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
Mobile Device Module Home Page

Welcome to Federated Testing for Mobile Devices. The following steps will guide you in testing a mobile forensic 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 2-9) and 2) setting up, running & documenting tests (steps 4-9).

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, SIMUCCs) 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 document the selected devices.
   a. IMPORTANT: Make sure that your log drive is mounted. You can mount your log drive by clicking on its icon in the launch bar.
   b. Click the "Write Quick Start Guide to Log Drive" button to write the QuickStartGuideForPopulatingTestDevices_v1.docx document to your log drive.
   c. Open QuickStartGuideForPopulatingTestDevices_v1.docx from your log drive and use it to populate and document the selected devices.
4. Describe the tool being tested using the "Enter Tool Name and Version" page.
5. Use "Create/Write 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 test result use 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.
Quick Start Guide

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 3 / 18

LibreOffice Writer
QuickStartGuideForPopulatingTestDevices v1.docx - LibreOffice Writer

NIST
National Institute of Standards and Technology
Department of Commerce
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

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**

<table>
<thead>
<tr>
<th>Select</th>
<th>Make</th>
<th>Model</th>
<th>OS</th>
<th>Version</th>
<th>Firmware</th>
<th>Network</th>
<th>SIM/UICC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Google</td>
<td>Pixel 2</td>
<td>Android</td>
<td>8.1</td>
<td>abcdefg</td>
<td>CDMA</td>
<td>SIM/UICC</td>
</tr>
<tr>
<td>2</td>
<td>Apple</td>
<td>iPhone X</td>
<td>iOS</td>
<td>11.1</td>
<td>highfreq</td>
<td>CDMA</td>
<td>No SIM/UICC</td>
</tr>
</tbody>
</table>

**Describe a new device or edit an existing device:**

- Enter the device manufacturer:
- Enter the device model and model number:
- Select the device OS: iOS
- Enter the device OS Version:
- Enter the device firmware:
- Select the device network: CDMA

- Test SIM/UICC card acquisition with this phone
- No test of SIM/UICC card acquisition test
Describe 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/ACC Setup' tables select either 'Populated' or 'Omitted.' By default the status for each data type is set to 'Populated.' Once you've 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**

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Setup</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PIM Data: Contacts/Address Book Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular Length</td>
</tr>
<tr>
<td>Maximum Length</td>
</tr>
<tr>
<td>Special Character</td>
</tr>
<tr>
<td>Blank Name</td>
</tr>
<tr>
<td>Regular Length, email</td>
</tr>
<tr>
<td>Regular Length, graphic</td>
</tr>
<tr>
<td>Regular Length, Address</td>
</tr>
<tr>
<td>Non-Latin Entry</td>
</tr>
<tr>
<td>Contact Groups</td>
</tr>
<tr>
<td>Deleted Entry</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PIM Data: Calendar, Memo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular Length</td>
</tr>
<tr>
<td>Maximum Length</td>
</tr>
<tr>
<td>Special Character</td>
</tr>
<tr>
<td>Black Entry</td>
</tr>
<tr>
<td>Deleted Entry</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stand-alone data files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio</td>
</tr>
<tr>
<td>Graphic</td>
</tr>
<tr>
<td>Video</td>
</tr>
<tr>
<td>Documents</td>
</tr>
<tr>
<td>Audio - Docked</td>
</tr>
<tr>
<td>Graphics - Deleted</td>
</tr>
</tbody>
</table>
Run Tests

Mobile Tool Testing - Test Runs

This page describes the procedures to be performed when acquiring a mobile device or SIMUICC 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.

<table>
<thead>
<tr>
<th>Essential and Optional Test Runs</th>
<th>Mobile Forensics Tool</th>
<th>SIMUICC Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquire All</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

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 SIMUICC, 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 SIMUICC.

Instructions:

1. Refer to the mobile forensic tool documentation on establishing connectivity and data extraction specifics for the mobile device and/or SIMUICC.
2. 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 SIMUICC.
## Tests Cases

<table>
<thead>
<tr>
<th>Test Case</th>
<th>Conformance Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquire All – required</td>
<td>Successful acquisition and data reporting</td>
</tr>
<tr>
<td>Connectivity – optional</td>
<td>Notification of connection disruption</td>
</tr>
<tr>
<td>Case File/Data Protection – optional</td>
<td>Notification that the case file has been modified</td>
</tr>
<tr>
<td>Hashing – optional</td>
<td>Consistent hash values – back to back acquisitions</td>
</tr>
<tr>
<td>UICC PIN/PUK - optional</td>
<td>Input PIN/correct number of remaining attempts</td>
</tr>
</tbody>
</table>
Record Results
Sample Test Report

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

Text formatted like this (Bold, Italic 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

- Lab/individual uses Federated Testing

- Testing

- Reports
  - Reports and logs files are sent to NIST (CFTT) for review
  - CFTT sends report to vendor

- Report

- Sharing Report
  - DHS & cftt.nist.gov
  - Between labs
  - * Kept private
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
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](https://www.cftt.nist.gov/federated-testing.html)
  - 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