ICS 13.310
A 92

GA

# 中华人民共和国公共安全行业标准

GA/T 825—2009

# 电子物证数据搜索检验技术规范

**Data search technical specifications of electronic forensics**

2009-04-07 发布　　2009-06-01 实施

中华人民共和国公安部　　发布

# 前　言

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:公安部物证鉴定中心。

本标准主要起草人:张国臣、尹春社、邢桂东、楚川红。

# 电子物证数据搜索检验技术规范

## 1 范围

本标准规定了数据搜索检验的方法。

本标准适用于法庭科学领域中的电子物证检验。

## 2 术语和定义

下列术语和定义适用于本标准。

2.1

**数据搜索 data search**

在送检存储设备或介质中查找已知内容或关键字检验，包括文件搜索和物理搜索两种方式。

2.1.1

**文件搜索 file search**

根据已知内容或关键字对送检存储设备或介质的数据文件进行搜索检验。

2.1.2

**物理搜索 physical search**

根据已知内容或关键字对送检存储设备或介质的二进制数据进行搜索检验。

2.2

**保全备份 safe backup**

对原始数据进行完整、精确、无损的备份。

## 3 仪器设备

### 3.1 硬件

存储介质、保全备份设备、具有只读接口的电子物证检验工作站。

### 3.2 软件

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

3.2.2 软件工具：EnCase、Forensic Toolkit、X-Ways Forensics、操作系统提供的资源(文件)管理器等。

## 4 操作步骤

### 4.1 检材和样本编号

对送检的检材和样本进行唯一性编号。

### 4.2 检材及样本拍照

对送检的检材和样本进行拍照。

### 4.3 检材及样本保全备份

对具备保全条件的检材和样本进行保全备份。

### 4.4 检验

4.4.1 启动杀毒软件对电子物证检验工作站系统进行杀毒。

4.4.2 对检材和样本(若已保全，使用保全的存储设备)通过只读接口接到电子物证检验工作站。

4.4.3 通过已知内容或关键字进行文件搜索可使用 EnCase、Forensic Toolkit、X-Ways Forensics 或操作系统提供的资源(文件)管理器等软件工具。

4.4.4 通过已知内容或关键字进行物理搜索可使用 EnCase、Forensic Toolkit、X-Ways Forensics 等软件工具。

4.4.5 搜索数据应按照各软件工具使用说明书进行操作。

4.4.6 将搜索结果按检验要求筛选后复制到专用的存储介质中。

### 4.5 检出数据刻录

4.5.1 将检验出的数据刻录在不可擦写的空白光盘上，应采用封盘刻录。

4.5.2 对光盘进行唯一性编号。

4.5.3 贴上盘签。盘签内容应包括检验单位名称、光盘编号、检验日期等；应加盖检验鉴定专用章。

## 5 检验结论的表述

经对编号为“$a_1$”～“$a_n$”的检材使用 rr 软件工具进行技术检验，检验结果如下：

在检材 i 中检出与 yy 有关数据文件 mm 个，大小计 bb(单位可以使用 Byte、kB、MB 或 GB)。检出的数据文件刻录在 dd 制作的编号为 gg 光盘中。(或：在检材 i 中未检出与 yy 有关的数据文件。)

注：$a_i$ 代表检材；n 代表检材个数；i 代表检材序号；rr 代表使用软件工具的名称及版本号；yy 代表检验要求或样本；mm 代表文件个数；bb 代表文件大小；dd 代表检验单位名称；gg 代表光盘的编号。

## 6 附则

6.1 在检验过程中应做检验记录。

6.2 在检验过程中，不应改变检验对象中的数据。

6.3 在检验过程中，搜索出的数据应存储到专用的存储介质中。

6.4 应对送检的检验对象做好防水、防磁、防静电和防震保护。

中华人民共和国公共安全
行 业 标 准
电子物证数据搜索检验技术规范
GA/T 825—2009
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 0.5 字数 5 千字
2009年6月第一版 2009年6月第一次印刷
*
书号:155066·2-19701

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68533533

GA/T 825-2009