司　法　鉴　定　技　术　规　范

SF/Z JD0401001-2014

电子数据复制设备鉴定实施规范

2014-3-17 发布　　2014-3-17 实施

中华人民共和国司法部司法鉴定管理局　　发布

目　　次

前　言

本技术规范按照GB/T 1.1-2009给出的规则起草
本技术规范由福建中证司法鉴定中心提出。
本技术规范由司法部司法鉴定管理局归口。
本技术规范起草单位：福建中证司法鉴定中心。
本技术规范主要起草人：赵庸，卢建斌，张雪峰。
本技术规范为首次发布。

引　言

制定本技术规范的依据包括以下国家或行业标准：中华人民共和国公安部于2012年2月1日颁布实施的GA/T 976-2012《电子数据法庭科学鉴定通用方法》和中华人民共和国司法部于2007年8月7日发布的《司法鉴定程序通则》。

本技术规范运用数据存储原理，结合电子数据取证、鉴定实践而制定，为电子数据复制设备的功能要求和检验方法提供科学、规范、统一的方法和标准。

电子数据复制设备鉴定实施规范

1 范围

本技术规范规定了电子数据复制设备的功能要求和检验方法,以及使用电子数据复制设备进行操作的步骤。

本技术规范适用于复制电子数据存储介质存储的数据的软件和硬件设备的检测。

2 术语和定义

2.1

源存储介质 source data storage

存储原始数据的电子数据存储介质。

2.2

目标存储介质 target data storage

存储目标对象的电子数据存储介质。

2.3

逐比特复制bit-stream duplicate

将数据的每个比特位准确复制到目标存储介质中。

注： 逐比特复制的对象可以是数据文件、磁盘分区、整个磁盘等。

2.4

目标对象 target object

从源存储介质复制获得的数据存储对象，包括镜像文件、柱面对齐备份和柱面非对齐备份。

2.5

镜像文件 image file

从源存储介质复制生成的一个或一组文件,从该文件或文件组中存储的数据可重新创建源存储介质存储的数据比特流。本规范所称镜像文件中的比特位是指从镜像文件重新创建获得的数据比特流中的比特位。

2.6

柱面对齐备份 cylinder aligned copy

将源存储介质数据逐比特复制到目标存储介质中，并对文件系统分区表和启动扇区做出适当调整，使分区的第一个扇区与磁盘柱面边界对齐，并对调整所增加的扇区进行合理填充获得的数据存储对象。

2.7

柱面非对齐备份 cylinder unaligned copy

将源存储介质数据逐比特复制到目标存储介质中,并且不调整文件系统分区表和分区启动扇区获得的数据存储对象。

2.8

复制设备 duplication device

读取源存储介质存储的数据并复制到目标对象的软件或硬件设备。

2.9

合理填充 benign fill

在数据复制过程中,当源存储介质特定数据存储区域无法读取或目标存储介质存在剩余数据存储区域时，向目标存储介质对应的数据存储区域填充不会与其他数据混淆的数据。

示例 ：比如填充常数0 或“This data is not from the source data storage”等明显标识该数据不是来自源存储介质的文本。

2.10

可见数据扇区 visible data sector

源存储介质中位于可用分区之内的扇区。

2.11

隐藏数据扇区 hidden data sector

源存储介质中位于可用分区之外的扇区。

2.12

损坏扇区 bad sector

由于物理损坏等原因，无法读取其存储的数据的扇区。

2.13

未解决错误 unresolved error

复制设备向源存储介质或目标存储介质发出指令时存储介质返回失败或错误状态码，如果复制设备通过重发指令或改为执行其他指令仍然无法完成其所要实现的目标或仍然返回失败或错误状态码，则称发生的错误为未解决错误。

3 要求

3.1 接口可用性要求

电子数据复制设备应能使用其支持的所有接口复制数据。

3.2 目标对象要求

复制设备应生成镜像文件、柱面对齐备份或柱面非对齐备份。

3.3 复制完整性要求

对于源存储介质所有可见数据扇区和隐藏数据扇区中的任一比特位，复制设备生成的目标对象中都可获得与其相对应的比特位。

3.4 复制准确性要求

如果源存储介质中的比特位可读取，复制设备生成的目标对象中的比特位与对应的源存储介质中的比特位数值应一致。

3.5 错误处理要求

a) 如果从源存储介质读取数据发生未解决错误，复制设备应告知用户发生的错误类型和位置；
b) 如果向目标对象写入数据发生未解决错误，复制设备应告知用户发生错误；
c) 如果源存储介质中存在损坏扇区，复制设备生成的目标对象中对应的比特位应被合理填充。

3.6 存储空间不匹配处理要求

3.6.1 存储空间不足处理要求

a) 如果目标存储介质存储空间不足，复制设备应告知用户；
b) 如果目标对象为镜像文件，且复制设备支持切换目标存储介质，复制设备应提示用户切换目标存储介质，并在目标存储介质切换后在新的目标存储介质上继续写入镜像文件。

3.6.2 存储空间过剩处理要求

如果目标对象为柱面非对齐备份，且数据复制后目标存储介质存在剩余存储空间，复制设备应保留剩余存储空间的数据不变或对剩余存储空间进行合理填充。

3.7 写保护要求

复制设备应在自带写保护功能或使用写保护设备保护源存储介质的情况下复制数据。

3.8 操作提示要求

3.8.1 风险提示要求

如果用户坚持在已知错误情况下复制，复制完成设备应告知相应风险。

3.8.2 标识要求

复制设备应有明确的标识区分源存储介质和目标存储介质。

3.8.3 状态显示要求

复制设备应能显示当前的操作状态、复制速度、操作进度等信息。

3.8.4 中断操作要求

如果复制设备正在执行使用者设置的某一类操作时，使用者因某些原因需要中止当前的操作，复制设备应允许使用者执行中断操作。

4 检测步骤

4.1 检测要求

检测要求如下：

a) 对于复制设备支持的所有访问接口，均应分别按照本章规定的方法逐一检测；
b) 对于复制设备支持的所有目标对象，均应分别按照本章规定的方法逐一检测。

4.2 对于复制设备支持的所有目标对象，均应分别按照本章规定的方法逐一检测。

4.2.1 对于目标对象为柱面非对齐备份的，按照以下步骤检测：

a) 准备两个型号相同、存储容量相同、不存在损坏扇区的电子数据存储介质，分别记为 A 和 B；
b) 在 A 上随机写入任意数据后进行分区，并使 A 上存在隐藏数据扇区；
c) 使用复制设备将 A 复制到 B 上；
d) 计算 A 和 B 上存储的所有数据的校验值，比较校验值，如果一致，则判定符合复制完整性要求和复制准确性要求，否则判定不符合复制完整性要求和复制准确性要求。

注： 校验值可以是MD5、SHA-1、SHA-256等。

4.2.2 对于目标对象为镜像文件的，按照以下步骤检测：

a) 准备两个型号相同、存储容量相同、不存在损坏扇区的电子数据存储介质，分别记为 A 和 B；
b) 准备一个存储容量大于 A 的电子数据存储介质，记为 C；
c) 在 A 上随机写入任意数据后进行分区，并使 A 上存在隐藏数据扇区；
d) 使用复制设备将 A 复制生成镜像文件存储到 C 上；
e) 从镜像文件重新创建源存储介质的比特流并写入到 B 上；
f) 计算 A 和 B 上存储的所有数据的校验值，如果校验值一致，则判定符合复制完整性要求和复制准确性要求,否则判定不符合复制完整性要求和复制准确性要求。

4.3 错误处理要求的检测

a) 准备两个存在损坏扇区的电子数据存储介质，其中存储容量较小的记为 A，存储容量较大的记为 B；
b) 准备与 A 型号相同、存储容量相同、不存在损坏扇区的电子数据存储介质，记为 C；
c) 使用复制设备将 A 中的数据复制到 B 上，并使复制过程中 A 的损坏扇区被读取，B 的损坏扇区被写入；
d) 检查复制设备是否报告 A 的损坏扇区读取错误和错误位置，如果未报告错误和错误位置，则判定不符合错误处理要求；
e) 检查复制设备是否报告 B 的损坏扇区写入错误，如果未报告错误，则判定不符合错误处理要求；
f) 对于目标对象为柱面非对齐备份的，检查 B 中与 A 损坏扇区对应的扇区是否得到合理填充，如果未得到合理填充则判定不符合错误处理要求；
g) 对于目标对象为镜像文件的，从镜像文件重新创建源存储介质的比特流并写入到 C 中，检查 C 中与 A 损坏扇区对应的扇区是否得到合理填充，如果未得到合理填充，则判定不符合错误处理要求；
h) 如果上述检测未判定不符合错误处理要求的，则判定符合错误处理要求。

4.4 存储空间不匹配处理要求的检测

4.4.1 存储空间不足处理要求的检测

检测方法为：

a) 准备两个存储容量不同、不存在损坏扇区的电子数据存储介质，其中存储容量较大的记为 A，存储容量较小的记为 B；
b) 对于目标对象为镜像文件的，准备存储容量大于 A 的电子数据存储介质，记为 C，准备型号和存储容量与 A 相同的电子数据存储介质，记为 D；
c) 将 A 分为两个分区，假定第一个分区起始扇区至第二个分区起始扇区的长度为 N 个扇区，保证 B 的存储空间大于 N 个扇区；
d) 使用复制设备将 A 复制到 B 上；
e) 检查复制设备是否报告目标存储空间不足；
f) 计算 B 上存储的所有数据的校验值和 A 从第一个物理扇区开始，存储空间大小与 B 相同的所有扇区的校验值，比较两个校验值是否一致；
g) 对于目标对象为镜像文件的，检查复制设备是否提示用户切换目标存储介质。如果提示用户切换目标存储介质，则切换到 C。在复制完成过后，从镜像文件重新创建 A 的比特流并写入到 D 中。计算 A 和 D 上存储的所有数据的校验值，比较两个校验值是否一致；
h) 对于复制过程中未提示用户目标存储空间不足或校验值不一致的，判定不符合存储空间不足处理要求，否则判定符合存储空间不足处理要求。

4.4.2 存储空间过剩处理要求的检测

检测方法为：

a) 准备两个存储容量不同、不存在损坏扇区的电子数据存储介质。存储容量较小的记为 A，存储容量较大的记为 B。假定 A 的扇区总数为 N，B 的扇区总数为 M；
b) 计算 B 的第 N+1 个扇区到最后一个扇区所保存的数据的校验值；
c) 使用复制设备将 A 复制到 B 上；
d) 检查 B 的第 N+1 个扇区至最后一个扇区是否得到合理填充，如果得到合理填充，则判定符合存储空间过剩处理要求；如果未得到合理填充，计算 B 的第 N+1 个扇区至最后一个扇区所保存的数据的校验值，如果校验值与数据复制前计算获得的校验值不一致，则判定不符合存储空间过剩处理要求，否则判定符合存储空间过剩处理要求。

注： 对目标对象为镜像文件的，可不检测存储空间过剩处理要求。

4.5 写保护要求的检测

a) 准备两个型号相同、存储容量相同、不存在损坏扇区的电子数据存储介质，分别记为 A 和 B；
b) 在 A 上随机写入任意数据；
c) 计算 A 上存储的所有数据的校验值；
d) 使用复制设备将 A 复制到 B 上；
e) 重新计算 A 上存储的所有数据的校验值，比较校验值，如果一致，则判定符合写保护要求，否则判定不符合写保护要求。

参 考 文 献

[1] GA/T 754-2008 电子数据存储介质复制工具要求及检测方法
[2] GA/T 755-2008 电子数据存储介质写保护设备要求及检测方法
[3] GA/T 976-2012 电子数据法庭科学鉴定通用方法