

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

Non-GSM Mobile Device Tool Specification

Version 1.1

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 Code Division Multiple Access (CDMA) network and test methods
55 used to determine whether a specific tool meets the requirements for producing measurable results.*
56 Test requirements are statements used to derive test cases that define expectations of a tool or
57 application. Test cases describe the combination of test parameters required to test each assertion.
58 Test assertions are described as general statements or conditions that can be checked after a test is
59 executed. Each assertion appears in one or more test cases consisting of a test protocol and the
60 expected test results. The test protocol specifies detailed procedures for setting up the test,
61 executing the test, and measuring the test results. The associated assertions and test cases are
62 defined in the test plan document entitled: [Non-GSM Mobile Device Tool Test Assertions and Test](#)
63 [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.

TABLE OF CONTENTS

67		
68		
69	1. Introduction	1
70	2. Purpose	1
71	3. Scope	2
72	4. Glossary	2
73	5. Handset Characteristics - Internal Memory	3
74	6. Digital Evidence	3
75	7. Test Methodology	4
76	8. Requirements	4
77	8.1 Requirements for Core Features	4
78	8.2 Requirements for Optional Features	5
79	8.2.1 Presentation	5
80	8.2.2 Protection	5
81	8.2.3 Physical Acquisition	5
82	8.2.4 Log Files	5
83	8.2.5 Foreign Language	5
84	8.2.6 Hashing	6
85		

86 **1. Introduction**

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

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

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

119

120 **2. Purpose**

121 This document defines requirements for mobile device forensic tools used in digital forensics
122 capable of acquiring internal memory from Code Division Multiple Access (CDMA) devices and
123 test methods used to determine whether a specific tool meets the requirements.

124

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

130

131 **3. Scope**

132 The scope of this specification is limited to software tools capable of acquiring CDMA devices.
133 The specifications are general and capable of being adapted to other types of mobile device forensic
134 software.

135

136 **4. Glossary**

137 This glossary provides context in the absence of an official lexicon recognized by the computer
138 forensics community.

139

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

142 **Acquisition File:** A snapshot of data contained within the internal memory of a target device.

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

146 **CDMA:** Code Division Multiple Access describes a communication channel access principle that
147 employs spread-spectrum technology and a special coding scheme.

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 **Electronic Serial Number (ESN):** ESNs, which uniquely identified CDMA phones, were issued
152 until 2005. An ESN number consist of a 32-bit alpha-numeric character set that allowed a
153 maximum of 4 billion unique numbers.

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

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

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

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

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

163 **IM:** Internal Memory.

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

166 **Mobile Equipment Identity (MEID):** An ID number that is globally unique for CDMA mobile
167 phones, identifying the device to the network and can be used to flag lost or stolen devices.

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

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

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

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

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

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

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

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

185 **User data:** Data populated onto the device using applications provided by the device.
186

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

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

198 **6. Digital Evidence**

199 The amount and richness of data contained on mobile devices is dependent upon device type (i.e.,
200 low-end, high-end) and personal usage. However, there is a core set of data that computer forensic
201 tools can recover that remains somewhat consistent on all devices with cellular capabilities. Tools
202 should have the ability to recover the following data elements stored in the device's internal handset
203 memory:
204

- 205 • Mobile Equipment Identifier (MEID) / Electronic Serial Number (ESN)
- 206 • Personal Information Management (PIM) data – (e.g., Address book, Calendar entries, to-do
207 list, Tasks)

- 208 • Call logs – Incoming and outgoing calls
 - 209 • Text messages (SMS, EMS)
 - 210 • Multi-media Messages (MMS)/email – and associated data
 - 211 • File storage – Stand-alone files such as audio, graphic and video
- 212

213 **7. Test Methodology**

214 To provide concise test results, the following test methodology will be strictly followed. Each
215 forensic application under evaluation will be installed on a dedicated (i.e., no other forensic
216 applications are installed) host computer operating with the required platform as specified by the
217 application. The internal memory of the source device will be populated with a pre-defined dataset.
218 Data population techniques and procedures are outlined in the Non-GSM Mobile Device Tool Setup
219 and Test Procedures document. Source devices will be stored in a protected state subsequent to
220 initial data population, thus eliminating the possibility of data modification due to network
221 connectivity. Each succeeding test entails recreating the host-testing environment for each specific
222 tool tested.

223
224 The following data elements will be used in populating the internal memory of the cellular device:
225 Address book, PIM data, call logs, text messages (SMS, EMS), MMS messages/email with
226 attachments (i.e., audio, graphic, video) and stand-alone data files (i.e., audio, graphic, video).

227

228 **8. Requirements**

229 The requirements are in two sections: 8.1 and 8.2. Section 8.1 lists requirements (i.e., Cellular
230 Forensic Tool-Internal Memory-01 [CFT-IM-01] through CFT-IM-05) that all acquisition tools
231 shall meet. Section 8.2 lists requirements (i.e., Cellular Forensic Tool-Internal Memory Optional-
232 01 [CFT-IMO-01] though CFT-IMO-08) that the tool shall meet on the condition that specified
233 features or options are offered by the tool.

234

235 **8.1 Requirements for Core Features**

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

238

239 **Internal Memory Requirements:**

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

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

243 **CFT-IM-03** A cellular forensic tool shall have the ability to notify the user of connectivity errors
244 between the device and application during acquisition.

245 **CFT-IM-04** A cellular forensic tool shall have the ability to provide the user with either a
246 preview pane or generated report view of data acquired.

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

249 **8.2 Requirements for Optional Features**

250 The following requirements define optional tool features. If a tool provides the capability defined,
251 the tool is tested for conformance to these requirements. If the tool does not provide the capability
252 defined, the requirement does not apply.

253

254 The following optional features are identified:

- 255 • Presentation
- 256 • Protection
- 257 • Physical acquisition
- 258 • Log file creation
- 259 • Foreign language character support
- 260 • Hashing

261

262 **8.2.1 Presentation**

263 Requirements CFT-IMO-01 and CFT-IMO-02 apply to Optional Presentation of Internal Memory.

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

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

268

269 **8.2.2 Protection**

270 Requirement CFT-IMO-03 applies to Optional Protection of Internal Memory.

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

273

274 **8.2.3 Physical Acquisition**

275 Requirement CFT-IMO-04 applies to Optional Physical Acquisition of Internal Memory.

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

278

279 **8.2.4 Log Files**

280 Requirement CFT-IMO-05 applies to Optional Log Filing of Internal Memory acquisition.

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

283

284 **8.2.5 Foreign Language**

285 Requirement CFT-IMO-06 applies to Optional Foreign Language acquisition from Internal
286 Memory.

287 **CFT-IMO-06** A cellular forensic tool shall have the ability to present data objects containing non-
288 ASCII character sets acquired from the internal memory of the device via the
289 suggested interface (i.e., preview pane, generated report). Non-ASCII characters
290 shall be printed in their native format (e.g., Unicode UTF-8).
291

292 **8.2.6 Hashing**

293 Requirements CFT-IMO-07 and CFT-IMO-08 apply to Optional Hashing of Internal Memory.

294 **CFT-IMO-07** A cellular forensic tool shall have the ability to provide a hash for individual data
295 elements.

296 **CFT-IMO-08** A cellular forensic tool shall have the ability to provide a hash for the overall case
297 file.