FORENSIC SCIENCE ERROR MANAGEMENT

INTERNATIONAL FORENSICS SYMPOSIUM

July 24-28, 2017 @NIST, Gaithersburg, MD

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

## July 24-28 @NIST, Gaithersburg, MD

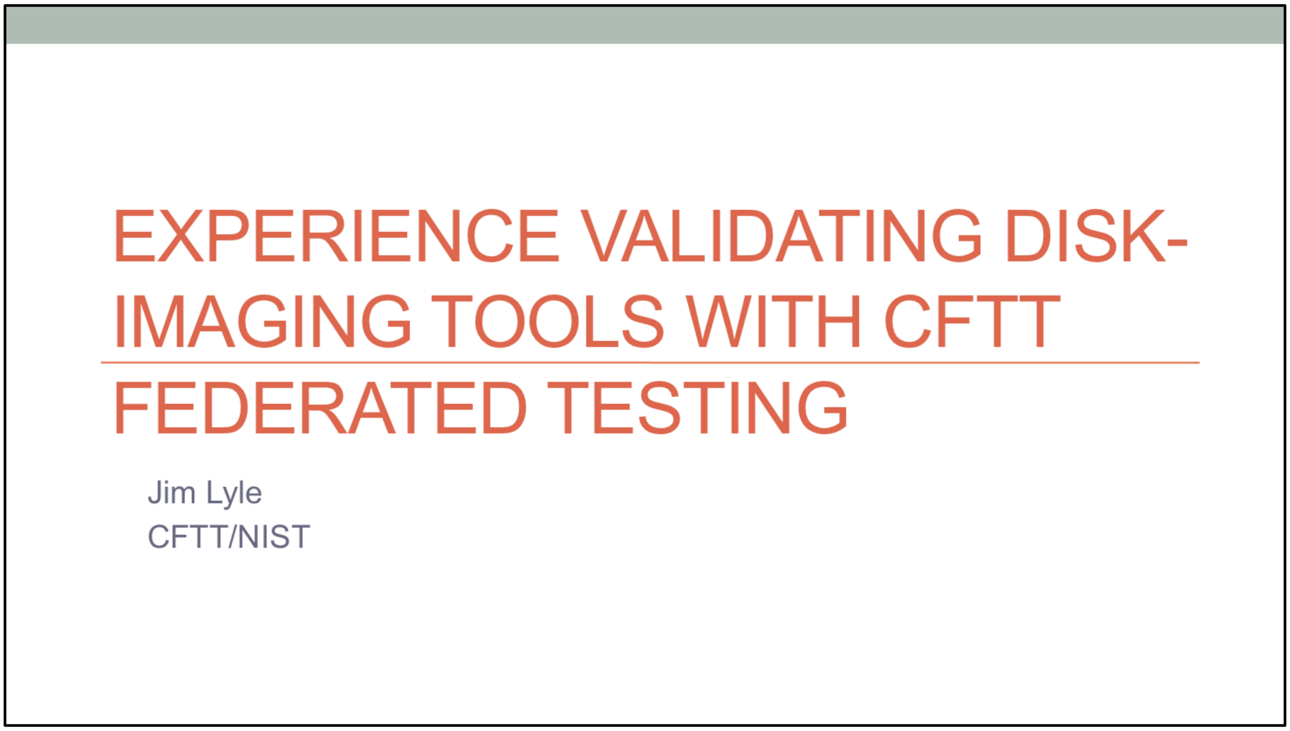
### Technical Tracks

- 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”

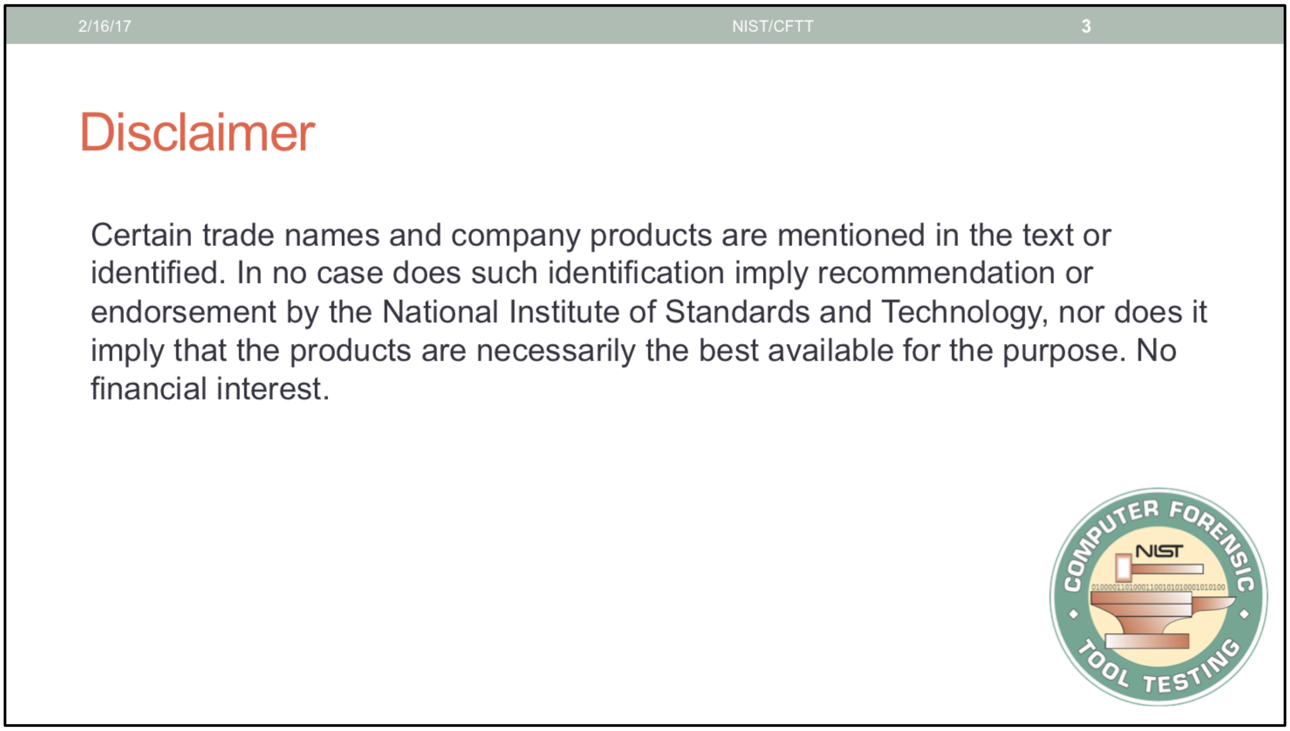
Last full Week of July NIST is hosting the forensic science error management conference at NIST in Gaithersburg.



# EXPERIENCE VALIDATING DISK-IMAGING TOOLS WITH CFTT FEDERATED TESTING

Jim Lyle
CFTT/NIST

Some time ago we posted a “test your imaging tool kit” on a downloadable CD called Federated Testing. We used Federated Testing ourselves to test 10 imaging tools. The test reports are posted on DHS website, we have links from CFTT to the DHS reports. We found the effort to test the tools and create the reports reasonable,

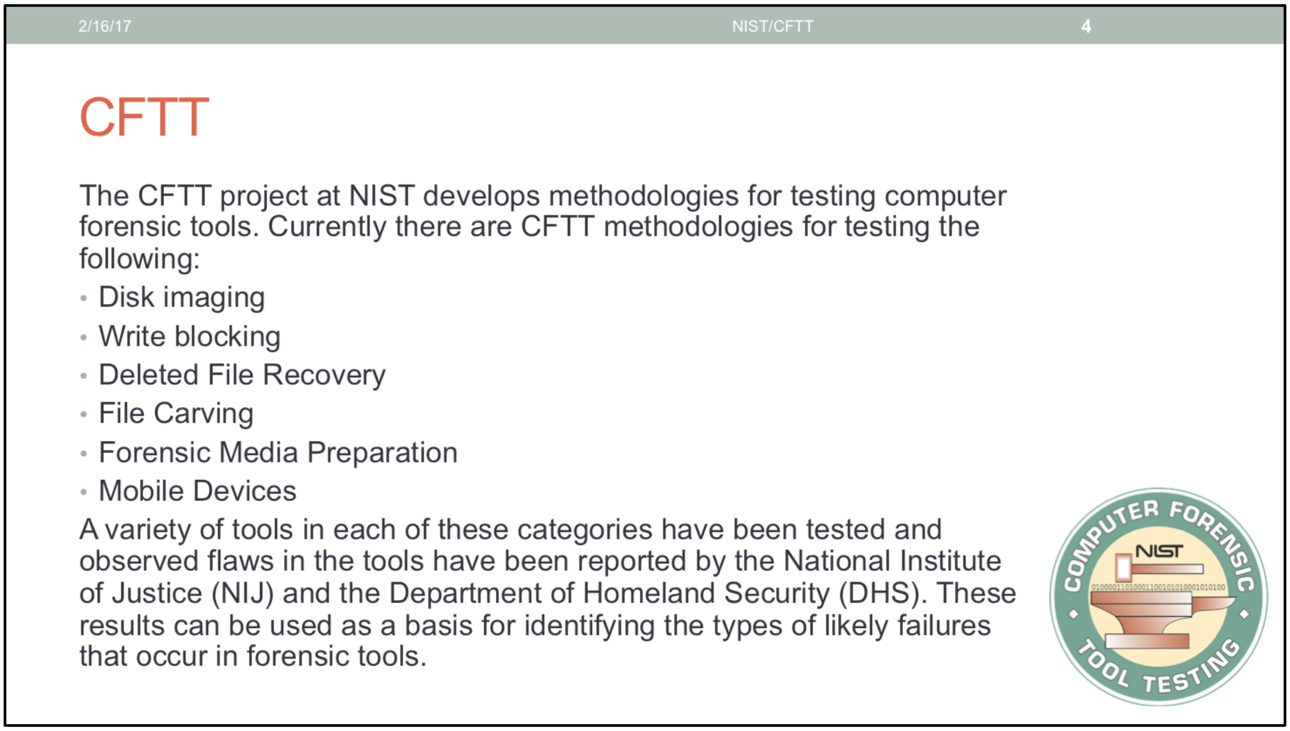


# Disclaimer

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. No financial interest.

COMPUTER FORENSIC
NIST
TOOL TESTING

I do not have any financial interest in any of these products. I do not endorse any of the products.



2/16/17 NIST/CFTT 4

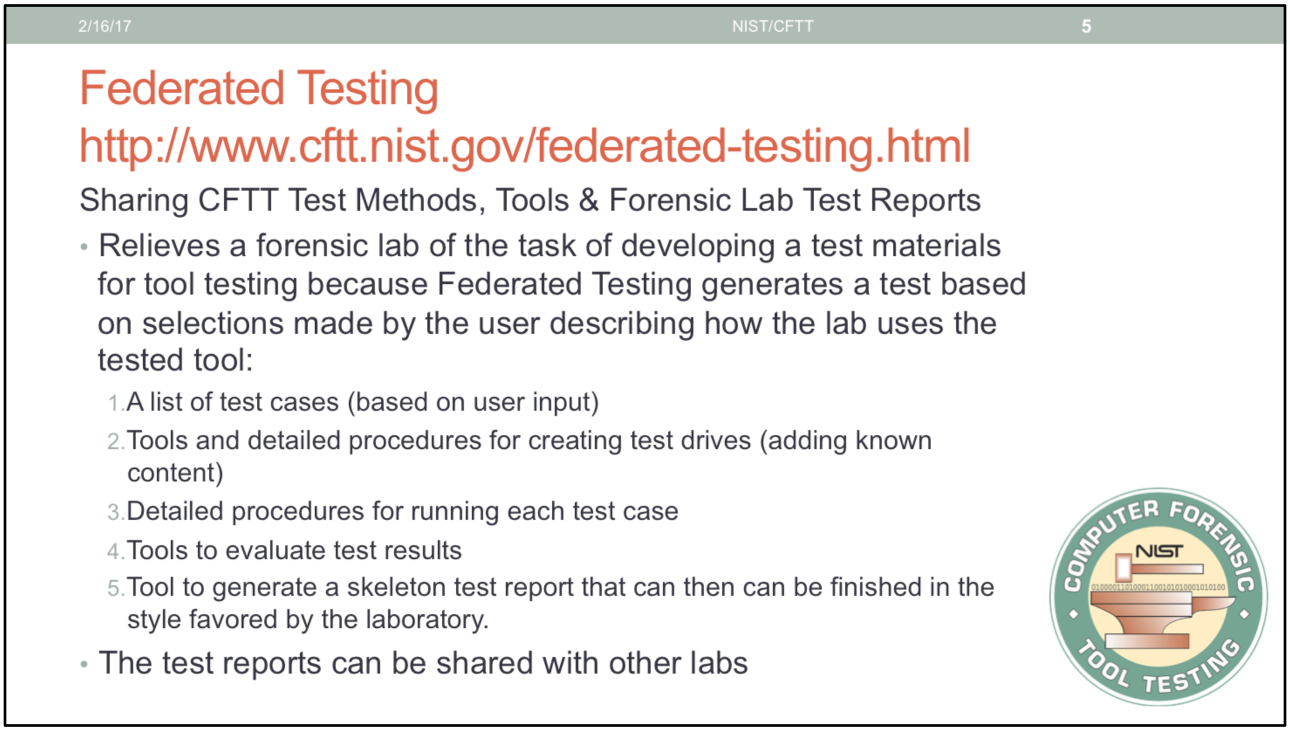
## CFTT

The CFTT project at NIST develops methodologies for testing computer forensic tools. Currently there are CFTT methodologies for testing the following:

- Disk imaging
- Write blocking
- Deleted File Recovery
- File Carving
- Forensic Media Preparation
- Mobile Devices

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

I am with the computer forensics tool testing project at the national Institute of standards and technology. We develop methodologies for testing forensic tools and we apply the methodology to specific tools and the Department of Homeland Security publishes the results. There is no way any one



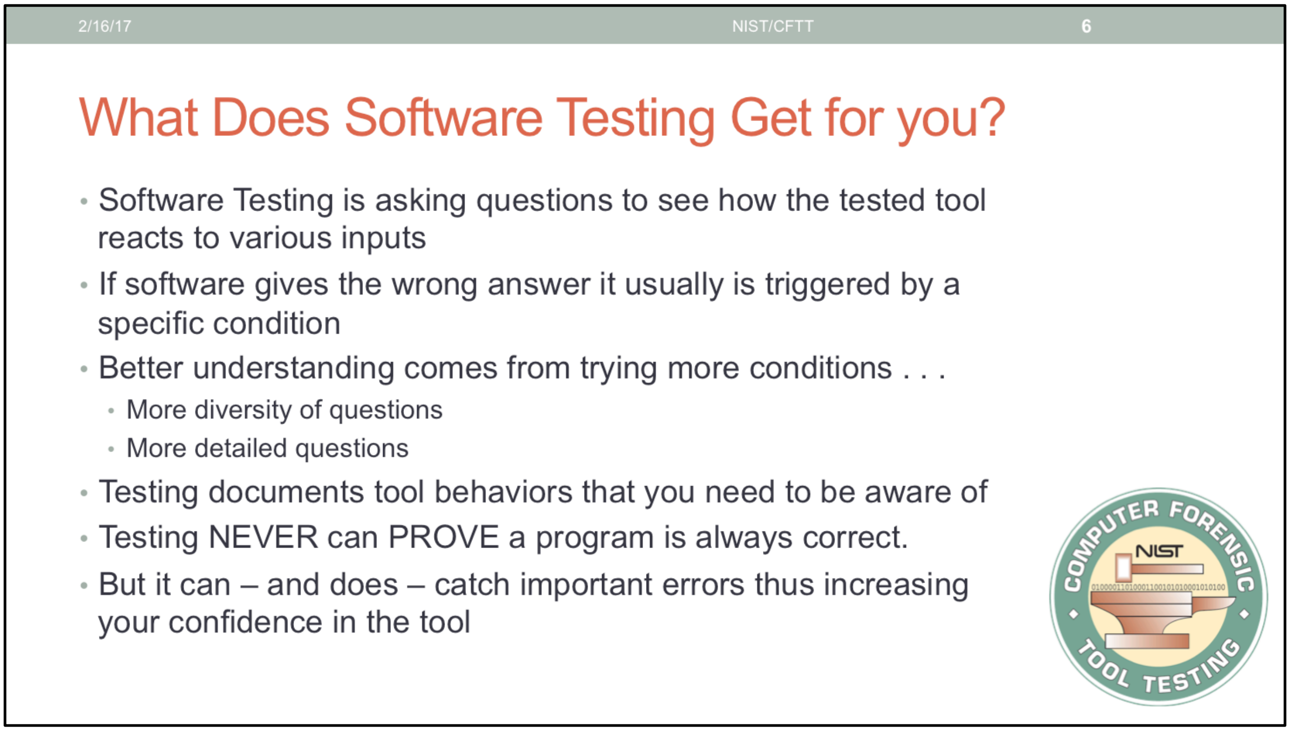
2/16/17 NIST/CFTT 5

## Federated Testing http://www.cftt.nist.gov/federated-testing.html

Sharing CFTT Test Methods, Tools & Forensic Lab Test Reports

- Relieves a forensic lab of the task of developing a test materials for tool testing because Federated Testing generates a test based on selections made by the user describing how the lab uses the tested 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.
- The test reports can be shared with other labs

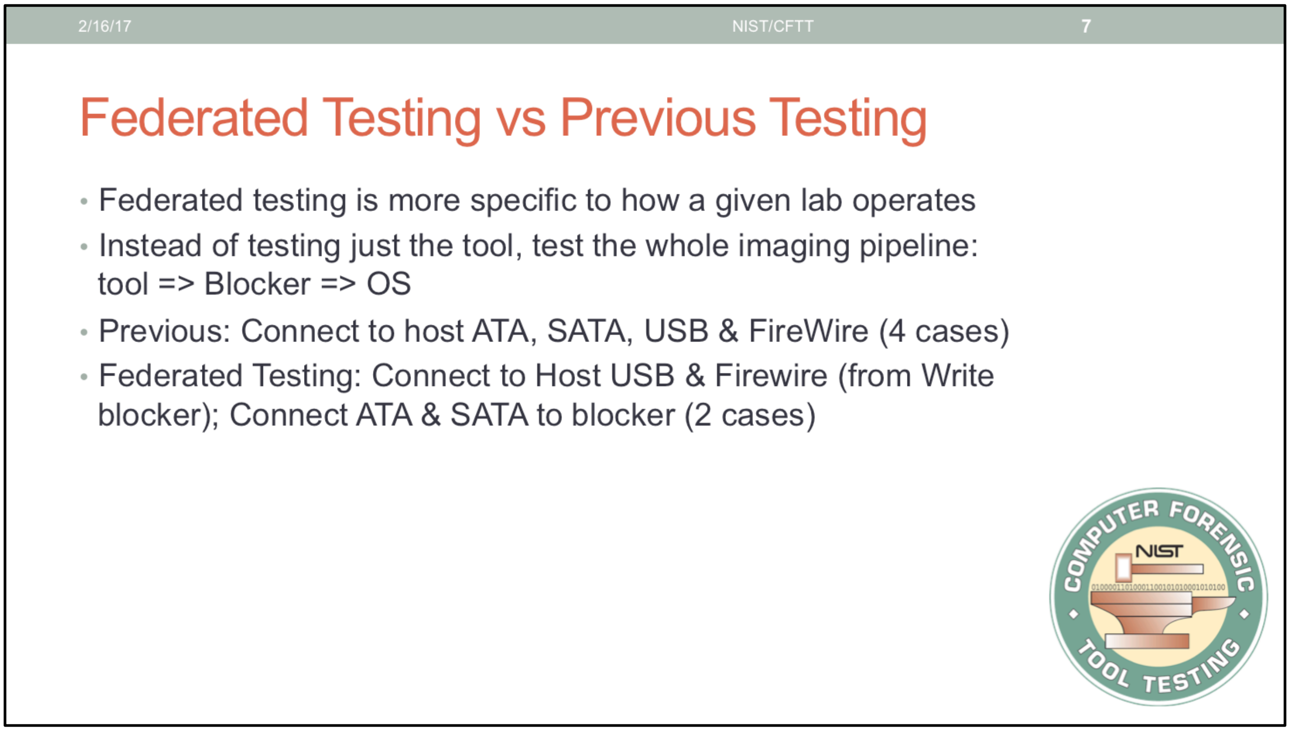
The goal of federated testing is to move high quality testing to labs and to produce more test reports for more tools to enable sharing the tool test results. Federated testing makes the NIST test methods available to a wide audience of users so that many organizations can use the same method to test tools and produced test reports in a similar format. By using the same or similar test data it is easy to compare results for testing tools by different organizations.  In this way, labs can help each other too.



## What Does Software Testing Get for you?

- Software Testing is asking questions to see how the tested tool reacts to various inputs
- If software gives the wrong answer it usually is triggered by a specific condition
- Better understanding comes from trying more conditions . . .
  - More diversity of questions
  - More detailed questions
- Testing documents tool behaviors that you need to be aware of
- Testing NEVER can PROVE a program is always correct.
- But it can – and does – catch important errors thus increasing your confidence in the tool

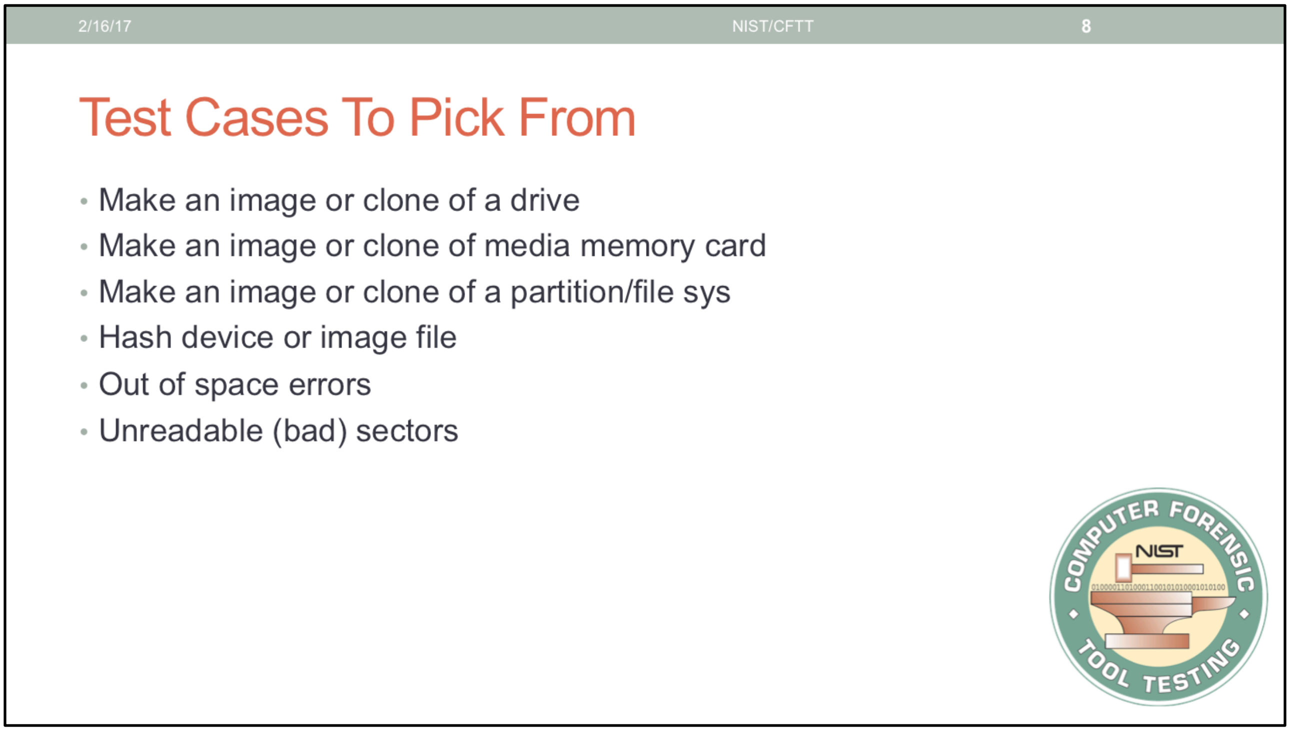
It is challenging to find the right questions. You want each question to bring something unique to the test. You want each question to encourage the tool to do something different. For example, you can image 10 GB Drive, a 20 GB Drive, a 70 GB Drive and these are all the same question Because nothing very different has to happen regardless of the size until you image a 140 GB Drive. Then you have asked a new question. Right about 137 GB there is a change in how software accesses the drive. For some really old OS versions everything works fine until you cross this line, then the tool can't see the rest of the drive.



## Federated Testing vs Previous Testing

- Federated testing is more specific to how a given lab operates
- Instead of testing just the tool, test the whole imaging pipeline: tool => Blocker => OS
- Previous: Connect to host ATA, SATA, USB & FireWire (4 cases)
- Federated Testing: Connect to Host USB & Firewire (from Write blocker); Connect ATA & SATA to blocker (2 cases)

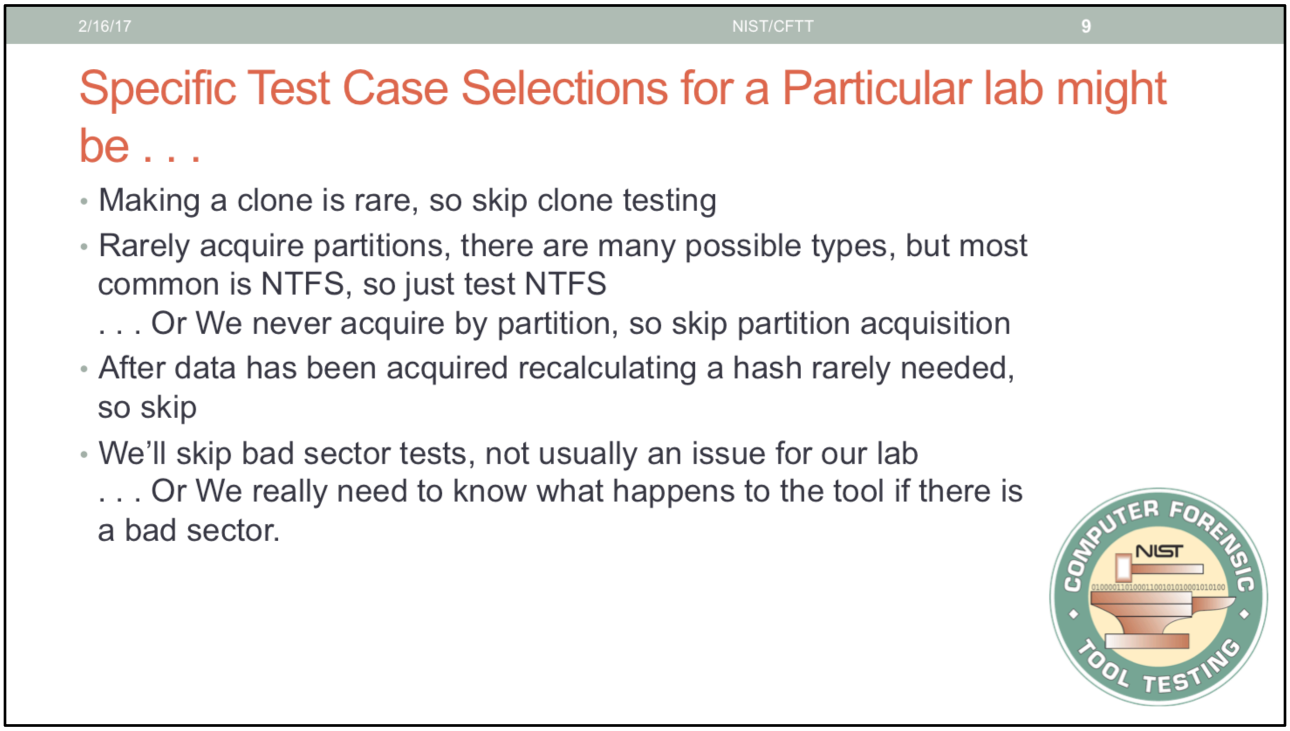
For federated testing we made a small change in how we look at disk imaging. Previously we've focused on testing the tool in isolation. For federated testing we changed the focus to the entire imaging process including the blocker and OS. At NIST, we have lots of disk imagers and blockers that need to be tested. For federated testing we want to focus on the individual lab set up of the lab testing the tool.



## Test 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

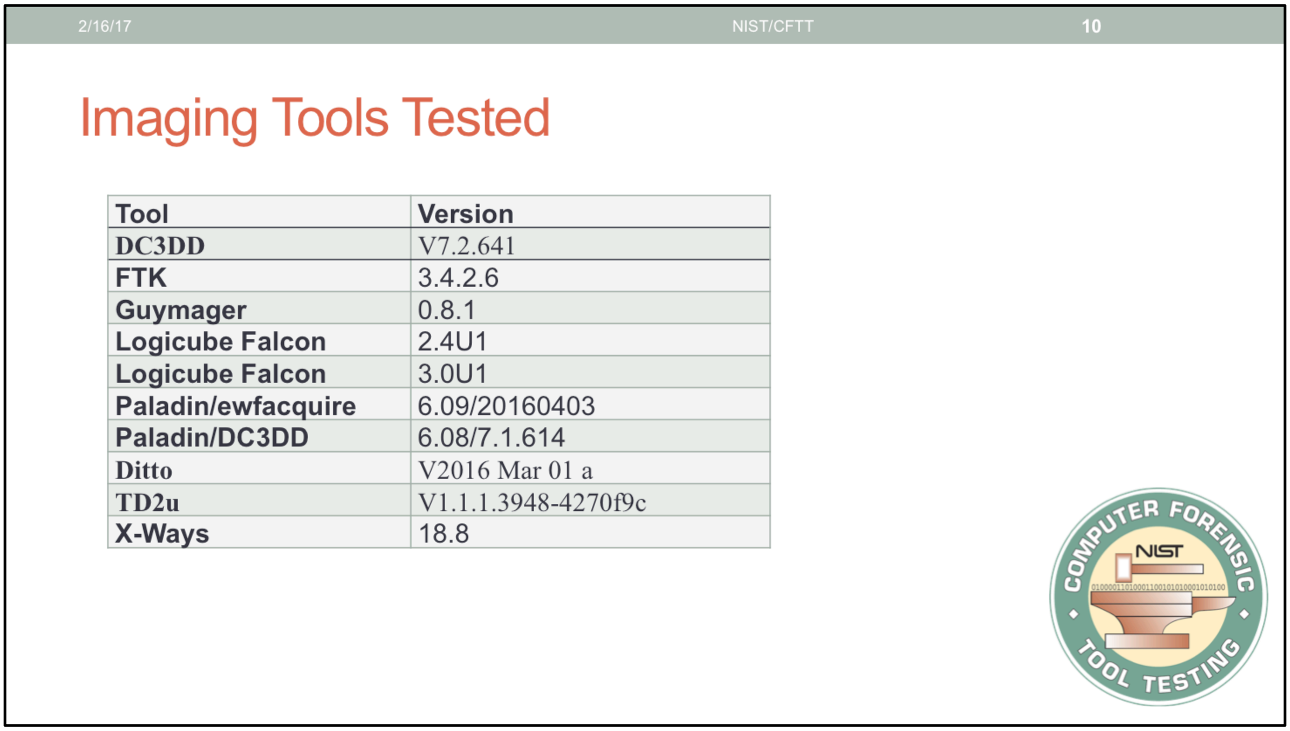
When you use federated testing you get a menu of potential things to test. But they're all variations on these choices. Each lab will pick different items based on the type of casework they see. A lab that deals with large servers say, will probably not see a lot of memory cards or partitions to image. So they'll just be working on making images of a drive. They probably never have to create a clone since that would be very inconvenient to clone 47 TB system. A lab may choose to skip rehashing a device or rehashing image files if they don't use that as part of their procedures. Out of space shares is also a likely candidate to skip. Testing tool behavior if there are bad sectors on a source drive may seem daunting at first, but it's actually quite easy to set up a test drive with reliable faulty sectors.



## Specific Test Case Selections for a Particular lab might be . . .

- Making a clone is rare, so skip clone testing
- Rarely acquire partitions, there are many possible types, but most common is NTFS, so just test NTFS
  . . . Or We never acquire by partition, so skip partition acquisition
- After data has been acquired recalculating a hash rarely needed, so skip
- We'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 a bad sector.

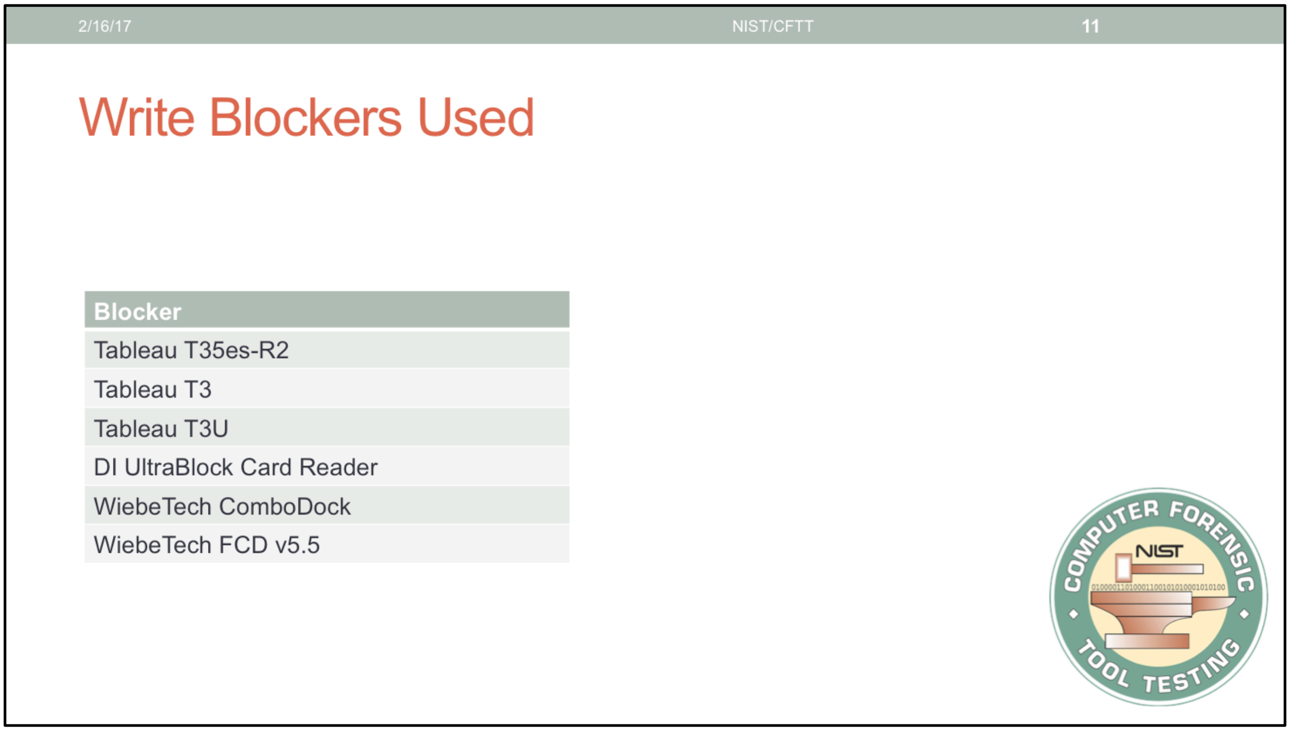
For the tools that we tested we made slightly different choices for each tool. Different labs might make different choices.



## Imaging 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 |

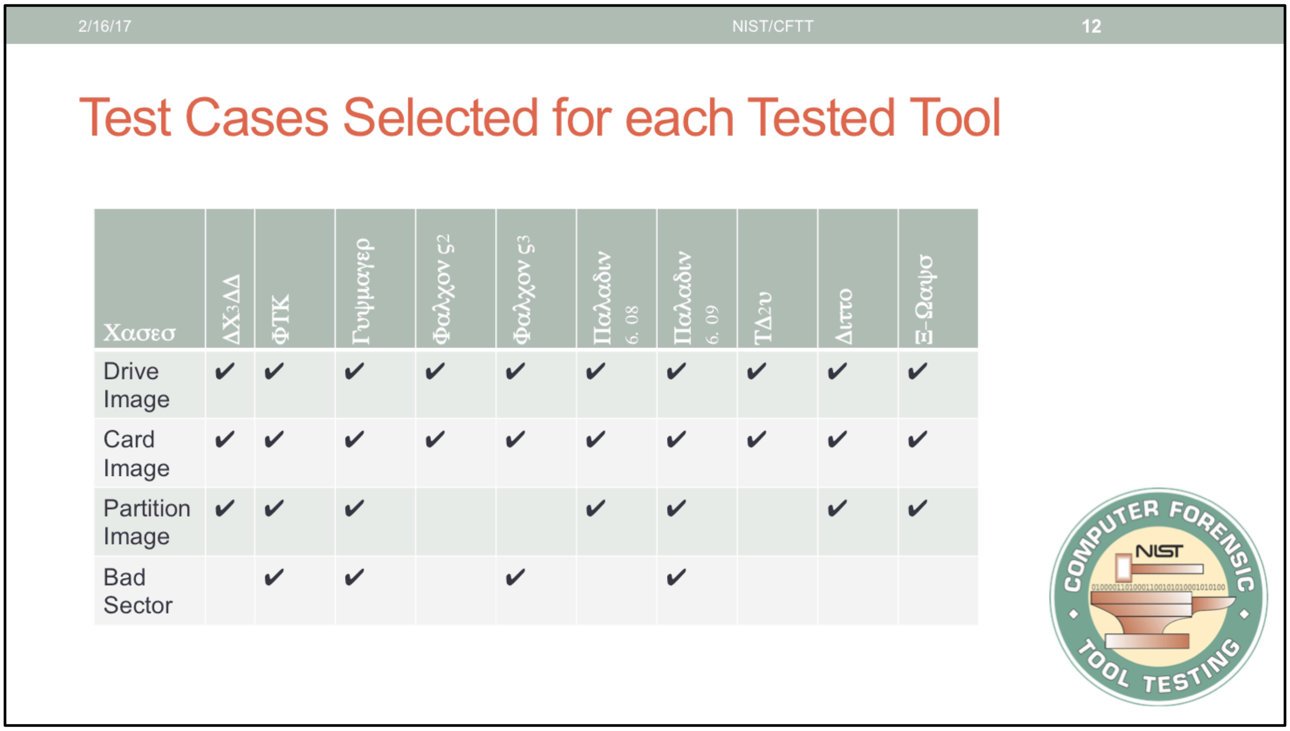
We tested Paladin twice because Paladin is just a wrapper for an underlying image tool. Selecting image file format selects the actual imaging tool tested.
As for the falcon, the unit arrived with 2.4 already installed so we tested that and then upgraded to the latest version which was three point 0.


COMPUTER FORENSIC
NIST
TOOL TESTING

## Write Blockers Used

| Blocker |
|---|
| Tableau T35es-R2 |
| Tableau T3 |
| Tableau T3U |
| DI UltraBlock Card Reader |
| WiebeTech ComboDock |
| WiebeTech FCD v5.5 |

Each time we tested the tool we picked a subset of these right blockers to use during the test. We expect that some labs Focus on one particular model of right blocker while other labs will have to use multiple write blockers.

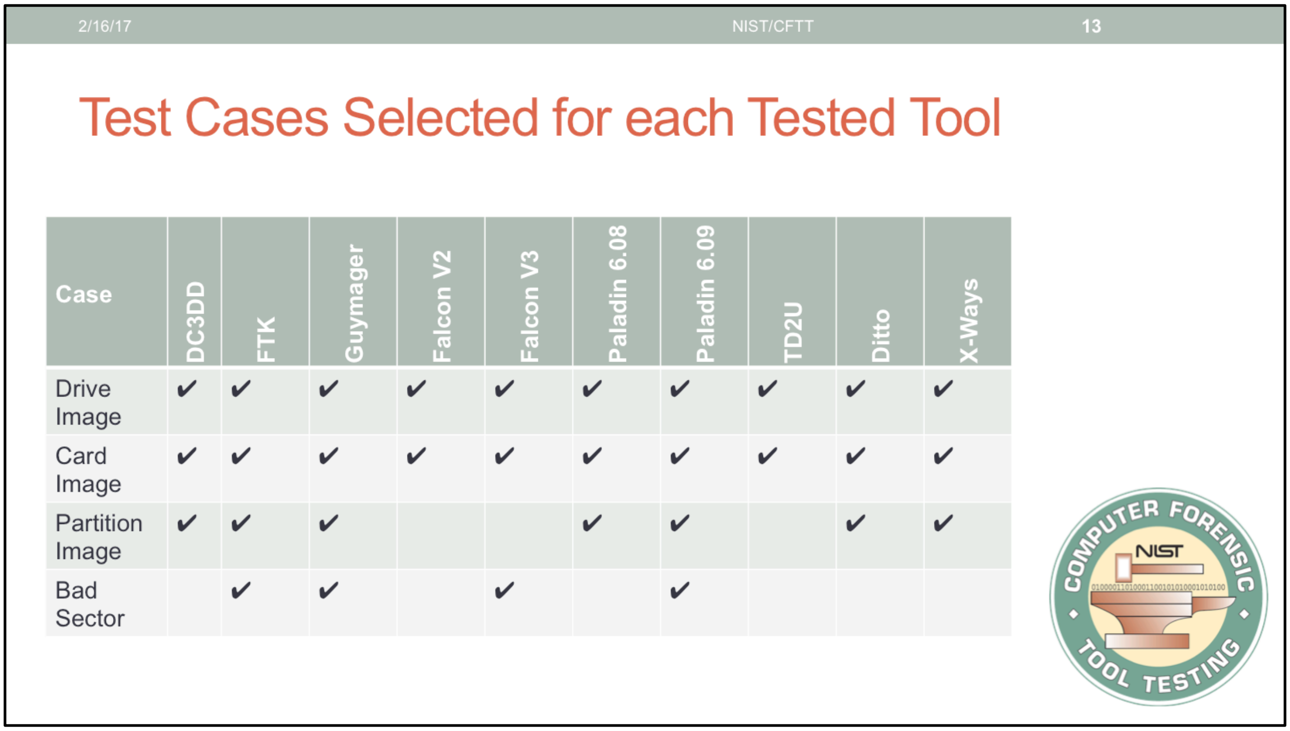


2/16/17 NIST/CFTT 12

## Test Cases Selected for each Tested Tool

| Χασεσ | ΔΧ3ΔΔ | ΦΤΚ | Γυψμαγερ | Φαλχον ς2 | Φαλχον ς3 | Παλαδιν 6. 08 | Παλαδιν 6. 09 | ΤΔ2υ | Διττο | Ξ-Ωαψσ |
|---|---|---|---|---|---|---|---|---|---|---|
| Drive Image | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Card Image | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Partition Image | ✔ | ✔ | ✔ | | | ✔ | ✔ | | ✔ | ✔ |
| Bad Sector | | ✔ | ✔ | | ✔ | | ✔ | | | |

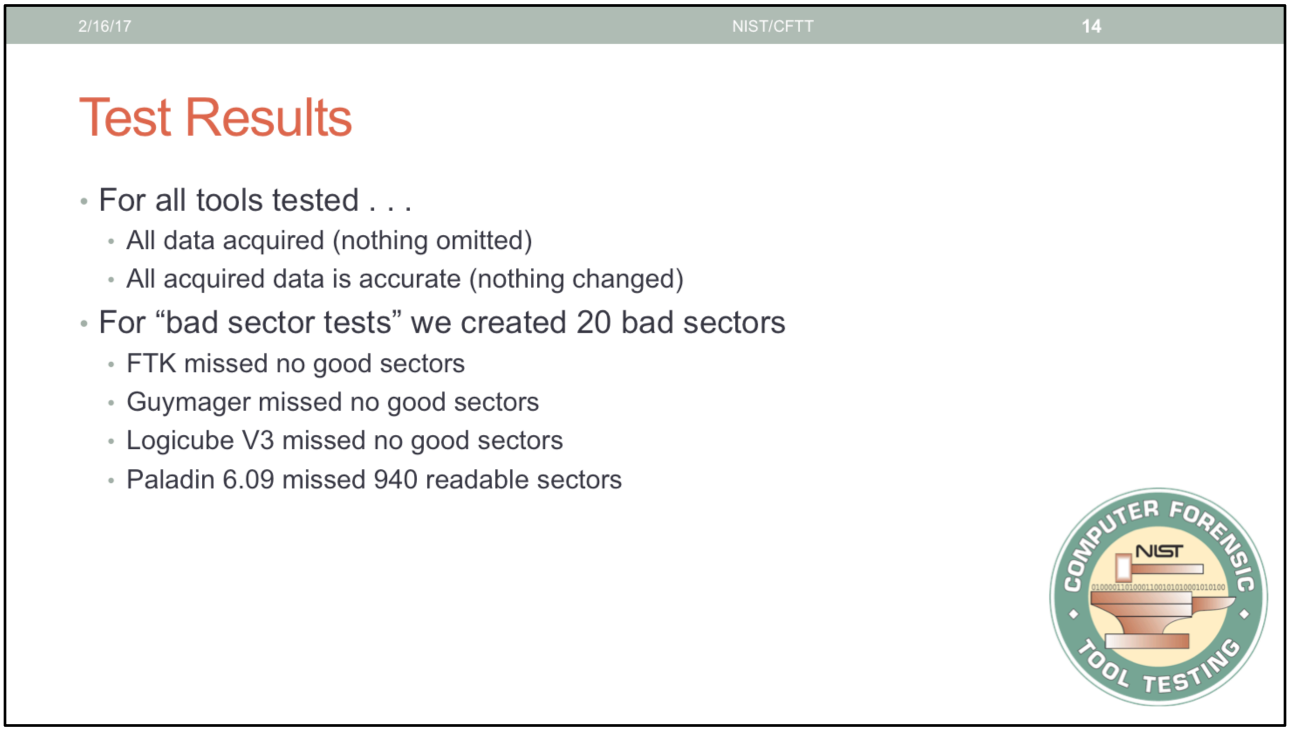
These are the options that we selected for each tool that we tested. As you see we have DC three DD, FTK, Guy manager, part two Falcons, our two paladins, TD two, ditto, and X ways. We varied selection of testing as different labs might very their choices for things to test.



## Test Cases Selected for each Tested Tool

| Case | DC3DD | FTK | Guymager | Falcon V2 | Falcon V3 | Paladin 6.08 | Paladin 6.09 | TD2U | Ditto | X-Ways |
|---|---|---|---|---|---|---|---|---|---|---|
| Drive Image | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Card Image | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Partition Image | ✔ | ✔ | ✔ | | | ✔ | ✔ | | ✔ | ✔ |
| Bad Sector | | ✔ | ✔ | | ✔ | | ✔ | | | |

These are the options that we selected for each tool that we tested. As you see we have DC three DD, FTK, Guy manager, part two Falcons, our two paladins, TD two, ditto, and X ways. We varied selection of testing as different labs might very their choices for things to test.

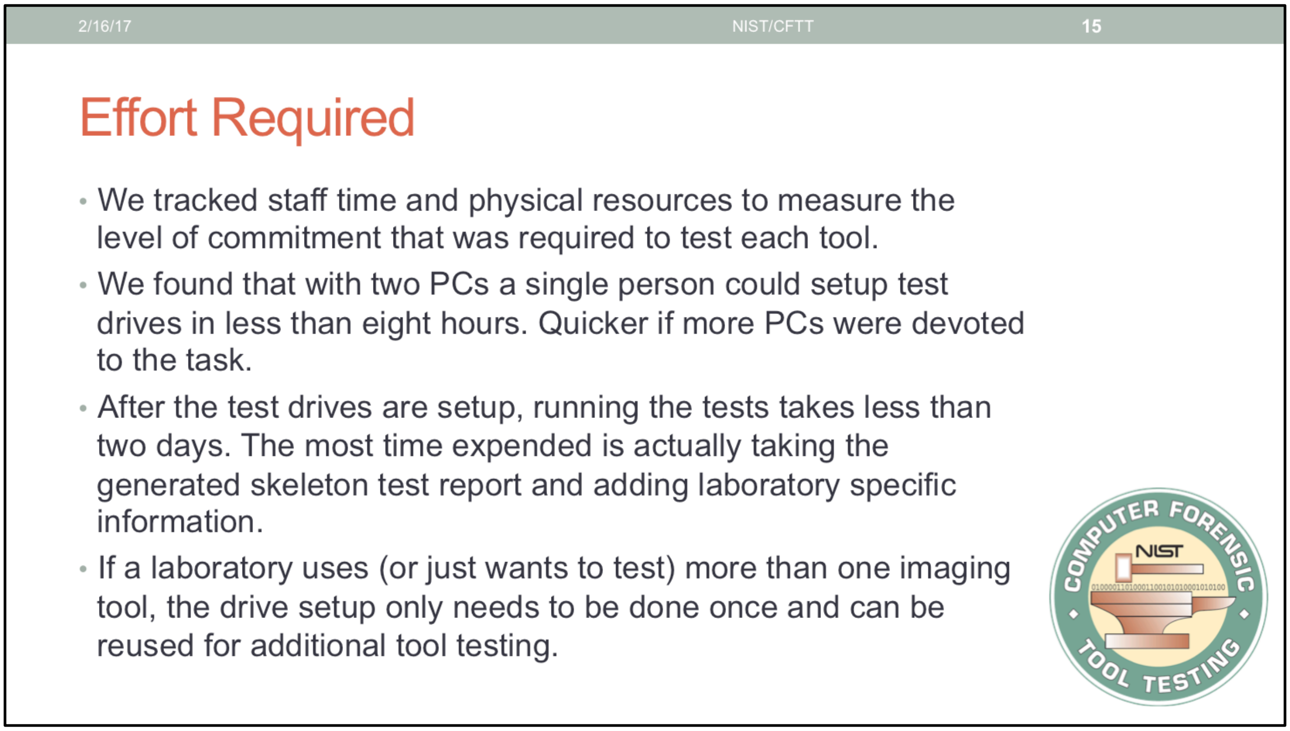


2/16/17 NIST/CFTT 14

# Test Results

- For all tools tested . . .
  - All data acquired (nothing omitted)
  - All acquired data is accurate (nothing changed)
- For "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

All the tools acquired the basic image completely and accurately. The places where we saw different behaviors was in imaging hard drives with bad sectors. Paladin 6.09 may have missed a few readable sectors, but compared to the entire drive this is really a tiny fraction that was missed. This is not necessarily a wrong answer. Tool designers have to choose between completeness and reasonable performance. On spinning drives if you have a bad sector and try to read the sectors near it this will often give you a large performance penalty and greatly extend the time to acquire the entire drive. To mitigate this a tool may offer you a choice in skipping good sectors around in the area of bad sectors to avoid the performance penalty.

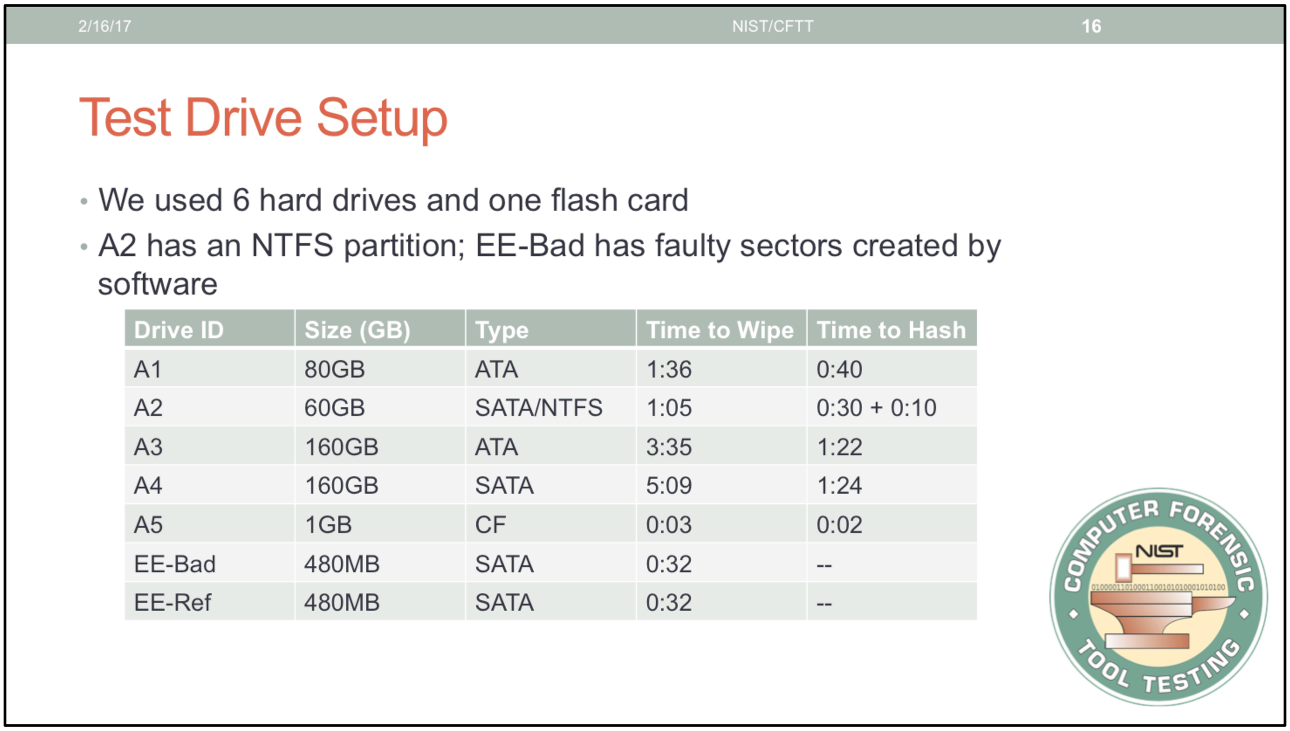


## Effort Required

- We tracked staff time and physical resources to measure the level of commitment that was required to test each tool.
- We found that with two PCs a single person could setup test drives in less than eight hours. Quicker if more PCs were devoted to the task.
- After the test drives are setup, running the tests takes less than two days. The most time expended is actually taking the generated skeleton test report and adding laboratory specific information.
- If a laboratory uses (or just wants to test) more than one imaging tool, the drive setup only needs to be done once and can be reused for additional tool testing.

The bottom line is if you follow Federated testing to test your tool you'll probably get done faster and have results that you can compare with someone else who has also used federated testing. You do not need to design a test protocol, write any software or develop or document test data.  We have done that for you. Just follow the plan that comes with federated testing.

Need to say that they were also able to do other tasks during drive setup.

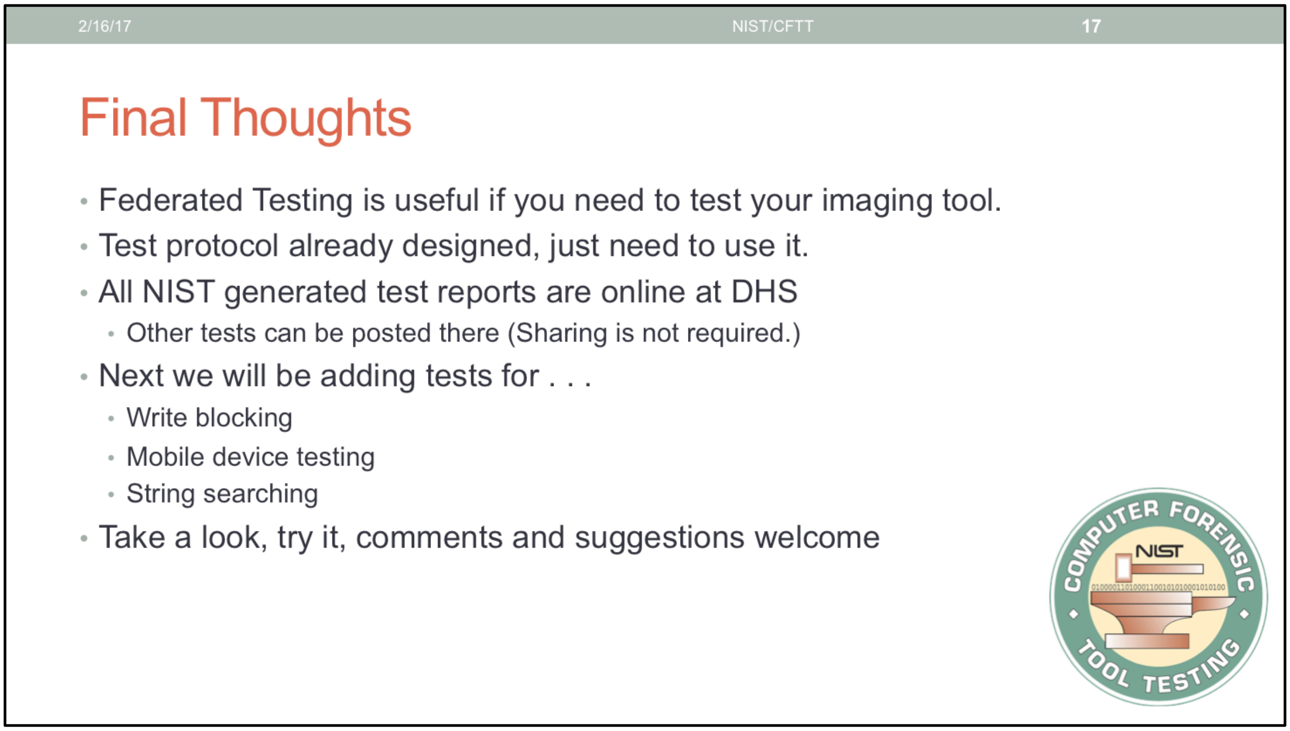


# Test Drive Setup

- We used 6 hard drives and one flash card
- A2 has an NTFS partition; EE-Bad has faulty sectors created by software

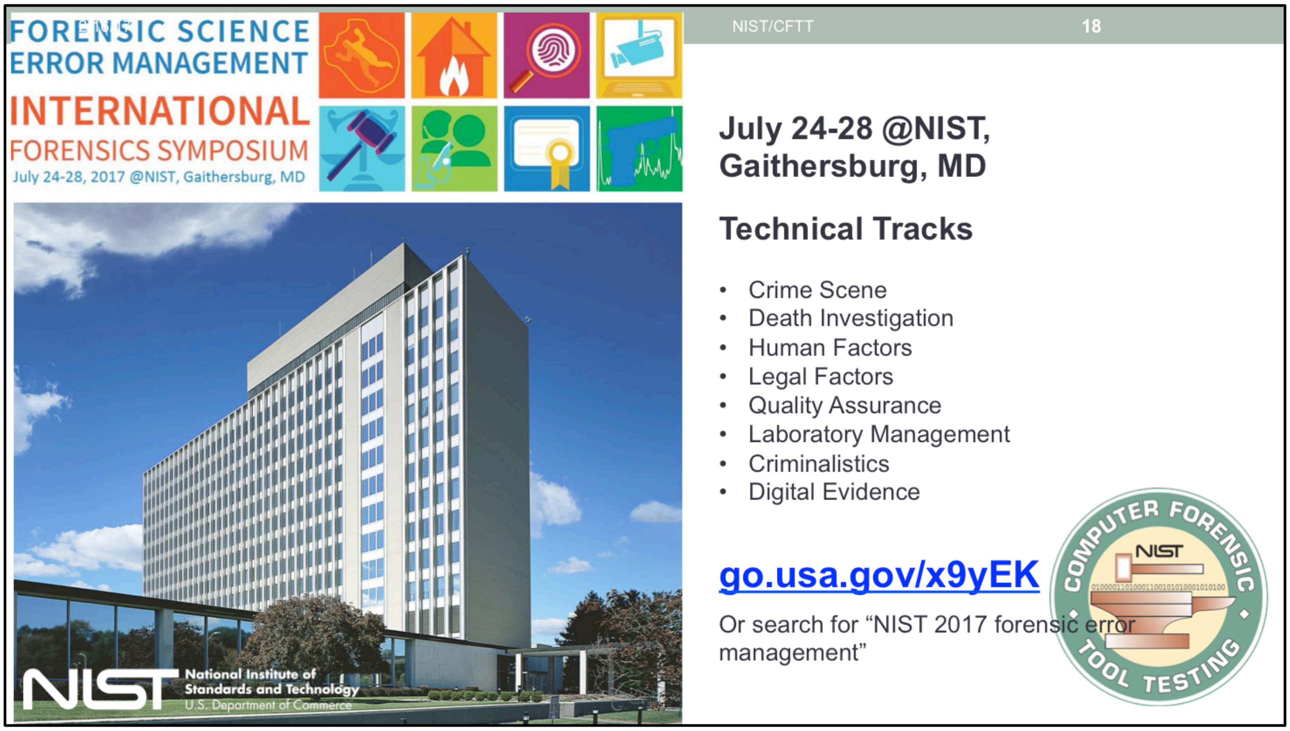
| Drive ID | Size (GB) | Type | Time to Wipe | Time to Hash |
|---|---|---|---|---|
| A1 | 80GB | ATA | 1:36 | 0:40 |
| A2 | 60GB | SATA/NTFS | 1:05 | 0:30 + 0:10 |
| A3 | 160GB | ATA | 3:35 | 1:22 |
| A4 | 160GB | SATA | 5:09 | 1:24 |
| A5 | 1GB | CF | 0:03 | 0:02 |
| EE-Bad | 480MB | SATA | 0:32 |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

As part of the test each drive has to be scanned three times. First you wipe it, Then you hash it, last you image it with the tool here testing. If you're testing more than one tool you can set up your test drives one time and use them in all your tool test. These are the times to wipe and to hash obtained from log files. Drive A2 also has an NTFS partition so 30 minutes to hash the drive 10 minutes to hash the partition. EE bad and EE ref are for the bad sector test. We created a DCO such that those two drives appear to be 480 MB in size. It makes the test go really fast.



# Final Thoughts

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


FORENSIC SCIENCE
ERROR MANAGEMENT
INTERNATIONAL
FORENSICS SYMPOSIUM
July 24-28, 2017 @NIST, Gaithersburg, MD
NIST National Institute of Standards and Technology U.S. Department of Commerce
COMPUTER FORENSIC • TOOL TESTING •
NIST

NIST/CFTT 18

## July 24-28 @NIST, Gaithersburg, MD

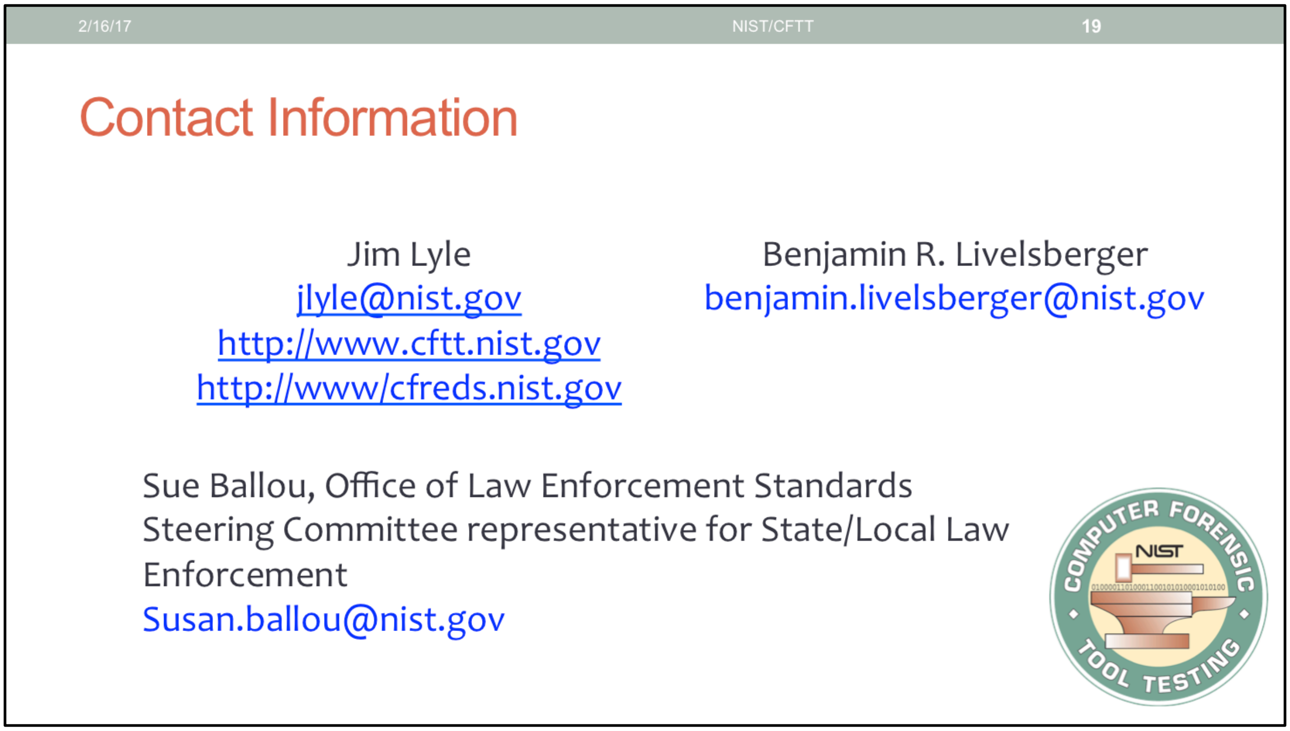
## Technical Tracks

- 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"

Don't forget



# Contact Information

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

Benjamin R. Livelsberger
benjamin.livelsberger@nist.gov

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