

Validating Mobile Forensics Tools in Your Lab with NIST's Federated Testing

NIST
Jenise Reyes-Rodriguez

AAFS – February 22nd, 2018
Seattle, Washington



Computer Forensic Tool Testing (CFTT) Background

- Established in year 2000
- Law enforcement + NIST = CFTT to support digital evidence
- Develops:
 - Specifications, Test Methods and Materials, Produce Test Reports
- Validate tools used in computer-based crime investigations
- Support admissibility in court – share reports
- Driven by a Steering Committee – federal, state & local law enforcement

Benefits of Testing

- Tool creators improve their tools
- Users make informed choices
- Reduces challenges to admissibility of digital evidence
- Supports validation of tools for accreditation and quality management

Challenges

- Hard to test all the tools that are being used in digital labs
- For each tool there are multiple versions
- Tool testing is expensive – time and resources
- Duplication of effort at labs
 - Different test methodologies
 - Different report formats

Approach

- NIST's Federated Testing!
 - Shared test material from NIST
 - Common test methodology
 - Common test report format
 - Common test data sets
 - Reports can be shared

NIST's Federated Testing

- What is it?
 - Expansion of CFTT - provides forensic community with:
 - test suites for validating digital forensics tools
 - support shared test reports - optional
- Goals
 - Make it easy for forensic labs to validate the digital tools that they are using
 - Support sharing of test reports within the community

NIST's Federated Testing – How it works

- Download Federated Testing - <https://www.cftt.nist.gov/federated-testing.html>
 - live Linux CD .iso file
 - Virtual Machine
 - Bootable flash drive can also be created
- Boot to Federated Testing
- Follow testing instructions
- Share test reports

NIST's Federated Testing – Test Suites

- Disk Imaging
- Hardware Write Block
- Mobile Devices

NIST's Federated Testing Home Page



The screenshot shows a Mozilla Firefox browser window displaying the NIST Federated Testing Home Page. The browser's address bar shows the URL `localhost/Federated_Testing_Home_Page.php`. The page features a header with the NIST logo and the text "Federated Testing". Below the header is a navigation menu with "Home", "About", and "Contacts" links. The main content area is titled "Home" and includes a "Welcome to the CFTT Federated Testing Forensic Tool Testing Environment" section. This section contains a paragraph explaining the purpose of the environment and a list of two instructions: "To get started, select the type of tool you want to test from the menu on the left." and "If you need help or have questions email cftt@nist.gov". On the left side of the page, there is a vertical menu titled "Select the type of tool you want to test" with three options: "Test a disk imaging tool", "Test a hardware write block tool", and "Test a mobile device tool". The footer of the page includes the text "The National Institute of Standards and Technology (NIST) is an agency of the U.S. Commerce Department." and "Federated Testinn Version: 3.0".

CFTT Federated Testing CD - Home Page - Mozilla Firefox

localhost/Federated_Testing_Home_Page.php

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

Home About Contacts

Home

Select the type of tool you want to test

- Test a *disk imaging* tool
- Test a *hardware write block* tool
- Test a *mobile device* tool

Welcome to the CFTT Federated Testing Forensic Tool Testing Environment

Welcome to the Federated Testing Forensic Tool Testing Environment produced by the Computer Forensics Tool Testing (CFTT) project at the National Institute of Standards and Technology. The purpose of this environment is to allow forensic labs to test their forensic tools with the same rigor as CFTT (see www.cftt.nist.gov) and to generate sharable test reports with the test results.

- To get started, select the type of tool you want to test from the menu on the left.
- If you need help or have questions email cftt@nist.gov.

The National Institute of Standards and Technology (NIST) is an agency of the U.S. Commerce Department.
[Home](#) / [About](#) / [Contacts](#)

Federated Testinn Version: 3.0
localhost/Federated_Testing_Home_Page.php

Mobile Device Module Home Page

The screenshot shows a web browser window with the URL `localhost/mobiledevice/mdt.php`. The page title is "Federated Testing" and it features the NIST logo (National Institute of Standards and Technology, U.S. Department of Commerce). A navigation menu includes "Home", "About", and "Contacts".

On the left side, there is a vertical menu titled "Select a Mobile Device Testing Task". The "Mobile Device" option is highlighted with a red box. Other options include "Format Your Log Drive 'FT-LOGS'", "Enter Tool Name and Version", "Create/Edit Mobile Device List", "Record Device Setup", "Mobile Tool Testing", "Record Device Test Results", "Generate a Test Report", "Share Your Results", and "Mobile Definitions".

The main content area is titled "Mobile Device Testing Home" and includes a welcome message: "Welcome to Federated Testing for Mobile Devices. The following steps will guide you in testing a mobile forensics data extraction tool. Use the selections from the left hand menu at any time to navigate to different parts of the testing process or to return to this page. Testing has two parts: 1) populating & documenting test devices using the Quick Start Guide (steps 2-3) and 2) setting up, running & documenting tests (steps 4-9)."

The steps listed are:

1. Use the ['Format Your Log Drive FT-LOGS'](#) page to prepare a flash drive for storing test logs.
2. Select a set of mobile devices (e.g., phones, tablets, SIM/UICCs) for use in testing. It is recommended you select devices that are similar to what you see in case work. Note: these can be used devices.
3. Populate and/or document the selected devices.
 - ⚠ **IMPORTANT:** Make sure that your log drive is mounted. You can mount your log drive by clicking on its icon in the launch bar.
 - Click the 'Write Quick Start Guide to Log Drive' button to write the `QuickStartGuideForPopulatingTestDevices_v1.docx` document to your log drive.
4. Describe the tool being tested using the ['Enter Tool Name and Version'](#) page.
5. Use ['Create/Edit Mobile Device List'](#) to record the devices.
6. For each device, use the ['Record Device Setup'](#) pages to document the device's contents.
7. Select ['Mobile Tool Testing'](#) and follow the directions to run the needed tests. It is recommended that you record test results after testing each device.
8. For each mobile device record test results using the ['Record Device Test Results'](#) pages.
9. Use the ['Generate a Test Report'](#) page to create a draft test report. It will be saved to the FT-LOGS flash drive.

The "Write Quick Start Guide to Log Drive" button is highlighted with a red box.

Quick Start Guide

LibreOffice Writer

QuickStartGuideForPopulatingTestDevices_v1.docx - LibreOffice Writer

File Edit View Insert Format Table Tools Window Help

Title Calibri 26

Quick Start Guide For Populating Test Devices

Introduction

There are two strategies for populating test devices: 1) populate a new or previously sanitized device or 2) start with a used device and add content if needed. This guide first describes the major data types and how to populate them onto the test device or ascertain what is already there. [Appendix A](#) is a template that should be filled out per device to document the device's content prior to testing. This will serve as the "answer key" for checking if the tool being tested was able to obtain all of the device's contents. [Appendix B](#) is a sample of a correctly filled out template.

This guide will step you through populating and documenting your test devices. This needs to be done per mobile device. You should select data types that are important for your lab. You do not need to include all of the data types. You can also include other data types by adding a section to Appendix A.

Used devices may include numerous data elements (e.g., contact entries, call logs, text messages, pictures, etc.). While a device may contain hundreds of a specific data type (e.g., contact entries), users should concentrate on documenting a non-exhaustive portion of data elements relevant to testing within Appendix A.

The guide is divided into the following sections and appendices describing how to document/populate data for a mobile device and a SIM/UICC:

- Section 1: Document Device Data
- Section 2: Personal Information Management (PIM) Data: Contacts, Calendar & Memos
- Section 3: Stand-alone Data Files
- Section 4: Call Logs
- Section 5: Text Messages
- Section 6: MMS Messages
- Section 7: Location Data
- Section 8: Browser/Email Data
- Section 9: Social Media Data

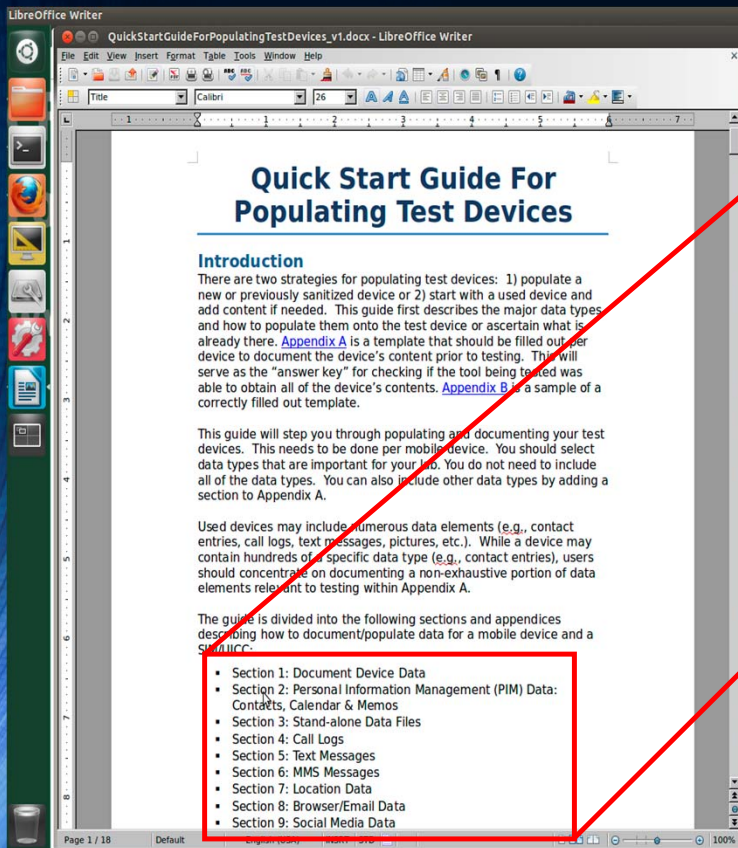
Page 1 / 18 Default English (USA) INSRT STD 100%

NIST
National Institute of Standards and Technology
Department of Commerce

gle

a mobile
e to
ng &
gs.
se can be
g drive by
se it to
ended that
FT-LOGS

Quick Start Guide



Section 1: Document Device Data

**Section 2: Personal Information Management (PIM) Data:
Contacts, Calendar & Memos**

Section 3: Stand-alone Data Files

Section 4: Call Logs

Section 5: Text Messages

Section 6: MMS Messages

Section 7: Location Data

Section 8: Browser/Email Data

Section 9: Social Media Data

Section 10: Other Applications of Interest

Section 11: SIM/UICC Card

[Appendix A](#): Mobile Device Data Documentation - provides users with a blank template to be used to document target mobile devices and/or SIM/UICC data.

[Appendix B](#): Mobile Device Data Example - offers examples of various data types that may be used to populate a target mobile device and/or SIM/UICC.

Record Test Devices

CFTT Federated Testing CD - test a Mobile Device tool - Mozilla Firefox

localhost/mobiledevice/ft_mdt_get_device.php

Home About Contacts

Select a Mobile Device Testing Task

- Mobile Device
- Format Your Log Drive 'FT-LOGS'
- Enter Tool Name and Version
- Create/Edit Mobile Device List**
- Record Device Setup
- Mobile Tool Testing
- Record Device Test Results
- Generate a Test Report
- Share Your Results
- Mobile Definitions

Home > Test a Mobile Device tool > Creating/Editing Mobile Device List

Creating/Editing Mobile Device List

Adding, Updating or Deleting a Mobile Device

Use this page to record your list of test devices. You may add a new device to the list, revise an existing device description, or delete a device.

- Add a new device:** fill out the fields in the form after the 'List of Test Devices' table to describe the device. Then select the 'Add New Device' button to save it to the list.
- As for testing SIM/UICC card acquisition, this is optional. If you want to test SIM/UICC card acquisition, select one or more phones that have a SIM/UICC card.
- Revise an existing device:** revise an existing device description by first selecting the device you want to change from the 'List of Test Devices' table and filling out only the description fields that you want to change. If you leave a field blank then the current value of the field is unchanged, however, the OS, Network and SIM/UICC fields have default values and must always be set to the value you want. Click the 'Update Selected Device' button to apply the changes.
- Delete a device:** first select the device you want to remove from the 'List of Test Devices' table then click the 'Delete Selected Device' button to remove it.

List of Test Devices

Select	Make	Model	OS	Version	Firmware	Network	SIM/UICC
<input type="radio"/>	Google	Pixel 2	Android	8.1	abcdefg	CDMA	SIM/UICC
<input type="radio"/>	Apple	iPhone X	iOS	11.1	hijklmnop	CDMA	No SIM/UICC

Describe a new device or edit an existing device:

Enter the device manufacturer:

Enter the device model and model number:

Select the device OS:

Enter the device OS Version:

Enter the device firmware:

Select the device network:

Test SIM/UICC card acquisition with this phone

No test of SIM/UICC card acquisition test

Describe Device Setup

CFTT Federated Testing CD - test a Mobile Device tool - Mozilla Firefox

localhost/mobiledevice/ft_mdt_record_setup.php

Home About Contacts

Select a Mobile Device Testing Task

- Mobile Device
- Format Your Log Drive 'FT-LOGS'
- Enter Tool Name and Version
- Create/Edit Mobile Device List
- Record Device Setup**
- Module your testing
- Record Device Test Results
- Generate a Test Report
- Share Your Results
- Mobile Definitions

Home > Test a Mobile Device tool > Recording Device Setup

Recording Device Setup (2 of 3)

Documenting Device Setup

Use this page to select and document the data types for the selected test device. For the selected device, for each data type in the 'Documenting Device Setup' and 'Documenting SIM/UICC Setup' tables select either 'Populated' or 'Omitted.' By default the status for each data type is set to 'Populated.' Once you're finished, click the 'Update Setup for Selected Device' button to save the setup to your log drive.

Selected Device:
Manufacturer: Google
Model: Pixel 2

Documenting Device Setup

Data Type	Setup
PIM Data: Contacts/Address Book Entries	Regular Length <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Maximum Length <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Special Character <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Blank Name <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Regular Length, email <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Regular Length, graphic <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Regular Length, Address <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Non-Latin Entry <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Contact Groups <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Deleted Entry <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
PIM Data: Calendar data, Memos	Regular Length <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Maximum Length <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Special Character <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Blank Entry <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Deleted Entry <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
Stand-alone data files	Audio <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Graphic <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Video <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Documents <input checked="" type="radio"/> Populated <input type="radio"/> Omitted
	Audio - Deleted <input checked="" type="radio"/> Populated <input type="radio"/> Omitted

Run Tests

Home > Test a Mobile Device tool > Mobile Tool Testing - Test Runs

Mobile Tool Testing - Test Runs

This page describes the procedures to be performed when acquiring a mobile device or SIM/UICC as part of testing a mobile forensics data extraction tool. It is divided into five *Test Runs*, each of which tests various aspects of the tool.

The **Acquire All Test Run** is essential. The remaining test runs are dependent upon the forensic tool's capabilities and your organizational requirements. Test results are recorded in the "[Record Device Test Results](#)" section of Federated Testing.

The table below identifies *Essential* and *Optional* Test Runs.

Fed Testing - Mobile	Acquire All	Connectivity	Case File/Data Protection	Hashing	SIM/UICC Authentication
<i>Essential</i>	x				
<i>Optional</i>		x	x	x	x

1. Acquire All

NOTE: This test run is performed once per mobile device.

- Complete data extraction from the internal memory of the target mobile device using the recommended data cable.
- If acquiring a SIM/UICC, complete data extraction from its internal memory using the recommended card reader.
- This test run shows the tool's ability to extract data from a mobile device and/or a SIM/UICC.

Instructions:

- Refer to the mobile forensic tool documentation on establishing connectivity and data extraction specifics for the mobile device and/or SIM/UICC.
- Initialize the mobile forensic tool to be tested and begin the test run. Use the tool to "acquire all" data from the mobile device and/or SIM/UICC.

Tests Cases

Test Case	Conformance Indicator
Acquire All – required	Successful acquisition and data reporting
Connectivity – optional	Notification of connection disruption
Case File/Data Protection – optional	Notification that the case file has been modified
Hashing – optional	Consistent hash values – back to back acquisitions
UICC PIN/PUK - optional	Input PIN/correct number of remaining attempts

Record Results

CFTT Federated Testing CD - test a Mobile Device tool - Mozilla Firefox

localhost/mobiledevice/ft_mdt_record_results.php

Home About Contacts

Select a Mobile Device Testing Task

- Mobile Device
- Format Your Log Drive 'FT-LOGS'
- Enter Tool Name and Version
- Create/Edit Mobile Device List
- Record Device Setup
- Mobile Tool Testing
- Record Device Test Results
- Generate a Test Report
- Share Your Results
- Mobile Definitions

Home > Test a Mobile Device tool > Recording Device Test Results

Recording Device Test Results (2 of 3)

Documenting Device Test Results

Use this page to document the results of acquiring the selected test device. For the selected device, for each entry in the 'Documenting Device Test Results' and 'Documenting SIM/UICC Test Results' tables select 'As Expected', 'Partial', 'Not as Expected' or 'N/A.' You may enter testing notes in the text box provided for each entry and/or in the 'General Comments and Observations' box at the bottom of this page. Once you're finished, click the 'Update Results for Selected Device' button to save the results to your log drive.

Selected Device:
 Manufacturer: Google
 Model: Pixel 2

Results Key

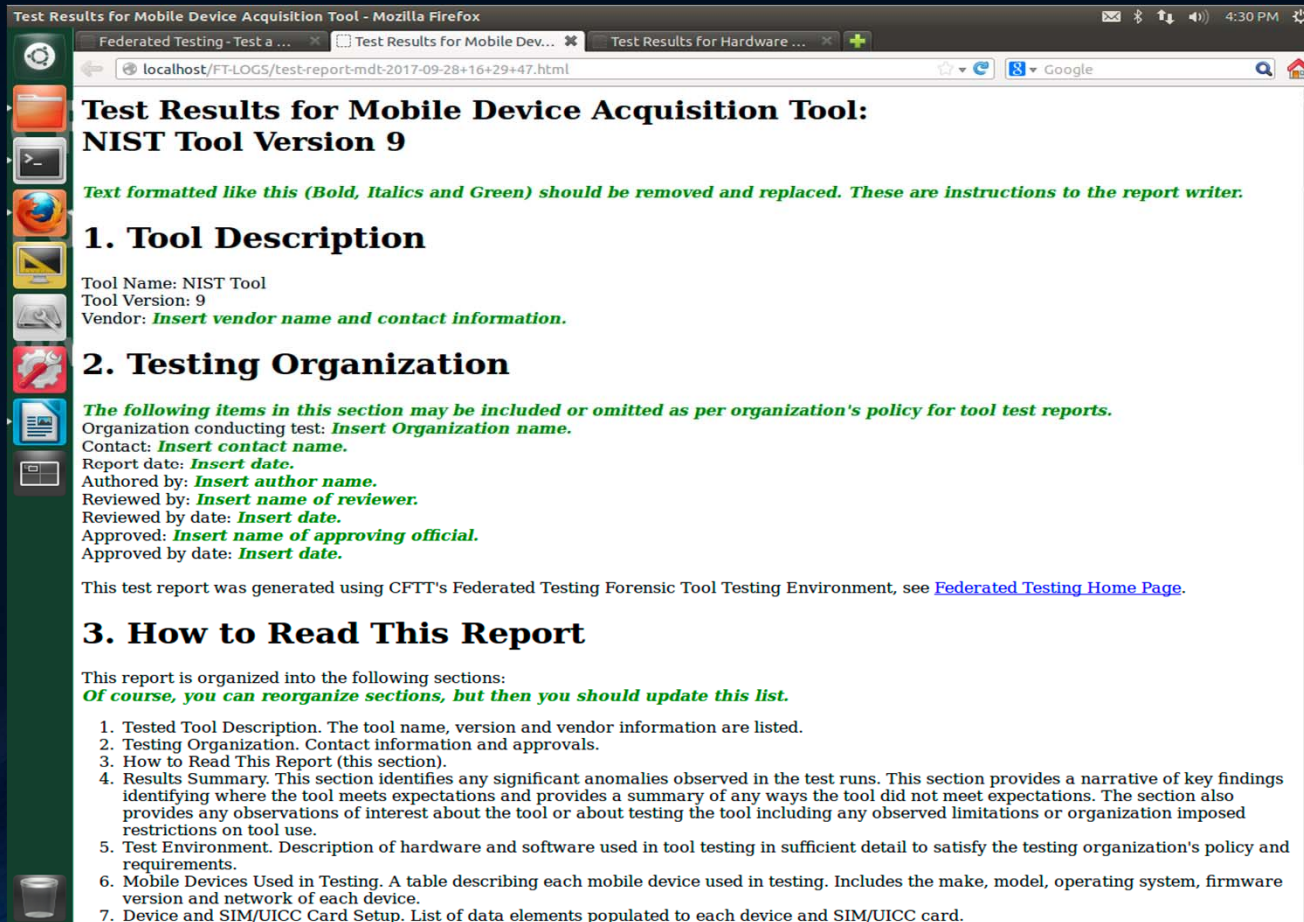
Result	Definition
As Expected	The mobile forensic application returned expected test results – the tool acquired and reported data from the mobile device or SIM/UICC successfully.
Partial	The mobile forensic application returned some of data from the mobile device or SIM/UICC.
Not as Expected	The mobile forensic application failed to return expected test results – the tool did not acquire or report supported data from the mobile device or SIM/UICC successfully.
N/A	Not Applicable – the mobile forensic application is unable to perform the test or the tool does not provide support for the acquisition for a particular data element.

Device Test Results

Documenting Device Test Results

Entry	Result
Acquisition	Acquire All <input checked="" type="radio"/> As Expected <input type="radio"/> Partial <input type="radio"/> Not as Expected <input type="radio"/> N/A
	Disrupted <input checked="" type="radio"/> As Expected <input type="radio"/> Partial <input type="radio"/> Not as Expected <input type="radio"/> N/A
	Notes: <input type="text" value="This tool is great!"/>
Reporting	Preview-Pane <input type="radio"/> As Expected <input checked="" type="radio"/> Partial <input type="radio"/> Not as Expected <input type="radio"/> N/A
	Generated Reports <input type="radio"/> As Expected <input type="radio"/> Partial <input checked="" type="radio"/> Not as Expected <input type="radio"/> N/A

Sample Test Report



Test Results for Mobile Device Acquisition Tool - Mozilla Firefox

Federated Testing - Test a ... Test Results for Mobile Dev... Test Results for Hardware ...

localhost/FT-LOGS/test-report-mdt-2017-09-28+16+29+47.html

Test Results for Mobile Device Acquisition Tool: NIST Tool Version 9

Text formatted like this (Bold, Italics and Green) should be removed and replaced. These are instructions to the report writer.

1. Tool Description

Tool Name: NIST Tool
Tool Version: 9
Vendor: *Insert vendor name and contact information.*

2. Testing Organization

The following items in this section may be included or omitted as per organization's policy for tool test reports.
Organization conducting test: *Insert Organization name.*
Contact: *Insert contact name.*
Report date: *Insert date.*
Authored by: *Insert author name.*
Reviewed by: *Insert name of reviewer.*
Reviewed by date: *Insert date.*
Approved: *Insert name of approving official.*
Approved by date: *Insert date.*

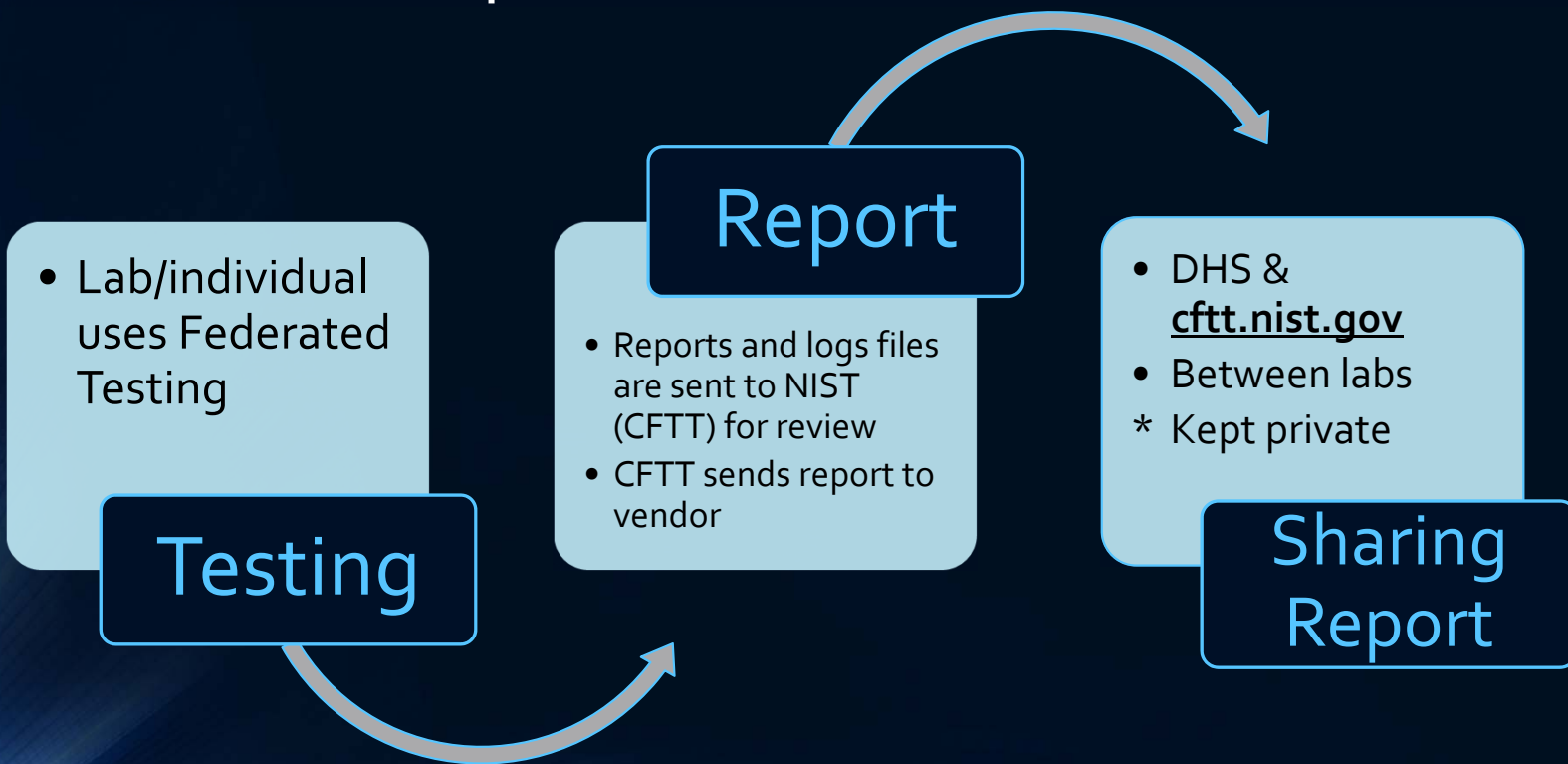
This test report was generated using CFTT's Federated Testing Forensic Tool Testing Environment, see [Federated Testing Home Page](#).

3. How to Read This Report

This report is organized into the following sections:
Of course, you can reorganize sections, but then you should update this list.

1. Tested Tool Description. The tool name, version and vendor information are listed.
2. Testing Organization. Contact information and approvals.
3. How to Read This Report (this section).
4. Results Summary. This section identifies any significant anomalies observed in the test runs. This section provides a narrative of key findings identifying where the tool meets expectations and provides a summary of any ways the tool did not meet expectations. The section also provides any observations of interest about the tool or about testing the tool including any observed limitations or organization imposed restrictions on tool use.
5. Test Environment. Description of hardware and software used in tool testing in sufficient detail to satisfy the testing organization's policy and requirements.
6. Mobile Devices Used in Testing. A table describing each mobile device used in testing. Includes the make, model, operating system, firmware version and network of each device.
7. Device and SIM/UICC Card Setup. List of data elements populated to each device and SIM/UICC card.

Share Test Reports Workflow



Advantages

- More tools validated
- Shared test reports
- Cost savings
- Faster testing

Results

- Test Reports shared with NIST:
 - 1 mobile device tool
 - 5 disk imaging tool
 - Around 800 downloads last year
- Missouri State Public Defender
& Korea University

Next Steps

- Add the following modules/test suites:
 - String Searching
 - Forensic Media Preparation (Disk Wiping)

Use Federated Testing!

- Visit <https://www.cftt.nist.gov/federated-testing.html> to:
 - Learn more
 - Download
 - Subscribe to email updates

CONTACTS

Jenise Reyes-Rodriguez

jenise.reyes@nist.gov

Ben Livelsberger

Benjamin.Livelsberger@nist.gov

James Lyle

james.lyle@nist.gov

Barbara Guttman

Barbara.Guttman@nist.gov