ICS 13.310
A 92

GA

中华人民共和国公共安全行业标准

GA/T 829—2009

电子物证软件一致性检验技术规范

Software 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:邢桂东、尹春社、张国臣、楚川红。

电子物证软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软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、电子物证检验工作站。

4.2 软件

送检软件所需系统运行环境。

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。

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 分别对送检的检材和样本软件中的文件进行哈希值计算，在检材和样本中查找哈希值相同的文件(公共程序库文件除外)。

5.4.2.1 若所有对应的文件哈希值相同，则软件相同。

5.4.2.2 若对应的文件哈希值不同，按下列步骤进行：

a) 对送检的检材软件与样本软件直接进行目录和文件名比对。

b) 安装过程比对。将两套软件安装在同一台检验设备上，比对安装过程中的屏幕显示和功能键等是否相同。

c) 安装完成后，比对安装后的目录名和文件，文件比对包括文件名、文件长度、文件哈希值和文件时间属性等。

d) 运行软件，进行使用过程比对，应忽略涉及的加密和解密，对使用过程中的屏幕显示、功能、功

能键、使用方法等进行比对。

e) 程序源代码比对。

6 检验结论的表述

6.1 结果相同的表述

经对检材和样本进行技术检验后，检材和样本目录、文件名、安装过程、安装后的目录及各文件、源程序(将相同的部分写上)相同。

6.2 结果不同的表述

经对检材和样本进行技术检验后，检材和样本不同。

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，不应改变检验对象中的数据。

7.3 对送检的检验对象要做好防水、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
电子物证软件一致性检验技术规范
GA/T 829—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 4 千字
2009年6月第一版 2009年6月第一次印刷
*
书号:155066·2-19705 定价 14.00 元

GA/T 829-2009