ICS 13.310
A 92

GA

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。