InFo-Cyber. Journal of Cybersecurity and Digital Forensics.
Volumen 1, Número 1. Año 2026. ISSN: en trámite.
https://revistas.ufasta.edu.ar/index.php/InFoCyber/index

La informática forense, una disciplina en constante evolución

Gustavo Daniel Presman

Ingeniero Electrónico egresado en 1987 de la Facultad de Ingeniería UBA, cuenta con un Máster en Tecnologías de la Información y las Comunicaciones del Programa GADEX realizado en España en 2011. Posee certificaciones Internacionales en tópicos forenses: CCE, EnCE, MCFE y CNPFA y es miembro de HTCIA y otras asociaciones internacionales de Informática Forense. Cuenta con más de treinta años de actividad profesional privada en las áreas de Informática y redes de computadoras.

En su amplia trayectoria fue Perito Judicial en Informática y electrónica con actuación en la Suprema Corte de Justicia, Cámaras nacionales y provinciales, consultor de la OEA en el programa OEA Cyber y de INTERPOL en el programa GLACY+ y miembro del Programa Nacional contra la Criminalidad Informática. Actualmente es consultor de UNODC en el programa global en Cibercrimen y expositor frecuente en todo Latinoamérica en conferencias sobre tópicos forenses.

Nota técnica

Recibido: 14-04-2025 Aceptado: 02-10-2025 . Publicado: 03-03-2026

Universidad FASTA. Facultad de Ingeniería; Mar del Plata, Argentina.

Cuando comencé a transitar el camino del peritaje informático, hace 30 años, prácticamente no existía tal especialidad criminalística. Todo se hacía de una manera empírica y poco se pensaba en cuanto a la preservación y tratamiento de la evidencia digital.

En esta nota voy a transitar fugazmente el camino que recorrí hasta nuestros días y aventurar qué es lo que se viene.

Génesis

En el principio, todo se resumía en ver qué había en una computadora e imprimirlo para agregarlo en un expediente de papel. El desconocimiento tanto de los peritos como de los operadores judiciales generaba una muy baja comprensión de esta prueba, que generalmente no era considerada y terminaba siendo dejada de lado. Hacía muy pocos años que esta disciplina había comenzado a ser valorada, sobre todo en Estados Unidos e Inglaterra.

Extraíamos y resguardábamos en un medio alternativo solo registros informáticos visibles. No teníamos en cuenta objetos eliminados hasta que empezaron a aparecer las primeras aplicaciones que permitían copiar todo el disco, incluyendo las áreas no controladas por el sistema operativo, como el espacio no asignado y el espacio sin particionar. Ello nos fue permitiendo recuperar, en algunos casos, archivos completos que habían sido borrados por acción positiva del usuario y que ya no se encontraban en la papelera de reciclaje o eran accesibles por medio del sistema operativo.

Esta capacidad comenzó a ser cuestionada fuertemente por los operadores judiciales al no poder comprender su origen ni, sobre todo, garantizar que provenían de donde el perito decía que los había obtenido, algo que también nos resultaba difícil de explicar a nosotros los peritos.

Es allí donde tuvimos que empezar a aprender cómo comunicarnos con los operadores judiciales, más allá de los aspectos procesales, para poder explicarles en lenguaje llano a qué respondían nuestros hallazgos y por qué los considerábamos válidos.

La irrupción en la informática forense de las funciones de *hash* lo cambió todo. La aparición de los digestos matemáticos como mecanismo de validación permitió asegurar la integridad de los registros informáticos y garantizar que aquella evidencia digital, inherentemente intangible, que se incorporaba en un proceso judicial podía ser validada en cualquier momento y asegurar que se trataba de la misma, de manera fehaciente.

El uso de las funciones de *hash* generó un ordenamiento en nuestra actividad, ya que los operadores judiciales empezaron a escuchar y de a poco entender para qué servía. En términos procesales, les dio una herramienta para conceptualizar y poder, de alguna forma, encajar esa evidencia digital en sus procesos.

La Edad de Oro

La aparición de las imágenes forenses fue un hito en la profesión. Hacer una copia completa del contenido de un dispositivo de almacenamiento, "bit a bit", "bloque a bloque" y a nivel físico, ya nos permitía tener visibilidad en las áreas en las que el sistema operativo normalmente no tiene acceso y, como broche de oro, una o dos funciones de Hash para contrarrestar los eventuales planteos por colisiones.

Realizar imágenes forenses o copias forenses pasó a ser una tarea cotidiana de los peritos que hasta empezó a ser ordenada, con lujo de detalle y variadas denominaciones como "clonado" o "copia espejo", por los operadores judiciales al plasmar el cuestionario pericial.

Comenzaron a aparecer copias forenses de todo tipo de dispositivos de almacenamiento, tales como discos duros, *pendrives* y discos ópticos, que combinadas con las nuevas herramientas de "uso forense", llevaron nuestra actividad a otra dimensión.

Ahora era posible explorar el contenido que antes era inaccesible y llevar a cabo búsquedas en lugares inesperados donde podía existir evidencia que el usuario desconocía o que voluntariamente depositaba en esas áreas para dificultar su hallazgo.

Un nuevo ingrediente comenzó a interesar al operador judicial a pesar de resultarle, en ocasiones, confuso: los metadatos, esos datos indirectos que permiten inferir algunos aspectos adicionales al contenido de un archivo y que en el ecosistema actual resultan una fuente de evidencia a tener en cuenta. Las imágenes forenses que conservan metadatos internos y externos, sumados a las aplicaciones de análisis forense con capacidad de identificarlos y procesarlos, llevaron a la prueba digital a un nivel de desarrollo que antes no había existido.

Las copias forenses se pueden realizar de manera directa extrayendo el dispositivo de almacenamiento o indirecta sobre el mismo equipo que lo contiene, tomando los recaudos necesarios para evitar la contaminación digital.

Es en estos tiempos que la informática forense encontró una nueva superficie de desarrollo en el ámbito corporativo.

El incipiente aumento de los incidentes informáticos en las diferentes organizaciones privadas comenzó a requerir, en las áreas de auditoría interna, de informes técnicos que necesitaban de la participación de un perito informático, ya sea para

sumarios internos o cumplimiento con organismos externos.

La recolección y preservación de evidencia digital, frecuentemente con el complemento de un acta notarial y la producción de dictámenes técnicos, comenzó a ser frecuente a nivel corporativo, tanto para la toma de decisiones internas como para una eventual judicialización del incidente, lo que requeriría cumplir con las buenas prácticas existentes en el tratamiento de la evidencia digital para soportar los eventuales planteos en sede judicial.

Naturalmente, en estos tiempos, el uso de dispositivos informáticos estaba masificado, por lo que su impacto en la vida cotidiana ya era muy alto, trasladándose ese impulso no solo a hechos delictivos, sino también a situaciones controversiales que se resolvían en el ámbito civil, por lo que el interés en nuestra profesión empezó a crecer tanto en la oferta de profesionales interesados como en la demanda judicial y ahora también la corporativa.

La ejecución de imágenes forenses se consolida en esta época como un procedimiento repetible y totalmente auditable.

Las herramientas forenses, en su gran mayoría, son desarrolladas como "de profundidad", es decir, que pueden penetrar en las entrañas del sistema operativo y de la estructura física de los dispositivos de almacenamiento, exigiendo una sólida preparación y conocimiento de los peritos informáticos.

Es en estos tiempos cuando empiezan a aparecer diversos documentos para ordenar nuestra actividad, como guías de trabajo, protocolos y normas que aún en nuestros días resultan necesarios, pero a la vez en ocasiones colisionan entre sí, no solo por sus requisitos, sino también por el vertiginoso avance de la práctica forense informática.

La Revolución industrial

Posiblemente el salto cualitativo y cuantitativo en nuestra especialidad se dio con la irrupción de los teléfonos celulares. Esos dispositivos móviles muy rápidamente evolucionaron de ser una versión desconectada de los teléfonos fijos a grandes repositorios de información personal. Producto de la proliferación geométrica de aplicaciones móviles que generan y procesan información, estos dispositivos cambiaron definitivamente el paradigma de la extracción, preservación y tratamiento de la evidencia digital.

En primer lugar, ya no resulta posible, como en las imágenes forenses, realizar una copia forense en los términos en que se encuentra definida, ya que no es posible extraer el "dispositivo de almacenamiento" ni iniciar el teléfono con un sistema operativo alternativo que impida las marcas de tiempo sobre su contenido. Por esta razón, al hablar de dispositivos móviles, el término apropiado es el de "extracción forense".

Para mayor complejidad, no existe una única forma de extracción forense de un teléfono celular y no todas las formas de extracción forense están disponibles en todos los celulares.

La extracción forense de un celular primero requiere contar con el PIN o patrón de desbloqueo, algo que frecuentemente y sobre todo en casos judiciales no tenemos, lo que deriva en disponer de herramientas que puedan obtener dicho código o acceder sin el mismo.

Estas herramientas, de muy alto costo, solo están disponibles en contadas ocasiones y, así y todo, no garantizan poder desbloquear el dispositivo y menos en un plazo conocido.

Una vez que se accede a contenido, dependiendo de la marca y modelo específico, se podrán realizar extracciones de tipo lógico, físico y de sistemas de archivo en general o algunas extracciones particulares y puntuales que en su mayoría requieren de la introducción de un agente, previo a la preparación y acondicionamiento de ciertas configuraciones en el dispositivo móvil.

Las distintas extracciones forenses constituirán la materia prima que permitirá posteriormente, mediante el análisis, obtener los artefactos forenses que podrían estar presentes en algún tipo de extracción y ausentes en otras.

El inconmensurable universo de marcas y modelos de teléfonos deriva en que las herramientas forenses para la extracción no tengan capacidades para todos ellos, pudiendo en algunos casos realizar extracciones más limitadas que en otros, razón por la cual algunos artefactos forenses aparecen al analizar algunas extracciones y en otras no.

Un aspecto crítico de la extracción de teléfonos celulares es que, para lograr su cometido, las aplicaciones forenses requieren que el dispositivo sea puesto en un modo de funcionamiento que generalmente se utiliza para propósitos de servicio técnico y que habilita la comunicación y transferencia de datos, permitiendo que las herramientas dialoguen con el dispositivo.

Estos métodos de acceso descritos tienen un alto grado de interacción perito-aplicación-dispositivo por lo que difícilmente las extracciones forenses de teléfonos celulares son repetibles en idénticas condiciones, lo que, sumado a que ciertas técnicas de acceso son irreversibles y de alto riesgo, deriva en un desafío auditar con posterioridad dichas extracciones.

Este escenario demanda peritos muy calificados para tomar

decisiones correctas al momento de la extracción, favoreciendo la mayor extracción de artefactos forenses y limitando los riesgos que amenazan la existencia de la evidencia misma.

Un capítulo aparte merece la evolución en las técnicas de análisis de los artefactos forenses de dispositivos móviles.

La enorme cantidad de aplicaciones móviles que almacenan sus registros en diferentes ubicaciones y formatos requiere que el software de análisis forense sea capaz de extraer e interpretar esos registros y formatos, generalmente incrustados en bases de datos, para poder acceder y mostrarlos con una visualización entendible a todos esos bits que constituyen la "jungla de artefactos".

La conjunción de las técnicas de extracción y análisis requiere herramientas con una base muy fuerte y dinámica de investigación y desarrollo, por lo que las herramientas más completas son licenciadas, quedando un nicho muy pequeño para iniciativas de *software* libre, básicamente destinado a la decodificación e interpretación de artefactos.

Las herramientas de uso forense comienzan a mutar del modelo de profundidad al modelo de artefactos, donde el procesamiento de las extracciones permite la clasificación e interpretación del contenido, presentándolo de una manera mucho más amigable y acelerando las investigaciones.

Teniendo en cuenta el sinnúmero de aplicaciones que aparecen continuamente, así como las actualizaciones de las existentes, la cantidad de artefactos a procesar demanda que la herramienta forense requiera permanentes actualizaciones para auxiliar al perito informático. Las herramientas comienzan a incorporar IA para algunas tareas de reconocimiento, en especial analizando imágenes y conversaciones.

Es durante esta época donde la evidencia digital de almacenamiento crece enormemente, no solo en capacidades, sino en la diversificación de dispositivos que la contienen, dando origen al Internet de las cosas (IoT).

Indudablemente, el escenario ha cambiado sustancialmente al planteado para la edad de oro

El rol del perito Informático

Para analizar cómo ha cambiado el rol del perito informático en estos años, voy a centrarme en el fuero criminal y correccional.

Dependiendo de la jurisdicción, el sistema penal puede ser inquisitivo o acusatorio. A nivel federal, en la República Argentina, el sistema predominante es el inquisitivo, donde existe la figura del perito oficial, un miembro de fuerzas de la ley, fuerzas de seguridad o poder judicial que conduce la experticia, y las partes pueden incorporar peritos de control, comúnmente llamados peritos de parte.

En este sistema, la pericia se realiza conjuntamente entre todos los peritos y el rol del perito de parte es eminentemente pasivo. Sin perjuicio de ello, los peritos de parte pueden sugerir metodologías, aportar recursos y formular las observaciones que consideren convenientes, pudiendo suscribir un informe conjunto o presentando uno propio.

De acuerdo con el código procesal penal nacional vigente en nuestro país, el perito debe tener un título universitario habilitante en la materia. Esto se exige para los peritos de parte, no ocurriendo mayormente para los peritos oficiales donde esta exigencia es suplantada por su pertenencia al organismo oficial. Esta situación ha generado, en ocasiones, planteos en múltiples expedientes judiciales a través de los años.

La irrupción del sistema acusatorio ha presentado un desafío a los distintos roles de perito y a la forma en que expiden sus dictámenes.

En el sistema acusatorio desaparece el concepto de perito oficial, ya que este sistema promueve la "igualdad de armas" entre los órganos fiscales que llevan la investigación y las partes, defensa y eventual querella, ambas sustentando sus teorías del caso apoyadas por sus peritos.

Por lo expresado, ya no existirían sesiones periciales conjuntas, sino que cada parte contaría con la misma evidencia para producir su dictamen, exceptuando aquellas operaciones de obtención y extracción que, por lo explicado anteriormente, requieren de un mayor control ante la eventual irreversibilidad de las acciones técnicas.

Una característica relevante del sistema acusatorio es la oralidad, es decir, que los peritos, por más que confeccionemos informes técnicos escritos, los mismos tienen que ser detallados en las audiencias orales que a tal fin se designen.

En las audiencias de juicio oral, el perito va a ser examinado por la parte que lo propuso para que exponga los hallazgos y conclusiones, basado en su teoría del caso, pero luego la parte contraria realizará el contraexamen, donde intentará desacreditar al perito y sobre todo al trabajo realizado. Este contraexamen representa un desafío para el perito informático, el que usualmente no está preparado para la mecánica de ese interrogatorio que frecuentemente tiene un tono agresivo y deberá soportar esos embates intentando hacerle "pisar el palito", sobre todo a los peritos con poca experiencia en juicios orales.

EL FUTURO

Mientras estás leyendo este artículo, la tecnología está avanzando y la informática forense debe acomodarse y dar respuesta a estos cambios.

Sin duda, irán apareciendo nuevas fuentes de evidencia digital con mayor capacidad y diversidad de almacenamiento, lo cual requerirá de mayores recursos para almacenar y sobre todo para procesar altos volúmenes de evidencia digital.

Posiblemente veamos la migración del procesamiento local hacia la nube con todos los desafíos que esto conlleva, sobre todo en la privacidad y el control de acceso que deberá ser administrado y documentado con nuevos registros de cadena de custodia adecuados a la normativa que necesariamente deberá acompañar.

Un actor relevante en los próximos tiempos será la IA. Por un lado, su incorporación al proceso pericial permitirá procesar y analizar casos más rápidamente, aunque será necesario evaluar, sobre todo al principio, la tasa de error y los falsos negativos mediante la intervención, siempre necesaria, del perito.

Por otro lado, tendremos que considerar, al analizar el contenido de la evidencia digital, en mi opinión, que el desafío principal en los peritajes informáticos vendrá de la mano del uso consciente de la inteligencia artificial.

Todos los días vemos aparecer diversas IA con capacidades para producir contenido que simula ser real. Imágenes, videos y audios pueden fraguarse como realizados por personas humanas y no falta nada para que puedan aparecer registros y acciones dentro de un sistema informático creados por medio de IA y que no respondan a un usuario real.

¿Podremos ser capaces de establecer pericialmente si un contenido digital corresponde a una acción real del usuario o fue generado por una IA? El tiempo dirá si la informática forense está a la altura de estos cambios.