Plaso Filtering

The Missing Manual

Mark Hallman

- Sr. Engineer with

  SANS Research Operations Center (SROC)
- 11 Years in DFIR
- Worked with Plaso FKA log2timeline
- Certifications: CHFI, CCE, EnCE, GCFE, GCFA

Email: mark.hallman@gmail.com
mhallman@sans.org
Skype: mhallman
Twitter: @mhallman

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Techno Security & Digital Forensics Conference

What are we going to cover today?

- Refresher on the Plaso Components
- Methods to filter in Plaso
  - Front End
    - image_export
    - log2timeline
  - Back End
    - psort
- Other complementary tools
  - Timeline Explorer – Eric Zimmerman
  - KAPE – Triage collection tool – Eric Zimmerman

Filtering – Why is it so important?

Data reduction by targeted collections allows:

- Focus on specific areas of interest
- Speed of processing
- Speed of analysis
- Manageable Output Size for Other Tools

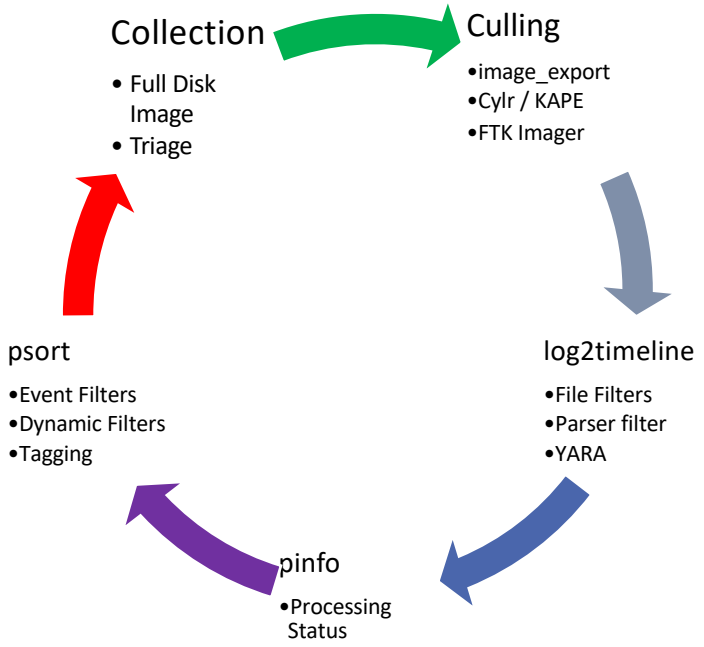
GitHub

Evidence of categories:

- User Communication
- File Download
- Program Execution
- File Opening/ Creation
- File Knowledge
- Physical Location
- USB Key Usage
- Account Usage
- Browser Usage

Plaso Components & Process Flow

- Can be an iterative process.
- The lines are blurring between Collection & Culling
- **image_export** – extracts files from images **(+VSS)**
  - Or, other tools like KAPE – Also processes VSS
- **log2timeline** – creates the Plaso storage file (sqlite)
- **pinfo** – provide information on log2timeline processing
- **psort** – processes /updates Plaso storage files (sort, filter, analysis)
- **psteal** – wrapper that runs log2timeline and then psort



image_export

- Extracts files by using a filter file
- Allows targeted extraction of specific files
- The filter file is the same format as used by **log2timeline**
- Significantly faster processing than processing the entire image
- Command line so it is scriptable /repeatable
- **VSS Support**
  - **image_export** will can grab matching files from the VSS
- ~~Other tools can do similar collections but…~~ KAPE

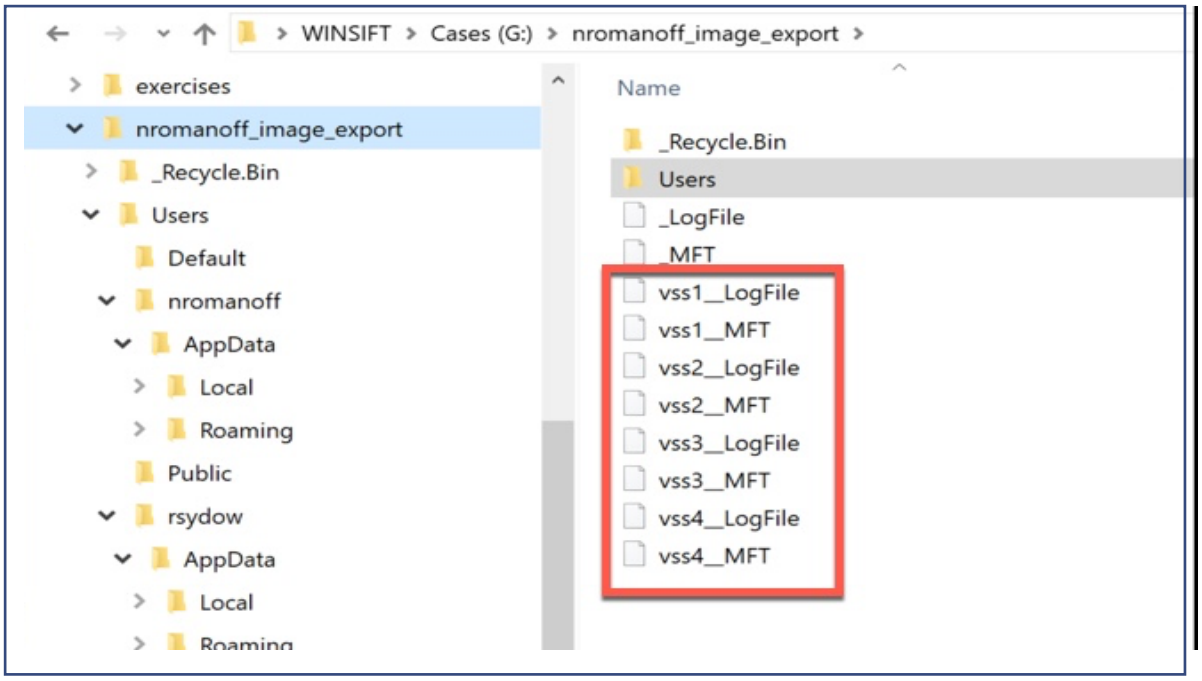
image_export: common options

```
optional arguments:
  -h, --help            Show this help message and exit.
  -V, --version         Show the version information.

  --no_vss              Do not process VSS
  --vss_only
                        Only process VSS.
  --vss_stores VSS_STORES
                        e.g. "3..5" or  "1,3,5" or "1,3..5" or "all".
  --date-filter TYPE_START_END, --date_filter
                        "TIME_VALUE,START_DATE_TIME,END_DATE_TIME" where
                        TIME_VALUE defines which file entry timestamp the
                        filter applies to e.g. atime, ctime, crtime, bkup,
                        etc.
  -f FILE_FILTER,       FILE_FILTER
                        List of files to include for targeted collection
  -x EXTENSIONS         Filter on file name extensions. Multiple multiple
                        comma separated values e.g. "csv,docx,pst".
  --names NAMES         Filter on file names. e.g. "NTUSER.DAT,UsrClass.dat".
  --signatures IDENTIFIERS
                        Filter on file format signature identifiers.  e.g.
                        "esedb,lnk,evtx,olecf". Use "list" for
                        supported file format signatures.
  -w PATH               PATH
```

image export: VSS Capability

```
image_export -f windows_filter.txt --vss_stores all -w
nromanoff_image_export demo.E01
```



- --no_vss
- --vss_only
- --vss_stores

image export: Export by File Extension

-x "doc,docx,xls,xlsx,ppt,pptx"

```
image_export -x "doc,docx,xls,xlsx,ppt,pptx"
--vss_stores all -w nromanoff_image_export_office_docs
nromanoff-c-drive.e01
```

image export: date

"crtime, 2013-10-22 00:00:00, 2013-10-22 23:59:59"

```
image_export.py --vss_stores all -x
"doc,docx,xls,xlsx,ppt,pptx"
--date-filter "atime, 2013-10-22 00:00:00, 2013-10-22 23:59:59"
--date-filter "crtime,2013-10-22 00:00:00, 2013-10-22 23:59:59"
-w blake_image_export_office_docs
../blake-c-drive/blake-c-drive.e01
```

log2timeline

- Processes source files into the Plaso database
  - Supports many image formats - Raw, VHD, E01 images, mount points & **other Plaso DB files**.
- Filtering Options available
  - File Filters
  - Filter by Parser
  - Filter by YARA rules. (artifacts in Release 20180630)

Most basic command format:

```
log2timeline.py OUTPUT INPUT

log2timeline.py demo.E01 demo.plaso
```

log2timeline usage: common options

```
usage: log2timeline.exe [-h] [-V]
                        [--parsers PARSER_LIST]
                        [-f FILE_FILTER]
                        [--no_vss] [--vss_only] [--vss_stores VSS_STORES]
                        [--no_dependencies_check]
                        [STORAGE_FILE] [SOURCE]
```

```
log2timeline.exe –z “UTC”  --file_filter  filter_windows.txt
--no_vss  --parsers prefetch,amcache,userassist,srum
demo.plaso  demo.E01
```

log2timeline: Collection Filters Files

- Filter Files are a list of files to collect
- Triage Approach: Collect / Process only what you want
  - Saves time during collection and analysis
- Relevant to image_export and log2timeline
  - Use the same file / file format
  - Some items in Filter File may only be relevant for image_export
    - No plugins to process some files that still; should be collected
    - Example: pagefile.sys, hiberfile.sys, etc.

log2timeline: Filter File Format

- One entry per line
- Each line defines a single location to collect/process
- Format is: FIELD 1 | SEPARATOR | FIELD 2 | SEPARATOR | FIELD 3 | ...
- Separator = slash "/"
- A field can be one of the following three options:
  - A string representing the exact directory name, case insensitive.
  - A regular expression denoting the name of the directory or file.
  - A name of an attribute collected during the preprocessing stage, denoted by a curly bracket {attribute_name}.
  - Attribute Name Example: {sysregistry}/.+evt

Source: https://github.com/log2timeline/plaso/wiki/Collection-Filters

Filter File Example

```
142 #####
143 # Users Registry hives & associated logs
144 #####
145 /(Users|Documents And Settings)/.+/NTUSER[.]DAT
146 /(Users|Documents And Settings)/.+/ntuser[.]DAT[.]LOG[1-9]
147 /Users/.+/AppData/Local/Microsoft/Windows/Usrclass[.]dat
148 /Users/.+/AppData/Local/Microsoft/Windows/Usrclass[.]DAT[.]LOG[1-9]
149
150 #####
151 # Recent file activity.
152 #####
153 /Users/.+/AppData/Roaming/Microsoft/Windows/Recent/.+[.]LNK
154 /Users/.+/AppData/Roaming/Microsoft/Office/Recent/.+[.]LNK
155 /Users/.+/Desktop/.+[.]LNK
156 /Documents And Settings/.+/Recent/.+[.]LNK
157 /Users/.+/AppData/Roaming/Microsoft/Windows/Recent/Automaticdestinations/.+[.
    ]automaticDestinations-ms
158 /Users/.+/AppData/Roaming/Microsoft/Windows/Recent/Customdestinations/.+[.]cu
    stomDestinations-ms
```

GitHub

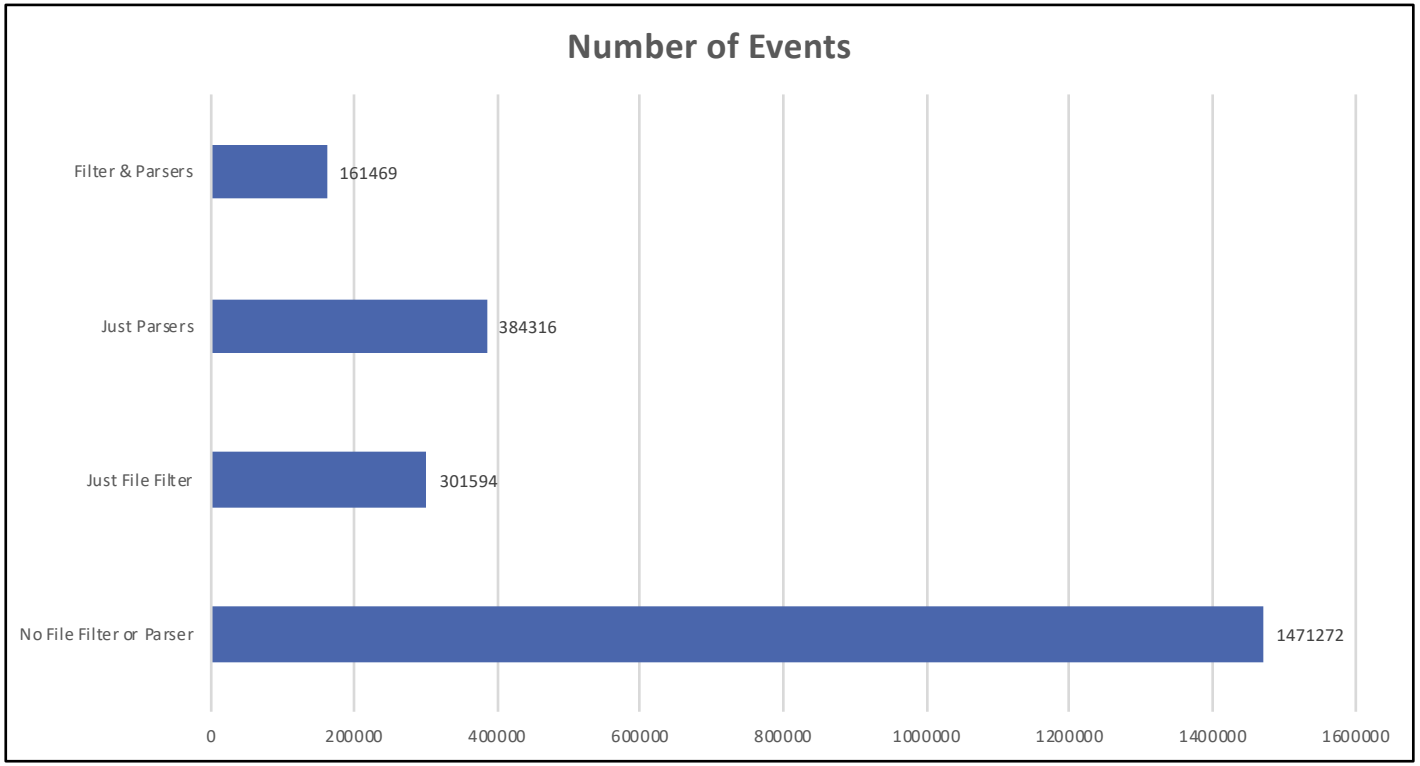
Complete File Available on my GitHub Page

Complete File: https://github.com/mark-hallman/plaso_filters

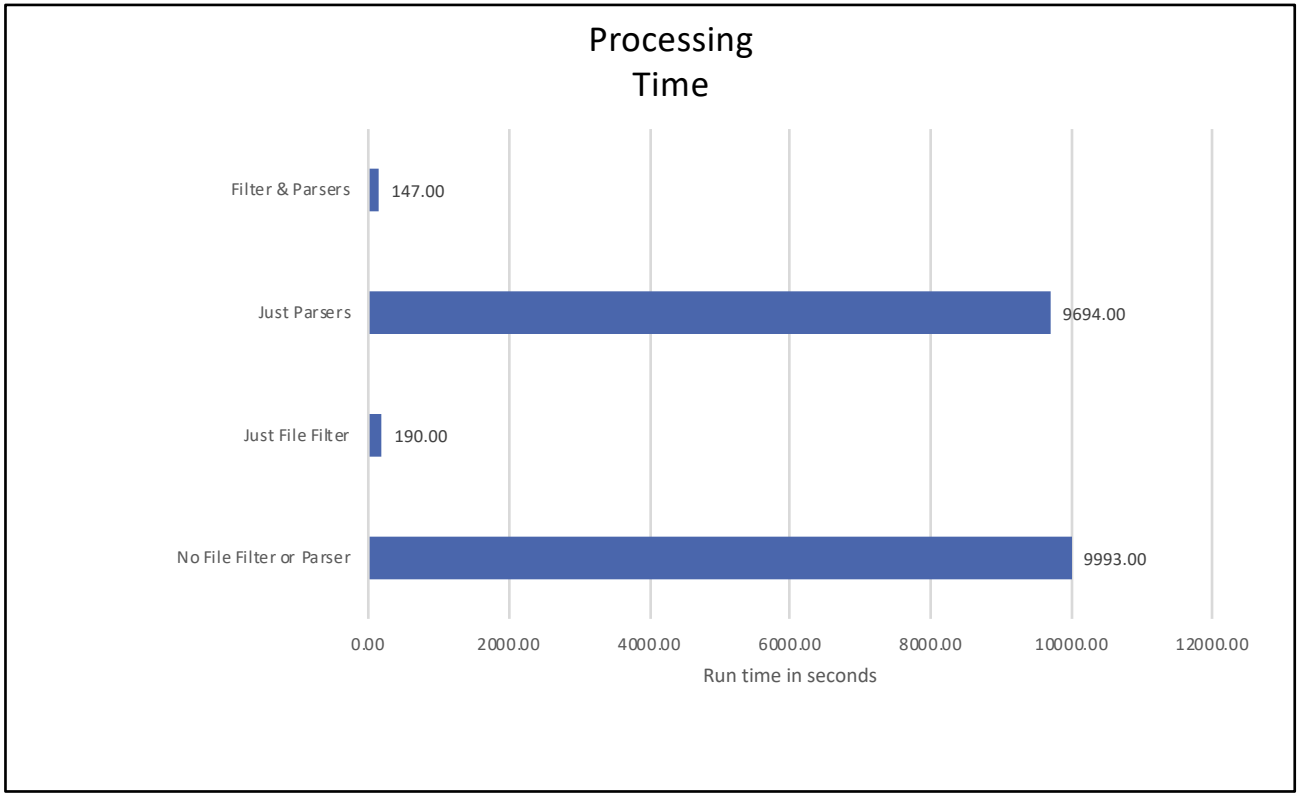
SANS DFIR DIGITAL FORENSICS & INCIDENT RESPONSE

Techno Security & Digital Forensics Conference

Filter Files – Performance Test - Events



Filter Files – Performance Test - Time



SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Techno Security & Digital Forensics Conference

Parsers

- Available on front & back end
- Limit processing to specific types of artifacts – missing ”not” operator
- Parser Catagories
  - Parsers: Processes individual artifacts
    - (amcache, lnk, mft, plist, prefetch …)
  - Parser Plugins: Processes artifact categories
    - (apple_id, bag_mru, cron, google_drive …)
  - Parser Presets: Sets of Parser Presets, Parsers Plugins & Parsers
    - (winreg, win7, macosx …)
    - Easy to create your own. Covered later in presentation.
- Help and list of all parsers
  - log2timeline.exe --info
  - log2timeline.exe --parsers list

Registry (winreg) Parsers

appcompatcache	shellbags	ccleaner	default	interface	lfu
mountpoints	mrulistex	mrulist	msie zones	officemru	outlook
run	sam_users	services	shutdown	task scheduler	terminal server
typedurls	usb	usbstor	userassist	winrar	winver

Windows Parsers (win_gen, winxp, win7)

Chrome	Esedb	EVT / EVTX	Filestat	Firefox	Google drive
IE 6-9	IE 10-11	IIS	Job Files	Jumplists	LNK
McAfee Logs	Olecf	Openxml	Peer to Peer	Prefetch	Recycle Bin
Registry	Skype	Skydrive Logs	Symantec Log	Winfirewall	

Web History (webhist) Parsers

Chrome cache	Chrome cookies	Chrome extension activity	Chrome history	Firefox cache
Firefox cookies	Firefox downloads	Firefox history	Java idx	MS Index.dat
MS webcache.dat	Opera global	Opera typed history	Safari history	

Linux/Andriod/Mac (android, linux, macOS)

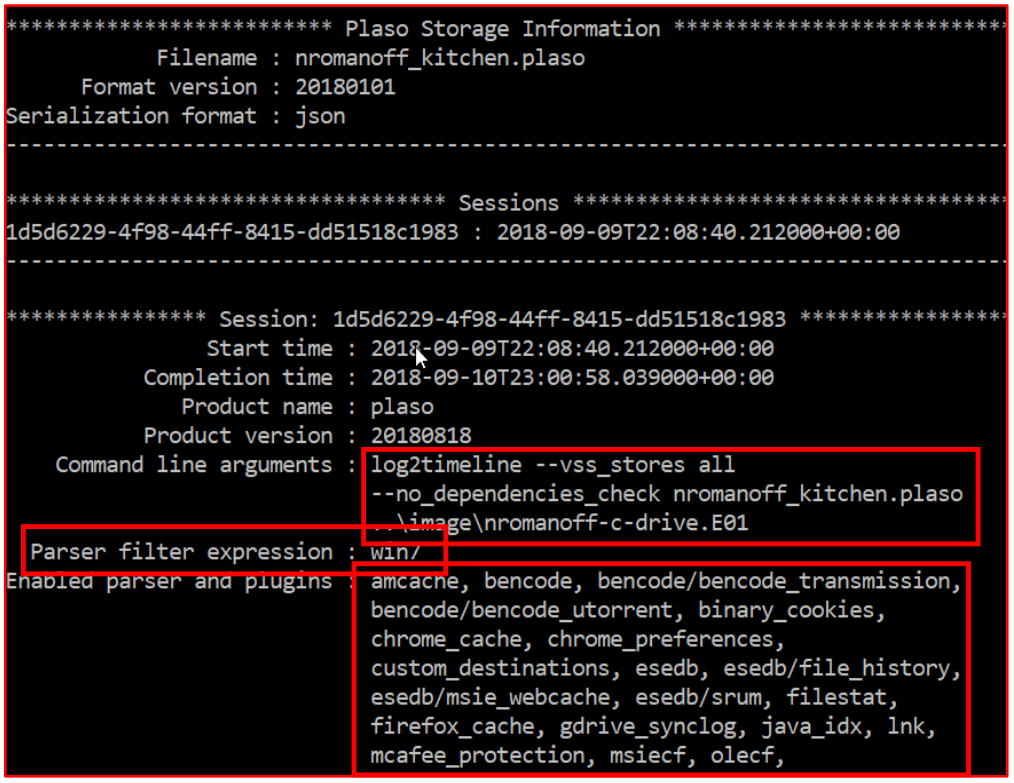
Android app usage	Android calls	Android sms	appusage	Asl log	bencode	Bsm log
Cups ipp	filestat	Google drive	Ipod device	Ls quarantine	Firewall log	Doc versions
Mackeeper cache	keychain	securityd	macwifi	olecf	openxml	Plist airport
Plist appleaccount	Plist bluetooth	Plist default	Plist install history	Plist macuser	Plist softwareupdate	Plist spotlight
Plist spotlight volume	Plist timemachine	Pls recall	Popularity contest	selinux	skype	syslog
utmp	utmpx	webhist	xchatlog	xchatscrollback	zeitgeist	

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Techno Security & Digital Forensics Conference

Parsers – Do I Really Want the Defaults?

- Maybe, if you really know what that means.
- No parser parameters == win7
- win7 ==
  - recycle_bin
  - amcache
  - custom_destinations
  - winevtx
  - esedb/file_history
  - olecf/olecf_automatic_destinations
  - **win_gen**



SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Techno Security & Digital Forensics Conference

Parsers – Create your own Presets

- Presets are grouping of parsers, plugins and other parsers invoked by a single name.
- In the Linux version of Plaso you can edit the presets.py file to add your own presets.

```
/usr/lib/python2.7/dist-packages/plaso/parsers/presets.py
```

Remove Event Log from win7 Parser

```
CATEGORIES = {
    'win_gen': [
        'bencode', 'esedb', 'filestat', 'sqlite/google_drive', 'gdrive_synclog',
        'java_idx', 'lnk', 'mcafee_protection', 'olecf', 'openxml', 'pe',
        'prefetch', 'sccm', 'skydrive_log', 'skydrive_log_old', 'sqlite/skype',
        'symantec_scanlog', 'usnjrnl', 'webhist', 'winfirewall', 'winjob',
        'winreg'],
    'winxp': ['recycle_bin_info2', 'rplog', 'win_gen', 'winevt'],
    'winxp_slow': ['hachoir', 'mft', 'winxp'],
    'win7': [
        'recycle_bin', 'custom_destinations', 'esedb/file_history',
        'olecf/olecf_automatic_destinations', 'win_gen', 'winevtx', 'amcache'],
    'win7_slow': ['hachoir', 'mft', 'win7'],
```

Copy & Rename (win7_custom)

/usr/lib/python2.7/dist-packages/plaso/parsers/**presets.py**

Remove Chrome Artifacts from win7

pinfo

- Provides info on the Plaso database
- Command line used for log2timeline
- Event counts, Parser Counts
- Tagging & other Analysis plugins runs
- Can be helpful to tune you log2timeline command options.

psort

- Backend Work horse
- Dedupping
- Filtering – This is key to using the tool effectively
- Analysis – Can be used to update the database and then filter on the updates

Most basic command format:

psort.py –w OUTPUT INPUT

psort.py –w nromanoff.csv nromanoff.plaso

psort – Options of Interest

- usage: psort.exe [-h] [-V]
- [--analysis PLUGIN_LIST] - A list of analysis plugin names to be loaded or "--analysis list" to see a list of available plugins
- [--slice DATE] - Create a time slice around a certain date.
- [--slice_size SLICE_SIZE] - Defines the slice size.
- [--slicer] - Create a time slice around every filter match.
- [-z TIMEZONE] - Explicitly define the timezone.
- [-o FORMAT] - The output format. Use "-o list" to see a list
- [-w OUTPUT_FILE] - Output filename.
- [--fields FIELDS] - Which fields should be included in the output
- [--additional_fields ADDITIONAL_FIELDS] - extra output, in addition to the default fields
- [STORAGE_FILE] – Plaso database created by log2timeline.
- [FILTER] – A filter applied to the database before it written to the output file(s)

Common use of psort and filters

Output file format: Several other formats besides “l2tcsv”

```
psort.py -z "UTC" -o l2tcsv -w nromanoff_l2tcsv
nromanoff.plaso
"date > '2012-04-03 00:00:00' AND
 date < '2012-04-07 00:00:00'"
```

Filter statement

psort: Output File Formats

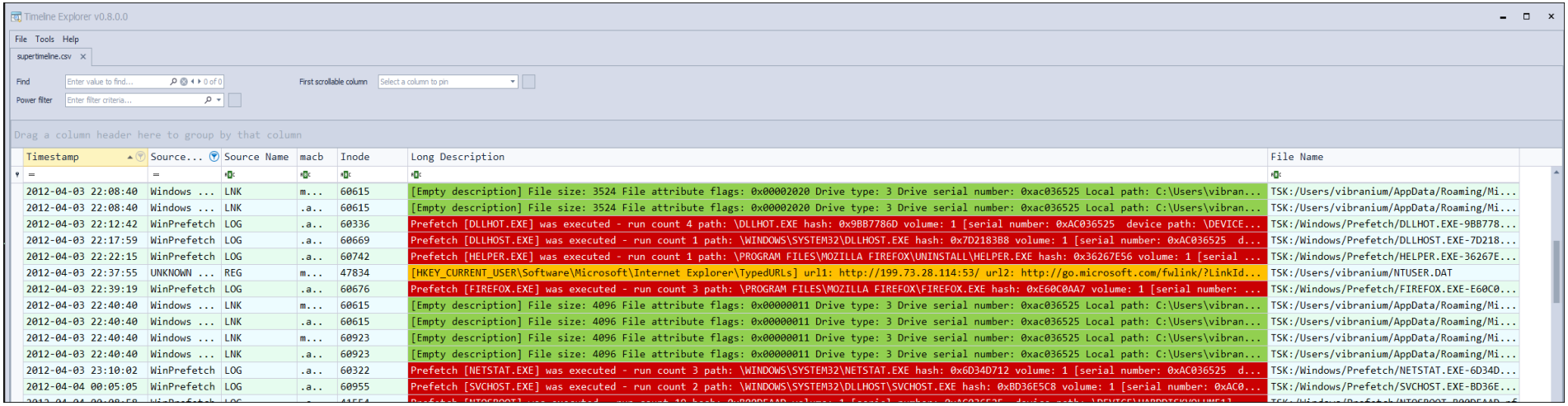
```
******************************** Output Modules ********************************
          Name : Description
-------------------------------------------------------------------------------
        l2tcsv : CSV format used by legacy log2timeline, with 17 fixed fields.
          xlsx : Excel Spreadsheet (XLSX) output
         l2ttln : Extended TLN 7 field | delimited output.
4n6time_sqlite : Saves the data in a SQLite database, used by the tool 4n6time.
           kml : Saves events with geography data into a KML format.
       dynamic : Dynamic selection of fields for a separated value output
                 format.
         rawpy : "raw" (or native) Python output.
          json : Saves the events into a JSON format.
          null : Output module that does not output anything.
           tln : TLN 5 field | delimited output.
     json_line : Saves the events into a JSON line format.
-------------------------------------------------------------------------------+---
```

L2TCSV Format – What to Fields to Focus on Initially

Date:	Date of the event, in the format of MM/DD/YYYY
Time:	Time of day, expressed in a 24h format, HH:MM:SS
Timezone:	Time zone that was used to call the tool with.
MACB:	MACB meaning of the fields, mostly for compatibility with the mactime format.
source:	Short name for the source. All web browser history is, for instance, WEBHIST, registry entries are REG, simple log file
sourcetype:	More comprehensive description of the source, "Internet Explorer" instead of WEBHIST, etc.
type:	Type of the timestamp itself, such as "Last Accessed," "Last Written," or "Last modified," and so on.
user:	Username
host:	Hostname
short:	Short description of the entry, usually contains less text than the full description field.
desc:	Description field, this is where most of the information is stored, the actual parsed description of the entry.
version:	Version number of the timestamp object.
filename:	Filename with the full path of the filename that contained the entry.
Inode:	Inode number of the file being parsed.
notes:	Some input modules insert additional information in the form of a note.
format:	Name of the input module that was used to parse the file.
extra:	Additional information parsed is joined together and put here.

psort: L2TCSV Output Format - Sample

If you have not tried this tool – you really should



Timestamp	Source...	Source Name	macb	Inode	Long Description	File Name
2012-04-03 22:08:40	Windows ...	LNK	m...	60615	[Empty description] File size: 3524 File attribute flags: 0x00002020 Drive type: 3 Drive serial number: 0xac036525 Local path: C:\Users\vibran...	TSK:/Users/vibranium/AppData/Roaming/Mi...
2012-04-03 22:08:40	Windows ...	LNK	.a..	60615	[Empty description] File size: 3524 File attribute flags: 0x00002020 Drive type: 3 Drive serial number: 0xac036525 Local path: C:\Users\vibran...	TSK:/Users/vibranium/AppData/Roaming/Mi...
2012-04-03 22:12:42	WinPrefetch	LOG	.a..	60336	Prefetch [DLLHOT.EXE] was executed - run count 4 path: \DLLHOT.EXE hash: 0x9BB7786D volume: 1 [serial number: 0xAC036525 device path: \DEVICE...	TSK:/Windows/Prefetch/DLLHOT.EXE-9BB778...
2012-04-03 22:17:59	WinPrefetch	LOG	.a..	60669	Prefetch [DLLHOST.EXE] was executed - run count 1 path: \WINDOWS\SYSTEM32\DLLHOST.EXE hash: 0x7D2183B8 volume: 1 [serial number: 0xAC036525 d...	TSK:/Windows/Prefetch/DLLHOST.EXE-7D218...
2012-04-03 22:22:15	WinPrefetch	LOG	.a..	60742	Prefetch [HELPER.EXE] was executed - run count 1 path: \PROGRAM FILES\MOZILLA FIREFOX\UNINSTALL\HELPER.EXE hash: 0x36267E56 volume: 1 [serial ...	TSK:/Windows/Prefetch/HELPER.EXE-36267E...
2012-04-03 22:37:55	UNKNOWN ...	REG	m...	47834	[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs] url1: http://199.73.28.114:53/ url2: http://go.microsoft.com/fwlink/?LinkId...	TSK:/Users/vibranium/NTUSER.DAT
2012-04-03 22:39:19	WinPrefetch	LOG	.a..	60676	Prefetch [FIREFOX.EXE] was executed - run count 3 path: \PROGRAM FILES\MOZILLA FIREFOX\FIREFOX.EXE hash: 0xE60C0AA7 volume: 1 [serial number: ...	TSK:/Windows/Prefetch/FIREFOX.EXE-E60C0...
2012-04-03 22:40:40	Windows ...	LNK	m...	60615	[Empty description] File size: 4096 File attribute flags: 0x00000011 Drive type: 3 Drive serial number: 0xac036525 Local path: C:\Users\vibran...	TSK:/Users/vibranium/AppData/Roaming/Mi...
2012-04-03 22:40:40	Windows ...	LNK	.a..	60615	[Empty description] File size: 4096 File attribute flags: 0x00000011 Drive type: 3 Drive serial number: 0xac036525 Local path: C:\Users\vibran...	TSK:/Users/vibranium/AppData/Roaming/Mi...
2012-04-03 22:40:40	Windows ...	LNK	m...	60923	[Empty description] File size: 4096 File attribute flags: 0x00000011 Drive type: 3 Drive serial number: 0xac036525 Local path: C:\Users\vibran...	TSK:/Users/vibranium/AppData/Roaming/Mi...
2012-04-03 22:40:40	Windows ...	LNK	.a..	60923	[Empty description] File size: 4096 File attribute flags: 0x00000011 Drive type: 3 Drive serial number: 0xac036525 Local path: C:\Users\vibran...	TSK:/Users/vibranium/AppData/Roaming/Mi...
2012-04-03 23:10:02	WinPrefetch	LOG	.a..	60322	Prefetch [NETSTAT.EXE] was executed - run count 3 path: \WINDOWS\SYSTEM32\NETSTAT.EXE hash: 0x6D34D712 volume: 1 [serial number: 0xAC036525 d...	TSK:/Windows/Prefetch/NETSTAT.EXE-6D34D...
2012-04-04 00:05:05	WinPrefetch	LOG	.a..	60955	Prefetch [SVCHOST.EXE] was executed - run count 2 path: \WINDOWS\SYSTEM32\DLLHOST\SVCHOST.EXE hash: 0xBD36E5C8 volume: 1 [serial number: 0xAC0...	TSK:/Windows/Prefetch/SVCHOST.EXE-BD36E...

Timeline Explorer – Eric Zimmer
https://ericzimmerman.github.io/#!index.md

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Techno Security & Digital Forensics Conference

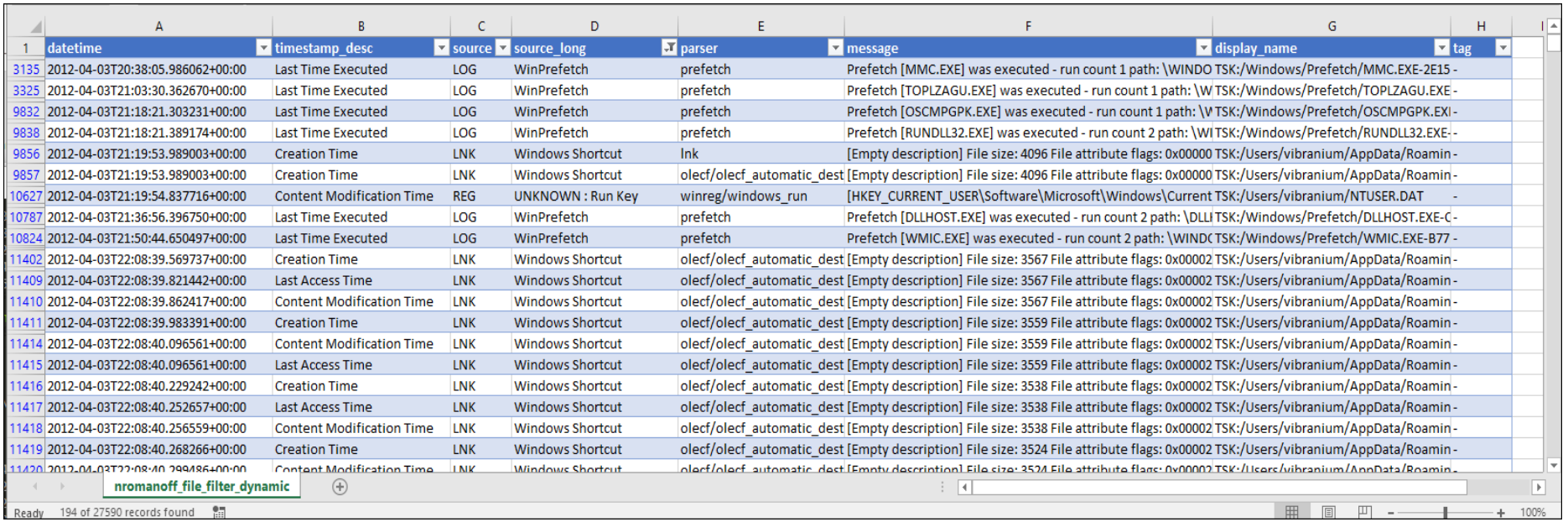
Dynamic Output Fields

These are the default fields for psort

Field Name	Description	Maps to L2TCSV
Datetime	Timestamp in ISO 8601 format	no single field
timestamp_desc	Type of the timestamp itself, such as “Last Accessed,” “Last Written,” or “Last modified,” and so on.	type
Source	Short name for the source. All web browser history is, for instance, WEBHIST, registry entries are REG, simple log files are LOG, and so on.	source
source_long	More comprehensive description of the source, “Internet Explorer” instead of WEBHIST, etc.	sourcetype
Message	Description field, this is where most of the information is stored, the actual parsed description of the entry.	desc
Parser	Name of the input module that was used to parse the file.	format
display_name	Filename with the full path of the filename that contained the entry.	filename
tag	Tag name populated by the psort analysis module(s)	N/A

psort: Dynamic Output Format - Sample

Default Format



	A	B	C	D	E	F	G	H
1	datetime	timestamp_desc	source	source_long	parser	message	display_name	tag
3135	2012-04-03T20:38:05.986062+00:00	Last Time Executed	LOG	WinPrefetch	prefetch	Prefetch [MMC.EXE] was executed - run count 1 path: \WINDO	TSK:/Windows/Prefetch/MMC.EXE-2E15	-
3325	2012-04-03T21:03:30.362670+00:00	Last Time Executed	LOG	WinPrefetch	prefetch	Prefetch [TOPLZAGU.EXE] was executed - run count 1 path: \W	TSK:/Windows/Prefetch/TOPLZAGU.EXE	-
9832	2012-04-03T21:18:21.303231+00:00	Last Time Executed	LOG	WinPrefetch	prefetch	Prefetch [OSCMPGPK.EXE] was executed - run count 1 path: \V	TSK:/Windows/Prefetch/OSCMPGPK.EXI	-
9838	2012-04-03T21:18:21.389174+00:00	Last Time Executed	LOG	WinPrefetch	prefetch	Prefetch [RUNDLL32.EXE] was executed - run count 2 path: \WI	TSK:/Windows/Prefetch/RUNDLL32.EXE-	-
9856	2012-04-03T21:19:53.989003+00:00	Creation Time	LNK	Windows Shortcut	lnk	[Empty description] File size: 4096 File attribute flags: 0x00000	TSK:/Users/vibranium/AppData/Roamin	-
9857	2012-04-03T21:19:53.989003+00:00	Creation Time	LNK	Windows Shortcut	olecf/olecf_automatic_dest	[Empty description] File size: 4096 File attribute flags: 0x00000	TSK:/Users/vibranium/AppData/Roamin	-
10627	2012-04-03T21:19:54.837716+00:00	Content Modification Time	REG	UNKNOWN : Run Key	winreg/windows_run	[HKEY_CURRENT_USER\Software\Microsoft\Windows\Current	TSK:/Users/vibranium/NTUSER.DAT	-
10787	2012-04-03T21:36:56.396750+00:00	Last Time Executed	LOG	WinPrefetch	prefetch	Prefetch [DLLHOST.EXE] was executed - run count 2 path: \DLLI	TSK:/Windows/Prefetch/DLLHOST.EXE-C	-
10824	2012-04-03T21:50:44.650497+00:00	Last Time Executed	LOG	WinPrefetch	prefetch	Prefetch [WMIC.EXE] was executed - run count 2 path: \WINDC	TSK:/Windows/Prefetch/WMIC.EXE-B77	-
11402	2012-04-03T22:08:39.569737+00:00	Creation Time	LNK	Windows Shortcut	olecf/olecf_automatic_dest	[Empty description] File size: 3567 File attribute flags: 0x00002	TSK:/Users/vibranium/AppData/Roamin	-
11409	2012-04-03T22:08:39.821442+00:00	Last Access Time	LNK	Windows Shortcut	olecf/olecf_automatic_dest	[Empty description] File size: 3567 File attribute flags: 0x00002	TSK:/Users/vibranium/AppData/Roamin	-
11410	2012-04-03T22:08:39.862417+00:00	Content Modification Time	LNK	Windows Shortcut	olecf/olecf_automatic_dest	[Empty description] File size: 3567 File attribute flags: 0x00002	TSK:/Users/vibranium/AppData/Roamin	-
11411	2012-04-03T22:08:39.983391+00:00	Creation Time	LNK	Windows Shortcut	olecf/olecf_automatic_dest	[Empty description] File size: 3559 File attribute flags: 0x00002	TSK:/Users/vibranium/AppData/Roamin	-
11414	2012-04-03T22:08:40.096561+00:00	Content Modification Time	LNK	Windows Shortcut	olecf/olecf_automatic_dest	[Empty description] File size: 3559 File attribute flags: 0x00002	TSK:/Users/vibranium/AppData/Roamin	-
11415	2012-04-03T22:08:40.096561+00:00	Last Access Time	LNK	Windows Shortcut	olecf/olecf_automatic_dest	[Empty description] File size: 3559 File attribute flags: 0x00002	TSK:/Users/vibranium/AppData/Roamin	-
11416	2012-04-03T22:08:40.229242+00:00	Creation Time	LNK	Windows Shortcut	olecf/olecf_automatic_dest	[Empty description] File size: 3538 File attribute flags: 0x00002	TSK:/Users/vibranium/AppData/Roamin	-
11417	2012-04-03T22:08:40.252657+00:00	Last Access Time	LNK	Windows Shortcut	olecf/olecf_automatic_dest	[Empty description] File size: 3538 File attribute flags: 0x00002	TSK:/Users/vibranium/AppData/Roamin	-
11418	2012-04-03T22:08:40.256559+00:00	Content Modification Time	LNK	Windows Shortcut	olecf/olecf_automatic_dest	[Empty description] File size: 3538 File attribute flags: 0x00002	TSK:/Users/vibranium/AppData/Roamin	-
11419	2012-04-03T22:08:40.268266+00:00	Creation Time	LNK	Windows Shortcut	olecf/olecf_automatic_dest	[Empty description] File size: 3524 File attribute flags: 0x00002	TSK:/Users/vibranium/AppData/Roamin	-
11420	2012-04-03T22:08:40.299486+00:00	Content Modification Time	LNK	Windows Shortcut	olecf/olecf_automatic_dest	[Empty description] File size: 3524 File attribute flags: 0x00002	TSK:/Users/vibranium/AppData/Roamin	-

nromanoff_file_filter_dynamic

Ready 194 of 27590 records found 100%

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Techno Security & Digital Forensics Conference

Additional Output Fields

- **--additional_fields option**
- Adds additional fields to the default output list
- Option works with “dynamic” output type
- Can be context sensitive
- Unfortunately, not compatible with “l2tcsv” output format
  - **But, <u>additional fields can be used in filters</u>**
  - Look at the JSON output for additional fields

Default Output Fields

1. datetime
2. timestamp_desc
3. source
4. source_long
5. message
6. parser
7. display_name
8. tag

data_type: Additional Filterable Fields

- Can provide more granularity that any other single field
- In some cases, sourcetype, parser and data_type can provide the same results

Windows Registry	FS Activity
windows:registry:amcache	fs:mactime:line
windows:registry:amcache:programs	fs:stat
windows:registry:appcompatcache	fs:stat:ntfs
windows:registry:installation	windows:lnk:link
windows:registry:key_value	windows:shell_item:file_entry
windows:registry:list	windows:volume:creation
windows:registry:network	
windows:registry:office_mru	

Data Types: 130+ Identified to Date

Windows Registry	FS Activity	MAC	Browser
windows:registry:amcache	fs:mactime:line	mac:appfirewall:line	firefox:cache:record
windows:registry:amcache:programs	fs:stat	mac:asl:event	firefox:cookie:entry
windows:registry:appcompatcache	fs:stat:ntfs	mac:document_versions:file	firefox:downloads:download
windows:registry:installation	windows:lnk:link	mac:keychain:application	firefox:places:bookmark
windows:registry:key_value	windows:shell_item:file_entry	mac:keychain:internet	firefox:places:bookmark_annotation
windows:registry:list	windows:volume:creation	mac:securityd:line	firefox:places:bookmark_folder
windows:registry:network		mac:utmpx:event	firefox:places:page_visited
windows:registry:office_mru		mac:wifilog:line	chrome:cache:entry
		imessage:event:chat	chrome:cookie:entry
windows:registry:sam_users		mackeeper:cache	chrome:extension_activity:activity_log
windows:registry:service		macos:fseventsd:record	chrome:history:file_downloaded
windows:registry:shutdown		macosx:application_usage	chrome:history:page_visited
windows:registry:userassist		macosx:lsquarantine	chrome:preferences:clear_history

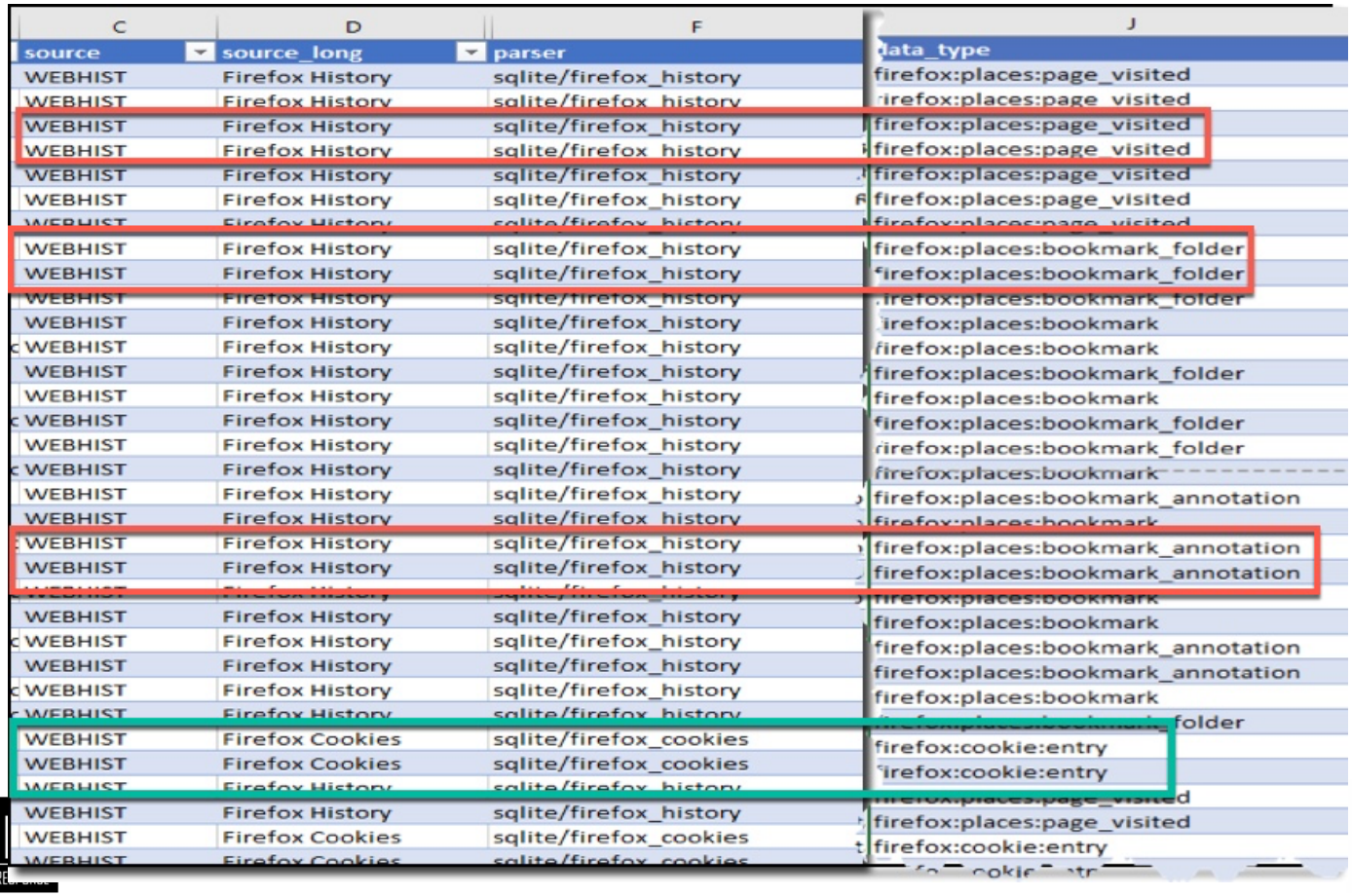
GitHub

Complete List Available on my GitHub Page

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Techno Security & Digital Forensics Conference

data_type Field as Filter – dynamic output More Granularity



C	D	F	J
source	source_long	parser	data_type
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:page_visited
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:page_visited
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:page_visited
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:page_visited
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:page_visited
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:page_visited
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark_folder
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark_folder
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark_folder
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark_folder
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark_folder
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark_folder
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark_annotation
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark_annotation
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark_annotation
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark_annotation
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark_annotation
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:bookmark
WEBHIST	Firefox History	sqlite/firefox_history	folder
WEBHIST	Firefox Cookies	sqlite/firefox_cookies	firefox:cookie:entry
WEBHIST	Firefox Cookies	sqlite/firefox_cookies	firefox:cookie:entry
WEBHIST	Firefox History	sqlite/firefox_history	firefox:places:page_visited
WEBHIST	Firefox Cookies	sqlite/firefox_cookies	firefox:cookie:entry

Red: Example of more detail

Green: Example other fields with same information

data_type Field as Filter – l2tcsv output More Granularity

378 rows

	date	time	source	sourcetype	type	desc	filename	format	extra
2	8/15/2011	14:12:28	WEBHIST	Firefox History	Last Visited Time	http://go.	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefc
3	8/15/2011	14:12:32	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefc
4	8/15/2011	14:13:32	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefc
5	8/15/2011	14:13:32	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefc
6	8/15/2011	14:13:38	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefc
7	8/15/2011	14:15:24	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefc
8	8/15/2011	14:15:58	WEBHIST	Firefox History	Last Visited Time	http://mc	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefc
9	3/15/2012	21:25:24	WEBHIST	Firefox History	Creation Time	N/A	TSK:/Users/	sqlite/firefox_history	parser_chain: sqlite/firefox_history; schema_match: False; sha256_hash: b3abee
10	3/15/2012	21:25:24	WEBHIST	Firefox History	Creation Time	Bookmark	TSK:/Users/	sqlite/firefox_history	parser_chain: sqlite/firefox_history; schema_match: False; sha256_hash: b3abee
11	3/15/2012	21:25:24	WEBHIST	Firefox History	Creation Time	Bookmark	TSK:/Users/	sqlite/firefox_history	parser_chain: sqlite/firefox_history; schema_match: False; sha256_hash: b3abee
12	3/15/2012	21:25:24	WEBHIST	Firefox History	Creation Time	Tags	TSK:/Users/	sqlite/firefox_history	parser_chain: sqlite/firefox_history; schema_match: False; sha256_hash: b3abee
13	3/15/2012	21:25:24	WEBHIST	Firefox History	Content Modification Time	N/A	TSK:/Users/	sqlite/firefox_history	parser_chain: sqlite/firefox_history; schema_match: False; sha256_hash: b3abee
14	3/15/2012	21:25:24	WEBHIST	Firefox History	Content Modification Time	Tags	TSK:/Users/	sqlite/firefox_history	parser_chain: sqlite/firefox_history; schema_match: False; sha256_hash: b3abee
15	3/15/2012	21:25:24	WEBHIST	Firefox History	Creation Time	Unsorted	TSK:/Users/	sqlite/firefox_history	parser_chain: sqlite/firefox_history; schema_match: False; sha256_hash: b3abee
16	3/15/2012	21:25:25	WEBHIST	Firefox History	Content Modification Time	Unsorted	TSK:/Users/	sqlite/firefox_history	parser_chain: sqlite/firefox_history; schema_match: False; sha256_hash: b3abee
17	3/15/2012	21:25:25	WEBHIST	Firefox History	Creation Time	Bookmark	TSK:/Users/	sqlite/firefox_history	host: moc.allizom.www.; parser_chain: sqlite/firefox_history; schema_match: Fa
18	3/15/2012	21:25:25	WEBHIST	Firefox History	Content Modification Time	Bookmark	TSK:/Users/	sqlite/firefox_history	host: moc.allizom.www.; parser_chain: sqlite/firefox_history; schema_match: Fa
19	3/15/2012	21:25:25	WEBHIST	Firefox History	Creation Time	Latest Hea	TSK:/Users/	sqlite/firefox_history	parser_chain: sqlite/firefox_history; schema_match: False; sha256_hash: b3abee
20	3/15/2012	21:25:25	WEBHIST	Firefox History	Creation Time	Bookmark	TSK:/Users/	sqlite/firefox_history	host: moc.allizom.www.; parser_chain: sqlite/firefox_history; schema_match: Fa
21	3/15/2012	21:25:25	WEBHIST	Firefox History	Content Modification Time	Latest Hea	TSK:/Users/	sqlite/firefox_history	parser_chain: sqlite/firefox_history; schema_match: False; sha256_hash: b3abee
22	3/15/2012	21:25:25	WEBHIST	Firefox History	Creation Time	Mozilla Fi	TSK:/Users/	sqlite/firefox_history	parser_chain: sqlite/firefox_history; schema_match: False; sha256_hash: b3abee
23	3/15/2012	21:25:25	WEBHIST	Firefox History	Content Modification Time	Bookmark	TSK:/Users/	sqlite/firefox_history	host: moc.allizom.www.; parser_chain: sqlite/firefox_history; schema_match: Fa
24	3/15/2012	21:25:25	WEBHIST	Firefox History	Creation Time	Bookmark	TSK:/Users/	sqlite/firefox_history	host: moc.allizom.www.; parser_chain: sqlite/firefox_history; schema_match: Fa
25	3/15/2012	21:25:25	WEBHIST	Firefox History	Content Modification Time	Bookmark	TSK:/Users/	sqlite/firefox_history	host: moc.allizom.www.; parser_chain: sqlite/firefox_history; schema_match: Fa
26	3/15/2012	21:25:25	WEBHIST	Firefox History	Creation Time	Bookmark	TSK:/Users/	sqlite/firefox_history	host: moc.allizom.www.; parser_chain: sqlite/firefox_history; schema_match: Fa
27	3/15/2012	21:25:25	WEBHIST	Firefox History	Content Modification Time	Bookmark	TSK:/Users/	sqlite/firefox_history	host: moc.allizom.www.; parser_chain: sqlite/firefox_history; schema_match: Fa

"sourcetype is 'Firefox History'"

25 rows

	date	time	source	sourcetype	type	desc	filename	format	extra
2	8/15/2011	14:12:28	WEBHIST	Firefox History	Last Visited Time	http://go.	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefox_histo
3	8/15/2011	14:12:32	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefox_histo
4	8/15/2011	14:13:32	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefox_histo
5	8/15/2011	14:13:32	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefox_histo
6	8/15/2011	14:13:38	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefox_histo
7	8/15/2011	14:15:24	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefox_histo
8	8/15/2011	14:15:58	WEBHIST	Firefox History	Last Visited Time	http://mo	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefox_histo
9	3/15/2012	21:36:53	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefox_histo
10	3/15/2012	21:36:56	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'visited from: http://www.mozilla.com/en-US/firefox/5.0.1/firstrun/ (www.mo
11	3/15/2012	21:38:07	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefox_histo
12	3/15/2012	21:38:17	WEBHIST	Firefox History	Last Visited Time	http://do	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefox_histo
13	3/15/2012	21:38:23	WEBHIST	Firefox History	Last Visited Time	http://dw	TSK:/Users/	sqlite/firefox_history	extra: [u'visited from: http://download.cnet.com/Free-File-Wiper/3000-2248_4-7544738
14	3/15/2012	21:38:23	WEBHIST	Firefox History	Last Visited Time	http://do	TSK:/Users/	sqlite/firefox_history	extra: [u'visited from: http://dw.com.com/redir?edId=3&siteId=4&oId=3000-2248_4-754
15	3/15/2012	21:38:24	WEBHIST	Firefox History	Last Visited Time	http://do	TSK:/Users/	sqlite/firefox_history	extra: [u'visited from: http://download.cnet.com/3001-2248_4-75447382.html?spi=31ed
16	3/15/2012	21:40:25	WEBHIST	Firefox History	Last Visited Time	http://do	TSK:/Users/	sqlite/firefox_history	extra: [u'visited from: http://download.cnet.com/Free-File-Wiper/3001-2248_4-7544738
17	4/3/2012	22:21:36	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefox_histo
18	4/3/2012	22:21:38	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'visited from: http://www.mozilla.com/en-US/firefox/5.0.1/firstrun/ (www.mo
19	4/3/2012	22:22:42	WEBHIST	Firefox History	Last Visited Time	http://ww	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefox_histo
20	4/3/2012	22:23:00	WEBHIST	Firefox History	Last Visited Time	http://en.	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: LINK']; parser_chain: sqlite/firefox_histo
21	4/3/2012	22:24:01	WEBHIST	Firefox History	Last Visited Time	http://19	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: TYPED']; parser_chain: sqlite/firefox_hist
22	4/3/2012	22:28:36	WEBHIST	Firefox History	Last Visited Time	http://19	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: TYPED']; parser_chain: sqlite/firefox_hist
23	4/3/2012	22:40:08	WEBHIST	Firefox History	Last Visited Time	http://207	TSK:/Users/	sqlite/firefox_history	extra: [u'(URL not typed directly)' u'Transition: TYPED']; parser_chain: sqlite/firefox_hist

"DATA_TYPE is 'firefox:places:page_visited'"

Context Sensitive Fields: LNK Files

Example: LNK File events can be filtered on all these fields

Field	Description
birth_droid_file_identifier	distributed link tracking birth droidÂ file identifier.
birth_droid_volume_identifier	distributed link tracking birth droidÂ Â volume identifier.
command_line_arguments	**command line arguments.**
description	description of the linked item.
drive_serial_number	**drive serial number where the linked itemÂ resides.**
drive_type	**drive type where the linked item resided.**
droid_file_identifier	distributed link tracking droid fileÂ identifier.
droid_volume_identifier	distributed link tracking droid volume identifier.
env_var_location	evironment variables loction.
file_attribute_flags	file attribute flags of the linked item.
file_size	size of the linked item.
icon_location	icon location.
link_target	shell item list of the link target.
local_path	local path of the linked item.
network_path	local path of the linked item.
relative_path	relative path.
volume_label	**volume label where the linked item resided.**
working_directory	working directory.

Data Type = windows:lnk:link

Output type == dynamic

datetime	timestamp_desc	source	source_long	parser	display_name	data_type	drive_serial_number	drive_type
2016-06-18T04:00:00+00:00	Last Access Time	LNK	Windows Shortcut	olecf/olecf_automatic_destinations/lnk	Recent\AutomaticDestinations\f01b4d95cf55d32a.automaticDest	windows:lnk:link	3031252929	2
2016-06-18T04:00:00+00:00	Last Access Time	LNK	Windows Shortcut	olecf/olecf_automatic_destinations/lnk	Recent\AutomaticDestinations\5f7b5f1e01b83767.automaticDes	windows:lnk:link	3031252929	2
2016-06-18T04:00:00+00:00	Last Access Time	LNK	Windows Shortcut	olecf/olecf_automatic_destinations/lnk	Recent\AutomaticDestinations\b8ab77100df80ab2.automaticDes	windows:lnk:link	3031252929	2
2016-06-18T04:00:00+00:00	Last Access Time	LNK	Windows Shortcut	lnk	Recent\Nondeflagellated Cultures.xlsx.lnk	windows:lnk:link	3031252929	2
2016-06-18T22:48:26+00:00	Content Modification Time	LNK	Windows Shortcut	olecf/olecf_automatic_destinations/lnk	Recent\AutomaticDestinations\f01b4d95cf55d32a.automaticDest	windows:lnk:link	3031252929	2
2016-06-18T22:56:55.940000+00:00	Creation Time	LNK	Windows Shortcut	olecf/olecf_automatic_destinations/lnk	Recent\AutomaticDestinations\f01b4d95cf55d32a.automaticDest	windows:lnk:link	3031252929	2
2016-06-18T22:56:58.380000+00:00	Creation Time	LNK	Windows Shortcut	olecf/olecf_automatic_destinations/lnk	Recent\AutomaticDestinations\5f7b5f1e01b83767.automaticDes	windows:lnk:link	3031252929	2
2016-06-18T22:56:58.380000+00:00	Creation Time	LNK	Windows Shortcut	olecf/olecf_automatic_destinations/lnk	Recent\AutomaticDestinations\b8ab77100df80ab2.automaticDes	windows:lnk:link	3031252929	2
2016-06-18T22:56:58.380000+00:00	Creation Time	LNK	Windows Shortcut	lnk	Recent\Nondeflagellated Cultures.xlsx.lnk	windows:lnk:link	3031252929	2
2016-06-29T19:14:10+00:00	Content Modification Time	LNK	Windows Shortcut	lnk	Recent\L8-Bio-jpg5.jpg.lnk	windows:lnk:link	1448121759	2
2016-06-29T19:14:10+00:00	Content Modification Time	LNK	Windows Shortcut	olecf/olecf_automatic_destinations/lnk	Recent\AutomaticDestinations\5f7b5f1e01b83767.automaticDes	windows:lnk:link	1448121759	2
2016-06-29T19:22:58+00:00	Content Modification Time	LNK	Windows Shortcut	lnk	Recent\L8-Bio-gif4.gif.lnk	windows:lnk:link	1448121759	2
2016-06-29T19:22:58+00:00	Content Modification Time	LNK	Windows Shortcut	olecf/olecf_automatic_destinations/lnk	Recent\AutomaticDestinations\5f7b5f1e01b83767.automaticDes	windows:lnk:link	1448121759	2
2016-06-29T19:22:58+00:00	Content Modification Time	LNK	Windows Shortcut	olecf/olecf_automatic_destinations/lnk	Recent\AutomaticDestinations\a52b0784bd667468.automaticDes	windows:lnk:link	1448121759	2

```
psort.exe -z "UTC" -o dynamic --additional_fields
"data_type,drive_serial_number,drive_type,droid_file_identifier"
-w add_fields_drive_type.csv file_filter.plaso "data_type is 'windows:lnk:link' and
drive_type == 2"
```

Data Type = windows:lnk:link

Output type == l2tcsv

date	time	MA	source	sourcetype	type	desc	filename	format
1/1/1970	12:00:00 AM	....	LNK	Windows Shortcut	Not a time	[Empty description] File size: 0 File attribute fl	\BitLocker Recovery Key 78E26069-03C3-46A7-9E8A-F366D2D9C	lnk
1/1/1970	12:00:00 AM	....	LNK	Windows Shortcut	Not a time	[Empty description] File size: 0 File attribute fl	\AutomaticDestinations\5f7b5f1e01b83767.automaticDestinati	olecf/olecf_automatic_destinations/lnk
1/1/1970	12:00:00 AM	....	LNK	Windows Shortcut	Not a time	[Empty description] File size: 0 File attribute fl	\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinati	olecf/olecf_automatic_destinations/lnk
1/1/1970	12:00:00 AM	....	LNK	Windows Shortcut	Not a time	[Empty description] File size: 0 File attribute fl	\Vanko-RAM.dmp.lnk	lnk
1/1/1970	12:00:00 AM	....	LNK	Windows Shortcut	Not a time	[Empty description] File size: 0 File attribute fl	\AutomaticDestinations\5f7b5f1e01b83767.automaticDestinati	olecf/olecf_automatic_destinations/lnk
1/1/1980	4:00:00 AM	MA.B	LNK	Windows Shortcut	Content Modification Time; Creatior	[Empty description] File size: 0 File attribute fl	\StarkResrch (D).lnk	lnk
1/1/1980	4:00:00 AM	MA.B	LNK	Windows Shortcut	Content Modification Time; Creatior	[Empty description] File size: 0 File attribute fl	\VankoBlue (D) (2).lnk	lnk
1/1/1980	4:00:00 AM	MA.B	LNK	Windows Shortcut	Content Modification Time; Creatior	[Empty description] File size: 0 File attribute fl	\VankoBlue (D).lnk	lnk
1/1/1980	4:00:00 AM	MA.B	LNK	Windows Shortcut	Content Modification Time; Creatior	[Empty description] File size: 0 File attribute fl	\STARK_ENT (D).lnk	lnk
1/1/1980	4:00:00 AM	MA.B	LNK	Windows Shortcut	Content Modification Time; Creatior	[Empty description] File size: 0 File attribute fl	\Secure Digital storage device (D).lnk	lnk
1/1/1980	4:00:00 AM	MA.B	LNK	Windows Shortcut	Content Modification Time; Creatior	[Empty description] File size: 0 File attribute fl	\DUCKY (D).lnk	lnk
1/1/1980	4:00:00 AM	MA.B	LNK	Windows Shortcut	Content Modification Time; Creatior	[Empty description] File size: 0 File attribute fl	\Stark-IR (D).lnk	lnk
10/16/2012	7:31:00 PM	M...	LNK	Windows Shortcut	Content Modification Time	[Empty description] File size: 0 File attribute fl	\help.lnk	lnk
10/16/2012	7:31:00 PM	M...	LNK	Windows Shortcut	Content Modification Time	[Empty description] File size: 0 File attribute fl	\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinati	olecf/olecf_automatic_destinations/lnk
10/16/2012	7:31:00 PM	M...	LNK	Windows Shortcut	Content Modification Time	[Empty description] File size: 0 File attribute fl	\enu.lnk	lnk
10/16/2012	7:31:00 PM	M...	LNK	Windows Shortcut	Content Modification Time	[Empty description] File size: 0 File attribute fl	\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinati	olecf/olecf_automatic_destinations/lnk
10/16/2012	7:31:00 PM	M...	LNK	Windows Shortcut	Content Modification Time	[Empty description] File size: 0 File attribute fl	\langs.lnk	lnk
10/16/2012	7:31:00 PM	M...	LNK	Windows Shortcut	Content Modification Time	[Empty description] File size: 0 File attribute fl	\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinati	olecf/olecf_automatic_destinations/lnk
8/22/2013	3:36:31 PM	...B	LNK	Windows Shortcut	Creation Time	[Empty description] File size: 0 File attribute fl	\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinati	olecf/olecf_automatic_destinations/lnk
5/17/2014	4:20:08 PM	M...	LNK	Windows Shortcut	Content Modification Time	[Empty description] File size: 0 File attribute fl	\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinati	olecf/olecf_automatic_destinations/lnk
7/13/2014	11:35:52 PM	.A..	LNK	Windows Shortcut	Last Access Time	[Empty description] File size: 0 File attribute fl	\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinati	olecf/olecf_automatic_destinations/lnk
12/24/2014	3:23:26 PM	M...	LNK	Windows Shortcut	Content Modification Time	[Empty description] File size: 0 File attribute fl	\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinati	olecf/olecf_automatic_destinations/lnk
8/8/2015	9:07:50 PM	.A..	LNK	Windows Shortcut	Last Access Time	[Empty description] File size: 0 File attribute fl	\Pics.lnk	lnk

```
psort.exe -z "UTC" -o l2tcsv -w filter_on_add_fields.csv file_filter.plaso "data_type
is 'windows:lnk:link' and drive_type == 2"
```

Context Sensitive Fields: SAM Registry

Example: SAM Users events can be filtered on all these fields

DATA_TYPE = 'windows:registry:sam_users'

Field	Description
account_rid (int)	account relative identifier (RID).
comments (str)	comments
fullname (str)	full name
key_path (str)	Windows Registry key path
login_count (int)	login count
username (str)	username (str)

Context Sensitive Fields: Prefetch Files

Example: Prefetch events can be filtered on all these fields

DATA_TYPE = 'windows:prefetch:execution '

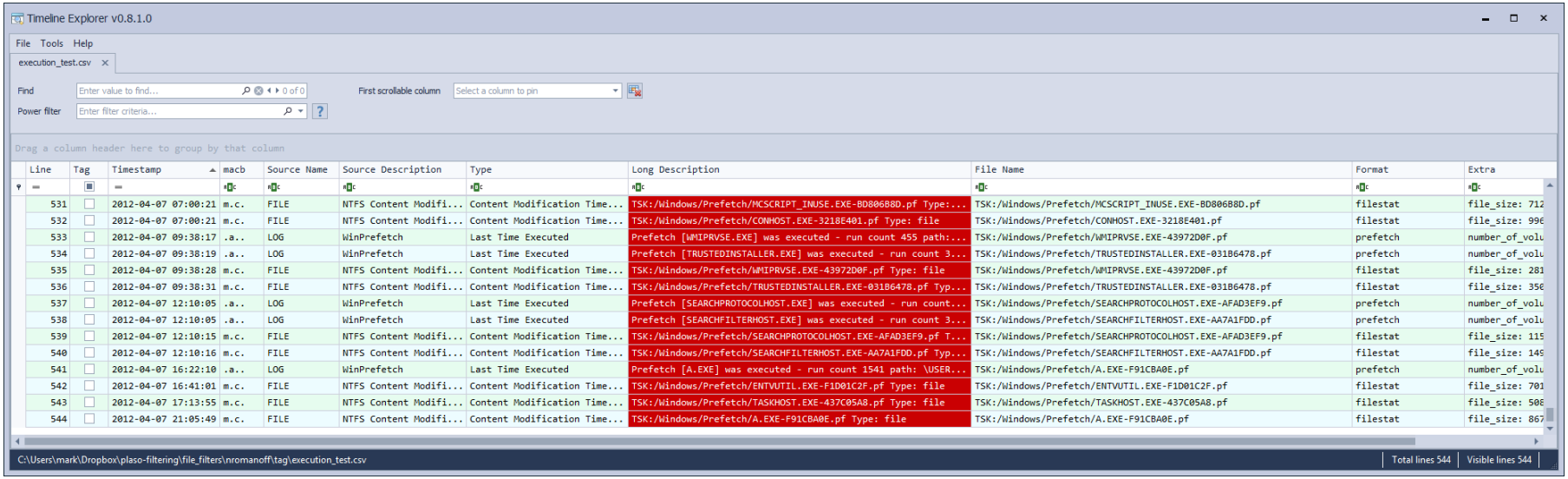
Field	Description
executable (str)	executable filename
format_version (int)	format version
mapped_files (list[str])	mapped filenames
number_of_volumes (int)	number of volumes
path (str)	path to the executable
prefetch_hash (int)	prefetch hash
mapped_files (list[str])	mapped filenames
volume_device_paths (list[str])	volume device paths
volume_serial_numbers (list[int])	volume serial numbers

Filter Example: Evidence of Execution

```
psort -z "UTC" -o l2tcsv -w execution_test.csv file_filter.plaso
"message contains 'Prefetch {' or
message contains 'AppCompatCache' or
message contains 'typed the following cmd' or
message contains 'CMD typed' or
message contains 'Last run' or
message contains 'RunMRU' or
message contains 'MUICache' or
message contains 'UserAssist key' or
message contains 'Time of Launch' or
message contains 'Prefetch' or
message contains 'SHIMCACHE' or
message contains 'Scheduled' or
message contains '.pf' or
message contains 'was run' or
message contains 'UEME_' or message contains '[PROCESS]'"
```

- Sample of Evidence of Execution logic used by Timeline Explorer. Developed by Eric Zimmerman.
- This logic can be implemented as a psort filter.
- Logic is not compatible with psort tagging. 😞

Filter Results: Evidence of Execution



psort -z "UTC" -o l2tcsv -w execution_test.csv file_filter.plaso "message contains 'Prefetch {' or message contains 'AppCompatCache' or message contains 'typed the following cmd' or message contains 'CMD typed' or message contains 'Last run' or message contains 'RunMRU' or message contains 'MUICache' or message contains 'UserAssist key' or message contains 'Time of Launch' or message contains 'Prefetch' or message contains 'SHIMCACHE' or message contains 'Scheduled' or message contains '.pf' or message contains 'was run' or message contains 'UEME_' or message contains '[PROCESS]'"

log2timeline parsers versus psort filters

```
D:\Dropbox (Personal)\plaso-filtering\file_filters\nromanoff
λ psort -z "UTC" -o l2tcsv -w nromanoff_USB_filter_parsers.csv nromanoff_file_filter.plaso "pa
rser is 'windows_usbstor_devices' or parser is 'windows_usb_devices'"
2018-06-05 22:33:11,549 [WARNING] (MainProcess) PID:17868 <psort_tool> Appending to an already existin
g storage file.
C:\Plaso\plaso\engine\process_info.py:41: FutureWarning: memory_info_ex() is deprecated and will be removed; u
se memory_info() instead
Processing completed.

********** Export results **********
      Events filtered : 301594
Events from time slice : 0
     Events processed : 0
------------------------------------------------------------------------

D:\Dropbox (Personal)\plaso-filtering\file_filters\nromanoff
```

log2timeline parsers versus psort filters

```
D:\Dropbox (Personal)\plaso-filtering\file_filters\nromanoff
λ psort -z "UTC" -o l2tcsv -w nromanoff_USB_filter_parser_message.csv nromanoff_file_filte
r.plaso "message contains 'MountPoints2' or message contains 'volume mounted' or message c
ontains 'USB' or message contains '/USB/Vid_' or message contains 'Enum/USBSTOR/Disk' or m
essage contains 'RemovableMedia' or message contains 'STORAGE/RemovableMedia' or message c
ontains 'drive mounted' or message contains 'Drive last mounted' or message contains 'Setu
pAPI Log'"
2018-06-05 22:18:32,346 [WARNING] (MainProcess) PID:19120 <psort_tool> Appending to an alr
eady existing storage file.
C:\Plaso\plaso\engine\process_info.py:41: FutureWarning: memory_info_ex() is deprecated an
d will be removed; use memory_info() instead
Processing completed.

********************************** Export results **********************************
        Events filtered : 208049
      Events processed : 2645
     Events MACB grouped : 2600
Duplicate events removed : 7
  Events from time slice : 0
------------------------------------------------------------------------------
```

Time Filtering – Data Range

```
psort.py -z "UTC" -o l2tcsv -w nromanoff_l2tcsv nromanoff.plaso
"date > '2012-04-03 00:00:00' AND date < '2012-04-07 00:00:00'"
```

Time Filtering – Slice

- Provides context around an date/time
- Create a time slice around a certain date
- Display all events that happened X minutes before and after the defined date
- --slice_size defines the size of the slice
- Defaults to 5 minutes.

```
psort.py -z "UTC" -o l2tcsv --slice '2012-04-05 22:12:00'
-w nromanoff_l2tcsv nromanoff.plaso "data_type
is 'windows:lnk:link’ and drive_type == 2"
```

Time Filtering – Slicer

- Creates a Time Slice Around every Filter match
- Will save all X events before and after a filter match
- X is set with the --slice option
- Defaults to 5 events.

```
psort.py -z "UTC" -o l2tcsv –slicer –slice_size 10
-w nromanoff_l2tcsv nromanoff.plaso "data_type is
'windows:lnk:link’
and drive_type == 2"
```

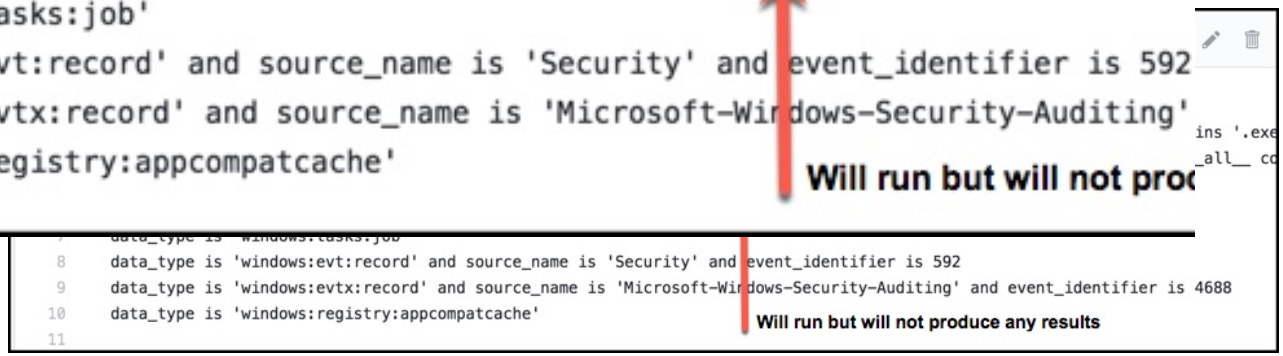
Tagging

93 lines (71 sloc) | 5.87 KB

```
1   application execution
2     data_type is 'windows:prefetch'
3     data_type is 'windows:lnk:link' and filename contains 'Recent' and (local_path contains '.e
4     data_type is 'windows:registry:key_value' AND (plugin contains 'userassist' or plugin conta
5     data_type is 'windows:evtx:record' and strings contains 'user mode service' and strings con
6     data_type is 'fs:stat' and filename contains 'Windows/Tasks/At'
7     data_type is 'windows:tasks:job'
8     data_type is 'windows:evt:record' and source_name is 'Security' and event_identifier is 592
9     data_type is 'windows:evtx:record' and source_name is 'Microsoft-Windows-Security-Auditing'
10    data_type is 'windows:registry:appcompatcache'
11
```

'windows:prefetch:executition'

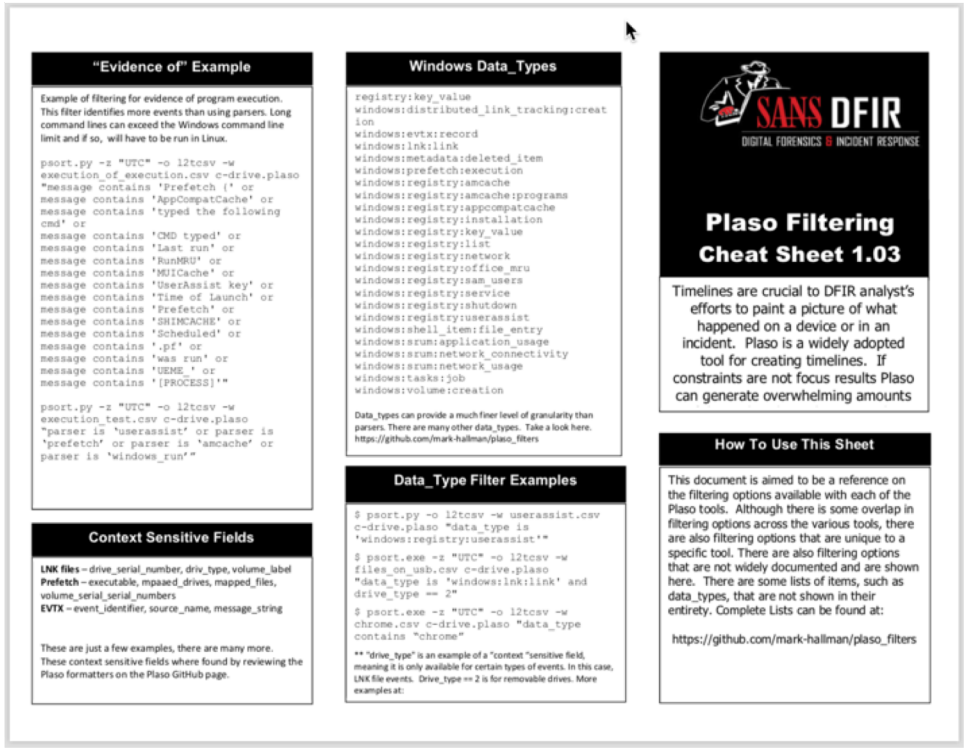
Will run but will not proc



Testing – How did you find these other fields?

- Looking at other formats (json, etc).
- Looking at code
- Looking at tagging files

Plaso Filtering Cheat Sheet



"Evidence of" Example

Example of filtering for evidence of program execution. This filter identifies more events than using parsers. Long command lines can exceed the Windows command line limit and if so, will have to be run in Linux.

```
psort.py -z "UTC" -o l2tcsv -w
execution_of_execution.csv c-drive.plaso
"message contains 'Prefetch (' or
message contains 'AppCompatCache' or
message contains 'typed the following
cmd' or
message contains 'CMD typed' or
message contains 'Last run' or
message contains 'RunMRU' or
message contains 'MUICache' or
message contains 'UserAssist key' or
message contains 'Time of Launch' or
message contains 'Prefetch' or
message contains 'SHIMCACHE' or
message contains 'Scheduled' or
message contains '.pf' or
message contains 'was run' or
message contains 'UEME_' or
message contains '[PROCESS]'"

psort.py -z "UTC" -o l2tcsv -w
execution_test.csv c-drive.plaso
"parser is 'userassist' or parser is
'prefetch' or parser is 'amcache' or
parser is 'windows_run'"
```

Context Sensitive Fields

LNK files – drive_serial_number, driv_type, volume_label
Prefetch – executable, mpaaed_drives, mapped_files, volume_serial_serial_numbers
EVTX – event_identifier, source_name, message_string

These are just a few examples, there are many more. These context sensitive fields where found by reviewing the Plaso formatters on the Plaso GitHub page.

Windows Data_Types

```
registry:key_value
windows:distributed_link_tracking:creat
ion
windows:evtx:record
windows:lnk:link
windows:metadata:deleted_item
windows:prefetch:execution
windows:registry:amcache
windows:registry:amcache:programs
windows:registry:appcompatcache
windows:registry:installation
windows:registry:key_value
windows:registry:list
windows:registry:network
windows:registry:office_mru
windows:registry:sam_users
windows:registry:service
windows:registry:shutdown
windows:registry:userassist
windows:shell_item:file_entry
windows:srum:application_usage
windows:srum:network_connectivity
windows:srum:network_usage
windows:tasks:job
windows:volume:creation
```

Data_types can provide a much finer level of granularity than parsers. There are many other data_types. Take a look here. https://github.com/mark-hallman/plaso_filters

Data_Type Filter Examples

```
$ psort.py -o l2tcsv -w userassist.csv
c-drive.plaso "data_type is
'windows:registry:userassist'"

$ psort.exe -z "UTC" -o l2tcsv -w
files_on_usb.csv c-drive.plaso
"data_type is 'windows:lnk:link' and
drive_type == 2"

$ psort.exe -z "UTC" -o l2tcsv -w
chrome.csv c-drive.plaso "data_type
contains "chrome"
```

** "drive_type" is an example of a "context "sensitive field, meaning it is only available for certain types of events. In this case, LNK file events. Drive_type == 2 is for removable drives. More examples at:

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Plaso Filtering Cheat Sheet 1.03

Timelines are crucial to DFIR analyst's efforts to paint a picture of what happened on a device or in an incident. Plaso is a widely adopted tool for creating timelines. If constraints are not focus results Plaso can generate overwhelming amounts

How To Use This Sheet

This document is aimed to be a reference on the filtering options available with each of the Plaso tools. Although there is some overlap in filtering options across the various tools, there are also filtering options that are unique to a specific tool. There are also filtering options that are not widely documented and are shown here. There are some lists of items, such as data_types, that are not shown in their entirety. Complete Lists can be found at:

https://github.com/mark-hallman/plaso_filters

image_export

Files can be extracted by filter file, extension, date filter, signature. The Filter File is the same format as the file used for log2timeline.

```
$ image_export -f filter_windows.txt
--no_vss -w export_folder_name c-
drive.e01
```

Timestamp types: atime, ctime, crtime, bkup

```
$ image_export.py -vss_stores all
-x "doc,docx,xls,xlsx,ppt,pptx,pdf"
--date_filter "crtime, 2013-10-21,
2013-10-23" -w c-drive_docs_export c-
drive.e01
```

log2timeline

Log2timeline Filtering Options: 1. File filters and 2. Parsers. These options can significantly decrease the number of events returned and time to execute. Eg. 2.5 hours down to 2.5 minutes.

Example filter files can be found at:
https://github.com/mark-hallman/plaso_filters

Get help and list all the parsers with:

```
$ log2timeline.py --info
```

Use filter file and process no VSS's:

```
$ log2timeline.py -f
filter_windows.txt
--no_vss c-drive.plaso c-drive.E01
```

Use filter file, process All VSS's (and live) and use a list of parsers

```
$ log2timeline.py -f
filter_windows.txt -parsers
"amcache,prefetch,userassist"
--vss_stores all c-drive.plaso c-
drive.E01
```

Source does not have to be an image

```
$ log2timeline.py triage.plaso
/mnt/windows_mount
```

psort

Output Formats

```
$ psort.py -o list
```

– Shows all available formats

Commonly used output formats

l2tcsv – 17 field legacy log2timeline fixed format
`date,time,timezone,MACB,source,sourcetype,type,user,host,short,desc,version,filename,inode,notes,format,extra`

dynamic – default output 9 fields. Fields can be added or removed from this format. `datetime, timestamp_desc, source, source_long,message, parser, display_name,tag`

dynamic output examples using --fields & --additional_fields

```
$ psort.py -z "UTC" -o dynamic –
additional_fields
"data_type,strings,event_type" -w
add_fields.csv
c-drive.plaso

$ psort.py -z "UTC" -o dynamic --fields
"datetime,macb,data_type,drive_serial_nu
mber,drive_type" -w winlnk.csv c-
drive.plaso "data_type is
'windows:lnk:link'"
```

Filter on fields that are not in output format

```
$ psort.py -z "UTC" -o l2tcsv -w
winlnk.csv c-drive.plaso "data_type is
'windows:lnk:link' and drive_type == 2"
```

Start with date as a filter. Best for larger ranges.

```
psort.py -z "UTC" -w date_filtered.csv
c-drive.plaso "date > '2018-10-11
00:00:00' AND date < '2018-10-22
023:59:59'"
```

Time Slice – Best for smaller, targeted, ranges.

```
psort.py -z "UTC" --slice '2018-10-22
010:59:59' -slice_size 1 -w sliced.csv
c-drive.plaso
```

Slicer – Event context- Nbr of events surrounding each filtered event

```
psort.py -z "UTC" --slice_size 20 --
slicer -w slicer.csv c-drive.plaso
```

Filtering Tips

- Parsers and file filters with log2timeline are a good practice most of the time.
- "contains" == case insensitive "is" == case sensitive
- No parsers == default to "win7"
- data_types are all lower case.
- All commands are shown with the .py as run from Ubuntu. Windows version has a .exe extension
- Image_export – easy way to get files out of VSS's
- Plaso runs very well in Windows. No VM, simple to install and you have easy access to your other Windows tools.
- "date" used in filters is the date field in the default (dynamic) output
- Multiple psort output files (csv) can be concatenated if you have filters that can't be expressed in a single statement.

Event Tagging

Tagging populates the "tag" field in the Plaso DB based upon rules define in the tag file. That tag value can then be used to filter. Tags are assigned to events based upon rules defined in the tagging file. An event can be responsive more than one tag rule or to no rule at all. Events that are responsive to more than one expression will have a tag value similar to (tag1,tag2,tag5). The tag field can included in your output when using the Dynamic output format (-o dynamic)

The message, also referred to as long_desc, can't be used in a tagging file expression.

Run the tagging process with tag_file

```
psort.exe -o null --analysis tagging
--tagging-file tag_windows.txt -w c-
drive.plaso
```

Use the tags that were populated in the step above to filter

```
psort.exe -o l2tcsv -w
```

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

https://digital-forensics.sans.org/media/Plaso-Cheat-Sheet.pdf

Techno Security & Digital Forensics Conference

Plaso Filter Presentation GitHub Link

- Repository is work in progress – will update as new info is discovered
- Link is https://github.com/mark-hallman/plaso_filters

A Peek at KAPE

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Techno Security &
Digital Forensics
Conference

Questions

Thanks for attending – Safe Travels home

https://github.com/mark-hallman/plaso_filters

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Techno Security & Digital Forensics Conference