ICS 07.140
CCS L77

SF

中华人民共和国司法行政行业标准

SF/T 0146—2023

文件恢复工具技术要求和测试评价方法

Technical requirement and evaluation approach for file recovery tool

2023－10－07 发布　　2023－12－01 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、国家信息中心、中国政法大学、厦门市美亚柏科信息股份有限公司、上海弘连网络科技有限公司、国网黑龙江省电力有限公司、四川效率源信息安全技术股份有限公司、北亚康成（北京）科技有限公司、厦门市兴百邦科技有限公司。

本文件主要起草人：李岩、郭弘、王笑强、戴士剑、韩冰、孙奕、张羽、尚方、钱志高、徐志强、张佳强、沈长达、刘思棋、田野、卢启萌、杨恺、李致君、耿浦洋、曾锦华、毛晓、凌嵘。

文件恢复工具技术要求和测试评价方法

1 范围

本文件描述了用于电子数据鉴定的文件恢复工具和测试评价方法，规定了文件恢复工具的功能性等九方面的技术要求。

本文件适用于司法鉴定领域中文件恢复工具或综合工具中文件恢复功能的设计、开发、测试和评估，不适用于评价在司法鉴定活动中工具选用和使用的正确性，也不适用于评价从物理故障存储介质中恢复数据的工具。

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。

GB/T 25000.10—2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第10部分：系统与软件质量模型

GB/T 25000.51—2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第51部分：就绪可用软件产品(RUSP)的质量要求和测试细则

GB/T 31500—2015 信息安全技术 存储介质数据恢复服务要求

SF/T 0105 存储介质数据镜像技术规程

3 术语和定义

GB/T 25000.51—2016、GB/T 31500—2015、SF/T 0105界定的以及下列术语和定义适用于本文件。

3.1

文件系统对象 file system object

文件系统存储和管理的基本数据单元。

示例：文件和文件夹/目录。

3.2

文件系统元数据 file system metadata

描述文件系统对象（3.1）的相关外围信息或属性。

示例：文件/目录名称、时间属性、访问权限、所有者和位置等。

3.3

文件系统解析 file system parsing

通过读取文件系统元数据(3.2)来识别未删除文件系统对象(3.1)和已删除的文件系统对象(3.1)的过程。

3.4

文件碎片 file fragment

属于同一文件的一个或多个连续的、且被不属于该文件的数据块分隔的数据块。

3.5

文件重构 file carving

不依赖文件系统元数据(3.2)，通过文件自身的数据特征从检材中识别、提取文件或文件碎片(3.4)，并使用文件碎片（3.4）重组文件的过程。

3.6

文件修复 file repairing

对已知结构损坏或局部数据缺失的文件，使用适当的方式修复损坏部分或填补缺失部分，以正常识别文件内容的过程。

3.7

文件恢复工具 file recovery tool

使用文件系统解析（3.3）和文件重构（3.5）等技术恢复已删除文件，或者使用文件修复（3.6）技术修复已损坏文件，输出恢复或修复的文件及相关过程记录数据的专用软件工具。

注：文件恢复工具可以是包含文件系统解析、文件重构和文件修复中一类或几类功能的独立工具，也可以是与其他功能整合而成的综合工具中的功能模块。

4 文件恢复工具描述

文件恢复工具（本文件中在不引起混淆的情况下简称为“工具”）使用特定的算法来实现还原被删除文件过程的自动化。由于删除过程的多样性，较难通过一个统一的场景来评价文件恢复工具的实际效果。但是，通过模拟特定方式增加或删除数据后形成测试样品（见附录A.1），可以评价文件恢复工具在相应的情况下的恢复效果。

5 总体要求

5.1 文件恢复工具的产品质量应符合GB/T 25000.10—2016中4.3定义的产品质量模型，包括功能性、性能效率、兼容性、易用性、可靠性、信息安全性和维护性7类要求，并应符合6.1～6.7的规定。

5.2 文件恢复工具属于GB/T 25000.51—2016中定义的就绪可用软件产品，用户文档集是用户正确使用工具和正确解释工具输出结果的基础，应符合GB/T 25000.51—2016中5.2的规定，并应符合6.8的规定，在测试评价方法中作为其他项目的必要条件，不单独进行测试评价。

6 技术要求

6.1 功能性

6.1.1 信息录入

工具应支持录入和存储检验相关信息，包括但不限于：

a) 案件编号；
b) 检材编号；
c) 检验人员；
d) 检验时间。

6.1.2 检材加载

6.1.2.1 工具应支持加载以下类型的检材：

a) 本地存储介质；
b) 存储介质镜像文件；
c) 由存储介质或其镜像文件构成的独立磁盘冗余阵列（RAID）；
d) 通过网络映射到本地的存储介质。

6.1.2.2 工具应支持在加载检材时显示其附属信息，包括但不限于：

a) 存储介质的型号和序列号；
b) 存储介质的自我监测、分析及报告技术（ S.M.A.R.T.）信息；
c) 存储介质镜像文件内含的存储介质信息和校验值；
d) 磁盘阵列的类型、编排方式和条带大小等信息；
e) 网络存储介质的连接信息。

6.1.2.3 工具同时加载多个同类检材时，应采取有效的措施区分各个检材。

6.1.2.4 工具应支持按照SF/T 0105的规定制作存储介质镜像文件。

6.1.3 文件系统解析

6.1.3.1 工具应支持根据指定的文件系统类型搜索丢失或曾经存在的分区（卷）。

6.1.3.2 工具应支持自动识别和解析文件系统元数据以及已删除、未删除的文件系统对象。

6.1.3.3 工具应支持按照用户指定的文件系统类型识别和解析文件系统元数据以及已删除、未删除的文件系统对象。

6.1.4 文件重构

6.1.4.1 工具应支持常见的文件类型，包括文档文件、压缩文件、图片文件、音频文件和视频文件等。
6.1.4.2 工具应支持将检材中指定地址范围的数据或文件系统未分配区域作为待恢复区域。
6.1.4.3 使用文件重构方式恢复的文件应使用能够与其他方式恢复的文件相区分的规则命名。
6.1.4.4 工具应支持特殊情况下的文件重构，包括但不限于：

a) 文件尾部缺失或无尾部特征；
b) 需要重组文件碎片。

6.1.5 文件修复

6.1.5.1 修复后的结果文件应能够按照预期格式正常打开，不应缺失既有信息，也不应引入与文件内容无关的信息。在修复具有特定结构特征的文件时填充的结构特征信息可不视为无关信息，但应予以说明。
6.1.5.2 对于无法修复或修复失败的情况应给出提示。

6.1.6 数据搜索

6.1.6.1 搜索对象应支持搜索检验相关信息、检材原始数据和恢复结果数据等。
6.1.6.2 工具应支持以十六进制数据、指定编码的文本关键字和正则表达式等形式的数据搜索。
6.1.6.3 工具应支持预览搜索结果上下文。
6.1.6.4 工具应支持文件列表项目的搜索，如文件名和文件时间等。

6.1.7 数据标记

6.1.7.1 工具应支持恢复结果数据的标记及取消标记，标记的对象应包括以下内容：

a) 单个文件系统对象或恢复结果对象；
b) 用户选择的多个文件系统对象或恢复结果对象；
c) 恢复结果搜索、筛选和过滤结果文件。

6.1.7.2 工具应支持利用标记数据生成报告及单独导出标记数据。

6.1.8 数据去重

工具应支持对相同数据来源的恢复结果的去重。

注：相同数据来源是指以不同恢复方式或算法检出的、物理位置相同的数据。

6.1.9 数据统计

6.1.9.1 工具应支持恢复结果数据的汇总统计，统计的项目包括但不限于：

a) 以案件、检材、分区（卷）和目录等为单位的文件数和汇总数据容量；
b) 已标记文件的文件数和汇总数据容量。

6.1.9.2 数据容量统计应按照导出数据大小预估。

6.1.10 数据溯源

6.1.10.1 工具应支持对恢复结果数据的溯源。若相关数据可用，应显示以下信息：

a) 文件的原始路径；
b) 文件的首字节地址或簇（块）号；
c) 文件碎片情况。

6.1.10.2 工具应支持对操作过程的溯源，相关记录应能追溯到对结果有影响的关键操作步骤和参数配置。

6.1.11 数据展示

6.1.11.1 工具应支持展示识别到的文件系统对象的状态。对于识别到的已删除文件系统对象，若相关数据可用，应显示以下信息：

a) 文件首簇（块）是否被覆盖；
b) 显示文件名是否为原有；
c) 文件类型是否与扩展名相符。

6.1.11.2 工具应支持对文件系统对象的展示，展示方式包括但不限于：

a) 以列表形式展示；
b) 以目录树形式展示；
c) 以时间线形式展示；
d) 以文件类型和日期等分组展示；
e) 以缩略图形式展示图像和视频文件；
f) 以预览形式展示文档。

6.1.12 数据导出

6.1.12.1 工具应支持导出恢复结果数据，导出选项应包括但不限于：

a) 同时导出文件列表；
b) 按照指定的上限条数（如 104 万条）拆分导出的文件列表；
c) 保留原目录结构；
d) 保留文件原有的时间属性；
e) 仅导出标记的文件；
f) 导出同时计算文件的校验值。

6.1.12.2 工具应采取适当的措施处理结果数据导出过程中的以下异常或冲突情况：

a) 文件名或目录名冲突；
b) 文件名或路径包含操作系统不支持的字符或格式；
c) 文件名或目录名超过文件系统支持的长度；
d) 导出数据容量大于目标位置的可用容量。

6.1.12.3 工具应至少提供以下通用格式中的 1 种导出恢复的文件列表：

a) 特定字符分隔数值文档（如以逗号或制表符分隔数值的文本文档）；
b) 数据库格式（如 SQL 脚本、SQLite）；
c) 可扩展标记语言（XML）；
d) JavaScript 对象表示法（JSON）。

6.1.12.4 工具应支持导出检验过程中对结果有影响的关键参数的值。

6.1.13 校验值计算

6.1.13.1 工具应支持计算以下项目的校验值：

a) 检材数据；
b) 列表展示的文件；
c) 导出的数据。

6.1.13.2 工具应支持 MD5、SHA1 和 SHA256 等常见的完整性校验算法，宜支持国产校验算法。

6.2 性能效率

6.2.1 用户发起操作到相应功能响应的时间延迟不应超过用户文档集声明的延迟时间值。

6.2.2 存在耗时计算或耗时操作时，应显示预估的结束时间。

6.2.3 存在耗时计算或耗时操作时，工具应能充分利用 CPU、内存和磁盘等硬件资源。

6.3 兼容性

6.3.1 在版本升级后，新版本应能兼容早期版本的案件数据。

6.3.2 在安装、使用和卸载过程中，不应影响设备上的其他软件的正常运行，不应强制要求重启系统。

6.3.3 工具应支持按照用户指定的路径存储检验过程数据和结果数据。

6.3.4 对于具有图形界面的工具，运行过程中应支持多种分辨率显示，并支持调整界面大小和位置。

6.4 易用性

6.4.1 在工具执行的各个步骤中，应支持随时停止或退出操作，在停止关键操作时宜提示可能产生的后果。

6.4.2 对于数据镜像、数据解析和数据搜索等操作应支持暂停，并支持从暂停处继续执行。

6.4.3 工具应支持中文用户界面，应包含足够的提示性和引导性内容，不应存在难以理解、误导或有歧义的表述。

6.5 可靠性

6.5.1 使用相同版本的工具、相同的参数配置和相同的操作流程，对同一检材多次执行恢复过程，应产生相同的恢复结果。

6.5.2 在工具正常退出以及由关机、重启系统和终止进程等操作引发的非正常退出后，再次运行工具时不应存在功能异常。

6.5.3 文件恢复工具应预警可识别的误操作，并采取预防措施。

示例：在导出数据时无法指定检材存储介质作为导出路径。

6.6 信息安全性

6.6.1 文件恢复工具应提供案件管理和身份认证功能，确保不同案件和不同用户的数据互相隔离。

6.6.2 文件恢复工具应提供审计功能，记录用户登录、案件管理、检材添加/删除和操作步骤等关键信息。

6.6.3 若需上传诊断数据，应支持从中删除与检材和案件有关的敏感信息。

6.7 维护性

6.7.1 文件恢复工具应为不同版本（包含模块、组件等）提供唯一的版本标识。

6.7.2 版本升级时，应同步发布包含具体更新内容的更新日志，并同步更新用户文档集。

6.7.3 应提供在线和离线两种方式用于版本更新和授权更新。

6.7.4 对于需要授权使用的工具，应显示授权的起止时间和授权类型。

注：授权类型包括硬件加密狗、软件加密狗和绑定机器码授权等。

6.7.5 对于需要获得授权的工具，其授权时间段内的所有历史版本应是能获得的；对于无需授权的工具，其所有历史版本应是能获得的。

6.7.6 工具出现技术故障后，应支持导出供追溯故障原因的诊断数据。

6.8 用户文档集

6.8.1 用户文档集应说明工具能完成的预期工作任务，具体包括：

a) 文件系统解析；
b) 文件重构；
c) 文件修复。

6.8.2 用户文档集应说明最终用户能调用的所有功能，具体包括：

a) 工具的安装和卸载方法（适用时）；
b) 工具所支持的检材类型；
c) 工具输入和输出数据的格式；
d) 工具界面中各个按钮、选项和表格列的说明。

6.8.3 用户文档集应说明工具的功能参数，包括但不限于：

a) 工具支持的检材类型；
b) 文件系统解析功能所支持的文件系统类型，以及所支持的归属于特定文件系统类型的文件系统对象类型；
c) 解析文件系统元数据及执行数据搜索时所支持的字符编码；
d) 文件重构所支持的文件类型及各文件类型的特征示例；
e) 文件修复支持的文件类型。

6.8.4 用户文档集应列出已知的操作风险，特别是会导致用户数据丢失和应用系统终止的情况。

示例：扫描有坏道的硬盘导致系统无响应，在终止工具运行后丢失前期扫描的结果。

6.8.5 用户文档集应陈述安装工具所需的最小磁盘空间以及工具运行所需的最低系统资源，以及主要的性能参数（如操作延迟）。

6.8.6 用户文档集应采用特定读者可理解的术语和文体，通过编排的目录、清单和索引等形式为理解提供便利。

6.8.7 用户文档集应指明工具在何处依赖于特定的软件（包括操作系统）、硬件和（或）接口。

6.8.8 用户文档集应给出用户可能遇到的所有已知的限制。

示例：试用版无法导出大于 2 MB 的文件。

6.8.9 用户文档集应给出用户可能碰到的所有已知的风险及应对方式。

示例：工具的必要组件被常用杀毒软件告警，工具开发方已确认其安全性，可忽略杀毒软件告警。

6.8.10 若工具提供技术支持，用户文档集应说明用户获得技术支持的渠道，如电话、电子邮件、网站在线客服和上门服务等。

7 测试评价方法

7.1 功能性

7.1.1 信息录入

信息录入的测试方法、预期结果和结果判定如下。

a) 测试方法
   1) 在工具中录入 6.1.1 中的检验相关信息；
   2) 保存案件后重新打开案件，并核对上述信息及操作时间信息。
b) 预期结果
   1) 工具正确存储了已录入的检验相关信息；
   2) 存储的检验相关信息与录入的信息一致；
   3) 工具正确记录了操作时间。
c) 结果判定
   若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.1.2 检材加载

检材加载功能的测试方法、预期结果和结果判定如下。

a) 测试方法
   1) 审查用户文档集中关于支持检材类型的描述；
   2) 依次加载 6.1.2.1 中列出的检材；
   3) 同时加载多个同类型检材；
   4) 加载存储介质，制作其镜像文件。
b) 预期结果
   1) 用户文档集中包含的内容满足 6.1.2 中的各项规定；
   2) 检材均正常加载，且正确显示了相应的附属信息；
   3) 同类型的多个检材可以有效区分；
   4) 成功生成存储介质镜像文件和相应的记录文件。
c) 结果判定
   若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.1.3 文件系统解析

文件系统解析功能的测试方法、预期结果和结果判定如下。

a) 测试方法
   1) 审查用户文档集中关于所支持文件系统类型的描述；
   2) 根据该工具支持文件系统类型选择相应的测试样品，可选的测试样品类别见附录 A.1；
   3) 使用自动识别和手动指定文件系统类型方式，观察文件系统识别结果，适用时，可给出结果的检全率（见附录 A.2.1）和检准率（见附录 A.2.2）指标。

b) 预期结果
   1) 工具支持分区搜索功能；
   2) 工具支持以自动和手动指定方式识别文件系统；
   3) 测试样品中的文件系统对象均能正确识别。
c) 结果判定
   若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.1.4 文件重构

文件重构功能的测试方法、预期结果和结果判定如下。

a) 测试方法
   1) 审查用户文档集中关于文件重构功能的描述；
   2) 选择或准备相应的测试样品，选择工具支持重构的文件类型执行恢复过程，观察恢复结果；
   3) 分别指定样品中的地址范围以及文件系统未分配区域执行恢复过程；
   4) 选择或准备相应的测试样品，对无文件尾特征以及包含两个碎片的文件执行恢复过程；
   5) 适用时，可给出结果的检全率（见附录 A.2.1）和检准率（见附录 A.2.2）指标。
b) 预期结果
   1) 用户文档集中包含的功能描述满足 6.1.4 中的各项规定；
   2) 工具所支持的文件类型均能够成功恢复，恢复文件命名满足 6.1.4.3 的规定；
   3) 工具可以将指定地址范围或文件系统未分配区域作为待恢复区域并成功恢复文件；
   4) 工具成功恢复了特殊情况下的文件。
c) 结果判定
   若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.1.5 文件修复

文件修复的测试方法、预期结果和结果判定如下。

a) 测试方法
   1) 审查用户文档集中关于文件修复功能的描述；
   2) 使用已知可修复的损坏文件作为测试样品，分别选择有参照文件和无参照文件的方式执行文件修复过程并查看修复结果文件；
   3) 使用已知无法修复的损坏文件作为测试样品，分别选择有参照文件和无参照文件的方式执行文件修复过程并查看修复结果。
b) 预期结果
   1) 用户文档集中包含的内容满足 6.1.5 中的各项规定；
   2) 工具提供了有参照文件和无参照文件的修复方式；
   3) 已知可修复的损坏文件修复结果文件可以正常打开，包含全部既有信息，不包含与文件内容无关的信息；
   4) 已知无法修复的损坏文件的修复结果给出了无法修复或修复失败的提示。
c) 结果判定
   若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.1.6 数据搜索

数据搜索的测试方法、预期结果和结果判定如下。

a) 测试方法
   1) 审查用户文档集中关于数据搜索功能的描述；
   2) 使用 6.1.1 中录入的检验信息执行搜索；
   3) 加载包含常见编码数据的测试样品后，使用其中的文本字符串执行搜索，查看搜索结果预览，标记部分搜索结果并导出文件；
   4) 使用测试样品中包含的十六进制数值执行搜索，查看搜索结果预览，标记部分搜索结果并导出文件；
   5) 在文件列表中根据文件名、文件时间执行搜索。

b) 预期结果
1) 用户文档集中包含的内容满足 6.1.6 中的各项规定；
2) 案件信息的搜索结果正确返回了所需检验信息；
3) 文本字符串搜索结果正确返回了所需数据，搜索结果上下文预览正常，被标记文件正确导出；
4) 十六进制数值的搜索结果正确返回了所需数据，搜索结果上下文预览正常，被标记文件正确导出；
5) 文件列表中根据文件名、文件时间可以搜索到所需文件。
c) 结果判定
若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.1.7 数据标记

数据标记的测试方法、预期结果和结果判定如下。
a) 测试方法
1) 审查用户文档集中关于数据标记功能的描述；
2) 使用测试样品执行数据恢复，在文件列表依次标记单个文件、批量标记多个文件；
3) 在搜索、筛选和过滤等操作后执行数据标记；
4) 使用标记数据生成报告；
5) 单独导出标记文件。
b) 预期结果
1) 用户文档集中包含的内容满足 6.1.7 的规定；
2) 标记操作均成功完成，需标记文件没有遗漏或多余；
3) 操作结果文件标记成功完成，需标记文件没有遗漏或多余；
4) 正确导出了标记数据报告；
5) 正确导出了标记文件。
c) 结果判定
若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.1.8 数据去重

数据去重的测试方法、预期结果和结果判定如下。
a) 测试方法
1) 审查用户文档集中关于数据去重功能的描述；
2) 使用测试样品执行文件系统数据恢复和文件重构两种数据恢复操作，并执行去重操作；
3) 观察工具是否有效合并了相同文件；
4) 计算结果文件校验值后，执行根据校验值的去重。
b) 预期结果
1) 用户文档集中包含的内容满足 6.1.8 中的各项规定；
2) 去重操作成功完成；
3) 文件列表中相同文件能有效合并显示；
4) 同一校验值文件去重后只保留 1 个，或合并显示。
c) 结果判定
若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.1.9 数据统计

数据统计的测试方法、预期结果和结果判定如下。
a) 测试方法
1) 审查用户文档集中关于数据统计功能的描述；
2) 新建检验案例，使用测试样品执行文件恢复，按需执行数据统计操作；
3) 标记多个文件，按需执行数据统计操作；
4) 分别导出被统计的数据，观察其大小与统计大小的是否相同。

b) 预期结果
   1) 用户文档集中包含的内容满足 6.1.9 中的各项规定；
   2) 数据统计自动完成或者在执行统计操作后成功完成，并显示了统计文件数和文件大小；
   3) 数据统计自动完成或者在执行统计操作后成功完成，并显示了统计文件数和文件大小；
   4) 导出数据大小与统计的大小相同。
c) 结果判定
   若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.1.10 数据溯源

数据溯源的测试方法、预期结果和结果判定如下。

a) 测试方法
   1) 审查用户文档集中关于数据溯源功能的描述；
   2) 使用测试样品执行基于文件系统的恢复，观察结果中显示的文件原始路径、文件首字节地址或簇（块）号、文件碎片情况；
   3) 使用测试样品执行文件重构恢复，观察结果中显示的文件首字节地址或簇（块）号、文件碎片情况；
   4) 查看工具中的操作过程溯源记录。
b) 预期结果
   1) 用户文档集中包含的内容满足 6.1.10 中的各项规定；
   2) 基于文件系统的恢复结果正确显示了文件原始路径、文件首字节地址或簇（块）号、文件碎片情况；
   3) 文件重构结果正确显示了文件首字节地址或簇（块）号、文件碎片情况；
   4) 溯源记录中能体现对结果有影响的关键操作步骤和操作参数。
c) 结果判定
   若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.1.11 数据展示

数据展示的测试方法、预期结果和结果判定如下。

a) 测试方法
   1) 审查用户文档集中关于数据展示功能的描述；
   2) 审查工具对于已删除文件系统对象的显示信息；
   3) 审查工具对文件系统对象的展示方式。
b) 预期结果
   1) 用户文档集中包含的内容满足 6.1.11 中的各项规定；
   2) 已删除文件系统对象的显示的信息满足 5.1.11.1 中的各项规定；
   3) 文件系统对象展示方式包括 6.1.11.2 中至少 4 种。
c) 结果判定
   若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.1.12 数据导出

数据导出的测试方法、预期结果和结果判定如下。

a) 测试方法
   1) 审查用户文档集中关于数据导出功能的描述；
   2) 使用测试样品执行基于文件系统的恢复，标记部分结果文件，执行导出操作，审查工具是否提供了 6.1.12.1 的导出选项；
   3) 执行导出过程，审查导出结果；
   4) 在 6.1.12.2 各个情况下执行导出操作，审查导出结果；
   5) 审查工具支持的通用格式，选择该格式导出数据；
   6) 导出检验过程中设置的参数值。
b) 预期结果

1) 用户文档集中包含的内容满足 6.1.12 中的各项规定；
2) 工具提供了 6.1.12.2 的各种导出选项；
3) 工具正确按照选项导出了结果数据；
4) 工具正确处理了导出过程中的异常情况；
5) 工具支持 6.1.12.3 中至少 1 种通用格式，且成功使用该格式导出了数据；
6) 检验过程中设置的、对结果有影响的参数值均正确导出。

c) 结果判定

若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.1.13 校验值计算

校验值计算的测试方法、预期结果和结果判定如下。

a) 测试方法
1) 审查用户文档集中关于校验值计算功能的描述；
2) 根据 6.1.13.1 规定的项目，分别计算数据的校验值，校验算法种类覆盖 6.1.13.2 的规定。

b) 预期结果
1) 用户文档集中包含的内容满足 6.1.13 中的各项规定；
2) 工具按照 6.1.13.1 的规定正确计算并得出相应数据的校验值。

c) 结果判定

若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.2 性能效率

性能效率的测试方法、预期结果和结果判定如下。

a) 测试方法
1) 审查用户文档集中关于操作延迟的描述；
2) 加载测试样品执行耗时操作（如字节级的文件重构和全盘文件恢复等），观察操作的响应时间；
3) 观察工具是否显示了结束时间；
4) 在硬件资源有显著差异的硬件环境下执行同一文件恢复操作，对比其用时。

b) 预期结果
1) 用户文档集中给出了关于操作延迟的描述；
2) 工具操作的响应延迟不超过用户文档集给出的数值；
3) 工具显示了结束时间；
4) 工具在不同硬件环境下体现出相匹配的性能效率差异。

c) 结果判定

若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.3 兼容性

兼容性的测试方法、预期结果和结果判定如下。

a) 测试方法
1) 在已有案件数据的情况下将工具从旧版本升级至待测版本，观察是否可以正常识别和加载旧版本案件数据；
2) 在运行常用应用软件（如文字处理软件和其他取证工具软件）的情况下，安装、运行和卸载工具，观察其他已运行软件是否出现异常，观察工具是否强制要求重启系统；
3) 审查用户文档集中关于设置数据保存位置的内容，重新设置过程数据和结果数据的存储路径；
4) 调整不同屏幕分辨率，将工具界面最大化，观察工具界面显示是否正常；将工具界面窗口化，调整大小和位置。

b) 预期结果
1) 工具的待测版本正常识别和加载了旧版本案件数据；

2) 工具安装、运行和卸载过程中未影响其他软件正常运行，未强制要求重启系统；
3) 过程数据和结果数据按照设定的路径存储；
4) 工具界面正常适配常见的屏幕分辨率，在窗口模式下可以调整界面大小和位置。

c) 结果判定

若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.4 易用性

易用性的测试方法、预期结果和结果判定如下。

a) 测试方法
1) 在工具运行过程中分别执行中止、停止和退出操作；
2) 切换工具的中文界面，审查文字是否存在难以理解、误导或有歧义的内容。

b) 预期结果
1) 执行中止操作后可以选择继续执行，执行停止操作后可以选择执行新任务，执行退出操作后工具退出；
2) 工具具有中文界面，包含必要的操作提示或引导，且不存在难以理解、误导或有歧义内容。

c) 结果判定

若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.5 可靠性

可靠性的测试方法、预期结果和结果判定如下。

a) 测试方法
1) 使用同一测试样品，按照相同流程多次执行工具的恢复功能，对比结果的一致性；
2) 工具运行过程中以关机、重启系统和终止进程等操作中断工具运行，再次运行工具，观察是否存在功能异常；
3) 使用存储介质作为测试样品，执行数据恢复操作后选择原介质作为导出路径。

b) 预期结果
1) 多次恢复得到了一致的结果；
2) 工具在非正常中断后，再次运行不存在功能异常；
3) 工具不支持选择原存储介质作为导出路径，或对其风险给出了必要的提示。

c) 结果判定

若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.6 信息安全性

信息安全性的测试方法、预期结果和结果判定如下。

a) 测试方法
1) 审查工具是否提供案件管理和用户身份认证功能；
2) 审查工具是否有效隔离了不同案件、不同用户的数据；
3) 审查工具对关键操作的审计记录；
4) 审查工具上传的诊断数据是否删除了与检材、案件相关的敏感信息。

b) 预期结果
1) 工具提供了案件管理和用户身份认证功能；
2) 工具有效隔离了不同案件、不同用户的数据；
3) 工具保留了对关键操作的审计记录；
4) 工具无上传诊断数据的功能，或上传前删除了诊断数据中的敏感信息。

c) 结果判定

若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

7.7 维护性

维护性的测试方法、预期结果和结果判定如下。

a) 测试方法

1） 审查工具（包含模块、组件等）不同版本的版本标识；
2） 审查各个版本的更新日志和用户文档集；
3） 审查工具版本及授权的更新方式；
4） 审查工具的授权信息；
5） 审查工具发布历史版本的网站或仓库等；
6） 审查用户文档集中故障诊断数据的描述。

b） 预期结果

1） 不同版本的版本标识唯一；
2） 工具的各个版本均有相应的更新日志和用户文档集；
3） 若适用，工具提供了在线和离线两种方式更新版本和授权；
4） 若适用，工具授权信息包含了授权的起止时间和授权类型；
5） 工具提供的历史版本覆盖了其授权时间段内的所有版本或全部版本；
6） 工具支持导出故障诊断数据。

c） 结果判定

若b）中预期结果均满足，则判定为符合，其他情况判定为不符合。

附 录 A
（资料性）
测试样品与功能指标

A.1 测试样品

A.1.1 文件系统解析测试样品

表A.1给出了文件系统解析测试样品的类型。

表A.1 文件系统解析测试样品

样品编号	样品描述	涵盖文件系统
FSP-01-01	恢复无文件碎片的删除文件	FAT、exFAT、NTFS、EXT、OSX
FSP-01-02	恢复清空后的回收站文件	FAT、NTFS、EXT
FSP-02	恢复有两个文件碎片的删除文件	FAT、exFAT、NTFS、EXT
FSP-03	恢复有多个文件碎片的删除文件	FAT、exFAT、NTFS、EXT
FSP-04	恢复无文件碎片、文件名包含非ASCII字符的文件	FAT、exFAT、NTFS、EXT、OSX
FSP-05-01	恢复多个文件碎片交错的文件（B1-B2-E1-E2）	FAT、exFAT、NTFS、EXT
FSP-05-02	恢复多个文件碎片交错的文件（B1-C1-B2-C2）	FAT、exFAT、NTFS、EXT
FSP-05-03	恢复多个文件碎片交错的文件（B1-D1-D2-B2）	FAT、exFAT、NTFS、EXT
FSP-06	恢复巨大文件	FAT、exFAT、NTFS、EXT
FSP-07-01	恢复覆盖的单个删除文件	FAT、exFAT、NTFS、EXT
FSP-07-02	恢复覆盖的单个删除文件	FAT、exFAT、NTFS、EXT
FSP-07-03	恢复覆盖的单个删除文件	FAT、exFAT、NTFS、EXT
FSP-08	恢复覆盖的多个删除文件	FAT、exFAT、NTFS、EXT
FSP-09	恢复大量未覆盖文件	FAT、exFAT、NTFS、EXT
FSP-10	恢复大量文件，其中部分为覆盖文件	FAT、exFAT、NTFS、EXT
FSP-11-01	恢复单个无文件碎片的目录	FAT、exFAT、NTFS、EXT
FSP-11-02	恢复单个无文件碎片的目录（NTFS MFT常驻）	NTFS
FSP-11-03	恢复单个无文件碎片的目录（NTFS压缩）	NTFS
FSP-12	恢复单个有文件碎片的目录	FAT、exFAT、NTFS、EXT
FSP-13	恢复文件系统活动	FAT、exFAT、NTFS、EXT
FSP-14	恢复其他文件系统对象	FAT、NTFS、EXT
FSP-15	列出文件系统对象	FAT、exFAT、NTFS、EXT
FSP-16	列出大量文件	FAT、exFAT、NTFS、EXT
FSP-17	列出深层目录下的文件	FAT、exFAT、NTFS、EXT

A.1.2 文件重构测试样品

表A.2给出了文件重构测试样品的类型。

表A.2 文件重构测试样品

样品编号	样品描述	涵盖文件类型
FC-G-01	无文件碎片的图片文件	JPG,PNG,BMP,GIF,TIF,PCX
FC-G-02	文件碎片按顺序排布的图片文件	JPG,PNG,BMP,GIF,TIF,PCX
FC-G-03	文件碎片不按顺序排布的图片文件	JPG,PNG,BMP,GIF,TIF,PCX
FC-G-04	缺失部分文件碎片的图片文件	JPG,PNG,BMP,GIF,TIF,PCX
FC-G-05	图片文件内嵌的图片文件	JPG,PNG,BMP,GIF,TIF,PCX
FC-G-06	文件碎片交错排布的图片文件	JPG,PNG,BMP,GIF,TIF,PCX
FC-D-01	无文件碎片的文档文件	DOC, XLS, PPT, PDF
FC-D-02	文件碎片按顺序排布的文档文件	DOC, XLS, PPT, PDF
FC-D-03	文件碎片不按顺序排布的文档文件	DOC, XLS, PPT, PDF
FC-D-04	缺失部分文件碎片的文档文件	DOC, XLS, PPT, PDF
FC-D-05	文档文件内嵌的文档文件	DOC, XLS, PPT, PDF

表 A.2 文件重构测试样品（续）

样品编号	样品描述	涵盖文件类型
FC-D-06	文件碎片交错排布的文档文件	DOC, XLS, PPT, PDF
FC-R-01	无文件碎片的压缩文件	7Z,BZ2,GZ,TAR,WIM,RAR,ZIP
FC-R-02	文件碎片按顺序排布的压缩文件	7Z,BZ2,GZ,TAR,WIM,RAR,ZIP
FC-R-03	文件碎片不按顺序排布的压缩文件	7Z,BZ2,GZ,TAR,WIM,RAR,ZIP
FC-R-04	缺失部分文件碎片的压缩文件	7Z,BZ2,GZ,TAR,WIM,RAR,ZIP
FC-R-05	压缩文件内嵌的压缩文件	7Z,BZ2,GZ,TAR,WIM,RAR,ZIP
FC-R-06	文件碎片交错排布的压缩文件	7Z,BZ2,GZ,TAR,WIM,RAR,ZIP
FC-A-01	无文件碎片的音频文件	MP3,WAV,AU,WMA
FC-A-02	文件碎片按顺序排布的音频文件	MP3,WAV,AU,WMA
FC-A-03	文件碎片不按顺序排布的音频文件	MP3,WAV,AU,WMA
FC-A-04	缺失部分文件碎片的音频文件	MP3,WAV,AU,WMA
FC-A-05	音频文件内嵌的音频文件	MP3,WAV,AU,WMA
FC-A-06	文件碎片交错排布的音频文件	MP3,WAV,AU,WMA
FC-V-01	无文件碎片的视频文件	MP4,AVI,MOV,FLV,MPG,WMV
FC-V-02	文件碎片按顺序排布的视频文件	MP4,AVI,MOV,FLV,MPG,WMV
FC-V-03	文件碎片不按顺序排布的视频文件	MP4,AVI,MOV,FLV,MPG,WMV
FC-V-04	缺失部分文件碎片的视频文件	MP4,AVI,MOV,FLV,MPG,WMV
FC-V-05	视频文件内嵌的视频文件	MP4,AVI,MOV,FLV,MPG,WMV
FC-V-06	文件碎片交错排布的视频文件	MP4,AVI,MOV,FLV,MPG,WMV

A.2 功能指标

A.2.1 检全率

检全率是指文件恢复工具正确恢复文件占全部待恢复文件的比率。检全率=(与预期相符的恢复文件数量/样品中应识别到的删除文件数量)×100%。

检全率指标与特定的测试样品关联。同一文件重复识别的情况在与分子中仅计入一次。

A.2.2 检准率

检准率是指文件恢复工具正确恢复文件占全部检出文件的比率。检准率=(与预期相符的恢复文件数量/工具识别的删除文件总数量)×100%。

检准率指标与特定的测试样品关联。同一文件重复识别的情况在分子中仅计入一次，分母中计入多次。

参 考 文 献

[1] GB/T 37729—2019 信息技术 智能移动终端应用软件（APP）技术要求

[2] GB/T 39720—2020 信息安全技术 移动智能终端安全技术要求及测试评价方法

[3] ISO/IEC 27041:2015 Guidance on Assuring the Suitability and Adequacy of Digital Investigation Method

[4] FSR-G-218 Issue 2. Forensic Science Regulator Guidance: Method Validation in Digital Forensics

[5] NIST Computer Forensics Tool Testing Program. Active file identification and deleted file recovery tool specification: Draft for comment 1 of version 1.1

[6] NIST Computer Forensics Tool Testing Program. Forensic file carving tool specification: Draft version 1.0 for public comment

[7] NIST Computer Forensics Tool Testing Program. Forensic file carving tool test assertions and test plan: Draft version 1.0 for public comment

[8] SWGDE Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics: Version 1.0