Mobile Device Forensics - Tool Testing

Richard Ayers

Disclaimer

Certain commercial entities, equipment, or materials may be identified in this presentation in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

NIST
National Institute of
Standards and Technology

Agenda

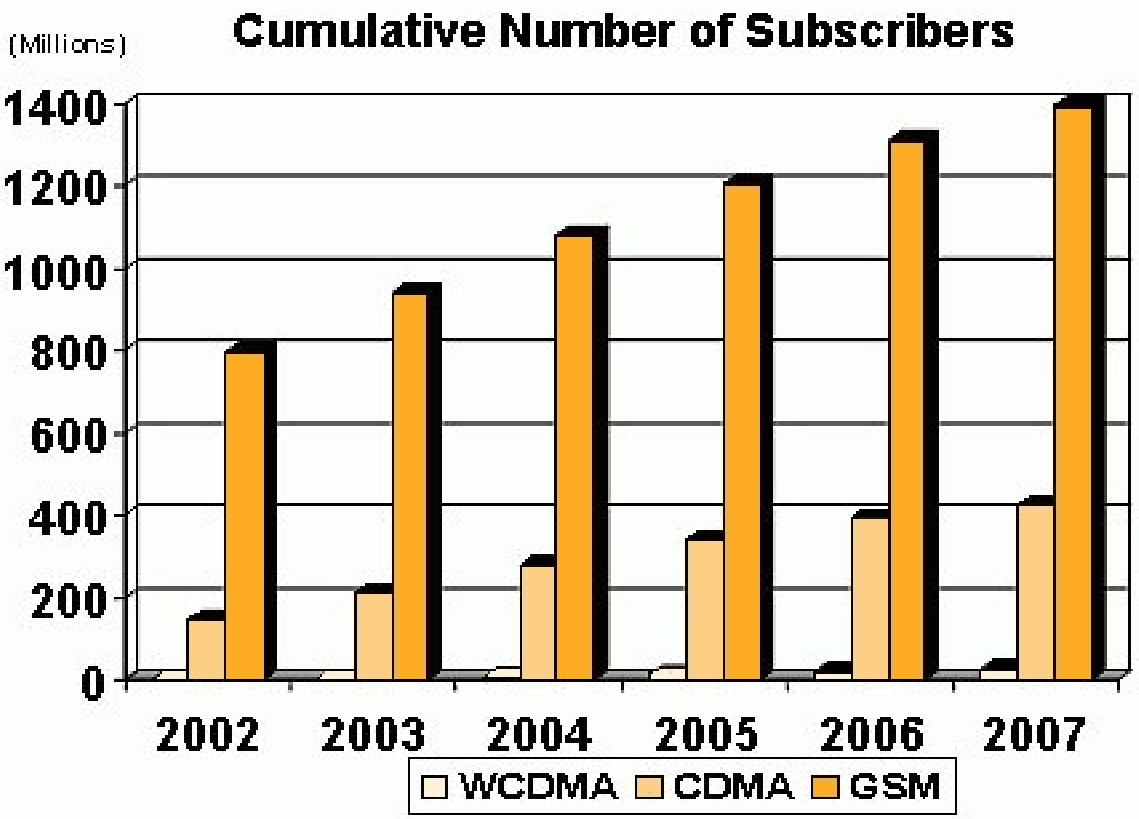
- Introduction
- Motivation
- CFTT Tool Validation
- CFTT Testing Methodology
- Test Findings
- Conclusions

Introduction

- Mobile devices are an evolving form of computing, used widely for personal and organizational purposes
- These compact devices are useful in managing information, such as contact details and appointments, and corresponding electronically
- Over time, they accumulate a sizeable amount of information about the owner
- When involved in crimes or other incidents, proper tools and techniques are needed to recover evidence from such devices and their associated media

Motivation

- AT&T rolled out the first cellular network in 1977 for 2,000 people in Chicago, with phones the size and weight of a brick
- Approximately 2 billion mobile phones are in the world today – 2 times the number of personal computers
- 1.1 billion handsets were sold in 2007
- Gartner estimates that about 1.9 trillion text messages were sent in 2007 and 2008 predictions reach the 2.3 trillion mark.



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 by CFTT staff. 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: NIJ, OLES, FBI, DoD, Secret Service and other agencies.

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**

Developing Test Specifications

- **Specification development process:**
  - **NIST and law enforcement staff develops requirements, assertions and test case documents (called the tool category specification).**
  - **Initial documents are posted on the CFTT site for peer review by members of the computer forensics community and for public comment by other interested parties.**
  - **Relevant comments and feedback are incorporated into the specification.**

CFTT Testing Process - Overview

- **After the specification has been written and a tool selected, the test process is as follows:**
  - **NIST acquires the tool to be tested.**
  - **NIST reviews the tool documentation.**
  - **NIST selects relevant test cases depending on features supported by the tool.**
  - **NIST develops test strategy.**
  - **NIST executes tests**
  - **NIST produces test report.**
  - **Steering Committee reviews test report.**
  - **Vendor reviews test report.**
  - **NIJ posts test report to web.**

CFTT Methodology

- Test Specification - Requirements
- Test Plan – Test Cases and Assertions
- Setup and Test Procedures
- Software / Scripts
- Final Test Results

Requirements

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

Core Requirements - Examples

Internal Memory

- Device Recognition
  - Cable, Bluetooth, IrDA
- Non-Supported Devices
  - Error message
- Connectivity Errors
- Report Generation
  - GUI, Report
- Logical Acquisition
  - Tool supported data objects

SIM

- Media Recognition
  - PC/SC, proprietary reader
- Non-Supported SIMs
  - Error message
- Connectivity Errors
- PIN
- Report Generation
  - GUI, Report
- Logical Acquisition
  - Tool supported data objects

Optional Requirements - Examples

Internal Memory / SIM Acquisition

- Data Presentation
  - GUI, Report
- Case Data Protection
- Physical Acquisition
- Access Card Creation
- Log File Generation
- Foreign Language
- Remaining Number of PIN/PUK attempts
- Stand-alone Acquisition
- Hashing
  - Overall Case File, Individual Acquired Files

Test Plan

- **Test Cases – Derived from requirements, describe the combination of test parameters required to test each assertion.**
  - **Core**
  - **Optional**
- **Assertions – General statements or conditions that can be checked after a test is executed.**
  - **Core**
  - **Optional**

Requirements -> Test Case: Example

- **<u>Requirement</u>:**
  - **CFT-IM-05: A cellular forensic tool shall have the ability to logically acquire all application supported data elements present in internal memory without modification.**

- **<u>Derives Test Cases</u>:**
  - **CFT-IM-05: Acquire mobile device internal memory and review reported subscriber and equipment related information.**
  - **CFT-IM-06: Acquire mobile device internal memory and review reported PIM related data.**
  - **CFT-IM-07: …incoming/outgoing call logs…**
  - **CFT-IM-08: …text messsages…**
  - **CFT-IM-09: …MMS messages…**
  - **CFT-IM-10: …stand-alone files (i.e., audio, graphics, video)…**

Test Case -> Assertions: Example

- Test Case:
  - CFT-IM-06: Acquire mobile device internal memory and review reported PIM related data

- => Assertions:
  - A_IM-07: If a cellular forensic tool successfully completes acquisition of the target device then all known address book entries shall be presented in a human-readable format without modification.
  - A_IM-08: …maximum length address book entries…
  - A_IM-09: …special character address book entries…
  - A_IM-10: …blank name address book entries…
  - A_IM-11: …address book entries containing email addresses…
  - A_IM-12: …address book entries containing an associated graphic…
  - A_IM-13: …datebook/calendar entries…
  - A_IM-14: …maximum length datebook/calendar entries…

Setup and Test Procedures

- Objective: Documentation on data population of target media and test procedures providing third parties with information for an independent evaluation of the process or independent replication of posted test results.
- Contents:
  - Software used for data population: application name, package, function
  - Media Setup: Type of media, procedures used to populate and source dataset
  - Test Case Execution Procedure
  - Description and execution procedure of each individual test case
  - Overview of software tested and procedures used

Scripts and Macros

- **Scripts and Macros**
  - **Customized scripts are written providing the ability to:**
    - **Categorize and store collected data from individual test cases per tool**
    - **Document the outcome of individual test cases with precision**
    - **Store data collected from individual test cases in a secure manner**
    - **Format data output**
  - **Customized macros provide:**
    - **Cosmetically consistent output with embedded test results.**

Mobile Forensic - CFTT Documents

- **Mobile Device Imaging Specs**
  - **Requirements:**
    - *GSM Mobile Device and Associated Media Tool Specification*
    - *Non-GSM Mobile Device Tool Specification*
  - **Test Plan:**
    - *GSM Mobile Device and Associated Media Tool Specification and Test Plan*
    - *Non-GSM Mobile Device Tool Specification and Test Plan*
- **Test Setup Documents**
  - **Setup and Test Procedures:**
    - *GSM Mobile Devices and Associated Media Tool Setup and Test Procedures*
- **Test Reports**
  - **Tool Test Reports:** Check URL below for updates…

http://www.cftt.nist.gov/mobile_devices.htm

Mobile Forensic - CFTT

- <u>**Mobile Forensic Application Anomalies**</u>
  - **Tool Type: Applications capable of acquiring data from GSM Devices and Subscriber Identity Modules (SIMs)**
  - **Overview of Results…**
    - **Four Tools**

GSM Formal Testing - Findings

- Proper reporting of ADNs
  - Maximum length
  - ADNs containing special characters i.e. ‘@’
- Unicode support
  - Proper reporting of foreign language address book entries and text messages
- EMS Messages
  - Tools not capturing data past the 160th character
- Proper reporting of MMS attachments
  - Audio
  - Video
  - Images

GSM Formal Testing - Findings

- **PIM data**
  - **Maximum length Notes**
- **Deleted Data Recovery**
  - **Non-overwritten text messages present on the SIM**
- **Data report inconsistencies**
  - **GUI versus generated report**
- **LOCI Data**
  - **Incorrect reporting of the LAI**
    - **MCC**
    - **MNC**
    - **LAC**

CFTT Overview - RECAP

- Steering committee selects a tool to be tested
- Tool Specification (Requirements) is produced and reviewed before finalized
- Test Plan (Test Cases and Assertions) is produced and reviewed before finalized
- Tool Setup and Test Procedures document is produced and checked for consistency during informal testing
- Test cases are executed
- Final Test Report is produced and reviewed by the steering committee, vendor then posted by NIJ.

Conclusions

- Mobile devices continue to evolve in storage capacity, processing power and Internet capabilities
- Market research has shown that mobile devices out number PCs 2-1.
- Manufacturers must evolve forensic applications at a rate that provides examiners with solutions to acquire newly released devices in addition to older devices.
- Therefore, maintaining quality control and validating tool functionality for mobile device forensic applications is paramount for proper data acquisition and reporting.

Sponsor Information

Supporting Organizations

Office of Law Enforcement and Standards (OLES)

National Institute of Justice (NIJ) &

Other Law Enforcement Organizations

Contact:

Susan Ballou

susan.ballou@nist.gov

Thank You!

Contact Information:

Rick Ayers

richard.ayers@nist.gov

- http://www.cftt.nist.gov
- http://www.cftt.nist.gov/mobile_devices.htm
- http://csrc.nist.gov/mobiledevices/projects.html