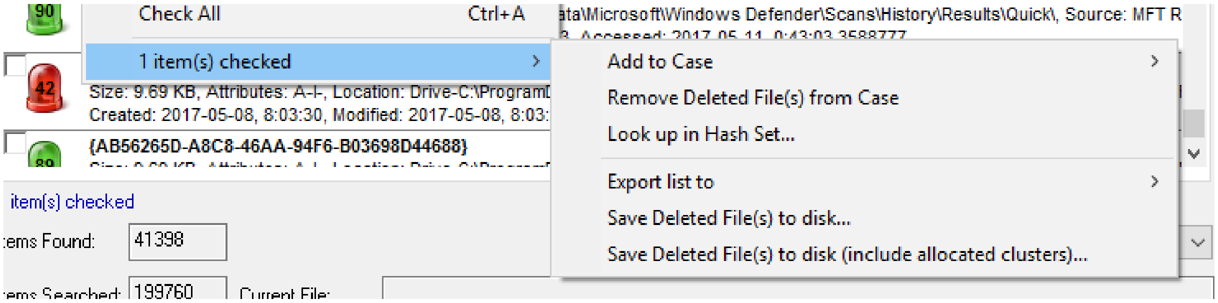
Add Results to Case
Add the list of the deleted files results to the case as an HTML or CSV file

Export Results to
Export the list of the deleted files results and associated attributes to a TXT, CSV or HTML file

Toggle Check
Toggle the check state of the current item

Check All
Check all the items in the list.

Right-click Sub-menu options
Additional sub-menu can be accessed when selecting the "item(s) checked" menu option.


90
Check All Ctrl+A
ata\Microsoft\Windows Defender\Scans\History\Results\Quick\, Source: MFT R
1 item(s) checked
42
Size: 9.69 KB, Attributes: A-I-, Location: Drive-C:\ProgramI
Created: 2017-05-08, 8:03:30, Modified: 2017-05-08, 8:03:
{AB56265D-A8C8-46AA-94F6-B03698D44688}
item(s) checked
Items Found: 41398
Items Searched: 199760 Current File:
Add to Case
Remove Deleted File(s) from Case
Look up in Hash Set...
Export list to
Save Deleted File(s) to disk...
Save Deleted File(s) to disk (include allocated clusters)...

Right-click selected items sub menu

Add to Case
Add the checked deleted file(s) or the list of selected item(s) to the case.

Remove Deleted Files(s) from Case
Remove the checked deleted file(s) from the case

Look up in Hash Set
Verify whether the checked deleted file(s) are contained in a hash set in the active database. See Hash Set Lookup.

Export List to
Export the checked deleted files and associated attributes to a TXT, CSV or HTML file

Save Deleted Files(s) to disk
Save the checked deleted files to disk. For clusters that have been allocated to another file, zeroes shall be written to the file

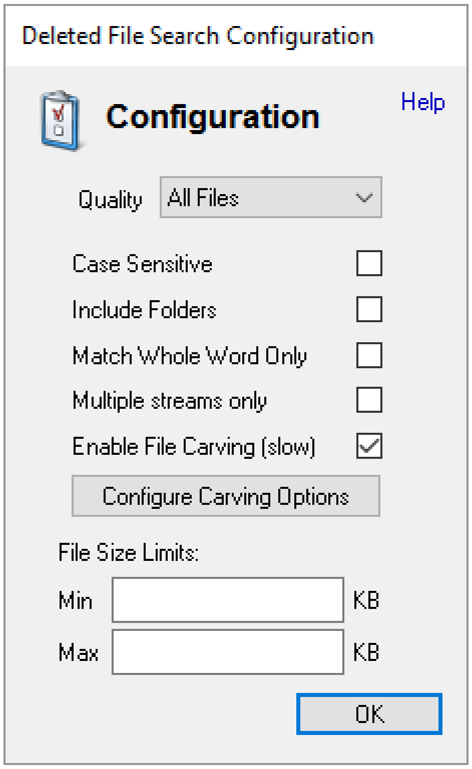
Save Deleted Files(s) to disk (include allocated clusters)
Save the checked deleted files to disk, including clusters that have been allocated to another file

For best results

- For best results in recovering a deleted file, it is important that as little file activity occurs on the disk in question (like creating or changing files) as possible. Ideally no changes would be made. These changes could overwrite file information or file content.
- Consider taking an image of the disk in question as soon as possible
- Recovered files should be saved to a different drive as recovery to the same drive may overwrite some file information.
- Consider running OSForensics from a USB drive. This allows the use of the software without installation on the system hence reducing the likelihood of file system changes.
- Consider switching off power to your system after file deletion occurs, mounting the drive on a second system and then recovering files using the second system. This approach will minimize the likelihood of files being written to the disk you are recovering from.
- Disk image files and physical disks should be mounted in read only mode, where possible, to avoid any overwriting of data by the operating system or other applications.

4.5.1 Deleted Files Search Configuration

The Deleted Files Search Configuration Window allows users to configure the search settings for deleted files. This window can be accessed by clicking on the "Config..." button in the main Deleted Files Search window.



Deleted File Search Configuration

Configuration

Help

Quality: All Files

Case Sensitive ☐

Include Folders ☐

Match Whole Word Only ☐

Multiple streams only ☐

Enable File Carving (slow) ☑

File Size Limits:

Min: KB

Max: KB

Quality
Determines the minimum quality level of the deleted file to include in the search results.

Case Sensitive
If checked, searches will be case sensitive. This option is disabled by default.

Include Folders

If checked, folder names will also be included in searches, not just filenames. This option is disabled by default.

Match Whole Word Only
If checked, results only include whether the search string is matched as a discreet word in the file name. In addition to spaces, the following characters are used as breaking characters around a word "_-.()[] ". For instance, searching for "Test" with this option enabled would return files like "_Test.txt", "A(Test).jpg", "This is a Test.docx" and "file.test". But it would not return "testing.txt", "testimony.pdf" or "contest.zip".

This option is disabled by default. This option has no effect on wildcard searches.

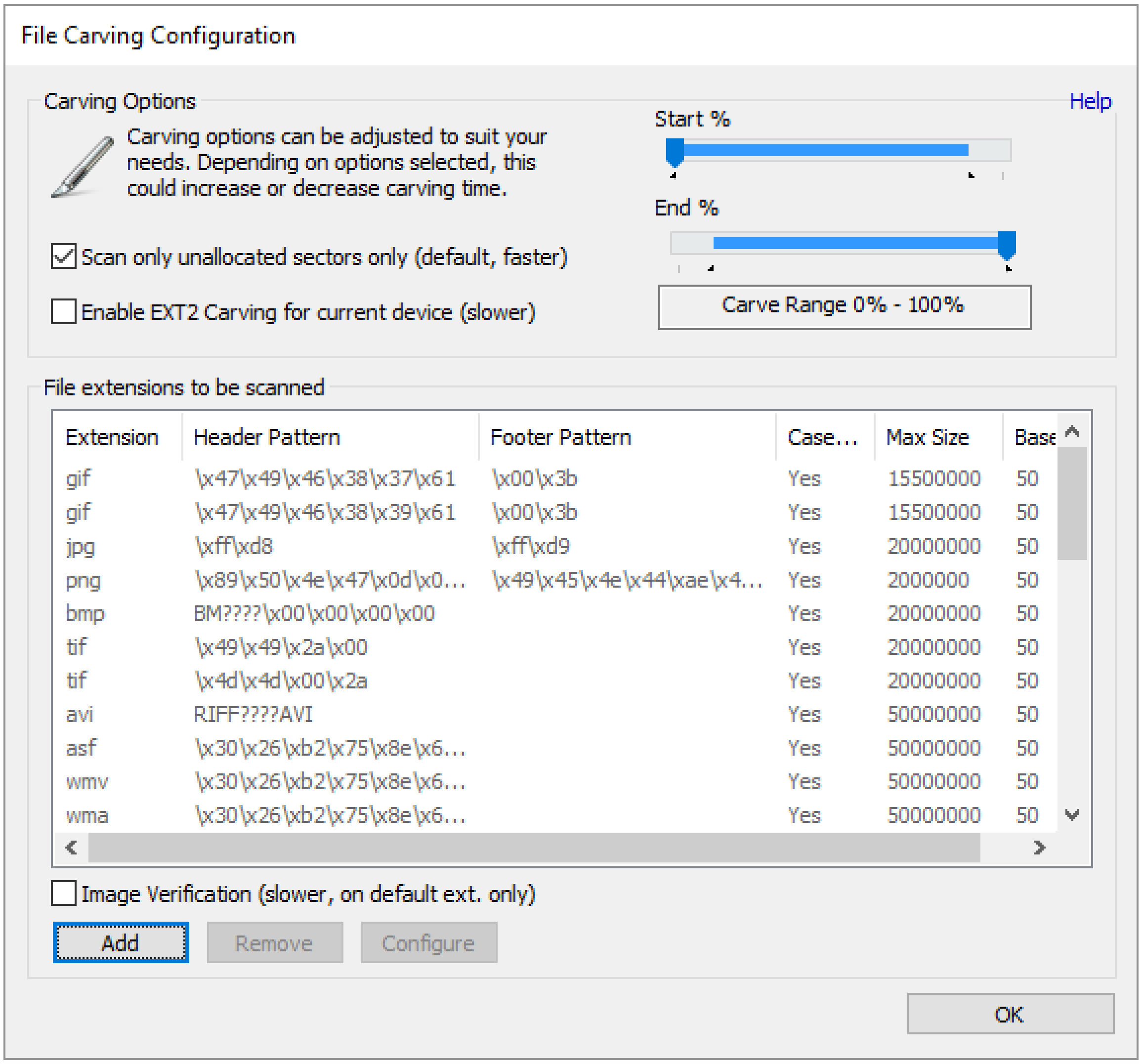
Multiple streams only

Enable File Carving
Instead of finding files from the master file tables, file carving looks at the raw physical disk data for file headers and attempts to recover files in this manner. This requires reading all data on the disk and as such is much slower than the standard method. Also it can only find a limited number of file types with known headers.

Configure Carving Options
Additional options for file carving. See File Carving Configuration below for available settings.

File Size Limits
Allows the user to specify file size limits for search results. The user may enter either a minimum, maximum, both or neither. The only restriction is that the maximum must be larger than the minimum.

File Carving Configuration



Carving options can be adjusted to suit your needs. Depending on options selected, this could increase or decrease carving time.

☑ Scan only unallocated sectors only (default, faster)

□ Enable EXT2 Carving for current device (slower)

Carve Range 0% - 100%

File extensions to be scanned

Extension	Header Pattern	Footer Pattern	Case…	Max Size	Base
gif	\x47\x49\x46\x38\x37\x61	\x00\x3b	Yes	15500000	50
gif	\x47\x49\x46\x38\x39\x61	\x00\x3b	Yes	15500000	50
jpg	\xff\xd8	\xff\xd9	Yes	20000000	50
png	\x89\x50\x4e\x47\x0d\x0…	\x49\x45\x4e\x44\xae\x4…	Yes	2000000	50
bmp	BM????\x00\x00\x00\x00		Yes	20000000	50
tif	\x49\x49\x2a\x00		Yes	20000000	50
tif	\x4d\x4d\x00\x2a		Yes	20000000	50
avi	RIFF????AVI		Yes	50000000	50
asf	\x30\x26\xb2\x75\x8e\x6…		Yes	50000000	50
wmv	\x30\x26\xb2\x75\x8e\x6…		Yes	50000000	50
wma	\x30\x26\xb2\x75\x8e\x6…		Yes	50000000	50

□ Image Verification (slower, on default ext. only)

Scan unallocated sectors only

For FAT and NTFS files systems, OSForensics has the ability to only index the unallocated sectors on the drive. This will reveal files in unused portion of the disk. Selecting this option will force OSForensics to instead scan the whole drive including sectors that may be allocated for a non deleted file.

When selecting a physical drive the entire contents of that drive will be searched, which may return files that are not actually deleted if there are working partitions on that drive. When selecting a single partition only unallocated space on that partition will be searched.

Image Verification

Applies extra level of checking to carved image files by trying to open the whole file with an image parser. Slows down the file carving process but provides better feedback on the file quality. If the image parser is successful in opening the image, the overall score is boosted by 25%. Similarly, if the image parser files to open the image, the overall score is decreased by 25%.

EXT2 Carving

In standard Linux file system such as EXT2, the contents of the files are stored in a series of data blocks. Each file on the system has a index node (inode) that contains pointers to these data blocks. Only the first 12 data blocks are directly pointed to within the inode. If a file is larger than the size of 12 data blocks, the file system will allocate a "indirect block" that holds the additional pointers to the file contents. The first indirect block is usually located directly after the first 12 content data blocks.

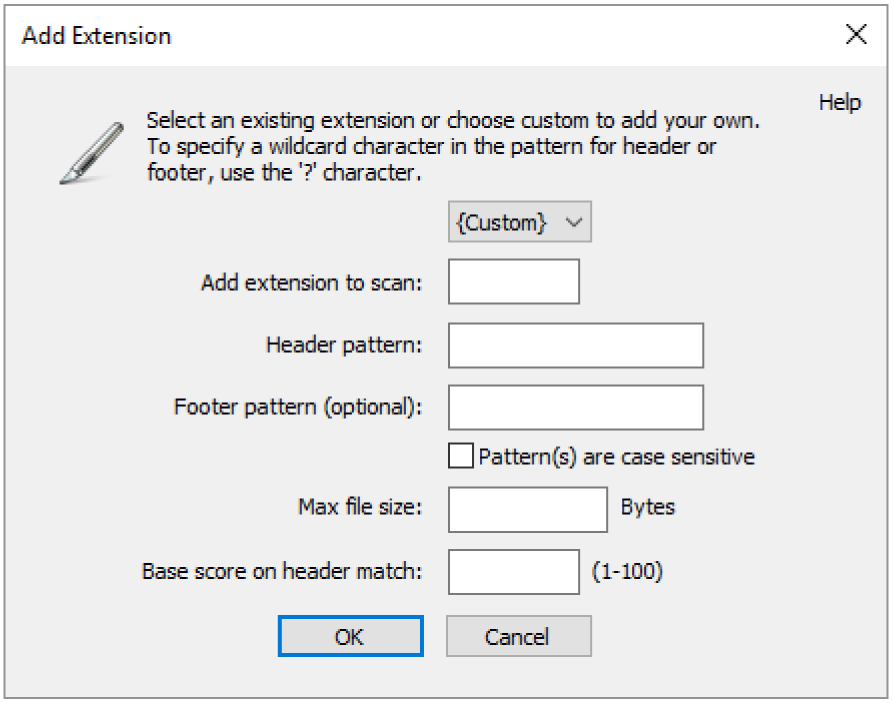
If Linux EXT2 carving is enabled, then during file carving, OSForensics will try to detect the indirect block for every file and carve around it. OSForensics only supports the detection and removal of the first indirect block. Double and Triply indirect blocks are not supported.

Range Selection
Allows the selection of carving range. Useful to look at a certain portion of the drive.

File extensions to be scanned
Currently default supported built-in file types are: gif, png, bmp, tif, asf, wmv, wma, mov, mpg, mp4, swf, flv, ole, doc, xls, ppt, msi, mst, msp, gra, zip, docx, xlsx, pptx, htm, pdf, wav, mp3, rar, eml and rtf.

The default file types are loaded from the "osf_filecarve.conf" file in the ProgramData directory, e.g. C:\ProgramData\Passmark\OSForensics. The pre-defined file types have coded file recovery functions that will do a superior job than a straight header/footer match.

Additional file types can be added or currently enabled file types can be removed. The default file types, identified by light grey text, in the list can be removed but cannot have their definitions edited.


Add Extension

Help

Select an existing extension or choose custom to add your own. To specify a wildcard character in the pattern for header or footer, use the '?' character.

{Custom}

Add extension to scan:

Header pattern:

Footer pattern (optional):

□ Pattern(s) are case sensitive

Max file size: Bytes

Base score on header match: (1-100)

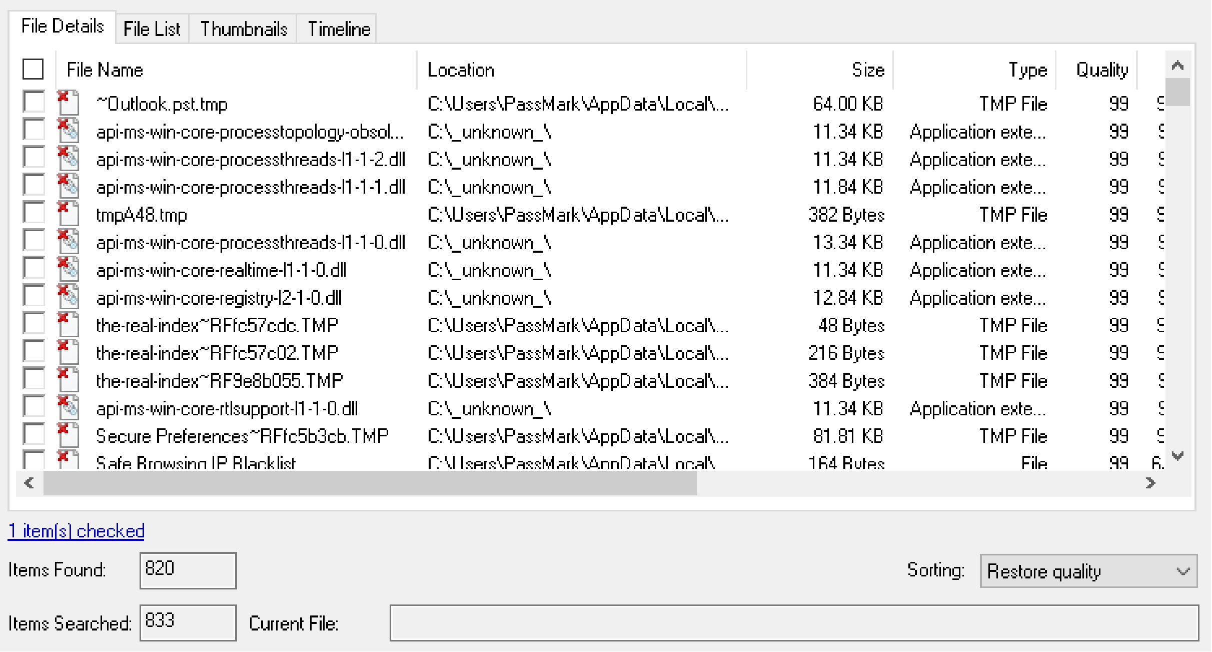
OSForensics will carve user defined file types, but will only look for header pattern and/or footer pattern. When a footer pattern is not specified. OSForensics will return default to the size of the maximum file size defined. When "File Carving" is enabled, OSForensics uses built-in values for maximum file size limits. The file size limit is dependent on the type of file, however, the overall file size limit for all files during carving is limited to 50MB.

Additional file types can also be added (or existing file types can be removed) by editing the above file. The file can be edited in a text editor. It is recommended that before any modification of this file takes place, a backup should be made in case the file needs to be reverted to its original state. Additional instructions for editing the file can be found within the file itself.

4.5.2 Deleted Files Search Results View

The user may view the deleted file search results in one of four views.

File Details View



□	File Name	Location	Size	Type	Quality	
□	~Outlook.pst.tmp	C:\Users\PassMark\AppData\Local\...	64.00 KB	TMP File	99	9
□	api-ms-win-core-processtopology-obsol...	C:_unknown_\	11.34 KB	Application exte...	99	9
□	api-ms-win-core-processthreads-l1-1-2.dll	C:_unknown_\	11.34 KB	Application exte...	99	9
□	api-ms-win-core-processthreads-l1-1-1.dll	C:_unknown_\	11.84 KB	Application exte...	99	9
□	tmpA48.tmp	C:\Users\PassMark\AppData\Local\...	382 Bytes	TMP File	99	9
□	api-ms-win-core-processthreads-l1-1-0.dll	C:_unknown_\	13.34 KB	Application exte...	99	9
□	api-ms-win-core-realtime-l1-1-0.dll	C:_unknown_\	11.34 KB	Application exte...	99	9
□	api-ms-win-core-registry-l2-1-0.dll	C:_unknown_\	12.84 KB	Application exte...	99	9
□	the-real-index~RFfc57cdc.TMP	C:\Users\PassMark\AppData\Local\...	48 Bytes	TMP File	99	9
□	the-real-index~RFfc57c02.TMP	C:\Users\PassMark\AppData\Local\...	216 Bytes	TMP File	99	9
□	the-real-index~RF9e8b055.TMP	C:\Users\PassMark\AppData\Local\...	384 Bytes	TMP File	99	9
□	api-ms-win-core-rtlsupport-l1-1-0.dll	C:_unknown_\	11.34 KB	Application exte...	99	9
□	Secure Preferences~RFfc5b3cb.TMP	C:\Users\PassMark\AppData\Local\...	81.81 KB	TMP File	99	9
□	Safe Browsing IP Blacklist	C:\Users\PassMark\AppData\Local\	164 Bytes	File	99	6.

1 item(s) checked

Items Found: 820

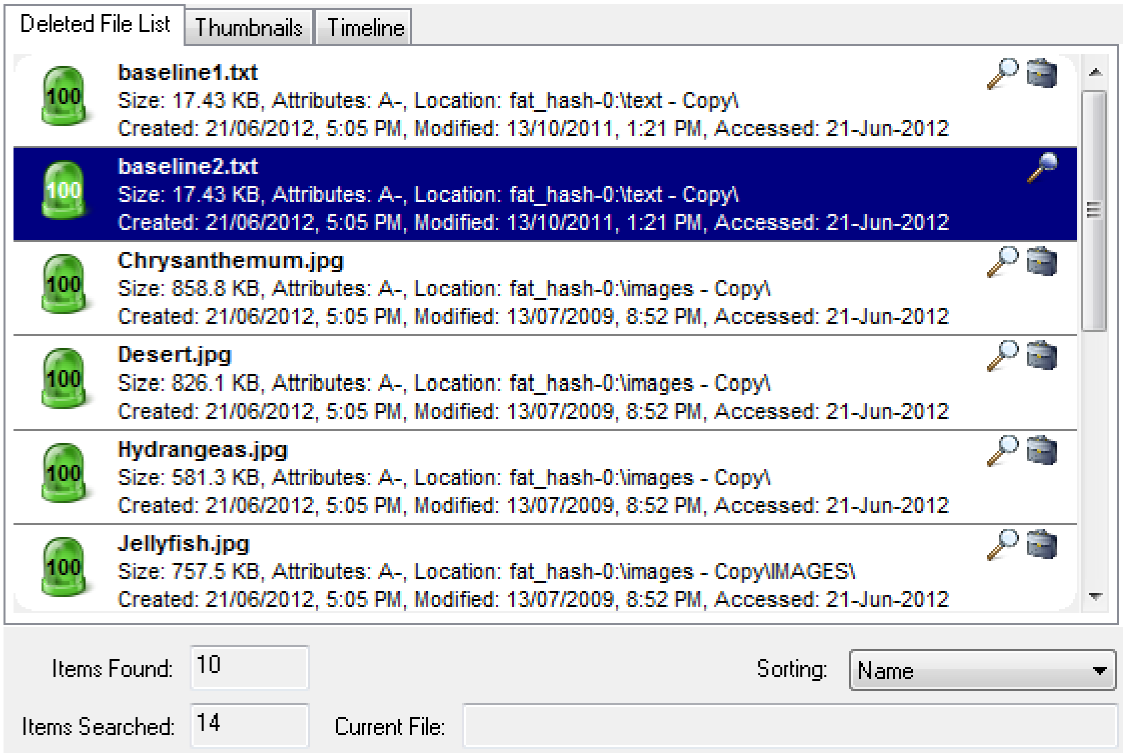
Sorting: Restore quality

Items Searched: 833

Current File:

The File Details View displays the search result in a table format, listing the file names along with relevant attributes and metadata. The results are sorted according to the criteria selected in the Sorting combo box.

Deleted File List View



baseline1.txt
Size: 17.43 KB, Attributes: A-, Location: fat_hash-0:\text - Copy\
Created: 21/06/2012, 5:05 PM, Modified: 13/10/2011, 1:21 PM, Accessed: 21-Jun-2012

baseline2.txt
Size: 17.43 KB, Attributes: A-, Location: fat_hash-0:\text - Copy\
Created: 21/06/2012, 5:05 PM, Modified: 13/10/2011, 1:21 PM, Accessed: 21-Jun-2012

Chrysanthemum.jpg
Size: 858.8 KB, Attributes: A-, Location: fat_hash-0:\images - Copy\
Created: 21/06/2012, 5:05 PM, Modified: 13/07/2009, 8:52 PM, Accessed: 21-Jun-2012

Desert.jpg
Size: 826.1 KB, Attributes: A-, Location: fat_hash-0:\images - Copy\
Created: 21/06/2012, 5:05 PM, Modified: 13/07/2009, 8:52 PM, Accessed: 21-Jun-2012

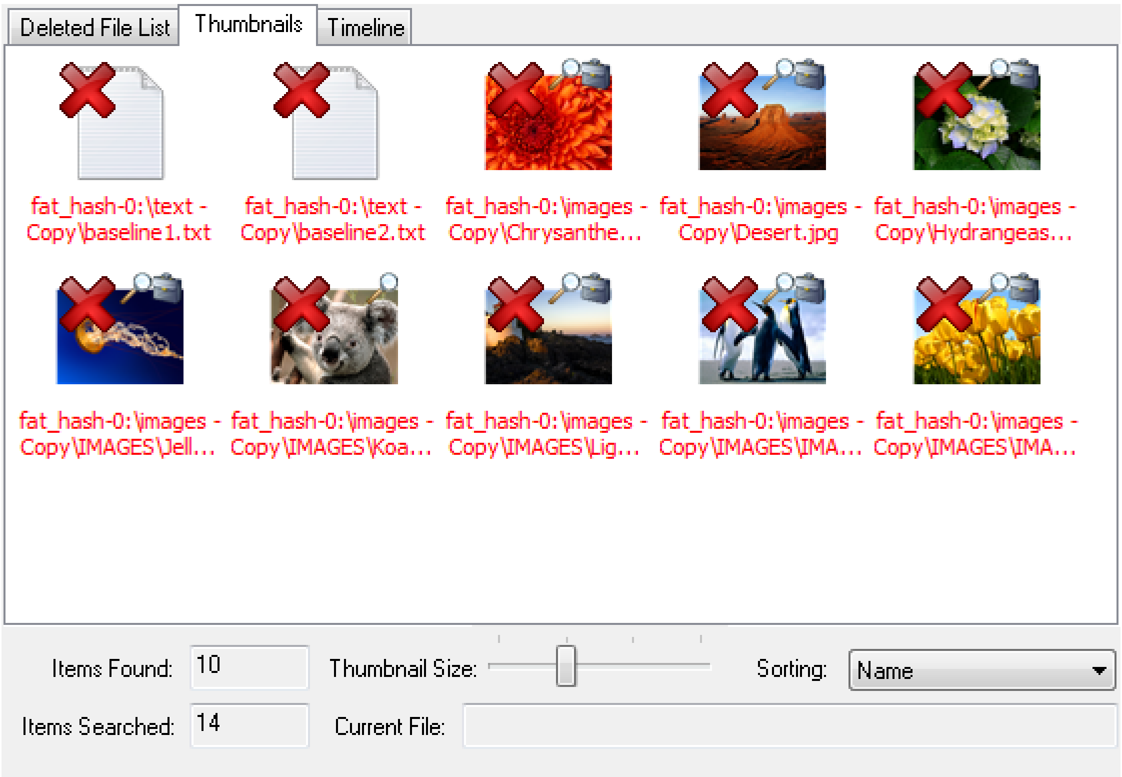
Hydrangeas.jpg
Size: 581.3 KB, Attributes: A-, Location: fat_hash-0:\images - Copy\
Created: 21/06/2012, 5:05 PM, Modified: 13/07/2009, 8:52 PM, Accessed: 21-Jun-2012

Jellyfish.jpg
Size: 757.5 KB, Attributes: A-, Location: fat_hash-0:\images - Copy\IMAGES\
Created: 21/06/2012, 5:05 PM, Modified: 13/07/2009, 8:52 PM, Accessed: 21-Jun-2012

Items Found: 10
Sorting: Name
Items Searched: 14
Current File:

The Deleted File List View displays the search result as a list of file names, along with the corresponding metadata and icon. The results are sorted according to the criteria selected in the Sorting combo box.

Thumbnails View

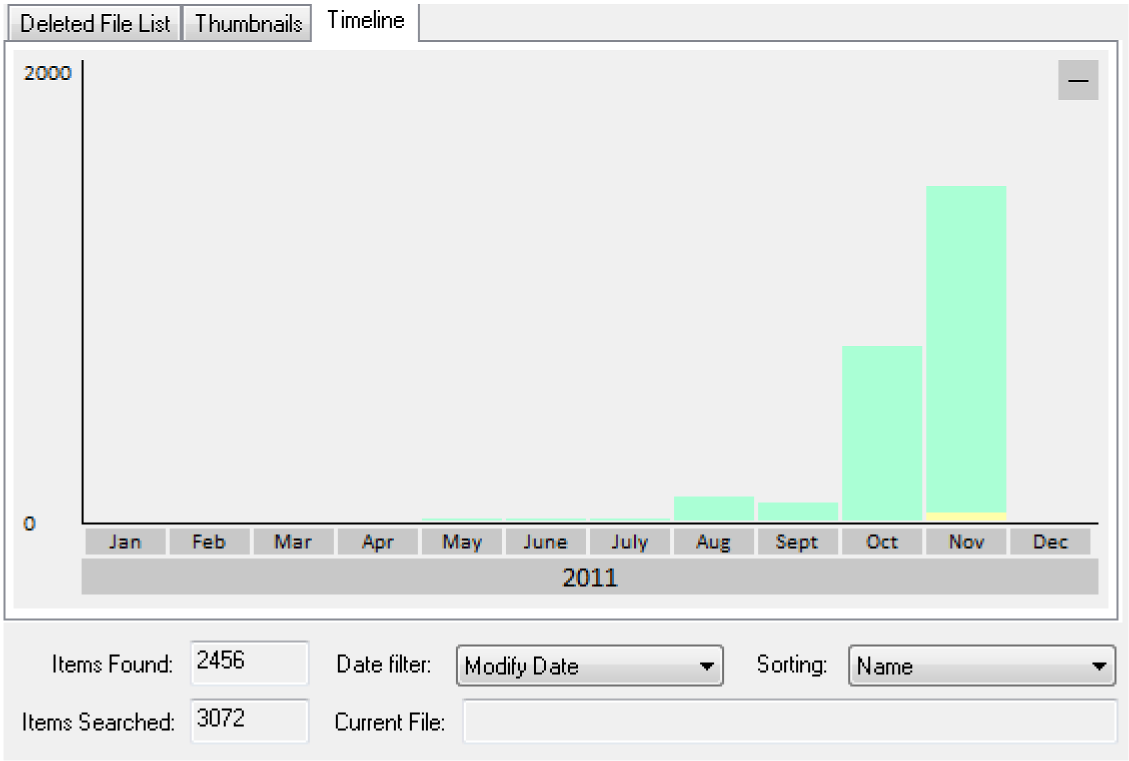


fat_hash-0:\text - Copy\baseline1.txt
fat_hash-0:\text - Copy\baseline2.txt
fat_hash-0:\images - Copy\Chrysanthe…
fat_hash-0:\images - Copy\Desert.jpg
fat_hash-0:\images - Copy\Hydrangeas…
fat_hash-0:\images - Copy\IMAGES\Jell…
fat_hash-0:\images - Copy\IMAGES\Koa…
fat_hash-0:\images - Copy\IMAGES\Lig…
fat_hash-0:\images - Copy\IMAGES\IMA…
fat_hash-0:\images - Copy\IMAGES\IMA…

Items Found: 10
Thumbnail Size:
Sorting: Name
Items Searched: 14
Current File:

The Thumbnails View displays the search results as a list of thumbnails as well as with its file path. This view is useful when searching for media files, allowing the user to quickly browse through the thumbnail images. Similar to the Deleted File List View, the results can be sorted via the Sorting combo box. The size of the thumbnails can be adjusted using the Thumbnail Size slider bar.

Timeline View



Items Found: 2456

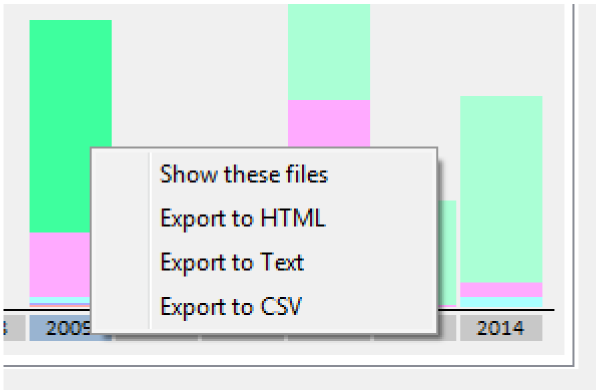
Date filter: Modify Date

Sorting: Name

Items Searched: 3072

Current File:

The Timeline View displays an interactive bar graph providing the user with a visual view of the distribution of files with respect to the date of the files. This view is useful for identifying date ranges where significant deleted file activity has occurred. The granularity of the scale can be adjusted by clicking on the bar graphs to zoom in or the '-' button on the top-right corner to zoom out. Right-clicking a bar section brings up the following menu:



Show these files
Filter the deleted files to show only those that belong to the selected time bar

Export to HTML
Export the deleted files contained in the highlighted bar to HTML

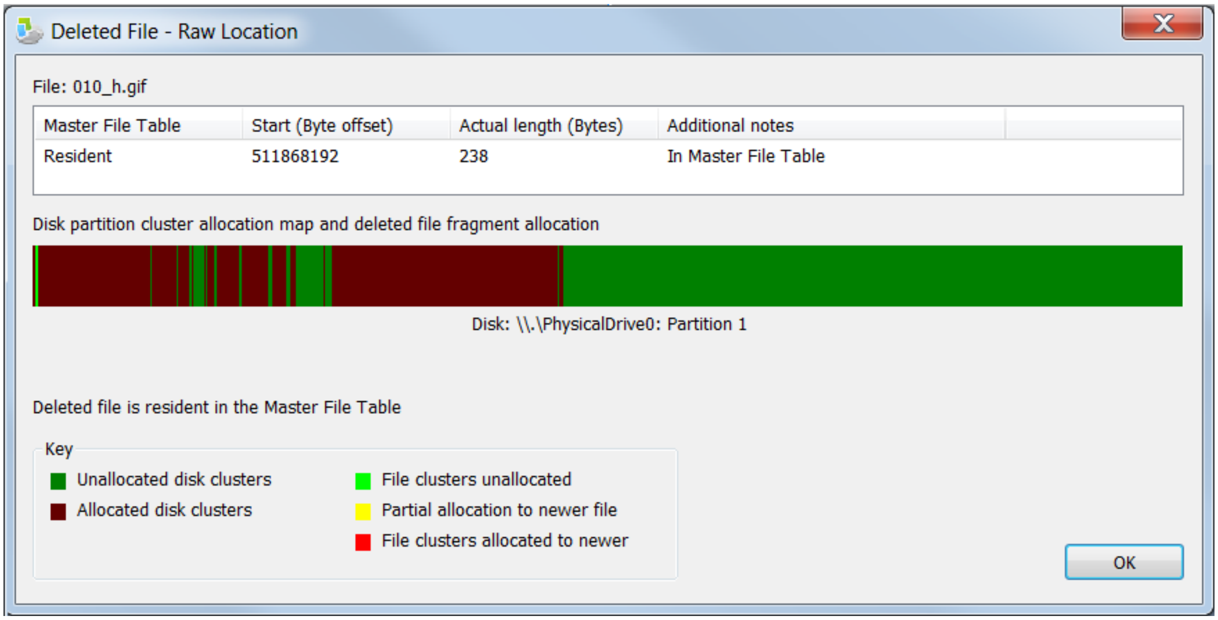
Export to Text
Export the deleted files contained in the highlighted bar to text

Export to CSV

Export the deleted files contained in the highlighted bar to CSV

4.5.3 Deleted File Cluster View

The Deleted File Cluster View window provides a graphical view of the allocation of the deleted file clusters on the physical disk. This window can be accessed by right-clicking a deleted file in the Deleted Files Search and selecting File Location Information.



Deleted File - Raw Location

File: 010_h.gif

Master File Table	Start (Byte offset)	Actual length (Bytes)	Additional notes
Resident	511868192	238	In Master File Table

Disk partition cluster allocation map and deleted file fragment allocation

Disk: \\.\PhysicalDrive0: Partition 1

Deleted file is resident in the Master File Table

Key

- 🟩 Unallocated disk clusters
- 🟥 Allocated disk clusters
- 🟩 File clusters unallocated
- 🟨 Partial allocation to newer file
- 🟥 File clusters allocated to newer

The table displays the fragmentation information of the deleted file. For smaller files, the deleted file may be resident in the MFT (NTFS only).

The map provides a graphical representation of the location of the fragments with respect to the physical disk it resides on.

4.5.4 Deleted Files Techincal Details

Background

A physical disk has a partition table that describes the partitions on the disk, such as where the partitions are located on the disk and the format of the partitions (e.g. NTFS, FAT32, FAT16).

An NTFS (NT File System) partition contains a boot sector, which contains information like the partition sector size, cluster size and boot code. An important concept for NTFS is the Master File Table (MFT), which is like an index for all files on the system. The Master File Table contains information like the Filename, size, attributes, and location of file data fragments on the disk. Very small files can be contained in the Master File Table record (called resident). When a file is deleted from an NTFS volume, the Master File Table entry for the file is marked as deleted. The file information such as name, size and location on the disk is not deleted and the data is not deleted. After deleting a file, the file system is free to re-allocate the MFT record and the data clusters to another file.

FAT (File Allocation Table) is a generally used on external drives, like USB drives. FAT32 is newer than FAT16, and allows for larger files and disks. A FAT partition contains a boot sector, a FAT and a data area. The boot sector contains information like the partition sector size, cluster size and boot code. The FAT contains a map of cluster allocation for the data area; with file data described as a set of linked clusters. The Data area contains both information about files and the actual file data. When a file is deleted from a FAT volume, all clusters in the FAT table related to the file are set to unallocated and the file information in the data area is marked as deleted (by changing the first character of the filename). The file data is not deleted. After a file is deleted we potentially have the first cluster the file used, but do not know which subsequent clusters were used, as this (chain link) information was removed from the FAT. As such, to recover a file, assumptions based on file system behavior and current cluster allocation, are needed to estimate the most likely clusters that were in the file. There are some cases were this will not work well for any FAT recovery tool. After deleting a file, the file system is free to re-allocate the FAT cluster map and the data area used for file information and file data.

Recovering files deleted from the recycling bin

Moving a file to the recycling bin in NTFS moves the file to the hidden system directory $RECYCLE.BIN and renames the file (e.g. file1.txt to $RH7IJX4.txt). It also creates a new file (e.g. $IH7IJX4.txt). This file contains recycle bin file restore data, such as the directory and the original filename (e.g. C:\dir1 \file1.txt).

When you delete the file from the recycling bin (such as emptying the recycling bin), both files are deleted by marking the MFT records as not in use. Both of these files are potentially recoverable, but with the new filenames. OS Forensics checks whether both files are available, and if they are, then the original filename is retrieved from the recycling bin metadata file and is shown as well as the recycling bin filename.

On searching for deleted files, when the original filename can be recovered from the recycling bin metadata file content, the search string specified is matched with the original deleted filename (e.g. file1.txt). When the recycling bin Meta data file content is not recoverable, a search for the recycle bin filename is required (e.g. on *.txt to match “$RH7IJX4.txt”).

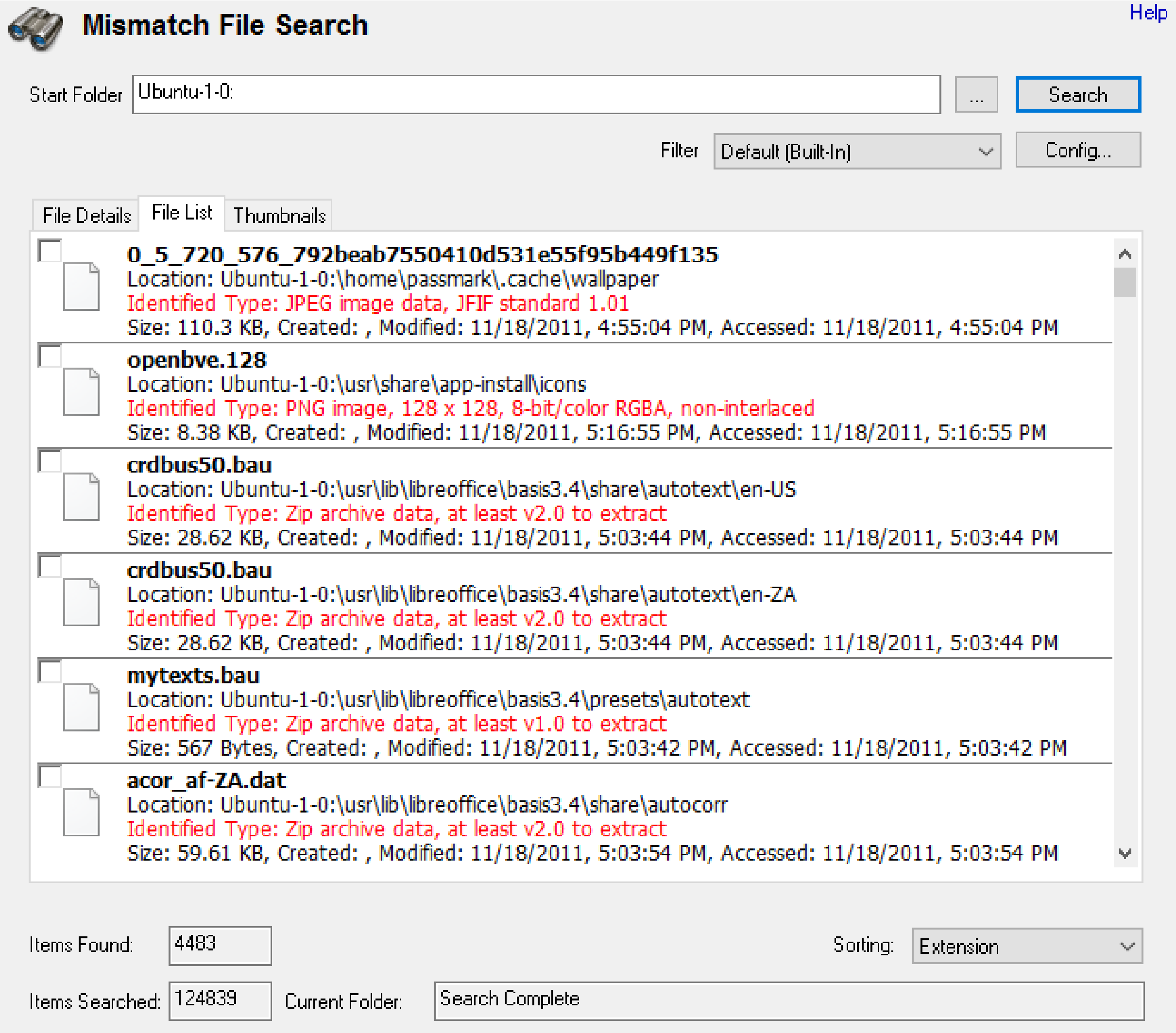
Examples:

(1) Where the information about the deleted files and metadata can be recovered, a search for “file1” will return the result “file1.txt (Recycle bin name: $RH7IJX4.txt)”. If the recycling bin metadata file content cannot be recovered, then the original file will only be known as “$RH7IJX4.txt”, and no match will occur.

(2) Where the information about the deleted files and metadata can be recovered, a search for *.txt would return the original filename “file1.txt (Recycle bin name: $RH7IJX4.txt)” and the recycling bin metadata file “$IH7IJX4.txt”. If the recycling bin metadata file content cannot be recovered, then the recycling bin name “$RH7IJX4.txt” and metadata file “$IH7IJX4.txt” will be returned. Further, if the recycling bin metadata file information cannot be recovered, then the recycling bin filename “$RH7IJX4.txt” will be returned. If the file content is recoverable, then the original content for file1.txt will be in the “$RH7IJX4.txt”.

4.6 Mismatch File Search

The Mismatch File Search Module can be used to locate files whose contents do not match its file extension. This module can uncover attempts to hide files under a false file name and extension by verifying whether the actual file format matches its intended file format based on the file extension.



Start Folder: Ubuntu-1-0:

Filter: Default (Built-In)

0_5_720_576_792beab7550410d531e55f95b449f135
Location: Ubuntu-1-0:\home\passmark\.cache\wallpaper
Identified Type: JPEG image data, JFIF standard 1.01
Size: 110.3 KB, Created: , Modified: 11/18/2011, 4:55:04 PM, Accessed: 11/18/2011, 4:55:04 PM

openbve.128
Location: Ubuntu-1-0:\usr\share\app-install\icons
Identified Type: PNG image, 128 x 128, 8-bit/color RGBA, non-interlaced
Size: 8.38 KB, Created: , Modified: 11/18/2011, 5:16:55 PM, Accessed: 11/18/2011, 5:16:55 PM

crdbus50.bau
Location: Ubuntu-1-0:\usr\lib\libreoffice\basis3.4\share\autotext\en-US
Identified Type: Zip archive data, at least v2.0 to extract
Size: 28.62 KB, Created: , Modified: 11/18/2011, 5:03:44 PM, Accessed: 11/18/2011, 5:03:44 PM

crdbus50.bau
Location: Ubuntu-1-0:\usr\lib\libreoffice\basis3.4\share\autotext\en-ZA
Identified Type: Zip archive data, at least v2.0 to extract
Size: 28.62 KB, Created: , Modified: 11/18/2011, 5:03:44 PM, Accessed: 11/18/2011, 5:03:44 PM

mytexts.bau
Location: Ubuntu-1-0:\usr\lib\libreoffice\basis3.4\presets\autotext
Identified Type: Zip archive data, at least v1.0 to extract
Size: 567 Bytes, Created: , Modified: 11/18/2011, 5:03:42 PM, Accessed: 11/18/2011, 5:03:42 PM

acor_af-ZA.dat
Location: Ubuntu-1-0:\usr\lib\libreoffice\basis3.4\share\autocorr
Identified Type: Zip archive data, at least v2.0 to extract
Size: 59.61 KB, Created: , Modified: 11/18/2011, 5:03:54 PM, Accessed: 11/18/2011, 5:03:54 PM

Items Found: 4483
Sorting: Extension
Items Searched: 124839
Current Folder: Search Complete

Basic Usage

A basic mismatch file search simply involves entering a search location and a filter. OSForensics will locate any files whose raw bytes are not consistent with the format that the file extension specifies. For instance, an image file (test.jpg) that has been renamed to a document file (test.doc) will appear in the results since the raw bytes of an image file do not correspond to the file format of a document file.

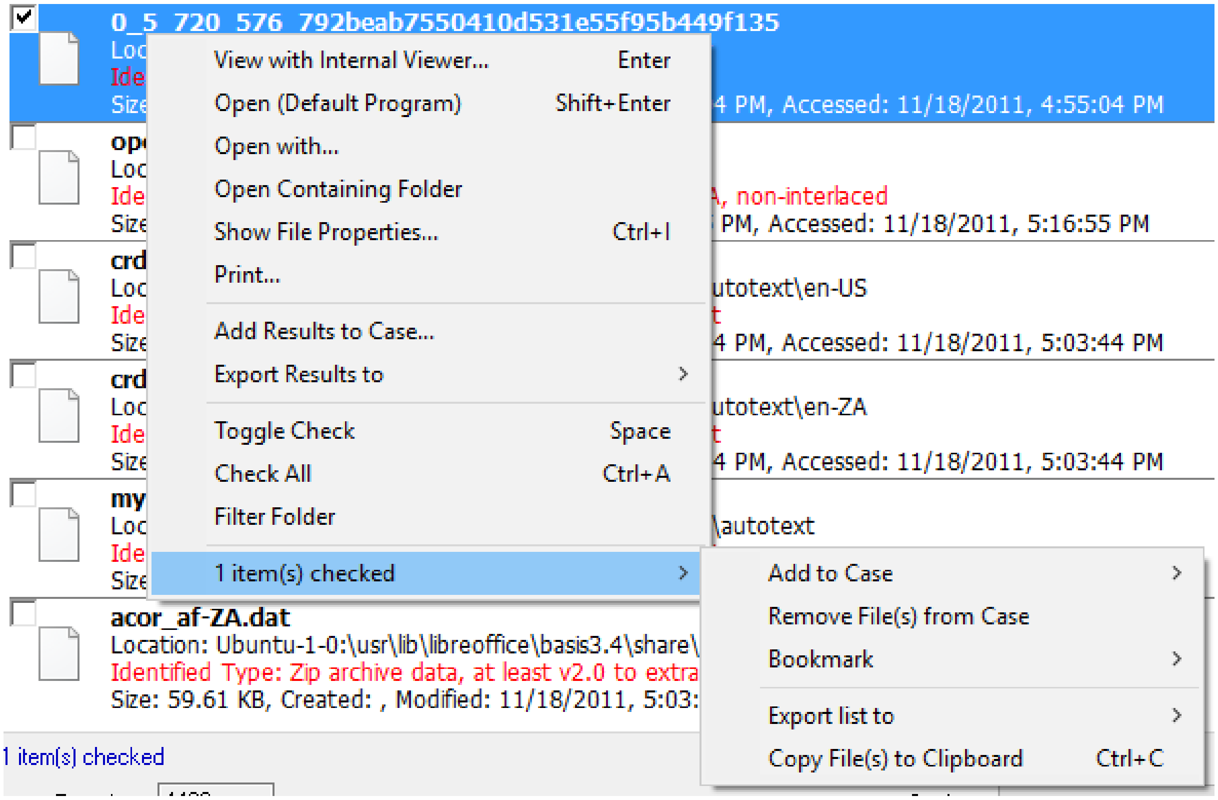
Filter
The user can choose one of the following built-in filters or a user-defined filter.

All - The search results are filtered using all built-in filters
Inaccessible - Only files that could not be accessed are displayed
Mismatch - Only files whose file extension/contents that are mismatched are displayed

To create a new filter, click the Config button.

Results

The results of the search are displayed in one of several views, along with a summary of the number of items searched/found. Right-clicking a file opens the following context menu.


0_5_720_576_792beab7550410d531e55f95b449f135
4 PM, Accessed: 11/18/2011, 4:55:04 PM
View with Internal Viewer... Enter
Open (Default Program) Shift+Enter
Open with...
Open Containing Folder
Show File Properties... Ctrl+I
Print...
Add Results to Case...
Export Results to
Toggle Check Space
Check All Ctrl+A
Filter Folder
1 item(s) checked
Add to Case
Remove File(s) from Case
Bookmark
Export list to
Copy File(s) to Clipboard Ctrl+C
, non-interlaced
PM, Accessed: 11/18/2011, 5:16:55 PM
utotext\en-US
4 PM, Accessed: 11/18/2011, 5:03:44 PM
utotext\en-ZA
4 PM, Accessed: 11/18/2011, 5:03:44 PM
\autotext
acor_af-ZA.dat
Location: Ubuntu-1-0:\usr\lib\libreoffice\basis3.4\share\
Identified Type: Zip archive data, at least v2.0 to extra
Size: 59.61 KB, Created: , Modified: 11/18/2011, 5:03:
1 item(s) checked

View with Interval Viewer
Opens the file with OSForensics Viewer to perform a more thorough analysis

Open (Default Program)
Open the file with the default program

Open With...
Allows the user to select the program to open the file

Open Containing Folder
Opens the folder than contains the file

Show File Properties
Opens the file with OSForensics Viewer in File Info mode.

Print...
Print the file (if applicable)

Add Results to Case...

Add the list of results as an HTML or CSV file to case

Export Results to
Export the list of results to a TXT, CSV or HTML file

Toggle Check
Toggle the check state of the selected item.

Check All
Check all the items in the list.

Filter Folder
Exclude the folder of the selected file from the search results

n Item(s) checked

Add to Case
Add the checked file(s) or list of checked file(s) to the case

Remove File(s) from Case
Remove the checked file(s) from the case

Bookmark

Green
Add/remove selected path from the list of Green bookmarks. *Keyboard shortcut: Ctrl+G*

Yellow
Add/remove selected path from the list of Yellow bookmarks. *Keyboard shortcut: Ctrl+Y*

Red
Add/remove selected path from the list of Red bookmarks. *Keyboard shortcut: Ctrl+R*

Export list to
Export the list of checked file(s) to a TXT, CSV or HTML file

Save to disk...
Save the checked file(s) to a location on disk.

Copy Files(s) to Clipboard
Copy the checked file(s) to clipboard. Once copied to the clipboard, the file(s) can be pasted to any other application that supports it (eg. Windows Explorer).

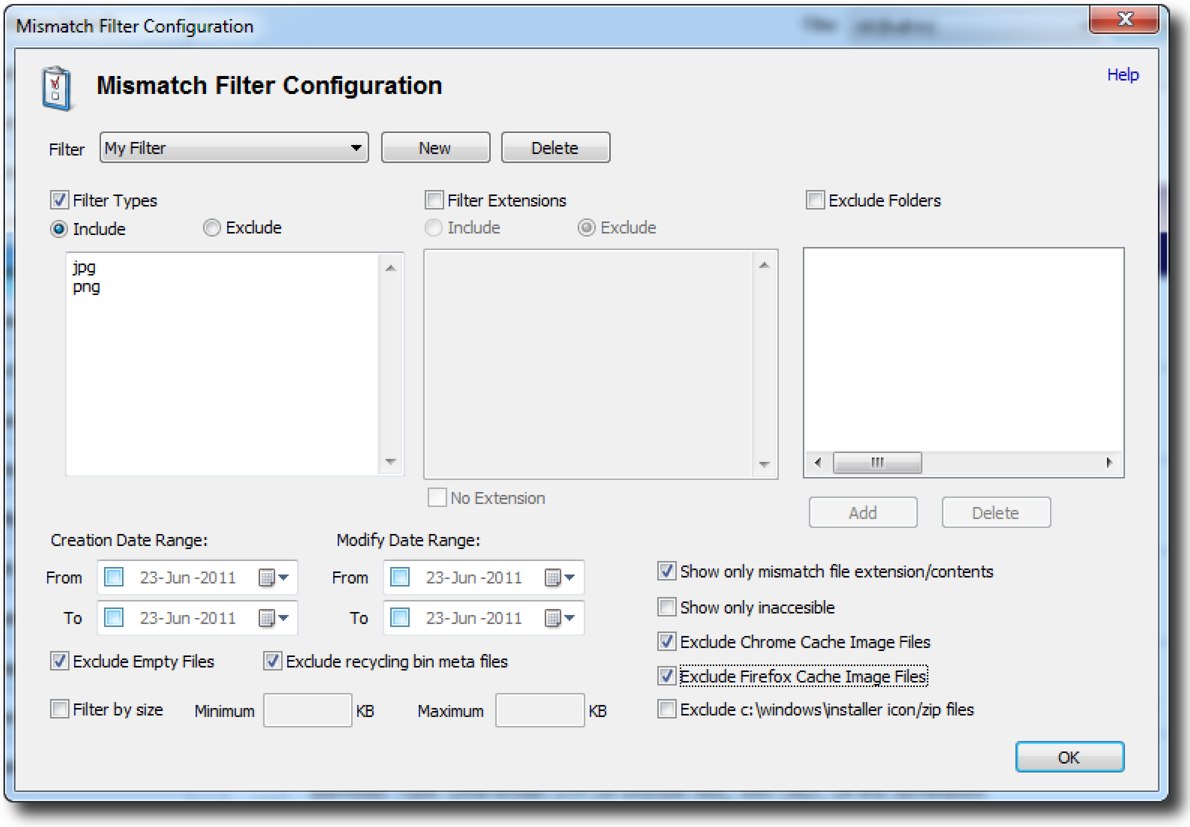
Note: In some cases, copy and pasting files to an explorer window may fail without an error message when "preparing to copy". This may happen if the file has already been deleted (eg a temp file) or if Windows Explorer does not have permissions to access the files (eg restricted system files and folders). In these cases, it is better to use the "Add to case" function.

Advanced Usage

There are some files that can be edited in OSForensics that allow you to modify/improve the mismatch lookup process. See this page for details.

4.6.1 Mismatch Filter Configuration

The Mismatch Filter Configuration Window allows users to define new search filters. This window can be accessed by clicking on the "Config..." button in the main Mismatch File Search window.



Mismatch Filter Configuration

Filter: My Filter

☑ Filter Types
● Include ○ Exclude
jpg
png

☐ Filter Extensions
○ Include ● Exclude
☐ No Extension

☐ Exclude Folders

Creation Date Range:
From ☐ 23-Jun -2011
To ☐ 23-Jun -2011

Modify Date Range:
From ☐ 23-Jun -2011
To ☐ 23-Jun -2011

☑ Exclude Empty Files ☑ Exclude recycling bin meta files

☐ Filter by size Minimum KB Maximum KB

☑ Show only mismatch file extension/contents
☐ Show only inaccessible
☑ Exclude Chrome Cache Image Files
☑ Exclude Firefox Cache Image Files
☐ Exclude c:\windows\installer icon/zip files

Filter
The selected filter to configure

New
Click this button to create a new filter

Delete
Click this button to delete the selected filter

Filter Types
If checked, allows the user to input filter types to include/exclude in the search results

Filter Extensions
If checked, allows the user to input filter extensions to include/exclude in the search results. To include/ exclude files with no extension, check the No Extension checkbox.

Exclude Folders
If checked, allows the user to add folders to exclude from the search results. Click 'Add' to add a folder, 'Delete' to remove a folder.

Only Include Date Range
If checked, allows the user to specify the date ranges to include in the search results.

Exclude Empty Files
If checked, files that are 0 bytes in file size are excluded from the search results

Exclude Recycling Bin Meta Files
If checked, files that are 0 bytes in file size are excluded from the search results

Filter by size
If checked, allows the user to specify file size limits for search results. The user may enter either a minimum, maximum, both or neither. The only restriction is that the maximum must be larger than the minimum.

Show only file extension/contents
If checked, the search results will only contain files whose contents and file extension are mismatched.

Show only inaccessible
If checked, the search results will only contain files that cannot be accessed.

Exclude Chrome Cache Image Files
If checked, the search results will not include Chrome Cache image files

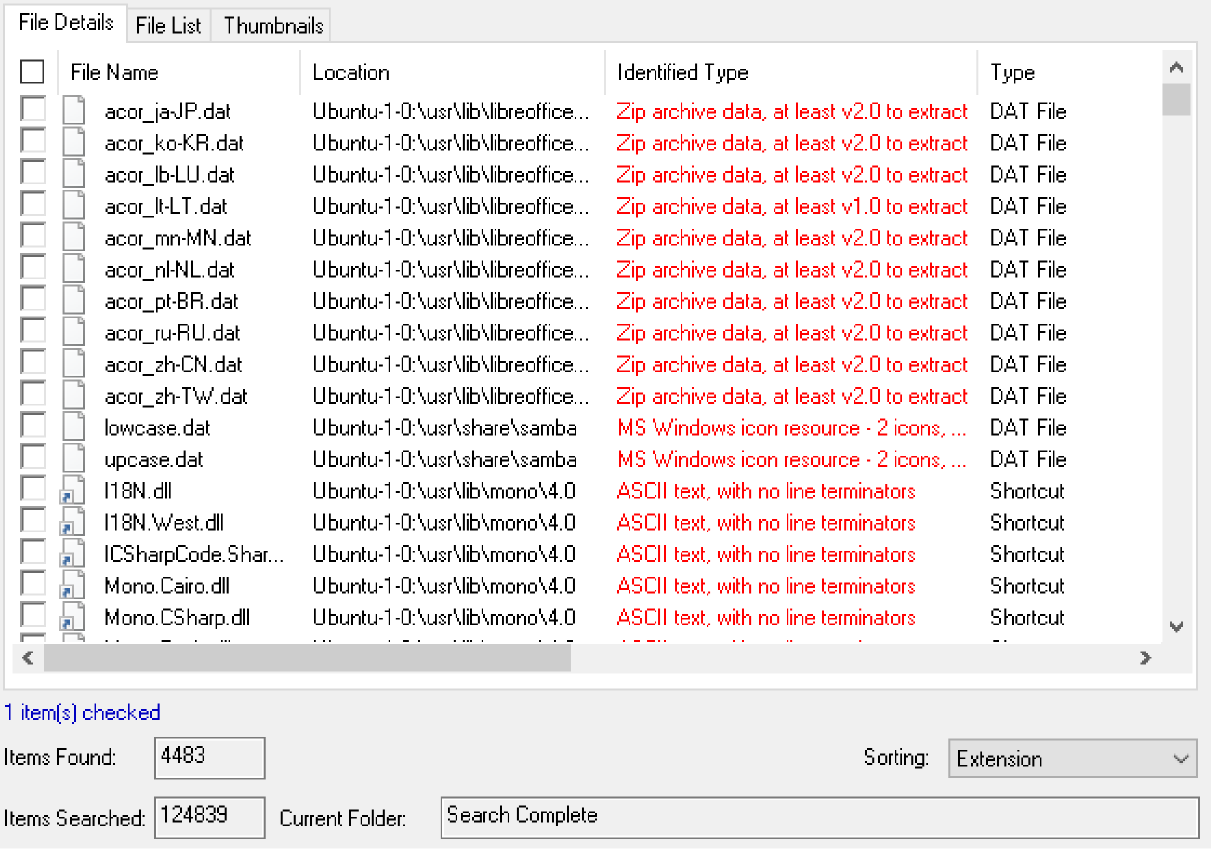
Exclude Firefox Cache Image Files
If checked, the search results will not include Firefox Cache image files

Exclude c:\windows\installer icon/zip files
If checked, the search results will not include icon/zip files under c:\windows\installer

4.6.2 Mismatch File Search Results View

The user may view the mismatch file search results in one of several views.

File Details View



□	File Name	Location	Identified Type	Type
□	acor_ja-JP.dat	Ubuntu-1-0:\usr\lib\libreoffice...	Zip archive data, at least v2.0 to extract	DAT File
□	acor_ko-KR.dat	Ubuntu-1-0:\usr\lib\libreoffice...	Zip archive data, at least v2.0 to extract	DAT File
□	acor_lb-LU.dat	Ubuntu-1-0:\usr\lib\libreoffice...	Zip archive data, at least v2.0 to extract	DAT File
□	acor_lt-LT.dat	Ubuntu-1-0:\usr\lib\libreoffice...	Zip archive data, at least v1.0 to extract	DAT File
□	acor_mn-MN.dat	Ubuntu-1-0:\usr\lib\libreoffice...	Zip archive data, at least v2.0 to extract	DAT File
□	acor_nl-NL.dat	Ubuntu-1-0:\usr\lib\libreoffice...	Zip archive data, at least v2.0 to extract	DAT File
□	acor_pt-BR.dat	Ubuntu-1-0:\usr\lib\libreoffice...	Zip archive data, at least v2.0 to extract	DAT File
□	acor_ru-RU.dat	Ubuntu-1-0:\usr\lib\libreoffice...	Zip archive data, at least v2.0 to extract	DAT File
□	acor_zh-CN.dat	Ubuntu-1-0:\usr\lib\libreoffice...	Zip archive data, at least v2.0 to extract	DAT File
□	acor_zh-TW.dat	Ubuntu-1-0:\usr\lib\libreoffice...	Zip archive data, at least v2.0 to extract	DAT File
□	lowcase.dat	Ubuntu-1-0:\usr\share\samba	MS Windows icon resource - 2 icons, ...	DAT File
□	upcase.dat	Ubuntu-1-0:\usr\share\samba	MS Windows icon resource - 2 icons, ...	DAT File
□	I18N.dll	Ubuntu-1-0:\usr\lib\mono\4.0	ASCII text, with no line terminators	Shortcut
□	I18N.West.dll	Ubuntu-1-0:\usr\lib\mono\4.0	ASCII text, with no line terminators	Shortcut
□	ICSharpCode.Shar...	Ubuntu-1-0:\usr\lib\mono\4.0	ASCII text, with no line terminators	Shortcut
□	Mono.Cairo.dll	Ubuntu-1-0:\usr\lib\mono\4.0	ASCII text, with no line terminators	Shortcut
□	Mono.CSharp.dll	Ubuntu-1-0:\usr\lib\mono\4.0	ASCII text, with no line terminators	Shortcut

1 item(s) checked

Items Found: 4483

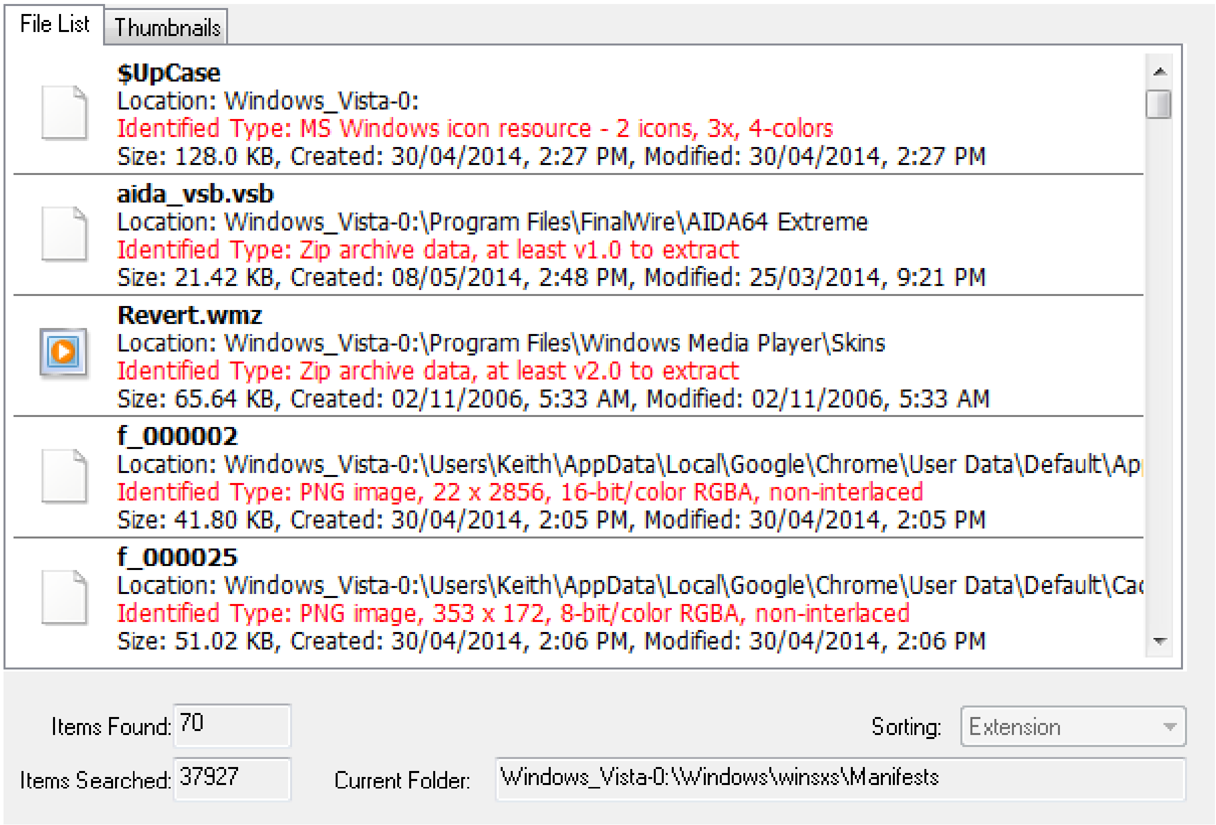
Sorting: Extension

Items Searched: 124839

Current Folder: Search Complete

The File Details View displays the search result in a table format, listing the file names along with relevant attributes and metadata.

File List View



$UpCase
Location: Windows_Vista-0:
Identified Type: MS Windows icon resource - 2 icons, 3x, 4-colors
Size: 128.0 KB, Created: 30/04/2014, 2:27 PM, Modified: 30/04/2014, 2:27 PM

aida_vsb.vsb
Location: Windows_Vista-0:\Program Files\FinalWire\AIDA64 Extreme
Identified Type: Zip archive data, at least v1.0 to extract
Size: 21.42 KB, Created: 08/05/2014, 2:48 PM, Modified: 25/03/2014, 9:21 PM

Revert.wmz
Location: Windows_Vista-0:\Program Files\Windows Media Player\Skins
Identified Type: Zip archive data, at least v2.0 to extract
Size: 65.64 KB, Created: 02/11/2006, 5:33 AM, Modified: 02/11/2006, 5:33 AM

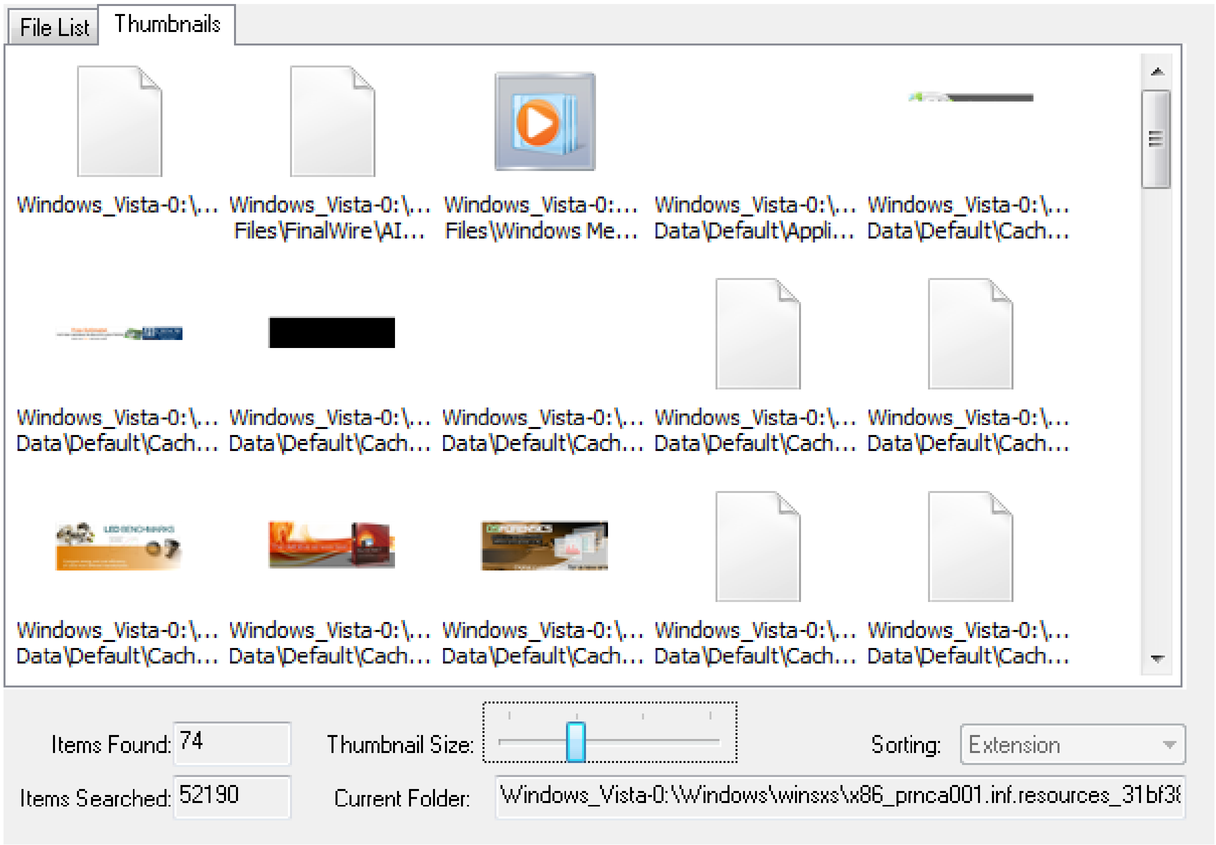
f_000002
Location: Windows_Vista-0:\Users\Keith\AppData\Local\Google\Chrome\User Data\Default\Ap
Identified Type: PNG image, 22 x 2856, 16-bit/color RGBA, non-interlaced
Size: 41.80 KB, Created: 30/04/2014, 2:05 PM, Modified: 30/04/2014, 2:05 PM

f_000025
Location: Windows_Vista-0:\Users\Keith\AppData\Local\Google\Chrome\User Data\Default\Ca
Identified Type: PNG image, 353 x 172, 8-bit/color RGBA, non-interlaced
Size: 51.02 KB, Created: 30/04/2014, 2:06 PM, Modified: 30/04/2014, 2:06 PM

Items Found: 70
Sorting: Extension
Items Searched: 37927
Current Folder: Windows_Vista-0:\Windows\winsxs\Manifests

The File List View displays the search result as a list of file names, along with the supposed file type, corresponding metadata and icon. The results are sorted according to the criteria selected in the Sorting combo box.

Thumbnails View


File List
Thumbnails
Windows_Vista-0:\...
Windows_Vista-0:\... Files\FinalWire\AI...
Windows_Vista-0:... Files\Windows Me...
Windows_Vista-0:\... Data\Default\Appli...
Windows_Vista-0:\... Data\Default\Cach...
Windows_Vista-0:\... Data\Default\Cach...
Windows_Vista-0:\... Data\Default\Cach...
Windows_Vista-0:\... Data\Default\Cach...
Windows_Vista-0:\... Data\Default\Cach...
Windows_Vista-0:\... Data\Default\Cach...
Windows_Vista-0:\... Data\Default\Cach...
Windows_Vista-0:\... Data\Default\Cach...
Windows_Vista-0:\... Data\Default\Cach...
Windows_Vista-0:\... Data\Default\Cach...
Windows_Vista-0:\... Data\Default\Cach...
Thumbnail Size:

Items Found: 74

Items Searched: 52190

Sorting: Extension

Current Folder: Windows_Vista-0:\Windows\winsxs\x86_prnca001.inf.resources_31bf3

The Thumbnails View displays the search result as a list of thumbnails as well as with its file path. This view is useful when the search results contain media files, allowing the user to quickly browse through the thumbnail images. Similar to the File List View, the results can be sorted via the Sorting combo box. The size of the thumbnails can be adjusted using the Thumbnail Size slider bar.

4.6.3 Advanced

There are two files that can be modified to change the behaviour of the Mismatch File search. Editing these files should only be done by advanced users. The files can be found in your common application data folder (ie. 'C:\ProgramData' or 'C:\Documents and Settings\All Users\') under 'Passmark \OSForensics'.

OSF.mg

This file contains the definitions used to identify file types, essentially containing templates showing what different types of files look like.

The file contains lines describing magic numbers which identify particular types of files. Lines beginning with a > or & character represent continuation lines to a preceding main entry:

>
If file finds a match on the main entry line, these additional patterns are checked. Any pattern which matches is used. This may generate additional output; a single blank separates each matching line's output (if any output exists for that line).

&

If file finds a match on the main entry line, and a following continuation line begins with this character, that continuation line's pattern must also match, or neither line is used. Output text associated with any line beginning with the & character is ignored.

Each line consists of four fields, separated by one or more tabs:

Field 1

The first field is a byte offset in the file, consisting of an optional offset operator and a value. In continuation lines, the offset immediately follows a continuation character.

If no offset operator is specified, then the offset value indicates an offset from the beginning of the file.

The * offset operator specifies that the value located at the memory location following the operator be used as the offset. Thus, *0x3C indicates that the value contained in 0x3C should be used as the offset.

The + offset operator specifies an incremental offset, based upon the value of the last offset. Thus, +15 indicates that the offset value is 15 bytes from the last specified offset.

An offset operator of the form (l+R) specifies an offset that is the total of the value of memory location specified by l and the value R.

An offset operator of the form (l-R) specifies an offset that is calculated by subtracting the value R from the value of memory location specified by l.

Field 2

The next field is a type: byte, short, long, string, Ustring (Unicode string). byte, short, long, beshort (big endian short), leshort (little endian short), belong (big endian long), lelong (little endian long). This can be followed by an optional mask which is bitwise ANDed to the value prior to comparison, for example, byte &0x80 looks at the high bit.

Note:

The types beshort and belong are equivalent to short and long, respectively.

Instead of a type, this field can contain the string search/N which indicates to search for the string indicated in the next field up to N byes from the offset.

Field 3

The next field is a value, preceded by an optional operator. Operators only apply to non-string types: byte, short, long, leshort, beshort lelong, and belong. The default operator is = (exact match). The other operators are:

=	equal
!	not equal
>	greater than
<	less than
&	all bits in pattern must match
^	any bits in pattern may match
x or ?	any value matches (must be the only character in the field) (? is an extension to traditional implementations of magic)

string or Ustring values to be matched may contain any valid ANSI C backslash sequence. Thus, to match a single backslash, \\ must be entered in the magic file.

Note:

Due to its format, the magic file must use a \t to match a tab character.

Field 4

The rest of the line is a string to be printed if the particular file matches the template. Note that the contents of this field are ignored, if the line begins with the & continuation character. The fourth field may contain a printf-type format indicator to output the magic number (See printf for more details on format indicators).

External Links
Above documentation taken from http://www.mkssoftware.com/docs/man4/magic.4.asp
Wikipedia entry on Magic Numbers http://en.wikipedia.org/wiki/File_format#Magic_number
Database of additional magic definitions http://www.magicdb.org/

MagicLookup.csv

This file defines the list of extensions 'known' by OSForensics. This file is a comma separated table with three columns, each line defines a new known file type. The first column defines a substring of the data type returned by the lookup. The second column defines the extension associated with this file description. The third column is contains additional flags defining this record. Currently the only supported flag is 1, which specifies that this type of file does not only belong to this extension.

Examples:

```
RAR archive data,rar,0
```

The first line specifies if the type contains the text 'Rar archive' then the extension should be 'rar'. The flag is 0 meaning that any file with an extension that isn't 'rar' is mis-labeled.

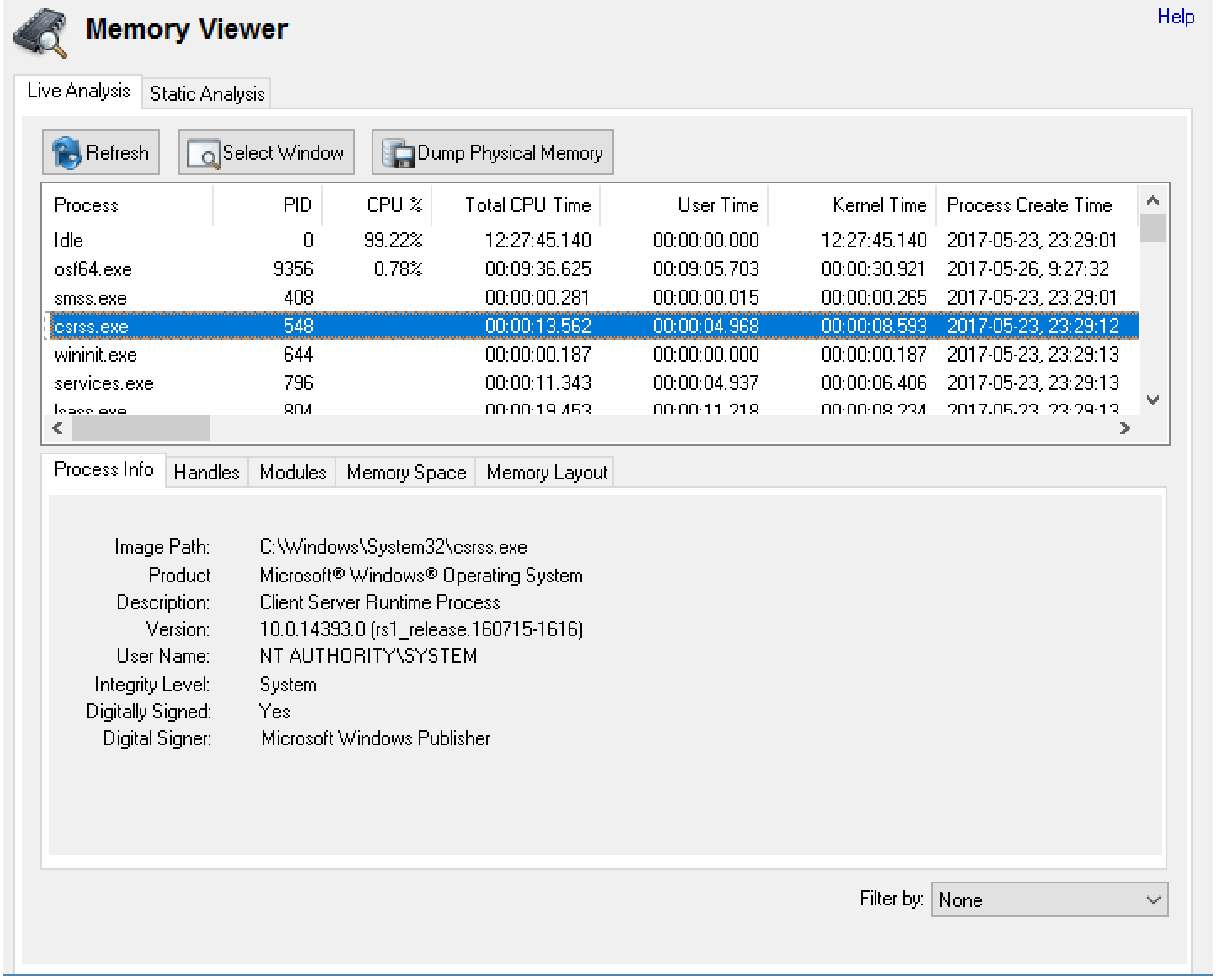
```
Text,htm,1
Text,txt,1
```

These two lines specify that files that have been identified as with 'Text' in their description can be either 'htm' or 'txt'. The '1' specifies files with other extensions that are text files are not necessarily mis-labeled.

4.7 Memory Viewer

The Memory Viewer module allows the user to perform memory forensics analysis on a live system or a static memory dump. There are 2 types of memory analysis that can be performed:

- Live Analysis
- Static Analysis



Process	PID	CPU %	Total CPU Time	User Time	Kernel Time	Process Create Time
Idle	0	99.22%	12:27:45.140	00:00:00.000	12:27:45.140	2017-05-23, 23:29:01
osf64.exe	9356	0.78%	00:09:36.625	00:09:05.703	00:00:30.921	2017-05-26, 9:27:32
smss.exe	408		00:00:00.281	00:00:00.015	00:00:00.265	2017-05-23, 23:29:01
csrss.exe	548		00:00:13.562	00:00:04.968	00:00:08.593	2017-05-23, 23:29:12
wininit.exe	644		00:00:00.187	00:00:00.000	00:00:00.187	2017-05-23, 23:29:13
services.exe	796		00:00:11.343	00:00:04.937	00:00:06.406	2017-05-23, 23:29:13
lsass.exe	804		00:00:19.453	00:00:11.218	00:00:08.234	2017-05-23, 23:29:13

Image Path: C:\Windows\System32\csrss.exe
Product: Microsoft® Windows® Operating System
Description: Client Server Runtime Process
Version: 10.0.14393.0 (rs1_release.160715-1616)
User Name: NT AUTHORITY\SYSTEM
Integrity Level: System
Digitally Signed: Yes
Digital Signer: Microsoft Windows Publisher

Filter by: None

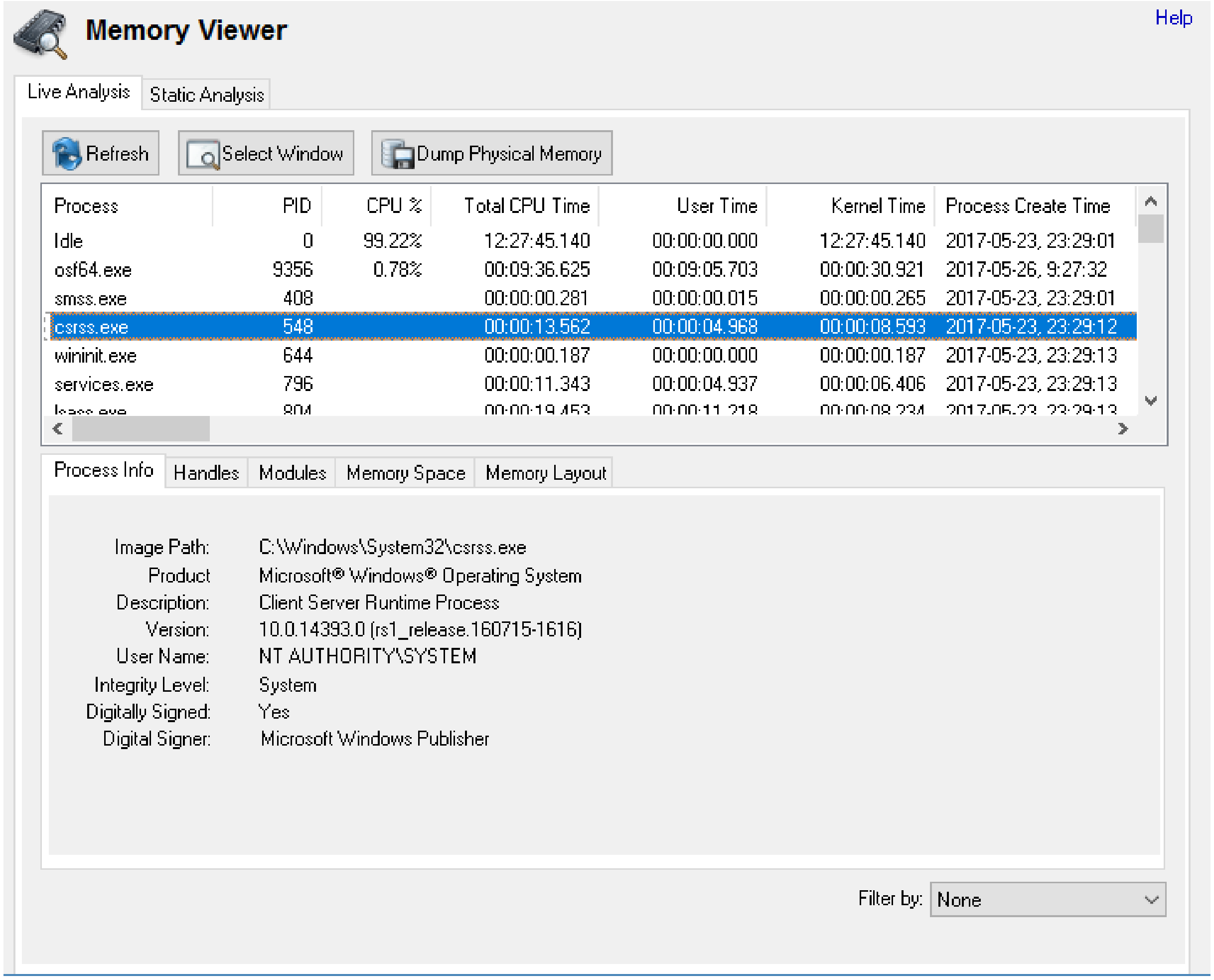
When performing 'Live Analysis', the memory details of all processes currently running on the system is displayed in a Task Manager-like view. Unlike non-volatile hard disks which can be analyzed statically, memory contents (RAM) can only be analyzed while the system is live. Furthermore, it is possible that potentially implicating evidence exists only in the system's physical memory, without any traces on the hard disk. This matter is complicated further if the data only exists in memory for a brief period of time.

'Static Analysis' allows an investigator to perform an analysis of a memory snapshot dump that had been taken recently. The results of a static analysis can include the following:

- List of processes that were running
- List of suspicious processes
- Installed drivers
- Detected Malware

4.7.1 Live Analysis

The Live Analysis tab of the Memory Viewer displays the real-time information of the processes that are running on the system.



Process	PID	CPU %	Total CPU Time	User Time	Kernel Time	Process Create Time
Idle	0	99.22%	12:27:45.140	00:00:00.000	12:27:45.140	2017-05-23, 23:29:01
osf64.exe	9356	0.78%	00:09:36.625	00:09:05.703	00:00:30.921	2017-05-26, 9:27:32
smss.exe	408		00:00:00.281	00:00:00.015	00:00:00.265	2017-05-23, 23:29:01
csrss.exe	548		00:00:13.562	00:00:04.968	00:00:08.593	2017-05-23, 23:29:12
wininit.exe	644		00:00:00.187	00:00:00.000	00:00:00.187	2017-05-23, 23:29:13
services.exe	796		00:00:11.343	00:00:04.937	00:00:06.406	2017-05-23, 23:29:13
lsass.exe	804		00:00:19.453	00:00:11.218	00:00:08.234	2017-05-23, 23:29:13

Image Path: C:\Windows\System32\csrss.exe
Product: Microsoft® Windows® Operating System
Description: Client Server Runtime Process
Version: 10.0.14393.0 (rs1_release.160715-1616)
User Name: NT AUTHORITY\SYSTEM
Integrity Level: System
Digitally Signed: Yes
Digital Signer: Microsoft Windows Publisher

Filter by: None

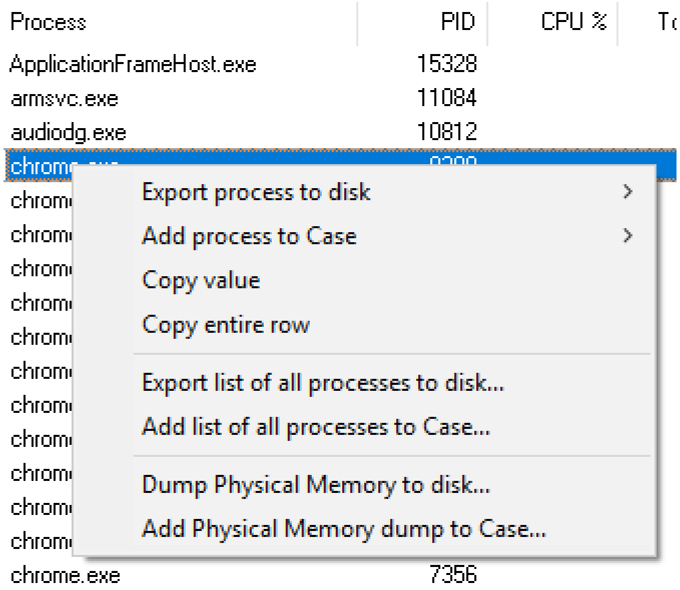
By selecting a process, the user may view the process information, virtual memory space and memory layout.

Refresh
Refreshes the list of active processes in the system.

Select Window
Allows the user to select a process by clicking on its window.

Dump Physical Memory
Dump the entire physical memory into a binary file. See Generating a Raw Memory Dump.

Right-clicking the process list view allows the user to save the list of processes to a CSV file.


Process
PID
CPU %
ApplicationFrameHost.exe 15328
armsvc.exe 11084
audiodg.exe 10812
chrome.exe
chrome.exe 7356
Export process to disk
Add process to Case
Copy value
Copy entire row
Export list of all processes to disk...
Add list of all processes to Case...
Dump Physical Memory to disk...
Add Physical Memory dump to Case...

Export process to disk

Process Details
Take a snapshot of the selected process details and save as CSV on disk

Process Memory Snapshot
Take a memory dump snapshot of the selected process details and save as a binary file on disk

Add process to Case
Take a snapshot of process details or memory dump of the selected process and add to the case.

Copy value
Copy the text of the selected cell to clipboard

Copy entire
Copy the text of the selected row to clipboard

Export list of all processes to disk...
Take a snapshot of the list of all running processes and save as CSV on disk

Add list of all processes to Case...
Take a snapshot of the list of all running processes and add to the case.

Dump Physical Memory to disk...
Dump the entire physical memory into a binary file on disk. See Generating a Raw Memory Dump.

Add Physical Memory dump to Case...
Dump the entire physical memory and add to the case. See Generating a Raw Memory Dump.

Process Info

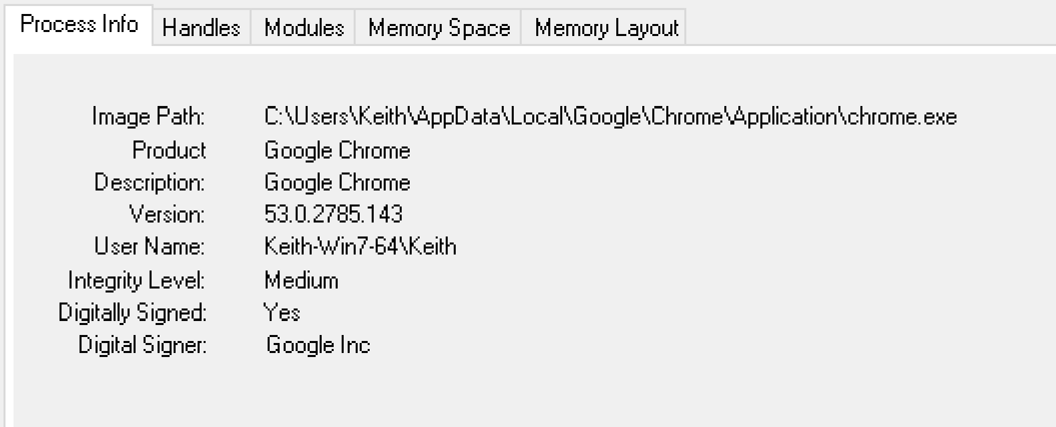
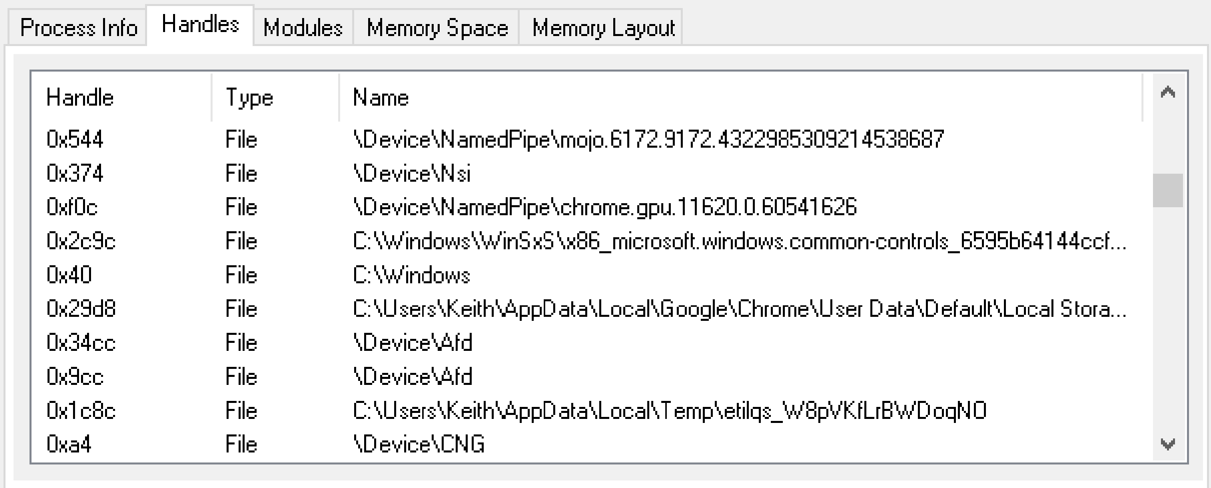


Image Path:	C:\Users\Keith\AppData\Local\Google\Chrome\Application\chrome.exe
Product	Google Chrome
Description:	Google Chrome
Version:	53.0.2785.143
User Name:	Keith-Win7-64\Keith
Integrity Level:	Medium
Digitally Signed:	Yes
Digital Signer:	Google Inc

This view shows the details of the application whose process was created.

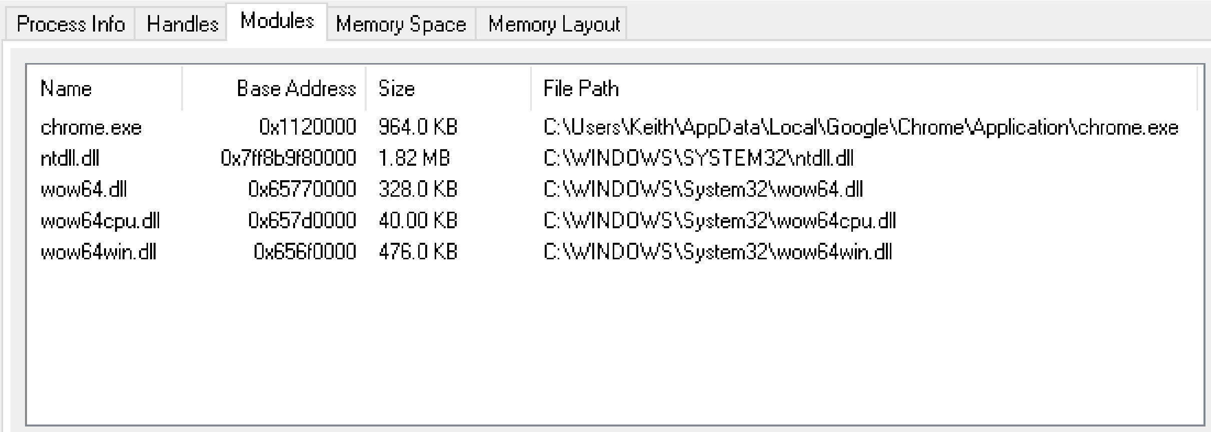
Handles



Handle	Type	Name
0x544	File	\Device\NamedPipe\mojo.6172.9172.4322985309214538687
0x374	File	\Device\Nsi
0xf0c	File	\Device\NamedPipe\chrome.gpu.11620.0.60541626
0x2c9c	File	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf...
0x40	File	C:\Windows
0x29d8	File	C:\Users\Keith\AppData\Local\Google\Chrome\User Data\Default\Local Stora...
0x34cc	File	\Device\Afd
0x9cc	File	\Device\Afd
0x1c8c	File	C:\Users\Keith\AppData\Local\Temp\etilqs_W8pVKfLrBWDoqNO
0xa4	File	\Device\CNG

This view shows the list of handles used by the process, including the handle type and name (if available).

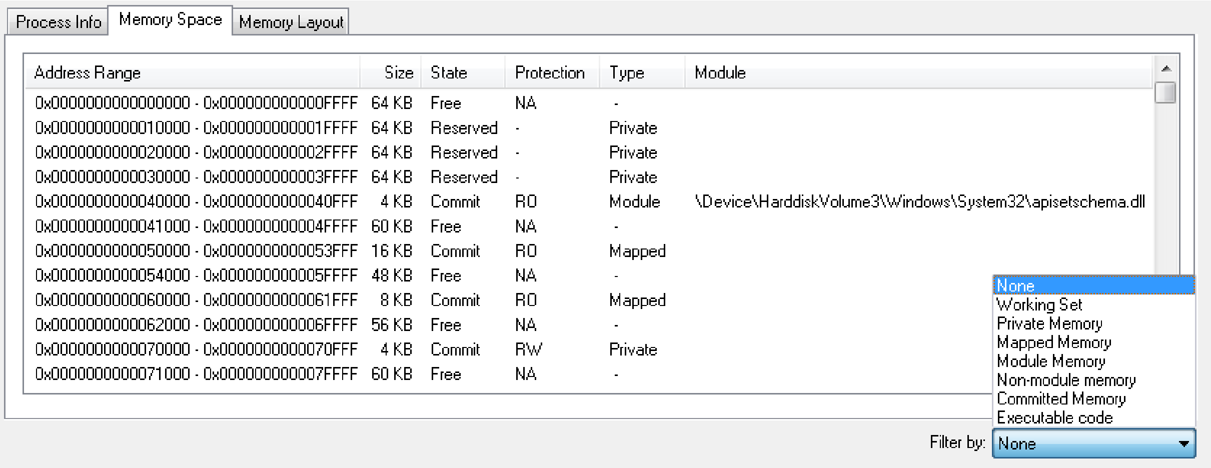
Modules



Name	Base Address	Size	File Path
chrome.exe	0x1120000	964.0 KB	C:\Users\Keith\AppData\Local\Google\Chrome\Application\chrome.exe
ntdll.dll	0x7ff8b9f80000	1.82 MB	C:\WINDOWS\SYSTEM32\ntdll.dll
wow64.dll	0x65770000	328.0 KB	C:\WINDOWS\System32\wow64.dll
wow64cpu.dll	0x657d0000	40.00 KB	C:\WINDOWS\System32\wow64cpu.dll
wow64win.dll	0x656f0000	476.0 KB	C:\WINDOWS\System32\wow64win.dll

This view shows the list of modules loaded by the process, including the location in process memory and the file path of the module.

Memory Space



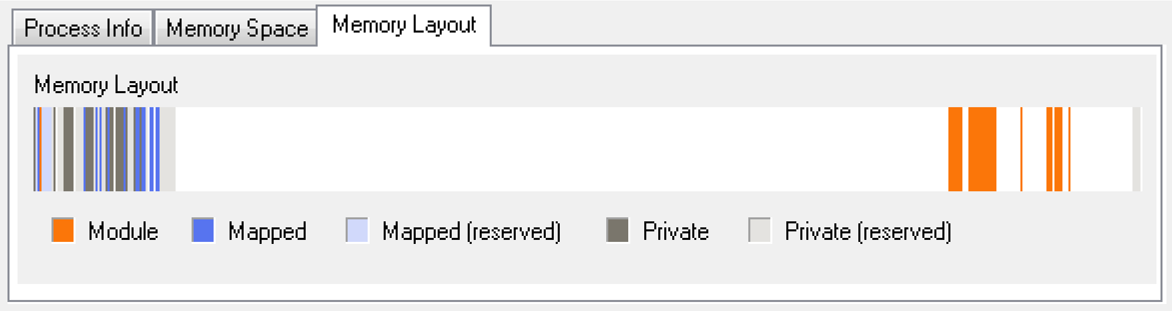
Address Range	Size	State	Protection	Type	Module
0x0000000000000000 - 0x000000000000FFFF	64 KB	Free	NA	-	
0x0000000000010000 - 0x000000000001FFFF	64 KB	Reserved	-	Private	
0x0000000000020000 - 0x000000000002FFFF	64 KB	Reserved	-	Private	
0x0000000000030000 - 0x000000000003FFFF	64 KB	Reserved	-	Private	
0x0000000000040000 - 0x0000000000040FFF	4 KB	Commit	RO	Module	\Device\HarddiskVolume3\Windows\System32\apisetschema.dll
0x0000000000041000 - 0x000000000004FFFF	60 KB	Free	NA	-	
0x0000000000050000 - 0x0000000000053FFF	16 KB	Commit	RO	Mapped	
0x0000000000054000 - 0x000000000005FFFF	48 KB	Free	NA	-	
0x0000000000060000 - 0x0000000000061FFF	8 KB	Commit	RO	Mapped	
0x0000000000062000 - 0x000000000006FFFF	56 KB	Free	NA	-	
0x0000000000070000 - 0x0000000000070FFF	4 KB	Commit	RW	Private	
0x0000000000071000 - 0x000000000007FFFF	60 KB	Free	NA	-	

Filter by: None

This view shows the process' memory allocation within its virtual address space. Double clicking on a memory section opens the Internal Viewer. Right-clicking a memory section allows the user to dump the memory contents into a file (See Generating a Raw Memory Dump). The memory sections can also be filtered based on the following criteria:

- *None* - The entire process (user) memory space is displayed
- *Working Set* - Only the memory sections that are in physical RAM are displayed
- *Private* - Only the memory sections that are private are displayed
- *Mapped* - Only the memory sections that are mapped are displayed
- *Module* - Only the memory sections that are part of an image are displayed
- *Non-module* - All memory sections that are not part of an image are displayed
- *Committed* - Only the memory sections that are in a commit state are displayed
- *Executable code* - Only the memory sections that have execute permissions are displayed

Memory Layout



This view shows a graphical layout of the allocated memory sections within the process virtual address space.

4.7.1.1 Generating a Raw Memory Dump

Using the OSForensics Memory Viewer, the user may perform a raw memory dump of a particular process' virtual memory space or the entire system's physical memory space.

Performing a process memory dump saves the contents of a process' virtual memory space (both in physical memory or paged out to hard disk) into a file. This is useful especially if there is a specific process that the user has identified to potentially contain information of interest.

Generating a raw physical memory dump takes a snapshot of the system's physical RAM contents, allowing the user to perform a static analysis of the raw memory contents. Since the contents of physical RAM are valid only when the system is live, performing a physical memory dump saves the RAM contents in a persistent state allowing for a more thorough analysis at a later time. Information that can be extracted from a raw physical memory dump includes the following:

- Printable strings (such as passwords, addresses, phone numbers, e-mail addresses)
- Kernel data structures (such as process list, thread list, module list)

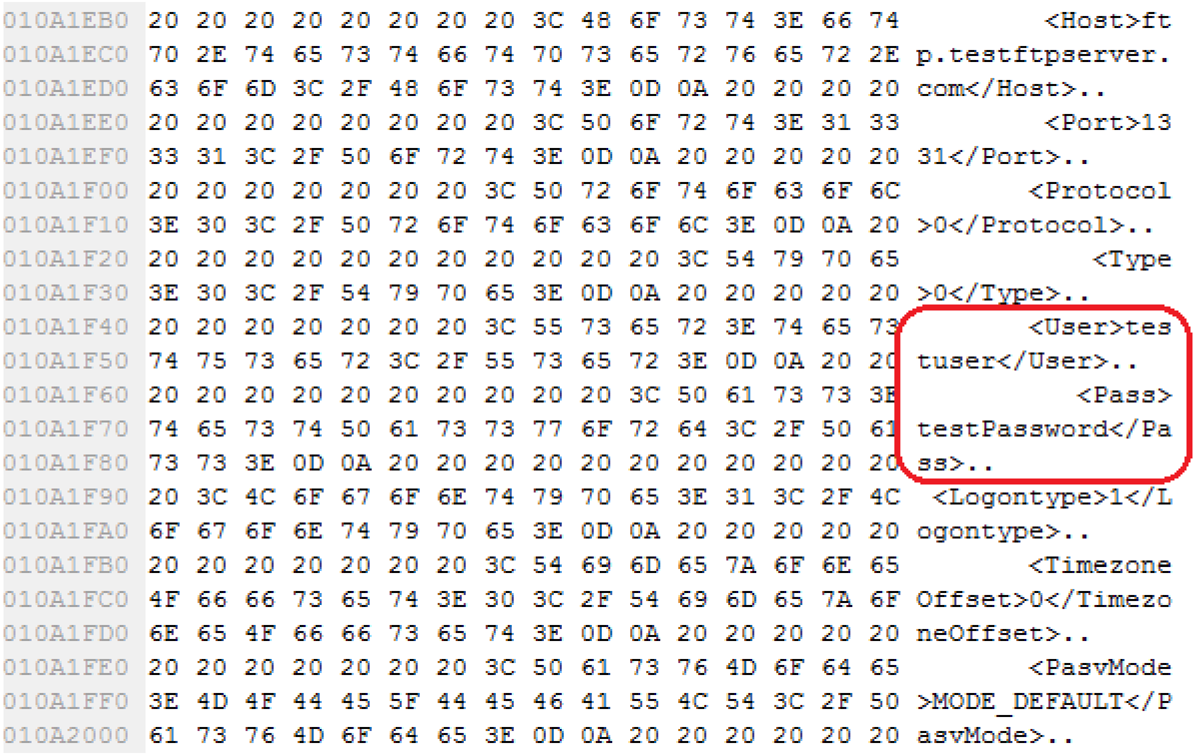
There are a variety of commercial and free 3rd party tools that scans raw physical memory dump files and extracts information that could be useful for forensic investigations. A physical memory dump, however, will unlikely contain the collective memory space of all processes running on the system. This is due to the fact that only a portion of a process' memory space resides in physical memory; the remaining portions reside in a page file on the hard disk.

Password Retrieval Example

To demonstrate a simple case of retrieving a password string from memory, we use a popular FTP client as an example. We configure a connection to a dummy FTP server using these parameters:

```
Host:          ftp.testftpserver.com
Port           1331
User           testuser
Password testPassword
```

After inputting these parameters, we attempt to connect to the dummy FTP server. While the FTP client is trying to connect to the non-existent server, we generate a raw memory dump of the FTP process using OSForensics. Using the OSForensics internal viewer (or any hex viewer/editor), we perform a simple search for our password string 'testPassword'. The screenshot below reveals the result of the string search.



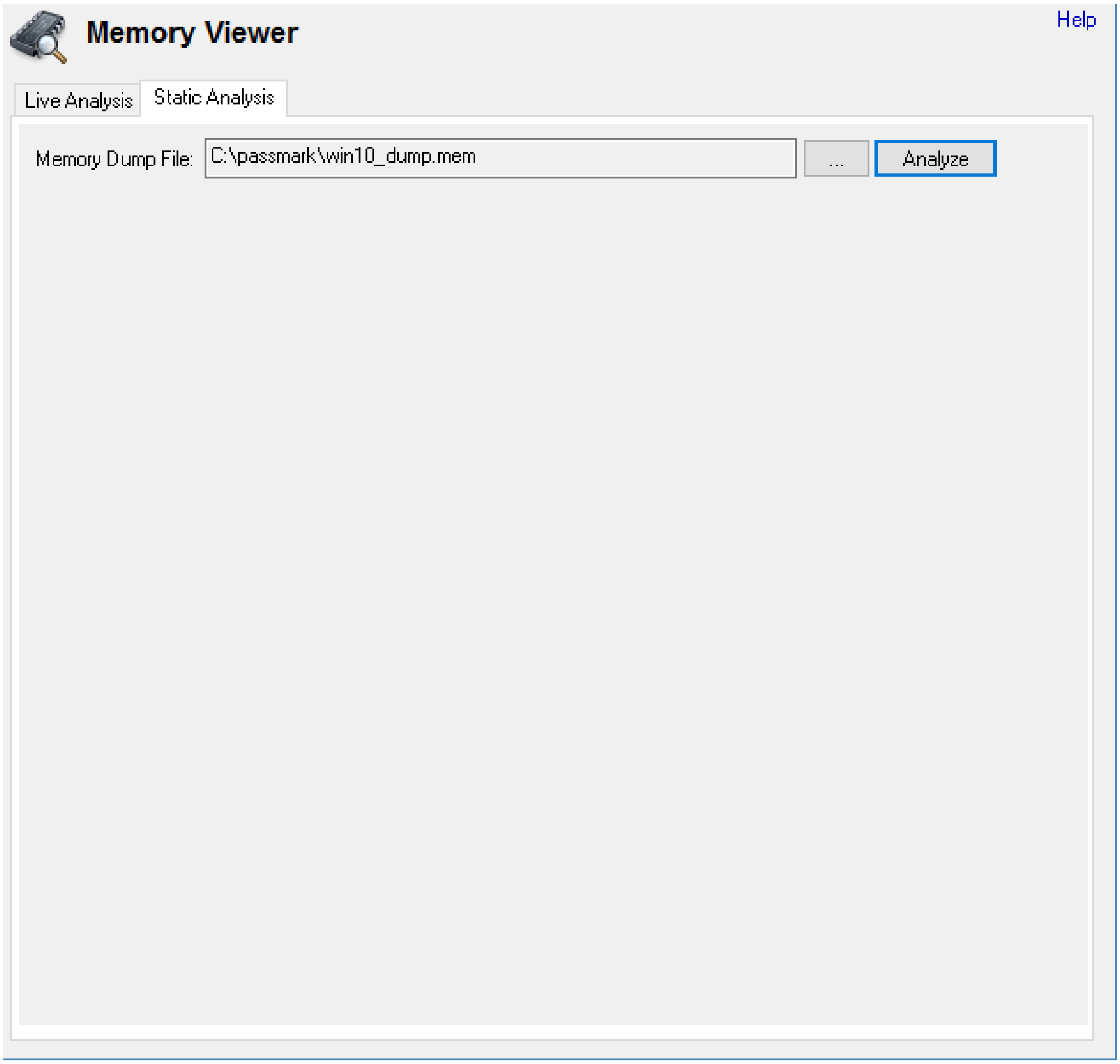
```
010A1EB0 20 20 20 20 20 20 20 20 3C 48 6F 73 74 3E 66 74         <Host>ft
010A1EC0 70 2E 74 65 73 74 66 74 70 73 65 72 76 65 72 2E p.testftpserver.
010A1ED0 63 6F 6D 3C 2F 48 6F 73 74 3E 0D 0A 20 20 20 20 com</Host>..
010A1EE0 20 20 20 20 20 20 20 20 3C 50 6F 72 74 3E 31 33         <Port>13
010A1EF0 33 31 3C 2F 50 6F 72 74 3E 0D 0A 20 20 20 20 20 31</Port>..
010A1F00 20 20 20 20 20 20 20 3C 50 72 6F 74 6F 63 6F 6C        <Protocol
010A1F10 3E 30 3C 2F 50 72 6F 74 6F 63 6F 6C 3E 0D 0A 20 >0</Protocol>..
010A1F20 20 20 20 20 20 20 20 20 20 20 20 3C 54 79 70 65            <Type
010A1F30 3E 30 3C 2F 54 79 70 65 3E 0D 0A 20 20 20 20 20 >0</Type>..
010A1F40 20 20 20 20 20 20 20 3C 55 73 65 72 3E 74 65 73        <User>tes
010A1F50 74 75 73 65 72 3C 2F 55 73 65 72 3E 0D 0A 20 20 tuser</User>..
010A1F60 20 20 20 20 20 20 20 20 20 20 3C 50 61 73 73 3E           <Pass>
010A1F70 74 65 73 74 50 61 73 73 77 6F 72 64 3C 2F 50 61 testPassword</Pa
010A1F80 73 73 3E 0D 0A 20 20 20 20 20 20 20 20 20 20 20 ss>..
010A1F90 20 3C 4C 6F 67 6F 6E 74 79 70 65 3E 31 3C 2F 4C  <Logontype>1</L
010A1FA0 6F 67 6F 6E 74 79 70 65 3E 0D 0A 20 20 20 20 20 ogontype>..
010A1FB0 20 20 20 20 20 20 20 3C 54 69 6D 65 7A 6F 6E 65        <Timezone
010A1FC0 4F 66 66 73 65 74 3E 30 3C 2F 54 69 6D 65 7A 6F Offset>0</Timezo
010A1FD0 6E 65 4F 66 66 73 65 74 3E 0D 0A 20 20 20 20 20 neOffset>..
010A1FE0 20 20 20 20 20 20 20 3C 50 61 73 76 4D 6F 64 65        <PasvMode
010A1FF0 3E 4D 4F 44 45 5F 44 45 46 41 55 4C 54 3C 2F 50 >MODE_DEFAULT</P
010A2000 61 73 76 4D 6F 64 65 3E 0D 0A 20 20 20 20 20 20 asvMode>..
```

We can see that the password is stored as plain text in the process' memory. Using this information, a forensics investigator may gain access to a remote machine containing evidence files that could implicate the suspected criminal.

4.7.2 Static Analysis

A full physical memory dump contains valuable information about the state of the system when the snapshot was taken. The Static Analysis tab of the Memory Viewer allows an investigator to analyze a memory dump file in order to extract valuable information such as:

- List of processes that were running
- List of suspicious processes
- Installed drivers
- Detected Malware



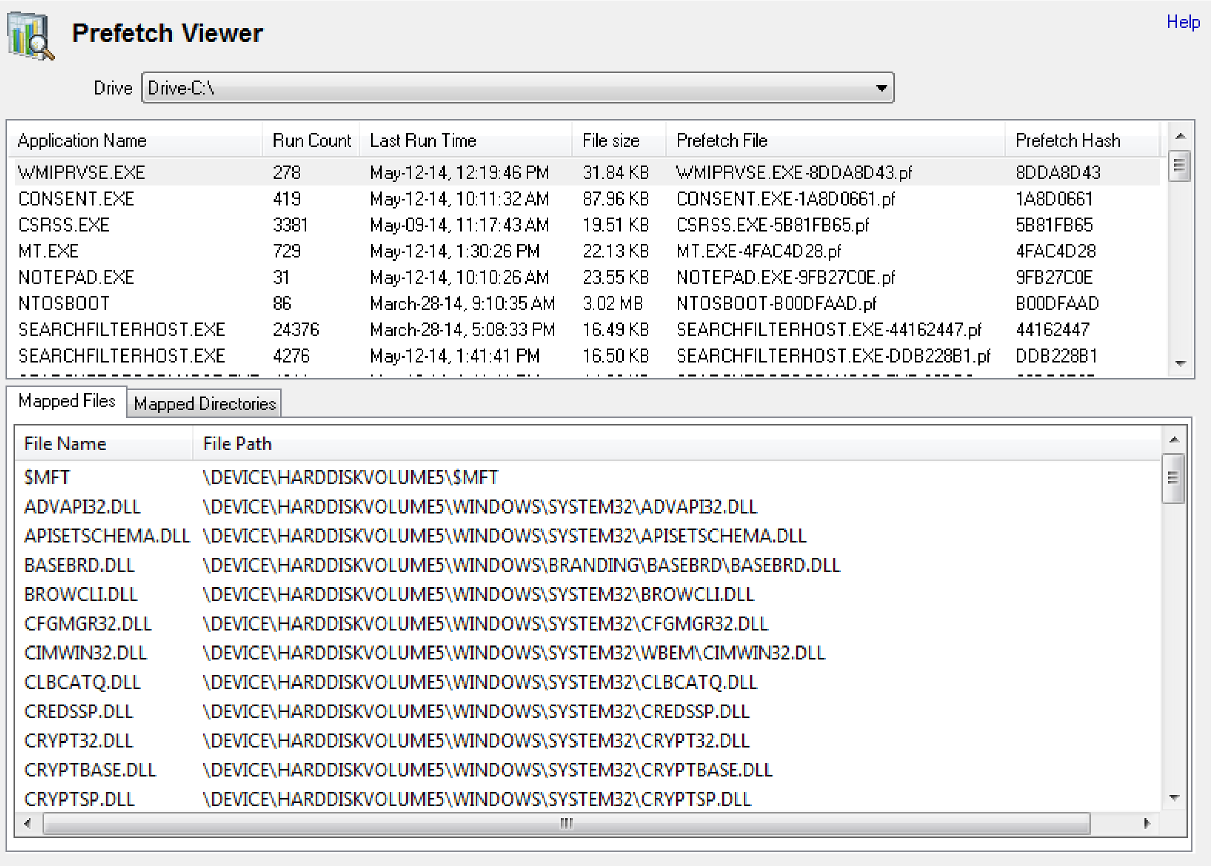
Memory Dump File: C:\passmark\win10_dump.mem

To analyze a memory dump file, browse to the location of the file and click Analyze. This shall launch Volatility Workbench, a GUI application for the Volatility tool.

Volatility is a command line memory analysis and forensics tool for extracting artifacts from memory dumps.

4.8 Prefetch Viewer

The Prefetch Viewer module allows the user to view the potentially valuable forensic information stored by the operating system's Prefetcher. The Prefetcher is a component that improves the performance of the system by pre-caching applications and its associated files into RAM, reducing disk access. To facilitate this, the Prefetcher collects application usage details such as the number of times the application has been executed, the last run time, and any files that the application uses when it is running. Using this information, forensics investigators can uncover suspect's application usage patterns (eg. "Cleaner" software used recently) and files that have been opened (eg. documents).



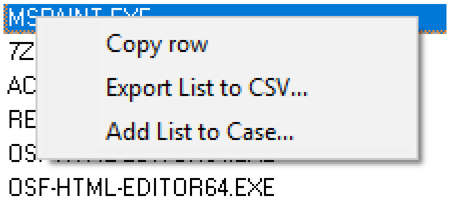
Prefetch Viewer

Drive: Drive-C:\

Application Name	Run Count	Last Run Time	File size	Prefetch File	Prefetch Hash
WMIPRVSE.EXE	278	May-12-14, 12:19:46 PM	31.84 KB	WMIPRVSE.EXE-8DDA8D43.pf	8DDA8D43
CONSENT.EXE	419	May-12-14, 10:11:32 AM	87.96 KB	CONSENT.EXE-1A8D0661.pf	1A8D0661
CSRSS.EXE	3381	May-09-14, 11:17:43 AM	19.51 KB	CSRSS.EXE-5B81FB65.pf	5B81FB65
MT.EXE	729	May-12-14, 1:30:26 PM	22.13 KB	MT.EXE-4FAC4D28.pf	4FAC4D28
NOTEPAD.EXE	31	May-12-14, 10:10:26 AM	23.55 KB	NOTEPAD.EXE-9FB27C0E.pf	9FB27C0E
NTOSBOOT	86	March-28-14, 9:10:35 AM	3.02 MB	NTOSBOOT-B00DFAAD.pf	B00DFAAD
SEARCHFILTERHOST.EXE	24376	March-28-14, 5:08:33 PM	16.49 KB	SEARCHFILTERHOST.EXE-44162447.pf	44162447
SEARCHFILTERHOST.EXE	4276	May-12-14, 1:41:41 PM	16.50 KB	SEARCHFILTERHOST.EXE-DDB228B1.pf	DDB228B1

File Name	File Path
$MFT	\DEVICE\HARDDISKVOLUME5\$MFT
ADVAPI32.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\ADVAPI32.DLL
APISETSCHEMA.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\APISETSCHEMA.DLL
BASEBRD.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\BRANDING\BASEBRD\BASEBRD.DLL
BROWCLI.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\BROWCLI.DLL
CFGMGR32.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\CFGMGR32.DLL
CIMWIN32.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\WBEM\CIMWIN32.DLL
CLBCATQ.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\CLBCATQ.DLL
CREDSSP.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\CREDSSP.DLL
CRYPT32.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\CRYPT32.DLL
CRYPTBASE.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\CRYPTBASE.DLL
CRYPTSP.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\CRYPTSP.DLL

Right-clicking an application entry brings up the following menu:



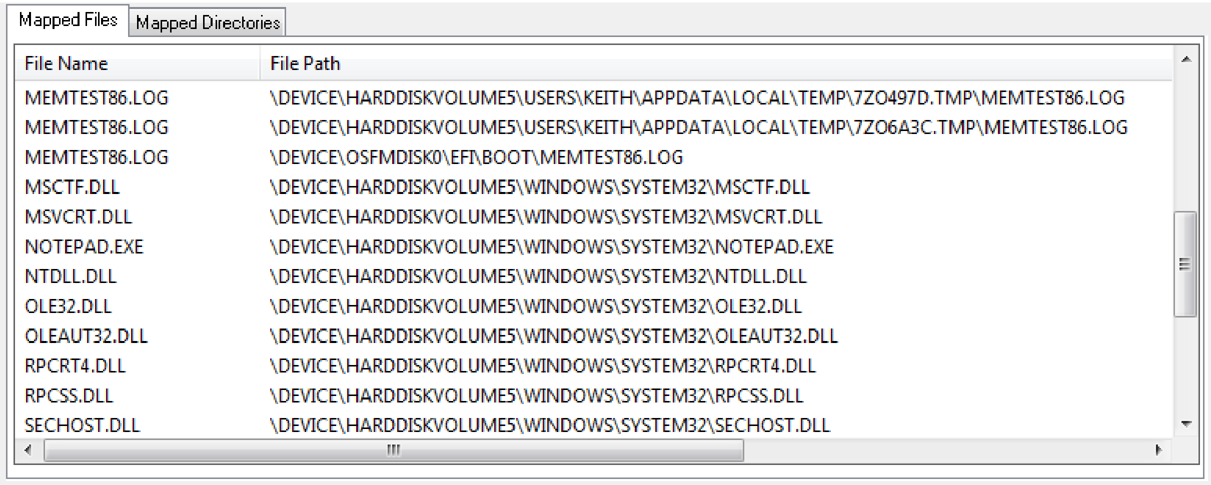
Copy row
Copies the selected prefetch item details to clipboard

Export List to CSV...
Export the list of prefetch items to a CSV file

Add List to Case...
Add the list of prefetch items to case as a CSV file

After selecting an application, the list of mapped files and directories used by the application is displayed.

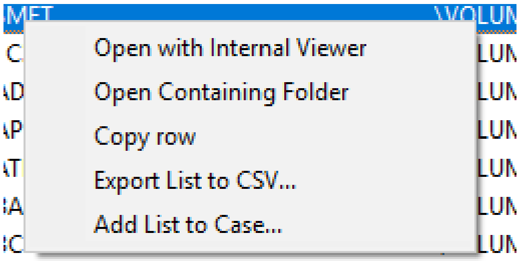
Mapped Files



File Name	File Path
MEMTEST86.LOG	\DEVICE\HARDDISKVOLUME5\USERS\KEITH\APPDATA\LOCAL\TEMP\7ZO497D.TMP\MEMTEST86.LOG
MEMTEST86.LOG	\DEVICE\HARDDISKVOLUME5\USERS\KEITH\APPDATA\LOCAL\TEMP\7ZO6A3C.TMP\MEMTEST86.LOG
MEMTEST86.LOG	\DEVICE\OSFMDISK0\EFI\BOOT\MEMTEST86.LOG
MSCTF.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\MSCTF.DLL
MSVCRT.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\MSVCRT.DLL
NOTEPAD.EXE	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\NOTEPAD.EXE
NTDLL.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\NTDLL.DLL
OLE32.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\OLE32.DLL
OLEAUT32.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\OLEAUT32.DLL
RPCRT4.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\RPCRT4.DLL
RPCSS.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\RPCSS.DLL
SECHOST.DLL	\DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32\SECHOST.DLL

This list view contains a ten-second snapshot of the list of files that were used by the application while executing. This includes the binary itself, associated system DLL files and files opened by the user using the application (such as document files for Microsoft Word). Forensically, this can reveal files of interest that were opened by the application (eg. document, image, e-mail files) and file paths that may have been hidden or no longer exists.

Right-clicking a file entry brings up the following menu:



Open with Internal Viewer
Attempts to locate the file on the drive and open it using the Internal Viewer.

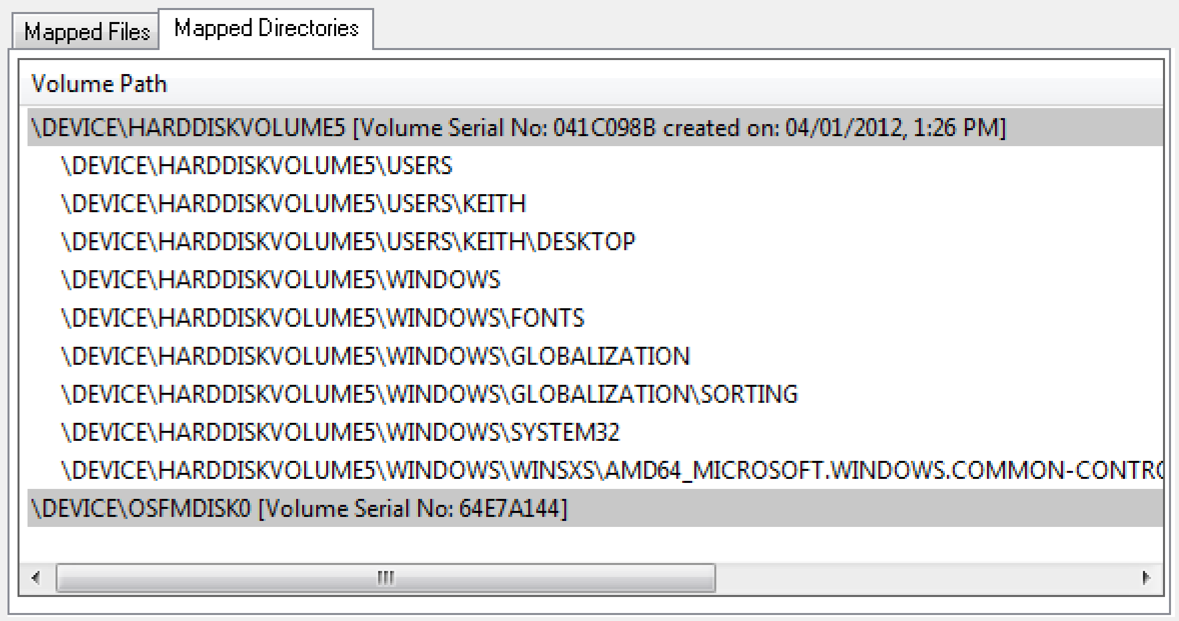
Open Containing Folder
Attempts to open the parent folder of the selected file

Copy row
Copy the file entry details to clipboard

Export List to CSV...
Export the list of mapped file entries to a CSV file

Add List to Case...
Add the list of mapped file entries to case as a CSV file

Mapped Directories

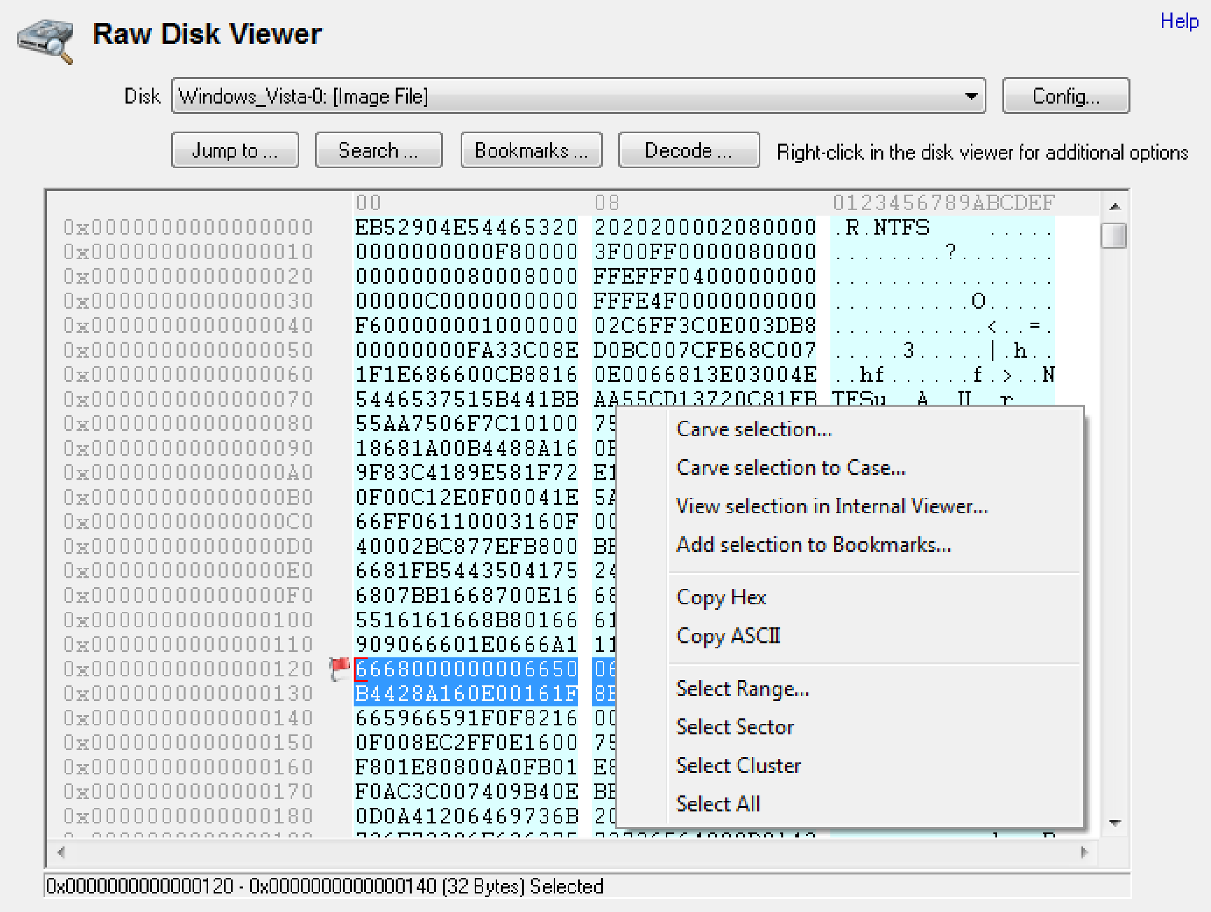


```
\DEVICE\HARDDISKVOLUME5 [Volume Serial No: 041C098B created on: 04/01/2012, 1:26 PM]
    \DEVICE\HARDDISKVOLUME5\USERS
    \DEVICE\HARDDISKVOLUME5\USERS\KEITH
    \DEVICE\HARDDISKVOLUME5\USERS\KEITH\DESKTOP
    \DEVICE\HARDDISKVOLUME5\WINDOWS
    \DEVICE\HARDDISKVOLUME5\WINDOWS\FONTS
    \DEVICE\HARDDISKVOLUME5\WINDOWS\GLOBALIZATION
    \DEVICE\HARDDISKVOLUME5\WINDOWS\GLOBALIZATION\SORTING
    \DEVICE\HARDDISKVOLUME5\WINDOWS\SYSTEM32
    \DEVICE\HARDDISKVOLUME5\WINDOWS\WINSXS\AMD64_MICROSOFT.WINDOWS.COMMON-CONTR
\DEVICE\OSFMDISK0 [Volume Serial No: 64E7A144]
```

This list view contains a list of directories and corresponding volumes that were accessed by the application while executing. This can be used to identify volumes and directory paths that may have been hidden or belonged to a removable disk.

4.9 Raw Disk Viewer

The Raw Disk Viewer module allows the user to analyze the raw sectors of all devices added to the case, along with all physical disks and partitions (including mounted images) attached to the system. This module provides the ability to perform a deeper inspection of a drive, looking beyond the data stored in the file system's files and directories. Performing this level of analysis may be required if information of interest is suspected to be hidden within the raw sectors of the drive, which are not normally accessible via normal operating system mechanisms (eg. free clusters, file slack space).

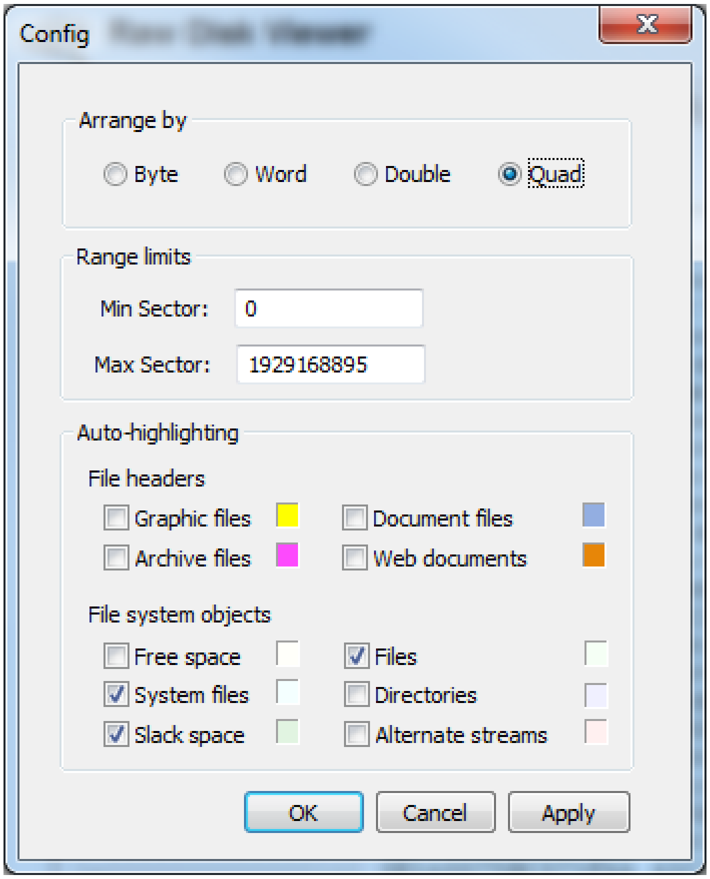

Raw Disk Viewer
Help
Disk
Windows_Vista-0: [Image File]
Config...
Jump to ...
Search ...
Bookmarks ...
Decode ...
Right-click in the disk viewer for additional options
Carve selection...
Carve selection to Case...
View selection in Internal Viewer...
Add selection to Bookmarks...
Copy Hex
Copy ASCII
Select Range...
Select Sector
Select Cluster
Select All

```
                    00                08                0123456789ABCDEF
0x0000000000000000  EB52904E54465320  2020200002080000  .R.NTFS    .....
0x0000000000000010  0000000000F80000  3F00FF0000080000  ........?.......
0x0000000000000020  0000000080008000  FFEFFF0400000000  ................
0x0000000000000030  00000C0000000000  FFFE4F0000000000  ..........O.....
0x0000000000000040  F600000001000000  02C6FF3C0E003DB8  ...........<..=.
0x0000000000000050  00000000FA33C08E  D0BC007CFB68C007  .....3.....|.h..
0x0000000000000060  1F1E686600CB8816  0E0066813E03004E  ..hf......f.>..N
0x0000000000000070  5446537515B441BB  AA55CD13720C81FB  TFSu  A  U  r
0x0000000000000080  55AA7506F7C10100  75
0x0000000000000090  18681A00B4488A16  0E
0x00000000000000A0  9F83C4189E581F72  E1
0x00000000000000B0  0F00C12E0F00041E  5A
0x00000000000000C0  66FF06110003160F  00
0x00000000000000D0  40002BC877EFB800  BE
0x00000000000000E0  6681FB5443504175  24
0x00000000000000F0  6807BB1668700E16  68
0x0000000000000100  5516161668B80166  61
0x0000000000000110  909066601E0666A1  11
0x0000000000000120  6668000000006650  06
0x0000000000000130  B4428A160E00161F  8E
0x0000000000000140  665966591F0F8216  00
0x0000000000000150  0F008EC2FF0E1600  75
0x0000000000000160  F801E80800A0FB01  E8
0x0000000000000170  F0AC3C007409B40E  BE
0x0000000000000180  0D0A41206469736B  20
```

0x0000000000000120 - 0x0000000000000140 (32 Bytes) Selected

To view the raw sectors of a drive, the user selects the device from the **Disk** drop-down box.

Config ...
Opens a dialog to configure the display settings of the viewer.



Config

Arrange by

○ Byte ○ Word ○ Double ● Quad

Range limits

Min Sector: 0

Max Sector: 1929168895

Auto-highlighting

File headers

□ Graphic files 🟨 □ Document files 🟦

□ Archive files 🟪 □ Web documents 🟧

File system objects

□ Free space ☑ Files

☑ System files □ Directories

☑ Slack space □ Alternate streams

Arrange by - Adjust how bytes are grouped on the viewer (1, 2, 4, 8 bytes respectively) .

Range limits - Configure the minimum and maximum sectors viewable on the currently selected drive

Auto-highlighting - Toggle auto-highlighting of bytes of interest

File headers

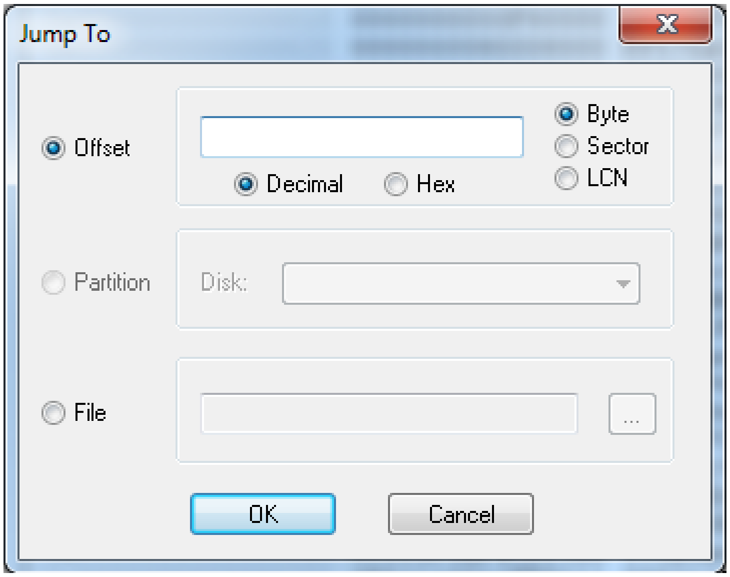
- *Graphic files* - gif, jpg, png, bmp
- *Archive files* - zip
- *Document files* - pdf, rtf
- *Web documents* - html

File system objects

- *Free space* - unallocated clusters of a partition
- *System files* - bytes internal to the disk/partition for bookkeeping/management purposes (eg. MBR, MFT)
- *Slack space* - allocated space unused by the file or volume
- *Files* - bytes occupied by files
- *Directories* - bytes used by directories to store indexing information
- *Alternate streams* - bytes occupied by files' alternate stream(s) (NTFS only)

Jump to ...

Allows the user to jump to a particular location on the raw disk.



Offset - Jump to the specified byte, sector, or LCN offset.

Partition - *(Physical disks only)* Jump to the start of the specified partition

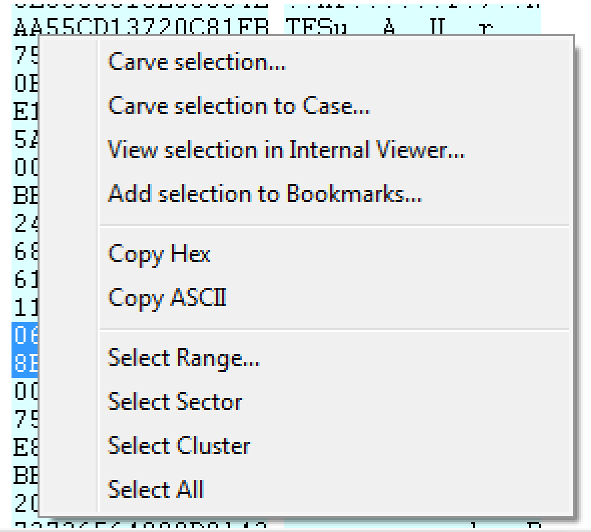
File - *(Valid file systems only)* Jump to the starting cluster of the specified file on the partition

Search ...
Opens a search window for locating hexadecimal/text patterns on the drive

Bookmarks ...
Opens the bookmark window for managing the bookmarks on the drive

Decode ...
Opens a separate decode window for displaying information about the current position in the viewer

Right Click Menu


Carve selection...
Carve selection to Case...
View selection in Internal Viewer...
Add selection to Bookmarks...
Copy Hex
Copy ASCII
Select Range...
Select Sector
Select Cluster
Select All

Carve selection...
Save the selected bytes into a file. If no selection is made, the current cluster is saved.

Carve selection to Case...
Save the selected bytes into a file, then add to case.

View Selection with Internal Viewer...
View the selected bytes in the OSForensics Viewer. If no selection is made, the current cluster is viewed.

Add selection to bookmarks...
Create a bookmark with the selected offset range. If no selection is made, a dialog prompting the user to create a bookmark is displayed.

Copy Hex
Copy the selected bytes as hex characters to clipboard

Copy ASCII
Copy the selected bytes as ASCII to clipboard

Select Range...
Prompts the user to enter a start and end offset to select

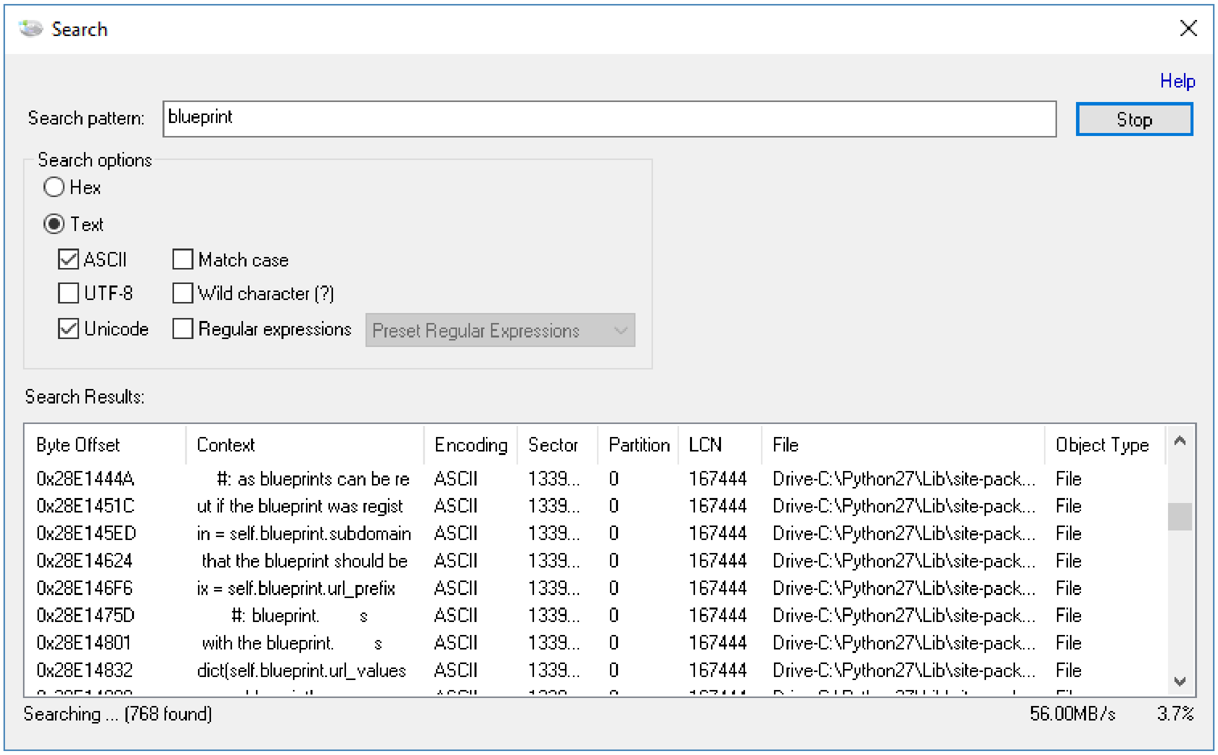
Select Sector
Select the sector that cursor is currently within

Select Cluster
Select the cluster that cursor is currently within

Select All
Select all bytes on the disk

4.9.1 Search Window

The Raw Disk Viewer search window allows the user to perform searches on the raw sectors of the current device. The search is performed sequentially from the first viewable sector of the device, with the results being updated instantaneously in the search results table.



Search pattern: blueprint

Search options

○ Hex

● Text

☑ ASCII ☐ Match case

☐ UTF-8 ☐ Wild character (?)

☑ Unicode ☐ Regular expressions Preset Regular Expressions

Search Results:

Byte Offset	Context	Encoding	Sector	Partition	LCN	File	Object Type
0x28E1444A	#: as blueprints can be re	ASCII	1339...	0	167444	Drive-C:\Python27\Lib\site-pack...	File
0x28E1451C	ut if the blueprint was regist	ASCII	1339...	0	167444	Drive-C:\Python27\Lib\site-pack...	File
0x28E145ED	in = self.blueprint.subdomain	ASCII	1339...	0	167444	Drive-C:\Python27\Lib\site-pack...	File
0x28E14624	that the blueprint should be	ASCII	1339...	0	167444	Drive-C:\Python27\Lib\site-pack...	File
0x28E146F6	ix = self.blueprint.url_prefix	ASCII	1339...	0	167444	Drive-C:\Python27\Lib\site-pack...	File
0x28E1475D	#: blueprint. s	ASCII	1339...	0	167444	Drive-C:\Python27\Lib\site-pack...	File
0x28E14801	with the blueprint. s	ASCII	1339...	0	167444	Drive-C:\Python27\Lib\site-pack...	File
0x28E14832	dict(self.blueprint.url_values	ASCII	1339...	0	167444	Drive-C:\Python27\Lib\site-pack...	File

Searching ... (768 found) 56.00MB/s 3.7%

Search pattern

The search string to locate on the drive

Search Options

Hex

Search for a particular hex pattern on the drive. The hex pattern must be in byte increments, and must contain only valid hexadecimal characters (0-9, a-f).

Text

Search for the specified text string on the drive

ASCII - If checked, search for the text pattern in ASCII

UTF-8 - If checked, search for the text pattern in UTF-8

Unicode - If checked, search for the text pattern in Unicode

Match case - If checked, the search will be case sensitive

Wildcard character (?) - If checked, a '?' in the search pattern will match any single character. Wildcards cannot be used in conjunction with regular expressions.

Regular expressions - If checked, the search pattern shall be interpreted as a regular expression. The regular expression pattern can be user-specified or selected from the list of preset expressions. Regular expressions cannot be used in conjunction with wildcards. See Regular Expressions for syntax information and examples.

Search Results

Displays (in real-time) all instances of the search pattern found on the drive. Double clicking on a result will highlight the matching bytes in the Raw Disk Viewer. The maximum length of matching strings is 256 characters.

Byte offset - the starting byte offset

Context - the context (10 characters before and after) of where the pattern is found

*Encoding - o*ne of Hex, ASCII, UTF8, or Unicode

Sector - the starting logical sector

Partition - the partition number on the selected drive

LCN - the starting logical cluster number

File - (Partition only) the file which the found pattern belongs to. Note that this information is not available for physical disks.

Object Type - any particular property of the allocated space containing the found pattern. (Eg. File, directory, free space, slack space)

4.9.1.1 Regular Expressions

The Raw Disk Viewer regular expression search is a powerful tool for identifying patterns that match a particular search specification on the raw device. The syntax and semantics of the search specifications are similar to Perl 5 (but not completely compatible), as the PCRE library is used for regular expression parsing and matching. The following is a quick reference of the supported regular expression syntax (as taken from the PCRE man pages), as well as several examples of forensics-related regular expressions.

Basic Syntax

```
QUOTING

         \x         where x is non-alphanumeric is a literal x
         \Q...\E    treat enclosed characters as literal

CHARACTERS

         \a         alarm, that is, the BEL character (hex 07)
         \cx        "control-x", where x is any ASCII character
         \e         escape (hex 1B)
         \f         formfeed (hex 0C)
         \n         newline (hex 0A)
         \r         carriage return (hex 0D)
         \t         tab (hex 09)
         \ddd       character with octal code ddd, or backreference
         \xhh       character with hex code hh
         \x{hhh..}  character with hex code hhh..


CHARACTER TYPES

         .          any character except newline
         \C         one byte, even in UTF-8 mode (best avoided)
         \d         a decimal digit
         \D         a character that is not a decimal digit
         \h         a horizontal whitespace character
         \H         a character that is not a horizontal whitespace character
         \N         a character that is not a newline
         \p{xx}     a character with the xx property
         \P{xx}     a character without the xx property
         \R         a newline sequence
         \s         a whitespace character
         \S         a character that is not a whitespace character
         \v         a vertical whitespace character
         \V         a character that is not a vertical whitespace character
         \w         a "word" character
         \W         a "non-word" character
         \X         an extended Unicode sequence


GENERAL CATEGORY PROPERTIES FOR \p and \P

         C          Other
         Cc         Control
         Cf         Format
         Cn         Unassigned
         Co         Private use
         Cs         Surrogate

         L          Letter
         Ll         Lower case letter
         Lm         Modifier letter
         Lo         Other letter
         Lt         Title case letter
         Lu         Upper case letter
         L&         Ll, Lu, or Lt

         M          Mark
         Mc         Spacing mark
         Me         Enclosing mark
         Mn         Non-spacing mark

         N          Number
         Nd         Decimal number
         Nl         Letter number
         No         Other number

         P          Punctuation
         Pc         Connector punctuation
         Pd         Dash punctuation
         Pe         Close punctuation
         Pf         Final punctuation
         Pi         Initial punctuation
         Po         Other punctuation
         Ps         Open punctuation

         S          Symbol
         Sc         Currency symbol
         Sk         Modifier symbol
         Sm         Mathematical symbol
         So         Other symbol

         Z          Separator
         Zl         Line separator
         Zp         Paragraph separator
         Zs         Space separator

         Xan        Alphanumeric: union of properties L and N
         Xps        POSIX space: property Z or tab, NL, VT, FF, CR
         Xsp        Perl space: property Z or tab, NL, FF, CR
         Xwd        Perl word: property Xan or underscore


CHARACTER CLASSES

         [...]       positive character class
         [^...]      negative character class
         [x-y]       range (can be used for hex characters)
         [[:xxx:]]   positive POSIX named set
         [[:^xxx:]]  negative POSIX named set

         alnum       alphanumeric
         alpha       alphabetic
         ascii       0-127
         blank       space or tab
         cntrl       control character
         digit       decimal digit
         graph       printing, excluding space
         lower       lower case letter
         print       printing, including space
         punct       printing, excluding alphanumeric
         space       whitespace
         upper       upper case letter
         word        same as \w
         xdigit      hexadecimal digit


QUANTIFIERS

         ?           0 or 1, greedy
         ?+          0 or 1, possessive
         ??          0 or 1, lazy
         *           0 or more, greedy
         *+          0 or more, possessive
         *?          0 or more, lazy
         +           1 or more, greedy
         ++          1 or more, possessive
         +?          1 or more, lazy
         {n}         exactly n
         {n,m}       at least n, no more than m, greedy
         {n,m}+      at least n, no more than m, possessive
         {n,m}?      at least n, no more than m, lazy
         {n,}        n or more, greedy
         {n,}+       n or more, possessive
         {n,}?       n or more, lazy


ANCHORS AND SIMPLE ASSERTIONS

         \b          word boundary
         \B          not a word boundary
         ^           start of subject
         \A          start of subject
         $           end of subject; also before newline at end of subject
         \Z          end of subject; also before newline at end of subject
         \z          end of subject
         \G          first matching position in subject


ALTERNATION

         expr|expr|expr...
```

Forensics Regular Expression Examples

URL

```
http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/[a-zA-Z0-9_\-\.]*)*
```

Matches:

- http://www.w3.org/2001/XMLSchema-instance
- http://crl.microsoft.com/pki/crl/products/WinPCA.crl
- http://ocsp.verisign.com

Non-matches

- ftp://intel.com
- http://www.microsoft/

Email

```
[\w\.=-]+@[\w\.-]+\.[\w]{2,3}
```

Matches:

- user@domain.com
- user@domain.jp.org
- user@domain.au

Non-Matches:

- user
- user@
- @domain

Credit Cards (AMEX, VISA, MasterCard)

```
((4\d{3})|(5[1-5]\d{2}))(-?|\040?)(\d{4}(-?|\040?)){3}|^(3[4,7]\d{2})(-?|\040?)\d{6}(-?|\040?)\d{5}
```

Matches:

- 3728-026478-55578
- 4056 1038 2489 4098
- 5259489765789863

Non-Matches

- 3056-1478-9785-8698

IP addresses

```
((0|1[0-9]{0,2}|2[0-9]{0,1}|2[0-4][0-9]|25[0-5]|[3-9][0-9]{0,1})\.){3}(0|1[0-9]{0,2}|2[0-9]{0,1}|2[0-4][0-9]|25[0-5]|[3-9][0-9]{0,1})
```

Matches

- 10.0.1.1
- 192.196.1.119
- 255.255.255.255

Non-Matches

- 001.010.0.0
- 192.168.01.119
- 256.257.258.259

US Phone numbers (Optional area code)

```
\(?[\d]{3}\)?[\s-]?[\d]{3}[\s-]?[\d]{4}
```

Matches

- (610)5647894
- 415-983-1066
- 525 189 1658

Non-Matches

- (610)(415)9898
- 415-11-9898

Zipcodes

```
\d{5}(-\d{4})?
```

Matches

- 90654
- 00989
- 55145-1679

Non-Matches

- 90654-
- 55897-178
- 5987

US dates (mm/dd/yyyy or m/d/yy or m.d.yyyy)

```
([0]?[1-9]|[1][0-2])[./-]([0]?[1-9]|[1|2][0-9]|[3][0|1])[./-]
([0-9]{4}|[0-9]{2})
```

Matches

- 02.25.1980
- 12/30/2004
- 01/01/2011

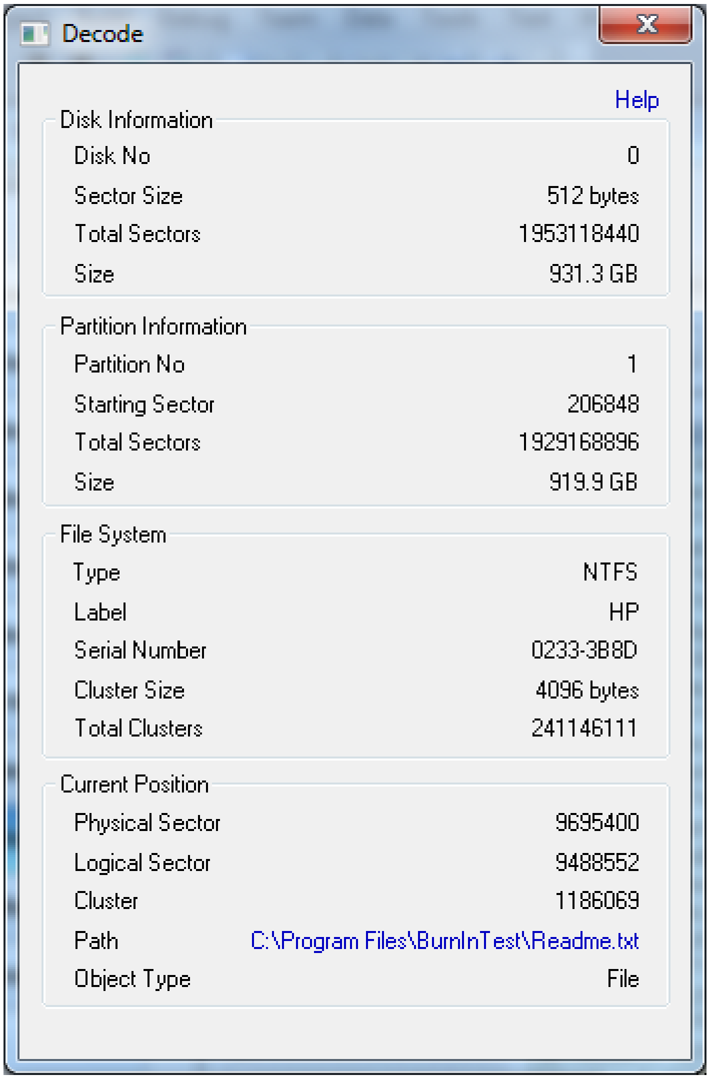
Non-Matches

- 02--25--1980
- 12-55-2004
- 13/12/2011

4.9.2 Decode Window

The Raw Disk Viewer decode windows provide detailed information about the current offset on the selected device. This information is updated in real time as the cursor is moved in the raw disk viewer.

Main Window



Disk Information

Disk No	0
Sector Size	512 bytes
Total Sectors	1953118440
Size	931.3 GB

Partition Information

Partition No	1
Starting Sector	206848
Total Sectors	1929168896
Size	919.9 GB

File System

Type	NTFS
Label	HP
Serial Number	0233-3B8D
Cluster Size	4096 bytes
Total Clusters	241146111

Current Position

Physical Sector	9695400
Logical Sector	9488552
Cluster	1186069
Path	C:\Program Files\BurnInTest\Readme.txt
Object Type	File

Disk Information

Disk No

The physical disk number of the selected device. Note that this information is not available for mounted images

Sector Size

The size of each sector in bytes

Total Sectors

The total number of sectors on the physical device. For mounted images, this is the number of sectors on the volume.

Size

The size of the physical device. For mounted images, this is the size of the volume.

Partition Information

Partition No

The partition number on the physical device. For mounted images, this is always zero.

Starting Sector
The physical sector offset of the partition on the physical device. For mounted images, this is always zero.

Total Sectors
The total number of sectors on the partition

Size
The size of the partition.

File System

Type
The file system type (eg. NTFS, FAT32)

Label
The volume label

Serial Number
The volume serial number

Cluster Size
The size of each cluster in bytes

Total Clusters
The total number of clusters in the volume

Current Position

Physical Sector
The sector number on the physical device of the current offset

Logical Sector
The sector number on the partition of the current offset

Cluster
The LCN (logical cluster number) on the volume of the current offset

File
The file path of the file that owns the current cluster. Clicking on the file path will open Windows Explorer to the location of the file. Note that this information is not available if the selected drive is a physical disk.

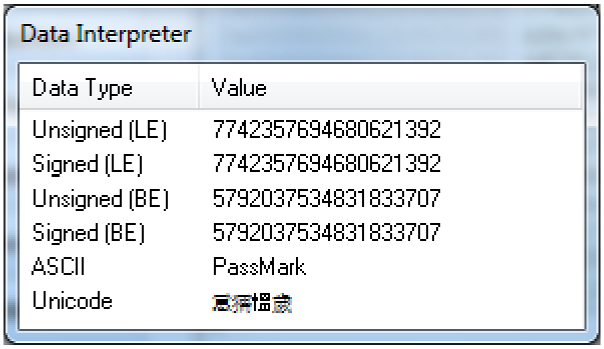
Object Type
Any particular property of the allocated space that contains the current offset. (Eg. File, directory, free space, slack space)

Data Interpreter

The Data Interpreter window parses the raw bytes into a human-readable format. Currently, there are two views available: *Data type interpreter* and *MBR interpreter*.

Data Type Interpreter

This is the default mode of the Data Interpreter window.



Data Interpreter

Data Type	Value
Unsigned (LE)	7742357694680621392
Signed (LE)	7742357694680621392
Unsigned (BE)	5792037534831833707
Signed (BE)	5792037534831833707
ASCII	PassMark
Unicode	慐獳慍歲

Unsigned (LE)
The selected bytes interpreted as unsigned, little-endian encoded. Note that this information is available only if 1-8 bytes are selected.

Signed (LE)
The selected bytes interpreted as signed, little-endian encoded. Note that this information is available only if 1-8 bytes are selected.

Unsigned (BE)
The selected bytes interpreted as unsigned, big-endian encoded. Note that this information is available only if 1-8 bytes are selected.

Signed (BE)
The selected bytes interpreted as signed, big-endian encoded. Note that this information is available only if 1-8 bytes are selected.

NTFS Filetime (BE)
The selected bytes interpreted as a 64-bit, big-endian encoded NTFS file time. Note that this information is available only if exactly 8 bytes are selected.

FAT Timestamp (LE)
The selected bytes interpreted as 32-bit, little-endian encoded FAT timestamp. Note that this information is available only if 4 bytes are selected.

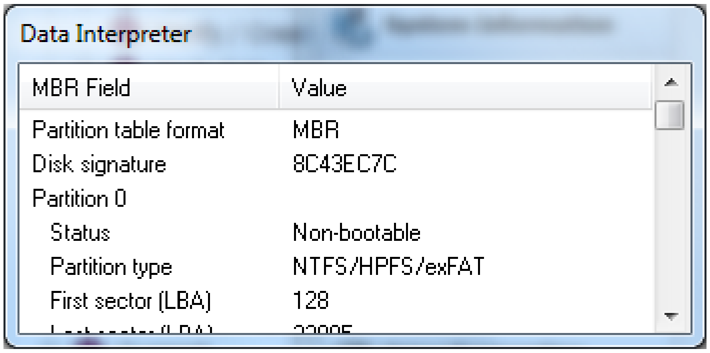
HFS+ Timestamp (BE)
The selected bytes interpreted as 32-bit, big-endian encoded HFS+ timestamp. Note that this information is available only if 4 bytes are selected.

ASCII
The selected bytes interpreted as ASCII-encoded text. Note that this information is available only if 1-32 bytes are selected.

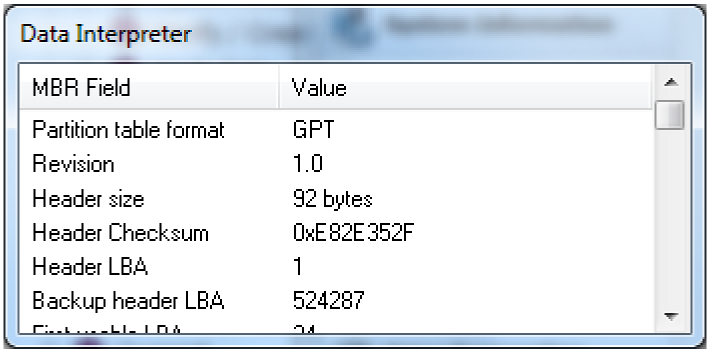
Unicode
The selected bytes interpreted as Unicode-encoded text. Note that this information is available only if 2-32 bytes are selected.

Partition Table Interpreter

This mode is automatically enabled when the current offset is within the first sector of a physical disk (ie. MBR). The partition table (MBR or GPT) is displayed in a human-readable format.



MBR Field	Value
Partition table format	MBR
Disk signature	8C43EC7C
Partition 0	
Status	Non-bootable
Partition type	NTFS/HPFS/exFAT
First sector (LBA)	128

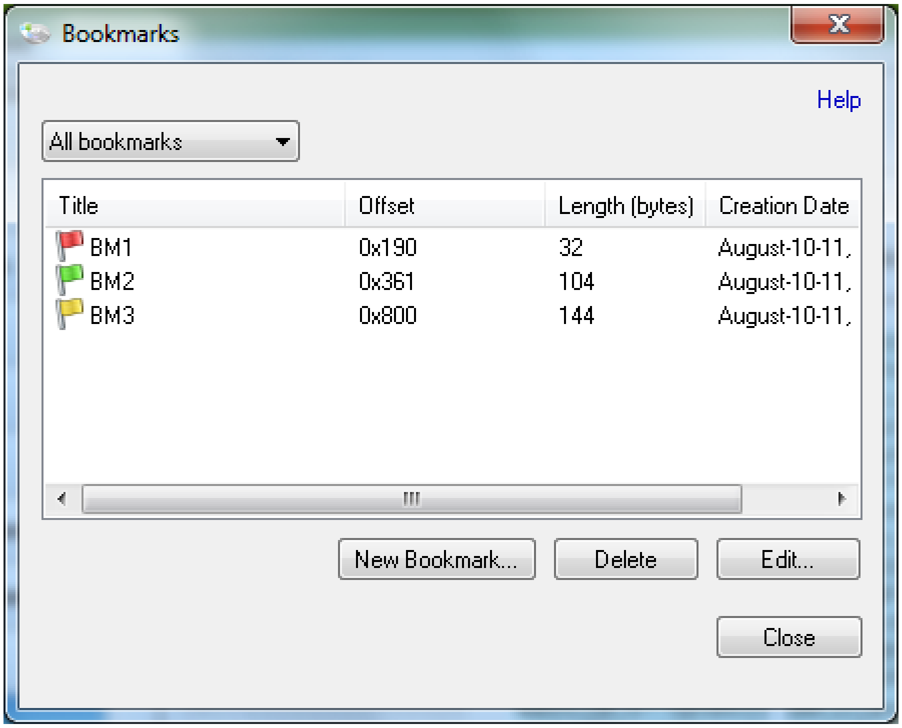


MBR Field	Value
Partition table format	GPT
Revision	1.0
Header size	92 bytes
Header Checksum	0xE82E352F
Header LBA	1
Backup header LBA	524287

Double-clicking on a LBA field will jump to the appropriate offset in the disk viewer.

4.9.3 Bookmark Window

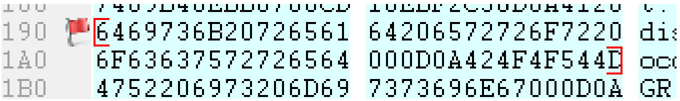
The Raw Disk Viewer bookmark window allows the user to manage the bookmarks on the selected device.



Title	Offset	Length (bytes)	Creation Date
BM1	0x190	32	August-10-11,
BM2	0x361	104	August-10-11,
BM3	0x800	144	August-10-11,

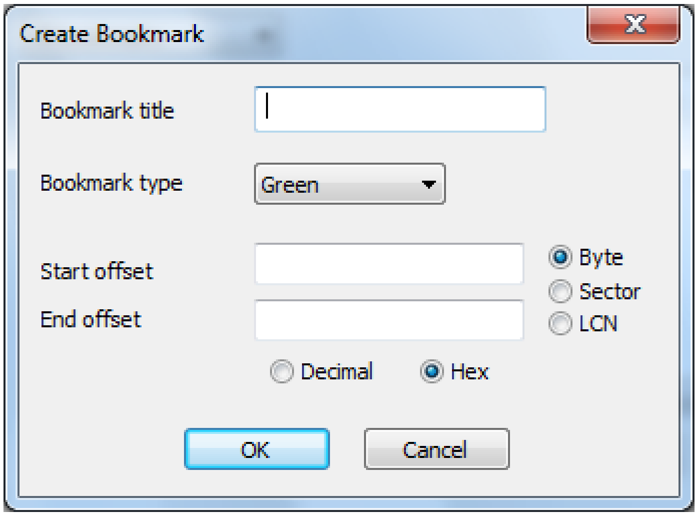
The details of all bookmarks visible on the raw disk viewer is displayed in the list. To filter the displayed bookmarks by type, select one of the bookmark types from the drop down list.

Bookmarks are useful for marking offset ranges of interest on the drive so that it is readily accessible at any time. Bookmarks are indicated by a flag icon, and square brackets to mark the beginning and end of the bookmark.



```
190 [6469736B20726561 6420657272 6F7220 dis
1A0  6F63637572726564 000D0A424F4F544D] occ
1B0  4752206973206D69 7373696E67000D0A GR
```

New Bookmark
Opens a dialog for specifying the properties of a new bookmark.



Create Bookmark

Bookmark title

Bookmark type: Green

Start offset

End offset

● Byte ○ Sector ○ LCN

○ Decimal ● Hex

Bookmark title - The name of the bookmark

Bookmark type - The category which the bookmark belongs to

Start offset - The starting offset of the bookmark

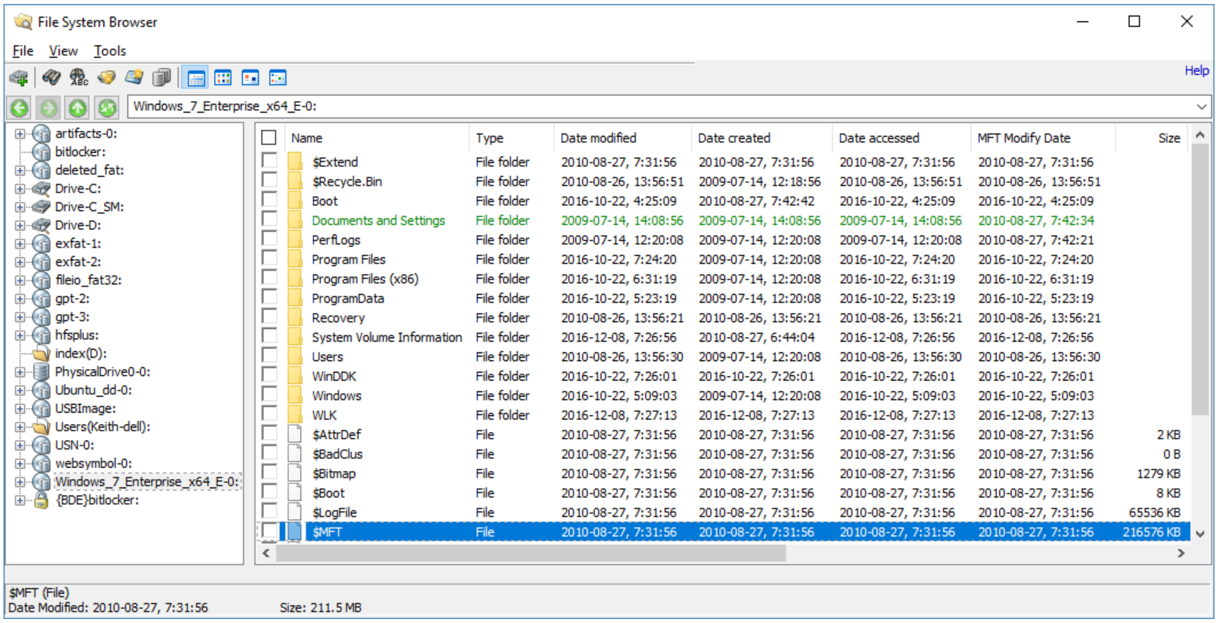
End offset - The ending offset of the bookmark

Delete
Delete the selected bookmark.

Edit ...
Change an existing bookmark's title and/or type.

4.10 File System Browser

The File System Browser provides an explorer-like view of all devices that have been added to the case. Unlike Windows Explorer, the File System Browser is able to display additional forensic-specific information, as well as allow analysis to be performed using OSForensics' integrated tools.



Name	Type	Date modified	Date created	Date accessed	MFT Modify Date	Size
$Extend	File folder	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2010-08-27, 7:31:56	
$Recycle.Bin	File folder	2010-08-26, 13:56:51	2009-07-14, 12:18:56	2010-08-26, 13:56:51	2010-08-26, 13:56:51	
Boot	File folder	2016-10-22, 4:25:09	2010-08-27, 7:42:42	2016-10-22, 4:25:09	2016-10-22, 4:25:09	
Documents and Settings	File folder	2009-07-14, 14:08:56	2009-07-14, 14:08:56	2009-07-14, 14:08:56	2010-08-27, 7:42:34	
PerfLogs	File folder	2009-07-14, 12:20:08	2009-07-14, 12:20:08	2009-07-14, 12:20:08	2010-08-27, 7:42:21	
Program Files	File folder	2016-10-22, 7:24:20	2009-07-14, 12:20:08	2016-10-22, 7:24:20	2016-10-22, 7:24:20	
Program Files (x86)	File folder	2016-10-22, 6:31:19	2009-07-14, 12:20:08	2016-10-22, 6:31:19	2016-10-22, 6:31:19	
ProgramData	File folder	2016-10-22, 5:23:19	2009-07-14, 12:20:08	2016-10-22, 5:23:19	2016-10-22, 5:23:19	
Recovery	File folder	2010-08-26, 13:56:21	2010-08-26, 13:56:21	2010-08-26, 13:56:21	2010-08-26, 13:56:21	
System Volume Information	File folder	2016-12-08, 7:26:56	2010-08-27, 6:44:04	2016-12-08, 7:26:56	2016-12-08, 7:26:56	
Users	File folder	2010-08-26, 13:56:30	2009-07-14, 12:20:08	2010-08-26, 13:56:30	2010-08-26, 13:56:30	
WinDDK	File folder	2016-10-22, 7:26:01	2016-10-22, 7:26:01	2016-10-22, 7:26:01	2016-10-22, 7:26:01	
Windows	File folder	2016-10-22, 5:09:03	2009-07-14, 12:20:08	2016-10-22, 5:09:03	2016-10-22, 5:09:03	
WLK	File folder	2016-12-08, 7:27:13	2016-12-08, 7:27:13	2016-12-08, 7:27:13	2016-12-08, 7:27:13	
$AttrDef	File	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2 KB
$BadClus	File	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2010-08-27, 7:31:56	0 B
$Bitmap	File	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2010-08-27, 7:31:56	1279 KB
$Boot	File	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2010-08-27, 7:31:56	8 KB
$LogFile	File	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2010-08-27, 7:31:56	65536 KB
$MFT	File	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2010-08-27, 7:31:56	2010-08-27, 7:31:56	216576 KB

$MFT (File)
Date Modified: 2010-08-27, 7:31:56 Size: 211.5 MB

OSForensics File System Browser

The left pane provides a hierarchical view of all devices added to the case. Clicking on a node shall load its contents into the right pane.

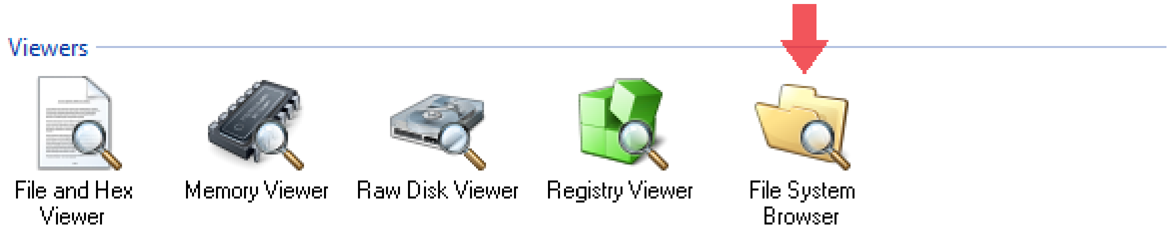
Understanding the File System Browser

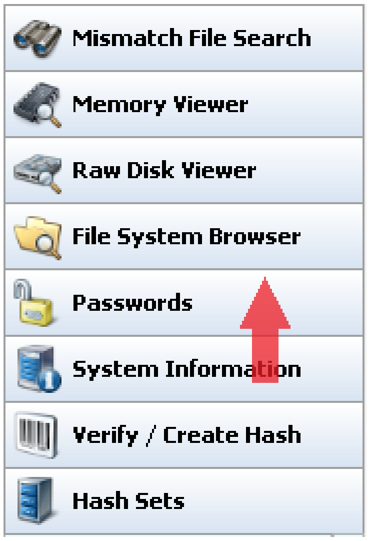
The table below summarizes the main components of the File System Browser.

Component	Description
Hierarchical View	Tree organization of all devices added to the case
File List	List view of the file entries contained in the current path. User may choose from several views. Red text - Deleted files Green text - Reparse points Blue text - Deleted file entries found in $I30 slack space Gray text - Shadow copy of the file
Metadata Columns	(Details view only) Contains metadata information for each file entry in the list
Navigation Bar	Shows the current path. Entering a new path shall navigate to the specified location.
Navigation Buttons	Navigate to the previous/parent path, or refresh the current path

Opening the File System Browser

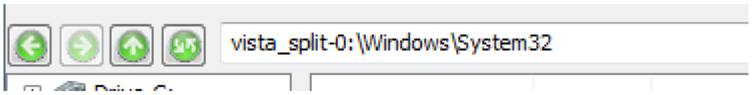
The File System Browser is accessible via the "File System Browser" icon in the "Viewers" group under the Start tab, as well as the right-side navigation "File System Browser" button. Once opened, all devices added to the case are listed in the left hierarchical view.





Usage

Navigation Bar/Buttons



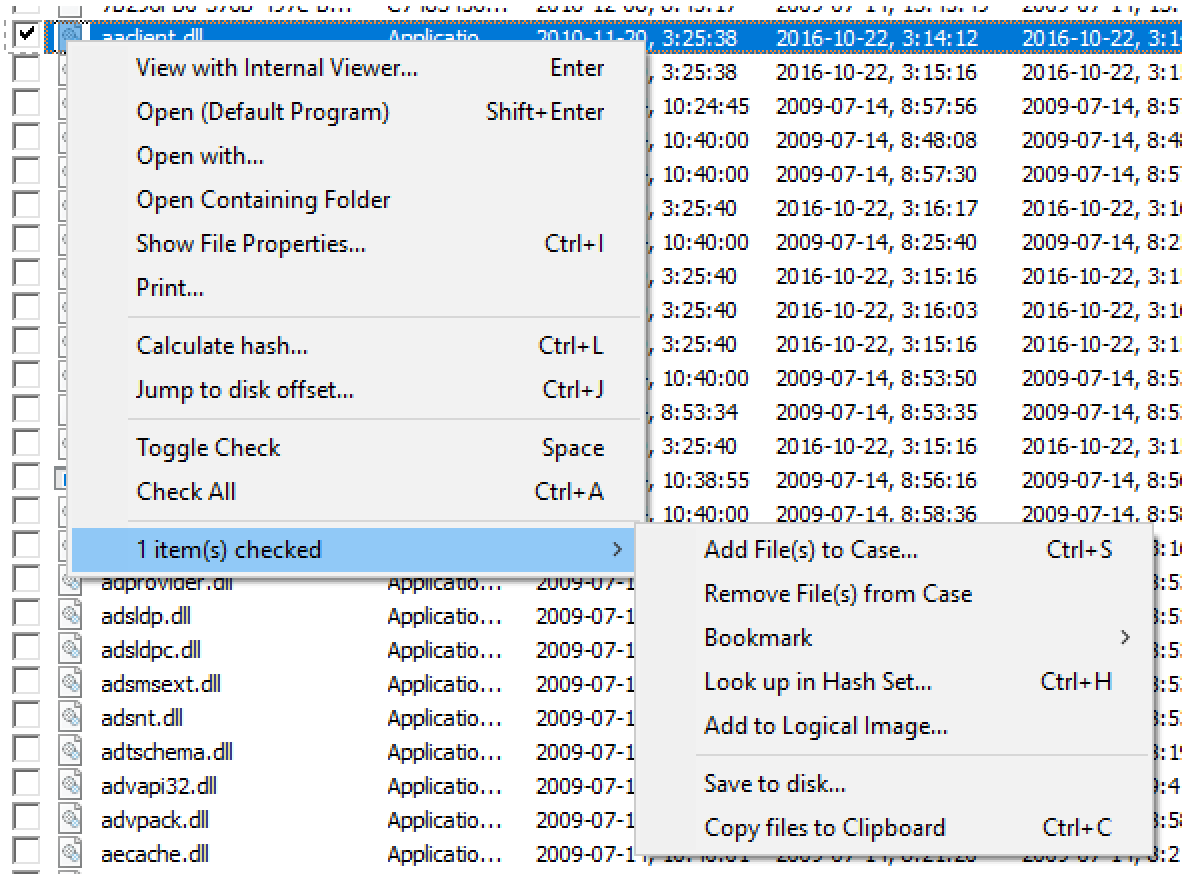
The navigation bar shows the current path that is being displayed in the File List view. The current path can be changed by typing the new path into the navigation bar.

To navigate to the previous or parent path, use the Back/Forward/Up buttons. To refresh the current path, use the Refresh button.

Right-click Menu

The right-click menu allows the user to perform forensic analysis on the file entries using OSForensics' integrated tools.

File List Menu



View with Interval Viewer...
Opens the file with OSForensics Viewer to perform a more thorough analysis. *Keyboard shortcut: Enter*

Open (Default Program)
Opens the file with the default program. *Keyboard shortcut: Shift+Enter*

Open With...
Allows the user to select the program to open the file

Open Containing Folder
Opens the folder than contains the file

Show File Properties...
Opens the file with OSForensics Viewer in File Info mode. *Keyboard shortcut: Ctrl+I*

Print...
Print the file (if applicable)

Calculate Hash...
Opens the Verify/Create Hash tab with the file path set to the selected file. *Keyboard shortcut: Ctrl+L*

Jump to disk offset...
Opens the Raw Disk Viewer tab and jumps to the disk offset of the selected file. *Keyboard shortcut: Ctrl+J*

Toggle Check
Toggle the check state of the selected item.

Check All
Check all the items in the list.

n Item(s) checked

Add to Case
Add the checked file(s) or list of checked file(s) to the case

Remove File(s) from Case
Remove the checked file(s) from the case

Bookmark

Green
Add/remove selected path from the list of Green bookmarks. *Keyboard shortcut: Ctrl+G*

Yellow
Add/remove selected path from the list of Yellow bookmarks. *Keyboard shortcut: Ctrl+Y*

Red
Add/remove selected path from the list of Red bookmarks. *Keyboard shortcut: Ctrl+R*

Look up in Hash Set
Verify whether the checked file(s) and files contained in selected folder(s) are in a hash set in the active database. See Hash Set Lookup. *Keyboard shortcut: Ctrl+H*

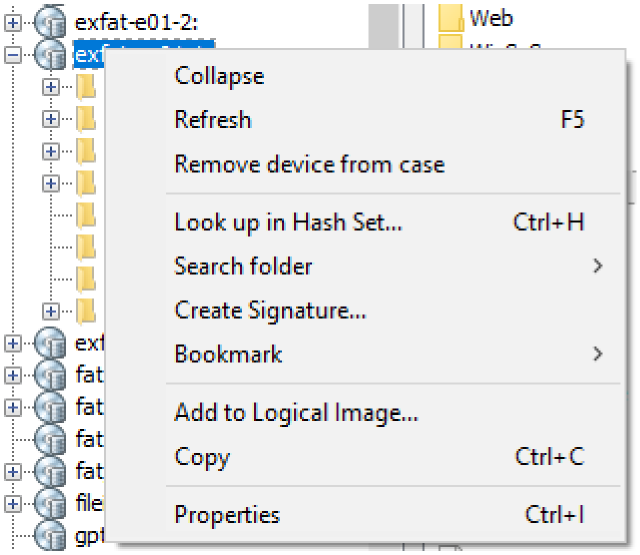
Add to Logical Image...
Add the selected file(s) to the list of Source Paths in the Forensic Imaging module in preparation for creating a logical image.

Save to disk...
Save the checked file(s) to a location on disk.

Copy File(s) to Clipboard
Copy the checked file(s) to clipboard. Once copied to the clipboard, the file(s) can be pasted to any other application that supports it (eg. Windows Explorer).

Note: In some cases, copy and pasting files to an explorer window may fail without an error message when "preparing to copy". This may happen if the file has already been deleted (eg a temp file) or if Windows Explorer does not have permissions to access the files (eg restricted system files and folders). In these cases, it is better to use the "Add to case" function.

Hierarchical View Menu



Expand/Collapse
Expand/collapse the selected folder

Refresh
Refresh the contents of the selected folder in the Object List pane. *Keyboard shortcut: F5*

Remove device from case
Remove the selected device from case *(Devices only)*

Look up in Hash Set...
Recursively determine whether the contents of the selected folder is contained in a hash set in the active database. See Hash Set Lookup. *Keyboard shortcut: Ctrl+H*

Search folder

File Name Search...
Opens the File Name Search tab with the file path set to the selected folder path. *Keyboard shortcut: Ctrl+F*

Mismatch File Search...
Opens the Mismatch File Search tab with the file path set to the selected folder path. *Keyboard shortcut: Ctrl+M*

Search folder
Opens the Create Signature tab with the file path set to the selected folder path.

Bookmark

Green
Add/remove selected path from the list of Green bookmarks. *Keyboard shortcut: Ctrl+G*

Yellow
Add/remove selected path from the list of Yellow bookmarks. *Keyboard shortcut: Ctrl+Y*

Red
Add/remove selected path from the list of Red bookmarks. *Keyboard shortcut: Ctrl+R*

Add to Logical Image...
Add the selected folder to the list of Source Paths in the Forensic Imaging module in preparation for creating a logical image.

Copy
Copies the selected folder to the clipboard. *Keyboard shortcut: Ctrl+C*

Advanced Options

The File System Browser includes several advanced options that can be accessed under Tools->Options...

Calculate Folder Sizes
When enabled, the total size of all contained files/folders are calculated

Shadow Copies
When enabled, previous shadow copies of files are shown alongside current files

Deleted Files
When enabled, deleted file entries contained in the current path are displayed.

4.10.1 File Metadata

The following is a description of the File System Browser columns in Details view:

Name
The name of the item (eg. file/directory)

Type
A short description of the item (eg. file type)

Date modified
The date the item was last modified

Date created
The date the item was first created

Date accessed
The date the item was last accessed

MFT/Attribute Modify Date *(NTFS/HFS+ only)*
The date the file system record for this item was last modified

Size
The size of the item (eg. file size)

Size on Disk
The size allocated to the item on disk storage.

For normal files, this is a multiple of the cluster size.

For NTFS files resident in the MFT, this is the same as the file size

For NTFS compressed/sparse files, this is the amount of physical disk space allocated to the file (usually smaller than the file size)

Attributes
The attributes of the item (eg. file attributes). Attributes are represented as single characters if present (eg. 'A') or a hyphen (eg. '-') if not present.

ACDEHRrsSdLU

A - Archived
C - Compressed
D - Directory
E - Encrypted
H - Hidden
R - Read-only
r - Reparse Point
s - Sparse file
S - System file
d - Deleted file
L - Symbolic link
U - Partially initialized file (ie. only part of the file is valid; the remaining part may contain remnants from a file it was previously allocated to)

# Streams
The number of alternative streams contained in the file, if applicable. This value does not include the default stream.

Total stream size
The total size of alternative streams contained in the file, if applicable. This value does not include the default stream.

# Fragments
The number of fragments of consecutive allocation units that the file is divided into.

Clusters/Fragments
The average number of clusters per fragment of the file

Starting LCN
The cluster number of the first cluster of the file

Flags
The flags assigned to the item by OSForensics. Each flag is represented by a single character if present (eg. 'H'), or a hyphen (eg. '-') if not present.

HGRYCV

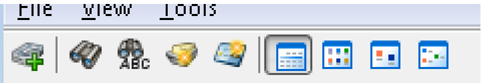
H|N - in Hash set/Not in hash set
G - Green bookmark
R - Red bookmark
Y - Yellow bookmark
C - Item was added to the Case
V - Item was Viewed in the internal viewer

4.10.2 File Browser Views

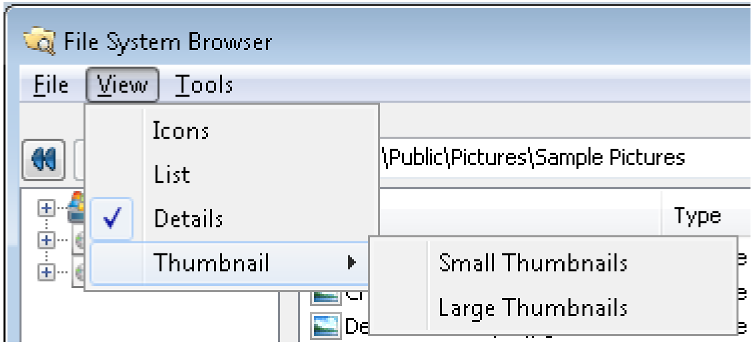
The user can choose from one of the following views in the File System Browser:

- Icon view
- List view
- Details view
- Small Thumbnails view
- Large Thumbnails view

The view can be changed via the toolbar icon,

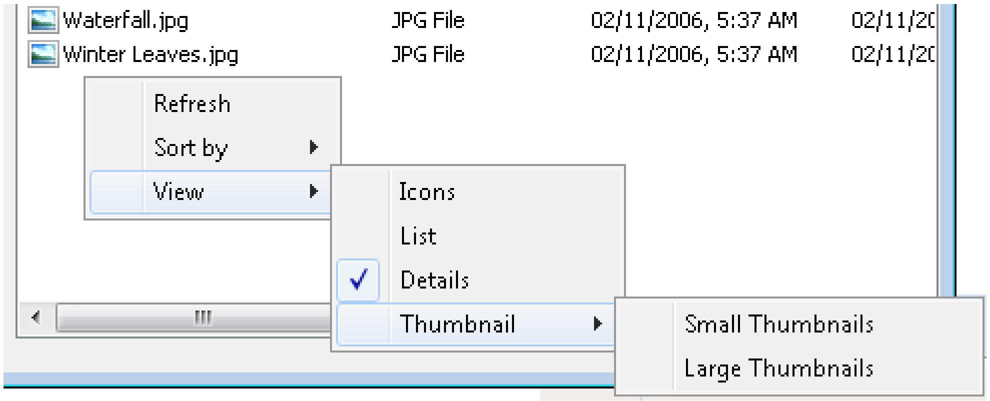


under 'View' in the system menu,



\Public\Pictures\Sample Pictures

or right-click context menu.

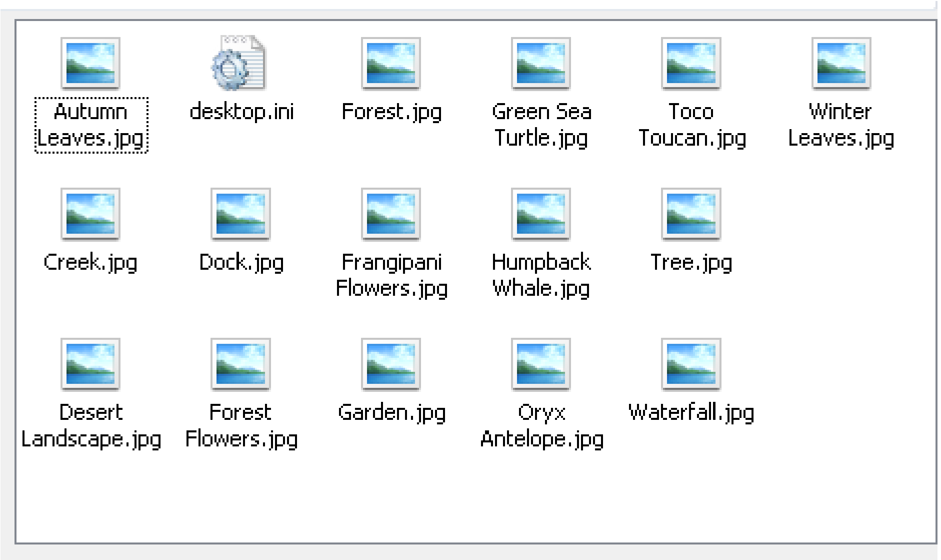


Waterfall.jpg JPG File 02/11/2006, 5:37 AM 02/11/20

Winter Leaves.jpg JPG File 02/11/2006, 5:37 AM 02/11/20

Icon View

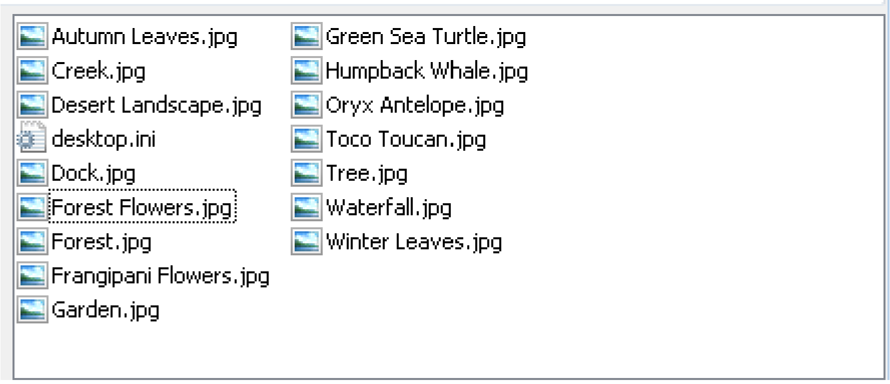
Icon view displays the object's name and associated icon.



Autumn Leaves.jpg
desktop.ini
Forest.jpg
Green Sea Turtle.jpg
Toco Toucan.jpg
Winter Leaves.jpg
Creek.jpg
Dock.jpg
Frangipani Flowers.jpg
Humpback Whale.jpg
Tree.jpg
Desert Landscape.jpg
Forest Flowers.jpg
Garden.jpg
Oryx Antelope.jpg
Waterfall.jpg

List View

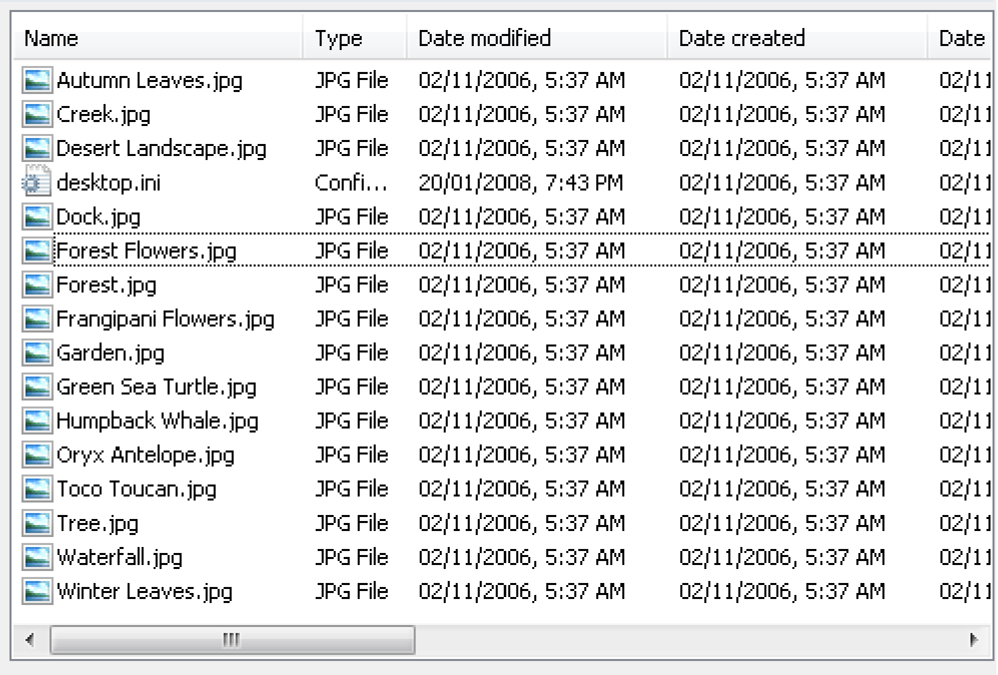
List view displays the object's name and associated icon in a compact fashion.



Autumn Leaves.jpg
Creek.jpg
Desert Landscape.jpg
desktop.ini
Dock.jpg
Forest Flowers.jpg
Forest.jpg
Frangipani Flowers.jpg
Garden.jpg
Green Sea Turtle.jpg
Humpback Whale.jpg
Oryx Antelope.jpg
Toco Toucan.jpg
Tree.jpg
Waterfall.jpg
Winter Leaves.jpg

Details View

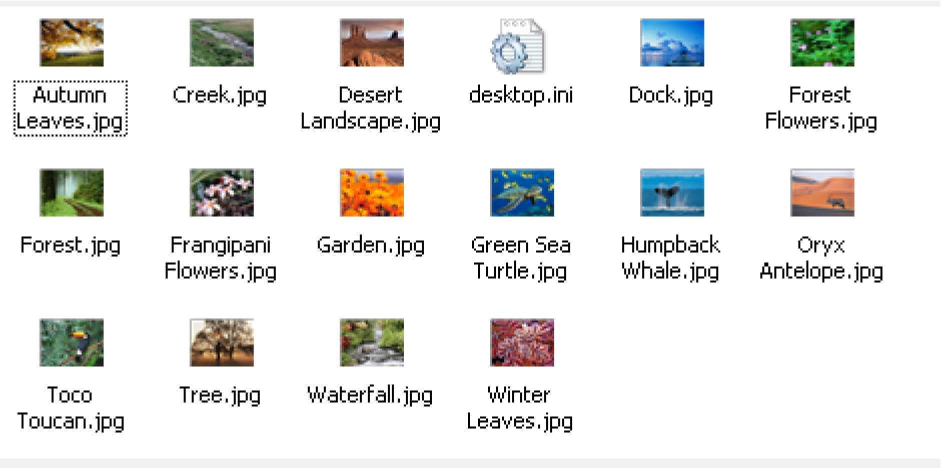
Details view displays the metadata associated with the object.



Name	Type	Date modified	Date created	Date
Autumn Leaves.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11
Creek.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11
Desert Landscape.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11
desktop.ini	Confi...	20/01/2008, 7:43 PM	02/11/2006, 5:37 AM	02/11
Dock.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11
Forest Flowers.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11
Forest.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11
Frangipani Flowers.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11
Garden.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11
Green Sea Turtle.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11
Humpback Whale.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11
Oryx Antelope.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11
Toco Toucan.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11
Tree.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11
Waterfall.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11
Winter Leaves.jpg	JPG File	02/11/2006, 5:37 AM	02/11/2006, 5:37 AM	02/11

Small Thumbnails View

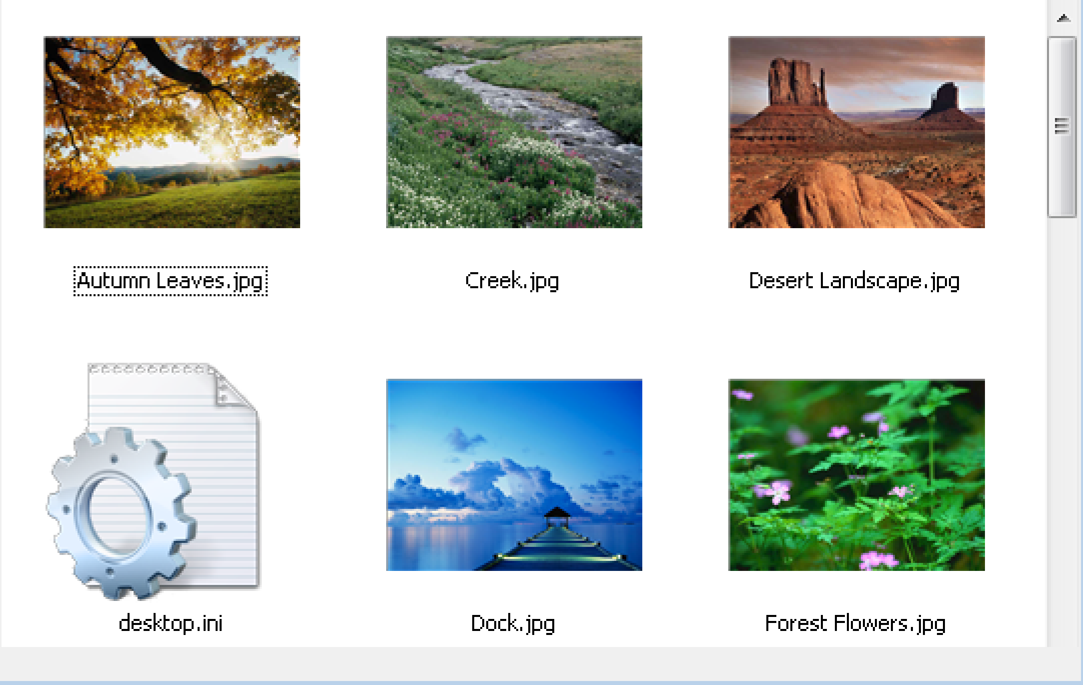
Small Thumbnails view is similar to Icon view, but a small thumbnail is displayed for image files.



Large Thumbnails View

Large Thumbnails view is similar to Icon view, but a large thumbnail is displayed for image files.

.



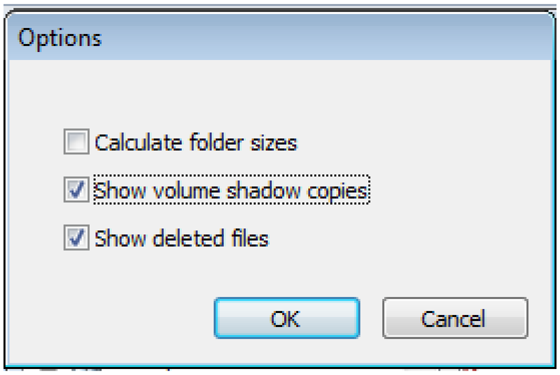
4.10.3 Shadow Copies

Previous shadow copies can be shown alongside current files within the File System Browser. Shadow copies are supported for certain devices that have been added to case. Supported devices are:

- Drive in Forensic Mode
- Physical Disks
- Volume Images

Enabling shadow copies in File System Browser

1. Add the supported device(s) to the current case.
2. Add the shadow copies for the volume added in step 1.
3. From the File System Browser window, select the "Tools->Options..." menu. Check the 'Show volume shadow copies" check box.


Options

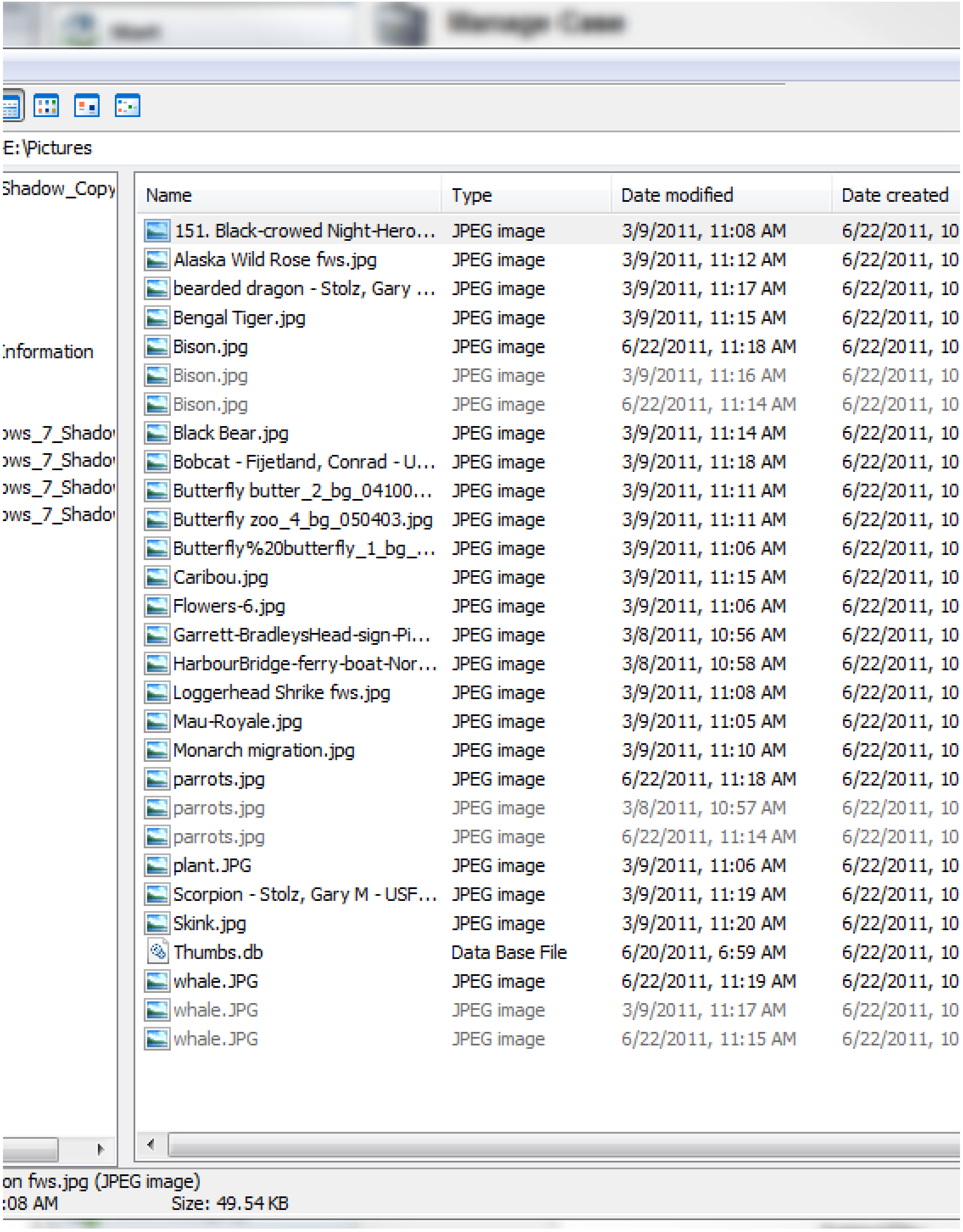
□ Calculate folder sizes

☑ Show volume shadow copies

☑ Show deleted files

4. From the File System Browser window, select the "Tools->Options..." menu. heck the 'Show volume shadow copies" check box.

5. Shadow copies of files will now appear along side the current files. A file will be consider a previous copy if the modified date differs from the current copy and other Shadow copies.Shadow copies will appear in Grey.

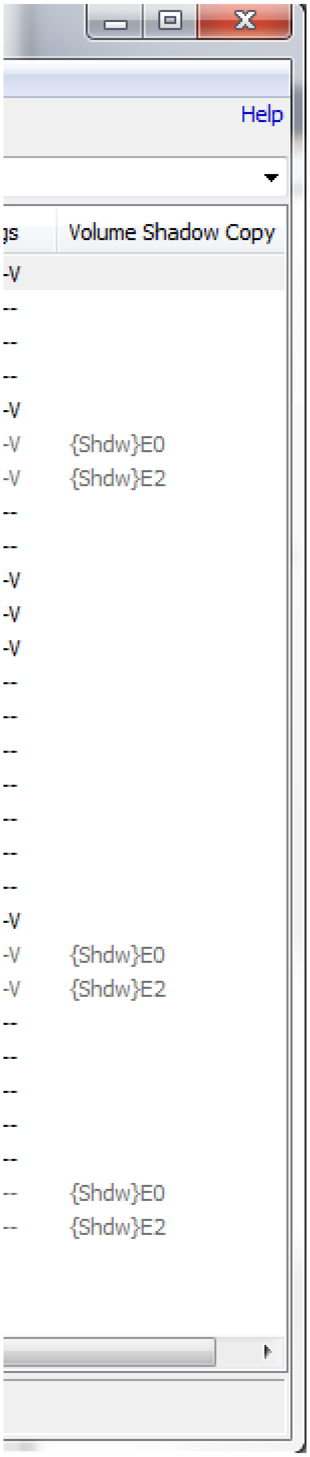


E:\Pictures

Name	Type	Date modified	Date created
151. Black-crowed Night-Hero...	JPEG image	3/9/2011, 11:08 AM	6/22/2011, 10
Alaska Wild Rose fws.jpg	JPEG image	3/9/2011, 11:12 AM	6/22/2011, 10
bearded dragon - Stolz, Gary ...	JPEG image	3/9/2011, 11:17 AM	6/22/2011, 10
Bengal Tiger.jpg	JPEG image	3/9/2011, 11:15 AM	6/22/2011, 10
Bison.jpg	JPEG image	6/22/2011, 11:18 AM	6/22/2011, 10
Bison.jpg	JPEG image	3/9/2011, 11:16 AM	6/22/2011, 10
Bison.jpg	JPEG image	6/22/2011, 11:14 AM	6/22/2011, 10
Black Bear.jpg	JPEG image	3/9/2011, 11:14 AM	6/22/2011, 10
Bobcat - Fijetland, Conrad - U...	JPEG image	3/9/2011, 11:18 AM	6/22/2011, 10
Butterfly butter_2_bg_04100...	JPEG image	3/9/2011, 11:11 AM	6/22/2011, 10
Butterfly zoo_4_bg_050403.jpg	JPEG image	3/9/2011, 11:11 AM	6/22/2011, 10
Butterfly%20butterfly_1_bg_...	JPEG image	3/9/2011, 11:06 AM	6/22/2011, 10
Caribou.jpg	JPEG image	3/9/2011, 11:15 AM	6/22/2011, 10
Flowers-6.jpg	JPEG image	3/9/2011, 11:06 AM	6/22/2011, 10
Garrett-BradleysHead-sign-Pi...	JPEG image	3/8/2011, 10:56 AM	6/22/2011, 10
HarbourBridge-ferry-boat-Nor...	JPEG image	3/8/2011, 10:58 AM	6/22/2011, 10
Loggerhead Shrike fws.jpg	JPEG image	3/9/2011, 11:08 AM	6/22/2011, 10
Mau-Royale.jpg	JPEG image	3/9/2011, 11:05 AM	6/22/2011, 10
Monarch migration.jpg	JPEG image	3/9/2011, 11:10 AM	6/22/2011, 10
parrots.jpg	JPEG image	6/22/2011, 11:18 AM	6/22/2011, 10
parrots.jpg	JPEG image	3/8/2011, 10:57 AM	6/22/2011, 10
parrots.jpg	JPEG image	6/22/2011, 11:14 AM	6/22/2011, 10
plant.JPG	JPEG image	3/9/2011, 11:06 AM	6/22/2011, 10
Scorpion - Stolz, Gary M - USF...	JPEG image	3/9/2011, 11:19 AM	6/22/2011, 10
Skink.jpg	JPEG image	3/9/2011, 11:20 AM	6/22/2011, 10
Thumbs.db	Data Base File	6/20/2011, 6:59 AM	6/22/2011, 10
whale.JPG	JPEG image	6/22/2011, 11:19 AM	6/22/2011, 10
whale.JPG	JPEG image	3/9/2011, 11:17 AM	6/22/2011, 10
whale.JPG	JPEG image	6/22/2011, 11:15 AM	6/22/2011, 10

on fws.jpg (JPEG image)
:08 AM Size: 49.54 KB

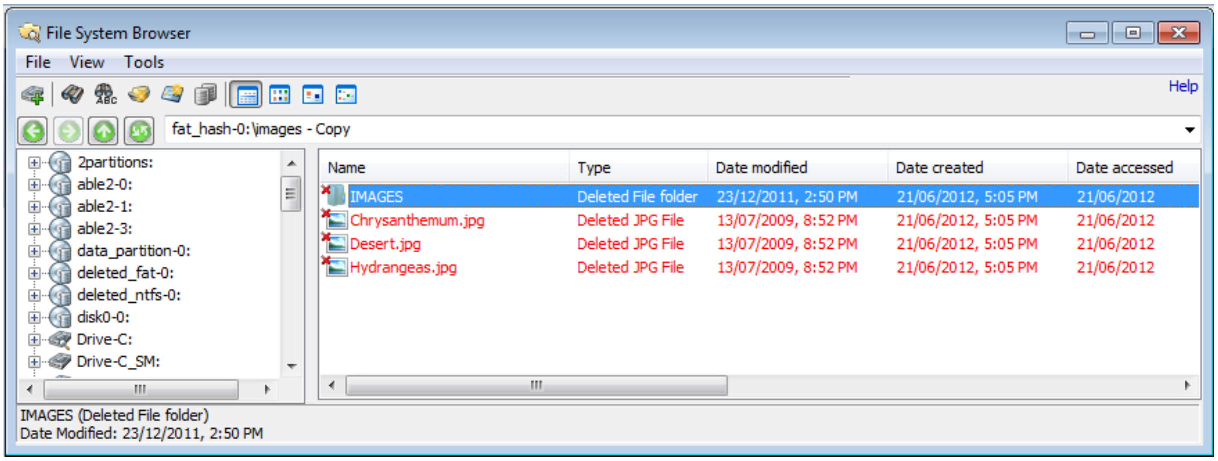
6. A new meta data column will be added to the end to indicate in which Volume Shadow Copy the file is from.



gs	Volume Shadow Copy
-V	
--	
--	
--	
-V	
-V	{Shdw}E0
-V	{Shdw}E2
--	
--	
-V	
-V	
-V	
--	
--	
--	
--	
--	
--	
--	
-V	
-V	{Shdw}E0
-V	{Shdw}E2
--	
--	
--	
--	
--	
--	{Shdw}E0
--	{Shdw}E2

4.10.4 Deleted Files

When enabled, the File System Browser is capable of displaying a list of deleted files in the current directory. Deleted file entries are displayed in red text, with a small, red 'X' overlaying its icon.



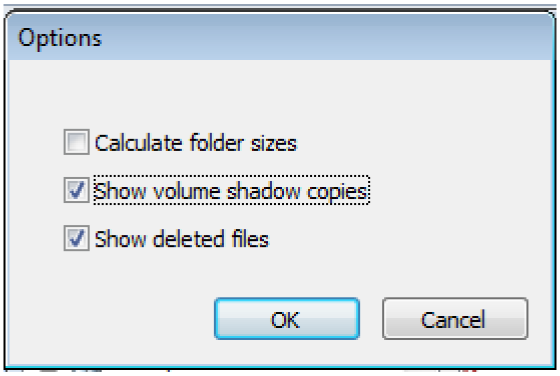
fat_hash-0:\images - Copy

Name	Type	Date modified	Date created	Date accessed
IMAGES	Deleted File folder	23/12/2011, 2:50 PM	21/06/2012, 5:05 PM	21/06/2012
Chrysanthemum.jpg	Deleted JPG File	13/07/2009, 8:52 PM	21/06/2012, 5:05 PM	21/06/2012
Desert.jpg	Deleted JPG File	13/07/2009, 8:52 PM	21/06/2012, 5:05 PM	21/06/2012
Hydrangeas.jpg	Deleted JPG File	13/07/2009, 8:52 PM	21/06/2012, 5:05 PM	21/06/2012

IMAGES (Deleted File folder)
Date Modified: 23/12/2011, 2:50 PM

Enabling deleted files in File System Browser

From the File System Browser window, select the "Tools->Options..." menu. Check the 'Show deleted files" check box.

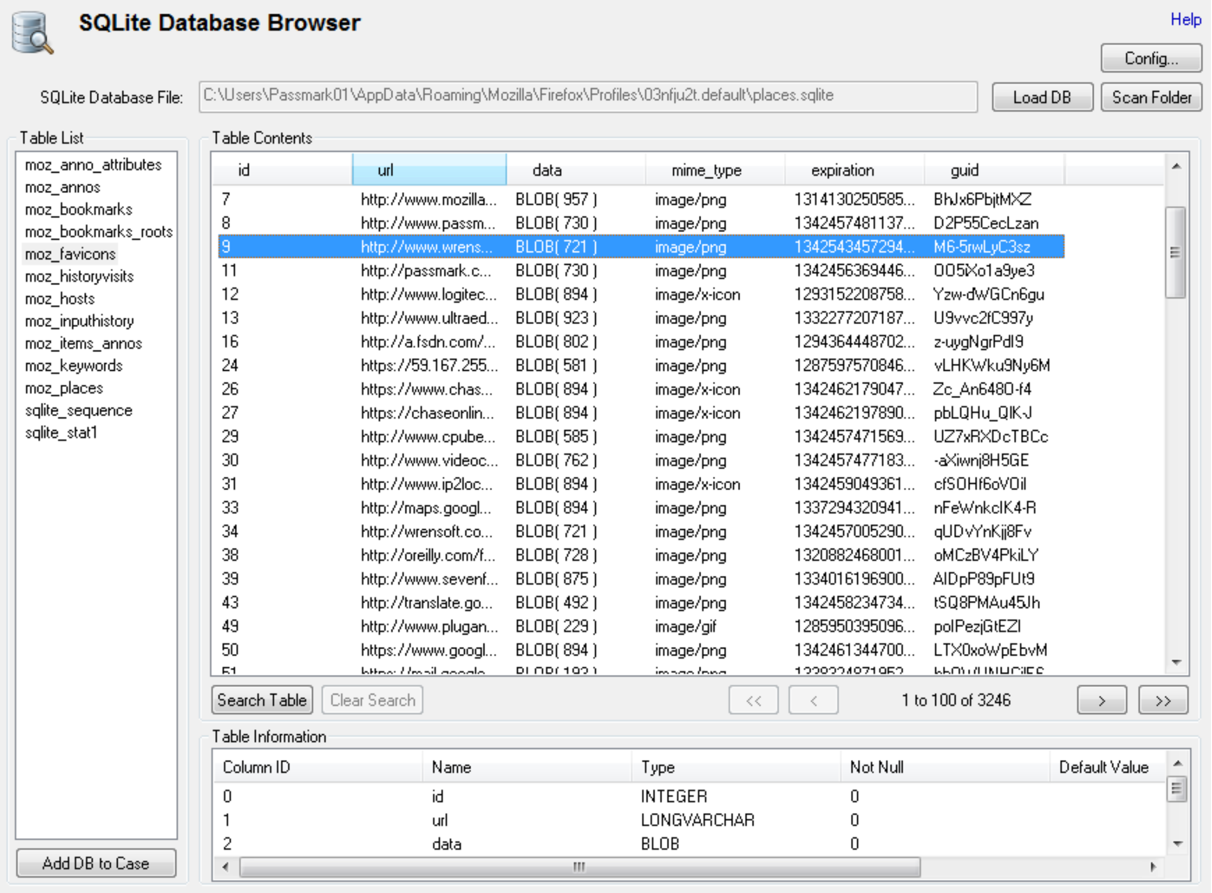


☐ Calculate folder sizes
☑ Show volume shadow copies
☑ Show deleted files

Note: Enabling deleted files will cause the file entries to take longer to load.

4.11 SQLite Database Browser

The SQLite Database (DB) Browser module allows the user to analyze the contents of SQLite database files. This module provides the ability to perform a deeper inspection of the contents and the ability to open BLOBs (binary data) with the Internal Viewer.



SQLite Database File: C:\Users\Passmark01\AppData\Roaming\Mozilla\Firefox\Profiles\03nfju2t.default\places.sqlite

- moz_anno_attributes
- moz_annos
- moz_bookmarks
- moz_bookmarks_roots
- moz_favicons
- moz_historyvisits
- moz_hosts
- moz_inputhistory
- moz_items_annos
- moz_keywords
- moz_places
- sqlite_sequence
- sqlite_stat1

id	url	data	mime_type	expiration	guid
7	http://www.mozilla...	BLOB(957)	image/png	1314130250585...	BhJx6PbjtMXZ
8	http://www.passm...	BLOB(730)	image/png	1342457481137...	D2P55CecLzan
9	http://www.wrens...	BLOB(721)	image/png	1342543457294...	M6-5rwLyC3sz
11	http://passmark.c...	BLOB(730)	image/png	1342456369446...	OO5iXo1a9ye3
12	http://www.logitec...	BLOB(894)	image/x-icon	1293152208758...	Yzw-dWGCn6gu
13	http://www.ultraed...	BLOB(923)	image/png	1332277207187...	U9vvc2fC997y
16	http://a.fsdn.com/...	BLOB(802)	image/png	1294364448702...	z-uygNgrPdl9
24	https://59.167.255...	BLOB(581)	image/png	1287597570846...	vLHKWku9Ny6M
26	https://www.chas...	BLOB(894)	image/x-icon	1342462179047...	Zc_An648O-f4
27	https://chaseonlin...	BLOB(894)	image/x-icon	1342462197890...	pbLQHu_QIK-J
29	http://www.cpube...	BLOB(585)	image/png	1342457471569...	UZ7xRXDcTBCc
30	http://www.videoc...	BLOB(762)	image/png	1342457477183...	-aXiwnj8H5GE
31	http://www.ip2loc...	BLOB(894)	image/x-icon	1342459049361...	cfSOHf6oVOil
33	http://maps.googl...	BLOB(894)	image/png	1337294320941...	nFeWnkcIK4-R
34	http://wrensoft.co...	BLOB(721)	image/png	1342457005290...	qUDvYnKjj8Fv
38	http://oreilly.com/f...	BLOB(728)	image/png	1320882468001...	oMCzBV4PkiLY
39	http://www.sevenf...	BLOB(875)	image/png	1334016196900...	AIDpP89pFUt9
43	http://translate.go...	BLOB(492)	image/png	1342458234734...	tSQ8PMAu45Jh
49	http://www.plugan...	BLOB(229)	image/gif	1285950395096...	polPezjGtEZI
50	https://www.googl...	BLOB(894)	image/png	1342461344700...	LTX0xoWpEbvM

1 to 100 of 3246

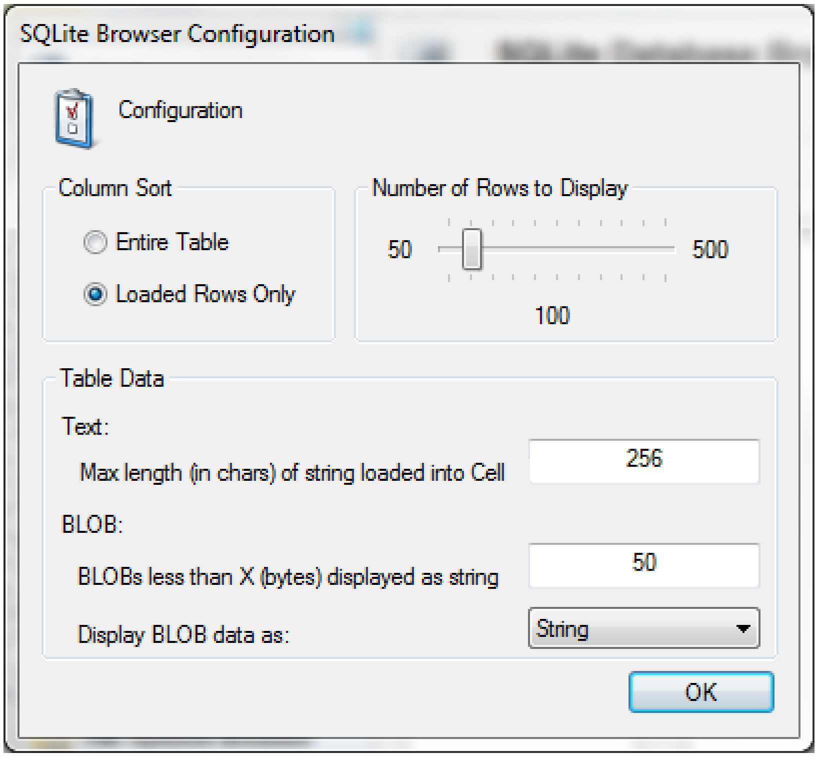
Column ID	Name	Type	Not Null	Default Value
0	id	INTEGER	0	
1	url	LONGVARCHAR	0	
2	data	BLOB	0	

Load DB

Load a SQLite database file.

Config ...

Opens a dialog to configure the display settings of the module.



SQLite Browser Configuration

Configuration

Column Sort

○ Entire Table

● Loaded Rows Only

Number of Rows to Display

50 — 500

100

Table Data

Text:

Max length (in chars) of string loaded into Cell: 256

BLOB:

BLOBs less than X (bytes) displayed as string: 50

Display BLOB data as: String

Column Sort – Adjust how the columns are sorted when clicking on the column header.

- Entire Table – Sort the table using the entire contents of the table.
- Loaded Rows Only – Sort the table using the rows currently loaded.

Number of Rows to Display - Configure the number of rows that are displayed in the table at one time.

Table Data -

- Text:

Max length (in chars) of string loaded into Cell - Specify the maximum number of characters that are displayed into each cell for Text data types.

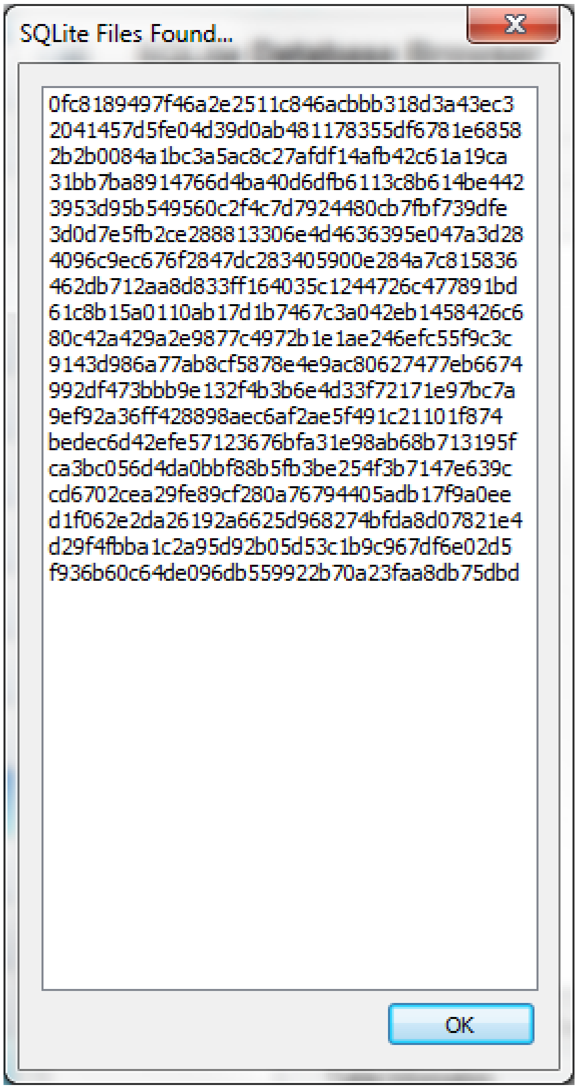
- BLOB:

*BLOBs less than X (bytes) displayed as string***-** Blobs under the number of bytes specified will have its contents displayed. Works in conjunction with next option.

Display BLOB data as: - BLOBs less than the bytes specified in the previous option will display its contents as **String** data or as **Hex** representation.

Scan Folder

Scans a folder for possible SQLite database files. Selecting a file on the file list will open the database in the viewer.



```
0fc8189497f46a2e2511c846acbbb318d3a43ec3
2041457d5fe04d39d0ab481178355df6781e6858
2b2b0084a1bc3a5ac8c27afdf14afb42c61a19ca
31bb7ba8914766d4ba40d6dfb6113c8b614be442
3953d95b549560c2f4c7d7924480cb7fbf739dfe
3d0d7e5fb2ce288813306e4d4636395e047a3d28
4096c9ec676f2847dc283405900e284a7c815836
462db712aa8d833ff164035c1244726c477891bd
61c8b15a0110ab17d1b7467c3a042eb1458426c6
80c42a429a2e9877c4972b1e1ae246efc55f9c3c
9143d986a77ab8cf5878e4e9ac80627477eb6674
992df473bbb9e132f4b3b6e4d33f72171e97bc7a
9ef92a36ff428898aec6af2ae5f491c21101f874
bedec6d42efe57123676bfa31e98ab68b713195f
ca3bc056d4da0bbf88b5fb3be254f3b7147e639c
cd6702cea29fe89cf280a76794405adb17f9a0ee
d1f062e2da26192a6625d968274bfda8d07821e4
d29f4fbba1c2a95d92b05d53c1b9c967df6e02d5
f936b60c64de096db559922b70a23faa8db75dbd
```

Table List

Shows the available tables in the loaded SQLite DB file. Selecting a table will load the contents in the adjacent **Table Contents** section.
Right clicking on a table will allow the user to "*Add selected table to case*"*.*

Add DB to Case

Allows the user to add the current SQLite file to the current case.

Table Contents

The view will show the contents of the current loaded table or the output from a custom search query.

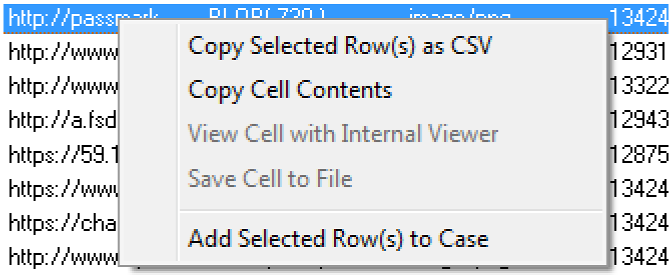
Search Table

Opens a search window that allows users to perform custom queries on the current loaded table. The results will be updated in the result table.

Clear Search
This button will be enabled when a custom search has been preformed. Selecting this will clear the custom query and reload the selected table.

Right clicking a cell will bring up a menu that will allow you to accomplish various tasks.

Right click menu


Copy Selected Row(s) as CSV
Copy Cell Contents
View Cell with Internal Viewer
Save Cell to File
Add Selected Row(s) to Case

Copy Selected Row(s) as CSV
Copy the selected rows to the clipboard in CSV format.

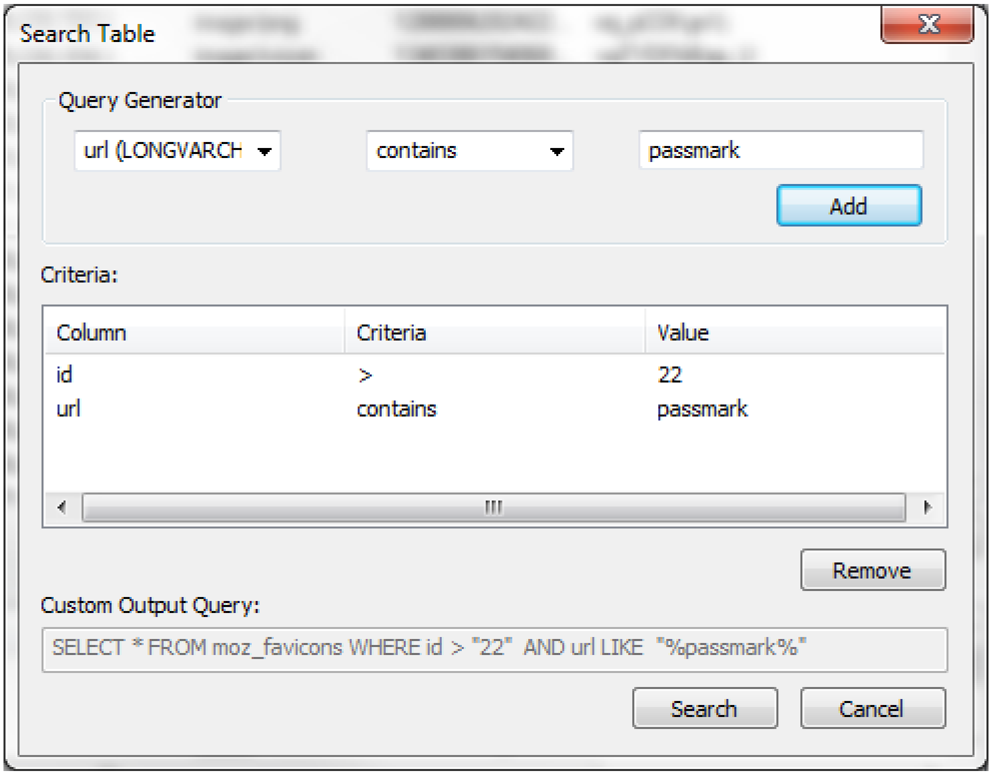
Copy Cell Contents
Copy the cell contents to the clipboard.

View Cell with Internal Viewer
Available only on binary/BLOB cells. The cell will be open with the OSForensics' Internal Viewer.

Save Cell to File
Available only on binary/BLOB cells. Allows saving the contents to a file.

Add Selected Row(s) to Case
Allows the user to add the current selected rows to the current open case.

Search Table



url (LONGVARCH | contains | passmark

Criteria:

Column	Criteria	Value
id	>	22
url	contains	passmark

Custom Output Query:

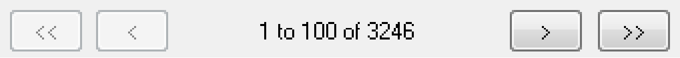
```
SELECT * FROM moz_favicons WHERE id > "22"  AND url LIKE  "%passmark%"
```

Query Generator
The first drop down box will be pre-populated with the column names for the loaded table. The second drop down box sets the criteria to be used on the chosen column. The text field allows further customization of the search criteria. The **Add** button will add the constraint to the query list.

Criteria
Shows a list of currently selected query constraints. To remove a constraint, select the criteria and click the **Remove** button.

Custom Output Query
Will show the query that will be performed on the SQLite table.

Navigation Buttons



1 to 100 of 3246

<<
Jump to the beginning (i.e. start with row 1) of the table.

<
Previous page.

X to Y of Z
Shows that rows from X to Y are loaded. Z is the total number of rows.

>
Next page.

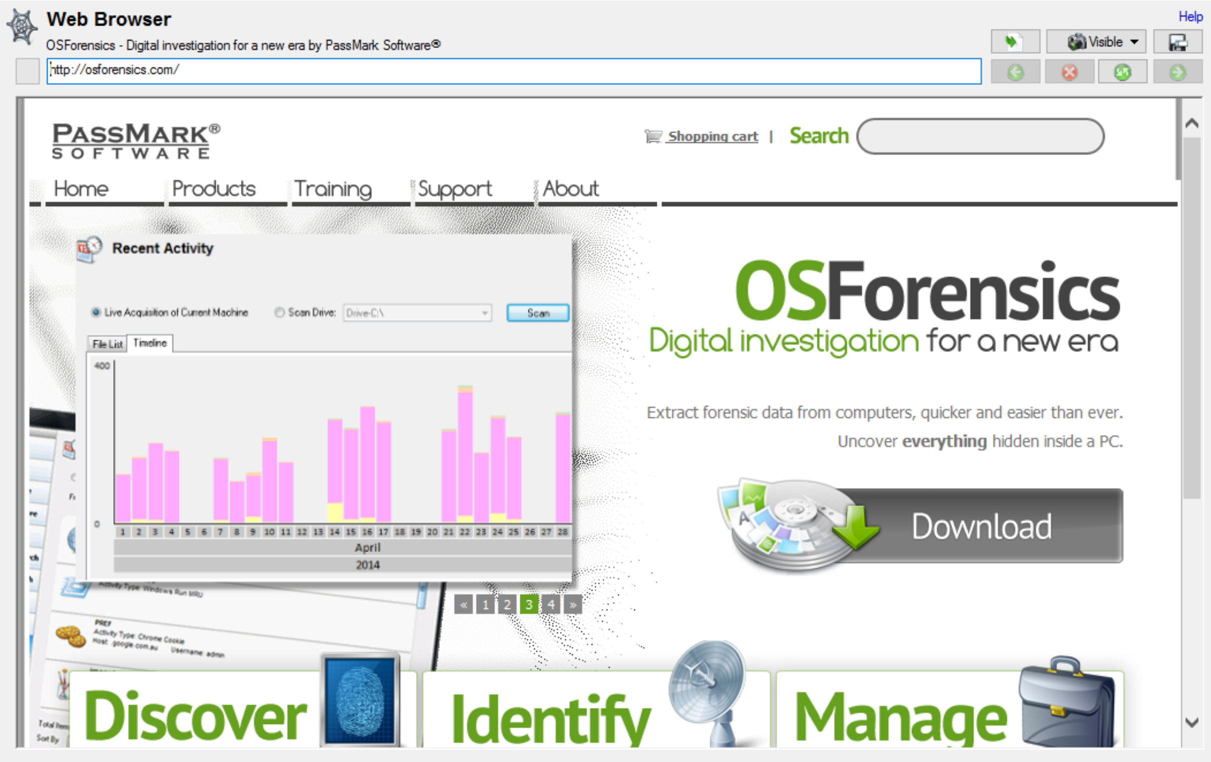
>>
Jump to the end of the table.

Table Information

Shows the table structure of the currently loaded table.

4.12 Web Browser

The Web Browser module provides a basic web viewer from within OSForensics. This module add the ability to load web pages from the web and save screen captures of web pages to the current opened case.



Web Browser

OSForensics - Digital investigation for a new era by PassMark Software®

http://osforensics.com/

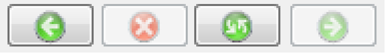
Caution:

The internal OSForeniscs' web browser module is implemented using Microsoft Internet Explorer Web Control COM object. In using the web browser, it will behave similarly to using Internet Explorer on Windows. As such it may leave artifacts (e.g. cookies, temp web files, entries in browser history) on the machine OSForensics is being operated on. Users should take caution if the web browser is being used on a live system that is under investigation.

Address Bar

Allows you to enter an URL to navigate to or shows the current URL of the loaded web page.

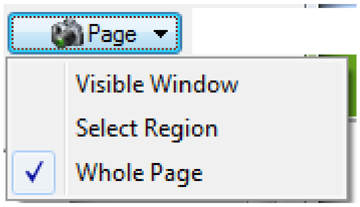
Navigation Buttons



Not all buttons will be enabled at all times. Buttons (starting from left):

- Back - Load the previous page.
- Stop - Active when the page is being downloading. Stop the current page from loading.
- Refresh - Reload the current page.
- Forward - Active when the "Back" button has been used. Goes Forward to the recently viewed page.

Screen Capture

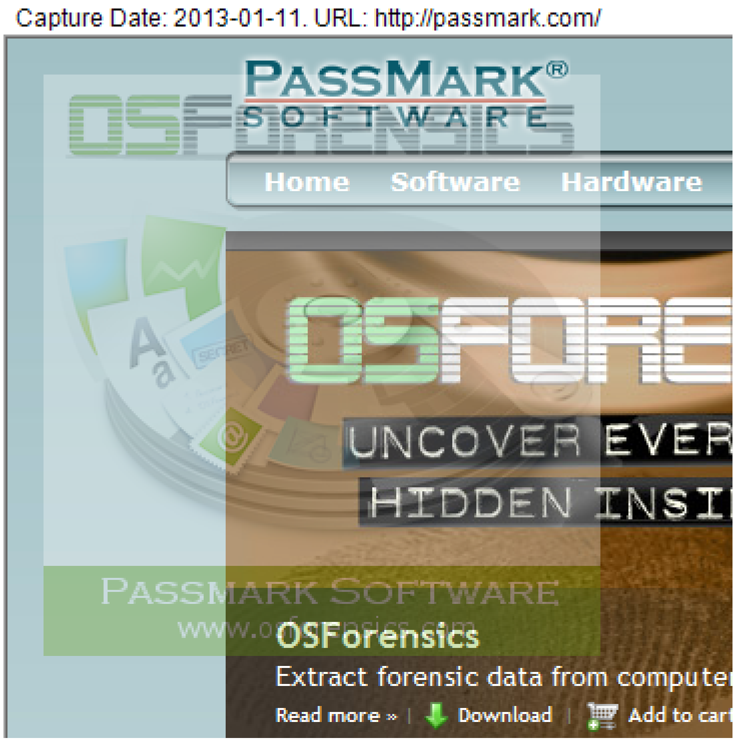


Pressing the screen capture button will capture the current page. Different capture options (Visible, Region, Page) allow you to choose what is captured. The image will been prefaced with capture date and the current URL. The captured screen will then be added to the case under "Files".

Visible Window
Captures what is current visible in the browser.

Select Region
Will bring up on screen prompts to allow you to capture only a certain region of the visible browser. (If the region width selected is too small, the info text added to the top of picture may not be shown completely).

Whole Page
The whole page will be saved as an image.



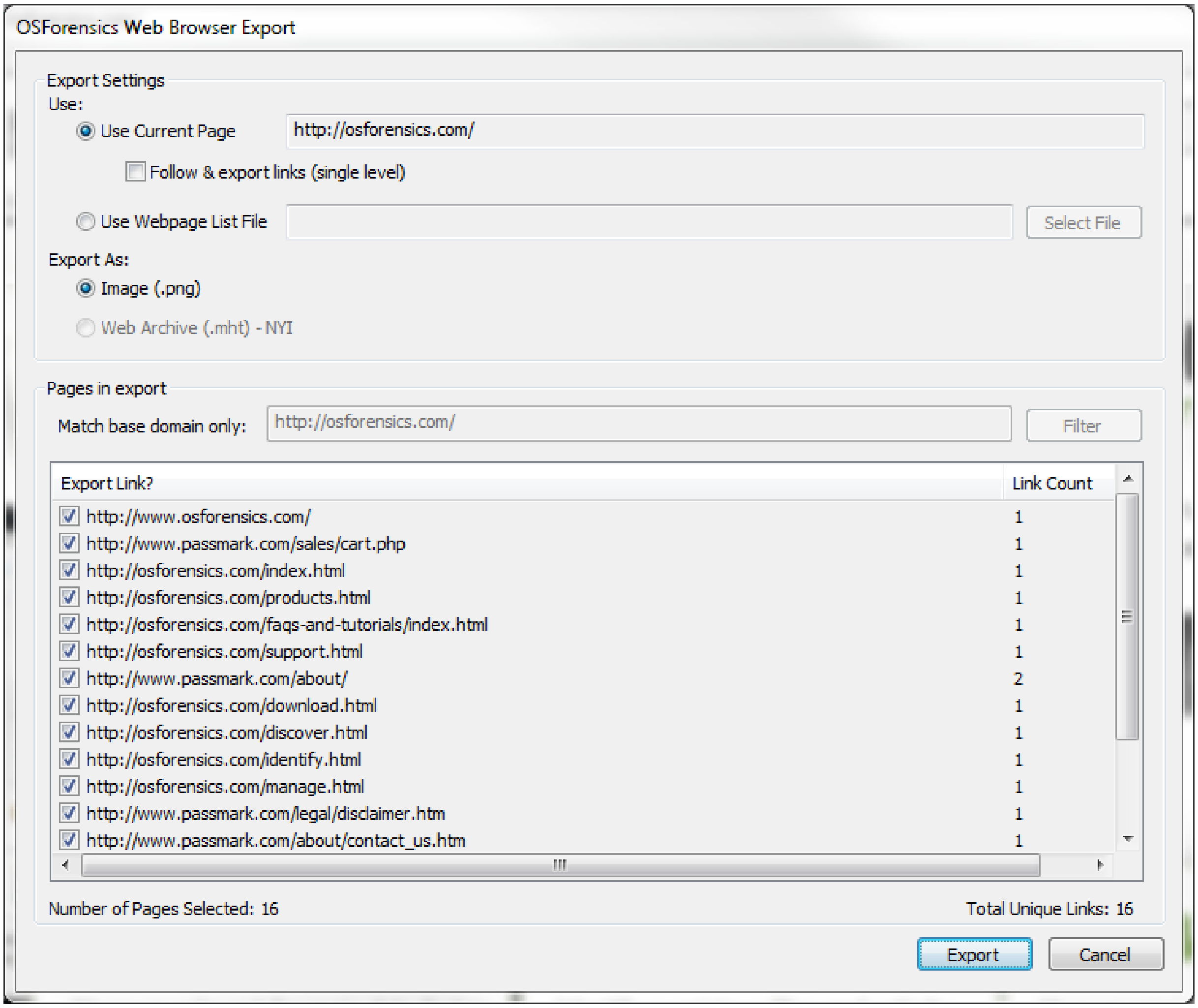
Capture Date: 2013-01-11. URL: http://passmark.com/

Screen Capture showing capture info text and OSForensics watermark.

*(Note: The **Free** version of OSForensics will have OSForensics logo watermarked throughout the image. The Pro version will not show the watermark.)*

Save/Export Page

Pressing the following button will launch the export page dialog. The dialog will allow you to capture all the pages currently linked from the Current Page. Or load a site list file to capture.



Use:
● Use Current Page http://osforensics.com/
□ Follow & export links (single level)
○ Use Webpage List File
Export As:
● Image (.png)
○ Web Archive (.mht) - NYI

Pages in export
Match base domain only: http://osforensics.com/

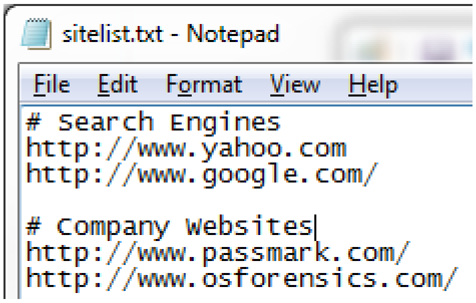
Export Link?	Link Count
☑ http://www.osforensics.com/	1
☑ http://www.passmark.com/sales/cart.php	1
☑ http://osforensics.com/index.html	1
☑ http://osforensics.com/products.html	1
☑ http://osforensics.com/faqs-and-tutorials/index.html	1
☑ http://osforensics.com/support.html	1
☑ http://www.passmark.com/about/	2
☑ http://osforensics.com/download.html	1
☑ http://osforensics.com/discover.html	1
☑ http://osforensics.com/identify.html	1
☑ http://osforensics.com/manage.html	1
☑ http://www.passmark.com/legal/disclaimer.htm	1
☑ http://www.passmark.com/about/contact_us.htm	1

Number of Pages Selected: 16
Total Unique Links: 16

Export Settings

Use Current Page - Use the current page that is loaded in the web browser. Selecting the "Follow & export links" checkbox will also export the pages linked on the current page. Further filtering can be done if not all pages are to be exported.

Use Webpage List File - Load a text file containing URLs to export. The list file should place each site on a new line. Lines starting with # are comment lines and will not be loaded.



```
# Search Engines
http://www.yahoo.com
http://www.google.com/

# Company Websites
http://www.passmark.com/
http://www.osforensics.com/
```

Export As - Currently all pages will be saved as .PNGs images.

Pages to Export

If using Current Page as the export option, in addition to the current URL, you can select additional linked pages to be captured. The list will show pages that are linked from the current page. The column Link Count shows how many times the link is found on the current page. If using the Webpage List option, then the list shows what sites were found in the file.

Match base domain only - Allow you to filter the list to match certain base domains. Domains should start with http:// or https://. You can specify multiple domains separated by a semicolon ";" character. The filter is case insensitive.

Export - This will start the export process of saving the page to your current case. OSForensics will pop up a web browser window during capture process. It is best to leave the capture process alone while it is in progress.

4.13 Passwords

Find Passwords/Keys

Retrieve passwords and product keys that have been stored by various applications and web browsers on the system.

Windows Login Passwords

Retrieve login passwords and hashes for the users of the system. Retrieved hashes can be used in conjunction with rainbow tables to find passwords.

Rainbow Tables

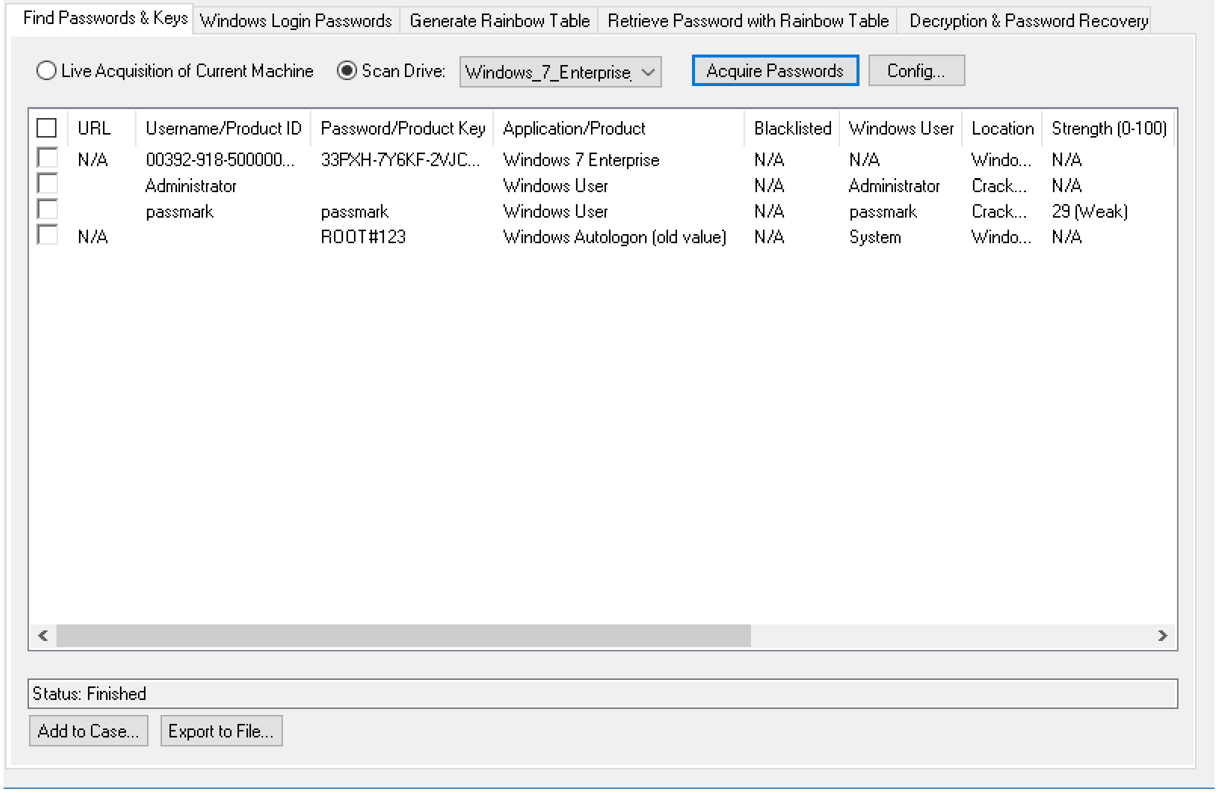
Use rainbow tables to do a reverse lookup on a password hash.

File Decryption & Password Recovery

Decrypt and access encrypted files.

4.13.1 Find Passwords/Keys

This feature can recover passwords for several types of applications, as well as Microsoft product keys.



Scan Drive: Windows_7_Enterprise

□	URL	Username/Product ID	Password/Product Key	Application/Product	Blacklisted	Windows User	Location	Strength (0-100)
□	N/A	00392-918-500000...	33PXH-7Y6KF-2VJC...	Windows 7 Enterprise	N/A	N/A	Windo...	N/A
□		Administrator		Windows User	N/A	Administrator	Crack...	N/A
□		passmark	passmark	Windows User	N/A	passmark	Crack...	29 (Weak)
□	N/A		ROOT#123	Windows Autologon (old value)	N/A	System	Windo...	N/A

Status: Finished

Browser Passwords
Passwords that been saved by users into their web browsers (IE, Edge, Firefox, Safari, and Opera). It can also find sites where a user has chosen not to remember a password.
Note: to recover FireFox password you must have FireFox installed on either the system that is running OSForensics or on the drive that OSForensics is currently scanning.

Email Passwords
Passwords saved by email account managers (Outlook and Windows Live Mail).

Wifi Passwords
Passwords for connecting to Wi-Fi networks that have been saved on the system.

Windows Autologon Password
Passwords that were provided for autologon of a particular User account when logging into Windows. When autologon has been enabled (e.g. by using netplwiz) and the password has been set, that password is saved on the system. Another way in which this value gets saved is when a password is provided during Windows installation, in some versions of Windows, it gets saved as the Autologon password even though Autologon is not enabled. Note that this password does not necessarily have to be the correct value, as it is still possible to set this value to an incorrect password (e.g. via netplwiz).

Windows Product Key
Product keys for certain versions of Windows, Microsoft Office, and Visual Studio.

Below is a table that shows which features are supported for diferent applications and their different versions.

Password Type	Versions	Login & Passwords
Windows Autologon Password	3,4,5,6+	Yes

Wifi	Vista, Win7, Win8, Win10	Current user **OR** when Windows user password is available*
Outlook	2002, 2003, 2007, 2010, 2013, 2016	Current user **OR** when Windows user password is available*
Outlook	Express, 98, 2000	Current user only*
Windows Live Mail	12, 2009, 2011, 2012	Current user only*
Chrome	8	Current user **OR** when Windows user password is available*
Internet Explorer	6,7,8	Current user **OR** when Windows user password is available*
Edge	20+	Current user only*
FireFox	2	Current user only*
FireFox	3,4,5,6+	Yes
Safari	4	No
Opera	20+	Current user only*
Opera	10, 11+	Yes
Opera	9	Yes

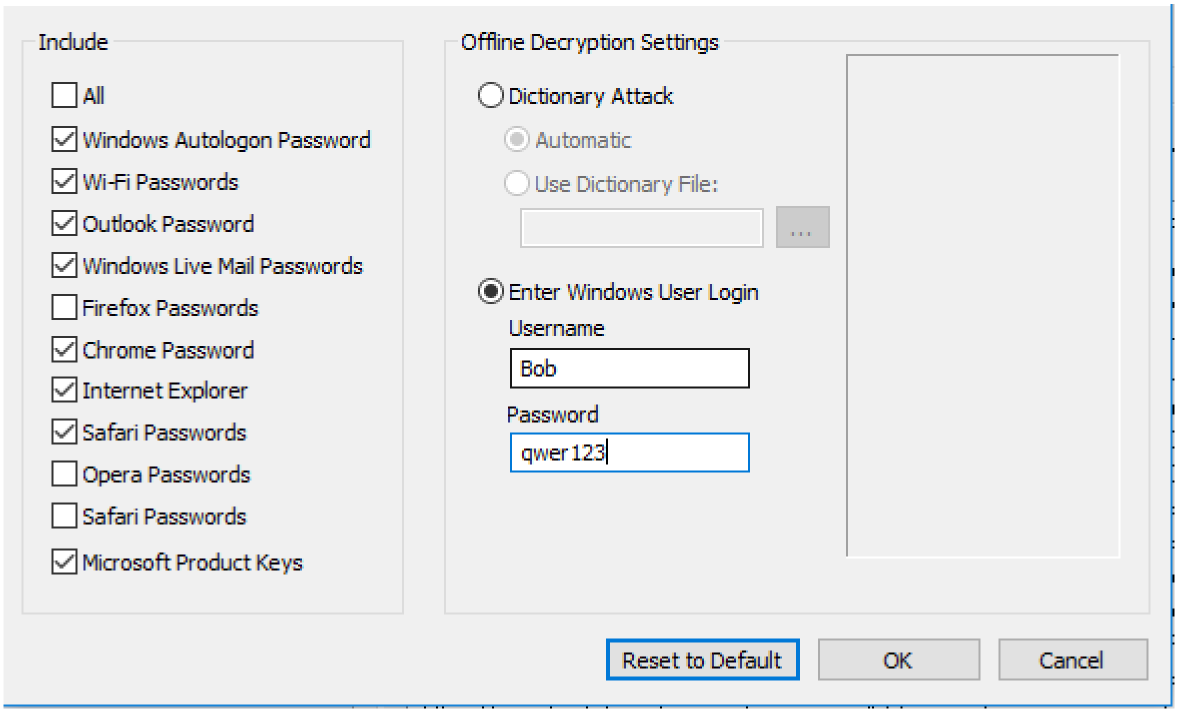
Product	**Versions**	**Product Keys**
Windows	Vista, 7, 8, 10	Yes
Microsoft Office	2003, 2007, 2010, 2013, 2016	Yes
Visual Studio	2008, 2010	Yes

*Current user only: This means information can only be retrieved with the Windows user to which the account belongs to. That is, you must be logged in to that Windows user when retrieving the password.

*Current user **OR** when Windows user password is available: This means that in addition to being available in the above circumstances, these passwords are also available for retrieval in an Offline manner, but only when the Windows User password that was used to decrypt the unknown password is available (e.g. by extracting the Windows Autologon password) or is provided by the investigator (i.e. in the Config window).

4.13.1.1 Offline Password Decryption

When retrieving passwords from an offline Windows installation (i.e. not a Live Acquisition) it is recommended that you provide the password of the Windows user account that is being investigated. To set the password, open the Config window, select "Enter Windows User Login" and type in the Username and Password of the Windows account that you wish to retrieve passwords from (see Fig 1. below).



Include

☐ All
☑ Windows Autologon Password
☑ Wi-Fi Passwords
☑ Outlook Password
☑ Windows Live Mail Passwords
☐ Firefox Passwords
☑ Chrome Password
☑ Internet Explorer
☑ Safari Passwords
☐ Opera Passwords
☐ Safari Passwords
☑ Microsoft Product Keys

Offline Decryption Settings

○ Dictionary Attack
● Automatic
○ Use Dictionary File:
● Enter Windows User Login
Username: Bob
Password: qwer123

Fig 1. Config Window

For many applications supported in this module, the Windows User password is required to retrieve passwords in an offline manner. This includes passwords for applications such as Chrome, IE, and Outlook. The user password is required because these applications save login information as encrypted data on the disk, and the key required to decrypt the data is the Windows User password.

If no Windows User password is provided, the default "Dictionary Attack" mode will be used. Here, OSForensics will automatically check if a password has been saved as the Autologon password and will attempt decryption using this password. Note that the Autologon password is also displayed by default in the list of retrieved passwords. The caveat is that this value is not always correct, nor always available, and it only applies to the user account that has been specified for autologon.

In addition to attempting decryption using the Windows Autologon password, a quick dictionary attack will be performed in which a list of common passwords will be tested. Alternatively, you can also specify a dictionary file to use.

Note that while this function searches each Windows user account on the system, you may only provide one user account password at a time.

If you do not know the Windows user password, you can try obtaining it with the following steps:

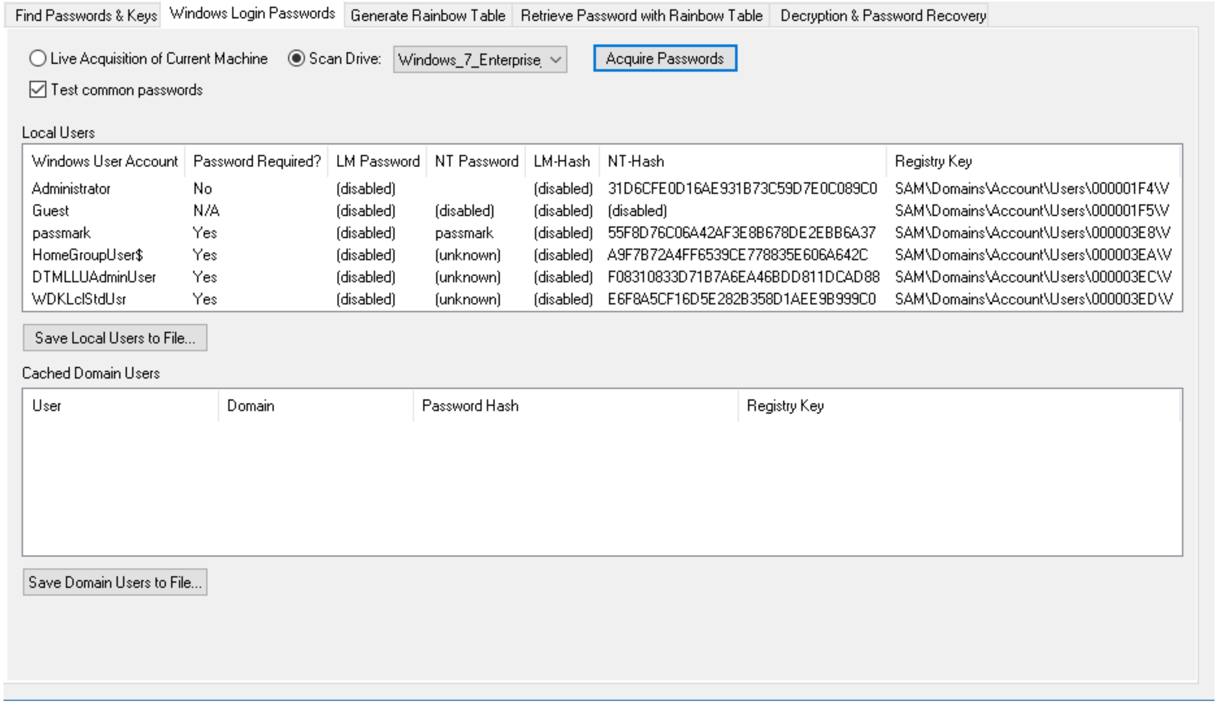
1. Use the Windows Login Passwords tab to dump the NTLM (a.k.a. NT) hash (or LM for WinXP) and save it to a file.
2. Obtain a decently sized NTLM Rainbow Table or collection of NTLM Rainbow Tables. Rainbow Tables are available for download from various sources, including our website. A hard drive containing a large collection of rainbow tables is also available for purchase at http://www.osforensics.com/rainbowtables_hashsets.html. You may also try generating one, but generating an effective rainbow table will require a lot of resources. Make sure you obtain rainbow tables that are compatible with OSForensics.
3. Use the Retrieve Password with Rainbow Table tab to crack the NTLM hash that was dumped in step 1. If this fails, try using a rainbow table with a different or larger character set. If the Rainbow table you used did not have a high success rate, try using one with a higher success rate.

4. Once you have obtained the password in plaintext, open the Config window, select "Enter Windows User Login" and enter the Username and Password that you have just recovered (see Fig 1. below). Click "OK" and then click "Retrieve Passwords". If you are still unable to decrypt passwords, it may be because it is under a different user account to the one that you entered in the Config window.

4.13.2 Windows Login Passwords

This will attempt to retrieve the LM and NT hashes from the Windows registry and save them to a file so Rainbow Tables can be used to match the hash values to a password. In some cases the password may be retrieved by OSForensics without the use of Rainbow Tables, for example where the password is the same as the username or it exists in the common passwords dictionary.

Any cached domain user names and passwords hashes will also be retrieved and displayed separately.


Find Passwords & Keys
Windows Login Passwords
Generate Rainbow Table
Retrieve Password with Rainbow Table
Decryption & Password Recovery
Acquire Passwords
Save Local Users to File...
Save Domain Users to File...

○ Live Acquisition of Current Machine ● Scan Drive: Windows_7_Enterprise

☑ Test common passwords

Local Users

Windows User Account	Password Required?	LM Password	NT Password	LM-Hash	NT-Hash	Registry Key
Administrator	No	(disabled)		(disabled)	31D6CFE0D16AE931B73C59D7E0C089C0	SAM\Domains\Account\Users\000001F4\V
Guest	N/A	(disabled)	(disabled)	(disabled)	(disabled)	SAM\Domains\Account\Users\000001F5\V
passmark	Yes	(disabled)	passmark	(disabled)	55F8D76C06A42AF3E8B678DE2EBB6A37	SAM\Domains\Account\Users\000003E8\V
HomeGroupUser$	Yes	(disabled)	(unknown)	(disabled)	A9F7B72A4FF6539CE778835E606A642C	SAM\Domains\Account\Users\000003EA\V
DTMLLUAdminUser	Yes	(disabled)	(unknown)	(disabled)	F08310833D71B7A6EA46BDD811DCAD88	SAM\Domains\Account\Users\000003EC\V
WDKLclStdUsr	Yes	(disabled)	(unknown)	(disabled)	E6F8A5CF16D5E282B358D1AEE9B999C0	SAM\Domains\Account\Users\000003ED\V

Cached Domain Users

User	Domain	Password Hash	Registry Key

Test Common Passwords

Selecting this option will test the found local user hashes against the common passwords dictionary file that is included in the OSForensics install.

Save Local Users to File

Saves the local user hashes in PWDUMP format (username:userid:LM hash:NT hash:comment:blank) so they can be used in conjunction with Rainbow Tables in OSForensics to find the passwords.

Save Domain Users to File

Saves the cached domain hashes so they can be used with external tools to find the passwords.

Once the registry files have been read the information will be displayed like the example below;

Local Users

Windows User Account: The Windows login user name
Password Required?: Whether a password is required to login.
LM Password: The password that matched the LM hash, if found, otherwise will contain "(unknown)" or "(disabled)". If blank then there is no password (an empty password).
NT Password: The password that matched the NT hash, if found, otherwise will contain "(unknown)" or "(disabled)". If blank then there is no password (an empty password).
LM-Hash: The LM hash that was retrieved from the registry or "(disabled)" if there was no hash.
NT-Hash: The NT hash that was retrieved from the registry or "(disabled)" if there was no hash.
Registry Key: The registry key location the data was retrieved from.

Domain Users
User: The user name.
Domain: The domain logged into.
Password hash: The stored password hash.
Registry Key: The registry key location the data was retrieved from.

4.13.2.1 Recovering Windows Passwords With Rainbow Tables

Once the hashes have been recovered Rainbow Tables can be used to try to find the password that matches the hash value. For this example we're using a rainbow table that was generated in OSForensics using "lm" as the hash setting, minimum 1 to maximum 7 characters and a character set of uppercase alpha-numeric (A-Z 0-9). This table is available for download from the OSForensics website.

First we need to retrieve the hash values from the registry and save them to a file, we are using a hard drive that had Windows XP installed on it. Opening the file in a text editor will let us select individual hashes to use with the Rainbow Tables if we were only trying to find a single value. If looking for multiple passwords then we can import the entire file on the Rainbow Table tab.

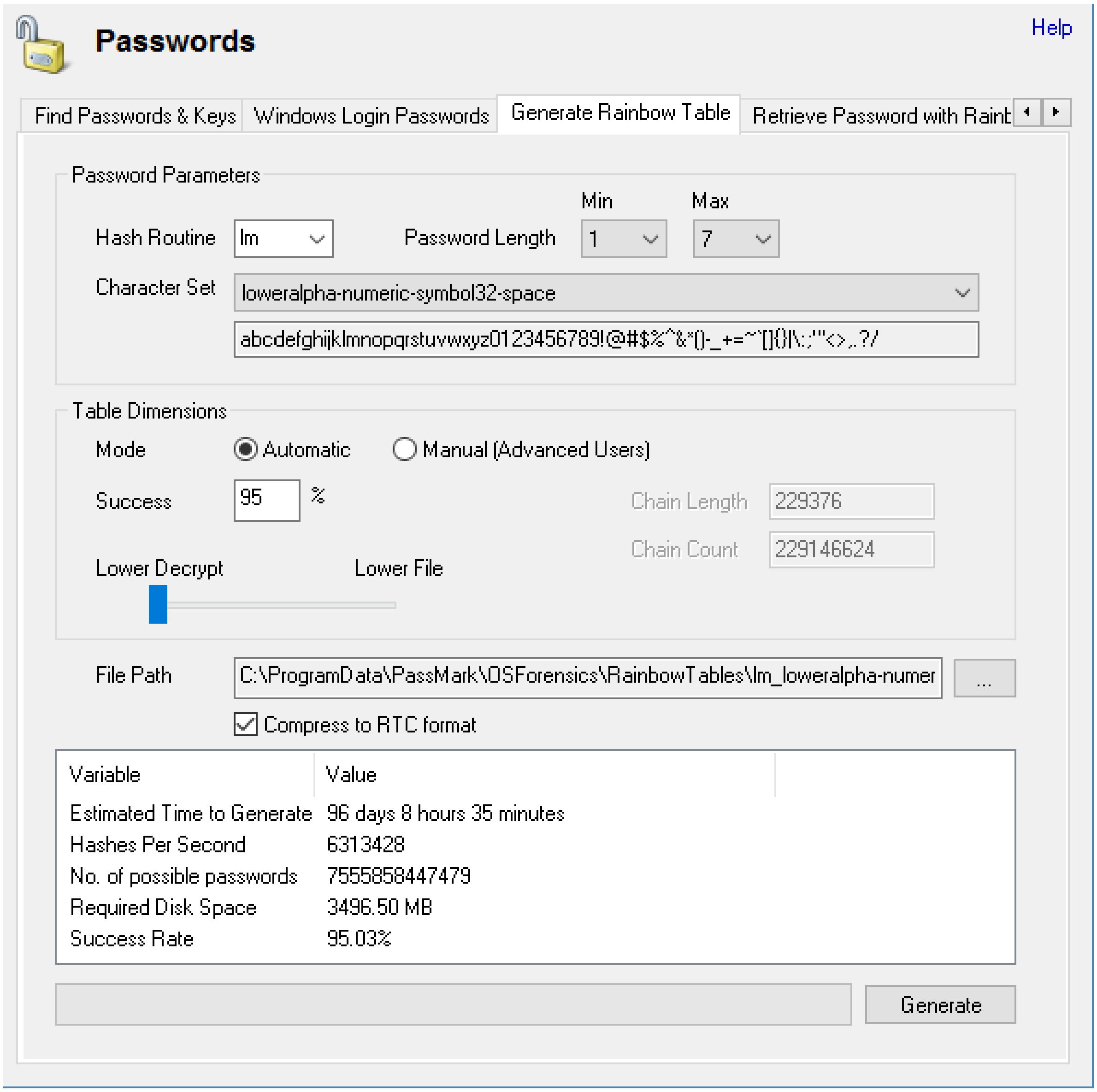
Once we have selected the file we need to choose the table to use and then start the process with "Recover Password/s".

If the values for the LM hash are all "(disabled)" this would indicate that either the LM hash has been disabled as part of a security policy for that Windows install or a password that is tool long for a LM hash has been used (15 or more characters).

For more information on LM and NT hashes see these Wikipedia articles.

4.13.3 Generating Rainbow Tables

This window is used for generating Rainbow Tables. These tables can then be used in the Rainbow Table Password Recovery Window.



Hash Routine: lm

Password Length: Min 1, Max 7

Character Set: loweralpha-numeric-symbol32-space

abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/

Mode: ● Automatic ○ Manual (Advanced Users)

Success: 95 %

Chain Length: 229376

Chain Count: 229146624

File Path: C:\ProgramData\PassMark\OSForensics\RainbowTables\lm_loweralpha-numer

☑ Compress to RTC format

Variable	Value
Estimated Time to Generate	96 days 8 hours 35 minutes
Hashes Per Second	6313428
No. of possible passwords	7555858447479
Required Disk Space	3496.50 MB
Success Rate	95.03%

To generate a **Rainbow Table**, fill in the input fields with the appropriate values under the Password Parameters box..

Under the **Hash Routine** field, select the hash routine that was used to encrypt the password into a hash. Currently, there are four hash routines to choose from, **md5**, **lm, ntlm,** and **sha1**.

Under the Password **Length** fields, select the suspected minimum and maximum length of the password.

Under the **Character Set** field, select the character set that contains the characters that the password is most likely to contain. The elements of the character set are listed in line following the name of that character set. For example, the character set "loweralpha" contains the lowercase letters of the alphabet.
Note: The size of the character set (i.e. the number of characters in that character set) will effect the efficiency of the recovery process. To decrease generation time, try to pick the smallest character set that also covers the possible characters of the password.

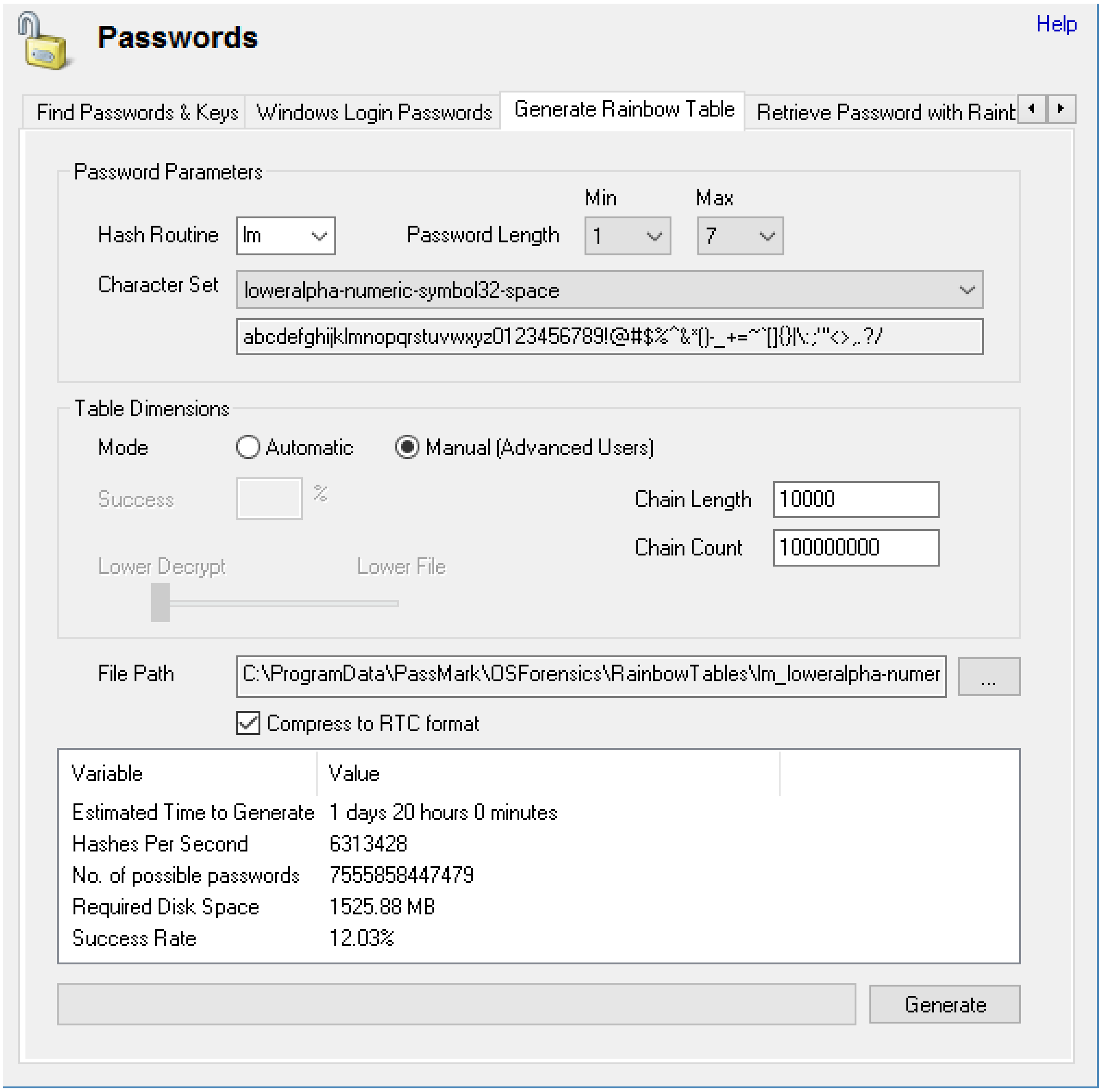
Before proceeding, use the **Automatic** and **Manual** radio buttons to select the input mode you would like to use in the Table Dimensions box. If you wish to input a success rate and have the dimensions calculated automatically, then select Automatic mode. Otherwise, if you wish to input the table dimensions (chain length and chain count) then select Manual mode.

Automatic mode

Under the **Minimum Success Rate** field, input the minimum success rate of recovering the password that you are willing to tolerate. A higher success rate will result in tables that are increasingly longer to generate, so the value should be as conservative as possible. The dimensions of the **Rainbow Table**, i.e. the **Chain Count** and **Chain Length** fields, will be filled out automatically. You can continue to adjust the **Chain Count** and **Chain Length** by using the Slider Control bar to achieve a desired balance between minimizing the decryption time and minimizing the file size. To begin generation, click the "Create Rainbow Table" button. Once generation has commenced, the process can be terminated by clicking "Cancel".

Manual mode

Fill in the **Chain Count** and **Chain Length** fields. If you are unsure about what these values mean, then it is recommended that you use **Automatic mode**. The Rainbow Table statistics will be calculated and displayed automatically. Increasing the size of the Rainbow Table will increase the generation time proportionately. Increasing the size also increases the success rate, but at a decreasing rate. Increasing the Chain Count will increase the Rainbow Table file size proportionately, while Increasing the Chain length will have no effect on the file size, but will increase the expected decryption time. To begin generation, click the "Create Rainbow Table" button. Once generation has commenced, the process can be terminated by clicking "Cancel".



Password Parameters

Hash Routine: lm

Password Length: Min 1, Max 7

Character Set: loweralpha-numeric-symbol32-space

abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/

Table Dimensions

Mode: ○ Automatic ● Manual (Advanced Users)

Success: %

Chain Length: 10000

Chain Count: 100000000

Lower Decrypt / Lower File

File Path: C:\ProgramData\PassMark\OSForensics\RainbowTables\lm_loweralpha-numer

☑ Compress to RTC format

Variable	Value
Estimated Time to Generate	1 days 20 hours 0 minutes
Hashes Per Second	6313428
No. of possible passwords	7555858447479
Required Disk Space	1525.88 MB
Success Rate	12.03%

File Naming

By default, a file name is given that denotes all the parameters of the Rainbow Table and generated Rainbow Tables will be saved in the OSForensics working folder under a folder named "RainbowTables". The default file name contains the parameters necessary to use the Rainbow Table for password recovery, and the default folder is also the folder used to populate the list of Rainbow Tables in the Recover Password feature. The save folder can be changed by clicking the "Save to folder..." button, but it is not possible to change the file name from the interface, as this is discouraged. If it is necessary to alter the filename, this can be done from explorer. If any parameter except the suffix is altered, the table will no longer be compatible with OSForensics. For more information on the file name convention used. please see File Naming Convention.

Note that if a Rainbow table of the same parameters is generated multiple times and saved in the same folder, OSForensics will assign a unique Rainbow table Index to the rainbow table so that the rainbow table is different from those previously generated.

RTC Format

RTC stands for Rainbow Table Compact. They are the result of .RT (raw rainbow table) files that have been compressed to save space. Since the raw data has been altered, they generally take a slightly longer time to extract passwords from. By default, OSForensics compresses rainbow tables to RTC format. This feature can be turned on/off simply by switching the "Compress to RTC format" checkbox.

4.13.3.1 Rainbow Tables

What are rainbow tables

Rainbow tables are tables of plain text passwords and hashes. They allow a password to be quickly looked up if a hash for that password is known.

What is a hash?
Passwords are generally not stored as plain text. Instead, passwords are stored as the output of a cryptographic hash function and the plain text password is discarded. Hashes are one-way mathematical operation, so the hash can be verified from a login page but can’t be reversed in theory. A password in plain text is given as input and a hash is created as output.

Plain text password input: TopSecret$89
MD5 Hash: FB34E3347894B0BA8AC2F34F56851095

Even if an attacker gained access to the hashed version of a password, it's not possible to directly reconstitute the password from the hash value alone. Common hashing algorithms have names like MD5, SHA1, SHA256.

Methods to recover the password?
Assuming the hashed password is known, or can be found on the system then there are 2 methods to recover the password. One is a brute force attack where every possible password is attempted until a match is found. This can be extremely slow, especially if it needs to be repeated for multiple hashes. The second method is to use a pre-computed table of hashes to speed up the process, known as rainbow tables.

Password space
With even short passwords there can be a lot of possible combinations, depending on the character set used. For example

Character set: A-Z
Password length: 1 to 7 character
Number of possible passwords: 8,353,082,582

Character set: A-Z and a-z and 0 to 9
Password length: 1 to 12 character
Number of possible passwords: 1,000,816,264,331,497,152

Rainbow table format
If every password and hash were stored in a file, the file would be enormous. Too large to be practical in fact. So instead of storing all possible hashes the data is divided up into “hash chains”. A hash chain is a sequence of hashes where each hash in the chain is generated from the prior hash. Only the beginning and end of the chain are then stored in the rainbow table. Dramatically reducing the size of

the file, but also increasing the time required to look up the file (as the chains need to be regenerated during the lookup process). So there trade off to be made in terms of file size, completeness of the table, lookup time and generation time.

Despite the optimisation of the table format, rainbow tables can still be very large. 500MB to several GB per table are common.

For each combination of hash algorithm, password lengths and character set a different rainbow table is required. So a MD5 table will only work on passwords encrypted with the MD5 algorithm. The smaller the password space, the smaller the table can be. Also not all possible hashes are generally stored in a table, so there is also a concept of success rate. A table with a 90% success rate can be expected to decrypt 9 out of 10 hashes. The higher the required success rate, the larger the table.

When rainbow tables won't work
Rainbow tables won't work, or are not practical, in the following situations.

1) The Password was encrypted with an unknown algorithm
2) The possible password length is long e.g. 12 characters or more
3) An unknown or random 'salt' is added to the password before hashing

It is also worth noting that no modern properly implemented password scheme is vulnerable. But there are still older, not so well implemented schemes, that are subject to attack.

Some common applications that use hashes
LM hash, an older hash algorithm used by Microsoft. LM hash is particularly vulnerable because passwords longer than 7 characters are broken into two sections, each of which is hashed separately. http://en.wikipedia.org/wiki/LM_hash

MySQL user accounts are listed in the user table of the mysql database. Each MySQL account is assigned a password, although what is stored in the Password column of the user table is not the plaintext version of the password, but a hash value computed from it. Password hash values are computed by the SQL PASSWORD() function. Prior to MySQL 4.1, password hashes computed by the PASSWORD() function are 16 bytes long. Such hashes look like this:

```
mysql> SELECT PASSWORD('mypass');
+-------------------------------------------+
| PASSWORD('mypass')                        |
+-------------------------------------------+
| *6f8c114b58f2ce9e                      |
+-------------------------------------------+
```

As of MySQL 4.1, the PASSWORD() function has been modified to produce a longer 41-byte hash value:

```
mysql> SELECT PASSWORD('mypass');
+-------------------------------------------+
| PASSWORD('mypass')                        |
+-------------------------------------------+
| *6C8989366EAF75BB670AD8EA7A7FC1176A95CEF4 |
+-------------------------------------------+
```

The Microsoft Windows NT/2000 family uses the LAN Manager and NT LAN Manager hashing method and is also unsalted, which makes it one of the more popularly generated tables.

Additional Information

Generating Rainbow Tables
Recovering Passwords Using Rainbow Tables
.RT Naming Convention

4.13.3.1.1 Compatible File Formats

OSForensics is fully compatible with .RT and .RTC, and partially compatible with .RTI file formats as long as the file name follows the correct naming convention.

OSForensics can generate and extract passwords from .RT and .RTC files.

OSForensics can extract passwords from .RTI files. OSForensics. RTI tables are available for download online at http://www.freerainbowtables.com/tables/.

RT Format

.RT files contain the raw values of the start and end points of each chain in a rainbow table. Each start and endpoint is an unsigned 64-bit integer value, and are also referred to as indexes. Chains are stored in ascending order with respect to their end point value.

Below is an example of a few rainbow chains in little endian.The start indexes are in purple and the end indexes are in blue.

```
000000000h: D2 0B 0E 00 00 00 00 00 91 06 00 00 00 00 00 00
000000010h: FA 2D 0E 00 00 00 00 00 9D 06 00 00 00 00 00 00
000000020h: CE 06 09 00 00 00 00 00 AD 06 00 00 00 00 00 00
000000030h: AB 03 04 00 00 00 00 00 AE 06 00 00 00 00 00 00
```

RTC Format (Rainbow Table Compact)

RTC Format is a compact version of RT format. It aims to save space by approximating the sorted end point values to a linear function, storing the parameters to this function in the header, and storing the error of each value to the linear function in place of the raw value. The number of bytes allocated to the start and end values of each chain is minimized and is stored in the header.

The advantage of RTC format over RT format is that it can potentially save a considerable amount of space. However, it is a generally slightly slower than RT format, due to the overhead of inverting the stored values back to the raw values.

RTI Format (Rainbow Table Indexed)

RTI Format is essentially and indexed version of RT format. RTI Format aims to saves space and increase search speed by indexing chains for every increase 2^16 (2 byte) increase in the end point values. The prefix (5 bytes) of each index entry, along with an additional 6 bytes is stored in the .rti.index file. For each chain, 6 bytes is given to the start point value, while 2 bytes are given for the suffix values of the end points. It is implied that start points values will lie within the 6 byte range and end points will lie within the 7 byte range.

4.13.3.1.2 File Naming Convention

Rainbow Table files in .RT, .RTC and .RTI format should follow a specific naming convention in order to be compatible with **OSForensics**. When Rainbow Tables are generated in **OSForensics** they will be given a default name (unless otherwise specified) that will follow this naming convention:

hashAlgorithmName_characterSetName_#minimumPasswordLength-maximumPasswordLength_RainbowTableIndex_ChainLength_ChainCount_OSF.rt*

For example:

"md5_alpha-numeric#1-5_0_20288x182592_OSF.rt"

4.13.3.1.3 How Chains are Generated

Rainbow tables are made up of chains of plaintext - hash pairs which we will refer to as 'rainbow chains'.

Generating the Chain

A rainbow chain is generated by producing a series of plaintext-hash pairs.

plaintext -> hash -> plaintext -> hash -> ... -> hash -> plaintext

The start of the rainbow chain, is a plaintext string that is generated randomly. To obtain a hash from a plaintext, the hash algorithm being used is applied to the plaintext. What isn't so obvious, is how to obtain the next plaintext. A mathematical function called a reduction function is applied to the hash to obtain the subsequent plaintext in the chain. The reduction function is essentially arbitrary, and can be defined in any way, as long as the same reduction function/s is used for the cracking process.

In a rainbow table, a different reduction function is used for each column, to avoid Rainbow Chains containing the same information.

This implementation uses a reduction function based on RainbowCrack 1.2. The reduction function is defined as follows:

f(hash) = (hash + i) % plaintext_space

where
i = the column number of the hash
plaintext_space = the plaintext space which is the total number of possible plaintexts/passwords given by the character set and the minimum and maximum plaintext lengths

This reduction function is suitable, because it is linear and can be computed fast.

A hash is usually represented by a hexadecimal number, is therefore essentially an integer, making it a suitable input for the reduction function. However the output will not immediately produce a plaintext. Thus there is an intermediate value, called an **index** that is produced by the reduction function. An index is simply an integer that corresponds to a plaintext/password. So in reality, a rainbow chain looks something like this:

index->plaintext->hash->**index**->plaintext->hash->...->hash->**index**

An index can be thought of, as an integer representation of a plaintext, in which the value of each plaintext depends on the character set and the plaintext space. For example, suppose we had a character set given by [abc] and a min/max plaintext length of 1. This would give us 3 possible passwords {a,b,c}. Then the indexes 0,1,2 would correspond to a, b, and c respectively.

The reduction function ensures that when the index produced, will always be within the appropriate range, which is [0,2] in this case, regardless of what the input hash is, by taking mod of the plaintext space, hence the name "reduction function".

This means that there is a space advantage in storing the indexes instead of storing either the hashes or plaintexts. The advantage of storing indexes over storing hashes is that the range of indexes stored will always be smaller than the range of hashes, which means there is more potential to save space should the file be compressed.

Similarly, it is more space conservative to store an index than to store the plaintext which would mean we would have to encode each individual ASCII character, which is inefficient since only a small portion of characters are used in a typical rainbow table.

Storing the Chain

The advantage of Rainbow tables, is that we do not need to retain every link in the chain in order to store all the information represented by the Rainbow Table. In fact, we only need to store the first and the last links in each chain to use the information effectively.

index~~->plaintext->hash->index->plaintext->hash->...->hash->~~**index**

All but the start and end index of the chain is discarded, and the indexes are written to file in binary, with the end indexes being sorted in ascending order, to allow for a binary search during decryption.

In a .RT file, both the raw values of the start and end index are stored as 64-bit integers. Below is an example of a few rainbow chains in little endian.The start indexes are in purple and the end indexes are in blue.

```
000000000h: D2 0B 0E 00 00 00 00 00 91 06 00 00 00 00 00 00
000000010h: FA 2D 0E 00 00 00 00 00 9D 06 00 00 00 00 00 00
000000020h: CE 06 09 00 00 00 00 00 AD 06 00 00 00 00 00 00
000000030h: AB 03 04 00 00 00 00 00 AE 06 00 00 00 00 00 00
```

There are various ways to store and compress rainbow tables. Please see Compatible File Formats for more information on this.

The parameters of the rainbow table file (including the hash algorithm, the number of chains, the chain length etc.) are kept in the filename. Please refer to .RT Naming Convention for details on how the parameters are stored.

4.13.3.1.4 Character Sets

Rainbow tables contain passwords belonging to a specific character set.

OSForensics uses a default list of character set definitions for both Rainbow Table generation and decryption.

Specifying a Character Set

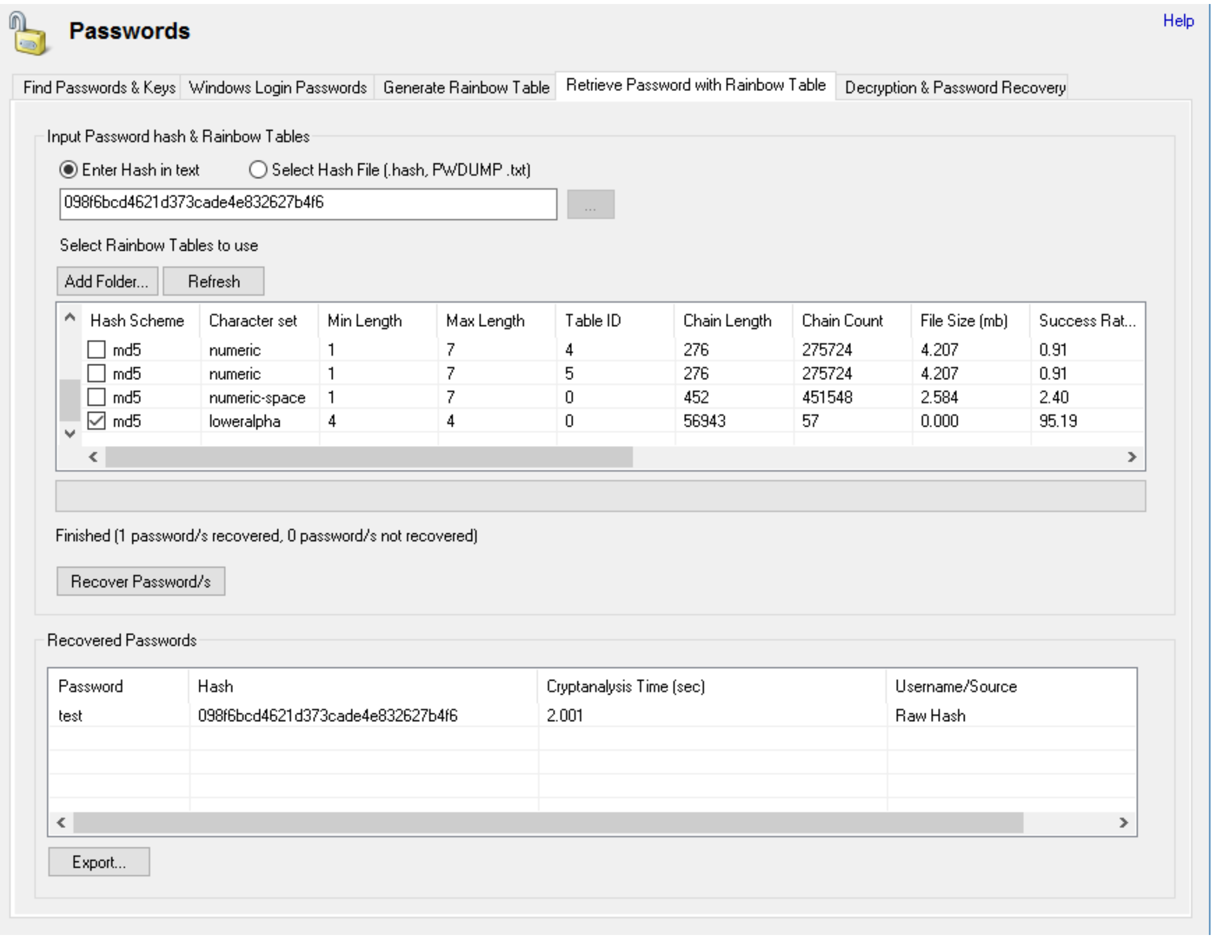
Users can specify a list of character set definitions by adding a configuration file named charset.txt to the RainbowTables folder in the OSForensics working path folder.

Inside charset.txt, there should be one character set definition per line. each character set definition should specify a character set name, and the contents of the character set inside square brackets assigned with an '='. For example:

```
alpha                          = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
alpha-space                    = [ABCDEFGHIJKLMNOPQRSTUVWXYZ ]
alpha-numeric                  = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
alpha-numeric-space            = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ]
alpha-numeric-symbol14         = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=]
```

4.13.4 Recovering Passwords Using Rainbow Tables

Passwords may be recovered using a suitable Rainbow Table and the hash of that password. Using this feature, a hash can be searched for within the Rainbow Table, and may successfully return the password in plain text.



Input Password hash & Rainbow Tables

● Enter Hash in text ○ Select Hash File (.hash, PWDUMP .txt)

098f6bcd4621d373cade4e832627b4f6

Select Rainbow Tables to use

Hash Scheme	Character set	Min Length	Max Length	Table ID	Chain Length	Chain Count	File Size (mb)	Success Rat...
□ md5	numeric	1	7	4	276	275724	4.207	0.91
□ md5	numeric	1	7	5	276	275724	4.207	0.91
□ md5	numeric-space	1	7	0	452	451548	2.584	2.40
☑ md5	loweralpha	4	4	0	56943	57	0.000	95.19

Finished (1 password/s recovered, 0 password/s not recovered)

Recovered Passwords

Password	Hash	Cryptanalysis Time (sec)	Username/Source
test	098f6bcd4621d373cade4e832627b4f6	2.001	Raw Hash

Before using this feature, either generate an appropriate Rainbow Table (see Generating Rainbow Tables), or use an existing rainbow table. Rainbow Tables are available for download from various sources online. We offer a small collection of sample Rainbow Tables that you can download for free from our website, but these are meant primarily as examples. For more serious investigations, you can purchase a hard drive containing a large collection of Rainbow Tables from our website: http://osforensics.com/rainbowtables_hashsets.html.

Rainbow tables in .RT, .RTC and .RTI format can be placed in the "RainbowTables" folder within the **OSForensics** working folder (Try *C:\ProgramData\PassMark\OSForensics\RainbowTables*). By default, tables generated by OSForensics will be saved in this folder. The refresh button can be clicked to update the list of Rainbow Tables if a table has just been created or moved to the RainbowTables folder in the same run of **OSForensics**. Tables in a folder can by added by clicking "Add Folder..." and then selecting a directory. Tables added in RTI format will be shown as a single entry in the Select Rainbow Tables list box.

Note that for **OSForensics** to recognize a Rainbow Table file it's file name must follow the File Naming Convention used by **OSForensics**.

Select the Rainbow Tables to search through by ticking the check box corresponding to that Rainbow Table. Note that selecting more rainbow tables can make the decryption process slower.

To recover a password using a Raw Hash, simply input the hash under the Raw Hash Field.

Decrypting a Hash List file

A hash list file contains one hash per line. To create a hash file, simply open a text file and write one hash per line. For example:

```
B03A340319A12864F8EBBD4FA5799B41
D253B68A594383481C80397D52C3A13E
3E8061DD481552E23DCC193F0B8C47E7
```

Then save the file with a .hash extension.

To recover passwords from a Hash List file, select the "Select File" radio button and then click the "..." button and select the file.

To start the decryption process click "Recover Password/s". To stop the process click "Cancel".

Decrypting a PWDUMP file

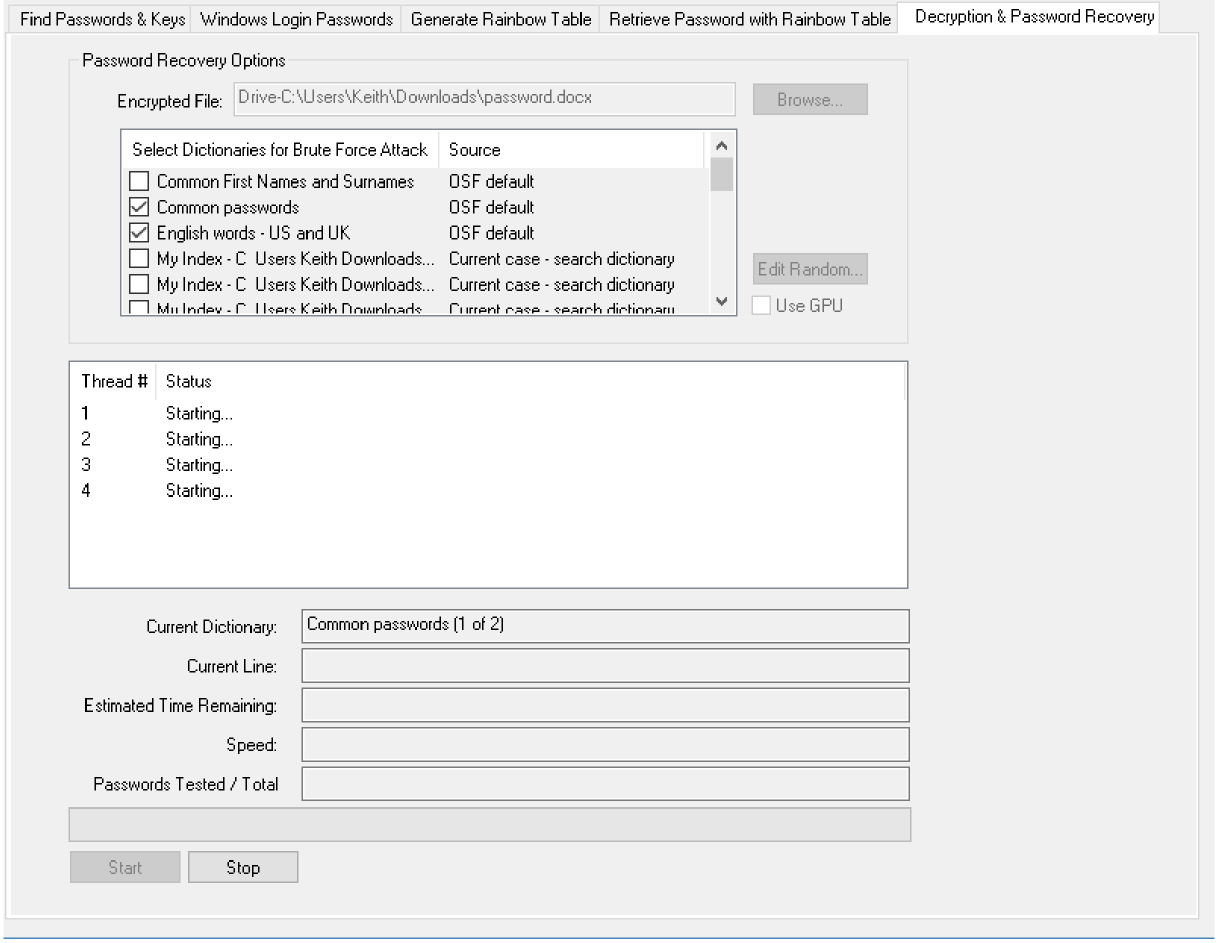
Either use an existing PWDUMP text file, or extract the LM hashes from a machine, use the Windows Login Passwords function in OSForensics, then save the extracted data to file.

"Select File" radio button and then click the "..." button and select the file.

To start the decryption process click "Recover Password/s". To stop the process click "Cancel".

4.13.5 File Decryption & Password Recovery

This function will allow you to decrypt files that use 40-bit encryption or run a dictionary based attack on files using different encryption methods to recover the password. OSForensics will display different options depending on the encryption method detected.



Encrypted File: Drive-C:\Users\Keith\Downloads\password.docx

Select Dictionaries for Brute Force Attack	Source
□ Common First Names and Surnames	OSF default
☑ Common passwords	OSF default
☑ English words - US and UK	OSF default
□ My Index - C Users Keith Downloads...	Current case - search dictionary
□ My Index - C Users Keith Downloads...	Current case - search dictionary
□ My Index - C Users Keith Downloads...	Current case - search dictionary

□ Use GPU

Thread #	Status
1	Starting...
2	Starting...
3	Starting...
4	Starting...

Current Dictionary: Common passwords (1 of 2)

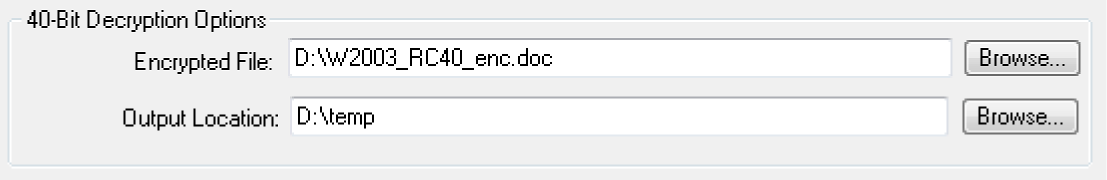
Current Line:

Estimated Time Remaining:

Speed:

Passwords Tested / Total

When OSForensics detects 40 bit encryption the following options will be displayed;



Encrypted File: D:\W2003_RC40_enc.doc

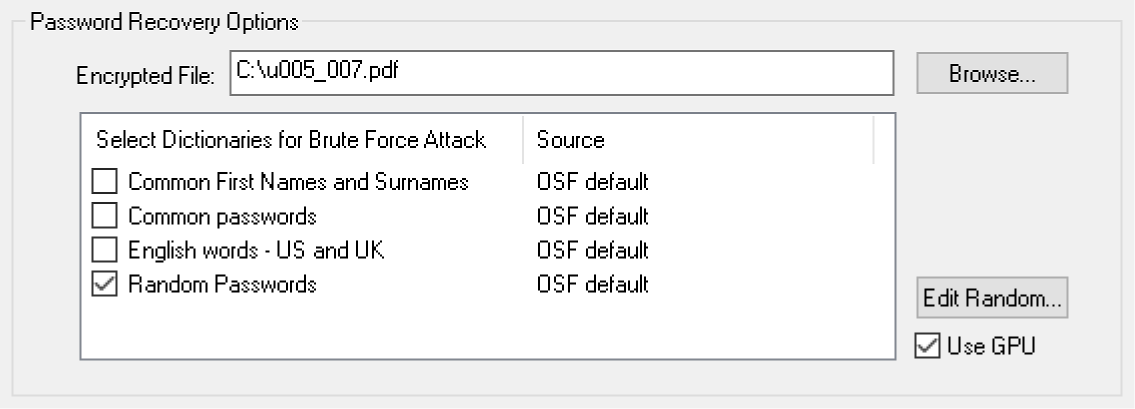
Output Location: D:\temp

Encrypted File: File name of a file encrypted using 40 bit keys. This can be a PDF, XLS or DOC file. To check if a PDF file uses 40 bit encryption you can open it in the OSForensics file and hex viewer, go to the meta data tab and check the "Encryption" entry, a version of 1.x can indicate 40bit encryption. For XLS and DOC files those encrypted in 97 and 2000 editions should use 40bit encryption.

Output Location: Working directory for temporary files and where decrypted output file is created.

40 bit decryption is guaranteed but can take several days, for example when running on an Intel® Core™2 Duo E8400 it can take approximately 1.8 days to test all the available 40bit keys.

When OSForensics detects other encryption methods the following options will be displayed;



Password Recovery Options

Encrypted File: C:\u005_007.pdf

Select Dictionaries for Brute Force Attack	Source
□ Common First Names and Surnames	OSF default
□ Common passwords	OSF default
□ English words - US and UK	OSF default
☑ Random Passwords	OSF default

☑ Use GPU

Encrypted File: File name of an encrypted file. The following file types are supported:

- Microsoft Office (doc, docx, docm, xls, xlsx, xlsb, ppt, pps, pptx, pptm, ppsm, pdf)
- Archives (zip, rar, 7z)
- OpenOffice (LibreOffice only) (odt, ott, odp, odf)

Select Dictionaries for Brute Force Attack: Clicking on the checkbox for a dictionary will select it for use with a brute force attack. If you have created a search index for the current case the dictionaries from these indexes will be available to use here. OSForensics provides several different dictionary options;

Common Passwords: This is a list of common used passwords created from statistical lists and published passwords lists.

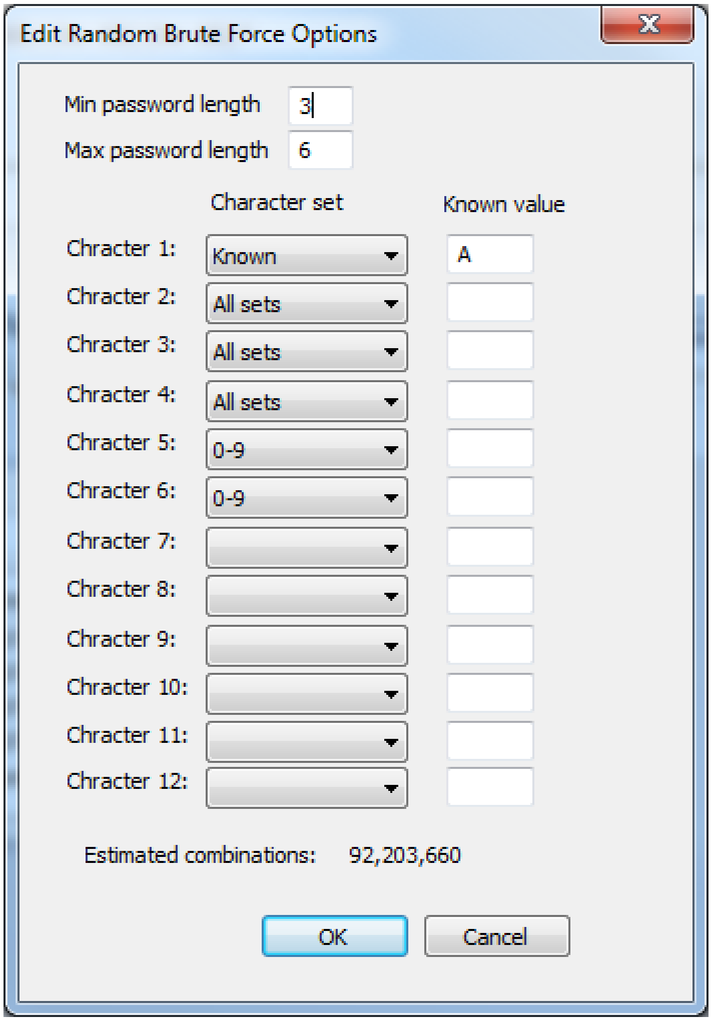
English words - US and UK: an English based dictionary. This dictionary contains 79165 lowercase words in a combination of UK and US spelling. After testing all lowercase words the first letter of each is capitalized and tested again. This word list was combined from several Ispell word lists.

Names: This is a list of common first names and surnames from the US, UK, Europe and Asia (550 in total). Each name is tried separately and then as various combinations which results in approximately 165,000 combinations.

Random: Depending on the settings chosen (see the **Edit Random** section) will generate different random passwords based on a combination of letters, symbols and numbers.

The rest of the entries in the list are the available search indexes from the currently select case. See the "Adding Dictionaries" section for information on how to add your own custom dictionaries.

Edit Random



Edit Random Brute Force Options

Min password length 3

Max password length 6

	Character set	Known value
Chracter 1:	Known	A
Chracter 2:	All sets	
Chracter 3:	All sets	
Chracter 4:	All sets	
Chracter 5:	0-9	
Chracter 6:	0-9	
Chracter 7:		
Chracter 8:		
Chracter 9:		
Chracter 10:		
Chracter 11:		
Chracter 12:		

Estimated combinations: 92,203,660

This feature is applied when only the "Random Passwords" dictionary is selected.

Min: Minimum password length

Max: Maximum password length

Character 1 - 12: For each character in the password the type of character it can be needs to be selected from the options;

- All sets - all available characters
- a-z - all lower case letters from a - z
- A-Z - all uppercase letters from A - Z
- a-z & A-Z - both cases of letters a - z
- 0-9 - all numbers from 0 - 9
- a-z & A-Z & 0-9 - all alphanumeric characters
- ~@#$% - special characters {}:"<>?[];\',./~!@#$^&*()_+`-=|
- Known - a known character, must be typed in the edit box for the character

The number of combinations will be displayed when the password parameters are changed. The image above will test password from 3 - 6 characters long, starting with "A", followed by up to 3 letters, symbols or numbers, and ending in up to 2 digits (For example, "A##", "A12z", "Abc#12" would all be generated by this option) and results in over 92 million passwords.

Use GPU

This option only applies for when the above method (Random Passwords) is being used.
Checking this box will enable use of the GPU for faster cracking. Note that not all GPUs are supported.

Start

When the "Start" button is clicked, decryption will begin in which a number of threads will be launched, one for each available logical processor. For example on a machine with a quad core CPU 4 threads will be launched. If "Use GPU" is checked, a single GPU thread, plus a CPU thread equal to the number of available logical processors minus one, will be launched.

Clicking the "Stop Decrypting" button will stop the threads. When decrypting a 40 bit file, if the temporary files have not been deleted when "Start Decryption" is clicked again decryption will resume from where it was last stopped.

4.13.5.1 Adding Dictionaries

The dictionary and password definition file used by OSForensics are located in the "OSForensics\PasswordRecovery\PDF" folder (in Win7/Vista this will default to C:\ProgramData\PassMark\OSForensics\PasswordRecovery\PDF) .To add your own custom dictionary you will need to create 2 files in this directory - a dictionary file (.dic) and a definition file (.def).

The dictionary file is a list of words, one word per line, for example;

```
aardvark
aardvark's
aardvarks
aaron
```

The definition file is a structured file that is used to set which dictionary is being used and can be used to make alterations to the words in the dictionary.
To define a dictionary use $w = "dictionary name", and $u = "dictionary name" if you want to combine two dictionaries.

"##" is a required section of the file and marks the end of the dictionary setup. After this you can use $w and $u to refer to a word from each dictionary, and use modifiers to alter the words.

The simplest definition file, that loads a dictionary and then tests each word in the dictionary is;

```
$w = "dictionary_name.dic"
##
$w
```

To use a modifier to capitalize the first letter of each word in the dictionary, effectively doubling the number of passwords, you can use "$w.u(1)".

```
$w = "english-us-uk-combined.dic"
##
$w
$w.u(1)
```

The other modifiers available are;

.u (upper)	to upper-case
.l (lower)	to lower-case
.t (truncate)	to truncate up to the given length
.j (joke)	to upper-case some letters
.r (reverse)	to reverse the word
.s(shrink)	to shrink the word
.d (duplicate)	to duplicate the word

Each modifier will accept a parameter in after itself,

.u or .u(0)	to upper-case the whole word (PASSWORD)
.u(1), .u(2)	to upper-case only the first (the second) letter (Password, pAssword)
.u(-), .u(-1)	to upper-case the last (the next to last) letter (passworD, passwoRd)
.t(-1)	to truncate the last letter in the word (passwor)
.j(0) or .j	to upper-case odd letters (PaSsWoRd)
.j(1)	to upper-case even letters (pAsSwOrD)
.j(2)	to upper-case vowels (pAsswOrd)
.j(3)	to upper-case consonants (PaSSWoRD)
.r(0) or .r	to reverse the word (drowssap)
.s(0) or .s	to reduce the word by discarding vowels unless the first one is a vowel (password -> psswrd, offset -> offst)
.d(0) or .d	to duplicate the word (passwordpassword)
.d(1)	to add reversed word (passworddrowssap)

4.13.6 Ispell Copyright Notice

Copyright 1993, Geoff Kuenning, Granada Hills, CA
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All modifications to the source code must be clearly marked as such. Binary redistributions based on modified source code must be clearly marked as modified versions in the documentation and/or other materials provided with the distribution.
4. All advertising materials mentioning features or use of this software must display the following acknowledgment:
   This product includes software developed by Geoff Kuenning and other unpaid contributors.
5. The name of Geoff Kuenning may not be used to endorse or promote products derived from this software without specific prior written permission.

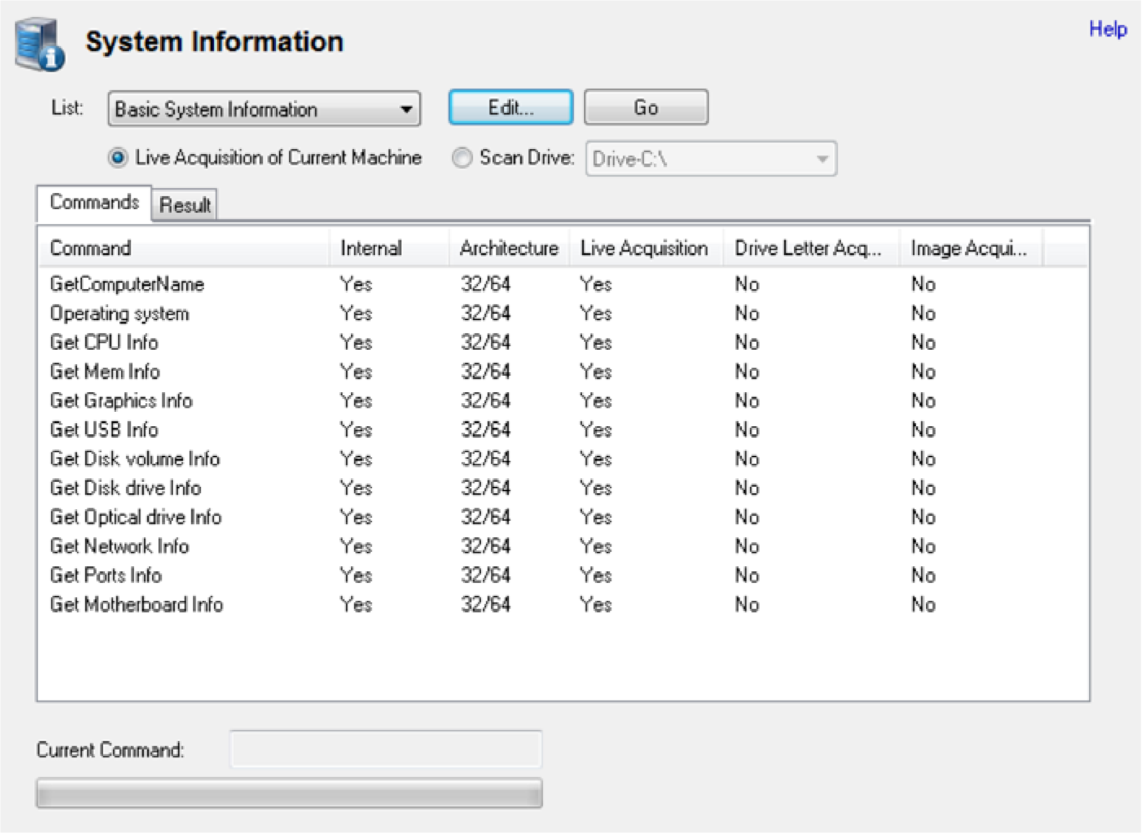
THIS SOFTWARE IS PROVIDED BY GEOFF KUENNING AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL GEOFF

KUENNING OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

4.14 System Information

The System Information module allows retrieval of detailed information about the core components of the system. This module comes with built-in test test lists that can retrieve the core details about the system such as;

- CPU, Motherboard and Memory
- BIOS
- Video card/Display devices
- USB controllers and devices
- Ports (Serial/Parallel)
- Network adapters
- Physical and Optical Drives



List: Basic System Information

● Live Acquisition of Current Machine ○ Scan Drive: Drive-C:\

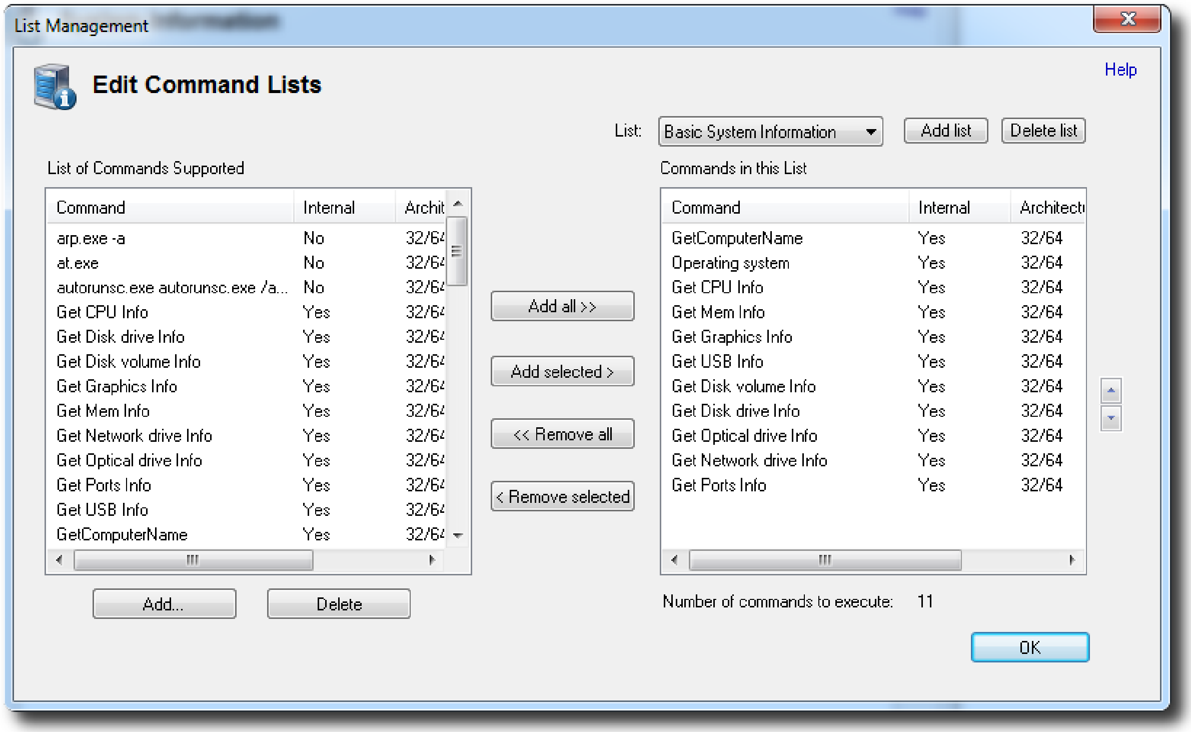
Command	Internal	Architecture	Live Acquisition	Drive Letter Acq...	Image Acqui...
GetComputerName	Yes	32/64	Yes	No	No
Operating system	Yes	32/64	Yes	No	No
Get CPU Info	Yes	32/64	Yes	No	No
Get Mem Info	Yes	32/64	Yes	No	No
Get Graphics Info	Yes	32/64	Yes	No	No
Get USB Info	Yes	32/64	Yes	No	No
Get Disk volume Info	Yes	32/64	Yes	No	No
Get Disk drive Info	Yes	32/64	Yes	No	No
Get Optical drive Info	Yes	32/64	Yes	No	No
Get Network Info	Yes	32/64	Yes	No	No
Get Ports Info	Yes	32/64	Yes	No	No
Get Motherboard Info	Yes	32/64	Yes	No	No

Once the commands have executed the output will appear on the results tab and can then be saved to a file or to case.

The default "Basic System Information" list can only be run on the local live system (Live acquisition only). The "System Information From Registry" list can be run on either the local system or on a specified drive letter, device or image. Currently these are the only commands that make use of the "Live acquisition of current machine" and "Scan drive" options. The other internal commands only run on the live system and external tools that have been added by a user will run on either the live system or a drive letter specified in the command itself. These commands, "Get Computer Name (Registry)", "Get Timezone Info (Registry)", "Get Network Info (Registry)" and "Get User Info (Registry)" will search for registry files available on the image, drive selected or the live system depending on the option selected.

If you have a number of different commands selected and choose the "Scan drive" option then only the commands that support changing their target location (the registry command mentioned above) will run on this drive letter while the others will execute at their default locations.

While OSForensics comes with four default command lists that can gather a fair bit of useful information you may want to customize or add to these lists. By clicking the edit button you can go to the list management window.



List: Basic System Information

List of Commands Supported

Command	Internal	Archit
arp.exe -a	No	32/64
at.exe	No	32/64
autorunsc.exe autorunsc.exe /a...	No	32/64
Get CPU Info	Yes	32/64
Get Disk drive Info	Yes	32/64
Get Disk volume Info	Yes	32/64
Get Graphics Info	Yes	32/64
Get Mem Info	Yes	32/64
Get Network drive Info	Yes	32/64
Get Optical drive Info	Yes	32/64
Get Ports Info	Yes	32/64
Get USB Info	Yes	32/64
GetComputerName	Yes	32/64

Commands in this List

Command	Internal	Architecti
GetComputerName	Yes	32/64
Operating system	Yes	32/64
Get CPU Info	Yes	32/64
Get Mem Info	Yes	32/64
Get Graphics Info	Yes	32/64
Get USB Info	Yes	32/64
Get Disk volume Info	Yes	32/64
Get Disk drive Info	Yes	32/64
Get Optical drive Info	Yes	32/64
Get Network drive Info	Yes	32/64
Get Ports Info	Yes	32/64

Number of commands to execute: 11

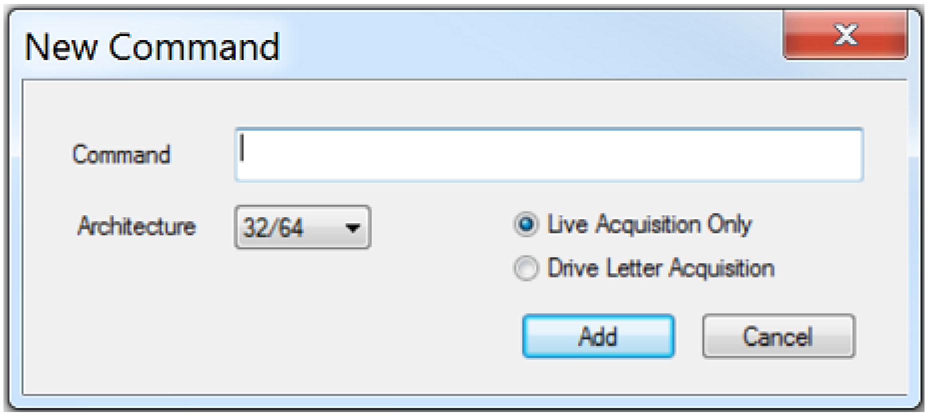
New external tools can be added using the Add button below the list of all commands supported. Also note that some of the default supported commands require external tools to be installed. See the External Tools page for more information.

4.14.1 External Tools

New third party tools can be easily added to the test suite. There are many applications which can be helpful in retrieving system information. These tools must first be installed if these commands will run correctly.

To install a new external tool simply place it in one of the following folders depending on your operating system;
Vista / Win7: C:\ProgramData\PassMark\OSForensics\SysInfoTools\
XP: C:\Documents and Settings\All Users\Application Data\PassMark\OSForensics\SysInfoTools\

To use one a new tool you added to this folder you need to add a command from the list management window using the add button below the list of all commands supported.



New Command

Command:

Architecture: 32/64

● Live Acquisition Only
○ Drive Letter Acquisition

The command should be the executable with any command line parameters needed. By default OSForensics gathers data from the command line output of the tool. There are also wildcards that can be used to have OSForensics fill in the details at run time.
%d: Places a drive letter in the form "c:", the drive letter is the current cases default drive or c if no case is open
%t: Inserts a path to a temp file, when this command is specified OSForensics will gather data from this file rather than from the command line output of the command.

Architecture specifies whether this command should be restricted to 32 or 64 bit systems.
The "Live Acquisition only" option specifies that the command should only run when during a live acquisition, otherwise the "Drive Letter Acquisition" should be chosen and can be executed when a drive letter is chosen for the "Scan drive" option.

There are a few internal functions of OSForensics that are able to be run on a live acquisition, on a drive letter or directly on an image (image acquisition) a that has been added to the case.

While none of the default test lists use any external tools, a number of commands are pre-configured to be added. These tools are listed here.

- Autorunsc: This tool gives comprehensive knowledge of auto-starting locations of any startup monitor.
- handle.exe: This is command line version of process explorer.
- PSTools: Its a very useful set of tools which include the following individual tools:
  - PsExec - execute processes remotely
  - PsFile - shows files opened remotely
  - PsGetSid - display the SID of a computer or a user
  - PsInfo - list information about a system
  - PsKill - kill processes by name or process ID

  - PsList - list detailed information about processes
  - PsLoggedOn - see who's logged on locally and via resource sharing (full source is included)
  - PsLogList - dump event log records
  - PsPasswd - changes account passwords
  - PsService - view and control services
  - PsShutdown - shuts down and optionally reboots a computer
  - PsSuspend - suspends processes
  - PsUptime - shows you how long a system has been running since its

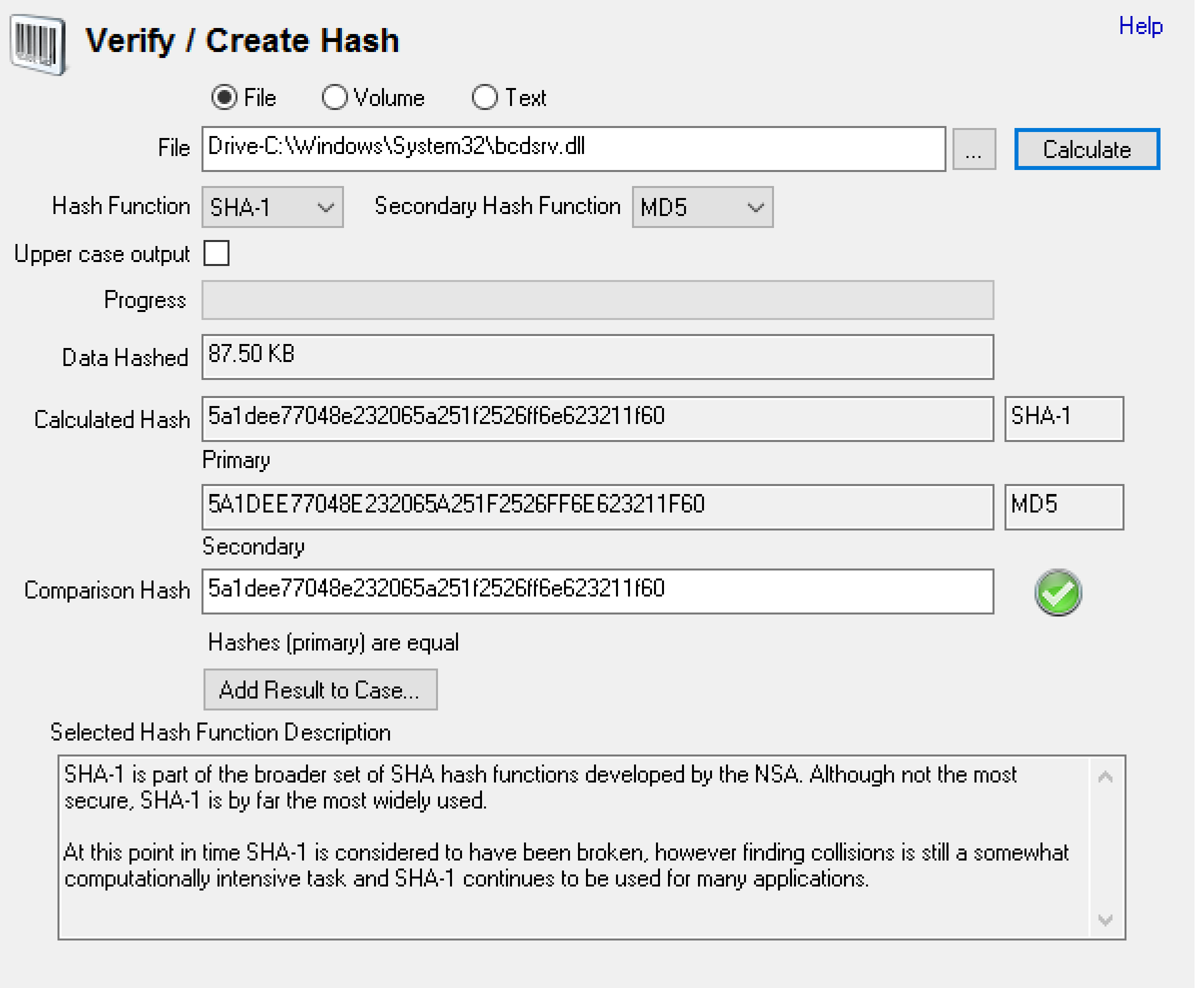
- showgrps.exe: This command-line tool shows the groups to which a user belongs within a given network domain.
- srvcheck.exe: SrvCheck is a simple ping-like program, which can check the availability of a given server. Part of Windows Server 2003 Resource Kit Tools package. Supports Windows Server 2003 and Windows XP. Not supported on 64 bit platform.

The above tools are maintained and distributed freely. These tools can be downloaded from following locations:

- Autorunsc: http://technet.microsoft.com/en-us/sysinternals/bb963902
- handle.exe:http://technet.microsoft.com/en-us/sysinternals/bb896655
- PSTools:http://technet.microsoft.com/en-us/sysinternals/bb896649
- showgrps.exe: http://technet.microsoft.com/en-us/systemcenter/bb676805.aspx
- srvcheck.exe: http://www.microsoft.com/downloads/en/confirmation.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en

4.15 Verify / Create Hash

The Verify / Create Hash module is used for verifying the integrity of files by calculating its hash value. It can also be used to create a hash of a whole partition or physical disk drive or a simple text string.



● File ○ Volume ○ Text

File: Drive-C:\Windows\System32\bcdsrv.dll

Hash Function: SHA-1 — Secondary Hash Function: MD5

Upper case output □

Progress:

Data Hashed: 87.50 KB

Calculated Hash: 5a1dee77048e232065a251f2526ff6e623211f60 — SHA-1

5A1DEE77048E232065A251F2526FF6E623211F60 — MD5

Comparison Hash: 5a1dee77048e232065a251f2526ff6e623211f60 ✓

Hashes (primary) are equal

Selected Hash Function Description

SHA-1 is part of the broader set of SHA hash functions developed by the NSA. Although not the most secure, SHA-1 is by far the most widely used.

At this point in time SHA-1 is considered to have been broken, however finding collisions is still a somewhat computationally intensive task and SHA-1 continues to be used for many applications.

To calculate a hash for a file, simply input the file path, select one of the available hash functions and press Calculate. To verify the calculated hash with a known hash value, copy the known hash value into the Comparison Hash field.

To create a hash for a partition or drive, select the 'Volume' radio button and then use the drop down to select from the available drives and partition. Note that administrator privileges are required for this feature.

To create a hash of a line of text select the text option and type or paste the text you want to hash into the text field.

Hash Function / Secondary Hash Function

Specify the hash function to use for hashing. A secondary hash function can also be specified to calculate the hash value simultaneously.

Upper case output

If checked, the calculated hash will be in upper case.

Add Result to Case...

Save the result of the hash calculation and add to the case.

4.16 Hash Sets

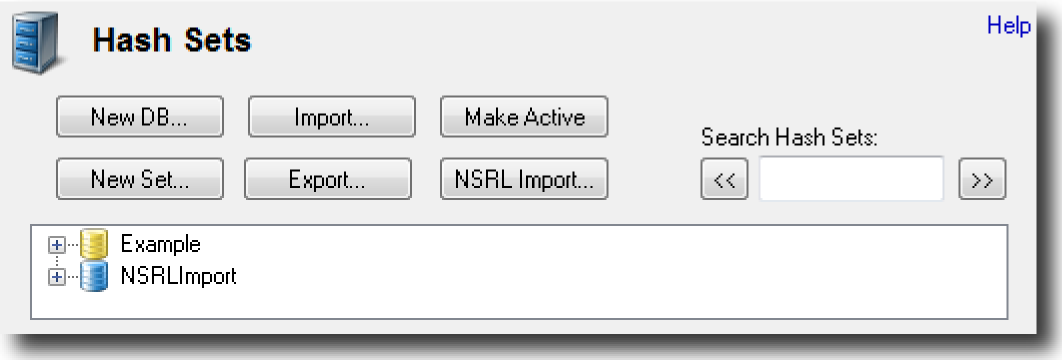
Hash Sets allow an investigator to quickly identify known safe files (such as Operating System and program files) or known suspected files (such as viruses, trojans, hacker scripts) to reduce the need for further time-consuming analysis. Hash Sets are used in a data analysis technique called Hash Analysis, which uses the MD5, SHA1 and SHA256 hash of files to verify the files on a storage device. A hash uniquely identifies the contents of a file, regardless of filename. In other words, any two files with the same hash are said to be the same. A collection of these hash values form a hash set, which can be used to reduce the time required to search a storage media for particular files of interest. In particular, files that are known to be safe or trusted can be eliminated from file searches. Hash sets can also be used to identify the presence of malicious, contraband, or incriminating files such as bootleg software, pornography, viruses and evidence files.

It is recommended when creating hash databases that safe files be kept in a sperate database to files that are illegal/incriminating.

Once the hash sets are created, they shall be used throughout OSF where applicable (such as File Searching).

Included as part of OSForensics are sample hash sets from NSRL, a US government project that provides a repository for hash sets of known files. Additional sample hash sets can be downloaded from the Passmark website.

Hash Set Management



New DB
Creates a new empty database. Clicking this button will prompt the user to provide a name for the database. After a valid name is entered, the database will appear in the list ready for use.

New Set
Creates a new hash set in the currently active database. Clicking this button will open the New Hash Set window where you can specify the creation options.

Export
Exports the currently selected item to csv format. If a single hash set is selected, then just the selected hash set is exported. If any other item is selected (eg. origin, DB) then all hash sets contained are exported.W

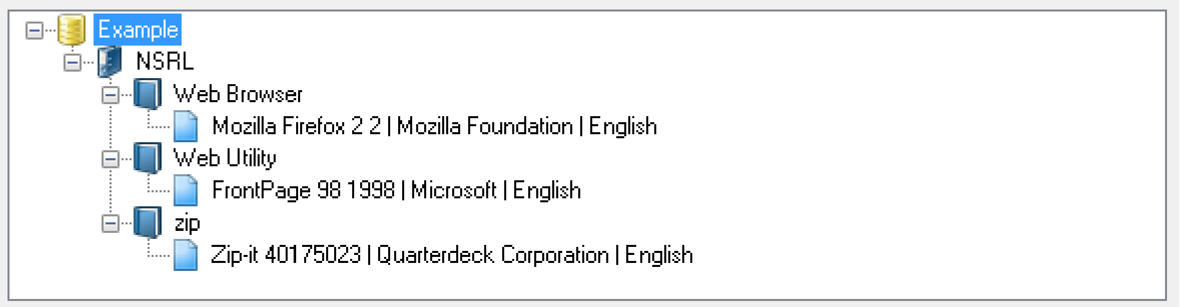
Import
Imports a hash set that was previously exported from OSF in csv format back into the currently active database.

Make Active
Makes the currently selected database active. The active database is the database that shall be used for all operations in OSF requiring hash sets. You can also make a DB active via right-click and selecting "Make Active". The currently active database is highlighted in yellow.

NSRL Import
Imports the NSRL (http://www.nsrl.nist.gov/) dataset into an OSForensics database. See this page for detailed instructions.

Search Hash Sets
This search box allows the user to search for a hash set by name. The search applies to all databases in the list. Enter all or part of the hash set name and use the ">>" and "<<" to move forwards and backwards through the list. The search is case insensitive.

Hash Set List



```
Example
  NSRL
    Web Browser
      Mozilla Firefox 2 2 | Mozilla Foundation | English
    Web Utility
      FrontPage 98 1998 | Microsoft | English
    zip
      Zip-it 40175023 | Quarterdeck Corporation | English
```

The hash set list displays a list of all hash sets under the following hierarchy:

Database
    |-- **Origin**
        |-- **Product Type**
            |-- **Hash Set**

Double clicking on a hash set will allow you to view its contents. Items (excluding databases) may be dragged and dropped to copy hash set(s) within/across databases. Right clicking on items in the list allows you to perform actions such as renaming and deleting.

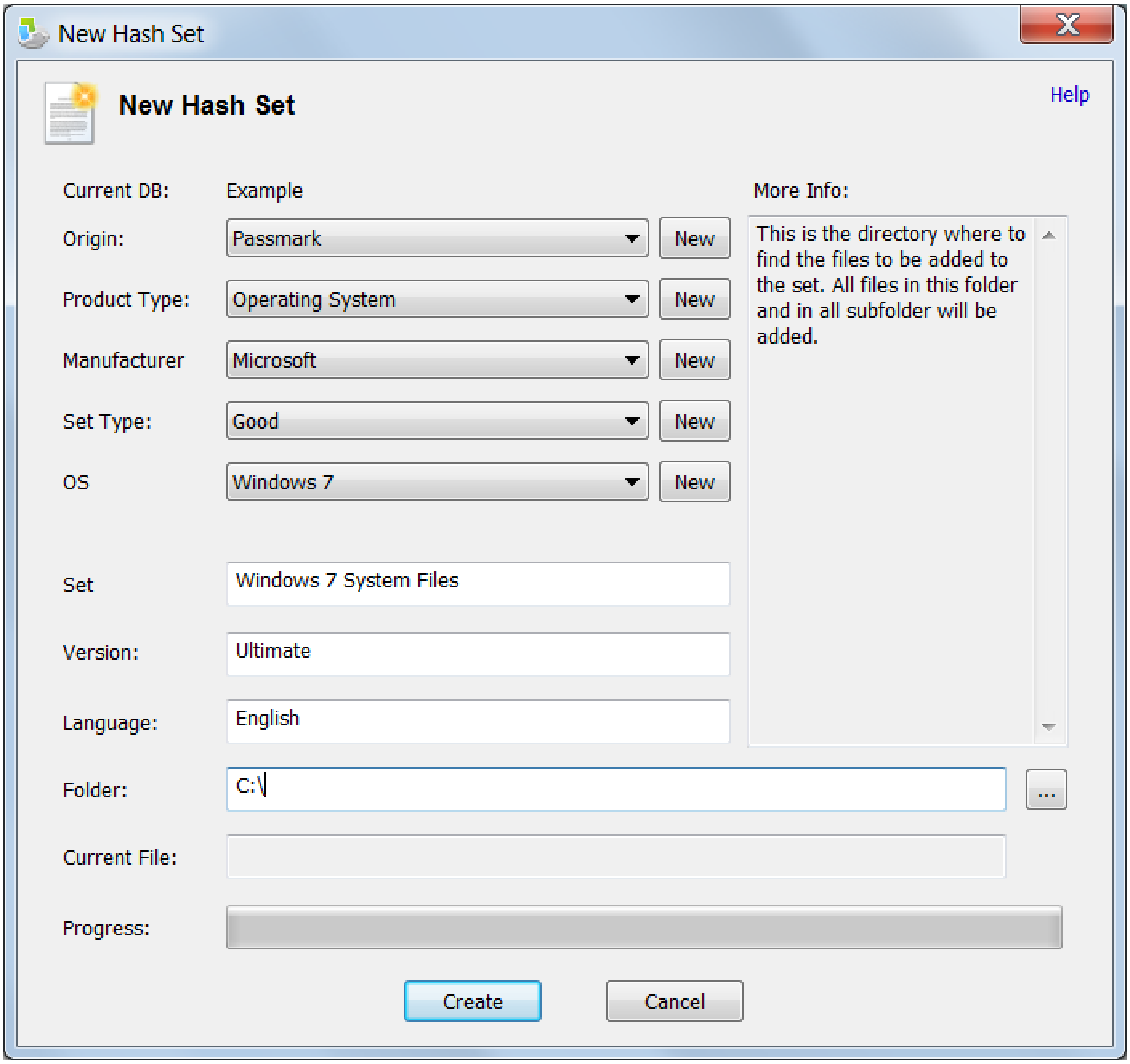
Due to the relational nature of the database, be aware that all Product Types appear under all Origins, regardless of whether they have any content.

Other Information

Installing Hash sets
Hash Set Lookup

4.16.1 New Hash Set

The New Hash Set window allows the user to enter the attributes for generating a new hash set. This window can be accessed by clicking on the "New Set" button in the main Hash Sets window.



Current DB: Example

Origin: Passmark

Product Type: Operating System

Manufacturer: Microsoft

Set Type: Good

OS: Windows 7

Set: Windows 7 System Files

Version: Ultimate

Language: English

Folder: C:\

Current File:

Progress:

More Info:

This is the directory where to find the files to be added to the set. All files in this folder and in all subfolder will be added.

Current DB
The name of the database that the hash set will belong to.

Origin
The origin of the files belonging to the hash set. Depending on the scope of the database this could be as specific as "Bob's PC" or as broad as an entire organization.

Product Type
The product type the files are associated with. *Eg. Word Processor, Image Editor, Operating System.*

Manufacturer
The original creator of the files in the hash set. *Eg. Apple, Microsoft, Google*

Set Type
A classification for the set of files. *Eg. Safe, malware, bootleg, trusted*

OS

The Operating System the files are associated with.

Set Name
The name for the hash set. Hash set names should briefly describe the contents of the hash set. *Eg. Windows XP system files, viruses, blueprints.*

Version
The version of the product the files are associate with. *Eg. Microsoft Word 2007, Adobe Reader 9.*

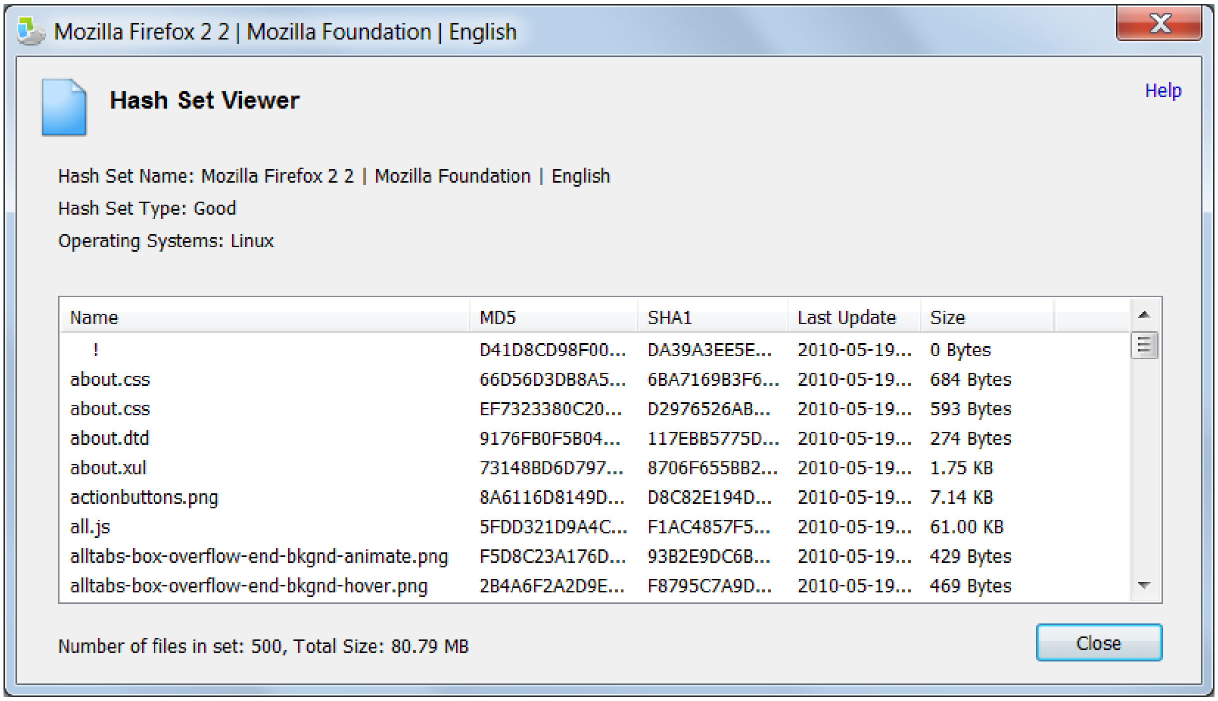
Language
The language of the files in the set.

Folder
The directory to be scanned for files to be added to the hash set. All files and subdirectories in this folder shall be added to the hash set.

Current File
The file that is currently being processed.

4.16.2 View Hash Set

The Hash Set Viewer window allows the user to view the details about an existing hash set. This window can be accessed by double clicking on a hash set or via the right click context menu in the main Hash Sets window.



Mozilla Firefox 2 2 | Mozilla Foundation | English

Hash Set Viewer

Hash Set Name: Mozilla Firefox 2 2 | Mozilla Foundation | English

Hash Set Type: Good

Operating Systems: Linux

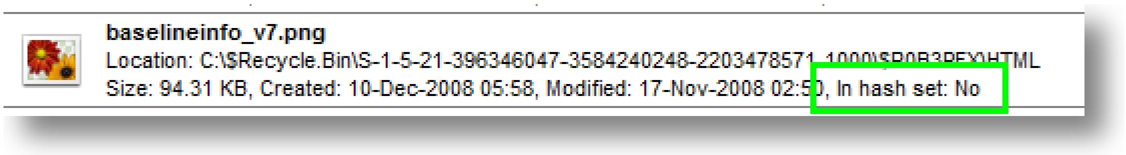
Name	MD5	SHA1	Last Update	Size
!	D41D8CD98F00...	DA39A3EE5E...	2010-05-19...	0 Bytes
about.css	66D56D3DB8A5...	6BA7169B3F6...	2010-05-19...	684 Bytes
about.css	EF7323380C20...	D2976526AB...	2010-05-19...	593 Bytes
about.dtd	9176FB0F5B04...	117EBB5775D...	2010-05-19...	274 Bytes
about.xul	73148BD6D797...	8706F655BB2...	2010-05-19...	1.75 KB
actionbuttons.png	8A6116D8149D...	D8C82E194D...	2010-05-19...	7.14 KB
all.js	5FDD321D9A4C...	F1AC4857F5...	2010-05-19...	61.00 KB
alltabs-box-overflow-end-bkgnd-animate.png	F5D8C23A176D...	93B2E9DC6B...	2010-05-19...	429 Bytes
alltabs-box-overflow-end-bkgnd-hover.png	2B4A6F2A2D9E...	F8795C7A9D...	2010-05-19...	469 Bytes

Number of files in set: 500, Total Size: 80.79 MB

The table contains a list of files in the hash set and corresponding hash values.

4.16.3 Hash Set Lookup

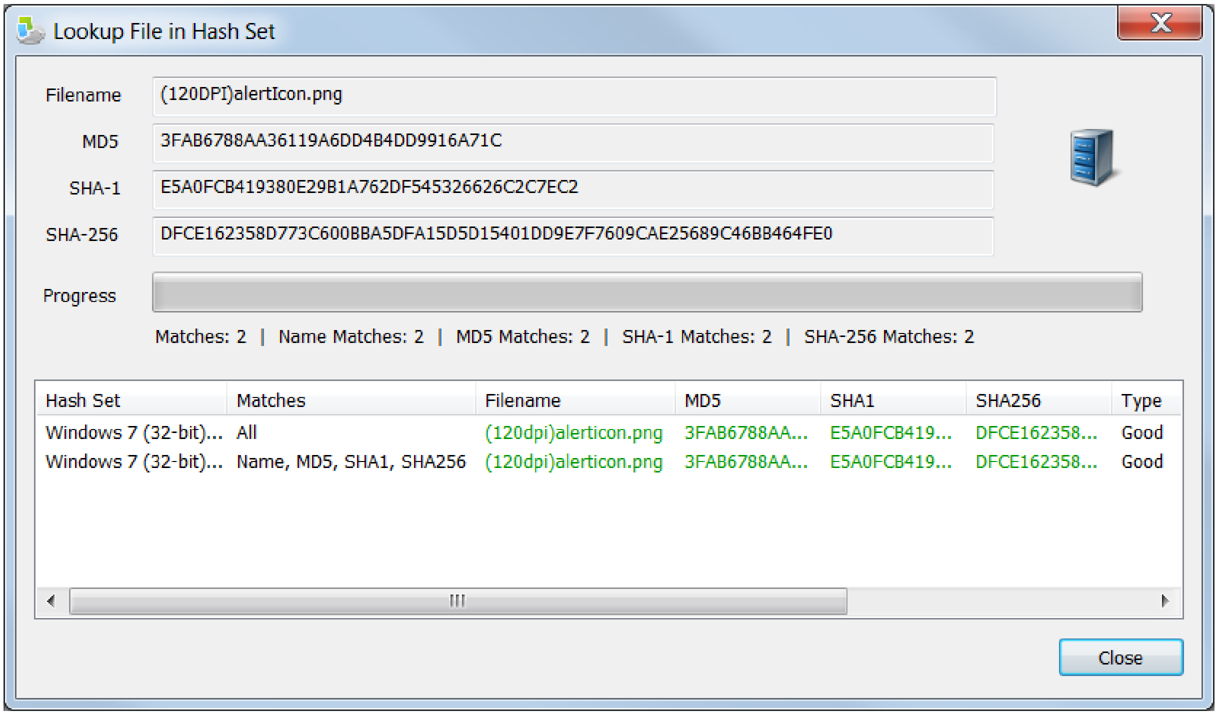
In either the file name search or the mismatch search it is possible to do a lookup on the files found to see if they exist within the current hash database. This is accomplished by right clicking in the list and choosing "Look up in Hash Set". Depending on wether you do this for a single file or multiple files you will get a different interface. In both cases however the file will be marked in the original list as to wether a match was found.



baselineinfo_v7.png
Location: C:\$Recycle.Bin\S-1-5-21-396346047-3584240248-2203478571-1000\$R0B3PFX\HTML
Size: 94.31 KB, Created: 10-Dec-2008 05:58, Modified: 17-Nov-2008 02:50, In hash set: No

Single File Hash Lookup

The results of the lookup are displayed in the table, listing any matches that were found in a hash set in the active database.



Lookup File in Hash Set

Filename: (120DPI)alertIcon.png
MD5: 3FAB6788AA36119A6DD4B4DD9916A71C
SHA-1: E5A0FCB419380E29B1A762DF545326626C2C7EC2
SHA-256: DFCE162358D773C600BBA5DFA15D5D15401DD9E7F7609CAE25689C46BB464FE0

Progress

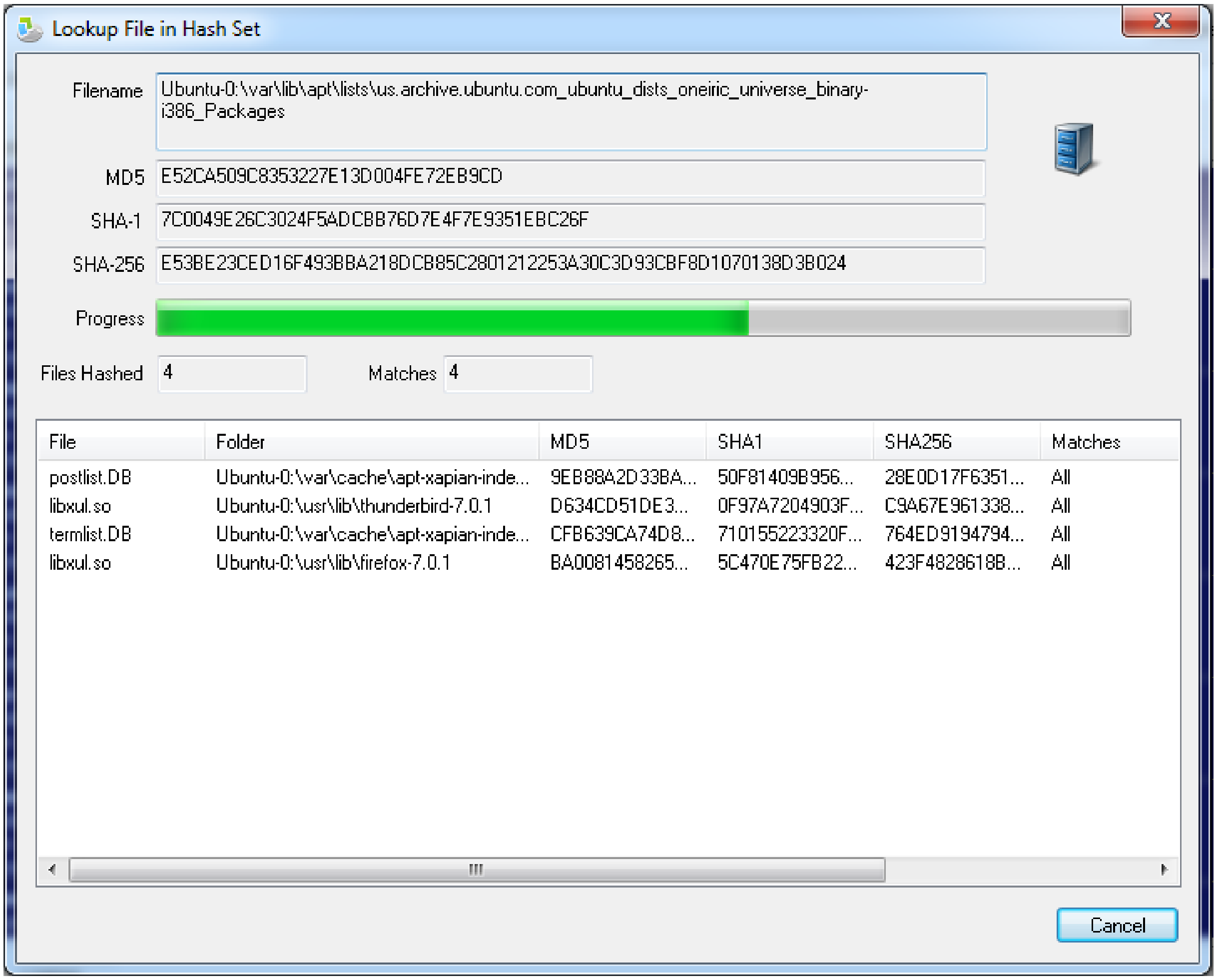
Matches: 2 | Name Matches: 2 | MD5 Matches: 2 | SHA-1 Matches: 2 | SHA-256 Matches: 2

Hash Set	Matches	Filename	MD5	SHA1	SHA256	Type
Windows 7 (32-bit)...	All	(120dpi)alerticon.png	3FAB6788AA...	E5A0FCB419...	DFCE162358...	Good
Windows 7 (32-bit)...	Name, MD5, SHA1, SHA256	(120dpi)alerticon.png	3FAB6788AA...	E5A0FCB419...	DFCE162358...	Good

Elements colored green indicate matches.

Multiple Files Hash Lookup

When hash comparing multiple files at once, the files that matched the entries contained in the hash set are displayed in the list view.



Filename: Ubuntu-0:\var\lib\apt\lists\us.archive.ubuntu.com_ubuntu_dists_oneiric_universe_binary-i386_Packages

MD5: E52CA509C8353227E13D004FE72EB9CD

SHA-1: 7C0049E26C3024F5ADCBB76D7E4F7E9351EBC26F

SHA-256: E53BE23CED16F493BBA218DCB85C2801212253A30C3D93CBF8D1070138D3B024

Progress

Files Hashed: 4

Matches: 4

File	Folder	MD5	SHA1	SHA256	Matches
postlist.DB	Ubuntu-0:\var\cache\apt-xapian-inde...	9EB88A2D33BA...	50F81409B956...	28E0D17F6351...	All
libxul.so	Ubuntu-0:\usr\lib\thunderbird-7.0.1	D634CD51DE3...	0F97A7204903F...	C9A67E961338...	All
termlist.DB	Ubuntu-0:\var\cache\apt-xapian-inde...	CFB639CA74D8...	710155223320F...	764ED9194794...	All
libxul.so	Ubuntu-0:\usr\lib\firefox-7.0.1	BA0081458265...	5C470E75FB22...	423F4828618B...	All

The list of matching files can be exported to a text file by selecting 'Export list to text...' in the right-click menu.

4.16.4 Installing Hash Sets

To install the hash sets from external sources, you must move them into the OSForensics program data folder.

On Vista, Windows 7 (aka Win7), and Server 2008, this would typically be the following folder (you may need to enable viewing of hidden directories to see it or enter it directly into the Explorer address bar):
C:\ProgramData\PassMark\OSForensics\hashSets

On XP and Server 2000/2003, it is typically something like this:
C:\Documents and Settings\All Users\Application Data\PassMark\OSForensics\hashSets

For a USB install
%OSF_Usb_Directory"%\AppData\hashSets
Note that while most files are automatically copied when installing to USB, hash sets are not as they can often be quite large.

You will then need to restart OSForensics if you have it currently open. When you next start OSForensics, you should now find additional sets listed in the tree view under the "Hash Sets" panel.

Some additional hash sets you can install can be found on the OSForensics download page http://www.osforensics.com/download.html

4.16.5 NSRL Import

The National Software Reference Library data set can be obtained from this site http://www.nsrl.nist.gov/. To import the data set into OSForensics you will need to follow these steps.

1. Download the dataset from http://www.nsrl.nist.gov/. Currently the dataset is distributed as a set of four .iso files. To access the contents of these files you will either need to burn them to DVD or mount them using a virtual disk manager such as OSFMount.
2. On each of the disks is a zip file, each of these zip files must be unzipped into a sperate folder in the same location. For example, you create a folder named "NSRLData" and then under that folder you create folders named "Disk1", "Disk2" etc. in which you extract the zip files from each disk.
3. Create a new empty database in OSForensics, you may import to a non empty database but this is not recommended.
4. Make the new database active.
5. Select the "NSRL Import.." button on the hash management window and then select the root folder for all the unzipped sub folders. (the "NSRLData" folder in the example from step 2).

Note this process can take a very long time to complete, up to several days on some systems. One way to make the process more manageable is to only import a disk at a time. This would mean in step 2 above you would only extract one of the zips, then remove it and extract the next and repeat the process importing into the same database. This is one scenario where importing to a non-empty database is recommended. This will actually take more time total but breaks the task up into shorter steps. You can also back-up the database in between each import in case an error occurs this way.

Another way to speed up the process is to make sure the database is on a solid state hard drive of a RAM drive. Import time is highly dependant on the random seek read/write performance of the drive. On an average system with a normal hard drive the process takes about 50 hours. On a RAM drive the process has been seen to take as little as 10-15. A solid state drive will likely have a import time somewhere between these two figures.

4.16.6 Hash DB Import/Export Format

The import / export format for the hash database is a flat CSV file with the following fields.

Origin	The origin of the file hash
Product	The product the hashed file belongs to.
Product Type	A description of the what type of product the product is.
Hash Set Name	The name of the hash set the file hash belongs to.
Hash Set ID	A Unique ID for this hash set.
Version	The version of the product.
Manufacturer	The manufacturer of the product.
Language	The language of the product.
Type	What type of hash set this is (known good files, known bad files, etc)
OS	What operating system this hash set is associated with.
Filename	The name of the file this hash was taken from.
MD5	The MD5 hash for this file.
SHA1	The SHA1 hash for this file.
SHA256	The SHA256 hash for this file.
LastUpdate	When this hash was last updated

Size   The size of the file that was hashed.

Example output:

```
Origin,Product Type,Hash Set Name,Hash Set ID,Version,Manufacturer,Language,Type,OS,Filename,MD5,SHA1,S
NSRL,Web Browser,Mozilla Firefox 2,5,2,Mozilla Foundation,English,Good,Linux,about.xul,73148BD6D79786C4
NSRL,Web Browser,Mozilla Firefox 2,5,2,Mozilla Foundation,English,Good,Linux,actionbuttons.png,8A6116D8
NSRL,Web Browser,Mozilla Firefox 2,5,2,Mozilla Foundation,English,Good,Linux,all.js,5FDD321D9A4C2329250
```

4.17 Signatures

Signatures allow users to identify changes in a directory structure between two points in time. Generating a signature creates a snapshot of the directory structure, which includes information about the contained files' path, size and attributes. Changes to a directory structure such as files that were created, modified and deleted can be identified by comparing two signatures. These differences can quickly identify potential files of interest on a suspected machine, such as newly installed software or deleted evidence files. Signatures differ from Hash Sets in the following ways:

1. The signature is not required to contain any file hashes
2. The file path, size and attributes of the files on the hard drive are included in the signature.

OSForensics provides the following File Signature Analysis functionality:

Create Signature

Module that handles all aspects of generating a signature.

Compare Signature

Module that allows the user to compare previously generated signatures. A summary of any changes between the signatures are displayed to the user.

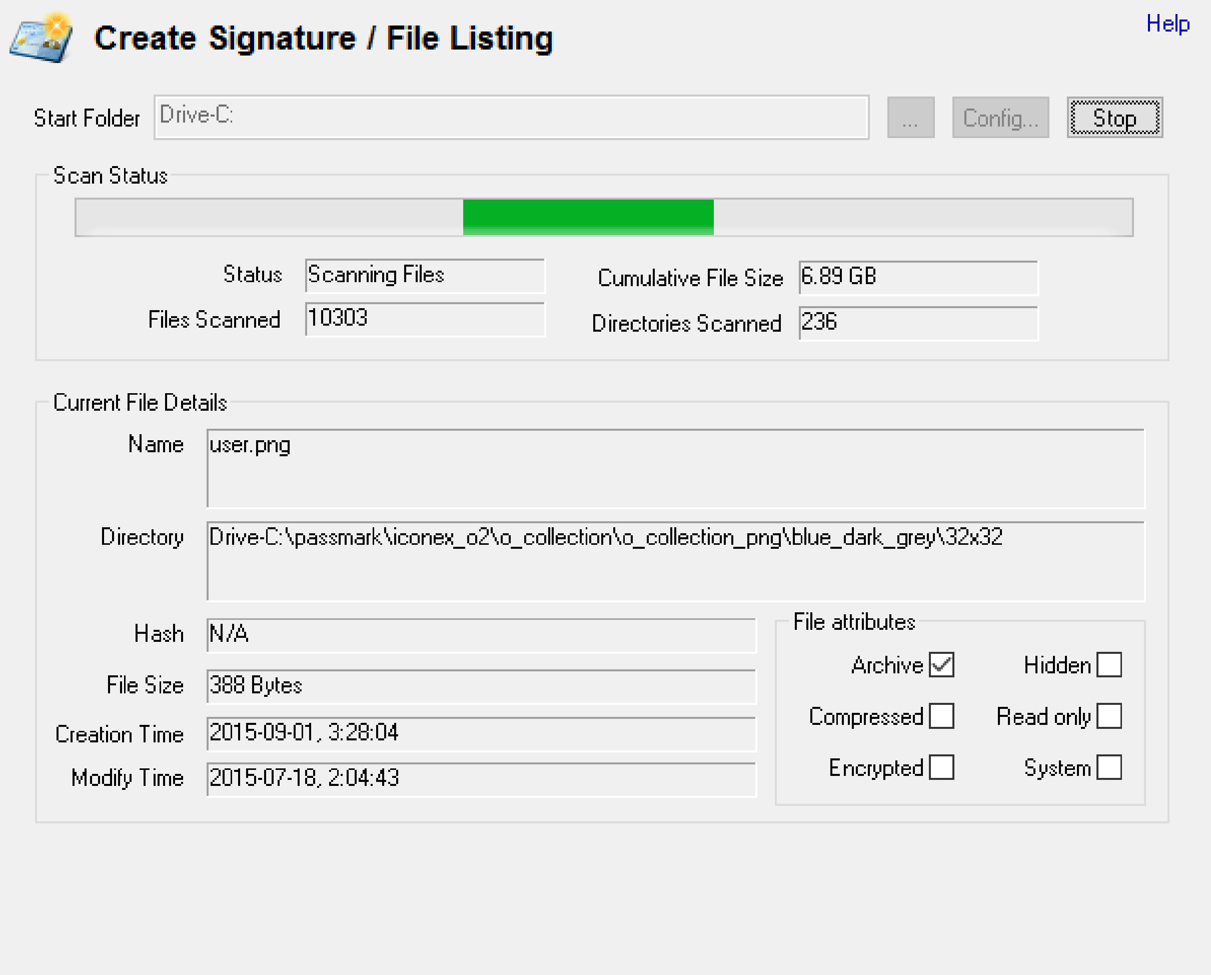
Other Uses

In addition to finding any suspicious changes to a system, signatures can be used for the following

- Finding the details of intentional changes, and creating a hash set based off a signature comparison.
  - For instance it can find all the files the an application's installer package makes to a system, including the total file size of those changes. Once these changes are found they can then be turned into a hash set that defines all the files related to that application.
- Determining whether two machines have any documents / photos / videos in common. (eg. due to the sharing of files)
- Making a list of all files on a drive.

4.17.1 Create Signature

The Create Signature module is used for creating a signature file. This is used for creating a snapshot of a system's directory structure at a particular point in time.



Create Signature / File Listing

Start Folder: Drive-C:

Scan Status

Status: Scanning Files
Cumulative File Size: 6.89 GB
Files Scanned: 10303
Directories Scanned: 236

Current File Details

Name: user.png
Directory: Drive-C:\passmark\iconex_o2\o_collection\o_collection_png\blue_dark_grey\32x32
Hash: N/A
File Size: 388 Bytes
Creation Time: 2015-09-01, 3:28:04
Modify Time: 2015-07-18, 2:04:43

File attributes

Archive ☑ Hidden □
Compressed □ Read only □
Encrypted □ System □

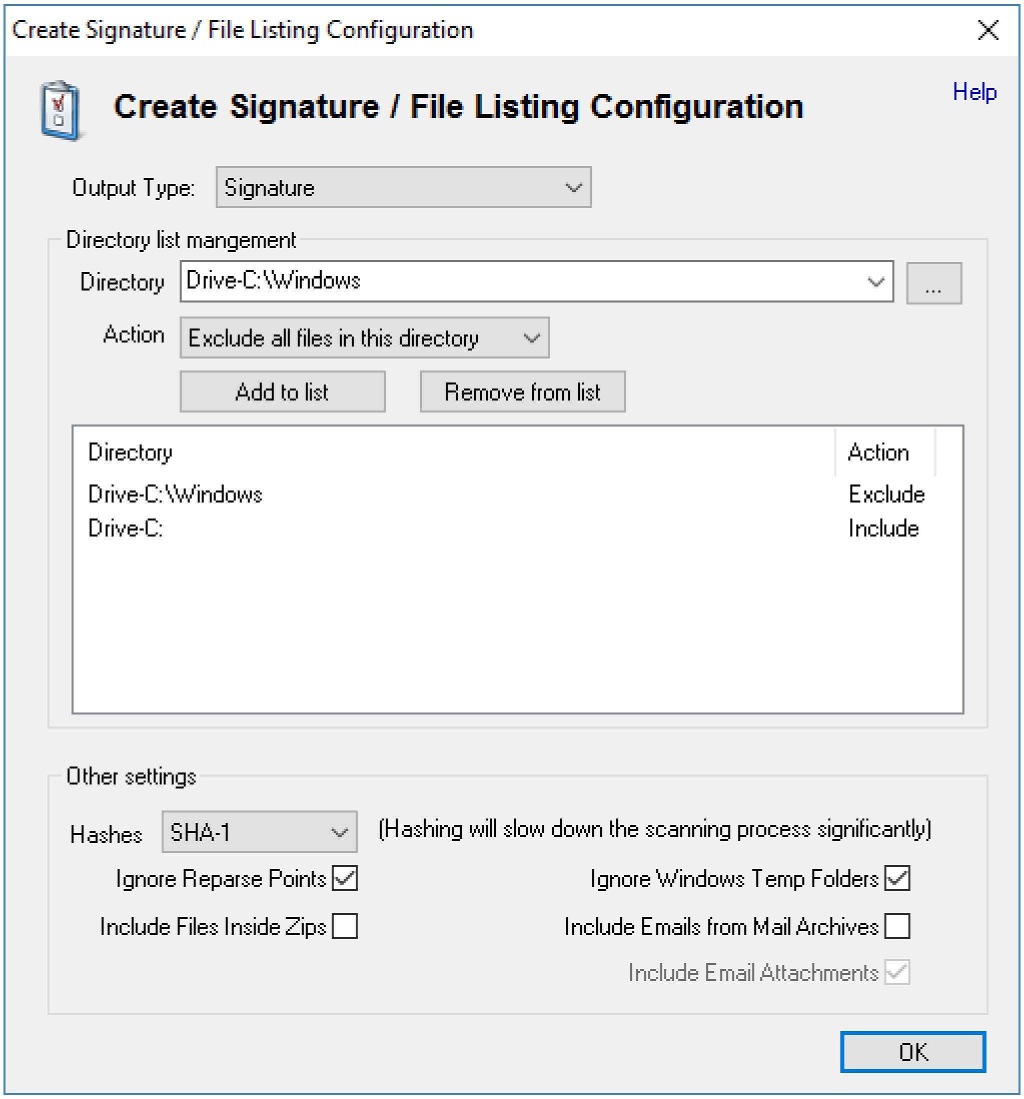
A signature can be created using the default options by simply specifying a starting directory and clicking the "Start" button. Advanced options for signature generation can be found by clicking the "Config..." button to open the Create Signature Configuration Window.

After the signature has been created, the user will be prompted to save the file signature. Saving should only take a couple of seconds, even for very large signatures.

The signature creation process can be canceled at any time by clicking the Stop button.

4.17.1.1 Create Signature Configuration

The Signature File Creation Configuration windows allows for more advanced configuration of the signature creation process. This window can be accessed by clicking on the "Config..." button in the main Create Signature window.



Create Signature / File Listing Configuration

Create Signature / File Listing Configuration

Output Type: Signature

Directory list mangement

Directory Drive-C:\Windows

Action Exclude all files in this directory

Directory	Action
Drive-C:\Windows	Exclude
Drive-C:	Include

Other settings

Hashes SHA-1 (Hashing will slow down the scanning process significantly)

Ignore Reparse Points ☑ Ignore Windows Temp Folders ☑

Include Files Inside Zips □ Include Emails from Mail Archives □

Include Email Attachments ☑

Directory List

Directories to be included/excluded from the signature can be configured here. When a signature is being created, each include directory shall be recursively scanned and included in the signature file. Excluded directories will be skipped during the recursion. Note that if an include directory in the list contains another include directory in the list, the common files will be included twice in the signature file.

You can include paths from the registry, the directory selection drop list has the registry root keys that can be added. Registry sub paths can be included/excluded the same as file system paths.

Other Settings

Calculate SHA1 Hashes

Check this box to calculate an SHA1 hash for every file in the signature. This will add a second step to the signature creation process that takes a significantly larger amount of time than a simple scan as every file in the signature needs to be read in its entirety off the hard drive. This option is disabled by default.

When creating a signature of registry paths this will hash the data stored in the registry values. Hashing of the registry has a far smaller performance penalty than the file system as there is a lot less data.

Ignore Reparse Points
Check this box to ignore reparse points. Reparse points exist on NTFS drives and appear as normal folders. However, they act as links between different parts of the file system. Windows creates a number of these reparse points in its initial install. This option is enabled by default. It is recommended that this option is checked. Otherwise the scan process may end up including the same file multiple times.

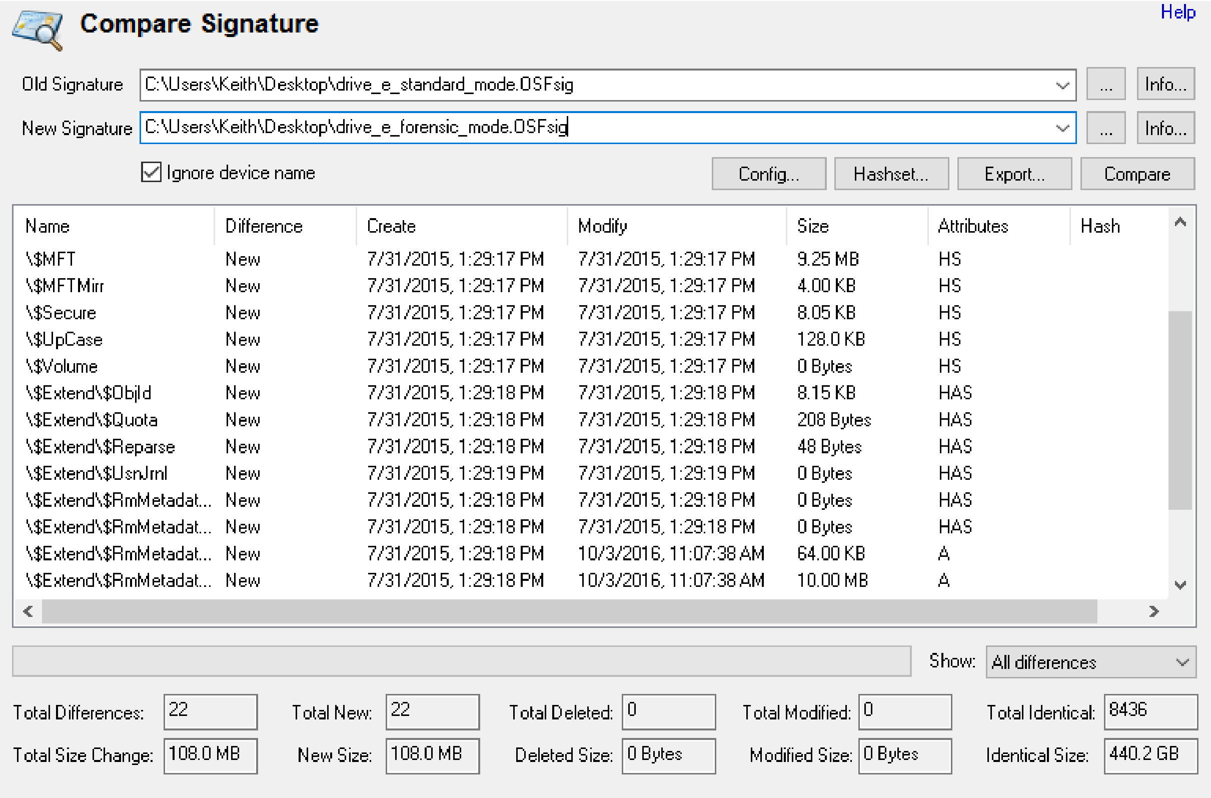
Ignore Windows Temp Folders
Ignores a hard coded list of the following known Windows temporary folders. This option is enabled by default.

```
"\AppData\Local\Microsoft\Windows\Temporary Internet Files"
"\AppData\Local\Temp"
"\AppData\Roaming\Microsoft\Windows\Cookies"
"\Users\All Users\Microsoft\Search\Data\Temp"
"\Users\All Users\Microsoft\Search\Data\Applications\Windows\Projects
\SystemIndex\Indexer"
"\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects
\SystemIndex\Indexer"
"\ProgramData\Microsoft\Search\Data\Temp"
"\Windows\Temp"
"\Windows\Prefetch"
"\Windows\System32\WDI"
"\Windows\System32\LogFiles"
"\Windows\System32\spool"
"\Windows\System32\config"
"\Windows\System32\winevt\Logs"
```

Include Files inside Zips / Include Emails from Mail Archives
Selecting these options will have the signature creation function examine the contents of zip files or email archives. In the case of emails extra meta data (ie. to and from addresses) will be stored. Attachments of emails will also be added as separate entries Note that these options are recursive, if there is a zip file inside a zip file or an email archive within an email they will also be examined. If both options are selecting zips attached to emails will be examined as well as email archives inside zips. There is no fixed limit as to how deep the recursion will go.

4.17.2 Compare Signature

The Compare Signature module is used for comparing two previously created signatures, in order to identify differences in the directory structure between two points in time. Differences include new files, modified files and deleted files.



Old Signature: C:\Users\Keith\Desktop\drive_e_standard_mode.OSFsig

New Signature: C:\Users\Keith\Desktop\drive_e_forensic_mode.OSFsig

☑ Ignore device name

Name	Difference	Create	Modify	Size	Attributes	Hash
\$MFT	New	7/31/2015, 1:29:17 PM	7/31/2015, 1:29:17 PM	9.25 MB	HS	
\$MFTMirr	New	7/31/2015, 1:29:17 PM	7/31/2015, 1:29:17 PM	4.00 KB	HS	
\$Secure	New	7/31/2015, 1:29:17 PM	7/31/2015, 1:29:17 PM	8.05 KB	HS	
\$UpCase	New	7/31/2015, 1:29:17 PM	7/31/2015, 1:29:17 PM	128.0 KB	HS	
\$Volume	New	7/31/2015, 1:29:17 PM	7/31/2015, 1:29:17 PM	0 Bytes	HS	
\$Extend\$ObjId	New	7/31/2015, 1:29:18 PM	7/31/2015, 1:29:18 PM	8.15 KB	HAS	
\$Extend\$Quota	New	7/31/2015, 1:29:18 PM	7/31/2015, 1:29:18 PM	208 Bytes	HAS	
\$Extend\$Reparse	New	7/31/2015, 1:29:18 PM	7/31/2015, 1:29:18 PM	48 Bytes	HAS	
\$Extend\$UsnJrnl	New	7/31/2015, 1:29:19 PM	7/31/2015, 1:29:19 PM	0 Bytes	HAS	
\$Extend\$RmMetadat...	New	7/31/2015, 1:29:18 PM	7/31/2015, 1:29:18 PM	0 Bytes	HAS	
\$Extend\$RmMetadat...	New	7/31/2015, 1:29:18 PM	7/31/2015, 1:29:18 PM	0 Bytes	HAS	
\$Extend\$RmMetadat...	New	7/31/2015, 1:29:18 PM	10/3/2016, 11:07:38 AM	64.00 KB	A	
\$Extend\$RmMetadat...	New	7/31/2015, 1:29:18 PM	10/3/2016, 11:07:38 AM	10.00 MB	A	

Show: All differences

Total Differences:	22	Total New:	22	Total Deleted:	0	Total Modified:	0	Total Identical:	8436
Total Size Change:	108.0 MB	New Size:	108.0 MB	Deleted Size:	0 Bytes	Modified Size:	0 Bytes	Identical Size:	440.2 GB

Old / New Signature
The file path of the signature files to compare. The chronologically older of the two signatures should be the "Old Signature" so that the terminology of the differences are correct.

Info
Open the Signature Info window which displays the details of the corresponding signature file.

Ignore device name
Check this option to compare the signature files without considering the differences in device name (eg. 'C:' 'D:' 'winxp:') in the file paths.

Config...
Open a configuration dialog which allows the user to adjust the signature comparison settings.

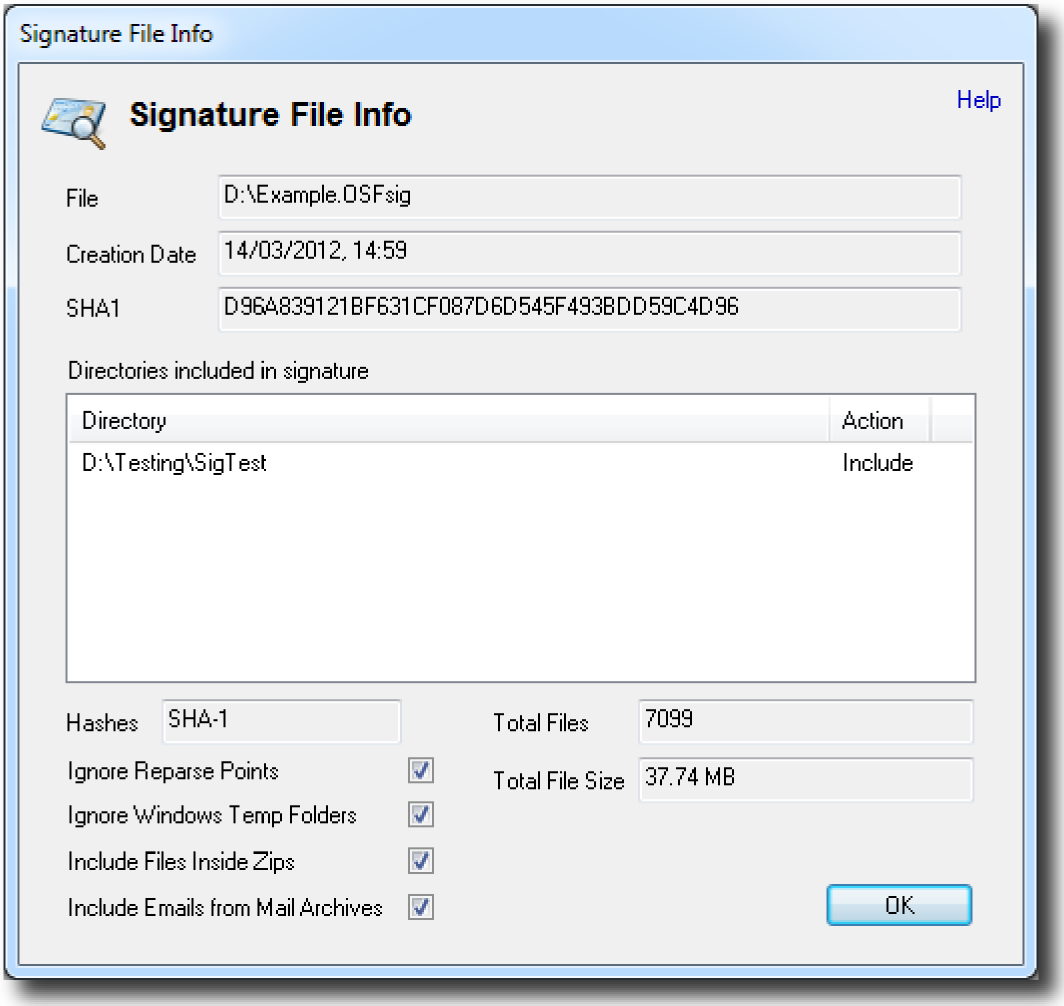
Hashset
Click this button to create a Hash Set using the list of differences from the comparison.

Export
Click this button to save the results of the signature comparison to a CSV file.

Compare
Click this button to perform the comparison between the signature files.

4.17.2.1 Signature Info

The Signature Info Window shows the details about the signature file. This window can be accessed by clicking on the "Info" button on a signature file in the main Compare Signature window.



Signature File Info

Signature File Info

File: D:\Example.OSFsig

Creation Date: 14/03/2012, 14:59

SHA1: D96A839121BF631CF087D6D545F493BDD59C4D96

Directories included in signature

Directory	Action
D:\Testing\SigTest	Include

Hashes: SHA-1

Total Files: 7099

Total File Size: 37.74 MB

Ignore Reparse Points ☑

Ignore Windows Temp Folders ☑

Include Files Inside Zips ☑

Include Emails from Mail Archives ☑

File
The file path of the signature file.

Creation Date
The date and time of when the signature file was created.

SHA1
The internal SHA1 hash of the signature. Note that due to the fact that the SHA1 hash is stored within the signature itself, running the hash function over the signature file will not generate the same hash. The hash is however recalculated and checked upon loading the signature and an error will appear if the signature has been modified.

Directories included in signature
The list of directories included/excluded in the creation of the signature file.

Hashes

This field will specify what type, if any, hashes were calculated for the entries in this signature.

Total Files
Total number of entries in this signature.

Total File Size
Cumulative size of all entries in this signature.

Ignore Reparse Points
If checked, reparse points were ignored in the creation of the signature file.

Ignore Windows Temp Folders
If checked, known Windows temporary folders were ignored in the creation of the signature file.

Include Files Inside Zips
Whether or not the signature creation process included files inside zip files.

Total Emails from Mail Archives
Whether or not the signature creation process included emails and attachments from inside mail archives.

4.17.3 Signature Technical Details

The following is a list of notes about how signatures and file listings handle certain special cases.

Email Date/Times

In the case of emails the Create Date is the Sent Date and the Modify Date is the Receive Date.

Single Email Containers

Files that only contain a single email (ie. eml, msg) still get two entries in the signature. One for the file itself, and one for the email. This is due to the fact that some shared data can be different. There is date/times for both the file itself and when the message was sent and received. Also the file size and hash will differ, see below.

File Sizes of Emails

The email file size is calculated as;

Message header + Message HTML content + Message plain text content + message RTF content + size of any attachments (where supported).

All fields except RTF are treated as double byte unicode for size purposes. RTF is left in its original single byte formatting.

The total size of all emails in a container will differ from the size of the file, in some cases total will be bigger. This is an artifact of the message HTML and plain text content always being treated as double byte, whereas internally it may have been stored as UTF-8 or some other compressed format.

Email Attachment Limitations

MBOX Attachments are limited to 50MB. If an attachment is large than this it is not included in the signature/file listing nor counted as part of the message hash / file size.
DBX attachments are not supported in any way.

Email Hashes

When generating hashes there are two separate hashes generated for emails. The first, which exists in the same field as normal hashes, is a hash of the content that makes up the message file size as described above in the email file size above.

The second hash is a hash of just the message content. The has is calculated on one of the three possible content fields. If more than one content type exists they are chosen in the following order of priority.

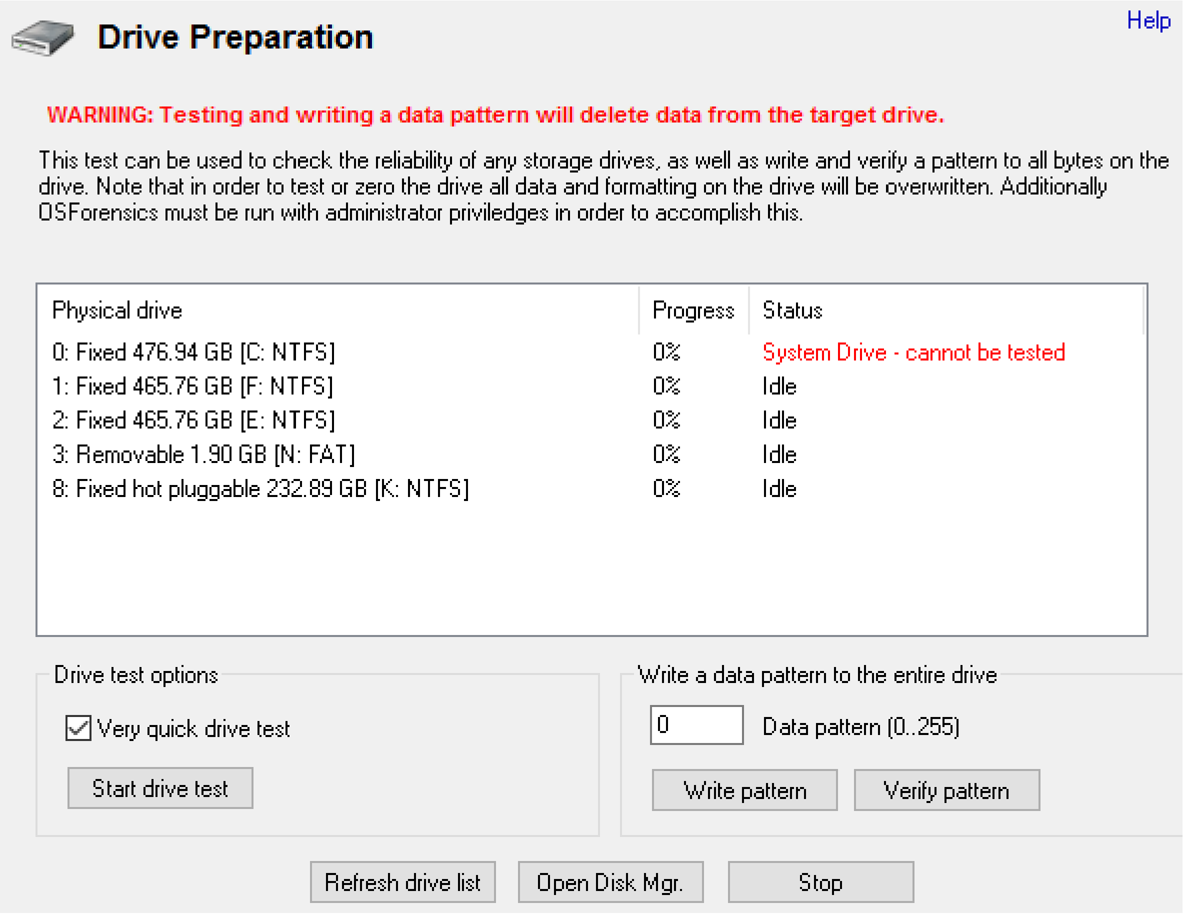
Plain text has the highest priority, it is treated as double byte unicode and all spaces, newlines, tabs and carriage returns are removed before hashing.
HTML has the second highest priority, it is treated as double byte hashed without modification.
RTF is the lowest priority, it is hashed as a single byte character string.

Large Zip Files

Zip archives greater than 4GB are not supported. Only the top level zip will be added to the signature, not any of the files within the zip.

4.18 Drive Preparation

This module provides two different features. Firstly it can test a drive for reliability, potentially identifying any faulty drives before they are put into active use in an investigation. Secondly it can set all bytes of a drive to a specified byte pattern (and verify the byte pattern has been written to the entire drive), making sure there is no chance of data contamination between investigations.



Drive Preparation

WARNING: Testing and writing a data pattern will delete data from the target drive.

This test can be used to check the reliability of any storage drives, as well as write and verify a pattern to all bytes on the drive. Note that in order to test or zero the drive all data and formatting on the drive will be overwritten. Additionally OSForensics must be run with administrator priviledges in order to accomplish this.

Physical drive	Progress	Status
0: Fixed 476.94 GB [C: NTFS]	0%	System Drive - cannot be tested
1: Fixed 465.76 GB [F: NTFS]	0%	Idle
2: Fixed 465.76 GB [E: NTFS]	0%	Idle
3: Removable 1.90 GB [N: FAT]	0%	Idle
8: Fixed hot pluggable 232.89 GB [K: NTFS]	0%	Idle

Drive test options

☑ Very quick drive test

Write a data pattern to the entire drive

Data pattern (0..255): 0

Drive List

The Drive list shows 3 columns:

- Drive: Shows the disk volume and/or physical drive number. May also show the volume name, type of disk, size and file system type.
- Progress: Progress of the test, zeroing or verification as a percentage.
- Status: A brief summary of the current activity or the result.

Multiple disks (up to 100 disks) can be acted on at once by selecting the multiple rows in the drive list. An action may be stopped at any time with the “Stop” button.

If additional drives have been added to the system since OSForensics has been started, you can refresh the list of drives that can be tested with the “Refresh drive list” button.

Drive test options

Very quick drive test: When selected, the testing is kept to about 3 minutes. Otherwise , the random samples stage of the test will continue until about 10% of the disk is tested.

The "Start drive test " button starts the drive testing. This test does not test the entire drive, as in most cases this would take very many hours. Rather, to provide the fastest possible test, while providing the greatest test coverage of the drive, the test writes and reads test data to the drive directly and not via the File System e.g. NTFS. The test will test the start of the drive, the end of the drive and random samples in between. As such, the drive test WILL DELETE the file system information (e.g. NTFS) and data on the drive. Administrator privileges are required for this test.

The drives that can be tested are shown in the physical drive list. The only drives allowed to be tested are fixed and removable drives. The system drive (ie. "C:") cannot be tested.

Write a data pattern to the entire drive

This action makes sets every byte on the hard drive to the specified value (default zero). Effectively blanking out a disk and removing any possibility of data cross-contamination when using the drive in a new investigation. After the write pattern process is complete the "Verify pattern" action can ensure the process was successful by reading back all data from the disk and checking each byte value is the specified byte value,

As this function acts on the entirety of a drive it may take some time, depending on the size of the drive.

Open Disk Manager

After the drive is tested or a data pattern written and verified, the drive will need to be formatted. The Open disk manager option opens Windows disk manager to allow the drive(s) to be partitioned and formatted as required.

Stop

Stops a drive test, writing a data pattern or verifying a data pattern.

4.19 Forensic Imaging

The disk imaging functionality allows the investigator to create and restore disk image files, which are bit-by-bit copies of a partition, physical disk or volume. Disk imaging is essential in securing an exact copy of a storage device, so it can be used for forensics analysis without risking the integrity of the original data. Conversely, an image file can be restored back to a disk on the system.

A forensics investigator may need to deal with physical disks that are part of a RAID configuration. Without having access to the RAID controller needed to recreate the RAID array, it may be difficult to reconstruct the logical disk for forensics analysis. Given a set of disk images, OSForensics can rebuild the logical image based on the specified RAID parameters. RAID parameters from software RAID created under Linux and Windows can be automatically detected.

A hard disk may also contain hidden areas that are normally inaccessible to users, namely Host Protected Area (HPA) and Device Configuration Overlay (DCO). The disk imaging module can detect for the presence of an HPA and/or DCO, and optionally create images of these hidden areas.

Create Image
Module that performs imaging on any disk attached to the system

Restore Image
Module that restores images to any disk attached to the system

Hidden Areas - HPA/DCO
Module that detects for the presence of HPA and DCO hidden areas on a disk. If present, these areas can be imaged or removed.

RAID Rebuild
Module that can rebuild a RAID array from a set of disk images and specified RAID parameters.

Create Logical Image
Module that creates a logical image that includes only the files/directories specified by the user.

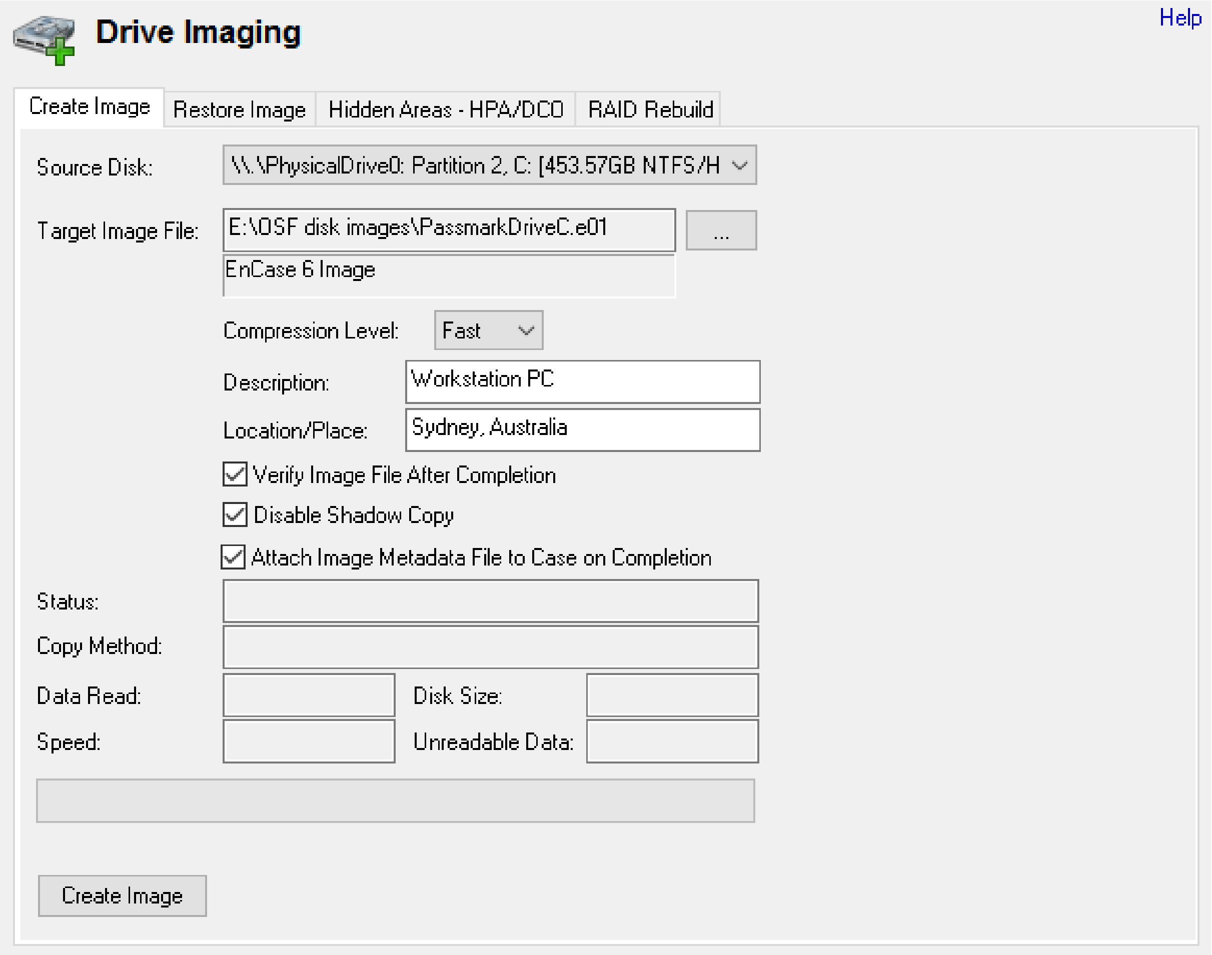
4.19.1 Create Image

OSForensics allows the user to take exact copies of partitions, disks and volumes of an active system, or any device added to the case. This is particularly useful for live acquisitions while running OSForensics from USB. However, if you want to make a copy of a drive from a non live system, see OSFClone.

Creating a disk image makes use of the Volume Shadow Copy service built in to Windows. This allows OSForensics to make copies of drives that are in use without resulting in data corruption from reading files that are currently being written to. This is especially important for imaging system drives which Windows is constantly modifying. Once a shadow copy has started, a snapshot state of the drive is frozen at that point in time, so even if important evidence is being removed by another process in the background it will still appear in the resulting image file.

If the shadow copy service is not available, OSForensics tries to lock the drive to prevent any other programs from writing to it. If this is not possible, a warning will appear. Drives copied without a shadow volume or a lock are prone to creating corrupt images on completion.

Once the drive image has been created it can later be analyzed by adding it to the case or mounting it with OSFMount.



Source Disk: \\.\PhysicalDrive0: Partition 2, C: [453.57GB NTFS/H

Target Image File: E:\OSF disk images\PassmarkDriveC.e01

EnCase 6 Image

Compression Level: Fast

Description: Workstation PC

Location/Place: Sydney, Australia

☑ Verify Image File After Completion

☑ Disable Shadow Copy

☑ Attach Image Metadata File to Case on Completion

Status:

Copy Method:

Data Read: Disk Size:

Speed: Unreadable Data:

Source Disk
The partition, disk, volume or device to create an image of. Note that only partitions with drive letters can be shadow copied.

Image File
The location to save the image file to. An .info file with the same name will also be created at this location. After specifying the image file path to save to, the image file format shall be displayed below depending on the file extension used.

Compression Level
If the image file format supports compression, one of the following level of compression of the image file can be specified: None, Fast, or Best.

Description
A simple description of the image that will be stored in the accompanying .info file.

Location / Place
A description of where the disk was obtained. This will be stored in the info file.

Verify Image File After Completion
Check this to verify the image file hash against the source disk hash. This can take as long as the initial imaging, thereby doubling the time for the entire process.

Disable Shadow Copy
The imaging process will not attempt to use the windows Volume Shadow Service to perform the copy.

Attach Image Metadata File to Case on Completion
Upon imaging process completion, prompt the user to attach the image validation file (.info.txt) to case.

Status
The current status of the imaging process. Also shows a duration where available. Note that the duration is only for that particular step or the process.

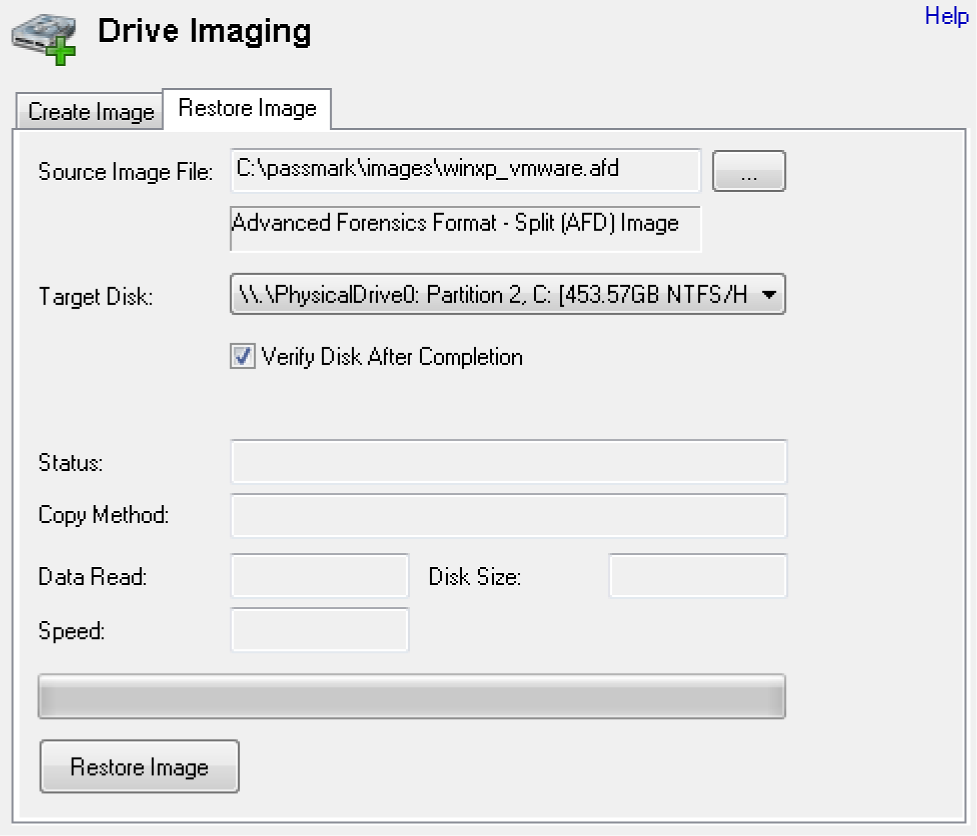
Copy Method
The method being used to create the disk image (either a shadow copy or a direct sector copy). Also whether OSF managed to lock the volume or not.

Unreadable Data
If a sector was unreadable, it will fill that sector with 0's and continue on. This field lets you know how much data was unreadable, due to restricted access or a damaged disk.

4.19.2 Restore Image

Restoring an image to a disk returns the disk contents back to a previous state, allowing an investigator to observe the changes that occur on the disk while being attached to the live system. This may be useful if an investigator wishes to boot an image of a system disk on a live machine in order view the state of system from the user's perspective.

OSForensics can only restore an image file if a lock to the disk is obtained. This is to prevent any other programs from writing to the disk while the restoration is in progress. For OSForensics to successfully obtain a lock, no programs can be accessing the disk at the time (eg. files on the disk being opened).



Source Image File: C:\passmark\images\winxp_vmware.afd
Advanced Forensics Format - Split (AFD) Image
Target Disk: \\.\PhysicalDrive0: Partition 2, C: [453.57GB NTFS/H
☑ Verify Disk After Completion
Status:
Copy Method:
Data Read:
Disk Size:
Speed:

Source Image File
The image file containing the disk contents to restore the disk to.

Target Disk
The disk to write the contents of the image file to.

Verify Disk After Completion
Check this to verify the target disk hash with the source image file hash. This can take as long as the restoring process, thereby doubling the time for the entire process.

Status
The current status of the restoring process. Also shows a duration where available. Note that the duration is only for that particular step or the process.

Copy Method
The method being used to restore the disk image. This will always be 'Direct Sector Copy'.

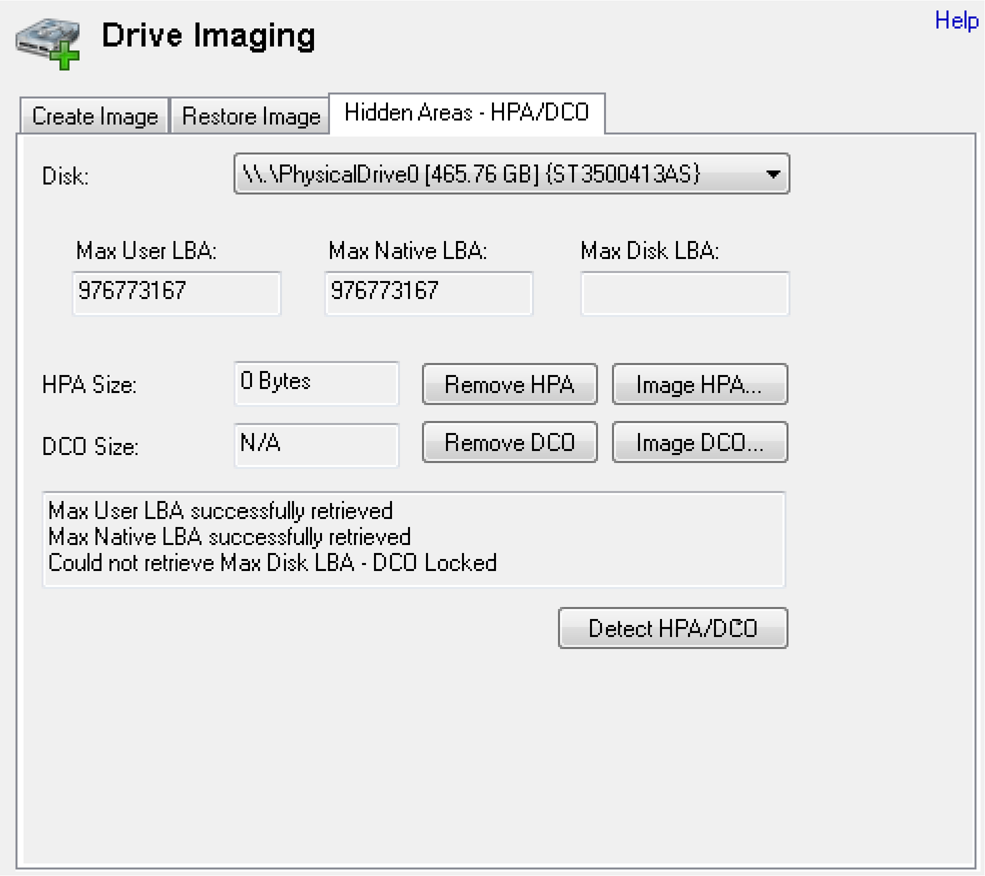
4.19.3 Hidden Areas - HPA/DCO

The Host Protected Area (HPA) and Device Configuration Overlay (DCO) are features for hiding sectors of a hard disk from being accessible to the end user.

A typical usage for an HPA is to store boot sector code or diagnostic utilities of the manufacturer. However, the HPA can also be used for malicious intent including hiding illegal data, which may be of interest to forensics investigators.

The DCO feature was proposed to allow system vendors to purchase hard disks of different sizes, but setting the hard disk capacity of each disk to the same size. Again, the hidden sectors can be used for hiding data of forensic interest.

***Note**: If the HPA and/or DCO is removed, you will need to detach/re-attach the hard disk before the system is able to access the previously hidden sectors. Ie. You will be unable to view the previously hidden sectors in the Raw Disk Viewer until you detach/re-attach the hard disk. However, you can still view the contents of the hidden areas without detaching your hard disk by imaging the HPA and/or DCO to a file, and opening the image file in the internal viewer.*



Disk: \\.\PhysicalDrive0 [465.76 GB] (ST3500413AS)

Max User LBA: 976773167

Max Native LBA: 976773167

Max Disk LBA:

HPA Size: 0 Bytes

DCO Size: N/A

```
Max User LBA successfully retrieved
Max Native LBA successfully retrieved
Could not retrieve Max Disk LBA - DCO Locked
```

Max User LBA
The maximum addressable sector by the user. This determines the capacity reported by the disk to the system.

Max Native LBA
The maximum addressable sector allowed by the disk.

Max Disk LBA
The maximum addressable sector of the physical disk.

HPA Size
The size of the area between the Max User LBA and Max Native LBA

Remove HPA
If present, the HPA on the specified disk is removed. The sectors that were previously hidden in the HPA are now accessible.

Image HPA
If present, an image of the HPA is created and saved to disk. The HPA is restored back to its original state after imaging.

DCO Size
The size of the area between the Max Native LBA and Max Disk LBA

Remove DCO
If present, the DCO on the specified disk is removed. The sectors that were previously hidden in the DCO are now accessible.

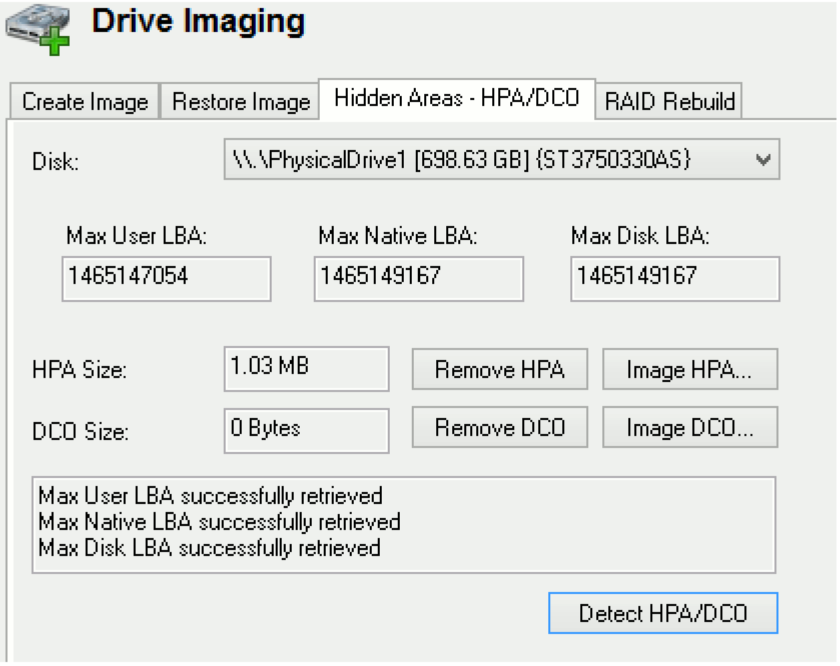
Image DCO
If present, an image of the DCO is created and saved to disk. The DCO is restored back to its original state after imaging.

Note: DCO can only be removed if no HPA exists on the disk. Ie. The HPA needs to be removed first before the DCO can be removed and/or imaged.

Depending on the hard disk, the HPA/DCO areas may be locked and therefore cannot be removed or imaged. This is indicated by "N/A" for the size of the area.

Accessing the HPA/DCO

Once a hidden area has been detected use the "Image" button that corresponds to the particular hidden area, this will allow you the save the contents of the area as an image file, in the example shown below clicking the "Image HPA..." button will allows us to save the contents of the detected HPA.



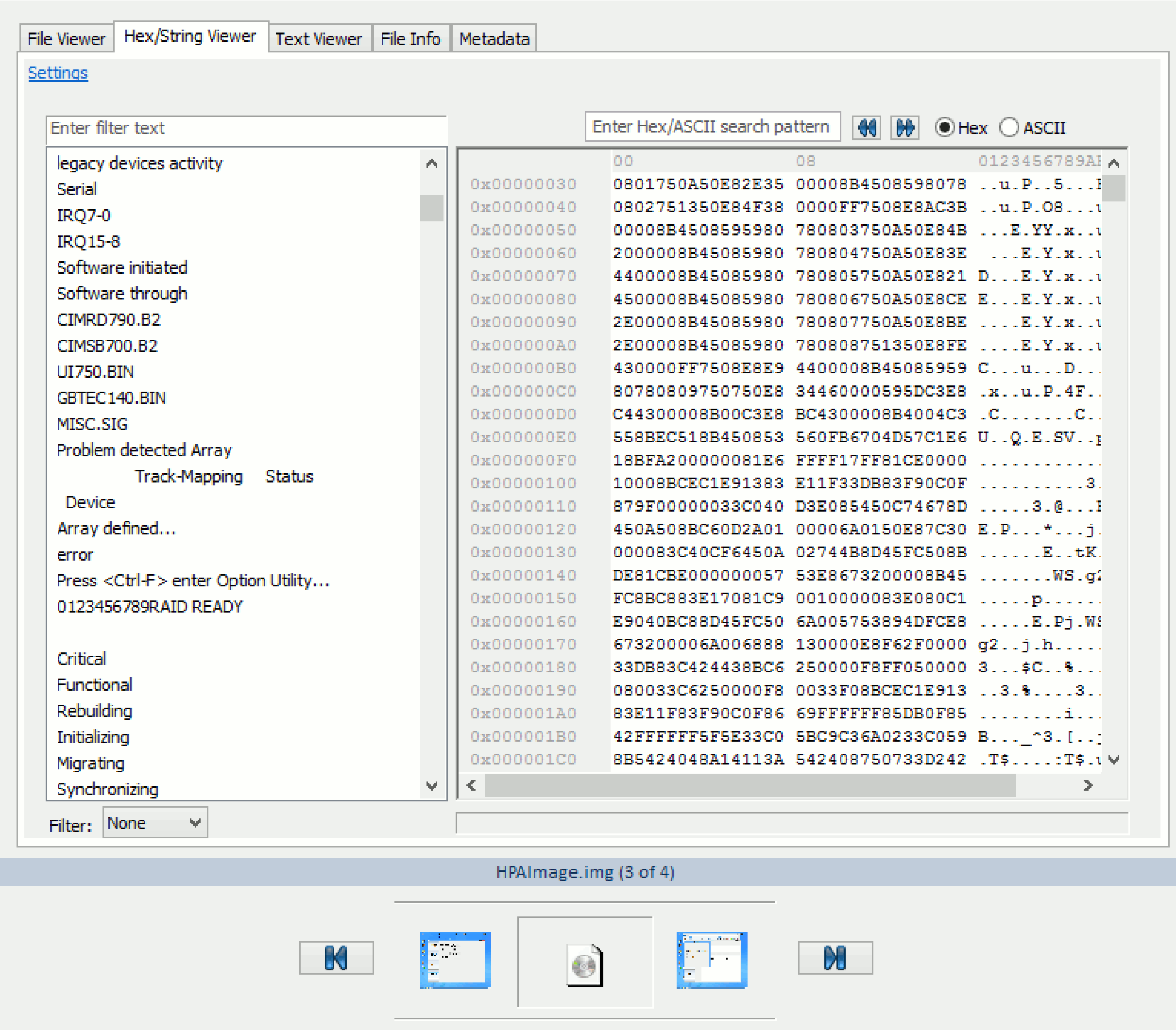
Disk: \\.\PhysicalDrive1 [698.63 GB] {ST3750330AS}

Max User LBA: 1465147054
Max Native LBA: 1465149167
Max Disk LBA: 1465149167

HPA Size: 1.03 MB
DCO Size: 0 Bytes

Max User LBA successfully retrieved
Max Native LBA successfully retrieved
Max Disk LBA successfully retrieved

Now that an image of the HPA has been created you can view it using the File System Browser and Internal Viewer. Navigate to the location where the HP image was saved, right click on the image file and choose the "View with Internal Viewer" options. Now you will able to see the HEX contents of the area and use the other internal viewer functions like "Extract Strings" as shown in the example below.



legacy devices activity
Serial
IRQ7-0
IRQ15-8
Software initiated
Software through
CIMRD790.B2
CIMSB700.B2
UI750.BIN
GBTEC140.BIN
MISC.SIG
Problem detected Array
Track-Mapping Status
Device
Array defined...
error
Press <Ctrl-F> enter Option Utility...
0123456789RAID READY

Critical
Functional
Rebuilding
Initializing
Migrating
Synchronizing

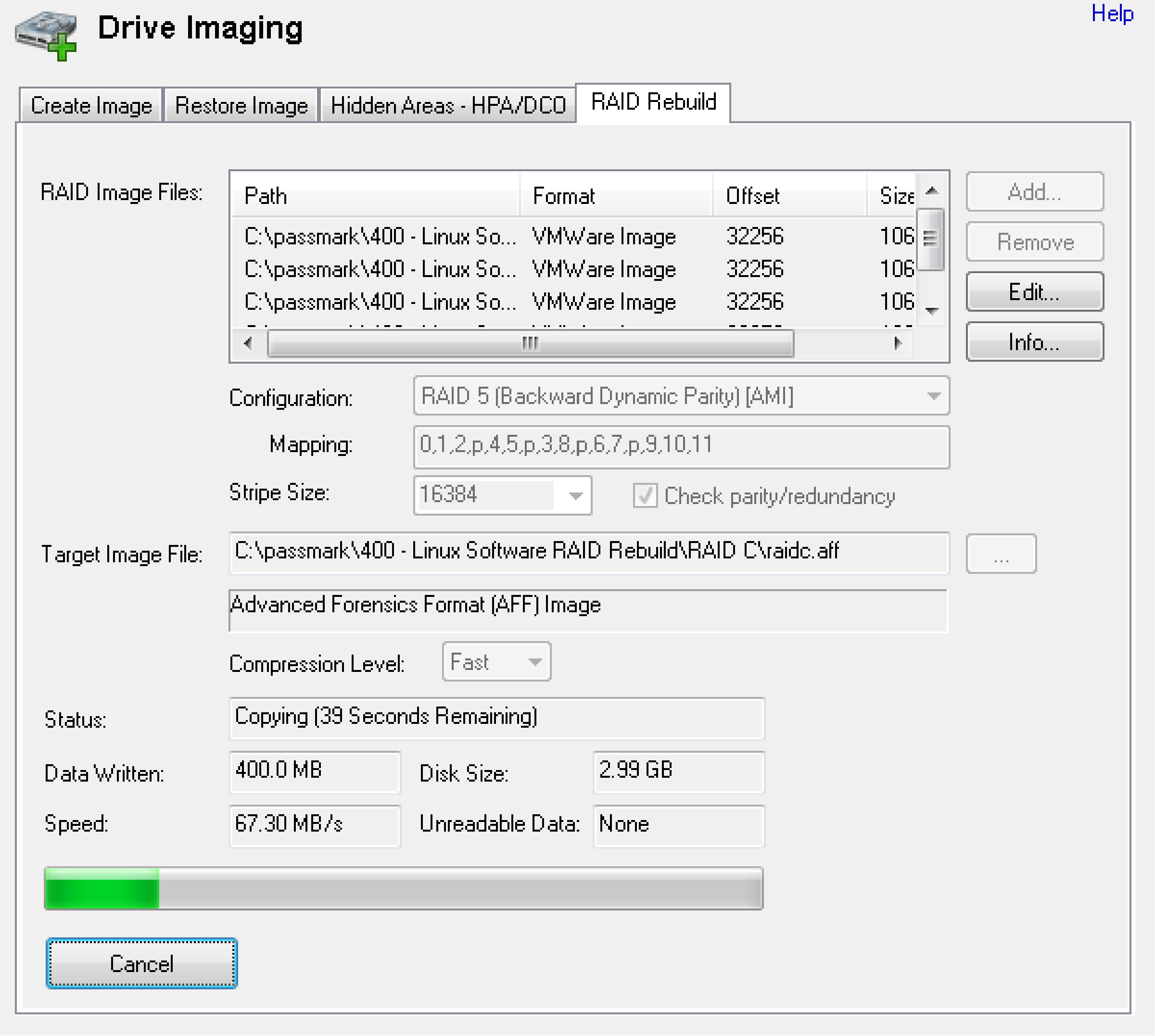
```
             00               08               0123456789A
0x00000030   0801750A50E82E35 00008B4508598078 ..u.P..5...
0x00000040   0802751350E84F38 0000FF7508E8AC3B ..u.P.O8...
0x00000050   00008B4508595980 780803750A50E84B ...E.YY.x..
0x00000060   2000008B45085980 780804750A50E83E  ...E.Y.x..
0x00000070   4400008B45085980 780805750A50E821 D...E.Y.x..
0x00000080   4500008B45085980 780806750A50E8CE E...E.Y.x..
0x00000090   2E00008B45085980 780807750A50E8BE ....E.Y.x..
0x000000A0   2E00008B45085980 780808751350E8FE ....E.Y.x..
0x000000B0   430000FF7508E8E9 4400008B45085959 C...u...D..
0x000000C0   80780809750750E8 34460000595DC3E8 .x..u.P.4F.
0x000000D0   C44300008B00C3E8 BC4300008B4004C3 .C.......C.
0x000000E0   558BEC518B450853 560FB6704D57C1E6 U..Q.E.SV..
0x000000F0   18BFA200000081E6 FFFF17FF81CE0000 ...........
0x00000100   10008BCEC1E91383 E11F33DB83F90C0F ..........3
0x00000110   879F00000033C040 D3E085450C74678D .....3.@...
0x00000120   450A508BC60D2A01 00006A0150E87C30 E.P...*...j
0x00000130   000083C40CF6450A 02744B8D45FC508B .......E..tK
0x00000140   DE81CBE000000057 53E8673200008B45 ........WS.g
0x00000150   FC8BC883E17081C9 0010000083E080C1 .....p.....
0x00000160   E9040BC88D45FC50 6A005753894DFCE8 ......E.Pj.W
0x00000170   673200006A006888 130000E8F62F0000 g2..j.h....
0x00000180   33DB83C424438BC6 250000F8FF050000 3...$C..%..
0x00000190   080033C6250000F8 0033F08BCEC1E913 ..3.%....3.
0x000001A0   83E11F83F90C0F86 69FFFFFF85DB0F85 .........i..
0x000001B0   42FFFFFF5F5E33C0 5BC9C36A0233C059 B..._^3.[..
0x000001C0   8B5424048A14113A 542408750733D242 .T$....:T$.
```

HPAImage.img (3 of 4)

4.19.4 RAID Rebuild

RAID configurations are becoming more commonly found in consumer machines, not just in server machines. As such, being able to properly image systems with RAID configurations for forensics analysis is critical and sometimes challenging. This is due to the fact that having access to the controllers that manages the RAID array may not be possible. The forensics investigator may only have access to a set of disk images without knowing which RAID controller was used, and the RAID parameters used in the configuration.

OSForensics can rebuild a logical disk image from a set of physical disk images from a RAID array, given a set of RAID parameters. Depending on the controller used (software or hardware), some of the RAID parameters can be automatically detected. See Supported RAID Metadata Formats for a list of metadata formats that can be automatically detected.



RAID Image Files:

Path	Format	Offset	Size
C:\passmark\400 - Linux So...	VMWare Image	32256	106
C:\passmark\400 - Linux So...	VMWare Image	32256	106
C:\passmark\400 - Linux So...	VMWare Image	32256	106

Configuration: RAID 5 (Backward Dynamic Parity) [AMI]

Mapping: 0,1,2,p,4,5,p,3,8,p,6,7,p,9,10,11

Stripe Size: 16384 ☑ Check parity/redundancy

Target Image File: C:\passmark\400 - Linux Software RAID Rebuild\RAID C\raidc.aff

Advanced Forensics Format (AFF) Image

Compression Level: Fast

Status: Copying (39 Seconds Remaining)

Data Written: 400.0 MB Disk Size: 2.99 GB

Speed: 67.30 MB/s Unreadable Data: None

RAID Image Files
List of source image files from disks to rebuild from, in the listed order.

Add...
Adds an image file to the list

Remove
Removes the selected image file(s) from the list

Edit...
Modify the offset and size of the selected image file

Info...
Displays any metadata information associated with the image file.

Configuration
Describes how the disks are arranged to achieve a particular level of redundancy and performance

RAID 0

Arranges the disks to provide increased performance and capacity. Blocks of data are striped consecutively on consecutive disks

RAID 1
Arranges the disks to provide increased reliability. Blocks of data are copied on the same physical block of all disks, resulting in all disks being mirror images of each other. Disk images configured in RAID 1 do not need to be reassembled (as all disks contain all blocks from the original image), but can be checked for integrity.

RAID 0+1
A nested RAID that combines RAID 0 and RAID 1, providing redundancy and performance. Two or more disks are arranged in RAID 0, which are then mirrored onto another set of disks. This creates a mirror of stripes.

RAID 1+0
Like RAID 0+1, RAID 1+0 is a hybrid of RAID 0 and RAID 1 configurations. In this case, a set of RAID 1 mirrors are arranged into RAID 0 configuration, creating a stripe of mirrors.

RAID 3
Arranges the disk to provide a balance between performance, capacity and reliability. Consecutive bytes are striped onto consecutive disks, with the last disk being used exclusively for parity bytes. As such, the last disk is not directly used in rebuilding the logical image but for verifying the integrity of the data.

RAID 4
Like RAID 3, this configuration provides a balance between performance, capacity and reliability. In this case, blocks of data (rather than single bytes) are striped consecutively on consecutive disks, with the last disk being used exclusively for parity blocks. Again, the last disk is not directly used in rebuilding the logical image but for verifying the integrity of the data.

RAID 5
Similar to RAID 4, the disk is arranged to provide a balance between performance, capacity and reliability. However, instead of having a disk exclusively for parity blocks, the parity blocks are distributed amongst all disks. This reduces the risk of losing data when a single disk fails.

Forward Parity (a.k.a. right asymmetric)
The parity block is rotated from the first disk to the last disk. For each stripe, the ordering of the data blocks start at the first disk, from left to right.

Forward Dynamic Parity (a.k.a. right symmetric)
The parity block is rotated from the first disk to the last disk. For each stripe, the ordering of the data blocks start at the parity block, from left to right.

Backward Parity (a.k.a. left asymmetric)
The parity block is rotated from the last disk to the first disk. For each stripe, the ordering of the data blocks start at the first disk, from left to right.

Backward Dynamic Parity (a.k.a. left symmetric)
The parity block is rotated from the last disk to the first disk. For each stripe, the ordering of the data blocks start at the parity block, from left to right.

Backward Delayed Parity
Similar to Backward Parity, the parity block is rotated from the last disk to the first disk. However, instead of the parity block rotating to the next disk on the next stripe, it

is written on the same disk for a set number of stripes (called the delay). If the delay is 1, then this will be the same as Backward Parity.

Spanned
This configuration is not a RAID level but is a simple concatenation of two or more disks to provide increased capacity.

Mapping
Provides the mapping pattern between a a physical disk/stripe pair to a logical block number, depending on the selected configuration. For example, the mapping for a RAID 5 (Backward dynamic) configuration is as follows:

	Disk 1	**Disk 2**	**Disk 3**
0	0	1	P
1	3	P	2
2	P	4	5

The numbers represent the logical block number and 'P' represents a parity block. Each row represents a stripe. The mapping pattern would be the following 1-D array:

0, 1, P, 3, P, 2, P, 4, 5

Stripe Size
The size of the smallest unit of contiguous data addressable in a RAID array. In order to rebuild the logical image, the stripe size along with the disk ordering specified by the RAID configuration determines how the source disk images are striped to form the logical image.

Check parity/redundancy
If checked, the parity blocks (if present) are checked to verify the integrity of the RAID array

Target Image File
The location to save the rebuilt RAID image file to. After specifying the image file path to save to, the image file format shall be displayed below depending on the file extension used.

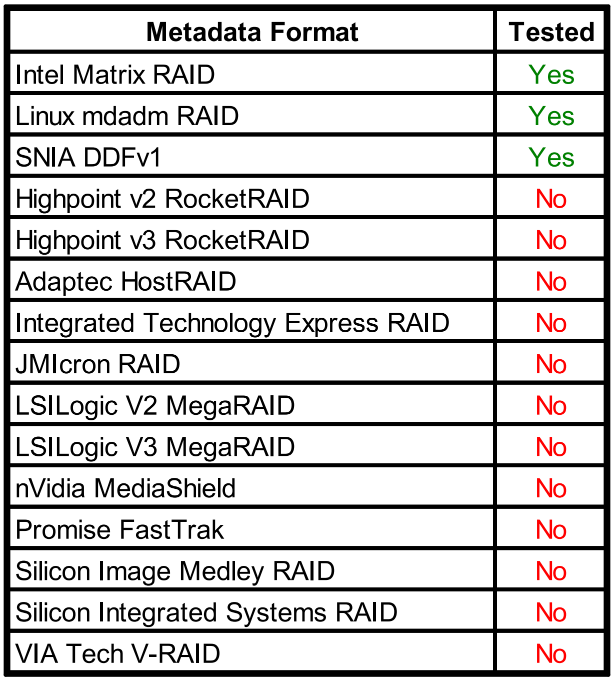
Compression Level
If the image file format supports compression, one of the following level of compression of the image file can be specified: None, Fast, or Best.

Status
The current status of the rebuilding process. Also shows a duration where available. Note that the duration is only for that particular step or the process.

Unreadable Data
If a sector was unreadable, it will fill that sector with 0's and continue on. This field lets you know how much data was unreadable, due to restricted access or a damaged disk.

4.19.4.1 Supported RAID Metadata Formats

Typically when a RAID array is managed by a RAID controller, metadata describing the specific RAID parameters (eg. stripe size, RAID level, etc.) is written to the beginning or end of each member disk. This allows the controller to properly assemble the RAID array each time on power-up. However, the format of the metadata is different depending on the manufacturer of the RAID controller. The following table summarizes the metadata format that can be automatically detected by OSForensics when rebuilding a RAID array:



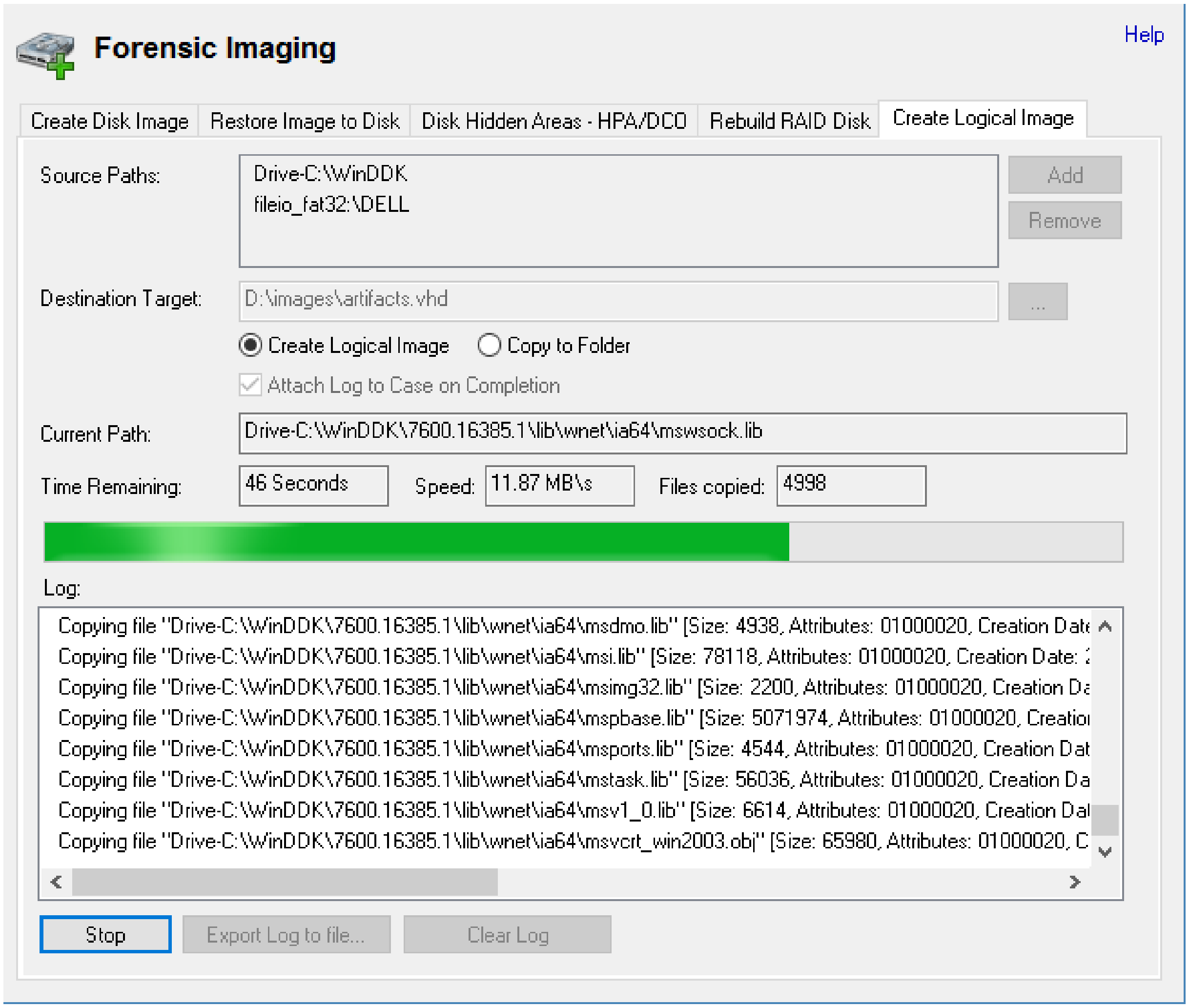
Metadata Format	Tested
Intel Matrix RAID	Yes
Linux mdadm RAID	Yes
SNIA DDFv1	Yes
Highpoint v2 RocketRAID	No
Highpoint v3 RocketRAID	No
Adaptec HostRAID	No
Integrated Technology Express RAID	No
JMIcron RAID	No
LSILogic V2 MegaRAID	No
LSILogic V3 MegaRAID	No
nVidia MediaShield	No
Promise FastTrak	No
Silicon Image Medley RAID	No
Silicon Integrated Systems RAID	No
VIA Tech V-RAID	No

4.19.5 Create Logical Image

Creating a logical image allows the investigator to copy files/directories from one or more source devices to a destination folder or image file, preserving as much file system metadata (eg. date/times, attributes) as possible. This is useful for cases where making a complete drive image of the evidence device is not preferable (eg. due to disk size). Note that while the directory structure, file contents, and some metadata are preserved, some data may be lost from the operation such as slack space, fragmentation, unallocated space, deleted files, etc.

When specifying a destination target, the investigation can either specify a folder or an image file (Windows 7 or later) to copy the directory contents to. If the 'Image File' option is selected, a Virtual Hard Disk (VHD) image file is generated which shall contain the directory and contents. Before the copy operation takes place, a VHD image file is created, attached, and mounted to the system to a drive letter as an NTFS volume. Once the operation is complete, the virtual disk is detached from the system upon which the image file can be added to the case or re-mounted using Disk Management in Windows.

While the operation is running, a log is generated which contains the files/directories that were copied, general status messages and any error messages. The most common reason for failure is that they are locked by another process or the current user does not have permissions to access them. The log can be exported to a text file and/or added to the case as an attachment.



Source Paths: Drive-C:\WinDDK
fileio_fat32:\DELL

Destination Target: D:\images\artifacts.vhd

● Create Logical Image ○ Copy to Folder

☑ Attach Log to Case on Completion

Current Path: Drive-C:\WinDDK\7600.16385.1\lib\wnet\ia64\mswsock.lib

Time Remaining: 46 Seconds Speed: 11.87 MB\s Files copied: 4998

Log:

```
Copying file "Drive-C:\WinDDK\7600.16385.1\lib\wnet\ia64\msdmo.lib" [Size: 4938, Attributes: 01000020, Creation Date
Copying file "Drive-C:\WinDDK\7600.16385.1\lib\wnet\ia64\msi.lib" [Size: 78118, Attributes: 01000020, Creation Date: 2
Copying file "Drive-C:\WinDDK\7600.16385.1\lib\wnet\ia64\msimg32.lib" [Size: 2200, Attributes: 01000020, Creation Da
Copying file "Drive-C:\WinDDK\7600.16385.1\lib\wnet\ia64\mspbase.lib" [Size: 5071974, Attributes: 01000020, Creatio
Copying file "Drive-C:\WinDDK\7600.16385.1\lib\wnet\ia64\msports.lib" [Size: 4544, Attributes: 01000020, Creation Dat
Copying file "Drive-C:\WinDDK\7600.16385.1\lib\wnet\ia64\mstask.lib" [Size: 56036, Attributes: 01000020, Creation Da
Copying file "Drive-C:\WinDDK\7600.16385.1\lib\wnet\ia64\msv1_0.lib" [Size: 6614, Attributes: 01000020, Creation Dat
Copying file "Drive-C:\WinDDK\7600.16385.1\lib\wnet\ia64\msvcrt_win2003.obj" [Size: 65980, Attributes: 01000020, C
```

The following table summarizes the metadata that is preserved when performign a forensics copy

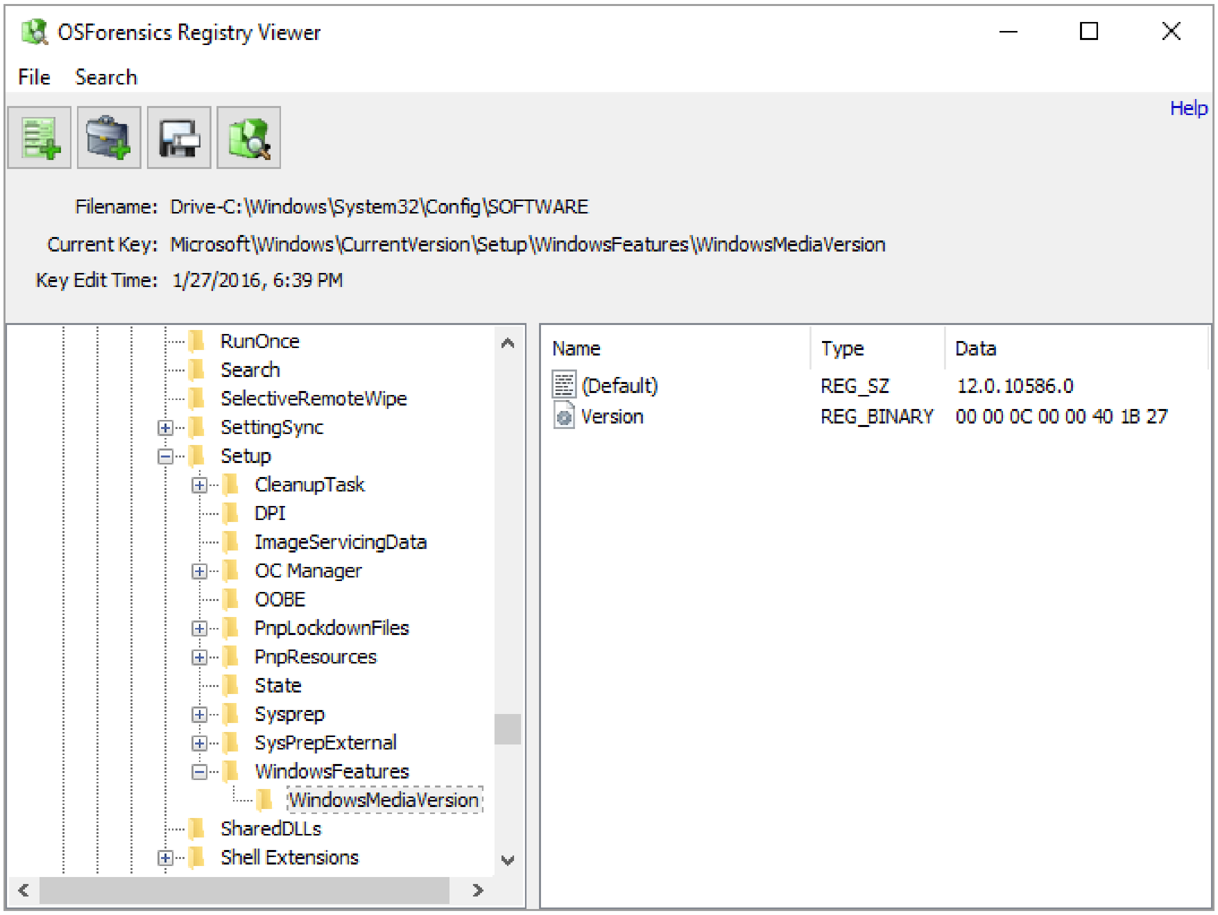
	Preserved
Creation Date	✓
Last Accessed Date	✓
Last Modified Date	✓
Last Attribute Modified Date	✗
File Attributes	✓
Short (8.3) file names	✓*
Streams	✓*
Owners / Groups	✓*

Permissions (ACL)	✓*
File fragmentation	✗
Slack space	✗
Deleted files/ directories	✗

** Only if supported by the source/destination file system*

4.20 Registry Viewer

OSForensics includes a built in registry viewer to display the contents of registry hive files and has options to copy value names, data and to export registry keys and their sub keys to a text file.



Filename: Drive-C:\Windows\System32\Config\SOFTWARE

Current Key: Microsoft\Windows\CurrentVersion\Setup\WindowsFeatures\WindowsMediaVersion

Key Edit Time: 1/27/2016, 6:39 PM

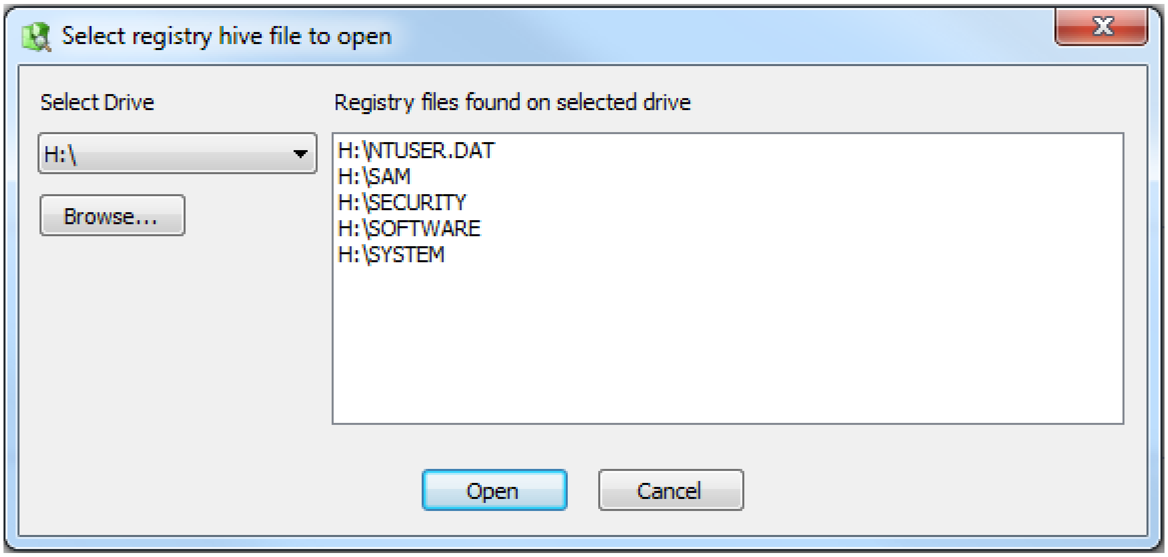
Name	Type	Data
(Default)	REG_SZ	12.0.10586.0
Version	REG_BINARY	00 00 0C 00 00 40 1B 27

OSForensics Registry Viewer

Right clicking on an item in the list view will allow you to copy the value's location (full key name and the value name), value data and to add the item to a save as a HTML os CSV formatted document.

Opening a Registry File

Clicking the "Registry Viewer" icon on the Start tab of OSForensics will open a dialog that will allow you to pick a registry file to open. When a drive is selected, the known locations of registry files as well as the root directory are scanned. Any registry files found will be displayed. If you have a collection of registry files in another location you can use the "Browse" button to navigate to their location and open them.

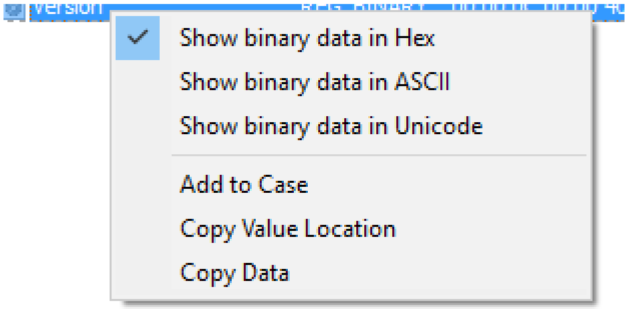


Selecting a file to open

Usage

Right-click Menu

Right-clicking a registry key brings up the following menu:



Show binary data in Hex
Display all registry data of type REG_BINARY in hex format

Show binary data in ASCII
Display all registry data of type REG_BINARY in ASCII format

Show binary data in Unicode
Display all registry data of type REG_BINARY in Unicode format

Add to Case
Save all values of the current key as a CSV/HTML list and add to the case

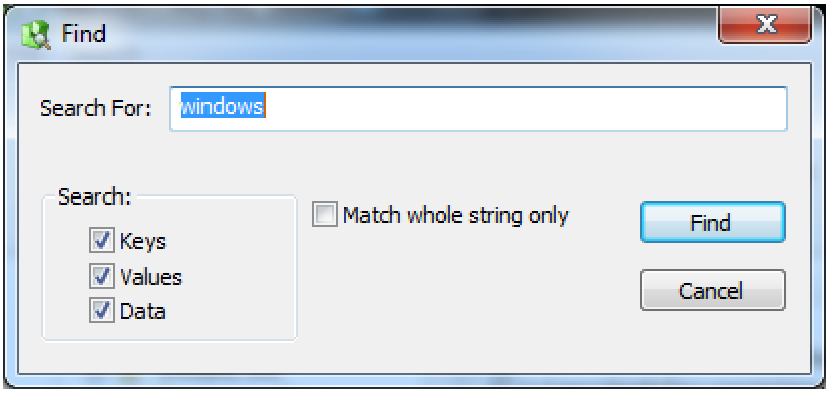
Copy Value Location
Copy the selected registry value location to clipboard

Copy Data

Copy the selected registry value data to clipboard

Search

To search for a string pattern in the registry, open the 'Search' menu and select 'Find...'. In the dialog (as shown below), you can specify a search term, whether keys, values and/or data are matched, and whether the whole search string must be matched.



Find

Search For: windows

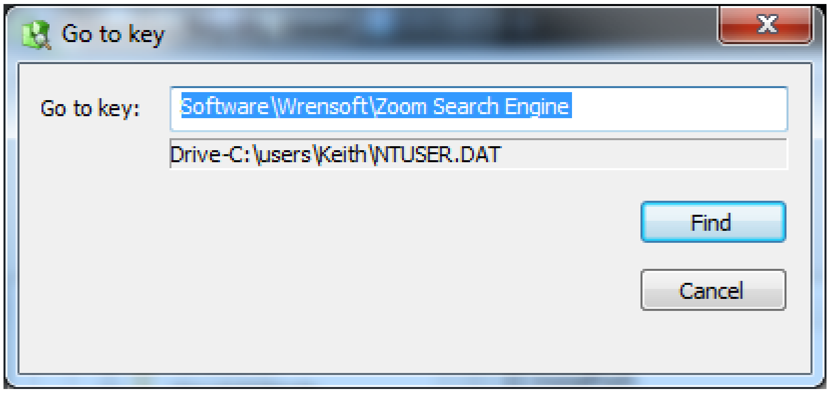
Search:
☑ Keys
☑ Values
☑ Data

□ Match whole string only

Once the search parameters are specified, click 'Find' to locate the next registry item that matches these parameters. You can also repeat the previous search by selecting 'Find Next' under the 'Search' menu

Go to Key

To jump to a particular key in the registry, open the 'Search' menu and select 'Go to Key...'. Enter the desired key, then click 'Find' to select and highlight the key in the Registry Viewer.



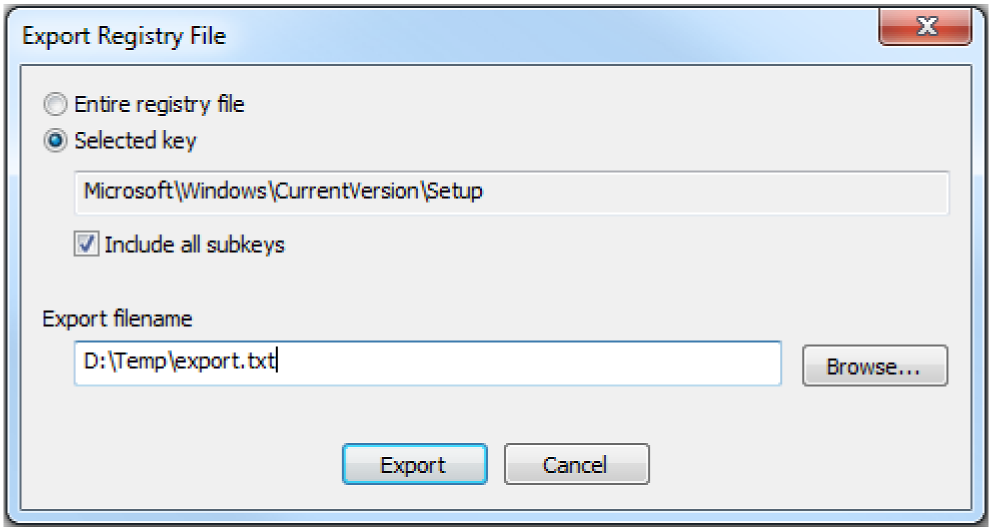
Go to key

Go to key: Software\Wrensoft\Zoom Search Engine

Drive-C:\users\Keith\NTUSER.DAT

Exporting

To export a registry key, or entire file, open the "File" menu and select the "Export to text..." option.


Export Registry File

○ Entire registry file

● Selected key

Microsoft\Windows\CurrentVersion\Setup

☑ Include all subkeys

Export filename

D:\Temp\export.txt

Exporting a registry key

4.21 Internal Viewer

OSForensics includes a built-in stream viewer for viewing the contents of files, deleted files, memory sections and raw sectors. The stream viewer consists of several viewing modes that aid specifically in forensic data analysis

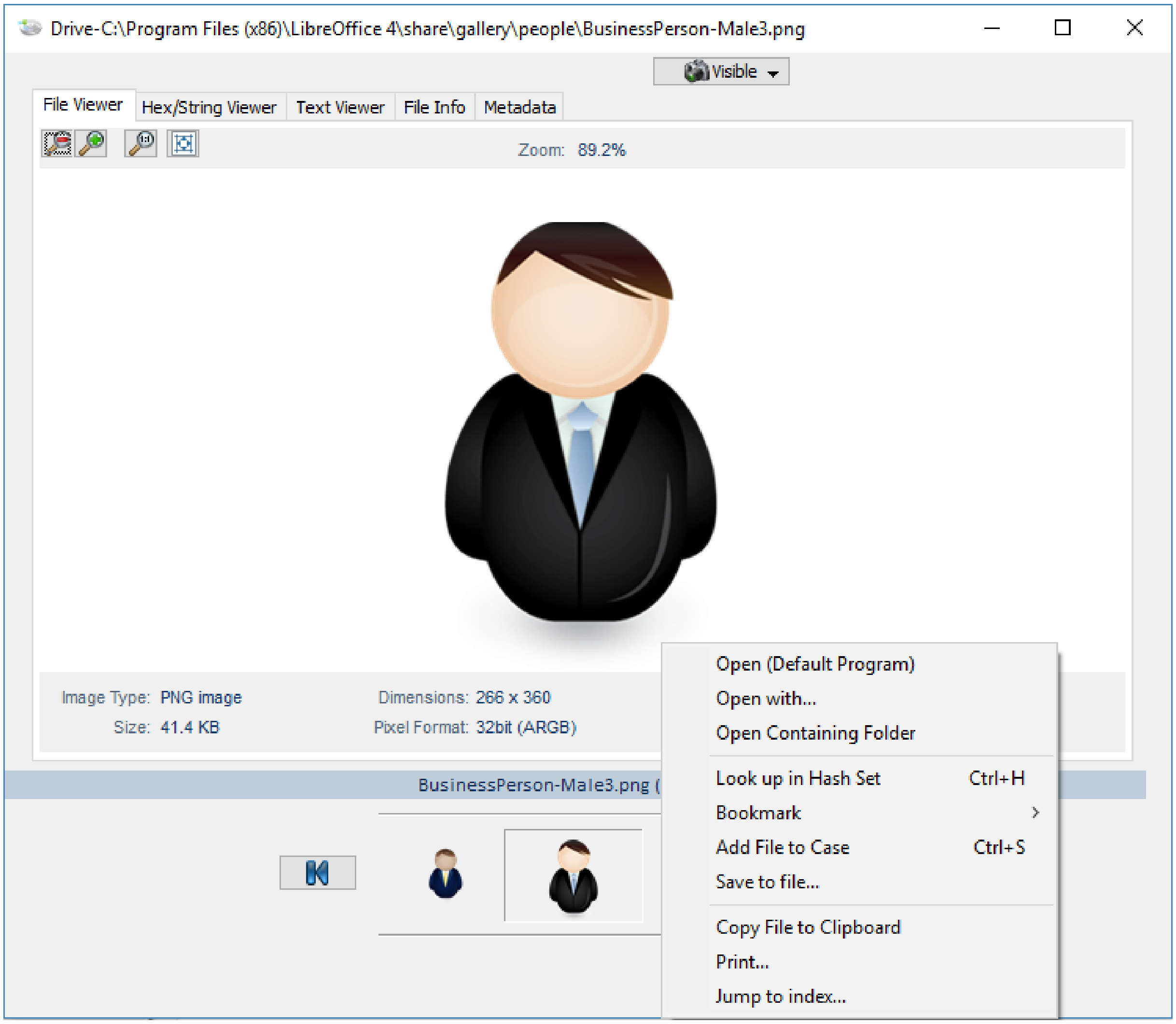


Image Type: PNG image
Size: 41.4 KB
Dimensions: 266 x 360
Pixel Format: 32bit (ARGB)

File Viewer

Previews the data stream as a common file format (ie. image, video, document)

Hex/String Viewer

Views the data stream as raw bytes (in hex) and extracts any strings contained in the stream

Text Viewer

Views the data stream as text

File Info

Displays the attributes of the data stream

Metadata

Display the file format specific metadata of the file

To scroll between the items, use the left/right buttons. Optionally, you can double click the previous/next thumbnails or press the left/right keys.

Keyboard shortcuts

Left/Numpad 4 key - Scroll to previous item

Right/Numpad 6 key- Scroll to next item

Home key - Scroll to first item

End key - Scroll to last item

Esc key - Close the internal viewer

Ctrl-A - Add file to case

Minus key - Reduce the scale of the image

Plus key - Increase the scale of the image

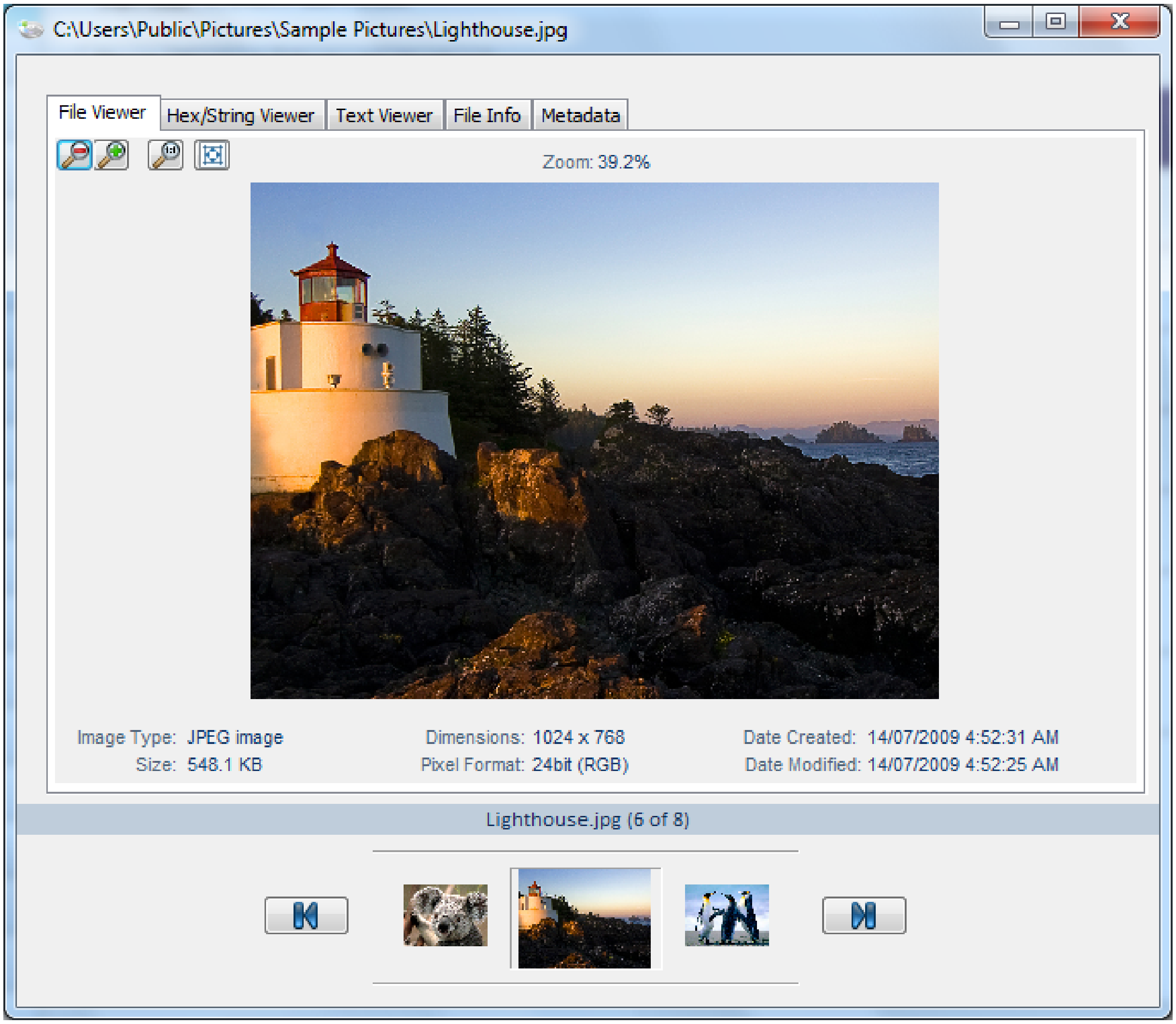
Backslash/Numpad 5 key - Fit image to screen

4.21.1 File Viewer

The file viewer attempts to view the data stream as a common file format. The following file formats are supported:

- Image formats (BMP, JPG, GIF, PNG, Exif, and TIFF)
- Video formats
- Audio formats
- Document formats (PDF, DOC, DOCX, XLS, XLSX, PPT, PPTX, RTF, WPD)
- Compressed formats (7z, XZ, BZIP2, GZIP, TAR, ZIP, WIM, AR, ARJ, CAB, CHM, LZH, LZMA, RAR, XAR and Z)

Image Formats



Zoom: 39.2%

Image Type: JPEG image
Size: 548.1 KB
Dimensions: 1024 x 768
Pixel Format: 24bit (RGB)
Date Created: 14/07/2009 4:52:31 AM
Date Modified: 14/07/2009 4:52:25 AM

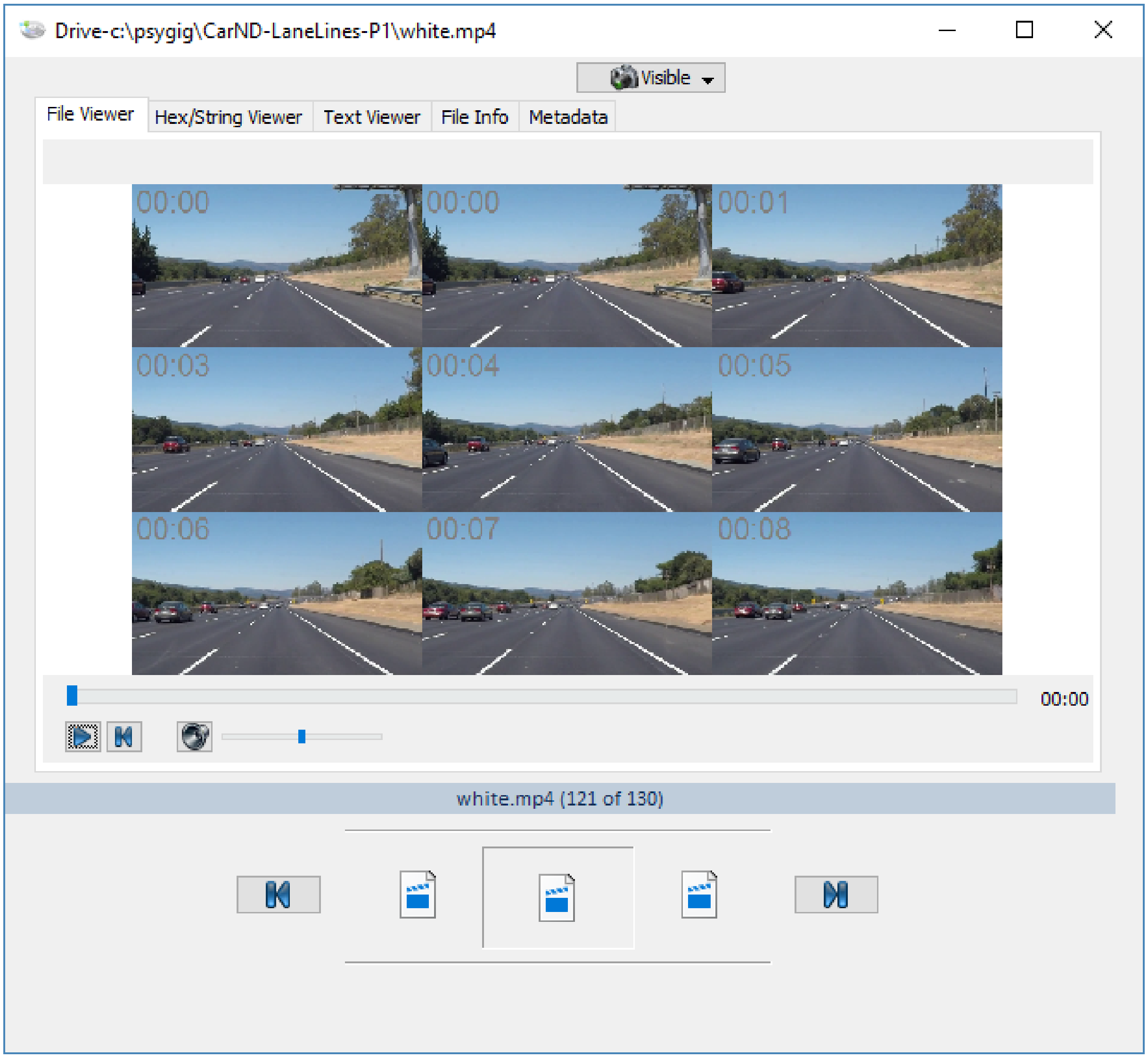
Lighthouse.jpg (6 of 8)

Zoom

To zoom on the image, use the buttons on the top left or alternatively, the scroll wheel on the mouse or +/- keys.

Pan
To pan the image, use the mouse to drag the image in any direction.

Video/Audio Formats



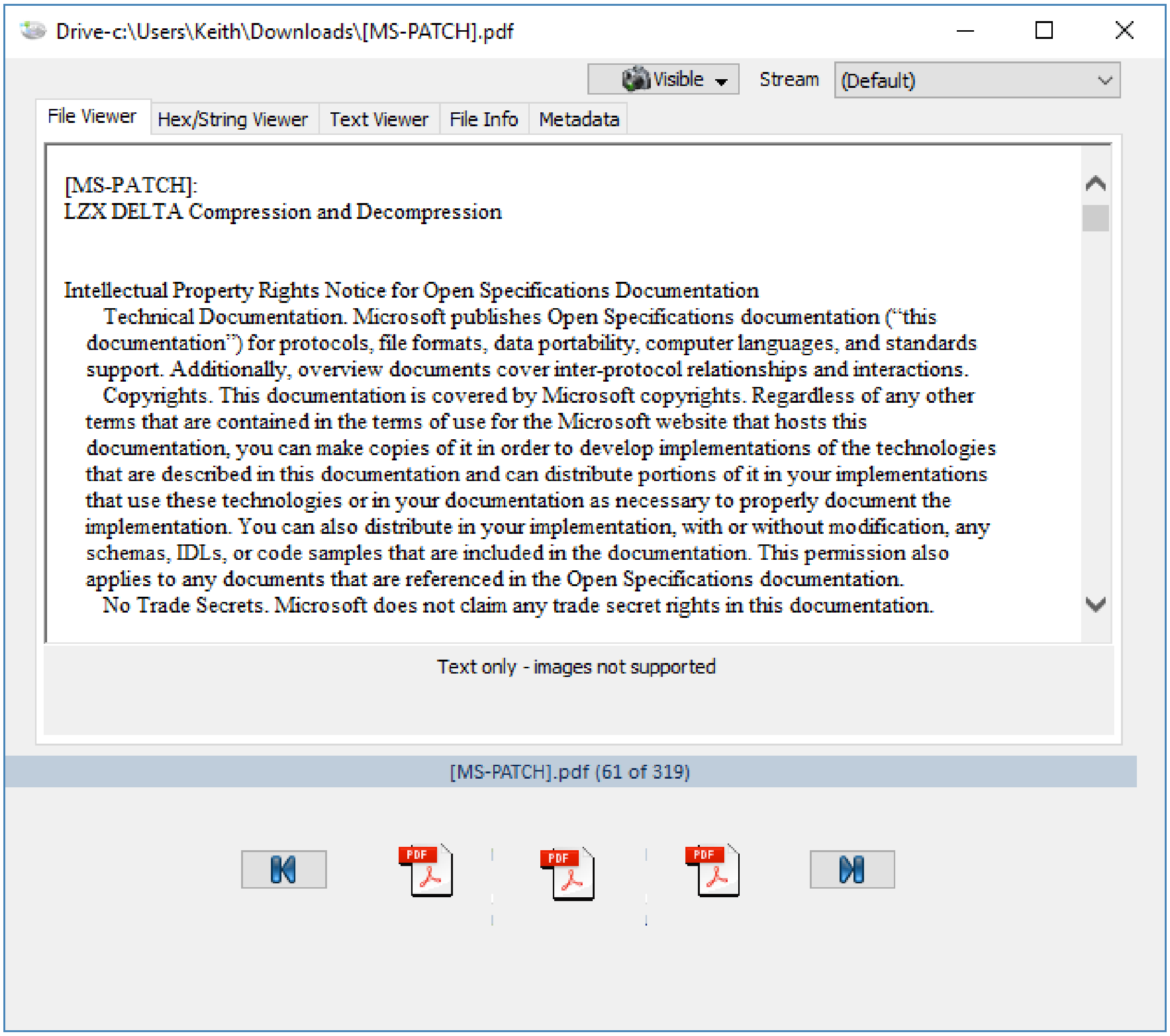
Play/Pause
To play/pause the media file, press the 'Play/Pause' button or click on the image (video only).

Seek
To seek within the media file, drag the slider bar to the desired position.

Rewind
To seek back to the beginning, press the 'Rewind' button.

Volume increase/decrease
To adjust the volume of the audio, use the 'Volume Increase' or 'Volume Decrease' buttons.

Document Formats



[MS-PATCH]:
LZX DELTA Compression and Decompression

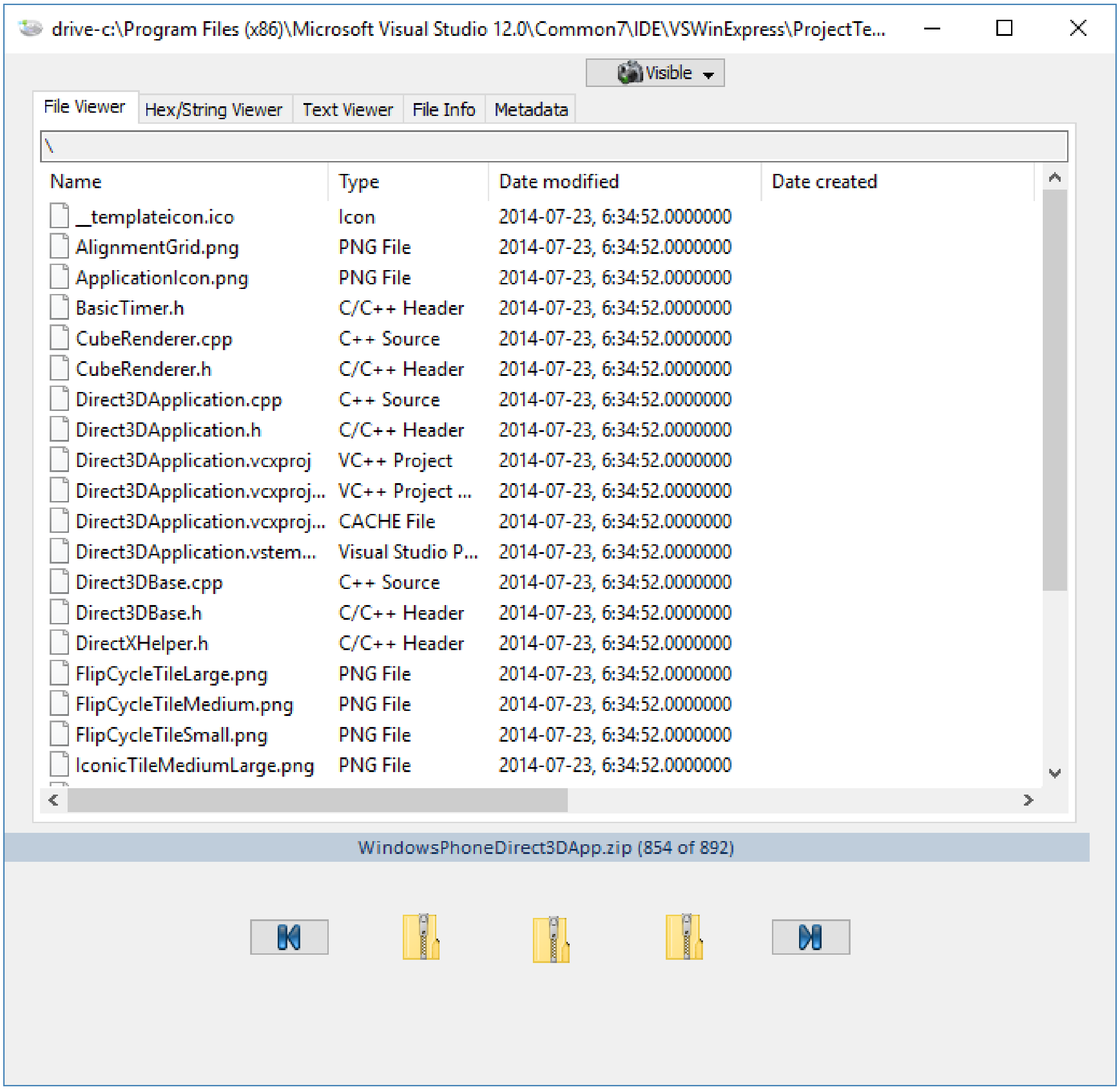
Intellectual Property Rights Notice for Open Specifications Documentation
Technical Documentation. Microsoft publishes Open Specifications documentation ("this documentation") for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
Copyrights. This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
No Trade Secrets. Microsoft does not claim any trade secret rights in this documentation.

Text only - images not supported

[MS-PATCH].pdf (61 of 319)

Only the text component of the document file is displayed. Formatting is not preserved.

Compressed Formats


drive-c:\Program Files (x86)\Microsoft Visual Studio 12.0\Common7\IDE\VSWinExpress\ProjectTe...
Visible
File Viewer
Hex/String Viewer
Text Viewer
File Info
Metadata

\

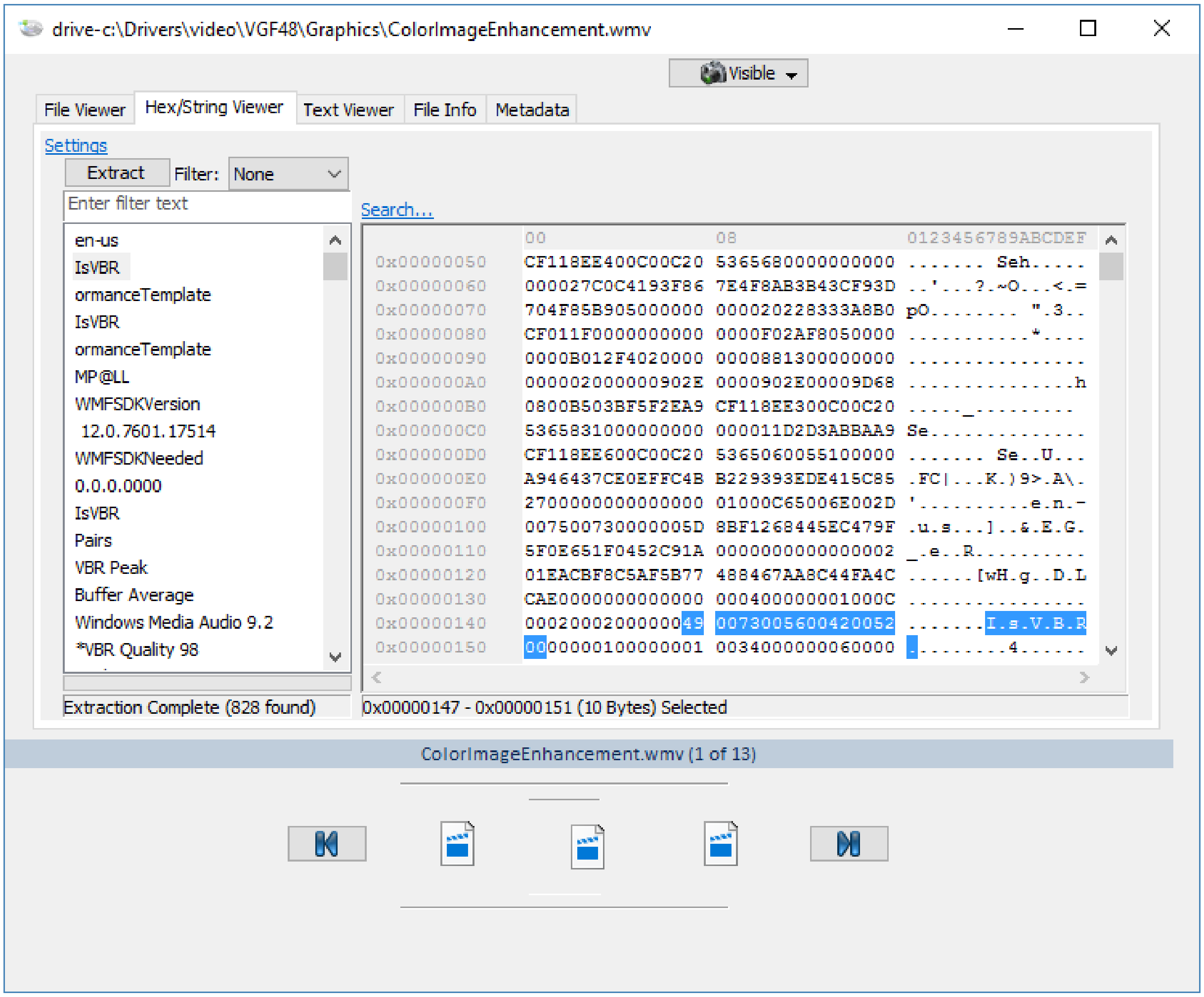
Name	Type	Date modified	Date created
__templateicon.ico	Icon	2014-07-23, 6:34:52.0000000	
AlignmentGrid.png	PNG File	2014-07-23, 6:34:52.0000000	
ApplicationIcon.png	PNG File	2014-07-23, 6:34:52.0000000	
BasicTimer.h	C/C++ Header	2014-07-23, 6:34:52.0000000	
CubeRenderer.cpp	C++ Source	2014-07-23, 6:34:52.0000000	
CubeRenderer.h	C/C++ Header	2014-07-23, 6:34:52.0000000	
Direct3DApplication.cpp	C++ Source	2014-07-23, 6:34:52.0000000	
Direct3DApplication.h	C/C++ Header	2014-07-23, 6:34:52.0000000	
Direct3DApplication.vcxproj	VC++ Project	2014-07-23, 6:34:52.0000000	
Direct3DApplication.vcxproj...	VC++ Project ...	2014-07-23, 6:34:52.0000000	
Direct3DApplication.vcxproj...	CACHE File	2014-07-23, 6:34:52.0000000	
Direct3DApplication.vstem...	Visual Studio P...	2014-07-23, 6:34:52.0000000	
Direct3DBase.cpp	C++ Source	2014-07-23, 6:34:52.0000000	
Direct3DBase.h	C/C++ Header	2014-07-23, 6:34:52.0000000	
DirectXHelper.h	C/C++ Header	2014-07-23, 6:34:52.0000000	
FlipCycleTileLarge.png	PNG File	2014-07-23, 6:34:52.0000000	
FlipCycleTileMedium.png	PNG File	2014-07-23, 6:34:52.0000000	
FlipCycleTileSmall.png	PNG File	2014-07-23, 6:34:52.0000000	
IconicTileMediumLarge.png	PNG File	2014-07-23, 6:34:52.0000000	

WindowsPhoneDirect3DApp.zip (854 of 892)

The contents of the compressed file are displayed in a list view. Pressing 'enter' or double-clicking the selected file shall extract and open the file in another OSForensics Viewer window.

4.21.2 Hex/String Viewer

The hex/string viewer displays the data stream as raw data bytes in hex. This mode also allows the user to extract ASCII/Unicode strings from the raw data bytes.



```
en-us
IsVBR
ormanceTemplate
IsVBR
ormanceTemplate
MP@LL
WMFSDKVersion
 12.0.7601.17514
WMFSDKNeeded
0.0.0.0000
IsVBR
Pairs
VBR Peak
Buffer Average
Windows Media Audio 9.2
*VBR Quality 98
```

Extraction Complete (828 found)

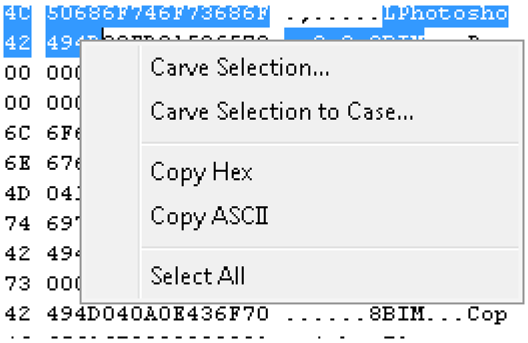
```
            00               08               0123456789ABCDEF
0x00000050  CF118EE400C00C20 5365680000000000 ........Seh.....
0x00000060  000027C0C4193F86 7E4F8AB3B43CF93D ..'...?.~O...<.=
0x00000070  704F85B905000000 00002022833A8B0 pO........ ".3..
0x00000080  CF011F0000000000 0000F02AF8050000 ...........*....
0x00000090  0000B012F4020000 0000881300000000 ................
0x000000A0  000002000000902E 0000902E00009D68 ...............h
0x000000B0  0800B503BF5F2EA9 CF118EE300C00C20 ....._.........
0x000000C0  5365831000000000 000011D2D3ABBAA9 Se..............
0x000000D0  CF118EE600C00C20 5365060055100000 ........Se..U...
0x000000E0  A946437CE0EFFC4B B229393EDE415C85 .FC|...K.)9>.A\.
0x000000F0  2700000000000000 01000C65006E002D '..........e.n.-
0x00000100  007500730000005D 8BF1268445EC479F .u.s...]..&.E.G.
0x00000110  5F0E651F0452C91A 0000000000000002 _.e..R..........
0x00000120  01EACBF8C5AF5B77 488467AA8C44FA4C ......[wH.g..D.L
0x00000130  CAE0000000000000 000400000001000C ................
0x00000140  0002000200000049 0073005600420052 .......I.s.V.B.R
0x00000150  0000000100000001 0034000000060000 .........4......
```

0x00000147 - 0x00000151 (10 Bytes) Selected

Hex View

The hex view displays the raw data bytes in hex. The starting offset of each line is identified by hex offset on the left margin. The byte groupings can be configured via the Settings window.

Right-clicking opens a context menu as shown below:



```
4C 50686F746F73686F .,......LPhotosho
42 494D040A0E436F70 ......8BIM...Cop
```

Carve Selection...

Carve the selected bytes to file

Carve Selection to Case...
Carve the selected bytes to file and add to the case

Copy Hex
Copy the selected bytes as hex characters to clipboard

Copy ASCII
Copy the selected bytes as ASCII to clipboard

Select All
Select all bytes in the hex viewer

Hex View Search

Clicking on 'Search...' opens a search window (similar to the Raw Disk Viewer search window) for locating hexadecimal/text patterns.

String Extraction

Click the 'Extract' button to locate ASCII/Unicode strings in the data stream. Note that for large files, this process may take some time. Advanced string extraction settings can be configured via the Settings window.

The extracted strings are displayed in this list. To filter the results, enter a search string to narrow the results in the string list. This search is case insensitive and is a substring match. Alternatively, the list of strings may be filtered based on a particular string format:

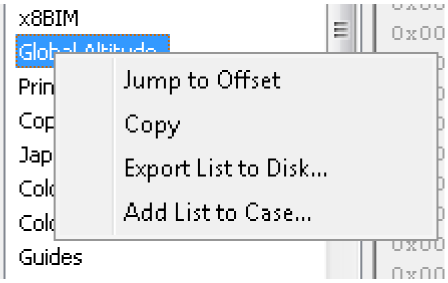
Filename - shows all strings that appear to be in a valid filename format

URL - shows all strings that appear to be in a valid URL address format

GUID - shows all strings that appear to be in a valid GUID identifier format

IP Address - shows all strings that appear to be a valid IP address format

Right-clicking opens a context menu as shown below:



Jump to Offset
Jump to the location of the string in the hex view

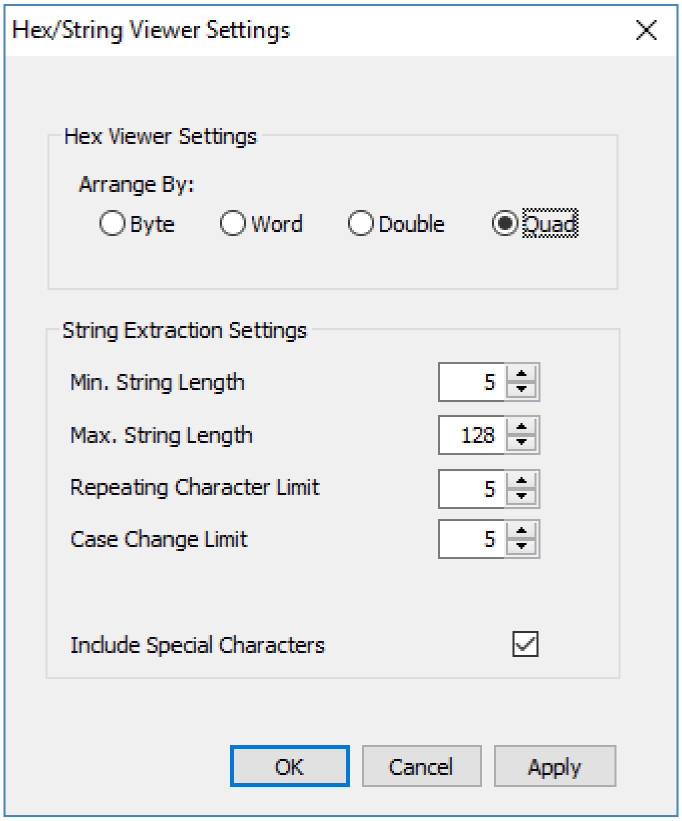
Copy
Copy the word into the clipboard

Export List To Disk...
Export the entire string list to a text file

Add List to Case...
Save the entire string list to a text file, then add to the case

4.21.2.1 Hex/String Viewer Settings

The Hex/String Viewer Settings window contains configuration options for the Hex/String Viewer.



Hex/String Viewer Settings

Hex Viewer Settings

Arrange By: ○ Byte ○ Word ○ Double ● Quad

String Extraction Settings

Min. String Length 5

Max. String Length 128

Repeating Character Limit 5

Case Change Limit 5

Include Special Characters ☑

Hex Viewer Settings

Arrange By
Change the hex groupings in the hex view

String Extraction Settings

Min. String Length
The minimum length of the string to be included in the extracted string list

Max. String Length
The maximum length of the string to be included in the extracted string list

Repeating Character Limit

The maximum number of repeating characters a string may contain to be included in the extracted string list

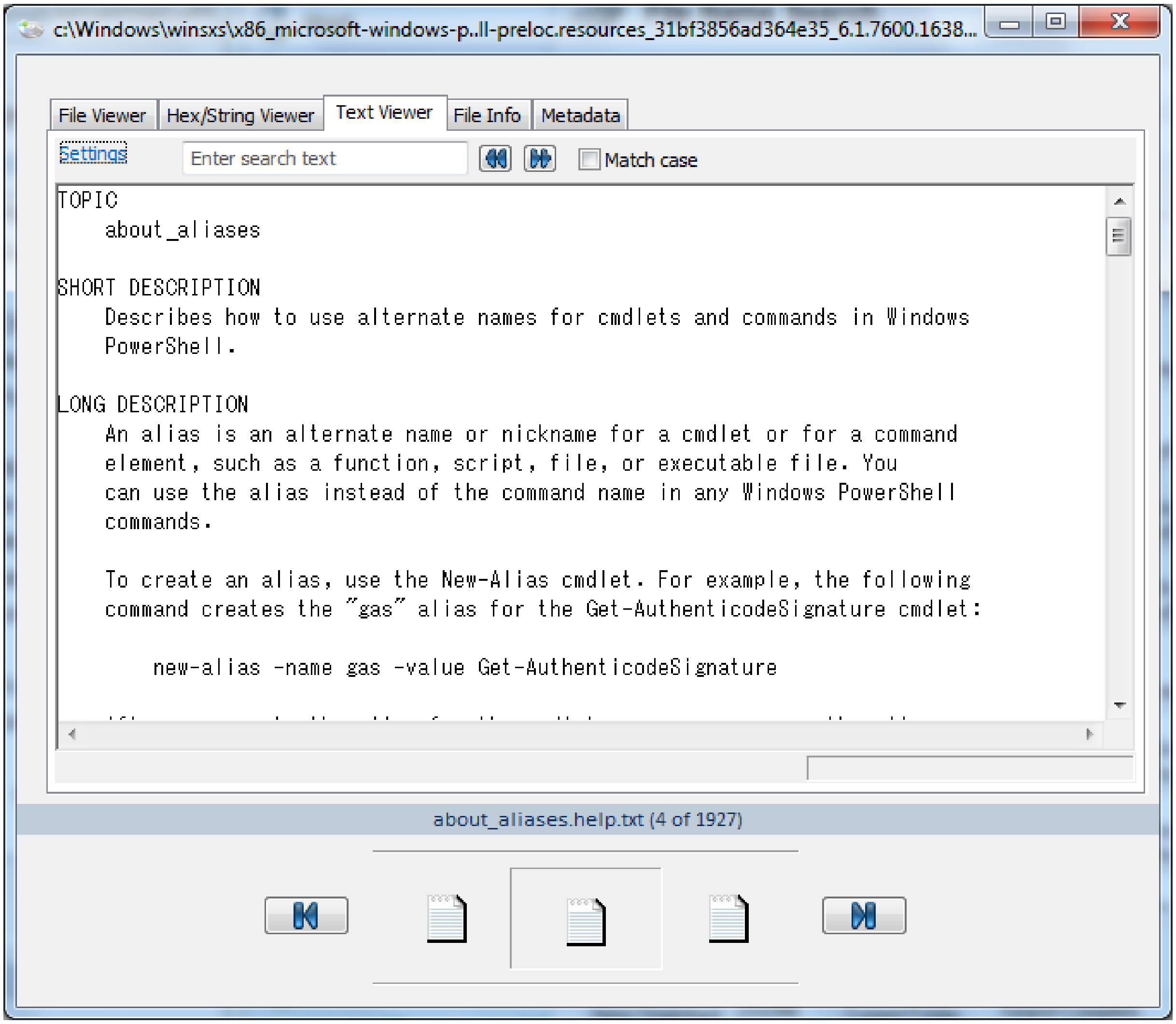
Case Change Limit
The maximum number of case changes for a string to be included in the extracted string list

Include Special Characters
If checked, strings containing the following special characters are included in the extracted string list:

```
~!@#$%^&*()-_=+[{]}\|;:,'.>/?
```

4.21.3 Text Viewer

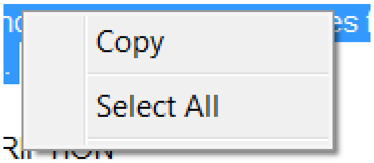
The text viewer displays the data stream as text.



c:\Windows\winsxs\x86_microsoft-windows-p..ll-preloc.resources_31bf3856ad364e35_6.1.7600.1638...
File Viewer
Hex/String Viewer
Text Viewer
File Info
Metadata
Settings
Enter search text
□ Match case
about_aliases.help.txt (4 of 1927)

```
TOPIC
    about_aliases

SHORT DESCRIPTION
    Describes how to use alternate names for cmdlets and commands in Windows
    PowerShell.

LONG DESCRIPTION
    An alias is an alternate name or nickname for a cmdlet or for a command
    element, such as a function, script, file, or executable file. You
    can use the alias instead of the command name in any Windows PowerShell
    commands.

    To create an alias, use the New-Alias cmdlet. For example, the following
    command creates the "gas" alias for the Get-AuthenticodeSignature cmdlet:

        new-alias -name gas -value Get-AuthenticodeSignature
```

Text View
The htext view displays the data stream as text. Right-clicking opens a context menu that allows the user to copy the text into the clipboard.

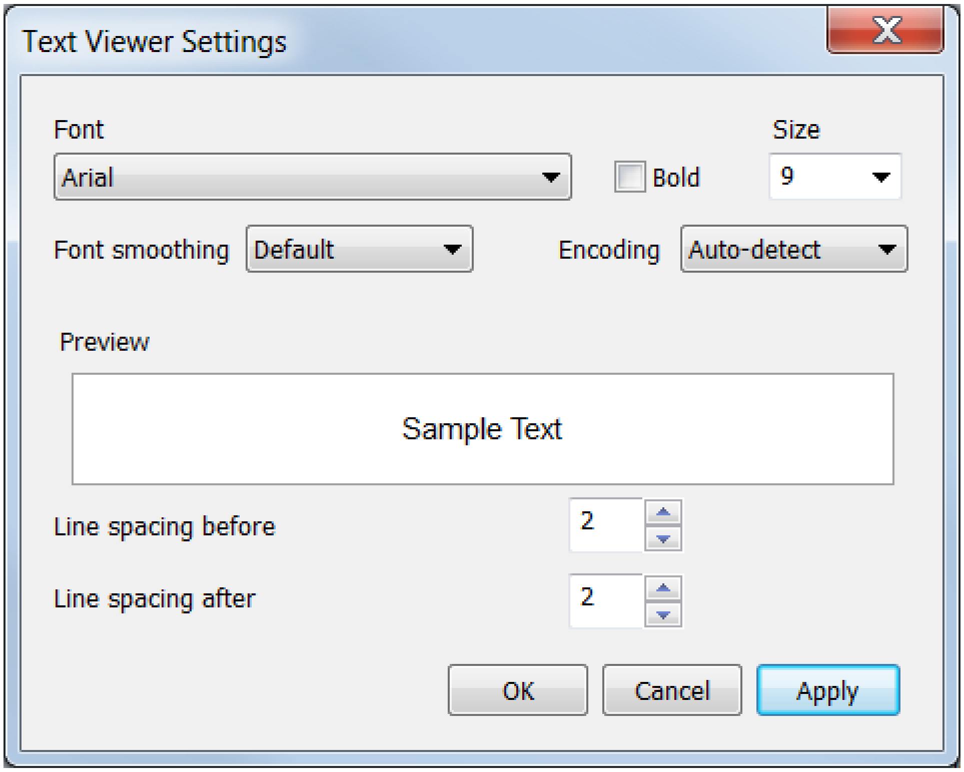


The font settings can be configured via the Settings window.

Text View Search
The user may enter a string pattern to search for in the text view. Use the left/right buttons to search for the previous/next match.

4.21.3.1 Text Viewer Settings

The Text Viewer Settings window contains configuration options for the Text Viewer.


Text Viewer Settings

Font: Arial

□ Bold

Size: 9

Font smoothing: Default

Encoding: Auto-detect

Preview: Sample Text

Line spacing before: 2

Line spacing after: 2

Font
The font to use when displaying the text in the text view

Bold
If checked, all text will be bolded

Size
The font size of the text

Font smoothing
The quality of the font to display the text in

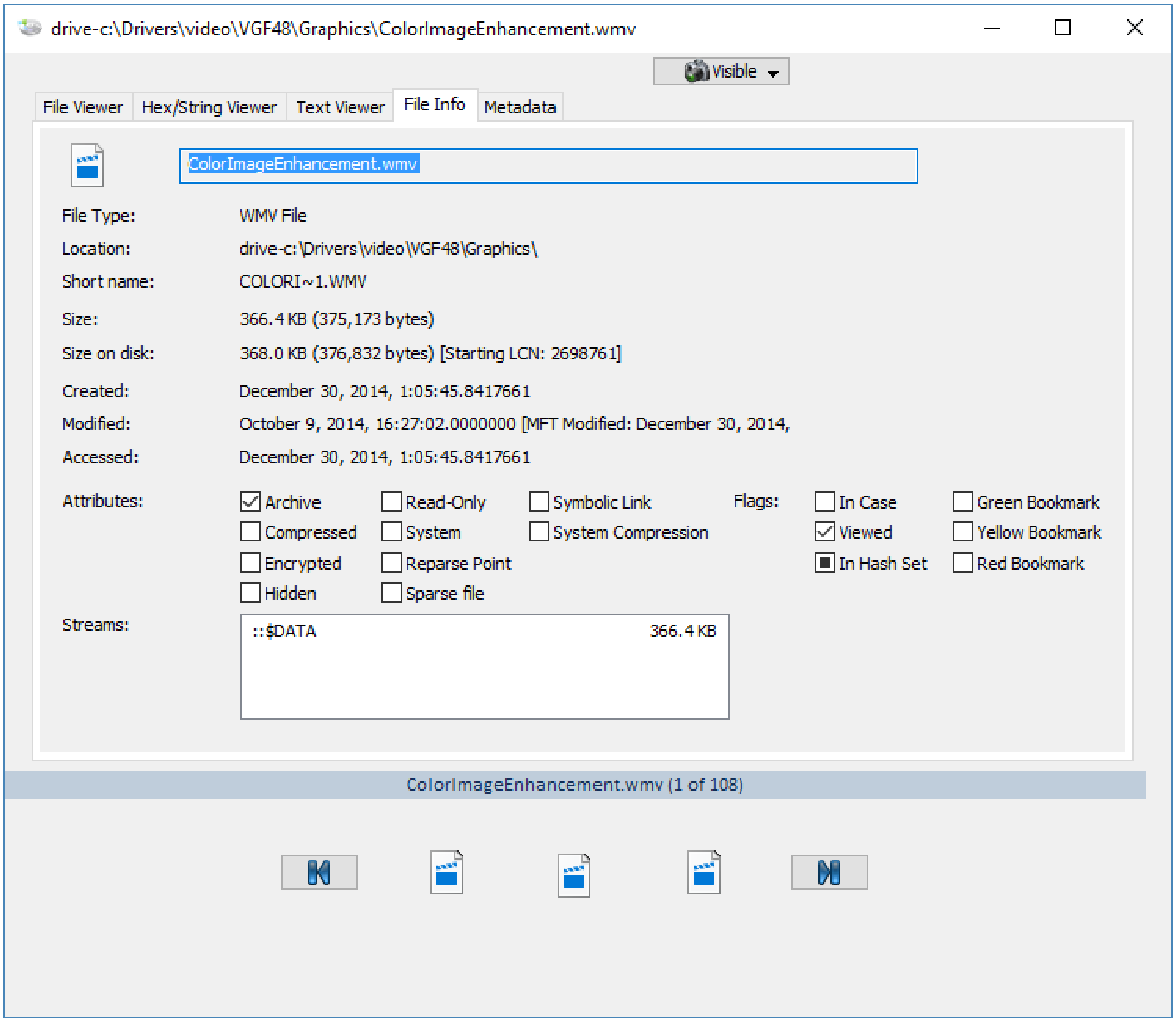
Encoding
The character encoding to view the text in. Choose Auto-detect to automatically determine the character encoding or a specific encoding to force the viewer to use.

Line spacing before
The spacing before each line

Line spacing after
The spacing after each line

4.21.4 File Info

The file info view displays attributes of the data stream.



drive-c:\Drivers\video\VGF48\Graphics\ColorImageEnhancement.wmv

ColorImageEnhancement.wmv

File Type: WMV File
Location: drive-c:\Drivers\video\VGF48\Graphics\
Short name: COLORI~1.WMV
Size: 366.4 KB (375,173 bytes)
Size on disk: 368.0 KB (376,832 bytes) [Starting LCN: 2698761]
Created: December 30, 2014, 1:05:45.8417661
Modified: October 9, 2014, 16:27:02.0000000 [MFT Modified: December 30, 2014,
Accessed: December 30, 2014, 1:05:45.8417661

Attributes: ☑ Archive □ Read-Only □ Symbolic Link
□ Compressed □ System □ System Compression
□ Encrypted □ Reparse Point
□ Hidden □ Sparse file

Flags: □ In Case □ Green Bookmark
☑ Viewed □ Yellow Bookmark
■ In Hash Set □ Red Bookmark

Streams: ::$DATA 366.4 KB

ColorImageEnhancement.wmv (1 of 108)

File Type
The type corresponding to the data stream. For files, this corresponding to the file extension.

Location

The location of the data stream on disk

Short name
If available, the 8.3 filename convention used by older versions of DOS and Windows.

Size
The size of the data stream

Size on disk
The size of the data stream that is actually allocated on disk

Created
The date that the file was created.

Modified
The date that the file was modified. If applicable, the date that the file's attribute was modified shall also be displayed (eg. MFT Modified Date).

Accessed
The date that the file was accessed.

Attributes
The attribute flags that are set for the data stream.

Archive *- This flag indicates whether or not the file has been backed up. When set, the file is flagged to be backed up.*
Compressed *- The file is compressed.*
Encrypted *- The file is encrypted.*
Hidden *- The file is hidden.*
Read-Only *- The file is read-only*
System *- The file is a system file.*
Reparse Point *- (NTFS only) The file contains a reparse point, which is a collection of user-defined data. Typically, reparse points are used to indicate NTFS hard links or system compression.*
Sparse File *- The file contains sparse data, which is a segment of data which contains all zeroes. This segment of data is not allocated on disk and therefore reduces the disk space used by the file.*
Symbolic Link *- (POSIX only) The file is a symbolic link to another file.*
System Compression *- (NTFS only) The file is compressed using the Windows 10 'CompactOS' or 'System Compression' feature.*

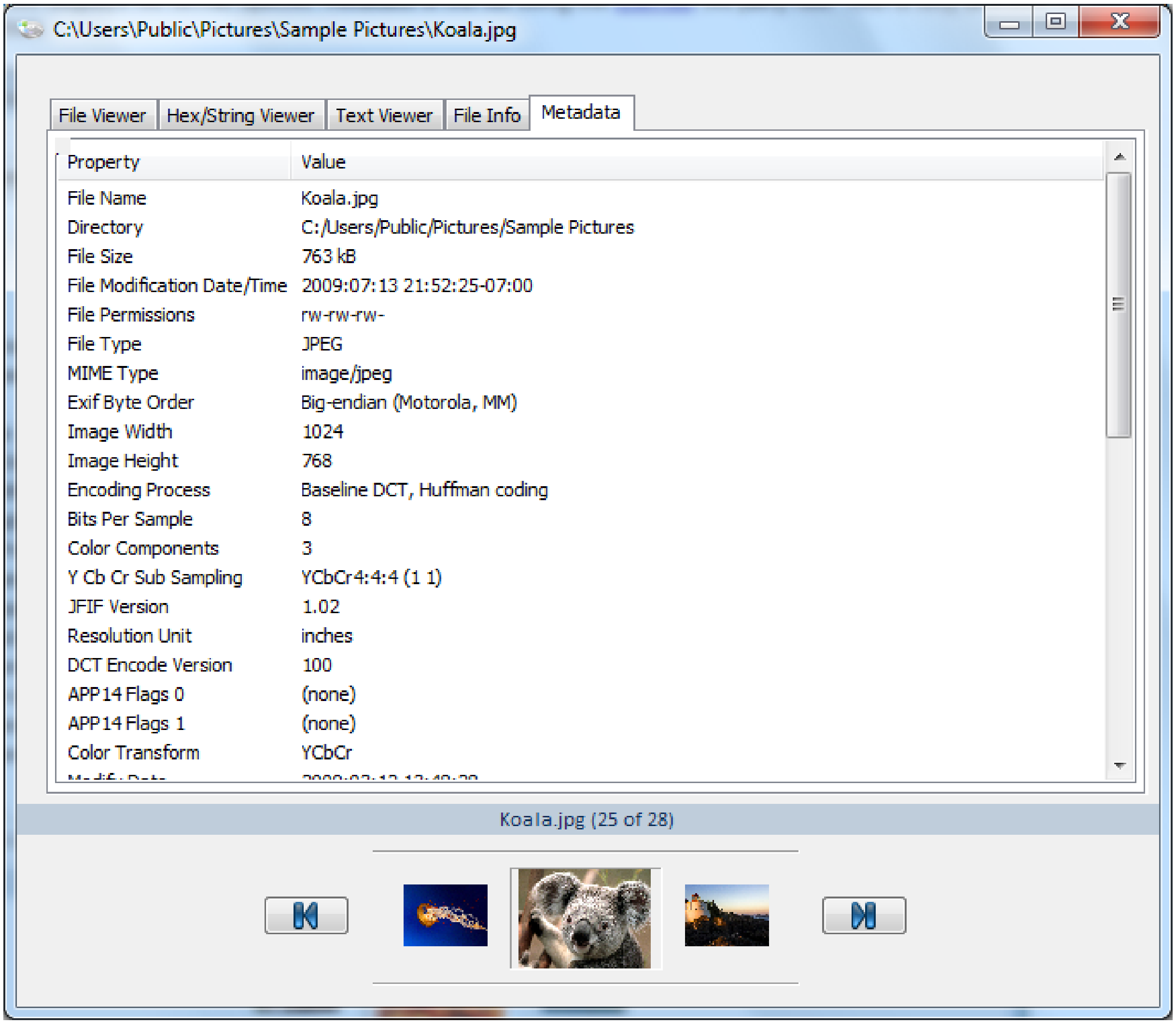
Streams
(NTFS only) The list of streams contained in the file, including the default stream.

4.21.5 Metadata

The metadata view displays file format specific metadata of the current item.

Files

For files, file format specific metadata obtained using the ExifTool 3rd party tool is displayed. This is only available for files and not memory sections or raw sectors.

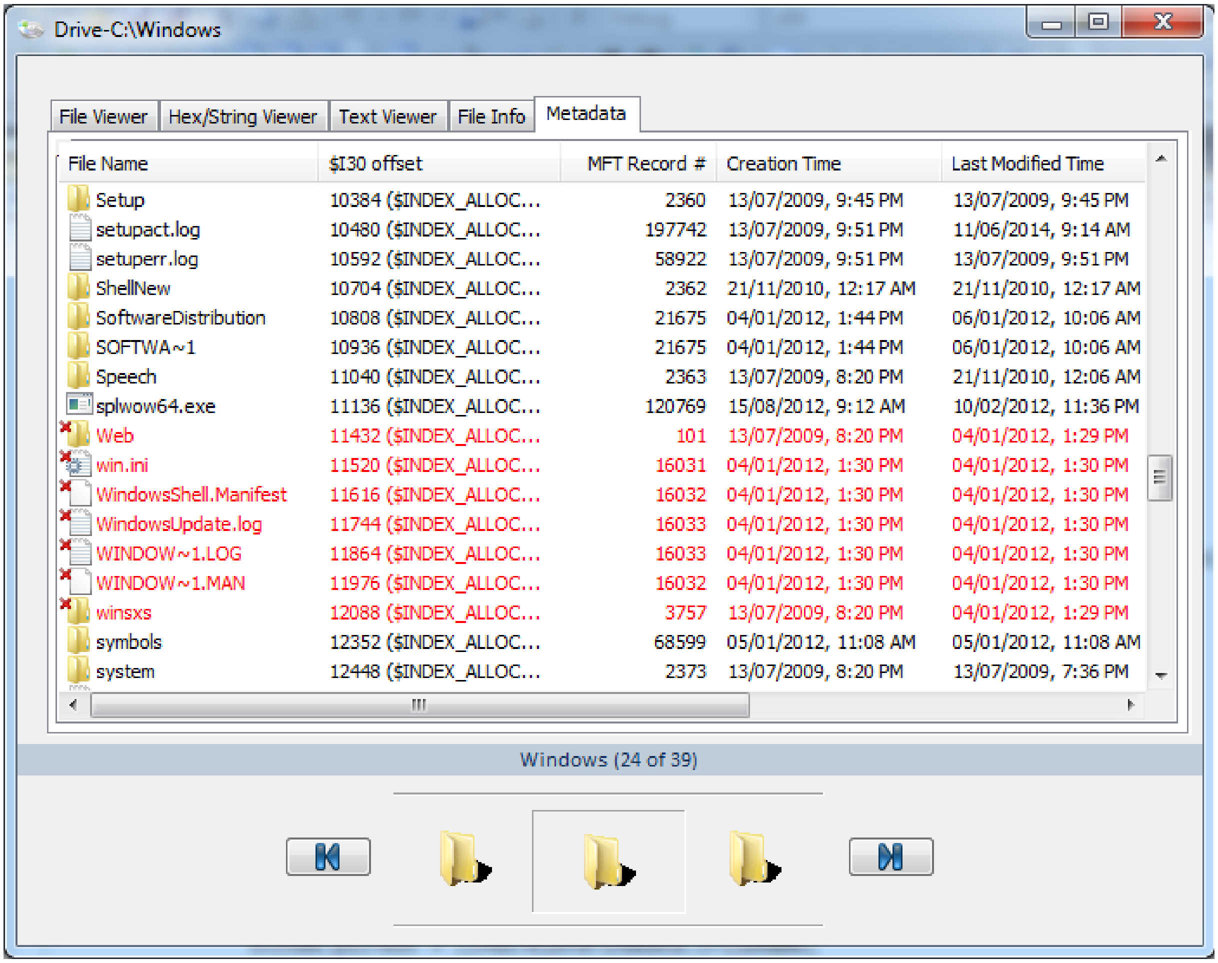


Property	Value
File Name	Koala.jpg
Directory	C:/Users/Public/Pictures/Sample Pictures
File Size	763 kB
File Modification Date/Time	2009:07:13 21:52:25-07:00
File Permissions	rw-rw-rw-
File Type	JPEG
MIME Type	image/jpeg
Exif Byte Order	Big-endian (Motorola, MM)
Image Width	1024
Image Height	768
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:4:4 (1 1)
JFIF Version	1.02
Resolution Unit	inches
DCT Encode Version	100
APP14 Flags 0	(none)
APP14 Flags 1	(none)
Color Transform	YCbCr
Modify Date	2009:03:12 13:48:28

The metadata can be copied to clipboard, or exported to a text file from the right-click menu.

NTFS Directories

In particular for NTFS directories, the metadata view displays the $I30 entries of the folder, which includes entries that have been deleted. This is useful for identifying files or folders that used to belong to the directory (which may or may not be found in a deleted files search)

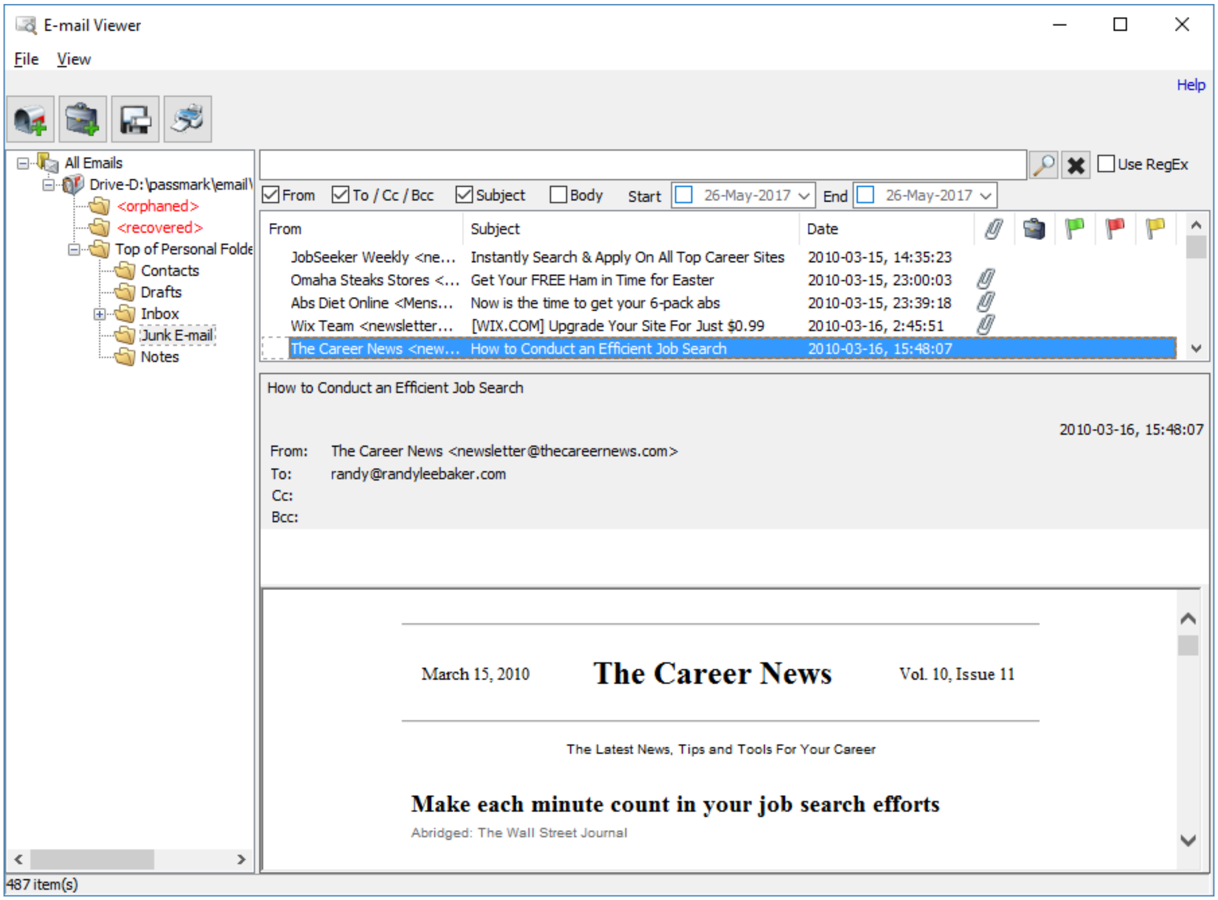


File Name	$I30 offset	MFT Record #	Creation Time	Last Modified Time
Setup	10384 ($INDEX_ALLOC...	2360	13/07/2009, 9:45 PM	13/07/2009, 9:45 PM
setupact.log	10480 ($INDEX_ALLOC...	197742	13/07/2009, 9:51 PM	11/06/2014, 9:14 AM
setuperr.log	10592 ($INDEX_ALLOC...	58922	13/07/2009, 9:51 PM	13/07/2009, 9:51 PM
ShellNew	10704 ($INDEX_ALLOC...	2362	21/11/2010, 12:17 AM	21/11/2010, 12:17 AM
SoftwareDistribution	10808 ($INDEX_ALLOC...	21675	04/01/2012, 1:44 PM	06/01/2012, 10:06 AM
SOFTWA~1	10936 ($INDEX_ALLOC...	21675	04/01/2012, 1:44 PM	06/01/2012, 10:06 AM
Speech	11040 ($INDEX_ALLOC...	2363	13/07/2009, 8:20 PM	21/11/2010, 12:06 AM
splwow64.exe	11136 ($INDEX_ALLOC...	120769	15/08/2012, 9:12 AM	10/02/2012, 11:36 PM
Web	11432 ($INDEX_ALLOC...	101	13/07/2009, 8:20 PM	04/01/2012, 1:29 PM
win.ini	11520 ($INDEX_ALLOC...	16031	04/01/2012, 1:30 PM	04/01/2012, 1:30 PM
WindowsShell.Manifest	11616 ($INDEX_ALLOC...	16032	04/01/2012, 1:30 PM	04/01/2012, 1:30 PM
WindowsUpdate.log	11744 ($INDEX_ALLOC...	16033	04/01/2012, 1:30 PM	04/01/2012, 1:30 PM
WINDOW~1.LOG	11864 ($INDEX_ALLOC...	16033	04/01/2012, 1:30 PM	04/01/2012, 1:30 PM
WINDOW~1.MAN	11976 ($INDEX_ALLOC...	16032	04/01/2012, 1:30 PM	04/01/2012, 1:30 PM
winsxs	12088 ($INDEX_ALLOC...	3757	13/07/2009, 8:20 PM	04/01/2012, 1:29 PM
symbols	12352 ($INDEX_ALLOC...	68599	05/01/2012, 11:08 AM	05/01/2012, 11:08 AM
system	12448 ($INDEX_ALLOC...	2373	13/07/2009, 8:20 PM	13/07/2009, 7:36 PM

The $I30 entries can be copied to clipboard, or exported to a text file from the right-click menu.

4.22 Email Viewer

The Email Viewer provides a simple yet powerful interface for browsing and analyzing e-mail messages across multiple e-mail files.



☑ From ☑ To / Cc / Bcc ☑ Subject □ Body Start □ 26-May-2017 End □ 26-May-2017

From	Subject	Date
JobSeeker Weekly <ne...	Instantly Search & Apply On All Top Career Sites	2010-03-15, 14:35:23
Omaha Steaks Stores <...	Get Your FREE Ham in Time for Easter	2010-03-15, 23:00:03
Abs Diet Online <Mens...	Now is the time to get your 6-pack abs	2010-03-15, 23:39:18
Wix Team <newsletter...	[WIX.COM] Upgrade Your Site For Just $0.99	2010-03-16, 2:45:51
The Career News <new...	How to Conduct an Efficient Job Search	2010-03-16, 15:48:07

How to Conduct an Efficient Job Search

2010-03-16, 15:48:07

From: The Career News <newsletter@thecareernews.com>
To: randy@randyleebaker.com
Cc:
Bcc:

March 15, 2010 **The Career News** Vol. 10, Issue 11

The Latest News, Tips and Tools For Your Career

Make each minute count in your job search efforts

Abridged: The Wall Street Journal

487 item(s)

OSForensics Email Viewer

The left pane provides a hierarchical view of all devices added to the case. Clicking on a node shall load its contents into the right pane.

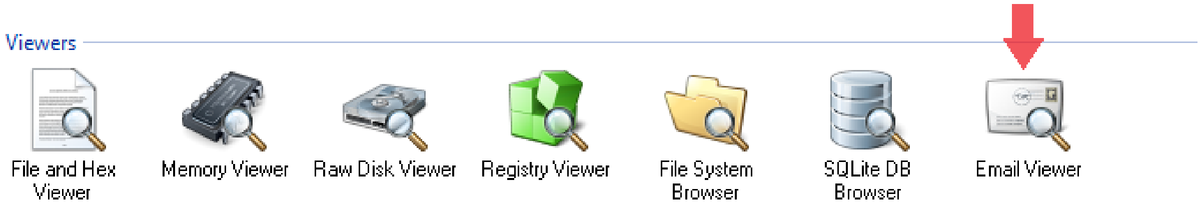
Understanding the Email Viewer

The table below summarizes the main components of the Email Viewer

Component	Description
E-mail Hierarchical View	Tree organization of all e-mail files currently being browsed. Selecting a folder will display the list of e-mail it contains.
E-mail List	List view of the e-mail contained in the current folder. Selecting an e-mail will display the e-mail contents in the Preview Pane.
E-mail Preview Pane	Displays the e-mail contents of the currently selected e-mail
E-mail Filter	Filters the list of e-mail to those that match the specified criteria

Opening the Email Viewer

The Email Viewer is accessible via the "Email Viewer" icon in the "Viewers" group under the Start tab. Once opened, the user is prompted to select an e-mail file to view.



Usage

Search

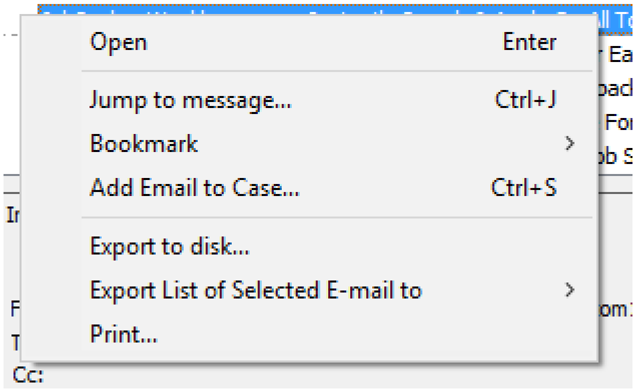
To search for e-mail messages that contain a particular text, enter a search expression in the search bar, specify any additional search parameters and click 'Search'. To use Regular Expressions, check the 'Use RegEx' checkbox. Additionally, e-mail messages can be filtered by when they were sent/ received.

To remove the search results, click 'Clear Search'.

Right-click Menu

The right-click menu integrates the E-mail Viewer with OSForensics' analysis tools.

E-mail List Menu


Open Enter
Jump to message... Ctrl+J
Bookmark >
Add Email to Case... Ctrl+S
Export to disk...
Export List of Selected E-mail to >
Print...
Cc:

Open
Opens the message in a separate window.

Jump to message
Jump to a message specified by a message ID.

Bookmark

Green

Add/remove selected e-mail from the list of Green bookmarks. *Keyboard shortcut: Ctrl+G*

Yellow
Add/remove selected e-mail from the list of Yellow bookmarks. *Keyboard shortcut: Ctrl+Y*

Red
Add/remove selected e-mail from the list of Red bookmarks. *Keyboard shortcut: Ctrl+R*

Add Email to Case...
Opens a dialog prompting the user to enter details for the selected e-mail to add to the case. *Keyboard Shortcut: Ctrl+S*

Export to disk...
Exports the selected e-mail to HTML and saves to disk.

Export List of Selected E-mail to

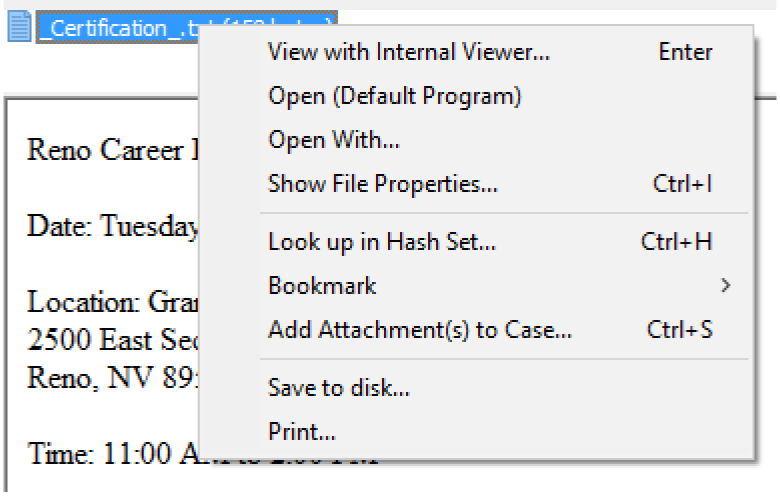
txt
Saves the list of selected e-mail to a text file

html
Saves the list of selected e-mail to an html file

CSV
Saves the list of selected e-mail to a CSV file

Print...
Prints the e-mail

Attachment Menu



View with Interval Viewer...
Opens the file with OSForensics Viewer to perform a more thorough analysis. *Keyboard shortcut: Enter*

Open (Default Program)
Opens the file with the default program. *Keyboard shortcut: Shift+Enter*

Open With...
Allows the user to select the program to open the file

Show File Properties...
Opens the file with OSForensics Viewer in File Info mode. *Keyboard shortcut: Ctrl+I*

Look up in Hash Set...
Verify whether the selected attachments are in a hash set in the active database. See Hash Set Lookup. *Keyboard shortcut: Ctrl+H*

Bookmark

Green
Add/remove selected attachment(s) from the list of Green bookmarks. *Keyboard shortcut: Ctrl+G*

Yellow
Add/remove selected attachment(s) from the list of Yellow bookmarks. *Keyboard shortcut: Ctrl+Y*

Red
Add/remove selected attachment(s) from the list of Red bookmarks. *Keyboard shortcut: Ctrl+R*

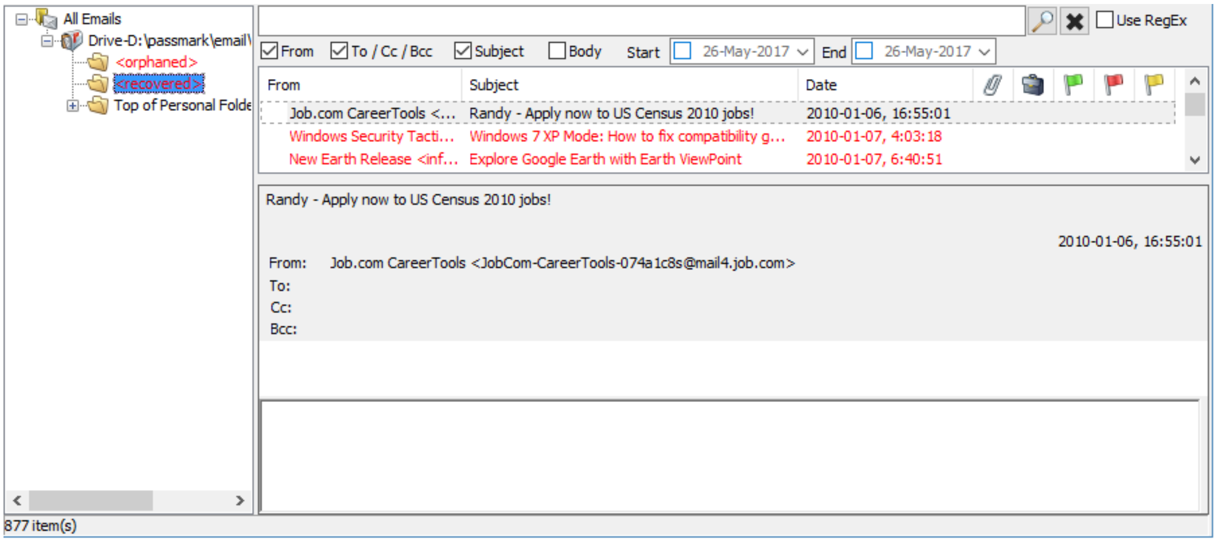
Add Attachment(s) to Case...
Opens a dialog prompting the user to enter details for the selected attachment(s) to add to the case. *Keyboard Shortcut: Ctrl+S*

Save to disk...
Saves the selected attachment(s) to a location on disk

Print...
Prints the attachment (if applicable)

Deleted E-mails

The Email Viewer supports recovering deleted and orphaned e-mails within PST files. To scan for deleted/orphaned e-mails, click on either the "<orphaned>" or "<recovered>" folders after loading the PST file.



All Emails
Drive-D:\passmark\email\
<orphaned>
<recovered>
Top of Personal Folde

☑ From ☑ To / Cc / Bcc ☑ Subject □ Body Start □ 26-May-2017 End □ 26-May-2017 □ Use RegEx

From	Subject	Date
Job.com CareerTools <...	Randy - Apply now to US Census 2010 jobs!	2010-01-06, 16:55:01
Windows Security Tacti...	Windows 7 XP Mode: How to fix compatibility g...	2010-01-07, 4:03:18
New Earth Release <inf...	Explore Google Earth with Earth ViewPoint	2010-01-07, 6:40:51

Randy - Apply now to US Census 2010 jobs!

2010-01-06, 16:55:01

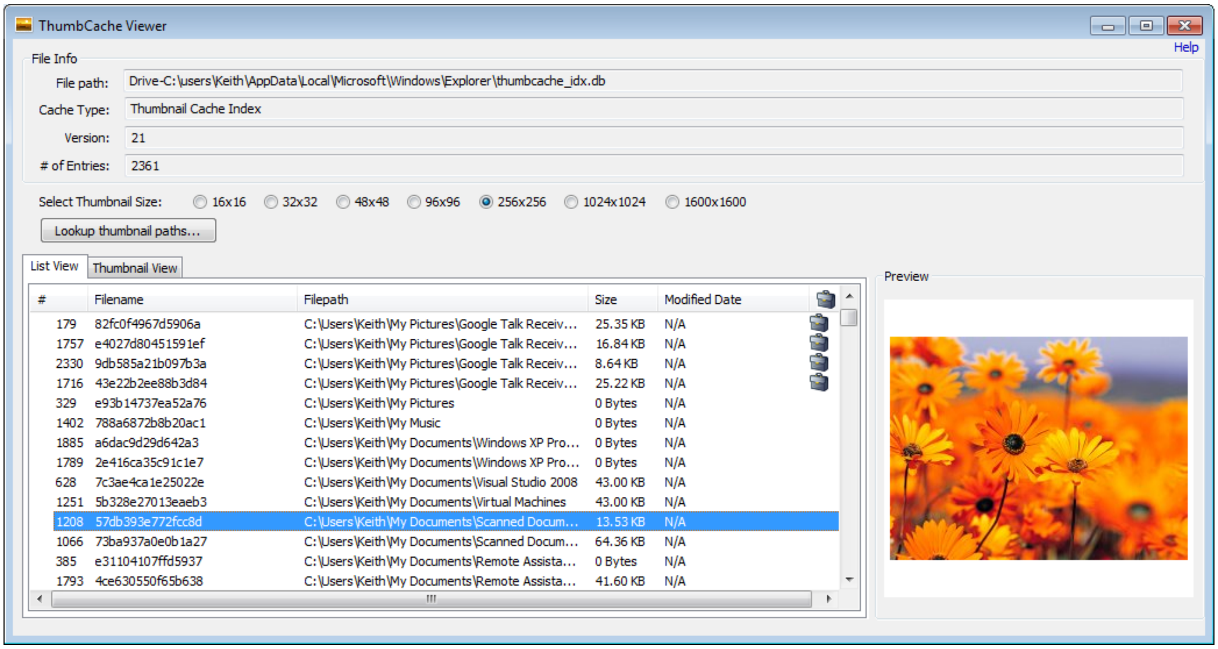
From: Job.com CareerTools <JobCom-CareerTools-074a1c8s@mail4.job.com>
To:
Cc:
Bcc:

877 item(s)

The "<orphaned>" folder contains all e-mail items that do not have a parent folder, possibly due to a corrupted file. The "<recovered>" folder contains all e-mails that have been deleted but the data still remains in the unallocated space of the PST file.

4.23 Thumbnail Cache Viewer

The Thumbnail Cache Viewer is another valuable tool in OSForensics' suite of viewers for locating artifacts of files that may have been deleted on the system. In particular, the Thumbnail Cache Viewer allows the investigator to browse image thumbnails stored in the Window's thumbnail cache database. When a user opens Windows Explorer to browse the contents of folders, Windows automatically saves a thumbnail of the files in the thumbnail cache database for quick viewing at a later time. This can be useful for forensics purposes especially for cases where even though the user has deleted the original image file, the thumbnail of the image still remains in the thumbnail cache.



File Info
File path: Drive-C:\users\Keith\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db
Cache Type: Thumbnail Cache Index
Version: 21
# of Entries: 2361

Select Thumbnail Size: ○ 16x16 ○ 32x32 ○ 48x48 ○ 96x96 ● 256x256 ○ 1024x1024 ○ 1600x1600

#	Filename	Filepath	Size	Modified Date
179	82fc0f4967d5906a	C:\Users\Keith\My Pictures\Google Talk Receiv...	25.35 KB	N/A
1757	e4027d80451591ef	C:\Users\Keith\My Pictures\Google Talk Receiv...	16.84 KB	N/A
2330	9db585a21b097b3a	C:\Users\Keith\My Pictures\Google Talk Receiv...	8.64 KB	N/A
1716	43e22b2ee88b3d84	C:\Users\Keith\My Pictures\Google Talk Receiv...	25.22 KB	N/A
329	e93b14737ea52a76	C:\Users\Keith\My Pictures	0 Bytes	N/A
1402	788a6872b8b20ac1	C:\Users\Keith\My Music	0 Bytes	N/A
1885	a6dac9d29d642a3	C:\Users\Keith\My Documents\Windows XP Pro...	0 Bytes	N/A
1789	2e416ca35c91c1e7	C:\Users\Keith\My Documents\Windows XP Pro...	0 Bytes	N/A
628	7c3ae4ca1e25022e	C:\Users\Keith\My Documents\Visual Studio 2008	43.00 KB	N/A
1251	5b328e27013eaeb3	C:\Users\Keith\My Documents\Virtual Machines	43.00 KB	N/A
1208	57db393e772fcc8d	C:\Users\Keith\My Documents\Scanned Docum...	13.53 KB	N/A
1066	73ba937a0e0b1a27	C:\Users\Keith\My Documents\Scanned Docum...	64.36 KB	N/A
385	e31104107ffd5937	C:\Users\Keith\My Documents\Remote Assista...	0 Bytes	N/A
1793	4ce630550f65b638	C:\Users\Keith\My Documents\Remote Assista...	41.60 KB	N/A

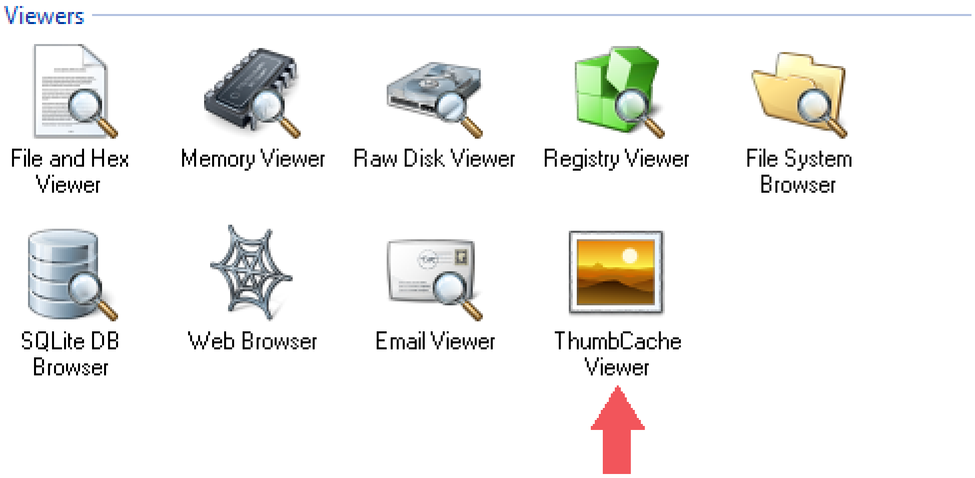
Understanding the Thumbnail Cache Viewer

The table below summarizes the main components of the Thumbnail Cache Viewer

Component	Description
File Info	Displays the details of the thumbnail cache database
List View	Displays a list of thumbnail entries contained in the thumbnail cache database
Thumbnail View	Displays a thumbnail view of the images contained in the thumbnail cache database
Preview Pane	Displays the image of the currently selected thumbnail

Opening the Thumbnail Cache Viewer

The Thumbnail Cache Viewer is accessible via the "ThumbCache Viewer" icon in the "Viewers" group under the Start tab.



Once opened, a list of detected thumbnail cache files are displayed for the selected device. Alternatively, the thumbnail cache file can be manually selected by clicking the 'Browse' button and locating the file itself.

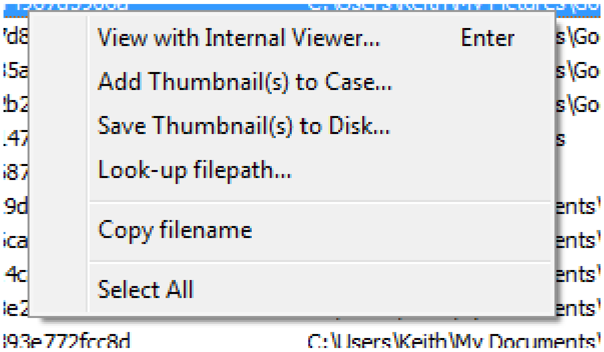
When attempting to open a recognized thumbnail cache file using the internal viewer, the user may be given the option to open the file using the Thumbnail Cache Viewer instead. Recognized thumbnail cache files include the following:

- Thumbs.db
- ehthumbs_vista.db
- ehthumbs.db
- thumbcache_idx.db
- thumbcache_1024.db
- thumbcache_256.db
- thumbcache_96.db
- thumbcache_32.db

Usage

Double-clicking or pressing 'Enter' on a thumbnail opens the internal viewer.

Right-click Menu


View with Internal Viewer... Enter
Add Thumbnail(s) to Case...
Save Thumbnail(s) to Disk...
Look-up filepath...
Copy filename
Select All

View with Internal Viewer...
Opens the thumbnail with OSForensics Viewer to perform a more thorough analysis. *Keyboard shortcut: Enter*

Add Thumbnail(s) to Case...
Opens a dialog prompting the user to enter details for the selected thumbnail(s) to add to the case

Save Thumbnail(s) to Disk...
Prompts the user to enter a location on disk to save the selected thumbnail(s) on disk

Look-up filepath...
Attempt to look-up the filepath of the select thumbnail(s) from a Windows Search database.

Copy filename
Copies the filename as text to the clipboard

Select All
Select all of the thumbnails in the thumbnail cache file

Additional Info

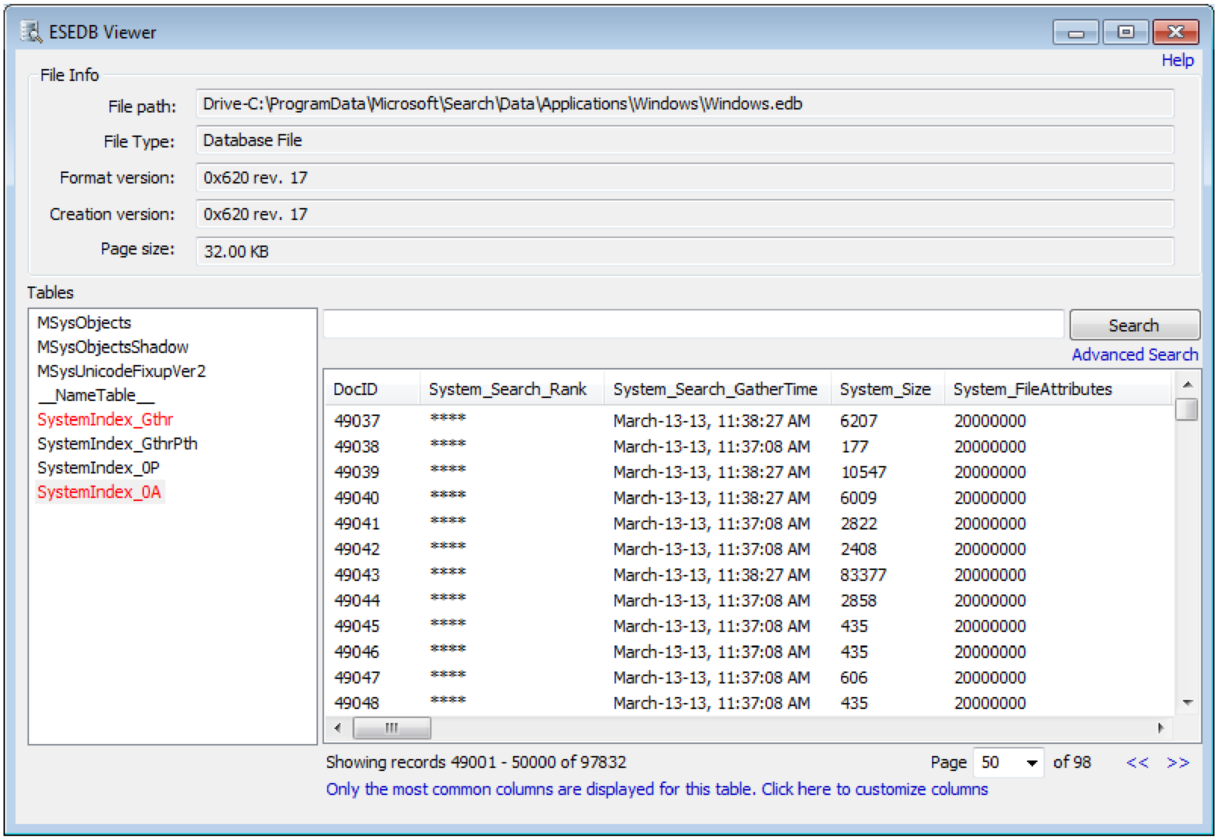
Filepath Look-up

Thumbnail caches, by itself, do not contain any filepath information about the individual thumbnail entries. However, it does include a hash for each thumbnail entry that can be mapped to its corresponding filepath. This filepath mapping can be found in the Windows Search database. By performing a filepath look-up, the Thumbnail Cache Viewer can automatically try to find the matching filepath in the Windows Search database. The corresponding filepath is then displayed beside the thumbnail entry in the table.

4.24 ESE Database Viewer

The ESE Database Viewer provides visibility into databases stored in the Extensible Storage Engine (ESE) file format. The ESEDB format, in particular, is used by several Microsoft applications that store data with potential forensics value, including the following:

- Windows (Desktop) Search
- Windows (Vista) Mail
- Microsoft Exchange Server



File Info

File path: Drive-C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb
File Type: Database File
Format version: 0x620 rev. 17
Creation version: 0x620 rev. 17
Page size: 32.00 KB

Tables

- MSysObjects
- MSysObjectsShadow
- MSysUnicodeFixupVer2
- __NameTable__
- SystemIndex_Gthr
- SystemIndex_GthrPth
- SystemIndex_0P
- SystemIndex_0A

DocID	System_Search_Rank	System_Search_GatherTime	System_Size	System_FileAttributes
49037	****	March-13-13, 11:38:27 AM	6207	20000000
49038	****	March-13-13, 11:37:08 AM	177	20000000
49039	****	March-13-13, 11:38:27 AM	10547	20000000
49040	****	March-13-13, 11:38:27 AM	6009	20000000
49041	****	March-13-13, 11:37:08 AM	2822	20000000
49042	****	March-13-13, 11:37:08 AM	2408	20000000
49043	****	March-13-13, 11:38:27 AM	83377	20000000
49044	****	March-13-13, 11:37:08 AM	2858	20000000
49045	****	March-13-13, 11:37:08 AM	435	20000000
49046	****	March-13-13, 11:37:08 AM	435	20000000
49047	****	March-13-13, 11:37:08 AM	606	20000000
49048	****	March-13-13, 11:37:08 AM	435	20000000

Showing records 49001 - 50000 of 97832 Page 50 of 98

Only the most common columns are displayed for this table. Click here to customize columns

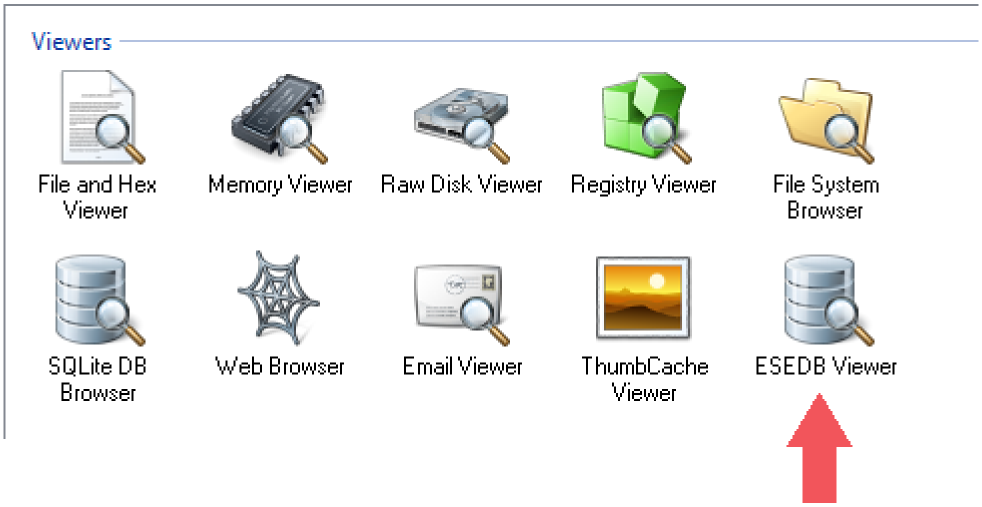
Understanding the ESE Database Viewer

The table below summarizes the main components of the ESE Database Viewer

Component	Description
File Info	Displays the details of the ESE database
Tables List	Displays a list of table contained in the database
Records List	Displays a list of records contained in the selected table

Opening the ESE Database Viewer

The ESE Database Viewer can be accessed via the "ESEDB Viewer" icon in the "Viewers" group under the Start tab.



Once opened, a list of known database files are displayed for the selected device. Alternatively, the database file can be manually selected by clicking the 'Browse' button and locating the file itself.

When attempting to open a file with a known ESE database file extension using the internal viewer, the user may be given the option to open the file using the ESE Database Viewer instead.

Usage

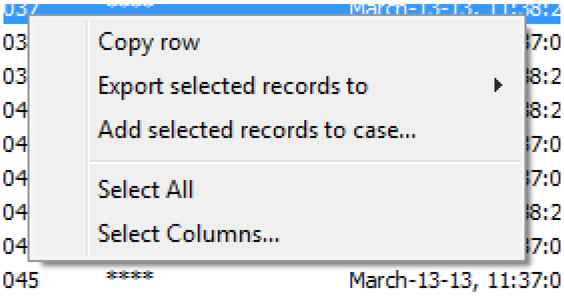
Once the database file is opened, the Tables list is populated with the tables contained in the database. To view the records contained in a particular table, select a table from the Tables list. Known tables with useful data are highlighted in red.

Note: For some known tables, only a subset of the most common columns are displayed (due to having a large number of columns). This message is shown on the bottom of the viewer. Clicking on the message allows for selecting the columns to display.

Search

To perform a simple text search of all records in the table, enter a search term and click 'Search'. This will locate records that contain the specified text as it is displayed on the table. A more comprehensive search can be performed based on the data type (eg. number, boolean, dates) of the fields by clicking on Advanced Search...

Right-click Menu


Copy row
Export selected records to
Add selected records to case...
Select All
Select Columns...
045 **** March-13-13, 11:37:0

Copy row
Copies the entire row as text to the clipboard

Export selected records to

txt
Saves the list of selected records to a text file

html
Saves the list of selected records to an html file

CSV
Saves the list of selected records to a CSV file

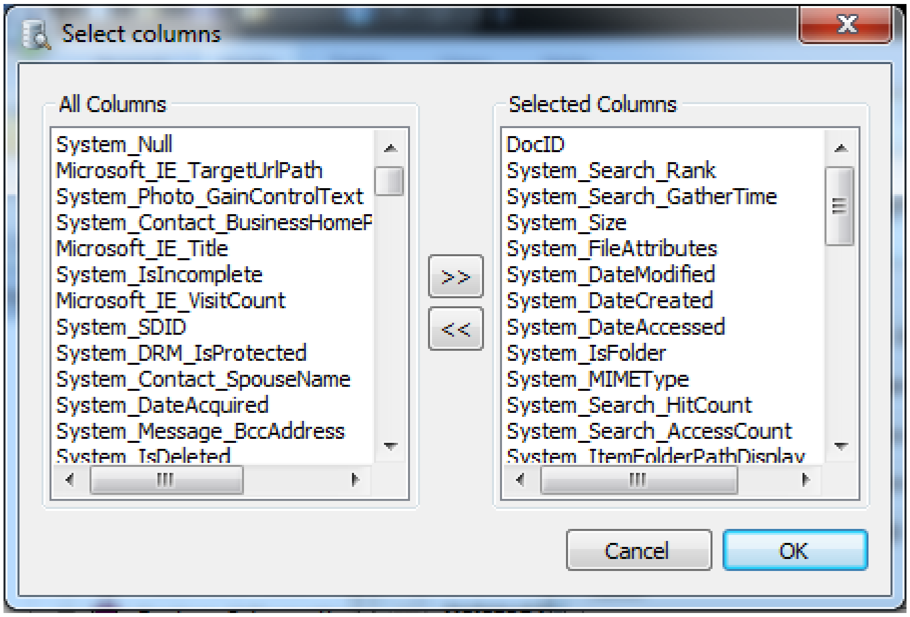
Add selected records to case...
Adds the list of selected records to the case as a CSV file

Select All
Select all of the records in the ESE Database file

Select Columns...
Select a subset of the columns to display

Selecting Columns

By selecting a subset of the columns to display, the user can focus on viewing the important fields of a a database record and ignoring the less relevant ones. To specify the list of columns to display, move the appropriate columns to the 'Selected Columns' list, while leaving the columns to be excluded in the 'All Columns' list.



All Columns:

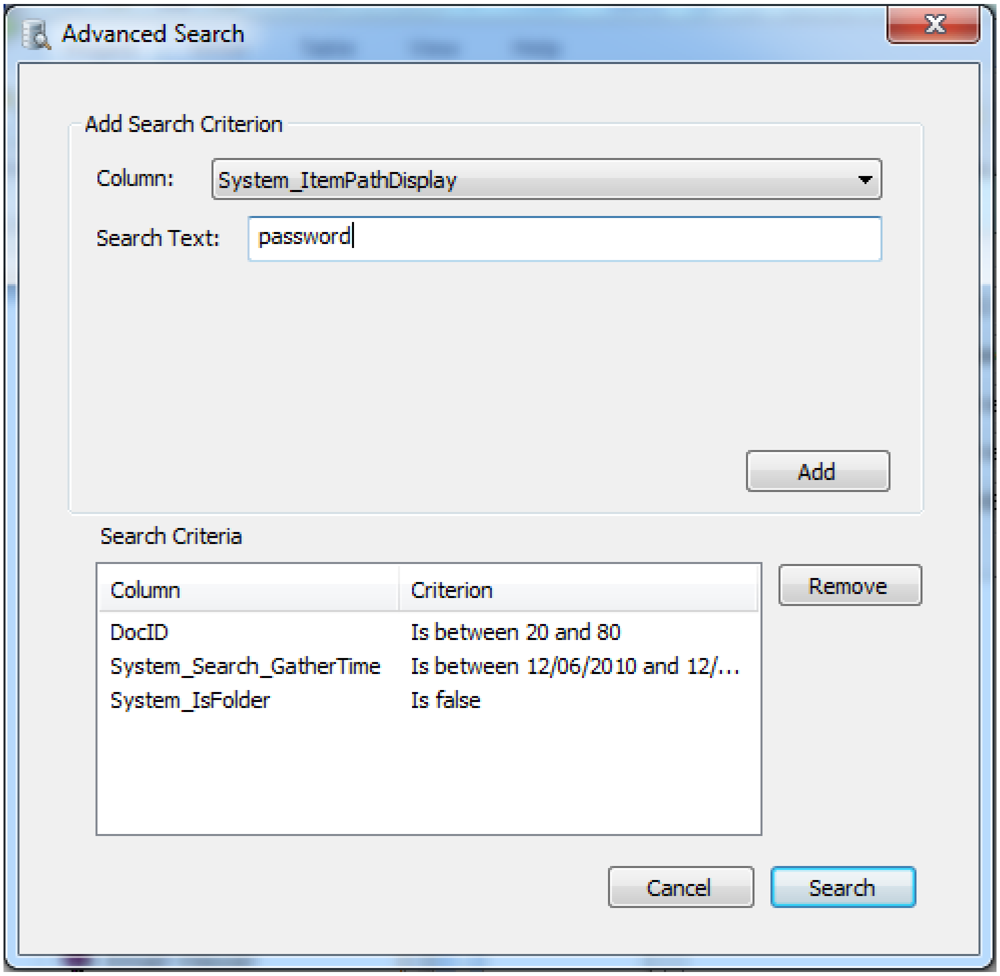
System_Null
Microsoft_IE_TargetUrlPath
System_Photo_GainControlText
System_Contact_BusinessHomeF
Microsoft_IE_Title
System_IsIncomplete
Microsoft_IE_VisitCount
System_SDID
System_DRM_IsProtected
System_Contact_SpouseName
System_DateAcquired
System_Message_BccAddress
System_IsDeleted

Selected Columns:

DocID
System_Search_Rank
System_Search_GatherTime
System_Size
System_FileAttributes
System_DateModified
System_DateCreated
System_DateAccessed
System_IsFolder
System_MIMEType
System_Search_HitCount
System_Search_AccessCount
System_ItemFolderPathDisplay

4.24.1 ESE Database Advanced Search

The ESE Database Advanced Search dialog allows the user to perform a more powerful search of database records based on one or more data type specific criteria.



Column: System_ItemPathDisplay

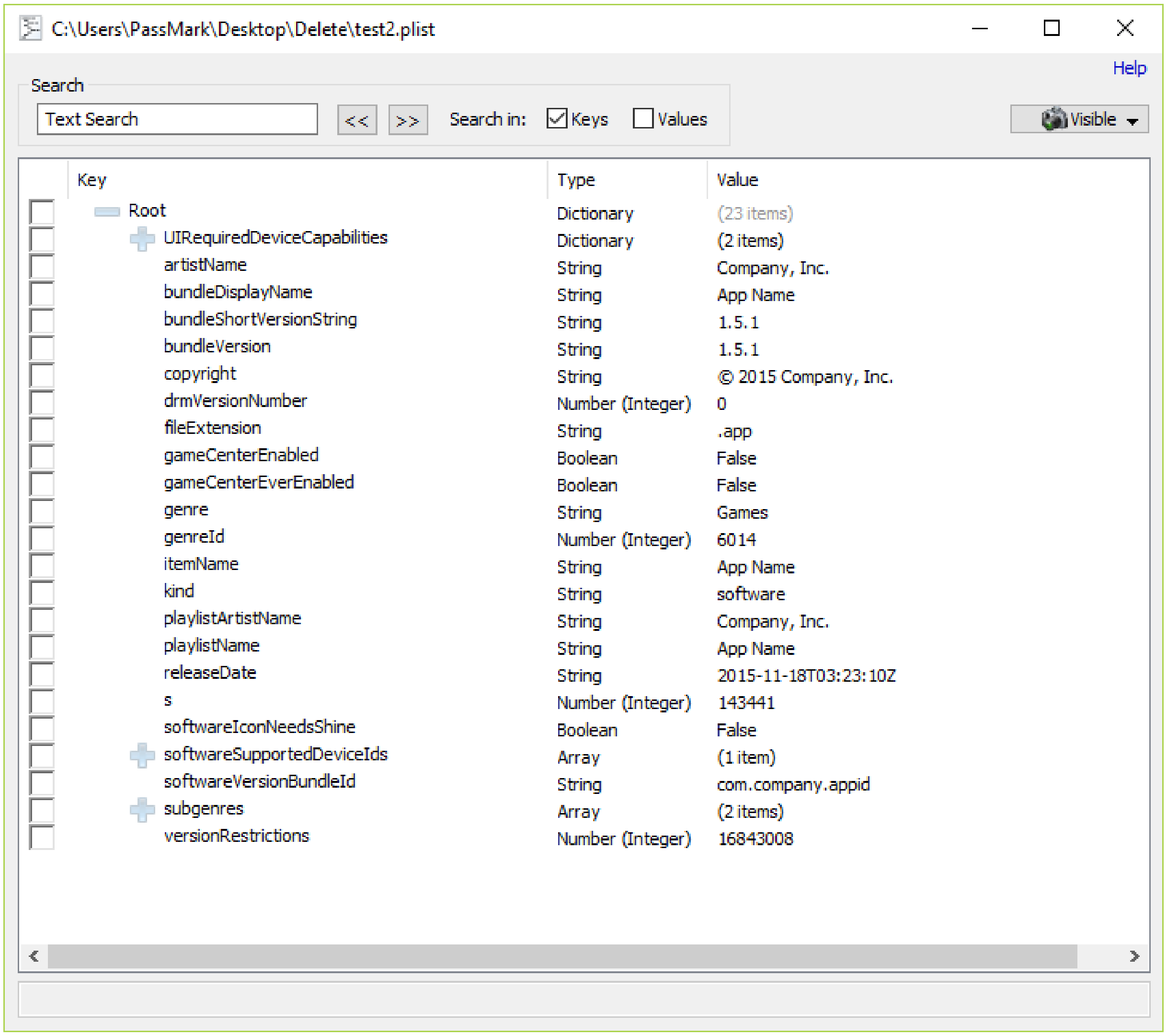
Search Text: password

Column	Criterion
DocID	Is between 20 and 80
System_Search_GatherTime	Is between 12/06/2010 and 12/...
System_IsFolder	Is false

To add a criterion, first select a column from the list. Based on the selected column's data type (eg. integer, date, boolean, text), a condition that must be satisfied by the record value can be specified. Once the condition has been specified, click 'Add' to add to the search criteria. To perform the search using the specified criteria, click 'Search' to perform the search. Once the search has been completed, the results are displayed in the ESE Database Viewer.

4.25 Plist Viewer

View the contents of Plist (property list) files which are commonly used by OSX and iOS to store settings and properties. Plist files typically have the extension of ".plist". The Plist Viewer within OSForensics is able to display both binaries and XML formatted plist files.



C:\Users\PassMark\Desktop\Delete\test2.plist

Search: Text Search

Search in: ☑ Keys ☐ Values

Key	Type	Value
Root	Dictionary	(23 items)
UIRequiredDeviceCapabilities	Dictionary	(2 items)
artistName	String	Company, Inc.
bundleDisplayName	String	App Name
bundleShortVersionString	String	1.5.1
bundleVersion	String	1.5.1
copyright	String	© 2015 Company, Inc.
drmVersionNumber	Number (Integer)	0
fileExtension	String	.app
gameCenterEnabled	Boolean	False
gameCenterEverEnabled	Boolean	False
genre	String	Games
genreId	Number (Integer)	6014
itemName	String	App Name
kind	String	software
playlistArtistName	String	Company, Inc.
playlistName	String	App Name
releaseDate	String	2015-11-18T03:23:10Z
s	Number (Integer)	143441
softwareIconNeedsShine	Boolean	False
softwareSupportedDeviceIds	Array	(1 item)
softwareVersionBundleId	String	com.company.appid
subgenres	Array	(2 items)
versionRestrictions	Number (Integer)	16843008

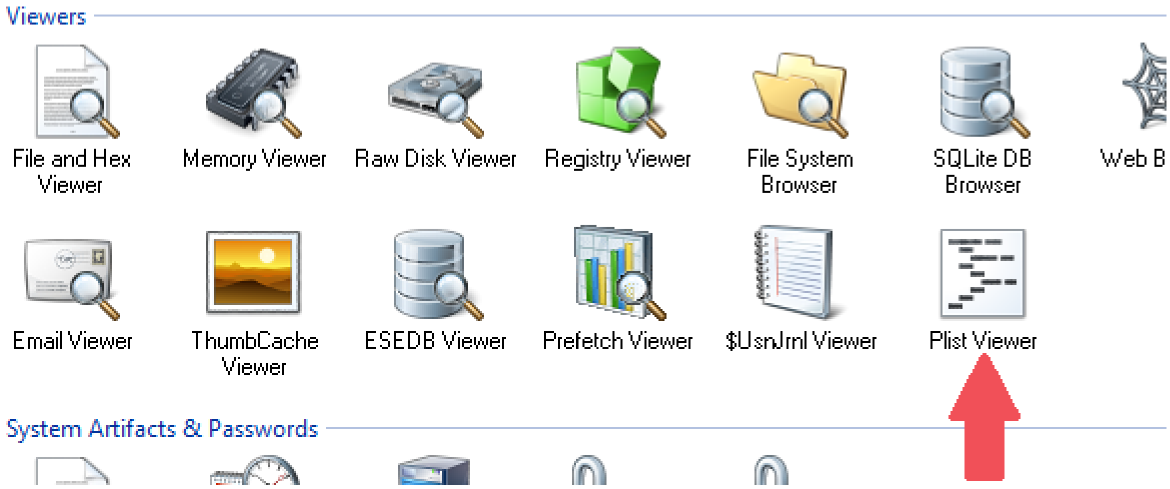
Understanding the Plist Viewer

The table below summarizes the main components of the Plist Viewer

Component	Description
Window Title	Displays the current file opened in the Plist Viewer.
Search	Controls to allow you to search the current Plist file.
Screen Capture	Screen Capture controls.
Records List	Displays a list of records contained in the Plist file.
Status Bar	Displays the path information on the current item selected.

Opening the Plist Viewer

The Plist Viewer can be accessed via the "Plist Viewer" icon in the "Viewers" group under the Start tab.



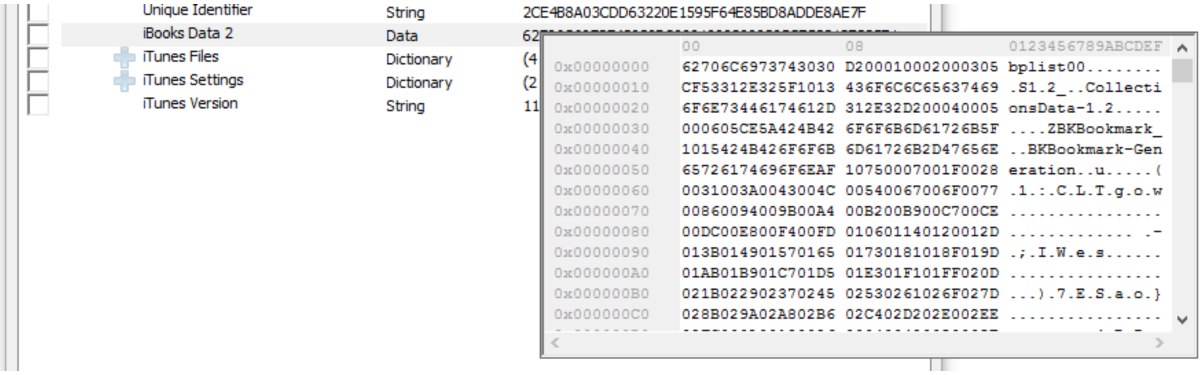
Once opened, a file selection dialog will allow you to select a file from devices added to case or on the current system itself.

When attempting to open a file with a known Plist file extension using the internal viewer, the user may be given the option to open the file using the Plist Viewer instead.

Usage

Once the plist file is opened, the list is populated with the contents contained in the property list. The four columns of the Plist viewer are Checkbox (for selecting/unselecting), Key, Key Type, and Key Value. The possible Key Types are: String, Boolean, Date, Data (binary), Number (Integer or Real) and collection types (Dictionary or Array). For collection types, it will display the number of immediate child items it contains for the Key Value. For a Key of Array type, the child items' keys does not actually have names, but are automatically given Key names of the format "Item n" where n is the index of the item starting with zero.

Items of type Data, the Key Value will only show the first 64 hex character representation of the binary data. A single left click will open a quick data preview window. A double left click will open the data in the internal viewer window.



□	Unique Identifier	String	2CE4B8A03CDD63220E1595F64E85BD8ADDE8AE7F
□	iBooks Data 2	Data	62
□	iTunes Files	Dictionary	(4
□	iTunes Settings	Dictionary	(2
□	iTunes Version	String	11

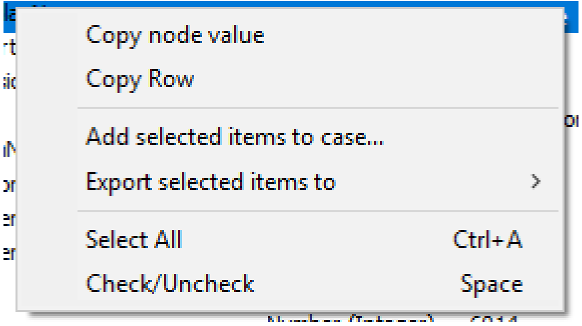
```
            00               08               0123456789ABCDEF
0x00000000  62706C6973743030 D200010002000305 bplist00........
0x00000010  CF53312E325F1013 436F6C6C65637469 .S1.2_..Collecti
0x00000020  6F6E73446174612D 312E32D200040005 onsData-1.2.....
0x00000030  000605CE5A424B42 6F6F6B6D61726B5F ....ZBKBookmark_
0x00000040  1015424B426F6F6B 6D61726B2D47656E ..BKBookmark-Gen
0x00000050  65726174696F6EAF 10750007001F0028 eration..u.....(
0x00000060  0031003A0043004C 00540067006F0077 .1.:.C.L.T.g.o.w
0x00000070  00860094009B00A4 00B200B900C700CE ................
0x00000080  00DC00E800F400FD 010601140120012D .............. .-
0x00000090  013B014901570165 01730181018F019D .;.I.W.e.s......
0x000000A0  01AB01B901C701D5 01E301F101FF020D ................
0x000000B0  021B022902370245 02530261026F027D ...).7.E.S.a.o.}
0x000000C0  028B029A02A802B6 02C402D202E002EE ................
```

When checking an item with child elements, the children will also be selected. There are three visual states for the checkbox: checked, unchecked, mixed-checked. Selecting a child item will automatically check the parent item. Parent items with some children selected and unselected will display the mixed-checked checkbox.

Search

To perform a simple text search of all records in the list, enter a search term and click 'Search'. The default will search the for matching text in the Keys. To search for text in the Values, check the Values checkbox. Note: Text search will not search elements with Data Key Types.

Right-click Menu



Copy node value
Copy the Key's Value to the clipboard

Copy Row
Copies the entire row as text to the clipboard

Add selected items to case...
Adds the list of selected records to the case as a CSV file

Export selected records to

txt
Saves the list of selected records to a text file

html
Saves the list of selected records to an html file

CSV
Saves the list of selected records to a CSV file

XML Plist
Saves the list of selected records to a XML Plist file

Select All
Select all of the records in the plist file

Check/Uncheck
Check/Uncheck all selected items.

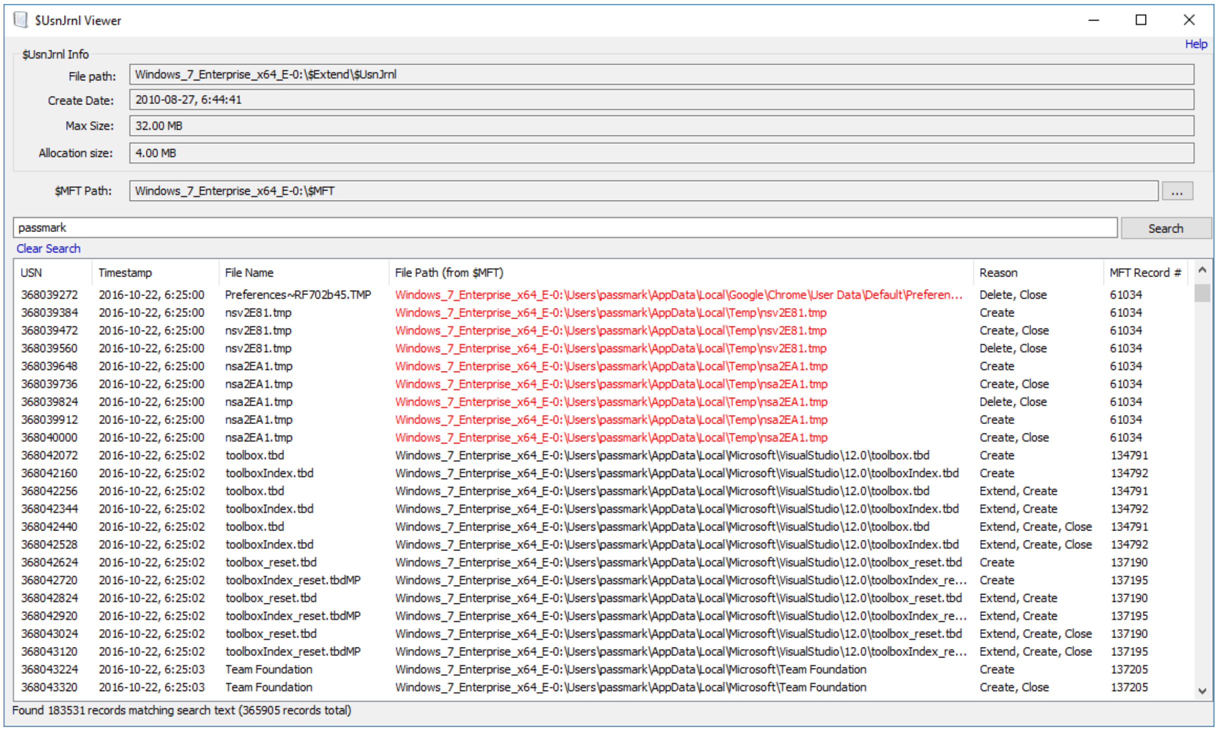
4.26 $UsnJrnl Viewer

The $UsnJrnl is a special file in NTFS that tracks the changes to files/directories made to the volume, usually several days to a week. This information is useful for identifying suspect files (eg. malware) that no longer exist in the file system or $MFT. Since Windows Vista, $UsnJrnl logging is turned on by default.

The USN journal is updated whenever changes to files and directories are made to a volume including:

- File Metadata changes
- File Creations
- File Deletions
- File Overwrites

It should be noted that the journal records do not indicate how the file contents have changed, rather whether it has been created, modified or deleted.



File path: Windows_7_Enterprise_x64_E-0:\$Extend\$UsnJrnl
Create Date: 2010-08-27, 6:44:41
Max Size: 32.00 MB
Allocation size: 4.00 MB

$MFT Path: Windows_7_Enterprise_x64_E-0:\$MFT

passmark

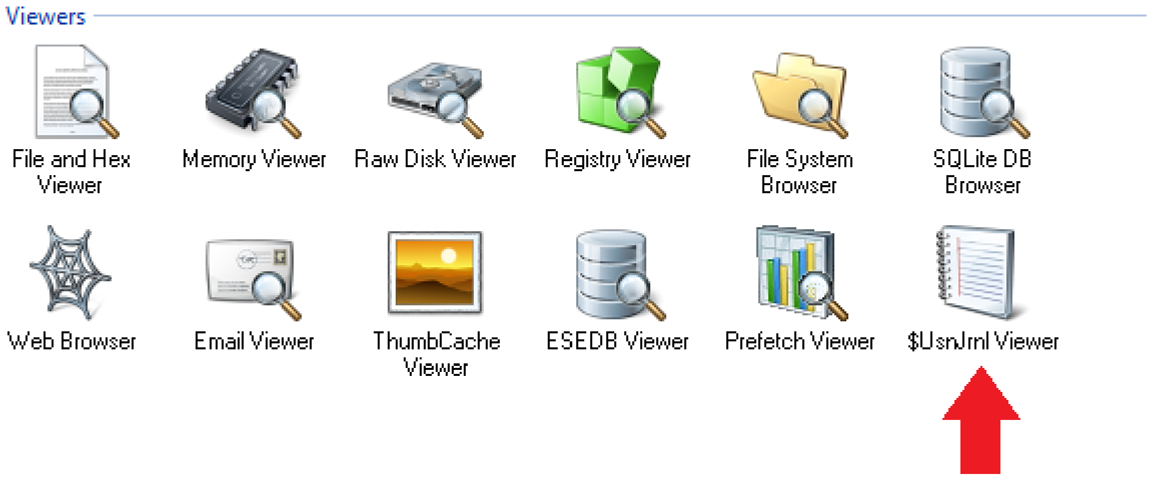
USN	Timestamp	File Name	File Path (from $MFT)	Reason	MFT Record #
368039272	2016-10-22, 6:25:00	Preferences~RF702b45.TMP	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Google\Chrome\User Data\Default\Preferen...	Delete, Close	61034
368039384	2016-10-22, 6:25:00	nsv2E81.tmp	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Temp\nsv2E81.tmp	Create	61034
368039472	2016-10-22, 6:25:00	nsv2E81.tmp	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Temp\nsv2E81.tmp	Create, Close	61034
368039560	2016-10-22, 6:25:00	nsv2E81.tmp	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Temp\nsv2E81.tmp	Delete, Close	61034
368039648	2016-10-22, 6:25:00	nsa2EA1.tmp	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Temp\nsa2EA1.tmp	Create	61034
368039736	2016-10-22, 6:25:00	nsa2EA1.tmp	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Temp\nsa2EA1.tmp	Create, Close	61034
368039824	2016-10-22, 6:25:00	nsa2EA1.tmp	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Temp\nsa2EA1.tmp	Delete, Close	61034
368039912	2016-10-22, 6:25:00	nsa2EA1.tmp	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Temp\nsa2EA1.tmp	Create	61034
368040000	2016-10-22, 6:25:00	nsa2EA1.tmp	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Temp\nsa2EA1.tmp	Create, Close	61034
368042072	2016-10-22, 6:25:02	toolbox.tbd	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Microsoft\VisualStudio\12.0\toolbox.tbd	Create	134791
368042160	2016-10-22, 6:25:02	toolboxIndex.tbd	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Microsoft\VisualStudio\12.0\toolboxIndex.tbd	Create	134792
368042256	2016-10-22, 6:25:02	toolbox.tbd	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Microsoft\VisualStudio\12.0\toolbox.tbd	Extend, Create	134791
368042344	2016-10-22, 6:25:02	toolboxIndex.tbd	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Microsoft\VisualStudio\12.0\toolboxIndex.tbd	Extend, Create	134792
368042440	2016-10-22, 6:25:02	toolbox.tbd	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Microsoft\VisualStudio\12.0\toolbox.tbd	Extend, Create, Close	134791
368042528	2016-10-22, 6:25:02	toolboxIndex.tbd	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Microsoft\VisualStudio\12.0\toolboxIndex.tbd	Extend, Create, Close	134792
368042624	2016-10-22, 6:25:02	toolbox_reset.tbd	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Microsoft\VisualStudio\12.0\toolbox_reset.tbd	Create	137190
368042720	2016-10-22, 6:25:02	toolboxIndex_reset.tbdMP	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Microsoft\VisualStudio\12.0\toolboxIndex_re...	Create	137195
368042824	2016-10-22, 6:25:02	toolbox_reset.tbd	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Microsoft\VisualStudio\12.0\toolbox_reset.tbd	Extend, Create	137190
368042920	2016-10-22, 6:25:02	toolboxIndex_reset.tbdMP	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Microsoft\VisualStudio\12.0\toolboxIndex_re...	Extend, Create	137195
368043024	2016-10-22, 6:25:02	toolbox_reset.tbd	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Microsoft\VisualStudio\12.0\toolbox_reset.tbd	Extend, Create, Close	137190
368043120	2016-10-22, 6:25:02	toolboxIndex_reset.tbdMP	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Microsoft\VisualStudio\12.0\toolboxIndex_re...	Extend, Create, Close	137195
368043224	2016-10-22, 6:25:03	Team Foundation	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Microsoft\Team Foundation	Create	137205
368043320	2016-10-22, 6:25:03	Team Foundation	Windows_7_Enterprise_x64_E-0:\Users\passmark\AppData\Local\Microsoft\Team Foundation	Create, Close	137205

Found 183531 records matching search text (365905 records total)

The $UsnJrnl Viewer displays the records of the changes that were made to each file in a volume within a specific time period.

Opening the $UsnJrnl Viewer

The $UsnJrnl Viewer can be accessed via the "$UsnJrnl Viewer" icon in the "Viewers" group under the Start tab.



Once opened, the location of $UsnJrnl file is displayed for the selected device, if exists. Alternatively, the $UsnJrnl file can be manually selected by clicking the 'Browse' button and locating the file itself. The file can either be the $UsnJrnl file itself or a separate file containing the extracted $UsnJrnl:$J stream.

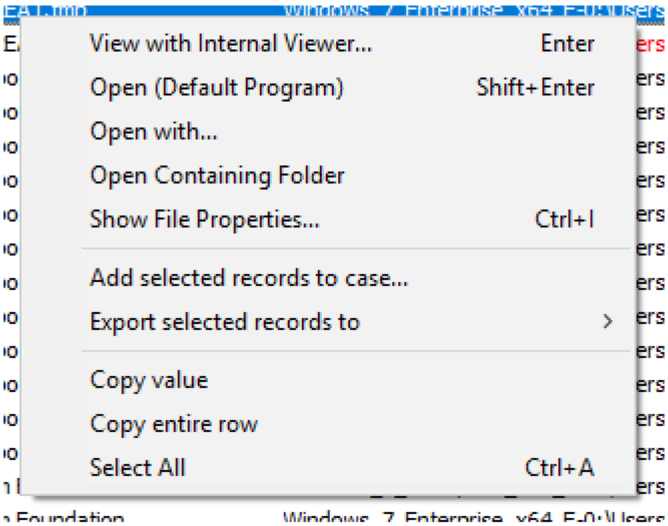
Usage

Once the $UsnJrnl file is opened, the table is populated with the list of records contained in the $UsnJrnl file. If the $MFT file exists on the drive's root directory, it shall be automatically parsed to determine the full path of the file referenced in each record. Otherwise, the location of the $MFT file can be manually specified.

Search

To perform a simple text search of all records in the table, enter a search term and click 'Search'. This will locate records that contain the specified text as it is displayed on the table.

Right-click Menu


View with Internal Viewer... Enter
Open (Default Program) Shift+Enter
Open with...
Open Containing Folder
Show File Properties... Ctrl+I
Add selected records to case...
Export selected records to
Copy value
Copy entire row
Select All Ctrl+A

View with Interval Viewer...
Opens the file with OSForensics Viewer to perform a more thorough analysis. *Keyboard shortcut: Enter*

Open (Default Program)
Opens the file with the default program. *Keyboard shortcut: Shift+Enter*

Open With...
Allows the user to select the program to open the file

Open Containing Folder
Opens the folder than contains the file

Show File Properties...
Opens the file with OSForensics Viewer in File Info mode. *Keyboard shortcut: Ctrl+I*

Add selected records to case...
Adds the list of selected records to the case as a CSV file

Export selected records to

txt
Saves the list of selected records to a text file

html
Saves the list of selected records to an html file

CSV
Saves the list of selected records to a CSV file

Copy value
Copies the cell as text to the clipboard

Copy row
Copies the entire row as text to the clipboard

Select All
Select all of the records in the table

4.27 Installing to a USB Drive or an Optical Disk

It is possible to install OSForensics onto a USB drive or CD/DVD/BD such that no installation is required on the test system. This can be useful in a number of scenarios, such as field analysis without installing OSForensics on the test system.

When OSForensics is ran from a removable drive when installed this way, the default directory for users files is the OSForensics directory, rather than the normal default directory of the users Document directory.

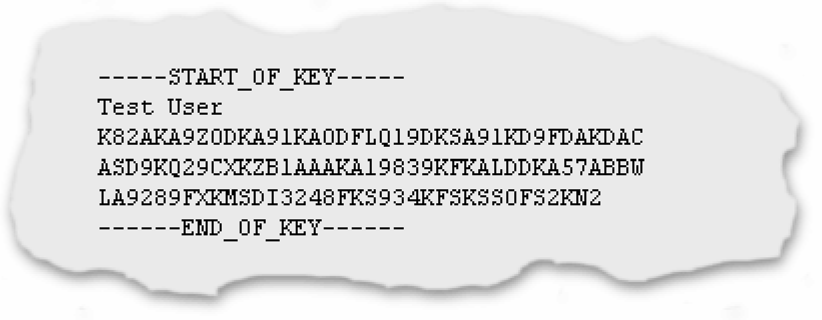
Installing OSForensics to a USB drive

This installation process can be performed for a USB drive installation (any writable drive) using the menu option "Install to USB".

From the "Install OSForensics to a USB drive" Window, you need to specify:

1. The USB drive and directory you want to install OSForensics to. For example, "F:\OSForensics". OSForensics will create the directory if it does not exist.
2. The type of installation. If you have a license key, then select Licensed, otherwise select Evaluation for a trial period.
3. If you selected a "Licensed" installation type, then enter the Username/Key;

Select the entire key, including the -----START_OF_KEY----- and -----END_OF_KEY----- flags.



```
-----START_OF_KEY-----
Test User
K82AKA9Z0DKA91KA0DFLQ19DKSA91KD9FDAKDAC
ASD9KQ29CXKZB1AAAKA19839KFKALDDKA57ABBW
LA9289FXKMSDI3248FKS934KFSKSS0FS2KN2
------END_OF_KEY------
```

Copy and paste this key into the username and key field.

When you select install, OSForensics will create the directory on the USB drive (e.g. F:\OSForensics), copy all of the files from the OSForensics directory (e.g. C:\Program Files\OSForensics) to the USB drive (e.g. F:\OSForensics) and install the license information onto the USB drive.

Installing OSForensics to an optical disk

To install OSForensics on an optical disk (CD/DVD/BD) follow the process above, but specify a writable temporary directory in step 1 (e.g. C:\OSForensics). On completing the installation to the temporary directory, burn the created directory to the optical disk.

Creating a bootable copy of OSForensics

OSForensics can be configured to start directly from a bootable CD/DVD or USB Flash Drive (UFD), rather than being started from within a machine's operating system. This can be useful when the machine you need to run OSForensics on has an invalid, incompatible or otherwise non-working operating system. To run OSForensics on a machine without a valid operating system, you will need to set up a “Pre-install environment” that allows Microsoft Windows to be booted from a CD/DVD or UFD.

PassMark Software has written a document, Building a Bootable Version of OSForensics using WinPE, to help guide you through setting up a Microsoft Window Pre-install 3.0 environment (WinPE) environment which includes both Windows and OSForensics on a bootable CD/DVD or UFD. The document also explains how to inject new device drivers into the Windows image for system specific hardware (where required).

Alternatively, on the "Install OSForensics to a USB drive" Window, you can check the "Launch PassMark WinPE Builder to Create Bootable Solution" checkbox and follow the following tutorial, Creating a self bootable OSForensics with PassMark WinPE Builder.

5 Advanced Topics

5.1 Free OSF Helper Tools

OSForensics has a number of free helper tools for performing tasks outside the scope of the main application. These can be found at this page.

http://www.osforensics.com/tools/index.html

OSFClone

OSFClone is a free, self-booting solution which enables you to create or clone exact raw disk images quickly and independent of the installed operating system. After creating or cloning a disk image, you can mount the image with PassMark OSFMount before conducting analysis with PassMark OSForensics.

OSFClone creates a forensic image of a disk, preserving any unused sectors, slack space, file fragmentation and undeleted file records from the original hard disk. Boot into OSFClone and create disk clones of FAT, NTFS and USB-connected drives! OSFClone can be booted from CD/DVD drives, or from USB flash drives.

Verify that a disk clone is identical to the source drive, by using OSFClone to compare the MD5 or SHA1 hash between the clone and the source drive. After image creation, you can choose to compress the newly created image, saving disk space.

OSFMount

OSFMount is bundled with OSForensics so there is no need to download this seperately. It can be launched from the side menu withing OSF.

OSFMount allows you to mount local disk image files (bit-for-bit copies of a disk partition) in Windows with a drive letter. You can then analyze the disk image file with PassMark OSForensics™ by using the mounted volume's drive letter. By default, the image files are mounted as read only so that the original image files are not altered.

OSFMount also supports the creation of RAM disks, basically a disk mounted into RAM. This generally has a large speed benefit over using a hard disk. As such this is useful with applications requiring high speed disk access, such a database applications, games (such as game cache files) and browsers (cache files). A second benefit is security, as the disk contents are not stored on a physical hard disk (but rather in RAM) and on system shutdown the disk contents are not persistent.

ImageUSB

ImageUSB is a free utility which lets you write an image concurrently to multiple USB Flash Drives. Capable of creating exact bit-level copies of USB Flash Drive (UFDs), ImageUSB is an extremely effective tool for the mass duplication of UFDs. ImageUSB can also be used to install OSFClone to a USB Drive for use with PassMark OSForensics™.

Unlike other USB duplication tools, ImageUSB can preserve all unused and slack space during the cloning process, including the Master Boot Record (MBR). ImageUSB can perform flawless mass duplications of all UFD images, including bootable UFDs.

5.2 Examining System Page File

The page file is a special system file Windows uses to temporarily offload data out of main memory from time to time. This file can contain portions of volatile data even after the system has been shut down.

Using OSForensics built in file viewer this file can be examined and searched for data strings of interest. It is however not possible to view the page file of an active system to do this the target drive must be mounted in an inactive state. (ie. Windows is not currently running from this drive)

To view the page file. Select "Internal File Viewer" from the OSF start page and browse to the location of pagefile.sys, which is usually located in the root of the drive Windows was installed to. It is possible the page file was moved to another drive or removed entirely by the user however so this will not always be true.

5.3 OSForensics Code Signing

OSForensics is protected by a signature across the whole executable to prevent tampering. Any modifications to the executable will remove this signature. This is useful to ensure that no malicious applications on a target machine in a live acquisition can modify OSForensics in order to hide things.

This signature can be viewed by right clicking osf.exe in the OSForensics install directory, selecting properties and going to the "Digital Signature" tab.

If this tab is not there, or the signature is not from "PassMark Software Pty Ltd", the executable has been tampered with.

5.4 Dates and Times

All date and time information in OSForensics is stored internally as UTC. Any date time information read in from external sources that is not already UTC is converted.

When displaying this information the time is converted to the time zone specified in the currently open case. By default this is the local time zone, if no case is open then the local time zone is also used. The case time zone can be modified when creating a new case or changing the properties of the existing case.

The format that the time is displayed in is specified by the current system's regional settings. If you wish to change the date/time display format you can go the the "Region and Language" settings in the Windows control panel.

5.5 Regular Expressions

Perl compatible regular expressions (PCRE) are used when filtering the results displayed when browsing the search index. Several regular expression have been pre defined for quick use but you can also type your own regular expressions in the edit below the list. Currently the search is case insensitive, so "TEST" will return the same results as "test".

For example to search for any entry containing the word "test" select the Custom option from the filter drop down list, type "test" and then click the search button. To find only entries that begin with the word "test" use "^test", the "^" character is used to indicate the pattern match must start at the beginning of the found word.

To search for one of the special characters (eg $ ^ .) you will need to escape the character with "\", eg "\.com". For more information on the format and special characters used see the Perl regular expressions help page.

There are several pre-configured regular expressions available from the drop down list, these are found in the the "RegularExpressions.txt" file in the OSForensics program data directory (ProgramData \PassMark\OSForensics). These have been collected from various sources and are kept as simple as possible while still returning fairly accurate results, please note these will not be 100% accurate in all situations.

The RegularExpressions.txt expect 2 lines per regular expression, the first being a name for the expression (that is used for displaying in drop down selection fields) and then the PCRE expression on the next line, for example the first two lines of the default file are;

```
American Express
3\d{3}(\s|-)?\d{6}(\s|-)?\d{5}
```

6 Support

System Requirements

License Keys

Contacting PassMark® Software

Free Version Limitations

6.1 System Requirements

- Windows XP SP2, Vista, Win 7, Win 8/8.1, Win 10; Windows Server 2000, 2003, 2008, 2012 (64-bit O/S recommended)
- Minimum 1GB of RAM. (8GB+ recommended, more for large document sets, see this forum post)
- 200MB of free disk space (1GB+ recommended, especially if working with large files)

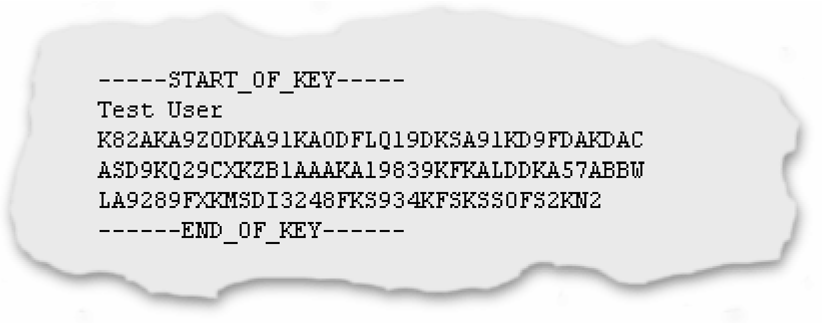
6.2 License Keys

After purchasing the software a license key is sent out via E-mail. This license key needs to be entered into the OSForensics software. The registration window can either be accessed form the welcome window by clicking "Upgrade to Professional Version" or using the "Register" button on the navigation side bar.

When entering a license key, copy and paste the license key from the E-mail. Doing a copy and paste will avoid the possibility of a typing mistake.

Find your license key

After you have placed an order you will receive an e-mail that contains details about your order, your user name and your license key. It should look something like this:



```
-----START_OF_KEY-----
Test User
K82AKA9ZODKA91KAODFLQ19DKSA91KD9FDAKDAC
ASD9KQ29CXKZB1AAAKA19839KFKALDDKA57ABBW
LA9289FXKMSDI3248FKS934KFSKSSOFS2KN2
------END_OF_KEY------
```

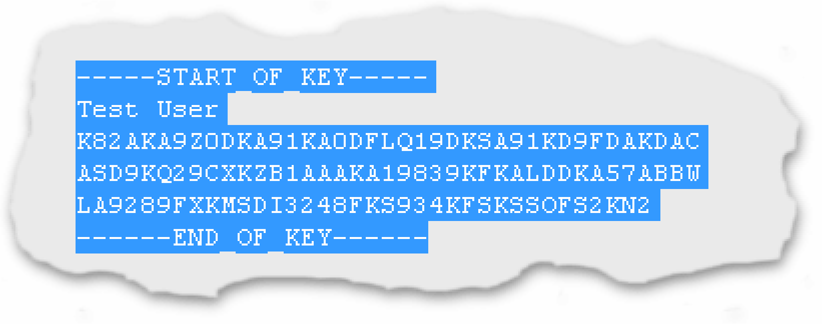
Note that the keys may vary in length and be shorter or longer than the examples above.

Step 1 - Make sure you have the right software

Make sure that the product that you have downloaded and installed, matches the version of the product you have purchased. Note that the key should be entered in the Free Edition of the software to transform it to the registered edition you purchased. Download and install the latest version of the software, if required.

Step 2 - Copy your user name and key from the E-mail

Select the entire key, including the -----START_OF_KEY----- and -----END_OF_KEY----- flags:

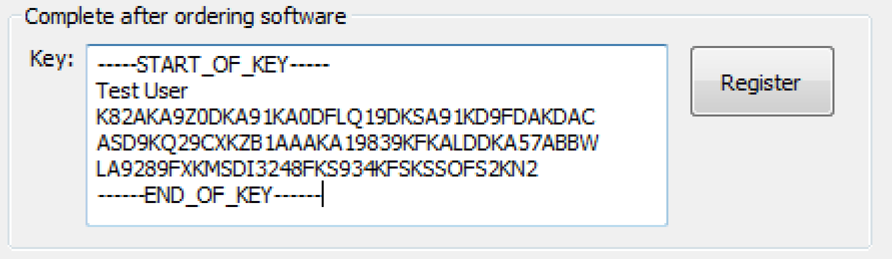


```
-----START_OF_KEY-----
Test User
K82AKA9ZODKA91KAODFLQ19DKSA91KD9FDAKDAC
ASD9KQ29CXKZB1AAAKA19839KFKALDDKA57ABBW
LA9289FXKMSDI3248FKS934KFSKSSOFS2KN2
------END_OF_KEY------
```

Copy your key to the clipboard. This can be done by using the Edit / Copy menu item in most E-Mail programs. Alternatively you can use the CTRL-C key combination on the keyboard.

Step 3 - Paste your user name and key into the software

Start OSF and go to the registration window either by clicking "Upgrade to Professional Version" on the welcome window or using the "Register" button on the navigation side bar. Paste the key in the window provided by right clicking and selecting "Paste" or by using the CTRL-V key combination on the keyboard.



```
-----START_OF_KEY-----
Test User
K82AKA9Z0DKA91KA0DFLQ19DKSA91KD9FDAKDAC
ASD9KQ29CXKZB1AAAKA19839KFKALDDKA57ABBW
LA9289FXKMSDI3248FKS934KFSKSSOFS2KN2
------END_OF_KEY------
```

Click on "Register". If the user name and key was accepted, the program will restart and identify itself as the registered edition of the software in the title bar of the window.

Remember to keep your key safe

The e-mail containing the license key should be kept in a safe place in case the software ever needs to be reinstalled. Your User Name and Key will also be required to be re-entered when software upgrades are released.

Still have a problem?

If you still have a problem, check the following.

- No extra characters were included, be especially careful about not copying extra space characters or new line characters.
- Your user name is exactly as it appears in the E-Mail, using a different user name will not work.
- If you typed in your user name or key, rather than copying and pasting, check that you have not made a typing mistake and check that upper and lower case characters are correct. Upper and lower case are important.

Contact us

If the above doesn't fix your problem, contact us and describe the problem you have encountered and include your order number and key.

6.3 Contacting PassMark® Software

On the Web

You can contact PassMark on the web at

http://www.passmark.com

http://www.osforensics.com

E-Mail

For technical support questions, suggestions

support@passmark.com

For any other issues

info@passmark.com

6.4 Free Version Limitations

The following is a list of limitations found in the free version of OSForensics.

- Number of cases limited to 3 at a time.
- Number of items per case limited to 10.
- Cannot undelete multiple files at once.
- Cannot search hard disk for files with multiple streams.
- Cannot create an index of more than 2,500 files.
- Index search results limited to 250 items.
- Cannot export more than 10 recent activity items
- Cannot edit system information gathering lists.
- Cannot export hash sets.
- Cannot import the NSRL database into a hash set.
- Password cracking is limited to a single core.
- Number of login details limited to 5 per browser.
- Cannot sort images by color.
- Cannot view NTFS $I30 directory entries
- Web browser screen capture contains a watermark
- Cannot boot without an operating system

To remove these restriction please Purchase OSForensics.

7 Copyright and License

SOFTWARE COVERED BY THIS LICENCE
This license agreement (“Agreement”) applies only to the version of the software package OSForensics V5 with which this Agreement is included. Different license terms may apply to other software packages from PassMark and license terms for later versions of OSForensics may also be changed.

TITLE

PassMark or its licensors own the OSForensics software package, including all materials included with the package. PassMark owns the names and marks of ‘PassMark’®, ‘OSForensics’ under copyright, trademark and intellectual property laws and all other applicable laws.

TERMINATION

This license will terminate automatically if you fail to comply with any of the terms and conditions, limitations and obligations described herein. On termination you must destroy all copies of the PassMark package and all other materials downloaded as part of the package.

Trial Version
If you are using a trial version of OSForensics, then you must uninstall the software after the trial period of thirty (30) days has elapsed.

DISCLAIMER OF WARRANTY

PassMark disclaims any and all warranties express or implied, including any implied warranties as to merchantability or fitness for a particular purpose. You acknowledge and agree that you had full opportunity to test OSForensics before any live, public or production use, that you assume full responsibility for selecting and using OSForensics and any files that may created through the use of OSForensics and that if you use OSForensics improperly or against instructions you can cause damage to your files, software, data or business. The entire risk as to quality and performance of OSForensics is borne by you. **This disclaimer of warranty constitutes an essential part of the agreement**. Some jurisdictions do allow exclusions of an implied warranty, so this disclaimer may not apply to you and you may have other legal rights that vary by jurisdiction.

LIMITATION OF LIABILITY

In no event shall PassMark, its officers, employees, affiliates, contractors, subsidiaries or parent organizations be liable for any incidental, consequential, or punitive damages whatsoever relating to the use of OSForensics, files created by OSForensics or your relationship with PassMark. Some jurisdictions do not allow exclusion or limitation of liability for incidental or consequential damages, therefore the above limitation may not apply to you.

HIGH RISK ACTIVITIES

OSForensics is not fault-tolerant and is not designed or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which failure of OSForensics could lead directly to death, personal injury, or severe physical or environmental damage (“High Risk Activities”). PassMark and its suppliers specifically disclaim any express or implied warranty of fitness for High Risk Activities.

LINKS TO THIRD-PARTY SITES

PassMark is not responsible for the contents of any third-party sites or services, any links contained in third-party sites or services, or any changes or updates to third-party sites or services. In the case where PassMark is providing those links and access to third-party sites and services to you only as a convenience, and the inclusion of any link of access does not imply an endorsement by PassMark of the third-party site of service.

ADDITIONAL SOFTWARE

This EULA applies to updates, supplements, add-on components or internet based services components of the software that PassMark may provide to you or make available after the date you obtain your initial copy of the software, unless they are accompanied by separate terms.

UPGRADES

To use software identified as an upgrade, you must first be licensed for the software identified by PassMark as eligible for the upgrade. After installing the upgrade, you may no longer use the original software that formed the basis of your upgrade eligibility, except as part of the upgraded software.

EXPORT RESTRICTIONS

You acknowledge that the software is subject to Australian export jurisdiction. You agree to comply with all applicable international and nationals laws that apply to the software including destination restrictions issued by Australia and other governments.

SOFTWARE TRANSFER
You may transfer your copy of the software to a different device. After the transfer, you must completely remove the software from the former device.

Transfer to Third Party
This license is granted exclusively to you, the original licensee, and therefore no right to resell, transfer, or re-assign the license is granted. An exception may exist for manufacturers, distributors and dealers/ resellers of computer systems or computer software who have specifically negotiated for such an exception with PassMark to resell a particular license key as part of an installed system or as an authorized reseller of the software on its own.

SITE LICENSES
If this software is being installed as part of a Site License purchase, then following conditions apply: The software may installed on an unlimited number of computer systems provided that:

1) The computers on which the software is installed belong to the one legal entity. Subsidiaries, parent companies, brother/sister companies, affiliates and/or agents are not considered to be the same legal entity and are therefore not entitled to have the software installed on their computer systems unless specific permission is granted by PassMark.
2) The computer systems must all be situated in the one country. It is permissible that the computers be located in different cities or states within the one country.
3) All such computers are the property of, or are being leased or borrowed by the licensee and are on the premises of the licensee.
4) In the event that the computers are leased or borrowed, the software must be removed prior to the computer being returned to its legal owner.

NO RENTAL/COMMERCIAL HOSTING
You many not rent, lease or lend the software.

LIMITATIONS ON REVERSE ENGINEERING, DECOMPILATION AND DISASSEMBLY
You may not reverse engineer, decompile, or disassemble the software, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

APPLICABLE LAW
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. You agree and consent that jurisdiction and proper venue for all claims, actions and proceedings of any kind relating to PassMark 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 they 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 PassMark herein.

ENTIRE AGREEMENT
This Agreement (including any addendum or amendment to this EULA which is included with the software) constitutes the entire Agreement between the parties with respect to the subject matter herein and supersedes all previous and contemporaneous agreements, proposals and communications, written or oral between you and PassMark. Waiver by PassMark of any violation of any provision of this Agreement shall not be deemed to waive any further or future violation of the same or any other provision.

This software contains some GNU LGPLv3 licensed code:
- Parts related to EnCase/SMART images by Joachim Metz
  https://github.com/libyal/libewf

- Parts related to VHD images by Joachim Metz
  https://github.com/libyal/libvhdi
- Parts related to ESEDB by Joachim Metz
  https://github.com/libyal/libesedb
- Parts related to Volume Shadow by Joachim Metz
  https://github.com/libyal/libvshadow
- Parts related to BitLocker by Joachim Metz
  https://github.com/libyal/libbde
  Copyright (C) Free Software Foundation, Inc.
  Read http://www.gnu.org/copyleft/lesser.html for the full GNU LGPLv3 license.

This software contains some BSD 3-Clause licensed code:
- Parts related to Peer-2-Peer BitTorrent decoding
  https://github.com/s3rvac/cpp-bencoding
  Read https://opensource.org/licenses/BSD-3-Clause for the full BSD 3-Clause license.

8 Credits

The following is a list of people and organizations that have provided assistance in the creation of OSForensics.

- Center For Digital Forensic Research, Inc. Pittsburgh, Samuel Norris

Index