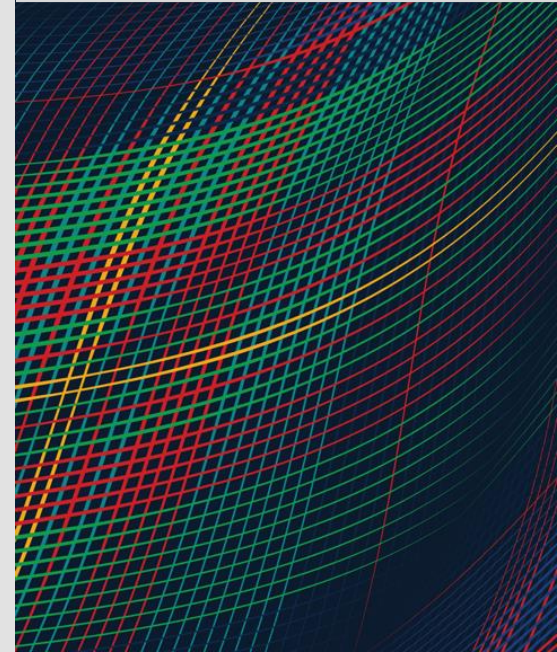


Creating Timelines with Plaso



Notices

Copyright 2024 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702 -15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM24-0301

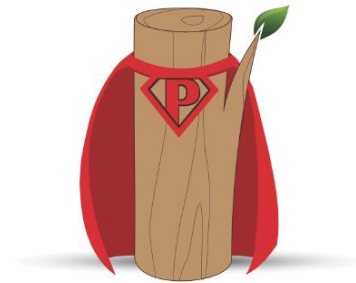
Introduction

This module explains and demonstrates how to

- **Use the Plaso family of tools to create timelines**
- **Some tips**

This module does not replace the Plaso documentation site which is here:

<https://plaso.readthedocs.io/en/latest/>



Creating Timelines with Plaso

Timelines

Timelines -1

An ordered by time list of items, typically events
Focus on a specific time and slowly expand the window
Aggregate as much data as possible

- Entries in log files
- Modified, accessed, and created times on files
- Browser history
- Etc., etc., etc.

Combined with physical timestamps

- Timestamps from video, audio, paper, witnesses, etc.

Timelines -2

Key concepts

1. CLOCKS MUST BE SYNCHRONIZED!

- If not synchronized, hard to “sort” data based on time
- Manual translation may be required
- What does an arbitrary time mean?
 - What is the month, day, year, hour, minute and time zone in:
03/01/02 12:00 p.m. EST

2. Data in question is just bits stored somewhere (e.g. disk)

- (Malicious) user with appropriate permissions can alter
- Try to find as many sources of “events” as possible to improve credibility
- Corroboration with physical events: video time codes, eyewitnesses, logs/journals

Timelines -3

Most systems can log many things

- System logs
- Application logs (e.g., a browser history file)
- Network/firewall logs
- File MAC times

Challenge is

- Extracting all this information
- Normalizing it
- "Publishing" it
- Efficiently



Creating Timelines with Plaso

Plaso

**Carnegie
Mellon
University**
Software
Engineering
Institute

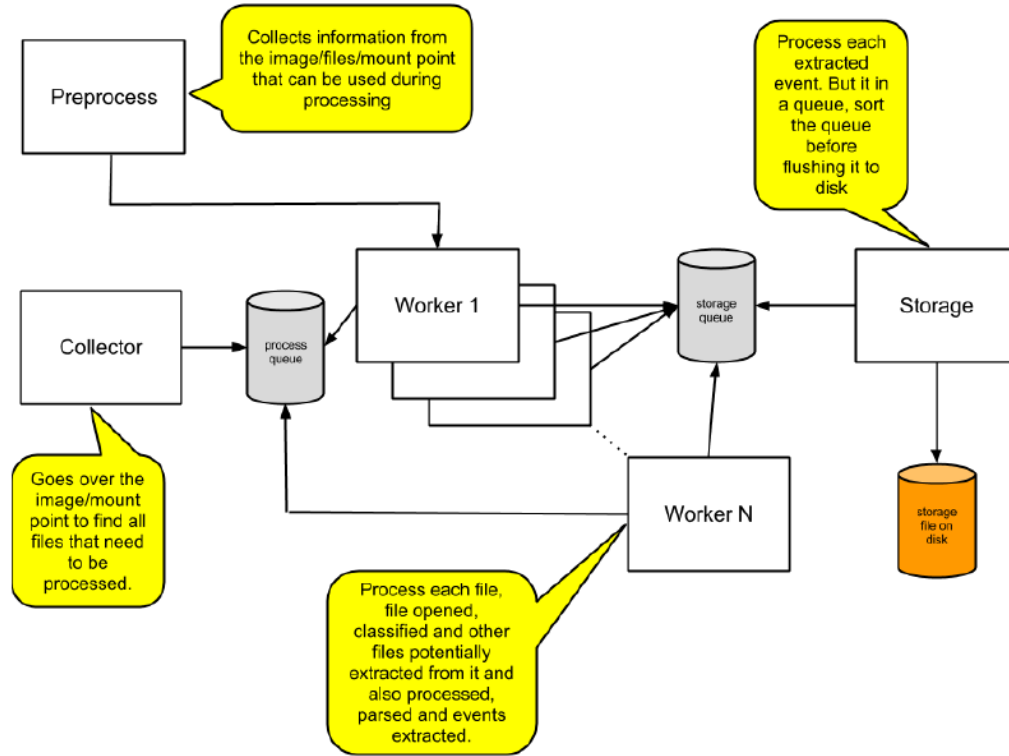
Plaso -1

Enter Plaso (Plaso Langar Að Safna Öllu)
Timeline framework

- Extensible (plugins and parsers)
- Windows, Linux, and MacOS
- Parse arbitrary timestamped data
- Front end that creates data repository (`psteal.py` and `log2timeline.py`)
- Operate on Plaso data repository metadata (`pinfo.py`)
- Postprocess data repository (`psort.py` and `image_export.py`)
- Written in Python 3
- Previous version in Perl (no longer supported)

Plaso -2

Overview



Plaso -3

Large datasets benefit from

- many CPUs/cores (16 cores)
- much memory

Plaso storage files (aka data repository files)

- SQLite 3 format
- Created by front end programs (`psteal.py` and `log2timeline.py`)
- Naming convention:
 - ISO 8601 timestamp-*ImageFileName*.plaso

Creating Timelines with Plaso

Plaso Tools

**Carnegie
Mellon
University**
Software
Engineering
Institute

Plaso Tools – psteal.py -1

From the help output of `psteal.py`:

psteal is a command line tool to extract events from individual files, recursing a directory (e.g. mount point) or storage media image or device. The output events will be stored in a storage file. This tool will then read the output and process the events into a CSV file.

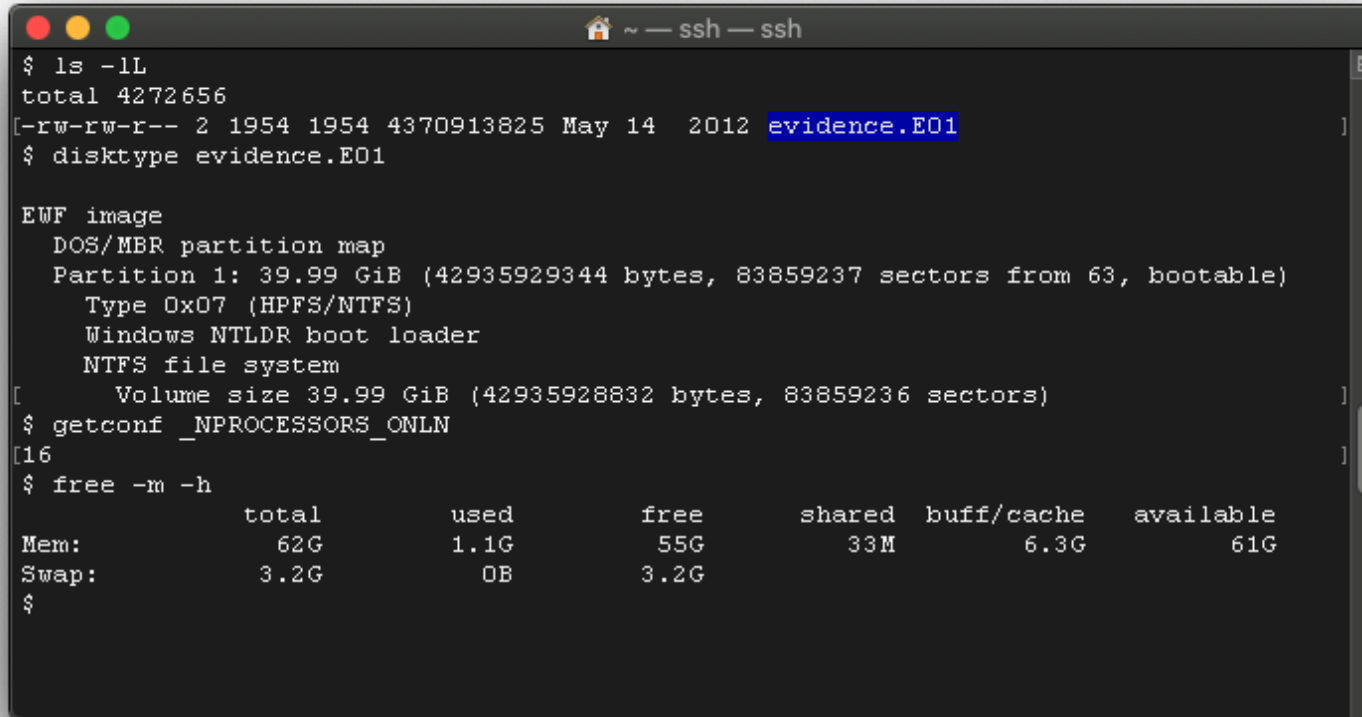
Example:

```
psteal.py --source imynd.dd -w imynd.timeline.txt
```

There are many, many options.

Plaso Tools – psteal.py -2

Let's look at an example



```
~ — ssh — ssh
$ ls -lL
total 4272656
[-rw-rw-r-- 2 1954 1954 4370913825 May 14 2012 evidence.E01
$ disktype evidence.E01

EWF image
DOS/MBR partition map
Partition 1: 39.99 GiB (42935929344 bytes, 83859237 sectors from 63, bootable)
Type 0x07 (HPFS/NTFS)
Windows NTLDR boot loader
NTFS file system
[ Volume size 39.99 GiB (42935928832 bytes, 83859236 sectors)
$ getconf _NPROCESSORS_ONLN
[16
$ free -m -h

```

	total	used	free	shared	buff/cache	available
Mem:	62G	1.1G	55G	33M	6.3G	61G
Swap:	3.2G	0B	3.2G			

```
$
```

Plaso Tools – psteal.py -3

```
psteal.py --source evidence.E01 -o l2tcsv -w timeline.csv
```

```

Source path      : /home/examiner/plaso/002/evidence.E01
Source type     : storage media image
Processing time  : 00:08:44

Tasks:          Queued  Processing  Merging  Abandoned  Total
                0         0           6         0           36761

Identifier  PID   Status   Memory   Sources   Events   File
Main        30055  merging  616.2 MiB  36761 (0)  1096170 (0)  b5201ae07f0647699950dab44e83b92d
Worker_00   30107  idle     461.2 MiB  1243 (0)   133339 (0)   GZIP:\Documents and Settings\domex1\Local Settings\Application Data\Mozilla\Firefox\Profiles\ngem72bk.default\Cache\C11C3B29d01
Worker_01   30109  idle     470.6 MiB  1534 (0)   166966 (0)   GZIP:\Documents and Settings\domex1\Local Settings\Temporary Internet Files\Content.IE5\W1QV09Y3\AIM_UAC_v2[1].adp
Worker_02   30111  idle     462.2 MiB  2087 (0)   135832 (0)   GZIP:\Documents and Settings\domex1\Local Settings\Application Data\Mozilla\Firefox\Profiles\ngem72bk.default\Cache\DC1EE471d01
Worker_03   30113  idle     441.4 MiB  1294 (0)   60280 (0)    GZIP:\Documents and Settings\domex2\Local Settings\Application Data\Mozilla\Firefox\Profiles\n2utfxqg.default\Cache\S845CE1Fd01
Worker_04   30115  idle     450.3 MiB  6409 (0)   126319 (0)   GZIP:\Documents and Settings\domex1\Local Settings\Application Data\Mozilla\Firefox\Profiles\ngem72bk.default\Cache\FBE7C7CDd01
Worker_05   30118  idle     431.2 MiB  4851 (0)   53118 (0)    GZIP:\Documents and Settings\domex1\Local Settings\Temporary Internet Files\Content.IE5\8P63W5MB\CreateAccount[1].comk2Fmail%2Fe-11-10Feb6499hh19b1894
597e2bdcf5800-4b084fd0dfd3884c9de751cc9047ae00e93da11a96type=2
Worker_06   30120  idle     489.7 MiB  1305 (0)   60800 (0)   GZIP:\Documents and Settings\domex1\Local Settings\Application Data\Mozilla\Firefox\Profiles\ngem72bk.default\Cache\6547027Cd01
Worker_07   30122  idle     418.4 MiB  1693 (0)   65786 (0)   GZIP:\Documents and Settings\domex1\Local Settings\Application Data\Mozilla\Firefox\Profiles\ngem72bk.default\Cache\636A5B76d01
Worker_08   30124  idle     485.3 MiB  4229 (0)   137646 (0)   NTFS:\WINDOWS\SoftwareDistribution\Download\cf8ec783e88561dddb53e1834cd05c3e\asms\60\msrt\windows\common\controls\conct132.d11
Worker_09   30126  idle     433.6 MiB  2700 (0)   57166 (0)   GZIP:\Documents and Settings\domex1\Local Settings\Application Data\Mozilla\Firefox\Profiles\ngem72bk.default\Cache\715E7B08d01
Worker_10   30132  idle     487.5 MiB  1142 (0)   104513 (0)  GZIP:\Documents and Settings\domex1\Local Settings\Application Data\Mozilla\Firefox\Profiles\ngem72bk.default\Cache\6499E1C3d01
Worker_11   30138  idle     456.1 MiB  1288 (0)   62441 (0)   GZIP:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\SS1VD02F\loc=100;crp=1;rndc=122454259;noperf=1;target=
blank;grp=542591739;misc=542591739[1]
Worker_12   30142  idle     449.0 MiB  3047 (0)   80117 (0)   GZIP:\Documents and Settings\domex2\Local Settings\Application Data\Mozilla\Firefox\Profiles\n2utfxqg.default\Cache\CBE9850Bd01
Worker_13   30148  idle     439.7 MiB  2781 (0)   86864 (0)   GZIP:\Documents and Settings\domex1\Local Settings\Application Data\Mozilla\Firefox\Profiles\ngem72bk.default\Cache\B917ASF2d01
Worker_14   30150  idle     464.3 MiB  1157 (0)   207338 (0)  GZIP:\Documents and Settings\domex1\Local Settings\Temporary Internet Files\Content.IE5\SS1VD02F\AIM_UAC_v2[1].adp

```

Plaso Tools – psteal.py -4

```

plaso - psteal version 20200717

Storage file      : 20200828T140305-evidence.E01.plaso
Processing time   : 00:19:56

Events:          Filtered      In time slice  Duplicates  MACB grouped  Total
                 0              0              1030         1523966       1538525

Identifier       PID      Status      Memory      Events      Tags      Reports
Main            30055  exporting  779.1 MiB   1538525 (0) 0 (0)     0 (0)

Processing completed.

***** Counter *****
-----
Storage file is 20200828T140305-evidence.E01.plaso
$ █

```

```

[$ wc -l timeline.csv
1484936 timeline.csv
$

```

Plaso Tools – psteal.py -5

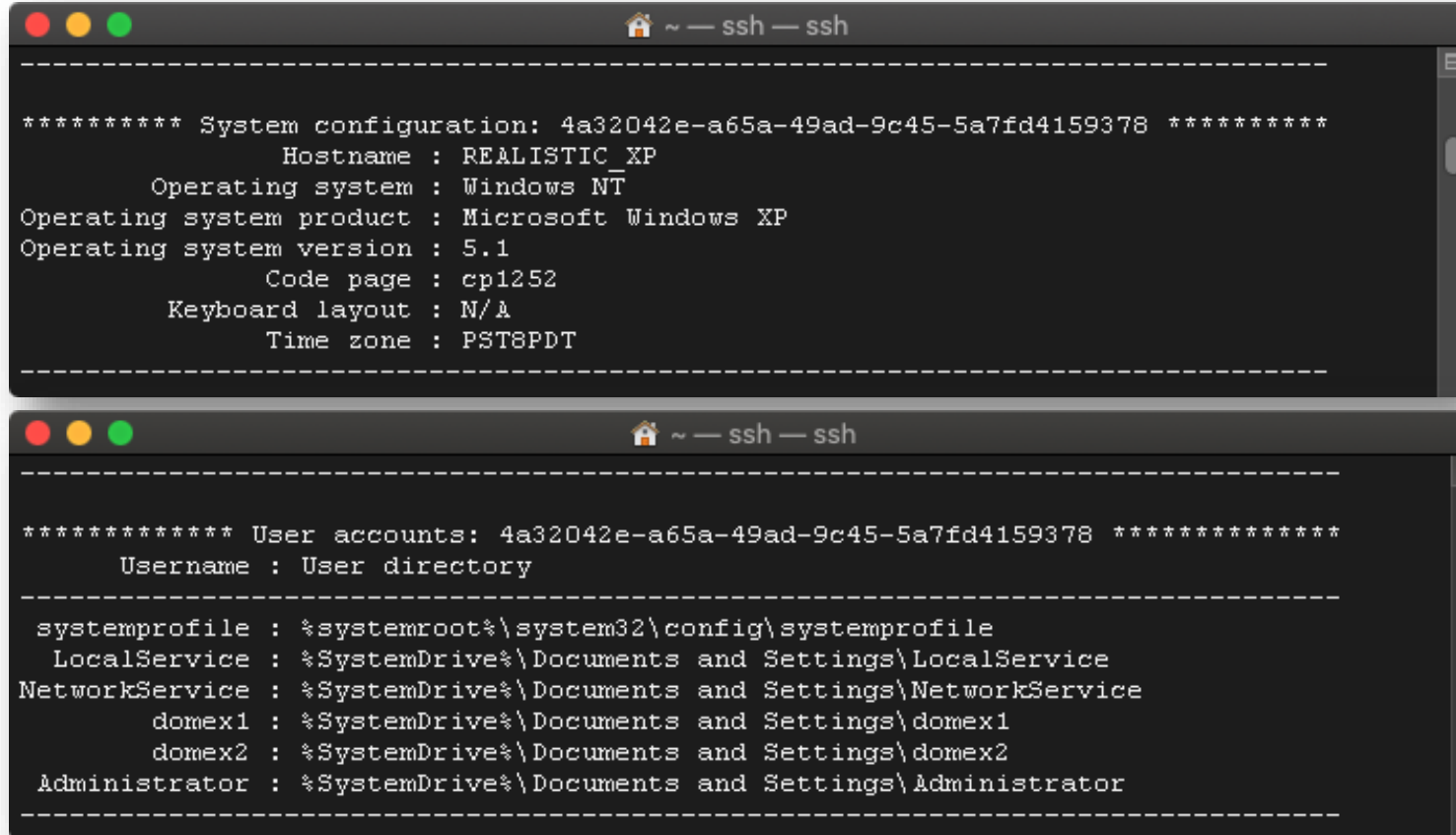


This timeline has too many rows for Excel and other spreadsheet programs to view. "Interesting" parts need to be extracted and those looked at.

We'll use **pinfo.py** – the Plaso Inventory Program – to slice and dice this information.

Plaso Tools – psteal.py -6

```
pinfo.py -v 20200828T140305-evidence.E01.plaso
```



```
-----  
***** System configuration: 4a32042e-a65a-49ad-9c45-5a7fd4159378 *****  
      Hostname : REALISTIC_XP  
      Operating system : Windows NT  
Operating system product : Microsoft Windows XP  
Operating system version : 5.1  
      Code page : cp1252  
      Keyboard layout : N/A  
      Time zone : PST8PDT  
-----  
  
-----  
***** User accounts: 4a32042e-a65a-49ad-9c45-5a7fd4159378 *****  
      Username : User directory  
-----  
systemprofile : %systemroot%\system32\config\systemprofile  
LocalService : %SystemDrive%\Documents and Settings\LocalService  
NetworkService : %SystemDrive%\Documents and Settings\NetworkService  
      domex1 : %SystemDrive%\Documents and Settings\domex1  
      domex2 : %SystemDrive%\Documents and Settings\domex2  
Administrator : %SystemDrive%\Documents and Settings\Administrator  
-----
```

Plaso Tools – psteal.py -7

What filters were applied and how much information did they find?

```
***** Events generated per parser *****
Parser (plugin) name : Number of events
-----
      appcompatcache : 5760
      bagmrU : 285
explorer_mountpoints2 : 493
explorer_programscache : 80
      filestat : 146926
      firefox_cache : 3300
      firefox_downloads : 2
      firefox_history : 585
      lnk : 933
      mrulist_string : 163
      mrulistex_string : 62
mrulistex_string_and_shell_item : 88
      msie_zone : 1548
      msiecf : 6844
      olecf_default : 384
      oxml : 125
      pe : 78604
      prefetch : 66
recycle_bin_info2 : 5
      rplog : 16
      shell_items : 5043
      userassist : 1021
windows_boot_execute : 72
      windows_run : 161
windows_sam_users : 191
windows_services : 9239
windows_shutdown : 30
windows_timezone : 36
windows_typed_urls : 41
windows_usb_devices : 216
windows_version : 38
      winevt : 1076
      winjob : 2
      winlogon : 754
      winreg_default : 1274336
      Total : 1538525
-----
```

Plaso Tools – psteal.py -8

Look at the recycle bin information

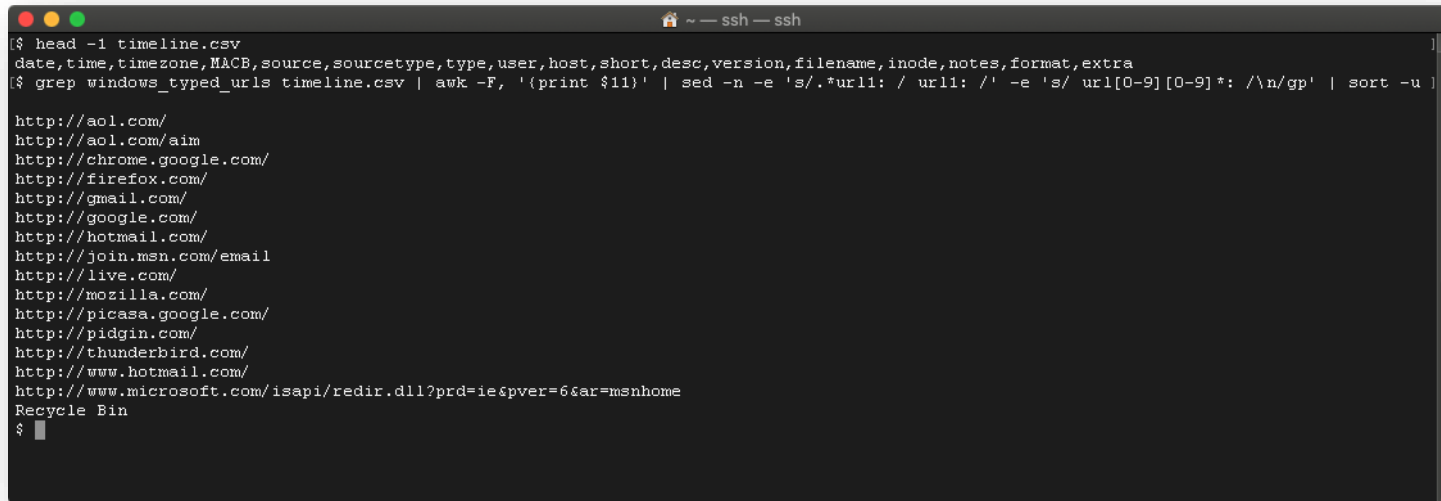
```
(head -1 timeline.csv ; grep -i recycle_bin_info2 timeline.csv) > RecycleBin.csv
```

	A	B	C	D	E	F	G	H	I
1	date	time	timezone	MACB	source	sourcetype	type	user	host
2	10/28/08	16:58:34	UTC	M...	RECBIN	Recycle Bin	Content Deletion Time	-	REALISTIC_XFI
3	10/30/08	3:39:29	UTC	M...	RECBIN	Recycle Bin	Content Deletion Time	-	REALISTIC_XFI
4	10/30/08	3:39:29	UTC	M...	RECBIN	Recycle Bin	Content Deletion Time	-	REALISTIC_XFI
5	10/30/08	3:39:32	UTC	M...	RECBIN	Recycle Bin	Content Deletion Time	-	REALISTIC_XFI
6	10/30/08	3:39:38	UTC	M...	RECBIN	Recycle Bin	Content Deletion Time	-	REALISTIC_XFI

J	K	L	M	N	O	P	Q
short	desc	version	filename	inode	notes	format	extra
F Deleted file: (DC1 -> C:\Documents and Settings\Administrator\Desktop\Office2007Enterprise (from drive: C)		2	-	29296	-	recycle_bin_i	drive_number: 2; file_size: 585256960
F Deleted file: (DC1 -> C:\Documents and Settings\domex1\My Documents\This is a spreadsheet deleted and emptied by domex user 1.xlsx (from drive: C)		2	-	28685	-	recycle_bin_i	drive_number: 2; file_size: 12288
F Deleted file: (DC2 -> C:\Documents and Settings\domex1\My Documents\This is a word document deleted and emptied by domex user 1.docx (from drive: C)		2	-	28685	-	recycle_bin_i	drive_number: 2; file_size: 12288
F Deleted file: (DC3 -> C:\Documents and Settings\domex1\My Documents\This is a word document deleted by domex user 1.docx (from drive: C)		2	-	28685	-	recycle_bin_i	drive_number: 2; file_size: 12288
F Deleted file: (DC4 -> C:\Documents and Settings\domex1\My Documents\This is a spreadsheet deleted by domex user 1.xlsx (from drive: C)		2	-	28685	-	recycle_bin_i	drive_number: 2; file_size: 12288

Plaso Tools – psteal.py -9

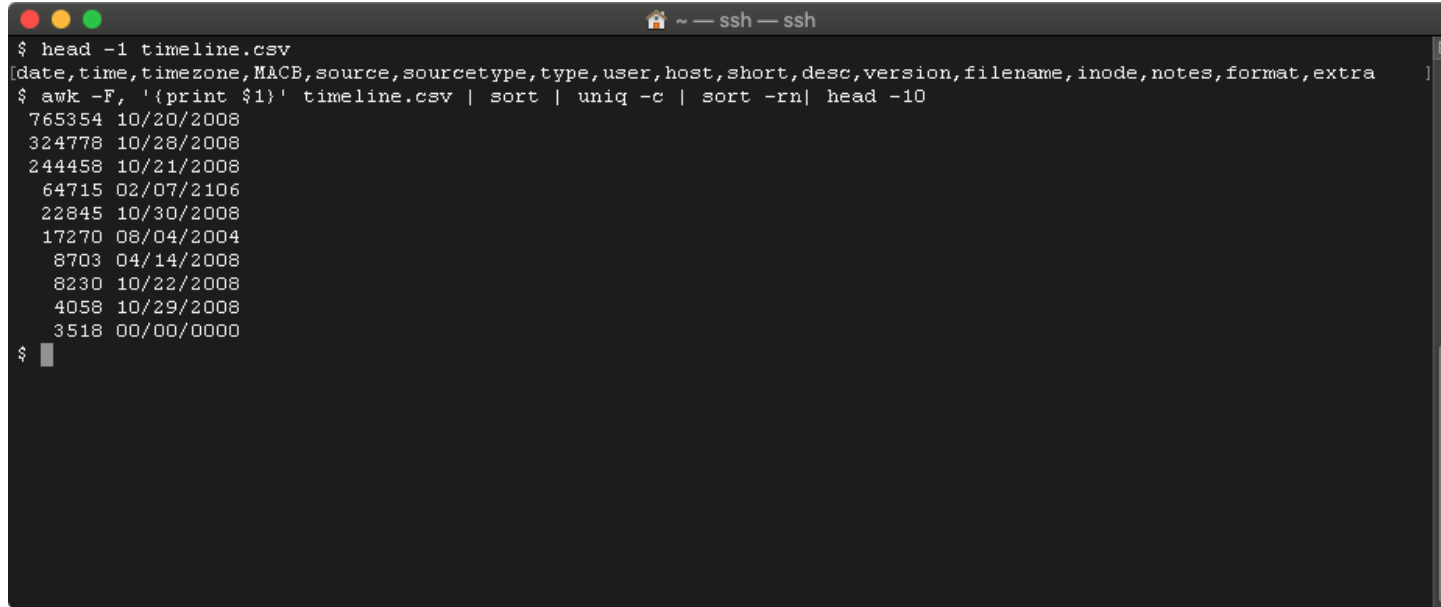
For the URLs that were typed into a browser, list all of those URLs



```
~ — ssh — ssh
[$ head -1 timeline.csv
date,time,timezone,MACB,source,sourcetype,type,user,host,short,desc,version,filename,inode,notes,format,extra
[$ grep windows_typed_urls timeline.csv | awk -F, '{print $11}' | sed -n -e 's/.*url1: / url1: /' -e 's/ url[0-9][0-9]*: /\n/gp' | sort -u ]
http://aol.com/
http://aol.com/aim
http://chrome.google.com/
http://firefox.com/
http://gmail.com/
http://google.com/
http://hotmail.com/
http://join.msn.com/email
http://live.com/
http://mozilla.com/
http://picasa.google.com/
http://pidgin.com/
http://thunderbird.com/
http://www.hotmail.com/
http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
Recycle Bin
$
```

Plaso Tools – psteal.py-10

When did most events happen?



```
~ — ssh — ssh
$ head -1 timeline.csv
[date,time,timezone,MACB,source,sourcetype,type,user,host,short,desc,version,filename,inode,notes,format,extra]
$ awk -F, '{print $1}' timeline.csv | sort | uniq -c | sort -rn | head -10
765354 10/20/2008
324778 10/28/2008
244458 10/21/2008
64715 02/07/2106
22845 10/30/2008
17270 08/04/2004
8703 04/14/2008
8230 10/22/2008
4058 10/29/2008
3518 00/00/0000
$
```

2106? Interesting

Plaso Tools – pinfo.py



pinfo.py can:

- Show information about a Plaso storage file
- This is metadata that describes what **psteal.py** or **log2timeline.py** found in the image file

Plaso Tools – log2timeline.py

Creating storage

- Details here: <https://plaso.readthedocs.io/en/latest/sources/user/Using-log2timeline.html>
- Prototype

```
log2timeline.py [OPTIONS] Output-File Input-File
```
- With **psteal.py**, you get a bunch of default options (the kitchen sink)
- With **log2timeline.py**, you can be more selective about processing a source file
- Many, many, many options

Plaso Tools – psort.py

psort.py can:

- Select events based on dates and a slice around that date
- Specify filters to reduce dataset size
- Specify alternative output formats
- Specify arbitrary filters: <https://plaso.readthedocs.io/en/latest/sources/user/Event-filters.html>
- Use `psort.py -h` to see the options and their format

Plaso Tools – `image_export.py`

`image_export.py` can:

- Export all files with a suffix (.pdf)
- Export all files with a name
- Export all files matching a signature
- Export files modified, accessed, or created between a date range
- Use `image_export.py -h` to see the options and their format

Creating Timelines with Plaso

Summary & If You Want to Know More

Summary



- Timeline important for telling a story
- **CLOCKS MUST BE SYNCHRONIZED**
- Plaso is one way to extract events from an image (e.g. dd, E01)
- Storage files – metadata about events in image
- Resource (CPUs and memory) intensive

If You Want to Know More

Topic	Reference
Plaso	https://plaso.readthedocs.io/en/latest/index.html
ISO 8601	https://www.iso.org/standard/70907.html
Sqlite 3	https://sqlite.org/index.html
Using log2timeline.py	https://plaso.readthedocs.io/en/latest/sources/user/Using-log2timeline.html
Plaso Filters	https://plaso.readthedocs.io/en/latest/sources/user/Event-filters.html
Plaso from DFIR – references an older version of Plaso	https://digital-forensics.sans.org/summit-archives/DFIR_Summit/Plaso-Reinventing-the-Super-Timeline-Kristinn-Gudjonsson.pdf

Questions

