Fases y metodología del análisis forense

PID_00273516

Josep Maria Arqués Soldevila
Miquel Colobran Huguet
Erik de Luis Gargallo

Tiempo mínimo de dedicación recomendado: 4 horas

Universitat Oberta de Catalunya

Josep Maria Arqués Soldevila

Ingeniero en informática por la Universitat Autònoma de Barcelona. Hizo el trabajo de investigación en el Departamento de Ingeniería de la Información y de las Comunicaciones (DEIC) de la mencionada universidad. Ha trabajado, como profesor ayudante y asociado, en el DEIC, y ha ejercido de profesor docente colaborador de varias asignaturas de la Universitat Oberta de Catalunya. Actualmente, ejerce de analista en informática forense y especialista en gestión de la calidad en ciencias forenses.

Miquel Colobran Huguet

Doctor en informática por la Universitat Autònoma de Barcelona. Es profesor docente colaborador en la UOC y coautor de varios materiales centrados en la administración y seguridad de sistemas e informática forense. Su investigación se enmarca dentro de la seguridad y del *social computing*, es decir, cómo los ordenadores influyen y son influidos por la sociedad, y cómo interviene la seguridad informática en este proceso.

Erik de Luis Gargallo

Ingeniero en informática y Máster en Seguridad de la Información por la Universitat Oberta de Catalunya. Tiene más de 10 años de experiencia en seguridad de la información, auditorías informáticas, informática forense e ingeniería de seguridad. Actualmente, trabaja estableciendo líneas estratégicas en el ámbito de la seguridad de las TIC y despliegue de las tecnologías que las aseguren. También es profesor colaborador de varios cursos y asignaturas de la Universitat Oberta de Catalunya.

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Jordi Serra (2020)

Primera edición: febrero 2020

Avda. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción..... 5

Objetivos..... 6

1. Informática forense y prueba digital..... 7
1.1. Etapas del análisis forense informático 8

2. Aseguramiento de la escena del suceso..... 11

3. Identificación de la evidencia digital..... 13

4. Recogida de la evidencia digital..... 16
4.1. Recogida de teléfonos móviles 19

5. Adquisición de la evidencia digital..... 21

6. Preservación de la evidencia digital..... 29
6.1. Verificación de la integridad mediante funciones *hash*..... 31
6.2. Digitalización de la cadena de custodia 33

7. Análisis de la prueba digital e investigación..... 35
7.1. *Write blockers*..... 37
7.2. Herramientas de análisis informático: Encase, Autopsy, distribuciones de Linux 39
7.3. Virtualización y análisis en vivo 39
7.4. Procedimiento general de análisis 40
7.5. Análisis e investigación 42
7.5.1. El marco legal 42
7.5.2. Análisis de correos electrónicos 43
7.5.3. Los ficheros de registro y la investigación de los delitos informáticos 44

8. Presentación e informe..... 46

9. El laboratorio de informática forense..... 47
9.1. Formación certificada de los analistas forenses 48

Resumen..... 50

Actividades..... 51

Ejercicios de autoevaluación..... 51

Solucionario..... 53

Glosario..... 54

Bibliografía..... 55

Introducción

La generalización del uso de las tecnologías de la información en la sociedad ha incrementado el valor de la información digital y ha creado, a su vez, la necesidad de protegerla ante los ataques malintencionados o atribuibles al desconocimiento de estas nuevas tecnologías. En los dos casos, los rastros o los indicios que podrían revelar la ejecución de un hecho (tanto si es constitutivo de delito como no) están almacenados en soportes digitales y se denominan genéricamente **pruebas digitales**.

Delito

Una conducta delictiva es la susceptible de ser sancionada por el derecho penal.

La prueba digital presenta, a grandes rasgos, las siguientes propiedades:

Pruebas digitales

En la comisión de una conducta delictiva, se denomina **prueba** a cualquier elemento que proporcione información que conduzca a alguna conclusión o algún hallazgo relacionado con el hecho que se investiga.

- Se puede modificar o eliminar fácilmente.
- Es posible obtener una copia exacta de un fichero sin dejar ningún rastro.
- La adquisición de la prueba puede comportar la alteración de los soportes digitales.

El **análisis forense** surgió de la necesidad de poder aportar elementos relevantes en los procesos judiciales en los que las nuevas tecnologías se encontraban presentes, o bien como objetivo (por ejemplo, una intrusión que comporte daños en un sistema informático) o bien como medio (por ejemplo, el envío de correos electrónicos amenazantes a un personaje público). En cualquier caso, la prueba digital es esencial para encontrar las respuestas a las preguntas habituales que se plantean en cualquier investigación:

Preguntas clave

- ¿**Qué** se ha cometido?
- ¿**Cuándo** se ha hecho?
- ¿**Dónde** se ha cometido?
- ¿**Quién** lo ha hecho?
- ¿**Cómo** se ha llevado a cabo?
- ¿**Por qué** se ha cometido?

Objetivos

Con el trabajo que se tiene que hacer sobre estos materiales didácticos, pretendemos que el estudiante logre los objetivos siguientes:

1. Conocer la definición de terminología forense básica.

2. Conocer el protocolo de metodología forense y los mecanismos de garantía de preservación de la evidencia digital.

3. Conocer las bases del análisis forense digital.

4. Conocer el *hardware* y *software* forense más empleado habitualmente.

5. Aprender a interpretar un informe pericial de análisis forense digital.

1. Informática forense y prueba digital

De una manera más precisa que el concepto expuesto en la introducción de estos materiales, el análisis forense se puede definir de la siguiente manera:

Definición de análisis forense informático

Se denomina **análisis forense informático** al proceso que resulta de aplicar métodos científicos a los sistemas informáticos y electrónicos con el fin de identificar, recoger, adquirir, analizar y presentar las evidencias digitales, de forma que estas sean aceptadas en un proceso judicial.

Hay muchas maneras de describir las diferentes subfases en las que se divide el análisis forense. Todas aluden al mismo procedimiento, aunque a veces se emplean nombres diferentes (lo cual puede llegar a ser bastante confuso).

Sin embargo, los analistas no siempre aportan pruebas en procesos judiciales. A menudo, sus informes se elaboran con finalidades privadas o empresariales. En este sentido, la definición de análisis forense que hemos proporcionado tiene un cierto tinte delictivo, lo cual no se ajusta, afortunadamente, en la mayoría de los casos, a la realidad que tenemos que estudiar. El análisis, de una manera más genérica, simplemente nos permite reconstruir lo que ha pasado en un sistema informático después de un incidente de seguridad. Por lo tanto, la finalidad del análisis puede ser simplemente de aprendizaje, una auditoría, la reconstrucción de un sistema dañado, o la adopción de medidas después del incidente que minimicen la probabilidad de que este vuelva a ocurrir. Sin embargo, consideramos que el caso judicial es el más restrictivo y el que exige más medidas de preservación, lo que puede ser muy didáctico y fácilmente extensible a todo tipo de análisis forense informático.

Siguiendo con el enfoque criminalístico, el informe del análisis forense, elaborado por un perito, podrá responder en algunos casos a las preguntas más directamente relacionadas con el ámbito técnico como por ejemplo: **qué** se ha cometido, en qué fechas y horas (**cuándo**), y **cómo** se ha llevado a cabo. Sin embargo, especialmente en las investigaciones de actividades delictivas, encontrar el resto de respuestas requerirá una investigación policial y los métodos que se le aplican. A pesar de esto, como ya se ha advertido, no todos los análisis tienen como destino la sede judicial. A menudo, el receptor será un cliente, normalmente una empresa. No obstante, en los dos casos, el analista

tiene que ser consciente de que el receptor del informe quizás no dispone de formación técnica suficiente y que, por lo tanto, conviene no abusar de los tecnicismos en la elaboración del informe que tiene que presentar.

1.1. Etapas del análisis forense informático

En general, las fases o etapas antes mencionadas, de que consta todo análisis forense informático, son las siguientes (se puede encontrar una descripción más esmerada de las etapas de identificación, recogida y adquisición en la norma ISO/IEC 27037):

- **Identificación**: esta etapa consiste en la búsqueda, el reconocimiento y la documentación de la evidencia digital en la escena del incidente. Este proceso tiene que permitir la identificación de los medios de almacenamiento que puedan contener evidencia digital potencial relevante relacionada con el incidente ocurrido. Esta etapa tendría que incluir un proceso de elección que permita priorizar la posterior recogida y/o adquisición de la evidencia en función de su volatilidad o relevancia.

- **Recogida**: una vez identificada la evidencia digital potencial, el especialista tendrá que decidir si recoge la evidencia o bien si la adquiere (véase la adquisición en el párrafo siguiente). Esta elección dependerá de varios factores como pueden ser: circunstancias, coste, tiempo y recursos disponibles. La recogida es la fase del procedimiento de gestión de la evidencia digital en la que los dispositivos que potencialmente pueden contener evidencia digital son recogidos y transportados a un laboratorio para una adquisición (esta operación también se puede hacer *in situ*) y un análisis posterior. La evidencia digital puede existir en dos condiciones: cuando el sistema se encuentra encendido o bien apagado.

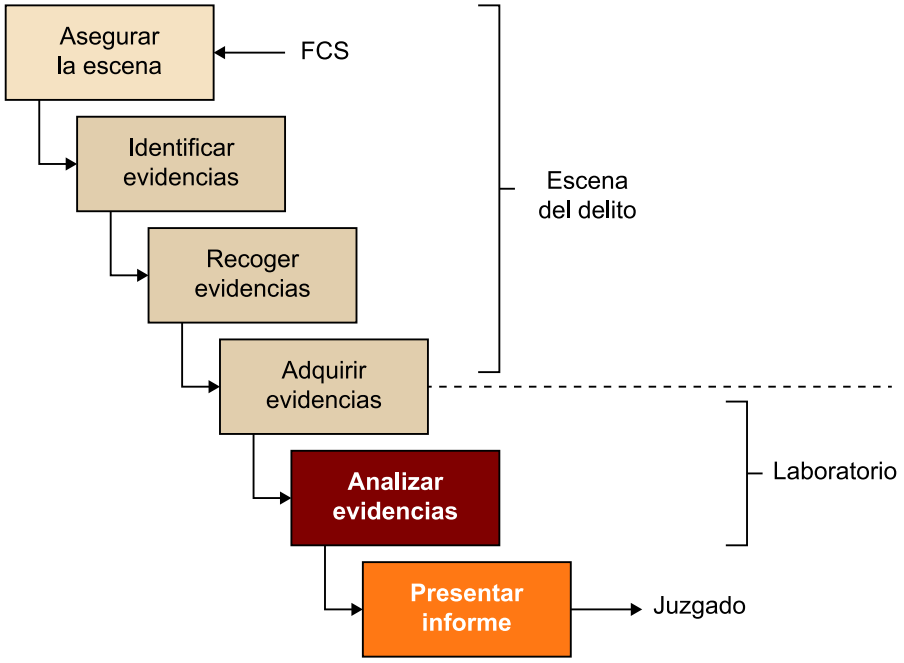
- **Adquisición**: el procedimiento de adquisición comporta la creación de una copia bit a bit de la evidencia contenida en los dispositivos digitales, así como la documentación de los métodos empleados y de los pasos realizados. Hay una gran variedad de métodos de adquisición y herramientas validadas (tanto de *hardware* como de *software*). El experto tiene que adoptar el mejor método de adquisición según la situación, el coste y tiempo disponible, así como documentar cualquier decisión que haya podido tomar.

- **Análisis**: en esta etapa, los peritos o analistas (*computer forensics analysts*) estudian las evidencias digitales obtenidas en la etapa anterior y elaboran sus hipótesis. Esta etapa requiere personal muy técnico, así como el uso de herramientas especializadas, como por ejemplo: Encase, Autopsy, etc. Esta etapa siempre se llevará a cabo en el laboratorio.

- **Presentación**: finalmente, como consecuencia de la etapa de análisis, se elaborará un informe pericial que puede tener varios destinatarios. En este

sentido, el informe se dirige a menudo a personas no técnicas en la materia (jueces, responsables de empresas, etc.). Por este motivo, es necesario que el informe contenga descripciones e indicaciones claras (por ejemplo, glosarios), así como las consecuencias y el desarrollo de los hechos sucedidos. Es muy importante que se tenga en cuenta que las evidencias digitales se tienen que haber adquirido al amparo de los requisitos legales para ser consideradas válidas en un procedimiento judicial.

Figura 1. Etapas del análisis forense informático



La figura 1 muestra las etapas antes mencionadas. El diagrama empieza, en este caso, por el aseguramiento de la escena del delito por parte de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y finaliza con la entrega del informe pericial en el juzgado. Como analistas y/o peritos, nuestras tareas se circunscribirán, casi con toda seguridad, a solo un subconjunto de las etapas que os mostramos, pero vale la pena tener en mente cómo sería el caso más complejo en el que podemos participar.

Hay que remarcar que, como ya se ha apuntado anteriormente, la adquisición se puede llevar a cabo (según circunstancias diversas), tanto en la escena del delito, como en el laboratorio de análisis. En todas estas etapas hay que tener muy presente la preservación de la integridad de las evidencias, tanto en lo concerniente a evitar la posibilidad que se puedan malograr accidentalmente (golpes, arcos magnéticos, etc.), como intencionadamente.

Hay multiplicidad de instituciones y manuales de buenas prácticas dedicados a la práctica forense en el ámbito digital. Nosotros destacamos el manual de buenas prácticas (de acceso público) elaborado por el ENFSI (European Network of Forensic Science Institute). Esta institución nació oficialmente en 1995 (aunque su primer congreso se remonta a 1993) y, entre otros objetivos, pro-

cura que todos los países miembros cumplan los estándares de calidad y sigan las recomendaciones de los manuales de buenas prácticas. ENFSI dispone de muchos grupos de trabajo según el ámbito forense (ADN, explosivos, drogas, imagen digital, tecnología digital, huellas, etc.). Además de promover el intercambio de información entre los miembros, ENFSI realiza congresos, muchos de carácter anual (ordinarios y según la especialidad), a los que asiste el personal de los laboratorios de los países miembros. España dispone de representantes en ENFSI de varios cuerpos policiales (Policía Nacional, Guardia Civil, Mossos d'Esquadra y Ertzaintza), como también del Instituto Nacional de Toxicología y Ciencias Forenses (órgano adscrito al Ministerio de Justicia).

2. Aseguramiento de la escena del suceso

Esta fase siempre es preceptiva en el curso de una actuación policial, aunque no siempre aparecerá en los casos reales de análisis. Sin embargo, a pesar de que difícilmente nos encontraremos con estos tipos de casos, las recomendaciones sobre medidas de protección del sistema y definición del marco de trabajo tienen un interés general y nos pueden ser de utilidad para cualquier caso. Con demasiada frecuencia, los analistas se circunscriben a los detalles técnicos del caso, eludiendo otras cuestiones, como la protección del sistema una vez acontecido el suceso, lo que podría llegar a invalidar la prueba digital ante un tribunal.

La finalidad de esta etapa consiste, básicamente, en asegurar la escena del suceso, y restringir el acceso a esta para que nadie la pueda alterar. Además, en esta fase, los actuantes también deben garantizar que nadie haga nada sin estar seguro de las consecuencias. El protocolo propuesto consta de los siguientes apartados:

- Identificar la escena donde se ha producido el hecho que hay que investigar y establecer un perímetro de seguridad.

- Restringir el acceso de personas y equipos informáticos en el interior del perímetro trazado.

- No permitir el uso de ningún dispositivo con tecnología inalámbrica por ninguna de las personas presentes.

- Preservar las huellas digitales mediante el uso de guantes de látex.

- En este momento, se tiene que valorar la posibilidad de desconectar las conexiones de red del sistema (dispositivos inalámbricos, cables de red, etc.). La desconexión podría evitar que un determinado delito o suceso se continúe produciendo (por ejemplo, podría evitar la eliminación remota de las pruebas digitales), pero también hay que valorar la utilización de la red para monitorizar las conexiones e investigar el origen del suceso (aunque hay que tener en cuenta que estas operaciones sobre el equipo que hay que investigar podrían implicar la pérdida de la validez de la prueba ante un juez).

- Si se encuentran impresoras en funcionamiento, permitir que acaben la impresión.

- Anotar la fecha y la hora del sistema[1] (marca horaria o *timestamp*) antes de apagarlo (siempre que aparezcan en el monitor, sin tener que manipular el sistema), y documentar estos valores e incluso fotografiarlos o grabarlos en vídeo.

(1)La fecha y la hora del sistema no tiene que coincidir necesariamente con la real. Este desfase puede ser crucial para el analista y tiene que ser documentado en este instante.

- Igualmente, en caso de que en el monitor aparezcan procesos relevantes (por ejemplo, los archivos que se están compartiendo en una aplicación de igual a igual o P2P), es importante fotografiar o grabar en vídeo esta información. En general, hay que documentar cualquier salida del sistema que se considere de interés.

- Apagar[2] los dispositivos encendidos tirando del cable de la corriente de la parte posterior del equipo[3] (especialmente, en los casos en que se detecte destrucción de información). En caso de quitar el cable directamente del enchufe, hay que tener presente que el sistema podría disponer de algún mecanismo de protección en caso de caída del fluido eléctrico, y se podrían escribir datos en el disco duro del equipo. Así mismo, el apagado «normal» del ordenador también podría ocasionar pérdidas graves de información si el apagado activa algún proceso de eliminación de pruebas (por ejemplo, un *hacker* malicioso podría disponer de medidas de protección de este tipo). En general, no hay un procedimiento ideal para resolver la cuestión de apagar los dispositivos y, en cada caso, el experto tendrá que valorar qué método se ha de utilizar en función del resultado que se persigue, el equipo que se debe analizar y el nivel de conocimientos que se supone al usuario del equipo.

(2)No siempre es posible parar el servicio: imaginemos, por ejemplo, el caso de una fábrica o de una empresa proveedora de servicios de Internet, un hospital, etc.

(3)En el caso de ordenadores portátiles apagados, hay que extraerles la batería.

A veces, el aseguramiento de la escena se produce durante la entrada y el registro en el lugar del suceso con la ayuda de los miembros de las FCSE. En este caso, la entrada será con la presencia del secretario judicial y lo que acontezca quedará registrado en acta. Por lo tanto, el secretario judicial registrará en acta las comprobaciones como, por ejemplo, la hora y la fecha que puedan aparecer en los monitores de los ordenadores, y no habrá que documentar la comprobación mediante fotografías o grabaciones. Así mismo, a pesar de la presencia del secretario judicial, a veces puede ser pertinente aportar fotografías de la escena o de la información que se muestra en los monitores. Por ejemplo, continuando con el caso ya descrito de las descargas de contenido ilícito mediante aplicaciones de igual a igual (*peer-to-peer*), podría resultar de interés hacer una captura del contenido de la pantalla, aunque esto implicara la alteración del sistema objeto de análisis. En todo caso, el secretario judicial tendrá que dar cuenta en acta de todo lo que ha acontecido durante la entrada, especialmente de las acciones que hayan podido alterar la prueba digital.

3. Identificación de la evidencia digital

Se denomina así el proceso de identificación y localización de las pruebas que es necesario recoger para analizar posteriormente. Este proceso no es trivial porque, a menudo, el analista se encontrará en disposición de empaquetar una cantidad ingente de material heterogéneo: una red entera de ordenadores, miles de DVD, datos en la nube, dispositivos inalámbricos escondidos, teléfonos móviles, etc. Por lo tanto, el analista debe encontrar una solución de compromiso entre la calidad, la validez de la prueba y el tiempo que ha invertido en ella.

Como ya hemos mencionado en apartados anteriores, se puede encontrar más información sobre la identificación, recogida, adquisición y preservación de la evidencia digital en la norma ISO/IEC 27037.

En primer lugar, el analista debe identificar el sistema informático o dispositivo que se debe analizar con el fin de saber dónde se almacenan las pruebas digitales que pueden resultar útiles para la investigación. Así mismo, también debe diferenciar entre las **pruebas volátiles** (memoria RAM, por ejemplo) y las que no lo son.

Pruebas volátiles

Esencialmente, las que desaparecen en ausencia de alimentación eléctrica.

El segundo paso consiste en valorar la necesidad de obtener las pruebas volátiles. Si es el caso, hay que grabarlas como un fichero en un dispositivo de almacenamiento externo al dispositivo que se debe analizar, de forma que en este momento se convierten en pruebas no volátiles (lo cual implica la obligatoriedad de acceder al sistema). Cualquier técnica que implique la manipulación del sistema original puede significar la invalidación de la prueba en un procedimiento judicial (por ejemplo, basta con abrir un archivo para modificar la fecha del último acceso). En caso de que sea imprescindible acceder a un disco duro original, hay soluciones de *hardware* y de *software* (profundizaremos en ello en próximos apartados) para hacerlo evitando la escritura en el disco duro. Finalmente, se debe tener en cuenta que, a veces, los sistemas informáticos susceptibles de ser analizados no se pueden interrumpir (por ejemplo, parar un sistema informático podría implicar el cese de la actividad de una fábrica), de forma que los datos hay que obtenerlos al instante, por ejemplo, solicitándolos al administrador del sistema.

En todo caso, las manipulaciones que se puedan hacer del sistema informático original deberán quedar claramente documentadas. A menudo, estas manipulaciones quedan recogidas por los secretarios judiciales (por ejemplo, en diligencias de entradas y registros en presencia de las FCSE) o por los notarios. En caso de que no dispongamos de ninguna de estas figuras, lo podremos hacer nosotros mismos, extendiendo un acta de las acciones que realizamos sobre el sistema informático.

Obtención de pruebas

Otras veces, las pruebas de interés se obtendrán, por ejemplo, al monitorizar una red, lo que puede significar, de nuevo, la invalidación de la prueba ante un tribunal. Como ya se ha mencionado, en caso de disponer de secretario judicial, será imprescindible documentar en acta todas las manipulaciones que se hayan llevado a cabo para llegar a obtener la prueba.

En general, el analista debe tener en cuenta que las pruebas no solamente se pueden localizar en los discos duros, y que actualmente prácticamente cualquier dispositivo electrónico (por ejemplo, un teléfono móvil, un GPS, etc.) es susceptible de almacenar información relevante.

Ejemplos de dispositivos electrónicos que pueden almacenar información relevante (o ser necesarios para poder llevar a cabo el análisis):

- Ordenadores y periféricos conectados a los ordenadores.
- Discos duros (no solo los internos, sino también los externos, NAS, etc.).
- CD o DVD.
- Dispositivos en desuso, como unidades ZIP o JAZ, disquetes de 5 1/4", etc.
- Componentes de red como, por ejemplo, un rúter o un *switch*.
- Puntos de acceso de las redes inalámbricas.
- Dispositivos móviles (teléfonos, PDA, etc.) y los elementos que contienen, como por ejemplo tarjetas SIM o de memoria.
- USB (notemos que los USB pueden tener aspectos inesperados, como figuras o juguetes) y tarjetas de memoria.
- Impresoras, escáneres y fotocopiadoras.
- Lectores/grabadores de tarjetas de banda magnética (las tarjetas en sí mismas también son elementos relevantes), buscapersonas, etc.
- Mochilas (*dongles*). Estos elementos pueden ser imprescindibles para, por ejemplo, poder ejecutar un determinado *software* en el laboratorio.
- Dispositivos para hacer copias de seguridad o *backups*.
- Dispositivos GPS.
- Sistemas de videovigilancia (normalmente, disponen de formatos de sistema de ficheros propios, lo que dificulta o imposibilita el análisis).
- Cámaras fotográficas y de vídeo digitales.
- Manuales, notas, papel impreso, etc.

Ejemplos de pruebas volátiles

Son pruebas volátiles las siguientes:

- Memoria RAM
- Ficheros temporales del sistema
- Estado de la red
- Ficheros abiertos
- Conexiones de red en uso
- Procesos en ejecución, etc.

La elección de los elementos o dispositivos que se deberán recoger para su análisis posterior dependerá en gran medida del objetivo del análisis. Por ejemplo, es posible que necesitemos coger una impresora de la escena del suceso para poder hacer pruebas posteriores (de conexión con un ordenador que se está analizando, para poder comparar una impresión encontrada con las impresiones que produce una cierta impresora, etc.). Además de discriminar los

elementos que serán analizados, hay que documentar aspectos generales del sistema, incluso de aquellos dispositivos que no se deban transportar al laboratorio, así como tener en cuenta las siguientes recomendaciones:

- Hacer una lista con los sistemas (y su descripción) involucrados en el suceso.

- En cuanto a las personas implicadas, solicitar los datos que se consideren relevantes como, por ejemplo: nombre, DNI, contraseñas del sistema y de usuarios, acciones que se hayan llevado a cabo desde el conocimiento del incidente, etc.

- Fotografiar y/o grabar en vídeo la escena del suceso[4]. A menudo, también es deseable representar esquemáticamente el sistema que se debe estudiar (por ejemplo, dibujar la topografía de una red, identificando cada uno de los ordenadores que la constituyen).

- Etiquetar los cables y los componentes. Muchos dispositivos, como los periféricos lectores/grabadores de tarjetas magnéticas, pueden necesitar un cableado específico sin el que el dispositivo no podrá funcionar y no se podrá analizar posteriormente en el laboratorio. Por lo tanto, además de los dispositivos que se analizarán, también debemos empaquetar todos los elementos y el cableado que, posteriormente, nos permitirán utilizar los dispositivos en el laboratorio, tanto para conectarlos a un sistema informático como para proveerlos de electricidad. Los cables deben ser etiquetados, de forma que se pueda identificar inequívocamente el puerto del sistema informático en el que estaban conectados.

- No encender ningún ordenador que esté apagado.

- Aparte, hay que mencionar los discos duros, en la mayoría de los casos objetos principales de análisis (el perito debe considerar la posibilidad de extraerlos para su posterior análisis; a menudo no es necesario el ordenador, sino solo la información contenida en el disco duro). En estas circunstancias, se deben documentar todos los elementos identificativos del disco duro (marca, modelo, número de serie, capacidad, etc.). Así mismo, debemos extraer de las ranuras de las unidades lectoras de CD, DVD o cualquier otro dispositivo, los soportes digitales que puedan contener, identificarlos y documentarlos adecuadamente.

- Fotografiar y grabar en vídeo los dispositivos con las etiquetas colocadas. Estas etiquetas también se pueden anotar en los esquemas creados en el tercer punto de esta lista de recomendaciones.

(4)Estos esquemas o estas anotaciones pueden ser de mucha utilidad en la fase de análisis.

4. Recogida de la evidencia digital

La fase de recogida implica la recogida de los dispositivos físicos (de su localización original) que pueden contener evidencia digital, y documentar todos los dispositivos recogidos y los pasos realizados.

A la hora de efectuar la recogida hay que evitar alterar, estropear o destruir la evidencia digital. Así pues, hay que evitar utilizar herramientas u objetos que provoquen electricidad estática o campos magnéticos, para mantener intactas las evidencias digitales (con esta finalidad se pueden utilizar, por ejemplo, bolsas y brazaletes antiestáticos para el personal actuante).

Notemos que habrá casos en los que no se podrá efectuar la recogida de los ordenadores o dispositivos diversos. Por ejemplo, no nos podremos llevar una red compleja al laboratorio (a pesar de que siempre tenemos la posibilidad de obtener las evidencias deseadas con la ayuda del administrador del sistema). Por lo tanto, las indicaciones que mostramos en este apartado se refieren más bien a los casos en que los ordenadores son dispositivos aislados (en caso de encontrarnos una red de ordenadores, el procedimiento puede ser bastante más complejo, pero en cualquier caso deberemos tener en cuenta las consideraciones que a continuación se exponen).

Por lo tanto, antes de proceder a la recogida del material se debe tener en cuenta:

1) Si el ordenador está encendido: en general, la forma más segura (a pesar de que normalmente no es esta la que elegiremos) de actuar ante un ordenador en funcionamiento, es **estirar el cable de la corriente**. Sin embargo, si la evidencia que estamos buscando está, por ejemplo, muy visible en la pantalla, o sospechamos que puede estar almacenada en la memoria RAM, entonces, en primer lugar, deberemos capturar y preservar la información volátil.

En las siguientes situaciones **es recomendable** estirar el cable de la corriente:

- Cuando hay sospechas o hay actividad en la pantalla que indica que la información se está borrando o sobrescribiendo.

- Cuando hay algún proceso que indica que se está destruyendo algún dispositivo de almacenamiento, como por ejemplo, el formato de un disco duro, la creación de nuevas particiones o un proceso de borrado seguro (*wipe*) en funcionamiento.

- Hay que valorar casos especiales en los que la acción de pulsar el botón *power* de un dispositivo digital pueda estar configurada para iniciar un *script* que modifique o borre la información de un sistema antes de apagarlo.

En las siguientes situaciones **no es recomendable** estirar el cable de la corriente:

- Cuando en la pantalla se muestra información claramente relacionada con el objeto de nuestra investigación.

- Cuando hay indicios de que hay alguno de los programas siguientes en uso:
  - Clientes de mensajería instantánea.
  - Documentos abiertos en pantalla.
  - Almacenamiento de datos remoto.
  - Programas de intercambio de ficheros con contenidos ilícitos.
  - Cifrado de datos (en este caso, se puede valorar la posibilidad de efectuar una adquisición lógica de la información antes de apagar el ordenador).

En definitiva, cuando el ordenador está encendido, antes de realizar la recogida, habrá que valorar si primero debemos capturar o documentar (por ejemplo, con una cámara fotográfica o de vídeo) aquella información que puede desaparecer al apagar la máquina. De hecho, el contenido de la memoria RAM puede ser capital en ciertos análisis, puesto que allí podemos encontrar información muy importante, como por ejemplo contraseñas de cifrado, lista de los procesos en ejecución, puertos abiertos, etc.

En caso de que la decisión tomada sea la de desconectar el ordenador de la electricidad, entonces hay que hacerlo estirando el cable del extremo de la máquina (no del enchufe). De este modo se evitará que si el dispositivo se encuentra conectado a un SAI (Sistema de Alimentación Ininterrumpida) se escriban datos en el disco duro y se pueda modificar la evidencia digital.

Sin embargo, hay que tener en cuenta que en la gran mayoría de casos no esperamos tener ni procesos de cifrado, ni *hackers* preparados para borrar la información. Por lo tanto, con un apagado normal del ordenador puede ser suficiente.

2) Si el ordenador está apagado: si tenemos dificultades para determinar si el ordenador se encuentra apagado o en funcionamiento, podemos poner en marcha el monitor (en caso de que no lo esté), y mover el ratón sin pulsar ningún botón. Si se produce algún indicio de actividad, procederemos según el apartado anterior. Si efectivamente comprobamos que está apagado, seguiremos las siguientes indicaciones:

- Si no lo hemos hecho todavía, hay que documentar y fotografiar el equipo, todas sus conexiones y los periféricos conectados. Es posible que en el laboratorio necesitemos reconstruir el sistema que se debe analizar.

- Desconectar el cable de la corriente desde la parte posterior del ordenador. Si se trata de un portátil, también hay que extraer la batería. Algunos portátiles se ponen en marcha al abrir la tapa. La extracción de la batería evita poner en funcionamiento el dispositivo de manera accidental.

- Desconectar el resto de conexiones indicándolas en la documentación.

- Si no lo hemos hecho todavía, documentar el modelo y el número de serie del ordenador.

- Precintar el ordenador, por ejemplo, depositándolo en el interior de una bolsa cerrada con una brida. Si utilizamos etiquetas adhesivas para precintar, deberemos tener en cuenta que los puertos que permiten la conexión del ordenador tienen que permanecer tapados e inaccesibles para evitar la modificación de las posibles evidencias. Igualmente, las etiquetas adhesivas deben evitar que se pueda extraer el disco duro o manipular el interior del ordenador o dispositivo. En el caso de utilizar bolsas precintadas, es importante colocar dentro de la bolsa todos aquellos cables, cargadores de electricidad o elementos varios (*dongles*, etc.) que originalmente estaban con el dispositivo en la escena del incidente.

En caso de que las condiciones lo permitan, y si es necesario, se puede considerar la posibilidad de extraer el disco duro (o discos duros) que pueda alojar el ordenador o dispositivo. En este caso, hay que tener presente que la extracción del disco duro facilita que se pueda estropear en caso de no estar suficientemente protegido. Para evitar este problema, el analista o perito que lo manipule puede emplear brazaletes antiestáticos y bolsas antiestáticas para el disco duro extraído.

Una vez recogidos los ordenadores o dispositivos, habrá que empaquetarlos para transportarlos al laboratorio de análisis. A la hora de empaquetar, precintar, transportar o almacenar las evidencias digitales hay que tener en cuenta que son frágiles y sensibles a temperaturas extremas, humedades, golpes, electricidad estática y campos magnéticos. Por este motivo, se deberán tomar precauciones para preservarlas.

Finalmente, en la fase de recogida también hay que tener en cuenta otros elementos de tamaño más pequeño, como por ejemplo un DVD, USB, o incluso las evidencias que podamos haber extraído de un sistema informático en funcionamiento, convenientemente identificadas y grabadas en medios como por ejemplo un DVD, que se tendrán que identificar, empaquetar y transportar

con las mismas precauciones. Si es necesario, el secretario judicial (o el notario), identificarán unívocamente en su acta los medios en los que habremos extraído las evidencias que habremos considerado relevantes.

Hay que tener presente que, según el dispositivo que se deba recoger, la metodología empleada puede contener matices diferenciadores, en relación con la vista, muy importantes. A continuación, veremos algunas recomendaciones importantes para el caso de los teléfonos móviles.

4.1. Recogida de teléfonos móviles

En los últimos años, el número de teléfonos móviles ha registrado un incremento espectacular hasta llegar a superar los seis mil millones de dispositivos en 2019, es decir, alrededor de un 70 % de la población mundial. Este hecho ha favorecido un interés creciente en la ciencia forense digital de telefonía móvil en detrimento de otras disciplinas forenses digitales como por ejemplo el análisis forense de ordenadores o el de las redes de comunicaciones. Actualmente, se estima que más del 75 % de los teléfonos móviles activos son inteligentes. Estos dispositivos, realmente son miniordenadores que pueden enviar y recibir llamadas, y que nos proporcionan una gran cantidad de información que podría resultar de interés desde un punto de vista forense.

A diferencia de los ordenadores, vistos en el apartado anterior, en el caso de los teléfonos móviles, la propia operativa de funcionamiento de estos dispositivos puede comprometer la integridad de los datos que contienen. Así pues, antes de trasladar el móvil, en muchas ocasiones, habrá que aislar el terminal para evitar que nuevas señales entrantes, como por ejemplo, SMS, puedan sobrescribir datos ya existentes en el móvil y, por lo tanto, se estropee la integridad de la evidencia (no solo pueden desaparecer datos, sino que la evidencia se altera, puesto que no es exactamente la misma que cuando se comisó el terminal). Además, si no se aísla, se podrían aprovechar remotamente vulnerabilidades para destruir evidencias.

Antes de llevarnos un móvil, pues, hay que valorar si es necesario aislar el terminal y, si lo es, efectuar las operaciones que sean necesarias para, efectivamente, aislarlo del exterior. Para conseguirlo, podemos elegir diferentes metodologías:

- **Poner el terminal en modo avión**: esta acción requiere interactuar con el terminal empleando el teclado, lo que implica asumir ciertos riesgos, especialmente si el perito o analista que lo manipula desconoce la marca o el modelo. Mientras el móvil está en modo avión no se podrá mantener ninguna conexión inalámbrica. Sin embargo, en este modo de operación también se puede emplear una red wifi o Bluetooth, de forma que la conectividad no se pierde del todo.

- **Apagar el terminal**: si lo apagamos, para encenderlo de nuevo podemos necesitar conocer varios códigos (PIN/PUK, patrón de desbloqueo, medidas biométricas), lo cual complicará la adquisición y retrasará el análisis).

- **Mantener el móvil en marcha, pero aislado (por ejemplo en una bolsa de Faraday)**: esta opción acorta la carga de la batería debido al incremento del consumo de energía que se produce cuando el dispositivo no se puede conectar a la red y aumenta la fuerza de la señal al máximo. Por otro lado, después de un periodo en el que el terminal no se ha podido conectar, algunos modelos pueden borrar datos de la red que podrían ser de interés para la investigación. Finalmente, es difícil garantizar que las bolsas de Faraday aíslen completamente el terminal, puesto que pueden estar mal cerradas, o incluso los cables conectados a la estación de trabajo podrían actuar de antenas.

Si, por el contrario, decidimos apagar el móvil, habrá que tener en cuenta que si no conocemos el PIN/PUK o el patrón del dispositivo, el análisis en el laboratorio se complicará mucho (o incluso no se podrá llevar a cabo).

Una vez determinada y realizada la operación que el perito o analista haya considerado, el terminal se deberá depositar en un contenedor adecuado y trasladarlo al laboratorio de análisis.

Cuando lleguemos al laboratorio, si el móvil lo hemos dejado en funcionamiento, tanto si se encuentra o no dentro de una bolsa de Faraday, hay que tener presente que habrá que mantener la carga de la batería para evitar que se pueda apagar, porque dificultará o incluso imposibilitará el análisis posterior.

5. Adquisición de la evidencia digital

La facilidad con la que las pruebas digitales se pueden modificar[5] e, incluso eliminar, determina un procedimiento esmerado de preservación de la prueba según las leyes vigentes y las soluciones tecnológicas del momento. Este apartado es uno de los más críticos de toda la secuencia, puesto que un error en este punto podría llegar a invalidar una prueba en el tribunal.

(5)Analizar u observar un componente del sistema alterará otros componentes.

No es posible obtener una imagen congelada de un sistema en un instante concreto (es decir, capturar la totalidad del sistema), si bien a menudo los datos más relevantes para la investigación se encuentran, simplemente, en el sistema de ficheros del equipo que se ha intervenido, con lo que la pérdida inevitable de una parte mínima de la información (debida a la imposibilidad mencionada) es un mal menor. Por otro lado, en caso de que no sea posible evitar la alteración del sistema (es decir, se deba hacer un análisis en vivo del sistema), habrá que documentar las acciones realizadas mediante actas, fotografías o grabaciones de vídeo. Afortunadamente para nosotros, a menudo no hay que actuar con presteza; tampoco se requieren medidas excepcionales para proteger el acceso al sistema, ni se necesita la obtención de las pruebas volátiles, puesto que con los datos del sistema de archivos es suficiente para desarrollar el análisis. En definitiva, en muchos casos el analista podrá dedicar el tiempo, con tranquilidad, a la tarea de duplicar la información que contienen los soportes (como por ejemplo discos duros) objeto de estudio. Esta duplicación o clonación se podrá llevar a cabo, según el caso, en el lugar del incidente, o posteriormente en el laboratorio (si, por ejemplo, podemos extraer los discos duros y transportarlos con garantía al laboratorio).

El procedimiento que se tiene que observar para adquirir la evidencia digital consta de los siguientes pasos:

1) Copia de bits de los soportes originales. Cualquier prueba digital identificada como relevante para la investigación se deberá copiar mediante *software* o *hardware*[6] que no altere la integridad y que permita su admisión en un tribunal de justicia. La copia o **clon** se tiene que hacer en el ámbito de los bits, es decir, su contenido tiene que ser exactamente el mismo que el del dispositivo original, incluyendo los ficheros ocultos, temporales, eliminados todavía no sobrescritos e, incluso, tiene que incluir el denominado ***file slack*** (se denomina así el espacio entre el final lógico de un fichero y el final físico), como también la información que contiene el espacio no asignado del disco duro (en definitiva, el clon tiene que ser una copia exacta del original).

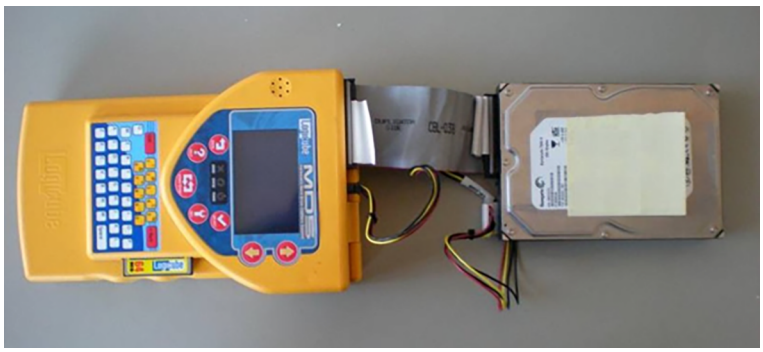
(6)Posteriormente, se incidirá en las herramientas de *software* o *hardware* que se pueden utilizar para crear una copia de bits.

Análisis de dispositivos

Hay procedimientos que permiten el examen de los soportes originales sin alterar su contenido. De todos modos, siempre que sea posible es preferible trabajar con un clon.

El proceso de clonación tendrá lugar sobre un dispositivo normalmente aportado por el grupo actuante: disco duro, CD-ROM, DVD, etc. La elección de uno u otro medio dependerá de la cantidad de información contenida en los soportes originales (normalmente se emplean discos duros). El uso de CD-ROM o DVD presenta la ventaja adicional que la información que contienen no se puede modificar y, por lo tanto, con su uso se garantiza la integridad de la prueba. En cuanto al **clon** o la **copia**, se pueden emplear métodos de *hardware* o de *software* (LinEn, Acronis True Image, distribuciones forenses de Linux, etc.). En la figura 2, podemos apreciar un duplicador de *hardware*.

Figura 2. Duplicador o clonador de discos duros (de Logicube)



Nota

Evidentemente, la capacidad del disco duro de destino tiene que ser mayor o igual que la del disco duro original.

Este tipo de dispositivo nos permite generar un clon de un disco duro sobre otro aportado por los actuantes. El original se coloca en el exterior del duplicador, y el receptor (del que se habrá eliminado previamente cualquier rastro de información que pudiera contener mediante técnicas de borrado seguro) en el interior. Por supuesto, tenemos que extremar la precaución en el momento de efectuar la conexión de los discos duros, puesto que el intercambio del disco de origen por el de destino provocaría la pérdida irrecuperable de la información original. La duplicación se efectuará de manera automática y transparente en el operador. Además, incluso es posible llevar a cabo la búsqueda automatizada de cadenas de caracteres (por ejemplo, la cadena literal «bomba») al mismo tiempo que se hace el duplicado.

Borrado seguro

Hay diferentes herramientas, tanto de *software* como de *hardware* (por ejemplo, los mismos clonadores suelen disponer de estas funciones), para llevar a cabo el borrado seguro de información (*wipe*). Se basan en la escritura de un determinado carácter (efectuando varias pasadas) en todos los sectores de un disco duro.

Los dispositivos duplicadores también pueden generar **archivos de imágenes (imágenes forenses)**, normalmente de tamaño más pequeño que el soporte original, que también contienen toda la información del original y permiten el análisis mediante el uso de herramientas de *software* especializadas, como Encase o Autopsy.

No solamente los discos duros son susceptibles de ser duplicados, también lo es, por ejemplo, la información que contienen los terminales de telefonía móvil[7]. Así, tanto las tarjetas que alojan como los datos de la memoria se pueden duplicar y almacenar, por ejemplo, en otra tarjeta de memoria aportada por el analista forense (o descargar directamente sobre el disco duro de análisis). En la figura 4, podemos ver un dispositivo utilizado para extraer la información que contiene un teléfono móvil. Este tipo de dispositivo necesita una gran diversidad de cables para garantizar la conexión con el máximo número posible de móviles. Naturalmente, la colección de cables se tiene que ampliar frecuentemente para poder acceder a los nuevos terminales de telefonía que vayan surgiendo en el mercado, y su coste económico de mantenimiento es muy elevado[8]. Las soluciones actuales suelen consistir en una combinación entre *hardware* y *software*.

(7)Aparte de los discos duros, hay otros muchos dispositivos electrónicos que pueden alojar evidencias digitales, como por ejemplo teléfonos móviles, GPS, dispositivos lectores/grabadores de tarjetas de banda magnética, etc.

(8)Hay que recordar que cada fabricante puede emplear un tipo de cableado diferente y, además, los diferentes modelos de cada fabricante suelen disponer de su propio cableado específico. Afortunadamente, actualmente los tipos de cableado son más estándares y principalmente solo se usan 2 o 3.

Evidencia digital en la telefonía móvil

Algunas pruebas que se pueden localizar en un teléfono móvil:

- SIM (*subscriber identity module*)
- Número IMEI (*international mobile equipment identity*)
- Agenda telefónica
- Fotografías y audio
- Configuración (fecha/hora, lenguaje, etc.)
- Ejecutables almacenados, etc.

Figura 3. Maleta de cableado del dispositivo de la figura 4 (de Cellebrite)

Figura 4. Extracción de información de un móvil a un dispositivo USB (de Cellebrite)

Además de estas soluciones generalistas, la mayoría de móviles disponen de sus propias aplicaciones para descargar contenidos y hacer copias de seguridad para uso de los usuarios. Estos programas se pueden encontrar en las páginas web de los fabricantes, aunque no suelen ofrecer muchas prestaciones como herramientas forenses.

Por supuesto, hay otros muchos dispositivos tecnológicos susceptibles de almacenar información en su interior. Por ejemplo, un dispositivo lector de tarjetas de banda magnética. En este caso, al no haber un dispositivo específico de duplicación, una estrategia posible para seguir consiste en extraer la memoria del lector, descargarla e interpretar el resultado obtenido. Esta operación puede revestir una gran complejidad, puesto que la memoria puede estar protegida por una contraseña, e incluso el contenido puede estar cifrado mediante algún algoritmo.

Finalmente, hay que señalar que una de las diferencias más importantes entre las diferentes prácticas forenses es que, en el ámbito de las ciencias forenses habituales (ADN, drogas, explosivos, etc.), la prueba, aunque a veces es divisible, no se puede duplicar, mientras que en el ámbito de la tecnología digital sí que se puede duplicar, lo cual es sin duda ventajoso, aunque esto pueda implicar problemas de verificación y preservación de la integridad de la prueba.

2) Verificación de la integridad de la copia o imagen. Una vez generada la copia o el clon del soporte original, el programa o el dispositivo de *hardware* empleado en este proceso hace el cálculo del valor ***hash*** del soporte original y del destino, con el fin de garantizar que los dos son idénticos y que la copia se ha producido sin ningún error (los dos valores deben ser coincidentes). Este cálculo se hace sobre todo el conjunto de ficheros del soporte clonado.

Funciones *hash*

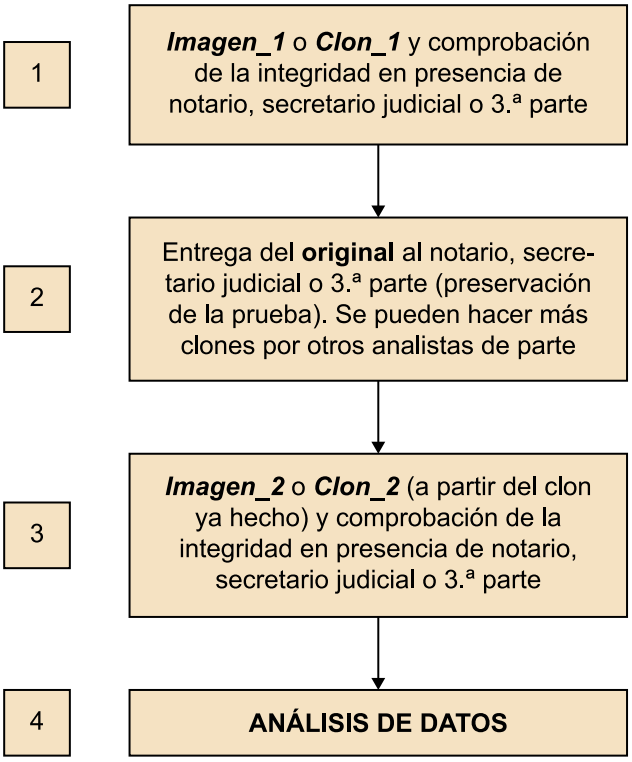
Para más información sobre las funciones *hash* se puede consultar el apartado de preservación de las evidencias digitales.

Función *hash*

Función matemática unidireccional que resume un mensaje de tamaño variable (por ejemplo, un archivo) en una representación de tamaño fijo. Es poco probable que dos ficheros diferentes tengan la misma representación *hash*, lo cual significa que este valor se puede utilizar para comprobar la integridad de un archivo (o de un sistema). Las funciones *hash* más conocidas son MD5 y SHA-1.

La figura 5 muestra el protocolo de actuación que debe seguir el analista para adquirir los datos preservando la integridad de la prueba. En este caso suponemos que se ha podido extraer el disco duro del dispositivo. Si no se hubiera podido extraer, en primer lugar se habrían tenido que obtener las evidencias (vaciado de memoria RAM, ficheros de registro, etc.) y después tratarlas siguiendo el protocolo que se expone en la figura 5:

Figura 5. Protocolo de adquisición y preservación de la prueba



En general, siempre deberemos mantener las siguientes precauciones:

- El análisis siempre hay que hacerlo a partir de una segunda copia (o imagen) del soporte que se debe analizar. Es decir, en caso de que esta segunda copia o imagen sufra algún daño, siempre se podrá reiniciar el análisis a partir de la primera copia que tenemos, de forma que obtendremos un nuevo clon o una nueva imagen.

- En caso de que el soporte que se debe analizar sea extraíble, es necesario que el original (una vez hechas las copias pertinentes) se entregue a la tercera parte del proceso, es decir, al fedatario del origen del soporte. Además, con esta acción permitimos que se pueda producir un contraperitaje y garantizamos que nuestras hipótesis se puedan reproducir, mediante otro analista, a partir de una copia del original custodiado.

- En cuanto a la presencia del secretario judicial durante el proceso de clonación, hay varias sentencias que determinan que no es preceptiva, puesto que no puede dar fe de un proceso técnico que no está obligado a conocer en el ejercicio de sus funciones.

El caso expuesto es de los más sencillos que se pueden encontrar, puesto que a menudo podemos encontrar problemas como los que se describen a continuación:

- Heterogeneidad de sistemas interconectados.

- Configuraciones complejas (sistemas RAID, por ejemplo).

- *Softwares* especializados (programas de contabilidad, grabadores de vídeo, etc.): en estos casos, aunque se haya clonado el disco duro que los contiene, puede no ser sencillo, durante la fase de análisis, abrir los ficheros que tengan un formato propio (y ver su contenido), específicamente diseñado para la aplicación.

- Servidores ubicados en lugares distantes a la escena del crimen.

- Datos en la nube: la adquisición de los datos en la nube, que pueden ser compartidos por varios usuarios, puede implicar la vulneración del derecho a la intimidad (además de necesitar una metodología de adquisición específica). Si los datos no se han adquirido según los preceptos legales vigentes, pueden no tener validez jurídica.

- Volumen muy grande de datos: en este caso nos podemos plantear realizar una adquisición lógica de las evidencias relevantes, y elegir solo aquello que sea relevante para el caso de estudio.

- Dispositivos SSD (*solid state drive*): el valor *hash* de adquisición de los dispositivos SSD puede cambiar (por causas inherentes a su funcionamiento) si se hacen varias clonaciones consecutivas, aunque la integridad de la prueba no se haya comprometido.

- Sistemas críticos que no se pueden parar (hospitales, empresas, etc.): en estos casos deberemos obtener las evidencias con el sistema informático en funcionamiento, a menudo con la ayuda de los administradores.

3) Retención de tiempo y fechas. Las fechas y las horas de creación, acceso y modificación de un fichero pueden resultar de mucha utilidad a la hora de elaborar un informe pericial. Estos datos están vinculados a la fecha y la hora del reloj del sistema y, a pesar de que pueden ser de mucha utilidad forense, lo cierto es que se pueden modificar con facilidad y pueden no ser significativas. La fecha y la hora de los ficheros analizados puede ser muy relevante en algunas investigaciones, como por ejemplo las intrusiones en los sistemas informáticos. En este tipo de análisis es muy importante poder relacionar los datos horarios proporcionados por los ficheros de registro (o ficheros log) de conexión con la información localizada en los dispositivos confiscados. Finalmente, siempre que sea posible (por ejemplo, en el caso del análisis de un ordenador aislado en un domicilio particular), es interesante comprobar la hora y la fecha almacenada en la BIOS del sistema.

GMT

Se toma como base la hora GMT (*Greenwich Mean Time*), que es el huso horario que pasa por el meridiano de Greenwich (hora 0). Según esta convención, la Tierra está dividida en veinticinco zonas, de –12 a +12, con la hora 0 como referencia. El huso horario que corresponde a España es GMT+1.

4) Documentar quién preservó la prueba, dónde la preservó, cómo lo hizo, cuándo y por qué. Esta información documental da inicio a lo que se denomina **cadena de custodia**, la finalidad de la cual no es otra que la de permitir el rastro de las pruebas adquiridas.

5) Embalar los dispositivos que contienen las pruebas. En cada paquete se debe anotar, como mínimo, la siguiente información:

- Identificador único.
- Nombre del técnico responsable del material confiscado.
- Descripción del material (marca, número de serie, etc.).
- Propietario o usuario del material confiscado y lugar donde se ha confiscado (por ejemplo, se puede indicar la habitación del domicilio donde se encontró la prueba).
- Día y hora de la confiscación.
- Información relacionada con la causa que se investiga (por ejemplo, las diligencias previas de la causa).

6) Los soportes magnéticos u ópticos (cintas de copias de seguridad o *backups*, DVD, discos duros, etc.), se deben introducir en bolsas antiestáticas y posteriormente hay que acondicionarlos con material protector contra posibles golpes durante el transporte[9].

[9]Si se encuentran soportes, como por ejemplo un disco duro, sumergidos en líquidos, se deben conservar en el medio donde se han encontrado, y no hay que extraerlos ni secarlos.

7) Los técnicos que participan en este tipo de análisis deben tomar precauciones para preservar la prueba de factores externos como, por ejemplo, la lluvia o el paso de los embalajes a través de un arco magnético de un juzgado.

8) Transporte de las pruebas a un lugar seguro y que tenga los factores ambientales que permitan conservar la integridad de la prueba. El embalaje y el transporte de los dispositivos también forma parte de la **cadena de custodia**, la cual permite garantizar la integridad de las pruebas desde la obtención hasta la puesta a disposición de la autoridad judicial (o la llegada al laboratorio). La documentación de la cadena de custodia debe registrar todos los eslabones por los que circulan las pruebas; esto nos permitirá saber dónde se almacenan y quiénes han podido tener acceso a ellas en cualquier momento.

6. Preservación de la evidencia digital

El proceso de preservación implica la salvaguarda de la evidencia digital y de los dispositivos que la pueden contener. El proceso de preservación tiene que empezar en la primera fase del proceso (identificación) y se debe mantener durante el resto de fases de la gestión de la evidencia digital.

En un escenario óptimo, no se debería producir ninguna alteración o destrucción de los datos o de los metadatos asociados (por ejemplo, las fechas de última modificación de un archivo). El analista o perito debe ser capaz de demostrar que la evidencia no se ha alterado desde que fue identificada, recogida o adquirida.

En cualquier investigación, el analista debe poder dar cuenta de los datos y de los dispositivos recogidos y/o adquiridos. Con esta finalidad empleará la **cadena de custodia**, que es un registro (documento físico o registro digital) que muestra, cronológicamente, el movimiento y la gestión de la evidencia en todo momento, desde que fue recogida y/o adquirida. Por lo tanto, la cadena de custodia permite la identificación de los accesos y movimientos sufridos por los dispositivos digitales y las evidencias en cualquier fecha y hora desde que fueron recogidos. La cadena de custodia debería contener, como mínimo, la información necesaria para identificar la evidencia, quién ha accedido a ella, cuándo y en qué lugar se ha realizado el acceso, etc.

En la figura 6 se puede ver un ejemplo (un formulario en papel) de cadena de custodia.

Figura 6. Ejemplo documental de cadena de custodia

Cadena de custodia

SECCIÓN 1 (para completar por la persona que inicia la cadena de custodia)

Número de expediente 374/16

Descripción de la muestra
Ordenador portátil XY, modelo Z, con número de serie 348238C (número de muestra 24).

Fecha	Hora	Lugar
30/09/2016	15:20	Castellar del Vallès

Recibido por **Firma**
Alice A.

Organización y dirección
Instituto Forense, calle sin nombre, Sabadell

SECCIÓN 2

Fecha	Hora	Lugar
31/09/2016	10:30	Sabadell

Recibido por **Firma**
Bob B.

Organización y dirección
Instituto Forense, calle sin nombre, Sabadell

En resumen, lo que es esencial en el establecimiento de la cadena de custodia es:

- La primera anotación en el documento (véase la sección 1 de la figura 6) debe incluir la identificación con la que se haya etiquetado el indicio (entendiendo por indicio un dispositivo informático cualquiera, una bolsa precintada, etc.).

- La primera anotación debe incluir una descripción del indicio, con la fecha, la hora de recogida, una identificación completa (teléfono, nombre, persona/organización y dirección, o los datos que determine la institución como preceptivos) de quien ha recogido la muestra, así como su firma.

- Seguidamente, hay que ir documentando los transportistas siguientes o custodios de la muestra, con la misma identificación indicada en el punto anterior (véase la sección 2 de la figura 6).

En caso de emplear cadenas de custodia en formato papel, es habitual que la persona que se entrega el formulario se guarde una fotocopia de esta antes de entregar el original al responsable de la cadena siguiente. En todo caso, el formulario original siempre se podrá localizar junto con las evidencias originales.

La tendencia actual, en cuanto a la cadena de custodia, es que se digitalice progresivamente, no solo en cuanto a la desaparición del documento en formato papel, sino también en relación con la trazabilidad y garantía de integridad de las evidencias, e incluso con la auditabilidad de la cadena en sí misma.

Es importante que la fecha y la hora anotadas sean, exactamente, aquellas en las que se transfieren los indicios, porque indican en qué momento ha cambiado la persona que es responsable de ellos y quién tiene la custodia a partir de entonces y, por lo tanto, es ahora el nuevo responsable.

Además de indicarlo en el documento que registra las acciones referentes a la cadena de custodia, los indicios o dispositivos (ordenadores, portátiles, teléfonos, discos, etc.) que eventualmente contendrán las evidencias deben ser etiquetados (marcados de manera permanente) al ser recogidos y, si procede, precintados adecuadamente para evitar posteriores manipulaciones no autorizadas. La persona que los ha recogido debe poder asegurar en un juicio que son los mismos indicios que recogió en su momento. Del mismo modo que se hace con los indicios, las anotaciones en el documento de la cadena de custodia hay que hacerlos con algún dispositivo permanente.

Si la cadena de custodia fuera incompleta, o se hubiera producido algún error que el juez considerara significativo, podría determinar, según la severidad de este error o vacío, que las evidencias fueran inadmisibles, o bien admitirlas y otorgarles un peso o significado diferente al inicialmente previsto por la parte que presentan las pruebas. Esto puede, además, llevar a objeciones o apelaciones por la parte contraria. Por lo tanto, aunque los indicios pudieran ser aceptados, estos tipos de errores pueden llegar a disminuir fatalmente el valor de la evidencia digital.

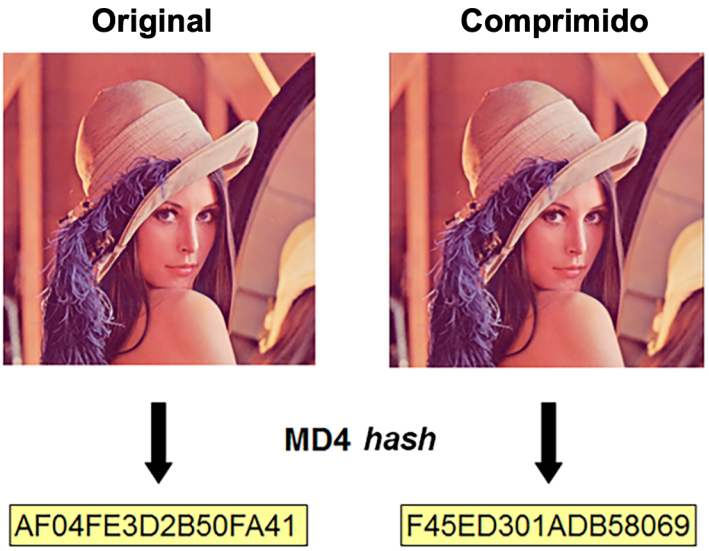
6.1. Verificación de la integridad mediante funciones *hash*

Cuando hemos introducido el concepto de clon se ha definido qué es una función *hash* y cómo se utilizaba para verificar que el proceso de clonación había sido correcto. Por la misma razón, este tipo de función también se puede emplear para comprobar que la integridad de una evidencia digital no ha sido comprometida.

Desde el punto de vista que nos ocupa, una función *hash* es una función matemática que, aplicada al contenido de un soporte informático (USB, disco duro, etc.), o incluso a un fichero individual, genera un resultado único, relevante a efectos de identificación del soporte o fichero. Debemos señalar que cualquier pequeña alteración en el soporte, incluso el cambio de un solo bit, produciría, al calcular un nuevo valor *hash*, un resultado completamente diferente del generado en primera instancia.

El cálculo de la función *hash* se realiza sobre los bits del archivo y no sobre el aparente contenido visual que este pueda tener. Así pues, dos fotografías pueden ser visualmente idénticas, pero si informáticamente tienen formatos diferentes o presentan un solo bit de diferencia, el cálculo de la función *hash* dará valores diferentes para los dos ficheros. Esta característica se puede comprobar en la figura 7.

Figura 7. Ejemplo de función *hash* (MD4)



En este ejemplo podemos comprobar que aunque el contenido visual de los dos ficheros es igual, como archivos informáticos (es decir, en cuanto a bits), las dos imágenes son diferentes, puesto que las dos fotografías no tienen el mismo formato (una es un archivo comprimido JPG y la otra un fichero BMP). En este ejemplo se ha empleado, con finalidades didácticas, la función *hash* MD4, aunque las que actualmente se usan en informática forense son las funciones SHA-2, SHA-1 y MD5.

Debido a esta propiedad de identificación unívoca de las funciones *hash*, a menudo se incorporan los valores *hash* generados durante el proceso de copia bit a bit de los soportes informáticos a los informes periciales. Así, en principio, si se compara el resultado del valor *hash* del soporte original con el del soporte copiado o clonado (por ejemplo, cuando un perito hace un contraperitaje y obtiene una nueva copia de análisis), los dos valores tendrían que ser idénticos, puesto que el segundo soporte contiene una copia íntegra del primero. Si no se obtiene el mismo resultado, podría significar que la cadena de custodia ha sido comprometida y los soportes informáticos alterados. A pesar de que esta consideración puede ser absolutamente errónea, como se verá a continuación, lo cierto es que desde la vertiente no técnica, a veces se ha considerado, de forma completamente errónea, el valor *hash* como un tipo de precinto digital, garante de la cadena de custodia.

Matemáticamente hablando, la función *hash* presenta, en cualquiera de sus formas, un problema inherente de colisión, es decir, es posible (aunque la probabilidad es muy pequeña) que dos soportes informáticos o dos ficheros diferentes, puedan tener el mismo valor *hash*. También hay que tener presente, como ya se ha indicado, que el cambio de un único bit implica el cambio absoluto del valor *hash*. Esto implica que si el dispositivo original (un disco duro, por ejemplo) ha sufrido cualquier golpe durante el transporte o su almacenamiento, o cualquier otro problema que lo haya podido dañar, es posible que las verificaciones de las funciones *hash* produzcan valores diferentes, sin que

la información relevante haya sido realmente alterada (el daño puede no haber afectado las evidencias de interés). Además, en el caso de los discos duros de los ordenadores personales, es posible que con el paso del tiempo la información se estropee sin que se haya producido ningún tipo de intervención, hecho que también producirá un valor *hash* diferente, a pesar de que no se hayan comprometido las evidencias.

Finalmente, el cálculo sucesivo de funciones *hash* sobre un dispositivo de tecnología SSD, también puede generar resultados diferentes, sin que nadie haya accedido tan solo al contenido del dispositivo (y mucho menos lo haya modificado).

Por lo tanto, hay que ser muy cuidadoso a la hora de interpretar el valor *hash* asociado a un dispositivo que contiene evidencias digitales y, en caso de obtener resultados divergentes, hay que tener presente que el hecho puede ser explicable, sin que nadie haya accedido o alterado la evidencia.

6.2. Digitalización de la cadena de custodia

La tendencia actual, en cuanto a la cadena de custodia, es que se digitalice progresivamente, no solo en cuanto a la desaparición del documento en formato papel, sino también en relación con la trazabilidad y garantía de integridad de las evidencias, e incluso con la auditabilidad de la cadena en sí misma.

Esta propuesta ya la podemos ver, por ejemplo, en el artículo de Ćosić y Bača (2010), donde se sugiere la incorporación de *timestamps* (sellos de tiempos) y la inclusión de medidas biométricas de los analistas para saber, de manera segura, quién tiene las evidencias. Por lo tanto, en este nuevo paradigma, la evidencia ya no viaja sola, sino que irá acompañada de varios datos que nos permiten auditar y trazar todos aquellos aspectos de interés en relación con la preservación de la evidencia durante todo su ciclo de vida.

El artículo ya mencionado describe conceptualmente los elementos que debe contener esta cadena de custodia, y que se deberían tener en cuenta a la hora de implementar la digitalización:

- **Quién** tiene la evidencia: en el ejemplo de la figura 8, el analista se identifica mediante una medida biométrica (una huella dactilar).

- **Cuál** es la evidencia: en este caso proponen el valor *hash* para identificarla.

- **Cuándo** se accede a la evidencia: se necesita establecer la fecha y la hora de cada acceso a la evidencia.

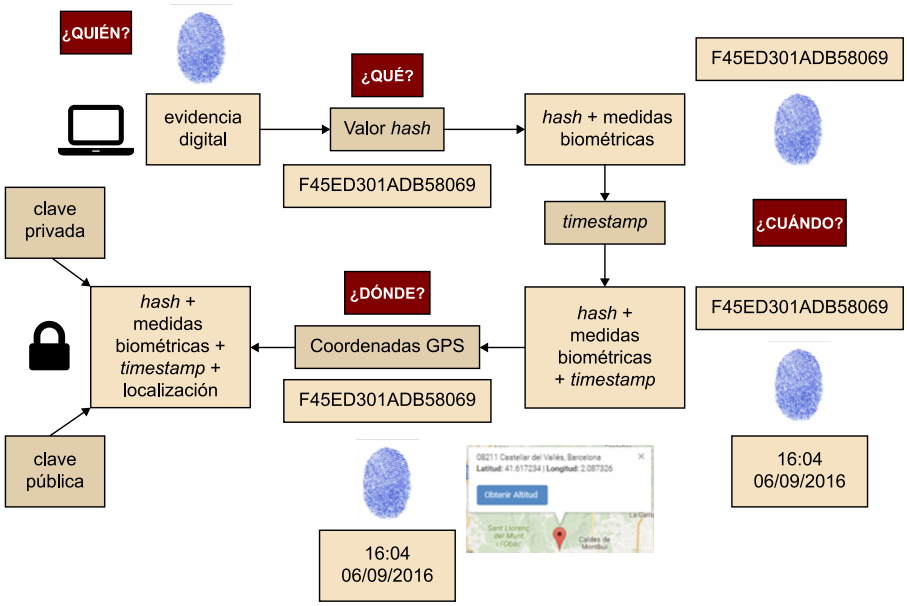
- **Dónde** se accede a la evidencia: también será necesario establecer el lugar donde se ha producido el acceso (por ejemplo, las coordenadas GPS donde

se ha adquirido la evidencia o las del laboratorio donde se haya podido transportar, etc.).

Y ya para acabar, para proteger la confidencialidad de la información, el esquema finaliza con la introducción de medidas criptográficas.

Con estos datos sería suficiente para poder gestionar la cadena de custodia de una evidencia digital.

Figura 8. Digitalización de la cadena de custodia



Otros estudios van más allá, y proponen una implementación del esquema antes descrito, en el que la cadena de custodia ya se ha digitalizado completamente y se ha convertido en información que se transmite entre dos o más dispositivos que controlan todo el proceso (Marqués Arpa, T.; Sierra Ruiz, J., 2014), y alcanza desde la creación del propio documento digital de la cadena de custodia, hasta la autenticación de las personas (proceso de confirmación de sus identidades) que pueden acceder a las evidencias, pasando también por la geolocalización de la evidencia en todo momento.

El dispositivo contiene el certificado personal que se transmite de manera segura a la central de datos, de forma que en todo momento se puede saber dónde está y quién tiene una determinada evidencia, y así poder revocar su acceso de manera remota, si se diera el caso. Una entidad de confianza proporciona el sello de tiempo en que las evidencias son accedidas o enviadas a otras personas, de forma que la cadena de custodia deja de ser un formulario físico para convertirse en un conjunto de datos que se van agregando a la evidencia de manera segura y donde se irá guardando de manera automática todo aquello que está sucediendo y que, posteriormente, si procede, podrá ser auditado.

7. Análisis de la prueba digital e investigación

En esta fase, el perito o el analista tiene que responder a las preguntas que se han expuesto en la introducción de este módulo, estudiando la prueba digital recogida en las fases anteriores. Este estudio se basará en el análisis del contenido de los ficheros (**datos**) y de la información sobre estos ficheros (**metadatos**).

Ejemplo de metadato

El contenido del campo «Autor» que aparece en todos los ficheros de Microsoft Word es un buen ejemplo de metadato.

En primer lugar, se tiene que revisar el embalaje que contiene las pruebas, con el fin de asegurar la integridad de la cadena de custodia y documentar cualquier anomalía que se pueda apreciar.

Normalmente, las pruebas se analizan en función de los extremos que debe responder el perito, puesto que un análisis exhaustivo requiere, en la mayoría de los casos, un esfuerzo desproporcionado en relación con el objeto del análisis. Así mismo, en el caso de peritaciones relacionadas con delitos, se tendrá que analizar un tipo concreto de pruebas y en un orden determinado en función del delito que se tenga que investigar. Finalmente, los parámetros del análisis también se tendrán que ajustar al sistema operativo (Mac OS, Windows, Linux, Android, etc.) del dispositivo que hay que analizar.

Justamente, una de las máximas del análisis forense tiene que ver con el funcionamiento intrínseco de los sistemas operativos y de las aplicaciones que hay:

> Por muy experto y conocedor que sea un usuario de un sistema operativo o de una aplicación, nunca podrá controlar y eliminar todas las trazas provocadas por el mismo funcionamiento de estos elementos.

En la fase de análisis pueden aparecer diferentes categorías de datos que se deben analizar, buena parte de los cuales serán lógicamente accesibles, es decir, datos contenidos en ficheros, directamente accesibles. En este proceso de análisis podemos encontrar varios problemas, como los que mencionamos a continuación:

- **Demasiada información**. Dispositivos con muchas gigas de información que se deben analizar y dificultad para discernir los ficheros con un contenido que puede ser relevante. Las herramientas de análisis disponen de muchas posibilidades para discriminar la información relevante (busca de cadenas, exclusión de ficheros con el valor *hash* conocido, etc.).

- **Ficheros troyanizados**. Es decir, ficheros que contienen un código oculto cuya ejecución puede tener consecuencias imprevisibles. Para detectar este tipo de ficheros, se pueden utilizar herramientas de comprobación de la integridad y programas detectores de virus y *malware*. Para comprobar el efecto y el funcionamiento de estos ficheros se pueden emplear técnicas diversas, como por ejemplo el análisis de la memoria RAM y la ejecución de este tipo de *software* (*malware*) en entornos seguros que permiten ser monitorizados fácilmente sin comprometer la seguridad del sistema. También existe la posibilidad de subir el fichero malicioso a webs que contienen un amplio catálogo de ficheros *hash* y que pueden generarlo, y cruzar el *hash* obtenido. De este modo, podemos obtener una descripción del fichero, así como de las acciones que realiza.

- **Ficheros cifrados o protegidos**. Los ficheros con métodos fuertes de cifrado (por ejemplo, GnuPG) no se pueden analizar (salvo excepciones puntuales). Sin embargo, otros métodos de protección, como las contraseñas de acceso a ficheros de texto (por ejemplo, Microsoft Office) o ficheros comprimidos, se pueden analizar utilizando aplicaciones desarrolladas por terceras partes y con un coste de computación relativamente bajo para contraseñas relativamente cortas.

Ficheros cifrados o protegidos

A menudo los usuarios cifran los archivos sin eliminar los originales. Por lo tanto, en todo análisis con archivos cifrados es aconsejable localizar los nombres de archivos iguales a los cifrados. Así mismo, los archivos temporales generados por algunas aplicaciones permiten acceder, de manera indirecta, al contenido (parcial o total) de los archivos cifrados. Para tratar ficheros protegidos con una contraseña, hay programas que la rompen por la fuerza bruta utilizando el cálculo distribuido entre varios ordenadores.

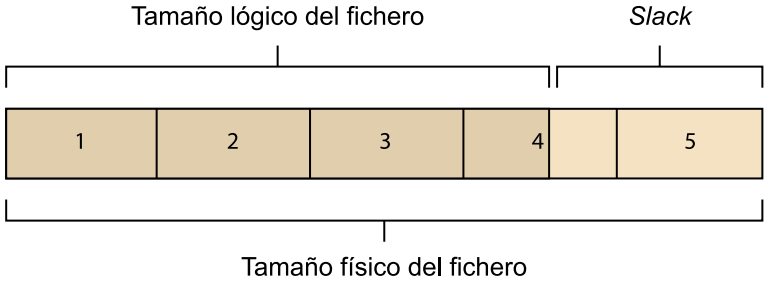
- **Datos ocultos mediante esteganografía**. A diferencia de la criptografía, la esteganografía esconde los datos entre otros tipos de datos (por ejemplo, un fichero de texto dentro de una fotografía). Así, el fichero que contiene la fotografía es lógicamente accesible, pero su visualización no nos permite ni siquiera intuir que contiene un mensaje oculto.

- **Archivos que se han eliminado** y todavía no se han sobrescrito.

- **Datos localizados en *ambient data***. Se denominan así los datos que aparecen en localizaciones que no son visibles directamente y que requieren un *software* específico para recuperarlos o visualizarlos. Por ejemplo:
  - *File slack*: tal como ya hemos definido, se denomina así el espacio que hay entre el final lógico de un fichero y el final físico.
  - *Unallocated cluster*[10]: clúster que, aunque no esté asociado a ningún fichero en concreto, a menudo puede contener información de carácter residual (por ejemplo, partes de un documento de texto que ya ha sido eliminado del disco duro o una versión antigua de un fichero ya existente, etc.).

(10)Un clúster es la unidad mínima de asignación en un disco duro y puede contener varios sectores.

Figura 9. Representación gráfica del *file slack* de un archivo



Los *unallocated clusters* y el *file slack*

Tanto los denominados *unallocated clusters* como el *file slack* son susceptibles de contener información residual, procedente de fragmentos de antiguos archivos. Además, el *file slack* es una ubicación excelente para almacenar información deliberadamente oculta. Si se encuentran pruebas en un *file slack*, se tiene que extraer el fichero atendiendo al límite físico o, en caso contrario, perderemos la información en el proceso de extracción. Si los datos relevantes aparecen en los *unallocated clusters*, claramente no están asignados a ningún fichero accesible; sin embargo, las herramientas de análisis nos permiten situar los datos en un sector físico determinado del disco duro (este dato es importante, puesto que nos permitirá situar la prueba en el soporte digital como si se tratara de una ruta en el sistema de ficheros).

7.1. *Write blockers*

A veces, habrá que manipular el disco duro original conectándolo directamente al ordenador de análisis. Hay soluciones, tanto de *software* como de *hardware*, que permiten filtrar las peticiones de escritura sobre el disco duro, de forma que el examen del soporte no altere la prueba[11].

[11]Estos tipos de dispositivos pueden ser de mucha utilidad para hacer tareas de preanálisis y de adquisición lógica de la evidencia *in situ*, sin alterarla.

Tal como podemos ver en las imágenes, el disco duro se colocaría en la conexión de la tarjeta y, mediante un cable USB, el dispositivo *write blocker* se conectaría al ordenador de análisis (es decir, entre el ordenador y el disco duro) y filtraría cualquier petición de escritura sobre el disco duro.

Figura 10. Dispositivo *write blocker* (FastBloc3, de Guidance Software)

Figura 11. *Write blocker* (FastBloc 3, de Guidance Software) con el cable USB de conexión al ordenador de análisis

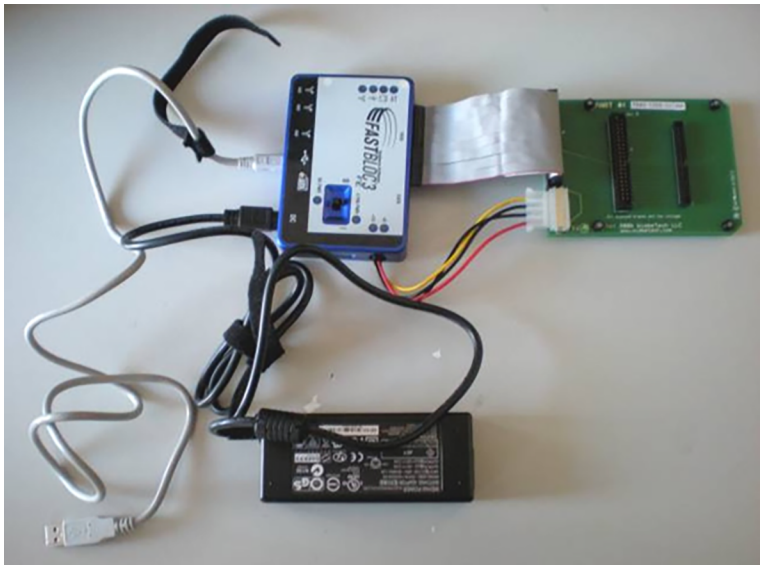


Figura 12. Maletín de tarjetas del dispositivo FastBloc

En definitiva, estos dispositivos pueden ser de gran utilidad en los siguientes casos:

- Realización de preanálisis urgentes, en los que no se dispone del tiempo necesario para llevar a cabo una clonación y el análisis posterior en el laboratorio.

- Adquisición de datos no invasiva en un entorno de sistema operativo: mediante estos dispositivos, también se pueden adquirir los datos de los soportes enteros examinados o de una parte (por ejemplo, los que se consideran relevantes después del preanálisis efectuado).

7.2. Herramientas de análisis informático: Encase, Autopsy, distribuciones de Linux

Algunas de las herramientas ya mencionadas, como Encase, permiten gestionar todas las fases del análisis forense, desde la adquisición de los soportes originales y el análisis, hasta la generación automática del informe final. Muchas de estas herramientas se basan en código propietario y, a pesar de ofrecer muchas garantías y ser muy amigables, a veces es preferible la flexibilidad que nos permiten las aplicaciones basadas en código abierto (*open source*). Quizás una de las herramientas más conocidas es la distribución de Linux CAINE (o, entre otras, SIFT, CAINE, DEFT, Kali, etc.). Este tipo de distribuciones se ejecutan, directamente, desde un DVD o USB e incluyen un gran número de herramientas relacionadas con el mundo de la seguridad informática. Otra herramienta, con una interfaz del estilo del Encase, pero *open source*, es Autopsy.

No hay ninguna aplicación que pueda cubrir todos los aspectos de un análisis forense. Normalmente, las aplicaciones que sean más generales y con interfaces amigables, serán de mucha utilidad para un porcentaje de casos elevado; sin embargo, en determinadas operaciones (por ejemplo, en la recuperación de archivos eliminados u otras muy específicas) pueden ser menos eficaces que las aplicaciones diseñadas específicamente para una finalidad concreta. Otras veces, como por ejemplo la gestión de los archivos criptográficos, siempre se tendrá que recurrir a programas específicos o diseñados por el mismo analista. En definitiva, los laboratorios de informática forense tienen que disponer necesariamente de una gran variedad de aplicaciones, generales y específicas, de código abierto y propietario, adecuadas a diferentes tipos de sistemas operativos y a los sistemas respectivos de ficheros.

Las extracciones de memoria RAM se pueden efectuar con la herramienta Volatility, un entorno de trabajo de código abierto para el análisis forense, escrito en Python y compatible con Microsoft Windows, OS X y Linux.

7.3. Virtualización y análisis en vivo

A menudo, los analistas solo disponen de los clones o de las imágenes forenses que se deben analizar y no tienen acceso a los ordenadores que alojaban los contenidos originales. Así pues, a veces, a pesar de tener acceso lógico a los ficheros del soporte que debemos analizar, no podremos examinar el contenido porque estos ficheros tienen un formato propio, solo accesible desde la aplicación que los ha generado. En lugar de adquirir la aplicación específica, se puede intentar ejecutar el sistema que debemos analizar por medio de una máquina virtual.

Esta técnica también nos puede ser muy útil, por ejemplo, para analizar un disco duro que contiene algún troyano. La ejecución del sistema mediante una máquina virtual nos podría permitir, por ejemplo, averiguar qué tipo de acciones lleva a cabo el troyano y a qué direcciones IP envía la información del ordenador local.

Por ejemplo, para ejecutar un clon, podemos emplear herramientas como WMware o VirtualBox. Para ejecutar imágenes forenses, podemos emplear, por ejemplo, Live View.

7.4. Procedimiento general de análisis

Una vez recibimos los dispositivos que se deben analizar, en primer lugar (y previamente a cualquier tarea de análisis), será necesario comprobar la corrección de los datos que figuran en la cadena de custodia de las evidencias susceptibles de ser analizadas.

En cuanto al análisis en sí mismo, y a pesar de que existen muchos métodos posibles e igualmente válidos, se podría tener en cuenta el procedimiento que se detalla a continuación.

1) Recuperación de los archivos borrados

Consiste en realizar una recuperación parcial o total de la información eliminada existente en los dispositivos susceptibles de ser analizados. Esta operación incluye los datos localizados en las áreas sin asignar del disco duro, así como una recuperación de los datos de archivos y directorios «huérfanos», cuya vinculación se ha perdido. Este método de recuperación puede incluir procedimientos de recuperación de archivos basados en *carving*.

2) Estudio del sistema operativo

En cuanto al estudio del sistema operativo, desde un punto de vista muy básico, se podrían efectuar las siguientes comprobaciones:

- Identificación del sistema operativo del equipo y localización de la partición que aloja el sistema.
- Identificación de la fecha de instalación del sistema.
- Identificación de los diferentes usuarios definidos en el sistema.
- Última fecha de acceso al equipo (para cada uno de los usuarios).
- Identificación de los dispositivos de *hardware* y *software* reconocidos por el sistema.

3) Estudio de la seguridad

En esta etapa, el objetivo consistirá en estudiar si las evidencias analizadas han sido comprometidas (o incluso añadidas deliberadamente con el fin de perjudicar a una persona). En definitiva, se deberá identificar cualquier *software* malicioso (virus, troyano, etc.), evaluar el daño sufrido, identificar los archivos que han sido comprometidos (eliminados, modificados, etc.), así como determinar la vía de acceso al sistema.

4) Análisis detallado de las evidencias digitales

Sin querer ser demasiado exhaustivos, el análisis detallado de las evidencias podría incluir los siguientes apartados, algunos de los cuales ya han sido tratados en apartados anteriores. Cada analista tendrá que decidir, según el caso, aquellas pruebas que tiene que practicar necesariamente y aquellas que, quizás, no sean relevantes.

- Información relativa al sistema analizado: *hardware* instalado y reconocido por el sistema operativo, fecha, hora y usuario que empleó el sistema por última vez, fecha de instalación.

- Estudio de los dispositivos físicos que en algún momento pudieron ser conectados al sistema analizado: móviles, USB, impresoras, escáneres, cámaras, tarjetas de memoria, etc.

- Estudio del escritorio y de la papelera de reciclaje.

- Conexiones de red, identificación de la MAC y direcciones IP.

- Estudio del registro del sistema y logs de auditoría del sistema operativo y de las aplicaciones instaladas (si se dispone de logs).

- Estudio de la información contenida en los *unallocated clusters* o en el *file slack*.

- Información contenida en los archivos de hibernación, paginación, particiones y archivos de intercambio (*swap*).

- Análisis de la cola de impresión.

- Visualización de los enlaces de los archivos y de los archivos a los que se ha accedido recientemente.

- Estudio de los directorios de usuario.

- Estudio de las aplicaciones instaladas relacionadas con actividades de programación, grabación y tratamiento de imágenes, procesamiento de audio y vídeo, *softwares* de contabilidad, ofimática, etc.

- Estudio de los metadatos de los archivos, si se considera que pueden ser relevantes para el caso.

- Estudio de las aplicaciones de virtualización.

- Estudio de las bases de datos instaladas y de las aplicaciones que permiten su gestión.

- Estudio de los *softwares* de cifrado, particiones cifradas, etc.

- Estudio de la navegación por Internet, de los históricos y de las *cookies*.

- Análisis de los clientes de correo electrónico y del correo web (suponiendo que el analista disponga de la autorización necesaria).

- Análisis de los registros de mensajería instantánea, chats y contactos.

Algunas de estas operaciones pueden ser difíciles de llevar a cabo si no se dispone del ordenador original o de las aplicaciones gestoras de los datos (por ejemplo, *softwares* de grabación de vídeo, de contabilidad, etc.). Hay que tener presente que es posible que en el laboratorio solo nos lleguen los discos duros para analizar, pero no los ordenadores que los contenían.

7.5. Análisis e investigación

7.5.1. El marco legal

No solamente los aspectos técnicos son relevantes en todo proceso de análisis informático. También hay que tener muy en cuenta que no todo aquello que es técnicamente posible es legal. Supongamos, por ejemplo, que en una empresa se sospecha que un trabajador envía y recibe muchos correos electrónicos relacionados con temas de ocio personal, que además ocupan un volumen de disco duro considerable. Técnicamente, lo más sencillo sería examinar los contenidos del correo electrónico del trabajador; sin embargo, tal como ya nos podemos imaginar, estaríamos incurriendo en un delito de graves consecuencias, inimaginables teniendo en cuenta la sencillez técnica con la cual un administrador del sistema podría efectuar estas comprobaciones. Del mismo modo, hay otros problemas, ya no tan evidentes, que pueden llegar a tener consecuencias desastrosas. Como en el supuesto que nos ocupa, a menudo deberemos investigar los hechos mediante técnicas indirectas (constatando, por ejemplo, un consumo desproporcionado de ancho de banda).

Por lo tanto, aunque no es el objetivo de este módulo, siempre tenemos que tener en cuenta el marco legal que nos limita y que, a menudo, lo importante no es obtener una prueba, sino conseguir presentarla como prueba en un juicio.

7.5.2. Análisis de correos electrónicos

El análisis de correos electrónicos es uno de los temas de investigación más recurrentes. Nuestra intención no es explicar cómo hacer una investigación de las cabeceras de un correo electrónico para descubrir la dirección IP de origen, sino más bien describir los problemas que comporta su análisis desde el punto de vista legal.

La apertura de los correos electrónicos no abiertos se tiene que hacer algunas veces ante el juez. Esto es así porque, en el marco legal, se ha asimilado el correo postal al correo electrónico. Desde el punto de vista estrictamente técnico, las diferencias entre los dos son apreciables y, en todo caso, el correo electrónico más bien se tendría que asimilar a una postal (es decir, a una carta sin sobre, con los datos y el remitente a la vista). La apertura de los correos ante el juez comporta innumerables problemas:

- Puede haber un gran número de correos, quizás miles, pendientes de abrir.
- La apertura se lleva a cabo en un ordenador de análisis, preferentemente portátil, aportado por el perito. Dada la gran diversidad de programas cliente de correo electrónico, es posible que la apertura no sea una tarea nada fácil, especialmente si no se ha podido preparar por adelantado.
- Técnicamente, es muy difícil determinar si un correo ha sido abierto o no.

Mención aparte merecen los correos electrónicos de correo web (*webmail*). En este caso, los correos aparecen, residualmente, en los directorios temporales de Internet, de donde se podrán recuperar con relativa facilidad (el usuario desconoce la existencia de estos documentos, puesto que se almacenan involuntariamente en los directorios temporales). A diferencia de los anteriores, en este caso no hay ninguna duda de que el usuario ha abierto previamente los correos, y analizarlos, probablemente, no tendría que comportar ningún problema (no tenemos que olvidar que el juez será quien decida, finalmente, si la apertura, a pesar de tratarse de correos web, se hará en su presencia o no).

Correo

Por ejemplo, los indicadores de seguimiento que determinan en los programes cliente si el correo ha sido abierto o no, pueden ser modificados fácilmente por el usuario.

7.5.3. Los ficheros de registro y la investigación de los delitos informáticos

La investigación de los delitos informáticos se realiza, como nos podemos imaginar, mediante el estudio de las direcciones IP involucradas en el presunto delito. La dirección IP tiene consideración de dato personal y, por lo tanto, los proveedores de servicios de Internet no podrán efectuar la cesión de estos datos sino es mediante un mandato judicial.

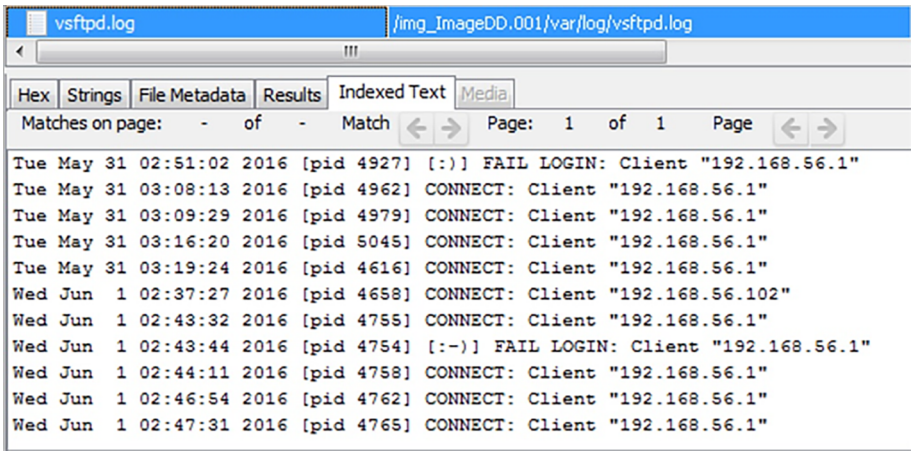
Para no imposibilitar la investigación de los delitos, **la ley de conservación de datos** determinará la obligatoriedad de que los proveedores tengan que conservar los logs o ficheros de registro (artículo 4), así como la duración de este periodo de conservación (artículo 5), que, como podemos ver, se puede modular en función del interés de la investigación.

Artículo 5. Periodo de conservación de los datos.

1. La obligación de conservación de datos impuesta **cesa al cabo de doce meses** a contar desde la fecha en que se haya producido la comunicación. Por reglamento, con la consulta previa a los operadores, se puede ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos **hasta un máximo de dos años o un mínimo de seis meses**, teniendo en cuenta el coste del almacenamiento y la conservación de los datos, así como su interés para los fines de investigación, detección y enjuiciamiento de un delito grave, con la consulta previa a los operadores.

A continuación, podemos ver un ejemplo de fichero de registro (vsftpd.log), extraído de los materiales *Com s'ha de fer l'informe pericial d'un delicte informàtic?* «Col·lecció H2PAC» de la UOC:

Figura 13. Fichero de registro del servicio FTP



En esta captura de pantalla podemos observar como, poco antes de que se produjeran los hechos investigados (este dato lo obtendríamos a partir del trabajo hecho por los investigadores del caso), se produce una conexión con éxito desde la dirección IP 192.168.56.1 (una dirección local). Si se examinara el

fichero de registro entero, se vería que se han producido varios intentos de acceso, con y sin éxito, en fechas y horas cercanas a los hechos investigados. Las direcciones IP implicadas en estos tipos de actividades se pueden encontrar en lugares geográficamente lejanos, en países extranjeros, por lo cual la persecución del delito (que siempre requerirá varios mandamientos judiciales para poder averiguar el camino hasta el titular del teléfono) puede ser muy difícil, e incluso puede resultar imposible de trazar hasta el origen. Sin embargo, observemos que sin las direcciones IP, muchos delitos informáticos no se podrían investigar.

8. Presentación e informe

En el informe elaborado por el experto se presentarán las pruebas relacionadas con el caso, las conclusiones y también la justificación del procedimiento empleado. A menudo, este informe se ratificará en presencia del juez, aunque a menudo las peritaciones irán destinadas a empresas. Sin embargo, en los dos casos no es necesario que el lector del informe tenga el bagaje técnico suficiente para comprender un análisis forense en profundidad. Por lo tanto, en general no se tiene que emplear el lenguaje técnico de manera abusiva y, siempre que sea necesario utilizarlo, convendrá poner notas aclaratorias a pie de página e, incluso, en forma de anexos y glosarios. Dado que muchos de estos informes se tienen que presentar ante un tribunal, el analista tiene que tener en cuenta que, además de aplicar el rigor técnico, debe ser lo suficientemente habilidoso para comunicar el resultado del análisis de manera concisa y clara.

Informes periciales

Se puede encontrar más información sobre el contenido y la estructura de los informes periciales en el módulo «El peritaje. El análisis forense y el sistema legal» de esta asignatura.

9. El laboratorio de informática forense

Una de las aspiraciones de cualquier laboratorio de informática forense consiste en obtener algún tipo de certificación que avale la calidad y la corrección en cuanto a la normativa vigente. Organizaciones como ENFSI promueven la acreditación de todos los laboratorios oficiales de criminalística que pertenecen a los países adscritos. En concreto, ENFSI promueve la adecuación de todos los laboratorios oficiales a la norma ISO/IEC 17025 de Requisitos generales para la competencia de laboratorios de ensayo y calibración. Sin embargo, observamos que esta norma no está específicamente pensada para laboratorios de criminalística (entre los cuales hay los laboratorios de informática forense).

La implantación de esta norma a ensayos tan dispares y alejados de los propósitos iniciales de la norma ISO/IEC 17025, como son el estudio de proyecciones de manchas de sangre o la clonación de discos duros, es una tarea compleja y con muchos vacíos que hay que interpretar, para adaptar la operatividad del laboratorio al contenido de la norma. A diferencia de otras normas, la norma ISO/IEC 17025 no se puede certificar, sino que solo es susceptible de ser acreditada. En términos generales, y para no incidir excesivamente en una cuestión tan ajena al objetivo de este curso, la acreditación alcanza ensayos concretos de cada laboratorio (por ejemplo, «identificación y cuantificación de cocaína») y no tiene un alcance tan «horizontal» como las certificaciones (que pueden alcanzar la actividad entera de una organización). Esto no quiere decir que las actividades de un laboratorio que se encuentran fuera del alcance se realicen sin ninguna garantía, puesto que los ensayos bajo la norma ISO/IEC 17025 pueden coexistir con otras normas o certificaciones que aseguren que el laboratorio entero trabaja correctamente en términos de calidad.

Además de la acreditación bajo la norma ISO/IEC 17025, también hay otras normas y manuales de buenas prácticas que el laboratorio puede emplear para definir sus procedimientos internos de trabajo. De hecho, el abanico de posibilidades es tan enorme que es causa de una gran confusión entre todos los actores implicados; sin embargo, el camino hacia la normalización es una cosa que, en nuestra opinión, es inevitable y que marcará el futuro de los que decidan hacer de este trabajo su profesión.

A nuestro entender, cualquier proceso de certificación se basa en los cuatro siguientes pilares:

Pilares del proceso de certificación

- Normalización de las instalaciones.
- Obtención de los medios materiales.
- Normalización de los procedimientos de trabajo.
- Formación certificada de los analistas.

Los medios materiales necesarios y las metodologías de trabajo ya se han estudiado en apartados anteriores, y la normalización de las instalaciones seguramente excedería el propósito de estos materiales. Sin embargo, creemos que es necesario aportar alguna información en cuanto a la certificación profesional.

9.1. Formación certificada de los analistas forenses

En primer lugar, hay que señalar que muchas herramientas forenses disponen de sus propias certificaciones, lo cual ya nos puede orientar sobre la formación que nos interesa. También hay otras certificaciones de carácter generalista que pueden ser de interés para iniciarse en la materia o para acreditar los conocimientos del analista. En cuanto a las universidades, visto el carácter reciente y multidisciplinario de esta materia, la informática forense todavía no aparece reflejada en la mayoría de planes de estudio.

De entre el aluvión de certificaciones y cursos forenses, creemos oportuno destacar las siguientes certificaciones[12] (es muy interesante completarlas con otras certificaciones más relacionadas con la seguridad informática):

[12]Algunas de las certificaciones tienen fecha de caducidad y requieren nuevas pruebas para mantener la validez de la certificación. Muchas ofrecen certificación a diferentes niveles de experiencia.

- Computer Hacking Forensic Investigator Certification (CHFI): Certificación profesional proporcionada por la International Council of E-Commerce Consultants (EC-Council).

- Guidance Software (EnCe): La certificación EnCase Certified Examiner (EnCE) reconoce el dominio de las metodologías propias de la informática forense empleando el *software* EnCase.

- IACIS Certified Forensic Computer Examiner (CFCE). IACIS (International Association of Computer Investigative Specialists) es una corporación sin ánimo de lucro, formada por profesionales policiales, dedicados a la formación en el campo de la informática forense. Están en los Estados Unidos.

- Certified Computer Examiner (CCE). Certificación ofrecida por la ISCFE (International Society of Computer Forensic Examiners) y dirigida tanto al sector policial como al privado.

- SANS Certifications. SANS (SysAdmin, Audit, Network and Security Institute), creado en 1989, ofrece multitud de certificaciones y certificados,

basados en la superación de cursos de cinco o seis días y uno o dos días (respectivamente). Su ámbito de actuación es enorme y una opción que se tiene que tener en cuenta.

Resumen

En este módulo hemos estudiado las diferentes etapas que conforman un análisis forense. Estos materiales no buscan constituirse en un compendio de fórmulas para gestionar cualquier tipo de análisis, sino ofrecer una imagen muy generalista de la materia, en la que se ha procurado dibujar una parte importante de todo el abanico de posibilidades que ofrece esta ciencia multidisciplinaria, de reciente creación.

Además de las técnicas y de los procedimientos asociados a las etapas del análisis forense, se han presentado algunas cuestiones de ámbito normativo, esenciales para entender cómo se investigan los delitos informáticos. En este sentido, es esencial comprender que hay que manipular con mucho cuidado las evidencias digitales para que puedan tener validez en un procedimiento judicial. Del mismo modo, es importante entender que no todo aquello que es técnicamente posible se encuentra conforme a la ley (por ejemplo, como peritos, podemos abrir un correo electrónico, pero si no tenemos la autorización, es posible que nuestra acción no solo invalide la prueba, sino que incluso podría tener responsabilidades penales).

Actividades

1. El cálculo del valor *hash* de un fichero se puede llevar a cabo en línea: http://onlinemd5.com/

Observación

Si el enlace anterior no funcionara, puedes encontrar en la red otros sitios web con funcionalidades similares.

Responde a las siguientes preguntas:

a) Crea un fichero con el procesador de textos que habitualmente uses y escribe una frase cualquiera. Guárdalo y calcula el valor *hash* MD5 en línea. Anota o copia el valor obtenido.

b) Vuelve a abrir nuevamente el fichero que has creado anteriormente, añade cualquier texto al fichero y vuélvelo a guardar. Calcula el valor *hash* del fichero y compáralo con el anterior[13].

[13]Podéis usar el Foro de la asignatura para comentar estas actividades.

c) ¿Son iguales los dos valores? Si son diferentes, ¿cuál crees que es la explicación? En relación con las propiedades de integridad, confidencialidad y disponibilidad, ¿cuál crees que puede tener alguna relación con las funciones *hash*? (si no sabes a que se refieren estas propiedades, puedes buscar más información en Internet).

2. Busca en Internet información sobre el llamado Machine Identification Code (*yellow dotes, tracking dotes* o *secret dotes*), en relación con las impresoras láser. ¿Qué valor forense crees que tienen estos puntos? ¿Qué relación tienen con la esteganografía?

3. ¿Qué relación hay entre la gestión de incidentes de seguridad y la informática forense?

Ejercicios de autoevaluación

1. ¿Cuál es el orden lógico de las fases de un análisis forense?

a) Adquisición, identificación, aseguramiento de la escena, análisis y presentación.
b) Identificación, análisis, adquisición, aseguramiento de la escena y presentación.
c) Aseguramiento de la escena, adquisición, identificación, presentación y análisis.
d) Aseguramiento de la escena, identificación, adquisición, análisis y presentación.

2. Se conoce con el nombre de esteganografía:

a) Una técnica de detección y corrección de errores de integridad en sistemas de ficheros.
b) Un conjunto de herramientas para la adquisición y el análisis de memoria RAM.
c) Un *hash* avanzado de 512 bits o más.
d) Una técnica de ocultación de la información.

3. Relaciona cada definición con el término adecuado:

Obtener el clon de un disco duro.	Asegurar la escena
Encontrar todos los documentos ofimáticos relacionados con la investigación de un caso.	Identificar y recoger la evidencia
Restringir el acceso a la escena del suceso.	Adquirir la evidencia
Elaborar las conclusiones de un análisis forense.	Analizar la evidencia
Decidir si se recogen o no unos dispositivos USB encontrados en un cajón de la escena del suceso.	Presentación e informe

4. ¿A que se refiere el principio de Locard?

a) A que todo proceso llevado a cabo, que no sea repetible por un tercer perito, no tendrá validez en un procedimiento legal.

b) Es un conjunto de principios básicos que hay que tener en cuenta en la fase de adquisición de evidencias.
c) Nos dice que las evidencias digitales son fácilmente alterables.
d) Cuando dos objetos entran en contacto se produce una transferencia de material.

5. La evidencia digital puede ser...

a) Física y volátil.
b) No volátil.
c) Volátil y no volátil.
d) Volátil.

6. Una función *hash* es...

a) Una técnica que nos permite identificar a todos aquellos ficheros que visualmente presentan el mismo contenido.
b) Una función matemática que genera un identificador resumido a partir de unos datos de entrada.
c) Una técnica empleada para generar clones de una evidencia forense.
d) Una función matemática inmune al problema de las colisiones.

Solucionario

Ejercicios de autoevaluación

1. d

2. d

3.

Restringir el acceso a la escena del suceso.	Asegurar la escena
Decidir si se recogen o no unos dispositivos USB encontrados en un cajón de la escena del suceso.	Identificar y recoger la evidencia
Obtener el clon de un disco duro.	Adquirir la evidencia
Encontrar todos los documentos ofimáticos relacionados con la investigación de un caso.	Analizar la evidencia
Elaborar las conclusiones de un análisis forense.	Presentación e informe

4. d

5. c

6. b

Glosario

ambient data *n* Datos que aparecen en localizaciones que no son directamente visibles y que requieren un *software* específico para ser recuperados o visualizados.

análisis forense informático *f* Proceso resultante de aplicar métodos científicos a los sistemas informáticos con el fin de asegurar, identificar, preservar, analizar y presentar la prueba digital, de forma que esta sea aceptada en un proceso judicial.

clon *m* Copia de bits del soporte original. Por lo tanto, tiene que contener, igual que el original, los archivos ocultos, los eliminados y no sobrescritos, el denominado espacio desaprovechado, etc.

clúster *m* Unidad mínima de asignación de un disco duro. Un clúster puede contener varios sectores, según el sistema de ficheros.

esteganografía *f* Conjunto de técnicas que permiten la ocultación de cualquier tipo de datos. A diferencia de la criptografía, la esteganografía esconde los datos entre otro tipo de datos, pero no los modifica para que no sean legibles.

file slack *n* Espacio entre el final lógico y el final físico de un fichero.

hash *n* Función matemática unidireccional que resume un mensaje de tamaño variable (por ejemplo, un archivo) en una representación de tamaño fijo. Es poco probable que dos ficheros diferentes tengan la misma representación *hash*, lo cual significa que este valor se puede utilizar para comprobar la integridad de un archivo (o de un sistema entero). Las funciones *hash* más conocidas son MD5 y SHA-1.

log o fichero de registro *n* Un log o fichero de registro es la grabación secuencial en un fichero o en una base de datos de todos los acontecimientos o todas las acciones que afectan a un proceso particular (una aplicación, la actividad de una red informática, etc.). El contenido de estos ficheros es muy importante para la investigación de los delitos informáticos.

logging *n* Procedimiento mediante el cual se registran, en un fichero, las actividades que acontecen en un sistema operativo o en una aplicación. Este fichero, denominado genéricamente log, almacena las trazas de todo lo que ha sucedido en el sistema (por ejemplo, un ataque del que haya podido ser objeto).

mac-time *n* Tiempo de modificación (*m*) y acceso (*a*) de archivos, y modificación de metadatos (*c*) de los archivos.

marca horaria *f* Véase *timestamp*.

prueba *f* Elemento que proporciona información que conduzca a alguna conclusión o hallazgo relacionado con el hecho que se investiga.

prueba digital *f* Prueba almacenada en soportes digitales.

prueba volátil *f* Prueba que desaparece en ausencia de alimentación eléctrica.

timeline *n* Presentación de los *mac-time* en orden temporal.

timestamp *n* Secuencia de caracteres que denota la fecha y/u hora en que se ha producido un acontecimiento determinado.

unallocated cluster *n* Clúster que, a pesar de no estar asignado a ningún fichero en concreto, puede contener información, a menudo de carácter residual.

Bibliografía

AENOR (norma UNE) (2013). UNE 71505-1:2013 Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales.

AENOR (norma UNE) (2013). UNE 71505-2:2013 Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas.

AENOR (norma UNE) (2013). UNE 71505-3:2013 Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 3: Formatos y mecanismos técnicos.

AENOR (norma UNE) (2013). UNE 71506:2013 Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas.

AENOR (norma UNE) (2015). UNE 197010:2015. Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC).

Arqués, J. M.; Colobran, M.; Iparraguirre, J. (2016). *Com s'ha de fer l'informe pericial d'un delicte informàtic?*«Col·lecció H2PAC». Editorial UOC. ISBN: 978-84-9116-584-2, 2016.

Arqués, J. M.; Guasch, A.; Sierra, J. (2016). «La cadena de custòdia de les evidències digitals». En: *La ciberseguretat a Catalunya. Informe de l'Observatori del Risc* (pág. 99-115). Institut d'Estudis de la Seguretat (IDES). ISBN: 978-84-617-7162-2.

Arqués Soldevila, J. M.; Colobran Huguet, M.; Guasch Pequeño, A. (2009). *Anàlisi forense de sistemes d'informació*. Barcelona: FUOC.

Blanquez, M. (2019). *Validació d'eines d'anàlisi forense digital sota la norma ISO/IEC 17025*. Treball Final de Màster MISTIC-UOC.

Colobran, M.; Morón, E. (2004). *Introducción a la seguridad informática*. Barcelona: Planeta UOC.

Ćosić, J.; Bača, M. (2010). A Framework to (Im)Prove «Chain of Custody» in Digital Investigation Process. Proceedings of the 21st Central European Conference on Information and Intelligent Systems. Faculty of Organization and Informatics. September 22-24 2010 (pág. 435-438). Croacia: Varaždin.

Cruz Allende, D. (2007). *Análisis forense de sistemas de información*. Barcelona: FUOC.

European Network of Forensic Science Institutes (ENFSI) (2015). *Best Practice Manual for the Forensic Examination of Digital Technology*. <http://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf>

International Organization for Standardization/International Electrotechnical Commission (2012). ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence.

Marqués-Arpa, T.; Sierra-Ruiz, J. (2014). Cadena de Custodia en el Análisis Forense. Implementación de un Marco de Gestión de la Evidencia Digital. Reunión Española de Criptografía y Seguridad de la Información. Alicante.

NIST Special Publication 800-101 Revision 1, Rick Ayers, Sam Brothers, Wayne Jansen (2014). Guidelines on Mobile Device Forensics. <http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf>