January 6, 2009

GSM Mobile Device and Associated Media Tool Specification

Version 1.2

National Institute of Standards and Technology
Technology Administration, 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 Global System for Mobile communication (GSM) network and test methods used to determine whether a specific tool meets the requirements, and assertions derived from requirements 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: GSM Mobile Device and Associated Media 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

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 Global System for Mobile communication (GSM) devices and related media (i.e., Subscriber Identity Module [SIM]) 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 GSM devices and related media (i.e., SIM). The specifications are general and capable of being adapted to other types of mobile device forensic software.

4. Glossary

This glossary was added to provide context in the absence of official definitions recognized by the computer forensics community.

Access card/Radio isolation card: Subscriber Identity Modules (SIMs) that contain necessary data elements allowing GSM equipment to operate without network connectivity.

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 or associated media (i.e. SIM).

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.

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

CFT: Cellular Forensic Tool.

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

Personal Identification Number (PIN): A numeric code used for preventing unauthorized access to a device generally associated with the SIM. PIN1 is the primary means of access to a handset. PIN2 when activated provides additional security for a small set of features (e.g., resetting call meters, changing fixed dialing numbers).

PIN UnlocK Code (PUK): A required code to unlock a disabled SIM due to three successive incorrect PIN attempts. PUK1 and PUK2 are used to unblock PIN1 and PIN2 respectively.

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

Subscriber Identity Module (SIM): A smart card which contains essential subscriber information and additional data providing network connectivity to mobile equipment operating over a GSM network.

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 (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. SIM Characteristics

Due to the GSM 11.11[1] standard, mobile device forensic tools designed to extract data from a SIM via an external reader should be able to properly acquire, decode, and present data in a human-readable format. An abundance of information is stored on the SIM such as Abbreviated Dialing Numbers (ADNs), Last Numbers Dialed (LND), Short Message Service (SMS) messages, subscriber information (i.e., IMSI), and location information (i.e., Location Information [LOCI], General Packet Radio Service Location [GPRSLOCI]). Tools optionally should provide support for Universal Subscriber Identity Modules (USIMs), the third generation (3G) card which carries out the same functions as its 2G cousin (i.e., SIM).

Optionally, mobile device forensic tools should provide the ability to create an access SIM[2] in the event that the mobile equipment (ME) is found without the SIM present. Devices found without the SIM present may cause difficulty in acquiring the internal memory of the related device. Therefore, the ability to create an access card bypasses this problematic situation and allows for completion of internal memory acquisition.

7. 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. GSM devices provide two areas for data storage: device internal memory and the SIM. Tools should have the ability to recover the following data elements stored in the device's internal handset memory:

- International Mobile Equipment Identifier (IMEI)
- 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

Tools shall have the ability to recover the following data elements stored on the SIM memory:

- Service Provider Name (SPN)
- Integrated Circuit Card Identifier (ICCID)
- International Mobile Subscriber Identity (IMSI)
- Mobile Subscriber International ISDN Number (MSISDN)
- Abbreviated Dialing Numbers (ADNs)
- Last Numbers Dialed (LND)
- Short Message Service (SMS) – text messages under 160 characters

[1] http://www.ttfn.net/techno/smartcards/gsm11-11.pdf

[2] Access cards or radio isolation cards contain necessary fields that allow the ME to function without network connectivity.

- Enhanced Message Service (EMS) – text messages greater than 160 characters
- Location Information (LOCI)
- General Packet Radio Service (GPRS) location – GPRSLOCI

8. Test Methodology

To provide concise test results of tools capabilities, the following test methodology will be strictly followed. The forensic application under evaluation will be installed on a dedicated (i.e., no other forensic applications are installed) host machine operating over the required platform as specified by the application. Two identical GSM devices will function as the source and target devices. The internal memory of the source and target devices will be populated with a pre-defined dataset as will the source and target SIMs. Source, target devices and associated media (i.e., SIM), subsequent to initial data population, will be stored in a protected state eliminating the possibility of data modification due to network connectivity. Each succeeding test entails recreating the host environment for each specific tool tested and re-populating the target device and SIM. During the acquisition process, all data transmissions (sent and received data packets) between the device and application will be captured and logged via a port monitoring utility.

The following data elements will be used for 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., images, audio, video) and stand-alone data files (i.e., audio, graphic, video). The following data elements will be used for populating the SIM: Abbreviated Dialing Numbers (ADNs), Last Numbers Dialed (LND), Short Messaging Service (SMS) messages marked as Read, Unread and Deleted, EMS messages, and location (LOCI) information.

9. Requirements

The requirements are in two sections: 9.1 and 9.2. Section 9.1 lists requirements (i.e., Cellular Forensic Tool-Internal Memory-01 [CFT-IM-01] through CFT-IM-05 and Cellular Forensic Tool-Subscriber Identity Module-01 [CFT-SIM-01] through CFT-SIM-06) that all acquisition tools shall meet. Section 9.2 lists requirements (i.e., Cellular Forensic Tool-Internal Memory Optional-01 [CFT-IMO-01] through CFT-IMO-10 and Cellular Forensic Tool-Subscriber Identity Module Optional-01 [CFT-SIMO-01] through CFT-SIMO-10) that the tool shall meet on the condition that specified features or options are offered by the tool.

9.1 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 and SIM 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.

SIM Requirements:

CFT-SIM-01 A cellular forensic tool shall have the ability to recognize supported SIMs via the vendor supported interface (e.g., PC/SC reader, proprietary reader).

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

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

CFT-SIM-04 A cellular forensic tool shall have the ability to provide the user with the opportunity to unlock a password protected SIM before acquisition.

CFT-SIM-05 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-SIM-06 A cellular forensic tool shall have the ability to acquire all application supported data elements present in the SIM memory without modification.

9.2 Requirements for Optional Features

The following requirements define optional tool features. If a tool provides the capability defined, the tool is tested as if the requirement were mandatory. If the tool does not provide the capability defined, the requirement does not apply.

The following optional features are identified:

- Presentation
- Protection
- Physical acquisition
- Access Card/Radio Isolation Card creation
- Log file creation
- Foreign language character support
- Remaining PIN attempts
- Remaining PUK attempts
- Stand-alone acquisition
- Hashing

9.2.1 Presentation

Requirements CFT-IMO-01 through CFT-IMO-02 apply to Optional Internal Memory Requirements. Requirements CFT-SIMO-01 through CFT-SIMO-02 apply to Optional SIM Requirements.

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.

CFT-SIMO-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-SIMO-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.

9.2.2 Protection

Requirement CFT-IMO-03 applies to Optional Internal Memory Requirements. Requirement CFT-SIMO-03 applies to Optional SIM Requirements.

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

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

9.2.3 Physical Acquisition

Requirement CFT-IMO-04 applies to Optional Internal Memory Requirements. Requirement CFT-SIMO-04 applies to Optional SIM Requirements.

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

CFT-SIMO-04 A cellular forensic tool shall have the ability to perform an acquisition of the data present on supported Subscriber Identity Modules (SIMs) without modification.

9.2.4 Access Card Creation

Requirement CFT-IMO-05 applies to Optional Internal Memory Requirements.

CFT-IMO-05 A cellular forensic tool shall have the ability to create an access card following manufacturer suggested protocols.

9.2.5 Log Files

Requirement CFT-IMO-06 applies to Optional Internal Memory Requirements. Requirement CFT-SIMO-05 applies to Optional SIM Requirements.

CFT-IMO-06 A cellular forensic tool shall have the ability to create user-accessible and readable log files outlining the acquisition process.

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

9.2.6 Foreign Language

Requirement CFT-IMO-07 applies to Optional Internal Memory Requirements. Requirement CFT-SIM-06 applies to Optional SIM Requirements.

CFT-IMO-07 A cellular forensic tool shall have the ability to present data objects containing foreign language 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).

CFT-SIMO-06 A cellular forensic tool shall have the ability to present data objects containing foreign language character sets acquired from the SIM 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).

9.2.7 PIN Attempts

Requirement CFT-SIMO-07 applies to Optional SIM Requirements.

CFT-SIMO-07 A cellular forensic tool shall have the ability to present the remaining number of CHV1/CHV2 PIN unlock attempts.

9.2.8 PUK Attempts

Requirement CFT-SIMO-08 applies to Optional SIM Requirements.

CFT-SIMO-08 A cellular forensic tool shall have the ability to present the remaining number of PUK unlock attempts.

9.2.9 Stand-alone Acquisition

Requirement CFT-IMO-08 applies to Optional Internal Memory Requirements.

CFT-IMO-08 A cellular forensic tool shall have the ability to acquire internal memory data without modifying data present on the SIM.

9.2.10 Hashing

Requirement CFT-IMO-09 through CFT-IMO-10 apply to Optional Internal Memory Requirements. Requirement CFT-SIMO-09 through CFT-SIMO-10 apply to Optional SIM Requirements.

CFT-IMO-09 A cellular forensic tool shall have the ability to provide a hash for individual data elements.

CFT-IMO-10 A cellular forensic tool shall have the ability to provide a hash for the overall case file.

CFT-SIMO-09 A cellular forensic tool shall have the ability to provide a hash for individual data elements.

CFT-SIMO-10 A cellular forensic tool shall have the ability to provide a hash for the overall case file.