ANÁLISIS FORENSE DIGITAL EN DISPOSITIVOS MÓVILES

Arnulfo Alemán Ariza
Peritos informáticos Panamá, República de Panamá
arnulfo.aleman@gmail.com
https://orcid.org/0009-0009-7925-978X

DOI: 10.37594/cathedra.n21.1419

Fecha de recepción:10/04/2024 Fecha de revisión:18/04/2024 Fecha de aceptación: 30/04/2024

RESUMEN

El análisis forense digital en dispositivos móviles presenta muchos retos ligados al avance tecnológico de los dispositivos que son utilizados como fuente de evidencia y por las connotaciones legales referente a la privacidad. Esta especialidad debe hacer frente a una serie de cambios tecnológicos los cuales el analista forense informático debe estar a la vanguardia para poder realizar extracciones exitosas de la información requerida para el caso en el cual se requiera. Debe estar anuente en todo momento de las normas que rigen el manejo de evidencia digital, del debido proceso al momento de realizar extracciones en dispositivos móviles y de garantizar la integridad de la información extraída. Es importante destacar que la actualización de los profesionales en el área forense en dispositivos es de suma importancia para poder hacerle frente a los retos de esta especialidad.

Palabras clave: Informática Forense, Análisis Forense Digital, Dispositivo Móvil, Copia Forense, Sistemas Operativos Móviles, Extracción Android, Extracción iOS.

DIGITAL FORENSIC ANALYSIS ON MOBILE DEVICES

ABSTRACT

Digital forensic analysis on mobile devices presents many challenges linked to the technological advance of the devices that are used as a source of evidence and the legal connotations regarding privacy. This specialty must face a series of technological changes of which the computer forensic analyst must be at the forefront in order to successfully extract the information required for the case in which it is required. You must be aware at all times of the rules that govern the handling of digital evidence, of due process when performing extractions on mobile devices and of guaranteeing the integrity of the extracted information. It is important to highlight that updating professionals in the device forensic area is of utmost importance to be able to face the challenges of this specialty.

Keywords: Computer Forensics, Digital Forensics, Mobile Device, Forensic Copy, Mobile

Operating Systems, Android Extraction, iOS Extraction.

INTRODUCCIÓN

El análisis forense digital en dispositivos móviles experimenta un crecimiento exponencial en la actualidad debido a la naturaleza ubicua de los dispositivos móviles, que se han convertido en extensiones personales del usuario, almacenando una vasta cantidad de información personal. Esta información abarca desde contactos, conversaciones, multimedia, datos financieros, historiales de navegación, hasta estadísticas de uso del dispositivo, entre otros aspectos. Esta riqueza de datos permite la identificación inequívoca de los usuarios basada en patrones de comportamiento.

Es primordial que esta disciplina cuente con normativas y procedimientos que salvaguarden la ética, privacidad y seguridad de la información recolectada a través de cualquier método de extracción. Además, se deben establecer metodologías de extracción que aseguren la integridad de los datos recuperados.

El análisis forense en dispositivos móviles enfrenta diversos desafíos, tanto a nivel de hardware como de software. Entre estos desafíos se encuentran la diversidad de marcas y modelos de dispositivos, sistemas de archivos, actualizaciones de software, tipos de procesadores, versiones de sistemas operativos y el estado físico del dispositivo. La presencia de tecnologías de encriptación también añade complejidad a la extracción de datos, al igual que las regulaciones legales relacionadas con la privacidad.

Esta especialidad, derivada de la informática forense, tiene como objetivo obtener datos de dispositivos móviles de manera íntegra y sin alteraciones, para su uso como evidencia en procedimientos legales. Esto se logra mediante el uso de herramientas especializadas que permiten realizar extracciones lógicas o físicas en dispositivos con sistemas operativos Android o iOS, así como realizar análisis detallados de los datos extraídos.

El analista forense informático desempeña un papel fundamental en esta disciplina, ya que debe estar familiarizado con las metodologías y buenas prácticas tanto técnicas como legales en el proceso de extracción. El desarrollo continuo de técnicas de extracción y herramientas específicas para el análisis forense en dispositivos móviles puede mejorar significativamente la eficiencia en la recuperación de evidencia, cumpliendo con las normativas legales y respetando la privacidad de los usuarios.

METODOLOGIA

Para abordar el análisis forense digital en dispositivos móviles y los retos que experimentan los analistas forenses, se adoptó un enfoque metodológico mixto el cual está desarrollado en base a conceptos, experiencias, revisión bibliográfica, y estudio de herramientas forenses pagas y gratuitas.

DESARROLLO

Antes de abordar el análisis forense digital en dispositivos móviles, es importante comprender el concepto general del análisis forense digital. Este proceso implica la identificación, adquisición, preservación, análisis y presentación de resultados relacionados con evidencia digital, aplicable a cualquier tipo de incidente que involucre elementos digitales, como computadoras, laptops, dispositivos móviles, comunicaciones y redes.

Fases del análisis forense digital:

• ***Identificación:*** En esta fase, se identifican las posibles fuentes de evidencia, que pueden estar presentes en dispositivos digitales como discos duros, laptops, celulares, servidores, así como en dispositivos en tránsito como routers y switches. La delimitación de esta fase está determinada por la naturaleza del incidente que se está investigando.

• ***Adquisición:*** Una vez identificadas las fuentes de evidencia, se procede a adquirir la evidencia digital. Este proceso es crucial y requiere experiencia y cumplimiento de lineamientos específicos para garantizar la integridad de la evidencia. Es importante tener en cuenta la volatilidad de la evidencia digital, por lo que se deben seguir protocolos rigurosos para su recolección y manejo. El uso de herramientas forenses puede facilitar este proceso, aunque no garantiza la prevención de contaminación o pérdida de evidencia.

• ***Preservación:*** En esta fase, se busca mantener la integridad a lo largo del tiempo de la evidencia recolectada, ya sea en forma granular o mediante copias forenses totales. Se utilizan algoritmos de comprobación como el hash para generar una cadena de longitud fija que sirva como referencia comparativa entre la evidencia original y la recolectada, garantizando su inalterabilidad. Se inician los protocolos de cadena de custodia para asegurar la trazabilidad de la evidencia durante análisis posteriores.

• ***Análisis:*** En esta etapa, la evidencia recolectada se procesa mediante herramientas forenses, indexando su contenido y aplicando filtros o técnicas de descifrado según sea necesario para extraer datos relevantes para la investigación. Se crean líneas de tiempo para analizar los eventos de manera ordenada.

• ***Informes:*** En esta fase se documentan los hallazgos obtenidos durante el análisis de la evidencia. La estructura del informe puede variar dependiendo del contexto legal y/o corporativo en el que se desarrolle la investigación. Por ejemplo, en Panamá, el informe pericial informático

debe seguir la estructura establecida en el artículo 411 del código procesal penal de la república de Panamá para casos penales. En entornos corporativos, el informe puede ser más técnico y dirigido a la alta gerencia, ofreciendo conclusiones y recomendaciones para prevenir futuros incidentes.

Es importante destacar que para cualquier dispositivo tecnológico que contenga datos digitales relevantes para un escenario legal, civil, o administrativo, es necesario seguir las cinco fases del análisis forense digital para garantizar la integridad y validez de la evidencia.

Para cada uno de los casos y dependiendo del dispositivo que contenga evidencia potencial existen diversas herramientas las cuales el Analista Forense podrá utilizar según el caso, todas las herramientas no tienen el mismo propósito, hay especializadas en la recuperación de información de discos, extracción de correos electrónicos, captura de trafico de red, extracción de contenido de dispositivos móviles, contenido en la nube, en fin, hay un abanico de herramientas para cada caso.

Herramientas Forenses para análisis de dispositivos móviles de pago Vs Gratuitas

En el ámbito del análisis forense digital, se ha suscitado un debate en torno a la utilidad y valoración de herramientas tanto gratuitas como de pago. Nuestra experiencia ha demostrado que muchas herramientas comerciales se basan en tecnologías gratuitas o de código abierto, que han sido mejoradas y optimizadas continuamente por empresas desarrolladoras. Al evaluar la elección entre herramientas comerciales y de código abierto, es crucial considerar el factor tiempo, especialmente durante las fases de adquisición y análisis, donde se utilizan herramientas forenses. Si bien las herramientas gratuitas pueden requerir procesos más prolongados y presentar ciertas limitaciones, las herramientas comerciales tienden a simplificar y acelerar estas etapas. Es importante destacar que, más allá de la herramienta utilizada, la habilidad y destreza del analista son fundamentales. Incluso la mejor herramienta carecerá de utilidad si el analista no posee un sólido entendimiento de los principios del análisis forense digital.

Algunas herramientas forenses pagas utilizadas más comúnmente en el área forense informática tenemos:

Fundada en 1999, Cellebrite es una empresa globalmente reconocida por sus avances tecnológicos en la industria móvil, con operaciones establecidas en Estados Unidos, Alemania, Singapur y Brasil.

Como líder mundial y autoridad en tecnología de datos móviles, Cellebrite estableció su división forense móvil en 2007, introduciendo una nueva línea de productos dirigidos al sector de la aplicación

de la ley. Utilizando métodos de extracción avanzados y técnicas de análisis, el Dispositivo de Extracción Forense Universal (UFED) de Cellebrite es capaz de extraer y analizar datos de una amplia gama de dispositivos móviles, que incluyen teléfonos tradicionales, smartphones y dispositivos GPS.

El UFED de Cellebrite es la herramienta preferida por miles de especialistas forenses en agencias de aplicación de la ley, militares, de inteligencia, seguridad y gobiernos en más de 60 países.

Cellebrite es una filial de propiedad total de Sun Corporation, una compañía japonesa que cotiza en bolsa (6736/JQ) http://www.cellebrite.com sales@cellebrite.com [2]

Oxygen Forensic® Detective es un software forense para la extracción y análisis de datos de teléfonos móviles, teléfonos [1] inteligentes y tablets.

Usando protocolos propietarios avanzados, use Oxygen Forensic Detective para extraer muchos más datos que generalmente contiene el dispositivo y garantiza un funcionamiento de footprint, sin dejar rastros y sin hacer modificaciones en el contenido del dispositivo.

El software se distribuye a la policía, los organismos gubernamentales, militares, investigadores privados y otros especialistas forenses. [3]

MobileEdit Forensic es una solución todo en uno para la extracción de datos de teléfonos smartwatches y nubes.

Utiliza tanto la adquisición de datos físicos como lógicos, realiza un excelente análisis de aplicaciones, recuperación de datos borrados, soporta una amplia gama de dispositivos, informes precisos, extracciones concurrentes e interfaz fácil de utilizar. Con un nuevo enfoque, MobileEdit Forensic es mucho más fuerte en bypass de seguridad que nunca antes.

MobileEdit Forensic ofrece la máxima funcionalidad a una fracción del precio de otras herramientas. Se puede utilizar como la única herramienta en un laboratorio o como complemento de otras herramientas. [4]

Belkasoft Evidence Center X (“ Belkasoft X “) es una muy buena herramienta de investigación forense digital todo en uno que permite al investigador agregar

fácilmente datos de múltiples fuentes, incluidos dispositivos informáticos, incluida la adquisición de RAM, teléfonos móviles, almacenamiento en la nube y análisis forense existentes. imágenes, o incluso simplemente una carpeta de datos. La herramienta de software también facilita la revisión y análisis de los datos procesados y facilita la tarea de gestionar varios casos simultáneamente y reportar los mismos. [5]

De uso gratuito:

Avilla Forensics es una herramienta imprescindible para los usuarios de Android, que permite realizar copias de seguridad y analizar dispositivos o descifrar datos de WhatsApp y muchas funciones adicionales que ayudan a los profesionales en Informática Forense, a obtener evidencias digitales completas.

Avilla Forensics se ubica en el primer lugar del premio internacional Forensics 4Cast en la categoría herramienta no comercial. Anuncio realizado en el evento por parte del Instituto SANS. [3]

El análisis forense digital en dispositivos móviles constituye una rama especializada de la informática forense, centrada en la investigación de dispositivos móviles. En este campo, se destacan dos principales sistemas operativos: Android, desarrollado por Google, y iOS, el sistema operativo de Apple utilizado en los dispositivos iPhone. Para comprender mejor el contexto de este análisis, es relevante explorar la historia detrás de estos sistemas operativos.

La historia de Android se remonta a alrededor del año 2003, aproximadamente cuatro años antes del lanzamiento del primer iPhone y su sistema operativo iOS por parte de Apple. Inicialmente, los fundadores de Android tenían como objetivo desarrollar sistemas operativos para cámaras fotográficas, pero luego cambiaron su enfoque hacia los dispositivos móviles. En 2005, Google adquirió Android y sus fundadores optaron por utilizar Linux como base para el sistema operativo. El lanzamiento del iPhone en 2007 marcó un hito en la historia de la computación móvil.

En septiembre de 2008, el primer teléfono Android, conocido como T-Mobile G1 o HTC Dream, fue lanzado en el mercado estadounidense. Desde entonces, los dispositivos Android han ganado una considerable popularidad, atribuible a varios factores, entre los cuales se incluyen:

Su presencia en la mayoría de los dispositivos móviles a nivel mundial su alta flexibilidad en términos de personalización y configuración. El análisis forense digital en dispositivos móviles constituye una rama especializada de la informática forense, centrada en la investigación de dispositivos móviles. En este campo, se destacan dos principales sistemas operativos: Android, desarrollado por Google, y iOS, el sistema operativo de Apple utilizado en los dispositivos iPhone. Para comprender mejor el contexto de este análisis, es relevante explorar la historia detrás de estos sistemas operativos.

La historia de Android se remonta a alrededor del año 2003, aproximadamente cuatro años antes del lanzamiento del primer iPhone y su sistema operativo iOS por parte de Apple. Inicialmente, los fundadores de Android tenían como objetivo desarrollar sistemas operativos para cámaras fotográficas, pero luego cambiaron su enfoque hacia los dispositivos móviles. En 2005, Google adquirió Android y sus fundadores optaron por utilizar Linux como base para el sistema operativo. El lanzamiento del iPhone en 2007 marcó un hito en la historia de la computación móvil.

En septiembre de 2008, el primer teléfono Android, conocido como T-Mobile G1 o HTC Dream, fue lanzado en el mercado estadounidense. Desde entonces, los dispositivos Android han ganado una considerable popularidad, atribuible a varios factores, entre los cuales se incluyen:

- Su presencia en la mayoría de los dispositivos móviles a nivel mundial.
- Su alta flexibilidad en términos de personalización y configuración.
- Posee una alta taza de actualización del sistema, operativo.
- Permite la instalación de fuente de terceros sin muchas restricciones.
- Integración con servicios de Google.

Dispositivos iOS

El sistema operativo iOS es específicamente diseñado para ejecutarse en dispositivos fabricados por Apple, incluyendo iPad, iPod y iPhone. Este sistema operativo tiene sus raíces en sistemas operativos anteriores desarrollados por Apple, los cuales también fueron utilizados en las computadoras MAC y dispositivos portátiles. A continuación se presenta un cuadro que detalla los lanzamientos anuales de las distintas versiones de iPhone.

Año de Lanzamiento	Versión de iPhone
2007	iPhone G2
2008	iPhone 3G
2010	iPhone 4
2011	iPhone 4s
2012	iPhone 5
2013	Iphone5c y iPhone 5s
2014	iPhone 6 u iPhone 6 plus
2015	iPhone 6s y iPhone 6s plus
2016	iPhone 7 y iPhone 7 Plus
2017	iPhone 8 y iPhone 8 Plus
2018	iPhone Xs, Xs Max
2019	iPhone 11
2020	iPhone Pro, Pro-Max
2021	iPhone Pro, Pro-Max
2022	iPhone Pro, Pro-Max
2023	iPhone 15 Pro, Pro-Max

Cuadro 1. Lanzamiento de versiones de iPhone por año. Fuente [6]

Algunas de las bondades que podemos mencionar del sistema iOS tenemos:

- Interfaz de usuario limpia e intuitiva.
- iOS tiene un fuerte desarrollo en la seguridad tanto del software y el hardware.
- Las aplicaciones desarrolladas para IOS pasan un riguroso proceso de filtro.

Al momento de realizar una extracción para un análisis de dispositivo móvil vale la pena abordar ciertos criterios que se deben de tomar en cuenta:

La privacidad del contenido del dispositivo móvil

El acceso a la información almacenada en un dispositivo móvil requiere un consentimiento explícito por parte de su propietario. En ciertas circunstancias de incautación, como aquellas en las que intervienen fuerzas del orden público, como la policía, se necesita una orden judicial para realizar dicha acción legalmente. Sin embargo, en nuestro contexto, nos referimos a un enfoque consensuado, en el cual el propietario del dispositivo otorga su consentimiento expreso para llevar a cabo la extracción de datos, los cuales se utilizarán como evidencia en un proceso determinado.

La proporcionalidad de Información expuesta

La correcta selección del contenido solicitado representa un aspecto fundamental al realizar

una solicitud de extracción de datos de un dispositivo móvil. Por ejemplo, al requerir un video específico capturado con un Samsung Galaxy Note 9 en una fecha determinada, es esencial extraer exclusivamente el contenido multimedia relevante y aplicar filtros apropiados para identificar el video en cuestión. Optar por una extracción integral del dispositivo y luego seleccionar el contenido multimedia puede resultar en exceder los límites del proceso, lo que podría llevar a la obtención de información no pertinente para el análisis requerido y a posibles violaciones de la privacidad en relación con la información restante.

La custodia del contenido extraído

Cuando se realiza una extracción, tanto total como parcial, del contenido de un dispositivo móvil, es fundamental priorizar la seguridad de la información extraída en todo momento. En el entorno del laboratorio forense, se debe establecer una trazabilidad clara que registre quién, cuándo y por qué accede a dicha información. Además, los dispositivos de almacenamiento utilizados deben cumplir con requisitos mínimos para mitigar el riesgo de filtración o eliminación accidental o intencionada del contenido. En este sentido, la adopción de discos encriptados representa una medida eficaz para reducir el riesgo en caso de robo o pérdida de los equipos utilizados en el proceso forense

Documentación en los procesos de extracción

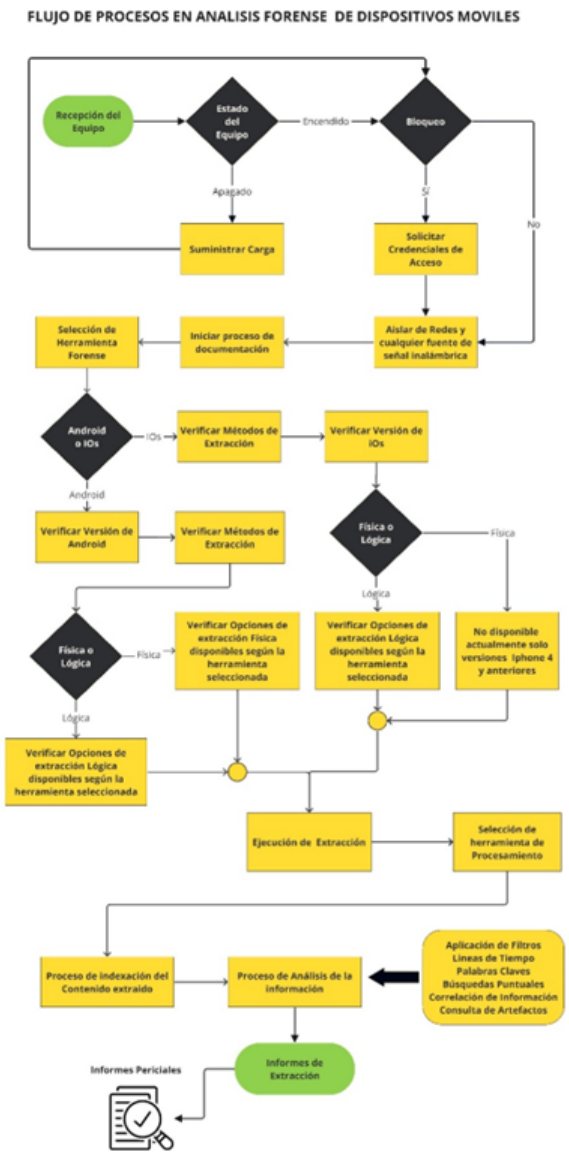
Es imprescindible mantener una documentación exhaustiva de naturaleza administrativa y procesal al operar con dispositivos móviles, que, junto con el consentimiento explícito, fortalezca la gestión del proceso. Esta documentación incluye registros relacionados con la recepción del dispositivo en el laboratorio, tales como la marca, modelo, IMEI, IMSI, número de registro, capacidad, color, estado físico, información del propietario, operador telefónico, fotografías, propósito de la extracción, solicitante, hora, fecha y lugar de recepción.

¿Por qué este proceso es crucial para los dispositivos móviles y no para otros equipos? La respuesta radica en que los dispositivos móviles contienen una cantidad significativa de información personal que identifica al propietario. Desde mensajes privados hasta historiales de navegación, esta información es altamente sensible y reveladora.

En cuanto al análisis forense digital de dispositivos móviles, es uno de los servicios más solicitados en el ámbito de la informática forense. Los dispositivos móviles se han convertido en una fuente rica de información que abarca desde registros de llamadas hasta datos de aplicaciones de terceros, tarjetas de crédito y contraseñas.

El análisis forense digital de dispositivos móviles se inicia cuando se identifica un dispositivo como fuente de evidencia en un caso o incidente legal. Esta evidencia puede ser requerida en diversos contextos legales, como procesos penales, civiles, laborales, familiares, administrativos o corporativos. Los datos extraídos de los dispositivos se categorizan como "artefactos" y pueden incluir una amplia gama de información, desde registros de comunicaciones hasta datos de geolocalización y configuraciones del dispositivo.

La solicitud de análisis forense de un dispositivo móvil puede provenir de una orden judicial, el equipo legal de una parte en disputa, los departamentos de cumplimiento de una empresa, entre otros. Es fundamental que esta solicitud esté debidamente registrada y acompañada de la documentación pertinente sobre el dispositivo en cuestión.



El proceso de análisis forense de un dispositivo móvil, desde la recepción hasta la generación de informes, implica una serie de pasos meticulosos. La herramienta forense Cellebrite es ampliamente utilizada en este proceso y ofrece diversos tipos de extracciones para sistemas iOS y Android, lo que facilita el análisis exhaustivo de los datos contenidos en los dispositivos móviles. Es imprescindible mantener una documentación exhaustiva de naturaleza administrativa y procesal al operar con dispositivos móviles, que, junto con el consentimiento explícito, fortalezca la gestión del proceso. Esta documentación incluye registros relacionados con la recepción del dispositivo en el laboratorio, tales como la marca, modelo, IMEI, IMSI, número de registro, capacidad, color, estado físico, información del propietario, operador telefónico, fotografías, propósito de la extracción, solicitante, hora, fecha y lugar de recepción.

¿Por qué este proceso es crucial para los dispositivos móviles y no para otros equipos? La respuesta radica en que los dispositivos móviles contienen una cantidad significativa de información personal que identifica al propietario. Desde mensajes privados hasta historiales de navegación, esta información es altamente sensible y reveladora.

En cuanto al análisis forense digital de dispositivos móviles, es uno de los servicios más solicitados en el ámbito de la informática forense. Los dispositivos móviles se han convertido en una fuente rica de información que abarca desde registros de llamadas hasta datos de aplicaciones de terceros, tarjetas de crédito y contraseñas.

El análisis forense digital de dispositivos móviles se inicia cuando se identifica un dispositivo como fuente de evidencia en un caso o incidente legal. Esta evidencia puede ser requerida en diversos contextos legales, como procesos penales, civiles, laborales, familiares, administrativos o corporativos. Los datos extraídos de los dispositivos se categorizan como "artefactos" y pueden incluir una amplia gama de información, desde registros de comunicaciones hasta datos de geolocalización y configuraciones del dispositivo.

La solicitud de análisis forense de un dispositivo móvil puede provenir de una orden judicial, el equipo legal de una parte en disputa, los departamentos de cumplimiento de una empresa, entre otros. Es fundamental que esta solicitud esté debidamente registrada y acompañada de la documentación pertinente sobre el dispositivo en cuestión.

El proceso de análisis forense de un dispositivo móvil, desde la recepción hasta la generación de informes, implica una serie de pasos meticulosos. La herramienta forense Cellebrite es ampliamente utilizada en este proceso y ofrece diversos tipos de extracciones para sistemas iOS y Android, lo que facilita el análisis exhaustivo de los datos contenidos en los dispositivos móviles.

Nos centraremos en dispositivos cuya extracción se realiza de manera consensuada, lo que implica que las credenciales de acceso son proporcionadas por el equipo jurídico o el propietario del dispositivo. Por lo tanto, el dispositivo sujeto al análisis debe estar desbloqueado.

El análisis forense de dispositivos móviles requiere la realización de una extracción del dispositivo para obtener la información contenida en él, lo que facilita llevar a cabo investigaciones pertinentes según el caso en cuestión.

El proceso de extracción de dispositivos móviles involucra una serie de pasos que comienzan

cuando el dispositivo a analizar está a nuestra disposición.

Estado del Equipo

En el inicio del procedimiento, es fundamental evaluar el estado operativo del dispositivo, que puede estar encendido o apagado. En caso de que el dispositivo se encuentre encendido al momento de su recepción, es necesario verificar el nivel de carga de la batería. Si este nivel es insuficiente, se recomienda conectar el dispositivo a una fuente de energía para asegurar un nivel adecuado de carga antes de iniciar el proceso de extracción. Durante el procedimiento de extracción, se puede proporcionar energía adicional al dispositivo para mantener niveles óptimos de carga.

Si el dispositivo se recibe apagado, es esencial conectarlo a una fuente de energía para garantizar una carga óptima antes de proceder con la extracción. Se debe tener en cuenta la posibilidad de que el dispositivo presente problemas con la batería, en cuyo caso se debe determinar si la batería es extraíble o está integrada dentro del dispositivo. En ambos casos, se deben realizar evaluaciones exhaustivas para determinar el mejor método de suministrar energía al dispositivo. En situaciones donde la batería está integrada, puede ser necesario realizar un proceso de apertura del dispositivo, involucrando herramientas especializadas para acceder a la información y llevar a cabo el proceso de extracción de manera efectiva.

Bloqueo del dispositivo

Se debe realizar una verificación para determinar si el dispositivo presenta algún tipo de bloqueo que restrinja el acceso a su contenido. Los bloqueos más comunes incluyen aquellos basados en PIN, Face ID o patrón de desbloqueo. Dado que los procedimientos de análisis forense son llevados a cabo con total acuerdo y consentimiento, estos bloqueos deben ser desactivados por el propietario del dispositivo o la persona responsable del mismo.

Aislamiento del Dispositivo

Para garantizar la integridad de los datos y evitar la interferencia externa durante el proceso de análisis, es necesario aislar el dispositivo de cualquier señal que pueda perturbar su funcionamiento. Esto implica desactivar funciones como wifi, Bluetooth y datos móviles, además de poner el dispositivo en modo avión o fuera de línea. El propósito de esta medida es prevenir cualquier comunicación externa que pueda resultar en la eliminación, modificación o inhabilitación de datos en el dispositivo. Es importante resaltar que, en el caso de un dispositivo incautado, se debe colocar en una bolsa especial conocida como bolsa de Faraday o caja de Faraday. Este tipo de bolsa aísla el dispositivo de cualquier conexión externa que pudiera comprometer su integridad, protegiendo así la información contenida en él o evitando su bloqueo.

Proceso de Documentación

Como se ha indicado previamente, es necesario documentar la entrada del dispositivo al laboratorio mediante información detallada que incluya la marca, modelo, IMEI, IMSI, número registrado, capacidad de almacenamiento, color, condiciones físicas, información del propietario, operador telefónico, así como el propósito de la extracción, la entidad solicitante, la hora, fecha y lugar de recepción. Durante este proceso, se pueden capturar imágenes del dispositivo para registrar su estado físico, así como de las pantallas de configuración e información general del mismo. Estas prácticas representan estándares de procedimiento que fortalecen la documentación del proceso de extracción, lo cual es crucial para mantener la integridad y transparencia en la gestión forense de datos.

Selección de la herramienta forense

Como mencionamos previamente, hay diversas herramientas disponibles para la extracción y análisis de contenido en dispositivos móviles. Entre estas, destaca Cellebrite, líder mundial en el ámbito forense móvil. Al considerar los dos principales sistemas operativos en el mercado, iOS de Apple y Android de Google, se observa que son sistemas distintos con métodos de extracción variables. La capacidad de la herramienta para extraer datos de ambos sistemas depende de su actualización. Cellebrite se compromete seriamente con la actualización de sus equipos, manteniéndolos al día con las últimas actualizaciones de Android e iOS. La actualización es fundamental para garantizar la capacidad de extracción de la herramienta; si el software no está actualizado para admitir las últimas versiones de iOS o Android, no podrá extraer datos de dispositivos más recientes.

Métodos de Extracción en dispositivos iOS

Cellebrite ofrece tanto extracciones lógicas como físicas para dispositivos iOS. Es importante destacar que las extracciones físicas han sido compatibles hasta el iPhone 4, lo que significa que en la actualidad solo están disponibles las extracciones lógicas. Estas extracciones lógicas permiten obtener una amplia gama de información de los dispositivos iPhone.

Entre los tipos de extracciones lógicas disponibles para iPhone, se encuentran:

Lógica Parcial: Este método de extracción es rápido y es compatible con la mayoría de los dispositivos. Permite extraer datos como registros de llamadas, contactos, mensajes de texto, eventos del calendario, archivos multimedia (videos, imágenes, audio) y datos de aplicaciones. Es importante tener en cuenta que los tipos de datos extraídos pueden variar según el fabricante y el modelo del dispositivo móvil. En la mayoría de los casos, no es posible realizar extracciones lógicas en dispositivos bloqueados.

Lógica Avanzada: Esta técnica de extracción permite acceder a archivos incrustados en la memoria del dispositivo. Es posible que el sistema de archivos contenga archivos ocultos que no sean visibles mediante una extracción lógica estándar. Con este tipo de extracción, se puede acceder a todos los archivos presentes en la memoria del dispositivo, incluyendo imágenes, videos, archivos de bases de datos, archivos del sistema y registros. También se pueden obtener datos como contraseñas, datos de aplicaciones de terceros, registros de llamadas, mensajes y chats. Esta técnica es funcional tanto para dispositivos iPhone como para dispositivos Android.

Además de las extracciones lógicas, otra opción para obtener datos de dispositivos iOS es mediante la creación de un respaldo en iTunes. Este respaldo puede realizarse en el propio dispositivo o utilizando la aplicación iTunes en sistemas Windows o Mac. El respaldo creado contiene todos los archivos de datos y configuraciones del iPhone. Estos respaldos pueden ser procesados por otras herramientas forenses, como Cellebrite o iPed Forensic, para ser indexados y permitir realizar búsquedas o aplicar filtros en busca de datos relevantes para una investigación.

Capturas de pantallas: Esta técnica se emplea en situaciones críticas en las que el acceso al sistema de archivos del dispositivo se torna inestable. Consiste en la realización de capturas de pantalla del dispositivo mediante un servicio proporcionado por Apple.

Métodos de Extracción en dispositivos Android

Cellebrite ofrece opciones de extracción tanto lógicas como físicas para dispositivos Android. Es importante tener en cuenta que la viabilidad de las extracciones físicas está sujeta al modelo específico del dispositivo y si el mismo ha sido sometido previamente a un proceso de “rooting”

Método ADB (Rooted): Este método de extracción es aplicable únicamente a dispositivos que han sido previamente “rooteados”. El término “rootear” hace referencia al proceso mediante el cual se otorgan privilegios de administrador en el sistema de archivos del dispositivo. Estos procedimientos pueden llevarse a cabo utilizando aplicaciones diseñadas específicamente para este propósito, siendo KINGO ROOT y Odín dos de las más reconocidas. Es importante tener en cuenta que realizar este procedimiento conlleva el riesgo de dejar el equipo inutilizable y, por ende, de perder la información almacenada en el dispositivo.

El método ADB (Android Debug Bridge): El Android Debug Bridge (ADB) es un protocolo de comunicación integrado que facilita la ejecución de comandos de depuración en dispositivos Android, lo que permite realizar extracciones físicas de su sistema de archivos. Para que esta

funcionalidad esté disponible, es necesario activar la opción de depuración USB en el dispositivo. Sin embargo, esta opción no está visible de forma predeterminada en la configuración del teléfono. Para activarla, el usuario debe acceder a la sección de Información del dispositivo y seleccionar el número de compilación, generalmente ubicado en Configuración. Al presionar el número de compilación siete veces consecutivas, se iniciará una cuenta regresiva para habilitar el modo desarrollador. Una vez activado, el modo desarrollador mostrará nuevas opciones de configuración, incluida la opción de depuración USB. Al activar esta opción, el dispositivo entrará en modo de depuración. Es importante destacar que la ubicación de esta opción puede variar según el modelo de dispositivo utilizado.

Método Boot Loader: Es un método de extracción física que realiza cuando el dispositivo este modo arranque, el sistema operativo se ejecuta y elude cualquier bloqueo del usuario y es forensemente seguro.

Qualcomm Live: Es un método similar al ADB (Android Debug Bridge), con la única diferencia que, si el dispositivo no está rooteado la herramienta intentara obtener temporalmente los permisos necesarios para la extracción, la opción de depuración USB debe estar activada.

Advanced ADB: Es un método similar al ADB (Android Debug Bridge), con la única diferencia que, si el dispositivo no está rooteado la herramienta intentara obtener temporalmente los permisos necesarios para la extracción, la opción de depuración USB debe estar activada y funciona con cualquier dispositivo Android con versión de firmware antes de diciembre de 2016.

Decrypted Boot Loader: Es un método de extracción que realiza una extracción de archivos para dispositivos cifrados con chipset MTK, el sistema operativo se ejecuta y elude cualquier bloqueo del usuario y forensemente seguro, también es funcional en extracciones tipo lógicas.

Para extracciones de tipo Lógica podemos mencionar algunas como:

Android Backup: Este enfoque se establece mediante la comunicación con el dispositivo Android conectado, facilitando la extracción de datos a través de comandos ejecutados por la herramienta. La cantidad de datos recuperados está sujeta a las especificaciones del dispositivo. Este método puede ser preferible en situaciones donde otras técnicas de extracción, como ADB, no sean viables o no estén disponibles. Sin embargo, es importante tener en cuenta que este método puede ofrecer una cantidad reducida de datos en comparación con otras técnicas. Además, es importante destacar que este tipo de extracción no es compatible con las versiones más recientes de WhatsApp debido a la encriptación de las bases de datos, lo que impide la decodificación de los

datos recuperados. Este método es compatible con dispositivos Android que ejecutan versiones 4.1 en adelante.

Android Backup APK Downgrade: Este método es utilizado para cambiar una versión de una aplicación por una inferior y así poder acceder a los datos utilizados por la aplicación, se utiliza más comúnmente en los casos donde se necesita extraer datos de la aplicación de mensajería WhatsApp, o Telegram, se debería utilizar como último recurso cuando los demás métodos de extracción no han sido satisfactorios.

Este método extrae los datos de las aplicaciones utilizando la copia de seguridad de Android.

Capturas de pantallas: Esta técnica es utilizada en últimas instancias donde el acceso al sistema de archivos del dispositivo se vuelve inestable, este método permite realizar capturas de pantallas del dispositivo.

Chat Capture: Es un proceso de captura de pantalla automatizado que le permite a los Analistas extraer y analizar conversaciones selectivas del chat desde datos de aplicaciones de terceros.

Existen 2 modos disponibles:

Por Aplicación: captura automáticamente los datos de las aplicaciones compatibles como WhatsApp según el nombre e intervalo de fechas de la conversación, igualmente se puede realizar búsqueda en el texto de las pantallas.

Genérico: modo semi automático para capturar cualquier área desplazable en la pantalla del dispositivo.

Después de la selección del método de extracción más apropiado, se procede a su ejecución para obtener un archivo de extracción que contenga los datos en un contenedor genérico o en el formato específico de la herramienta utilizada. Este archivo extraído debe ser procesado para su indexación según los datos obtenidos.

Cellebrite ofrece una herramienta de procesamiento y análisis llamada Physical Analyzer, que toma la extracción realizada, la procesa e indexa para realizar posteriormente un análisis exhaustivo de los datos. Una vez completado el procesamiento del archivo de extracción, se inicia el proceso de análisis, el cual implica búsquedas generales en la extracción, aplicación de filtros, identificación de palabras clave, verificación de líneas de tiempo y correlación de datos, con el

objetivo de resolver o evidenciar lo solicitado en el objetivo del análisis.

Después de la fase de análisis y la identificación de los datos relevantes para el caso, se procede a generar un informe de extracción que contiene la información filtrada y seleccionada, el cual será presentado en el caso correspondiente. Este informe debe ser acompañado de la asignación de valores hash y el inicio de la cadena de custodia según sea necesario para el caso en cuestión.

Métodos avanzados de extracción

En ocasiones, cuando los métodos convencionales de extracción lógica y física no son efectivos debido a daños físicos en el dispositivo, se recurre a métodos especializados proporcionados por empresas y personal calificado. Estos métodos, como JTAG y ChipOff, son utilizados cuando el dispositivo ha sufrido daños estructurales significativos que impiden la conectividad con herramientas forenses.

El método JTAG implica la soldadura de cables a puntos específicos en el dispositivo para enviar comandos al procesador y acceder a la información dentro de la memoria NAND. Aunque menos invasivo que el método ChipOff, el método JTAG también puede utilizarse en dispositivos bloqueados. Sin embargo, el cifrado de datos puede ser una limitación.

El método ChipOff es extremadamente invasivo y se utiliza cuando el método JTAG no es viable o el dispositivo está significativamente dañado. En este método, se desmonta el chip de memoria y se monta en adaptadores especializados para obtener una imagen de este. Este método es de último recurso y puede resultar en la pérdida del dispositivo. Además, el cifrado de datos aumenta la complejidad del proceso, pudiendo requerir la extracción del procesador para acceder a los datos.

El análisis forense de dispositivos móviles debe llevarse a cabo conforme a las normativas legales y éticas establecidas, garantizando la confidencialidad y el respeto de los derechos asociados. Esta disciplina requiere una actualización continua sobre los diversos tipos de dispositivos y las técnicas de extracción disponibles. Es imprescindible contar con un sólido conocimiento legal y una ética profesional firme, dado que los resultados obtenidos pueden tener repercusiones importantes en ámbitos legales y personales. Se debe prestar especial atención al alcance requerido en cada investigación.

RESULTADOS

El análisis forense en dispositivos móviles se caracteriza por su complejidad y constantes desafíos, atribuibles al rápido desarrollo tanto de hardware como de sistemas operativos que estos dispositivos incorporan. Dada la amplia variedad de dispositivos y sistemas operativos disponibles en el mercado, cada uno con sus propias particularidades, el análisis forense enfrenta una diversidad de escenarios y exigencias. La encriptación de datos en las versiones más recientes de dispositivos móviles representa uno de los desafíos más significativos para los analistas forenses, ya que preserva la privacidad de la información almacenada en el dispositivo. Además, muchas aplicaciones de terceros utilizan cifrado de extremo a extremo, lo que dificulta aún más el proceso de extracción de datos, requiriendo que los analistas se mantengan actualizados respecto a nuevas tecnologías y metodologías.

La complejidad se ve aumentada por las actualizaciones periódicas de los sistemas operativos móviles, que pueden limitar la efectividad de las herramientas forenses disponibles. Es crucial tener en cuenta las consideraciones éticas y legales en esta especialidad, ya que los dispositivos móviles son extensiones personales del usuario, y acceder a su información sin consentimiento puede vulnerar la privacidad y comprometer la ética profesional. Por lo tanto, el análisis debe realizarse dentro de un marco legal y ético estricto, respetando los derechos individuales.

El respaldo de herramientas actualizadas es esencial para aquellos que deseen incursionar en esta especialidad con propósitos comerciales. En el caso de las extracciones en dispositivos iOS, estas se basan en copias de seguridad de iTunes, que pueden ser procesadas por diversas herramientas forenses. A diferencia de los dispositivos Android, que presentan una amplia variedad de fabricantes y, por ende, de sistemas operativos, iOS tiene un único fabricante, lo que simplifica el proceso de análisis en cierta medida.

Las herramientas forenses han desarrollado diversas técnicas, desde las menos invasivas hasta las más agresivas, para acceder al contenido de los dispositivos, incluyendo la aplicación de exploits, agentes de instalación de aplicaciones, degradación de aplicaciones y “rooteo” del dispositivo. Cada tipo de extracción presenta una serie de consideraciones particulares que deben ser abordadas por el analista forense, quien debe seguir un protocolo de fases para preservar la integridad de la evidencia digital en todo momento.

El análisis forense digital abarca desde el acceso inicial al dispositivo hasta la generación de informes, utilizando tanto herramientas comerciales como gratuitas. Es fundamental que el analista forense evalúe si la herramienta utilizada cumple con los requisitos forenses necesarios para su

aplicación.

DISCUSIÓN

A pesar del constante avance en las tecnologías de encriptación de datos, diseñadas para salvaguardar la privacidad y seguridad de los dispositivos, estas también plantean un desafío significativo para las herramientas forenses en su capacidad de acceder a los datos y llevar a cabo extracciones exitosas. Los fabricantes de herramientas forenses para dispositivos móviles se encuentran en una competencia continua para mantenerse al día con los cambios implementados por los fabricantes de dispositivos móviles, especialmente aquellos con múltiples versiones, como es el caso de Android. En última instancia, es crucial tener en cuenta las consideraciones legales y éticas para proteger los derechos individuales mientras se busca facilitar la administración de justicia.

CONCLUSIONES

Este estudio resalta la complejidad y los desafíos recurrentes enfrentados en el ámbito del análisis forense digital de dispositivos móviles. Es importante destacar que no existe un método estándar para llevar a cabo este tipo de análisis en equipos móviles, ya que existen diversas variables que deben ser consideradas. La selección del método adecuado dependerá del criterio del analista forense informático, quien debe garantizar la preservación de la evidencia y realizar un análisis exhaustivo.

Es fundamental mantener una comunicación estrecha y colaborativa entre las áreas legales, de tecnología y seguridad, con el propósito de asegurar que las investigaciones forenses se lleven a cabo de manera efectiva y ética. Además, la educación continua y la formación profesional son aspectos críticos para que los profesionales forenses se mantengan actualizados respecto a las tendencias tecnológicas y los marcos legales vigentes.

REFERENCIAS BIBLIOGRÁFICAS

- Cellebrite. (n.d.). Cellebrite. Recuperado el 5 de mayo de 2024, de https://cellebrite.com/en/home/ [1]
- PR Newswire. (n.d.). Cellebrite amplía su gama de soluciones forenses móviles con el software UFED basado en PC y hardware listo para su uso. Recuperado el 13 de mayo de 2024, de https://www.prnewswire.com/news-releases/cellebrite-amplia-su-gama-de-soluciones-forenses-moviles-con-el-software-ufed-basado-en-pc-y-hardware-listo-para-su-uso-229843161.html [2]
- On Retrieval. (n.d.). Oxygen Forensic Detective. Recuperado el 13 de mayo de 2024, de

https://onretrieval.com/productos/hardware/oxygen-forensic/oxygen-forensic-detective/ [3]

- Mobiledit. (n.d.). Mobiledit. Recuperado el 13 de mayo de 2024, de https://www.mobiledit.com/ [4]
- Jeffries, A. (n.d.). Belkasoft. Recuperado el 13 de mayo de 2024, de https://belkasoft.com/alan-jeffries-review-belkax [5]
- Peña, L. B. L. B. J. (2023). El arte y la ciencia de las investigaciones digitales forenses Volumen 3 Sistemas Android - iOS. Columbia SC, USA. [6]
- Roa, M. M. (2024, marzo 30). El mapa mundial de Android e iOS. Recuperado de https://es.statista.com/grafico/29620/sistema-operativo-movil-con-la-mayor-cuota-de-mercado-por-pais/ [7]
- Henriques, A. (2023). Academia de Forense Digital. Recuperado el 13 de mayo de 2024, de https://academiadeforensedigital.com.br/avilla-forensics-ferramenta-gratuita-de-analise-de-smartphones/ [8]
- Oxygen Forensics. (2024). Oxygen Forensics. Recuperado el 13 de mayo de 2024, de https://oxygenforensics.com/en/ [9]
- Belkasoft. (n.d.). Belkasoft. Recuperado el 13 de mayo de 2024, de https://belkasoft.com/ [10]
- XRY - Mobile Forensics and Data Recovery Software. (n.d.). XRY - Mobile Forensics and data Recovery Software. Recuperado el 13 de mayo de 2024, de https://www.msab.com/product/xry-extract/ [11]
- Magnet Forensics. (n.d.). Magnet Forensics. Recuperado el 13 de mayo de 2024, de https://www.magnetforensics.com/ [12]