文章编号：2095-2163(2023)10-0035-05 中图分类号：DF793.2 文献标志码：A

手机取证工具调研及质量评价

仲利静，田雪梅，龙 源，廖才轶，刘 静，刘浩田，卢 亮，马纪强，朱士元
（公安部鉴定中心，北京 100038）

摘 要：使用手机取证工具对手机数据进行提取和分析，通过手机数据获得破案线索、固定犯罪证据，已经成为案件侦办的重要手段。本文对国内市场上主流产品按照不同种类进行调研归纳，详细分析对比了国内手机取证技术及工具的主要特点、优势与应用情况，立足于案件一线应用，给出手机数据取证工具目前需应对的挑战与未来的研究重点，并对其质量评价存在的难点提出思考。

关键词：手机取证工具；云取证；手机解锁；数据分析；反诈

Survey and guality evaluation of mobile forensic tools

ZHONG Lijing, TIAN Xuemei, LONG Yuan, LIAO Caiyi, LIU Jing, LIU Haotian, LU Liang, MA Jiqiang, ZHU Shiyuan
(Institute of Forensic Science of China, Beijing 100038, China)

【Abstract】 Using mobile phone forensics tools to extract and analyze mobile phone data and obtain clues and fixed criminal evidence with mobile phone data has become an important means of case investigation. This paper investigates and summarizes the mainstream products in the domestic market according to different types, analyzes and compares the main characteristics, advantages and applications of domestic mobile phone forensics technologies and tools in detail based on the application of the front-line cases. This paper demonstrates the challenges that mobile phone data forensics tools need to deal with at present and the future research focus, and puts forward considerations on the difficulties in its quality evaluation.

【Key words】 mobile phone forensics tools; cloud forensics; mobile phone unlocking; data analysis; anti-fraud

0 引 言

随着社会经济和信息技术的快速发展，手机中存储的数据呈爆炸性增长，涉及到使用者的衣食住行等各个方面，可记录使用者的日常行为、通联对象、运动轨迹等信息[1]。因此，对于手机数据的提取和分析，在实战中发挥着越来越重要的作用，已经成为案件侦办的重要手段。手机取证工具可针对手机、sim 卡、SD 卡、手机备份文件、手机镜像等检材进行取证、分析、导出报告，并可绕过、破解手机屏幕锁、应用锁，恢复删除数据。本文对国内不同类型手机取证工具进行了调研分析，提出手机取证工具存在的问题及面对的挑战，并对国内外产品质量评价进行了探讨。

1 手机取证工具现状及需解决的问题

目前国内外研发了多种产品化的手机取证工具，如国外 Cellebrite 的 UFED、Susteen 的 SecureView、Oxgen 的 Oxgen Forensic Suite、Micro Systemation 的 XRY 等等。其中，Cellebrite 公司的 UFED Touch [2]，支持获取手机物理镜像、逻辑和文件系统；支持对 iOS 系统的用户密码获取；支持对 BlackBerry®操作系统的解密和解析以及山寨机数据提取。美国 Susteen 公司的 SecureView4 手机取证包[3]，可支持上千种手机，支持物理提取和逻辑提取，支持时间轴、关联图、活动统计图和网络行为等数据分析。国内手机取证工具按照功能和提取检材对象的不同，大致分为以下类型：反诈手机快速取证工具、手机解锁取证工具、云取证工具、手机数据恢复工具、手机数据分析工具、手机综合取证工具等。

由于厂家技术优势不同，手机数据恢复工具、解锁工具及数据分析工具、云取证等不仅可作为内嵌功能模块组合成产品，也可作为单独产品。而随着各手机厂商对手机数据安全保护机制的优化、应用

基金项目：中央级公益性科研院所基本科研业务费专项基金(2019JB008)。

作者简介：仲利静(1986-)，女，硕士，助理研究员，主要研究方向：刑事技术产品质量监督检验。

收稿日期：2022-10-10

程序的升级及新设备以及新环境的快速发展,手机取证面临新的挑战。如:密码锁/屏幕锁机制越发复杂、删除数据恢复率低、小众 APP 取证难、云取证能力不足等问题急需解决。受各种因素所限,本文仅对国内主流手机取证工具进行调研分析,见表 1。

表 1 国内产品调研分类

Tab. 1 Categories of domestic product

序号	产品种类	代表性产品
1	反诈手机快速取证工具	DC-4275 反诈卫士手机特定信息采集系统(厦门市美亚柏科信息股份有限公司)、DC-4215 反诈卫士手机信息精准快速采集系统(厦门市美亚柏科信息股份有限公司)网勘通 ES-90 Pro(广州市高奈特网络科技有限公司)、平航手机数据定向采集软件 PC502(杭州平航科技有限公司)、盘古石星驰快速提取系统 V2.0(网神信息技术(北京)股份有限公司)、新型涉网案件自助举证终端 ES-701(北京海鑫科金高科技股份有限公司)、新型案件勘验取证系统 RC-931(辽宁瑞思科技有限公司)、新型涉网案件全过程智能采集研判系统 YY-E.NET-01(陕西英苑信息技术有限公司)等
2	手机锁屏密码解锁/提权工具	平航手机镜像软件 PH-ExtractorS(杭州平航科技有限公司)、手机多路解锁取证系统 RH-5820(大连睿海信息科技有限公司)等
3	云取证工具	平航 PF5100V3.17(杭州平航科技有限公司)、美亚 DC-5500 手机云勘大师(厦门市美亚柏科信息股份有限公司)、云端数据取证宝 RH-8301(大连睿海信息科技有限公司)、盘古石手机云取证系统 V2.0(网神信息技术(北京)股份有限公司)等
4	手机应用程序逆向分析工具	PM210 应用逆向取证工作站(杭州平航科技有限公司)、DC-6100 魔剑应用程序检测大师系统(厦门市美亚柏科信息股份有限公司)、手机 APK 逆向取证系统 RH-3602(大连睿海信息科技有限公司)、新型涉网案件智勘联侦分析系统掠影者 ES-30(广州市高奈特网络科技有限公司)等。
5	手机数据提取、解析及恢复综合取证工具	108 全采通系列产品(广州市高奈特网络科技有限公司)、手机数据全向取证系统、RH-8800(大连睿海信息科技有限公司)、FL-901 手机取证塔系统.V4、FL-3000 手机取证航母系统(厦门市美亚柏科信息股份有限公司)、PF5200 V1.2(杭州平航科技有限公司)等
6	数据分析平台	人像案情分析系统 RH-8400(大连睿海信息科技有限公司)、美亚 FS-7700 画像大师电子数据研判分析系统(厦门市美亚柏科信息股份有限公司)、云眼多网大数据应用平台(广州市高奈特网络科技有限公司)、盘古石星图多维数据分析系统 V2.0(网神信息技术(北京)股份有限公司)等

1.1 反诈手机快速取证工具

该类产品主要用于对智能手机中指定数据进行快速采集,可解决基层采集受害人手机速度慢、操作繁琐、隐私保护不足的问题。针对目前电信网络诈骗高发,证据线索获取难度大的现状[4],可从受害人手机入手,实现诈骗人相关信息的快速提取,并可将数据一键上传后台进行汇聚和分析挖掘。为后台的综合分析研判提供大量标准化数据。

产品特点如下:

(1)操作简便:向导式操作,适合现场基层民警使用;

(2)提取全面:可获取物证中的短信、联系人、通讯录、聊天记录、照片、语音、图片、视频等数据,支持录屏、截屏方式提取数据;

(3)多种提取方式:APP 解析支持二维码、直连等多种方式提取涉诈 APK、IPA 信息,并进行快速静动态解析;

(4)隐私保护:可实现“非接触式采集”,由被采集人选择被采集数据,保护隐私;

(5)可通过选配高拍仪实现拍照固定证据,并可通过 OCR 识别功能录入手机检材、证件及支付凭证等信息,支持电子签名;

(6)可生成标准数据包和证据固定清单。

此类产品虽然提取速度快、操作简单,但相应提取数据的全面性不如实验室设备,且提取速度依赖网络环境。产品在 OCR 识别录入信息正确率方面,差别较大。

电诈案件发展至今,诈骗通联已由 QQ、微信等传统通联工具引流转移到短视频社交平台、小众通联 APP 上,此类应用程序种类繁多,大多仅支持截屏、录屏方式提取固定数据,面临提取结构化数据难的困境。目前,APP 存活时间短、变异快、防护高等问题,整体表现出新型引流 APP 勘查效率低、无法提取结构化数据,涉诈 APP 难以分析出真实服务器

等问题。因此，应加强除支付宝、微信、QQ 以外的应用程序数据提取能力。

1.2　手机锁屏密码解锁/提权

手机中的聊天、行程、支付等应用可为案件突破带来关键性线索，进行手机解锁及提权获取手机取证权限，对取证有重要意义。此类产品内置多种解锁及物理/逻辑镜像提取技术，具备手机解锁、提权及机身数据无损镜像提取固定功能[5]，同时配合专业化的取证工作站，可以实现多部手机同时提取固定的多任务工作。

目前，厂家破解密码类型主要针对数字密码，小米、三星、vivo 等部分型号可以支持任意密码移除，而华为鸿蒙 2.0 以上、OPPO 较新型号、三星高通芯片组系列、安卓 11 及以上系统版本的手机破解难度较大。安卓手机利用取证工具进行的提权操作，提权后的安卓手机可获取较完整的逻辑镜像，有利于最大程度获取和恢复手机数据。由于安卓高版本系统全盘加密原因，且目前主流高通芯片组在常规情况下破解密码难度较大，利用取证软件工具可实现部分破解，新型号和系统版本可能需要拆机拆芯片等操作，因此需要送检取证实验室进行破解[6]。安卓 8 以后，手机芯片全盘加密以及安卓系统的安全性不断提升，镜像数据提取越来越困难，不同品牌型号和系统版本的手机提权技术不同，产品普适性较差。iPhone 手机可以利用临时越狱等技术实现对解除屏幕锁的手机进行提权，以达到提取常规备份无法获取的数据。

此类产品解锁/提权难度越来越大，迭代后的手机解锁/提权成功率低，避开密码锁和设备锁的手机取证方式及更新加密技术，研究各种芯片取证技术将是取证工具的发展趋势。

1.3　云取证工具

该类产品能够将手机 APP 云端的数据下载，固定到本地设备。通过云端备份数据固定解析，获取通讯录、备忘录、图库、云盘等数据；其中包含支付类、银行类、交通旅行、社交类、购物类、邮件类等，覆盖“衣食住行游购娱”等各个方面。可实现云端数据提取，支持获取手机厂商云备份数据，其中包括华为、vivo、OPPO、小米等主流手机厂商的产品。

由于电子数据规模大，异构数据的混合存储，大量结构化、半结构化、非结构化的数据同时存储在云服务端，增大了取证和分析难度[7]。另外，在云计算平台下篡改和删除的数据难以恢复。云服务提供商为保护用户和数据隐私，会将用户删除数据及相关的元数据完全删除，为云取证带来挑战。目前产品差异较大，部分产品在未登录 APP 的情况下无法提取云端数据，因此应加强研究云环境中的电子证据固定保全、海量取证数据分析技术。

1.4　手机应用程序逆向分析工具

该类产品可在检测手机或模拟器上完成动静态行为检测，是一种对 APP 后台网络行为进行实时分析的工具。可通过多种逆向分析方法对涉诈 APP 进行取证分析[8]，主要包括 Android、iOS 应用安装包静态逆向分析、基于模拟器的动态逆向分析及基于真实手机的动态逆向分析技术、URL/IP 数据分析等。目前，Android、iOS 应用安装包静态逆向分析（APK、IPA 文件）技术较为成熟，可获取应用名称、版本、包名、清单文件、权限、签名证书、应用加固类型等信息；动态逆向分析内容主要涵盖涉案 APP 与远程服务器的网络交互数据，以及应用程序的行为功能代码审计，其中包括权限读取、文件读写、进程通信等数据。URL/IP 数据分析是手机应用程序逆向分析的衍生取证技术，应用程序关联远程服务器，对关联的 URL/IP 进行取证分析，可获取 APP 的关键行为数据，如嫌疑手机号、邮箱、嫌疑后台主服务器、第三方可调证信息等。

由于涉诈 APP 往往具有下载不正规、存活时间短、经常更换 APP 名称或更换 APP 外壳、使用各种防护措施隐藏真实服务器地址，以及更新迭代快、种类繁多等特点，因此需掌握案件中常见的数十种有加密加固等技术防护的 APP 应用原理，实现解密还原，抽取源代码中涉及的手机号、邮箱、URL、IP 等可疑线索。随着涉案 APP 防护能力不断提升，模拟器检测、root 检测、防抓包等反取证技术也不断涌现，需要继续探索真机动态逆向分析技术，提高取证工具的普适性。

1.5　手机综合取证工具

该类产品支持可支持批量手机并行取证，可提供手机取证、手机云数据取证、手机解锁、数据分析等一站式服务。集手机屏幕解锁、镜像下载、手机数据和手机云数据提取、删除恢复、数据浏览、智能分析、生成报告等功能于一体，可多案件多路手机并行取证，提取数据全面、效率高。

由于产品集数据提取、解析、恢复、分析、导出报告于一体，因此存在部分产品功能全而不精，嵌入功能模块取证能力参差不齐，以及数据恢复功能受手机数据提取方法、是否结构化数据恢复、是否恢复出厂设置、机主使用习惯、数据是否为云数据类型等影

响,存在数据恢复难的问题。目前案件涉及的小众社交软件,如存在有端对端加密、阅后即焚等功能的软件,数据提取和解析难度较大[9]。

1.6 数据分析平台

该类产品支持电子数据深入挖掘和可视化智能分析、智能研判等功能[10],集人像刻画、时序分析、经济分析、行为特征、活动轨迹、社会关系分析、涉案预警、可视化数据统计为一体,可对数据内容进行系统性的整理,通过关联分析、对比碰撞,以图形及表格、关系网形式分类展示,形成直观的可视化图谱,可为一线用户取证和研判分析时,扩展线索和提供研判情报。

产品支持与大数据平台联动,可对分析对象进行人物刻画。可多部检材进行数据分析、关联,联动大数据平台查实身份、社会关系,达到扩展线索和深入研判的目的。该类产品需要及时对各个厂商提取数据包兼容,但在数据挖掘、分析模型建立、界面设计、操作便捷性上差别较大,部分产品存在分析模型过于简单、数据挖掘不深、操作复杂等问题,需要进一步改进。

2 手机取证工具质量评价

在国内外相关文献中,已有文献研究手机取证工具质量评价。如范红等[11-12]提出了建立数据取证设备一致性评价标准体系,对产品的工作环境、存储环境、信号屏蔽、一机两用等硬件参数评价;对终端设备的文件信息、各类软件中的应用信息、用户信息、数据恢复能力等数据提取功能评价,以及对各种软硬件平台的支持率、数据提取速度等性能方面的评价。美国国家标准和技术研究所(NIST)[13-17]建立了数据取证设备的技术标准、检测流程、检测规范及检测用例等标准,如智能手机工具规范、移动电话法医取证指南、数据采集工具测试规范(2004)等。(NIST)“移动设备取证工具测试”项目是计算机取证工具测试(CFTT)[18-20]项目的延伸。可为用户更好的选择、获取和使用取证工具及更全面的理解所感兴趣的工具各方面能力提供了必要的信息,也为制造商改进取证工具提供参考。NIST 开发了取证参考数据集(CFReDS)[21-22],给研究者提供了模拟数字证据集。CFReDS 站点是一个镜像库,可将数据内容文档化。调查人员可以通过多种方式使用 CFReDS,包括验证软件工具、设备检查、培训调查人员、实验室认证人员能力测试。CFReDS 从手机品牌型号上此镜像库包含 Ellipsis 8、HTC 10、Samsung、LG、Apple、Motorola 6 种品牌部分手机型号数据集。但随着手机芯片的加密及操作系统的升级,利用镜像文件对手机取证工具进行评价适用性受限,近年 NIST 也开始用实体手机制备数据,对手机取证工具取证能力进行验证。印度 Veermata Jijabai 技术学院[23]基于预定的参数,采用跨设备和测试驱动的方法对各种商业和开源移动设备取证工具进行比较分析;艾哈迈德·达赫兰大学[24]介绍了移动取证工具能力的研究和技术,对基于 LINE 分析的数字证据进行了评价,并验证了 3 种取证工具 WA Key/DB Extractor、Oxygen Forensics 和 Magnet AXIOM 对三星 Galaxy S4 和三星 A3 上的 WhatsApp (WA)应用的数据取证能力[25]。以上文献所涉及的检测用例较少,且手机品牌、数据类型较少,尤其是缺少 QQ、微信、支付宝、淘宝、抖音等国内常用 APP 数据,未涉及云取证等新取证方式,未涉及应用程序逆向分析功能、手机分析功能等。

目前国内常见产品功能、性能也存在差异性,在界面友好性、操作便捷性、取证能力方面存在差异,部分产品存在可提取应用程序种类较少、数据漏提取率高、解析失败率高、数据恢复率低、数据分析模型简单等问题。用于质量评价的测试手机所包含应用程序种类不足、所存数据量小,则不能有效评价产品质量。因此,可通过不同厂家型号和同厂家不同型号产品对比研究,确定影响手机取证工具质量的关键性功能,并确定影响各个功能模块质量的关键性技术指标,得出更系统科学的数据结果来指导检验检测方法建立。产品检测用手机样机、标准数据的制备、更新及日常管理,对于手机取证能力及产品质量科学评价尤为重要,需建立完善的样本制备及管理程序。目前手机实体样机、标准数据制备存在的难点主要有以下几方面:

(1)手机涉及品牌种类、芯片类型、操作系统类型及版本较多,文件系统结构、数据存储方式不同,样本需合理设计、选择;

(2)手机更新换代较快,手机样本需要不断更新,经济成本高;

(3)手机为电子产品,易损坏,需注意日常维护及管理;

(4)应用程序种类繁多(涉及上百种)且版本更新比较快,需及时更新数据并记录。

3 结束语

本文对国内手机取证技术及工具应用情况、特

点优势进行了分类调研，并对反诈手机快速取证工具、手机锁屏密码解锁/提权工具、云取证工具、手机应用程序逆向分析工具、手机数据提取解析及恢复综合类取证工具、数据分析平台等主流产品面对的挑战及需要解决的问题做了详细的分析，指出避开密码锁和设备锁、更新加密技术、研究各种芯片取证技术将是取证工具的研究重点；需加强手机动态仿真模拟技术进行 APP 网络流分析，实施抓取应用程序的通讯数据，分析应用程序的行为特征，并继续探索真机动态逆向分析技术，提高取证工具的普适性；需加强研究云环境中的电子证据固定保全，取证工具与后端平台相结合，利用大数据分析进行数据深度挖掘，实现案件综合研判分析；需加强取证工具取证的自动化、智能化水平；取证技术与物联网等技术相结合，获取智能穿戴设备、智能终端等数据，对使用者行为特征分析也是未来的研究方向。本文还对手机取证工具质量评价难点进行了分析，仅为本领域研究工作提供参考。

参考文献

[1] SAXENA N, CONTI M, CHOO K K R, et al. BAS-VAS: A novel secure protocol for value added service delivery to mobile devices[J]. IEEE Transactions on Information Forensics and Security, 2019, 15: 1470-1485.

[2] Standards N I O. Test results for mobile device acquisition tool: celleBrite UFED 1.1.3.3-report manager 1.6.5[EB/OL]. http://www.cftt.nist.gov.

[3] Test Results for Mobile Device Acquisition Tool Susteen DataPilot Secure View 1.12.0[EB/OL]. http://www.cftt.nist.gov.

[4] 余绯.网络诈骗案件中电子物证取证的相关探究[J].法制与社会,2020 (16):87-88.

[5] 贾钊,丁兆锟,谢波,等. 浅谈司法鉴定中 Android 手机的解锁及镜像[J].电脑知识与技术,2019,15(35):264-265.

[6] 王即墨, 计超豪, 裴洪卿. Android 智能手机锁屏密码及破解方法研究[J]. 刑事技术, 2015,40(2): 142-145.

[7] 李翠. 云计算环境下电子数据取证研究[D]. 重庆:重庆邮电大学,2018.

[8] 杨峻. Android 系统安全和反编译实战[M]. 北京:人民邮电出版社,2015.

[9] 李刚. 案件侦办中手机电子数据取证难点及解决方法[J]. 广西警察学院学报,2018,31(5):68-72.

[10] 康艳荣, 范玮, 赵露,等,基于微信聊天记录时间信息的人物关系刻画技术研究[J]. 刑事技术,2018,43 (3):187-192.

[11] 范红,王冠,杜大海. 智能取证设备一致性评价的几点思考[J]. 信息安全与技术,2014,5(11):15-18.

[12] 范红,胡志昂,杜大海,等 .数据取证设备一致性评价及标准体系研究[J]. 信息网络安全,2014,165(9):58-62.

[13] KUHN R. Smart phone tool test assertions and test plan[EB/OL]. http://www.cftt.nist.gov.

[14] JANSEN W, AYERS R. Guidelines on cell phone forensics[J]. NIST Special publication, 2007, 800(101): 800-101.

[15] Draft.Digital Data Acquisition Tool Test Assertions and Test Plan [EB/OL]. http://www.cftt.rist.

[16] JANSEN W A, DELAITRE A. Reference material for assessing forensic SIM tools [C]//2007 41st Annual IEEE International Carnahan Conference on Security Technology. IEEE, 2007: 227-234.

[17] AYERS R P. Non-GSM Mobile Device Tool Specification[EB/OL]. http://www.tsapps.nist.gov.

[18] AYERS R P. Smart Phone Tool Test Assertions and Test Plan [EB/OL]. http://www.cftt.nist.gov.

[19] GSM Mobile Device and Associated Media Tool Test Assertions and Test Plan[EB/OL]. http://www.cftt.nist.gov.

[20] GSM Mobile Device and Associated Media Tool Specification [EB/OL]. http://www.cftt.nist.gov.

[21] Non-GSM Mobile Device Tool Test Assertions and Test Plan [EB/OL]. http://www.cftt.nist.gov.

[22] Test Results for Mobile Device Acquisition Tool: Oxygen Forensics v10.0.0.81[EB/OL]. http://www.cftt.nist.gov.

[23] PADMANABHAN R, LOBO K, GHELANI M, et al. Comparative analysis of commercial and open source mobile device forensic tools [C]//2016 Ninth International Conference on Contemporary Computing (IC3). IEEE, 2016: 1-6.

[24] RIADI I, FADLIL A, FAUZAN A. A study of mobile forensic tools evaluation on android - based LINE messenger [J]. Technology (NIST), 2018, 9(10):201-206.

[25] ZAMRONI G M, RIADI I. Mobile forensic tools validation and evaluation for instant messaging [J]. International Journal on Advanced Science Engineering and Information Technology, 2020, 10(5): 1860-1866.