

January 6, 2009

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
33
34
35
36
37
38

GSM Mobile Device and Associated Media Tool Specification

Version 1.2



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

39 **Abstract**

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

52

53 This paper defines requirements for mobile device applications capable of acquiring data from
54 mobile devices operating over a Global System for Mobile communication (GSM) network and test
55 methods used to determine whether a specific tool meets the requirements, and assertions derived
56 from requirements producing measurable results.* Test requirements are statements used to derive
57 test cases that define expectations of a tool or application. Test cases describe the combination of
58 test parameters required to test each assertion. Test assertions are described as general statements or
59 conditions that can be checked after a test is executed. Each assertion appears in one or more test
60 cases consisting of a test protocol and the expected test results. The test protocol specifies detailed
61 procedures for setting up the test, executing the test, and measuring the test results. The associated
62 assertions and test cases are defined in the test plan document entitled: [GSM Mobile Device and
63 Associated Media Tool Test Assertions and Test Plan](#).

64

65 Your comments and feedback are welcome; revisions of this document are available for download
66 at: http://www.cfft.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.

67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90

TABLE OF CONTENTS

1. Introduction	1
2. Purpose	1
3. Scope	2
4. Glossary	2
5. Handset Characteristics - Internal Memory	3
6. SIM Characteristics	4
7. Digital Evidence	4
8. Test Methodology	5
9. Requirements	5
9.1 Requirements for Core Features	5
9.2 Requirements for Optional Features	6
9.2.1 Presentation	6
9.2.2 Protection	7
9.2.3 Physical Acquisition	7
9.2.4 Access Card Creation	7
9.2.5 Log Files	7
9.2.6 Foreign Language	8
9.2.7 PIN Attempts	8
9.2.8 PUK Attempts	8
9.2.9 Stand-alone Acquisition	8
9.2.10 Hashing	8

90 **1. Introduction**

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

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

117
118 The central requirement for a sound forensic examination of digital evidence is that the original
119 evidence must not be modified (i.e., the examination or capture of digital data from a mobile device
120 and associated media must be performed without altering the device or media content). In the event
121 that data acquisition is not possible using current technology to access information without
122 configuration changes to the device (e.g., loading a driver), the procedure must be documented.

123

124 **2. Purpose**

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

129

130 The requirements that will be tested are used to derive assertions. The assertions are described as
131 general statements of conditions that can be checked after a test is executed. Each assertion
132 generates one or more test cases consisting of a test protocol and the expected test results. The test

133 protocol specifies detailed procedures for setting up the test, executing the test, and measuring the
134 test results.
135

136 **3. Scope**

137 The scope of this specification is limited to software tools capable of acquiring GSM devices and
138 related media (i.e., SIM). The specifications are general and capable of being adapted to other types
139 of mobile device forensic software.
140

141 **4. Glossary**

142 This glossary was added to provide context in the absence of official definitions recognized by the
143 computer forensics community.
144

145 **Access card/Radio isolation card:** Subscriber Identity Modules (SIMs) that contain necessary data
146 elements allowing GSM equipment to operate without network connectivity.

147 **Associated data:** Multi-media data (i.e., graphic, audio, video) that are attached
148 and delivered via a multi-messaging service (MMS) message.

149 **Acquisition File:** A snapshot of data contained within the internal memory of a target device or
150 associated media (i.e. SIM).

151 **Case File:** A file generated by a forensic tool that contains the data acquired from a mobile device
152 or associated media and case-related information (e.g., case number, property/evidence
153 number, agency, examiner name, contact information, etc.) provided by the examiner.

154 **Cellular phone:** A device whose major function is primarily handling
155 incoming/outgoing phone calls with limited task management applications.

156 **CFT:** Cellular Forensic Tool.

157 **Enhanced Message Service (EMS):** Text messages over 160 characters or
158 messages that contain either Unicode characters or a 16x16, 32x32 black and white image.

159 **Flash memory:** Non-volatile memory that retains data after the power is removed.

160 **GSM:** Global System for Mobile communications is an open, digital cellular technology
161 for transmitting mobile voice and data services.

162 **Hashing:** The mathematical algorithmic process of creating a numeric fingerprint value that
163 facilitates uniqueness.

164 **Human-readable format:** Acquired data (e.g., text, images) that is interpreted by the forensic
165 application and presented in a human-readable format without decoding.

166 **IM:** Internal Memory.

167 **Logical acquisition:** Implies a bit-by-bit copy of logical storage objects (e.g.,
168 directories and files) that reside on a logical store (e.g., a file system partition).

169 **Mobile Subscriber International Subscriber Directory Number (MSISDN):** The MSISDN
170 conveys the telephone number assigned to the subscriber for receiving calls on the phone.

171 **Multimedia Messaging Service (MMS) message:** Provides users with the ability
172 to send text messages containing multimedia objects (i.e., graphic, audio, video).

173 **Preview pane:** Section of the Graphical User Interface (GUI) that provides a snapshot of the
174 acquired data.

175 **Physical acquisition:** A bit-by-bit copy of the data layer.

176 **Personal Information Management (PIM) data:** Data that contains personal information such as:
177 calendar entries, to-do lists, memos, reminders, etc.

178 **Personal Identification Number (PIN):** A numeric code used for preventing unauthorized access
179 to a device generally associated with the SIM. PIN1 is the primary means of access to a
180 handset. PIN2 when activated provides additional security for a small set of features (e.g.,
181 resetting call meters, changing fixed dialing numbers).

182 **PIN Unlock Code (PUK):** A required code to unlock a disabled SIM due to three successive
183 incorrect PIN attempts. PUK1 and PUK2 are used to unblock PIN1 and PIN2 respectively.

184 **Short Message Service (SMS):** A service used for sending text messages (up to 160 characters) to
185 mobile devices.

186 **Subscriber Identity Module (SIM):** A smart card which contains essential subscriber
187 information and additional data providing network connectivity to mobile equipment
188 operating over a GSM network.

189 **Smart phone:** A full-featured mobile phone that provides users with personal
190 computer like functionality by incorporating PIM applications, enhanced Internet
191 connectivity and email operating over an Operating System supported by superior
192 processing and high capacity storage.

193 **Stand-alone data:** Data (e.g., graphic, audio, video) that is not associated with or has not been
194 transferred to the device via email or MMS message.

195 **User data:** Data populated onto the device using applications provided by the device.
196

197 **5. Handset Characteristics - Internal Memory**

198 Mobile devices, designed with the primary purpose of placing and receiving calls, maintain data in
199 flash memory. Typically, the first part of flash memory is filled with the operating system and the
200 second part is allocated for user data. Although information is stored in a proprietary format,
201 forensic tools tailored for mobile device acquisition should minimally be able to perform a logical
202 acquisition for supported devices and provide a report of the data present in the internal memory.
203 Tools that possess a low-level understanding of the proprietary data format for a specific device
204 may provide examiners with the ability to perform a physical acquisition and generate reports in a
205 meaningful (i.e., human-readable) format. Currently, the tools capable of performing a physical
206 acquisition on a mobile device are limited.
207

208 **6. SIM Characteristics**

209 Due to the GSM 11.11¹ standard, mobile device forensic tools designed to extract data from a SIM
210 via an external reader should be able to properly acquire, decode, and present data in a human-
211 readable format. An abundance of information is stored on the SIM such as Abbreviated Dialing
212 Numbers (ADNs), Last Numbers Dialed (LND), Short Message Service (SMS) messages,
213 subscriber information (i.e., IMSI), and location information (i.e., Location Information [LOCI],
214 General Packet Radio Service Location [GPRSLOCI]). Tools optionally should provide support for
215 Universal Subscriber Identity Modules (USIMs), the third generation (3G) card which carries out
216 the same functions as its 2G cousin (i.e., SIM).

217
218 Optionally, mobile device forensic tools should provide the ability to create an access SIM² in the
219 event that the mobile equipment (ME) is found without the SIM present. Devices found without the
220 SIM present may cause difficulty in acquiring the internal memory of the related device. Therefore,
221 the ability to create an access card bypasses this problematic situation and allows for completion of
222 internal memory acquisition.

223

224 **7. Digital Evidence**

225 The amount and richness of data contained on mobile devices is dependent upon device type (i.e.,
226 low-end, high-end) and personal usage. However, there is a core set of data that computer forensic
227 tools can recover that remains somewhat consistent on all devices with cellular capabilities. GSM
228 devices provide two areas for data storage: device internal memory and the SIM. Tools should have
229 the ability to recover the following data elements stored in the device's internal handset memory:

230

- 231 • International Mobile Equipment Identifier (IMEI)
- 232 • Personal Information Management (PIM) data – (e.g., Address book, Calendar entries, to-do
233 list, Tasks)
- 234 • Call logs – Incoming and outgoing calls
- 235 • Text messages (SMS, EMS)
- 236 • Multi-media Messages (MMS)/email – and associated data
- 237 • File storage – Stand-alone files such as audio, graphic and video

238

239 Tools shall have the ability to recover the following data elements stored on the SIM memory:

240

- 241 • Service Provider Name (SPN)
- 242 • Integrated Circuit Card Identifier (ICCID)
- 243 • International Mobile Subscriber Identity (IMSI)
- 244 • Mobile Subscriber International ISDN Number (MSISDN)
- 245 • Abbreviated Dialing Numbers (ADNs)
- 246 • Last Numbers Dialed (LND)
- 247 • Short Message Service (SMS) – text messages under 160 characters

¹ <http://www.tfn.net/techno/smartcards/gsm11-11.pdf>

² Access cards or radio isolation cards contain necessary fields that allow the ME to function without network connectivity.

- 248 • Enhanced Message Service (EMS) – text messages greater than 160 characters
- 249 • Location Information (LOCI)
- 250 • General Packet Radio Service (GPRS) location – GPRSLOCI

251

252 **8. Test Methodology**

253 To provide concise test results of tools capabilities, the following test methodology will be strictly
254 followed. The forensic application under evaluation will be installed on a dedicated (i.e., no other
255 forensic applications are installed) host machine operating over the required platform as specified
256 by the application. Two identical GSM devices will function as the source and target devices. The
257 internal memory of the source and target devices will be populated with a pre-defined dataset as
258 will the source and target SIMs. Source, target devices and associated media (i.e., SIM), subsequent
259 to initial data population, will be stored in a protected state eliminating the possibility of data
260 modification due to network connectivity. Each succeeding test entails recreating the host
261 environment for each specific tool tested and re-populating the target device and SIM. During the
262 acquisition process, all data transmissions (sent and received data packets) between the device and
263 application will be captured and logged via a port monitoring utility.

264

265 The following data elements will be used for populating the internal memory of the cellular device:
266 Address book, PIM data, call logs, text messages (SMS, EMS), MMS messages/email with
267 attachments (i.e., images, audio, video) and stand-alone data files (i.e., audio, graphic, video). The
268 following data elements will be used for populating the SIM: Abbreviated Dialing Numbers
269 (ADNs), Last Numbers Dialed (LND), Short Messaging Service (SMS) messages marked as Read,
270 Unread and Deleted, EMS messages, and location (LOCI) information.

271

272 **9. Requirements**

273 The requirements are in two sections: 9.1 and 9.2. Section 9.1 lists requirements (i.e., Cellular
274 Forensic Tool-Internal Memory-01 [CFT-IM-01] through CFT-IM-05 and Cellular Forensic Tool-
275 Subscriber Identity Module-01 [CFT-SIM-01] through CFT-SIM-06) that all acquisition tools shall
276 meet. Section 9.2 lists requirements (i.e., Cellular Forensic Tool-Internal Memory Optional-01
277 [CFT-IMO-01] through CFT-IMO-10 and Cellular Forensic Tool-Subscriber Identity Module
278 Optional-01 [CFT-SIMO-01] through CFT-SIMO-10) that the tool shall meet on the condition that
279 specified features or options are offered by the tool.

280

281 **9.1 Requirements for Core Features**

282 The following requirements are mandatory and shall be met by all mobile device forensic tools
283 capable of acquiring internal handset memory and SIM memory.

284

285 **Internal Memory Requirements:**

286 **CFT-IM-01** A cellular forensic tool shall have the ability to recognize supported devices via the
287 vendor supported interfaces (e.g., cable, Bluetooth, Infrared).

288 **CFT-IM-02** A cellular forensic tool shall have the ability to identify non-supported devices.

- 289 **CFT-IM-03** A cellular forensic tool shall have the ability to notify the user of connectivity errors
290 between the device and application during acquisition.
291 **CFT-IM-04** A cellular forensic tool shall have the ability to provide the user with either a
292 preview pane or generated report view of data acquired.
293 **CFT-IM-05** A cellular forensic tool shall have the ability to logically acquire all application
294 supported data elements present in internal memory without modification.
295

296 **SIM Requirements:**

- 297 **CFT-SIM-01** A cellular forensic tool shall have the ability to recognize supported SIMs via the
298 vendor supported interface (e.g., PC/SC reader, proprietary reader).
299 **CFT-SIM-02** A cellular forensic tool shall have the ability to identify non-supported SIMs.
300 **CFT-SIM-03** A cellular forensic tool shall have the ability to notify the user of connectivity errors
301 between the SIM reader and application during acquisition.
302 **CFT-SIM-04** A cellular forensic tool shall have the ability to provide the user with the opportunity
303 to unlock a password protected SIM before acquisition.
304 **CFT-SIM-05** A cellular forensic tool shall have the ability to provide the user with either a
305 preview pane or generated report view of data acquired.
306 **CFT-SIM-06** A cellular forensic tool shall have the ability to acquire all application supported data
307 elements present in the SIM memory without modification.
308

309 **9.2 Requirements for Optional Features**

310 The following requirements define optional tool features. If a tool provides the capability defined,
311 the tool is tested as if the requirement were mandatory. If the tool does not provide the capability
312 defined, the requirement does not apply.
313

314 The following optional features are identified:

- 315 • Presentation
- 316 • Protection
- 317 • Physical acquisition
- 318 • Access Card/Radio Isolation Card creation
- 319 • Log file creation
- 320 • Foreign language character support
- 321 • Remaining PIN attempts
- 322 • Remaining PUK attempts
- 323 • Stand-alone acquisition
- 324 • Hashing
- 325

326 **9.2.1 Presentation**

327 Requirements CFT-IMO-01 through CFT-IMO-02 apply to Optional Internal Memory
328 Requirements. Requirements CFT-SIMO-01 through CFT-SIMO-02 apply to Optional SIM
329 Requirements.

- 330 **CFT-IMO-01** A cellular forensic tool shall have the ability to provide a presentation of acquired
331 data in a human-readable format via a generated report.

332 **CFT-IMO-02** A cellular forensic tool shall have the ability to provide a presentation of acquired
333 data in a human-readable format via a preview pane view.

334
335 **CFT-SIMO-01** A cellular forensic tool shall have the ability to provide a presentation of acquired
336 data in a human-readable format via a generated report.

337 **CFT-SIMO-02** A cellular forensic tool shall have the ability to provide a presentation of acquired
338 data in a human-readable format via a preview pane view.

339

340 **9.2.2 Protection**

341 Requirement CFT-IMO-03 applies to Optional Internal Memory Requirements. Requirement CFT-
342 SIMO-03 applies to Optional SIM Requirements.

343 **CFT-IMO-03** A cellular forensic tool shall have the ability to protect the overall case file and
344 individual data elements from modification.

345

346 **CFT-SIMO-03** A cellular forensic tool shall have the ability to protect the overall case file and
347 individual data elements from modification.

348

349 **9.2.3 Physical Acquisition**

350 Requirement CFT-IMO-04 applies to Optional Internal Memory Requirements. Requirement CFT-
351 SIMO-04 applies to Optional SIM Requirements.

352 **CFT-IMO-04** A cellular forensic tool shall have the ability to perform a physical acquisition of the
353 device's internal memory without modification for supported devices.

354

355 **CFT-SIMO-04** A cellular forensic tool shall have the ability to perform an acquisition of
356 the data present on supported Subscriber Identity Modules (SIMs) without
357 modification.

358

359 **9.2.4 Access Card Creation**

360 Requirement CFT-IMO-05 applies to Optional Internal Memory Requirements.

361 **CFT-IMO-05** A cellular forensic tool shall have the ability to create an access card following
362 manufacturer suggested protocols.

363

364 **9.2.5 Log Files**

365 Requirement CFT-IMO-06 applies to Optional Internal Memory Requirements. Requirement CFT-
366 SIMO-05 applies to Optional SIM Requirements.

367 **CFT-IMO-06** A cellular forensic tool shall have the ability to create user-accessible and readable
368 log files outlining the acquisition process.

369

370 **CFT-SIMO-05** A cellular forensic tool shall have the ability to create user-accessible and readable
371 log files outlining the acquisition process.

372 **9.2.6 Foreign Language**

373 Requirement CFT-IMO-07 applies to Optional Internal Memory Requirements. Requirement CFT-
374 SIM-06 applies to Optional SIM Requirements.

375 **CFT-IMO-07** A cellular forensic tool shall have the ability to present data objects containing
376 foreign language character sets acquired from the internal memory of the device via
377 the suggested interface (i.e., preview pane, generated report). Non-ASCII characters
378 shall be printed in their native format (e.g., Unicode UTF-8).
379

380 **CFT-SIMO-06** A cellular forensic tool shall have the ability to present data objects containing
381 foreign language character sets acquired from the SIM via the suggested interface
382 (i.e., preview pane, generated report). Non-ASCII characters shall be printed in their
383 native format (e.g., Unicode UTF-8).
384

385 **9.2.7 PIN Attempts**

386 Requirement CFT-SIMO-07 applies to Optional SIM Requirements.

387 **CFT-SIMO-07** A cellular forensic tool shall have the ability to present the remaining number of
388 CHV1/CHV2 PIN unlock attempts.
389

390 **9.2.8 PUK Attempts**

391 Requirement CFT-SIMO-08 applies to Optional SIM Requirements.

392 **CFT-SIMO-08** A cellular forensic tool shall have the ability to present the remaining number of
393 PUK unlock attempts.
394

395 **9.2.9 Stand-alone Acquisition**

396 Requirement CFT-IMO-08 applies to Optional Internal Memory Requirements.

397 **CFT-IMO-08** A cellular forensic tool shall have the ability to acquire internal memory data without
398 modifying data present on the SIM.
399

400 **9.2.10 Hashing**

401 Requirement CFT-IMO-09 through CFT-IMO-10 apply to Optional Internal Memory
402 Requirements. Requirement CFT-SIMO-09 through CFT-SIMO-10 apply to Optional SIM
403 Requirements.

404 **CFT-IMO-09** A cellular forensic tool shall have the ability to provide a hash for individual data
405 elements.

406 **CFT-IMO-10** A cellular forensic tool shall have the ability to provide a hash for the overall case
407 file.
408

409 **CFT-SIMO-09** A cellular forensic tool shall have the ability to provide a hash for individual data
410 elements.

411 **CFT-SIMO-10** A cellular forensic tool shall have the ability to provide a hash for the overall case
412 file.
413
414