Your workflow is NOT my workflow!

SANS DFIR Summit EU - 2014

A short rant about “tool imposed workflow”

by Joachim Metz

Google™

Your workflow is NOT my workflow!

- Stop the BS: ~~super timeline~~, ~~sniper forensics~~"Whatever works (most optimal) for you."
- Incident Response: first triage then analyze
  1. Hypothesize; first ask the 5-w's:
     who, what, when, where, why (and how?)
  2. Determine scope and priority:
     What do I need? ~~Now~~ Yesterday, what can wait?
  3. Start collecting data and analyzing:
     How many systems? Where? Do I call in support?
  4. Continuously revisit points 1, 2, 3.
  5. Aftercare: Peer review, fix issues and/or tooling.

Get Security.Evtx of a volume snapshot from a BitLocker image

- Steps: start case?, add evidence?, preserve evidence and wait?, BDE support?, VSS support?, process evidence and wait?, EVTX + message strings support?

- The suite, e.g. <enter name here> versus the toolbox e.g. SIFT
- How about x 10 systems. Can I script it?
- Remote location(s)? Do I need a dongle?
- How interact with 3rd party tools?

My ideal tooling

1. Does not get in the way of the analysis!
2. No dongle!
3. Supports one-off scripts, targeted analysis and auto-processing.
4. Allows for analysis and exploring, also useful for research purposes.
5. Easily adaptable and extendable.
6. Be transparent all the way.
7. ...

What has been achieved

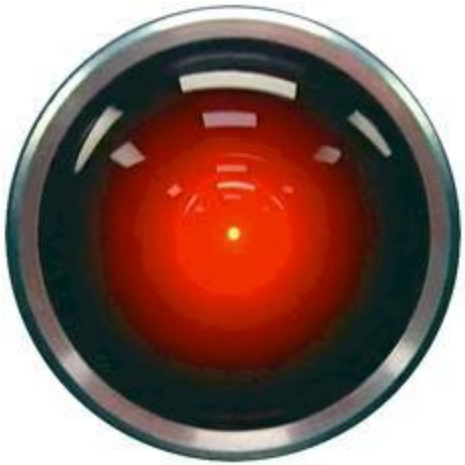
- 2006: “Timelining with mactime is better than most other tools. Alas it only reads RAW. Why not have the SleuthKit read the E01 format?” => libewf
- 2009: “We have this mactime timeline, why not include more time sources into it?”
  => log2timeline
- 2012/2013: “What I really need is a forensic Swiss army knife”
  => plaso + libyal

What I want to achieve

- Domain knowledge reuse
  - Enriching data
  - Forensic artifacts
- Visualization
  - Heatmaps, clustering, charts, tree/graphs
- Automated analysis support
  - Better one-off script support, e.g. pyvfs
  - Semantic technology: AFF4,
    GRR semantic proto

Conclusion

~~“I'm sorry, Dave, I'm afraid I can't do that.”~~



Have the tools work for you! Not vice versa.

References

Google logo (Used with permission)

Digital chalk outline (Creative Commons)

http://www.forensicswiki.org/wiki/File:Joachim_Metz.jpeg

swiss army knife (Creative Commons)

http://en.wikipedia.org/wiki/File:Wenger_EvoGrip_S17.JPG

Plaso logo (Used with permission)

https://lh6.googleusercontent.com/Imix4Wnn8v__wXcv4vXdXwzOzlFuiV6i5uVvUm2_8F6FMY7Qjze-qcHLiugFjwsOdNn9s5aVrk94diS2kRumQPPPZZHLzNq1VdSk8vSuoHrqPwCot1RoifA6UMU

Hall9000 (Creative Commons)

http://en.wikipedia.org/wiki/File:HAL9000.svg