ICS 13.310
A 92

中华人民共和国国家标准

GB/T 29360—2012

电子物证数据恢复检验规程

Technical specification for data recovery of electronic forensic

2012-12-31 发布　　2013-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

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、楚川红、张国臣、尹春社。

电子物证数据恢复检验规程

1 范围

本标准规定了电子物证检验中数据恢复检验的方法。

本标准适用于法庭科学领域中的电子物证检验。

本标准不适用于物理损坏存储介质的数据恢复。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

GB/T 29362 电子物证数据搜索检验规程

3 术语和定义

GB/T 29362 界定的术语和定义适用于本文件。

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：具有数据恢复功能的软件。

5 操作步骤

5.1 检材及样本编号

对送检的检材(样本)进行唯一性编号。

5.2 检材及样本拍照

对送检的检材(样本)加上唯一性编号进行拍照。

5.3 检材及样本保全备份

对具备保全条件的检材(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 将检材(若已保全,使用保全的存储设备)通过只读方式连接到电子物证检验工作站。
5.4.3 计算检材(样本)的哈希值。
5.4.4 根据检验要求,使用软件工具进行数据恢复。
5.4.5 恢复数据文件方法应按照软件工具使用说明书进行操作。
5.4.6 将恢复的数据进行筛选后复制到检验专用存储介质中。

5.5 检出数据刻录

5.5.1 将检出数据刻录在不可擦写的空白光盘上,应采用封盘刻录。
5.5.2 计算光盘的哈希值。
5.5.3 对光盘进行唯一性编号。
5.5.4 贴上盘签。盘签应注明检验单位名称、光盘编号、光盘哈希值、光盘制作日期等;应加盖检验鉴定专用章。

6 检验结论的表述

经对编号为"a_1"至"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 a_i 中检出与 yy 有关数据文件 mm 个,大小合计 bb。检出的数据文件刻录在编号为 gg 光盘中,该光盘的 HH 哈希值为 hh。(或:在检材 a_i 中未检出与 yy 有关的数据文件。)

注:a_i 代表检材编号;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,单位可以使用 Byte、KB、MB 或 GB;gg 代表光盘的编号;HH 代表哈希值算法;hh 代表光盘的哈希值。

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,不应改变送检检验对象中的数据。
7.3 在检验过程中,检出数据应存储到专用的存储介质中。
7.4 应对送检检验对象做好防水、防磁、防静电和防震保护。

中 华 人 民 共 和 国
国 家 标 准
电子物证数据恢复检验规程
GB/T 29360—2012
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
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
2013年3月第一版 2013年3月第一次印刷
*
书号:155066·1-46263 定价 14.00 元

GB/T 29360-2012

打印日期:2014年3月24日 F053