December 21, 2007

GSM Mobile Device and Associated Media Tool Specification and Test Plan

Draft 1 for public comment of Version 1.0

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

Abstract

Mobile devices incorporating cellular capabilities are ubiquitous and contain a wealth of personal information useful in criminal cases, civil disputes, employment proceedings, and recreation of incidents. Due to the rapid rate of mobile devices appearing on the market, cellular forensic tools capable of data acquisition are continually evolving. In general, forensic examination of mobile devices is a small part of digital forensics. Consequentially, tools possessing the ability to acquire data from these devices are relatively new and continually expanding.

This paper defines requirements for mobile device applications capable of acquiring data from mobile devices operating over a Global System for Mobile communication (GSM) network, test methods used to determine whether a specific tool meets the requirements, and assertions derived from requirements producing measurable results.[•] The 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.

As this document evolves through comments updated versions will be posted at http://www.cftt.nist.gov.

[•] Certain commercial products and trade names are identified in this paper to illustrate technical concepts. However, it does not imply a recommendation or an endorsement by NIST.

TABLE OF CONTENTS

1. Introduction

As the intelligence and storage capabilities of mobile devices continue to advance, the need to ensure the reliability of mobile device forensic tools intensifies. 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 by development of general tool specifications, test procedures, test criteria, test sets, and test hardware. The results provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensic tools, and for interested parties to understand the tools capabilities. Our approach for testing computer forensic tools is based on well-recognized international methodologies for conformance testing and quality testing. This project is further described at: http://www.cftt.nist.gov/.

The Computer 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 changes must be documented and minimal (i.e., file size) to accomplish the required task.

2. Purpose

This document defines requirements for mobile device forensic tools used in digital forensics capable of acquiring internal memory from Global System for Mobile communication (GSM) devices and related media (i.e., Subscriber Identity Module [SIM]) and test methods used to determine whether a specific tool meets the requirements.

The requirements that will be tested are used to derive assertions. The 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.

As this document evolves through comments updated versions will be posted at http://www.cftt.nist.gov.

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. Assertions

Each assertion specifies a set of conditions that can be tested and the expected results. A traceability matrix relating requirements and assertions is illustrated below.

4.1 Assertions for Core Features

This section lists assertions that all Cellular/SIM forensic tools should meet.

Internal Memory Assertions:

CFT-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, Infrared).

CFT-IM-02 If a cellular forensic tool attempts to connect to a non-supported device then the tool shall have the ability to identity that the device is not supported.

CFT-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.

CFT-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 format via either a preview-pane or generated report.

CFT-IM-05 If a cellular forensic tool successfully completes acquisition of the target device then all subscriber and equipment related information (i.e., IMEI, MSISDN) shall be presented in a human-readable format without modification.

CFT-IM-06 If a cellular forensic tool successfully completes acquisition of the target device then all PIM related data shall be presented in a human-readable format without modification.

CFT-IM-07 If a cellular forensic tool successfully completes acquisition of the target device then all call logs (incoming/outgoing) maintained in device memory shall be presented in a human-readable format without modification.

CFT-IM-08 If a cellular forensic tool successfully completes acquisition of the target device then all text messages stored in device memory shall be presented in a human-readable format without modification.

CFT-IM-09 If a cellular forensic tool successfully completes acquisition of the target device then all pre-populated MMS multi-media related data (i.e., text, audio, graphics, video)

shall be presented via either an internal application or suggested third-party viewer without modification.

CFT-IM-10 If a cellular forensic tool successfully completes acquisition of the target device then all stand alone multi-media data (e.g., audio, graphics, video) shall be presented via either an internal application or suggested third-party viewer without modification.

SIM Assertions:

CFT-SIM-01 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).

CFT-SIM-02 If a cellular forensic tool attempts to connect to a non-supported SIM then the tool shall have the ability to identity that the SIM is not supported.

CFT-SIM-03 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.

CFT-SIM-04 If the SIM is password-protected then the CFT shall provide the examiner with the opportunity to input the PIN before acquisition.

CFT-SIM-05 If a cellular forensic tool successfully completes acquisition of the target SIM then the tool shall have the ability to present acquired data elements in a human-readable format via either a preview-pane or generated report.

CFT-SIM-06 If a cellular forensic tool successfully completes acquisition of the target SIM then all subscriber and equipment related information (i.e., SPN, ICCID, IMSI, MSISDN) shall be presented in a human-readable format without modification.

CFT-SIM-07 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.

CFT-SIM-08 If a cellular forensic tool successfully completes acquisition of the target SIM then the last numbers dialed (LND) shall be presented in a human-readable format without modification.

CFT-SIM-09 If a cellular forensic tool successfully completes acquisition of the target SIM then all text messages (i.e., SMS, EMS) stored in SIM memory shall be presented in a human-readable format without modification.

CFT-SIM-10 If a cellular forensic tool successfully completes acquisition of the target SIM then all location related data (i.e., LOCI, GPRSLOCI) shall be presented in a human-readable format without modification.

4.2 Assertions for Optional Features

The following requirements are defined for tool features that might be implemented for some cellular forensic tools. If a tool provides the optional feature, the tool is tested as if the requirement were mandatory. If the tool does not provide the capability defined, the requirement does not apply.

A formal statement of these requirements follows:

Optional Internal Memory Assertions:

CFT-IMO-01 If a cellular forensic tool successfully completes acquisition of the target device then the tool shall present the acquired data without modification via all supported generated report formats.

CFT-IMO-02 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.

CFT-IMO-03 If a cellular forensic tool provides the examiner with a preview-pane view and a generated report of the acquired data then the reports shall maintain consistency of all reported data elements.

CFT-IMO-04 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.

CFT-IMO-05 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.

CFT-IMO-06 If the cellular forensic tool supports a physical acquisition of the target device then the tool shall report recoverable deleted data in a human-readable format without modification.

CFT-IMO-07 If the cellular forensic tool supports SIM access card creation then the card creation shall be completed without errors via manufacturer suggested protocols.

CFT-IMO-08 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.

CFT-IMO-09 If the cellular forensic tool supports proper display of foreign language character sets then the application should present data objects containing foreign language characters in their native format without modification.

CFT-IMO-10 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.

CFT-IMO-11 If the cellular forensic tool supports hashing for individual data objects then the tool shall present the user with a hash value for each acquired data object.

CFT-IMO-12 If the cellular forensic tool supports hashing for the overall case file then the tool shall present the user with one hash value representing the entire case data.

Optional SIM Assertions:

CFT-SIMO-01 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 all supported generated report formats.

CFT-SIMO-02 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.

CFT-SIMO-03 If a cellular forensic tool provides the examiner with a preview-pane view and a generated report of the acquired data then the reports shall maintain consistency of all reported data elements.

CFT-SIMO-04 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.

CFT-SIMO-05 If the cellular forensic tool successfully completes acquisition of the target SIM and recoverable deleted data elements exist then the tool shall present recoverable deleted data in a human-readable format without modification.

CFT-SIMO-06 If a cellular forensic tool supports creation of log files then the application should present the log files in a human-readable format outlining the acquisition process.

CFT-SIMO-07 If a cellular forensic tool supports proper display of foreign language character sets then the application should present data objects containing foreign language characters in their native format without modification.

CFT-SIMO-08 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.

CFT-SIMO-09 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.

CFT-SIMO-10 If the cellular forensic tool supports hashing for individual data objects then the tool shall present the user with a hash value for each acquired data object.

CFT-SIMO-11 If the cellular forensic tool supports hashing for the overall case file then the tool shall present the user with one hash value representative of the entire case data.

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 environment. This allows different environments to be substituted under the test cases for testing different products and options.

A set of test parameters is chosen to cover the assertions from various aspects. The test cases are described below in Table 1. The primary goal of test cases CFT-IM-01 – CFT-SIMO-71 is to determine the tools ability to acquire specific data elements pre-populated onto the device without modification.

5.1 Test Case Summaries

The following table gives a summary for each test case.

Table 1: Test Case Summaries

CFT-IM-01	Connect a supported target device via all manufacturer supported interfaces (e.g., cable, Bluetooth, Infrared), and determine if connectivity to the device is successful by initiating internal memory acquisition.
CFT-IM-02	Connect a non-supported target device and determine if the application identifies the device as illegitimate by attempting internal memory acquisition.
CFT-IM-	Begin acquisition; disrupt connectivity by unplugging the device. Note any notification messages provided to the user of device to application

03	connectivity disruption.
CFT-IM-04	Acquire device contents; View acquired data contents either via a preview-pane or generated report for readability and completeness.
CFT-IM-05	Acquire device contents; compare known MSISDN data with the acquired data for consistency and completeness.
CFT-IM-06	Acquire device contents; compare known IMEI data with the acquired data for consistency and completeness.
CFT-IM-07	Acquire device contents; compare known address book entries with the acquired data output for consistency and completeness.
CFT-IM-08	Acquire device contents; compare known maximum length address book entries with the acquired data output for consistency and completeness.
CFT-IM-09	Acquire device contents; compare known special character address book entries with the acquired data output for consistency and completeness.
CFT-IM-10	Acquire device contents; compare known blank name address book entries with the acquired data output for consistency and completeness.
CFT-IM-11	Acquire device contents; compare known address book entries containing email addresses with the acquired data output for consistency and completeness.
CFT-IM-12	Acquire device contents; compare known address book entries containing a graphic with the acquired data output for consistency and completeness.
CFT-IM-13	Acquire device contents; compare known PIM data (i.e., datebook/calendar, notes) with the acquired data output for consistency and completeness.
CFT-IM-14	Acquire device contents; compare known maximum length PIM data (i.e., datebook/calendar, notes) entries with the acquired data output for consistency and completeness.
CFT-IM-15	Acquire device contents; compare known call logs (i.e., incoming, outgoing) with the acquired data output for consistency and completeness.
CFT-IM-16	Acquire device contents; compare known text messages (i.e., SMS, EMS) with the acquired data output for consistency and completeness.
CFT-IM-17	Acquire device contents; compare known MMS messages and associated audio attachments with the acquired data output for consistency and completeness.
CFT-IM-18	Acquire device contents; compare known MMS messages and associated image attachments with the acquired data output for consistency and completeness.
CFT-IM-19	Acquire device contents; compare known MMS messages and associated video attachments with the acquired data output for consistency and completeness.
CFT-IM-	Acquire device contents; compare known multi-media files (i.e. audio) transferred to the device with the acquired data output for consistency and

20	completeness.
CFT-IM-21	Acquire device contents; compare known multi-media files (i.e., images) transferred to the device with the acquired data output for consistency and completeness.
CFT-IM-22	Acquire device contents; compare known multi-media files (i.e., video) transferred to the device with the acquired data output for consistency and completeness.
CFT-SIM-23	Connect a supported target SIM via manufacturer supported interfaces (e.g., PC/SC reader, proprietary reader), and determine if connectivity to the SIM is successful by initiating SIM acquisition.
CFT-SIM-24	Connect a non-supported SIM and determine if the application identifies the SIM as illegitimate by attempting acquisition.
CFT-SIM-25	Begin SIM acquisition; disrupt connectivity by unplugging the SIM. Note any notification messages provided to the user of SIM to application connectivity disruption.
CFT-SIM-26	Attempt acquisition with a password-protected SIM to determine if the application prompts the examiner to authenticate when attempting to acquire a password-protected SIM.
CFT-SIM-27	Acquire SIM contents; View acquired data contents either via a preview-pane or generated report for readability and completeness.
CFT-SIM-28	Acquire SIM contents; compare the known SPN with the acquired data for consistency and completeness.
CFT-SIM-29	Acquire SIM contents; compare the known ICCID with the acquired data for consistency and completeness.
CFT-SIM-30	Acquire SIM contents; compare the known IMSI with the acquired data for consistency and completeness.
CFT-SIM-31	Acquire SIM contents; compare the known MSISDN with the acquired data for consistency and completeness.
CFT-SIM-32	Acquire SIM contents; compare known ADNs with the acquired data output for consistency and completeness.
CFT-SIM-33	Acquire SIM contents; compare known LND with the acquired data output for consistency and completeness.
CFT-SIM-34	Acquire SIM contents; compare known SMS messages with the acquired data output for consistency and completeness.
CFT-SIM-35	Acquire SIM contents; compare known EMS messages with the acquired data output for consistency and completeness.
CFT-SIM-36	Acquire SIM contents; compare known network information (i.e., LOCI) with the acquired data output for consistency and completeness.
CFT-	Acquire SIM contents; compare known network information (i.e., GPRSLOCI) with the acquired data output for consistency and

SIM-37	completeness.
CFT-IMO-38	Acquire device contents; compare generated reports with known internal memory data elements with items reported via the generated report for consistency and completeness.
CFT-IMO-39	Acquire device contents; compare known internal memory data elements with items presented in the preview-pane view for consistency and completeness.
CFT-IMO-40	Acquire device contents; Compare output of preview-pane and generated report (if both supported) for readability, consistency and completeness.
CFT-IMO-41	Attempt to modify internal memory case file data via a third-party application; re-open the case file to determine if the case is reported as faulty.
CFT-IMO-42	Initialize forensic application, select physical acquisition of the target device if supported, and check data output for consistency, completeness and readability.
CFT-IMO-43	Perform a physical acquisition; compare known deleted address book entries with the acquired data output for consistency, completeness and readability.
CFT-IMO-44	Perform a physical acquisition; compare known deleted PIM data (i.e., calendar entries, notes) with the acquired data output for consistency, completeness and readability.
CFT-IMO-45	Perform a physical acquisition; compare known deleted call logs with the acquired data output for consistency, completeness and readability.
CFT-IMO-46	Perform a physical acquisition; compare known deleted outgoing SMS messages with the acquired data output for consistency, completeness and readability.
CFT-IMO-47	Perform a physical acquisition; compare known deleted outgoing EMS messages with the acquired data output for consistency, completeness and readability.
CFT-IMO-48	Perform a physical acquisition; compare known deleted audio files with the acquired data output for consistency, completeness and readability.
CFT-IMO-49	Perform a physical acquisition; compare known deleted image files with the acquired data output for consistency, completeness and readability.
CFT-IMO-50	Perform a physical acquisition; compare known deleted video files with the acquired data output for consistency, completeness and readability.
CFT-IMO-51	Connect the supported access card via the suggested protocol; determine if the process is successful by initializing the access card creation and verifying the vendor documented functionality of the created access card.
CFT-IMO-52	Acquire device contents; check log files for readability, completeness and consistency with the vendor-supported output.

CFT-IMO-53	Acquire device contents; compare known address book entries containing foreign language character sets for readability, consistency and completeness.
CFT-IMO-54	Acquire device contents; compare known outgoing text messages containing foreign language character sets for readability, consistency and completeness.
CFT-IMO-55	Acquire device contents in stand-alone mode; Acquire the SIM; compare known status flags for text messages contained on the SIM to determine data has not been altered from unread to read.
CFT-IMO-56	Acquire device contents; check for completeness of reported hashes for individual data objects
CFT-IMO-57	Acquire device contents; check for completeness of a reported hash for the overall case file.
CFT-SIMO-58	Acquire SIM contents; compare generated reports with known data elements with items reported via the generated report for consistency and completeness.
CFT-SIMO-59	Acquire SIM contents; compare known data elements with items presented in the preview-pane view for consistency and completeness.
CFT-SIMO-60	Acquire SIM contents; Compare output of preview-pane and generated report (if both supported) for readability, consistency and completeness.
CFT-SIMO-61	Attempt to modify SIM acquisition case file data via a third-party application; re-open the case file to determine if the case is reported as faulty.
CFT-SIMO-62	Perform acquisition; compare known deleted ADNs with the acquired data output for consistency, completeness and readability.
CFT-SIMO-63	Perform acquisition; compare known deleted incoming SMS messages with the acquired data output for consistency, completeness and readability.
CFT-SIMO-64	Perform acquisition; compare known deleted incoming EMS messages with the acquired data output for consistency, completeness and readability.
CFT-SIMO-65	Acquire SIM contents; check log files for readability, completeness and consistency with the vendor-supported output.
CFT-SIMO-66	Acquire SIM contents; compare known ADNs containing foreign language character sets for readability, consistency and completeness.
CFT-SIMO-67	Acquire SIM contents; compare known EMS messages containing foreign language character sets for readability, consistency and completeness.
CFT-SIMO-68	Initialize the SIM application with a protected SIM; determine if the application provides the remaining number of PIN (authentication) attempts and properly decrements the attempts when inputting an incorrect PIN.
CFT-SIMO-69	Initialize the SIM application with a locked SIM; determine if the application provides the remaining number of PUK attempts and properly

	decrements the attempts when inputting an incorrect PUK.
CFT-SIMO-70	Acquire SIM contents; check for completeness of reported hashes for individual data objects
CFT-SIMO-71	Acquire SIM contents; check for completeness of a reported hash for the overall case file.

5.2 Test Case Expected Results

Table 2 illustrated below presents the expected results for each test assertion. The Expected Results column contains a message template for the related assertion. The Comments column presents additional information about the assertion. For assertions that have more than one possible expected result, the Comments column documents any conditions that select the particular expected result.

Table 2: Expected Results

Assertion	Expected Results	Comments
A_IM-01	Successful acquisition for all vendor supported interfaces (e.g., cable, Bluetooth, IrDA) without errors	Connect device via supported interface; Begin acquisition to determine if successful
A_IM-02	Examiner is informed that the tool cannot perform an acquisition due to lack of device support	Connect a device not supported by the tool; Begin acquisition
A_IM-03	Examiner is informed that connectivity has been disrupted during acquisition	Begin acquisition; Disconnect interface or interrupt connectivity (i.e., unplug cable) during acquisition
A_IM-04	Device contents are displayed in a human-readable format via either a preview-pane or generated report view	Successful acquisition of a supported device
A_IM-05	Accurate acquisition of subscriber related data (i.e., MSISDN)	MSISDN is reported
A_IM-06	Accurate acquisition of equipment related data (i.e., IMEI)	IMEI is reported
A_IM-07	Complete and accurate acquisition of all known active address book entries	Address book entries and associated data are reported
A_IM-08	Complete and accurate acquisition of all known maximum length active address book entries	Maximum length address book entries are reported in totality
A_IM-09	Complete and accurate acquisition of all	Address book entries

	known active address book entries containing special characters	containing special characters are reported
A_IM-10	Complete and accurate acquisition of all known active address book entries containing blank names	Address book entries containing blank names are reported
A_IM-11	Complete and accurate acquisition of all known active address book entries containing email addresses	Address book entries containing an email addresses are reported
A_IM-12	Complete and accurate acquisition of all known active address book entries containing a graphic	Address book entries containing an graphic are reported
A_IM-13	Complete and accurate acquisition of all known active PIM data	Datebook/Calendar, notes entries are reported
A_IM-14	Complete and accurate acquisition of maximum length PIM data entries	Maximum length Datebook/Calendar, notes entries are reported
A_IM-15	Complete and accurate acquisition of all known active call logs	Incoming and outgoing calls are reported
A_IM-16	Complete and accurate acquisition of all known active text (i.e., SMS, EMS) messages	Text messages stored in the internal memory are reported
A_IM-17	Complete and accurate acquisition of all known active MMS messages and associated audio attachments	Incoming and outgoing MMS message data including text and audio are reported
A_IM-18	Complete and accurate acquisition of all known active MMS messages and associated image attachments	Incoming and outgoing MMS message data including text and image are reported
A_IM-19	Complete and accurate acquisition of all known active MMS messages and associated video attachments	Incoming and outgoing MMS message data including text and video are reported
A_IM-20	Complete and accurate acquisition of all known active audio multi-media files	Acquisition and reporting of audio files
A_IM-21	Complete and accurate acquisition of all known active image multi-media files	Acquisition and reporting of image files
A_IM-22	Complete and accurate acquisition of all known active video multi-media files	Acquisition and reporting of video files
A_SIM-23	Successful acquisition for all vendor supported interfaces (e.g., PC/SC reader,	Connect SIM via supported interface; Begin acquisition

	proprietary reader) without error	to determine if successful
A_SIM-24	Examiner is informed that the tool cannot perform an acquisition due to the lack of SIM support	Connect a SIM not supported by the tool; Begin acquisition
A_SIM-25	Examiner is informed that connectivity has been disrupted during acquisition	Begin acquisition; Disconnect interface or interrupt connectivity (i.e., unplug cable) during acquisition
A_SIM-26	Application prompts examiner to input PIN on password protected SIMs before acquisition begins.	Password-protected SIM
A_SIM-27	SIM contents are displayed in a human-readable format via either a preview-pane or generated report view	Successful acquisition of a supported SIM
A_SIM-28	Accurate acquisition of the SPN	Service Provider Name is reported
A_SIM-29	Accurate acquisition of the ICCID	ICCID is reported
A_SIM-30	Accurate acquisition of the IMSI	IMSI is reported
A_SIM-31	Accurate acquisition of the MSISDN	MSISDN is reported
A_SIM-32	Complete and accurate acquisition of all known active ADNs	ADNs and associated data are reported
A_SIM-33	Complete and accurate acquisition of all known active LND	LNDs are reported
A_SIM-34	Complete and accurate acquisition of all known active SMS messages	Incoming SMS messages are reported
A_SIM-35	Complete and accurate acquisition of all known active EMS messages	Incoming EMS messages are reported
A_SIM-36	Complete and accurate acquisition of location related network data (i.e., LOCI)	LOCI data is reported
A_SIM-37	Complete and accurate acquisition of location related network data (i.e., GPRSLOCI)	GPRSLOCI data is reported
A_IMO-38	Generated reports after a successful complete acquisition are consistent with known data elements populated onto the device.	Check report output with known data elements for consistency and completeness
A_IMO-39	Data elements presented via the preview-pane view after a complete acquisition are	Check preview-pane output with known data elements

	consistent with the known data elements populated onto the device.	for consistency and completeness
A_IMO-40	Data output from the generated reports and the preview-pane are complete and consistent	Check generated report and preview-pane for consistency if both supported
A_IMO-41	Application disallows re-opening a case file whose data has been modified via a third-party application.	Data integrity
A_IMO-42	Device contents are displayed in a human-readable format via either a preview-pane or generated report view after a successful physical acquisition	Complete file-system read
A_IMO-43	After a physical acquisition, non-overwritten deleted address book entries are either completely recoverable or data remnants are reported	Recovery of deleted address book entries after a physical acquisition
A_IMO-44	After a physical acquisition, non-overwritten deleted PIM data are either completely recoverable or data remnants are reported	Recovery of deleted calendar, notes entries after a physical acquisition
A_IMO-45	After a physical acquisition, non-overwritten deleted call logs are either completely recoverable or data remnants are reported	Recovery of deleted call logs after a physical acquisition
A_IMO-46	After a physical acquisition, non-overwritten deleted outgoing SMS messages are either completely recoverable or data remnants are reported	Recovery of deleted outgoing SMS messages
A_IMO-47	After a physical acquisition, non-overwritten deleted outgoing EMS messages are either completely recoverable or data remnants are reported	Recovery of deleted outgoing EMS messages
A_IMO-48	After a physical acquisition, non-overwritten deleted audio files are either completely recoverable or data remnants are reported	Recovery of deleted audio files
A_IMO-49	After a physical acquisition, non-overwritten deleted image files are either completely recoverable or data remnants are reported	Recovery of deleted image files
A_IMO-50	After a physical acquisition, non-overwritten deleted video files are either completely recoverable or data remnants are reported	Recovery of deleted video files
A_IMO-51	Access cards are successfully written by	Cards may act as a radio-isolation card or may

	following vendor specified protocol	contain data objects from a target SIM
A_IMO-52	Generated log files are readable, complete and consistent with capturing data specified by the vendor	Log file creation
A_IMO-53	Acquisition of foreign address book entries are readable, complete and consistent with the target data set and displayed in their native format.	Acquisition and display of foreign language character sets
A_IMO-54	Acquisition of outgoing text messages containing foreign characters are readable, complete and consistent with the target data set and displayed in their native format.	Acquisition and display of foreign language character sets
A_IMO-55	Devices acquired in stand-alone mode does not alter the status flags of UNREAD text messages contained on the SIM to READ	Stand-alone acquisition protects modification of SIM status flags
A_IMO-56	Application provides examiner with a hash for individual data objects acquired	Individual data object hash
A_IMO-57	Application provides examiner with a hash for the entire case file	Case file hash
A_SIMO-58	Generated reports after a successful complete acquisition are consistent with known data elements populated onto the SIM	Check report output with known data elements for consistency and completeness
A_SIMO-59	Data elements presented via the preview-pane view after a complete acquisition are consistent with the known data elements populated onto the SIM	Check preview-pane output with known data elements for consistency and completeness
A_SIMO-60	Data output from the generated reports and the preview-pane are complete and consistent	Check generated report and preview-pane for consistency if both supported
A_SIMO-61	Application disallows re-opening a case file whose data has been modified via a third-party application	Data-integrity
A_SIMO-62	Non-overwritten deleted ADNs are either completely recoverable or data remnants are reported	Recovery of deleted ADNs
A_SIMO-63	Non-overwritten deleted SMS messages are either completely recoverable or data remnants are reported	Recovery of deleted SMS messages

A_SIMO-64	Non-overwritten deleted EMS messages are either completely recoverable or data remnants are reported	Recovery of deleted EMS messages
A_SIMO-65	Generated log files are readable, complete and consistent with capturing data specified by the vendor	Log file creation
A_SIMO-66	Acquisition of foreign language ADNs are readable, complete and consistent with the target data set and displayed in their native format	Acquisition and display of foreign language character sets
A_SIMO-67	Acquisition of foreign language text messages are readable, complete and consistent with the target data set and displayed in their native format	Acquisition and display of text messages containing foreign language character sets
A_SIMO-68	The remaining number of PIN attempts are displayed before acquisition begins on a password protected SIM	Password protected SIMs
A_SIMO-69	The remaining number of PUK attempts are displayed before acquisition begins on a SIM whose PIN attempts have exhausted	Remaining PUK attempts displayed
A_SIMO-70	Application provides examiner with a hash for individual data objects acquired	Individual data object hash
A_SIMO-71	Application provides examiner with a hash for the entire case file	Case file hash

Requirements to Assertions (Device Memory - Core Features)

		Test Assertions									
		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	•			•	•	•	•	•	•	•

Requirements to Assertions (SIM Memory – Core Features)

		Test Assertions									
		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	•				•	•	•	•	•	•

298 **Requirements to Assertions (Device Memory – Optional Features)**

		Test Assertions											
		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	•	•										•

299

Requirements to Assertions (SIM Memory – Optional Features)

		Test Assertions										
		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	•	•									•

Assertions to Test Cases (Device Memory – Core Features) – Part 1

		Test Cases											
		01	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**
Device Memory Assertions (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	•			•								

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

		Test Cases									
		13	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
Device Memory Assertions (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								•	•	•

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

		Test Cases								
		23	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
SIM Memory Assertions (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	•				•				

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

		Test Cases					
		32	**33**	**34**	**35**	**36**	**37**
SIM Memory Assertions (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					•	•

Assertions to Test Cases (Device Memory – Optional Features) – Part 1

		Test Cases											
		38	**39**	**40**	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**
Device Memory Assertioins (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	•	•										

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

		Test Cases							
		50	**51**	**52**	**53**	**54**	**55**	**56**	**57**
Device Memory Assertions (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								•

312

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

		Test Cases						
		58	**59**	**60**	**61**	**62**	**63**	**64**
SIM Memory Assertions (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	•	•					

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

		Test Cases						
		65	**66**	**67**	**68**	**69**	**70**	**71**
SIM Memory Assertions (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							•