



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.gb168.cn

服务热线: 400-168-0010

010-68522006

2014年9月第一版

*

书号: 155066·2-27340

版权专有 侵权必究

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、徐隼。

移动终端取证检验方法

1 目的和范围

本标准规定了电子数据检验时,从移动终端(不包括具有无线上网功能的笔记本电脑)获取、分析与呈现证据数据的检验方法。

本标准适用于电子数据检验工作中,从移动终端(不包括具有无线上网功能的笔记本电脑)获取、分析与呈现证据数据。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GA/T 756—2008 数字化设备证据数据发现提取固定方法

GA/T 976—2012 电子数据法庭科学鉴定通用方法

3 术语和定义

GA/T 756—2008 和 GA/T 976—2012 界定的以及下列术语和定义适用于本文件。

3.1

移动终端 mobile terminal

基于移动网络应用的设备,包括但不限于手机、无线上网卡等通讯终端、具有无线上网功能的笔记本电脑、平板电脑、游戏机、PDA、MP4 等设备,以及无线定位、无线监控等终端。

3.2

蓝牙 bluetooth

一种无线数据和语音传输技术,将各种通信设备、计算机及其终端设备、各种数字数据系统,甚至家用电器采用无线方式连接起来,传输距离为 10 cm 至 10 m。采用分散式网络结构以及快跳频和短包技术,支持点对点及点对多点通信,工作在全球通用的 2.4GHz ISM 频段。

3.3

无线保真 Wi-Fi

一种无线局域网通讯技术,基于 IEEE 802.11 标准,属于在办公室和家庭中使用的短距离无线技术。

3.4

红外通信 infrared communication

一种无线通讯技术,利用红外线进行点对点数据传输。

3.5

底座 cradle

一种对接站,使用户的计算机和移动终端能够端连接进行通信和充电。

3.6

文件系统 file system

操作系统的一个组成部分,是实现数据的存储、分级组织、访问和获取等操作的抽象数据类型。