#OSDFCon
OPEN SOURCE DIGITAL FORENSICS CONFERENCE

What's Missing in Open Source?

Motivation

- Collect ideas about what people need.
- Raise awareness about features that developers could write.

Summary of Themes from 2018 (part 1)

- Inputs: APFS, cloud data, mobile device acquisition, PCAP, VMFS, collection agents.
- Analysis:
  - Mobile: More apps and iOS data
  - Analytics: log files, timeline analysis, behavior analytics
  - Integrate more 3rd party modules
  - Encryption: Password cracking, BitLocker support, File Vault,…
  - Email de-duping
  - Baseline comparison

Summary of Themes from 2018 (part 2)

- Review:
  - Automated / quick triage preview
  - Web-based agent case review
- Reporting:
  - Unified output (such as CASE/UCO)
  - HTML reports that don't include tagged images
  - "Improved reporting"
- Training:
  - Basic user guides
  - Online training
- Many of these were also in the 2017 survey

What's Changed?

- More mobile support
- APFS is in progress
- More web support (past year's request)
- 3rd Party modules were integrated (next release)
- Continued focus on triage
- Started support for CASE/UCO
- Online Autopsy training is in progress
  - Will be free for law enforcement for a year
  - Released by end of the year

What Else Planned (from this list)?

- Starting web-based review approach (building REST APIs)
- Continuing:
  - APFS & Logical Disk Management
  - Mobile
  - CASE/UCO
  - Triage

What Else?

- The floor is open..