ICS 13.310
A 92

GA

中华人民共和国公共安全行业标准

GA/T 827—2009

电子物证文件一致性检验技术规范

File identification 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:尹春社、邢桂东、楚川红、张国臣。

电子物证文件一致性检验技术规范

1 范围

本标准规定了电子物证检验技术中文件一致性检验的方法。

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

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GA/T 825—2009 电子物证数据搜索检验技术规范

3 术语和定义

GA/T 825—2009 中确立的术语和定义适用于本标准。

4 仪器设备

4.1 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。

4.2 软件

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

4.2.2 软件工具：EnCase、Forensic ToolKit、X-ways Forensics、Macforensicslab 等。

5 操作步骤

5.1 检材和样本编号

对送检的检材和样本进行唯一性编号。

5.2 检材及样本拍照

对送检的检材及样本进行拍照。

5.3 检验

5.3.1 启动杀毒软件对电子物证检验工作站系统进行杀毒。

5.3.2 将检材数据文件和样本数据文件刻录在光盘中备份。

5.3.3 将保全的检材数据文件和样本数据文件复制到电子物证检验工作站中。

5.3.4 使用软件工具分别计算检材数据文件和样本数据文件的哈希值。哈希值的计算方法应按照各软件工具使用说明书进行操作。

5.3.5 比较检材数据文件和样本数据文件的哈希值。若两个哈希值相同，则可以判断两个文件的数据相同；若两个哈希值不同，则可以判断两个文件的数据不同。

6 检验结论的表述

经对编号为“n”的检材与编号为“m”的样本使用 rr 软件工具进行技术检验后，两个数据文件中的数据相同(或不同)。

注：n 代表检材的编号；m 代表样本的编号；rr 代表所使用软件工具的名称及版本号。