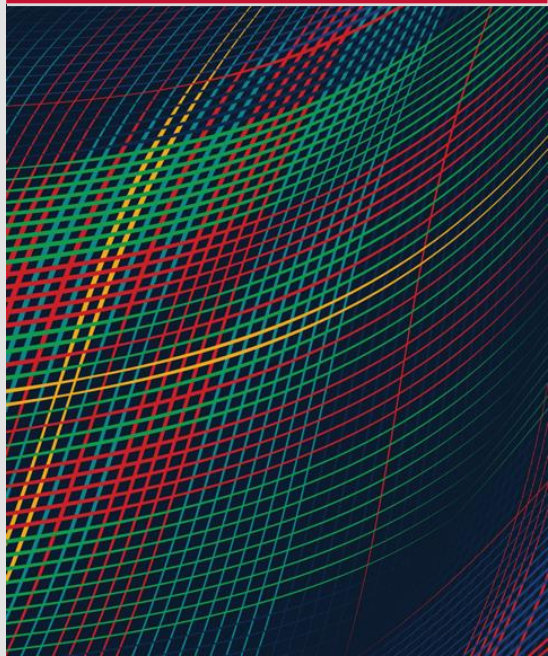
Creating Timelines with Plaso

Carnegie Mellon University
Software Engineering Institute



Notices

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.

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

Carnegie Mellon University
Software Engineering Institute

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

Carnegie Mellon University Software Engineering Institute

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

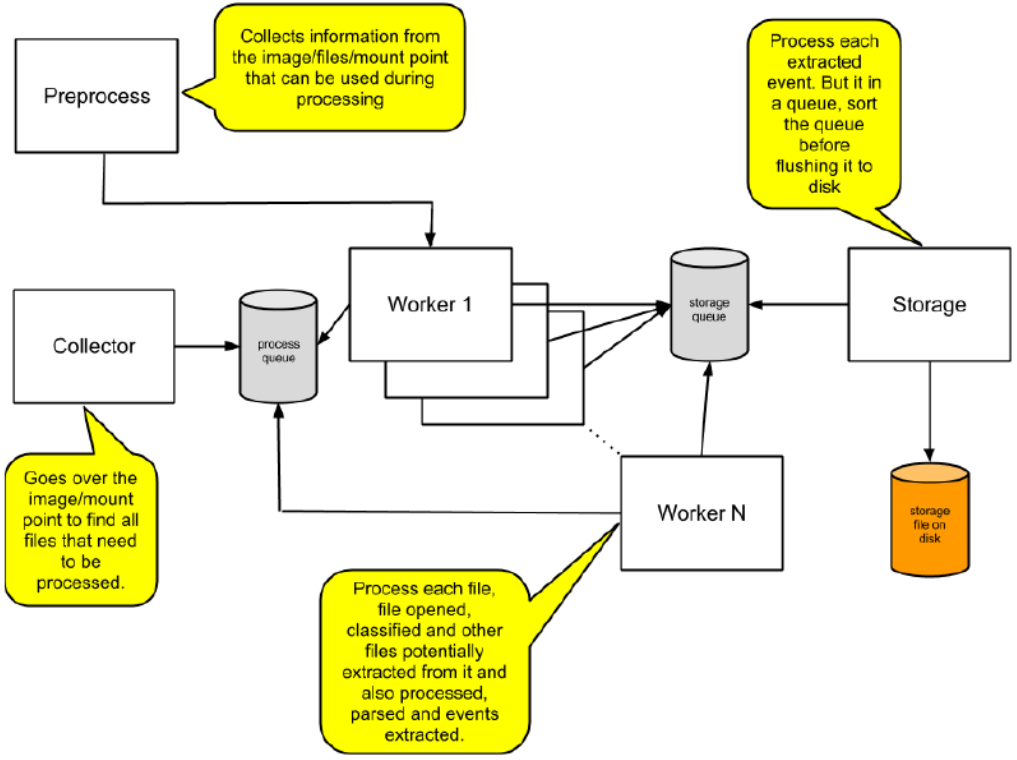
Plaso -1

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.*

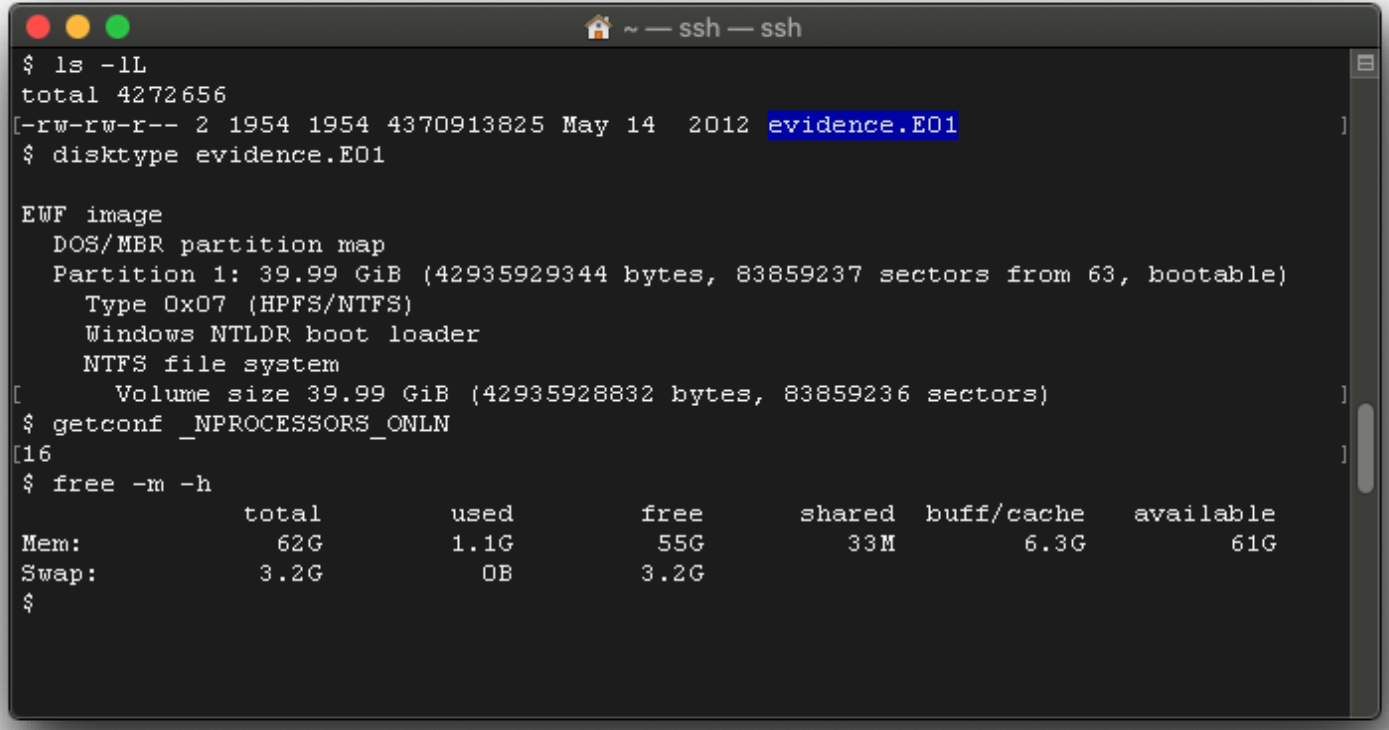
Example:

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

There are many, many options.

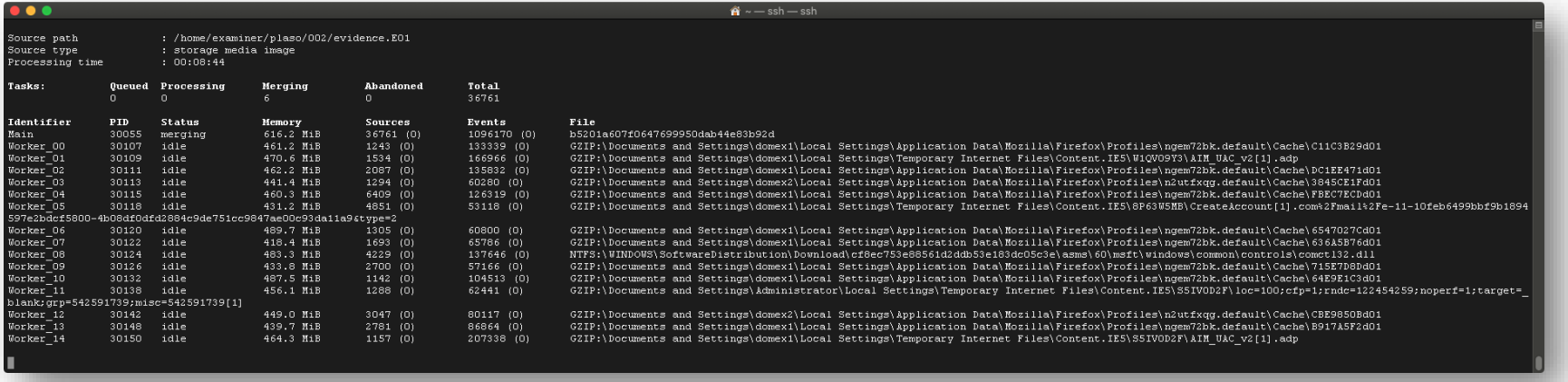
Plaso Tools – psteal.py -2

Let's look at an example

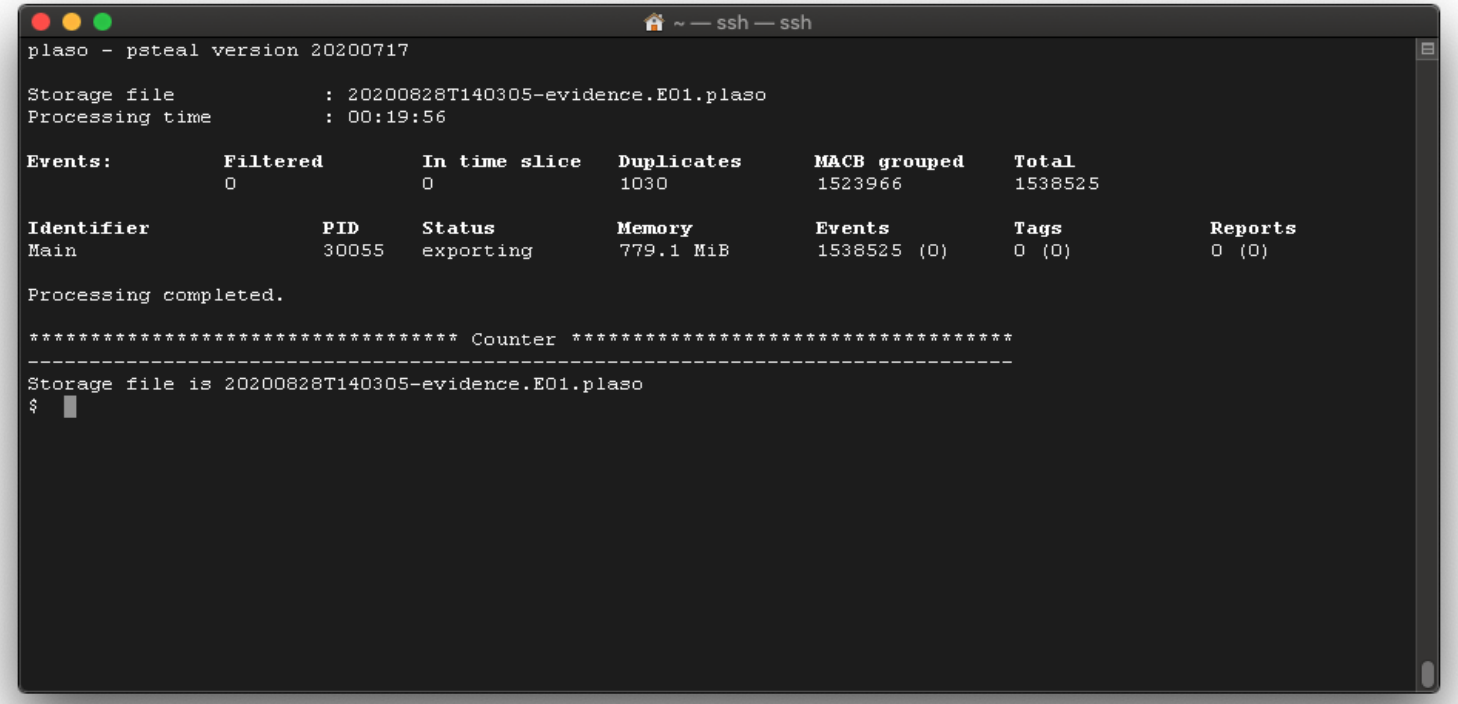


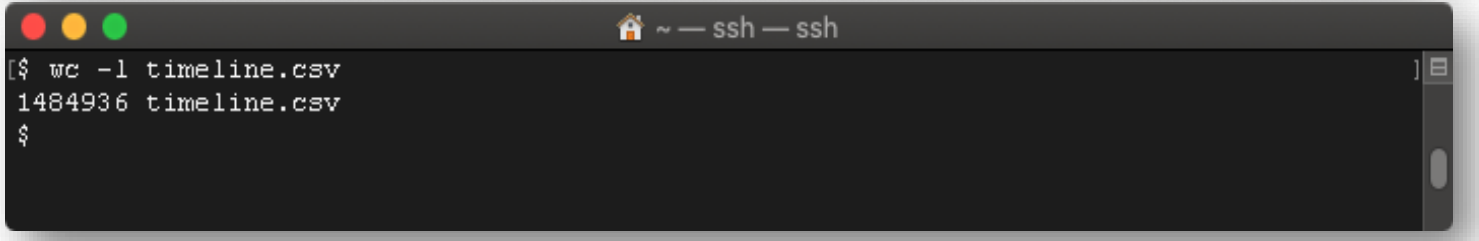
Plaso Tools – psteal.py -3

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



Plaso Tools – psteal.py -4





Plaso Tools – psteal.py -5

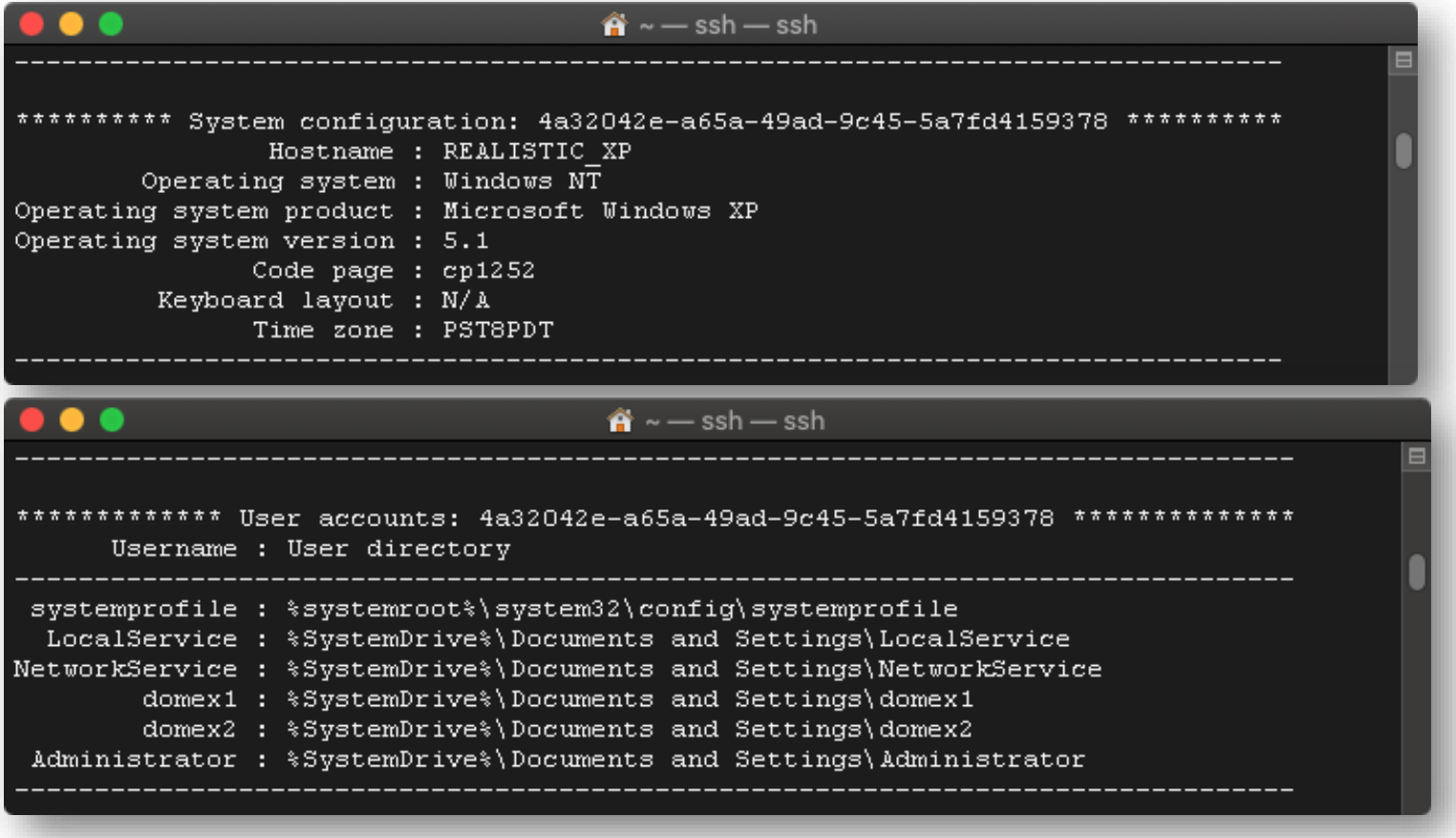
This timeline has too many rows for Excel and other spreadsheet programs to view.

”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



Plaso Tools – psteal.py -7

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

~ — ssh — ssh

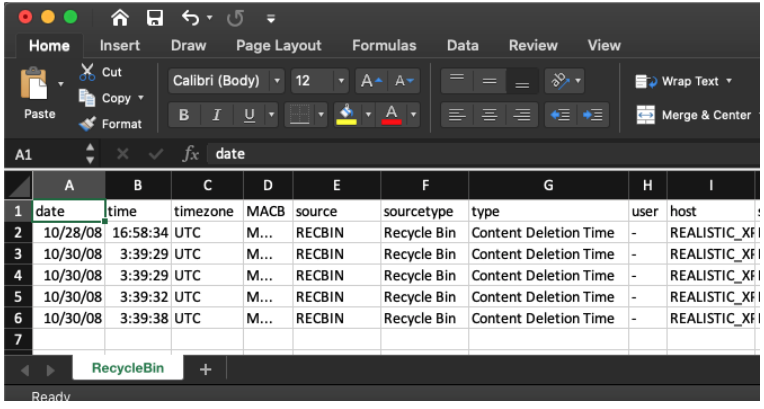
```
************************* Events generated per parser ***************************
           Parser (plugin) name : Number of events
-------------------------------------------------------------------------------
                 appcompatcache : 5760
                        bagmru : 285
          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

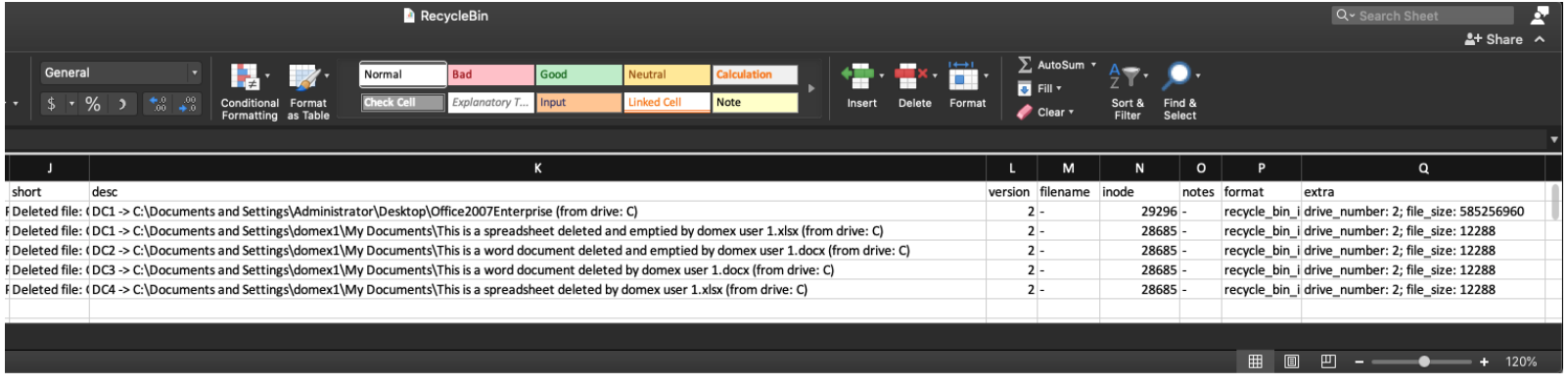
Carnegie Mellon University Software Engineering Institute

Look at the recycle bin information

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



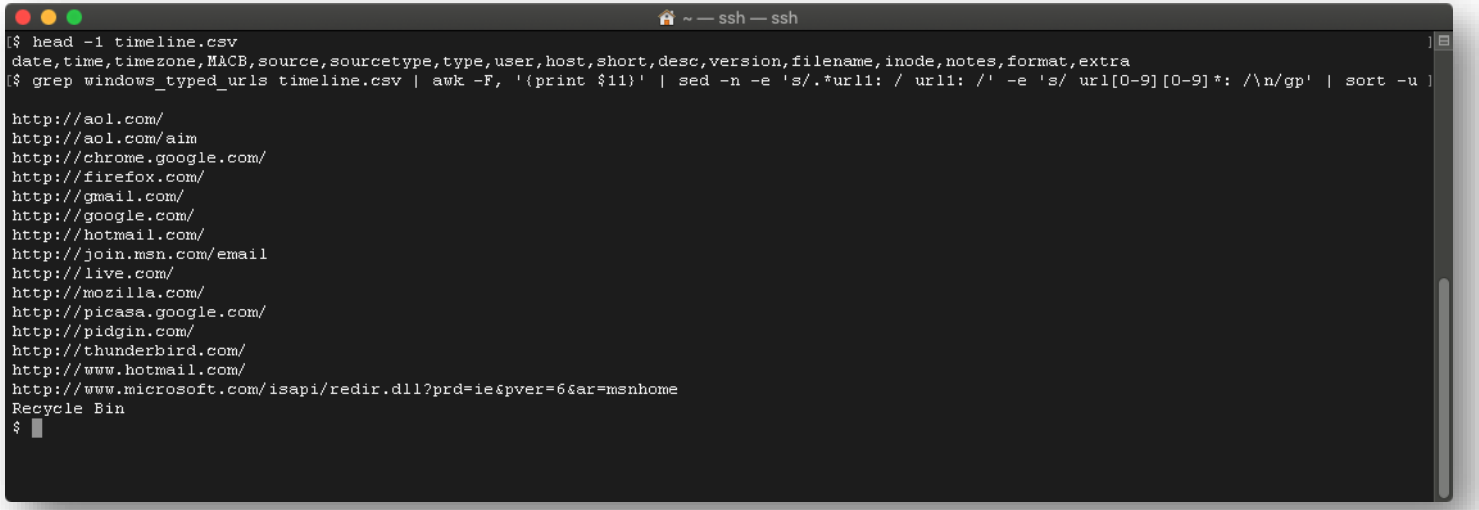
	A	B	C	D	E	F	G	H	I
1	date	time	timezone	MACB	source	sourcetype	type	user	host
2	10/28/08	16:58:34	UTC	M...	RECBIN	Recycle Bin	Content Deletion Time	-	REALISTIC_XF
3	10/30/08	3:39:29	UTC	M...	RECBIN	Recycle Bin	Content Deletion Time	-	REALISTIC_XF
4	10/30/08	3:39:29	UTC	M...	RECBIN	Recycle Bin	Content Deletion Time	-	REALISTIC_XF
5	10/30/08	3:39:32	UTC	M...	RECBIN	Recycle Bin	Content Deletion Time	-	REALISTIC_XF
6	10/30/08	3:39:38	UTC	M...	RECBIN	Recycle Bin	Content Deletion Time	-	REALISTIC_XF
7									



	J	K	L	M	N	O	P	Q
	short	desc	version	filename	inode	notes	format	extra
	Deleted file: (	DC1 -> C:\Documents and Settings\Administrator\Desktop\Office2007Enterprise (from drive: C)	2	-	29296	-	recycle_bin_i	drive_number: 2; file_size: 585256960
	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
	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
	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
	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

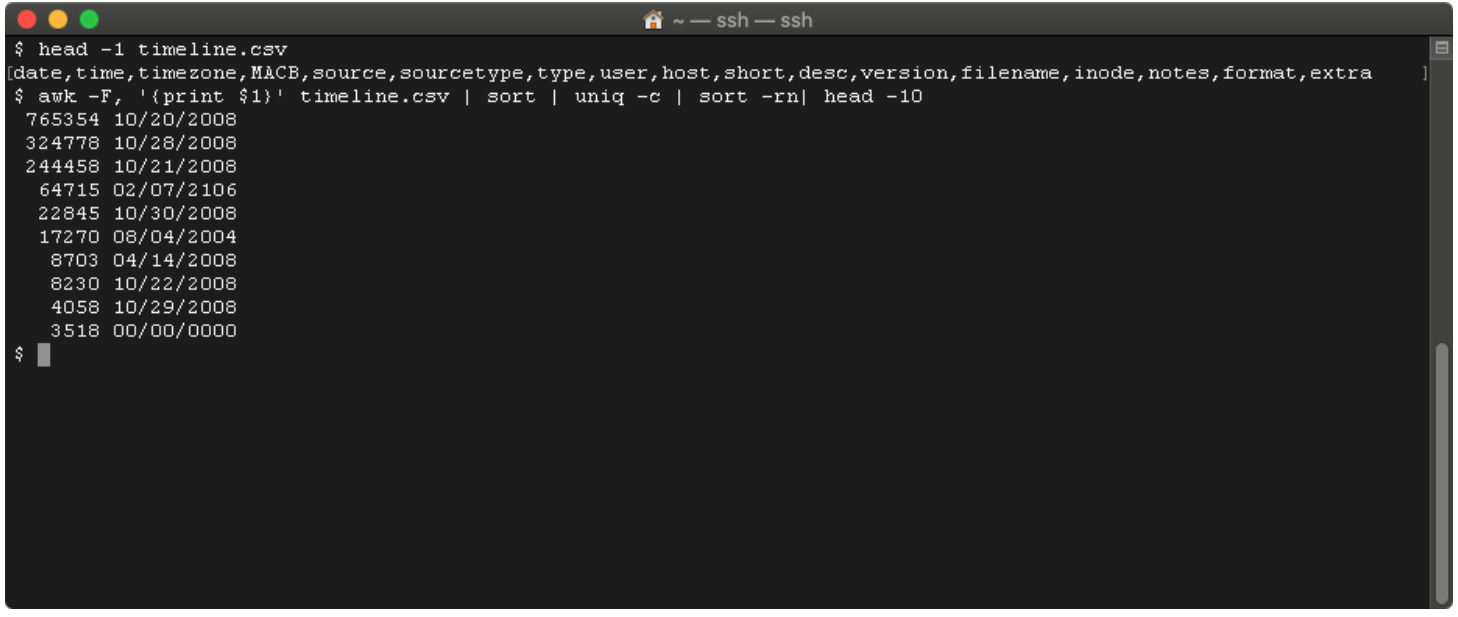
Plaso Tools – psteal.py -9

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



Plaso Tools – psteal.py-10

When did most events happen?



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

Carnegie Mellon University
Software Engineering Institute

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