ICS 13.310
A 92

GA

中华人民共和国公共安全行业标准

GA/T 1477—2018

法庭科学计算机系统接入外部设备使用痕迹检验技术规范

Technical specifications for examination of traces of using external equipment in computer systems 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:中国刑事警察学院物证鉴定中心、公安部物证鉴定中心。

本标准主要起草人:罗文华、汤艳君、段严兵、秦玉海、高洪涛、彭丽娟、王强、张国臣。

法庭科学计算机系统接入外部设备使用痕迹检验技术规范

1 范围

本标准规定了典型计算机系统环境下外部接入设备使用痕迹检验的方法。

本标准适用于法庭科学领域中的电子物证检验。

2 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—2012 电子物证数据恢复检验规程

GA/T 756—2008 数字化设备证据数据发现提取固定方法

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

3 术语和定义

GB/T 29360—2012、GA/T 756—2008、GA/T 1071—2013 界定的以及下列术语和定义适用于本文件。

3.1

外部设备 external equipment

在计算机主机处理数据前后，负责数据的传输、转送及存储的设备。

3.2

系统文件 system file

用于存放操作系统重要信息的文件，一般在操作系统启动或运行过程中自动创建及维护。

3.3

用户文件 user file

用于存放用户信息的文件，一般通过用户行为创建与维护。

4 仪器设备

4.1 硬件

存储介质、保全备份设备、只读设备和专用电子物证检验设备。

4.2 软件

4.2.1 操作系统：Windows、Unix/Linux、Mac OS 等。

4.2.2 软件工具：电子物证检验综合分析软件、系统文件专用查看类工具、用户文件专用查看类工具。