司　法　鉴　定　技　术　规　范

SF/Z JD0401002——2015

手机电子数据提取操作规范

2015-11-20 发布　　2015-11-20 实施

中华人民共和国司法部司法鉴定管理局　发布

目　　次

前　言

本技术规范按照GB/T 1.1-2009给出的规则起草。

本技术规范由上海辰星电子数据司法鉴定中心提出。

本技术规范由司法部司法鉴定管理局归口。

本技术规范起草单位：上海辰星电子数据司法鉴定中心。

本技术规范主要起草人：崔宇寅、郭弘、雷云婷、蔡立明、金波、杨涛、高峰、沙晶、张云集、张颖、黄道丽、张晓、孙杨。

手机电子数据提取操作规范

1 范围

本技术规范规定了电子数据鉴定中手机电子数据提取的方法和流程步骤。

本技术规范适用于各类手机内置存储数据、存储卡中数据和SIM卡中数据的检验。

2 术语和定义

SF/Z JD0400001－2014 和 SF/Z JD0401001－2014 界定的以及下列术语和定义适用于本技术规范。

2.1

SIM卡 Subscriber Identity Module Card

保存移动电话服务的用户身份识别数据的智能卡，也称为用户身份模块卡。SIM卡主要用于GSM系统，但是兼容的模块也用于UMTS的UE（USIM）和IDEN电话。CDMA2000和cdmaOne的RUIM卡和UIM卡，也称作SIM卡；按照物理规格可分为Full-Size、Mini-Size、Micro-Size和Nano-Size。

2.2

外置存储卡 Removable Storage Card

用于扩展数字移动电话存储空间的外部闪存介质。

2.3

信号屏蔽容器 Radio Isolation Container

可完全隔离手机所具备的3G、GSM、Wifi、红外和蓝牙等通信信号的容器，如信号屏蔽袋。

2.4

PIN Personal Identity Number

PIN码(PIN1)是用户和SIM卡系统间的身份识别密码，只有用户输入的PIN码和SIM卡系统中存储的密码相同时，用户才被授权访问。

2.5

IMSI International Mobile Subscriber Identification Number

国际移动用户识别码（IMSI）是区别移动用户的标志，储存在SIM卡中，可用于区别移动用户的有效信息。其结构为MCC+MNC+MSIN,其中MCC是移动用户所属国家代号，占3位数字；MNC是移动网号码，由两位或者三位数字组成，用于识别移动用户所归属的移动通信网；MSIN是移动用户识别码，用以识别某一移动通信网中的移动用户。

2.6

ICCID Integrate circuit card identity

集成电路卡识别码（ICCID），为SIM卡的唯一识别号码，共有20位数字组成，其编码格式为：XXXXXX 0MFSS YYGXX XXXXX，其中前六位运营商代码。

2.7

JTAG Joint Test Action Group

一种国际标准测试协议，主要用于芯片内部测试及对系统进行仿真、调试，JTAG技术是一种嵌入式调试技术，它在芯片内部封装了专门的测试电路TAP（Test Access Port，测试访问口），通过专用的JTAG测试工具对内部节点进行测试。

2.8

IMEI International Mobile Equipment Identity

国际移动设备识别码（手机序列号），用于在手机网络中识别每一部独立的手机，是国际上公认的手机标志序号。

3 现场获取

3.1 准备

在进行手机电子数据现场获取之前，需分析案情并进行准备工作，包括：

a) 现场获取的目的和范围；
b) 现场获取的人员，需明确分工，落实责任；
c) 明确手机现场获取需携带的仪器设备；
d) 明确手机现场获取采用的方法、标准和规范；
e) 明确手机现场获取步骤；
f) 明确手机现场获取操作可能造成的影响。

3.2 证据获取

3.2.1 静态获取

对于已经关闭的手机，在法律允许的范围内并在获得授权的情况下，对手机进行拍照或者拍摄，获取并记录手机的相关附件设备和信息，包括但不限于：

a） 手机品牌和型号；
b） 手机唯一性标示（如：IMEI号）；
c） 手机SIM卡和外置存储卡；
d） 手机的启动密码和PIN码；
e） 手机附件设备（如：电源线、数据线和其它配备设备）和相关手册。

3.2.2 动态获取

3.2.2.1 对于处于运行状态的手机，如未启用安全验证机制（如开机密码和 PIN 码）或能获取解决安全验证机制的方法，应按照 3.2.1 方法进行获取，并记录手机的操作系统。

3.2.2.2 如手机已启用安全验证机制（如开机密码和 PIN 码），且无法获取解决安全验证机制的方法，应将手机从无线网络隔离后提取数据。将手机从无线网络隔离的方法包括：

a） 电子/射频屏蔽；
b） 设置为“飞行”模式；
c） 禁用Wi-Fi、蓝牙和红外通信。

3.2.2.3 如需获取证据数据的手机正连接计算机进行同步，应采取以下措施：

a） 在获取计算机安全机制的情况下，关闭计算机电源，防止数据传输或同步覆盖；
b） 同时获取手机和连接的数据线、底座和与其同步的计算机，用于从计算机的硬盘中获取手机中未获取的同步数据；
c） 不可取出手机中的数据存储卡和SIM卡。

3.3 封存

3.3.1 已经关闭的手机，应采取以下措施进行封存：

a） 如手机的电池可拆卸，应取下电池；
b） 使用信号屏蔽容器进行封存，并予以标记；

c） 封存前后应对手机进行拍照或录像，照片或者录像应当从各个角度反映手机封存前后的状况，清晰反映封口或张贴封条处的状况。

3.3.2 处于运行状态的手机，如需保持开机状态，应采取以下措施进行封存：

a） 使用带有适配电源的信号屏蔽容器进行封存，并予以标记；

b） 将手机放置在专门设计的硬质容器中，防止无意触碰按键；

c） 封存前后应对手机进行拍照或录像，照片或者录像应当从各个角度反映手机封存前后的状况，清晰反映封口或张贴封条处的状况。

注1：信号屏蔽容器在使用前需经过测试，确保对3G、GSM、WIFI、红外和蓝牙等通信信号的屏蔽。

注2：手机信号与基站通信并非实时，当手机放入信号屏蔽容器中，信号完全屏蔽需要等待10-20秒时间。

注3：对于多个送检手机，应独立封存，防止送检手机之间的交叉污染。

4 实验室检验

4.1 记录送检手机的情况

4.1.1 对送检手机进行唯一性编号。

4.1.2 对送检手机进行拍照，并记录其特征。

4.1.3 获取和记录送检手机的相关信息，应包括但不限于：

a） 品牌、型号和操作系统；

b） 唯一性标示；

c） SIM 卡；

d） 外置存储卡；

e） 开机密码和 PIN 码；

f） 附件设备（如：电源线、数据线和其它配备设备）和相关手册。

4.2 数据的检验分析

4.2.1 手机存储数据获取

根据送检要求，对送检手机的获取可分层次进行，根据情况选择以下的一项或多项进行：

a） 手工获取：不借助其他手机取证设备，对屏显数据进行获取；

b） 逻辑获取：对送检手机的文件系统进行获取；

c） 物理获取（镜像获取/JTAG）：对送检手机文件系统进行镜像备份，或使用JTAG方式进行获取；

d） 芯片获取：对送检手机中的物理内存芯片进行获取；

e） 微读获取：使用高倍电子显微镜检验对手机内存单元进行物理观察以获取数据。

注1：根据送检要求，可对送检手机进行提高操作权限的检验手段<如root等>。

4.2.2 SIM卡的数据获取

通过手机取证设备或者SIM卡取证设备对SIM卡进行复制，从复制的SIM卡中提取数据。SIM卡中提取的数据包含但不限于：

a） IMSI；

b） ICCID；

c） 短消息；

d） 通讯录；

e） 通话记录。

4.2.3 外置存储卡数据获取

外置存储卡中数据的恢复和获取按照GB/T 29360－2012和GA/T 756－2008的要求进行。

5 检出数据

计算检出数据的哈希值，并复制到专用的存储介质中。

6 检验记录

检验时需做好检验记录，记录应贯穿整个检验过程，记录的内容应包括但不限于：

a) 检验开始的时间和日期；
b) 送检手机和相关附件的物理状况；
c) 送检手机接受时的状态（关闭或开启）；
d) 送检手机的品牌、型号、服务提供商等信息；
e) 检验过程中使用的方法、标准和规范；
f) 检验过程中使用的软、硬件工具；
g) 检验过程所在的环境；
h) 检验的人员信息；
i) 检验过程中发生的异常；
j) 检验过程数据。