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。