July 8, 2014

Mobile Device Tool Test Assertions and Test Plan

Version 1.0

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. 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

85

1. Introduction

The need to ensure the reliability of mobile device forensic tools intensifies as the embedded intelligence and ever-increasing storage capabilities of mobile devices expand. The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing computer forensic software tools. This is accomplished by the development of both specific and common rules that govern tool specifications. We adhere to a disciplined testing procedure, established test criteria, test sets, and test hardware requirements, that result in providing necessary feedback information to toolmakers so they can improve their tool's effectiveness; end users benefit in that they gain vital information making them more informed about choices for acquiring and using computer forensic tools, and lastly, we impart knowledge to interested parties by increasing their understanding of a specific tool's capability. Our approach for testing computer forensic tools is based on established well-recognized international methodologies for conformance testing and quality testing. For more information on mobile device forensic methodology please visit us at: http://www.cftt.nist.gov.

The Computer Forensic Tool Testing (CFTT) program is a joint project of the National Institute of Justice (NIJ), the research and development organization of the U.S. Department of Justice, and the National Institute of Standards and Technology's (NIST's) Law Enforcement Standards Office (OLES) and Information Technology Laboratory (ITL). CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense Cyber Crime Center, U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program, U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection, and the U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

The central requirement for a sound forensic examination of digital evidence is that the original evidence must not be modified (i.e., the examination or capture of digital data from a mobile device and associated media must be performed without altering the device or media content). In the event that data acquisition is not possible using current technology to access information without configuration changes to the device (e.g., loading a driver), the procedure must be documented.

2. Purpose

This document defines test assertions and test cases derived from requirements for mobile device forensic tools capable of acquiring the internal memory from smart phones, feature 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 smart phones, feature 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 the smart phones, feature 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 smart phone, feature 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 support for connectivity of the target device then the tool shall successfully recognize the target device via all tool-supported interfaces (e.g., cable, Bluetooth, IrDA).	Connect supported device via tool-supported interface(s); Acquire data.
MDT-CA-02	If connectivity between the mobile device 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., unplug cable) during acquisition.
MDT-CA-03	If a mobile device forensic tool completes 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-04	If a mobile device forensic tool completes acquisition of the target device without error then subscriber and equipment related information shall be presented in a useable format.	Acquisition of MSISDN, IMSI, IMEI, MEID/ESN
MDT-CA-	If a mobile device forensic tool completes acquisition of the target device without error	Acquisition of tool supported

05	then all supported data elements shall be presented in a useable format.	data elements
MDT-CA-06	If a mobile device forensic tool provides the user with an “***Acquire All***” device data objects acquisition option then the tool shall complete the acquisition of all data objects without error.	Acquire all supported device data objects
MDT-CA-07	If a mobile device forensic tool provides the user with an “***Select All***” individual device data objects then the tool shall complete the acquisition of all individually selected data objects without error.	Acquire all supported device data objects by individually selecting each supported data object
MDT-CA-08	If a mobile device forensic tool provides the user with the ability to “***Select Individual***” device data objects for acquisition then the tool shall acquire each exclusive data object without error.	Acquire each supported device data object individually
MDT-CA-09	If a mobile device forensic tool completes two consecutive logical acquisitions of the target device without error then the payload (data objects) on the mobile device shall remain consistent.	Perform two consecutive logical acquisitions; check mobile device for payload modifications
MDT-AO-01	If a mobile device forensic tool provides support for connectivity of the target UICC then the tool shall successfully recognize the target UICC via all tool-supported interfaces (e.g., PC/SC reader, proprietary reader, smart phone itself).	Connect UICC via tool-supported interface(s); Acquire data.
MDT-AO-02	If a mobile device forensic tool loses connectivity with the UICC reader 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-03	If a mobile device forensic tool completes acquisition of the target UICC without error then the subscriber and equipment related data shall be presented in a useable format.	Acquisition of SPN, ICCID, IMSI, MSISDN
MDT-AO-04	If a mobile device forensic tool completes acquisition of the target UICC without error then all acquired data shall be presented in a useable format.	Acquisition of all supported data objects
MDT-AO-05	If a mobile device forensic tool provides the user with an “***Acquire All***” UICC data objects acquisition option then the tool shall	Acquire all supported UICC data objects

	complete the acquisition of all data objects without error.	
MDT-AO-06	If a mobile device forensic tool provides the user with an “***Select All***” individual UICC data objects then the tool shall complete the acquisition of all individually selected data objects without error.	Acquire all supported UICC data objects by individually selecting each supported data object
MDT-AO-07	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.	Acquire each supported UICC data object individually
MDT-AO-08	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.	Alter case file; Attempt to re-open altered case file with application
MDT-AO-09	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.	Input correct UICC PIN; Acquire UICC
MDT-AO-10	If a mobile device forensic tool provides the examiner with the remaining number of authentication attempts then the application should provide an accurate count of the remaining PIN attempts.	Input incorrect PIN; Check tool output for correct number of remaining PIN attempts
MDT-AO-11	If a mobile device forensic tool provides the examiner with the remaining number of PUK attempts then the application should provide an accurate count of the remaining PUK attempts.	Input incorrect PUK; Check tool output for correct number of remaining PUK attempts
MDT-AO-12	If the mobile device forensic tool supports a physical acquisition of the target device then the tool shall complete the acquisition without error.	Physical Acquisition; Data is presented in a useable format.
MDT-AO-13	If the mobile device forensic tool supports proper display of non-ASCII characters then acquired data containing non-ASCII characters should be presented in their native format.	Acquisition of data containing non-ASCII characters
MDT-AO-14	If the mobile device forensic tool supports stand-alone acquisition of internal memory with the UICC present, then the contents of the UICC shall not be modified during internal memory acquisition.	Acquire data in Stand-alone acquisition mode; Check UICC status flags (e.g., Read, Unread) associated with text messages
MDT-AO-	If the mobile device forensic tool supports	Acquire data; Check known

15	hashing for individual data objects then the tool shall present the user with a hash value for each supported data object.	hash values for consistency
MDT-AO-16	If the mobile device forensic tool supports acquisition of GPS data then the tool shall present the user with the longitude and latitude coordinates for all GPS-related data in a useable format.	Acquire data; Check GPS data for consistency

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 support for connectivity of the target device then the tool shall successfully recognize the target device via all tool-supported interfaces (e.g., cable, Bluetooth, IrDA).
Test Action**:** Attempt to acquire data objects from a tool supported mobile device.
Conformance Indicator**:** Successful acquisition of at least one data object.

Assertion**:** MDT-CA-02 If connectivity between the mobile device 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 acquisition.
Conformance Indicator**:** Notification of acquisition disruption.

Assertion**:** MDT-AO-01 If a mobile device forensic tool provides support for connectivity of the target UICC then the tool shall successfully recognize the target UICC via all tool-supported interfaces (e.g., PC/SC reader, proprietary reader, smart phone itself).
Test Action**:** Attempt to acquire data objects present on a supported UICC.
Conformance Indicator**:** Successful acquisition of at least one data object.

Assertion**:** MDT-AO-02 If a mobile device forensic tool loses connectivity with the UICC reader then the tool shall notify the user that connectivity has been disrupted.
Test Action**:** Disrupting connectivity during stand-alone UICC acquisition.
Conformance Indicator**:** Notification of connectivity disruption during acquisition.

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-03 If a mobile device forensic tool completes 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.
Test Action**:** Acquire data objects outlined above in sections 5.2.1 through 5.5.2 from the target mobile device.
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-04 If a mobile device forensic tool completes acquisition of the target device without error then subscriber-related and equipment related information shall be presented in a useable format.
Test Action**:** Acquire subscriber and equipment related data (IMSI, IMEI, MEID/ESN, MSISDN) from the mobile device internal memory.
Conformance Indicator**:** Acquired data matches known data.

Assertion**:** MDT-AO-03 If a mobile device forensic tool completes acquisition of the target UICC without error then the subscriber-related and equipment related information shall shall be presented in a useable format.
Test Action**:** Acquire subscriber and equipment related data (SPN, ICCID, IMSI, MSISDN) from the SIM.
Conformance Indicator**:** Acquired data matches known data.

5.2.3 Internal Memory Data Acquisition

Assertion**:** MDT-CA-05 If a mobile device forensic tool completes acquisition of the target device without error then all supported data elements shall be presented in a useable format.
Test Action**:** Populate device with known data; acquire all supported data elements.
Conformance Indicator**:** Acquired data matches known data.

Assertion**:** MDT-AO-04 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**:** Populate the UICC with known data; acquire UICC data.
Conformance Indicator**:** Acquired data matches known data.

5.3 Tool Acquisition Variations

Assertion**:** MDT-CA-06 If a mobile device forensic tool provides the user with an "***Acquire All"*** data objects acquisition option then the tool shall complete the acquisition of all data objects without error.
Assertion**:** MDT-CA-07 If a mobile device forensic tool provides the user with an "***Select All"*** individual data objects then the tool shall complete the acquisition of all individually selected data objects without error.
Assertion**:** MDT-CA-08 If a mobile device forensic tool provides the user with the ability to "***Select Individual***" data objects for acquisition then the tool shall acquire each exclusive data object without error.
Test Action**:** Acquire device data objects by specifying ***acquire all*** which automatically selects all supported data objects for acquisition; ***select all*** which all supported data objects are individually selected for acquisition; ***select individual*** which each supported data object is selected exclusively for acquisition.
Conformance Indicator**:** Successful acquisition of the selected device data objects.

Assertion**:** MDT-AO-05 If a mobile device forensic tool provides the user with an "***Acquire All***" SIM data objects acquisition option then the tool shall complete the acquisition of all data objects without error.

Assertion**:** MDT-AO-06 If a mobile device forensic tool provides the user with an "***Select All***" individual UICC data objects then the tool shall complete the acquisition of all individually selected data objects without error.
Assertion: MDT-AO-07 If a mobile device forensic tool provides the user with the ability to "***Select Individual***" UICC data object for acquisition then the tool shall acquire each exclusive data object without error.
Test Action**:** Acquire UICC data objects by specifying ***acquire all*** which automatically selects all supported data objects for acquisition; ***select all*** which all supported data objects are individually selected for acquisition; ***select individual*** which each supported data object is selected exclusively for acquisition.
Conformance Indicator**:** Successful acquisition of the selected UICC data objects.

5.4 Device Data Not Modified

Assertion**:** MDT-CA-09 Data objects present on the device are not modified by acquisition.
Test Action**:** Perform two consecutive logical device internal memory acquisitions
Conformance Indicator**:** Data objects present on the mobile device remain consistent.

5.5 Case File/Data Protection

Assertion**:** MDT-AO-08 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 U(SIM) PIN/PUK Authentication

Assertion**:** MDT-AO-09 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-10 If a mobile device forensic tool provides the examiner with the remaining number of authentication attempts then the application should provide an accurate count of the remaining PIN attempts.
Test Action**:** Begin acquisition on a password protected UICC; Input incorrect PIN.
Conformance Indicator**:** The correct number of remaining PIN attempts are reported.

Assertion**:** MDT-AO-11 If a mobile device forensic tool provides the examiner with the remaining number of PUK attempts then the application should provide an accurate count of the remaining PUK attempts.
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 PUK attempts are reported.

5.7 Physical Acquisition

Assertion: MDT-AO-12 If the mobile device forensic tool supports a physical acquisition of the target device then the tool shall complete the acquisition without error.
Test Action: Acquire populated data from the internal memory of the target device.
Conformance Indicator: The acquired data matches the known data populated onto the device.

5.8 Non-ASCII Character Presentation

Assertion: MDT-AO-13 If the mobile device forensic tool supports display of non-ASCII characters then the application should present acquired data in their native format.
Test Action: Populate device and UICC with known non-ASCII data address book entries; Acquire data.
Conformance Indicator: Acquired data entries match the known list of non-ASCII address book entries.

5.9 Stand-alone Acquisition

Assertion: MDT-AO-14 If the mobile device forensic tool supports stand-alone acquisition of internal memory with the UICC present, then the contents of the UICC shall not be modified during internal memory acquisition.
Test Action: Populate the internal memory of the target UICC with text messages (i.e., SMS, EMS); Do not read text messages ensuring the status flags are marked as UNREAD; Acquire the internal memory of the mobile device in stand-alone acquisition mode.
Conformance Indicator: The status flags for text messages present on the UICC maintain their status as UNREAD.

5.10 Hashing

Assertion: MDT-AO-15 If the mobile device forensic tool supports hashing for individual data objects then the tool shall present the user with a hash value for each supported data object.
Test Action: Populate and acquire supported data objects.
Conformance Indicator: The hash values for acquired data objects match hash values of the populated data objects.

5.11 GPS Reporting

Assertion: MDT-AO-16 If the mobile device forensic tool supports acquisition of GPS data then the tool shall present the user with the longitude and latitude coordinates for all GPS-related data in a useable format.
Test Action: Populate the internal memory of the target device with known GPS coordinate data; Acquire the internal memory of the device.
Conformance Indicator: The acquired data matches the known data populated onto the device.

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-06. Section 6.2 lists optional test cases i.e., MDT-07 through MDT-24.

6.1 Test Cases for Core Features

MDT-01 Acquire mobile device internal memory over tool-supported interfaces (e.g., cable, Bluetooth, IrDA).

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

MDT-03 Acquire mobile device internal memory and review reported data via the preview-pane or generated reports for readability.

MDT-04 Acquire mobile device internal memory and review reported subscriber and equipment related information (e.g., IMSI, IMEI, MEID/ESN, MSISDN).

MDT-05 Acquire mobile device internal memory and review supported data elements (i.e., PIM data, call logs, SMS, MMS, stand-alone files: audio, pictures, video; application related data: documents, spreadsheets, presentations, social-media data and Internet related data: bookmarks, visited sites).

MDT-06 Acquire mobile device internal memory by selecting a combination of supported data elements.

This test case may be executed with the following variations:

Variation IM_Comp**:** Acquire mobile device internal memory by selecting the ***acquire all*** function, if supported by the tool.

Variation IM_SlctAll**:** Acquire mobile device internal memory by selecting all supported data objects individually for acquisition. *Note: This variation requires one acquisition of all individually selected data objects.*

Variation IM_SlctIndv**:** Acquire mobile device internal memory by performing an acquisition for each supported data object individually. *Note: This variation requires an acquisition for each individual supported data object.*

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.

UICC Acquisition

MDT-07 Acquire UICC memory over supported interfaces (e.g., PC/SC reader).

MDT-08 Begin UICC acquisition and interrupt connectivity by interface disengagement.

MDT-09 Acquire UICC memory and review reported subscriber and equipment related information (i.e., SPN, ICCID, IMSI, MSISDN).

MDT-10 Acquire UICC memory and review supported data elements (i.e., Abbreviated Dialing Numbers, Last Numbers Dialed, SMS/EMS text messages, and location related data: LOCI, GPRSLOCI).

MDT-11 Acquire UICC memory by selecting a combination of supported data elements.

This test case may be executed with the following variations:

***Variation UICC_Comp*:** Acquire mobile device UICC memory by selecting acquire all, if supported by the tool.

***Variation UICC_SlctAll*:** Acquire mobile device UICC memory by selecting all supported data elements individually for acquisition. Note: This variation requires one acquisition of all individually selected data objects.

***Variation UICC_SlctIndv*:** Acquire mobile device UICC memory by performing an acquisition for each supported data object individually. Note: This variation requires an acquisition for each individual supported data object.

Case File/Data Protection

MDT-12 After a successful mobile device internal memory, alter the case file via third-party means and attempt to re-open the case.

MDT-13 After a successful UICC acquisition, alter the case file via third-party means and attempt to re-open the case.

Password-Protected UICC

MDT-14 Attempt acquisition of a password-protected UICC.

PIN/PUK attempts

MDT-15 Begin acquisition on a PIN protected UICC to determine if the tool provides an accurate count of the remaining number of PIN attempts and if the PIN attempts are decremented when entering an incorrect value.

MDT-16 Begin acquisition on a UICC whose PIN attempts have been exhausted to determine if the tool provides an accurate count of the remaining number of PUK attempts and if the PUK attempts are decremented when entering an incorrect value.

Physical Acquisition

MDT-17 Perform a physical acquisition and review data output for readability.

MDT-18 Perform a physical acquisition and review reports for recoverable deleted data.

Non-ASCII Character Presentation

MDT-19 Acquire mobile device internal memory and review data containing non-ASCII characters.

MDT-20 Acquire UICC memory and review data containing non-ASCII characters.

Stand-alone acquisition

MDT-21 Perform a stand-alone mobile device internal memory acquisition and review the status flags for text messages present on the UICC.

Hashing

MDT-22 Acquire mobile device internal memory and review hash values for vendor supported data objects.

MDT-23 Acquire UICC memory and review hash values for vendor supported data objects.

GPS Reporting

MDT-24 Acquire mobile device internal memory and review data containing GPS longitude and latitude coordinates.

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

Requirements to Assertions (Core Features)

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

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

Requirements to Assertions (Optional Features)

		Assertions															
		01	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Requirements (Optional Features)	**MDT-RO-01**	•															
	MDT-RO-02		•														
	MDT-RO-03			•	•	•	•	•									
	MDT-RO-04								•								
	MDT-RO-05									•							
	MDT-RO-06										•						
	MDT-RO-07											•					
	MDT-RO-08												•				
	MDT-RO-09													•			
	MDT-RO-10														•		
	MDT-RO-11															•	
	MDT-RO-12																•

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

Assertions to Test Cases (Core Features)

		01	02	03	04	05	06
Assertions (Core Features)	**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						•

The following traceability matrices relate optional assertions to test cases.

Assertions to Test Cases (Optional Features)

		07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Assertions (Optional Features)	**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																		●