January 7, 2009

Non-GSM Mobile Device Tool Specification

Version 1.1

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

Abstract

As mobile devices proliferate, incorporating a host of integrated features and capabilities, their use can be seen everywhere in our world today. Mobile communication devices contain a wealth of sensitive and non-sensitive information. In the investigative community their use is not restricted to data recovery alone as in criminal cases, but also civil disputes and proceedings, and their aggregate use in research and criminal incident recreation continues to increase. Due to the exploding rate of growth in the production of new mobile devices appearing on the market each year is reason alone to pay attention to test measurement means and methods. The methods a tool uses to capture, process, and report data must incorporate a broad range of extensive capabilities to meet the demand as a robust data acquisition tool. In general, a forensic examination conducted on a mobile device is only a small subset of the larger field of digital forensics. Consequentially, tools possessing an exhaustive array of capabilities to acquire data from these portable mobile devices are relatively few in number.

This paper defines requirements for mobile device applications capable of acquiring data from mobile devices operating over a Code Division Multiple Access (CDMA) network and test methods used to determine whether a specific tool meets the requirements for producing measurable results.[•] Test requirements are statements used to derive test cases that define expectations of a tool or application. Test cases describe the combination of test parameters required to test each assertion. Test assertions are described as general statements or conditions that can be checked after a test is executed. Each assertion appears in one or more test cases consisting of a test protocol and the expected test results. The test protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results. The associated assertions and test cases are defined in the test plan document entitled: Non-GSM Mobile Device Tool Test Assertions and Test Plan.

Your comments and feedback are welcome; revisions of this document are available for download at: http://www.cftt.nist.gov/mobile_devices.htm.

[•] NIST does not endorse nor recommend products or trade names identified in this paper. All products used in this paper are mentioned for use in research and testing by NIST.

TABLE OF CONTENTS

1. Introduction 1
2. Purpose 1
3. Scope 2
4. Glossary 2
5. Handset Characteristics - Internal Memory 3
6. Digital Evidence 3
7. Test Methodology 4
8. Requirements 4
8.1 Requirements for Core Features 4
8.2 Requirements for Optional Features 5
8.2.1 Presentation 5
8.2.2 Protection 5
8.2.3 Physical Acquisition 5
8.2.4 Log Files 5
8.2.5 Foreign Language 5
8.2.6 Hashing 6

1. Introduction

The need to ensure the reliability of mobile device forensic tools intensifies, as the embedded intelligence and ever-increasing storage capabilities of mobile devices expand. The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing computer forensic software tools. This is accomplished by the development of both specific and common rules that govern tool specifications. We adhere to a disciplined testing procedure, established test criteria, test sets, and test hardware requirements, that result in providing necessary feedback information to toolmakers so they can improve their tool's effectiveness; end users benefit in that they gain vital information making them more informed about choices for acquiring and using computer forensic tools, and lastly, we impart knowledge to interested parties by increasing their understanding of a specific tool's capability. Our approach for testing computer forensic tools is based on established well-recognized international methodologies for conformance testing and quality testing. For more information on mobile device forensic methodology please visit us at: http://www.cftt.nist.gov/.

The Computer Forensic Tool Testing (CFTT) program is a joint project of the National Institute of Justice (NIJ), the research and development organization of the U.S. Department of Justice, and the National Institute of Standards and Technology's (NIST's) Office of Law Enforcement Standards (OLES) and Information Technology Laboratory (ITL). CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense Cyber Crime Center, U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program, U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection, and the U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

The central requirement for a sound forensic examination of digital evidence is that the original evidence must not be modified (i.e., the examination or capture of digital data from a mobile device and associated media must be performed without altering the device or media content). In the event that data acquisition is not possible using current technology to access information without configuration changes to the device (e.g., loading a driver), the procedure must be documented.

2. Purpose

This document defines requirements for mobile device forensic tools used in digital forensics capable of acquiring internal memory from Code Division Multiple Access (CDMA) devices and test methods used to determine whether a specific tool meets the requirements.

The requirements that will be tested are used to derive assertions. The assertions are described as general statements of conditions that can be checked after a test is executed. Each assertion generates one or more test cases consisting of a test protocol and the expected test results. The test protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results.

3. Scope

The scope of this specification is limited to software tools capable of acquiring CDMA devices. The specifications are general and capable of being adapted to other types of mobile device forensic software.

4. Glossary

This glossary provides context in the absence of an official lexicon recognized by the computer forensics community.

Associated data: Multi-media data (i.e., graphic, audio, video) that are attached and delivered via a multi-messaging service (MMS) message.

Acquisition File: A snapshot of data contained within the internal memory of a target device.

Case File: A file generated by a forensic tool that contains the data acquired from a mobile device or associated media and case-related information (e.g., case number, property/evidence number, agency, examiner name, contact information, etc.) provided by the examiner.

CDMA: Code Division Multiple Access describes a communication channel access principle that employs spread-spectrum technology and a special coding scheme.

Cellular phone: A device whose major function is primarily handling incoming/outgoing phone calls with limited task management applications.

CFT: Cellular Forensic Tool.

Electronic Serial Number (ESN): ESNs, which uniquely identified CDMA phones, were issued until 2005. An ESN number consist of a 32-bit alpha-numeric character set that allowed a maximum of 4 billion unique numbers.

Enhanced Message Service (EMS): Text messages over 160 characters or messages that contain either Unicode characters or a 16x16, 32x32 black and white graphic image.

Flash memory: Non-volatile memory that retains data after the power is removed.

GSM: Global System for Mobile communications is an open, digital cellular technology for transmitting mobile voice and data services.

Hashing: The mathematical algorithmic process of creating a numeric fingerprint value that facilitates uniqueness.

Human-readable format: Acquired data (e.g., text, images) that is interpreted by the forensic application and presented in a format without decoding.

IM: Internal Memory.

Logical acquisition: Implies a bit-by-bit copy of logical storage objects (e.g., directories and files) that reside on a logical store (e.g., a file system partition).

Mobile Equipment Identity (MEID): An ID number that is globally unique for CDMA mobile phones, identifying the device to the network and can be used to flag lost or stolen devices.

Mobile Subscriber International Subscriber Directory Number (MSISDN): The MSISDN conveys the telephone number assigned to the subscriber for receiving calls on the phone.

Multimedia Messaging Service (MMS) message: Provides users with the ability to send text messages containing multimedia objects (i.e., graphic, audio, video).

Preview pane: Section of the Graphical User Interface (GUI) that provides a snapshot of the acquired data.

Physical acquisition: A bit-by-bit copy of the data layer.

Personal Information Management (PIM) data: Data that contains personal information such as: calendar entries, to-do lists, memos, reminders, etc.

Short Message Service (SMS): A service used for sending text messages (up to 160 characters) to mobile devices.

Smart phone: A full-featured mobile phone that provides users with personal computer like functionality by incorporating PIM applications, enhanced Internet connectivity and email operating over an Operating System supported by superior processing and high capacity storage.

Stand-alone data: Data object (e.g., graphic, audio, video) that is not associated with or has not been transferred to the device via email or MMS message.

User data: Data populated onto the device using applications provided by the device.

5. Handset Characteristics - Internal Memory

Mobile devices, designed with the primary purpose of placing and receiving calls, maintain data in flash memory. Typically, the first part of flash memory is filled with the operating system and the second part is allocated for user data. Although information is stored in a proprietary format, forensic tools tailored for mobile device acquisition should minimally be able to perform a logical acquisition for supported devices and provide a report of the data present in the internal memory. Tools that possess a low-level understanding of the proprietary data format for a specific device may provide examiners with the ability to perform a physical acquisition and generate reports in a meaningful (i.e., human-readable) format. Currently, the tools capable of performing a physical acquisition on a mobile device are limited.

6. Digital Evidence

The amount and richness of data contained on mobile devices is dependent upon device type (i.e., low-end, high-end) and personal usage. However, there is a core set of data that computer forensic tools can recover that remains somewhat consistent on all devices with cellular capabilities. Tools should have the ability to recover the following data elements stored in the device’s internal handset memory:

- Mobile Equipment Identifier (MEID) / Electronic Serial Number (ESN)
- Personal Information Management (PIM) data – (e.g., Address book, Calendar entries, to-do list, Tasks)

- Call logs – Incoming and outgoing calls
- Text messages (SMS, EMS)
- Multi-media Messages (MMS)/email – and associated data
- File storage – Stand-alone files such as audio, graphic and video

7. Test Methodology

To provide concise test results, the following test methodology will be strictly followed. Each forensic application under evaluation will be installed on a dedicated (i.e., no other forensic applications are installed) host computer operating with the required platform as specified by the application. The internal memory of the source device will be populated with a pre-defined dataset. Data population techniques and procedures are outlined in the Non-GSM Mobile Device Tool Setup and Test Procedures document. Source devices will be stored in a protected state subsequent to initial data population, thus eliminating the possibility of data modification due to network connectivity. Each succeeding test entails recreating the host-testing environment for each specific tool tested.

The following data elements will be used in populating the internal memory of the cellular device: Address book, PIM data, call logs, text messages (SMS, EMS), MMS messages/email with attachments (i.e., audio, graphic, video) and stand-alone data files (i.e., audio, graphic, video).

8. Requirements

The requirements are in two sections: 8.1 and 8.2. Section 8.1 lists requirements (i.e., Cellular Forensic Tool-Internal Memory-01 [CFT-IM-01] through CFT-IM-05) that all acquisition tools shall meet. Section 8.2 lists requirements (i.e., Cellular Forensic Tool-Internal Memory Optional-01 [CFT-IMO-01] though CFT-IMO-08) that the tool shall meet on the condition that specified features or options are offered by the tool.

8.1 Requirements for Core Features

The following requirements are mandatory and shall be met by all mobile device forensic tools capable of acquiring internal handset memory.

Internal Memory Requirements:

CFT-IM-01 A cellular forensic tool shall have the ability to recognize supported devices via the vendor supported interfaces (e.g., cable, Bluetooth, Infrared).

CFT-IM-02 A cellular forensic tool shall have the ability to identify non-supported devices.

CFT-IM-03 A cellular forensic tool shall have the ability to notify the user of connectivity errors between the device and application during acquisition.

CFT-IM-04 A cellular forensic tool shall have the ability to provide the user with either a preview pane or generated report view of data acquired.

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.

8.2 Requirements for Optional Features

The following requirements define optional tool features. If a tool provides the capability defined, the tool is tested for conformance to these requirements. If the tool does not provide the capability defined, the requirement does not apply.

The following optional features are identified:

- Presentation
- Protection
- Physical acquisition
- Log file creation
- Foreign language character support
- Hashing

8.2.1 Presentation

Requirements CFT-IMO-01 and CFT-IMO-02 apply to Optional Presentation of Internal Memory.

CFT-IMO-01 A cellular forensic tool shall have the ability to provide a presentation of acquired data in a human-readable format via a generated report.

CFT-IMO-02 A cellular forensic tool shall have the ability to provide a presentation of acquired data in a human-readable format via a preview pane view.

8.2.2 Protection

Requirement CFT-IMO-03 applies to Optional Protection of Internal Memory.

CFT-IMO-03 A cellular forensic tool shall have the ability to protect the overall case file and individual data elements from modification.

8.2.3 Physical Acquisition

Requirement CFT-IMO-04 applies to Optional Physical Acquisition of Internal Memory.

CFT-IMO-04 A cellular forensic tool shall have the ability to perform a physical acquisition of the supported device's internal memory without modification.

8.2.4 Log Files

Requirement CFT-IMO-05 applies to Optional Log Filing of Internal Memory acquisition.

CFT-IMO-05 A cellular forensic tool shall have the ability to create user-accessible and readable log files outlining the acquisition process.

8.2.5 Foreign Language

Requirement CFT-IMO-06 applies to Optional Foreign Language acquisition from Internal Memory.

CFT-IMO-06 A cellular forensic tool shall have the ability to present data objects containing non-ASCII character sets acquired from the internal memory of the device via the suggested interface (i.e., preview pane, generated report). Non-ASCII characters shall be printed in their native format (e.g., Unicode UTF-8).

8.2.6 Hashing

Requirements CFT-IMO-07 and CFT-IMO-08 apply to Optional Hashing of Internal Memory.

CFT-IMO-07 A cellular forensic tool shall have the ability to provide a hash for individual data elements.

CFT-IMO-08 A cellular forensic tool shall have the ability to provide a hash for the overall case file.