Importance of Memory as Digital Evidence in Forensic Computing

Tiffany Viviana Estupiñan Londoño, Est. Ingeniería de Sistemas[1], Karen Tatiana Mora Merchán, Est. Ingeniería de Sistemas[2], y Claudia Patricia Santiago Cely, Msc. Gestión de Información,[1]
[1]Escuela Colombiana de Ingeniería Julio Garavito, Colombia,
tiffany.estupinan@mail.escuelaing.edu.co,claudia.santiago@escuelaing.edu.co,
[2]Escuela Colombiana de Ingeniería Julio Garavito, Country, karen.mora@mail.escuelaing.edu.co

Abstract -- The present investigation raises the importance of the relationship between memory and the management of digital evidence against a forensic investigation, through the analysis of techniques, methodologies and tools that allow the forensic compilation of information in this component available in each device. Considering the different factors that must be taken into account, as well as the types of existing memory in order to reach the conclusion of their importance in front of the legal processes and forensic scenarios in which they are analyzed.

Keywords – Forensic, Memory, Evidence, information.

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2019.1.1.477
ISBN: 978-0-9993443-6-1 ISSN: 2414-6390

IMPORTANCIA DE LA MEMORIA COMO EVIDENCIA DIGITAL EN LA INFORMÁTICA FORENSE

Tiffany Viviana Estupiñan Londoño, Est. Ingeniería de Sistemas[1], Karen Tatiana Mora Merchán, Est. Ingeniería de Sistemas[2], y Claudia Patricia Santiago Cely, Msc. Gestión de Información,[1]
[1]Escuela Colombiana de Ingeniería Julio Garavito, Colombia,
tiffany.estupinan@mail.escuelaing.edu.co,claudia.santiago@escuelaing.edu.co,
[2]Escuela Colombiana de Ingeniería Julio Garavito, Country, *karen.mora@mail.escuelaing.edu.co*

Resumen- ***La presente investigación plantea la importancia que tiene la relación entre la memoria y la gestión de evidencia digital frente a una indagación forense, mediante el análisis de técnicas, metodologías y herramientas que permiten hacer la recopilación forense de la información en este componente disponible en cada dispositivo. Considerando los diferentes factores que deben tenerse en cuenta, así como los tipos de memoria existentes, para de esta manera llegar a la conclusión de su importancia frente a los procesos legales y escenarios forenses en los que se analizan.***

Palabras Clave - ***forense, memoria, evidencia, información***

I. INTRODUCCIÓN

Actualmente con el rápido crecimiento de las tecnologías de la información, la gran cantidad de datos que recolectan y el aumento de los ataques, es necesario no solo cada uno de ellos sino crear mecanismos que permitan conocer cómo recuperar la información que se puede perder en caso de incidente como es el caso del robo de información empresarial, suplantación e incluso pornografía infantil.

La memoria, como componente principal de un dispositivo que genera y almacena datos, es el objetivo principal de los ataques informáticos, razón por la cual es fundamental conocer su significado y su importancia dentro de una investigación forense para de esta manera saber cómo responder ante un incidente relacionado a un delito informático. Teniendo en cuenta todo esto, el artículo presentará la definición de la memoria, su clasificación, su capacidad, el tipo de información que puede contener y los tipos de memoria que existen, así como también su relación con la forensia digital aplicando las técnicas y metodologías existentes como lo son el volcado de memoria o la copia forense, que permitan hacer un análisis correcto de la información que contienen y que puede ser muy importante ante la investigación frente a un delito informático para de esta manera obtener pistas del ataque realizado y su perpetrador.

Finalmente, el articulo busca presentar una serie de conclusiones del por qué se considera que la memoria es base fundamental frente a una investigación forense ante cualquier tipo de dispositivo vulnerado. Para esto se planteará un escenario general y se llevarán a cabo una serie de pruebas que buscan comprobar el trabajo en conjunto de las memorias definidas y las técnicas y metodologías que plantea el análisis de evidencia digital en los sistemas operativos (SO) más comunes existentes como lo son Windows, Linux y MacOS, de igual manera se realizará en dispositivos móviles con el sistema Android.

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2019.1.1.477
ISBN: 978-0-9993443-6-1 ISSN: 2414-6390

II. MARCO TEÓRICO

A. Memoria

La memoria en informática es un dispositivo a base de circuitos que permite almacenar limitadamente la información de la computadora, muchas veces conteniendo información vital no solo para el propietario sino para el funcionamiento de la máquina como tal, pues son clave para el arranque del dispositivo o la ejecución de instrucciones. Son diversos los tipos de memoria y de acuerdo a sus características, difieren sus funciones. Entre las características principales se encuentra su capacidad que es medida en bytes, pues es una referencia importante al momento de calcular la potencia de un computador, haciendo énfasis que en cuanto mayor sea la cantidad de memoria que posea un dispositivo mejor será su rendimiento.

Ya que la memoria hace parte fundamental de la arquitectura del dispositivo, como componente también posee su propia arquitectura que define los tipos de memoria existentes, así como el tipo de información que almacena.

Los niveles que componen la jerarquía de memoria habitualmente son:

- Nivel 0: Registros del microprocesador o CPU
- Nivel 1: Memoria caché
- Nivel 2: Memoria primaria (RAM)
- Nivel 3: Memorias flash
- Nivel 4: Disco duro (con el mecanismo de memoria virtual)
- Nivel 5: Cintas magnéticas (consideradas las más lentas, con mayor capacidad, de acceso secuencial)
- Nivel 6: Redes (actualmente se considera un nivel más de la jerarquía de memorias). [1]

En el nivel 0 se encuentran los registros del procesador que usa el sistema operativo para controlar la ejecución de programas y ofrecen un nivel de memoria más rápido y pequeño que la memoria principal, que permite a los usuarios conocedores del lenguaje de ensamble acceder a estos registros y hacer uso óptimo de la memoria principal. Así mismo contiene registros utilizados por el procesador para el sistema operativo para controlar la ejecución de programas.
En el nivel 1, se encuentra la memoria caché, la cual almacena datos de rápido acceso con información volátil lo que le permite ser de apoyo para la memoria principal y de esta

manera mejorar la capacidad de procesamiento (Fig.1). Cuando un dato es accedido por primera vez una copia del acceso es guardada en caché haciendo más rápido su posterior acceso, razón por la cual se renueva constantemente. Un elemento a considerar es el tamaño de la memoria caché, en la actualidad los procesadores indican que usan 3 niveles de caché: L1 de 10KB a 20 KB, L2 de 128KB a 512KB y L3 de 4M a 12MB.

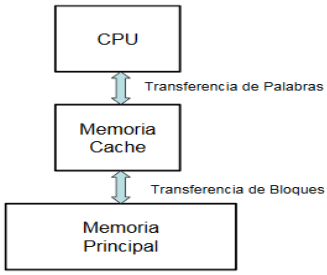

Fig. 1 Memoria Caché [2]

La memoria caché L1, es un tipo de memoria pequeña y rápida que está en la unidad de procesamiento central, utilizada para acceder a datos importantes de uso frecuente. La memoria caché L2, es utilizada para almacenar información reciente fue diseñado para reducir el tiempo de acceder a datos que han sido usados anteriormente, se usa para almacenar los datos e instrucciones de programas. La memoria caché L3 es una memoria que está integrada en la placa madre. Se utiliza para alimentar a la memoria caché L2, y generalmente es más rápida que la memoria principal del sistema.

En el nivel 2 se encuentra la memoria Random Access Memory (RAM) la cual es considerada como uno de los componentes más importantes de la CPU puesto que es la encargada de almacenar y ejecutar todas las instrucciones asignadas por el procesador, así como las órdenes de otros componentes tales como la tarjeta gráfica, el disco duro e incluso aplicaciones que se ejecuten en el equipo, pero de manera volátil, por lo que al momento de apagar el equipo toda esta información va a desaparecer. Cabe resaltar que al igual que la memoria cache, la memoria RAM presenta variaciones que difieren de su uso, pero cuentan con la misma funcionalidad, entre las que se encuentran VRAM, DRAM, SRAM, DDR RAM y DDR (DDR2, DDR3, DDR4) donde estás últimas son las más usadas en la actualidad pues presentan un mejor rendimiento a un costo muy bajo en el consumo de energía.

De esta manera cuanta más memoria RAM tenga un dispositivo más posibilidades tiene de poder abrir varios programas al tiempo, pues incluso aunque no lo parezca, el entorno gráfico, el fondo de pantalla o el uso del ratón representan un consumo de memoria RAM. Al referirse a la memoria RAM es inevitable mencionar la relación con la arquitectura Von Neumann, que a pesar de ser de rendimiento limitante para el dispositivo sigue siendo muy usada en la actualidad, pues esta plantea que el tamaño de la unidad de memoria está fijado por el ancho del bus que comunica la memoria con la CPU. [3]

Teniendo en cuenta la arquitectura Von Neumann [4], además de la memoria RAM aparece un tipo diferente de memoria no mencionado en los niveles de la jerarquía, esto es porque muchas veces es confundida con la memoria RAM y se trata de la memoria Read Only Memory (ROM) que tiene la función de almacenar los datos e instrucciones necesarias para que el dispositivo pueda arrancar por lo tanto no es volátil lo que hace su acceso más lento pues como su nombre lo indica es de solo lectura. La memoria flash tiene una relación directa con la memoria ROM, pero permite que múltiples áreas de memoria sean escritas o borradas en una misma operación, y esta es la que utilizan en la actualidad la mayoría de dispositivos con memoria flash como las memorias USB, tarjetas SD y más recientemente los SSD y también disponibles en dispositivos móviles e inteligentes. [5].

Es así como llegamos al nivel 3, memorias Flash, señalando su principal característica y es la resistencia a los golpes, pues al no incluir elementos mecánicos en su interior puede moverse con mayor libertad lo que la hace ideal para dispositivos móviles. Adicionalmente esto lo hace mucho más silencioso, de bajo consumo y de tamaño reducido. No obstante, no todo son ventajas, puesto que solo permite una cantidad finita de escrituras y borrados, generalmente entre 10.000 y 1 millón), lo que hacen los controladores de estos dispositivos es ir añadiendo datos nuevos a partes que nunca se han usado para así no quemarlas demasiado pronto. Inicialmente almacenaban 8 MB, pero actualmente almacenan más de 64 GB, con una velocidad de hasta 20 MB/s.

Con estas grandes capacidades de almacenamiento alcanzamos el nivel 4 de la arquitectura de memoria que son los discos duros, también llamados, hard disk (HDD). Es un dispositivo de almacenamiento magnético que aloja de forma permanente la información del ordenador, incluyendo el sistema operativo y las aplicaciones. Éste funciona por medio de un sistema de grabación magnética y está compuesto por uno o más discos que se unen y giran a gran velocidad, sin embargo, actualmente existen los discos duros de estado sólido que usan procesos químicos para grabar la información, lo que lo hace mucho más resistente a daños y golpes, así como representa una mejora en velocidad de lectura y escritura, comparado con el disco magnético.

Para los últimos niveles de la jerarquía es importante destacar que son los usados para hacer copias de seguridad o de soporte. La cinta magnética es un tipo de soporte de almacenamiento de información que permite grabar datos sobre una banda de material magnético, que son usualmente utilizadas para hacer Backus, sin embargo, aunque algunos expertos aseguran que poco a poco ha entrado en desuso, se desarrollan avances en esta tecnología [6].

Por otra parte, en el último nivel se encuentran los sistemas de almacenamiento de red, la cual es una arquitectura de almacenamiento a nivel de archivos en la que uno o más

servidores almacenan datos en discos dedicados y los comparte, lo que hace que los datos sean más accesibles entre los dispositivos de una red. Los tres principales sistemas de almacenamiento usados son:

- SAN: (Storage Area Network),
- DAS (Direct Attached Storage)
- NAS: (Network Attached Storage)

Habiendo definido a manera general la memoria y su jerarquía, es necesario entender cómo se relaciona con la forensia digital. Por lo tanto, se denomina Análisis Forense Digital como un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial. Por evidencia digital se entiende al conjunto de datos en formato binario que comprende los archivos, su contenido o referencias a éstos (meta-datos) que se encuentren en los soportes físicos o lógicos del sistema atacado y que se encuentra almacenado en la memoria del equipo. [7]

Cabe resaltar que el papel de este componente en la recopilación de evidencia digital es de vital importancia, pues sin importar el tipo de memoria que se esté manejando en una investigación, es necesario asegurar que su información no sea alterada de ninguna manera dado que esto comprometería su admisibilidad ante la corte.

De acuerdo a [8] la Constitución Política de Colombia en su artículo 15 permite fundamentar el diseño de la técnica informática en cuanto a la extracción de la evidencia digital para anclar la cadena de custodia, donde se establece el derecho a la intimidad, por lo que se deben respetar la libertad y promover las demás garantías consagradas en la Constitución, apoyado en la Ley 527 de Agosto 18 de 1999 que trata de los instrumentos magnéticos e informáticos, así como la ley 527 de 1999 sobre el comercio electrónico para Colombia, la Ley 1273 de 2009 para la protección de la información y de los datos y la Ley 1273 del 2009 que tipifica los delitos informáticos con el fin de penalizar a los infractores.

En todos y cada uno de los casos analizados se debe tener en cuenta el procedimiento adecuado para realizar la recopilación de la información. Para este procedimiento es necesario comenzar por llevar una orden de recopilación de información dando la posibilidad de ser admitidos en un proceso judicial. Luego se debe determinar el tipo de evidencia que se busca en la investigación, lo que ayuda a determinar la relevancia de los datos. Una vez se ha establecido el tipo de información que se busca y lugares probables donde encontrarlos, es necesario fijar qué datos son volátiles y pueden contener información sensible, necesaria para la investigación. Hay que considerar adicionalmente que, para comenzar el proceso de recopilación, se debe eliminar la interferencia externa, establecer las herramientas necesarias, así como documentar todas las acciones realizadas para validar el proceso de recolección de evidencia. Finalmente es necesario hacer el análisis de la evidencia, el cual se dará por terminado cuando se descubra cómo fue realizado el delito, el porqué, quien o quienes lo cometieron, bajo qué circunstancias, cuál era el objetivo del ataque y qué daños causaron.

B. Evidencia Digital

La evidencia digital se presenta en diferentes formas y debe ser recopilada de acuerdo a su tipo: volátil, persistente, lógica y física. En el caso de la evidencia volátil y persistente se debe hacer directamente sobre la memoria del equipo, pues a diferencia de tipo lógico y físico no implica el uso de hardware externo que pueda alterar la evidencia.

a. <u>Técnicas de recolección de datos</u>

Son procedimientos especiales utilizados para obtener y evaluar las evidencias necesarias, suficientes y competentes que le permitan formar un juicio profesional y objetivo, que facilite la calificación de los hallazgos detectados en la materia examinada. [9]

i. Volcado de memoria

Los volcados de memoria son una representación binaria que tienen los sistemas o registro no estructurado del contenido de la memoria en un momento determinado, ésta técnica está relacionada generalmente a RAM, sin embargo, es posible hacer el mismo proceso en el disco principal del equipo. Por la naturaleza de sus datos es necesario tener en cuenta que es prioridad generar el volcado de memoria antes de avanzar con cualquier otro análisis o tarea en el equipo. Para esto se debe tener claro qué tipo de volcado se va a realizar según su clasificación:

- Disco a imagen: Creando una copia bit stream que consiste en crear una imagen virtual de la memoria con sus respectivos hashes de seguridad que aseguran su veracidad en una corte. Es el método más habitual y más rápido. Además, permite realizar tantas copias como sea necesario de una manera fácil y sencilla para la fase de análisis.
- Disco a disco: es utilizado en caso de que no sea posible realizar una copia bit stream de disco a imagen, pues consiste en generar la copia de un disco a otro. Del mismo modo que el método anterior se puede realizar tantas copias como sean necesarias, no obstante, para esto sería necesario tener varios discos disponibles. La realización de un clonado mediante un dispositivo hardware conlleva una mayor fiabilidad y rapidez.
- Creación de una copia de datos dispersos de una carpeta o archivo: es decir, realizar una copia selectiva, ya que en muchas ocasiones dependiendo del tipo de incidente puede no ser necesario volcar todo el disco y sea suficiente copiar ciertas carpetas o archivos.

En caso de que se requiera hacer una copia sectorizada del disco es necesario usar la técnica, Master Boot Record que

hace referencia al primer sector, sector 0, de un dispositivo de almacenamiento de datos. Posee un tamaño de 512 bytes y almacena información relativa a cómo iniciar el sistema, qué tipo de particiones hay en el dispositivo y el tamaño de las mismas, etc., lo que la hace útil para el análisis de registros.

ii. Copia Forense

Esta técnica consiste en copiar todo el contenido de un disco duro, bit a bit, en otro dispositivo de almacenamiento con una herramienta que permita generar una firma hash de los bits leídos durante el proceso. obteniendo de esta forma, una copia exacta a bajo nivel de todo el contenido del disco duro además de certificar su contenido con la firma hash. Se realiza con el fin de certificar y mantener la cadena de custodia de las evidencias, ya que, de no hacerse correctamente, las pruebas recolectadas quedarían invalidadas. Con el gin de garantizar la fiabilidad de la evidencia es necesario crear un hash que asegure la evidencia y la mantenga sin modificaciones (fig. 3) [10].

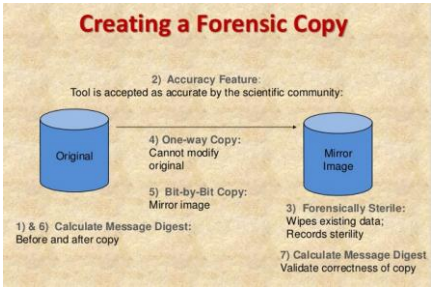

Fig. 2 Pasos de creación de copia forense

iii. Imagen Forense

Es una técnica particular que permitirá crear una copia exacta del dispositivo o equipo original en uno nuevo. Esto significa que el original y la copia serán idénticos al momento preciso en que se hizo la imagen, al grado que incluso, de ambas se pueda recuperar información borrada a través de técnicas, tan sencillas con herramientas especializadas en cómputo forense o de técnicas más tediosas como el análisis manual de archivos en hexadecimal. La imagen forense cumple entonces con los conceptos básicos del cómputo forense: identificar, preservar, recuperar, analizar y presentar hechos y opiniones. Por tanto, al **preservar** todos los atributos del origen permiten que los hechos y opiniones puedan presentarse en tribunales.

b. Metodología para el tratamiento de Evidencia digital

La metodología general del procedimiento de evidencia digital, se centra en 4 pasos principales [11]:

1. Aislamiento de la escena: Restringir el acceso a la zona del incidente, para evitar algún tipo de alteración en la posible evidencia a recolectar.
2. Identificación de fuentes de información: Los datos relacionados con un evento específico son identificados y evaluados a su vez que el incidente se controla, para posteriormente proceder con la fase de recolección y examinación.
3. Examinación y Recolección de Información: Técnicas y herramientas forenses son aplicadas a los datos recolectados para extraer la información relevante, sin alterar la integridad de los datos.
4. Análisis de datos: Técnicas y herramientas forenses son aplicadas a los datos recolectados para extraer la información relevante, sin alterar la integridad de los datos.
5. Reporte: Informe de los resultados del análisis que puede incluir los procedimientos que se llevaron a cabo, si quedaron verificaciones pendientes, mejoras, cambios entre otros.

IV. PROPUESTA PARA LA RECOPILACIÓN DE EVIDENCIA DIGITAL

Previo a la iniciación del procedimiento de análisis de evidencia digital, es necesario verificar que el evento reportado como incidente de seguridad, realmente atenta contra la confidencialidad, integridad o disponibilidad de la información. Una vez confirmado el incidente, se procede a aplicar la metodología anteriormente descrita, lo que permite determinar si es el incidente requiere o no de un análisis forense. Por lo general el equipo, sin importar su SO, se puede encontrar en 2 posibles estados, encendido, con procesos en ejecución, conectado a la red y con información de interés en medios como la memoria volátil y muerto, en que el dispositivo se encuentra desconectado, sin procesos activos y con información no volátil. En cualquiera de los dos casos, es necesario asegurar que el estado del equipo no cambie y de esta manera evitar la alteración de la evidencia.

Con base en lo anteriormente descrito, esta investigación se encuentra centrada en la parte fundamental dentro del proceso de análisis forense, la etapa de examinación y recolección de información. Para esto se identificaron los elementos y dispositivos más usados, generando un ambiente digital frecuente en una organización. En una infraestructura tecnológica moderna es común encontrar computadores con SO Windows, Linux y MacOS, así como dispositivos móviles, Android y IOS. Por otro lado, es usual encontrar estos dispositivos con niveles de privilegios o protegidos con claves de acceso. A partir de esta identificación tecnológica del entorno en que se desarrolla esta investigación, se presenta una propuesta de las herramientas y procedimientos que se deben seguir dentro del proceso de recopilación de evidencia.

Por lo general el equipo se puede encontrar en 2 posibles estados, encendido, con procesos en ejecución, conectado a la red y con información de interés en medios como la memoria volátil y muerto, en que el dispositivo se encuentra desconectado, sin procesos activos y con información no volátil.

Tomando como referencia los capítulos 17, 18 y 19 del libro "Digital Evidence and Computer Crime" en los que aplican un análisis forense a los diferentes Sistemas operativos existentes, a continuación, se busca evidenciar el proceso aplicado a la memoria del dispositivo. [12]

a. *Windows*

En el sistema operativo Windows lo primero a tener en cuenta son las herramientas disponibles para hacer la recuperación de información, luego la manera en la que este sistema operativo almacena los registros del equipo. Dado que tienen contraseña de administrador para acceder al sistema operativo, es necesario usar herramientas que permitan saltar estos permisos sin alterar la información, para esto se usa la herramienta Kon-boot que pertenece a la suite de Hiren'sBoot y permite adquirir permisos de administrador. Sin embargo, para poder usarlo el equipo debe encontrarse apagado pues se debe correr desde el arranque del equipo, de lo contrario será necesario obtener la contraseña directamente desde el administrador. Para el escenario planteado algunos equipos se encontraron encendidos y otros apagados de manera que ambos métodos fueron usados. Luego es necesario hacer una copia bit a bit de los medios de almacenamiento para lo que se recomienda el uso de herramientas tipo LIVECD como DEFT con lo que se genera el correspondiente Hash en MD5 y SHA-1 para garantizar la integridad de los datos adquiridos.

A Continuación, es necesario analizar la imagen lo que por medio de la misma herramienta es posible hacerlo, pues la mayoría de las suites permiten montar de manera segura la imagen para poder recorrer directorios y archivos con mayor facilidad, usualmente se usa una herramienta como dd2vmdk para crea un disco virtual de la imagen y poder analizarla sin correr riesgos, pues la información se aísla totalmente del sistema lo que evita un cambio inesperado.

En la fase de análisis de Datos se realiza el análisis temporal, la búsqueda de contenido, recuperar los binarios y documentos borrados o corruptos, búsqueda de archivos ocultos o no usuales, búsqueda de procesos en ejecución, búsqueda de cuentas de usuario. todo esto con el objetivo de encontrar evidencia relacionada al caso.

Pruebas y Resultados

Se hizo una prueba específica en la recopilación de datos en una memoria flash, más específicamente en una memoria USB con el fin de conocer las funciones de las herramientas. Las herramientas usadas en este caso fueron, Helix y Deft, para de esta manera obtener la línea de tiempo de la información registrada en la memoria. Para esto, se debe comenzar con una copia de disco, realizada a través de Helix , que nos permite analizar la información sin comprometer su integridad. Pese a que Helix contiene múltiples funcionalidades, en este caso particular se quiso usar para la recopilación de información antes y actualmente contenida en la memoria USB, para esto se usa la herramienta FTKimager contenida en el kit de Helix CDLive (fig. 5). Al terminar la copia, genera cuatro tipos de archivos, donde uno corresponde a la imagen como tal de memoria y los otros tres corresponden a informes tanto de información recopilada como de las herramientas utilizadas.

Fig. 3 Menú Helix CDLive

Al momento de analizar cada uno de estos archivos, encontramos que en el caso del archivo en formato txt, se trata de un informe generado por la herramienta FTK imager, con el fin de garantizar la autenticidad de la copia pues en este se incluye información de los investigadores, de la imagen y del hardware, así como la verificación del MD5 y SHA1 generados al comenzar la copia. Por otra parte, el archivo formato .xls entrega toda la información relacionada a los datos almacenados (o alguna vez almacenados) en la memoria, facilitando el análisis de la información organizándolo en las siguientes categorías: filename, Full path, size, created, Modified, Accessed, Is deleted, permitiendo de esta forma conocer qué tipo de información se encuentra almacenada, cual estuvo alguna vez almacenada, así como las fechas de creación, modificación y eliminación de los archivos.

Adicionalmente arroja un informe en formato pdf como se puede ver en la figura 5, que permite conocer a detalle todos y cada uno de los movimientos realizados por los investigadores en la herramienta, desde el momento en que se ejecutó Helix., todo esto con el fin de asegurar el correcto manejo y recopilación de la información.

Fig. 4 Informe de Uso de la herramienta Helix

Durante la segunda parte de la recopilación de datos en la memoria, se usa DEFT mediante una máquina virtual en la que se procede a recuperar la mayor cantidad de información

posible. Con la herramienta recuva disponible en el kit de Deft fue posible recuperar muchos de los archivos que se encontraron en con la anterior herramienta como eliminados, lo que permitió en la investigación hacer un comparativo de información recuperada. Con este primer acercamiento al funcionamiento de las herramientas, se dio paso a un proceso más completo de la recolección de memoria. Realizado en un equipo de cómputo donde se buscaba recopilar la mayor cantidad posible de actividades realizadas en el equipo comprometido. Este procedimiento se llevó acabo en 3 diferentes puntos de la organización , pero en todos se hicieron pruebas muy similares comenzando con un volcado de memoria que arrojaba los mismos resultados que en la recolección realizada con la memoria USB, obteniendo los mismos archivos anteriormente mencionados y adicionalmente realizando la copia 3 veces con el fin de mantener inalterable la información recopilada con lo que se recomienda tener discos de gran capacidad donde se permita hacer tal copia sin inconvenientes. Con el objetivo de hacer un uso más exhaustivo de las herramientas disponibles se usó DART, disponible con la distribución de DEFT y se realizó un análisis más exhaustivo sobre una de las copias generadas anteriormente en el que se obtuvieron resultados de información almacenada en cache, como contraseñas e imagenes. Como es el caso de WinAudit disponible en Incident Response de DART el cual genera un archivo pdf con todas las especificaciones de la máquina evaluada. De igual manera con la herramienta forensic – browser forensic tool para detectar todas aquellas búsquedas realizadas en el PC, que de acuerdo a una clasificación predeterminada puede clasificar las búsquedas como redes sociales, pornografía, hacking entre otras. De esta manera y con el uso de varias aplicaciones disponibles en este kit fue posible hacer un análisis profundo de la copia generada llegando a conclusiones tan básicas como el uso dado a los equipos en sus búsquedas de navegadores (aunque el historial fuera borrado), hasta las posibles actualizaciones que hicieran que el equipo tuviera reinicios inesperados o que pudieran simbolizar una vulnerabilidad al sistema.

i. Linux

Para el caso de Linux, se encuentran muchas más herramientas forenses ya que por su facilidad de ser de código abierto permite mejor adaptabilidad a las necesidades del peritaje en cada caso concreto. Esto hace que Linux sea la mejor opción para construir entornos específicos para el análisis forense que pueden ser iniciados desde discos externos (LIVE CD) o en máquinas virtuales. De esta manera permite utilizar las herramientas para extraer y analizar las evidencias procedentes de otros sistemas operativos pues al ser de código abierto, supone un ahorro para los peritos y la hace compatible con muchos de los sistemas analizados. Sin embargo, por la misma razón, puede generar inseguridad entre los agentes legales frente a una investigación.

No obstante, es un sistema que ofrece varias utilidades nativas que permite hacer la recopilación de evidencia sin alterar, por accidente, la información con la instalación de herramientas externas. Adicionalmente posee comandos que pueden ser usados en un entorno forense sobre la copia forense de cualquier dispositivo con sistema operativo Linux. Tal es el caso del comando "Dataset Definition" (dd) el cual permite la creación bit a bit de particiones del disco o del disco completo. El uso de este comando es simple, sin embargo, existen varias consideraciones a tener en cuenta; Lo primero es conocer las particiones / discos duros que tiene el sistema, algo que se puede conocer fácilmente con el comando "`sudo fdisk -l`" o con algún programa gráfico de particiones como `gparted`, pero esto último es poco recomendable, pues podría alterar los registros del dispositivo. Aunque no es un comando difícil de usar y su información se puede consultar con el comando "`man dd`" e "`info dd`", se recomienda usarlo con precaución pues, así como copia la información de un disco, así mismo la puede eliminar si se usa una instrucción mal. Otra consideración a tener en cuenta, es que, por ser un comando reservado, no es posible visualizar su proceso de ejecución por lo que muchas veces se usa acompañado del comando "`pv`" que permite obtener en el terminal una especie de barra de progreso, la información sobre bytes transferidos, el tiempo que lleva ejecutándose y la tasa de transferencia, todo esto en tiempo real.

Otros comandos de interés nativos que ofrece Linux son "`uname -a`" y "`lsb_release -a`" nos mostrarán las principales características del sistema, como pueden ser la versión de kernel y la distribución del sistema operativo. Por otra parte, como se mencionó de manera sutil anteriormente el comando "`fdisk -lu /dev/sda`" permitirá obtener las diferentes particiones existentes en el disco duro `/dev/sda`, así como los sectores de inicio y fin de cada una de ellas. Esto también nos servirá para comprobar el *hash* de las imágenes de cada partición en caso de ser necesario.

Básicamente Linux, permite desde su propio sistema por medio de comandos obtener información y más allá de las prestaciones que pueda ofrecer una herramienta implementada en el mismo sistema operativo, muchas veces será más útil y eficaz hacerlo directamente.

Pruebas y Resultados

Lo primero a tener en cuenta es verificar el estado de la máquina, en caso de que se encuentre apagada, será útil el uso de herramientas como deft o Helix en modo arranque.

Por otra parte, si la máquina se encuentra encendida lo primero a hacer es realizar el volcado de memoria o la copia bit a bit del disco, que como se mencionó con anterioridad se puede realizar usando el comando dd. Sin embargo, antes de recopilar la evidencia de memoria es necesario obtener información sobre el disco y sus particiones. Para lo que se usa el comando. Para listar todas las particiones existentes en

nuestro sistema pasaremos el argumento "-l" (fig. 6), que hará que se listen ordenadas por el nombre del dispositivo.

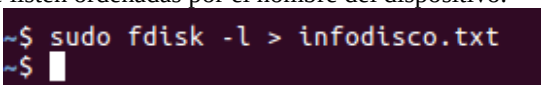

Fig. 5 comando para recopilar

Esto creará el archivo "infodisco.txt" en la carpeta en la que estamos ubicados por defecto, donde el archivo contendrá la misma información mostrada en pantalla. Conociendo el disco y sus particiones, es posible realizar la copia (clonación de disco) bit a bit con el comando dd, mediante la instrucción `root#dd if=/dev/sdx of=/dev/sdy bs=1M.`
Donde if significa "input file=archivo de entrada ", es decir, lo que se quiere copiar y of significa "output file=archivo de salida ", o sea, el archivo destino (donde se van a copiar los datos); origen y destino pueden ser dispositivos (lectora de CD o DVD, disco duro, USB, partición, etc.), archivo de copia de seguridad o imagen de disco, etc, pero no carpetas o subcarpetas. Cómo se explicó anteriormente, el comando es "ciego" por lo que no permite ver el progreso del proceso, para que esto sea posible se agrega un comando adicional, obteniendo como resultado una instrucción de la siguiente forma:
En el experimento, se puede observar que el comando pv permite ver una barra de progreso de la copia. Así como para que esto sea posible, fue necesario instalar la instrucción `pv`, lo cual sería un riesgo a cambiar la información recolectada y caso en el que se recomendaría hacer uso de las herramientas anteriormente mencionadas. Otra información importante y fácil de recuperar por medio de los comandos de Linux son los procesos que corren en el momento de realizar la investigación. Para esto será necesario usar el comando "`Ps`" que permitirá visualizar todos los procesos que corren, de igual manera, si se quiere guardar esta información en un archivo de texto bastará con añadir "`>procesos.txt`". Este comando permitirá no solo visualizar los resultados sino guardarlos en un archivo para su posterior (fig. 7). Obteniendo un archivo de texto con la misma información mostrada en terminal.

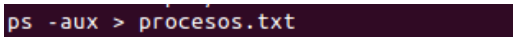

Fig. 6 Comando para extraer procesos

Otro comando importante que nos ayudará en todo este proceso de la recopilación de información es "`top`" la cual nos ayuda a conocer los procesos de ejecución del sistema en tiempo real que se va a ir actualizando cada 3 segundos. Muestra un resumen del estado de nuestro sistema y la lista de procesos que se están ejecutando. Aunque es posible enviar esta información a un archivo de la misma manera que se ha hecho con los otros comandos, el archivo resultante no es del todo claro y su lectura es casi imposible. Además del hecho, que, por actualizarse cada 3 segundos, la copia al archivo podría nunca terminar y es necesario cancelarla para poder continuar. Sin embargo, es posible realizar el análisis con la información mostrada en pantalla.

Finalmente, los últimos comandos que podrían considerarse de utilidad en una investigación forense, son "`w`" y "`last`" que hacen relación a los usuarios y accesos al sistema respectivamente. Por una parte "`w`" muestra qué usuarios están en nuestro sistema, y qué están ejecutando. Por otro lado, el comando "`last`" muestra un listado con los últimos accesos (`login`) al sistema. En conclusión, cabe destacar que, aunque el sistema operativo trae por defecto varios comandos que pueden ser utilizados durante una investigación forense, lo más recomendable es usar herramientas que garanticen la integridad de la información recopilada y dado el caso de análisis se pueden usar las mismas que se usaron en Windows, siendo que lo único que cambia es su forma de ejecución y permite hacer una recolección y análisis más exhaustivo.

ii. Mac OS

Una de las características principales de MacOS es que, por ser cerrado, presenta bajos porcentajes de ataques o incidentes de seguridad, sin embargo, pues en los últimos años se ha evidenciado el gran aumento de ataques a estos sistemas operativos. Es por esto que MacOS requiere una metodología única y especial para investigar ataques en sistemas de Apple, no obstante, herramientas forenses son muy escasas para este sistema. Esto no quiere decir que hacer forensia en sistemas MacOS sea imposible, pues al igual que con Linux y Windows, solo se requiere el conocimiento básico del tipo de archivos y extensiones que maneja, con el fin de conocer dónde y qué clase de información buscar. Cabe destacar que las herramientas para hacer forensia en este SO, no son nada fácil de encontrar y muchas veces deben ser pagas lo que representa una brecha muchas veces en las funciones de un perito.

Pruebas y Resultados

Se usó una máquina con sistema operativo MAC versión El capitán (10.11.3) donde se realizó el análisis con una de las herramientas más recomendadas por expertos para Mac que es Pac4Mac de código libre y fácil ejecución. Esta herramienta se descarga directamente desde github y contiene herramientas python, las cuales basta con ejecutarlas desde la terminal para usarlas. Lo que desplegará un menú numérico que permite escoger la herramienta a utilizar de pendiendo de la información que se pretenda recolectar como se puede ver en la figura 8.

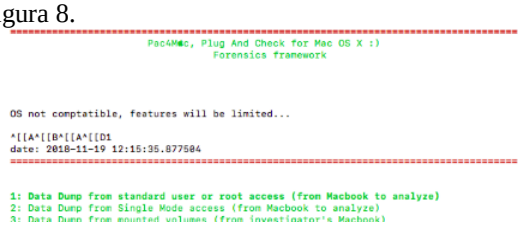

Fig. 7 PAC4MAC

Aunque la herramienta indicaba que el sistema operativo no era compatible, esto no fue impedimento para permitir su uso. Las opciones que despliega hacen referencia al volcado de memoria sobre el equipo, por lo que es lo primero que se ejecuta. El resultado de esto, es una carpeta llamada "Results" que se crea automáticamente, donde se encuentra el volcado de la memoria y registros del sistema operativo. Adicionalmente presenta en diferentes carpetas la demás información recopilada, tal es el caso de la carpeta "Users", que contiene archivos en formato txt con la información relacionada a los usuarios autorizados en el equipo como se muestra en la figura 9.

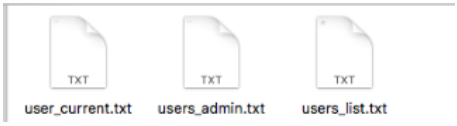

Fig. 8 Información obtenida

Por otro lado, se observa que la mayoría de archivos recuperados son en el formato propio del sistema plist (fig.10). Acompañado de un archivo en .txt que básicamente es la copia de la información recuperada.

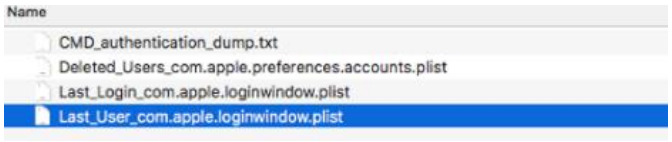

Fig. 9 Información Relacionada

Adicionalmente esta herramienta cuenta con muchas funcionalidades que permiten obtener la información en consola sin generar archivos adicionales con el simple hecho de permitir un análisis más concienzudo y rápido del sistema. Adicionalmente por ser una herramienta forense, arroja un informe final del trabajo hecho y cada uno de los archivos generados contienen un hash que asegura la integridad de la información.

iii. Dispositivos Móviles

Ya que el dispositivo móvil representa una parte importante en nuestra vida diaria y hace parte del escenario planteado, el enfoque de recopilación de evidencia digital no se puede sesgar únicamente a computadores, es necesario pensar también en la navaja suiza digital que representa un dispositivo móvil. Gracias a esto la información que guardan estos dispositivos es muy relevante y en caso de que se cometa algún delito puede llegar a ser de mucha utilidad y esto facilita algunos procesos judiciales, es entonces donde entra en juego el análisis forense de dispositivos móviles y las herramientas que existen a disposición para el objetivo. Se presume que la información que se puede recopilar de este tipo de dispositivos es mucho más amplia que en un dispositivo convencional, pues se pueden recuperar historiales de llamadas, de mensajes, de emails, de navegación, así como, fotos, videos y en general cualquier tipo de archivo que haya sido almacenado o incluso borrado del dispositivo.

Hay que tener en cuenta que la mayoría de las terminales están bloqueados con algún tipo de patrón o contraseña (incluso aunque sean biométricos, tienen de contraseña de respaldo que permiten acceder al dispositivo) por eso es que lo primero que se debe hacer es tener herramientas que permitan desbloquear la contraseña. Sin embargo, una recomendación general que se hace respecto al punto anterior es clonar el dispositivo en caso de que se llegue al límite de intentos impuesto por el fabricante, de modo que al introducir varias veces la contraseña errónea no se bloquee y destruya la información que contiene.

Pese a que no existe una metodología estándar sobre la manera específica de hacer análisis forense de dispositivos móviles, hay una serie de guías que pueden servir de pauta a seguir para la correcta realización del proceso. Por un lado se encuentra el documento "Guidelines on Mobile Device Forensics" del NIST (National Institute of Standards and Technology) [13] en que habla a nivel general del dispositivo, la estructura de sus archivos, de la memoria, el tipo de conexión a internet que usa, mientras que a nivel de forensia habla de la clasificación de extracción que usan las herramientas disponibles (manual , lógica, JTAG, etc) , además de esto sugieren algunas herramientas y muestran sus utilidades de acuerdo a los niveles de adquisición lo que lo hace un documento con información muy completa a la hora de recopilar evidencia digital .

En el momento de realizar el proceso de extracción existe un número notable de herramientas que se deben tener en consideración. Dependiendo de su funcionamiento interno pueden ser catalogadas de diferentes maneras. Como base para su clasificación se puede utilizar la pirámide propuesta por Sam Brothers en la U.S. Cybercrime Conference de 2011 (fig 11).

Fig. 10 Pirámide de tipos de extracción en dispositivos móviles

Por otro lado, se encuentra el documento "Developing Process for Mobile Device Forensics" presentado en la SANS por la detective Cindy Murphy [14] que realmente es un poco más general y habla específicamente de la metodología. Sin embargo, la metodología general en dispositivos móviles no difiere mucho de la tecnología convencional, teniendo de esta forma la preservación, adquisición, análisis, documentación y presentación de la evidencia recopilada en móviles. Al

momento de seleccionar el método más adecuado, se tienen en cuenta muchos de aspectos como, por ejemplo: el nivel de exhaustividad requerido, la limitación de tiempo para realizar el proceso, qué tipo de información es necesario obtener: información volátil, información que ha sido previamente eliminada, información de aplicaciones de terceros, etc.

Para poder seleccionar la forma más adecuada se recomiendan algunas pautas, destacando diferentes aspectos necesarios como tener en cuenta si la depuración del USB está activa, si el dispositivo se encuentra bloqueado o tenemos acceso al mismo, entre otros.

Métodos para analizar dispositivos móviles:

- El teléfono está encendido.
- ¿Está la depuración del USB encendida?
    - No. ¿Está el arranque bloqueado?
        - Sí, sin posibilidad de desbloquearlo: Utilizar el método de adquisición física.
        - No: Activar depuración USB.

Sí, es necesario autorizar al PC: poner el dispositivo en modo avión y utilizar el método de adquisición lógica.

Pruebas y Resultados

Se hace uso de un celular Samsung J5 Prime sin permisos de root o bootloader. Haciendo uso de la herramienta Santoku que se ejecuta sobre una máquina virtual (figura 12) con el celular conectado y habilitado a depuración por usb se hace uso herramienta AF logical OSE disponible en el kit, el que desde la terminal permite recuperar llamadas, mensajes de texto, números de celular guardados. En caso de no reconocer el dispositivo se debe revisar que la depuración por usb está activa.

Fig. 11 Herramienta de extracción móvil Santoku

Para comenzar la extracción basta con usar el comando "`aflogical-ose -h`" en la terminal de la herramienta, esto tomará toda la información contenida en el dispositivo y creará automáticamente una carpeta en el escritorio de la máquina virtual que contiene toda la información extraída como se puede observar en la figura 13.

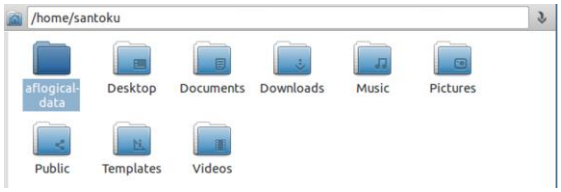

Fig. 12 Información extraída

Dentro de esta carpeta, en formato .csv, es posible encontrar toda la evidencia hallada desde la última vez que el dispositivo se apagó. Sin embargo, también es posible recuperar información anteriormente borrada. (fig.14)

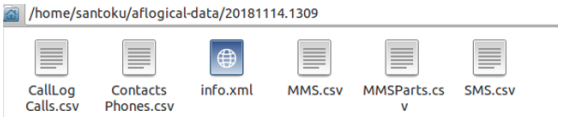

Fig. 13 Evidencia recopilada

En el archivo .csv se encuentra en orden descendente por fecha las ultimas llamadas realizadas, mensajes recibidos.

Por lo tanto, es posible recuperar no solo las llamadas realizadas con total registro de numero receptor, numero emisor y duración, sino también es posible recuperar los mensajes de texto con la información del mensaje en texto plano incluso aquellos que habían sido eliminados (como fue el caso de los mensajes publicitarios). Por otro lado, cabe resaltar que por ser un dispositivo que cuenta con el componente de memoria, es posible realizar las mismas actividades que en dispositivos convencionales, como lo son copia forense, volcado de memoria y recuperación de imágenes, incluso usando las mismas herramientas pues la operación es realizada sobre memorias de tipo flash.

V. CONCLUSIONES

Es evidente durante toda la investigación que, la mayor parte de la información que se considera vital frente a una investigación forense se encuentra en la memoria de los dispositivos, pues es allí donde se almacenan los registros de cada evento relacionado con el mismo. Sin importar el tipo de memoria analizado, se sabe que siempre habrá información que pueda constituir una prueba admisible ante un juez. Por lo que cabe destacar que a pesar de las facilidades que ofrecen las herramientas como apoyo a las técnicas de recopilación de evidencias, son muchas las recomendaciones a tener en cuenta al utilizarlas en los componentes de memoria. Sin embargo, la principal de todas es entender el sistema operativo al que se enfrenta y el tipo de información que intenta encontrar.

Teniendo esto en mente, se puede decir que Windows al ser el sistema operativo más comercial, permite tener mayor conocimiento del manejo de sus archivos y de las mejores herramientas para la recopilación de los mismos, lo que facilita la recolección de evidencia. Herramientas que además de ser de gran utilidad y confiabilidad, son ampliamente reconocidas

por el ámbito legal, lo que genera mayor fiabilidad a la evidencia recolectada.

Por otra parte, los sistemas operativos Linux por ser de baja demanda y conocimiento empresarial, son aprovechados ampliamente por los crackers, lo que por el hecho de ser de código abierto hace que las herramientas disponibles para la recopilación de evidencia sean de opciones más amplias. Sin embargo, también tiene desventajas para el perito pues al ser de código abierto, el sistema permite borrar completamente la información sin dejar rastro y esto muchas veces hace que legalmente las evidencias sean insuficientes o invalidas ante la corte. Por lo que en ese caso toda la investigación depende más de la pericia del perito para recopilar la evidencia, que de las herramientas que puedan servir de apoyo.

No obstante, para el caso de MacOs pasa todo lo contrario, pues al ser un sistema más cerrado al fabricante hace que las herramientas sean escasas y algunas veces de alto costo comercial, lo que conlleva una mayor dificultad al realizar la investigación y recopilación de evidencia.

Finalmente, para el caso de los dispositivos móviles, al ser un dispositivo cualquiera con componente de memoria es posible realizar la recopilación de evidencia, incluso aunque no se usen herramientas especializadas para dispositivos móviles, los cuales únicamente se usan para tareas concretas como la recuperación de llamadas, mensajes o información de GPS y bluetooth. Esto claramente representa una ventaja para el perito informático pues al usar las herramientas convencionales garantiza que la evidencia sea admisible ante la corte.

VI. Referencias

[1] -, «Arquitectura de computadores.,» -, - - -. [En línea]. Available: https://sites.google.com/site/arquitecturadecomputadoresis/. [Último acceso: - - 2018].

[2] «1,» 2010. [En línea]. Available: https://www.fing.edu.uy/inco/cursos/arqsis2/teorico/clase06-jerarquia.pdf.

[3] -, «atc uniovi,» -, - - -. [En línea]. Available: http://www.atc.uniovi.es/inf_med_gijon/3ingcomp/practicas/SMC/teor%C3%ADa-conceptos.htm. [Último acceso: - - 2018].

[4] R. Camacho, «Computo Integrado,» Blogger, 09 abril 2012. [En línea]. Available: http://rcmcomputointegrado.blogspot.com/2012/04/arquitectura-von-neumann.html. [Último acceso: 2018].

[5] -, «Tecnologia_facil,» -, 20 11 2017. [En línea]. Available: https://tecnologia-facil.com/que-es/la-memoria-rom/. [Último acceso: 2018].

[6] cienciaPlus, «europaPress,» -, 03 08 2017. [En línea]. Available: https://www.europapress.es/ciencia/laboratorio/noticia-cinta-magnetica-vuelve-competir-soporte-almacenar-datos-20170803125354.html. [Último acceso: - - 2018].

[7] MinTIC, «MinTIC,» 28 03 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf. [Último acceso: 2018].

[8] M. L. Delgado, «Analisis forense Digital,» -, 09 junio 2017. [En línea]. Available: https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf. [Último acceso: 2018].

[9] D. Garcia, «Biblioteca Vritual,» eumed.net, - - 2014. [En línea]. Available: http://www.eumed.net/libros-gratis/2010f/852/TECNICAS%20DE%20RECOLECCION%20DE%20INFORMACION.htm. [Último acceso: - - 2018].

[10] D. F. Pereira y J. D. Vico, «Guia de toma de evidencia en entornos windows,» -, - - -. [En línea]. Available: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe_toma_evidencias_analisis_forense.pdf. [Último acceso: - - 2018].

[11] C. Villamiza, A. Orjuela y M. Adarme, «ANÁLISIS FORENSE EN UN SISTEMA DE INFORMACIÓN EN EL,» -, 18 10 2014. [En línea]. Available: http://revistas.unisimon.edu.co/index.php/innovacioning/article/view/2036/1928. [Último acceso: 2018].

[12] E. Casey, «Digital Evidence on Windows Systems,» de *Digital Evidence and Computer Crime*, USA, ELSEVIER, 2011, p. 837.

[13] G. o. M. D. Forensics, «NIST,» -, - 05 2014. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf. [Último acceso: 2018].

[14] D. C. Murphy, «DEVELOPING PROCESS FOR THE EXTRACTION AND DOCUMENTATION OF CELL PHONE EVIDENCE,» -, - - 2016. [En línea]. Available: https://files.sans.org/summit/mobile12/PDFs/ExpertBriefingMobileForensicsStoriesfromtheField.pdf. [Último acceso: - - 2018].