ICS 07.140
CCS A92

SF

中华人民共和国司法行政行业标准

SF/T 0143—2023

移动终端数据鉴定设备技术要求和测试评价方法

Technical requirement and test evaluation approach for mobile terminal data examination device

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、最高人民检察院检察技术信息研究中心、上海市人民检察院、河北省公安厅、广西壮族自治区公安厅、浙江省公安厅、大连市公安局、西安邮电大学、公安部第三研究所、厦门市美亚柏科信息股份有限公司、奇安信科技集团股份有限公司、上海弘连网络科技有限公司、杭州平航科技有限公司、苏州龙信信息科技有限公司。

本文件主要起草人：郭弘、李岩、杜文玉、孙奕、杨恺、高峰、韩马剑、陈兴文、刘浩阳、吴坚、高梓铭、韦同胜、张艳、钱志高、韩争光、朱元栋、王海啸、田野、卢启萌、李致君、耿浦洋、顾健、曾锦华、毛晓、凌嵘。

移动终端数据鉴定设备技术要求和测试评价方法

1 范围

本文件给出了移动终端数据鉴定设备的产品描述，规定了检材支持、功能性、信息安全性、可靠性、易用性、维护性和性能效率的技术要求，描述了测试评价方法。

本文件适用于移动终端数据鉴定设备的设计、开发、测试和评估。

注：本文件所指的移动终端数据鉴定设备，不包括针对移动终端进行解密和解锁，以及对移动终端云存储数据进行鉴定的专用设备，也不包括采用拆焊芯片等特殊方式进行移动终端数据鉴定的专用设备。

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 25000.24 系统与软件工程 系统与软件质量要求和评价(SQuaRE) 第24部分：数据质量测量

GB/T 25000.51 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 35278 信息安全技术 移动终端安全保护技术要求

SF/T 0157 移动终端电子数据鉴定技术规范

3 术语和定义

GB/T 25000.24、GB/T 25000.51、GB/T 35278、SF/T 0157界定的以及下列术语和定义适用于本文件。

3.1

逻辑提取 logical extraction

以提取移动终端文件系统层面的文件（及目录结构）为目标的提取方法。

注：通常利用终端的同步协议或备份工具等实现。

3.2

物理提取 physical extraction

以提取移动终端物理存储介质的位对位镜像为目的的提取方法。

注：通常包括侵入式和非侵入式方法。

3.3

数据解析 data parsing

为使数据可识别，对其进行格式转换、解码、转义和关联等操作的方法。

3.4

衍生数据 derived data

原始数据通过转换或处理等方式形成的可读取的数据。

4 产品描述

移动终端数据鉴定设备是针对各类移动终端及其附属的可移动存储卡等存储介质中所保存的电子数据，进行提取、解析和恢复，并在其基础上进行关联、标记和统计分析后，形成数据结果报告的软硬件设备。

5 技术要求

5.1 检材支持

5.1.1 移动终端

5.1.1.1 设备应支持对主流的移动终端及其操作系统的数据鉴定，包括主流版本和既往发布版本，操作系统的类型包括：

a) iOS 操作系统；
b) Android 操作系统及衍生版本；
c) HarmonyOS 操作系统；
d) 其他智能及非智能移动终端操作系统。

5.1.1.2 对于所支持的移动终端操作系统，设备宜能自动适配驱动程序，并识别移动终端的品牌、型号、操作系统版本及设备标识等信息。

5.1.1.3 设备应支持以逻辑提取或物理提取等方式提取移动终端机身数据，包括但不限于：

a) 机身中的文件及文件系统结构等数据；
b) 系统原生应用数据；
c) 第三方应用程序的数据；
d) 屏幕所显示的信息。

5.1.2 移动终端衍生数据

5.1.2.1 设备应支持对移动终端衍生数据的数据鉴定，衍生数据的类型包括但不限于：

a) 利用移动终端同步、备份和换机等方式所获得的数据；
b) 对移动终端制作的镜像。

5.1.2.2 对于移动终端的衍生数据中有标识其所属移动终端的关联信息时，设备应能准确识别其与所属移动终端的关联关系。

5.1.3 通用集成电路卡（UICC）

设备应支持对移动终端所使用的UICC中的数据鉴定，UICC的类型包括但不限于：

a) 用户身份模块（SIM）卡；
b) 全球用户识别模块（USIM）卡；
c) 用户标识模块（UIM）卡；
d) 可移动用户识别模块（RUIM）卡。

5.1.4 可移动存储卡

设备应支持对移动终端所使用的可移动存储卡中的数据鉴定，可移动存储卡的类型包括但不限于：

a) 安全数码（SD）卡；
b) 微型安全数码（microSD）卡；
c) 多媒体存储卡（MMC）；
d) 记忆棒（MS）；
e) 超微型存储卡（NM）。

5.2 功能性

5.2.1 信息录入

设备应支持对检材进行信息录入，包括但不限于：

a) 案件编号；
b) 检材编号；
c) 检验人员。

5.2.2 数据提取

5.2.2.1 移动终端的数据提取

5.2.2.1.1 逻辑提取

设备应支持对移动终端机身数据进行逻辑提取，提取方式包括但不限于：

a) 利用移动终端同步、备份、换机和数据传输等方式提取移动终端的文件及目录结构，包括系统数据和应用程序数据等；
b) 利用权限提升等方式提取完整或部分移动终端的文件及目录结构，包括系统文件、应用程序数据、多媒体文件和其他用户数据；
c) 利用特定的应用程序提取移动终端的文件及目录结构、应用程序数据、多媒体文件和其他用户数据等。

5.2.2.1.2 物理提取

设备宜支持对移动终端机身数据进行物理提取，提取方式包括但不限于：

a) 利用技术手段进行权限提升后制作移动终端的存储镜像；
b) 利用刷机回读和在线编程等方式制作移动终端的存储镜像。

5.2.2.1.3 照相录像提取

设备应支持拍照和录像等方式提取移动终端屏幕显示的信息。

5.2.2.2 移动终端衍生数据提取

设备应支持对移动终端的衍生数据进行提取。

5.2.2.3 UICC 的数据提取

5.2.2.3.1 设备应支持对移动终端 UICC 的数据进行提取，支持的提取方式包括：

a) 单独对 UICC 进行提取；
b) 与移动终端机身数据共同进行提取。

5.2.2.3.2 设备对移动终端 UICC 提取的内容应包括但不限于：

a) 网络服务提供商名称；
b) 标识信息，如集成电路卡识别码（ICCID）、国际移动用户识别码（IMSI）、国际移动设备识别码（IMEI）和移动基站国际用户识别码（MSISDN）等；
c) 短消息；
d) 通讯录；
e) 通话记录。

5.2.2.4 可移动存储卡的数据提取

设备应支持对移动终端所使用的可移动存储卡进行数据提取，提取可通过移动终端进行，也可直接对可移动存储卡单独进行。

针对移动终端所使用的可移动存储卡进行提取的，应符合SF/T 0157的规定。

5.2.3 数据解析

5.2.3.1 数据解析类型

5.2.3.1.1 系统数据

设备应支持对移动终端提取的系统数据进行解析，包括但不限于以下内容：

a) 移动终端基本信息；
b) 通讯录；
c) 通话记录；
d) 短消息；
e) 日历和待办事项；
f) 应用程序列表；
g) 全部或部分系统日志数据；
h) 文件列表；
i) 无线局域网（WLAN）连接记录；

j） 蓝牙连接记录。

5.2.3.1.2 应用程序数据

设备应支持对提取的移动终端应用程序数据进行解析。

5.2.3.2 数据解析数量

设备应支持对超大数据量（数据条目大于1000万）数据进行解析。

5.2.4 数据恢复

设备应支持对移动终端进行数据恢复，包括但不限于以下数据：

a） 多媒体文件；
b） 日志文件；
c） 缓存文件；
d） 数据库文件。

5.2.5 数据搜索

设备应支持文件搜索、数据内容全文检索和结果报告数据检索等搜索功能。

5.2.6 数据关联

设备应支持对提取、解析和恢复后的结果数据进行数据关联。

5.2.7 数据标记

设备应支持对特定数据和特定文件进行标记，并注释相关信息的功能。

5.2.8 数据去重

设备应支持按需求对提取、解析、恢复和关联后的结果数据进行去重，进行去重的条件应明确展示。

5.2.9 数据统计

5.2.9.1 设备应支持对提取、解析、恢复和去重后的结果数据进行统计，统计的项目包括：

a） 以项目（如案件和事件）为单位的总数据量；
b） 以检材（如移动终端）为单位的总数据量；
c） 每个数据分类（如通讯录和短消息）的数据数量；
d） 每个应用程序的数据数量；
e） 按照条件进行搜索、筛选和标记后的数据数量；
f） 其他按需求进行统计的数据数量。

5.2.9.2 对于提取的移动终端数据进行解析、恢复、关联及去重后的结果数据，设备应支持分开统计。

5.2.10 数据溯源

设备应支持对提取、解析、恢复和关联后的结果数据提供其原始来源分析和展示。

5.2.11 数据展示

5.2.11.1 设备应支持对提取、解析、恢复和关联后的结果数据进行展示，展示方式包括：

a） 通过列表方式展示（如文件列表和数据记录）；
b） 通过对话方式展示（如即时通讯对话记录和短消息收发记录）；
c） 通过缩略图方式展示（如图片和视频文件）；
d） 通过地图方式展示（如地理位置和轨迹信息）；
e） 通过时间线方式展示；
f） 其他易于阅读和查看的展示方式。

5.2.11.2 数据展示的方式应采用与移动终端原始数据一致或相近的分类或分组方式。

5.2.11.3 对于提取的移动终端数据进行解析、恢复和关联后产生的结果数据，设备应支持分开展示。

5.2.12 数据导出

设备应支持对提取、解析、恢复和关联后的结果数据以项目、检材为分类导出数据，导出的方式包括压缩文件和生成特定格式文件等。

5.2.13 数据校验

设备应支持对结果数据计算完整性校验值，算法宜包括国产密码算法。

5.2.14 结果报告

5.2.14.1 结果数据的选择

设备应支持按需求对提取、解析、恢复、关联和去重后的结果数据进行选择，按需求生成结果报告。

5.2.14.2 结果报告的格式

设备应支持按需求格式生成文本型文件的结果报告，并满足以下要求：

a) 文本型文件以 HTML、XML、RTF、TXT、DOC（DOCX）、CSV、PDF 和 ODF 等为通用格式；
b) 结果报告应包含具有原始格式的音频文件、图像文件和视频文件等；
c) 对于非通用格式的音频文件、图像文件和视频文件等，结果报告宜将原始格式转换为通用格式的音频文件、图像文件和视频文件等；音频文件以 WAV 和 MP3 等为通用格式；图像文件以 JPEG（JPG）和 PNG 等为通用格式；视频文件以 MP4、AVI 和 MOV 等为通用格式。

5.2.15 其他功能

设备应支持即时停止或退出操作，操作停止后应不影响设备的正常使用。

5.3 信息安全性

5.3.1 用户管理

设备应具备用户管理功能，应符合以下技术要求：

a) 能建立唯一的用户标识（账号）；
b) 凡需进入系统操作的用户，具备唯一的用户标识（账号）；
c) 明确用户标识的权限，如用户管理员、审计管理员等。

5.3.2 身份鉴别

设备应具备用户的身份鉴别功能，应符合以下技术要求：

a) 在用户执行任何修改或删除项目（如案件和事件）或检材数据的操作前，进行用户身份鉴别；
b) 进入系统时进行用户身份鉴别，鉴别的方式包括但不限于口令、数字证书或生物特征等；
c) 鉴别信息采用加密等方式进行安全保护，如：不以明文形式显示和存储等；
d) 进行用户身份鉴别时，提供反馈信息给被鉴别的用户；用户身份鉴别失败时，提供鉴别失败的处理措施，如失败提示等；
e) 当非法鉴别请求和连接超时等异常状态发生时，具备锁定账号等功能。

5.3.3 审计日志

设备宜支持日志记录审计，应符合以下技术要求：

a) 设备支持用户操作行为（包括操作步骤、操作参数和操作结果等）的记录，并形成审计日志记录，审计日志记录的内容包括但不限于事件发生的日期、时间、类型描述和结果；
b) 确保审计日志记录生成和维护等过程的安全，避免被非法修改、访问和破坏；并仅允许授权管理员访问审计日志；
c) 当审计系统分配的存储空间不足时，提供告警和处理措施。

5.3.4 访问控制

设备应具备用户的访问控制功能，仅允许用户访问授权范围内的项目（如案件和事件）或检材（如移动终端）的数据。

5.3.5 用户数据保护

设备应具备用户数据保护功能，应符合以下技术要求：

a) 设备不应破坏移动终端内的用户数据；
b) 对操作过程中所涉及的原始数据进行完整性校验；
c) 保证用户数据不被非授权查阅或篡改。

5.3.6 升级保护

设备升级应保护原有的鉴定数据和系统原有功能，要求如下：

a) 不应改变设备中原有的鉴定数据；
b) 新增功能不应改变系统原有功能。

5.3.7 报告和导出数据保护

设备宜支持对报告和导出数据进行保护，包括但不限于设置报告文件密码和针对导出数据进行加密。

5.4 可靠性

5.4.1 失效解决和故障排除

设备应提供发生软件失效或故障后的失效方案或故障排除方案。

5.4.2 恢复出厂状态/设置

设备应提供还原到出厂状态/设置的功能。

5.4.3 结果数据一致

对于同一检材，除有特殊情况外（需说明），多次鉴定所获得的结果数据应一致。

5.5 易用性

5.5.1 界面易用性

设备应支持简体中文用户界面，界面设计宜清晰明确，引导用户执行正确的操作。

5.5.2 帮助系统

设备应提供简洁明了的使用指导手册或帮助文档，并提供基本操作的互动指引，包括但不限于：

a) 陈述所有功能以及最终用户能调用的功能的产品说明；
b) 安装和卸载的操作说明；
c) 停止或退出等操作可能产生后果的提示；
d) 用户首次使用系统时基本或简易操作说明；
e) 标识能完成的预期的工作任务和服务所需时长；
f) 防止用户误操作的功能的说明。

5.6 维护性

5.6.1 版本号唯一性

设备的不同版本（包含模块和底层等）应提供唯一的版本标识。

5.6.2 时钟同步

设备应提供与外部标准授时服务器进行时钟同步的功能。

5.6.3 系统升级

设备应支持在线版本查新以及在线和（或）离线方式进行更新或升级，并应符合以下技术要求：

a) 更新或升级前，提示用户确认；
b) 系统的升级信息保存为标准文档，其中包含具体的更新内容以及升级前后的版本号；

c） 升级失败时，不应影响系统使用。

5.6.4 版本兼容性

设备更新或升级后的版本应兼容设备早期版本的数据。

5.7 性能效率

5.7.1 操作响应

设备的单项操作响应时间宜小于30秒，响应时间超过30秒时，系统应有提示。

5.7.2 容量告警

设备应支持对存储空间容量及系统资源占用率进行超阈值告警的功能。

6 测试评价方法

6.1 检材支持的测试评价方法

6.1.1 移动终端支持

移动终端支持的测试方法、预期结果和结果判定如下。

a） 测试方法

1） 审查设备厂商提供的文档，检查设备的移动终端支持能力；

2） 在设备上接入不同操作系统的移动终端（包括 iOS、Android 及其衍生版本、HarmonyOS 操作系统等），检查其是否符合 5.1.1.2 的规定；

3） 检查设备是否符合 5.1.1.3 的规定。

b） 预期结果

设备能满足厂商文档中支持的移动终端的识别、适配和提取。

c） 结果判定

若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.1.2 移动终端衍生数据支持

移动终端衍生数据支持的测试方法、预期结果和结果判定如下。

a） 测试方法

1） 审查设备厂商提供的文档，检查设备的移动终端衍生数据支持能力；

2） 分别在设备上加载移动终端的备份和镜像文件等衍生数据，检查其是否符合 5.1.2.2 的规定。

b） 预期结果

设备能满足厂商文档中支持的移动终端衍生数据的识别和解析。

c） 结果判定

若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.1.3 移动终端 UICC 支持

移动终端UICC支持的测试方法、预期结果和结果判定如下。

a） 测试方法

1） 审查设备厂商提供的文档，检查设备的移动终端 UICC 支持能力；

2） 在设备或附带组件上接入 UICC，检查其是否能准确识别 5.1.3 中规定的相关信息。

b） 预期结果

设备能满足厂商文档中支持的移动终端UICC的识别。

c） 结果判定

若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.1.4 移动终端所包含的可移动存储卡支持

移动终端所包含的可移动存储卡支持的测试方法、预期结果和结果判定如下。

a) 测试方法
   1) 审查设备厂商提供的文档，检查设备的移动终端所包含的可移动存储卡支持能力；
   2) 在设备或附带组件上接入移动终端所包含的可移动存储卡，检查其是否能准确识别 5.1.4 规定的相关信息。
b) 预期结果
   设备能满足厂商文档中支持的移动终端所包含的可移动存储卡的识别。
c) 结果判定
   若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.2 功能性的测试评价方法

6.2.1 信息录入

设备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) 审查设备厂商提供的文档，检查设备的信息录入功能；
   2) 检查设备是否具备 5.2.1 规定的功能。
b) 预期结果
   设备能满足厂商文档中支持的对检材进行信息录入。
c) 结果判定
   若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.2.2 数据提取

移动终端数据提取的测试方法、预期结果和结果判定如下。

a) 测试方法
   1) 审查设备厂商提供的文档，检查设备的移动终端的数据提取功能；
   2) 在设备上接入移动终端，检查其是否具备 5.2.2.1.1 和 5.2.2.1.2 规定的功能；
   3) 检查设备是否具备 5.2.2.1.3 中规定的功能；
   4) 在设备上接入移动终端，检查其是否具备 5.2.2.2 规定的功能；
   5) 在设备上或附带组件上接入 UICC，检查其是否具备 5.2.2.3 规定的功能；
   6) 在设备上或附带组件上接入可移动存储卡，检查其是否具备 5.2.2.4 规定的功能。
b) 预期结果
   设备能满足厂商文档中支持的提取移动终端机身存储的逻辑数据、通过物理提取方式获取移动终端存储镜像、通过照相录像等方式提取移动终端屏幕显示的信息、提取移动终端上的衍生数据、提取移动终端UICC的数据以及提取移动终端可移动存储卡数据。
c) 结果判定
   在样本数据稳定的前提下，通过物理提取方式获取移动终端存储镜像、提取移动终端UICC的数据以及提取移动终端可移动存储卡数据不产生偏差，提取其他数据偏差为样本数据的±5%、通过照相录像等方式提取移动终端屏幕显示的信息能清晰显示为符合，其他情况判定为不符合。

6.2.3 数据解析

移动终端提取数据解析的测试方法、预期结果和结果判定如下。

a) 测试方法
   1) 审查设备厂商提供的文档，检查设备的移动终端数据解析功能；
   2) 在设备上加载已提取的移动终端的系统数据，检查其是否具备 5.2.3.1.1 规定的功能；
   3) 在设备上加载已提取的移动终端应用程序数据，检查其是否具备 5.2.3.1.2 规定的功能；
   4) 检查设备是否具备 5.2.3.2 中规定的功能。
b) 预期结果
   设备能满足厂商文档中支持的解析已提取的移动终端的系统数据、解析已提取的移动终端应用程序数据、解析超大数据量（数据条目大于1000万）数据。

c） 结果判定

在样本数据稳定的前提下，解析数据归类正确，具备解析超大数据量的能力，且解析结果正确为符合，其他情况判定不符合。

6.2.4 数据恢复

移动终端数据恢复的测试方法、预期结果和结果判定如下。

a） 测试方法

1） 审查设备厂商提供的文档，检查设备的移动终端数据恢复功能；

2） 在设备上接入移动终端或已提取的移动终端数据，检查其是否具备 5.2.4 规定的功能。

b） 预期结果

设备能满足厂商文档中支持的恢复移动终端数据。

c） 结果判定

在样本数据稳定的前提下，数据恢复结果数据量偏差为样本数据标准恢复数据量的±10%为符合，其他情况判定不符合。

6.2.5 数据搜索

移动终端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） 审查设备厂商提供的文档，检查设备的数据搜索功能；

2） 检查设备是否具备 5.2.5 规定的功能。

b） 预期结果

设备能满足厂商文档中支持的搜索移动终端数据。

c） 结果判定

若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.2.6 数据关联

移动终端结果数据关联的测试方法、预期结果和结果判定如下。

a） 测试方法

1） 审查设备厂商提供的文档，检查设备的数据关联功能；

2） 检查设备是否具备 5.2.6 规定的功能。

b） 预期结果

设备能满足厂商文档中支持的关联移动终端数据结果数据。

c） 结果判定

若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.2.7 数据标记

移动终端数据的标记的测试方法、预期结果和结果判定如下。

a） 测试方法

1） 审查设备厂商提供的文档，检查设备的数据标记功能；

2） 检查设备是否具备 5.2.7 规定的功能。

b） 预期结果

设备能满足厂商文档中支持的标记特定数据、特定文件，并能注释相关信息。

c） 结果判定

若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.2.8 数据去重

移动终端结果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） 审查设备厂商提供的文档，检查设备的数据去重功能；

2） 检查设备是否具备 5.2.8 规定的功能。

b） 预期结果
设备能满足厂商文档中支持的按需求对提取、解析、恢复和关联后的结果数据进行去重，并能明确展示去重的条件。
c） 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.2.9 数据统计

移动终端数据结果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） 审查设备厂商提供的文档，检查设备的数据统计功能；
2） 检查设备是否具备 5.2.9.1 规定的项目的功能；
3） 检查设备是否符合 5.2.9.2 的规定。
b） 预期结果
1） 设备能满足厂商文档中支持的对提取、解析、恢复、去重后的结果数据进行统计；
2） 设备能满足厂商文档中支持的对于提取的移动终端数据进行解析、恢复、关联及去重后的结果数据进行分开统计。
c） 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.2.10 数据溯源

移动终端结果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） 审查设备厂商提供的文档，检查设备的数据溯源功能；
2） 检查设备是否具备 5.2.10 规定的功能。
b） 预期结果
设备能满足厂商文档中支持的对提取、解析、恢复和关联后的结果数据提供其原始来源展示。
c） 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.2.11 数据展示

移动终端结果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） 审查设备厂商提供的文档，检查设备的数据展示功能；
2） 检查设备是否具备 5.2.11.1 规定的结果展示方式的功能；
3） 检查设备是否符合 5.2.11.2 和 5.2.11.3 的规定。
b） 预期结果
1） 设备能满足厂商文档中支持的展示移动终端结果数据；
2） 设备能满足厂商文档中支持的展示方式采用与移动终端原始数据一致或相近的分类或分组方式；
3） 设备能满足厂商文档中支持的对于提取的移动终端数据进行解析、恢复和关联后产生的结果数据分开展示。
c） 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.2.12 数据导出

移动终端结果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） 审查设备厂商提供的文档，检查设备的数据导出功能；
2） 检查设备是否具备 5.2.12 规定的功能；
3） 检查设备导出数据的方式。

b) 预期结果
1) 设备能满足厂商文档中支持的对提取、解析、恢复和关联后的结果数据以项目、检材为分类导出数据；
2) 设备能满足厂商文档中支持的导出数据的方式（包括压缩文件、生成特定格式文件等）。
c) 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.2.13 数据校验

移动终端结果数据校验的测试方法、预期结果和结果判定如下。
a) 测试方法
1) 审查设备厂商提供的文档，检查设备的数据校验功能；
2) 检查设备是否具备 5.2.13 规定的功能；
3) 检查设备完整性校验算法是否包含国产密码算法。
b) 预期结果
设备能满足厂商文档中支持的计算结果数据的完整性校验值。
c) 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.2.14 结果报告

移动终端结果数据结果报告的测试方法、预期结果和结果判定如下。
a) 测试方法
1) 审查设备厂商提供的文档，检查设备的结果报告功能；
2) 检查设备是否具备 5.2.14.1 规定的生成结果报告的功能；
3) 检查设备是否具备 5.2.14.2 规定的结果报告的格式的功能。
b) 预期结果
1) 设备能满足厂商文档中支持的按需求对提取、解析、恢复、关联和去重后的结果数据进行选择，并按需求生成结果报告；
2) 设备能满足厂商文档中支持的结果报告的格式。
c) 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.2.15 其他功能

设备应符合移动终端数据鉴定设备所必须满足的其他技术要求，其测试方法、预期结果和结果判定如下。
a) 测试方法
检查设备是否符合5.2.15的规定。
b) 预期结果
设备能随时响应停止或退出操作，操作停止后不影响设备的正常使用。
c) 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.3 信息安全性的测试评价方法

6.3.1 用户管理

移动终端鉴定设备用户管理的测试方法、预期结果和结果判定如下。
a) 测试方法
1) 审查设备厂商提供的文档，检查设备的用户管理功能；
2) 检查设备是否符合 5.3.1 的规定。
b) 预期结果
1) 设备能建立唯一的用户标识（账号）；

2) 设备满足进入系统操作的用户具备唯一的用户标识（账号）；
3) 设备明确用户标识的权限，如用户管理员和审计管理员等。

c) 结果判定

若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.3.2 身份鉴别

移动终端鉴定设备身份鉴别的测试方法、预期结果和结果判定如下。

a) 测试方法
1) 审查设备厂商提供的文档，检查设备的身份鉴别功能；
2) 检查设备是否符合 5.3.2 的规定。

b) 预期结果
1) 设备能在用户执行任何修改或删除项目或检材数据的操作前对用户身份进行鉴别；
2) 设备能对进入系统的用户进行用户身份鉴别；
3) 设备能对鉴别信息进行安全保护；
4) 设备能在进行用户身份鉴别时提供反馈信息；在用户身份鉴别失败时提供处理措施；
5) 设备能在出现非法鉴别请求、连接超时等异常状态时锁定账号。

c) 结果判定

若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.3.3 审计日志

移动终端鉴定设备审计日志的测试方法、预期结果和结果判定如下。

a) 测试方法
1) 审查设备厂商提供的文档，检查设备的审计日志功能；
2) 检查设备是否能按照时间顺序，清晰、完整的记录用户操作行为，并检查设备是否符合 5.3.3 的规定。

b) 预期结果
1) 设备能记录用户操作行为（包括操作步骤、操作参数和操作结果等），并形成审计日志记录，其中至少包括事件发生的日期、时间、类型描述和结果等；
2) 设备能确保审计日志记录生成和维护等过程的安全；并仅允许授权管理员访问审计日志；
3) 设备能在审计系统分配的存储空间不足时提供告警和处理措施。

c) 结果判定

若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.3.4 访问控制

移动终端鉴定设备访问控制的测试方法、预期结果和结果判定如下。

a) 测试方法
1) 审查设备厂商提供的文档，检查设备的访问控制功能；
2) 检查设备是否符合 5.3.4 的规定。

b) 预期结果

设备满足仅允许用户访问授权范围内的项目（如案件和事件）或检材（如移动终端）的数据。

c) 结果判定

若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.3.5 用户数据保护

移动终端鉴定设备用户数据保护的测试方法、预期结果和结果判定如下。

a) 测试方法
1) 审查设备厂商提供的文档，检查设备的用户数据保护功能；
2) 检查设备是否符合 5.3.5 的规定。

b) 预期结果
1) 设备能不破坏移动终端内的用户数据；

2） 设备能对操作过程中所涉及的原始数据进行完整性校验；
3） 设备能保证用户数据不被非授权查阅或篡改。

c） 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.3.6 升级保护

移动终端鉴定设备升级保护的测试方法、预期结果和结果判定如下。

a） 测试方法
1） 审查设备厂商提供的文档，检查设备的升级保护功能；
2） 检查设备是否符合 5.3.6 的规定。

b） 预期结果
1） 设备升级能保证不改变设备中原有的鉴定数据；
2） 设备升级满足新增功能不改变系统原有功能。

c） 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.3.7 报告和导出数据保护

移动终端鉴定设备报告和导出数据保护的测试方法、预期结果和结果判定如下。

a） 测试方法
1） 审查设备厂商提供的文档，检查设备的报告和导出数据保护功能；
2） 检查设备是否符合 5.3.7 的规定。

b） 预期结果
设备能对报告和导出数据进行保护。

c） 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.4 可靠性的测试评价方法

6.4.1 失效解决和故障排除

移动终端鉴定设备失效解决和故障排除的测试方法、预期结果和结果判定如下。

a） 测试方法
在设备上对不同功能进行测试，检查发生软件失效或故障后，设备是否符合5.4.1的规定。

b） 预期结果
设备能在发生软件失效或故障后提供失效方案或故障排除方案。

c） 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.4.2 恢复出厂状态/设置

移动终端鉴定设备恢复出厂状态/设置的测试方法、预期结果和结果判定如下。

a） 测试方法
检查设备是否具备5.4.2规定的功能。

b） 预期结果
设备能提供还原到出厂状态/设置的功能。

c） 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.4.3 结果数据一致

移动终端鉴定设备结果数据一致的测试方法、预期结果和结果判定如下。

a） 测试方法
对于同一检材，检查设备是否符合5.4.3的规定。

b) 预期结果
对于同一检材，除有特殊情况外（需说明），设备能保证多次鉴定所获得的结果数据一致。
c) 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.5 易用性的测试评价方法

6.5.1 界面易用性

移动终端鉴定设备界面易用性的测试方法、预期结果和结果判定如下。
a) 测试方法
检查设备用户界面是否符合5.5.1的规定。
b) 预期结果
1) 设备能支持简体中文用户界面，界面设计宜清晰明确；
2) 设备能引导用户执行正确的操作。
c) 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.5.2 帮助系统

移动终端鉴定设备帮助系统的测试方法、预期结果和结果判定如下。
a) 测试方法
1) 检查设备是否具备使用指导手册或帮助文档；
2) 检查设备是否具备 5.5.2 中规定的基本操作的互动指引。
b) 预期结果
设备提供简洁明了的使用指导手册或帮助文档，并提供基本操作进行指引。
c) 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.6 维护性的测试评价方法

6.6.1 版本号唯一性

移动终端鉴定设备版本号唯一性的测试方法、预期结果和结果判定如下。
a) 测试方法
检查设备是否符合5.6.1的规定。
b) 预期结果
设备的不同版本提供唯一的版本标识。
c) 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.6.2 时钟同步

移动终端鉴定设备时钟同步的测试方法、预期结果和结果判定如下。
a) 测试方法
检查设备是否具备5.6.2中规定的功能。
b) 预期结果
设备在在线状态下都能与外部标准授时服务器进行时钟同步。
c) 结果判定
若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.6.3 系统升级

移动终端鉴定设备系统升级的测试方法、预期结果和结果判定如下。
a) 测试方法
1) 审查厂商提供的文档，检查设备的系统升级功能；

2） 检查设备是否符合 5.6.3 的规定。

b） 预期结果

1） 设备能在更新或升级前提示用户确认；

2） 设备能将系统的升级信息保存为标准文档，其中包含具体的更新内容以及升级前后的版本号；

3） 设备能在系统升级失败时，不影响系统使用。

c） 结果判定

若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.6.4 版本兼容性

移动终端鉴定设备版本兼容性的测试方法、预期结果和结果判定如下。

a） 测试方法

1） 在不同版本设备上验证相同移动终端和样本数据，检查设备是否符合 5.6.4 的规定；

2） 检查相同数据更新或升级版本中有效数据的数量是否少于原版本，若少于原版本，是否明确展示原因。

b） 预期结果

设备更新或升级后能兼容早期版本的数据，且除有特殊原因外（需明确展示）数据在新版本中有效数据的数量不少于早期版本。

c） 结果判定

若b）中的预期结果均满足判定为符合，其他情况判定为不符合。

6.7 性能效率的测试评价方法

6.7.1 操作响应

移动终端鉴定设备操作响应的测试方法、预期结果和结果判定如下。

a） 测试方法

在设备上对不同功能进行测试，检查每次单项操作设备的响应时间，并检查设备的操作响应是否符合 5.7.1 的规定。

b） 预期结果

设备对用户单项操作的响应时间不超过 30 秒，响应时间超过 30 秒，系统有提示。

c） 结果判定

响应时间不超过 30 秒，且超过 30 秒时有对当前运行状态的提示判定为符合，其他情况判定为不符合。

6.7.2 容量告警

移动终端鉴定设备容量告警的测试方法、预期结果和结果判定如下。

a） 测试方法

1） 审查设备厂商提供的文档，检查设备的容量告警功能；

2） 检查设备是否具备 5.7.2 中规定的功能，是否会出现存储容量不足等影响使用体验的情况。

b） 预期结果

设备能对存储空间容量及系统资源占用率进行超阈值告警的功能。

c） 结果判定

设备出现任何形式的空间不足、且未进行告警时判定为不符合。

参 考 文 献

[1] GB/T 18894—2016 电子文件归档与电子档案管理规范
[2] 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
[3] GB/T 25069—2022 信息安全技术 术语
[4] GB/T 29361—2023 法庭科学 电子数据文件一致性检验规程
[5] GB/T 29362—2023 法庭科学 电子数据搜索检验规程
[6] GB/T 34975—2017 信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法
[7] GB/T 34976—2017 信息安全技术 移动智能终端操作系统安全技术要求和测试评价方法
[8] GB/T 34977—2017 信息安全技术 移动智能终端数据存储安全技术要求与测试评价方法
[9] GB/T 34979.1—2017 智能终端软件平台测试规范 第1部分：操作系统
[10] GB/T 34979.2—2017 智能终端软件平台测试规范 第2部分：应用与服务
[11] GB/T 34980.1—2017 智能终端软件平台技术要求 第1部分：操作系统
[12] GB/T 34980.2—2017 智能终端软件平台技术要求 第2部分：应用与服务
[13] GB/T 37729—2019 信息技术 智能移动终端应用软件(APP)技术要求
[14] GB/T 39576—2020 具有融合功能的移动终端安全能力测试方法
[15] GB/T 39720—2020 信息安全技术 移动智能终端安全技术要求和测试评价方法
[16] GB/T 39788—2021 系统与软件工程 性能测试方法
[17] GB/T 40856—2021 车载信息交互系统信息安全技术要求及试验方法
[18] GB/T 42107—2022 国家科技重大专项文件归档与档案管理规范
[19] GA/T 754—2008 电子数据存储介质复制工具要求及检测方法
[20] GA/T 755—2008 电子数据存储介质写保护设备要求及检测方法
[21] GA/T 756—2021 法庭科学 电子数据收集提取技术规范
[22] GA/T 976—2012 电子数据法庭科学鉴定通用方法
[23] GA/T 1069—2021 法庭科学 电子物证手机检验技术规范
[24] GA/T 1170—2014 移动终端取证检验方法
[25] GA/T 1568—2019 法庭科学 电子物证检验术语
[26] SF/Z JD0400001—2014 电子数据司法鉴定通用实施规范
[27] YD/T 1080—2018 数字蜂窝移动通信名词术语