PADF
FUNDACIÓN PANAMERICANA PARA EL DESARROLLO

Guía técnica sobre análisis forense y evidencia digital

Proyecto de creación de capacidades del sector judicial ecuatoriano para combatir la delincuencia transnacional y el narcotráfico

CON EL APOYO DE LA OFICINA INTERNACIONAL DE ASUNTOS ANTINARCÓTICOS Y APLICACIÓN DE LA LEY (INL)

Marcela Bueno
Directora PADF Ecuador

Roberto Obando
Director de Programas

EQUIPO CTOC

Andrés Ormaza
Director de proyecto CTOC

Ana María Garzón
Asesora principal

María José Freire
Oficial de proyecto

Johanna Chalén
Apoyo técnico

Yefrin Garavito
Consultor experto

Presentación

La presente Guía técnica para el análisis forense y la evidencia digital se elaboró en el marco del Proyecto de creación de capacidades del sector judicial ecuatoriano para combatir la delincuencia transnacional y el narcotráfico, adelantado por la Pan American Development Foundation (PADF), con el apoyo del Gobierno de los Estados Unidos a través de la Oficina de Asuntos Antinarcóticos y Aplicación de la Ley (INL).

Este documento es una herramienta orientada a apoyar a los funcionarios que ejercen un rol relevante en el sistema de justicia penal. Busca facilitar el diseño e implementación de acciones estratégicas, estructuradas y planificadas, que permitan optimizar los recursos disponibles para fortalecer las instituciones y obtener resultados de alto impacto desde una perspectiva de lucha contra el crimen organizado, esto es, de redes ilícitas complejas.

Contenido

Tabla de ilustraciones:

Abreviaturas:

(ADB) Android Debug Bridge

(DEFR) Primer Responsable de Evidencia Digital

(DES) Especialista en Evidencia Digital

(DVR) Dispositivo Grabador de Video

(FTK) Forensic Toolkit

(IEC) La Comisión Electrotécnica Internacional

(IoT) Internet de las Cosas

(ISO) Organización Internacional de Estandarización

(NIST) Instituto Nacional de Estándares y Tecnología

(RFC) Solicitud de comentarios

(SGEE) Sistema de Gestión de Evidencias Electrónicas

Introducción

El desarrollo de la tecnología ha logrado avances muy importantes para la sociedad actual y se ha convertido en un elemento indispensable para el funcionamiento de las empresas, de los gobiernos, de las instituciones educativas y de las personas en general. Sin embargo, esta dependencia de los sistemas de información y de tecnología ha sido aprovechada por los criminales para cometer delitos informáticos y convencionales en los que se usan los sistemas de información para estafar, robar, suplantar, entre otros.

Este panorama evidencia que las agencias de ley y los órganos de administración de justicia tienen la necesidad de mantenerse actualizados y capacitados sobre la importancia, el uso correcto, la recolección y el análisis de la evidencia digital y la prueba electrónica. En los últimos años se evidencia un incremento de los casos criminales en los que se ha utilizado la evidencia digital como probatoria, esto debido al constante uso de equipos celulares inteligentes, dispositivos de grabación de video (DVR), equipos de cómputo, dispositivos de almacenamiento, entre muchos otros que conservan información importante para el esclarecimiento de preguntas esenciales en la investigación criminal, como: ¿el cómo?, ¿el dónde?, ¿el cuándo?, ¿el qué?, ¿el quién? y ¿con qué?

La Fundación Panamericana para el Desarrollo (PADF), en virtud del convenio de colaboración con las autoridades del sistema de justicia penal de Ecuador, y conociendo la necesidad de sus funcionarios en estandarizar conceptos clave que sirvan como base para la correcta fijación, recolección, análisis, procesamiento y presentación en audiencia de la evidencia digital y la prueba electrónica, ha decidido presentar esta guía para su uso dentro de las etapas del proceso penal ecuatoriano, con el fin de unificar criterios que estén acordes a los estándares internacionales y a las buenas prácticas.

Informática forense

La informática forense es la disciplina de las ciencias forenses que utiliza los conocimientos técnicos y generales de las ciencias computacionales y de la ingeniería de sistemas para apoyar la administración de justicia en la investigación de delitos en los que se encuentren vinculados sistemas de información, medios de almacenamiento digital o electrónico, sistemas de telecomunicaciones o similares, con el propósito de lograr el esclarecimiento de los hechos mediante la identificación, la preservación, la extracción, el análisis, la interpretación, la documentación y la presentación final de la evidencia y los resultados obtenidos dentro de un proceso judicial.

A nivel internacional, se pueden encontrar otros nombres como *network forensics* (forensia en redes), *computer forensics* (computación forense) o *digital forensics* (forensia digital), términos utilizados en algunos escenarios que podrían causar confusión; sin embargo, todos convergen a la rama general de la informática forense.

Principios de la informática forense

Toda ciencia cuenta con principios, que rigen sus metodologías, análisis y prácticas. Los principios se entienden como generales para todas las investigaciones relacionadas con la informática forense y siempre van acompañados por un método científico que permite sustentar y comprobar los resultados generados por el investigador o perito en cualquier parte del mundo.

En esta medida, el conocimiento de los cuatro principios fundamentales de la informática forense son determinantes para desarrollar investigaciones rigurosas y de validez científica. Estos principios son: confidencialidad, disponibilidad, integridad y no repudio.

Confidencialidad

Es la propiedad de la información que garantiza que la información obtenida no sea disponible o divulgada a los individuos, entidades o procesos no autorizados (ISO/IEC 27000, 2018).

Disponibilidad

Propiedad de los datos y sistemas de información que garantiza que sean accesibles y utilizables en el tiempo y la forma autorizada (OCDE).

Integridad

Es la propiedad, exactitud y completitud de la información (ISO/IEC 27000, 2018). La Integridad considera todas las posibles causas de modificación, incluyendo fallos en software y hardware, eventos medioambientales e intervención humana (ITIL, 2007).

No repudio

Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron. (UNE-ISO/IEC 27000, 2014). Se entiende como la forma de probar que un suceso fue originado por un sistema o iniciador, así mismo que fue recibido por el receptor.

Aplicaciones y usos

La informática forense, hoy en día, es una disciplina transversal en la administración de justicia ya que gracias a sus procedimientos, técnicas y herramientas se pueden encontrar, analizar y presentar evidencia de tipo digital y pruebas electrónicas que permitan demostrar circunstancias de modo, tiempo o lugar, para lograr la efectiva judicialización de las personas que infringen las leyes. Así mismo, la informática forense tiene aplicación en el campo penal y ha ganado terreno en los procesos civiles, administrativos, comerciales, familiares y disciplinarios.

Cabe resaltar que para que esta evidencia digital sea válida dentro de cualquier tipo de proceso judicial, es importante que cumpla con unos requisitos y estándares que se han establecido a nivel internacional y que deben ser adquiridos bajo buenas prácticas de los funcionarios, peritos o personal que tenga contacto con este tipo de elemento o evidencia.

Procedimientos estandarizados

ISO/IEC 27037 y 27042

La Organización Internacional de Estandarización (ISO) promueve el desarrollo y la implementación de estándares internacionales, está compuesta por diversas organizaciones nacionales de normalización y actualmente cuenta con 164 miembros; es una de las autoridades en cuanto a normas técnicas y estándares internacionales. De igual forma, la Comisión Electrotécnica Internacional (IEC, por su sigla en inglés) es una organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas.

Si se tiene en cuenta la importancia de la gestión de la información, las organizaciones ISO e IEC crearon un conjunto de estándares de la familia 27000, enfocadas a los sistemas de gestión de seguridad de la información.

El estándar internacional ISO/IEC 27037 da las directrices para identificar, recolectar, adquirir y preservar la evidencia digital. En este proceso participan dos actores importantes: el Primer Responsable de Evidencia Digital (DEFR, por su sigla en inglés) y el Especialista en Evidencia Digital (DES, por su sigla en inglés). El papel del DEFR es identificar, recolectar, consolidar y preservar la posible evidencia digital en la escena del incidente, de igual manera incluye elaborar un informe de recopilación y adquisición, pero no necesariamente el informe de análisis, ya que este será responsabilidad del DES.

Uno de los roles importantes del DEFR es asegurar la integridad y autenticidad de la evidencia digital potencial mediante el uso de herramientas adecuadas y funciones de algoritmos alfanuméricos, como el HASH. En esta medida, el DEFR debe contar con la experiencia adecuada, habilidades y conocimientos en el manejo de la evidencia digital potencial, esto es indispensable ya que la evidencia digital potencial puede ser fácilmente vulnerable.

Por su parte, el DES proporciona conocimientos especializados que pueden ser utilizados para analizar, interpretar y generar conclusiones del estudio de la evidencia digital.

Familia UNE

La Asociación Española de Normalización, desde el 2013, publicó las siguientes normas:

UNE 71505-1:2013 Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales.

UNE 71505-2:2013 Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas.

UNE 71505-3:2013 Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 3: Formatos y mecanismos técnicos.

UNE 71506:2013 Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas.

Estas normas definen el sistema de gestión de evidencias electrónicas (SGEE), los formatos de intercambio y los mecanismos técnicos aplicables para el mantenimiento de su confiabilidad. Las tres partes

de la norma 71505 se aplican en cualquier organización independiente de su actividad o tamaño, así mismo, son aplicables a las entidades o empresas que proporcionen servicios parciales o totales relacionados al ciclo de vida de las evidencias o controles del sistema de gestión de evidencias electrónicas.

RFC 3227

Los RFC (Request For Comments) son documentos globales que consolidan propuestas (3227, 2002) de expertos en una rama del conocimiento generalmente enfocado a la informática, con el fin de establecer, por ejemplo, una serie de pautas para llevar a cabo un proceso, la creación de estándares o la implementación de algún protocolo. No todas las RFC son normas, a cada RFC se le asigna una denominación con respecto al estado en el proceso de estandarización de internet. La denominación puede ser: informativo, experimental, mejor práctica actual (BCP, por su sigla en inglés), pistas estándar, o históricos.

El RFC 3227 es un documento (BCP) que recoge las directrices para recopilar y almacenar evidencias, y sirve como estándar de facto para la recopilar información en incidentes de seguridad informática. Este documento está en línea desde el 2002 y sigue siendo una guía para actividades de recolección y tratamiento de evidencia digital.

HB171-2003

El Manual de Buenas Prácticas para las Directrices de la Gestión de Evidencias de TI publicado en el 2003 por la Oficina Australiana de Estándares define el ciclo de vida de la evidencia digital y pruebas electrónicas desde el momento de la recolección hasta la presentación dentro de la audiencia pública, así mismo, dicta los lineamientos para el código de conducta de los testigos expertos y los principios rectores en la producción probatoria.

Este manual de buenas prácticas ha sido la base fundamental para guías a nivel internacional de las agencias de ley que procesan y recolectan evidencia digital.

NIST SP-800-86

El Instituto Nacional de Estándares y Tecnología (NIST), del Departamento de Comercio de los Estados Unidos, creó esta publicación especial denominada Guía para la Integración de Técnicas Forenses en la Respuesta a Incidentes, que establece lineamientos básicos y buenas prácticas, e incluye las sugerencias para la creación de políticas y definición de roles en los laboratorios forenses, las recomendaciones y directrices para realizar el procedimiento de identificación, recolección forense, y finalmente presenta los lineamientos generales para el análisis de datos, tráfico de redes y aplicaciones. De esta forma promueve un marco general de buenas prácticas.

Herramientas

Al ser la informática forense una disciplina de la investigación criminal, que estudia la evidencia digital, es indispensable utilizar las herramientas tecnológicas que permitan el acceso, fijación, recolección, extracción, aseguramiento, análisis y procesamiento de datos. Dentro de las herramientas que son necesarias para el apoyo de las actividades de investigación forense digital se encuentran los software y hardware especializados, tanto libres como comerciales.

A la hora de adquirir estas herramientas, es indispensable tener en cuenta que hay organizaciones mundiales que se encargan de realizar las pruebas para comprobar su fiabilidad y garantizar su uso efectivo dentro de los procesos judiciales. Una de las organizaciones encargadas de estos estudios es el Instituto Nacional de Estándares y Tecnología (NIST), del Departamento de Comercio de los Estados Unidos, especialmente por medio de su Programa de Prueba de Herramientas de Informática Forense (CFTT).

MSAB XRY

Micro Systemation (MSAB) es una compañía líder y pionera en desarrollar soluciones forenses orientadas a dispositivos móviles, enfocadas a cubrir necesidades de departamentos de investigación alrededor del mundo. Su producto principal XRY permite a los investigadores lograr extraer gran cantidad de información de las diversas fuentes de almacenamiento vinculadas a los dispositivos móviles (Memoria interna, tarjeta SIM, tarjeta de almacenamiento externa y la nube), además, de permitir realizar extracciones simultáneas a través de un HUB de extracción de alta velocidad. Otra característica resaltante de XRY es que sus extracciones de nivel lógico y físico contienen información de auditoría al proceso de extracción, generación automática de código HASH, posibilidad de extraer data eliminada, posibilidad de acceder a una serie de dispositivos que se encuentren protegidos por contraseña de acceso, brindar protección a través de encriptación a su archivo propietario de extracción, lo cual en su conjunto lo hace la solución más completa para laboratorios forenses que deben garantizar la auditabilidad e integridad de la información de principio a fin.

Ilustración 1: Micro Systemation (MSAB) - XRY

Micro Systemation MSAB, a través de XAMN y sus módulos integrados de análisis, permite a los investigadores buscar y analizar las evidencias de manera sencilla y fácil en un entorno de trabajo limpio y práctico para los investigadores, permitiendo crear relaciones y vínculos de manera automática a partir de registros de intercambio de mensajes de texto, mensajes por aplicaciones y/o registros de llamadas, asimismo, cuenta con una vista de chats que permite entender de mejor manera información de aplicaciones como Facebook Messenger, Instagram o WhatsApp, por mencionar algunas. También, es capaz de presentar una vista de posicionamiento geográfico a partir de identificar de manera automática los metadatos de posicionamiento (GPS) dentro de toda la evidencia extraída. XAMN, cuenta con un motor de inteligencia artificial (IA) que permite agilizar la identificación automática de imágenes relacionada a desnudez, armas, drogas, dinero, entre otras.

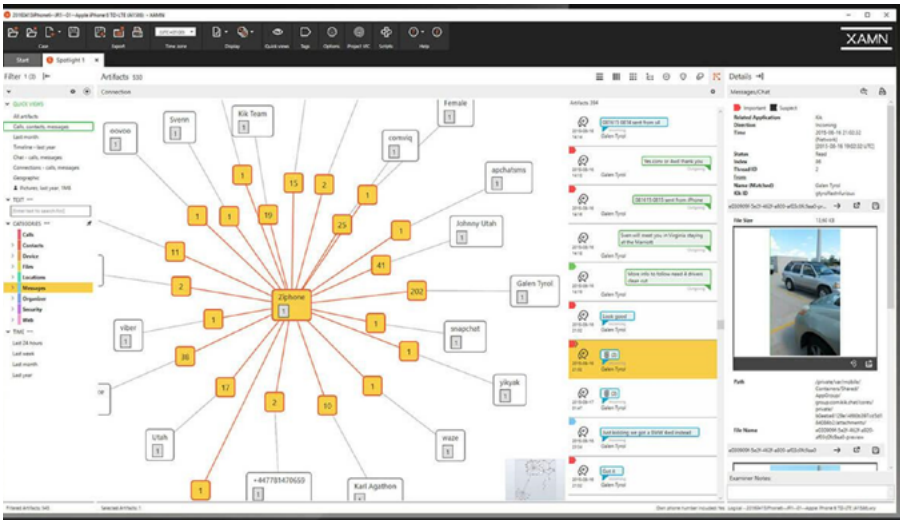


Ilustración 2: Micro Systemation (MSAB) - XAMN

Software

En el mercado existe gran variedad de software que puede ser adquirido de forma comercial o gratuita. A continuación, se relacionarán las herramientas forenses más usadas por las agencias de ley, haciendo énfasis en algunas herramientas gratuitas que son válidas para emplear dentro de procesos judiciales por los operadores judiciales:

FTK Imager

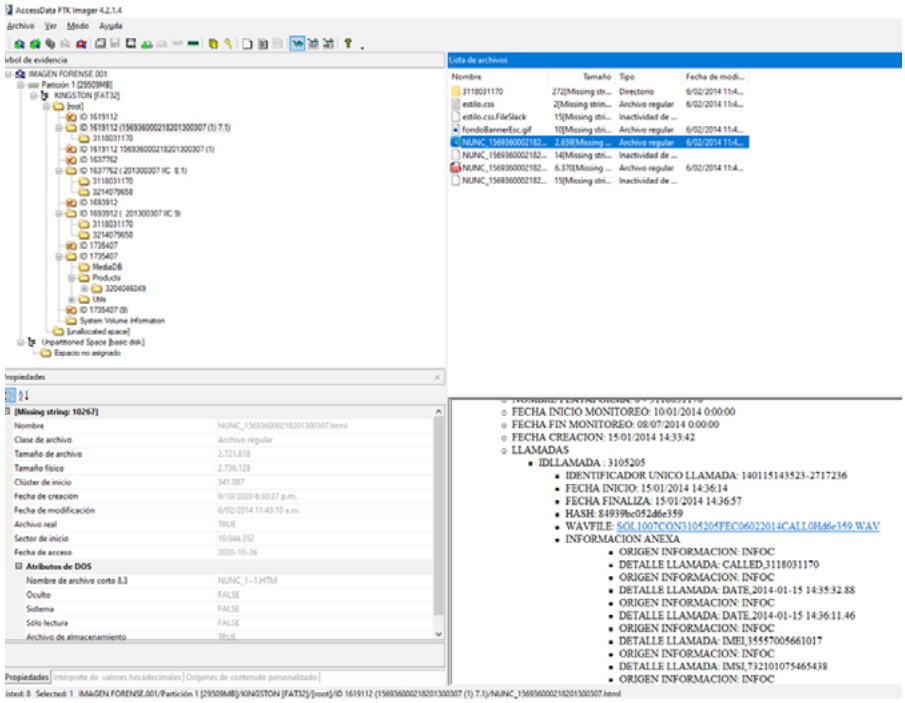


Ilustración 3: Impresión de pantalla de FTK Imager

FTK Imager es una herramienta gratuita para obtener imágenes y vistas previas de los datos que permiten evaluar rápidamente la evidencia electrónica para determinar si se justifica un análisis adicional con una herramienta forense de procesamiento.

FTK Imager también puede crear copias bit a bit (imágenes forenses) de datos informáticos sin realizar cambios en la evidencia original. La imagen forense que se obtiene es idéntica en todos los aspectos a la original, incluido el tamaño del archivo y el espacio no asignado o el espacio libre en la unidad. Esto permite almacenar los medios originales lejos para tenerlos a salvo de daños, mientras continúa la investigación a través de la imagen obtenida.

Finalmente, esta herramienta también se usa para generar informes hash de archivos regulares e imágenes de disco, como punto de referencia para demostrar la integridad de la evidencia de su caso. Cuando se crea una imagen de una unidad completa se puede usar un hash generado por FTK Imager para verificar que el hash de la imagen y el hash de la unidad coinciden después de que se crea la imagen y así concluir que la imagen no ha cambiado desde la adquisición (AccessData, s.f.).

FTK (Forensic Tool Kit)

Esta herramienta de access data es una de las más usadas a nivel global por las agencias de ley, ya que gracias a sus robustos motores de búsqueda permite realizar un análisis y procesamiento de la evidencia en el laboratorio, a través de la búsqueda indexada de artefactos, por lo que hace la tarea de los analistas mucho más simple. Es importante tener en cuenta que para lograr mejores resultados, los investigadores o líderes de la investigación deben saber qué es lo que se necesita buscar para optimizar el trabajo.

A través de esta herramienta de procesamiento de evidencia digital se puede recuperar archivos borrados, contraseñas, realizar análisis automatizados de imágenes y archivos comunes, entre otras funciones útiles en los procesos investigativos.

EnCase

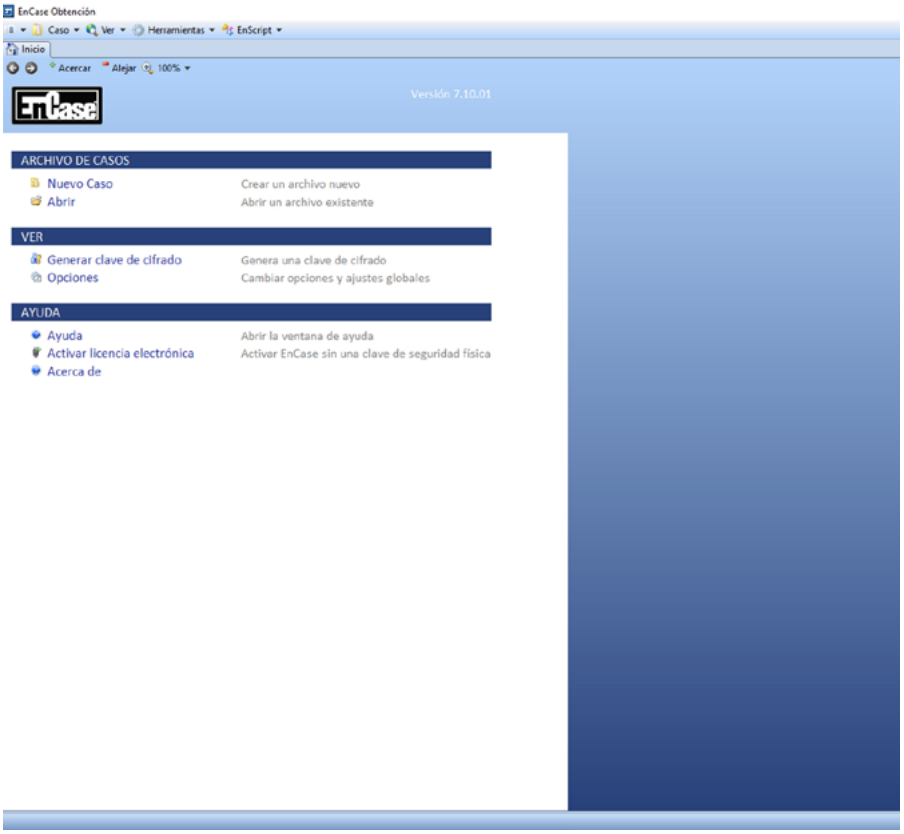


Ilustración 4: Impresión de pantalla EnCase

Este software de la casa matriz Guidance Software, se encarga de todas las etapas del proceso, desde recolectar, asegurar, analizar hasta generar reportes sobre la evidencia digital. Es usado por muchas agencias de la ley y empresas privadas, ya que brinda apoyo en el análisis de evidencia de equipos móviles, tabletas, GPS entre otros.

Autopsy

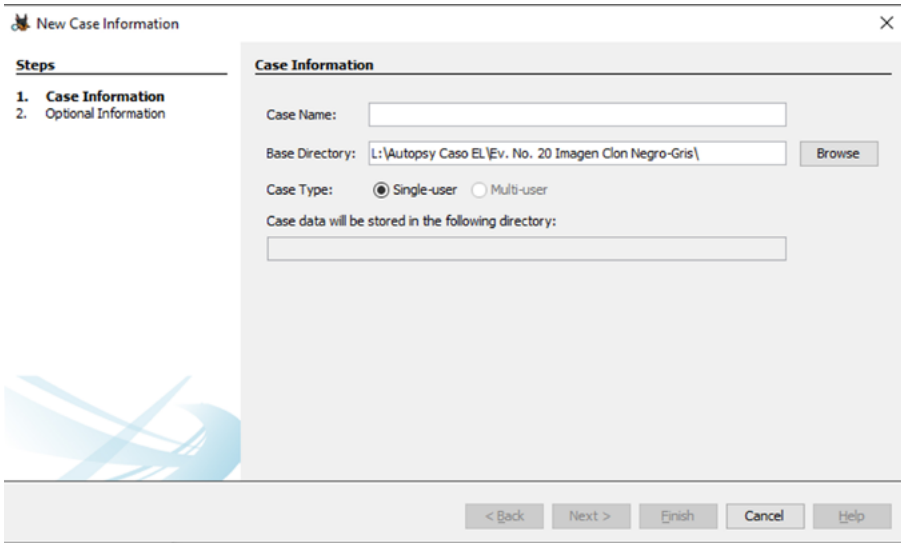


Ilustración 5: Impresión de pantalla Autopsy

Esta herramienta es la principal plataforma de análisis forense digital de código abierto de un extremo a otro, con decenas de miles de usuarios y desarrolladores en todo el mundo. Autopsy evoluciona con las necesidades del usuario ya que presenta nuevos módulos creados por la comunidad activa de Autopsy y actualizaciones periódicas aportadas por Basis Technology. Al ser una herramienta gratuita y muy completa, ha ganado mucho terreno dentro de algunas agencias de la ley, sobre todo en Europa y Estados Unidos, puede ser complementada con algunas otras herramientas.

Axiom

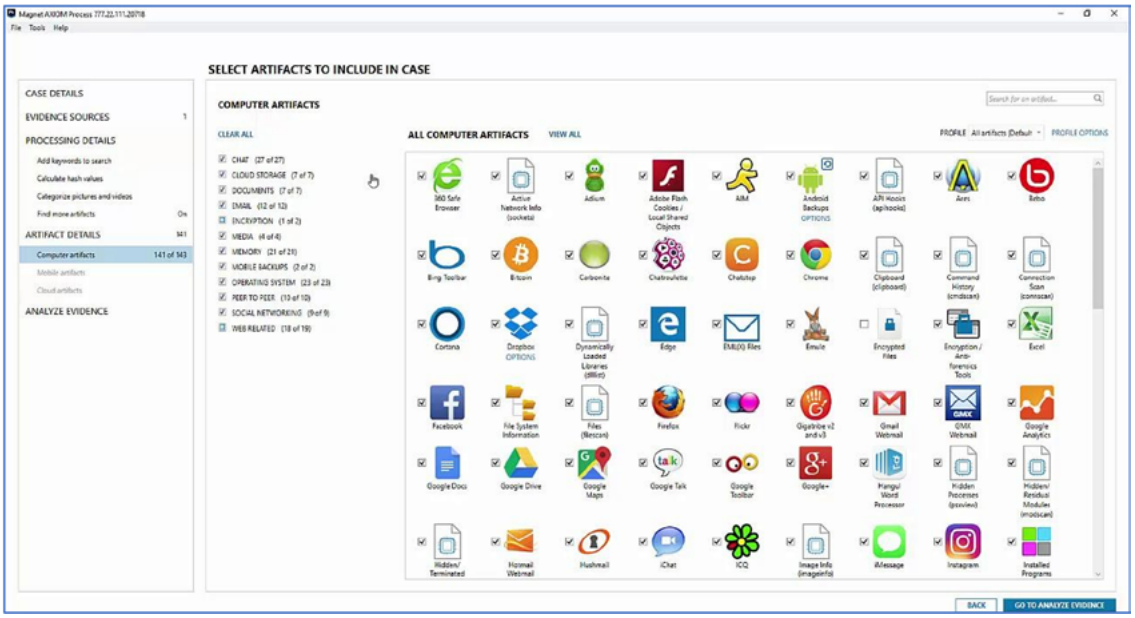


Ilustración 6: Impresión de pantalla Magnet Axiom

Axiom es la plataforma de investigación más completa, ya que tiene la capacidad de recuperar, analizar e informar sobre datos de fuentes móviles, informáticas y en la nube; su función más reconocida es la elaboración de la línea de tiempo que analiza datos en todas las fuentes probatorias, integrándolos visualmente para el investigador. Esta herramienta es una de las más nuevas en el mercado por su gran versatilidad.

Cellebrite UFED Physical Analyzer

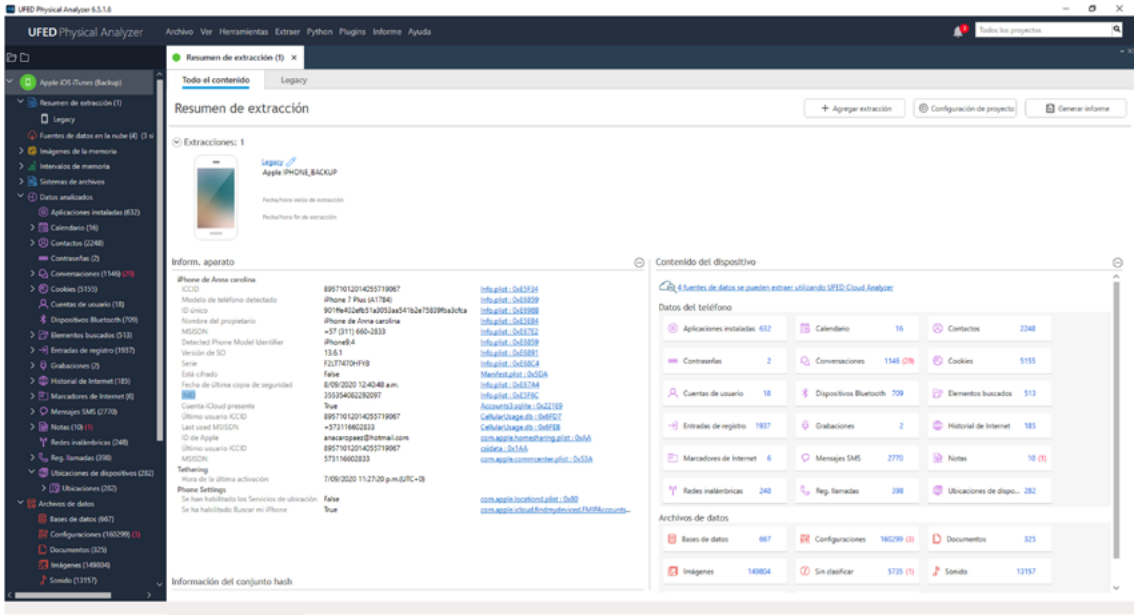


Ilustración 7: Impresión de pantalla UFED PA.

Esta herramienta complemento del equipo UFED permite examinar múltiples fuentes de datos desde la más amplia gama de aplicaciones móviles, dispositivos digitales, devolución por órden judicial y de la nube. Es uno de los productos más usados en el procesamiento de evidencia de dispositivos móviles, gracias a que, junto con las herramientas de extracción, es capaz de recuperar los elementos borrados de aplicaciones tan comunes como WhatsApp, Telegram o similares.

Su uso ha sido importante durante los últimos años gracias a la integración de sus bases de datos con otras herramientas de análisis, lo que permite hacer un trabajo más completo y eficaz.

MOBILedit Forensic Express

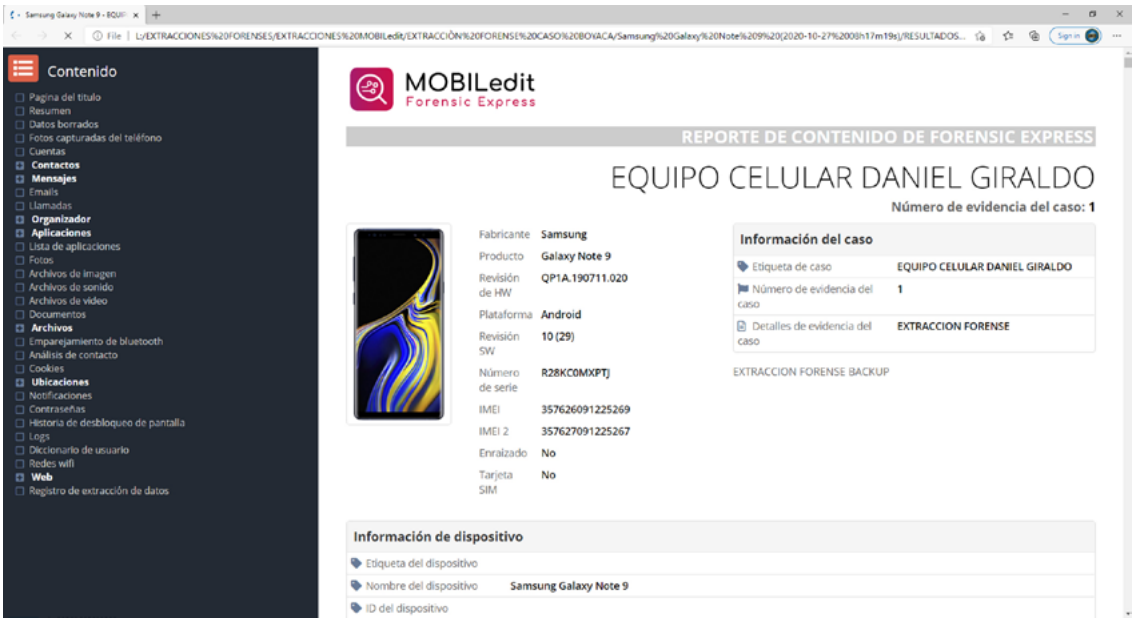


Ilustración 8: Impresión de pantalla MOBILedit Forensic Express

Es una herramienta dedicada a la extracción forense de información de celulares y de la nube, ya que es un gran analizador de datos y generador de reportes que usan el método de adquisición de datos físicos y lógicos. MOBILedit es destacado por su avanzado análisis de aplicaciones y de recuperación de los datos eliminados, tiene una variedad amplia de celulares compatibles incluso con modelos nuevos, además de una fácil interfaz de usuario.

Cuenta con la función para saltar la contraseña y PIN, así como también puede obtener acceso a bases de datos ADB o iTunes (Compelson Soft, s.f.).

Oxygen Forensic® Detective

Es una plataforma todo en uno de software forense, creada para extraer, decodificar y analizar los datos de múltiples fuentes digitales: dispositivos móviles y de IoT, copias de seguridad de dispositivos, UICC y tarjetas de medios, drones y servicios en la nube. Oxygen Forensic® Detective también puede encontrar y extraer una amplia gama de artefactos, archivos de sistema y credenciales de máquinas Windows, macOS y Linux (Oxygen Forensic, s.f.).

CAINE

CAINE (Computer Aided Investigative Environment) es una distribución gratuita en vivo de GNU / Linux italiana creada como un proyecto de Digital Forensics. CAINE ofrece un entorno forense completo que está organizado para integrar herramientas de software existentes, como módulos de software, y proporcionar una interfaz gráfica amigable, que provee un entorno interoperable que apoya al investigador digital durante las cuatro fases de la investigación digital.

Esta versión es muy usada por los investigadores como herramienta en vivo para recolectar evidencia volátil de los equipos de cómputo, gracias a su variedad de funciones incluidas, además genera un registro que puede ser auditado.

X1 Social Discovery

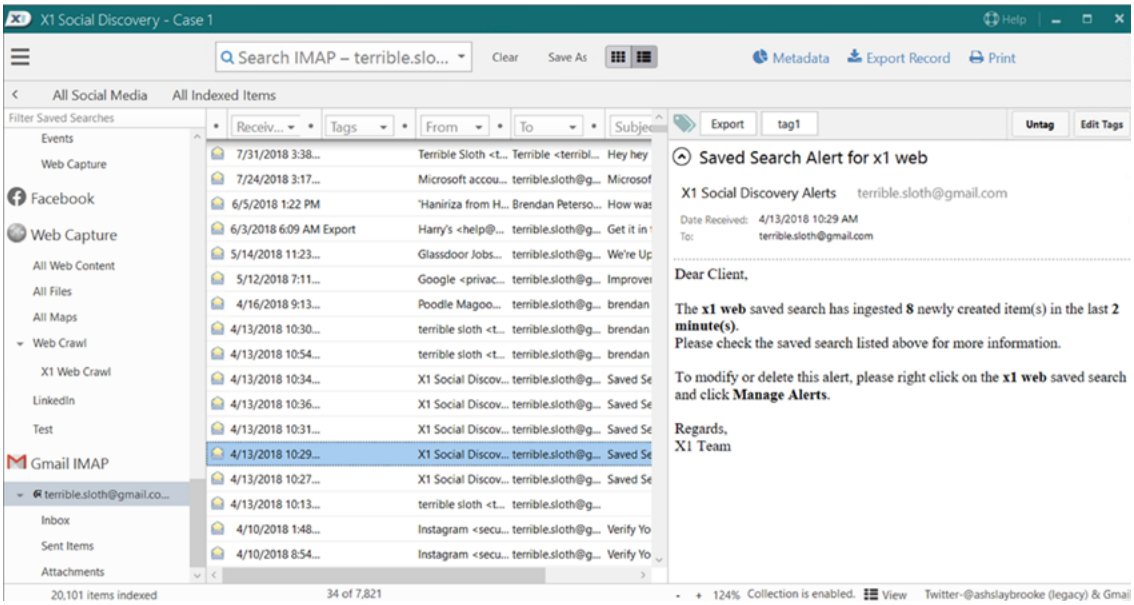


Ilustración 9: Impresión de pantalla X1 Social Discovery

El software X1 Social Discovery está diseñado para asegurar con eficacia el contenido de las redes sociales como Instagram, Facebook, Twitter y Tumblr, Youtube, entre otras. Además, puede rastrear, capturar y buscar al instante contenidos de sitios web, correo web como Hotmail y Gmail.

A diferencia de las soluciones de archivo y captura de imágenes, X1 Social Discovery prevé un flujo de trabajo de caso centrado en la búsqueda y recogida de material de producción en formato nativo de búsqueda, mientras que la preservación de metadatos críticos no es posible a través de la captura de imágenes, impresiones, o de archivo de datos en bruto de los canales RSS.

Hardware

Para las diversas fases de la investigación digital forense, se requieren algunos equipos de hardware que garantizan el cumplimiento de las buenas prácticas y normativas internacionales para recolectar y preservar la evidencia. A continuación se enunciarán las más comunes:

Bloqueadores de escritura

Ilustración 10: Bloqueador forense (fuente: Open text Security)

Los medios digitales son objeto de alteración voluntaria o involuntaria, por eso, para los investigadores forenses, es indispensable proteger los elementos materiales probatorios, en este caso la evidencia digital. En la actualidad existen diversas marcas de bloqueadores de escritura que impiden que se modifique o altere un medio de almacenamiento que esté en proceso de adquisición o análisis, para facilitar y garantizar la integridad y autenticidad del medio probatorio.

Este dispositivo bloqueador permite la ejecución de comandos de lectura, pero no permite que se ejecuten comandos de escritura en la unidad de almacenamiento. La mayoría de las herramientas de creación de imágenes forenses tienen un bloqueador de escritura anexo que el perito puede utilizar para crear la imagen forense del dispositivo de almacenamiento. Aunque se debe aclarar que el bloqueo de escritura también se puede realizar por medio de herramientas de software, se considera mejor optar, en todas las ocasiones, por las soluciones de hardware.

Duplicador forense

Ilustración 11: Duplicador forense Tx1 y TD2U (Fuente: Open Text Security)

Los duplicadores forenses son herramientas que permiten realizar una imagen forense o una copia exacta de un dispositivo de almacenamiento digital. Al ser dispositivos dedicados, el tiempo de creación de imagen es inferior que al realizado vía software, incluso por hardware se puede completar la tarea en menos de la mitad del tiempo.

Los formatos usados por los duplicadores son universales para la mayoría de las plataformas de análisis y procesamiento, como FTK, Encase, Axiom, Autopsy, entre otros.

Extractores de información de dispositivos móviles

Ilustración 12: Equipos de extracción forense (Fuente: Oxygen - MobilEdit)

Ilustración 13: Equipos de extracción forense (Fuente: UFED)

En complemento con las herramientas de software para el análisis de evidencia digital extraída de dispositivos móviles o tecnologías convergentes de cómputo, los dispositivos de extracción forense tienen los accesorios y complementos necesarios para acceder a las memorias y sistemas operativos de estos dispositivos. Estas herramientas ayudan a saltar contraseñas o pines de las casas fabricantes y tiene el potencial de extraer y asegurar todo el contenido incluso el que está eliminado.

Dentro de los más populares están el UFED (Universal Forensic Extraction Device), Oxygen Forensic Extractor y MSAB Office XRY, entre otras.

Bioseguridad

Así como es indispensable el uso de herramientas de hardware y software para la recolección y buen manejo de la evidencia, también se requieren implementos de bioseguridad y protección para garantizar la integridad física y lógica de los elementos recolectados, dentro de estos elementos encontraremos:

Bolsas de Faraday

Ilustración 14: Bolsa de Farady (Fuente OnData)

Conocidas también como jaulas de Faraday, son elementos en forma de caja o bolsa que permiten bloquear cualquier tipo de señal electromagnética o de comunicación con los dispositivos que se encuentren en su interior. Son muy utilizadas para realizar análisis o para preservar equipos móviles o portátiles sin que se conecten con redes fijas o de celular, ya que si el equipo está conectado a una red puede existir alteración de la evidencia o incluso los datos importantes pueden ser borrados de forma remota.

Implementos antiestáticos

Ilustración 15: Bolsa y manilla antiestática (Fuente: Control estática)

Las bolsas, guantes, manillas y trajes antiestáticos son muy importantes al momento de manipular equipos electrónicos, con el fin de protegerlos de las cargas estáticas del ser humano y de algunos equipos establecidos en edificios o aeropuertos. Algunos manuales de cadena de custodia a nivel internacional exigen el uso de bolsas antiestáticas para almacenar los elementos digitales.

Evidencia digital

La evidencia digital se define como cualquier dato o información almacenada en forma de mensaje de datos (MD), para ello, entonces, debemos entender que desde 1996, con la publicación de la Ley Modelo sobre Comercio Electrónico aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, en su artículo 2, se indicó que por 'mensaje de datos' se entiende la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax. Mientras el 'intercambio electrónico de datos (EDI)' se entiende como la transmisión electrónica de información de una computadora a cuya estructura de información está conforme a alguna norma técnica convenida al efecto (Naciones Unidas, 1996).

Teniendo en cuenta estas definiciones y el sistema del comercio electrónico, a la luz de la legislación ecuatoriana, en la ley 2002-67 del Congreso Nacional fueron ratificadas las siguientes reglas:

1. Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterán al cumplimiento de lo establecido en esta Ley y su reglamento (Congreso Nacional, 2002, artículo 2).

2. Conservación de los mensajes de datos.- Toda información sometida a esta Ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:

    a. Que la información que contenga sea accesible para su posterior consulta;
    b. Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;
    c. Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado (Congreso Nacional, 2014); y,
    d. Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.

La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores (Congreso Nacional, 2014).

Características, principios y requisitos

La evidencia digital debe cumplir con unas características, principios y requisitos que han sido definidos a nivel internacional por estándares y normativas, esto hace que el manejo de la evidencia sea un desafío para los investigadores y analistas forenses.

Características técnicas

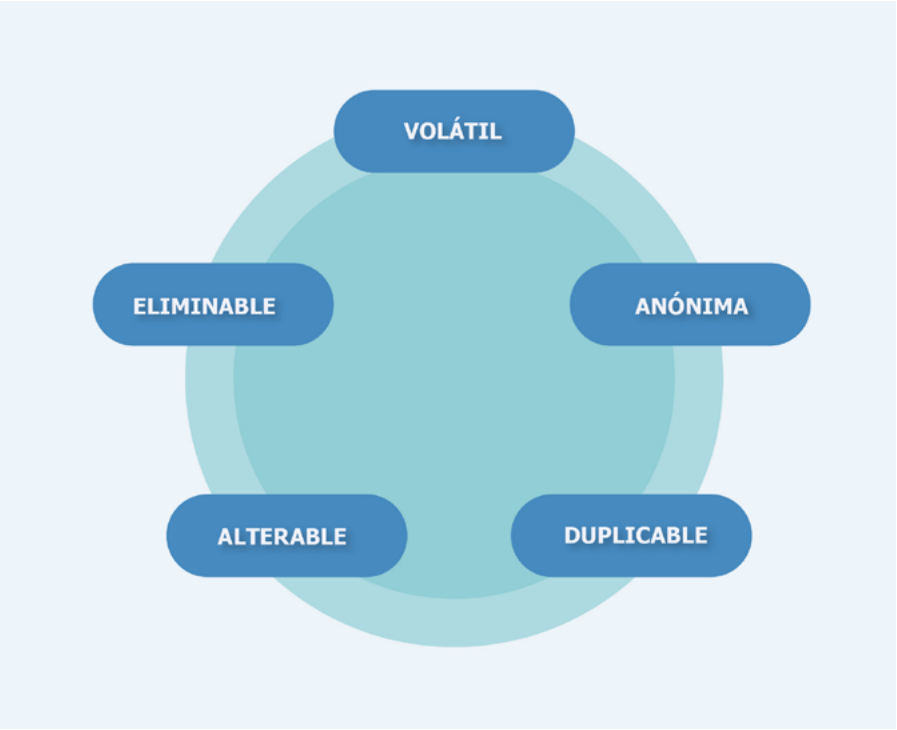


Ilustración 16: Características técnicas de la evidencia digital

Volátil

La gran cantidad de evidencia que se puede encontrar en la memoria RAM o en los archivos de paginación del sistema, así como en los registros de eventos, realmente es significativa para la mayoría de las investigaciones digitales, sin embargo, esta evidencia se pierde por completo cada vez que un dispositivo se apaga o pierde el flujo eléctrico. De esta evidencia se puede destacar los procesos, documentos, contraseñas, sitios web, programas en ejecución, entre otros.

Anónima

La evidencia digital generalmente es anónima, ya que, en muchas ocasiones, no se puede identificar plenamente la procedencia de un dato o información.

Duplicable

Otra de las características de la evidencia digital es que se la puede duplicar las veces que sean necesarias para no usar el elemento original, por este motivo se realizan las imágenes forenses para tener copias exactas y trabajar sobre ellas.

Alterable

La modificación de la evidencia digital puede ser voluntaria por un atacante o involuntaria por el usuario e, incluso, por el investigador digital forense, por lo cual es importante garantizar siempre la integridad de los elementos de estudio.

Eliminable

De acuerdo con las características anteriores, la evidencia digital puede ser eliminada fácilmente no solo por acción humana sino también por acción del ambiente o daños físicos, razón por la cual se debe conservar y custodiar en debida forma para evitar pérdidas, daños o manipulación no autorizada. copias exactas y trabajar sobre ellas.

Características legales

De acuerdo con lo establecido en el RFC 3227, las consideraciones legales que se deben tener en cuenta al momento de adquirir, almacenar y presentar evidencia digital son:

Admisible

Debe ajustarse a las normas legales vigentes en la jurisdicción de la investigación antes de que pueda llevarse ante un tribunal, así mismo se debe pensar en los marcos normativos internacionales ya que en la actualidad no solo se recolecta evidencia in situ, sino que también se lo hace en la nube.

Auténtica

Debe ser posible vincular positivamente las evidencias recolectadas al incidente investigado, para esto nos apoyamos en los procesos internacionales de cadena de custodia.

Completa

Debe contar toda la historia y no solo una perspectiva particular.

Confiable

No debe existir duda alguna acerca de cómo la evidencia fue recolectada y tratada.

Creíble

Debe ser creíble y comprensible para un tribunal.

Principios

La evidencia digital se rige por tres principios importantes: la pertinencia o relevancia, confiabilidad y suficiencia.

Pertinencia o relevancia

Debe ser posible demostrar que el material adquirido es relevante para la investigación, es decir, que contiene información de valor para ayudar al conocimiento del incidente particular y que hay una buena razón del porqué se ha adquirido.

Confiabilidad

Todos los procedimientos usados en el manejo de la potencial evidencia digital deben ser auditables y repetibles. Los resultados de la aplicación de tales procesos deben ser reproducibles por cualquier perito.

Suficiencia

Se debe tener en cuenta que se ha recopilado material suficiente para permitir que una investigación adecuada se lleve a cabo (ISO/IEC, 2012).

Requisitos

Hay cuatro aspectos importantes para tener en cuenta cuando se realizan los procedimientos de investigación digital forense de pruebas, estos son: la auditabilidad, justificación, repetibilidad y reproducibilidad, todas estas en función de las circunstancias particulares de cada caso.

Auditabilidad

Debe ser posible que un evaluador independiente o de otras partes interesadas puedan, gracias a la documentación realizada, verificar todas las acciones tomadas.

Repetibilidad

Se establece cuando los mismos resultados de la prueba se producen bajo las siguientes condiciones:

- Al usar el mismo procedimiento de medición y método.
- Al utilizar los mismos instrumentos y en las mismas condiciones.
- Al repetir en cualquier momento después de la prueba original.

Se debe tener en cuenta que puede haber circunstancias en las que no será posible repetir la prueba, por ejemplo, cuando un disco duro original ha sido copiado y devuelto en servicio, o cuando un elemento yace en la memoria volátil. En este caso, se debe verificar que el proceso de adquisición es fiable.

Reproducibilidad

Se establece cuando los mismos resultados de la prueba se producen bajo las siguientes condiciones:

- Al utilizar el mismo método de medición.
- Al usar diferentes instrumentos y en diferentes condiciones.
- Al repetir en cualquier momento después de la prueba original.

Justificabilidad

Se debe justificar todas las acciones y los métodos utilizados en el manejo de la potencial evidencia digital (ISO/IEC, 2012).

Fuentes de evidencia digital

A lo largo de las últimas décadas se han incrementado notablemente las fuentes de evidencia digital debido al nacimiento de nuevas tecnologías y a la hiperconvergencia, estas fuentes las podemos dividir en cuatro grupos principales:

Sistemas informáticos

Dentro de esta categoría encontraremos todos los sistemas informáticos compuestos por software y hardware tradicionales, como equipos de escritorio o personales (PC), portátiles, servidores, y los periféricos como impresoras, discos duros externos, dispositivos USB, memorias SD, consolas de videojuegos, impresoras, sistemas de video vigilancia (DVR, NVR, NDVR), entre otros.

Sistemas de comunicación

Los sistemas de información están interconectados a través de redes de comunicaciones, estas, a su vez, almacenan información relativa al tráfico, tipos de conexión, identificación de terminales, entre otros datos que son importantes para las investigaciones, sobre todo cuando se tiene conocimiento del uso de redes para actividades ilícitas; en esta categoría encontramos cualquier dispositivo que sirva para la comunicación digital y telecomunicaciones, incluyendo enrutador, conmutador, puntos de acceso, módems, etc.

Sistemas convergentes de computación y dispositivos móviles

La convergencia ha logrado centralizar tecnologías y ha permitido una sinergia de trabajo en un solo dispositivo, gracias a su gran capacidad de procesamiento, uso y almacenamiento. Este recurso es importante para las investigaciones digitales forenses. Entre los elementos más usados que encontramos en esta categoría son los teléfonos inteligentes o smartphone, las tabletas digitales o tablets, los PDA, los drones y lo que actualmente conocemos como el IoT (internet de las cosas).

Sistemas basados en la nube (cloud)

Uno de los grandes retos de la actualidad para las agencias de ley es la hiperconvergencia tecnológica y la migración de los sistemas a la nube, ya que los proveedores están distribuidos por todo el mundo, lo que dificulta el acceso físico a los equipos. Es por esto que los servicios basados en la nube como el SaaS (software como servicio), PaaS (plataformas como servicio) y IaaS (infraestructura como servicio) han obligado a generar nuevas herramientas y procedimientos para garantizar la integridad, confiabilidad y disponibilidad de las evidencias.

Dentro de este grupo de sistemas en la nube encontramos sitios web, redes sociales, correos electrónicos, plataformas de almacenamiento de datos, aplicaciones web empresariales, entre otras.

Imagen forense

Si se tiene en cuenta la naturaleza propia de la evidencia digital, para almacenarla correctamente en un contenedor (DVD, memoria USB, disco duro, etc.) se debe generar un archivo digital que garantice y satisfaga los requisitos técnicos y legales. Este procedimiento se realiza mediante la creación de la imagen forense, que no es más que una copia exacta de la información existente en el equipo.
Cabe resaltar que hay varios tipos de información forense y varios formatos.

En primer lugar, para la toma correcta de la imagen forense se recomienda que el software utilizado cuente con las siguientes características:

- Realice imágenes forenses de múltiples dispositivos.
- Realice imágenes forenses en múltiples destinos al mismo tiempo.
- Reconozca áreas ocultas.
- Fraccione archivos.
- Verifique el hash con algoritmos estándar.
- Verifique el hash en diferentes etapas del proceso de creación de imágenes forenses.
- Admita los formatos más comunes para la realización de imágenes forenses.
- Cree imágenes forenses encriptadas.
- Cree imágenes forenses comprimidas.
- Reanude un proceso de creación de una imagen forense interrumpida.
- Tolere errores de hardware.

Respecto a los formatos de archivo, existen varios formatos, como el raw, dd o ad, estos formatos almacenan todos los datos del medio original en un archivo crudo o bruto (sin esquema, sin formato). Los archivos crudos o en bruto son los más recomendados ya que al ser universales permiten la lectura en la mayoría de las herramientas de análisis y procesamiento.

Otros formatos como el de testigo experto (EWF) y el forense avanzado (AFF) incluyen otras características adicionales, pero son patentados por algunas casas matrices.

En cuanto a la imagen forense, existen dos tipos: la imagen física y la imagen lógica. La imagen física incluye todos los datos en bruto (bit a bit). La recolección de datos físicos a nivel del disco completo es una copia de todos los datos, incluido el esquema de particiones, el área particionada, el área no particionada y el espacio no asignado.

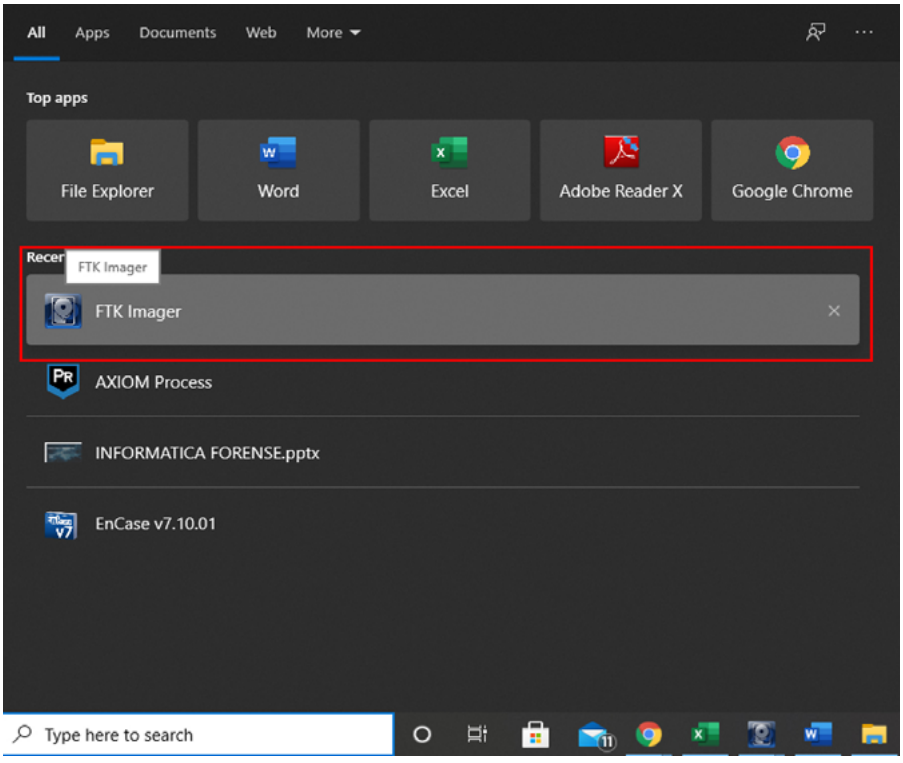
En la imagen lógica o personalizada se incluye únicamente un subconjunto asignado de datos. La recolección de datos lógicos a nivel de disco es una copia solamente de un área lógica particionada (sistema de archivos, partición, carpetas o archivos individuales).

¿Cómo realizar una imagen forense a un dispositivo?

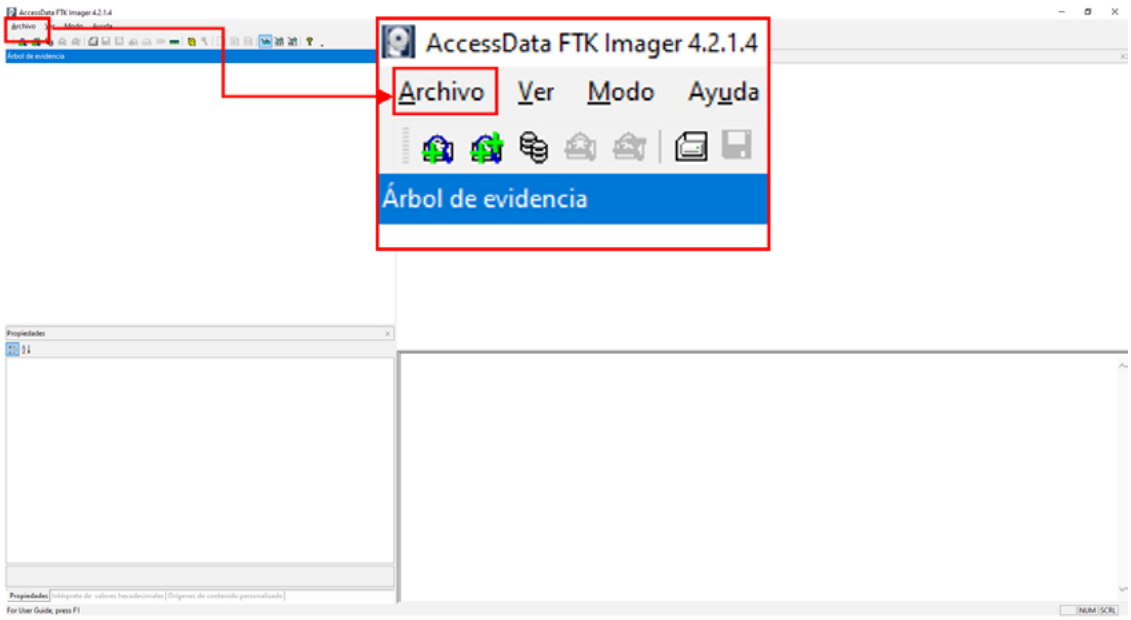
A continuación, se describe el paso a paso para adquirir una imagen forense a través de un ejemplo real que servirán como guía para el uso de la herramienta. La herramienta utilizada fue FTK Imager, la cual es una herramienta gratuita y con plena validez a nivel internacional usada por diversas agencias de ley y empresas de seguridad de la información.

Creación de imagen forense

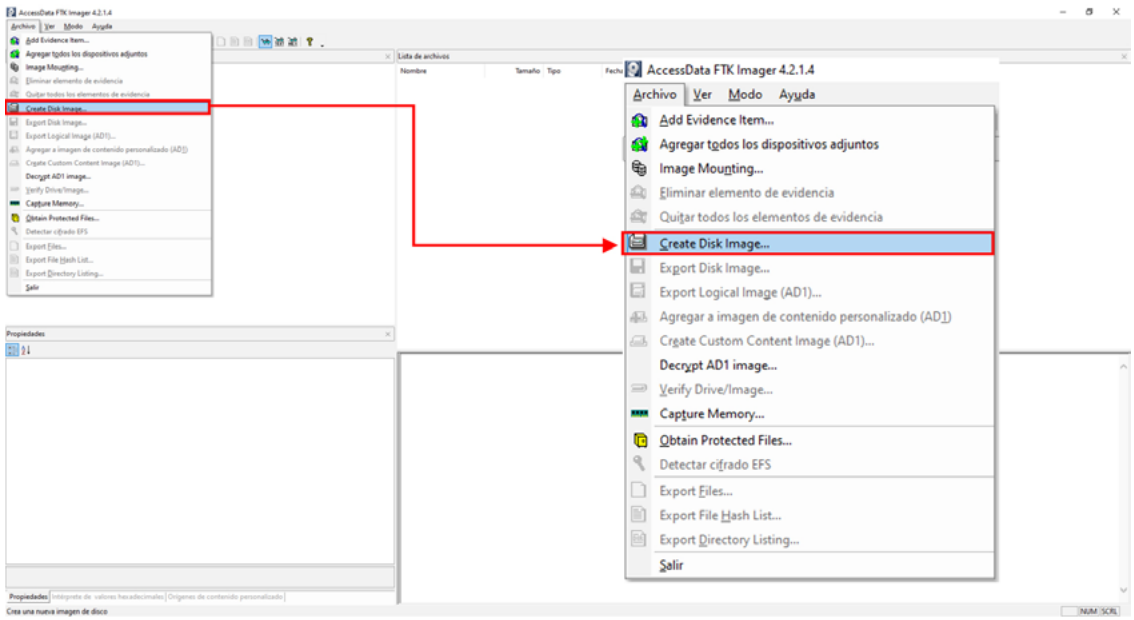
1. Se ejecuta la herramienta forense FTK Imager



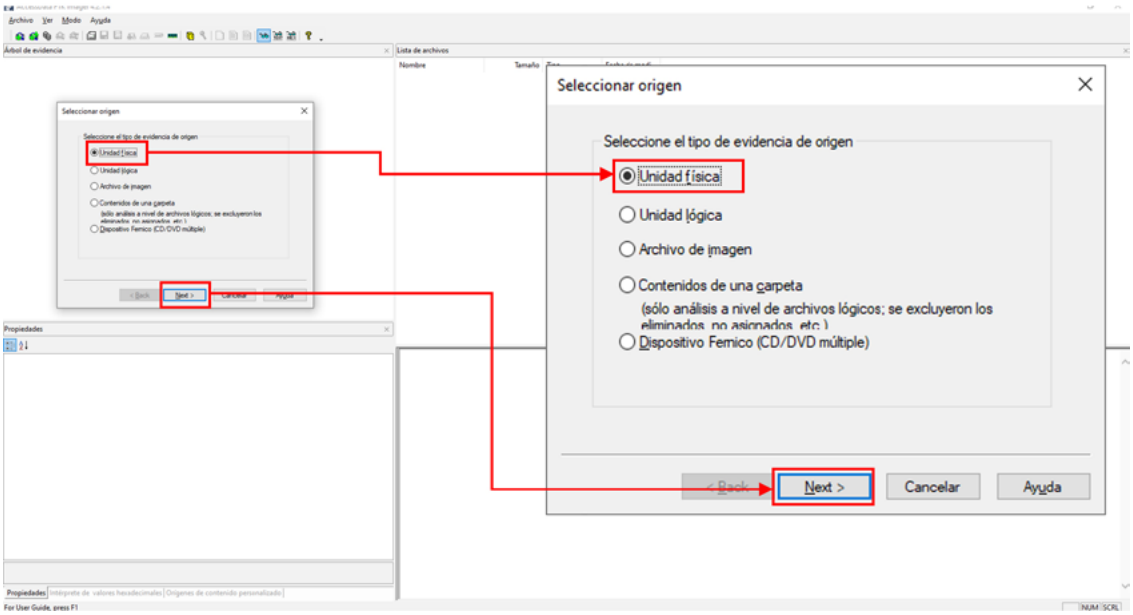
2. Cuando carga la herramienta FTK, nos ubicamos en la pestaña Achivo.



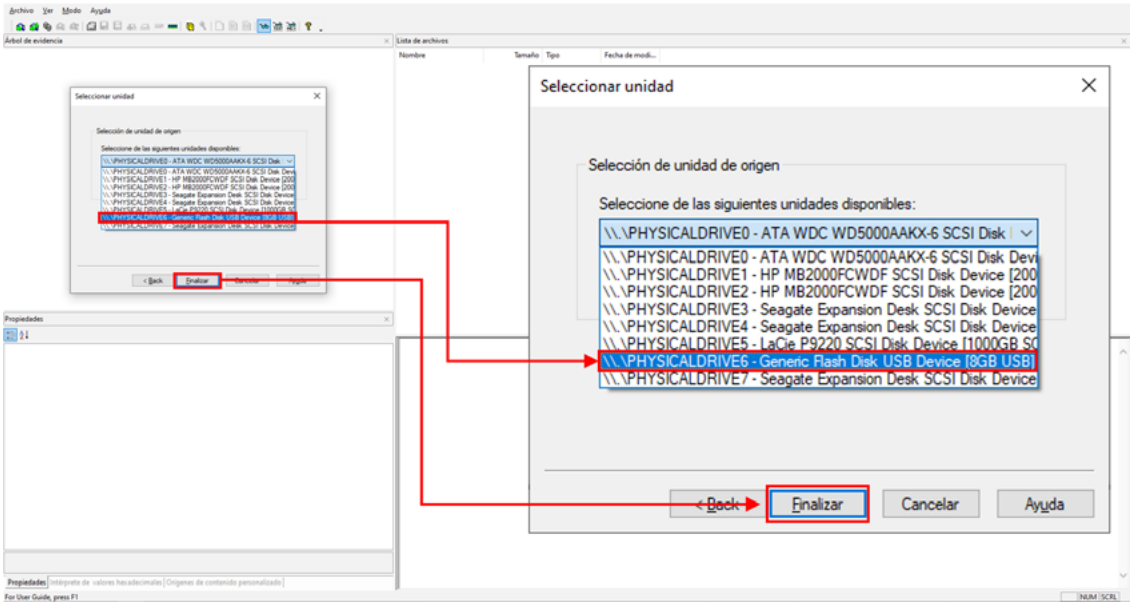
3. En esta pestaña se hace clic en la opción Create Disk Image (crear imagen de disco).



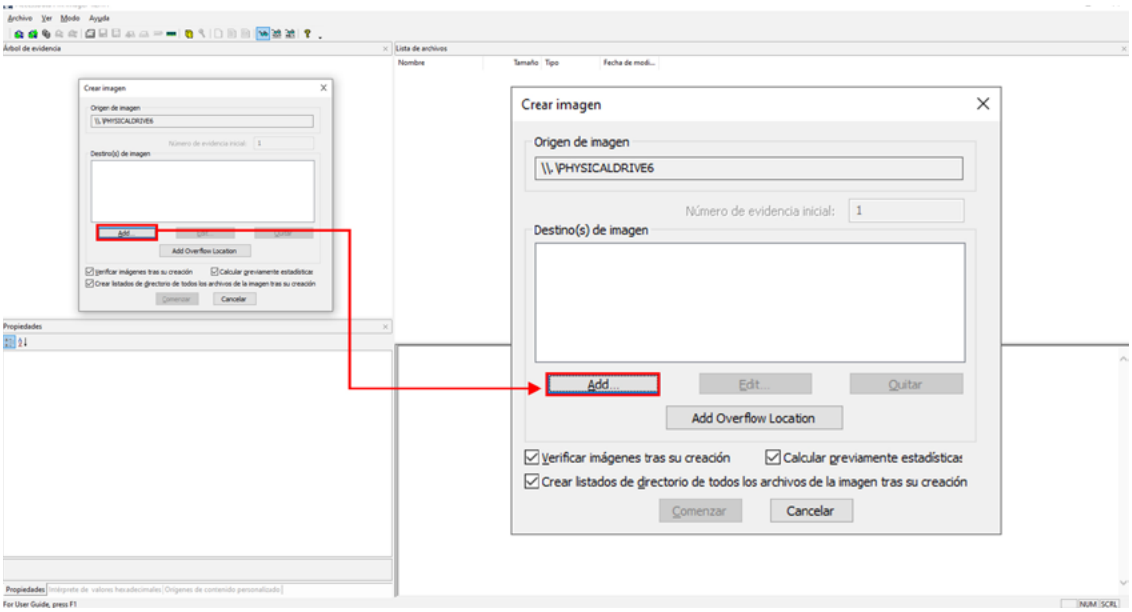
4. A continuación, se abre una ventana donde se debe seleccionar el tipo de evidencia de origen, para este ejercicio se realiza una imagen forense a la unidad física.



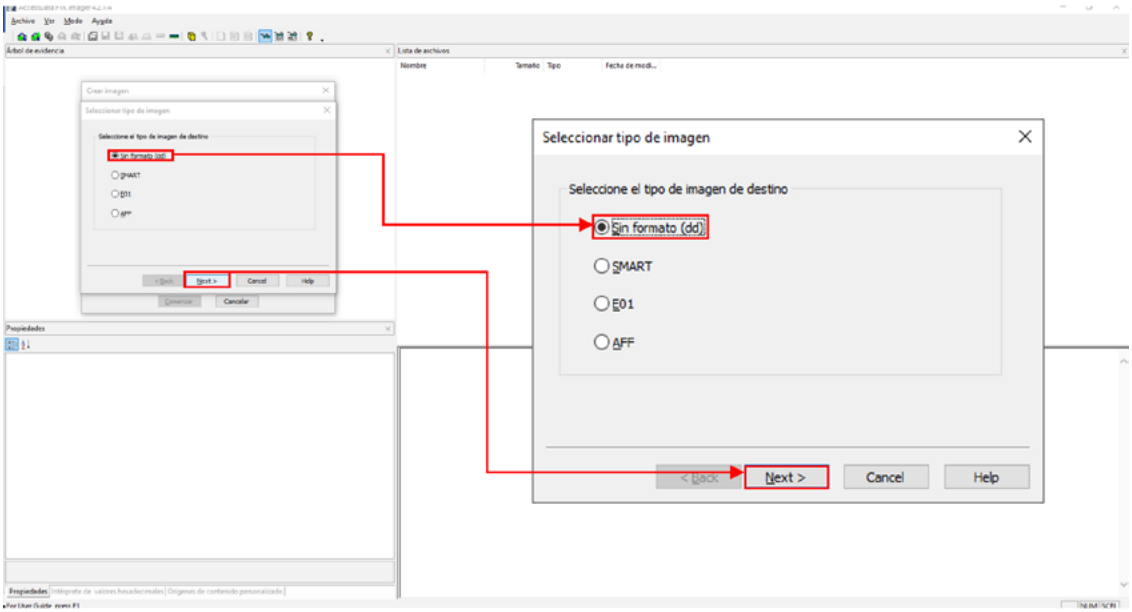
5. Luego, se abrirá una nueva ventana donde se muestra el menú de las unidades disponibles que se encuentran conectadas en el equipo de cómputo, se debe tener en cuenta la unidad a la que se le realizará la imagen forense y luego se hace clic en el botón de finalizar.



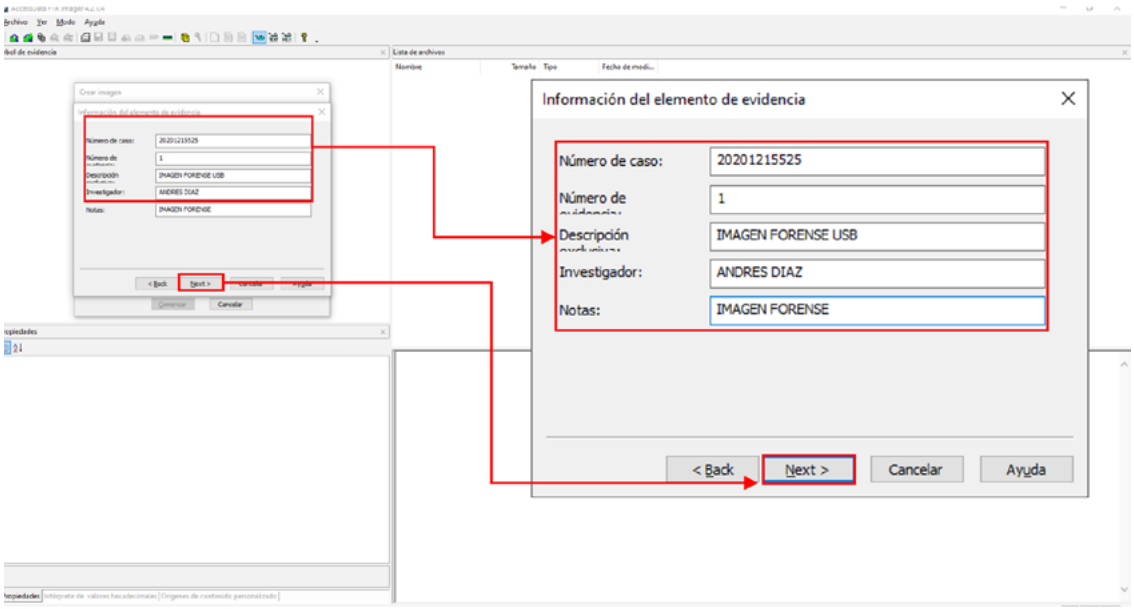
6. En este punto, la herramienta abre una ventana donde se definirá el destino para almacenar la imagen forense, luego clic en el botón Add.



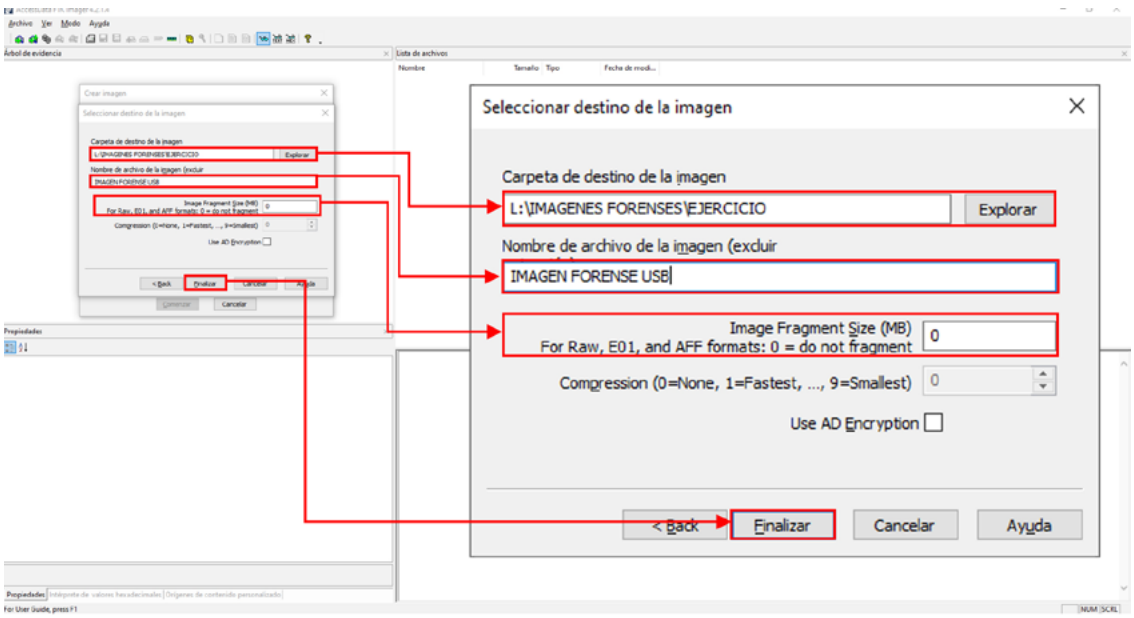
7. En la siguiente ventana se define el tipo de la imagen a crear, para este ejercicio se usó la opción dd, luegodamos clic en Next.



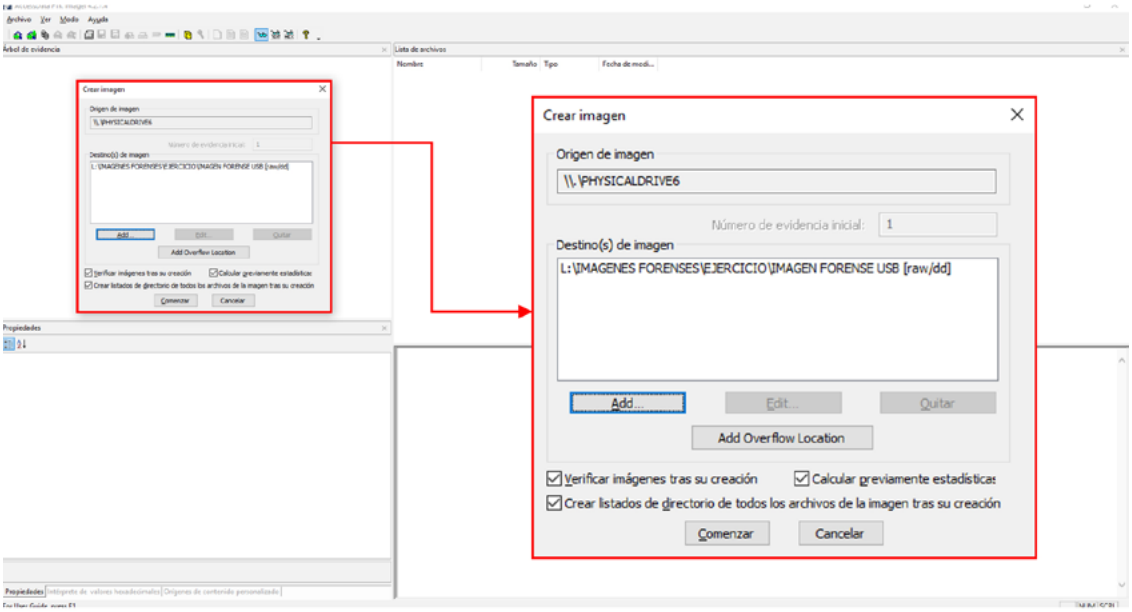
8. A continuación, se ingresa la información sobre los ítems de evidencia, cuando se complete esta información hacemos clic en Next.



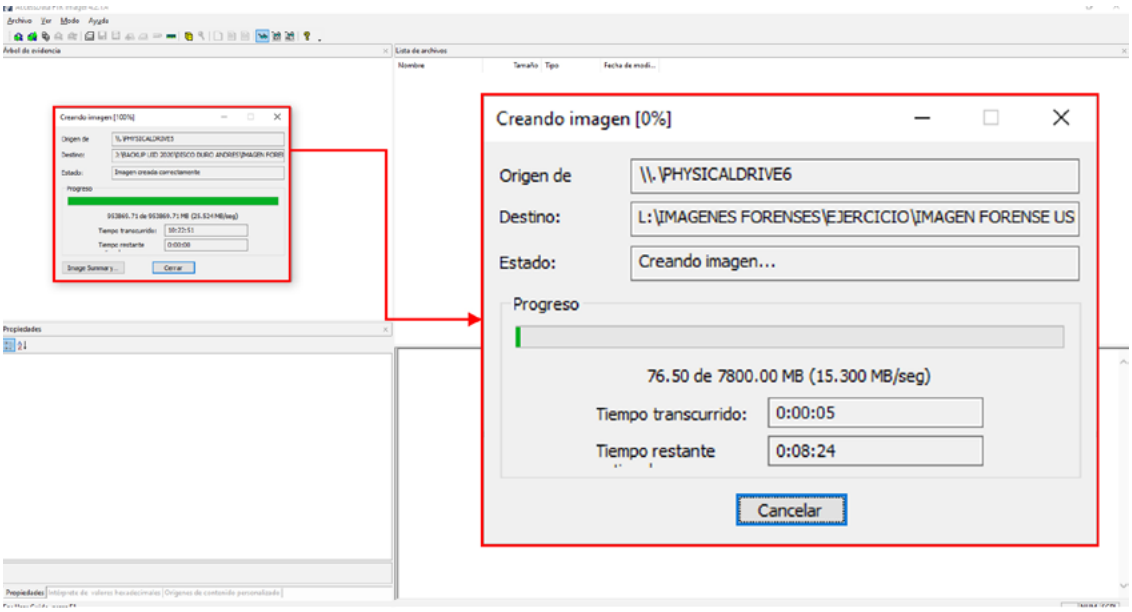
9. En seguida, se define la carpeta donde se almacenará la imagen forense, opcionalmente se define si la imagen será dividida en varias partes o no. Para este ejercicio no será dividida, por lo tanto, se define el valor 0 en el campo Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment.



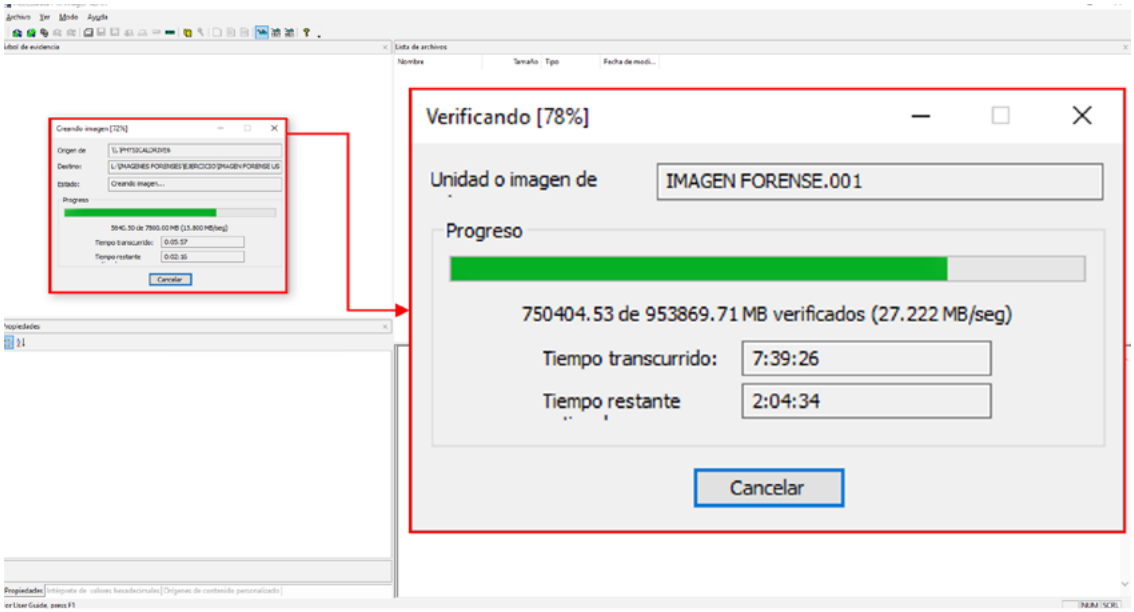
10. Al hacer clic en el botón Finalizar se mostrará un resumen de las opciones seleccionadas.



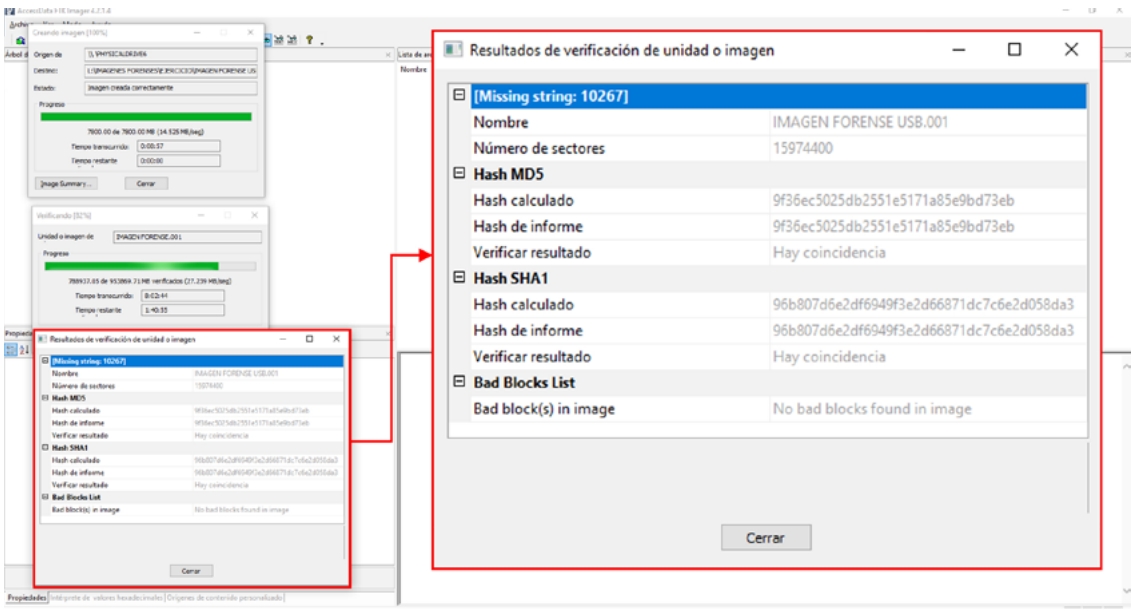
11. Una vez revisadas las opciones se hace clic en Comenzar y se iniciará la creación de la imagen forense.



12. Al terminar la creación de la imagen forense, inicia la verificación de la imagen creada.



13. Al final, se presentan algunos resultados que muestran el número de sectores copiados. La generación de un hash MD5 y un hash SHA-1, muestra la coincidencia entre el campo Hash Calculado, es decir el hash obtenido desde la unidad USB o Memory Stick, y el campo Report Hash (Hash Reportado), que se genera desde la imagen forense creada de nombre IMAGEN FORENSE USB.001.



Nota: En el mismo directorio o unidad donde se ha creado la imagen forense, se encuentra un archivo de texto con el mismo nombre de la imagen forense creada (IMAGEN FORENSE USB.txt), en el cual se encuentra toda la información detallada del proceso realizado.

Esterilización de medios (wipping)

Es importante que los contenedores donde se van a almacenar las evidencias digitales se encuentren esterilizados, es decir, que no tengan ningún tipo de archivo almacenado previamente. En los discos ópticos (CD, DVD, BluRay, etc.) no se tendrá inconveniente si están en blanco, sin embargo, en algunas ocasiones cuando los investigadores usan dispositivos de almacenamiento como memorias USB o disco duros, por lo que es importante verificar que no exista ningún elemento, ni siquiera borrados previamente, ya que al realizar el procedimiento de análisis es posible que el sistema analice los archivos que no sean parte de la evidencia recolectada.

Para realizar este proceso, el NIST realizó la publicación especial 800-88, que establece una serie de criterios para la eliminación o destrucción segura de datos, se pueden utilizar herramientas gratuitas como Eraser, disponible en el siguiente enlace: https://eraser.heidi.ie/download/

Hash

El algoritmo hash o suma de verificación es una función matemática que realiza el cálculo de cualquier archivo digital y se utiliza para demostrar la integridad de este, ya que, al cambiar cualquier carácter, pixel o bit de un archivo, el algoritmo tiene una variación.

Existen diversas sumas de verificación hash como las funciones MD5, SHA-1, SHA-256, etc. En su mayoría, las herramientas de creación de imagen forense generan un listado hash de toda la evidencia.

Investigación digital forense

La investigación en el lugar de los hechos siempre ha sido el eje central de las investigaciones criminales en las que se hace necesario proteger, fijar, recolectar y embalar todos los medios de prueba; a nivel informático esto no queda atrás. Esta guía pretende que el funcionario judicial, sin necesidad de tener conocimientos avanzados en informática forense, pueda ser el primer responsable de una escena que contenga evidencia digital y recolecte evidencias válidas con capacidad demostrativa dentro de un proceso judicial.

La mayor cantidad de procedimientos investigativos involucran, por lo menos, una fuente de evidencia digital, por ejemplo un accidente de tránsito, un homicidio o un hurto, que se soportan inicialmente en los videos de seguridad encontrados en las vías públicas. Los videos son evidencia digital y deben ser tratados de acuerdo con las disposiciones técnicas y legales. De igual forma, en un procedimiento de captura o detención por cualquier delito en el que se incauta o aprehende un equipo celular, se debe seguir lo estipulado por las Buenas Prácticas para el Manejo de la Información Digital.

Gestión de escenas

Para realizar una efectiva gestión dentro de una escena donde exista evidencia digital, se deben seguir las siguientes fases para cumplir los estándares y las buenas prácticas internacionales:

1. Fase de recolección
2. Fase de tratamiento
3. Fase de análisis
4. Fase de presentación

Nota: Cada caso es único; sin embargo, es importante mantener una metodología clara y documentada para evitar errores, daños o pérdidas de evidencia. Recuerde que usted podría verse inmerso en un delito o una investigación si comete una equivocación.

Fase de recolección

Preparación y medidas previas

Para recolectar la evidencia digital debemos seguir las reglas de la criminalística y la inspección a lugar de los hechos. En esta medida se debe realizar una preparación previa para verificar que se cuenten con los elementos necesarios para desarrollarla.
Se sugiere al perito o investigador tener una lista de chequeo de los implementos necesarios, expuestos a continuación:

a. Guantes de látex o antiestáticos
b. Traje o bata de bioseguridad antiestática
c. Manilla antiestática
d. Bolsas antiestáticas o papel aluminio
e. Bolsas de Faraday
f. Kit de destornilladores y herramientas
g. Extensión de energía
h. Cámara fotográfica y/o grabadora de video
i. Bolsas de evidencia
j. Cinta de evidencia
k. Marcadores permanentes
l. Rótulos de cadena de custodia

Una vez se encuentre en el lugar de los hechos se debe identificar y verificar si existe o no la necesidad de realizar un aislamiento o acordonamiento de la escena, evaluando los posibles riesgos y adaptando las medidas de seguridad necesarias. De igual forma recuerde conservar el espacio para evitar cualquier contaminación, alteración, manipulación o pérdida de la potencial evidencia.

Identificación de la evidencia digital

Antes de tener un contacto directo con un equipo o dispositivo, es importante verificar su estado y el entorno en el que se encuentra. Por eso, se recomienda documentar el estado de conservación, funcionamiento e identificación del equipo, para lo cual se realiza una fijación fotográfica o video gráfica mediante tomas panorámicas, generales y de detalle. Así mismo, hay que documentar por escrito la siguiente información:

- Tipo de dispositivo, marca, modelo, serial, color, estado físico y dispositivos periféricos conectados. En caso de ser una unidad de almacenamiento, identificar externamente, si es posible, la capacidad, velocidad, interfaz de conexión (IDE, Sata, SAS, etc.), entre otros datos que permitan la identificación única al dispositivo.

Equipos de cómputo

¿Qué hacer si el dispositivo de cómputo se encuentra encendido?

1. Fije fotográficamente la pantalla (teniendo especial cuidado en identificar la hora y fecha del sistema y, si hay variación con la hora oficial, también debe documentarla).
2. Verifique si el equipo está protegido con contraseña.
   a. En caso de estar protegido y no cuenta con la contraseña, quite la corriente del dispositivo.
   b. En caso de no estar protegido con contraseña, realizar la recolección de elementos volátiles (recolección en vivo), para obtener lo siguiente:
      i. Datos de la memoria caché.
      ii. Datos de la memoria RAM a través de imagen.
      iii. Datos de los archivos de intercambio (sistemas de archivos temporales, espacio de intercambio SWAP, hiberfil.sys, pagefile.sys).
      iv. iv. Datos de los procesos de red (tabla de enrutamiento, caché ARP).

   v. Datos de los procesos del sistema (lista de procesos, estadísticas del kernel)
3. Una vez obtenida toda la información volátil se debe verificar si el equipo cuenta con algún tipo de cifrado en el disco o mediante el sistema operativo.
   a. En caso de tener algún tipo de cifrado se debe realizar una imagen forense en vivo de tipo lógico.
4. Para dispositivos electrónicos en los que sea posible, desconecte el cable de alimentación, retire la batería.
5. Desconecte todos los cables, dispositivos externos y periféricos de entrada y salida y etiquételos.
6. Proteger los puertos USB, lectores de disco óptico, lectores de memoria, y otros puertos de entrada y salida con cintas de seguridad.
7. Recolecte los dispositivos susceptibles de aprehensión, incautación o aseguramiento, siguiendo las reglas de la cadena de custodia.
8. Tener en cuenta recolectar la documentación, anotaciones, entre otros, que se encuentren en la escena (evidencia no digital).
9. Documentar el proceso con el mayor nivel de detalle.

¿Qué hacer si el dispositivo de cómputo se encuentra apagado?

1. No lo encienda.
2. Desconecte todos los cables, dispositivos externos y periféricos de entrada y salida y etiquételos.
3. Proteger los puertos USB, lectores de disco óptico, lectores de memoria, y otros puertos de entrada y salida con cintas de seguridad.
4. Recolecte los dispositivos susceptibles de aprehensión, incautación o aseguramiento, siguiendo las reglas de la cadena de custodia.
5. Si no es posible aprehender o incautar el equipo, proceda a extraer los dispositivos de almacenamiento en el sitio para hacer el proceso de adquisición forense (recolección post mortem).
6. Tener en cuenta recolectar la documentación, anotaciones, entre otros, que se encuentren en la escena (evidencia no digital).
7. Documentar el proceso con el mayor nivel de detalle.

Nota: Para tener que sea tenida en cuenta, toda evidencia digital debe estar almacenada en una imagen forense.

Equipos móviles o tabletas

Debido al tipo de tecnología de cómputo convergente, la extracción de evidencia digital de los dispositivos móviles funciona diferente a la de un equipo de cómputo convencional, por esto, es importante que el perito conozca las necesidades del caso para determinar los tipos de datos requeridos del dispositivo móvil y de esta forma identificar el método más adecuado para recolectar la evidencia.

Antes de iniciar el trabajo, se recomienda reunir, en lo posible, todos los códigos de acceso, contraseñas o patrones de seguridad del dispositivo móvil, ya que la mayoría de los métodos de recolección requieren que los dispositivos móviles se encuentren desbloqueados. Por lo tanto, siempre es una buena práctica intentar obtener los códigos de desbloqueo en el momento de la incautación o cuando el dispositivo haya llegado al laboratorio.

Según la Interpol (2019), los cinco diferentes tipos de recolección de datos para dispositivos móviles son los siguientes:

Extracción física

Es la recolección de datos binarios sin procesar del medio de almacenamiento del dispositivo electrónico. Estos datos en bruto posteriormente deben ser analizados y procesados en fases siguientes por el *software* forense. Esta extracción es la más recomendada ya que se puede llegar a obtener elementos eliminados del dispositivo, así mismo, las bases de datos de las aplicaciones.

Extracción lógica

La extracción lógica obtiene la información disponible del dispositivo móvil, es decir, que solo se puede acceder a lo visible en el dispositivo, generalmente no recupera información eliminada y en muchas ocasiones no se puede acceder a las bases de datos de algunas aplicaciones; es muy útil cuando solo se requiere asegurar algunas imágenes, documentos, audios o videos.

Volcado del sistema de archivos

El volcado del sistema de archivos (FSD) es una extracción híbrida entre una extracción lógica y una física. El FSD recupera los archivos del sistema del dispositivo electrónico e interpreta los datos durante la etapa de procesamiento. Esto permite que el perito recupere, por ejemplo, bases de datos que contienen mensajes eliminados que pueden no estar disponibles en una extracción lógica y pueden no estar accesibles durante una extracción física. Sin embargo, este tipo de extracción no recupera todos los datos eliminados de la manera en que lo hace una extracción física.

Extracción manual

Debido al incremento de las casas matrices dedicadas a la venta de equipos móviles, la actualización constante de los sistemas operativos, hacen que las herramientas forenses no sean compatibles con todos los dispositivos móviles existentes. Para los casos en los que no exista compatibilidad del dispositivo móvil, es aceptable que el perito use el método manual de extracción de datos, en el que se accede al dispositivo y se guardan los datos mostrados en la pantalla del móvil, mediante fotografías, videos o realizando la transcripción de los datos. En otros casos se puede considerar el uso de herramientas de *software* o realizar capturas de pantalla, este método puede requerir que el teléfono esté conectado a través de los comandos ADB, con el modo desarrollador habilitado.

JTAG / Chip-Off / Rooting / Jail Breaking

En el caso de los dispositivos móviles que se encuentren dañados o bloqueados por una contraseña, se pueden utilizar los métodos JTAG y Chip-Off para extraer los datos. La extracción por medio de JTAG requiere quitar del dispositivo su placa lógica, y soldar el cable a una determinada conexión en la placa, esto requiere de una gran habilidad técnica. Con este método, el perito debería poder recuperar los datos binarios sin procesar del medio de almacenamiento del dispositivo móvil.

Chip-Off permite extraer los datos binarios sin procesar del medio de almacenamiento del dispositivo móvil, al igual que el método JTAG, pero en este caso se debe remover permanentemente el chip de memoria de la placa de memoria del dispositivo. Cuando el perito utiliza el método Chip-Off, el dispositivo se dañará y ya no podrá usarse. El uso de este método debe ser moderado y debe ser la última opción, además hay que tener en cuenta que los dispositivos móviles recientes almacenan datos cifrados en su chip de memoria y en otros casos encriptan la información de manera predeterminada. La técnica Chip-Off también se puede aplicar para los dispositivos utilizados en IoT (Internet of things), los cuales, generalmente, almacenan datos en texto claro.

Rooting o también llamado Jail Breaking es un método menos destructivo, pero no tan útil, ya que implica aprovechar las características del sistema operativo para elevar los permisos y privilegios del usuario en ejecución (obtener acceso como *root*). Sin embargo, este método no se considera una técnica forense, ya que implica la modificación de los archivos del sistema y puede dañar el dispositivo, por lo tanto, se debería usar cuando no exista otra forma de extraer datos.

Nota: Los métodos mencionados anteriormente se deben usar en el orden nombrado, los peritos deben esforzarse por utilizar el método de extracción que sean menos invasivo y destructivo, pero que produzca la mayor extracción de datos, ya que solo así se podrá recuperar, almacenar o capturar áreas que podrían dañarse o sobrescribirse en etapas posteriores. Los métodos de extracción JTAG y Chip-Off solo se deben considerar como último recurso, especialmente Chip-Off, ya que el proceso puede ser destructivo e irrecuperable (INTERPOL, 2019).

¿Qué debo hacer si tengo un dispositivo móvil como evidencia?

1. Identifique la evidencia electrónica y su respectivo medio de almacenamiento

Es importante observar e identificar el tipo de dispositivo móvil. Generalmente los equipos móviles tienen una etiqueta pegada en el interior del dispositivo o impresa en la parte posterior en donde se puede establecer la identidad internacional del equipo móvil (IMEI), el número de serie, marca y modelo, en caso de ser impreso, corroborar la información, ya que puede ser una etiqueta falsa.

Una vez recuperados estos datos, se consideran claves para enviar la solicitud de registros de facturación o para analizar celdas de celulares en las etapas posteriores de la investigación. El IMEI, MEID, marca y modelo también se pueden utilizar para determinar el nivel de soporte de la herramienta forense.

Cabe resaltar la importancia de identificar si el dispositivo cuenta con una memoria extraíble y una tarjeta SIM.

2. Aislar el dispositivo móvil de la red

Para realizar la extracción de datos de un dispositivo móvil, generalmente se requiere que el dispositivo esté encendido. Sin embargo, se debe evitar cualquier intento de conexión a red, ya que eso potencia el riesgo de generar cambios en los datos, o de sufrir un posible borrado remoto de la información.

Dependiendo del presupuesto, el aislamiento se puede lograr a través de diferentes formas, tales como:

- Clonación de la tarjeta SIM / IDEN. Una tarjeta SIM / IDEN es usada en los dispositivos para identificar al suscriptor y conectarse a la red. Una tarjeta SIM / IDEN clonada se parece y en general tiene las mismas características de la tarjeta original, pero carece de la capacidad de conectarse a la red móvil. Los teléfonos móviles más actuales pueden tener función de eSim que es virtual y no física.

- Sala o cuarto blindado de red. Es un laboratorio instalado con blindaje Faraday para evitar que ingresen las señales electromagnéticas. Sin embargo, esta es una solución muy costosa, por lo que se recomienda usar cámaras, cajas o bolsas de Faraday más pequeñas, que pueden ser consideradas como una alternativa efectiva.

- Equipo bloqueador de frecuencias. Este equipo bloquea las señales de red entrantes, sin embargo, en algunas jurisdicciones es ilegal su uso, por lo que, antes de adquirir este dispositivo, se debe verificar su legalidad en las normativas de cada país.

- Método manual. Este es el método de configuración más económico y sencillo de utilizar, sin embargo, necesita que el perito acceda al dispositivo móvil, esto implica un riesgo ya que se pueden modificar algunos datos. El perito debe configurar el dispositivo móvil en "Modo Avión" para deshabilitarlo de cualquier tipo de red, esto es un requisito para el funcionamiento de algunas herramientas forenses.

3. Extraer datos relevantes

En la mayoría de las técnicas de extracción de evidencia de equipos móviles, es complejo usar un bloqueo contra escritura, ya que se requiere ajustar configuraciones o habilitar permisos, por eso es importante que el investigador digital forense esté consciente de las consecuencias de sus acciones al manipular los dispositivos móviles y además pueda justificar y explicar las acciones realizadas, que deben estar totalmente documentadas.

Los dispositivos móviles pueden contener tres medios distintos de almacenamiento de datos separados, que requieren técnicas de extracción o aseguramiento distintas. Los medios de almacenamiento, según la Interpol (2019) son:

- Tarjeta SIM / IDEN. La tarjeta SIM requiere de herramientas forenses para dispositivos móviles. El método para extraer los datos de la SIM es por medio de la extracción lógica, debido a que la extracción física no es compatible. Para realizar la extracción

de datos es preferible que la tarjeta SIM se retire del dispositivo móvil durante el proceso.

- Tarjetas de memoria externa. Estas tarjetas de memoria tienen la ventaja de que pueden ser examinadas como un disco duro de una computadora. Mientras las herramientas forenses lo permitan, se pueden realizar extracciones tanto lógicas como físicas. Para extraer los datos, el perito debe remover la tarjeta temporalmente, luego debe volver a colocarla en el dispositivo móvil antes de encenderlo. Algunos dispositivos móviles almacenan datos en la tarjeta de memoria, y si el equipo detecta que la tarjeta no está disponible puede causar la pérdida de datos importantes del dispositivo móvil.
  Si el tiempo y los recursos lo permiten, se debería crear un clon bit a bit de la tarjeta de memoria e insertar la tarjeta clon en el dispositivo móvil.

- Memoria Interna. Esta memoria requiere de herramientas forenses para los dispositivos móviles, algunos equipos son compatibles con las herramientas forenses para una extracción física del *boot loader*, que se puede realizar a menudo sin la tarjeta SIM dentro del dispositivo móvil.
  Las herramientas forenses iniciarán el dispositivo móvil de una manera particular y realizará una extracción física, sin generar ningún cambio o alteración de los datos del usuario en el dispositivo. Este método puede recuperar potencialmente los códigos de bloqueo del dispositivo, lo que será de gran ayuda para el perito, ya que contará con acceso completo al dispositivo móvil una vez lo encienda (INTERPOL, 2019).

El proceso para extraer datos relevantes cambiará dependiendo del método de extracción elegido. La mayoría de las herramientas forenses brindan una guía que explica el procedimiento que se debe seguir para realizar una extracción de datos exitosa. En algunos casos, realizar el tratamiento y posterior análisis del dispositivo móvil requiere modificar los archivos del sistema o el sistema operativo para extraer los datos. En otros casos, es necesario cargar o instalar aplicaciones en el dispositivo móvil, práctica que se debe evitar en lo posible, ya que este proceso puede hacer que algunos datos se pierdan definitivamente, sin embargo, esto solo afectaría a los archivos del sistema con poco valor probatorio. El conocimiento de lo que se modifica al realizar cualquiera de estos procedimientos puede aprenderse a través de certificaciones y

cursos adecuados, como las capacitaciones que brindan los fabricantes de *software* forense móvil o la experiencia práctica que implica realizar los datos de dispositivos móviles.

Otra fuente importante de evidencia forense es el archivo de respaldo del dispositivo móvil. Algunos usuarios y dispositivos crean copias de seguridad en otros dispositivos, como en la computadora o en la nube. Estas copias de seguridad pueden ayudar a construir una línea de tiempo de la evidencia y también se pueden utilizar para lograr el acceso a un dispositivo con contraseña bloqueada. De esta forma es posible analizar algunas copias de seguridad como si fuera un dispositivo físico.

4. Verificar la evidencia y los datos extraídos

Una vez finalizado el proceso de extracción de los datos, se recomienda verificar si la información que el investigador obtuvo está completa, de igual forma deberá establecer si la información, como la fecha y hora, se encuentran alineadas con la zona horaria de su país. En caso de necesitar más información se puede intentar otro tipo de extracción.

5. Documentar todas las acciones realizadas.

Aunque se menciona en último lugar, en realidad es transversal a los anteriores, ya que es muy importante documentar todo lo hecho, las herramientas, técnicas e instrumentos utilizados, así como la información de los investigadores e intervinientes. El proceso se debe documentar de forma escrita.

Evidencia digital en la nube (páginas web y redes sociales)

Uno de los grandes retos de los investigadores forenses en la actualidad es la computación forense en la nube (*cloud forensic*). Debido a la hiperconvergencia de tecnología en la red, recolectar datos que se encuentran almacenados en servidores remotos, como páginas web, servidores de correos, redes sociales, plataformas de almacenamiento en la nube y otros servicios, son requisitos diarios dentro de las investigaciones digitales.

Como se explicó anteriormente, existen herramientas dedicadas a automatizar los procesos para recolectar esta evidencia en particular; sin embargo, estas herramientas generalmente tienen un alto costo y, por lo tanto, no todas las unidades o personal podrán obtenerlo. Es por esto que se propone el manejo de metodologías básicas para recolectar información en páginas web y redes sociales y así garantizar los requisitos técnicos y legales expuestos anteriormente.

¿Qué hacer si debo recolectar información pública en una página web?

Para realizar un aseguramiento de página web se requiere un navegador web, en este caso se sugiere Google Chrome, ya que además de ser una herramienta gratuita, permite el uso de extensiones útiles para la actividad, como: SingleFile y Save Page WE.

A continuación, se muestra cómo recolectar la información pública en una página web:

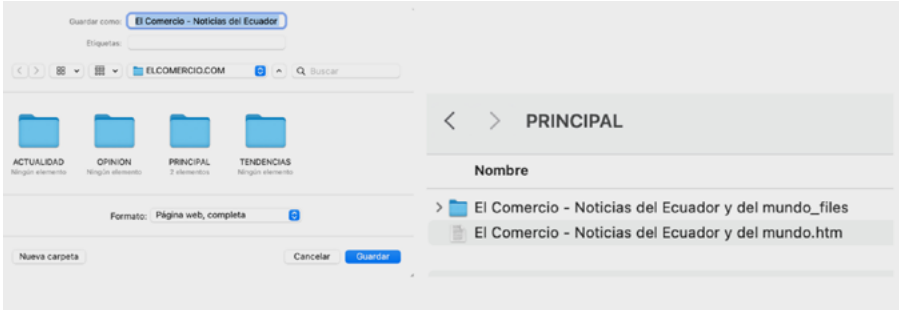
1. Identificar la página web con la cual trabajará en el proceso de 'aseguramiento'. Para el ejemplo, se usará la página web de El Comercio www.elcomercio.com.

2. En el equipo cree una carpeta y subcarpetas para el caso, que incluirán las secciones de la página, tal como se muestra en la imagen a continuación:

3. Una vez creadas las carpetas, se accede a la página que se requiere asegurar y se cargan cada una de las secciones por medio de la memoria caché. Para este procedimiento se debe navegar hasta la última parte de la página para guardar todo el contenido.

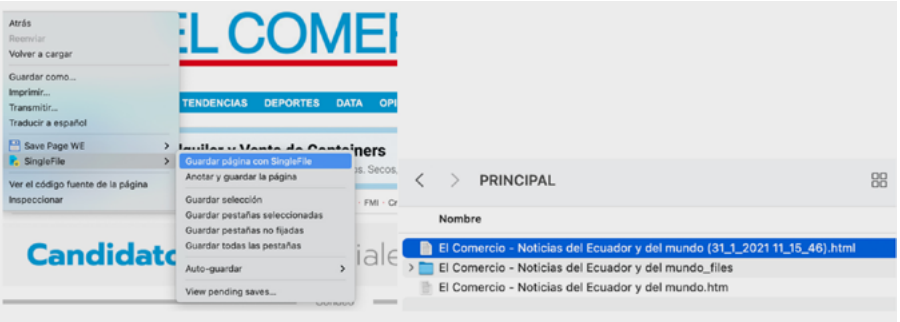
   El contenido de las páginas se puede almacenar de dos formas: la primera utilizando el método por defecto del navegador en la que se accede al Menú, Archivo y Guardar (Ctrl + S), de esta forma cada una de las páginas correspondientes quedará guardada en las carpetas previamente creadas. Para este proceso se debe tener en cuenta guardar la página web completa.

   Para el caso del ejemplo, se almacenará una página en formato htm y una carpeta con todo el contenido como se muestra en la imagen a continuación:



La segunda forma de almacenamiento es utilizando cualquiera de las extensiones mencionadas anteriormente, que sirven para guardar un único archivo sin necesidad de carpetas anexas. En este caso se ingresa a la página que se va a asegurar y se da clic derecho, a continuación, se selecciona la extensión, para este caso SingleFile. Luego se selecciona Guardar página con SingleFile. Finalmente. el archivo se almacena como archivo único en formato html y estará disponible con el nombre de la página, la fecha y hora de la adquisición.

Tal como se muestra en la imagen a continuación:



4. Una vez archivada la página web y todas las páginas de complemento que se requieren para el caso, se procede a crear una imagen forense lógica mediante la herramienta FTK Imager. La imagen forense se realiza a la carpeta creada inicialmente. En este proceso se debe tener especial énfasis en generar el listado hash de cada uno de los archivos.
5. Finalmente, la imagen forense se almacena en un contenedor estéril (USB, CD, DVD BluRay, etc.), que se debe embalar, rotular y someter al proceso de cadena de custodia.

¿Qué hacer si debo recolectar información pública en una red social?

Igual que las páginas web, las redes sociales se pueden asegurar siguiendo el mismo procedimiento, sin embargo, para lograr mejores resultados y poder posteriormente realizar solicitudes de colaboración judicial internacional, se debe conocer el ID (número único de identificación de usuario, publicación, página, etc.) que asigna la red social al usuario, para evitar confusiones por la cantidad de personas con el mismo nombre y facilidad que existe para cambiar o alterar el nombre.
A continuación, se muestra una de las formas para obtener el ID del usuario de las redes sociales más conocidas, la descripción del proceso va acompañada de una imagen que servirá como ejemplo:

Facebook

Se debe dirigir al perfil que requiere identificar, una vez en el perfil debe dar clic derecho y seleccionar Ver el código fuente de la página, a continuación, use el comando buscar y allí digite UserID.
De esta forma se obtendrá el número de usuario, de la forma en la que se muestra en la imagen a continuación:

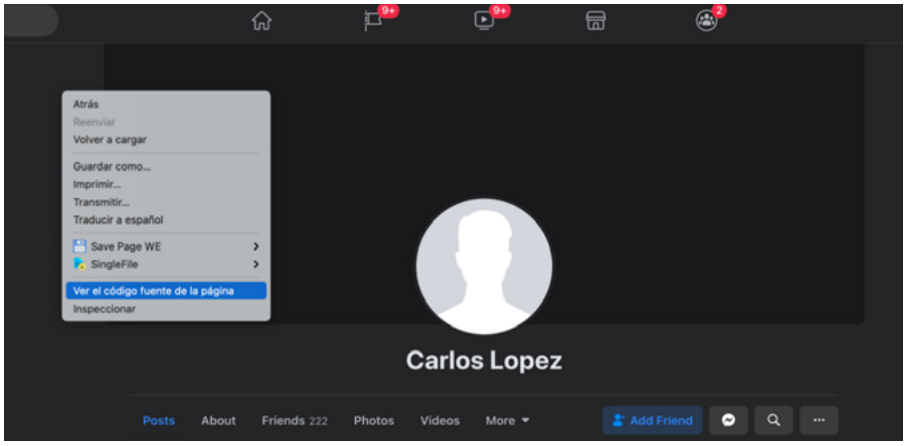


Ilustración 17: Análisis código fuente Facebook

Nota: Si se requiere buscar el ID de una página web se debe digitar PageID en lugar de UserID.

Twitter

Se debe dirigir al perfil que necesita identificar, dé clic derecho y use la función Ver código fuente de la página, allí debe digitar el comando id_str, de esta forma obtendrá el ID del perfil. Tal como se muestra en la imagen a continuación:

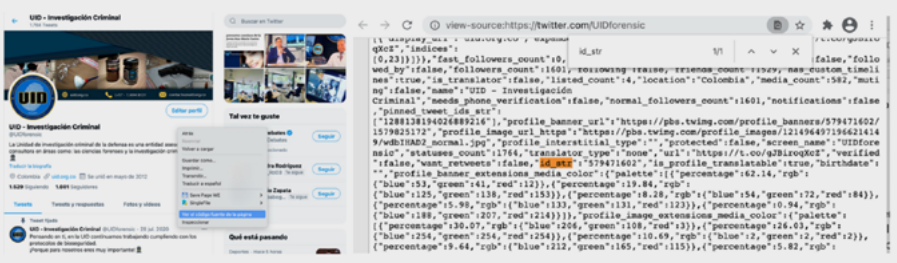


Ilustración 18: Análisis código fuente Twitter

Instagram

Instagram actualmente es propiedad de Facebook y los requerimientos judiciales son atendidos por la misma compañía. Debe ingresar al perfil del investigado por medio de un equipo de cómputo, dar clic derecho y usar la función de buscar con la palabra id. Recuerde que si selecciona viewerId le mostrará su propio ID y no el del investigado.

Lo veremos en la imagen a continuación:

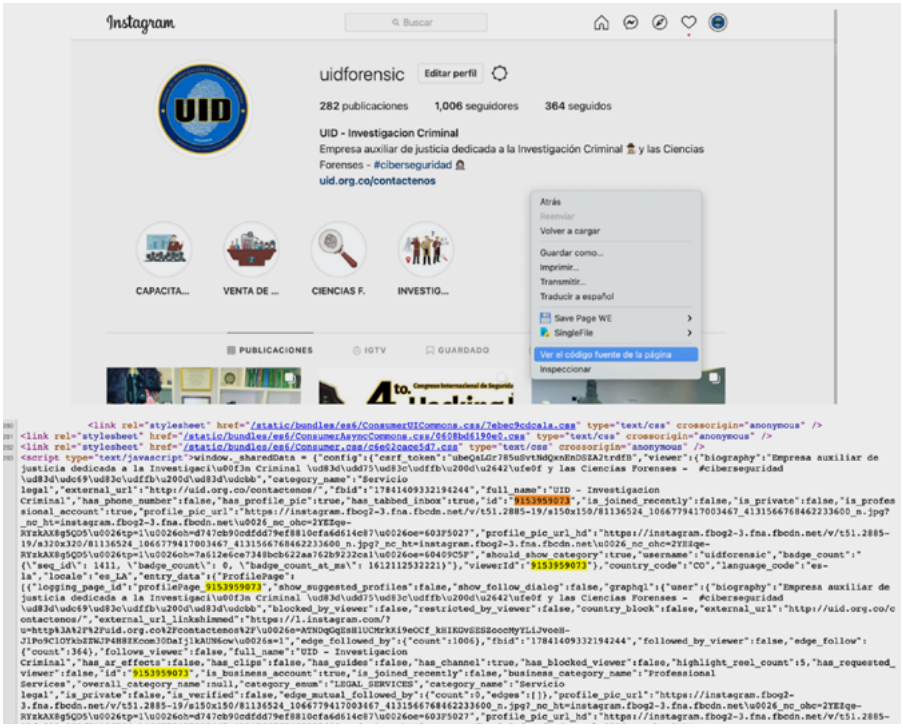


Ilustración 19: Análisis código fuente Instagram

Fase de examen o procesamiento

De acuerdo con las buenas prácticas internacionales, el examen no se debe realizar sobre la evidencia original sino sobre las imágenes forenses, en caso de no haber logrado una imagen forense por una causa mayor, se debe realizar el examen de la evidencia mediante el uso de bloqueadores de escritura. Este examen debe ser realizado por un experto para disminuir el riesgo de una mala práctica de manipulación, que termine en el daño o la eliminación de la evidencia.

Recepción de la evidencia digital o contenedores

Para la recepción de la evidencia se debe seguir lo establecido en el Manual de Cadena de Custodia, que determina las prácticas que deben seguir los responsables del almacenamiento, de la custodia y los peritos responsables de realizar el procesamiento de la evidencia. Para ejecutar la recepción de la evidencia se requiere contar con las órdenes necesarias y las solicitudes debidamente formalizadas por parte de la autoridad competente.

Clasificación o triaje

Al igual que los servicios de emergencias, el laboratorio de informática forense debe priorizar los casos y las evidencias que se enviarán a la fase de análisis. Este proceso se hace de acuerdo con los requerimientos de la autoridad solicitante, es posible que algunas evidencias o datos no pasen a la fase de análisis por su irrelevancia en el caso.

Generalmente, este proceso se realiza en casos que no disponen de una gran cantidad de evidencias o cuando tienen gran relevancia, por lo que se necesita agilizar los procedimientos. Se debe tener en cuenta que existen herramientas comerciales y de código abierto que permiten ejecutar búsquedas rápidas para realizar los procesos de priorización, sin embargo, existe la posibilidad de que fallen, ya que no realizan un proceso de análisis profundo.

Procesamiento de la evidencia

Una vez realizada la clasificación y priorización se inicia el procesamiento de la evidencia. Con ayuda de las herramientas forenses se obtiene mayor cantidad de datos con los que se puede completar con éxito lo solicitado dentro de las ordenes emitidas por la autoridad competente. Sin embargo, si el perito tiene la habilidad y el conocimiento necesarios puede realizar esta actividad de forma manual.

Para procesar la evidencia se debe tener claro qué tipo de recolección se efectuó (en vivo o post mortem) para decidir qué procedimientos, técnicas y herramientas se van a usar. Si el caso que se va a procesar es una evidencia obtenida de un sistema activo (en vivo) se debe tener en cuenta procesar la siguiente información:

- Memoria de acceso aleatorio (RAM)
- Memoria caché
- Procesos en ejecución, de red y del sistema
- Información de los archivos y configuraciones del sistema
- Medios de almacenamiento
- Servicios en la nube

Si la evidencia fue obtenida en un sistema inactivo (post mortem) es importante procesar, entre otros, los archivos activos, archivos borrados, particiones slack, discos slack, archivos ocultos, artefactos del dispositivo (datos del sistema), archivos del sistema operativo, registro de archivos, metadatos de archivos, archivos cifrados, archivos de registro (logs), archivos de bases de datos, historial de navegación, correo electrónico, redes sociales y archivos compartidos.

Las herramientas forenses realizan el procedimiento de forma automatizada y brindan la posibilidad de descifrar algunos archivos, la búsqueda de elementos en archivos comprimidos, la recuperación de archivos dañados, el reconocimiento de caracteres (OCR) de algunas imágenes y archivos pdf, la comparación hash de archivos, la indexación de palabras y el filtrado de datos, entre otros elementos, que permitirán un mejor análisis posterior de la información.
En el caso de los dispositivos móviles, las herramientas forenses hacen un procesamiento automatizado, seleccionan y clasifican los artefactos de manera gráfica para poder analizarlos, ya que la gran cantidad de sistemas operativos, marcas y modelos hacen que el procesamiento manual sea más complejo.

Fase de análisis

En la fase de análisis, el perito debe buscar la evidencia digital relacionada con el objetivo de la actividad ordenada en las imágenes forenses que obtuvo, esta actividad generalmente toma mucho tiempo y por tanto es muy importante prever una metodología adecuada que permita optimizar los recursos. De igual forma es indispensable que las autoridades judiciales hagan requerimientos claros y concisos para poder realizar un análisis exacto.

Análisis en evidencia de sistemas informáticos

Es una investigación por corrupción en donde se buscan hojas de cálculo, bases de datos, correos electrónicos y archivos similares.

Por tal motivo, se debe tener en cuenta qué tipo de evidencia se puede encontrar en estos análisis, como:

- Documentos ofimáticos y similares (archivos de procesadores de texto, hojas de cálculo, bases de datos de usuario, archivos pdf, presentaciones, etc.)
- Archivos multimedia (imágenes, videos, audios, etc.)
- Archivos de correo electrónico (archivos de correo o generados por clientes de correo con extensiones pst, ost, pab, eml, etc.)

- Evidencia de navegación por internet (archivos temporales, historial de navegación, marcadores, favoritos, cookies, información de sesiones, usuarios y contraseñas, campos de formularios entre otros).
- Bases de datos de aplicaciones.
- Software (Identificar el software comercial, el de comunicaciones, de transferencia de archivos, de criptomonedas, de cifrado, de esteganografía, etc.)
- Actividad de usuario
  - Tiempos de encendido y apagado
  - Configuración de software
  - Configuración del entorno del usuario
  - Conexiones wifi
  - Listas de archivos usados más recientemente
  - Archivos a los que se accede con mayor frecuencia
  - Programas preferidos
  - Uso del dispositivo
  - Inicios de sesión de usuario (último inicio, último inicio fallido, nombres de usuario, ID)
  - Uso de periféricos (impresora, escáner, etc.)
- Archivos de registro (logs) del sistema y de las aplicaciones
- Espacio sin asignar
- Almacenamiento en la nube y remoto
- Memoria RAM, (información de los procesos [identificadores], claves de cifrado, archivos abiertos, documentos no guardados, nombres de usuario, contraseñas, procesos en ejecución, entre otros).

Si se tiene en cuenta la gran cantidad de información, se sugiere usar las ayudas de las herramientas forenses para el análisis de datos, como por ejemplo las líneas de tiempo, los diagramas de relación y los diagramas de flujo.

Análisis en evidencia de dispositivos móviles

Los dispositivos móviles cumplen funciones similares a los sistemas de cómputo, sin embargo, al ser tecnología convergente tienen asignadas actividades adicionales, estos dispositivos generalmente pertenecen a un usuario específico y pueden brindar información valiosa sobre sus actividades, gustos, lugares visitados y comunicaciones (llamadas

y textos). En esta medida es necesario que los operadores judiciales conozcan estos artefactos para poder solicitar a los analistas que verifiquen la información en el dispositivo.

Los dispositivos móviles cuentan con los siguientes elementos:

- Información del dispositivo
- Cuentas vinculadas
- Historial de llamadas
- Lista de contactos
- Mensajes de texto (SMS), multimedia (MSM) y correos electrónicos
- Archivos multimedia (imágenes, videos, audios)
- Aplicaciones y software
- Registros de chat (WhatsApp, Telegram, Skype, Line, Weebo, WeChat, etc.)
- Historial de navegación y búsquedas
- Palabras del diccionario personalizado
- Conexiones de redes celulares, wifi y Bluetooth
- Cuentas y tokens de redes sociales
- Calendario y notas
- Mapas y ubicaciones (GPS y metadatos)
- Contraseñas
- Bases de datos

Fase de presentación

Una vez completado el análisis, inicia una de las fases más importantes para la administración de justicia ya que definirá si todo lo realizado con anterioridad servirá para la judicialización o no de los responsables en un crimen. Por esto, la ejecución de los procedimientos deben ser impecables y regirse por los estándares internacionales y las buenas prácticas que guían el uso de una metodología acertada y legal de la jurisdicción donde se pertenece.

En esta fase se muestran todos los procedimientos, las metodologías, las herramientas, el análisis, los hallazgos y las conclusiones de una manera clara, comprensible y precisa para que los intervinientes del proceso penal (fiscal, juez, defensa y acusados) entiendan fácilmente lo que se quiere presentar.

Informe forense

El informe es el documento base de la opinión pericial, en este se plasma todo lo relevante a la actividad de investigación digital forense y se caracteriza por ser preciso, oportuno, exhaustivo, imparcial, claro, relevante y completo.

El informe debe contener información, como:

- Entidad que emite el informe
- Número de proceso o caso
- Fecha y hora de la emisión del informe
- Normatividad local que respalde las actuaciones
- Destino del informe: (nombre, cargo, dirección, ciudad)
- Objetivo de la diligencia o solicitud recibida
- Descripción precisa de los elementos recibidos y la forma en que fueron entregados
- Descripción clara de las técnicas, procedimientos o guías empleadas sobre cómo se realizó la actividad técnico-científica
- Informe del grado de aceptación por la comunidad técnico-científica del procedimiento que se va a emplear y de las herramientas forenses que fueron utilizadas
- Instrumentos empleados y estado del instrumento al momento del examen (incluyendo su mantenimiento, versión o calibración)
- Explicación de los principios técnicos y científicos aplicados.
- Descripción paso a paso de los procedimientos o guías técnico-científicas utilizadas en el caso específico (puede incluir imágenes de apoyo)
- Interpretación de los resultados obtenidos
- Relación de los elementos de almacenamiento digital (CD, DVD, discos duros), que contengan la información encontrada en los dispositivos que fueron analizados, incluyendo sus respectivos hash y números de serie.
- Constancia de que se hace la devolución de la evidencia analizada, la cual debe ser entregada con su respectiva cadena de custodia.
- Información del tiempo que el laboratorio de informática forense va a tener guardada la evidencia digital.

Presentación en audiencia

La presentación del informe en audiencia debe ser realizada por un testigo experto que, en virtud de la educación, habilidad o experiencia, está capacitado con conocimientos especializados más allá de la persona promedio. El conocimiento del testigo es suficiente para que otros puedan confiar oficial y legalmente en su opinión especializada (científica, técnica u otra) sobre la evidencia o un hecho dentro del alcance de su experiencia, conocida como opinión experta (INTERPOL, 2019).

Para la presentación de este tipo de informes es importante tener en cuenta que el investigador digital forense debe tener la capacidad de expresar de manera clara y comprensible todo los procedimientos técnicos y legales, así como las conclusiones que se dejaron plasmadas en el informe a un público que en su mayoría son abogados o personas procesadas por delitos, y que no cuentan con formación técnica en sistemas. Se recomienda una revisión previa del informe, un simulacro de presentación con la parte que solicitó su testimonio y unos apuntes que generalmente se plasman en una libreta para usar de guía en la exposición.

Técnicas antiforenses

Así como la tecnología forense avanza, los cibercriminales buscan y encuentran formas para evitar ser descubiertos por las agencias de ley o para demorar las investigaciones digitales forenses, estas metodologías usadas son conocidas como las técnicas antiforenses, dentro de las cuales se destacan las siguientes:

1. **Técnica de borrado o destrucción de los MD**. Mediante esta técnica se borran los datos del sistema operativo o de los dispositivos de almacenamiento de un sistema de información. A través de herramientas especializadas se puede llegar a recuperar y/o reconstruir la información. Sin embargo, cuando se opta por un borrado seguro no existe forma alguna a nivel forense de recuperar dicha información.

   Si la evidencia se encuentra en la nube, es posible contar con archivos de caché de buscadores o páginas de indexación que pueden servir para documentar lo que existía en la red.

2. **Ocultación**. Mediante software o modificación de las propiedades de los archivos se intenta ocultar información usando técnicas como la estenografía, que se encarga de embeber archivos de cualquier tipo, como Word, imágenes o archivos de audio, haciendo que estos archivos sean invisibles para los investigadores. Esto hace complejo para las autoridades identificar lo que se está buscando.Algunas de las herramientas forenses presentadas en esta guía, permiten el procesamiento y análisis de estos archivos ocultos.

3. **Sobreescritura de metadatos**. Los metadatos son la información relevante de cada archivo, en ellos se encuentra la fecha de creación, modificación, y acceso, así como también el propietario, editor y equipos utilizados. Por ejemplo, en el caso de los archivos de imágenes se encuentran datos como las cámaras usadas, los píxeles e incluso información de geoetiquetas o referencias geográficas, elementos útiles para vincular estos archivos con hechos delictivos y usuarios; por este motivo algunos cibercriminales los modifican para dificultar la actividad investigativa.

4. **Cifrado de información.** Esta es una de las técnicas más complejas de investigar, ya que los delincuentes acceden a los ficheros y transforman los códigos, imposibilitando su lectura. Esto impide que los investigadores y las herramientas forenses tengan acceso a los ficheros, ya que no van a ser de fácil lectura.

Buenas prácticas en la investigación digital forense del crimen organizado

Uno de los grandes retos de las agencias de ley es la investigación digital del crimen organizado, debido a los diferentes problemas que se pueden presentar al recolectar la evidencia en la jurisdicción internacional, la cooperación de las agencias públicas y privadas, la volatilidad de la información en la nube y las legislaciones internacionales.

Es por esto que las policías en diversas partes del mundo, han enfocado sus esfuerzos a mejorar los procesos investigativos de análisis y prevención y han creado mecanismos de participación a través de la INTERPOL, EUROPOL, AMERIPOL, las Naciones Unidas y la Organización de Estados Americanos.

Dentro del crimen organizado digital se encuentran conductas como el ciberlavado de activos, explotación sexual infantil en línea, apuestas ilegales, crimen ciberdependiente (*ramsomware*, programa maligno, ataque de CEO, entre otros), tráfico de armas, narcotráfico, y estafas de criptodivisas.

Investigación trasnacional de cibercrimen organizado

Para realizar una efectiva investigación de los casos relacionados con el crimen organizado es necesario que el investigador digital forense investigue y conozca las modalidades y los posibles mecanismos de cooperación judicial internacional.

Deep web y dark web

Estos dos términos *deep web* y *dark web*, suelen confundirse, sin embargo, su significado es diferente. La *deep web* es una red que está formada por todos los sitios web, aplicaciones, contenidos de bases de datos, entre otros, que no están indexados por los motores de búsqueda como Google, Yahoo! y similares, este contenido no es contenido criminal necesariamente, ya que también almacena información académica, empresarial y estatal. Sin embargo, no es necesario ingresar a ellos a través de dominio o buscadores. La *dark web* es una red encriptada que solo se tiene acceso a través de la red TOR, que usa diversas capas para mantener el anonimato y las conexiones.

Las recomendaciones para los investigadores digitales para realizar patrullaje o investigaciones en la Deep web son:

1. Antes de acceder preferiblemente utilice un equipo independiente al de trabajo normal o cree una maquina virtual para usarla como Sand Box o Caja de Arena.

2. Instale el navegador Tor obtenido desde la pagina oficial https://www.torproject.org/es/

3. Como cualquier software, siempre es mejor mantenerlo actualizado, por lo que la opción de "actualizar automáticamente" debería estar seleccionada.

4. Seleccionar el modo permanente de navegación privada.

5. Para una mayor seguridad es preferible evitar otorgar permisos a los sitios que visitamos, especialmente el de ubicación.

6. Al descargar archivos de la Deep web se deben abrir de manera controlada para evitar cualquier tipo de intrusión.

7. Al estar dentro de las paginas de la Deep web o Dark web debemos tener en cuenta que por fallos de seguridad podemos ser victimas de ataques, razón por la cual siempre se debe estar alerta.

8. Recuerde que las paginas web de la Dark net y Deep web no tienen un dominio ni se encuentran indexadas por lo cual es importante conocer el enlace para poder ingresar, estos enlaces no tienen palabras conocidas o comunes, son solo combinaciones alfanuméricas lo cual dificulta su identificación.

Convergencia en el terrorismo y el internet

El terrorismo, a lo largo de los años, ha aprovechado los medios tecnológicos para lograr dos de sus objetivos principales, como captar fanáticos para fines terroristas y causar o trasmitir terror al mundo. A través de los foros habilitados en la *deep web*, las redes sociales y las aplicaciones de mensajería instantánea encriptadas, las organizaciones terroristas han logrado perfilar, ubicar, entrenar y adoctrinar a personas con ideales terroristas para realizar actos de espionaje o de terrorismo, incluso existen casos en los que estas conductas terroristas han sido realizadas en vivo, grabadas y expuestas en varias plataformas mundiales.

Crimen como Servicio (CaaS)

A través de la *dark web* se ha incrementado la modalidad de crimen como servicio (CaaS), mediante esta actividad el crimen organizado ofrece sus servicios a cambio de pagos generalmente en criptomonedas.
Dentro de los servicios se encuentra la venta de todo tipo de estupefacientes (convencionales y sintéticos), contrabando de cualquier índole, medicamentos falsos, servicios de *hacking*, ataques dirigidos, venta de mercancía robada, tráfico de armas, documentos de identificación falsos, sicarios a sueldo, entre otros.

Administración de la justicia y el ámbito internacional de la evidencia digital

Junto al crecimiento exponencial del cibercrimen, dentro de las dinámicas de los mercados criminales los países y organizaciones han tomado medidas desde hace varios años, que buscan fortalecer las capacidades investigativas y las herramientas de cooperación judicial internacional. Sin embargo, estos esfuerzos se complejizan debido al aumento significativo de los casos y la demora en la creación de nuevas leyes internas de cada país que permitan la adhesión de los países a los convenios internacionales.

Instrumentos de cooperación internacional

Convenio de Budapest

El Convenio sobre la Cibercriminalidad, firmado en Budapest en 2001, es uno de los esfuerzos más grandes que existen en la actualidad. Fue creado con el fin de fomentar una política criminal común entre todos los países participantes, para prevenir la criminalidad en el ciberespacio mediante la adopción de la legislación apropiada y la participación de mecanismos de cooperación judicial internacional.
Para el 2020, 106 países miembros de las Naciones Unidas (es decir aproximadamente el 55 %) contaban con legislación nacional para tipificar delitos informáticos y cometidos por medios informáticos. El Convenio de Budapest que puede ser consultado en la página oficial[1] hace una estandarización de conceptos y términos para que los países firmantes manejen la misma terminología, y así generar los requisitos mínimos para tipificar las normas que enmarquen los delitos informáticos. Hay que tener en cuenta que los delitos informáticos son aquellos que atentan contra la integridad, disponibilidad y confidencialidad de la información, así como los que son cometidos a través de cualquier sistema informático.

1 https://www.coe.int/en/web/cybercrime/the-budapest-convention

Los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos se identifican como:

- Acceso ilícito (artículo 2)
- Interceptación ilícita (artículo 3)
- Ataques a la integridad de los datos (artículo 4)
- Ataques a la integridad del sistema (artículo 5)
- Abuso de los dispositivos (artículo 6)

Delitos informáticos

- Falsificación informática (artículo 7)
- Fraude informático (artículo 8)

Delitos relacionados con el contenido

- Delitos relacionados con la pornografía infantil (artículo 9)
- Delitos relacionados con infracciones de la propiedad

De igual manera, el Convenio de Budapest define las normas procesales en las que se establecen los procedimientos para obtener y custodiar la evidencia digital, y las herramientas necesarias para tal fin. Dentro de estas normas procesales se abarca cualquier delito cometido por un medio informático o cualquier tipo de evidencia en formato digital con el fin de ser usadas como pruebas dentro de un proceso. Las herramientas pueden ser: la conservación rápida de datos informáticos almacenados, la obtención en tiempo real de datos relativos al tráfico, la interceptación de datos relativos al contenido, entre otras.

Por último, se definen las normas de cooperación judicial internacional para estos delitos y los procedimientos para definir la jurisdicción, localización, captura de sospechosos y extradición y, por último, el convenio que define un eje central para la creación de un punto de contacto 24/7 en el que se atenderá cualquier tipo de solicitud de los países firmantes.

Model Law on Computer and Computer Related Crime

Es una ley modelo sobre delitos informáticos desarrollada por la *Commonwealth of Nations* o Mancomunidad de Naciones. De acuerdo con su sitio web oficial esta ley fue un esfuerzo de los países de la *Commonwealth* para armonizar su derecho penal relacionado con la informática con el Convenio de Budapest. La ley modelo sirve como ejemplo de principios comunes que cada país puede utilizar para adaptar la legislación al marco compatible con otros países del *Commonwealth.*

Proyecto SIRIUS

El proyecto SIRIUS fue creado por la Europol en octubre de 2017, como respuesta a la creciente necesidad de la comunidad policial de la Unión Europea (UE) de acceder a pruebas electrónicas para investigaciones basadas en internet. Más de la mitad de las investigaciones penales en la actualidad incluyen una solicitud de acceso transfronteriza o evidencia electrónica (como mensajes de texto, correos electrónicos o aplicaciones de mensajería).

El proyecto SIRIUS, encabezado por el Centro Europeo de Lucha contra el Terrorismo y el Centro Europeo de Ciberdelincuencia de Europol, en estrecha colaboración con Eurojust y la Red Judicial Europea, tiene como objetivo ayudar a los investigadores a hacer frente a la complejidad y el volumen de información en un entorno en línea que cambia rápidamente, proporciona directrices sobre proveedores de servicios en línea (OSP) y herramientas de investigación específicas. El proyecto anima a compartir las experiencias con compañeros, tanto en línea como en persona. Gracias a la colaboración continua con Eurojust y la Red Judicial Europea, el proyecto SIRIUS está abierto a las autoridades judiciales.

La comunidad multidisciplinar de SIRIUS (en la plataforma restringida de la plataforma Europol para expertos) tiene acceso a una amplia gama de recursos actualizados continuamente. La comunidad representa a los 28 Estados miembros y a varios países terceros que tienen un acuerdo operativo con Europol.

En el futuro, el proyecto SIRIUS continuará brindando capacitaciones virtuales de alta calidad a través de la plataforma CEPOL, herramientas innovadoras para ayudar con las investigaciones en línea, así como las pautas actualizadas que reflejan los últimos cambios en las políticas de aplicación de la ley de los principales proveedores de servicios en línea. De esta forma, SIRIUS tendrá una contribución significativa en la perspectiva judicial del proyecto (EUROPOL, 2021).

Solicitudes internacionales de cooperación judicial

Para el proceso investigativo, el perito o investigador digital forense debe conocer de manera clara y precisa cómo y dónde realizar las solicitudes a los proveedores de servicios a nivel internacional, así mismo debe saber qué solicitudes puede pedir para no tener demoras en la actividad investigativa (Garavito, 2008).

Las peticiones comunes son: requerimiento directo para cooperación voluntaria, requerimiento de preservación (PR), requerimiento de emergencia (EDR), requerimiento de obtención (DR) y asistencia judicial (MLA).

A continuación, se realizará un resumen de los proveedores de servicios más comunes, haciendo la distinción que en ocasiones no basta con una orden judicial local o solicitud de conservación, sino que se requerirá un exhorto o carta rogatoria a través de oficinas consulares.

Facebook e Instagram

Para obtener información de Facebook e Instagram, que no puede ser obtenida a través de los métodos convencionales ya descritos o incluso con la autorización del titular que es una opción muy usada, es importante indicar que se puede consultar las guías para las agencias de ley en el siguiente enlace:

https://es-la.facebook.com/safety/groups/law/guidelines/

Así mismo se pueden enviar los requerimientos a la dirección postal de los Estados Unidos para ambas aplicaciones, ya que pertenecen a la misma compañía:
1601 Willow Road, Menlo Park, CA 94025
Attention: Facebook Security, Law Enforcement Response Team

Cabe resaltar que para usar los canales establecidos por las agencias de ley se debe enviar, mediante el correo institucional, los soportes pertinentes a través del Portal para Agencias de Ley de Facebook para requerimientos de conservación y emergencia: records@records.facebook.com

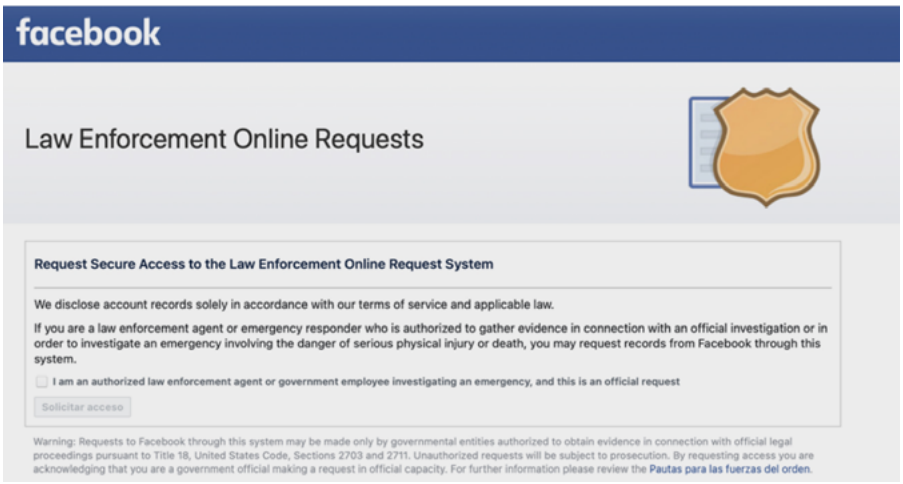


Ilustración 20: Portal agencias de ley Facebook

¿Qué se puede solicitar a Facebook mediante un MLA?

Los tipos de datos que se pueden solicitar a través de asistencia judicial mutua incluyen, pero no se limitan a:

Información del usuario

- Nombre, sexo y fecha de nacimiento
- Nombre personalizado
- Información "Acerca de"
- Teléfono móvil
- Información sobre trabajo y educación
- Lugares donde el usuario ha vivido o vive
- Eventos de la vida
- Canciones agregadas al perfil del usuario
- Fecha de registro y dirección IP con sello de tiempo
- Libreta de direcciones
- Información de contactos
- Información de pago
- Número de tarjeta de crédito o débito u otra información de la tarjeta

Ubicación

- Historial de ubicaciones precisas recibidas a través de los dispositivos del usuario
- Ubicación principal del usuario

Publicaciones

- Publicaciones (fotos, videos, texto y actualizaciones de estado) compartidas por el usuario, incluidas las eliminadas
- Publicaciones (fotos, videos, texto y actualizaciones de estado) donde se etiqueta al usuario específico
- Publicaciones de otras personas en la cronología del usuario
- Publicaciones ocultas en la cronología del usuario
- Notas creadas por el usuario o donde se han etiquetado
- Encuestas creadas por el usuario o en las que ha participado

- Metadatos del contenido cargado
- Videos vistos en Facebook

Me gusta y reacciones

- Publicaciones, comentarios y páginas a las que el usuario ha calificado como Me gusta o ha reaccionado.

Comentarios

- Comentarios o respuestas en publicaciones del usuario, en publicaciones de otras personas o en grupos a los que se unió

Amigos

- Amigos con los que el usuario está conectado actualmente
- Amigos eliminados a los que el usuario ya no está conectado
- Solicitudes de amistad enviadas y recibidas por el usuario
- Personas bloqueadas por el usuario
- Personas que han bloqueado al usuario
- Configuración de notificaciones
- Configuración / bloqueos de privacidad

Grupos

- Grupos a los que pertenece el usuario y fechas de incorporación
- Publicaciones y comentarios realizados en grupos
- Siguiendo y seguidores

Personas, organizaciones o empresas seguidas

- Mensajes
  Mensajes intercambiados con otras personas en Messenger
- Eventos
  Lista de eventos creados por el usuario
  Respuestas a eventos que incluyen ("Asistir", "Quizás", "Interesado" y "No asistir")
  Invitaciones a eventos recibidas por el usuario
- Páginas
  Páginas de las que el usuario es administrador
- Mercado:

Actividad del usuario en Marketplace

- Historial de pagos
  Historial de pagos realizados por el usuario a través de Facebook
- Colecciones y artículos guardados:
  Publicaciones, fotos y videos guardados por el usuario
  Colecciones de publicaciones, fotos y videos guardados por el usuario
  Colecciones de las que el usuario forma parte

Lugares

- Nombre de los lugares creados por el usuario, sus ubicaciones y el momento de la creación
- Lugares de registro
- Aplicaciones y sitios web

Aplicaciones y sitios web en los que el usuario inicia sesión cuando usa Facebook

- Aplicaciones de las que el usuario es administrador
- Publicaciones de las aplicaciones que el usuario ha dado permiso para publicar en su nombre
- Productos o servicios vinculados a la cuenta de Facebook del usuario

Anuncios

- Intereses publicitarios
- Anunciantes en cuyos anuncios el usuario hizo clic en Facebook

Buscar historia

- Palabras, frases y nombres que el usuario ha buscado
- Videos que el usuario ha buscado

Otra actividad

- Pokes dados y recibidos por el usuario
- Encuestas y programas de juegos en los que el usuario ha participado y respondido preguntas
- Regalos
- Donaciones

Información de inicio de sesión y cookies

- Historial de inicios y salidas de sesión y duración de la sesión
- Computadoras y otros dispositivos que el usuario haya guardado en su cuenta de Facebook
- Registros de actividad
- Dispositivos utilizados para iniciar sesión
- Atributos de dispositivos
- Señales del dispositivo: señales de Bluetooth e información sobre los puntos de acceso wifi, balizas y torres de telefonía móvil cercanos
- Datos de la configuración del dispositivo: información recibida a través de la configuración del dispositivo que el usuario activa, como el acceso a la ubicación GPS, la cámara o las fotos
- Red y conexiones: información como el nombre del operador de telefonía móvil, OSP del usuario, idioma, zona horaria, número de teléfono móvil, dirección IP, velocidad de conexión e información sobre otros dispositivos que se encuentran cerca o en la red del usuario
- Datos de *cookies*: datos de cookies almacenados en el dispositivo del usuario, incluidas las ID y la configuración de las *cookies*
- Otras cuentas y dispositivos de Facebook que utilizaron las *cookies* del usuario

WhatsApp

La aplicación de WhatsApp es una de las más populares a nivel mundial, es importante indicar que WhatsApp no tiene habilitada la posibilidad de compartir datos con las agencias de ley ni gobiernos sobre el contenido relativo al tráfico de las comunicaciones entre los usuarios, sin embargo sí permite a los usuarios descargar su propia información. Esta función permite exportar un informe de la información y la configuración de la cuenta de WhatsApp, revelando la siguiente información:

Información del usuario

- Solicitud de informe y tiempo de generación
- Número de teléfono
- Nombre
- Estado de conexión

- En línea / Fuera de línea / Inactivo desde
- IP de conexión anterior / actual
- Tipo de dispositivo / Número de compilación del SO / Fabricante / Modelo
- Versión de la aplicación
- Versión Web / Escritorio / Plataforma / Conectado desde / Estado de disponibilidad / Inactivo desde
- Acerca de
- Acerca de la hora establecida
- Imagen de perfil y tiempo de carga
- Contactos
- Grupos

Términos de servicio aceptados
Información de registro

- Plataforma
- Red y nombre de la red
- Dispositivo
- Hora de registro

Configuración

- Privacidad vista por última vez
- Privacidad de la foto de perfil
- Acerca de la privacidad y la privacidad del estado

Números bloqueados
Confirmación de lectura

En el caso de WhatsApp, los requerimientos deben ser remitidos a la dirección:

WhatsApp Inc.,
Law Enforcement Response Team
1601 Willow Road, Menlo Park, California 94025, United States of America
records@records.whatsapp.com

Portal de acceso de agencias de ley de WhatsApp

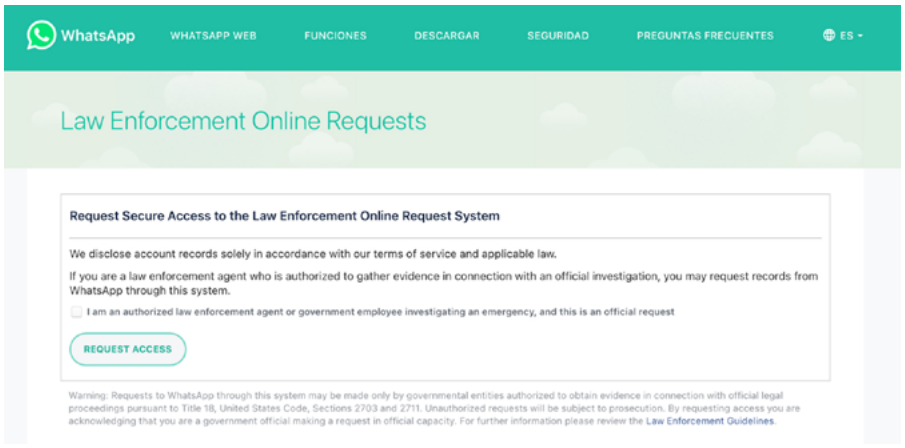


Ilustración 21: Portal agencias de ley WhatsApp

*Es importante indicar que WhatsApp puede informarle al usuario sobre el requerimiento judicial.

Twitter

Para conocer los requisitos de Twitter para las agencias de ley, se deber ingresar al siguiente enlace:

https://help.twitter.com/es/rules-and-policies/twitter-law-enforcement-support

En el caso de Twitter, los requerimientos deben ser dirigidos a la dirección:

Twitter, Inc.
c/o Trust & Safety - Legal Policy
1355 Market Street, Suite 900
San Francisco, CA 94103

Portal de acceso de agencias de ley de Twitter:

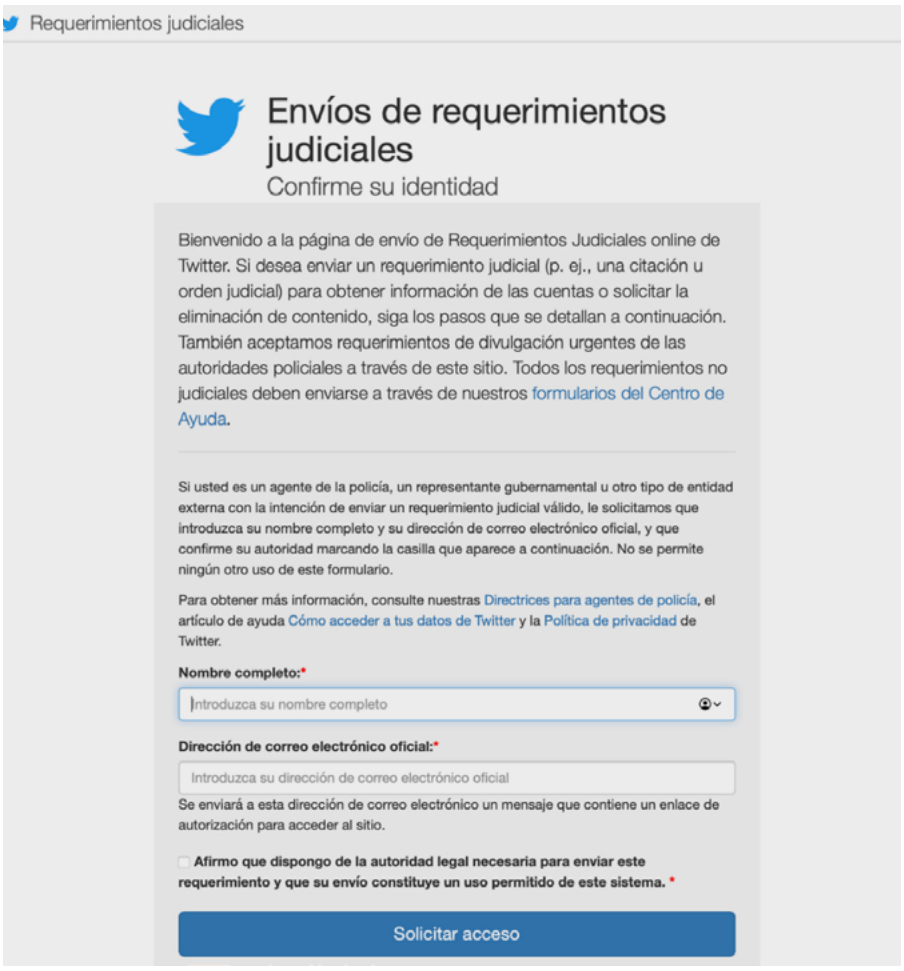


Ilustración 20: Portal agencias de ley Twitter

Microsoft

Microsoft es una empresa que centraliza información de los siguientes servicios:

- Cuenta Microsoft
- Correo electrónico
- Xbox
- One Drive
- Skype

En el caso de Microsoft, para realizar requerimientos judiciales de información se debe ingresar al portal de agencias de ley para Latinoamérica, en caso de ser requerimiento de emergencia se pueden realizar a través al correo electrónico LEALERT@microsoft.com, la información que se puede solicitar, hay que tener en cuenta que en algunos casos se requiere un tratado de asistencia judicial mutua (MLAT) es:

Datos de cuenta Microsoft

- Detalles de registro (información obtenida al momento de registro de la cuenta)
- Información de cobro (puede incluir dirección y medio(s) de pago)
- Transacciones de cobro (MLAT)
- Registros IP (direcciones IP obtenidas al momento de inicio de sesión del usuario a un servicio específico)
- Correo electrónico alternativo y/o alias
- Servicios utilizados

Datos de servicio de correo electrónico

- Detalles de registro (información obtenida al momento de registrar la cuenta)
- Registros IP (dirección IP utilizada al momento de iniciar sesión al servicio de correo electrónico)
- Encabezados en correo electrónico (requiere MLAT)
- Contenido del correo electrónico (requiere MLAT)
- Contactos de correo electrónico (MLAT)

Datos de servicio de XBOX

- Detalles de registro (información obtenida al momento de registro de la cuenta)
- Número de serial o Gamertag
- Registros IP (direcciones IP obtenidas al momento de iniciar sesión en algún servicio XBOX)
- Historial de cambio de Gamertag (requiere MLAT)
- Contactos de XBOX (requiere MLAT)
- Historial de juegos en línea de XBOX (requiere MLAT)
- Comunicaciones almacenadas (requiere MLAT)

Datos de servicio OneDrive

- Detalles de registro (información obtenida al momento de registro de la cuenta)
- Registros IP (direcciones IP obtenidas al momento de iniciar sesión en algún servicio OneDrive)
- Archivos almacenados (requiere MLAT)
- Registro de transacciones (requiere MLAT)

Datos del servicio de Skype

- Detalles de registro (obtenidos al momento de registrar la cuenta)
- Dirección de facturación (dirección de facturación provista por el usuario)
- Método de pago / Instrument Data
- Registros IP (dirección IP utilizada al momento de iniciar sesión al servicio de correo electrónico)
- Historial de números de servicio de Skype (lista de número(s) de Skype asociados a un usuario)
- Registros de llamas Skype Out (historial de llamadas hechas a una línea adscrita a una Red Telefónica Pública Conmutada)
- Registros de Skype Numbers (historial de llamadas recibidas de una línea adscrita a una Red Telefónica Pública Conmutada)
- Historial de compras (datos de transacciones) (requiere MLAT)
- Datos de SMS (Historial de detalle de SMS) (requiere MLAT)
- Datos de correo electrónico (datos históricos de cambio de correo electrónico) (requiere MLAT)
- Lista de contactos del nombre de usuario de Skype (requiere MLAT)
- Contenido de chats/media del usuario de Skype (requiere MLAT)

Bibliografía

RFC 3227. (2002). *Guidelines for Evidence Collection and Archiving.* Recuperado de: https://tools.ietf.org/html/rfc3227

AccessData. (n.d.). *FTK Imager.* Recuperado de: https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager

Oxygen Forensic. (n.d.). Recuperado de: https://www.oxygen-forensic.com/es/products/oxygen-forensic-detective

Compelson Soft. (n.d.). Recuperado de: https://www.mobiledit.com/forensic-express/esp

Naciones Unidas. (1996). *Ley Modelo sobre Comercio Electrónico aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.*

ISO/IEC. (2012). *ISO/IEC 27037:2012.*

INTERPOL. (2019). *INTERPOL Global guidelines for digital forensics laboratories.* Singapore: INTERPOL Global Complex for Innovation.

EUROPOL. (2021, 01 20). SIRIUS PROJECT. Recuperado de: https://www.europol.europa.eu/activities-services/sirius-project

Garavito, Y. (2008). Factores que inciden en la no judicialización de la explotación sexual cometida a través de las redes sociales en Colombia (2013-2015). *En Introducción del desarrollo científico en la investigación criminal*. Policia Nacional de Colombia.

Congreso Nacional. (2014). Código Orgánico Integral Penal.

Congreso Nacional. (2002). Ley de comercio electrónico, firmas electrónicas y mensajes de datos. En: *Ley 2002-67.*

Guía técnica sobre análisis forense y evidencia digital

PADF
FUNDACIÓN PANAMERICANA PARA EL DESARROLLO

CON EL APOYO DE LA
OFICINA INTERNACIONAL
DE ASUNTOS ANTINARCÓTICOS Y
APLICACIÓN DE LA LEY (INL)