

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32

# Mobile Device Tool Test Assertions and Test Plan

Version 2.0



33  
34



36 **Abstract**

37 As mobile devices proliferate, incorporating a host of integrated features and capabilities, their use  
38 can be seen everywhere in our world today. Mobile communication devices contain a wealth of  
39 information. In the investigative community their use is not restricted to data recovery alone as in  
40 criminal cases, but also civil disputes and proceedings, and their aggregate use in research and  
41 criminal incident recreation continues to increase. Due to the exploding rate of growth in the  
42 production of new mobile devices appearing on the market each year is reason alone to pay  
43 attention to test measurement means and methods. The methods a tool uses to capture, process, and  
44 report data must incorporate a broad range of capabilities to meet the demand as a robust data  
45 acquisition tool. In general, a forensic examination conducted on a mobile device is only a small  
46 subset of the larger field of digital forensics. Consequentially, tools possessing an exhaustive array  
47 of capabilities to acquire data from these portable mobile devices are relatively few in number.

48

49 This paper defines assertions and test cases for mobile device applications capable of acquiring data  
50 from mobile devices (i.e., feature phones, smart phones, tables, associated media), to determine  
51 whether a specific tool meets the requirements producing measurable results. The assertions and  
52 test cases are derived from the requirements defined in the document entitled: [Mobile Device Tool  
53 Specification Version 2.0](#). Test cases describe the combination of test parameters required to test  
54 each assertion. Test assertions are described as general statements of conditions that can be  
55 checked after a test is executed. Each assertion appears in one or more test cases consisting of a test  
56 protocol and the expected test results. The test protocol specifies detailed procedures for setting up  
57 the test, executing the test, and measuring the test results.

58

59 Your comments and feedback are welcome; revisions of this document are available for download  
60 at: <http://www.cfft.nist.gov>.

61

---

• 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.



63 **TABLE OF CONTENTS**

64

65 1. Introduction ..... 1

66 2. Purpose ..... 1

67 3. Scope ..... 2

68 4. Test Assertions ..... 2

69 5. Assertion Measurement ..... 7

70 5.1 Connectivity..... 7

71 5.2 Data Acquisition and Interpretation..... 8

72 5.3 Non-ASCII Character Presentation ..... 9

73 5.4 Hashing..... 9

74 5.5 Case File/Data Protection ..... 9

75 5.6 UICC PIN/PUK Authentication ..... 10

76 5.7 Authentication Mechanism Bypass ..... 10

77 6. Abstract Test Cases ..... 11

78 6.1 Test Cases for Core Features ..... 11

79 6.2 Test Cases for Optional Features..... 11

80

81



83 **1. Introduction**

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

97  
98 The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of  
99 Homeland Security (DHS), the National Institute of Justice (NIJ), and the National Institute of  
100 Standards and Technology Special Program Office (SPO) and Information Technology Laboratory  
101 (ITL). CFTT is supported by other organizations, including the Federal Bureau of Investigation, the  
102 U.S. Department of Defense Cyber Crime Center, U.S. Internal Revenue Service Criminal  
103 Investigation Division Electronic Crimes Program, and the U.S. Department of Homeland  
104 Security's Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection  
105 and U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to  
106 practitioners, researchers, and other applicable users that the tools used in computer forensics  
107 investigations provide accurate results. Accomplishing this requires the development of  
108 specifications and test methods for computer forensics tools and subsequent testing of specific tools  
109 against those specifications

110  
111 The central requirement for a sound forensic examination of digital evidence is that the original  
112 evidence must not be modified (i.e., the examination or capture of digital data from a mobile device  
113 and associated media must be performed without altering the device or media content). In the event  
114 that data acquisition is not possible using current technology to access information without  
115 configuration changes to the device (e.g., loading a driver), the procedure must be documented.

116  
117 **2. Purpose**

118 This document defines test assertions and test cases derived from requirements for mobile device  
119 forensic tools capable of acquiring the internal memory from feature phones, smart phones, tablets  
120 and Universal Integrated Circuit Cards (UICCs). The test assertions are described as general  
121 statements of conditions that can be checked after a test is executed. Each assertion generates one  
122 or more test cases consisting of a test protocol and the expected test results. The test protocol  
123 specifies detailed procedures for setting up the test, executing the test, and measuring the test  
124 results.

125 **3. Scope**

126 The scope of this specification is limited to software tools capable of acquiring the internal memory of  
 127 feature phones, smart phones, tablets and UICCs. While mobile devices and tablets often have  
 128 companion PC-based software that provides users the ability to synchronize data between the device  
 129 and a personal computer this test assertion and test plan does not address device data synchronized  
 130 with personal computers. The assertions and test cases are specific to data stored in the internal  
 131 memory of feature phones, smart phones, tablets or UICCs. The test cases are general and capable  
 132 of being adapted to other types of mobile device forensic software.  
 133

134 **4. Test Assertions**

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

144  
 145

**Table 1: Test Assertions**

ID	Test Assertion	Comments
MDT-CA-01	If a mobile device forensic tool provides the user with an “ <i>Acquire All</i> ” 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 “ <i>Select All</i> ” 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 “ <i>Select Individual</i> ” 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

**DRAFT FOR COMMENTS**

	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

**DRAFT FOR COMMENTS**

	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 “ <i>Acquire All</i> ” 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 “ <i>Select All</i> ” UICC data objects then the tool shall complete the acquisition	Select all supported data objects; Begin acquisition

**DRAFT FOR COMMENTS**

	of all individually selected data objects without error.	
MDT-AO-11	If a mobile device forensic tool provides the user with a “ <i>Select Individual</i> ” 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

**DRAFT FOR COMMENTS**

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

146

147

148 **5. Assertion Measurement**

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

150 **5.1 Connectivity**

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

153  
154 **Assertion:** MDT-CA-01 If a mobile device forensic tool provides the user with an “*Acquire All*”  
155 data objects acquisition option then the tool shall complete the logical/filesystem acquisition of all  
156 data objects without error.

157 **Assertion:** MDT-CA-02 If a mobile device forensic tool provides the user with an “*Select All*”  
158 individual data objects then the tool shall complete the logical/filesystem acquisition of all  
159 individually selected data objects without error.

160 **Assertion:** MDT-CA-03 If a mobile device forensic tool provides the user with the ability to “*Select*  
161 *Individual*” data objects for acquisition then the tool shall shall complete the logical/filesystem  
162 acquisition for each exclusive data object without error.

163 **Assertion:** MDT-AO-01 If the mobile device forensic tool supports a physical acquisition of the  
164 target device then the tool shall complete the acquisition without error.

165 **Assertion:** MDT-AO-09 If a mobile device forensic tool provides the user with an “*Acquire All*”  
166 UICC data objects acquisition option then the tool shall complete the acquisition of all data objects  
167 without error.

168 **Assertion:** MDT-AO-10 If a mobile device forensic tool provides the user with an “*Select All*”  
169 UICC data objects then the tool shall complete the acquisition of all individually selected data  
170 objects without error.

171 **Assertion:** MDT-AO-11 If a mobile device forensic tool provides the user with the ability to “*Select*  
172 *Individual*” UICC data objects for acquisition then the tool shall acquire each exclusive data object  
173 without error.

174 **Test Action:** Acquire target mobile device / UICC data objects by specifying an acquisition  
175 variation: *acquire all, select all, select individual*.

176 **Conformance Indicator:** Successful acquisition of at least one data object.

177  
178 **Assertion:** MDT-CA-04 If connectivity between the mobile device and mobile device forensic tool  
179 is disrupted for a logical/filesystem acquisition then the tool shall notify the user that connectivity  
180 has been disrupted.

181 **Assertion:** MDT-AO-02 If connectivity between the mobile device and mobile device forensic tool  
182 for a physical acquisition is disrupted then the tool shall notify the user that connectivity has been  
183 disrupted.

184 **Assertion:** MDT-AO-15 If connectivity between the UICC and mobile device forensic tool is  
185 disrupted then the tool shall notify the user that connectivity has been disrupted.

186 **Test Action:** Disrupt connectivity during mobile device or UICC acquisition.

187 **Conformance Indicator:** Notification of acquisition disruption.

188

189

190

191 **5.2 Data Acquisition and Interpretation**

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

194 **5.2.1 Presentation**

195 *Assertion:* MDT-CA-05 If a mobile device forensic tool completes logical/file system acquisition of  
196 the target device without error then the tool shall have the ability to present acquired data objects in  
197 a useable format via either a preview-pane or generated report.

198 *Assertion:* MDT-AO-03 If a mobile device forensic tool completes physical acquisition of the target  
199 device without error then the tool shall have the ability to present acquired data objects in a useable  
200 format via either a preview-pane, generated report or output file.

201 *Assertion:* MDT-AO-16 If a mobile device forensic tool completes acquisition of the target UICC  
202 without error then acquired data shall be presented in a useable format.

203 *Test Action:* Acquire supported data objects from the target mobile device / UICC.

204 *Conformance Indicator:* Acquired data is presented in either a preview-pane view or generated  
205 report.  
206

207 **5.2.2 Subscriber and Equipment Related Data**

208 *Assertion:* MDT-CA-06 If a mobile device forensic tool completes logical/file system acquisition of  
209 the target device without error then subscriber-related and equipment related information shall be  
210 presented in a useable format.

211 *Assertion:* MDT-AO-04 If a mobile device forensic tool completes physical acquisition of the target  
212 device without error then subscriber-related and equipment related information (e.g., IMSI, IMEI,  
213 MEID/ESN, MSISDN) shall be presented in a useable format.

214 *Assertion:* MDT-AO-17 If a mobile device forensic tool completes acquisition of the target UICC  
215 without error then the subscriber-related and equipment related information (i.e., SPN, ICCID,  
216 IMSI, MSISDN) shall be presented in a useable format.

217 *Test Action:* Acquire subscriber and equipment related data (IMSI, IMEI, MEID/ESN, MSISDN)  
218 from the target mobile device / UICC.

219 *Conformance Indicator:* Acquired data matches known data.  
220

221 **5.2.3 Data Acquisition**

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

227 *Assertion:* MDT-AO-05 If a mobile device forensic tool completes physical acquisition of the target  
228 device without error then all supported data elements: PIM data (address book, calendar, notes), call  
229 logs, SMS, MMS, chat logs, stand-alone files (audio, pictures, video), application, social media and  
230 Internet related data (bookmarks, browsing history), email and GPS data shall be presented in a  
231 useable format.

232 *Assertion:* MDT-AO-18 If a mobile device forensic tool completes acquisition of the target UICC  
233 without error then all supported data elements (e.g., Abbreviated Dialing Numbers, Last Numbers

234 Dialed, SMS text messages, and location related data: LOCI, GPRSLOCI) shall be presented in a  
235 useable format.

236 **Test Action:** Populate target mobile device / UICC with known data; acquire all supported data  
237 objects.

238 **Conformance Indicator:** Acquired data matches known data.

### 239 **5.3 Non-ASCII Character Presentation**

240 **Assertion:** MDT-CA-08 If the mobile device forensic tool completes logical/filesystem acquisition  
241 of the target device without error, acquired data containing non-Latin characters shall be presented  
242 in their native format.

243 **Assertion:** MDT-AO-06 If the mobile device forensic tool completes physical acquisition of the  
244 target device without error, acquired data containing non-Latin characters shall be presented in their  
245 native format.

246 **Assertion:** MDT-AO-19 If the mobile device forensic tool completes acquisition of the target UICC  
247 without error, acquired data containing non-Latin characters shall be presented in their native  
248 format.

249 **Test Action:** Populate target mobile device / UICC with known non-ASCII data; Acquire data.

250 **Conformance Indicator:** Acquired non-ASCII data is presented in its native format.

### 251 **5.4 Hashing**

252 **Assertion:** MDT-CA-09 If the mobile device forensic tool completes logical/filesystem acquisition  
253 of the target device without error, hash values are reported for acquired data objects or overall case  
254 file.

255 **Assertion:** MDT-AO-07 If the mobile device forensic tool completes physical acquisition of the  
256 target device without error, hash values are reported for acquired data objects or overall case file.

257 **Assertion:** MDT-AO-20 If the mobile device forensic tool completes acquisition of the target UICC  
258 without error, hash values are reported for acquired data objects or overall case file.

259 **Test Action:** Populate target mobile device / UICC with known data; acquire supported data objects.

260 **Conformance Indicator:** Hash values are reported for individually acquired data objects or overall  
261 case file.

262

### 263 **5.5 Case File/Data Protection**

264 **Assertion:** MDT-CA-10 If the logical/filesystem generated case file or individual data objects are  
265 modified via third-party means then the tool shall provide protection mechanisms disallowing or  
266 reporting data modification.

267 **Assertion:** MDT-AO-08 If the case file or individual data objects for a physical acquisition are  
268 modified via third-party means then the tool shall provide protection mechanisms disallowing or  
269 reporting data modification.

270 **Assertion:** MDT-AO-21 If the case file or individual data objects are modified via third-party  
271 means then the tool shall provide protection mechanisms disallowing or reporting data modification.

272 **Test Action:** Modify a saved case file with a hex editor; re-open the modified case file with the  
273 mobile device tool.

274 **Conformance Indicator:** Notification that the case file has been altered.

275

276 **5.6 UICC PIN/PUK Authentication**

277 *Assertion:* MDT-AO-12 If the UICC is password-protected then the mobile device forensic tool  
278 shall provide the examiner with the opportunity to input the PIN before acquisition.

279 *Test Action:* Password protect the target UICC; Attempt to acquire data from the password-  
280 protected UICC by entering the password.

281 *Conformance Indicator:* The tool successfully acquires all requested data.

282  
283 *Assertion:* MDT-AO-13 If a mobile device forensic tool provides the examiner with the remaining  
284 number of authentication attempts for a UICC acquisition then the application should provide an  
285 accurate count of the remaining PIN attempts when entering an incorrect PIN.

286 *Test Action:* Begin acquisition on a password protected UICC; Input incorrect PIN.

287 *Assertion:* MDT-AO-14 If a mobile device forensic tool provides the examiner with the remaining  
288 number of PUK attempts for a UICC acquisition then the application should provide an accurate  
289 count of the remaining PUK attempts when entering an incorrect PUK.

290 *Test Action:* Begin acquisition on a password protected UICC whose PIN attempts have been  
291 exhausted; Input incorrect PUK.

292 *Conformance Indicator:* The correct number of remaining number of PIN/PUK attempts are  
293 reported.

294

295 **5.7 Authentication Mechanism Bypass**

296 *Assertion:* MDT-AO-22 If a mobile device forensic tool provides the ability to circumvent a  
297 password-protected device then the tool shall complete the bypass attempt without error.

298 *Test Action:* Attempt authentication mechanism bypass of a password protected mobile device /  
299 UICC.

300 *Conformance Indicator:* The mobile device forensic tool attempts authentication bypass without  
301 error.

302

303

304 **6. Abstract Test Cases**

305 Abstract test cases describe the combinations of test parameters required to fully test each assertion  
306 and the results expected for the given combination of test parameters. The test cases are abstract in  
307 that they do not prescribe the exact environment in which the tests are to be performed. They are  
308 written at the next level above the actual test environment, thus abstract test cases allowing  
309 substitution and variation of setup environment variables under dissimilar products and options  
310 prior to engagement in official testing. Section 6.1 lists test cases i.e., MDT-01 through MDT-03.  
311 Section 6.2 lists optional test cases i.e., MDT-04 through MDT-10.  
312

313 **6.1 Test Cases for Core Features**

314 **MDT-01** Acquire mobile device internal memory using tool-supported interfaces (e.g., cable,  
315 Bluetooth) by selecting a combination of supported data elements. (*Variation IM\_Comp,*  
316 *Variation IM\_SlctAll, Variation IM\_SlctIndv*)

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

319 **MDT-03** Perform a logical/filesystem data extraction of the target mobile device and review data  
320 output.  
321

322 **6.2 Test Cases for Optional Features**

323 The following test cases are defined for tool features that might be implemented for some mobile  
324 device forensic tools. If a tool provides the optional feature, the tool is tested as if the test case were  
325 core. If the tool does not provide the capability defined, the test case does not apply.  
326

327 Physical Acquisition

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

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

332 **MDT-06** Perform a physical data extraction of the target mobile device and review data output.  
333

334 UICC Acquisition

335 **MDT-07** Acquire UICC internal memory using tool-supported interfaces (e.g., PC/SC reader) by  
336 selecting a combination of supported data elements. (*Variation IM\_Comp, Variation IM\_SlctAll,*  
337 *Variation IM\_SlctIndv*)

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

339 **MDT-09** Acquire UICC internal memory and review data output.  
340

341 Bypass Authentication Mechanisms

342 **MDT-10** Begin authentication mechanism attempt by establishing connectivity to the mobile  
343 device.  
344  
345  
346

347  
 348 The following traceability matrices relate core requirements to core assertions. The requirements are  
 349 defined in the document entitled: [Mobile Device Tool Specification v2.0](#).  
 350

351 **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					•	•	•	•	•	•

352  
 353 The following traceability matrices relate optional requirements to optional test assertions.  
 354

355 **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									•	•	•

356

		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											•	

357  
 358

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

360

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

362

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			•

363

364 The following traceability matrices relate optional assertions to test cases.

365

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

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

367