6 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。

7 记录

检验时需做好检验记录，记录应贯穿整个检验过程，记录应包括：

a) 检验开始的时间和日期；
b) 送检移动终端的物理状况；
c) 送检移动终端和其部件的照片；
d) 送检移动终端接受时的状态(关闭或开启)；
e) 送检移动终端的品牌、型号、服务提供商等信息；
f) 检验过程中所使用的软、硬件工具。

GA/T 1170—2014

GA/T 1170-2014

*
书号：155066・2-27340
定价： 14.00 元

ICS 35.240.01
A 92

GA

中华人民共和国公共安全行业标准

GA/T 1170—2014

移动终端取证检验方法

Examination methods for evidence collection from mobile terminals

2014-07-09 发布 2014-07-09 实施

中华人民共和国公安部 发布

中华人民共和国公共安全
行 业 标 准
移动终端取证检验方法
GA/T 1170—2014
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 0.5 字数 8 千字
2014年9月第一版 2014年9月第一次印刷
*
书号:155066·2-27340 定价 14.00 元

5 实验室检验

5.1 识别

通过查看品牌、型号、服务提供商和设备标识,识别送检移动终端。

5.2 准备检验用的设备

用于移动终端检验的实验室设备应满足以下要求:

a) 进行定期验证,确保性能稳定;
b) 定期审查设备的当前信息(如用户手册)以及其他相关文件,确保可随时获取;
c) 确保检验用的应用程序是最新的稳定版本,并在使用前进行验证。

5.3 数据的检验分析

5.3.1 移动终端的检验分析

移动终端中数据的检验和分析应分层次进行,根据情况选择以下的一项或多项进行检验:

a) 手工分析:通过移动终端键盘和移动终端显示屏查看并记录移动终端内存中的数据;
b) 逻辑分析:使用数据电缆连接到移动终端采集数据,不包括访问已被删除的数据;
c) 镜像备份(物理分析):对移动终端文件系统进行物理镜像备份,对备份数据进行分析,恢复未被覆盖的被删除数据;
d) 卸载内存芯片分析(物理分析):卸载移动终端的存储芯片,读取芯片中的数据;
e) 微读(物理分析):使用高倍电子显微镜检验存储器的电子电路以采集数据。

5.3.2 记忆卡的检验分析

记忆卡中数据的检验分析按照GA/T 756—2008的要求进行。

5.3.3 SIM卡的检验分析

SIM卡中数据的检验分析使用专用的SIM卡读取设备进行。

5.3.4 注意事项

检验分析过程应注意以下事项:

a) 记录移动终端的状况;
b) 采取预防措施隔离移动终端连接网络;
c) 检验过程中,确保移动终端被持续供电;
d) 如移动终端能进行多项检验,先进行物理分析,后进行逻辑分析;
e) 根据以下顺序,使用一种或多种方式获取数据:
   1) 电缆;
   2) 拍照/录像;
   3) 红外线;
   4) 蓝牙;
f) 单独分析移动终端的内存、SIM卡和存储卡等证据介质,以免破坏数据;
g) 所有含SIM卡的移动终端需检验两次:安装SIM卡检验和卸载SIM卡检验。

4 现场证据的获取

4.1 评估现场

确定对移动终端中的证据数据进行现场获取的人员和需携带的必要设备，人员应具备识别不同类型的移动终端并熟悉其特性和相关配件的能力。

对移动终端中的证据数据进行现场获取前，需对现场情况进行评估，根据现场情况制定计划，包括：

a) 现场获取的目的和范围；
b) 现场获取采用的标准规范；
c) 现场获取的顺序。

4.2 获取和保护证据设备

4.2.1 获取

按照所制定的计划，获取移动终端及相关附件设备和资料。如需获取证据数据的移动终端正连接计算机进行同步，应采取以下措施：

a) 关闭计算机电源，防止数据传输或同步覆盖；
b) 同时获取移动终端和连接的电缆、底座和与其同步的计算机，以便从计算机的硬盘中获取移动终端中未获取的同步数据；
c) 不可取出移动终端中的数据存储卡和 SIM 卡；
d) 获取移动终端的相关附件设备和资料，如：电源、电缆、底座、产品说明书和软件等。

4.2.2 隔离

为防止移动终端中的证据数据被破坏，应将移动终端从无线网络隔离，方法包括：

a) 立即关闭移动终端，不得再次打开，以免破坏数据。如电池可拆卸，取出电池；
b) 紧急情况下，可保持移动终端开机状态作紧急处理。如果移动终端需保持开机，需在供电状态下将其从网络上隔离，方法包括：
   1) 射频屏蔽；
   2) 将移动终端设置为“飞行”模式；
   3) 禁用 Wi-Fi、蓝牙和红外通信。

4.2.3 包装

对移动终端的包装应满足以下要求：

a) 将移动终端密封在防静电袋中，并予以标记；
b) 正确保护移动终端，防止无意触碰按键，如放置在专门设计的硬质容器中；
c) 使用射频隔离袋屏蔽移动终端的无线电信号。

4.2.4 运输

对移动终端的运输应满足以下要求：

a) 谨慎处理、充分保护移动终端，防止震动、湿度和极端温度对移动终端造成影响；
b) 移动终端保持开机状态时，应使用独立的外部电源进行充电；
c) 如电源适配器与无线频率隔离袋一起使用，应妥善保护电缆，防止隔离袋失效。

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部第三研究所提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部第三研究所。

本标准主要起草人：郭弘、黄道丽、金波、赵戈、杭强伟、徐隽。