July 24-28 @NIST, Gaithersburg, MD

Technical Tracks

- Crime Scene
- Death Investigation
- Human Factors
- Legal Factors
- Quality Assurance
- Laboratory Management
- Criminalistics
- Digital Evidence

go.usa.gov/x9yEK

Or search for “NIST 2017 forensic error management”

EXPERIENCE VALIDATING DISK-IMAGING TOOLS WITH CFTT FEDERATED TESTING

Jim Lyle

CFTT/NIST

isclaimer

ertain trade names and company products are mentioned in the text or
entified. In no case does such identification imply recommendation or
ndorsement by the National Institute of Standards and Technology, nor does
nply that the products are necessarily the best available for the purpose. No
nancial interest.

FTT

e CFTT project at NIST develops methodologies for testing computer ensic tools. Currently there are CFTT methodologies for testing the owing:

- isk imaging
- /rite blocking
- eleted File Recovery
- ile Carving
- orensic Media Preparation
- lobile Devices

variety of tools in each of these categories have been tested and served flaws in the tools have been reported by the National Institute Justice (NIJ) and the Department of Homeland Security (DHS). These sults can be used as a basis for identifying the types of likely failures it occur in forensic tools.

ederated Testing
tp://www.cftt.nist.gov/federated-testing.html

aring CFTT Test Methods, Tools & Forensic Lab Test Reports

elieves a forensic lab of the task of developing a test materials or tool testing because Federated Testing generates a test based n selections made by the user describing how the lab uses the ested tool:

1. A list of test cases (based on user input)
2. Tools and detailed procedures for creating test drives (adding known content)
3. Detailed procedures for running each test case
4. Tools to evaluate test results
5. Tool to generate a skeleton test report that can then can be finished in the style favored by the laboratory.

he test reports can be shared with other labs

/hat Does Software Testing Get for you?

oftware Testing is asking questions to see how the tested tool eacts to various inputs

software gives the wrong answer it usually is triggered by a pecific condition

etter understanding comes from trying more conditions . . .

- More diversity of questions
- More detailed questions

esting documents tool behaviors that you need to be aware of

esting NEVER can PROVE a program is always correct.

ut it can – and does – catch important errors thus increasing our confidence in the tool

ederated Testing vs Previous Testing

ederated testing is more specific to how a given lab operates

nstead of testing just the tool, test the whole imaging pipeline:
ool => Blocker => OS

revious: Connect to host ATA, SATA, USB & FireWire (4 cases)

ederated Testing: Connect to Host USB & Firewire (from Write
locker); Connect ATA & SATA to blocker (2 cases)

est Cases To Pick From

- Make an image or clone of a drive
- Make an image or clone of media memory card
- Make an image or clone of a partition/file sys
- Hash device or image file
- Out of space errors
- Unreadable (bad) sectors

pecific Test Case Selections for a Particular lab might e . . .

- laking a clone is rare, so skip clone testing
- arely acquire partitions, there are many possible types, but most ommon is NTFS, so just test NTFS
- . . Or We never acquire by partition, so skip partition acquisition
- fter data has been acquired recalculating a hash rarely needed, o skip
- Ve'll skip bad sector tests, not usually an issue for our lab
- . . Or We really need to know what happens to the tool if there is bad sector.

naging Tools Tested

Tool	Version
DC3DD	V7.2.641
FTK	3.4.2.6
Guymager	0.8.1
Logicube Falcon	2.4U1
Logicube Falcon	3.0U1
Paladin/ewfacquire	6.09/20160403
Paladin/DC3DD	6.08/7.1.614
Ditto	V2016 Mar 01 a
TD2u	V1.1.1.3948-4270f9c
X-Ways	18.8

/rite Blockers Used

ocker
bleau T35es-R2
bleau T3
bleau T3U
UltraBlock Card Reader
iebeTech ComboDock
iebeTech FCD v5.5

est Cases Selected for each Tested Tool

ασεσ	ΑΧ3ΔΔ	ΦΤΚ	Γυψμαγερ	Φαλχον ς2	Φαλχον ς3	Παλαδιν 6. 08	Παλαδιν 6. 09	ΤΔ2υ	Διττο	Ξ-Ωαψσ
rive mage	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
ard mage	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
artition mage	✔	✔	✔			✔	✔		✔	✔
ad ector		✔	✔		✔		✔			

est Cases Selected for each Tested Tool

	DC3DD	FTK	Guymager	Falcon V2	Falcon V3	Paladin 6.08	Paladin 6.09	TD2U	Ditto	X-Ways
e	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
e	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
on e	✓	✓	✓			✓	✓		✓	✓
r		✓	✓		✓		✓			

est Results

- or all tools tested . . .
  - All data acquired (nothing omitted)
  - All acquired data is accurate (nothing changed)
- or “bad sector tests” we created 20 bad sectors
  - FTK missed no good sectors
  - Guymager missed no good sectors
  - Logicube V3 missed no good sectors
  - Paladin 6.09 missed 940 readable sectors

ffort Required

Ve tracked staff time and physical resources to measure the evel of commitment that was required to test each tool.

Ve found that with two PCs a single person could setup test rives in less than eight hours. Quicker if more PCs were devoted o the task.

fter the test drives are setup, running the tests takes less than wo days. The most time expended is actually taking the enerated skeleton test report and adding laboratory specific nformation.

a laboratory uses (or just wants to test) more than one imaging ool, the drive setup only needs to be done once and can be eused for additional tool testing.

est Drive Setup

Ve used 6 hard drives and one flash card

2 has an NTFS partition; EE-Bad has faulty sectors created by oftware

Drive ID	Size (GB)	Type	Time to Wipe	Time to Hash
A1	80GB	ATA	1:36	0:40
A2	60GB	SATA/NTFS	1:05	0:30 + 0:10
A3	160GB	ATA	3:35	1:22
A4	160GB	SATA	5:09	1:24
A5	1GB	CF	0:03	0:02
EE-Bad	480MB	SATA	0:32	--
EE-Ref	480MB	SATA	0:32	--

inal Thoughts

- ederated Testing is useful if you need to test your imaging tool.
- est protocol already designed, just need to use it.
- ll NIST generated test reports are online at DHS
  - Other tests can be posted there (Sharing is not required.)
- lext we will be adding tests for . . .
  - Write blocking
  - Mobile device testing
  - String searching
- ake a look, try it, comments and suggestions welcome

July 24-28 @NIST, Gaithersburg, MD

Technical Tracks

- Crime Scene
- Death Investigation
- Human Factors
- Legal Factors
- Quality Assurance
- Laboratory Management
- Criminalistics
- Digital Evidence

go.usa.gov/x9yEK

Or search for “NIST 2017 forensic error management”

ontact Information

Jim Lyle
jlyle@nist.gov
http://www.cftt.nist.gov
http://www/cfreds.nist.gov

Benjamin R. Livelsberger
benjamin.livelsberger@nist.g

Sue Ballou, Office of Law Enforcement Standards
Steering Committee representative for State/Local Law Enforcement
Susan.ballou@nist.gov