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

KEYWORD

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 resolver 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 aumentó, 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 (Noblett, Pollitt, & Presley, 2000). Siendo necesario un análisis detallado para comprender su efectivo significado, corresponde 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, incluso mínima, 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 del historial de navegación, la recuperación de archivos de texto o imágenes borrados de forma poco segura, entre otros procedimientos. Y, finalmente:

- 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 interesados de los resultados de esta actividad pericial.

En tanto, al referirse a que "han sido procesados y/o almacenados de forma electrónica", se alude 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 lo forense a este contexto solamente, ya que en la esfera 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 (Herrera, 2016).

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 a que es aquella que permite demostrar la verdad de un hecho de acuerdo con los criterios establecidos por la ley, siendo la que otorga la certeza clara, manifiesta y perceptible de un evento que nadie racionalmente puede poner en duda.

La evidencia digital, que nos centra en este artículo, puede definirse como cualquier información probatoria almacenada o transmitida en forma digital que una parte de un caso judicial puede usar en el juicio (Department of Justice, s. f.).

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

Usualmente se asociaba la evidencia digital con delitos electrónicos como falsificación de documentos electrónicos, fraudes en cajeros automáticos y tarjetas de crédito, robo de identidad, fraudes electrónicos y pornografía infantil (Gallegos, Purcachi, & Almeida, 2016). 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 o 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 que 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 solicitada 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" (Código Procesal Penal, s. f.). 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, bases de datos relacionales, 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 susceptibles de contener 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 brindan programas específicos que pueden tener configuraciones complejas, llaves de seguridad o tratamientos en materias concretas. Estamos hablando de casos en los que se necesita asistencia calificada, como por ejemplo en el peritaje de software contable, donde el perito requerirá ser asistido por un contador o experto en el tema, entre otros casos.

- Medio activo: el programa que se use para recolectar la evidencia puede alterarla; por lo tanto, nunca hay que realizar la copia con herramientas del mismo sistema operativo. Esto se debe a que pueden llegar a modificar los metadatos y así alterar la integridad de los 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 la universalidad (es decir, la disponibilidad del medio de prueba en el momento de la pericia); la obsolescencia (la accesibilidad al medio empleado); y la confiabilidad (asociada a la seguridad del medio para preservar la prueba) (Presman, 2004).

D. EL PERITO

Un perito informático forense es un profesional con conocimientos, habilidades y experiencia que son necesarios para asistir en los juicios y los tribunales a esclarecer delitos cibernéticos (MuyComputerPro, 2014).

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.

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 distribuciones de código abierto como Deft, Caine, Helix, EnCase, Forlex, Kali Linux y Parrot Forensic; herramientas libres como Sleuth Kit, Volatility y Kft Imager; y software comercial como OsForensics, Magnet IEF, Spektor u Oxygen Forensics (García, 2016).

Con estos instrumentos deberá abarcar un ámbito de acción muy amplio, debido a 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 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, lo 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 qué queremos probar, dónde está la evidencia y si se puede obtener 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, luego de realizarse una copia forense que permite chequear su fidelidad con un valor hash, que después profundizaremos.
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 memoria para manipularlo. Por este motivo se considera una buena práctica aislarlos de la red, ya sea poniéndolos en modo avión o colocándolos en una bolsa aislante, también conocida como bolsa de Faraday, evitando así 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, la memoria RAM y el tráfico de red.
La memoria de almacenamiento es la más común, siendo aquella que persiste. Aquí tenemos discos rígidos, memorias, CD, DVD, pendrives, cintas de resguardo, entre otras. Es la que contiene mayor información y la más fácil de peritar, siendo la característica distintiva que posee información predatada, es decir, información previa al secuestro del dispositivo. Solo puede borrarse sobrescribiéndose, dado que el sistema operativo, como mencionábamos 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 para brindar una experiencia agradable a los usuarios y 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.

La memoria RAM es aquella memoria de procesamiento que tiene información solo desde que el equipo ha sido encendido por última vez; por lo tanto, solo podrá ser recolectada si se accede al sistema estando encendido. Aquí podemos encontrar conductas de usuario, contraseñas, entre otras actividades realizadas desde el momento del inicio.

El tráfico de red es aquella información que circula por la red local o Internet. En la práctica es uno de los datos que menos se recolectan y que más importancia tendrán 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 las actividades de tráfico. Aquí será significativa la recolección basada en la actividad registrada por los navegadores mediante una imagen forense y, principalmente, la solicitud de informes al ISP para que intervenga respecto del usuario investigado. En lo que respecta a la conducta en la red, tenemos tres elementos a considerar:

- Historial de navegación: es un conjunto de archivos que se depositan en la memoria de almacenamiento siguiendo sus reglas de borrado seguro y nos indica los sitios consultados.
- Caché: es un área del navegador donde se guardan elementos asociados a los sitios a los que se ingresó, a fin de evitar la descarga nuevamente si el elemento persiste en un futuro reingreso. Estos elementos pueden ser fotos, imágenes, entre otros contenidos.
- Cookies: son archivos pequeños que descarga la web en la que se navega, impactando en el ordenador del usuario según su tipo. Tenemos primero las cookies de preferencia, que "recuerdan" al navegador la predilección del usuario sobre el contenido de la página para que, en el próximo ingreso, sean mostrados estos o contenidos asociados. Las cookies de transición son las que se usan para compras electrónicas, indicando los detalles de la operación, y duran pocas horas. Para concluir, las cookies analíticas son aquellas que recaban información sobre los gustos para analizar las preferencias de varios grupos de usuarios. Una vez realizada la adquisición, preservación, obtención y presentación, quedará analizar la intencionalidad del acceso, dado que el usuario puede haber sido redireccionado; es así que no necesariamente demuestra una 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 (Zucker, 2007). Por el contrario, el análisis forense de redes implica la recopilación de pruebas digitales que pueden ser transitorias y no conservarse en medios de almacenamiento permanentes, distribuyéndose a través de redes complejas y de 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 que muchas herramientas comerciales de análisis de intrusiones resultan inadecuadas para los entornos distribuidos en red de la actualidad.

Además, en el sector comercial, el uso de los servicios y aplicaciones populares de la red como Facebook, YouTube, WhatsApp, Twitter, Google, entre otros, es gratuito, ya que la fuente principal de ingresos es la publicidad. En este sentido, el objetivo de los 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 (Azzolin & Sain, 2017).

F. ELEMENTOS DEL PROCEDIMIENTO FRENTE A UN SISTEMA

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

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

Con este contexto, debemos interactuar con el equipo. En el supuesto de que esté apagado, debe mantenerse 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 debe moverse el mouse periódicamente para evitar un posible bloqueo por inactividad. Entre los procedimientos a

seguir se encuentran la adquisición de la IP si el equipo está conectado a la red y el registro de la información de los menús y archivos activos, realizando la menor actividad posible con el teclado. Si el equipo está encendido y existe una creencia razonable de que el sistema está destruyendo la evidencia, se deberá proceder a su desconexión inmediata, siendo recomendable en las notebooks remover la batería.

Una vez hecho esto, se deberán retirar con bolsas especiales antiestáticas o, en su defecto, de papel madera, los discos rígidos y otros dispositivos de almacenamiento informático electromagnéticos que se encuentren al alcance. Deben colocarse etiquetas en los cables para facilitar la reconexión posterior, y sellar cada entrada o puerto de información con cinta de evidencia. También deben llevarse los manuales, documentación, anotaciones asociadas, cables y accesorios.

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 concepto de 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. Es, 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 el profesional deberá detectar cuáles son los importantes para luego secuestrarlos y realizar un peritaje profundo. Además, cuenta con la ventaja de ser de simple realización, no siendo necesario un recurso altamente capacitado para esta fase.

Con este método, finalmente podrá extraerse del dispositivo del sospechoso lo que se denomina archivo de evidencia lógica, que es un contenedor que solo incluye los archivos relevantes para la investigación.

F.2. OBSERVACIONES EN MEMORIAS DE ALMACENAMIENTO

Al actuar sobre la información, el especialista no realiza un respaldo de los datos, dado que debe trascender más allá de las herramientas que le presenta el sistema operativo. Por ello

ejecuta una copia forense, la cual emplea una técnica de copiado bit a bit que permite 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 verifica la integridad de la reproducción mediante un valor que debe ser coincidente. Este valor es conocido como hash, que definimos como 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 (Donohue, s. f.).

Este valor es una especie de firma que surge de un cálculo matemático derivado del contenido del disco o dispositivo de almacenamiento. Por este motivo, el valor hash del disco del sospechoso deberá ser exactamente el mismo que el de la copia forense cuando esta se haya realizado correctamente.

Las funciones de hash pueden ejecutarse utilizando algoritmos criptográficos como MD5 (128 bits), SHA-1 (160 bits) o SHA-256 (256 bits). No obstante, los dos primeros han comenzado a usarse únicamente en forma combinada, calculando ambos valores para un mismo archivo, debido a que individualmente son vulnerables y los abogados pueden cuestionar la validez de la evidencia.

Este valor quedará registrado en el acta de procedimiento como prueba de fidelidad de la copia bit a bit, o podrá adjuntarse directamente el reporte emitido por el software utilizado.

Es importante destacar que desde el momento en que se realizó la copia forense hasta que se perita la información contenida puede pasar mucho tiempo, incluso años, y es probable que no sea el mismo perito quien realice ambas actividades. Por este motivo, antes de iniciar la pericia debe verificarse nuevamente la integridad de la copia, recalculando el valor hash para asegurarse de que no fue alterada.

Por último, debemos mencionar la particularidad de los dispositivos móviles, en los cuales no existe una copia forense tradicional, sino una extracción forense. Esto es debido a que el hardware de un teléfono celular está compuesto por diferentes memorias físicas, como chips soldados, y requieren que el equipo esté encendido para su funcionamiento. En cambio, en las computadoras de escritorio, notebooks o servidores, el hardware consiste en un conjunto de componentes que integran un sistema, pero que pueden analizarse 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 anonimato absoluto en la navegación ni en el uso de Internet. Aunque se utilicen programas que ofrecen navegación anónima como TOR, proxys u otros, estos servicios también pueden verse comprometidos o contener fallas.

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

Es importante aclarar la diferencia entre hacking ético y hacking malicioso. La distinción radica en el uso que se da a la información y al acceso obtenido. Ambas modalidades comparten prácticamente las mismas metodologías y herramientas, motivo por el cual muchos programas antivirus pueden impedir la ejecución de herramientas de hacking.

En este punto se vuelve imprescindible usar máquinas virtuales, sistemas ejecutables desde Live CDs o dispositivos de arranque que no contengan software de seguridad, como antivirus o firewalls, que pueda interferir con las herramientas utilizadas en el peritaje. El hacker ético, al igual que el malicioso, no debe utilizar un sistema común que pueda ser fácilmente identificado o que contenga información personal del investigador o de la institución.

Así como no existe una única forma o vector de ataque, tampoco es posible recomendar un único programa que sirva para investigar o frenar todos los ataques. Este trabajo presenta una serie de pautas seguidas por los atacantes en distintos entornos y evalúa diversos programas que pueden ayudar a identificar y obtener evidencias de la actividad del agresor (Proaño Freire, 2012). El tiempo es un elemento valioso para 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 hayan sido borrados los registros y exista colaboración de los equipos intermedios.

F.4. INVESTIGACIÓN DEL CORREO ELECTRÓNICO

El análisis forense de correos electrónicos requiere actividad sobre el equipo y sobre la red, dado que podemos encontrar datos distribuidos que permitan darle consistencia a los correos

hallados, logrando que sean evidencia válida. Para poder emplearlos como prueba es necesario analizar completamente un correo, ya que consta de dos partes de investigación:

- Investigación estática: está compuesta por el análisis del contenido de un correo electrónico proveniente de servidores locales, corporativos o de la web. Se indaga el cuerpo del correo y los archivos adjuntos de las distintas bandejas, recabándose los datos depurados, es decir, los eliminados. Se analiza el intercambio de correos, verificando el envío y la recepción de la casilla, y se realiza la búsqueda simple, compleja e indexada del contenido.
- Investigación dinámica: es aquella que alcanza información del origen geográfico y los logs de servidores SMTP, es decir, de correo saliente que emplea el protocolo simple de transferencia de correo.

Para que un correo sea presentado como prueba, se requiere que se introduzca la información completa, incluyendo las cabeceras y los datos de tráfico. Por este motivo no es válido presentar únicamente la impresión en papel del cuerpo del mensaje.

F.5. REDES SOCIALES

La creación de perfiles falsos es habitual y puede detectarse fácilmente en los residuos de navegación de los dispositivos. 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, acreditar una suplantación de identidad en una red social y documentar un caso de violencia digital como ciberacoso, ciberbullying o sextorsión (Grupo Globatica, s. f.).

También es necesario acceder a los datos de los servidores de las empresas que brindan servicios de mensajería o redes sociales. Para ello deberá realizarse un pedido formal de resguardo de información, datos de navegación, entre otros, siguiendo el procedimiento de solicitud requerido por la empresa prestadora.

En el ámbito civil la información se solicita mediante oficios judiciales dirigidos a las empresas o a otros juzgados, según se trate de datos de tráfico o de contenido. En el ámbito penal existen mecanismos especiales o servicios ofrecidos discrecionalmente por algunas empresas, así como canales específicos como GDTLDTI o INTERPOL.

Con herramientas específicas, el perito puede complementar los datos hallados en los dispositivos secuestrados, integrando fechas y fragmentos de conversaciones con los archivos temporales de Internet del navegador.

Respecto de las fotografías e imágenes, constituyen un elemento relevante de peritaje para la adquisición de evidencias. Los metadatos EXIF (Exchangeable Image File Format) son un estándar creado para almacenar información de las fotos tomadas con cámaras digitales, incluyendo datos relativos a la propia imagen y a cómo ha sido capturada. Estos metadatos permiten obtener información como la marca de la cámara o teléfono con que se tomó la imagen, la fecha e incluso la ubicación GPS.

G. CADENA DE CUSTODIA

La cadena de custodia es el registro detallado del movimiento de la evidencia durante el proceso probatorio. En este registro se indican todas las actividades efectuadas, las personas responsables y el momento y el estado en el que se encuentra la evidencia. El registro no evita que la evidencia sea vulnerada, sino que permite saber, en caso de que suceda, qué fue lo que ocurrió y quién era el responsable en ese momento. Su finalidad es asegurar y demostrar la identidad, integridad, preservación y continuidad de la prueba, iniciándose al momento de su recolección y finalizando con la culminación de la etapa probatoria.
La cadena de custodia se registra en un formulario específico y en el expediente judicial, debiendo incluir, entre otros datos, el nombre de la persona responsable, la fecha de contacto con la evidencia y las actividades realizadas.

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 sean de cumplimiento obligatorio. A nivel mundial se destacan ISO IEC 27037:2012, ISO IEC 27042:2015 y RFC 3227. En Argentina no existe normativa local, mientras que a nivel europeo corresponde mencionar algunas, como 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. Proporciona pautas para actividades específicas en el manejo de evidencia digital, como identificación, recopilación, adquisición y preservación de evidencia digital potencialmente valiosa. Además suministra orientación respecto de situaciones comunes del proceso de manejo de evidencia digital y ayuda

a las organizaciones en sus procedimientos disciplinarios, así como en el intercambio de evidencia potencial entre jurisdicciones (ISO, 2012).

La norma brinda una lista indicativa y no exhaustiva de 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, dispositivos electrónicos personales, tarjetas de memoria.
- Sistemas de navegación móviles.
- Cámaras digitales fijas y de video, incluido CCTV.
- Computadoras estándar con conexiones de red.
- Redes basadas en TCP IP y otros protocolos digitales.
- Dispositivos con funciones similares a los anteriores.

Otra norma importante es la ISO IEC 27042:2015, denominada guía con lineamientos para el análisis e interpretación de evidencia digital. Brinda orientación sobre el estudio de la evidencia digital abordando cuestiones de continuidad, validez, reproducibilidad y repetibilidad. Agrupa las mejores prácticas para la elección, diseño e implementación de procesos analíticos y exige registrar suficiente información para permitir el escrutinio independiente del procedimiento cuando sea necesario. También proporciona orientación sobre mecanismos adecuados para demostrar la competencia del equipo de investigación.

El análisis y la interpretación de evidencia digital pueden ser procesos complejos. En algunos casos puede haber varios métodos posibles y el equipo de investigación deberá justificar la selección del proceso particular y mostrar equivalencias con métodos utilizados por otros investigadores. En otras circunstancias puede ser necesario desarrollar nuevas técnicas para examinar pruebas digitales no consideradas previamente, debiendo demostrarse que el procedimiento es adecuado para su propósito.

La evidencia digital disponible puede influir en la selección de métodos adicionales aplicados sobre información ya adquirida. La ISO IEC 27042:2015 proporciona un marco común para los elementos analíticos e interpretativos del manejo de incidentes de seguridad de la información, que puede utilizarse para implementar nuevos métodos y ofrecer un estándar mínimo común para la evidencia digital producida en tales actividades (ISO, 2015).

El documento publicado por el Grupo de Trabajo de Ingeniería de Internet recoge directrices para recopilar y almacenar evidencias sin ponerlas en riesgo. RFC 3227 proporciona pautas generales para la recolección y 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 se analiza el mecanismo de protección de la integridad proporcionado por EnCase y FTK, basado en códigos de resumen de mensajes conocidos como MDC. Dichos códigos no son totalmente resistentes a la manipulación y pueden falsificarse. El modelo propuesto para proteger la integridad de la evidencia digital mediante el uso de tarjetas inteligentes y criptografía de clave pública establece una plataforma segura para firmar digitalmente los códigos de resumen de mensajes y superar estas debilidades (Saleem & Popov, 2011).

Finalmente, también resulta relevante mencionar las normas empleadas en España. Las regulaciones de la Asociación Española de Normalización y Certificación para UNE 71505 y UNE 71506 proporcionan una metodología para la preservación, adquisición, documentación, análisis y presentación de pruebas digitales. Según la asociación, estas normas permiten dar respuesta a infracciones legales e incidentes informáticos en empresas y entidades, logrando pruebas más robustas y fiables y facilitando la determinación de si la causa del incidente fue intencional o negligente. Son aplicables a cualquier organización, independientemente de su actividad o tamaño, y a cualquier profesional competente del ámbito pericial. Se dirigen especialmente al personal de seguridad, de gestión de incidentes y al personal técnico que trabaje en laboratorios o entornos de análisis forense de evidencias electrónicas (Gervilla Rivas, 2014).

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 técnicas avanzadas empleadas por los ciberdelincuentes para realizar sus delitos, sino también al mayor conocimiento de los usuarios y a la competencia entre las empresas desarrolladoras de sistemas operativos y dispositivos para brindar productos con la menor cantidad posible de vulnerabilidades.

Por ello es necesario contar con lineamientos amplios que permitan ser adaptados a cualquier tecnología y que no se vuelvan rápidamente obsoletos ante la diversidad o el progreso constante. En combinación con procedimientos más flexibles, esto permite atender las solicitudes específicas que cada caso requiera. En este sentido, con normativas que faciliten el acceso más

completo posible al profesional y con la comprensión de la complejidad de estas labores por parte de los operadores del derecho, se logrará obtener la evidencia digital más efectiva.

BIBLIOGRAFÍA

Azzolin, H., & Sain, G. (2017). *Delitos informáticos: Investigación criminal, marco legal y peritaje*. B de F.

Código Procesal Penal de la Provincia de Buenos Aires. (s. f.). Sistema Argentino de Información Jurídica. http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/383/texact.htm

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

Department of Justice. (s. f.). *New approaches to digital evidence acquisition and analysis*. https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis

Donohue, B. (s. f.). ¿Qué es un hash y cómo funciona? *Kaspersky Daily*. https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

Gallegos, M., Purcachi, C., & Almeida, C. (2016). *Informática jurídica*. Universidad Técnica del Norte. https://issuu.com/utnuniversity/docs/ebook-informatica-juridica

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

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

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

Herrera, J. L. (2016). *Informática forense: El manejo integral de la evidencia digital*. Praxiomática. https://praxiomatica.wordpress.com/2016/09/18/informatica-forense-el-manejo-de-evidencia-digital/

ISO. (2012). *ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*. https://www.iso.org/standard/44381.html

ISO. (2015). *ISO/IEC 27042:2015 Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence*. https://www.iso.org/standard/44406.html

MuyComputerPro. (2014). *Perito informático forense, una de las profesiones con más salidas*. https://www.muycomputerpro.com/2014/08/25/perito-informatico-forense

Noblett, M., Pollitt, M., & Presley, L. (2000). Recuperación y examen de evidencia en informática forense. *Ciencias de la Comunicación Forense*, 2(4), 1.

Presman, G. (2004). *Manejo de pruebas digitales en investigaciones de delitos informáticos*. Presentación 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, O. (2011). *Digital forensics and cyber crime: Second International ICST Conference*.

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

Zucker, S. (2007). *Cyber forensics: Part one*. National Criminal Justice Reference Service. https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=242828