Hello!

Je travaille @ Google dans l'équipe Incident Response

....

Et toujours un peu un padawan

...

Mais je vais quand même vous parler Digital Forensics!

plaso & timesketch

Forensics made easy: New generation timelining

Hands up !

Qui a déjà entendu parler de Plaso/Log2timeline ?

... et a réussi à s'en servir?

... sans passer par une VM toute prête?

... ne ferait pas confiance à un tool sans dongle?

Plaso

Plaso (Plaso Langar Að Safna Öllu)

Plaso (Python) regroupe plusieurs outils.

1. Parser tout ce qui a des timestamp et générer des Events normalisés (`log2timeline.py`)
2. Trier/filtrer ces Events (`psort.py`)
3. Forensiquer (`vous.rb`)

Plaso est simple à utiliser

```
$ log2timeline.py patient_zero.plaso patient_zero.dd

          … aller prendre un café…

$ psort.py patient_zero.plaso | <ici le 2eme meilleur outil DF>
```

Plaso est simple à utiliser

```
$ log2timeline.py patient_zero.plaso patient_zero.dd

          … aller prendre un café…

$ psort.py patient_zero.plaso | egrep -i \

                              "(temp.*\.exe|(invoice.*\.(zip|js))"
```

Plus qu'à écrire le rapport !

Dedans log2timeline.py

1) Parser l'input (DfVFS)

```
renzo@trusty:~$ log2timeline.py /tmp/plaso /raid/incoming/img
Checking availability and versions of plaso dependencies.
[OK]

The following partitions were found:
Identifier      Offset (in bytes)       Size (in bytes)
p1              1536 (0x00000600)       1.0GiB / 1.1GB (1073741824 B)
p2              1074790912 (0x40100200) 512.0MiB / 536.9MB (536870400 B)
p3              1611661824 (0x60100200) 10.0MiB / 10.5MB (10485760 B)
p4              1622147584 (0x60b00200) 400.0MiB / 419.4MB (419429888 B)

Please specify the identifier of the partition that should be processed.
All partitions can be defined as: "all". Note that you can abort with Ctrl^C.
```

Storage media types

EWF, QCOW, Raw, VDI or VHD, VMDK, etc.

Volume systems

APM, GPT, MBR, BitLocker, Windows VSS

(Bientôt LVM, LUKS)

File systems

EXT, FAT HFS, HFS+, HFSX, NTFS, UFS, etc.

Dedans log2timeline

1) Parser l’input (DfVFS)
2) Preprocessors

Détermine par exemple :

- Timezone
- Windows Codepage, OS version, users
- Linux hostname, users

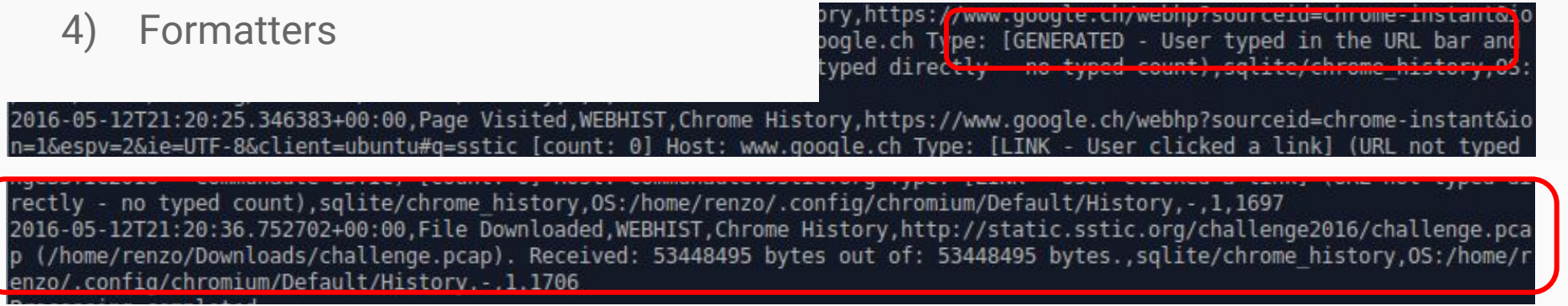
Dedans log2timeline

1) Parser l'input (DfVFS)
2) Preprocessors
3) Parsers / Extraction

- Android app usage, logs appels, SMS
- FF&IE&Chrome: historique & cache & prefs
- Mac: system & keychain & wifi logs, .plist
- ESEdb, PE
- IIS logs, SCCM client logs, EVT/X
  $MFT, $UsnJrnl:$J, Prefetch
- Registry, OLE files
- SElinux audit, UTMP, syslog
- PCAPs, AVs Logs
- etc.

Dedans log2timeline

1) Parser l'input, générer des pathspecs (DfVFS)
2) Preprocessors
3) Parsers / Extraction
4) Formatters



Dedans log2timeline: greffons d'analyse

Plaso est aussi **cyber-threat-intelligence** aware

- VirusTotal
- Viper

Extensible avec des tags:

```
$ psort.py -o null --analysis tagging --tagging-file tag_windows.txt test.plaso
```

```
application_execution
  data_type is 'windows:prefetch'
  data_type is 'windows:lnk:link' and filename contains 'Recent' and (local_path contains '.exe' or network_path contains '.
  data_type is 'windows:registry:key_value' AND (plugin contains 'userassist' or plugin contains 'mru') AND regvalue.__all__
  data_type is 'windows:evtx:record' and strings contains 'user mode service' and strings contains 'demand start'
  data_type is 'fs:stat' and filename contains 'Windows/Tasks/At'
  data_type is 'windows:tasks:job'
  data_type is 'windows:evt:record' and source_name is 'Security' and event_identifier is 592
  data_type is 'windows:evtx:record' and source_name is 'Microsoft-Windows-Security-Auditing' and event_identifier is 4688
  data_type is 'windows:registry:appcompatcache'

application_install
  data_type is 'windows:evtx:record' and source_name is 'Microsoft-Windows-Application-Experience' and event_identifier is 9
  data_type is 'windows:evtx:record' and source_name is 'Microsoft-Windows-Application-Experience' and event_identifier is 9

application_update
  data_type is 'windows:evtx:record' and source_name is 'Microsoft-Windows-Application-Experience' and event_identifier is 9

application_removal
  data_type is 'windows:evtx:record' and source_name is 'Microsoft-Windows-Application-Experience' and event_identifier is 9
  data_type is 'windows:evtx:record' and source_name is 'Microsoft-Windows-Application-Experience' and event_identifier is 9

document_open
  data_type is 'windows:registry:key_value' AND plugin contains 'mru' AND regvalue.__all__ not contains '.exe' AND timestamp

login_failed
  data_type is 'windows:evtx:record' and source_name is 'Microsoft-Windows-Security-Auditing' and event_identifier is 4625
```

Dedans log2timeline

1) Parser l'input (DfVFS)
2) Preprocessors
3) Parsers / Extraction
4) Formatters
5) Storage

- CSV
- XLS
- JSON
- raw Python code
- ElasticSearch
- timesketch

Plaso est super simple à installer

Do you Ubuntu?

```
apt-add-repository universe
apt-add-repository ppa:gift/stable
apt-get update
apt-get install python-plaso
```

https://packages.debian.org/source/sid/plaso

Plaso est super simple à installer

Pour ceux qui paient pour leur OS

https://github.com/log2timeline/plaso/releases/tag/1.4.0

timesketch

timesketch

Utilise Elasticsearch comme backend, workflow de la réponse à incident

- Annotation des Events
- Plusieurs systèmes sur une timeline
- Collaboratif

Timesketch & Plaso workflow

1. psort.py machine1.plaso -o timesketch
2. Forensication (rechercher & filtrer les Events)

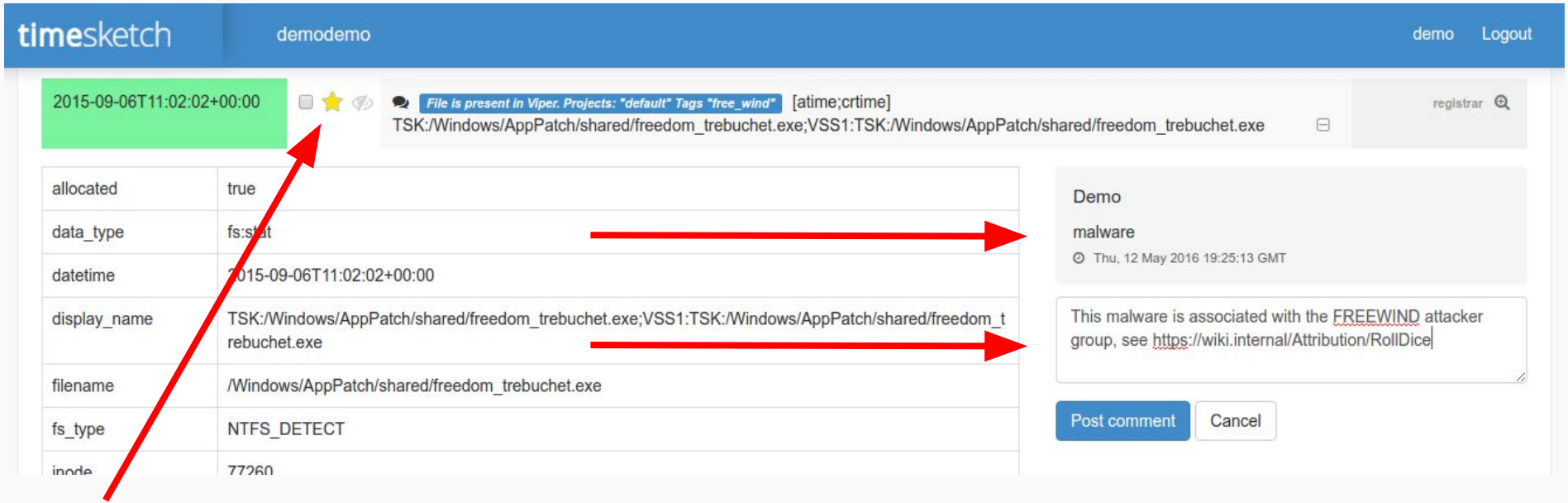
736064 events (0.096s) **Wow, that is a lot of events! I will only show you 500 of them.**

Sort | Export | Toggle all | Add star | Remove star

2015-01-05T09:14:34+00:00	[Content Modification Time] Entry identifier: 616 Container identifier: 1 Cache identifier: 0 URL: http://c.dx.com/banner/201501/left.jpg Access count: 2 Sync count: 0 Filename: left[1].jpg Cached file size: 8451 Response headers: HTTP/1.1 200 OKContent-Type: image/jpegContent-Length: 8451	registrar
2015-01-05T09:14:34+00:00	[Content Modification Time] Entry identifier: 616 Container identifier: 1 Cache identifier: 0 URL: http://c.dx.com/banner/201501/left.jpg Access count: 2 Sync count: 0 Filename: left[1].jpg Cached file size: 8451 Response headers: HTTP/1.1 200 OKContent-Type: image/jpegContent-Length: 8451	registrar

1 days

2015-01-07T03:03:28+00:00	[Content Modification Time] Entry identifier: 1583 Container identifier: 1 Cache identifier: 0 URL: https://images-na.ssl-images-amazon.com/images/I/51vXaZ9QBVL._AC_SY220_.jpg Access count: 1 Sync count: 0 Filename: 51vXaZ9QBVL._AC_SY220_[1].jpg Cached file size: 10139 Response headers: HTTP/1.1 200 OKContent-Type: image/jpegContent-Length: 10139	registrar
2015-01-07T03:03:28+00:00	[Content Modification Time] Entry identifier: 1583 Container identifier: 1 Cache identifier: 0 URL: https://images-na.ssl-images-amazon.com/images/I/51vXaZ9QBVL._AC_SY220_.jpg Access count: 1 Sync count: 0 Filename: 51vXaZ9QBVL._AC_SY220_[1].jpg Cached file size: 10139 Response headers: HTTP/1.1 200 OKContent-Type: image/jpegContent-Length: 10139	registrar
2015-01-07T09:53:00+00:00	[Content Modification Time] Entry identifier: 1077 Container identifier: 1 Cache identifier: 0 URL: http://paintball-arena.ch/paintball/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 Access count: 4	registrar


timesketch
demodemo
demo
Logout
2015-09-06T11:02:02+00:00
File is present in Viper. Projects: "default" Tags "free_wind"
[atime;crtime]
TSK:/Windows/AppPatch/shared/freedom_trebuchet.exe;VSS1:TSK:/Windows/AppPatch/shared/freedom_trebuchet.exe
registrar
allocated
true
data_type
fs:stat
datetime
2015-09-06T11:02:02+00:00
display_name
TSK:/Windows/AppPatch/shared/freedom_trebuchet.exe;VSS1:TSK:/Windows/AppPatch/shared/freedom_trebuchet.exe
filename
/Windows/AppPatch/shared/freedom_trebuchet.exe
fs_type
NTFS_DETECT
inode
77260
Demo
malware
Thu, 12 May 2016 19:25:13 GMT
This malware is associated with the FREEWIND attacker group, see https://wiki.internal/Attribution/RollDice
Post comment
Cancel

Timesketch & Plaso workflow

1. psort.py machine1.plaso -o timesketch
2. Forensication (rechercher & filtrer les Events)
3. Trouver d'autres machines intéressantes, les passer dans l2t.py
4. psort.py machine2.plaso -o timesketch
5. Forensication sur les 2 timelines à la fois

19 events (4 hidden) (0.025s)

2015-08-25T21:01:48+00:00	[crtime] TSK:/Users/dean/.ssh
2015-08-25T21:01:50+00:00	[crtime;ctime;mtime] TSK:/Users/dean/.ssh/id_rsa
2015-08-25T21:01:50+00:00	[crtime;ctime;mtime] TSK:/Users/dean/.ssh/id_rsa.pub

3 days

2015-08-29T12:30:36+00:00	[ctime;mtime] TSK:/Users/dean/.ssh
2015-08-29T12:30:36+00:00	[crtime;ctime;mtime] TSK:/Users/dean/.ssh/known_hosts
2015-08-29T13:21:37+00:00	[atime] TSK:/Users/dean/.ssh
2015-08-29T13:23:05+00:00	[crtime] TSK:/home/dean/.ssh
2015-08-29T13:23:28+00:00	[atime] TSK:/home/dean/.ssh
2015-08-29T13:23:45+00:00	[ctime] TSK:/home/dean/.ssh/authorized_keys

Timesketch & Plaso workflow

1. psort.py machine1.plaso -o timesketch
2. Forensication (search & filter events)
3. Find other interesting systems
4. psort.py machine2.plaso -o timesketch
5. Investigation sur la timeline unifiée
6. Ajout de nouvelles machines, etc.

N. Rapport !

2015-08-24T09:50:09+00:00	[Page Visited] file:///C:/Users/bchang/Documents/Prospective%20Students.xlsx [count: 0] Host: file:///C:/Users/bchang/Documents/Prospective%20Students.xlsx Visit Source: [SOURCE_IE_IMPORTED] Type: [LINK - User clicked a link] (URL not typed directly - no typed count)	registrar

1 days

2015-08-25T21:01:50+00:00	[crtime;ctime;mtime] TSK:/Users/dean/.ssh/id_rsa	dean-mac

11 days

2015-09-06T11:01:03+00:00	[Last Time Executed] Prefetch [CMD.EXE] was executed - run count 2 path: \WINDOWS\SYSTEM32\CMD.EXE hash: 0x4A81B364 volume: 1 [serial number: 0x885029E6, device path: \DEVICE\HARDDISKVOLUME2]	registrar
2015-09-06T11:02:02+00:00	*File is present in Viper. Projects: "default" Tags "free_wind"* [atime;crtime] TSK:/Windows/AppPatch/shared/freedom_trebuchet.exe;VSS1:TSK:/Windows/AppPatch/shared/freedom_trebuchet.exe	registrar
2015-09-06T11:02:04+00:00	*File is present in Viper. Projects: "default" Tags "free_wind"* [ctime;mtime] TSK:/Windows/AppPatch/shared/freedom_trebuchet.exe;VSS1:TSK:/Windows/AppPatch/shared/freedom_trebuchet.exe	registrar
2015-09-06T11:06:31+00:00	[atime;crtime] TSK:/Windows/AppPatch/Shared/plink.exe;VSS1:TSK:/Windows/AppPatch/Shared/plink.exe	student-pc1
2015-09-06T11:06:33+00:00	*Application Execution* [File Last Modification Time] [\ControlSet001\Control\Session Manager\AppCompatCache] Cached entry: 16 Path: \??\C:\Windows\AppPatch\shared\plink.exe	student-pc1
2015-09-06T16:47:50+00:00	[Creation Time] Type: OpenSSH login (32800) Information: [BSM_TOKEN_SUBJECT32_EX: aid(502), euid(502), egid(20), uid(502), gid(20), pid(4957), session_id(4957), terminal_port(49519), terminal_ip(192.168.1.11)]. [BSM_TOKEN_TEXT: successful login dean]. [BSM_TOKEN_RETURN32: Success (0), System call status: 0]	dean-mac

9 days

2015-09-15T19:39:51+00:00	[atime;mtime] TSK:/Users/bchang/Google Drive/Prospective Students.xlsx	registrar

DEMO

Si j'ai le temps et que les dieux de la démo sont avec moi....

https://demo.timesketch.org

Dans le future (pas trop far away)

Plaso

- Plus d'attributs NTFS
- Support LVM & LUKS
- Timestamp précision

Timesketch

- Intégration avec GRR
- Gestion des droits

Greetz:

log2timeline-maintainers@googlegroups.com

timesketch

Thanks !

github.com/log2timeline/plaso
github.com/log2timeline/dfvfs
github.com/google/timesketch

3x Apache License 2.0

~~PRs~~ CLs welcome