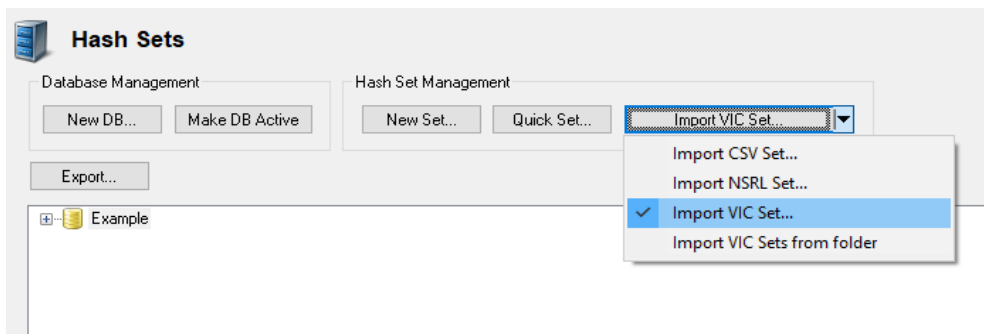


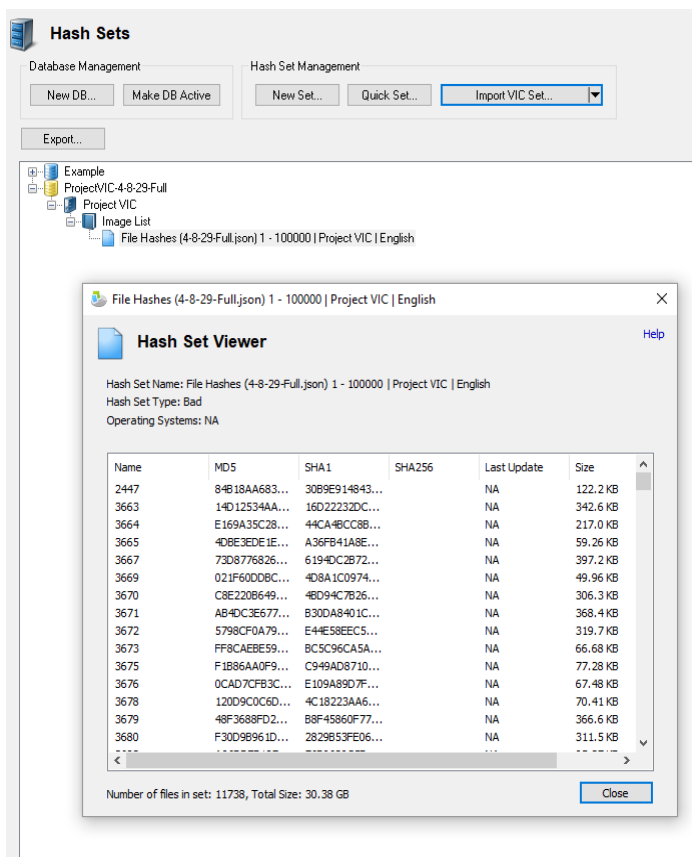
OSForensics by PassMark Software Project VIC Integration

Importing Project VIC .json files

OSForensics provides a “Hash Set” feature which is a database of hashes that can be compared against a selection of files on the drive or image being investigated.

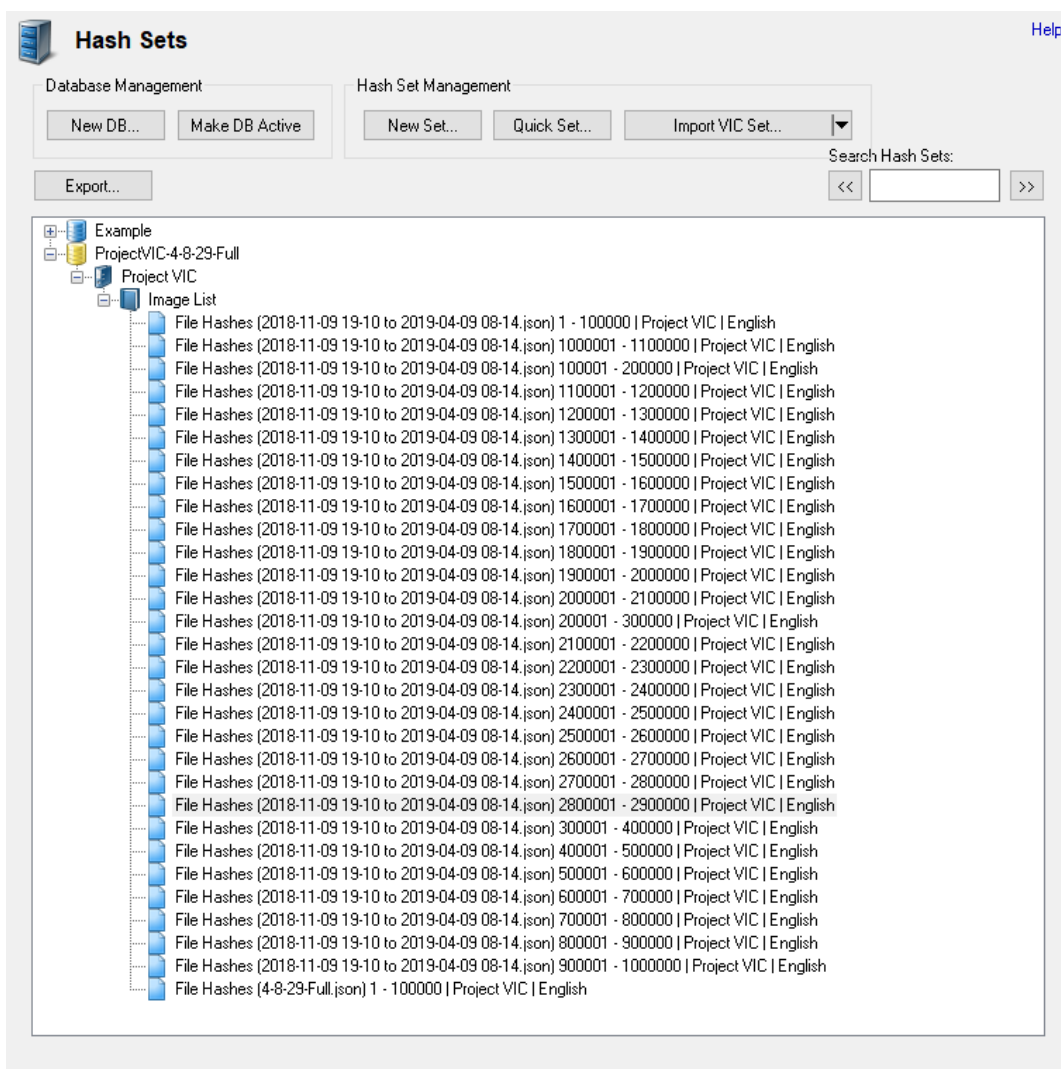
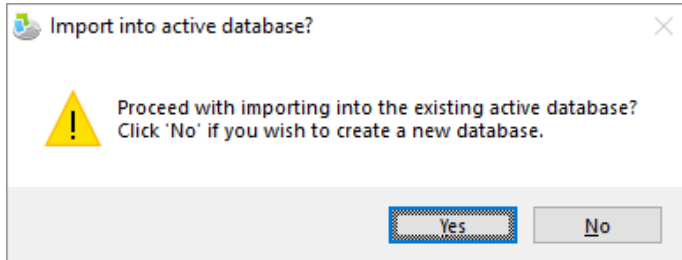


Once the JSON file has been imported, you can browse the hashes by double clicking on the Image List in the tree view.



Incremental update

To incrementally add new JSON files to the same database, simply make sure to select the desired database before clicking on “Import VIC Set” and you will be prompted to add to the existing database. If you select “No”, it will create a new database for the import.



Note that all Category 0 (Zero) hashes are excluded from import as they are considered to be Safe or Unknown files.

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

How to use Hash Set

In the OSF modules “File Name Search” and “Mismatch File Search”, you can compare a selected list of files against the active hash set and OSF will report the files that matches.

The screenshot displays the "File Name Search" application window. At the top, there is a search string field, a "Presets" dropdown set to "All Files", and a "Search" button. Below this is the "Start Folder" field, currently set to "C:\", with a "Config..." button. A configuration option "Include Sub - Folder names" is checked. The main area is a table with columns for "File Name", "Location", "Type", "Date modified", and "Date created". A context menu is open over the file "\$163W902.msg", showing options like "View with Internal Viewer...", "Open (Default Program)", and "Add list of all results to case...". At the bottom, a status bar shows "101667 item(s) checked", "Items Found: 101667", "Items Searched: 101667", and "Current Folder: Search Stopped".

File Name	Location	Type	Date modified	Date created
\$10V47V3.txt	C:\\$RECYCLE.BIN\1-5-21-1964354803-3058...	Text Document	4/23/2018, 15:06:35.8912178	4/23/2018, 15:06:35.888213
\$133YMM9	C:\\$RECYCLE.BIN\1-5-21-1964354803-3058...	File	11/22/2018, 14:38:05.79744...	11/22/2018, 14:38:05.79442
\$15ZPKZZ	C:\\$RECYCLE.BIN\1-5-21-1964354803-3058...	File	11/22/2018, 14:38:05.83345...	11/22/2018, 14:38:05.83043
\$163W902.msg		File	4/23/2018, 15:06:35.8872115	4/23/2018, 15:06:35.884207
\$169P590.docx		Microsoft Word Document	4/15/2019, 10:55:50.5471016	4/15/2019, 10:55:50.547101
\$16DVKQS		File	11/22/2018, 14:38:05.61606...	11/22/2018, 14:38:05.61306
\$16PYUBK.pdf		PDF Document	4/15/2019, 10:55:56.2655824	4/15/2019, 10:55:56.265582
\$16YQRSQ		File	11/22/2018, 14:38:05.65169...	11/22/2018, 14:38:05.64769
\$18YYWVW.jpg		Image	4/30/2019, 18:01:26.5878420	4/30/2019, 18:01:26.584832
\$19QGBFG		File	11/22/2018, 14:38:05.65970...	11/22/2018, 14:38:05.65669
\$1A9VLBX.notworking		File	1/2/2019, 14:10:06.9422329	1/2/2019, 14:10:06.9372315
\$1BCTSEU.msg		File	4/23/2018, 15:06:35.8822041	4/23/2018, 15:06:35.878198
\$1DCWBJ1		File	11/22/2018, 14:38:05.74372...	11/22/2018, 14:38:05.74072
\$1EY5Q93		File	11/22/2018, 14:38:05.75543...	11/22/2018, 14:38:05.75241
\$1F0ZBW4		File	11/22/2018, 14:38:05.71772...	11/22/2018, 14:38:05.71471
\$1FFZLRU		File	11/22/2018, 14:38:05.70571...	11/22/2018, 14:38:05.70271
\$1GN9WAC		File	11/22/2018, 14:38:05.67171...	11/22/2018, 14:38:05.66870
\$1OCHEED		File	11/22/2018, 14:38:05.58205...	11/22/2018, 14:38:05.57805
\$1PFDXV		File	4/10/2019, 17:12:36.7818299	4/10/2019, 17:12:36.778830
\$1RSGQ00		File	11/22/2018, 14:38:05.78056...	11/22/2018, 14:38:05.77742
\$1SXWCVO		File	11/22/2018, 14:38:05.62506...	11/22/2018, 14:38:05.62506
\$1T6YOK6		File	11/22/2018, 14:38:05.78642...	11/22/2018, 14:38:05.78642
\$1TH9I5T		File	11/22/2018, 14:38:05.60406...	11/22/2018, 14:38:05.60406
\$1TIVSKT.mak	C:\\$RECYCLE.BIN\1-5-21-1964354803-3058...	Makefile	11/22/2018, 14:38:05.56468...	11/22/2018, 14:38:05.56468
\$1UHM8K7	C:\\$RECYCLE.BIN\1-5-21-1964354803-3058...	File	11/22/2018, 14:38:05.56468...	11/22/2018, 14:38:05.56468
\$1VHV9AW.pdf	C:\\$RECYCLE.BIN\1-5-21-1964354803-3058...	PDF Document	11/22/2018, 14:38:05.56468...	11/22/2018, 14:38:05.56468
\$1VZDUZE	C:\\$RECYCLE.BIN\1-5-21-1964354803-3058...	File	11/22/2018, 14:38:05.56468...	11/22/2018, 14:38:05.56468
\$1XDR9K4.txt	C:\\$RECYCLE.BIN\1-5-21-1964354803-3058...	Text Document	11/22/2018, 14:38:05.56468...	11/22/2018, 14:38:05.56468
\$1YVQA4N.OSFHashSet	C:\\$RECYCLE.BIN\1-5-21-1964354803-3058...	OSF Hash Set	11/22/2018, 14:38:05.56468...	11/22/2018, 14:38:05.56468
\$1ZL707B	C:\\$RECYCLE.BIN\1-5-21-1964354803-3058...	File	11/22/2018, 14:38:05.56468...	11/22/2018, 14:38:05.56468
\$1R69P590.docx	C:\\$RECYCLE.BIN\1-5-21-1964354803-3058...	Microsoft Word Document	11/22/2018, 14:38:05.56468...	11/22/2018, 14:38:05.56468
\$1R6PYUBK.pdf	C:\\$RECYCLE.BIN\1-5-21-1964354803-3058...	PDF Document	11/22/2018, 14:38:05.56468...	11/22/2018, 14:38:05.56468
\$1RYYWVW.jpg	C:\\$RECYCLE.BIN\1-5-21-1964354803-3058...	Image	11/22/2018, 14:38:05.56468...	11/22/2018, 14:38:05.56468



Lookup File in Hash Set



Filename



MD5

SHA-1

SHA-256

Progress

Files Hashed

Matches

Hash Set [ProjectVIC-4-8-29-Full](#)

File	Folder	Size	MD5	SHA1	SHA256
\$RXDR\$4.txt	C:\\$RECYCLE.BIN\S-1-5-21-196435...	0 Bytes	D41D8CD98F00...	DA39A3EE5E6...	N/A
bindingInfo.tmp	C:\inetpub\temp\appPools	0 Bytes	D41D8CD98F00...	DA39A3EE5E6...	N/A
zoom_autocompl...	C:\inetpub\wwwroot\zoomaspx	0 Bytes	D41D8CD98F00...	DA39A3EE5E6...	N/A
install .pfx files to ...	C:\Limpet\SignTool	0 Bytes	D41D8CD98F00...	DA39A3EE5E6...	N/A

