MPD
Argentina

AUDITORÍA FORENSE

Y ANÁLISIS DE DATOS CON UFED READER

Dra. Verónica Blanco
Ing. Natalia Passarini García

Passarini, Natalia
Auditoría Forense : y Análisis de datos con UFED Reader / Natalia Passarini ; Verónica Blanco. - 1a ed - Ciudad Autónoma de Buenos Aires : Defensoría General de la Nación, 2024.
Libro digital, PDF

Archivo Digital: descarga y online
ISBN 978-987-48966-7-4

1. Pericias. 2. Auditoría Forense. 3. Auditoría Informática. I. Blanco, Verónica II. Título
CDD 004

Ministerio Público de la Defensa

Defensora General de la Nación
Dra. Stella Maris Martínez

Secretaría General de Política Institucional
Javier Lancestremere

Contenidos:
Natalia Passarini
Verónica Blanco

Diseño y diagramación:
Subdirección de Comunicación Institucional

Defensoría General de la Nación
Av. Callao 970 - Ciudad Autónoma de Buenos Aires
Te. 011 4814-8400
www.mpd.gov.ar

Presentación

Este libro ha sido elaborado como material de apoyo para el curso "Auditoría Forense y Análisis de Datos con UFED Reader", impartido por la Escuela de la Defensa Pública. Su contenido ha sido diseñado específicamente para complementar y reforzar los conocimientos impartidos en el curso, ofreciendo a los estudiantes una herramienta práctica y accesible que los acompañará en su proceso de aprendizaje. El objetivo de este curso es proporcionar las habilidades necesarias para analizar, cuestionar y validar la evidencia digital:

- Adquirir un conocimiento sólido sobre las funcionalidades y capacidades de UFED Reader.

- Desarrollar habilidades para interpretar correctamente los datos extraídos de dispositivos móviles utilizando UFED Reader.

- Desarrollar habilidades para realizar un análisis forense detallado, identificando y extrayendo información relevante para construir una estrategia de defensa efectiva.

Esperamos que les sea de mucha utilidad.

Dra. Verónica Blanco
Ing. Natalia Passarini García

Índice

Presentación **3**

Capítulo I

La evidencia digital **8**

Características de la evidencia digital **9**

Procesos para el manejo de la evidencia digital **10**

Análisis del tratamiento de la evidencia digital por parte de la defensa de asistidos **11**

Principios de la evidencia digital **12**

Requisitos para el manejo de la evidencia digital **13**

Excepciones al principio de reproducibilidad y repetibilidad en dispositivos electrónicos **14**

Capítulo II

Conceptos fundamentales de la informática fosense. **16**

Imagen forense o copia forense

ICCID

IMEI (International Mobile Equipment Identity)

Hash

Dirección IP

IMSI (International Mobile Subscriber Identity)

Potencial elemento de prueba (PEP)

Tethering

Dirección MAC (Media Access Control)

Implantación de información digital

El BSSID (Basic Service Set Identifier

El SSID (Service Set Identifier)

Carving

Capítulo III
La cadena de custodia 21

El valor de la cadena de custodia y su impacto en el proceso judicial 22

Aspectos que la defensa de imputados debe evaluar en la cadena de custodia 23

La importancia de evaluar la integridad de la información en la defensa de asistidos: más allá de la cadena de custodia 24

Principios criminalísticos que se aplican a la informática forense ..25

- Principio de compatibilización
- Principio de identidad pericial
- Principio de identidad atípico o principio de identidad de copias forenses
- El principio de sensibilidad remota
- El principio de oportunidad
- Principio de protección y preservación
- El principio de vinculación estricta
- El principio de correspondencia o de identificación comparativa
- El principio de reconstrucción de los hechos
- Principio de probabilidad

Relación entre la cadena de custodia y la protección de la privacidad 26

Requisitos de validez de la cadena de custodia 26

Esquema de la cadena de custodia e integridad del PEP 27

Procedimientos para dispositivos móviles 29

- Identificación y registro
- Protección del dispositivo
- Embalaje y traslado

Intervención notarial en la recolección de prueba informático forense 31

Capítulo IV
Cellebrite UFED 32

Niveles de extracción **33**

Extracción lógica (Logical)

Extracción de sistema de archivos o lógica avanzada (File System or Logical Advanced)

Extracción Física (Physical)

Zonas Horarias **37**

¿Como se cambia la zona horaria en el UFED?

La marca de tiempo en una extracción de UFED

La importancia de la marca de tiempo en el contexto de la defensa

¿Como visualizar la cronología?

Capítulo V

Introducción al análisis forense de dispositivos móviles 42

Tipos de datos extraíbles de un dispositivo móvil **43**

Datos de comunicación

Datos de ubicación

Archivos multimedia

Datos de aplicaciones

Datos del sistema

Metadatos

Archivos de sistema y logs

Datos eliminados u ocultos

Panel "Datos Analizados" del UFED **45**

Filtrado de información para enfocar el análisis

Marcadores

Exportación de datos UFED

Crear informes personalizados UFED

Filtrado de información para enfocar el análisis **46**

Marcadores **48**

Exportación de datos UFED **50**

Crear informes personalizados UFED **52**

Anexo
Protocolo para la evidencia digital 57

Glosario 59

Bibliografía 62

Capítulo I

La evidencia digital

La evidencia digital es cualquier tipo de información o dato almacenado o transmitido en formato digital que poseen valor probatorio y pueden ser utilizados en procesos legales para sustentar o refutar hechos en un juicio.

CARACTERÍSTICAS DE LA EVIDENCIA DIGITAL

Es volátil y efímera: la evidencia digital puede desaparecer rápidamente si no se actúa de inmediato. Por ejemplo, la memoria RAM o el caché del sistema se borran al apagar o reiniciar un dispositivo. Debido a su naturaleza temporal, es crucial recuperarla y preservarla tan pronto como sea posible para evitar su pérdida.

Anónima: Vincular la evidencia digital a una persona específica suele ser complejo. Se lo puede vincular a un dispositivo, pero es difícil probar que una persona en particular lo creó, es necesario recurrir a un análisis más profundo para intentar establecer una conexión con el responsable.

Editable y susceptible a la corrupción: La evidencia digital es altamente modificable. Un archivo puede ser editado o alterado, con o sin dejar rastros evidentes de las modificaciones. Por esta razón, es crucial aplicar técnicas forenses que detecten cambios en los datos y se aseguren de que la evidencia sea preservada en su forma original mediante el uso de hashes.

Eliminable sin dejar rastro: La evidencia digital puede ser completamente eliminada o destruida, y en algunos casos, es posible

hacerlo sin dejar ningún rastro visible. Herramientas especializadas permiten borrar datos de manera que se hace casi imposible recuperarlos. Esto resalta la importancia de actuar con rapidez en la preservación de evidencia y el cuidado de la cadena de custodia.

PROCESOS PARA EL MANEJO DE LA EVIDENCIA DIGITAL

La normativa ISO/IEC 27037:2012 estructura el tratamiento de las evidencias en cuatro procesos principales, que sirven como un modelo genérico para el tratamiento de la evidencia.

1. **Identificación**: localizar y reconocer donde se encuentra la información potencial, ya sea en estado físico o lógico, que pueda contener datos relevantes para la investigación.

2. **Recolección**: consiste en obtener los dispositivos que pueden contener evidencia digital potencial. Este proceso debe realizarse de forma controlada y siguiendo los procedimientos de custodia establecidos, evitando cualquier manipulación que pueda comprometer los datos.

3. **Adquisición**: implica producir una copia forense de la información y documentar de manera clara y detallada los métodos utilizados y las actividades realizadas.

4. **Preservacion**: la evidencia digital debe ser almacenada de manera segura para prevenir modificaciones accidentales o deliberadas. Esto puede incluir medidas como el uso de jaula de Faraday, el cifrado de los datos y la documentación de cada paso en la cadena de custodia.

ANÁLISIS DEL TRATAMIENTO DE LA EVIDENCIA DIGITAL POR PARTE DE LA DEFENSA DE ASISTIDOS

La evidencia digital, por su naturaleza, puede ser adulterada de manera intencional o accidental debido a un manejo inadecuado. Por ello, es fundamental verificar que las personas encargadas de manejar evidencia digital sean competentes y sigan métodos científicos propios del campo forense.

La falta de pericia en el manejo de dispositivos digitales puede convertir las potenciales evidencias digitales (PEP) en pruebas inservibles.

Se debe realizar un análisis exhaustivo del tratamiento que tuvo la evidencia digital para asegurar que el asistido reciba un juicio justo. Algunos de los aspectos fundamentales que deben ser considerados, organizados según los cuatros procesos:

Identificación

Se debe evaluar si la evidencia identificada es realmente relevante para el caso y que los datos que se identificaron como evidencia estén directamente relacionados con los hechos.

Recolección

Se debe evaluar la legalidad en la obtención de la evidencia, verificando si fue obtenida de acuerdo con la leyy asegurando que la recolección de la evidencia no violó los derechos fundamentales del asistido.

Además, es necesario verificar que la recolección incluyó la creación de copias forenses de los datos, garantizando que la evidencia original no se haya alterado durante la extracción.

Adquisición

Se debe comprobar que los métodos utilizados para adquirir la evidencia digital aseguran su autenticidad. Esto incluye la verifi-

cación de integridad mediante herramientas como los hashes, garantizando que los datos no han sido alterados.

Preservación

Se debe examinar si la preservación de la evidencia digital siguió un protocolo estricto de cadena de custodia. Cualquier falla en la documentación o manejo de la evidencia puede abrir la puerta a cuestionamientos sobre su validez.

Es fundamental verificar que la evidencia digital se ha mantenido intacta durante todo el proceso judicial. Cualquier modificación, ya sea accidental o deliberada, podría invalidar la prueba.

PRINCIPIOS DE LA EVIDENCIA DIGITAL

La normativa ISO/IEC 27037:2012 establece tres elementos esenciales que deben estar presentes para que la información digital sea considerada como Evidencia Ddigital.

Pertinencia: La evidencia digital es pertinente cuando sirve para demostrar o descartar un elemento del caso que se investiga.

Confiabilidad: Debe garantizar que la evidencia digital es auténtica y no ha sido alterada.

Suficiencia: Es necesario recolectar suficiente evidencia para realizar una investigación apropiada.

REQUISITOS PARA EL MANEJO DE LA EVIDENCIA DIGITAL

Además, la norma **ISO/IEC 27037:2012** establece cuatros aspectos fundamentales para la gestión de evidencia:

Proceso Auditable: Un evaluador independiente puede revisar las actividades realizadas por los peritos, así como la metodología y la documentación empleadas. El perito debe justificar todas las acciones realizadas, y se debe evaluar si siguió una metodología científica y un procedimiento adecuado.

Proceso Reproducibles y Repetibles: Los métodos y procesos utilizados deben ser reproducibles, de manera que, al aplicar los mismos procedimientos, métodos de medición, instrumentos y condiciones, se obtengan los mismos resultados.

Proceso Justificable: El perito debe justificar todas las acciones y métodos utilizados en el manejo de la potencial evidencia digital mediante la **demostración y la validación de las actuaciones.**

La demostración se refiere a que debe poder explicar qué hizo y cómo lo hizo. La validación de las actuaciones significa que los métodos utilizados han sido probados previamente como efectivos y confiables dentro del campo forense.

EXCEPCIONES AL PRINCIPIO DE REPRODUCIBILIDAD Y REPETIBILIDAD EN DISPOSITIVOS ELECTRÓNICOS

Aunque el principio de reproducibilidad y repetibilidad son esenciales en la ciencia forense, existen limitaciones prácticas en su aplicación a dispositivos móviles y aquellos en los que no se puede hacer una copia bit a bit, o que tengan limitaciones técnicas, cifrado avanzado o daños físicos. Todos estos factores pueden impedir que dos extracciones produzcan resultados idénticos. Las principales excepciones son:

Dispositivos dañados o con fallos de almacenamiento

Cuando un dispositivo ha sufrido daños físicos o tiene fallos en su almacenamiento (como sectores dañados en el chip de memoria), no siempre es posible hacer una copia bit a bit ni asegurar que todas las extracciones sean iguales, dependiendo del grado de daño; las partes recuperadas pueden variar en cada intento.

Acceso limitado por parte del fabricante

Las políticas de seguridad del fabricante o las características del dispositivo pueden impedir copias forenses completas.

En versiones recientes de sistemas operativos, las medidas de seguridad limitan la cantidad de datos que se pueden extraer.

Dispositivos con memoria volátil

La memoria volátil (RAM) almacena datos solo temporalmente mientras el dispositivo está encendido. Una vez que el dispositivo se apaga o reinicia, los datos en esta memoria se pierden o se modifican. Esto dificulta que dos extracciones forenses realizadas en diferentes momentos sean idénticas.

Sistemas operativos con particiones dinámicas

Los sistemas operativos como iOS y Android utilizan mecanismos de aislamiento de datos en aplicaciones (sandboxing), lo que limita la capacidad de acceso a toda la información del dispositivo. Algunos datos podrían no ser extraíbles en su totalidad o de la misma manera en diferentes intentos, lo que afecta la repetibilidad del proceso.

Dispositivos móviles con cifrado avanzado

Algunos dispositivos móviles usan cifrados avanzados, como el cifrado completo del dispositivo (FDE), lo que impide hacer una copia bit a bit sin la clave o desbloqueo. La extracción de datos varía según el estado del dispositivo y los métodos usados para acceder al cifrado.

Los archivos thumbnails

Un Thumbnail es una representación visual pequeña y compacta de un contenido más grande de un vídeo o una imagen. Estos archivos proporcionan una referencia visual que ayuda al usuario a decidir si acceder o no al contenido. La generación de estos archivos es automática y de carácter temporal. Estos factores hacen que las miniaturas no sean siempre idénticas o estén siempre presentes entre diferentes extracciones.

Capítulo II

Conceptos fundamentales de la informática forense

Imagen Forense: Es una réplica exacta, bit a bit, de toda la información contenida en un medio digital (como un disco duro, pendrive, celular, etc.). A diferencia de un backup, la copia forense no solo copia los archivos visibles, sino también los sectores del disco que contienen datos, incluso los espacios no utilizados pero escritos.

Copia Forense: es una copia exacta de un dispositivo digital, pero no de todos los datos que contiene.

Se diferencia también del clonado de disco, donde se copian particiones específicas, pero no necesariamente todas las particiones ni toda la información almacenada en el disco. En cambio, la copia forense garantiza la captura de absolutamente todo el contenido del dispositivo, asegurando una representación fiel de todos los datos, visibles o no.

ICCID (Integrated Circuit Card Identifier): es el número de identificación único asignado a cada tarjeta SIM.

El ICCID Identifica a la tarjeta SIM y es fundamental para que las operadoras de telecomunicaciones gestionen las suscripciones y autentiquen el acceso a la red móvil.

IMEI (International Mobile Equipment Identity): es un número único de identificación asignado a cada dispositivo móvil. El IMEI identifica los dispositivos móviles a nivel mundial.

Hash: Es una función criptográfica que aplica un algoritmo matemático para convertir un bloque de datos en una cadena de caracteres de longitud fija, sin importar el tamaño de los datos originales.

Un hash es único para un conjunto específico de datos, por lo que cualquier cambio, incluso mínimo, en los datos originales producirá un hash completamente diferente.

El hash se utiliza para garantizar la integridad de los datos copiados. Al crear una copia forense de un dispositivo o archivo, se genera un hash de los datos originales antes de la copia y otro hash de los datos después de la copia. Si ambos hashes coinciden, se confirma que la copia es una réplica exacta de los datos originales y sin alteraciones. Con este proceso se preserva la validez de la evidencia digital.

Dirección IP: La IP (Protocolo de Internet) es una dirección que identifica de manera única a un dispositivo en una red. La dirección IP puede ser pública o privada.

La dirección IP pública: es asignada por un proveedor de servicios de Internet (ISP) que identifica un dispositivo en la red global de Internet. Permite que los dispositivos sean accesibles desde cualquier parte del mundo. Un dispositivo usa una IP pública para conectarse a Internet, mientras que internamente opera con IP privadas. Por Ejemplo, una PC usara la IP Pública para poder conectarse a internet y la IP privada para poder comunicarse con otros equipos como una impresora u otros equipos.

La dirección de IP privada: es una dirección asignada a un dispositivo dentro de una red local para permitir su comunicación con otros dispositivos en esa misma red. Estas direcciones no son accesibles desde Internet.

IMSI (International Mobile Subscriber Identity): es un número único utilizado para identificar de forma global a un abonado en una red móvil. Este número está vinculado a la tarjeta SIM y no al dispositivo, y es utilizado por las operadoras para autenticar y gestionar la conexión del usuario a la red.

MSISDN (Mobile Station International Subscriber Directory Number): es el número de teléfono completo de un usuario móvil que

incluye el código de país, el código de área, y el número del abonado. Se diferencia del IMSI (International Mobile Subscriber Identity) en que este último se utiliza solo dentro de la red del operador para identificar y localizar al suscriptor, mientras que el MSISDN es el número de teléfono que se usa para llamar o enviar mensajes.

SMSC (short Message Service Center): es el centro de mensajes de texto en una red móvil, encargado de recibir, almacenar y enviar SMS entre teléfonos. El número de SMSC es el número de teléfono que identifica a este centro en la red.

Potencial elemento de prueba (PEP): son aquellos dispositivos susceptibles de contener información y potencialmente contener evidencia digital.

Tethering: es el proceso mediante el cual un dispositivo comparte su conexión a Internet con otros dispositivos, permitiéndoles acceder a la red. Esto se puede hacer a través de Wi-Fi , Bluetooth o un cable USB.

Dirección MAC (Media Access Control): es un identificador único asignado a la tarjeta de red de un dispositivo para la comunicación en redes locales (LAN). Está compuesta por 48 bits (6 bloques de dos caracteres hexadecimales de 8 bits). Esta dirección física permite que los dispositivos de una misma red se identifiquen y se comuniquen entre sí. A diferencia de una dirección IP, que es modificable, la dirección MAC es asignada por el fabricante de la tarjeta de red y es exclusiva para cada dispositivo.

Implantación de información digital: Es la acción de introducir deliberadamente datos falsos en un sistema, archivo o dispositivo con el propósito de distorsionar los hechos y alterar el curso de una investigación, generando evidencia que no corresponde a la realidad.

El BSSID (Basic Service Set Identifier) es un identificador único que se utiliza en redes inalámbricas Wi-Fi para identificar un punto de acceso (Access Point, AP) o una estación de red. Es la dirección MAC (Media Access Control) del punto de acceso.

El SSID (Service Set Identifier) es el nombre de una red inalámbrica Wi-Fi. El SSID es lo que se ve cuando se buscas redes Wi-Fi disponibles en un dispositivo.

Ilustración 1. SSID

Carving: es una herramienta utilizada para recuperar datos eliminados, o información que se encuentren en un sistema de archivo dañado, en la memoria, en el archivo de paginación y tráfico o en fragmentos de archivos que no están indexados en el sistema de archivos del dispositivo.

Capítulo III

La cadena de custodia

La cadena de custodia traza el camino recorrido por la evidencia desde su descubrimiento hasta su presentación en el tribunal.

Cada acceso, manipulación o modificación se documenta minuciosamente, creando un registro sólido que garantice la integridad de la evidencia. Este proceso es fundamental para asegurar la fiabilidad de la prueba y su validez en el juicio.

La cadena de custodia actúa como una garantía de que los datos obtenidos son auténticos y no han sido manipulados.

EL VALOR DE LA CADENA DE CUSTODIA Y SU IMPACTO EN EL PROCESO JUDICIAL

La cadena de custodia, como un hilo conductor a lo largo del proceso, se convierte en la base sobre la cual se construye la confiabilidad de la prueba. Los tribunales confían en que la evidencia presentada es auténtica y no ha sido alterada de ninguna manera. La cadena de custodia garantiza:

Mantenimiento de la integridad de la prueba: La cadena de custodia asegura que la evidencia se mantiene en su estado original, sin modificaciones que puedan afectar su valor probatorio.

La autenticidad: La cadena de custodia asegura que la evidencia no ha sido manipulada, alterada o contaminada desde el momento de su recolección hasta su presentación en el tribunal.

La confiabilidad de la evidencia: al garantizar que los procedimientos fueron seguidos rigurosamente, se refuerza la credibilidad de todo el proceso judicial.

Protección de los derechos del imputado: La cadena de custodia protege los derechos de los asistidos, al asegurar que cualquier prueba utilizada en su contra sea legítima y fiable.

ASPECTOS QUE LA DEFENSA DE IMPUTADOS DEBE EVALUAR EN LA CADENA DE CUSTODIA

Es necesario analizar si en la cadena de custodia existen posibles errores o violaciones en el manejo de la evidencia que puedan comprometer su integridad y, por ende, su admisibilidad en juicio. Cualquier deficiencia en la documentación, trazabilidad o procedimientos seguidos podría servir como fundamento para impugnar la validez de la evidencia presentada por la fiscalía.

Los puntos fundamentales que la defensa debe considerar son:

Integridad de la Evidencia. Es fundamental evaluar si la evidencia ha sido alterada o manipulada desde su recolección (desde el secuestro del dispositivo hasta la extracción). Cualquier alteración podría comprometer su validez. Es necesario verificar las condiciones en las que se almacenó la evidencia.

Revisar los registros de la cadena de custodia. Cada paso en el manejo de la evidencia debe quedar documentado. La defensa debe asegurarse de que los registros sean completos, precisos y detallados, con la identificación de todas las personas que manipularon la evidencia.

Trazabilidad de la evidencia. La defensa debe asegurarse de que la evidencia se puede rastrear cronológicamente desde su secuestro. Además, se debe comprobar que los sellos y empaques de la evidencia no hayan sido alterados.

LA IMPORTANCIA DE EVALUAR LA INTEGRIDAD DE LA INFORMACIÓN EN LA DEFENSA DE ASISTIDOS: MÁS ALLÁ DE LA CADENA DE CUSTODIA

La cadena de custodia se implementa con el fin de garantizar la integridad de la información. Si un perito añade un registro durante la búsqueda de información sin documentarlo en la cadena de custodia, se habrá violado la integridad de la información, sin que la cadena de custodia, en sí misma, se haya roto, por esto es importante ir más allá de verificar la violación de la cadena de custodia.

La cadena de custodia se encarga de rastrear y documentar quién tuvo acceso a la evidencia y en qué condiciones, pero esto no garantiza automáticamente que la información no haya sido alterada o manipulada. Un error o acción no documentada durante la investigación, como la adición o modificación de registros por parte de un perito, puede afectar la integridad de la información, aun cuando todos los pasos en la cadena de custodia hayan sido formalmente seguidos. Por lo tanto, es relevante evaluar tanto la cadena de custodia como el contenido y los procesos de manejo de la información para asegurar su fiabilidad y autenticidad.

PRINCIPIOS CRIMINALÍSTICOS QUE SE APLICAN A LA INFORMÁTICA FORENSE

La norma **IRAM 36100:2024** enumera los siguientes principios:

Principio de compatibilización. Este principio establece que la validez de la prueba digital no solo depende de su integridad técnica, sino también de su compatibilidad con las leyes del país y con los tratados internacionales.

Principio de identidad pericial. La informática forense debe ser tratada como una disciplina pericial específica dentro del marco de la criminalística, y que su manejo requiere de métodos, cuidados y técnicas particulares para asegurar su validez.

Principio de identidad atípico o principio de identidad de copias forenses. A diferencia de otros tipos de pruebas, las copias forenses no son "similares" al original, sino que son idénticas.

Debido a que la copia forense es una copia bit a bit no es posible establecer cuál es el original y cuál es la copia, salvo que se haya presenciado el proceso de duplicación y se sepa cuál era el dispositivo que contenía el original y cuál el de la copia.

Este principio permite que la copia forense pueda ser utilizada para el análisis, evitando así, cualquier riesgo para el original.

El principio de sensibilidad remota. Se refiere a la alta vulnerabilidad que tienen los soportes digitales frente a influencias externas, ya sea de manera intencional (dolosa) o por negligencia (culposa). Esto significa que los dispositivos que almacenan información digital son extremadamente sensibles a manipulaciones, y pueden ser modificados tanto localmente como de manera remota. Por este motivo es de suma importancia que se conserve siempre la cadena de custodia.

El principio de oportunidad. La necesidad de actuar de manera inmediata en la recolección de evidencias digitales para evitar que puedan ser destruidas o alteradas.

Principio de protección y preservación. La cadena de custodia debe ser estricta y se debe aplicar algoritmos de hash para poder garantizar la integridad de la evidencia digital.

El principio de vinculación estricta. La evidencia digital recolectada puede ser relevante no solo para el delito investigado inicialmente, sino también para otros delitos o actividades delictivas conectadas.

El principio de correspondencia o de identificación comparativa. La conexión que existe entre los indicios y el autor del hecho. Este principio establece que los indicios encontrados en la escena del crimen o relacionados con un hecho delictivo se comparan con características del autor para determinar una coincidencia.

El principio de reconstrucción de los hechos. Permite deducir cómo ocurrieron los hechos a partir de los indicios encontrados y el análisis de la evidencia recolectada en el lugar del hecho.

Principio de probabilidad. La probabilidad de ocurrencia de un hecho en función del número de coincidencias encontradas entre los indicios y la situación investigada.

Se utiliza para medir la certeza o grado de confianza en los resultados obtenidos.

RELACIÓN ENTRE LA CADENA DE CUSTODIA Y LA PROTECCIÓN DE LA PRIVACIDAD

La norma **IRAM 36100:2024** indica que la cadena de custodia garantiza la integridad de la prueba, pero no basta por sí sola para asegurar el respeto a la privacidad. Para que una prueba sea admisible, es necesario no solo preservar la cadena de custodia, sino también que su recolección se haya realizado conforme a la ley.

REQUISITOS DE VALIDEZ DE LA CADENA DE CUSTODIA

La norma **IRAM 36100:2024** establece que los requisitos de validez de la cadena de custodia en informática forense se centran en asegurar dos elementos clave:

1. La trazabilidad:

Humana: es necesario que se identifique de manera precisa a cada persona responsable de manipular la prueba, desde el momento en que se recolecta hasta su disposición final.

Física: se debe poder determinar en todo momento la ubicación física exacta de la prueba.

Lógica: debe haber una descripción precisa y un esquema que especifique cómo se distribuye y protege la información que ha sido accedida y almacenada.

2. La trazabilidad:

Integridad: la prueba no debe haber sido alterada desde su recolección.

Autenticidad: se debe poder verificar que la prueba es genuina.

Confidencialidad: se debe proteger la información de accesos no autorizados.

No repudio: se debe garantizar que el evento ocurrió y que fue realizado por las entidades que lo llevaron a cabo.

ESQUEMA DE LA CADENA DE CUSTODIA E INTEGRIDAD DEL PEP

La norma IRAM 36100:2024 elaboró un esquema que describe los pasos y procedimientos para asegurar que la evidencia digital sea recolectada, preservada y transportada de manera correcta y sin alteraciones. Este esquema es esencial para mantener la integridad de la prueba a lo largo de todo el proceso.

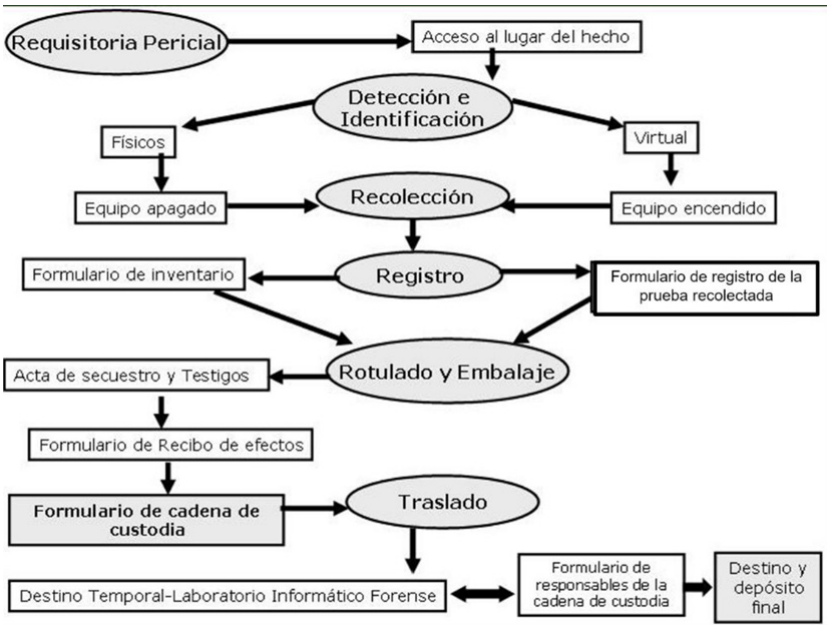


Ilustración 2 Protocolo Norma IRAM 36100:2024 para preservar la integridad del PEP

Acceso al lugar del hecho: donde se realizará la recolección o adquisición de la prueba sin contaminar, transformar o modificar la naturaleza de los PEPs.

Identificación, detección y registro: se debe identificar inequívocamente todos los elementos informáticos dubitados y registrarlo en el formulario del inventario.

Recolección de los elementos informáticos dubitados físicos o virtuales: donde se utilizan herramientas y técnicas específicas según el tipo de indicio.

Autenticación, duplicación y resguardo de la prueba: este proceso incluye la generación del digesto matemático (hash) que se encuentre vigente y que no hayan sido vulnerados para asegurar su integridad.

Resguardo de la prueba y preparación para su traslado: el resguardo de los indicios consiste en aplicar métodos adecuados de conservación que permitan preservar, asegurar y proteger el indicio, según su naturaleza, con el objetivo de mantener su integridad para su análisis y estudio posterior.

Traslado de la prueba: El traslado de la prueba debe tener como destino el sitio de resguardo asignado, asegurando que la cadena de custodia sea mantenida y actualizada durante todo su ciclo de vida.

PROCEDIMIENTOS PARA DISPOSITIVOS MÓVILES

La norma IRAM 36100:2024 establece de manera detallada los procedimientos aplicables a todos los dispositivos. En nuestro caso, nos enfocaremos específicamente en el procedimiento para los dispositivos móviles.

Identificación y registro

El primer interviniente en la evidencia digital (PIED) debe:

1. Usar guantes para manipular el dispositivo.

2. Fotografiar el dispositivo.

3. Registrar la marca y el modelo del dispositivo, número de serie, etc.

4. Si es posible, solicitar al gabinete de criminalística que identifique huellas digitales u otros elementos químicos.

5. Acomodar los dispositivos para su rotulado y registro.

6. Registrar todos los detalles relevantes en el formulario de registro de la prueba.

Protección del dispositivo

Los dispositivos pueden encontrarse en dos estados (encendido o apagado) y se toman medidas diferentes según el caso:

a) Si está encendido:

1. Mantener el dispositivo cargado y no manipularlo, evitando tocar la pantalla táctil si es un dispositivo de este tipo.

2. Aislar el teléfono de la red envolviéndolo en varias capas de papel de aluminio o colocándolo en una caja de Faraday y configurarlo en modo avión.

3. Si el dispositivo es GSM, remover la tarjeta SIM para deshabilitar las llamadas, mensajes y transmisión de datos. Esto no desactiva las redes inalámbricas.

Mantener el equipo encendido puede llevar a la pérdida de datos si la batería se agota o si el dispositivo se desconecta de la red. Si se apaga, se pueden perder datos temporales, y al encenderlo puede solicitarse una clave de acceso.

b) Si está apagado:

1. Mantener el dispositivo apagado para evitar la sobreescritura de datos.

2. No conectar el dispositivo a un cargador ya que esto es como si se lo hubiese encendido, se recomienda conectarlo al cargador solo después de haberlo puesto en modo DFU (o modo de prueba de fallos) y hasta que sea seguro realizar la recolección de datos.

Embalaje y traslado

El PIED (primer interviniente en la evidencia digital) debe:

1. Colocar el dispositivo en una bolsa de aluminio o en una jaula de Faraday para aislarlo de las señales externas y sellarla adecuadamente.

2. Asegurar que el equipo esté inmovilizado dentro de un recipiente para evitar daños durante el traslado.

3. Completar el formulario de cadena de custodia con todos los datos pertinentes.

Este procedimiento asegura que los dispositivos móviles sean manipulados, preservados y trasladados adecuadamente, manteniendo la integridad de los datos.

INTERVENCIÓN NOTARIAL EN LA RECOLECCIÓN DE PRUEBA INFORMÁTICO FORENSE

En la recolección de prueba informática forense, la intervención notarial tiene un rol específico, pero limitado en cuanto a las acciones que puede certificar. Si bien un escribano tiene la capacidad de otorgar fe pública a ciertos actos, como la generación de un hash o digesto matemático para asegurar la integridad de la evidencia digital, no está capacitado para certificar las acciones técnicas que realiza un perito forense durante la recolección y análisis de la prueba digital. Estas acciones, como la duplicación forense de discos duros, el análisis de dispositivos móviles o la extracción de datos, requieren conocimientos técnicos especializados en informática forense, un campo en el que los escribanos no tienen formación.

El perito informático forense es el profesional especializado y responsable de la recolección, preservación y análisis de la prueba digital según lo establecido en las normas **IRAM-ISO-IEC 27037: 2024, IRAM-ISO-IEC 27042:2024 y IRAM 36100:2024.**

Capítulo IV

Cellebrite UFED

EL UFED es una herramienta avanzada de hardware y software desarrollada por la empresa Cellebrite, que se utiliza en las investigaciones forenses para la extracción y análisis de datos de dispositivos móviles.

El UFED Reader es una herramienta complementaria de Cellebrite diseñada para visualizar y analizar los informes generados por UFED tras la extracción de datos de dispositivos móviles. Esta aplicación permite acceder fácilmente a la información extraída, como también exportar reportes y generar informes.

NIVELES DE EXTRACCIÓN

Dependiendo del tipo de dispositivo, pueden existir varios métodos de extracción de datos, y es frecuente realizar más de una extracción en el mismo equipo.

Es importante entender las diferencias entre los distintos niveles de extracción, ya que cada uno puede recuperar una cantidad variable de datos. Sin embargo, no todos los dispositivos son compatibles con todos los niveles de extracción disponibles.

Extracción lógica (Logical)

Este es el nivel más básico de extracción, donde se recopilan los datos accesibles directamente a través del sistema operativo del dispositivo.

En este nivel se extrae: registros de llamadas contactos, mensajes SMS, datos de aplicaciones como WhatsApp, redes sociales, entre otros.

Ventajas de este tipo de extracción: rápida, segura y generalmente no invasiva.

Limitaciones: no se accede a datos eliminados ni a información almacenada en áreas protegidas o del sistema.

Extracción de sistema de archivos o lógica avanzada (File System or Logical Advanced)

Este método proporciona un acceso más profundo al sistema de archivos del dispositivo, permitiendo la recuperación de una mayor cantidad de datos, incluyendo aquellos que no son accesibles desde la interfaz de usuario.

En este nivel se extrae: además de los datos accesibles mediante la extracción lógica, se puede acceder a archivos de sistema, carpetas ocultas, y algunas veces a datos de aplicaciones que no son accesibles desde la interfaz de usuario.

Ventajas de este tipo de extracción: recupera más datos que la extracción lógica, incluyendo archivos de sistema y otros datos que podrían ser importantes.

Limitaciones: es mucho más lento que la extracción lógica, no siempre se puede acceder a todos los archivos, especialmente en dispositivos con mayor seguridad.

Extracción física (Physical)

Una extracción física copiará toda la memoria del dispositivo y recuperará la mayor cantidad de datos.

Este método crea una copia bit a bit de toda la memoria del dispositivo, lo que permite recuperar prácticamente todos los datos almacenados, incluidos los que han sido eliminados, los datos ocultos y los que no son accesibles a través de la interfaz de usuario del sistema operativo.

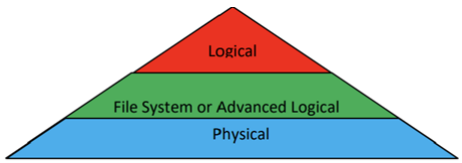
En este nivel se extrae: además de los datos que se obtiene en la lógica avanzada, se obtienen datos eliminados (siempre y cuando no hayan sido sobrescritos en la memoria del dispositivo), archivos ocultos, datos del sistema, etc.

Ventajas de este tipo de extracción: es el método más completo para recuperar la mayor cantidad posible de datos de un dispositivo.

Limitaciones: requiere más tiempo debido a la cantidad de datos extraídos, este proceso es más lento y consume más recursos que los métodos lógicos o de sistema de archivos.

Compatibilidad limitada: no todos los dispositivos permiten la extracción física, especialmente aquellos con altos niveles de cifrado o seguridad.

Riesgo de Daño: existe un riesgo mayor de alterar o dañar el dispositivo durante el proceso, especialmente en dispositivos más sensibles o antiguos.



Extraction Type	Level	Data Recovered
1. Logical	Basic level	Current data
2. File System	Intermediate level	Current and some deleted
3. Physical	Advanced level	Current data and deleted

Ilustración 3. Niveles según tipo de extracción.

Identificación del tipo de extracción en UFED

Para identificar el tipo de extracción, simplemente dirígete a la sección "Hogar" o "Tipo de Hogar" según la versión que estés utilizando. En el "**Resumen de extracción**", se encuentra el detalle del tipo de extracción, como se muestra en la siguiente imagen.

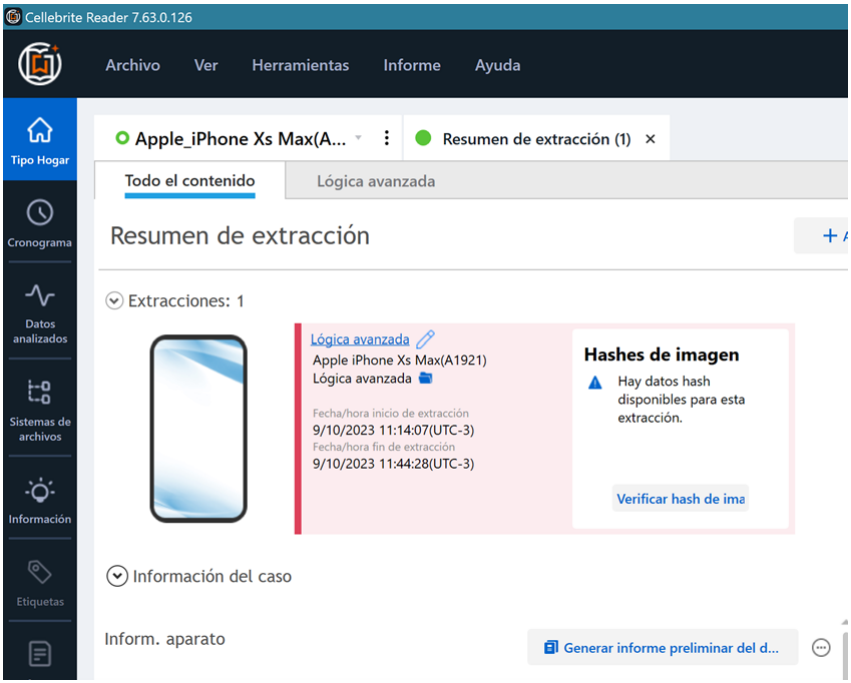


Ilustración 4. Resumen de Extracción UFED

En algunos casos, puede haberse realizado más de una extracción, lo cual depende del tipo de dispositivo y de la versión de UFED utilizada. A menudo, se comienza con el tipo de extracción más básica para garantizar que la extracción se realice correctamente, ya que una extracción más avanzada puede implicar ciertos riesgos.

Una vez asegurada la extracción inicial, se procede a realizar una extracción avanzada.

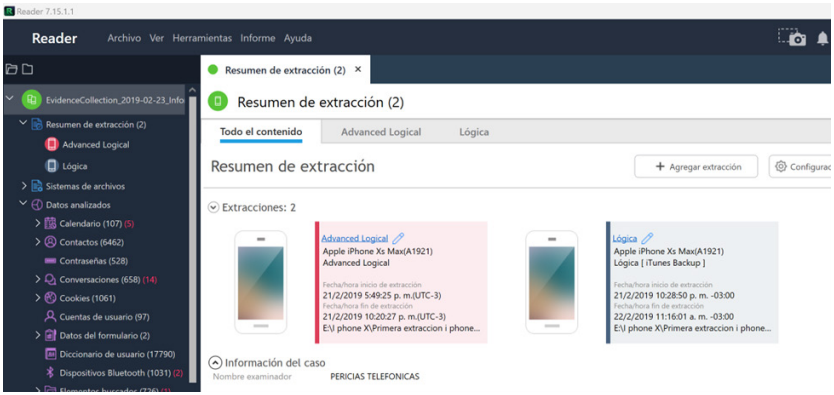


Ilustración 5. Resumen UFED con 2 extracciones

ZONAS HORARIAS

La **UTC** (Hora Universal Coordinada, es el estándar de tiempo internacional utilizado para regular los relojes y la hora en todo el mundo.

UTC representa una línea vertical trazada en la Tierra que cruza Greenwich (0° de longitud), que se encuentra en Inglaterra. Las zonas horarias de todo el mundo se aplican al este o al oeste de esta línea, creando un desplazamiento UTC negativo () o positivo (+).

En Argentina, la hora estándar corresponde a UTC-3. Esto significa que si tenemos un evento registrado en UTC (±0), debemos restarle 3 horas para convertirlo al horario argentino. Por ejemplo, un evento registrado a las 17:00 HS en UTC (±0) equivaldría a las 14:00 HS en UTC-3, que es el horario de Argentina.

El horario de verano (DST): es una práctica utilizada en algunos países para aprovechar mejor la luz natural durante los meses de verano, consiste en adelantar los relojes una hora respecto al horario estándar durante la primavera y verano, para extender la luz del día en las horas de la tarde.

¿Como se cambia la zona horaria en el UFED?

Para cambiar la zona horaria en toda extracción del teléfono, ir al **menú herramientas**, luego seleccionar "**Configuración del proyecto**".

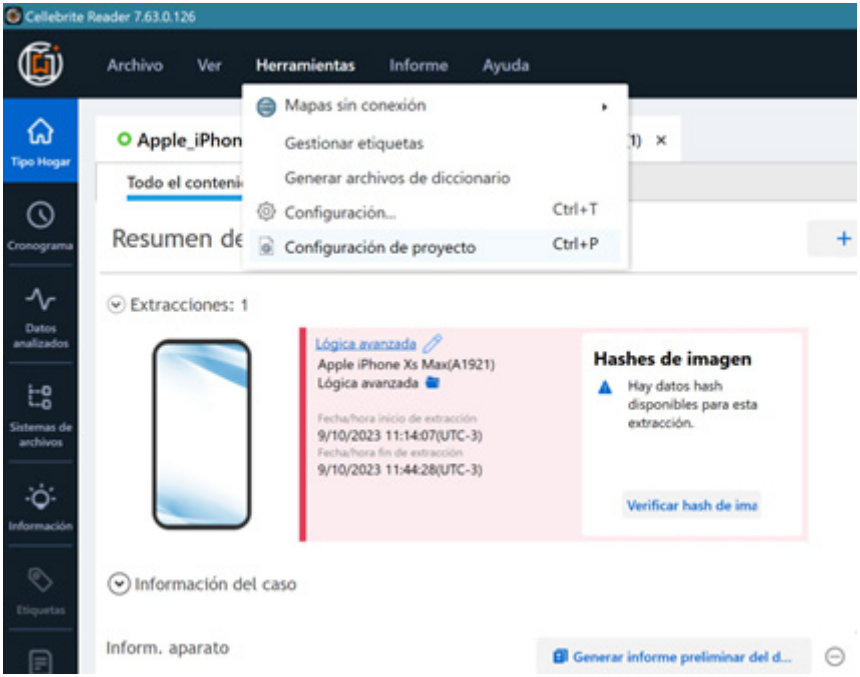


Ilustración 6. Configuración del proyecto. Configuración de la zona horaria

Dentro de **configuración del proyecto**, en **Configuración general** debemos ir a la **configuración de zona horaria (UTC)** y elegir la zona horaria que corresponda, luego hacer clic en **aceptar**.

Es importante verificar y ajustar esta configuración cada vez que se abra UFED, para asegurarse de que la zona horaria esté correcta y, si es necesario, realizar las correcciones pertinentes.

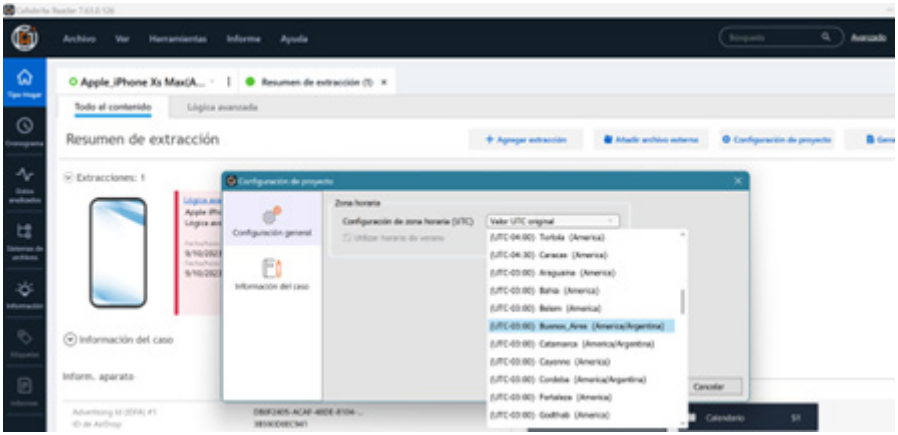


Ilustración 7. Cambio de zona horaria

La marca de tiempo en una extracción de UFED

La marca de tiempo en la extracción de UFED es un registro preciso del momento en que una acción o evento específico ocurrió en un dispositivo móvil. Esta marca de tiempo se asocia siempre con elementos de datos como mensajes, llamadas, fotos, videos, etc. Esta se guarda en formato UTC y debe ser convertida a la hora local según la ubicación del dispositivo para asegurar que la hora registrada sea consistente y pueda ser interpretada correctamente con un hecho.

La importancia de la marca de tiempo en el contexto de la defensa

La marca de tiempo desempeña un papel crucial en la defensa de los asistidos, cumpliendo varias funciones esenciales:

Nos permite construir una línea del tiempo detallada (cronología): Permite establecer una cronología de eventos o actividades realizadas en el dispositivo. Esto puede ayudar a demostrar

cuándo ocurrieron ciertos eventos, lo cual es fundamental para esclarecer hechos en una causa.

Identificar patrones de comportamiento: se pueden identificar patrones de uso del dispositivo, como la frecuencia de comunicación con ciertos contactos, los horarios habituales de actividad, o los momentos en que el dispositivo fue inusualmente activo.

Identificar violación de cadena de custodia: todo movimiento después del secuestro del dispositivo o posterior a la pericia, que no esté documentado en el formulario de la cadena de custodia, implicara una violación de la misma.

Corroborar o refutar declaraciones: pueden ser utilizadas para verificar si los eventos ocurrieron en los tiempos declarados.

Evidenciar manipulaciones: Si las marcas de tiempo presentan inconsistencias o si se detectan modificaciones, esto puede ser un indicio de que el dispositivo ha sido manipulado.

Correlacionar eventos: las marcas de tiempo permiten correlacionar diferentes eventos relacionados entre sí, por ejemplo: podemos observar en la línea de tiempo que hubo actividad en los sensores de movimiento, lo que indica que el dispositivo fue trasladado (cuando el dispositivo debería haber estado apagado). Posteriormente, se registró un evento que evidencia la manipulación del teléfono para visualizar un mensaje de WhatsApp, y este evento no estar registrado en el formulario de la cadena de custodia.

En resumen, las marcas de tiempo en una extracción de UFED son esenciales para analizar posibles violaciones de la cadena de custodia, proporcionar contexto a hechos específicos, recrear escenarios, etc.

¿Como visualizar la cronología?

Para visualizar la **cronología**, tendremos que ir al panel de navegación en la parte izquierda y seleccionar la opción "**Cronograma**".

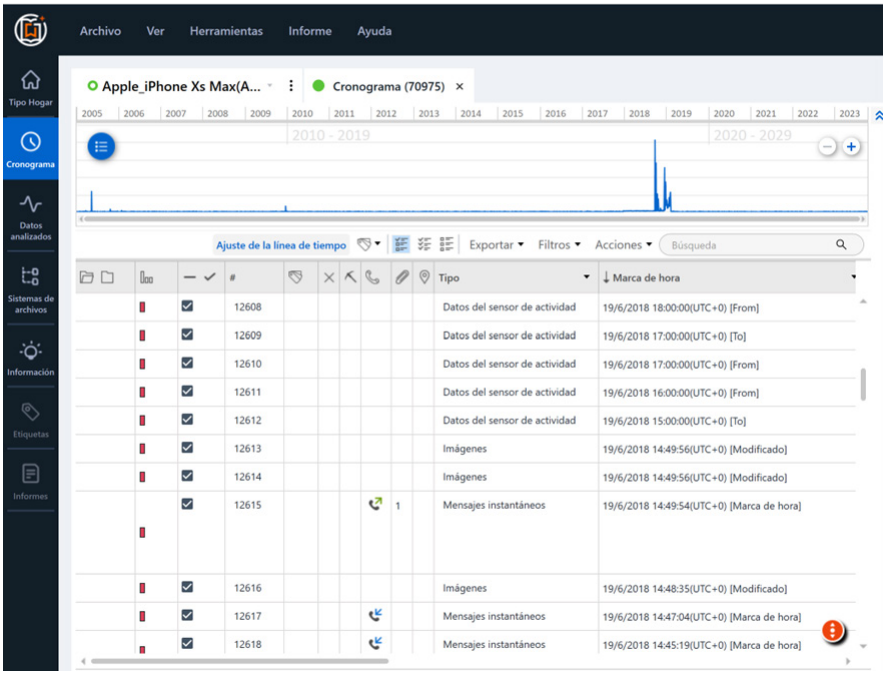


Ilustración 8. Panel. Cronograma

Capítulo V

Introducción al análisis forense de dispositivos móviles

TIPOS DE DATOS EXTRAÍBLES DE UN DISPOSITIVO MÓVIL

Datos de comunicación

Estos datos generalmente tienen contenido multimedia (imágenes, videos, etc.).

Mensajes de texto (SMS/MMS): Son los mensajes enviados y recibidos a través de la red de telefonía móvil.

Mensajería instantánea: los mensajes enviados a través de aplicaciones de chat. (WhatsApp, Telegram, etc.):

Historial de llamadas: registros de llamadas entrantes, salientes y perdidas, que incluyen números de teléfono, duración de la llamada y marcas de tiempo.

Datos de ubicación

Datos de GPS: Información sobre las ubicaciones geográficas del dispositivo obtenidas por el GPS o a través de torres de telefonía móvil y redes Wi-Fi.

Historial de ubicación: Lugares visitados por el usuario, con información detallada de fechas y horas brindados por app como Waze, Google Maps, etc.

Archivos multimedia:

Fotos y videos: imágenes y videos almacenados en la memoria del dispositivo, que pueden incluir metadatos como la ubicación, la fecha y la hora en que se capturaron.

Archivos de audio: grabaciones de voz, notas de voz, o archivos de audio descargados.

Datos de aplicaciones

Historial de navegación web: registros de los sitios web visitados, cookies y datos almacenados por los navegadores.

Marcadores web: Son las páginas web que se guardan como favorita para acceder a ellas de manera fácil y rápida.

Datos de aplicaciones sociales: información almacenada por estas apps, como mensajes, publicaciones, comentarios (Facebook, Instagram, etc.):.

Archivos temporales y Caché: archivos almacenados por las aplicaciones para un uso más eficiente o temporal.

Datos del sistema

Contactos: lista de contactos guardados en el dispositivo, que incluyen nombres, números de teléfono, correos electrónicos, etc.

Calendarios y eventos: registros de eventos programados en las aplicaciones de calendario.

Notas y recordatorios: información almacenada en las aplicaciones de notas y recordatorios

Metadatos

Metadatos de archivos: que describen el contenido informativo sobre un archivo, como la fecha de creación, modificación, la ubicación desde donde se generó o accedió a ese archivo.

Metadatos de comunicaciones: información sobre el emisor, receptor, duración y hora de las llamadas o mensajes, sin incluir el contenido del mensaje en sí.

Archivos de sistema y logs

Registros de eventos (Logs): estos son archivos que registran las actividades del sistema y de las aplicaciones, como las veces que se abrió una app o el uso de redes Wi-Fi, etc.

Archivos de configuración: son archivos de texto que contiene configuraciones utilizadas para controlar el funcionamiento de un programa o sistema, estos archivos pueden proporcionar información sobre el uso del dispositivo.

Datos eliminados u ocultos

Datos recuperables: son todos los datos eliminados que se pueden recuperar por medio de herramientas especializadas.

Particiones ocultas o encriptadas: Áreas del dispositivo que contienen información cifrada, las cuales pueden ser descifradas utilizando herramientas forenses especializadas para acceder a los datos.

PANEL "DATOS ANALIZADOS" DEL UFED

El panel "Datos analizados" en UFED Reader es una sección que permite visualizar y gestionar la información extraída de dispositivos móviles, como mensajes, llamadas, ubicaciones, archivos multi-

media, etc. En este panel, los datos están organizados en columnas que representan distintos tipos de información, como fechas, contactos, ubicaciones, etc.

Desde esta vista, el usuario puede aplicar filtros para restringir la visualización a datos específicos, facilitando el enfoque en patrones clave o eventos de interés. También permite ordenar los datos por criterios como fecha o categoría, lo que simplifica la identificación de elementos relevantes para el análisis de los hechos.

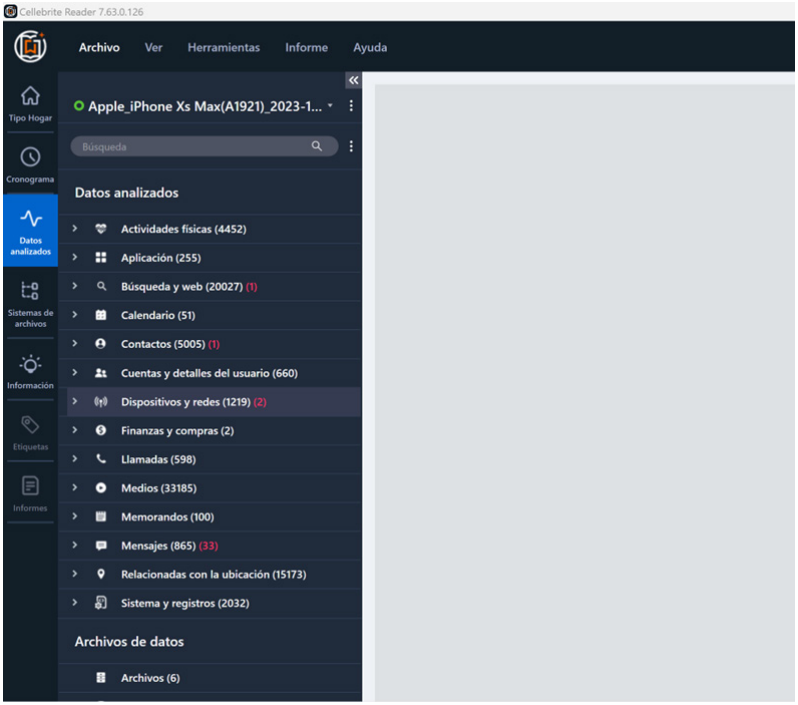


Ilustración 9. Panel "Datos Analizados"

FILTRADO DE INFORMACIÓN PARA ENFOCAR EL ANÁLISIS

En cualquier ventana de datos analizados, los resultados pueden filtrarse por columna según el tipo de información. El método

de filtrado dependerá del contenido de la variable (columna), permitiendo, por ejemplo, filtrar por fecha o por categoría, de acuerdo a los datos almacenados. Es posible filtrar por una o varias columnas de datos, lo que permite controlar tanto la información que se desea visualizar como la que se quiere excluir.

Filtrar la información es esencial para enfocarse en los datos más relevantes, y evitar la distracción que puede generar un exceso de información. Por ejemplo, si se desean analizar eventos posteriores al secuestro del teléfono, es más eficiente aplicar un filtro de fecha. De igual manera, para seguir una conversación específica, filtrar por número telefónico facilita el análisis de los chats con ese contacto.

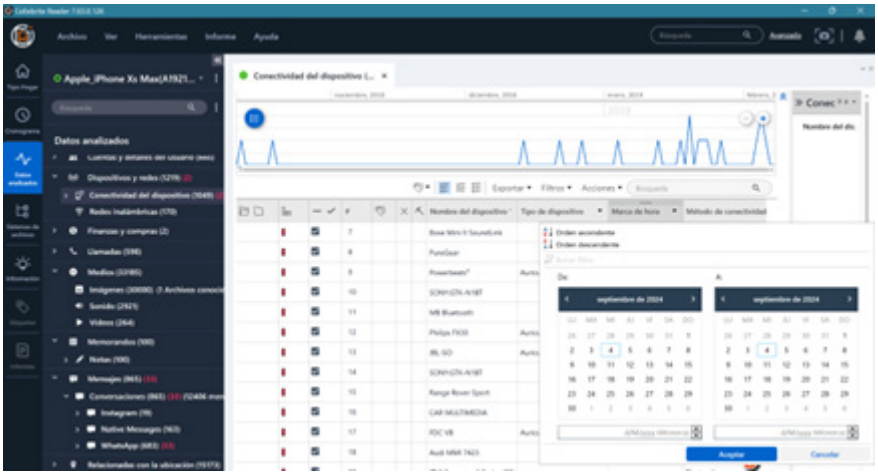


Ilustración 10. Filtro por fecha

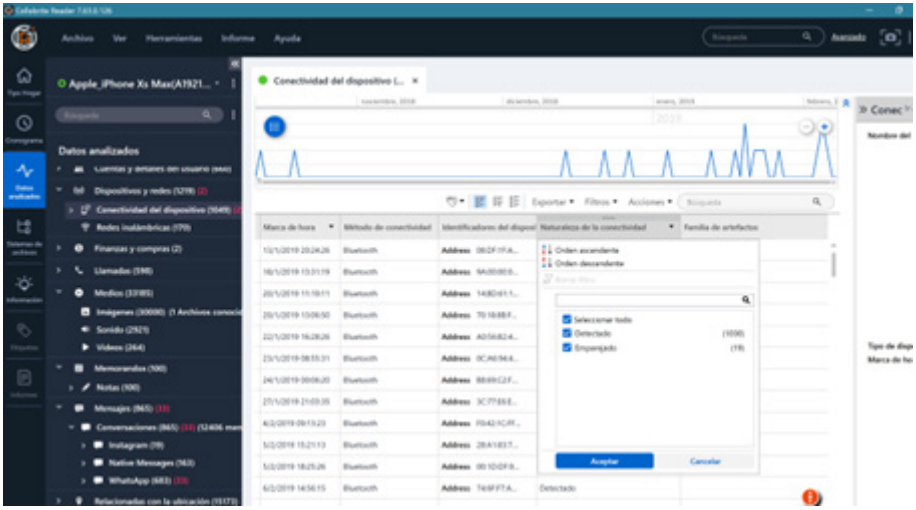


Ilustración 11. Filtro por categoría

MARCADORES

Con UFED Reader, cualquier dato relevante identificado puede marcarse para su inclusión en un informe. Para agregar elementos al informe, es necesario seleccionar la casilla de verificación junto a cada elemento de datos de la siguiente manera:

Primero, se debe deseleccionar toda la columna haciendo clic en el signo de menos, y luego seleccionar únicamente los datos de interés haciendo clic en el recuadro, si se quiere seleccionar todos los datos de nuevo se debe hacer clic en el símbolo de tilde.

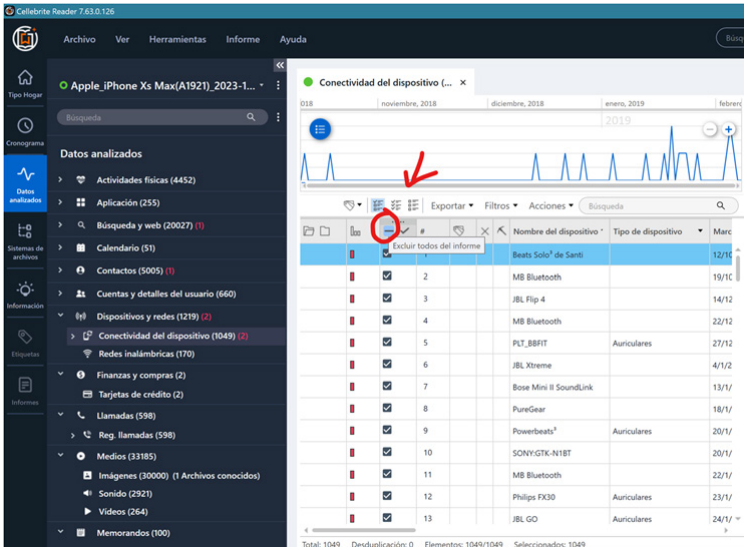


Ilustración 12. Deseleccionar datos en el UFED

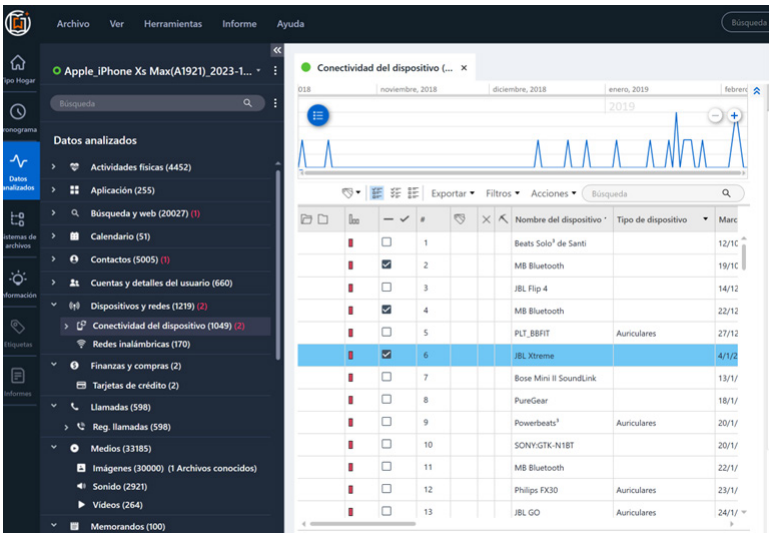


Ilustración 13. Seleccionado algunos datos

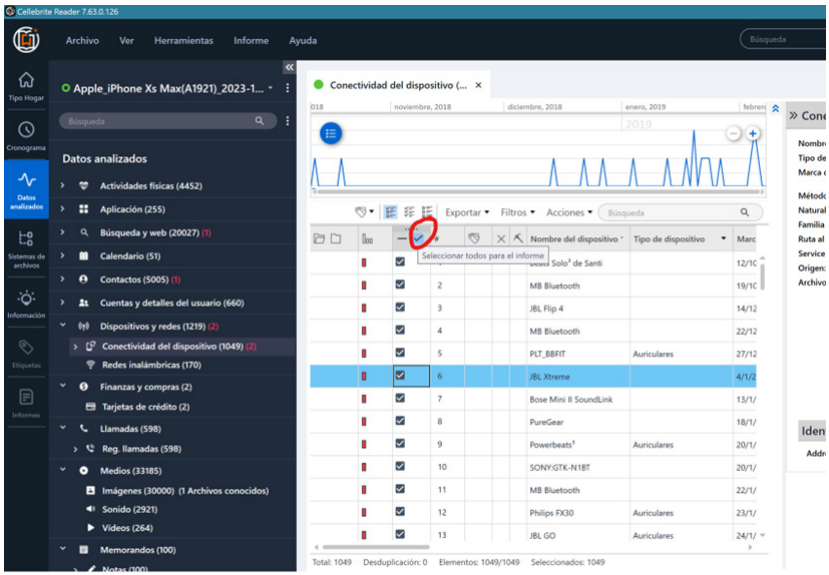


Ilustración 14. Seleccionado todos los datos

EXPORTACIÓN DE DATOS UFED

En UFED Reader, todos los datos extraídos de dispositivos móviles pueden exportarse en varios formatos, como Excel, Word, PDF, XML, entre otros. Esto permite una mayor flexibilidad en la presentación y análisis de la información, facilitando su integración en informes o su revisión en otras plataformas según las necesidades del caso. Además, la exportación en diferentes formatos asegura que los datos puedan compartirse de manera accesible. Solo se debe hacer clic en el ítem "**Exportar**" y elegir el tipo de formato.

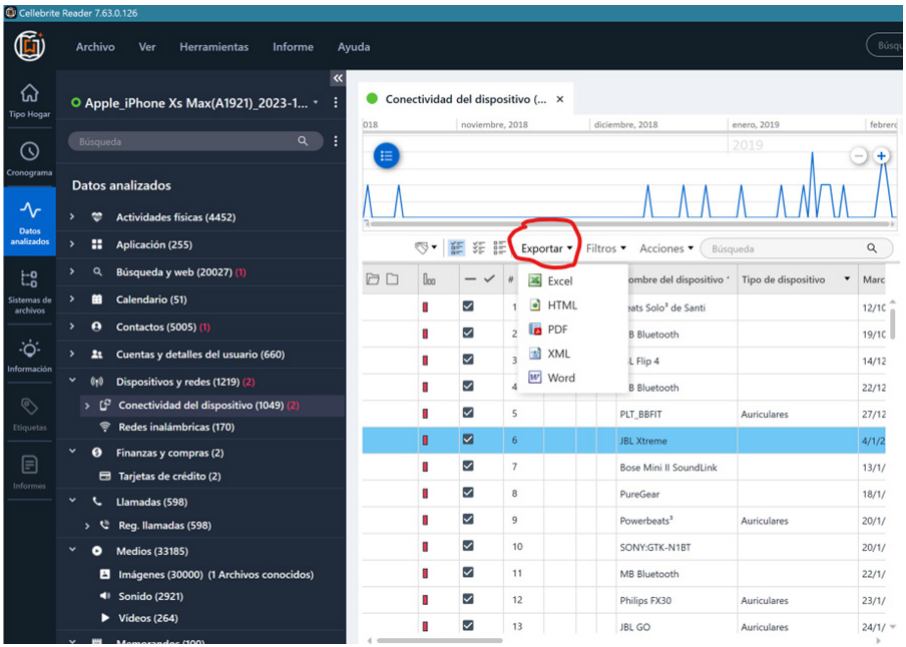


Ilustración 15. Exportación de datos

La búsqueda en UFED puede realizarse de dos maneras: **por extracción o por pestaña**. La opción de **búsqueda por extracción** realiza una búsqueda global en toda la extracción de datos. Para utilizarla, simplemente ingrese el término deseado en el cuadro de búsqueda ubicado en el encabezado que se muestra a continuación.

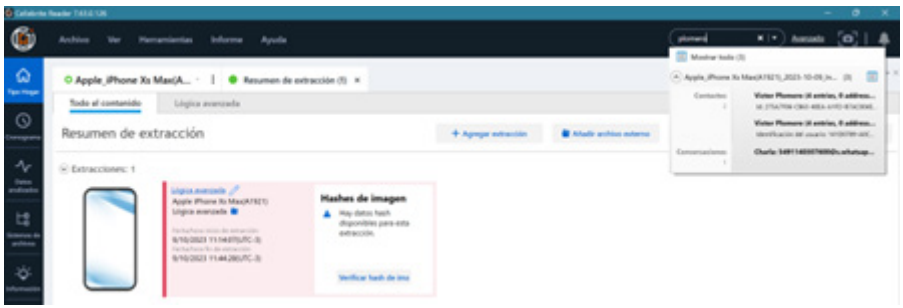


Ilustración 16. Búsqueda por extracción

La opción de **búsqueda por Pestaña** permite realizar búsquedas específicas dentro de una sección particular de los datos extraídos, enfocándose exclusivamente en esa área.

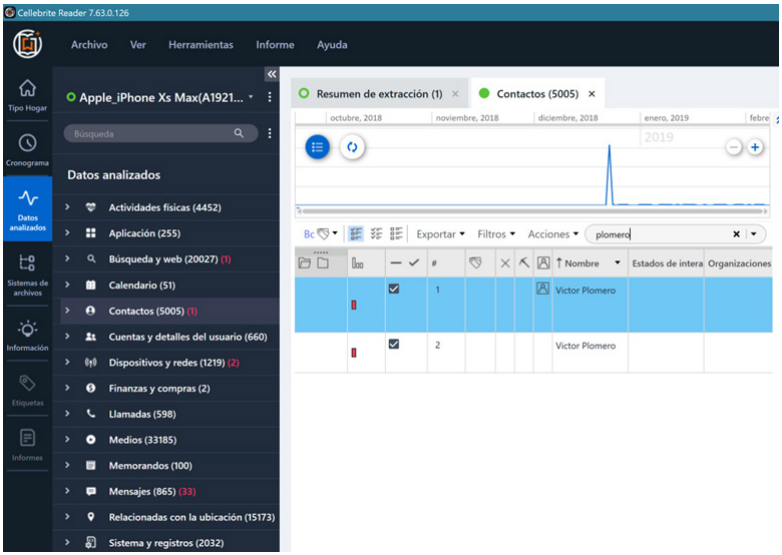


Ilustración 17. Búsqueda por pestaña.

CREAR INFORMES PERSONALIZADOS UFED

UFED Reader nos ofrece la posibilidad de generar dos tipos de informes: "**Crear informe** "y "**generar informe preliminar del dispositivo**."

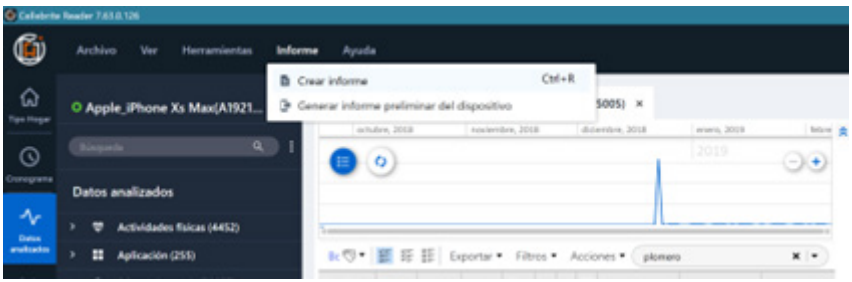


Ilustración 18. Menu Informe UFED

La opción "**Crear informe**" nos permite crear un Informe personalizado, este tipo de informe está diseñado para personalizar el contenido según las necesidades del caso, permitiendo incluir solo información específica, aplicando todos los datos de un período determinado o seleccionar cierto tipo de datos dentro de un intervalo de tiempo particular, entre otras opciones.

Al seleccionar la opción "**Crear informe**", se mostrará una pantalla en la que deberemos elegir el formato del archivo (PDF, Excel, Word, etc.) y especificar la ubicación para guardarlo. Por defecto, el informe se guarda en la carpeta "**My Reports**" dentro de "**Mis Documentos**".

Los demás campos se autocompletarán automáticamente con la información de la extracción, por lo que solo será necesario hacer clic en "**Siguiente**" para avanzar a la siguiente pantalla.

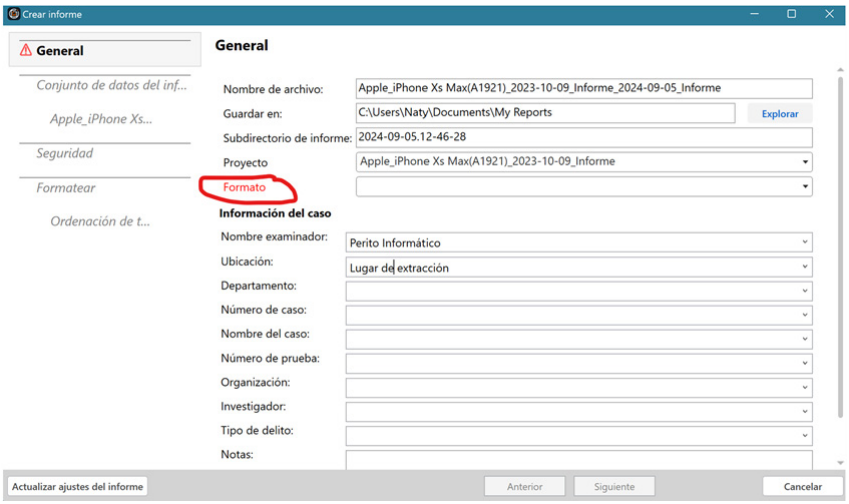


Ilustración 19. Primera pantalla de "Crear informes"

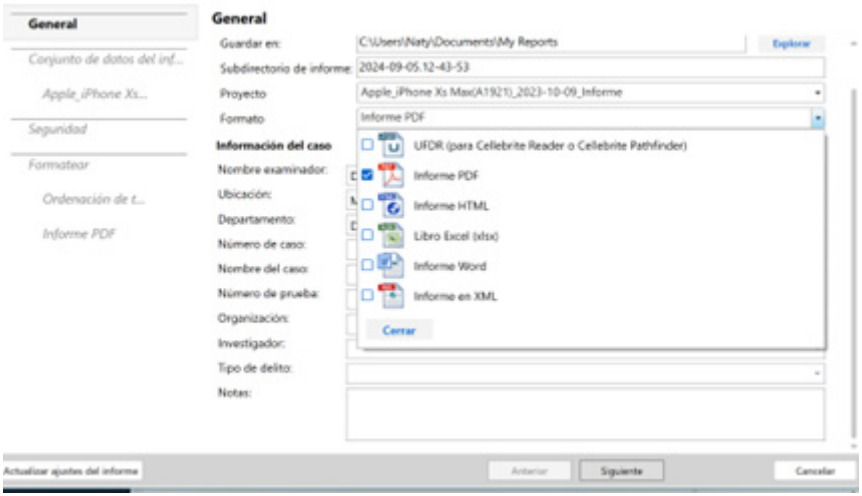


Ilustración 20. Tipo de Formatos para Exportar.

En la segunda pantalla de "**Crear informe**", se nos presentarán las opciones de filtrado. Aquí podremos gestionar los datos por fecha, tipo de información o ambas opciones. Si se elige el filtro por fecha, es importante hacer clic en "**Aplicar**" para que los cambios se guarden. Una vez seleccionados todos los filtros, haremos clic en "**Finalizar**" para generar el informe.

Ilustración 21. Pantalla de Filtros para generar informe personalizado

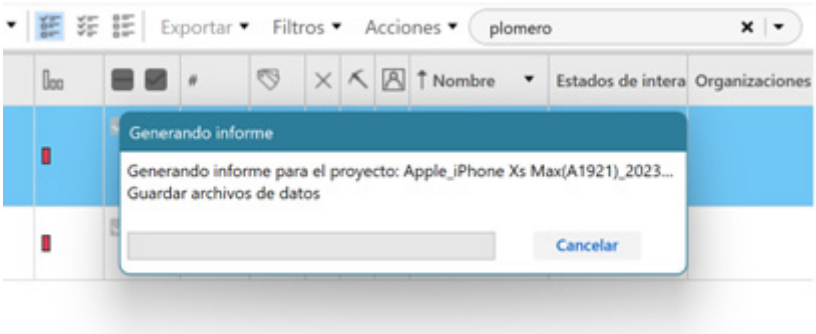
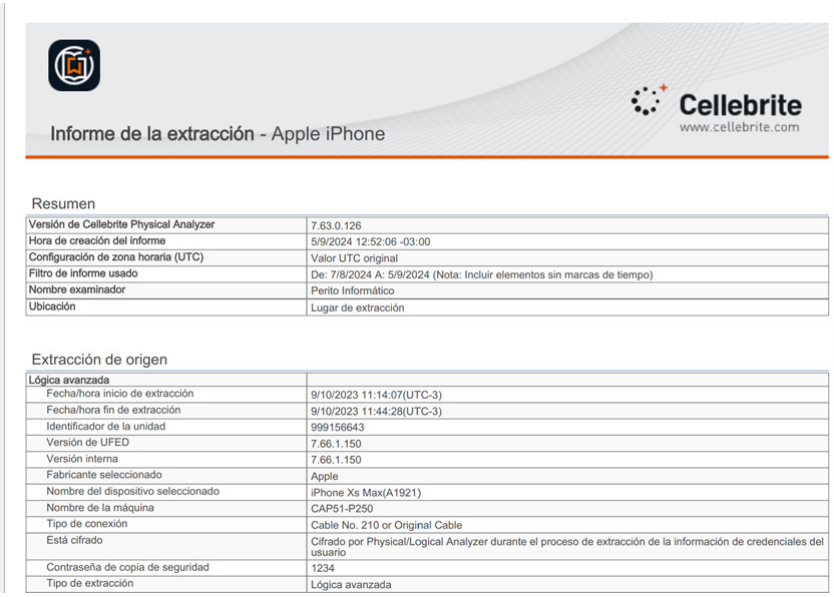


Ilustración 22. Generar informe



Informe de la extracción - Apple iPhone

Cellebrite
www.cellebrite.com

Resumen

Versión de Cellebrite Physical Analyzer	7.63.0.126
Hora de creación del informe	5/9/2024 12:52:06 -03:00
Configuración de zona horaria (UTC)	Valor UTC original
Filtro de informe usado	De: 7/8/2024 A: 5/9/2024 (Nota: Incluir elementos sin marcas de tiempo)
Nombre examinador	Perito Informático
Ubicación	Lugar de extracción

Extracción de origen

Lógica avanzada	
Fecha/hora inicio de extracción	9/10/2023 11:14:07(UTC-3)
Fecha/hora fin de extracción	9/10/2023 11:44:28(UTC-3)
Identificador de la unidad	999156643
Versión de UFED	7.66.1.150
Versión interna	7.66.1.150
Fabricante seleccionado	Apple
Nombre del dispositivo seleccionado	iPhone Xs Max(A1921)
Nombre de la máquina	CAP51-P250
Tipo de conexión	Cable No. 210 or Original Cable
Está cifrado	Cifrado por Physical/Logical Analyzer durante el proceso de extracción de la información de credenciales del usuario
Contraseña de copia de seguridad	1234
Tipo de extracción	Lógica avanzada

Ilustración 23. Portada del informe generado (formato PDF)

La opción "**Crear informe preliminar del dispositivo**" genera un informe predeterminado que incluye todos los datos presentes en la extracción. Este informe se guarda en la carpeta "My Reports" dentro de "Mis Documentos.

Anexo

Protocolo para la evidencia digital

El Protocolo para la identificación, recolección, preservación, procesamiento y presentación de la evidencia digital fue elaborado por el Ministerio de Seguridad de Argentina en conjunto con las fuerzas federales policiales y el Ministerio Público Fiscal de la Nación.

Es de aplicación obligatoria para todo el personal de la Policía Federal Argentina, Gendarmería Nacional Argentina, Policía de Seguridad Aeroportuaria y Prefectura Naval Argentina en todo el territorio nacional.

Se basa en la norma IRAM-ISO-IEC 27037:2022, que establece los procedimientos para garantizar la manipulación adecuada de la evidencia digital, protegiendo su integridad y asegurando su admisibilidad.

Es de suma importancia, en el marco de la defensa de asistidos, conocer y entender este protocolo, ya que cualquier falla en la correcta aplicación de los procedimientos establecidos puede comprometer la validez de la evidencia digital presentada en juicio.

Conocer estos procedimientos permite a la defensa identificar errores en la cadena de custodia o en la recolección de datos, lo cual puede derivar en la impugnación de la evidencia. Además, cuestionar la admisibilidad de la evidencia en caso de que no se haya seguido el protocolo podría resultar en que sea desestimada como prueba.

Accedé al texto completo [aquí].

Glosario

Autenticidad: atributo de la evidencia que demuestra que es genuina y que representa fielmente los datos originales sin haber sido manipulada o alterada.

Hash: es un código alfanumérico generado a partir de un conjunto de datos, que se utiliza para identificar o resumir ese conjunto. Los hashes se obtienen mediante una función hash, que opera sobre la información de entrada y produce un valor único.

Los hashes tienen varias características que los hacen útiles para diversas aplicaciones:

- Univocidad: cada conjunto de datos tiene un hash único, y es muy improbable que dos conjuntos de datos diferentes generen el mismo hash.

- Unidireccionalidad: es extremadamente difícil determinar los datos de entrada a partir de un hash, lo que dificulta descifrar la información original.

- Determinismo: una función hash determinista siempre devuelve el mismo hash para una cadena de entrada específica.

Integridad: cualidad de la evidencia digital que asegura que los datos no han sido alterados desde el momento de su recolección. La integridad se verifica mediante técnicas como el hashing.

Jaulas de Faraday: es un contenedor recubierto por materiales conductores de electricidad (como planchas o mallas metálicas) que bloquea las ondas electromagnéticas. Se usa para aislar dispositivos de señales externas, evitando tanto la entrada como la salida de señales. Esto es útil para proteger la información y evitar que dispositivos electrónicos sean manipulados a distancia.

Memoria RAM o Random Access Memory: es un tipo de almacenamiento temporal que permite a los dispositivos electrónicos acceder a la información de manera rápida y aleatoria. Almacena los datos que un programa necesita mientras se ejecuta, lo que facilita un rendimiento eficiente.

Memoria Caché: es un tipo de memoria temporal que almacena datos de forma rápida, permitiendo un acceso más eficiente. Se encuentra ubicada entre la unidad central de procesamiento (CPU) y la memoria de acceso aleatorio (RAM).

Metadatos: datos que describen otros datos, proporcionando información adicional sobre un archivo o documento, como su fecha de creación, autor, ubicación y modificaciones.

Paginación: técnica de administración de memoria que permite al sistema operativo mover datos entre la memoria RAM y el disco duro. Los archivos de paginación pueden contener fragmentos de datos eliminados.

Tarjeta SIM (Subscriber Identity Module): es un chip que se inserta en dispositivos móviles para almacenar de manera segura la información del suscriptor de una red móvil. Esta tarjeta contiene un número de identificación único (IMSI) que permite a los operadores de telecomunicaciones identificar al usuario, gestionar su acceso a la red, y habilitar servicios como llamadas, mensajes de texto y datos

móviles. Además, la tarjeta SIM puede almacenar contactos y mensajes de texto, y facilita la portabilidad del número al cambiar de dispositivo.

UFED (Universal Forensic Extraction Device): dispositivo y software especializado en extraer datos de dispositivos móviles para análisis forense. Útil para obtener comunicaciones, historial de llamadas y otros datos de interés.

Bibliografía

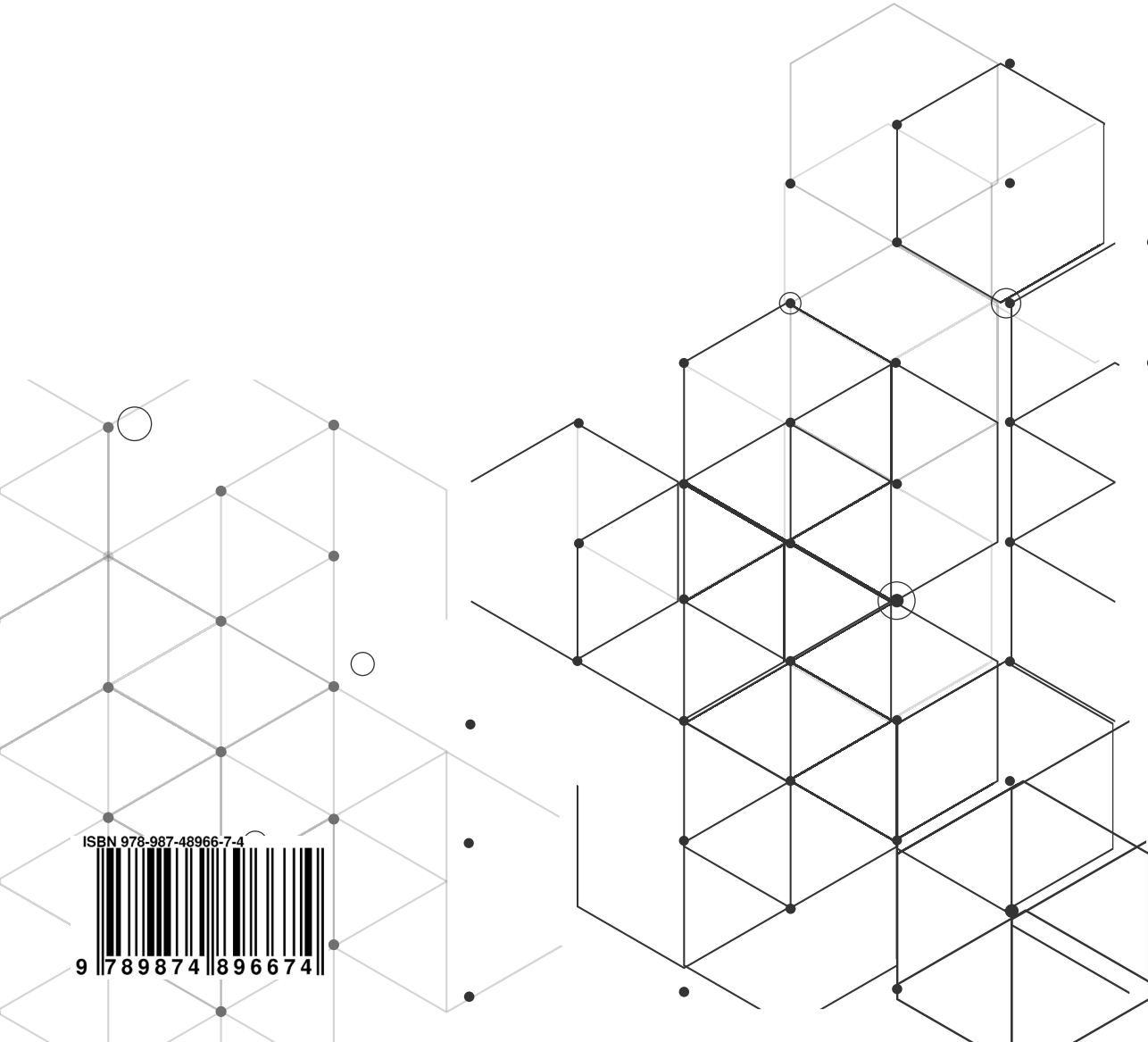
Oleg Afonin, Vladimir Katalov.(2016). **Mobile Forensics: Advanced Investigative Strategies**. Editorial Packt Publishing.

Eoghan Casey. **Digital Evidence and Computer Crime** (2011). Editorial Elsevier.

Norma IRAM-ISO-IEC 27037:2024 (2024). IRAM

Norma IRAM 36100:2024 (2024). IRAM.

MPD
Argentina



ISBN 978-987-48966-7-4