February 1, 2016

# Mobile Device Tool Test Assertions and Test Plan

Version 2.0

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

34

# 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 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 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 assertions and test cases for mobile device applications capable of acquiring data from mobile devices (i.e., feature phones, smart phones, tables, associated media), to determine whether a specific tool meets the requirements producing measurable results.· The assertions and test cases are derived from the requirements defined in the document entitled: Mobile Device Tool Specification Version 2.0. Test cases describe the combination of test parameters required to test each assertion. Test assertions are described as general statements of 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.

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

· 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.

61

# TABLE OF CONTENTS

81

# 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 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 document defines test assertions and test cases derived from requirements for mobile device forensic tools capable of acquiring the internal memory from feature phones, smart phones, tablets and Universal Integrated Circuit Cards (UICCs). 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 feature phones, smart phones, tablets and UICCs. While mobile devices and tablets often have companion PC-based software that provides users the ability to synchronize data between the device and a personal computer this test assertion and test plan does not address device data synchronized with personal computers. The assertions and test cases are specific to data stored in the internal memory of feature phones, smart phones, tablets or UICCs. The test cases are general and capable of being adapted to other types of mobile device forensic software.

# 4. Test Assertions

The primary goal of the test assertions, presented below in Table 1, is to determine a tool's ability to accurately acquire specific data objects populated onto the feature phone, smart phone, tablet or UICC. An accurate acquisition copies data objects from the powered device (i.e., active) such that the bytes of the acquired data object are identical to the bytes of the data object on the device. The ID column identifies the assertion. For instance MDT-CA-01 (i.e., Mobile Device Tool-Core Assertion-#) is a core assertion. An assertion for optional features, MDT-AO-01 (i.e., Mobile Device Tool-Assertion Optional-#) is an optional assertion and only tested if a tool supports the feature. The Test Assertion column states the assertion and the comments column provides additional information pertaining to the assertion.

**Table 1: Test Assertions**

| ID | Test Assertion | Comments |
|---|---|---|
| MDT-CA-01 | If a mobile device forensic tool provides the user with an "***Acquire All***" data objects acquisition option then the tool shall complete the logical/filesystem acquisition of all data objects without error. | Select Acquire all; Begin acquisition |
| MDT-CA-02 | If a mobile device forensic tool provides the user with a ***"Select All"*** individual data objects then the tool shall complete the logical/filesystem acquisition of all individually selected data objects without error. | Select all supported data objects; Begin acquisition |
| MDT-CA-03 | If a mobile device forensic tool provides the user with the ability to ***"Select Individual"*** data objects for acquisition then the tool shall complete the logical/filesystem acquisition for each exclusive data object without error. | Select one or more supported data objects; Begin acquisition |
| MDT-CA-04 | If connectivity between the mobile device and forensic tool is disrupted for a logical/filesystem acquisition then the tool shall notify the user that connectivity has | Begin acquisition; Disconnect interface or interrupt connectivity (i.e., unplug |

| | | |
|---|---|---|
| | been disrupted. | cable) during acquisition |
| MDT-CA-05 | If a mobile device forensic tool completes logical/filesystem acquisition of the target device without error then the tool shall have the ability to present acquired data objects in a useable format via either a preview-pane or generated report. | Acquire device data; Review data for readability in a useable format |
| MDT-CA-06 | If a mobile device forensic tool completes logical/filesystem acquisition of the target device without error then the tool shall have the ability to present subscriber and equipment related information (e.g., IMSI, IMEI, MEID/ESN, MSISDN) in a useable format. | Acquire device data; Review acquisition of IMSI, IMEI, MEID/ESN, MSISDN |
| MDT-CA-07 | If a mobile device forensic tool completes logical/filesystem acquisition of the target device without error then all supported data elements: PIM data (address book, calendar, notes), call logs, SMS, MMS, chat logs, stand-alone files (audio, pictures, video), application, social media and Internet related data (bookmarks, browsing history), email and GPS data shall be presented in a useable format. | Acquire device data; Review acquisition of tool supported data elements |
| MDT-CA-08 | If the mobile device forensic tool completes logical/filesystem acquisition of the target device without error, acquired data containing non-Latin characters shall be presented in their native format. | Acquire device data; Review acquisition of data containing non-Latin characters |
| MDT-CA-09 | If the mobile device forensic tool completes logical/filesystem acquisition of the target device without error, hash values are reported for acquired data objects or overall case file. | Acquire device data; Check known hash values for consistency |
| MDT-CA-10 | If the logical/filesystem generated case file or individual data objects are modified via third-party means then the tool shall provide protection mechanisms disallowing or reporting data modification. | Acquire device data; Alter case file; Attempt to re-open altered case file with application |
| MDT-AO-01 | If the mobile device forensic tool supports a physical acquisition of the target device then the tool shall complete the physical acquisition without error. | Select Physical Acquisition; Begin acquisition |
| MDT-AO-02 | If connectivity between the mobile device and mobile device forensic tool for a | Begin acquisition; Disconnect interface or interrupt |

| | | |
|---|---|---|
| | physical acquisition is disrupted then the tool shall notify the user that connectivity has been disrupted. | connectivity (i.e., unplug cable) during acquisition |
| MDT-AO-03 | If a mobile device forensic tool completes physical acquisition of the target device without error then the tool shall have the ability to present acquired data objects in a useable format via a preview-pane, generated report or output file. | Perform physical acquisition; Review data for readability in a useable format |
| MDT-AO-04 | If a mobile device forensic tool completes physical acquisition of the target device without error then subscriber-related and equipment related information (e.g., IMSI, IMEI, MEID/ESN, MSISDN) shall be presented in a useable format. | Physical acquisition; Review acquisition of IMSI, IMEI, MEID/ESN, MSISDN |
| MDT-AO-05 | If a mobile device forensic tool completes physical acquisition of the target device without error then all supported data elements: PIM data (address book, calendar, notes), call logs, SMS, MMS, chat logs, stand-alone files (audio, pictures, video), application, social media and Internet related data (bookmarks, browsing history), email and GPS data shall be presented in a useable format. | Physical acquisition; Review acquisition of tool supported data elements |
| MDT-AO-06 | If the mobile device forensic tool completes physical acquisition of the target device without error, acquired data containing non-Latin characters shall be presented in their native format. | Physical acquisition; Review acquisition of data containing non-ASCII characters |
| MDT-AO-07 | If the mobile device forensic tool completes physical acquisition of the target device without error, hash values are reported for acquired data objects or overall case file. | Physical acquisition; Check known hash values for consistency |
| MDT-AO-08 | If the case file or individual data objects for a physical acquisition are modified via third-party means then the tool shall provide protection mechanisms disallowing or reporting data modification. | Physical acquisition; Alter case file; Attempt to re-open altered case file with application |
| MDT-AO-09 | If a mobile device forensic tool provides the user with an *"**Acquire All**"* UICC data objects then the tool shall complete the acquisition of all data objects without error. | Select Acquire all; Begin acquisition |
| MDT-AO-10 | If a mobile device forensic tool provides the user with a *"**Select All**"* UICC data objects then the tool shall complete the acquisition | Select all supported data objects; Begin acquisition |

| | | |
|---|---|---|
| | of all individually selected data objects without error. | |
| MDT-AO-11 | If a mobile device forensic tool provides the user with a *"**Select Individual**"* UICC data objects for acquisition then the tool shall acquire each exclusive data object without error. | Select one or more supported data objects; Begin acquisition |
| MDT-AO-12 | If the UICC is password-protected then the mobile device forensic tool shall provide the examiner with the opportunity to input the PIN before acquisition. | Begin acquisition of password protected UICC; Input correct UICC PIN |
| MDT-AO-13 | If a mobile device forensic tool provides the examiner with the remaining number of authentication attempts for a UICC acquisition then the application should provide an accurate count of the remaining PIN attempts when entering an incorrect PIN. | Input incorrect PIN; Check tool output for correct number of remaining PIN attempts |
| MDT-AO-14 | If a mobile device forensic tool provides the examiner with the remaining number of PUK attempts for a UICC acquisition then the application should provide an accurate count of the remaining PUK attempts when entering an incorrect PUK. | Input incorrect PUK; Check tool output for correct number of remaining PUK attempts |
| MDT-AO-15 | If connectivity between the UICC and mobile device forensic tool is disrupted then the tool shall notify the user that connectivity has been disrupted. | Begin acquisition; Disconnect interface or interrupt connectivity (i.e., remove UICC from reader) during acquisition |
| MDT-AO-16 | If a mobile device forensic tool completes acquisition of the target UICC without error then acquired data shall be presented in a useable format. | UICC acquisition; Data is presented in a useable format |
| MDT-AO-17 | If a mobile device forensic tool completes acquisition of the target UICC without error then the subscriber-related and equipment related information (i.e., SPN, ICCID, IMSI, MSISDN) shall be presented in a useable format. | UICC acquisition; Review acquisition of SPN, ICCID, IMSI, MSISDN |
| MDT-AO-18 | If a mobile device forensic tool completes acquisition of the target UICC without error then all supported data elements (e.g., Abbreviated Dialing Numbers, Last Numbers Dialed, SMS text messages, and location related data: LOCI, GPRSLOCI) shall be presented in a useable format. | UICC acquisition; Review acquisition of all supported data objects |

| | | |
|---|---|---|
| MDT-AO-19 | If the mobile device forensic tool completes acquisition of the target UICC without error, acquired data containing non-Latin characters shall be presented in their native format. | UICC acquisition; Review acquisition of data containing non-ASCII characters |
| MDT-AO-20 | If the mobile device forensic tool completes acquisition of the target UICC without error, hash values are reported for acquired data objects or overall case file. | Acquire data; Check known hash values for consistency |
| MDT-AO-21 | If the case file or individual data objects of a UICC acquisition are modified via third-party means then the tool shall provide protection mechanisms disallowing or reporting data modification. | UICC acquisition; Alter case file; Attempt to re-open altered case file with application |
| MDT-AO-22 | If a mobile device forensic tool provides the ability to circumvent a password-protected device/UICC then the tool shall attempt the bypass without error. | Attempt authentication mechanism bypass |

145

146

# 5. Assertion Measurement

The following sections provide an overview of how individual test assertions are measured.

## 5.1 Connectivity

Connectivity between the mobile device and forensic software is required to acquire data from a mobile device.

***Assertion*:** MDT-CA-01 If a mobile device forensic tool provides the user with an "*Acquire All"* data objects acquisition option then the tool shall complete the logical/filesystem acquisition of all data objects without error.
***Assertion*:** MDT-CA-02 If a mobile device forensic tool provides the user with an "*Select All"* individual data objects then the tool shall complete the logical/filesystem acquisition of all individually selected data objects without error.
***Assertion*:** MDT-CA-03 If a mobile device forensic tool provides the user with the ability to "*Select Individual*" data objects for acquisition then the tool shall shall complete the logical/filesystem acquisition for each exclusive data object without error.
***Assertion*:** MDT-AO-01 If the mobile device forensic tool supports a physical acquisition of the target device then the tool shall complete the acquisition without error.
***Assertion*:** MDT-AO-09 If a mobile device forensic tool provides the user with an "*Acquire All"* UICC data objects acquisition option then the tool shall complete the acquisition of all data objects without error.
***Assertion*:** MDT-AO-10 If a mobile device forensic tool provides the user with an "*Select All"* UICC data objects then the tool shall complete the acquisition of all individually selected data objects without error.
***Assertion*:** MDT-AO-11 If a mobile device forensic tool provides the user with the ability to "*Select Individual*" UICC data objects for acquisition then the tool shall acquire each exclusive data object without error.
***Test Action*:** Acquire target mobile device / UICC data objects by specifying an acquisition variation: *acquire all, select all, select individual*.
***Conformance Indicator*:** Successful acquisition of at least one data object.

***Assertion*:** MDT-CA-04 If connectivity between the mobile device and mobile device forensic tool is disrupted for a logical/filesystem acquisition then the tool shall notify the user that connectivity has been disrupted.
***Assertion*:** MDT-AO-02 If connectivity between the mobile device and mobile device forensic tool for a physical acquisition is disrupted then the tool shall notify the user that connectivity has been disrupted.
***Assertion*:** MDT-AO-15 If connectivity between the UICC and mobile device forensic tool is disrupted then the tool shall notify the user that connectivity has been disrupted.
***Test Action*:** Disrupt connectivity during mobile device or UICC acquisition.
***Conformance Indicator*:** Notification of acquisition disruption.

## 5.2 Data Acquisition and Interpretation

Sections 5.2.1 through 5.2.3 describes assertion measurements for acquisition of supported data objects. Review acquired data for completeness and accuracy.

### 5.2.1 Presentation

***Assertion*:** MDT-CA-05 If a mobile device forensic tool completes logical/file system acquisition of the target device without error then the tool shall have the ability to present acquired data objects in a useable format via either a preview-pane or generated report.
***Assertion*:** MDT-AO-03 If a mobile device forensic tool completes physical acquisition of the target device without error then the tool shall have the ability to present acquired data objects in a useable format via either a preview-pane, generated report or output file.
***Assertion*:** MDT-AO-16 If a mobile device forensic tool completes acquisition of the target UICC without error then acquired data shall be presented in a useable format.
***Test Action*:** Acquire supported data objects from the target mobile device / UICC.
***Conformance Indicator*:** Acquired data is presented in either a preview-pane view or generated report.

### 5.2.2 Subscriber and Equipment Related Data

***Assertion*:** MDT-CA-06 If a mobile device forensic tool completes logical/file system acquisition of the target device without error then subscriber-related and equipment related information shall be presented in a useable format.
***Assertion*:** MDT-AO-04 If a mobile device forensic tool completes physical acquisition of the target device without error then subscriber-related and equipment related information (e.g., IMSI, IMEI, MEID/ESN, MSISDN) shall be presented in a useable format.
***Assertion*:** MDT-AO-17 If a mobile device forensic tool completes acquisition of the target UICC without error then the subscriber-related and equipment related information (i.e., SPN, ICCID, IMSI, MSISDN) shall be presented in a useable format.
***Test Action*:** Acquire subscriber and equipment related data (IMSI, IMEI, MEID/ESN, MSISDN) from the target mobile device / UICC.
***Conformance Indicator*:** Acquired data matches known data.

### 5.2.3 Data Acquisition

***Assertion*:** MDT-CA-07 If a mobile device forensic tool completes logical/file system acquisition of the target device without error then all supported data elements: PIM data (address book, calendar, notes), call logs, SMS, MMS, chat logs, stand-alone files (audio, pictures, video), application, social media and Internet related data (bookmarks, browsing history), email and GPS data shall be presented in a useable format.
***Assertion*:** MDT-AO-05 If a mobile device forensic tool completes physical acquisition of the target device without error then all supported data elements: PIM data (address book, calendar, notes), call logs, SMS, MMS, chat logs, stand-alone files (audio, pictures, video), application, social media and Internet related data (bookmarks, browsing history), email and GPS data shall be presented in a useable format.
***Assertion*:** MDT-AO-18 If a mobile device forensic tool completes acquisition of the target UICC without error then all supported data elements (e.g., Abbreviated Dialing Numbers, Last Numbers

Dialed, SMS text messages, and location related data: LOCI, GPRSLOCI) shall be presented in a useable format.
***Test Action*:** Populate target mobile device / UICC with known data; acquire all supported data objects.
***Conformance Indicator*:** Acquired data matches known data.

## 5.3 Non-ASCII Character Presentation

***Assertion*:** MDT-CA-08 If the mobile device forensic tool completes logical/filesystem acquisition of the target device without error, acquired data containing non-Latin characters shall be presented in their native format.
***Assertion*:** MDT-AO-06 If the mobile device forensic tool completes physical acquisition of the target device without error, acquired data containing non-Latin characters shall be presented in their native format.
***Assertion*:** MDT-AO-19 If the mobile device forensic tool completes acquisition of the target UICC without error, acquired data containing non-Latin characters shall be presented in their native format.
***Test Action*:** Populate target mobile device / UICC with known non-ASCII data; Acquire data.
***Conformance Indicator*:** Acquired non-ASCII data is presented in its native format.

## 5.4 Hashing

***Assertion*:** MDT-CA-09 If the mobile device forensic tool completes logical/filesystem acquisition of the target device without error, hash values are reported for acquired data objects or overall case file.
***Assertion*:** MDT-AO-07 If the mobile device forensic tool completes physical acquisition of the target device without error, hash values are reported for acquired data objects or overall case file.
***Assertion*:** MDT-AO-20 If the mobile device forensic tool completes acquisition of the target UICC without error, hash values are reported for acquired data objects or overall case file.
***Test Action*:** Populate target mobile device / UICC with known data; acquire supported data objects.
***Conformance Indicator*:** Hash values are reported for individually acquired data objects or overall case file.

## 5.5 Case File/Data Protection

***Assertion*:** MDT-CA-10 If the logical/filesystem generated case file or individual data objects are modified via third-party means then the tool shall provide protection mechanisms disallowing or reporting data modification.
***Assertion*:** MDT-AO-08 If the case file or individual data objects for a physical acquisition are modified via third-party means then the tool shall provide protection mechanisms disallowing or reporting data modification.
***Assertion*:** MDT-AO-21 If the case file or individual data objects are modified via third-party means then the tool shall provide protection mechanisms disallowing or reporting data modification.
***Test Action*:** Modify a saved case file with a hex editor; re-open the modified case file with the mobile device tool.
***Conformance Indicator*:** Notification that the case file has been altered.

## 5.6 UICC PIN/PUK Authentication

***Assertion*:** MDT-AO-12 If the UICC is password-protected then the mobile device forensic tool shall provide the examiner with the opportunity to input the PIN before acquisition.
***Test Action*:** Password protect the target UICC; Attempt to acquire data from the password-protected UICC by entering the password.
***Conformance Indicator*:** The tool successfully acquires all requested data.

***Assertion*:** MDT-AO-13 If a mobile device forensic tool provides the examiner with the remaining number of authentication attempts for a UICC acquisition then the application should provide an accurate count of the remaining PIN attempts when entering an incorrect PIN.
***Test Action*:** Begin acquisition on a password protected UICC; Input incorrect PIN.
***Assertion*:** MDT-AO-14 If a mobile device forensic tool provides the examiner with the remaining number of PUK attempts for a UICC acquisition then the application should provide an accurate count of the remaining PUK attempts when entering an incorrect PUK.
***Test Action*:** Begin acquisition on a password protected UICC whose PIN attempts have been exhausted; Input incorrect PUK.
***Conformance Indicator*:** The correct number of remaining number of PIN/PUK attempts are reported.

## 5.7 Authentication Mechanism Bypass

***Assertion*:** MDT-AO-22 If a mobile device forensic tool provides the ability to circumvent a password-protected device then the tool shall complete the bypass attempt without error.
***Test Action*:** Attempt authentication mechanism bypass of a password protected mobile device / UICC.
***Conformance Indicator*:** The mobile device forensic tool attempts authentication bypass without error.

# 6. Abstract Test Cases

Abstract test cases describe the combinations of test parameters required to fully test each assertion and the results expected for the given combination of test parameters. The test cases are abstract in that they do not prescribe the exact environment in which the tests are to be performed. They are written at the next level above the actual test environment, thus abstract test cases allowing substitution and variation of setup environment variables under dissimilar products and options prior to engagement in official testing. Section 6.1 lists test cases i.e., MDT-01 through MDT-03. Section 6.2 lists optional test cases i.e., MDT-04 through MDT-10.

## 6.1 Test Cases for Core Features

**MDT-01** Acquire mobile device internal memory using tool-supported interfaces (e.g., cable, Bluetooth) by selecting a combination of supported data elements. (*Variation IM_Comp*, *Variation IM_SlctAll*, *Variation IM_SlctIndv*)

**MDT-02** Begin mobile device internal memory acquisition and interrupt connectivity by interface disengagement.

**MDT-03** Perform a logical/filesystem data extraction of the target mobile device and review data output.

## 6.2 Test Cases for Optional Features

The following test cases are defined for tool features that might be implemented for some mobile device forensic tools. If a tool provides the optional feature, the tool is tested as if the test case were core. If the tool does not provide the capability defined, the test case does not apply.

*Physical Acquisition*

**MDT-04** Perform a physical data extraction (e.g., boot loader, JTAG, ISP) over tool supported interfaces.

**MDT-05** Begin mobile device physical data extraction and interrupt connectivity by interface disengagement.

**MDT-06** Perform a physical data extraction of the target mobile device and review data output.

*UICC Acqusition*

**MDT-07** Acquire UICC internal memory using tool-supported interfaces (e.g., PC/SC reader) by selecting a combination of supported data elements. (*Variation IM_Comp, Variation IM_SlctAll, Variation IM_SlctIndv)*

**MDT-08** Begin UICC data extraction and interrupt connectivity by interface disengagement.

**MDT-09** Acquire UICC internal memory and review data output.

*Bypass Authentication Mechanisms*

**MDT-10** Begin authentication mechanism attempt by establishing connectivity to the mobile device.

The following traceability matrices relate core requirements to core assertions. The requirements are defined in the document entitled: Mobile Device Tool Specification v2.0.

**Requirements to Assertions (Core Features)**

| Requirements (Core Features) | | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | MDT-CR-01 | • | • | • | | | | | | | |
| | MDT-CR-02 | | | | • | | | | | | |
| | MDT-CR-03 | | | | | • | • | • | • | • | • |

The following traceability matrices relate optional requirements to optional test assertions.

**Requirements to Assertions (Optional Features)**

| | Assertions | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Requirements (Optional Features) | | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 |
| | MDT-RO-01 | • | | | | | | | | | | |
| | MDT-RO-02 | | • | | | | | | | | | |
| | MDT-RO-03 | | | • | • | • | • | • | • | | | |
| | MDT-RO-04 | | | | | | | | | • | • | • |

| | Assertions | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Requirements (Optional Features) | | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| | MDT-RO-04 | • | • | • | | | | | | | | |
| | MDT-RO-05 | | | | • | | | | | | | |
| | MDT-RO-06 | | | | | • | • | • | • | • | • | |
| | MDT-RO-07 | | | | | | | | | | | • |

The following traceability matrices relate core assertions to core test cases.

**Assertions to Test Cases (Core Features)**

| Assertions (Core Features) | | 01 | 02 | 03 |
|---|---|---|---|---|
| | **MDT-CA-01** | • | | |
| | **MDT-CA-02** | • | | |
| | **MDT-CA-03** | • | | |
| | **MDT-CA-04** | | • | |
| | **MDT-CA-05** | | | • |
| | **MDT-CA-06** | | | • |
| | **MDT-CA-07** | | | • |
| | **MDT-CA-08** | | | • |
| | **MDT-CA-09** | | | • |
| | **MDT-CA-10** | | | • |

The following traceability matrices relate optional assertions to test cases.

**Assertions to Test Cases (Optional Features)**

| Assertions (Optional Features) | 04 | 05 | 06 | 07 | 08 | 09 | 10 |
|---|---|---|---|---|---|---|---|
| MDT-AO-01 | • | | | | | | |
| MDT-AO-02 | | • | | | | | |
| MDT-AO-03 | | | • | | | | |
| MDT-AO-04 | | | • | | | | |
| MDT-AO-05 | | | • | | | | |
| MDT-AO-06 | | | • | | | | |
| MDT-AO-07 | | | • | | | | |
| MDT-AO-08 | | | • | | | | |
| MDT-AO-09 | | | | • | | | |
| MDT-AO-10 | | | | • | | | |
| MDT-AO-11 | | | | • | | | |
| MDT-AO-12 | | | | • | | | |
| MDT-AO-13 | | | | • | | | |
| MDT-AO-14 | | | | • | | | |
| MDT-AO-15 | | | | | • | | |
| MDT-AO-16 | | | | | | • | |
| MDT-AO-17 | | | | | | • | |
| MDT-AO-18 | | | | | | • | |
| MDT-AO-19 | | | | | | • | |
| MDT-AO-20 | | | | | | • | |
| MDT-AO-21 | | | | | | • | |
| MDT-AO-22 | | | | | | | • |