ICS 07.140
CCS A92

SF

中华人民共和国司法行政行业标准

SF/T 0145—2023

智能移动终端应用程序功能鉴定技术规范

Technical specification for functionality analysis of smart mobile application

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、国家信息中心、国家工业信息安全发展研究中心、西安邮电大学、公安部第三研究所、广西壮族自治区公安厅、重庆市公安局、江苏省公安厅、大连市公安局、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。

本文件主要起草人：李岩、郭弘、李佳、王笑强、孙奕、刘浩阳、陈兴文、潘妍、高梓铭、韦同胜、吴松洋、田庆宜、李峰、文静、刘善军、孙文琦、卢启萌、耿浦洋、曾锦华、田野、杨恺、李致君、毛晓、凌嵘、刘海飞。

智能移动终端应用程序功能鉴定技术规范

1 范围

本文件规定了智能移动终端应用程序[以下简称“应用程序”（APP）]功能鉴定中使用的仪器设备、鉴定原则、鉴定步骤、鉴定记录以及鉴定意见的要求。

本文件适用于司法鉴定领域中智能移动终端APP的功能鉴定，对搭载智能移动终端同类操作系统的电子设备上的APP功能鉴定参照使用。

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。

SF/T 0105 存储介质数据镜像技术规程

SF/T 0157 移动终端电子数据鉴定技术规范

3 术语和定义

SF/T 0157界定的以及下列术语和定义适用于本文件。

3.1

反编译 decompile

将智能移动终端应用程序还原成汇编语言代码或高级语言代码的过程。

3.2

静态检验分析 static analysis

在智能移动终端应用程序没有运行的情况下对其代码和数据进行的检验分析过程。

3.3

动态检验分析 dynamic analysis

在智能移动终端应用程序运行状态下对其代码、数据和行为进行的检验分析过程。

3.4

加壳 packing

使用加密、隐藏和混淆等技术保护智能移动终端应用程序的代码、数据和资源，防止智能移动终端应用程序被修改或二次分发的技术手段。

3.5

脱壳 unpacking

绕过或者解除保护，获得加壳（3.4）智能移动终端应用程序代码文件的技术手段。

4 仪器设备

4.1 硬件

APP功能鉴定所用的硬件设备宜包括但不限于：

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) 数据连接线及转接口；
e) 实验用智能移动终端；
f) 网络设备（无线路由器等）；
g) 数码照相机/物证翻拍仪；

h) 数码摄像机。

4.2 软件

APP功能鉴定所用的软件工具宜包括但不限于：

a) 移动终端检验分析系统；
b) APP 功能分析工具；
c) 加壳检测工具；
d) 脱壳工具；
e) 逆向分析工具；
f) 程序开发工具；
g) 系统监控工具；
h) 移动终端操作系统仿真工具/移动终端模拟器；
i) 内存数据获取和分析工具；
j) 网络数据流捕获和分析工具；
k) 完整性校验值计算工具；
l) 屏幕录像工具；
m) 软件测试工具。

5 鉴定原则

5.1 全面原则：鉴定过程尽可能覆盖委托鉴定事项中需检功能的所有相关功能点或子功能。

5.2 兼顾原则：鉴定过程兼顾动态检验分析和静态检验分析，鉴定意见的依据以动态检验分析为主，静态检验分析为辅。

5.3 可重复原则：鉴定过程确保在原环境或原环境相近环境下的可重复性；对于其中不能重复的环节，以录像形式记录。

5.4 可追溯原则：完整、准确、全面地记录与鉴定过程相关的信息，以保证鉴定结果的可追溯性。

5.5 及时性原则：鉴定过程中及时固定和提取时效性电子数据，防止数据发生变化或灭失。

6 鉴定步骤

6.1 明确要求

6.1.1 在鉴定委托的受理阶段，应与委托人沟通明确以下内容并留存记录：

a) 基本案情及需通过鉴定解决的技术问题；
b) 需检 APP 的名称、来源及版本；
c) 需检 APP 的载体或获取方式；
d) 需检功能的清晰描述（可通过开发文档、技术报告等形式体现），包括其触发条件等；
e) 需检 APP 的特定运行环境（适用时）；
f) 需检 APP 的开发、编译环境（适用时）；
g) 需检 APP 运行时所需的身份认证信息（适用时）。

6.1.2 委托鉴定事项应清晰、无歧义、可操作。

示例：在“红包助手”APP（版本：2.1）后台运行状态下，是否具有抢微信红包的功能。

6.2 固定提取和编译

6.2.1 实物检材

对于实物检材，按照以下流程固定提取：

a) 对检材进行唯一性编号后拍照；
b) 若检材为具备存储介质镜像条件的存储介质或电子设备，应按照 SF/T 0105 的规定制作并留存镜像文件；

c) 若检材为不具备存储介质镜像条件存储介质或电子设备，可直接对其中的需检 APP 的安装包、代码及相关数据进行提取，提取过程宜以录像形式记录；
d) 若检材为智能移动终端，提取过程应符合 SF/T 0157 的规定；
e) 若需检 APP 位于移动终端模拟器等环境中，则对其进一步解析后提取。

6.2.2 网络检材

位于网络上的检材，按照以下流程固定提取：
a) 应启动屏幕录像工具，或使用数码摄像机拍摄屏幕显示内容；
b) 应从可信的时间源获取并记录开始时间；
c) 应从 6.1.1 确定的来源下载或远程提取需检 APP、代码或其他相关数据，若来源为网络链接或二维码链接，宜记录链接跳转或重定向过程；
d) 应按照 6.2.4 的规定处理结果数据并进行检验记录；
e) 应再次从可信的时间源获取并记录结束时间，结束屏幕录像或摄像机拍摄。

6.2.3 编译

6.2.3.1 若需检 APP 需要通过编译源代码获得，应对编译过程进行全程录像，并记录编译参数及使用的库文件等。
6.2.3.2 若编译过程修改了源代码或配置文件，应记录修改内容和修改理由。

6.2.4 固定提取结果

6.2.4.1 对于 APP 安装包，应记录来源、安装包文件名和版本号（如有）。
6.2.4.2 无法获得独立安装包时，应使用屏幕录像工具记录下载安装过程。
6.2.4.3 对于 APP 源代码，应保留目录结构生成压缩包。
6.2.4.4 应计算固定提取得到的每个文件及录像文件的完整性校验值，并生成列表作为记录留存。

6.3 方法选择

6.3.1 应根据委托鉴定事项从 6.3.2 列出的方法中选择一种或多种，按照 6.4 的规定准备检验分析环境，然后根据方法内容选择 6.5 和 6.6 中对应的项目进行检验，并记录检验过程使用的工具、检验项目、检验步骤和检验发现。
6.3.2 可供选择的方法如下：
a) 测试并记录需检功能的执行过程和结果；
b) 提取需检 APP 基本信息、资源文件或源代码中的关键信息；
c) 通过源代码分析需检功能的实现流程；
d) 修改需检功能的源代码或配置文件后执行，对比执行结果的差异；
e) 通过改变外部运行环境，测试需检功能在特定状态或特定时间的执行结果；
f) 通过断点、应用层钩子等技术获得需检功能执行过程数据。

6.4 环境准备

6.4.1 应根据 6.3 所选用的方法搭建相应的检验分析环境，该检验分析环境应符合需检 APP 的软硬件兼容性要求。
6.4.2 进行静态检验分析前，应在电子数据鉴定专用计算机中根据委托鉴定事项选择安装适当的程序开发工具、加壳检测工具、脱壳工具或程序逆向分析工具等软件。
6.4.3 进行动态检验分析前，应在电子数据鉴定专用计算机或实验用智能移动终端、移动终端模拟器中根据委托鉴定事项选择安装系统监控工具、内存数据获取和分析工具、网络数据流捕获和分析工具等软件。分析环境宜与需检 APP 原有运行环境相近，可使用系统初始化等方式避免其中安装的其他 APP 对需检 APP 造成干扰。
6.4.4 应避免检验分析环境中的安全防护软件对需检 APP 造成影响。
6.4.5 检验环境准备的过程及检验环境中对检验结果有直接影响的软硬件配置应详细记录。

6.5 静态检验分析项目

6.5.1 基本信息检验

应根据委托鉴定事项，选择以下一项或多项内容进行检验：

a) APP 名称、图标和包名；
b) APP 使用情况；
c) 证书信息；
d) 安装包文件名、大小和校验值；
e) 版本信息；
f) 开发者及 APP 数字签名信息；
g) 集成的软件开发工具包（SDK）名称、版本、提供商和用户标识；
h) 申请权限列表。

6.5.2 脱壳和反编译

6.5.2.1 对于采用加壳等方式保护的 APP，可使用加壳检测工具进行检测并记录壳信息，并使用对应的脱壳工具进行脱壳，宜记录使用的脱壳工具版本和操作步骤。

6.5.2.2 可使用逆向分析工具获取 APP 的字节码文件，并将字节码文件反编译为代码文件。

6.5.3 资源文件检验

对APP安装包进行解包和释放后，可分析APP中所包含的资源索引、配置文件以及对应的资源文件。

6.5.4 代码检验分析

对于送检的APP源代码或通过反编译得到的APP源代码，可通过语法分析、语言结构分析和数据流分析等技术，检验APP的数据结构和需检功能的逻辑实现流程。若代码中存在注释，应分析其中的关键信息。

6.5.5 用户数据检验

可收集用户数据区域下属于需检APP的文件和数据并进行检验和分析。

6.5.6 日志检验

可收集并分析由APP或操作系统产生的日志文件。

6.6 动态检验分析项目

6.6.1 基本信息检验

检验内容宜包括但不限于：

a) APP 运行需检功能的界面内容；
b) APP 运行需检功能时的输入输出；
c) APP 在安装、运行和卸载等过程中表现出的可安装性和可执行性；
d) APP 运行过程中的各类权限请求；
e) APP 运行过程中反映出的异常情况。

6.6.2 内存分析

可获取智能移动终端（或仿真环境）的运行内存，分析需检APP相关数据的生成、变化和释放情况。

6.6.3 数据操作分析

可通过相应的数据记录分析APP对系统和用户数据的创建、访问、修改和删除等行为。

6.6.4 网络行为分析

可捕获APP在安装、运行和卸载等过程中所发送和接收的网络通讯数据流，分析其传输协议、访问地址、时间和内容等信息。

6.6.5 动态调试

可使用断点和应用层钩子等技术对特定函数进行监控，对APP运行后的情况进行观察分析。必要时可用权限提升的方式进行。

6.6.6 运行结果数据检验

可收集APP运行过程中产生的数据（如用户数据和日志等），并分析与需检功能的关联性。

6.7 综合分析

应对检验过程中发现的情况和输出数据，针对委托鉴定事项进行逐项分析，以提供鉴定意见所需的支撑依据。

7 鉴定意见

7.1 鉴定意见分类

APP功能鉴定的鉴定意见应在以下4类中选择：

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。

7.2～7.5 鉴定意见表述中的“需检 APP”和“需检功能”可用其等价表述替代。

7.2 具有需检功能

7.2.1 判断依据：经过充分的动态检验分析和静态检验分析，检验结果有充足依据支持需检功能可以实现。

7.2.2 鉴定意见宜表述为“需检 APP（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，可予以补充说明。”

7.3 不具有需检功能

7.3.1 判断依据应满足以下条件之一：

a) 经过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 APP 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。

7.3.2 鉴定意见宜表述为“需检 APP（版本号）（适用时注明限制条件）不具有需检功能。”

7.4 倾向具有需检功能

7.4.1 判断依据：需检 APP 不具备动态检验条件或动态检验分析未发现需检功能，但经过静态检验分析发现实现需检功能的代码。应说明需检 APP 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。

7.4.2 鉴定意见宜表述为“倾向认为需检 APP（版本号）（适用时注明触发条件或限制条件）具有需检功能。”

7.5 无法判断

7.5.1 判断依据：经过充分的检验分析后仍无法得出充足依据。

7.5.2 鉴定意见宜表述为“无法判断需检 APP（版本号）是否具有需检功能。”

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] GA/T 756—2021 法庭科学电子数据收集提取技术规范
[3] GA/T 757—2008 程序功能检验方法
[4] GA/T 828—2009 电子物证软件功能检验技术规范
[5] GA/T 1571—2019 法庭科学 Android系统应用程序功能检验方法
[6] GA/T 1713—2020 法庭科学 破坏性程序检验技术方法
[7] SF/Z JD0400001—2014 电子数据司法鉴定通用实施规范
[8] SF/Z JD0403002—2015 破坏性程序检验操作规范
[9] SF/Z JD0403004—2018 软件功能鉴定技术规范