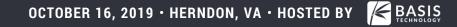


What's Missing in Open Source?





- 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:
 - \circ $\,$ 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:
 - \circ $\,$ Automated / quick triage preview
 - \circ $\,$ Web-based agent case review $\,$
- Reporting:
 - Unified output (such as CASE/UCO)
 - $\circ~$ HTML reports that don't include tagged images
 - "Improved reporting"
- Training:
 - Basic user guides
 - \circ 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
 - \circ $\,$ Will be free for law enforcement for a year $\,$
 - \circ $\,$ Released by end of the year $\,$

What Else Planned (from this list)?

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



• The floor is open..

