ACCCF / 应用知识库

05

卷

设备、应用程序、账户和供应商

西班牙语版 · 2026

手机与即时通讯取证手册

接收、隔离、取证获取、分析、语境与负责任归属

审查移动通信时，不把截图当作数据源，不把提取当作完整获取，也不把账户当作实际使用人。

适用于鉴定人、第一响应人员、律师、调查人员和保管负责人。程序取决于设备、系统、应用程序、版本、加密和授权；不提供绕过锁定或访问他人账户的方法。

编辑统筹：Jocsan Laguna · 美国网络安全与计算机取证委员会

通用技术指南和开放教育材料。不构成法律意见、专家鉴定意见，也不构成未经授权访问系统的操作指导。示例和数据均为虚构；图示为编辑重构。

目录

可见页码对应 PDF 版本。Word 打开文档时可能会更新此索引；标题保留内部导航。

前言：手机不会自己开口作证 3

第1章 设备接收与状态 3

- **1.1 可供他人还原的接收记录** 3
- **1.2 丢失与改动风险** 4

第2章 按层级的数据源 4

- **2.1 设备、应用程序与关联数据** 4
- **2.2 账户、会话和关联设备** 5
- **2.3 供应商和其他参与者** 5

第3章 隔离、供电与移交 6

- **3.1 真实且经过验证的隔离** 6
- **3.2 包装、移交和保管** 7

第4章 取证获取方法 7

- **4.1 手动记录与截图** 7
- **4.2 应用程序导出与备份** 7
- **4.3 逻辑提取、高级提取和供应商获取** 8
- **4.4 工具与输出验证** 8

第5章 对话与内容审查 9

- **5.1 重建会话线程，而不只是单句消息** 9
- **5.2 已编辑、已删除和已转发消息** 9
- **5.3 附件、缩略图和元数据** 10

第6章 归属与沟通 10

- **6.1 账户、设备和个人** 10
- **6.2 时间线与印证** 10
- **6.3 范围明确的报告** 11

附录A 操作格式 12

- **A.1 设备接收** 12
- **A.2 账户和数据源清单** 12
- **A.3 取证获取记录** 12
- **A.4 归属矩阵** 13

附录B 法律框架与最终核查 13

前言：手机不会自己开口作证

手机包含对话、文件、传感器、账户和活动痕迹，但它也可能只是通往云端或其他参与者的窗口。首要问题不是用哪个程序打开它，而是需要证明哪项主张，以及哪些数据源能够回答。如果目标是确定谁写了某条消息，屏幕照片并不足够：还需要会话、设备、验证因素、内容和语境。

移动分析会因系统、应用程序、版本、加密和设备状态而变化。一种提取可能获得可访问的数据库，另一种则只能获得可见文件或导出内容。“取证”一词不会改变实际覆盖范围。报告必须说明实施了什么、获得了什么、哪些内容被排除，不能承诺恢复已删除消息或提供普遍访问。

NIST SP 800-101 Rev. 1 将移动设备的保全、取证获取、检查、分析和报告组织起来，并强调验证和记录。它是方法指南，不是各工具最新能力的清单。具体能力必须在相应型号和版本上，使用测试数据和可验证的结果进行确认。[1]

> **首要规则**
> 不得出于好奇而开机、查看、重置或连接。记录状态和授权，保留配件，并在作出任何更改前确定哪些信息可能消失。

第1章 设备接收与状态

1.1 可供他人还原的接收记录

接收记录应描述类型、品牌、型号、可见标识符、物理状态、开机状态、锁定、电池、可见网络、日期和时区、人员、配件和先前操作。通用记录中不得写入密码。如果有解锁授权，应记录其存在及安全使用该授权的机制。既有标签应保留并与新标识符关联。

在可能的情况下，应在不交互的前提下拍摄可见屏幕：时间、网络图标、电池、通知和状态。照片只能证明当时呈现的状态，不能证明全部内容。如果有人已经打开过应用程序或尝试提取，也应记录。接收过程不完美时须如实记录，不得改写成对象完好到达。

字段	虚构示例	有助于决策
设备	手机 DEMO-MBL-003，型号和序列号可见。	识别并与接收记录核对。

[1] NIST SP 800-101 Rev. 1。移动设备取证分析指南：保全、取证获取、检查、分析、验证和报告。具体技术和能力必须在当前设备和工具上验证。 官方在线来源

字段	虚构示例	有助于决策
状态	已开机、已锁定、电量 43 %，可见移动网络。	优先保全和隔离。
配件	数据线、充电器、SIM 和保护壳分别标记。	保留访问路径和语境。
所声明的历史	持有人在交付前曾尝试导出一段对话。	将先前操作与分析分开。
授权	审查指定对话和账户。	限制对第三方和其他应用程序的访问。
决策	保持状态并联系专业人员。	避免未经授权的更改。

1.2 丢失与改动风险

设备可能接收消息、同步、远程擦除、因闲置锁定或耗尽电池，也可能包含关机后会丢失的会话和密钥。应识别哪种风险最紧迫，以及具备哪些技术能力应对。关机并不总是保全，保持开机也不总是分析。记录必须解释所作选择。

如果目标对话可以从其他参与者或供应商处获得，先申请该数据源可能比干预设备侵扰更小。如果目标是易失性活动或加密密钥，则可能需要经授权的现场取证获取。奥卡姆剃刀原则要求选择区分能力更强且改动更小的数据源，而不是最复杂的工具。

> **何时停止**
> 缺乏授权、存在擦除风险、工具未经验证、加密情况不明或危及人员时，必须暂停并上报。为了查看会发现什么而探索，可能改变证据并在未经许可的情况下扩大范围。

第2章 按层级的数据源

2.1 设备、应用程序与关联数据

设备内存可能包含应用程序数据库、文件、缩略图、日志、受保护的凭据、缓存和传感器数据，其可用性取决于设备状态和访问权限。如果存在同步，一个图片文件夹并不等于整个照片库。本地删除的消息可能仍存在于其他参与者或备份中，也可能无法恢复。分析不能保证任何一种极端结果。

配件同样重要：SIM 或 eSIM、存储卡、充电器、数据线、适配器、保护壳、文档和其他同步设备。手表、平板电脑或计算机可能包含通知或会话，其中的信息各不相同。应列出这些对象，但不能自动扩大授权：某对象已连接，并不意味着其全部内容都属于委托范围。

2.2 账户、会话和关联设备

应用程序可能支持多会话、桌面客户端、备份，以及通过电子邮件或运营商恢复。应申请关联设备列表、添加和移除记录、验证因素、日期、恢复方式变更和会话活动（如可用）。账户名称描述的是逻辑关联，自然人身份需要更多证据。

IP 地址可以提供网络线索，但不能证明住址或个人身份。电话号码可能被重新分配，或在此期间关联到另一个人。IMEI 在其语境中标识设备或配置，不一定标识携带者。归属应通过信息汇聚并考虑其他可能解释：借用、共享使用、远程访问、会话被盗或他人管理。

2.3 供应商和其他参与者

供应商可能保存元数据、连接日志或账户信息，却不保存加密内容。其他参与者可能以不同表现形式持有消息和原始附件。申请应明确账户、时间段、字段、原生格式、时区和生成过程。不能仅因向平台提出请求，就承诺平台会交付内容；必须记录其能力和实际答复。

墨西哥 2025 年《电信和广播法》针对其适用对象和主管机关规定了数据保存和交付规则。分析必须确认申请是否属于该制度，以及相关记录来自电信运营商、应用程序还是其他供应商。不得把即时通讯平台的所有信息都当作电话通话记录表。[2]

> **独立数据源**
> 截图及其打印件不是两项独立证据。他人收到的消息、应用程序导出和会话日志可能具有不同来源和误差。

[2]《电信和广播法》，发布于 16-07-2025。第 182 和 183 条：数据要求和保存、实时查询，以及按阶段在 48 小时内交付。 官方在线来源



图1 手机只是一个层级，不是整个案件。对话可能存在于不同对象中。编辑重构；不构成真实证据。

第3章 隔离、供电与移交

3.1 真实且经过验证的隔离

隔离旨在控制远程改动和新的通信。应评估蜂窝网络、Wi-Fi、蓝牙、NFC、数据线和同步。启用飞行模式需要操作设备，可能改变日志；关机可能丢失会话；如果未经验证或设备尝试重连，隔离容器可能失效。必须记录实施的操作及其影响。

防静电袋用于防止放电，不一定能隔离射频。称其为法拉第袋不会改变其功能。隔离方案必须通过安全方法并在类似条件下验证：信号类型、封闭方式、材料、距离和设备状态。验证不得未经授权拨打某人的号码，而应使用测试设备。

选项	主要风险	必要记录
飞行模式	交互、日志变化和剩余连接。	屏幕、操作、时间和连接均已验证。
关机	内存、会话或加密访问丢失。	理由、状态和获取能力。
射频隔离容器	隔离不足或未经验证。	测试、封闭方式、材料和条件。
保持连接	同步、消息或远程擦除。	必要性、控制和观察。
供电	发热、活动或状态变化。	充电器、数据线和用途均有记录。

3.2 包装、移交和保管

包装应根据物理和逻辑功能选择：防止碰撞、静电、潮湿和访问，同时保持已采取的隔离决定。配件应分别包装并建立关联。封条应包括标识符、日期和负责人；每次拆封或更换都必须记录。如果设备活动可能改变数据，不得在电池和连接不受控制的情况下运输。

保管链应记录由谁交付、由谁接收、为何移交、在哪里、处于何种状态以及如何验证。电子移交应记录权限、渠道、版本、下载和相应对象的哈希值。与复核人共享提取内容时，应交付受控副本，并限制范围之外的第三方数据。

> **实用规则**
> 包装无法弥补错误决策，但可以防止新的改动。封条也不能证明内容真实，只能证明在有记录的顺序中某次封闭状态。

第4章 取证获取方法

4.1 手动记录与截图

当问题仅限于一段对话或其他数据源不可用时，人工检查可能有用。应记录应用程序、版本、设备、日期和时区、操作员、查看路径和显示内容。屏幕录制可以提供视觉连续性，但仍是界面允许查看内容的选择，不能证明整个数据库或不可见事件。

截图前应确定范围，避免暴露其他聊天、照片或通知。如果从应用程序导出，应保存格式、筛选条件、附件、原始名称和日期。导出文件应作为新对象计算哈希值并与设备关联。保全前不得重命名数据源。

4.2 应用程序导出与备份

聊天导出可以包含文本和附件，其结构由应用程序决定。必须检查其中是否包括已编辑、已删除的消息、表情回应、引用、回复或参考，以及日期和参与者如何表示。备份可能包含不同时间点的快照，并使用独立密钥加密。应记录可用能力，不得声称其与物理提取等效。

目标是保全对话时，应将导出与语境截图和其他参与者的数据源结合。目标是分析未包含的事件时，应评估经授权的提取。导出之间的差异可能源于筛选条件或版本，不能自动认定为操控。两个对象都应使用关联标识符保存。

4.3 逻辑提取、高级提取和供应商获取

逻辑提取通过兼容工具获得可访问的文件或数据库。高级提取在设备和方法允许时可以扩大覆盖范围，但需要培训、授权和验证。如果只覆盖特定分区或应用程序，报告不得使用笼统的“完整提取”标签。错误、未解密对象和排除事项均应保留。

通过供应商获取可能提供手机中不存在的账户信息或日志。应申请字段、时区、原生格式、生成过程和字段字典。收到的文件应与 EML 及完整性声明关联（如有）。供应商可能没有加密内容，或采用不同的保存期限；答复不得被表述为通用的电话记录表。[34]

4.4 工具与输出验证

应使用包含已知数据的虚构设备或数据集，验证工具能够生成预期对象、正确解读日期、参与者和附件，并且不会超出记录范围修改数据源。应记录名称、版本、环境、许可、配置和结果。更新可能改变行为，必须重新验证。

输出必须能够打开，并与选定的可见数据源比较：一段受控对话、一个文件、一个日期或一条序列。未解码的对象应标记，不得隐藏。如果第二个工具生成另一种表现形式，应记录差异并评估哪种更能回答问题。工具不能成为证人，它只是方法的组成部分。

> **验收标准**
>
> 取证获取的完成标准不是程序显示“100 %”，而是输出能够打开、与设备关联、说明覆盖范围、保留异常情况，并支持相容的复核。

[3]RFC Editor. RFC 5322, Internet Message Format：消息结构、邮件头和正文。这是保存和理解电子邮件的技术参考，并不能自动证明人的身份。 官方在线来源

[4]NIST SP 800-101 Rev. 1。移动设备取证分析指南：保全、取证获取、检查、分析、验证和报告。具体技术和能力必须在当前设备和工具上验证。 官方在线来源



图2 截图、导出和提取不是同义词。选择取决于问题和覆盖范围。编辑重构；不构成真实证据。

第5章 对话与内容审查

5.1 重建会话线程，而不只是单句消息

应分析参与者、标识符、被引用的消息、回复、附件、表情回应、编辑、删除、发送、接收和阅读时间（如果数据源包含）。截图可能隐藏被回复的消息。序列必须使用数据源中的标识符记录，不得编造编号来暗示未经证实的连续性。

对话应结合语境比较：通话、文件、联系人、应用程序活动、大致位置、电子邮件和证言。解释一句话需要语言、关系、事件和序列。如果缺少被引用的消息，一个“是”可能回答的是另一个问题。分析不得用想象补全含义。

5.2 已编辑、已删除和已转发消息

“已编辑”标签表示可见状态，不说明先前内容。“已删除”标签不能证明所有痕迹均已消失，也不能证明删除目的是隐瞒。转发可能增加另一层来源。应检查可用日志、副本、其他参与者和备份，不得承诺恢复先前文本。

观察	可能意味着什么	进一步结论需要什么
已编辑	应用程序中的事后更改。	版本、日志或持有先前内容的参与者。
已为所有人删除	客户端中显示为已删除。	删除的覆盖范围和可用副本。

观察	可能意味着什么	进一步结论需要什么
已转发	从另一条消息传输的内容。	初始来源和日期（如可用）。
无附件	附件未下载、已过期或未包含。	日志、链接、其他参与者或副本。
时间不同	时区、时钟、转换或编辑。	原始值和数据源配置。

5.3 附件、缩略图和元数据

附件应单独保存并与消息关联。缩略图可能对应不同版本，文件名也可能在下载时改变。应检查内部元数据、内容、大小、格式和系统日期，但不能把这些字段当作来源的自动证明。其他参与者持有的副本可能质量更高或包含额外信息。

文档、图像或音频可能需要专门的原始性和内容分析。手机取证只能证明某文件与消息或文件夹关联，不能证明其场景真实，也不能证明作者是发送者。这种区分可以避免利用良好的获取结果为内容过度结论辩护。

> **虚构案例**
> 一段对话先出现威胁，随后出现一条已删除消息。另一位参与者保留了之后由同一作者发送的澄清消息。辩护方和指控方都必须分析两者。恢复语境不能证明无辜或有罪，但可以避免把孤立的一句话当作全部通信。

第6章 归属与沟通

6.1 账户、设备和个人

归属应分解为几个问题：哪个账户生成或接收消息、哪台设备保持会话、谁能够解锁、谁控制验证因素、谁可以访问，以及事件序列显示什么活动。线路的合同归属可以提供语境，但不能单独证明当时由谁使用。

应考虑借用、共享、委派、凭据被盗、持久会话、远程访问和第三方管理。辩护方不需要证明其中某种替代解释，就可以指出归属不足；指控方则需要以证据排除这些解释。如果信息汇聚很强，应描述其范围，不得直接跳到绝对确定。

6.2 时间线与印证

应保留每个日期的原始值、时区和精度。发送、接收、阅读、编辑和截图是不同事件。导出日期不是消息日期，通知时间可能取决于另一层级。将差异表现为伪造之前，应先结合字段字典和时钟分析。

印证可以来自其他参与者、会话日志、副本、收据、摄像头或传感器序列。不能把截图数量当作独立数据源数量。应追问每个数据源可能存在什么误差，以及这种汇聚能否排除其他解释。

6.3 范围明确的报告

级别	可辩护的表述	不得断言
对象	收到具有这些标识符和配件的设备。	仅凭外观就断言“这是被告的手机”。
取证获取	工具在所说明的范围内获得了这些文件和数据库。	“已提取所有存在的内容。”
内容	数据源中该消息显示此日期和这些参与者。	没有使用证据就断言“由持有人编写”。
分析	数据源与该序列相符，并存在这些局限。	“不存在任何其他解释。”
缺失	在该覆盖范围和筛选条件下未观察到事件。	“该事件从未存在。”

分析结束

不能仅凭一个标签推断个人。独立数据源本可以反驳却未反驳时，归属会增强；当其中一个证明另一种可能性时，归属会减弱。



图3 从账户到个人：仍缺前提。归属因独立性而增强，而不是因形容词而增强。编辑重构；不构成真实证据。

附录A 操作格式

A.1 设备接收

虚构记录

案件：EXP-DEMO-2026-005
设备 / ID：DEMO-MBL-003
品牌、型号和可见标识符：[记录]
状态：[开机、锁定、电池、网络、损坏]
配件：[数据线、SIM、存储卡、保护壳、其他]
交付/接收：[职能、日期、时区、地点]
先前操作：[观察结果和陈述分别记录]
授权：[应用程序、账户、时间段、排除事项]
风险：[易失性、擦除、电池、隐私]
初始决策：[隔离、供电、上报]
照片和封条：[标识符和关联关系]
备注：[不含密钥或不必要的数据]

A.2 账户和数据源清单

层级	账户/数据源	可用性和授权	局限
设备	[应用程序和版本]	[状态、访问和范围]	[加密、覆盖范围]
账户	[标识符]	[会话、验证因素和权限]	[第三方使用]
参与者	[获授权的联系人]	[可用数据源]	[不同的表现形式]
供应商	[服务和保管人]	[申请和答复]	[内容或保存期限]
备份	[日期和位置]	[密钥和访问]	[快照和覆盖范围]

A.3 取证获取记录

输出日志

数据源和授权：DEMO-MBL-003 / [范围]
方法：[手动、导出、逻辑、高级、供应商]
设备、系统和应用程序：[版本]
工具、版本和验证：[虚构测试]
开始/结束日期和时区：[原始值]
对设备的操作：[交互和更改]
获取的对象：[文件、数据库、导出文件]
筛选条件和覆盖范围：[时间段、账户、排除事项]
哈希值和清单文件：[按对象]
异常情况：[错误、未解码、缺失]
验证：[打开、样本和复核]
后续保管：[工作副本和访问]

A.4 归属矩阵

陈述	有利数据源	其他解释	限定性结果
账户发送了消息	[日志]	[可能存在其他会话]	[ ]
设备处于活动状态	[屏幕、日志]	[日期或会话不同]	[ ]
此人使用了该设备	[验证因素、语境]	[借用、盗窃、委派]	[ ]
对话是完整的	[导出]	[筛选条件和其他层级]	[ ]
文件属于该事件	[消息、元数据]	[转发或先前编辑]	[ ]

附录B 法律框架与最终核查

对电子文件的认可，并不意味着每张截图都是真实的，也不意味着账户能够识别个人。在墨西哥，应审查 CCom 89–94 和 1205、按过渡情况适用的 CFPC/CNPCF 制度，以及相应领域的 LMTR。秘鲁的制度分布在签名、程序和档案规范之间；智利区分签名类型和日期；阿根廷强调可靠性；哥伦比亚和厄瓜多尔详细规定保存；西班牙结合 eIDAS 和 LEC。适用时必须核查版本、事项和法域。[5][6][7][8][9][10][11][12][13][14]

数据保护贯穿整个程序：限制应用程序、时间段、账户和第三方数据；区分工作版本和交付版本；保存授权和访问证据。报告不得公开密码、私钥、完整号码或可能促成其他损害的信息。[15][16][17]

最终核查	验收问题
身份	设备、配件和记录是否一致？

[5]墨西哥《商法典》第 89–94 和 1205 条：中立性、归属、书面形式、原件、完整性、可访问性和数据电文采纳。官方汇编。 官方在线来源

[6]《国家民事和家庭诉讼法典》第 348–350 条。汇编包含 15-01-2026 的修订。逐步适用，并取决于相关宣告。 官方在线来源

[7]《电信和广播法》，发布于 16-07-2025。第 182 和 183 条：数据要求和保存、实时查询，以及按阶段在 48 小时内交付。 官方在线来源

[8]秘鲁。IOFE 条例，DS 052-2008-PCM，第 3 和 4 条：经数字签名的电子文件的要求与认可。 官方在线来源

[9]秘鲁。《民事诉讼法典》第 188–197 和 245.5 条：目的、合法性、证据、举证责任、评价和通过技术手段确定日期。 官方在线来源

[10]智利。关于电子文件和电子签名的第 19.799 号法律，第 1–5 条：等效性、书面形式、简单/高级签名、日期和证据效力。 官方在线来源

[11]阿根廷。《民商法典》第 318–319 条：允许以任何方式通信，并评价介质和技术程序的可靠性。 官方在线来源

[12]哥伦比亚。1999 年第 527 号法律，第 5–13、16–25 和 28 条：数据电文、书面形式、原件、完整性、可采性、保存、发送、接收和数字签名。 官方在线来源

[13]厄瓜多尔。《电子商务、电子签名和数据电文法》，第 67 号法律，第 2、6–8、10–16 条：等效性、书面形式、原件、保存、来源、发送、接收和电子签名。 官方在线来源

[14]西班牙。《民事诉讼法》第 326 和 384 条：私人文件、质疑、用于归档、了解或复制数据的措施、检查、保管和合理审查。 官方在线来源

[15]墨西哥。《联邦私人持有个人数据保护法》，文本发布于 20-03-2025，修订于 14-11-2025。第 5–9、18–20 和 31 条：原则、安全、保密、数据泄露和权利请求受理。现行联邦主管机关为反腐败与善治部。 官方在线来源

[16]厄瓜多尔。《个人数据保护基本法》，26-05-2021《官方公报》第 459 号增刊。第 10、37–44 条：原则、安全措施、设计保护、风险和事件处理。 官方在线来源

[17]欧盟。（UE）2016/679 号条例，第 5、25、28 和 32–34 条：原则、设计保护、受托处理方、安全及数据安全泄露的通知/告知。西班牙还要求审查适用的国家和行业法律。 官方在线来源

最终核查	验收问题
状态	是否记录了隔离和供电决策?
覆盖范围	提取是否声明筛选条件、局限和错误?
语境	对话是否保留会话线程、附件和其他层级?
归属	账户、设备和个人是否分开分析?
隐私	是否排除了与委托无关的数据?
复核	他人能否定位并核验该对象?

结语

手机可能保存事件的决定性部分。方法决定这部分内容能否被理解，同时不把一块屏幕变成指控。