

November 15, 2007

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**

Draft 2 for public comment of Version 1.0

39 **Abstract**

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

46

47 This paper defines requirements for mobile device applications capable of acquiring data from  
48 mobile devices operating over a Global System for Mobile communication (GSM) network, test  
49 methods used to determine whether a specific tool meets the requirements, and assertions derived  
50 from requirements producing measurable results.\* The assertions are described as general  
51 statements of conditions that can be checked after a test is executed. Each assertion generates one  
52 or more test cases consisting of a test protocol and the expected test results. The test protocol  
53 specifies detailed procedures for setting up the test, executing the test, and measuring the test  
54 results.

55

56 As this document evolves through comments updated versions will be posted at  
57 <http://www.cfft.nist.gov>.

58

---

\* 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

59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82

## 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

## 83 **1. Introduction**

84 As the intelligence and storage capabilities of mobile devices continue to advance, the need to  
85 ensure the reliability of mobile device forensic tools intensifies. The goal of the Computer Forensic  
86 Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to  
87 establish a methodology for testing computer forensic software tools by development of general tool  
88 specifications, test procedures, test criteria, test sets, and test hardware. The results provide the  
89 information necessary for toolmakers to improve tools, for users to make informed choices about  
90 acquiring and using computer forensic tools, and for interested parties to understand the tools  
91 capabilities. Our approach for testing computer forensic tools is based on well-recognized  
92 international methodologies for conformance testing and quality testing. This project is further  
93 described at: <http://www.cftt.nist.gov/>.

94  
95 The Computer Forensic Tool Testing (CFTT) program is a joint project of the National Institute of  
96 Justice (NIJ), the research and development organization of the U.S. Department of Justice, and the  
97 National Institute of Standards and Technology's (NIST's) Office of Law Enforcement Standards  
98 (OLES) and Information Technology Laboratory (ITL). CFTT is supported by other organizations,  
99 including the Federal Bureau of Investigation, the U.S. Department of Defense Cyber Crime Center,  
100 U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program, U.S.  
101 Department of Homeland Security's Bureau of Immigration and Customs Enforcement, U.S.  
102 Customs and Border Protection and the U.S. Secret Service. The objective of the CFTT program is  
103 to provide measurable assurance to practitioners, researchers, and other applicable users that the  
104 tools used in computer forensics investigations provide accurate results. Accomplishing this  
105 requires the development of specifications and test methods for computer forensics tools and  
106 subsequent testing of specific tools against those specifications.

107  
108 The central requirement for a sound forensic examination of digital evidence is that the original  
109 evidence must not be modified (i.e., the examination or capture of digital data from a mobile device  
110 and associated media must be performed without altering the device or media content). In the event  
111 that data acquisition is not possible using current technology to access information without  
112 configuration changes to the device (e.g., loading a driver), the changes must be documented and  
113 minimal (i.e., file size) to accomplish the required task.

114

## 115 **2. Purpose**

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

120

121 The requirements that will be tested are used to derive assertions. The assertions are described as  
122 general statements of conditions that can be checked after a test is executed. Each assertion  
123 generates one or more test cases consisting of a test protocol and the expected test results. The test  
124 protocol specifies detailed procedures for setting up the test, executing the test, and measuring the  
125 test results.

126

127 As this document evolves through comments updated versions will be posted at  
128 <http://www.cfft.nist.gov>.

129

### 130 **3. Scope**

131 The scope of this specification is limited to software tools capable of acquiring GSM devices and  
132 related media (i.e., SIM). The specifications are general and capable of being adapted to other types  
133 of mobile device software tailored for non-GSM devices.

134

### 135 **4. Glossary**

136 This glossary was added to provide context in the absence of official definitions recognized by the  
137 computer forensics community.

138

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

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

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

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

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

150 **CFT:** Cellular Forensic Tool.

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

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

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

156 **Hashing:** The process of creating a digital fingerprint by issuing a mathematical algorithm against a  
157 data element to produce a numeric value.

158 **Human-readable format:** Data (e.g., text, images) that is presented in a format that is able to be  
159 displayed and interpreted without decoding.

160 **IM:** Internal Memory.

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

163 **Mobile Subscriber International Subscriber Directory Number (MSISDN):** is intended to  
164 convey the telephone number assigned to the subscriber for receiving calls on the phone.

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

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

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

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

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

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

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

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

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

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

189 **User data:** Data populated onto the device using applications provided by the device.  
190

## 191 **5. Handset Characteristics - Internal Memory**

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

201

## 202 **6. SIM Characteristics**

203 Due to the GSM 11.11<sup>1</sup> standard, mobile device forensic tools designed to extract data from a SIM  
204 via an external reader should be able to properly acquire, decode, and present data in a human-  
205 readable format. An abundance of information is stored on the SIM such as Abbreviated Dialing  
206 Numbers (ADNs), Last Numbers Dialed (LND), Short Message Service (SMS) messages,  
207 subscriber information (i.e., IMSI), and location information (i.e., Location Information [LOCI],  
208 General Packet Radio Service Location [GPRSLOCI]). Tools optionally should provide support for  
209 Universal Subscriber Identity Modules (USIMs), the third generation (3G) card which carries out  
210 the same functions as its 2G cousin (i.e., SIM).

211  
212 Optionally, mobile device forensic tools should provide the ability to create an access SIM<sup>2</sup> in the  
213 event that the mobile equipment (ME) is found without the SIM present. Devices found without the  
214 SIM present may cause difficulty in acquiring the internal memory of the related device. Therefore,  
215 the ability to create an access card bypasses this problematic situation and allows for completion of  
216 internal memory acquisition.

217

## 218 **7. Digital Evidence**

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

224

- 225 • International Mobile Equipment Identifier (IMEI)
- 226 • Personal Information Management (PIM) data – (e.g., Address book, Calendar entries, to-do  
227 list, Tasks)
- 228 • Call Logs – Incoming and outgoing calls
- 229 • SMS text messages
- 230 • Multi-media Messages (MMS)/email – and associated data
- 231 • File Storage – Stand-alone files such as audio, graphic and video

232

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

234

- 235 • Service Provider Name (SPN)
- 236 • Integrated Circuit Card Identifier (ICCID)
- 237 • International Mobile Subscriber Identity (IMSI)
- 238 • Mobile Subscriber International ISDN Number (MSISDN)
- 239 • Abbreviated Dialing Numbers (ADNs)
- 240 • Last Numbers Dialed (LND)

---

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

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

- 241 • Short Message Service (SMS) – read, unread, deleted (that have not been overwritten)
- 242 • Enhanced Message Service (EMS) – messages over 160 characters
- 243 • Location Information (LOCI)
- 244 • General Packet Radio Service (GPRS) location – GPRSLOCI
- 245

## 246 **8. Test Methodology**

247 To provide concise test results of tools capabilities, the following test methodology will be strictly  
248 followed. The forensic application under evaluation will be installed on a dedicated (i.e., no other  
249 forensic applications are installed) host machine operating over the required platform as specified  
250 by the application. Two identical GSM devices will function as the source and target devices. The  
251 internal memory of the source device will be populated with a pre-defined dataset as will the SIM.  
252 Source, target devices and associated media (i.e., SIM), subsequent to initial data population, will  
253 be stored in a protected state eliminating the possibility of data modification due to network  
254 connectivity. The source SIM will be populated onto re-writeable SIMs (i.e., access cards), not  
255 capable of radio activity. Each succeeding test entails recreating the host testing environment for  
256 each specific tool tested and re-populating the target device and access SIM. During the acquisition  
257 process, all data transmissions (sent and received data packets) between the device and application  
258 will be captured and logged via a port monitoring utility.

259  
260 The following data elements will be used for populating the internal memory of the cellular device:  
261 Address book, PIM data, call logs, SMS messages, MMS messages/email with attachments (i.e.,  
262 images, audio, video) and stand-alone data files (i.e., audio, graphic, video). The following data  
263 elements will be used for populating the SIM: Abbreviated Dialing Numbers (ADNs), Last  
264 Numbers Dialed (LND), Short Messaging Service (SMS) messages marked as Read, Unread and  
265 Deleted, EMS messages, and location (LOCI) information.  
266

## 267 **9. Requirements**

268 The requirements are in two sections: 9.1 and 9.2. Section 9.1 lists requirements that all acquisition  
269 tools shall meet. Section 9.2 lists requirements that the tool shall meet on the condition that  
270 specified features or options are offered by the tool.

### 271 **9.1 Requirements for Core Features**

272 The following requirements are mandatory and shall be met by all mobile device forensic tools  
273 capable of acquiring internal handset memory and SIM memory.  
274

#### 275 **Internal Memory Requirements:**

- 276 **CFT-IM-01** A cellular forensic tool shall have the ability to recognize supported devices via the  
277 vendor supported interfaces (e.g., cable, Bluetooth, Infrared).
- 278 **CFT-IM-02** A cellular forensic tool shall have the ability to identify non-supported devices.
- 279 **CFT-IM-03** A cellular forensic tool shall have the ability to notify the user of connectivity errors  
280 between the device and application during acquisition.
- 281 **CFT-IM-04** A cellular forensic tool shall have the ability to provide the user with either a  
282 preview pane or generated report view of data acquired.

283 **CFT-IM-05** A cellular forensic tool shall have the ability to logically acquire all application  
284 supported data elements present in internal memory without modification.  
285  
286

287 **SIM Requirements:**

288 **CFT-SIM-01** A cellular forensic tool shall have the ability to recognize supported SIMs via the  
289 vendor supported interface (e.g., PC/SC reader, proprietary reader).

290 **CFT-SIM-02** A cellular forensic tool shall have the ability to identify non-supported SIMs.

291 **CFT-SIM-03** A cellular forensic tool shall have the ability to notify the user of connectivity errors  
292 between the SIM reader and application during acquisition.

293 **CFT-SIM-04** A cellular forensic tool shall have the ability to provide the user with the opportunity  
294 to unlock a password protected SIM before acquisition

295 **CFT-SIM-05** A cellular forensic tool shall have the ability to provide the user with either a  
296 preview pane or generated report view of data acquired.

297 **CFT-SIM-06** A cellular forensic tool shall have the ability to acquire all application supported data  
298 elements present in the SIM memory without modification  
299

300 **9.2 Requirements for Optional Features**

301 The following requirements define optional tool features. If a tool provides the capability defined,  
302 the tool is tested as if the requirement were mandatory. If the tool does not provide the capability  
303 defined, the requirement does not apply.  
304

305 The following optional features are identified:

- 306 • Presentation
- 307 • Protection
- 308 • Physical acquisition
- 309 • Access Card/Radio Isolation Card creation
- 310 • Log file creation
- 311 • Foreign language character support
- 312 • Remaining PIN attempts
- 313 • Remaining PUK attempts
- 314 • Stand-alone acquisition
- 315 • Hashing
- 316

317 **9.2.1 Presentation**

318 Requirements CFT-IMO-01 through CFT-IMO-02 apply to Optional Internal Memory  
319 Requirements. Requirements CFT-SIMO-01 through CFT-SIMO-02 apply to Optional SIM  
320 Requirements.

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

323 **CFT-IMO-02** A cellular forensic tool shall have the ability to provide a presentation of acquired  
324 data in a human-readable format via a preview pane view.  
325

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

328 **CFT-SIMO-02** A cellular forensic tool shall have the ability to provide a presentation of acquired  
329 data in a human-readable format via a preview pane view.  
330

### 331 **9.2.2 Protection**

332 Requirement CFT-IMO-03 applies to Optional Internal Memory Requirements. Requirement CFT-  
333 SIMO-03 applies to Optional SIM Requirements.

334 **CFT-IMO-03** A cellular forensic tool shall have the ability to protect the overall case file and  
335 individual data elements from modification.  
336

337 **CFT-SIMO-03** A cellular forensic tool shall have the ability to protect the overall case file and  
338 individual data elements from modification.  
339

### 340 **9.2.3 Physical Acquisition**

341 Requirement CFT-IMO-04 applies to Optional Internal Memory Requirements. Requirement CFT-  
342 SIMO-04 applies to Optional SIM Requirements.

343 **CFT-IMO-04** A cellular forensic tool shall have the ability to perform a physical acquisition of the  
344 device's internal memory without modification for supported devices.  
345

346 **CFT-SIMO-04** A cellular forensic tool shall have the ability to perform an acquisition of  
347 the data present on supported Subscriber Identity Modules (SIMs) without  
348 modification.  
349

### 350 **9.2.4 Access Card Creation**

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

352 **CFT-IMO-05** A cellular forensic tool shall have the ability to create an access card following  
353 manufacturer suggested protocols.  
354

### 355 **9.2.5 Log Files**

356 Requirement CFT-IMO-06 applies to Optional Internal Memory Requirements. Requirement CFT-  
357 SIMO-05 applies to Optional SIM Requirements.

358 **CFT-IMO-06** A cellular forensic tool shall have the ability to create user-accessible and readable  
359 log files outlining the acquisition process.  
360

361 **CFT-SIMO-05** A cellular forensic tool shall have the ability to create user-accessible and readable  
362 log files outlining the acquisition process.  
363

364 **9.2.6 Foreign Language**

365 Requirement CFT-IMO-07 applies to Optional Internal Memory Requirements. Requirement CFT-  
366 SIM-06 applies to Optional SIM Requirements.

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

371  
372 **CFT-SIMO-06** A cellular forensic tool shall have the ability to present data objects containing  
373 foreign language character sets acquired from the SIM via the suggested interface  
374 (i.e., preview pane, generated report). Non-ASCII characters shall be printed in their  
375 native format (e.g., Unicode UTF-8).

376

377 **9.2.7 PIN Attempts**

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

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

381

382 **9.2.8 PUK Attempts**

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

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

386

387 **9.2.9 Stand-alone Acquisition**

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

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

391

392 **9.2.10 Hashing**

393 Requirement CFT-IMO-09 through CFT-IMO-10 apply to Optional Internal Memory  
394 Requirements. Requirement CFT-SIMO-09 through CFT-SIMO-10 apply to Optional SIM  
395 Requirements.

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

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

400

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

403 **CFT-SIMO-10** A cellular forensic tool shall have the ability to provide a hash for the overall case  
404 file.

405

406