Universidad Zaragoza
1542

Trabajo Fin de Grado

Análisis Forense del Sistema Android

Autor

Jesús David Isaac Pírez

Directores

Director académico: Dra. Lacramioara-Sinziana Dranca Dranca
Director militar: Cap. D. Yago Fábregues Barambio

Centro Universitario de la Defensa-Academia General Militar
2016

Agradecimientos

Si bien este proyecto de fin de grado ha requerido un gran esfuerzo y dedicación por parte del presente, no hubiera sido posible su finalización sin la ayuda y máximo interés por parte de las personas que a continuación se cita.

Primero y antes de nada, dar las gracias a mi familia por el gran apoyo recibido durante todos estos años de esfuerzo. Especialmente a mi hermana Cristina y a mi madre Francisca, que tras haber estado viviendo momentos difíciles no han parado de apoyarme.

De igual manera mi más sincero agradecimiento a mis dos tutores de proyecto, la Dra. Licri Dranca y el Cap. D. Yago Fábregues Barambio, que me han estado orientando en todo momento, así como al Tte. D. Daniel Iglesias Plaza por haberme facilitado todo aquello que he necesitado para realizar los aspectos más importantes del proyecto.

Por último agradecer al personal de la unidad de Guerra Electrónica, en especial a Ciberdefensa que me ha ayudado a realizar la fase de investigación. En especial al Cabo Primero Torres y al Soldado Molón por sus grandes conocimientos y gran aportación a este trabajo.

Tabla de contenido

Tabla de ilustraciones

Tabla de tablas

Lista de acrónimos

AOT Ahead of time (inglés), Antes de Tiemo (español).

API Application Programming Interface (inglés), Interfaz de Programación de Aplicaciones (español).

ART Android Routine (inglés), Rutina Android (español).

CP Código Penal.

GPS General Position System (Inglés), Sistema de Posicionamiento Global (español).

HAL Hardware Abstraction Layer (inglés), Capa de abstracción de hardware (español).

HTTPS Hypertext Transfer Protocol Secure (inglés), Protocolo Seguro de Transferencia de Hipertexto (español)

LOPJ Ley Orgánica del Poder Judicial.

PIN Personal Identification Number (inglés), Número de Identificación Personal (español)

PUK Personal Unlock Key (inglés), Clave Personal de Desbloqueo (español).

RFC Request For Comment (inglés), Petición de comentario (español).

SIM Suscriber Identity Module (inglés), Módulo de Identificación de Abonado (español).

SMS Short Message Service (inglés), Servicio de Mensajes Cortos (español).

TSJ Tribunal Superior de Justicia.

UNE Una Norma Española

Resumen

El objetivo principal de este Trabajo de Fin de Grado es el de estudiar y comparar el dispositivo empleado por parte de la unidad de ciberdefensa para realizar análisis forenses con una herramienta que un usuario normal podría acceder a través de internet de forma gratuita. Este análisis se centra en el de la extracción de información de un teléfono móvil con sistema operativo Android.

Esta investigación se rige a las leyes que existen en España con respecto a este tipo de operaciones. Además se basa en las normas y los estándares: ISO / IEC 27037, RFC 3227, UNE 71505 y UNE 71506. La metodología que se emplea para llevar a cabo el análisis forense consta de cuatro etapas: adquisición, preservación, análisis y presentación de resultados.

Además este trabajo explica cómo funciona el sistema operativo Android, así como las principales vulnerabilidades que tiene dicho sistema operativo.

Por último, se exponen los resultados del análisis forense llevado a cabo con cada una de las herramientas empleadas. El primer análisis se realiza con el dispositivo empleado por el Ejército de Tierra tanto en Territorio de Operaciones como en Territorio Nacional. El segundo se realiza con una herramienta que un usuario particular puede utilizar para poder extraer información de un teléfono móvil. Además, estos análisis se realizan en base a un caso de estudio que recoge una situación ficticia pero que podría darse en Territorio de Operaciones.

Abstract

The main objetive of this research is to study and compare the device used by unit of cyberdefense to perform forensic analysis with another programme that a normal user could access by internet for free. This analysis is focus on the extraction of information from a mobile phone with Android operating system.

This investigation is governed by the laws that exist in Spain regarding this type of analisys. In addition this investigation is base on the following standars: ISO / IEC 27037, RFC 3227, UNE 71505 y UNE 71506. The methodology used is structured in four phases as follows: acquisition, preservation, analysis and presentation of results.

Furthermore, this document explain the Android operating system and the main vulnerabilities that Android has.

Finally, the results of the forensic analysis conducted with each of the tools used are set. The first scan is performed with the device used by the Army in both Territory Operations and Homeland. The second is done with a tool that a particular user can use to extract information from a mobile phone. Moreover, these analyzes are performed on the basis of a case study that includes a fictitious situation but could be in Territory of Operations.

Capítulo 1: Plan de trabajo.

1.1 Propósito y justificación

En la actualidad gran parte de la población mundial está en continua comunicación. De hecho según un estudio realizado por 'Mobility Report' de Ericsson la cifra de líneas móviles alcanzó la cifra de la población mundial, 7300 millones de suscripciones. A esto hay que sumarle el aumento de tráfico de datos, que aumentó en un 65 por ciento [1]. Esto conlleva el envío de mucha información a través de los teléfonos móviles ya pueden ser fotografías personales, contactos, ubicaciones GPS (sistema de posicionamiento global), etc. Sin embargo, el hecho de manejar toda esta información a través de estos medios supone que pueda ser robada por hackers o ciberdelincuentes, siendo, cada vez más difícil enviar o guardar información de forma segura. De hecho, según un artículo de "ESET Latinoamerica" las familias de malwares[1] están aumentando conforme aumenta el número de dispositivos móviles. Es más, en el año 2012 se detectaron 55 nuevas familias de malwares y tan solo un año después, en el 2013, se detectaron 79 nuevas familias [2].

La seguridad informática supone un gran reto, tanto a nivel civil como militar debido a la información tanto privada como confidencial que se maneja. Ante esta información los ciberdelincuentes realizan ataques a la seguridad del sistema informático para poner en peligro la integridad, disponibilidad y confidencialidad de la información. Todos estos ataques tienen tanto fines económicos como militares, como el reciente caso de las 500 millones de cuentas robadas a Yahoo [3]. Debido a esto cada vez se invierte más en seguridad en la red para evitar este tipo de robos.

Cuando se está en territorio de operaciones (que es el principal marco de actuación del Ejército de Tierra) no se busca un dispositivo móvil para analizarlo, más bien se utiliza la guerra electrónica para realizar escuchas de radio. Sin embargo, el hecho de detener a algún sospechoso e incautarle ya puede ser una Tablet, ordenador o dispositivo móvil puede proporcionar mucha información acerca de posibles futuras actuaciones de terroristas contra las bases del ejército español. Para ello se utiliza el análisis forense.

El análisis forense es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal [4]. Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Hoy en día el sistema operativo Android [5] está presente en múltiples dispositivos electrónicos como smartphones, tablets, etc. En particular, este estudio se centra en comparar diferentes métodos para realizar el análisis forense a un teléfono móvil.

1.2 Objetivos

El objetivo principal de este trabajo es el de estudiar y comparar el análisis forense de un teléfono móvil que es capaz de realizar el dispositivo UFED Touch (empleado por parte de la unidad militar de Guerra Electrónica nº31, en concreto la compañía de ciberdefensa) con una herramienta que un usuario normal podría acceder a través de internet de forma gratuita.

[1] Tipo de software malicioso que trata de infectar un ordenador, un teléfono o una Tablet.

Para poder alcanzarlo se han establecido varios objetivos específicos:

- Conocer la situación actual de la informática forense, así como las regulaciones que existen en este sector.
- Entender la metodología para llevar a cabo un análisis forense.
- Conocer de manera general la arquitectura del sistema operativo Android.
- Estudiar la seguridad y vulnerabilidades que presenta el sistema operativo Android.
- Estudiar distintas herramientas para realizar análisis forenses.
- Realizar un análisis forense con la herramienta comercial UFED TOUCH Y UFED Physical Analizer [6].
- Identificar una herramienta gratuita comparable con UFED TOUCH para realizar análisis forense.
- Realizar un análisis forense con esta herramienta gratuita.

1.3 Resultados esperados

Una vez realizado este trabajo se espera conocer la ventaja que supone el realizar un análisis forense con UFED TOUCH con respecto a otras herramientas.

1.4 Estructura del trabajo

El presente trabajo se estructura en cinco capítulos:

En el primer capítulo, "Plan de trabajo", se exponen los diferentes objetivos que se quieren conseguir y los resultados esperados tras finalizar la investigación

Para saber cómo se realiza un análisis forense se debe estudiar cómo está actualmente la informática forense, así como las regulaciones que existen para llevar a cabo este tipo de análisis. Todo esto se recoge en un segundo capítulo: "Situación actual informática forense".

Una correcta metodología a seguir es fundamental para alcanzar los objetivos planteados con el mayor éxito. En el tercer capítulo ("Metodología para el análisis forense") se identifican las diferentes etapas que hay que llevar a cabo para realizar con éxito un análisis forense.

El sistema Android es un sistema operativo con una estructura compleja. Para llevar a cabo un análisis forense se ha tenido que estudiar el funcionamiento de lo que se pretende analizar. En el capítulo "Sistema Android" se explica la arquitectura y el funcionamiento de este sistema.

En el último capítulo, "Análisis forense Sistema Android" se exponen diferentes métodos para llevar a cabo el análisis forense. Se realiza un análisis forense con la herramienta UFED Physical Analizer y con otra herramienta a la que un usuario particular pueda acceder gratuitamente a ella.

Capítulo 2: Situación actual informática forense.

Este capítulo recoge la situación actual de la informática forense así como las diferentes regulaciones que existen tanto a nivel estatal como a nivel internacional y las diferentes normativas y estándares que existen sobre la informática forense.

2.1 Qué es la informática forense

El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. [4].

La necesidad de llevar a cabo este tipo de técnicas nace del almacenamiento de casi toda la información en medios electrónicos.

A la hora de recuperar información que ha sido borrada en el teléfono móvil, el forense puede tener muchos problemas si las estructuras administrativas del software del sistema de archivos han sido borradas o corrompidas. Esta información se puede haber perdido por un error humano o por un problema de fallo de la tecnología de hardware y/o software.

En informática forense se habla también de descubrimiento de información y no solo de recuperación de información. Esto se debe a que no hubo necesariamente un error humano o un fallo del sistema para perder información, sino que pudo haber una actividad subrepticia para borrar, adulterar u ocultar información.

2.2 Marco legal y normativo

Ante un incidente tecnológico, siempre bajo la legislación vigente, se debe dar respuesta a las siguientes cuestiones:

- ¿Qué ha sucedido?
- ¿Dónde ha sucedido?
- ¿Cómo ha sucedido?
- ¿Por qué ha sucedido?
- ¿Quién o qué lo ha provocado?

Se parte de que en un Estado de Derecho (Garantista), como es el Estado Español, la Constitución establece unas pautas generales que garantizan en todo momento el derecho a la Intimidad personal. Estas pautas, se materializan en un “Marco Normativo y Legal” y que afectan directamente a la adquisición y tratamiento de datos.

2.2.1 Marco Legal

Se han de tener en cuenta los siguientes ámbitos:

1. El ámbito Constitucional. (Constitución Española).
2. El ámbito Jurídico, Ley Orgánica del Poder Judicial (LOPJ).
3. El ámbito Laboral. (Estatuto de los trabajadores).

4. El ámbito Personal. (LOPD (Ley Orgánica de Protección de Datos Personal), LSSI (Ley de Servicios de la Sociedad de la Información), etc.).

Aplicando todo ello a la actividad forense y en particular a la adquisición de datos de dispositivos (apartado 3.1), se puede decir que:

- Cualquier actuación sobre dispositivos tanto de almacenamiento como de proceso de datos que contentan información de carácter personal o sea susceptible de ello (Discos duros, Pendrives, Cuentas de correo electrónico, etc.), ya sea de empleados, como de clientes, se ha de tratar con las debidas autorizaciones y/o requerimientos Judiciales para su intervención.
- Además, en el momento de la intervención, se ha de contar SIEMPRE con la presencia de la persona propietaria del sistema o recurso intervenido o en su defecto un testigo que de fe de que dicha intervención se ha limitado al objeto del requerimiento o de la autorización.

  El ANEXO A amplia esta información relacionada con el marco legal y normativo.

Capítulo 3: Metodología para el análisis forense.

Respecto a la normativa vigente relacionada con la informática forense se extraen varios puntos importantes a los cuales hay que hacer hincapié. Uno de los puntos más importantes es el no alterar la información que se está analizando ya que sino ésta no servirá para presentarla ante un tribunal. Otros de los puntos importantes en cuanto a la normativa es el hecho de cómo se guardan las pruebas, como se conservan, su transporte, etc. Posteriormente recalcan como se analizan las pruebas para obtener el máximo rendimiento posible de tal información. Por último, es muy importante el redactar un informe de los resultados de manera que cualquier persona pueda entender la conclusión que se ha obtenido.

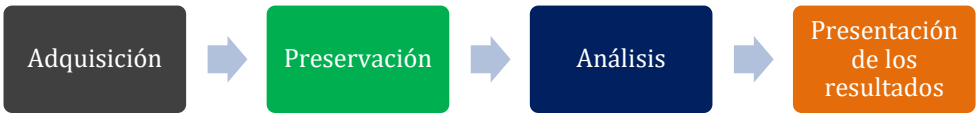


Ilustración 1 Fases metodología Análisis Forense

Teniendo en cuenta lo anterior y la información de experto recogida se explicarán las distintas fases: adquisición, preservación, análisis y presentación de los resultados, que hay que llevar a cabo para un correcto análisis forense. [7]

3.1 Adquisición.

Durante una investigación forense se ha de tener mucho cuidado con la adquisición de las evidencias, ya que es imprescindible que el proceso de adquisición se realice de forma correcta sin que pueda alegarse que haya habido una posible manipulación de los datos. Además ha de quedar constancia del proceso y se debe establecer la cadena de custodia para garantizar la preservación e integridad de las evidencias.

El proceso de adquisición de evidencias digitales es la fase más crítica del proceso forense. De ella depende el buen resultado de una investigación puesto que en esta fase es donde se deberá extraer toda aquella información que después será procesada en la fase de análisis. Este procedimiento por lo tanto se desarrolla bajo la norma ISO/IEC 27037:2012 de obligado cumplimiento para la adquisición de evidencias electrónicas y que se alinea con la norma ISO/IEC 27042:2015, que proporciona una orientación para identificar y evaluar evidencias digitales y ayudar a interpretar un incidente tecnológico. Bajo estas premisas, se verificarán los siguientes 3 principios fundamentales:

- Principio de relevancia sobre aquellos elementos que son pertinentes a la situación que se analiza o investiga.

- Principio de confiabilidad que busca validar la repetibilidad y auditibilidad de un proceso aplicado para obtener una evidencia digital.

- Principio de suficiencia que está relacionada con la completitud de pruebas informáticas, es decir que, con las evidencias recolectadas y analizadas se tienen elementos suficientes para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada.

Todas las tareas para realizar una buena adquisición de evidencias digitales han de ser debidamente documentadas tal y como se describirá a continuación en cada uno de los documentos diseñados a tal fin. A efectos prácticos, a continuación se muestra todo el proceso de la investigación forense con sus tareas asociadas:

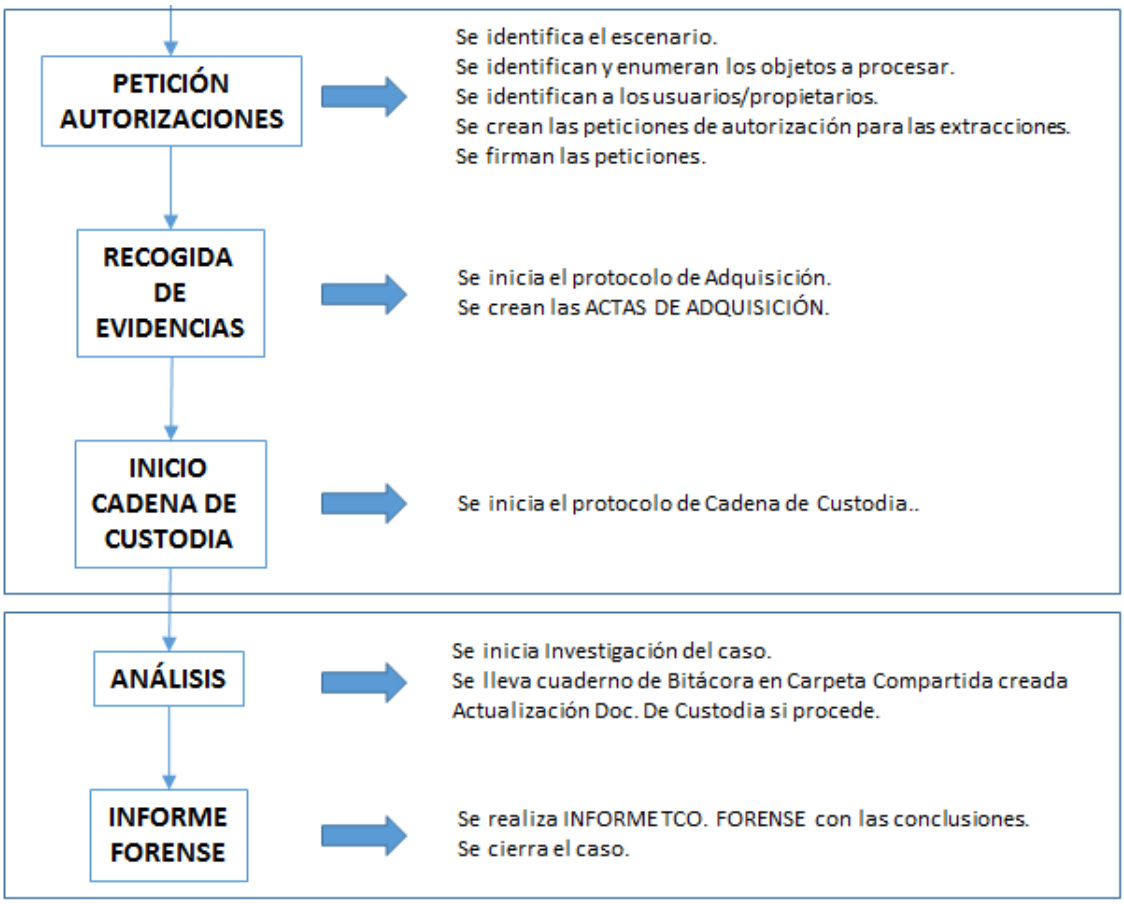


Ilustración 2 Proceso investigación forense.

Según la RFC3227 se define una serie de tareas a realizar para la recolección de evidencias forenses tras un incidente tecnológico:

- La identificación del entorno donde se ha producido el incidente.
- La identificación y selección de los objetos a procesar.
- El tratamiento/Adquisición de cada uno de los objetos (Copia, extracción, etc.).
- La cadena de custodia.
- El almacenamiento de las evidencias.

Como normal general, para realizar la adquisición de evidencias forenses de un sistema, ya sea de un servidor, un ordenador personal o un Smartphone, se ha de tener en cuenta el orden, estableciéndose en la RFC3227 que dicha adquisición deberá hacerse en orden DE MAYOR A MENOR VOLATILIDAD.

De esta manera, el orden de procesado sería:

1. Memoria RAM.
2. Disco Duro.
3. Soportes de Almacenamiento externo (HDD USB, Pendrive's, Tarjetas SD, etc.).

En términos generales, el esquema para la actuación en la fase de adquisición sería:

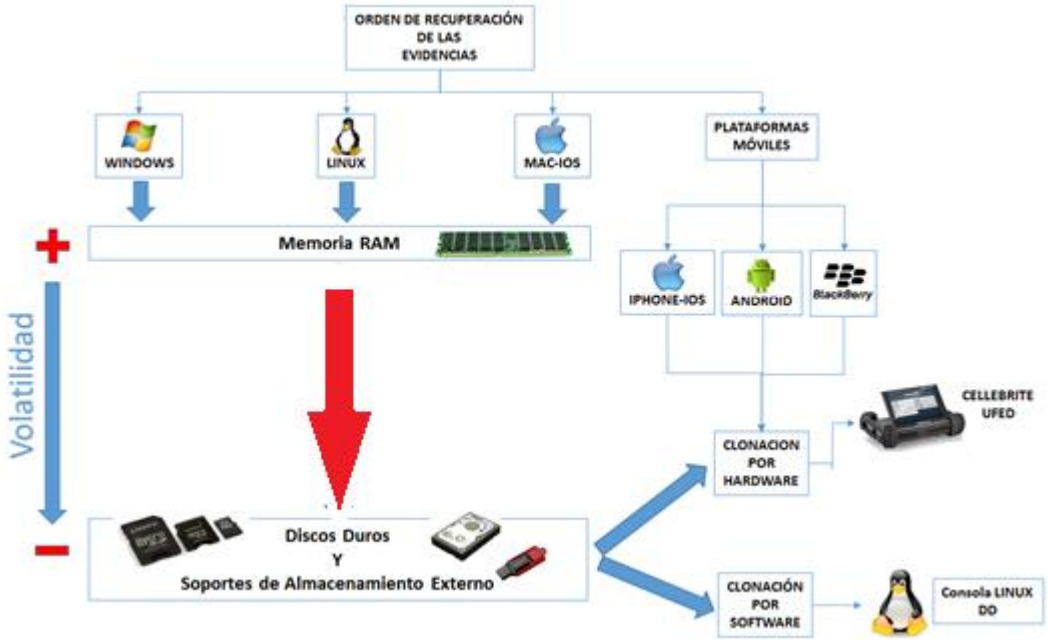


Ilustración 3 Esquema fase de adquisición.

En este caso al tratarse de un teléfono móvil el orden de procesado corresponde a los de menos volatilidad.

Esta fase incluye la generación de imágenes para poder llevar a cabo el análisis de la información. Las imágenes son copias de la información y a través de estas copias es de donde se hará el análisis posterior. Estas copias se realizan utilizando tecnología punta para evitar cualquier tipo de modificación de la información que pueda alterarla. En este trabajo se trabajará con UFED TOUCH y Autopsy 4.1.1. Cuando se genera la imagen se refiere a hacer una copia bit a bit de todo el disco duro.

Una vez obtenida la imagen es de vital importancia la conservación de la misma. Para asegurarse que la información obtenida no sufre alteración alguna se protege mediante el uso del algoritmo hash, que es un algoritmo de comprobación de integridad y que genera un valor/clave para algún dato/archivo. De esta manera, si la información ha sido modificada o alterada el valor hash ya no será el mismo y por lo tanto la información no será la misma.

Es muy común que se realicen varias copias de los disco a analizar, ya que si la durante la fase del análisis la copia resulta dañada o incluso es robada se asegura el poder seguir la investigación.

3.2 Preservación

Esta fase se centra en el cuidado a la hora de manejar la información. Una mala preservación o un mal uso de la información puede llevar a cabo a la alteración de esta y por lo tanto podría quedar invalidada toda la investigación si tuviera que ser presentada ante un tribunal.

Para ello hay tener muy claros cuáles son los fines que se persiguen cuando se procede a extraer la información de los dispositivos, en este caso los teléfonos móviles. En el caso que se pretende utilizar esa información para obtener una orden de detención y, por lo tanto tener que presentar las pruebas ante un tribunal, ya pueda ser civil o militar, es muy importante no alterar la información y conservar la escena tal y como estaba al principio. Para ello se inicia la cadena de custodia para evitar esas alteraciones y realizar esta fase de manera controlada. El investigador tiene que conocer plenamente las normativas y los límites de la ley hasta los cuales puede llegar para obtener la información, de lo contrario la información extraída no servirían como prueba ante un tribunal. Sin embargo, si los fines son a nivel inteligencia para saber posibles futuras actuaciones de grupos terroristas, o el hecho de obtener información de utilidad, se puede alterar el método de acceso a la información. Alterar el método de acceso a la información significa que, para poder acceder a la información de un terminal se tienen que realizar algunas modificaciones del terminal. Esto conlleva la modificación de la prueba original y por lo tanto no sería válida ante un tribunal.

Al realizar la imagen de la información a extraer hay que realizar varias copias. Se han de realizar al menos 3 copias de la información. La primera ha de ser la original, que será la que se presente como prueba ante el tribunal. La segunda es para el forense, que será a través de la cual trabajará y realizará todo tipo de análisis. Y la tercera y última copia de respaldo por si sufriera daños la segunda copia.

Hay que tener en cuenta que los dispositivos que guardan las copias que se van a analizar son dispositivos electrónicos. Esto significa que pueden sufrir daños y por lo tanto la pérdida de la copia. Para ello hay que tomar medidas de seguridad tanto en el transporte como en el almacenamiento de los dispositivos que contienen la información. Además es conveniente que mientras que no se está analizando la información precintar los dispositivos que albergan la información a analizar con etiquetas. De esta manera cada dispositivo estará identificado con una etiqueta única para evitar posibles confusiones.

3.3 Análisis

En esta fase el investigador se centra en buscar la información más relevante. Al generar una imagen se obtiene toda la información que contiene el teléfono móvil.

Sin embargo, no siempre es preciso utilizar toda esa información, sino que el investigador se centra en la información que le sea más útil dependiendo de lo que esté buscando.

Para llevar un correcto análisis de la información es importante seguir unos pasos que permitan entender mejor la información:

3.3.1 Preparar un entorno de trabajo

Antes de empezar el análisis se toma la decisión de si se quiere realizar el análisis en caliente o en frío.

Si se realiza el análisis en caliente significa que se trabaja directamente sobre el disco duro o el dispositivo a analizar. Este proceso tiene más complicaciones ya que si se comete algún error puede desencadenar en la invalidación de la información. En cuanto a las medidas que se tienen que tener en cuenta es en la de poner el disco duro en modo lectura y no lectura y escritura ya que de esta manera no se puede modificar la información

Si se realiza el análisis en frio se genera una imagen del disco duro mediante una máquina virtual. De esta manera se puede indagar más en la información sin tener tanta precaución como en el análisis en caliente.

3.3.2 Reconstruir una línea temporal con los hechos sucedidos

Cuando se analiza la información el investigador se tiene que centrar en los cambios o alteraciones más destacables que puedan ayudar a crear una secuencia de hechos.

En primer lugar se debe analizar la información que se ve a simple vista, es decir la información al que un usuario podría acceder si tuviera en posesión el disco duro, el dispositivo móvil, etc. Se analizarían las últimas llamadas, ficheros, frecuencia de actividad, etc.

En segundo lugar se debe analizar la información que no está a simple vista, es decir, aquella información que ha sido borrada pero que mediante técnicas informáticas se puede recuperar. Probablemente esta acción es la que más información dé ya que el atacante habría eliminado información relevante.

3.3.3 Evaluar el impacto causado

Tras haber analizado la secuencia de los hechos es hora de analizar el impacto causado y sacar las conclusiones. El investigador debe evaluar si la información que ha obtenido todavía tiene relevancia o si ya se queda obsoleta. También debe evaluar si el impacto económico que ha supuesto dicha investigación ha sido rentable o si va a suponer un gasto innecesario de dinero. Finalmente debe evaluar si el tiempo invertido en tal investigación ha sido rentable. Esta evaluación en temas de inteligencia es de vital importancia, ya que la rapidez es fundamental para evitar posibles ataques del atacante analizado.

3.4 Presentación de los resultados.

En esta última etapa se exponen las conclusiones obtenidas. Se ha de obviar los detalles muy técnicos y las técnicas utilizadas para obtener dichos resultados. Es de vital importancia

exponer unos resultados claros y concisos, de manera que cualquier persona pueda entender cuáles son las conclusiones.

Capítulo 4: Sistema Android

Para poder realizar un análisis forense sobre un dispositivo con el sistema operativo Android, se ha visto la necesidad de estudiar cómo funciona este sistema. El interés se centra sobre todo como se puede acceder a la información de un dispositivo móvil. La mayor parte de la información ha sido consultada según los apartados de la bibliografía [8] [9] [10].

4.1 ¿Qué es Android?

Android es un sistema operativo que se creó para dispositivos móviles, especialmente teléfonos móviles y tablets basado en el núcleo Linux.

Este sistema operativo está construido sobre el kernel de Linux y ejecuta una máquina virtual especialmente creada para Android para optimizar recursos de memoria y de hardware en un entorno móvil. Android es de código abierto, lo que significa que este sistema operativo es distribuido y desarrollado libremente. Esta característica es lo que hace a este sistema operativo tan atractivo a los usuarios ya que cualquiera puede crear una aplicación y ejecutarla en Android. Además, el hecho de ser un código abierto facilita el incremento de aplicaciones y por lo tanto la competencia, lo que hace que haya múltiples herramientas o aplicaciones de muy buena calidad.

4.2 Arquitectura sistema Android

La arquitectura interna de Android está formada por cuatro componentes: aplicaciones, armazón de aplicaciones, librerías y kernel/Linux. Una de las características más importantes es que todas las capas están basadas en software libre. La siguiente gráfica muestra la arquitectura del sistema operativo.

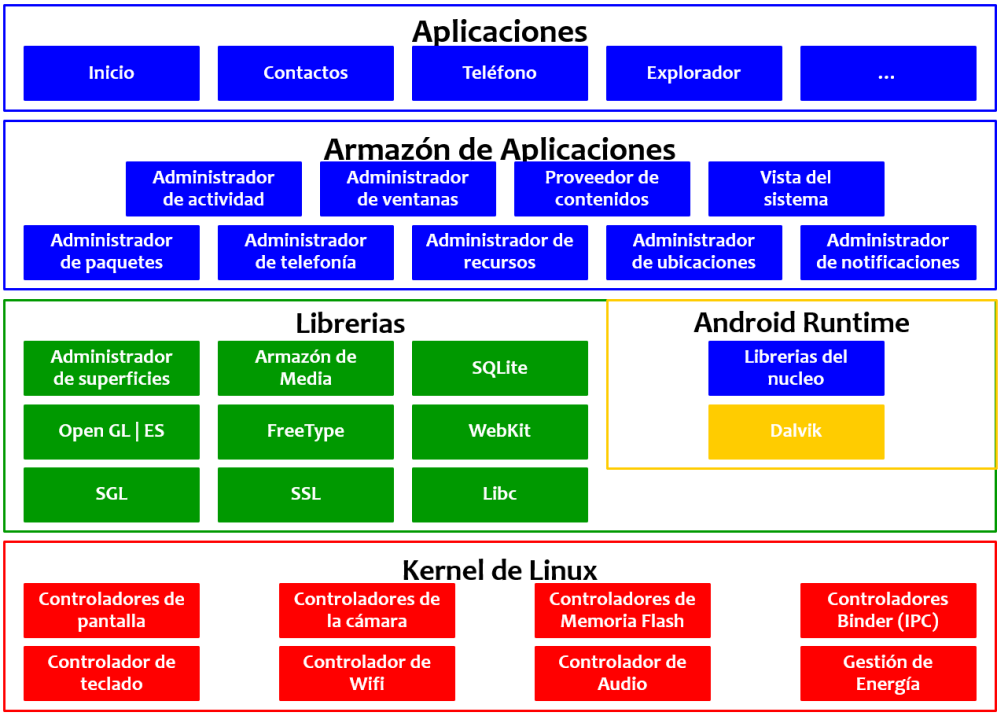


Ilustración 4 Arquitectura Sistema Operativo Android

El ANEXO B detalla la función de cada componente de la arquitectura del sistema operativo Android.

4.3 Seguridad sistema Android

Para garantizar la seguridad en el sistema Android el usuario debe de actualizar siempre que pueda el sistema operativo. Para ello una vez que el móvil tiene conexión 3G o esté conectado a una red Wi-Fi se verifica automáticamente si existe una nueva versión o actualización del sistema operativo.

Para saber si existen nuevas actualizaciones se establece una conexión cifrada con el servidor "Android.clients.google.com" mediante HTTPS (Hypertext Transfer Protocol Secure) (TCP/443). Si existe tal actualización, Android establecerá una conexión no cifrada HTTP con el servidor "Android.clients.google.com" para descargar la actualización. En teoría la integridad de las actualizaciones se verifican a través de una firma digital asociada a un fichero de actualización (.zip). Debido a que no hay cifrado en esta descarga da la posibilidad a la manipulación de este intercambio de información.

Para aumentar la seguridad, Android aplica el principio de mínimo privilegio, donde cada aplicación solamente puede acceder a sus propios componentes. De esta manera las aplicaciones no pueden actuar sobre otras aplicaciones. Además, si las aplicaciones quieren acceder a información compartida del usuario o de otras aplicaciones, las aplicaciones deben solicitar una serie de permisos para acceder a tal información. Estos permisos son notificados al usuario en el momento de la instalación de la aplicación. Una vez autorizada por el usuario las aplicaciones podrán disponer de la información que han solicitado.

En el siguiente ejemplo se muestran los distintos permisos que la aplicación solicita para su funcionamiento. Inicialmente sólo despliega una serie de permisos pero si se le dá al botón "Ver todo" aparecerá la lista completa de los datos compartidos a lo que va a acceder la aplicación.

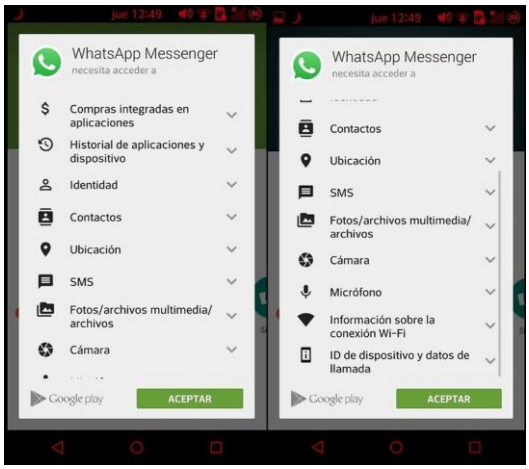


Ilustración 5 Permisos Aplicación Whatsapp

En cuanto a la seguridad proporcionada por Android para acceder físicamente al dispositivo móvil cuenta con varias opciones. Para evitar que un atacante acceda a la información, el usuario puede fijar una contraseña o PIN (Personal Identification Number) tanto al dispositivo móvil como a la tarjeta SIM (Suscriber Identity Module).

4.3.1 Pin de la tarjeta SIM

El pin de la tarjeta SIM bloquea el acceso no autorizado tanto a los servicios como a la información guardada en la SIM. Solamente el dispositivo móvil podría utilizarse para realizar llamadas de emergencia.

El sistema Android posibilita el establecer un PIN entre 4-8 dígitos. Por defecto la contraseña suele contar con 4 dígitos pero se recomienda cambiar la contraseña y establecer una más larga. Además incluye otro sistema de seguridad, el cual tras haber introducido de manera incorrecta el PIN más de 3 veces automáticamente la tarjeta SIM se bloquea. En este caso para poder desbloquear la tarjeta SIM es necesario introducir otra contraseña denominada PUK (Personal Unlock Key).

4.3.2 PIN, contraseña o patrón de acceso al dispositivo móvil.

El PIN bloquea el acceso no autorizado al terminal. De esta manera no se puede acceder a los datos, capacidades de comunicación ni aplicaciones.

Android permite establecer tres tipos de restricción de acceso al terminal. El primero sería un PIN, compuesto de al menos 4 dígitos. El segundo sería una contraseña compuesta por al menos cuatro caracteres alfanuméricos. El tercer y último modo de acceso al terminal sería el patrón de desbloqueo de pantalla.

Debido a la debilidad de este tipo de contraseñas, el sistema Android ha establecido un mecanismo de seguridad el cual tras haber introducido más de 5 intentos de PIN, contraseñas o patrones el móvil se bloqueará durante 30 segundos hasta poder volver a introducir otra vez la contraseña. Sin embargo, esto permite el realizar ataques de adivinación, posibilitando realizar 600 intentos por hora por parte de un atacante.

4.4 Vulnerabilidades sistema Android

Desde que Android salió publicado, numerosos fallos del sistema operativo han provocado falta de seguridad en los dispositivos, lo que supone un gran número de vulnerabilidades. Se entiende por vulnerabilidad una debilidad del sistema operativo que puede ser utilizada para causar daño. Una de las últimas vulnerabilidades de Android ha afectado a cerca de 900 millones de teléfono móviles, permitiendo el control total del teléfono móvil por parte de los ciberdelincuentes sin que el usuario se diese cuenta [11]. Sin embargo, tal y como muestra el siguiente gráfico que data del año 2016, son múltiples las vulnerabilidades de Android [12]

Ilustración 6 Tipos de vulnerabilidades de Android

Para poder evitar estas vulnerabilidades el sistema operativo se va actualizando. Estas actualizaciones incluyen parches que solucionarán las vulnerabilidades de la antigua actualización. Sin embargo, mientras que el usuario no actualice el sistema operativo quedará expuesto a las vulnerabilidades ya resueltas por la nueva actualización.

Android ha ido haciendo hincapié especialmente en la seguridad a partir de la versión 4.0. Sin embargo, al mismo tiempo que va evolucionando el sistema operativo también lo hacen los elementos maliciosos como pueden ser los virus o troyanos. Mediante estos elementos maliciosos los hackers pretenden obtener una información que resulte útil para poder manipularla de cualquier manera. Estos objetivos pueden ser conocer la ubicación mediante google maps del dispositivo, realizar una foto mediante la cámara del móvil, formatear el dispositivo móvil, etc.

Hay que tener en cuenta que al instalar una aplicación, ésta no dispone de ningún permiso por defecto. Sin embargo, si durante la instalación una aplicación no solicita ningún permiso no quiere decir que (debido a vulnerabilidades en Android) no puede llevar a cabo acciones que afecten la privacidad del usuario, por lo que el usuario debe evaluar minuciosamente la instalación de nuevas aplicaciones incluso cuando estas no soliciten ningún permiso.

Otra de las vulnerabilidades encontradas en una reciente actualización de Android es agrupar los permisos individuales en uno común que tengan capacidades o funciones específicas. De esta manera se conseguía reducir el interfaz gráfico de usuario (GUI) de manera que los usuarios pueden entender más fácilmente los permisos que demanda la aplicación. Sin embargo, a través de esto se han introducido nuevas vulnerabilidades. A modo de ejemplo, cuando antes una aplicación pedía un permiso para leer un SMS (Short Message Service) solicitaba el permiso "READ_SMS", mientras en las últimas versiones solicita el grupo de permisos "SMS". De esta manera la aplicación tendrá acceso también al envío de SMS aunque el usuario no haya aprobado este permiso.

Una de las formas más fáciles de hackear un dispositivo móvil con Android es mediante la creación de aplicaciones malignas. Inicialmente cuando el atacante decide subir la aplicación al mercado de Android (GOOGLE PLAY) la aplicación tiene que pasar una serie de controles por parte de Android y necesita la aprobación por parte del usuario de permisos para acceder a información compartida. En ese momento la aplicación está sana y pasa tanto los controles de Android como la aprobación del usuario. Sin embargo, el atacante podría introducir un código maligno o malware en la siguiente actualización de la aplicación que ya no necesita la aprobación del usuario y es cuando el usuario decide actualizar la aplicación cuando el malware entra en el sistema operativo. Al haber autorizado inicialmente el acceso de información compartido, como puede ser ubicación, contactos, etc. la aplicación tiene acceso a esa información y es cuando el atacante substrae toda la información.

Otra forma para hackear un dispositivo móvil es a través de las redes Wi-Fi públicas. Al conectar el dispositivo móvil con una de estas redes saldrá un navegador tipo google para que el usuario se dé de alta en alguna página y así obtener el internet gratuito. Sin embargo, esta página puede ser un virus pudiendo robar la información ya que se ha dado permiso al aceptar las condiciones. Siempre que se pueda hay que evitar este tipo de redes públicas ya que no se sabe que fines tiene.

Capítulo 5: Análisis forense Sistema Android

En el mercado actual existen múltiples métodos para realizar análisis forense, desde aplicaciones software sencillas útiles para obtener información general de un dispositivo, hasta aplicaciones software muy sofisticadas capaces de obtener información más detallada.

Para poder obtener la mayor información posible acerca de las herramientas y métodos empleados por defensa en los análisis forense se han realizado varias entrevistas (consultar Anexo C) al personal experto en la materia, en concreto al personal especializado en realizar los análisis forenses en la compañía de Cieberdefensa del Ejército de Tierra.

Tras realizar dichas entrevistas se ha decidido centrarse en el dispositivo que utiliza el Regimiento de Guerra Electrónica 31. Se trata del UFED TOUCH, una herramienta perteneciente a Cellebrite Mobile Synchronization, una compañía Israelí cuya especialidad es el análisis forense de dispositivos. El motivo de utilizar UFED TOUCH es que es la única herramienta que tiene valor judicial. Cuando se trata de temas de análisis forense, tanto en territorio de operaciones como en territorio nacional, es de vital importancia el poder presentar las pruebas ante un tribunal si fuera necesario. Es por ello que la unidad de Guerra Electrónica utiliza UFED TOUCH. Además es una herramienta que permite extraer todo tipo de información como se expondrá más adelante.

A partir de las entrevistas se ha identificado otra herramienta adecuada a comparar con la herramienta UFED TOUCH. Se trata del programa Autopsy 4.1.1 para Windows, ya que es considerado como la mejor herramienta gratuita para poder realizar un análisis forense de un teléfono móvil. Posteriormente se presentará un análisis forense realizado con cada una de las herramientas para poder sacar una serie de conclusiones y así comparar las prestaciones de cada una de las herramientas.

Los análisis forenses que se han realizado responden a un caso ficticio que recoge a una posible situación que se muestra en el ANEXO D. Para la construcción del caso de estudio se ha contado con la opinión del personal experto en la materia.

5.1 UFED TOUCH

UFED TOUCH es un producto de origen israelí. Se puede analizar la información directamente en el dispositivo móvil (UFED TOUCH) o también en el software diseñado para ordenador denominado UFED PHYSICAL ANALIZER.

Ilustración 7 UFED TOUCH

El modo para poder utilizar UFED PHYSICAL ANALIZER no vale solo con instalar el programa (se puede descargar gratuitamente desde la página oficial) sino que aparte de pagar la licencia que caduca cada año, la cual incluye todas las actualizaciones anuales (10 actualizaciones anuales), hay que conectar al ordenador un pendrive que actúa como una llave (ilustración 8). En el caso que se quiera utilizar el dispositivo portátil no es necesario el uso de dicha llave. Este método ofrece doble protección para poder utilizar el software de manera legal, ya que sin el pendrive no se puede utilizar el software y por lo tanto no se puede acceder a la información que se haya extraído con el programa anteriormente.

Ilustración 8 Llave UFED Cellebrite

UFED TOUCH puede trabajar con dispositivos móviles, tarjetas SIM y dispositivos USB o tarjetas de memoria. Además puede trabajar con todo tipo de sistemas operativos: Android, IOS, Symbian, etc. Sin embargo, dependiendo del sistema operativo el software podrá sacar más o menos información dependiendo de las medidas de seguridad que disponga el sistema operativo.

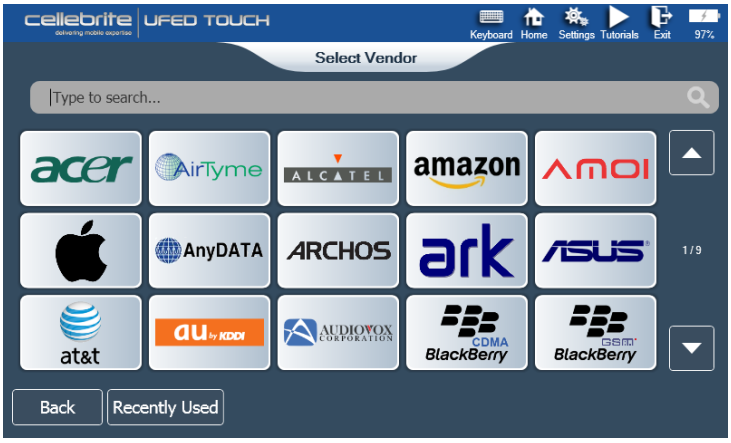


Ilustración 9 Algunos de los S.O. con los que puede trabajar UFED TOUCH

En cuanto a la obtención de información UFED TOUCH puede realizar tres tipos de extracciones: Física (realiza una copia de toda la memoria flash), Lógica (extrae información limitada) y de Sistema de archivos (extrae la información de los archivos). Una descripción más detallada sobre los tres tipos de extracciones puede consultarse en el ANEXO E. Dependiendo del sistema operativo se podrán hacer las tres extracciones o ninguna. Por ejemplo, si se intenta extraer información con IOS, el software informa que solo puede realizar una extracción lógica y extracción del sistema de archivos pero no física. Por el contrario, si se intenta extraer información del sistema Android, permite realizar los tres tipos de extracciones. Al realizar la extracción UFED TOUCH tiene un formato propietario. Esto significa que no se puede trabajar con dicha copia con ninguna otra herramienta y que por lo tanto la copia no puede ser modificada. Este aspecto es muy importante ya que es lo que le aportará la validez judicial.

Uno de los inconvenientes que presenta UFED TOUCH es la dificultad a extraer la información de dispositivos Apple. Aunque en este trabajo no se estudia análisis forense de dispositivos Apple es interesante resaltarlo ya que en territorio de operaciones los forenses se pueden encontrar ante este tipo de dispositivos.

UFED Physical Analizer tiene también conectividad a red. Con esto al extraer las localizaciones vía GPS (Sistema de posicionamiento global) del dispositivo móvil el software puede conectarse a internet y mostrar por la pantalla las ubicaciones. Sin duda es una de las funcionalidades más útiles para los investigadores. Además este software permite introducir una serie de filtros de acuerdo a la información que se quiere buscar.

Como última característica de UFED Physical Analizer es la generación de informes en múltiples formatos (PDF, Microsoft Word, etc.). Con esta funcionalidad el investigador se ahorra mucho tiempo en generar un informe aparte.

5.1.1 Extracción de la información UFED TOUCH.

A la hora de realizar el análisis forense del dispositivo móvil basta con conectar uno de los conectores , en este caso el A-100, que lleva el maletín de UFED TOUCH y conectar el teléfono móvil al UFED TOUCH con dicho conector. Probablemente no se sepa cuál sea el conector ya que el dispositivo dispone de múltiples conectores (ilustraciones 11 y 12). Sin embargo, UFED TOUCH dispone de una herramienta que facilita dicha búsqueda. Al escribir el modelo de móvil indicará una numeración que se corresponderá con un conector.

Ilustración 11 Conectores UFED TOUCH

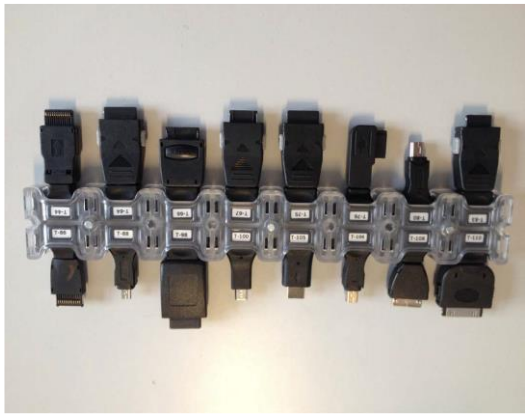


Ilustración 10 Conectores UFED TOUCH

Cuando se conecta el conector en el teléfono móvil automáticamente el teléfono móvil entra en modo recovery. El modo recovery (modo de recuperación) es una partición del sistema operativo que tiene su propio kernel. De esta manera si el modo recovery no está dañado, se puede acceder al sistema operativo sin necesidad de pasar por ninguna medida de seguridad. Con este modo UFED TOUCH puede acceder a las particiones de Android y extraer todo tipo de información, incluida la extracción física que supone una copia total.

Una vez conectado el teléfono al UFED TOUCH aparece en la pantalla qué tipo de extracción se quiere realizar (ilustración 12). Una vez seleccionado el tipo de extracción UFED TOUCH procede a extraer toda la información correspondiente. Si se trata de una copia bit a bit el proceso de extraer toda la información puede llevar alrededor de dos horas.

Ilustración 12 Tipos de análisis UFED TOUCH.

Una vez realizada la copia de la información, la pantalla muestra toda la información que ha extraído. A la izquierda de la pantalla se despliega un menú con los apartados de toda la información que se ha extraído, llamadas, mensajes, coordenadas GPS, cronología, etc. UFED TOUCH informa además de la información que ha extraído y que había sido borrada por el propietario del dispositivo móvil. De esta manera el investigador se puede centrar en esa información, ya que puede que sea la más útil.

Cuando UFED TOUCH está realizando la copia, el dispositivo móvil está funcionando y por lo tanto durante este proceso gasta batería. Para evitar que el dispositivo móvil se quede sin batería UFED TOUCH incorpora una serie de pinzas que se conectan a la batería y va cargando el móvil a la vez que realiza la copia.

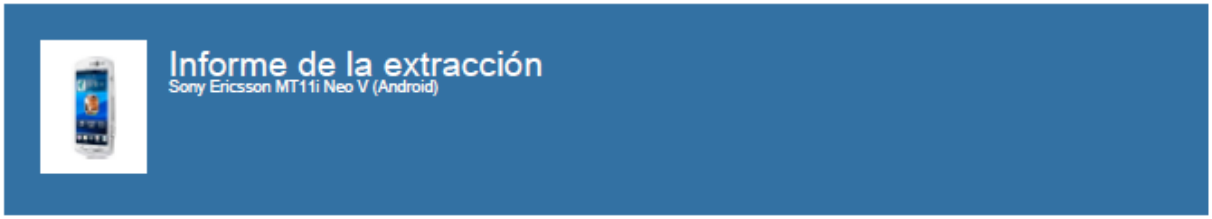
Una vez realizado la extracción del teléfono móvil se puede trabajar bien con UFED TOUCH o con el software UFED Physical Analizer. Si hay la posibilidad de trabajar con este último mejor ya que al tener una pantalla más grande (se trabaja en el ordenador) se puede visualizar mucho mejor la información que con el dispositivo UFED TOUCH.

Como se muestra en la ilustración 13 se ha trabajado con UFED TOUCH para realizar la extracción física y con UFED Physical Analizer para realizar el análisis de la información.

Ilustración 13 Teléfono móvil, UFED TOUCH, UFED Physical Analizer (De izquierda a derecha).

5.1.2 Informe Análisis Forense UFED TOUCH

En base al caso de estudio se ha obtenido el siguiente informe:



Resumen

Versión de UFED Physical Analyzer	5.3.0.2
Fecha de creación de informe	17/10/2016 9:48:26 +02:00
Configuración de zona horaria (UTC)	(UTC+01:00) Madrid (Europe)
Número de caso	1
Nombre del caso	Trabajo Fin de Grado
Número de prueba	1
Nombre examinador	Jesús David Isaac Pírez
Departamento	/
Ubicación	/

Extracción de origen

Física	
Fecha/hora inicio de extracción	14/10/2016 11:14:17(UTC+2)
Fecha/hora fin de extracción	14/10/2016 11:55:33(UTC+2)
Identificador de la unidad	UFED S/N 5926566
Versión de UFED	5.3.0.731
Versión interna	4.3.11.731
Fabricante seleccionado	Sony (SonyEricsson)
Nombre del dispositivo seleccionado	Xperia Neo V MT11i
Tipo de conexión	Cable No. 100
Tipo de extracción	Física [Android ADB]
ID de extracción	71AF9394-681C-49EF-B6F0-2D290B51E141

Ilustración 14 Informe extracción UFED Physical Analizer

Se puede apreciar que la herramienta extrae información de contactos, contraseñas, etc. Además, indica el número total de información que ha extraído de cada aparatado y entre paréntesis la información que había sido borrada y que ha recuperado. Esta información se puede consultar de manera detallada en los diferentes apartados del amplio informe que genera la aplicación, que por motivos de espacio no será publicado en el presente informe ya que consta de 6500 páginas.

Tipo	Incluido en el informe		Total	
Contactos	1067	(228 borrado)	1067	(228 borrado)
Contraseñas	28	(4 borrado)	28	(4 borrado)
Conversaciones	440	(315 borrado)	440	(315 borrado)
Facebook	1	(1 borrado)	1	(1 borrado)
WhatsApp	439	(313 borrado)	439	(313 borrado)
Cookies	150	(101 borrado)	150	(101 borrado)
Cuentas de usuario	10		10	
Desplazamientos	6		6	
Historial de Internet	271	(21 borrado)	271	(21 borrado)
Mensajes	68	(12 borrado)	68	(12 borrado)
Mensajes SMS	1217	(20 borrado)	1217	(20 borrado)
Reg. llamadas	549	(50 borrado)	549	(50 borrado)
Ubicaciones	83	(46 borrado)	83	(46 borrado)
Archivos de datos	1032	(2 borrado)	1032	(2 borrado)
Bases de datos	189		189	
Imágenes	843	(2 borrado)	843	(2 borrado)
Análisis de actividad	1771		1771	
Análisis de correos electrónicos	194		194	
[redacted]	194		194	
Análisis de teléfonos	449		449	
WhatsApp	716		716	

Ilustración 15 Características extracción UFED Physical Analizer

A continuación se detallan los apartados que tienen interés para el caso de estudio.

Llamadas

Se han registrado un total de 549 llamadas, de las cuales 50 habían sido borradas y se han recuperado. El número registrado es el (+034) 62------- .

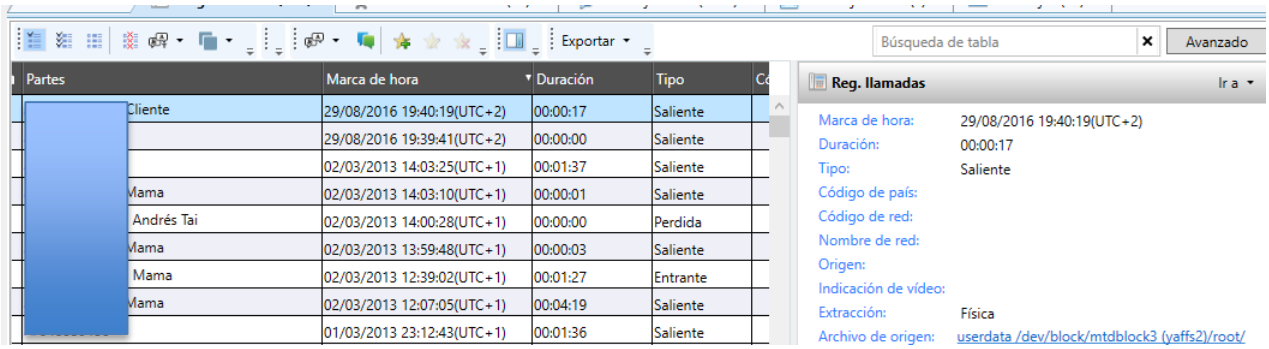


Ilustración 16 Registro llamadas UFED Physical Analizer

La aplicación muestra información detallada de cada llamada: destinatario, marca de hora, duración, tipo de llamada (entrante/saliente) tal y como se aprecia en la ilustración 16.

Correos electrónicos

La aplicación identifica la cuenta de correo electrónico que utiliza el dispositivo. Además, muestra la información de los emails (marca de hora, origen, etc,), incluso si se selecciona cualquier email la aplicación mostrará el contenido de éste (véase ilustración 17). La aplicación ha recuperado 12 emails que habían sido borrados.

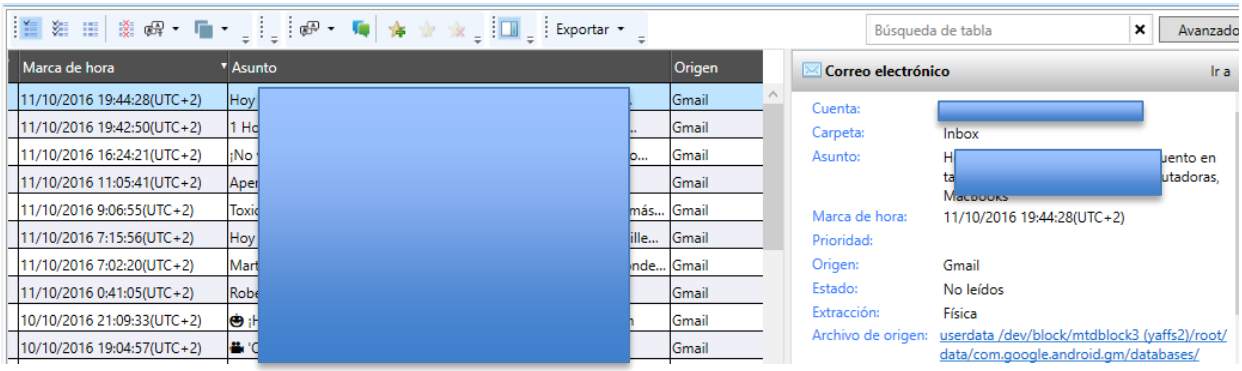


Ilustración 17 Correos electrónicos UFED Physical Analizer

Contactos

Se han extraído 1067 contactos de los cuales 228 habían sido borrados.

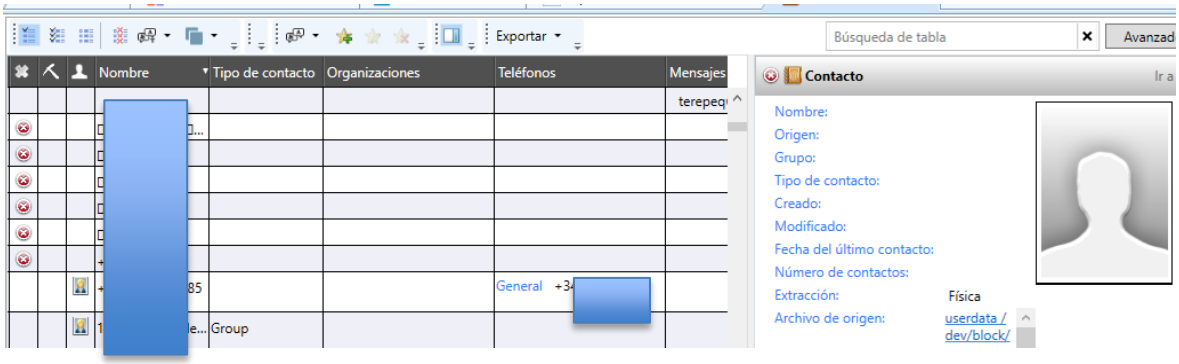


Ilustración 18 Contactos UFED Physical Analizer

Coordenadas

Se han encontrado un total de 92 ubicaciones GPS de las cuales 48 habían sido borradas. Además si seleccionamos cualquier posición, la aplicación ejecutará GOOGLE EARTH mostrando dónde se encuentra tal coordenada.

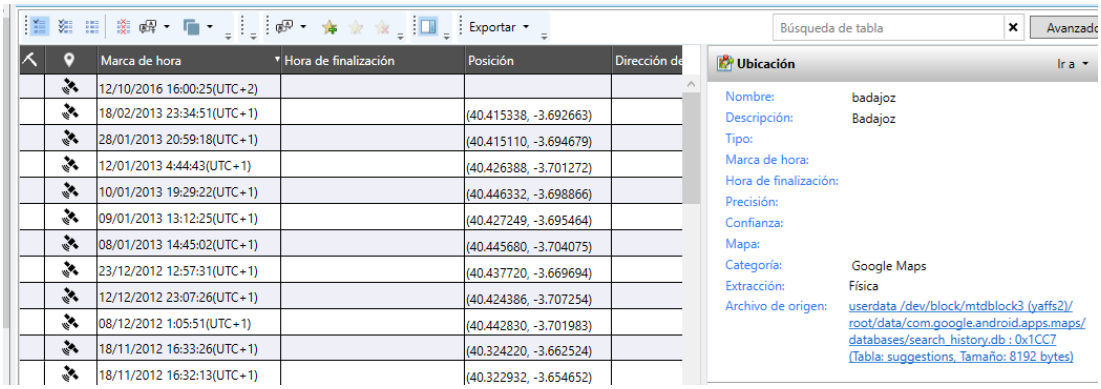


Ilustración 19 Coordenadas UFED Physical Analizer

Imágenes

Se han encontrado un total de 940 imágenes:

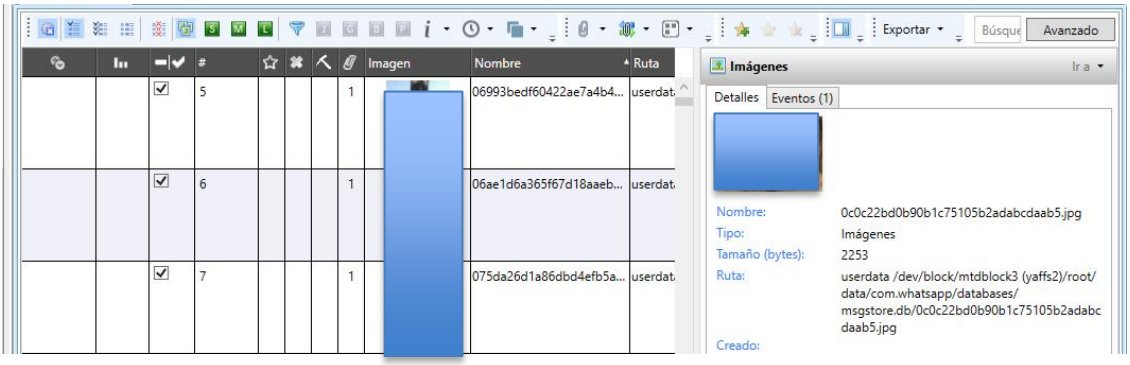


Ilustración 20 Imágenes UFED Physical Analizer

Mensajes

La aplicación muestra información detallada de cada mensaje: marca de hora, carpeta, partes, contenido, etc., como se muestra en la ilustración 21. En total se han extraído 1225 mensajes, de los cuales 20 habían sido borrados.

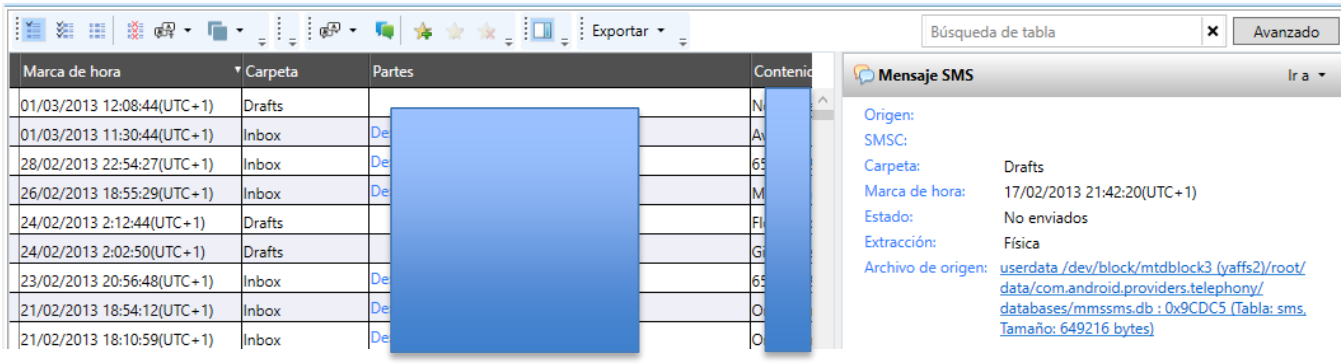


Ilustración 21 Mensajes UFED Physical Analizer

Conversaciones

Se han extraído un total de 440 conversaciones, de las cuales 315 estaban borradas y se han recuperado. Estas conversaciones se pueden consultar tanto en la aplicación como en el informe detallado. Además la aplicación muestra información de interés como los participantes de las conversaciones.

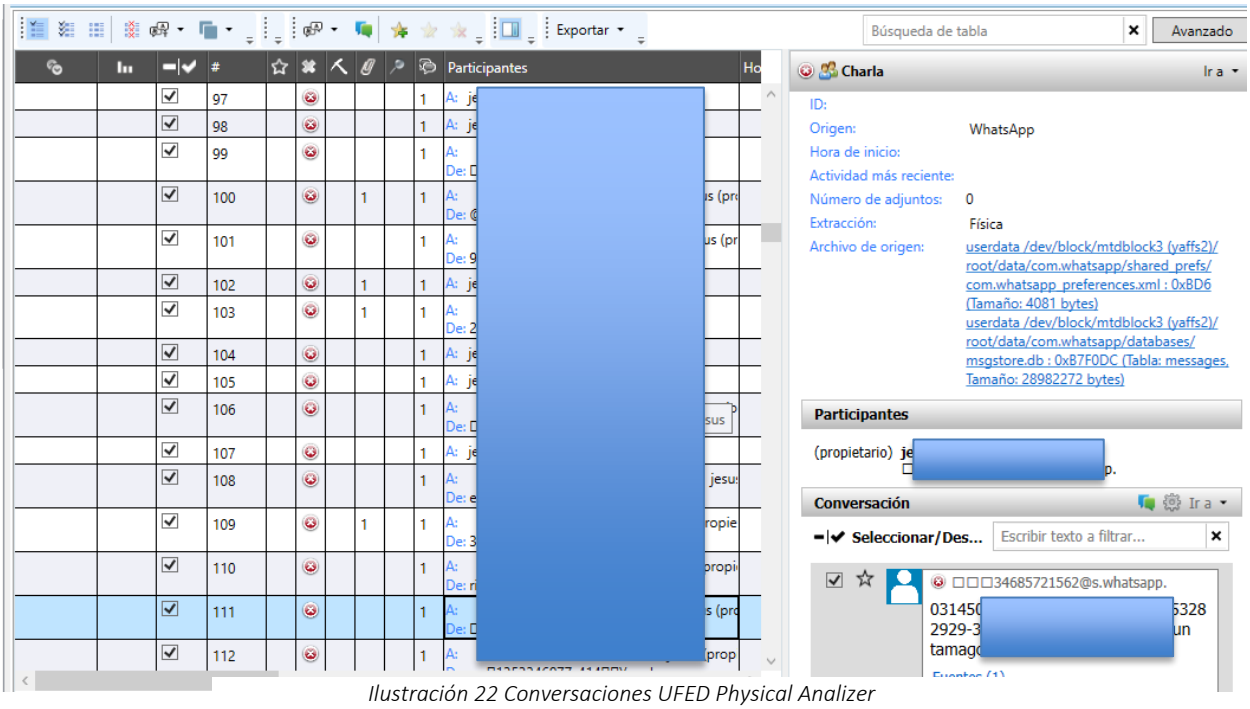


Ilustración 22 Conversaciones UFED Physical Analizer

Movimiento de datos

El movimiento de datos se concentra principalmente en el año 2012 y a principios de 2013. Se observar un pequeño movimiento de datos en el año 2016. Esto último es destacable debido al período de inactividad del teléfono móvil durante 3 años y el nuevo funcionamiento de éste en este año.

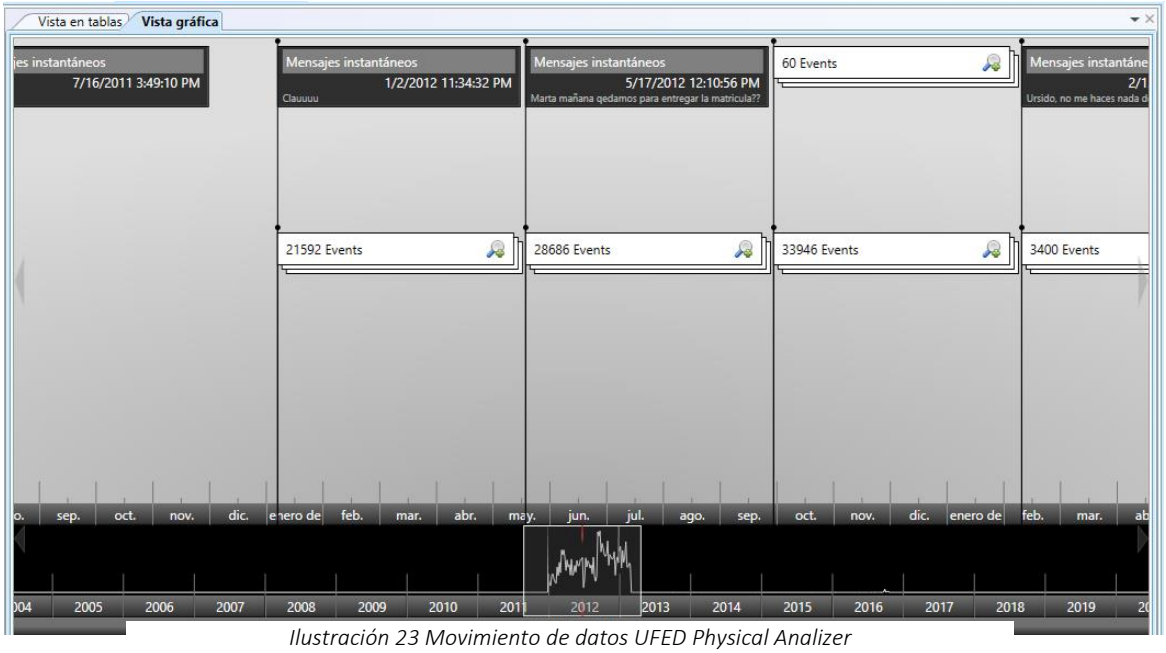


Ilustración 23 Movimiento de datos UFED Physical Analizer

5.2 Autopsy 4.1.1

Autopsy 4.1.1 es una herramienta gratuita que cualquier usuario puede obtener mediante internet [11]. El número de actualizaciones por parte del programa es bastante alto, de hecho 4.1.0 salió publicado en julio de 2016 y Autopsy 4.1.1 sólo dos meses después. Al igual que UFED TOUCH, se encarga de realizar análisis forense digital. Esta herramienta es de open source, que inicialmente fue desarrollada para plataformas UNIX y que actualmente se encuentra disponible tanto para Windows como para OS X. Permite analizar tanto discos duros como sistemas de archivos de smartphones de una manera eficiente. Este tipo de herramientas se pueden encontrar en Kali Linux (ilustración 24), que es un sistema operativo diseñado para la auditoría de la Seguridad Informática y que tiene pre-instaladas Autopsy 4.1.1. Sin embargo, se realizará la práctica en Windows.

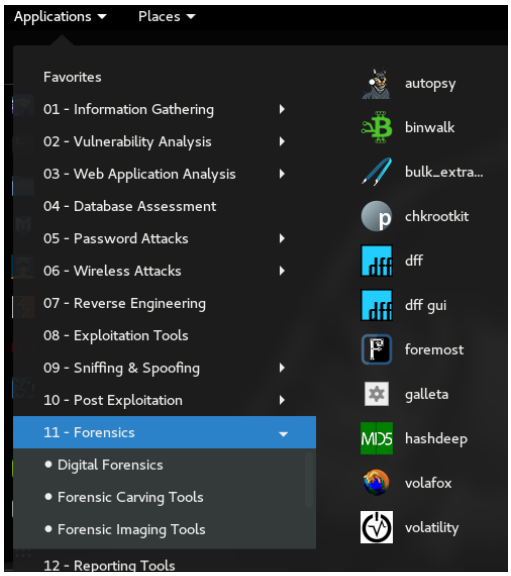


Ilustración 24 Menú Forensía Kali Linux.

Autopsy 4.1.1 es muy utilizada en el mundo del análisis forense informático debido a que es un software que incluye múltiples herramientas de análisis forense. Esto le ofrece al investigador un análisis muy completo del dispositivo que se está analizando.

Una de las principales desventajas de esta herramienta es que a la hora de extraer la información de teléfonos móviles es que solo puede extraer la información de la memoria externa. Autopsy no puede acceder al resto de la información a no ser que el teléfono móvil este rooteado. Rootear un teléfono móvil significa modificar el sistema operativo para conseguir el control total de él [10]. Esto permite trasladar toda la información de la memoria interna a la memoria externa. De esta manera el ordenador detectaría toda la información de la memoria externa del teléfono móvil y Autopsy 4.1.1 podría acceder a toda esa información y así realizar el análisis forense. El rootear el móvil conlleva modificar la prueba que los forenses reciben, es decir, la prueba original. Esto supone que si se pretende presentar esta prueba no tendría ningún valor judicial. En este aspecto Autopsy se queda muy corto para realizar análisis forenses de teléfonos móviles. Se podría realizar un buen análisis si el teléfono móvil se encontrara rooteado en el momento de adquirirlo.

Para poder realizar el análisis con Autopsy 4.1.1 se debe tener, aparte del dispositivo a analizar, el cable compatible para conectar el dispositivo a un ordenador.

Al ejecutar Autopsy 4.1.1, ofrece la posibilidad de crear un nuevo caso, de abrir un caso reciente o de abrir un caso existente. En este caso se ha creado un nuevo caso.

Una vez marcada la opción de nuevo caso se despliega una nueva pestaña donde se pide al usuario que especifique donde quiere guardar el caso. Posteriormente el programa solicita el nombre del forense. Tras haber rellenado estos dos últimos pasos Autopsy 4.1.1 crea el nuevo caso y salta una pestaña donde solicita que el analista indique de donde quiere que se extraiga la información a analizar. El programa ofrece al usuario la posibilidad de analizar una imagen, un disco o archivos. En el caso de analizar teléfonos móviles habrá que crear una imagen para poder trabajar con Autopsy 4.1.1 o bien trabajar con la memoria externa del teléfono. En el ámbito de Defensa se suele trabajar con la imagen del teléfono móvil por temas legales. De esta manera el teléfono puede ser devuelto y se trabaja con la imagen del teléfono en el momento de su obtención. En este trabajo se ha extraído la información de la memoria externa ya que la información que se va a extraer de la imagen y de la memoria externa es la misma. Para poder realizar la imagen del móvil se ha utilizado el programa FTK Imager Lite **(Consultar Anexo E).**

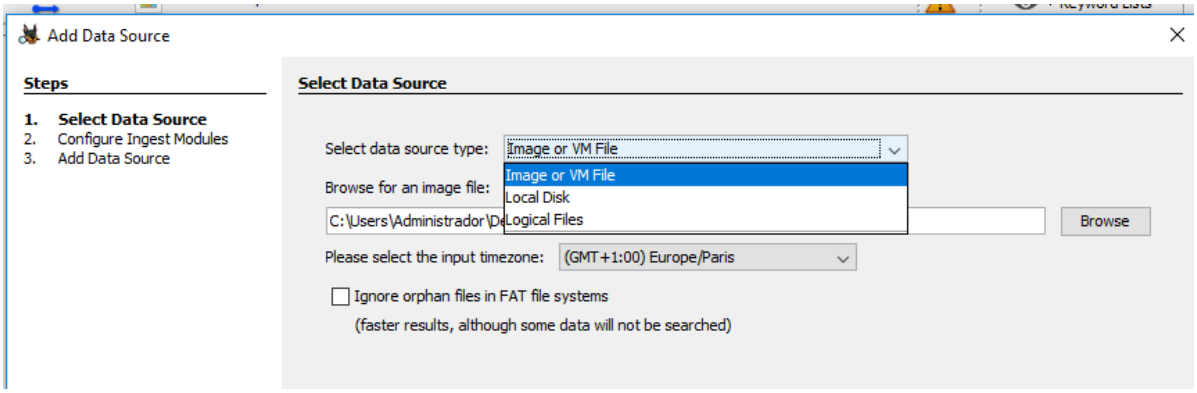


Ilustración 25 Selección fuente de datos Autopsy 4.1.1.

Autopsy 4.1.1 ofrece una serie de módulos que se deben solucionar dependiendo del tipo de extracción que se quiera realizar. En la versión actual (4.1.1) Autopsy ofrece 13 módulos (ilustración 25). Esto significa que este software contiene muchas herramientas para realizar un análisis forense y sin duda es bastante interesante desde el punto de vista de un usuario que no quiere pagar licencia [12].

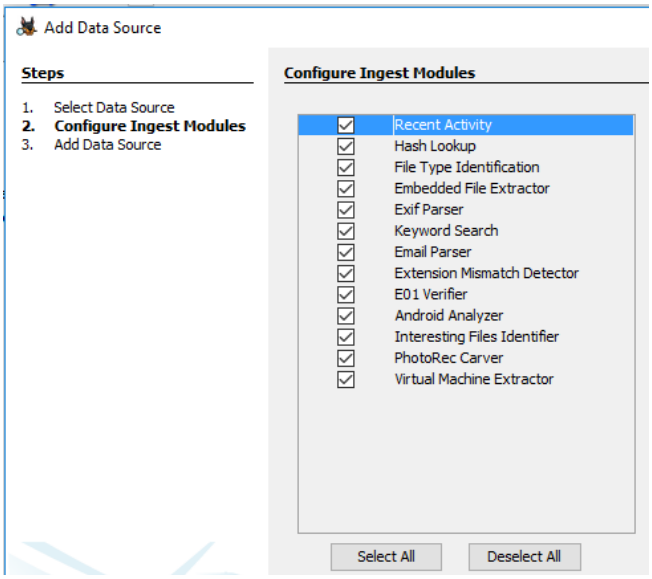


Ilustración 26 Módulos Autopsy 4.1.1

Para el ámbito de defensa son bastante interesantes varios módulos que Autopsy ofrece como puede ser Recent Activity (para saber la actividad reciente que ha tenido el dispositivo móvil), Email Parser (para obtener los emails del dispositivo móvil), etc

Una vez seleccionado los distintos módulos que se pretenden analizar, que en este caso se seleccionaran todos los módulos para extraer la mayor información posible, Autopsy 4.1.1 empieza a realizar el análisis forense. Esta herramienta inicialmente desplegará una lista en la parte izquierda mostrando todos los datos que ha detectado. Es interesante la recuperación de los datos que habían sido borrados anteriormente. Sin embargo, realizar la extracción del sistema de archivos puede llevar bastante tiempo. Esto supone un hándicap ya que Autopsy 4.1.1 tarda mucho en cargar los datos. Inicialmente Autopsy 4.1.1 empieza cargando los datos que habitualmente son considerados más importantes. Sin embargo, esto puede no coincidir con las preferencias del investigador. Por ello hay que haber muy bien qué datos son más interesantes para realizar el análisis forense ya que si el investigador decide empezar cargando otros datos, esto le llevará a la herramienta varias horas y si luego esa información no es de interés habrá que empezar de nuevo la extracción de la información.

Autopsy 4.1.1 ofrece también una serie de opciones de gran interés para el investigador. En el ámbito de defensa se suele utilizar bastante la opción de timeline ya que genera un gráfico bastante fácil de entender de todos los movimientos de datos que ha sufrido el dispositivo analizado. Además se pueden ver los movimientos por años, meses, días e incluso horas. Esto es de gran interés para las unidades de guerra electrónica, ya que aparte de buscar toda la información posible también es de gran interés observar los picos de transferencia de información o llamadas telefónicas.

Como última característica de interés para realizar los análisis forenses, Autopsy 4.1.1 ofrece la posibilidad de generar los informes. Puede hacer 6 informes, de los cuales destacan el de informe de HTML (compatible con cualquier navegador web), los resultados mostrados en un fichero Excel y un informe incluyendo las coordenadas de donde se ha encontrado el teléfono móvil que al abrirlo se ejecutará GOOGLE EARTH y automáticamente se cargarán las coordenadas, mostrando al investigador las ubicaciones del teléfono móvil.

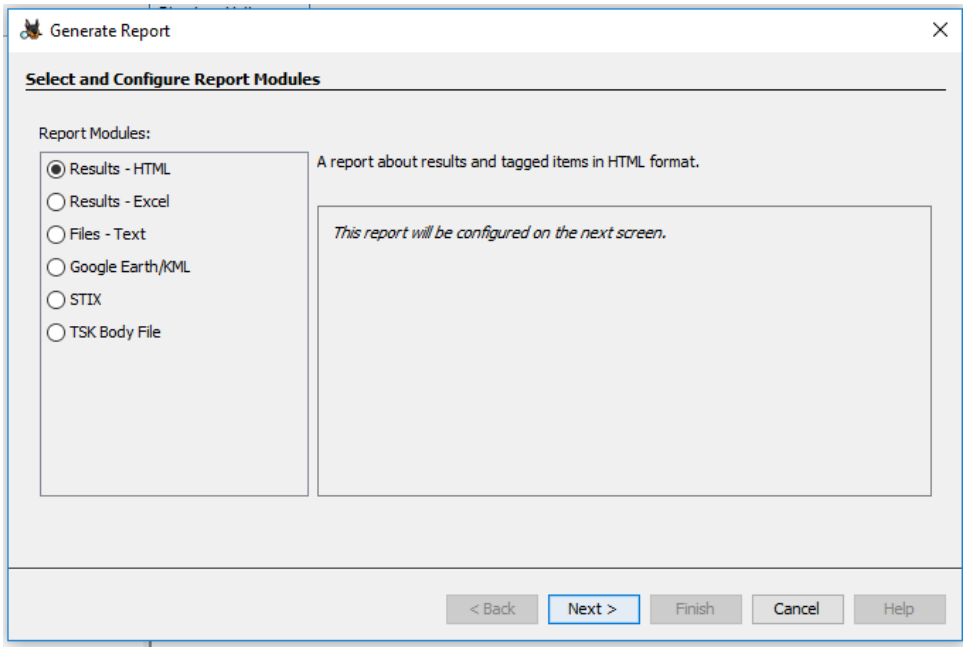


Ilustración 27 Informes Autopsy 4.1.1.

5.2.1 Extracción de la información Autopsy 4.1.1.

Para realizar el análisis forense se ha creado una imagen del teléfono móvil y posteriormente se ha procedido al análisis realizado por Autopsy 4.1.1. El tiempo necesario para realizar la extracción ha sido de 1 hora 40 minutos. La información que se ha extraído se puede apreciar en la ilustración 28.

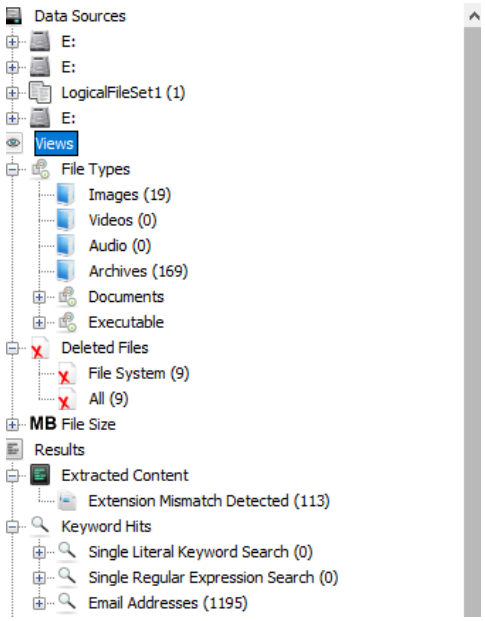


Ilustración 28 Información Análisis Autopsy 4.1.1.

Una vez extraído la información se ha procedido a generar los informes forenses de HTML y de coordenadas GPS. De esta manera Autopsy genera una serie de listas donde incluye los correos electrónicos, números de teléfono y coordenadas GPS. El informe de coordenadas lo vincula con GOOGLE EARTH, donde GOOGLE EARTH carga la base de datos generada por Autopsy y muestra las coordenadas.

5.2.2 Informe análisis forense Autopsy 4.1.1.

En base al caso de estudio se ha obtenido la siguiente información:

Las características del teléfono móvil son las siguientes:

Marca	Sony Ericsson
Sistema Operativo (S.O.)	Android
Versión S.O.	2.3.4
IMEI	35----------
Número modelo	MT11i
Número de teléfono	(+034) 626------

Tabla 1 Características Teléfono Móvil.

A continuación se detallan los apartados que tienen interés para el caso de estudio.

Llamadas

No se ha podido extraer ningún registro de llamadas.

Correos electrónicos

La cuenta de correo electrónico que utiliza el dispositivo es ----------@gmail.com, Se han encontrado un total de 1195 cuentas de correo. En este caso Autospy 4.1.1 agrupa todas las cuentas de correo, ya sean de Gmail, Hotmail, Whatsapp, etc. Además, el programa muestra información detallada del correo: destinatario, fecha de emisión, etc.

Ilustración 29 Correos electrónicos Autopsy 4.1.1

Contactos

La base de datos que se ha analizado del teléfono móvil contenía los siguientes contactos

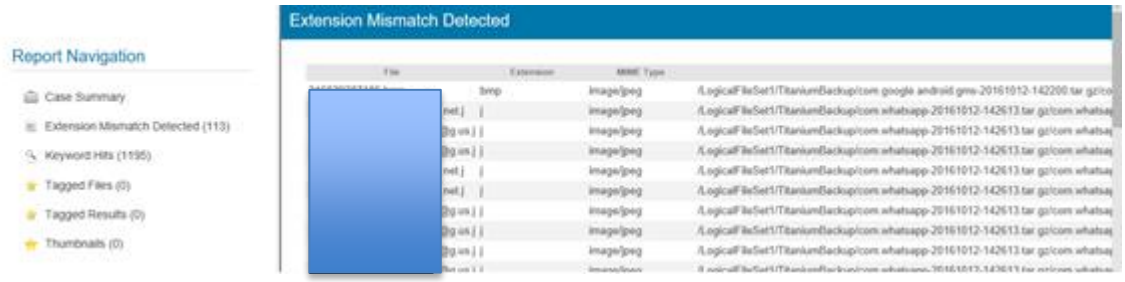


Ilustración 30 Contactos análisis forense Autopsy 4.1.1.

Coordenadas

Las coordenadas que ha mostrado el análisis sólo corresponden a una imagen. La dirección corresponde con un barrio a las afueras de Madrid con coordendas: -- --- ----------

Ilustración 31 Coordenadas Autopsy 4.1.1.

Imágenes

Las imágenes que se han encontrado que resulten de interés son las asociadas a los contactos telefónicos. Un total de 113 contactos telefónicos llevan asociadas imágenes (ilustración 32).

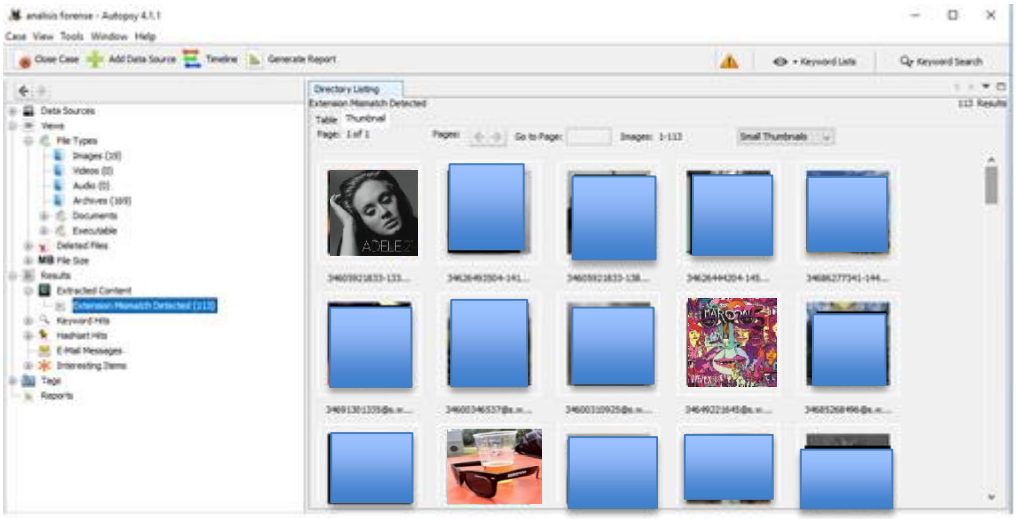


Ilustración 32 Imágenes Autopsy 4.1.1.

Mensajes

No se han podido extraer ningún mensaje.

Conversaciones

No se han podido extraer ninguna conversación.

Movimiento de datos.

El movimiento de los datos en el teléfono móvil se concentra principalmente en los años 2012,2013 y 1016. También hay movimiento de datos en el año 2008, aunque probablemente esto es debido a una mala configuración del teléfono móvil con la fecha.

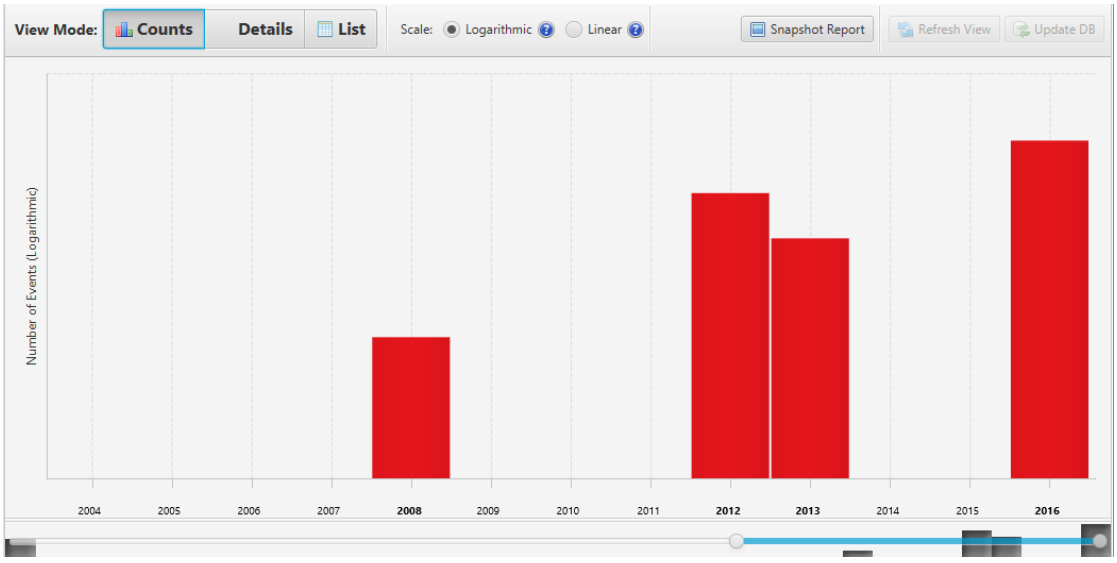


Ilustración 33 Timeline Autopsy 4.1.1.

Comparación de Resultados

Respondiendo a las pruebas mostradas anteriormente, los resultados de las extracciones con Autopsy 4.1.1 y UFED TOUCH son los siguientes:

	UFED TOUCH	Autopsy 4.1.1
Tiempo en realizar la extracción	41 minutos	100 minutos
Llamadas	549	0
Correos electrónicos (emails)	74	0
Contactos	1067	113
Coordenadas GPS	92	1
Imágenes	940	113
Mensajes	1225	0
Conversaciones	440	0
Movimiento de datos	Incluye gráfica	Incluye gráfica
Precio	10000	Gratuito
Información extraída	Memoria Interna y externa	Memoria externa
Tipo de clonación	Clonación hardware	Clonación software

Tabla 2 Resultados.

En cuanto a la facilidad de manejo para operar, UFED TOUCH ofrece una interfaz bastante intuitiva. Solamente basta con seguir los pasos que van saliendo en la pantalla y se podrá realizar la extracción de manera muy fácil, proporcionado cables compatibles con los dispositivos móviles a analizar. Sin embargo, Autopsy 4.1.1 puede dar mayores dificultades si se quieren analizar móviles antiguos, ya que dependerá de un conector válido para el ordenador ya que si el ordenador no identifica el móvil Autopsy 4.1.1 no podrá acceder a la información.

Los costes asociados a cada herramienta son muy dispares. UFED TOUCH tiene un valor aproximado de 10000 euros, mientras que Autopsy 4.1.1 tiene un coste gratuito. Sin embargo, las prestaciones que ofrece UFED TOUCH son muy buenas y necesarias si se quiere llevar a cabo un análisis forense completo y sobre todo si el análisis quiere ser presentado ante un tribunal.

Con estos resultados se observa que UFED TOUCH supera en gran medida a la herramienta gratuita Autopsy 4.1.1. UFED TOUCH ha realizado una extracción física y ha podido extraer toda la información que se pedía en el caso (ANEXO C), mientras que Autopsy 4.1.1 ha realizado una extracción de sistema de archivos y la información extraída ha sido bastante reducida. Además UFED TOUCH ha extraído toda la información 59 minutos más rápido que Autopsy 4.1.1, algo esencial para llevar a cabo operaciones de inteligencia, donde prima la rapidez. Cabe destacar que UFED TOUCH ha extraído toda la información de la memoria interna y externa del teléfono móvil, mientras que Autopsy 4.1.1 sólo ha extraído la información de la memoria externa. De ahí a la gran diferencia en muchos datos.

Aunque el caso solamente pedía extraer llamadas, emails, contactos, coordenadas GPS, imágenes, mensajes, conversaciones y una gráfica de movimiento de datos, UFED TOUCH podía haber dado mucha información. De hecho en la ilustración 15 aparece toda la información que ha podido extraer, como puede ser la obtención de contraseñas, cookies, cuentas de usuario, etc.

Conclusiones

Los análisis forenses se llevan a cabo siguiendo unas pautas ya definidas. No es necesario tener un gran conocimiento previo para realizar estos análisis ya que siguiendo la metodología explicada se puede realizar un análisis forense sin ningún tipo de problema.

El principal problema es el disponer de las herramientas adecuadas para llevar a cabo estos análisis ya que si se pretende presentar la prueba ante un tribunal se debe de disponer de UFED TOUCH. Las otras herramientas gratuitas, como el programa Autopsy 4.1.1, pueden ser utilizadas para fines personales como el recuperar información eliminada, como una foto, un contacto, etc.

Los productos analizados en este trabajo muestran diferencias muy claras. El primero, UFED TOUCH, demuestra que es una de las mejores herramientas para realizar análisis forense. Ha sido capaz de extraer toda la información que se pedía así como incluso mucha más información que no ha sido analizada. Además la extracción se ha podido hacer en el tiempo pedido por el informe. El único problema es que la licencia es muy cara. El segundo, Autopsy 4.1.1, es una herramienta bastante útil para el análisis forense pero la información que extrae no es suficiente con respecto a lo que se pedía. Además el tiempo para extraer la información es muy elevado. De esta manera aunque la licencia de UFED TOUCH sea muy cara es completamente necesario disponer de tal licencia para poder llevar a cabo análisis forenses en Defensa.

Tanto el marco legal como la normativa que se muestra en este trabajo sólo es válida si el análisis forense se lleva a cabo en España. Si la investigación se realiza en otros países el investigador deberá regirse las leyes vigentes en esos países.

La empresa encargada de vender el sistema operativo Android está continuamente lanzando actualizaciones de este sistema operativo para poder corregir los errores que tiene. De esta manera los analistas forenses se enfrentan a constantes desafíos ya que con cada actualización es más difícil acceder a la extracción de la información.

Por último, los análisis forenses es una tarea que actualmente está adquiriendo bastante importancia en el ámbito de Defensa. Prueba de ello es la reciente creación del Mando Conjunto de Ciberdefensa, dónde actualmente uno de los aspectos en los que se está centrando la instrucción del personal es a la realización de análisis forenses. De hecho, se está destinando mucho dinero a la adquisición de UFED TOUCH ya que se está convirtiendo en una herramienta indispensable en Territorio de Operaciones.

Bibliografía

[1]2016. [Online]. Available: https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf. [Accessed: 09- Oct- 2016].

[2]Tendencias 2014: El desafío de la privacidad en Internet, 1st ed. ESET, 2014.

[3]"Yahoo sufre "uno de los mayores ataques informáticos de la historia" con el robo de información de unos 500 millones de cuentas de sus usuarios - BBC Mundo", BBC Mundo, 2016. [Online]. Available: http://www.bbc.com/mundo/noticias-internacional-37444591. [Accessed: 22- Oct- 2016].

[4]"Cómputo forense", Es.wikipedia.org, 2016. [Online]. Available: https://es.wikipedia.org/wiki/C%C3%B3mputo_forense. [Accessed: 13- Sep- 2016].

[5]"Android", *Android*, 2016. [Online]. Available: https://www.android.com/intl/es-419_mx/. [Accessed: 22- Oct- 2016].

[6]"Cellebrite - UFED Physical Analyzer", *Cellebrite.com*, 2016. [Online]. Available: http://www.cellebrite.com/es/Mobile-Forensics/Applications/ufed-physical-analyzer. [Accessed: 22- Oct- 2016].

[7]"Metodología para un análisis forense", 2014. [Online]. Available: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39681/6/cgervillarTFM1214memoria.pdf. [Accessed: 12- Oct- 2016].

[8]"Los dispositivos móviles", 2016. [Online]. Available: https://www.incibe.es/extfrontinteco/img/File/empresas/kit_concienciacion/Pildoras_informativas/incibe_presentacin_4__los_dispositivos_mviles__texto.pdf. [Accessed: 22- Oct- 2016].

[9]GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-453) SEGURIDAD DE DISPOSITIVOS MÓVILES: ANDROID, 1st ed. 2013.

[10]R. Tamma and D. Tindall, Learning Android forensics, 2015.

[11]"Descubren una nueva vulnerabilidad que pone en riesgo a 900 millones de dispositivos Android", *abc*, 2016. [Online]. Available: http://www.abc.es/tecnologia/moviles/telefonia/abci-descubren-nueva-vulnerabilidad-pone-riesgo-900-millones-dispositivos-android-201608081307_noticia.html. [Accessed: 22- Oct- 2016].

[12]"Google Android : CVE security vulnerabilities, versions and detailed reports", *Cvedetails.com*, 2016. [Online]. Available: http://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224. [Accessed: 22- Oct- 2016].

[13]"Autopsy: Download", *Sleuthkit.org*, 2016. [Online]. Available: http://www.sleuthkit.org/autopsy/download.php. [Accessed: 15- Oct- 2016].

[14]"Autopsy User Documentation: Autopsy User's Guide", Sleuthkit.org, 2016. [Online]. Available: http://www.sleuthkit.org/autopsy/docs/user-docs/4.0/. [Accessed: 08- Oct- 2016].

[15]"Título I. De los derechos y deberes fundamentales - Constitución Española", Congreso.es, 2016. [Online]. Available: http://www.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=18&tipo=2. [Accessed: 13- Sep- 2016].

[16]"Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. TíTULO PRELIMINAR.Del Poder Judicial y del ejercicio de la potestad jurisdiccional.", Noticias Jurídicas, 2016. [Online]. Available: http://noticias.juridicas.com/base_datos/Admin/lo6-1985.tp.html. [Accessed: 14- Sep- 2016].

[17]"Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (Vigente hasta el 13 de Noviembre de 2015).", Noticias Jurídicas, 2016. [Online]. Available: http://noticias.juridicas.com/base_datos/Laboral/rdleg1-1995.html. [Accessed: 16- Sep- 2016].

[18]"ISO/IEC 27037:2012 - Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence", ISO, 2012. [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=44381. [Accessed: 26- Sep- 2016].

[19]"RFC 3227 - Guidelines for Evidence Collection and Archiving", Rfc-base.org, 2016. [Online]. Available: http://www.rfc-base.org/rfc-3227.html. [Accessed: 27- Sep- 2016].

[20]"AENOR: Norma UNE 71505-1:2013", Aenor.es, 2016. [Online]. Available: http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051411#.V_TvRyiLTIV. [Accessed: 27- Sep- 2016].

[21]"AENOR: Norma UNE 71506:2013", Aenor.es, 2016. [Online]. Available: http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051414#.V_TvgSiLTIU. [Accessed: 09- Oct- 2016].

[22]A. Dalvik, "ART and Dalvik | Android Open Source Project", Source.android.com, 2016. [Online]. Available: https://source.android.com/devices/tech/dalvik/. [Accessed: 09- Oct- 2016].

ANEXOS

ANEXO A Marco Legal y normativo de la informática forense.

1- Ámbito constitucional (Constitución Español).

Lo recogido en el Artículo 18 de la Constitución Española, en los puntos 18.1, 18.2, 18.3 y 18.4 en los que se establece en términos generales el derecho a la intimidad y la honorabilidad personal y familiar así como de la imagen de los ciudadanos, contemplando para ello la Inviolabilidad del Domicilio (18.2) y especial referencia al secreto de las Comunicaciones (18.3). Así mismo, se incorpora el apartado 18.4 en el que se especifica que:

"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

Siendo este último apartado el que determine como se ha de realizar la actividad forense dentro de los términos de Legalidad. [13]

2- Ámbito Jurídico (Ley Orgánica del Poder Judicial).

En éste apartado y siguiendo el hilo del Artículo 18.4 de la Constitución Española citado en el punto anterior, se tiene la L.O.P.J., establece en su Artículo 11, Punto Primero que:

"En todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales."

Es decir, el procedimiento para la obtención de las pruebas ha de GARANTIZAR SIEMPRE, que no se ha "invadido el espacio de privacidad del individuo" recogido en las Leyes Españolas o no contempladas en el Auto del Juez que solicita la investigación. [14]

3- Ámbito Jurídico (Código Penal, LO. 1/2015, LO 2/2015 y L 4/2015 Actualizadas).

En lo que respecta a la aplicación del Código Penal (C.P.) sobre las actividades forenses en cuanto a la adquisición de evidencias digitales, tan solo decir la importancia de que los métodos y herramientas de adquisición/tratamiento y análisis se han de aplicar sin vulnerar ninguna de las leyes anteriormente citadas y que en el caso del Código Penal Español, el marco sancionador se encuentra definido en los Artículos 197 y 264 y que dichos artículos han sido actualizados en la reforma del Código Penal de Marzo de 2015.

4- Ámbito Laboral. (Estatuto de los Trabajadores).

En este ámbito, tan solo existen dos artículos que pueden afectar a la intervención de recursos informáticos y/o digitales (Ordenadores, cuentas de correo electrónico, etc.), y serían:

Artículo 18. Inviolabilidad de la persona del trabajador [15].

Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los

demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible.

Sin embargo, hay sentencias del T.S.J. (Tribunal Superior de Justicia), que claramente especifica que los ordenadores estarían fuera de ese grupo denominado "efectos personales" considerando que:

"El ordenador es un instrumento de producción del que es titular el empresario como propietario o por otro título y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen."

Artículo 20. Dirección y control de la actividad laboral [15].

1. El trabajador estará obligado a realizar el trabajo convenido bajo la dirección del empresario o persona en quien éste delegue.

2. En el cumplimiento de la obligación de trabajar asumida en el contrato, el trabajador debe al empresario la diligencia y la colaboración en el trabajo que marquen las disposiciones legales, los convenios colectivos y las órdenes o instrucciones adoptadas por aquél en el ejercicio regular de sus facultades de dirección y, en su defecto, por los usos y costumbres. En cualquier caso, el trabajador y el empresario se someterán en sus prestaciones recíprocas a las exigencias de la buena fe.

3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.

4. El empresario podrá verificar el estado de enfermedad o accidente del trabajador que sea alegado por éste para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones

Estos dos artículos estarían cubiertos por lo tanto por tres medidas:

- Por la autorización firmada del usuario frente a una intervención de su equipo y/o de su cuenta de correo electrónico (Autorización para intervención forense).
- Por la existencia de AVISO ESCRITO de las medidas de vigilancia en el recurso de la empresa utilizado por la persona (El usuario).
- Por la existencia de clausula sobre la utilización de los recursos informáticos empresariales cedidos al trabajador (El usuario), y las medidas establecidas por la empresa para la vigilancia y el control del buen uso de éstas para su fin productivo

5- Ámbito Personal. (LOPD)

En este apartado se expondrán las Normas tanto de adquisición como de análisis forense:

SO/IEC 27037: Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. [16]

Documento que publicó la Organización Internacional para la Estandarización (ISO), proporciona directrices para actividades periciales en el escenario de la identificación, recolección, adquisición y preservación de la evidencia digital como medio probatorio. Utiliza procedimientos disciplinarios para facilitar el intercambio de la evidencia entre jurisdicciones y orienta a las personas en todo el proceso de manipulación de dicha evidencia.

➢ RFC 3227: Guidelines for Evidence Collection and Archiving. [17]

Proporciona a los administradores de sistemas directrices para la recopilación y archivo de las pruebas en un incidente de seguridad. Cuando la recopilación de pruebas se realiza de forma correcta, se evita graves errores y facilita la detección del atacante, lo que permite, aumentar en gran proporción la posibilidad de admitir el caso a un proceso judicial.

➢ UNE 71505: Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales. [18]

Los logs de actividades proporcionan información sobre los sucesos en un sistema de información. La parte frágil de los logs es la demostración que los hechos no se han alterado en la cadena de custodia. Define y describe conceptos de seguridad que se relacionan con la evidencia, identifica las relaciones entre el Sistema de Gestión de Evidencias Electrónicas (SGEE) y el Sistema de Gestión de Seguridad (SGSI), especifica controles de seguridad a la gestión de evidencias.

➢ UNE 71506: Tecnologías de la Información (TI). [19]

Metodología para el análisis forense de las evidencias electrónicas. [4] Esta norma define los procesos para el análisis forense dentro del ciclo de gestión de evidencias electrónicas. Completa los procesos que conforma la Norma UNE 71505 a cerca del Sistema de Gestión de Evidencias Electrónicas.

ANEXO B Arquitectura del sistema operativo Android.

Kernel de Linux

El kernel de Android o núcleo está formado por el sistema operativo Linux versión 2.6. Esta capa proporciona muchos servicios entre los cuales se encuentran la seguridad, el manejo de la memoria, el multiproceso, la pila de protocolos y el soporte de drivers para dispositivos. Es el responsable de facilitar la posibilidad de que los distintos programas tengan acceso al hardware de forma segura. Además, debido a que hay muchos programas que quieren acceder al hardware y el acceso al hardware es limitado, el kernel se encarga de decidir de dar la prioridad a un programa a acceder a un dispositivo del hardware y por un tiempo limitado, lo que se conoce como multiplexado.

Esta capa actúa como la capa de abstracción entre el hardware y el resto de la pila. Para acceder directamente al hardware se necesita de un proceso muy complejo, por lo que los núcleos suelen implementar una serie de abstracciones del hardware. Mediante estas abstracciones el acceso al hardware es más fácil y facilita el trabajo al programador.

Cuando se emplea una HAL (capa de abstracción de hardware), los programas o aplicaciones no acceden directamente al hardware, sino que acceden a la capa provista por la HAL y acceden al hardware mediante software.

Android Runtime (ART)

En el sistema operativo Android no es posible ejecutar una máquina virtual Java estándar debido a las limitaciones del sistema operativo (poca memoria y procesador limitado). Por ello Google creó una nueva máquina virtual que fuera similar a Java pero que respondieran a las limitaciones del sistema operativo. Esta máquina virtual es virtual Dalvik [20]. Aparte de esta máquina virtual en esta capa se encuentran multitud de clases java, que junto con la máquina virtual Dalvik forman las LibreriasCore.

Debido a la necesidad de ejecutar varias máquinas virtuales a la vez en los nuevos smartphones la máquina virtual Dalvik se quedó obsoleta. Como solución a este problema Google decidió sustituir Dalvik por una nueva máquina virtual denominada ART.

Las principales mejoras de ART con respecto a la anterior máquina virtual son:

- *Compilation Ahead-of-time (AOT):* mejora la rapidez de las aplicaciones debido a que durante la instalación realizara una pre-compilación, lo que permite realizar una pequeña carga de datos y esto permitirá que las tareas de inicio o de cierre sea mucho más rápida. Esto permite reducir los tiempos de uso de la CPU y por lo tanto aumenta el rendimiento de la batería.

- *Mejoras en el recolector de basura:* La recolección de basura (GC) puede perjudicar el rendimiento de una aplicación, lo que puede resultar la pantalla entrecortada, baja reacción de interfaz de usuario, y otros problemas. Esto se soluciona con medidas como realizar una pausa en vez de dos que realiza el recolector de basura, durante el tiempo en que tarde en completar una tarea.

- *Mejoras en el desarrollo y depuración de aplicaciones.*

Librerías

En esta capa se incluyen un conjunto de librerías en C/C++ que se usan en varios componentes de Android. Esta capa se encuentra por encima del Kernel para proveer una interfaz de programación (API) unificada para que pueda acceder a las necesidades que el kernel provee. Muchas librerías utilizan proyectos de código abierto. Entre las múltiples librerías que hay se destacan:

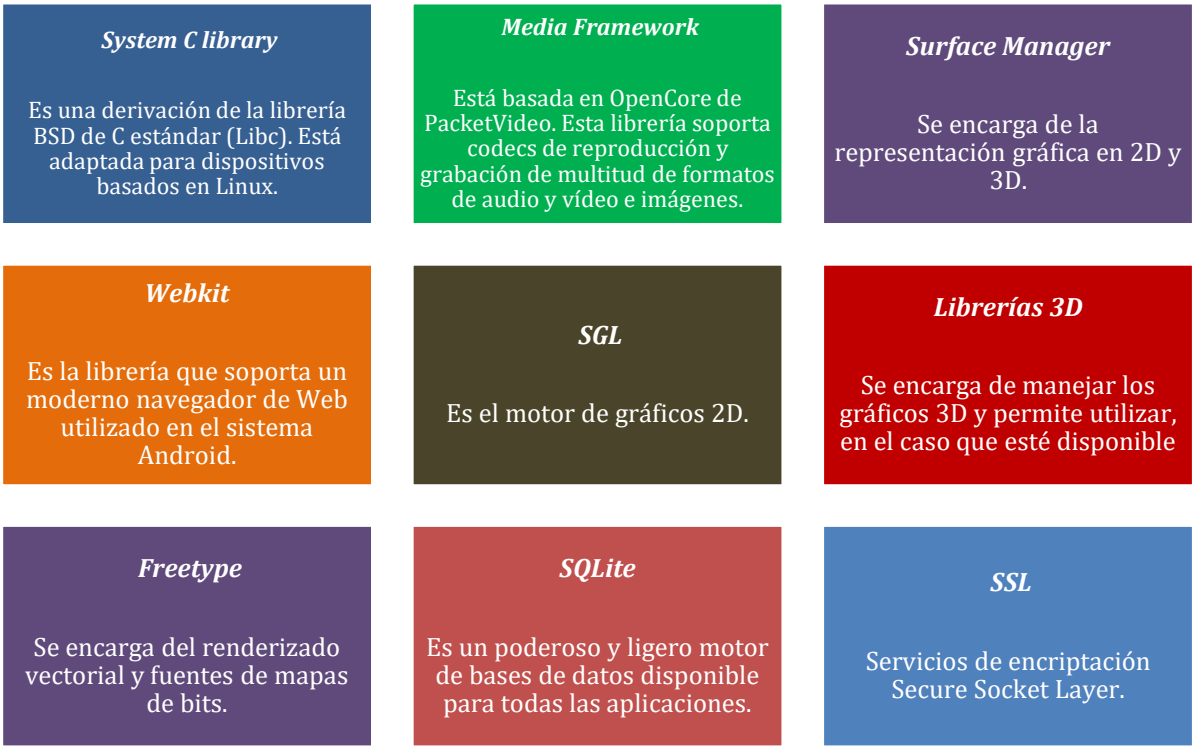


Ilustración 34 Librerías Sistema Operativo Android.

Armazón de aplicaciones

En esta capa se encuentran los recursos necesarios para que las aplicaciones puedan funcionar correctamente y sepan interpretar comandos en Android. Todas las aplicaciones que se vayan a usar en el sistema operativo Android utilizan el mismo conjunto de API y el mismo framework, representado en este nivel.

Los servicios más importantes que proporciona este nivel son:

- Views: es la parte visual de los componentes.
- Resource Manager: cuando los recursos no son en códigos este servicio proporciona su acceso.
- Activity Manager: gestiona el ciclo de actividades de las aplicaciones. Un componente activity refleja una determinada acción llevada a cabo por una aplicación. Debido a que una aplicación permite la ejecución de varias acciones, estas acciones se llevan a cabo por una ventana independiente y a su vez cada una de esas ventanas es representada a través de una componente activity. De esta manera se puede lanzar una actividad o dormir otra.

- Notification Manager: mediante un mismo formato comunica al usuario las diferentes notificaciones o eventos que ocurran durante su ejecución: una llamada entrante, conexión Wi-Fi disponible, etc.

- Content Providers: mediante este componente las aplicaciones pueden almacenar información en un fichero o en cualquier otro formato que considere y compartir esta información con otras aplicaciones.

Aplicaciones.

En esta capa se encuentran todas las aplicaciones que tiene el dispositivo. Estas aplicaciones pueden ser bien las que vienen por defecto en el sistema operativo o las que el usuario se haya descargado. Todas estas aplicaciones se tienen que ejecutar a través de la máquina virtual ART para garantizar la seguridad del sistema.

ANEXO C Entrevista a personal experto.

Con esta entrevista se pretende obtener la mayor información posible acerca de los procedimientos de análisis forenses llevados a cabo por la unidad de Guerra Electrónica. Se le ha preguntado al entrevistado por diferentes puntos que resultan de interés para la investigación.

La entrevista ha constado de las siguientes preguntas:

¿Qué herramientas suelen utilizar, además del UFED TOUCH, para realizar análisis forenses informáticos de Android cuando despliegan en territorio de operaciones?

¿Cuál es el procedimiento a seguir para realizar el análisis forense?

¿Qué tipo de información se busca cuando se realizan análisis forense en territorio de operaciones?

¿Cuál es su opinión personal acerca de las herramientas empleadas por Ciberdefensa?, ¿Propondría utilizar otro tipo de herramientas?

ANEXO D Caso ficticio de estudio.

El día 06 de Octubre del 2016 ,tras haber realizado un reconocimiento por el itinerario marcado según Orden de Operaciones, un equipo de Ciberdefensa encuadrado en el Batallón de Guerra Electrónica nº31 encontró un teléfono móvil que podría ser de algún sospechoso. Según inteligencia en un radio de 200 m donde se encontró el teléfono móvil se están llevando a cabo numerosos ataques terroristas así como tráfico ilegal de armas.

Se trata de un teléfono móvil de la marca Sony Ericsson neo v, aparentemente en buen estado.

La misión que se le encomienda al equipo de Guerra Electrónica es obtener toda la información posible que pudiera resultar de gran valor para evitar posibles ataques terroristas tanto a la base en la que se encuentra desplegada la unidad como los posibles ataques que pudieran sufrir los convoyes. Además esta información sería crucial disponer de ella en la mayor brevedad posible ya que según Inteligencia en las próximas 8-10 horas hay muchas posibilidades de que grupos terroristas ataquen contra la base o pudieran explosionar algún tipo de mina.

La información que se espera obtener del teléfono móvil es la siguiente:

- Llamadas.
- Correos electrónicos.
- Contactos.
- Coordenadas GPS.
- Imágenes.
- Mensajes.
- Conversaciones.
- Movimiento de datos.

ANEXO E Tipos de extracciones de UFED TOUCH.

De acuerdo a la información consultada en la página principal de UFED [8] la definición de extracción lógica, de sistema de archivos y física es:

Extracción lógica

La extracción lógica de datos es la que menos información puede obtener. Esta extracción se lleva a cabo mediante la API (Interfaz de programación de aplicaciones) que es específica del dispositivo. Cuando UFED se conecta al dispositivo carga el API específico del dispositivo para poder llevar a cabo la extracción lógica. Una vez conectada y cargada el API, UFED hace llamadas API de solo lectura para solicitar la información del dispositivo. Tras esto, el dispositivo responde a estas llamadas y de esta manera se puede extraer la información demandada por UFED. Mediante este proceso se permite la adquisición de la mayor parte de los datos en vivo del dispositivo, en un formato legible y de forma válida a nivel forense.

Los tipos de datos incluyen contraseñas, registros de llamadas, registro de llamadas eliminados de la SIM, información del teléfono (IMEI/ESN), registros de la libreta de teléfonos, SMS, imágenes, videos, archivos de audio, datos de apps de dispositivos Android, etc. En la mayoría de los casos, no es posible realizar extracción lógica de dispositivos bloqueados.

El método de extracción lógica es el más fácil de realizar para la herramienta, ya que tiene limitaciones de la cantidad de datos que puede extraer, al contrario de los métodos de extracción físicos.

Extracción de sistema de archivos

La extracción de sistema de archivos es la adquisición de los archivos incorporados en la memoria de los dispositivos móviles.

Obtiene acceso a todos los archivos existentes en la memoria del dispositivo móvil, incluyendo imágenes, videos, archivos de base de datos, archivos del sistema y registros. La mayoría de las aplicaciones incorporadas y del usuario almacenan los datos en estos archivos de bases de datos. Al llevar a cabo una extracción de sistema de archivos, se puede tener acceso a datos tales como contraseñas, datos de apps, información del directorio telefónico, registro de llamadas, mensajes y espacio sin asignar.

El espacio sin asignar es de donde se pueden recuperar los datos eliminados y ocultos, incluyendo datos de apps, historial web, datos EXIF de las imágenes y datos del sistema. El acceso total a la base de datos permite recuperar los registros eliminados de estos archivos.

Extracción física

La extracción física obtiene la información del dispositivo móvil realizando una copia bit por bit de toda la memoria flash. Gracias a este método de extracción permite adquirir los datos intactos, así como los datos ocultos o que han sido eliminados.

Los datos eliminados pueden ser recuperados en dos niveles: El primer nivel es el sistema de archivos y el segundo nivel es la recuperación de información eliminada de los archivos de bases de datos. En el primer nivel durante el proceso de reconstrucción del sistema de archivos,

en ocasiones es posible recuperar los archivos eliminados. En el segundo nivel se puede recuperar información eliminada ya que en algunos archivos de bases de datos que se pueden encontrar en los teléfonos inteligentes, es posible recuperar los registros eliminados, tales como los registros de llamadas, contactos, mensajes, etc.

Nota: el segundo nivel de recuperación también se puede llevar a cabo en una extracción de sistema de archivos.

Los tipos de datos compatibles que se obtienen usando la extracción física incluyen las contraseñas intactas y eliminadas, las aplicaciones instaladas, geo etiquetas, los archivos de medios tales como fotografías y videos tomados por el usuario, las posiciones de GPS, los correos electrónicos, los chats y mucho más.

Los gestores de arranque personalizadas con frecuencia se desarrollan durante este proceso para extraer la información almacenada en el dispositivo, y con frecuencia omitir los bloqueos de usuario o los códigos de acceso. Estos gestores de arranque son desarrollados exclusivamente por Cellebrite y son los únicos que incluyen funcionalidad de solo lectura, asegurando que los datos se extraigan de los dispositivos móviles de forma válida a nivel forense.

Esta investigación se centra en el sistema Android, por lo tanto se puede acceder a cualquier tipo de información.

ANEXO F Crear una imagen a través de FTK Imager Lite.

El modo de crear una imagen a través de este programa es bastante fácil e intuitivo. Con solo un par de pasos podemos crear la imagen con la que posteriormente se puede trabajar para analizar el contenido.

Primeramente se selecciona la opción de Create Disk Image, que se encuentra arriba a la izquierda, como muestra la ilustración 34.

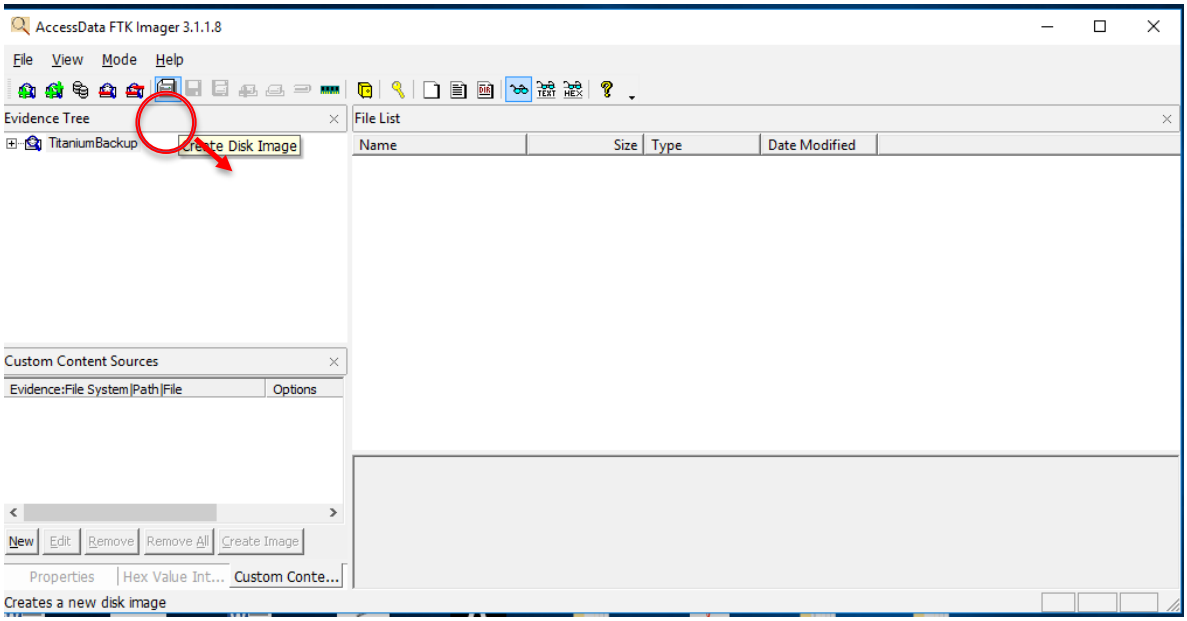


Ilustración 35 Crear Imagen de Disco FTK Imager

A continuación se selecciona donde está ubicada la fuente de datos donde se quiere extraer la información (ilustración 35). Se puede elegir entre unidad física (Physical Drive), unidad lógica (Logical Drive), archivo de imagen (Image File), contenido de una carpeta (Contents of a Folder) o un CD/DVD (Fernico Device).

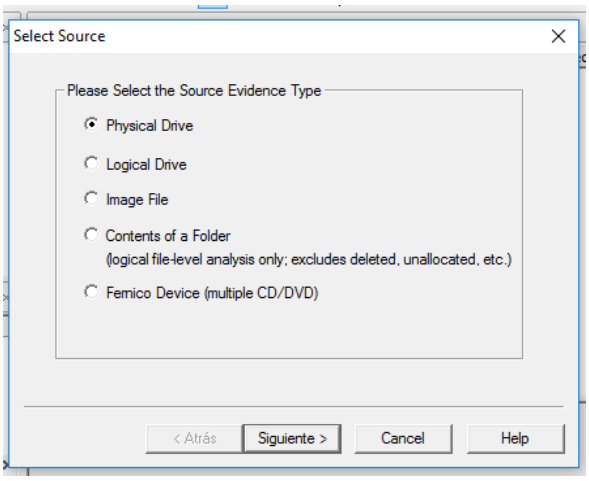


Ilustración 36 Selección de la fuente FTK Imager

Posteriormente el programa empezará a realizar la imagen (ilustración 36). Este proceso tardará dependiendo de la carga de información.

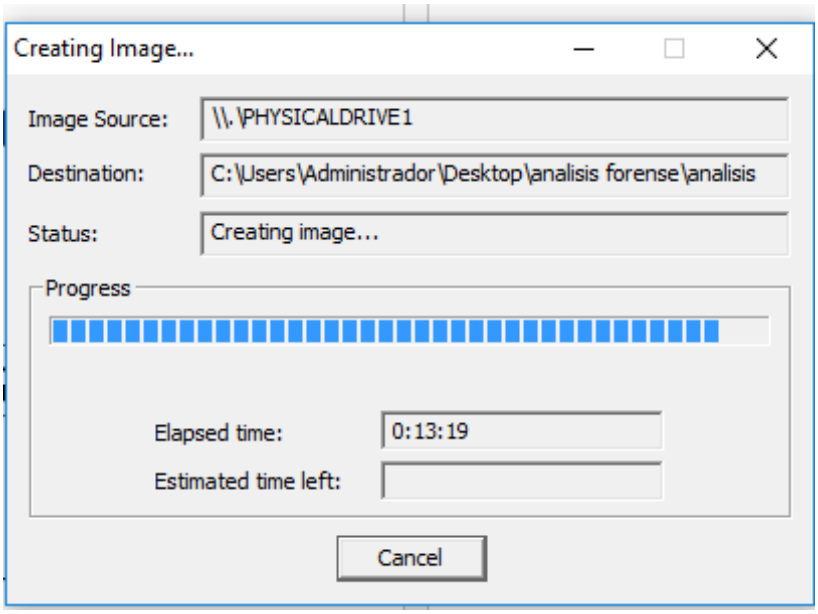


Ilustración 37 Creacción de la Imagen FTK Imager

Finalmente el programa crea una imagen que la guardará donde anteriormente el usuario lo haya especificado. Es interesante la tabla que muestra una vez finalizada la imagen (ilustración 37) ya que muestra lo Hash tanto del disco original como el de la imagen. Esto permite asegurarse de que la imagen es una copia de la original.

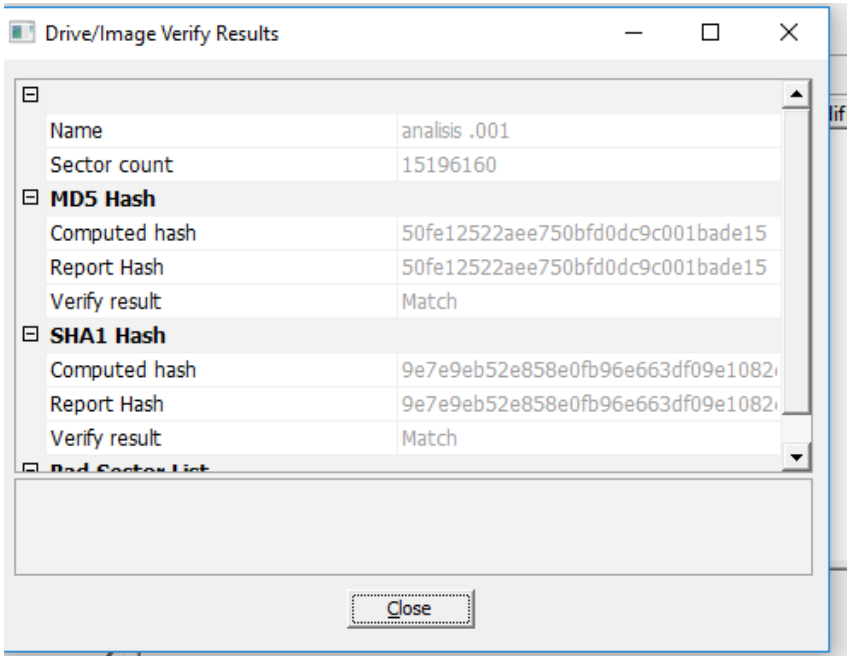


Ilustración 38 Verificación de resultados FTK Imager