Persistent Storage Analysis – Part II

Helping Hands

Tobias Dussa
WP8-T1

Webinar, May 2022

Public

www.geant.org

Game Plan

- Ultra-quick recap,
- Showcase some useful tools:
  - tabledevil's docker containers,
  - Plaso,
  - Fimetis,
  - Autopsy.
- Questions/discussion/open mike session.

Preparatory Remarks and Intro
(This Should Feel Familiar)

The Bigger Picture

So there is some sort of persistent storage that you would like to analyze.

We have seen this is tedious work. Now let's look at some examples of tools that make things easier.

For the demos in this talk, we look at raw disk images of our target systems.

Show Time!

Some Simplification With Docker

You might need to do some forensics work on the road → Your usual lab equipment is not available. Neat idea to handle these cases:

Put some useful things into highly-portable docker containers. As an example, consider **`tabledevil`**'s containers on Docker hub:

`https://hub.docker.com/r/tabledevil`

Super Timelines: Plaso

So far, we have scraped file systems for timeline data. But as was already hinted at, there is much more data to harvest and sort into timelines. “Plaso Langar Að Safna Öllu” (or “Plaso” for short) helps scape and unify data sources:

https://github.com/log2timeline/plaso

Timeline Analysis and Visualization: Fimetis

Timelines contain a lot of information, but it can be hard to find and extract. Fimetis (“Filesystem Metadata Analysis”) is an academic project at Masaryk University with the support of CSIRT-MU and helps visualizing and filtering filesystem timelines:

https://github.com/CSIRT-MU/fimetis

Grand Integration: Autopsy

Autopsy has been along for a very long time. It integrates timeline examination with data and metadata harvesting, analysis, reporting, and a lot of other functionality:

https://sleuthkit.org/autopsy/

Wrap-Up

Forensics is a LOT of Painstaking Work

All things told, forensic analysis is mostly tedious and boring work, wading through lots and lots and lots of digital artifacts, searching for the clue that unlocks the puzzle.

Any automation helps.

BUT powerful tools require effort to get acquainted and learn how to use them properly *beforehand*.

Closing Remarks

- Even though there are long stretches of boring and tedious footwork, forensic analysis can be thrilling and fun!
- Be open-minded to new techniques, approaches and tools, and make sure to practice in order to develop and hone skills!
- For any given investigation, set a clear target so that you have a breakout condition!
- Don’t be afraid to ask others for help!

Thank you! Enjoy! :)

Any questions?

www.geant.org

The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).