February 2021

Mobile Device Forensic Tool Specification, Test Assertions and Test Cases

Version 3.1

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

Disclaimer

Certain commercial entities, equipment, or materials may be identified in this document 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.

Abstract

This specification defines requirements, test assertions and test cases for extracting and reporting evidence of probative value from mobile devices, including smart phones, tablets, Universal Integrated Circuit Cards (UICCs) and feature phones. Mobile devices contain a wealth of information potentially relevant to an investigation.

This document defines mobile forensic data acquisition tool requirements. The requirements are used to derive test assertions, statements of conditions that are checked after a test case is run. Each test assertion is covered by one or more test cases consisting of a test protocol and the expected test results. The test case protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results.

Comments and feedback are welcome. This document, and future revisions, are available for download at: https://www.cftt.nist.gov/mobile_devices.htm.

TABLE OF CONTENTS

1 Introduction

There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools. A capability is required to ensure that forensic tools consistently produce accurate, repeatable and objective test results. 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 tools by the development of functional specifications, test procedures, test criteria, test sets, and test hardware. The results provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the tools' capabilities. This approach for testing computer forensic tools is based on well-recognized international methodologies for conformance testing and quality testing. This project is further described at http://www.cftt.nist.gov/.

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security (DHS) Science and Technology Directorate, the National Institute of Justice (NIJ), and the National Institute of Standards and Technology.

2 Purpose

This specification defines requirements, test assertions and test cases for mobile device forensic tools capable of performing the following tasks:

1. Performing a logical acquisition of mobile device data artifacts into an image file.
2. Performing a physical acquisition via bootloader of a mobile device's memory into an image file.
3. Extraction and presentation of data artifacts from an image file created by the tool.
4. Extraction and presentation of data artifacts from an image file created by a hardware technique such as JTAG (Joint Test Action Group) or chip-off.

The requirements are used to derive test assertions, statements of conditions that are checked after a test case is run. Each test assertion is covered by one or more test cases consisting of a test protocol and the expected test results. The test case protocol specifies detailed procedures for setting up the test, executing the test, and measuring the test results.

Changes to version 3.1 include addressing SQLite databases and explicitly requiring tools to present supported data to the user rather than the user having to search for a specific file or find the data within a hex dump.

3 Scope

The scope of this specification is limited to software and hardware tools capable of extracting and presenting the internal memory of feature phones, smart phones, tablets and Universal Integrated Circuit Cards (UICC). 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 defines terms used within this document.

Acquisition – The process by which digital data from a mobile device is copied into an image file. There are several types of acquisitions:

- Logical acquisition: Extraction of a set of supported digital artifacts from the device memory.
- Selective acquisition: Extraction of a subset of supported digital artifacts from the device memory.
- File system acquisition: Extraction of the file system structure and content from the device memory.
- Physical acquisition: A copy of the device physical memory.
- UICC acquisition: Extraction of the supported artifacts from a UICC.

Active SQLite data – Table information that comprises the current state of the database (and all associated journal mode files) as of the latest successful commit.

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

Associated data – Data (e.g., graphics, address, notes, etc.) that are attached with a specific data object such as an address book entry/Contact, Multimedia Messaging Service (MMS) message, etc.

Binary Large OBject (BLOB) – A Binary Large Object is a string of binary data stored as a single entity within a database management system. BLOB's can typically be images, audio, Plists or other multimedia objects.

Bluetooth – A wireless protocol that allows two similarly equipped devices to communicate with each other within a short distance (e.g., 9 m).

Boot loader – Software temporarily installed on a mobile device enabling access to perform a physical data extraction including unallocated data areas.

Case file – A file containing case description data and possibly an image file containing data from an acquisition.

Chip-off – Data extraction which involves physically removing flash memory chip(s) from a mobile device.

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 Removable User Identity Module (R-UIM) card.

Data Artifacts – Files or directories stored in the internal memory of a mobile device or UICC such as address book entries, Personal Information Management (PIM) data, call logs, text messages, standalone files (e.g., audio, documents, graphic, video).

Deleted File – A file that has been logically, but not necessarily physically, erased from the operating system. Deleting files does not always eliminate the possibility of recovering all or part of the original data.

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 provides 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.

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).

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 the Universal Mobile Telecommunications System (UMTS) mobile devices.

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

Joint Test Action Group (JTAG) – A method for performing a physical data extraction involving connecting to Test Access Ports (TAPs) of supported devices and instructing the processor to transfer the raw data stored on memory chips.

Journal mode – SQLite functionality that provides rollback abilities in accordance with Atomic, Consistent, Isolated, and Durable (ACID) transactions. This refers to either a -journal or -wal file.

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: A bit-by-bit copy of active 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).

Image File – A file created from the data present on a mobile device. This may be a stand-alone file, (e.g., a binary bit-stream image of a digital device memory from a JTAG or chip-off acquisition), or may be embedded in another file, (e.g., embedded in a case file).

Mobile Device Tool (MDT) –A tool capable of presenting and possibly acquiring the contents of the internal memory of a mobile device.

Mobile Devices – A hand-held device that has a display screen with touch input and/or a keyboard and may provide users with telephony capabilities. *Mobile devices* are used for both, phones and 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, graphic, 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 mobile device.

Physical acquisition: A bit-by-bit acquire of the mobile device internal memory. This allows recovery of more deleted data than a logical or file system data acquisition.

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 Universal Integrated Circuit Card (UICC) whose PIN attempts have been exhausted.

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

Rollback journal – This is a file associated with each SQLite database that holds information used to restore the database file to its initial state during the course of a transaction while in journal mode. This file is located in the same directory as the database with the string "-journal" appended to its filename.

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, native, hybrid and web applications, enhanced Internet connectivity and email.

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

SQLite – SQLite is an embedded Structured Query Language (SQL) relational database engine that implements a self-contained, serverless, zero-configuration, transactional SQL database engine.

SQLite Table – A data structure that organizes information into rows and columns. It can be used to store and display data in a structured format.

Subscriber Identity Module (SIM) – A smart card chip specialized for use in GSM equipment.

Supported Data Artifacts – Data artifacts (e.g., subscriber, equipment information, PIM data, text messages, stand-alone data, MMS messages and associated data) that the mobile device forensic tool has the ability to acquire according to the tool documentation.

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, R-UIM or CSIM, and is used interchangeably with those terms.

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

User data – Data stored in the memory of a mobile device.

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

Write-Ahead Log (WAL) – A file that records SQLite transactions that have been committed, but not yet applied to the database. This file is in the same directory as the database with the string "-wal" appended to its filename. As of version 3.7.0 (dated 7/21/2010) this file type is the most commonly used method when SQLite journaling mode is enabled.

5 Background

5.1 Mobile Device Characteristics – Internal Memory

Mobile devices contain both volatile and non-volatile memory. Volatile memory (i.e., Random Acess Memory (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 (e.g., solid-state drives (SSD) that store persistent data on solid-state flash memory).

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 or UICC) are used 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 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 is 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 the UICC, but may also be read from an element of the file system.

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. A limited amount of information may be 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]).

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

5.3 Extractable Digital Artifacts

The amount and richness of data contained on mobile devices varies based upon the manufacturer and OS. Installed applications provide investigators with a rich repository of data that can be relevant to an investigation. However, there is a core set of data that mobile device forensic tools can recover that remains constant across most mobile devices. Tools should have the ability to recover the following supported data artifacts stored in the device's internal memory and UICC memory outlined in sections 5.3.1 and 5.3.2.

5.3.1 Internal Memory Artifacts

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

5.3.2 UICC Memory Artifacts

- 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)

5.4 SQLite Databases

SQLite was developed nearly twenty years ago. It has become the most widely deployed and used database engine in the world. It is used by every instance of Google Chrome and Firefox browser in existence. Particularly important to mobile forensic analysts, it is also installed on every Android and iOS device in existence today. It is the default database storage format for the millions of mobile device applications for both of these operating systems.

As of January 2020, Statistia reports that there are over 1,840,000 applications in the Apple App Store (iOS devices) and 2,570,000 applications in the Google Play Store (Android devices)[2]. That's a combined total of over 4.3 million different applications that an examiner may encounter for any

[2] Source: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

particular case. The focus of testing will be on popular apps that are most likely to be forensically relevant, such as communications including social media apps.

The SQLite data covered within this mobile specification addresses active data as contained within SQLite databases. Deleted SQLite data is quite complex in nature and therefore, not covered within this document. This topic is covered in *SQLite Deleted Data Recovery Specification, Test Assertions and Test Cases*.

6 Requirements & Test Assertions

This section lists the mobile device forensic tool requirements that are tested. Each requirement is followed by a set of one or more test assertions, statements that can be checked after a test case is performed. There are requirements for core features that all tools must meet and also requirements for optional features. The requirements for optional features only apply if the tool supports the feature.

6.1 Requirements for Core Features

The following requirements define the essential elements of a mobile acquisition tool.

MDT-CR-01. A mobile device forensic tool extracts and presents all supported data artifacts from a mobile device image file.

- **MDT-CA-01.** The tool presents all subscriber and equipment information available from an image file.
- **MDT-CA-02.** The tool presents all PIM (address book, calendar & notes) data available from an image file.
- **MDT-CA-03.** The tool presents all call data (call type (incoming, outgoing, missed), date-time stamps, duration) available from an image file.
- **MDT-CA-04.** The tool presents all message (SMS, MMS & instant messages) data available from an image file.
- **MDT-CA-05.** The tool presents all stand-alone (audio, documents, graphic & video,) files available from an image file.
- **MDT-CA-06.** The tool presents all browsing (history & bookmarks) data available from an image file.
- **MDT-CA-07.** The tool presents all email data available from an image file.
- **MDT-CA-08.** The tool presents all social media application data available from an image file.
- **MDT-CA-09.** The tool presents all geo-location application data available from an image file.

MDT-CR-02. The tool renders text correctly.

- **MDT-CA-10.** Presented text is rendered with the correct character glyphs.

MDT-CR-03. A mobile device forensic tool does not modify a mobile device image file being examined.

- **MDT-CA-11.** The tool does not modify an image file.

MDT-CR-04. A mobile device forensic tool notifies the tool user if a mobile device image file has been modified.

- **MDT-CA-12.** If an image file is modified, the tool notifies the user that a change has been made to the image file.

6.2 Requirements for Optional Features

This section lists requirements for optional tool features. If a tool provides the defined feature, the tool is tested for conformance to the requirements for the feature. If the tool does not support the feature, the requirement does not apply.

The following optional features are identified:

6.2.1 Image File Creation

The following requirements and test assertions only apply if a mobile device forensic tool supports acquisition of a supported mobile device.

MDT-RO-01. A mobile device forensic tool creates an image file from a physical memory acquisition (e.g., boot loader).

MDT-AO-01. An image file is created of physical memory.

MDT-RO-02. A mobile device forensic tool creates an image file from a logical acquisition of all supported memory artifacts.

MDT-AO-02. An image file is created containing supported memory artifacts.

MDT-RO-03. A mobile device forensic tool creates an image file from a logical acquisition of selected memory artifacts.

MDT-AO-03. An image file is created containing selected artifacts.

MDT-RO-04. A mobile device forensic tool creates an image file from an acquisition of the mobile device file system.

MDT-AO-04. An image file is created of the device file system.

MDT-RO-05. A mobile device forensic tool notifies the user if there is a failure to access a connected mobile device.

MDT-AO-05. The user is notified if the tool fails to establish a connection or acquire data from a connected mobile device.

MDT-RO-06. A mobile device forensic tool notifies the user if an acquisition is interrupted before completion.

MDT-AO-06. The user is notified if an acquisition is disrupted.

6.2.2 UICC Access, Acquisition and Presentation

The following requirements and test assertions only apply if a mobile device forensic tool supports acquisition and presentation of data from a UICC.

MDT-RO-07. A mobile device forensic tool allows access to a locked UICC via PIN code and PUK code.

MDT-AO-07. A mobile device forensic tool provides a count of remaining authentication attempts for a locked UICC acquisition if an incorrect PIN is entered.

MDT-AO-08. A mobile device forensic tool unlocks a locked UICC if the correct PIN code is given to the tool.

MDT-AO-09. A mobile device forensic tool provides the examiner with a count of remaining authentication attempts for a locked UICC acquisition if an incorrect PUK code is entered.

MDT-AO-10. A mobile device forensic tool unlocks a locked UICC that has been given the maximum number of incorrect PIN codes if the correct PUK code is given to the tool.

MDT-RO-08. A mobile device forensic tool creates an image file from an acquisition of an unlocked UICC.

MDT-AO-11. An image file is created containing supported UICC artifacts.

MDT-RO-09. A mobile device forensic tool extracts and presents all supported data artifacts from a UICC image file.

MDT-AO-12. A mobile device forensic tool presents Service Provider Name (SPN) from a UICC image file.

MDT-AO-13. A mobile device forensic tool presents Integrated Circuit Card Identifier (ICCID) from a UICC image file.

MDT-AO-14. A mobile device forensic tool presents International Mobile Subscriber Identity (IMSI) from a UICC image file.

MDT-AO-15. A mobile device forensic tool presents Mobile Subscriber International ISDN Number (MSISDN) from a UICC image file.

MDT-AO-16. A mobile device forensic tool presents Abbreviated Dialing Numbers (ADNs) from a UICC image file.

MDT-AO-17. A mobile device forensic tool presents Last Numbers Dialed (LND) from a UICC image file.

MDT-AO-18. A mobile device forensic tool presents Text messages (SMS) from a UICC image file.

MDT-AO-19. A mobile device forensic tool presents Location (LOCI, GPRSLOCI) from a UICC image file.

6.2.3 Deleted Data Artifacts Recovery

A forensic tool recovers deleted data artifacts dependent upon its capability.

MDT-RO-10. A mobile device forensic tool presents recoverable deleted artifacts.

MDT-AO-20. If an image file contains recoverable deleted data artifacts and the tool supports data recovery, then the tool presents the recovered deleted items.

6.2.4 SQLite Data

A forensic tool provides SQLite functionality.

MDT-RO-11. A mobile device forensic tool shall report the data content of all rows for each active table in the database.

MDT-AO-21. The tool shall display numeric values (e.g., integer and floating point values).

MDT-AO-22. The tool shall display integer time values as a conventional human readable date and time.

MDT-AO-23. The tool shall render text for Text fields, table names, and column names encoded in Unicode Transformation Format (UTF) 8, UTF 16BE, and UTF 16LE.

MDT-AO-24. The tool shall decode and display base64 encoded text.

MDT-AO-25. The tool shall display graphic image data recorded as a BLOB in the database.

MDT-AO-26. The tool shall decode data recorded as a BLOB in the database.

MDT-AO-27. The tool shall have the ability to display SQLite BLOB data (e.g., graphic files and plist).

MDT-AO-28. The tool shall report all currently active data when WAL mode is in use.

MDT-AO-29. The tool shall report all currently active data when journal mode is in use.

MDT-RO-12. A mobile device forensic tool provides embedded SQLite functionality.

MDT-AO-30. The tool shall execute SQLite commands and report the results.

MDT-AO-31. The tool shall have the ability to save SQLite commands for later recall.

7 Mobile Device Test Cases

The actual test cases selected depends on the tool features supported for a particular mobile device. For example, a tablet would not usually have call logs, but a phone would. A given phone might or might not have a UICC. A given tool may not support particular image file acquisition types and possibly no acquisitions at all but provide analysis capabilities of mobile device images.

Tools tested are expected to report supported data elements to the user within the GUI. This does not mean having to physically search for data artifacts within a hex view.

If a mobile device forensic tool supports selective logical acquisition then the three variations of ONE, SUBSET and SELECTED should be done. A challenge of selected acquisition is the large number of possible combinations that could be tested. The compromise between the time required to run a large number of different combinations and expending a reasonable amount of time is to use three selection set variations (ONE, SUBSET and SELECTED) for each device tested, but use a different selection set for each device. The selection sets for each variation are as follows:

- Variation SELECTED: Select all supported data items. Do this for each device tested.
- Variation ONE: Select just one supported data item. Select a different data item for each device tested. If there are more devices than data items, then repeat selected data items.
- Variation SUBSET: Select a subset of supported data items. Use a different one of the following patterns for each device, the expectation is to select about a third to a half of the data items for each tested device. If you have more devices than there are patterns you will need to repeat patterns already used, just use all the patterns approximately an equal number of times:
    - Mentally number the supported data items: 1, 2, 3, … select the odd numbered items.
    - Mentally number the supported data items: 1, 2, 3, … select the even numbered items.
    - Mentally number the supported data items: 1, 2, 3, … select every third item starting with item 2.

- Select the first half of the supported items.
- Select the last half of the supported items.

MDT-01. Disruption notification.

This test case only applies for acquisition types supported by the tool. Begin an acquisition, wait a suitable time interval and then disrupt the connection to the mobile device. There can be case variations for each acquisition type:

- MDT-01-LOG for logical acquisition
- MDT-01-ONE for selective acquisition of one data item
- MDT-01-SUBSET for selected acquisition of subset of data items
- MDT-01-SELECTED for selected acquisition of all supported data items
- MDT-01-FILE for file system acquisition
- MDT-01-PHY for physical acquisition

Test Assertions:

MDT-AO-06 The user is notified if an acquisition is disrupted.

MDT-02. Create an image file.

Acquire data from a mobile device. This test case only applies for acquisition types supported by the tool. If the tool supports selective logical acquisition then all of the three selective acquisition variations should be run (ONE, SUBSET and SELECTED). There can be case variations for the different acquisition types:

- MDT-02-LOG for logical acquisition
- MDT-02-ONE for selective acquisition of one data item
- MDT-02-SUBSET for selected acquisition of subset of data items
- MDT-02-SELECTED for selected acquisition of all supported data items
- MDT-02-FILE for file system acquisition
- MDT-02-PHY for physical acquisition

Test Assertions (only one of the first 4 applies depending of the variation):

MDT-AO-01 An image file is created of physical memory. (PHY)

MDT-AO-02 An image file is created containing supported memory artifacts. (LOG)

MDT-AO-03 An image file is created containing selected artifacts. (ONE, SUBSET and SELECTED)

MDT-AO-04 An image file is created of the device file system. (FILE)

MDT-AO-05 The user is notified if the tool fails to establish a connection or acquire data from a connected mobile device.

MDT-03. View artifacts from an image file.

View data acquired from a mobile device to an image file. Open an image file and try to view the expected data items present. There can be case variations for the different acquisition methods used to create the image file:

- MDT-03-LOG for logical acquisition
- MDT-03-ONE for selective acquisition of one data item
- MDT-03-SUBSET for selected acquisition of subset of data items

- MDT-03-SELECTED for selected acquisition of all supported data items
- MDT-03-FILE for file system acquisition
- MDT-03-PHY for physical boot loader acquisition
- MDT-03-JTAG for JTAG acquisition (acquired via separate hardware device)
- MDT-03-CHIP for Chip-off acquisition (acquired via separate hardware device)

Test assertions:

MDT-CA-01 The tool presents all subscriber and equipment information available from an image file.

MDT-CA-02 The tool presents all PIM (address book, calendar & notes) data available from an image file.

MDT-CA-03 The tool presents all call data (call type (incoming, outgoing, missed), date-time stamps, duration) available from an image file.

MDT-CA-04 The tool presents all message (SMS, MMS & instant messages) data available from an image file.

MDT-CA-05 The tool presents all stand-alone (audio, documents, graphic & video,) files available from an image file.

MDT-CA-06 The tool presents all browsing (history & bookmarks) data available from an image file.

MDT-CA-07 The tool presents all email data available from an image file.

MDT-CA-08 The tool presents all social media application data available from an image file.

MDT-CA-10 Presented text is rendered with the correct character glyphs.

MDT-AO-20 If an image file contains recoverable deleted data artifacts and the tool supports data recovery, then the tool presents the recovered deleted items.

MDT-CA-11 The tool does not modify an image file.

MDT-04. Detect change to an image file.

Make a change to an image file, then open the image file. There can be case variations for the different acquisition types:

- MDT-04-LOG for logical acquisition
- MDT-04-ONE for selective acquisition of one data item
- MDT-04-SUBSET for selected acquisition of subset of data items
- MDT-04-SELECTED for selected acquisition of all supported data items
- MDT-04-FILE for file system acquisition

Test assertions:

MDT-CA-12 If an image file is modified, the tool notifies the user that a change has been made to the image file.

MDT-05. Unlock a UICC

Connect to a locked UICC and attempt to unlock the UICC. There are two variations:

- MDT-05-PIN Unlock with a PIN code a locked UICC.
- MDT-05-PUK Unlock with a PUK code a UICC that has had the maximum number of failed PIN attempts.

Test Assertions for MDT-05-PIN:

MDT-AO-07 A mobile device forensic tool provides a count of remaining authentication attempts for a locked UICC acquisition if an incorrect PIN is entered.

MDT-AO-08 A mobile device forensic tool unlocks a locked UICC if the correct PIN code is given to the tool.

Test Assertions for MDT-05-PUK:

MDT-AO-09 A mobile device forensic tool provides the examiner with a count of remaining authentication attempts for a locked UICC acquisition if an incorrect PUK code is entered.

MDT-AO-10 A mobile device forensic tool unlocks a locked UICC that has been given the maximum number of incorrect PIN codes if the correct PUK code is given to the tool.

MDT-06. Create UICC image file

Create a image file of an unlocked UICC.

Test assertion:

MDT-AO-11 An image file is created containing supported UICC artifacts.

MDT-07. View artifacts from UICC image file

View acquired artifacts from a UICC.

Test Assertions:

MDT-AO-12 A mobile device forensic tool presents Service Provider Name (SPN) from a UICC image file.

MDT-AO-13 A mobile device forensic tool presents Integrated Circuit Card Identifier (ICCID) from a UICC image file.

MDT-AO-14 A mobile device forensic tool presents International Mobile Subscriber Identity (IMSI) from a UICC image file.

MDT-AO-15 A mobile device forensic tool presents Mobile Subscriber International ISDN Number (MSISDN) from a UICC image file.

MDT-AO-16 A mobile device forensic tool presents Abbreviated Dialing Numbers (ADNs) from a UICC image file.

MDT-AO-17 A mobile device forensic tool presents Last Numbers Dialed (LND) from a UICC image file.

MDT-AO-18 A mobile device forensic tool presents Text messages (SMS) from a UICC image file.

MDT-AO-19 A mobile device forensic tool presents Location (LOCI, GPRSLOCI) from a UICC image file.

MDT-AO-20 If an image file contains recoverable deleted data artifacts and the tool supports data recovery, then the tool presents the recovered deleted items.

MDT-CA-11 The tool does not modify an image file.

MDT-08. View active table data within an SQLite database.

View acquired artifacts within the embedded SQLite viewer.

Test Assertions:

MDT-AO-21 The tool shall display numeric values (e.g., integer and floating point values).

MDT-AO-22 The tool shall display integer time valules as a conventional human-readable date and time.

MDT-AO-23 The tool shall render text for Text fields, table names, and column names encoded in UTF 8, UTF 16BE, and UTF 16LE.

MDT-AO-24 The tool shall decode and display base64 encoded text.

MDT-AO-25 The tool shall display graphic image data recorded as a BLOB in the database.

MDT-AO-26 The tool shall decode data recorded as a BLOB in the database.

MDT-AO-27 The tool shall have the ability to display SQLite BLOB data.

MDT-AO-28 The tool shall report all currently active data when WAL mode is in use.

MDT-AO-29 The tool shall report all currently active data when journal mode is in use.

MDT-09. Execute SQLite commands stored within the image file.
Run and save SQLite commands.

Test Assertions:

MDT-AO-30 If an image file contains recoverable deleted data artifacts and the tool supports data recovery, then the tool presents the recovered deleted items.

MDT-AO-31 The tool shall have the capability to save SQLite commands for later recall.