ICS 35.240
CCS A92

SF

中华人民共和国司法行政行业标准

SF/T 0157—2023
代替 SF/Z JD0401002—2015

移动终端电子数据鉴定技术规范

Technical specification for electronic data examination of mobile terminal

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。

本文件代替SF/Z JD0401002—2015《手机电子数据提取操作规范》，与SF/Z JD0401002—2015相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了第4章“仪器设备”（见第4章）；
b) 增加了第5章“总体要求”（见第5章）；
c) 将“现场获取”与“实验室检验”合并为“鉴定步骤”，并更改了表述（见第6章，2015年版的第3章和第4章）；
d) 更改了“鉴定结果保存”的内容（见第7章，2015年版的第5章）；
e) 更改了“鉴定记录”的内容（见第8章，2015年版的第6章）；
f) 增加了第9章“鉴定意见”（见第9章）。

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、最高人民检察院检察技术信息研究中心、广西壮族自治区公安厅、河北省公安厅、上海市公安局、大连市公安局、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、厦门市兴百邦科技有限公司。

本文件主要起草人：郭弘、吴松洋、李佳、李岩、孙奕、陈兴文、刘浩阳、韩马剑、阎皓、钱志高、段继平、朱元栋、王海啸、卢启萌、田野、杨恺、李致君、施少培、耿浦洋、刘善军、孙文琦、曾锦华、毛晓、凌嵘、徐志强、崔宇寅、高峰、雷云婷、张颖。

本文件及其所代替文件的历次版本发布情况为：

——2015年首次发布为SF/Z JD0401002—2015；
——本次为第一次修订。

移动终端电子数据鉴定技术规范

1 范围

本文件规定了移动终端电子数据鉴定的总体要求，以及仪器设备、鉴定步骤、鉴定结果保存、鉴定记录和鉴定意见的要求。

本文件适用于司法鉴定领域中对移动终端中电子数据的存在性鉴定、真实性鉴定以及对移动终端中应用程序的功能鉴定。

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 29360 法庭科学 电子数据恢复检验规程

GB/T 35278—2017 信息安全技术 移动终端安全保护技术要求

GB/T 37729 信息技术 智能移动终端应用软件（APP）技术要求

SF/T 0105 存储介质数据镜像技术规程

SF/T 0145 智能移动终端应用程序功能鉴定技术规范

SF/T 0156 电子邮件鉴定技术规范

3 术语、定义和缩略语

3.1 术语和定义

GB/T 35278—2017、GB/T 37729界定的以及下列术语和定义适用于本文件。

3.1.1

移动终端 mobile terminal

在移动通信网络中使用的具有显示屏的手持式移动计算设备。

注：包括手机、平板电脑及其他具有类似功能的终端设备等。

[来源：GB/T 35278—2017，3.1.1，有修改]

3.1.2

可移动存储卡 removable memory card

用于扩展移动终端（3.1.1）物理存储空间的存储介质。

注：包括SD卡、MicroSD卡、多媒体存储卡（MMC）和记忆卡（MS）等。

3.1.3

完整性校验值 integrity check value

使用安全的哈希算法对电子数据进行计算，得出的用于校验数据完整性的数据值。

3.1.4

移动终端安全保护机制 security mechanism in mobile terminal

用于保护移动终端数据所采取的措施。

注：包括数据加密［如基于文件级加密（FBE）、全盘加密（FDE）］和数据保护（如密码、安全问答和生物特征识别）等。

3.1.5

权限提升 privilege escalation

对移动终端（3.1.1）进行获取root权限或越狱等特定操作，实现突破设备制造商、操作系统或用户层面施加的限制，以访问或获取更多的电子数据的技术。

3.1.6

信号屏蔽 signal shielding

利用主动或被动方式将移动终端（3.1.1）与无线通信网络[包括蜂窝无线通信、无线通信技术（Wi-Fi）、蓝牙、近场通信及红外线等]隔离的技术。

3.2 缩略语

ICCID：集成电路卡识别码（Integrate Circuit Card Identity）
IMEI：国际移动设备识别码（International Mobile Equipment Identity）
ISP：在线可编程（In-System Programming）
JTAG：联合测试工作组（Joint Test Action Group）
MSISDN：移动基站国际用户识别码（Mobile Station ISDN）
PIN：个人识别码（Personal Identification Number）
SIM：用户身份模块（Subscriber Identity Module）
UICC：通用集成电路卡（Universal Integrated Circuit Card）

4 仪器设备

4.1 硬件

鉴定所用仪器设备硬件宜包括但不限于：

a) 移动终端电子数据鉴定工作站；
b) UICC 读卡器；
c) 信号屏蔽设备；
d) 照相录像设备；
e) 存储介质只读设备；
f) 存储介质复制设备；
g) 芯片拆焊设备；
h) 芯片数据提取设备。

4.2 软件

鉴定所用仪器设备软件宜包括但不限于：

a) 移动终端检验分析软件；
b) 芯片读取软件；
c) 移动终端互联网数据提取软件；
d) 数据库分析软件；
e) 数据恢复软件；
f) 元数据检验分析软件；
g) 网络数据流获取分析软件；
h) 完整性校验值计算软件；
i) 截屏软件；
j) 屏幕录像软件。

5 总体要求

5.1 结果充分：鉴定结果应覆盖委托要求中的所有相关数据。
5.2 风险控制：对移动终端所进行的任何更改（包括权限提升和联网等）都应进行风险评估，并与委托人确认。对于可能产生风险的操作过程进行录像记录。
5.3 操作可追溯：应及时、客观、全面地记录与鉴定有关的操作，对不可再现情况的录像记录，应确保鉴定过程和结果的可追溯性。
5.4 设备可靠：移动终端鉴定的软硬件设备宜经过检测和验证，并定期进行更新和维护，以确保鉴定结果准确可靠。

6 鉴定步骤

6.1 记录检材情况

6.1.1 应记录移动终端的封存状态。对于处于封存状态移动终端，应对拆封过程进行拍照或录像。

6.1.2 应对移动终端进行唯一性编号。

6.1.3 应对移动终端及其附件进行拍照，附件应包括但不限于：

a) UICC（如SIM卡）；

b) 可移动存储卡。

6.1.4 应记录移动终端的基本信息，基本信息宜包括：

a) 移动终端外观所标识的品牌和型号；

b) 移动终端的唯一性标识（如IMEI）；

c) 移动终端开关机状态；

d) 移动终端网络连接的状态（如飞行模式的开/关状态）；

e) 随移动终端移送的相关账号、密码和SIM卡的PIN码等信息。

6.2 预检和预处理

在进行移动终端电子数据鉴定工作前，应对移动终端及其附件（如UICC和可移动存储卡等）进行检查，并做好鉴定准备工作，应符合以下要求。

a) 对移动终端采取信号屏蔽措施后，检查移动终端的开关机状态，并根据其开关机状态，按照以下方式进行操作：

1) 移动终端处于关机状态：确保移动终端在信号屏蔽的环境中进行开机操作；

2) 移动终端处于开机状态：先判断移动终端是否设置为“飞行模式”，在确保移动终端在开启“飞行模式”并处于信号屏蔽的条件下进行操作。

b) 检查移动终端的外观状态，判断是否存在影响启动和操作的异常状况，如存在，则在确保鉴定人员、鉴定场所安全以及不影响移动终端中电子数据的前提下，做好预处理并记录相关情况。在异常情况被解决后，再进行鉴定工作。

注：影响移动终端启动和操作的异常情况包括黑屏、开裂、扭曲、鼓胀、电池漏液或异常发热等。

c) 检查移动终端的数据接口及电源接口，判断接口类型并准备适用的电源适配设备和数据连接线。如存在数据连接和充电故障，则在不影响移动终端中电子数据的前提下尝试进行故障排除并记录相关情况。在设备故障被解决后，再进行鉴定工作。

d) 检查移动终端得到安全保护机制状态，如移动终端启用了安全保护机制，在确保数据安全的前提下，可采取以下1种或多种措施：

1) 通过已知的账号和密码（如屏幕锁定密码和PIN码）进行验证；

2) 通过提取镜像等方式绕过；

3) 通过绕过安全保护机制等方式进入移动终端系统。

注：移动终端的密码保护和安全保护机制会在移动终端开机等情况下要求输入密码或其他安全验证方式进行验证，或针对移动终端存储介质进行数据加密。

6.3 电子数据提取

6.3.1 移动终端机身数据提取

根据检验目的和要求，对移动终端机身数据的提取可根据情况选择以下一种或多种方式进行。

a) 逻辑提取：利用移动终端的同步协议或备份机制，提取移动终端中指定的文件、目录、分区和移动终端应用程序（APP）的全部或部分数据。

b) 镜像提取：使用移动终端的专用工具（如高通和MTK等）、利用权限提升操作，以及使用JTAG、ISP、硬件调试接口等方式提取逻辑镜像及物理镜像。

c) 芯片提取：拆卸移动设备存储芯片，使用镜像转储等方式提取芯片中的数据。

d) 照相录像提取：通过拍照和录像等方式提取检材移动终端屏幕显示的信息。

6.3.2 UICC数据提取

对于有UICC的移动终端，如需单独对UICC进行数据提取，应在完成移动终端数据提取后，拆卸UICC进行数据提取。UICC中提取的数据宜包括：

a) 网络服务提供商名称；
b) 标识信息，如 ICCID、IMSI 和 MSISDN 等；
c) 短消息；
d) 通讯录；
e) 通话记录。

6.3.3 可移动存储卡数据提取

对于包含可移动存储卡的移动终端，如需单独对可移动存储卡进行数据提取，应在完成移动终端数据提取后，拆卸可移动存储卡，按照SF/T 0105的规定制作镜像并核对其完整性校验值，然后采用只读方式对该镜像进行数据提取。如需进行数据恢复，应按照GB/T 29360的规定对镜像进行数据恢复。

6.3.4 移动终端互联网（云端）数据提取

6.3.4.1 对于存储于互联网的移动终端电子数据，可根据需提取数据的具体情况，选择以下适当方式进行数据提取：

a) 对于通过给定的用户名/密码等鉴权信息进行网络数据提取，可在不使用移动终端的情况下，直接采用远程提取方式提取存储于互联网的电子数据；
b) 对于需要使用移动终端进行联网操作以提取网络数据，应在完成移动终端机身数据提取后，在获得委托人授权的前提下，可使用具备远程数据提取功能的移动终端检验分析软件进行。

6.3.4.2 对于存储于互联网的移动终端电子数据的提取过程，应使用录像或者录屏的方式进行记录，并从可信时间源获取并记录开始时间和结束时间。

6.4 电子数据分析

6.4.1 电子数据存在性分析

移动终端电子数据的存在性分析包括对文件、目录结构以及经过解码、转换和解析后的数据记录、恢复的已删除文件、以碎片化存在的数据以及从数据库等文件中恢复的记录数据进行分析，宜包括但不限于以下内容：

a) 关键字/词；
b) 数据字段和值；
c) 文件或数据属性；
d) 删除状态；
e) 与具体应用相关的内容（如社交好友关系和通联行为等）；
f) 系统信息。

6.4.2 电子数据真实性分析

6.4.2.1 根据检验目的和要求对移动终端中数据的真实性分析，宜包括但不限于以下内容：

a) 对移动终端中短信/即时通讯记录进行检验，分析发送人、接收人、发送/接收时间、内容数据和附件文件等，并对与其相关的短信/即时通讯记录、文件或数据进行检验，分析数据之间的关联性；
b) 对移动终端中照片、录音和视频等多媒体文件进行检验，分析文件的属性、元数据信息和数据库记录等；
c) 对移动终端中临时文件和缩略图等进行检验，分析其与待证实文件之间的关系；
d) 对移动终端中特定结构的数据（如 SQLite 数据库、Plist 属性列表、日志文件、缓存和索引等）进行检验，分析相互之间的关系；
e) 对移动终端中电子邮件进行检验，按照 SF/T 0156 的规定进行。

6.4.2.2 检验过程充分考虑使用移动终端的同步协议、备份机制或权限提升等可能产生的影响。在获得授权的情况下，可使用测试移动终端连接网络、登录应用，同步应用数据后进行内容的比对检验。

6.4.3 应用程序功能分析

对移动终端中的应用程序进行功能分析，根据移动终端的类型，应选择以下适当方式进行分析。

a) 智能移动终端：按照 SF/T 0145 的规定进行分析。
b) 非智能移动终端：启动待鉴定应用程序，逐一运行该应用程序需要鉴定的各项功能并进行记录；若待鉴定应用程序无法正常运行，则停止运行并进行记录。

7 鉴定结果保存

应计算检出数据的完整性校验值，将检出数据采取封盘刻录方式刻录在空白光盘上或者保存在专用存储介质中，并核验光盘或专用存储介质中检出数据的完整性校验值。

8 鉴定记录

鉴定记录宜包括但不限于：

a) 移动终端外观所标识的品牌和型号；
b) 移动终端的唯一性标识（如 IMEI 号）；
c) 移动终端的封存情况；
d) 移动终端的操作系统及版本号；
e) 移动终端 UICC 的数量；
f) 可拆卸存储卡的品牌及容量；
g) 移动终端配件设备（如电源线、数据连接线和其他配件设备）；
h) 随移动终端移送的相关账号、密码、PIN 码等信息；
i) 移动终端开关机状态；
j) 移动终端网络连接的状态（如飞行模式开/关状态）；
k) 鉴定环境状况；
l) 鉴定开始和结束时间；
m) 鉴定过程中所使用的仪器设备信息；
n) 移动终端安全保护机制的状态以及采取的措施；
o) 移动终端互联网电子数据获取过程中的网络环境信息、鉴权信息；
p) 鉴定过程中对检材所做的操作；
q) 鉴定过程中的异常情况（如适用）；
r) 检出数据及其完整性校验值；
s) 鉴定过程录像文件的文件名和完整性校验值（如适用）。

9 鉴定意见

9.1 存在性鉴定意见

移动终端中电子数据存在性鉴定意见应表述为检出、未检出和不具备鉴定条件三种，表述内容应符合以下要求：

a) 检出数据表述至少包含检材编号、检出情况、检出数据（或保存检出数据介质）的完整性校验值和保存检出数据的存储介质编号等信息；
b) 未检出数据表述至少包含检材编号和检验情况；
c) 不具备鉴定条件表述至少包含检材编号和不具备鉴定条件原因。

9.2 真实性鉴定意见

9.2.1 鉴定意见分类

移动终端中电子数据真实性鉴定意见应分为以下四种：

a) 经过伪造/篡改；
b) 未经过伪造/篡改；
c) 未发现伪造/篡改；

d) 无法判断。

9.2.2 鉴定意见判断依据及表述

9.2.2.1 经过伪造/篡改

9.2.2.1.1 判断依据：发现移动终端中数据存在异常，并分析异常为伪造/篡改形成。

9.2.2.1.2 鉴定意见表述为“需检数据[1)]经过伪造/篡改。”

9.2.2.2 未经过伪造/篡改

9.2.2.2.1 判断依据：未发现需检数据存在异常,并分析不存在通过现有技术手段无法发现的伪造/篡改可能性。

9.2.2.2.2 鉴定意见表述为“需检数据未经过伪造/篡改。”

9.2.2.3 未发现伪造/篡改

9.2.2.3.1 判断依据：未发现需检数据存在异常或发现的异常能得到合理解释，但尚不能完全排除存在根据现有技术手段难以发现的伪造/篡改痕迹的可能性。

9.2.2.3.2 鉴定意见表述为“未发现需检数据伪造/篡改。”

9.2.2.4 无法判断

9.2.2.4.1 判断依据：需检数据存在异常，但无法准确判断其性质或形成原因；或需检数据信息量过少，无法形成明确意见。

9.2.2.4.2 鉴定意见表述为“无法判断需检数据是否经过伪造/篡改。”

9.3 功能鉴定意见

9.3.1 鉴定意见分类

移动终端中应用程序功能鉴定意见应分为以下四种：

a) 具有需检功能；
b) 不具有需检功能；
c) 倾向具有需检功能；
d) 无法判断。

9.3 中的“需检功能”可用其等价描述替代。

9.3.2 具有需检功能

9.3.2.1 判断依据：对需检应用程序进行了充分的动态检验分析和静态检验分析，检验结果有充足的依据支持需检功能可以实现。

9.3.2.2 鉴定意见表述为“需检应用程序（版本号）（适用时注明触发条件或限制条件）具有需检功能。”若需检功能与其功能描述存在不符合，可进行补充说明。

9.3.3 不具有需检功能

9.3.3.1 判断依据应满足以下条件之一：

a) 对需检应用程序进行了充分的动态检验分析和静态检验分析，动态检验分析未发现需检功能可以实现，静态检验分析能得出充足依据支撑需检功能不能实现；
b) 需检应用程序不具备动态检验条件，但经过充分的静态检验分析能得出充足依据证明需检功能不能实现。

9.3.3.2 鉴定意见表述为“需检应用程序（版本号）（适用时注明限制条件）不具有需检功能。”

9.3.4 倾向具有需检功能

1) 本文件中的“需检数据”可用其等价描述替代，如需检短信、需检即时通讯记录和需检电子邮件等。

9.3.4.1　判断依据：需检应用程序不具备动态检验条件或动态检验分析未发现需检功能，但通过静态检验分析发现实现需检功能的代码。应说明需检应用程序不具备动态检验条件或动态检验未发现需检功能，并列出其功能代码的静态分析结果。

9.3.4.2　鉴定意见表述为“倾向认为需检应用程序（版本号）（适用时注明触发条件或限制条件）具有需检功能。”

9.3.5　无法判断

9.3.5.1　判断依据：在进行了充分的检验和分析后仍无法得到足够的依据。

9.3.6　鉴定意见表述为“无法判断需检应用程序（版本号）是否具有需检功能。”

参 考 文 献

[1] GB/T 29361—2023 法庭科学 电子数据文件一致性检验规程
[2] GB/T 29362—2023 法庭科学 电子数据搜索检验规程
[3] GA/T 754—2008 电子数据存储介质复制工具要求及检测方法
[4] GA/T 755—2008 电子数据存储介质写保护设备要求及检测方法
[5] GA/T 756—2021 法庭科学 电子数据收集提取技术规范
[6] GA/T 976—2012 电子数据法庭科学鉴定通用方法
[7] GA/T 1069—2021 法庭科学 电子物证手机检验技术规范
[8] GA/T 1170—2014 移动终端取证检验方法
[9] GA/T 1568—2019 法庭科学 电子物证检验术语
[10] SF/Z JD0400001—2014 电子数据司法鉴定通用实施规范
[11] YD/T 1080—2018 数字蜂窝移动通信名词术语
[12] ISO 21043—1:2018,Forensic sciences—Part 1:Terms and definitions
[13] ISO 21043—2:2018,Forensic sciences—Part 2:Recognition, recording collecting, transport and storage of items
[14] ISO/IEC 27037:2012,Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence
[15] ISO/IEC 30121,Information technology—Governance of digital forensic risk framework
[16] CWA 17865:2022, Requirements and Guidelines for a complete end-to-end mobile forensic investigation chain
[17] INTERPOL.(2021). Guidelines for digital Forensics—First responders—Best practices for search and seizure of electronic and digital evidence