Plug Me In Renzik, Autopsy Plugins Now And In The Future.

Mark McKinnon

DAVENPORT UNIVERSITY

About Me

Assistant Professor

25+ years in IT field

Developed 25+ Autopsy Modules

10+ years in Digital Forensics field

BS in Computer Science

MS in Computer Information Systems

CCE, GCFA, GCIH Certifications

Where Can You Get The Plugins?

All the plugins can be downloaded from my github repository

https://github.com/markmckinnon/Autopsy-Plugins

OSDFCon 2016 Plugins Recap

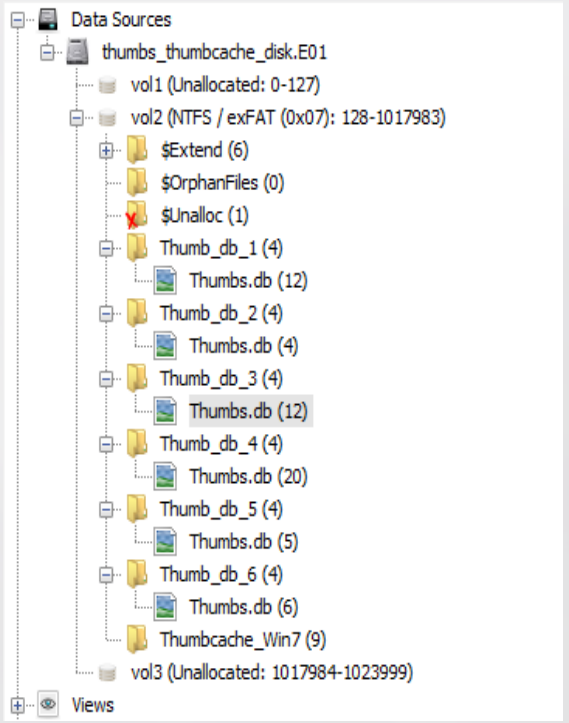
- Evtx Log Parser
- SAMParse
- JL parser
- Amcache Parser
- SRUDB database
- Webcache
- Parse SQLiteDB
- Parse SQLite Deleted Records
- Shimcache
- Plist parser
- Shellbags
- USNJ

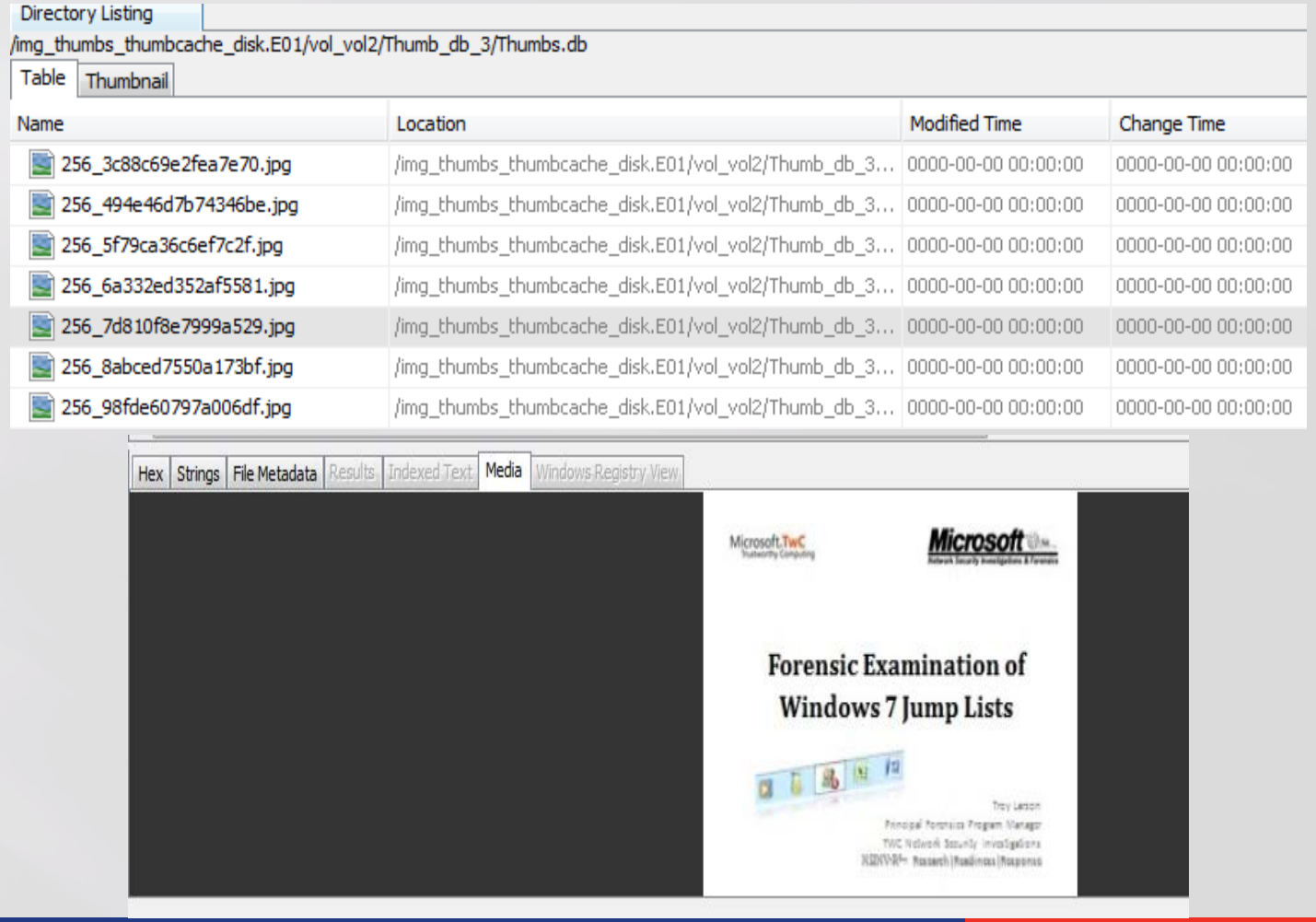
OSDFCon 2017 Plugins Created

- Volatility
- Plaso
- File History
- Safari OSX
- Cuckoo
- CCM_Recently_Used
- FS Events Mac
- Mac OSX Recents
- Volume Shadow
- Thumbs DB
- Thumbcache
- Process EVTX files By Event Id

Thumbs and Thumbcache Plugin

Searches for Thumbs.db/Thumbcache file(s), extracts them and adds them back into Autopsy as a derived file.



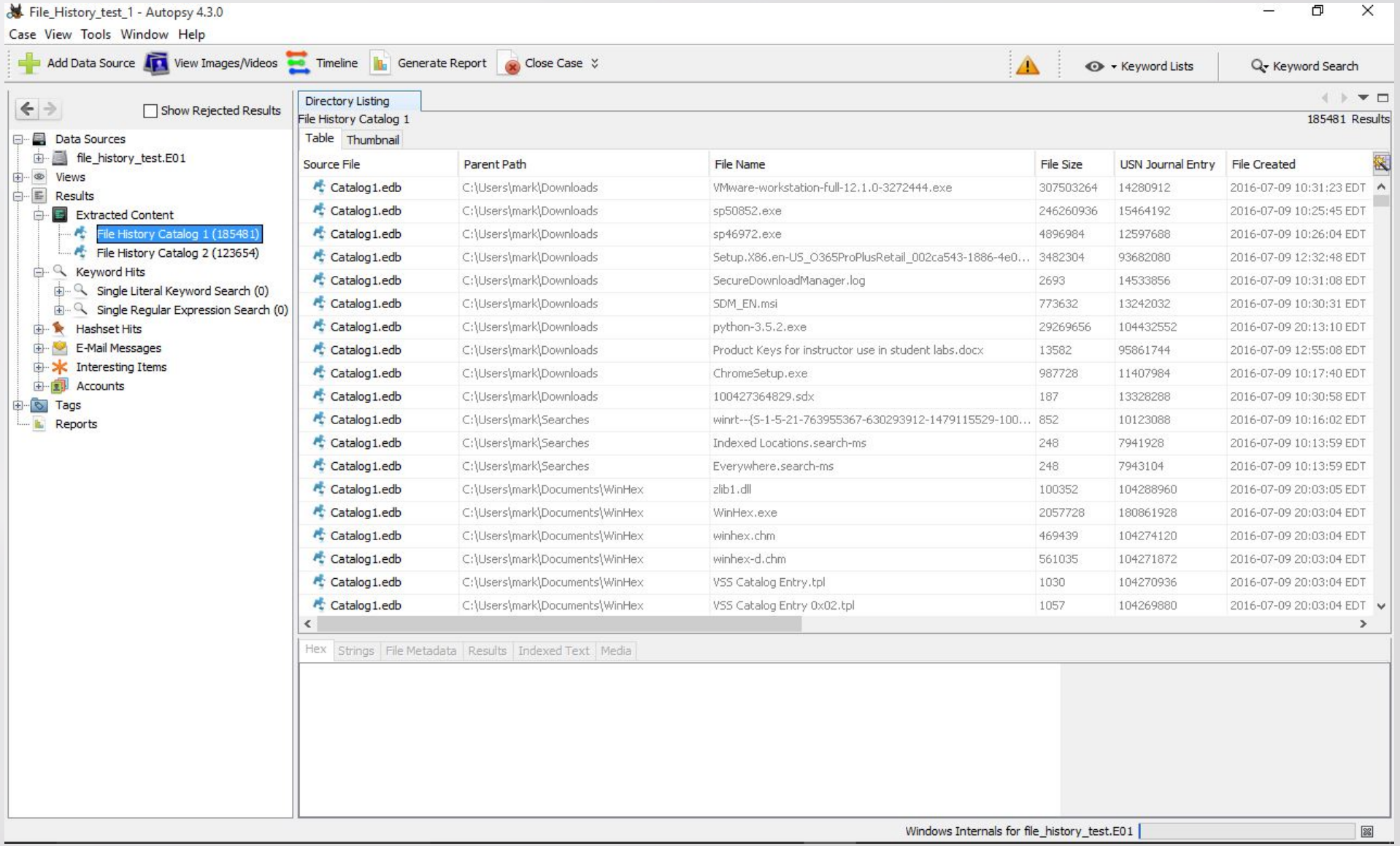


File History Plugin

Based on the research by Ken Johnson.

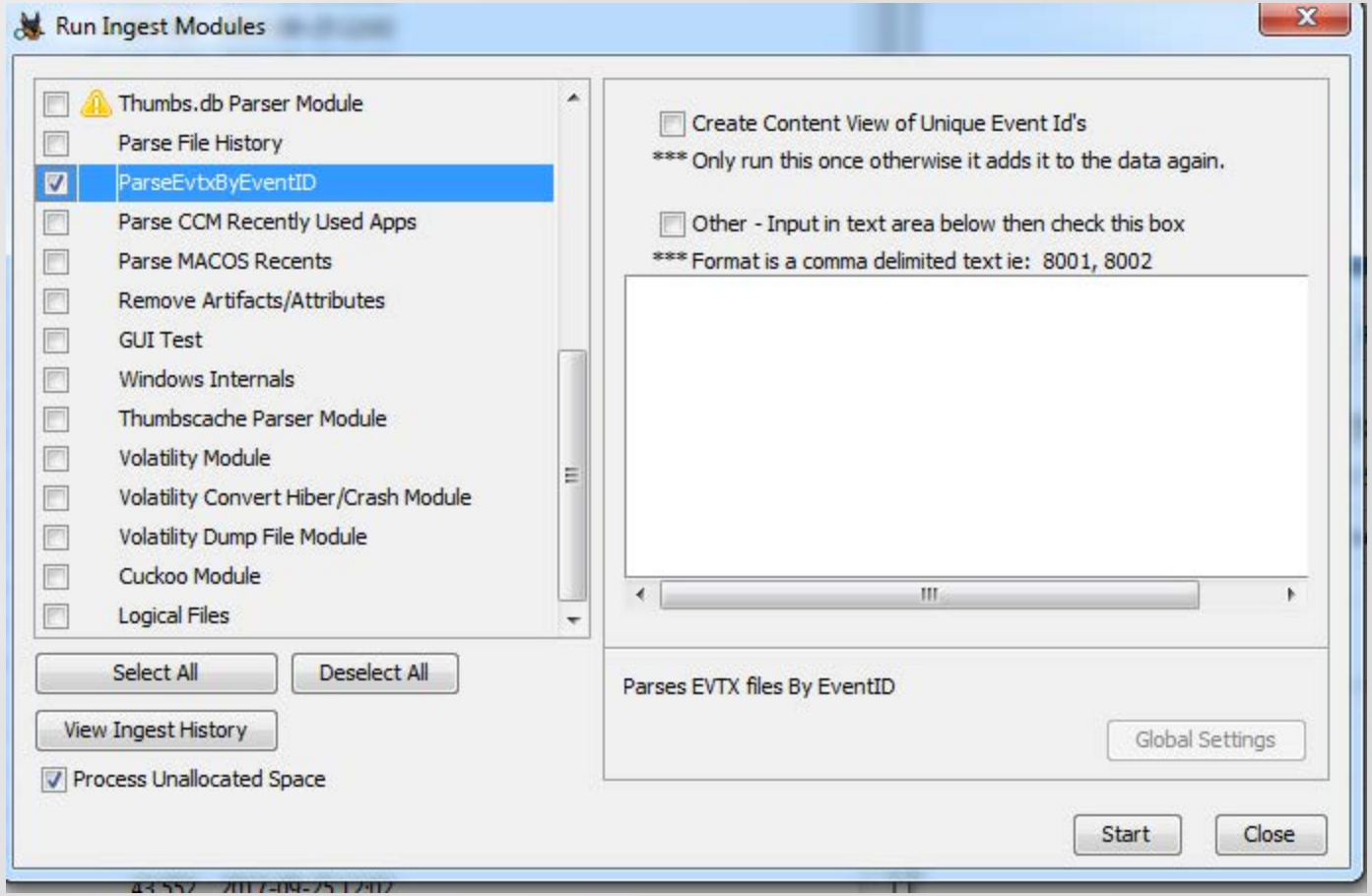
Parses the Catalog1.edb and the Catalog2.edb for each user

File History Plugin

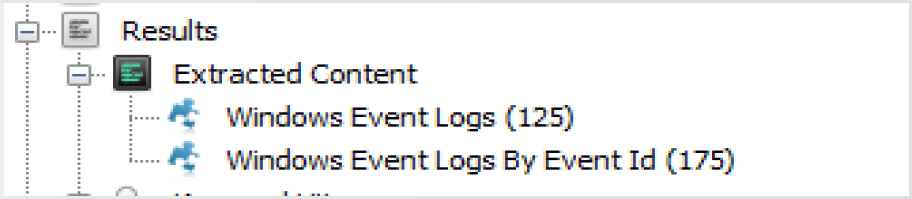


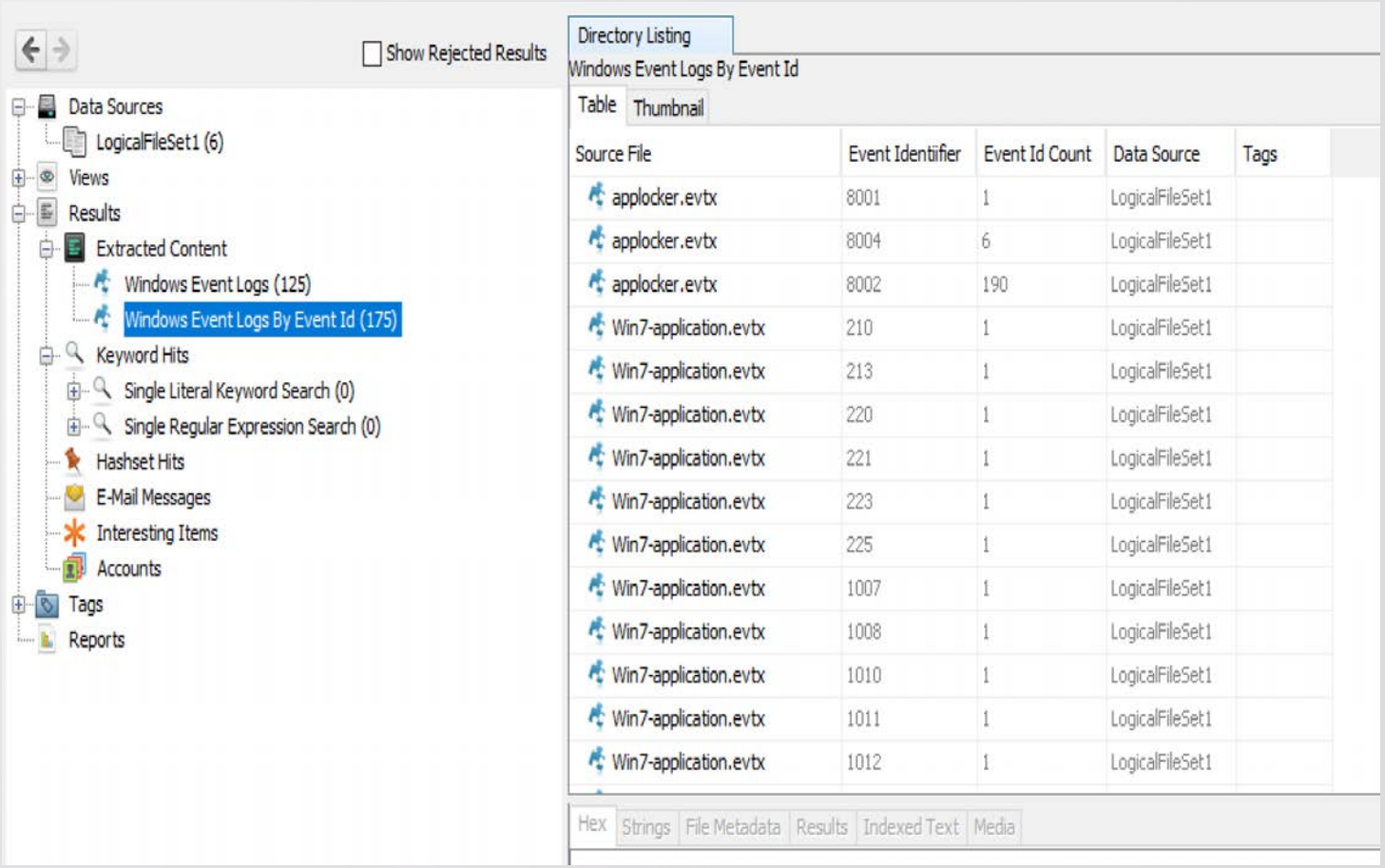
Process EVTX Files By Event Id Plugin

Parses *all* event logs and provides a list of unique events found in each event log. You can then cherry pick the events of interest.



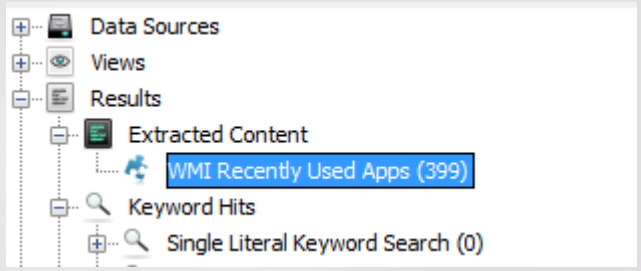
Process EVTX Files By Event Id Plugin





CCM Recently Used Plugin

Based on James Habben's post about recently used apps.



Directory Listing

WMI Recently Used Apps

Table | Thumbnail

Source File	Path	Explorer File Name	File Size	User ID	Last Used Time	Time Zone Offset	Launch Count
OBJECTS.DATA	C:\Program Files\7-Zip\	7z.exe	446976	mckinnon	2017-10-03 10:47:17 EDT	="+000"	2
OBJECTS.DATA	C:\Program Files\7-Zip\	7zFM.exe	839168	mckinnon	2017-10-05 11:47:51 EDT	="+000"	565
OBJECTS.DATA	C:\Program Files\7-Zip\	7zG.exe	553984	mckinnon	2017-10-03 13:14:43 EDT	="+000"	290
OBJECTS.DATA	C:\Program Files\AccessData\FTK Imager\	ADIso.exe	63848	mckinnon	2017-07-11 17:53:19 EDT	="+000"	7
OBJECTS.DATA	C:\Program Files (x86)\Common Files\Apple\Apple Applicati...	APSDaemon.exe	43816	mckinnon	2017-09-18 13:32:30 EDT	="+000"	30
OBJECTS.DATA	C:\Program Files (x86)\Common Files\Aimersoft\Aimersoft ...	ASHelper.exe	2138272	mckinnon	2017-10-05 11:47:51 EDT	="+000"	30
OBJECTS.DATA	C:\Program Files (x86)\Adobe\Reader 11.0\Reader\	AcroRd32.exe	1550872	mckinnon	2017-10-03 14:11:42 EDT	="+000"	1114
OBJECTS.DATA	C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\	AdobeARM.exe	1160408	mckinnon	2017-09-18 13:32:37 EDT	="+000"	6

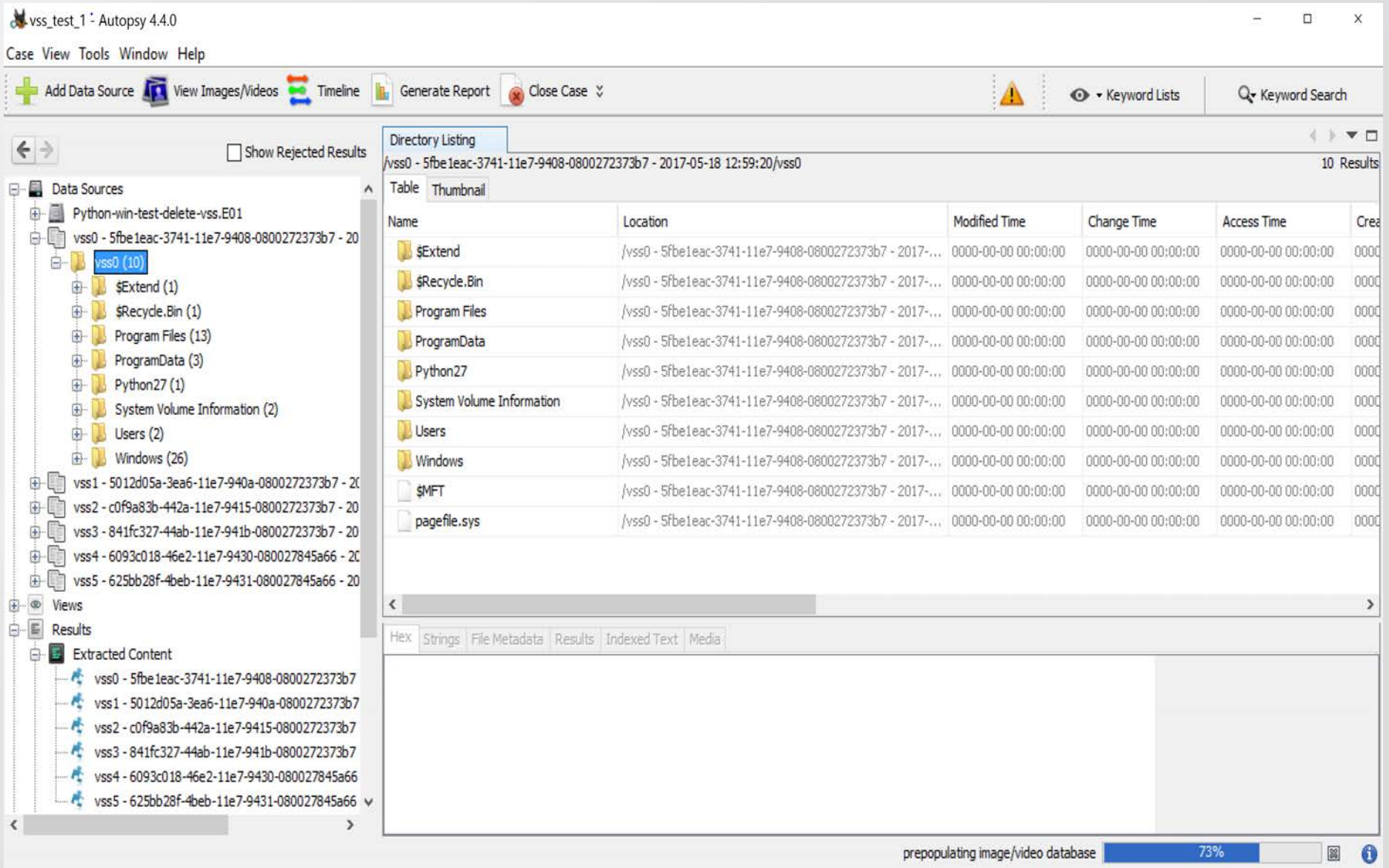
Volume Shadow Plugin

Parses Volume Shadow using DFVFS

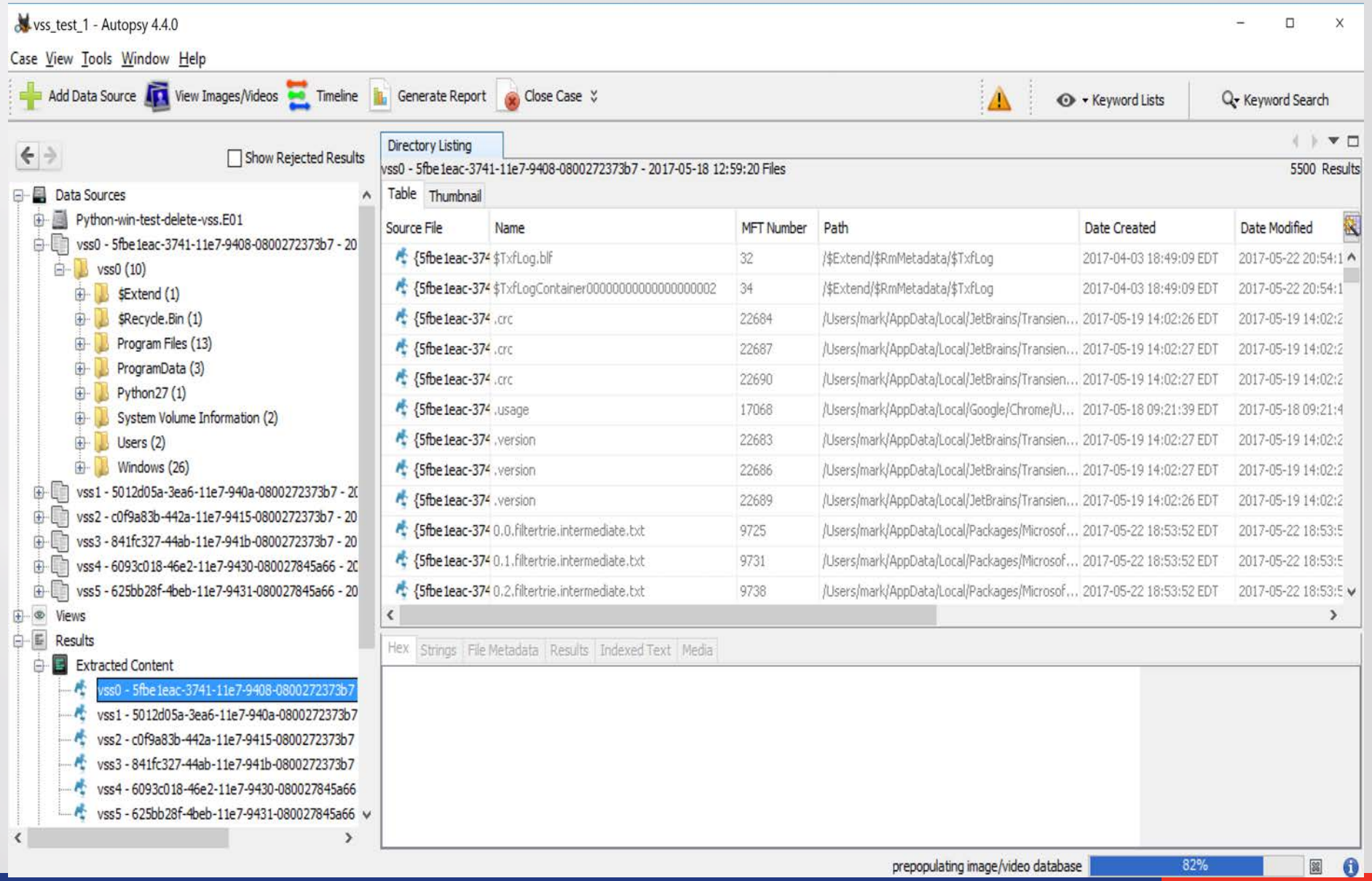
Creates a new logical file data source and adds the extracted content to it for each Volume Shadow. This way you can run other plugins against that data source.

In the Extracted Content view is a list of all the files that were extracted.

Volume Shadow Plugin

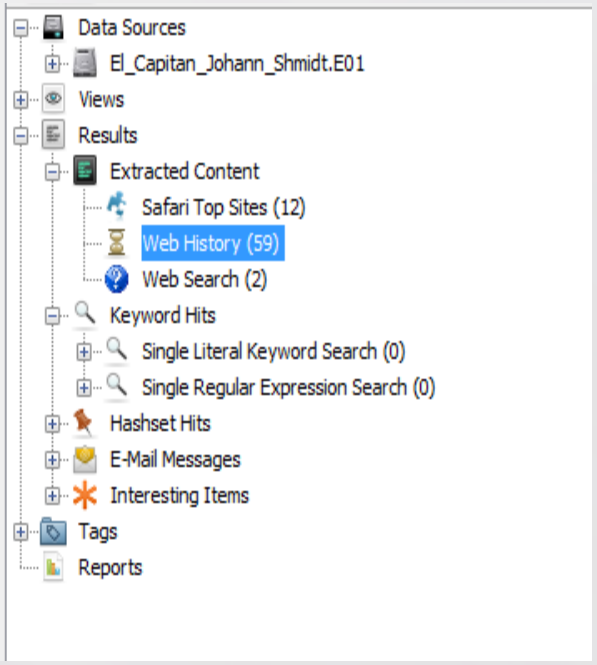


Volume Shadow Plugin



Safari OSX Plugin

Parses the Safari browser information from Mac os. Collects data from History, Bookmarks, Downloads, Last Session, Recently Closed Tabs and Top Sites and Web Searches.



Safari Top Sites

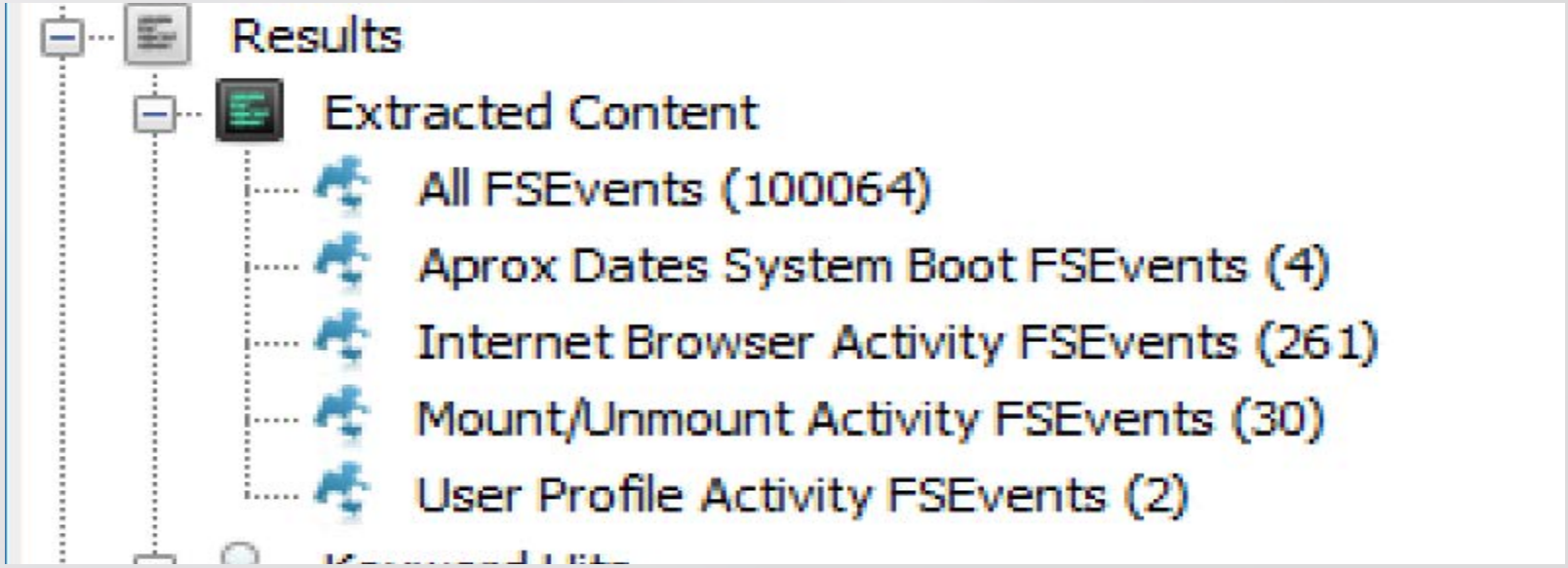
Table | Thumbnail

Source File	Username	URL	Title	Site Last Modified
TopSites.plist	redskull	http://www.apple.com/startpage/		2017-04-29 22:39:46 EDT
TopSites.plist	redskull	https://www.icloud.com/	iCloud	0000-00-00 00:00:00
TopSites.plist	redskull	https://www.yahoo.com/	Yahoo	0000-00-00 00:00:00
TopSites.plist	redskull	https://www.bing.com/	Bing	0000-00-00 00:00:00
TopSites.plist	redskull	https://www.google.com/?client=safari&channel=mac_bm	Google	0000-00-00 00:00:00
TopSites.plist	redskull	https://www.wikipedia.org/	Wikipedia	0000-00-00 00:00:00
TopSites.plist	redskull	https://www.facebook.com/	Facebook	0000-00-00 00:00:00
TopSites.plist	redskull	https://twitter.com/	Twitter	0000-00-00 00:00:00
TopSites.plist	redskull	https://www.linkedin.com/	LinkedIn	0000-00-00 00:00:00
TopSites.plist	redskull	http://www.weather.com/	The Weather Channel	0000-00-00 00:00:00
TopSites.plist	redskull	http://www.yelp.com/	Yelp	0000-00-00 00:00:00
TopSites.plist	redskull	http://www.tripadvisor.com/	TripAdvisor	0000-00-00 00:00:00

FS Events Mac os Plugin

Based on the work of Nicole Ibrahim.

Once the events are parsed it groups the data based on different events. This is controlled using a SQLite database that defines the events, this allows the user to define more events in the future.



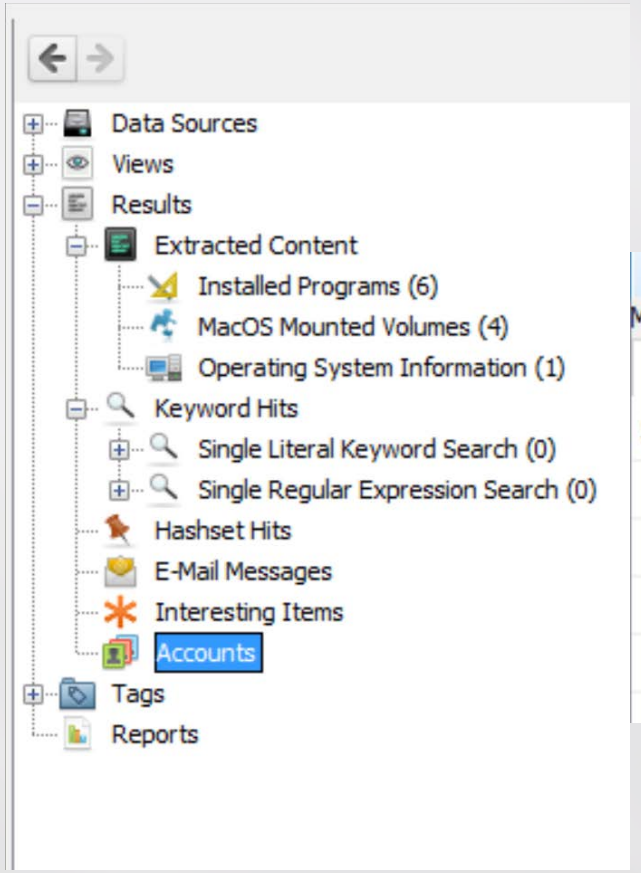
Mac OSX Recents

This plugin will parse plists and SQLite databases on the system.

This uses a database of defined artifacts in a SQLite database so it can be expanded for future use.

Artifact Type	File Type	OS version
OS version	Plist	10.6 – 10.12
Install History	Plist	10.12
Accounts	SQLite	10.11 – 10.12
Mounted Volumes	Plist	10.9 – 10.12

Mac OSX Recents



Listing

Installed Programs

Table | Thumbnail

Source File	Display Version	Program Name	Installation Method	Data Source	Tags
InstallHistory.plist		OS X	OS X Installer	El_Capitan_Johann_Shmidt.E01	
InstallHistory.plist	10.1.6	VMware Tools	Installer	El_Capitan_Johann_Shmidt.E01	
InstallHistory.plist	4.3.2	Twitter	storedownloadd	El_Capitan_Johann_Shmidt.E01	
InstallHistory.plist	0.2.4239	WhatsApp	storedownloadd	El_Capitan_Johann_Shmidt.E01	
InstallHistory.plist	110	Gatekeeper Configuration Data	softwareupdated	El_Capitan_Johann_Shmidt.E01	
InstallHistory.plist	4.22	Chinese Word List Update	softwareupdated	El_Capitan_Johann_Shmidt.E01	

Listing

MacOS Mounted Volumes

Table | Thumbnail

Source File	MAC Mounted Volume	Data Source	Tags
com.apple.sidebarlists.plist	Computer	El_Capitan_Johann_Shmidt.E01	
com.apple.sidebarlists.plist	EL_CAPITAN	El_Capitan_Johann_Shmidt.E01	
com.apple.sidebarlists.plist	Install OS X El Capitan	El_Capitan_Johann_Shmidt.E01	
com.apple.sidebarlists.plist	Network	El_Capitan_Johann_Shmidt.E01	

Listing

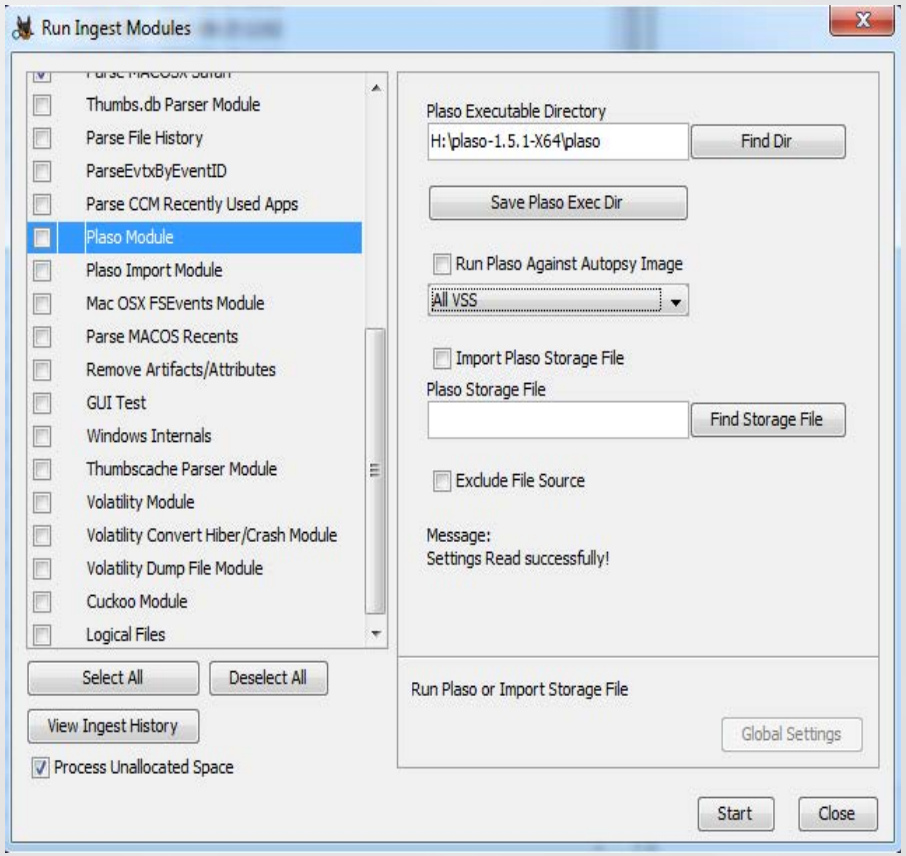
Operating System Information

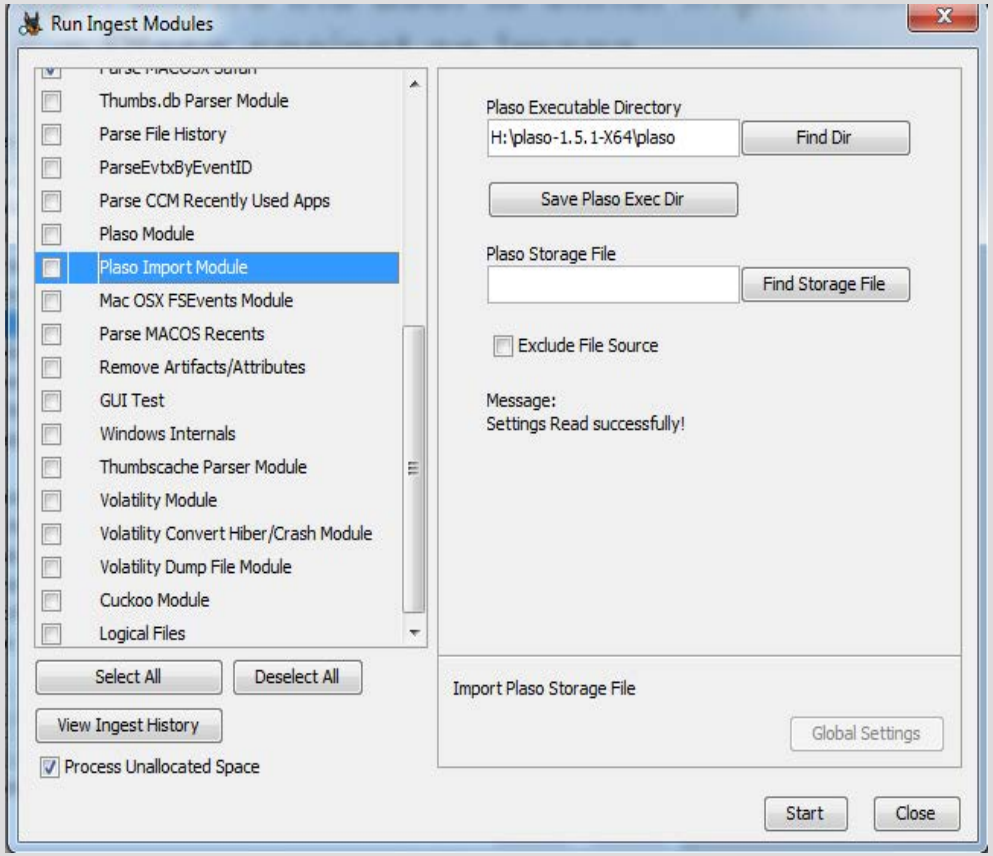
Table | Thumbnail

Source File	Name	Version	MAC Build Version	Data Source
SystemVersion.plist	Mac OS X	10.11.6	15G31	El_Capitan_Johann_Shmidt.E01

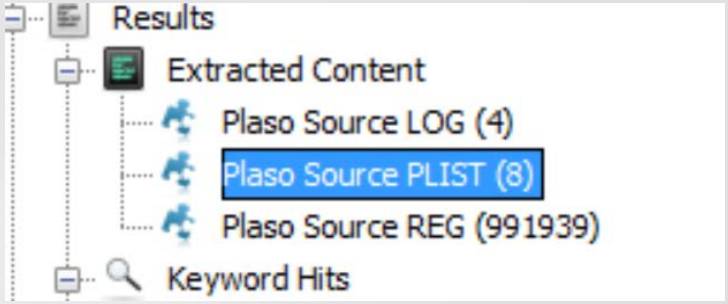
Plaso Plugin

This plugin allows the user to either import data from a plaso run or run plaso against an Image.





Plaso Plugin



Listing

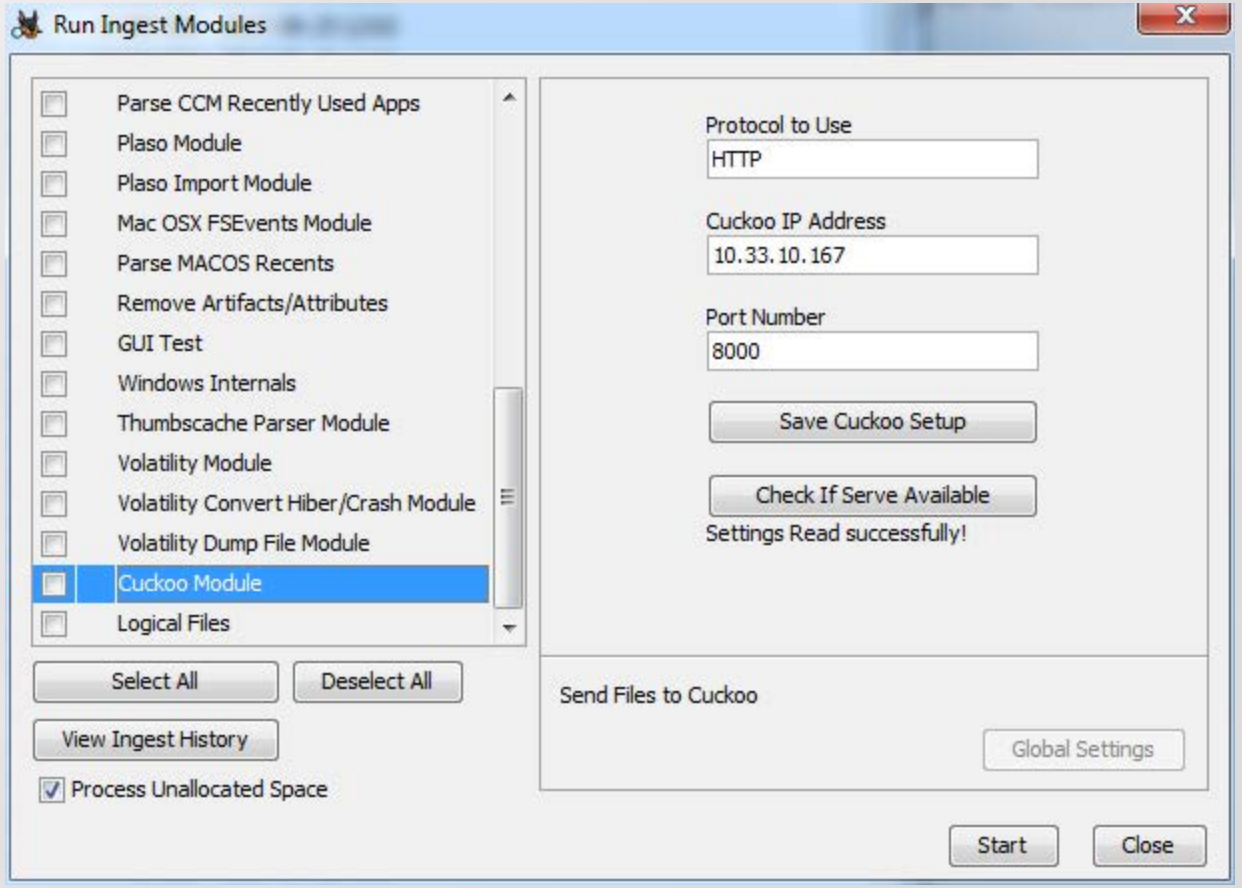
Plaso Source PLIST

Table | Thumbnail

Source File	Plaso Source Type	Plaso Type	Plaso Description	Plaso File Name
Plaso_Import.db3	Plist Entry	Content Modification Time	/item/ Installation of [OS X] using [OS X Installer]. Packag...	/Library/Receipts/InstallHistory.plist
Plaso_Import.db3	Plist Entry	Content Modification Time	/Stores/ Spotlight Volume 083A296C-CA2B-4BC3-9483-2C3...	/.Spotlight-V100/VolumeConfiguration.
Plaso_Import.db3	Plist Entry	Content Modification Time	/item/ Installation of [VMware Tools 10.1.6] using [Installer...	/Library/Receipts/InstallHistory.plist
Plaso_Import.db3	Plist Entry	Content Modification Time	/item/ Installation of [Twitter 4.3.2] using [storedownloadd...	/Library/Receipts/InstallHistory.plist
Plaso_Import.db3	Plist Entry	Content Modification Time	/item/ Installation of [WhatsApp 0.2.4239] using [storedo...	/Library/Receipts/InstallHistory.plist
Plaso_Import.db3	Plist Entry	Content Modification Time	/item/ Installation of [Gatekeeper Configuration Data 110] ...	/Library/Receipts/InstallHistory.plist
Plaso_Import.db3	Plist Entry	Content Modification Time	/item/ Installation of [Chinese Word List Update 4.22] usin...	/Library/Receipts/InstallHistory.plist
Plaso_Import.db3	Plist Entry	Content Modification Time	/item/ Installation of [CoreLSKD Configuration Data 8] usin...	/Library/Receipts/InstallHistory.plist

Cuckoo Plugin

This plugin will allow you to send tagged items to a Cuckoo server.



Volatility Plugin General

This plugin allows you to run Volatility against a memory Image.

The memory image needs to be added as a Logical File.

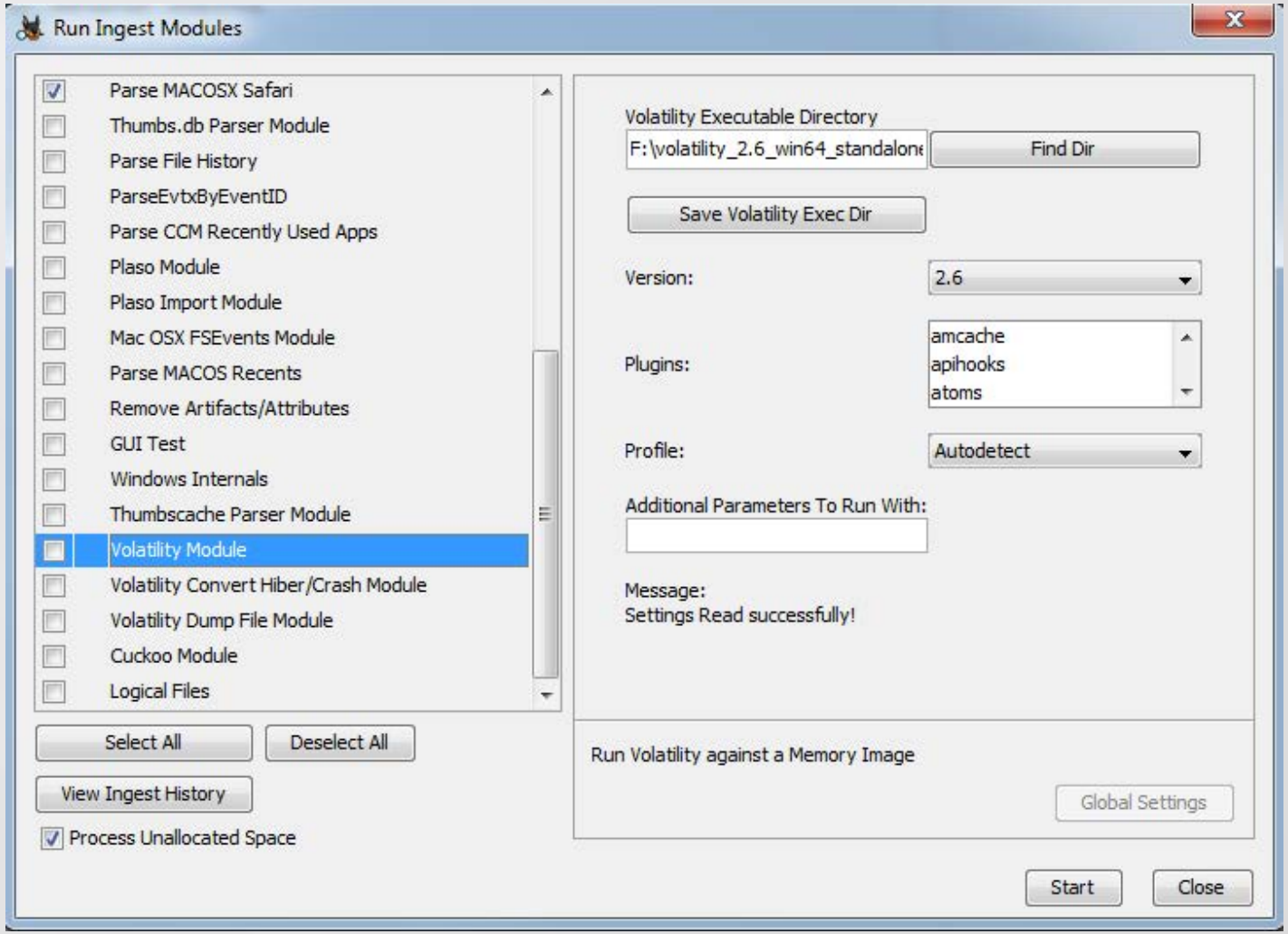
This can run the Volatility executable or the Python script

Uses Version 2.5 or 2.6 of Volatility.

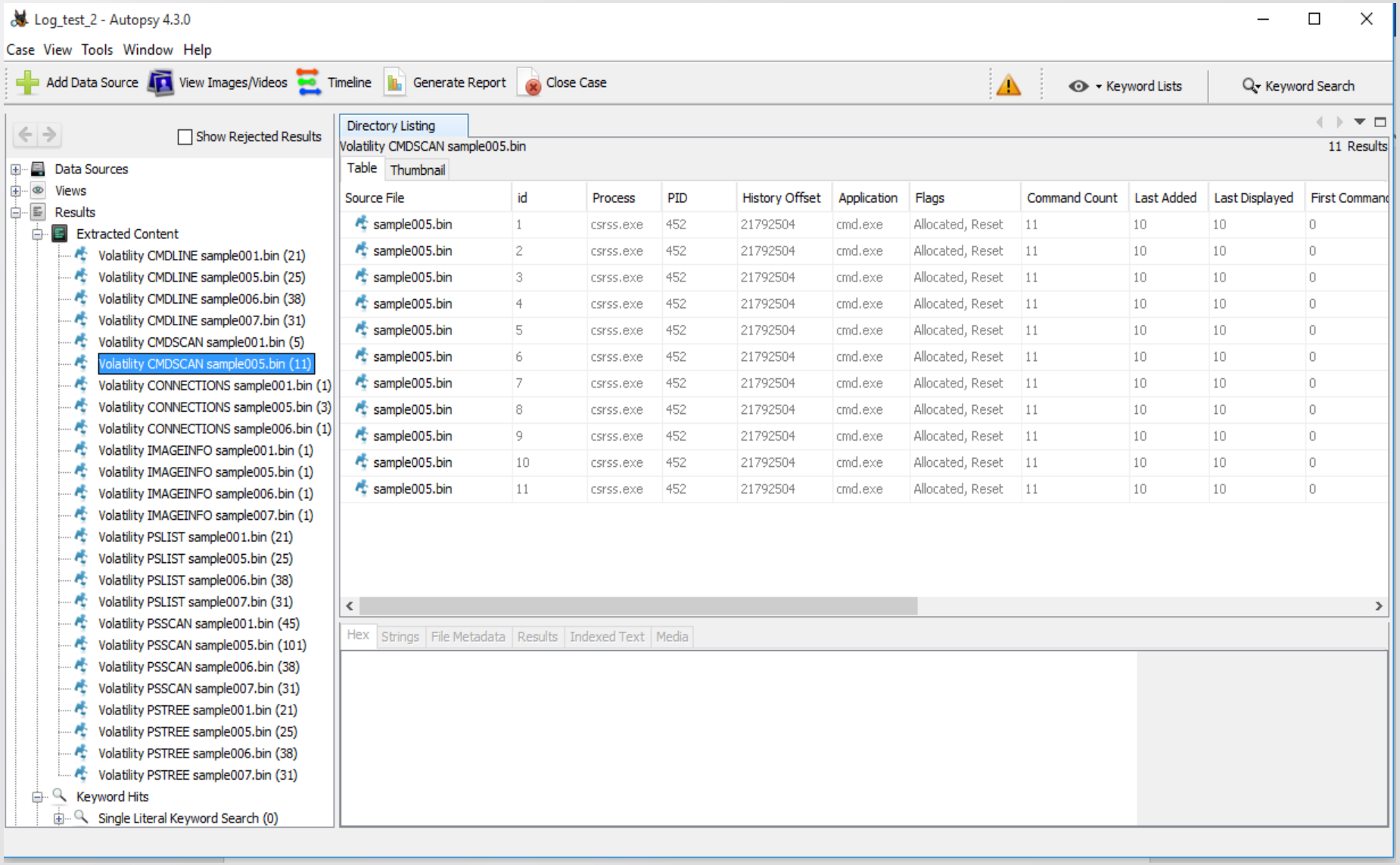
Only uses stock plugins. Plugin info is stored in SQLite database so other plugins may be added by user.

Autodetect will only run once. If Autodetect is selected again it will pull the memory profile from what was saved from the first run.

Volatility Plugin

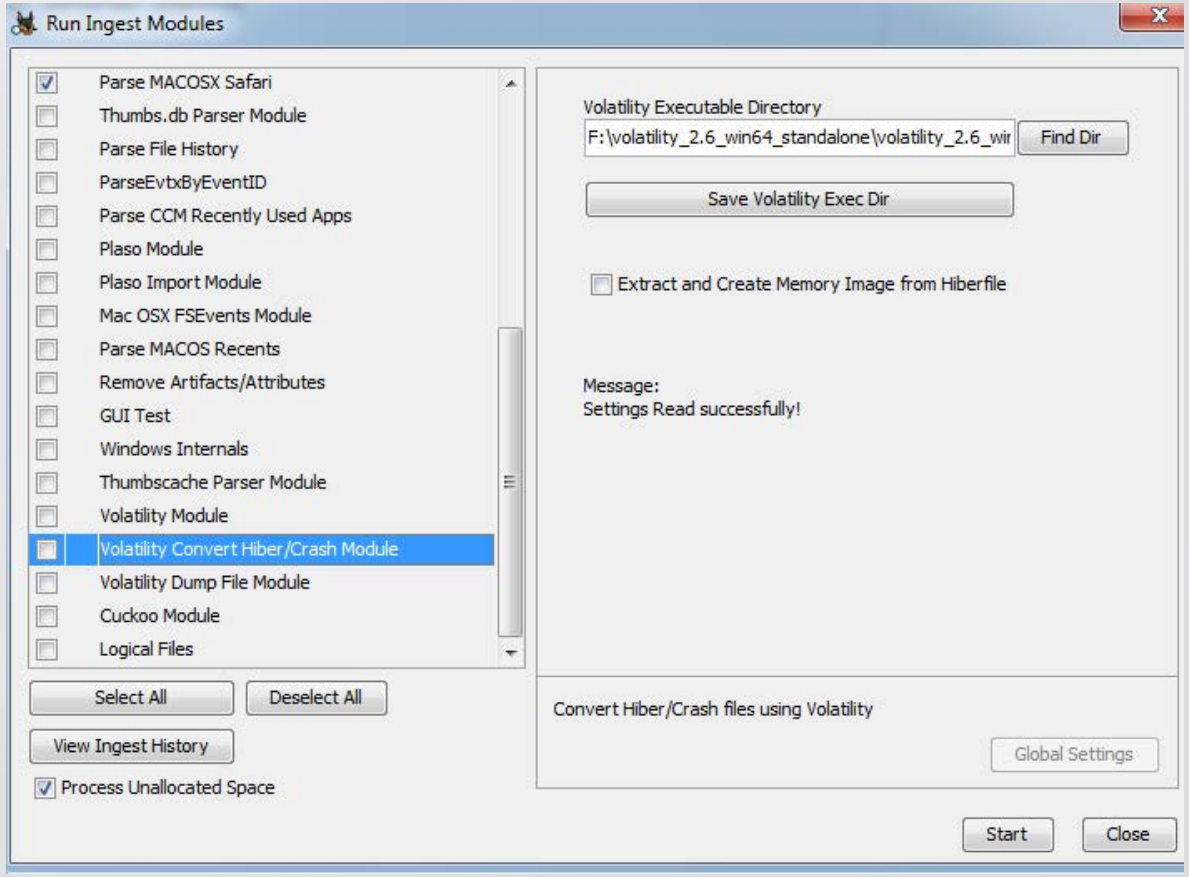


Volatility Plugin



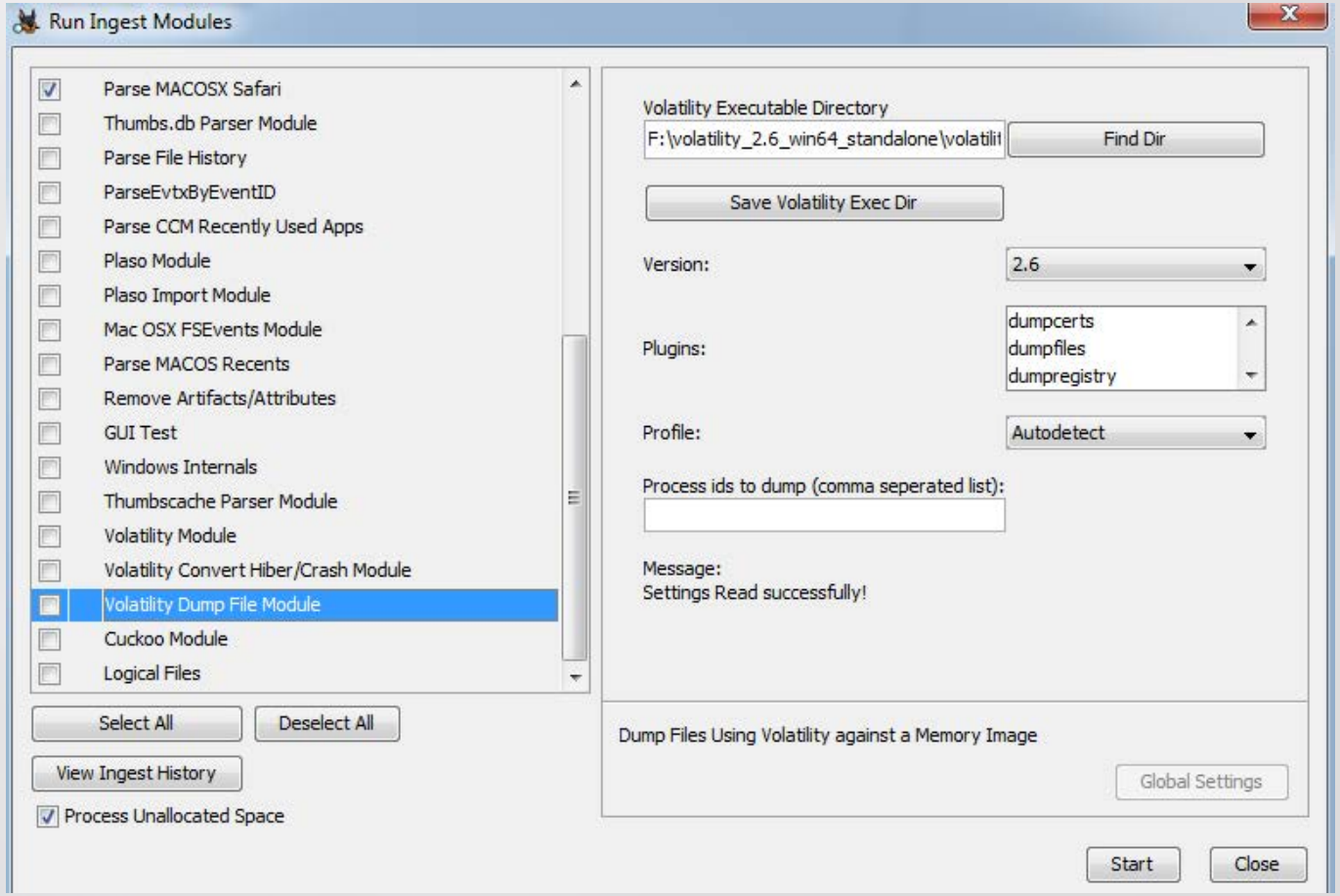
Volatility Dump Hiber File Plugin

To be run against a disk image. Will use Volatility to convert the hiberfil.sys and store as a Logical File to run the Volatility plugins against.

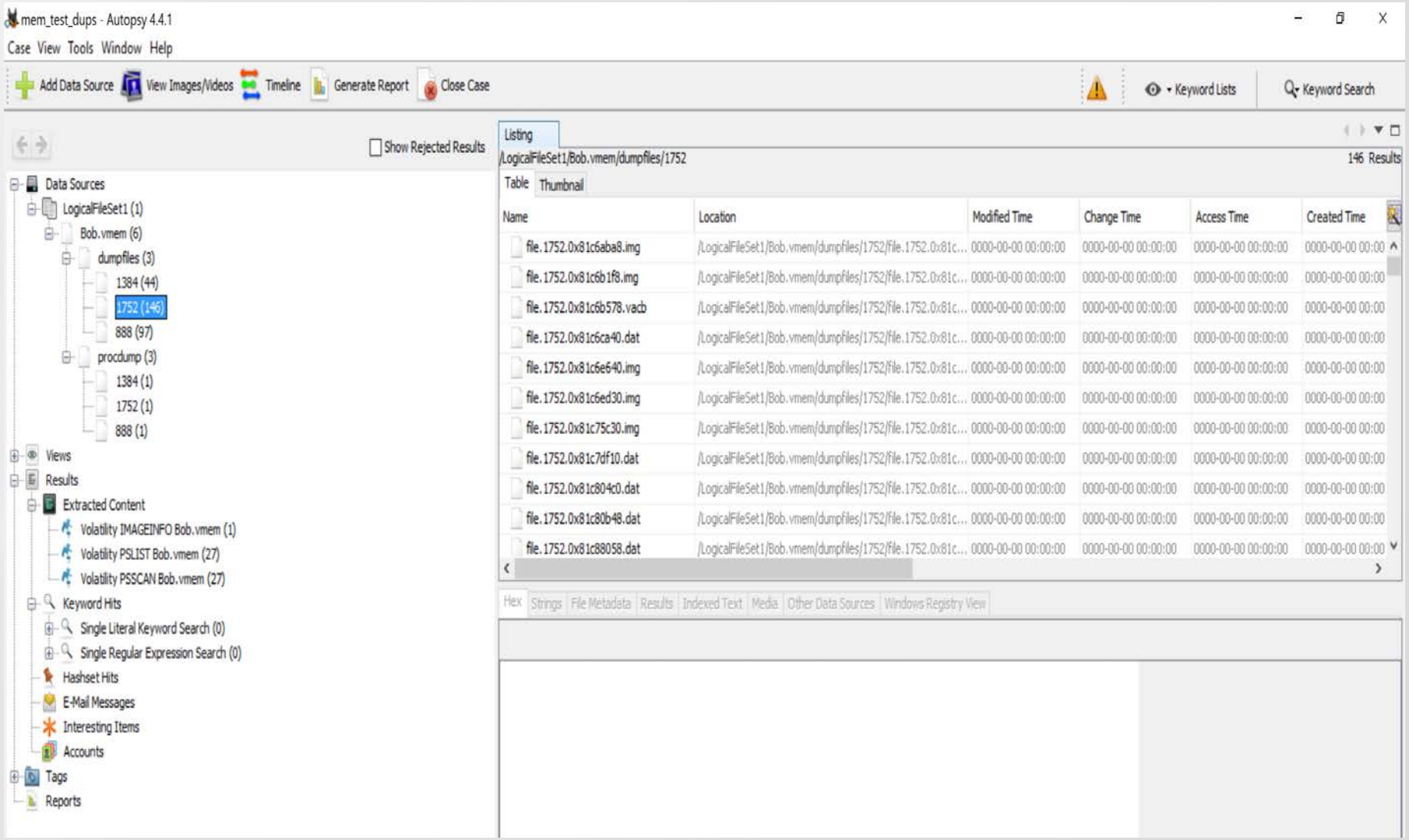


Volatility Dump Plugin

Dumps files to Module Output directory then adds them back into Autopsy as a derived file in a directory structure under the memory image.



Volatility Dump Plugin



Future – What's Next

What do you want to see?

More data processing plugin's?

More content viewer's?

Help shape the future of plugin development.

References

File History - https://forensic4cast.com/2016/04/ken-johnson/

CCM Recently Used - http://blog.4n6ir.com/2017/02/secret-archives-of-execution-evidence.html

FS Events Mac - http://nicoleibrahim.com/apple-fsevents-forensics/

Volume Shadow - http://dfvfs.readthedocs.io/en/latest/

Questions?