ICS 13.310
A 92

GA

中华人民共和国公共安全行业标准

GA/T 1564—2019

法庭科学　现场勘查电子物证提取技术规范

Forensic sciences—Technical specifications for collection of electronic evidence during scene investigation

2019-05-27 发布　　2019-05-27 实施

中华人民共和国公安部　发布

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国刑事技术标准化技术委员会电子物证检验分技术委员会(SAC/TC 179/SC 7)提出。

本标准由全国刑事技术标准化技术委员会(SAC/TC 179)归口。

本标准起草单位:北京市公安司法鉴定中心、公安部物证鉴定中心。

本标准起草人:朱秀云、姚波、贾永生、宋润、汤瑾玥、邢桂东。

法庭科学　现场勘查电子物证提取技术规范

1　范围

本标准规定了案(事)件现场勘查中电子物证提取的技术方法。

本标准适用于法庭科学领域中电子物证现场提取。

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。

GB/T 29360—2012　电子物证数据恢复检验规程

GB/T 29362—2012　电子物证数据搜索检验规程

GA/T 1069—2013　法庭科学电子物证手机检验技术规范

3　术语和定义

下列术语和定义适用于本文件。

3.1

电子物证现场提取　scene collection of electronic evidence

对案(事)件现场及其场所电子物证的发现、固定、收集的过程。

3.2

易失性数据　volatile data

存在于网络中传输的数据或运行于计算机等电子设备中随电源切断或关机而消失的数据。

3.3

在线提取　electronic evidence collection online

在目标系统运行的情况下,获取目标系统中的电子数据的过程。

3.4

远程勘验　remote inspection

通过网络对远程目标系统实施勘验,以提取、固定远程目标系统的状态和存留的内容。

3.5

手机信号屏蔽设备　mobile phone signal shielding device

对手机通信信号进行隔离,阻断手机通信的专用设备。

3.6

保全备份设备　safe backup device

对存储介质中的原始数据进行完整、精确、无损备份的设备。

3.7

只读设备　read-only device

对接入的存储介质具有写保护功能的设备。

4 现场提取设备

4.1 硬件

照录像设备、电子物证现场勘查箱、手机信号屏蔽设备、手机屏蔽箱(袋)、手机取证设备、仿真设备、保全备份设备、专用存储介质、便携式计算机、打印机等。

4.2 软件

综合取证分析软件、手机取证分析软件、仿真软件、在线取证软件、免安装和免系统注册软件等。

5 电子物证现场实物提取

5.1 计算机物证提取

5.1.1 关机状态的提取

5.1.1.1 对物证进行唯一性编号。

5.1.1.2 对物证的连线及设备接口一对一进行唯一性编号。

5.1.1.3 对现场进行拍照或录像,包括物证的品牌、唯一性编号等信息。

5.1.1.4 绘制网络拓扑图。

5.1.1.5 拆除物证设备间连线及电源线。

5.1.1.6 封存物证。

5.1.2 开机状态的提取

5.1.2.1 对物证进行唯一性编号。

5.1.2.2 对现场、屏幕进行拍照或录像。

5.1.2.3 对有屏保密码的设备应现场获取或使用免安装和免系统注册软件解除密码,对获取的密码应验证并记录。不能解除屏保密码时,应先关闭物证设备,再按照 5.1.1.2～5.1.1.5 步骤执行。

5.1.2.4 使用在线取证软件在线提取易失性数据,保存在有唯一性编号的专用存储介质中,并计算、记录哈希值。

5.1.2.5 应查看硬盘分区状况、文件显示属性,并进行记录。

5.1.2.6 接入互联网的设备,应查看正在运行的浏览器、QQ 等软件设置,关闭软件退出即自动删除数据的功能设置;若虚拟机、VPN 等特殊软件正在运行,应记录使用状态,并记录本环境所处接入互联网中的 IP。

5.1.2.7 记录物证的系统时间和北京时间。

5.1.2.8 对正在运行的有密码保护的数据进行提取,保存在有唯一性编号的专用存储介质中,并计算、记录哈希值;记录有密码的设备、软件、载体;现场获取或解除密码,对获取的密码应验证并记录。

5.1.2.9 记录数据提取路径和保存的路径。

5.1.2.10 关闭物证设备操作如下:

——对于切断电源不会导致数据损坏的物证,可直接切断电源;

——对于切断电源会导致数据损坏的物证,应按正常步骤关闭。

5.1.2.11 按照 5.1.1.2～5.1.1.5 步骤执行。

5.1.2.12 封存物证和专用存储介质。

5.2 手机物证的实物提取

5.2.1 关机状态的提取

5.2.1.1 对物证进行唯一性编号。
5.2.1.2 对现场进行拍照或录像，包括物证的品牌、唯一性特征等信息。
5.2.1.3 获取加密设备、加密扩展存储卡等密码。对获取的密码应验证并记录。
5.2.1.4 封存物证。

5.2.2 开机状态的提取

5.2.2.1 对物证进行唯一性编号。
5.2.2.2 对现场、屏幕进行拍照或录像，包括物证的品牌、唯一性特征等信息。
5.2.2.3 记录物证的系统时间和北京时间。
5.2.2.4 关闭各种通讯功能。
5.2.2.5 解除或获取加密设备、加密扩展存储卡等密码并记录。
5.2.2.6 根据需要可在开启手机信号屏蔽设备情况下，依据 GA/T 1069—2013 的要求，使用手机取证设备、手机取证分析软件或屏幕拍照的方式提取、固定手机内的信息。
5.2.2.7 使用手机屏蔽箱(袋)封存物证。

5.3 硬盘监控录像机的实物提取

5.3.1 关机状态的提取

按照 5.1.1.1～5.1.1.6 步骤执行。

5.3.2 开机状态的提取

5.3.2.1 对物证进行唯一性编号。
5.3.2.2 停止正在进行的录像操作。
5.3.2.3 对现场、屏幕进行拍照或录像。
5.3.2.4 记录物证的系统时间和北京时间。
5.3.2.5 获取或解除视频监控系统的登录密码。对获取的密码应验证并记录。
5.3.2.6 关闭物证设备。
5.3.2.7 按照 5.1.1.2～5.1.1.6 步骤执行。

5.4 其他电子设备的实物提取

按 5.2.1.1～5.2.1.4 执行。

6 电子数据提取

6.1 远程勘验在线提取数据

6.1.1 对提取操作现场环境、使用设备进行拍照或录像。
6.1.2 确定远程数据存储的位置，记录远程存储设备的域名、域名对应的 IP。
6.1.3 登录、浏览远程目标设备、网站账户，对操作过程进行截屏、拍照并全程录像，记录登录的用户名、密码、路径等信息。
6.1.4 依据 GB/T 29362—2012 进行数据搜索，提取远程目标中的网页、邮件、文件等数据内容，保存在

有唯一性编号的专用存储介质中，并计算、记录提取数据的哈希值。对操作过程进行截屏、拍照并全程录像。

6.1.5 记录远程勘验在线提取数据的北京时间、地点、人员及使用的软硬件等信息。

6.1.6 记录数据提取的路径和保存的路径。

6.1.7 封存专用存储介质。

6.2 计算机和硬盘监控录像机数据提取

6.2.1 全部数据提取

6.2.1.1 对物证进行唯一性编号。

6.2.1.2 对现场进行拍照或录像。

6.2.1.3 对物证内置硬盘进行保全备份操作如下：

——物证设备处于开机状态且不允许关机，应使用在线取证软件进行保全备份，并记录提取数据的哈希值、物证的系统时间和北京时间；

——物证设备处于关机状态或允许关机，开机状态应按照 5.1.2.3～5.1.2.10 或 5.3.2.2～5.3.2.6 步骤执行关机，然后使用保全备份设备进行保全备份，并记录提取数据的哈希值。

6.2.1.4 对保全备份硬盘进行唯一性编号并封存。

6.2.2 部分数据提取

6.2.2.1 对物证进行唯一性编号。

6.2.2.2 对现场进行拍照或录像。

6.2.2.3 提取目标数据操作如下：

——设备处于开机状态且不允许关机，应使用在线取证软件并依据 GB/T 29362—2012 进行数据搜索，在线提取目标数据，保存在有唯一性编号的专用存储介质中，并记录提取数据的哈希值、物证的系统时间和北京时间；

——设备处于关机状态或允许关机，开机状态应按照 5.1.2.3～5.1.2.10 或 5.3.2.2～5.3.2.6 步骤执行关机，然后通过电子物证现场勘查箱中的只读设备，将物证存储介质连接到已装载综合取证分析软件的便携式计算机上，使用综合取证分析软件依据 GB/T 29360—2012 和 GB/T 29362—2012 进行数据恢复搜索，提取目标数据，保存在有唯一性编号的专用存储介质中，并记录提取数据的哈希值、物证的系统时间和北京时间；

——有特殊类型的文件需要使用物证设备中特定的应用软件进行浏览，应使用仿真设备或使用保全备份设备制作的备份盘启动物证设备，依据 GB/T 29360—2012 和 GB/T 29362—2012 进行数据恢复搜索，提取目标数据，保存在有唯一性编号的专用存储介质中，并记录提取数据的哈希值、物证的系统时间和北京时间。

6.2.2.4 对保存数据信息的专用存储介质进行封存。

6.3 其他电子设备的数据提取

6.3.1 对物证进行唯一性编号。

6.3.2 对现场进行拍照或录像。

6.3.3 将物证与保全备份设备相连或将物证通过电子物证现场勘查箱中的只读设备连接到已装载综合取证分析软件的便携式计算机上，并启动取证分析软件。

6.3.4 使用保全备份设备或综合取证分析软件制作镜像文件或提取目标数据，保存在有唯一性编号的专用存储介质中，并记录提取数据的哈希值。

6.3.5 对保存数据信息的专用存储介质进行封存。

7 对物证及数据提取全过程进行现场记录

7.1 应对操作步骤进行详细记录。

7.2 应记录物证的唯一性编号、物证名称、物证型号及特征、物证所处的空间位置、专用存储介质唯一性编号、数据在专用存储介质中的存储路径、数据在物证设备中的存储路径、提取数据使用的软件和设备、提取数据的哈希值。

7.3 物证及数据提取人员应在提取记录上签字并注明提取日期。若使用计算机进行记录时，应将现场记录文件打印后再进行签字。

8 附则

8.1 在提取易失性数据之前，不应关闭已打开的电子设备。有屏保密码且无法解除的除外。

8.2 不应将非接触式智能卡放置在智能卡读写器附近。

8.3 应立即终止操作系统正在进行的整理硬盘、格式化硬盘、删除文件、重装系统、批量拷贝信息、批量下载信息、杀毒等操作。

8.4 应停止数码摄像机正在执行的摄像操作、录音设备正在执行的录音操作。

8.5 应将电子物证设备配套的数据线、驱动光盘、软件或设备说明书等一并提取。

8.6 激活屏保时，应采用轻移动鼠标或轻按键盘方向键的方法。

8.7 现场提取的电子数据均应保存于专用的存储介质中，并记录提取数据的哈希值。

8.8 宜首选实物提取，数据提取宜全部提取。

8.9 需现场浏览计算机物证设备信息时，应使用在线取证软件、仿真设备（或仿真软件）、备份盘启动浏览。

8.10 对于提取的电子物证要做好防水、防磁、防静电和防震保护。

GA/T 1564—2019

中华人民共和国公共安全
行业标准
法庭科学　现场勘查电子物证
提取技术规范
GA/T 1564—2019
*
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.org.cn
服务热线:400-168-0010
2019年10月第一版
*
书号:155066·2-34595

GA/T 1564-2019