July 8, 2014

Mobile Device Tool Specification

Version 1.0

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 specification defines requirements for mobile device applications capable of acquiring data from smart phones, feature phones, tablets, Universal Integrated Circuit Cards (UICCs), 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: Mobile Device Tool Test Assertions and Test Plan.

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

92

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: 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) Law Enforcement Standards Office (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 specification defines requirements for mobile device forensic tools used in digital forensics capable of acquiring internal memory from smart phones, feature phones, tablets and associated media i.e., Universal Integrated Circuit Cards (UICCs).

The mobile device tool requirements are used to derive test assertions. The test 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 the internal memory of smart phones, feature phones, tablets and UICCs. The mobile device tool specification is general and capable of being adapted to other types of mobile device forensic software.

4. Definitions

This glossary was added to provide context in the absence of definitions 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 mobile device (e.g., feature phone, smart phone, tablet) or associated media i.e., UICC.

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 method that employs spread-spectrum technology and a special coding scheme.

CHV: Card Holder Verification is a personal identification number (PIN) that provides access to a Universal Integrated Circuit Card (UICC).

CDMA Subscriber Identity Module (CSIM) – CSIM is an application to support CDMA2000 phones that runs on a UICC, with a file structure derived from the R-UIM card.

Data Objects: Files or directories stored in the internal memory of the device or UICC such as address book entries, Personal Information Management data, call logs, text messages, stand-alone files (e.g., graphic files, audio, video).

Electronic Serial Number (ESN): ESNs were issued until 2005, which uniquely identified CDMA phones. An ESN number consist of a 32-bit alphanumeric string 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 image.

Feature phone: A device whose major function is primarily handling incoming/outgoing phone calls over a wireless network (e.g., GSM, CDMA) with limited task management applications.

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

Global Positioning System (GPS): A navigational system involving satellites and computers that can determine the latitude and longitude of a receiver.

Global System for Mobile Communications (GSM): An open, digital cellular technology for transmitting mobile voice and data services.

Hard reset: The process used to reboot the smart phone returning the device back to the initial factory install state, potentially erasing all user data (e.g., contacts, tasks, calendar entries).

Hashing: The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.

Human-readable format: Acquired data shown in a human language rather than binary data.

IM: Internal Memory. Volatile and non-volatile storage space for user data.

Logical acquisition: Implies a bit-by-bit copy of logical storage objects (e.g., Address book, Personal Information Management data, Call logs, text messages, stand-alone data 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 that identifies the device to the network and can be used to flag lost or stolen devices.

Mobile Subscriber International Subscriber Directory Number (MSISDN): The MSISDN is 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).

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

Physical acquisition: A bit-by-bit acquire of the mobile device internal memory.

PIN: A Personal Identification Number that is 4 to 8 digits in length used to secure mobile devices from unauthorized access.

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

PUK: A Personal Unblocking Key used to regain access to a locked mobile device whose PIN attempts have been exhausted.

Recoverable data objects: Logically deleted data objects that have not been overwritten.

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 accelerated processing and larger storage capacity compared with present cellular phones.

MDT: Mobile Device Tool. A tool capable of acquiring the internal memory from a smart phone, feature phone, tablet or UICC.

Removable User Identity Module (R-UIM) – A card developed for cdmaOne/CDMA2000 handsets that extends the GSM SIM card to CDMA phones and networks.

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.

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

Supported Data Objects: Data objects (e.g., subscriber information, PIM data, text messages, stand-alone data, MMS messages and associated data) that the cellular forensic tool has the ability to acquire according to the cellular forensic tool documentation.

Tablet: A Tablet PC is a laptop PC equipped with a stylus or a touchscreen. This form factor is intended to offer a more mobile PC.

Universal Integrated Circuit Card: An integrated circuit card that securely stores the international mobile subscriber identity (IMSI) and the related cryptographic key used to identify and authenticate subscribers on mobile devices. A UICC may be referred to as a: SIM, USIM, R-UIM or CSIM, and is used interchangeably with those terms.

UMTS Subscriber Identity Module (USIM) – A module similar to the SIM in GSM/GPRS networks, but with additional capabilities suited to 3G networks.

User data: Data populated onto the device using mobile device default applications.

5. Background

5.1 Mobile Device Characteristics – Internal Memory

Mobile devices typically contain one or two different types of non-volatile flash memory. These types are NAND and NOR. NOR flash has slower read/write times and is nearly immune to corruption and bad blocks while allowing random access to any memory location. NAND flash offers higher memory storage capacities, is less stable and only allows sequential access.

Memory configurations among mobile devices have evolved over time. Feature phones were among the first types of devices that contained NOR flash and RAM memory. System and user data are stored in NOR and copied to RAM upon booting for faster code execution and access. This is known as the first generation of mobile memory configurations.
As smartphones were introduced, memory configurations evolved, adding NAND flash memory.

This arrangement of NOR, NAND and RAM memory is referred to as the second generation. This generation of memory configurations stores system files in NOR flash and user files in NAND; RAM is used for code execution. The latest smartphones contain only NAND and RAM memory (i.e., third generation), due to higher transaction speed, greater storage density and lower cost.

Although data present on mobile devices may be 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.

5.2 UICC Characteristics

Due to the GSM 11.11[1] standard, mobile device forensic tools designed to extract data from a UICC either internally or with an external Personal Computer/Smart Card (PC/SC) reader, should be able to properly acquire, decode, and present data in a human-readable format. An abundance of information is stored on UICCs such as Abbreviated Dialing Numbers (ADNs), Last Numbers Dialed (LND), SMS messages, subscriber information (e.g., IMSI), and location information (i.e., Location Information [LOCI], General Packet Radio Service Location [GPRSLOCI]).

5.3 Digital Evidence

The amount and richness of data contained on mobile devices vary based upon the manufacturer and OS. Pre-loaded applications and the ability to install customized applications provide users with endless solutions. However, there is a core set of data that computer forensic tools can recover that remains somewhat consistent across the majority of mobile devices. Tools should have the ability to recover the following data objects stored in the device's internal memory and associated media:

- International Mobile Equipment Identifier (IMEI) – GSM device memory
- Mobile Equipment Identifier (MEID) / Electronic Serial Number (ESN) – CDMA device memory
- Service Provider Name (SPN) – UICC memory
- Integrated Circuit Card Identifier (ICCID) – UICC memory
- International Mobile Subscriber Identity (IMSI) – UICC memory
- Mobile Subscriber International ISDN Number (MSISDN) – UICC memory
- Personal Information Management (PIM) data - (e.g., Address book, Calendar entries, to-do list, Tasks, Memos) – device memory
- Abbreviated Dialing Numbers (ADNs) – UICC memory
- Call logs – Incoming and outgoing calls – device memory
- Last Numbers Dialed (LND) – UICC memory
- Text messages (SMS, EMS) – device memory, UICC memory
- Multi-media Messages (MMS)/email - and associated data (i.e., audio, graphics, video) – device memory
- Application data - (e.g., Word documents, spreadsheet data, presentation data, etc.) – device memory
- File storage - Stand-alone files such as audio, graphic and video – device memory
- Internet data - (e.g., bookmarks, visited sites, cached URLs) – device memory
- Social media related data - (e.g., facebook, twitter, Linkedin, Instagram) – device memory
- GPS related data - Longitude and latitude coordinates – device memory

5.4 Test Methodology

To provide repeatable test results, the following test methodology is strictly followed. Each forensic application under evaluation is 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 and UICC is populated with a known dataset. Source devices

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

are stored in a protected state subsequent to initial data population, thus eliminating the possibility of data modification due to network connectivity.

The following data objects (if supported) are used in populating the internal memory of the mobile devices: address book, PIM data, application data, Internet data, call logs, text messages (SMS, EMS), MMS messages/email with attachments (i.e., audio, graphic, video), stand-alone data files (i.e., audio, graphic, video), social media related data and GPS coordinates.

The following data objects are used for populating the UICC: Abbreviated Dialing Numbers (ADNs), Last Numbers Dialed (LND), Short Messaging Service (SMS) messages – (marked as Read, Unread and Deleted) and EMS messages.

6. Requirements

The mobile device tool requirements are in two sections: 6.1 and 6.2. Section 6.1 lists requirements i.e., Mobile Device Tool-Core Requirement-01, MDT-CR-01 through MDT-CR-04 that all acquisition tools shall meet. Section 6.2 lists requirements i.e., Mobile Device Tool-Requirement Optional-01, MDT-RO-01 through MDT-RO-11 that the tool shall meet on the condition that specified features or options are offered by the tool.

6.1 Requirements for Core Features

All mobile device forensic tools capable of acquiring the internal memory of a mobile device shall meet the following core requirements.

MDT-CR-01 A mobile device forensic tool shall have the ability to recognize supported devices via the vendor-supported interfaces (e.g., cable, Bluetooth, Infrared).

MDT-CR-02 A mobile device forensic tool shall have the ability to notify the user of connectivity errors between the device and application during acquisition.

MDT-CR-03 A mobile device forensic tool shall have the ability to provide the user with either a preview pane or generated report view of data acquired.

MDT-CR-04 A mobile device forensic tool shall have the ability to logically acquire all application supported data objects present in internal memory without modifying the data objects present on the device.

6.2 Requirements for Optional Features

The following mobile device tool 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:

- UICC acquisition
- Data Integrity
- Password-protected UICCs
- PIN/PUK input
- Physical acquisition

- Non-ASCII character support
- Hashing
- GPS Coordinates

6.2.1 UICC Acquisition

MDT-RO-01 A mobile device forensic tool shall have the ability to recognize supported UICCs via the vendor supported interface (e.g., PC/SC reader, proprietary reader, internal).

MDT-RO-02 A mobile device forensic tool shall have the ability to notify the user of connectivity errors between the UICC reader and application during acquisition.

MDT-RO-03 A mobile device forensic tool shall have the ability to acquire all application-supported data objects present in the UICC memory.

6.2.2 Data Integrity

MDT-RO-04 A mobile device forensic tool shall have the ability to protect previously acquired data objects within a saved case file from modification.

6.2.3 Password Protected UICCs

MDT-RO-05 A mobile device forensic tool shall have the ability to provide the user with the ability to unlock a password protected UICC before acquisition.

6.2.4 PIN Attempts

MDT-RO-06 A mobile device forensic tool shall have the ability to present the remaining number of CHV1/CHV2 PIN unlock attempts.

6.2.5 PUK Attempts

MDT-RO-07 A mobile device forensic tool shall have the ability to present the remaining number of PUK unlock attempts.

6.2.6 Physical Acquisition

MDT-RO-08 A mobile device forensic tool shall have the ability to perform a physical acquisition of the device's internal memory for supported devices.

6.2.7 Non-ASCII Characters

MDT-RO-09 A mobile device forensic tool shall have the ability to present data objects containing non-ASCII characters acquired from the internal memory of the mobile device or UICC. Non-ASCII characters shall be printed in their native representation.

6.2.8 Stand-alone Acquisition

SPT-RO-10 A mobile device forensic tool shall have the ability to acquire internal memory data without modifying data present on the UICC.

6.2.9 Hashing

MDT-RO-11 A mobile device forensic tool shall have the ability to compute a hash for individual data objects.

6.2.10 GPS Coordinates

MDT-RO-12 A mobile device forensic tool shall have the ability to acquire GPS related data present in the internal memory.