ICS 13.310
CCS A 92

GA

中华人民共和国公共安全行业标准

GA/T 1071—2021
代替 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

Forensic sciences—Technical specifications for Windows operating system log examination

2021-10-14 发布　　2022-05-01 实施

中华人民共和国公安部　　发 布

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替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》，与GA/T 1071—2013相比，除编辑性修改外，主要技术变化如下：

——更改了范围，增加了操作系统类型（见第1章，2013年版的第1章）；

——增加了规范性引用文件（见第2章）；

——更改了硬件设备（见4.1，2013年版的3.1）；

——更改了软件设备，将2013年版的3.2.1和3.2.2内容重新整合为4.2（见4.2，2013年版的3.2）；

——更改了检验对象，增加了样本（见5.1～5.4，2013年版的4.1～4.4）；

——更改哈希值为数据完整性校验值（见5.4.3，2013年版的4.4.3）；

——更改了日志检验步骤（见5.4.4～5.4.8，2013年版的4.4.4～4.4.7）；

——更改了检出数据的保存方法及要求（见5.5，2013年版的4.5）；

——更改了检验结果表述（见第6章，2013年版的第5章）；

——更改了附则（见第7章，2013年版的第6章）。

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专利的责任。

本文件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。

本文件起草单位：中国刑事警察学院、公安部物证鉴定中心、公安部网络安全保卫局。

本文件主要起草人：汤艳君、秦玉海、楚川红、郭丽莉、高洪涛、刘奇志、罗文华、吴倩、高杨。

本文件所代替文件的历次版本发布情况为：

——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

1　范围

本文件规定了法庭科学领域中电子物证 Windows 操作系统，包括 Windows 2000、Windows XP、Windows 2003、Windows Vista、Windows 7、Windows 8、Windows 10 和 Windows Server 2000/2003/2008/2012/2016 等日志检验的术语和定义、仪器设备、操作步骤、检验结果表述及附则。

本文件适用于法庭科学领域中电子物证 Windows 操作系统日志的检验。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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　电子物证数据恢复检验规程

GB/T 29362　电子物证数据搜索检验规程

3　术语和定义

GB/T 29360、GB/T 29362 界定的以及下列术语和定义适用于本文件。

3.1

系统日志　system log

Windows 操作系统组件产生的事件记录，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。

3.2

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。

3.3

应用程序日志　application log

应用程序产生的事件记录。

3.4

安全日志　security log

安全相关的事件记录，包括成功和不成功的登录或退出、系统资源使用等。

4　仪器设备

4.1　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、照相录像设备。