



# 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。

## 5 操作步骤

### 5.1 检材编号

对送检的检材进行唯一性编号。

### 5.2 检材拍照

对送检的检材加上唯一性编号进行拍照。

### 5.3 检材保全备份

对具备保全条件的检材进行保全备份。

### 5.4 检验

5.4.1 启动杀毒软件对电子物证检验工作站系统进行杀毒。

5.4.2 对检材(若已保全,使用保全的存储设备)通过只读设备接到电子物证检验工作站。

5.4.3 使用电子物证检验综合分析软件或专用工具针对计算机系统上的系统文件进行检验,获取外部接入设备使用痕迹,包括设备序列号、设备制造厂商、设备类型、首次接入时间、最近接入时间等信息。

对于 Windows 系列操作系统,重点检验注册表中与设备相关的表项信息;在注册表证据源被破坏的情况下,可依次检验设备安装文件及系统事件日志。对于 Unix/Linux,主要检验设备管理文件,Mac OS 则检验设备树文件。

5.4.4 在未能够基于系统文件获取到关键信息的情况下,可通过用户文件分析源文件存放路径,进而判断其是否来自外部设备;也可通过用户自行安装的客户端或服务器管理软件挖掘外部设备的接入记录。

5.4.5 对于已被删除的系统文件及用户文件,依据 GB/T 29360—2012 进行数据恢复后,再按步骤 5.4.3 与 5.4.4 所述方法开展检验。

### 5.5 检出数据保存

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。

## 7 附则

7.1 在检验过程中应做检验记录。

- 7.2 在检验过程中,不宜改变检验对象中的数据。
  - 7.3 在检验过程中,检验出的数据应存储到专用的存储介质中。
  - 7.4 应对送检的检验对象做好防水、防磁、防静电和防震保护。
-