# Federated Testing: Well-Tested Tools, Shared Test Materials & Shared Test Reports; The Computer Forensics Tool Catalog Website: Connecting Forensic Examiners With the Tools They Need

U.S. Cyber Crime Conference – May 2, 2014

Ben Livelsberger
NIST Information Technology Laboratory,
Computer Forensics Tool Testing 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

- Overview of CFTT
- Computer Forensic Tool Catalog website
- Federated Testing Project
- Summary
- Sponsors
- Questions

# CFTT Overview

- **Computer Forensics Tool Testing Project**

**James Lyle, Project Leader**

100 Bureau Drive, Stop 8970

Gaithersburg, MD 20899-8970 USA

E-mail cftt@nist.gov

**Website: www.cftt.nist.gov**

# CFTT Overview

- CFTT – Computer Forensics Tool Testing Program provides a measure of assurance that the tools used in the investigations of computer-related crimes produce valid results.
- Directed by a steering committee composed of representatives of the law enforcement community.
- The steering committee selects tool categories for investigation and testing. A vendor may request testing of a tool, however the steering committee makes the decision about which tools to test.
- CFTT is a joint project of: DHS, OLES, FBI, DoD, Secret Service, NIJ and other agencies.

# CFTT Methodology

- **Test Specification – Requirements**
- Test Plan – Test Cases and Assertions
- Setup and Test Procedures
- Final Test Report Generation

# Requirements

- Requirements – Statements used to derive test assertions that define expectations of a tool or application.
  - Core Requirements – Requirements that all mobile device acquisition tools shall meet.
  - Optional Requirements – Requirements that all mobile device acquisition tools shall meet on the condition that specified features or options are offered by the tool.

# CFTT Methodology

- Test Specification – Requirements
- **Test Plan – Test Cases and Assertions**
- Setup and Test Procedures
- Final Test Report Generation

# Test Plan

- Test Cases – Describe the combination of test parameters required to test each assertion.
- Assertions – General statements or conditions that can be checked after a test is executed

# CFTT Methodology

- Test Specification – Requirements
- Test Plan – Test Cases and Assertions
- **Setup and Test Procedures**
- Final Test Report Generation

# Setup and Test Procedures

- Objective: Documentation on data population of target media and test procedures providing third parties with information for an independent evaluation or replication of posted test results.

- Contents:
  - Techniques used for data population
  - Test Case Execution Procedures

# CFTT Methodology

- Test Specification – Requirements
- Test Plan – Test Cases and Assertions
- Setup and Test Procedures
- **Final Test Report Generation**

# Test Report

- Results summary
- Test case selection
- Results by Test Case-Variation
- Testing environment
- Test results

# Tool Validation

- Tool validation results issued by the CFTT project at NIST provide information necessary for:
  - Toolmakers to improve tools
  - Users to make informed choices about acquiring and using computer forensic tools
  - And for interested parties to understand the tools capabilities

# Computer Forensics Tool Catalog Website – 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*

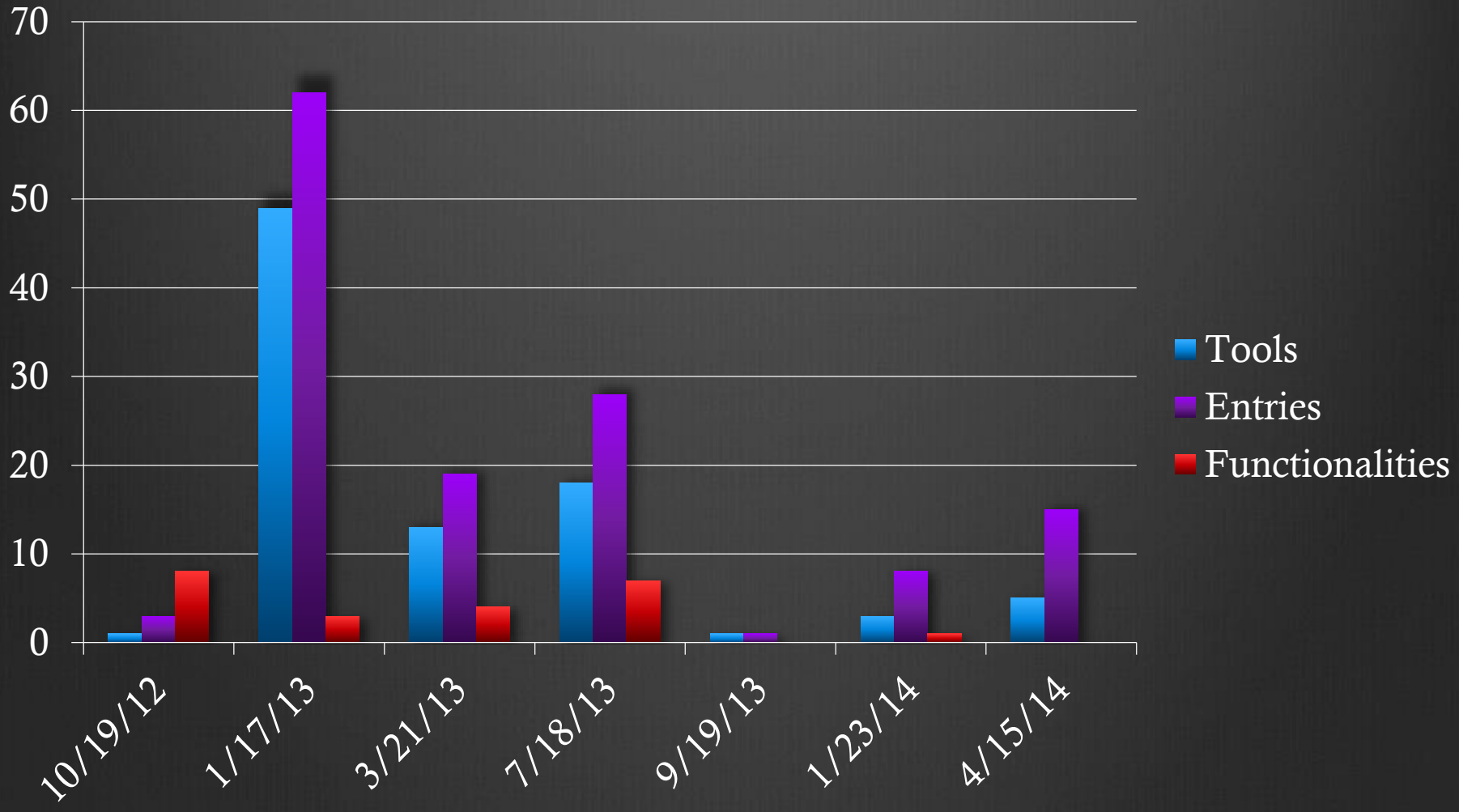
Technical Parameters:

- "*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

# New Tools, Entries, Functionalities by Month



# What's in the Catalog?

| | | | | | |
|---|---|---|---|---|---|
| Cloud Services | 1 | Hardware Write Block | 14 | Remote Capabilities/Remote Forensics | 2 |
| Deleted File Recovery | 9 | Hash Analysis | 9 | Social Media | 5 |
| Disk Imaging | 12 | Image Analysis (Graphic Files) | 2 | Software Write Block | 5 |
| Email Parsing | 10 | Instant Messenger | 3 | Steganalysis | 4 |
| File Carving | 2 | Media Sanitization/Drive Reuse | 4 | String Search | 6 |
| Forensic Boot Environment | 2 | Memory Capture & Analysis | 11 | Web Browser Forensics | 2 |
| Forensic Tool Suite (Mac Investigations) | 3 | Mobile Device Acquisition & Analysis | 19 | Windows Registry Analysis | 3 |
| Forensic Tool | 4 | P2P Analysis | 4 | | |

# Community/Vendor Participation

ATC-NY

AccessData

Arsenal Recon

ArxSys

Backbone Security - Steganography Analysis and Research Center (SARC)

Belkasoft

BlackBag Technologies

CRU-DataPort / WiebeTech

CYANLINE LLC

Cellebrite Mobile Synchronization Ltd.

Computer Evidence Specialists LLC

Defense Cyber Crime Center (DC3)

Defense Cyber Crime Center

Elcomsoft Co Ltd

Fookes Software Ltd

Forensic Telecommunications Services Ltd

ForensicSoft, Inc.

Fox-IT

HBGary

Hot Pepper Technology, Inc.

Intelligent Computer Solutions, Inc

Katana Forensics Inc.

Magnet Forensics

Micro Systemation AB (MSAB)

Paraben Corporation

Sleuth Kit

Susteen Inc.

SysTools Software Private Limited

Tableau by Guidance Software

Teel Technologies

The Sleuth Kit

X-Ways Software Technology AG

dtSearch Corp.

maresware

perlustro lp

viaForensics

# Demo

# Federated Testing: Shared Test Materials & Well-Tested Tools

- Tools, methods and procedures must be validated
  - Correct and efficient processing of digital evidence
  - Admissibility to courts/judicial proceedings
- Tool validation
  - Difficult
  - Expensive
  - Time consuming

# What is Federated Testing?

- Same tools used across agencies, labs and digital evidence sections – a lot of duplicated work
- The Computer Forensics Tool Testing (CFTT) Project at NIST currently creates tool specifications, test methods and test reports.
- Federated Testing is an expansion of CFTT to provide the digital forensics community with shared test materials for tool validation.
- Benefits:
  - Cost savings
  - Can improve quality of testing (rigorous methods and high quality testing materials)

# Target Areas

- CFTT has methodologies for:
  - disk imaging
  - Hardware Write Block*
  - Mobile Devices*
  - Forensic Media Preparation*
  - Deleted File Recovery
  - File Carving
- Implementing:
  - disk imaging ← available Fall 2014

# What will the test materials look like?

- Platform for delivering the materials: live Linux (Ubuntu) CD
- Components:
  - Website
    - Reference information
    - Test Plan
    - Final report
  - Command line test support tools
    - Test case setup and analyze results

# Demo

# Summary

- Computer Forensics Tool Catalog Website
  - Purpose: provide an effective way for connecting practitioners with the tools they need
  - Taxonomy-driven, vendor populated & searchable
- Federated Testing
  - Tool validation is difficult, expensive and time consuming
  - Federated Testing is an expansion of CFTT to provide the digital forensics community with shared test materials for tool validation – coming this Fall!

# Summary (cont.)

- Computer Forensics Tool Catalog website - Spread the word. Ask vendors you work with to list their tools. Give us feedback; tell us what you like/don't like.
- Federated Testing – Give me you contact information. We'd love to get your feedback!

# 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

benjamin.livelsberger@nist.gov

www.cftt.nist.gov

cftt@nist.gov

Sue Ballou, Office of Special Programs

susan.ballou@nist.gov

# Questions?