ICS 13.310
A 92

GA

中华人民共和国公共安全行业标准

GA/T 1070—2013

法庭科学计算机开关机时间检验技术规范

Technical specifications for computer switch time examination in forensics

2013-09-30 发布　　2013-09-30 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归口。

本标准起草单位：中国人民公安大学刑事科学技术系、公安部物证鉴定中心。

本标准起草人：丁锰、郭威、邢桂东。

法庭科学计算机开关机时间检验技术规范

1 范围

本标准规定了电子物证检验中操作系统为 Windows 2000、Windows XP、Windows 2003、Windows Vista、Windows 7 的计算机开关机时间的检验方法。

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

计算机开机时间 time of switch on computer

计算机开机进入操作系统时的系统时间。

2.2

计算机关机时间 time of switch off computer

计算机关机退出操作系统时的系统时间。

3 检验工具

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 2000、Windows XP、Windows 2003、Windows Vista、Windows 7。

3.2.2 工具软件：具有日志查看功能的软件、Windows 操作系统提供的事件查看器、具有解析注册表功能的软件以及文本编辑器。

4 操作步骤

4.1 检材及样本编号

对送检的检材(样本)进行唯一编号。

4.2 检材及样本拍照

对送检的检材(样本)加上唯一性编号进行拍照。

4.3 检材及样本保全

对具备保全条件的检材(样本)进行保全备份。

4.4 检验工作站杀毒

启动杀毒软件对电子物证检验工作站系统进行杀毒。

4.5 检材连接方法

将检材(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。

4.6 系统时区检验

4.6.1 查找系统注册表 CurrentControlSet 键的数据源

使用具有解析注册表功能的工具软件加载%SYSTEMROOT%\system32\config路径下的 system 文件,查找文件包含注册表的 HKEY_LOCAL_MACHINE\SYSTEM\Select子键,记录该键中的 Current 值,根据 Current 值确定注册表中 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet 子键的数据源。当 Current 值为"1"时,CurrentControlSet 键的数据源为 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001;当 Current 值为"2"时,CurrentControlSet 键的数据源为 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002,以此类推。

4.6.2 检验系统时区信息

查找 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00X(X 为 4.6.1 中的 Current 值)\Control\TimeZoneInformation 子键,记录该键中 StandardName 的值为系统的时区信息。

4.7 系统开关机时间检验

4.7.1 检验与任务计划程序服务有关的时间信息

以"SchedLgU.Txt"为关键字在检材中进行搜索,搜索结果记为 W1。该文件中"已启动于"字符串后的时间为开机时间、"已退出于"字符串后的时间为关机时间。

4.7.2 检验与系统日志有关的时间信息

在 Windows 2000、Windows XP 或 Windows 2003 中以"SysEvent.evt"为关键字、在 Windows Vista 或 Windows 7 中以"System.evtx"为关键字进行搜索。使用具有日志查看功能的软件导出事件记录,筛选记录中 ID 为 6005 的事件为开机时间、ID 为 6006 的事件为关机时间,筛选后的文件记为 W2。

4.7.3 时间信息分析和对比

对比 W1 文件和 W2 文件中的开关机时间。

如果两个文件中的开关机时间相同,取 W1 文件中的开关机时间作为检出结果。

如果两个文件中的开关机时间不同,合并两个文件中的开关机时间作为检出结果。

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:

a) 检出与 yy 有关的开关机时间时,表述为:

在检材 a_i 中检出与 yy 有关的开关机时间为:依次列出所有检出的开机和关机时间;系统时区为 tt。

b） 未检出与 yy 有关的开关机时间时，表述为：

在检材 a_i 中未检出与 yy 有关的开关机时间。

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；tt 为系统时间信息。

6 附则

6.1 在检验过程中应做检验记录。

6.2 在检验过程中，不应改变送检检验对象中的数据。

6.3 对送检的检材和样本应做好防水、防磁、防震及防静电保护。

GA/T 1070—2013

中华人民共和国公共安全
行 业 标 准
法庭科学计算机开关机时间检验技术规范
GA/T 1070—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12月第一版 2013年12月第一次印刷
*
书号:155066·2-26235 定价 14.00元

GA/T 1070-2013

打印日期:2014年3月24日 F053