

ICS 35.240.01
A 92

GA

中华人民共和国公共安全行业标准

GA/T 1174—2014

GA/T 1174—2014

电子证据数据现场获取通用方法

General methods for capture of live electronic evidence data

中华人民共和国公共安全
行业标准
电子证据数据现场获取通用方法
GA/T 1174—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

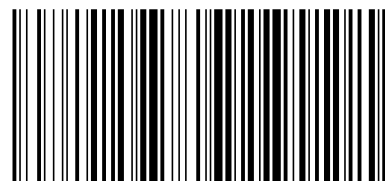
*

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: 155066·2-27344 定价 14.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107



GA/T 1174—2014

2014-07-09 发布

2014-07-09 实施

中华人民共和国公安部 发布

进行封存,方法如下:

- a) 采用的封存方法应当保证在不解除封存状态的情况下,无法使用被封存的存储介质和启动被封存电子设备;
- b) 封存前后应当拍摄或者录像被封存电子设备和存储介质并进行记录,照片或者录像应当从各个角度反映设备封存前后的状况,清晰反映封口或张贴封条处的状况;
- c) 对系统附带的电子设备和存储介质也应实施封存。

4.4 电子证据数据的动态获取

4.4.1 概述

对于运行中的系统,应进行电子证据数据的动态获取,其中又分为易丢失数据的提取和固定、在线获取以及电子设备和存储介质的封存三个部分。电子设备和存储介质的封存见 4.3。

4.4.2 遵循原则

易丢失数据的提取、固定和在线获取应遵照以下原则:

- a) 不得将生成、提取的数据存储在原始存储介质中;
- b) 不得在目标系统中安装新的应用程序。如果因为特殊原因,需要在目标系统中安装新的应用程序的,应当记录所安装的程序及其目的;
- c) 应当详细、准确记录实施的操作以及对目标系统可能造成的影响。

4.4.3 易丢失数据的提取和固定

易丢失数据的提取和固定应遵照以下步骤:

- a) 优先搜索并固定保全随机存取内存转储中的以下数据:
 - 1) 打开并未保存的文档;
 - 2) 最近的聊天记录;
 - 3) 用户密码;
 - 4) 其他取证活动相关的文件信息。
- b) 获取系统中相关电子证据数据的信息,包括:
 - 1) 存储介质的状态,确认是否存在异常状况等;
 - 2) 正在运行的进程;
 - 3) 操作系统信息,包括打开的文件,使用的网络端口,网络连接(其中包括 IP 信息,防火墙配置等);
 - 4) 尚未存储的数据;
 - 5) 共享的网络驱动和文件夹;
 - 6) 连接的网络用户;
 - 7) 其他取证活动相关的电子数据信息。
- c) 确保证据数据独立于电子数据存储介质的软硬件;逻辑备份证据数据以及所有权、时间等相关信息。

4.4.4 在线获取

需要进行在线获取的情况如下所示:

- a) 案件情况紧急,且证据数据具有时效性或者易丢失性,在现场不实施数据获取可能会造成严重后果的;

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:张颖、金波、郭弘、黄道丽、崔宇寅、雷云婷。