ICS 35.240
CCS L60

SF

中华人民共和国司法行政行业标准

SF/T 0105—2021

存储介质数据镜像技术规程

Code of practice for forensic imaging of storage media

2021－11－17 发布　　2021－11－17 实施

中华人民共和国司法部　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由司法鉴定科学研究院提出。

本文件由司法部信息中心归口。

本文件起草单位：司法鉴定科学研究院、公安部第三研究所、上海市人民检察院、厦门市美亚柏科信息股份有限公司、厦门市兴百邦科技有限公司。

本文件主要起草人：李岩、施少培、郭弘、吴松洋、高峰、徐志强、孙奕、卢启萌、曾锦华、杨恺、李致君、张辉极、刘善军、胡壮。

存储介质数据镜像技术规程

1 范围

本文件规定了存储介质数据镜像获取的仪器设备、程序、过程要求和记录内容。

本文件适用于司法鉴定/法庭科学领域中存储介质数据镜像的获取和使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GA/T 1476—2018 法庭科学远程主机数据获取技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

源 source

镜像获取过程的输入数据、存储介质或电子设备。

3.2

目标 target

镜像获取过程的输出文件或存储介质。

3.3

镜像文件 image file

从数据源复制生成的，可重新构建数据源数据比特流的一个或一组目标文件。

3.4

坏块 bad block

存储介质中由物理故障导致的无法读取的数据区域。

3.5

合理填充 benign fill

在镜像获取过程中，当数据源特定数据区域无法读取时，或目标存储介质存在多余数据存储区域时，向镜像文件（3.3）或者目标存储介质对应的数据存储区域填充指定数据的过程。

注：填充的指定数据可以是二进制全0、二进制全1或者“BADBLOCK”等显著标示该数据不是来自数据源的文本内容，以避免与其他数据产生混淆。

3.6

在线镜像获取 live image acquisition

在电子设备运行状态下，以其中的存储介质、分区（卷）为源（3.1）的镜像获取过程。

4 缩略语

下列缩略语适用于本文件。

ATA 高级技术附件（Advanced Technology Attachment）
BIOS 基本输入输出系统（Basic Input/Output System）
DCO 设备配置覆盖区（Device Configuration Overlay）
FC 光纤通道（Fiber Channel）
HPA 主机保护区（Host Protected Area）
IDE 集成磁盘电子接口（Integrated Drive Electronics）
iSCSI 基于因特网的小型计算机系统接口（Internet Small Computer System Interface）
PCIe 外设组件互连快线（Peripheral Component Interconnect Express）
RAID 独立磁盘冗余阵列（Redundant Array of Independent Disks）
SAS 串行小型计算机系统接口（Serial Attached SCSI）
SATA 串行高级技术附件（Serial Advanced Technology Attachment）
SCSI 小型计算机系统接口（Small Computer System Interface）
S.M.A.R.T. 自我监测、分析及报告技术(Self-Monitoring Analysis and Reporting Technology)
TPM 可信平台模块（Trusted Platform Module）
USB 通用串行总线（Universal Serial Bus）

5 仪器设备

5.1 硬件

存储介质数据镜像获取和使用所涉及的硬件设备包括但不限于：

a) 电子数据鉴定专用计算机；
b) 存储介质复制设备；
c) 存储介质只读设备；
d) 多功能只读读卡器；
e) 存储介质诊断检测设备；
f) 故障硬盘修复设备；
g) 光盘修复设备；
h) 免拆机硬盘复制工具；
i) 计算机绕密取证工具；
j) 存储介质转接接口及数据线；
k) 分线器；
l) 系统引导盘；
m) 网络设备；
n) 数码照相机/物证翻拍仪；
o) 数码摄像机。

5.2 软件

存储介质数据镜像获取和使用所涉及的软件工具包括但不限于：

a) 只读软件；
b) 具备镜像获取功能的软件；
c) RAID 阵列重组工具；
d) 完整性校验值计算工具；
e) 内存获取软件；
f) 内存数据分析软件；
g) 镜像文件格式转换工具；
h) 镜像挂载工具；
i) 屏幕录像软件。

6 镜像获取程序

6.1 常规镜像获取方式

常规镜像获取方式一般遵循以下程序：

a) 将源存储介质从所在电子设备上断开；
b) 准备目标存储介质并对其进行清洁性检查；
c) 将源存储介质及目标存储介质连接至检验设备，并采取只读措施防止改变源存储介质数据；
d) 读取源存储介质的数据，逐比特复制到镜像文件或目标存储介质；
e) 校验镜像文件或目标存储介质的数据完整性。

6.2 免拆机镜像获取方式

不满足常规镜像获取方式条件时，可选用以下方式进行免拆机镜像获取：

a) 在线镜像获取方式：使用电子设备运行中的操作系统环境获取镜像；
b) 引导获取方式：使用系统引导盘启动电子设备，挂载源存储介质和目标存储介质后获取镜像；
c) 网络获取方式：通过网络访问或挂载源存储介质获取镜像；
d) 外部加载获取方式：将源存储介质所在的电子设备作为外部存储介质连接至检验设备获取存储介质镜像。

示例：部分型号的苹果计算机可在启动时设置为目标磁盘模式，连接至另一台苹果计算机后获取镜像。

7 过程要求

7.1 准备阶段

7.1.1 发现与识别存储介质

7.1.1.1 检材为电子设备时，可通过以下一种或多种方法发现与识别源存储介质：

a) 检查电子设备上的存储介质接口，寻找内置或外接的源存储介质。应关注的接口包括但不限于以下类型：
   1) IDE 接口；
   2) SATA 接口及其衍生接口（MicroSATA、mSATA 等）；
   3) SCSI 接口；
   4) SAS 接口；
   5) FC 接口；
   6) 火线（FireWire）接口（1394A、1394B）；
   7) USB 接口（USB-A、USB-B、USB-C）及其衍生接口（mini-USB、Micro-USB 等）；
   8) M.2 接口；
   9) U.2 接口；
   10) PCIe 接口；
   11) 雷雳（Thunderbolt）接口；
   12) 厂商专有接口（如苹果计算机固态硬盘接口）。
b) 通过 BIOS、操作系统和 RAID 控制器等界面检查并识别连接至电子设备的存储介质；
c) 检查并识别基于 iSCSI 协议的网络存储介质。

7.1.1.2 识别具有特定关联性的存储介质组合形态（如 RAID、混合存储等）。

7.1.2 判断存储介质状态

7.1.2.1 可通过读取 S.M.A.R.T.信息、辨识存储介质运转声音等方法，或通过制造商或第三方提供的存储介质诊断检测工具初步判断源存储介质状态，状态分类及分类原则如下：

a) 正常：没有坏块，或未检测出异常；
b) 稳定损坏：数据区域有坏块，多次读取时坏块位置不变，且读取过程中跳过坏块不会降低性能；

c) 不稳定损坏：数据区域有坏块，多次读取时坏块位置不稳定，或读取过程中会出现明显性能下降、持续报错或异响；
d) 无法读取：全部数据区域均无法读取。

7.1.2.2 包含源存储介质的电子设备处于运行状态时，如需断开电源，应先确认源存储介质的加密情况。

7.1.3 选择镜像获取方式

7.1.3.1 满足以下全部条件时，适用常规镜像获取方式：
a) 源存储介质便于从所在电子设备移除或断开；
b) 源存储介质具有通用数据接口；
c) 源存储介质具备只读条件。

7.1.3.2 满足以下一个或多个条件时，适用免拆机镜像获取方式：
a) 断电或关机可能导致数据源无法访问；
b) 源存储介质不便于拆卸；
c) 源存储介质加密，且不具备独立解密条件（如受 TPM 和 Apple T2 等硬件加密芯片保护的磁盘）；
d) 源存储介质具有特殊的数据接口或特殊的数据组成方式等，使用常规镜像获取方式无法获得完整数据。

7.1.4 连接检验设备

7.1.4.1 将存储介质从电子设备断开前，宜记录电子设备接口与存储介质的对应关系。

7.1.4.2 宜选用存储介质原有接口连接至检验设备。

示例：安装于 USB 接口硬盘盒内的 SATA 接口硬盘宜选择 SATA 接口连接。

7.1.4.3 对于存在多个接口的存储介质或电子设备，宜选用传输带宽和稳定性高的接口连接至检验设备。

7.1.4.4 源存储介质或电子设备接口无法直接被检验设备支持时，应选用经过稳定性及兼容性验证的转接接口及数据线进行转换。

7.1.4.5 使用分线器扩展接口时，宜选用独立供电的分线器。

7.1.4.6 具备只读条件的，应采取只读措施，避免改变源存储介质数据；不具备只读条件的，应对镜像获取过程进行录像。

7.1.4.7 检验设备运行过程中应确保全程持续稳定供电，并关闭自动休眠、屏幕保护程序等可能产生干扰的功能或程序。

7.1.5 确定镜像目标

7.1.5.1 镜像获取前，应确保目标存储介质或存储目标镜像文件的位置有充足的可用空间。

7.1.5.2 镜像目标的格式及压缩、分段、加密等特性的选择可根据镜像源、存储位置、检验设备情况以及后续检验要求确定。

7.2 各类存储介质的镜像获取

7.2.1 磁介质硬盘

7.2.1.1 若磁盘存在 ATA 加密，应先移除加密。

7.2.1.2 若检验要求关注隐藏数据，应对隐藏区域进行处理（如移除 HPA 和 DCO）。

7.2.2 固态硬盘

宜采取避免或抑制 TRIM 指令的方式获取镜像，具体方法包括但不限于：
a) 禁用检验设备自动挂载分区（卷）的功能；
b) 使用具备禁用自动挂载功能的引导盘以引导获取方式获取镜像；
c) 使用工厂访问模式(Factory Access Mode)获取镜像；

d) 执行特定的系统命令。

7.2.3 USB 闪存盘

7.2.3.1 若读取过程中遇到坏块，应断电后重新加电，或重置 USB 闪存盘所连接的 USB 总线。

7.2.3.2 不宜将源存储介质与目标存储介质连接至同一 USB 分线器。

7.2.4 存储卡

连接至适配的只读读卡器，参照USB闪存盘获取镜像。

7.2.5 光盘

7.2.5.1 非染料层刮花、磨损，或盘片不平整，影响读取时，应先进行修复。

7.2.5.2 对于多区段光盘，获取镜像时应包含所有区段。

7.2.6 RAID

RAID可采用以下方法之一获取镜像：

a) 对于已挂载状态的 RAID，以整个卷为源获取镜像；
b) 使用引导启动方式，加载 RAID 驱动后，采取只读措施获取 RAID 卷镜像；
c) 记录磁盘排列顺序、RAID 类型和条带大小等 RAID 配置信息后，获取 RAID 中的每个成员盘的镜像。

7.2.7 混合存储

对于非RAID方式组成的混合存储（如苹果Fusion Drive、微软Storage Spaces和英特尔Optane Memory等），可采用以下方式获取镜像：

a) 采用免拆机获取方式，以混合存储中的卷为源获取镜像；
b) 分别获取每个成员盘的镜像，再对数据进行重组。

7.2.8 小型存储系统

使用在线镜像获取方式时，在不影响数据可用性的情况下宜停用镜像获取过程中可能修改磁盘数据的服务（如数据库）。

7.2.9 远程服务器

7.2.9.1 对于远程服务器中的源存储介质，可按照 GA/T 1476—2018 中的 4.6 要求，以网络获取方式获取镜像。

7.2.9.2 对于云端系统，可从云服务提供商的管理界面下载镜像。

7.3 加密存储介质处理

若源存储介质存在全盘加密或部分加密，可采用以下一种或多种方法处理：

a) 对于运行状态的电子设备，将处于解密状态的存储介质、分区（卷）作为镜像源，进行在线镜像获取；
b) 对于运行状态的计算机设备，可获取其物理内存的镜像后，分析、提取解密密钥，也可通过系统命令或绕密工具导出解密密钥；
c) 使用委托人提供的解密口令或解密密钥；
d) 在其他存储介质、电子设备或纸质材料上查找解密口令或解密密钥。

7.4 损坏存储介质处理

7.4.1 当源存储介质存在磁头故障、电路板故障、外电路故障、晶振损坏、电机故障或固件损坏等非数据存储区硬件故障，造成存储介质的数据无法读取时，宜先修复硬件故障，再获取镜像。

7.4.2 当源存储介质存在磁盘或闪存芯片坏块、盘片划痕、磁头读数据性能弱或磁存储信息弱等数据存储区的硬件故障，造成存储介质稳定损坏或不稳定损坏时，可尝试直接获取镜像。

7.4.3 获取稳定损坏存储介质的镜像时，可定位并跳过存储介质的损坏区域，对未损坏的数据区域进行镜像。

7.4.4 获取不稳定损坏存储介质的镜像时，在综合评估后可选用以下策略中的一种或多种方法定位存储介质的损坏区域，对未损坏的数据区域进行镜像：

a) 绕过 BIOS 和操作系统使用 ATA 指令读取；
b) 禁用坏块自动重映射；
c) 逆向读取；
d) 跳过定长区域；
e) 硬件复位（如重新加电）；
f) 调整每次读取的块大小及超时时间；
g) 多次读取。

7.4.5 对于数据区域不能完整读取的存储介质，应采用分段校验，确保可读取数据区域的数据完整性；无法读取的数据区域在镜像中应被合理填充。

8 记录内容

8.1 存储介质镜像获取过程记录宜包含以下内容：

a) 案件信息（如案件编号和案件名称等）；
b) 源存储介质或电子设备的品牌、型号及序列号等信息；
c) 源存储介质或电子设备送检时的性状；
d) 源存储介质或电子设备的照片；
e) 源存储介质或电子设备的唯一性标识（如唯一性编号或资产标签等）；
f) 源存储介质所在电子设备内部时钟的时间；

注：记录时钟时间时宜关注不同操作系统对硬件时钟读取方式的差异。

g) 镜像获取方式及镜像类型；
h) 镜像获取工具的名称、版本号、运行方式及参数；
i) 镜像获取的操作人员；
j) 镜像获取过程的开始和结束时间；
k) 镜像源的起始和终止物理地址；
l) 镜像源和镜像目标的完整性校验值；
m) 镜像文件名及保存位置；
n) 镜像获取过程中的错误或异常情况（若适用）；
o) 口令或密钥等解密所需信息（适用于已加密镜像）；
p) 合理填充的内容及起止位置（适用于合理填充过程）。

8.2 检验设备生成的记录文件若包含 8.1 中的任一要素，可导出后作为镜像获取过程记录使用。

参 考 文 献

[1] GB/T 31500—2015 信息安全技术 存储介质数据恢复服务要求
[2] DL/T 1757—2017 电子数据恢复和销毁技术要求
[3] SF/Z JD0400001—2014 电子数据司法鉴定通用实施规范
[4] SF/Z JD0401001—2014 电子数据复制设备鉴定实施规范
[5] SWGDE. SWGDE best practices for computer forensic acquisitions. Version 1.0
[6] Nikkel Bruce. Practical forensic imaging: securing digital evidence with Linux tools. No Starch Press,2016
[7] Carrier Brian. File system forensic analysis. Addison-Wesley Professional,2005