

May 1, 2008

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

Draft 1 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, mobile 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 Code Division Multiple Access (CDMA) network, test methods
49 used to determine whether a specific tool meets the requirements, and assertions derived from
50 requirements producing measurable results.* The assertions are described as general statements of
51 conditions that can be checked after a test is executed. Each assertion generates one or more test
52 cases consisting of a test protocol and the expected test results. The test protocol specifies detailed
53 procedures for setting up the test, executing the test, and measuring the test results.

54

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

57

* 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

58

59

60 1. Introduction 1

61 2. Purpose 1

62 3. Scope 2

63 4. Glossary 2

64 5. Handset Characteristics - Internal Memory 3

65 6. Digital Evidence 3

66 7. Test Methodology 4

67 8. Requirements 4

68 8.1 Requirements for Core Features 4

69 8.2 Requirements for Optional Features 5

70 8.2.1 Presentation 5

71 8.2.2 Protection 5

72 8.2.3 Physical Acquisition 5

73 8.2.4 Log Files 5

74 8.2.5 Foreign Language 6

75 8.2.6 Hashing 6

76

77 1. Introduction

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

88
89 The Computer Forensic Tool Testing (CFTT) program is a joint project of the National Institute of
90 Justice (NIJ), the research and development organization of the U.S. Department of Justice, and the
91 National Institute of Standards and Technology's (NIST's) Office of Law Enforcement Standards
92 (OLES) and Information Technology Laboratory (ITL). CFTT is supported by other organizations,
93 including the Federal Bureau of Investigation, the U.S. Department of Defense Cyber Crime Center,
94 U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program, U.S.
95 Department of Homeland Security's Bureau of Immigration and Customs Enforcement, U.S.
96 Customs and Border Protection and the U.S. Secret Service. The objective of the CFTT program is
97 to provide measurable assurance to practitioners, researchers, and other applicable users that the
98 tools used in computer forensics investigations provide accurate results. Accomplishing this
99 requires the development of specifications and test methods for computer forensics tools and
100 subsequent testing of specific tools against those specifications.

101
102 The central requirement for a sound forensic examination of digital evidence is that the original
103 evidence must not be modified (i.e., the examination or capture of digital data from a mobile device
104 and associated media must be performed without altering the device or media content). In the event
105 that data acquisition is not possible using current technology to access information without
106 configuration changes to the device (e.g., loading a driver), the changes must be documented and
107 minimal (i.e., file size) to accomplish the required task.

108

109 2. Purpose

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

113

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

119

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

122

123 **3. Scope**

124 The scope of this specification is limited to software tools capable of acquiring CDMA devices.
125 The specifications are general and capable of being adapted to other types of mobile device
126 software tailored for GSM devices.

127

128 **4. Glossary**

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

131

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

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

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

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

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

143 **CFT:** Cellular Forensic Tool.

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

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

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

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

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

153 **IM:** Internal Memory.

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

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

158 **Multimedia Messaging Service (MMS) message:** Provides users with the ability
159 to send text messages containing multimedia objects (i.e., graphic, audio, video).
160 **Preview pane:** Section of the Graphical User Interface (GUI) that provides a snapshot of the
161 acquired data.
162 **Physical acquisition:** A bit-by-bit copy of the data layer.
163 **Personal Information Management (PIM) data:** Data that contains personal information such as:
164 calendar entries, to-do lists, memos, reminders, etc.
165 **Short Message Service (SMS):** A service used for sending text messages (up to 160 characters) to
166 mobile devices.
167 **Smart phone:** A full-featured mobile phone that provides users with personal
168 computer like functionality by incorporating PIM applications, enhanced Internet
169 connectivity and email operating over an Operating System supported by superior
170 processing and high capacity storage.
171 **Stand-alone data:** Data (e.g., graphic, audio, video) that is not associated with or has not been
172 transferred to the device via email or MMS message.
173 **User data:** Data populated onto the device using applications provided by the device.
174

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

176 Mobile devices, designed with the primary purpose of placing and receiving calls, maintain data in
177 flash memory. Typically, the first part of flash memory is filled with the operating system and the
178 second part is allocated for user data. Although information is stored in a proprietary format,
179 forensic tools tailored for mobile device acquisition should minimally be able to perform a logical
180 acquisition for supported devices and provide a report of the data present in the internal memory.
181 Tools that possess a low-level understanding of the proprietary data format for a specific device
182 may provide examiners with the ability to perform a physical acquisition and generate reports in a
183 meaningful (i.e., human-readable) format. Currently, the tools capable of performing a physical
184 acquisition on a mobile device are limited.
185

186 **6. Digital Evidence**

187 The amount and richness of data contained on mobile devices is dependent upon device type (i.e.,
188 low-end, high-end) and personal usage. However, there is a core set of data that computer forensic
189 tools can recover that remains somewhat consistent on all devices with cellular capabilities. GSM
190 devices provide two areas for data storage: device internal memory and the SIM. Tools should have
191 the ability to recover the following data elements stored in the device's internal handset memory:
192

- 193 • International Mobile Equipment Identifier (IMEI)
- 194 • Personal Information Management (PIM) data – (e.g., Address book, Calendar entries, to-do
195 list, Tasks)
- 196 • Call logs – Incoming and outgoing calls
- 197 • Text messages (SMS, EMS)

- 198
- Multi-media Messages (MMS)/email – and associated data
 - File storage – Stand-alone files such as audio, graphic and video
- 199

200

201 **7. Test Methodology**

202 To provide concise test results of tools capabilities, the following test methodology will be strictly
203 followed. The forensic application under evaluation will be installed on a dedicated (i.e., no other
204 forensic applications are installed) host machine operating over the required platform as specified
205 by the application. Two identical CDMA devices will function as the source and target devices.
206 The internal memory of the source device will be populated with a pre-defined dataset. Source and
207 target devices subsequent to initial data population, will be stored in a protected state eliminating
208 the possibility of data modification due to network connectivity. Each succeeding test entails
209 recreating the host testing environment for each specific tool tested and re-populating the target.
210 During the acquisition process, all data transmissions (sent and received data packets) between the
211 device and application will be captured and logged via a port monitoring utility.

212

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

216

217 **8. Requirements**

218 The requirements are in two sections: 8.1 and 8.2. Section 8.1 lists requirements that all acquisition
219 tools shall meet. Section 8.2 lists requirements that the tool shall meet on the condition that
220 specified features or options are offered by the tool.

221

222 **8.1 Requirements for Core Features**

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

225

226 **Internal Memory Requirements:**

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

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

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

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

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

236

237

238 **8.2 Requirements for Optional Features**

239 The following requirements define optional tool features. If a tool provides the capability defined,
240 the tool is tested as if the requirement were mandatory. If the tool does not provide the capability
241 defined, the requirement does not apply.

242
243 The following optional features are identified:

- 244 • Presentation
 - 245 • Protection
 - 246 • Physical acquisition
 - 247 • Log file creation
 - 248 • Foreign language character support
 - 249 • Hashing
- 250

251 **8.2.1 Presentation**

252 Requirements CFT-IMO-01 through CFT-IMO-02 apply to Optional Internal Memory
253 Requirements.

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

256 **CFT-IMO-02** A cellular forensic tool shall have the ability to provide a presentation of acquired
257 data in a human-readable format via a preview pane view.
258

259 **8.2.2 Protection**

260 Requirement CFT-IMO-03 applies to Optional Internal Memory Requirements.

261 **CFT-IMO-03** A cellular forensic tool shall have the ability to protect the overall case file and
262 individual data elements from modification.
263

264 **8.2.3 Physical Acquisition**

265 Requirement CFT-IMO-04 applies to Optional Internal Memory Requirements.

266 **CFT-IMO-04** A cellular forensic tool shall have the ability to perform a physical acquisition of the
267 device's internal memory without modification for supported devices.
268

269 **8.2.4 Log Files**

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

271 **CFT-IMO-05** A cellular forensic tool shall have the ability to create user-accessible and readable
272 log files outlining the acquisition process.
273
274
275

276 **8.2.5 Foreign Language**

277 Requirement CFT-IMO-06 applies to Optional Internal Memory Requirements.

278 **CFT-IMO-06** A cellular forensic tool shall have the ability to present data objects containing
279 foreign language character sets acquired from the internal memory of the device via
280 the suggested interface (i.e., preview pane, generated report). Non-ASCII characters
281 shall be printed in their native format (e.g., Unicode UTF-8).
282

283 **8.2.6 Hashing**

284 Requirement CFT-IMO-07 through CFT-IMO-08 apply to Optional Internal Memory
285 Requirements.

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

288 **CFT-IMO-08** A cellular forensic tool shall have the ability to provide a hash for the overall case
289 file.
290
291
292
293
294
295