# Informática Forense: El camino de la evidencia digital

## Computer Forensics: The path of digital evidence

**AUTOR:**
Torres Ponce, Mariano Enrique
Abogado y Especialista en Derecho Informático

**RESUMEN**

La presente monografía, tiene por objetivo exponer una noción racional que demarque las principales actividades que se deben llevar adelante para establecer la «evidencia digital». El abordaje empleando, contiene aspectos jurídicos y técnicos que permiten obtener una perspectiva teórica y práctica. De esta manera, podremos presentar el escenario que propone el avance tecnológico y las propiedades de incorporarlo al proceso judicial.

**ABSTRACT**

The objective of this monograph is to expose a rational notion that demarcates the main activities that must be carried out to establish "digital evidence". The approach used contains legal and technical aspects that allow a theoretical and practical perspective to be obtained. In this way, we will be able to present the scenario proposed by technological progress and the properties of incorporating it into the judicial process.

**PALABRAS CLAVE**

Derecho Civil, Derecho de la informática, Derecho del ciberespacio.

**KEYWORDS**

Civil law, Computer law, Cyberspace law.

**ÍNDICE**

## A. INTRODUCCIÓN

La elaboración de este texto, tiene como objetivo principal acercar una noción rápida y concreta de las principales actividades que llevan a la adquisición de una evidencia digital. El abordaje empleando, contiene aspectos técnicos y jurídicos permitiendo el estudio de forma más completa. De esta manera, podremos presentar lo diverso y extenso del nuevo escenario gracias al avance tecnológico y los inconvenientes de incorporarlo al proceso judicial.

## B. INFORMÁTICA FORENSE

La informática forense es una disciplina, relativamente nueva, que nació en base a la necesidad de una especialidad técnico legal de la justicia moderna para poder revolver los métodos y habilidades esgrimidas en principio por los delincuentes informáticos. La misma se encarga, entre tantas otras actividades, de recuperar información tras un desastre, restaurar datos y rastrear manipulación de información por parte de personas no autorizadas.

Es importante destacar que, con la creciente necesidad de respuestas, la expansión del campo de acción de esta disciplina aumento, convirtiéndose eventualmente en un complemento de investigaciones que no se centran en delitos desarrollados en medios tecnológicos.

Es así que, para una real comprensión, debemos acceder a la definición instituida por el F.B.I., quienes describieron a la informática forense como: la ciencia que se encarga de aplicar técnicas informáticas en el proceso de adquirir, preservar, obtener y presentar datos que han sido procesados y/o almacenados de forma electrónica y que son relevantes en el ámbito judicial.[1]

Siendo necesario un análisis detallado para comprender su efectivo significado examinar los elementos de la descripción:

- La adquisición: habla de la recolección efectiva del objeto de estudio o elemento de análisis;
- La preservación: el mantenimiento de dicho elemento de examen a peritar en su estado original, evitando su alteración en lo más mínimo que pueda brindar un resultado erróneo;
- La obtención: es la observación en sí, determinándose que la información es efectivamente la que se desea indagar. Siendo los casos más normales, como para ejemplificar, el chequeo de historial de navegación, recuperación de archivos de texto o imágenes borrados de forma poco segura, entre otros procedimientos. Y finalmente;

[1] Noblett, Michael; Pollitt, Mark; Presley, Lawrence. "Recuperación y examen de evidencia en informática forense". Revista Ciencias de la comunicación forense. (EE.UU.) publicación de la Oficina Federal de Investigación (FBI) 2000, N° 4 - vol. 2 - pág. 1

- La presentación: la cual hace referencia a la exposición de un informe utilizando un lenguaje acorde a quienes sean los destinatarios del análisis. Dado que, tanto las partes como el juez son los principales ingresados de los resultados de esta actividad pericial.

En tanto, al referirse que "han sido procesados y/o almacenados de forma electrónica", hace referencia a dispositivos físicos de retención de información y a los transmitidos en una red de datos.

En este sentido, podemos apreciar que la referencia al ámbito judicial que concluye la enunciación refiere a la esfera pública. Pero no limitamos a lo forense a este contexto solamente, ya que en la privada puede aplicarse para la detección de ataques informáticos o accesos no autorizados a información de empresas y organizaciones, sin que sea necesaria la intervención de profesionales o autoridades del área jurídica.[2]

## C. EVIDENCIA DIGITAL

El principal objeto de estudio de la informática forense. En el derecho, una evidencia es una prueba determinante en un proceso judicial, debido que es aquella que permite demostrar la verdad de un hecho de acuerdo a los criterios establecidos por la ley. Siendo la que otorga la certeza clara, manifiesta y perceptible de un evento que nadie racionalmente puede dar lugar a dudas de su acontecer.

La evidencia digital, que nos centra en este artículo, la podemos definir como cualquier información probatoria almacenada o transmitida en forma digital que una parte de un caso judicial puede usar en el juicio.[3]

Estas pruebas se pueden encontrar en diversos dispositivos de almacenamiento, o transmisión pudiendo ser discos rígidos, cintas de respaldo, distintos tipos de tarjetas de memorias de teléfonos celulares, computadoras o cualquier terminal tecnológica.

Usualmente se asociaba la evidencia digital con delitos electrónicos como falsificación de documentos electrónicos, cajeros automáticos y tarjetas de crédito, robo de identidad, fraudes

[2] Herrera, Juan Luis. "Informática Forense: El manejo integral de la evidencia digital". Portal Praxiomática. Publicado el 18 septiembre, 2016 con el link https://praxiomatica.wordpress.com/2016/09/18/informatica-forense-el-manejo-de-evidencia-digital/

[3] Department of Justice. "New Approaches to Digital Evidence Acquisition and Analysis" (EE.UU.). https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis

electrónicos y pornografía infantil.[4] Sin embargo, en la actualidad se utiliza para procesar todo tipo de delitos, pudiendo señalar como los más destacados:

- Prosecución criminal: evidencias incriminatorias pueden ser usadas para procesar una variedad de crímenes, incluyendo homicidios, estafa financiera, tráfico y venta de drogas, evasión de impuestos o pornografía infantil;
- Litigación civil: casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados con este tipo de pruebas;
- Investigación de seguros: la evidencia encontrada en computadoras, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones;
- Temas corporativos: puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o espionaje industrial;
- Mantenimiento de la ley: la informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

El momento en el que se solicita la evidencia digital es muy variable, pudiendo ser solicitado por el juez o por alguna de las partes. El art. 253 del Código Procesal Penal establece que "El juez podrá ordenar pericias siempre que para conocer o apreciar algún hecho o circunstancia pertinente a la causa, sean necesarios o convenientes conocimientos especiales en alguna ciencia, arte o técnica."[5]

Provocándose el resguardo voluntario mediante acta notarial.

## C.1. MANEJO DE LA EVIDENCIA

El cuidado de la evidencia digital es uno de los pasos más importantes para la obtención del resultado sin alteraciones. Para la correcta manipulación de la misma, es necesario tener en cuenta cinco aspectos:

- Unicidad de formato: hace referencia a aquellos documentos electrónicos que solo pueden preservarse en su estado digital, estos son archivos multimedia, base de datos relacionales,

[4] Gallegos, M.; Purcachi, C.; Almeida, C. "Informática Jurídica". Pág 49. Universidad Técnica del Norte (Ecuador). 2016. https://issuu.com/utnuniversity/docs/ebook-informatica-juridica/49

[5] **"**Código Procesal Penal". Portal InfoLeg de Información Legislativa. Publicado con el link http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/383/texact.htm

documentos simples con metadatos, entre otros que no pueden plasmarse en papel u otro formato diferente al original.

- Alterabilidad: son todos aquellos archivos digitales que poseen metadatos asociados, por lo tanto, no pueden manipularse por ser susceptible de tener información relevante como puede ser: la fecha de creación, modificación, acceso u otros datos que exceden al contenido del fichero mismo.
- Interpretación: es la forma de entender los datos que me brindan programas específicos que pueden tener configuraciones complejas, llaves de seguridad o tratamientos en materias concretas. Estamos hablando de casos en los que necesiten de asistencia calificada como, por ejemplo: en el caso de peritar software contable, donde el perito requerirá que sea asistido por un contador o experto en el tema, entre otros casos.
- Medio activo: el programa que usemos para recolectar la evidencia pueda alterarla, por lo tanto, nunca hay que realizar la copia con herramientas del mismo sistema operativo. Esto es debido a que pueden llegar a modificar los metadatos y así alteran la integridad de documentos, siendo recomendado el empleo de software específico para hacer una copia fiel.
- Medio de destino: es el hardware donde se almacenará la información a peritar, aquí hay que considerar varios elementos como pueden ser: la universalidad, es decir la disponibilidad del medio de prueba en el momento de la pericia; la obsolescencia, es la accesibilidad al medio empleado y; la confiabilidad, que este asociado a lo seguridad del medio para preservar la prueba.[6]

## D. EL PERITO

Un Perito Informático Forense es un profesional con conocimientos, habilidades y experiencia que es necesario para asistir en los juicios y los tribunales a esclarecer delitos cibernéticos.[7]
Frente al crecimiento técnico para la concreción de amenazas, estos investigadores son los encargados de ejecutar una aguda indagación y perfeccionamiento de la tecnología forense preparándose para ataques cibernéticos cada vez más complejos.

---

[6] Presman, Gustavo "Manejo de Pruebas Digitales en Investigaciones de Delitos Informáticos". Presentación COPITEC. 2004

[7] "Perito Informático Forense, una de las profesiones con más salidas". Portal MuyComputerPro. Publicado en agosto de 2014 con el link https://www.muycomputerpro.com/2014/08/25/perito-informatico-forense

Entre las competencias indispensables de investigación manual, debe conocer el acceso a la memoria del sistema, ficheros de hibernación, tablas MFT de partición de archivos, logs del sistema, registros de Windows, visor de eventos, ficheros de la carpeta Prefetch, la papelera de reciclaje, metadatos de imágenes, backups, volume shadow, entre otras habilidades.

Aunque, mayormente se utiliza software especializado que permite ahorrar tiempo en el rastreo de datos. Entre varios programas, tenemos en código abierto distribuciones como lo son Deft, Caine, Helix, EnCase, Forlex, Kali Linux y Patrrot Forensic; herramientas libres como Sleuth Kit, Volatility y Kft Imager; y software comercial como OsForensics, Magnet IEF, Spektor, Oxygen Forensics.[8]

Con estos instrumentos deberá abarcar un ámbito de acción muy amplio, debido a que los avances tecnológicos que generaron una mayor capacidad de almacenamiento de datos y al desarrollo y uso de redes de todo tipo. El incremento en el número de usuarios de computadoras personales y teléfonos celulares provocó un notable aumento de delitos informáticos. Para combatir esta dificultad, el campo de la ciencia forense cibernética se centra no solo en la tecnología forense informática tradicional fuera de línea, sino en pruebas en línea en tiempo real como lo son: el seguimiento de correos electrónicos, mensajes instantáneos, así como todas las demás formas de comunicaciones relacionadas con las nuevas aplicaciones.

De esta manera vemos que, el análisis forense cibernético consta de dos componentes: análisis forense informático y análisis forense de redes. Que nos lleva a clasificar los tipos de evidencia digital.

## E. CLASIFICACIONES DE EVIDENCIA DIGITAL

Para hacer un buen planeo de los puntos de pericia es importante tener en claro que queremos probar, donde está la evidencia y si se puede hacer con los medios disponibles. Es por este motivo que es indispensable planificar antes de actuar, realizar una recolección efectiva sin contaminación, no manipular la evidencia y contar con asesoramiento previo para lograr un mejor escenario. Por este motivo debemos clasificar la evidencia en estática o dinámica.

La *evidencia estática*, es aquella que se mantiene en el tiempo, esto sería una copia de un disco duro, que luego de realizarse una copia forense que permite chequear su fidelidad con un valor hash, que después profundizaremos.

[8] García, José Aurelio "Cómo hacer una forense informática y no morir en el intento". Congreso de Seguridad HoneyCON. 2016

Por su parte, la *evidencia dinámica*, es la que cambia constantemente, esto ocurre en los teléfonos celulares, ya que, a diferencia de las computadoras, no se puede extraer el chip de memora para manipularlo. Esto que consideramos una buena práctica aislarlo de la red, ya sea poniéndolo en modo avión o ponerlo en una bolsa aislante, también conocida como bolsa de Faraday, y así además evitamos que la información pueda ser eliminada remotamente.

Otra clasificación está asociada con el almacenamiento y/o transferencia de datos, teniendo como elementos la memoria de almacenamiento, memoria RAM y tráfico de red.

La *memoria de almacenamiento* es el más común, siendo aquella memoria que persiste. Aquí tenemos discos rígidos, memorias, CD, DVD, pendrives, cintas de resguardo, entre otras. Esa es la que tiene mayor información y la más fácil de peritar, siendo la característica distintiva que tiene información predatada, o sea información previa al secuestro del dispositivo. Solo puede borrarse sobrescribiéndose, dado que el sistema operativo, como marcábamos anteriormente, en realidad lo que hace es sacar los archivos de su índice de accesibles. Este tipo de evidencia suele presentar buenos resultados dado que los sistemas mencionados están pensados en brindar una experiencia agradable a los usuarios y que la seguridad es un factor secundario. Es por eso que, en este medio podemos conseguir pruebas salvo que se haya realizado un borrado eficiente de información empleando técnicas como los métodos DoD 5220.22-M o Peter Gutmann Secure Deletion, entre otros de sobreescritura.

La *Memoria RAM* es aquella memoria de procesamiento que tiene información solo desde que el equipo ha sido prendido por última vez, por lo tanto, solo podrá ser recolectada si se accede al sistema estando encendido. Aquí podemos encontrar conductas de usuario, passwords, entre otras actividades que se realizaron desde el momento de ser iniciado.

El *Trafico de red* es aquella información que circula por la red local o Internet, en la práctica son los datos que menos se recolectan y que más importante serán a futuro con los servicios de streaming y almacenamiento en la nube. Esta información tiene una estructura de paquete de datos y lo importante será copiar paquetes para reconstruir la información y actividades de tráfico. Aquí será significativo la recolección basada en la actividad registrada por los navegadores con una imagen forense y la principalmente la solicitud de informes al ISP para que intervenga a su usuario. Lo que respecta a la conducta en la red tenemos tres elementos considerar:

- Historial de navegación: es un conjunto de archivos que se depositan en la memoria de almacenamiento siguiendo sus reglas de borrado segur y nos indica los sitios consultados en la red.

- Cache: es un área del navegador donde se guardan elementos asociados a los sitios dónde se ingresó a fin de evitar la descarga nuevamente si el elemento persiste en un futuro reingreso a una determinada página web. Estos son fotos, imágenes, entre varios contenidos.
- Cookies: es un archivo pequeño que descarga la web en la que se navega impactando en el ordenador del usuario según su tipo. Teniendo primero las cookies de preferencia que le "recuerdan" al navegador la predilección del usuario del contenido de la página para que en el próximo ingreso sean mostrados estos o asociados. Las cookies de transición son las que se usan para compras electrónicas indicando los detalles de la misma, dura pocas horas. Para concluir las cookies analíticas, son aquellas que recaban información de los gustos para analizar las preferencias de varios grupos de usuarios. Una vez realizada la adquisición, presesión, obtención y presentación quedara analizar la intencionalidad del acceso, dado que el usuario puede haber sido redireccionado, es así que no necesariamente demuestra la actividad reprochable del usuario del sistema.

Es así que, en estos tres casos es importante destacar que, los métodos utilizados deben ser tecnológicamente sólidos para garantizar que se recupere toda la información probatoria, que la evidencia original no se altere y que no se agreguen ni eliminen datos de la colección original. Generalmente, las investigaciones forenses informáticas se llevan a cabo después de que ocurrió el crimen o evento, al igual que las investigaciones en la medicina forense tradicional. Los archivos perdidos o eliminados por accidente pueden ser recuperados por un experto en informática forense. La información potencialmente valiosa para casos penales o civiles en un tribunal de justicia se identifica y recopila utilizando técnicas de investigación.

Por el contrario, el análisis forense de redes implica la recopilación de pruebas digitales, que pueden ser transitorias y no conservarse con medios de almacenamiento permanentes y se distribuyen a través de redes complejas a gran escala. La ciencia forense de redes es un área técnicamente más desafiante de la ciencia forense cibernética, ya que se ocupa del análisis en profundidad de la evidencia de intrusión en la red informática. La dificultad radica en las herramientas comerciales de análisis de intrusiones que son inadecuadas para hacer frente a los entornos distribuidos en red de la actualidad. [9]

Además de que, en el sector comercial, el uso de los servicios y aplicaciones populares de la red como lo son Facebook, YouTube, WhatsApp, Twitter, Google, entre otros, es gratuito, ya que la fuente principal de sus ingresos es la publicidad. En este sentido, el objetivo de los

[9] Zucker, Susan. "Cyber Forensics: Part One". Portal National Criminal Justice Reference Service (EE.UU.) Publicado en Enero de 2007 con el link https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=242828

proveedores no está puesto en la identificación de la persona que se encuentra detrás de la pantalla, sino en sus gustos y preferencias. De esta manera, Internet favorece la construcción de identidades ficticias ante la ausencia de mecanismos de acreditación de identidad certeros por parte de las empresas proveedoras de servicios.[10]

## F. ELEMENTOS DEL PROCEDIMIENTO FRENTE A UN SISTEMA.

El primer contacto con el sistema debe ser analizado y siguiendo los pasos necesarios para evitar la pérdida de posibles pruebas. Al acceder al recinto donde se encuentran los equipos se debe principalmente asegurar el lugar, pudiendo acceder sin intervención de terceros o personas ajenas al peritaje que con su accionar tengan la posibilidad de alterar la escena. Para intervenir correctamente, se deberá hacer con los guantes adecuados para preservar las huellas, dado que las que estén en la superficie del hardware de los sistemas investigados permutaran saber quiénes fueron usuarios de aquel.

Una vez cubierto el sistema de modo físico, tenemos que ser conscientes de que aún existe el peligro de que se encuentre actuando una persona de forma remota o software de protección y que nuestro accionar no altere la información.

Con este contexto, ya debemos interactuar con el equipo, debiendo en el supuesto de estar apagado, mantenerlo sin encender para evitar alterar datos. Si se encuentra activo, el sistema no debe ser apagado, ya que puede rescatarse información de la memoria RAM y moverse el mouse periódicamente para evitar un posible bloqueo por inactividad. Siendo procedimientos a seguir, la adquisición de la IP si el equipo está conectado a la red y la registración de la información de los menús y los archivos activos realizando la menor actividad posible con el teclado.[11]

Si el equipo este encendido y hay una creencia razonablemente de que el sistema está destruyendo la evidencia, se deberá proceder a la desconexión inmediatamente. Siendo en las notebooks recomendable remover la batería.

Una vez eso se tendrá que retirar con bolsas especiales antiestática o en su defecto de papel madera los discos rígidos y otros dispositivos de almacenamiento informáticos que sean electromagnéticos que se encuentren al alcance. Coloque etiquetas en los cables para facilitar

---

[10] Azzolin, Horacio. y Sain, Gustavo: "Delitos informáticos: investigación criminal, marco legal y peritaje". Editorial BdeF. 2017.

[11] Acurio Del Pino, Santiago. "Manual de Manejo de Evidencias Digitales y Entornos Informáticos. v 2.0". Portal de Organización de los Estados Americanos con link http://www.oas.org/juridico/english/cyb_pan_manual.pdf

reconexión posteriormente y sellare cada entrada o puerto de información con cinta de evidencia. Llevar los manuales, documentación, anotaciones asociadas como así también cables y accesorios.
Por último, es indispensable anotar todo número de identificación a fin de poder mantener la cadena de custodia.

## F.1. CRITERIOS DE PRIORIZACION DE EQUIPOS.

Frente a los grandes volúmenes de información y el poco tiempo para determinar o buscar contenido relevante en un equipo aparece el "triage". Este término es utilizado en la medicina para priorizar la atención de pacientes en función de su estado de gravedad. Llevado al ámbito de la informática forense, dicha técnica se aplica para la selección de aquella evidencia digital que debe ser priorizada para llevar a cabo un posterior análisis forense exhaustivo, en función de diversos indicadores o características que pueden ser determinadas de forma inmediata. Siendo, en otras palabras, una técnica de muestreo rápido que permite obtener resultados limitados, pero muy veloces que dan la posibilidad de avanzar rápidamente en determinados casos. El escenario más común para su implementación, es el de empresas con muchas computadoras, servidores y otros dispositivos, donde tendrá el profesional que detectar cuales son los importantes para luego secuestrarlos y que se realice un peritaje profundo. Además de contar con la ventaja de ser de simple realización, no siendo necesario contar con un recurso altamente capacitado para realizar esta tarea.
Con este método, finalmente podremos sacar del dispositivo del sospechoso lo que denominamos "archivo de evidencia lógica" que es un contenedor que solo tiene los archivos relevantes para la investigación.

## F.2. OBSERVACIONES EN MEMORIAS DE ALMACENAMIENTO.

Al actuar sobre la información el especialista no realiza un backup de los datos, dado que debe trascender más allá de las herramientas que le presenta el sistema operativo. Es así que, ejecuta una "copia forense", la cual emplea una técnica de copiado *bit a bit* permitiendo la recuperación de archivos borrados por la plataforma operativa del dispositivo. Esto se debe a que, en realidad, solo fueron desindexados los datos, pero pueden encontrarse ocultos en el dispositivo.
Las copias forenses se realizan con herramientas de hardware y software especiales para dicho fin, siguiendo un procedimiento que chequea la integridad de la reproducción mediante un valor que debe ser coincidente. Este valor es conocido como *hash*, que definimos de esta manera a

una función criptográfica generada por un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la extensión de los datos de entrada, el valor hash de salida tendrá siempre la misma amplitud.[12]

Este valor, es una suerte de firma que surge de un cálculo matemático derivado de valores que varían según el contenido del disco o dispositivo de almacenamiento. Siendo así que, el valor hash del disco del sospechoso deberá ser exactamente el mismo que el de la copia forense en caso de estar correctamente realizada.

Las funciones del hash pueden realizarse utilizando cualquier algoritmo criptográfico, como puede ser MD5 (128 bits), SHA-1 (160 bits) o SHA-256 (256 bits). Aunque los primeros dos ya están empezando a usarse solamente en forma combinada, o sea calculando ambos valores de un mismo archivo, debido a que individualmente son vulnerables y los abogados pueden cuestionar la validez de la evidencia.

Dicho valor ira en el acta de procedimiento como prueba de fidelidad de la copia *bit a bit* o directamente todo el reporte que realiza el software.

Por su parte, también es necesario destacar que desde que se realizo la copia forense hasta que se perita la información contenida puede pasar mucho tiempo, hasta años y es probable que no se realice por el mismo perito ambas actividades. Por este motivo es importante, antes de hacer la pericia, chequear la integridad nuevamente de la copia para asegurarse que no fue alterada recalculando el valor hash.

Por último, debemos hacer especial mención a la particularidad de los dispositivos móviles, en los cuales no existe la copia forense, sino que es una extracción forense. Esto es debido a que, el hardware de un teléfono celular este compuesto por diferentes memorias que físicamente podemos observar en su interior como chips soldados y requieren que el equipo este encendido para su funcionamiento. En cambio, a diferencia de las computadoras de escritorio, notebooks o servidores, el hardware es un conjunto de componentes que integran un todo, pero pueden analizarse los componentes de manera independiente.

## F.3. ANALISIS DEL TRÁFICO DE DATOS EN REDES.

El análisis forense de redes se basa en la certeza de que no existe el anonimato ni en la navegación ni en el uso de Internet. Aunque se utilicen programas que ofrecen navegación

[12] Donohue, Brian. "¿Qué Es Un Hash Y Cómo Funciona?" Portal Kaspersky Daily (Rusia). Publicado con el link https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

anónima como TOR, Proxy y otros; estos servicios también pueden resultar comprometidos o pueden contener fallas.

Los peritos especializados se basan en utilizar los conocimientos acerca del funcionamiento del protocolo TCP/IP y de los instrumentos que emplean los crackers para atacar un sistema informático. Esta especialidad se vale de técnicas y programas que buscan los logs y los archivos de actividad de los distintos protocolos de red. Muchas veces se vale de técnicas de hacking ético para obtener acceso a los datos o equipos que normalmente no están disponibles para el usuario promedio.

Es importante aclarar aquí la diferencia entre el hacking ético y el hacking malicioso, radicando dicha distinción en el uso de la información y acceso obtenido. Ambas modalidades de hacking comparten prácticamente las mismas metodologías y herramientas, motivo por el cual muchos programas antivirus van a impedir que los programas de hacking entre en ejecución.

Es entonces, cuando se vuelve imprescindible usar máquinas virtuales, Live CDs o un dispositivo de arranque que no contenga software de seguridad como antivirus o firewalls que pueda confundirse frente a las herramientas utilizadas para peritar. El hacker ético, al igual que el malicioso, no debe utilizar un sistema común que pueda ser fácilmente identificado o que pueda contener información personal del investigador o de la institución.

Así como, no existe una sola forma o vector de ataque, no es posible establecer o recomendar un único programa que sirva para investigar o frenar todos los ataques. Lo que se ha hecho en este trabajo es presentar una serie de pautas que siguen los atacantes bajo distintos ambientes y evaluar una serie de programas que pueden ayudar a identificar y obtener evidencias de la actividad del atacante.[13] En este contexto, el tiempo es un elemento valioso para poder rastrear por completo el tráfico y la actividad del atacante. Pudiendo determinar el camino de los datos y la actividad desde el equipo de origen hasta el de la víctima, siempre que no sean borrado los registros y, por supuesto, siempre que exista la colaboración de los equipos intermedios.

## F.4. INVESTIGACIÓN DEL CORREO ELECTRÓNICO.

El análisis forense de correos electrónicos es aquel que requiere actividad sobre el equipo y en la red, dado que podemos encontrar datos distribuidos que nos sirvan para darle consistencia a los mails encontrados, permitiendo que sean evidencia valida. Para poder emplearlos como

[13] Proaño Freire, Margoth. "Estudio de software libre para realizar el análisis forense en redes de computadores para entidades ecuatorianas dedicadas a la seguridad ciudadana". Publicado Por La Pontificia Universidad Católica Del Ecuador. 2012

prueba es necesario analizar el completamente un correo, viendo que consta de dos partes la investigación:

- Investigación estática: está compuesta por el análisis del contenido de un correo electrónico de servidores locales, corporativos y en la web. Indagándose sobre su cuerpo del correo y los archivos adjuntos de las distintas bandejas, recabándose datos que son depurados, o sea los eliminados; el análisis del intercambio de mails, o sea chequeo del envío y recepción de la casilla; y la búsqueda simple, compleja e indexada del contenido.
- Investigación dinámica: es aquella que alcanza información del origen geográfico y los logs de servidores SMTP o sea de mail que emplea el protocolo de simple de transferencia de correo.

  Al presentarse como prueba, es requisito que sea de la información completa incluyendo datos de tráfico, por tal motivo no es válido presentar la impresión en papel del cuerpo del contenido del correo.

## F.5. REDES SOCIALES

La creación de perfiles falsos es normal, encontrado fácilmente en los residuos de navegación de los dispositivos. Aquí se podrá actuar en aquellos supuestos donde sea indispensable certificar la veracidad de una conversación, publicación o comentario, comprobar la existencia de un usuario falso, certificar una suplantación de identidad en una red social y certificar un caso de violencia digital como ciberacoso, ciberbullying o sextorsión.[14]

Pero también debemos poder acceder a los datos de los servidores de las empresas que brindan servicios de mensajería o redes sociales, para ello se deberá hacer un pedido formal de resguardo de información, datos de navegación, entre otros, realizando el procedimientos de solicitud que requerirá la empresa prestadora del servicio.

En el ámbito civil son solicitadas por oficios judiciales a las empresas o a jueces según se trate de datos de tráfico o de contenido. En el ámbito penal existen atajos con servicios ofrecidos discrecionalmente por algunas empresas u otros como GDTLDTI /INTERPOL.

Aquí el perito, con herramientas específicas puede complementar los datos que tiene en algún medio de almacenamiento secuestrado, integrando con fechas y algunos chats de los archivos temporales de Internet del navegador.

[14] "Peritaje Informático en Redes Sociales". Portal Grupo Globatica - Peritos Informáticos. Publicado con el link http://peritoinformaticojudicial.com/peritaje-en-redes-sociales/

Por su parte, tenemos en las fotos e imágenes otro elemento a peritar relevante para adquirir evidencias. Los metadatos EXIF (Exchangeable image file format), son un estándar creado para almacenar información de las fotos hechas con cámaras digitales, teniendo datos relativo a la propia imagen y a cómo ha sido tomada, o sea mucha mas información además de la misma foto. Estos metadatos nos dan la posibilidad de obtener desde la marca de la cámara o teléfono con el que se tomó hasta la fecha o ubicación de GPS.

## G. CADENA DE CUSTODIA

La cadena de custodia es el registro detallado del movimiento de la evidencia durante el proceso probatorio. En este se indican todas las actividades efectuadas, las personas responsables y el momento y estado en el que se encuentra la evidencia. El registro no evita que se vulnere la evidencia, sino que permite saber en caso que suceda, que fue lo que sucedió y quien era el responsable en aquel momento. Siendo la finalidad de esta documentación asegurar y demostrar la identidad, integridad, preservación y registro en la continuidad de la prueba, iniciándose al momento de recolectarse hasta la finalización de la etapa probatoria.
La misma es registrada en un formulario específico y en el expediente judicial, debiendo incluir entre sus datos el nombre de la persona, fecha de contacto con la evidencia, actividades realizadas, entre otros requerimientos.

## H. NORMAS Y ESTANDARES DE BUENAS PRÁCTICAS DE PERITAJE

Las normas de estandarización son muy importantes para determinar cuáles son las buenas prácticas para realizar el peritaje. Estas regulaciones marcan el camino a seguir en el tratamiento y seguridad del objeto a analizar, siendo importante seguirlas, aunque no son de cumplimiento obligatorio. Es así que, destacamos a nivel mundial la ISO/IEC 27037:2012, ISO/IEC 27042:2015 y RFC 3227. En Argentina no tenemos normativa local, mientas que a nivel europeo nos resulta al menos importante mencionar algunas. En España las normas UNE 71505:2013 y UNE 71506:2013.
La primera es la ISO/IEC 27037:2012, conocida como la guía para la identificación, recolección, adquisición y preservación de evidencia digital. La cual proporciona pautas para actividades específicas en el manejo de evidencia digital, que son la identificación, recopilación, adquisición y preservación de evidencia digital potencial que puede tener valor probatorio.

Suministra orientación a las personas con respecto a situaciones comunes que se encuentran a lo largo del proceso de manejo de evidencia digital y ayuda a las organizaciones en sus procedimientos disciplinarios y a facilitar el intercambio de evidencia digital potencial entre jurisdicciones.[15]

La norma brinda, es una lista indicativa y no exhaustiva, orientación para los siguientes dispositivos y circunstancias:

- Medios de almacenamiento digital utilizados en computadoras estándar como discos rígidos, disquetes, discos ópticos y magneto ópticos, dispositivos de datos con funciones similares;
- Teléfonos celulares, asistentes digitales personales (PDA), dispositivos electrónicos personales (PED), tarjetas de memoria;
- Sistemas de navegación móviles;
- Cámaras digitales fijas y de video (incluido CCTV);
- Computadora estándar con conexiones de red;
- Redes basadas en TCP / IP y otros protocolos digitales, y;
- Dispositivos con funciones similares a las anteriores.

Otra norma que es importante es la ISO/IEC 27042:2015, denominada como la guía con lineamientos para el análisis e interpretación de evidencia digital. La misma brinda orientación sobre el estudio de evidencia digital abordando cuestiones de continuidad, validez, reproducibilidad y repetibilidad. Agrupando las mejores prácticas para la elección, diseño e implementación de procesos analíticos y registra suficiente información para permitir que dichos procesos se sometan a un escrutinio independiente cuando sea necesario. Proporciona orientación sobre los mecanismos adecuados para demostrar la competencia y competencia del equipo de investigación.

El análisis y la interpretación de la evidencia digital puede ser un proceso complejo. En algunas circunstancias, puede haber varios métodos que podrían aplicarse y los miembros del equipo de investigación deberán justificar su selección de un proceso en particular y mostrar cómo es equivalente a otro proceso utilizado por otros investigadores. En otras circunstancias, es posible que los investigadores tengan que idear nuevas técnicas para examinar pruebas digitales que no se hayan considerado previamente y deberían poder demostrar que el procedimiento producido es "adecuado para su propósito".

---

[15] "ISO/IEC 27037:2012 Information technology -Security techniques- Guidelines for identification, collection, acquisition and preservation of digital evidence". Portal ISO. Publicado en 2012 con el link https://www.iso.org/standard/44381.html

La aplicación de un método en particular puede influir en la interpretación de la evidencia digital procesada por esa técnica. La evidencia digital disponible puede influir en la selección de usos para un análisis adicional de la evidencia digital que ya ha sido adquirida.

Es así como, la ISO/IEC 27042:2015 proporciona un marco común, para los elementos analíticos e interpretativos del manejo de incidentes de seguridad de los sistemas de información, que se puede utilizar para ayudar en la implementación de nuevos métodos y proporcionar un estándar común mínimo para la evidencia digital producida a partir de tales actividades.[16]

Por otro lado, tenemos el documento publicado por la Grupo de Trabajo de Ingeniería de Internet (IETF) que recoge directrices para recopilar y almacenar evidencias sin ponerlas en riesgo. RFC 3227 proporciona pautas generales para la recopilación y el archivo de pruebas digitales, mientras que la Organización Internacional de Pruebas Informáticas ofrece pautas para las mejores prácticas en el examen forense digital. A la luz de estas directrices, analizaremos el mecanismo de protección de la integridad proporcionado por EnCase y FTK, que se basa principalmente en códigos de resumen de mensajes conocidos también como MDC. Estos códigos para protección de la integridad, no son a prueba de manipulaciones, por lo que pueden falsificarse. Con el modelo propuesto para proteger la integridad de la evidencia digital mediante el uso de tarjetas inteligentes establece una plataforma segura para firmar digitalmente el código de resumen de mensajes en combinación con la criptografía de clave pública (PKC), se puede mostrar para que esta debilidad se supere.[17]

Por último, también resulta interesante en este estudio ver aquellas normas empleadas en España. Es así que, las regulaciones de la Asociación Española de Normalización y Certificación para UNE 71505 y UNE 71506 también nos resultan llamativas. Las mismas tienen como finalidad dar una metodología para la preservación, adquisición, documentación, análisis y presentación de pruebas digitales. Según la asociación, esta norma debe dar respuesta a las infracciones legales e incidentes informáticos en las distintas empresas y entidades. Con la obtención de dichas pruebas digitales, que serán más robustas y fiables siguiendo el procedimiento, pudiéndose discernir si su causa tiene como origen un carácter intencional o negligente. Las normativas son de aplicación a cualquier organización con independencia de su actividad o tamaño, como así también a cualquier profesional competente en este ámbito. Se

[16] "ISO/IEC 27042:2015 Information technology -Security techniques- Guidelines for the analysis and interpretation of digital evidence. Portal ISO. Publicado en 2015 con el link https://www.iso.org/standard/44406.html

[17] Saleem, Shahzad; Popov, Digital Forensics and Cyber Crime: Second International ICST Conference. 2011.

dirige especialmente a incidentes y seguridad, además del personal técnico que trabaje en laboratorios o entornos de análisis forense de evidencias electrónicas. [18]

## I. CONCLUSIONES

La informática forense se ha convertido en una ciencia central para lograr llevar justicia a nuestros tribunales. La actividad de los peritos informáticos es cada vez más compleja. Esto no solo se debe a las complejas técnicas empleadas por los ciberdelincuentes para realizar sus delitos, sino también por el mayor conocimiento de los usuarios y la gran competencia de las empresas desarrolladoras de sistemas operativos y dispositivos en brindar productos con nos cantidad de vulnerabilidades.

Por ello vemos que, es necesario contar con lineamientos amplios que permitan se adaptados a cualquier tecnología y que no se vuelvan rápidamente obsoletos con la diversidad o progreso de la misma. Esto combinado con procedimientos más flexibles permita completar para cada caso las solicitudes específicas. Es en este sentido que, con normativas que le permitan el acceso lo más completo posible al profesional y con la comprensión de la complejidad de estas labores por parte de los operadores del derecho, se lograra la más efectiva evidencia digital.

## J. BIBLIOGRAFIA


Azzolin, H., & Sain, G. (2017). *Delitos informáticos: investigación criminal, marco legal y peritaje*. Editorial BdeF.

Código Procesal Penal de la Provincia de Buenos Aires. (s.f.). Portal Sistema Argentino de Información Jurídica.

Department of Justice. (s.f.). *New Approaches to Digital Evidence Acquisition and Analysis*.

Del Peso Navarro, E. (1994). *Confidencialidad y seguridad de la información*. Díaz de Santos.

Donohue, B. (s.f.). ¿Qué es un hash y cómo funciona? Portal Kaspersky Daily.

García, J. A. (2016). *Cómo hacer una forense informática y no morir en el intento*. Congreso de Seguridad HoneyCON.

Gallegos, M., Purcachi, C., & Almeida, C. (2016). *Informática jurídica*. Universidad Técnica del Norte.


[18] Gervilla Rivas, Carles. "Metodología para un análisis forense". Portal Universitat Oberta de Catalunya INCIBE (Instituto Nacional de Ciberseguridad) (INTECO). 2014.

Gervilla Rivas, C. (2014). *Metodología para un análisis forense*. Universitat Oberta de Catalunya / INCIBE.

Gratton, P. (1998). *Protección informática*. Editorial Trillas.

Herrera, J. L. (2016). *Informática forense: El manejo integral de la evidencia digital*. Praxiomática.

Noblett, M., Pollitt, M., & Presley, L. (2000). Recuperación y examen de evidencia en informática forense. *Ciencias de la Comunicación Forense*.

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

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

Grupo Globatica. (s.f.). *Peritaje informático en redes sociales*.

MuyComputerPro. (2014). *Perito informático forense, una de las profesiones con más salidas*.

Presman, G. (2004). *Manejo de pruebas digitales en investigaciones de delitos informáticos*. COPITEC.

Proaño Freire, M. (2012). *Estudio de software libre para realizar el análisis forense en redes de computadores para entidades ecuatorianas dedicadas a la seguridad ciudadana*. Pontificia Universidad Católica del Ecuador.

Saleem, S., & Popov, L. (2011). *Digital forensics and cyber crime* (Second International ICST Conference).

Sosa, T. E. (2006). *Peritos judiciales: Teoría y práctica para la actuación procesal*. Librería Editorial Platense.

Zucker, S. (2007). *Cyber forensics: Part one*. National Criminal Justice Reference Service.