ISBN: 978-628-96613-3-0. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2026.1.1.1921

Digital Forensic Analysis of Criminal Evidence in Mobile Devices: A Literature Review

Andy Alessandro, Chiroque Adanaque[1], Jose Manuel, Talavera Flores [2], Victor Angel, Ancajima Miñan[3]
[1,2, 3] Universidad Tecnológica del Perú, Perú, *U21227923@utp.edu.pe, U20208586@utp.edu.pe, C25994@utp.edu.pe*

Abstract

Changing the way crime is investigated in the mobile era requires rigor and humanity: recovering the stories stored in phones without compromising their integrity. With that premise, this review sought to identify how effective and reliable current mobile forensic methodologies and tools are, and how they are being used in real investigative contexts. A structured systematic review was conducted using the PICO model, a Scopus search, and a PRISMA flowchart: from 229 records, 20 recent studies were screened and evaluated, examining research designs, methodological frameworks, extraction techniques, and performance by application and operating system. The results reveal an operational consensus: DFRWS and NIST frameworks guide the sequential phases of identification, preservation, acquisition, analysis, and reporting; commercial forensic suites (Cellebrite UFED, Magnet AXIOM, XRY, Oxygen, Belkasoft, MOBILedit) achieve high recovery rates, although with heterogeneous performance depending on the app, version, and encryption; and emerging automation approaches (ML/LLM and multimodal semantic analysis) accelerate triage and improve the correlation of textual, audio, image, and video evidence. Limitations persist, including modern encryption, cloud dependencies, uneven parsers, and explainability issues that affect legal admissibility. In conclusion, the evidence supports an integrated model—"standard framework + validated tool + explainable automation"—sustained by strict chain of custody and reproducible documentation. The review recommends open test datasets, cross-tool validation by case/OS/encryption level, and governance/ethical guidelines that balance investigative efficiency with privacy protection.

Keywords — Digital forensics, Mobile devices, Digital evidence, Analysis methodologies, Reliability and validity.

Análisis forense digital evidencias delictivas en dispositivos móviles: una revisión de la literatura

Andy Alessandro, Chiroque Adanaque[1], Jose Manuel, Talavera Flores [2], Victor Angel, Ancajima Miñan[3]
[1,2, 3] Universidad Tecnológica del Perú, Perú, *U21227923@utp.edu.pe, U20208586@utp.edu.pe, C25994@utp.edu.pe*

Resumen

Cambiar la forma en que se investiga el delito en la era móvil exige rigor y humanidad: recuperar la historia que guardan los teléfonos sin romper su integridad. Con esa premisa, esta revisión buscó identificar qué tan efectivas y confiables son las metodologías y herramientas actuales de análisis forense móvil, y cómo se están usando en contextos reales. Se aplicó una RSL estructurada con PICO, búsqueda en Scopus y trazado PRISMA: de 229 registros se cribaron y evaluaron 20 estudios recientes, valorando diseños, marcos metodológicos, tipos de extracción y desempeño por aplicación/sistema operativo. Los resultados muestran un consenso operativo: los marcos DFRWS y NIST articulan las fases de identificación, preservación, adquisición, análisis y reporte; las suites comerciales (Cellebrite UFED, Magnet AXIOM, XRY, Oxygen, Belkasoft, MOBILedit) logran altas tasas de recuperación, aunque con rendimientos heterogéneos según app, versión y cifrado; y emergen enfoques de automatización (ML/LLM y análisis semántico multimodal) que aceleran el tamizaje y mejoran la correlación de evidencias de texto, audio, imagen y video. Persisten límites: cifrado moderno, dependencias de nube, parsers desiguales y retos de explicabilidad que condicionan la admisibilidad. En conclusión, la evidencia respalda un modelo integrado "marco estándar + herramienta validada + automatización explicable", sostenido por cadena de custodia y documentación reproducible. Se recomiendan bancos de prueba abiertos, validación cruzada multi-herramienta por caso/OS/cifrado y guías de gobernanza/ética que equilibren eficacia investigativa y protección de la privacidad.

Palabra clave — Forense digital, Dispositivos móviles, Evidencia digital, Metodologías de análisis, Confiabilidad y validez.

I. Introducción

En los últimos cinco años, el análisis forense digital en dispositivos móviles ha experimentado un crecimiento acelerado debido al papel central que los smartphones cumplen como repositorios de vida digital y como fuentes primarias de evidencia penal y cibernética. La literatura revisada muestra que los dispositivos móviles concentran datos de ubicación, mensajería, metadatos y trazas de uso que permiten reconstruir eventos con rigor técnico y probabilístico [1]. En paralelo, las investigaciones recientes han consolidado catálogos de herramientas y técnicas de extracción lógica, física y avanzada, capaces de recuperar artefactos desde aplicaciones, sistemas operativos y entornos IoT asociados [2]. Asimismo, se han presentado avances significativos en la incorporación de machine learning, análisis multimodal y modelos semánticos que mejoran el tamizaje de evidencias y aceleran la interpretación de grandes volúmenes de datos [5], [6], [7]. A pesar de estas innovaciones, la literatura coincide en que la estandarización mediante marcos como NIST y DFRWS sigue siendo fundamental para garantizar trazabilidad, validez y consistencia probatoria en entornos judiciales [1], [8], [10], [11], [16].

A pesar del avance metodológico y tecnológico, persisten discrepancias significativas que muestran la ausencia de una visión panorámica integrada del estado actual del análisis forense móvil. Estudios recientes destacan brechas en confiabilidad pericial, variabilidad en la recuperación de evidencia según la herramienta empleada y diferencias sustantivas en la capacidad de extracción frente a cifrado avanzado, aplicaciones emergentes o sistemas de seguridad reforzados [9], [10], [11]. Además, varias investigaciones muestran inconsistencias en validación, trazabilidad y documentación, lo que compromete la admisibilidad jurídica de los resultados [9]. La rápida evolución tecnológica —caracterizada por nuevos dispositivos, formatos de almacenamiento, sistemas de cifrado y modelos de comunicación— supera la capacidad de actualización de muchas metodologías actuales, generando vacíos de conocimiento que dificultan identificar cuáles técnicas y herramientas son realmente efectivas y confiables. A esto se suman dimensiones éticas vinculadas a privacidad, percepción pública y aceptación del análisis automatizado, que influyen directamente en la interpretación y legitimidad del proceso forense [12]. En conjunto, la literatura evidencia la necesidad urgente de una síntesis sistemática que evalúe la eficacia, confiabilidad y limitaciones del ecosistema forense móvil contemporáneo.

Este estudio se desarrolla con el propósito de responder a la necesidad científica y profesional de consolidar el conocimiento disperso existente en los últimos cinco años y proporcionar una revisión sistemática que permita comprender de manera clara, comparativa y crítica las metodologías y herramientas predominantes en el análisis forense móvil. Desde una perspectiva académica, la revisión permite identificar vacíos de investigación, estandarizar criterios y orientar nuevas líneas de estudio hacia técnicas emergentes como IA multimodal, modelos semánticos y extracción en entornos cifrados. Desde una perspectiva técnica, los resultados ofrecen a peritos, investigadores y profesionales de ciberseguridad un recurso actualizado que facilita la selección adecuada de procedimientos, herramientas y estrategias de análisis según el tipo de evidencia o escenario investigativo [5], [6], [13]. Finalmente, desde una dimensión social y jurídica, el fortalecimiento de las capacidades forenses móviles contribuye a mejorar la calidad de la evidencia digital, elevar su admisibilidad y asegurar procesos judiciales más confiables y transparentes. Este trabajo, por tanto, se escribe para aportar una base sólida que permita estandarizar, mejorar y evolucionar continuamente las prácticas forenses en dispositivos móviles,

respondiendo directamente al problema detectado y al objetivo planteado.

El objetivo general de este estudio es analizar de manera sistemática la literatura científica existente sobre el análisis digital forense en dispositivos móviles, con el fin de identificar, comparar, evaluar y sintetizar las metodologías, herramientas y limitaciones más relevantes y predominantes, para así contribuir de manera significativa a la estandarización, mejora continua y evolución de las prácticas forenses en este campo.

En este documento, la Sección II describe la metodología utilizada para la Revisión Sistemática de la Literatura (RSL), detallando la aplicación del modelo PICO para la formulación de las preguntas de investigación, así como los criterios de inclusión y exclusión empleados. La Sección III presenta los resultados del análisis bibliométrico y la síntesis de la literatura revisada, destacando las metodologías aplicadas, las herramientas más utilizadas y los principales desafíos técnicos en el análisis forense digital de evidencias obtenidas desde dispositivos móviles. La Sección IV desarrolla la Discusión, interpretando los hallazgos en relación con la literatura existente y los objetivos del estudio, ofreciendo una visión crítica sobre los avances y limitaciones identificados. Finalmente, la Sección V expone las conclusiones y propone futuras líneas de investigación orientadas a mejorar, optimizar y estandarizar las prácticas forenses digitales.

II. Metodología

Para desarrollar la revisión sistemática sobre el análisis forense digital en dispositivos móviles, se aplicó una metodología estructurada basada en una búsqueda exhaustiva y filtrada en la base de datos Scopus. Con el fin de asegurar coherencia y precisión en la formulación de la pregunta de investigación, se empleó el modelo PICO, reconocido por delimitar con claridad los componentes del estudio. Bajo este enfoque, se planteó la siguiente pregunta principal de investigación: **¿Qué tan efectivas y confiables son las metodologías y herramientas de análisis forense digital empleadas para obtener evidencia en dispositivos móviles dentro de investigaciones forenses?** A partir de esta formulación, se definieron preguntas específicas vinculadas a cada componente del modelo PICO, tal como se muestra en la Tabla I:

TABLA I
PREGUNTAS DERIVADAS DESARROLLADAS DEL MODELO PICO

P	¿Qué tipos de evidencias digitales se encuentran en dispositivos móviles que puedan ser útiles dentro de una investigación forense?
I	¿Qué metodologías y herramientas de análisis digital forense se han aplicado para la extracción, preservación y análisis de la evidencia en dispositivos móviles?
O	¿Qué tan efectivas y confiables son estas metodologías y herramientas en términos de validez, precisión, calidad y admisibilidad legal de la evidencia obtenida?
C	¿En qué escenarios y tipos de investigaciones forenses se han implementado estas metodologías y herramientas, y cuáles han sido sus principales limitaciones y alcances?

De igual modo, se destacan las palabras clave que permitieron definir la ecuación de búsqueda, tal como se presenta en la tabla I.

TABLA II
PALABRAS CLAVE DEFINIDAS

P	Mobile devices, Smartphones, Cell phones, Mobile phones, Mobile data
I	Mobile forensic
O	Effectiveness, Accuracy, Reliability, Validity, Evaluation, Benchmark
C	Forensic investigation, Criminal, Legal, Judicial, Law enforcement, Prosecution, Cybersecurity, Cybercrime, Digital crime, Computer crime, Proceedings, Trial

La búsqueda de información se realizó aplicando estrictamente los criterios de inclusión y exclusión, lo que permitió construir una ecuación de búsqueda adecuada para la base de datos y seleccionar únicamente los documentos pertinentes al tema de investigación. La ecuación empleada fue la siguiente:

(TITLE-ABS-KEY (Mobile devices OR Smartphones OR Cell phones OR Mobile phones OR Mobile data) AND TITLE-ABS-KEY (Mobile forensic*) AND TITLE-ABS-KEY (effectiv* OR accurac* OR reliab* OR valid* OR evaluat* OR benchmark*) AND TITLE-ABS-KEY (“forensic investigation" OR criminal* OR legal* OR judicial* OR "law enforcement" OR prosecution OR cybersecurity OR cybercrime OR "digital crime" OR "computer crime" OR proceeding* OR trial*))

Con la estrategia de búsqueda definida, se aplicó el diagrama PRISMA para documentar las etapas de identificación, selección y evaluación de elegibilidad de los estudios. La única base de datos consultada fue Scopus, que reportó un total de 229 registros. Además, se establecieron y aplicaron de manera rigurosa los criterios de inclusión y exclusión, detallados en las Tablas III y IV, con el fin de asegurar la pertinencia, calidad y relevancia de los estudios finalmente incorporados en la revisión.

TABLA III
CRITERIOS DE INCLUSIÓN

CI1	Los estudios incluidos deben abordar metodologías o herramientas de análisis forense digital aplicadas a dispositivos móviles (smartphones, tablets, celulares, etc.).
CI2	Los estudios incluidos deben reportar resultados empíricos o evaluaciones sobre la efectividad, calidad, precisión o confiabilidad de dichas metodologías y herramientas.
CI3	Los estudios incluidos deben estar publicados en los últimos 4 a 5 años, considerando la rápida evolución de las tecnologías en el campo del análisis forense digital.
CI4	Los estudios deben incluir información sobre el contexto de aplicación (investigaciones forenses, procesos judiciales, investigaciones policiales, ciberseguridad, delitos informáticos).

TABLA IV
CRITERIOS DE EXCLUSIÓN

CE1	Estudios que no aborden específicamente el análisis forense digital aplicado a dispositivos móviles, centrándose únicamente en otros entornos.
CE2	Estudios que no describan metodologías o herramientas de análisis forense digital en dispositivos móviles, o que se enfoquen solo en aspectos legales sin componente tecnológico ni evaluación de resultados.
CE3	Estudios publicados en idiomas diferentes al español o inglés.

En la fase de identificación, se registraron 229 artículos provenientes de la base de datos Scopus. No se encontraron registros duplicados; sin embargo, 172 artículos presentaban acceso restringido, por lo que solo 57 quedaron disponibles para el cribado. Durante la fase de cribado, se excluyeron 33 artículos por no cumplir con los criterios de inclusión establecidos, quedando 24 registros elegibles, todos ellos recuperados exitosamente para su revisión completa. En la fase de elegibilidad, se evaluaron los 24 artículos restantes. En esta etapa, se excluyeron 2 publicaciones por el criterio CE1, 2 por el criterio CE2 y ninguna por el criterio CE3.

Finalmente, 20 artículos fueron seleccionados e incorporados a la revisión sistemática, constituyendo la base principal del análisis y el marco de evidencia científica para el desarrollo de la investigación. La Figura 1 muestra el diagrama de flujo PRISMA, que sintetiza de manera visual cada etapa del proceso de identificación, cribado, elegibilidad y selección de los estudios.

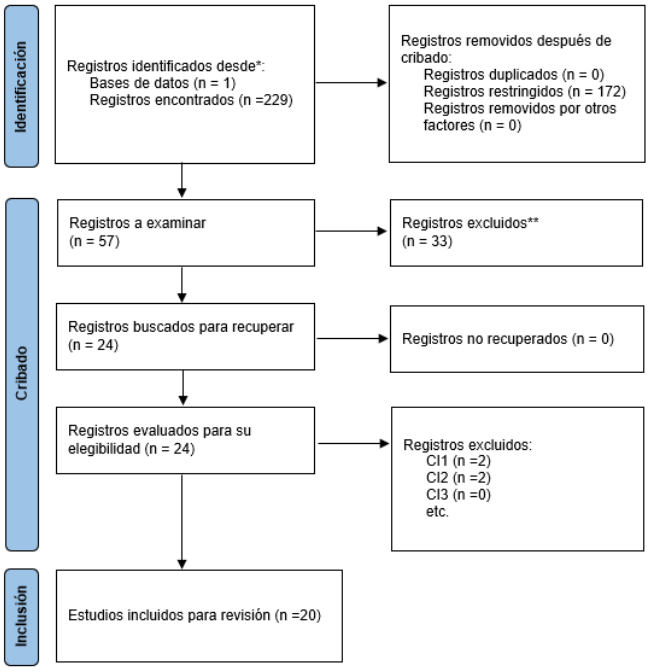

Fig. 1. Identificación de artículos vía metodología PRISMA

III. RESULTADOS

Para una comprensión integral, los resultados se presentan en dos partes. La primera corresponde al análisis bibliométrico, donde se examinan datos generales, tendencias de publicación y distribución geográfica. La segunda es una síntesis de los artículos, organizada según las preguntas de investigación, lo que permite integrar los hallazgos clave de manera coherente con los objetivos del estudio.

A) *Resultados bibliométricos.*

El análisis bibliométrico comienza exponiendo las investigaciones seleccionadas para la revisión. La Tabla V complementa esta sección, detallando la autoría y los títulos de cada estudio incluido en el análisis.

TABLA V
ARTICULOS DE REVISIÓN

Autores	Título
E. Casey, D. O. Jaquet-Chiffelle, H. Spichiger, E. Ryser, T. R. Souvignet [1]	Structuring the Evaluation of Location-Related Mobile Device Evidence
T. Sutikno [2]	Mobile forensics tools and techniques for digital crime investigation: a comprehensive review
L. R. Pace, L. S. A. Salmon, C. J. Bowen, I. M. Baggili, G. G. Richard [3]	Every step you take, I'll be tracking you: Forensic analysis of the Tile tracker application
D. Wijnberg, N. A. Le-Khac [4]	Identifying interception possibilities for WhatsApp communication
A. Bhattarai, A. Sahin, M. Veksler, A. Kurt, D. Aras, C. Imery, K. Akkaya [5]	Cryptocurrency forensics automation: a deep learning and NLP-based approach for mobile platforms
K.-j. Kim, C. Lee, S.-e. Bae, J.-h. Choi, W. Kang [6]	Digital forensics in law enforcement: A case study of LLM-driven evidence analysis
J. Xi, M. Siegel, D. Labudde, M. Spranger [7]	Towards a joint semantic analysis in mobile forensics environments
A. Fukami, R. A. Stoykova, Z. J. M. H. Geradts [8]	A new model for forensic data extraction from encrypted mobile devices
R. A. Stoykova, S. Andersen, K. Y. Franke, S. Axelsson [9]	Reliability assessment of digital forensic investigations in the Norwegian police
I. Riadi, A. Yudhana, G. P. I. Fanani [10]	Comparative Analysis of Forensic Software on Android-based MiChat using ACPO and DFRWS Framework
N. Herman, I. Riadi, I. A. Rafiq [11]	Forensic Mobile Analysis on Social Media Using National Institute Standard of Technology Method
J. R. Hildebrandt, E. M. Schomakers, M. Ziefle, A. Calero Valdez [12]	Understanding indirect users' privacy concerns in mobile forensics — A mixed method conjoint approach
A. Almuqren, H. K. Alsuwaelim, M. M. Hafizur Rahman, A. I. Abubakar [13]	A Systematic Literature Review on Digital Forensic Investigation on Android Devices
B. M. V. Bernardo, H. S. Mamede, J. M. P. Barroso, V. D. dos Santos [14]	Mobile Device Forensics Framework: A Toolbox to Support and Enhance This Process
M. M. Moreb, S. Salah, B. M. Amro [15]	A Novel Framework for Mobile Forensics Investigation Process
I. Riadi, N. Herman, N. H. Siregar [16]	Mobile Forensic Analysis of Signal Messenger Application on Android using Digital Forensic Research Workshop (DFRWS) Framework
G. M. Jones, S. Godfrey Winster, P. Valarmathie [17]	An Advanced Integrated Approach in Mobile Forensic Investigation
G. M. Jones, S. Godfrey Winster, P. Valarmathie [18]	Integrated Approach to Detect Cyberbullying Text: Mobile Device Forensics Data
X. Xie, C. Chang, Z. Yang, L. Li [19]	Antitamper Image Watermarking Based on Cellular Network Topology for IoT-Themed Mobile Forensics
W. Bosma, S. Dalm, E. J. van Eijk, R. El Harchaoui, E. Rijgersberg, H. T. Tops, A. Veenstra, R. J. Ypma [20]	Establishing phone-pair co-usage by comparing mobility patterns

Las publicaciones incluidas en la RSL abarcan múltiples países; destacan los aportes de Países Bajos con métodos probabilísticos para inferir co-uso de teléfonos a partir de patrones de movilidad y expresar la fuerza de la evidencia mediante razones de verosimilitud (LR) [20], junto con una guía bayesiana para evaluar evidencia de geolocalización y

comunicar su solidez en contextos forenses [1]. Desde Indonesia se reportan comparativos de herramientas aplicando marcos DFRWS y NIST en mensajería y redes sociales, con diferencias claras en capacidad de recuperación y cobertura de artefactos [10], [11]. Arabia Saudita aporta una RSL centrada en Android que mapea técnicas, herramientas y futuros desarrollos [13]. En conjunto, los resultados muestran buen desempeño en tareas específicas, pero subrayan que la confiabilidad probatoria exige evaluación estructurada, validación de herramientas y documentación trazable de métodos y hallazgos, tal como evidencian los estudios metodológicos y de fiabilidad en Europa [1],[9]. La Figura 2 presenta la distribución cuantitativa de los artículos seleccionados organizados por país de publicación, reflejando la geografía del esfuerzo investigativo en análisis forense digital de dispositivos móviles.

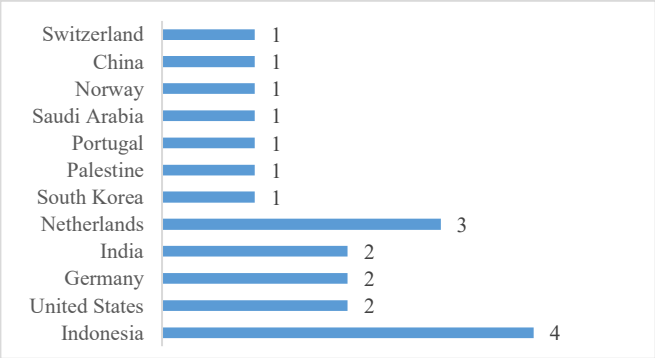

Fig. 2. Distribución cuantitativa de artículos seleccionados según país de publicación.

La RSL muestra que el 25% de los estudios se centra en la fiabilidad metodológica, destacando validaciones sistemáticas, marcos bayesianos y procedimientos de trazabilidad que fortalecen la robustez probatoria [1], [9], [15], [20]. Otro 25% aborda la incorporación de IA y aprendizaje automático, donde el análisis semántico multimodal, el deep learning y los LLMs agilizan el tamizaje y la interpretación de grandes volúmenes de datos móviles [5], [7], [17], [18]. El 20% compara herramientas de extracción y análisis, evidenciando diferencias en precisión y cobertura entre Magnet AXIOM, MOBILedit y Belkasoft bajo marcos ACPO, NIST y DFRWS [3], [10], [11], [16]. Un 10% corresponde a revisiones y modelos integrales, útiles para estandarizar procesos y fortalecer la calidad investigativa [2], [13]. Temas emergentes (5% cada uno) incluyen interceptación en tiempo real [4], extracción en dispositivos cifrados [8], técnicas antitamper para IoT [19] y preocupaciones éticas y de privacidad [12]. En conjunto, el campo avanza hacia métodos reproducibles, auditables y compatibles con IA, sin descuidar la solidez jurídica y la protección de datos [1], [6], [9], [13].

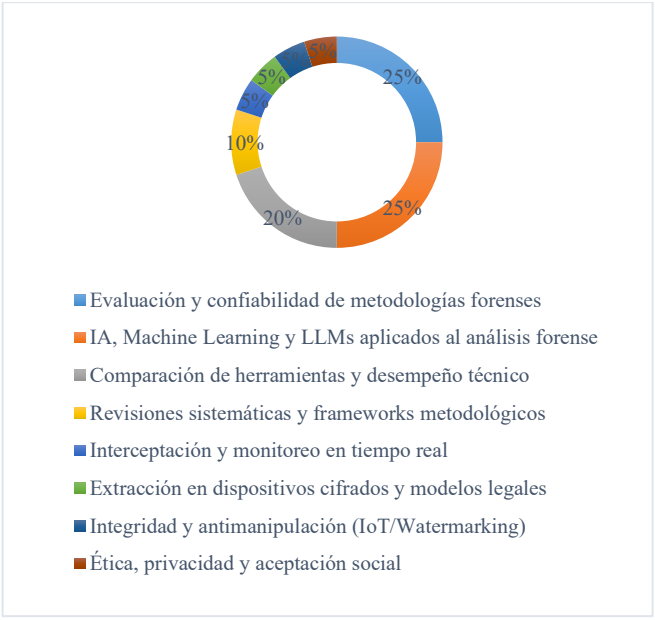

Fig. 3. Distribución cuantitativa de artículos seleccionados según tema principal.

El análisis de palabras clave extraídas de los veinte artículos de la RSL muestra una concentración temática claramente delimitada. Los términos “Investigation Forensic”, “Mobile Forensics” y “Digital Evidence” se posicionan como conceptos dominantes, expresando el foco central en la extracción, preservación y validación científica de evidencias digitales en dispositivos móviles [1], [2], [15], [20]. Junto a ellos, destacan de forma reiterada las palabras “Machine Learning”, “Artificial Intelligence” y “Automation”, que evidencian la incorporación de técnicas inteligentes para optimizar la detección de artefactos, el análisis multimodal y la interpretación automatizada de datos forenses en contextos de alta complejidad [5], [6], [7], [17], [18]. Asimismo, conceptos como “Reliability”, “Validation” y “Framework” revelan la importancia de la estandarización y la evaluación estructurada de herramientas, pilares necesarios para asegurar la robustez metodológica y la reproducibilidad de los hallazgos en investigaciones digitales [9], [13], [14]. En menor frecuencia, aunque con alta relevancia estratégica, emergen términos como “Encryption”, “Privacy” e “Interception”, que reflejan los desafíos técnicos y éticos vinculados al tratamiento de información cifrada, la protección de comunicaciones seguras y los procesos de interceptación regulada [4], [8], [12]. En conjunto, estas palabras clave evidencian una convergencia entre automatización, confiabilidad probatoria y responsabilidad ética, delineando una evolución donde la tecnología no solo amplía la capacidad investigativa, sino que exige marcos metodológicos sólidos que aseguren la validez científica y jurídica del análisis forense digital [1], [6], [9], [16]. La Figura 4 ilustra visualmente la frecuencia relativa de estos términos, mostrando cómo convergen la tecnología avanzada, los procesos confiables y los desafíos de privacidad en la configuración actual del campo de la forensia móvil.

Fig. 4. Distribución cuantitativa de las palabras claves más comunes de los artículos seleccionados.

B) *Resultados basados en las preguntas pico.*

Esta sección presenta los resultados y la valoración crítica de los estudios sobre metodologías y herramientas de análisis forense móvil, organizados según la estrategia PICO. Los hallazgos se integraron mediante formatos de extracción y comparación, permitiendo evaluar de manera sistemática la efectividad y confiabilidad de las técnicas forenses para obtener evidencia digital útil en investigaciones judiciales.

1) ¿Qué tipos de evidencias digitales se encuentran en dispositivos móviles que puedan ser útiles dentro de una investigación forense?

Los dispositivos móviles se han convertido en una fuente central de evidencia digital para la investigación forense, pues concentran información comunicacional, contextual y conductual de alto valor probatorio. Entre los tipos de evidencia más relevantes destacan los mensajes de texto, mensajería instantánea y registros de llamadas, que permiten reconstruir interacciones, secuencias temporales y vínculos entre usuarios, incluso tras eliminaciones, gracias a técnicas de extracción física y lógica [2], [4], [6].

Los archivos multimedia —fotografías, videos y audios— constituyen otra categoría clave, ya que sus metadatos EXIF brindan datos precisos sobre ubicación, fecha, hora y dispositivo, facilitando la autentificación y correlación de eventos, en línea con los avances en análisis multimodal [7], [9]. Asimismo, redes sociales y servicios en la nube conservan artefactos residuales significativos aun tras sincronizaciones o borrados, como demuestran estudios centrados en plataformas sociales y recuperación de contenidos distribuidos [10], [14].

Los registros de ubicación y conectividad son esenciales para reconstruir trayectorias y patrones de movilidad, coherentes con investigaciones sobre análisis espacial, co-uso de dispositivos y correlación temporal [16], [17], [19]. Finalmente, los metadatos del sistema, logs, bases SQLite y cachés permiten documentar accesos, acciones y modificaciones, apoyando la detección de actividad sospechosa según marcos de validación forense [3], [8].

En conjunto, estos tipos de evidencia reflejan el potencial investigativo del dispositivo móvil y la necesidad de metodologías estandarizadas para garantizar su fiabilidad probatoria [1], [9]. La Figura 5 muestra visualmente la distribución de estas categorías dentro de la RSL.

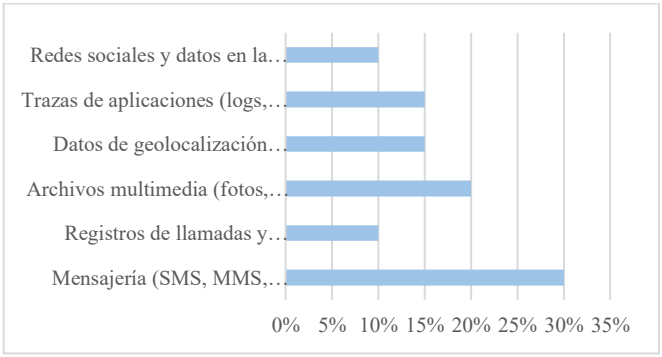

Fig. 5. Distribución cuantitativa de tipos de evidencias en dispositivos móviles.

2) ¿Qué metodologías y herramientas de análisis digital forense se han aplicado para la extracción, preservación y análisis de la evidencia en dispositivos móviles?

A A la luz de la literatura analizada, la extracción, preservación y análisis de evidencia en dispositivos móviles dependen de un ecosistema metodológico que articula estándares forenses consolidados con herramientas especializadas y técnicas emergentes basadas en inteligencia artificial. En concordancia con los modelos propuestos por el NIST y el marco DFRWS, considerados referentes operativos en investigaciones reales, los estudios revisados señalan que estas guías estructuran el ciclo forense mediante fases secuenciales de identificación, preservación, adquisición, análisis e interpretación, asegurando trazabilidad, reproducibilidad y consistencia probatoria en cada etapa [1], [8], [10], [11], [16]. Su aplicación uniforme contribuye a minimizar la manipulación inadvertida de artefactos, garantizar la integridad mediante hashing y fortalecer la validez jurídica del proceso.

En el plano instrumental, la literatura confirma el uso predominante de Cellebrite UFED, Magnet AXIOM, Oxygen Forensic Detective, XRY/XAMN, Belkasoft Evidence Center y MOBILedit, herramientas que posibilitan extracciones lógicas, físicas y avanzadas (JTAG, ISP, chip-off), así como el procesamiento profundo de bases de datos, metadatos, elementos multimedia, geolocalización y artefactos de aplicaciones como WhatsApp, Signal, Instagram, Telegram o Tile [2], [3], [4], [10], [11], [16], [18]. Los estudios comparativos demuestran que su rendimiento varía en precisión, cobertura de artefactos y capacidad de reconstrucción, lo que ha impulsado la recomendación de validación cruzada, uso de herramientas complementarias y documentación exhaustiva para reducir sesgos y pérdidas de información [9].

A esta infraestructura se suman metodologías contemporáneas basadas en IA, aprendizaje automático y análisis semántico multimodal, empleadas para clasificar evidencia, detectar patrones delictivos, priorizar artefactos relevantes y automatizar el tamizaje en escenarios con altos volúmenes de datos. En particular, los modelos de deep learning y los enfoques LLM-driven permiten acelerar el análisis más del 40 % en ciertos contextos, mejorar la identificación de relaciones en comunicaciones y correlacionar datos provenientes de múltiples canales (texto, audio, imágenes, videos) [3], [5], [6], [7], [18]. Su contribución resulta especialmente crítica ante la creciente complejidad del ecosistema móvil.

Asimismo, los estudios recientes incorporan técnicas de blockchain y hashing para garantizar inmutabilidad e integridad, junto con modelos probabilísticos de geolocalización y co-movilidad que facilitan inferencias sobre interacción y co-uso de dispositivos [19], [20].

En conjunto, la revisión evidencia que la fiabilidad del análisis forense móvil depende de la convergencia entre metodologías estandarizadas, herramientas validadas y estrategias avanzadas de automatización, siempre sustentadas por una cadena de custodia rigurosa. Las Figuras 6, 7 y 8 ilustran esta distribución, mostrando el predominio de los marcos DFRWS/NIST, la recurrencia de herramientas comerciales especializadas y la amplitud de técnicas de extracción utilizadas.

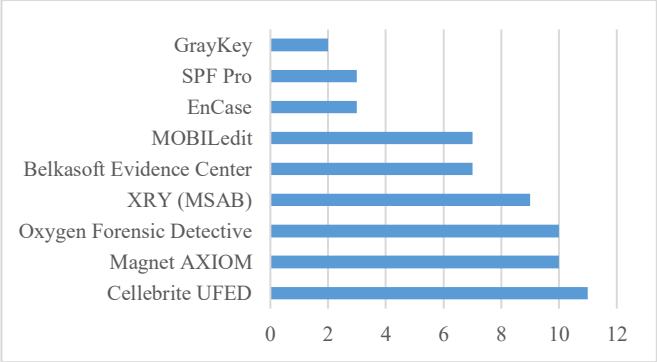

Fig. 6. Representación comparativa de la frecuencia de uso de herramientas forenses móviles.

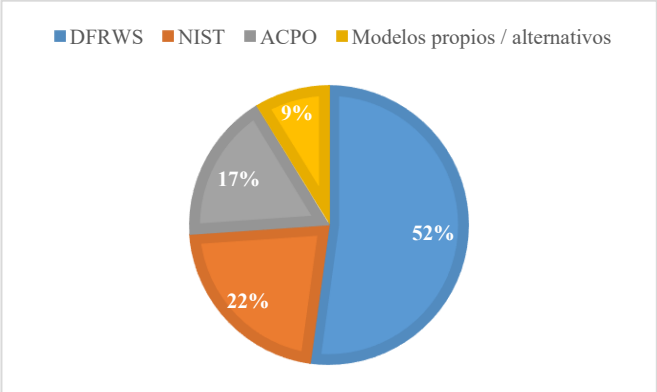

Fig. 7. Distribución de los marcos metodológicos utilizados en los estudios de análisis forense móvil.

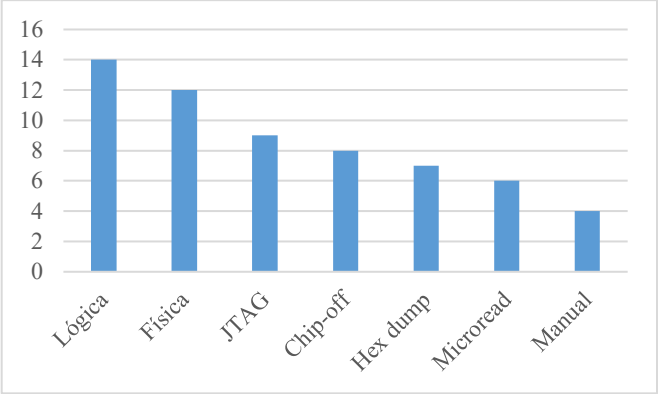

Fig. 8. Frecuencia de técnicas de extracción empleadas en los estudios de análisis forense móvil.

3) ¿Qué tan efectivas y confiables son estas metodologías y herramientas en términos de validez, precisión, calidad y admisibilidad legal de la evidencia obtenida?

La efectividad y confiabilidad de las metodologías y herramientas de análisis forense móvil se fundamentan en su capacidad para producir evidencia válida, precisa, técnicamente sólida y jurídicamente admisible. La literatura coincide en que los frameworks estandarizados —principalmente NIST y DFRWS— constituyen el eje central para garantizar rigor procedimental, trazabilidad y reproducibilidad, reduciendo la variabilidad operativa y asegurando que los resultados cumplan con los criterios probatorios exigidos por tribunales y organismos reguladores [1], [8], [10], [11], [16].

En términos de precisión y calidad técnica, los estudios comparativos muestran desempeños superiores al 90 % en la recuperación de artefactos vinculados a mensajería, redes sociales, geolocalización y aplicaciones cifradas. Herramientas como Cellebrite UFED, Magnet AXIOM, Oxygen Forensic Detective, XRY, MOBILedit y Belkasoft destacan de forma consistente, con resultados particularmente sólidos en contextos Android e iOS. Evaluaciones específicas —como la realizada en Signal Messenger— reportan que Belkasoft alcanza un 78.69 % de recuperación, mientras que UFED y AXIOM mantienen ventajas en profundidad de extracción y cobertura de artefactos [2], [4], [7], [16].

Las líneas recientes basadas en IA y aprendizaje automático alcanzan precisiones entre el 90 % y 96 % al priorizar y correlacionar evidencias, optimizando el tamizaje de grandes volúmenes de datos. Sin embargo, su admisibilidad legal presenta limitaciones asociadas a la falta de transparencia algorítmica, riesgos de sesgo y dificultades para asegurar reproducibilidad ante escrutinio judicial [11], [12], [15].

A ello se suman métodos avanzados de extracción en dispositivos cifrados, uso sistemático de hashes, cadenas de custodia verificables y esquemas antitampering, los cuales refuerzan autenticidad y detección de manipulación [5], [8], [18], [19].

En conjunto, las metodologías más confiables son aquellas que integran estandarización, precisión técnica y mecanismos robustos de integridad, siempre sometidos a validaciones continuas e interoperabilidad institucional [1], [9], [20]. La

Figura 9 sintetiza estos rangos de efectividad, evidenciando alta capacidad técnica frente a los desafíos persistentes en admisibilidad legal.

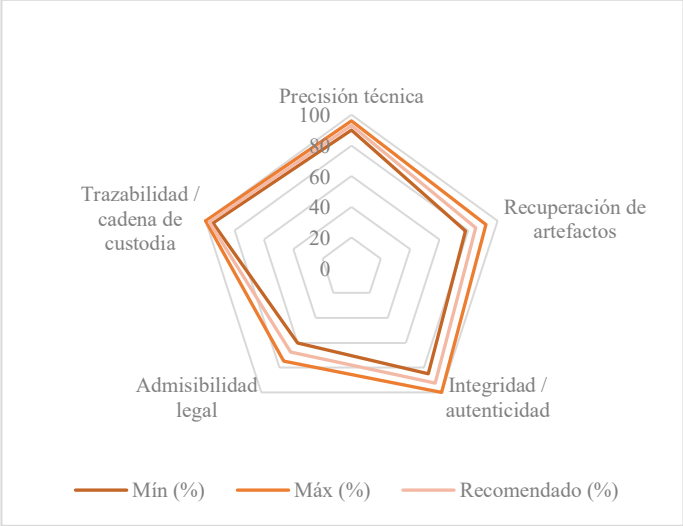

Fig. 9. Comparativa de enfoques metodológicos y herramientas forenses en términos de validez, precisión, calidad y admisibilidad legal.

4) ¿En qué escenarios y tipos de investigaciones forenses se han implementado estas metodologías y herramientas, y cuáles han sido sus principales limitaciones y alcances?

Las publicaciones analizadas muestran que las metodologías y herramientas forenses móviles se aplican en un espectro amplio de escenarios criminales donde los dispositivos móviles actúan como fuente primaria de evidencia. Su uso es predominante en investigaciones de cibercrimen, fraude, acoso/cyberbullying, tráfico de drogas, suplantación y coordinación delictiva, especialmente cuando la comunicación se desarrolla en mensajería cifrada como WhatsApp, Signal, MiChat o Instagram [3], [4], [11], [16]. En estos contextos, marcos estandarizados como NIST y DFRWS permiten estructurar fases de identificación, preservación y análisis, garantizando trazabilidad probatoria en delitos donde el flujo de ubicación, mensajes y metadatos resulta crítico [1], [8].

Asimismo, la literatura evidencia su implementación en entornos policiales para delitos sexuales, extorsión, desaparición de personas, movilidad sospechosa, así como en auditorías corporativas ligadas a acceso indebido o manipulación de datos [9], [20]. En reconstrucción de hechos y validación de co-presencia, los estudios que evalúan patrones de movilidad, geolocalización y análisis de dispositivos Tile revelan un alto valor forense para rastrear trayectorias y verificar interacción entre actores [3], [20].

Sin embargo, el contraste técnico muestra que, aunque herramientas como Magnet AXIOM, UFED, Oxygen y Belkasoft alcanzan altos niveles de recuperación en mensajería, bases de datos y artefactos multimedia, siguen enfrentando limitaciones ante cifrado moderno, Secure Enclave, FBE/FDE, autenticación biométrica y datos alojados exclusivamente en la nube, donde el acceso depende de credenciales o jurisdicción internacional [8], [12]. Además, investigaciones recientes refuerzan que las técnicas de IA/ML agilizan el análisis masivo y la clasificación de evidencia, pero su admisibilidad legal continúa restringida por la falta de explicabilidad algorítmica [6], [5].

En conjunto, las metodologías y herramientas muestran un desempeño robusto en escenarios donde predominan delitos como fraude digital, tráfico ilícito, acoso/cyberbullying, estafa, narcotráfico, hostigamiento, extorsión, suplantación, amenazas y difusión de hoaxes, aunque su alcance operativo depende del estado del dispositivo, su nivel de cifrado y la volatilidad del dato. Las Figuras 10 y 11 permiten visualizar de manera complementaria los patrones identificados en la revisión. Mientras la Figura 11 muestra la distribución de los delitos más frecuentes en los que se emplean metodologías y herramientas forenses móviles, la Figura 10 compara su alcance y limitaciones en los escenarios específicos donde estas técnicas se aplican. En conjunto, ambos gráficos contextualizan los ámbitos de mayor incidencia del análisis forense digital móvil y revelan las fortalezas y restricciones operativas presentes en cada tipo de investigación.

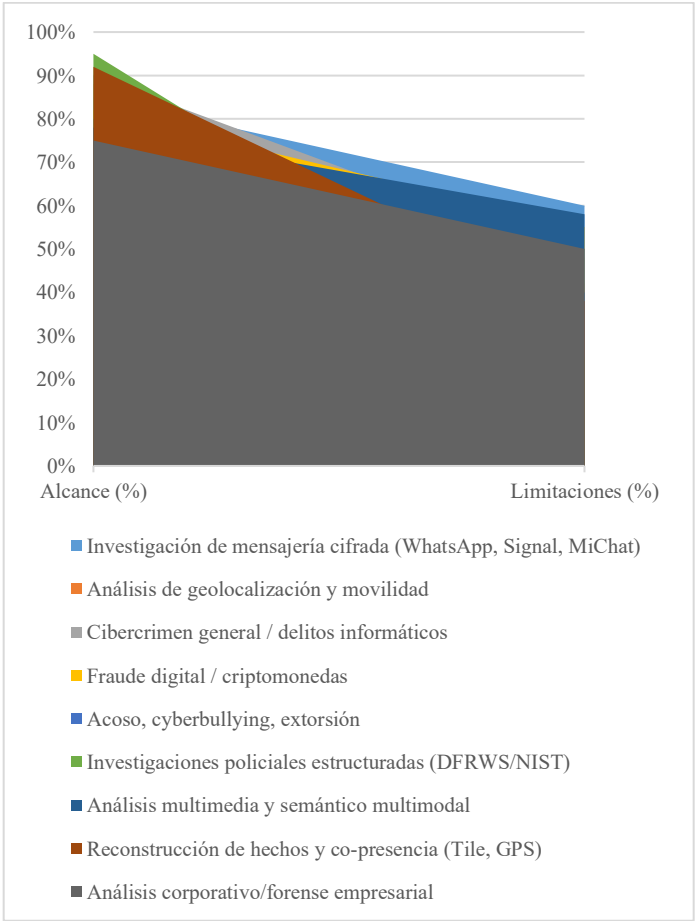

Fig. 10. Evaluación comparativa de escenarios forenses móviles en términos de alcance operativo y restricciones técnicas

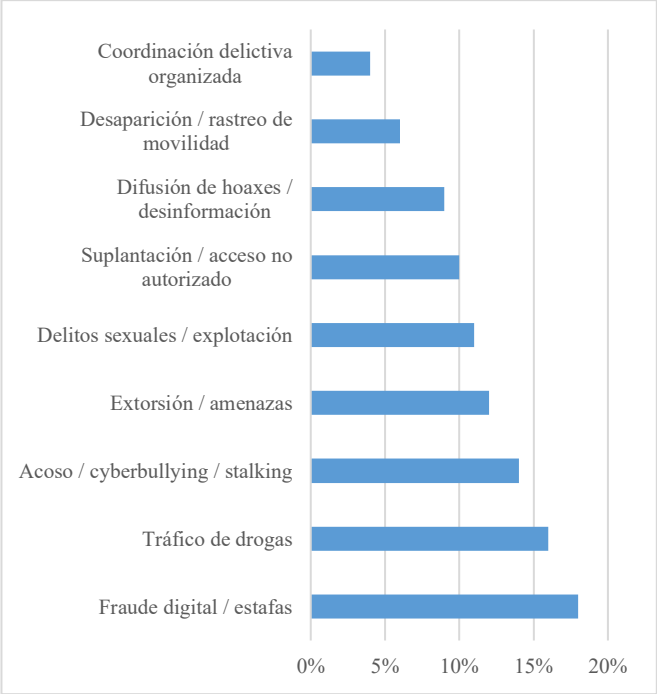

Fig. 11. Distribución de los delitos más frecuentes asociados a investigaciones forenses móviles

IV. DISCUSIÓN

Los hallazgos de esta RSL muestran una convergencia clara entre estudios que coinciden en que la confiabilidad probatoria en forense móvil depende de tres ejes: (i) marcos estandarizados como DFRWS y NIST, (ii) herramientas validadas con documentación trazable y (iii) automatización capaz de acelerar el tamizaje sin comprometer la auditabilidad. Sin embargo, cuando estos elementos se llevan a escenarios reales —especialmente mensajería y redes sociales— emerge una heterogeneidad significativa. En WhatsApp e Instagram, por ejemplo, los estudios comparativos reportan recuperaciones altas pero disparejas: Magnet AXIOM supera a MOBILedit en ciertas categorías, pero ambos fallan de manera consistente en artefactos específicos como videos largos [11]. Estas diferencias no parecen aleatorias, sino que reflejan la interacción entre versiones de app/OS, parsers propietarios, niveles de cifrado y políticas de sandboxing.

Este patrón reaparece en Signal, donde Belkasoft muestra un rendimiento global superior a AXIOM y MOBILedit [16]. La literatura interpreta este resultado no como superioridad universal de una herramienta, sino como evidencia de que la eficacia depende del tipo de caso, del dataset y del entorno tecnológico. Así, la noción de "mejor herramienta" pierde sentido fuera de contextos controlados, lo que refuerza la necesidad de validación cruzada y análisis multifuente.

En paralelo, la investigación reciente sobre IA aporta mejoras sustantivas: los LLM, los modelos multimodales y el topic modeling guiado por conocimiento incrementan la precisión, el F1 y la velocidad de tamizaje [6], [7], [18]. No obstante, estos avances abren nuevos dilemas: la explicabilidad limitada, el riesgo de alucinación y la dificultad de documentar transformaciones internas plantean tensiones con los estándares de admisibilidad y obligan a mantener supervisión pericial. La literatura coincide en que la automatización puede ser aliada, pero no sustituye el razonamiento experto, especialmente en comunicaciones cifradas, datos ruidosos o interacciones multimodales complejas.

En la dimensión social, los estudios de percepción pública muestran una mayor disposición a liberar geodatos que imágenes, y una preferencia por análisis automatizado en lugar de lectura humana [12]. Este hallazgo resulta relevante porque sugiere que la aceptación social del forense móvil no depende solo del rendimiento técnico, sino también de la alineación con expectativas de proporcionalidad y respeto a la privacidad.

Finalmente, la literatura metodológica avanza hacia la construcción de catálogos, frameworks y toolboxes que buscan reducir la dispersión de prácticas y fortalecer la gobernanza de datos [14], [13]. Sin embargo, persisten brechas importantes: ausencia de bancos de prueba estandarizados, heterogeneidad de métricas y documentación insuficiente en muchos estudios. Esta combinación explica parte de los resultados "sorprendentes" —como el desempeño desigual entre suites comerciales— y muestra que la variabilidad no proviene únicamente de las herramientas, sino del ecosistema técnico y metodológico en su conjunto.

V. CONCLUSIONES

En conclusión, la evidencia converge en tres pilares fundamentales: (i) la adopción de marcos estandarizados (DFRWS/NIST), que funcionan como la espina dorsal de la trazabilidad y la admisibilidad; (ii) el uso de suites consolidadas (Cellebrite UFED, Magnet AXIOM, XRY, Oxygen, Belkasoft, MOBILedit), cuyo desempeño es alto pero heterogéneo según aplicación, sistema operativo o nivel de cifrado, lo que demanda validación cruzada y documentación rigurosa; y (iii) la incorporación de automatización "explicable" —LLM, ML y análisis semántico multimodal— que acelera el tamizaje sin desplazar el criterio pericial. Diversos hallazgos fortalecen estas conclusiones: el mayor rendimiento de Belkasoft en Signal (78,69%) frente a AXIOM y MOBILedit; la disposición social a liberar geodatos por encima de contenidos visuales; los avances en análisis semántico conjunto que integran texto, audio, imagen y video; y la automatización aplicada a dominios emergentes, como criptomonedas, con niveles elevados de recall y accuracy.

Asimismo, la revisión confirma que la combinación articulada de "marco + herramienta validada + automatización auditada" es la que ofrece mayor validez técnica y jurídica. Los marcos aseguran coherencia en las fases de adquisición, análisis y reporte; las suites forenses permiten recuperar grandes volúmenes de artefactos de mensajería y redes sociales, aunque su cobertura depende del cifrado, la versión del software y los parsers utilizados; y los enfoques de IA mejoran la precisión y reducen los tiempos de análisis, siempre que se apliquen

controles de alucinación, trazabilidad de prompts y reportes completamente reproducibles para sostener su admisibilidad.

De forma complementaria, la literatura subraya la necesidad de guías operativas y "toolbox" integrados que reduzcan la dispersión metodológica y fortalezcan la gobernanza de datos y la cadena de custodia, especialmente en ecosistemas cloud e IoT. Para futuras investigaciones, se recomienda estandarizar bancos de prueba abiertos, desarrollar validaciones multi-herramienta por tipo de caso, sistema operativo y nivel de cifrado, e impulsar soluciones de IA con explicabilidad verificable que permitan mantener integridad, auditoría y transparencia en todo el proceso forense.

REFERENCIAS

[1] E. Casey, D. O. Jaquet-Chiffelle, H. Spichiger, E. Ryser y T. R. Souvignet, «Structuring the Evaluation of Location-Related Mobile Device Evidence,» *Forensic Science International: Digital Investigation,* vol. 32, p. 300928, 2020.

[2] T. Sutikno, «Mobile forensics tools and techniques for digital crime investigation: a comprehensive review,» *International Journal of Informatics and Communication Technology,* vol. 13, nº 2, p. 321–332, 2024.

[3] L. R. Pace, L. S. A. Salmon, C. J. Bowen, I. M. Baggili y G. G. Richard, «Every step you take, I'll be tracking you: Forensic analysis of the Tile tracker application,» *Forensic Science International: Digital Investigation,* vol. 45, p. 301559, 2023.

[4] D. Wijnberg y N. A. Le-Khac, «Identifying interception possibilities for WhatsApp communication,» *Forensic Science International: Digital Investigation,* vol. 38, nº 301132, 2021.

[5] A. Bhattarai, A. Sahin, M. Veksler, A. Kurt, D. Aras, C. Imery y K. Akkaya, «Cryptocurrency forensics automation: a deep learning and NLP-based approach for mobile platforms,» *Discover Computing,* vol. 28, nº 1, p. 123, 2025.

[6] K.-j. Kim, C. Lee, S.-e. Bae, J.-h. Choi y W. Kang, «Digital forensics in law enforcement: A case study of LLM-driven evidence analysis,» *Forensic Science International: Digital Investigation,* vol. 54, nº 10.1016/j.fsidi.2025.301939, p. 301939, 2025.

[7] J. Xi, M. Siegel, D. Labudde y M. Spranger, «Towards a joint semantic analysis in mobile forensics environments,» *Forensic Science International: Digital Investigation,* vol. 52, nº 10.1016/j.fsidi.2024.301846, p. 301846, 2025.

[8] A. Fukami, R. A. Stoykova y Z. J. M. H. Geradts, «A new model for forensic data extraction from encrypted mobile devices,» *Forensic Science International: Digital Investigation,* vol. 38, p. 301169, 2021.

[9] R. A. Stoykova, S. Andersen, K. Y. Franke y S. Axelsson, «Reliability assessment of digital forensic investigations in the Norwegian police,» *Forensic Science International: Digital Investigation,* vol. 40, p. 301351, 2022.

[10] I. Riadi, A. Yudhana y G. P. I. Fanani, «Comparative Analysis of Forensic Software on Android-based MiChat using ACPO and DFRWS Framework,» *Jurnal RESTI,* vol. 7, nº 2, p. 286–292, 2023.

[11] N. Herman, I. Riadi y I. A. Rafiq, «Forensic Mobile Analysis on Social Media Using National Institute Standard of Technology Method,» *International Journal of Safety and Security Engineering,* vol. 12, nº 6, p. 707–713, 2022.

[12] J. R. Hildebrandt, E. M. Schomakers, M. Ziefle y A. Calero Valdez, «Understanding indirect users' privacy concerns in mobile forensics — A mixed method conjoint approach,» *Frontiers in Computer Science,* vol. 5, p. 972186, 2023.

[13] A. Almuqren, H. K. Alsuwaelim, M. M. Hafizur Rahman y A. I. Abubakar, «A Systematic Literature Review on Digital Forensic Investigation on Android Devices,» *Procedia Computer Science,* vol. 235, p. 1332–1352, 2024.

[14] B. M. V. Bernardo, H. S. Mamede, J. M. P. Barroso y V. D. dos Santos, «Mobile Device Forensics Framework: A Toolbox to Support and Enhance This Process,» *Emerging Science Journal,* vol. 8, nº 3, p. 972–998, 2024.

[15] M. M. Moreb, S. Salah y B. M. Amro, «A Novel Framework for Mobile Forensics Investigation Process,» *International Journal of Computing and Digital Systems,* vol. 16, nº 1, p. 125–136, 2024.

[16] I. Riadi, n. Herman y N. H. Siregar, «Mobile Forensic Analysis of Signal Messenger Application on Android using Digital Forensic Research Workshop (DFRWS) Framework,» *Ingenierie des Systemes d'Information,* vol. 27, nº 6, p. 903–913, 2022.

[17] G. M. Jones, S. Godfrey Winster y P. Valarmathie, «"An Advanced Integrated Approach in Mobile Forensic Investigation",» *Intelligent Automation and Soft Computing,* vol. 33, nº 1, p. 87–102, 2022.

[18] G. M. Jones, S. Godfrey Winster y P. Valarmathie, «"Integrated Approach to Detect Cyberbullying Text: Mobile Device Forensics Data",» *Computer Systems Science and Engineering,* vol. 40, nº 3, p. 963–978, 2021.

[19] X. Xie, C. Chang, Z. Yang y L. Li, «"Antitamper Image Watermarking Based on Cellular Network Topology for IoT-Themed Mobile Forensics",» *Wireless Communications and Mobile Computing,* 2021.

[20] W. Bosma, S. Dalm, E. J. van Eijk, R. El Harchaoui, E. Rijgersberg, H. T. Tops, A. Veenstra y R. J. Ypma, «"Establishing phone-pair co-usage by comparing mobility patterns",» *Science and Justice,* vol. 60, nº 2, p. 180–190, 2020.