



OSFORENSICS

OSForensics

© 2022 PassMark™ Software

OSForensics

© 2022 PassMark™ Software

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

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: October 2022

Table of Contents

Foreword	0
Part I Introduction and Overview	8
Part II How to Purchase OSForensics	8
Part III Navigating OSForensics	9
Part IV OSForensics Settings	12
Part V Features	12
1 Android Artifacts.....	15
Android Artifacts Configuration	19
2 Auto Triage.....	21
3 Boot Virtual Machine.....	25
4 Case Management.....	29
Editing Case Details	33
HTML/Text Editor	41
Customizing Report Appearances	43
Add Device	49
Supported Image Formats.....	52
Supported File Systems.....	53
Supported Partitioning Schemes.....	53
Support for Volume Shadow Copy.....	53
Support for BitLocker Encrypted Drives.....	56
Manage Devices	59
Case Activity Log	61
USB Write-Blocking	63
5 Clipboard Viewer.....	64
6 Deleted Files Search.....	66
Deleted Files Search Configuration	69
Deleted Files Search Results View	73
Deleted File Cluster View	78
Deleted Files Technical Details	79
7 Drive Preparation.....	80
8 Email Viewer.....	83
9 ESE Database Viewer.....	90
ESE Database Advanced Search	94
10 Event Log Viewer.....	95
11 File Name Search.....	104
File Name Search Configuration	109
File Name Search Results View	113
File Name Search Default Presets	117
12 File System Browser.....	119

	File Metadata	125
	File Browser Views	127
	Shadow Copies	130
	Deleted Files	132
13	Forensic and Cloud Imaging.....	133
	Create Image	134
	Restore Image	137
	Hidden Areas - HPA/DCO	138
	RAID Rebuild	141
	Supported RAID Metadata Formats	144
	Create Logical Image	145
	Create Logical Android Image	148
	OSFExtract.....	151
14	Hash Sets.....	153
	New Hash Set	155
	View Hash Set	157
	Hash Set Lookup	158
	Installing Hash Sets	160
	NSRL Import	161
	VIC Import	162
	Hash DB Import/Export Format	162
15	Image Analysis.....	163
16	Indexing.....	163
	Create Index	164
	Indexing Problems and Solutions.....	170
	Save Indexing Configuration.....	171
	Advanced Indexing Options	172
	RAM drive.....	177
	Precognitive Search.....	178
	ECMA Regular Expressions	179
	Search Index	183
	Search Index Configuration.....	185
	Index Search Results View	186
	Browse Index.....	194
17	Installing to a USB Drive or an Optical Disk.....	196
18	Internal Viewer.....	198
	File Viewer	200
	Hex/String Viewer	204
	Hex/String Viewer Settings.....	207
	Text Viewer	208
	Text Viewer Settings.....	209
	File Info	210
	Metadata	212
19	JSON Viewer.....	214
20	Map Viewer.....	217
21	Memory Viewer.....	218
	Live Analysis	219
	Generating a Raw Memory Dump.....	223
	Static Analysis	225
22	Mismatch File Search.....	226

	Mismatch Filter Configuration	228
	Mismatch File Search Results View	230
	Advanced	233
23	Passwords.....	235
	Find Passwords/Keys	236
	Offline Password Decryption.....	238
	Windows Login Passwords	239
	Recovering Windows Passwords With Rainbow Tables	241
	Generating Rainbow Tables	241
	Rainbow Tables.....	245
	Compatible File Formats.....	247
	File Naming Convention.....	247
	How Chains are Generated.....	248
	Character Sets.....	249
	Recovering Passwords Using Rainbow Tables	250
	File Decryption & Password Recovery	251
	Adding Dictionaries.....	257
	Remote Decryption Clients.....	258
	Install PFX Certificate	260
	Ispell Copyright Notice	260
24	Plist Viewer.....	261
25	Program Artifacts.....	264
	Prefetch Viewer	264
	AmCache Viewer	267
26	Raw Disk Viewer.....	269
	Search Window	273
	Regular Expressions	275
	Disk Info	280
	Data Decode Window	281
	Tag Window	284
27	Registry Viewer.....	286
28	Remote Acquisition.....	289
	Network Drive Setup	291
	Troubleshooting Connection Issues	294
29	Script Player.....	295
	Python API Reference	298
30	Signatures.....	299
	Create Signature	299
	Create Signature Configuration	300
	Compare Signature	303
	Signature Info.....	304
	Signature Technical Details	305
	File Listing	307
31	SQLite Database Browser.....	309
32	System Information.....	314
	External Tools	316
33	ThumbCache Viewer.....	318
34	User Activity.....	321
	User Activity Configuration	325
	User Activity Filters	328

	OSX Activity	330
	Registry Activity	330
	Event Logs	332
	Jump Lists	338
	Shellbags	338
	SRUM	338
	Prefetch	339
	Windows Search	339
	Cortana History	339
	BAM / DAM	340
	Anti-Forensics Artifacts	340
	Downloads	340
	Browser History	342
	Search Terms	343
	Website Logins	344
	Form History	345
	Bookmarks	346
	Chat Logs	347
	Peer-to-Peer	347
	Cookies	348
	Cryptocurrency Wallet Apps	349
	USB	350
35	Verify / Create Hash.....	351
36	Web Browser.....	353
	Web Browser (Non-supported OS)	358
37	Web Server Log Viewer.....	363
	Access Log	364
	Error Log	367
	IIS Logs	368
	Custom Logs	372
	Automatic Filters	374
38	\$UsnJrnl Viewer.....	376
Part VI Advanced Topics		379
1	Free OSF Helper Tools.....	379
2	Examining System Page File.....	380
3	OSForensics Code Signing.....	380
4	Dates and Times.....	381
5	Regular Expressions.....	381
6	Adding items to a case.....	381
7	Windows Encrypting File System (EFS).....	382
8	Tags.....	383
9	Recovered Partitions.....	384
Part VII Support		384
1	System Requirements.....	384
2	License Keys.....	385
3	Contacting PassMark® Software.....	386

4 Free Version Limitations.....	387
Part VIII Copyright and License	387
Part IX Credits	390
Index	391

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

With the release of OSForensics V8, PassMark has introduced a subscription option. The licensing option best suited to you will depend on your use case, how frequently you use the software and your need to access the latest updates and user support.

Subscription License

Monthly: \$79.00 USD

Yearly: \$799.00 USD

Perpetual License

OSForensics, including 12 months of Support and Updates: \$1499.00 USD

OSForensics, including 36 months of Support and Updates: \$3299.00 USD

See [here](#) for license inclusions and a detailed license comparison.

[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 into the full licensed version.

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 user 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.

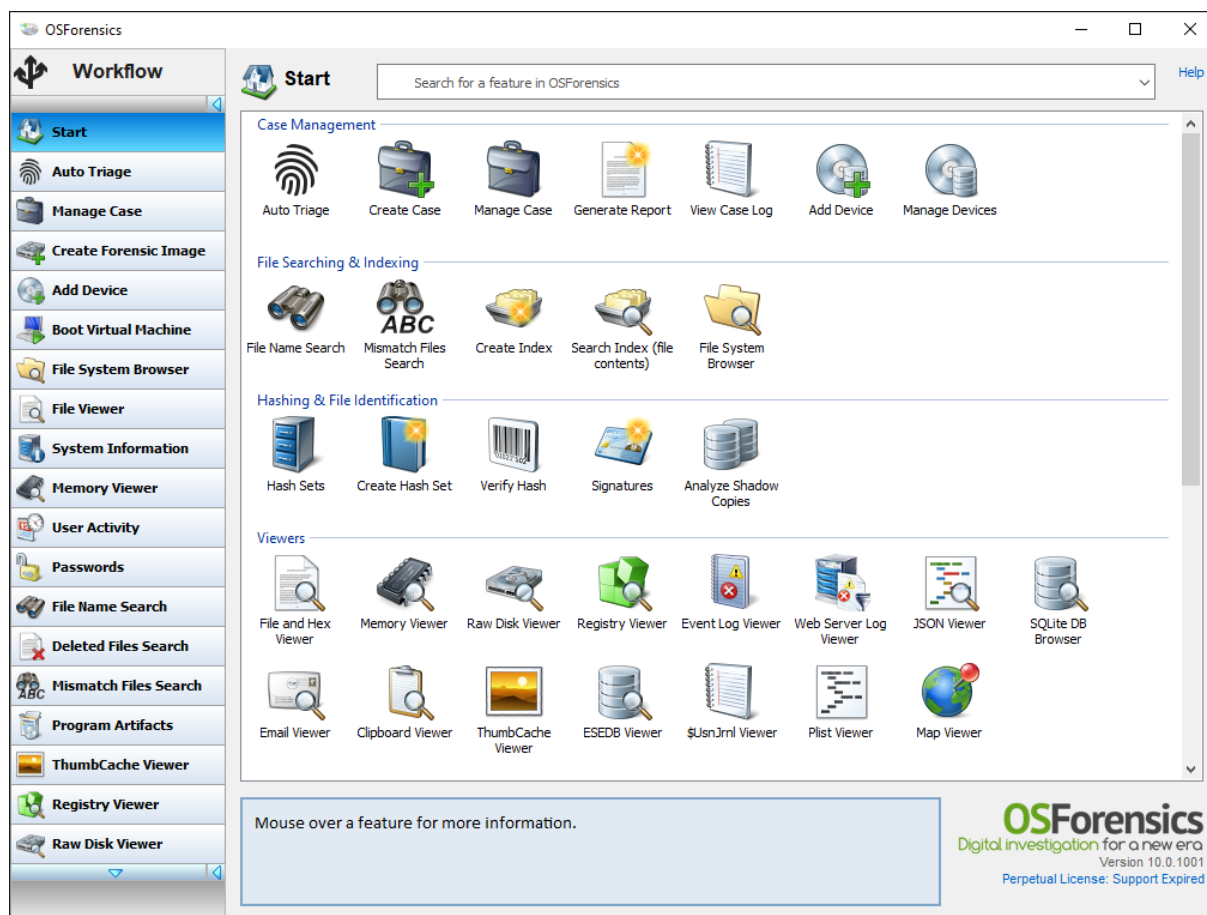
Questions & more information

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.

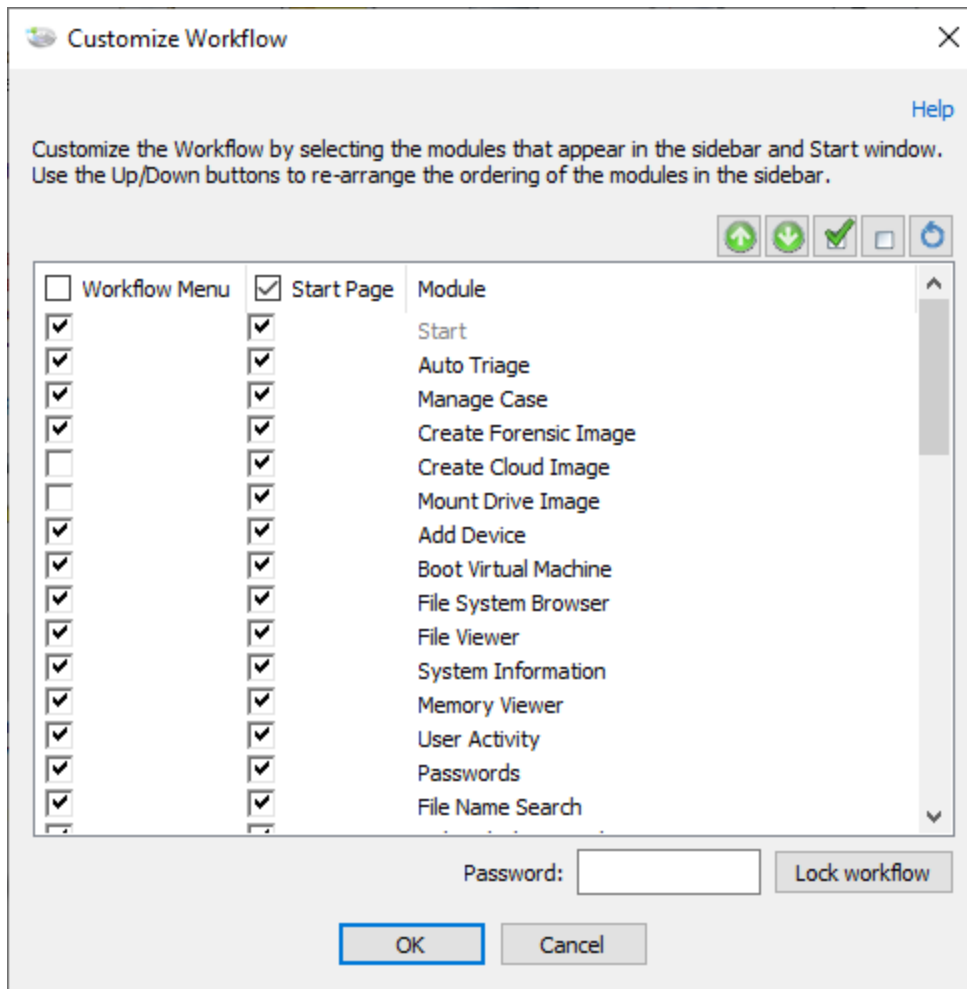


The start window contains a brief description of each feature on mouse over. A green pulsating light appearing next to the sidebar button means that the module is currently performing a task. A blue light means that a task has been completed.

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 be 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

This window allows you to re-arrange the navigation buttons that appear in the *Workflow* menu on the left side of the OSForensics window, as well as the icons that appear in the *Start Window*.

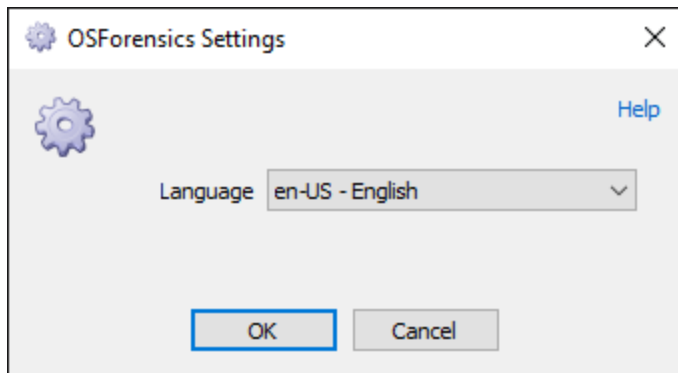


By entering a password and clicking *Lock workflow*, you can deter end users from changing the workflow and accessible options in the *Start Window*.

To unlock the workflow, simply re-enter the password and click the *Unlock workflow* button.

Note that this feature is only designed to act as a deterrent from allowing end users (such as field agents) to use particular features. It does not ensure the disabled features can not be accessed. The lock can be manually removed by clearing the setting in the XML configuration file.

4 OSForensics Settings



Language

Select the language in use. After changing OSForensics will be required to restart to use the selected language.

5 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.

Android Artifacts

Scan Android case devices and backups for evidence of user activity, such as accessed call logs, websites, messages, and contacts.

Auto Triage

Automate common forensic tasks in order to triage the most relevant evidence data in time-limited situations. Auto Triage allows non-forensics trained personnel to acquire intelligence on-site which can be volatile and high-risk.

Boot Virtual Machine

Boot a disk image containing a functional operating system on a virtual machine, recreating the live desktop environment of the system of interest.

Case Management

Manage evidence obtained from OSForensic modules into a single *Case*. Generate HTML and PDF reports to summarize forensic analysis results.

Clipboard Viewer

Display the contents stored in the clipboard on the live system, including the clipboard history and pinned items if available.

Deleted Files Search

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

Drive Preparation

Perform byte pattern verification tests on fixed and removable drives attached to the system.

Email Viewer

Browse and analyze e-mail files including orphaned and deleted e-mails.

ESE Database Viewer

Navigate and search the tables, fields 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.

Event Log Viewer

View Windows Event Logs. Scan, search, filter, export and time-line analysis can be performed on the Event Logs.

File Name Search

Search for files/directories based on name and other file attributes such as size, attributes, and time.

File System Browser

Display the file system of all devices added to a case in an explorer-like view. In addition to standard file system attributes such as file size and file times, other forensic-related metadata is displayed.

Forensic Imaging

Create exact, bit-by-bit duplicates of a disk into an image file. Restore an image file back to the disk. Create a forensically sound logical image of files/directories of interest, preserving file dates, attributes and owners.

Hash Sets

Identify known safe or known suspected files using *Hash Sets* to reduce the need for further time-consuming analysis.

Image Analysis

Performs deep learning image analysis on image files for face detection or illicit image detection.

Indexing

Scan and search for text strings within the contents of a file. Also capable of searching within email archives and pulling text out of unallocated disk sectors.

Internal Viewer

View and analyze files within OSForensics without needing to open an external application. This can be used for files in devices added to the Case such as disk images, which cannot be opened normally in the operating system.

Map Viewer

Search, import and plot location-based evidence on a world map. This includes IP addresses in e-mail headers and server logs, and GPS coordinates in EXIF metadata.

Memory Viewer

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.

Mismatch Search

Identify files that may show evidence of tampering due to having a file extension that is different from what the contents of the file suggests. Eg. A .jpeg file renamed to a .txt file.

Passwords

Recover and decrypt passwords from various sources.

Plist Viewer

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

Program Artifacts

Collect traces of Prefetch and AmCache hive artifacts left by applications. The Prefetch Viewer displays the information stored by the operating system's Prefetcher, which includes when and how often an application is run. The AmCache Viewer shows information from the AmCache hive that contains meta information on program executables and installation.

Raw Disk Viewer

Open and view raw sectors of a disk. Data hidden in the sectors outside the file system can be identified and analyzed with this module.

Registry Viewer

View Windows Registry Hives, including the live system where files can be locked / in use

Signatures

Create a snapshot of a system's directory structure at specific point in time using *Signatures*. *Signatures* can be compared in order to identify files that have been added, deleted and changed.

SQLite Database Browser

Navigate and search the tables, fields and records of SQLite database files.

System Information

View and export hardware, platform and operating system details which can be used for evidence inventory management.

ThumbCache Viewer

Extract 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.

User Activity

Scan the system for evidence of user activity such as accessed websites, USB drives, wireless networks, and recent downloads.

Verify/Create Hash

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

Web Browser

Provide 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.

Web Server Log Viewer

Extract and analyze log data generated by Apache, IIS, NGINX or other custom web server logs.

\$UsnJrnl Viewer

View 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.

5.1 Android Artifacts

This module allows an investigator to scan case devices and backups for evidence of user activity, such as accessed call logs, websites, messages, and contacts. This is especially useful for identifying trends and patterns of the user, and any material that had been accessed recently on a suspect's device.

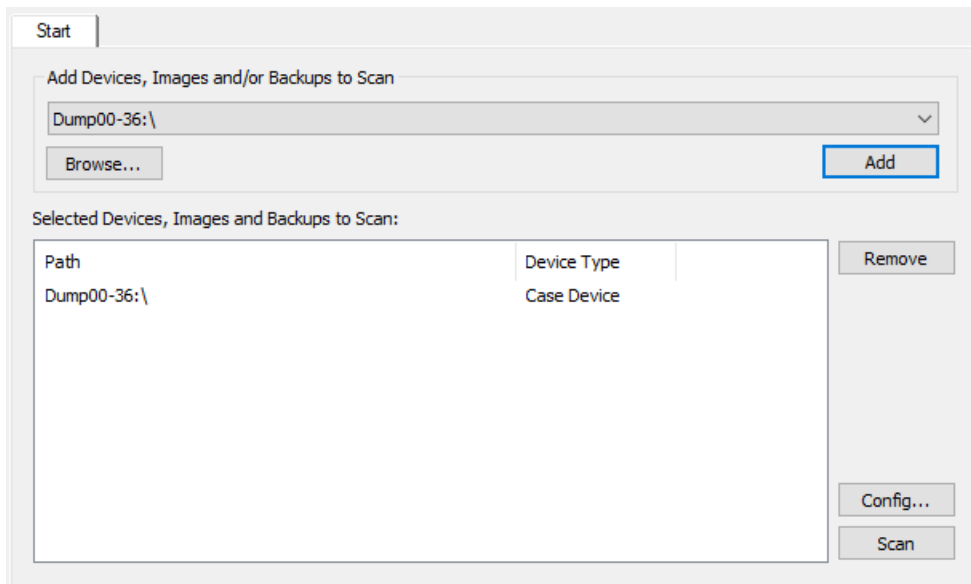
The screenshot displays the 'Android Artifacts' application interface. On the left, a sidebar lists various data categories such as Call Log (500), MMS Messages (0), SMS Messages (11), Contacts (322), Emails (8), Gmail (8), Outlook (0), Installed Applications (34), Browser (388), History (217), Bookmarks (15), Searches (2), Cached Images (154), Snapchat (219), Friends (148), Chat (71), Facebook (3353), Friends (1966), and Messages (1387). The main window shows a list of messages with columns for Date, Date Sent, Type, Number, and Body. A specific message is selected, and a detailed view of the thread is shown on the right, including the thread ID (4727) and the message body text.

Date	Date Sent	Type	Number	Body
<input type="checkbox"/> 7/18/1978, 1:50:48	7/17/1978, 11:08:00	Received	944	I'm on my way
<input type="checkbox"/> 8/5/1978, 8:02:56	8/4/1978, 19:58:00	Received	944	I'm here. Call me if you can
<input type="checkbox"/> 8/16/1978, 12:55:51	8/15/1978, 22:21:20	Received	195	You busy bae
<input type="checkbox"/> 8/23/1978, 23:56:37	8/23/1978, 12:51:20	Received	429	Hey handsome how are u? I miss h
<input type="checkbox"/> 8/26/1978, 10:12:05	8/25/1978, 23:11:20	Received	026	Call me back so I can know you OK
<input type="checkbox"/> 10/27/1978, 15:42:14	10/27/1978, 3:58:00	Received	367	U ight G? Let me know sum
<input type="checkbox"/> 12/14/1978, 22:47:40	12/14/1978, 11:08:00	Received	248	You ok bro
<input checked="" type="checkbox"/> 10/28/1979, 6:55:28	10/27/1979, 18:24:40	Received	690	Good morning how u feeling
<input type="checkbox"/> 10/28/1979, 19:28:00	10/28/1979, 8:01:20	Received	690	I want to see u
<input type="checkbox"/> 12/15/1979, 13:56:13	12/15/1979, 2:08:00	Received	601	I swear u need to answer your phc
<input type="checkbox"/> 12/30/1982, 3:53:31	8/13/1980, 16:54:40	Received	195	Hey bae I was just checking up on

The detailed view on the right shows the thread ID 4727 and the following messages:

- 10/28/1979, 6:55:28: Good morning how u feeling
- 10/28/1979, 19:28:00: I want to see u

A scan for mobile artifacts can be initiated by adding case devices or backup files¹ to the list of devices to scan and then simply pressing the *Scan* button on the *Start* Tab.



More Scan Options

By clicking the *Config...* button you will be taken to the Android Artifacts Configuration window where others options can be selected.

Tab Views

After a scan, a double left click on the artifact type list will open a new tab to display artifacts found during the scan. Different tab views will be open depending on which artifact type is selected.

Details View

The Details View displays the activity presented in a table format. This view is useful for quickly identifying, locating and sorting activities of interest.

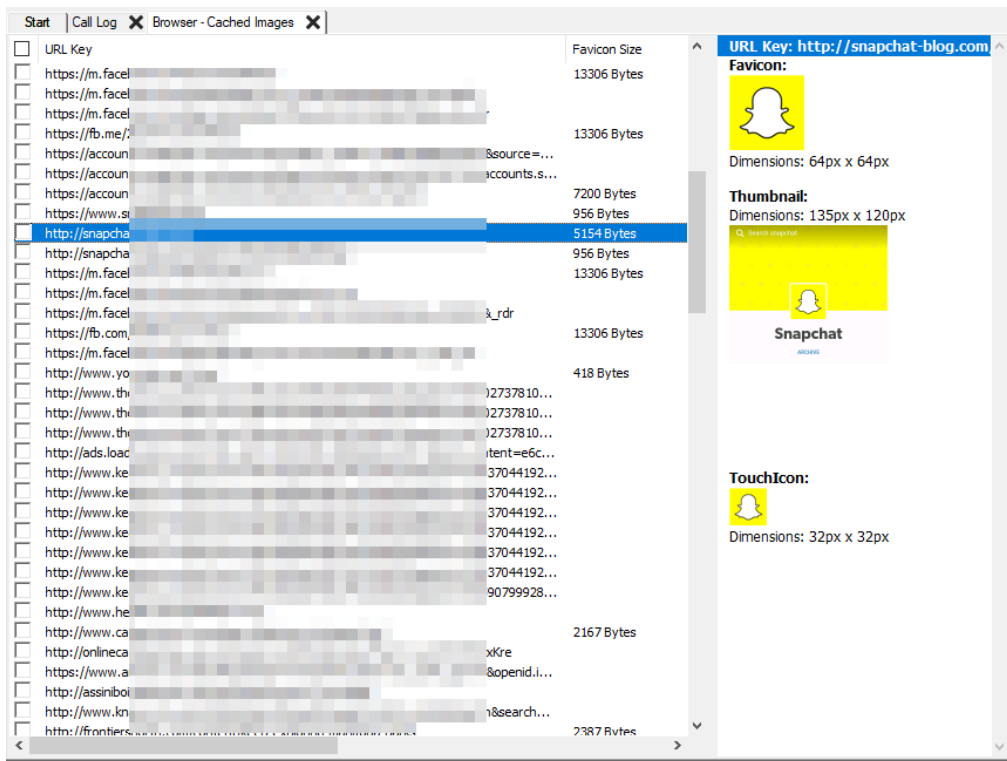
Start Call Log X

Phone Number	Name	Timestamp	Duration	Type	Source
+1-588	Nai	12/31/1966, 4:08:21	43 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-320		1/7/1967, 21:45:41	26 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-558	Tba	1/9/1967, 2:20:47	47 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-558	Tba	1/14/1967, 18:46:01	29 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-558	Tba	1/18/1967, 18:18:38	5 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-512	Tac Cousin	1/27/1967, 2:20:26	28 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-512	Tac Cousin	1/29/1967, 6:57:52	3 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-512	Tac Cousin	1/30/1967, 20:45:57	37 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-462	Lil	2/10/1967, 22:42:19	49 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-462	Lil	2/12/1967, 11:20:03	43 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-248	Ch	2/16/1967, 7:44:11	55 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-195	Do	2/26/1967, 21:12:27	42 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-493	Fill	3/6/1967, 9:31:53	62 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-323	Tia	3/8/1967, 6:08:22	72 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-462	Lil	3/9/1967, 6:56:09	23 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-112	Jar	3/10/1967, 14:40:04	82 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-149	Dre	3/15/1967, 10:17:58	95 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-323	Tia	3/16/1967, 8:50:57	12 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-149	Dre	3/21/1967, 18:47:19	27 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-462	Lil	3/25/1967, 7:35:26	20 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-534		3/26/1967, 11:09:11	17 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-149	Dre	3/29/1967, 16:59:10	29 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-071	Bo	4/11/1967, 7:18:30	227 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-211	Joe	5/11/1967, 15:01:54	109 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-493	To	5/11/1967, 22:38:03	79 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-542	Sm	5/13/1967, 12:54:37	7 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-739	Fla	5/14/1967, 14:08:35	107 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-547	Bar	5/18/1967, 8:43:45	2 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-547	Bar	5/18/1967, 10:48:24	1 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-212	File	5/18/1967, 22:05:34	161 s	Incoming	Dump00-36:\data\com.android.providers.contacts!
+1-345		6/4/1967, 14:07:11	31 s	Outgoing	Dump00-36:\data\com.android.providers.contacts!
+1-045		6/10/1967, 9:45:49	0 s	Missed	Dump00-36:\data\com.android.providers.contacts!
+1-718		8/7/1967, 19:27:04	0 s	Missed	Dump00-36:\data\com.android.providers.contacts!
+1-218	Girl	10/8/1967, 1:02:25	0 s	Missed	Dump00-36:\data\com.android.providers.contacts!

Details View with Artifact Side View

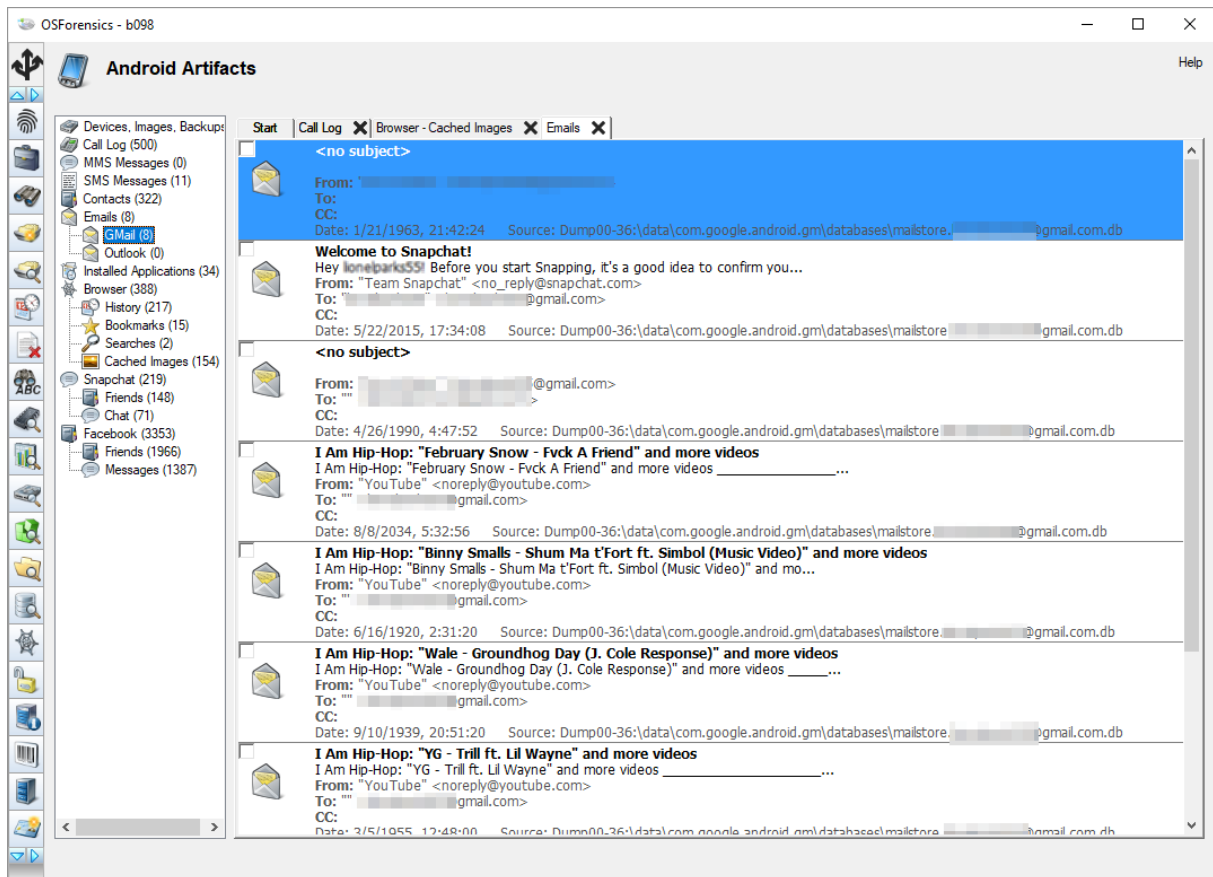
The Details View with artifact side view displays the activity presented in a table format and also displays an additional view to help present the currently selected item.

- **Conversation Tracking Side View** - The side view presents the conversation the currently message belongs to. This additional view is useful for following the conversation from a particular thread or user. See first screenshot for example.
- **Images Side View** - The side view presents preview images associated with the currently selected item.



Artifact List View

The List View displays the activity presented in a list. This view is useful for activities with contents that may be more easily comprehended than in the detailed table format.



Additional Information

See the following pages for more detailed information about the specifics of some of the data gathering. Android Artifacts collected

¹OSForensics currently only supports non-password protected Android Backup Files (.ab).

5.1.1 Android Artifacts Configuration

The Android Artifacts Configuration Window allows the user to configure the Android Artifacts scan options. This window can be accessed by clicking on the "Config..." button on the **Start** tab of the Android Artifacts Module window.

Android Artifacts Configuration

Configuration [Help](#)

Select the items to include in the scan:

System

- Call Log
- MMS
- SMS
- Photos
- Installed Applications
- Contacts
- E-mails

Browser

- Browser History
- Browser Bookmarks
- Browser Searches
- Cached Images

Social Media

- Snapchat
- Facebook

Select a date range to scan:

Search all items

Search date range only

From: 01-Aug-2022 To: 01-Aug-2022

Include dateless items

Call Log

If checked, enables scanning for Call Logs in
"data\com.android.providers.contacts\databases\contacts2.db".

MMS

If checked, enables scanning for MMS messages in
"data\com.android.providers.telephony\databases\mmssms.db".

SMS

If checked, enables scanning for SMS messages in
"data\com.android.providers.telephony\databases\mmssms.db".

Installed Applications

If checked, enables scanning for application installed in
"data\com.google.android.googlequicksearchbox\databases\icingcorpora.db".

Contacts

If checked, enables scanning for contacts in "data\com.android.providers.contacts\databases\contacts2.db".

Emails

If checked, enables scanning for emails located in "data\com.google.android.gm\databases\mailstore.<#####>@gmail.com.db".

Photos

If checked, enables scanning for photos entries in "data\com.google.android.apps.photos\db\gphotos0.db".

Browser History

If checked, enables scanning for browser URL history in "apps\com.android.browser\databases\browser2.db"

Browser Bookmarks

If checked, enables scanning for browser bookmarks in "apps\com.android.browser\databases\browser2.db"

Browser Searches

If checked, enables scanning for browser searches in "apps\com.android.browser\databases\browser2.db"

Cached Images

If checked, enables scanning for browser cached images (e.g. favicon, thumbnail, touchicon) in "apps\com.android.browser\databases\browser2.db"

Snapchat

If checked, enables scanning for contacts and message artifacts from Snapchat application in "data\com.snapchat.android\databases\tcspahn.db"

Facebook

If checked, enables scanning for contacts and message artifacts from Facebook application in "data\com.facebook.orca\databases\contacts_db2" and in "data\com.facebook.orca\databases\threads_db2".

Search all items

Searches all items for user activity.

Search date ranges only

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

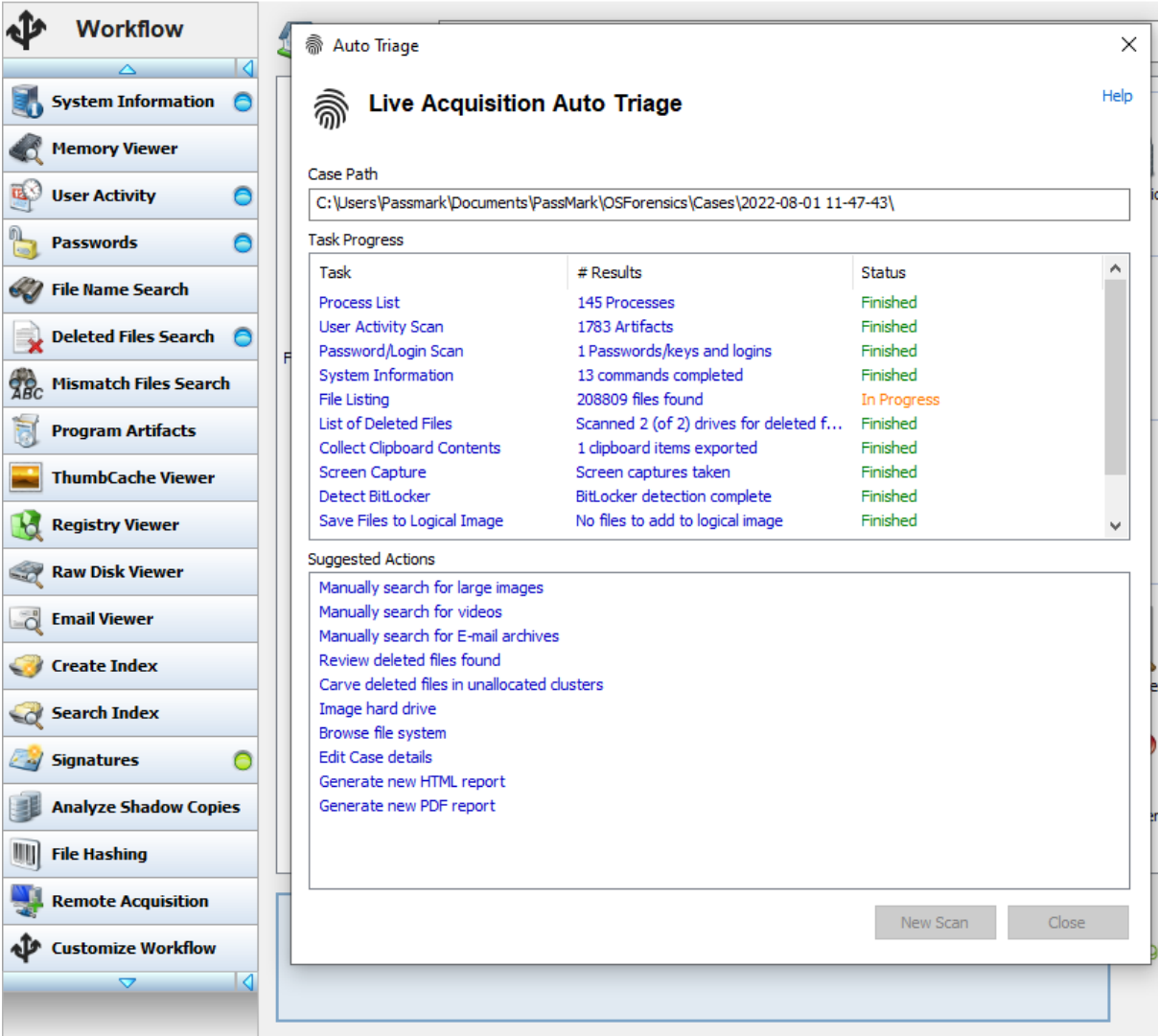
Include dateless items

If checked, will include items without an access date.

5.2 Auto Triage

Forensics triage is the process of obtaining the most relevant evidence data from a system within a limited time frame. This is the case in particular for field personnel with limited forensics knowledge needing to collect forensics data in a time-critical situation. This practice is useful for non-forensic trained personnel, first responders, military personnel who are tasked with acquiring intelligence on-site, especially in potentially volatile situations (such as for Probation & Parole Officers on home visits). By collecting and prioritizing the most valuable evidence on-site, field personnel do not need to submit vast

amounts of data for investigation and therefore can quickly focus on a specific area of interest (eg. internet and application history for probation officers).



OSForensics

Workflow

- System Information
- Memory Viewer
- User Activity
- Passwords
- File Name Search
- Deleted Files Search
- Mismatch Files Search
- Program Artifacts
- ThumbCache Viewer
- Registry Viewer
- Raw Disk Viewer
- Email Viewer
- Create Index
- Search Index
- Signatures
- Analyze Shadow Copies
- File Hashing
- Remote Acquisition
- Customize Workflow

Auto Triage

Live Acquisition Auto Triage

Case Path
C:\Users\Passmark\Documents\PassMark\OSForensics\Cases\2022-08-01 11-47-43\

Task Progress

Task	# Results	Status
Process List	145 Processes	Finished
User Activity Scan	1783 Artifacts	Finished
Password/Login Scan	1 Passwords/keys and logins	Finished
System Information	13 commands completed	Finished
File Listing	208809 files found	In Progress
List of Deleted Files	Scanned 2 (of 2) drives for deleted f...	Finished
Collect Clipboard Contents	1 clipboard items exported	Finished
Screen Capture	Screen captures taken	Finished
Detect BitLocker	BitLocker detection complete	Finished
Save Files to Logical Image	No files to add to logical image	Finished

Suggested Actions

- Manually search for large images
- Manually search for videos
- Manually search for E-mail archives
- Review deleted files found
- Carve deleted files in unallocated clusters
- Image hard drive
- Browse file system
- Edit Case details
- Generate new HTML report
- Generate new PDF report

New Scan Close

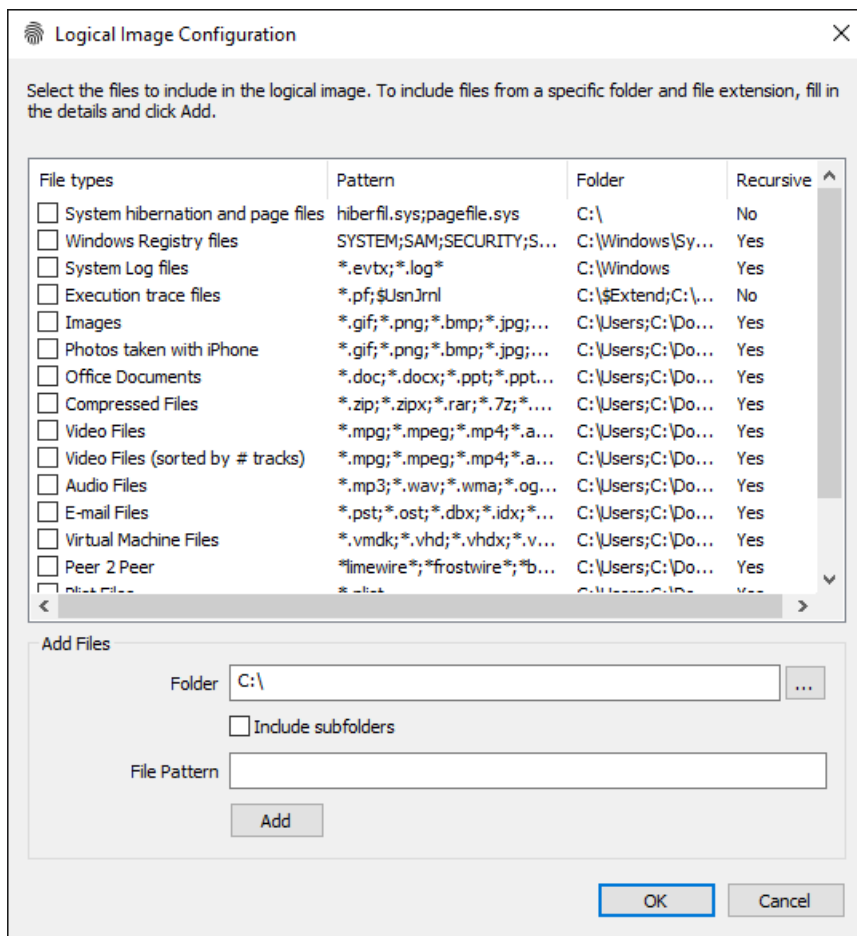
Starting a Triage Scan

The forensics triaging process can be started by clicking on Auto Triage in the Workflow or Start window. Upon doing so, the following configuration dialog is shown which allows the investigator to customize the triaging process.

The screenshot shows the 'Auto Triage' application window. The title bar reads 'Auto Triage' with a close button. The main window title is 'Live Acquisition Auto Triage' with a 'Help' link. The interface includes the following elements:

- Case Name:** A dropdown menu containing '2022-08-01 11-45-02'.
- Investigator:** An empty dropdown menu.
- Case Format:** Radio buttons for 'Folder Path' (selected) and 'Compressed File'.
- Path:** A text box containing 'C:\Users\Passmark\Documents\PassMark\OSForensics\Cases\2022-08-01 11-45-02' and a 'Browse' button.
- Scan Options:** A section with two columns of checkboxes:
 - Left column: Process List, Memory Dump, User Activity, Passwords/Logins, File Listing (Select drives), List of Deleted Files (Select drives), Clipboard Contents.
 - Right column: System Information, Screen Capture, Detect Bitlocker Encryption, Save files to Logical Image (Config...), Generate HTML Report, Generate PDF Report, Upload Case to FTP Server (Config...).
- Memory:** A text box showing 'Total Memory: 8.00 GB'.
- Configuration:** A text box with the instruction 'Click on 'Config...' to determine size of files to be copied'.
- Buttons:** 'Check All', 'Uncheck All', 'Start Scan', and 'Close'.
- Instruction:** A light blue box containing the text 'Mouse over an item for more information.'

By default, the triage scan is pre-configured with the most common settings to allow the investigator to create a new case and initiate the evidence collection immediately. The investigator, however, can configure the files to be saved to a logical image by clicking on the [\(Config...\)](#) link.

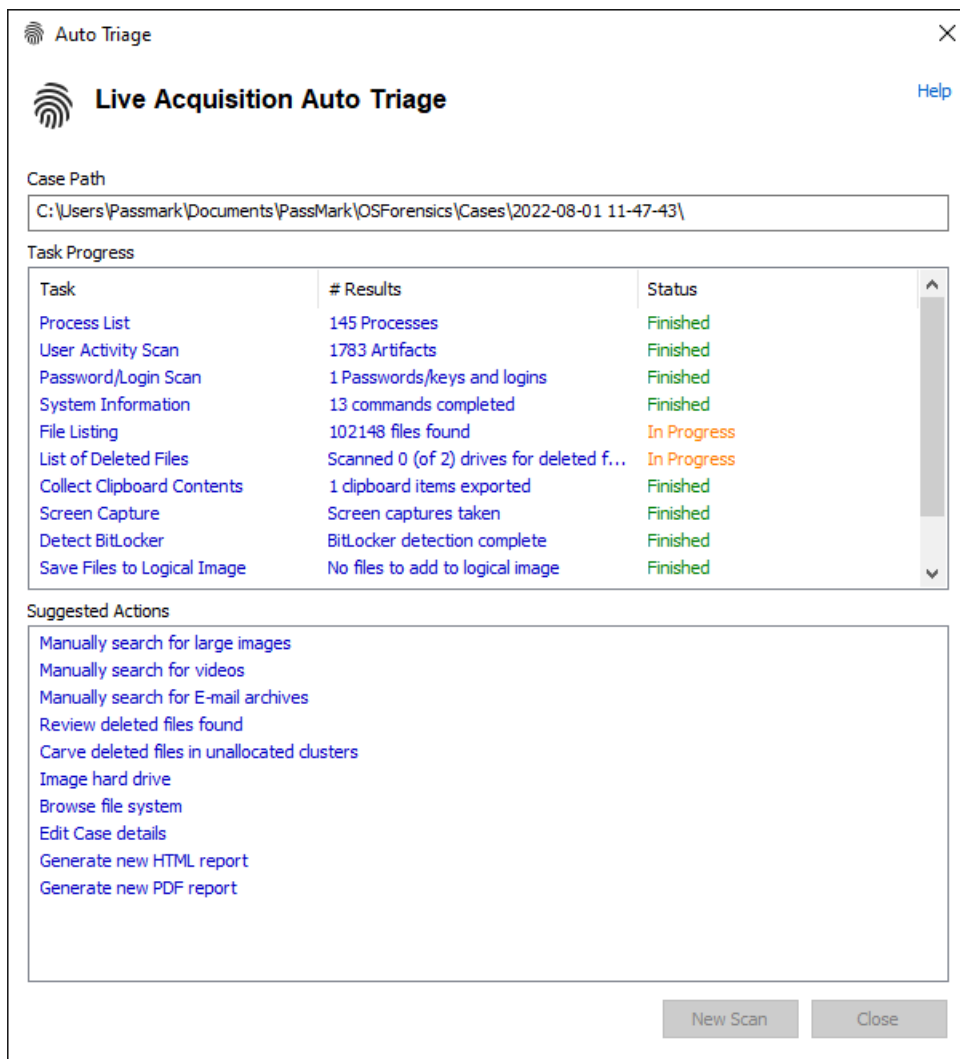


In this dialog, the files to be saved to a logical image can be selected from a default list or a user-specified start folder and file pattern to match. The default list of file types can be found (and modified) in the OSForensics Program Data folder, which is typically located in the following location:

```
C:\ProgramData\PassMark\OSForensics\FileNameSearchPresets.cfg (Vista and newer)
```

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

To start the triaging, click 'Start Scan'. Once the triaging process has started, the following progress dialog is shown which shows the state of all forensic tasks that are running.



The progress of each configured task is displayed and updated in real-time. Once a task has completed, the results are automatically added to the case. The results can be accessed by clicking on the 'Finished' link upon completion.

In addition, a set of suggested actions is provided to supplement the data collected during the triaging process. By clicking on a specific action, the corresponding module is opened and configured appropriately for the investigator to initiate.

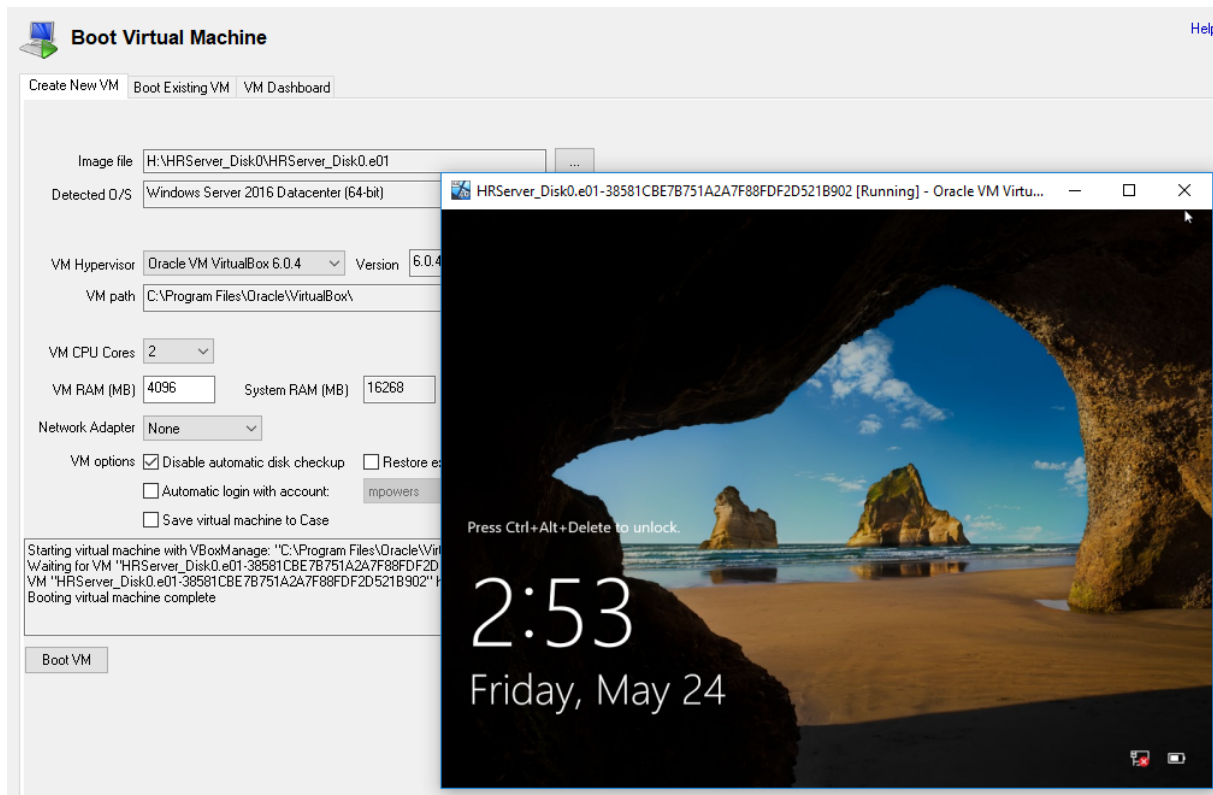
5.3 Boot Virtual Machine

Booting a disk image containing a functional operating system in a virtual environment provides the forensics investigator with a visual context of the system of interest, uncovering additional opportunities for evidence collection and analysis. In addition to being able to view the desktop environment of the system, files and executables that were inaccessible from static analysis can now be opened within the virtual environment.

Support for booting partition images by pre-pending an MBR image to the disk in the .vmdk file (normally it is impossible to boot just a bare partition). This includes images that use ntldr for booting (Windows

XP) and bootmgr + BCD images (Vista and above). Machines with EFI System Partitions are also supported. Images format support includes E01, Raw, Split images, VMDK, VHD.

VMWare 14,15 and VirtualBox 6 are supported as hypervisors. The host machine needs to be 64bit while the guest can be 32bit or 64bit. Guest image can be Mac OS X 10.13 (High Sierra), Windows XP to Win10 and some Linux distributions.



Booting a new virtual machine

Create New VM | Boot Existing VM | VM Dashboard

Image file: H:\FileServer_Disk0\FileServer_Disk0.e01

Detected O/S: Windows Server 2008 R2 Enterprise (64-bit)

VM Hypervisor: Oracle VM VirtualBox 6.0.4 | Version: 6.0.4.128413

VM path: C:\Program Files\Oracle\VirtualBox\

VM CPU Cores: 2

VM RAM (MB): 4096 | System RAM (MB): 16268

Network Adapter: None

VM options:
 Disable automatic disk checkup
 Restore existing disk state
 Automatic login with account: mpowers
 Save virtual machine to Case

Starting virtual machine with VBoxManage: "C:\Program Files\Oracle\VirtualBox\VBoxManage.exe startvm "HRServer_Disk(
 Waiting for VM "HRServer_Disk0.e01-38581CBE7B751A2A7F88FDF2D521B902" to power on...
 VM "HRServer_Disk0.e01-38581CBE7B751A2A7F88FDF2D521B902" has been successfully started.
 Booting virtual machine complete

Boot VM

Image file

Select a disk image file to boot a new virtual machine instance. All disk writes within the virtual machine shall be stored in a separate delta write cache file, preserving the integrity of the disk image file.

Detected O/S

The operating system found on the disk

VM Hypervisor

Select one of the virtual machine hypervisors installed on the host machine

VM path

The virtual machine hypervisor install path

VM CPU Cores

Specify the number of CPU cores for the virtual machine

VM RAM (MB)

Specify the amount of system RAM for the virtual machine

System RAM (MB)

The amount of physical RAM available on the host system. the amount of VM RAM must not exceed this value.

Disable automatic disk checkup

Check to disable automatic disk checkup on boot due to a dirty file system. This can occur if the disk image was acquired before the system was properly shutdown.

Restore existing disk state

Check to restore the disk state from a previous boot using the disk image's delta write cache file. Otherwise, the original disk image is used and a new delta write cache file is created.

Automatic login with account

Check to bypass the Windows account login screen and logon as the selected user. *Note: This option attempts to bypass password verification, which may or may not be successful depending on the Windows version.*

Save virtual machine to Case

Check to add the virtual machine to the case. This would be useful for booting or restoring the virtual machine at a later time.

Boot VM

Start the virtual machine

Booting an existing virtual machine

VM Name	Size	Operating System	CPU	RAM	Disk
Desktop-Disk0.e01	50.00 GB	Windows 10 Enterprise (64...	2	4096 MB	H:\Desktop-Disk0\Desktop-Disk0.e01
nps-2009-domexusers...	40.00 GB	Microsoft Windows XP	2	4096 MB	H:\nps-2009-domexusers.E01
HRServer_Disk0.e01	50.00 GB	Windows Server 2016 Dat...	2	4096 MB	H:\HRServer_Disk0\HRServer_Disk0.e01
Win10.Ex01	40.00 GB	Windows 10 Enterprise (64...	2	4096 MB	H:\Win10\Win10.Ex01
DellVostro1400_EX0...	59.63 GB	Windows 8.1 Pro (64-bit)	2	4096 MB	H:\Dell Vostro ex01\ex01\DellVostro1400_EX0...

VM Hypervisor	Oracle VM VirtualBox 6.0.4	Version	6.0.4.128413
VM path	C:\Program Files\Oracle\VirtualBox\		
VM CPU Cores	2		
VM RAM (MB)	4096	System RAM (MB)	16268
Network Adapter	None		
VM options	<input checked="" type="checkbox"/> Disable automatic disk checkup <input type="checkbox"/> Restore existing disk state <input type="checkbox"/> Automatic login with account: mpowers		

Reboot VM

Virtual machines that have been added to the case can be rebooted or restored from its previous state. Select the desired virtual machine, modify any virtual machine settings and click on 'Reboot VM' to boot the virtual machine.

Virtual Machine Dashboard

The screenshot displays the 'VM Dashboard' interface. At the top, there are three tabs: 'Create New VM', 'Boot Existing VM', and 'VM Dashboard'. Below the tabs is a table listing virtual machines:

Disk	Status	Hypervisor	Size	Operating System	CPU	RAM	Mount Point
H:\HRServer_Disk0\HRServer_Disk0.e01	Stopped	Oracle VM VirtualBox 6.0.4	50.00 GB	Windows Server 2016 Datacenter (64-bit)	2	4096 MB	\\.\PhysicalDrive3
H:\HRServer_Disk0\HRServer_Disk0.e01	Stopped	Oracle VM VirtualBox 6.0.4	50.00 GB	Windows Server 2016 Datacenter (64-bit)	2	4096 MB	\\.\PhysicalDrive3

Below the table are three buttons: 'Dismount Drive', 'Clear all', and 'Refresh'. A preview window titled 'HRServer_Disk0.e01-38581CBE7B751A2A7F88FDF2D521B902 [Running] - Oracle VM Virtu...' is open, showing a Windows lock screen with a beach scene. The lock screen displays the time '3:06' and the date 'Friday, May 24'. A message 'Press Ctrl+Alt+Delete to unlock.' is visible. The taskbar at the bottom right shows the Start button and a few icons.

Once a virtual machine has been successfully booted, it shall be added to the dashboard. The status of all virtual machines that have been booted shall be displayed in the list.

Dismount Drive

Dismount the virtual physical drive from the host if the virtual machine is no longer running.

Clear all

Removes all virtual machines from the dashboard.

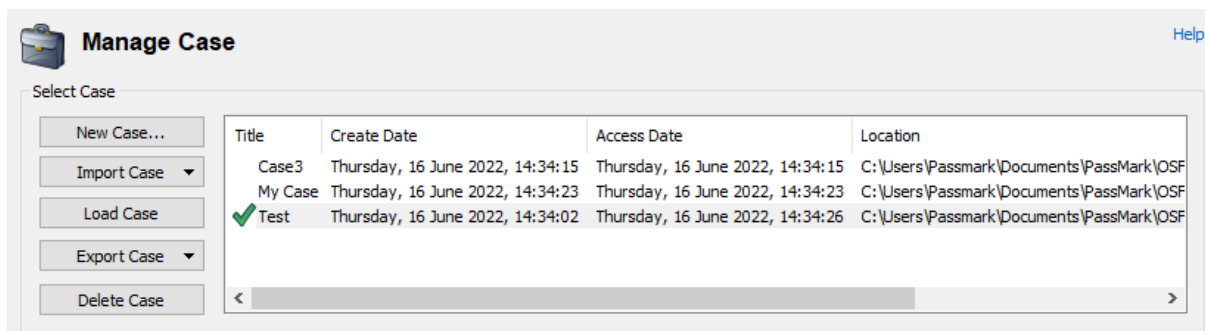
Refresh

Refresh the status of all virtual machines.

5.4 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.



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

Import Case Folder

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

Note that this does not copy the case folder, it just makes a reference to that folder selected. If the folder disappears (e.g. by removing the USB drive containing the case folder), then the case cannot be accessed.

In some cases it might make sense to manual copy the Case folder from the USB drive, to the internal drive before importing it.

Import Case File

Add a case to the list that is not in the default case folder using a .zip file.

Load Case

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

Export Case

Exports the currently selected case from the list to a specified directory.

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.

The screenshot shows the Case Manager interface with several toolbars and a main table. The toolbars include 'Case Properties' (Edit Case Details..., Edit Narrative..., Edit Categories..., Manage Devices...), 'Case Exports' (Generate Report..., View & Export Log...), 'Add to Case' (Device..., Attachment..., Photos of Evidence..., External Report..., Notes..., Clipboard Data...), and 'Case Items' (Open, Delete, Properties, Verify).

Case Item ID	Title	Module	Case Item	Category	Date Added
Exported Items					
2	[Current Clipboard] Bitma...	Clipboard Viewer	[Current Clipboard] Bitmap (1.56 MB...		Thursday, 16 June 2022, ...
3	Detect BitLocker	System Informa...	SI 2022-06-16 04-36-12.bitlocker.html		Thursday, 16 June 2022, ...
7	Process List	Memory Viewer	MV 2022-06-16 04-36-15.csv		Thursday, 16 June 2022, ...
9	System Information	System Informa...	SI 2022-06-16 04-36-30.html		Thursday, 16 June 2022, ...
10	Password/Login Scan	Password Reco...	PR 2022-06-16 04-36-44.csv		Thursday, 16 June 2022, ...
11	User Activity Scan	User Activity	UA 2022-06-16 04-36-11.csv		Thursday, 16 June 2022, ...
12	List of Deleted Files	Deleted Files	DF Drive-C 2022-06-16 04-36-12.csv		Thursday, 16 June 2022, ...
13	List of Deleted Files	Deleted Files	DF Drive-E 2022-06-16 04-36-12.csv		Thursday, 16 June 2022, ...
Attachments					
4	Screen Capture	Case Manager	2022-06-16 04-36-13 Fullscreen.png	Images	Thursday, 16 June 2022, ...
5	Screen Capture	Case Manager	2022-06-16 04-36-14 Application Fr...	Images	Thursday, 16 June 2022, ...
6	Screen Capture	Case Manager	2022-06-16 04-36-14 eViewer for Wi...	Images	Thursday, 16 June 2022, ...
8	File Listing	Create Signature	2022-06-16 04-36-12 FileListing.csv		Thursday, 16 June 2022, ...
Devices					
0	Drive-C	Case Manager	C:		Thursday, 16 June 2022, ...
1	Drive-E	Case Manager	E:		Thursday, 16 June 2022, ...

A special group is the Tagged Items group. This group contains a list of items that need checking / verifying by an investigator before adding to the case.

The screenshot shows the 'Tagged Items' section with a list of items. Each item includes a title, a file path, and a date.

Title	File Path	Date
User Activity	<wlan>:C:\ProgramData\Microsoft\W...	Thursday, June 24
User Activity	<cookie>:C:\Users\Richard\AppData...	Friday, June 25, 21
User Activity	<cookie>:C:\Users\Richard\AppData...	Friday, June 25, 21
File System Browser	OSF_Password_Crack(C):\big_dic_te...	Monday, June 28,
File System Browser	OSF_Password_Crack(C):\password i...	Monday, June 28,
File System Browser	OSF_Password_Crack(C):\WinZip_st...	Monday, June 28,
File Name Search	C:\Camera\20190805_103345.jpg	Monday, June 28,
Mismatch Search	C:\\$Recycle.Bin\S-1-5-21-11226048...	Monday, June 28,
Mismatch Search	C:\Program Files\Blender Foundatio...	Monday, June 28,
Mismatch Search	C:\android-ndk\android-ndk-r16b\pre...	Monday, June 28,
User Activity	<wlan>:Drive-C:\ProgramData\Micros...	Wednesday, June
Case Manager	C:\Camera\20190805_111447.jpg	Wednesday, June
Case Manager	C:\Camera\20190805_215219.jpg	Wednesday, June
File/Hex Viewer	C:\Camera\20190805_111641.jpg	Wednesday, June
User Activity	<registry>:C:\WINDOWS\appcompat...	Friday, July 2, 202
User Activity	<registry>:HKEY_LOCAL_MACHINE*...	Friday, July 2, 202
User Activity	https://se	Friday, July 2, 202
User Activity	https://fo	Friday, July 2, 202
User Activity	https://w	Friday, July 2, 202
User Activity	https://yc	Friday, July 2, 202
User Activity	https://se	Friday, July 2, 202

If the tagged items is referencing a file, the item can be added to case directly by right-clicking and selecting "Add to Case".

Tagged Items		
User Activity	<wlan>:C:\ProgramData\Microsoft\W...	
User Activity	<cookie>:C:\Users\Richard\AppData...	
User Activity	<cookie>:C:\Users\Richard\AppData...	
File System Browser	OSF_Password_Crack(C)\big_dic_te...	
File System Browser	OSF_Password_Crack(C)\password i...	
File System Browser	OSF_Password_Crack(C)\WinZip.st...	
File Name Search	C:\Camera\20190805_103345.jpg	
Mismatch Search	C:\\$Recycle.Bin\S-1-5-21-11226048...	
Mismatch Search	C:\Program Files\Blender Foundation...	
Mismatch Search	id-ndk-r16b\pre...	
User Activity	ramData\Micros...	
Case Manager	C:\Camera\20190805_111447.jpg	

If however, the tagged item is a reference to an artifact (e.g. entry from within a database file), it would be necessary to Rerun the Module where the tagged item was added to continue investigation.

Tagged Items		
User Activity	<wlan>:C:\Program	Thurs
User Activity	<cookie>:C:\Users'	Friday
User Activity	<cookie>:C:\Users'	Friday
File System Bro...	OSF_Password_Cr...	Mond
File System Bro...	OSF_Password_Cr...	Mond
File System Bro...	OSF_Password_Cr...	Mond
File Name Search	C:\Camera\201908	Mond
Mismatch Search	C:\\$Recycle.Bin\S	Mond

Manage Current Case

Case Properties

Edit Case Details

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

Edit Narrative

Edit the case narrative which includes additional case analysis details to be included in the generated report.

Edit Categories

Add or modify the list of categories that a case item can be assigned to.

Manage Devices

Manage all devices that have been added to the case.

Case Exports

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 & Export Log

If logging is enabled for the case, opens the log viewer for viewing and exporting the log entries.

Add to Case

Device

Add a storage device to the case for analysis.

Attachment

Add a generic file to the case as an attachment.

Photos of Evidence

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

External Report

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

Notes

Edit the a note to the case as a text file.

Clipboard Data

Add existing bitmap or text content stored in the clipboard to the case.

Case Items

Open

Opens the currently selected case item.

Delete

Deletes the currently selected case item.

Properties

Display or edit the properties for the currently selected case item. The case item can be modified by assigning to a category and/or editing the comments associated with the item.

Verify

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

5.4.1 Editing Case Details

The Edit Case Details window allows the user to specify properties (e.g. name, investigator, time zone, logging options) of the case. Property editing is presented to the user when creating a New Case or when editing an existing case details.

Basic Case Data

New Case Help

Basic Case Data | Case Categories | Offense & Custody Data | Description of Evidence | Chain of Custody | Custom Fields | C < >

Case Name

Investigator

Organization

Contact Details

Timezone Local (GMT +10:00) Australian Eastern Standard Time

Default Drive C:\[Local]

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

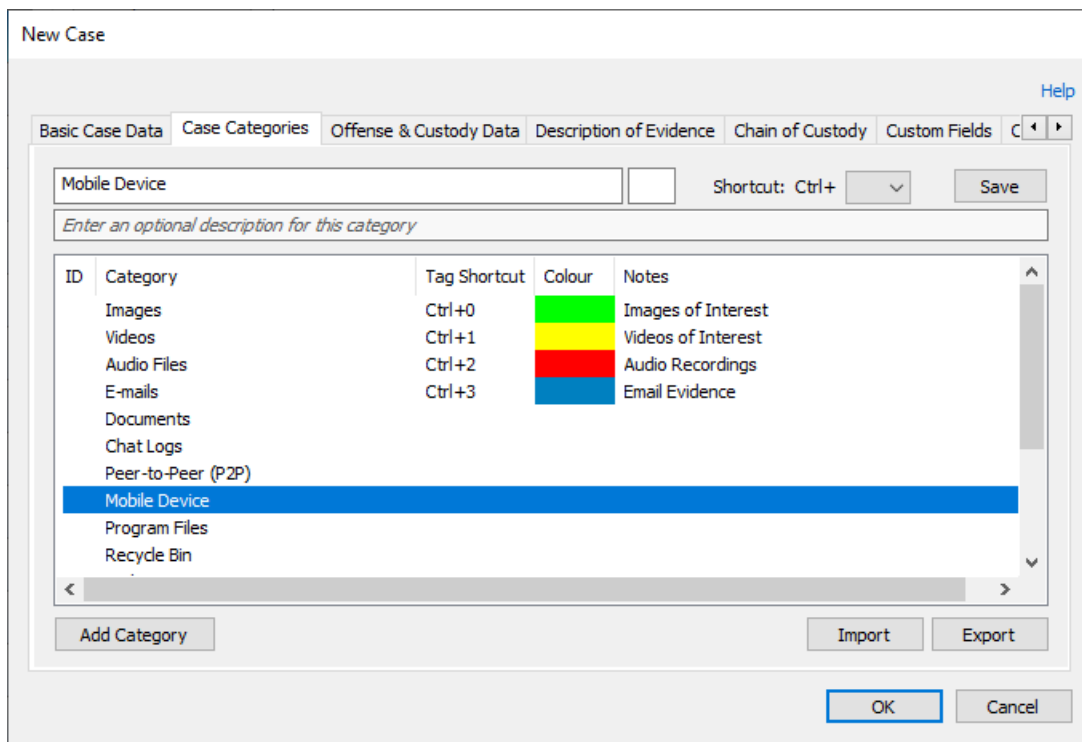
Enable USB Write-block

Case Folder Default Location Custom Location

Log case activity

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.

Case Categories



This tab contains the list of categories defined in the case. The default list of categories can be found (and modified) in the OSForensics Program Data folder, which is typically located in the following location:

```
C:\ProgramData\PassMark\OSForensics\Categories.txt (Vista and newer)
```

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

Clicking on the category allows modifying of its attributes. Once the changes to the category have been made, click 'Save' to apply the changes.

To add a new category, click 'Add Category'.

A category consists of a unique name, optional notes, highlight colour and a shortcut key for tagging. New or existing case items can be assigned to a category.

If a highlight colour is assigned to the category, any item belonging to the category shall be marked with the specified colour as shown in the following screenshot.

Modified category options can be saved by clicking the 'Export' button and selecting a location.

An exported category template can then be loading by selecting the saved file with the 'Import' button.

By default category templates are saved to:

```
C:\ProgramData\PassMark\OSForensics\CategoryTemplates\
```

<input type="checkbox"/>	File Name	Location	Type	Date modified	Date created	Date accessed
<input type="checkbox"/>	0 bk11.jpg	C:\Program Files\WindowsApps\...	JPG File	8/8/2017, 10:30:24.4673232	8/8/2017, 10:30:24.4673232	8/8/2017, 10:30:24.467...
<input type="checkbox"/>	001.jpg	C:\Program Files\WindowsApps\...	JPG File	8/8/2017, 10:30:41.9221914	8/8/2017, 10:30:41.9065660	8/8/2017, 10:30:41.906...
<input type="checkbox"/>	002.jpg	C:\Program Files\WindowsApps\...	JPG File	8/8/2017, 10:30:41.9378180	8/8/2017, 10:30:41.9221914	8/8/2017, 10:30:41.922...
<input type="checkbox"/>	003.jpg	C:\Program Files\WindowsApps\...	JPG File	8/8/2017, 10:30:41.9534463	8/8/2017, 10:30:41.9378180	8/8/2017, 10:30:41.937...
<input type="checkbox"/>	004.jpg	C:\Program Files\WindowsApps\...	JPG File	8/8/2017, 10:30:41.9690729	8/8/2017, 10:30:41.9534463	8/8/2017, 10:30:41.953...
<input type="checkbox"/>	005.jpg	C:\Program Files\WindowsApps\...	JPG File	8/8/2017, 10:30:41.9846998	8/8/2017, 10:30:41.9690729	8/8/2017, 10:30:41.969...
<input type="checkbox"/>	006.jpg	C:\Program Files\WindowsApps\...	JPG File	8/8/2017, 10:30:42.0004999	8/8/2017, 10:30:42.0004999	8/8/2017, 10:30:42.000...
<input type="checkbox"/>	007.jpg	C:\Program Files\WindowsApps\...	JPG File	8/8/2017, 10:30:42.0161644	8/8/2017, 10:30:42.0161644	8/8/2017, 10:30:42.016...
<input type="checkbox"/>	008.jpg	C:\Program Files\WindowsApps\...	JPG File	8/8/2017, 10:30:42.0315780	8/8/2017, 10:30:42.0161644	8/8/2017, 10:30:42.016...
<input type="checkbox"/>	009.jpg	C:\Program Files\WindowsApps\...	JPG File	8/8/2017, 10:30:42.0472049	8/8/2017, 10:30:42.0315780	8/8/2017, 10:30:42.031...
<input type="checkbox"/>	01 16-9.png	C:\Program Files\WindowsApps\...	PNG File	8/8/2017, 10:29:17.3779013	8/8/2017, 10:29:17.3779013	8/8/2017, 10:29:17.377...
<input type="checkbox"/>	01 4-3.png	C:\Program Files\WindowsApps\...	PNG File	8/8/2017, 10:29:17.3779013	8/8/2017, 10:29:17.3779013	8/8/2017, 10:29:17.377...
<input type="checkbox"/>	010.jpg	C:\Program Files\WindowsApps\...	JPG File	8/8/2017, 10:30:42.0628326	8/8/2017, 10:30:42.0472049	8/8/2017, 10:30:42.047...
<input type="checkbox"/>	011.jpg	C:\Program Files\WindowsApps\...	JPG File	8/8/2017, 10:30:42.0840448	8/8/2017, 10:30:42.0628326	8/8/2017, 10:30:42.062...
<input type="checkbox"/>	012.jpg	C:\Program Files\WindowsApps\...	JPG File	8/8/2017, 10:30:42.0949054	8/8/2017, 10:30:42.0898934	8/8/2017, 10:30:42.089...
<input type="checkbox"/>	013.jpg	C:\Program Files\WindowsApps\...	JPG File	8/8/2017, 10:30:42.1105404	8/8/2017, 10:30:42.1105404	8/8/2017, 10:30:42.110...

If a shortcut key is specified, items can be tagged and assigned to the associated category by pressing the shortcut key sequence as shown in the following screenshot.

<input type="checkbox"/>	File Name	Category
<input type="checkbox"/>	04_lensflare_screen.jpg	
<input type="checkbox"/>	04_lightleak_screen.png	
<input type="checkbox"/>	04_scratch_screen.jpg	
<input checked="" type="checkbox"/>	05 16-9.png	Images
<input checked="" type="checkbox"/>	05 4-3.png	Images
<input checked="" type="checkbox"/>	05_grunge_overlay.jpg	Images
<input checked="" type="checkbox"/>	05_lensflare_screen.jpg	Images
<input checked="" type="checkbox"/>	05_lightleak_screen.png	Images
<input checked="" type="checkbox"/>	05_scratch_screen.jpg	Images
<input checked="" type="checkbox"/>	06 16-9.png	Images
<input checked="" type="checkbox"/>	06 4-3.png	Images
<input type="checkbox"/>	06_grunge_overlay.jpg	
<input type="checkbox"/>	06_lensflare_screen.jpg	

Offense & Custody Data

New Case Help

Basic Case Data | Case Categories | **Offense & Custody Data** | Description of Evidence | Chain of Custody | Custom Fields | C ◀ ▶

Offense

Analysis Requested By

Suspect Name

Date/Time Evidence Seized 16/06/2022 4:23 AM

Location of Seizure

Legal Authority for Search

Summary of Job

Advance Edit...

This tab contains the case custody data that is used when generating the default Chain of Custody Report. All fields are optional.

Description of Evidence

Edit Case Help

Basic Case Data | Case Categories | Offense & Custody Data | **Description of Evidence** | Chain of Custody | Custom Fields | C ◀ ▶

Evidence #	Quantity	Description of Item
1	1	Evidence 1
1234ABCD	2	Evidence 2

Add/Edit

Add a new evidence item collected to the case.

Add Evidence

Evidence Number: 1

Quantity: 1

Description of Evidence: Evidence 1

Chain of Custody

Date & Time	Released by	Received by
16/06/2022, 14:46:04, GMT +10:00	Pass	Mark

Buttons: Add, Edit, Delete, OK, Cancel

Edit

Edit an existing evidence item previously added in the case.

Un/Delete

Delete a previously added evidence item in the case. To prevent accidental deletions, the actual deletion is done when choosing "OK" to save the case.

Chain of Custody

The screenshot shows the 'Edit Case' dialog box with the 'Chain of Custody' tab selected. The dialog has a 'Help' link in the top right corner. Below the tabs, there is a table with the following data:

Evidence #	Date & Time	Released by	Received by
1234ABCD	16/06/2022, 14:47:39, GMT +10:00	Mark	Pass
1	16/06/2022, 14:47:25, GMT +10:00	Pass	Mark

Below the table, there is a note: "Note: Editing the chain of custody data is done through the Description of Evidence tab." At the bottom right, there are 'OK' and 'Cancel' buttons.

Shows the Chain of Custody for the added evidence items added to the case. Editing of the Chain of Custody can be accomplished in the Description of Evidence Tab. Select the Evidence and choose Edit.

The screenshot shows the 'Add Chain of Custody' dialog box. It has a close button (X) in the top right corner. The dialog contains the following fields and controls:

- 'Transferred From' text box with a vertical cursor.
- 'Transferred To' text box.
- 'Date/Time Evidence Transferred' field with a date picker showing '16/06/2022' and a time picker showing '2:48 PM' with a checked checkbox.
- 'OK' and 'Cancel' buttons at the bottom.

When the Evidence Window opens, options are to Add a new chain entry, Edit an existing chain entry or Delete an existing chain entry.

Custom Fields

Edit Case

Basic Case Data | Case Categories | Offense & Custody Data | Description of Evidence | Chain of Custody | Custom Fields | C | < | >

Witness | John Doe

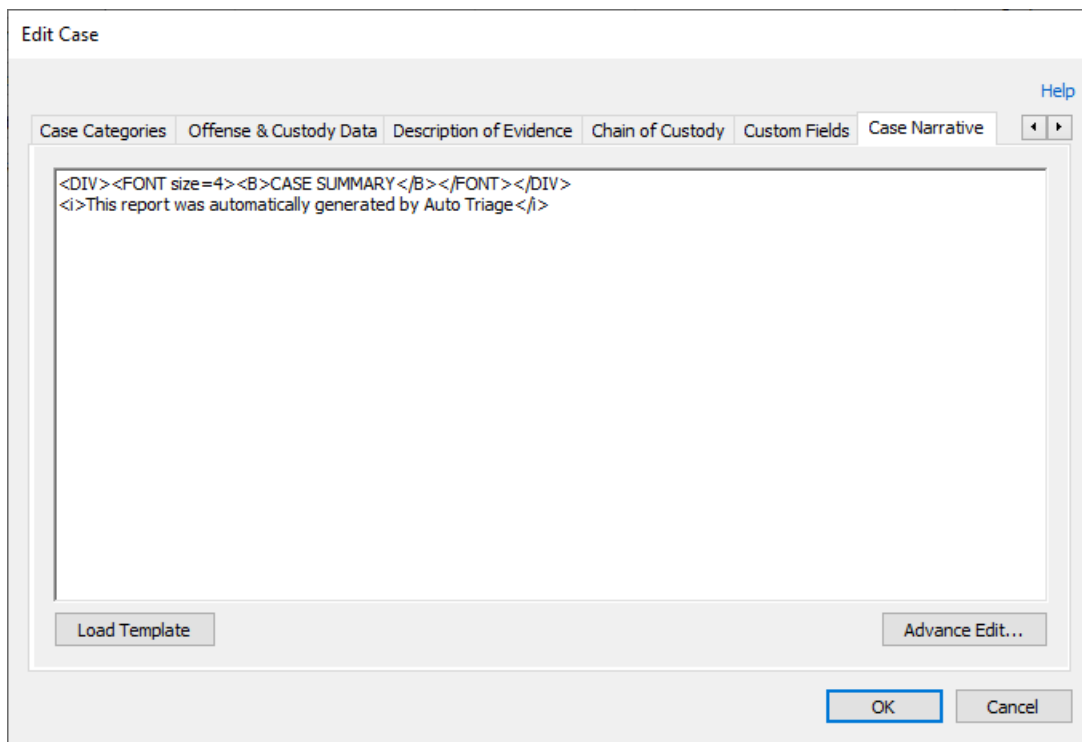
Custom 2 |

Note: Custom Fields do not appear in the default Reports Templates. Users are required to edit the template if custom fields are required.

OK Cancel

User specified Custom Fields to include in the report for other properties the investigator may want to specify but does not currently exist. Custom Fields do not appear in the default Reports Templates. If custom fields are required, users can edit the templates. Specifically adding `<!-- OSF_CASE_CUSTOMFIELD1_NAME-->` and `<!-- OSF_CASE_CUSTOMFIELD1_VALUE-->` or `<!-- OSF_CASE_CUSTOMFIELD2_NAME-->` and `<!-- OSF_CASE_CUSTOMFIELD2_VALUE-->` to the templates where the fields need to appear.

Case Narrative



The Case Narrative allows the examiner to write their complete case analysis report. Text entered here is included in the generated report. Case Narrative is editable after the case is created.

Load Template

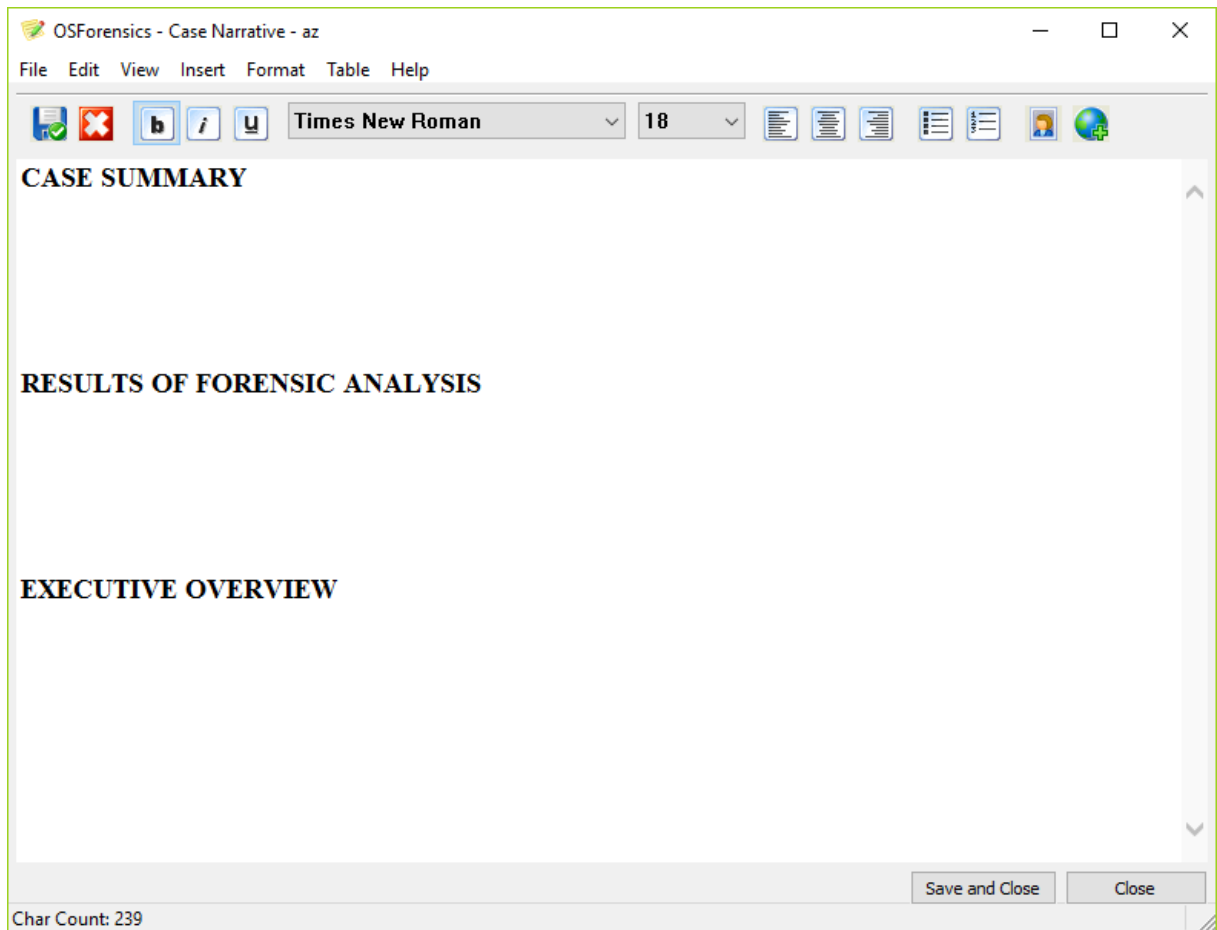
Load an existing saved template to be reused for this case.

Advance Edit...

Opens an advance HTML/Text Editor to write the case narrative.

5.4.2 HTML/Text Editor

The HTML/Text Editor allows for customization of the entered text. Text can be formatted using HTML elements such as lists, tables and images.



Menu



Save and Exit

Save the current contents and exit the editor.

Exit

Exit the editor, if changes were detected, editor will prompt to user to save or discard changes.

Text Style and Size

Allows changing of supported text styles and fonts/fonts sizes.

Text Alignment

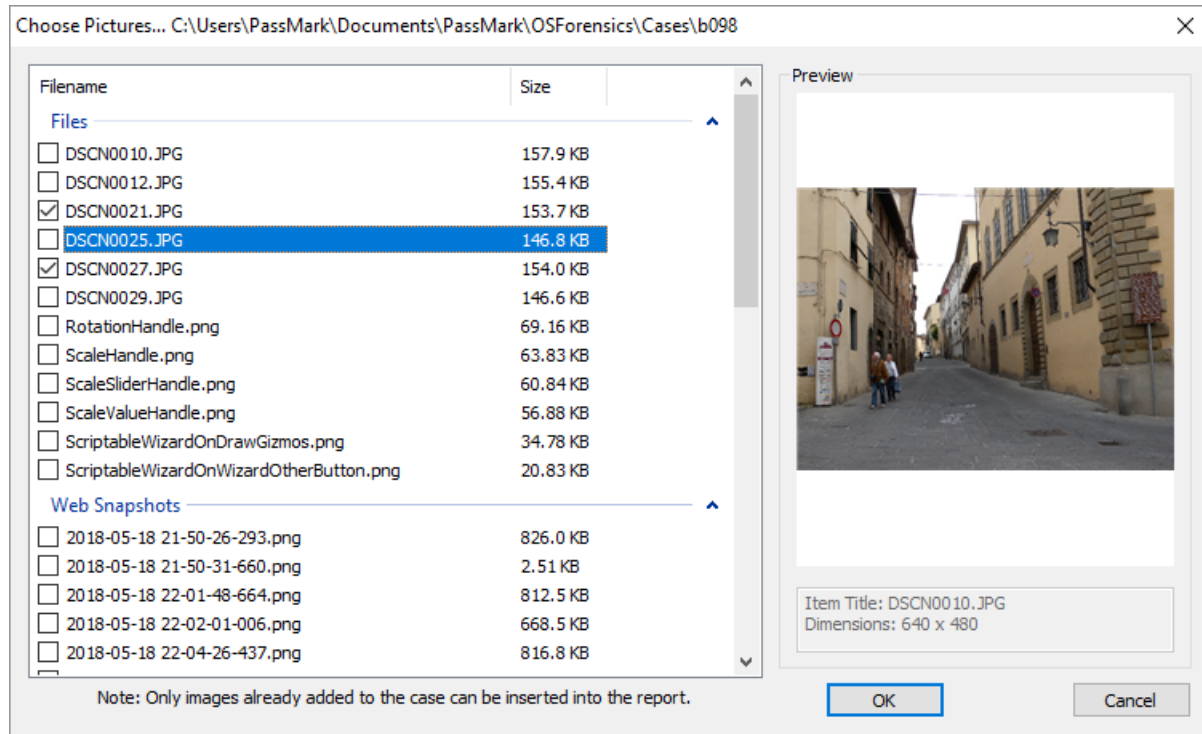
Right, Left or Center justify text in the editor.

Bullets and List

Start a new bullet-ed or numbered list.

Insert Images

Will open a window to allow multiple selection of images already added to case to be included into the document.



5.4.3 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: Extra Information

Style:

Create Redacted Report
 Create Full Length Report
 Include Chain of Custody report
 Include Software Verification

Sections To Include:

Case Materials

<input checked="" type="checkbox"/> Evidence Photos	<input checked="" type="checkbox"/> Forensic Copy Logs
<input checked="" type="checkbox"/> Attachments	<input checked="" type="checkbox"/> Drive Imaging Logs
<input checked="" type="checkbox"/> External Reports	<input type="checkbox"/> Case Activity Log
<input checked="" type="checkbox"/> Notes	<input checked="" type="checkbox"/> Tagged Items

O/S Artifacts

<input checked="" type="checkbox"/> System Information	<input checked="" type="checkbox"/> Web Server Log Artifacts
<input checked="" type="checkbox"/> User Activity	<input checked="" type="checkbox"/> Registry Artifacts
<input checked="" type="checkbox"/> Login/Passwords	<input checked="" type="checkbox"/> Process/Memory Snapshots
<input checked="" type="checkbox"/> \$JsnJrnl Records	<input checked="" type="checkbox"/> Program Artifacts
<input checked="" type="checkbox"/> Event Log Artifacts	<input checked="" type="checkbox"/> Clipboard Contents

Other Artifacts

<input checked="" type="checkbox"/> Files	<input checked="" type="checkbox"/> Search Results
<input checked="" type="checkbox"/> Deleted Files	<input checked="" type="checkbox"/> Extracted Strings
<input checked="" type="checkbox"/> E-mails	<input checked="" type="checkbox"/> Raw Disk
<input checked="" type="checkbox"/> Web Snapshots	<input checked="" type="checkbox"/> Android Artifacts
<input checked="" type="checkbox"/> Database Records	

Categorized Artifacts


Skip empty sections

Output Location: ...


Encrypt PDF using password

Custom Report Logos [Help](#)


Banner (Recommended Size 375x65)



Small Company Logo (Recommended Size 155x46)



Company Logo (Recommended Size 200x160)



Note: Some logos specified may not be utilized as the various report templates uses different sets of logos.

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.

Create Redacted Report

Links to case items in the report. Does not include images in generated report directory.

Create Full Length Report

Copies case items in report into generate report folder. Links to newly copied items in report folder.

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.

Include Chain of Custody Report

If checked, a Chain of Custody report will be exported along side the standard Case 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. Depending on the report type, not all tags appear in the template. The following table summarizes the HTML comment tags that are recognized by OSForensics and replaced accordingly.

IMPORTANT: If any changes are made to the templates, make sure to keep a backup. Reinstalls and updates may overwrite previous changes.

<!--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_NARRATIVE--> This is the Case Narrative for the case.

<!-- OSF_CASE_OFFENSE--> This is the Offense field for the case.

<!-- OSF_CASE_ANALYSISREQUESTEDBY--> This is the Analysis Requested By field for the case.

<!-- OSF_CASE_SUSPECTINFO--> This is the Suspect's Name.

<!-- OSF_CASE_SEIZEDDATE--> This is the date that the evidence was seized.

<!-- OSF_CASE_SEIZEDSHORTDATE--> This is the date the evidence was seized without timezone information.

<!-- OSF_CASE_LOCATIONOFSEIZURE--> This is the Location of Seizure for the case.

<!-- OSF_CASE_LEGALAUTHORITY--> This is the Legal Authority for Seizure for the case.

<!-- OSF_CASE_SUMMARYOFJOB--> This is the Summary of the Job for the case.

<!-- This table contains all evidence images added to the case
OSF_CASE_EVIDENCEIM
AGES-->

<!-- This table contains all attachments added to the case.
OSF_CASE_ATTACHMEN
TSTABLE-->

<!-- This table contains all notes added to the case.
OSF_CASE_NOTESTABL
E-->

<!-- This table contains all tagged items in the case.
OSF_CASE_TAGGEDITEM
S-->

<!-- This table contains the logs of images acquired using the
OSF_CASE_ACQUIREDIM Drive Imaging module that have been added to the case.
AGES-->

<!-- This table contains the logs of forensic copy operations
OSF_CASE_FORENSICSC that have been added to the case.
OPY-->

<!-- This table contains all external reports that been added to
OSF_CASE_EXTERNALRE the case.
PORTS-->

<!-- This table contains all System Information reports that
OSF_CASE_SYSDINFO--> have been added to the case.

<!-- This table contains all User Activity scan results that have
OSF_CASE_USERACTIVIT been added to the case.
Y-->

<!-- This table contains all File Name Search results that have
OSF_CASE_FILESEARCH- been added to the case.
->

<!-- This table contains all Deleted File Search results that
OSF_CASE_DELETEDFILE have been added to the case.
SEARCH-->

<!-- This table contains all Index Search results that have been
OSF_CASE_INDEXSEARC added to the case.
H-->

<!-- This table contains all Mismatch Search results that have
OSF_CASE_MISMATCHSE been added to the case.
ARCH-->

<!-- This table contains all Program Artifacts lists that have
OSF_CASE_PROGRAMA been added to the case.
RTIFACTS-->

<!-- This table contains all Password retrieval scan results that
OSF_CASE_PASSWORD have been added to the case.
S-->

<!-- This table contains all files added to the case.
OSF_CASE_FILESTABLE-
->

<!-- This table contains all deleted files added to the case.
OSF_CASE_UNDELETETA
BLE-->

<!--OSF_CASE_EMAILS-- This table contains all e-mails that have been added to the
> case.

```

<!-- This table contains all web snapshots that have been
OSF_CASE_WEBSNAPSH added to the case.
OTS-->

<!-- This table contains all registry keys that have been added
OSF_CASE_REGISTRY--> to the case.

<!-- This table contains all ESEDB database records that have
OSF_CASE_ESEDBRECO been added to the case.
RDS-->

<!-- This table contains all SQLite database records that have
OSF_CASE_SQLITERECO been added to the case.
RDS-->

<!-- This table contains all Thumbnail Cache database records
OSF_CASE_THUMBDBRE that have been added to the case.
CORDS-->

<!-- This table contains all process snapshots that have been
OSF_CASE_PROCSNAPS added to the case.
HOTS-->

<!-- This table contains all memory dumps that have been
OSF_CASE_MEMORYDU added to the case.
MP-->

<!-- This table contains all string lists extracted from the
OSF_CASE_STRINGLIST-- internal view er that have been added to the case.
>

<!-- This table contains all p-list properties and values that
OSF_CASE_PLISTRECOR have been added to the case.
DS-->

<!-- This is w here the navigation links to the different sections
OSF_CASE_NAVIGATION of the report shall be placed
-->

<!--OSF_CASE_FOOTER-- This is w here the report footer shall be placed
>

<!--OSF_CASE_LOGO--> This is w here the company logo shall be placed

<!-- This is w here the banner logo shall be placed
OSF_CASE_LOGO_BANN
ER-->

<!-- This is w here the small company logo shall be placed
OSF_CASE_LOGO_COMP
ANY-->

```

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

| th.OSFLists | | | |
|---------------------------|----------------------|-----------------------------|---------------------|
| th.OSFListsTitleCol | th.OSFListsModuleCol | th.OSFListsFilenameCol | th.OSFListsNotesCol |
| 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 | |
| td.OSFListsTitleCol | td.OSFListsModuleCol | td.OSFListsFilenameCol | td.OSFListsNotesCol |

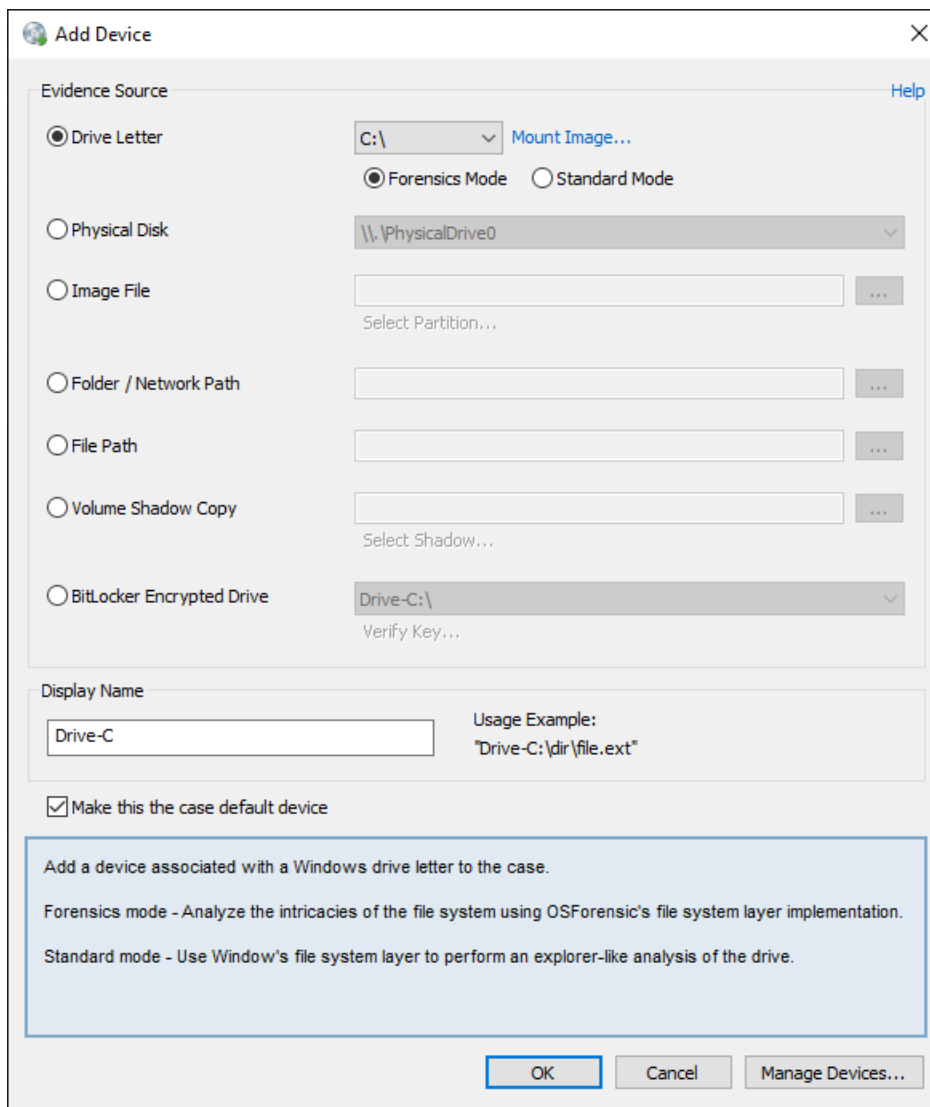
Files table

| th.OSFFiles | | | |
|-----------------------------|--------------------------------------|---|---|
| th.OSFFilesTitleCol | th.OSFFilesFilenameCol | th.OSFFilesFilepathCol | th.OSFFilesNotesCol |
| 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. |
| td.OSFFilesTitleCol | td.OSFFilesFilenameCol | td.OSFFilesFilepathCol | td.OSFFilesNotesCol |

The other tables follow a similar naming convention.

5.4.4 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).



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 Windows 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 an entire physical disk or partition attached to the 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.

If the entire physical disk is added to the case, the contained partitions appear as subfolders of the device as shown below.

If recovered partitions are found on the disk, they can also be added to the case.

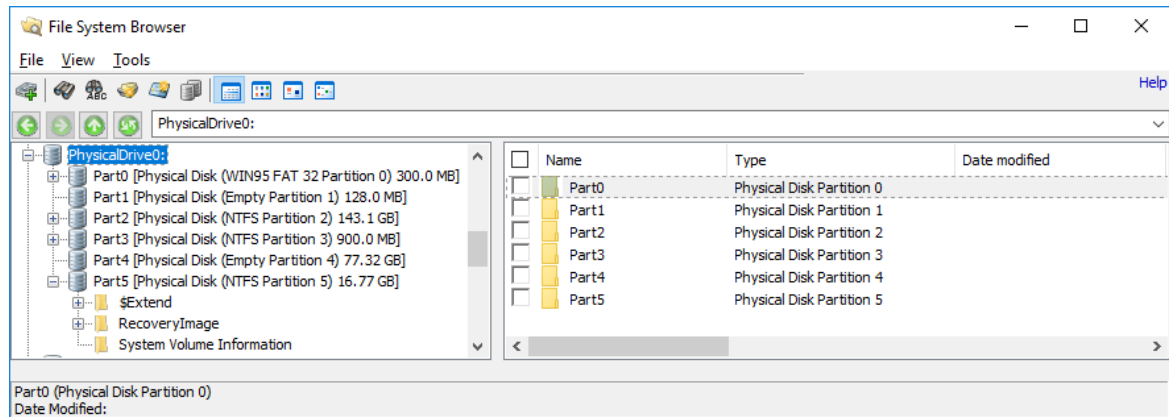
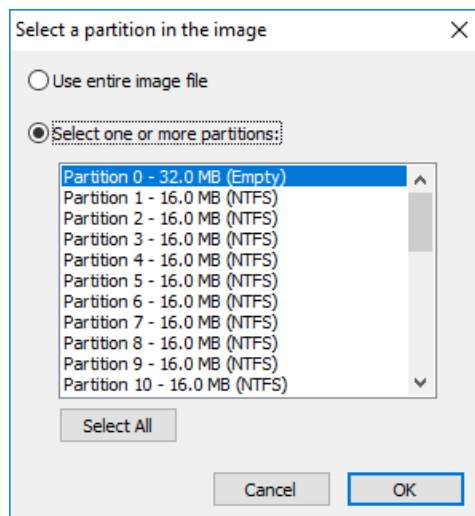


Image File

Add an image file of a physical disk or partition to the case. The image file can contain a single volume or multiple partitions under a supported partition scheme. 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.*

To add individual partitions to the case, click on the 'Select Partition...' link.



One or more partitions can be added to the case by selecting the desired partitions. These partitions shall be added as individual devices to the case.

Recovered partitions, if found on the image file, can also be selected.

If the entire image file is added to the case, it will appear as a single device in the case. Any contained partitions appear as subfolders of the device, similar to adding an entire physical disk.

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.

Manage Devices

Manage all devices that have been added to the case.

5.4.4.1 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)
- Advanced Forensics File Format 4 (.aff4)

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

5.4.4.2 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)
- APFS (MacOS, iOS, tvOS, watchOS, audioOS)***

* 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.

*** APFS support is experimental. Not all functionality supported by the file system may work properly. ZLIB and LZVN compression are supported. Encryption is not supported.

5.4.4.3 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)

5.4.4.4 Support for Volume Shadow Copy

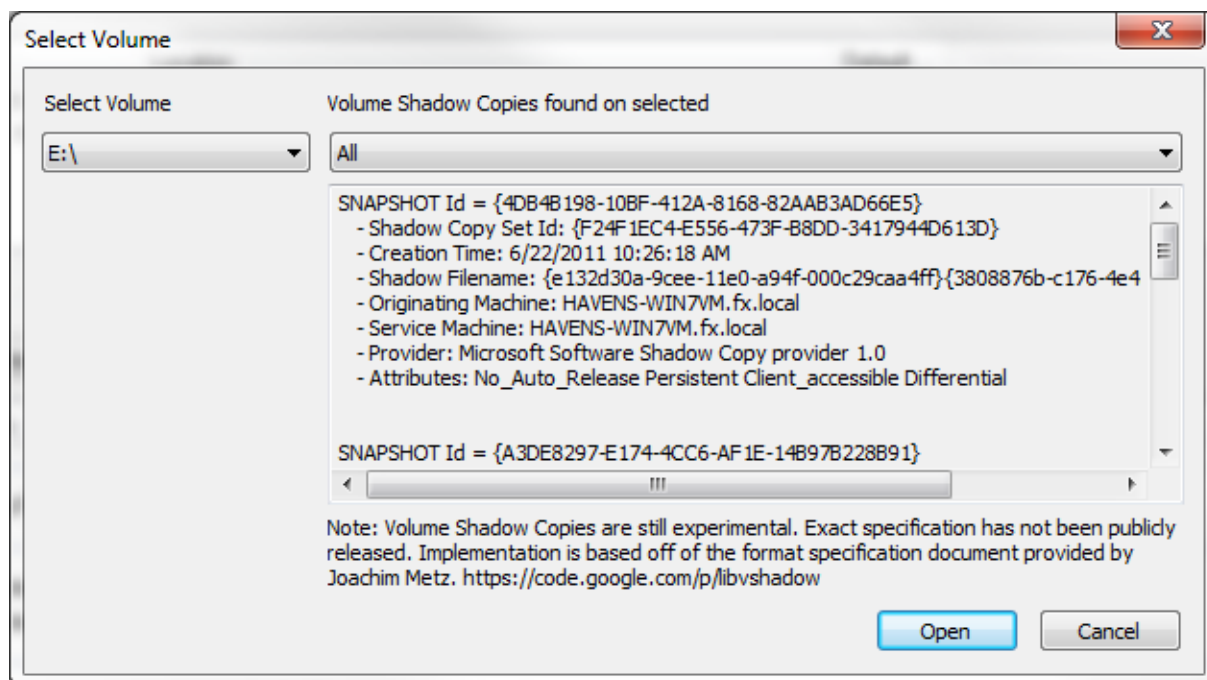
Background

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 known 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.

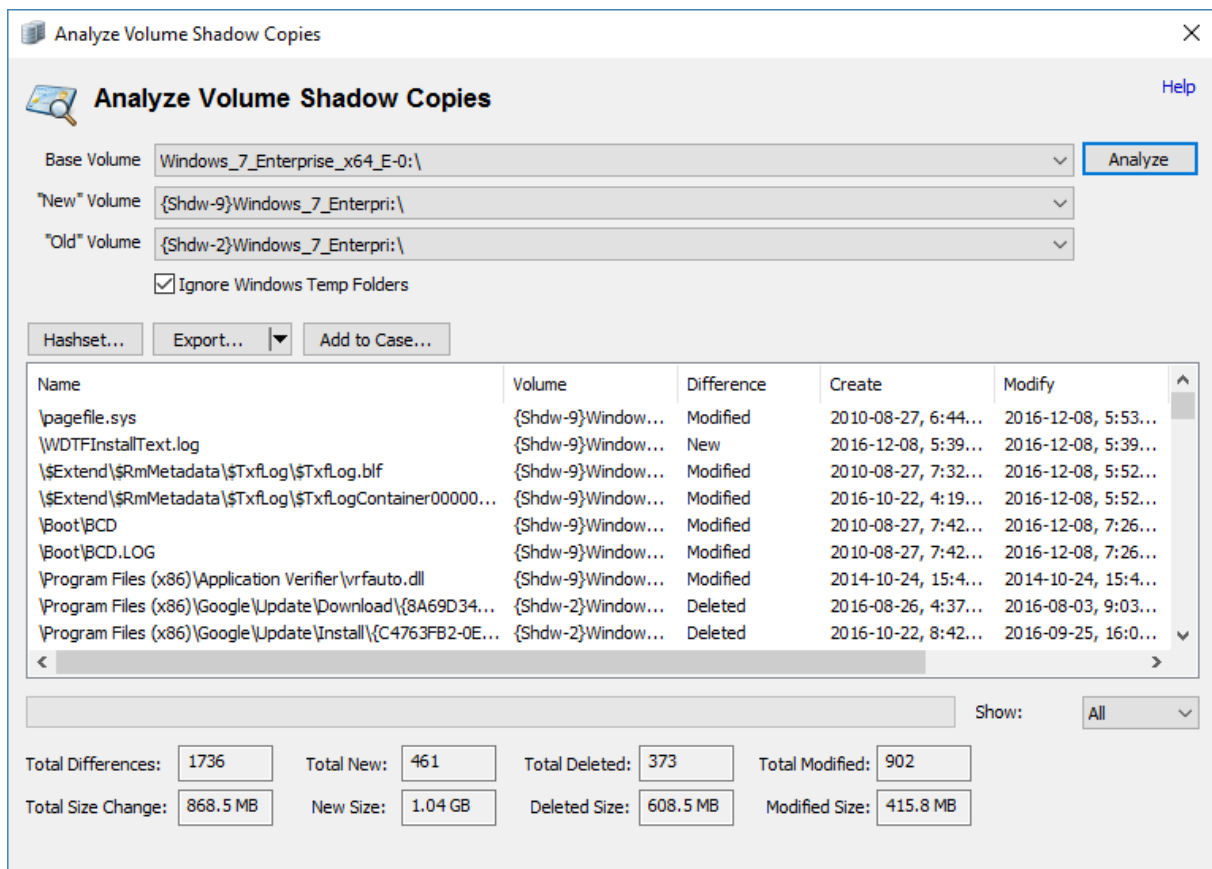
Usage

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).



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.



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.

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

5.4.4.5 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 can be used to unlock a drive:

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

OSForensics supports the following encryption algorithms BitLocker uses to encrypt the drive:

- AES-CBC 128-bit encryption with diffuser
- AES-CBC 256-bit encryption with diffuser
- AES-CBC 128-bit encryption
- AES-CBC 256-bit encryption
- AES-XTS 128-bit encryption
- AES-XTS 256-bit encryption

Usage

To add a BitLocker encrypted drive to the case, the image file or disk must first be added in its 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 [Help](#)

Drive Letter [Mount image...](#)
 Forensics mode Standard mode

Physical Disk

Image File
[Partition: <entire image file>](#)

Folder / Network Path


File Path

Volume Shadow Copy
[Select shadow...](#)

BitLocker Encrypted Drive
[Verify Key...](#)

Display Name 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 [Help](#)

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 bitlocker:\ [Verify Key...](#)

Display Name 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.

Enter BitLocker Key to Unlock Volume

Volume GUID: d69f0c0c-d205-2c4e-9835350151a99441

Description: MSI Bitlocker 5/24/2019

Creation time: Friday, May 24, 2019, 5:30:59

Encryption: AES-XTS 256-bit encryption

Key protectors: Password; Recovery key; Startup key;

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

Password

Recovery Key

Startup Key File (.bek)

...

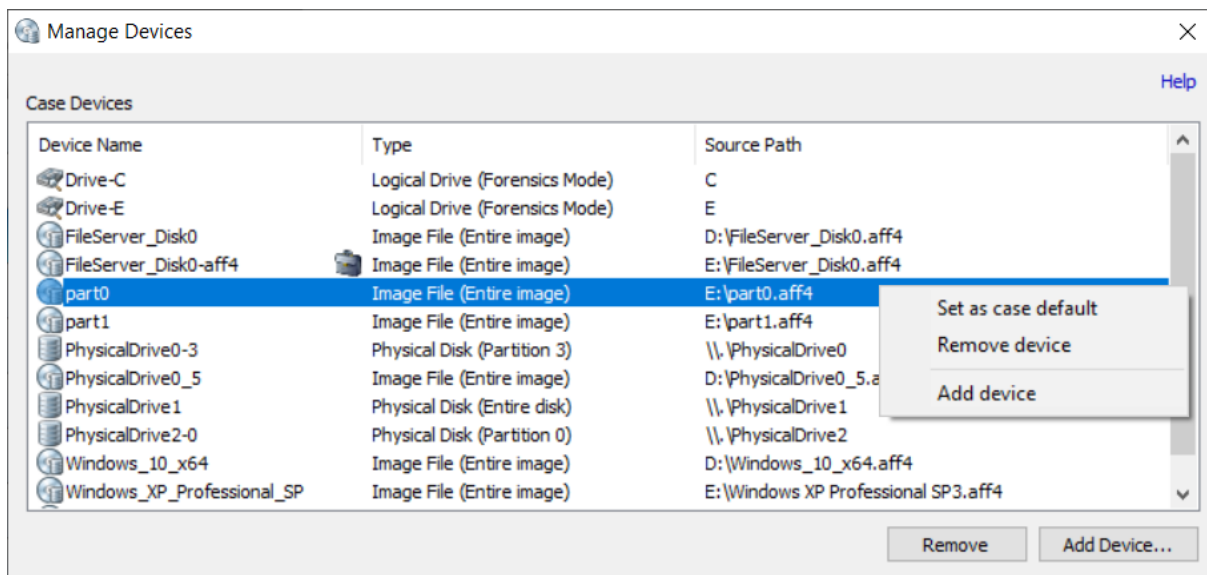
OK Cancel

Select one of the key protectors to use and enter the corresponding key for the drive. The list of key protectors that can be used to unlock the drive is listed in the *Key protectors* field. Key protectors that cannot be used to unlock the drive are disabled.

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.

5.4.5 Manage Devices

The Manage Devices window displays the list of devices added to the case.



Device Name

The name used to reference the device

Type

One of the following devices types: Image File, Logical Drive, Physical Disk, File System Path (UNC), Volume Shadow, Bitlocker-encrypted Drive

Source Path

The path of the source image, disk or path backing the device

Usage

Add Device...

Add a new storage device to the case.

Remove

Remove the selected devices from the case. *Note: Any paths that refer to the device name (eg. tags) would no longer be valid.*

Right-Click Menu

Set as case default

Specify the selected device as the case default drive

Remove device

Remove the selected device from the case. *Note: Any paths that refer to the device name (eg. tags) would no longer be valid*

Add Device...

Add a new storage device to the case.

5.4.6 Case Activity Log

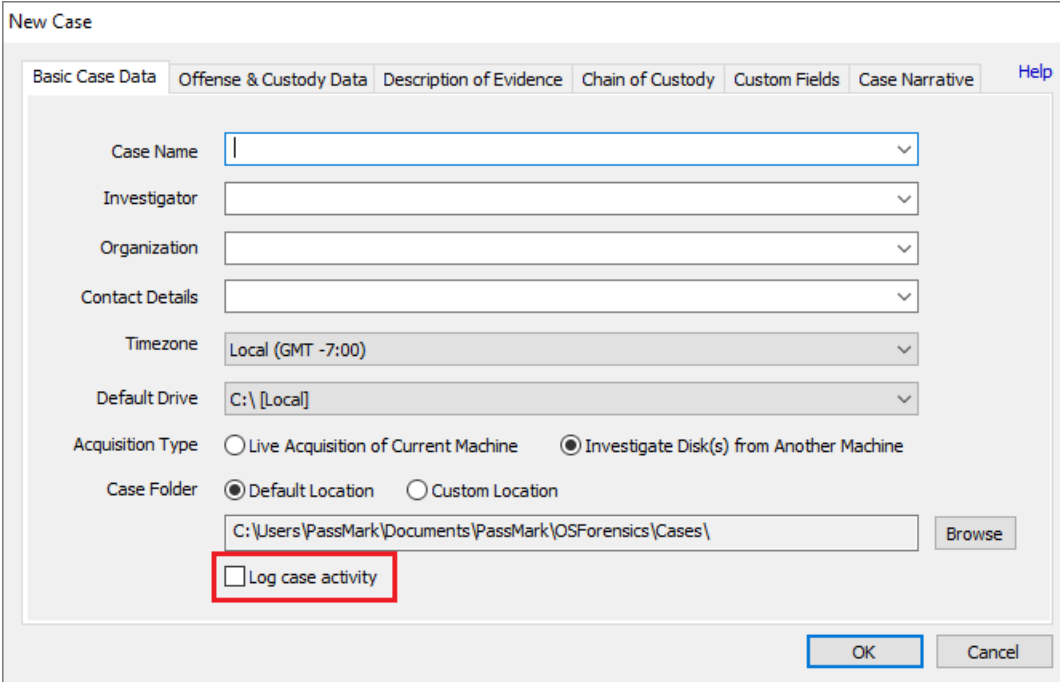
When performing forensic investigations, it is important to maintain an audit trail of the exact activities carried out during the course of the investigation for several purposes including the following:

- 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



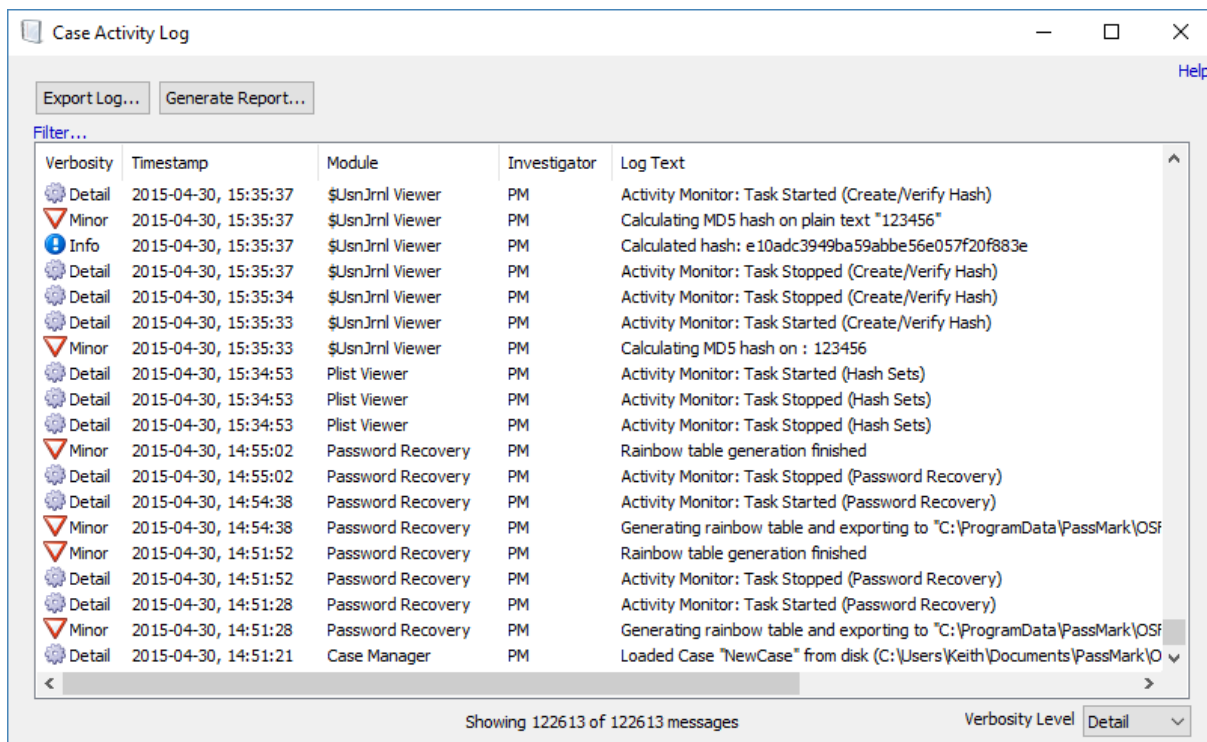
The screenshot shows the 'New Case' dialog box with the following fields and options:

- Case Name: [Empty text box]
- Investigator: [Empty text box]
- Organization: [Empty text box]
- Contact Details: [Empty text box]
- Timezone: Local (GMT -7:00)
- Default Drive: C:\ [Local]
- Acquisition Type: Live Acquisition of Current Machine Investigate Disk(s) from Another Machine
- Case Folder: Default Location Custom Location
- Case Folder Path: C:\Users\PassMark\Documents\PassMark\OSForensics\Cases\ [Browse]
- Log case activity (highlighted with a red box)

Buttons: OK, Cancel

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.



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.

5.4.7 USB Write-Blocking

USB write blocking can be enabled when editing the case details.

The screenshot shows the 'Edit Case' dialog box with the 'Basic Case Data' tab selected. The 'Enable USB Write-block' checkbox is checked and highlighted with a red box. Other visible fields include Case Name (Case 1), Investigator, Organization, Contact Details, Timezone (Local (GMT +10:00) Australian Eastern Standard Time), Default Drive (C:\ [Local]), Acquisition Type (Investigate Disk(s) from Another Machine), Case Folder (Custom Location), and a file path (C:\temp\Case1\).

When enabled OSForensics will change some Windows registry settings so that USB writing will be blocked. USB drives that are already connected will have to be unplugged and reconnected in order for the settings to take effect.

The current USB write status will be displayed on the start page, clicking this icon will toggle the "Enable USB Write-block" setting in the currently opened case.



USB Write:
Disabled

USB writing is disabled (USB Write-block setting is selected)



USB Write:
Enabled

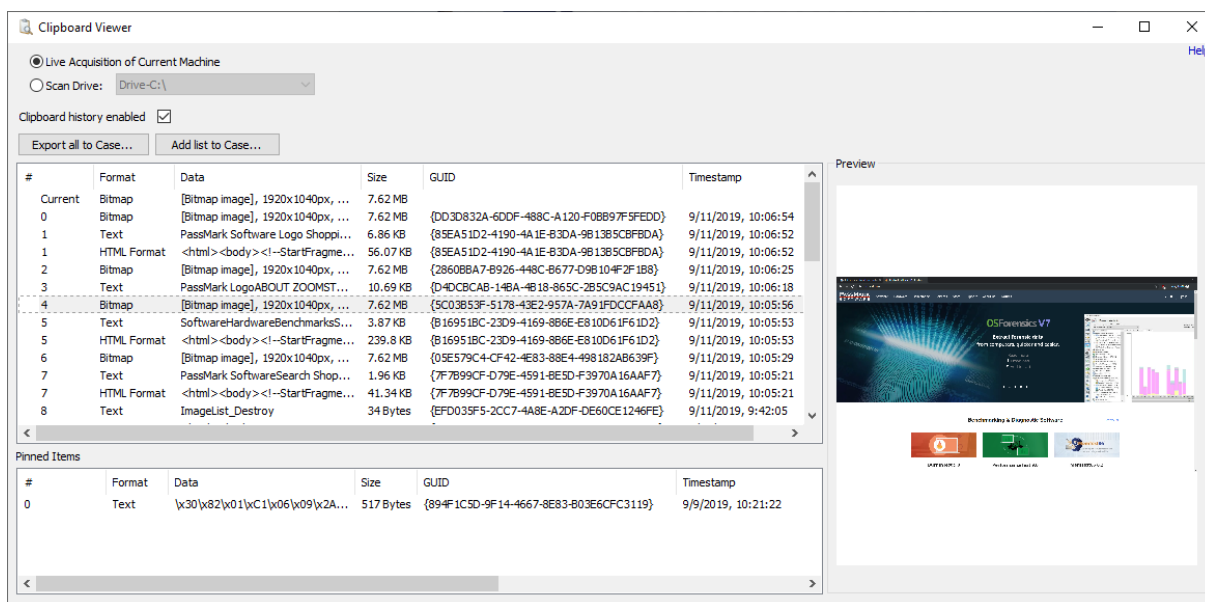
USB writing is enabled (USB Write-block setting is unselected)

When OSForensics exits the registry settings will be returned to what they were before OSForensics changed them.

If for some reason OSForensics exits unexpectedly or is forcibly closed then the settings will not be restored. If this happens the setting can be restored to the required value by opening OSForensics, toggling the USB write to the required setting and then force closing OSForensics using task manager.

5.5 Clipboard Viewer

The Clipboard Viewer allows the investigator to browse the contents stored in the clipboard on the live system, which can contain forensic artifacts of interest such as passwords, images, or contraband files. In newer versions of Windows, a clipboard history is available which can provide as many as 25 items that have been previously added to the clipboard. In addition, if an item is "pinned" to the clipboard, the data will persist on disk even on reboot or shutdown.



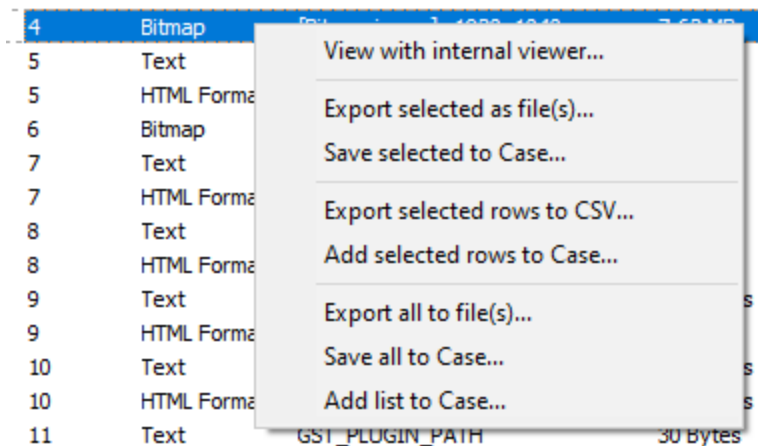
Usage

To view the clipboard contents of the live system, select 'Live Acquisition of Current Machine'. Selecting a disk via 'Scan Drive' is also possible, but only "pinned" items stored on disk shall be displayed.

The data that is currently stored in clipboard is indicated by 'Current'. If clipboard history is enabled, the items in the history shall also be displayed in the list. Select an item to see a preview of its contents on the right pane.

Double-clicking or pressing 'Enter' on a thumbnail opens the internal viewer.

Right-click Menu



View with Internal Viewer...

Opens the clipboard item with OSForensics Viewer to perform a more thorough analysis. *Keyboard shortcut: Enter*

Export selected as file(s)...

Prompts the user to enter a location on disk to save the selected clipboard item(s)

Save selected to Case...

Opens a dialog prompting the user to enter details for exporting selected clipboard item(s) as files to the case

Export selected rows to CSV...

Prompts the user to enter a location on disk to save the list of selected clipboard item(s) to CSV

Added selected rows to Case...

Opens a dialog prompting the user to enter details for exporting a list of selected clipboard item(s) as a CSV file to the case

Export all to file(s)...

Prompts the user to enter a location on disk to save all clipboard item(s)

Save all to Case...

Opens a dialog prompting the user to enter details for exporting all clipboard item(s) to the case

Add list to Case...

Opens a dialog prompting the user to enter details for exporting a list of all clipboard item(s) as a CSV file to the case

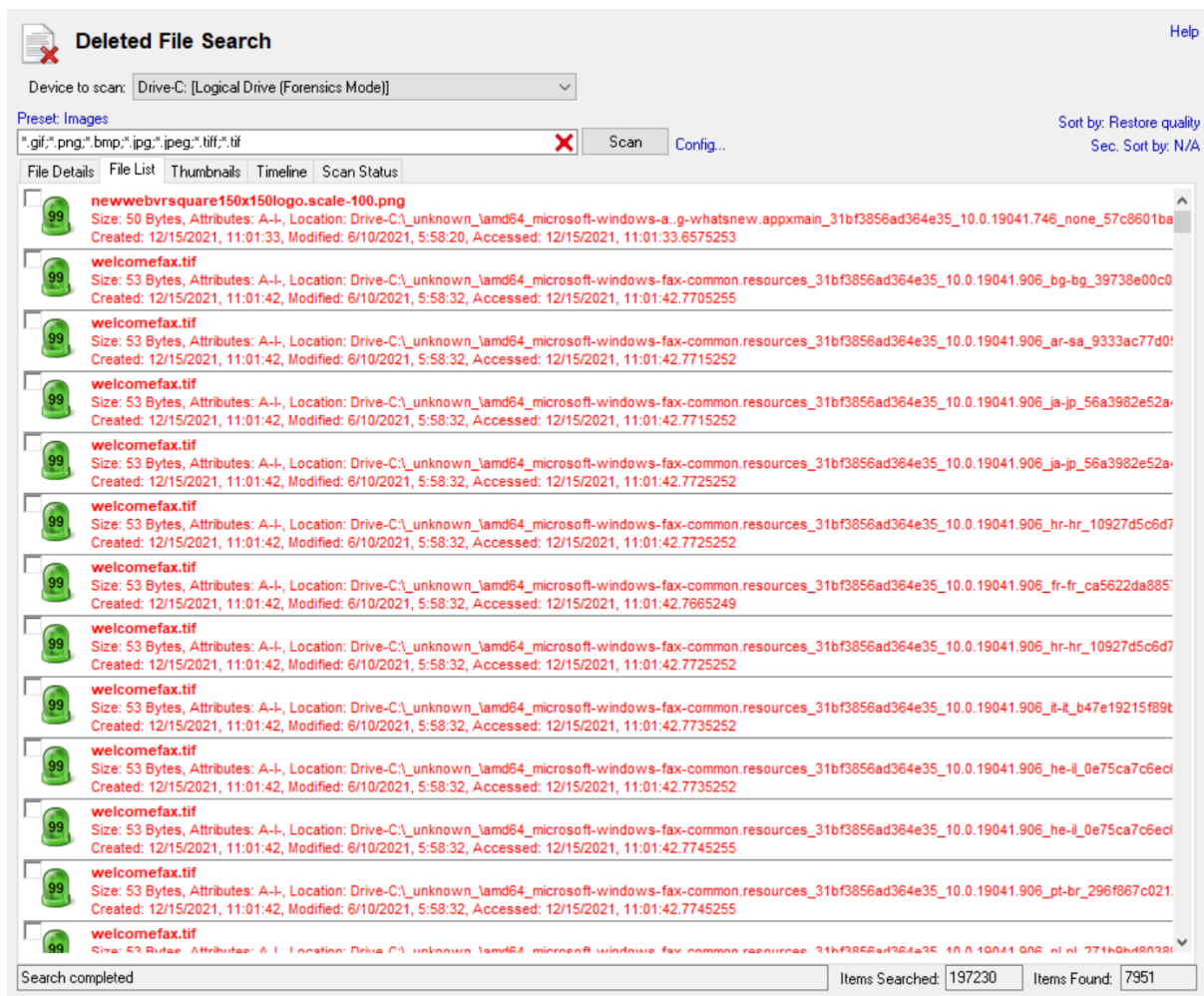
Additional Info

Pinned Items

In newer versions of Windows with clipboard history enabled, items can be pinned so that will persist on disk even on reboot or shutdown. When scanning for drives (ie. non-live acquisition), only pinned items shall be displayed, if available. However, the contents of the pinned item is encrypted on disk and can only be displayed in unencrypted form (in the main list of clipboard items) when logged in as the proper user.

5.6 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.



Basic Usage

A basic deleted file search simply involves entering a search string and selecting a device to scan. 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.

Recovered partitions, if found on the disk, can also be scanned for deleted files.

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

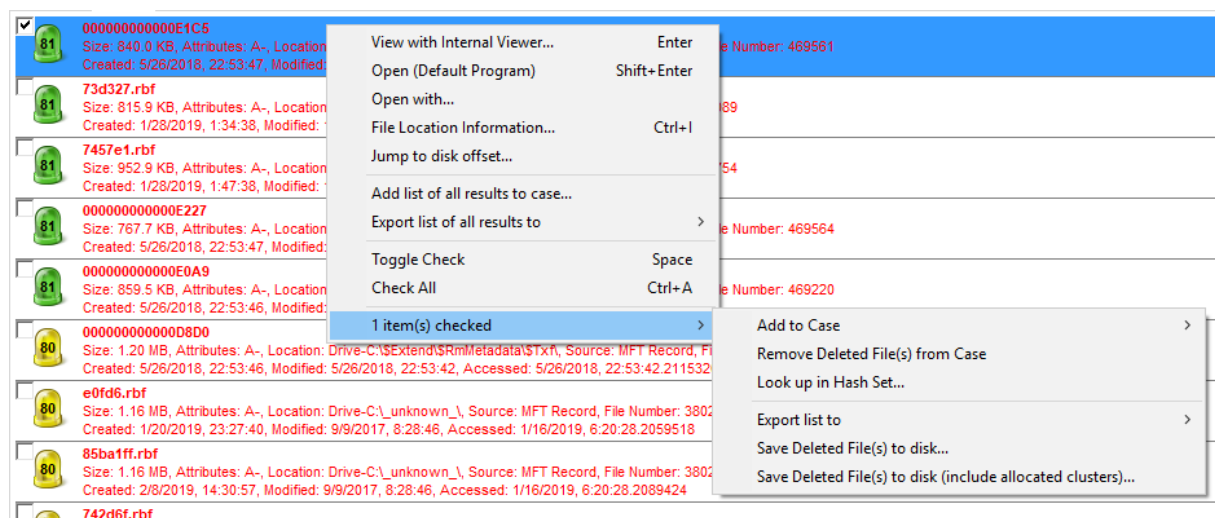
The results of the search are displayed in one of several views, along with a summary of the number of items searched/found. The File List view contains a list of file names, along with the corresponding metadata and a quality indicator between 0-100. A value close to 100 means that the deleted file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

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

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.

n item(s) checked**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.

5.6.1 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](#)

Scan method

Scan file index records
(Default, fast scanning for deleted MFT/FAT/inode file records. Can recover file names/paths)

Carve known file signatures
(Slow, but useful for recovering files from corrupted file systems. Cannot recover file names/paths)

Carve file index records
(Slow, but useful for recovering files from recently quick-formatted volumes. Can recover some file names/paths)

Scan file index records options

Multiple streams only Case Sensitive

Include folders Match Whole Word Only

Carve known file signatures options

Results Filters

Minimum Quality: Mediocre ▼

Disable thumbnails

File Size Limits:

Min KB

Max KB

Scan Method

Specifies the method(s) that will be used to in the deleted file search. The default is for the deleted file search module to search in the Master File Table (MFT) and to perform file carving on the selected disk. If desired, scanning can be set to search the MFT or File Carve only. Note: When enabling 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.

Scan file index records options

Multiple streams only

This option is disabled by default.

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.

Carve known file signatures options

Configure Carving Options

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

Results Filters

Minimum Quality

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

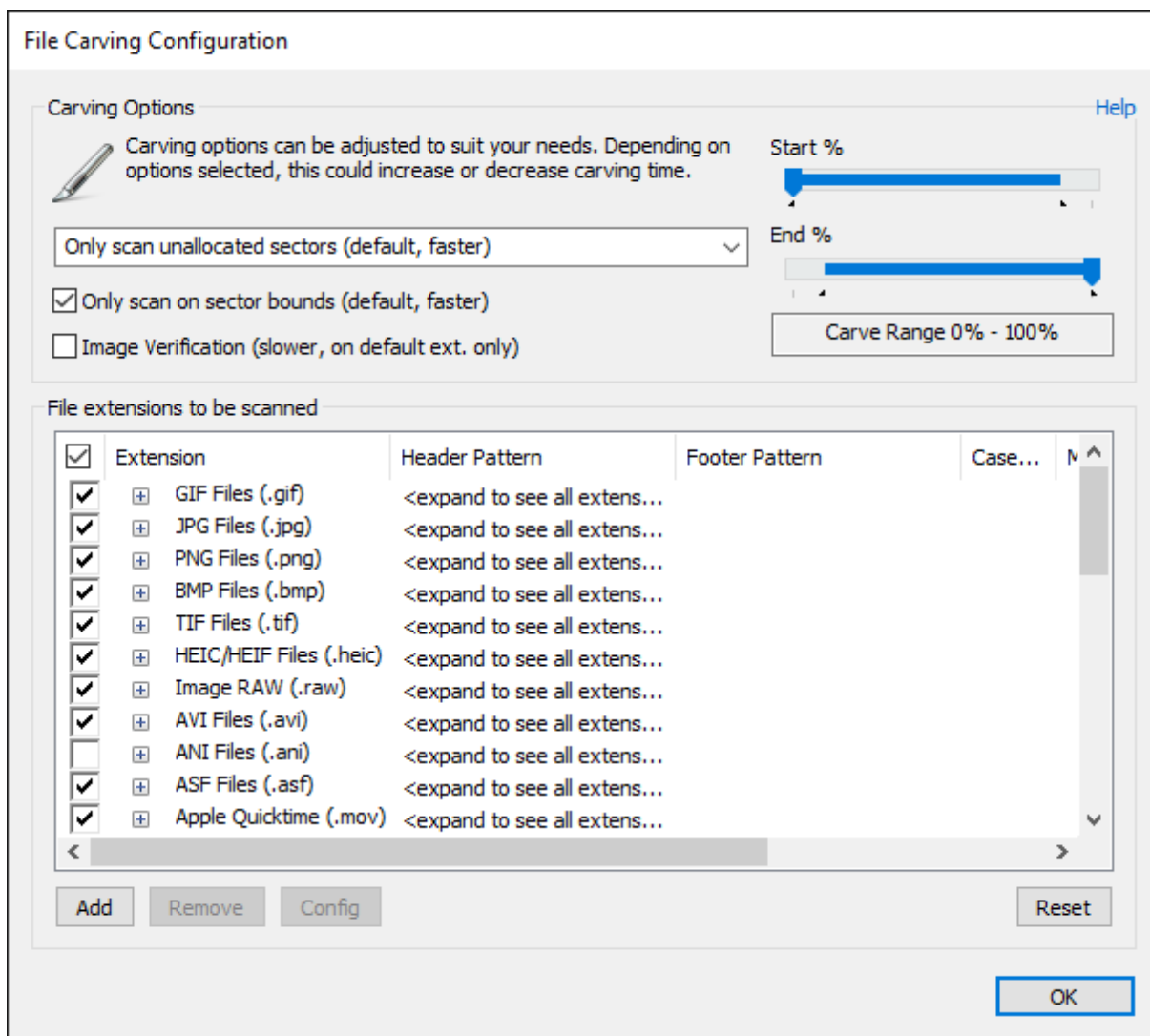
Disable thumbnails

Thumbnails are not automatically generated on the thumbnails tab. Thumbnail generation requires the found deleted files to be scanned and can slow down the recovery process. This option is enabled by default.

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



Only scan unallocated sectors

For FAT and NTFS file systems, OSForensics has the ability to only index the unallocated sectors on the drive. This will reveal files in unused portions 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.

Only scan on sector bounds

With this option enabled, only the beginning bytes of a sector will be used to look for a **header pattern** match. By default, this option is enabled as files are typically only saved to disk on free sectors (the file contents are stored beginning at the start of the sector). By disabling this option, OSForensics will try to look for **header patterns** anywhere within the whole sector. This can be useful for carving for files (e.g. images) that may be embedded within another file (e.g. PDF document). However, this option should be used with caution as it can greatly increase carving time and will likely return many false matches.

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 fails to open the image, the overall score is decreased by 25%.

Range Selection

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

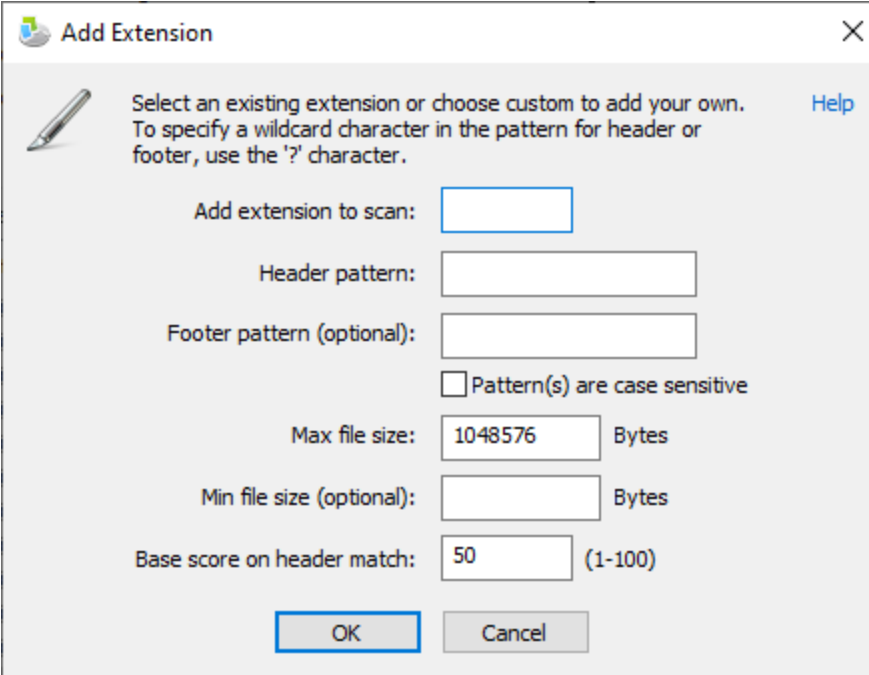
File extensions to be scanned

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 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



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

Add extension to scan:

Header pattern:

Footer pattern (optional):

Pattern(s) are case sensitive

Max file size: Bytes

Min file size (optional): 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.

5.6.2 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 | Source | Quality | Date created |
|------------------------|---|----------|----------------|------------|---------|------------------------------|
| 8{3808876b-c176-4e4... | Drive-E:\System Volume Information\ | 32.00 MB | [Deleted] File | MFT Record | 84 | 1/08/2022, 11:48:22.4863008 |
| ~bittestE00003 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:26.4443... |
| ~bittestE00004 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:26.6941... |
| ~bittestE00005 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:26.8977... |
| ~bittestE00006 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:27.1003... |
| ~bittestE00007 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:27.3350... |
| ~bittestE00008 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:27.5846... |
| ~bittestE00009 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:27.6942... |
| ~bittestE00010 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:27.8033... |
| ~bittestE00011 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:27.9126... |
| ~bittestE00012 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:28.0532... |
| ~bittestE00013 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:28.2876... |
| ~bittestE00014 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:28.5063... |
| ~bittestE00015 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:28.7408... |
| ~bittestE00016 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:28.9287... |
| ~bittestE00017 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:29.1313... |
| ~bittestE00018 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:29.3344... |
| ~bittestE00019 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:29.5378... |
| ~bittestE00020 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:29.7407... |
| ~bittestE00021 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:29.9439... |
| ~bittestE00022 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:30.1625... |
| ~bittestE00023 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:30.4128... |
| ~bittestE00024 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:30.6469... |
| ~bittestE00025 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:30.8501... |
| ~bittestE00026 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:31.0688... |
| ~bittestE00027 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:31.2719... |
| ~bittestE00028 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:31.4752... |
| ~bittestE00029 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:31.6942... |
| ~bittestE00030 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:31.8969... |
| ~bittestE00031 | Drive-E:\System Volume Information\EDP\ | 96.00 MB | [Deleted] File | MFT Record | 69 | 30/05/2022, 15:37:32.1003... |

Search completed Items Searched: 244 Items Found: 238

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 options.

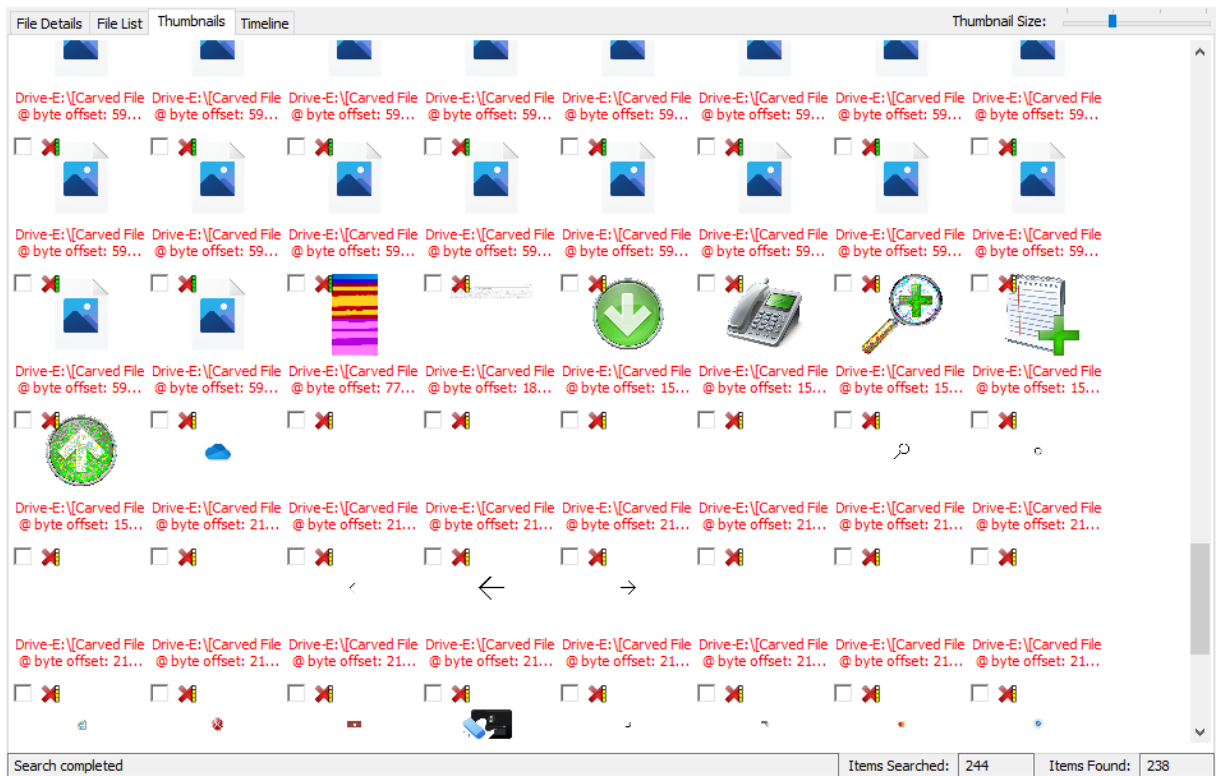
Deleted File List View

| File Details | File List | Thumbnails | Timeline |
|---|---|------------|----------|
|  | 8{3808876b-c176-4e48-b7ae-04046e6cc752} | | |
| | Size: 32.00 MB, Attributes: H-S-A-, Location: Drive-E:\System Volume Information\, Source: MFT Record, File Number: 45
Created: 1/08/2022, 11:48:22, Modified: 1/08/2022, 11:48:22, Accessed: 1/08/2022, 11:48:22.4863008 | | |
|  | ~bittestE00003 | | |
| | Size: 96.00 MB, Attributes: A-, Location: Drive-E:\System Volume Information\EDPI, Source: MFT Record, File Number: 46
Created: 30/05/2022, 15:37:26, Modified: 30/05/2022, 15:37:26, Accessed: 30/05/2022, 15:37:26.6313280 | | |
|  | ~bittestE00004 | | |
| | Size: 96.00 MB, Attributes: A-, Location: Drive-E:\System Volume Information\EDPI, Source: MFT Record, File Number: 47
Created: 30/05/2022, 15:37:26, Modified: 30/05/2022, 15:37:26, Accessed: 30/05/2022, 15:37:26.8349378 | | |
|  | ~bittestE00005 | | |
| | Size: 96.00 MB, Attributes: A-, Location: Drive-E:\System Volume Information\EDPI, Source: MFT Record, File Number: 48
Created: 30/05/2022, 15:37:26, Modified: 30/05/2022, 15:37:27, Accessed: 30/05/2022, 15:37:27.0533157 | | |
|  | ~bittestE00006 | | |
| | Size: 96.00 MB, Attributes: A-, Location: Drive-E:\System Volume Information\EDPI, Source: MFT Record, File Number: 49
Created: 30/05/2022, 15:37:27, Modified: 30/05/2022, 15:37:27, Accessed: 30/05/2022, 15:37:27.2726874 | | |
|  | ~bittestE00007 | | |
| | Size: 96.00 MB, Attributes: A-, Location: Drive-E:\System Volume Information\EDPI, Source: MFT Record, File Number: 50
Created: 30/05/2022, 15:37:27, Modified: 30/05/2022, 15:37:27, Accessed: 30/05/2022, 15:37:27.5220756 | | |
|  | ~bittestE00008 | | |
| | Size: 96.00 MB, Attributes: A-, Location: Drive-E:\System Volume Information\EDPI, Source: MFT Record, File Number: 51
Created: 30/05/2022, 15:37:27, Modified: 30/05/2022, 15:37:27, Accessed: 30/05/2022, 15:37:27.6313548 | | |
|  | ~bittestE00009 | | |
| | Size: 96.00 MB, Attributes: A-, Location: Drive-E:\System Volume Information\EDPI, Source: MFT Record, File Number: 52
Created: 30/05/2022, 15:37:27, Modified: 30/05/2022, 15:37:27, Accessed: 30/05/2022, 15:37:27.7412934 | | |
|  | ~bittestE00010 | | |
| | Size: 96.00 MB, Attributes: A-, Location: Drive-E:\System Volume Information\EDPI, Source: MFT Record, File Number: 53
Created: 30/05/2022, 15:37:27, Modified: 30/05/2022, 15:37:27, Accessed: 30/05/2022, 15:37:27.8504281 | | |
|  | ~bittestE00011 | | |
| | Size: 96.00 MB, Attributes: A-, Location: Drive-E:\System Volume Information\EDPI, Source: MFT Record, File Number: 54
Created: 30/05/2022, 15:37:27, Modified: 30/05/2022, 15:37:27, Accessed: 30/05/2022, 15:37:27.9906743 | | |
|  | ~bittestE00012 | | |
| | Size: 96.00 MB, Attributes: A-, Location: Drive-E:\System Volume Information\EDPI, Source: MFT Record, File Number: 55
Created: 30/05/2022, 15:37:28, Modified: 30/05/2022, 15:37:28, Accessed: 30/05/2022, 15:37:28.2251127 | | |
|  | ~bittestE00013 | | |
| | Size: 96.00 MB, Attributes: A-, Location: Drive-E:\System Volume Information\EDPI, Source: MFT Record, File Number: 56 | | |

Search completed Items Searched: 244 Items Found: 238

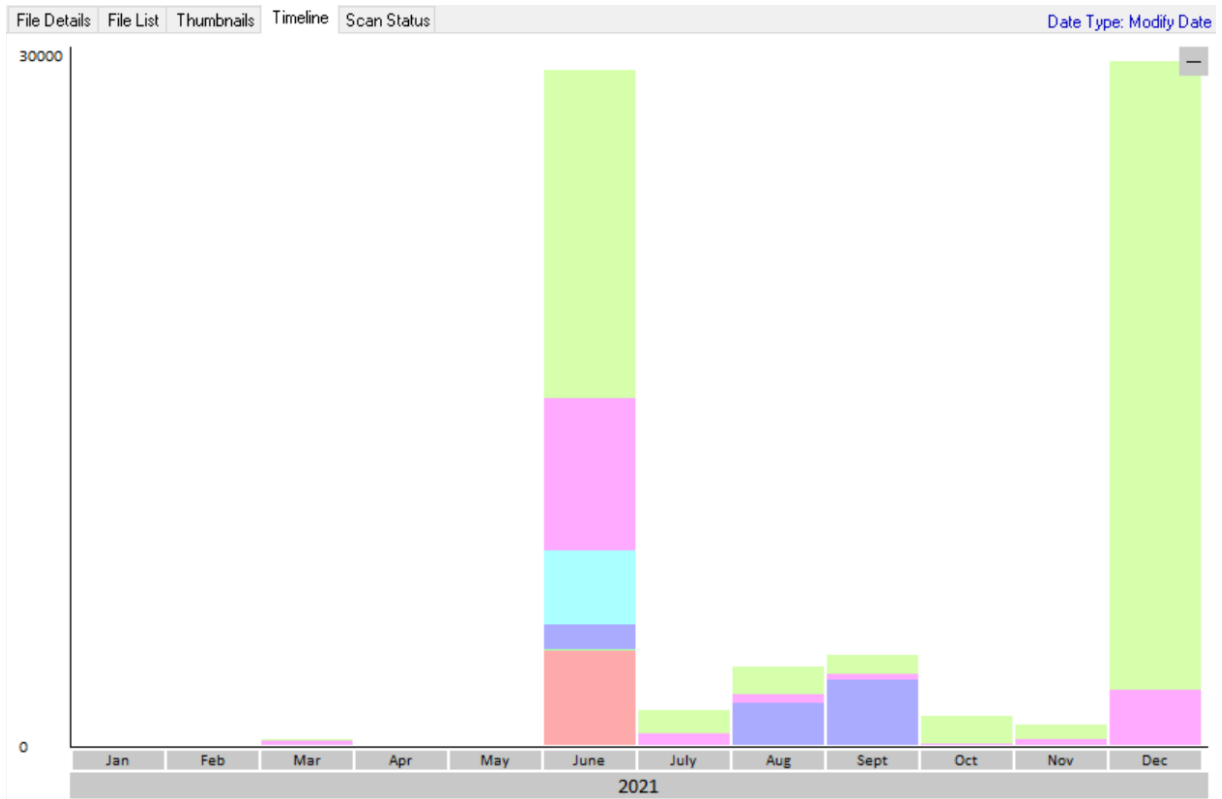
The Deleted File List View displays the search result as a list of file names, along with the corresponding metadata and icon. The results are sorted according to the criteria selected in the Sorting options.

Thumbnails View

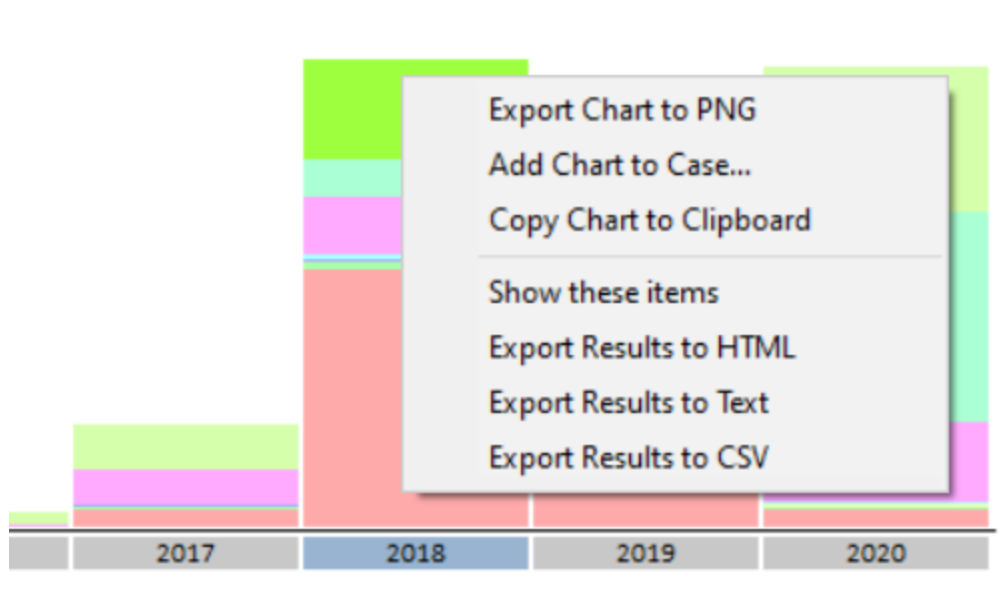


The Thumbnails View displays the search results as a list of thumbnails as well as with its file path. This view is useful when searching for media files, allowing the user to quickly browse through the thumbnail images. The size of the thumbnails can be adjusted using the Thumbnail Size slider bar.

Timeline View



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

5.6.3 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 NTFS or FAT filesystem deleted file in the Deleted Files Search and selecting File Location Information.

The screenshot shows a window titled "Deleted File - Raw Location" with a close button (X) in the top right corner. The window displays the file name "File: helpman_topicinit[4].js". Below the file name is a table with the following data:

| Fragment number | Start (LCN) | Number of clusters | Additional notes |
|-----------------|-------------|--------------------|------------------|
| 1 | 3329010 | 5 | |

Below the table is a graphical representation of the disk partition cluster allocation map and deleted file fragment allocation. The map shows a horizontal bar representing the disk, with a scale from 0 (cluster number) to 7765120. The bar is divided into segments of different colors: green for unallocated disk clusters, dark red for allocated disk clusters, light green for file clusters unallocated, yellow for partial allocation to newer file, and red for file clusters allocated to newer file. The deleted file's fragments are shown as a small green segment within the unallocated disk clusters.

0.0% of the deleted file clusters are currently reallocated to other files.

Key

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

OK

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.

For files that reside on FAT filesystems, only the first cluster fragment is shown and the number of clusters field will be the count of free clusters following the start cluster. If the file is fragmented, then the number of clusters may not match the filesize. FAT file system uses a directory entry for each file and folder allocated on the drive. In the directory entry in FAT it stores the starting cluster only. To access the file, the OS looks in directory finds file and notes the starting cluster. Then it proceeds to the FAT (file allocation table) cluster that corresponds to the starting cluster. The starting cluster entry contains the cluster number of the next cluster. The next cluster entry points to the next cluster and so on until you come to an end of file marker. When you delete a file or folder. It locates the directory entry the file resides in and mark it as deleted and it deletes the FAT chain. That is why you can typically only recover contiguous files in FAT system once a file is deleted.

5.6.4 Deleted Files Technical 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 where 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".

5.7 Drive Preparation

This module provides three 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. Lastly, it can format the drive to either NTFS or FAT32 file system to be ready to be used for investigation.

Drive Preparation
Help

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 privileges in order to accomplish this.

Open Disk Mgr.
Refresh Drive List

| Physical Drive | Progress | Disk Test | Write/Verify Pattern | Format | Status |
|--------------------------------------|----------|-----------|----------------------|--------|---------------------------------|
| 0: Fixed 40.00 GB [C: NTFS, E: NTFS] | 0% | | | | System Drive - cannot be tested |

Drive Preparation Options

Drive Test

Very Quick Test

Write Data Pattern to Entire Drive

Verify Pattern Data pattern (0..255)

Format Drive NTFS

Quick Format

Write Drive Prep Log to Drive Root

Stop on Error Start

Drive List

The Drive list shows 6 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, or file system format as a percentage.
- Disk Test: Shows In Progress when testing or testing pass or failure upon completion.
- Write/Verify Pattern: Shows In Progress when writing or verifying or pass or failure upon completion.
- Format: Shows In Progress when formatting or pass or failure upon completion.
- 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 Preparation Options

Drive Test

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. The random samples stage of the test will continue until about 10% of the disk is tested. 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.

Very quick drive test: When selected, the testing is kept to about 3 minutes.

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.

Format Drive

This action will setup the partition and format the drive. Any previous partitions or file systems that may be present will be removed and replaced with a single volume containing either NTFS or FAT32 file system. FAT32 is only allowed on drives no larger than 2 TB in total size. If "Quick Format" is unselected, then the free disk space for the volume will be written with zeros.

The "Write Drive Prep Log to Drive Root" option will write a short text log of the test and options chosen during preparation of the drive. The Drive log can only be written if the formatting was successful and the volume is accessible.

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.

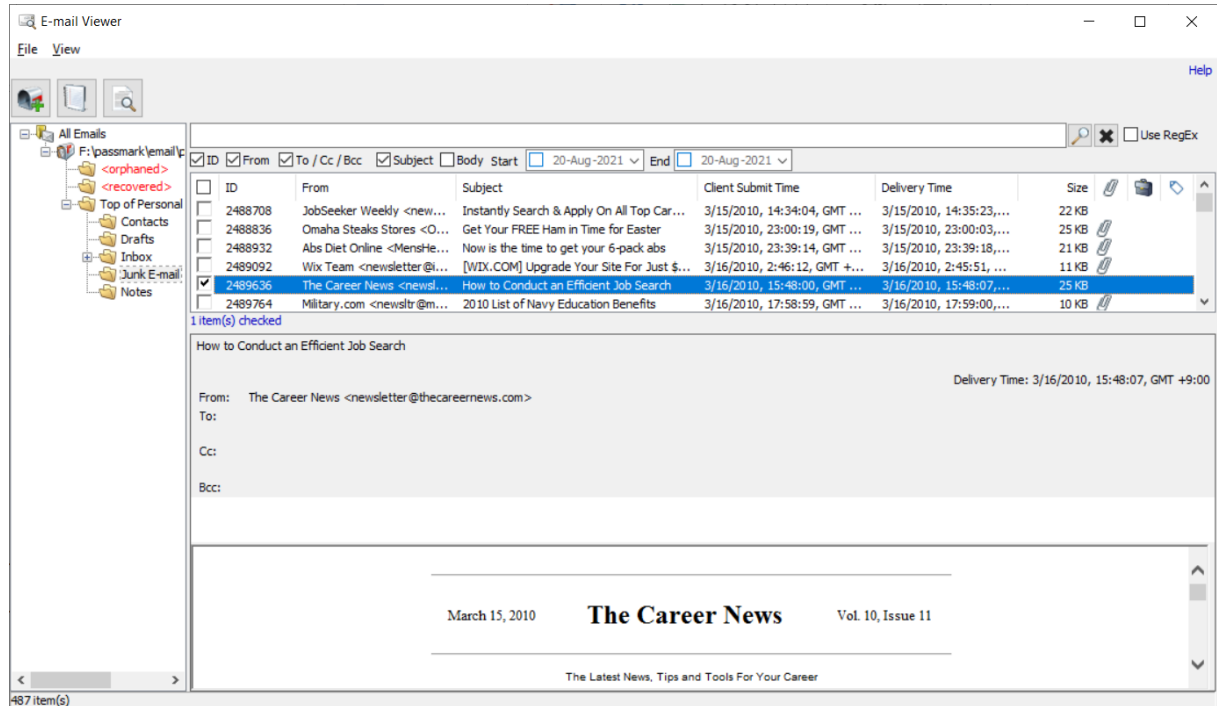
Start/Stop

Start will start the selected operations on the drives selected. The order of the operations if selected is "Drive Test"->"Write Pattern"->"Verify Pattern"->"Format"->"Write Log". You can select one more operations to start continuous one click testing. When "Stop on Error" is enabled. Individual drives will halt their preparation and will not move to their next step if an error occurs in the previous step. Other drives will continue as normal until completion.

Stop will signal a stops to all ongoing operations (e.g. drive test, writing/verifying a data pattern or formatting).

5.8 Email Viewer

The Email Viewer provides a simple yet powerful interface for browsing and analyzing e-mail messages across multiple e-mail files.



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

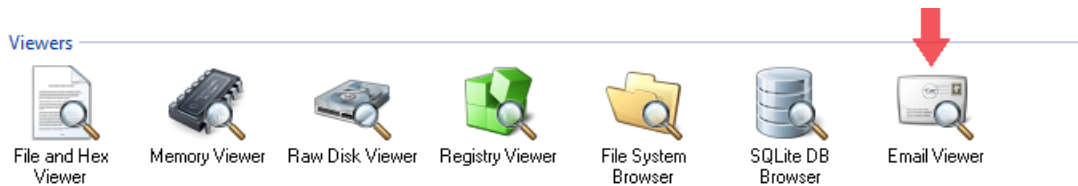
The table below summarizes the main components of the Email Viewer

| 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

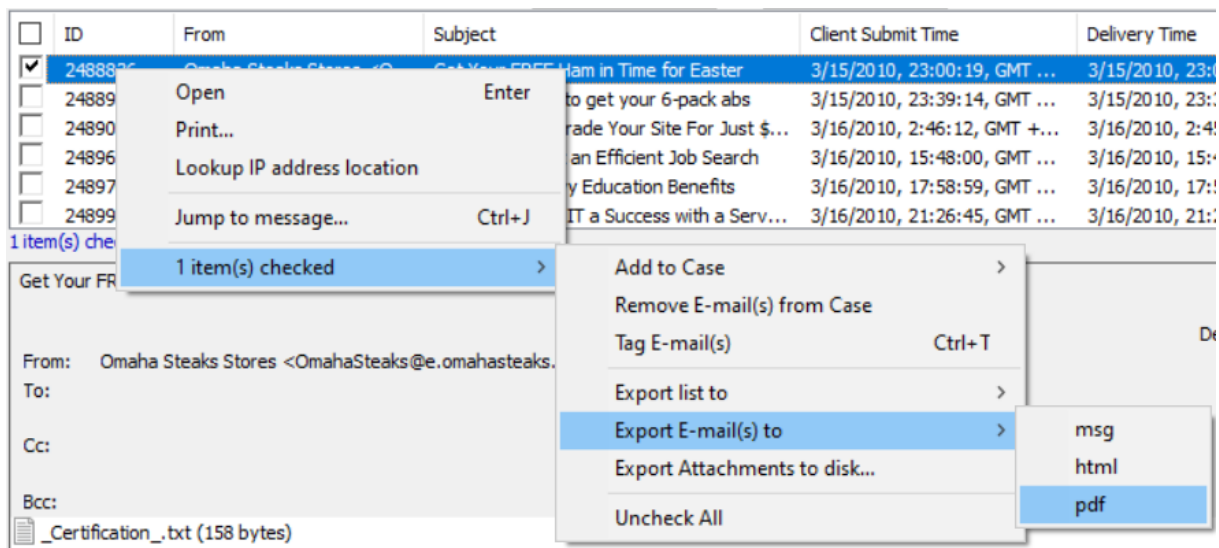
To search for e-mail messages that contain a particular text, enter a search expression in the search bar, specify any additional search parameters and click 'Search'. To use Regular Expressions, check the 'Use RegEx' checkbox. Additionally, e-mail messages can be filtered by when they were sent/received.

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

Opens the message in a separate window.

Jump to message

Jump to a message specified by a message ID.

Print...

Print the e-mail

Lookup IP address location

Parse the e-mail header for IP addresses and plot the geolocation in the Map Viewer.

n Item(s) checked

Add to Case

Add the checked e-mail(s) or list of checked e-mail(s) to the case

Remove File(s) from Case

Remove the checked e-mail(s) from the case

Tag E-mail(s)

Tag the selected e-mail(s) for future reference. *Keyboard shortcut: Ctrl+T*

Export list to

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

Export E-mail(s) to

Exports the checked e-mail(s) to HTML, MSG or PDF file(s)

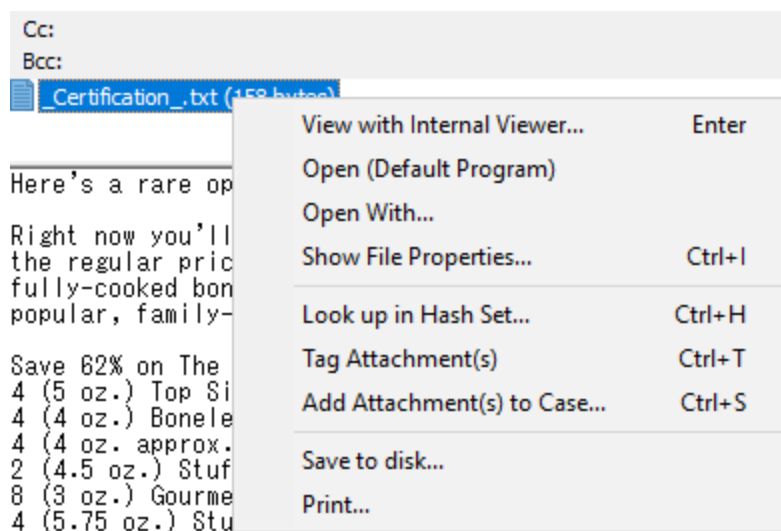
Export Attachments to disk

Exports the attachments of all checked e-mail(s) to a location on disk

Uncheck All

Uncheck all checked e-mail(s)

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*

Tag Attachment(s)

Tag attachment(s) for future reference. *Keyboard shortcut: Ctrl+T*

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...

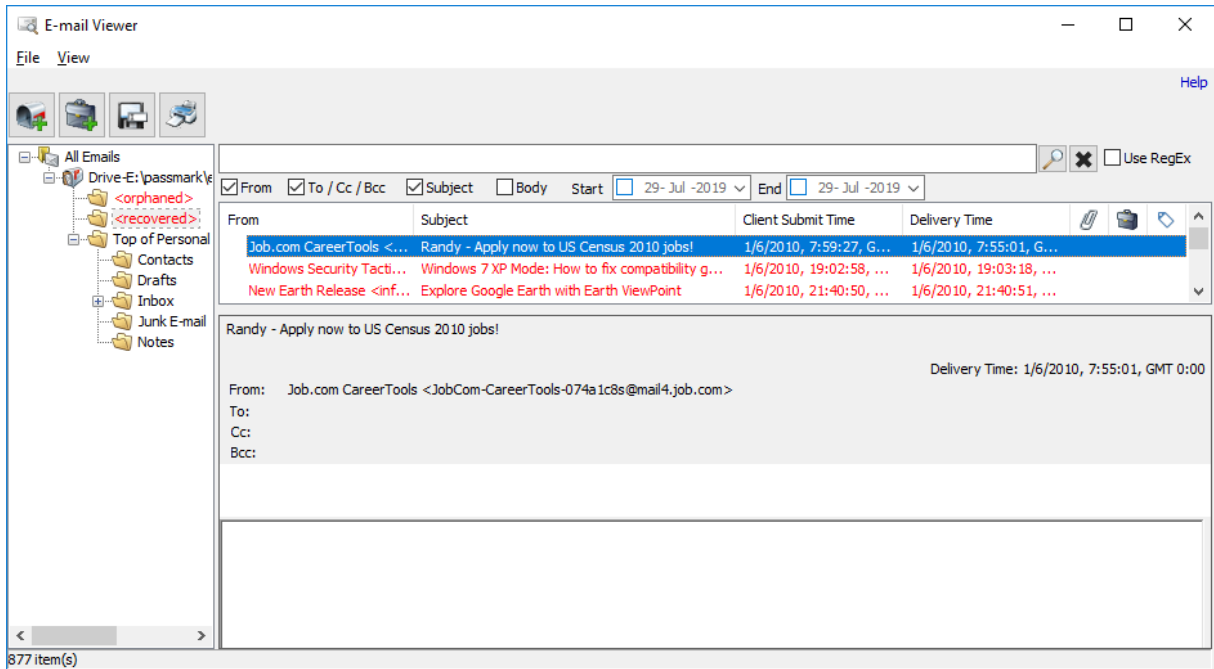
Saves the selected attachment(s) to a location on disk

Print...

Prints the attachment (if applicable)

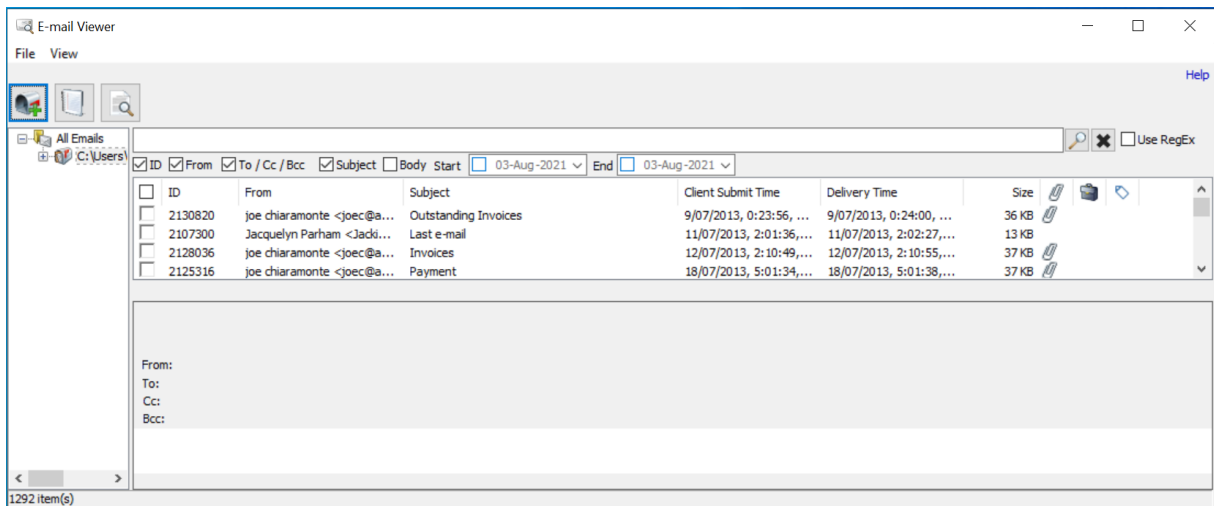
Deleted E-mails

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.



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.

Email Overview



Full Mailbox Overview

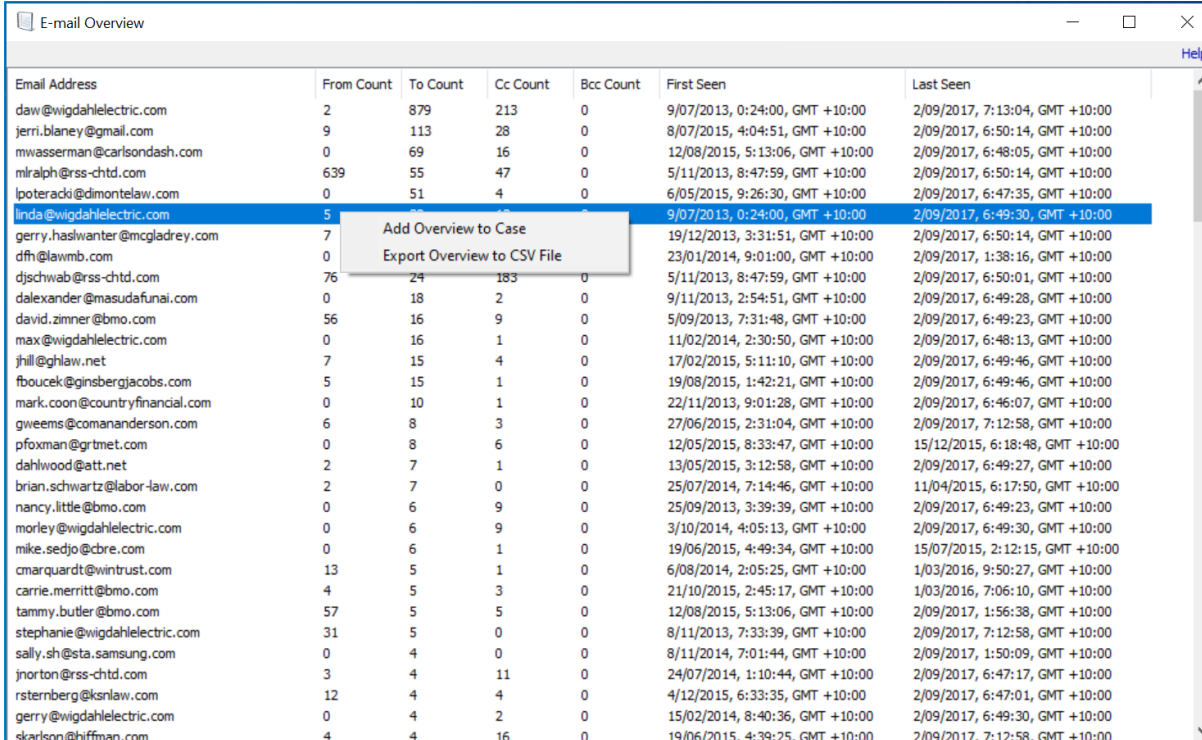
From the main window click this button to generate a summary of all emails currently opened.

If multiple mailboxes are opened they will be combined into one summary.

The summary consists of a table showing the counts of how many times every address has appeared in the corresponding header field, as well as the time of the first and last occurrence of an address.

The table can be sorted by any column by clicking on the columns heading.

You can add the table to the case or export it to a CSV file via the right click menu.



| Email Address | From Count | To Count | Cc Count | Bcc Count | First Seen | Last Seen |
|----------------------------------|------------|-----------|------------|-----------|---------------------------------------|---------------------------------------|
| daw@wigdahlelectric.com | 2 | 879 | 213 | 0 | 9/07/2013, 0:24:00, GMT +10:00 | 2/09/2017, 7:13:04, GMT +10:00 |
| jerri.blaney@gmail.com | 9 | 113 | 28 | 0 | 8/07/2015, 4:04:51, GMT +10:00 | 2/09/2017, 6:50:14, GMT +10:00 |
| mwasserma@carlsondash.com | 0 | 69 | 16 | 0 | 12/08/2015, 5:13:06, GMT +10:00 | 2/09/2017, 6:48:05, GMT +10:00 |
| mlralph@rss-cthd.com | 639 | 55 | 47 | 0 | 5/11/2013, 8:47:59, GMT +10:00 | 2/09/2017, 6:50:14, GMT +10:00 |
| lpoteradi@dimontelaw.com | 0 | 51 | 4 | 0 | 6/05/2015, 9:26:30, GMT +10:00 | 2/09/2017, 6:47:35, GMT +10:00 |
| linda@wigdahlelectric.com | 5 | 24 | 183 | 0 | 9/07/2013, 0:24:00, GMT +10:00 | 2/09/2017, 6:49:30, GMT +10:00 |
| gerry.haslwanter@mcgladrey.com | 7 | 10 | 1 | 0 | 19/12/2013, 3:31:51, GMT +10:00 | 2/09/2017, 6:50:14, GMT +10:00 |
| dfh@lawmb.com | 0 | 2 | 0 | 0 | 23/01/2014, 9:01:00, GMT +10:00 | 2/09/2017, 1:38:16, GMT +10:00 |
| djschwab@rss-cthd.com | 76 | 24 | 183 | 0 | 5/11/2013, 8:47:59, GMT +10:00 | 2/09/2017, 6:50:01, GMT +10:00 |
| dalexander@masudafunai.com | 0 | 18 | 2 | 0 | 9/11/2013, 2:54:51, GMT +10:00 | 2/09/2017, 6:49:28, GMT +10:00 |
| david.zimmer@bmo.com | 56 | 16 | 9 | 0 | 5/09/2013, 7:31:48, GMT +10:00 | 2/09/2017, 6:49:23, GMT +10:00 |
| max@wigdahlelectric.com | 0 | 16 | 1 | 0 | 11/02/2014, 2:30:50, GMT +10:00 | 2/09/2017, 6:48:13, GMT +10:00 |
| jhill@ghlaw.net | 7 | 15 | 4 | 0 | 17/02/2015, 5:11:10, GMT +10:00 | 2/09/2017, 6:49:46, GMT +10:00 |
| fboucek@ginsbergjacobs.com | 5 | 15 | 1 | 0 | 19/08/2015, 1:42:21, GMT +10:00 | 2/09/2017, 6:49:46, GMT +10:00 |
| mark.coon@countryfinancial.com | 0 | 10 | 1 | 0 | 22/11/2013, 9:01:28, GMT +10:00 | 2/09/2017, 6:46:07, GMT +10:00 |
| gweems@comananderson.com | 6 | 8 | 3 | 0 | 27/06/2015, 2:31:04, GMT +10:00 | 2/09/2017, 7:12:58, GMT +10:00 |
| pfoxman@grtmet.com | 0 | 8 | 6 | 0 | 12/05/2015, 8:33:47, GMT +10:00 | 15/12/2015, 6:18:48, GMT +10:00 |
| dahlwood@att.net | 2 | 7 | 1 | 0 | 13/05/2015, 3:12:58, GMT +10:00 | 2/09/2017, 6:49:27, GMT +10:00 |
| brian.schwartz@labor-law.com | 2 | 7 | 0 | 0 | 25/07/2014, 7:14:46, GMT +10:00 | 11/04/2015, 6:17:50, GMT +10:00 |
| nancy.little@bmo.com | 0 | 6 | 9 | 0 | 25/09/2013, 3:39:39, GMT +10:00 | 2/09/2017, 6:49:23, GMT +10:00 |
| morley@wigdahlelectric.com | 0 | 6 | 9 | 0 | 3/10/2014, 4:05:13, GMT +10:00 | 2/09/2017, 6:49:30, GMT +10:00 |
| mike.sedjo@cbre.com | 0 | 6 | 1 | 0 | 19/06/2015, 4:49:34, GMT +10:00 | 15/07/2015, 2:12:15, GMT +10:00 |
| cmarquardt@wintrust.com | 13 | 5 | 1 | 0 | 6/08/2014, 2:05:25, GMT +10:00 | 1/03/2016, 9:50:27, GMT +10:00 |
| carrie.merritt@bmo.com | 4 | 5 | 3 | 0 | 21/10/2015, 2:45:17, GMT +10:00 | 1/03/2016, 7:06:10, GMT +10:00 |
| tammy.butler@bmo.com | 57 | 5 | 5 | 0 | 12/08/2015, 5:13:06, GMT +10:00 | 2/09/2017, 1:56:38, GMT +10:00 |
| stephanie@wigdahlelectric.com | 31 | 5 | 0 | 0 | 8/11/2013, 7:33:39, GMT +10:00 | 2/09/2017, 7:12:58, GMT +10:00 |
| sally.sh@sta.samsung.com | 0 | 4 | 0 | 0 | 8/11/2014, 7:01:44, GMT +10:00 | 2/09/2017, 1:50:09, GMT +10:00 |
| jnorton@rss-cthd.com | 3 | 4 | 11 | 0 | 24/07/2014, 1:10:44, GMT +10:00 | 2/09/2017, 6:47:17, GMT +10:00 |
| rsternberg@ksnlaw.com | 12 | 4 | 4 | 0 | 4/12/2015, 6:33:35, GMT +10:00 | 2/09/2017, 6:47:01, GMT +10:00 |
| gerry@wigdahlelectric.com | 0 | 4 | 2 | 0 | 15/02/2014, 8:40:36, GMT +10:00 | 2/09/2017, 6:49:30, GMT +10:00 |
| skarison@hiffman.com | 4 | 4 | 16 | 0 | 19/06/2015, 4:39:25, GMT +10:00 | 2/09/2017, 7:12:58, GMT +10:00 |



Single Email Overview and Flow Graph

Click this button to generate an overview table and flow graph for a single email address.

The table shows the count of all incoming and outgoing emails sent from a specified email address.

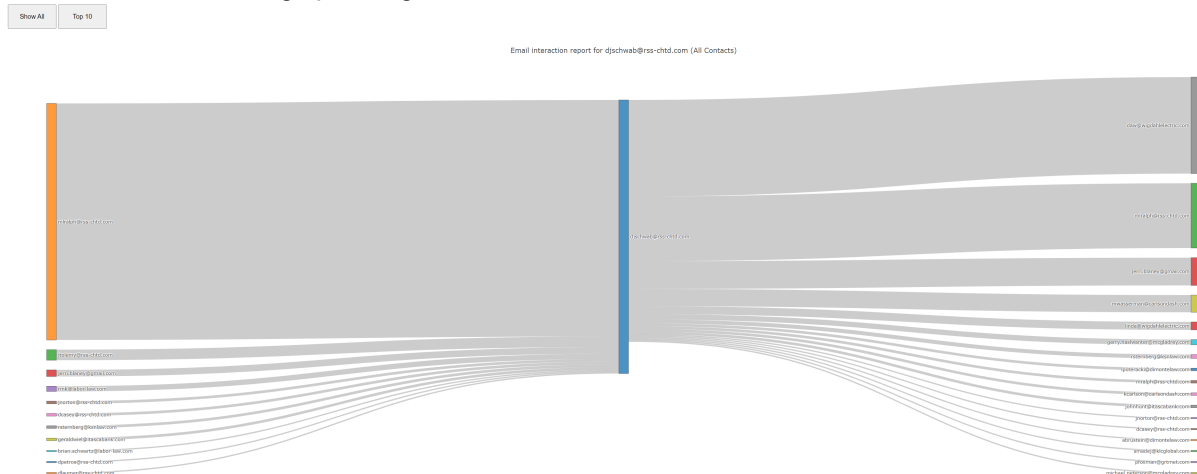
The table and graph can be added to the case via the right click menu.

| Email Address | Sent To djschwab@rss-cthd.com | Received From djschwab@rss-cthd.com |
|--------------------------------|-------------------------------|-------------------------------------|
| mlralph@rss-cthd.com | 179 | 49 |
| jtology@rss-cthd.com | 8 | 0 |
| jerri.blaney@gmail.com | 5 | 21 |
| rmk@labor-law.com | 4 | 0 |
| jnorton@rss-cthd.com | 2 | 1 |
| dcasey@rss-cthd.com | 2 | 1 |
| rsternberg@ksnlaw.com | 2 | 3 |
| geraldwiel@itascabank.com | 2 | 0 |
| brian.schwartz@labor-law.com | 1 | 0 |
| dpetros@rss-cthd.com | 1 | 0 |
| dlaumer@rss-cthd.com | 1 | 0 |
| daw@wigdahlelectric.com | 0 | 73 |
| mwasserman@carlsondash.com | 0 | 13 |
| gerry.haslwanter@mcgladrey.com | 0 | 4 |
| lpoteracki@dimontelaw.com | 0 | 2 |
| abrustein@dimontelaw.com | 0 | 1 |
| smadej@kcgglobal.com | 0 | 1 |
| linda@wigdahlelectric.com | 0 | 6 |
| pfoxman@grtmet.com | 0 | 1 |
| mlralph@rss-cthd.com | 0 | 2 |
| kcarlson@carlsondash.com | 0 | 2 |
| johnhunt@itascabank.com | 0 | 2 |
| michael.peterson@mcgladrey.com | 0 | 1 |

The flow graph will open in your default browser, it shows a visual representation of the email flow into and from a specified address.

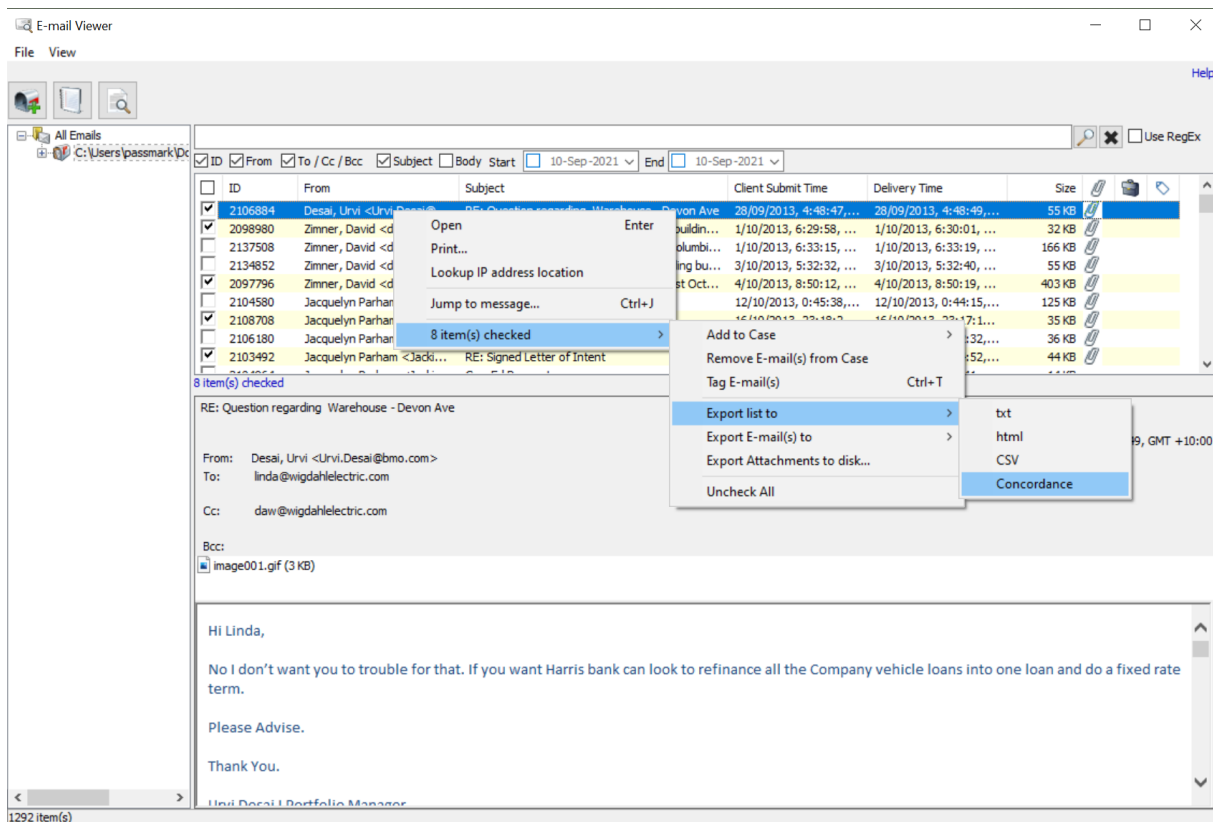
You can limit the graph to show only the top 10 incoming and outgoing addresses using the button in the top left.

You can also zoom the graph using the mouse scroll wheel.



Exporting E-mails to Concordance Load File

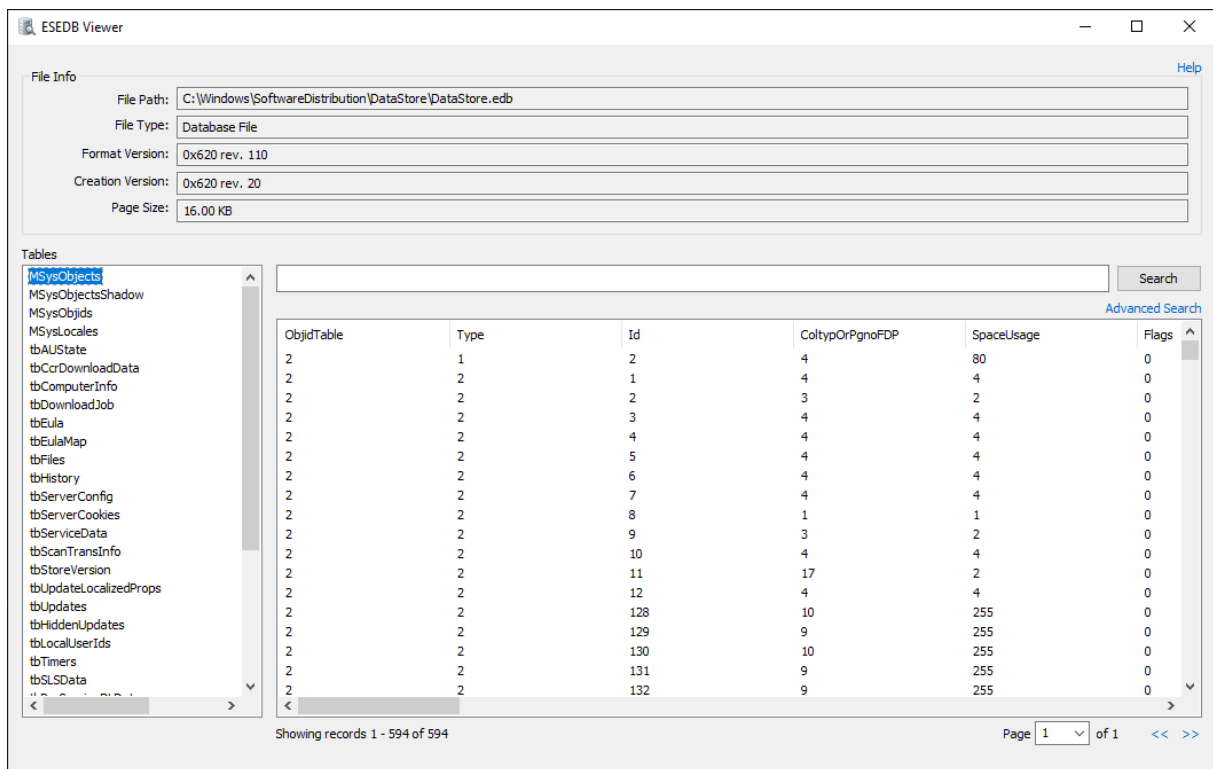
Emails can be exported to a Concordance load file for use in eDiscovery software. Select the emails to be exported and right click to view the menu.



5.9 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



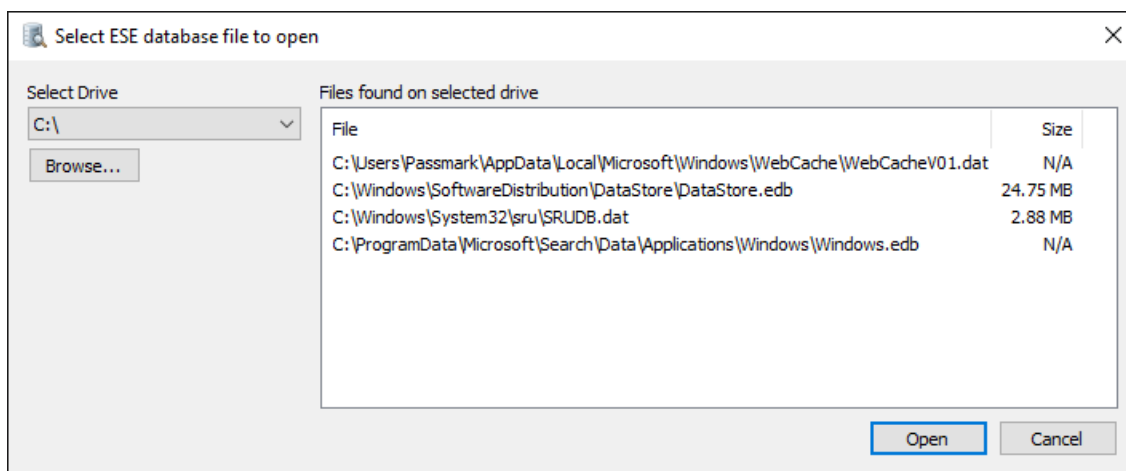
Understanding the ESE Database Viewer

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

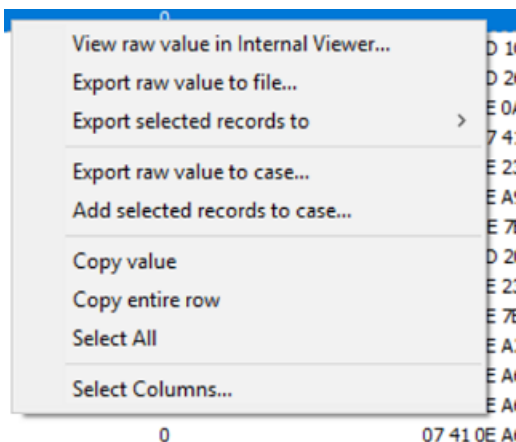
Once the database file is opened, the Tables list is populated with the tables contained in the database. To view the records contained in a particular table, select a table from the Tables list. Known tables with useful data are highlighted in red.

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

Copies the entire row as text to the clipboard

View raw value in Internal Viewer...

Opens the column value under the mouse cursor (szKey, Data etc) in the OSForensics internal viewer.

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

Export raw value to case...

Adds the column value under the mouse cursor (szKey, Data etc) as a .bin file to the exported items for the currently active case.

Add selected records to case...

Adds the list of selected records to the case as a CSV file

Select All

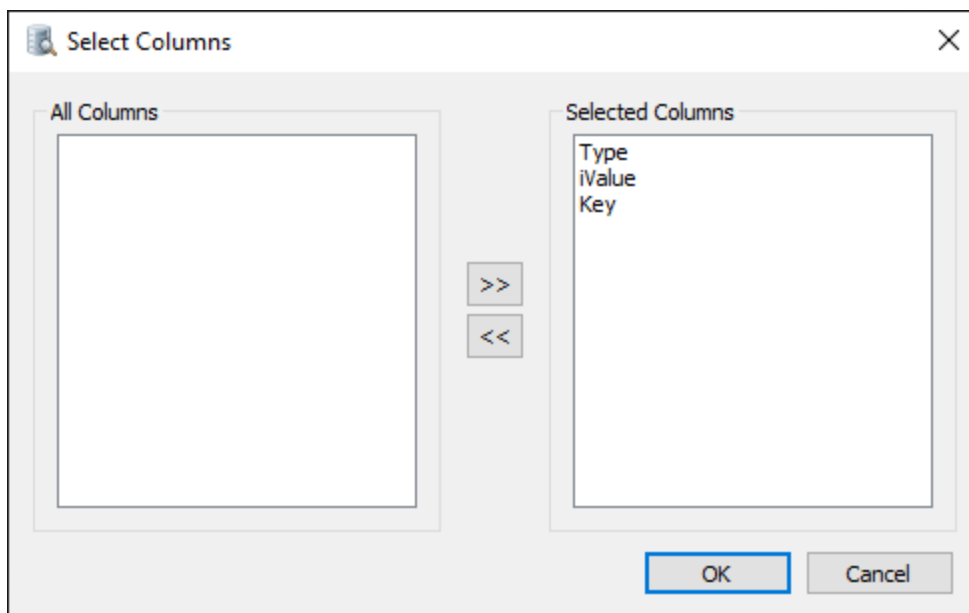
Select all of the records in the ESE Database file

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 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.



5.9.1 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.

Advanced Search

Add Search Criterion

Columns: ObjidTable

From: To:

To enter hexadecimal, prepend number with '0x'

Add

Search Criteria

| Column | Criterion |
|--------|-----------|
|--------|-----------|

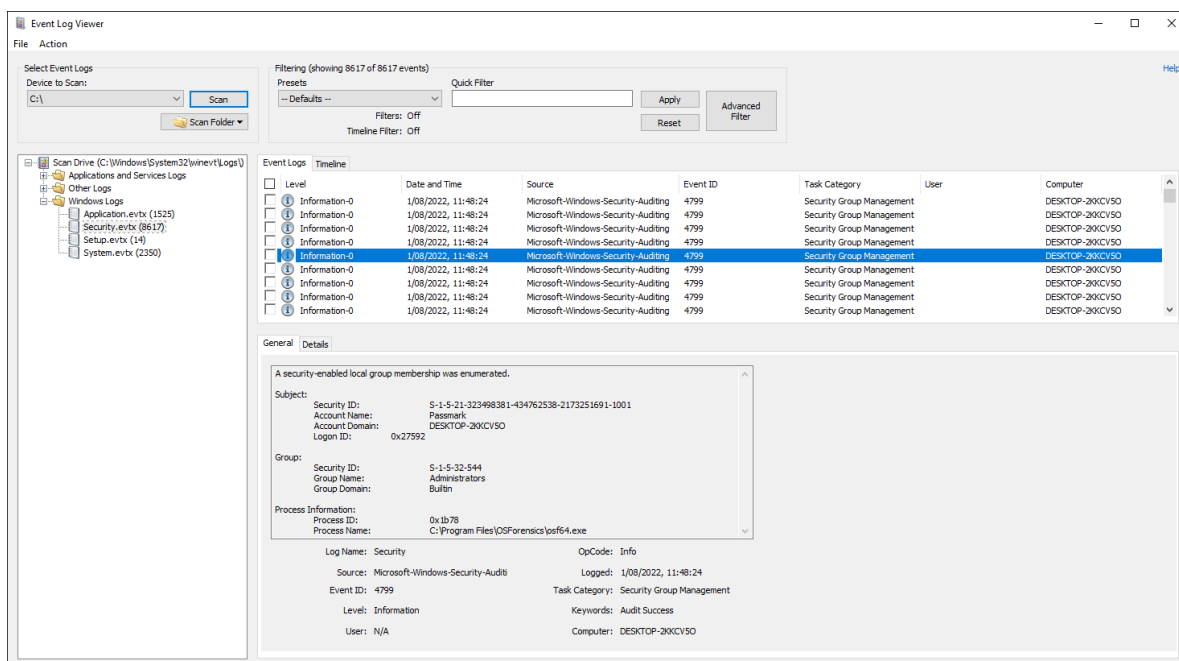
Remove

Search Cancel

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.

5.10 Event Log Viewer

The Event Log Viewer allows users to view and examine event logs created by Windows Vista and beyond. It supports event logs with file extension .evt located in the **%System32%\winevt\Logs** directory.



Event Log Viewer

Usage

Scan Drive

To scan Windows Event Log files, select a Drive from the drop-down list and click 'Scan'. OSForensics Event Log Viewer will search the default **%System32%\winevt\Logs** directory for event log files.

The found event log files will be listed on the left-hand tree-view pane with the file name followed by a number in brackets showing the number of logs in that file.

The tree-view items are grouped into four different sections "Applications and Services Logs", "Windows Logs", "Archived Logs" and "Other Logs". The grouping is done based on the file names.

Note that when searching Event Log files in the Scan process, it only checks the file extension .evtx of the files in the directory, it does not verify whether or not the file is a 'true' Event Log file (e.g. ABC.txt renamed as ABC.evtx).

Scan Folder

To scan a folder, select a folder to scan by clicking Scan Folder button in the main dialog or from the top menu.

Add Log

To add an event log file, select a file to open by clicking Add Log button in the main dialog or from the top menu.

View Logs

To view list of logs in the event log file, click one tree-view item on the left-hand pane. After then, you can perform sorting and filtering of the results.

If you click one log item from the list-view, right-bottom preview pane will show the detailed properties of the selected log. Shifting to 'Details' tab allows you to view the XML information of the event.

Filtering

Filtering is where you will spend the most amount of time, culling down voluminous logs to something more manageable. To filter the event logs list, click the 'Advanced Filters' and then add filters by selecting different filter conditions. Once you've selected the conditions click 'Add Filter' to add the filter to the Filters list-view.

Filters are also able to be exported to a file and then imported as required.

Alternatively, you can use 'Quick Filter' to filter the results. The operation of performing Quick Filter is the same as adding an advanced filter with Parameter set as "All Fields", Condition set as "Contains" and the entered keywords as the "Value", which will search against fields including "Level, Date and Time, Source, Event ID, Task Category, User, Computer, Event Record ID and **XML information**".

For investigators, allowing to search through XML message might be very useful and it can be very efficient in some cases.

* Tip: if you're going to search keywords which include XML syntax, please replace the double quotation marks with single quotation marks, such that you could get the desired results. (e.g. <Data Name='LogonType'>7</Data>)

Filter by... option is another way to quickly narrow down the scopes for searches. Right-click on the specific column of a specific event record, you could quickly add a relevant filter to the advanced filtering list.

Event Log Viewer Filter Results

Filters [Help](#)

| Parameter | Condition | Value |
|---|------------|---|
| <input checked="" type="checkbox"/> Date and Time | Date Range | Date Range: From: 1/07/2022 To: 1/08/2022 |
| <input checked="" type="checkbox"/> All Fields | Contains | TEST |

Remove Filter Remove All

Match: All Checked Any Checked

Add Filter

Event ID
=

4624

Add Filter

Date/Time Range

From: 1/07/2022 12:59:06 PM

To: 1/08/2022 12:59:06 PM

Import Export OK

Adding filters

OSForensics Event Log Viewer

File Action

Select Event Logs
Drive: Windows_7_Enterprise_x64_E-0:\ Scan Drive Add Log

Filtering (showing 6 of 3734 events)
Presets: Successful Logon Quick Filter: <Data Name="LogonType">7</Data> Apply Advanced Filter
Filters: Active - Match All Reset
Timeline Filter: Off

Event Logs Timeline

| Level | Date and Time | Source | Event ID | Task Category | User | Computer |
|---------------|----------------------|-------------------------------------|----------|---------------|------|-------------------|
| Information-0 | 28/11/2019, 12:53:17 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 12:53:17 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 12:20:20 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 12:20:20 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 10:19:29 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 10:19:29 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |

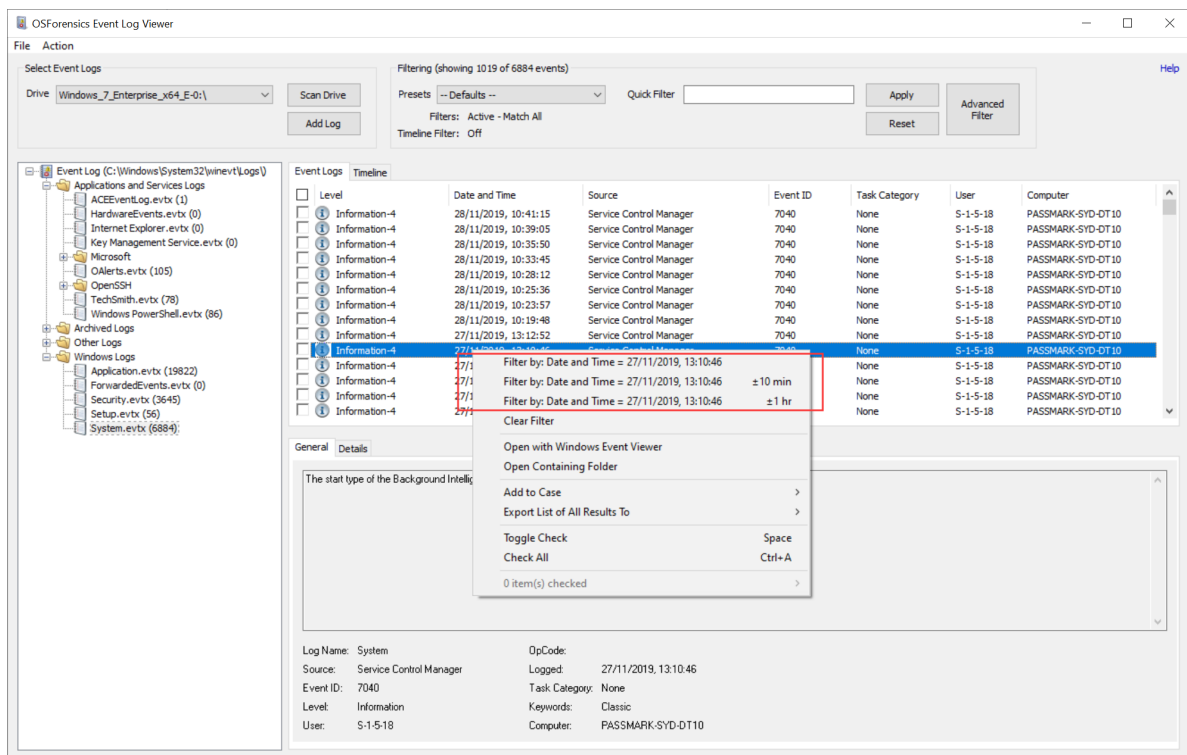
General Details

```

<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2019-11-28T01:53:17.988491400Z" />
<EventRecordID>716698</EventRecordID>
<Correlation />
<Execution ProcessID="664" ThreadID="3448" />
<Channel>Security</Channel>
<Computer>PASSMARK-SYD-DT10</Computer>
<Security />
</System>
- <EventData>
  <Data Name="SubjectUserSid">S-1-5-18</Data>
  <Data Name="SubjectUserName">PASSMARK-SYD-DT$</Data>
  <Data Name="SubjectDomainName">WORKGROUP</Data>
  <Data Name="SubjectLogonId">0x3e7</Data>
  <Data Name="TargetUserSid">S-1-5-21-3060852132-2509393673-3125877351-1002</Data>
  <Data Name="TargetUserName">jayh.passmark@outlook.com</Data>
  <Data Name="TargetDomainName">MicrosoftAccount</Data>
  <Data Name="TargetLogonId">0x1fd208a5</Data>
  <Data Name="LogonType">7</Data>
  <Data Name="LogonProcessName">lsass.exe</Data>
  <Data Name="AuthenticationPackage">ntlmssp</Data>
  <Data Name="WorkstationName">PASSMARK-SYD-DT10</Data>
  <Data Name="LogonGuid">{00000000-0000-0000-0000-000000000000}</Data>
  <Data Name="TransmittedServices"></Data>
  <Data Name="LmPackageName"></Data>
  <Data Name="KeyLength">0</Data>
  <Data Name="ProcessId">0x298</Data>
  <Data Name="ProcessName">C:\Windows\System32\lsass.exe</Data>

```

Quick filter



Filter by...

Presets

Presets are list of predefined filters which can be customized by users. Preset works after a drive has been scanned, and it works on the last scanned drive.

To customize the preset list, there are two steps to do:

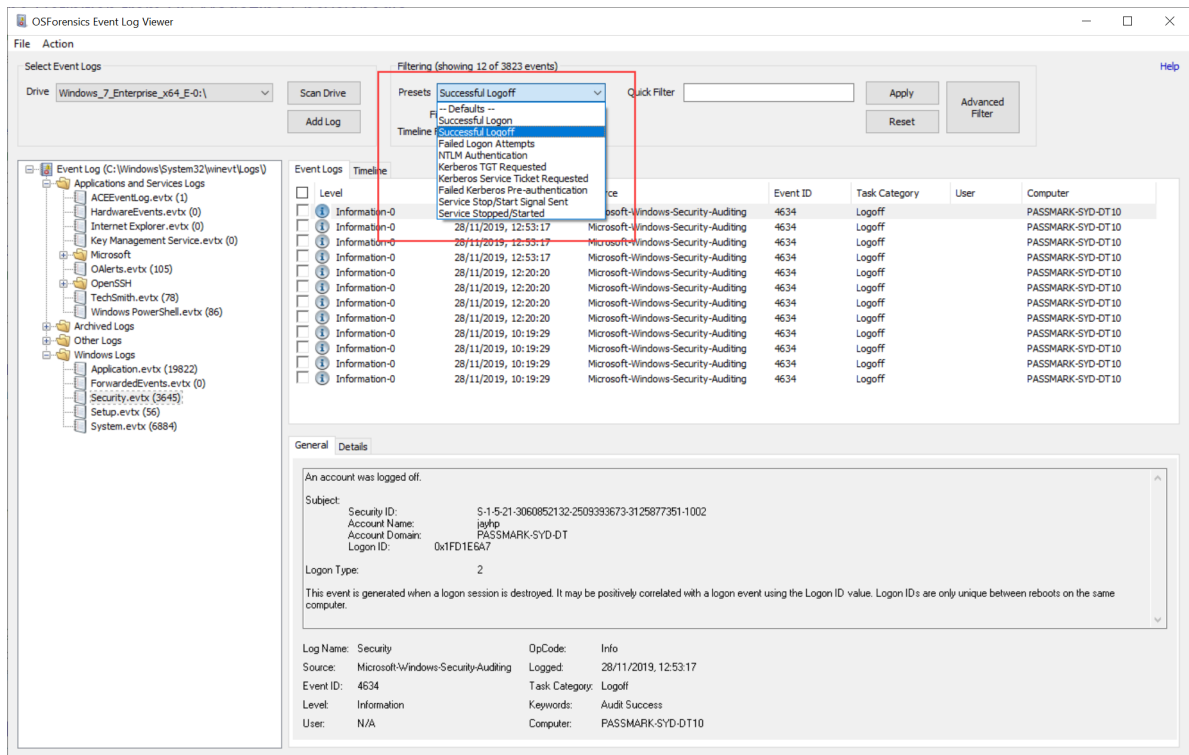
- Step 1. Edit the Presets config file in the ProgramData directory which usually located at:
C:\ProgramData\PassMark\OSForensics\EventLogPresets.txt

Three lines as a set for one preset entry, the first line is the name of the preset filter, second line is filter file name, and the third needs to be the name of the event log file in which the events are stored.

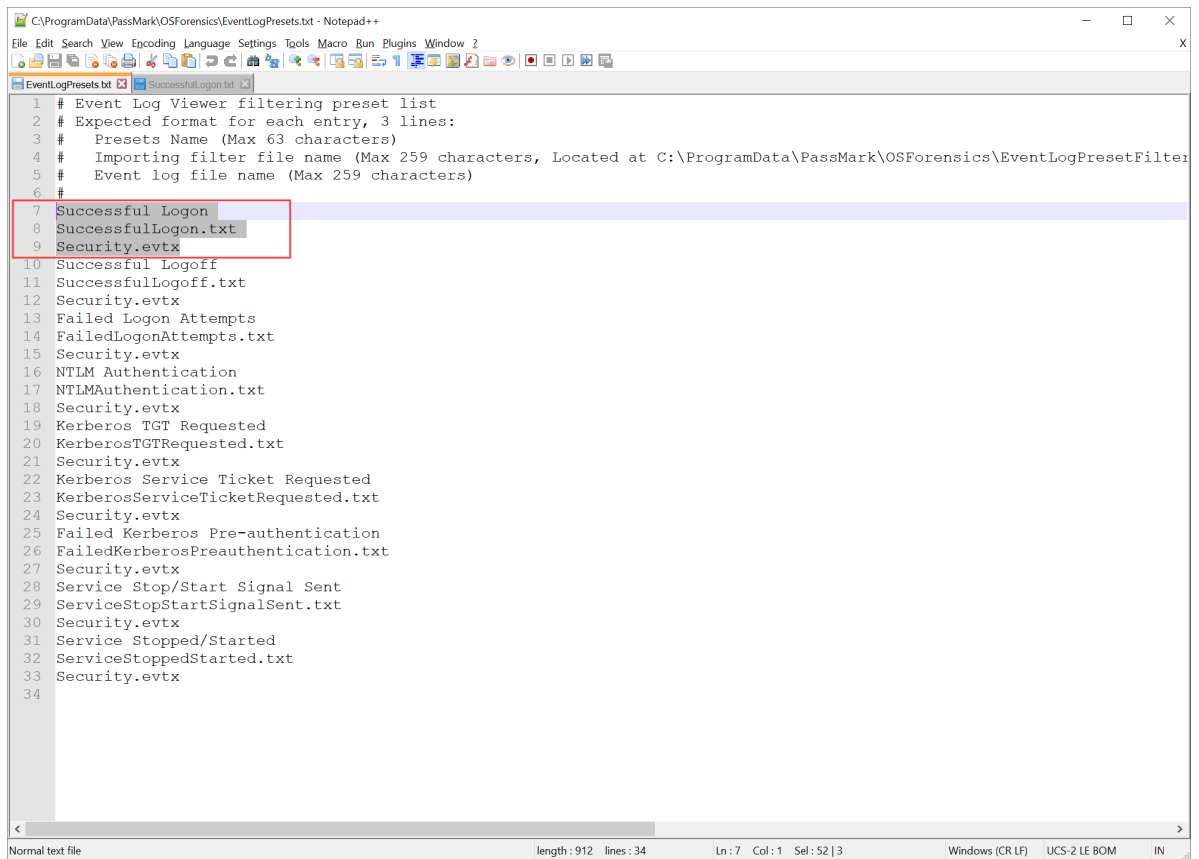
- Step 2. Create filter file and put in the directory "EventLogPresetFilters" located at:
C:\ProgramData\PassMark\OSForensics\EventLogPresetFilters\

You could create a filter file by exporting from Event Log Viewer, or editing the sample file.

* Note that the FilterType value should be set as 2 indicating this is a Preset filter.



Preset filter

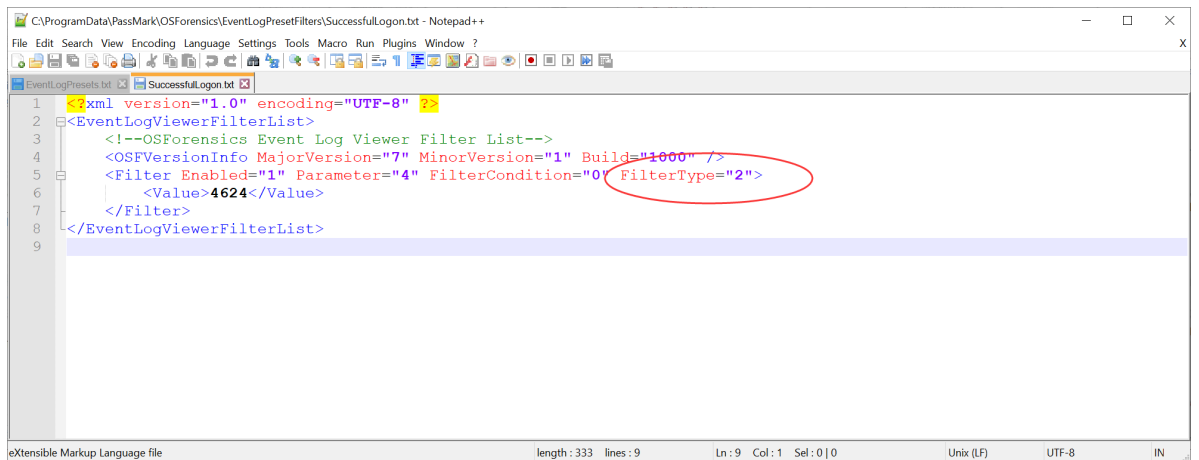


```

1 # Event Log Viewer filtering preset list
2 # Expected format for each entry, 3 lines:
3 #   Presets Name (Max 63 characters)
4 #   Importing filter file name (Max 259 characters, Located at C:\ProgramData\PassMark\OSForensics\EventLogPresetFilter
5 #   Event log file name (Max 259 characters)
6 #
7 Successful Logon
8 SuccessfulLogon.txt
9 Security.evtx
10 Successful Logoff
11 SuccessfulLogoff.txt
12 Security.evtx
13 Failed Logon Attempts
14 FailedLogonAttempts.txt
15 Security.evtx
16 NTLM Authentication
17 NTLMAuthentication.txt
18 Security.evtx
19 Kerberos TGT Requested
20 KerberosTGTRequested.txt
21 Security.evtx
22 Kerberos Service Ticket Requested
23 KerberosServiceTicketRequested.txt
24 Security.evtx
25 Failed Kerberos Pre-authentication
26 FailedKerberosPreauthentication.txt
27 Security.evtx
28 Service Stop/Start Signal Sent
29 ServiceStopStartSignalSent.txt
30 Security.evtx
31 Service Stopped/Started
32 ServiceStoppedStarted.txt
33 Security.evtx
34

```

Customize presets



```

1 <?xml version="1.0" encoding="UTF-8" ?>
2 <EventLogViewerFilterList>
3   <!--OSForensics Event Log Viewer Filter List-->
4   <OSForensics MajorVersion="7" MinorVersion="1" Build="1000" />
5   <Filter Enabled="1" Parameter="4" FilterCondition="0" FilterType="2">
6     <Value>4624</Value>
7   </Filter>
8 </EventLogViewerFilterList>
9

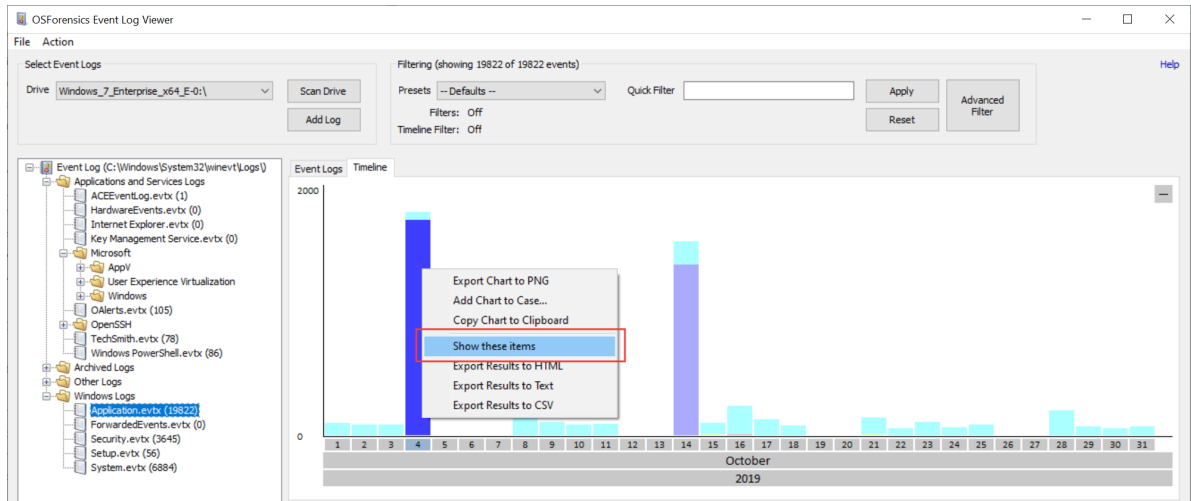
```

Presets filter file

Time Line

Timelines are graphical representations of events in chronological order.

The Timeline view displays an interactive bar graph providing users with a time-based view of Event Logs. This view is useful for identifying trends where significant number of events occurred. Each bar is color-coded by the different Level of events.



Timeline right click menu

Export to CSV/HTML/Text

To export the logs to a file with format CSV, HTML or txt, select some or all logs and right-click on the list.

The screenshot shows the OSForensics Event Log Viewer interface with a list of events. The 'Filtering' section shows 'Successful Logon' with 13 of 3646 events displayed. A context menu is open over the list, showing options like 'Filter by: Date and Time = 28/11/2019, 11:43:35 ±10 min' and 'Export List of All Results To'. A sub-menu is open over the 'Export To' option, showing 'txt', 'html', and 'CSV' as available formats. The 'Details' pane at the bottom shows information for a specific log entry.

| Level | Date and Time | Source | Event ID | Task Category | User | Computer |
|---------------|----------------------|-------------------------------------|----------|---------------|------|-------------------|
| Information-0 | 28/11/2019, 11:00:43 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 11:06:11 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 11:09:01 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 11:20:24 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 11:24:01 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 11:37:13 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 11:39:01 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 11:43:34 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 11:43:35 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 11:43:35 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 11:43:35 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |
| Information-0 | 28/11/2019, 11:43:35 | Microsoft-Windows-Security-Auditing | 4624 | Logon | | PASSMARK-SYD-DT10 |

General Details

An account was successfully logged on

Subject:

- Security ID: S-1-5-18
- Account Name: PASSMARK-SYD-DT\$
- Account Domain: WDRKGROUP
- Logon ID: 0x3E7

Logon Information:

- Logon Type: 5
- Restricted Admin Mode: No
- Virtual Account: No
- Elevated Token: Yes

Log Name: Security OpCode: Info

Source: Microsoft-Windows-Security-Auditing Logged: 28/11/2019, 11:43:35

Event ID: 4624 Task Category: Logon

Level: Information Keywords: Audit Success

User: N/A Computer: PASSMARK-SYD-DT10

Export results to

Additional Info

Level

Level field shows the type of event that is recorded. There are five different types - Information, Critical, Error, Warning and Verbose.

OSForensics Event Log Viewer displays a number followed by these types names, that is the number retrieved from Level field in System section of XML message.

Note that both '0' and '4' numbers indicate the same Information type.

Date and Time

When the logs are recorded by Windows systems the time stamp is stored in GMT.

OSForensics Event Log Viewer uses whatever time zone is currently set in the Case Properties of Manage Case module. If you are going to change the time zone setting, please close the Event Log Viewer and reopen it after the setting is done.

Event ID

It is recommended to perform analysis on a version of Windows that is at least as new as the computer that generated the event logs to be analyzed. This is because the Event IDs have been added over time and the information representing each ID has also been changed.

For additional information on Event IDs please visit: <http://www.eventid.net/>

User

User field in OSForensics Event Log Viewer is showing Security Identifiers (SIDs). For the well-known SIDs please visit: <https://support.microsoft.com/en-gb/help/243330/well-known-security-identifiers-in-windows-operating-systems>

Using Regular Expression

Event Log Viewer supports Regular Expressions search. Here is an example of searching logs that contain IP addresses.

By using keyword `((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})` with the regular expression condition, we easily got the interesting 10 records which include IP addresses among 38,566 records.

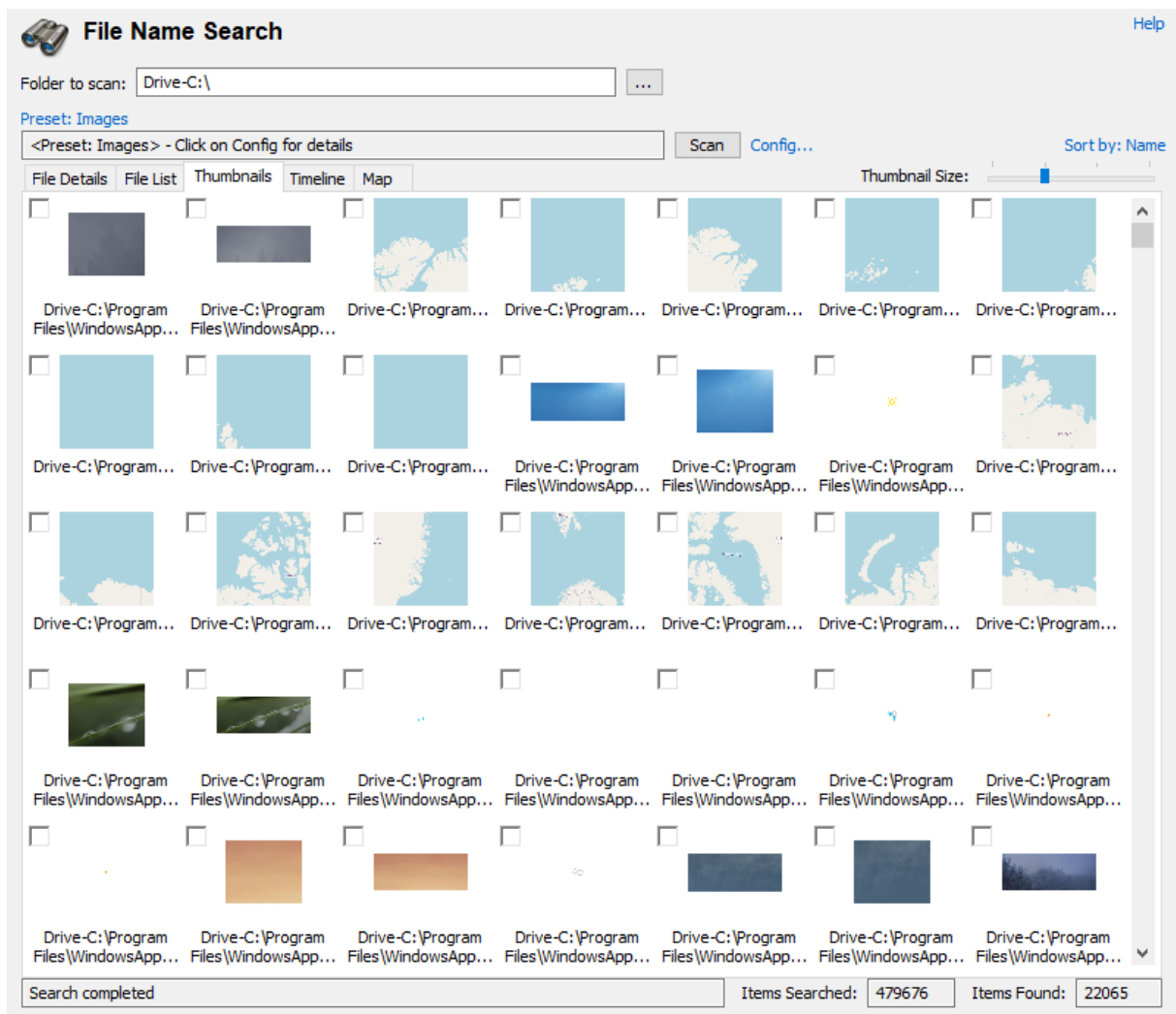
The screenshot displays the OSForensics Event Log Viewer interface. On the left, a tree view shows various event logs, with 'Security' selected. The main pane shows a list of events with columns for Level, Date and Time, Source, Event ID, Task Category, and User. A filter dialog box is open, showing the 'Filters' tab. The filter is a regular expression: `(0[0-9]{0,2})2[0-9]{0,1}2[0-4][0-9]{25[0-5][3-9]{0-1}`. The dialog also shows the 'Details' tab with XML data for the selected event, including fields like SubjectUserSid, SubjectUserName, SubjectDomainName, SubjectLogonId, TargetUserSid, TargetUserName, TargetDomainName, TargetLogonId, LogonType, LogonProcessName, AuthenticationPackageName, WorkstationName, LogonGuid, TransmittedServices, LmPackageName, KeyLength, ProcessId, ProcessName, IpAddress, and ImpersonationLevel.

| Level | Date and Time | Source | Event ID | Task Category | User |
|---------------|----------------------|-------------------------------------|----------|---------------|------|
| Information-0 | 28/11/2019, 15:42:48 | Microsoft-Windows-Security-Auditing | 4648 | Logon | |
| Information-0 | 28/11/2019, 15:42:48 | Microsoft-Windows-Security-Auditing | 4624 | Logon | |
| Information-0 | 28/10/2019, 15:02:15 | Microsoft-Windows-Security-Auditing | 4648 | Logon | |
| Information-0 | 28/10/2019, 15:02:15 | Microsoft-Windows-Security-Auditing | 4624 | Logon | |
| Information-0 | 28/10/2019, 14:48:12 | Microsoft-Windows-Security-Auditing | 4624 | Logon | |
| Information-0 | 28/10/2019, 14:48:12 | Microsoft-Windows-Security-Auditing | 4648 | Logon | |
| Information-0 | 16/10/2019, 12:41:23 | Microsoft-Windows-Security-Auditing | 4648 | Logon | |
| Information-0 | 16/10/2019, 12:41:23 | Microsoft-Windows-Security-Auditing | 4624 | Logon | |
| Information-0 | 16/10/2019, 12:41:18 | Microsoft-Windows-Security-Auditing | 4625 | Logon | |
| Information-0 | 15/10/2019, 16:19:07 | Microsoft-Windows-Security-Auditing | 4624 | Logon | |

Regular Expression

5.11 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.



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.

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.

Note: The search string can only be specified when Preset is set to User-defined Search

Presets

You can select one of the preset search options to quickly locate files of certain file type (eg. image files or office documents). Presets are loaded from a default Preset file and user custom presets are loaded/stored from the OSForensics config file. Adding or editing custom presets can be done so in the File Name Search Configuration window.

The default presets are loaded from the `FileNameSearchPresets.cfg` file in the OSForensics program data folder (generally `C:\ProgramData\PassMark\OSForensics`). The default presets can be customized by altering the file. This file needs to be opened and saved in Unicode format. The `FileNameSearchPresets.cfg` may be overwritten upon upgrade or new installs, it is recommend adding custom presets using the configuration window.

Image Analysis Presets (Face-Detect-AI, Illicit-Detect-AI)

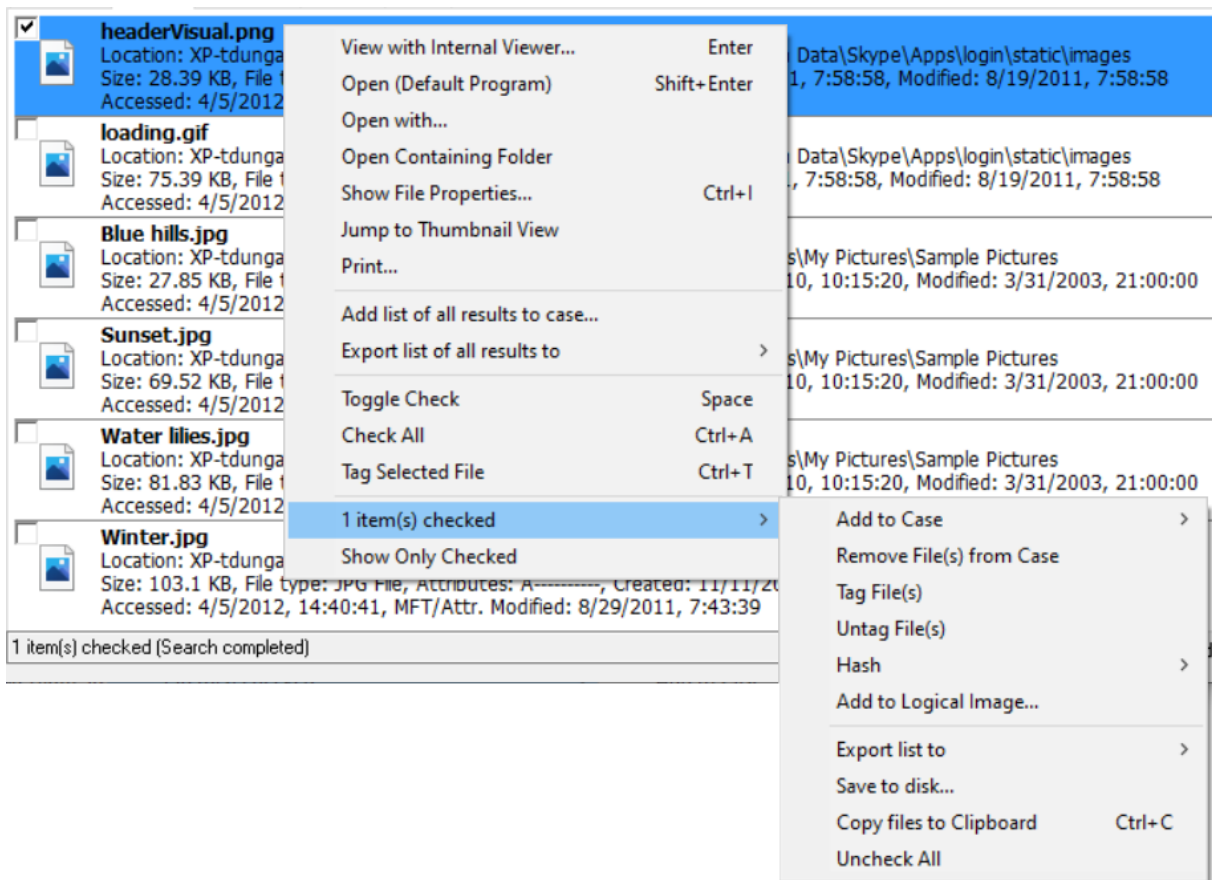
For more information on "Face detect" and "Illicit Image" detection options, please see the Image Analysis module.

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.

Jump to Thumbnail View/Jump to Details List

Show the current file selected in the Thumbnail View or Details List tab

Print...

Print the file (if applicable)

Add list of all results to Case...

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

Export list of all 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.

Tag Selected File

Tag the selected item.

n Item(s) checked**Add to Case**

Add the checked file(s) or list of checked file(s) to the case, see Adding items to a case.

Remove File(s) from Case

Remove the checked file(s) from the case

Tag File(s)

Tag the checked file(s). *Keyboard shortcut: Ctrl+T*

Hash**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.

Calculate Hash of File(s)...

Calculate the hash of the checked files.

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.

Uncheck All

Uncheck the checked file(s).

Show only Checked/Show All Files

Toggle to show only the checked items or to show all files

5.11.1 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

Directory List Management

Directory: C:\

Action: Include this and all subdirectories

Add to list Remove from list

| Directory | Action |
|-----------|---------------|
| Drive-C: | Include & Sub |

Common File Search Options

Search for Folders Names

Search Deleted Files

Case Sensitive

Match Whole Word Only

Search in Hash Set Database

Cryptocurrency Make Database Active

Create Quick Hash Set...

Show \$FILE_NAME Dates (NTFS)

Current Search Settings

* Remember to save any changes to custom presets

Preset: TEST Delete Save Save as...

Search String: *.gif;*.png;*.bmp;*.jpg;*.jpeg;*.jpe;*.tif;*.tif... Include folders Exclude folders Add

File Size Limits: Min KB Max KB

File Attributes: Archive Hidden Encrypted Reparse Point Compressed Read-Only Sparse File System

Creation Date Range: From To (01-Aug-2022)

Modify Date Range: From To (01-Aug-2022)

Access Date Range: From To (01-Aug-2022)

MFT Modify Date Range: From To (01-Aug-2022)

Gather Alternate Stream Info (Slow) Filter on EXIF Metadata (Slow)

Minimum number of alternate streams: Search String: Use RegEx

Minimum size of alternate streams: KB Preset: Keyword Suggestions

OK Reset

Directory List Management - List of Directories to be included or excluded from the search

Directory

Specify the directory to be included or excluded

Action

Options are: *Include this directory*, *Include this directory and all sub-directories*, *Exclude this directory* and *Exclude this directory and all sub-directories*.

Sub folders will also be included or excluded in searches, not just the files in the start directory.

Add to List

Add the currently Directory and Action to the list

Remove from List

Remove the currently selected start point in the list.

Common File Search Options - Options that are applied to every search performed by File Name Search.**Search for Folder Names**

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

Case Sensitive

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

Search deleted files

If checked, deleted files (and \$130 slack entries, for NTFS drives) will also be included in the results. Enabling this option may reduce the speed of the search.

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 wild-card searches.

Search in Hash Set Database

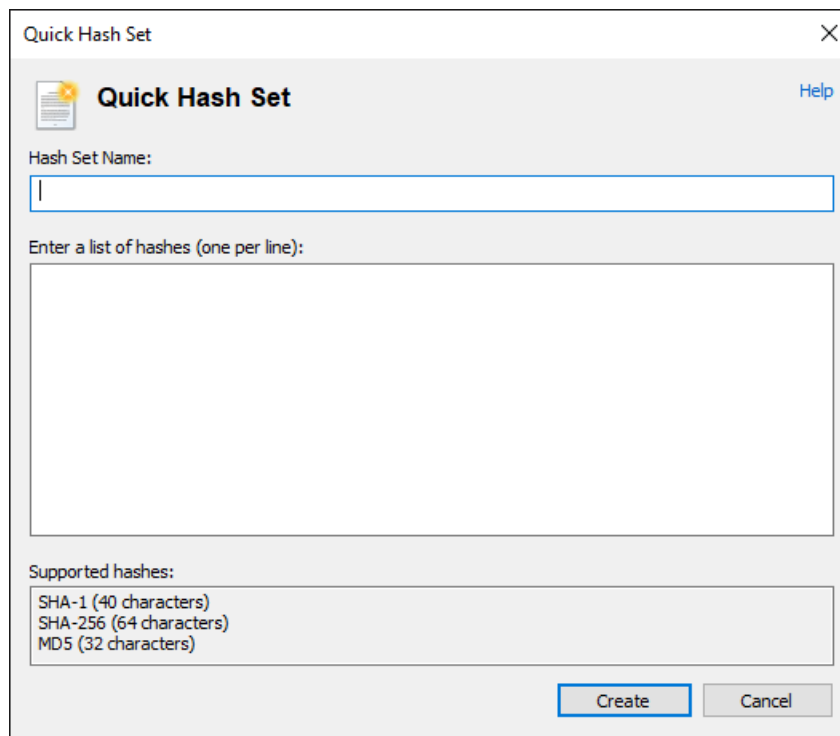
If checked, file matching current search setting will be check for in the specified Hash Set Database.

Make Database Active

If checked and Search in Hash Set Database is enabled, the currently selected database will be made active.

Create Quick Hash Set...

Create a quick hash set by specifying a list of hashes.



Current Search Settings - Settings that are applied to the current search performed by File Name Search. Also allow creating and editing of Custom Presets.

Preset

Dropdown selection of the current preset being used. Default presets are loaded from a local text file and user specified custom presets will be shown at the bottom of the list.

If *User-defined Search* is selected, the search string can be edited in the text box. Otherwise, a list of search strings and corresponding include/exclude folders are displayed in the list view. Search strings can be edited or deleted by right-clicking the item. Click 'Add' to add a new search string to the list.

Delete

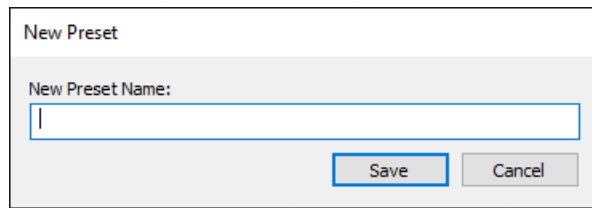
Delete an existing preset. Default presets cannot be deleted using the configuration window. Edit `FileNameSearchPresets.cfg` file to remove default presets.

Save

Save the current settings to the currently selected preset. Default presets cannot be edited using the configuration window. Edit `FileNameSearchPresets.cfg` file to change default presets.

Save As...

Save the current settings under a new custom preset. You will be prompted to enter in a name for the new preset to be saved under. Custom Presets are stored in the OSForensics configuration file.



The image shows a dialog box titled "New Preset". Inside the dialog, there is a label "New Preset Name:" followed by a text input field. At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

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.

Filter on EXIF Metadata

Allows to search against the EXIF metadata of an image file. Turning this on will slow down the search slightly.

Exiv2 (V0.27.3) tool is used to obtain the image metadata.

* Note that image files larger than 50 MB will be skipped from searching and will not be displayed in the result.

Exiv2 utility has little support on Movie file formats. Check here to see the supported image formats.

Use RegEx (Regular Expressions)

Allows to use the regular expression search of EXIF metadata.

Some examples of regular expressions are provided below:

▪ Photos taken with common digital cameras

```
(Make)[\s]+(Ascii)[\s]+[d]+[\s]+(Canon|Nikon|Sony|Olympus|Pentax|Fujifilm|Panasonic|Leica|Kodak|GoPro|Polaroid|Ricoh|Hasselblad|Casio)
```

▪ Photos taken with Canon or Nikon camera

```
(Make)[\s]+(Ascii)[\s]+[d]+[\s]+(Canon|Nikon)
```

▪ Photos taken with common camera lenses

```
(Lens([\w+]))[\s]+[\w]+[\s]+[d]+[\s]+(Canon|Nikon|Sigma|Tamron|Yongnuo|Rokinon|Pentax|Sony|Fujifilm|Olympus|Panasonic|Leica|Samyang|Tokina|Zeiss|Laowa)
```

▪ Photos taken with Sigma lens

```
(Lens([\w+]))[\s]+[\w]+[\s]+[d]+[\s]+(Sigma)
```

▪ Photos taken with a flash

```
(Flash)[\s]+(Short)[\s]+(1)[\s]+(Yes|Fired)
```

For more forensics regular expression examples see here.

5.11.2 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 | Date created | Date accessed |
|-------------------|---|----------|-----------------------------|-----------------------------|-----------------------------|
| 0.jpg | Drive-C:\Program Files\WindowsApps\Microsoft... | JPG File | 7/12/2019, 19:55:29.7062330 | 7/12/2019, 19:55:29.6925301 | 1/08/2022, 11:16:26.5764941 |
| 0.jpg | Drive-C:\Program Files\WindowsApps\Microsoft... | JPG File | 7/12/2019, 19:55:29.7365071 | 7/12/2019, 19:55:29.7365071 | 1/08/2022, 11:16:26.7169348 |
| 0.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 13:01:42.0907670 | 1/08/2022, 13:01:42.0747262 | 1/08/2022, 13:01:42.0907670 |
| 0.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 13:01:42.0214004 | 1/08/2022, 13:01:42.0062170 | 1/08/2022, 13:01:42.0214004 |
| 0.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 13:01:42.0062170 | 1/08/2022, 13:01:41.9899343 | 1/08/2022, 13:01:42.0062170 |
| 0.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 13:01:42.0907670 | 1/08/2022, 13:01:42.0907670 | 1/08/2022, 13:01:42.0907670 |
| 0.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 13:01:42.1529678 | 1/08/2022, 13:01:42.1375262 | 1/08/2022, 13:01:42.1529678 |
| 0.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 13:01:42.2071710 | 1/08/2022, 13:01:42.2071710 | 1/08/2022, 13:01:42.2071710 |
| 0.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 13:01:42.1594963 | 1/08/2022, 13:01:42.1529678 | 1/08/2022, 13:01:42.1594963 |
| 0.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 13:01:42.2071710 | 1/08/2022, 13:01:42.1914026 | 1/08/2022, 13:01:42.2071710 |
| 1.jpg | Drive-C:\Program Files\WindowsApps\Microsoft... | JPG File | 7/12/2019, 19:55:29.7365071 | 7/12/2019, 19:55:29.7365071 | 1/08/2022, 11:16:26.7169348 |
| 1.jpg | Drive-C:\Program Files\WindowsApps\Microsoft... | JPG File | 7/12/2019, 19:55:29.7062330 | 7/12/2019, 19:55:29.7062330 | 1/08/2022, 11:16:26.5921061 |
| 1.png | Drive-C:\Program Files\WindowsApps\Microsoft... | PNG File | 7/12/2019, 19:55:29.5644675 | 7/12/2019, 19:55:29.5644675 | 1/08/2022, 11:16:26.1701022 |
| 1.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 11:30:04.3943305 | 1/08/2022, 11:30:04.3783264 | 1/08/2022, 11:30:04.3943305 |
| 1.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 13:01:42.1594963 | 1/08/2022, 13:01:42.1594963 | 1/08/2022, 13:01:42.1594963 |
| 1.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 11:30:04.3943305 | 1/08/2022, 11:30:04.3943305 | 1/08/2022, 11:30:04.3943305 |
| 1.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 11:30:04.3095697 | 1/08/2022, 11:30:04.3095697 | 1/08/2022, 11:30:04.3095697 |
| 1.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 11:30:04.3095697 | 1/08/2022, 11:30:04.3095697 | 1/08/2022, 11:30:04.3095697 |
| 1.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 11:30:04.3410453 | 1/08/2022, 11:30:04.3410453 | 1/08/2022, 11:30:04.3410453 |
| 1.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 11:30:04.3563512 | 1/08/2022, 11:30:04.3410453 | 1/08/2022, 11:30:04.3563512 |
| 1.png | Drive-C:\ProgramData\PassMark\OSForensics\... | PNG File | 1/08/2022, 13:01:42.1594963 | 1/08/2022, 13:01:42.1594963 | 1/08/2022, 13:01:42.1594963 |
| 10.jpg | Drive-C:\Program Files\WindowsApps\Microsoft... | JPG File | 7/12/2019, 19:55:29.7062330 | 7/12/2019, 19:55:29.7062330 | 1/08/2022, 11:16:26.5921061 |
| 10.jpg | Drive-C:\Program Files\WindowsApps\Microsoft... | JPG File | 7/12/2019, 19:55:29.7365071 | 7/12/2019, 19:55:29.7365071 | 1/08/2022, 11:16:26.7169348 |
| 10.png | Drive-C:\Program Files\WindowsApps\Microsoft... | PNG File | 7/12/2019, 19:55:29.5644675 | 7/12/2019, 19:55:29.5644675 | 1/08/2022, 11:16:26.1701022 |
| 10px.png | Drive-C:\Program Files\WindowsApps\Microsoft... | PNG File | 7/12/2019, 19:55:29.5025251 | 7/12/2019, 19:55:29.5025251 | 1/08/2022, 11:16:26.0918672 |
| 10px.png | Drive-C:\Program Files\WindowsApps\Microsoft... | PNG File | 7/12/2019, 19:55:29.5025251 | 7/12/2019, 19:55:29.5025251 | 1/08/2022, 11:16:26.0918672 |
| 11.png | Drive-C:\Program Files\WindowsApps\Microsoft... | PNG File | 7/12/2019, 19:55:29.5644675 | 7/12/2019, 19:55:29.5644675 | 1/08/2022, 11:16:26.1856481 |
| 1113_20x20x32.png | Drive-C:\Program Files\WindowsApps\microsof... | PNG File | 7/12/2019, 19:56:31.7524697 | 7/12/2019, 19:56:31.7524697 | 1/08/2022, 11:16:35.6858557 |
| 1113_20x20x32.png | Drive-C:\Program Files\WindowsApps\Microsoft... | PNG File | 7/12/2019, 19:56:31.7524697 | 7/12/2019, 19:56:31.7524697 | 1/08/2022, 11:16:35.6858557 |

Search completed Items Searched: 479676 Items Found: 22065

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

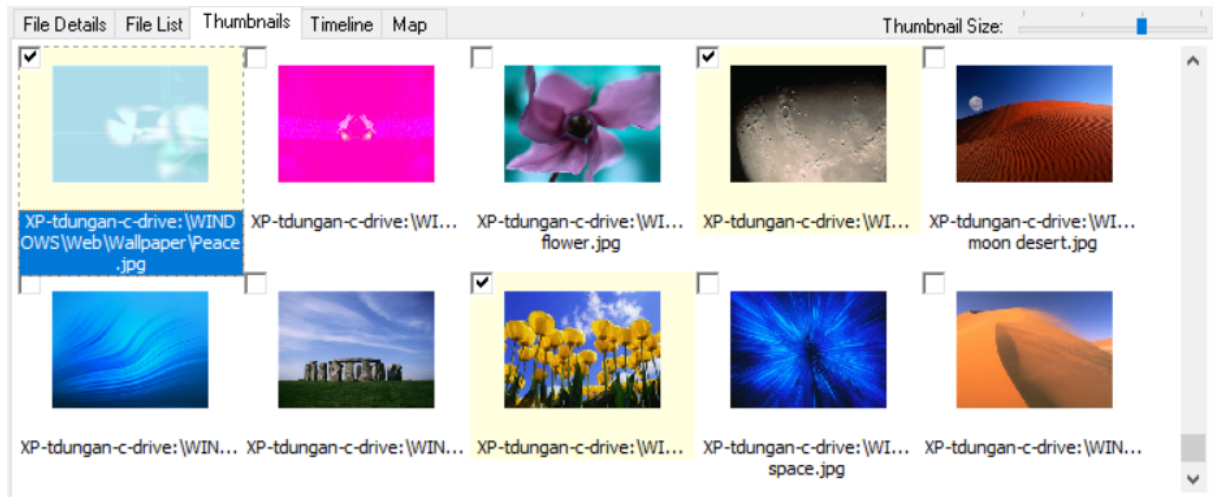
File List View

| File Name | Location | Type | Date modified | Date created | Date accessed |
|-----------|--|----------|---|--------------|--|
| 0.jpg | Location: Drive-C:\Program Files\WindowsApps\Microsoft.BingWeather_4.53.41681.0_x64__8wekyb3d8bbwe\Assets\AppTiles\WeatherImages\210x173 | JPG File | Size: 14.50 KB, File type: JPG File, Attributes: A-----, Created: 7/12/2019, 19:55:29, Modified: 7/12/2019, 19:55:29 | | Accessed: 1/08/2022, 11:16:26, MFT/Attr. Modified: 1/08/2022, 11:13:26 |
| 0.jpg | Location: Drive-C:\Program Files\WindowsApps\Microsoft.BingWeather_4.53.41681.0_x64__8wekyb3d8bbwe\Assets\AppTiles\WeatherImages\423x173 | JPG File | Size: 16.85 KB, File type: JPG File, Attributes: A-----, Created: 7/12/2019, 19:55:29, Modified: 7/12/2019, 19:55:29 | | Accessed: 1/08/2022, 11:16:26, MFT/Attr. Modified: 1/08/2022, 11:13:26 |
| 0.png | Location: Drive-C:\ProgramData\PassMark\OSForensics\MapCache\3\2 | PNG File | Size: 5.02 KB, File type: PNG File, Attributes: A-----, Created: 1/08/2022, 13:01:42, Modified: 1/08/2022, 13:01:42 | | Accessed: 1/08/2022, 13:01:42, MFT/Attr. Modified: 1/08/2022, 13:01:42 |
| 0.png | Location: Drive-C:\ProgramData\PassMark\OSForensics\MapCache\3\4 | PNG File | Size: 1.07 KB, File type: PNG File, Attributes: A-----, Created: 1/08/2022, 13:01:42, Modified: 1/08/2022, 13:01:42 | | Accessed: 1/08/2022, 13:01:42, MFT/Attr. Modified: 1/08/2022, 13:01:42 |
| 0.png | Location: Drive-C:\ProgramData\PassMark\OSForensics\MapCache\3\3 | PNG File | Size: 3.52 KB, File type: PNG File, Attributes: A-----, Created: 1/08/2022, 13:01:41, Modified: 1/08/2022, 13:01:42 | | Accessed: 1/08/2022, 13:01:42, MFT/Attr. Modified: 1/08/2022, 13:01:42 |
| 0.png | Location: Drive-C:\ProgramData\PassMark\OSForensics\MapCache\3\5 | PNG File | Size: 1.78 KB, File type: PNG File, Attributes: A-----, Created: 1/08/2022, 13:01:42, Modified: 1/08/2022, 13:01:42 | | Accessed: 1/08/2022, 13:01:42, MFT/Attr. Modified: 1/08/2022, 13:01:42 |
| 0.png | Location: Drive-C:\ProgramData\PassMark\OSForensics\MapCache\3\1 | PNG File | Size: 959 Bytes, File type: PNG File, Attributes: A-----, Created: 1/08/2022, 13:01:42, Modified: 1/08/2022, 13:01:42 | | Accessed: 1/08/2022, 13:01:42, MFT/Attr. Modified: 1/08/2022, 13:01:42 |
| 0.png | Location: Drive-C:\ProgramData\PassMark\OSForensics\MapCache\3\7 | PNG File | Size: 103 Bytes, File type: PNG File, Attributes: A-----, Created: 1/08/2022, 13:01:42, Modified: 1/08/2022, 13:01:42 | | Accessed: 1/08/2022, 13:01:42, MFT/Attr. Modified: 1/08/2022, 13:01:42 |
| 0.png | Location: Drive-C:\ProgramData\PassMark\OSForensics\MapCache\3\6 | PNG File | Size: 902 Bytes, File type: PNG File, Attributes: A-----, Created: 1/08/2022, 13:01:42, Modified: 1/08/2022, 13:01:42 | | Accessed: 1/08/2022, 13:01:42, MFT/Attr. Modified: 1/08/2022, 13:01:42 |

Search completed Items Searched: 479676 Items Found: 22065

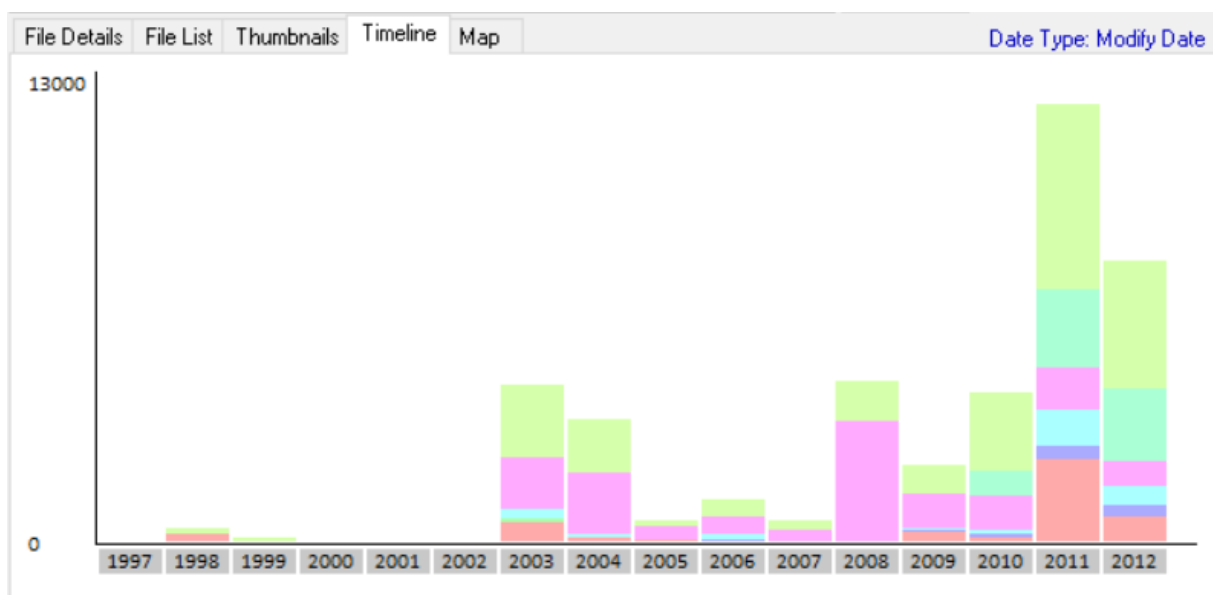
The File List View displays the search result as a list of file names, along with the corresponding metadata and icon.

Thumbnails View



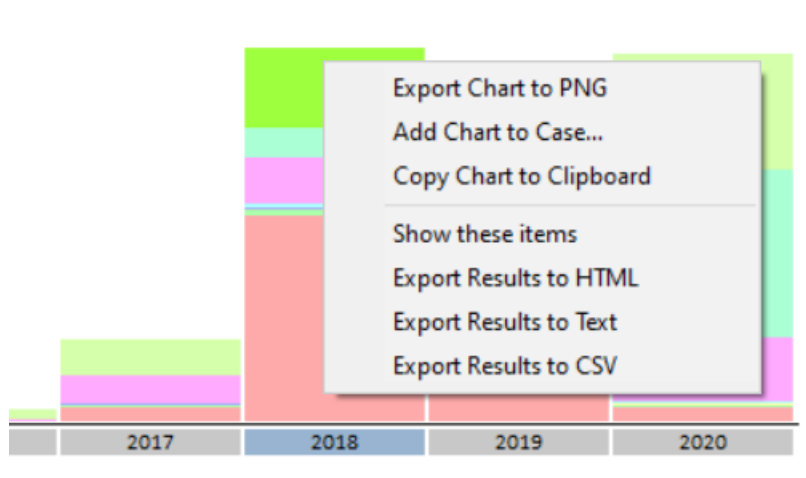
The Thumbnails View displays the search result as a list of thumbnails as well as with its file path. This view is useful when searching for media files, allowing the user to quickly browse through the thumbnail images. The size of the thumbnails can be adjusted using the *Thumbnail Size* slider bar.

Timeline View



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:



Export Chart to PNG

Export the chart as a PNG image file

Add Chart to Case...

Add the chart to the case as a PNG image file

Copy Chart to Clipboard

Copy the chart to the clipboard as a bitmap

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

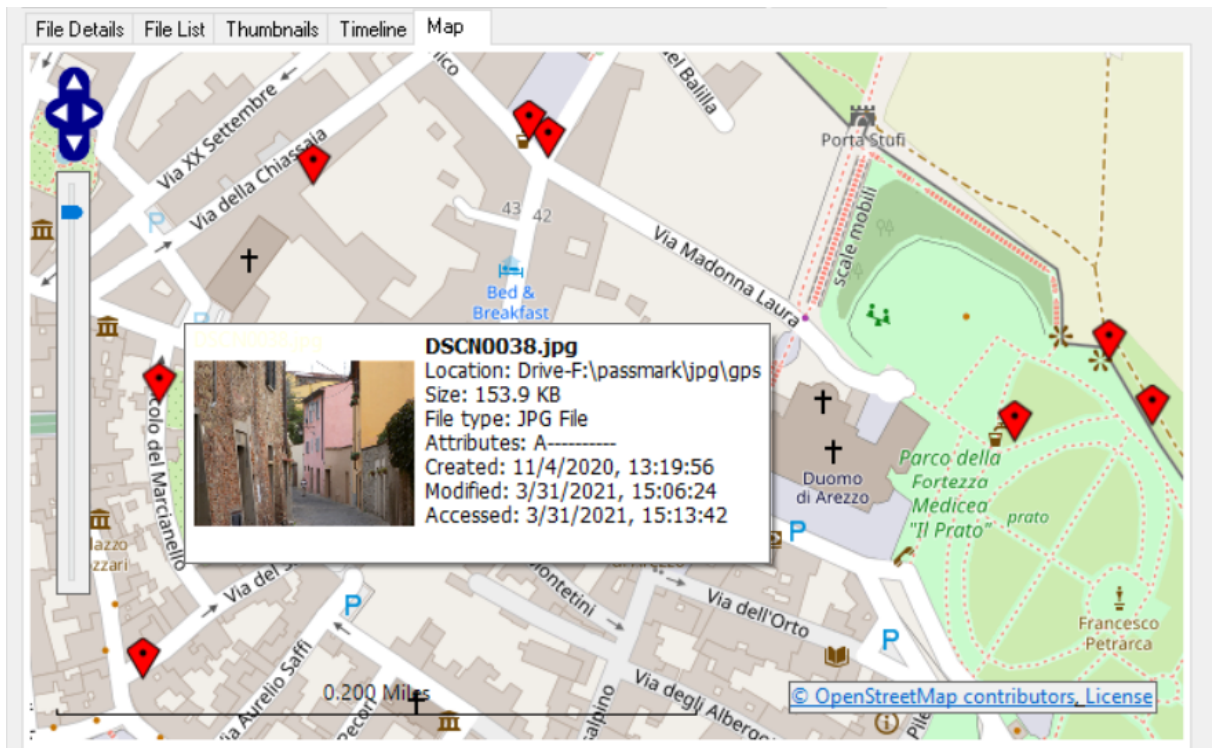
Export to Text

Export the results contained in the highlighted bar to text

Export to CSV

Export the results contained in the highlighted bar to CSV

Map View



The Map View plots files with GPS coordinates in EXIF metadata on a world map. This view is useful for visualizing geographic proximity of files with geotag information such as photos or videos. To change the zoom level, use the left slide bar or mouse wheel. To pan the world map, use the left directional arrows or mouse drag.

5.11.3 File Name Search Default Presets

The File Name Search module obtains the default list of preset searches from the `FileNameSearchPresets.cfg` file in the OSForensics program data folder (generally `C:\ProgramData\PassMark\OSForensics`).

The presets are specified using an XML schema and may be modified if required. However, the `FileNameSearchPresets.cfg` may be overwritten upon upgrade or new installs, it is recommend adding custom presets using the configuration window.

Modifying the Default Presets

The following is a snippet of the default `FileNameSearchPresets.cfg` file.

```

<?xml version="1.0" encoding="UTF-8" ?>
<FilenameSearchDefaultPresets>
  <Preset Desc="All Files">
    <FileSpec SearchString="*" />
  </Preset>
  ...
  <Preset Desc="E-mail Files">
    <FileSpec SearchString="*.pst;*.ost" />
    <FileSpec SearchString="*.dbx">
      <ExcludeFolder SubString="Dropbox" />
    </FileSpec>
    <FileSpec SearchString="*.idx">
      <IncludeFolder SubString="Outlook Express" />
    </FileSpec>
    <FileSpec SearchString="*.mbx;*.mbox" />
    <FileSpec SearchString="*.eml" />
    <FileSpec SearchString="*.dat">
      <IncludeFolder SubString="\\data\\3" />
    </FileSpec>
  </Preset>
  ...
</FilenameSearchDefaultPresets>

```

Each preset is defined using a `<Preset>` tag, with the `Desc` attribute specifying the name of the preset. In addition, the following optional attributes may be specified:

```

MinSize - Minimum file size in bytes
MaxSize - Maximum file size in bytes
Attributes - One or more of the following: ARCHIVE, COMPRESSED, ENCRYPTED, HIDDEN, READONLY, SYSTEM
AltStreams - "True" to enable scanning alternate streams, otherwise "False"
MinAltStreams - Minimum number of alternate streams
MinAltStreamSize - Minimum size of alternate streams in bytes
FromCreateDate - Earliest file creation date in number of 100-nanosecond intervals since January 1, 1601
ToCreateDate - Latest file creation date in number of 100-nanosecond intervals since January 1, 1601
FromModifyDate - Earliest file modify date in number of 100-nanosecond intervals since January 1, 1601
ToModifyDate - Latest file modify date in number of 100-nanosecond intervals since January 1, 1601
FromAccessDate - Earliest file access date in number of 100-nanosecond intervals since January 1, 1601
ToAccessDate - Latest file access date in number of 100-nanosecond intervals since January 1, 1601
FromExtraDate - Earliest file extra date in number of 100-nanosecond intervals since January 1, 1601
ToExtraDate - Latest file extra date in number of 100-nanosecond intervals since January 1, 1601
SortCriteria - The sort criteria to use to order the results
FilterOnEXIF - "True" to enable searching EXIF metadata
EXIFSearchString - Search keyword (string or pattern) for EXIF metadata search
UseRegExp - "True" to enable regular expression pattern matching

```

A `<Preset>` tag contains an array of `<FileSpec>` tags, which define a search string (`searchString` attribute) along with folder to include (`<IncludeFolder>`) and exclude (`<ExcludeFolder>`) for the corresponding search string.

If the file matches any of the `<FileSpec>` definitions, it shall be included in the results.

In the following example, any file names that match `*.idx` where the folder includes the string `"Outlook Express"` shall be included in the results.

```

<FileSpec SearchString="*.idx">
  <IncludeFolder SubString="Outlook Express" />
</FileSpec>

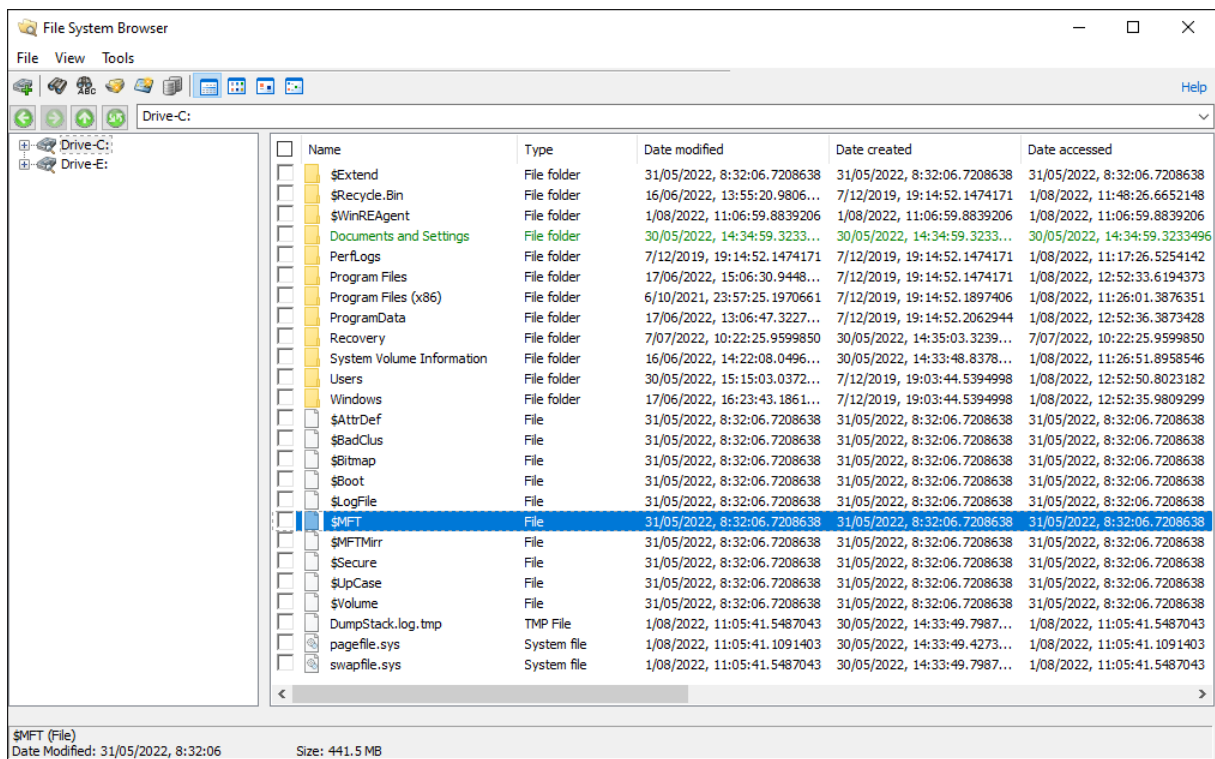
```

In this example, any file names that match `*.dbx` where the folder **does not** include the string `"Dropbox"` Or `"Dont_look_here"` shall be included in the results.

```
<FileSpec SearchString="*.dbx">
  <ExcludeFolder SubString="Dropbox" />
  <ExcludeFolder SubString="Dont_look_here" />
</FileSpec>
```

5.12 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.



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

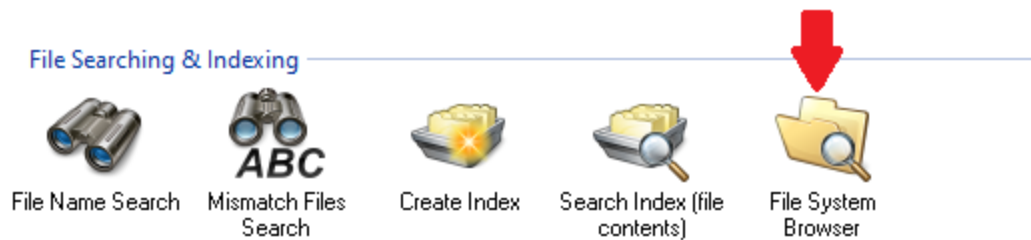
The table below summarizes the main components of the File System Browser.

Component	Description
t	

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

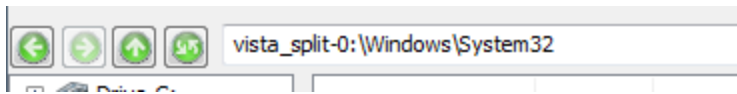
The File System Browser is accessible via the "File System Browser" icon in the "File Searching & Indexing" group under the Start tab, as well as the right-side navigation "File System Browser" button. Once opened, all devices added to the case are listed in the left hierarchical view.





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

Name	Type	Date modified	Date created	Date accessed
AppVEntVirtualization.dll	Application ext...	7/4/2019, 9:45:25.9263872	7/10/2019, 9:09:19.9303897	7/10/2019, 9:09
appverif.chm	Compiled HTML	9/28/2017, 6:49:46.0000000	9/28/2017, 6:49:46.0000000	2/15/2018, 0:01
appverif.exe				
appverifUI.dll				
appvetwclientres.dll				
appvetwsharedperfo				
appvetwstreamingux				
AppVFileSystemMeta				
AppVIntegration.dll				
AppVManifest.dll				
AppVNice.exe				
AppVOrchestration.d				
AppVPolicy.dll				
AppVPublishing.dll				
AppVReporting.dll				
AppVScripting.dll				
AppVSentinel.dll				
AppVShNotify.exe				
AppVStreamingUX.dll				
AppVStreamMap.dll				
AppVTerminator.dll	Application ext...	6/8/2018, 19:07:09.9314		
appwiz.cpl	Control panel item	4/11/2018, 23:34:23.680		
AppxAllUserStore.dll	Application ext...	7/4/2019, 4:21:33.67970		
AppxApplicabilityBlob.dll	Application ext...	6/7/2019, 5:23:08.43430		
AppxApplicabilityEngine.dll	Application ext...	4/11/2018, 23:34:06.364		
AppXDeploymentClient.dll	Application ext...	7/4/2019, 4:56:20.38531		
AppXDeploymentExtensions....	Application ext...	7/4/2019, 4:22:01.61406		
AppXDeploymentExtensions....	Application ext...	7/4/2019, 4:22:47.33648		
AppXDeploymentServer.dll	Application ext...	7/4/2019, 4:25:01.79406		
AppXDeploymentServer.dll	Application ext...	7/4/2019, 4:56:20.38531		

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

Tag File(s)

Tag file(s) for future reference. *Keyboard shortcut: Ctrl+T*

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.

Export list to

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

Save to disk...

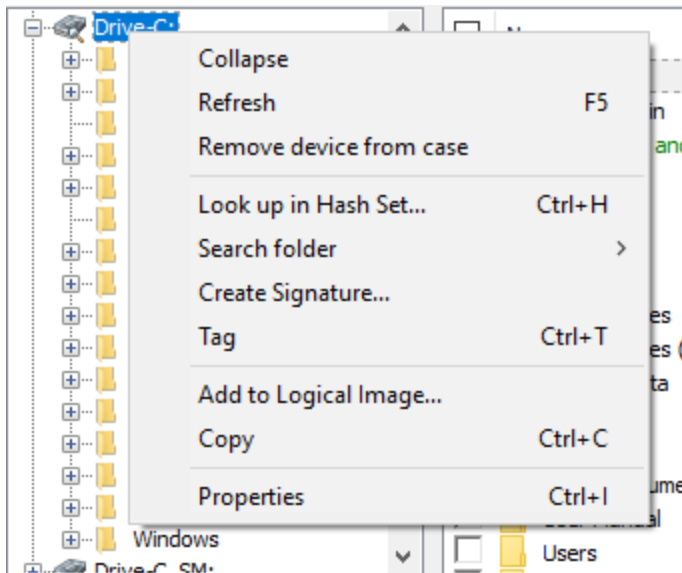
Save the checked file(s) to a location on disk.

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.

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.

Tag

Tag path for future reference. *Keyboard shortcut: Ctrl+T*

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.

5.12.1 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 *(for supported file systems 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.

HTCV

H|N - in Hash set/Not in hash set

T - Item is tagged

C - Item was added to the Case

V - Item was Viewed in the internal viewer

Category

The category of the item if it has been added to the case.

5.12.2 File Browser Views

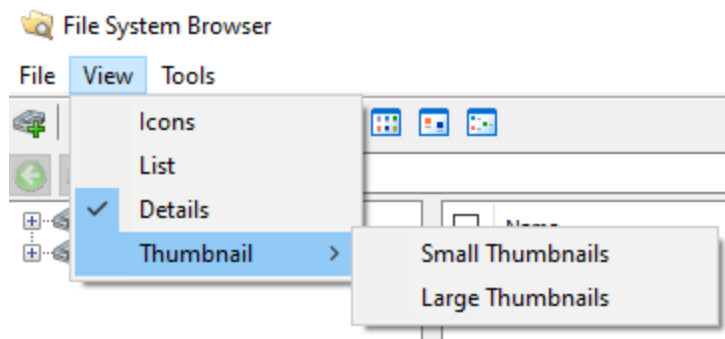
The user can choose from one of the following views in the File System Browser:

- Icon view
- List view
- Details view
- Small Thumbnails view
- Large Thumbnails view

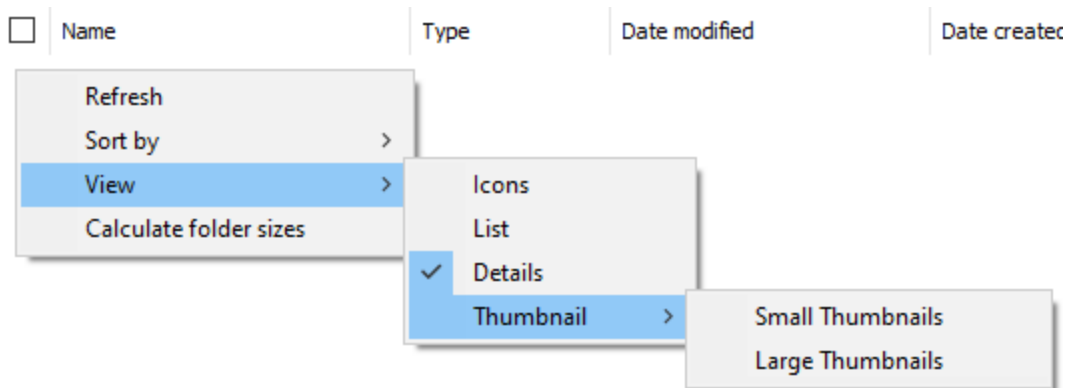
The view can be changed via the toolbar icon,



under 'View' in the system menu,

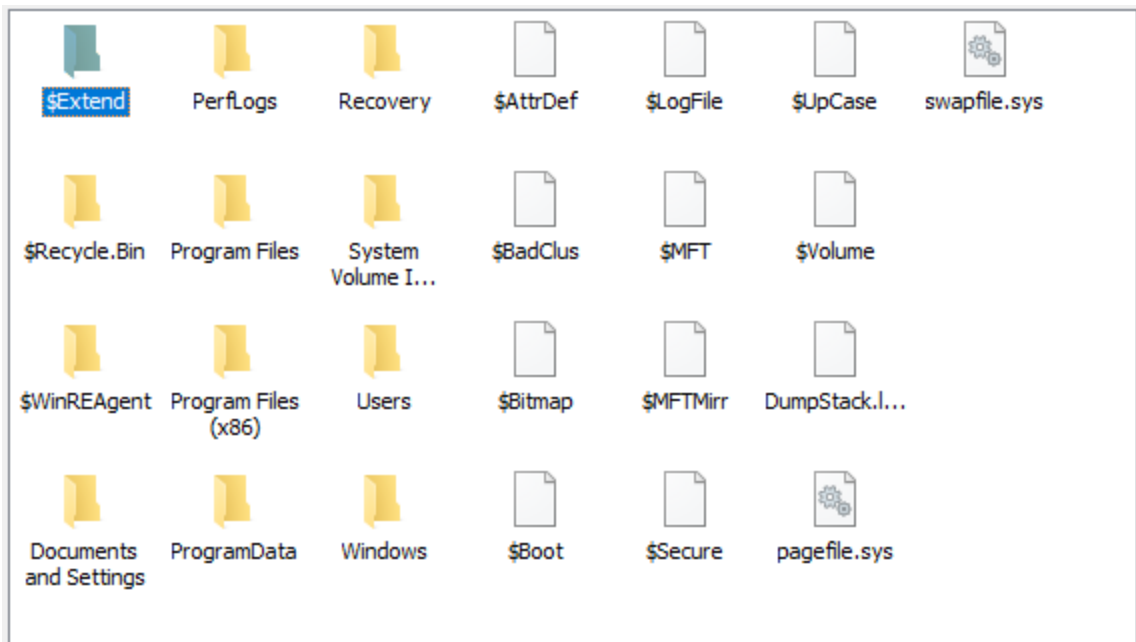


or right-click context menu.



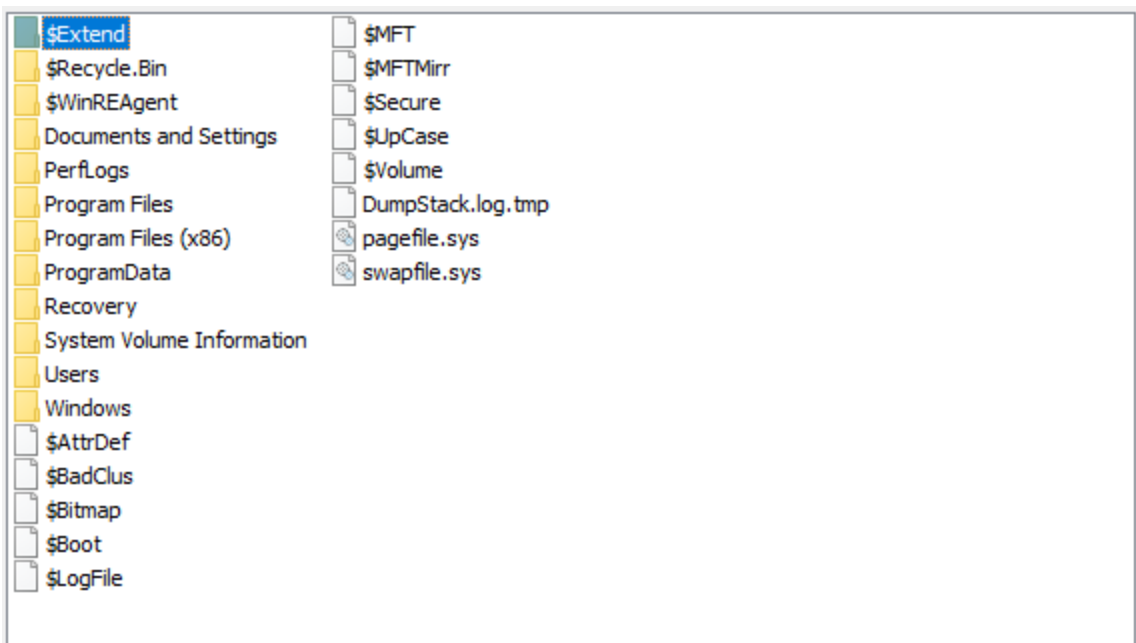
Icon View

Icon view displays the object's name and associated icon.



List View

List view displays the object's name and associated icon in a compact fashion.



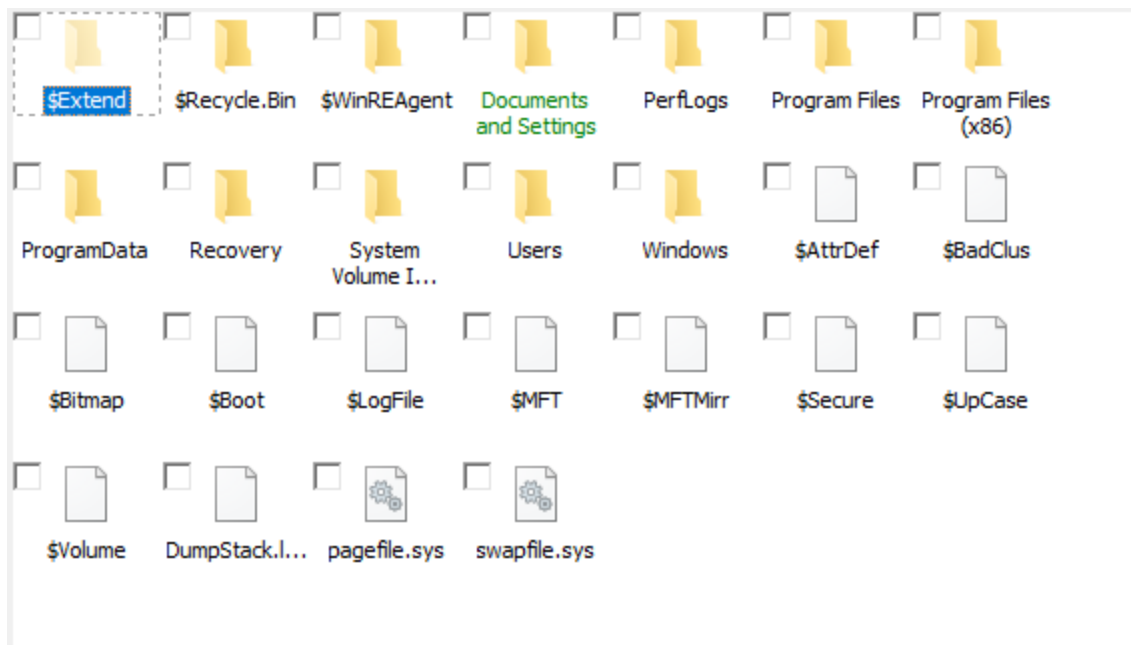
Details View

Details view displays the metadata associated with the object.

<input type="checkbox"/>	Name	Type	Date modified	Date created
<input type="checkbox"/>	\$Extend	File folder	31/05/2022, 8:32:06.7208638	31/05/2022, 8:
<input type="checkbox"/>	\$Recycle.Bin	File folder	16/06/2022, 13:55:20.9806...	7/12/2019, 19:
<input type="checkbox"/>	\$WinREAgent	File folder	16/06/2022, 13:54:21.8236...	16/06/2022, 13:
<input type="checkbox"/>	Documents and Settings	File folder	30/05/2022, 14:34:59.3233...	30/05/2022, 14:
<input type="checkbox"/>	PerfLogs	File folder	7/12/2019, 19:14:52.1474171	7/12/2019, 19:
<input type="checkbox"/>	Program Files	File folder	16/06/2022, 13:56:14.6810...	7/12/2019, 19:
<input type="checkbox"/>	Program Files (x86)	File folder	6/10/2021, 23:57:25.1970661	7/12/2019, 19:
<input type="checkbox"/>	ProgramData	File folder	30/05/2022, 15:16:54.7218...	7/12/2019, 19:
<input type="checkbox"/>	Recovery	File folder	30/05/2022, 14:35:03.3239...	30/05/2022, 14:
<input type="checkbox"/>	System Volume Information	File folder	16/06/2022, 14:22:08.0496...	30/05/2022, 14:
<input type="checkbox"/>	Users	File folder	30/05/2022, 15:15:03.0372...	7/12/2019, 19:
<input type="checkbox"/>	Windows	File folder	17/06/2022, 9:24:08.7500654	7/12/2019, 19:
<input type="checkbox"/>	\$AttrDef	File	31/05/2022, 8:32:06.7208638	31/05/2022, 8:
<input type="checkbox"/>	\$BadClus	File	31/05/2022, 8:32:06.7208638	31/05/2022, 8:
<input type="checkbox"/>	\$Bitmap	File	31/05/2022, 8:32:06.7208638	31/05/2022, 8:
<input type="checkbox"/>	\$Boot	File	31/05/2022, 8:32:06.7208638	31/05/2022, 8:

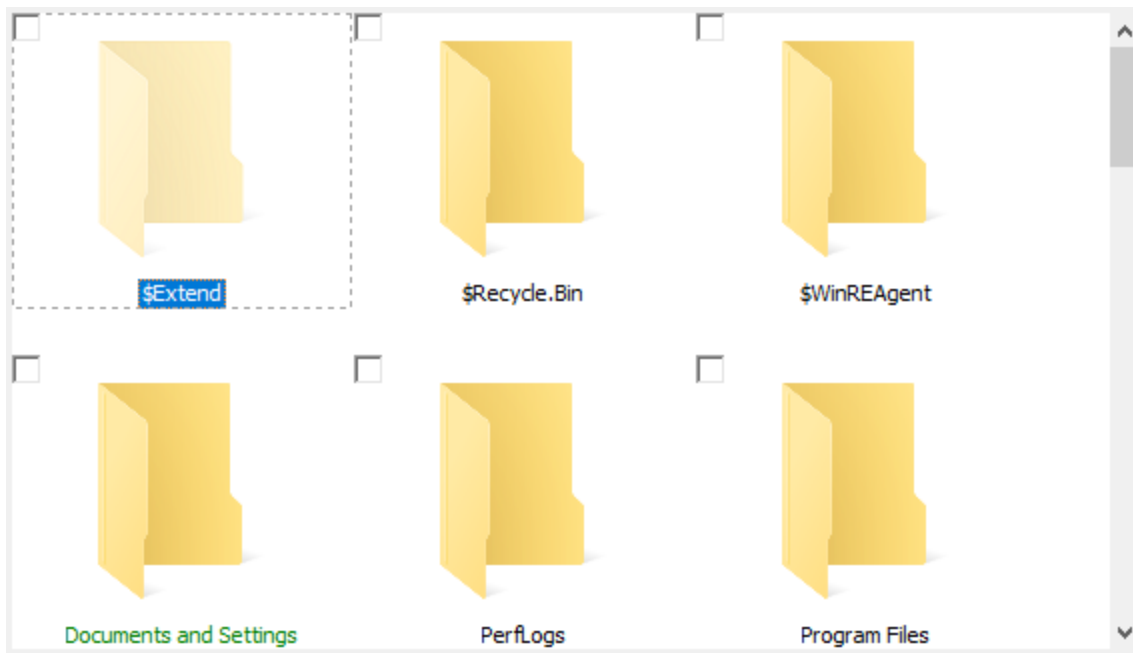
Small Thumbnails View

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.



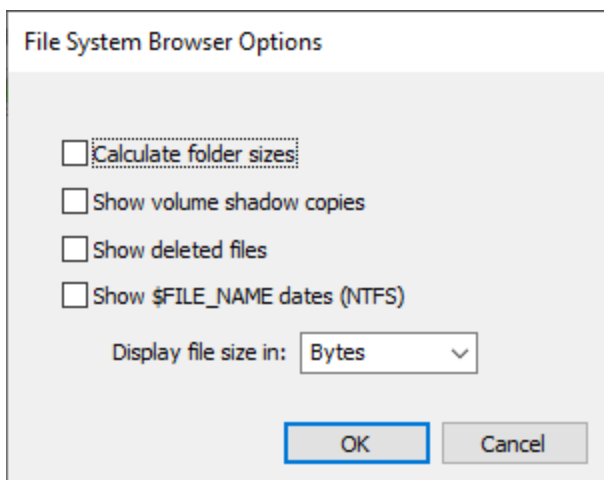
5.12.3 Shadow Copies

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:

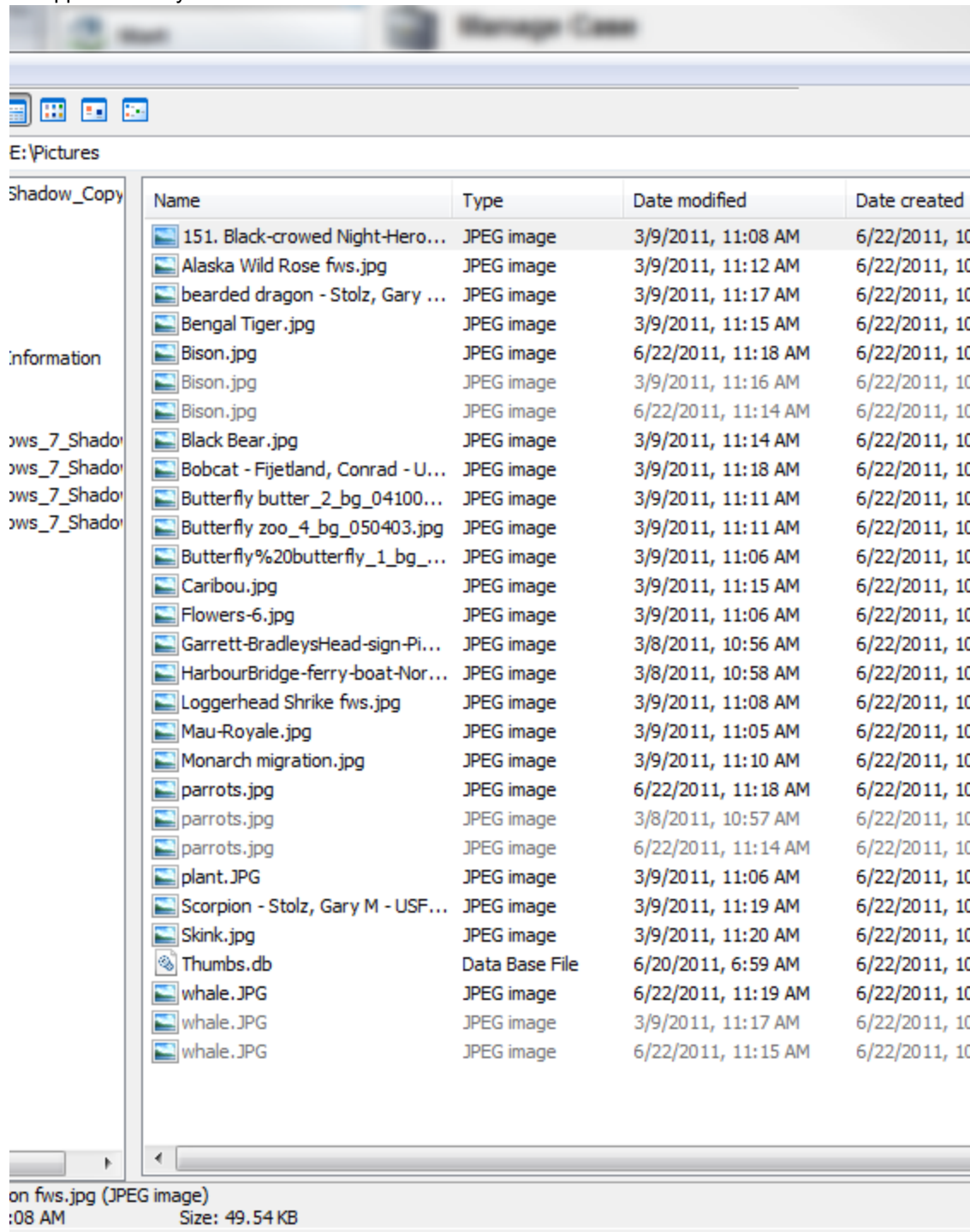
- Drive in Forensic Mode
- Physical Disks
- Volume Images

Enabling shadow copies in File System Browser

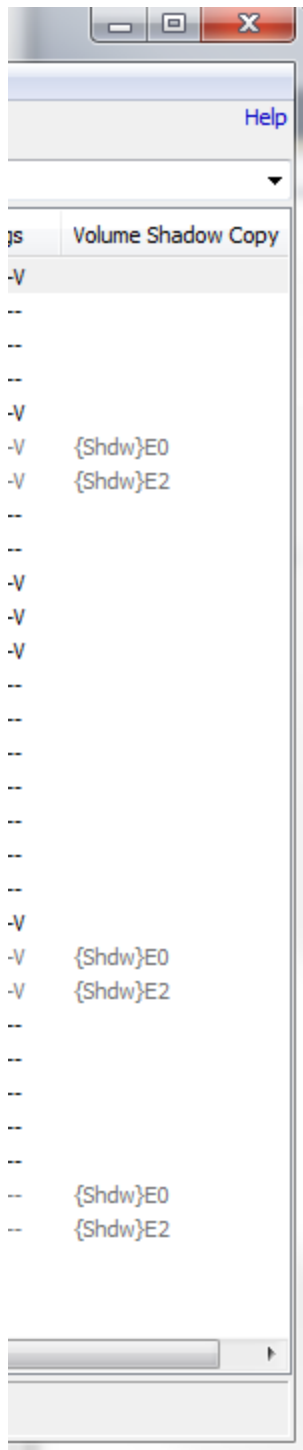
1. Add the supported device(s) to the current case.
2. Add the shadow copies for the volume added in step 1.
3. From the File System Browser window, select the "Tools->Options..." menu. Check the 'Show volume shadow copies' check box.



4. From the File System Browser window, select the "Tools->Options..." menu. Check the "Show volume shadow copies" check box.
5. Shadow copies of files will now appear along side the current files. A file will be considered a previous copy if the modified date differs from the current copy and other Shadow copies. Shadow copies will appear in Grey.

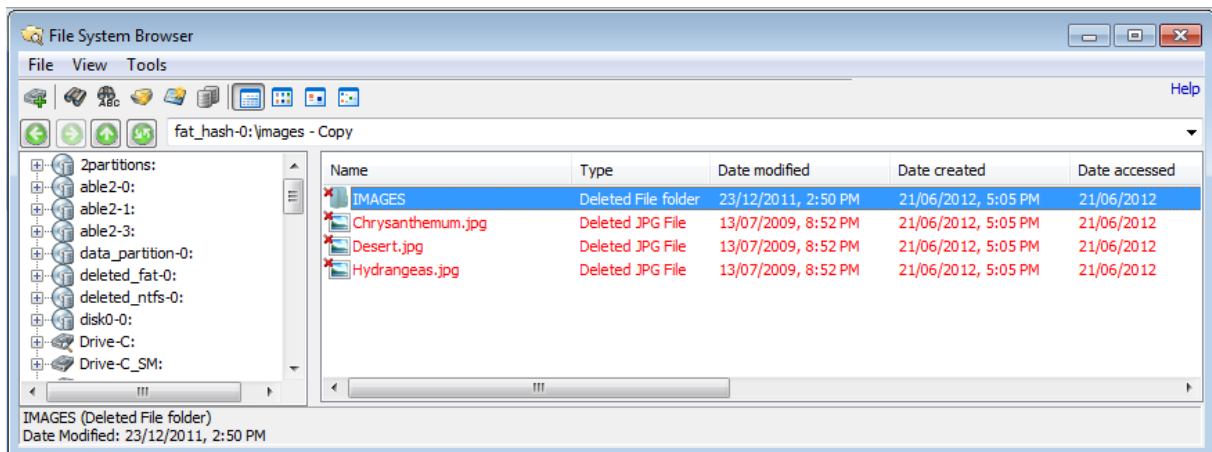


6. A new meta data column will be added to the end to indicate in which Volume Shadow Copy the file is from.



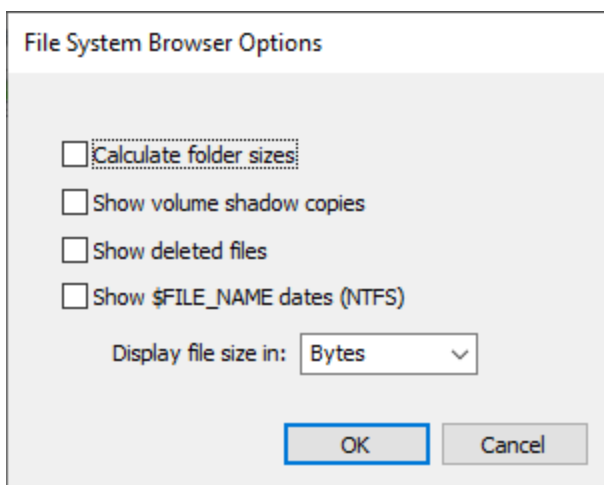
5.12.4 Deleted Files

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.



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.



Note: Enabling deleted files will cause the file entries to take longer to load.

5.13 Forensic and Cloud 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 and contents from supported Cloud Drive services.

Create Logical Android Image

Module that creates a logical Android image from an Android device using adb.exe.

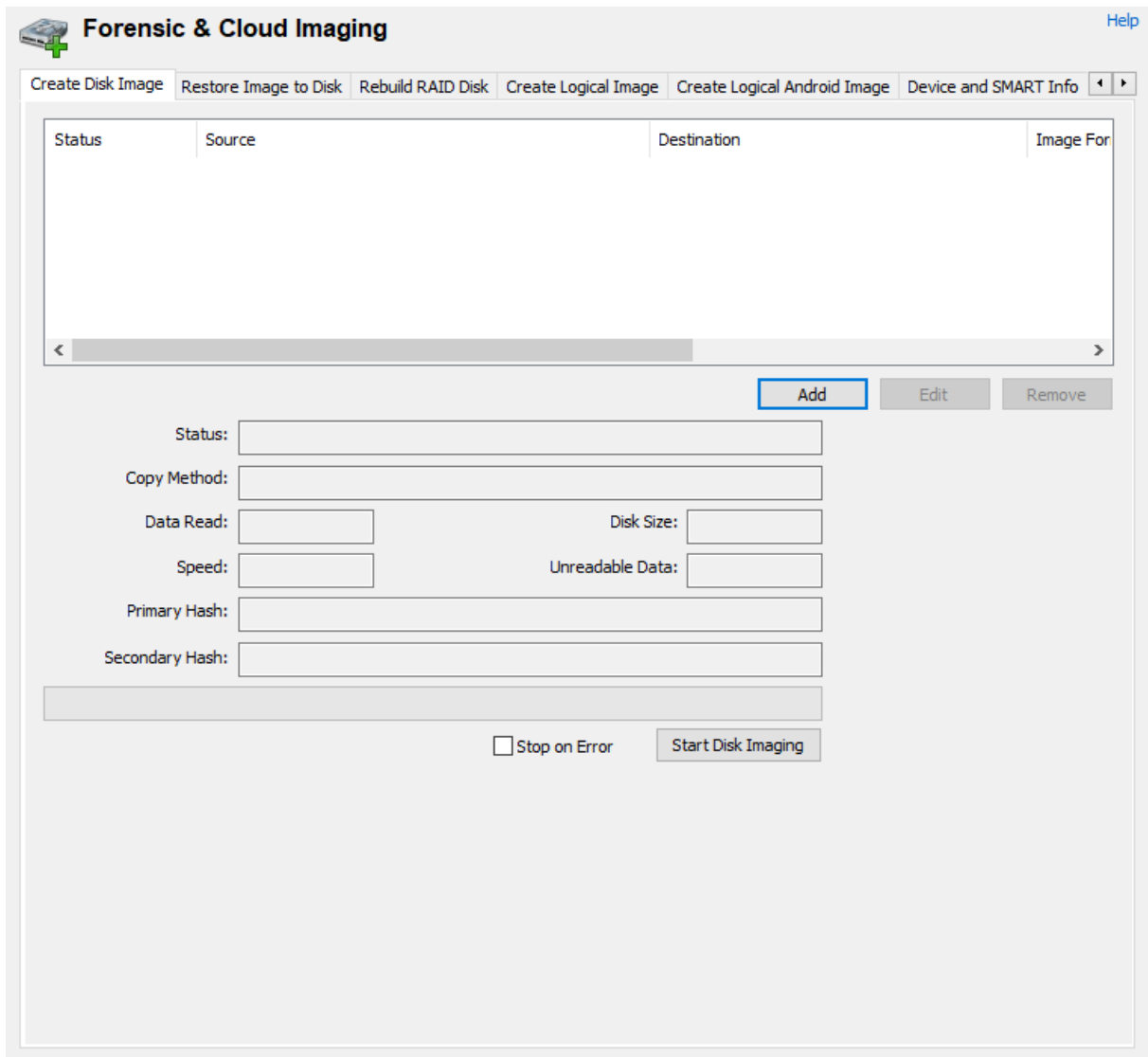
5.13.1 Create Image

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.



The screenshot shows the 'Forensic & Cloud Imaging' application window. The title bar includes a 'Help' link. The main menu contains several options: 'Create Disk Image', 'Restore Image to Disk', 'Rebuild RAID Disk', 'Create Logical Image', 'Create Logical Android Image', and 'Device and SMART Info'. Below the menu is a table with columns for 'Status', 'Source', 'Destination', and 'Image For'. The table is currently empty. Below the table are three buttons: 'Add', 'Edit', and 'Remove'. The 'Add' button is highlighted with a blue border. Below the buttons are several input fields: 'Status', 'Copy Method', 'Data Read', 'Speed', 'Primary Hash', and 'Secondary Hash'. There are also 'Disk Size' and 'Unreadable Data' fields. At the bottom, there is a checkbox labeled 'Stop on Error' and a 'Start Disk Imaging' button.

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

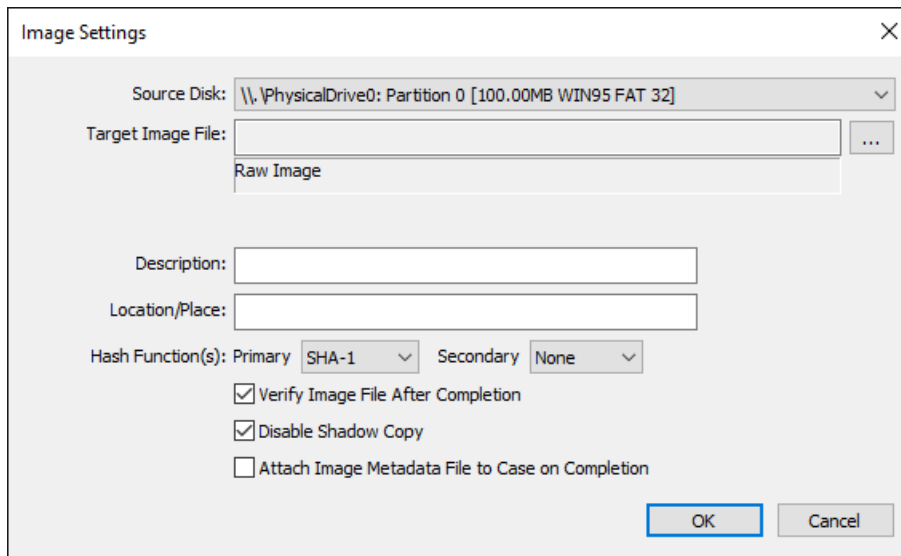
The method being used to create the disk image (either a shadow copy or a direct sector copy). Also whether OSF managed to lock the volume or not.

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.

Adding Source Disk to Image

To add source disk(s) to image, click the *Add* button to view the following dialog.



Source Disk

The partition, disk, volume or device to create an image of. Note that only partitions with drive letters can be shadow copied.

Target 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 (Fastest), Medium (Slow), or Highest (V. Slow).

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.

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.

In some cases this will slow down the imaging time as it can be slower to calculate a hash value than read or write to the disk however the speed will be different for each hash type and is very hardware dependent.

In order of speed we recommend;

- No hashing if speed is more important than being able to verify the image later
- SHA-1 on newer CPUs that support SHA instructions (AMD Zen 2017 and later, Intel Ice Lake 2019 and later)
- CRC32-C on older CPUs where an ability to verify the image is required (CPUs with SSE 4.1 support)
- MD5 on older CPUs where a more robust check of the image is required

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.

5.13.2 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).

The screenshot shows the 'Forensic & Cloud Imaging' application window. The 'Restore Image to Disk' tab is active. The 'Source Image File' field is empty with a browse button (...). The 'Target Disk' dropdown is set to '\\.\PhysicalDrive0'. There is an unchecked checkbox for 'Verify Disk After Completion'. Below these are fields for 'Status', 'Copy Method', 'Data Read', 'Speed', and 'Disk Size'. A 'Start Restoration' button is located at the bottom right of the main panel.

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'.

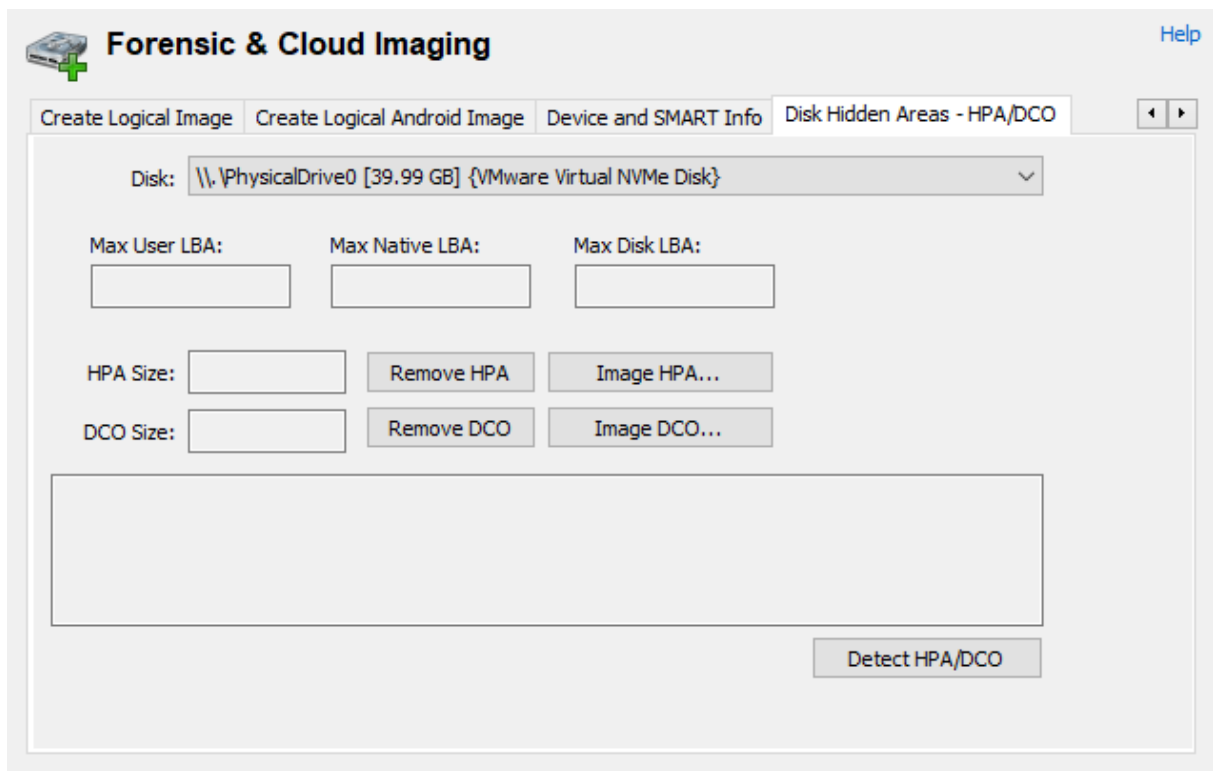
5.13.3 Hidden Areas - HPA/DCO

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. I.e. 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.*



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

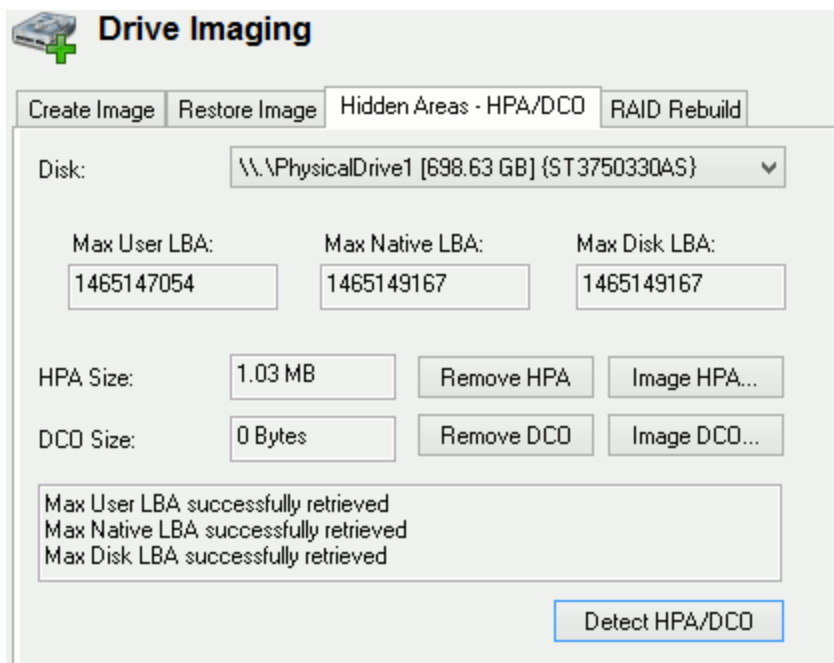
If present, an image of the DCO is created and saved to disk. The DCO is restored back to its original state after imaging.

Note: DCO can only be removed if no HPA exists on the disk. I.e. The HPA needs to be removed first before the DCO can be removed and/or imaged.

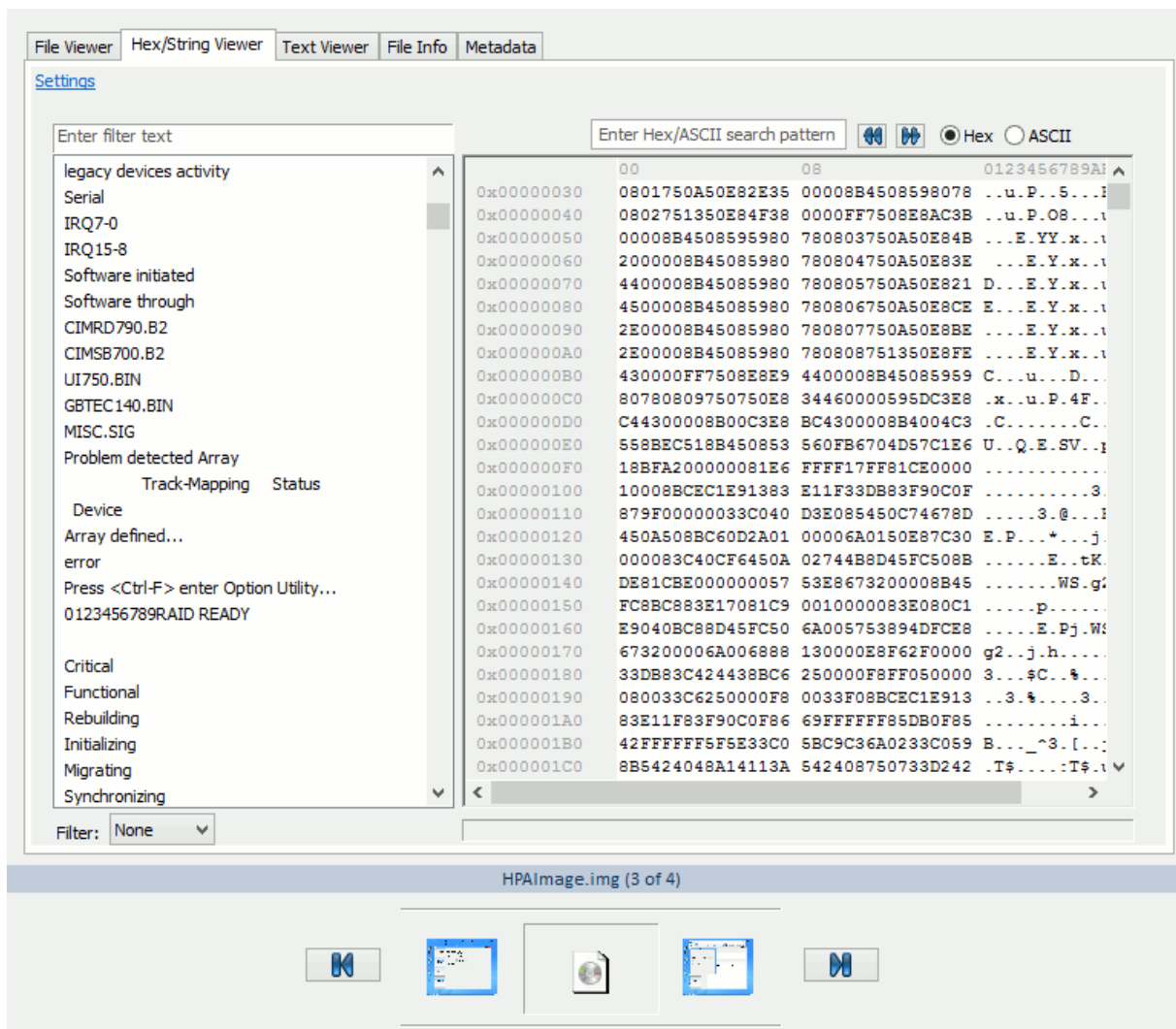
Depending on the hard disk, the HPA/DCO areas may be locked and therefore cannot be removed or imaged. This is indicated by "N/A" for the size of the area.

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 to save the contents of the area as an image file, in the example shown below clicking the "Image HPA..." button will allow us to save the contents of the detected HPA.



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 be 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.



5.13.4 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.

Forensic & Cloud Imaging Help

Create Disk Image | Restore Image to Disk | **Rebuild RAID Disk** | Create Logical Image | Create Logical Android Image

RAID Image Files:	Path	Format	Offset	Size	
					Add...
					Remove...
					Edit...
					Information

Configuration: RAID 0

Mapping:

Stripe Size: 512 Check parity/redundancy

Target Image File: ...

Status:

Data Written: Disk Size:

Speed: Unreadable Data:

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 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.

5.13.4.1 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:

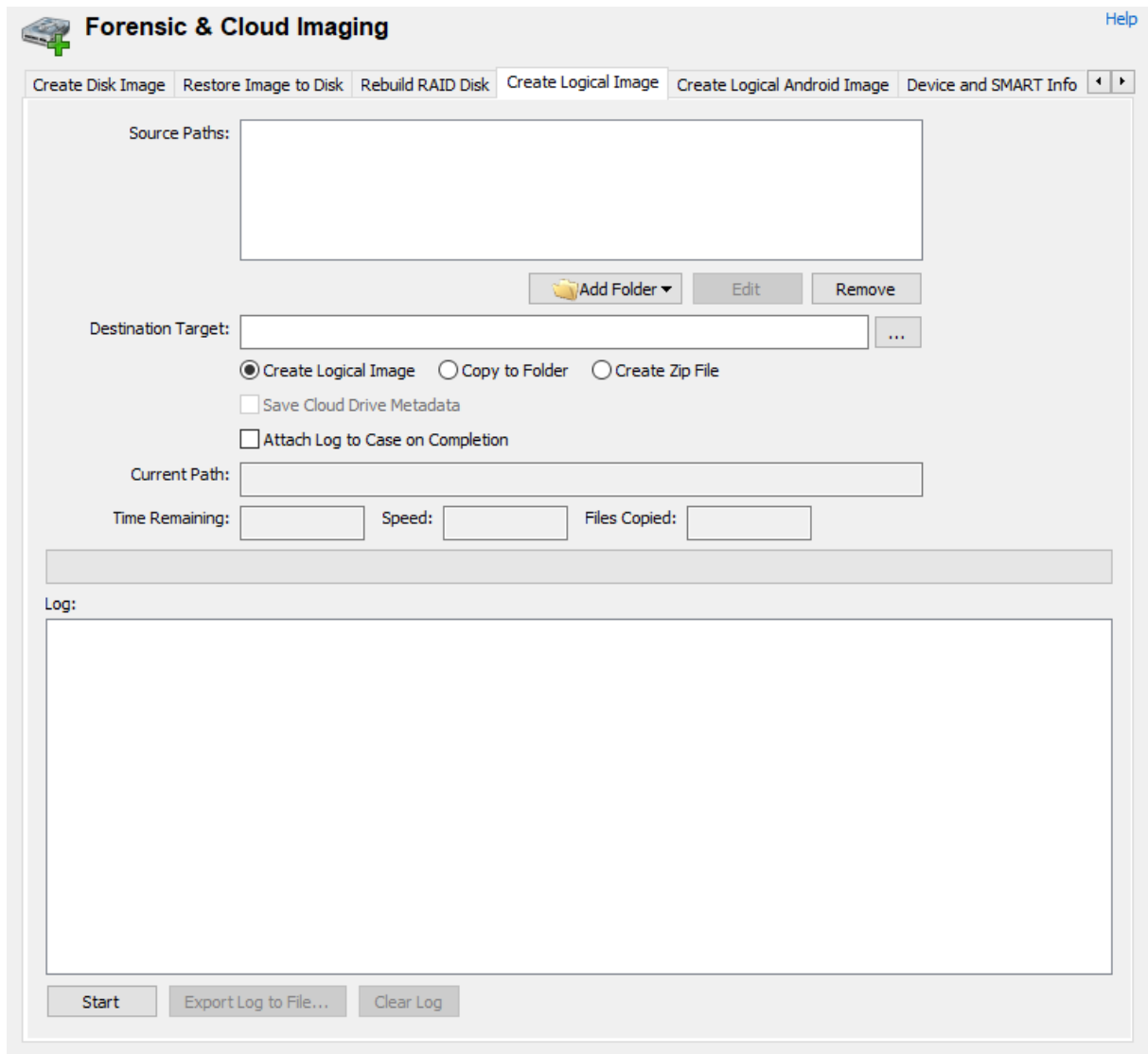
Metadata Format	Tested
Intel Matrix RAID	Yes
Linux mdadm RAID	Yes
SNIA DDFv1	Yes
Highpoint v2 RocketRAID	No
Highpoint v3 RocketRAID	No
Adaptec HostRAID	No
Integrated Technology Express RAID	No
JMIcron RAID	No
LSILogic V2 MegaRAID	No
LSILogic V3 MegaRAID	No
nVidia MediaShield	No
Promise FastTrak	No
Silicon Image Medley RAID	No
Silicon Integrated Systems RAID	No
VIA Tech V-RAID	No

5.13.5 Create Logical Image

Creating a logical image allows the investigator to copy files/directories from one or more source devices or complete Cloud Drives 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 (e.g. 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.



Settings and Options:

Source Paths

The partition, disk, volume or device to create an image of. Note that only partitions with drive letters can be shadow copied.

Add Folder - Add a folder to be imaged

Add File - Add a file to be included in the image

Cloud Drive - Add the contents of a Cloud Drive to the image

Cloud Email - Export the emails of a Cloud Webmail as an MBOX to the image

Destination Target

The location to save the image file (VHD) to (if **Create Logical Image** is selected) or the path to a local destination on the computer (if **Copy to Folder** is selected).

Save Cloud Drive Metadata

When Cloud Drive is added to the source list, the option can be selected. When enabled, in addition to the file downloaded from the Cloud Drive, an metadata file with the extension ".meta-json" will be created in the same folder for each file. This file will contain the response from the cloud service API that may contain additional information that was stored with the file. The contents of the metadata will vary by the Cloud Drive Service.

Attach Log to Case on Completion

Upon imaging process completion, prompt the user to attach the imaging log file to case.

File or Folder Source Items:

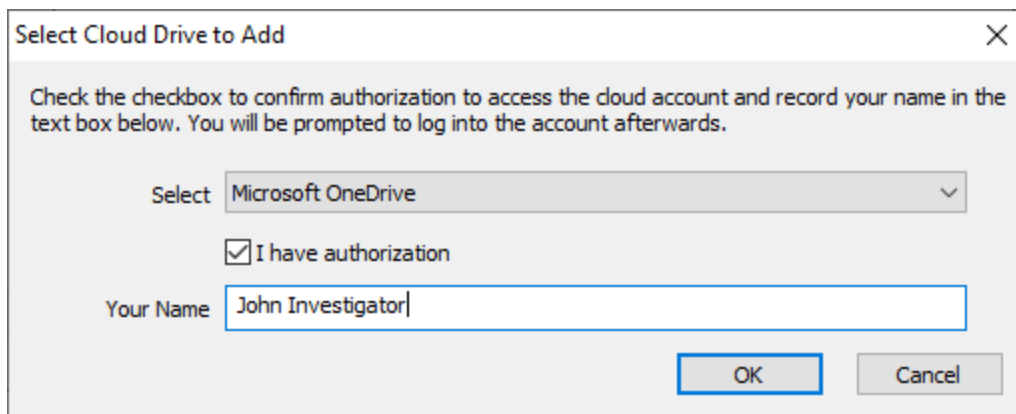
The following table summarizes the metadata that is preserved when performing a forensics copy of a **File** or **Folder** source Items

	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

Cloud Drive Source Item:

OSForensics currently supports downloading from Google Drive (Owned/Shared files), Microsoft OneDrive (Owned files) and Dropbox (Owned/Shared files) accounts. When adding a cloud drive source, the user will be required to acknowledge authorization to access the remote drive and will be prompted via the system's default browser to log into the service afterward.



When **Save Cloud Drive Metadata** is enabled, an additional file (with extension .meta-json) will be created along with the downloaded file. The contents of the file will contain additional information that was obtained from the Cloud Drive service. The metadata will vary by service.

Example metadata from Dropbox:

```
{
  ".tag": "file",
  "client_modified": "2018-06-18T18:13:31Z",
  "content_hash": "f7ad488deb7d81790340ecd676fe6e47f0a6064fb99b982685b752d58611c1cb",
  "has_explicit_shared_members": false,
  "id": "id:qWFLFkvdeUAAAAAAAAAABQ",
  "is_downloadable": true,
  "name": "Get Started with Dropbox.pdf",
  "path_display": "/Get Started with Dropbox.pdf",
  "path_lower": "/get started with dropbox.pdf",
  "rev": "2c82b3d90",
  "server_modified": "2018-06-18T18:13:32Z",
  "size": 1102331
}
```

Cloud Mail Source Item:

OSForensics currently supports exporting webmail to MBOX format from Google Gmail and Microsoft Hotmail/Outlook accounts. When adding a cloud mail source, the user will be required to acknowledge authorization to access the remote mailbox and will be prompted via the system's default browser to log into the service afterward. The resultant MBOX file can be accessed later using OSForensics' Email Viewer.

5.13.6 Create Logical Android Image

Creating a logical Android image allows the investigator to copy files/directories from an Android device 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 obtaining an complete drive image of the evidence device is not possible (eg. device not rooted). 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. Files are obtained using adb.exe pull command with the '-a' option which will try to preserve file timestamp and mode.

Additional artifacts can be retrieved using the **Extract Data with OSFExtract App** option. This will install the OSFExtract app onto the Android device and allow the retrieval of Messages (SMS, MMS), Contacts and Call Log from the device, that may not been retrievable using the Logical Copy method.

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 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.

IMPORTANT: To use adb with an Android device connected over USB, you must enable USB debugging on the device. This can be done in the device system settings, under Developer options on the Android Device itself.

Android Device

This drop-down list will show a list of Android Devices currently connected to the PC.

Extract Data with OSFExtract App

Use the companion OSFExtract App to retrieve additional data during the imaging process.

Logical Copy with Adb Pull

Copy files/directories from an Android device to a destination folder using adb.exe pull command. adb.exe is distributed by Google and a copy of the application is installed with OSForensics.

Copy Empty Files

Enable this checkbox to include files that are listed as 0 bytes in size during the copy process.

Ignore OS Directories

Enable this checkbox to skip known Android OS Directories from being scanned/copied. Directories on the ignore list are: /sys, /proc, /dev, /etc, /sbin, /d, /acct.

Destination Target:

The directory to save the files from the device (Copy to Folder) or location of an image file to write the contents to (Create Logical Image).

Attach Log to Case on Completion

A log is generated which contains the files/directories that were copied, general status messages and any error messages. When enabled, upon completion, OSForensics will add the log to the case.

Add Image as Device to Case

On completion, the specified target directory can be added to the current case as a device to be used in other modules.

Add to Scan List in Android Artifacts Module

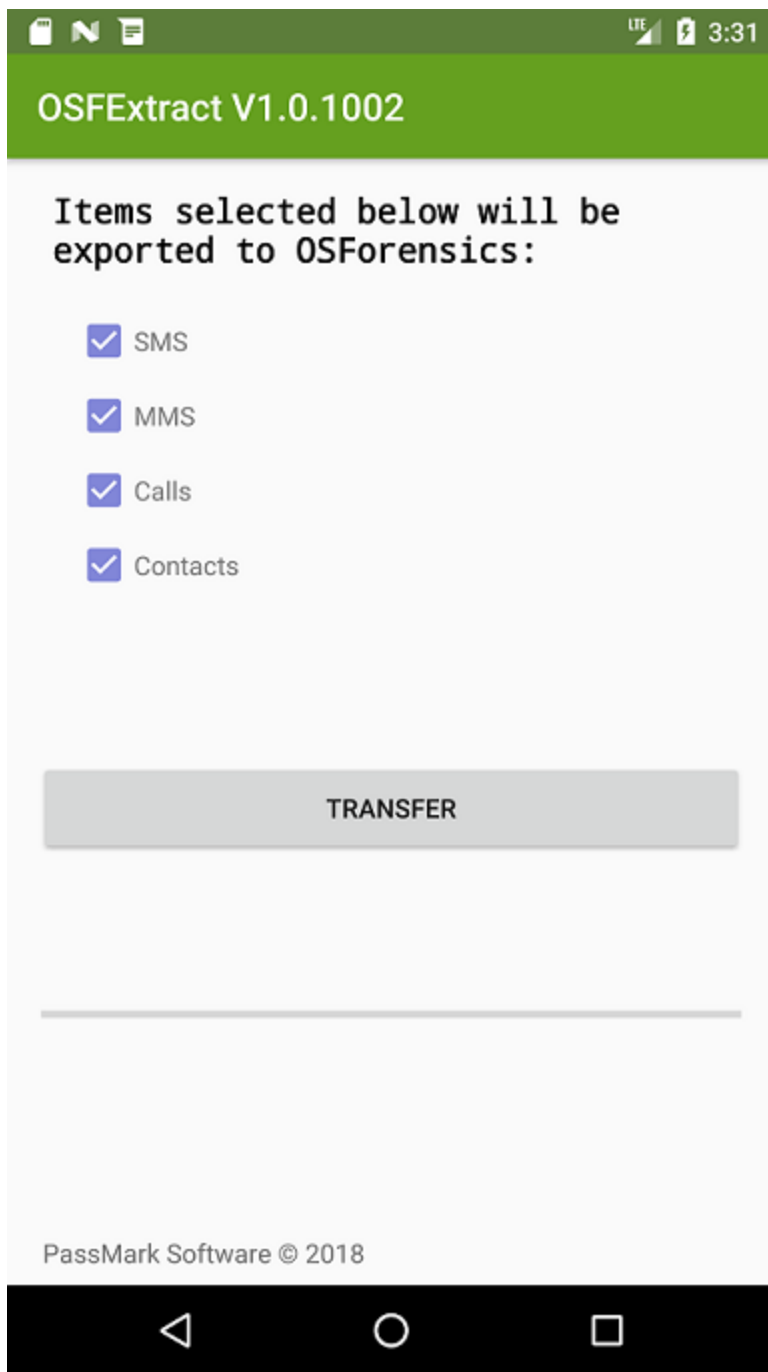
The path of the acquired image will be added to the scan list in the Android Artifact Module.

5.13.6.1 OSFExtract

OSFExtract is a supplemental Android application that aids in the retrieval of Messages (SMS, MMS), Contacts and Call Log from a device. The application must be installed on the Android device and granted permissions to properly function and communicate with OSForensics. The app is installed onto the device when Extract Data with OSFExtract App option is checked when doing Logical Android Copy. Note: The device must be placed in Developer mode for OSForensics via Android Debug Bridge (adb) to install¹ and launch the app and to correctly forward ports to retrieve the data over USB.

The following permissions must be allowed for OSFExtract to access data on the device:

- Allow OSFExtract to send and view SMS messages.
- Allow OSFExtract to access your contacts.
- Allow OSFExtract to make and manage phone calls.
- Allow OSFExtract to access photos, media and files on your device.



¹To manually side-load the app, osfextract.apk can be found in the adb sub-directory in the program executable directory. However the program is not much use without OSForensics.

5.14 Hash Sets

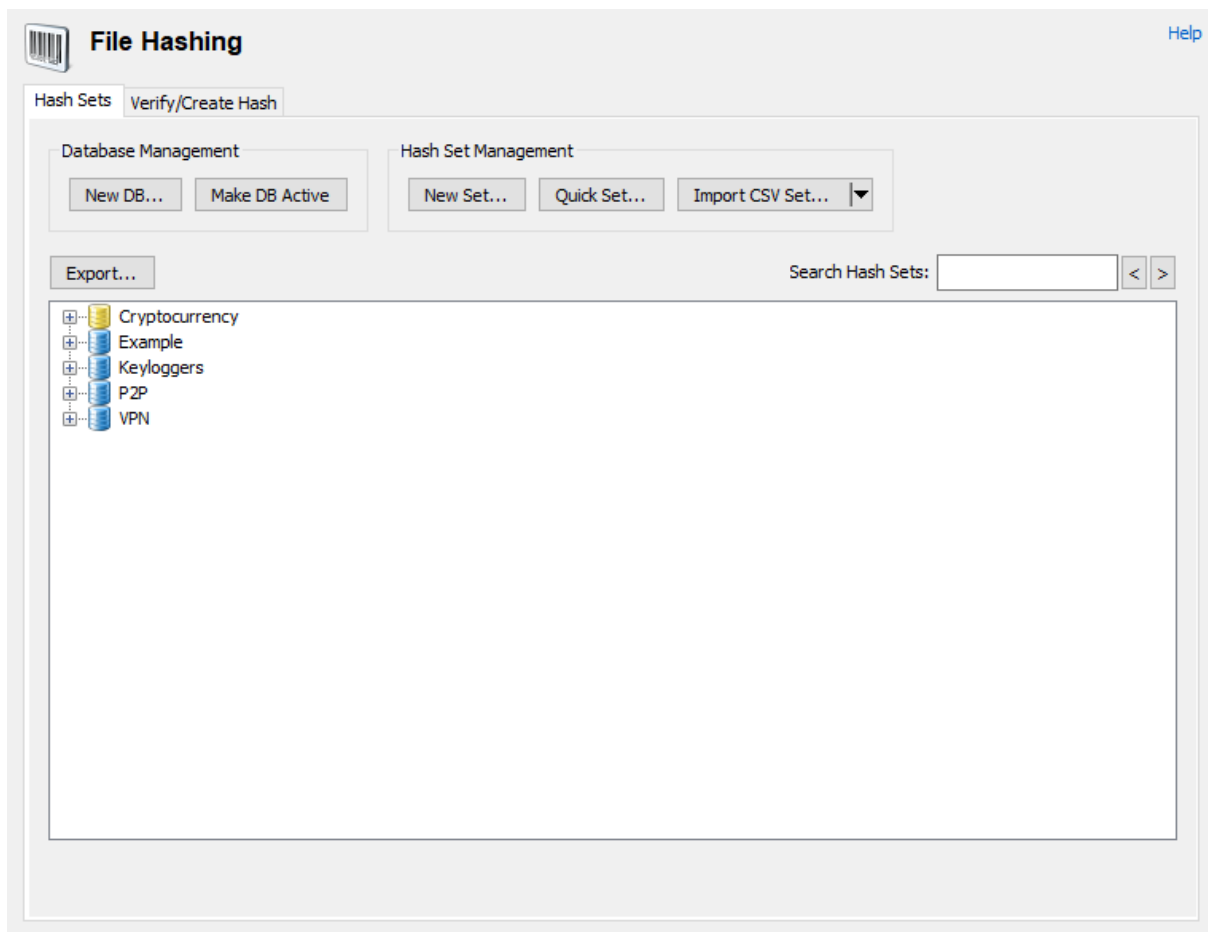
Hash Sets allow an investigator to quickly identify known safe files (such as Operating System and program files) or known suspected files (such as viruses, trojans, hacker scripts) to reduce the need for further time-consuming analysis. Hash Sets are used in a data analysis technique called Hash Analysis, 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.

Make DBActive

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.

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.

Import CSV/NSRL/VIC Set

Imports a hash set that was previously exported from OSF in csv format back into the currently active database.

Imports the NSRL (<http://www.nsrل.nist.gov/>) dataset into an OSForensics database. See this page for detailed instructions

Imports a VIC dataset into an OSForensics database. See this page for detailed instructions

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

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



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

5.14.1 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.

New Hash Set X

New Hash Set Help

Current DB: Cryptocurrency

Origin: PassMark New

Product Type: Cryptocurrency New

Manufacturer: AntPool New

File Set Type: Bad New

Hash Set Name: Windows 10 x64 New

OS:

Version:

Language: English

Folder: ...

Skip files smaller than... 5 bytes

Current File:

Files Hashed: Files Skipped: Time Elapsed:

Progress:

Create Cancel

More Info:
The origin of the files. Depending on the scope of the database this could be as specific as "Bob's PC" or as broad as an entire organization.

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.

Skip files

If this checkbox is checked then any files smaller than the entered byte count will be skipped and not added to the hash set.

This is enabled by default due to the large amount of 0 byte and small files that can be present on a system which will create a hash entry that will match many files (due to the limited amount of unique hashes generated for small byte files).

Current File

The file that is currently being processed.

5.14.2 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.

CryptoMining APMiner 1.0.8 | AntPool | English

Hash Set Viewer Help

Hash Set Name: CryptoMining APMiner 1.0.8 | AntPool | English
 Hash Set Type: Bad
 Operating Systems: Windows 10 x64

Name	MD5	SHA 1	SHA256	Last Update	Size	Category	Internal ID
SERVICEREMEDI...	E5E715FD96...	660FC20970...	2C5EC5B9E0...	2019-03-29 1...	64.00 KB		2710
SERVICEREMEDI...	24C408E1E5...	DD458A93C0...	D71123DAD5...	2019-03-29 1...	128.0 KB		2711
UPDATESESSIO...	9EA2A2DA1C...	CF5F226280...	39DBEB7A3A...	2019-03-29 1...	8.00 KB		2712
{3DA71D5A-20C...	9DD598B973...	CE32969D25...	A43EF5B572...	2019-03-29 1...	81.65 KB		2713
APPCACHE1319...	00E25757619...	0854A1E260...	673B3520DB...	2019-03-29 1...	94.93 KB		2714
APMINERTOOL_...	1D2760C03B...	194508B8041...	324BC4575A...	2019-03-29 1...	2.26 MB		2715
APMINERTOOL....	138152EA0C...	C7951C6B7C...	3699A56A00...	2019-03-29 1...	2.95 MB		2716
APMINERTOOL....	D7795D7C80...	1911882F300...	88F73F308D...	2019-03-29 1...	17.79 KB		2717
APMINERTOOL....	12427512AA...	2E46D410F8...	25C3211C2A...	2019-03-29 1...	599.5 KB		2718
APP.CONFIG	A6F94FCA3D...	304B78AF33...	5E971DFC00...	2019-03-29 1...	16.92 KB		2719
APP.XAML.CS	2F778403797...	502F155D7F...	253DED77F0...	2019-03-29 1...	338 Bytes		2720
CONFIG.XML	CB2A827782...	65B2D363C3...	9B99B31B41E...	2019-03-29 1...	10.83 KB		2721
EN_US.XAML	CEDF1A4370...	89DA9749D7...	D93AF699D8...	2019-03-29 1...	21.99 KB		2722
ZH_CN.XAML	36682EDD3D...	A68A7AD11B...	AA3E976A76...	2019-03-29 1...	21.81 KB		2723
LOG_2019-3-29...	159D7046D4...	30558CBF99...	B0C3B46030...	2019-03-29 1...	39 Bytes		2724
128X128.ICO	B1B44C9C2A...	134FF9DD1E...	C3756C14BE...	2019-03-29 1...	66.06 KB		2725

Number of files in set: 31, Total Size: 6.36 MB

Close

The table contains a list of files in the hash set and corresponding hash values.

5.14.3 Hash Set Lookup

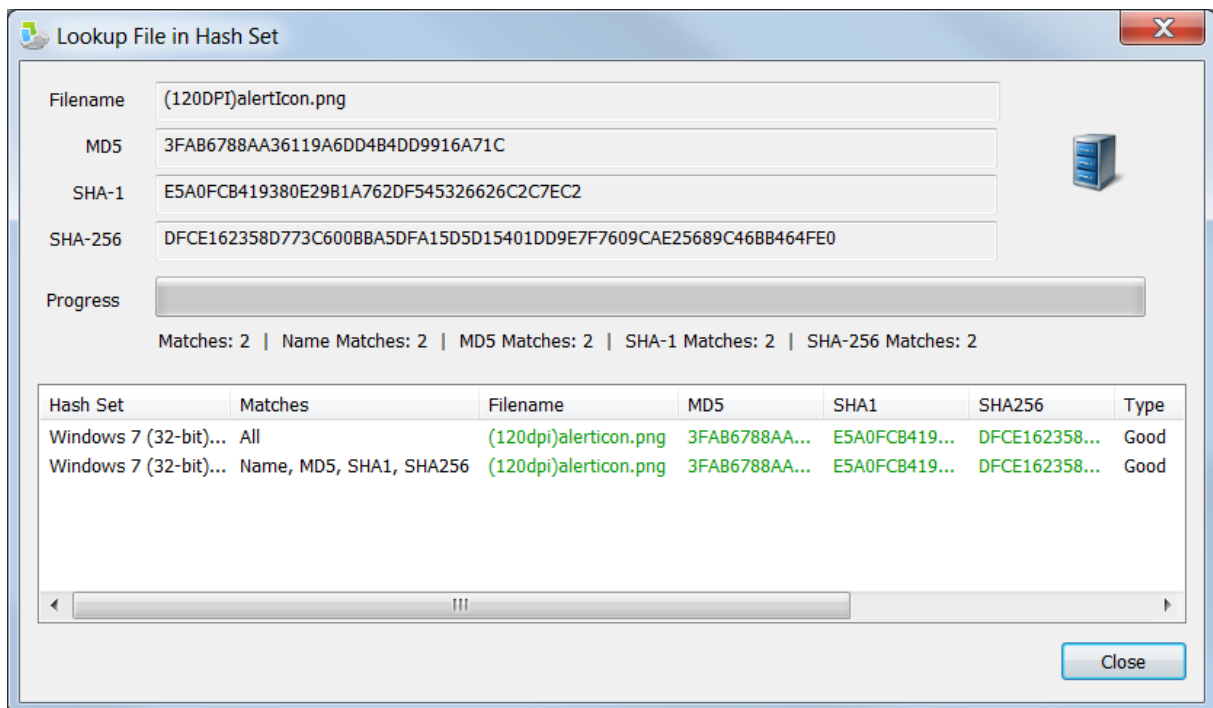
In either the File Name Search or the Mismatch Search module, it is possible to do a lookup on the files found to see if they exist within the current hash database. This is accomplished by right clicking in the list and choosing "Look up in Hash Set".

Depending on whether 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 whether a match was found.

baselineinfo_v7.png
 Location: C:\\$Recycle.Bin\S-1-5-21-396346047-3584240248-2203478571-1000\SP0B3REYHTML
 Size: 94.31 KB, Created: 10-Dec-2008 05:58, Modified: 17-Nov-2008 02:50, In hash set: No

Single File Hash Lookup

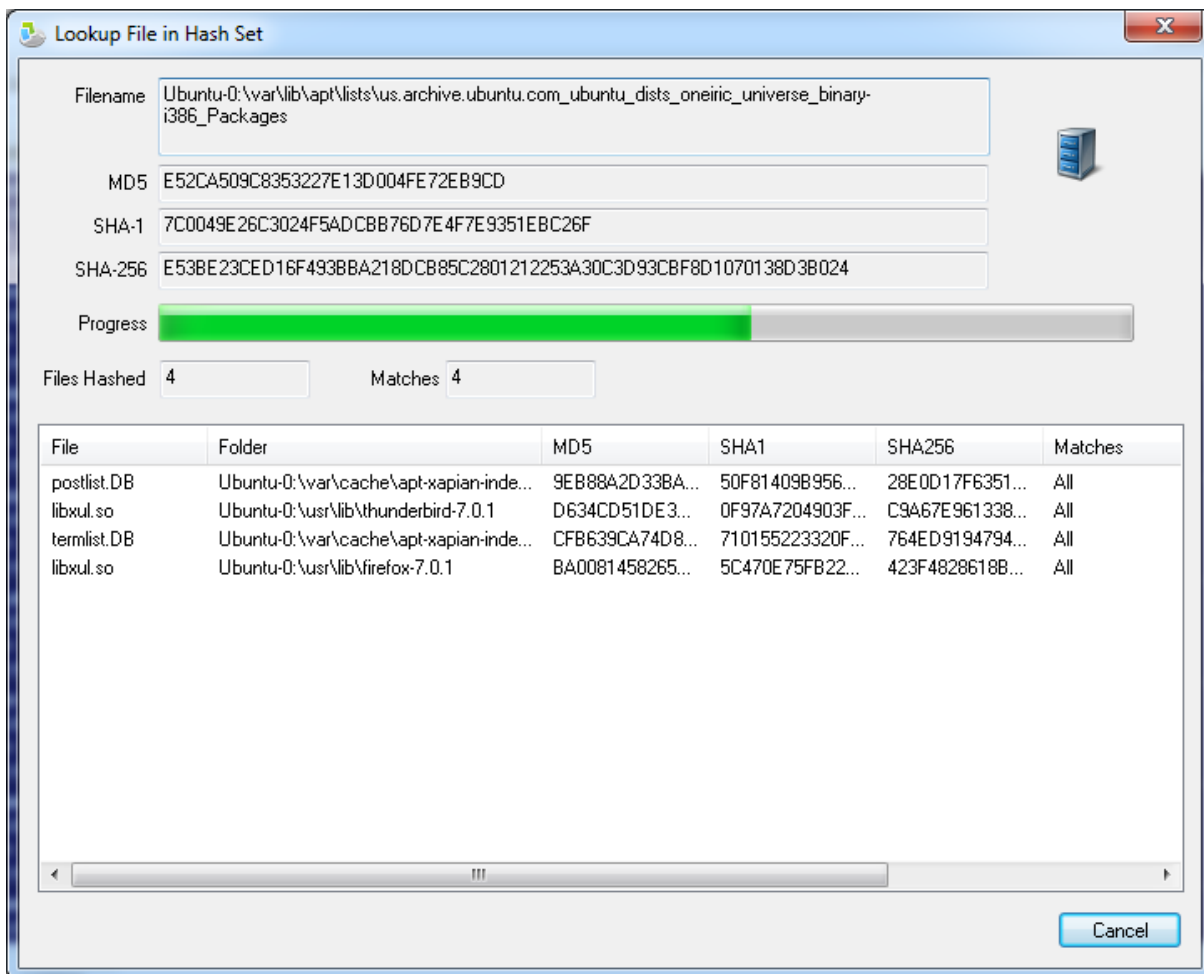
The results of the lookup are displayed in the table, listing any matches that were found in a hash set in the active database.



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.



The list of matching files can be exported to a text file by selecting 'Export list to text...' in the right-click menu.

5.14.4 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>

5.14.5 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 can be distributed as a set of .iso files or as a zip, if the files are contained in a zip then unzip the files to a temporary folder (eg named "NSRLData") and go to step 3. To access the contents of the .iso 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 separate 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. Select the "NSRL Import.." button on the hash management window.
4. Specify the input data folder, this will be the root folder for all the unzipped sub folders (the "NSRLData" folder in the example from step 2).
5. Specify the temp output folder. If this field is left blank, the database will be written directly to the final default location for hash sets. Otherwise, if this folder is specified, OSForensics will write the output database to a temp folder before copying it over to the final location. Therefore, specifying a location on a fast SSD or RAM drive can help speed up the import significantly (see below for more information).
6. Click "OK" and allow the import complete. A new database will be created automatically, and the database name will default to the format 'NSRL-YYMMDD-HH-MM'. To use a different name, wait for the import to complete, right-click the database in the tree, and select "Rename".

One way to speed up the process is to make sure the input data and the output data folder are on a fast solid state hard drive or a RAM drive. Import time is highly dependent 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 an import time somewhere between these two figures.

Important Note: The NSRL Import function assumes that in the input NSRLFile.text file, lines have been sorted in alphanumeric order. If not, errors may occur during the import.

Using a RAM drive

When creating a RAM drive to store both the input files and output files, it is important to allocate enough memory on the RAM drive, otherwise the import will fail once the drive runs out of space. While it is not possible to accurately predict what the exact size of the output files will be, the following example may be used as a rough guide:

For the NSRL RDS Version 2.59 December 2017 Modern RDS (minimal) dataset, the total size of the input files was 13.7 GB.

Once the import was complete, the output database file was 19.9 GB. (~1.5x the size of the input data) Thus, at least 24GB was needed on the RAM drive to store both the input and output files.

Roughly this gives the following formulation:

Required memory = Size of input data x 2.5

It is also advised to add on a margin for error (e.g. 10%) if possible.

Note that this example is for the Modern RDS **microcomputer applications** dataset which contains many redundant entries due to there being multiple entries per file appearance in an application. OSForensics only stores one file hash entry per file appearance in an application (appearances occurring on different operating systems are ignored by OSForensics).

The Modern RDS **minimal** dataset also contains some redundant entries but less so than the above, so the output file size factor would be higher.

The Modern RDS **unique** dataset contains only unique hash values, so the output file size factor would be higher than both of the datasets mentioned above.

More information on the different datasets can be found at the NIST website.

5.14.6 VIC Import

To import a Project VIC .json file, make sure you have selected an active database, then click "*Import VIC Set...*", select the .json file to import, and click "OK".

You will then be prompted if you wish to import the VIC set into the selected database. This allows you to incrementally add hashes into the same database. Click "Yes" to proceed, or "No" to create a new database.

Correctly formatted project VIC files will import file hashes into a series of file sets with a maximum number of 100,000 file hashes per file set.

Note that the process can several hours to complete, and could even take several days on some systems.

An indicator of bytes read displayed at the bottom of the window can be used as a rough guide to calculate the time remaining.

You can also select "*Import VIC Set Folder*" and specify a folder that contains .json files. OSF will attempt to import each of these .json files into the same database and omit any which are duplicates.

OSF currently supports Project VIC file formats version 1.2, 1.3 and 2.0.

NOTE: While "Category 0 (Zero)" is officially documented as files of "Unknown" category, in the data we've seen this has been treated as a category for "safe" files, and so OSF currently excludes importing all hashes with a "zero" category.

5.14.7 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	A description of the what type of product the product is.
Type	
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.

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.

5.16.1 Create Index

Creating an index allows the investigator to perform lightning 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.

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 Check All Uncheck All

E-mails Attachments Executables and binary files

Office + PDF documents Memory dump files

ZIP and compressed archives All other supported file types

Images Unknown files

Plain text files System hibernation and paging files

Web files + XML Use OCR for images and PDF documents

Video, audio and other media

Use previously saved configuration:

Configuration	File Types
---------------	------------

Next

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 load from a previously saved configuration. 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, .ost, .msg, .eml, .mbox, .mbx, .dbx and .msf files.

Attachments

Scan all attachment documents found in email messages.

Office + PDF Documents

Scan Microsoft Office documents, OpenOffice documents and PDF files. Supports .doc, .dot, .ppt, .pps, .pot, .xls, .xlt, .docx, .pptx, .xlsx, .dotx, .pdf, .odt, .sxw, .ods, and .odp.

ZIP and compressed archives

Scan the contents of 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. Other compressed archives supported are: .zipx, .tar.gz, .tar, .tgz, .taz, .rar, .arj, .dmg, .iso, .chm, .bz2, .lzo, and .7z

Images

Scan image files for metadata information. Supports .jpg, .gif, .tiff, .png and .bmp.

Plain Text Files

Scan plain text files and rich text documents.

Web Files + XML

Scan HTML web pages and scripts including .html, .htm, .shtml, .shtm, .xml, .xhtml, .php, .asp, .aspx, .cfm, .js, .pl, .cgi, and .swf 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, .qbb

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?

File Details	Type
C:	Folder

Add...
Remove

Advanced settings (optional)

File extensions	Edit	Precognitive search	Edit
Skip files/folders	Edit	Binary string extraction	Edit
Languages & Stemming	Edit	Email attachments	Edit

Back Next

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:

Add Start Location [X]

Whole 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:\

OK Cancel

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 a .doc file, it still isn't processed like a Word document. Only string extraction is done.

Advanced settings (optional)

On Step 2, you can also configure advanced indexing settings such as File Extensions, Skip files/folders, Languages, Precognitive searches, and more. Click on the "Edit" button to configure each of these groups of settings. For more information, see "Advanced Indexing Options".

Step 3: Memory optimization / Indexing limits

Step 3 of 5

Memory optimization / Indexing limits

Estimate the number of files (and size) being indexed. This will help optimize memory usage and index more efficiently.

Small
 Medium
 Large
 Extreme
 Don't know (Pre-scan required)
 Custom

Max number of files = 500,000
 Max file size* = 47 MB
 Estimated RAM required: 4,600 MB (4.6 GB)
 Available RAM: 5,072 MB (5.1 GB)

*Max file size does not apply to some file formats

Select number of threads:

Use RAM drive for temporary files to speed up indexing

In order to index the files more efficiently, OSForensics needs to know the approximate number of files and the maximum file size that will be scanned. If this is not known, you can select 'Don't know' which will conduct a preliminary scan of the location and files to determine the proper limits for the indexing process. To set custom limits, select 'Custom' and click on 'Edit' to bring up a dialog box for specifying the limits.

Custom Indexing Limits [X]

If you need to override the preset limits available, you can specify custom limits below. [Help](#)

Max number of files:

Max file size: KB (100.00 MB)

TIP: To reduce indexing time even further, check 'Use RAM drive'. For more information see 'Indexing with a RAM drive'.

Step 4: Case Details

Step 4 of 5

Please enter some details for the index

Index Title
My Index - C

Index Notes

Index of files in:
C:
File extensions:
.pst, .ost, .msg, .eml, .emlx, .mbox, .mbx, .dbx, .msf, .doc, .dot, .ppt, .pps, .pot, .xls, .xlt, .docx, .pptx, .xlsx, .dotx, .pdf, .odt, .sxw, .ods, .odp, .zip, .tgz, .taz, .tar.gz, .tar, .zipx, .rar, .arj, .dmg, .iso, .chm, .bz2, .lzo, .7z, .jpg, .jpeg, .jpe, .gif, .tiff, .tif, .png, .bmp, .heif, .heic, .txt, .text, .rtf, .html, .htm, .shtml, .shtm, .xml, .xhtml, .php, .php3, .asp, .aspx, .cfm, .js, .pl, .cgi, .swf, .nfo, .dat, .wpd, .mp3, .dwf, .torrent, .mht, .avi, .wmv, .wma, .mpg, .mpeg, .rmv, .rmvb, .flv, .mov, .qt, .exe, .dgn, .cab, .psd, .qbb, .dmp, .mdmp, .mem
(No ext)
(Unknown ext)
(System hibernation and page files)

Back Start Indexing

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 5: Indexing

Step 5 of 5

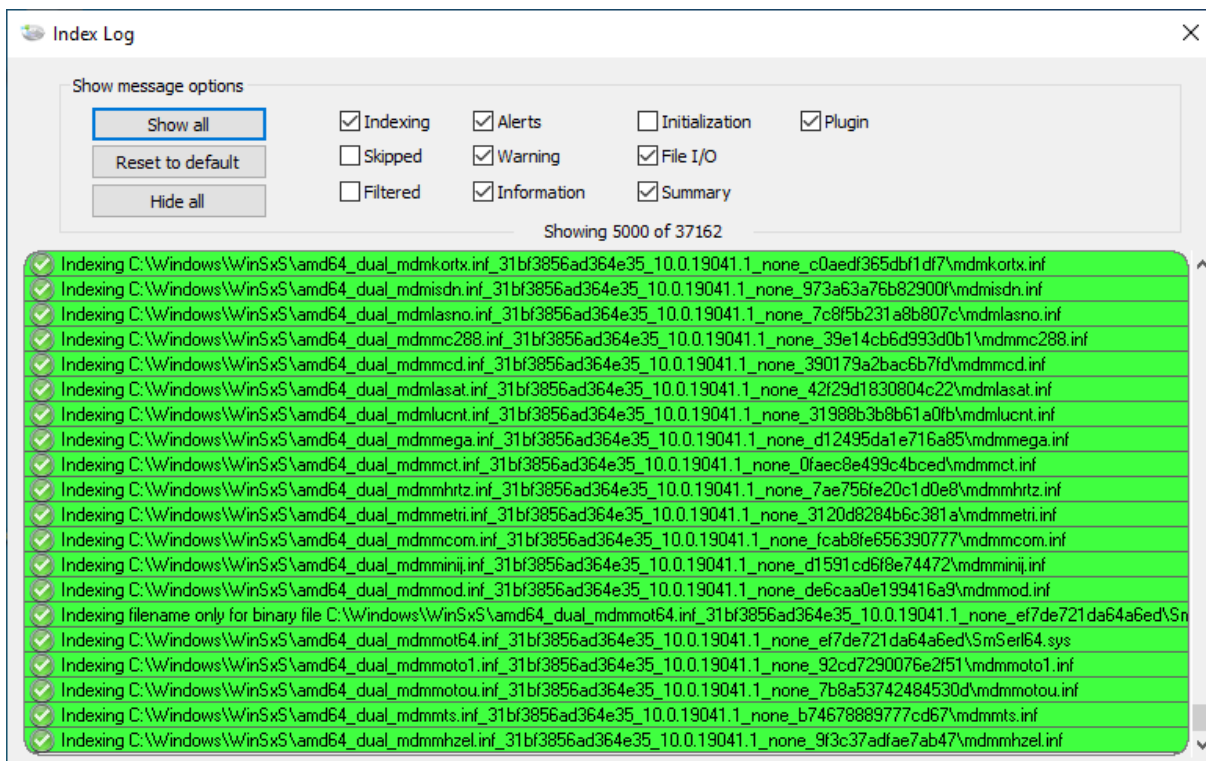
Start Time	Finish Time
Mon Aug 1 14:08:18 2022	Mon Aug 1 14:08:21 2022
Files Indexed	Time Elapsed
8	00:00:03
Emails Indexed	Peak Phys. Mem. Used
737	241 MB
Alerts	Peak Virt. Mem. Used
0	4530 MB
Warnings	Max File & Emails
0	500000
Total Bytes	Unique Words
851.2 KB	9057

Current Action:

Thread #	Indexing file
Thread 1	{Finished}
Thread 2	{Finished}
Thread 3	{Finished}
Thread 4	{Finished}

< >

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.



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

5.16.1.1 Indexing Problems and Solutions

The indexing process fails due to not enough memory

Indexing uses a lot of 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 than 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 inaccessible. 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.

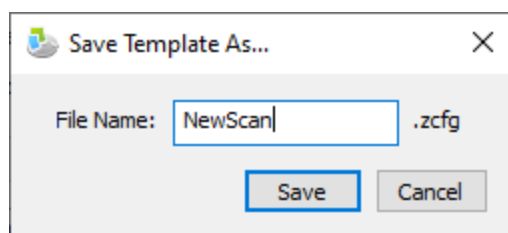
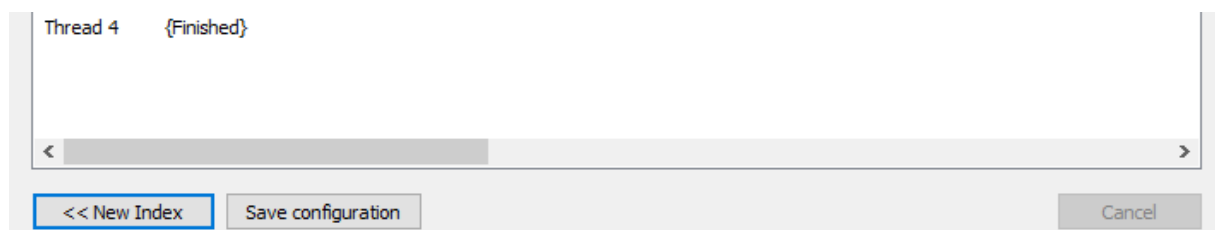
Limits on recursive indexing

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.

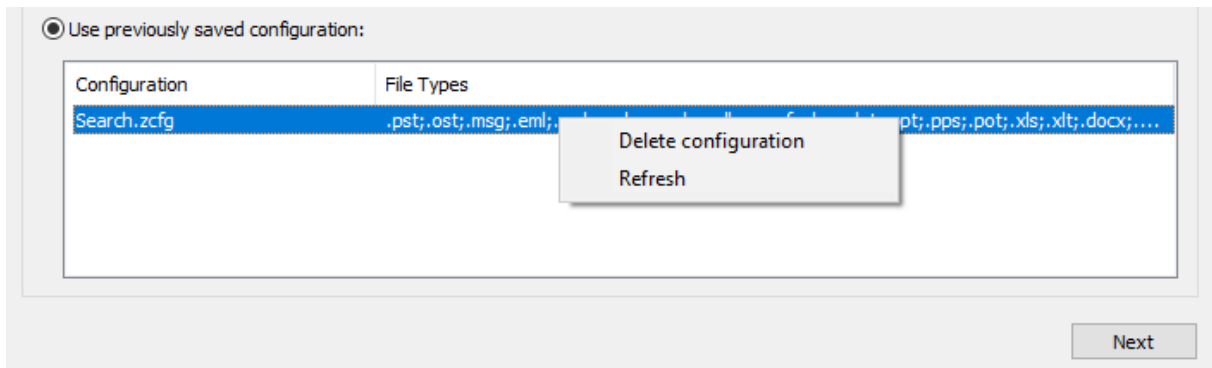
For e-mails containing attachments (which may themselves be another e-mail containing yet another attachment), OSF will successfully index recursively until the URL is too long to return meaningfully as a search result. There is no fixed depth limit for recursively indexing e-mail attachments.

5.16.1.2 Save Indexing Configuration

Saved configurations allow the user to specify a previously saved configuration. Once indexing has completed, you can save your configuration in Step 5 of the index creation procedure.



To use the saved configuration, select 'Use previously saved configuration' from Step 1 of the index creation procedure.



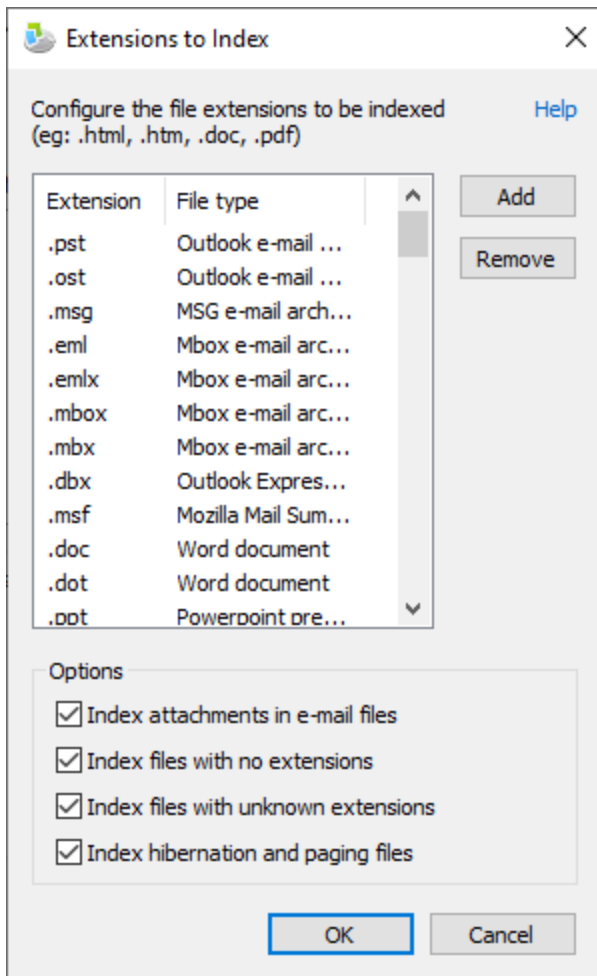
Delete configuration

Deletes the template file from OSForensics

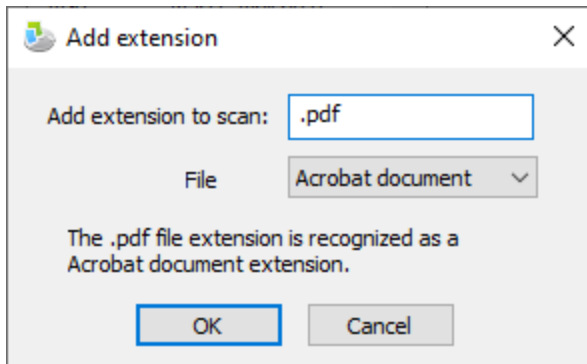
5.16.1.3 Advanced Indexing Options

Under step 2 of the "Create Index" module, you can Edit the following advanced indexing options.

File 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.



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

Index attachments in e-mail files

If checked, attachment files found in e-mails will be indexed. Note that attachment files can be of many different file types.

Index files with no extensions

If checked, files without an extension are included in the indexing process

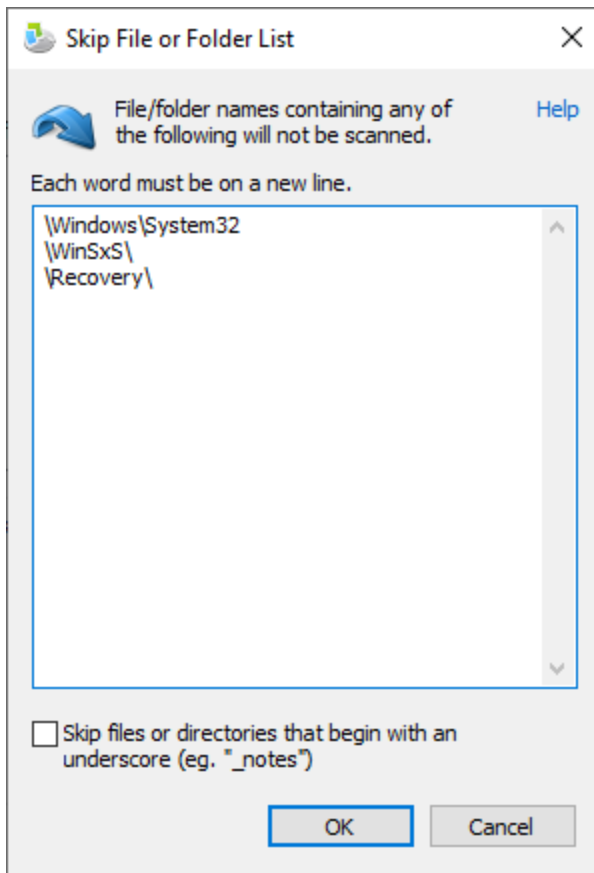
Index files with unknown extensions

If checked, files not included in the list are included in the indexing process

Index hibernation and paging files

If checked, Windows system hibernation (hiberfile.sys) and page files (pagefile.sys) are indexed. 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.

Page and folder skip list

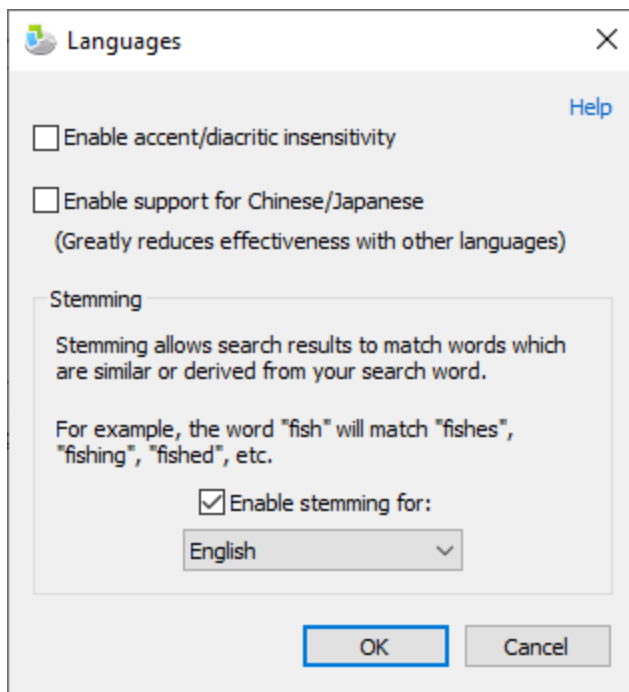


Pages and folders containing particular words can be excluded from the scan by adding the words to the list. Note that the folder the created index files are written to is also automatically added so that the indexing process does not index the files it is creating. This folder is a sub folder of the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

Languages and Stemming



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".

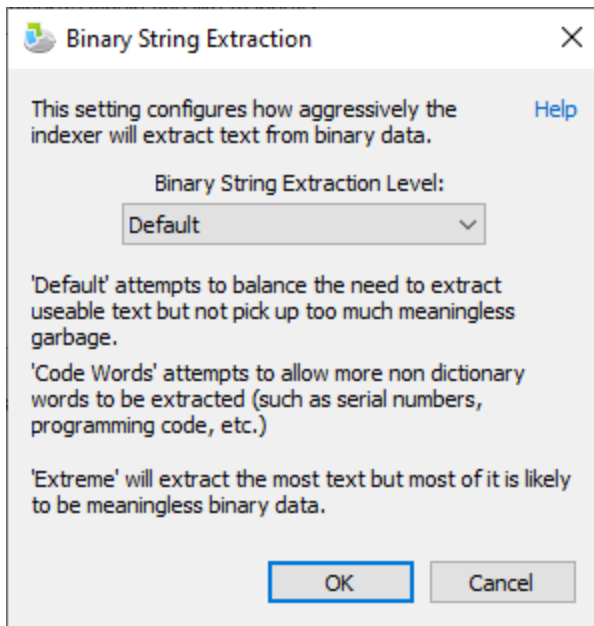
Support for Chinese/Japanese

Enabling this feature will ignore space delimiting rules (important for Latin based languages) that typically helps when matching against Asian languages such as Chinese and Japanese. However note that this greatly reduces effectiveness when searching with English and other Latin-based languages. It is advised to create a separate index with this setting enabled if you need to search for both types of languages.

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.

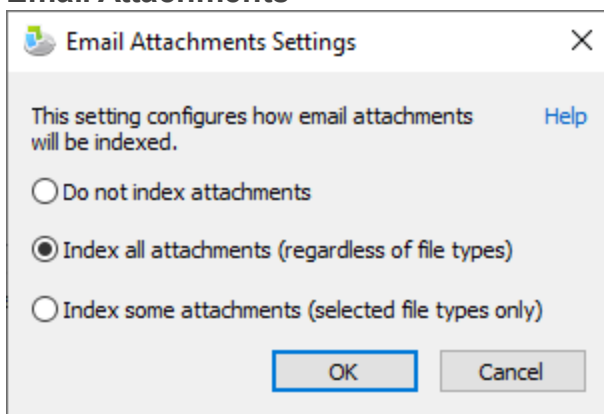
Binary String Extraction



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.

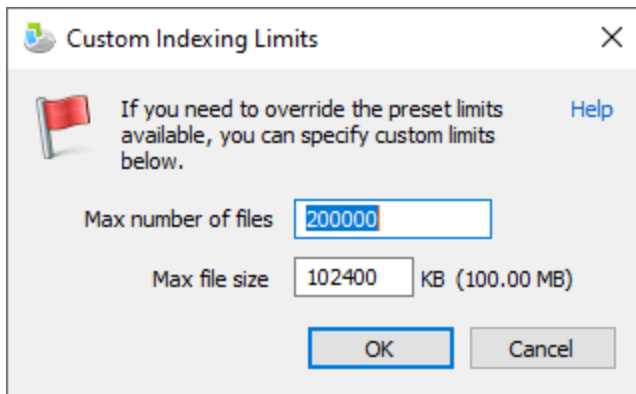
Changing this option will determine how lenient/strict the indexer is when making this decision. Generally leaving this on default, the most strict option, is recommended as this will aggressively remove nonsense data a keep the index to a more manageable size. The Code Words setting is useful if you 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.

Email Attachments



Changing the option determines if/all/some emails attachments are indexed.

Custom Indexing 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 as zip and mail files (but does apply to the files extracted from within them).

5.16.1.4 RAM drive

By selecting the option to "Use a RAM drive" during the "Create Index" process, you allow OSF to create a drive in memory which is faster than any SSD or HDD.

This replaces the typical use of a "swap drive" for temporary files used during the indexing process (for example when a ZIP file is unzipped to access its contents). By writing, reading and deleting files in RAM, we achieve the highest speed and lowest latency possible when indexing certain file types such as ZIP files, and email attachments.

System Requirements

When enabled, depending on the amount of memory available, the indexer will allocate a minimum 1 GB of memory for the RAM drive. If the indexing computer has more than 16 GB of memory available, it will double the size of the RAM drive, incrementing up to a maximum 8 GB RAM drive when a computer has more than 48 GB of memory available.

What to expect

Besides significantly faster indexing for certain file types and higher memory usage, you will notice a new drive letter on your indexing computer under "Windows Explorer" or similar (e.g. "E:") with a volume name of "OSF_TEMP".

When indexing is completed, this drive will be dismantled and removed.

If you are indexing from multiple instances of OSForensics at the same time, then each will get its own RAM drive (with a different drive letter).

Troubleshooting

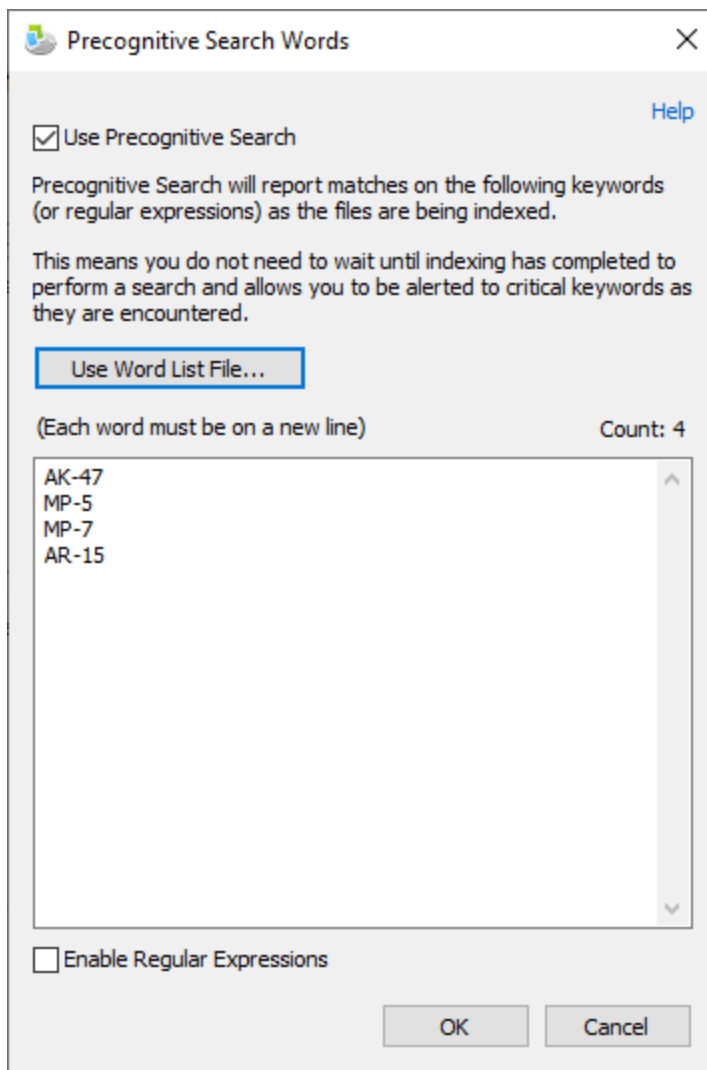
While we have done our utmost to ensure the indexing happens seamlessly and without problems, indexing can be a long and complicated process involving massive amounts of data, so there is the

possibility that something can go wrong. If the indexer crashes or does not complete properly, there is a chance the RAM drive will remain after an indexing session and you have already closed OSForensics.

Should this happen, simply restart OSF and it will notice this stray RAM drive and clean up properly. If it still remains, then rest assured that restarting your computer will also remove the RAM drive.

Note that there is no permanent effect from using a RAM drive. By its nature, everything done in RAM is erased when a computer is switched off or restarted.

5.16.1.5 Precognitive Search



Precognitive Search allows you to enter a list of up to 400 keywords (or regular expressions) that will be checked against during the indexing process.

This means that instead of waiting until the index is fully built before you can perform a search, you can now get results hours or even days earlier. This allows you to start your investigation while the indexing process continues in the background.

Click on the "Use Word List File..." button to import a list of words from a text file.

Note that only 400 keywords are supported, as a longer list would slow down indexing to the point where it would be more time effective to complete indexing before performing such an extensive search. The same Word Lists can be used in the "Search Index" module.

Enable Regular Expressions

Check this option to enable the use of Regular Expressions in the word list above. The regular expression syntax supported for this feature is ECMAScript.

Regular Expression can be very powerful but also very complex. There are many comprehensive references and tutorials for ECMA syntax Regular Expressions online which we would advise referencing for a more complete guide. We have included a brief Quick Reference for ECMA Regular Expression [here](#).

Show Precog Results

Once you have specified your Precog keywords, and you have proceeded with indexing, you will notice a "Show Precog Results" button on the Indexing Status window. Click on this button to display the matches being found during indexing. You can double click on any file to open the file in the Internal Viewer.

5.16.1.5.1 ECMA Regular Expressions

This is a quick reference for the Regular Expression syntax used by the Precognitive Search function in the Indexing module.

PLEASE NOTE: The Raw Disk Viewer uses a different (PCRE) regular expression syntax. For more information on the syntax used by the Raw Disk Viewer, please [click here](#).

Quick Reference for ECMAScript Regular Expression

SPECIAL PATTERN CHARACTERS

Special pattern characters are characters (or sequences of characters) that have a special meaning when they appear in a regular expression pattern, either to represent a character that is difficult to express in a string, or to represent a category of characters. Each of these *special pattern characters* is matched in the target sequence against a single character (unless a quantifier specifies otherwise).

character	description	matches
.	not newline	any character except <i>line terminators</i> (LF, CR, LS, PS).
\t	tab (HT)	a horizontal tab character (same as \u0009).
\n	newline (LF)	a newline (line feed) character (same as \u000A).
\v	vertical tab (VT)	a vertical tab character (same as \u000B).
\f	form feed (FF)	a form feed character (same as \u000C).

character s	description	matches
<code>\r</code>	carriage return (CR)	a carriage return character (same as <code>\u000D</code>).
<code>\cletter</code>	control code	a control code character whose <i>code unit value</i> is the same as the remainder of dividing the <i>code unit value</i> of <i>letter</i> by 32. For example: <code>\ca</code> is the same as <code>\u0001</code> , <code>\cb</code> the same as <code>\u0002</code> , and so on...
<code>\xhh</code>	ASCII character	a character whose <i>code unit value</i> has an hex value equivalent to the two hex digits <i>hh</i> . For example: <code>\x4c</code> is the same as <code>L</code> , or <code>\x23</code> the same as <code>#</code> .
<code>\uhhhh</code>	unicode character	a character whose <i>code unit value</i> has an hex value equivalent to the four hex digits <i>hhhh</i> .
<code>\0</code>	null	a null character (same as <code>\u0000</code>).
<code>\int</code>	backreference	the result of the submatch whose opening parenthesis is the <i>int</i> -th (<i>int</i> shall begin by a digit other than 0). See groups below for more info.
<code>\d</code>	digit	a decimal digit character (same as <code>[[:digit:]]</code>).
<code>\D</code>	not digit	any character that is not a decimal digit character (same as <code>[^[:digit:]]</code>).
<code>\s</code>	whitespace	a whitespace character (same as <code>[[:space:]]</code>).
<code>\S</code>	not whitespace	any character that is not a whitespace character (same as <code>[^[:space:]]</code>).
<code>\w</code>	word	an alphanumeric or underscore character (same as <code>[[:alnum:]]</code>).
<code>\W</code>	not word	any character that is not an alphanumeric or underscore character (same as <code>[^[:alnum:]]</code>).
<code>\character</code>	character	the character <i>character</i> as it is, without interpreting its special meaning within a regex expression. Any <i>character</i> can be escaped except those which form any of the special character sequences above. Needed for: <code>^ \$ \ . * + ? () [] { } </code>
<code>[class]</code>	character class	the target character is part of the class (see character classes below)
<code>[^class]</code>	negated character class	the target character is not part of the class (see character classes below)

QUANTIFIERS

Quantifiers follow a character or a *special pattern character*. They can modify the amount of times that character is repeated in the match:

character s	times	effects
<code>*</code>	0 or more	The preceding atom is matched 0 or more times.
<code>+</code>	1 or more	The preceding atom is matched 1 or more times.
<code>?</code>	0 or 1	The preceding atom is optional (matched either 0 times or once).
<code>{int}</code>	<i>int</i>	The preceding atom is matched exactly <i>int</i> times.

character s	times	effects
<code>{int,}</code>	<i>int</i> or more	The preceding atom is matched <i>int</i> or more times.
<code>{min,max}</code>	between <i>min</i> and <i>max</i>	The preceding atom is matched at least <i>min</i> times, but not more than <i>max</i> .

By default, all these quantifiers are greedy (i.e., they take as many characters that meet the condition as possible). This behavior can be overridden to *ungreedy* (i.e., take as few characters that meet the condition as possible) by adding a *question mark* (?) after the quantifier.

For example:

Matching "(a+).*" against "aardvark" succeeds and yields aa as the first submatch.

While matching "(a+?).*" against "aardvark" also succeeds, but yields a as the first submatch.

GROUPS

Groups allow to apply quantifiers to a sequence of characters (instead of a single character). There are two kinds of groups:

characters	description	effects
<code>(subpattern)</code>	Group	Creates a backreference.
<code>(?:subpattern)</code>	Passive group	Does not create a backreference.

When a group creates a backreference, the characters that represent the *subpattern* in the target sequence are stored as a *submatch*. Each submatch is numbered after the order of appearance of their opening parenthesis (the first submatch is number 1, the second is number 2, and so on...).

ASSERTIONS

Assertions are conditions that do not consume characters in the target sequence: they do not describe a character, but a condition that must be fulfilled before or after a character.

characters	description	condition for match
<code>^</code>	Beginning of line	Either it is the beginning of the target sequence, or follows a <i>line terminator</i> .
<code>\$</code>	End of line	Either it is the end of the target sequence, or precedes a <i>line terminator</i> .
<code>\b</code>	Word boundary	The previous character is a <i>word character</i> and the next is a <i>non-word character</i> (or vice-versa). Note: The beginning and the end of the target sequence are considered here as <i>non-word characters</i> .
<code>\B</code>	Not a word boundary	The previous and next characters are both <i>word characters</i> or both are <i>non-word characters</i> . Note: The beginning and the end of the target sequence are considered here as <i>non-word characters</i> .
<code>(?=subpattern)</code>	Positive lookahead	The characters following the assertion must match <i>subpattern</i> , but no characters are consumed.
<code>(?!subpattern)</code>	Negative lookahead	The characters following the assertion must not match <i>subpattern</i> , but no characters are consumed.

ALTERNATIVES

A pattern can include different alternatives:

character	description	effects
	Separator	Separates two alternative patterns or subpatterns.

A regular expression can contain multiple alternative patterns simply by separating them with the *separator operator*(|): The regular expression will match if any of the alternatives match, and as soon as one does.

Subpatterns (in groups or assertions) can also use the *separator operator* to separate different alternatives.

CHARACTER CLASSES

A character class defines a category of characters. It is introduced by enclosing its descriptors in square brackets ([and]).

The regex object attempts to match the entire character class against a single character in the target sequence (unless a quantifier specifies otherwise).

The character class can contain any combination of:

- **Individual characters:** Any character specified is considered part of the class (except the characters \, [,] and - when they have a special meaning as described in the following paragraphs).
For example:
[abc] matches a, b or c.
[^xyz] matches any character except x, y and z.
- **Ranges:** They can be specified by using the *hyphen character* (-) between two valid characters.
For example:
[a-z] matches any lowercase letter (a, b, c, ... until z).
[abc1-5] matches either a, b or c, or a digit between 1 and 5.
- **POSIX-like classes:** A whole set of predefined classes can be added to a custom character class. There are three kinds:

class	description
[: <i>classname</i> :]	character class
[. <i>classname</i> .]	collating sequence
[= <i>classname</i> =]	character equivalents

The choice of available classes depend on the regex traits type and on its selected locale. But at least the following character classes shall be recognized by any regex traits type and locale:

class	description
[: <i>alnum</i> :]	alpha-numerical character
[: <i>alpha</i> :]	alphabetic character
[: <i>blank</i> :]	blank character
[: <i>cntrl</i> :]	control character
[: <i>digit</i> :]	decimal digit character

class	description
<code>[[:graph:]]</code>	character with graphical representation
<code>[[:lower:]]</code>	lowercase letter
<code>[[:print:]]</code>	printable character
<code>[[:punct:]]</code>	punctuation mark character
<code>[[:space:]]</code>	whitespace character
<code>[[:upper:]]</code>	uppercase letter
<code>[[:xdigit:]]</code>	hexadecimal digit character
<code>[[:d:]]</code>	decimal digit character
<code>[[:w:]]</code>	word character
<code>[[:s:]]</code>	whitespace character

Please note that the brackets in the class names are additional to those opening and closing the class definition.

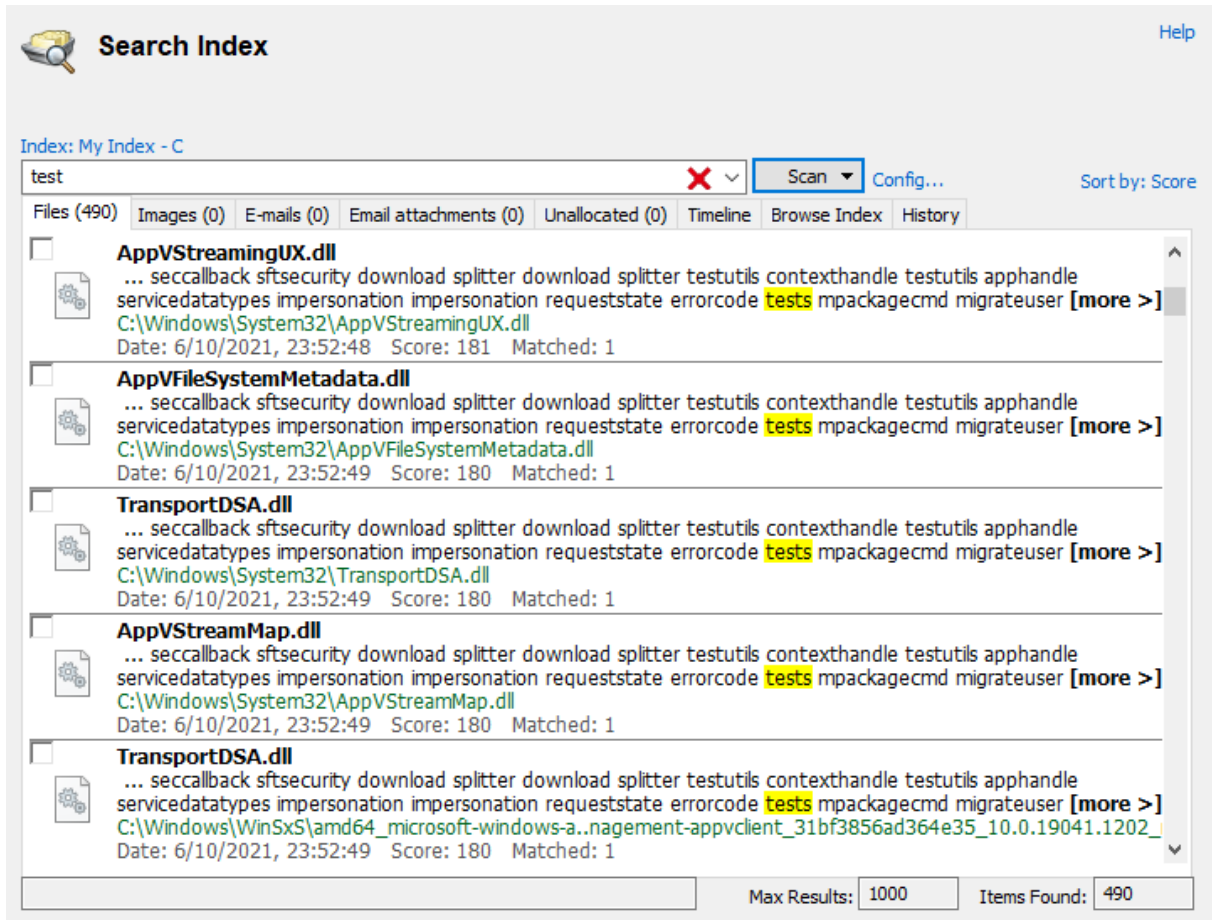
For example:

`[[:alpha:]]` is a character class that matches any alphabetic character.
`[abc[:digit:]]` is a character class that matches a, b, c, or a digit.
`[^[:space:]]` is a character class that matches any character except a whitespace.

- **Escape characters:** All escape characters described above can also be used within a character class specification. The only change is with `\b`, that here is interpreted as a backspace character (`\u0008`) instead of a word boundary. Notice that within a class definition, those characters that have a special meaning in the regular expression (such as `*`, `.`, `$`) don't have such a meaning and are interpreted as normal characters (so they do not need to be escaped). Instead, within a class definition, the hyphen (`-`) and the brackets (`[` and `]`) do have special meanings under some circumstances, in which case they should be placed within the class in other locations where they do not have such special meaning, or be escaped with a backslash (`\`).

5.16.2 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 or other file attributes) for the user-specified search words.



The screenshot displays the 'Search Index' window. At the top, there is a search bar containing the text 'test'. Below the search bar, there are several tabs: 'Files (490)', 'Images (0)', 'E-mails (0)', 'Email attachments (0)', 'Unallocated (0)', 'Timeline', 'Browse Index', and 'History'. The 'Files (490)' tab is selected. The search results are sorted by 'Score' and show five entries, each with a checkbox, a gear icon, and a list of associated keywords. The keywords for each entry include 'seccallback', 'sftsecurity', 'download', 'splitter', 'testutils', 'contexthandle', 'testutils', 'apphandle', 'servicedatatypes', 'impersonation', 'impersonation', 'requeststate', 'errorcode', 'tests', 'mpackagecmd', and 'migrateuser'. The file paths and dates are also visible for each entry. At the bottom of the window, there are fields for 'Max Results: 1000' and 'Items Found: 490'.

Usage

To perform a search, first select an index or multiple indices to search. Multiple indices can be specified by selecting *Multiple Index Search Options* link in the *Index* link drop-down menu. 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 *Config...* link).

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.

5.16.2.1 Search Index Configuration

The Search Index Configuration 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.

Search Index Configuration

Match Any search words
 All search words

Maximum Results

Date Range
 Use Date Range
From: To:

Email Search Options
From
To
CC
BCC

OK

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.

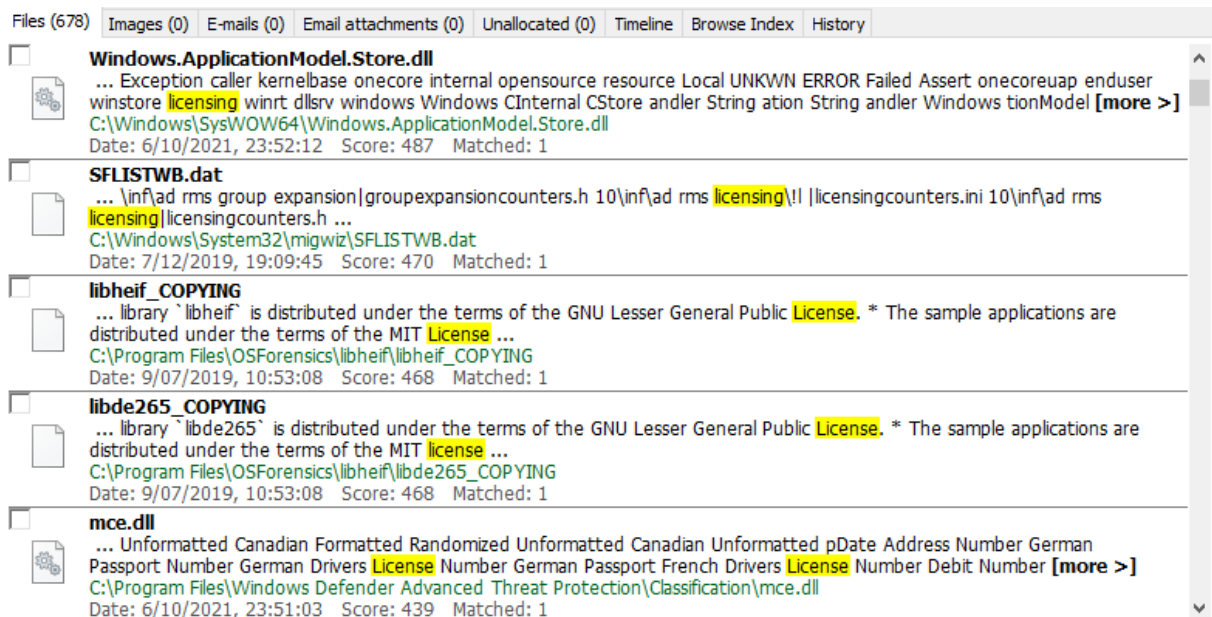
Email Search Options

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

5.16.2.2 Index Search Results View

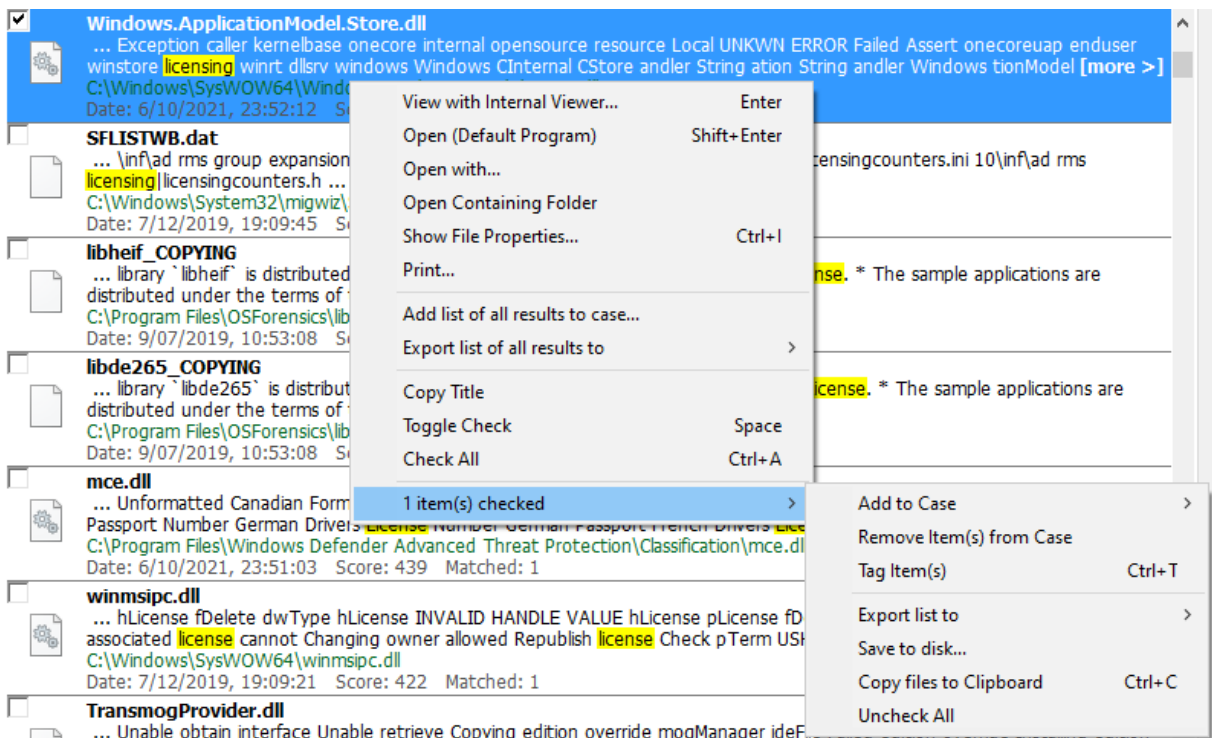
After an index search is performed, the results are displayed in the Results View. The results are organized into several views, depending on the file type.

Types of Views**Files View**



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, see Adding items to a case.

Remove Item(s) from Case

Remove the checked file(s) from the case

Tag Item(s)

Tag file(s) for future reference. *Keyboard shortcut: Ctrl+T*

Export list to

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

Save to disk...

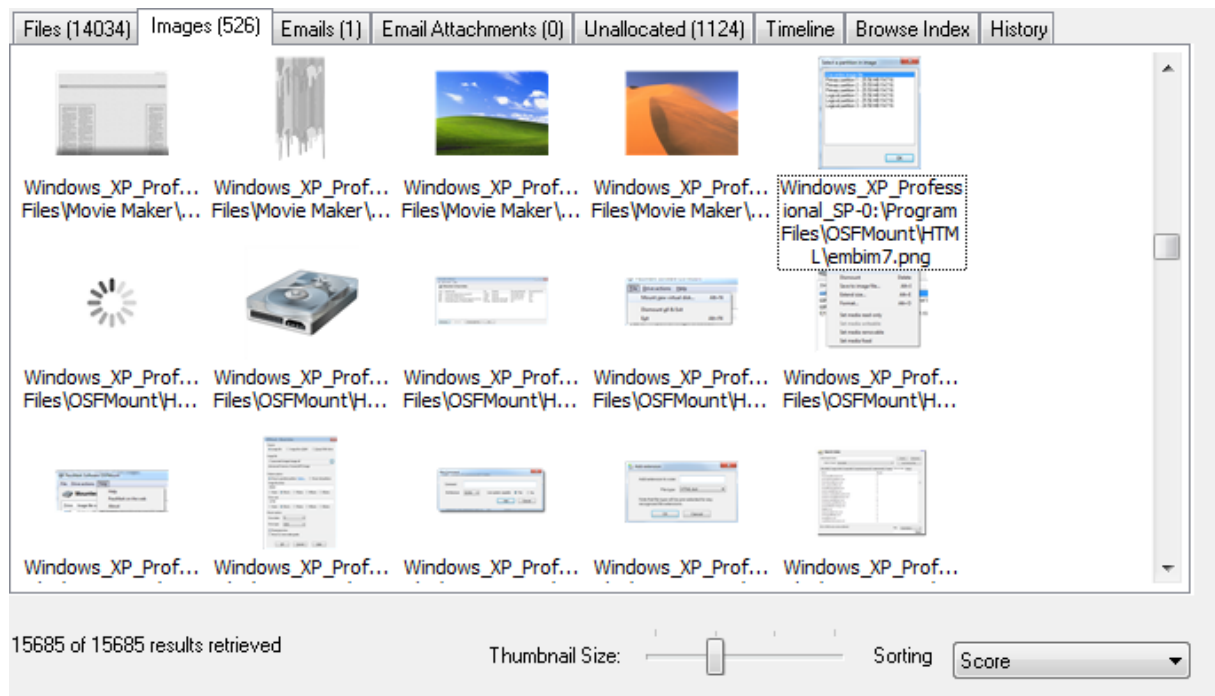
Save the checked file(s) to disk. Note that files within another file (such as files within ZIP files or emails and attachments within PST files) will save the container file to disk.

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.

Images View

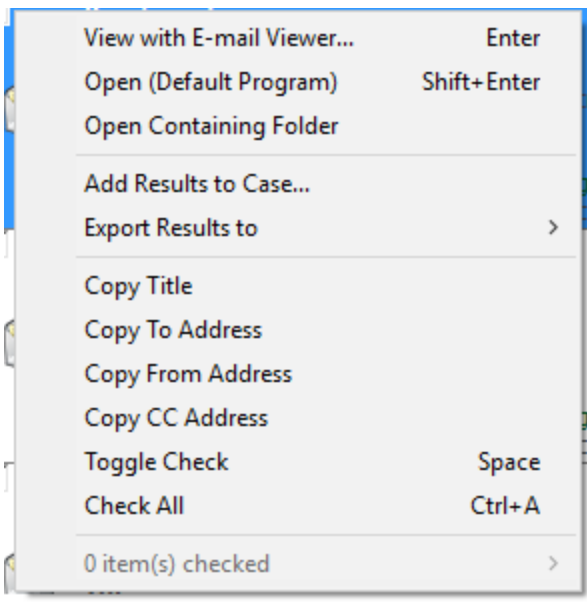


The Images View displays only the search results that contain images as a list of thumbnails. This view is useful when the search results contain media files, allowing the user to quickly browse through the thumbnail images. Similar to the File View, the results can be sorted via the Sorting combo box.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

Email View



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

Files (2859) | Images (136) | Emails (1289) | Email Attachments (619) | Unallocated (0) | Timeline | Browse Index | History

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*000000002981706B94693848AA8543E2DAB32AA464C82C
 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*000000002981706B94693848AA8543E2DAB32AA404672C
 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*000000002981706B94693848AA8543E2DAB32AA424672C
 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*000000002981706B94693848AA8543E2DAB32AA4A4FF2C
 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

Files (0) | Images (0) | Emails (0) | Email Attachments (0) | Unallocated (5) | Timeline | Browse Index | History

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

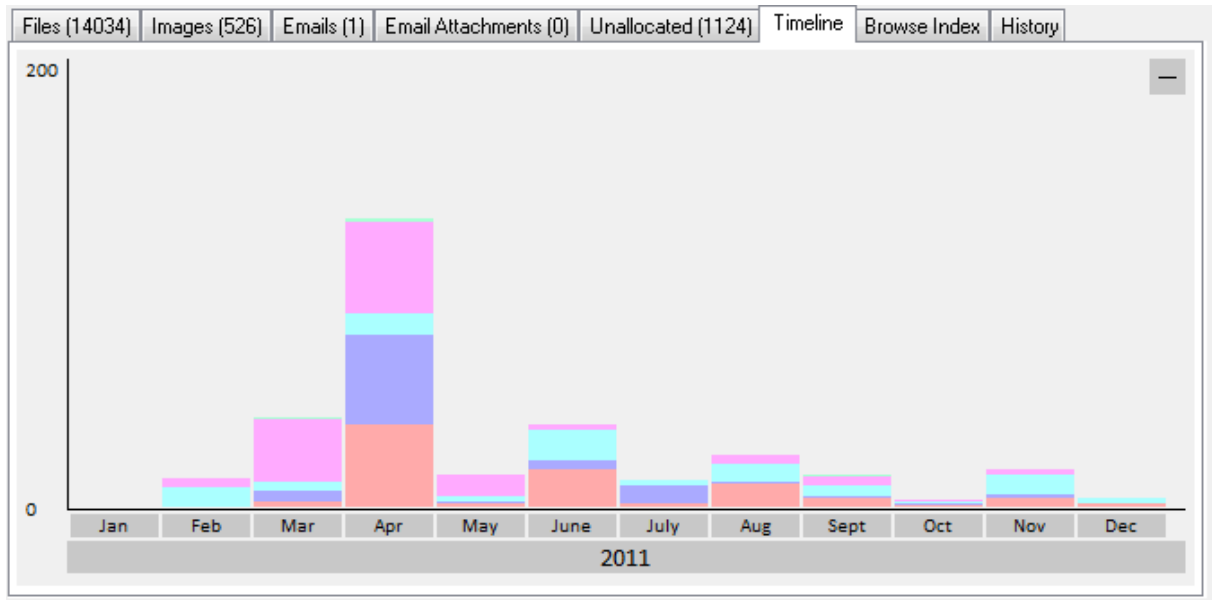
Unallocated cluster (disk macos-0:) LCN Range: 26353 - 26354
 ... version encoding DOCTYPE plist Apple PLIST apple plist version resource array Attributes string string CFName string Protective Master string string string string Protective Master string Attributes [more >]
 Date: N/A Score: 51 Matched: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

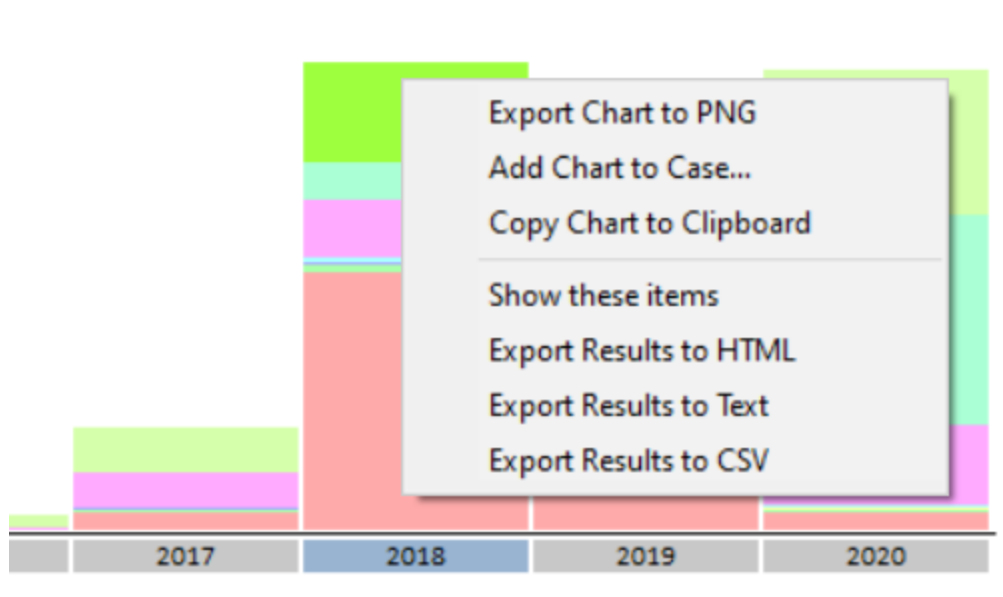
Unallocated cluster (disk macos-0:) LCN Range: 26121 - 26127
 ... version encoding DOCTYPE plist Apple PLIST apple plist version string string policySearch integer integer plist ...
 Date: N/A Score: 18 Matched: 1

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

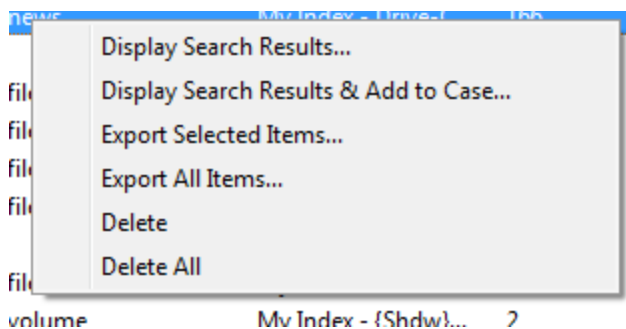
Browse Index View

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 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

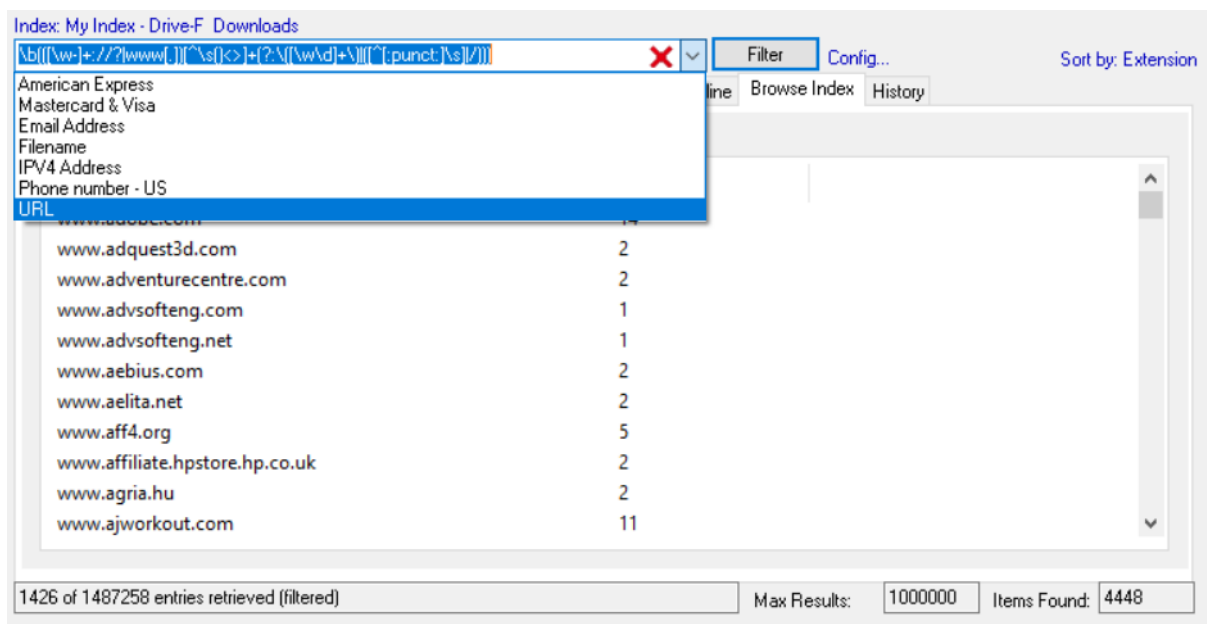
Delete the selected history item(s)

Delete All

Delete all history items in the list

5.16.2.3 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.

**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.

deper	Search For Selected Items	274
deplet	Search For Selected Items & Add To Case	8
deplot	Export Selected Items...	46
Depos	Export All Items...	115
Dept	Index properties...	50
depth		16

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.

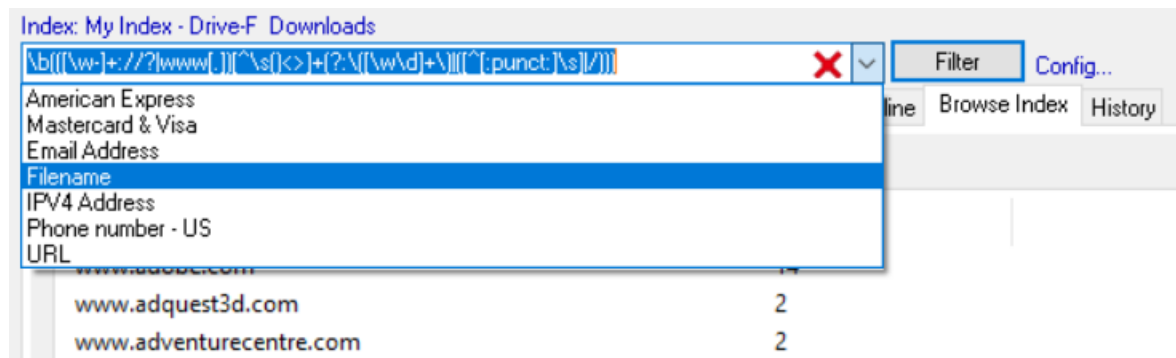
Export All Items...

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 predefined regular expressions that can be selected in the search bar 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 in the search bar 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", type "test" in the search box and then click the *Filter* 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.

5.17 Installing to a USB Drive or an Optical Disk

It is possible to install OSForensics portably onto a USB or network drive 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 running OSForensics Portable, 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 or Network drive

This installation process can be performed for a USB drive or network share using the menu option "Install to USB or Network".

From the 'Install OSForensics Portable' window, you need to specify:

1. The USB drive or network path you want to install OSForensics Portable. For example, "F:\OSForensics". OSForensics will create the directory if it does not exist.
2. If you have large password recovery dictionaries or large rainbow tables you can choose to exclude them from the USB copy process by unchecking the options.
3. Enter the Username/Key;
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 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 destination folder (e.g. F:\OSForensics) and install the license information.

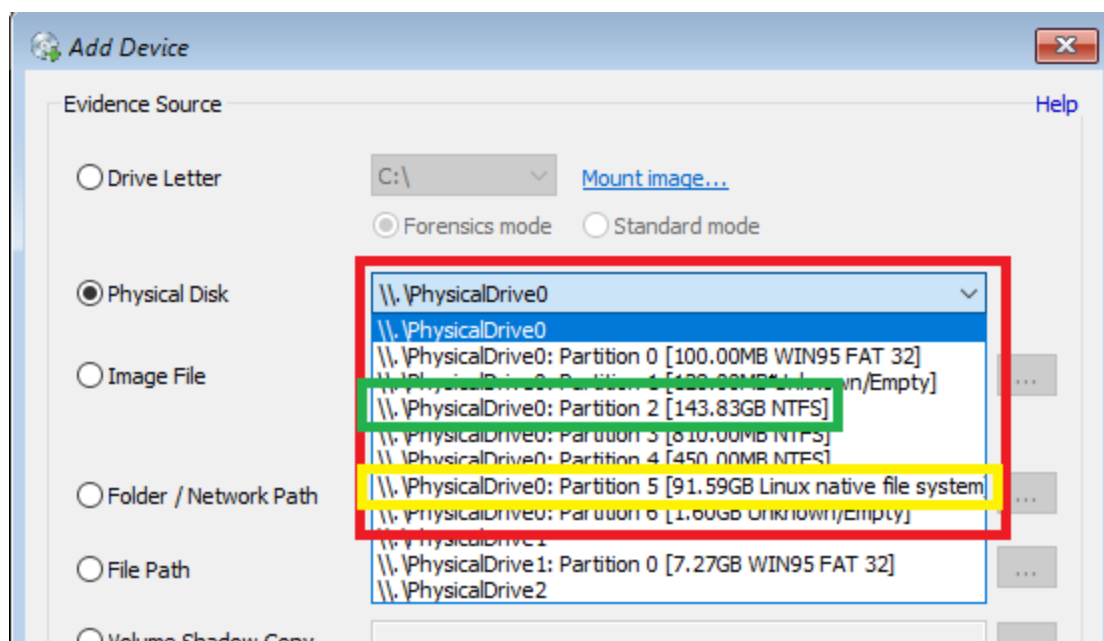
Creating a bootable copy of OSForensics

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 Windows Pre-install 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*.

Limitations

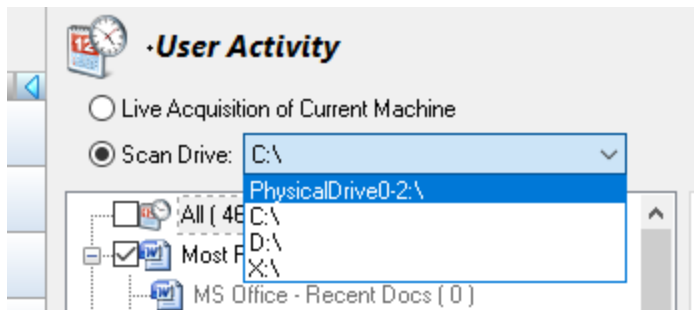
- **Create Index:** You will not be able to index some file formats from 64-bit WinPE. This is due to the fact that 64-bit WinPE does not support 32-bit executables, and indexing some file formats require the use of 32-bit components. Instead, we recommend imaging the disk, and performing the indexing from an investigation machine (which should be faster and have more resources than the machine being investigated). This is generally the most practical approach given that indexing is very resource intensive.
- **Disk/Volume Access:** Storage Area Network (SAN) Policy can control whether or not disks are mounted when WinPE is started. When using SAN Policy **3 (Doesn't mount storage devices)** or **4 (Makes internal disks offline, but all external disks and the boot disk are online)**, the internal storage locations are not mounted when booting. To process the drives on the system, first add them to the case using "Add Device". The volumes can be added by using the Physical Disk option in Add Devices.



Note: The Physical Drive listing/order may vary on different systems. Example is shown with different partitions highlighted, does not represent view in OSForensics.

The **Red Box** shows the system's main storage, PhysicalDrive0 with various partitions on the disk. The **Green Box** shows the user's installed Windows OS partition, PhysicalDrive0: Partition 2. The **Yellow Box** shows the user's installed Linux OS partition, PhysicalDrive0: Partition 5. The WinPE boot USB Flash Drive (UFD) is PhysicalDrive1. When booting from a WinPE disk, the WinPE image is loaded into RAM Disk and the volume letter assigned to RAM Disk is X:\. When using option (4), the RAM Disk is still X:\, but the physical UFD and other external storage devices will be assigned drive letters as well, e.g. C:\, D:\, etc.

Internal storage devices added to OSForensic using PhysicalDrive access method can be used within the different modules and will be listed in the dropdowns as selectable devices. e.g. User Activity



C:\ is the UFD, D:\ is SD Card Reader, X:\ is the WinPE RAM Disk and PhysicalDrive0-2:\ is the user/system's Windows OS partition added with "Add Device".

5.18 Internal Viewer

OSForensics includes a built-in viewer for previewing the contents of files, deleted files, memory sections and raw sectors. The internal viewer consists of several viewing modes that aid specifically in forensic data analysis



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

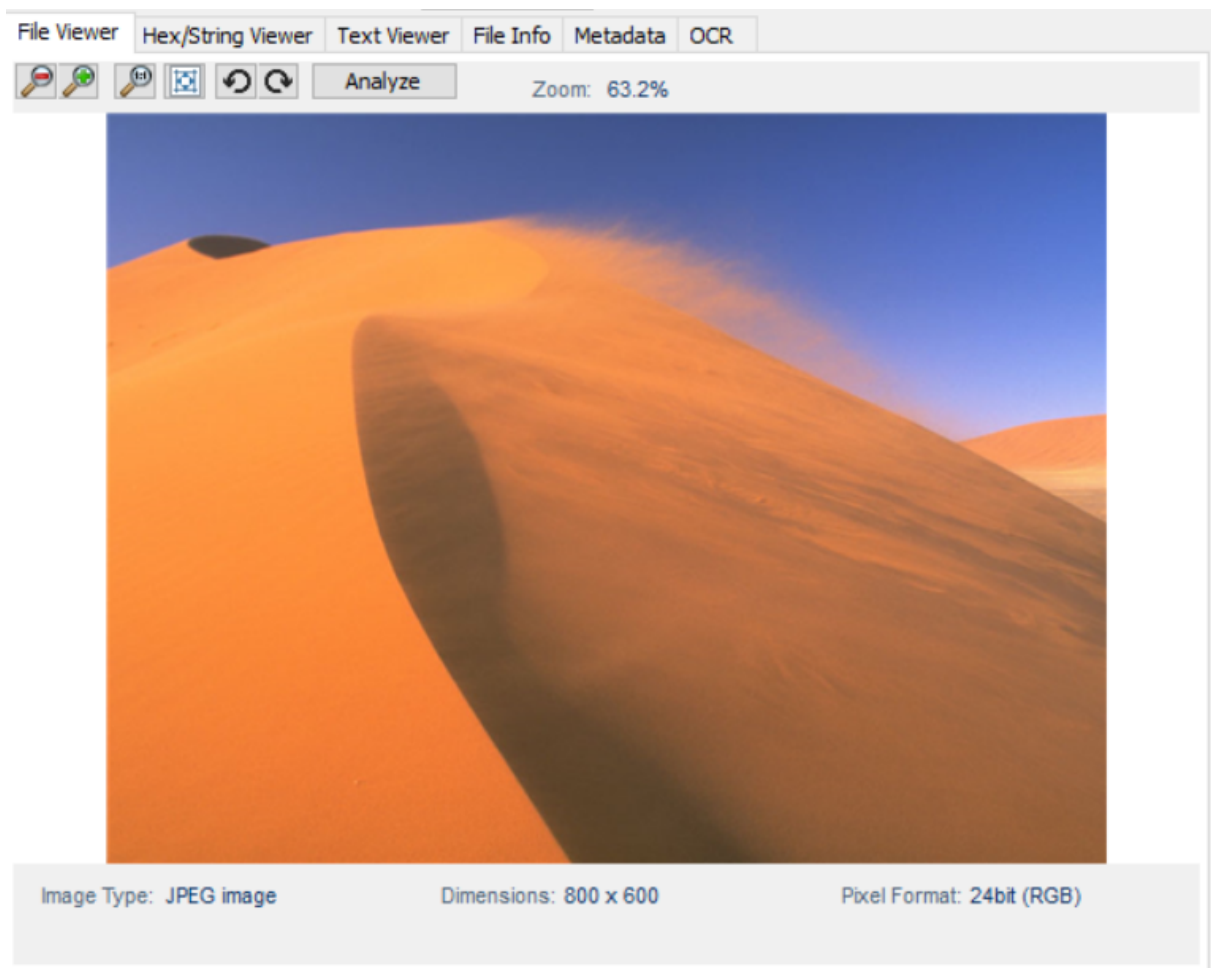
Backslash/Numpad 5 key - Fit image to screen

5.18.1 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

To zoom on the image, use the buttons on the top left  or alternatively, the scroll wheel on the mouse or +/- keys.

Rotate

To rotate image, use the rotate buttons on the top left.

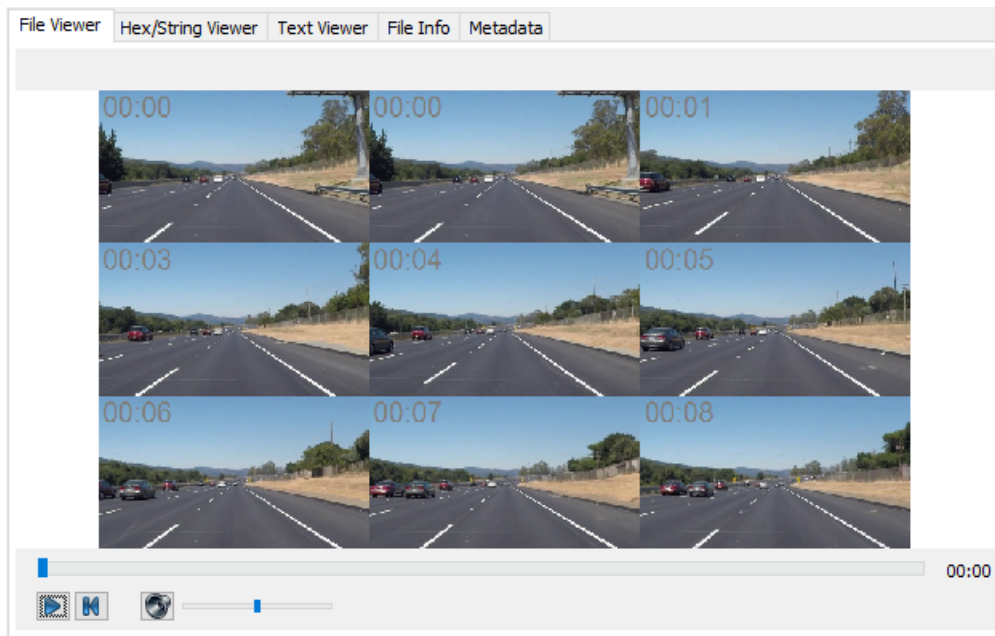
Pan

To pan the image, use the mouse to drag the image in any direction.

Analyze

For more information, see the Image Analysis module.

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.

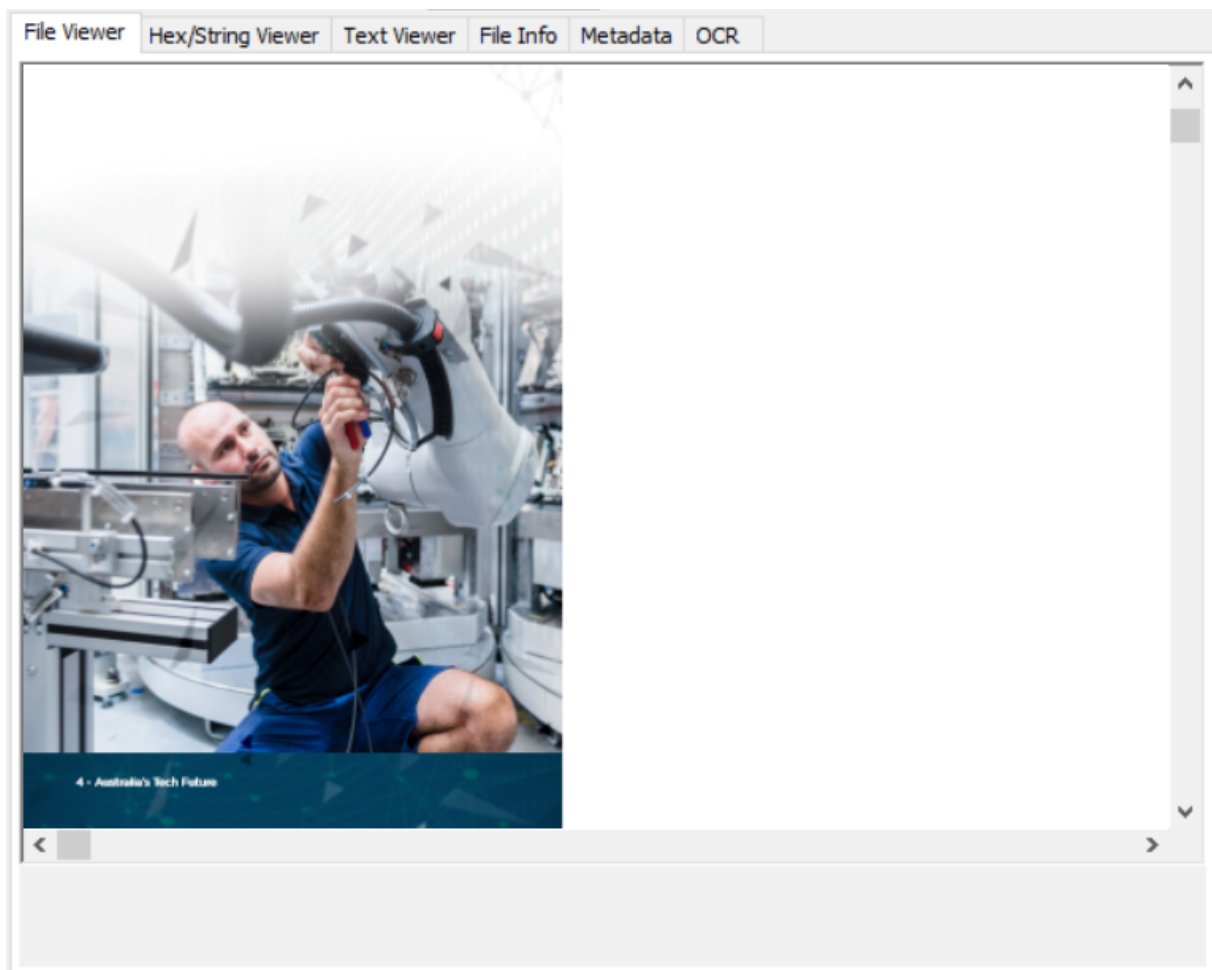
Rewind

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.

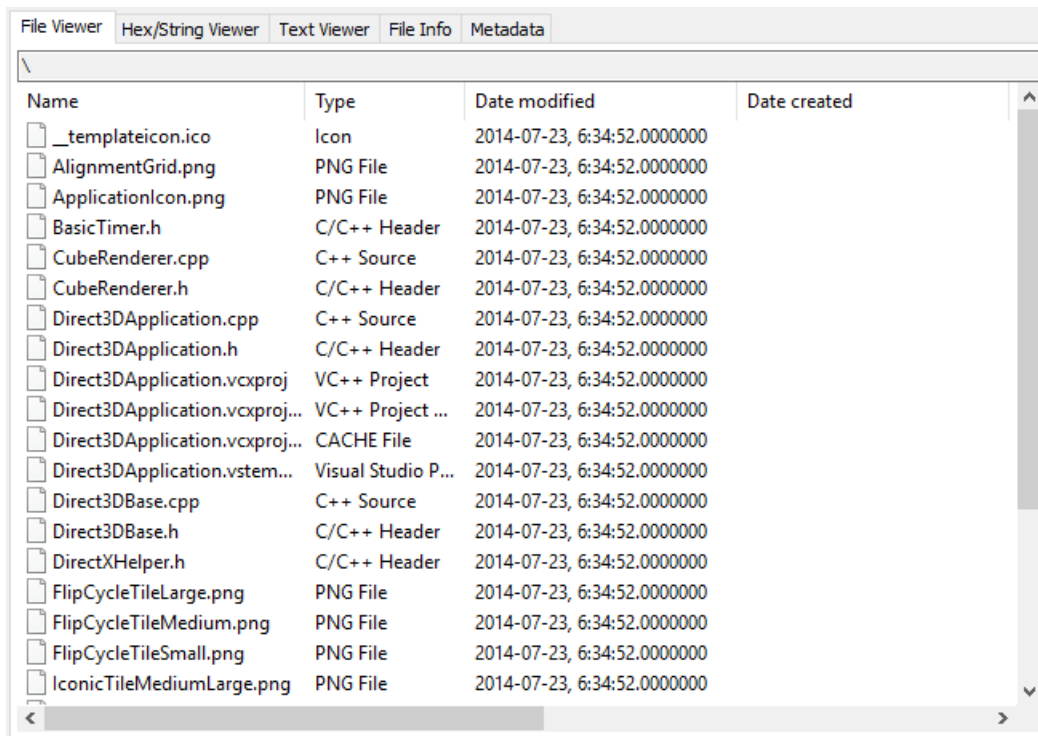
Document Formats



For PDF files, the full document including images and text is rendered. (Windows 8 and later).

For other documents, only the text component of the document file is displayed. Formatting is not preserved.

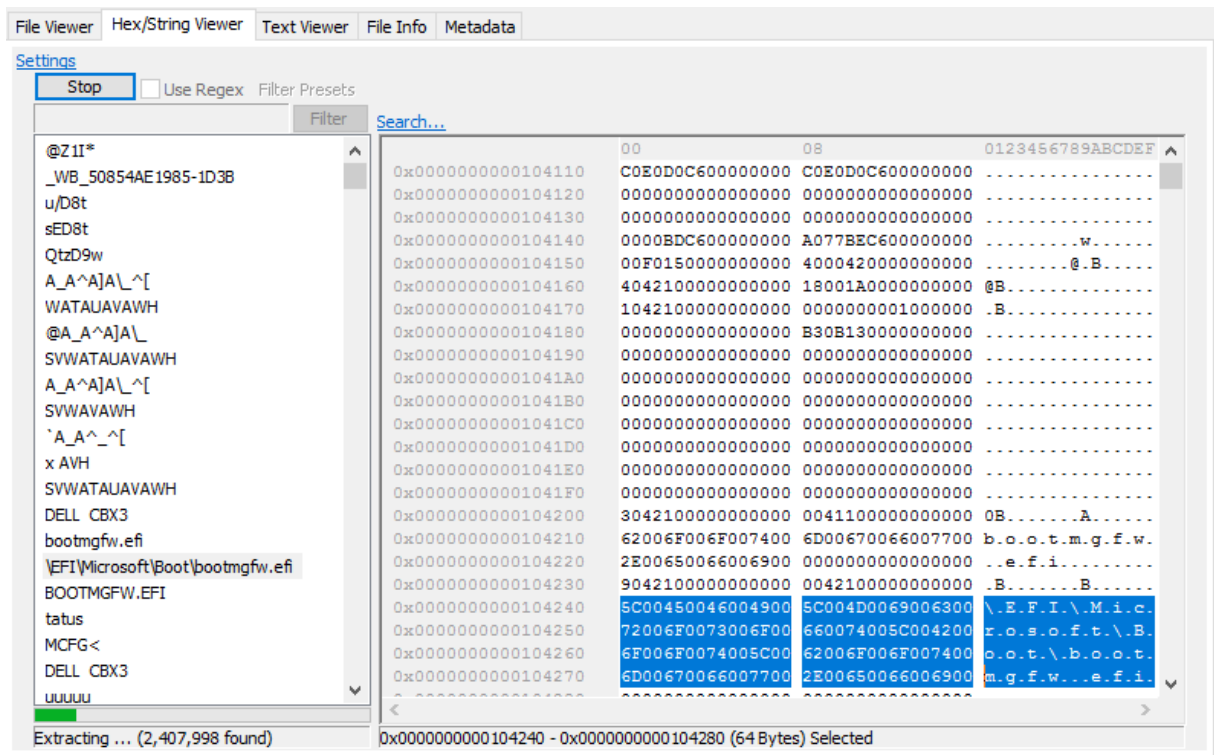
Compressed Formats



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.

5.18.2 Hex/String Viewer

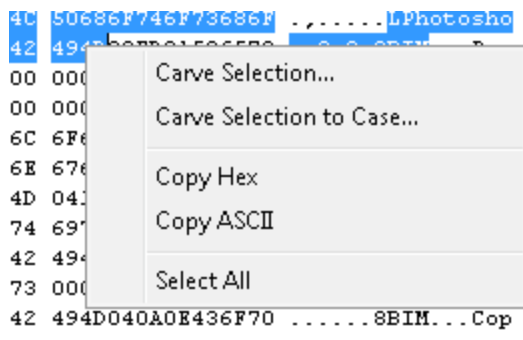
The hex/string viewer displays the data stream as raw data bytes in hex. This mode also allows the user to extract ASCII/Unicode strings from the raw data bytes.



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:



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 - filters all strings that appear to be in a valid filename format

E-mail - filters all strings that appear to be in a valid e-mail address format

URL - filters all strings that appear to be in a valid URL address format

GUID - filters all strings that appear to be in a valid GUID identifier format

IPv4 Address - filters all strings that appear to be a valid IPv4 address format

IPv6 Address (Standard Notation) - filters all strings that appear to be a valid IPv6 address in standard notation (ie. full 8-word in hexadecimal)

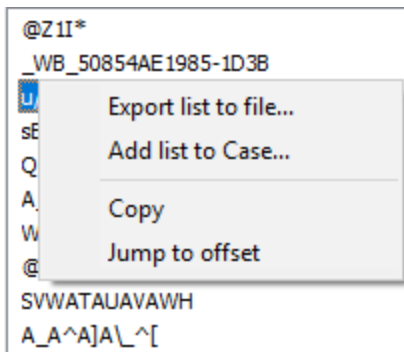
IPv4 Address (Standard or Compressed Notation) - filters all strings that appear to be a valid IPv6 address in either standard or compressed notation. Due to the validity of double colons (::) in compressed notation, this regular expression may capture strings that are not IPv6 addresses.

Date - filters all strings that appear to be a valid Gregorian date format

Phone Number (North American) - filters all strings that appear to be a valid North American phone number

Use Word List... - filters all strings that contain any of the words included in the user-specified word list file

Right-clicking opens a context menu as shown below:



Export List to file...

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

Copy

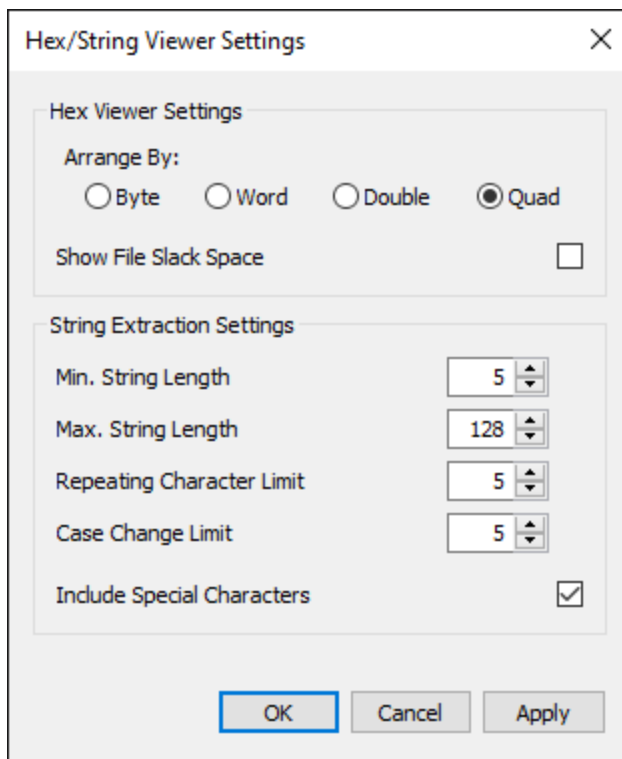
Copy the string into the clipboard

Jump to Offset

Jump to the location of the string in the hex view

5.18.2.1 Hex/String Viewer Settings

The Hex/String Viewer Settings window contains configuration options for the Hex/String Viewer.



Hex Viewer Settings

Arrange By

Change the hex groupings in the hex view

Show File Slack Space

If checked, the end of file slack space (up to the end of cluster) will be shown in the hex view.

```

0x016F9FC0 1E7B1A0135E9E119 34B5DD163FC9DBD1 .{...5...4...?...
0x016F9FD0 D9DD74555233488B 015F9B645372BB3D ..tUR3H..._dSr.=
0x016F9FE0 A142C1B1EE88FA4D 789E9AC0A496EC61 .B.....Mx.....a
0x016F9FF0 7A7A25D82255DE45 C39EAB2437097C76 zz%. "U.E...$7. |v
0x016FA000 5557F2C21C4BFC64 575EF0DB74664A52 UW...K.dW^...tfJR
0x016FA010 EFF283682F0CB71A 36888CA7CAD4B767 ...h/...6.....g
0x016FA020 1C069418E4AF0000 0000000000000000 .....
0x016FA030 0000000000000000 0000000000000000 .....
0x016FA040 0000000000000000 0000000000000000 .....
0x016FA050 0000000000000000 0000000000000000 .....
0x016FA060 0000000000000000 0000000000000000 .....
0x016FA070 0000000000000000 0000000000000000 .....
0x016FA080 0000000000000000 0000000000000000 .....
0x016FA090 0000000000000000 0000000000000000 .....
0x016FA0A0 0000000000000000 0000000000000000 .....

```

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

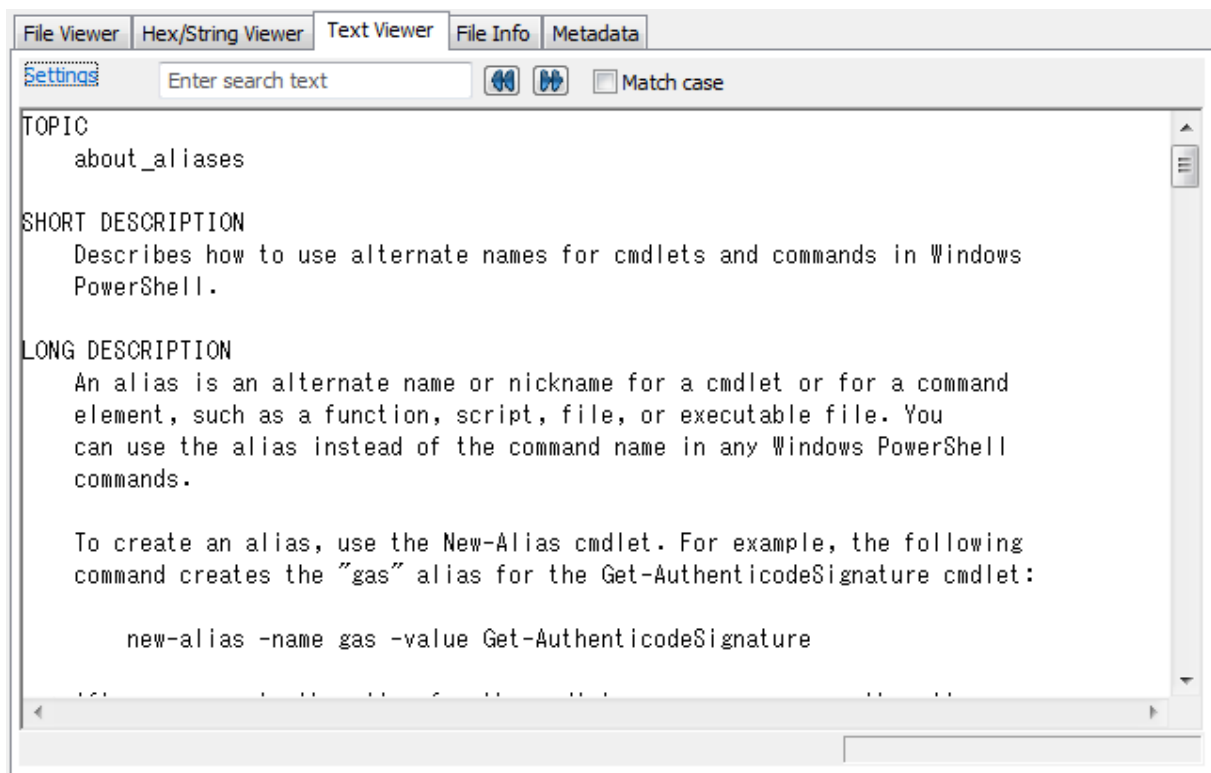
Include Special Characters

If checked, strings containing the following special characters are included in the extracted string list:

```
~!@#$%^&* () -_ =+ [ { ] \ | ; : , ' . > / ?
```

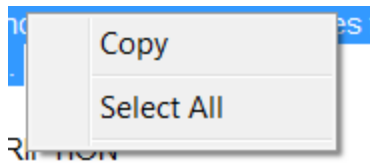
5.18.3 Text Viewer

The text viewer displays the data stream as text.



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.



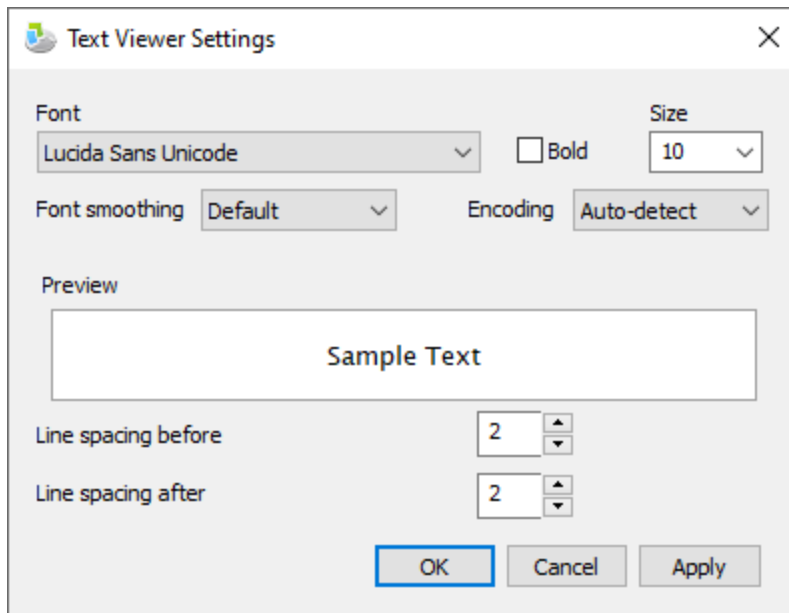
The font settings can be configured via the Settings window.

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.

5.18.3.1 Text Viewer Settings

The Text Viewer Settings window contains configuration options for the Text Viewer.

**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

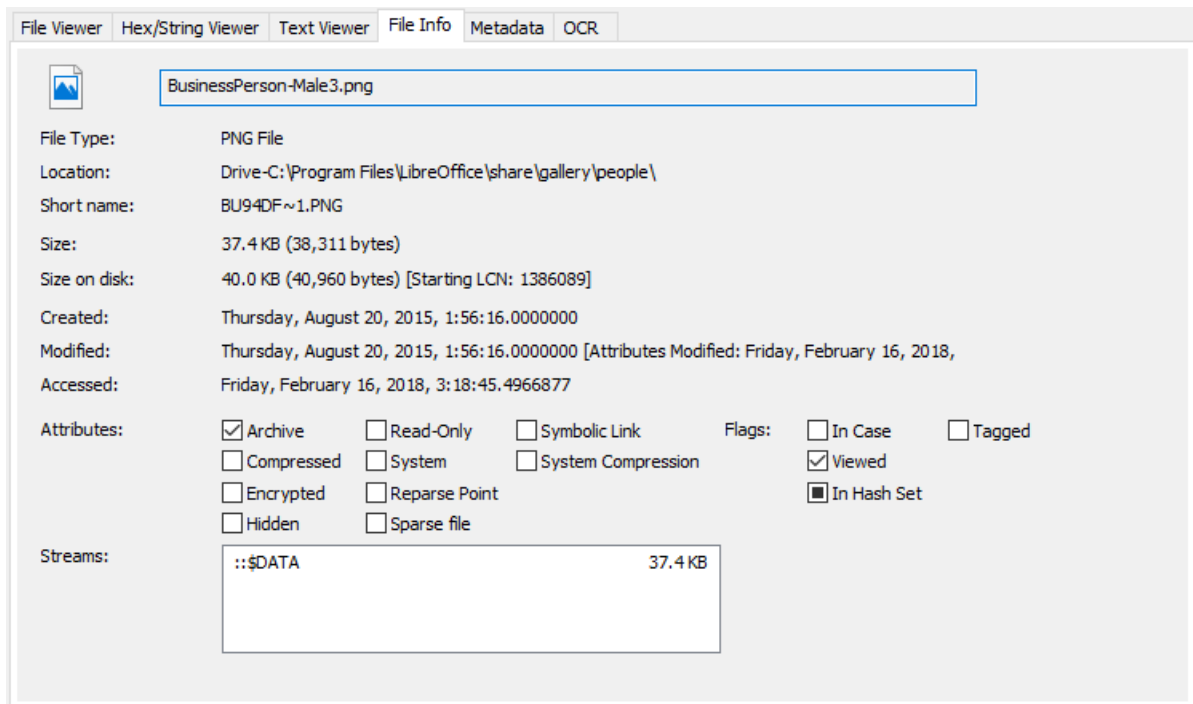
The spacing before each line

Line spacing after

The spacing after each line

5.18.4 File Info

The file info view displays attributes of the data stream.



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.

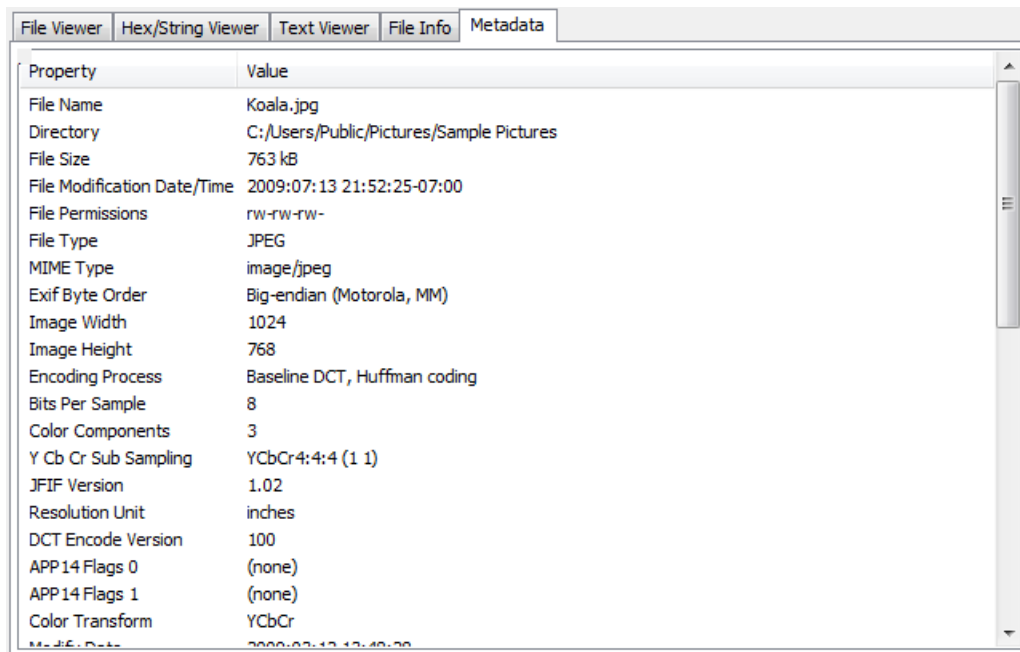
Note: When opening files that belong to a case, the location and file times of the original file shall be displayed.

5.18.5 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
Modif Date	2009:07:13 21:52:25

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.

LNK Files

The metadata view displays the embedded information that can be found within a shortcut (.lnk) file. Which includes information when the shortcut was created and current and birth MAC address of the machine the shortcut resides on.

Property	Value
Target Path	C:\Program Files\OSFMount\OSFMount.exe
Volume Label	
Serial Number	3397129908
Drive Type	Fixed
Attributes	Archive
File Size	2093592
Create Time	3/29/2018, 15:33:27
Access Time	9/17/2018, 13:24:26
Modified Time	3/22/2018, 10:27:08
RELATIVE_PATH	..\..\..\Program Files\OSFMount\OSFMount.exe
WORKING_DIR	C:\Program Files\OSFMount
Machine ID	passmarkus-w8p
Volume ID	{428F79D0-981B-485D-82F9-20D3B4893F8E}
Object ID	{CB3FC110-32E0-11E8-8449-10C37B69C100}
Object Timestamp	3/28/2018, 16:36:09
Object MAC Address	10:C3:7B:69:C1:00
Birth Volume ID	{428F79D0-981B-485D-82F9-20D3B4893F8E}
Birth Object ID	{CB3FC110-32E0-11E8-8449-10C37B69C100}
Birth Object Timestamp	3/28/2018, 16:36:09
Birth Object MAC Address	10:C3:7B:69:C1:00

The entries can be copied to clipboard, or exported to a text file from the right-click menu.

5.19 JSON Viewer

The JSON Viewer parses and displays JSON file contents.

JSON Viewer basic features:

- Syntax highlighting for JSON documents
- Treeview shows the hierarchical dependencies between JSON nodes
- JSON formatting and indenting
- Compressing (minifying) JSON documents
- Supported encoding: UTF8, ASCII, UTF16 BE/LE

The font settings can be configured via the Settings window.

JSON Parser

Google Hangouts

A parser for Google Hangouts conversation history.

Download Hangouts chat history from Google Takeout and load the "Hangouts.json" file for decoding.

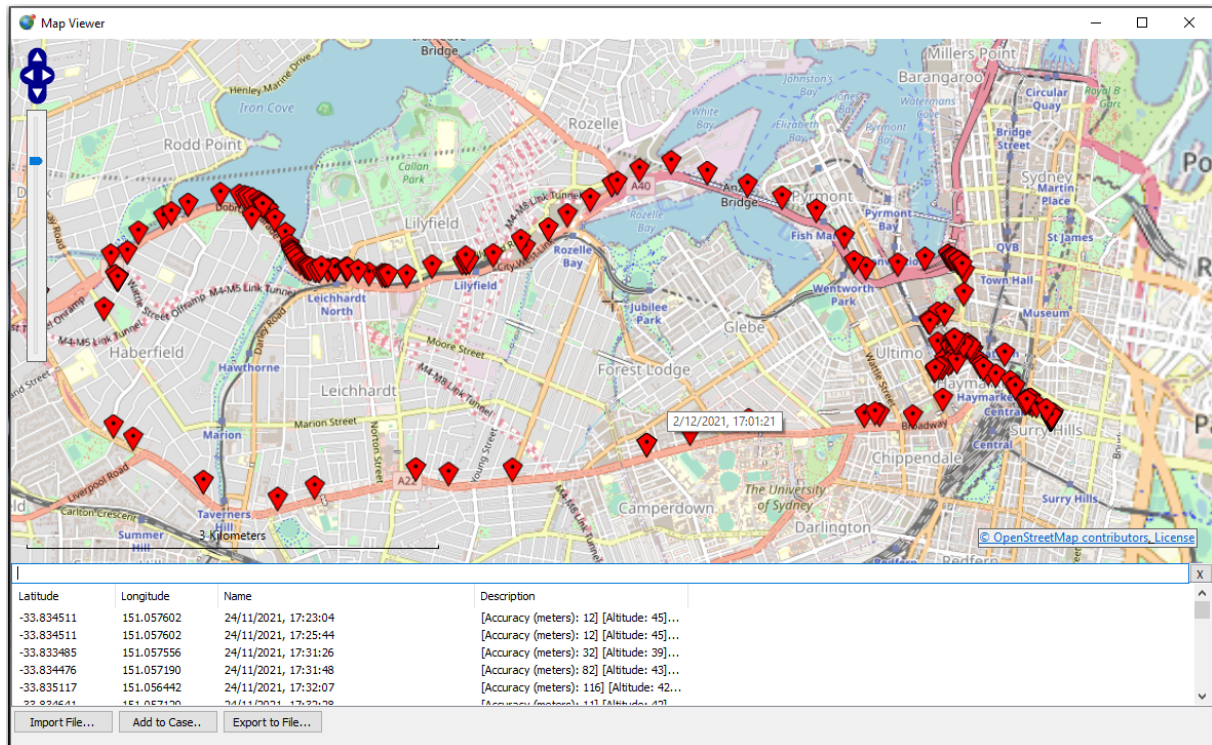
- View conversations in HTML with nicely formatted chatting app style
- Export to HTML/CSV/TXT file formats

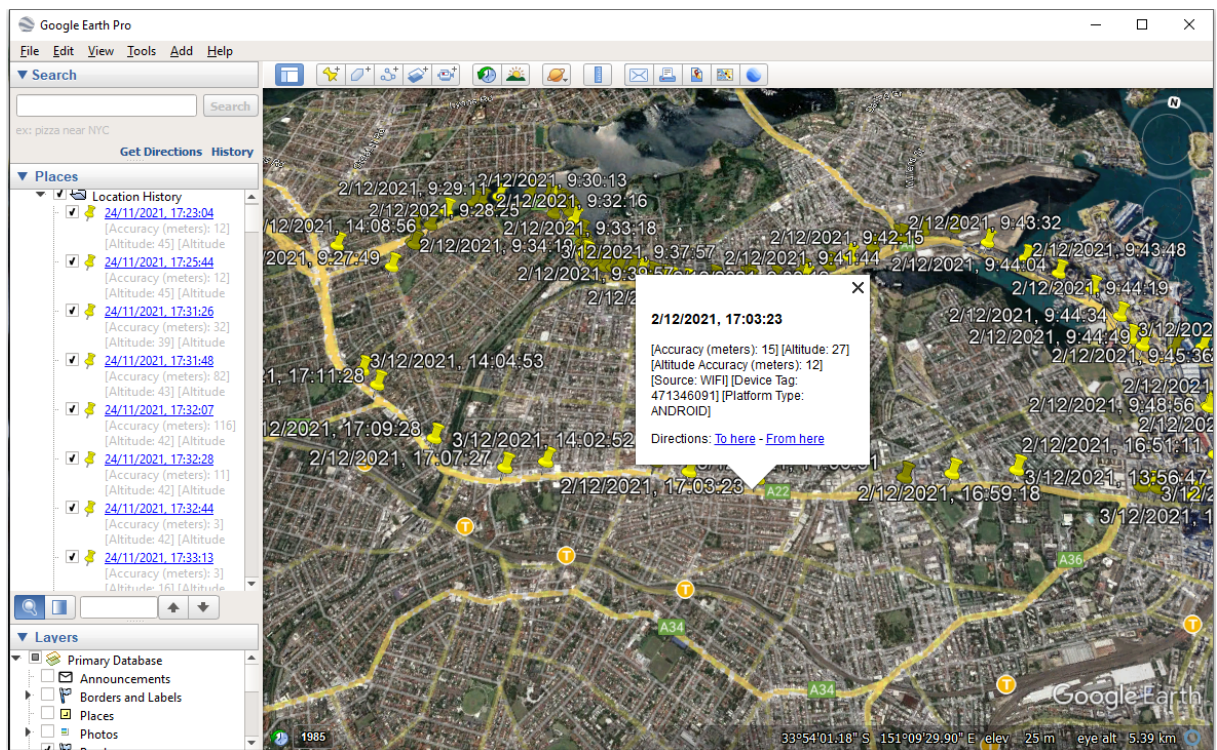
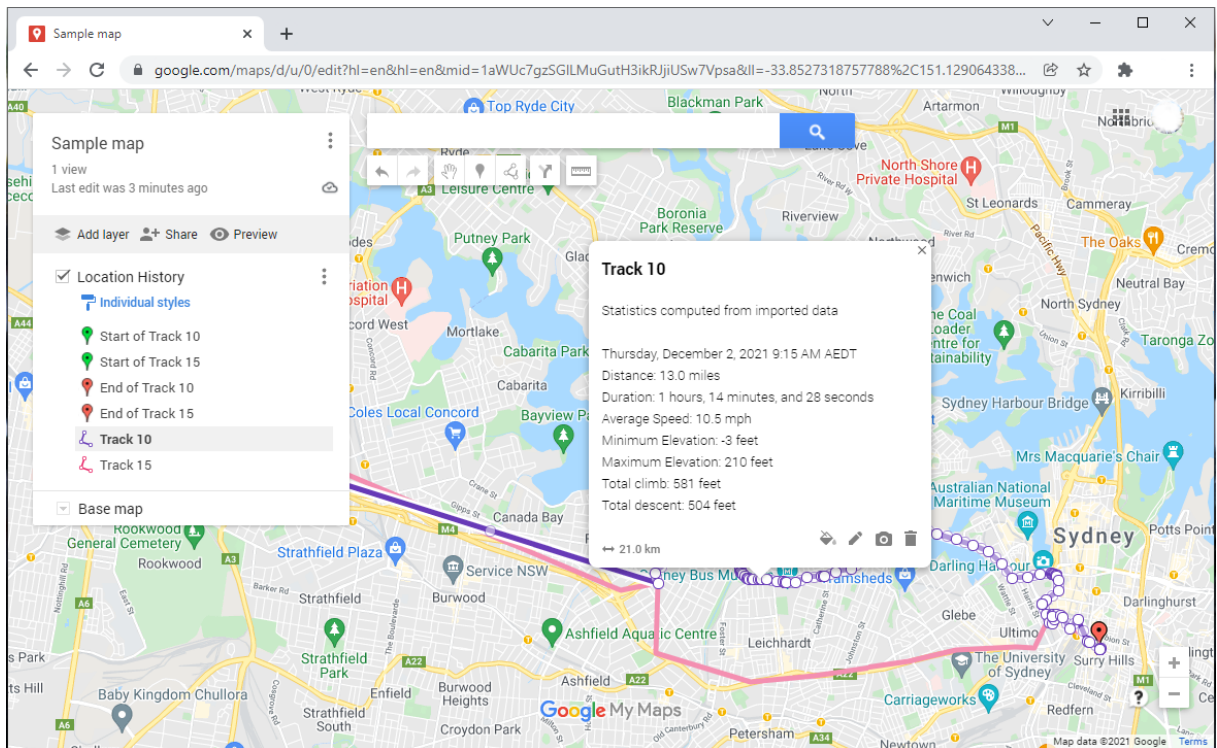
Google Location History

A parser for Google Location History data.

Download Location History in Json format from Google Takeout and load the "Location History.json" file for decoding.

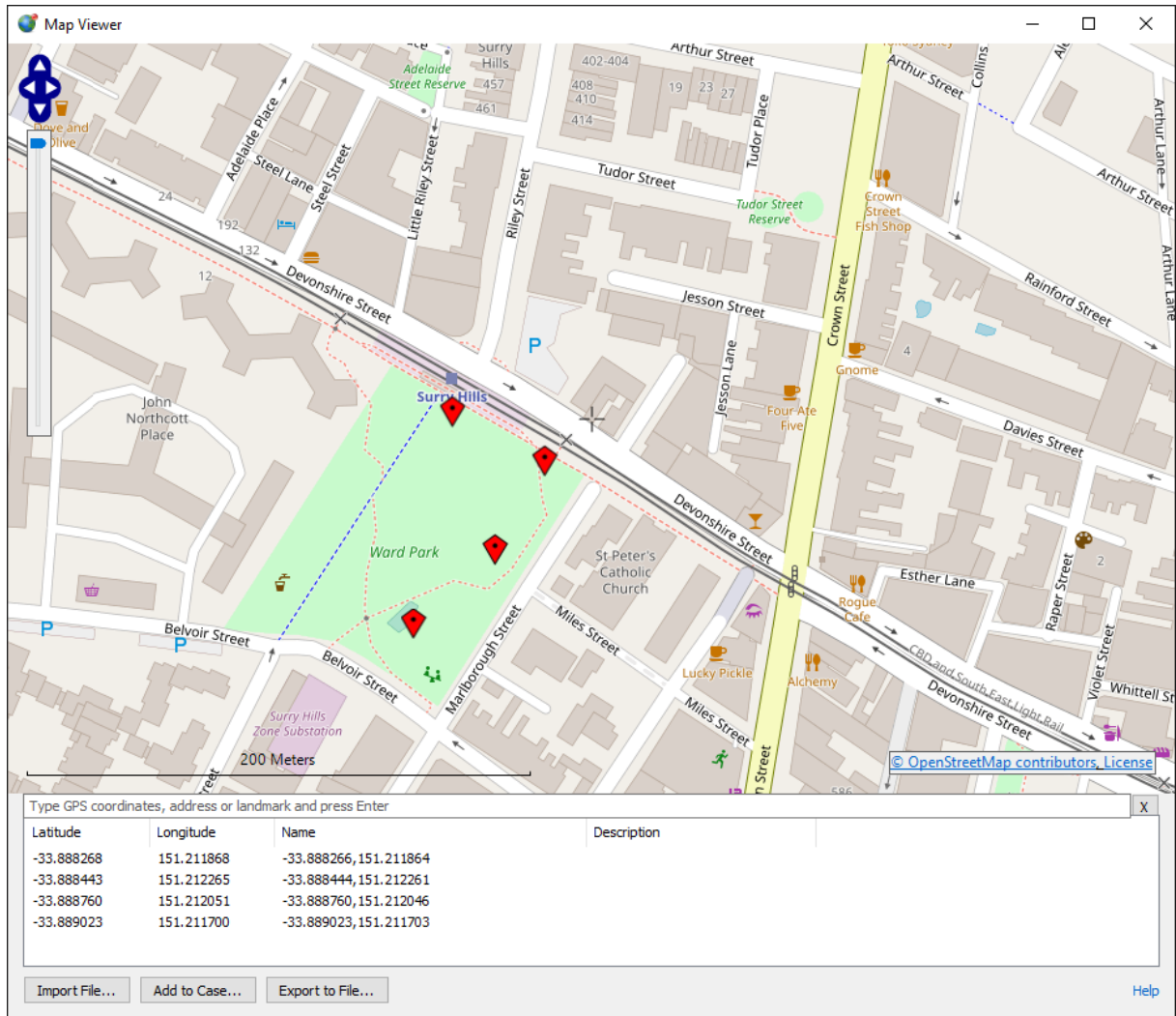
- Locations can be viewed on internal Map Viewer
- Export to KML/GPX/CSV file formats
- Analyze exports using Google Earth, Google Maps My Maps or Power BI ... (see the examples below)





5.20 Map Viewer

The Map Viewer provides an interface for searching, importing and plotting location-based evidence on a world map. This includes GPS coordinates IP addresses, physical addresses and landmarks found in digital evidence.



Search

Search for GPS coordinates IP addresses, physical addresses and landmarks on the world map.

Import File...

Import GPX, KML or CSV files containing GPS coordinates or IP addresses as pins on the map.

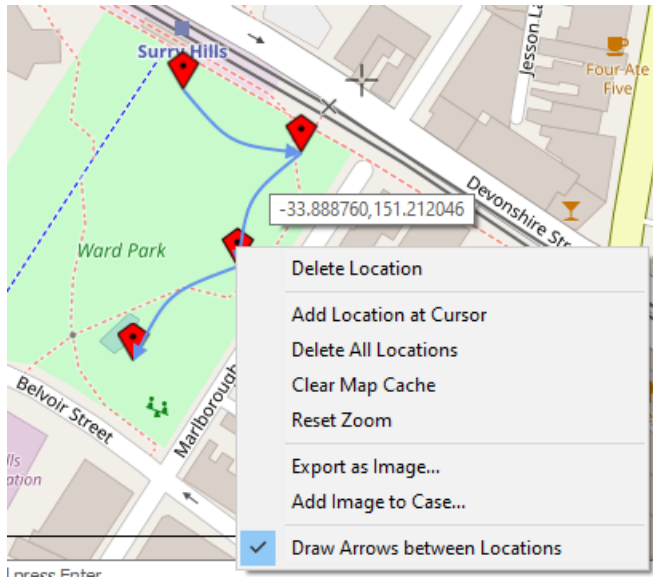
Add to Case...

Add the list of locations indicated by the pins on the map to the Case.

Export to File...

Save the list of locations indicated by the pins on the map to a CSV file.

Right-click Menu



Delete location

Delete the selected location indicated by the pin.

Add location at cursor

Add and insert a pin at the location indicated by the cursor to the list.

Delete all locations

Delete and remove all pins from the map.

Clear map cache

Delete the downloaded map tiles cached on disk. This may fix issues related to map tiles not being drawn properly.

Reset zoom

Reset the zoom and pan to ensure all pins are visible.

Export as image...

Save the current map image as a PNG file on disk.

Add image to Case...

Add the current map image to the Case.

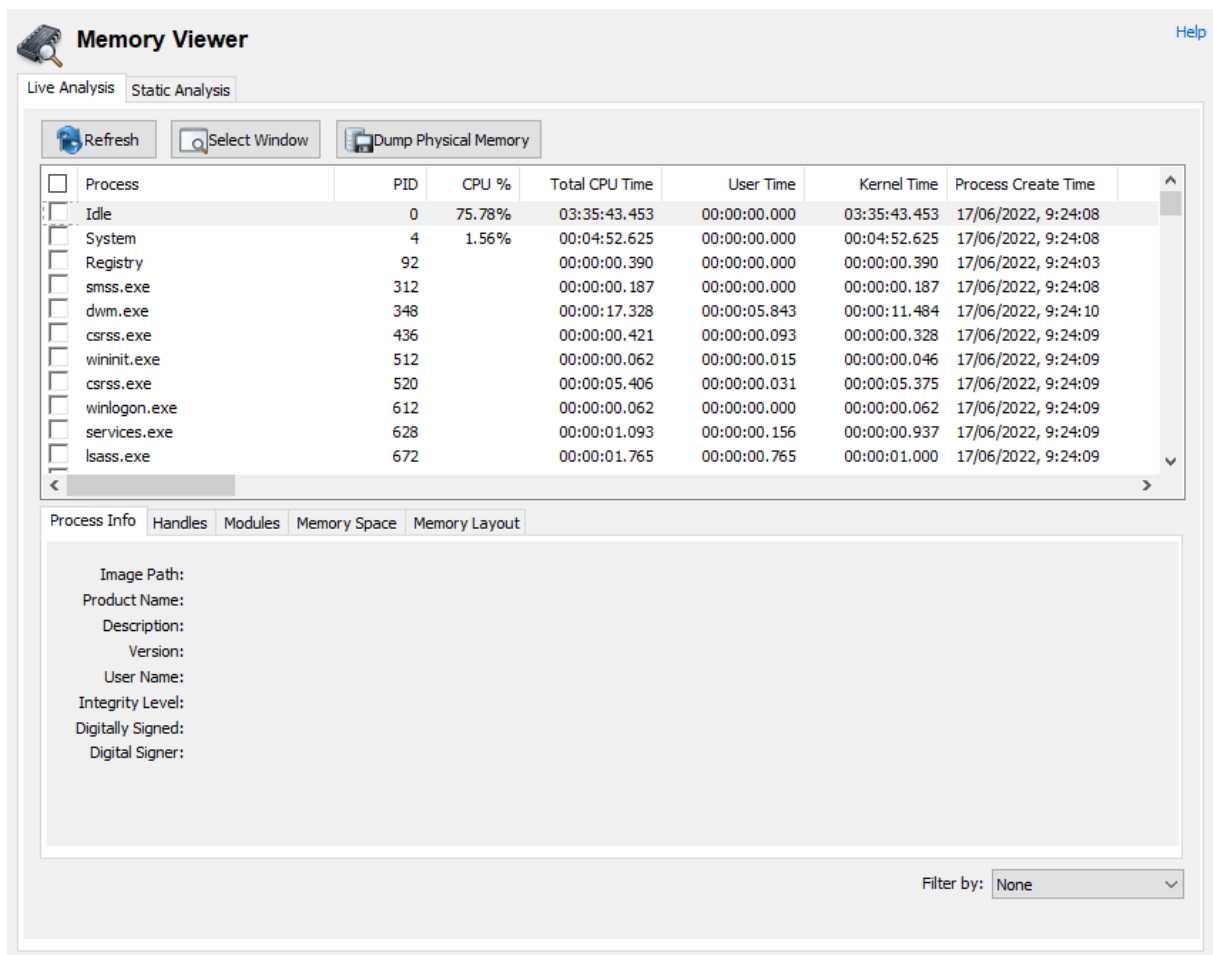
Draw arrows between locations

Draw arrows between each pin according to the list order.

5.21 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



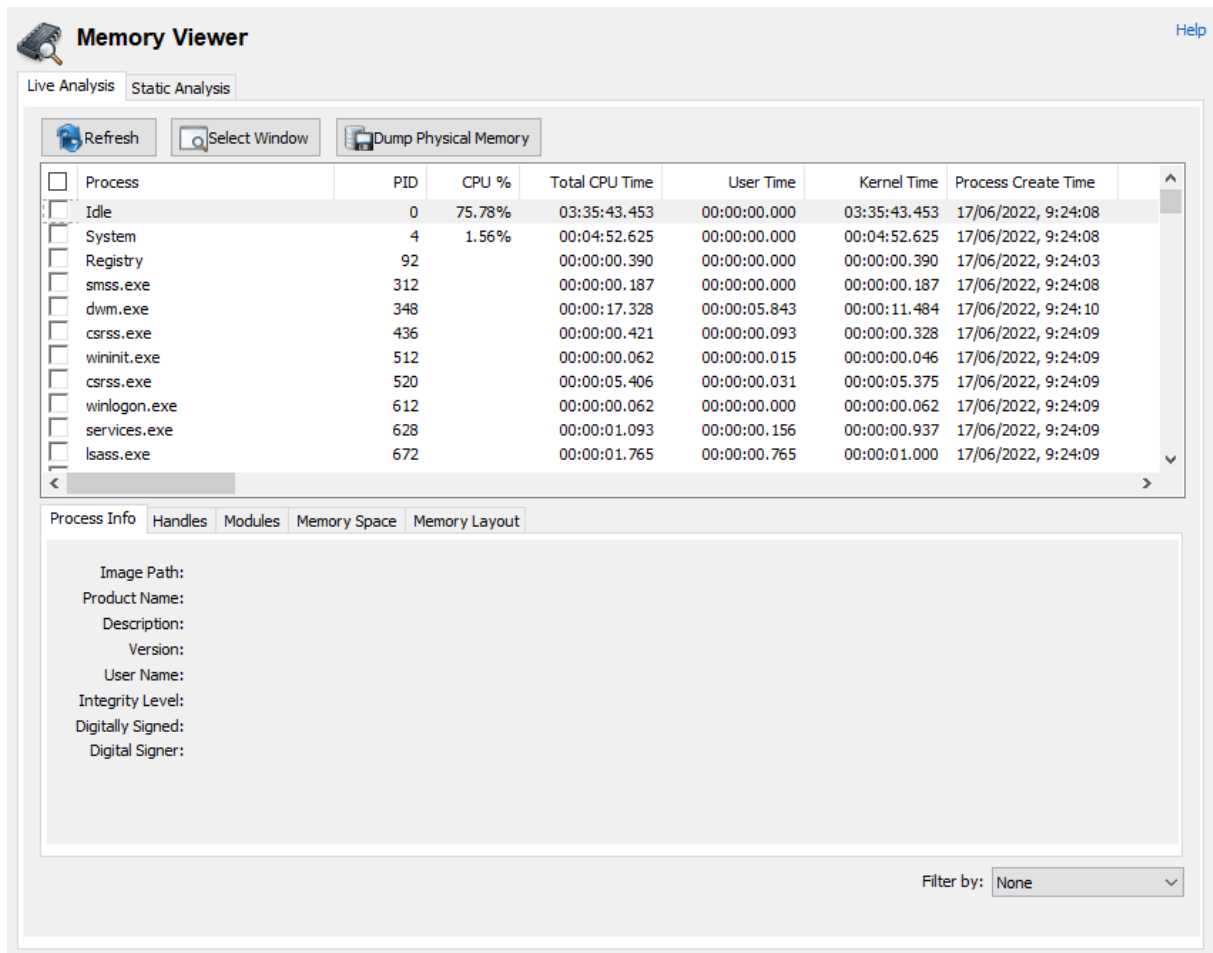
When performing 'Live Analysis', the memory details of all processes currently running on the system is displayed in a Task Manager-like view. Unlike non-volatile hard disks which can be analyzed statically, memory contents (RAM) can only be analyzed while the system is live. Furthermore, it is possible 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

5.21.1 Live Analysis

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



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.

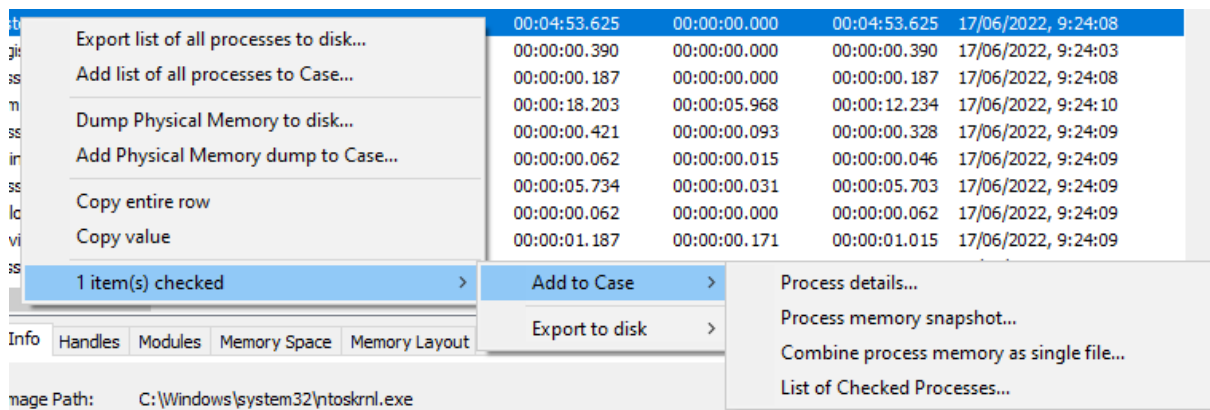
Select Window

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.



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.

Copy entire row

Copy the text of the selected row to clipboard

Copy value

Copy the text of the selected cell to clipboard

X item(s) checked

Add to Case/Export to disk

Process Details...

Take a snapshot of the selected process details and save to case/disk

Process Memory Snapshot...

Take a memory dump snapshot of the selected process details and save to case/disk

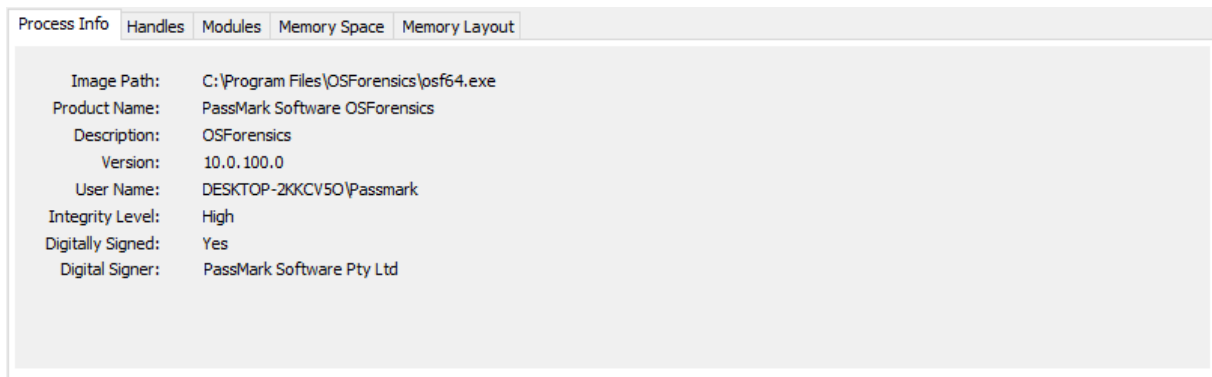
Combine Process Memory as single file...

List of Checked Processes...

Add process to Case

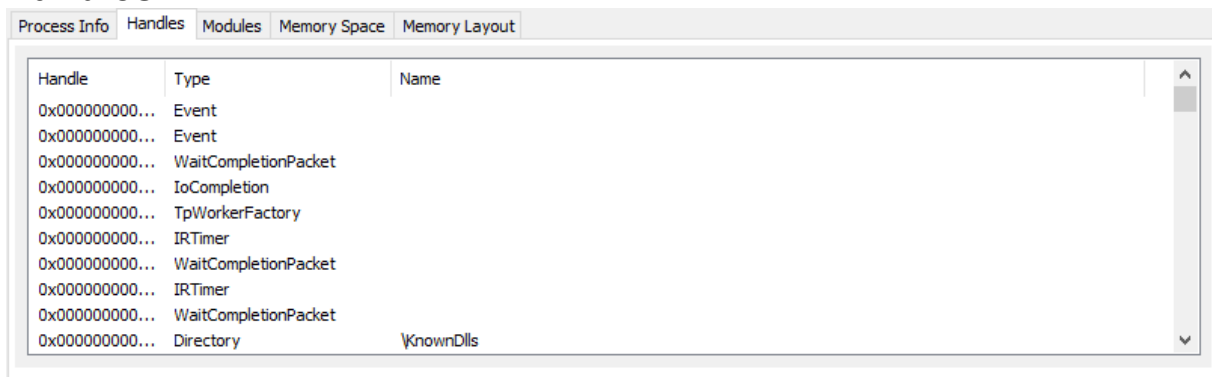
Take a snapshot of process details or memory dump of the selected process and add to the case.

Process Info



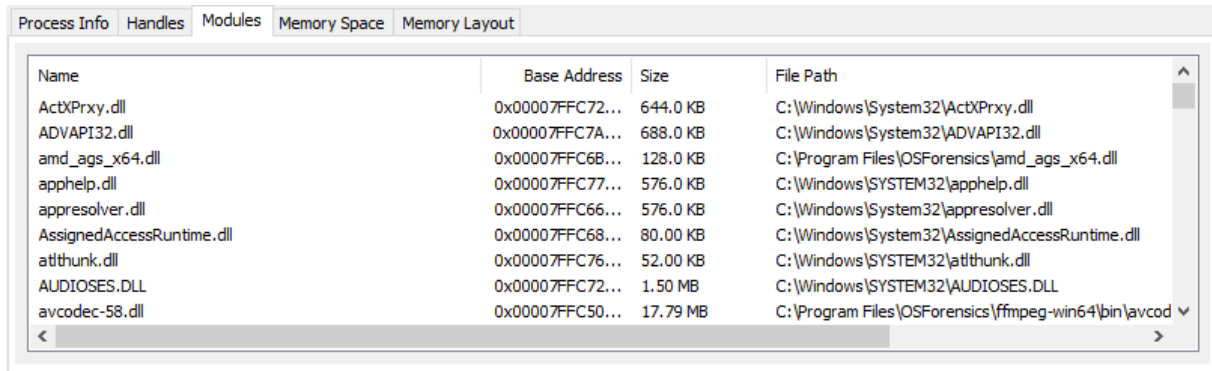
This view shows the details of the application whose process was created.

Handles



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

Modules



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

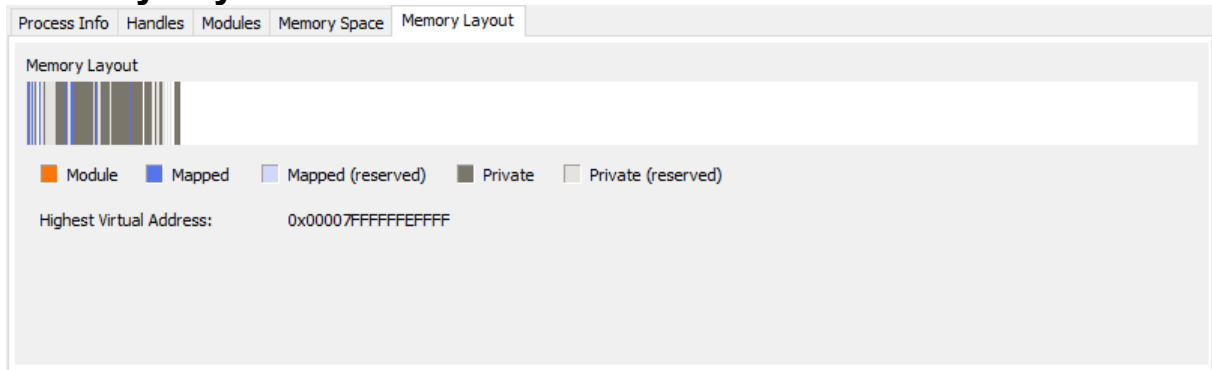
Address Range	Size	State	Protection	Type	Module
0x0000000000000000 - 0x00000...	64 KB	Free	NA	-	
0x00000000000010000 - 0x00000...	64 KB	Commit	RW	Mapped	
0x00000000000020000 - 0x00000...	32 KB	Commit	RW	Private	
0x00000000000028000 - 0x00000...	20 KB	Reserved	-	Private	
0x0000000000002D000 - 0x00000...	12 KB	Free	NA	-	
0x00000000000030000 - 0x00000...	116 KB	Commit	RO	Mapped	
0x0000000000004D000 - 0x00000...	12 KB	Free	NA	-	
0x00000000000050000 - 0x00000...	16 KB	Commit	RO	Mapped	
0x00000000000054000 - 0x00000...	48 KB	Free	NA	-	
0x00000000000060000 - 0x00000...	8 KB	Commit	RO	Mapped	

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.

5.21.1.1 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.

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

To view the raw data and extract the strings from the memory dump file, click View & Extract Strings. This opens the internal viewer in hex view which provides tools to extract and discover strings of interest (eg. passwords) in the memory dump file.

5.22 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.

Mismatch File Search

Folder to scan: Drive-C:\

Preset: Default

Exclude ext: {Unknown}, Exclude folders: , Exclude empty files, Ex

Scan Config...

Sort by: Extension

File Details	File List	Thumbnails
	\$UPCase Location: Drive-C: Identified Type: MS Windows icon resource - 2 icons, 3x, 4-colors Size: 128.0 KB, Created: 31/05/2022, 8:32:06, Modified: 31/05/2022, 8:32:06, Accessed: 31/05/2022, 8:32:06	
	037c36f003651fb9c10e544af926af8dd51fa017892c82b2d8c8f3a6ab154a25 Location: Drive-C:\Users\Passmark\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2bxewy\LocalState\Assets Identified Type: PNG image, 142 x 142, 8-bit/color RGBA, non-interlaced Size: 5.64 KB, Created: 30/05/2022, 15:02:14, Modified: 30/05/2022, 15:02:14, Accessed: 30/05/2022, 15:02:14	
	0b426d2ed0dfa40b7c7c747cc7779b1a09fde88e69eeb8fc36887239874cca8d Location: Drive-C:\Users\Passmark\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2bxewy\LocalState\Assets Identified Type: PNG image, 142 x 142, 8-bit/color RGBA, non-interlaced Size: 16.54 KB, Created: 30/05/2022, 15:02:14, Modified: 30/05/2022, 15:02:15, Accessed: 30/05/2022, 15:02:15	
	1247a657fb7ca61cda4214de9c943daebada7b739fe43a43074c015ba0b4455 Location: Drive-C:\Users\Passmark\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2bxewy\LocalState\Assets Identified Type: PNG image, 142 x 142, 8-bit/color RGBA, non-interlaced Size: 2.57 KB, Created: 30/05/2022, 15:02:14, Modified: 30/05/2022, 15:02:15, Accessed: 30/05/2022, 15:02:15	
	16ea5037abdd0a917fc4c833ba99e9886f8cef06b335435ec31c1f309440c4e7 Location: Drive-C:\Users\Passmark\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2bxewy\LocalState\Assets Identified Type: PNG image, 142 x 142, 8-bit/color RGBA, non-interlaced Size: 15.94 KB, Created: 30/05/2022, 15:02:14, Modified: 30/05/2022, 15:02:15, Accessed: 30/05/2022, 15:02:15	
	1bcd41517ed0bc63bb85b376a9f8ffc3273cad2542b1080f6d963050c7074d8 Location: Drive-C:\Users\Passmark\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2bxewy\LocalState\Assets Identified Type: PNG image, 142 x 142, 8-bit/color RGBA, non-interlaced Size: 5.22 KB, Created: 30/05/2022, 15:02:14, Modified: 30/05/2022, 15:02:15, Accessed: 30/05/2022, 15:02:15	
	1d4f3e84a24b7244e09e554581355185db0ca1016b4023b4537acc793d50b31 Location: Drive-C:\Users\Passmark\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2bxewy\LocalState\Assets Identified Type: PNG image, 142 x 142, 8-bit colormap, non-interlaced Size: 1.46 KB, Created: 30/05/2022, 15:02:14, Modified: 30/05/2022, 15:02:14, Accessed: 30/05/2022, 15:02:14	

Search cancelled Items Searched: 202185 Items Found: 1275

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.

Preset

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

Default - Only known files whose file extension/contents that are mismatched are displayed

All - The search results are filtered using all built-in filters

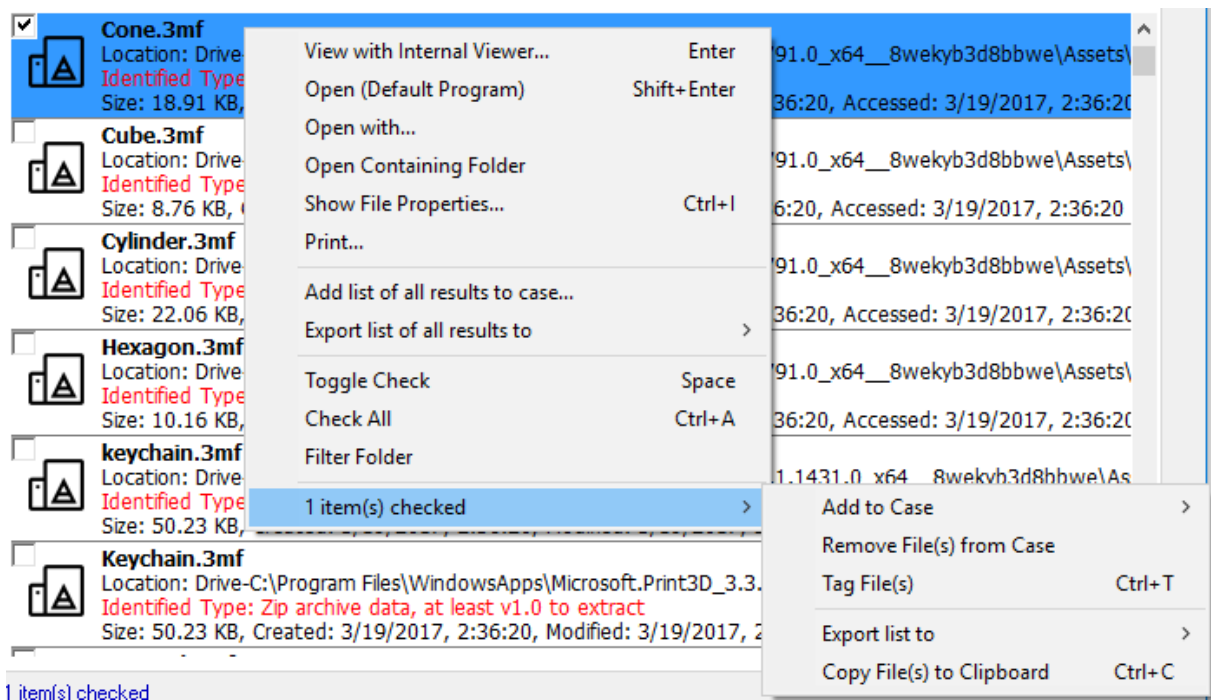
Inaccessible - Only files that could not be accessed are displayed

Mismatch - Files (including unknown files) whose file extension/contents that are mismatched are displayed

To create a new filter, click the *Config...* link.

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.

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

Tag File(s)

Tag file(s) for future reference. *Keyboard shortcut: Ctrl+T*

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.

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.

5.22.1 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.

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, Note: This is used to filter based on the 'Identified type' column:

File Name	Location	Identified Type	Type
<input type="checkbox"/> 2550FDABB65ABC15B...	C:\Users\Passmark\AppData\Local\Mozilla\Fir...	gzip compressed data, max compressi...	File
<input type="checkbox"/> B3316860430DA0966...	C:\Users\Passmark\AppData\Local\Mozilla\Fir...	gzip compressed data, max compressi...	File
<input type="checkbox"/> 16C6B40DA5C76207C...	C:\Users\Passmark\AppData\Local\Mozilla\Fir...	JPEG image data, EXIF standard	File
<input checked="" type="checkbox"/> 998F6186761E05A574...	C:\Users\Passmark\AppData\Local\Mozilla\Fir...	JPEG image data, JFIF standard 1.01	File
<input type="checkbox"/> 9BE839B987F4E477F...	C:\Users\Passmark\AppData\Local\Mozilla\Fir...	JPEG image data, JFIF standard 1.01	File
<input type="checkbox"/> 96EE5B9CEF94F67E1...	C:\Users\Passmark\AppData\Local\Mozilla\Fir...	JPEG image data, JFIF standard 1.01	File

For example, if you want to include/exclude the 'JPEG image data...' you can add that into the text box. You can also enter just part of the type e.g. 'image' and this will include/exclude all files with 'image' in its Identified type.

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, search results will not include Chrome Cache image files in the below directory:

```
..\AppData\Local\Google\Chrome\User Data\Default\Cache\*
```

Exclude Firefox Cache Image Files

If checked, search results will not include Firefox Cache image files in the below directory

```
..\AppData\Local\Mozilla\Firefox\Profiles\[profile]\Cache*
```

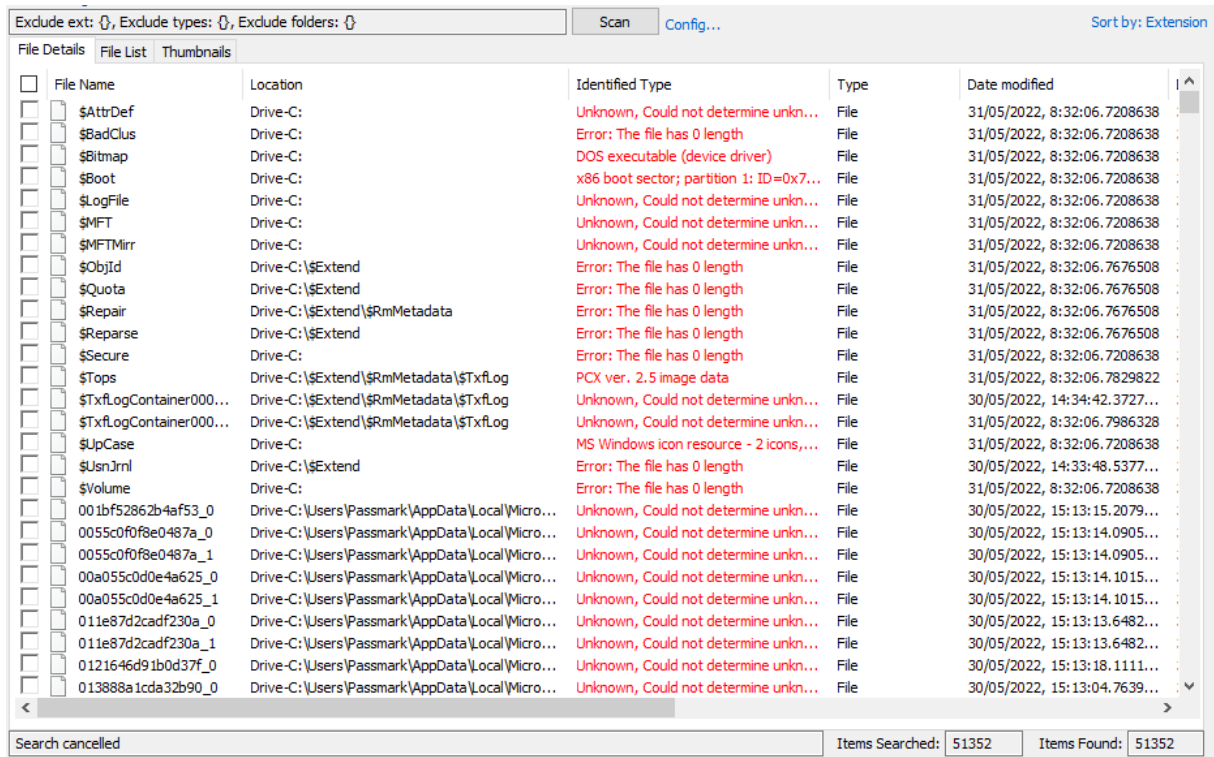
Exclude c:\windows\installer icon/zip files

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

5.22.2 Mismatch File Search Results View

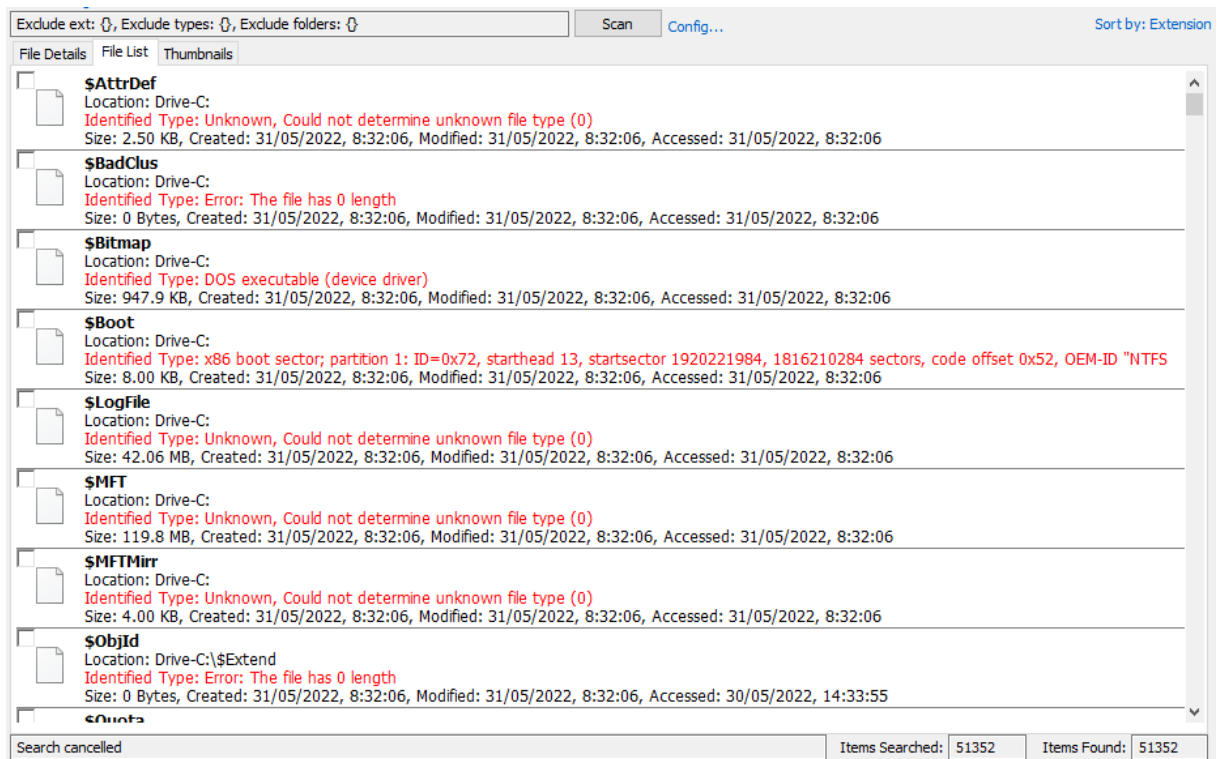
The user may view the mismatch file search results in one of several views.

File Details View



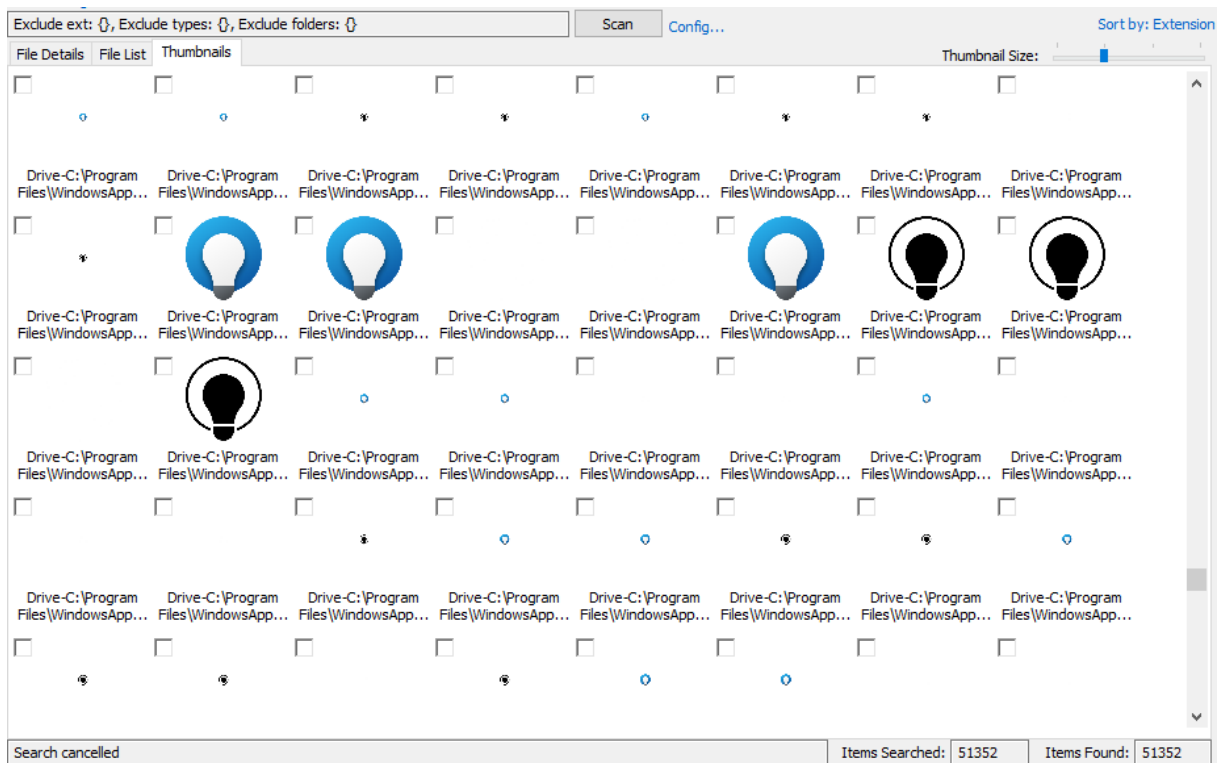
The File Details View displays the search result in a table format, listing the file names along with relevant attributes and metadata.

File List View



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



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.

5.22.3 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 (I+R) specifies an offset that is the total of the value of memory location specified by I and the value R.

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

Field 2

The next field is a type: byte, short, long, string, Ustring (Unicode string), 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 bytes 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.mksssoftware.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.

5.23 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

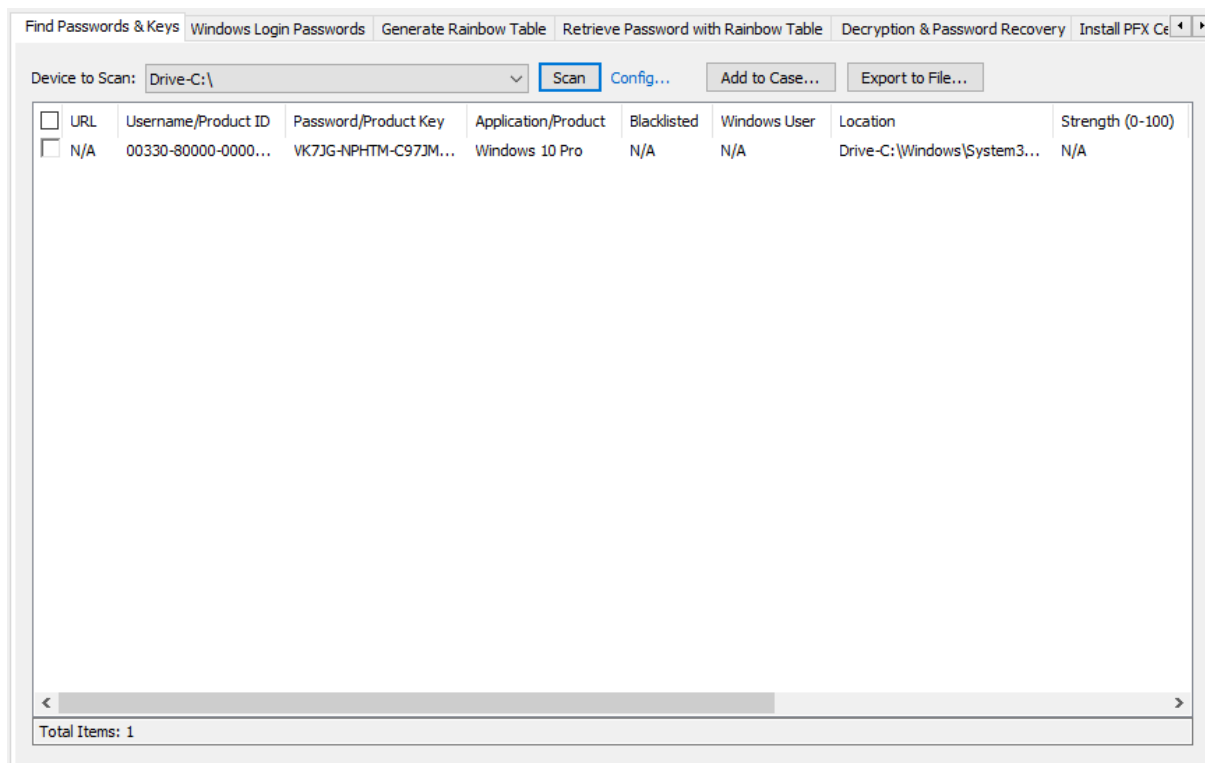
Decrypt and access encrypted files.

Install PFX Certificate

Install a PFX certificate so Windows EFS files can be decrypted and opened.

5.23.1 Find Passwords/Keys

This feature can recover passwords for several types of applications, as well as Microsoft product keys.



Artifacts Extracted

1. **URL** - This column contains the URL that browser passwords were used for. For non-browser passwords and product keys, this field does not apply.
2. **Username/Product ID** - This is the username or login that a password is associated with. For product keys, this column will contain the product ID instead.
3. **Password/Product Key** - This contains the plaintext password or product key.
4. **Application/Product** - This column contains the type of password that was extracted (see below for a list of applications), or in the case of a product key, it contains the name of the product the license key is for.
5. **Blacklisted** - These are websites for which a user has selected to never save a password for. In this case only the website visited will be displayed and no password.
6. **Windows User** - This contains the Windows user to which the login information is associated.

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.

Supported applications

Below is a table that shows which features are supported for different 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).

5.23.1.1 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).

The screenshot shows the 'Configure Password Retrieval' dialog box. It is divided into several sections:

- Include:** A list of checkboxes for various password types, all of which are checked: All, Chrome Passwords, Internet Explorer Passwords, Microsoft Edge Passwords, Opera Passwords, Microsoft Product Keys, Windows Autologon Password, Wi-Fi Passwords, Outlook Passwords, Windows Live Mail Passwords, and Firefox Passwords.
- Offline Decryption Settings:** Two radio button options are present: 'Dictionary Attack' (selected) and 'Enter Windows User Login'. Under 'Dictionary Attack', there are sub-options for 'Automatic' (selected) and 'Use Dictionary File:' with an empty text box and a browse button (...). The 'Enter Windows User Login' option has two text boxes labeled 'Username' and 'Password', both of which are empty.
- Note:** A text box containing the following text: "This mode is recommended if you do not know any Windows User passwords for the offline disk/image that you are investigating. OSForensics will attempt to crack Windows User passwords using a common passwords dictionary. If successful, it will use this password to unlock DPAPI encrypted logins stored on the system."
- Scan Options:** A checkbox labeled 'Scan "Windows.old" folder' which is checked.
- Buttons:** At the bottom right, there are three buttons: 'Reset to Default', 'OK' (highlighted with a blue border), and 'Cancel'.

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.

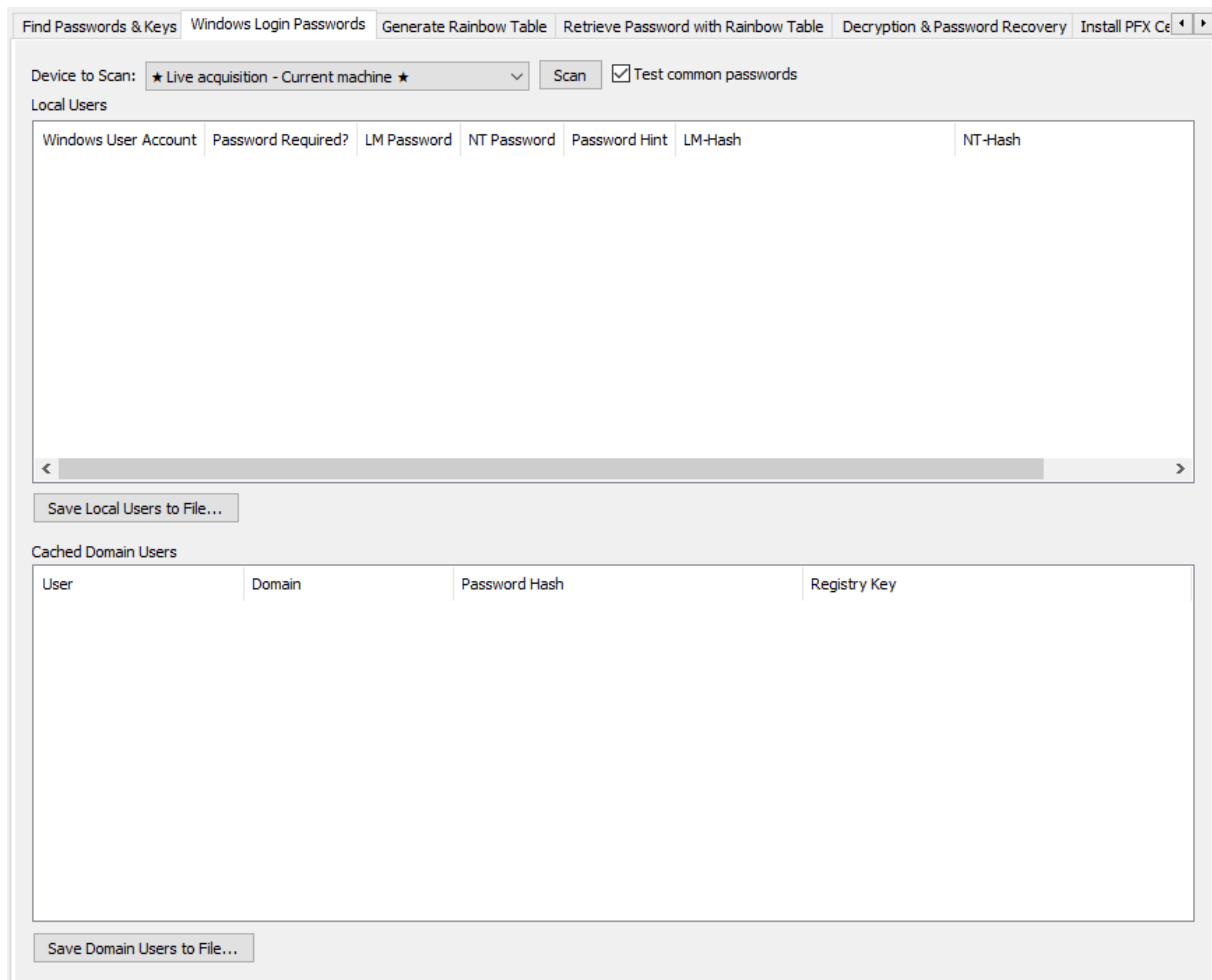
If you do not know the Windows user password, you can try obtaining it with the following steps:

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.

5.23.2 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.



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.

5.23.2.1 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 too long for a LM hash has been used (15 or more characters).

For more information on LM and NT hashes see these Wikipedia articles.

5.23.3 Generating Rainbow Tables

This window is used for generating Rainbow Tables. These tables can then be used in the Rainbow Table Password Recovery Window.

Passwords Help

Find Passwords & Keys | Windows Login Passwords | **Generate Rainbow Table** | Retrieve Password with Rainbow Table

Password Parameters

Hash Routine: md5 Min: 1 Max: 7
 Password Length: 1 - 7
 Character Set: numeric
 0123456789

Table Dimensions

Mode: Automatic Manual (Advanced Users)
 Success Rate: 95 % Chain Length: 276
 Chain Count: 275724
 Lower Decrypt Time: Lower File Size

File Path: C:\ProgramData\PassMark\OSForensics\RainbowTables\md5_numeric#1-7_0_276 ...
 Compress to RTC format

Variable	Value
Estimated Time to Generate	< 1 minute
Hashes Per Second	15228828
No. of possible passwords	11111110
Required Disk Space	4.21 MB
Success Rate	95.05%

Generate

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".

Passwords Help

Find Passwords & Keys | Windows Login Passwords | **Generate Rainbow Table** | Retrieve Password with Rainl

Password Parameters

Hash Routine: Password Length: Min Max

Character Set:

Table Dimensions

Mode: Automatic Manual (Advanced Users)

Success Rate: % Chain Length:

Lower Decrypt Time: Lower File Size: Chain Count:

File Path: ...

Compress to RTC format

Variable	Value
Estimated Time to Generate	< 1 minute
Hashes Per Second	15610584
No. of possible passwords	11111110
Required Disk Space	4.21 MB
Success Rate	95.05%

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.

5.23.3.1 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

5.23.3.1.1 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
000000010h: FA 2D 0E 00 00 00 00 00 9D 06 00 00 00 00 00
000000020h: CE 06 09 00 00 00 00 00 AD 06 00 00 00 00 00
000000030h: AB 03 04 00 00 00 00 00 AE 06 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 an indexed version of RT format. RTI Format aims to save 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.

5.23.3.1.2 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"

5.23.3.1.3 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:

$$f(\text{hash}) = (\text{hash} + i) \% \text{plaintext_space}$$

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.

5.23.3.1.4 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

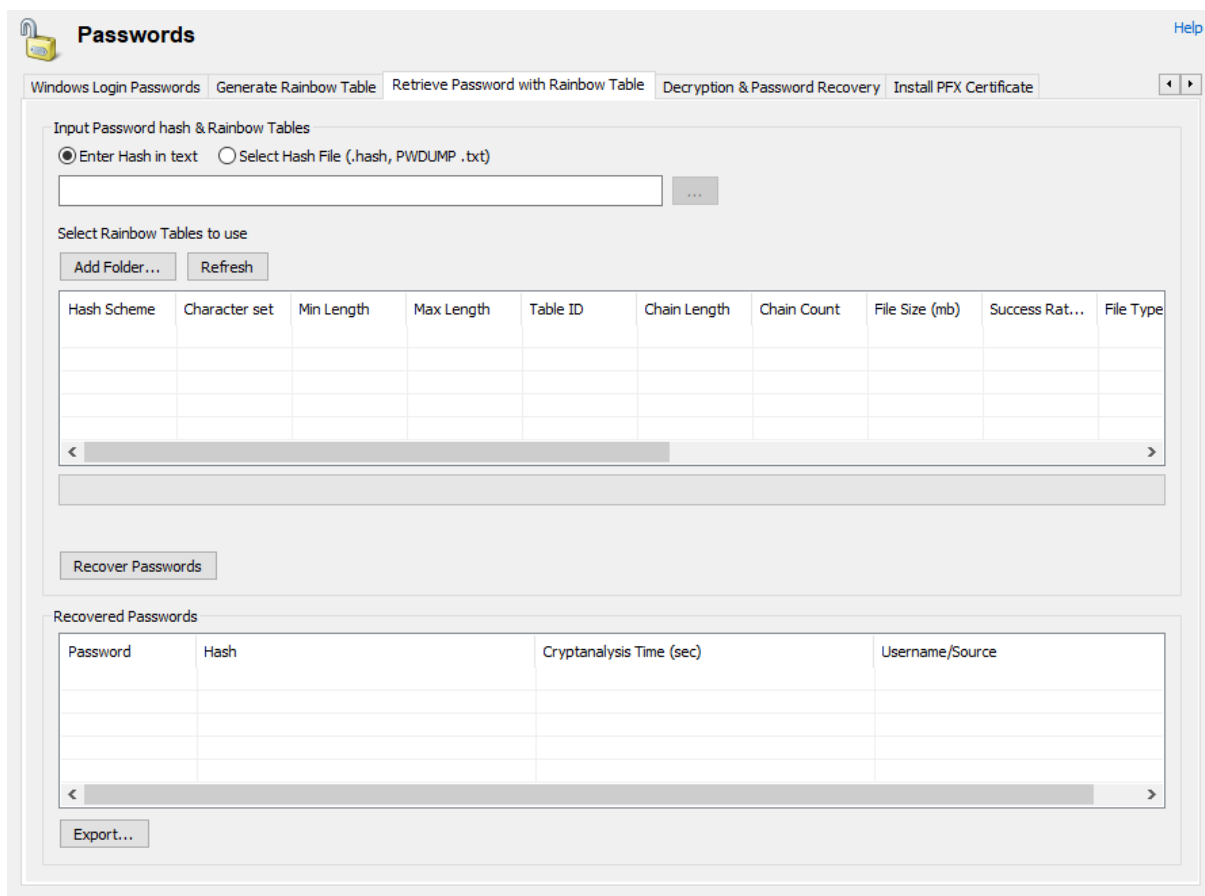
Users can specify a list of character set definitions by adding a configuration file named charset.txt to the RainbowTables folder in the OSForensics working path folder.

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!@#$%^&*()-_+=]
```

5.23.4 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.



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 be 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 its 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

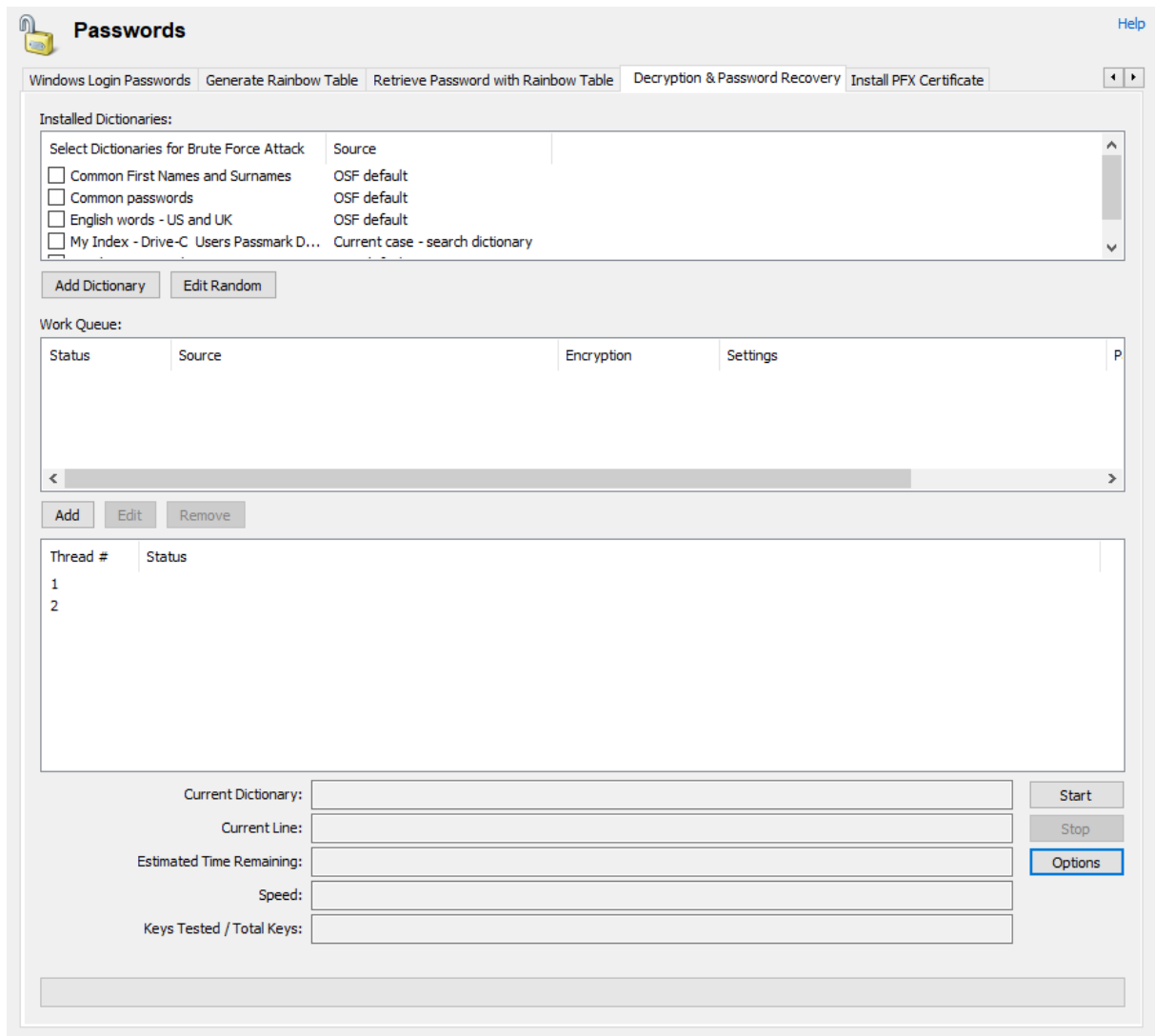
Either use an existing PWDUMP text file, or extract the LM hashes from a machine, use the Windows Login Passwords function in OSForensics, then save the extracted data to file.

"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".

5.23.5 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. Files can be added to the work queue to be processed sequentially.



Installed Dictionaries

Shows the dictionaries that are installed. If you have created a search index for the current case the dictionaries from these indexes will shown 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.

Select Dictionaries for Brute Force Attack: Clicking on the check-box for a dictionary here will select it for use with a brute force attack.

Add Dictionary

Using this button will prompt for a text file containing a list of words (one per line) to be used as a dictionary. This file will be copied to the directory:

ProgramData\Passmark\OSForensics>PasswordRecovery\Dictionaries

A simple definition file (.def) used by the decryption software will be created when adding dictionary text file. See the "Adding Dictionaries" section for more information about how the dictionaries work and more advanced ways of using them.

Edit Random

Min password length [Help](#)

Max password length

	Character Set	Known Value
Character 1:	a-z	
Character 2:	a-z	
Character 3:	All sets	
Character 4:	All sets	
Character 5:	All sets	
Character 6:	a-z	
Character 7:	a-z	
Character 8:	a-z	
Character 9:	a-z	
Character 10:	a-z	
Character 11:	a-z	
Character 12:	a-z	

Estimated combinations: 567,511,464

Example time @ 1000 pw/sec: 6 days 13 hours 38 minutes

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.

Work Queue

Files added to the work queue and their selected settings will be shown here. During the cracking process, the **status** of each file will be updated to show if a process was successful or unsuccessful. For brute-force password recovery the password will be shown upon success.

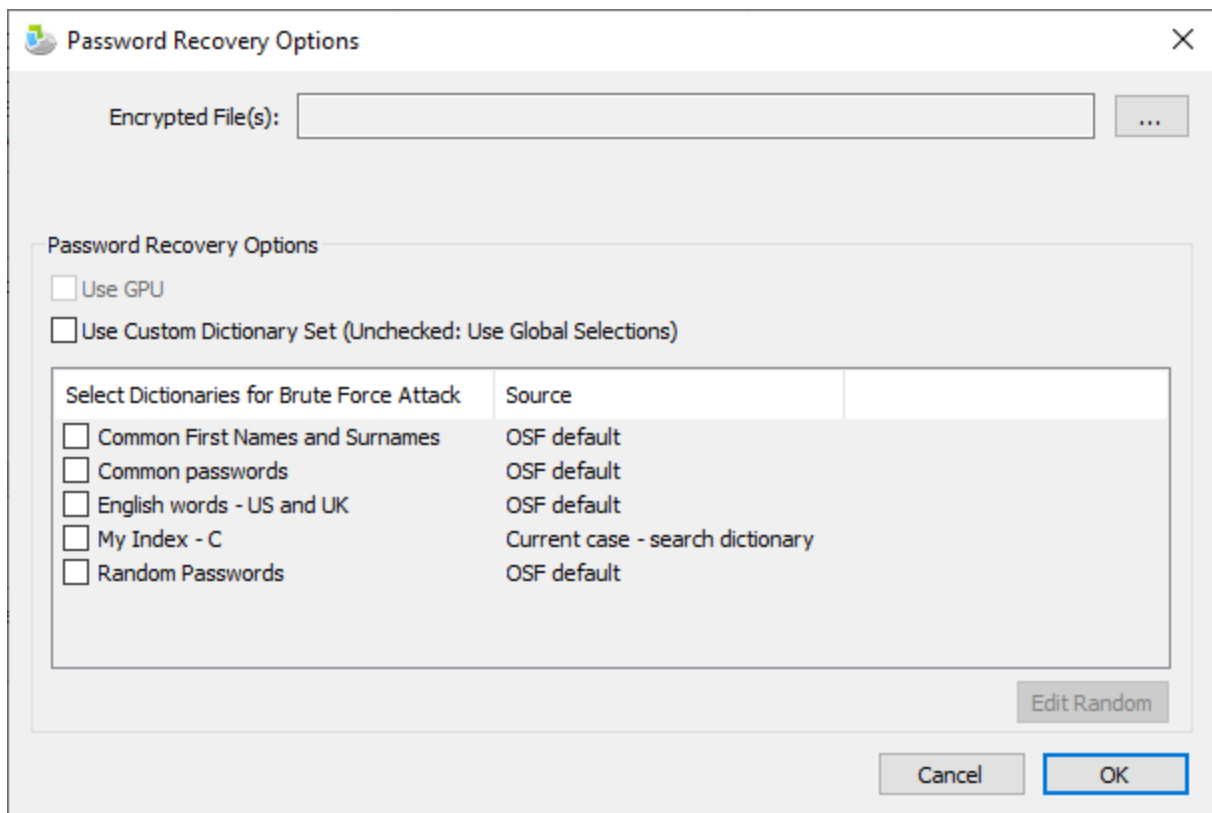
Remove

Remove a file from the work queue.

Edit

Edit the recovery settings for a file added to the queue.

Add File



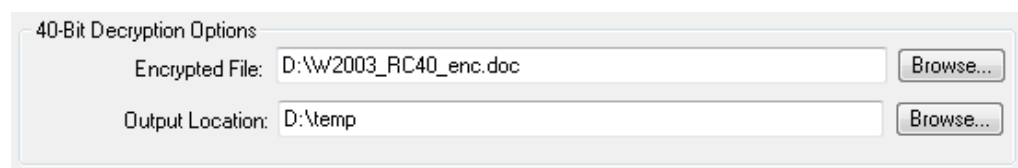
Encrypted File

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)

40-Bit Decryption:

OSForensics will display different options depending on the encryption method detected. When OSForensics detects **40-Bit Encryption** the following options will be displayed. 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.



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.

Password Recovery Options

These options are only enabled and available for selection for password recovery: (Note: Although they are displayed the dictionaries are not used when 40bit encryption is detected.)

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. When decrypting a 40 bit file, use of GPU to decrypt is not currently supported.

Use Custom Dictionary Set

If unchecked, the brute force attack will use the dictionaries selected on the main cracking module. Select this option if use different dictionaries than the global selection is required. Clicking on the checkbox for a dictionary here will select it for use with a brute force attack for this file only.

Running & Recovery Status

Options

- **Number of Local CPU Clients:** The number of local clients that will be started. The default (recommended) will be the same as the number of logical cores that is seen by Windows OS. Decryption is compute intensive and can slow down other computer operations when running, if not desirable, lower the number of clients to run.
- **Allow Remote Clients (Pro Only):** This will allow users to run additional clients on a separate machine to aid in password decryption. You will need to make sure the server application (ext_run_server.exe) is allowed through the firewall and may need to forward ports on your network to allow outside traffic to communicate with the server. See Using external PWRecClientMgr application for setup. The TOTAL number of clients supported either local or remote is 1000 clients.

Start/Stop

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.

5.23.5.1 Adding Dictionaries

The dictionary and password definition file used by OSForensics are located in the "OSForensics\PasswordRecovery\Dictionaries" folder (in Win7/Vista this will default to C:\ProgramData\PassMark\OSForensics\PasswordRecovery\Dictionaries). 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 -> psswr, offset -> offst)
.d(0) or .d to duplicate the word (passwordpassword)
.d(1) to add reversed word (passworddrowssap)

5.23.5.2 Remote Decryption Clients

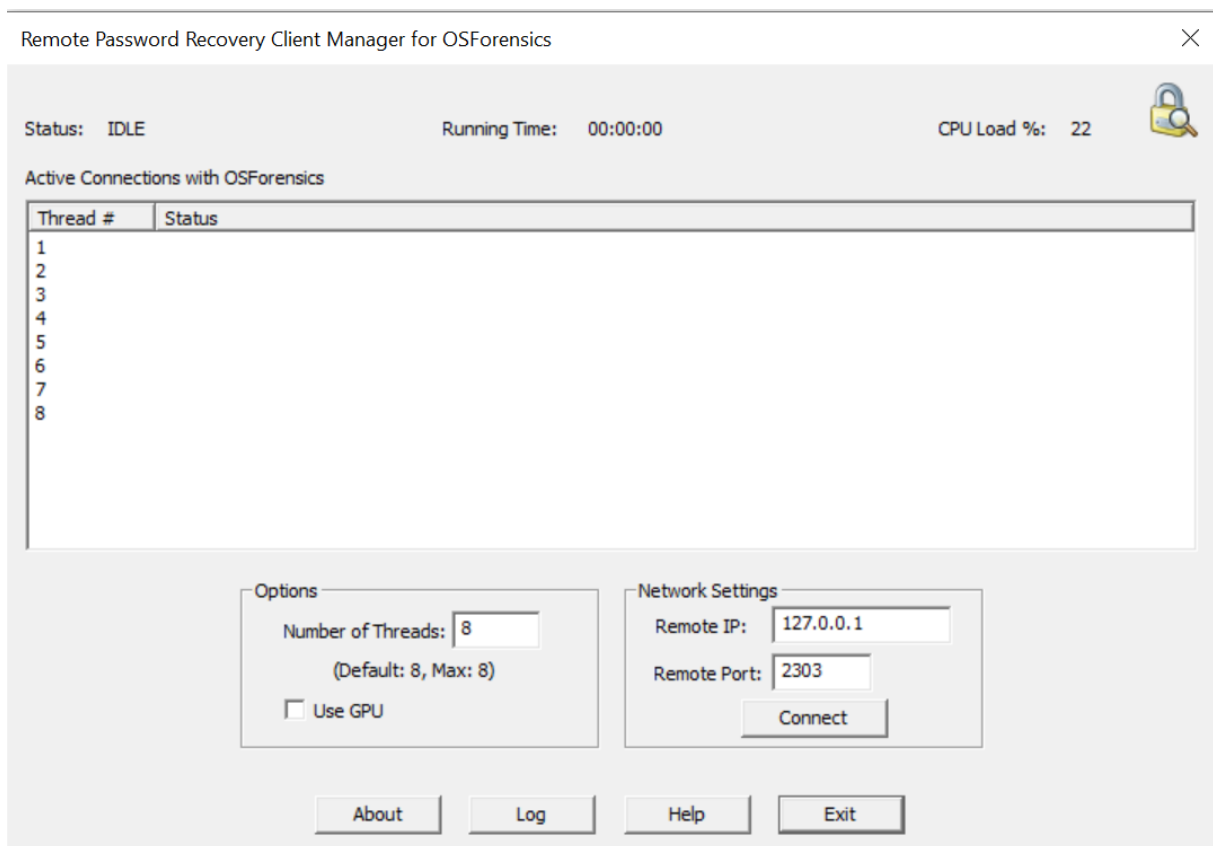
Using external application, Password Recovery Client Manager (PWRecClientMgr.exe), users can run additional clients on a separate/multiple machines to aid in password decryption. The PWRecClientMgr is a standalone application that is started on a remote machine.

The "PWRecClientMgr.exe" application and other required files (see below) are included in the OSForensics ProgramData directory and should be copied to the remote PC's and run from these systems. For example the files should be copied from the OSForensics ProgramData directory on the main PC, C:\ProgramData\Passmark\OSForensics\PasswordRecovery, to each remote PC to same directory, e.g. C:\PWRecClientMgr. The application can be started by double clicking on the PWRecClientMgr.exe file.

Required Files/Directories:

- ext_cpu_client.exe
- ext_gpu_client.exe
- PWRecClientMgr.exe
- pthreadVC2.dll
- GPUSupport.dll
- test_dll (Entire directory)

Using the external Password Recovery Client Manager



Number of Threads

The number of local CPU clients that will be started. The default will be the same as the number of logical cores that is seen by Windows OS. Decryption is compute intensive and can slow down other computer operations when running, if not desirable, lower the number of clients to run.

Use GPU

Checking this box will enable use of the GPU for faster cracking. Not all GPUs are supported. The number of GPUs supported will be shown. If enabled, the total of clients started will be the number of GPU clients supported plus the number of threads specified, e.g. Number of Threads is 8, Use GPU is checked with two GPUs supported, then 10 clients (8 CPU threads + 2 GPU threads) will be started.

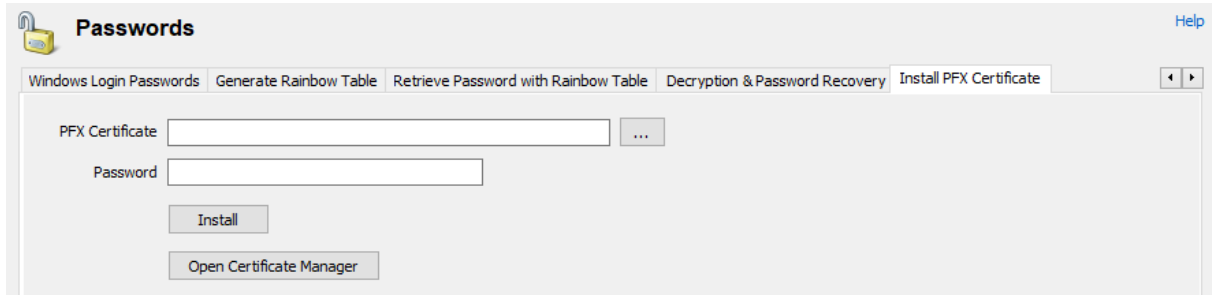
Remote IP/Remote Port

The IP address and Port of the machine running OSForensics with an active password decryption queue.

Connect

Clicking Connect will signal the application to start the clients and connect to the computer running OSForensics.

5.23.6 Install PFX Certificate



This function will allow you to install a PFX backup or recovery certificate that is associated with Windows EFS encrypted files from a disk image or another system. Use the browse button to select the PFX certificate. Enter the password (if required) for the certificate and then click the install button.

To view and delete installed certificates use the "Open certificate manager" button to open the certmgr windows program, EFS certificates are located in the Personal -> Certificates folder.

5.23.7 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:

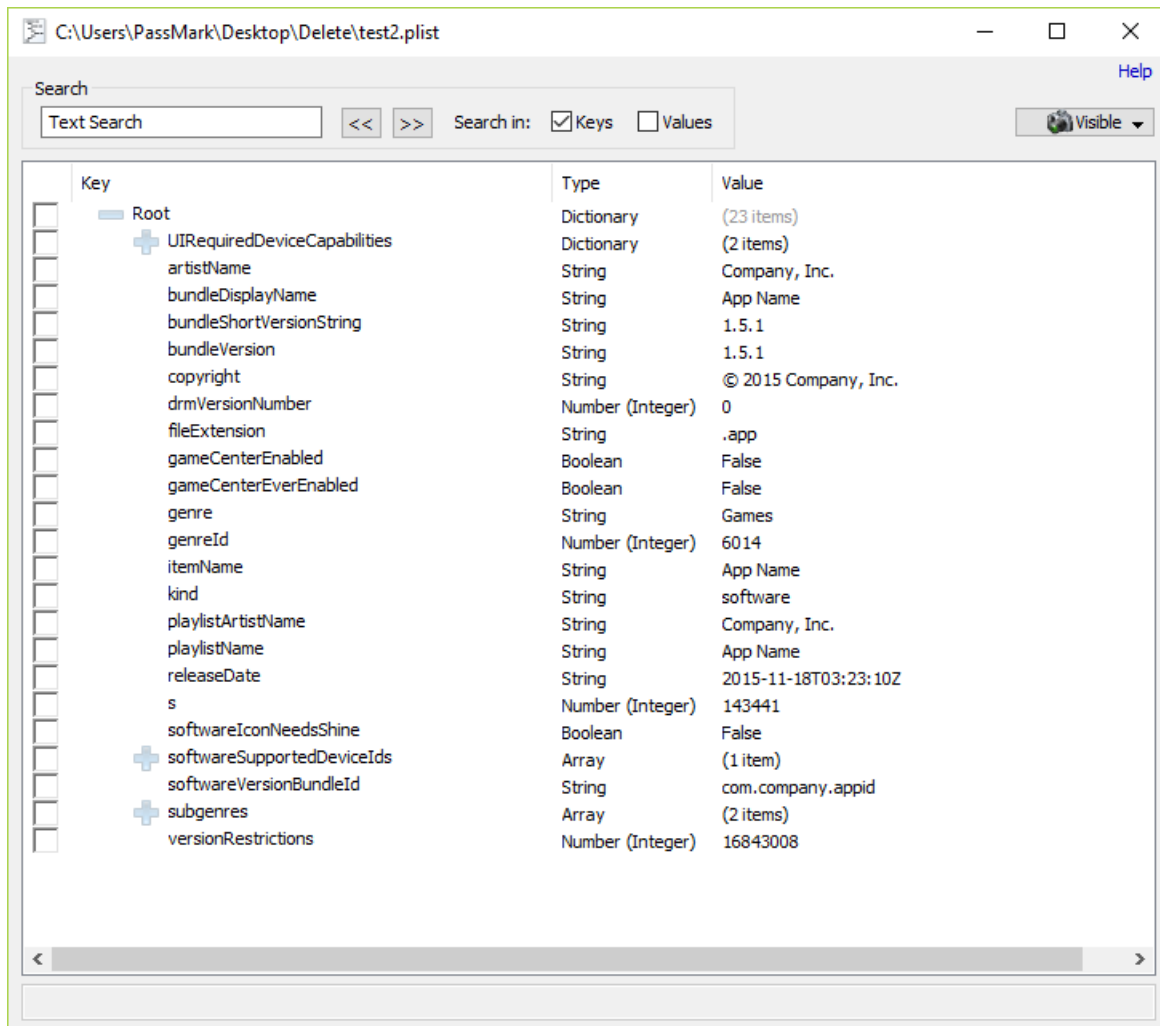
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials 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.

5.24 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.



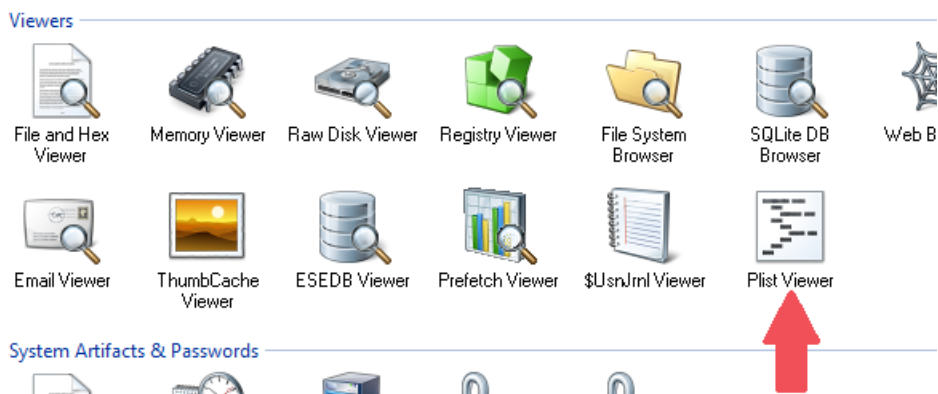
Understanding the Plist Viewer

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.



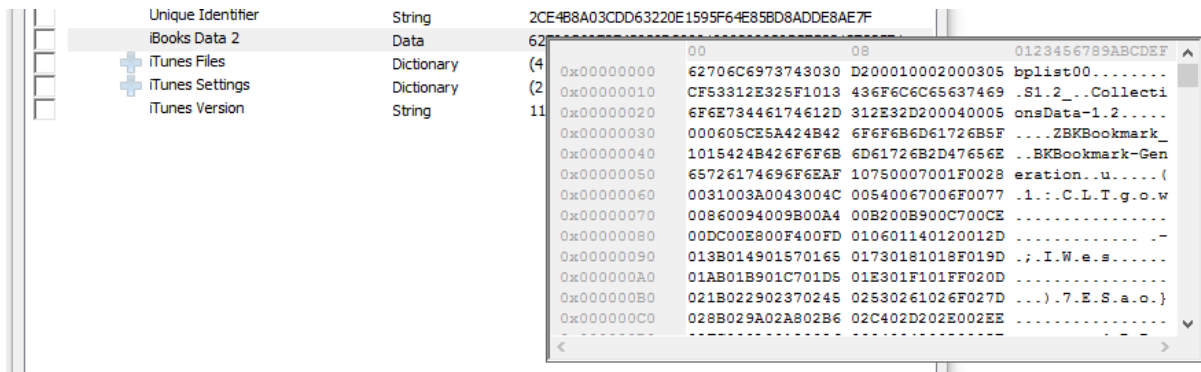
Once opened, a file selection dialog will allow you to select a file from devices added to case or on the current system itself.

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.

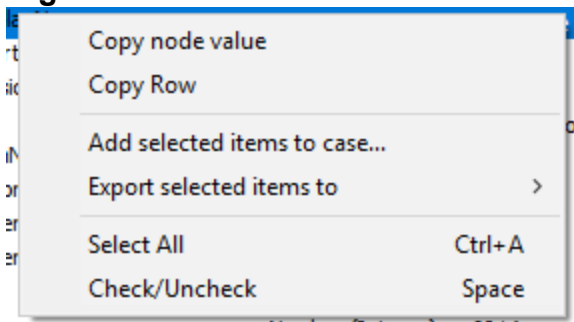


When checking an item with child elements, the children will also be selected. There are three visual states for the checkbox: checked, unchecked, mixed-checked. Selecting a child item will automatically check the parent item. Parent items with some children selected and unselected will display the mixed-checked 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 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.

5.25 Program Artifacts

The Program Artifacts module collects program artifact traces left by applications. This includes artifacts from the Windows Prefetcher or AmCache hive which can be viewed in the Prefetch Viewer and AmCache Viewer.

Program Name	Root Path	Version
Microsoft.Windows.Apprep.ChxApp	C:\Windows\SystemApps\Microsoft.Windows.AppRep.ChxApp_cw5n1h2bxewy	1000.19041.102...
Microsoft.Windows.CapturePicker	C:\Windows\SystemApps\Microsoft.Windows.CapturePicker_cw5n1h2bxewy	10.0.19041.1023
Microsoft.Office.OneNote	C:\Program Files\WindowsApps\Microsoft.Office.OneNote_16001.14326.20838.0_...	16001.14326.20...
Microsoft Visual C++ 2019 X64 Mi...	C:\ProgramData\Package Cache\{EECDD137-13DA-46ED-ADA0-BDF7F8BE65B8}\v...	14.28.29913
Microsoft Edge Update		1.3.165.21
Microsoft OneDrive	c:\Users\Passmark\AppData\Local\microsoft\OneDrive\22.141.0703.0002	22.141.0703.0002
Microsoft.WebMediaExtensions	C:\Program Files\WindowsApps\Microsoft.WebMediaExtensions_1.0.42192.0_x64...	1.0.42192.0

Value	Data
ProgramId	00000bc19da022eb94eca75a727b615c201e00000904
ProgramInstancelid	0000da39a3ee5e6b4b0d3255bfef95601890afd80709
Name	Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29913
Version	14.28.29913
Publisher	Microsoft Corporation
Language	0x00000409 (1033)
Source	Msi
Type	Application
StoreAppType	
MsiPackageCode	{285D758A-D254-455A-9CC0-B95B085E9DD0}
MsiProductCode	{EECDD137-13DA-46ED-ADA0-BDF7F8BE65B8}
HiddenArp	0x00000001 (1)
InboxModernApp	0x00000000 (0)

5.25.1 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).

Program Artifacts Viewer

Prefetch Viewer AmCache Viewer

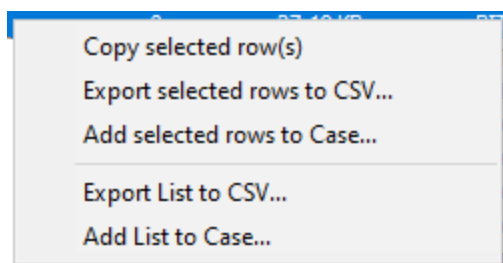
Device to Scan: C:\

Application Name	Run Count	File size	Prefetch File	Prefetch Hash	Last Run Time
BACKGROUNDTRANSFERHOST.EXE	4	34.37 KB	BACKGROUNDTRANSFERHOST.EXE-621...	621DBAF8	30/05/2022,
BIT.EXE	3	113.3 KB	BIT.EXE-AD0B05EC.pf	AD0B05EC	30/05/2022,
BITWINDOWS.EXE	0	27.19 KB	BITWINDOWS.EXE-D18E3A9D.pf	D18E3A9D	30/05/2022,
BYTECODEGENERATOR.EXE	0	33.20 KB	BYTECODEGENERATOR.EXE-FB938A53.pf	FB938A53	16/06/2022,
CMD.EXE	0	10.43 KB	CMD.EXE-0BD30981.pf	BD30981	16/06/2022,
COMPATTELRUNNER.EXE	0	8.71 KB	COMPATTELRUNNER.EXE-B7A68ECC.pf	B7A68ECC	16/06/2022,
COMREG.EXE	0	28.04 KB	COMREG.EXE-B18E07FD.pf	B18E07FD	30/05/2022,
CONHOST.EXE	0	23.64 KB	CONHOST.EXE-0C6456FB.pf	C6456FB	17/06/2022,
CONSENT.EXE	3	423.8 KB	CONSENT.EXE-40419367.pf	40419367	16/06/2022,
CSRSS.EXE	0	19.27 KB	CSRSS.EXE-F3C368CB.pf	F3C368CB	30/05/2022,

Mapped Files Mapped Directories

File Name	File Path
SMFT	\\VOLUME{01d8747517d435be-e017db84}\SMFT
ADVAPI32.DLL	\\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSTEM32\ADVAPI32.DLL
APPHELP.DLL	\\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSTEM32\APPHELP.DLL
BITWINDOWS.EXE	\\VOLUME{01d8747517d435be-e017db84}\USERS\PASSMARK\DOWNLOADED\BITWINDOWS.EXE
BITWINDOWS.TMP	\\VOLUME{01d8747517d435be-e017db84}\USERS\PASSMARK\APPDATA\LOCAL\TEMP\IS-E3PFB.TMP\B
COMBASE.DLL	\\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSTEM32\COMBASE.DLL
COMCTL32.DLL	\\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSTEM32\COMCTL32.DLL
GDI32.DLL	\\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSTEM32\GDI32.DLL
GDI32FULL.DLL	\\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSTEM32\GDI32FULL.DLL
IMM32.DLL	\\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSTEM32\IMM32.DLL
KERNEL32.DLL	\\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSTEM32\KERNEL32.DLL
KERNEL32.DLL	\\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSTEM32\KERNEL32.DLL
KERNEL32.DLL.MUI	\\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSTEM32\KERNEL32.DLL.MUI

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



Copy row(s)

Copies the selected prefetch item details to clipboard

Export selected rows to CSV...

Export the selected prefetch items to a CSV file

Add selected rows to Case...

Add the selected prefetch items to case as a CSV file

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

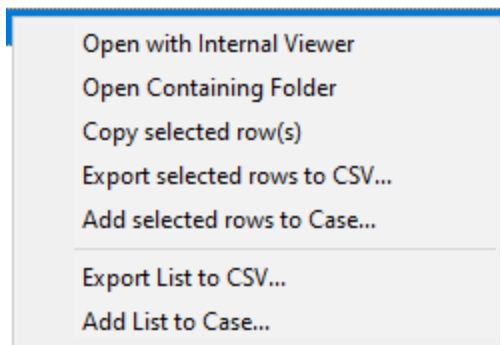
After selecting an application, the list of mapped files and directories used by the application is displayed.

Mapped Files

File Name	File Path
SMFT	\VOLUME{01d8747517d435be-e017db84}\SMFT
ADVAPI32.DLL	\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSWOW64\ADVAPI32.DLL
APPHELP.DLL	\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSWOW64\APPHELP.DLL
BITWINDOWS.EXE	\VOLUME{01d8747517d435be-e017db84}\USERS\PASSMARK\DOWNLOADS\BITWINDOWS.EXE
BITWINDOWS.TMP	\VOLUME{01d8747517d435be-e017db84}\USERS\PASSMARK\APPDATA\LOCAL\TEMP\IS-E3PFB.TMP\B
COMBASE.DLL	\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSWOW64\COMBASE.DLL
COMCTL32.DLL	\VOLUME{01d8747517d435be-e017db84}\WINDOWS\WINSXS\X86_MICROSOFT.WINDOWS.COMMON-
GDI32.DLL	\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSWOW64\GDI32.DLL
GDI32FULL.DLL	\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSWOW64\GDI32FULL.DLL
IMM32.DLL	\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSWOW64\IMM32.DLL
KERNEL32.DLL	\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSTEM32\KERNEL32.DLL
KERNEL32.DLL	\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSWOW64\KERNEL32.DLL
KERNEL32.DLL.MUI	\VOLUME{01d8747517d435be-e017db84}\WINDOWS\SYSTEM32\EN-US\KERNEL32.DLL.MUI

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 selected row(s)

Copy selected file entry details to clipboard

Export selected rows to CSV...

Export selected file entry details to a CSV file

Add selected rows to case

Add selected file entry details to case

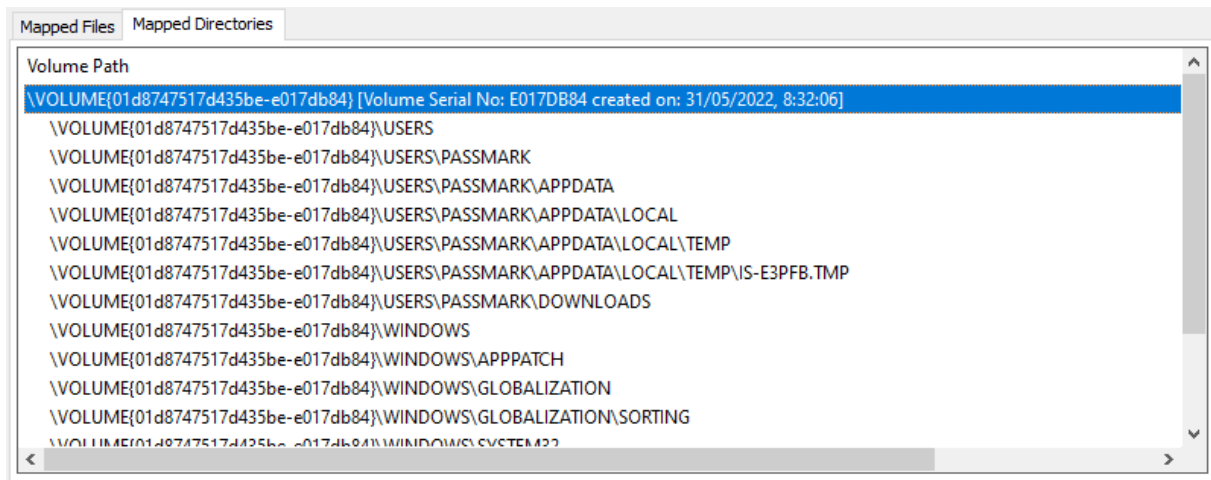
Export List to CSV...

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

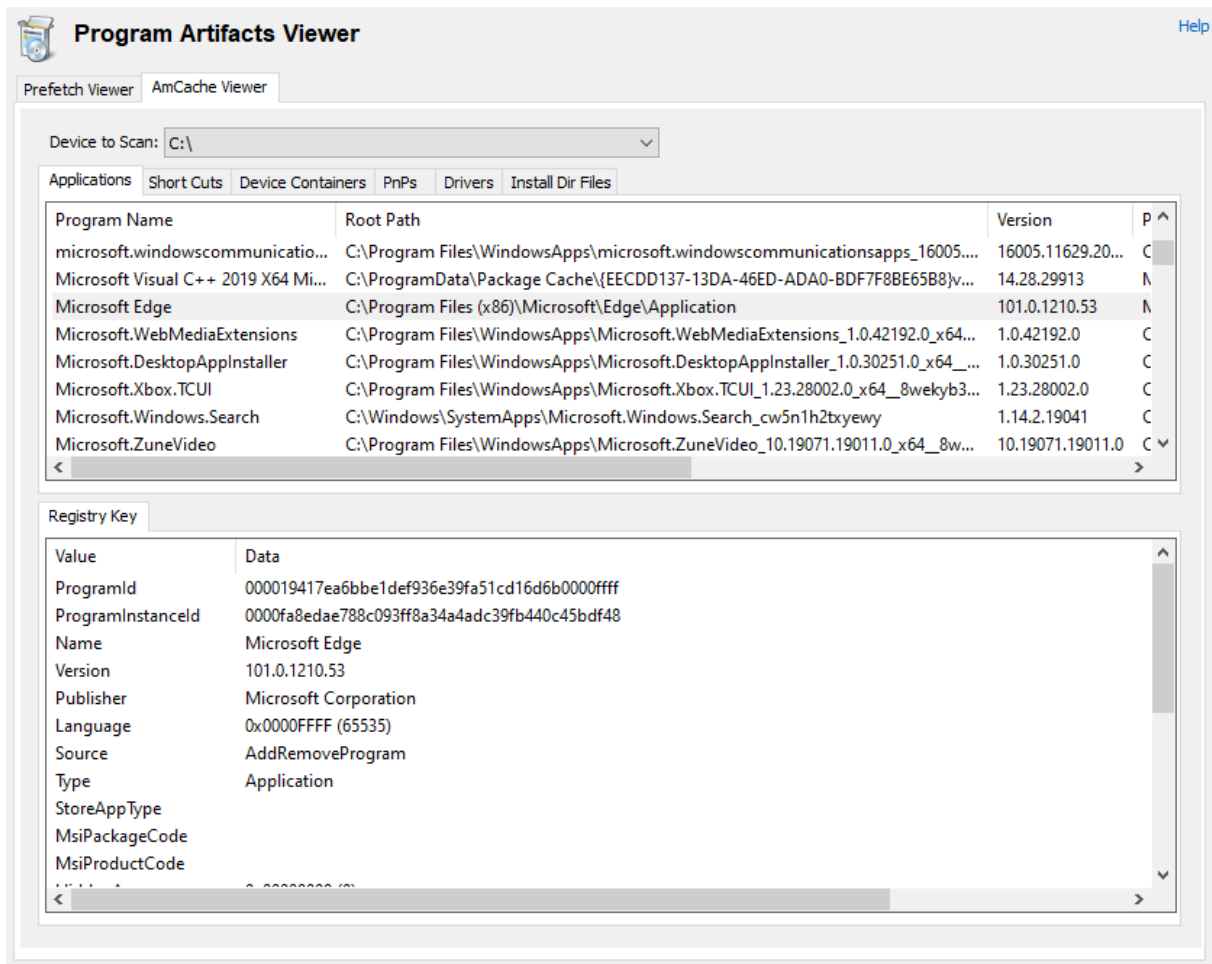
Mapped Directories



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.

5.25.2 AmCache Viewer

The AmCache Viewer module allows the user to view the potentially valuable forensic information stored in amcache registry hive. The AmCache hive stores metadata from programs installation and execution on Windows 7 and later machines. The AmCache hive keeps artifacts related to applications such as timestamps of creation and last modification of any application; name, description, publisher name and version of applications; execution file path, SHA-1 hash of executable files etc. These artifacts may persist even after the applications have been deleted from the system. The default location of the AmCache hive can be found on the system drive <system drive>:
 \Windows\appcompat\Programs\Amcache.hve.



Applications

Contains metadata about EXEs if they are shimmed or executed and have a GUI or if they are in scanned directories. It also records metadata about EXE and SYS files if they were created on the system following a program installation.

Shortcuts

List LNK files found on the computer.

Device Containers

List of physical devices that were plugged into the system.

PnPs

List of plug and play devices that were plugged into the system.

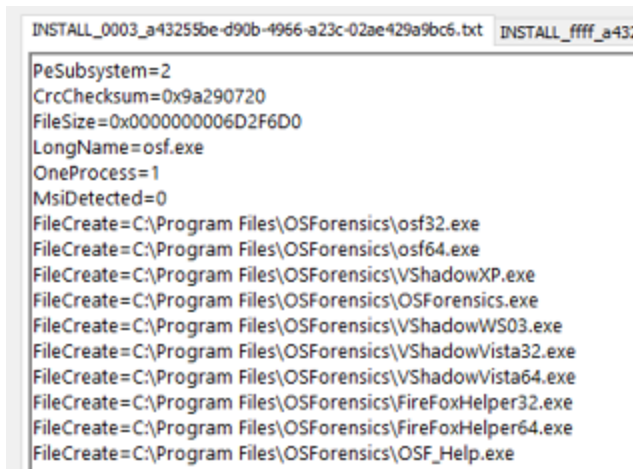
Drivers

Contains metadata about driver files installed on the system.

Install Dir Files

List contains files found in the <system drive>\Windows\appcompat\Programs\Install directory. This folder contains TXT files that records the installation of some programs, it is unknown why some

programs do not have text file created. For setups that may install multiple EXE installed, a file is created for each whose filenames respectively starts with INSTALL_0000, INSTALL_0001 and INSTALL_#### and one main file, INSTALL_ffff. These files list a wealth of information such as all the files that were installed along with the program. A tab is created for each #### file.



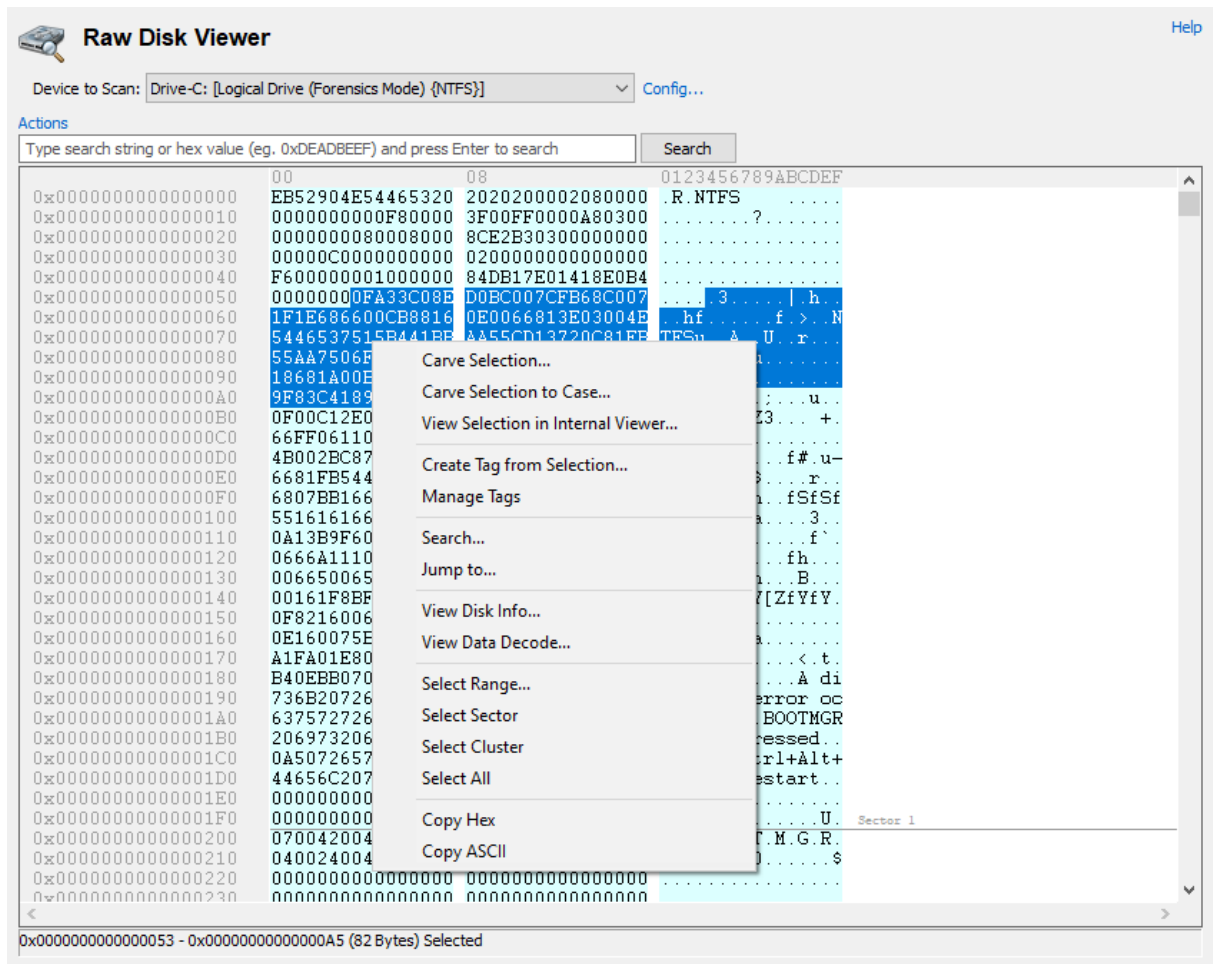
```
INSTALL_0003_a43255be-d90b-4966-a23c-02ae429a9bc6.txt  INSTALL_ffff_a43:
PeSubsystem=2
CrcChecksum=0x9a290720
FileSize=0x0000000006D2F6D0
LongName=osf.exe
OneProcess=1
MsiDetected=0
FileCreate=C:\Program Files\OSForensics\osf32.exe
FileCreate=C:\Program Files\OSForensics\osf64.exe
FileCreate=C:\Program Files\OSForensics\VShadowXP.exe
FileCreate=C:\Program Files\OSForensics\OSForensics.exe
FileCreate=C:\Program Files\OSForensics\VShadowWS03.exe
FileCreate=C:\Program Files\OSForensics\VShadowVista32.exe
FileCreate=C:\Program Files\OSForensics\VShadowVista64.exe
FileCreate=C:\Program Files\OSForensics\FireFoxHelper32.exe
FileCreate=C:\Program Files\OSForensics\FireFoxHelper64.exe
FileCreate=C:\Program Files\OSForensics\OSF_Help.exe
```

Registry Key

After selecting an entry in the list (Applications, Device Containers, PnPs or Drivers), the corresponding registry key values are displayed.

5.26 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).

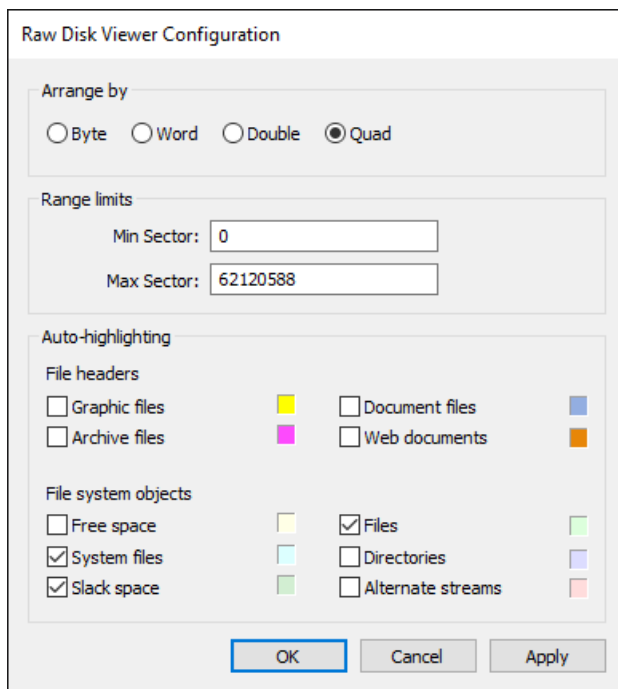


To view the raw sectors of a drive, the user selects the device from the *Device to scan* drop-down box.

Recovered partitions, if found on the disk, can also be selected.

Config ...

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



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)

Actions / Right Click Menu

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.

Create tag from selection...

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

Manage tags

Opens the tag window for managing the tags on the drive

Search...

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

Jump to ...

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

The screenshot shows a dialog box titled "Jump to". On the left, there are four radio button options: "Offset" (which is selected), "Partition", "File", and "File Records". The "Offset" section contains a text input field, three radio buttons for "Byte" (selected), "Sector", and "LCN", and two radio buttons for "Decimal" (selected) and "Hex". Below these is a "From:" dropdown menu with "Beginning" selected. The "Partition" section has a "Disk:" dropdown menu. The "File" section has a text input field and a browse button (...). The "File Records" section has a text input field. At the bottom of the dialog are "OK" and "Cancel" buttons.

Offset - Jump to the specified byte, sector, or logical cluster number (LCN) offset.

From - Specifies where (beginning of disk, current position or end of disk) to jump from when selecting byte or sector offset. A negative value (eg. -4096 in Dec., or -1F84 in Hex) will jump backwards from the current *Jump From* selection.

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

File Record - (Valid file systems only) Jump to the file record structure of the specified file on the partition (eg. MFT record for NTFS file systems)

View disk info...

Opens a separate disk info window for displaying information about the current device.

View data decode ...

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

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

Copy Hex

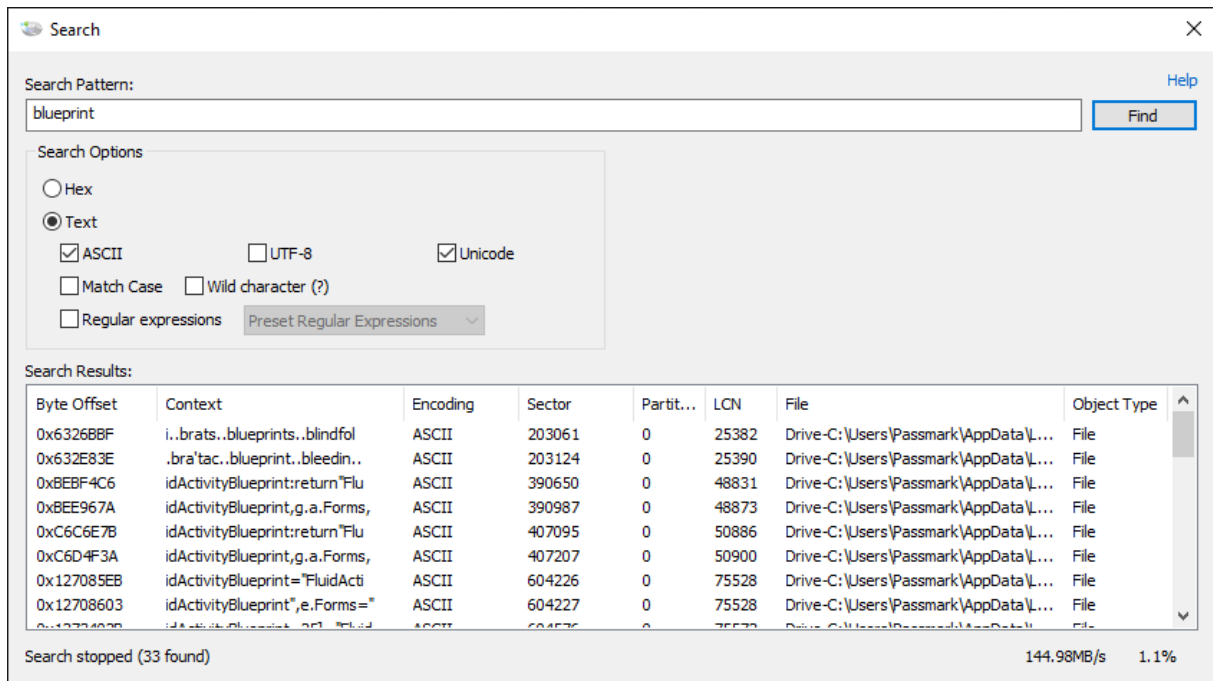
Copy the selected bytes as hex characters to clipboard

Copy ASCII

Copy the selected bytes as ASCII to clipboard

5.26.1 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

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 - one 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)

5.26.1.1 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.

NOTE: The regular expression option for Precognitive Search in the Indexing module uses a different syntax.

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
----	---------------

<code>\B</code>	not a word boundary
<code>^</code>	start of subject
<code>\A</code>	start of subject
<code>\$</code>	end of subject; also before newline at end of subject
<code>\Z</code>	end of subject; also before newline at end of subject
<code>\z</code>	end of subject
<code>\G</code>	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

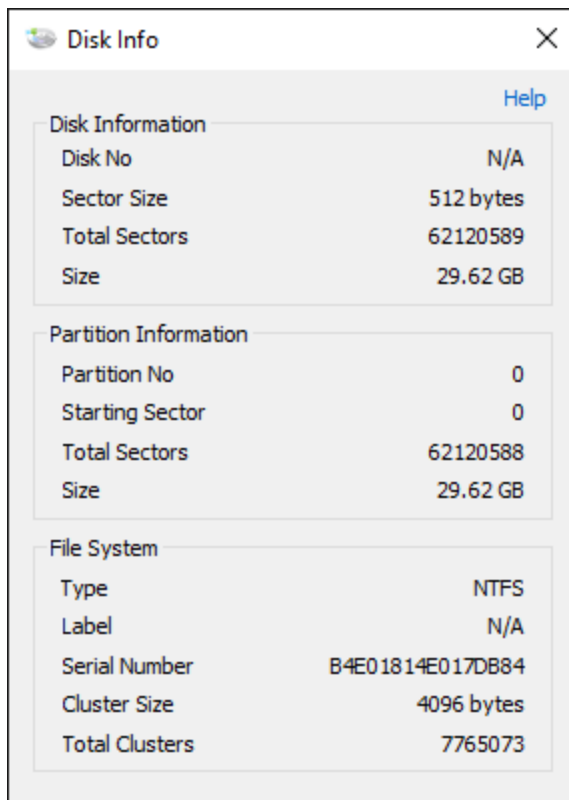
Non-Matches

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

5.26.2 Disk Info

The Raw Disk Viewer disk info window provides detailed information about the selected device.

Main Window



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

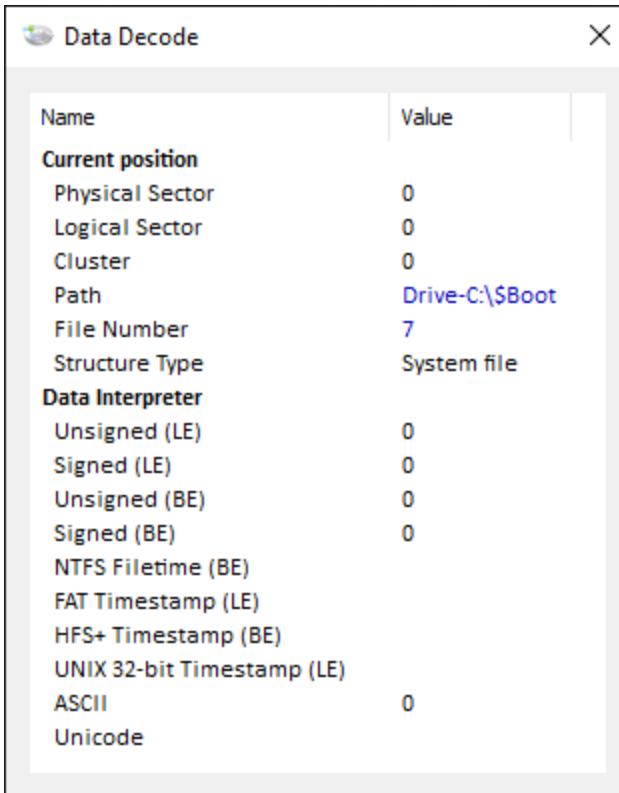
The size of each cluster in bytes

Total Clusters

The total number of clusters in the volume

5.26.3 Data Decode Window

The Raw Disk Viewer data decode window provides 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.



Name	Value
Current position	
Physical Sector	0
Logical Sector	0
Cluster	0
Path	Drive-C:\\$Boot
File Number	7
Structure Type	System file
Data Interpreter	
Unsigned (LE)	0
Signed (LE)	0
Unsigned (BE)	0
Signed (BE)	0
NTFS Filetime (BE)	
FAT Timestamp (LE)	
HFS+ Timestamp (BE)	
UNIX 32-bit Timestamp (LE)	
ASCII	0
Unicode	

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

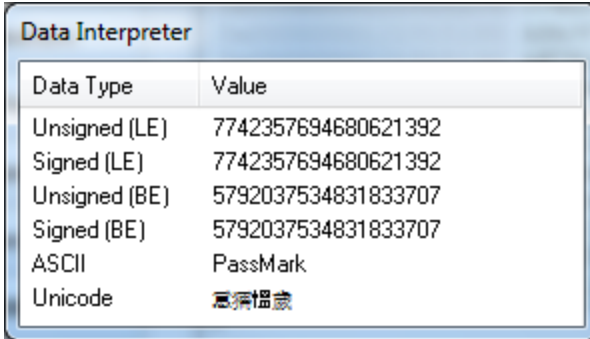
Any particular property of the allocated space that contains the current offset. (Eg. File, directory, free space, slack space)

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 Type	Value
Unsigned (LE)	7742357694680621392
Signed (LE)	7742357694680621392
Unsigned (BE)	5792037534831833707
Signed (BE)	5792037534831833707
ASCII	PassMark
Unicode	密码标志

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

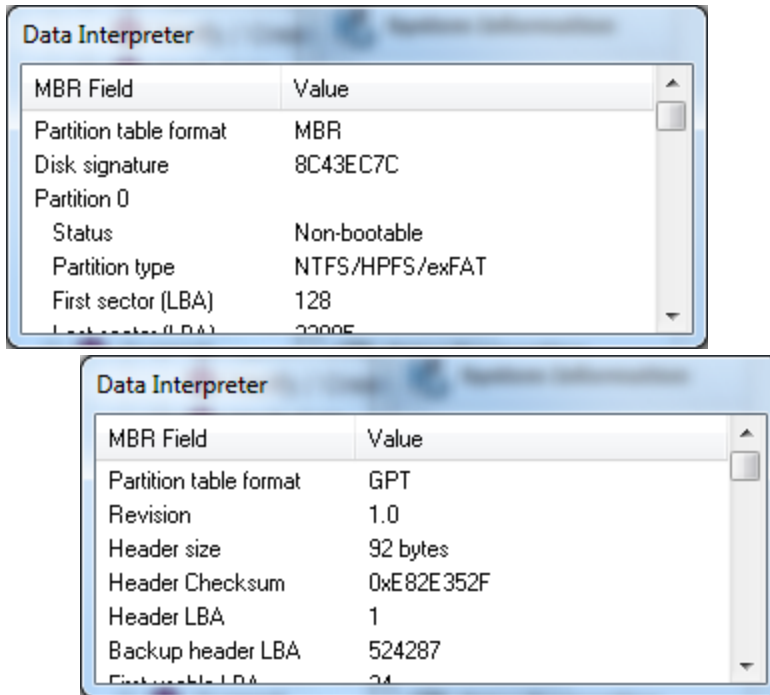
The selected bytes interpreted as ASCII-encoded text. Note that this information is available only if 1-32 bytes are selected.

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

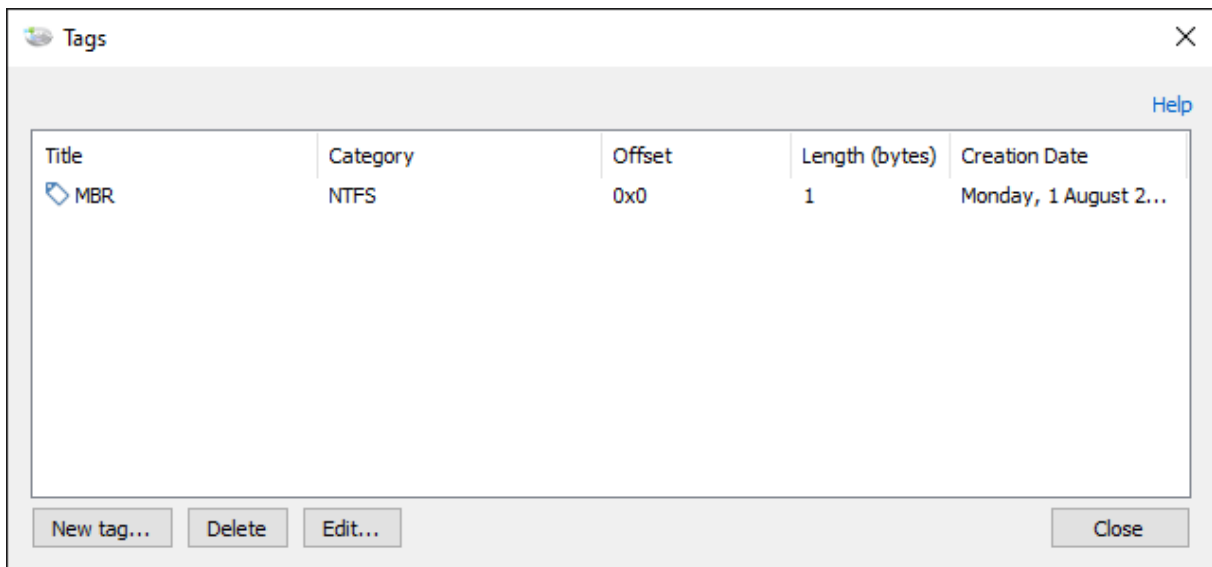
This mode is automatically enabled when the current offset is within the first sector of a physical disk (ie. MBR). The partition table (MBR or GPT) is displayed in a human-readable format.



Double-clicking on a LBA field will jump to the appropriate offset in the disk viewer.

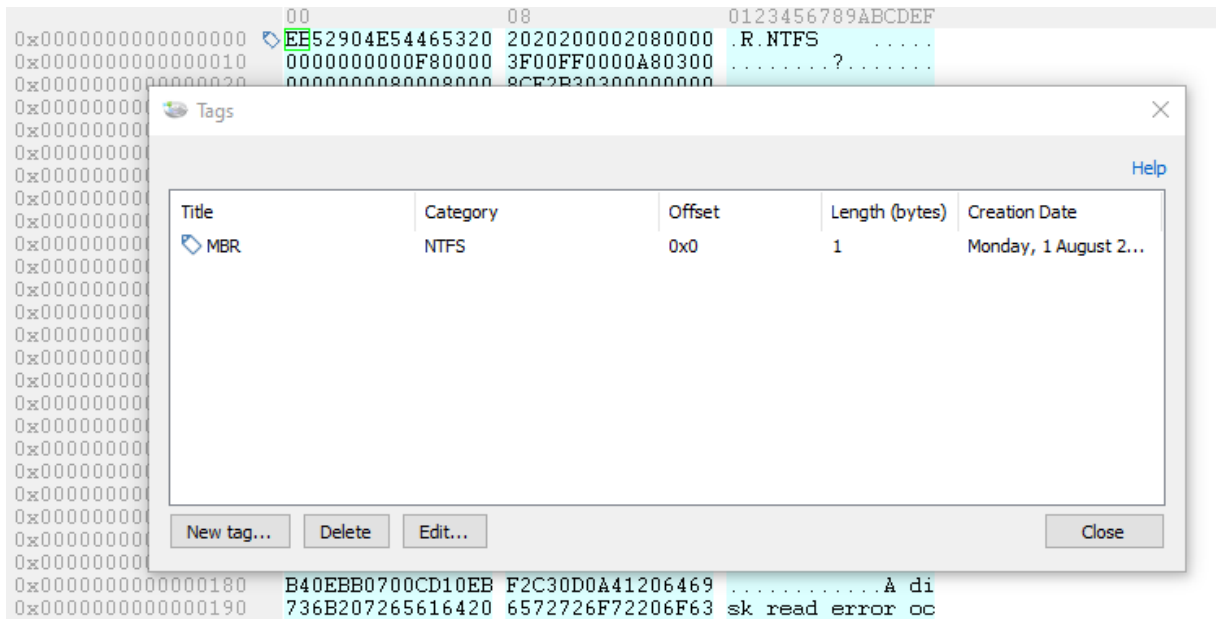
5.26.4 Tag Window

The Raw Disk Viewer tag window allows the user to manage the tagged offsets on the selected device.



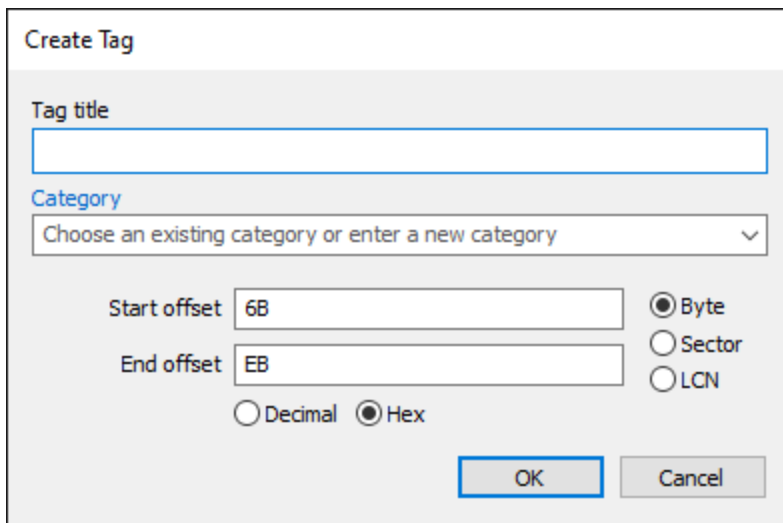
The details of all tags visible on the raw disk viewer is displayed in the list.

Tags are useful for marking offset ranges of interest on the drive so that it is readily accessible at any time. tags are indicated by a tag icon, and square brackets to mark the beginning and end of the tag.



New Tag

Opens a dialog for specifying the properties of a new tag.



Tag name - The name of the tag

Start offset - The starting offset of the tag

End offset - The ending offset of the tag

Delete

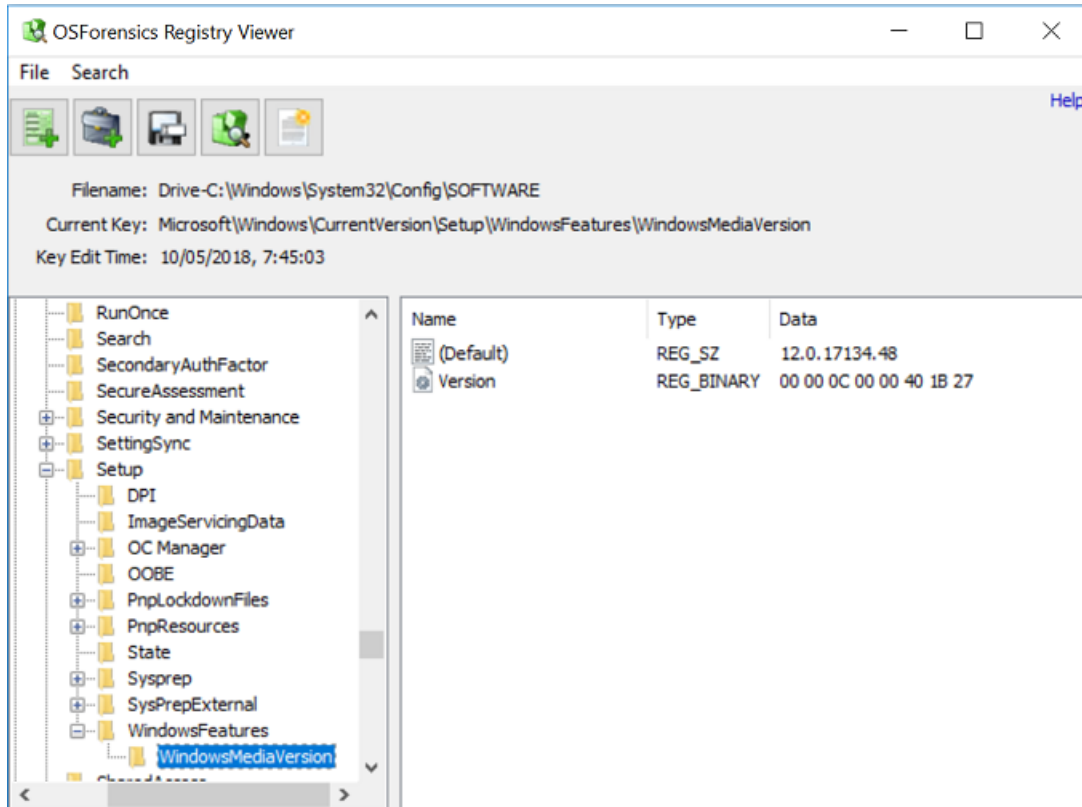
Delete the selected tag.

Edit ...

Change an existing tag's name and/or type.

5.27 Registry Viewer

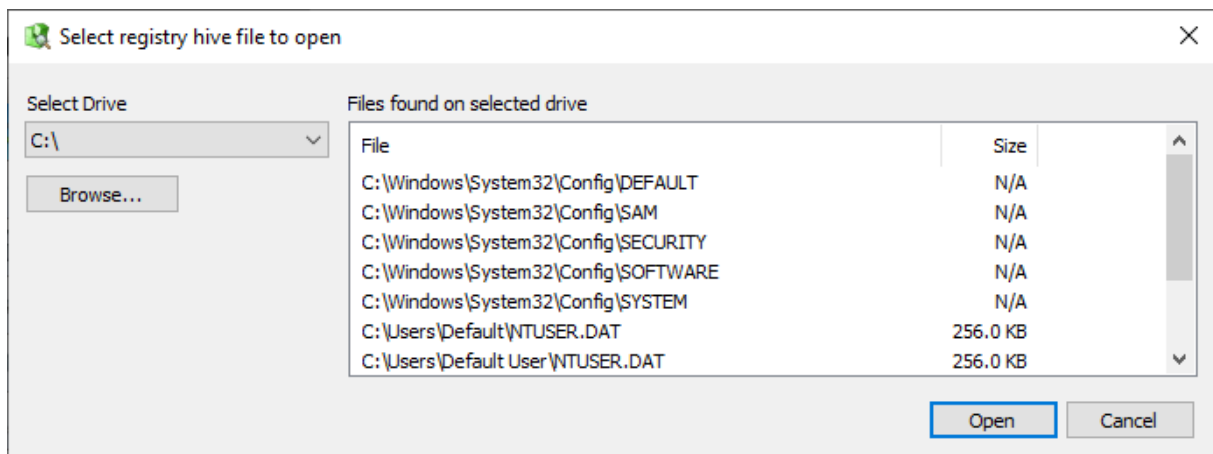
OSForensics includes a built in registry viewer to display the contents of registry hive files and has options to copy value names, data and to export registry keys and their sub keys to a text file.



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 or 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.

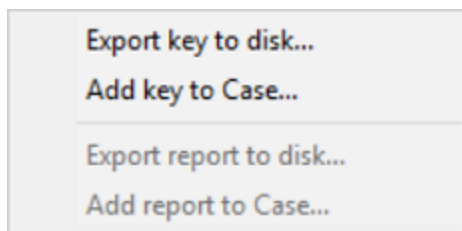


Usage

Right-click Menu

Registry Key Tree View

Right-clicking a registry key in the tree view brings up the following menu:



Export key to disk...

Save all values of the selected key as a CSV/HTML list

Add key to Case...

Save all values of the selected key as a CSV/HTML list and add to the case

Export report to disk...

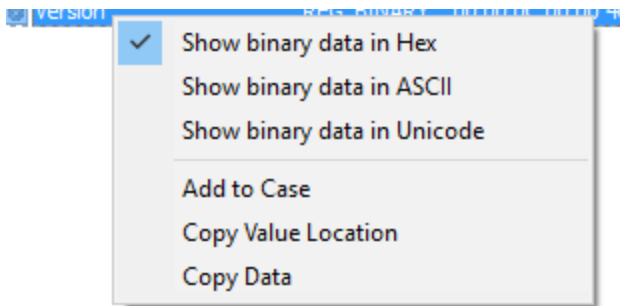
Generate a CSV/HTML report of the selected registry hive. Supported registry hives include SOFTWARE, SYSTEM, SAM, and NTUSER.dat.

Add report to Case...

Save a CSV/HTML report of the selected registry hive to the case. Supported registry hives include SOFTWARE, SYSTEM, SAM, and NTUSER.dat.

Registry Key Values List View

Right-clicking a registry key value in the list view 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

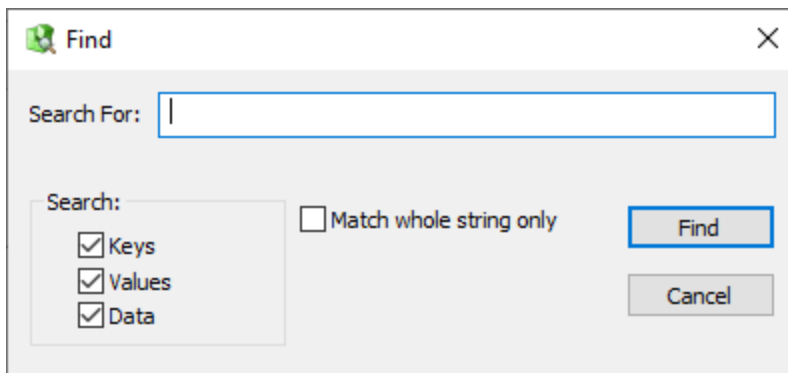
Copy the selected registry value location to clipboard

Copy Data

Copy the selected registry value data to clipboard

Search

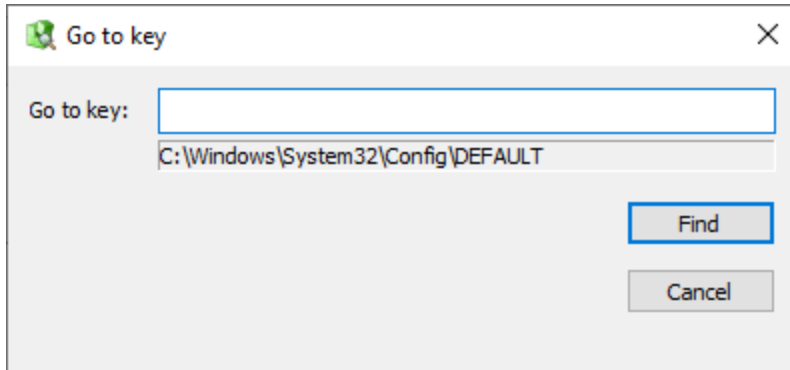
To search for a string pattern in the registry, open the 'Search' menu and select 'Find...'. In the dialog (as shown below), you can specify a search term, whether keys, values and/or data are matched, and whether the whole search string must be matched.



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

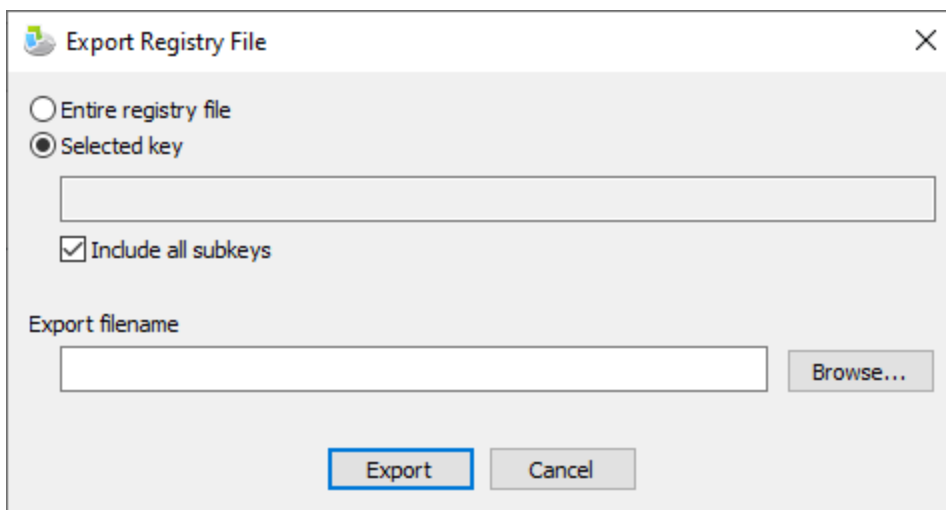
Go to Key

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.



Exporting

To export a registry key, or entire file, open the "File" menu and select the "Export to text..." option.



Exporting a registry key

5.28 Remote Acquisition

Remote Acquisition refers to the process of collecting forensics artifacts from machines connected to the network, without the need to perform manual, on-site live acquisition. The ability to perform simultaneous collection of digital evidence over the network greatly reduces the investigation time over offline methods.

OSForensics provides a step-by-step module to initiate simultaneous Auto Triage operations on remote machines.

Remote Acquisition Help

Load/Save ▼

Step 1: Install OSForensics to shared network drive (or pick location of existing install)

Network Path:

Step 2: Configure Auto Triage options

Default options Custom options (Config...)

Scan options

- Process List
- Physical Memory Dump
- User Activity Scan
- Password/Login Scan
- System Information
- File Listing
- List of Deleted Files

Step 3: Enter Remote PC credentials

Machine name/IP: Domain (optional): Username: Password (optional):

Use local account credentials

Remote PC	Domain	Username	Password	Status
REMOTEPC1		<Local account>	<Local account>	Idle
REMOTEPC2		passmark	*****	Idle
REMOTEPC3	domain	passmark	*****	Idle

Step 1: Install OSForensics to shared network drive

To enable acquisition of forensics artifacts on remote machines, a network install of OSForensics Portable must be accessible on the remote machine.

Once a network share is enabled, browse to the network path of where OSForensics Portable shall be installed. Click 'Install' to Install OSForensics Portable.

Step 2: Configure Auto Triage options

The types of forensics artifacts to be collected on remote machines can be configured in this step.

To collect a default set of forensics artifacts, select 'Default options'. Otherwise, select 'Custom options' then click on 'Config...' to configure Auto Triage Options.

Step 3: Enter Remote PC credentials

Next, enter the list of remote machines that collection of forensics artifacts shall be performed on.

Machine name/IP

Name of IP address of the Windows machine accessible on the network. Omit the initial backslashes (eg. \\REMOTEP1) from the input.

Domain

Domain where the machine is located in. This field can be omitted if the machine does not belong in a domain.

Note - Machines not belonging to a domain will require specific registry permissions to be enabled. See Troubleshooting Connection Issues for instructions.

Username

The user name of an account with Administrator access on the machine

Password

The password associated with the account (if set).

Use local account credentials

Use the current user on the local machine's credentials (ie. the user session currently running OSForensics) to access the remote machine.

Step 4: Press Acquire to initiate Remote Acquisition

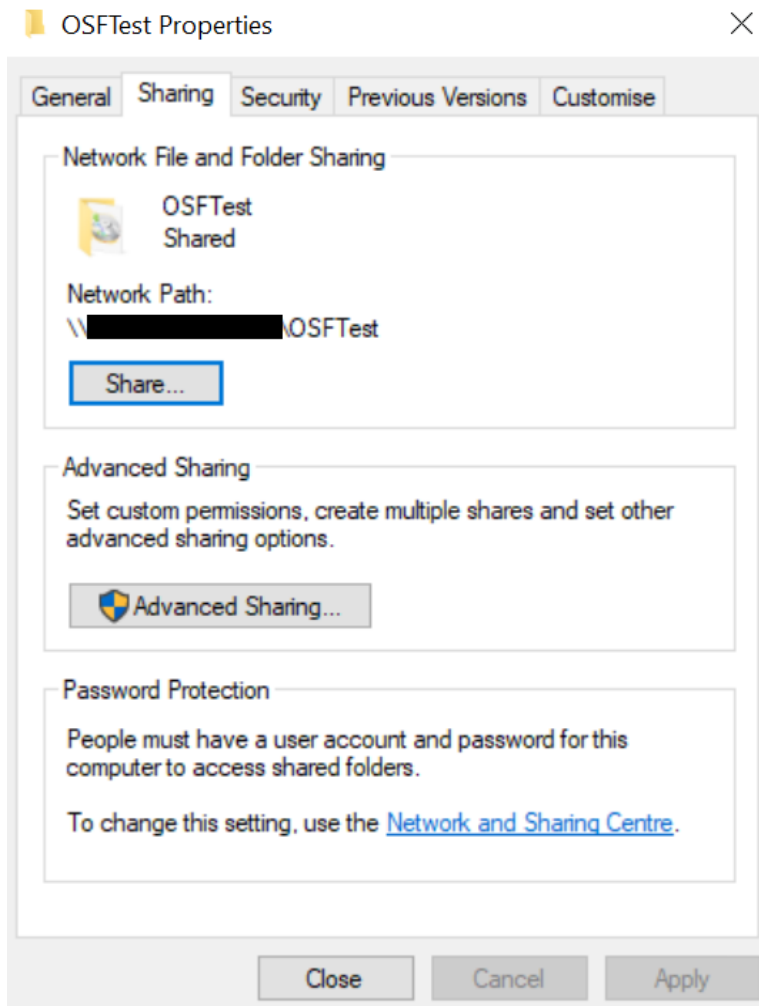
To troubleshoot connection or permission issues, See Troubleshooting Connection Issues.

5.28.1 Network Drive Setup

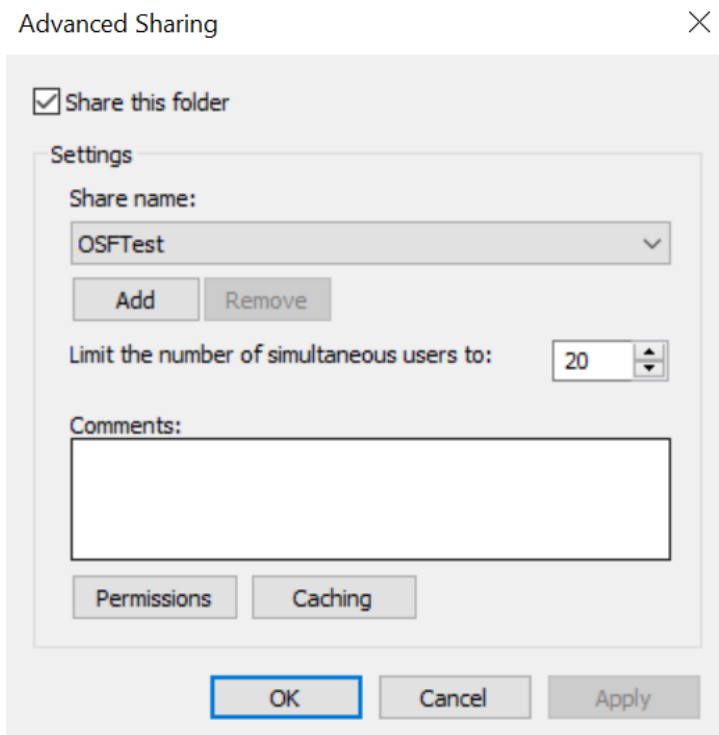
There are several methods to create a shared network drive, some methods include:

Shared folder

Create a new folder on the machine to host the shared folder, then right-click and go to 'Properties' and to the 'Sharing' tab.



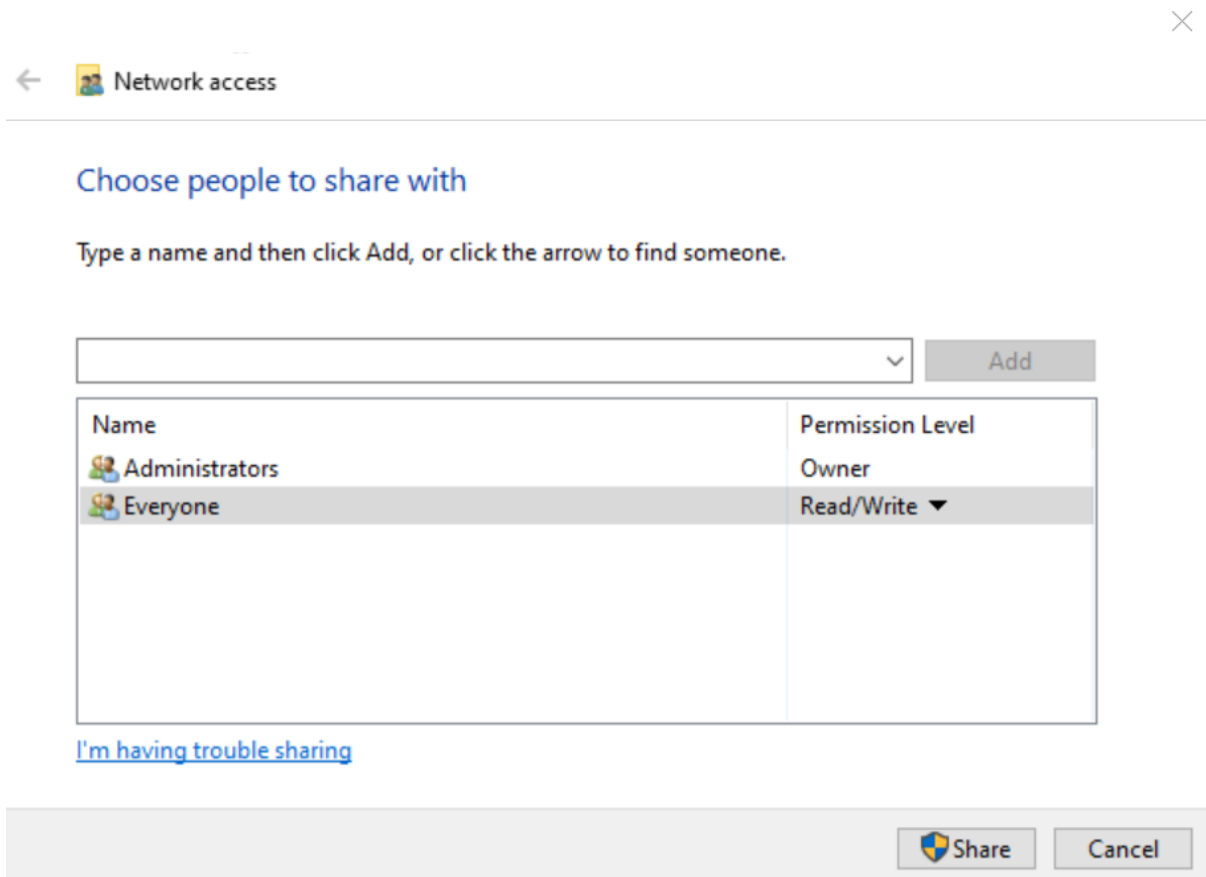
Then click on 'Advanced Sharing...' then check 'Share this folder'



Click 'OK' then 'Close'. Then go to the machine to be remote into and check that the folder being shared can be accessed.

Enter credentials for host of the shared folder if required.

You can also change the share so everyone can access without credentials by going to the above properties window and click on 'Share...' to open the Network Access window:



And in the drop-down menu, select 'Everyone', and 'Add'. Then change the Permission Level to 'Read/Write' using the down arrow in the same column.

Network-attached storage (NAS)

If you have a NAS, you can create a network folder/drive following the instructions provided by the manufacturer and make sure that both the host and remote machines can access the folder.

5.28.2 Troubleshooting Connection Issues

I get an error when my login credentials does not require a password

For security reasons, Windows does not allow remote access with a blank password by default, even if it is permitted when logging in locally.

The obvious workaround is to set a password for the account. Otherwise, this security setting can be disabled as follows:

1. Press Windows+R to open the "Run" box. Type gpedit.msc, and then press ENTER
2. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**
3. Change **Accounts: Limit local accounts use of blank passwords to console logon only** to **Disabled**

I get an "Access Denied" error even though my login credentials are correct

This may occur if the remote machine is not under a domain. In Windows Vista or newer, User Account Control (UAC) restricts remote access using an account from the local Administrators group. This is a security mechanism which prevents remote attacks from malicious parties with login credentials for a local Administrative account. This mechanism is described in further detail in the following article: [User Account Control and remote restrictions - Windows Server | Microsoft Docs](#)

UAC restrictions do not apply if it is a domain user with Administrative access.

To disable UAC restrictions on the remote machine, the following steps need to be performed:

4. Press Windows+R to open the "Run" box. Type regedit, and then press ENTER
5. Navigate to the following registry key

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

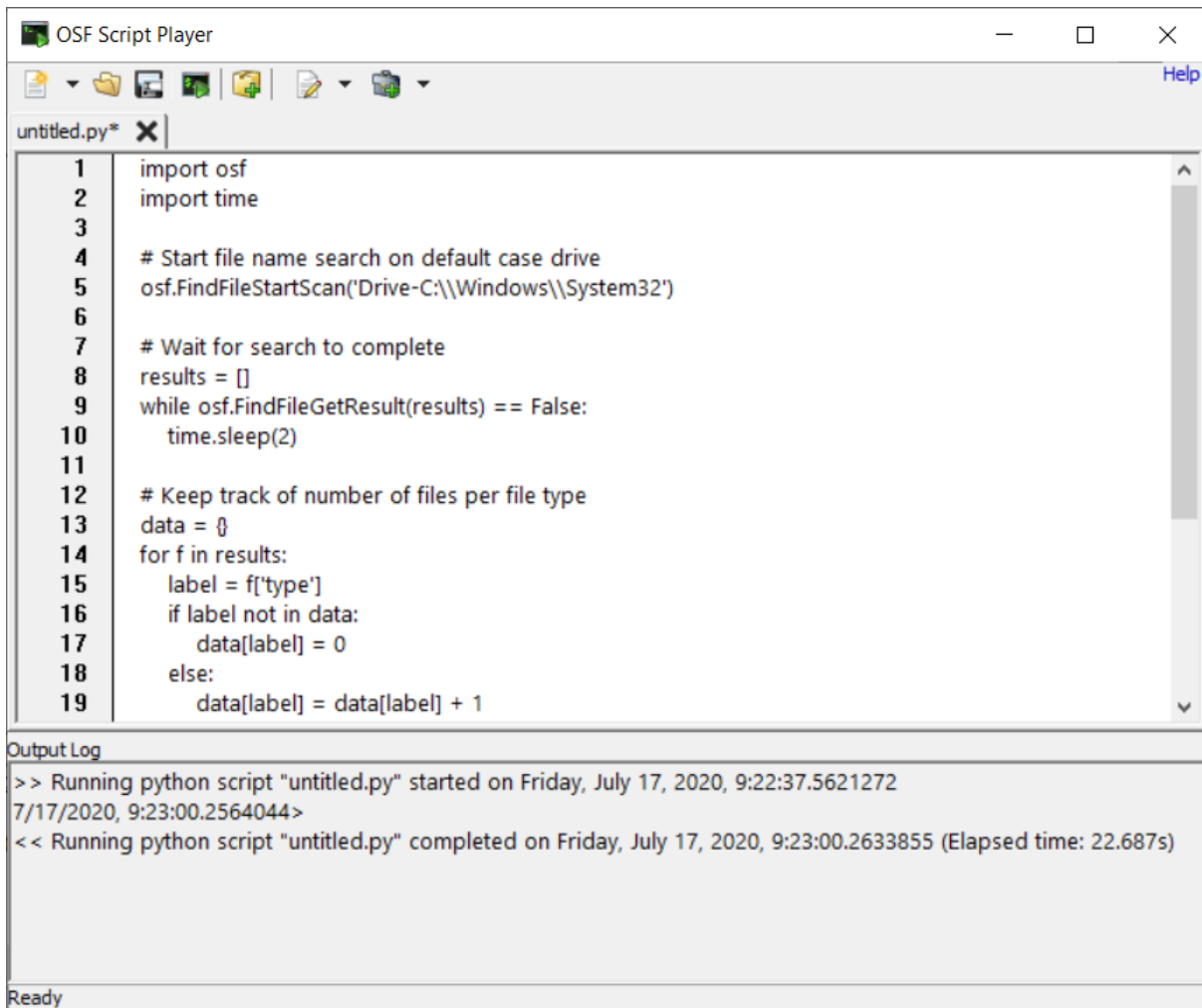
6. Locate the **LocalAccountTokenFilterPolicy** registry entry. If it doesn't exist, create one by opening the right-click menu and selecting **New > DWORD (32-bit) Value**
7. Double click **LocalAccountTokenFilterPolicy** to modify the value
8. Type **1** in the Value data field
9. Exit Registry Editor

I see the remote machine under Network but get "Remote PC not found" error

Remote Acquisition requires **File and Printer Sharing** to be enabled. This can be found under **Network and Sharing Center > Advanced sharing** settings.

5.29 Script Player

To support workflow automation of common or complex forensic tasks, scripts can be developed and executed in the Script Player to automate OSForensics discovery and analysis tasks. By developing and maintaining scripts as part of the forensics workflow, standard tasks and procedures can be repeated by any investigator in order to boost efficiency, minimize human error and reduce training costs. Scripts are written using the Python language, and can access OSForensics analysis via the OSForensics Python API implemented as a Python module.



The screenshot shows the OSF Script Player application window. The title bar reads "OSF Script Player" and includes standard window controls (minimize, maximize, close) and a "Help" button. Below the title bar is a toolbar with icons for file operations. The main area displays a Python script named "untitled.py" with the following code:

```
1 import osf
2 import time
3
4 # Start file name search on default case drive
5 osf.FindFileStartScan('Drive-C:\\Windows\\System32')
6
7 # Wait for search to complete
8 results = []
9 while osf.FindFileGetResult(results) == False:
10     time.sleep(2)
11
12 # Keep track of number of files per file type
13 data = {}
14 for f in results:
15     label = f['type']
16     if label not in data:
17         data[label] = 0
18     else:
19         data[label] = data[label] + 1
```

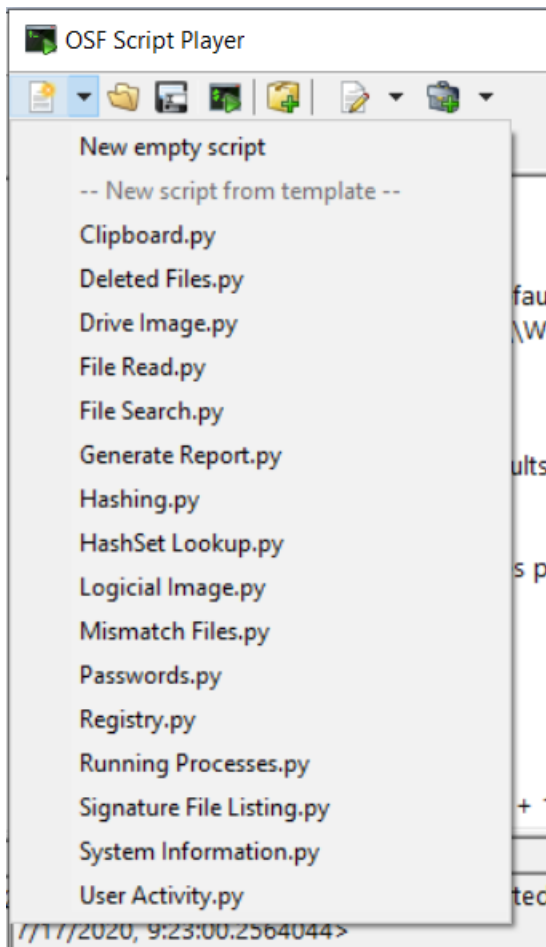
Below the script editor is an "Output Log" section showing the execution details:

```
>> Running python script "untitled.py" started on Friday, July 17, 2020, 9:22:37.5621272
7/17/2020, 9:23:00.2564044>
<< Running python script "untitled.py" completed on Friday, July 17, 2020, 9:23:00.2633855 (Elapsed time: 22.687s)
```

The status bar at the bottom of the window displays "Ready".

Getting Started

To start developing scripts, click on the 'New Script' icon to open a new tab with a blank script template, or click on the drop-down button to select a built-in template script.



The built-in template scripts provide a starting point for using OSForensics Python API, which can be extended to building more sophisticated scripts

An existing script can also be opened by clicking on the 'Open Script' icon.

Scripts are written in the Python language, which access the OSForensics functionality via the provided `osf` Python module. This module defines a list of methods that allows forensic tasks to be performed without needing to manually perform the operation using the GUI. These methods can be called within your scripts, allowing the returned data to be manipulated further by importing built-in or 3rd party Python packages. For example, Python AI packages can be used to train image recognition models using the images returned from an OSForensics File Search.

See the Python API Reference for code examples.

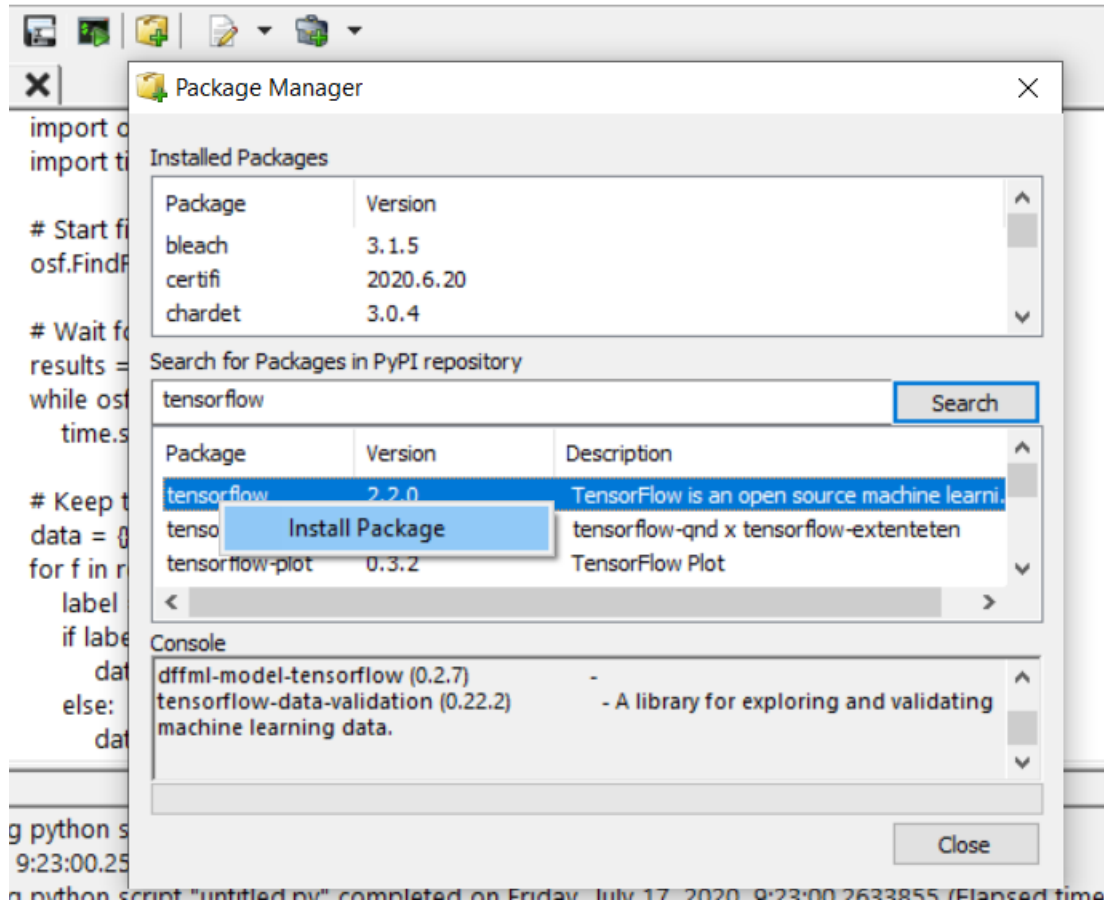
Running Scripts

Once the script is ready to be executed, click on the 'Run Script' icon. The output of the script execution, including syntax errors, is shown in the Output window.

To export or save the output to the case, click on the 'Export output to file' or 'Add output to case' icons, respectively.

Installing Packages

Importing 3rd party Python packages requires installation via a Python package manager (pip). Click on the 'Package' icon to open the Package Manager.



To search or install a Python package, enter the (partial) name of the package and click 'Search'. Right-click the desired package and select 'Install Package'.

To remove or upgrade a package, right-click the package under 'Installed Packages' and select 'Remove Package' or 'Upgrade Package' respectively.

5.29.1 Python API Reference

See Python API for OSForensics for API specifications.

5.30 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.

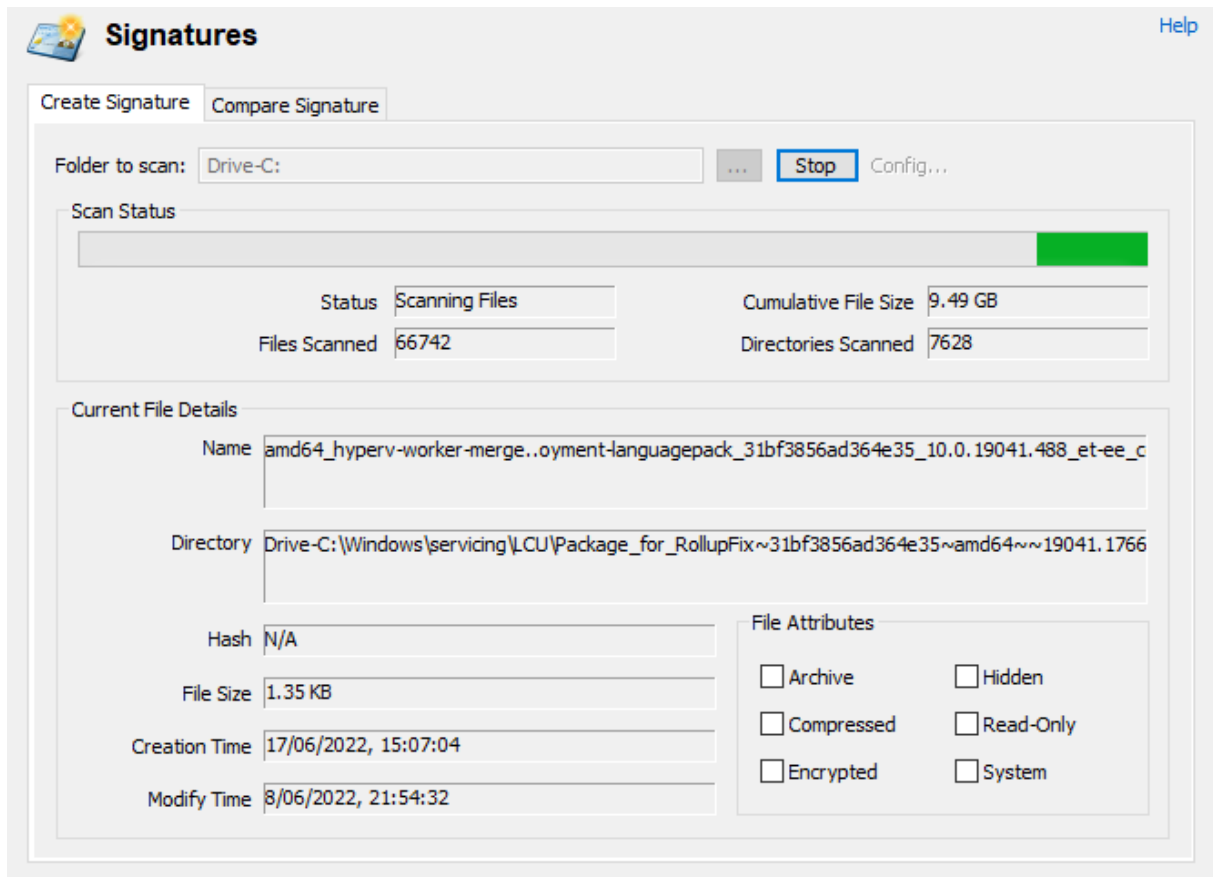
Other Uses

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.

5.30.1 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.



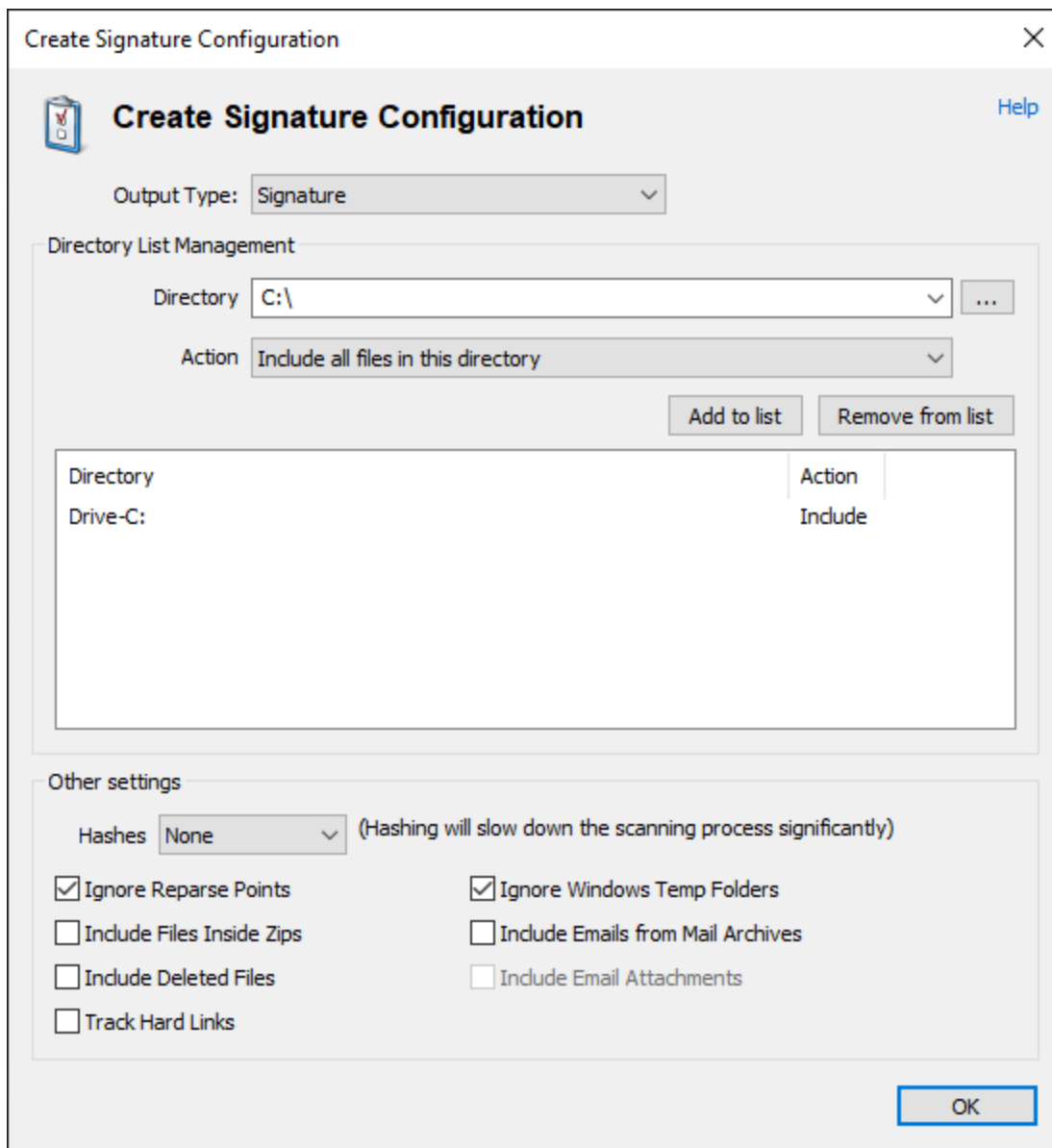
A signature can be created using the default options by simply specifying a starting directory and clicking the *Start* button. Advanced options for signature generation can be found by clicking the *Config...* link to open the Create Signature Configuration Window.

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.

5.30.1.1 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.



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 Hashes

Check this box to calculate an SHA1 or MD5 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\Index  
er"  
"\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemInd  
ex\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 Deleted Files

Scan for deleted files (and \$I30 slack entries, for NTFS drives) and include the files in the signature file. Enabling this option will slow down the signature creation process.

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.

Track Hard Links

Selecting this option will have the signature creation function track hard links for each file. A hard link is the file system representation of a file by which more than one path references a single file on the same volume. When enabled, only the first encounter of file is added to the total file size. Subsequent

encounters of hard links to the file will not increase the total file size. Enabling this option will slow down the signature creation process. Only supported for folders on NTFS.

5.30.2 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.

The screenshot shows the 'Signatures' application window with the 'Compare Signature' tab selected. The 'Old Signature' and 'New Signature' fields both point to 'C:\Users\passmark\Desktop\drive-c-win.OSFsig'. Below these fields are 'Compare' and 'Config...' buttons. A table displays the results of the comparison, with columns for Name, Difference, Create, Modify, Size, and Attributes. The table lists various files and folders, including deleted files, repair files, and program files. At the bottom, a summary section provides totals for differences, new files, deleted files, modified files, and identical files, along with their respective sizes.

Name	Difference	Create	Modify	Size	Attributes
\\\$extend\\$\Deleted\001D000000...	New	5/7/2021, 10:59:46	8/18/2021, 16:31:02	24 Bytes	A.....
\\\$extend\\$\Deleted\002A000000...	New	9/11/2020, 19:29:35	8/18/2021, 16:31:02	7.24 KB	A.....
\\\$extend\\$\RmMetadata\\$\Repair	New	1/17/2018, 20:48:21	1/17/2018, 20:48:21	0 Bytes	A--H--S--
\\\$extend\\$\RmMetadata\\$\TxLog...	New	1/17/2018, 20:48:21	1/17/2018, 20:48:21	0 Bytes	A--H--S--
\\\$extend\\$\RmMetadata\\$\TxLog...	New	1/17/2018, 20:48:21	8/13/2021, 0:29:05	64.00 KB	A.....
\\\$extend\\$\RmMetadata\\$\TxLog...	New	8/12/2020, 18:17:11	8/13/2021, 0:29:05	10.00 MB	A.....
\\\$extend\\$\RmMetadata\\$\TxLog...	New	1/16/2021, 12:48:28	8/13/2021, 0:28:51	10.00 MB	A.....
\\Program Files (x86)\Common File...	Attributes Mod...	1/10/2018, 10:39:43	1/10/2018, 10:39:43	1.93 KB	A.....
\\Program Files (x86)\Common File...	Attributes Mod...	1/10/2018, 10:39:44	1/10/2018, 10:39:44	9.56 KB	A.....
\\Program Files (x86)\Common File...	Attributes Mod...	1/10/2018, 10:39:47	1/10/2018, 10:39:47	30 Bytes	A.....
\\Program Files (x86)\Common File...	Attributes Mod...	1/10/2018, 10:39:43	1/10/2018, 10:39:43	1.05 MB	A.....
\\Program Files (x86)\Common File...	Attributes Mod...	1/10/2018, 10:39:47	1/10/2018, 10:39:47	6.75 MB	A.....
\\Program Files (x86)\Common File...	Attributes Mod...	1/10/2018, 10:39:47	1/10/2018, 10:39:47	7.45 MB	A.....

Summary Statistics:

Total Differences:	271191	Total New:	23637	Total Deleted:	56633	Total Modified:	190921	Total Identical:	319937
Total Size Change:	2.01 GB	New Size:	3.05 GB	Deleted Size:	1.05 GB	Modified Size:	-3.73 MB	Identical Size:	105.3 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.

Clicking on the *Old Signature*/*New Signature* link opens the Signature Info window which displays the details of the corresponding signature file.

Compare

Click this button to perform the comparison between the signature files.

Config...

Open a configuration dialog which allows the user to adjust the signature comparison settings.

Filter

Filter the results by new, deleted, modified or identical files

Actions Menu

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 Deleted Files

Whether or not the signature creation process included deleted files (and \$I30 slack entries, for NTFS drives).

Include Files Inside Zips

Whether or not the signature creation process included files inside zip files.

Include Emails from Mail Archives / Include Email Attachments

Whether or not the signature creation process included emails and attachments from inside mail archives.

Track Hard Links

Whether or not the signature creation process tracked hard links. If hard links are tracked, only the first encounter of a file will be counted toward the file size and each subsequent encounter of the file will mark the file size as 0 to not increase the total file size count.

5.30.3 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.

Deleted File Hashes

Calculating hashes for the contents in deleted files is supported (except for \$I30 slack entries). However, be aware that the deleted file clusters may have been overwritten and/or allocated to another file causing the calculated hash to be different from the original file.

Large Zip Files

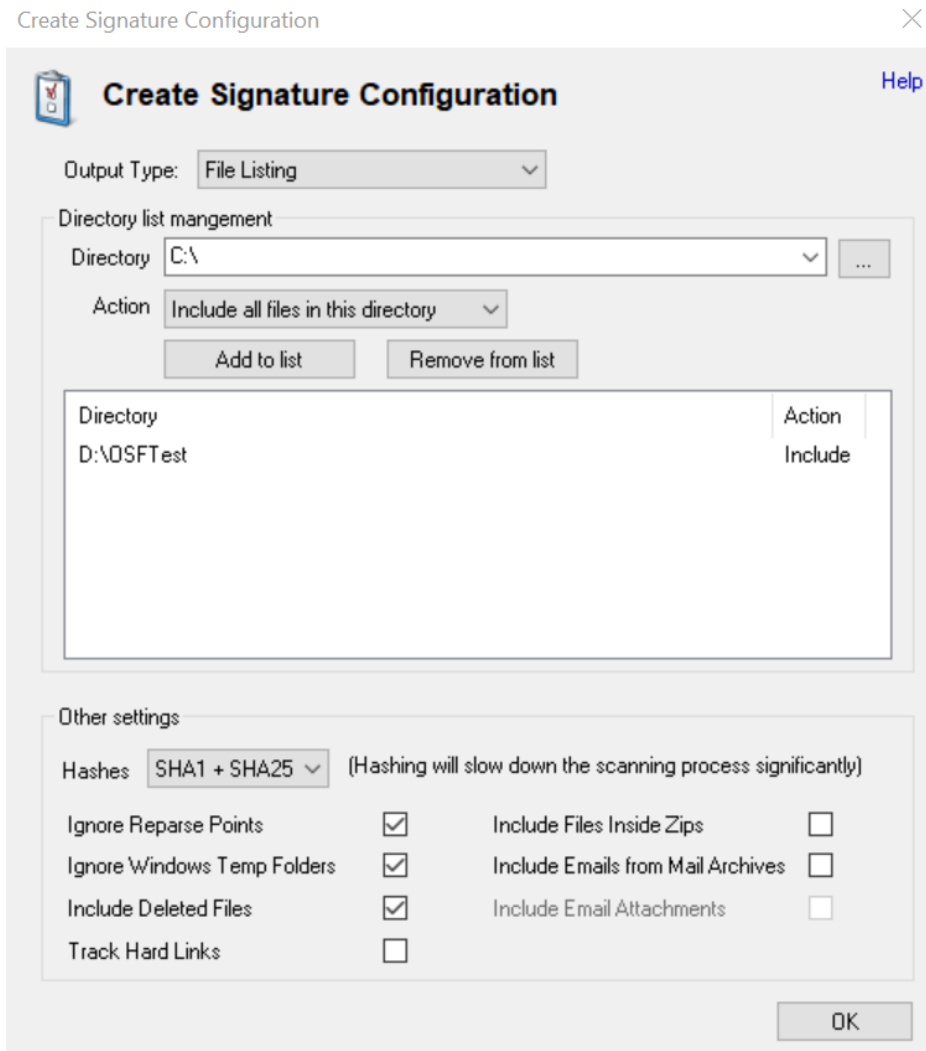
Zip archives greater than 4GB are not supported. Only the top level zip will be added to the signature, not any of the files within the zip.

Track Hard Links

Only supported for selected folders locations that resides on NTFS.

5.30.4 File Listing

You can also select File Listing in the Configuration window to export a list of files in CSV format. To do this, click on the 'Config...' link, and in the configuration window, expand the 'Output Type' dropdown and select 'File Listing'.



An example of a file listing CSV export:

ID	ParentID	Path	Create Date, Create Date	Create Time	Modify Date, Modify Date	Modify Time	Access Date/Tir	Access Date	Access Time	Attr. Modify Dat	Attr. Modify Date	Attr. Modify Size (bytes)	Attributes	Parent	Child		
0		Drive-C:\Intel\Logs\HDEVENT	1.3183E+17	10/2/2018	32:19.8	1.3183E+17	10/4/2018	13:13.6	1.32543E+17	1/4/2021	25:45.2	1.31832E+17	10/4/2018	13:13.6	40908 A	FALSE	FALSE
1		Drive-C:\Intel\Logs\IntelCPHS	1.3183E+17	10/2/2018	39:25.6	1.3183E+17	10/2/2018	39:25.6	1.3183E+17	10/2/2018	39:25.6	1.3183E+17	10/2/2018	39:25.6	0 A	FALSE	FALSE
2		Drive-C:\Intel\Logs\IntelGFX.N	1.3183E+17	10/2/2018	06:46.1	1.3183E+17	10/4/2018	07:35.6	1.32543E+17	1/4/2021	25:45.2	1.31832E+17	10/4/2018	07:35.6	113180 A	FALSE	FALSE
3		Drive-C:\\$AttrDef	1.3183E+17	10/2/2018	05:52.6	1.3183E+17	10/2/2018	05:52.6	1.3183E+17	10/2/2018	05:52.6	1.3183E+17	10/2/2018	05:52.6	2560 HS	FALSE	FALSE
4		Drive-C:\\$BadClus	1.3183E+17	10/2/2018	05:52.6	1.3183E+17	10/2/2018	05:52.6	1.3183E+17	10/2/2018	05:52.6	1.3183E+17	10/2/2018	05:52.6	0 HS	FALSE	FALSE
5		Drive-C:\\$Bitmap	1.3183E+17	10/2/2018	05:52.6	1.3183E+17	10/2/2018	05:52.6	1.3183E+17	10/2/2018	05:52.6	1.3183E+17	10/2/2018	05:52.6	7593792 HS	FALSE	FALSE
6		Drive-C:\\$Boot	1.3183E+17	10/2/2018	05:52.6	1.3183E+17	10/2/2018	05:52.6	1.3183E+17	10/2/2018	05:52.6	1.3183E+17	10/2/2018	05:52.6	8192 HS	FALSE	FALSE

ID

Unique identifier for each file

Parent ID

If files are part of a ZIP file, this field will be filled with the ZIP file's ID.

Path

Full path of where the file is located.

Create Date/Time

Microsoft FILETIME number for when file was created.

Create Date

Conversion of the above FILETIME number into a readable date.

Create Time

Conversion of the above FILETIME number into a readable time.

Modify Date/Time

Microsoft FILETIME number for when file was last modified.

Modify Date

Conversion of the above FILETIME number into a readable date.

Modify Time

Conversion of the above FILETIME number into a readable time.

Access Date/Time

Microsoft FILETIME number for when file was last accessed.

Access Date

Conversion of the above FILETIME number into a readable date.

Access Time

Conversion of the above FILETIME number into a readable time.

Attr. Modify Date/Time

Microsoft FILETIME number for when file attributes were last modified.

Attr. Modify Date

Conversion of the above FILETIME number into a readable date.

Attr. Modify Time

Conversion of the above FILETIME number into a readable time.

Size (bytes)

Size of the file in bytes.

Attributes

File attributes, e.g. Read-only, Hidden.

Hashes

This can be enabled in the configuration window, you can select up to two different hashes between SHA1, SHA256 and MD5.

Parent

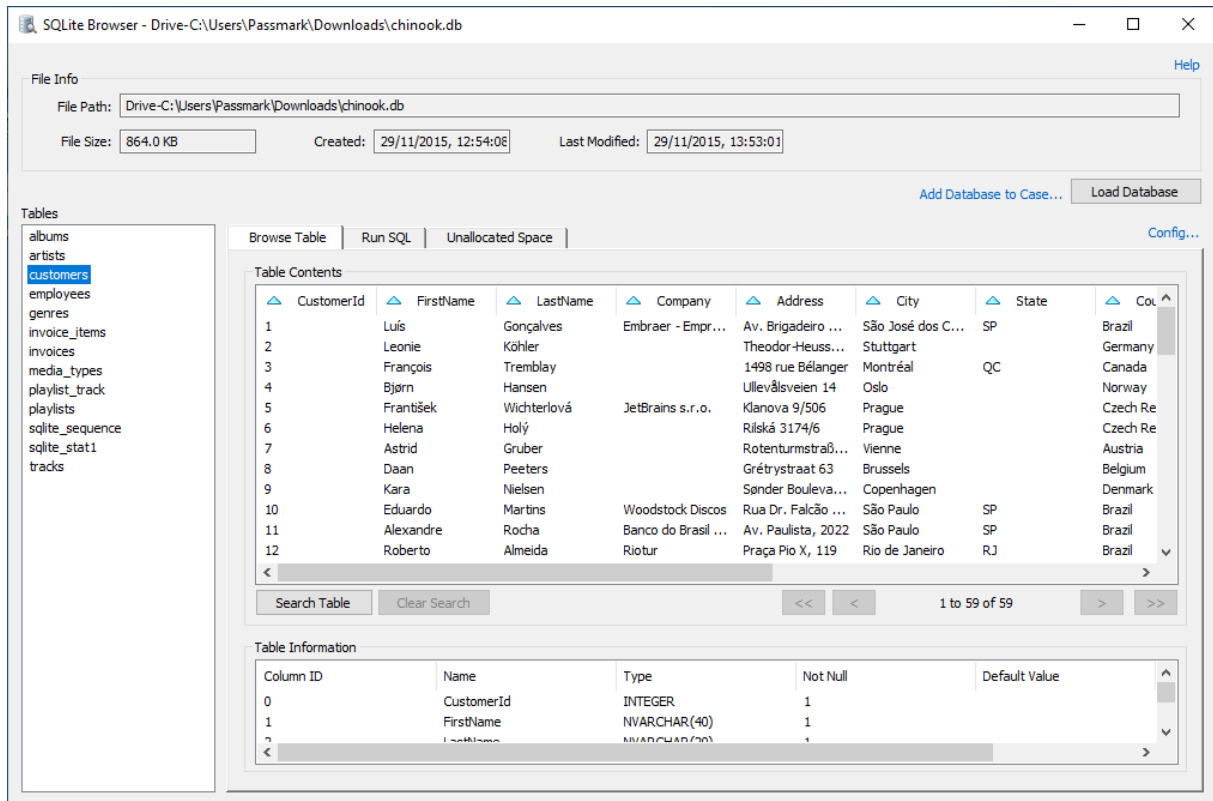
TRUE/FALSE - if file is a parent of child files.

Child

TRUE/FALSE - if file is child of a parent file.

5.31 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.

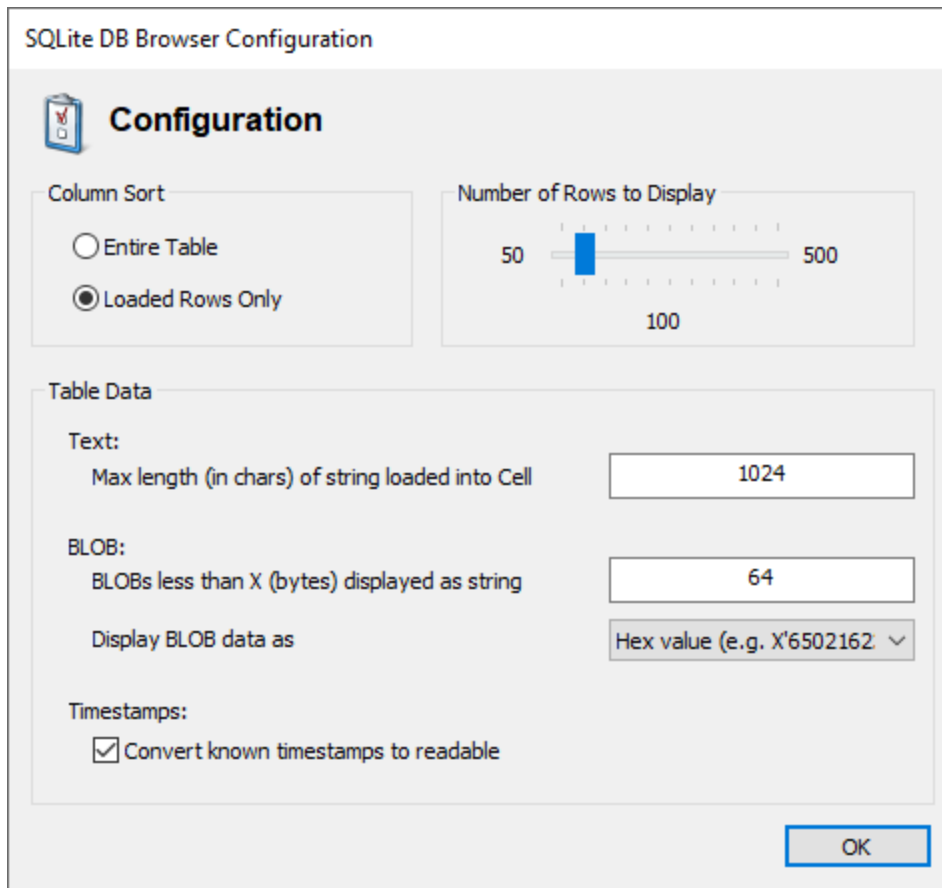


Load Database

Load a SQLite database file.

Config ...

Opens a dialog to configure the display settings of the module.



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.

Timestamps: Convert known timestamps to readable - Identified and known timestamps field will display the value as a readable string along with the original timestamp value, e.g. "9/14/2017, 13:07:17 (13149893237645538)"

Scan Folder

Scans a folder for possible SQLite database files. Selecting a file on the file list will open the database in the viewer.

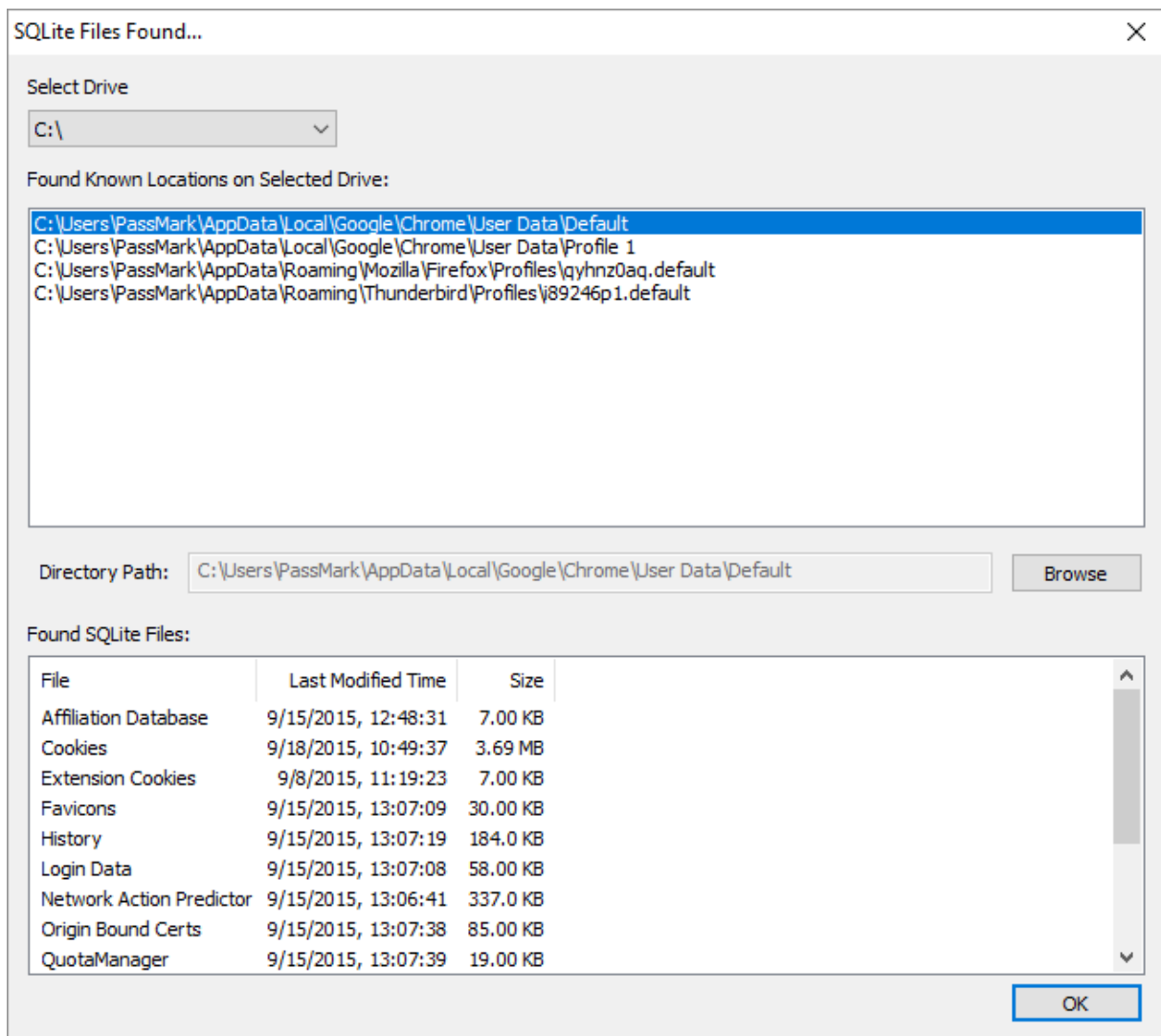


Table List

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

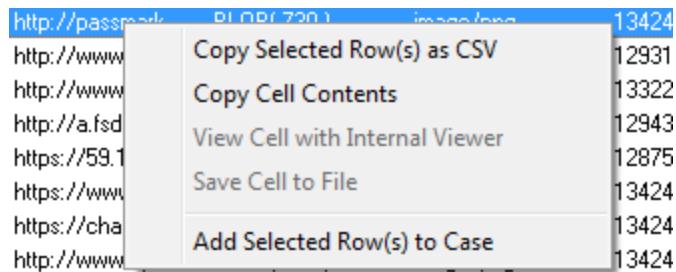
Opens a search window that allows users to perform custom queries on the current loaded table. The results will be updated in the result table.

Clear Search

This button will be enabled when a custom search has been performed. 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



http://passmark	BLOB(720)	image.png	13424
http://www			12931
http://www			13322
http://a.fsd			12943
https://59.1			12875
https://www			13424
https://cha			13424
http://www			13424

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

Search Table

Query Generator:

CustomerId (INTEGER) =

Add

Current Criteria(s):

Column	Criteria	Value
--------	----------	-------

Remove

Custom Output Query:

Search Cancel

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.

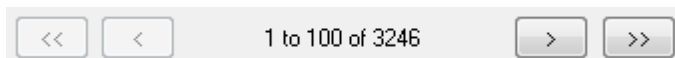
Criteria

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



<<

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.

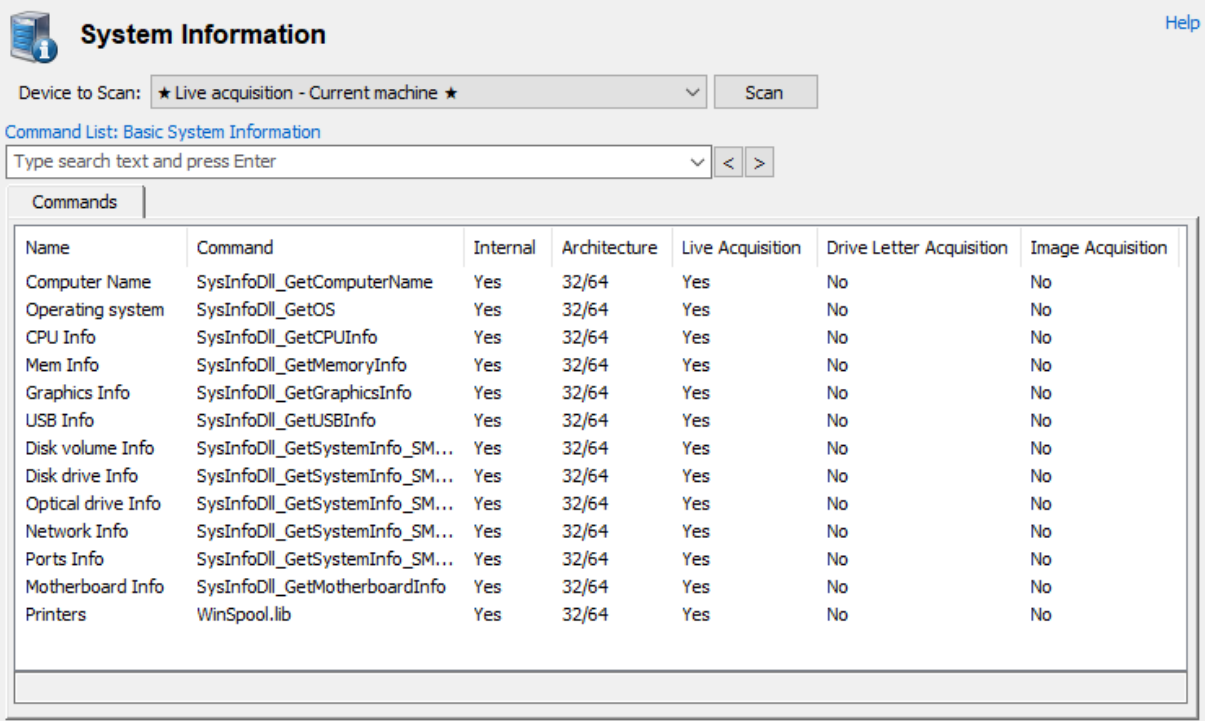
Table Information

Shows the table structure of the currently loaded table.

5.32 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 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



Name	Command	Internal	Architecture	Live Acquisition	Drive Letter Acquisition	Image Acquisition
Computer Name	SysInfoDll_GetComputerName	Yes	32/64	Yes	No	No
Operating system	SysInfoDll_GetOS	Yes	32/64	Yes	No	No
CPU Info	SysInfoDll_GetCPUInfo	Yes	32/64	Yes	No	No
Mem Info	SysInfoDll_GetMemoryInfo	Yes	32/64	Yes	No	No
Graphics Info	SysInfoDll_GetGraphicsInfo	Yes	32/64	Yes	No	No
USB Info	SysInfoDll_GetUSBInfo	Yes	32/64	Yes	No	No
Disk volume Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	No	No
Disk drive Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	No	No
Optical drive Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	No	No
Network Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	No	No
Ports Info	SysInfoDll_GetSystemInfo_SM...	Yes	32/64	Yes	No	No
Motherboard Info	SysInfoDll_GetMotherboardInfo	Yes	32/64	Yes	No	No
Printers	WinSpool.lib	Yes	32/64	Yes	No	No

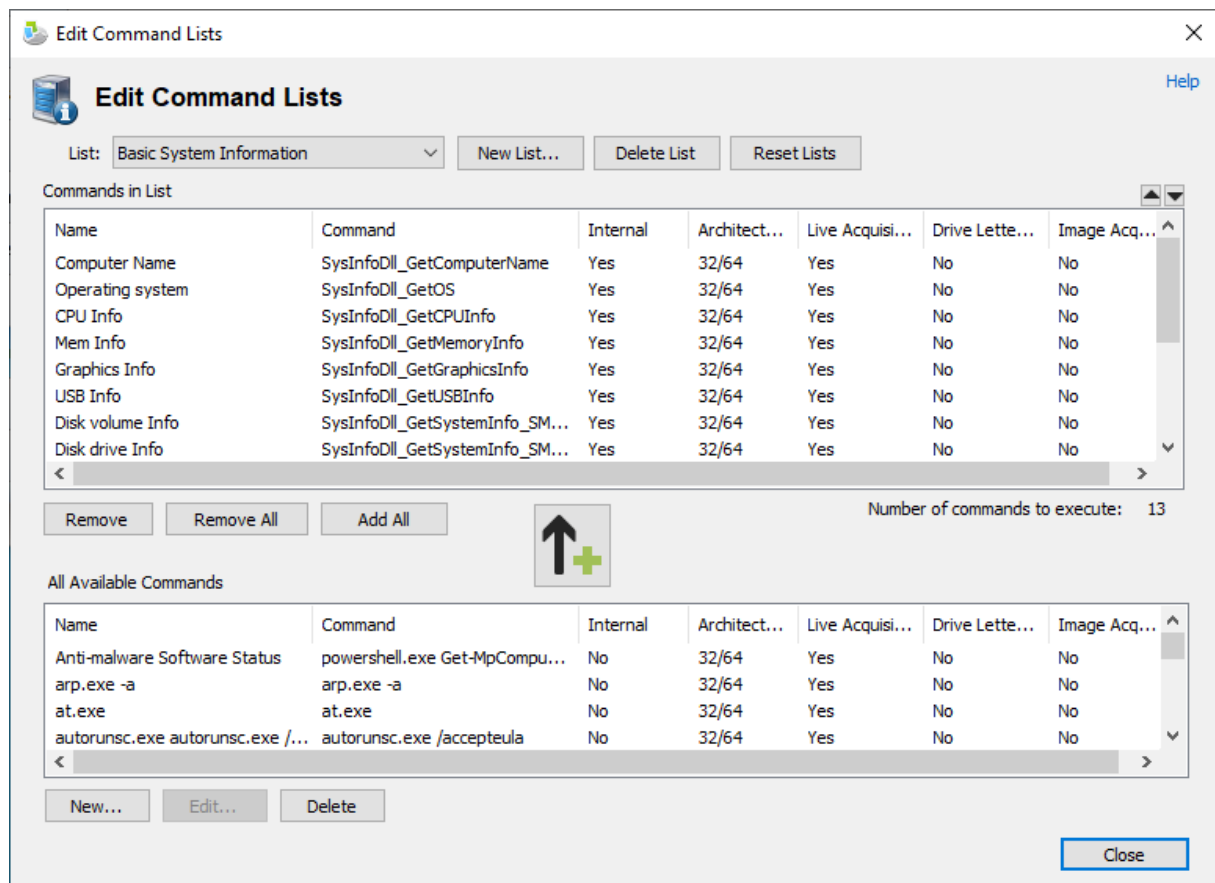
Once the commands have executed the output will appear on the results tab and can then be saved to a file or to case.

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.

The *Python Scripts* list and any external tools commands that have been added by a user will run on either the live system or a drive letter specified in the command itself.

While OSForensics comes with several 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 *Command List* link and selecting *Edit Command Lists...* drop-down option, you can go to the list management window.



New external tools and Python scripts 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.

The following commands will search for registry files available on the drive selected or the live system depending on the option selected:

- *Get Computer Name (Registry)*
- *Get Timezone Info (Registry)*
- *Get Network Info (Registry)*

- *Get User Info (Registry)*

If you have a number of different commands selected and have not selected *Live acquisition*, 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.

Get User Info (Registry)

Information collected by this command is read from the SAM registry file. The account creation date is taken from the registry key creation time for the user while the other dates are read from the "F" value for the user entry.

If running on a live system you will receive a warning message about changing permissions on the registry keys in order to access it. If you continue then some dates in the registry will be altered (for example the user account creation date that is displayed). To avoid this you can add the C drive to the case in forensics mode (eg Drive-C) and run the command on Drive-C.

5.32.1 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.

External Tools Directories:

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 install a new Python script simply place it in one of the following folders depending on your operating system;

Vista / Win7: C:\ProgramData\PassMark\OSForensics\Python\

XP: C:\Documents and Settings\All Users\Application Data\PassMark\OSForensics\Python\

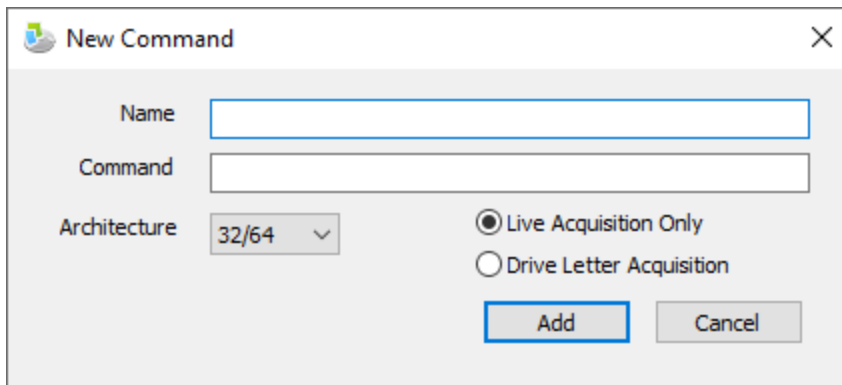
To add a new Python module/library simply place it in one of the following folders depending on your operating system;

Vista / Win7: C:\ProgramData\PassMark\OSForensics\Python\OtherLibs

XP: C:\Documents and Settings\All Users\Application Data\PassMark\OSForensics\Python\OtherLibs

Adding New Commands:

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.



The command should be the executable with any command line parameters needed. External commands that specify .py extension will be considered a Python script and ran through the Python Interpreter. 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:

- Autoruncs: <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>

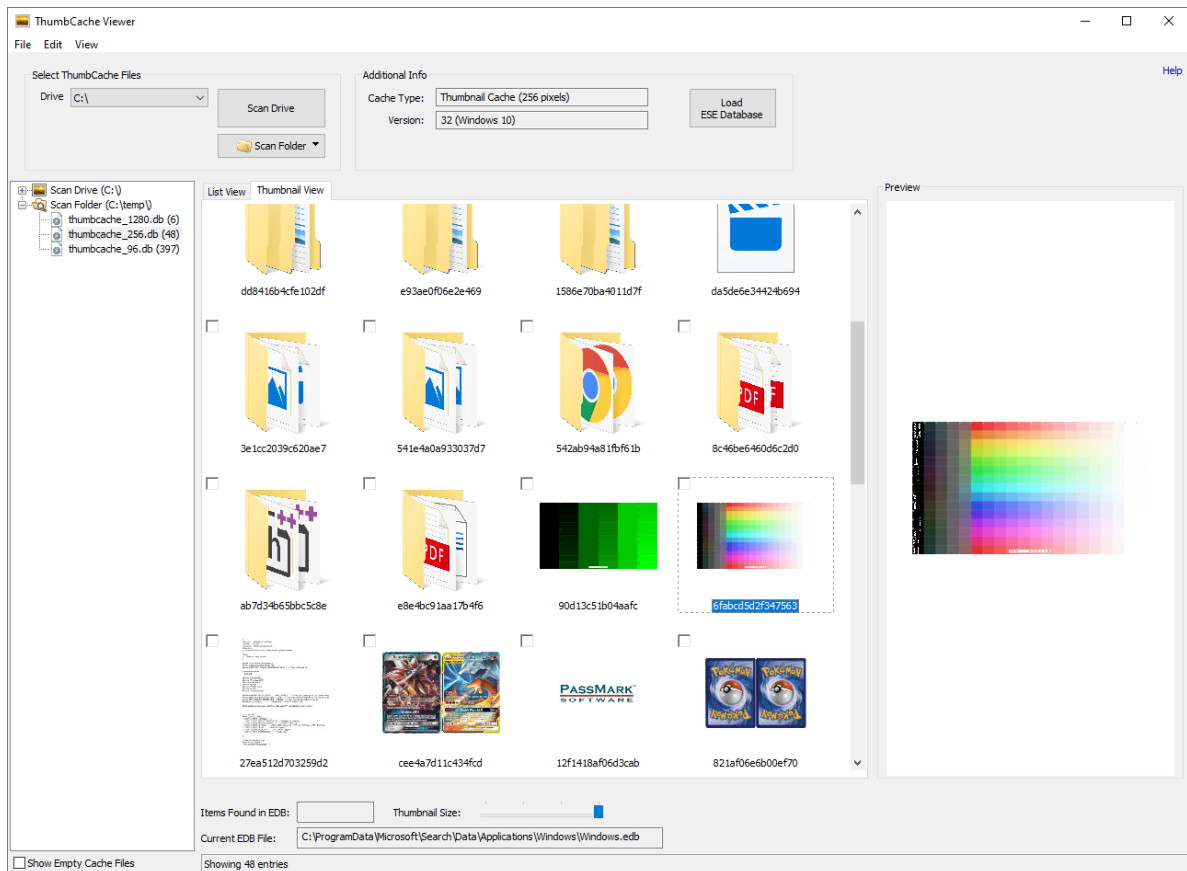
Notes concerning Python Scripts:

- The embedded version of Python included with OSForensics is V3.6.5
- Python Scripts only work on Live Acquisition or on System Drive Letters only.
- In normal Python, scripts that call sys.exit() would exit the program. However, to prevent scripts from closing OSForensics, OSForensics will intercept sys.exit calls from scripts. However, Python Scripts that throw SystemExit Exception explicitly can/will OSForensics process to exit immediately.
- See **External Tools Directories** above to see where scripts and library are required to be located.

5.33 ThumbCache Viewer

The ThumbCache 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 ThumbCache Viewer allows the investigators to browse thumbnail pictures stored in the cache database files. 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. ESE Database (Windows.edb) stores additional information of the thumbnails, such as the original full path, file size, extension, and other meta data.



ThumbCache Viewer

The table below summarizes the main components of the ThumbCache Viewer

Component	Description
Tree View	Displays the cache database files.
List View	Displays a list of thumbnail entries contained in the thumbnail cache file.
Thumbnail View	Displays a thumbnail view of the images contained in the thumbnail cache file.
Preview Pane	Displays the image of the currently selected thumbnail entry.

Usage

To scan thumbnail cache files on Windows Vista and beyond systems, select a Drive from the drop-down list and click 'Scan Drive'. It will search the default thumbnail cache directory **[Drive]:\Users\[User_Name]\AppData\Local\Microsoft\Windows\Explorer** for the cache files listed below.

Icon Cache Files List:

- iconcache_16.db
- iconcache_32.db
- iconcache_48.db
- iconcache_96.db
- iconcache_256.db
- iconcache_768.db
- iconcache_1280.db
- iconcache_1920.db
- iconcache_2560.db
- iconcache_custom_stream.db
- iconcache_exif.db
- iconcache_idx.db
- iconcache_sr.db
- iconcache_wide.db
- iconcache_wide_alternate.db

Thumbnail Cache Files List:

- thumbcache_16.db
- thumbcache_32.db
- thumbcache_48.db
- thumbcache_96.db
- thumbcache_256.db
- thumbcache_768.db
- thumbcache_1280.db
- thumbcache_1920.db
- thumbcache_2560.db
- thumbcache_custom_stream.db
- thumbcache_exif.db
- thumbcache_idx.db
- thumbcache_sr.db
- thumbcache_wide.db
- thumbcache_wide_alternate.db

In the tree view pane, the iconcache database files are grouped together put under the category "IconCache Files", while thumbcache files listed under "ThumbCache Files". Clicking these two tree view items allows to view all cache entries of iconcache or thumbcache files at once.

ThumbCache Viewer also supports to load "Thumbs.db" database in the older Windows versions such as Windows 95, 98, ME, 2000, XP and 2003. The files can be added to the tree view by clicking "Add File" or "Scan Folder".

Load ESE Database

To view extended information of the cache entries, users need to load the Windows Desktop search file, Windows.edb, which stores additional information for some indexed entries. The Windows.edb file is by default located at:

[Drive]:\ProgramData\Microsoft\Search\ Data\Applications\Windows\

By loading an EDB file, ThumbCache Viewer will search all the records in the **System_ThumbnailCacheId** table of the current Windows.edb database and find out the associated date. Then, they are displayed on the list view, or they can be viewed from the Extended Information dialog.

The mapping is done by searching the matching ThumbCache IDs.

List View Columns

Column Name	Data Origin	Description
ThumbCache ID	Cache file	Unique identification string (thumbnail cache ID) made up of sixteen hexadecimal characters.
Cache Entry Offset	Cache file	Offset of cache entry in cache file.
Cache Entry Size	Cache file	Complete size of cache entry.
Data Offset	Cache file	Offset of thumbnail data.
Data Size	Cache file	Thumbnail data size.
File Name	ESE Database file	Original file name obtained from loaded ESE Database.
Item Path Display	ESE Database file	Original file path obtained from loaded ESE Database.
Image Size	ESE Database file	Original image dimensions obtained from ESE Database.
Date Modified	ESE Database file	Original file modified date and time obtained from ESE Database.
Date Photo Taken	ESE Database file	Original file photo taken date and time obtained from ESE Database.
Location		The path of the cache file that the cache entry is retrieved from.

Reference List:

- Morris, S & Chivers, H 2011, An Analysis of the Structure and Behaviour of the Windows 7 Operating System Thumbnail Cache, <<http://dspace.lib.cranfield.ac.uk/handle/1826/13547>>.
- Quick, D, Tassone, C & Choo, KKR 2014, Forensic Analysis of Windows Thumbcache Files, <<https://ssrn.com/abstract=2429795>>.
- Morris, SLA 2013, An Investigation into the Identification, Reconstruction, and Evidential Value of Thumbnail Cache File Fragments in Unallocated Space, <<http://dspace.lib.cranfield.ac.uk/handle/1826/13547>>.

5.34 User Activity

The User Activity module scans the system for evidence of user 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.

The screenshot displays the 'User Activity' interface. At the top, the 'Device to Scan' is set to 'Live acquisition - Current machine'. Below this, there are buttons for 'Quick Scan' and 'Create Full Timeline'. A search bar is present with the text 'Type keyword and press Enter to search'. On the left, a tree view shows various activity categories such as 'All (21401)', 'Most Recently Used (451)', 'Installed Programs (656)', 'Clipboard (1)', 'Event Logs (0)', 'UserAssist (320)', 'Jump Lists (1080)', 'Shellbags (0)', 'Windows 10 Timeline (3048)', 'Cortana History (11)', 'Recycle Bin (53)', 'Shimcache (0)', 'SRUM (0)', 'Prefetch (0)', 'Windows Search (0)', 'BAM/DAM (0)', 'Downloads (206)', 'Browser History (13985)', 'Search Terms (1297)', 'Website Logins (43)', 'Form History (47)', 'Bookmarks (159)', 'Chat Logs (0)', 'Peer-to-Peer (0)', 'WLAN (0)', 'Cryptocurrency Wallet Apps (0)', 'Cookies (0)', 'Browser Custom Dictionary (1)', 'USB (28)', 'Mounted Volumes (2)', and 'Mobile Backups (0)'. The main area shows a table with the following columns: 'Item', 'Serial Number', and 'Evidence Location'. The table lists various hardware and software items with their respective serial numbers and evidence locations.

Item	Serial Number	Evidence Location
VirtualBox (VID_80EE) Pid_CAFE	ZY227BLWQL	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Motorola Mobility Inc. (VID_22B8) PID_2E82	ZY227BLWQL	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Aladdin Knowledge Systems (VID_0529) Token JC (PID_0620)	582cf646268087	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
ASUSTek Computer Inc. (VID_0805) PID_19AF&MI_00	68de2eaf58080000	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Logitech Inc. (VID_046D) PID_085C&MI_00	681275ad668080000	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Logitech Inc. (VID_046D) PID_085C&MI_02	681275ad668080002	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Toshiba America Inc (VID_0480) PID_8207	20160528003771F	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
ASUSTek Computer Inc. (VID_0805) PID_19AF&MI_02	68de2eaf58080002	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
VirtualBox (VID_80EE) Pid_CAFE	0000000000000006	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Alcor Micro, Corp. (VID_058F) USB Hub (PID_6254)	582cf6462680813	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Aladdin Knowledge Systems (VID_0529) Token JC (PID_0620)	681ac4990d8082	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Aladdin Knowledge Systems (VID_0529) Token JC (PID_0620)	681ac4990d8081	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Logitech Inc. (VID_046D) PID_085C	CC9D989F	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
ASUSTek Computer Inc. (VID_0805) PID_19AF	9876543210	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Logitech Inc. (VID_046D) Classic Keyboard 200 (PID_C315)	682ec54fe68082	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Microsoft Corporation (VID_045E) Basic Optical Mouse v2.0 ...	682ec54fe68081	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
VIA Labs, Inc. (VID_2109) Hub (PID_2811)	582cf6462680810	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
VIA Labs, Inc. (VID_2109) Hub (PID_3110)	582cf6462680825	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Aladdin Knowledge Systems (VID_0529) Token JC (PID_0620)	582cf646268088	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Toshiba Corporation (VID_0930) Kingston DataTraveler 102...	C860008BD9EBFB0AA18558A	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
VirtualBox (VID_80EE) Pid_CAFE	9876543210	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Kingston DataTraveler 2.0	C8600088637DFB0CA08EB1B80	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Toshiba Corporation (VID_0930) Kingston DataTraveler 102...	C8600088637DFB0CA08EB1B	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Afatech Technologies, Inc. (VID_15A4) SDHC/MicroSD/MMC...	0000000000000006	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Future Technology Devices International Limited (VID_0403)...	D30CZU86	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
TOSHIBA External USB 3.0	20160528003771F&0	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Kingston DataTraveler 2.0	C860008BD9EBFB0AA18558A&0	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...
Generic Storage Device	000000000000006&0	HKEY_LOCAL_MACHINE\SYSTEM\CurrentC...

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

Device to scan

Gather the user activity from the live machine or a particular drive. For non-live acquisitions, the 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.

★ Live acquisition - Current machine ★

User activity is gathered from the currently running operating system.

Quick Scan / Create Full Timeline

Clicking the "Quick Scan" button will run the scan with the currently selected activity types and options. Clicking the "Create Full Timeline" button will enabled all activity types and available options, including those which can take some time to run so the scan will be much slower.

More Scan Options

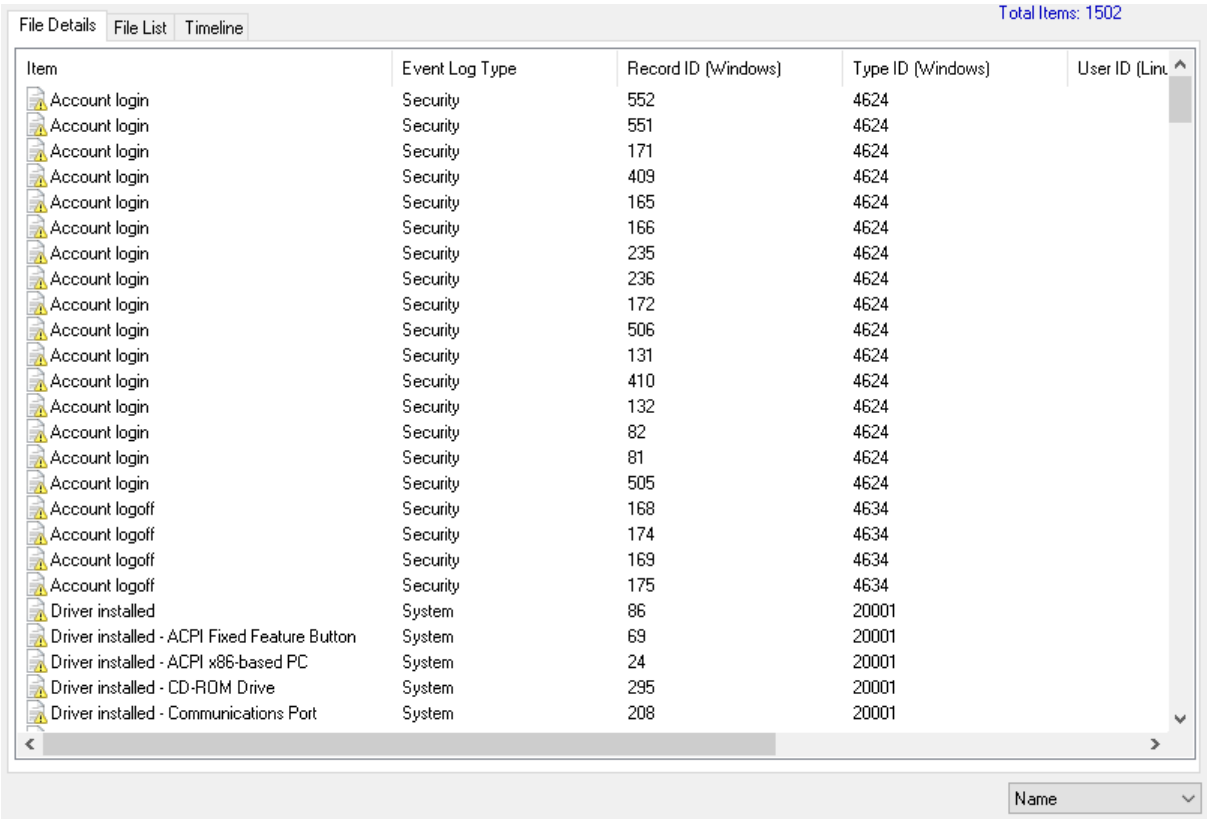
By clicking the "Config..." button you will be taken to the User Activity Configuration window where more advanced options can be selected.

Activity Filters

By clicking the *Activity Filters* link, you can configure or clear filter settings. Selecting *Configure...* opens *the* User Activity Filters window where you can further refine what activity types are displayed.

The search box can also be used to filter results based on text contained in the item description.

File Details View

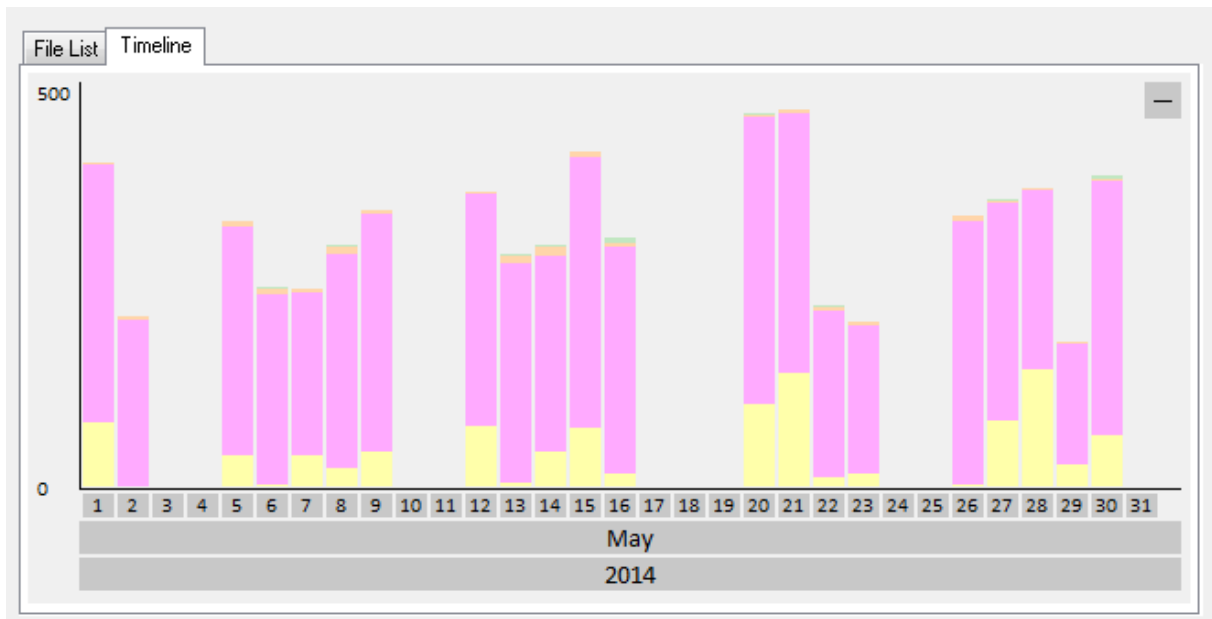


The screenshot shows a window titled "File Details" with a tabbed interface containing "File Details", "File List", and "Timeline". The "File Details" tab is active, displaying a table of system events. The table has five columns: "Item", "Event Log Type", "Record ID (Windows)", "Type ID (Windows)", and "User ID (Lin...". The "Total Items: 1502" is displayed in the top right corner. The table contains 20 rows of data, including "Account login", "Account logoff", and "Driver installed" events.

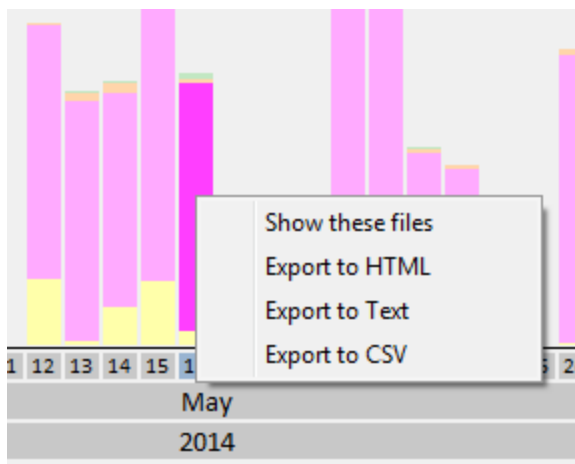
Item	Event Log Type	Record ID (Windows)	Type ID (Windows)	User ID (Lin... ^
Account login	Security	552	4624	
Account login	Security	551	4624	
Account login	Security	171	4624	
Account login	Security	409	4624	
Account login	Security	165	4624	
Account login	Security	166	4624	
Account login	Security	235	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 user 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 user 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.

Registry Activity

Windows Event Log

Windows Jump Lists

Windows Search

Chat Logs

Peer-2-Peer

Windows Prefetch

OSX Activity

SRUM Database

Clipboard Activity

5.34.1 User Activity Configuration

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

User Activity Configuration

Configuration Select the items to include in the scan: [Help](#)

OS Artifacts

Most Recently Used Jump Lists

Installed Programs Shellbags

Autorun Commands Windows 10 Timeline

Clipboard Recycle Bin

Event Logs BAM/DAM

UserAssist Anti-Forensics Artifacts

Advanced Scan

Shimcache

SRUM

Prefetch

Windows Search

Internet Artifacts

Downloads Chat Logs

Browser History Peer-to-Peer

Search Terms WLAN

Website Logins Cryptocurrency Wallet Apps

Form History

Bookmarks

Advanced Scan

Cookies

Moved Downloads (Slow)

External Device Usage

USB Mounted Volumes Mobile Backups

Scan Options

Scan Common File Locations

Scan Full Drive(s) [\(Select drives\)](#)

Date Range: From: 26-Jul-2021 To: 26-Jul-2021

Include dateless items

OS Artifacts

Item	Enabled by Default?	Description
Most Recently Used (MRU)	Yes	See Registry Activity for more details.
Installed Programs	Yes	See Registry Activity for more details.
Autorun Commands	Yes	See Registry Activity for more details.
Clipboard	Yes	-
Event Logs	Yes	See Event Logs for more details.
UserAssist	Yes	See Registry Activity for more details.
Jump Lists	Yes	See Jump Lists for more details.

Item	Enabled by Default?	Description
Shellbags	Yes	See Shellbags for more details.
Windows 10 Timeline	Yes	-
Recycle Bin	Yes	-
BAM/DAM	Yes	See BAM/DAM for more details.
Anti-Forensics Artifacts	Yes	See Anti-Forensics Artifacts for more details.
Shimcache	No	-
SRUM	No	-
Prefetch	No	See Prefetch Viewer for more details.
Windows Search	No	See Windows Search for more details.

Internet Artifacts

Item	Enabled by Default?	Description
Downloads	Yes	-
Browser History	Yes	-
Search Terms	Yes	-
Website Logins	Yes	-
Form History	Yes	-
Bookmarks	Yes	-
Chat Logs	Yes	Enables scanning for chat logs from MSN Messenger, AIM, Yahoo Messenger, ICQ, Skype, Miranda IM, and Pidgin.
Peer-to-Peer	Yes	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.
WLAN	Yes	See Registry Activity for more details.
Cryptocurrency Wallet Apps	Yes	See Cryptocurrency Wallet Apps for more details.
Cookies	No	-
Moved Downloads (Slow)	No	Scan the selected drive for files that have been downloaded and then moved from the download folder (using Zone.Identifier stream information). This can only be run on drives/images that use NTFS. As this process can be very slow this option is disabled by default. If the downloads option is selected via the treeview control on the user activity page this option is not enabled

Item	Enabled by Default?	Description
		automatically and can only be enabled from the configuration dialog.

External Device Usage

Item	Enabled by Default?	Description
USB	Yes	See Registry Activity for more details.
Mounted Volumes	Yes	See Registry Activity for more details.
Mobile Backups	Yes	Scanning for iOS backups that may have been stored on the system.

Scan Common File Locations / Scan Full Drives

The common file locations will be scanned by default.

If the Scan Full Drives option is checked, OSForensics will perform a full drive scan across the selected drives to search for the artifacts.

Search date ranges only

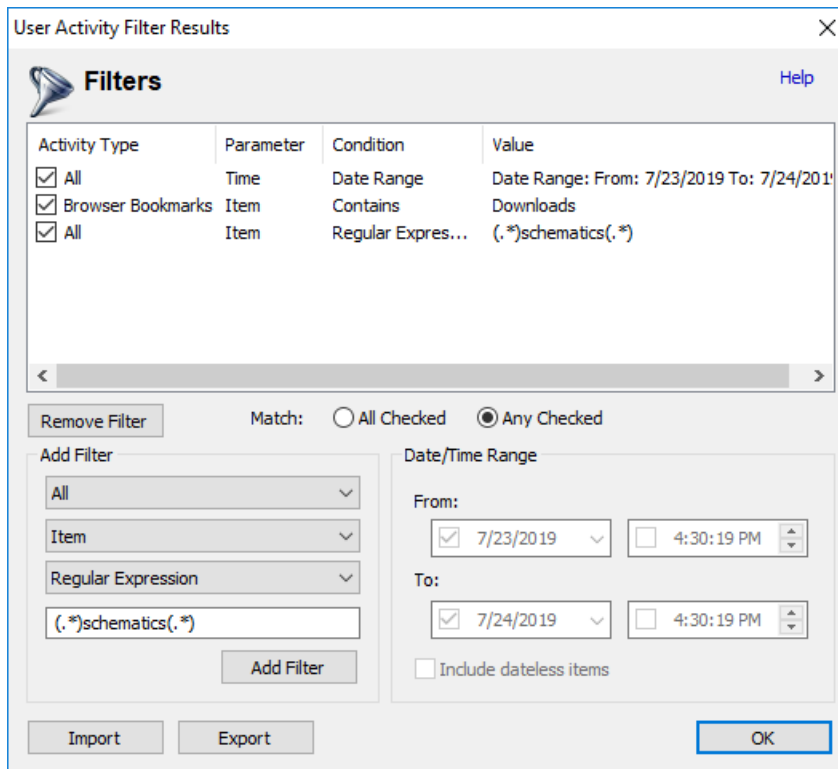
Allows the user to specify a particular access date range for the search results.

Include dateless items

If checked, will include items without an access date.

5.34.2 User Activity Filters

The User Activity Filters Window allows the user to add filters to narrow down the results from a User Activity scan. This window can be accessed by clicking on the *Configure...* option in the *Activity Filters* link drop-down menu in the main User Activity window.



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	Less	Less Than or Greater	Greater	Contai	Regular	Date
(=)	Equal	Than	Equal	Than or	ns	Expression	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
File size	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.

5.34.3 OSX Activity

OSForensics User 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.

5.34.4 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

MS Office - Recent Docs	Searches known registry keys for Microsoft Office MRU Documents for Office versions: 9.0, 11.0, 12.0, 14.0, 15.0, 16.0 and
Windows - 'Run' Entry	Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
Windows - Mapped Network Drives	<ul style="list-style-type: none"> • Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU • Network
Windows - Search History	<ul style="list-style-type: none"> • Software\Microsoft\Search Assistant\ACMRU\5603 • Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
Windows XP - Media Search History	Software\Microsoft\Search Assistant\ACMRU\5604
Windows XP - Internet Search Assistant	Software\Microsoft\Search Assistant\ACMRU\5001
Windows XP - People, Computer, Printers	Software\Microsoft\Search Assistant\ACMRU\5647
Wordpad - Recent Docs	Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Recent File List
MS Paint - Recent Files	Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List
Media Player - Recent Files	<ul style="list-style-type: none"> • Registry Locations: <ul style="list-style-type: none"> ○ Software\Microsoft\MediaPlayer\Player\RecentFileList ○ Software\Microsoft\MediaPlayer\Player\RecentURLList • Disk Locations: <ul style="list-style-type: none"> ○ VLC (vlc-qt-interface.ini on Windows or vlc-qt-interface.conf on Linux) ○ WMP (lastplayed.wpl and wmpfolders.wmdb)
Windows - Recent Documents	Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
Adobe Reader - Recent Files	Searches known registry keys for Adobe Reader MRU for versions: 9.0, 10.0, 11.0, DC
Windows Explorer - Last Visist	<ul style="list-style-type: none"> • Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU • Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU
Windows Explorer - Open/Save	<ul style="list-style-type: none"> • Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU • Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU
Windows Explorer - Resent Items	Disk Location: <user>\AppData\Roaming\Microsoft\Windows\Recent
OSX - ...	See OSX Activity

AutoRun Entries

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

Dates are read from the 'InstallDate' value where available and where this doesn't exist the last write date of the registry key where the information is located is used.

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 Entries

The UserAssist key from the registry 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 '{ }'.

¹The 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.

5.34.5 Event Logs

Windows Event Logs record the various events occur on the system which are of interest to forensic investigators.

User Activity Event Logs scan the logs created by Windows Vista and beyond. It supports event logs with file extension .evtx located in the **%System32%\winevt\Logs** directory.

You could use the OSForensics built-in Event Log Viewer module to perform advanced scan and filtering operations.

The following Event IDs are included in the User Activity scan:

Logon/Logoff

Event ID	Description (Item column)	Event Schema Element / Data Item	Reference
Microsoft-Windows-User Profile Service%4Operational.evtx			
1	Received User Logon Notification	EventData / Session	[1]
2	Finished Processing User Logon Notification	EventData / Session	[1]
3	Received User Logoff Notification	EventData / Session	[1]
4	Finished Processing User Logoff Notification	EventData / Session	[1]
Security.evtx			
4624	Successful Logon (Logon type 5 is excluded due to the overwhelming amount of these events generated by Windows)	EventData / TargetUserName EventData / TargetDomainName EventData / TargetLogonId EventData / LogonType EventData / WorkstationName EventData / IpAddress	[2] [3]
4634	Successful Logoff	EventData / TargetUserName EventData / TargetDomainName EventData / TargetLogonId EventData / LogonType	[2] [3]
4647	User Initiated Logoff	EventData / TargetUserName EventData / TargetDomainName EventData / TargetLogonId	[3]
4648	Logon Attempted Using Explicit Credentials	EventData / SubjectUserName EventData / SubjectDomainName EventData / SubjectLogonId EventData / TargetUserName EventData / IpAddress	[1] [3]
4625	Failed Logon Attempts	EventData / TargetUserName EventData / TargetDomainName EventData / FailureReason EventData / LogonType EventData / WorkstationName EventData / IpAddress	[2] [3]
4740	User Account Locked Out	EventData / TargetUserName EventData / TargetDomainName	[2]
4767	User Account Unlocked	EventData / TargetUserName EventData / TargetDomainName	[2]
4776	Successful/Failed NTLM Authentication	EventData / TargetUserName EventData / Workstation EventData / Status	[2] [3]

Storage Devices Usage

Event ID	Description (Item column)	Event Schema Element / Data Item	Reference
System.evtx			
10000	Installing/Updating Device Driver	UserData / DeviceId	[1]

Event ID	Description (Item column)	Event Schema Element / Data Item	Reference
20001	Driver Installation Completed	UserData / DeviceInstanceID UserData / DriverDescription	[1]
20003	Service Addition Process Completed	UserData / DeviceInstanceID	[1]
Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx			
2003	UMDF Host Process is Requested to Load Drivers for Device	UserData / InstanceId	[1]
2101	Pnp or Power Operation Completed for Device	UserData / InstanceId	[1]
2102	Finished Pnp or Power Operation Forwarded for Device	UserData / InstanceId	[1]
1006	Device Connected/Disconnected	EventData / DiskNumber EventData / Manufacturer EventData / Model EventData / Revision EventData / SerialNumber EventData / DiskId EventData / BusType EventData / PartitionStyle EventData / PartitionCount EventData / PartitionTableBytes	

Application Install

Event ID	Description (Item column)	Event Schema Element / Data Item	Reference
Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx			
17	Application Installation EXE Path	UserData / ExePath	[1]
Application.evtx			
11707	Software Package Installation Success	EventData / Data	[4]
11708	Software Package Installation Failure	EventData / Data	[4]
11724	Software Package Removal Success	EventData / Data	

Windows Services

Event ID	Description (Item column)	Event Schema Element / Data Item	Reference
System.evtx			
7034	Service Terminated Unexpectedly	EventData / param 1 EventData / param 2	[3]
7035	Service Stop/Start Control Sent	-	[2] [3]
7036	Service Status Changed	EventData / param 1 EventData / param 2	[2] [3]
7040	Service Start Type Changed	EventData / param 1 EventData / param 2 EventData / param 3	[3]
7045	Service Installed	EventData / ServiceName	[3]

Event ID	Description (Item column)	Event Schema Element / Data Item	Reference
		EventData / ImagePath EventData / ServiceType EventData / StartType EventData / AccountName	

Windows Update

Event ID	Description (Item column)	Event Schema Element / Data Item	Reference
System.evtx			
19	Windows Update Success	EventData / updateTitle	[5]
20	Windows Update Failure	EventData / errorCode EventData / updateTitle	
43	Windows Started Installing Update	EventData / updateTitle	
44	Windows Started Downloading Update	EventData / updateTitle	

Microsoft Office Usage

Event ID	Description (Item column)	Event Schema Element / Data Item	Reference
OAlerts.evtx			
300	Microsoft Office Alert	EventData / Data	[1]

System Start/Shutdown

Event ID	Description (Item column)	Event Schema Element / Data Item	Reference
System.evtx			
12	Operating System Started At	EventData / StartTime	[1]
13	Operating System Shutting Down At	EventData / StopTime	[1]
1074	Process Initialed Power Off/Restart	EventData / param1 EventData / param2 EventData / param3 EventData / param4 EventData / param5 EventData / param7	[1]
6005	Event Log Service Started	-	
6006	Event Log Service Stopped	-	
6013	System Uptime	EventData / Data	[1]

Remote Access

Event ID	Description (Item column)	Event Schema Element / Data Item	Reference
Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx			
1102	Client Initiated a Multi-transport Connection to Server	EventData / Name EventData / Value	[1]

Event ID	Description (Item column)	Event Schema Element / Data Item	Reference
1105	Multi-transport Connection Disconnected		[1]
1024	RDP ClientActiveX is Trying to Connect to Server	EventData / Name EventData / Value	[1]
1026	RDP ClientActiveX Disconnected	EventData / Name EventData / Value	[1]
1027	Connected to Domain	EventData / DomainName EventData / SessionId	[1]
Security.evtx			
4778	Session Reconnected to Window Station	EventData / AccountName EventData / AccountDomain EventData / LogonID EventData / SessionName EventData / ClientName EventData / ClientAddress	[6]
4779	Session Disconnected from Window Station	EventData / AccountName EventData / AccountDomain EventData / LogonID EventData / SessionName EventData / ClientName EventData / ClientAddress	[6]
Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx			
261	Listener Received a Connection	UserData / listenerName	[1]
1149	Remote Desktop Services: User Authentication Succeeded	UserData / Param1 UserData / Param2 UserData / Param3	[1] [6]
Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx			
21	Remote Desktop Services: Session Logon Succeeded	UserData / User UserData / SessionID UserData / Address	[6]
22	Remote Desktop Services: Shell Start Notification Received	UserData / User UserData / SessionID UserData / Address	[6]
24	Remote Desktop Services: Session Disconnected	UserData / User UserData / SessionID UserData / Address	[1] [6]
25	Remote Desktop Services: Session Reconnection Succeeded	UserData / User UserData / SessionID UserData / Address	[1] [6]
42	End Session Arbitration	UserData / User UserData / SessionID	[1]
Microsoft-Windows-SmbClient%4Connectivity.evtx			
30804	Client's Connection to Server Disconnected	EventData / ServerName EventData / Address	[1]
30805	Client Lost Session to Server	EventData / SessionId EventData / ServerName	[1]

Event ID	Description (Item column)	Event Schema Element / Data Item	Reference
30806	Client Re-established Session to Server	EventData / SessionId EventData / ServerName EventData / Address	[1]
30807	Connection to Share Lost	EventData / SessionId EventData / ServerName	[1]
30808	Connection to Share Re-established	EventData / SessionId EventData / ServerName EventData / Address	[1]

Printer Usage

Event ID	Description (Item column)	Event Schema Element / Data Item	Reference
Microsoft-Windows-PrintService%4Operational.evtx			
307	Document Printed	UserData / Param1 UserData / Param2 UserData / Param3 UserData / Param4 UserData / Param5 UserData / Param7 UserData / Param8	[1]
801	Printing Job	UserData / JobId	[1]
802	Deleting Job	UserData / JobId UserData / JobSize UserData / Pages	[1]
842	Print Job Sent to Printer	UserData / JobId UserData / Printer	[1]

List View Columns

Column Name	Data Origin
Item	See the Description in the above tables
Event Channel	Channel property of the System section
Event Time	TimeCreated property of the System section
Event ID	EventID property of the System section
Event Record ID	EventRecordID property of the System section
Event ID (Linux)	-
Event Information	See the Event Schema Element / Data Item in the above tables
User	EventData / SubjectUserName EventData / TargetUserName

Reference List:

[1] Kang, S, Kim, S, Park, M & Kim, J 2018, Study on Windows Event Log-Based Corporate Security Audit and Malware Detection, <<https://doi.org/10.13089/JKIISC.2018.28.3.591>>.

- [2] Anson, S, Bunting, S, Johnson, R & Pearson, S 2012, Mastering Windows Network Forensics and Investigation, 2nd edn, John Wiley & Sons, United States of America.
- [3] Lee, R 2019, 'Windows Forensic Analysis', SANS Institute, <<https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download>>.
- [4] Microsoft 2018, 'Event Logging', <<https://docs.microsoft.com/en-us/windows/win32/msi/event-logging>>.
- [5] Do, Q, Martini, B, Looi, J, Wang, Y & Choo KK 2014, Windows Event Forensic Process, <https://doi.org/10.1007/978-3-662-44952-3_7>.
- [6] Poling, J 2018, 'Windows RDP-Related Event Logs: Identification, Tracking, and Investigation', <<https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation/>>.

5.34.6 Jump Lists

Jump 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 Microsoft 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

5.34.7 Shellbags

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

5.34.8 SRUM

OSForensics will scan for the system resource usage monitor database in the Windows\System32\sru\ folder.

If found it will read information from these parts of the database;

- Windows network data usage monitor table {973F5D5C-1D90-4944-BE8E-24B94231A174}
- Application resource usage table {D10CA2FE-6FCF-4F6D-848E-B2E99266FA89}
- Windows network connectivity usage monitor table {DD6636C4-8929-4683-974E-22C046A43763}
- Windows push notification table {D10CA2FE-6FCF-4F6D-848E-B2E99266FA86}

An attempt will be made to convert the User-SID's present in the table to user names (where available).

5.34.9 Prefetch

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.

5.34.10 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 can 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.

5.34.11 Cortana History

Cortana is a digital personal assistance present on Windows computers after Windows 10. Cortana acts as a natural language interface between the user and a number of common operating system related tasks. These include activities such as adding calendar reminders, managing personal contacts, sending email and performing web searches.

In a forensics point of view, much of the information Cortana collects can be used for mapping user activity as well as other personally identifiable information. Many users are unaware of the nature of the data that the feature stores and thus are not likely to consider it when attempting to remove forensics artifacts.

In an attempt to provide more geographically relevant results to searches and created events, the GPS location where certain queries were made is stored. This can be used to identify the location of the device at a certain point in time.

Cortana also stores the contact information of other users interacted with. This includes contacts accessed over email, SMS and instant messaging services.

In addition to this, all web searches and the results therein are stored alongside other information.

5.34.12 BAM / DAM

Background Activity Moderator (BAM) exists in Windows 10 only after version 1709. It controls the activity of background applications.

Desktop Activity Moderator (DAM) is present only on Windows 8 machines that support connected standby. It controls the activity of desktop applications.

BAM/DAM provides full path of the executable file that was run on the system and the last execution timestamp.

5.34.13 Anti-Forensics Artifacts

OSForensics supports collecting evidences of the following Anti-Forensics tools usage:

- CCleaner
- Eraser
- File Shredder
- R-Wipe and Clean
- BCWipe
- DiskBoss
- Free Wipe Wizard
- Slacker
- VeraCrypt
- AxCrypt
- Gpg4win
- Timestomp
- Tor Browser

5.34.14 Downloads

The browser built-in download manager keeps a history of files downloaded.

Supported Browsers and Evidence Location

Browser	File Format	Location
Chrome	SQLite	%USERPROFILE%/AppData/Local/Google/Chrome/User Data/[Profile_Name]/History
Edge (Chromium)	SQLite	%USERPROFILE%/AppData/Local/Microsoft/Edge/User Data/[Profile_Name]/History
Opera	SQLite	%USERPROFILE%/AppData/Roaming/Opera Software/Opera Stable/History

Browser	File Format	Location
Firefox	SQLite	%USERPROFILE%/AppData/Roaming/Mozilla/Firefox/Profiles/[Profile_Name]/places.sqlite

List View Columns (Chrome, Edge-Chromium, Opera)

Column Name	Data Origin (column)	Data Origin (table)
File Name	"current_path" or "url"	"downloads" or "downloads_url_chains"
Source URL	"url"	"downloads_url_chains"
Downloaded To	"current_path"	"downloads"
File Size	"received_bytes"	"downloads"
Date Download Started	"start_time"	"downloads"
Date Download Ended	"end_time"	"downloads"

List View Columns (Firefox)

Column Name	Data Origin (column)	Data Origin (table)
File Name	"content" or "url"	"moz_annos" or "moz_places"
Source URL	"url"	"moz_places"
Downloaded To	"content"	"moz_annos"
File Size	"content"	"moz_annos"
Date Download Started	"dateAdded"	"moz_annos"
Date Download Ended	"content"	"moz_annos"

List View Columns (Other)

OSForensics also scans the files in the location: %USERPROFILE%/Downloads.

Column Name	Data Origin	Description
File Name	File attributes	
Source URL	-	
Downloaded To	File path	
File Size	File attributes	
Date Download Started	File creation time	
Date Download Ended	File creation time	

5.34.15 Browser History

Visited URLs stored on the system.

Supported Browsers and Evidence Location

The browser history files are by default located at:

Browser	File Format	Location
Chrome	SQLite	%USERPROFILE%/AppData/Local/Google/Chrome/User Data/ [Profile_Name]/History %USERPROFILE%/AppData/Local/Google/Chrome/User Data/ [Profile_Name]/Top Sites
Edge (Chromium)	SQLite	%USERPROFILE%/AppData/Local/Microsoft/Edge/User Data/ [Profile_Name]/History %USERPROFILE%/AppData/Local/Microsoft/Edge/User Data/ [Profile_Name]/Top Sites
Opera	SQLite	%USERPROFILE%/AppData/Roaming/Opera Software/Opera Stable/History
Firefox	SQLite	%USERPROFILE%/AppData/Roaming/Mozilla/Firefox/Profiles/ [Profile_Name]/places.sqlite
Internet Explorer	ESE database Registry	%USERPROFILE% %/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs
Edge (Legacy)	ESE database	%USERPROFILE% %/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat

List View Columns (Chrome, Edge-Chromium)

Column Name	Data Origin (column)	Data Origin (table)
Title	"title" "title"	"urls" "top_sites"
URL	"url" "url"	"urls" "top_sites"
Date Last Accessed	"last_visit_time" -	"urls" "top_sites"
Visit Count	"visit_count" -	"urls" "top_sites"

List View Columns (Opera)

Column Name	Data Origin (column)	Data Origin (table)
Title	"title"	"urls"
URL	"url"	"urls"
Date Last Accessed	"last_visit_time"	"urls"
Visit Count	"visit_count"	"urls"

List View Columns (Firefox)

Column Name	Data Origin (column)	Data Origin (table)
Title	"title"	"moz_places"
URL	"url"	"moz_places"
Date Last Accessed	"last_visit_date"	"moz_places"
Visit Count	"visit_count"	"moz_places"

List View Columns (Internet Explorer)

Column Name	Data Origin (column)	Data Origin (table/key)
Title	- -	- "TypedURLs" key in the Registry
URL	"Url" "Data"	"Container_#" table of WebCacheV01.dat file "TypedURLs" key in the Registry
Date Last Accessed	"AccessedTime" -	"Container_#" table of WebCacheV01.dat file "TypedURLs" key in the Registry
Visit Count	"AccessCount" -	"Container_#" table of WebCacheV01.dat file "TypedURLs" key in the Registry

5.34.16 Search Terms

Browser history of search terms in search engines.

Supported Browsers and Evidence Location

The browser search terms files are by default located at:

Browser	File Format	Location
Chrome	SQLite	%USERPROFILE%/AppData/Local/Google/Chrome/User Data/[Profile_Name]/History
Edge (Chromium)	SQLite	%USERPROFILE%/AppData/Local/Microsoft/Edge/User Data/[Profile_Name]/History
Opera	SQLite	%USERPROFILE%/AppData/Roaming/Opera Software/Opera Stable/History
Firefox	SQLite	%USERPROFILE%/AppData/Roaming/Mozilla/Firefox/Profiles/[Profile_Name]/formhistory.sqlite

List View Columns (Chrome, Edge-Chromium, Opera)

Column Name	Data Origin (column)	Data Origin (table)
Search Text	"term"	"keyword_search_terms"
Date Last Searched	"last_visit_time"	"urls"
URL	"url"	"urls"
Visit Count	"visit_count"	"urls"

List View Columns (Firefox)

Column Name	Data Origin (column)	Data Origin (table)
Search Text	"value"	"moz_formhistory"
Date Last Searched	"lastUsed"	"moz_formhistory"
URL	-	-
Visit Count	"timesUsed"	"moz_formhistory"

5.34.17 Website Logins

Login credentials of user for websites.

Supported Browsers and Evidence Location

The browser login data files are by default located at:

Browser	File Format	Location
Chrome	SQLite	%USERPROFILE%/AppData/Local/Google/Chrome/User Data/[Profile_Name]/Login Data
Edge (Chromium)	SQLite	%USERPROFILE%/AppData/Local/Microsoft/Edge/User Data/[Profile_Name]/Login Data
Opera	SQLite	%USERPROFILE%/AppData/Roaming/Opera Software/Opera Stable/Login Data
Firefox	Json	%USERPROFILE%/AppData/Roaming/Mozilla/Firefox/Profiles/[Profile_Name]/logins.json

List View Columns (Chrome, Edge-Chromium, Opera)

Column Name	Data Origin (column)	Data Origin (table)
Origin URL	"origin_url"	"logins"
Action URL	"action_url"	"logins"
Username	"username_value"	"logins"
Password	"password_value"	"logins"
Date First Used	"date_created"	"logins"

Column Name	Data Origin (column)	Data Origin (table)
Date Last Used	"date_last_used"	"logins"
Times Used	"times_used"	"logins"

List View Columns (Firefox)

Column Name	Data Origin (keyword)	
Origin URL	"hostname"	
Action URL	"formSubmitURL"	
Username	"encryptedUsername"	
Password	"encryptedPassword"	
Date First Used	"timeCreated"	
Date Last Used	"timeLastUsed"	
Times Used	"timesUsed"	

5.34.18 Form History

Auto fill data used to fill the website forms.

Supported Browsers and Evidence Location

The browser form history files are by default located at:

Browser	File Format	Location
Chrome	SQLite	%USERPROFILE%/AppData/Local/Google/Chrome/User Data/[Profile_Name]/Web Data
Edge (Chromium)	SQLite	%USERPROFILE%/AppData/Local/Microsoft/Edge/User Data/[Profile_Name]/Web Data
Opera	SQLite	%USERPROFILE%/AppData/Roaming/Opera Software/Opera Stable/Web Data
Firefox	SQLite	%USERPROFILE%/AppData/Roaming/Mozilla/Firefox/Profiles/[Profile_Name]/formhistory.sqlite

List View Columns (Chrome, Edge-Chromium, Opera)

Column Name	Data Origin (column)	Data Origin (table)
Field Name	"name"	"autofill"
Value	"value"	"autofill"
Date First Used	"date_created"	"autofill"
Date Last Used	"date_last_used"	"autofill"

Column Name	Data Origin (column)	Data Origin (table)
Times Used	"count"	"autofill"

List View Columns (Firefox)

Column Name	Data Origin (column)	Data Origin (table)
Field Name	"fieldname"	"moz_formhistory"
Value	"value"	"moz_formhistory"
Date First Used	"firstUsed"	"moz_formhistory"
Date Last Used	"lastUsed"	"moz_formhistory"
Times Used	"timesUsed"	"moz_formhistory"

5.34.19 Bookmarks

Saved web pages for users to quickly visit favorite websites.

Supported Browsers and Evidence Location

The browser bookmark data files are by default located at:

Browser	File Format	Location
Chrome	Json	%USERPROFILE%/AppData/Local/Google/Chrome/User Data/[Profile_Name]/Bookmarks
Edge (Chromium)	Json	%USERPROFILE%/AppData/Local/Microsoft/Edge/User Data/[Profile_Name]/Bookmarks
Opera	Json	%USERPROFILE%/AppData/Roaming/Opera Software/Opera Stable/Bookmarks
Firefox	SQLite	%USERPROFILE%/AppData/Roaming/Mozilla/Firefox/Profiles/[Profile_Name]/places.sqlite
Internet Explorer	Internet Shortcut	%USERPROFILE%/Favorites/

List View Columns (Chrome, Edge-Chromium, Opera)

Column Name	Data Origin (keyword)	
Item	"name"	
URL	"url"	
Date Added	"date_added"	

List View Columns (Firefox)

Column Name	Data Origin (column)	Data Origin (table)
Item	"title"	moz_bookmarks
URL	"url"	moz_places
Date Added	"dateAdded"	moz_bookmarks

List View Columns (Internet Explorer)

Column Name	Data Origin	
Item	Internet Shortcut file name	
URL	"URL"	
Date Added	File creation time	

* Note that MS Edge legacy (before V79) versions are not supported in the OSForensics Bookmarks scan.

5.34.20 Chat Logs

OSForensics will search for chat logs from these programs:

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

5.34.21 Peer-to-Peer

OSForensics supports collecting forensic artifacts from the following peer-to-peer sharing applications and platforms:

- BitTorrent/uTorrent
- Ares
- eMule
- UseNet (SABnzbd, Newshosting)
- Shareaza

OSForensics also parses the .NZB and .torrent file formats to display their contents details.

List View Columns

Column Name	Description
Item	File name.
Record Type	-
Content Size	Size of the P2P content.
Poster	Used for UseNet NZB files and the data is obtained from the "poster" attribute of the NZB file.
Content Creation Date	For the NZB files, this data is obtained from the "date" attribute. Note that this time info may not completely reliable as the recorded data was the representation of the date the server saw the shared NZB content, plus the timezones could be different (see the link). For the .torrent files, this data is from the value of the key "creation date". For the artifacts collected from the BitTorrent/uTorrent resume.data file, this data is obtained from the value of the key "added_on" of the resume.dat file.
Evidence Location	-
Evidence File Creation Date	The time of the evidence file was created.
Date Last Used	The last used time (Last time the server was pinged for eMule Server.met config file OR last torrent seeded time for Shareaza OR last shared time for eMule Known.met).
Download Location	For BitTorrent/uTorrent clients, this data is obtained from the value of the key "path" of the resume.dat file.
Downloaded Size	For BitTorrent/uTorrent clients, this data is obtained from the value of the key "downloaded" of the resume.dat file.
Download Status	-
Date Completed	For BitTorrent/uTorrent clients, this data is obtained from the value of the key "completed_on" of the resume.dat file.

5.34.22 Cookies

Cookie are files which are created when users visit websites.

Supported Browsers and Evidence Location

The browser cookie files are by default located at:

Browser	File Format	Location
Chrome	SQLite	%USERPROFILE%/AppData/Local/Google/Chrome/User Data/[Profile_Name]/Cookies
Edge (Chromium)	SQLite	%USERPROFILE%/AppData/Local/Microsoft/Edge/User Data/[Profile_Name]/Cookies
Opera	SQLite	%USERPROFILE%/AppData/Roaming/Opera Software/Opera Stable/Cookies
Firefox	SQLite	%USERPROFILE%/AppData/Roaming/Mozilla/Firefox/Profiles/[Profile_Name]/cookies.sqlite

List View Columns (Chrome, Edge-Chromium, Opera)

Column Name	Data Origin (column)	Data Origin (table)
Host	"host"	"cookies"
Path	"path"	"cookies"
Name	"name"	"cookies"
Value	"encrypted_value"	"cookies"
Date Created	"creation_utc"	"cookies"
Date Last Accessed	"last_access_utc"	"cookies"
Expiry Date	"expires_utc"	"cookies"

List View Columns (Firefox)

Column Name	Data Origin (column)	Data Origin (table)
Host	"host"	"moz_cookies"
Path	"path"	"moz_cookies"
Name	"name"	"moz_cookies"
Value	"value"	"moz_cookies"
Date Created	"creationTime"	"moz_cookies"
Date Last Accessed	"lastAccessed"	"moz_cookies"
Expiry Date	"expiry"	"moz_cookies"

5.34.23 Cryptocurrency Wallet Apps

OSForensics supports collecting evidences of the following Cryptocurrency Wallet applications:

- Binance
- Ledger Live
- Bitcoin Core
- Electrum
- Litecoin Core
- TokenPocket
- Daedalus Mainnet
- Electron Cash
- Melis Wallet
- Interstellar
- Solar Wallet
- Keybase
- Litemint

5.34.24 USB

OSForensics supports collecting evidentiary information from Registry and Windows Event Log that helps in tracking USB devices plugged into a machine.

There are two sub-categories under the USB section.

USB Devices

Displays list of USB devices connected.

The different sources of artifacts considered in this category include:

Artifacts	Location
PnP manager log file	[System Drive]:\Windows\INF\setupapi.dev.log
Windows Registry hives	SYSTEMCurrentControlSet\Control\DeviceClasses SYSTEMCurrentControlSet\Enum\USBSTOR SYSTEMCurrentControlSet\Enum\USB SYSTEMCurrentControlSet\Enum\SCSI
Windows Event logs Event ID 1006	[System Drive]:\Windows\System32\winevt\Logs\Microsoft-Windows-Partition%4Diagnostic.evtx

USB History

Displays connection and disconnection timestamps of USB storage devices.

The sources of artifacts considered in this category include:

Artifacts	Location
Windows Event logs Event IDs 2003, 2102 Event ID 1006	[System Drive]:\Windows\System32\winevt\Logs\Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx [System Drive]:\Windows\System32\winevt\Logs\Microsoft-Windows-Partition%4Diagnostic.evtx

*Note that this event logging is not enabled by default.

The "Filter Results for This Device" option in the right-click menu allows you to quickly filter in the specified USB device and only display the relevant information.

File Details#	File List#	Timeline#			
<input type="checkbox"/>	Item	Device Type	Product ID	Serial Number	Revision
<input type="checkbox"/>	WD My Passport 0837	USB	My Passport 0837	WWD1A26FK42K	1072
<input type="checkbox"/>	Seagate Expansion	USB	Exp		10
<input type="checkbox"/>	Seagate Technology L...	USB Attached SCSI (UAS) ...	PID,		EV_0710
<input type="checkbox"/>	Verbatim STORE N GO	USB	STC		00
<input type="checkbox"/>	Verbatim STORE N GO	Disk	STC	Enter#	00
<input type="checkbox"/>	Verbatim, Ltd (VID_18...	USB Mass Storage Device	Flas		EV_0100
<input type="checkbox"/>	Kingston DataTraveler...	Disk	Dat		
<input type="checkbox"/>	Kingston Technology ...	USB Mass Storage Device	Dat		EV_0001
<input type="checkbox"/>	Sony Corporation (VID...	USB Input Device	PID,		EV_0100
<input type="checkbox"/>	Sony Corporation (VID...	USB Audio Device	PID,		EV_0100
<input type="checkbox"/>	Sony Corporation (VID...	USB Input Device	PID,		EV_0100
<input type="checkbox"/>	Sony Corporation (VID...	USB Audio Device	PID,		EV_0100
<input type="checkbox"/>	Microsoft Corporation ...	USB Input Device	Xbo		
<input type="checkbox"/>	Microsoft Corporation ...	USB Input Device	Xbo		
<input type="checkbox"/>	Microsoft Corporation ...	USB Input Device	Xbo		
<input type="checkbox"/>	Microsoft Corporation ...	USB Input Device	Xbox360 Controller (PID_...	683922cc1580803	
<input type="checkbox"/>	Logitech Inc. (VID_04...	USB Input Device	PID_C33F&MI_01	682fc599be&0&0001	REV_3100
<input type="checkbox"/>	Logitech Inc. (VID_04...	USB Input Device	PID_C33F&MI_00	682fc599be&0&0000	REV_3100

5.35 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 Hashing Help

Hash Sets **Verify/Create Hash**

File
 Volume
 Text

File: ...

Hash Function: Secondary Hash Function:

Upper case output

Progress:

Data Hashed:

Calculated Hash:

Primary:

Secondary:

Comparison Hash:

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.

5.36 Web Browser

For computers supporting the newer Webview2 based on Chromium Edge the Web Browser module will open in a new window. 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.



Caution:

The internal OSForensics' web browser module is implemented Webview2 based on Chromium Edge. Several right click options including "Save As..." and possibly Print will not work due to OSForensics running with elevated permissions. We have not disable the options, but until a workaround is available or the API is changed. the options will not work. If you require those options, you can run OSForensics without elevated permissions, by starting the osf32.exe or osf64.exe executable directly from the the OSForensics program files directory.

Address Bar

Allows you to enter an URL to navigate to or shows the current URL of the loaded web page.

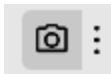
Navigation Buttons



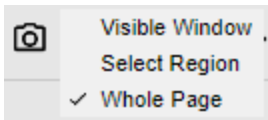
Not all buttons will be enabled at all times. Buttons (starting from left):

- Back - Load the previous page.
- Forward - Active when the "Back" button has been used. Goes Forward to the recently viewed page.
- Refresh/Stop - Reload the current page or when the page is being loading, stop the current page from loading.

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 be 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.



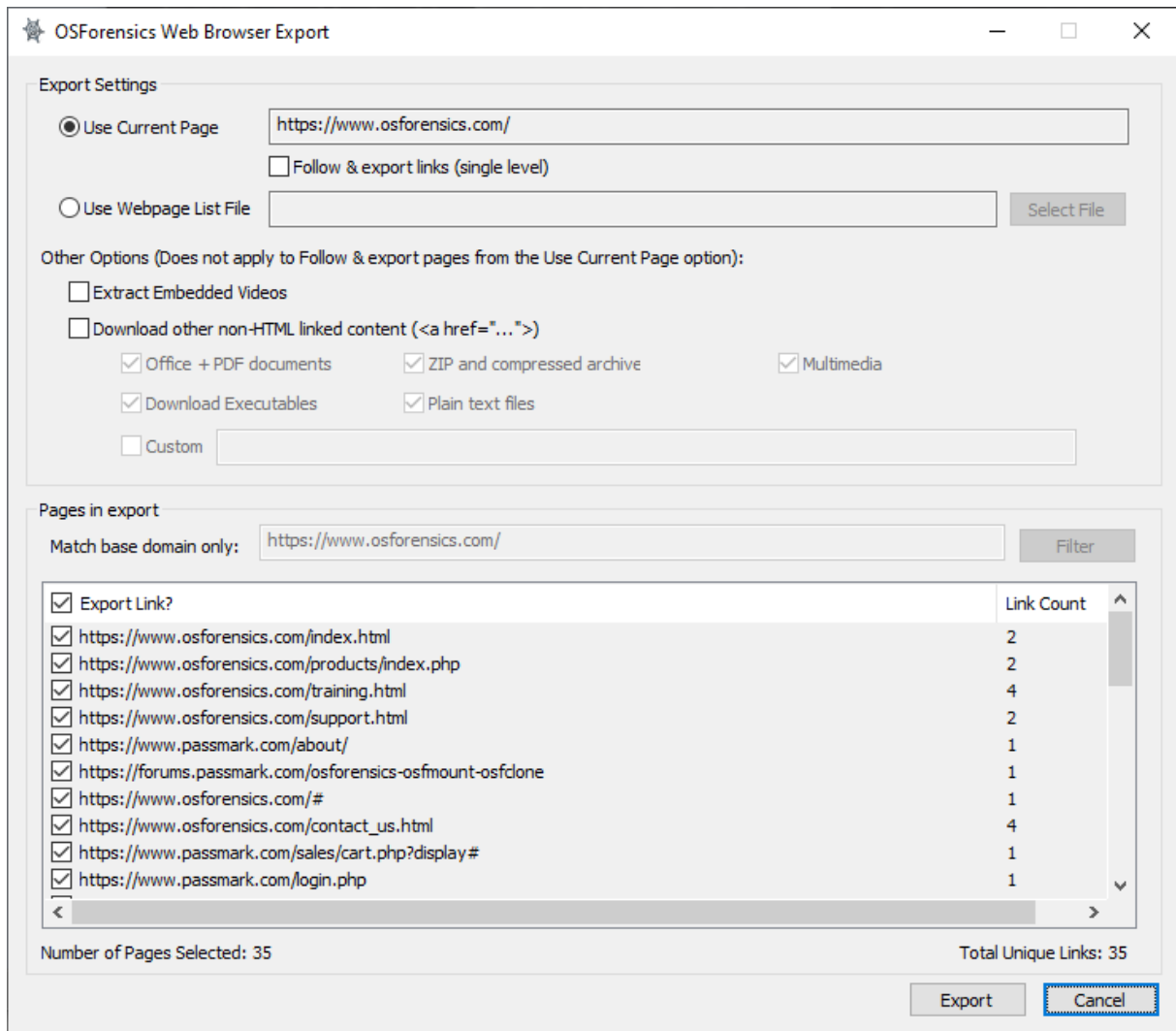
Screen Capture showing capture info text and OSForensics watermark.

*(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



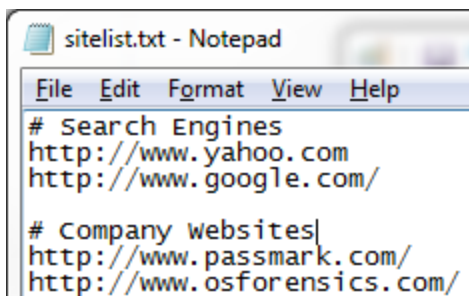
Pressing the following button will launch the export page dialog. The dialog will allow you to capture all the pages currently linked from the Current Page. Or load a site list file to capture.



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.



```

sitelist.txt - Notepad
File Edit Format View Help
# Search Engines
http://www.yahoo.com
http://www.google.com/

# Company websites
http://www.passmark.com/
http://www.osforensics.com/

```

Other Options - These options only apply to the top level page only when Use Current Page option or apply to all pages if using Webpage List File. Files will be saved and added to case in a subfolder of where the original case item is located.

Extract Embedded Video - Will attempt to extract the first embedded video on the webpage. Video is saved in .mp4 format.

Download other non-HTML linked content - Will download and saved other files that may be linked via anchor on the webpage. User can select a chosen preset or specify their own extensions to download.

- Office + PDF Documents -
.doc;.dot;.ppt;.pps;.pot;.xls;.xlt;.docx;.pptx;.xlsx;.dotx;.pdf;.odt;.sxw;.ods;.odp
- Zip and compressed archive - .zip;.tgz;.taz;.tar.gz;.tar;.zipx;.rar;.arj;.dmg;.iso;.chm;.bz2;.lzo;.7z
- Multimedia -
.jpg;.jpeg;.jpe;.gif;.tiff;.tif;.png;.bmp;.wmv;.mpg;.mpeg;.rmv;.rmvb;.flv;.mov;.qt;.avi.mp3;.mp4;.mkv;.wma
- Download Executables - .exe;.cab;.msi (*Note: Executable files with .exe extension will be renamed to .exe_ to prevent accidental opening of the file.*)
- Plain Text Files - .txt;.text;.rtf
- Custom - User specified extensions to download, separate extensions with semicolon;

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.

5.36.1 Web Browser (Non-supported OS)

For system that do not support the new Webview2 browser, OSForensics will start the older browser module. 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.



Caution:

The internal OSForensics' 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.

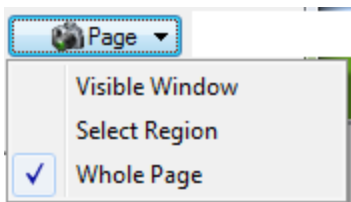
Navigation Buttons



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 be 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.

OSForensics Web Browser Export

Export Settings

Use Current Page

Follow & export links (single level)

Use Webpage List File

Export HTML Pages As:

Image (.png)

Web Archive (.mht)

Other Options (Does not apply to Follow & export pages from the Use Current Page option):

Extract Embedded Videos

Download other non-HTML linked content ()

Office + PDF documents ZIP and compressed archive Multimedia

Download Executables Plain text files

Custom

Pages in export

Match base domain only:

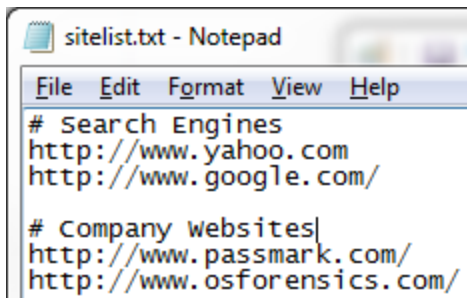
<input checked="" type="checkbox"/> Export Link?	Link Count
<input checked="" type="checkbox"/> http://www.osforensics.com/	1
<input checked="" type="checkbox"/> http://www.passmark.com/sales/cart.php	1
<input checked="" type="checkbox"/> https://www.osforensics.com/index.html	1
<input checked="" type="checkbox"/> https://www.osforensics.com/products.html	1
<input checked="" type="checkbox"/> https://www.osforensics.com/training.html	1
<input checked="" type="checkbox"/> https://www.osforensics.com/support.html	1
<input checked="" type="checkbox"/> http://www.passmark.com/about/	1
<input checked="" type="checkbox"/> https://www.osforensics.com/osforensics.html	1
<input checked="" type="checkbox"/> https://www.osforensics.com/discover.html	1
<input checked="" type="checkbox"/> https://www.osforensics.com/identify.html	1
<input checked="" type="checkbox"/> https://www.osforensics.com/manage.html	1
<input checked="" type="checkbox"/> https://www.passmark.com/legal/disclaimer.htm	1
<input checked="" type="checkbox"/> https://www.passmark.com/about/	1

Number of Pages Selected: 17 Total Unique Links: 17

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.



```
sitelist.txt - Notepad
File Edit Format View Help
# Search Engines
http://www.yahoo.com
http://www.google.com/
# Company websites
http://www.passmark.com/
http://www.osforensics.com/
```

Export As - Image or Web Archive. Pages will be saved as .PNGs images or .MHT web-archive format.

Other Options - These options only apply to the top level page only when Use Current Page option or apply to all pages if using Webpage List File. Files will be saved and added to case in a subfolder of where the original case item is located.

Extract Embedded Video - Will attempt to extract the first embedded video on the webpage. Video is saved in .mp4 format.

Download other non-HTML linked content - Will download and saved other files that may be linked via anchor on the webpage. User can select a chosen preset or specify their own extensions to download.

- Office + PDF Documents -
.doc;.dot;.ppt;.pps;.pot;.xls;.xlt;.docx;.pptx;.xlsx;.dotx;.pdf;.odt;.sxw;.ods;.odp
- Zip and compressed archive - .zip;.tgz;.taz;.tar.gz;.tar;.zipx;.rar;.arj;.dmg;.iso;.chm;.bz2;.lzo;.7z
- Multimedia -
.jpg;.jpeg;.jpe;.gif;.tiff;.tif;.png;.bmp;.wmv;.mpg;.mpeg;.rmv;.rmvb;.flv;.mov;.qt;.avi;.mp3;.mp4;.mkv;.wma
- Download Executables - .exe;.cab;.msi (*Note: Executable files with .exe extension will be renamed to .exe_ to prevent accidental opening of the file.*)
- Plain Text Files - .txt;.text;.rtf
- Custom - User specified extensions to download, separate extensions with semicolon;

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.

- Automatic Filters

5.37.1 Access Log

Web Server Log Viewer supports the following Access Log fields.

Column Name	Format String	Description
Client IP	%a	Client IP address of the request.
Server IP	%A	Local IP address.
Bytes Sent	%b	Size of response in bytes, excluding HTTP headers.

Column Name	Format String	Description
Cookie	"%{CookieName} C"	The contents of cookie VARNAME in the request sent to the server.
Time Taken (us)	%D	The time taken to serve the request, in microseconds.
Remote Hostname Remote Host IP	%h	Remote hostname or IP address.
Protocol Version	%H	The request protocol.
Referer	"%{Referer}i"	The referer.
User Agent	"%{User-agent}i"	The user agent.
Remote Logname	%l	The remote Logname.
Log ID (Request)	%L	The request log ID from the error log.
Request Method	%m	The request method.
Server Port	%p	The canonical port of the server serving the request.
Server Actual Port	%{local}P	The server actual port.
Client Port	%{remote}P	The client's actual port.
URI Query	%q	The query string.
Request Method Request Method Protocol Version	"%r"	First line of request. Same as "%m %U%q %H".
Status	%>s	The status code.
Date and Time	%t	Time the request was received.
Time Taken (sec)	%{s}T	The time taken to serve the request, in seconds.
Time Taken (ms)	%{ms}T	The time taken to serve the request, in milliseconds.
Time Taken (us)	%{us}T	The time taken to serve the request, in microseconds.
User Name	%u	Remote user if the request was authenticated.
Requested Resource	%U	The URL path requested, not including any query string.
Host Name	%v	The canonical ServerName of the server serving the request.
Server Name	%V	The server name according to the UseCanonicalName setting.
Bytes Received	%I	Bytes received, including request and headers.
Bytes Sent (inc headers)	%O	Bytes sent, including headers.
Bytes Transferred	%S	Bytes transferred (received and sent), including request and headers.

Some commonly used Access Log format strings supported by Web Server Log Viewer:

Common Log Format

```
"%h %l %u %t \"%r\" %>s %b"
```

Common Log Format with Virtual Host

```
"%v %h %l %u %t \"%r\" %>s %b"
```

Combined log format (NCSA extended)

```
"%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
```

Select Common Log Format > Access Log (Apache or NGINX) option when loading these common log files.

Select Custom Log and choose fields if loading a customized format log.

Add Log File Options

Common Log Format

- Access Log (Apache or NGINX)
- Error Log (Apache or NGINX)
Select Server Timezone: Local (GMT +10:00)
- IIS Log (W3C Logging, IIS Logging, NCSA Logging, HTTP Server API Error Log)
Select Server Timezone: Local (GMT +10:00) (for IIS Logging only)

Custom Format

- Custom Log
Select Server Timezone: Local (GMT +10:00)
Separator: Space
Date and Time Format: [28/Feb/2020:14:01:59 -0700]

All Fields

- Remote Hostname
- [Client IPv4:Port]
- Remote Logname
- User Name
- Date and Time
- Request Line
- Request Method
- Requested Resource
- Status Code
- Bytes Sent
- Referer
- User Agent
- Log Level
- Process ID
- Process ID:Thread ID

Selected Fields

#Example

```
192.168.1.1 - - [28/Feb/2020:14:01:59 -0700] "GET /favicon.ico HTTP / 1.1" 200 1538  
"https://www.passmark.com" "Mozilla/5.0 (Android 9; Mobile; rv:68.0)"
```

OK Cancel

Reference

http://httpd.apache.org/docs/2.4/mod/mod_log_config.html

5.37.2 Error Log

Web Server Log Viewer supports the following Error Log fields.

Column Name	Format String	Description
Client IP	%a	Client IP address and port of the request.
Server IP	%A	Local IP address and port.
Error Status Code	%E	APR/OS error status code and string.
Source File	%F	Source file name and line number of the log call.
Log Level	%l	Loglevel of the message.
Log ID (Request)	%L	Log ID of the request.
Module Name	%m	Name of the module logging the message.
Log Message	%M	The actual log message.
Process ID	%P	Process ID of current process.
Thread ID	%T	Thread ID of current thread.
Date and Time	%t	The current time.
Host Name	%v	The canonical ServerName of the current server.
Server Name	%V	The server name of the server serving the request according to the UseCanonicalName setting.

Some commonly used Error Log format strings supported by Web Server Log Viewer:

Apache Error Log Format

```
"[%t] [%l] [pid %P] %F: %E: [client %a] %M"
```

Apache Error Log Format with Virtual Host

```
"%v [%t] [%l] [pid %P] %F: %E: [client %a] %M"
```

NGINX Error Log Format

```
"%t [%l] %P#%T: %M"
```

Select Common Log Format > Error Log (Apache or NGINX) option when loading these common Error Logs, and choose the Server Timezone set on the server when logging the logs.

Select Custom Log and choose fields if loading a customized format log.

Add Log File Options

Common Log Format

Access Log (Apache or NGINX)

Error Log (Apache or NGINX)

Select Server Timezone: Local (GMT +10:00)

IIS Log (W3C Logging, IIS Logging, NCSA Logging, HTTP Server API Error Log)

Select Server Timezone: Local (GMT +10:00) (for IIS Logging only)

Custom Format

Custom Log

Select Server Timezone: Local (GMT +10:00)

Separator: Space

Date and Time Format: [28/Feb/2020:14:01:59 -0700]

All Fields

- Remote Hostname
- [Client IPv4:Port]
- Remote Logname
- User Name
- Date and Time
- Request Line
- Request Method
- Requested Resource
- Status Code
- Bytes Sent
- Referer
- User Agent
- Log Level
- Process ID
- Process ID:Thread ID

Selected Fields

#Example

Apache Server:
[Fri Feb 28 14:01:59 2020] [error] [pid 99980] core.c(4599): [client 192.168.1.1:443] AH01618: user not found: /www/OSForensics/

NGINX Server:
2020/02/28 14:01:59 [error] 1629#1629: open() "/www/index.htm" failed (2: No such file or directory)

OK Cancel

Reference

<https://httpd.apache.org/docs/2.4/mod/core.html>

5.37.3 IIS Logs

IIS log formats supported by Web Server Log Viewer:

- W3C Logging
- IIS Logging
- NCSA Logging

FTP Log and HTTP Server API Error Log files with W3C format are also supported.

W3C Logging:

Column Name	Format String	Description
Date and Time	date time	The date and time in UTC.
Service Name	s-sitename	The Internet service name and instance number that was running on the client.
Server Name	s-computername	The name of the server on which the log file entry was generated.
Server IP	s-ip	The IP address of the server on which the log file entry was generated.
Request Method	cs-method	The requested verb.
Requested Resource	cs-uri-stem	The target of the verb.
URI Query	cs-uri-query	The query that the client was trying to perform.
Server Port	s-port	The server port number that is configured for the service.
User Name	cs-username	The name of the authenticated user that accessed the server.
Client IP	c-ip	The IP address of the client that made the request.
Protocol Version	cs-version	The HTTP protocol version that the client used.
User Agent	cs(User-Agent)	The browser type that the client used.
Cookie	cs(Cookie)	The content of the cookie sent or received.
Referer	cs(Referer)	The site that the user last visited.
Host Name	cs-host	The host header name.
Status	sc-status	The HTTP status code.
Sub-status	sc-substatus	The substatus error code.
Win32 Status	sc-win32-status	The Windows status code.
Bytes Sent	sc-bytes	The number of bytes sent by the server.
Bytes Received	cs-bytes	The number of bytes received and processed by the server.
Time Taken (ms)	time-taken	The length of time that the action took, in milliseconds.
Stream ID	streamid	The Stream Id.

Other supported fields that using W3C extended log file format:

Column Name	Format String	Description
Session ID	x-session	FTP session identifier for the client's session.
Full Path	x-fullpath	Full relative path from the FTP root directory for the target of the action.
Additional Information	x-debug	Descriptive information for the sc-status code.
Client Port	c-port	The port of the client that made the request.
URI Query	cs-uri	The URL and any query that is associated with it.
Site ID	s-siteid	Not used. A placeholder hyphen always appears in this field.
Reason Phrase	s-reason	String that identifies the kind of error that is being logged.

Column Name	Format String	Description
Queue Name	s-queueName	The request queue name.

IIS Logging:

Column Name	Format String	Description
Client IP	Client IP address	The IP address of the client that made the request.
User Name	User name	The name of the authenticated user that accessed the server.
Date and Time	Date Time	The date and time on which the activity occurred.
Service Name	Service and instance	The Internet service name and instance number that was running on the client.
Server Name	Server name	The name of the server on which the log file entry was generated.
Server IP	Server IP address	The IP address of the server on which the log file entry was generated.
Time Taken (ms)	Time taken	The length of time that the action took, in milliseconds.
Bytes Received	Client bytes sent	The number of bytes sent by the client.
Bytes Sent	Server bytes sent	The number of bytes sent by the server.
Status	Service status code	Service status code.
Win32 Status	Windows status code	Windows status code.
Request Method	Request type	The request verb.
Requested Resource	Target of operation	The target of the verb.
Parameters	Parameters	The parameters that are passed to a scrip.

The fields in the above table are in the order of occurrence in the IIS Logging log file. The IIS log file format is a fixed ASCII text-based format that cannot be customized.

NCSA Logging:

Column Name	Format String	Description
Client IP	Remote host address	The IP address of the client that made the request.
Remote Logname	Remote log name	Not used. This value is always a hyphen.
User Name	User name	The name of the authenticated user that accessed the server.
Date and Time	Date, time, and Greenwich mean time (GMT) offset	The local date and time at which the activity occurred.
Protocol Version	Request and Protocol version	The HTTP protocol version that the client used.

Column Name	Format String	Description
Status	Service status code	The HTTP status code.
Bytes Sent	Bytes sent	The number of bytes sent by the server.

The NCSA Common log file format is a fixed ASCII text-based format that cannot be customized.

Select Common Log Format > IIS Log (W3C Logging, IIS Logging, NCSA Logging, HTTP Server API Error Log) option when loading these type logs.

Choose the Server Timezone if adding a IIS Logging log file.

Select Custom Log and choose fields if loading a customized format log.

Add Log File Options

Common Log Format

Access Log (Apache or NGINX)

Error Log (Apache or NGINX)

Select Server Timezone: Local (GMT +10:00)

IIS Log (W3C Logging, IIS Logging, NCSA Logging, HTTP Server API Error Log)

Select Server Timezone: Local (GMT +10:00) (for IIS Logging only)

Custom Format

Custom Log

Select Server Timezone: Local (GMT +10:00)

Separator: Space

Date and Time Format: [28/Feb/2020:14:01:59 -0700]

All Fields

- Remote Hostname
- [Client IPv4:Port]
- Remote Logname
- User Name
- Date and Time
- Request Line
- Request Method
- Requested Resource
- Status Code
- Bytes Sent
- Referer
- User Agent
- Log Level
- Process ID
- Process ID:Thread ID

Selected Fields

#Example

```
#Fields: date time cs-method cs-uri-stem c-ip cs(User-Agent) cs(Referer) sc-status time-taken
2020-02-28 14:01:59 GET /favicon.ico 192.168.1.1 Mozilla/5.0+(Android+9;+Mobile;+rv:68.0)
https://www.passmark.com/index.htm 404 8
```

OK Cancel

Reference

<https://docs.microsoft.com/en-us/windows/win32/http/w3c-logging>

<https://docs.microsoft.com/en-us/windows/win32/http/iis-logging>

<https://docs.microsoft.com/en-us/windows/win32/http/ncsa-logging>

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831624\(v%3Dws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831624(v%3Dws.11))

<https://support.microsoft.com/en-au/help/820729/error-logging-in-http-apis>

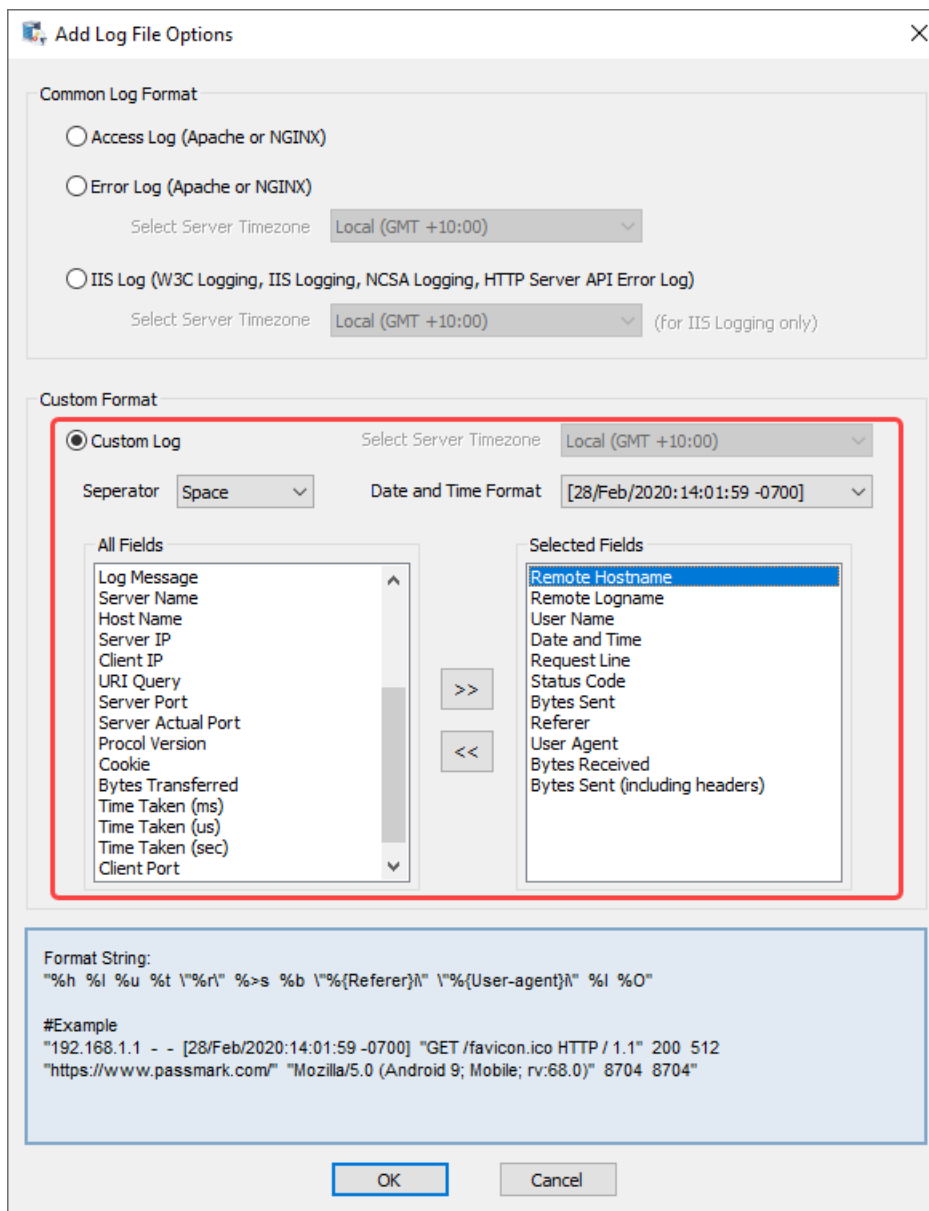
5.37.4 Custom Logs

Log formats in various servers are highly configurable, Web Server Log Viewer supports the following custom log fields.

Column Name	Field	Format String	Description
Remote Hostname	Remote Hostname	%h	Remote hostname or IP address.
Client IP	[Client IPv4:Port]	[client %a]	Client IP address and port of the request.
Remote Logname	Remote Logname	%l	The remote Logname.
User Name	User Name	%u	Remote user if the request was authenticated.
Date and Time	Date and Time	%t	Time the request was received.
Request Method Request Method Protocol Version	Request Line	"%r"	First line of request. Same as "%m %U%q %H".
Request Method	Request Method	%m	The request method.
Requested Resource	Requested Resource	%U	The URL path requested, not including any query string.
URI Query	URI Query	%q	The query string.
Protocol Version	Procol Version	%H	The request protocol.
Status	Status Code	%>s	The status code.
Bytes Sent	Bytes Sent	%b	Size of response in bytes, excluding HTTP headers.
Referer	Referer	"%{Referer}i"	The referer.
User Agent	User Agent	"%{User-agent}i"	The user agent.
Bytes Sent (inc headers)	Bytes Sent (including headers)	%O	Bytes sent, including headers.
Bytes Received	Bytes Received	%l	Bytes received, including request and headers.
Bytes Transferred	Bytes Transferred	%S	Bytes transferred (received and sent), including request and headers.
Log Level	Log Level	[%l]	Loglevel of the message.
Process ID	Process ID	[pid %P]	Process ID of current process.
Process ID Thread ID	Process ID:Thread ID	[pid %%P:tid %%T]	Process ID of current process. Thread ID of current thread.
Process ID Thread ID	Process ID#Thread ID:	%P:%T:	Process ID of current process. Thread ID of current thread.

Column Name	Field	Format String	Description
Source File	Source File	%F:	Source file name and line number of the log call.
Error Status Code	Error Status Code	%E:	APR/OS error status code and string.
Log Message	Log Message	%M	The actual log message.
Server Name	Server Name	%V	The server name according to the UseCanonicalName setting.
Host Name	Host Name	%v	The canonical ServerName of the server serving the request.
Server IP	Server IP	%A	Local IP address.
Client IP	Client IP	%a	Client IP address of the request.
Server Port	Server Port	%P	The canonical port of the server serving the request.
Server Actual Port	Server Actual Port	%{local}P	The server actual port.
Client Port	Client Port	%{remote}P	The client's actual port.
Cookie	Cookie	"% {CookieName} }C"	The contents of cookie VARNAME in the request sent to the server.
Time Taken (ms)	Time Taken (ms)	%{ms}T	The time taken to serve the request, in milliseconds.
Time Taken (us)	Time Taken (us)	%{us}T	The time taken to serve the request, in microseconds.
Time Taken (sec)	Time Taken (sec)	%{s}T	The time taken to serve the request, in seconds.
Log ID (Request)	Log ID (Request)	%L	The request log ID from the error log.

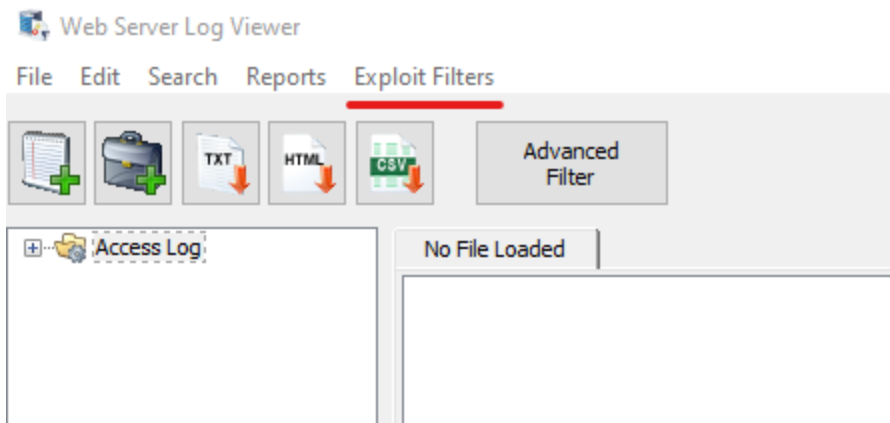
Select Custom Log option when loading log files with customized log fields. Choose the fields and add them to the list in order. Then the #Example will show how the log file looks like.



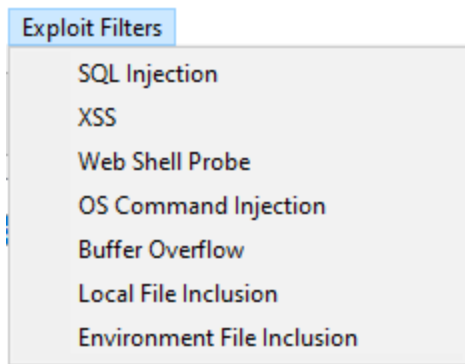
5.37.5 Automatic Filters

Automatically filter results according to the most common categories of web server exploits.

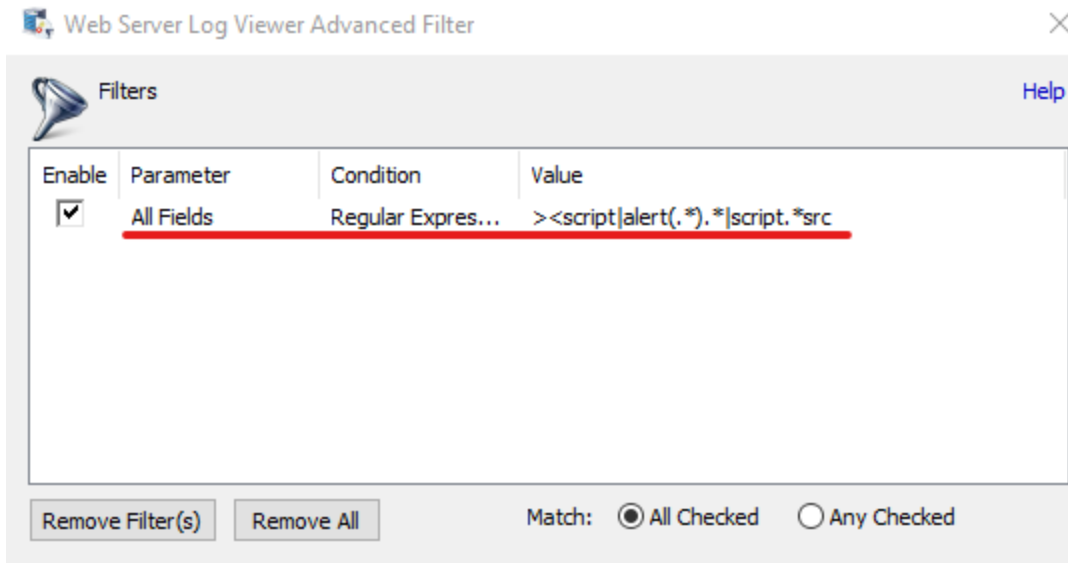
Select exploit under Toolbar > Exploit Filters



Select Exploit Filters > Filter



Filters are added under the Advanced Filters menu



When applying a new filter, all previous advanced filters will be deactivated.

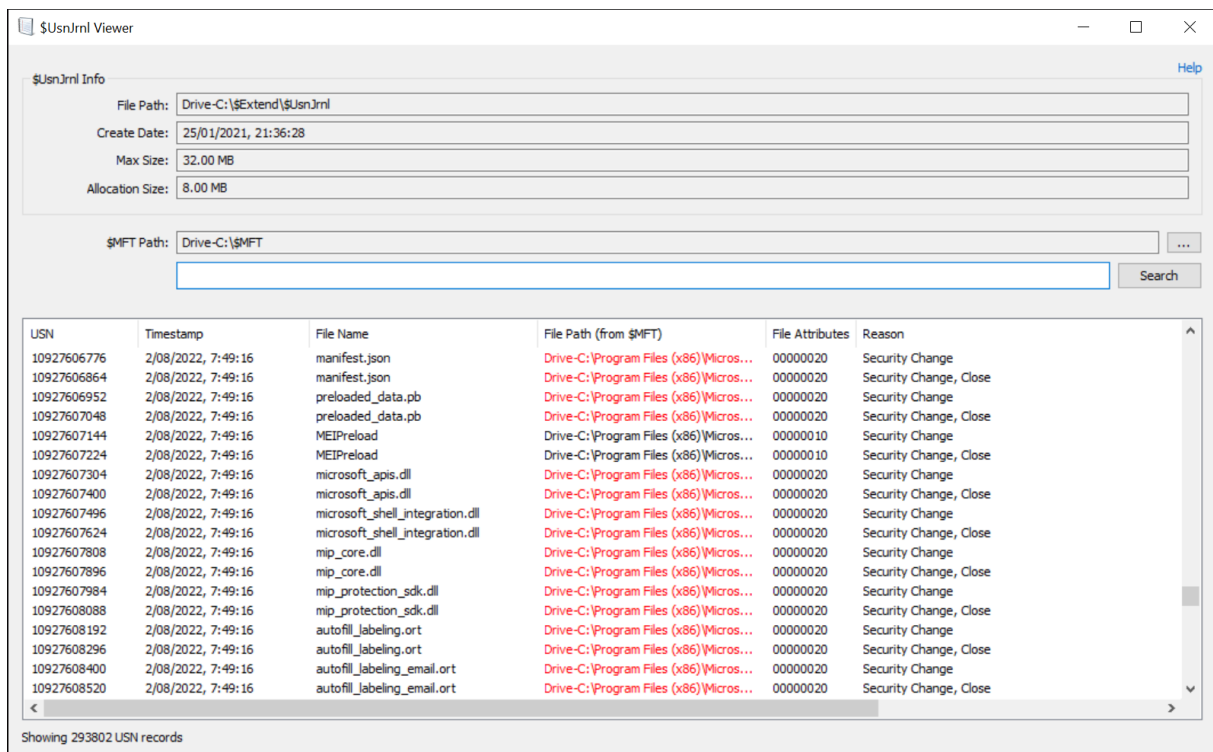
5.38 \$UsnJrnl Viewer

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

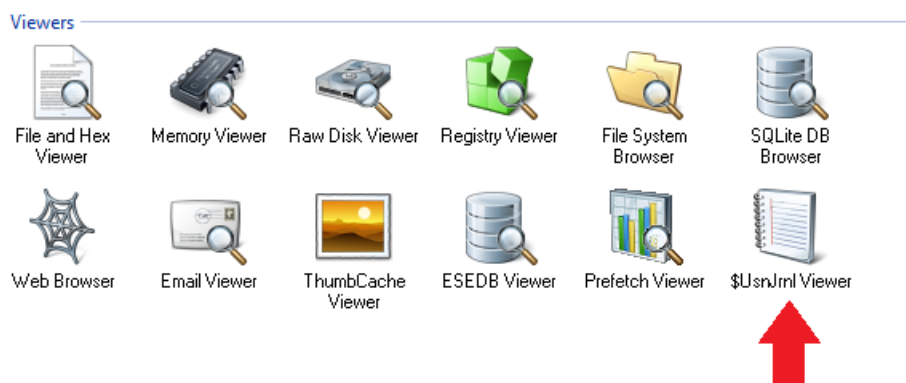
It should be noted that the journal records do not indicate how the file contents have changed, rather whether it has been created, modified or deleted.



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.

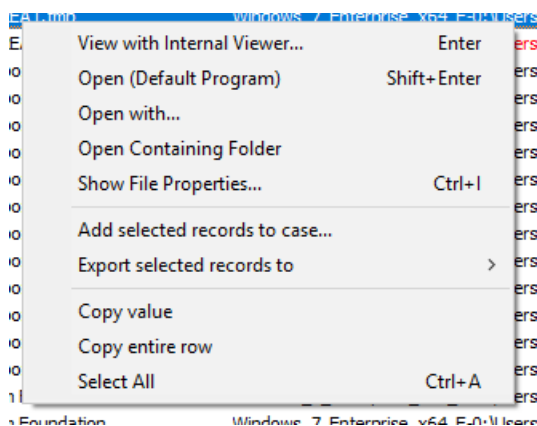
Usage

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 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

6 Advanced Topics

Free OSF Helper Tools

Examining System Page File

OSForensics Code Signing

Dates and Times

Regular Expressions

Windows Encrypting File System (EFS)

6.1 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 separately. 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.

6.2 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.

6.3 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.

6.4 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 to the "Region and Language" settings in the Windows control panel.

6.5 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.

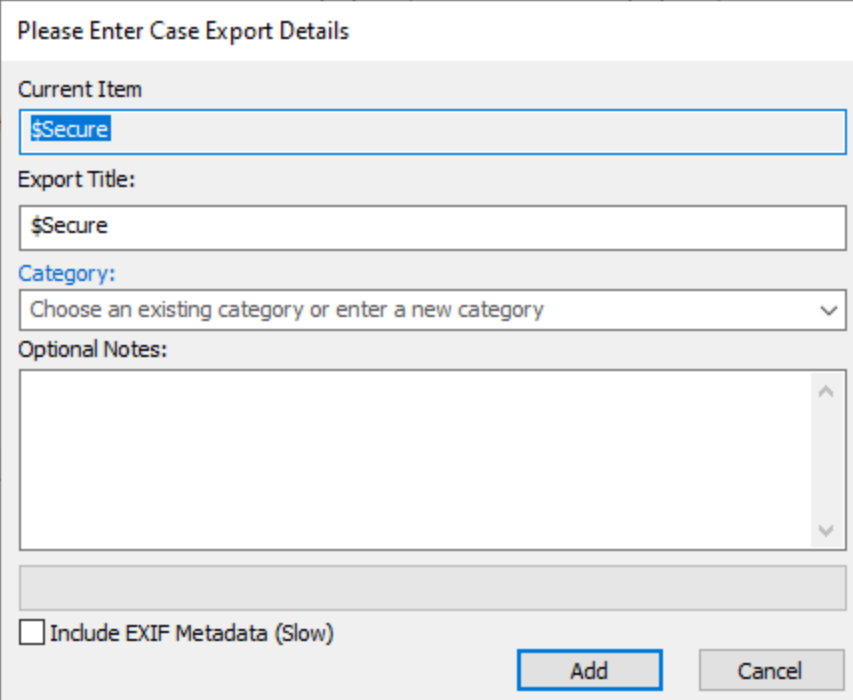
There are several pre-configured regular expressions available from the drop down list, these are found in the "RegularExpressions.txt" file in the OSForensics program data directory (ProgramData\PassMark\OSForensics). These have been collected from various sources and are kept as simple as possible 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}
```

6.6 Adding items to a case

Many items have an "Add to case" option in their right click menu. When choosing this option a dialog similar to the one pictured below will be displayed.



Please Enter Case Export Details

Current Item
\$Secure

Export Title:
\$Secure

Category:
Choose an existing category or enter a new category

Optional Notes:

Include EXIF Metadata (Slow)

Add Cancel

Current Item

This is the file name or identifier for the current item and cannot be changed.

Export title

This is a title to be used for displaying in the case manager and exported lists & reports. This will default to the current item name or when the "Use same details for all" option is checked will change to the special flag "<Use item name>" and each item will default to using its name as the title.

Category

Items can be assigned a category when added to a case, the default list contains entries based on the FBI UCR Program definitions. These categories can be customised by editing the Categories.txt file in the ProgramData\Passmark\Osforensics folder.

Optional Notes

Notes to be saved for this file (or collection of files)

Use same details for all

When checked will use the same title and notes for each file, see above for an explanation of the "<Use item name>" flag. If this option is selected then the files will be added to the case in a bulk operation without and more user input, otherwise the "Add" button will need to be clicked for each item being added to the case.

Include EXIF Metadata (Slow)

When checked will call the command line ExifTool on each file to gather and store any available EXIF metadata which can be a slow process.

6.7 Windows Encrypting File System (EFS)

Files on an image that have been encrypted using Windows EFS encryption can be decrypted if the recovery or backup PFX certificate (and any password for the certificate) is available.

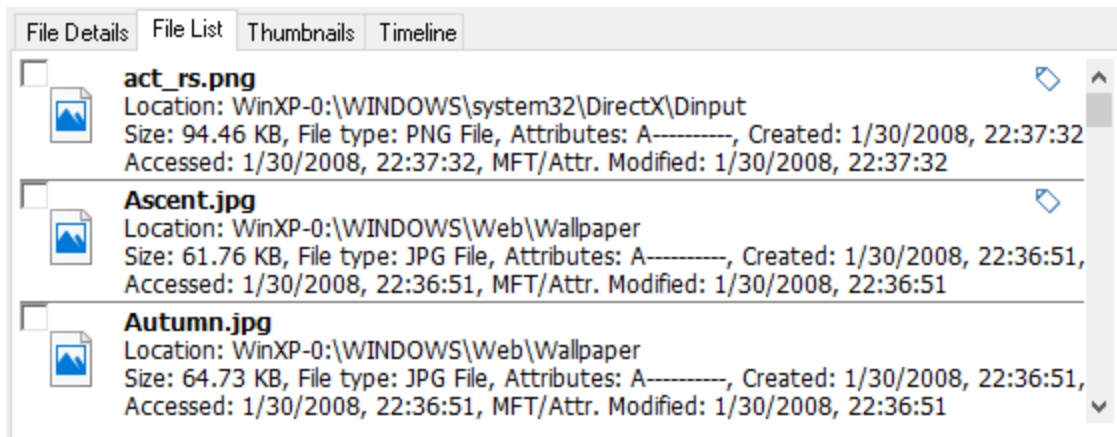
The PFX certificate can be installed to the local machine using the "Install PFX Certificate" tab of the Passwords section of OSForensics. Once the certificate is installed any EFS encrypted files that match the certificate can be exported from an image in OSForensics to a temporary folder and opened in the associated program (eg Word, Notepad etc).

To view and delete installed certificates use the "Open certificate manager" button to open the certmgr windows program, EFS certificates are located in the Personal -> Certificates folder.

6.8 Tags

Tags allow forensic investigators to mark any artifact for reference, for later analysis and/or inclusion in the forensics report. Unlike case files, a copy of the tagged item is not saved to the case, but contain hints/information where the item was located so the investigator can go back to review the items in depth later on. As such, thousands of items can be tagged instantaneously for later review.

Most items in OSForensics can be tagged with Ctrl+T keyboard shortcut or have a "Tag Item(s)" option in their right click menu. When tagged, the item appears under "Tagged Items" in the Case Management window. Tagged items are identified with the "tag" icon as follows.



Tagged items can optionally include a title or note, as well as being assigned to a category for grouping with related artifacts.

Artifacts that can be tagged include the following:

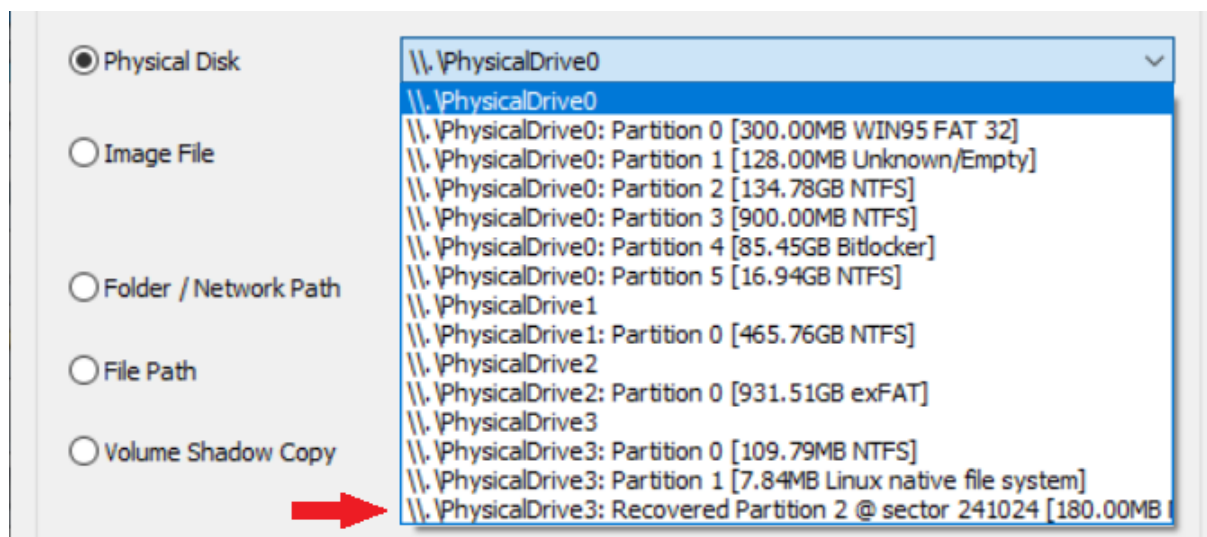
- Files
- Deleted files
- E-mail messages
- E-mail attachments
- URLs
- Registry keys
- Thumbnails
- Database records
- Event records
- Disk offsets
- Most user activity artifacts (Mobile, Cookie, Form, P2P, SRUM, Windows timeline, etc)

6.9 Recovered Partitions

Recovered Partitions are remnants of partitions and/or file systems found on a disk but are not indicated in the partition table. These partitions are found in the unpartitioned space of a disk.

Depending on the partitioning tool used, deleting a partition may only remove the entry from the partition table (eg. MBR or GPT), but does not erase the sectors allocated to the partition itself. As a result, the file system data remains on the disk even though the partition no longer exists. For example, Windows Disk Management does not erase the file system data when deleting a volume/partition.

OSForensics supports detection of recovered partitions by scanning the unpartitioned space of a disk for file system signatures. The following screenshot shows a recovered partition found on a disk.



Recovered partitions can be analyzed using OSForensics modules (eg. Deleted Files Search, Raw Disk Viewer) and added to the case just like a normal partition.

7 Support

System Requirements

License Keys

Contacting PassMark® Software

Free Version Limitations

7.1 System Requirements

- Windows Vista, Win 7, Win 8/8.1, Win 10, Win 11; 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)

7.2 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 from 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  
ASD9KQ29CXKZB1AAAKA19839KFKALDDKA57ABW  
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

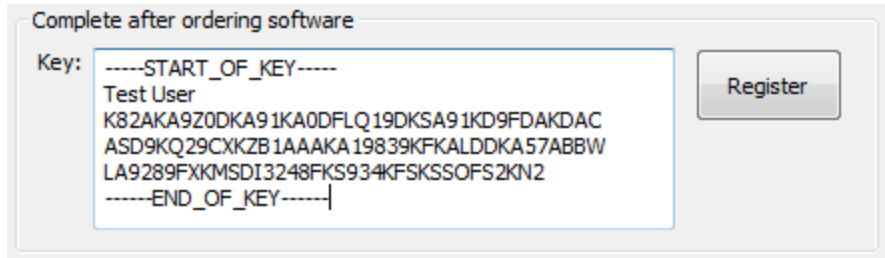
Select the entire key, including the -----START_OF_KEY----- and -----END_OF_KEY----- flags:

```
-----START OF KEY-----  
Test User  
K82AKA9ZODKA91KAODFLQ19DKSA91KD9FDAKDAC  
ASD9KQ29CXKZB1AAAKA19839KFKALDDKA57ABW  
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.



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.

7.3 Contacting PassMark® Software

On the Web

You can contact PassMark on the web at

<https://www.passmark.com>

<https://www.osforensics.com>

E-Mail

For technical support questions, suggestions

help@passmark.com

7.4 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 user 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.

8 Copyright and License

SOFTWARE COVERED BY THIS LICENCE

This license agreement ("Agreement") applies only to the version of the software package [OSForensics V8](#) 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 be 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 national 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 be 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 may 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 the remainder of the Agreement shall be fully enforceable as if the unenforced part or provision never existed. There are no third party beneficiaries or any promises, obligations or representations made by 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.

This software contains some MIT licensed code

- Parts related to Cloud Drive Imaging uses cpprestsdk library by Microsoft
<https://github.com/microsoft/cpprestsdk>
Read <https://github.com/microsoft/cpprestsdk/blob/master/license.txt> for license
- Parts related to JSON Viewer uses rapidjson and JSON-Viewer libraries
<https://github.com/Tencent/rapidjson>
Read <https://github.com/Tencent/rapidjson/blob/master/license.txt> for license

<https://github.com/kapilratnani/JSON-Viewer>
Read <https://github.com/kapilratnani/JSON-Viewer/blob/master/LICENSE> for license

<https://github.com/David-Byrne/Hangons>
Read <https://github.com/David-Byrne/Hangons/blob/master/LICENSE> for license

<https://github.com/Scarygami/location-history-json-converter>
Read <https://github.com/Scarygami/location-history-json-converter/blob/master/LICENSE> for license

9 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

- \$ -

\$UsnJrnl Viewer 376

- A -

analyze volume shadow 54
auditing 61
Automation 295

- B -

Binary string extraction 175
BitLocker 56
Bootable USB 196
Browse index 194
Browser Passwords 236
Button 9

- C -

case activity logging 61
Case management 29
 add device 49
 case activity logging 33
 case folder 33
 case narrative 33
 categories 33
 chain of custody 33
 contact details 33
 customizing report appearances 43
 default drive 33
 evidence 33
 investigator 33
 logging 61
 manage devices 59
 offence & custody data 33
 organization 33
 USB write block 33
Case Narrative 40
Categories 34
Chat logs 347

Clipboard 64
clipboard history 64
Clipboard Viewer 64
Compare signature 54
 create hash 303
 export 303
 ignore drive 303
 old new signature 303
Copyright and license 387
create index 164
 indexing problems and solutions 170
 indexing templates 171
Create signature config
 Directory list 300
 ignore reparse 300
 ignore temp folder 300
 SHA1 hashes 300
Credits 390
Cryptocurrency Wallet Apps 349

- D -

Data decode window 281
Dates and Times 381
Deleted e-mails 83
Deleted file search
 cluster view 78
 tech details 79
Deleted files search 66
 config 69
 result view 73
Deleted files search config
 case sensitive 69
 file size 69
 include folders 69
 match whole word 69
 quality 69
Deleted files search result view
 list view 73
 thumbnail 73
 timeline 73
Deleted partitions 384
Digital signature 380
Disk Info 280
drive imaging 133
 create image 134
 hidden areas - HPA/DCO 138
 RAID rebuild 141

drive imaging 133
 restore image 137
 Drive preparation 80
 Drive test 80

- E -

Email Viewer 83
 ESE database viewer 90
 advanced search 94
 ESEDB Viewer 90
 Event log 332

- F -

Features 12
 \$UsnJrnl viewer 376
 boot virtual machine 25
 case management 29, 33
 clipboard viewer 64
 drive imaging 133
 drive preparation 80
 email viewer 83
 ESE database viewer 90
 file system browser 119
 forensic copy 145
 hash sets 153
 hashing 351
 internal viewer 198
 logging 61
 Map viewer 217
 memory viewer 218
 password recovery 235
 prefetch viewer 264
 raw disk viewer 269
 registry viewer 286
 Script Player 295
 signature 299
 SQLite database browser 309
 system information 314
 ThumbCache Viewer 318
 user activity 321
 web browser 353
 File Carving Configuration 69
 File decryption & password recovery 251
 Adding dictionaries 257
 File name search 104

config 109
 default presets 117
 result view 113
 File name search config
 case sensitive 109
 creation date 109
 folder name 109
 modify date 109
 size limit 109
 subfolder 109
 whole word 109
 File name search default presets
 FileNameSearchPresets.cfg 117
 xml 117
 File Search
 deleted files 66
 indexing 163
 mismatch 226
 name 104
 File Search - Name
 config 109
 result view 113
 File search result view
 list view 113
 map view 116
 thumbnail 113
 timeline 113
 timeline view 76, 115
 file system browser 119
 deleted files 132
 metadata 125
 shadow copies 130
 views 127
 Forensic Copy 145

- G -

Generating rainbow tables 241

- H -

Hash set management 153
 hash set lookup 158
 import/export 162
 installing hash sets 160
 new hash set 155
 NSRL import 161

Hash set management 153
view hash set 157

- I -

ImageUSB 379
import 298
Imrpove 233
Index search result view 186
Indexer advance config 175
Limits 176
Stemming 174
Indexer advance options
scan extensions 172
skip list 172
Indexing 163
create index 164
search index 183
indexing problems and solutions 170
Indexing templates 171
Installing to a USB drive 196
Internal Viewer 198
file info 210
file viewer 200
hex/string viewer 204
metadata 212
text viewer 208
Introduction 8

- J -

Jump Lists 338

- L -

LED 9
Light 9
limit 176
logging
encrypted 61
hash chain 61
integrity 61
security 61
tamper-resistant 61
verbosity 61

- M -

magicLookup.csv 233
Map Viewer 217
Memory viewer 218
generate raw mem dump 223
Menu 9
Mismatch 233
Mismatch file search 226
config 228
result view 230
Mismatch file search result view
list view 230
thumbnail view 230
Mismatch filter configuration
by size 228
data range 228
exclude cache 228
exclude empty files 228
exclude folders 228
exclude recycling bin meta files 228
filter extentions 228
show inaccessible 228
Modify 233

- N -

Navigate 9

- O -

Ordering info 8
OSF.mg 233
OSFClone 379
OSFMount 379

- P -

Package Manager 295
packages 298
Password Recovery 235
browser passwords 236
File decryption & password recovery 251
Rainbow tables 245
Windows login 239
Peer-2-Peer 347

pip 295
Prefetch viewer 264
python 295, 298
Python Packages 295

- R -

Rainbow tables 241, 245
 Character sets 249
 Compatible file formats 247
 File naming convention 247
 Generating rainbow tables 241
 Rainbow table chains 248
 Recovering passwords 250
Raw disk viewer 269, 280, 281
 search 273
 tags 284
Recovered partitions 384
Registry activity 330
Registry Viewer 286
Regular expressions 275, 381
Results 233

- S -

Script Player 295
Scripting 295
Search index 183
 advanced search options 185
 browse index 194
 result view 186
Search index config
 any all 185
 date range 185
 email search 185
 index location 185
Shellbag 338
Signature info
 date 304
 directories included 304
 ignore reparse 304
 ignore temp folders 304
 SHA1 304
Signature Technical Details 305
Signatures 299
 compare 303
 configuration 300

 create 299
 info window 304
SQLite Database Browser 309
Support 384
 contact 386
 Free Version limitations 387
 license 385
 system requirements 384
supported file systems 53
supported image formats 52
supported partitioning schemes 53
System info 304
System Information 314
 external tools 316
System page file 380

- T -

tags 383
ThumbCache Viewer 318
triage 21
triage wizard 21

- U -

User activity 321
 Chat logs 347
 config 325
 Cryptocurrency Wallet Apps 349
 event log 332
 filters 328
 jump lists 338
 Peer-2-Peer 347
 Prefetch 339
 Registry activity 330
 Shellbag 338
 Windows search 339
User activity config
 autorun 325
 bookmarks 325
 cookies 325
 downloads 325
 events 325
 forms 325
 history 325
 installed programs 325
 jump lists 325

User activity config
MRU 325
prefetch 325
USB 325
UserAssist 325
volumes 325
windows search 325
WLAN 325
UsnJrnl Viewer 376

- V -

Verify/create hash 351
Viewer Settings
hex/string settings 207
text viewer settings 209
Virtual Machine 25
volume shadow 53

- W -

Web Browser 353
Windows login 239
Windows passwords 241
Windows search 339