



# 中华人民共和国国家标准

GB/T 29362—2023

代替 GB/T 29362—2012

## 法庭科学 电子数据搜索检验规程

Forensic sciences—Code of practice for electronic data search examination

2023-03-17 发布

2023-10-01 实施

国家市场监督管理总局 发布  
国家标准化管理委员会

## 前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 29362—2012《电子物证数据搜索检验规程》，与 GB/T 29362—2012 相比，除结构调整和编辑性改动外，主要技术变化如下：

- 更改了硬件的要求(见 4.1,2012 年版的 3.1)；
- 更改了软件的要求(见 4.2,2012 年版的 3.2)；
- 更改了检材及样本编号、拍照的部分内容(见 5.1,2012 年版的 4.1、4.2)；
- 更改了“检验”的部分内容(见 5.4,2012 年版的 4.4)；
- 更改了检出数据保存的要求(见 5.5,2012 年版的 4.5)；
- 增加了检验记录的要求(见第 6 章)；
- 更改了检验结果表述的要求(见第 7 章,2012 年版的第 5 章)；
- 增加了关于故障存储介质的注意事项(见 8.2)；
- 增加了关于加密情况的注意事项(见 8.3)；
- 增加了关于需要数据重组情况的注意事项(见 8.4)；
- 增加了关于多媒体文件内容搜索的注意事项(见 8.5)。

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专利的责任。

本文件由中华人民共和国公安部提出。

本文件由全国刑事技术标准化技术委员会(SAC/TC 179)归口。

本文件起草单位：公安部物证鉴定中心、最高人民检察院检察技术信息研究中心、司法鉴定科学研究院。

本文件主要起草人：邢桂东、楚川红、赵露、赵宪伟、施少培、张国臣、尹春社。

本文件所代替文件的历次版本发布情况为：

- GB/T 29362—2012；
- 本次为第一次修订。

# 法庭科学 电子数据搜索检验规程

## 1 范围

本文件规定了法庭科学领域电子数据搜索检验的仪器设备、操作步骤、检验记录、检验结果表述的要求及注意事项。

本文件适用于法庭科学领域存储介质及保全备份数据文件的电子数据搜索检验。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GA/T 1554 法庭科学 电子物证检验材料保存技术规范

GA/T 1568 法庭科学 电子物证检验术语

## 3 术语和定义

GA/T 1568 界定的术语和定义适用于本文件。

## 4 仪器设备

### 4.1 硬件

电子物证检验工作站、保全备份设备、只读设备、存储介质、解密设备、照录像设备等。

### 4.2 软件

具有数据搜索功能的软件、具有数据库查询功能的软件、具有解密功能的软件、具有数据重组功能的软件等。

## 5 操作步骤

### 5.1 检材(样本)编号和拍照

对检材(样本)加上唯一性编号进行拍照。

### 5.2 杀毒

启动杀毒软件对电子物证检验工作站系统进行杀毒。

### 5.3 检材(样本)保全备份

计算检材(样本)的完整性校验值,宜对具备保全备份条件的检材(样本)进行保全备份。

## 5.4 检验

5.4.1 将检材(样本)或已保全备份的存储介质,通过只读方式连接到电子物证检验工作站;对于已保全备份的镜像文件,将其加载到电子物证检验工作站。

5.4.2 根据检材(样本)情况选择一种或多种电子数据搜索方式进行检验,可选搜索方式包括但不限于:

- a) 根据文件名、文件类型、文件属性、文件内容、文件哈希值或关键字,使用具有数据搜索功能的软件工具进行文件搜索;
- b) 根据文件名、文件或关键字对应的二进制编码或其他编码,使用具有数据搜索功能的软件工具进行物理搜索;
- c) 根据数据库文件类型,使用具有数据库查询功能的软件工具打开数据库文件并进行数据搜索。

5.4.3 对搜索后的数据文件根据检验要求进行筛选(可对筛选后的数据文件进行数据压缩),形成检出数据。

5.4.4 计算检出数据的完整性校验值。

## 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保存在专用存储介质中。

## 6 检验记录

检验记录至少应包含检验地点、检验人员、起止时间、检验技术方法、检验仪器设备、检验软件及版本、操作步骤、检验情况、检出数据的完整性校验值,保证检验过程的可追溯性。

## 7 检验结果表述

7.1 检出数据时,检验结果表述至少应包含检材(样本)编号、检出数据情况、检出数据(或保存检出数据介质)的完整性校验值、保存检出数据的存储介质编号。

7.2 未检出数据时,检验结果表述至少应包含检材(样本)编号和未检出数据情况。

7.3 不具备检出数据条件时,检验结果表述至少应包含检材(样本)编号,并根据检材情况进行表述。

## 8 注意事项

8.1 应按照 GA/T 1554 的要求,对检材(样本)做好防水、防磁、防静电和防震保护。

8.2 故障存储介质应排除故障后再进行搜索检验。

8.3 对于加密的检材及检材中加密的数据,可使用具有解密功能的软件工具解密后再进行搜索检验。

8.4 对于需要数据重组的检材(如磁盘阵列),应使用具有数据重组功能的软件工具重组后再进行搜索检验。

8.5 对于多媒体文件,可进行内容识别处理后再进行搜索检验。