February 1, 2016

Mobile Device Tool Specification

Version 2.0

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

36

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 feature phones, smart 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 Version 2.0.

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.

66

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: www.cftt.nist.gov.

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security (DHS), the National Institute of Justice (NIJ), and the National Institute of Standards and Technology Special Program Office (SPO) 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, and the U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection and 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 capable of acquiring internal memory from feature phones, smart 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 and hardware tools capable of acquiring the internal memory of feature phones, smart phones, tablets and UICCs. The mobile device tool specification is general and capable of being adapted to other types of mobile device forensic hardware and software.

4. Definitions

This glossary provides context in the absence of definitions recognized by the digital forensics community.

Acquisition – A process by which digital evidence is duplicated, copied, or imaged.

Analysis – The examination of acquired data for its significance and probative value.

Associated data – Multi-media/metadata data (i.e., graphic, audio, video, address, notes) that are attached with a specific data object (e.g., Address book, MMS messages).

Authentication Mechanism – Hardware or software-based mechanisms that challenge users to prove their identity before accessing data on a device.

Bluetooth – A wireless protocol that allows two similarly equipped devices to communicate with each other within a short distance (e.g., 30 ft.).

Code Division Multiple Access (CDMA) – A spread spectrum technology for cellular networks based on the Interim Standard-95 (IS-95) from the Telecommunications Industry Association (TIA).

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 (PIM) data, call logs, text messages, standalone files (e.g., graphic files, audio, video).

Electronic Serial Number (ESN) – A unique 32-bit number programmed into CDMA phones when they are manufactured.

Examination – A technical review that makes the evidence visible and suitable for analysis; as well as tests performed on the evidence to determine the presence or absence of specific data.

Feature Phone – A mobile device that primarily provide users with simple voice and text messaging services.

File System – A software mechanism that defines the way that files are named, stored, organized, and accessed on logical volumes of partitioned memory.

General Packet Radio Service (GPRS) – A packet switching enhancement to GSM and TDMA wireless networks to increase data transmission speeds.

Global Positioning System (GPS) – A system for determining position by comparing radio signals from several satellites.

Global System for Mobile Communications (GSM) – A set of standards for second generation, cellular networks currently maintained by the 3rd Generation Partnership Project (3GPP).

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

Internal Memory (IM) – Volatile and non-volatile storage space for user data.

Instant Messages – A facility for exchanging messages in real-time with other people over the Internet and tracking the progress of a given conversation.

Integrated Circuit Card ID (ICCID) – The unique serial number assigned to, maintained within, and usually imprinted on the UICC.

International Mobile Equipment Identity (IMEI) – A unique identification number programmed into GSM and UMTS mobile devices.

International Mobile Subscriber Identity (IMSI) – A unique number associated with every GSM mobile phone subscriber, which is maintained on a UICC.

Location Information (LOCI) – The Location Area Identifier (LAI) of the phone's current location, continuously maintained on the UICC when the phone is active and saved whenever the phone is turned off.

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

Mobile Devices – A mobile device is a small hand-held device that has a display screen with touch input and/or a QWERTY keyboard and may provide users with telephony capabilities. Mobile devices are used interchangeably (phones, tablets) throughout this document.

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 Integrated Services Digital Network (MSISDN) – The international telephone number assigned to a cellular subscriber.

Multimedia Messaging Service (MMS) – An accepted standard for messaging that lets users send and receive messages formatted with text, graphics, audio, and video clips.

Personal Information Management (PIM) Applications – A core set of applications that provide the electronic equivalents of such items as an agenda, address book, notepad, and reminder list.

Personal Information Management (PIM) Data – The set of data types such as contacts, calendar, notes, memos, and reminders maintained on a device, which may be synchronized with a personal computer.

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

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

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

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

Short Message Service (SMS) – A cellular network facility that allows users to send and receive text messages made up of alphanumeric characters on their handset.

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.

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 chip specialized for use in GSM equipment.

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 (UICC) – 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, RUIM 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.

Universal Serial Bus (USB) – A hardware interface for low-speed peripherals such as the keyboard, mouse, joystick, scanner, printer, and telephony devices.

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

Volatile Memory – Memory that loses its content when power is turned off or lost.

5. Background

5.1 Mobile Device Characteristics – Internal Memory

Mobile devices contain both non-volatile and volatile memory. Volatile memory (i.e., RAM) is used for dynamic storage and its contents are lost when power is drained from the mobile device. Non-volatile memory is persistent as its contents are not affected by loss of power or overwriting data upon reboot. For example, solid-state drives (SSD) that stores persistent data on solid-state flash 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, user files in NAND and RAM is used for code execution.

The latest smartphones contain only NAND and RAM memory (i.e., third generation), due to requirements for higher transaction speed, greater storage density and lower cost. To facilitate the lack of space on mobile device mainboards and the demand for higher density storage space (i.e., 2GB – 128GB) the new Embedded MultiMedia Cards (eMMC) style chips are present in many of today's smartphones.

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 Identity Module (UICC) Characteristics

Identity modules (commonly known as SIM cards) are synonymous with mobile devices that interoperate with GSM cellular networks. Under the GSM framework, a mobile device is referred to as a Mobile Station and is partitioned into two distinct components: the Universal Integrated Circuit Card (UICC) and the Mobile Equipment (ME). A UICC, commonly referred to as an identity module (e.g., Subscriber Identity Module [SIM], Universal Subscriber Identity Module [USIM], CDMA Subscriber Identity Module [CSIM]), is a removable component that contains essential information about the subscriber. The ME and the radio handset portion cannot fully function without a UICC. The UICC's main purpose entails authenticating the user of the mobile device to the network providing access to subscribed services. The UICC also offers storage for personal information, such as phonebook entries, text messages, last numbers dialed (LND) and service-related information.

A preset number of attempts (usually three) are allowed for providing the correct PIN code to the UICC before further attempts are blocked completely, rendering communications inoperative. Only by providing a correct PIN Unblocking Key (PUK) may the value of a PIN and its counter be reset on the UICC. If the number of attempts to enter the correct PUK value exceeds a set limit, normally ten, the card becomes blocked permanently. The PUK for a UICC may be obtained from the service provider or network operator by providing the identifier of the UICC (i.e., Integrated Circuit Chip Identifier or ICCID). The ICCID is normally imprinted on the front of UICC, but may also be read from an element of the file system.

UICCs are available in three different size formats. They are: Mini SIM (2FF), Micro SIM (3FF), and Nano SIM (4FF). The Mini SIM with a width of 25 mm, a height of 15 mm, and a thickness of .76 mm, is roughly the footprint of a postage stamp and is currently the most common format used worldwide. Micro (12mm x 15mm x .76mm) and Nano (8.8mm x 12.3mm x .67mm) SIMs are found in newer mobile devices (e.g., iPhone 5 uses the 4FF).

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. Native applications and the ability to install third-party 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 supported data objects stored in the device's internal memory and associated media types outlined in sections 5.3.1 and 5.3.2.

5.3.1 Internal Memory

- Subscriber and equipment identifiers: IMEI, MEID/ESN
- PIM data: phonebook/contacts, calendar, memos, etc.
- Call logs: incoming, outgoing, missed
- Text messages: SMS, MMS (audio, graphic, video)
- Instant messages
- Stand-alone files: audio, graphic, video
- Electronic documents: supported text files, doc, pdf, slideshow, etc.
- Electronic mail
- Third-party application data
- Web activity: history, bookmarks
- Social media related data
- GPS / Geo-location related data: longitude and latitude coordinates

5.3.1 UICC 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)
- Text messages (SMS)
- Location (LOCI, GPRSLOCI)

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

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

The data objects identified in sections 5.3.1 and 5.3.2 are used in populating the internal memory of mobile devices and UICCs.

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-03 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-07 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 suggested interfaces (e.g., cable, Bluetooth).

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 data extraction.

MDT-CR-03 A mobile device forensic tool shall have the ability to perform a logical data extraction of supported data objects without modification.

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:

- Physical data extraction
- UICC data extraction
- Authentication mechanism bypass

6.2.1 Physical Data Extraction

MDT-RO-01 A mobile device forensic tool shall have the ability to perform a physical data extraction for supported devices.

MDT-RO-02 A mobile device forensic tool shall have the ability to notify the user of connectivity errors between the device and application during a physical data extraction.

MDT-RO-03 A mobile device forensic tool shall have the ability to perform a physical data extraction (boot loader, JTAG, ISP) of readable memory without modification.

6.2.2 UICC Data Extraction

MDT-RO-04 A mobile device forensic tool shall have the ability to recognize supported UICCs via supported interfaces (e.g., USB, PC/SC reader).

MDT-RO-05 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-06 A mobile device forensic tool shall have the ability to acquire all application-supported data objects present in the UICC memory.

6.2.3 Authentication Mechanism Bypass

MDT-RO-07 A mobile device forensic tool shall have to attempt to bypass password/authentication mechanisms for supported devices.