

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

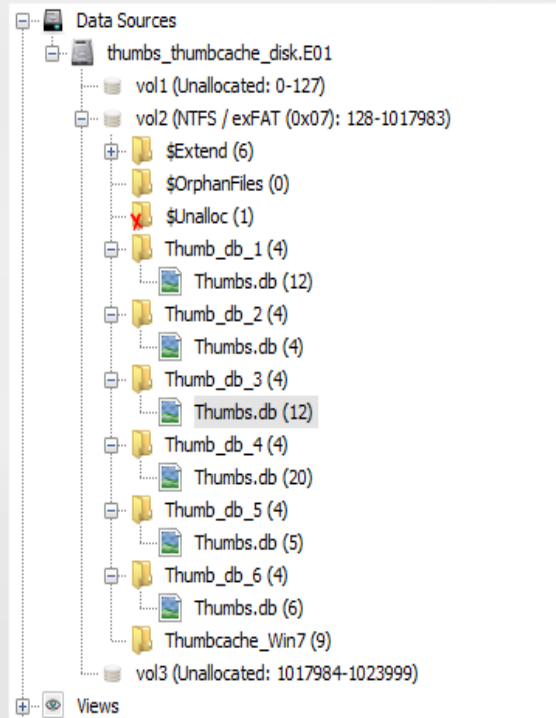
- Evtx Log Parser
- SAMParse
- JL parser
- Amcache Parser
- SRUDB database
- Webcache
- Parse SQLiteDB
- Parse SQLite Deleted Records
- Shimcache
- Plist parser
- Shellbags
- USNJ

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.



Directory Listing

/img_thumbs_thumbcache_disk.E01/vol_vol2/Thumb_db_3/Thumbs.db

Table Thumbnail

Name	Location	Modified Time	Change Time
256_3c88c69e2fea7e70.jpg	/img_thumbs_thumbcache_disk.E01/vol_vol2/Thumb_db_3...	0000-00-00 00:00:00	0000-00-00 00:00:00
256_494e46d7b74346be.jpg	/img_thumbs_thumbcache_disk.E01/vol_vol2/Thumb_db_3...	0000-00-00 00:00:00	0000-00-00 00:00:00
256_5f79ca36c6ef7c2f.jpg	/img_thumbs_thumbcache_disk.E01/vol_vol2/Thumb_db_3...	0000-00-00 00:00:00	0000-00-00 00:00:00
256_6a332ed352af5581.jpg	/img_thumbs_thumbcache_disk.E01/vol_vol2/Thumb_db_3...	0000-00-00 00:00:00	0000-00-00 00:00:00
256_7d810f8e7999a529.jpg	/img_thumbs_thumbcache_disk.E01/vol_vol2/Thumb_db_3...	0000-00-00 00:00:00	0000-00-00 00:00:00
256_8abced7550a173bf.jpg	/img_thumbs_thumbcache_disk.E01/vol_vol2/Thumb_db_3...	0000-00-00 00:00:00	0000-00-00 00:00:00
256_98fde60797a006df.jpg	/img_thumbs_thumbcache_disk.E01/vol_vol2/Thumb_db_3...	0000-00-00 00:00:00	0000-00-00 00:00:00



File History Plugin

Based on the research by Ken Johnson.

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

File History Plugin

File_History_test_1 - Autopsy 4.3.0

Case View Tools Window Help

+ Add Data Source View Images/Videos Timeline Generate Report Close Case

Keyword Lists Keyword Search

Directory Listing

File History Catalog 1 185481 Results

Table Thumbnail

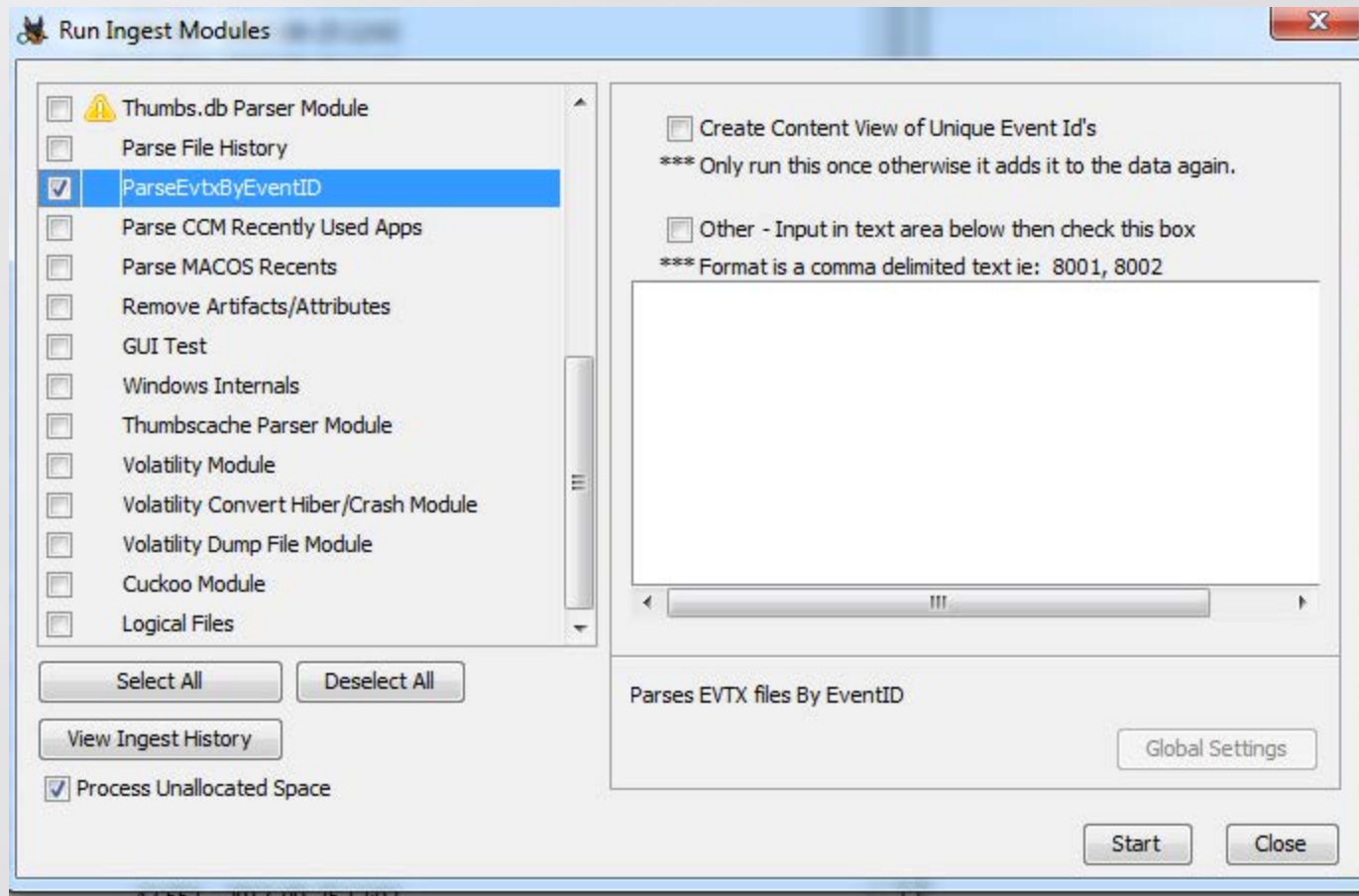
Source File	Parent Path	File Name	File Size	USN Journal Entry	File Created
Catalog1.edb	C:\Users\mark\Downloads	VMware-workstation-full-12.1.0-3272444.exe	307503264	14280912	2016-07-09 10:31:23 EDT
Catalog1.edb	C:\Users\mark\Downloads	sp50852.exe	246260936	15464192	2016-07-09 10:25:45 EDT
Catalog1.edb	C:\Users\mark\Downloads	sp46972.exe	4896984	12597688	2016-07-09 10:26:04 EDT
Catalog1.edb	C:\Users\mark\Downloads	Setup.X86.en-US_O365ProPlusRetail_002ca543-1886-4e0...	3482304	93682080	2016-07-09 12:32:48 EDT
Catalog1.edb	C:\Users\mark\Downloads	SecureDownloadManager.log	2693	14533856	2016-07-09 10:31:08 EDT
Catalog1.edb	C:\Users\mark\Downloads	SDM_EN.msi	773632	13242032	2016-07-09 10:30:31 EDT
Catalog1.edb	C:\Users\mark\Downloads	python-3.5.2.exe	29269656	104432552	2016-07-09 20:13:10 EDT
Catalog1.edb	C:\Users\mark\Downloads	Product Keys for instructor use in student labs.docx	13582	95861744	2016-07-09 12:55:08 EDT
Catalog1.edb	C:\Users\mark\Downloads	ChromeSetup.exe	987728	11407984	2016-07-09 10:17:40 EDT
Catalog1.edb	C:\Users\mark\Downloads	100427364829.sdx	187	13328288	2016-07-09 10:30:58 EDT
Catalog1.edb	C:\Users\mark\Searches	wintr--{5-1-5-21-763955367-630293912-1479115529-100...	852	10123088	2016-07-09 10:16:02 EDT
Catalog1.edb	C:\Users\mark\Searches	Indexed Locations.search-ms	248	7941928	2016-07-09 10:13:59 EDT
Catalog1.edb	C:\Users\mark\Searches	Everywhere.search-ms	248	7943104	2016-07-09 10:13:59 EDT
Catalog1.edb	C:\Users\mark\Documents\WinHex	zlib1.dll	100352	104288960	2016-07-09 20:03:05 EDT
Catalog1.edb	C:\Users\mark\Documents\WinHex	WinHex.exe	2057728	180861928	2016-07-09 20:03:04 EDT
Catalog1.edb	C:\Users\mark\Documents\WinHex	winhex.chm	469439	104274120	2016-07-09 20:03:04 EDT
Catalog1.edb	C:\Users\mark\Documents\WinHex	winhex-d.chm	561035	104271872	2016-07-09 20:03:04 EDT
Catalog1.edb	C:\Users\mark\Documents\WinHex	V55 Catalog Entry.tpl	1030	104270936	2016-07-09 20:03:04 EDT
Catalog1.edb	C:\Users\mark\Documents\WinHex	V55 Catalog Entry 0x02.tpl	1057	104269880	2016-07-09 20:03:04 EDT

Hex Strings File Metadata Results Indexed Text Media

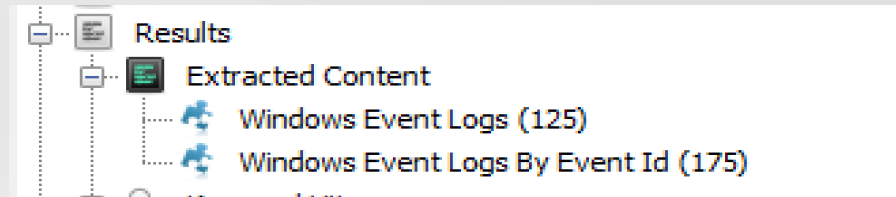
Windows Internals for file_history_test.E01

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



← → ☐ Show Rejected Results

Directory Listing

Windows Event Logs By Event Id

Table Thumbnail

Source File	Event Identifier	Event Id Count	Data Source	Tags
aplocker.evtx	8001	1	LogicalFileSet1	
aplocker.evtx	8004	6	LogicalFileSet1	
aplocker.evtx	8002	190	LogicalFileSet1	
Win7-application.evtx	210	1	LogicalFileSet1	
Win7-application.evtx	213	1	LogicalFileSet1	
Win7-application.evtx	220	1	LogicalFileSet1	
Win7-application.evtx	221	1	LogicalFileSet1	
Win7-application.evtx	223	1	LogicalFileSet1	
Win7-application.evtx	225	1	LogicalFileSet1	
Win7-application.evtx	1007	1	LogicalFileSet1	
Win7-application.evtx	1008	1	LogicalFileSet1	
Win7-application.evtx	1010	1	LogicalFileSet1	
Win7-application.evtx	1011	1	LogicalFileSet1	
Win7-application.evtx	1012	1	LogicalFileSet1	

Hex Strings File Metadata Results Indexed Text Media

Data Sources

- LogicalFileSet1 (6)

Views

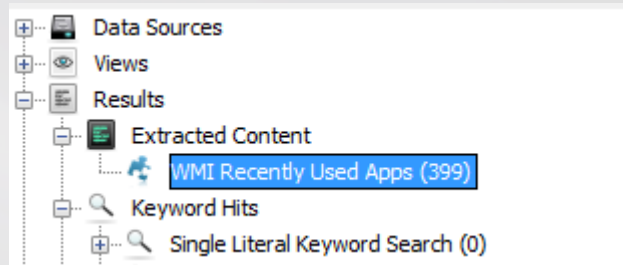
- Results
 - Extracted Content
 - Windows Event Logs (125)
 - Windows Event Logs By Event Id (175)
- Keyword Hits
 - Single Literal Keyword Search (0)
 - Single Regular Expression Search (0)
- Hashset Hits
- E-Mail Messages
- Interesting Items
- Accounts

Tags

- Reports

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

vss_test_1 - Autopsy 4.4.0

Case View Tools Window Help

+ Add Data Source View Images/Videos Timeline Generate Report Close Case

! Keyword Lists Keyword Search

Directory Listing

/vss0 - 5f8e1eac-3741-11e7-9408-0800272373b7 - 2017-05-18 12:59:20/vss0 10 Results

Name	Location	Modified Time	Change Time	Access Time	Created
\$Extend	/vss0 - 5f8e1eac-3741-11e7-9408-0800272373b7 - 2017-...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
\$Recycle.Bin	/vss0 - 5f8e1eac-3741-11e7-9408-0800272373b7 - 2017-...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Program Files	/vss0 - 5f8e1eac-3741-11e7-9408-0800272373b7 - 2017-...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
ProgramData	/vss0 - 5f8e1eac-3741-11e7-9408-0800272373b7 - 2017-...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Python27	/vss0 - 5f8e1eac-3741-11e7-9408-0800272373b7 - 2017-...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
System Volume Information	/vss0 - 5f8e1eac-3741-11e7-9408-0800272373b7 - 2017-...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Users	/vss0 - 5f8e1eac-3741-11e7-9408-0800272373b7 - 2017-...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Windows	/vss0 - 5f8e1eac-3741-11e7-9408-0800272373b7 - 2017-...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
\$MFT	/vss0 - 5f8e1eac-3741-11e7-9408-0800272373b7 - 2017-...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
pagefile.sys	/vss0 - 5f8e1eac-3741-11e7-9408-0800272373b7 - 2017-...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

Hex Strings File Metadata Results Indexed Text Media

prepopulating image/video database 73%

Data Sources

- Python-win-test-delete-vss.E01
- vss0 - 5f8e1eac-3741-11e7-9408-0800272373b7 - 20
 - vss0 (10)
 - \$Extend (1)
 - \$Recycle.Bin (1)
 - Program Files (13)
 - ProgramData (3)
 - Python27 (1)
 - System Volume Information (2)
 - Users (2)
 - Windows (26)
- vss1 - 5012d05a-3ea6-11e7-940a-0800272373b7 - 20
- vss2 - c0f9a83b-442a-11e7-9415-0800272373b7 - 20
- vss3 - 841fc327-44ab-11e7-941b-0800272373b7 - 20
- vss4 - 6093c018-46e2-11e7-9430-080027845a66 - 20
- vss5 - 625bb28f-4beb-11e7-9431-080027845a66 - 20

Views

Results

- Extracted Content
 - vss0 - 5f8e1eac-3741-11e7-9408-0800272373b7
 - vss1 - 5012d05a-3ea6-11e7-940a-0800272373b7
 - vss2 - c0f9a83b-442a-11e7-9415-0800272373b7
 - vss3 - 841fc327-44ab-11e7-941b-0800272373b7
 - vss4 - 6093c018-46e2-11e7-9430-080027845a66
 - vss5 - 625bb28f-4beb-11e7-9431-080027845a66

Volume Shadow Plugin

vss_test_1 - Autopsy 4.4.0

Case View Tools Window Help

+ Add Data Source View Images/Videos Timeline Generate Report Close Case

Keyword Lists Keyword Search

Directory Listing

vss0 - 5fbc1eac-3741-11e7-9408-0800272373b7 - 2017-05-18 12:59:20 Files 5500 Results

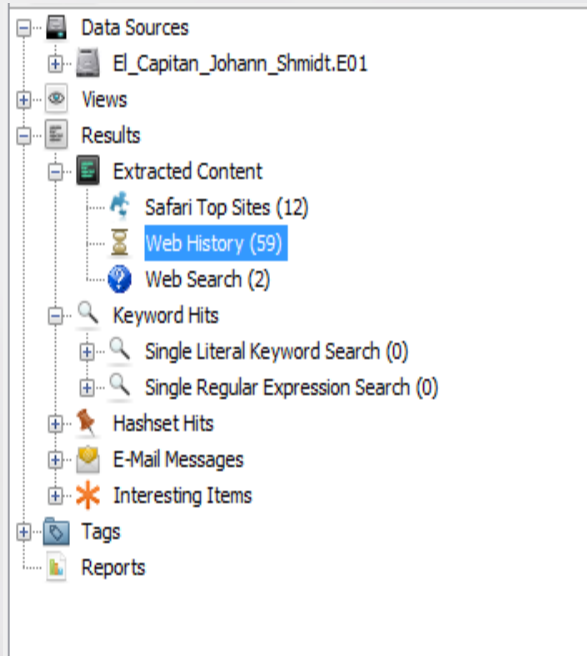
Source File	Name	MFT Number	Path	Date Created	Date Modified
{5fbc1eac-3741-11e7-9408-0800272373b7} \$TxfLog.blf		32	/\$Extend/\$RmMetadata/\$TxfLog	2017-04-03 18:49:09 EDT	2017-05-22 20:54:1
{5fbc1eac-3741-11e7-9408-0800272373b7} \$TxfLogContainer00000000000000000002		34	/\$Extend/\$RmMetadata/\$TxfLog	2017-04-03 18:49:09 EDT	2017-05-22 20:54:1
{5fbc1eac-3741-11e7-9408-0800272373b7} .csrc		22684	/Users/mark/AppData/Local/JetBrains/Transien...	2017-05-19 14:02:26 EDT	2017-05-19 14:02:2
{5fbc1eac-3741-11e7-9408-0800272373b7} .csrc		22687	/Users/mark/AppData/Local/JetBrains/Transien...	2017-05-19 14:02:27 EDT	2017-05-19 14:02:2
{5fbc1eac-3741-11e7-9408-0800272373b7} .csrc		22690	/Users/mark/AppData/Local/JetBrains/Transien...	2017-05-19 14:02:27 EDT	2017-05-19 14:02:2
{5fbc1eac-3741-11e7-9408-0800272373b7} .usage		17068	/Users/mark/AppData/Local/Google/Chrome/U...	2017-05-18 09:21:39 EDT	2017-05-18 09:21:4
{5fbc1eac-3741-11e7-9408-0800272373b7} .version		22683	/Users/mark/AppData/Local/JetBrains/Transien...	2017-05-19 14:02:27 EDT	2017-05-19 14:02:2
{5fbc1eac-3741-11e7-9408-0800272373b7} .version		22686	/Users/mark/AppData/Local/JetBrains/Transien...	2017-05-19 14:02:27 EDT	2017-05-19 14:02:2
{5fbc1eac-3741-11e7-9408-0800272373b7} .version		22689	/Users/mark/AppData/Local/JetBrains/Transien...	2017-05-19 14:02:26 EDT	2017-05-19 14:02:2
{5fbc1eac-3741-11e7-9408-0800272373b7} 0.0.filtertrie.intermediate.txt		9725	/Users/mark/AppData/Local/Packages/Microsof...	2017-05-22 18:53:52 EDT	2017-05-22 18:53:5
{5fbc1eac-3741-11e7-9408-0800272373b7} 0.1.filtertrie.intermediate.txt		9731	/Users/mark/AppData/Local/Packages/Microsof...	2017-05-22 18:53:52 EDT	2017-05-22 18:53:5
{5fbc1eac-3741-11e7-9408-0800272373b7} 0.2.filtertrie.intermediate.txt		9738	/Users/mark/AppData/Local/Packages/Microsof...	2017-05-22 18:53:52 EDT	2017-05-22 18:53:5

Hex Strings File Metadata Results Indexed Text Media

prepopulating image/video database 82%

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.

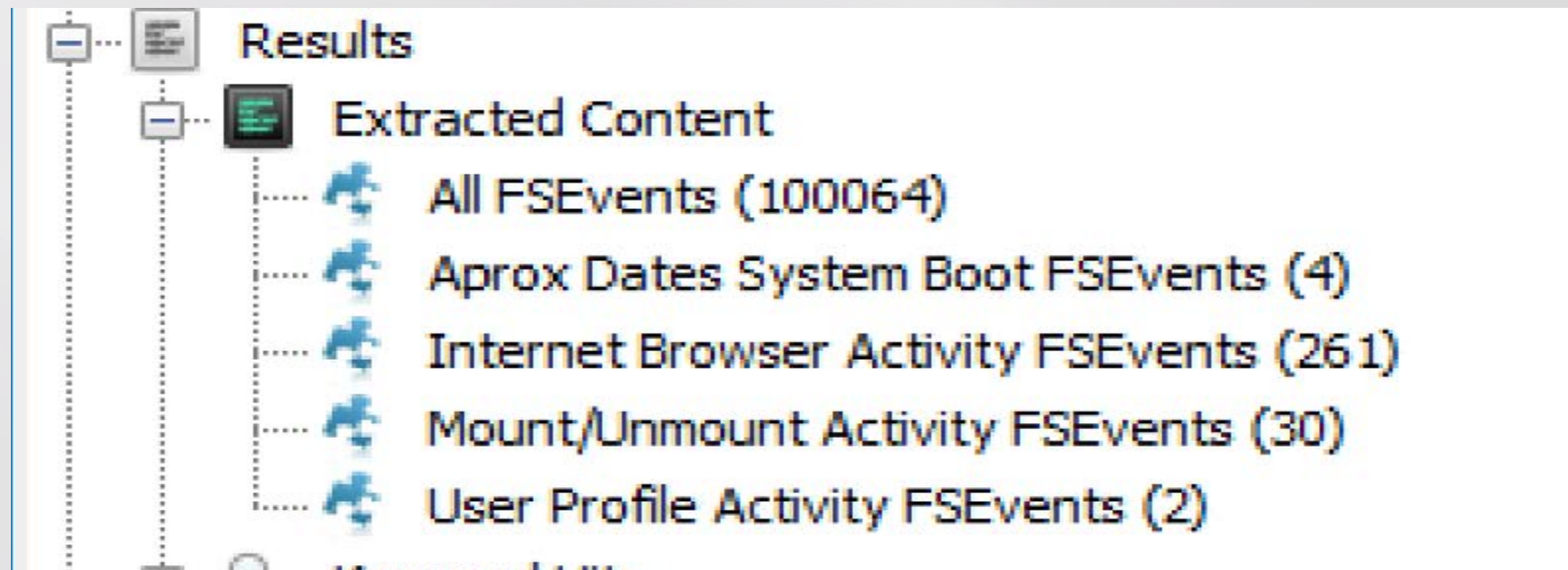


Safari Top Sites				
Table Thumbnail				
Source File	Username	URL	Title	Site Last Modified
TopSites.plist	redskull	http://www.apple.com/startpage/		2017-04-29 22:39:46 EDT
TopSites.plist	redskull	https://www.icloud.com/	iCloud	0000-00-00 00:00:00
TopSites.plist	redskull	https://www.yahoo.com/	Yahoo	0000-00-00 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.



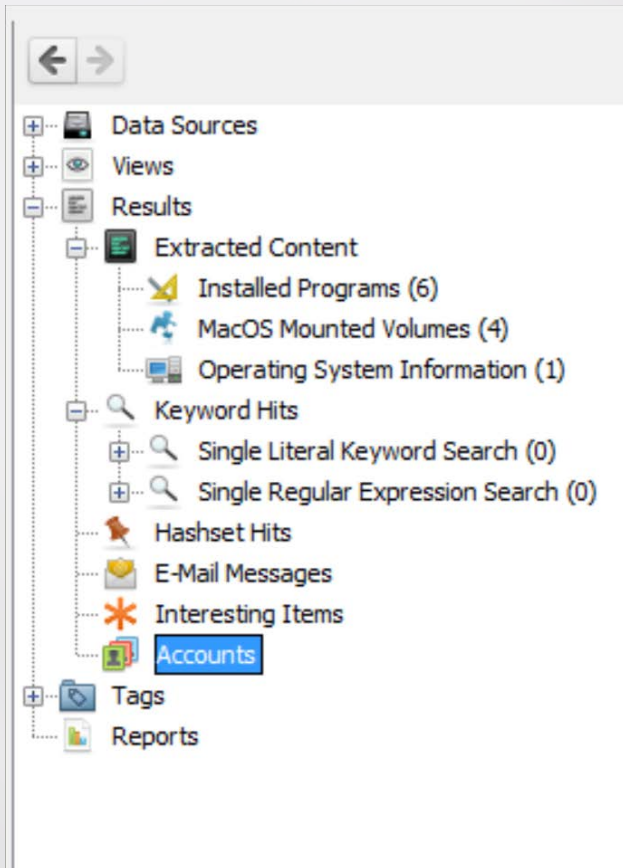
Mac OSX Recents

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



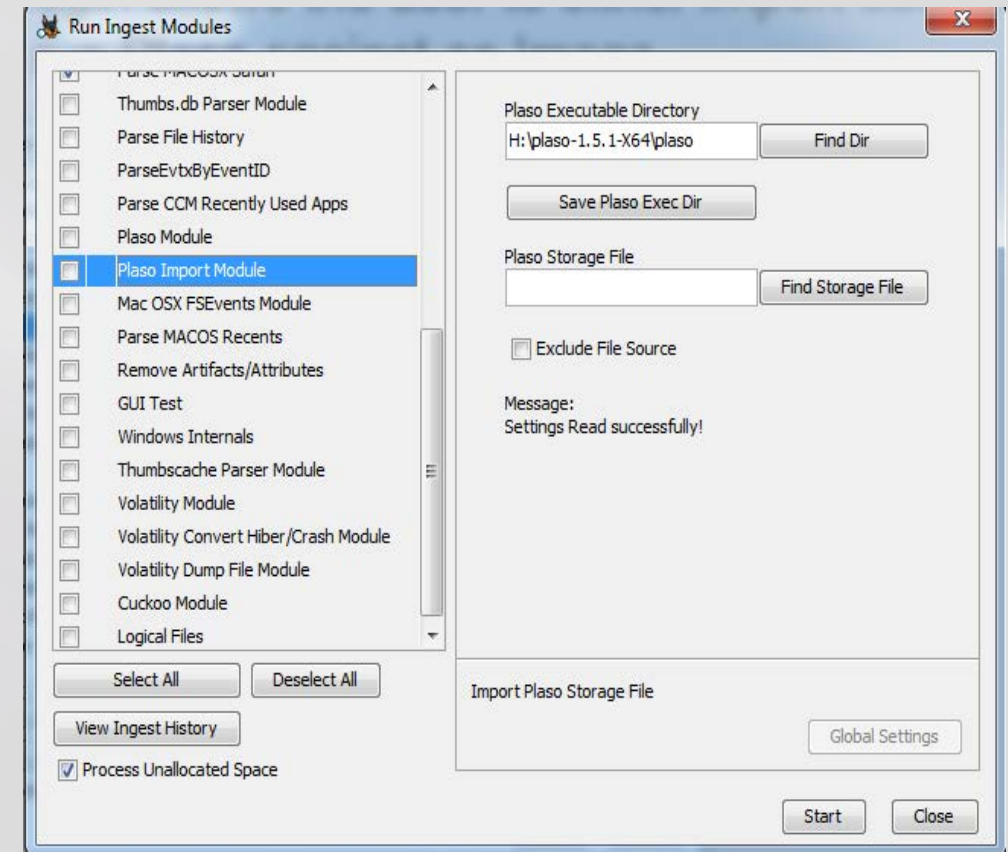
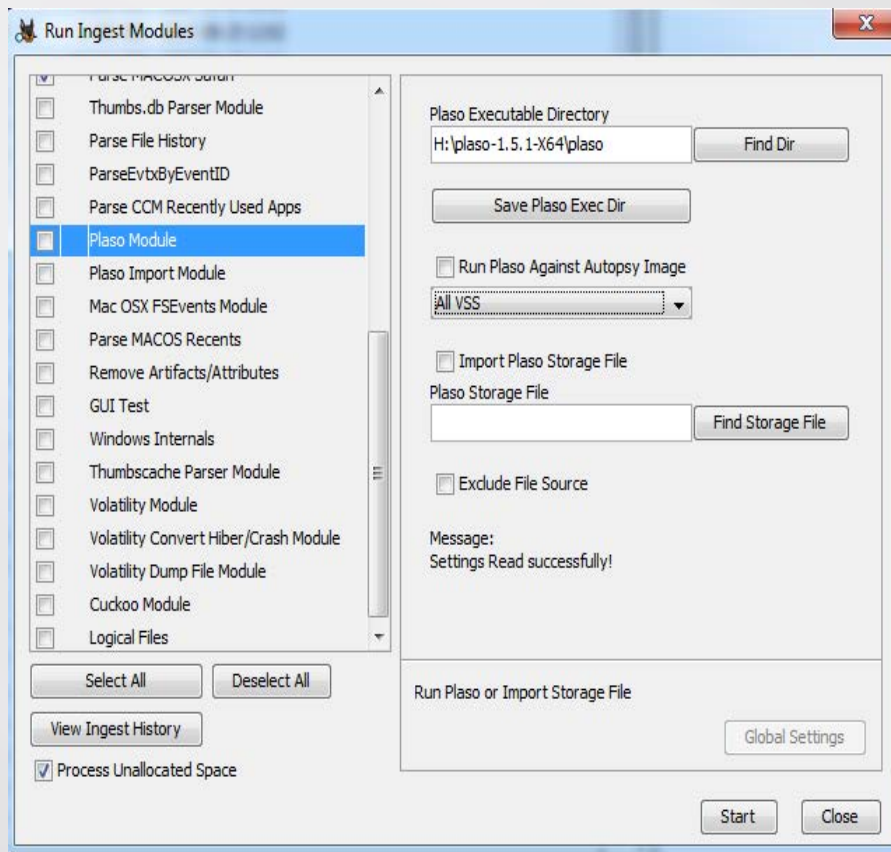
Listing					
Installed Programs					
Table		Thumbnail			
Source File	Display Version	Program Name	Installation Method	Data Source	Tags
InstallHistory.plist		OS X	OS X Installer	El_Capitan_Johann_Shmidt.E01	
InstallHistory.plist	10.1.6	VMware Tools	Installer	El_Capitan_Johann_Shmidt.E01	
InstallHistory.plist	4.3.2	Twitter	storedownload	El_Capitan_Johann_Shmidt.E01	
InstallHistory.plist	0.2.4239	WhatsApp	storedownload	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	

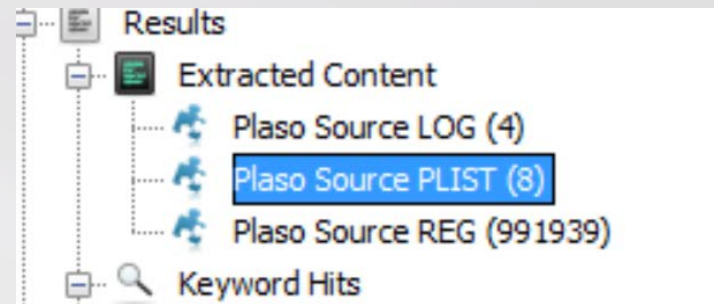
Listing				
Operating System Information				
Table		Thumbnail		
Source File	Name	Version	MAC Build Version	Data Source
SystemVersion.plist	Mac OS X	10.11.6	15G31	El_Capitan_Johann_Shmidt.E01

Plaso Plugin

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



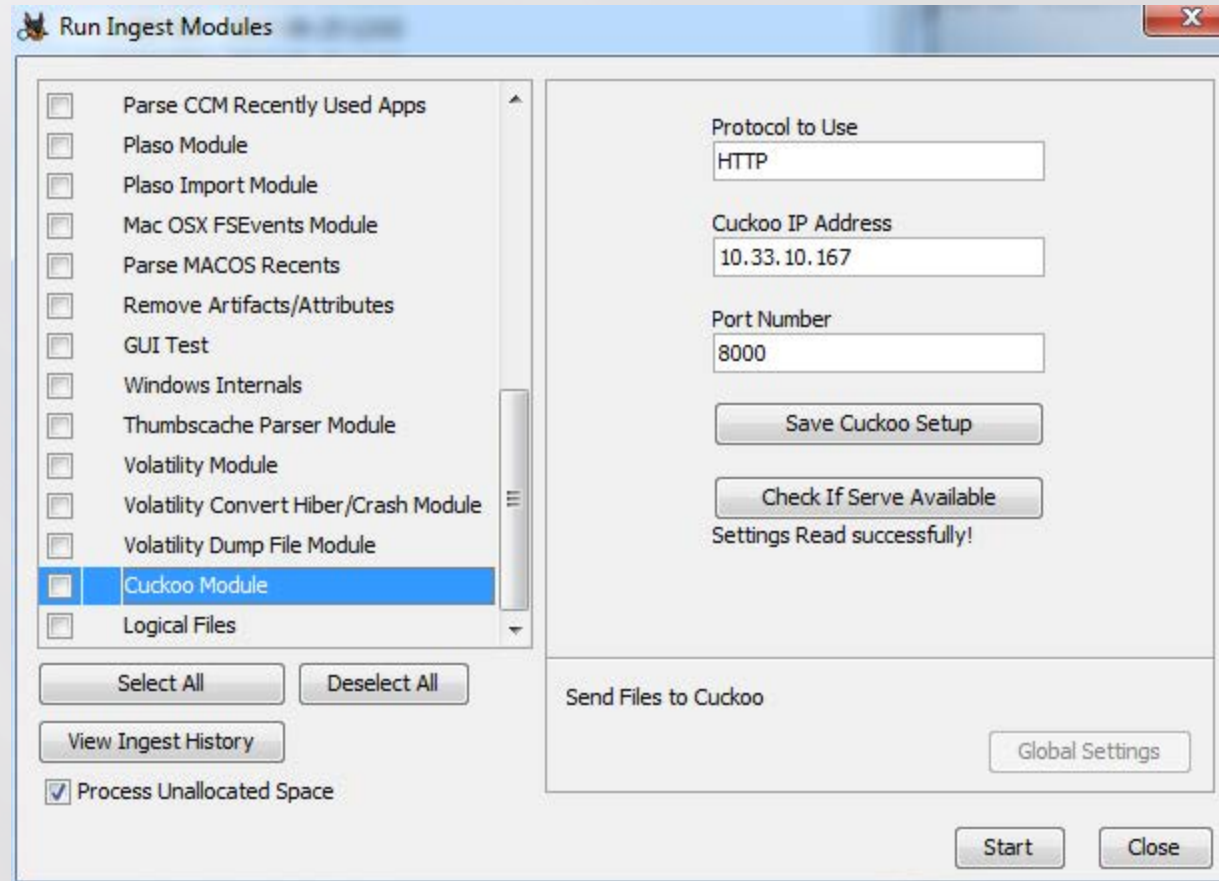
Plaso Plugin



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 [storedownload...	/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.

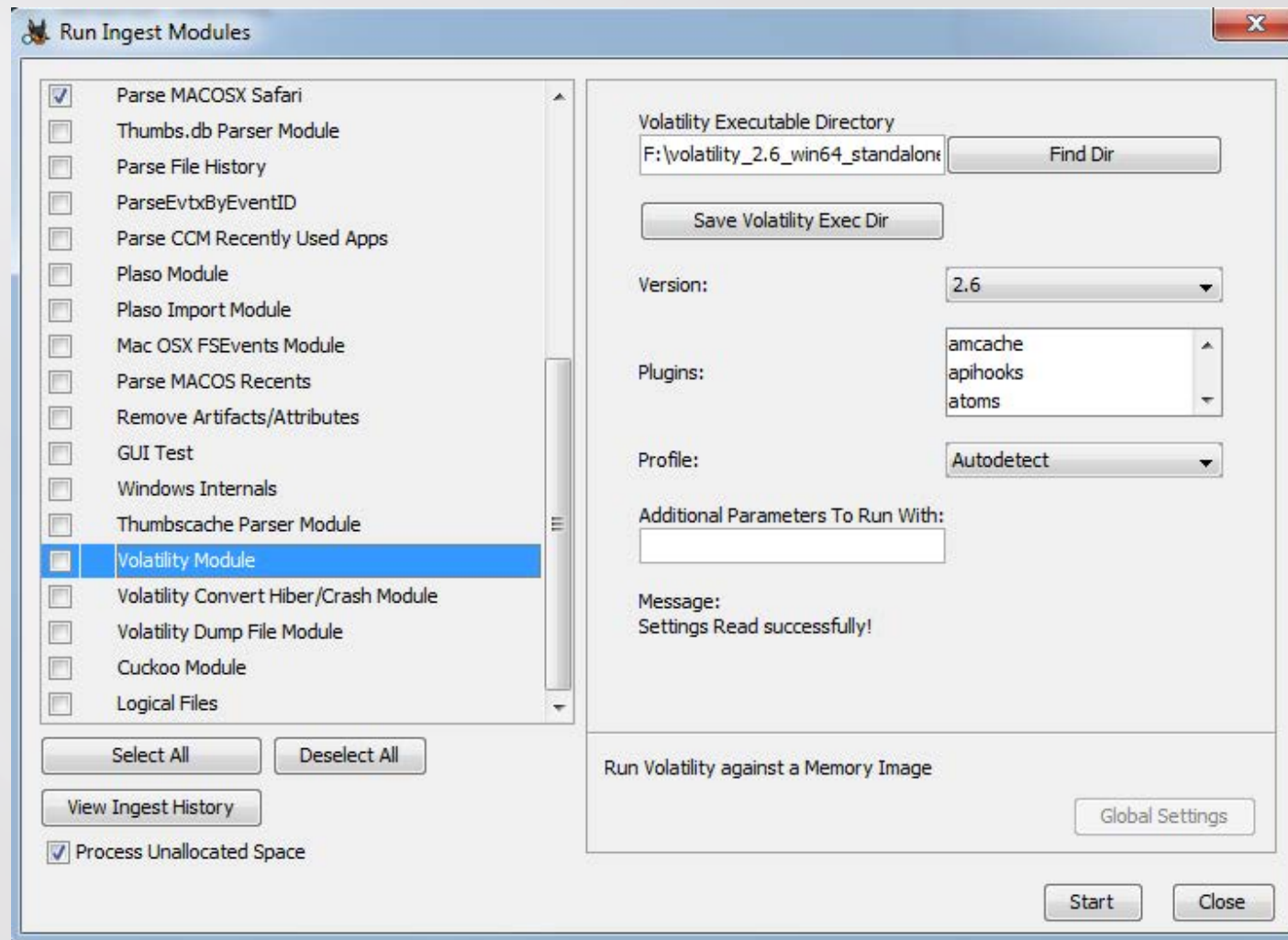
This can run the Volatility executable or the Python script

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

Log_test_2 - Autopsy 4.3.0

Case View Tools Window Help

+ Add Data Source View Images/Videos Timeline Generate Report Close Case

⚠ Keyword Lists 🔍 Keyword Search

◀ ▶ ◻

Directory Listing

Volatility CMDSCAN sample005.bin 11 Results

Table Thumbnail

Source File	id	Process	PID	History Offset	Application	Flags	Command Count	Last Added	Last Displayed	First Command
sample005.bin	1	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	2	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	3	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	4	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	5	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	6	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	7	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	8	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	9	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	10	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0
sample005.bin	11	csrss.exe	452	21792504	cmd.exe	Allocated, Reset	11	10	10	0

< >

Hex Strings File Metadata Results Indexed Text Media

Keyword Hits

Single Literal Keyword Search (0)

◀ ▶ ◻

◻ Show Rejected Results

Data Sources

Views

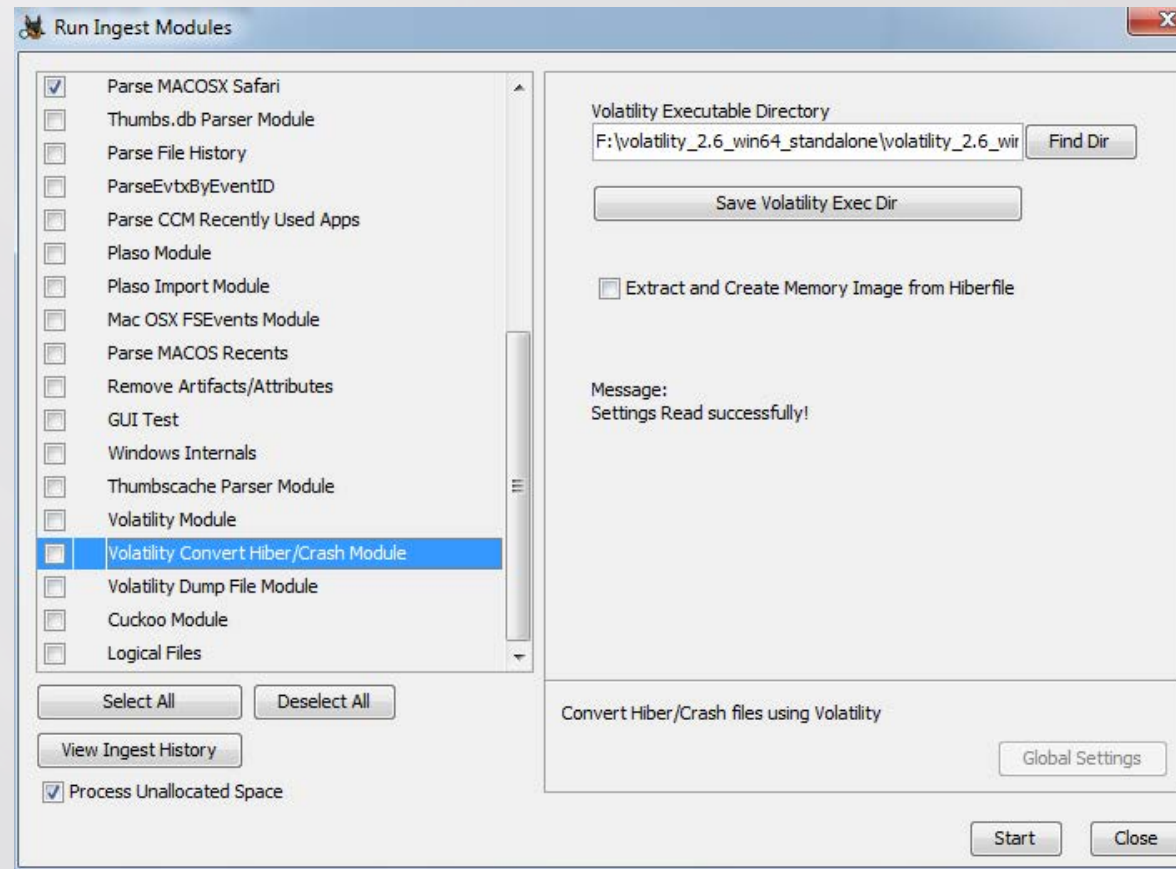
Results

Extracted Content

- Volatility CMDLINE sample001.bin (21)
- Volatility CMDLINE sample005.bin (25)
- Volatility CMDLINE sample006.bin (38)
- Volatility CMDLINE sample007.bin (31)
- Volatility CMDSCAN sample001.bin (5)
- Volatility CMDSCAN sample005.bin (11)**
- Volatility CONNECTIONS sample001.bin (1)
- Volatility CONNECTIONS sample005.bin (3)
- Volatility CONNECTIONS sample006.bin (1)
- Volatility IMAGEINFO sample001.bin (1)
- Volatility IMAGEINFO sample005.bin (1)
- Volatility IMAGEINFO sample006.bin (1)
- Volatility IMAGEINFO sample007.bin (1)
- Volatility PSLIST sample001.bin (21)
- Volatility PSLIST sample005.bin (25)
- Volatility PSLIST sample006.bin (38)
- Volatility PSLIST sample007.bin (31)
- Volatility PSSCAN sample001.bin (45)
- Volatility PSSCAN sample005.bin (101)
- Volatility PSSCAN sample006.bin (38)
- Volatility PSSCAN sample007.bin (31)
- Volatility PSTREE sample001.bin (21)
- Volatility PSTREE sample005.bin (25)
- Volatility PSTREE sample006.bin (38)
- Volatility PSTREE sample007.bin (31)

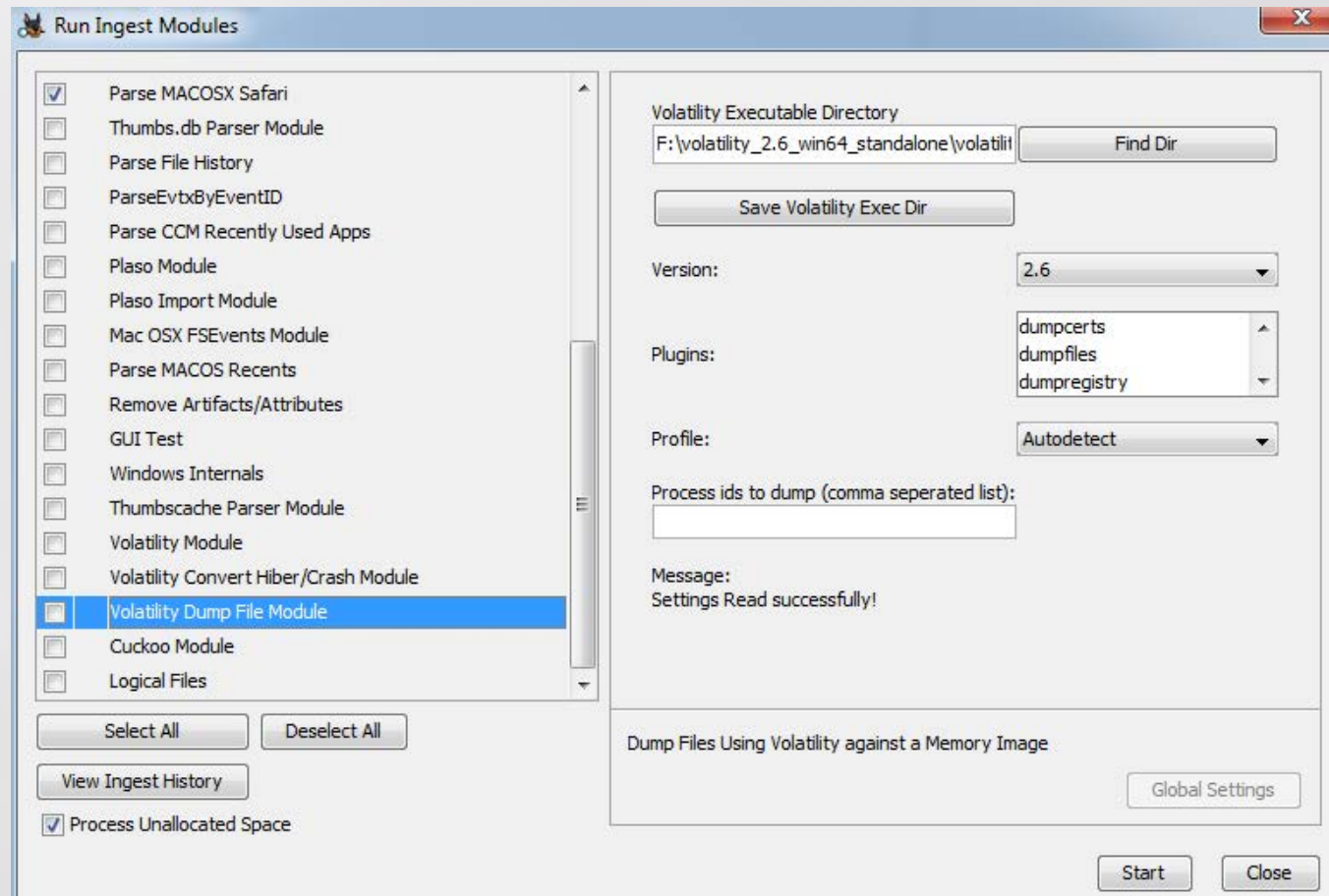
Volatility Dump Hiber File Plugin

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

mem_test_dups - Autopsy 4.4.1

Case View Tools Window Help

+ Add Data Source View Images/Videos Timeline Generate Report Close Case

⚠ Keyword Lists 🔍 Keyword Search

⏪ ⏩ ☐ Show Rejected Results

Data Sources

- LogicalFileSet1 (1)
 - Bob.vmem (6)
 - dumpfiles (3)
 - 1384 (44)
 - 1752 (146)**
 - 888 (97)
 - procdump (3)
 - 1384 (1)
 - 1752 (1)
 - 888 (1)

Views

- Results**
 - Extracted Content
 - Volatility IMAGEINFO Bob.vmem (1)
 - Volatility PSLIST Bob.vmem (27)
 - Volatility PSSCAN Bob.vmem (27)
 - Keyword Hits
 - Single Literal Keyword Search (0)
 - Single Regular Expression Search (0)
 - Hashset Hits
 - E-Mail Messages
 - Interesting Items
 - Accounts
- Tags
- Reports

Listing 146 Results

Table Thumbnail

Name	Location	Modified Time	Change Time	Access Time	Created Time
file.1752.0x81c6aba8.img	/LogicalFileSet1/Bob.vmem/dumpfiles/1752/file.1752.0x81c...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
file.1752.0x81c6b1f8.img	/LogicalFileSet1/Bob.vmem/dumpfiles/1752/file.1752.0x81c...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
file.1752.0x81c6b578.vacb	/LogicalFileSet1/Bob.vmem/dumpfiles/1752/file.1752.0x81c...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
file.1752.0x81c6ca40.dat	/LogicalFileSet1/Bob.vmem/dumpfiles/1752/file.1752.0x81c...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
file.1752.0x81c6e640.img	/LogicalFileSet1/Bob.vmem/dumpfiles/1752/file.1752.0x81c...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
file.1752.0x81c6ed30.img	/LogicalFileSet1/Bob.vmem/dumpfiles/1752/file.1752.0x81c...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
file.1752.0x81c75c30.img	/LogicalFileSet1/Bob.vmem/dumpfiles/1752/file.1752.0x81c...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
file.1752.0x81c7df10.dat	/LogicalFileSet1/Bob.vmem/dumpfiles/1752/file.1752.0x81c...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
file.1752.0x81c804c0.dat	/LogicalFileSet1/Bob.vmem/dumpfiles/1752/file.1752.0x81c...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
file.1752.0x81c80b48.dat	/LogicalFileSet1/Bob.vmem/dumpfiles/1752/file.1752.0x81c...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
file.1752.0x81c88058.dat	/LogicalFileSet1/Bob.vmem/dumpfiles/1752/file.1752.0x81c...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

Hex Strings File Metadata Results Indexed Text Media Other Data Sources Windows Registry View

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?