



中华人民共和国公共安全行业标准

GA/T 1474—2018

法庭科学计算机系统用户操作行为 检验技术规范

Technical specifications for examination of computer system user
operation behaviors in forensics

2018-04-17 发布

2018-04-17 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:司法部司法鉴定科学技术研究所、公安部物证鉴定中心。

本标准主要起草人:施少培、杨旭、李岩、卢启萌、曾锦华、楚川红。

法庭科学计算机系统用户操作行为 检验技术规范

1 范围

本标准规定了计算机系统用户操作行为检验的技术方法和步骤。
本标准适用于法庭科学领域中的计算机系统用户操作行为检验。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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
GA/T 756 数字化设备证据数据发现提取固定方法
GA/T 976 电子数据法庭科学鉴定通用方法
GA/T 1172 电子邮件检验技术方法
GA/T 1173 即时通讯记录检验技术方法
GA/T 1176 网页浏览器历史数据检验技术方法

3 术语和定义

GA/T 976 界定的以及下列术语和定义适用于本文件。

3.1

用户操作行为 user operation behavior

用户使用计算机系统的特定行为,如开/关机、登录/登出、接入外部设备、文件操作、打印、软件使用、浏览网页、即时通讯、收发电子邮件等。分为正在进行的行为和已经发生的行为。

3.2

操作痕迹 operation trace

反映用户操作行为过程的数据,存在于日志、注册表、临时文件、配置文件、数据库等区域。

4 检验步骤

4.1 准备

4.1.1 了解检材的使用情况,包括用户信息、系统状态、可能的操作行为类别等。

4.1.2 如检材有登录口令或加密密钥保护,宜获取口令或密钥信息。

4.2 固定保全

4.2.1 对检材进行唯一性编号。

4.2.2 对检材进行拍照或录像,记录其特征。

4.2.3 根据检材情况和检验需要,按照 GA/T 756 的相关要求进行完整性备份。无法进行完整性备份的,对检验过程进行全程录像。

4.3 搜索和恢复

根据检验需要,按照 GB/T 29360 和 GB/T 29362 搜索、恢复保存在检材中的相关文件和数据。

4.4 行为检验

4.4.1 根据检材具体情况和计算机操作系统类型,视检验需要对包括但不限于 4.4.2~4.4.9 的内容进行检验和分析。

4.4.2 开/关机及登录/登出检验至少应包括以下内容:

- a) 检验系统日志、应用程序日志及系统安全日志等日志文件中与开/关机及登录/登出相关的记录;
- b) 检验系统配置信息,如 Windows 系统注册表中的相关数据;
- c) 在系统中其他位置查找与开/关机及登录/登出相关的信息,如系统中文件的修改时间、防病毒软件及其他软件的启动/关闭记录等。

4.4.3 接入外部设备检验至少应包括以下内容:

- a) 检验系统驱动安装日志中与外部设备相关的数据;
- b) 检验系统配置信息,如 Windows 系统注册表中的相关数据;
- c) 检验快捷方式中与外部设备相关的数据,如最近访问记录等;
- d) 检验缓存文件中与外部设备相关的数据,如图标缓存等;
- e) 检验系统中的文件与外部设备中的文件的相似性及复制关系;
- f) 对于存在自动备份机制的外部设备,检验其备份在计算机系统的数据。

4.4.4 文件操作检验至少应包括以下内容:

- a) 检验文件的属性信息;
- b) 检验文件的元数据信息;
- c) 检验文件操作形成的临时文件、备份文件、快捷方式等;
- d) 检验文件在相关软件及系统中的最近打开记录;
- e) 对于被删除的文件,检验其状态、位置及内容。

4.4.5 打印检验至少应包括以下内容:

- a) 检验系统中安装的打印机驱动程序;
- b) 检验打印临时文件,如 Windows 系统的 SHD、SPL 及 TMP 文件;
- c) 查找打印源文件,检验其中的打印时间。

4.4.6 软件使用检验至少应包括以下内容:

- a) 检验系统中需检软件文件的属性信息;
- b) 检验软件运行时生成的配置文件、临时文件及其属性信息;
- c) 检验软件的日志信息;
- d) 检验软件在系统中其他位置留下的信息,如 Windows 系统注册表、系统还原点、系统镜像、最近打开文档等;
- e) 对于含有数据库的软件,对数据库中的数据进行检验。

4.4.7 浏览网页检验至少应包括以下内容:

- a) 根据网页浏览器类型和版本,查找其历史数据保存位置;
- b) 检验网页浏览历史数据,如地址栏网址输入记录、网址重定向记录、网页浏览历史记录等;

- c) 检验与被浏览网页相关的图片、文档、压缩包、Cookies、脚本等信息；
- d) 查找并检验系统中与被浏览网页相关的其他文件，如收藏夹、保存的网页、下载的文件等；
- e) 其他内容可参照 GA/T 1176 的相关要求进行检验。

4.4.8 即时通讯检验至少应包括以下内容：

- a) 查找系统中安装的即时通讯软件及其数据文件；
- b) 检验客户端软件版本、用户账号等信息及数据文件的属性信息；
- c) 检验数据文件中的聊天记录等信息；
- d) 查找并检验通过即时通讯传输的图片、文档、多媒体文件等信息；
- e) 其他内容可参照 GA/T 1173 的相关要求进行检验。

4.4.9 电子邮件收发检验至少应包括以下内容：

- a) 查找系统中安装的电子邮件客户端软件及其数据文件；
- b) 根据客户端类型分析数据文件中的电子邮件及其相互之间的关联；
- c) 在系统中搜索其他与需检电子邮件相关的信息；
- d) 对于通过网页电子邮件服务收发的电子邮件，可参照 GA/T 1172 的相关要求进行检验。

4.4.10 其他操作行为，根据操作行为类别及操作系统特点，有针对性地对相关操作痕迹进行检验。

5 检验结果保存

将检出数据采用封盘刻录方式刻录在不可擦写的空白光盘上或者保存在专用存储介质中，并计算检出数据的哈希值。

6 检验记录

与检验有关的情况应及时、客观、全面地记录，保证检验过程和结果的可追溯性。

7 检验结果表述

检验结果表述应符合以下规定：

- a) 检验结果分为检出、未检出、不具备检验条件 3 种；
- b) 检验结果应根据检验要求对检验对象、检验范围、检验所得进行客观、概括、有针对性的描述；
- c) 结果表述应包含检材编号、检出情况、检出数据文件或保存检出数据介质哈希值、保存检出数据介质编号等必要信息。

8 附则

8.1 计算机系统的时间信息与标准时间并非完全一致，检验中应注意系统时间与标准时间（如国家授时中心标准时间源）的差值。

8.2 对于加密的数据，检验前宜先对其进行解密。

8.3 在查找操作痕迹时，应注意搜索、恢复的全面性。

8.4 检验中应注意查找并分析可以相互印证的数据。

8.5 对于检验中发现的存疑现象，可以通过实验进行分析。