ICS 13.310
A 92

GA

中华人民共和国公共安全行业标准

GA/T 1071—2013

法庭科学电子物证 Windows 操作系统日志检验技术规范

Technical specifications for Windows operating system log examination of electronic forensics

2013-05-27 发布　　2013-06-01 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)提出并归口。

本标准起草单位:中国刑事警察学院司法鉴定中心、公安部物证鉴定中心。

本标准主要起草人:汤艳君、秦玉海、高洪涛、刘奇志、罗文华、高扬、楚川红。

法庭科学电子物证 Windows 操作系统日志检验技术规范

1 范围

本标准规定了 Windows 操作系统，包括 Windows 2000、Windows XP、Windows 2003、Windows Vista 和 Windows 7 日志检验的方法。

本标准适用于法庭科学领域中的电子物证检验。

2 术语和定义

下列术语和定义适用于本文件。

2.1

Windows 操作系统日志 Windows operating system log

Windows 操作系统所指定对象的操作和其操作结果按时间排列有序的集合。包括应用程序日志、安全日志和系统日志。

2.2

应用程序日志 application log

记录由应用程序产生的事件。

2.3

安全日志 security log

记录与安全相关事件，包括成功和不成功的登录或退出、系统资源使用等。

2.4

系统日志 system log

记录由 Windows 操作系统组件产生的事件，主要包括驱动程序、系统组件和应用软件的崩溃以及数据丢失错误等。

3 仪器设备

3.1 硬件

存储介质、保全备份设备、具有只读接口的电子物证检验工作站。

3.2 软件

3.2.1 操作系统：Windows。

3.2.2 软件工具：具有 Windows 操作系统日志查看功能的软件、Windows 操作系统提供的事件查看器等。

4 操作步骤

4.1 检材编号

对送检的检材进行惟一性编号。

4.2 检材拍照

对送检的检材加上惟一性编号进行拍照。

4.3 检材保全备份

对具备保全条件的检材进行保全备份。

4.4 检验

4.4.1 启动杀毒软件对电子物证检验工作站系统进行杀毒。

4.4.2 对检材(若已保全,使用保全的存储设备)通过只读方式连接到电子物证检验工作站。

4.4.3 计算检材的哈希值。

4.4.4 使用操作系统提供的资源管理器中搜索功能或具有搜索功能软件的过滤功能查找日志文件。Windows 2000、Windows XP、Windows 2003 系统默认存储路径是%systemroot%\system32\config,应用程序日志、安全日志和系统日志对应的文件名分别为 AppEvent.evt、SecEvent.evt 和 SysEvent.evt;Windows Vista、Windows 7 系统日志默认存储路径是%systemroot%\system32\winevt\logs,应用程序日志、安全日志和系统日志对应的文件名分别为 Application.evtx、Security.evtx 和 System.evtx。

4.4.5 使用软件工具对日志文件内容进行浏览和检验。

4.4.6 检验时应按照软件工具使用说明书进行操作。

4.4.7 将检验结果按检验要求筛选后复制到检验专用存储介质中。

4.5 检出数据刻录

4.5.1 将检出的数据刻录在不可擦写的空白光盘上,应采用封盘刻录。

4.5.2 计算哈希值。

4.5.3 对光盘进行惟一性编号。

4.5.4 贴上盘签,盘签内容应注明检验单位名称、光盘编号、光盘哈希值、光盘制作日期等;应加盖检验鉴定专用章。

5 检验结论的表述

经对编号为“a_1”~“a_n”的检材使用 rr 软件工具进行技术检验,检验结果如下:

在检材 a_i 中检出与 yy 有关的 Windows 操作系统日志文件 mm 个,大小计 bb。检出的数据文件刻录在编号为 gg 光盘中,光盘(或文件)的 HH 哈希值为 hh(或在检材 a_i 中未检出与 yy 有关的日志文件)。

注:a_i 代表检材编号;n 代表检材个数;i 代表检材序号;rr 代表使用软件工具的名称及版本号;yy 代表检验要求或样本;mm 代表文件个数;bb 代表文件大小,单位可以使用 Byte、kB、MB 或 GB;gg 代表光盘的编号;HH 代表哈希算法名称;hh 代表哈希值。

中华人民共和国公共安全
行 业 标 准
法庭科学电子物证 Windows 操作系统
日志检验技术规范
GA/T 1071—2013
*
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(100013)
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
2013 年 7 月第一版 2013 年 7 月第一次印刷
*
书号:155066·2-25735 定价 14.00 元

GA/T 1071-2013

打印日期:2014年3月24日 F053