Low-Intrusion Mobile Forensic Acquisition in the Field: An Operational Approach to Selective Digital Evidence Collection

Maximiliano Facundo Telmo Gonzalez[1]

[1] Dirección de Investigación Operativa / Ministerio Público Fiscal de Córdoba
mtelmo@justiciacordoba.gob.ar

Abstract. The acquisition of digital evidence from mobile devices relies mostly on laboratory processes with high operational costs and lengthy timeframes, or on poorly traceable manual inspections that, in dynamic investigation scenarios, limit the early retrieval of relevant information. This paper proposes a low-intrusion mobile forensic acquisition model for field surveys, based on the selective collection of evidence from Android devices through standard debugging interfaces (ADB), without requiring superuser privileges or persistent modifications to the device. The approach prioritizes minimal intervention, preservation of the original state, and the capture of high probative value artifacts. We present CAPTA (Agile Collection of Auditable Technical PEP), a tool that implements this model by incorporating integrity verification through SHA-256 hashing, cryptographic chaining of events, chronological logging of actions, and structured organization of evidence with full traceability. Evaluation in real-world contexts shows a reduction in collected data volume of between 300 and 700 times compared to traditional extractions and an average field execution time of 58 minutes, enabling early decisions without immediate referral to a laboratory. Scope, limitations, and conditions of application are discussed. The model is proposed as a preliminary stage within tiered forensic strategies, contributing to expanding operational field investigation capabilities.

Keywords: mobile forensics, low-intrusion acquisition, ADB, digital evidence, field investigation.

Adquisición forense móvil de baja intrusión en campo: un enfoque operativo para la recolección selectiva de evidencia digital

Resumen. La adquisición de evidencia digital en dispositivos móviles depende mayormente de procesos de laboratorio con altos costos operativos y tiempos prolongados, o bien de inspecciones manuales poco trazables que, en escenarios de investigación dinámica, limitan la obtención temprana de información relevante. Este trabajo propone un modelo de adquisición forense móvil de baja

intrusión para relevamientos en campo, basado en la recolección selectiva de evidencia en dispositivos Android mediante interfaces de depuración estándar (ADB), sin requerir privilegios de superusuario ni modificaciones persistentes del dispositivo. El enfoque prioriza la mínima intervención, la preservación del estado original y la captura de artefactos de alto valor probatorio. Se presenta CAPTA (Colecta Ágil de PEP Técnico Auditable), una herramienta que implementa este modelo incorporando verificación de integridad mediante hash SHA-256, encadenamiento criptográfico de eventos, registro cronológico de acciones y organización estructurada de evidencias con trazabilidad completa. La evaluación en contextos reales muestra una reducción del volumen recolectado de entre 300 y 700 veces respecto de extracciones tradicionales y un tiempo promedio de ejecución de 58 minutos, habilitando decisiones tempranas sin derivación inmediata a laboratorio. Se discuten alcances, limitaciones y condiciones de aplicación. El modelo se propone como etapa preliminar dentro de estrategias forenses escalonadas, contribuyendo a ampliar las capacidades operativas de investigación en campo.

Palabras clave: forensia móvil, adquisición de baja intrusión, ADB, evidencia digital, investigación en campo.

1 Introducción

La informática forense móvil enfrenta un desafío estructural en contextos de investigación dinámica: los procedimientos de adquisición disponibles fueron diseñados para entornos de laboratorio, donde el tiempo, los recursos técnicos y las condiciones de trabajo son controlables. En escenarios de campo esta dependencia se traduce en demoras, costos elevados y pérdida de oportunidad para obtener información temprana que oriente decisiones críticas. El riesgo no es únicamente técnico sino metodológico: ausencia de registro estructurado, falta de trazabilidad verificable y dependencia exclusiva del testimonio del operador.

Este trabajo propone y evalúa un modelo de adquisición forense móvil de baja intrusión orientado a relevamientos en campo, basado en la recolección selectiva de artefactos de alto valor probatorio en dispositivos Android mediante ADB (Android Debug Bridge) por USB o WiFi, sin requerir privilegios de superusuario ni modificaciones persistentes del dispositivo.

Su implementación es CAPTA (Colecta Ágil de PEP Técnico Auditable) versión 2.1.1, desarrollada en Python en el ámbito de la Dirección de Investigación Operativa del Ministerio Público Fiscal de Córdoba, aprobada mediante Resolución FG N° 7/26 (Ministerio Público Fiscal de Córdoba, 2026). Sus contribuciones principales son: un modelo conceptual con identificación explícita del riesgo metodológico como dimensión independiente del riesgo técnico; la implementación de CAPTA con mecanismos de integridad, trazabilidad y licenciamiento individualizado; y la evaluación empírica.

2 Antecedentes

Las herramientas comerciales de mayor adopción, Cellebrite UFED, Oxygen Forensic Detective, y las abiertas como Autopsy, Andriller y MVT comparten el paradigma de laboratorio: asumen entorno controlado, tiempo disponible y extracción previa completa del dispositivo. Han sido ampliamente documentadas como referencia en buenas prácticas forenses (Ayers et al., 2014) y su panorama técnico ha sido relevado en encuestas como la de Barmpatsalou et al. (2018) pero no están diseñadas para operar en el momento y lugar del procedimiento investigativo.

La interfaz ADB ha sido identificada como vector válido de adquisición forense lógica sin privilegios de superusuario (Ayers et al., 2014), aunque los modelos existentes la abordan como técnica de extracción en entornos de análisis, sin desarrollar un modelo operativo para campo. El triaje forense (recolección rápida de evidencia de alto valor como etapa previa al análisis completo) ha ganado atención como respuesta a la saturación de laboratorios (Casey, 2011), pero sigue asumiendo laboratorio como contexto de operación.

La brecha identificada no es técnica sino contextual. Los procedimientos de campo presentan restricciones radicalmente distintas: tiempo acotado, equipamiento mínimo y decisiones inmediatas. ADB presenta además una limitación inherente: no ofrece modo de solo lectura nativo ni compatibilidad con bloqueadores físicos de escritura USB, lo que exige diseño explícito de mitigación del riesgo de sobreescritura. Ningún modelo relevado combina recolección selectiva mediante ADB con mitigación documentada, integridad criptográfica, encadenamiento de eventos, licenciamiento individualizado y trazabilidad automatizada, validado en un organismo público. CAPTA se propone como respuesta a esa brecha.

En tal sentido en el ámbito local, herramientas como Captura Digital, desarrollada por el Gabinete de Pericias Informáticas del Poder Judicial del Neuquén, y Espejo Chubut, desarrollada por el Ministerio Público Fiscal de Chubut y adoptada por al menos 15 provincias argentinas, comparten el principio de evitar el secuestro o la extracción completa del dispositivo (ADNSUR, 2024). Ambas, sin embargo, parecieran posicionarse como herramientas de preservación o captura testimonial con un enfoque y alcance diferente al propuesto en este trabajo.

3 Modelo de adquisición de baja intrusión

3.1 Principios del modelo

Mínima intervención. Toda acción se limita a lo necesario para la recolección. No se modifican configuraciones, no se instalan aplicaciones ni se ejecutan comandos con impacto sobre el estado del dispositivo más allá de la lectura. Las condiciones previas (habilitación de depuración USB o WiFi) son requisitos de aplicabilidad documentados antes de la sesión, no intervenciones del modelo.

Preservación del estado original. Las operaciones de lectura mediante ADB no modifican el sistema de archivos ni los metadatos de los artefactos accedidos.

Selectividad orientada al valor probatorio. La recolección apunta a artefactos con alta probabilidad de relevancia investigativa: comunicaciones, ubicaciones, metadatos de aplicaciones y actividad reciente. Esta selectividad habilita la reducción drástica de volumen respecto de extracciones tradicionales.

Integridad verificable. Cada artefacto recibe un hash SHA-256 y los eventos se encadenan criptográficamente, de modo que cualquier alteración posterior sea detectable.

Trazabilidad completa. Cada acción queda registrada con precisión temporal, encadenamiento criptográfico secuencial centralizado, permitiendo reconstruir en forma completa las intervenciones.

Detectabilidad como garantía explícita. El modelo no promete inviolabilidad, limitación inherente a cualquier sistema sin bloqueo físico de escritura, sino detectabilidad verificable de cualquier alteración respecto del estado al momento del bloqueo. La solidez probatoria no descansa en una promesa de inviolabilidad sino en la capacidad de verificación independiente y reproducible. Estos seis principios son consistentes con las directrices de identificación, recolección, adquisición y preservación de evidencia digital de la norma ISO/IEC 27037 (International Organization for Standardization, 2012).

3.2 **Condiciones de aplicabilidad**

Del dispositivo: Android con depuración USB o WiFi habilitada y pantalla desbloqueada. Sin root ni modificaciones previas.

Del entorno: computadora con conexión USB o WiFi en la misma red local. Equipamiento deliberadamente mínimo, abarcando trabajo online y offline.

Del kit de ejecución: CAPTA opera desde dispositivo de almacenamiento externo con licencia atada criptográficamente a ese hardware, garantizando que el kit sea el autorizado institucionalmente.

De la intervención: dentro del marco legal habilitante, orden judicial, consentimiento informado u otro instrumento, con registro documental previo al inicio.

3.3 **Artefactos objetivo**

Registros de llamadas y mensajes; datos de ubicación (GPS, WiFi, celdas); actividad de aplicaciones; registros del sistema; metadatos de archivos; capturas de pantalla vía ADB; grabación de pantalla y audio del dispositivo.

3.4 **Relación con estrategias forenses escalonadas**

El modelo opera como etapa preliminar dentro de una estrategia forense escalonada, habilitando decisiones tempranas, continuar o no con extracción completa, identificar dispositivos prioritarios, sin reemplazar el laboratorio. Los Potenciales Elementos Probatorios (PEP) extraídos, pueden coexistir con extracciones profundas posteriores, aportando un registro temprano con integridad verificable. Esta articulación con etapas posteriores es consistente con los principios y procesos de investigación de

incidentes descriptos en la norma ISO/IEC 27043 (International Organization for Standardization, 2015c).

3.5 **Gestión de documentación y custodia**

Al finalizar cada sesión se genera automáticamente un reporte en formato pdf estructurado con datos del dispositivo, operador, fecha, artefactos y hashes SHA-256, documento primario de la cadena de custodia. Los artefactos se organizan en estructura de directorios estandarizada vinculada a cada hash y timestamp. El encadenamiento criptográfico del log hace detectable cualquier alteración posterior. La identidad del operador queda registrada y vinculada a cada decisión de recolección. Luego el sistema asiste al operador en la confección de un acta de adquisición con información propia del procedimiento (entrevista/allanamiento) de los participantes, el dispositivo analizado, hashes SHA-256 del reporte pdf, de la versión del ejecutable y la posibilidad de firmar digitalmente. Dicho documento se incorpora al expediente físico y digital, funcionando como anclaje externo que refuerza la seguridad documental. Este reporte estructurado, con datos del operador, hashes y trazabilidad de las decisiones de recolección, se alinea con los lineamientos de documentación del análisis y de interpretación de la evidencia digital establecidos en la norma ISO/IEC 27042 (International Organization for Standardization, 2015b).

4 Características técnicas de CAPTA

4.1 **Arquitectura general**

CAPTA adopta una arquitectura de tres capas con separación estricta entre interfaz, lógica de negocio e infraestructura de servicios. Esta separación garantiza que ninguna lógica forense resida en los callbacks de la interfaz gráfica: la UI dispara acciones, pero las decisiones y operaciones con impacto sobre la evidencia se ejecutan exclusivamente en los módulos del núcleo.

Los componentes principales se organizan en tres grupos funcionales:

Interfaz y coordinación: el módulo principal gestiona la ventana de la aplicación, el estado de sesión y la conexión entre módulos. La barra lateral, el panel de herramientas y el panel de evidencias constituyen los puntos de interacción del operador.

Núcleo forense (capta.core): concentra los servicios críticos gestión de sesión, servicio ADB, sistema de archivos, grabación, captura, cadena forense de log, integridad, seguimiento de eventos y política de escritura en dispositivo.

Parsers y documentación: módulos de parseo de exportaciones WhatsApp, generación del reporte PDF forense y redacción del acta de recolección.

4.2 **Sistema de licencias y atadura al dispositivo de ejecución**

CAPTA implementa un sistema de licencias de desarrollo propio que ata criptográficamente el ejecutable al dispositivo físico desde el cual opera ya sea un

pendrive o un disco externo, según la modalidad de despliegue institucional. Este mecanismo tiene implicancias tanto operativas como forenses.

Mecanismo técnico: cada kit CAPTA se compone del ejecutable (.exe), un archivo de licencia (licencia.dat) y la identidad del dispositivo de almacenamiento. La licencia se genera mediante un proceso administrativo centralizado que firma con clave privada RSA un payload JSON que contiene el hash SHA-256 del ejecutable, el identificador del kit y opcionalmente fecha de vigencia. Ese payload firmado se cifra con AES-256-GCM usando una clave derivada de atributos del dispositivo físico.

Al iniciar, CAPTA verifica tres condiciones simultáneas: que la licencia pueda descifrarse, que la firma RSA sea válida contra la clave pública embebida en el ejecutable, y que el hash SHA-256 del propio ejecutable coincida con el registrado en la licencia. Si cualquiera de estas condiciones falla, CAPTA no arranca.

Valor forense: el sistema de licencias contribuye a la trazabilidad en dos dimensiones. Primero, cada kit queda individualizado criptográficamente copiar el kit a otro dispositivo físico no permite ejecutarlo, ya que la licencia no puede descifrarse en otro medio. Segundo, cada arranque de CAPTA exitoso o fallido, queda registrado en inicio_forense.log, el host donde corrió, el identificador del kit y el resultado de la verificación. Este log implementa el mismo mecanismo de encadenamiento criptográfico secuencial descripto en 4.5, garantizando que cualquier alteración del historial de inicios sea detectable.

El sistema permite afirmar en informes técnicos y en sede judicial que cada intervención fue realizada con un kit individualizado y que el ejecutable utilizado no fue modificado respecto del autorizado institucionalmente. Cualquier alteración del ejecutable o intento de reutilización del kit en otro dispositivo queda expuesta por los mecanismos de verificación.

4.3 **Flujo operativo**

El flujo de trabajo de CAPTA se organiza en cuatro etapas secuenciales:

Preparación: el operador registra los datos del caso, número de expediente, investigador a cargo, datos del dispositivo intervenido. El inicio de sesión forense crea la carpeta única del relevamiento, identificada por expediente y marca temporal (EXPEDIENTE_CASO_YYYYMMDD_HHMMSS), que constituye el contenedor exclusivo de toda la evidencia recolectada durante esa intervención.

Relevamiento: el operador ejecuta las acciones de recolección capturas de pantalla, grabación de pantalla y audio del dispositivo vía ADB sobre conexión USB o WiFi, recolección de archivos desde el dispositivo (ADB), desde el equipo local (PC) o desde exportaciones de WhatsApp (ZIP). La conexión WiFi amplía las posibilidades operativas en campo, permitiendo la adquisición en contextos donde una conexión física no es viable, entrevistas, inspecciones in situ, dispositivos en uso activo. Cada acción queda registrada automáticamente en el log forense encadenado.

Documentación: completados los datos del dispositivo, el operador genera el reporte forense en PDF que incluye hashes SHA-256, rutas de custodia, metadatos y versión del sistema y redacta el acta de recolección, que incorpora el reporte y constituye el documento primario de la cadena de custodia.

Bloqueo: al finalizar la intervención, el operador ejecuta el bloqueo del relevamiento. Esta acción genera el manifiesto de hashes (manifest_hashes.json),

establece la carpeta en modo solo lectura e impide nuevas escrituras desde CAPTA. El bloqueo es irreversible dentro del sistema.

4.4 **Recolección de PEP digitales**

CAPTA habilita tres orígenes de recolección, cada uno con su propio flujo de trazabilidad:

Desde dispositivo (ADB): archivos sueltos o estructuras de carpetas extraídos mediante pull a la carpeta de custodia respetando el estado en el que se encontraban en el punto de origen con todas sus subcarpetas. Se calculan hashes SHA-256 en origen y en destino y, cuando aplica, se extraen metadatos EXIF y GPS. Los artefactos se clasifican por origen para su inclusión estructurada en el reporte PDF.

Desde equipo local (PC): archivos o carpetas del disco del operador, copiados a la carpeta de custodia con hash y registro, permitiendo incorporar evidencia digital preexistente en el mismo contenedor verificable.

Exportación WhatsApp: incorporación de un ZIP de exportación desde el equipo local o directamente desde el dispositivo vía ADB. En ambos casos se realiza copia del ZIP a custodia, extracción segura con protección anti zip-slip, cálculo de hash del ZIP y de su contenido, parseo del archivo de chat y generación de una vista HTML con burbujas de conversación, adjuntos y marca de agua CAPTA, enlazada desde el reporte PDF.

Adicionalmente, CAPTA permite captura de pantalla en tiempo real y grabación de pantalla y audio del dispositivo vía ADB, documentando el estado visual y el comportamiento del dispositivo durante la intervención.

4.5 **Integridad y encadenamiento criptográfico**

El núcleo de las garantías de integridad descansa en dos mecanismos complementarios:

Hash por artefacto: cada elemento recolectado recibe un hash SHA-256 incluido en el reporte PDF, en el acta y en el manifiesto generado al bloquear.

Encadenamiento criptográfico secuencial: el archivo registro_forense.log implementa un mecanismo donde cada evento registrado depende criptográficamente del anterior. Al registrar un evento se forma un bloque compuesto por el hash anterior, la marca temporal y el texto del evento; se calcula el SHA-256 de ese bloque; y ese valor se escribe en el log como hash del evento actual, convirtiéndose en el hash anterior del siguiente. La inicialización parte de un hash semilla de 64 ceros cuando el log está vacío. Cualquier modificación, eliminación o inserción de eventos en cualquier posición de la cadena altera todos los hashes subsiguientes, haciendo detectable la manipulación. Al bloquear se escribe un HASH_FINAL_LOG que ancla la cadena completa y queda incluido en el manifiesto, vinculando el registro forense con el resto de la evidencia.

4.6 **Manifiesto y bloqueo**

Al ejecutar el bloqueo, CAPTA genera manifest_hashes.json con la ruta relativa, hash SHA-256, tamaño en bytes y fecha de última modificación de cada archivo del relevamiento, incluyendo el HASH_FINAL_LOG del registro forense. La carpeta pasa a modo solo lectura. CAPTA no promete imposibilidad de modificación externa; garantiza detectabilidad de cualquier alteración respecto del estado al momento del bloqueo.

4.7 **Verificador independiente**

CAPTA Verificador opera exclusivamente en modo lectura sobre la carpeta del relevamiento, sin requerir el entorno original de generación. Reconstruye la cadena del registro forense evento a evento, verifica que cada hash coincida con el recálculo esperado, y comprueba que los archivos del relevamiento mantengan los hashes registrados en el manifiesto. Cualquier archivo modificado, eliminado o añadido con posterioridad al bloqueo es identificado e informado. Puede ejecutarse en cualquier máquina, habilitando la verificación independiente en cualquier momento posterior, incluyendo audiencias judiciales.

4.8 **Política de escrituras en dispositivo**

CAPTA implementa una lista blanca estricta para las escrituras en el dispositivo intervenido. Las únicas operaciones de escritura permitidas son la grabación de pantalla hacia una ruta fija temporal y operaciones de copia temporales para pull de rutas problemáticas, con eliminación inmediata del temporal tras la extracción. Toda operación de escritura queda registrada en el log forense con timestamp, operación, ruta afectada y resultado. No se utilizan adb push, escritura en /data, dd ni redirecciones. Este modelo no sustituye bloqueadores físicos, pero documenta técnicamente cada excepción al principio de solo lectura y garantiza su detectabilidad posterior. Las rutas temporales utilizadas son fijas, propias de CAPTA y ajenas a la estructura de archivos del dispositivo intervenido, por lo que no sobrescriben artefactos preexistentes que pudieran ser relevantes para la investigación; el riesgo de sobreescritura queda así acotado a esas rutas temporales, eliminadas inmediatamente tras la extracción y registradas en el log forense.

5 **Evaluación empírica**

La evaluación se desarrolló en dos etapas: una prueba piloto formal entre agosto y noviembre de 2025 sobre 20 dispositivos Android heterogéneos en condiciones reales de operación seleccionados con solo dos criterios: que estuvieran en un procedimiento de campo real y que poseyeran sistema operativo compatible y un período de uso operativo continuo posterior a la aprobación mediante Resolución FG N° 7/26. Esta evaluación en condiciones reales de operación responde a los criterios de aseguramiento de la idoneidad y adecuación del método de investigación establecidos en la norma ISO/IEC 27041 (International Organization for Standardization, 2015a).

5.1 **Resultados**

Dimensión	**Resultado**
Compatibilidad	100% de dispositivos procesados.
Volumen	300-700x respecto de extracción tradicional completa
Tiempo de ejecución	58 minutos promedio en campo
Tiempo de respuesta	100% de requirentes con resultados en menos de 24hs
Cadena de Custodia	100% valoró preservación adecuada
Claridad de reporte	Fueron valorados como "Altamente claros" vs. el 58% de fiscales a nivel internacional consideran que los informes tradicionales son difíciles de interpretar. (Cellebrite, 2026).
Satisfacción de operador	100% satisfecho, dificultad baja, 100% volvería a usar
Obtención de información potencialmente probatoria.	100% obtuvo elementos probatorios relacionados al hecho investigado.

5.2 **Uso operativo posterior**

Cuatro operadores activos procesaron aproximadamente 30 dispositivos adicionales post-piloto. En octubre de 2025 CAPTA fue utilizada en un operativo de alta relevancia pública con cuatro dispositivos simultáneos (Infobae, 2025). Al momento de la redacción, la Dirección de Investigación Operativa se encuentra capacitando 50 nuevos operadores, señalando el cierre de la Fase 1 del despliegue institucional.

5.3 **Discusión**

El 100% de procesamiento sobre muestra heterogénea confirma la viabilidad operativa en condiciones reales. La reducción de 300-700x no implica reducción equivalente en valor probatorio: el 100% de requirentes obtuvo PEP claros, lo que indica que la selectividad no sacrifica utilidad investigativa. Los 58 minutos de relevamiento demuestran viabilidad dentro de la ventana temporal de un allanamiento o entrevista. La respuesta en menos de 24 horas representa un cambio cualitativo respecto del paradigma de laboratorio, durante la prueba piloto esta inmediatez permitió identificar a un agresor sexual y rescatar a su víctima menor de edad en el transcurso de una mañana.

6 Alcances y limitaciones

6.1 Alcances

CAPTA opera como herramienta del primer interventor en procedimientos de campo donde la derivación inmediata a laboratorio no es viable. Sobre dispositivos Android con depuración habilitada y pantalla desbloqueada, ADB provee acceso a artefactos de alto valor como llamadas, SMS, ubicación, logs, metadatos, mensajería, archivos, estructuras de archivos, elementos suficiente para orientar la investigación en la totalidad de los casos evaluados. Las garantías de integridad por SHA-256, trazabilidad por encadenamiento criptográfico y detectabilidad por manifiesto son reproducibles e independientes del entorno de generación.

6.2 Limitaciones técnicas

Sin acceso root, datos en particiones del sistema, contenido cifrado y espacios privados de aplicaciones quedan fuera del alcance por lo cual requieren derivación a laboratorio. Dispositivos bloqueados: ADB no ofrece modo de solo lectura nativo ni compatibilidad con bloqueadores físicos USB, las escrituras mínimas necesarias se controlan por lista blanca y quedan registradas. CAPTA garantiza detectabilidad respecto del estado al bloqueo, no certifica autenticidad de origen ni impide modificaciones externas con privilegios administrativos. Versión actual: solo Android y derivados.

6.3 Limitaciones operativas

WiFi requiere la misma red WIFI local; USB requiere cable compatible y puerto en buen estado. La selección de artefactos relevantes según el tipo de caso se beneficia de criterio investigativo, CAPTA estructura el proceso pero no reemplaza el juicio del operador. Actualmente sin repositorio centralizado; la custodia depende de procedimientos institucionales vigentes.

6.4 Posicionamiento

CAPTA no compite con el laboratorio, compite con la ausencia de procedimiento estructurado en el primer contacto con la evidencia. En una estrategia forense escalonada ocupa la primera etapa: triaje lógico selectivo con garantías de integridad. Las etapas siguientes se aplican donde la primera identifica necesidad, evitando el costo de intervención máxima sobre todos los dispositivos. Esta afirmación se basa en los datos operativos agregados de la sección de cibercrimen de la DIO (oficina donde se gestó la idea de CAPTA). Cuyos integrantes entre los años 2023 y 2025 Realizaron triajes manuales sobre un total de 1.232 (en su gran mayoría teléfonos móviles), lo cual permitió evitar el secuestro físico de aproximadamente dos tercios de ellos (67 %; datos internos no publicados). Cabe precisar que estas cifras corresponden a procedimientos de triaje anteriores a la incorporación de CAPTA y reflejan, por tanto, el rendimiento del método de selección en el lugar como práctica consolidada de la

unidad, con independencia del instrumento empleado. El aporte específico de la herramienta no es reducir el secuestro, resultado que el triaje ya alcanzaba, sino dotar a la decisión de descarte de respaldo documental y trazable, transformando un criterio operativo en una decisión auditable y defendible ante eventuales cuestionamientos.

7 Conclusiones

Este trabajo presentó un modelo de adquisición forense móvil de baja intrusión orientado a relevamientos en campo, (triaje lógico selectivo + registro visual) y su implementación concreta en CAPTA (Colecta Ágil de PEP Técnico Auditable), una herramienta desarrollada institucionalmente en el Ministerio Público Fiscal de Córdoba y aprobada mediante Resolución FG N° 7/26.

El punto de partida fue un diagnóstico operativo concreto: los procedimientos de adquisición forense móvil disponibles fueron diseñados para el laboratorio, y su aplicación en contextos de campo genera una brecha metodológica que no es solo técnica sino probatoria. La ausencia de registro estructurado, la falta de trazabilidad verificable y la dependencia exclusiva del testimonio del operador constituyen riesgos que debilitan la cadena de custodia desde el primer contacto con la evidencia digital.

El modelo propuesto responde a esa brecha con seis principios articulados: mínima intervención, preservación del estado original, selectividad orientada al valor probatorio, integridad verificable, trazabilidad completa y detectabilidad de alteraciones. Estos principios se materializan en CAPTA a través de mecanismos técnicos que en conjunto garantizan que cada intervención sea documentada, verificable y defendible técnicamente.

La evaluación empírica sobre 20 dispositivos en condiciones reales de operación produjo resultados que confirman la viabilidad del modelo: tasa de procesamiento del 100%, reducción del volumen recolectado de entre 300 y 700 veces respecto de extracciones tradicionales, tiempo de adquisición promedio en sólo 58 minutos, disponibilidad de resultados en menos de 24 horas, y valoración unánime de los requirentes sobre la preservación adecuada de la cadena de custodia y la claridad de los informes generados. El uso operativo posterior, aunque aún limitado en el número de operadores, incluyó procedimientos de alta relevancia pública, consolidó estos resultados en condiciones de campo exigentes.

Tres contribuciones centrales emergen de este trabajo. La primera es conceptual: la distinción explícita entre riesgo técnico y riesgo metodológico en la adquisición forense de campo, y la propuesta de un modelo que aborda ambas dimensiones de manera integrada. La segunda es técnica: la implementación de CAPTA como herramienta que combina recolección selectiva mediante ADB, mecanismos de integridad criptográfica y licenciamiento individualizado del kit de ejecución, validada en un organismo público. La tercera es institucional: la demostración de que es posible desarrollar capacidades forenses de campo desde adentro de un organismo público, con recursos acotados, tecnología abierta y estándares internacionales como referencia, obteniendo aprobación formal y adopción operativa sostenida.

Las limitaciones del modelo están documentadas y son parte de su diseño: CAPTA no reemplaza la pericia de laboratorio, no opera sobre dispositivos bloqueados ni sobre sistemas distintos de Android, y no certifica autenticidad de origen. Define su

espacio de aplicación con precisión porque esa precisión es condición de su solidez probatoria.

CAPTA no es solo una herramienta. Es una propuesta de orden metodológico para el relevamiento preliminar digital en el ámbito judicial. Lo que no puede ser explicado, documentado y reproducido, no puede ser sostenido.

Referencias

Ayers, R., Brothers, S., y Jansen, W. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-101r1

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the Internet (3.a ed.). Academic Press.

Barmpatsalou, K., Cruz, T., Monteiro, E., & Simões, P. (2018). Current and future trends in mobile device forensics: A survey. ACM Computing Surveys, 51(3), 1–34. https://dl.acm.org/doi/epdf/10.1145/3177847

Cellebrite. (2026). Industry trends survey report. Cellebrite. https://cellebrite.com

Infobae. (29 de octubre de 2025). Un imputado por amenazar a la madre de Blas Correas, el chico que fue asesinado por policías en Córdoba. Infobae. https://www.infobae.com/sociedad/policiales/2025/10/29/un-imputado-por-amenazar-a-la-madre-de-blas-correas-el-chico-que-fue-asesinado-por-policias-en-cordoba/

International Organization for Standardization. (2012). ISO/IEC 27037: Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. ISO.

International Organization for Standardization. (2015a). ISO/IEC 27041: Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method. ISO.

International Organization for Standardization. (2015b). ISO/IEC 27042: Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence. ISO.

International Organization for Standardization. (2015c). ISO/IEC 27043: Information technology — Security techniques — Incident investigation principles and processes. ISO.

Ministerio Público Fiscal de Córdoba. (2026). Resolución FG N° 7/26: Aprobación del uso de CAPTA en el ámbito del Ministerio Público Fiscal de Córdoba. MPF Córdoba.

ADNSUR. (2024, 29 de noviembre). Cómo funciona "Espejo Chubut", el software forense que ya se utiliza en 15 provincias del país.

ADNSUR.https://www.adnsur.com.ar/policiales---judiciales/como-funciona--espejo-chubut---el-software-forense-que-ya-se-utiliza-en-15-provincias-del-pais_a67d07d77d56c6cd2a3367e19

Gabinete de Pericias Informáticas, Poder Judicial del Neuquén. (s.f.). Captura Digital. https://gpineuquen.gob.ar/CapturaDigital.html

Durante la preparación de este trabajo, los autores utilizaron Claude (Anthropic) con el fin de mejorar el lenguaje y la legibilidad del manuscrito. Tras utilizar esta herramienta, los autores revisaron y editaron el contenido según fuera necesario y asumen plena responsabilidad por el contenido de la publicación.