Universidad de Alcalá
Escuela Politécnica Superior

GRADO EN INGENIERÍA ELECTRÓNICA DE COMUNICACIONES

Trabajo Fin de Grado

Electrónica e informática forense: extracción de evidencias digitales en un teléfono smartphone mediante JTAG, análisis de datos con aplicaciones forenses de software libre.

Autor: Alberto Benegas García

Tutor/es: Pedro Alfonso Revenga de Toro

2020

UNIVERSIDAD DE ALCALÁ
Escuela Politécnica Superior

Grado en Ingeniería Electrónica de Comunicaciones

Trabajo Fin de Grado

Electrónica e informática forense: extracción de evidencias digitales en un teléfono smartphone mediante JTAG, análisis de datos con aplicaciones forenses de software libre.

Autor: Alberto Benegas García

Tutor/es: Pedro Alfonso Revenga de Toro

TRIBUNAL:

Presidente: Alfredo Gardel Vicente

Vocal 1º: Ana Isabel De Andres Rubio

Vocal 2º: Pedro Alfonso Revenga de Toro

FECHA: 6/10/2020

RESUMEN

Actualmente y cada vez más, hay un uso masivo de telefonía móvil por parte de la población. Estos dispositivos almacenan gran cantidad de información personal que podría ser muy útil en una investigación policial, judicial o empresarial.

El análisis forense de estos dispositivos llevando acabo la extracción, análisis y documentación de la información no es sencilla ni inmediata por la gran cantidad de modelos en el mercado, el estado defectuoso en el que se pudieran encontrar y las medidas de seguridad que tienen actualmente.

En este trabajo se pretende proporcionar una visión general de la metodología de investigación y las posibilidades que actualmente ofrece el software libre para llevar a cabo un análisis completo y minucioso de los datos de un dispositivo con tecnología móvil.

PALABRAS CLAVE: telefonía móvil, análisis forense, software libre, Android.

ABSTRACT

Currently, and increasingly, there is a massive use of mobile telephony by the population. These devices store a lot of personal information that could be very useful in a police, judicial or business investigation.

The forensic analysis of these devices carrying out the extraction, analysis and documentation of information is not simple or immediate due to the large number of models on the market, the defective state in which they might be found and the security measures they currently have.

This document try to provide an overview of the research methodology and the possibilities that free software offers to carry out a complete and thorough analysis of the data of a device with mobile technology.

RESUMEN EXTENDIDO

Los dispositivos personales con tecnología móvil se han convertido en los últimos años en una fuente muy completa y fiable de información. Estos terminales almacenan datos personales, cuentas de correo, geolocalización, mensajería, claves y contraseñas, fotografías, etc. El uso de estos aparatos es masivo y continuo por lo que pueden proporcionar una información excelente para esclarecer hechos delictivos en el marco una investigación policial. Además del análisis forense judicial, las mismas herramientas de software libre pueden ser muy útil la recuperación de datos para un empresa o una persona.

El análisis forense no es en muchos casos tarea sencilla. Multitud de modelos distintos, fragilidad de los dispositivos, securización de los datos o problemas de acceso son trabas que pueden impedir o dificultar la extracción de esta información.

Un problema añadido es la posible falta de formación jurídica del experto en tecnología. Para hacer una extracción se deben de adoptar unos procedimientos muy estrictos para que la prueba documental no se vea comprometida en juicio y sea válida y fiable. Por ello, en este trabajo se ha hecho hincapié tanto a la parte legal del análisis como a la parte técnica.

Los siguientes puntos son las claves para el desarrollo del TFG:

1. Metodología de investigación policial.
2. Fases del análisis forense pericial.
3. Descripción de los procedimientos legales.
4. Análisis de las herramientas de software libre para el peritaje forense.
5. Ejercicio práctico de extracción forense de evidencias digitales mediante JTAG.

Índice de contenido

1 INTRODUCCIÓN Y DEFINICIONES

La tecnología en telefonía móvil ha evolucionado de forma vertiginosa en los últimos años, formando ecosistemas en el que el mundo Android y el mundo iPhone son gigantes tecnológicos que están presentes en la vida cotidiana de todas las personas, y en casi todas las facetas (personal, familiar, empresarial, ocio...). También es muy reseñable que España es el país con mayor numero "smartphone" por habitante del mundo junto a Singapur (según la información publicada por BackMarket).

Hay que tener en cuenta que en los teléfonos actuales se almacena información personal, fidedigna y muy valiosa para una investigación policial: historial de navegación, llamadas, fotos, videos, información de redes sociales, localización gps, contactos... Y todo en un único dispositivo.

Un dispositivo de este tipo puede proporcionar una información muy destacable para reconstruir hechos delictivos, y conocer los posibles movimientos y actuaciones tanto de víctimas como de autores. Un perito judicial especialista en informática y electrónica es el encargado de obtener la información válida en un juicio y capaz de desvirtuar la presunción de inocencia de una persona. Es una labor muy compleja que requiere de amplios y actualizados conocimientos técnicos, que requiere una poseer una titulación oficial reconocida como es la de Grado en Ingeniería de Comunicaciones.

1.1 DELITOS TECNOLÓGICOS Y CIBERDELITOS

Es imposible hacer una peritaje informático y electrónico del tipo que sea si no se sabe qué es y qué no es un delito. La labor del investigador es saber qué hay que buscar y qué información es interesante y cual no es relevante para la investigación. Sin embargo, el perito ha de saber unas naciones básicas de legislación penal para saber si en un momento dado se encuentra con un delito o no. También es posible que buscando las evidencias de un delito encuentre las de otro. Ha de saber qué hacer, y como no romper la cadena de custodia, ni desvirtuar las pruebas.

En primer lugar tendremos que distinguir entre los delitos [1] puramente informáticos (crakeo de

licencias, uso de software malicioso) de los demás delitos. Es decir, distinguir entre delitos tecnológicos propiamente dicho, de los delitos que usan la tecnología como instrumento para su comisión. Por ejemplo, un delito de amenazas puede hacerse a través de un mensaje de WhatsApp, pero no deja de ser un delito de amenazas. El problema radica en que se usa un medio virtual (entendido como no tangible) para cometerlo, pero la evidencia es igual de válida que una carta amenazante escrita de puño y letra y enviada por correo postal.

El análisis de los tipos penales sobrepasa, y mucho, la pretensión de este trabajo fin de grado, por lo que haremos una simple enumeración de los delitos exclusivamente informáticos, y los delitos que comúnmente se sirven de la tecnología para su comisión y difusión.

1.1.1 Delitos informáticos

En este apartado enmarcamos los delitos que son propios de la tecnologías para la informática y las comunicaciones. Son delitos informáticos aquellos delitos que no se podrían dar si no se utilizan estas tecnologías.

- Infracciones contra la propiedad intelectual. Aquí tendríamos desde las licencias propietarias de software como las licencias de música, marcas, etc.
- Sabotajes informáticos. Denegación de servicios a webs, daños a los sistemas, revelación de datos personales informáticos, etc.

1.1.2 Delitos que comúnmente se sirven de la tecnología para su comisión

Estos delitos los englobamos como aquellos que no son necesarios para su comisión el uso de la tecnología, pero que gracias a ella se facilita su ejecución. Son delitos comunes pero que se sirven de la informática y las comunicaciones para facilitar la comisión además de dificultar la identificación del autor de los hechos. Muchos de estos delitos se ven agravados por la difusión pública a grupo indeterminado de personas, es decir, difundir en redes sociales e internet. Los más representativos son los siguientes:

- Pornografía infantil.

- Fraudes y estafas.
- Amenazas.
- Delitos de odio.
- Falsedades. De moneda, documentales, servicios de telecomunicación, tarjetas bancarias...
- Calumnias e injurias.
- Ataques contra la intimidad. Acenso y difusión a material audiovisual u otros datos sin consentimiento.

1.2 ANÁLISIS FORENSE

Un análisis forense es una técnica especializada [2] que tiene como fin identificar, preservar y analizar evidencias criminales con las garantías legales suficientes como para poder desvirtuar la presunción de inocencia de un acusado en un juicio. Para ello es fundamental mantener una cadena de custodia intachable.

El análisis forense informático o electrónico no difiere en objetivos con el análisis forense 'clásico' ni en metodología; sin embargo, presenta ciertas particularidades que hay que tener muy en cuenta como la volatilidad de la información, la posibilidad de eliminar pruebas en remoto, o la dificultad de defensa en un juicio ante personal no técnico.

Un análisis o peritaje forense tiene que ser metódico, técnico, fiable, objetivo, exhaustivo y analítico. Y además, cumplir fielmente la legislación vigente.

1.2.1 Fases del análisis forense

Evaluar: autorización, legislación y adquisición

Antes de lanzarnos a realizar el análisis forense en sí hay que hacerse una serie de preguntas. ¿Estamos autorizados a realizar el análisis? ¿Sabemos la legislación aplicable? ¿Realmente se pueden adquirir los datos?

Si hacemos un análisis sin autorización judicial todo lo actuado no tendría valor legal y las evidencias serían consideradas prueba nula. Además de esto, hay que atenerse a la legislación

vigente y tener en cuenta los procedimientos legales para la adquisición y conservación de las evidencias.

Por otro lado, también hay que preguntarse si la información que necesitamos recabar realmente se puede adquirir y conservar. Pues quizás sea información volátil que ya no esté disponible, o datos encriptados de imposible desencriptación.

Adquirir: investigación, recopilar datos y archivar

Una vez que tenemos autorización y en el marco de una investigación el juez nos nombra como peritos para la causa, es la hora de recopilar los datos y almacenarlos.

Para ello, existe un documento estándar para la adquisición de evidencias digitales, el RFC3227. Existen muchos RFC «Request For Comments». Los RFC son documentos que recogen propuestas de expertos en una materia concreta, con el fin de establecer una serie de pautas para llevar a cabo un proceso, la creación de estándares o la implantación de algún protocolo. El RFC 3227 es un documento que recoge las directrices para la recopilación de evidencias y su almacenamiento.

Sin entrar en detalles, el documento nos da pautas de cómo recolectar evidencias (por orden de volatilidad, acciones a evitar, consideraciones de privacidad, procedimientos de recolección), y también procedimientos de almacenamiento (cadena de custodia, dónde almacenar la información y cómo, herramientas necesarias...)

Analizar: datos (red, host, hardware), almacenamiento

Una vez que hemos recogido todos los datos respetando la cadena de custodia, es hora de analizarlos. Esto es, sacarle la información útil y que realmente necesitamos para el fin propuesto de la investigación, habrá mucha que no nos interese para la causa.

En este caso, además de extraer la información para que sea fácilmente consultada (importante la organización y la presentación de la información), hay que clasificarla como relevante o no para el delito concreto que se está buscando (no se puede analizar a ver qué hay, tiene que estar más o menos definido lo que se espera encontrar). Por este motivo, la coordinación con el personal investigador es crucial. Puede ser que un dato que para el técnico es irrelevante, para el investigador

no lo es. Por ejemplo, una fotografía de un individuo que está de vacaciones con unos amigos puede poner en relación a dos personas investigadas por delitos distintos que el investigador conoce, pero el perito no.

Informe: organización, redacción, síntesis

Todo lo actuado ha de plasmarse en un documento que es el que contendrá los pasos que se han dado para extraer las pruebas, quienes y cuándo se han realizados. Este documento, denominado informe pericial, es el que se le entrega al juez, al fiscal y a las demás partes. Se incorporará al resto de las actuaciones judiciales en el sumario.

Por ello el documento tomará la forma de diligencias judiciales aunque su valor en el juicio será como el de testimonio. Deberá ser ratificado en juicio en la fase de plenario. Es decir, tendremos que ir al juicio a ratificar que hemos hecho el peritaje, cómo lo hemos hecho, y que nos hagan las preguntas que las partes consideren oportunas.

1.2.2 Tipos de análisis forense informático

El tipo de hardware, software, sistema operativo, firmware, el tipo de información, etc, condiciona enormemente la complejidad y el procedimiento de análisis forense.

Hoy en día, con el internet de las cosas, la variedad de dispositivos e información es amplísima, con lo que es casi imposible abarcarlo todo. La especialización se hace imprescindible para abarcar todos los recursos de una manera actualizada. Así, normalmente hay una especialidad de forense en redes y comunicaciones, otros se especializan en ordenadores y servidores; y otros en dispositivos móviles (telefonía, smart watch, gps, tablets...)

Una vez que tengamos una petición judicial de análisis forense informático tendremos que evaluar:

- **Tipos de dispositivo:** servidores, ordenadores, movil/tablet, disco duro/pendrive, smart tv.
- **Tipos de sistemas operativos:** windows, MAC OS, android, linux, ios, windows phone, symbian.
- **Tipos de información:** memoria ram, datos en red, móviles, malware (analisis de procesos

del sistema).

Cada uno de ellos por separado o en conjunto nos da una forma de trabajar distinta, utilizar unas herramientas diferentes y requieren una especialización y recursos de tiempo singulares.

En el caso de este trabajo fin de grado, nos vamos a centrar solamente en obtener información de un dispositivo móvil con sistema operativo Android, y analizaremos la información que consigamos.

1.3 PERITO INFORMÁTICO

Un perito [3] es una persona que tiene unos conocimientos especiales o experiencia para que, de una manera objetiva, pueda valorar unos hechos o circunstancias y plasme sus conclusiones en un informe pericial.

Un perito tiene muchos ámbitos, el más usual es el perito judicial (de los distintos órdenes jurisdiccionales: civil, penal, social, contencioso-administrativo o militar), pero puede ser también un perito extrajudicial (convenio entre partes, arbitraje). También puede intervenir en tasaciones económicas, de daños, etc.

En concreto, el perito judicial interviene en un proceso jurídico para declarar, con finalidad probatoria, acerca de hechos relativos al procedimiento y aportando unos determinados conocimientos específicos, artísticos o prácticos. Un perito a nivel procesal tiene la consideración de testigo cualificado, esto es, declara lo que sabe o a descubierto a través de un informe pericial.

La razón de ser del perito es porque el ámbito del juez es el conocimiento del derecho, y se vale del perito ya que éste tiene una serie de cocimientos especializados o técnicos que el juez no tiene.

Un perito como testigo cualificado que es, tiene unas obligaciones (decir la verdad, objetividad), y una responsabilidad (mayor pena en caso de falso testimonio).

Así, por su responsabilidad el código deontologico de un perito tiene estos conceptos claves:

- **Integridad:** honestidad en el contenido haciendo lo justo y lo correcto, diligencia en dictar los resultados, responsabilidad en las pruebas realizadas. Respeto a la ley y a la profesión.
- **Independencia:** actuar sin dejarse influir por las partes (aunque sean contratadas por éstas), neutralidad política, abstención en caso de conflicto o intereses directos o indirectos en la causa.
- **Objetividad:** evaluación imparcial de los resultados.
- **Confidencialidad:** prudencia en el uso y protección de la información adquirida, secreto profesional. No comprometer los objetivos éticos por lucro personal.
- **Competencia profesional:** Suficientes conocimientos, aptitudes y experiencia. Formación continua, desarrollo profesional y actualización de las capacidades.

1.4 CADENA DE CUSTODIA

La cadena de custodia es el proceso de captación de la información, preservación y conservación de la prueba.

El objetivo de la cadena de custodia es demostrar que todo lo actuado no ha sido manipulado intencionadamente para alterar aquellos vestigios que puedan desvirtuar la presunción de inocencia de una persona. Y que todo el procedimiento ha sido conforme a derecho. Por tanto, es imprescindible que cualquiera de las partes en litigio sea incapaz de derribar la fiabilidad y la confianza de la cadena de custodia.

Las etapas de la cadena de custodia son:

- **Ocupación:** esto es captar la información. En el caso de este trabajo consistiría en extraer la información del teléfono móvil.
- **Conservación:** almacenar en un soporte seguro y libre de posibles manipulaciones. Los programas deberán estar en modo “solo lectura”.
- **Manipulación:** inmediatamente cuando se extraigan los archivos o las imágenes de memoria, se hará un Hash para comprobar cuando sea necesario que el fichero no ha sido manipulado. Seguidamente se hará una copia y se procederá para el análisis la copia,

conservando siempre un original intacto.

- **Transporte y traslado:** El transporte físico de las pruebas se hará también de forma segura. Sobre todo si ha de trasladarse a sede judicial para la práctica de la prueba.
- **Custodia y preservación:** se tendrá constancia documental en todo momento de lo actuado, en especial la fecha, hora y persona que ha llevado cada etapa. Se ha de tener una información sin interrupciones de quien y cuando ha trabajado en la evidencia digital.

REGISTRO DE EVIDENCIA DIGITAL
Versión 1.0

Código documento		**Fecha**	D D M M A A
Nombre del caso		**Código de caso**	
Dispositivo de origen			
Tipo	Teléfono ( ) Tablet ( ) Otro: _____		
Marca		Modelo	
Sistema operativo		Versión	
Tipo de memoria		Capacidad	

Medio de almacenamiento de la prueba			
Nro. de serie	Tipo	Capacidad	Ubicación del medio de almacenamiento

Observaciones
_____
_____
_____
_____

Responsable	
Encargado: Identificación: Cargo:	Firma:

Figura 1: Ejemplo de formato para hoja de cadena de custodia

1.5 EVIDENCIA DIGITAL

Una evidencia digital es aquella información almacenada o transmitida en forma digital que puede ser utilizada como prueba en un juicio.

Aunque pudiera parecer que la evidencia digital es muy distinta a una prueba clásica tampoco se diferencia demasiado. La evidencia digital es intangible, como también lo es el testimonio de un testigo. La evidencia digital puede ser volátil, como lo es el acelerante del fuego en un incendio provocado. Una evidencia digital es dinámica y manipulable como puede ser una falsedad documental.

De hecho, la policía científica se sigue el mismo principio clásico para pruebas analógicas y las digitales; el conocido principio de Edmond Locard: “Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto".

Este principio, también conocido como principio de intercambio, pudiera parecer *a priori* que no es aplicable a la evidencia digital, pero cualquier acción en un dispositivo suele dejar rastro en muchas partes. Por ejemplo, en una conexión web, podemos borrar el historial del navegador, pero se queda rastro en el log del servidor.

Para la prueba digital es imprescindible tener una certificación electrónica. Esto es, un mecanismo que permita demostrar que una serie de datos han existido y que no han sido alterados desde un momento determinado del tiempo (la captación de la prueba).

Esta certificación, que preserva la prueba tiene que demostrar que no hay alteración, que el contenido es íntegro, mostrar fecha y hora de la adquisición, y la autenticidad e identidad de la evidencia.

1.6 INFORME PERICIAL

Un informe pericial es un documento que recoge el estudio que ha realizado un perito nombrado

por un juez a petición del propio juez instructor, o por alguna de las partes (fiscal, victimas, acusados...), para ayudar a clarificar un asunto, resolver una controversia o como medio probatorio. Éste debe ser didáctico, con un lenguaje asequible, objetivo, independiente, y con argumentos y evaluaciones contundentes.

El dictamen pericial es un medio probatorio, por lo que tiene carácter de prueba documental que tiene que ser ratificada en la parte del plenario del proceso judicial.

1.6.1 Fases del informe pericial

Presentación del caso y aceptación

Un perito puede ser seleccionado por un juzgado que está inscrito en una bolsa de peritos judiciales. También una de las partes puede contratar un perito para que aporte pruebas para su causa. Por tanto, el perito debe tener en cuenta los detalles del trabajo que se le encomienda, elaborar un presupuestos y aceptar o renunciar a la elaboración del peritaje. Un perito debe abstenerse si está implicado o tiene intereses directos o indirectos en la causa, y puede ser objeto de recusación por alguna de las partes.

Realización del informe pericial

El perito debe tener definido claramente los objetivos que se le han solicitado, y analizar otros estudios e informes periciales sobre casos similares. Luego viene la toma de las evidencias que será reflejado en el informe y respetando la cadena de custodia. Posteriormente se examinarán y analizarán todos los datos e informaciones posibles buscando los objetivos requeridos. Todo se redactará en el informe con el análisis y se plasmará la síntesis en un apartado de conclusiones. Si el perito está colegiado o asociado puede visar el informe. Este visado es un acto administrativo que acredita la identidad y la habilitación profesional del autor, y evita que la parte contraria pueda impugnarlo, así como garantizar que el informe se ha realizado de manera correcta. El visado no es obligatorio, pero si bastante conveniente.

Declaración en los juzgados

El trabajo del perito no acaba con la elaboración del informe. El análisis realizado y el informe redactado solo es un trabajo para plasmar por escrito los pasos que se han dado para obtener unas conclusiones. Toda prueba debe ser reproducida en el juicio oral, y de no ser posible, se plasma por escrito teniendo que estar presente el perito para dar testimonio de lo realizado. En ese momento la prueba y el informe pericial se pone en contradicción por las partes y se dirimen aquellos puntos que no quedan claro. Quedando el perito a disposición de las partes para ser preguntado de cualquier cuestión relativa a las pruebas realizadas, estando obligado el perito a declarar como testigo. Por tanto, es importante preparar a conciencia la vista oral, ya que al acudir al juicio el perito tendrá que aclarar todas las cuestiones que se le planteen de manera contundente y sin titubeos. Es necesario dar confianza y seguridad al tribunal para dar credibilidad a la prueba que se presenta. La preparación del juicio hay que hacerla con la vista puesta en la fecha del mismo, ya pueden pasar semanas o meses desde que realizó el informe pericial.

2 CAMPO DEL PERITAJE FORENSE COMO TRABAJO DE INGENIERÍA

Dentro del mundo universitario no es habitual que un ingeniero recién graduado piense en el trabajo de perito como una de las opciones principales a tener en cuenta para desarrollar su carrera profesional. Normalmente el campo de trabajo va orientado más el desarrollo e implementación de tecnología o de la ingeniería en concreto.

Sin embargo, el uso intenso de las tecnologías por parte de los ciudadanos, unido a la complejidad, variabilidad y volumen de información que manejan de los mismos, la especialización en peritaje judicial es un campo en alza con muchas posibilidades de trabajo.

Para este trabajo nos hemos enfocado en la labor del perito judicial, pero como se ha comentado anteriormente el ámbito de la seguridad privada, las empresas para gestión de sus incidentes de seguridad lógica o infidelidad de sus propios empleados; los ciudadanos para recuperar información

personal; las instituciones para analizar sus fallos en los sistemas, etc...

Para ser perito se ha de poseer una titulación oficial, no siendo válidos por sí sólo los cursos o másteres propios que ofrecen algunas instituciones universitarias.

La titulación del grado de Electrónica para Comunicaciones faculta para el trabajo de perito informático/electrónico. Pero además de la titulación hay que tener unos conocimientos y experiencia que sí se puede obtener mediante los cursos referidos anteriormente, o el trabajo en una empresa especializada en peritajes.

Por tanto, se considera que es un campo de trabajo que ofrece múltiples posibilidades profesionales como para tenerla muy en cuenta.

Para ser perito judicial es conveniente colegiarse para certificar el trabajo realizado mediante visados, y para entrar en las bolsas de peritos que utilizan los juzgados cuando requieren uno durante el proceso judicial.

Existen múltiples colegios, asociaciones, empresas y grupos de trabajo para desarrollarse en este interesante ámbito.

3 LA INVESTIGACIÓN POLICIAL

Para hacernos una idea de cómo se realiza una investigación judicial o policial y qué papel tiene el perito dentro de la investigación, es conveniente conocer cómo se lleva a cabo la investigación, cuales son sus fases y objetivos, y cómo hay una constante interacción entre investigadores y peritos.

Los objetivos de una investigación criminal son:

- Comprobar si realmente se ha cometido un hecho delictivo tipificado en las normas penales.
- Investigar los hechos de los que tengan conocimiento las Fuerzas y Cuerpos de Seguridad, juzgados o ministerio fiscal.
- Recopilar y conservar las pruebas que relacionen el hecho con el presunto autor con arreglo a lo establecido en la legislación procesal.

- Identificar a los responsables del hecho criminal.
- Proceder a la detención y puesta a disposición judicial del presunto autor así como aportar y conservar las pruebas que relacionen a éste en el hecho criminal.

La investigación debe tener estos principios:

- Fiabilidad: una investigación posterior con los mismos datos debe llegar a idénticas conclusiones.
- Validez: todos los datos obtenidos ser demostrables, reproducibles y ajustados a la investigación.
- Relevancia: hay que asegurar la presencia de todos los elementos e hipótesis necesarios para considerar agotado el proceso, y dar por acertado el resultado.

Siguiendo estas pautas, el perito puede ser requerido en cualquier momento de la investigación, o incluso durante todo el tiempo que dure la investigación en una colaboración estrecha.

Por ello, conocer cómo se trabaja a nivel policial y judicial puede ser un plus para el desarrollo profesional del perito.

4 ANÁLISIS FORENSE EN TECNOLOGÍA MÓVIL

Después de haber comentado brevemente cómo es un análisis forenses, qué hace un perito judicial y toda la variabilidad de tipos de situaciones que se nos puede encargar como peritos, nos centraremos en algo muy concreto: un análisis forense de un móvil para extraer los datos que se interesen. Pero antes, se hace necesario tener que explicar algunos detalles más acerca de las particularidades de un análisis forense en tecnología móvil.

4.1 DIFICULTADES ESPECÍFICAS EN ANÁLISIS FORENSE DE MÓVILES

Anteriormente hemos comentado las características de un análisis forense digital en comparación con un análisis forense en otros ámbitos no tecnológicos. Dentro de lo que es un análisis forense digital, las particularidades de la tecnología móvil (smartphones, tablets, etc) la hacen aún más complejas. A continuación veremos cuales son las dificultades que un perito forense digital especializado en tecnologías móviles se tiene que enfrentar.

- **Multitud de modelos distintos.** Hay en el mercado actualmente muchos dispositivos distintos. Además de eso, existen distintos modelos, versiones de hardware, de firmware, de software y de implementaciones. Diariamente salen nuevas marcas, actualizaciones, etc. La diversidad es muy grande y compleja, lo que implica una imprescindible actualización constante.

- **Diferentes sistemas operativos.** Aunque desde hace unos años se han impuesto casi como ampliamente mayoritarios los sistemas operativos de Apple y Google (iOS y Android), coexisten otros como Windows Phone o BlackBerry; también se han casi extinguido otros sistemas operativos como Symbian. Pero en definitiva existen diversos sistemas operativos, y sus actualizaciones son semestrales o anuales. Los cambios de sistemas operativos incluyen nuevas funcionalidades y soportan cada vez aplicaciones más pesadas y complejas. Todo ello conlleva también una variedad enorme de modos de trabajo y de especializaciones. Nunca sabemos qué tipo de dispositivo y con qué software vamos a tener que trabajar.

- **Características de seguridad avanzadas.** Los dispositivos tienen cada vez más mecanismos de seguridad y más robustos para la identificación del usuario. Contraseñas, pin, patrones táctiles, huella dactilar, biometría... Esto complica la extracción de datos sin el consentimiento del usuario. Además de la autentificación, muchos dispositivos vienen ya

con cifrado de sus datos.

- **Técnicas anti-forense.** Sobre todo en la delincuencia organizada, los criminales pueden usar herramientas antiforense para bloquear, dificultar el acceso, o borrar datos comprometidos en caso de incautación o pérdida del terminal. Por ello es que se procura aislarlo de la red en la incautación.

4.2 MÉTODOS DE AISLAMIENTO DE LA RED

Además del análisis forense propiamente dicho, se han de tener en cuenta cómo llevar a cabo la aprehensión de los dispositivos. Si bien es algo que como peritos normalmente no vamos a tener que realizar, es importante conocer cómo aislar los terminales, tanto por si hemos de llevarlo a cabo nosotros como para indicarselo a las personas que lo incauten.

El aislamiento se hace de redes y conexiones y se realiza para evitar que remotamente se pueda dar instrucciones de borrado o destrucción de pruebas. A continuación, se dan algunos métodos de aislamiento del teléfono de las redes:

Figura 2: Bolsa de Faraday

- **Bolsa de Faraday.** Es una bolsa que envuelve el teléfono y hace de jaula de Faraday, impidiendo que lleguen o salgan ondas electromagnéticas.

- **Jammer.** Es un bloqueador de señal electromagnéticas. Funciona haciendo un barrido de todas las frecuencias utilizadas en los smartphone y emite tal cantidad de señal en forma de ruido que interfiere en la señal del teléfono. Hay que tener en cuenta que también interferirán en todos los teléfonos de su radio de acción.

- **Modo avión.** Es un método rápido y eficaz de intentar aislar el teléfono. También hemos de asegurarnos que desconectamos el wifi, bluetooth y la ubicación.

Figura 3: Jammer: bloqueador de señales

- **Extracción de tarjeta SIM.** Es necesario otros métodos de aislamiento además de extraer la SIM. Al extraerla nos aseguramos que no hay posibilidad de llamar o utilizar internet móvil. Sin embargo, los teléfonos móviles pueden estar conectados a wifi o bluetooth aunque no tenga la tarjeta SIM.

- **Papel de aluminio.** Consiste simplemente en envolver el teléfono en papel de aluminio como si fuera un bocadillo. No es el método más eficaz, pero sin duda es el más socorrido en una emergencia.

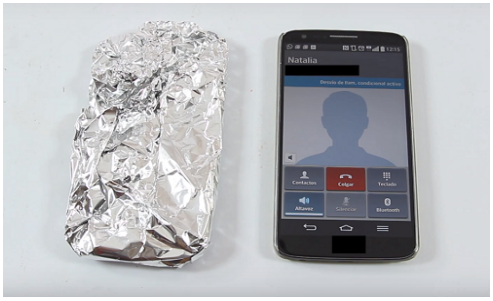

Figura 4: Jaula de Faraday casera

4.3 TIPOS DE EXTRACCIÓN DE DATOS

Una de las partes del proceso del peritaje que hemos señalado es la extracción de datos. Ésta puede ser de varios tipos según lo que necesitemos obtener y el estado del teléfono (si está apagado, tiene contraseña, no enciende, o esta parcialmente destruido).

Hay varios tipos de extracción y suelen representarse gráficamente de forma piramidal. Conforme subamos de la pirámide, desde la extracción manual a la micro lectura, la complejidad técnica se acrecienta, el tiempo de análisis es mayor, la formación y especialización también aumentará y será más invasiva en el dispositivo (podemos incluso tener que destruirlo para extraer

los chips de memoria a nivel de microelectrónica). Cuanto más bajemos de la pirámide la extracción será lo contrario, más sencilla y menos costosa.

Figura 5: Pirámide de clasificación de herramientas de análisis forense para dispositivos móviles

Extracción manual: se adquieren los datos manejando el móvil como si fuera un usuario normal. Se visualizan y almacenan los datos a mano mediante "pantallazos" o mediante fotografías de las diferentes navegaciones que vayamos haciendo con el teléfono. Tiene la ventaja de ser muy rápido y no requiere cables ni ninguna herramienta forense. Puede ser útil en caso que el móvil vaya a quedarse sin batería o los datos vayan a perderse por su volatilidad. Sin embargo, no podemos acceder a datos eliminados y podemos tener que necesitar las claves de acceso al terminal.

Este método se puede utilizar para comprobar de manera rápida si el terminal contiene información que nos pudiera interesar para la investigación.

Extracción lógica: se realiza una copia de los datos que necesitemos desde el teléfono móvil al ordenador u otro dispositivo, y de esta manera conseguir visualizar, almacenar y analizar los datos. Se utilizan las herramientas nativas de sincronización de datos que proporciona el fabricante del

teléfono: conexión por usb, bluetooh, wifi, etc. Es un proceso sencillo pero no siempre es posible, ya que necesitaríamos, como en el caso anterior, las claves de acceso al terminal. No obstante, podríamos intentar crackear las claves de acceso.

Extracción física: es una extracción bit a bit que se hace directamente a un microchip. Esta extracción puede realizarse al encapsulado de la memoria interna, a la tarjeta SD o incluso a los registros internos del microprocesador. La información obtenida corresponde con la estructura interna del chip en cuestión, por lo que se ha de analizar posteriormente para extraer e interpretar la información que contienen esos bits clonados.

La extracción en informática forense para tecnología móvil puede hacerse de dos formas:

- **JTAG** (Joint Test Action Group). Los teléfonos móviles suelen traer unos pines más o menos accesibles que se usan para la depuración del dispositivo. Suelen ser 4 o 5: TDI (Entrada de Datos de Testeo), TDO (Salida de Datos de Testeo), TCK (Reloj de Testeo), TMS (Selector de Modo de Testeo), TRST (Reset de Testeo) es opcional. También suelen incluir más pines para VCC y GND. Pero es difícil de encontrar información sobre qué pines son cada uno o cuál es la frecuencia de trabajo del reloj, ya que es información interna de los fabricantes y no la suelen distribuir. Es una técnica difícil de implementar, en la que se usa comúnmente un dispositivo llamado RIFF BOX v2, que también es complicado de obtener, para extraer la información. Este dispositivo de extracción tampoco es válido para todas las tarjetas de memoria de todos los teléfonos.

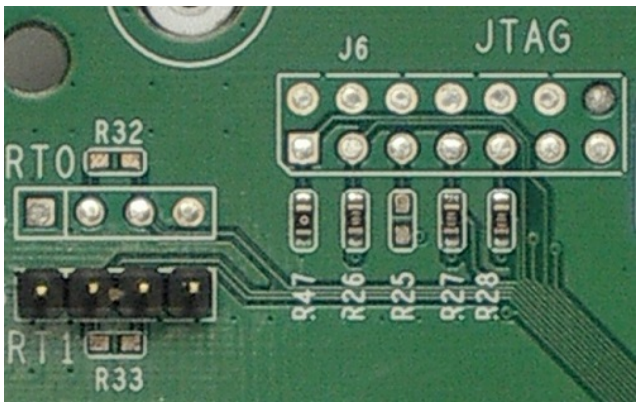

Figura 6: Pines del JTAG

- **CHIP-OFF**. Esta técnica consiste en la extracción del chip desoldandolo con calor de la placa PCB, para luego hacer una copia bit a bit de la información que contiene. Una vez desoldado se limpiarán los pines y se introducirán en un zócalo específico para la lectura mediante software específico.

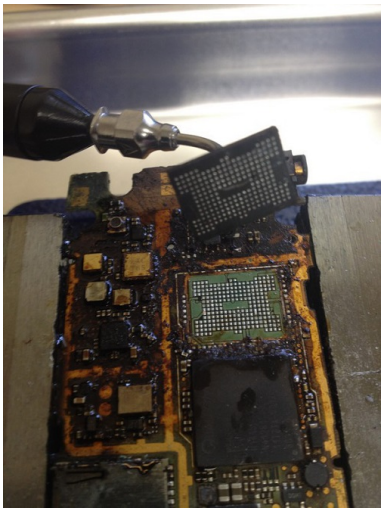

Figura 7: Extracción del chip de un terminal móvil muy deteriorado

- **MICRO LECTURA.** Esta técnica consiste en la captura de imagen de la estructura de datos mediante un microscopio electrónico. Es la más costosa en tiempo y dinero; y la más invasiva, ya que hay que desencapular el chip de silicio. Una vez obtenido el chip, mediante un microscopio electrónico, se fotografían las puertas de silicio. A continuación con un software de visión artificial se interpretan las imágenes para extraen los 0 o 1 de cada puerta lógica.

- **Otras tecnologías:** Continuamente hay investigaciones para extraer los datos de los dispositivos móviles y electrónicos. Tanto a nivel de desencriptación como reconstrucción de datos de archivos eliminados. Por ejemplo, la NSA (Agencia de Seguridad Nacional) ha obtenido recientemente una tecnología para recuperar la información de un disco duro mediante el campo magnético residual de los discos magnéticos.

4.4 MÉTODO DE ADQUISICIÓN DE DATOS

Cuando pensamos en un análisis forense digital tendemos a imaginarnos solamente un laboratorio y un ingeniero abriendo un dispositivo electrónico extraer sus datos. Sin embargo, las actuaciones para una adquisición efectiva deben comenzar mucho antes. Según el estado de

funcionamiento del dispositivo cuando se incaute tendremos que elegir entre los distintos métodos de adquisición. Este método hace variar la efectividad y facilidad de la extracción de datos. Por ejemplo, si nos proporcionan un terminal encendido, utilizable y desbloqueado, el método de adquisición de la evidencia es lógicamente mucho más sencillo que si está quemado a propósito para ocultar pruebas.

Aunque esto es evidente, puede pasar que durante la aprehensión del dispositivo esto no se tenga en cuenta. Se puede dar el caso que la persona que incauta el terminal lo apague para "ahorrar batería".

En el siguiente esquema [4] se proponen unas pautas de actuación en caso de que se encuentre un terminal en un hecho delictivo y se prevea que pueda contener pruebas incriminatorias. Estas sencillas actuaciones pueden facilitar mucho el trabajo del perito forense y sobre todo, aumentan la posibilidad de extraer evidencias digitales.

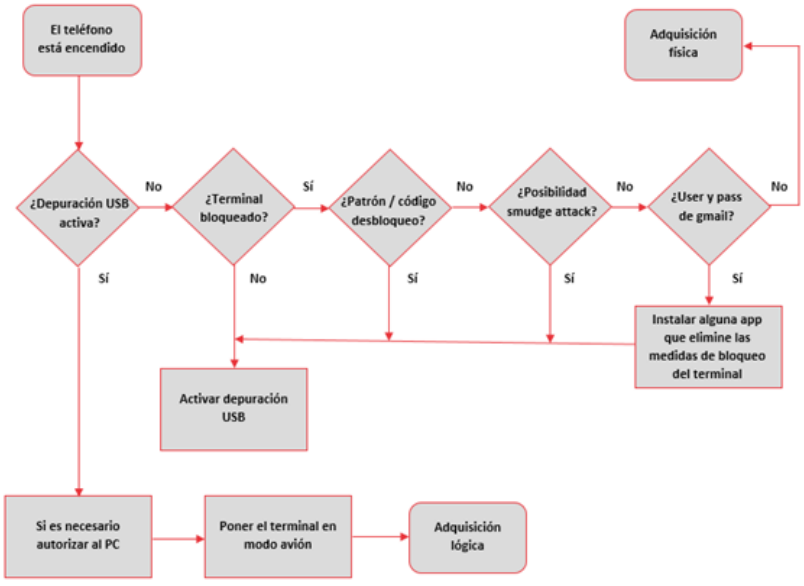

Figura 8: Metodología para la adquisición de datos

Como vemos en este sencillo diagrama de flujo siempre que se pueda se configurará el dispositivo en modo depuración USB. Y que finalmente tendremos que hacer o una adquisición

lógica (más garantía de éxito), o una adquisición física (mayor coste y menor fiabilidad). En la mayoría de los casos nos encontraremos el teléfono móvil apagado y sin claves de acceso.

4.5 ARQUITECTURA DEL SISTEMA OPERATIVO ANDROID

Es necesario, aunque sea de manera somera, conocer cómo es la arquitectura de los dispositivos Android. De esta manera sabremos cómo se distribuyen los distintos ficheros e información dentro de los dispositivos que vamos a analizar.

La arquitectura de Android es sólida y robusta. Parte del kernel de linux 2.6 para manejo de hardware y la ejecución de aplicaciones se basa en la maquina virtual de Java. Esto le proporciona unas características de fácil desarrollo y amplia compatibilidad, sobre todo teniendo en cuenta que se trata software libre. Lo que en principio es una ventaja para el desarrollo de app's, también tiene la contra que es más susceptible de ataques maliciosos por su gran distribución y fácil programación de software.

Comentaremos brevemente cada bloque de la pila de software de Android:

Linux Kernel: Es el núcleo del sistema kernel, que parte de linux 2.6. Es una capa de abstracción del hardware, la cual contiene los drivers necesarios para que cualquier nuevo componente hardware pueda ser utilizado por los fabricantes. Facilita la nueva implementación hardware, ya que los fabricantes solamente tienen que añadir las librerías de estos drivers dentro del kernel de Linux embebido.

HAL (Hardware Abstaction Layer): Son interfaces entre el hardware y la API de Java. Contiene las bibliotecas de la interfaz que traduce la comunicación entre hardware y Java, proporcionando el marco de trabajo para que la API se comunique con cada componente hardware.

Librerías C/C++ nativas: constituyen el corazón de Android junto con el kernel, están escritas

en lenguaje C/C++ y proporciona la base de las funcionalidades que utilizan las aplicaciones de usuario e internas de Android. Estas funciones son la gestión de ventanas, contenido multimedia, gráficos, fuentes de escritura, securización de comunicaciones, base de datos internas, navegador nativo, etc. Es decir, las demás aplicaciones se apoyan en estas librerías para evitar tener que programar las funciones comunes y básicas.

Android Runtime: proporciona el marco de trabajo de Java, la cual es una plataforma que ejecuta aplicaciones desarrolladas en este lenguaje y otros. Esta ejecución se realiza mediante una máquina virtual y contiene ciertas librerías de uso común que aligeran la programación de aplicaciones.

Java API Framework: son un conjunto de herramientas de desarrollo para las aplicaciones. Son los cimientos de las aplicaciones de usuario y simplifica el desarrollo software, además de proporcionar la reutilización de componentes centrales y modulares. Son los sistemas de vista, administración de recursos, notificaciones, administración de actividad, proveedores de contenido, manejador de teléfono, mensajes, llamadas, etc.

System Apps: son las aplicaciones de usuario. Corresponde con la interfaz gráfica y la lógica de negocio de las diferentes aplicaciones que se pueden usar en el dispositivo. Se incluyen tanto a las que lleva por defecto el dispositivo de fábrica, como las que el usuario va añadiendo.

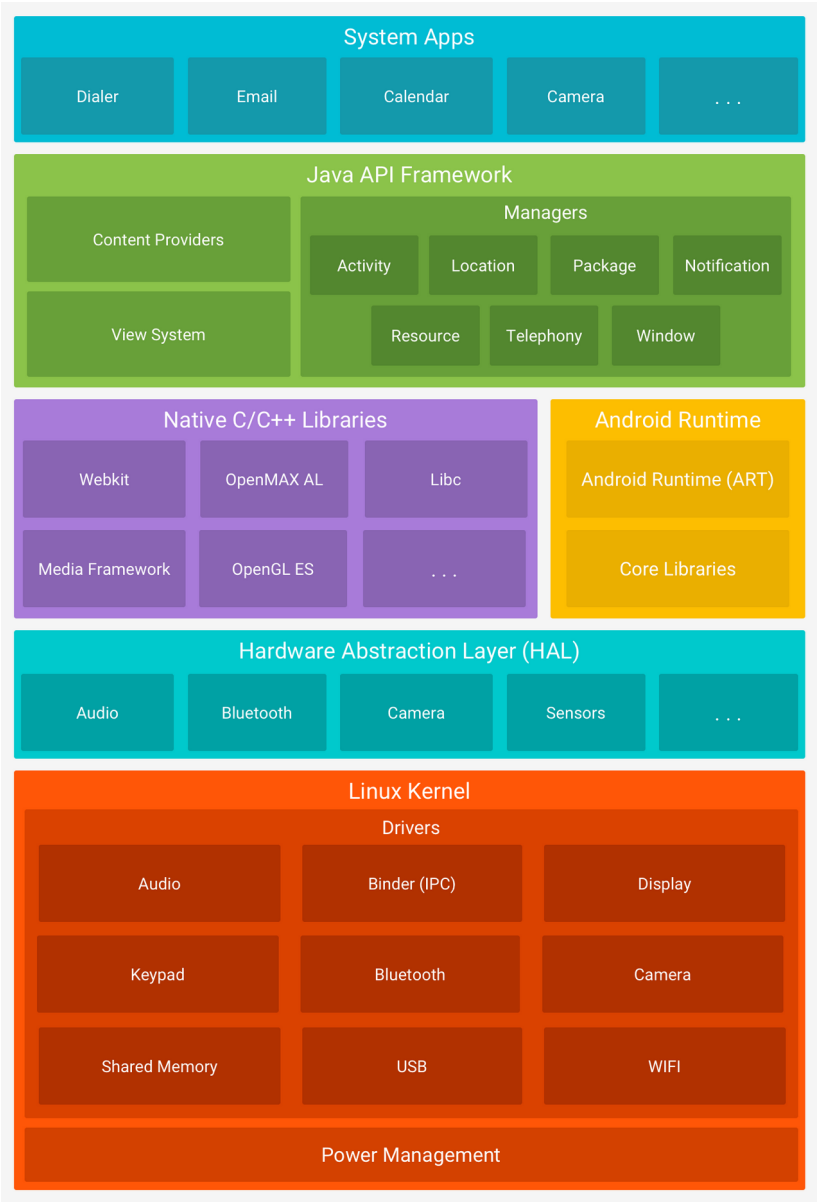

Figura 9: Capas del sistema Android

4.5.1 Sistema de archivos Android

Como Android parte de la estructura más interna de Linux (el kernel), no es de extrañar que el sistema de archivo tenga la estructuras de particiones propias de los sistemas Linux.

La memoria de los sistemas Linux está dividida en particiones para organizar los recursos de

almacenamiento del teléfono. Cada partición tiene una finalidad concreta y tiene asignada una capacidad máxima distribuida entre toda la memoria disponible del terminal. Todos los móviles que cuentan con Android como sistema operativo llevan las mismas particiones.

A continuación las comentamos brevemente puesto que son de mucha utilidad a la hora de bucear en los entresijos de datos e información de los terminales móviles:

/boot

Es la parte de arranque del dispositivo. Cuando encendemos el terminal las primeras zonas de memoria que se leen son estas, y es el encargado de ir abriendo todas las demás según la configuración. Consta del kernel y una ramdisk (pequeña memoria virtual para el encendido y configuración).

/system

Aquí es donde se almacenan todos los archivos del sistema operativo, como la interfaz gráfica de Android, las apps de sistema y el bloatware (software preinstalado de fábrica que varía según fabricante). Esta partición es difícil de modificar si no rooteamos el dispositivo o modificamos el recovery.

/recovery

Esta es una partición de recuperación para "casos de emergencia". Podría considerarse una partición /boot alternativa para restaurar el teléfono. Contiene una consola de comandos de manteamiento para borrar memoria, restaurar de fábrica, cargar archivos por ADB (herramienta de linea de comandos para comunicar con el dispositivo).

/data

Contiene los datos del usuario, las apps instaladas, archivos descargados, contactos, mensajes, logs de llamas, etc. Es lo que comúnmente se conoce como la "memoria interna" del teléfono. Cuando se restaura de fábrica se borra esta partición.

/cache

Es una memoria de intercambio de archivos y uso temporales de los mismos. Su utilidad es dar agilidad a las aplicaciones para mostrar y manejar información.

/misc

Es una partición para datos misceleneos, es decir, sin una función predeterminada; pero puede contener datos importantes para nuestro análisis forense. En este almacenamiento se guardan ajustes relacionados con el operador, aspectos de hardware, etc.

/sdcard

Es la partición para montar la tarjeta SD, o lo que es lo mismo la "memoria externa" del dispositivo. Es opcional, no siempre la encontraremos, y en ella las apps pueden almacenar importantes datos para nuestro trabajo forense, como imágenes, archivos, mensajes, emails....

/sd-ext

Es una expansión de la partición /data en la memoria externa. Cuando la capacidad de la "memoria interna" se agota, el sistema puede almacenar las aplicaciones aquí, e incluso las aplicaciones pueden almacenar subsidiariamente sus datos. Es decir, para un completo análisis forense es imprescindible saber si se ha creado esta partición, ya que no la encontraremos en todos los dispositivos.

5 ANALISIS HERRAMIENTAS FORENSES DE SOFTWARE LIBRE

El campo de la informática forense es relativamente nuevo si lo comparamos con otros ámbitos forenses. Sin embargo, la rápida expansión de la tecnología y dispositivos en nuestras vidas ha

propiciado también que exista un gran abanico de herramientas para la recuperación y análisis forenses de estos dispositivos.

Comercialmente existen muchas herramientas integrales que realizan esta funcionalidad. Se adquiere un paquete con todas las herramientas necesarias, software para el análisis, hardware para conectar al dispositivo y hacer la extracción, distintas configuraciones (análisis rápido o en profundidad), etc. Las plataformas más utilizadas son Cellebritie, Encase Forensis, Oxygen Forensic Suit, etc.

No obstante, en este trabajo se van a analizar y utilizar algunas herramientas de código abierto. Estas herramientas con licencias GNU nos dan mucha versatilidad a la hora de usarlas, también están enteramente disponibles y descargables, no tienen coste y son potentes. Si bien, entre sus contras están que no suelen dar soporte técnico, o que el uso no está tan automatizado como las herramientas de pago. Además suelen ser más complejas y necesitan conocimientos de electrónica y programación.

En cualquier caso, las herramientas de análisis forenses de código abierto son un punto de partida excelente para iniciarse en el mundo de la informática forense, también como herramienta educativa, hacking ético, pruebas de vulnerabilidad, etc.

Las herramientas forenses de software libre más utilizadas vienen dentro de una distribución de Linux. En estas distribuciones se proporciona el sistema operativo y tienen preinstaladas las aplicaciones que necesitamos para el análisis forense. Hay varias distribuciones según el tipo de análisis o dispositivo que necesitemos utilizar. En nuestro caso analizaremos las distribuciones que se pueden utilizar para el análisis de terminales móviles, pero estas mismas herramientas dan además soporte para el análisis de ordenadores, discos duros, registros de Windows, análisis de red, etc.

Otra de las grandes ventajas que tienen estas distribuciones, es que al ser distribuciones libres y de código abierto, podemos nosotros mismos desarrollarlas, modificarlas, configurarlas y adaptarlas a nuestras necesidades para así crear un entorno propio, o nuestro propio laboratorio forense.

5.1 USO DISTRIBUCIÓN EN LIVE

Como se ha comentado anteriormente la mayoría del software libre para el análisis forense viene configurado como una distribución Linux. Estas distribuciones suelen venir con la opción live CD/ USB. Esta posibilidad permite que la podamos analizar ordenadores y discos duros extrayendo datos sin modificar el contenido de los mismos. Conservando de esta manera la integridad y la cadena de custodia.

Cabe destacar que aunque las distribuciones permitan el funcionamiento en "Live" también pueden ser instaladas para su uso como sistema operativo normal o en un entorno estable y fijo (un ordenador portátil) para el analista forense.

5.1.1 USB BOOT

En ocasiones puede ser necesario tener de manera portátil las herramientas de análisis forense, sin tener que llevar un ordenador portátil o dispositivos más pesados. Ésto pude llevarse a cabo usando una memoria externa USB donde instalamos un Linux booteable. Este pendrive lo podemos introducir en cualquier ordenador apagado, y que al encenderlo se arranque la distribución Linux sin tener que instalar nada en el ordenador.

Este USB ejecutable se genera desde la imagen ISO de la distribución Linux y mediante una aplicación concerta. Hay varias tanto comerciales como libres: Rufus, Unetbootin, Etcher, etc. Para este proyecto se ha utilizado Linux Live USB Creator, que es libre, de código abierto y disponible para Windows y GNU/Linux

5.2 USO DE MÁQUINAS VIRTUALES

Un analista forense, como cualquier buen profesional, no se limita solamente a utilizar una herramienta y basar toda su pericia en una única forma de trabajar. Dada la complejidad de los peritajes forenses y la aparición continua de herramientas y dispositivos, necesitamos alguna manera de poder utilizar de forma rápida y eficaz todas esas opciones. Como la mayoría de las herramientas de análisis forense de software libre viene dentro de una distribución Linux, la mejor manera de integrar todas las distribuciones en un mismo equipo es mediante el uso de máquinas

virtuales.

En este trabajo hemos utilizado la aplicación VirtualBox de Oracle, que nos permite la descarga gratuita y tiene licencia libre GNU. Esta herramienta es fácil de usar y nos permite tanto trabajar en Windows como en Linux, y tener varias distribuciones funcionando a la vez.

5.3 SANTOKU

Figura 10: Pantalla de inicio de la distribución Santoku

Es una distribución Linux que está desarrollada específicamente para el análisis forense para telefonía móvil. Con ella se puede auditar vulnerabilidaes, fallos de seguridad, privacidad, etc. Además del análisis forense, también se puede analizar el maldware de los teléfonos y la posible vulneración de la seguridad lógica. Es completamente libre, gratuita y de código abierto.

El proyecto de Santoku [5] tiene una web donde contiene información de la distribución, documentación del uso, comunidad de usuarios y descarga gratuita. (https://santoku-linux.com/)

Las funcionalidades que ofrece se pueden dividir en tres apartados:

Análisis forense

La distribución proporciona herramientas para la adquisición y análisis de datos, lista de

imágenes de sistemas operativos de Android para diferentes marcas y modelos (firmware que podemos instalar en los dispositivos) e imágenes de tarjetas de memoria y RAM. Además, contiene algunas versiones libre de herramientas forenses comerciales, scripts y utilidades diversas para el análisis forense en dispositivos móviles.

Análisis de maldware movil

En este apartado se encuentran herramientas para el examen de malware para móviles. Encontramos emuladores de dispositivos móviles para el análisis del funcionamiento de distintas versiones de los sistemas operativos, utilidades para simular servicio de redes para el análisis dinámico, acceso a base de datos de malware, etc.

Análisis de seguridad

Santoku también ofrece herramientas de evaluación de aplicaciones móviles. Herramientas de decompilación y desemsamblado de aplicaciones, scripts para detectar problemas comunes en las aplicaciones, scripts para automatizar desencriptado de código binario, enumeración de detalles de la aplicación, etc.

5.3.1 Herramientas nativas

A continuación vamos a referenciar las principales herramientas y describiremos brevemente las aplicaciones más importantes.

Herramientas de desarrollo:

En el caso del desarrollo de software no vamos a entrar en detalles, ya que se escapa de la pretensión de este trabajo. Solo comentaremos que el lenguaje utilizado para las aplicaciones android es muy parecido al Java, y que también se pueden utilizar módulos de C y C++. Cabe destacar la cantidad de aplicaciones que hay para el desarrollo en los dispotivios blackBerry de esta distribución.

Android SDK Manager

DroidBox

Eclipse IDE

AXMLPrinter2

Fastboot

Heimdall

SBF Flash

BlackBerry JDE

BlackBerry Tablet OS SDK

BlackBerry Ripple

BlackBerry WebWorks

Windows Phone SDK

SecurityCompass Lab Server (HTTP y HTTPS)

Analizadores Wireless:

Con los analizadores de redes, podemos analizar exactamente qué paquetería y datos son los que mandan y reciben las aplicaciones. Muy útil para descomponer y reconstruir loas paquetes de mensajes y comprobar si hay datos enviados que no queremos en aplicaciones maliciosas.

Chaosreader

dnschef

DSniff

TCPDUMP

Wireshark. Tiene una interfaz gráfica muy intuitiva y sencilla. Es quizás, el analizador de redes más utilizado, sobre todo a nivel de enseñanza en universidades.

Ingeniería inversa:

Tampoco en este caso nos detendremos ya que no nos interesa demasiado descomponer las aplicaciones para este trabajo.

Androguard
Antilvl
APK Tool
Baksmali
Dex2Jar
Jasmin
JD-GUI
Mercury
Radare2
Smali

Herramientas forenses:

AFLogical Open Source Edition. Es una aplicación para móviles, es decir, es una apk para instalarla directamente en el terminal. Una vez instalada, permite extraer información de la tarjeta SD (registro llamadas, contactos, aplicaciones instaladas, mensajería, multimedia..). Esta información se puede extraer a un dispositivo externo o mediante ADB.

Android Brute Force Encryption. Con esta aplicación se pretende crakear el pin usado para encriptar un dispositivo android (Ice Cream Sandwich y Jelly Bean API)

ExifTool. Aplicación para analizar metadados de archivos. Permite leer, escribir y editar metadados de imágenes, audio, video y pdf.

iPhone Backup Analyzer. Es una utilidad diseñada para explorar las carpetas de copia de seguridad de un iPhone y otros dispositivos iOS. Extrae datos y artefactos sin alterar ninguna información.

Libimobiledevice. Es una librería multiplataforma que permite comunicarse con los

dispositivos iOS mediante los protocolos que soporta este sistema operativos. Permite a otras aplicaciones acceder fácilmente al sistema de ficheros, información del dispositivo, backup; así como restaurar el dispositivo, hacer una copia de seguridad del terminal, etc. Básicamente provee protocolos de comunicación para interactuar con el dispositivo.

Scalpel. Es un grabador e indexador de archivos rápido que compara de una base de datos cabeceras y pie de numerosos formato de archivos. Con esta aplicación podemos identificar archivos ya que el programa analiza las cabecera y final del archivo. Con esta aplicación, ademas de grabar archivos podemos recuperar archivos dañados, borrados o perdidos.

Sleuth Kit. Es una librería y colección de utilidades para facilitar el análisis forenses. Puede usarse como linea de comandos o unidas a otras herramientas como Autopsy o log2timeline. Permite analizar diferentes sistemas de archivo e imágenes de archivos en crudo (dd). Contiene un modulo para analizar el sistema de Android.

Pruebas de Penetración:

Con las pruebas de penetración comprobamos las vulnerabilidades de las aplicaciones, redes o sistemas. Tampoco es el objetivo de este trabajo, por lo que nos limitaremos a nombrar las aplicaciones de esta distribucióin.

Burp Suite

Ettercap

nmap

SSL Strip

w3af

ZAP

Zenmap

Infraestructura móvil:

Son diferentes herramientas para configurar y gestionar la configuración de los dispositivos. Tampoco vamos a entrar en valorarlas en detalle.

BES Express

Google Mobile Management

iPhone Configuration Tool

Documentación

La distribución tiene disponible documentación de cómo instalarla tanto en linux como en Mac.

Ademas de la instalación también contiene varios manuales para las herramientas de desarrollo como una guía de inicio en SDK de Android, compilar AFLogical OSE, o cómo correr Heimdall (herramienta para flashear firmware) en dispositivos Samsung.

En cuanto a las herramientas forense, Santoku ofrece manual de cómo usar AFLogical OSE para el análisis forense, también iPhone Backup Analyzer, Brute Dorce Android Encryption, o cómo crear una copia de seguridad con libimobiledevice.

5.4 CAINE

Es una distribución de linux de filosofía Open Source, basada en Ubuntu, que ofrece un completo entorno para el análisis forense. Está organizada para integrar una serie de herramientas software así como módulos de software en una amigable interfaz gráfica.

La versión actual de Caine [6] es la 11.0 "WORMHOLE", lanzada el 1/12/2019. También viene distribuida en Live por lo que se puede arrancar desde una unidad extraible como un disco físico o virtual.

El propósito de esta distribución es el de proporcional un entrono completo y profesional con todas las herramientas necesarias para realizar una investigación de informática forense en los cuatro procesos de la investigación (preservación, colección, examen y análisis de pruebas). Cabe

destacar que es una distribución de propósito general para el análisis, pero no es específico para el análisis de telefonía móvil como Santoku.

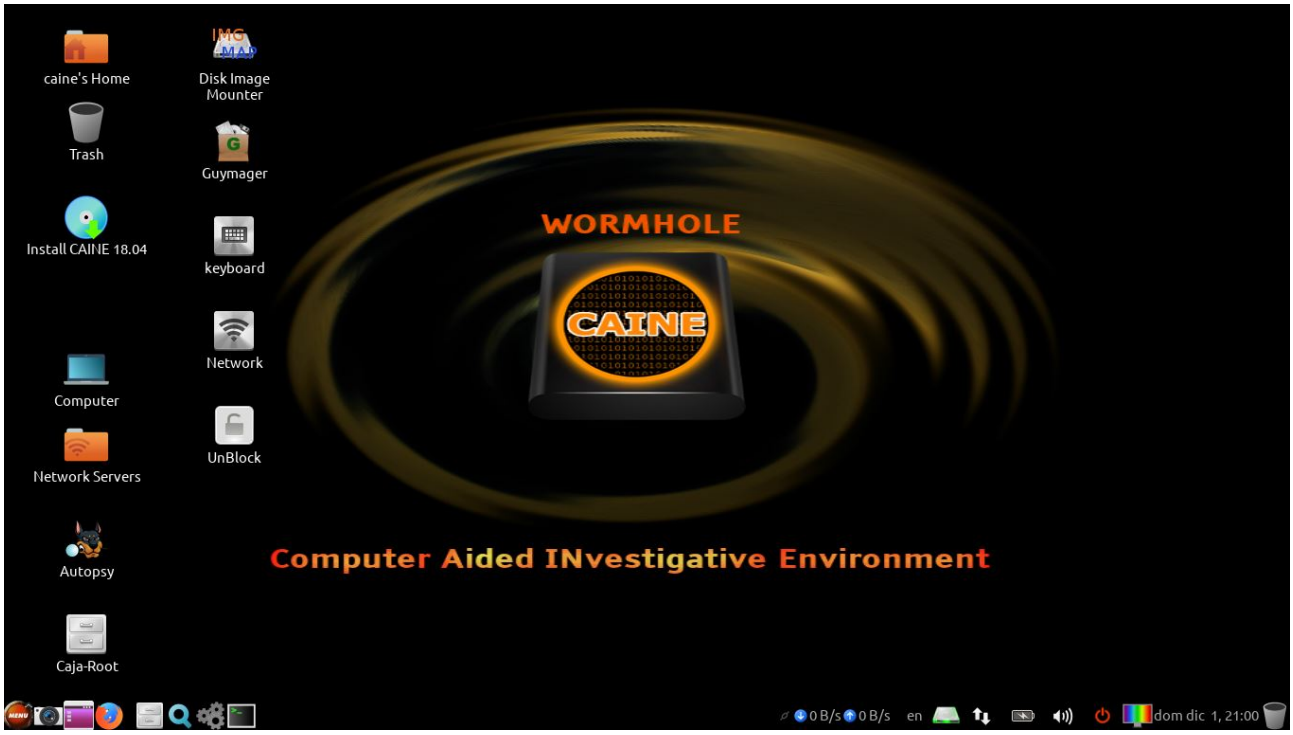

Figura 11: Pantalla de inicio de la distribución Caine

5.4.1 Herramientas nativas

Como veremos en este apartado, Caine provee las herramientas suficientes para hacer un análisis completo a un sistema, tanto para base de datos, memorias, redes etc. Comentaremos brevemente alguna de las herramientas más útiles para este trabajo, y simplemente nos detendremos a nombrar las demás, o las que ya hemos detallado anteriormente.

Autopsy. Es una plataforma para el análisis forense y además la interfaz gráfica de The Sleuth Kit y otras herramientas. Con él podemos hacer análisis de ficheros, filtro de hash, búsqueda de palabras claves, emails y artefactos web.

The Sleuth Kit. Comentado anteriormente.

RegRipper. Es una de las herramientas más utilizadas para la extracción de datos (llaves, valores y datos) del registro de windows.

Tinfoleak. Este software realiza una extracción automática de información de Twitter y facilita el análisis posterior para la generación de inteligencia. Mediante el identificador de usuario, coordenadas geográficas o palabras clave, analiza el timeline de la red social y extrae los datos mostrando la información útil y estructurada para el analista forense.

Wireshark. Analizador de redes, comentado anteriormente.

PhotoRec. Con esta aplicación podemos recuperar multitud de archivos perdidos de un disco duro, cámara digital o sistemas ópticos. Recupera tanto video y fotografía como documentos.

Fsstat. Esta herramienta permite la supervisión y extracción de información estadística del sistema de archivos de una imagen u otro objeto almacenado.

5.5 KALI LINUX

Figura 12: Pantalla de inicio de la distribución Kali Linux

Kali Linux [7] es una distribución Debian para test de penetración avanzado. También se puede usar para hacking ético y evaluación de seguridad de redes. Pese a ser de código abierto está creada y mantenida por la empresa privada Offensive Security Ltd.

Proporciona más de 600 programas y herramientas. Y además de ser utilizada como Live, tiene la peculiaridad de poder instalada en dispositivos con arquitectura ARM (Advance RISC Machime-usado en PDA, tabletas, smartphones,…) y teléfonos android 2.1 y superiores.

La hemos incluido en este trabajo porque es una herramienta utilizada para el análisis forense, pero se aparta un poco de la pretensión del TFG. Esta distribución está más diseñada para la prevención de ataques que para el análisis forense, aunque si incluye aplicaciones forenses.

La distribución es bastante completa, tiene infinidad de herramientas, que se pueden consultar en su web (https://tools.kali.org/tools-listing). En este caso no vamos a detallar ni comentar ningún software ya que el gran volumen que tiene es inabarcable para este trabajo. Nos remitiremos

únicamente a comentar la clasificación de la lista de herramientas que tiene la distribución para tener una ligera idea de las aplicaciones que lleva: herramientas de recopilación de información, análisis de vulnerabilidad, herramientas de explotación, ataque de redes inalambricas, herramientas forenses, aplicaciones web, pruebas de estrés, rastreadores de redes y suplantación de identidades, ataque de contraseñas, mantenimiento de accesos, hardware hacking, ingeniería inversa, herramientas de informes.

Hay que destacar los numerosos recursos para los usuarios que proveen los desarrolladores de esta distribución. En su web (https://www.kali.org/) podemos encontrar tanto un blog, como documentación muy completa de la distribución y de sus herramientas, un apartado de comunidad de usuarios, y una sección para entrenamiento y aprendizaje.

Sin duda, es una distribución muy recomendable para iniciarse y desarrollarse como técnico en seguridad informática y de redes.

5.6 DEFT

Figura 13: Pantalla de inicio de la distribución Deft Zero

Deft (Digital Advanced Respose Toolkit) [8] es otra distribución linux creada para profesionales y expertos de ciber seguridad. Corresponde a un ecosistema para analizar datos, redes y dispositivos. El mayor problema es que es demasiado pesado, por lo que en 2017 lanzaron una nueva versión más ligera basada en Lubuntu llamada DEFT ZERO.

Vamos a centrarnos en esta versión ligera. Esta versión es tan ligera que funciona con tan solo 400 Mb, por lo que puede cargarse al completo en la memoria RAM de casi cualquier ordenador. También puede arrancarse desde un USB y puede usarse en modo texto o con interfaz gráfica.

5.6.1 Herramientas

Además de varias herramientas que ya hemos visto anteriormente, destaca en esta distribución

DART(Digital Advanced Response Toolkit). Es una recopilación de herramientas para el análisis y extracción de evidencias en entorno Windows. Si bien este sistema operativo no es objetivo de este trabajo, sin duda es de lo más destacable de esta distribución.

Además de este software de propósito general para el análisis forense, contiene otros específicos para el análisis de dispositivos móviles para base de datos de SQLite, para Android, Iphone, Ipad, BlackBerry, etc. También contiene software para hacer copias de seguridad de los terminales.

5.7 SIFT

Figura 14: Pantalla de inicio de la distribución SIFT

SIFT (SANS Investigative Forensic Toolkit) [9] es una distribución linux basada en Ubuntu. Desarrollada por un grupo de expertos apoyados por el SANS Institute (Institudo Americano especializado en seguridad informática). Su objetivo es dar respuesta a incidentes de seguridad y hacer un análisis forense digital.

Provee un kit de herramientas forenses y guiás rápidas de los comandos y operaciones más utilizadas. El instituto SANS se dedica a la certificación y formación de personas en el ámbito de la ciberseguridad, por lo que utiliza esta herramienta desarrollados por ellos para dar sus propios cursos. Esto hace que sea una herramienta útil para empezar a formarse en el campo de la informática forense.

Es una distribución muy completa y prestigiosa, se pueden encontrar en su web los cursos de formación que ofrece así como diversos manuales.

SIFT proporciona herramientas para examinar discos duros, dispositivos de múltiples sistemas de ficheros, diversos formatos de evidencia, examen de evidencias en modo solo lectura, etc.

Como particularidades podemos decir que soporta multitud de distintos sistemas de ficheros y copia de imágenes de discos para salvaguarda de evidencias en numerosos formatos. Esto nos da pie a que podamos analizar las evidencias con casi cualquier software que necesitemos.

Aunque está desarrollado principalmente para dar respuesta a incidentes informáticos como ataques a sistemas, mal funcionamiento de servicios, y caída de sistemas, puede también usarse como análisis forense judicial. Contiene más de cien aplicaciones incluidas en la distribución.

6 DISPOSITIVOS CELLEBRITE

Cellebrite [10] es una empresa que se dedica al diseño de software y hardware para la extracción y análisis de datos en distintos dispositivos. Está orientada más a instituciones gubernamentales (cuerpos de seguridad, fuerzas armadas) que a empresas particulares. Ofrece así mismo diferentes recursos y formación.

Se ha incluido en este trabajo su mención aunque no forma parte de la filosofía del Open Source, ya que la empresa ofrece soluciones integrales muy potentes y con validez jurídica. Esta validez junto con la facilidad de uso por parte de personal no técnico hace que sea muy utilizados por la policía en nuestro país.

Los productos más destacados son una tablet y un ordenador. Ambos son portables y conectando directamente el terminal que queremos analizar, el dispositivo es detectado e inmediatamente se puede comenzar a analizar y extraer la información.

Figura 15: Tablet todo en uno de Cellebrite

Figura 16: Laboratorio forense portátil de Cellebrite

7 EJERCICIO PRÁCTICO EXTRACCIÓN DE EVIDENCIAS

En los apartados anteriores se ha perfilado cómo es la metodología de un análisis forense informático en general y cuales son las características de la investigación policial. A continuación, se describirán todas las fases que se van a realizar para hacer un caso práctico sobre el análisis forense en tecnología móvil.

En el primer apartado detallaremos todos los pasos secuenciales que se deberían realizar para vamos a realizar el análisis que ya se comentaron en el apartado “Las fases del análisis forense”. Aquí se tratarán con más detalle y se ajustarán al caso en concreto del análisis forense para un terminal móvil.

En el segundo apartado, se describirá el caso práctico que se ha realizado para poner en ejecución estos procedimientos, detallando los pasos con fotografías descriptivas.

7.1 DESARROLLO DEL PERITAJE FORENSE PARA UN DISPOSITIVO MÓVIL

7.1.1 Descripción de las fases del peritaje forense para tecnología "smart phone"

Fase de recepción de los casos

En esta fase debemos tener un procedimiento por el cual se nos requieren los servicios de análisis forense. Dependiendo del tipo de empresa en el que trabajemos o si trabajamos como peritos autónomo mediante una bolsa de peritos se nos solicitará el análisis mediante diferentes procedimientos. Así podemos recibir peticiones directamente de un juzgado, de la policía judicial, de un abogado particular, de los interesados en un juicio, etcétera.

En el entorno de los delitos públicos (aquellos perseguibles de oficio) es el juzgado el que requiere a la policía judicial o científica la pericia en la mayoría de los casos. También es habitual que el juzgado se ponga en contacto con algún colegio profesional de peritos judiciales solicitando los servicios necesarios.

Nosotros debemos tener muy claro el cauce por el que se nos requiere para dar una respuesta profesional y concisa respetando las formas y procedimientos de los requerimientos.

Fase de identificación

Para cada caso que nos soliciten tenemos que identificar los siguientes aspectos de la petición:

1. Autoridad legal para el examen del dispositivo. Es fundamental que determinemos y documentemos si estamos legalmente autorizados para hacer el examen del dispositivo. Para ello deberemos exigir conocer los objetivos del examen, así como la profundidad y alcance

que tendremos que hacer a la información. Debemos tener máxima precaución si el dispositivo se encuentra relacionado en una investigación penal, pero también saber si somos competentes para un caso civil, administrativo o particular. Debemos tener una especial consideración y respeto a la ley de Protección de Datos Personales.

2. Objetivos del examen. Un examen general del dispositivo puede ser un proceso bastante genérico para cualquier tipo de dispositivo. Sin embargo, el objetivo de cada análisis hará diferente las circunstancias de cada caso particular. Así, para un caso muy básico puede bastar un perito con un entrenamiento básico para el examen del teléfono. En casos más complicados, requiere una mayor especialización. Por otro lado, para un caso particular la obtención de fotografías, videos, historial de llamados, mensajes de textos puede ser muy importante, y en otros casos puede ser una información irrelevante.

   Los objetivos del análisis también pueden tener restricciones legales, y verse limitadas por la necesidad de autorización judicial para el acceso y extracción.

   El objetivo del examen puede además incluir la reconstrucción de datos borrados de la memoria. Esto es normalmente solo posible si existe una herramienta disponible para un dispositivo en particular que pueda extraer datos a nivel de sistema. No todas las herramientas valen para todos los terminales.

   La definición de los objetivos del análisis puede hacer una diferencia significativa en la elección de tipo de herramientas, técnicas y método de examen. Dedicar un tiempo y esfuerzo inicial en la identificación de los objetivos del examen pude incrementar la eficiencia del proceso del análisis. Este tipo de procesos deberían ser dirigidos por personal cualificado con un entrenamiento en el proceso de triaje del dispositivo según las circunstancias individuales y la severidad del caso.

3. Marca, modelo e información del dispositivo. El forense debe de documentar el dispositivo particular que se propone analizar. Esto no vale solo para individualizar exactamente qué dispositivo vamos a analizar, si no también para saber qué herramientas tenemos disponibles para ese dispositivo en particular. Todos los teléfonos incluyen entre su información el

fabricante, marca, modelo y número de serie asociado. Todo esto debe ser identificado y documentado.

Según la tecnología del dispositivo, la información y numeración puede variar:

- Teléfonos con tecnología CDMA: Se utilizan para los teléfonos de segunda (2G) y tercera generación (3G). Se numeraban mediante el ESN (Electronic Serial Number) localizado bajo la batería, con una cifra de 32 bit en decimal (11 digiyos) o hexadecimal. Esta conversión hexadecimal ↔ decimal no es una conversión numérica (Se puede convertir en http://www.elfqrin.com/esndhconv.html) .

  Esta numeración fue remplazada por el MEID (Mobile Equipment ID) de 52 bits debido a que se terminó agotando la numeración anterior. Este MEID está listado en hexadecimal.

  Esta tecnología tiene otros dos número de identificación MIN (Mobile Identificaction Number) de 24 bit y MDN (Mobile Directory Number).

  Los teléfonos con tecnología dual, se numeran con el número ESN/MEID y además con el IMEI.

  Este tipo de tecnología se utilizan principalmente en algunas partes de EEUU y de Rusia, pero debido a que nuestro país es un destino principal turístico, puede ser que nos encontremos algún teléfono con este tipo de tecnología.
- Teléfonos con tecnología GSM. Es la tecnología más ampliamente utilizada. Utiliza para la identificación del dispositivo el IMEI (International Mobile Equipment Identifier), que es un número de 15 dígitos que identifica el teléfono en su rede. Generalmente se encuentra bajo la batería. Los primeros 8 dígitos se corresponden con el TAC (Type Allocation Code) y los restantes 6 al DSN (Device Serial Number). El último dígito es de control y usualmente es 0.

  Un teléfono GSM debe tener al mensos un módulo de identificador de suscripción (la tarjeta SIM), que suele estar alojado bajo la batería. La tarjeta SIM suele estar grabada con el nombre y la red con la que se registra, y el número ICCID (Integrated Circuit Card Identifiacation) de entre 18 y 20 dígitos e identifica de manera unívoca cada tarjeta

SIM.

- Tecnología iDEN. Se utiliza en pocos países (en España no se comercializa) y provee comunicación directa sin establecer conexión entre los teléfonos. Se identifican mediante IMEI y también tienen tarjeta SIM pero que no son compatibles con GSM

4. Dispositivos de almacenamiento asociados (Externos o extraibles). La mayoría de los teléfonos incluyen ranuras para almacenamiento externo, habitualmente memorias SD. Estas memorias externas deben ser extraídas por el forense y pueden ser analizadas usando técnicas de análisis forense digital tradicional. Hay que tener en cuenta que procesar los datos desde el teléfono puede variar datos de tiempo y fecha en los archivos de la tarjeta.

   El acceso a memorias externas alojadas en servidores externos (datos en la nube) pueden requerir permisos judiciales adicionales, pero su acceso puede ser muy valioso para el analista forense.

   Muchos teléfonos están asociados y sincronizados a otros dispositivos como ordenadores, tablets, etc. Copias de seguridad y otros datos del teléfono pueden ser localizados en los ordenadores y dispositivos a los que está sincronizado el teléfono. La existencia de estos almacenamientos alternativos deben ser tenidos en cuenta por el examinador como otras fuentes de datos.
5. Otras fuentes potenciales de evidencias digitales. Los smartphones hoy en día son mucho más que un teléfono y han avanzado mucho los sistemas de verificación de identidad. Se ha de tener en cuenta los datos contenidos en los dispositivos de las huellas digitales, características biometricas y también evidencias biológicas. Tanto para verificar el usuario, como listar los usuarios que han accedido al mismo.

Fase de preparación

Tras la fase de identificación, habremos hecho una preparación significativa para el análisis forense. Sin embargo, en la fase de preparación se realizará una planificación específica para el dispositivo que se va a examinar. Esto implica una elección de herramientas determinadas, cables,

software, drivers, etc.

En internet se pueden encontrar información técnica de hardware y software de los diferentes modelos de telefonía, en web como www.phonescoop.com

- Elección de herramientas apropiadas: eligiremos las herramientas forenses que nos den soporte suficiente para el análisis del dispositivo. Para ello, debemos de tener perfectamente identificado el dispositivo en la fase anterior, así como conocer las capacidades de cada herramienta forense.
- Capacidad de las herramientas forenses: No existe una herramienta que abarque todo el espectro de posibilidades de análisis forense. Más bien, lo que encontramos son herramientas específicas y especializadas para cada proceso, y también algunas para una marca o modelo específico. Según el objeto de nuestro análisis, tipos de datos que necesitamos, o estado del dispositivo, se emplean diferentes métodos de extracción: extracción lógica, extracción física, de sistema de ficheros, etc (Ver apartado "Tipos de extracción de datos").

Cadena de custodia

Una vez que la fase preliminar de recogida de documentación e información técnica, debemos comenzar a registrar todo lo que hacemos con las evidencias.

Así, haremos un reportaje fotográfico del teléfono móvil en el estado en el que se nos presenta y registraremos los datos relativos al terminal.

Cada vez que operemos sobre el terminal o los datos, lo recogeremos documentalmente mediante un formulario redactado al efecto. Ver aparado 1.4 CADENA DE CUSTODIA.

Cada modificación debe estar documentada, con vistas a que todos los pasos que realicemos puedan ser seguidas por el tribunal y repetidas de nuevo si fuera necesario por otro perito.

Fase de aislamiento

Cualquier dispositivo móvil tiene capacidad para conexión inalámbrica mediante diferentes redes

(Bluetooth, infrarojos, Wifi...). El aislamiento del dispositivo previene la modificación de datos por recepción de llamadas, mensajes o borrado intencionado. Por ello, una de las primeras acciones que debemos de llevar a cabo es "matar las señales". Las distintas formas de aislar al dispositivo están descritas en el apartado "Métodos de aislamiento de la red".

Fase de extracción

Una vez identificado el dispositivo, elegidas las herramientas y aislado de la red, es el momento de extraer la información convenientemente. Como se comentó anteriormente, las memorias extraibles deben analizarse separadamente del dispositivo, ya que el teléfono puede acceder a esa información y modificarla, así que la extraeremos del dispositivo.

Dependiendo de las circunstancias, objetivos, dispositivos etc, se procederá de distintas formas a la extracción, lo que hace inviable recogerlas todas en un mismo texto. Veremos un caso práctico y cómo se hace en otro apartado.

Fase de verificación e integridad de la prueba

Tras la extracción de los datos, es necesario que se verifiquen la integridad y exactitud de dicha información. No es extraño que las diferentes herramientas reporten información errónea, incompleta o distinta entre herramientas. El proceso de verificación puede ser complementado por diferentes vías:

- Comparación con el propio terminal. Podemos comparar los datos extraídos con los que el propio teléfono muestra en la pantalla y comprobar que la información es correcta.
- Comprobar la información hexadecimal. Si hemos realizado una extracción física o de sistema, con herramientas forenses tradicionales podemos verificar si la información y su decodificación son consistentes con los que proporciona la herramienta forense móvil. Este método requiere un cierto nivel de formación y experiencia. Hay muchos formatos de archivos y métodos de codificación de la información para los distintos dispositivos

móviles, lo cual puede ser un inconveniente para el examinador.

- Usar más de una herramienta y comparar los resultados. Al comparar podemos ver si hay inconsistencias. Si las hubiera debemos de utilizar otros medios para verificar la exactitud de la información. Incluso si dos herramientas dan los mismos resultados, una inspección manual del terminal es conveniente, puesto que incluso ambas herramientas pueden proporcionar los mismo informes erróneos.
- Uso de Hash. Si la extracción del sistema de archivos es posible, las herramientas tradicionales de informática forense pueden utilizarse de varias forma. El examinador después de extraer el sistema de archivos completo, hace un hash de los ficheros resultantes. Cada fichero puede ser hasheado y comprobado con el original para verificar la integridad de cada uno.

  Otra forma de trabajar sería extraer el sistema de archivo, analizarlo y luego extraer por segunda vez el sistema de archivo. Los dos sistemas (el analizado y el no analizado) pueden hashearse y comprobar si hubo modificaciones durante el proceso de análisis. Si hay cambios, pueden examinarse para determinar cuál es la razón por la que el sistema de archivos a cambiado. Los casos en los que el proceso de análisis modifican el archivo debería ser documentado y añadido al informe.

  En algunos casos, combinar varias técnicas de verificación puede ser necesaria para validar completamente la integridad de los datos extraídos.

Fase de documentación y redacción de informes

La documentación debe realizarse conforme se trabaja en las distintas fases del análisis. La documentación de trabajo puede ser útil durante todo el proceso para asegurarse que se sigue con la metodología y que la información está siendo guardada correctamente.

La documentación del análisis debería de constar de al menos estos documentos:

- Fecha y hora del inicio del examen
- Estado y condiciones del teléfono.
- Fotografías del teléfono y componentes (SIM, memorias externas), etiquetados e

identificados.

- El estado de funcionamiento del teléfono cuando lo recibimos (apagado, modo avión, sin batería, etc.)
- Marca, modelo e información para individualizar el terminal.
- Herramientas usadas durante el proceso forense.
- Datos que se documentan durante el examen.

La mayoría de las herramientas forenses incluyen herramientas de informes de los resultados, aunque no suelen ser suficientes para las necesidades de documentación. Sobre todo, son insuficientes para peritajes judiciales. Además, en estos informes automáticos la información que reportan puede ser en ocasiones errónea (incorrecto IMEI, marca y modelo, fecha y hora del examen, etc.)

EL proceso usado de extracción, la metodología, los tipos de datos extraídos y documentados, y la información encontrada, debe ser correctamente documentada en informes. Incluso si se tiene éxito en encontrar la información buscada usando las herramienta forenses, documentación adicional a través de fotografías puede ser útil, sobre todo en casos para juzgados.

- Ajustes de fecha y hora. Se debe tener una particular atención al establecimiento de las fechas y horas. Todas las fechas y horas documentadas deberían ser informadas en el horario UTC u otro estándar, pero el los teléfonos muestran la hora local. Ajustar las horas al formato estándar suele ser olvidado y diferir entre las distintas herramientas forenses. Un conflicto entre horas puede ser un error que haga confuso el informe, e incluso desvirtuarlo como prueba válida en un juicio. Hay que mencionar en los informes los ajustes de hora realizados, para evitar confusión, y explicar las diferencias relativas a las fechas y horas.

Comprobación por terceros

Todos nuestros pasos deben podre ser reproducidos en juicio oral o realizados de la misma manera por otro perito a instancias de parte o asignado por el juez. Esto quiere decir, que debemos

documentar y registrar todo de tal manera que otra persona pueda reproducirlos obteniendo los mismos datos y deduciendo conclusiones similares a las que nosotros hemos llegado.

Fase de presentación

Debe tenerse en cuenta a qué agente va presentarse toda la documentación, ya que puede variar si vamos a presentarlo a otro investigador (por ejemplo, para que continúe la investigación en el punto donde la dejamos), al ministerio fiscal, a un particular o directamente en juicio oral. En la mayoría de los casos se ha de presentar tanto en formato papel como electrónico, donde se incluirán todos los archivos extraídos, sus hash y la documentación relativa. Esta entrega de documentación ha de hacerse en vista que otro forense pueda replicar nuestro análisis en un juicio para corroborar la información; o para comprender las conclusiones obtenidas en nuestro informe.

Para casos judiciales, fotografías y videos de los datos existentes pueden ser útil para la comprensión y visualización en un juicio por parte de un jurado o personal judicial. Incluso fotografías de los mensajes de textos y chats facilitan la comprensión y son más familiares que simplemente el texto en plano en un documento.

Es muy útil presentar una serie de fotografías de las conversaciones o textos, historial de llamadas, etc. en forma de diapositivas, ya que clarifica y simplifica la compresión para una audiencia. Esto es especialmente útil para casos complejos y con varios teléfonos implicados.

Fase de archivo. Almacenamiento

La preservación de los datos extraídos y documentados es una parte importante del proceso. Es necesario una buena organización y almacenado claro para acceder al dato cuando sea necesario. Hay que tener en cuentas que desde que hacemos el análisis hasta que lo presentamos en juicio pueden pasar incluso años.

El almacenamiento con herramientas propietarias pude hacer que la versión del software con la que realizamos el análisis ya no esté disponible. Se recomienda guardar los datos en formatos no

propietarios para asegurarnos la disponibilidad y no necesitar actualizar licencias. Es asimismo una idea interesante almacenar una copia del software con la versión utilizada por si en el futuro tenemos que volver a instalarlo para replicar alguna parte del proceso.

Hacer copias de seguridad y asegurarnos que el almacenamiento es seguro es indispensable para tener disponible todo nuestro trabajo cuando sea necesario. Estos procesos de almacenamiento seguro dan garantía y continuidad a la cadena de custodia de todo el proceso.

7.1.2 Especial referencia en la extracción con el método JTAG

Qué es JTAG y cuándo lo utilizaremos

JTAG (Joint Test Action Group) se utiliza para denominar a la norma internacional IEEE 1149.1, titulada como Standart Test Access Port and Boundary-Scan Architecture. Es decir, es un estándar para acceder a los puertos de una placa de circuito impreso y así poder depurarla y probarla. Se estandarizó en 1990.

Se utiliza principalmente para depurar aplicaciones embebidas en un circuito impreso ya que provee una puerta trasera para acceder al sistema interno. Con esta depuración, el programador puede comprobar el estado correcto del sistema y corregir errores de código.

Casi cualquier sistema embebido tiene puertos JTAG y los teléfonos móviles no son una excepción. Por tanto, para el análisis forense, se aprovecha esta puerta trasera del hardware para acceder a la memoria interna del teléfono y hacer una copia bit a bit de la misma. Es lo que llamamos una extracción física de los datos.

La interfaz del JTAG se componen de cuatro o cinco pines, de tal manera que varios chips pueden tener sus lineas JTAG conectadas en forma “daisy chain” (cadena margarita) y con un solo puerto JTAG acceder a todos los chips del circuito impreso.

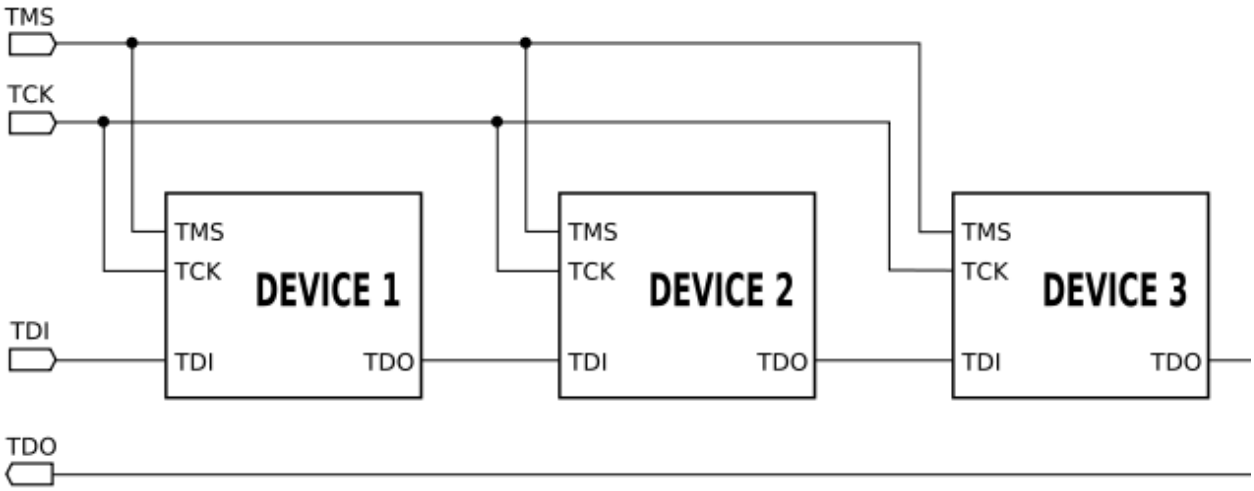

Figura 17: Esquema margarita o Daisy Chain

- TDI (Entrada de Datos de Testeo)
- TDO (Salida de Datos de Testeo)
- TCK (Reloj de Testeo)
- TMS (Selector de Modo de Testeo)
- TRST (Reset de Testeo) es opcional

Como se observa el protocolo de acceso es serie, y la frecuencia del reloj varía según el circuito, estando entorno a 10-100 Mhz.

Uno de los grandes inconvenientes que nos podemos encontrar a la hora de acceder a los JTAG de los teléfonos es que el fabricante no especifica cuál de los pines se corresponde a cada función, ya que normalmente se trata de documentación interna. Por lo tanto, encontrar esa información es crucial para no dañar los circuitos al intentar acceder a los datos.

Hardware y software necesario para la extracción

Existe hardware y software de propósito general para la conexión JTAG de las PCB tanto con

licencia libre como privada. Sin embargo, vamos a utilizar preferentemente un hardware que facilita la extracción de la información de los teléfonos conectando el teléfono a un dispositivo que, mediante un software específico, vuelca directamente al ordenador los datos.

Uno de los más utilizados es el Riff Box V 2. Consiste en una caja que tiene varios conectores, a los cuales conectamos el teléfono y el ordenador mediante un USB. El Riff Box es capaz de leer la información de los procesadores a los que conectamos y a las internas de memoria, así como hacer bit a bit de todos los datos o una partición o punto de memoria concreta.

Provee un software específico (JTAG Manager for RIFF BOX) para lanzar las instrucciones de JTAG (BYPASS, SAMPLE, IDCODE, EXTES, etc.) y además los drivers para conectar al ordenador, así como un esquema de los pines del JTAG de algunos fabricantes y modelos, y la manera de soldar los pines al conector.

Hay que destacar que no lee todos los procesadores del mercado, y debemos de saber si es compatible con el teléfono que vamos a analizar.

Como otro ejemplo de dispositivos hardware para hacer la lectura JTAG podemos citar el Easy Z3X Plus LITE (Easy Jtag Plus Box), que pueden verse los detalles en el siguiente en este enlace: https://multi-com.eu/,details,id_pr,22020,key,easy-z3x-plus-lite-easy-jtag-box,smenu,forensic_tools.html

Procedimiento de extracción con JTAG

Describiremos paso a paso cómo hacer una extracción simple de la tarjeta de memoria y su volcado al ordenador en formato de imagen de memoria con la aplicación JTAG Manager for RIFF BOX.

1. Soldamos unos cables de lo pines JTAG del teléfono y lo insertamos al conector del RIFF Box.
2. Conectamos el Riff box al ordenador mediante el USB e iniciamos el programa JTAG

Manager for Riff Box.

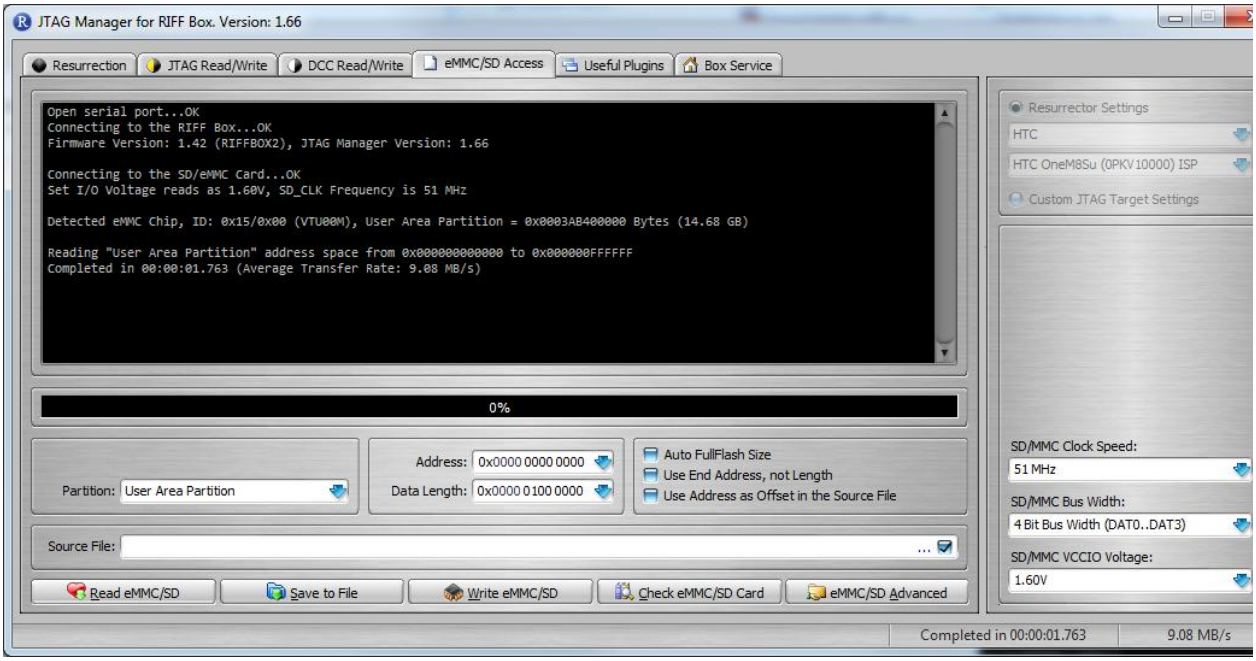

Figura 18: JTAG Manager for RIFF BOX

3. En la pestaña eMMC/SD Access del programa seleccionamos la velocidad del reloj, el Interfaz el tamaño del bus y el voltaje.
4. Pulsamos a check eMMC/ SD card para comprobar que esta todo correcto. El software leerá la tarjeta y nos proporcionaría en la pantalla información sobre el numero de serie, fecha de fabricación, nombre del producto, configuración del Boot, particiones, etc.
5. Pulsaremos el botón Read eMMC /SD Card.
6. Cuando termine, pulsaremos el botón Save to File lo que guardará un archivo con la información con la extensión .bin. El cual usaremos para analizarlo posteriormente con las herramientas forenses apropiadas.

Podremos volcar toda la memoria o una parte de ella indicando el punto de memoria que

queremos.

7.2 EJEMPLO PRÁCTICO PASO A PASO

Requerimiento del juzgado (oficio)

Juzgado de Primera Instancia e Instrucción Número 1 de Alcalá de Henares.

En virtud de lo acordado en el procedimiento de referencia, remito a Vd. el presente, junto con paquete contenedor de teléfono móvil, marca AIRIS, modelo TM55QZ, con número de IMEI 352500058495923, a fin de que procedan al examen de su contenido, y, en concreto, del material relativo a la información de un presunto delito de amenazas y de violencia de género, así como información relativa sobre registro de llamadas, mensajería sms y otros datos que pudieran ser de interés para la causa; y remitan a este Juzgado el informe pertinente, acotando las fechas a los últimos tres años desde la fecha del presente escrito.

Fase de identificación

- Autoridad legal.

Comprobamos que quien nos solicita la información es un juzgado directamente, por lo que estamos seguros que el caso se encuentra ya judiacializado y estamos autorizados a analizar el dispositivo. Además, se nos ha nombrado como peritos por el juez, por lo que no es necesario más requisitos legales para proceder al análisis forense del terminal.

- Definición de objetivos

Nos remiten un teléfono móvil y nos solicitan la información relativa a un supuesto caso de amenazas y violencia de género. Por tanto, nos interesará obtener como mínimo toda la mensajería de sms y el registro de llamadas. Además, añadiremos toda la información que podamos obtener en

las fechas comprendidas en el oficio. Tenemos que tener en cuenta que nuestro trabajo consiste en obtener la información posible para que esos datos sean investigados por personal policial o judicial.

- Identificación del dispositivo

Además de los datos que nos proporciona el propio juzgado en el oficio para individualizar el terminal, buscaremos más información del mismo. También comprobamos que no hay errores al recibir el terminal y que el teléfono corresponde con el solicitado en el oficio.

El teléfono tiene los siguientes datos:

Marca: AIRIS

Modelo: TM55QZ

S/N: TM55QZ160600916

IMEI1: 352500058495923

IMEI2: 352500058495931

- Dispositivos asociados

Comprobamos que ni se nos solicita ni en el terminal hay tarjeta sim ni tarjeta de memoria asociada. Por lo que nos limitaremos a analizar solamente la memoria interna del teléfono móvil.

Fase de preparación

- Documentación

Obtenemos la información técnica del terminal en la siguiente web: https://www.moviles.com/airis/tm55qz/caracteristicas-detalle

Los datos técnicos más importantes para nuestro análisis son:

Sistema: Dual SIM Procesador Quad-core 1.3 Ghz

Sistema operativo: Android 5.1 Lollipop

Red 3G (HSDPA): 2100, 900

Red GSM: 1800, 1900, 850, 900

Memoria RAM: 2 Gb

Memoria teléfono interna: 16 Gb

Conectividad: Bluetooth 4.0, Wi-Fi 802.11 b/g/n

Conectores: Jack 3,5 mm para auriculares, Micro USB

- Documentación gráfica del estado del teléfono

Fotografiamos el teléfono tal como nos llega. Así como todas las manipulaciones que le vayamos haciendo:

1. Estado del teléfono a la recepción.

Figura 19: Estado del terminal a la recepción

2. Quitamos la batería. Observamos que no tiene ni tarjeta SIM ni memoria extraible. Comprobamos números de serie del dispositivo e IMEI.

Figura 20: Extracción de la batería y verificación de números de serie

3. Desatornillamos la carcasa trasera y observamos la PCB.

Figura 21: Desatornillamos la carcasa trasera

4. Detalle de la electrónica visible.

Figura 22: Detalle de la placa PCB de un teléfono AIRIS

5. Detalle de los terminales del JTAG.

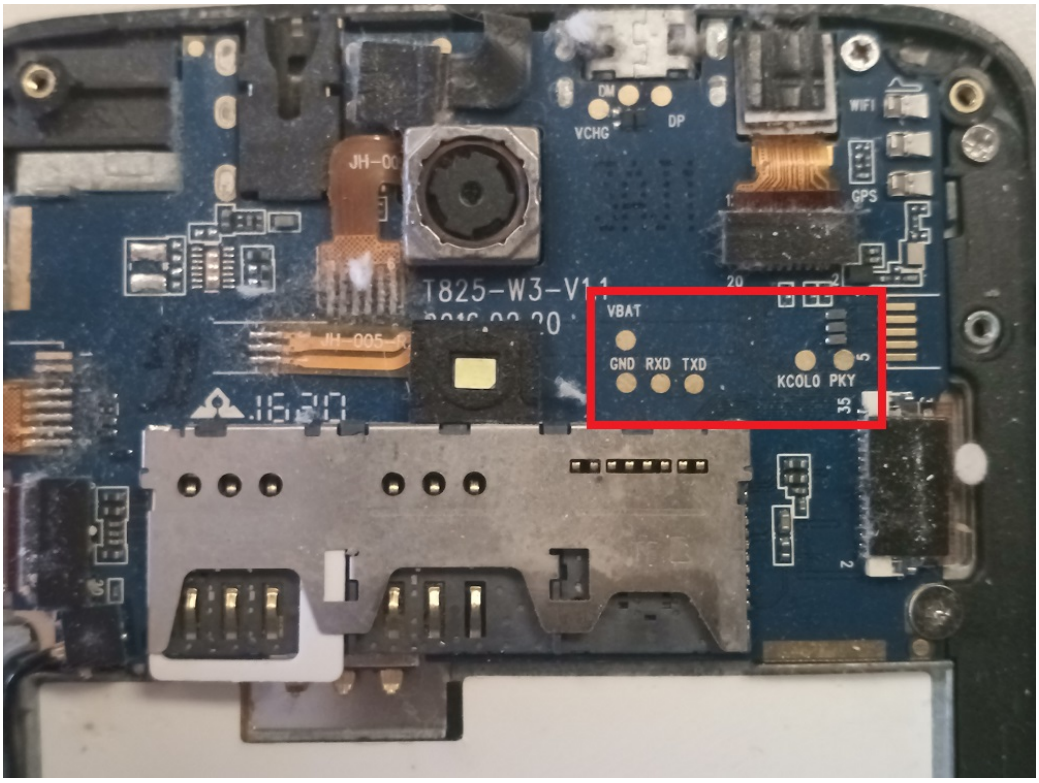

Figura 23: Detalle de los terminales JTAG del teléfono AIRIS

- Elección de herramientas

Para la extracción de la imagen de la memoria interna del teléfono vamos a utilizar el Riff Box V2 junto al software específico de JTAG Manager for RIFF BOX.

Comprobaremos la integridad de la imagen mediante la aplicación FTK imager y calcularemos el hash.

Para el análisis de la imagen usaremos Autopsy, que es la interfaz gráfica de Sleut Kit. Este es software libre con el cual obtendremos los diferentes datos así como un informe automático del

dispositivo.

Fase de aislamiento

El teléfono nos llega apagado y sin batería, con lo cual primeramente lo cargamos al máximo, y luego lo encendemos. A continuación, lo configuraremos en modo avión para aislarlo de cualquier conexión inalámbrica.

Toma de pruebas (simulación JTAG)

La extracción de JTAG tiene muchas dificultades, no todos los terminales son compatibles, y es difícil encontrar la documentación que indique qué pines son los que corresponden a cada función. Además, hemos tenido dificultades en conseguir el dispositivo Riff box ya que no es un dispositivo que se pueda encontrar en la distribución habitual en electrónica.

Por ello vamos a explicar el análisis forense a partir del archivo de imagen obtenido por otros medios.

En un apartado anterior (7.1.2 Especial referencia en la extracción con el método JTAG), explicamos cómo se obtenía la imagen física de un dispositivo.

No obstante, aunque en este ejercicio no hayamos realizado propiamente la extracción mediante JTAG, se ha intentado sacar la imagen de la memoria interna del teléfono mediante extracción física conectándolo con un usb. El terminal ha dado problemas, no se encendía por estar dañado y no hemos podido sacar la información.

Asimismo, se ha probado con varios terminales distintos pero ha sido imposible rootearlo para acceder a los datos. Configurar el terminal móvil como super usuario es necesario para hacer una copia bit a bit de la memoria del teléfono. Por defecto vienen sin los privilegios de administrador y hay que “hackearlos”. Sin embargo, este proceso no es sencillo y las herramientas disponibles no son válidas para todos los terminales. Por ese motivo, no nos ha sido posible con los otros dos

terminales que se disponía para probar.

Se puede concluir que estas técnicas forenses no son muy accesibles y no son viables para cualquier modelo de dispositivo.

Finalmente hemos realizado el análisis forense con una imagen de memoria disponible como ejemplo en la web https://www.cfreds.nist.gov/mobile/index.html [11]

A pesar de ello, comentaremos brevemente cómo se extrae la imagen de memoria de un teléfono móvil mediante un cable USB:

1. El terminal lo encendemos y lo configuramos para tener las opciones de desarrolladores. Seguidamente activamos el modo depuración por USB.
2. Necesitamos los privilegios de super usuario, por lo cual tenemos que rootearlo mediante la aplicación de escritorio KingoRoot.
3. Con los comandos de ADB conectaremos y mandaremos instrucciones al teléfono mediante conexión USB. Mediante el comando “adb devices” vemos que el dispositivo está conectado.
4. Levantamos una terminal en el teléfono con la instrucción “adb -d shell”.
5. Comprobamos los datos del dispositivo y vemos el árbol del sistema con el comando ls /data
6. Vemos las particiones con “cat /proc/partitions”
7. Instalamos la apk Bussy boxen el teléfono con:”adb install "C:\Tools\APK\BusyBox.apk"
8. Preparamos el puerto de red sobre la que trabajaremos mediante “adb forward tcp:9999 tcp:9999”
9. Procedemos a la creación de imagen forense con el comando: “dd if=/dev/block/mmcblk0 | busybox nc -l -p 9999”
10. Sacamos la imagen a nuestro ordenador “nc 127.0.0.1 9999 > C:\Evidences\AIRIS.dd”
11. Calculamos hash con el archivo para empezar con la cadena de custodia.

Análisis de pruebas

Como comentamos anteriormente, para el análisis vamos a usar una imagen ejemplo descargada

de la web https://www.cfreds.nist.gov/mobile/index.html [11] ante la imposibilidad de conseguir extraer una con los terminales disponibles.

Se trata de un rerminal móvil Samsung Galaxy S4 – SGH-M919, con número de IMEI 356420053614244.

Con la imagen del dispositivo con la extensión ".bin" nos dispondremos a realizar el análisis forense e intentar obtener la información solicitada por el juzgado.

Lo primero es hacer una copia de seguridad, la cual guardaremos sin modificarla en un pendrive extraible y otra copia la subiremos a un almacenamiento en la nube. Esta copia servirá para comprobar los hash y volver a hacer el proceso de análisis si fuera necesario.

Calculamos el hash con la aplicación FTK imager.

Nos da como resultado un hash MD5: 8a4dd45985d8311b2c62f5e248da51a3

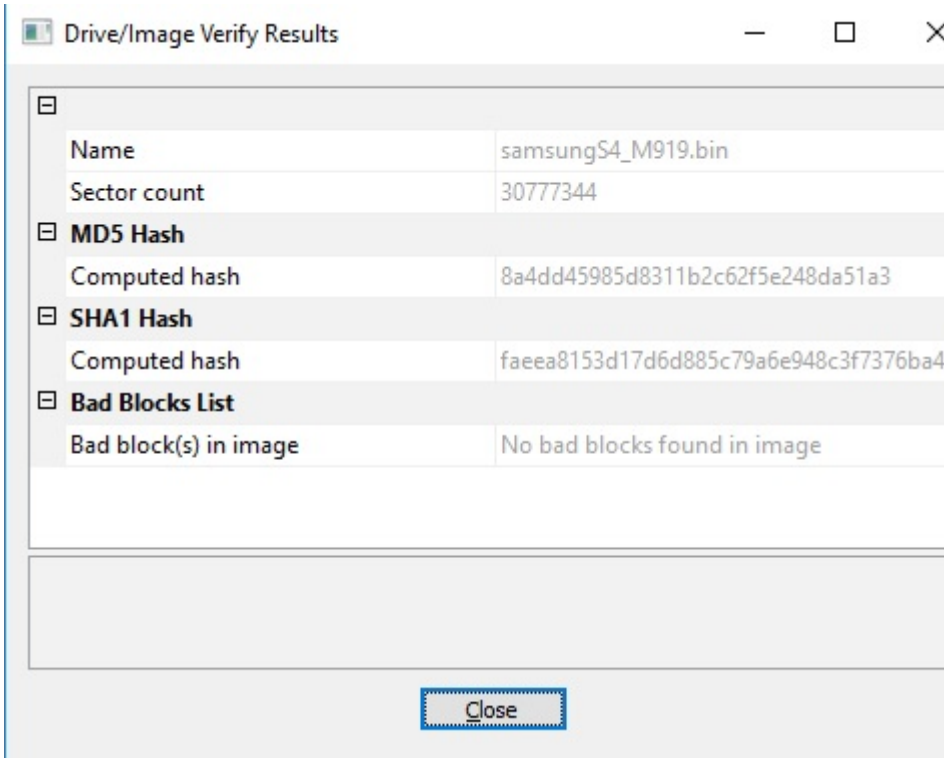

Figura 24: Hash del terminal Samsung S4 obtenido con FTK imager

Rellenaremos la cadena de custodia correspondiente para registrar la copia de seguridad, el hash para la verificación de la integridad de la prueba, con la fecha, hora y lugar de la copia.

Posteriormente abrimos la aplicación Autopsy y creamos un caso nuevo.

Rellenamos diferentes datos como el nombre del caso, número, examinador, etc.

Pulsamos añadir “Data Source” y seleccionamos la imagen de la memoria.

La aplicación abre la imagen, seleccionamos todas las características posibles para analizar.

Pulsamos terminar y la aplicación empieza a analizar la imagen.

La duración del análisis es variable pero suele tardar una hora o más tiempo.

Tras el análisis podemos observar que podemos acceder muy fácilmente a las imágenes, videos, mensajes de texto, etc.

Todos los datos pueden visualizarse desde la aplicación o extraerse y guardarse aparte. También se da la opción de extraerse los listados de los datos en formato .cvs

Entregaremos al juzgado todas los datos y archivos para que sean ellos los que valoren si son relevantes para el caso.

A continuación extraeremos todos los datos posibles:

- Imagenes/Videos

En este apartado buscamos las imágenes que se han realizado con la cámara. Exploramos en la carpeta de la cámara y visualizamos las imágenes. Podemos acceder fácilmente a los metadatos para ver información adicional.

Seleccionamos todas las imágenes de la cámara y las extraemos a nuestro ordenador mediante la función especifica para ello.

Registramos en la hoja de cadena de custodia los datos a la extracción realizada con fecha, hora y lugar, así como la localización de los archivos.

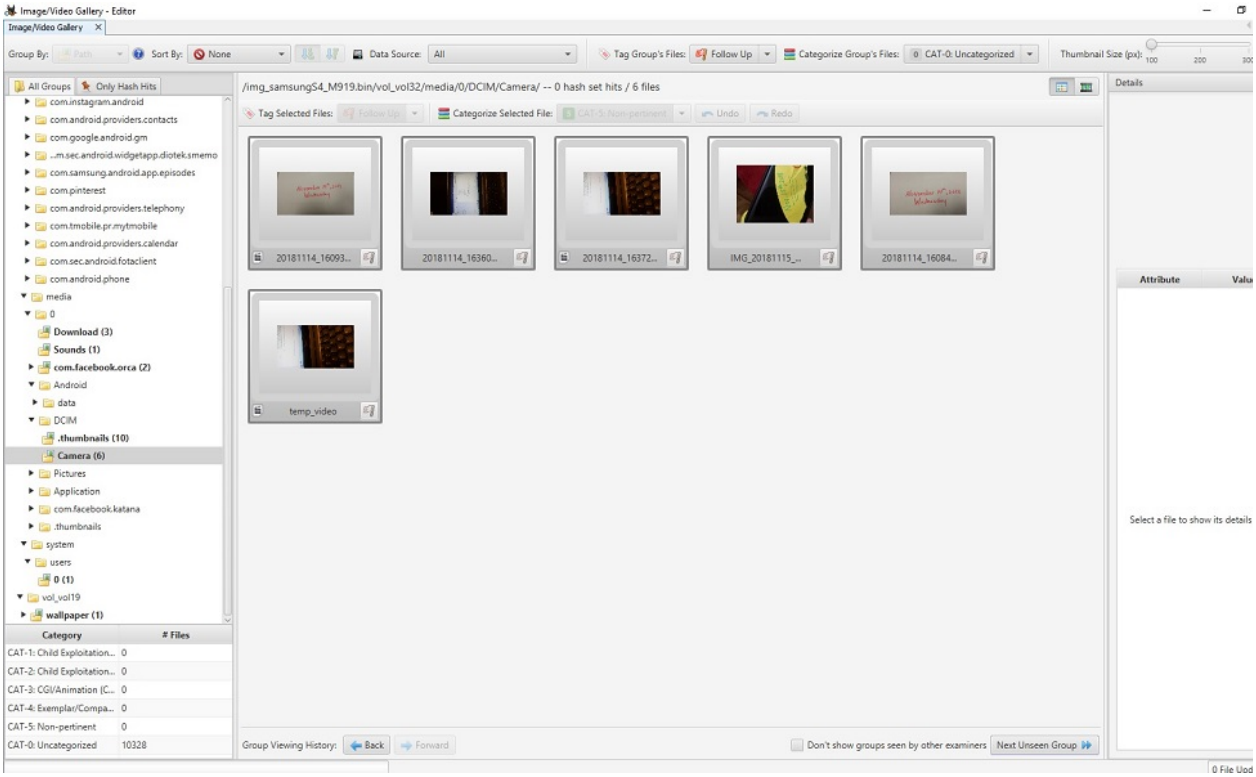

Figura 25: Extracción de Imágenes / Videos con aplicación Autopsy

- Comunicaciones

En esta función vamos a extraer los datos relativos a las comunicaciones que se han realizado con diversos teléfonos.

En el análisis vemos varios números de teléfono pero no sabemos cuál es el de la víctima. Para evitar hacer una intromisión en datos personales que no son relevantes al caso, nos ponemos en contacto con el Juzgado para que nos facilite el número de teléfono de la víctima, a fin de hacer un análisis más profundo del mismo para ese número en concreto. Le enviamos el listado de todos los teléfonos y les instamos a que indiquen cuál de ellos tiene interés para la causa a fin de hacer un análisis más exhaustivo.

Nos responden que tienen interés en dos números de teléfono en concreto sin concretarnos más información.

En la aplicación los seleccionamos uno a uno y visualizamos los mensajes de texto, el registro de

llamadas, el contacto con más información etc. Extraemos todos esos datos para entregarlos al juzgado.

Registramos en la hoja de cadena de custodia los datos a la extracción realizada con fecha, hora y lugar, así como la localización de los archivos.

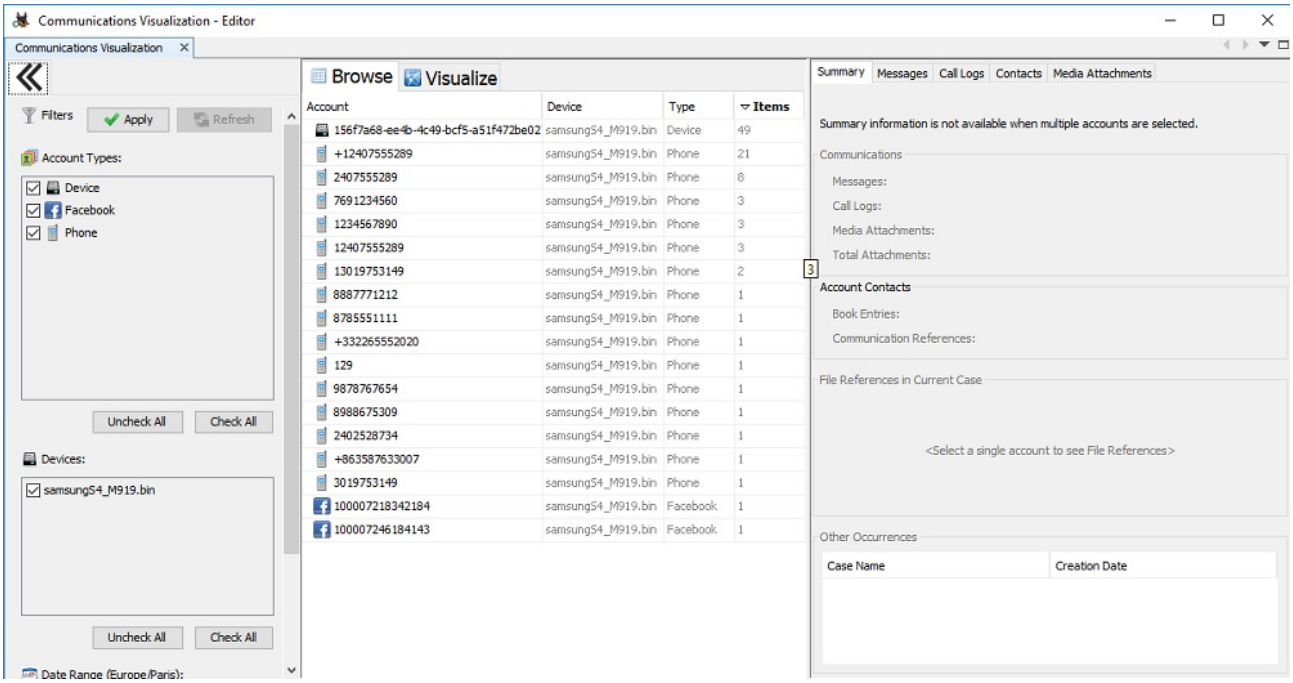

Figura 26: Análisis de comunicaciones de la aplicación Autopsy

- Geolocalización

En este apartado podemos visualizar las localizaciones del teléfono por su GPS, por la información de los navegadores de internet, conexiones WIFI, etc. Como no nos han pedido expresamente esta información simplemente daremos un pantallazo al mapa con las localizaciones y lo remitiremos como información extra. Instando al juzgado que si requiere más información sobre localización, está disponible para su análisis.

Registramos en la hoja de cadena de custodia los datos a la extracción realizada con fecha, hora y lugar, así como la localización de los archivos.

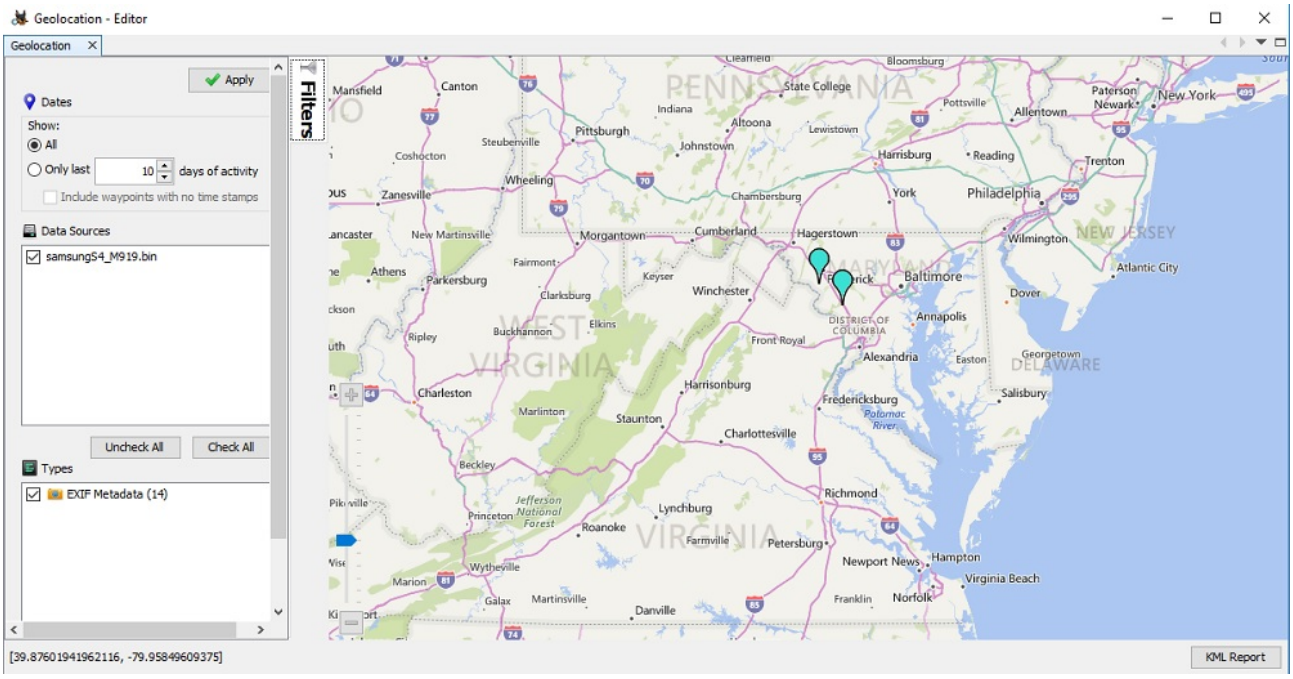

Figura 27: Geolocalización aplicación Autopsy

- Línea del tiempo

Esta función sirve para generar una linea temporal de la evidencia y ver los eventos que ha tenido un dispositivo o archivo. Estos eventos son información sobre creación, modificación, copia, creación de logs, eliminación, permisos, etc.

En el caso solicitado nos piden solamente los archivos y la información para el caso, no un seguimiento temporal de un archivo concreto. Puesto que no se nos solicita, no remitiremos ninguna información al respecto.

- Explorador de archivos

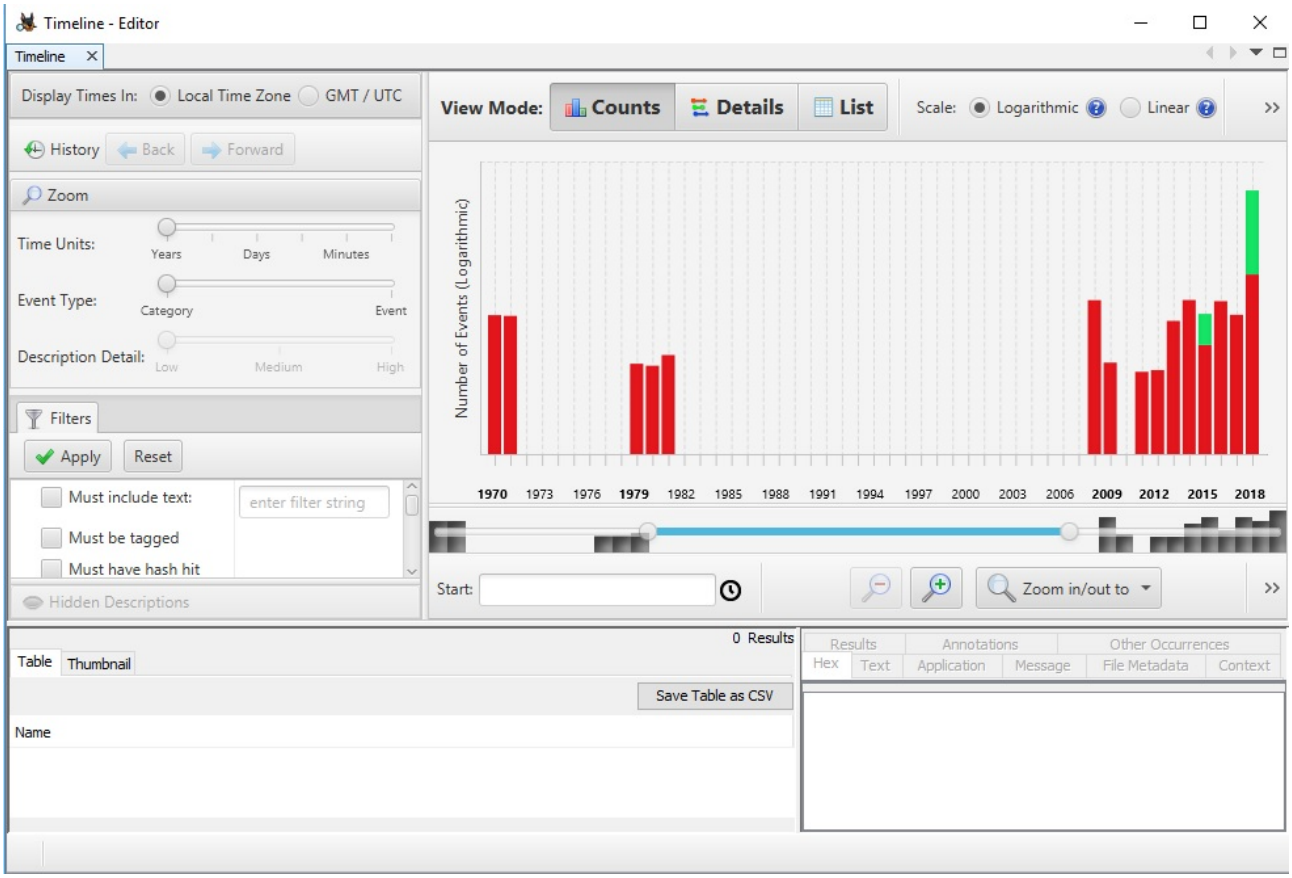

Figura 28: Línea del tiempo de la aplicación Autopsy

En esta función podemos buscar archivos de imágenes, videos y documentos según varios filtros: tamaño de almacenamiento en memoria, fuente de datos y posibilidad de ser creado por el usuario del terminal.

Para nuestro caso no vamos a usar esta función porque no nos es necesaria.

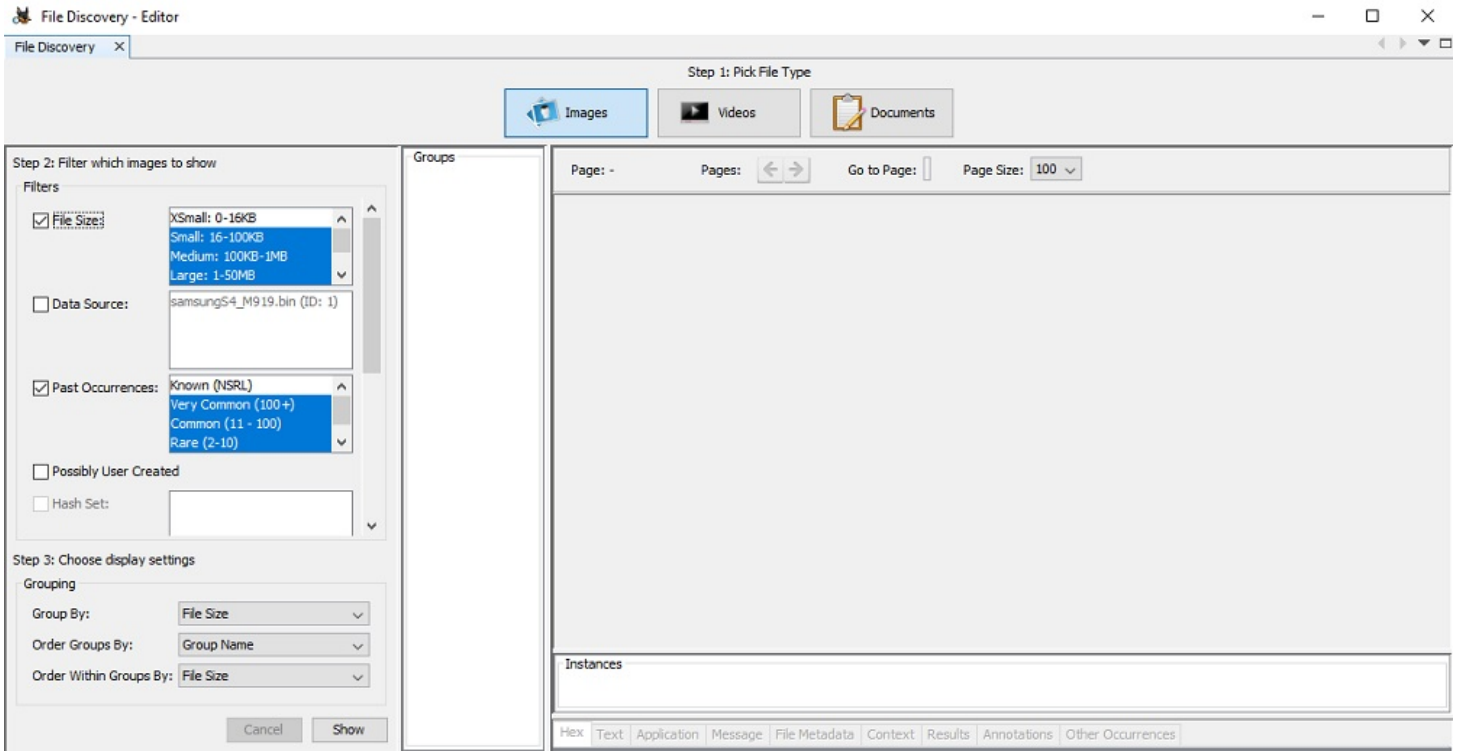

Figura 29: Explorador de archivos de la aplicación Autopsy

- Archivos eliminados

Con esta herramienta podemos visualizar los archivos que se han eliminado. En algunos podemos acceder al contenido tanto con la propia aplicación de Autopsy como una externa. También podemos extraerlos a nuestro ordenador, ver la linea del tiempo de creación, modificación y eliminación; etc. En este caso, no vamos a extraer los archivos eliminados, pero si facilitaremos al juzgado un listado en formato .csv para que tengan constancia de ellos y que nos soliciten el contenido de alguno de ellos si es de interés para el caso.

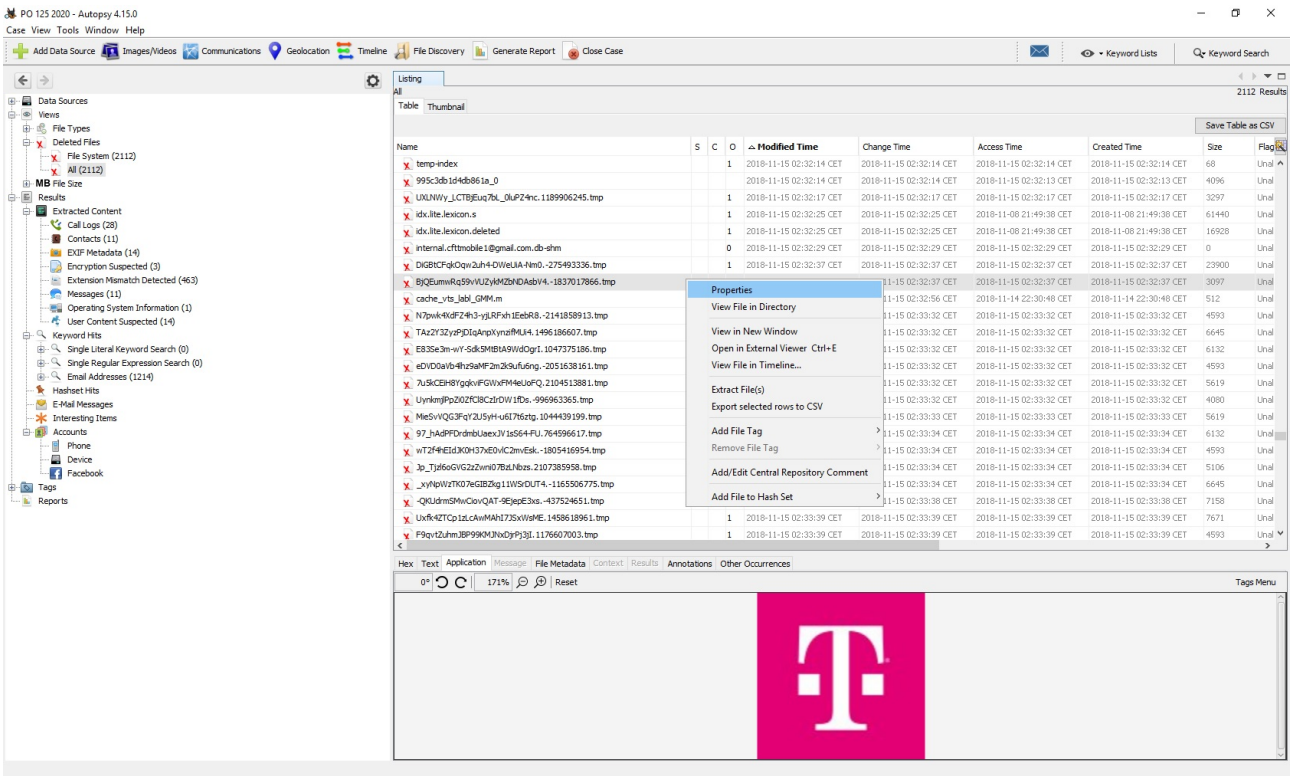

Figura 30: Extracción de archivos eliminados de aplicación Autopsy

- Informe automático

Autopsy genera un informe automático con un resumen de todos los datos que contiene el terminal. Nos proporciona en un único archivo los datos del software utilizado para la extracción, fuente de los datos, las cuentas del teléfono, contactos, marcas de geolocalización, etc.

Este informe automático lo podemos obtener en varios formatos. Los más comunes son como HTML para visualizarlo en un navegador web, o en formato de hoja de cálculo

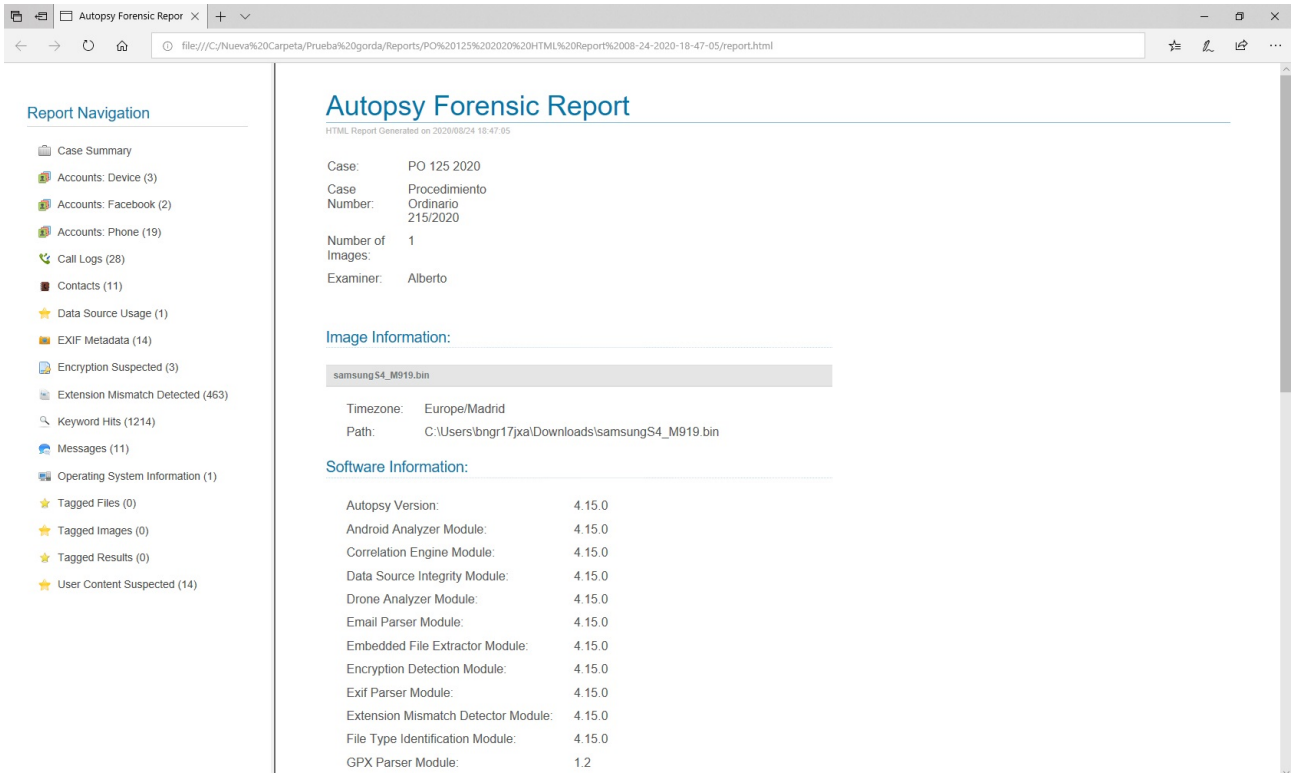

Figura 31: Informe automático de la aplicación Autopsy

Conclusiones del análisis

Se han extraído todos los datos que nos han solicitado así como otra información que podría ser útil para la causa. Como no conocemos los detalles del caso ni sabemos qué información es relevante y cual no, remitimos lo que se nos ha pedido e informamos al juzgado de los datos disponibles que se encuentran en el terminal como la geolocalización o los archivos eliminados por si fuera necesario extraerlos.

Como conclusión podemos asegurar que se han podido extraer suficiente información para que puedan ser analizados por los investigadores y tenemos a disposición judicial de otra información que podría ser interesante para el caso.

Redacción del informe pericial

Tras el análisis del dispositivo y la extracción de todas las evidencias, registradas todas ellas en la hoja de cadena de custodia, debemos plasmar todo el proceso en un informe pericial. Como explicamos en el apartado 1.6 INFORME PERICIAL, éste es un documento técnico que sirve para documentar todo nuestro trabajo de análisis y en el que constan todos los pasos realizados que hemos realizado en este apartado, pero sin las explicaciones didácticas.

Como venimos comentando durante todo este trabajo, uno de los apartados importantes del informe pericial es la hoja de custodia y registro del dispositivo y los archivos extraídos en todo el proceso de análisis. Este documento se adjuntará como anexo en un acta aparte del informe para ser verificado por el juzgado y las partes implicadas.

Juicio oral y preparación de la información

Además del informe pericial que es un documento técnico, necesitamos explicar todos los pasos realizados en un juicio. Es decir, debemos de presentar la información a personas que no tienen porqué tener conocimientos de informática ni electrónica, por lo que debemos usar un lenguaje asequible.

En nuestro caso, una presentación tipo Power Point con los pasos realizados que se observen visualmente con fotografías cómo se han realizado los pasos, debería ser suficiente para hacerse una idea clara de cómo se ha realizado el análisis forense.

8 CONCLUSIONES

El paradigma de la ingeniería como disciplina especialista en un campo concreto está cambiando al aprendizaje transversal. La unión de distintas áreas de conocimiento para el entorno laboral es una necesidad cada vez más demandada. Tener competencias en ramas aparentemente inconexas dan como resultado una gran fortaleza interdisciplinar, una visión más completa de los problemas y unas capacidades resolutivas mayores.

En este proyecto se han unido las ciencias jurídicas, la metodología policial, y las competencias

de ingeniería de comunicaciones, electrónica e informática. Esta transversalidad es necesaria para la labor de un perito judicial especialista en TIC, un área muy demandada actualmente y con amplias proyecciones de futuro.

El software libre es un recurso excelente para el aprendizaje y desarrollo profesional de la labor del perito judicial. Provee herramientas completas y específicas para el peritaje y solventa los problemas de validez jurídica de los procedimientos penales.

El aprendizaje continuo y la actualización de conocimientos son imprescindibles para dar un servicio correcto a las demandas actuales de evolución tecnológica.

Por otro lado, también hemos comprobado que la extracción física de la memoria con JTAG es una técnica compleja con poca posibilidad de éxito. Es por ello un recurso que se utiliza únicamente cuando no hay otra posibilidad de extracción por otros medios.

Hemos tenido dificultades para el acceso al hardware necesarios para la extracción JTAG, y también hemos verificado que no todos los terminales son compatibles. Tampoco la extracción física a través de USB es viable en todos los terminales, y la configuración del dispositivo para tener los privilegios de administrador es no es posible en algunos casos.

El peritaje forense de dispositivos móviles es un campo inabarcable en un trabajo fin de grado como éste, requiere una gran especialización así como una formación continua y actualizada de los forenses, pero ofrece un área interesante de desarrollo profesional.

9 LEGISLACIÓN APLICABLE

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

- Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Estándares y normativas internacionales:

- RFC 3227. Manejo y recolección de evidencias.
- Familia UNE 71505:2013. Mecanismos y buenas prácticas para la gestión de evidencias electrónicas.
- Normas ISO/IEC 27037. Tratamiento de la evidencia digital.

10 BIBLIOGRAFÍA Y WEBGRAFÍA

Bibliografía y webgrafía

[1] E. Velasco Núñez. Delitos tecnológicos: definición, investigación y prueba en el proceso penal. Ed.SEPIN.2016

[2] D.G. Policía.Temario para ascenso a Oficial de Policía. (2018) [Publicación restringida] Available: https://www.policia.es/org_central/division_forma_perfe/contacto.html

[3] Asociacion profesional de peritos judiciales .Codigo deontológico. (2020) [Online] Available: https://www.aspejure.com/codigo-deontologico.php

[4] INCIBE.Referencia de herramientas forenses del Centro de respuesta a incidentes de seguridad. (2020) [Online] Available: https://www.incibe-cert.es/blog/herramientas-forense-moviles

[5] NowSecure .Web de la distribución de Santoku. (2020) [Online] Available: https://santoku-linux.com

[6] Nanni Bassetti.Web de la distribución de Caine . (2020) [Online] Available: https://www.caine-live.net/

[7] Ben Wilson.Web de la distribución de Kali linux. () [Online] Available: https://www.kali.org/

[8] Deft Community.Web de la distribución de DEFT Zero . (2020) [Online] Available: http://na.mirror.garr.it/mirrors/deft/

[9] SANS Incident Response.Web de la distribución de SIFT. (2020) [Online] Available: https://digital-forensics.sans.org/

[10] Cellebrite.Web oficial de la empresa Cellebrite . (2020) [Online] Available: https://www.cellebrite.com/es/pagina-principal/

[11] Agencia NIST.Web del Computer Forensic Reference Data Sets (CFReDS) for digital evidence, de la agencia NIST https://www.cfreds.nist.gov/mobile/index.html . (2020) [Online] Available: https://www.cfreds.nist.gov/mobile/index.html

Universidad de Alcalá
Escuela Politécnica Superior