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。