Computer Forensics Tool Catalog: Connecting Users With the Tools They Need

AAFS –February 21, 2013

Ben Livelsberger
NIST
Information Technology Laboratory
CFTT Project

Disclaimer

Certain trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose. Neither NIST nor myself has financial interest in any of the real products mentioned as part of this talk.

Overview

- Introduction
- How the Catalog Works
- Features / Benefits
- Website Demo
- Conclusion
- Sponsors
- Questions

Introduction: The Perfect Tool

- Idea: one tool that does everything
- Reality: need a bunch of tools

- Solution: an effective way for connecting practitioners to the tools they need

How Does the Tool Catalog Work?

It's taxonomy-driven

Taxonomy: Forensic functionalities + associated technical parameters and technical parameter values

Example: *Deleted File Recovery*

Technical Parameters:

- "*Tool host OS / runtime environment*": Windows, Linux, Mac
- "*Supported file systems*": FAT16, FAT32, NTFS, exFAT, EXT3
- "*Overwritten file identification*": supported, not supported

Taxonomy-driven: benefits

- It's searchable
- Uniform information across tools
- It's vendor populated
  - tool info more accurate, easier to collect
  - tool submissions reviewed at NIST before posting
  - field to list available test reports

Demo

Conclusion

- Purpose: connect practitioners w/ the tools they need
- Taxonomy driven, searchable, vendor populated
- Spread the word. Ask vendors you work with to list their tools. Give us feedback; tell us what you like/don't like.

Project Sponsors

- Department of Homeland Security, Science and Technology Directorate (Major funding)
- NIST/OLES (Program management)

Contacts

Computer Forensics Tool Catalog:

www.cftt.nist.gov/tool_catalog/index.php

Ben Livelsberger

livebe01@nist.gov

www.cftt.nist.gov

cftt@nist.gov

Sue Ballou, Office of Law Enforcement Standards

susan.ballou@nist.gov

Questions?