Updating Digital Forensics to the 21st Century

Bruno Constanzo[1], María Fernanda Rosales [1], María Fernanda Díaz [2], Belén Álvarez[1], Ana Haydée Di Iorio[1], Marisa Repetto[2]

[1] InFo-Lab, Facultad de Ingeniería, Universidad FASTA, Mar del Plata, Buenos Aires
[2] Facultad de Derecho, Universidad Champagnat
{bconstanzo, rosalesmar, mbelenalvarez, diana}@ufasta.edu.ar
{diazmf22, marisitarepetto}@gmail.com

Abstract. Digital Forensics is a branch of knowledge that works with digital evidence, information stored in a digital storage medium that is relevant to an investigation. For many years, digital forensics knowledge has been built upon foundations that are no longer valid: computers, communication networks, and digital devices have been changing for the past three decades (and more), and so the body of knowledge is slowly becoming stagnant and no longer applicable. This paper discusses several aspects that the authors have identified as slowly drifting from the current reality of digital devices but are still being taught and being used as if they were still relevant. It also discusses some aspects of regulation in Argentina with respect to digital evidence, at the time of writing.

Keywords: digital forensics, good practices guidelines, regulation.

Actualizando la Informática Forense al Siglo XXI

Resumen. La Informática Forense es una rama del conocimiento que trabaja con evidencia digital, información almacenada en un medio digital que es relevante para una investigación. Por años, el conocimiento de informática forense se ha construido sobre fundamentos que ya no son válidos: las computadoras, redes de comunicación, y dispositivos digitales han cambiado durante las últimas tres décadas (y más), y así el cuerpo de conocimiento se está estancando lentamente y ya no es aplicable. Este artículo discute varios aspectos que los autores han identificado como lentamente a la deriva de la realidad de los dispositivos digitales, pero que todavía se enseñan y utilizan como si fueran relevantes. También discute algunos aspectos de la regulación en Argentina al respecto de la evidencia digital, al momento de escritura.

Palabras clave: informática forense, guías de buenas prácticas, regulación.

1 Introducción

Las Tecnologías de la Información y la Comunicación (TICs) han invadido nuestra sociedad moderna a lo largo de los últimos años, al punto que hoy una enorme cantidad de interacciones sociales y actividades de la vida diaria se ven mediadas por la

tecnología. Para brindar algunos ejemplos: WhatsApp es en Argentina el principal servicio de mensajería instantánea[1]; los pagos con billeteras virtuales son cada vez más frecuentes[2]; el uso de boletos electrónicos para el transporte público (ej: tarjeta SUBE, RedBUS, etc), registra el viaje, posición de GPS, fecha y hora, número línea e interno, entre otros datos; el caminar por la vía pública puede resultar en ser registrado por cámaras de videovigilancia, de privados o gestionadas por el estado[3]. Todos estos ejemplos ilustran cómo actividades que no son inherentes al ámbito digital, hoy tienen impacto en sistemas informáticos, y dejan rastros digitales.

En Argentina y el resto del mundo la doctrina especializada y la jurisprudencia están reconociendo a la evidencia digital[4] como un tipo particular de prueba, incluso siendo incorporada en los nuevos Códigos Procesales Penales de varias provincias (Sueiro 2025).

La Informática Forense, la ciencia de aplicación forense dedicada a la adquisición, preservación, análisis, y presentación de evidencia digital, su objeto de estudio. Para dar una breve definición, puede decirse que la evidencia digital es todo dato almacenado en un sistema informático o soporte digital que resulta útil para una investigación (Saín & Azzolín 2017)[5]. Al ser digital, este tipo de evidencia presenta características únicas que la distinguen de otros tipos de evidencia: se pueden hacer infinidad de copias[6]; la evidencia digital es volátil, es decir que se puede degradar[7] o incluso perder con el paso

---

[1] Según datos públicos de consultoras, el porcentaje de uso varía entre el 80% y el 96%, dependiendo cuál se consulte. Ver: sinch "The most popular messaging apps in the world by country" (https://sinch.com/blog/most-popular-messaging-apps-by-country/), GrabOn "WhatsApp Statistics" (https://grabon.com/blog/whatsapp-statistics/) e infobip "WhatsApp Statistics 2025: Market analysis & global usage data" (https://www.infobip.com/blog/whatsapp-statistics).

[2] La Cámara Argentina Fintech publicó en 2023 un resumen de distintas fuentes, junto con un informe de la consultora taquion, que está disponible online: https://camarafintech.org/estudio-de-billeteras-virtuales-2023/.

[3] El Observatorio de Derecho Informático Argentino ha recopilado noticias al respecto del sistema de reconocimiento facial de la Ciudad Autónoma de Buenos Aires, suspendido por órden judicial en 2022. Ver: https://odia.ar/casos/reconocimiento-facial. Discusiones similares se han dado en distintas ciudades del país, por ejemplo Neuquén (https://www.lmneuquen.com/neuquen/videovigilancia-neuquen-experto-la-comparo-la-casa-gran-hermano-n1065544), Mendoza (https://www.mdzol.com/politica/empezaron-probar-las-camaras-seguridad-reconocimiento-facial-inteligencia-artificial-n1372460), y Mar del Plata (https://vencedoresyvencidos.com/la-patrulla-municipal-se-prepara-para-usar-las-body-cam/), con distintos grados de éxito y recepción por parte de la ciudadanía.

[4] A veces también llamada "prueba electrónica" o "prueba digital".

[5] En los primeros borradores de este artículo se había identificado a la definición como (Interpol 2026), sin embargo, una lectura detallada y una investigación de fuentes secundarias y terciarias más rigurosa permitió refinarla, llevando esta definición a (Noblett et al 2000).

[6] Usualmente se indica "copias idénticas al original". Esta frase no es de agrado de los autores, ya que, si algo es idéntico e indistinguible del original en todo sentido y en la máxima expresión de detalle, es imposible distinguir un original de una copia. En el mundo físico las copias presentan algún tipo de degradación, pero esto no sucede en el mundo digital.

[7] La degradación de los objetos digitales no es equiparable a una degradación física, sino que se pierden fragmentos completos de la información con el paso del tiempo.

del tiempo; se dice que es frágil para referirse a que es fácilmente alterable, intencional o accidentalmente; y por último es necesario el uso de herramientas específicas y la aplicación de conocimientos pertinentes para su tratamiento (Di Iorio et al. 2017).

Actualmente nos encontramos con un problema que nace en la informática forense, y se traslada al plano legal normativo: en el año 2026 se sigue definiendo y trabajando cuestiones de esta disciplina como si se tratara de los años 80s. Las computadoras han cambiado sustancialmente los últimos 30 años, especialmente con el avance de los llamados dispositivos electrónicos. La telefonía celular, en particular las conexiones móviles a internet, han tenido un gran impacto en la sociedad y en su cultura al punto que los *smartphones* se han convertido en la principal computadora que utiliza la mayoría de las personas. Ante este escenario cada vez más avasallante, gran parte de la bibliografía, cursos, material de formación, protocolos y guías de "buenas prácticas" en evidencia digital e informática forense ignoran estos cambios y sigue refiriendo a multiplicidad de cuestiones y conceptos como si las últimas décadas no hubieran sucedido, o estos cambios y desarrollos fueran cuestiones aisladas.

El objetivo de este trabajo es plantear una discusión alrededor de los cambios relevantes en el mundo tecnológico, y proponer nuevas definiciones y conceptos, con fundamentación interdisciplinaria tecnológico-legal. La siguiente sección el trabajo profundiza estas discusiones procurando dar contexto teórico, y desarrolla aspectos particulares que pueden resultar problemáticos, con propuestas para mejorarlos. Finalmente, las conclusiones redondean las ideas centrales a criterio de los autores.

2 Discusión y Marco Teórico

2.1 Computadoras y Dispositivos Electrónicos en General

Se entiende por sistema de computación a un conjunto de *hardware* y *software* que persigue un propósito específico, en general el procesamiento y/o la transmisión de información (Stallings 1997). El *hardware* son los componentes físicos que dan funcionamiento al sistema, y el *software* son el conjunto de instrucciones, usualmente organizado bajo la forma de programas, que interactúa con el *hardware* de manera que pueda llevar a cabo su funcionalidad.

Las computadoras modernas son computadoras electrónicas digitales y programables. Cada una de estas palabras conlleva un significado específico:

- Computadora nos indica que es un ente (una máquina) cuyo propósito es realizar cálculos u operaciones matemáticas. En general hoy se distingue en las computadoras el CPU (del inglés *Central Processing Unit*,) como el componente que procesa los datos, a la par de otros componentes que son los que, en su conjunto, denominamos "computadora".
- Electrónica digital se refiere al uso de componentes electrónicos que operan señales digitales[8]. La electrónica digital trata la relación entre datos de entrada y salida binarios, procesados por componentes electrónicos como amplificadores, resistencias, capacitores, y compuertas lógicas, entre otros.

[8] Señales en tiempo discreto con amplitud cuantizada. Es decir, la señal se muestrea con una cierta frecuencia, y el valor de la amplitud se mapea a un conjunto discreto de valores

- Programable indica que el funcionamiento de la computadora no es fijo, y puede cambiarse por medio de un programa, un conjunto de instrucciones simples ejecutadas por un microprocesador, con un objetivo específico, ej: resolver un problema, transformar y/o transmitir datos.

En general a lo largo de este trabajo el término "computadora moderna" se usa para referir a desarrollos de hardware y/o software que se dieron en las décadas del 2000 en adelante, o se popularizó el uso de implementaciones en tiempos recientes. Por supuesto que también hay desarrollos y conceptos de la computación y electrónica de los años 50s, 60s, y 70s que aún hoy se mantienen vigentes contemplando algunos cambios de implementación para adaptarlos al hardware y/o software moderno.

Los principales recursos de un sistema de computación son el procesador o CPU, una memoria principal usualmente llamada RAM (del inglés *Random Access Memory*, memoria de acceso aleatorio), periféricos de Entrada/Salida que permiten a la computadora interactuar con el mundo exterior (monitor, teclado, mouse, módem, placa de red, medios de almacenamiento, etc), y la información de el/los usuario/s del sistema, ya sea en la memoria principal (RAM) o en memoria secundaria (almacenamiento).

Los componentes físicos, el *hardware*, se conectan entre sí a través de un *motherboard* que permite la comunicación entre el procesador, la memoria, y los distintos dispositivos de entrada salida a través de distintos buses de datos: los canales de memoria, los canales PCI Express, Serial ATA, NVME, USB, entre otros[9]. Dependiendo el diseño de la computadora, los componentes pueden encontrarse soldados entre sí, o pueden estar conectados por medio de *sockets* o conectores que permiten el reemplazo de las distintas partes por otras compatibles. En general las computadoras de escritorio suelen ser más flexibles y extensibles, mientras que las *notebooks* y dispositivos móviles suelen inclinarse hacia una integración más estrecha y contar con una mayor cantidad, o la totalidad de sus componentes integrados en una sola placa o chip.

Todas las computadoras modernas utilizan un sistema operativo como interfaz entre el usuario[10] y el hardware, por medio de interfaces gráficas y de programación (Tanenbaum 2009). Estas interfaces son niveles de abstracción que simplifican la problemática de interactuar con distintos dispositivos y tipos de hardware. Por ejemplo, un programa como Word al guardar un documento en un pen drive utiliza las mismas funciones de programación que utilizaría para guardar el mismo archivo en un disco duro, aún cuando se trata de distintos sistemas de archivos, distintos dispositivos, y distintas tecnologías de almacenamiento. El que se encarga de manejar esta complejidad es el sistema operativo, que implementa en sus capas de abstracción de sistema de archivos, y la *Hardware Abstraction Layer* las funcionalidades específicas para cada variable involucrada.

---

[9] Los canales de comunicación mencionados son los que encontraríamos en una computadora actual. Si fuéramos a revisar literatura previa a la década de 2010 (ej: (Tanenbaum 2009)) podríamos encontrar menciones a otros buses de datos y protocolos de comunicación: puerto serie/RS-232, ATA/IDE, ISA, PCI, entre muchos otros.

[10] En general se entiende por usuario a la persona que utiliza la computadora, pero el sistema operativo también considera "usuarios" a los programas en ejecución.

Una de las distinciones que se suele dar en la práctica de la informática forense es hablar de "computadoras" para referirse a equipos de escritorio, *notebooks*, y servidores, mientras que se habla de "dispositivos electrónicos" para referirse a teléfonos y *tablets*, medios de almacenamiento, dispositivos *wearables* o incluso electrodomésticos *smart*. Esta categorización es arbitraria y puede resultar en problemas de interpretación, manejo, y comprensión de los distintos elementos tecnológicos, presentes y futuros.

Distinguir si una cosa es una computadora o no, en el ecosistema tecnológico moderno, pierde sentido ya que la informática y las computadoras invaden cada vez más aspectos de nuestra vida, y se insertan en lugares inesperados. Una cerradura electrónica, el equipo que lee los *tags* (la llave electrónica), es una computadora: tiene CPU, periféricos para realizar la lectura de los *tags*, un sistema operativo y un programa encargado de validar la clave que le presenta un *tag* para determinar si abre o no una puerta. El *tag*, por otro lado, suele ser un elemento pasivo que responde al estímulo del campo magnético del lector, y al ser activado reacciona enviando su clave. Para la clasificación de "computadoras y dispositivos", sin embargo, la cerradura probablemente sería considerada como un dispositivo electrónico, e incluso podría ser clasificada como un elemento que no reviste interés para un caso.

Otro ejemplo son los *smartwatches*, relojes "inteligentes" que llevan consigo un cúmulo de sensores (de movimiento, aceleración, ritmo cardíaco, GPS algunos, entre otros) que les permiten reunir información. En general se los diseña para estar conectados con un *smartphone* por medio de Bluetooth, y volcar en el teléfono toda la información que recopilan. Las características de *hardware* de los *smartwatchs* suelen ser tremendamente limitadas en comparación con otro tipo de computadoras modernas, y por lo tanto su capacidad de almacenamiento. Esto no quiere decir que no lleve información, por ejemplo, podría almacenar una fracción de datos a la espera de volcarla hacia el teléfono con el que está vinculado, una vez que recupere conexión. Pero la principal fuente de evidencia digital en este caso es el teléfono que funciona como *hub* o concentrador, potencialmente no sólo del reloj, sino también de auriculares, anteojos, u otros dispositivos *smart*.

Nuestra propuesta a futuro es que se considere la funcionalidad de cada equipo y determine su interacción con otros dispositivos. Aquellos equipos que orquestan otros dispositivos/periféricos serán los que resulten de mayor interés, y donde debiera enfocarse la atención de los expertos en informática forense. Si no es posible trabajar sobre éstos, entonces podría recurrirse a un análisis de "más bajo nivel"[11] sobre los dispositivos secundarios que puedan haberse encontrado.

2.2 *Smartphones* y dispositivos móviles

Como se indicó en la subsección anterior, debemos tener en cuenta que los *smartphones* y *tablets* son computadoras: cuentan con un CPU, placa de video, módem de la(s) tecnología(s) de comunicación de datos móviles adecuada (3G, 4G, 5G), aceleradores de procesamiento de imágenes y/o inferencia de modelos de IA, memoria RAM, almacenamiento, entre otros componentes. Todo esto suele estar integrado en un SoC

[11] Esta frase refiere a los niveles de abstracción con los que se trabaja en informática. Se plantea un esquema de complejidad desde el "bajo nivel" (procesadores, dispositivos electrónicos, circuitos incluso), y a medida que se agregan capas de abstracción, éstas aíslan y simplifican la información para los niveles superiores, se habla de un "más alto nivel" de abstracción.

(del inglés, *System-on-a-Chip*) o a veces se pueden encontrar en chips separados, dependiendo del diseño de cada dispositivo.

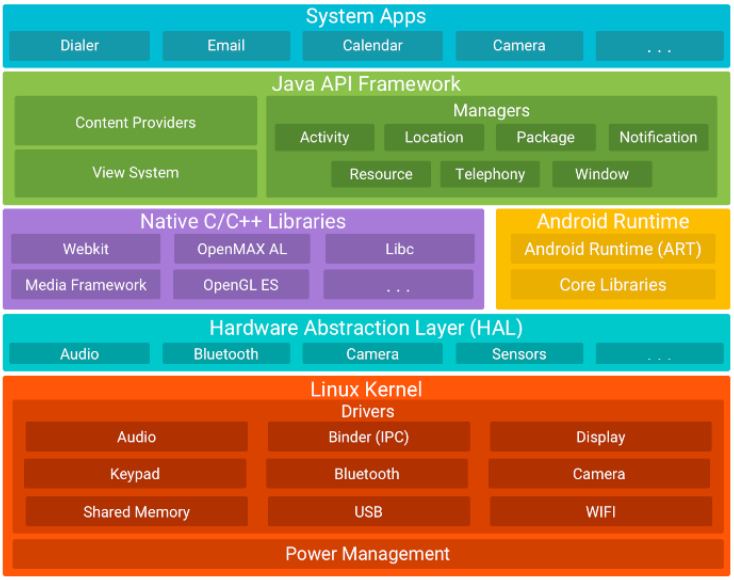

Fig. 1. Capas de abstracción de Android, ubicadas sobre el *hardware* del dispositivo para brindar los servicios del sistema operativo. Adaptado de la *Android Developers Platform* (ADP).

El *software* en los *smartphones* también es complejo. Android es un sistema operativo de código abierto, que utiliza el kernel Linux y lo complementa con distintos componentes propios, *drivers* de dispositivo específicos, y distintas librerías, *runtimes* y APIs[12] para que cada aplicación interactúe con el sistema (ver Fig. 1)

Además, las actualizaciones del sistema operativo suelen incluir cambios en el comportamiento que afectan aspectos propios del análisis forense digital. Uno de los cambios notables en este sentido fue la incorporación del cifrado de sistema de archivos, primero utilizando una clave general (*Full-disk Encryption* o FDE, Android 4.4 y 5, ver (AOSP-a)) y luego con claves por archivo (*File-based Encryption* o FBE en Android 7 y posterior, ver (AOSP-b)). Desde iOS 4 en adelante Apple también incorporó mecanismos de FDE, y luego FBE a sus dispositivos móviles iPhone y iPad[13]. El cambio a *file-based encryption* en particular hace que dejen de tener sentido hablar de "extracciones físicas", debido a que cada archivo pasa a tener una clave de cifrado que le es propia. Esto ocasiona que si tenemos espacio libre que fue asignado previamente a un archivo, este contenido fue cifrado con una clave que ya no se encuentra disponible, y esos bytes son indistinguibles de una secuencia aleatoria. La

[12] API del inglés *Application Programming Interface*, son interfaces de programación que permiten acceder a funcionalidad a través de un protocolo estandarizado.

[13] Apple documenta pocos detalles, pero se pueden consultar las filminas de (Belenko 2014) para seguir la cronología de estos cambios. También se recomiendan los *webinars* de Cellebrite dictados por Heather Barnhart (Mahalik 2021).

ventaja de las extracciones físicas era permitir el *file carving*, y eventualmente recuperar archivos que hubieran sido eliminados, pero esto ya no es posible.

Sin embargo, en protocolos, guías de buenas prácticas, cursos que se dictan a empleados judiciales, miembros de las fuerzas de seguridad, peritos y profesionales en formación para serlo, se sigue hablando de "extracción lógica", "extracción de archivos", y "extracción física", planteándolas como 3 niveles de cantidad y calidad de datos. Esta terminología se deriva de la herramienta UFED de Cellebrite, y no es aplicable a otras herramientas de volcado de información de dispositivos móviles. Estamos entonces ante una situación de doble error: en primer lugar, la terminología nunca fue general, y en segundo lugar ya ni siquiera es aplicable.

Actualmente el mejor nivel de extracción que se puede obtener es el llamado *full-filesystem*, que significa que la herramienta de volcado (sea cual sea) ha logrado hacer una extracción de todos los archivos del dispositivo, accediendo a ellos a través de los mecanismos propios del sistema operativo, descifrando su contenido tal como lo vería una aplicación con los permisos correspondientes en el sistema. Este tipo de extracción tampoco es conducente para realizar *file-carving*, aunque pueden ser viables otras técnicas de recuperación de información que trabajen sobre los archivos extraídos específicamente, como podría ser, por ejemplo, recuperar registros eliminados de una base de datos SQLite[14].

2.3 *File carving* como técnica de recuperación de información

Se conoce como *file-carving* a toda una familia de técnicas de recuperación de datos capaz de reconstruir archivos eliminados sin utilizar las estructuras de datos propias del sistema de archivos[15]. Durante años estas técnicas fueron uno de los pilares de la recuperación de información, pero esta problemática se resolvió rápidamente[16], y el interés migró hacia otras técnicas como el análisis de memoria, o el análisis de aplicaciones específicas, como se da generalmente en dispositivos móviles.

Desde el punto de vista técnico, también ha ido perdiendo relevancia con el paso del tiempo, tanto por las soluciones de cifrado (BitLocker en bajo Windows, FileVault en Mac OS, y LUKS en Linux), así como por el desarrollo de la tecnología de almacenamiento en estado sólido y el comando TRIM. La tecnología Flash, utilizada en los dispositivos de almacenamiento de estado sólido (SSD, del inglés *Solid State Drive*) si bien brinda ventajas de velocidad y rendimiento con respecto a los discos rígidos de platos (HDD, del inglés *Hard Disk Drive*), solamente puede realizar una cantidad limitada de escrituras sobre cada celda que almacena información, ya que en el proceso de escritura el circuito sufre un desgaste que, eventualmente, termina por romperlo.

Durante la primera década del 2000 se desarrollaron estrategias de *wear leveling* (balanceo de desgaste), desacoplando la *logical block address* (LBA, el número de bloque o dirección lógica de un bloque) de su ubicación física en las celdas del

---

[14] Para una breve explicación técnica sobre recuperación de datos en bases de datos SQLite se recomienda ver la conferencia de Valentina Funes en InFoConf 2025 (Funes 2025).

[15] Ver (Pal Memon 2009) y (Constanzo Waimann 2017), que si bien son referencias de hace varios años ya, dan un panorama general del tema en inglés y en español. Desde la década de 2010 en adelante no ha habido grandes desarrollos en esta materia.

[16] PhotoRec es una herramienta de código abierto que permite recuperar archivos mediante *file-carving* y sus resultados lo ubican entre los líderes del mercado (CGSecurity 2024).

dispositivo, necesitando que se establezca un mapeo entre los bloques lógicos y las celdas físicas que los componen[17]. En conjunto también se incorporaron estrategias de *overprovisioning*[18] y *garbage collection*[19]. La última pieza de este rompecabezas es el comando TRIM, que permite al sistema operativo indicarle al SSD que una LBA ya no contiene datos útiles, por ejemplo, al borrar un archivo o liberar espacio en disco. Esto permite al SSD remapear ese LBA, y/o responder de manera determinística como si el bloque se encontrara vacío si se lo intenta leer (Afonin 2025).

Este comportamiento rompe los supuestos básicos de las técnicas de *file carving*, que están basados en el comportamiento de los sistemas de archivos sobre dispositivos HDD que eran comunes en los 80s y los 90s. Debido a la baja velocidad de escritura en este tipo de dispositivos, en lugar de eliminar la información lo que hacen la mayoría de los sistemas de archivos es un "borrado lógico". Este consiste en indicar en un campo de metadatos que el archivo fue eliminado y marcar como libres los bloques asignados, pero sin eliminar o modificar el contenido de los bloques propiamente dichos. En los sistemas operativos que manejan los dispositivos SSD adecuadamente (y esto puede variar por dispositivo y por sistema operativo), además se envía un comando TRIM para indicar al SSD que ya puede disponer de dichos bloques, efectivamente eliminando la información que un proceso de *file carving* hubiera podido recuperar.

Luego de esta explicación, debiera resultar sorprendente que se plantee el uso de *file carving* en una pericia actual. Sin embargo, muchos peritos siguen utilizando este término para referirse genéricamente a técnicas de recuperación de información, incluso cuando se trabaja en condiciones donde el *file carving* en si no es aplicable, ya sean extracciones de dispositivos móviles de tipo lógicas o *full filesystem*, o imágenes forenses de dispositivos SSD donde hay una muy baja probabilidad de efectivamente recuperar información de esta manera[20].

2.4 Regulación de la prueba digital

La regulación de la prueba digital adquiere cada vez más importancia pues, como se ha indicado en distintas instancias en este trabajo, ésta es un medio de prueba con altísima incidencia en los procesos judiciales y distinto a los demás, con características únicas que lo distinguen. Según Sueiro (Sueiro 2025), la prueba digital no se encuentra regulada por los distintos códigos procesales al año 2025, a excepción de las provincias

---

[17] En un anexo de (Constanzo & Waimann 2017) se da una mirada macroscópica sobre el funcionamiento de los dispositivos de estado sólido.

[18] Reservar una porción del espacio de almacenamiento para gestión exclusiva del dispositivo.

[19] El *garbage collector* realiza el blanqueo de páginas/bloques/celdas del dispositivo que fueron marcadas como libres, de manera que siempre haya un determinado porcentaje de la capacidad de almacenamiento listo para ser escrito. Trabaja en conjunto con el sistema de *wear-leveling*, y en general opera sobre el área de almacenamiento reservada para uso interno del dispositivo.

[20] Como excepción, los pen drives, memorias tipo SD, y otros tipos de almacenamiento portátil moderno utilizar tecnología Flash, pero no los mecanismos de *wear leveling*, *overprovisioning*, y *garbage collection*, por lo cual puede utilizarse *carving* sobre éstos. El eventual acceso y preservación a los bloques de acceso reservado es, en teoría, una ventana que mantiene abierta la posibilidad del *carving*, con todos los desafíos pre-existentes pero además una complejidad adicional. Hay escasa bibliografía al respecto, y no hay protocolos establecidos para el

de Corrientes[21], Mendoza[22], Neuquén[23], Río Negro[24], Salta[25], y Tucumán[26] que si incorporan la prueba digital expresamente. Se analizarán en particular los casos de Corrientes y Neuquén.

En el caso de Corrientes hay 5 artículos que Sueiro identifica relativos a la prueba digital, Arts. 216, 217, 218, 219, y 220, cuyo texto indica:

> ***ARTÍCULO 216. Vigilancia de las comunicaciones.*** *Podrá autorizarse el acceso al contenido de comunicaciones a través de la intervención de las terminales o de los medios de comunicación que la persona utiliza habitual u ocasionalmente.*
>
> *Las empresas que brinden el servicio de comunicación respectivo deberán posibilitar el cumplimiento inmediato de la diligencia, bajo apercibimiento de desobediencia.*
>
> ***ARTÍCULO 217. Vigilancia remota sobre equipos informáticos.*** *Podrá autorizarse el acceso remoto al contenido de ordenadores, dispositivos electrónicos, sistemas informáticos, bases de datos o instrumentos de almacenamiento masivo de datos informáticos, a través de un software que lo permita o facilite.*
>
> *El juez podrá exigir al fiscal que precise la forma en que se procederá al acceso y captación de los datos o archivos informáticos, así como la identificación del software mediante el cual se ejecutará el control de la información.*
>
> ***ARTÍCULO 218. Vigilancia acústica.*** *Podrán autorizarse escuchas y grabaciones de conversaciones privadas que tengan lugar fuera del domicilio de cualquiera de los interlocutores, a través de medios técnicos.*
>
> ***ARTÍCULO 219. Vigilancia a través de dispositivos de captación de imagen.*** *Podrá autorizarse la obtención y grabación de imágenes de una persona en espacios públicos, a través de cualquier medio técnico.*
>
> ***ARTÍCULO 220. Vigilancia por seguimiento y localización****. Podrá autorizarse el seguimiento y localización de una persona, mediante la utilización de dispositivos o medios técnicos de seguimiento y localización.*
>
> *El juez podrá exigir al fiscal que especifique el motivo de la vigilancia y el medio técnico que será utilizado.*

Estos artículos son parte del Título III sobre Técnicas y Medidas Especiales de Investigación, dividido en dos capítulos: Capítulo 1. Técnicas especiales de investigación; y Capítulo 2. Medidas especiales de investigación. Según el art. 213 se consideran medidas especiales de investigación las medidas de vigilancia sobre una persona ejecutadas de modo no ostensible, sean de vigilancia de las comunicaciones,

---

[21] Código Procesal Penal de Corrientes, Ley 6518.

[22] Código Procesal Penal de Mendoza, Ley 6730.

[23] Código Procesal Penal de Neuquén, Ley 2784.

[24] Código Procesal Penal de Río Negro, Ley 5020.

[25] Código Procesal Penal de Salta, Ley 7690.

[26] Código Procesal Penal de Tucumán, sancionado el 20 de octubre de 2016 y publicado en el Boletín Oficial el 17 de noviembre de 2016.

sobre equipos informáticos, acústica, por captación de imagen o mediante seguimiento y localización.

En líneas generales estos artículos no regulan la evidencia digital como objeto, sino el modo de acceder a la información y de obtenerla, en el marco de un proceso penal de investigación de delitos de especial gravedad.

En particular los artículos 216 y 217, vistos a la luz de lo que se indicó anteriormente de los *smartphones*[27], son prácticamente equivalentes. El art. 216 al indicar que se podrá intervenir el terminal de las comunicaciones es redundante con el art. 217. La diferencia, sutil, que el art. 216 especifica que se puede requerir a las prestadoras de servicio la intervención de las comunicaciones. El Art. 217 si bien menciona el acceso remoto al contenido, no indica cuestiones sobre la copia, adquisición, y/o preservación de los datos a los que se acceda. También, al referirse específicamente al acceso remoto, parecería no dejar margen al acceso local o directo a la información contenida en una computadora o medio tecnológico, es decir, el trabajar directamente sobre los equipos o dispositivos de interés.

Los artículos 218, 219, y 220 en cambio se refieren a elementos que son almacenadas como datos digitales, porque pueden provenir de sistemas informáticos. Sin embargo, el objeto del que versan (la acústica, imagen, o localización) no son inherentemente digitales, sino cuestiones del mundo físico reflejadas en medios digitales como un detalle de implementación. Estas cuestiones también podrían reflejarse en medios analógicos (ej: grabaciones en discos de vinilo o casettes, fotografías de rollo, o registrar la ubicación de una persona en un mapa en papel), con la única diferencia de la dificultad de obtención de este tipo de información en dichos medios.

El Ministerio Público Fiscal de la Provincia de Corrientes ha publicado un Protocolo de Actuaciones para Informática Forense[28], que podría considerarse complementario a la ley provincial. Este protocolo adolece de algunas carencias importantes, a destacar: en ningún momento define qué es la evidencia digital; detalla procedimientos específicos y particulares, pero no brinda cuestiones generales aplicables en otros contextos; confunde a la evidencia digital (contenido) con su soporte físico (contenedor); no especifica verificaciones de integridad aplicables sobre la evidencia digital. Finalmente, según el art. 221 de la ley citada, al regular sobre registros y cadena de custodia, señala que *"las medidas del presente Capítulo serán registradas mediante un medio técnico idóneo que asegure la legitimidad de la ulterior valoración de la información obtenida. Los registros serán conservados por el fiscal, quien dispondrá las medidas correspondientes para asegurar su fidelidad e inalterabilidad y para resguardar la cadena de custodia"*.

Ni la ley ni el protocolo definen qué es la evidencia digital. En consecuencia, resultará difícil determinar qué constituye evidencia digital, consintiendo así que se incluya cuestiones que no son digitales, o se ignore evidencia digital por no haberla considerado.

No regular la evidencia digital a través de un marco normativo genérico y el desarrollo de principios y garantías procesales básicas conllevará a que sólo se

---

[27] Léase, que los *smartphones* son "computadoras de bolsillo".

[28] Actuación para Informática Forense UDT-UFIE del Ministerio Público Fiscal (Acdo. N° 14/16, pto. 14° – 02/06/2016), listado en el sitio del Poder Judicial de Corrientes, online: https://www.juscorrientes.gov.ar/protocolos/.

contemplen en la práctica judicial las medidas específicas que han sido enumeradas, y no se cumpla con procedimientos básicos y aplicables a cualquier tipo de evidencia digital en el marco del debido proceso constitucional.

Más grave aún es la confusión de la evidencia digital con su soporte físico. Todas las medidas de integridad que detalla el protocolo citado son exclusivamente para los elementos físicos que almacenan la evidencia digital[29], en particular por la redacción parecería indicar que se pretende el bloqueo de puertos de comunicación y suministro de energía de computadoras de escritorio, *notebooks*, y/o teléfonos, aunque no especifica. En el punto 5) k) del mencionado protocolo, se indica:

> *No se podrá asegurar la integridad de la evidencia digital (por lo tanto se pierde la posibilidad de utilizar el medio de prueba) si el material informático tiene rotos los precintos al momento de ser entregado, siempre que no esté descripta en el expediente judicial la intervención realizada utilizando una metodología y herramientas forenses por profesionales calificados.*

Nuevamente se advierte que al momento de redactar este protocolo sólo se tuvieron en cuenta los soportes físicos de la evidencia digital, sin mencionar la utilización de hashes criptográficos para verificar la integridad de las copias forenses de la evidencia digital (propiamente dicha) que pueda ser adquirida en un procedimiento.

Por su parte, el Código Procesal Penal de la provincia de Neuquén en cambio tiene un enfoque genérico, pero técnicamente correcto de la evidencia digital. Si bien Sueiro identifica los Arts. 150, 151, y 153, estos versan en general sobre comunicaciones, interceptaciones telefónicas, e información digital respectivamente, y a criterio de los autores solamente el Art. 153 trata en concreto sobre la evidencia digital:

> ***Artículo 153 Información digital.*** *Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, se procederá a su secuestro, y de no ser posible, se obtendrá una copia. O podrá ordenarse la conservación de los datos contenidos en los mismos, por un plazo que no podrá superar los noventa (90) días. Quien deba cumplir esta orden deberá adoptar las medidas necesarias para mantenerla en secreto.*
>
> *También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota. A cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, podrá requerírsele la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos.*
>
> *La información que no resulte útil a la investigación, no podrá ser utilizada y deberá ser devuelta, previo ser puesta a disposición de la defensa, que podrá pedir su preservación. Regirán las limitaciones aplicables a los documentos.*

---

[29] Cita textual de Protocolo de Actuaciones para Informática Forense – Ministerio Público Fiscal de la Provincia de Corrientes: *"4.c) Preservación de evidencia digital. Se deberá utilizar precintos o fajas de seguridad al momento del secuestro de los elementos informáticos y todo medio necesario para garantizar la autenticidad e integridad de los elementos secuestrados. A tal fin se deben seguir los lineamientos indicados en el "Instructivo para la utilización de etiquetas de seguridad sobre dispositivos informáticos" que complementa el presente protocolo."*. Dicho instructivo refiere al etiquetado de elementos físicos, e indica que deben taparse con las etiquetas todos los conectores de energía o que permitan acceder al dispositivo.

La redacción es sintética pero muy pertinente: habla en general de dispositivos informáticos, de manera que cubre tanto los dispositivos existentes en la actualidad como aquellos que puedan existir en el futuro; menciona "información útil a la investigación", que coincide con la definición de evidencia digital dada; refiere tanto al secuestro de los soportes físicos, como a la obtención de copias de la evidencia digital, y los pedidos de preservación. Al tener una redacción sencilla y prolija, esta ley promulgada en 2012 sigue plenamente vigente desde los aspectos técnicos propios de la informática forense, aún frente a los cambios tecnológicos posteriores a su redacción, precisamente por cubrir aspectos generales de manera sólida.

Una particular mención merece, a esta altura del desarrollo tecnológico, la redacción sobre las copias de la información como excepción frente a la imposibilidad del secuestro de los dispositivos de almacenamiento. Se reitera en este punto la importancia de centrar el objeto de estudio en el contenido (la información digital) y no el contenedor (dispositivo de almacenamiento), salvo para aquellos casos en el que sea el contenedor en sí mismo un elemento fundamental para el análisis forense.

2.5 Mitos y rituales: descontaminación de discos

Como último punto del trabajo, y en relación con algunos temas que se mencionaron en la sección 2.3, se abordará el tema de "descontaminación de discos" (a veces referido por su nombre en inglés *"disk wiping"*). Este tema está siendo mencionado cada vez con más frecuencia en planteos y discusiones judiciales, y también ha aparecido en protocolos y normas, por ejemplo, el protocolo de evidencia digital del Ministerio de Seguridad (MinSeg 2023). Este concepto resulta problemático porque los dispositivos de almacenamiento no funcionan de ninguna manera en la cual esta práctica tenga sentido, y su incorporación e institucionalización en normas y protocolos implica introducir en la estandarización de la práctica forense un error que no tiene base científica, bajo la única justificación de "es lo que indica el protocolo".

Se puede rastrear en foros de discusiones especializados de informática forense[30] al menos tres razones que intentan justificar esta práctica:

- La primera justificación es que evita el planteo de nulidades antes pregunta de la contraparte si los discos fueron "descontaminados". Debido a que lleva más tiempo y esfuerzo al perito explicar cómo funcionan los medios de almacenamiento y por qué es imposible que se de dicha situación, se opta por "perder tiempo en el laboratorio para ahorrarlo en el juzgado".
- Algunas herramientas forenses guardan información en carpetas temporales genéricas, y pueden filtrar información por fuera cada caso.
- La eliminación segura de información como medida de protección de datos, especialmente en entornos empresariales sujetos a regulaciones estrictas y con deber de *compliance*.

La primera situación perpetúa un procedimiento que no tiene sentido para "ahorrar tiempo". La solución implicaría que no se lugar a planteos ajenos a la ciencia y los métodos de la informática. Un medio de almacenamiento debe, por definición,

[30] Ver discusión en los foros de Forensic: https://www.forensicfocus.com/forums/general/why-should-i-wipe-a-drive-before-putting-evidence-on-it/ y reporte de Forensium sobre *leaks* de Encase v7 https://www.forensium.com/Web_log/3_EnCase_7.x_Evidence_Leakage.

almacenar la información que se le envía sin cambios ni modificaciones. Si la presencia de datos anteriores afectara de alguna manera los datos que se pretenden almacenar, no podría ser, por definición, un medio de almacenamiento.

En el segundo planteo lo que se debiera "descontaminar" no es el medio de almacenamiento donde se harán copias forenses, sino las estaciones de trabajo de los peritos. Implica tomar medidas operativas para subsanar un fallo conocido de una herramienta específica. Si no se utiliza dicha herramienta, ni hay razones para sospechar que podría darse una situación similar, se está instaurando un "ritual" que busca prevenir una situación que no se va a presentar. Por otro lado, si las herramientas tienen errores, radica en sus desarrolladores la responsabilidad de resolverlos.

El último caso es el único que se puede considerar como una justificación válida: se elimina la información de un caso luego de finalizadas las actuaciones para cumplir con las reglamentaciones de protección de datos. Lo importante en esta situación es remarcar el *cuándo* y el *por qué*. En una operatoria normal, la información de un caso se elimina luego que se ha terminado de trabajar con él, dejando libre el espacio en el medio de almacenamiento. Si el dispositivo fuera a ser decomisado, entonces el *wiping* tiene sentido, pero en otro caso la normal operatoria de escribir nueva información eliminará naturalmente cualquier información previamente almacenada en el medio[31].

3 Conclusiones y trabajo futuro

A lo largo de este trabajo se han expuesto disitntos aspectos que deben actualizarse en el ejercicio actual de la informática forense en Argentina, tanto desde los aspectos del conocimiento, procedimentales tecnológicos, y de la regulación desde lo legal de la prueba digital. Varios aspectos quedaron sin mencionar si quiera en este trabajo, por nombrar algunos: la correcta utilización de hashes criptográficos y el extremadamente bajo riesgo de colisiones; el uso de otros tipos de hashes, tales como de similitud y perceptuales; el análisis forense de memoria RAM, tanto en computadoras como en *smartphones*; el uso de Inteligencia Artificial en el análisis y procesamiento de evidencia digital. Este listado no es exhaustivo, simplemente ilustra algunas cuestiones que son consideradas de interés por los autores, pero por extensión y tiempos no pudieron ser cubiertos en este artículo.

Al momento de escribir este trabajo, la provincia de Catamarca ha incluido también la prueba digital su código civil, entre otras reformas[32]. Una lectura rápida ha permitido identificar algunos artículos en esta nueva ley que son, cuanto menos, problemáticos. En el afán de "incluir la inteligencia artificial generativa en el proceso", se han incluido cuestiones en artículos de la prueba digital que pueden ser cuestionadas, tanto desde los aspectos legal e informático.

Se debe continuar el trabajo de actualizar el ejercicio y la reglamentación de la informática forense y evidencia digital, en Argentina y el resto del mundo. La actualización del conocimiento tecnológico es desafiante por el constante desarrollo de

[31] Tener en cuenta las consideraciones hechas sobre almacenamiento Flash, que naturalmente elimina información, o el uso de sistemas de archivos con cifrado en los que la eliminación de la(s) clave(s) de cifrado resulta en la pérdida de los datos almacenados en el mismo.

[32] Código Procesal Civil y Comercial de Catamarca, Ley 5925.

la tecnología, pero la cuestión pericial y el auxilio a la justicia lo demandan como un imperativo ético y moral que debe responderse.

Referencias

Afonin, O. (2025) *What TRIM, DRAT, and DZAT Really Mean for SSD Forensics*. Blog ELCOMSOFT. https://blog.elcomsoft.com/2025/06/what-trim-drat-and-dzat-really-mean-for-ssd-forensics/ (consultado el 12 de abril de 2026).

Android Developers Platform (ADP). *Platform architecture*. Platform, Technology. https://developer.android.com/guide/platform (consultado el 14 de abril de 2026).

Android Open Source Project (AOSP). *Full-disk encryption*. Documentation, Security. https://source.android.com/docs/security/features/encryption/full-disk (consultado el 14 de abril de 2026)

Android Open Source Project (AOSP). *File-based encryption*. Documentation, Security. https://source.android.com/docs/security/features/encryption/file-based (consultado el 14 de abril de 2026)

Belenko, A. (25-26 de noviembre 2014). *iOS Forensics with Open-Source Tools* [Workshop]. BlackHat Regional Summit Sao Paulo 2014, Sao Paulo, Brasil. https://blackhat.com/sp-14/speakers/Andrey-Belenko.html (consultado 16 de abril de 2026).

CGSecurity (2024). *TestDisk & PhotoRec* (versión 7.2) [software informático]. https://www.cgsecurity.org/wiki/PhotoRec.

Constanzo, B., Waimann, J. (2017). File y Data Carving. En *El Rastro Digital del Delito* (p. 400-478). Universidad FASTA.

Di Iorio, A. H., Castellote, M. A., Constanzo, B., Curti, H., Waimann, J., Alberdi, J. I., Cistoldi, P. A., Giaccaglia, M. F., Greco, F., Iturriaga, J. I., Lamperti, S. B., Nuñez, L., Podestá, A., Ruiz de Angeli, G. M., Trigo, S. (2017). *El Rastro Digital del Delito: aspectos técnicos, legales y estratégicos de la infomrática forense.* Universidad FASTA.

Funes, V., Constanzo, B. (28 de noviembre 2025). *SQLite y WhatsApp* [Conferencia]. InFo-Conf 2025, Jujuy, Argentina. https://www.youtube.com/watch?v=CaMTGzO57AE (consultado 16 de abril 2026).

Interpol. *Análisis forense digital*. Interpol. https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital (consultado el 15 de abril de 2026).

Mahalik, H. (2021) *Fundamentals Matter - Part 2* [Webinar online]. Cellebrite. https://cellebrite.com/en/resources/webinars/part-2-fundamentals-matter-understanding-the-available-data-collection-methods-offerings/ (consultado el 16 de abril de 2026).

Ministerio de Seguridad. *Resolución 232/2023*. Resolución publicada en Boletín Oficial. https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-232-2023-382307/texto.

Noblett, M., Pollit, M., Presley, L. (2000). *Recuperación y examen de evidencia en informática forense*. Revista Ciencias de la Comunicación Forense, vol 2, N° 4, Oficina Federal de Investigaciones (FBI).

Pal. A, Memon. N. (2009). *The evolution of file carving*. IEEE Signal Processing Magazine, 26(2), 59 – 71. https://doi.org/10.1109/MSP.2008.931081.

Sueiro, C. C. (2025). La prueba digital y su incorporación al proceso penal. En *Tratado de Prueba Electrónica* (p. 235-276). La Ley, Thomson Reuters.

Stallings, W. (1997). *Sistemas Operativos*. Prentice Hall.

Tanenbaum, A. S. (2000). *Organización de computadoras: un enfoque estructurado, 4ta edición*. Prentice Hall.

Tanenbaum A.S. (2009). *Sistemas Operativos Modernos, 3ra edición*. Prentice Hall.