1 January 6, 2008

GSM Mobile Device and Associated Media Tool Test Assertions and Test Plan

Version 1.3

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

Abstract

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

This paper defines assertions and test cases for mobile device applications capable of acquiring data from mobile devices operating over a Global System for Mobile communication (GSM) network, used 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: GSM Mobile Device and Associated Media 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/mobile_devices.htm.

---

[*] NIST does not endorse nor recommend products or trade names identified in this paper. All products used in this paper are mentioned for use in research and testing by NIST.

TABLE OF CONTENTS

1.   Introduction

The need to ensure the reliability of mobile device forensic tools intensifies, as the embedded intelligence and ever-increasing storage capabilities of mobile devices expand. The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing computer forensic software tools. This is accomplished by the development of both specific and common rules that govern tool specifications. We adhere to a disciplined testing procedure, established test criteria, test sets, and test hardware requirements, that result in providing necessary feedback information to toolmakers so they can improve their tool's effectiveness; end users benefit in that they gain vital information making them more informed about choices for acquiring and using computer forensic tools, and lastly, we impart knowledge to interested parties by increasing their understanding of a specific tool's capability. Our approach for testing computer forensic tools is based on established well-recognized international methodologies for conformance testing and quality testing. For more information on mobile device forensic methodology please visit us at: 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) Office of Law Enforcement Standards (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 Global System for Mobile communication (GSM) devices and related media (i.e., Subscriber Identity Module [SIM]). 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 GSM devices and related media (i.e., SIM). The specifications are general and capable of being adapted to other types of mobile device software tailored for non-GSM devices.

4.   Test Assertions

The primary goal of test assertions A_IM-01 – A_SIMO-70, presented below in Table 1, is to determine the tools ability to acquire specific data elements pre-populated onto the device without modification. The ID column identifies the medium (i.e., mobile device internal memory, Subscriber Identity Module [SIM] card) the test is being performed on. For instance A_IM-01 (i.e., Assertion_InternalMemory-#) is a mobile device internal memory (IM) assertion, A_SIM-23 (i.e., Assertion_SubscriberIdentityModule-#) is a Subscriber Identity Module (SIM) internal memory assertion. Assertions A_IMO-# (i.e., Assertion_InternalMemoryOptional-#) or A_SIMO-# (i.e., Assertion_SubscriberIdentityModule Optional-#) are optional assertions and only tested if a tool supports the feature. If the tool does not provide the capability defined, the test assertion does not apply.   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
A_IM-01	If a cellular forensic tool provides support for connectivity of the target device then the tool shall successfully recognize the target device via all vendor supported interfaces (e.g., cable, Bluetooth, IrDA).	Connect supported device via supported interface(s); Begin acquisition to determine if successful
A_IM-02	If a cellular forensic tool attempts to connect to a non-supported device then the tool shall have the ability to identify that the device is not supported.	Connect a non-supported device; Begin acquisition to determine if application provides a message that the device is not supported
A_IM-03	If a cellular forensic tool encounters disengagement between the device and application then the application shall notify the user that connectivity has been disrupted.	Begin acquisition; Disconnect interface or interrupt connectivity (i.e., unplug cable) during acquisition to determine if the tool provides an error message
A_IM-04	If a cellular forensic tool successfully completes acquisition of the target device then the tool shall have the ability to present acquired data elements in a human-readable	Examine acquired data via supported report for readability

	format via either a preview-pane or generated report.	
A_IM-05	If a cellular forensic tool successfully completes acquisition of the target device then subscriber related information shall be presented in a human-readable format without modification.	MSISDN is reported
A_IM-06	If a cellular forensic tool successfully completes acquisition of the target device then equipment related information shall be presented in a human-readable format without modification.	IMEI is reported
A_IM-07	If a cellular forensic tool successfully completes acquisition of the target device then all known address book entries shall be presented in a human-readable format without modification.	Address book entries and associated data (i.e., phone number) are reported
A_IM-08	If a cellular forensic tool successfully completes acquisition of the target device then all known maximum length address book entries shall be presented in a human-readable format without modification.	Maximum length address book entries (i.e., contact name) are reported in totality
A_IM-09	If a cellular forensic tool successfully completes acquisition of the target device then all known address book entries containing special characters shall be presented in a human-readable format without modification.	Address book entries containing special characters (e.g., #, !, *) are reported
A_IM-10	If a cellular forensic tool successfully completes acquisition of the target device then all known address book entries containing blank names shall be presented in a human-readable format without modification.	Address book entries containing blank names are reported
A_IM-11	If a cellular forensic tool successfully completes acquisition of the target device then all known email addresses associated with address book entries shall be presented in a human-readable format without modification.	Address book entries containing an email addresses are reported
A_IM-12	If a cellular forensic tool successfully completes acquisition of the target device then all known graphics associated with	Address book entries containing an graphic are reported

	address book entries shall be presented in a human-readable format without modification.	
A_IM-13	If a cellular forensic tool successfully completes acquisition of the target device then all known datebook, calendar, note entries shall be presented in a human-readable format without modification.	Datebook/Calendar, notes entries are reported
A_IM-14	If a cellular forensic tool successfully completes acquisition of the target device then all maximum length datebook, calendar, note entries shall be presented in a human readable format without modification.	Maximum length Datebook/Calendar, notes entries are reported
A_IM-15	If a cellular forensic tool successfully completes acquisition of the target device then all call logs (incoming/outgoing) shall be presented in a human-readable format without modification.	Incoming and outgoing calls are reported
A_IM-16	If a cellular forensic tool successfully completes acquisition of the target device then all text messages (i.e., SMS, EMS) messages shall be presented in a human-readable format without modification.	Text messages are reported
A_IM-17	If a cellular forensic tool successfully completes acquisition of the target device then all MMS messages and associated audio shall be presented properly without modification.	MMS messages and associated audio data are reported
A_IM-18	If a cellular forensic tool successfully completes acquisition of the target device then all MMS messages and associated images shall be presented properly without modification.	MMS messages and associated graphical images are reported
A_IM-19	If a cellular forensic tool successfully completes acquisition of the target device then all MMS messages and associated video shall be presented properly without modification.	MMS messages and associated video data are reported
A_IM-20	If a cellular forensic tool successfully completes acquisition of the target device then all stand-alone audio files shall be playable via either an internal application or suggested third-party application without	Stand-alone audio files are reported

	modification.	
A_IM-21	If a cellular forensic tool successfully completes acquisition of the target device then all stand-alone image files shall be viewable via either an internal application or suggested third-party application without modification.	Stand-alone graphic files (i.e. images) are reported
A_IM-22	If a cellular forensic tool successfully completes acquisition of the target device then all stand-alone video files shall be viewable via either an internal application or suggested third-party application without modification.	Stand-alone video files are reported
A_SIM-23	If a cellular forensic tool provides support for connectivity of the target SIM then the tool shall successfully recognize the target SIM via all vendor supported interfaces (e.g., PC/SC reader, proprietary reader).	Connect SIM via supported interface; Begin acquisition to determine if successful
A_SIM-24	If a cellular forensic tool attempts to connect to a non-supported SIM then the tool shall have the ability to identify that the SIM is not supported.	Connect a non-supported SIM; Begin acquisition to determine if application provides a message that the device is not supported
A_SIM-25	If a cellular forensic tool encounters disengagement between the SIM reader and application then the application shall notify the user that connectivity has been disrupted.	Begin acquisition; Disconnect interface or interrupt connectivity (i.e., unplug cable) during acquisition to determine if the tool provides an error message
A_SIM-26	If the SIM is password-protected then the cellular forensic tool shall provide the examiner with the opportunity to input the PIN before acquisition.	Aquire a password-protected SIM
A_SIM-27	If a cellular forensic tool successfully completes acquisition of the target SIM then the tool shall have the ability to present acquired data in a human-readable format via either preview-pane or generated report.	Examine acquired data via supported report for readability
A_SIM-28	If a cellular forensic tool successfully completes acquisition of the target SIM then the SPN shall be presented in a human-readable format without modification.	Service Provider Name is reported

A_SIM-29	If a cellular forensic tool successfully completes acquisition of the target SIM then the ICCID shall be presented in a human-readable format without modification.	ICCID is reported
A_SIM-30	If a cellular forensic tool successfully completes acquisition of the target SIM then the IMSI shall be presented in a human-readable format without modification.	IMSI is reported
A_SIM-31	If a cellular forensic tool successfully completes acquisition of the target SIM then the MSISDN shall be presented in a human-readable format without modification.	MSISDN is reported
A_SIM-32	If a cellular forensic tool successfully completes acquisition of the target SIM then all Abbreviated Dialing Numbers (ADN) shall be presented in a human-readable format without modification.	ADN and associated data (i.e., phone number) are reported
A_SIM-33	If a cellular forensic tool successfully completes acquisition of the target SIM then all Last Numbers Dialed (LND) shall be presented in a human-readable format without modification.	LND are reported
A_SIM-34	If a cellular forensic tool successfully completes acqusition of the target SIM then all SMS text messages shall be presented in a human-readable format without modification.	Incoming SMS messages are reported
A_SIM-35	If a cellular forensic tool successfully completes acqusition of the target SIM then all EMS text messages shall be presented in a human-readable format without modification.	Incoming EMS messages are reported
A_SIM-36	If a cellular forensic tool successfully completes acquisition of the target SIM then all location related data (i.e., LOCI) shall be presented in a human-readable format without modification.	Location data is reported
A_SIM-37	If a cellular forensic tool successfully completes acquisition of the target SIM then all location related data (i.e., GRPSLOCI) shall be presented in a human-readable format without modification.	GPRS Location data is reported

A_IMO-38	If a cellular forensic tool successfully completes acquisition of the target device then the tool shall present the acquired data without modification via supported generated report formats.	Check report output with known data elements for consistency and completeness
A_IMO-39	If a cellular forensic tool successfully completes acquisition of the target device then the tool shall present the acquired data without modification in a preview-pane view.	Check preview-pane output with known data elements for consistency and completeness
A_IMO-40	If a cellular forensic tool provides a preview-pane view and a generated report of the acquired data then the reports shall maintain consistency of all reported data elements.	Check generated report and preview-pane for consistency if both supported
A_IMO-41	If modification is attempted to the case file or individual data elements via third-party means then the tool shall provide protection mechanisms disallowing or reporting data modification.	Data integrity
A_IMO-42	If the cellular forensic tool supports a physical acquisition of the target device then the tool shall successfully complete the acquisition and present the data in a human-readable format.	Physical acquisition readability of acquired data
A_IMO-43	If the cellular forensic tool supports a physical acquisition of address book entries present on the target device then the tool shall report recoverable deleted data or address book data remnants in a human-readable format.	Physical acquisition; Recovery of deleted address book entries
A_IMO-44	If the cellular forensic tool supports a physical acquisition of calendar, tasks, or notes present on the target device then the tool shall report recoverable deleted calendar, tasks, or note data remnants in a human-readable format.	Physical acquisition; Recovery of deleted calendar, notes entries
A_IMO-45	If the cellular forensic tool supports a physical acquisition of call logs present on the target device then the tool shall report recoverable deleted call or call log data remnants in a human-readable format.	Physical acquisition; Recovery of deleted call logs
A_IMO-46	If the cellular forensic tool supports a physical acquisition of SMS messages	Physical acquisition; Recovery of deleted SMS

	present on the target device then the tool shall report recoverable deleted SMS messages or SMS message data remnants in a human-readable format.	messages
A_IMO-47	If the cellular forensic tool supports a physical acquisition of EMS messages present on the target device then the tool shall report recoverable deleted EMS messages or EMS message data remnants in a human-readable format.	Physical acquisition; Recovery of deleted EMS messages
A_IMO-48	If the cellular forensic tool supports a physical acquisition of audio files present on the target device then the tool shall report recoverable deleted audio data or audio file data remnants in a human-readable format.	Physical acquisition; Recovery of deleted audio files
A_IMO-49	If the cellular forensic tool supports a physical acquisition of graphic files present on the target device then the tool shall report recoverable deleted graphic file data or graphic file data remnants in a human-readable format.	Physical acquisition; Recovery of deleted image files
A_IMO-50	If the cellular forensic tool supports a physical acquisition of video files present on the target device then the tool shall report recoverable deleted video file data or video file data remnants in a human-readable format.	Physical acquisition; Recovery of deleted video files
A_IMO-51	If the cellular forensic tool supports SIM access card creation then the card creation shall be completed without errors via manufacturer suggested protocols.	Access cards characteristics should be consistent with vendor documentation. Cards may act as a radio-isolation card or may contain data objects from a target SIM
A_IMO-52	If the cellular forensic tool supports log creation then the application should present the log files outlining the acquisition process in a human-readable format.	Log file creation
A_IMO-53	If the cellular forensic tool supports proper display of foreign language character sets then the application should present address book entries containing foreign language characters in their native format without	Acquisition and display of foreign language character sets

	modification.	
A_IMO-54	If the cellular forensic tool supports proper display of foreign language character sets then the application should present text messages containing foreign language characters in their native format without modification.	Acquisition and display of foreign language character sets
A_IMO-55	If the cellular forensic tool supports stand-alone acquisition of internal memory with the SIM present, then the contents of the SIM shall not be modified during internal memory acquisition.	Stand-alone acquisition protects modification of SIM status flags (e.g., Read, Unread) associated with text messages
A_IMO-56	If the cellular forensic tool supports hashing for individual data objects then the tool shall present the user with a hash value for each supported data object.	Individual data object hash reporting
A_IMO-57	If the cellular forensic tool supports hashing the overall case file then the tool shall present the user with one hash value representing the entire case data.	Case file hash reporting
A_SIMO-58	If a cellular forensic tool successfully completes acquisition of the target media (i.e., SIM) then the tool shall present the acquired data in a human-readable format without modification via supported generated report formats.	Check report output with known data elements for consistency and completeness
A_SIMO-59	If a cellular forensic tool successfully completes acquisition of the SIM then the tool shall present the acquired data in a human-readable format without modification in a preview-pane view.	Check preview-pane output with known data elements for consistency and completeness
A_SIMO-60	If a cellular forensic tool provides a preview-pane view and a generated report of the acquired data then the reports shall maintain consistency of all reported data elements.	Check generated report and preview-pane for consistency if both supported
A_SIMO-61	If modification is attempted to the case file or individual data elements via third-party means then the tool shall provide protection mechanisms disallowing or reporting data modification.	Data-integrity
A_SIMO-62	If the cellular forensic tool successfully completes acquisition of the target SIM and recoverable deteled SMS messages exist	Recovery of deleted SMS messages

	then the tool shall present recoverable deleted data in a human-readable format without modification.	
A_SIMO-63	If the cellular forensic tool successfully completes acquisition of the target SIM and recoverable deleted EMS messages exist then the tool shall present recoverable deleted data in a human-readable format without modification.	Recovery of deleted EMS messages
A_SIMO-64	If a cellular forensic tool supports the creation of log files then the application should present the log files in a human-readable format outlining the acquisition process.	Log file creation
A_SIMO-65	If the cellular forensic tool supports proper display of foreign language character sets then the application should present abbreviated dialing numbers (ADN) containing foreign language characters in their native format without modification.	Acquisition and display of foreign language character sets
A_SIMO-66	If the cellular forensic tool supports proper display of foreign language character sets then the application should present text messages containing foreign language characters in their native format without modification.	Acquisition and display of text messages containing foreign language character sets
A_SIMO-67	If a cellular 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.	Remaining PIN attempts displayed
A_SIMO-68	If a cellular 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.	Remaining PUK attempts displayed
A_SIMO-69	If the cellular forensic tool supports hashing for individual data objects then the tool shall present the user with a hash value for each supported data object.	Individual data object hash
A_SIMO-70	If the cellular forensic tool supports hashing for the overall case file then the tool shall present the user with one hash value	Case file hash

	representative of the entire case data.	

136

137

5.   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 5.1 lists test cases i.e., Cellular Forensic Tool-Internal Memory-01 (CFT-IM-01) through CFT-IM-10 and Cellular Forensic Tool-Subscriber Identity Module-01 (CFT-SIM-01) through CFT-SIM-10. Section 5.2 lists optional test cases i.e., Cellular Forensic Tool-Internal Memory Optional-01 (CFT-IMO-01) through CFT-IMO-12 and Cellular Forensic Tool-Subscriber Identity Module Optional-01 (CFT-SIMO-01) through CFT-SIMO-11.

5.1   Test Cases for Core Features

Mobile Device Internal Memory Test Cases:

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

CFT-IM-02   Attempt internal memory acquisition of a non-supported mobile device.

CFT-IM-03   Begin mobile device internal memory acquisition and interrupt connectivity by interface disengagement.

CFT-IM-04   Acquire mobile device internal memory and review reported data via the preview-pane or generated reports for readability.

CFT-IM-05   Acquire mobile device internal memory and review reported subscriber and equipment related information (i.e., IMEI, MSISDN).

CFT-IM-06   Acquire mobile device internal memory and review reported PIM related data.

CFT-IM-07   Acquire mobile device internal memory and review reported call logs.

CFT-IM-08   Acquire mobile device internal memory and review reported text messages.

CFT-IM-09   Acquire mobile device internal memory and review reported MMS multi-media related data (i.e., text, audio, graphics, video).

CFT-IM-10   Acquire mobile device internal memory and review reported stand-alone multi-media data (i.e., audio, graphics, video).

SIM Internal Memory Test Cases:

CFT-SIM-01 Acquire SIM over supported interfaces (e.g., PC/SC reader, proprietary reader).

CFT-SIM-02 Attempt acquisition of a non-supported SIM.

CFT-SIM-03 Begin SIM acquisition and interrupt connectivity by interface disengagement.

CFT-SIM-04 Attempt acquisition on a password-protected SIM.

CFT-SIM-05 Acquire SIM internal memory and review reported data via the preview-pane or generated reports for readability.

CFT-SIM-06 Acquire SIM internal memory and review reported subscriber and equipment related information (i.e., SPN, ICCID, IMSI, MSISDN).

181   **CFT-SIM-07** Acquire SIM internal memory and review reported Abbreviated Dialing Numbers
182   (ADN).
183   **CFT-SIM-08** Acquire SIM internal memory and review reported Last Numbers Dialed (LND).
184   **CFT-SIM-09** Acquire SIM internal memory and review reported text messages (i.e., SMS, EMS).
185   **CFT-SIM-10** Acquire SIM internal memory and review reported location related data (i.e., LOCI,
186   GPRSLOCI).
187

188 **5.2   Test Cases for Optional Features**

189   The following test cases are defined for tool features that might be implemented for some cellular
190   forensic tools. If a tool provides the optional feature, the tool is tested as if the test case were core.
191   If the tool does not provide the capability defined, the test case does not apply.
192

193   <u>**Optional Mobile Device Internal Memory Test Cases**</u>**:**
194   **CFT-IMO-01** Acquire mobile device internal memory and review reported data via supported
195   generated report formats.
196   **CFT-IMO-02** Acquire mobile device internal memory and review reported data via the preview-
197   pane.
198   **CFT-IMO-03** Acquire mobile device internal memory and compare reported data via the preview-
199   pane and supported generated reports.
200   **CFT-IMO-04** After a successful mobile device internal memory acquisition, alter the case file via
201   third party means and attempt to re-open the case.
202   **CFT-IMO-05** Perform a physical acquisition and review data output for readability.
203   **CFT-IMO-06** Perform a physical acquisition and review reports for recoverable deleted data.
204   **CFT-IMO-07** Create a SIM access card via vendor documentation.
205   **CFT-IMO-08** Acquire mobile device internal memory and review generated log files.
206   **CFT-IMO-09** Acquire mobile device internal memory and review data containing foreign language
207   characters.
208   **CFT-IMO-10** Perform a stand-alone mobile device internal memory acquisition and review the
209   status flags for text messages present on the SIM.
210   **CFT-IMO-11** Acquire mobile device internal memory and review hash values for vendor supported
211   data objects.
212   **CFT-IMO-12** Acquire mobile device internal memory and review the overall case file hash.
213
214
215   <u>**Optional SIM Internal Memory Test Cases**</u>**:**
216   **CFT-SIMO-01** Acquire SIM internal memory and review acquired data via supported generated
217   report formats.
218   **CFT-SIMO-02** Acquire SIM internal memory and review acquired data via the preview-pane.
219   **CFT-SIMO-03** Acquire SIM internal memory and compare acquired data via the preview-pane and
220   supported generated reports.
221   **CFT-SIMO-04** After a successful SIM internal memory acquisition, alter the case file via third
222   party means and attempt to re-open the case.
223   **CFT-SIMO-05** Acquire SIM internal memory and review reports for recoverable deleted data.
224   **CFT-SIMO-06** Acquire SIM internal memory and review generated log files.
225   **CFT-SIMO-07** Acquire SIM internal memory and review data containing foreign language

226		characters.
227	**CFT-SIMO-08**	Begin acquisition on a PIN protected SIM to determine if the tool provides an
228		accurate count of the remaining number of PIN attempts and if the PIN attempts are
229		decremented when entering an incorrect value.
230	**CFT-SIMO-09**	Begin acquistion on a SIM whose PIN attempts have been exhausted to determine
231		if the tool provides an accurate count of the remaining number of PUK attempts and
232		if the PUK attempts are decremented when entering an incorrect value.
233	**CFT-SIMO-10**	Acquire SIM internal memory and review hash values for vendor supported data
234		objects.
235	**CFT-SIMO-11**	Acquire SIM internal memory and review the overall case file hash.
236		

237 The following traceability matrices relate core requirements to core test cases. The requirements are
238 defined in the document entitled: GSM Mobile Device and Associated Media Tool Specification.
239
240 **Requirements to Test Cases (Device Memory - Core Features)**

		Test Cases									
		01	02	03	04	05	06	07	08	09	10
Device Memory Requirements (Core Features)	CFT-IM-01	●									
	CFT-IM-02		●								
	CFT-IM-03	●		●							
	CFT-IM-04	●			●						
	CFT-IM-05	●			●	●	●	●	●	●	●

241
242 **Requirements to Test Cases (SIM Memory – Core Features)**

		Test Cases									
		01	02	03	04	05	06	07	08	09	10
SIM Memory Requirements (Core Features)	CFT-SIM-01	●									
	CFT-SIM-02		●								
	CFT-SIM-03	●		●							
	CFT-SIM-04	●			●						
	CFT-SIM-05	●				●					
	CFT-SIM-06	●				●	●	●	●	●	●

243
244
245

246   The following traceability matrices relate optional requirements to optional test cases.
247
248   **Requirements to Test Cases (Device Memory – Optional Features)**

		Test Cases											
		01	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**
Device Memory Requirements (Optional Features)	**CFT-IMO-01**	●		●									
	CFT-IMO-02		●	●									
	CFT-IMO-03				●								
	CFT-IMO-04	●	●			●	●						
	CFT-IMO-05							●					
	CFT-IMO-06								●				
	CFT-IMO-07	●	●							●			
	CFT-IMO-08	●	●								●		
	CFT-IMO-09	●	●									●	
	CFT-IMO-10	●	●										●

249
250

251 **Requirements to Test Cases (SIM Memory – Optional Features)**

		Test Cases										
		01	02	03	04	05	06	07	08	09	10	11
SIM Memory Requirements (Optional Features)	**CFT-SIMO-01**	●		●								
	CFT-SIMO-02		●	●								
	CFT-SIMO-03				●							
	CFT-SIMO-04	●	●			●						
	CFT-SIMO-05						●					
	CFT-SIMO-06	●	●					●				
	CFT-SIMO-07								●			
	CFT-SIMO-08									●		
	CFT-SIMO-09	●	●								●	
	CFT-SIMO-10	●	●									●

252
253

254 The following traceability matrices relate core test cases to core test assertions.
255
256 **Test Cases to Assertions (Device Memory – Core Features) – Part 1**

		Test Assertions											
		01	02	03	04	05	06	07	08	09	10	11	12
Device Memory Test Cases (Core Features)	CFT-IM-01	●											
	CFT-IM-02		●										
	CFT-IM-03	●		●									
	CFT-IM-04	●			●								
	CFT-IM-05	●			●	●	●						
	CFT-IM-06	●			●			●	●	●	●	●	●
	CFT-IM-07	●			●								
	CFT-IM-08	●			●								
	CFT-IM-09	●			●								
	CFT-IM-10	●			●								

257
258

259 **Test Cases to Assertions (Device Memory – Core Features) – Part 2**

		13	14	15	16	17	18	19	20	21	22
		Test Assertions									
Device Memory Test Cases (Core Features)	CFT-IM-01										
	CFT-IM-02										
	CFT-IM-03										
	CFT-IM-04										
	CFT-IM-05										
	CFT-IM-06	●	●								
	CFT-IM-07			●							
	CFT-IM-08				●						
	CFT-IM-09					●	●	●			
	CFT-IM-10								●	●	●

260
261

262   **Test Cases to Assertions (SIM Memory – Core Features) – Part 1**

		23	24	25	26	27	28	29	30	31
		Test Assertions								
SIM Memory Test Cases (Core Features)	**CFT-SIM-01**	●								
	CFT-SIM-02		●							
	CFT-SIM-03	●		●						
	CFT-SIM-04	●			●					
	CFT-SIM-05	●				●				
	CFT-SIM-06	●				●	●	●	●	●
	CFT-SIM-07	●				●				
	CFT-SIM-08	●				●				
	CFT-SIM-09	●				●				
	CFT-SIM-10	●				●				

263

264 **Test Cases to Assertions (SIM Memory – Core Features) – Part 2**

		32	33	34	35	36	37
	Test Assertions						
	CFT-SIM-01						
	CFT-SIM-02						
	CFT-SIM-03						
SIM Memory Test Cases (Core Features)	CFT-SIM-04						
	CFT-SIM-05						
	CFT-SIM-06						
	CFT-SIM-07	●					
	CFT-SIM-08		●				
	CFT-SIM-09			●	●		
	CFT-SIM-10					●	●

265
266

267 The following traceability matrices relate optional test cases to optional test assertions.
268
269 **Test Cases to Assertions (Device Memory – Optional Features) – Part 1**

		Test Assertions											
		38	**39**	**40**	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**
Device Memory Test Cases (Optional Features)	**CFT-IMO-01**	•											
	CFT-IMO-02		•										
	CFT-IMO-03	•	•	•									
	CFT-IMO-04				•								
	CFT-IMO-05	•	•			•							
	CFT-IMO-06	•	•				•	•	•	•	•	•	•
	CFT-IMO-07												
	CFT-IMO-08												
	CFT-IMO-09	•	•										
	CFT-IMO-10	•	•										
	CFT-IMO-11	•	•										
	CFT-IMO-12	•	•										

270
271

272 **Test Cases to Assertions (Device Memory – Optional Features) – Part 2**

		Test Assertions							
		50	**51**	**52**	**53**	**54**	**55**	**56**	**57**
Device Memory Test Cases (Optional Features)	**CFT-IMO-01**								
	CFT-IMO-02								
	CFT-IMO-03								
	CFT-IMO-04								
	CFT-IMO-05								
	CFT-IMO-06	●							
	CFT-IMO-07		●						
	CFT-IMO-08			●					
	CFT-IMO-09				●	●			
	CFT-IMO-10						●		
	CFT-IMO-11							●	
	CFT-IMO-12								●

273
274

275   **Test Cases to Assertions (SIM Memory – Optional Features) – Part 1**

		Test Cases					
		58	59	60	61	62	63
SIM Memory Test Cases (Optional Features)	**CFT-SIMO-01**	●					
	CFT-SIMO-02		●				
	CFT-SIMO-03	●	●	●			
	CFT-SIMO-04				●		
	CFT-SIMO-05	●	●			●	●
	CFT-SIMO-06						
	CFT-SIMO-07	●	●				
	CFT-SIMO-08						
	CFT-SIMO-09						
	CFT-SIMO-10	●	●				
	CFT-SIMO-11	●	●				

276
277

278   **Test Cases to Assertions (SIM Memory – Optional Features) – Part 2**

		64	65	66	67	68	69	70
	CFT-SIMO-01							
	CFT-SIMO-02							
	CFT-SIMO-03							
	CFT-SIMO-04							
	CFT-SIMO-05							
SIM Memory Test Cases (Optional Features)	**CFT-SIMO-06**	●						
	CFT-SIMO-07		●	●				
	CFT-SIMO-08				●			
	CFT-SIMO-09					●		
	CFT-SIMO-10						●	
	CFT-SIMO-11							●

279
280
281
282
283
284