

---

## *TEMA 2: La metodología forense*

*IES Zaidín-Vergeles*

*10 de diciembre de 2020*



---

## Tabla de contenidos

---

<b>1. Objetivos del tema</b>	<b>1</b>
<b>2. La evidencia digital</b>	<b>3</b>
2.1. Tipos de evidencias y orden de volatilidad . . . . .	3
2.2. Acotando la escena del crimen . . . . .	4
2.3. Adquisición de evidencias . . . . .	5
2.3.1. Diferencias entre una adquisición física y una adquisición lógica	7
2.3.2. Adquisición de evidencias volátiles . . . . .	8
2.3.3. Adquisición de evidencias no volátiles . . . . .	9
2.4. Preservación de la integridad e identidad de las evidencias . . . . .	9
2.5. Normativa ISO/IEC 27037 . . . . .	11
2.5.1. Adquisición . . . . .	11
2.5.2. Adquisición de evidencias en dispositivos encendidos . . . . .	11
2.5.3. Adquisición de evidencias en dispositivos apagados . . . . .	11
2.5.4. Adquisición de evidencias en dispositivos críticos . . . . .	12
2.5.5. Adquisición parcial de evidencias . . . . .	12
2.5.6. Adquisición de dispositivos de almacenamiento . . . . .	12
2.5.7. Preservación . . . . .	12
<b>3. La metodología forense informática</b>	<b>13</b>
3.1. Adquisición de pruebas (imaging) . . . . .	14
3.1.1. Asegurar la escena . . . . .	14
3.1.2. Identificación y Recolección de evidencias . . . . .	15
3.1.3. Preservación de evidencias . . . . .	18
3.2. Análisis . . . . .	19
3.2.1. Preparar un entorno de trabajo . . . . .	20
3.2.2. Creación de la línea temporal . . . . .	21
3.2.3. Determinar cómo se actuó . . . . .	22
3.2.4. Identificar a los autores . . . . .	23
3.2.5. Impacto causado . . . . .	23
3.3. Redacción de informes y Presentación . . . . .	24
<b>4. Requisitos de la investigación forense</b>	<b>25</b>
4.1. Aceptabilidad . . . . .	25
4.2. Integridad . . . . .	25

4.3.	Credibilidad . . . . .	25
4.4.	Relación causa-efecto . . . . .	26
4.5.	Carácter repetible . . . . .	26
4.6.	Documentación . . . . .	26
<b>5.</b>	<b>Valoración jurídica de la prueba digital</b>	<b>27</b>
5.1.	Interés legal de la prueba . . . . .	27
5.2.	Prueba física y prueba personal . . . . .	27
5.3.	Cualificación del investigador forense . . . . .	28
5.4.	La adquisición: fase crucial . . . . .	28
<b>6.</b>	<b>Más información</b>	<b>29</b>
6.1.	Webgrafía . . . . .	29
6.1.1.	<b>SANS: Evidence acquisition</b> . . . . .	29
6.1.2.	Básica . . . . .	29
6.1.3.	Avanzada . . . . .	30
6.1.4.	Referencias . . . . .	31

# CAPÍTULO 1

---

## Objetivos del tema

---

Para estudiar este tema lee los siguientes documentos, además de las Ideas clave:

- El artículo [Best Practices In Digital Evidence Collection](#), publicado por **Sans**.
- Otro artículo que habría que leer, es el titulado como [Collect evidence from a running computer](#), publicado por **Search-**
- El documento titulado [Forensic Images: For Your Viewing Pleasure](#) explica los conceptos básicos sobre qué es una imagen o un clonado, sus diferencias y los tipos de formatos que se utilizan.
- La [Normativa ISO/IEC 27037](#). Directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas.
- Para quién quiera comprender la base matemática de las funciones Hash, es recomendable la lectura del artículo [On the Use of Hash Functions in Computer Forensics](#), publicado por CASED. En este texto se comenta sobre el uso de las funciones **hash** en el ámbito de la informática forense.

En este tercer tema de la asignatura vamos a hablar de evidencias, qué tipos de evidencias existen, cómo adquirirlas y cómo preservarlas. Las evidencias son la parte fundamental de un análisis forense, pues sin ellas el resto del estudio no se podría realizar. Es por ello, que durante el tratamiento de las mismas debemos de tener un especial cuidado.

---

**Importante:** Los objetivos de este tema son:

- Conocer los tipos de evidencias que existen.
- Saber discernir qué evidencias son de importancia para la investigación y cuáles no lo son.
- Saber cómo adquirir evidencias.
- Conocer la importancia de tratar las evidencias con minuciosidad, asegurando su integridad y preservación.

- Establecer una metodología de análisis forense de dispositivos informáticos.
-

# CAPÍTULO 2

---

## La evidencia digital

---

### 2.1 *Tipos de evidencias y orden de volatilidad*

---

**Importante:** Las evidencias digitales se pueden englobar dentro de dos grandes grupos:

- **Evidencias volátiles:** Son aquellas que cambian con facilidad como pueden ser las memorias caché, tablas de enrutamiento, los procesos que están en ejecución o la memoria RAM, entre otros. Este tipo de evidencias son las que primeramente tendremos que adquirir puesto que nuestras acciones pueden modificar su valor original y desaparecen al apagar el equipo.
  - **Evidencias no volátiles:** Como su mismo nombre indica, no cambian con tanta facilidad , aunque por supuesto nuestras acciones pueden alterar su valor si no actuamos con cuidado. Dentro de este tipo de evidencias se engloban los discos duros, pendrives, CDs, etc.
- 

El orden de volatilidad (de mayor a menor) de las evidencias digitales es (Henry 2009):

1. La caché de la CPU (no lo vamos a poder capturar).
  2. La tabla de enrutamiento, la caché ARP, la lista de usuarios que han iniciado sesión en el equipo, la lista de procesos y en general cualquier otra evidencia volátil que pueda desaparecer al apagar el equipo.
  3. La memoria RAM.
  4. Los archivos temporales y el espacio de intercambio.
  5. Los datos del disco duro.
  6. Datos almacenados remotamente.
  7. Datos almacenados en dispositivos removibles. Basándonos en los tipos de evidencias antes descritos y en el orden de volatilidad de las mismas, el **procedimiento**
-

**de adquisición** de las evidencias sería (Henry 2009):

8. Fotografiar la pantalla del equipo (si se encuentra encendida).
9. Capturar la memoria RAM y cualquier otra información volátil que necesitemos (procesos en ejecución, usuarios que han iniciado sesión en el equipo, etc.).
10. Si el disco duro se encuentra encriptado, o suponemos que puede estarlo, realizar una adquisición en caliente del mismo.
11. Desconectar el equipo tirando del cable de alimentación. Si es un portátil, además se quita la batería. Con este tipo de apagado evitamos el que se ejecute algún programa preparado para lanzarse antes de apagar el equipo.
12. Recoger el resto de evidencias que se encuentren en la escena (dispositivos removibles, CDs, etc.) y llevarnos el equipo.

Por supuesto, si el equipo se encontrara apagado, solo realizaríamos el paso número cinco de los descritos anteriormente.

## *2.2 Acotando la escena del crimen*

Qué pasaría si lo que tenemos que analizar es el servidor de la empresa, un ordenador que gestiona una cadena de suministro o cualquier otro sistema crítico para la empresa. ¿Qué hacemos?

En estos casos no queda más remedio que **acotar** la escena del crimen. Para ello debemos de tener en cuenta:

1. ¿Qué equipos han sufrido de manera directa el incidente?
2. ¿Qué otros equipos que sin haber sufrido el incidente pueden estar **relacionados** con el mismo?

Una vez tengamos la respuesta a las anteriores preguntas podremos plantearnos si es viable una adquisición en caliente de las evidencias, si tenemos que realizar análisis en caliente de las mismas o si es posible llevarnos las evidencias y analizarlas en el laboratorio.

Así, por ejemplo, si nos encontramos con algún equipo crítico, es decir, equipos que son elementales para el funcionamiento de la empresa y que no pueden ser retirados ni apagados, será necesario realizar una adquisición «en caliente» del mismo y, por norma general, contar con el asesoramiento del personal técnico de la empresa.

Para qué llevarme esto...



... Si solo necesito esto..



## 2.3 Adquisición de evidencias

En los apartados anteriores hemos visto cuál es el orden de volatilidad de las evidencias digitales, el orden en que estas tienen que ser adquiridas y la necesidad de acortar la escena del crimen. En este apartado vamos a ver, de manera práctica, cómo se realiza dicha adquisición.

Pero antes de comenzar, es posible que os preguntéis: ¿qué es adquirir una evidencia? y ¿para qué las adquirimos?

**Adquirir** una evidencia es sencillamente **crear un archivo (o un clon)** que contenga **toda la información** contenida en la evidencia **original**. Incluidos los espacios marcados como vacíos o libres (si estamos hablando de dispositivos como un disco duro o un *pendrive* ).

Esta copia se puede obtener en dos formatos diferentes: la **imagen forense** y el **clonado forense**. Los términos imagen y clonado **no son sinónimos**.

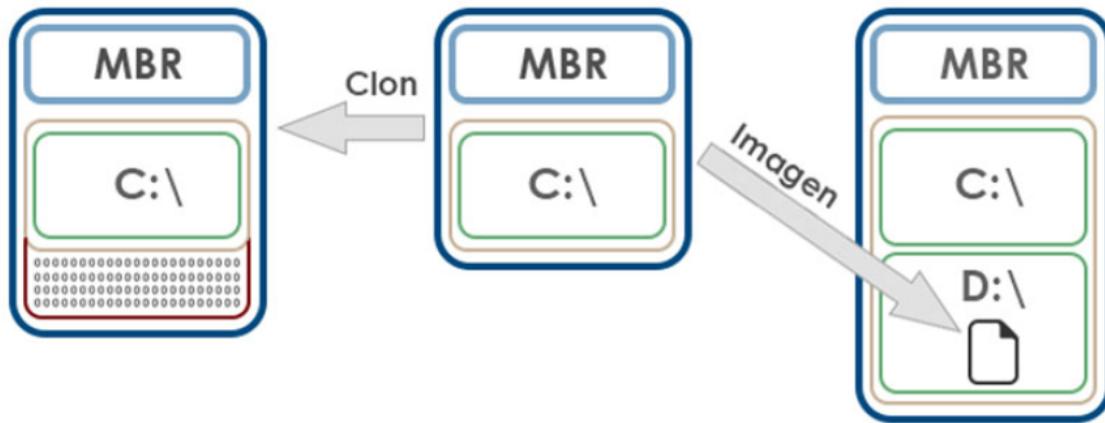
---

### Importante:

- **Imagen forense:** Es una copia exacta de un dispositivo físico (que puede ser un pendrive, un disco duro, un CD, etc.) que es almacenada en un archivo, el cual puede ser guardado en cualquier tipo de dispositivo capaz de almacenar archivos.
- **Clonado forense:** Es una copia «bit a bit» de un dispositivo físico en otro dispositivo físico similar (un disco duro en otro disco duro, un pendrive en otro pendrive,

etc.). De esta forma, el dispositivo original y el dispositivo clonado son idénticos en cuanto a contenido.

---



A modo de comparativa, las características propias de una imagen forense y un clonado son:

Tabla 1: Comparativa Imagen forense vs Clonado.

Imagen forense Clonado	Clonado
La copia del dispositivo origen es almacenada en un archivo.	El dispositivo destino debe ser del mismo tamaño o mayor que el dispositivo origen.
Pueden almacenarse en un único dispositivo de almacenamiento destino, archivos de imagen correspondientes a la copia de varios dispositivos de almacenamiento origen.	En un dispositivo clon, la información es almacenada exactamente igual que en el dispositivo origen.
Es necesario el uso de software específico para visualizar el contenido de la imagen generada.	Cada dispositivo destino solo puede ser el clon de un único dispositivo origen.
	No es necesario el uso de ningún software específico para visualizar el contenido del dispositivo clon.

Cuando se realiza un clonado, hay que tener en cuenta que el dispositivo destino debe tener una capacidad de almacenamiento igual o mayor al dispositivo origen y que previamente, al dispositivo destino se le debe de haber realizado un borrado seguro.

---

**Importante: Borrado seguro:** Es un método de borrado que sobrescribe la información original de forma que esta no pueda ser recuperada. El método más común consiste en la sobrescritura de la información original con ceros, aunque también es posible sobrescribirla con cualquier otro valor o valores.

---

Normalmente, el proceso más recomendado es el de creación de una imagen forense. Un archivo que almacene la copia del dispositivo físico de origen.

El motivo por el que utilizamos una imagen forense en lugar de un clon es que se trabaja de manera más sencilla con un archivo que con un disco duro físico. El archivo puede ser

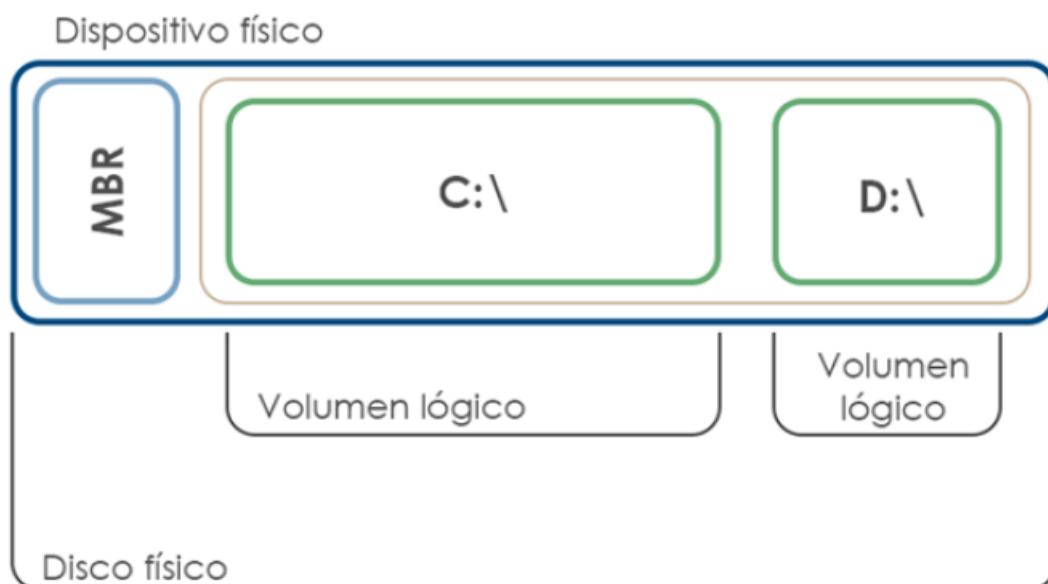
utilizado por varios analistas a la vez, puede ser fácilmente copiado y enviado, contener información adicional de la evidencia, podemos marcar archivos de interés dentro de la evidencia y esa información se queda almacenada en el propio archivo de la evidencia, etc.

Los tipos de archivos de evidencia más comunes son:

- **EnCase image file format (\*.Exx):** De la suite de análisis forense EnCase.
- **Advanced Forensics Format (\*.AFF):** Un formato abierto de evidencias forenses.
- **RAW (\*.\*):** Un formato en el que la información de la evidencia se almacena tal cual está en la propia evidencia original, sin compresión ni metadatos (como si tienen los anteriores formatos).

### 2.3.1 Diferencias entre una adquisición física y una adquisición lógica

La siguiente imagen representa de manera esquemática la información de un disco duro con un esquema de particionado MBR:



En esta representación se puede observar que el dispositivo contiene un MBR (Master Boot Record) con la tabla de particiones y dos particiones: C y D.

Cuando toda la información contenida en el disco se copia exactamente igual del origen al destino (ya sea el destino otro disco duro, o un archivo de imagen forense), decimos que hemos realizado una **adquisición física del dispositivo**.

En la representación anterior, la adquisición física incluiría el MBR y las dos particiones. Incluyendo los sectores del disco que no se encontraran en uso o partes del disco que directamente no pertenezcan a ninguna partición (espacio sin particionar).

Por otro lado, cuando la copia realizada se limita a un volumen (C: o D: en la representación anterior), o a una parte del mismo como puede ser un conjunto de archivos o carpetas, o a una base de datos concreta del dispositivo, decimos que hemos realizado una adquisición lógica de la información del dispositivo.

En la presentación anterior, si únicamente adquirimos el volumen lógico «C», estaríamos realizando una adquisición lógica, ya que no nos llevamos el espacio sin particionar, ni el

MBR, ni tampoco, el segundo volumen lógico.

### 2.3.2 Adquisición de evidencias volátiles

Las evidencias volátiles, como la memoria RAM, tendremos que **adquirirlas en caliente**, esto es, con el **equipo** a examinar **encendido** (pues como ya se ha dicho, estas evidencias desaparecen al apagar el equipo). El principal problema de este tipo de adquisición, es que las evidencias del equipo se degradan, pudiendo incluso llegar a perderse evidencias si no tenemos cuidado con nuestras acciones.

La **primera evidencia** que hay que adquirir es la memoria **RAM**. La memoria **RAM** es un tipo de memoria donde el ordenador almacena los **datos** que están siendo **usados** en un **determinado momento**. Así pues, **cualquier programa** que ejecutamos en nuestro equipo ha de **ubicarse primeramente** en la memoria RAM.

Para adquirir la memoria RAM, haremos uso de programas preparados a tal efecto como *DumpIt* (para sistemas operativos Windows). El problema que existe a la hora de adquirir la memoria RAM, es que como acabamos de comentar el propio **programa** que **utilicemos** para adquirir la memoria RAM va a tener que cargarse en dicha memoria, **alterando** parte de ella. Este tipo de modificación es inevitable.

Del análisis de la memoria RAM se puede obtener:

1. Contraseñas de acceso (en claro o el hash de las mismas)
2. Documentos abiertos por el usuario, aunque no se hubieran guardado
3. **Imágenes** que se estuvieran visualizando
4. Programas en ejecución (es posible extraer un ejecutable completo de la captura de la memoria RAM)
5. Etcétera

Al igual que es posible la captura de la memoria RAM, también se pueden capturar otro tipo de evidencias volátiles como la **lista de procesos en ejecución**, **lista de usuarios** que han iniciado sesión en el equipo, etc.

Para la adquisición de este tipo de evidencias haremos uso de programas específicos en función de lo que se pretenda adquirir, como *Process Monitor* para la obtención de la lista de procesos y subprocesos en ejecución o *FileMon* que muestra la actividad del sistema de archivos en tiempo real, ambas pertenecientes al conjunto de herramientas denominado *Windows Sysinternals* (<http://technet.microsoft.com/es-es/sysinternals>).

---

**Importante:** Eso sí, teniendo siempre en cuenta que los **programas** que **utilicemos** deben ser **independientes** del **equipo** a examinar (no utilizaremos un programa que tenga instalado el propio equipo). Esto es así, porque dichos programas pueden haber sido alterados de manera que dificulten o directamente impidan el realizar nuestra labor.

---

### 2.3.3 Adquisición de evidencias no volátiles

Al contrario que las evidencias volátiles, las no volátiles podemos adquirirlas tanto en **frío** , con el equipo apagado, como en **caliente** , con el equipo en funcionamiento. El que nos **decantemos** por una forma u otra de adquisición dependerá de varios **factores**.

Entre los factores más importantes a la hora de decantarnos por una adquisición en caliente o en frío tenemos:

- Que el equipo pertenezca o no a un sistema crítico que tenga que mantenerse encendido de manera ininterrumpida.
- Que el dispositivo que pretendemos adquirir se encuentre o no cifrado. Si lo está puede ser imposible realizar la adquisición en frío.
- Que el equipo se encuentre expuesto a ataques desde el exterior, lo que puede hacer que las evidencias se alteren durante una adquisición en caliente.
- Etcétera.

Para la adquisición de evidencias no volátiles en caliente utilizaremos programas como *AccessData FTK Imager* , que permiten la adquisición física de los dispositivos conectados al equipo.

Durante una adquisición en caliente, todos los pasos que se realicen sobre el equipo objeto del análisis deben estar concienzudamente documentados con el fin de diferenciar las modificaciones realizadas por nosotros, de las realizadas por un tercero.

Para la adquisición de evidencias no volátiles en frío podemos utilizar los mismos programas que para la adquisición en caliente, como *AccessData FTK Imager* , teniendo además una especial precaución en que los dispositivos que pretendamos adquirir se encuentren conectados como solo lectura, para evitar que podamos alterar su contenido.

Así pues, al conectar a nuestro equipo de análisis el disco duro que pretendamos adquirir, tenemos que asegurarnos la no escritura en el mismo utilizando *hardware* como *Forensics Ultradock* , software como *FastBloc SE* o directamente montando el dispositivo como solo lectura (para sistemas operativos Linux o Mac OS).

## 2.4 Preservación de la integridad e identidad de las evidencias

Como se ha comentado anteriormente, a la hora de realizar una adquisición en frío (en caliente esto no es posible) debemos de **proteger contra escritura el dispositivo** que se pretende adquirir con el fin de evitar la modificación del mismo.

Este aspecto, que si bien es de suma importancia a la hora de conseguir que las evidencias adquiridas tengan validez en un proceso judicial, no es el único que debemos de llevar a cabo, ya que aunque garantiza la no alteración de la evidencia original, no nos asegura que lo que estemos analizando sea exactamente lo mismo que lo contenido en la evidencia original.

Para **verificar** que lo **analizado** es una **copia** exacta de la evidencia **original** , o que la **integridad** de dicha copia se mantiene a lo **largo** de todo el **proceso** de análisis hacemos

uso de las conocidas como funciones **hash**.

Una función **hash** es un tipo de función que debe reunir como mínimo las siguientes dos características:

- Para cada entrada «E», la función generará siempre una salida «S» única. Lo que implica que cualquiera alteración en la entrada , por mínima que sea, alterará la salida.
- A partir de la salida «S» de la función, es imposible obtener la entrada original «E».

El proceso de la adquisición de una evidencia queda entonces de la siguiente manera:



Para concluir que no hemos alterado la evidencia original y que la copia realizada es exacta, el **primer \*hash\*** a la evidencia **original** (HA1) ha de ser **igual** al **segundo hash** a la evidencia original (HA2) e **igual** al **hash** de la **copia** (HB).

Además, para verificar en cualquier momento del análisis que lo que se está analizando es lo mismo que se obtuvo de la evidencia original, solo tenemos que realizar nuevamente un *hash* a la evidencia objeto del análisis y compararlo con el primer *hash* de la evidencia original (HA1). Si son idénticos estamos analizando una copia exacta de la evidencia original, mientras que si son distintos, la evidencia que estamos analizando ha sido alterada.

Este proceso de preservación de la integridad e identidad de las evidencias, programas como las suite forenses *EnCase* o *Forensic ToolKit* , lo realizan de manera transparente al analista, mostrando una advertencia en el caso de que dichos valores no coincida.

Ahora bien, el proceso de preservación de la integridad de las evidencias **varía** cuando realizamos adquisiciones «en caliente». El problema de este tipo de adquisiciones es que, en la mayoría de los casos, **no** es posible **bloquear** contra **escritura** el origen (por ejemplo, la memoria RAM), por lo que el hacer un Hash a la evidencia original carecería de sentido.

El proceso de adquisición y preservación de la integridad cuando se realiza una adquisición en caliente sería: **Adquisición** de la evidencia y **hash** al resultado de la adquisición. **No** realizamos el **hash** a la evidencia **original**.



Al igual que en frío, para verificar en cualquier momento del análisis que lo que se está analizando es lo mismo que se adquirió inicialmente, solo tenemos que realizar nuevamente un hash a la copia y compararlo con el primer hash de la misma (HB). Si son idénticos estamos analizando una copia exacta de lo adquirido, mientras que, si son distintos, la copia que estamos analizando ha sido alterada.

## 2.5 Normativa ISO/IEC 27037

### 2.5.1 Adquisición

La **normativa ISO/IEC 27037** divide el procedimiento de adquisición de evidencias en: Adquisición de evidencias en dispositivos encendidos, en dispositivos apagados, en dispositivos críticos, adquisiciones parciales y adquisiciones de dispositivos de almacenamiento.

### 2.5.2 Adquisición de evidencias en dispositivos encendidos

Para la adquisición de evidencias en equipos encendidos el primer paso que propone es la **verificación de si el dispositivo se encuentra encriptado** o no.

En el caso de encontrarnos con un dispositivo encriptado, como puede ser el disco duro de un equipo, debemos realizar la **adquisición en caliente** de dicho dispositivo, puesto que es posible que no seamos capaces de desencriptar dicho dispositivo si se apaga el equipo.

Si no se encuentra encriptado, o si ya hemos realizado la adquisición del dispositivo cifrado, el siguiente paso es verificar si dicho dispositivo contiene **información volátil** que debamos adquirir. Como, por ejemplo, la memoria RAM.

Si contiene información volátil que sea necesaria adquirir, se realizará la adquisición en caliente de la misma. En caso contrario, o, una vez adquirida la información volátil, el siguiente paso consistirá en comprobar si existe **información no volátil** que debamos adquirir.

Si existe información no volátil que debamos adquirir y el dispositivo no puede ser apagado, realizaremos una adquisición en caliente de esa información no volátil. En el caso de que el dispositivo pueda ser apagado, se realizará un apagado del mismo y se procederá a la adquisición de la información no volátil mediante la conexión del dispositivo que la contenga a un **bloqueador contra escritura** para evitar su modificación durante la adquisición.

Una vez adquirida la información volátil y la no volátil, se puede dar por concluido el proceso de adquisición.

### 2.5.3 Adquisición de evidencias en dispositivos apagados

La adquisición de evidencias en equipos apagados es bastante más sencilla que en dispositivos encendidos, aunque también **permite obtener menor cantidad de información**, ya que las evidencias volátiles que pudieramos encontrar en el equipo, se han perdido.

El proceso de adquisición consiste en la extracción del dispositivo de almacenamiento, la conexión, si es posible, del mismo a un bloqueador contra escritura y la adquisición de la información contenida en el dispositivo.

#### *2.5.4 Adquisición de evidencias en dispositivos críticos*

En ocasiones es posible encontrarse con dispositivos críticos para el funcionamiento de una empresa u organización, como pueden ser los servidores de bancos o los equipos médicos.

En estos casos, y siempre que sea posible y/o necesario, se solicitará la **ayuda del personal técnico encargado de la gestión de dichos dispositivos** y se procederá de manera similar a una adquisición de evidencias en dispositivos encendidos o a una adquisición parcial de evidencias.

#### *2.5.5 Adquisición parcial de evidencias*

En determinadas ocasiones no será posible la adquisición total de las evidencias. Por ejemplo, cuando la información a adquirir es muy grande, cuando únicamente sea de interés para el estudio una parte de la información o cuando legalmente no tengamos más autoridad.

En las **adquisiciones parciales** se actuará siguiendo los procedimientos indicados en las adquisiciones de dispositivos encendidos o las adquisiciones de dispositivos apagados, según sea el caso. La diferencia con este tipo de adquisiciones radica en que primeramente será necesaria la **identificación de la parte de interés para el análisis**, carpetas, archivos o bases de datos sobre las que va a versar el posterior estudio.

Una vez identificada la parte de interés se procederá a la adquisición lógica de la información.

#### *2.5.6 Adquisición de dispositivos de almacenamiento*

Es posible encontrar diversos tipos de dispositivos de almacenamiento en la escena de un incidente. Por norma general, estos serán los **dispositivos menos volátiles**, por lo tanto, serán los últimos en ser adquiridos, lo que no indica que sean los menos importantes a la hora del estudio.

El proceso de adquisición de este tipo de dispositivos consiste en la conexión, si es posible, del mismo a un bloqueador contra escritura y la adquisición de la información contenida.

#### *2.5.7 Preservación*

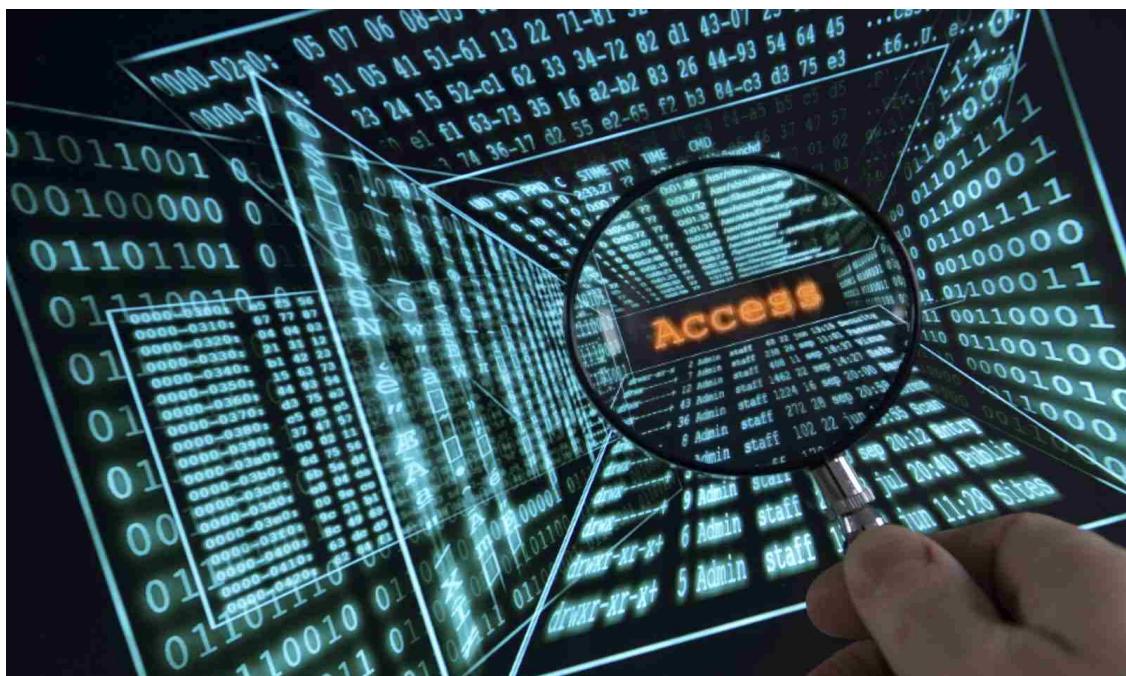
Una vez completado el proceso de adquisición debe realizarse la **verificación de las firmas digitales** de las evidencias adquiridas para comprobar que lo adquirido es copia fiel de la evidencia original.

En ocasiones, dada la relevancia de las evidencias, es posible que sea necesario asociar al personal que ha realizado la adquisición con la evidencia adquirida. Ya sea mediante la firma digital del archivo de evidencia o procedimientos biométricos o fotográficos.

Todas las evidencias recolectadas deben ser adecuadamente preservadas. Distintos tipos de dispositivos requieren distintos **métodos de preservación**, puesto que el objetivo es el mantenimiento a largo plazo de las evidencias.

# CAPÍTULO 3

## La metodología forense informática



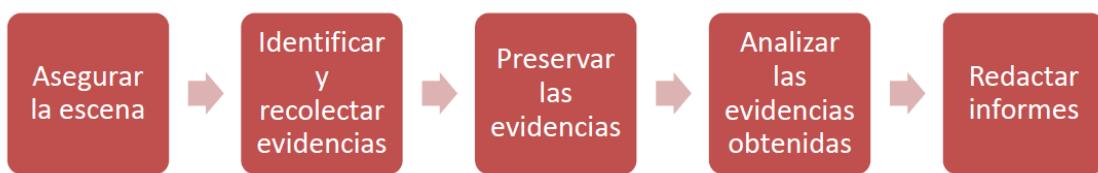
Con el análisis realizado sobre las normas y estándares que existen tanto a nivel nacional como internacional se ha podido ver que hay un conjunto de puntos importantes a tener en cuenta para realizar un análisis forense exitosamente. Por ejemplo, la mayoría recalcan la importancia de preservar el entorno de pruebas, no modificando el escenario encontrado.

También aluden a la importancia de cómo se guardan las pruebas, su transporte, conservación, etcétera. Posteriormente se centran en cómo analizar las pruebas para obtener el máximo rendimiento de las mismas y poder esclarecer al máximo los hechos ocurridos. Finalmente, la importancia de unos buenos informes que sean claros, concisos y que sirvan, por ejemplo en caso de juicio, para que una persona no entendida en el tema sea capaz de comprender lo ocurrido y lo que le queremos transmitir sin influir en una posterior decisión.

Así pues, atendiendo a estas recomendaciones y consejos, más o menos extendidos en toda

la literatura sobre este asunto, parece oportuno dividir en distintas fases la metodología para un análisis forense exitoso. Esta será la estructura del presente capítulo. Se analizarán las siguientes fases:

1. Asegurar la escena.
2. Identificar y recolectar las evidencias.
3. Preservar las evidencias.
4. Analizar las evidencias obtenidas.
5. Redactar informes sobre los resultados.



### 3.1 Adquisición de pruebas (imaging).

#### 3.1.1 Asegurar la escena.

A grandes rasgos en esta etapa deberíamos realizar las siguientes acciones básicas:

- a) Es recomendable **realizar fotografías del entorno del equipo** para evidenciar el estado original de la escena, identificando así el perímetro de la escena a analizar y protegiéndolo de accesos de personal no autorizado.
- b) Una vez dentro del perímetro de seguridad cabe destacar que hay que **proteger las huellas dactilares** que pueda haber en los equipos para que los demás cuerpos y unidades de policía e investigadores puedan realizar su tarea. Es por lo tanto recomendable el uso de **guantes de látex o similar** para esta finalidad.
- c) Hay que anotar la **hora y fecha de los equipos implicados** que no tiene por qué coincidir con la real, esto es importante para la investigación posterior y para la **realización de una línea temporal** con todos los sucesos que han ocurrido. En caso de haber desfase entre la hora del equipo y la real, este desfase se tiene que documentar para tenerlo en cuenta posteriormente. La captura de la hora y fecha se puede realizar fotografiando la pantalla o grabando un vídeo de la misma, siempre y cuando no haya que manipular el equipo para ello.
- d) Debemos **ver si en pantalla hay algún proceso** que nos aporte información útil sobre lo que esté pasando en directo, en ese caso, grabar todo lo que ocurre. Es importante valorar las entradas y salidas de los equipos, pues nos pueden aportar pistas importantes. De igual modo con otros periféricos de entrada/salida, tales como impresoras, teléfonos IP, escáneres, etcétera.
- e) Llegados a este punto hay que centrarse en la desconexión de los equipos tanto de la red como de la alimentación eléctrica. Estas desconexiones pueden alterar la investigación y por lo tanto debe documentarse exactamente lo que se ha realizado y lo que lo ha motivado.

- **Desconexión de red:** si se realiza, podemos lograr que un determinado hecho siga realizándose, por ejemplo una descarga de datos no autorizada o el borrado remoto de datos que podrían dificultar el análisis. En cambio, perderemos información sobre posibles conexiones que nos den el origen del incidente o valiosos indicios.
- **Desconexión de la corriente eléctrica:** habrá que valorar qué repercusiones tendrá la desconexión del fluido eléctrico. Una desconexión evitará que algún proceso siga escribiendo en disco o incluso eliminando datos, aunque también podría provocar alguna escritura de datos en disco si el equipo tiene alguna configuración programada para fallos eléctricos. También se podría haber planificado un borrado de datos en caso de desconexión del equipo y entonces se perdería parte o toda la información del equipo dando al traste con la investigación. Así, habrá que ser muy cuidadoso con este punto y valorar qué opción nos es más útil en cada caso, no todas las investigaciones que se hagan se resolverán del mismo modo.

Una vez finalizada la primera fase, y con la escena bien asegurada teniendo en cuenta todos los puntos expuestos anteriormente, se podrá pasar a la segunda fase de la metodología. A continuación nos enfrentaremos a la identificación y recolección de pruebas.

### *3.1.2 Identificación y Recolección de evidencias.*

- a) Llegados a este punto hay que tener en cuenta una serie de principios acerca de la identificación de las evidencias y más específicamente sobre la volatilidad de las mismas. **Es vital conocer qué datos son más o menos volátiles**, identificarlos correctamente y posteriormente proceder a su recolección.

**Entendemos por volatilidad de los datos el período de tiempo en el que estarán accesibles en el equipo.** Por lo tanto, se deberán recolectar previamente aquellas pruebas más volátiles. Según la RFC 3227, el que se presenta a continuación, es un posible orden de volatilidad de mayor a menor:

Registros y contenidos de la memoria caché del equipo

Tablas de enrutamiento de redes, caché ARP, tabla de procesos, estadísticas del kernel y memoria

Información temporal del sistema

Datos contenidos en disco

Logs del sistema

Configuración física y topología de la red donde se encuentra el equipo.

Documentos

- b) Se deberán **listar los equipos y sus características** que estén implicados en los hechos. Así mismo también se deberá hacer un listado con las personas implicadas en los equipos. Será útil recoger su nombre, identificación, contraseñas de los sistemas y acciones que hayan realizado desde el conocimiento del incidente, entre otras.



- c) Será útil, en caso de varios **equipos conectados en red, dibujar la estructura de la misma**, es decir, su topología, con la identificación de cada equipo en ella. Además también es importante identificar todos los cables y los puertos donde están conectados los distintos periféricos del equipo para poder realizar una posterior conexión en laboratorio en caso de ser necesario.

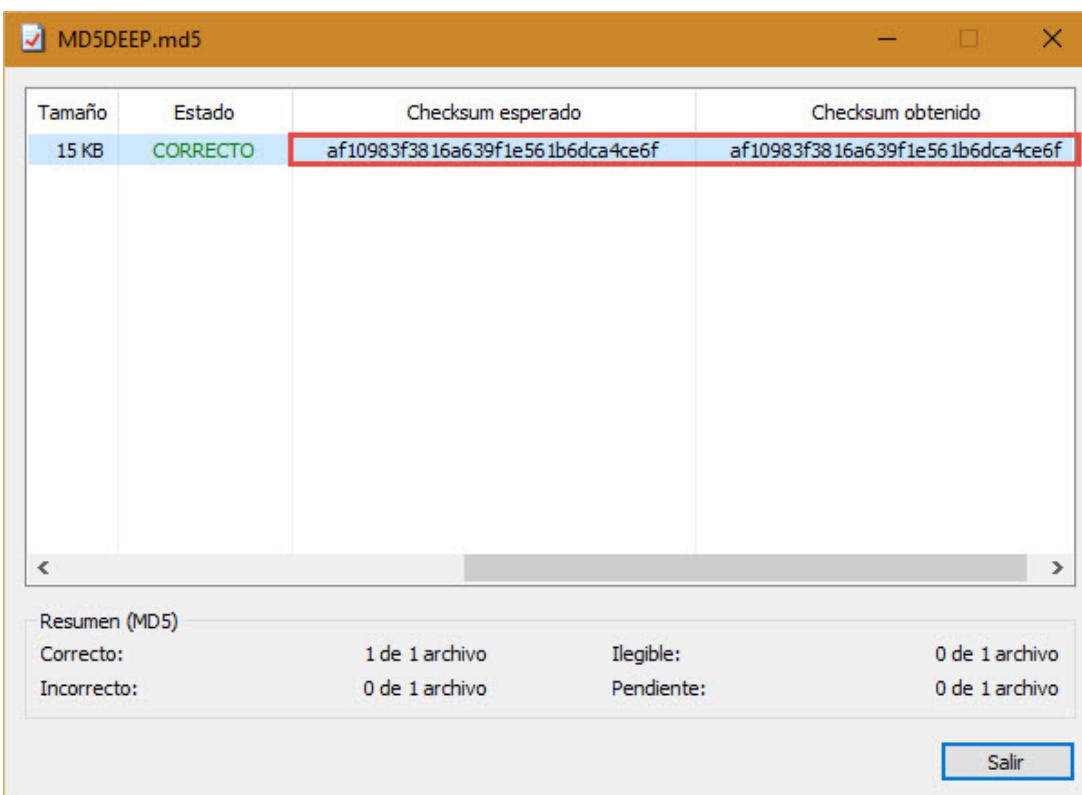
- d) **Los discos duros también deben ser identificados correctamente**, pues conforman el núcleo duro, en la mayoría de los casos, de nuestra investigación. Esto incluye anotar

marca y modelo, número de serie, capacidad, posición de los jumpers y documento gráfico que lo pruebe. Lo mismo ocurre con los discos ópticos y sus unidades lectoras, como DVD, CD, etcétera.

e) Finalmente, y no menos importante, hay que recalcar el considerar las **pautas de la empresa en cuanto a privacidad**. Se suele solicitar autorización por escrito para efectuar la recolección de evidencias. Esto es muy importante ya que en ocasiones se pueden manejar datos confidenciales o incluso que la disponibilidad de los servicios quede afectada. Además, a menos que haya indicios suficientes y fundamentados no se deben recopilar datos de lugares a los que no se accede normalmente, como por ejemplo ficheros con datos personales.

Tras la correcta identificación de las evidencias se puede proceder a su recolección, para ello se pueden seguir los siguientes pasos:

- Copia bit a bit de los discos que se quieran analizar**, es decir, se requiere una copia exacta del contenido de los discos incautados. Esto incluye todos los archivos del disco, por ejemplo los temporales, los ocultos, los de configuración, los eliminados y no sobrescritos y la información relativa a la parte del disco no asignada, es lo que se conoce como copia a bajo nivel. Esta copia se llevará a cabo sobre un soporte limpio mediante un borrado seguro de los datos que pudiera contener anteriormente para evitar así contaminaciones con otros casos.
- Una vez realizada la copia se debe **verificar la integridad** de la misma. **Para ello se calcula el hash o CRC de la copia**, normalmente los equipos destinados al clonado de discos ya incorporan esa característica. Así con el hash del disco original y el de la copia se puede certificar que ambos son idénticos a todos los niveles y ante un juez, por ejemplo, quedará probado que no se ha manipulado de ningún modo. Con este procedimiento también nos aseguraremos que no se han producido errores en la copia.



The screenshot shows a software window titled "MD5DEEP.md5". It displays a table comparing checksums for a single file. The table has four columns: "Tamaño" (Size), "Estado" (State), "Checksum esperado" (Expected Checksum), and "Checksum obtenido" (Obtained Checksum). The first row shows a file size of 15 KB, a state of "CORRECTO" (Correct), an expected checksum of "af10983f3816a639f1e561b6dca4ce6f", and an obtained checksum of "af10983f3816a639f1e561b6dca4ce6f". A red border highlights the expected and obtained checksum columns. Below the table, a summary section titled "Resumen (MD5)" provides a breakdown of file status: 1 de 1 archivo (Correcto) and 0 de 1 archivo (Incorrecto, Illegible, Pendiente). A "Salir" (Exit) button is visible at the bottom right.

Tamaño	Estado	Checksum esperado	Checksum obtenido
15 KB	CORRECTO	af10983f3816a639f1e561b6dca4ce6f	af10983f3816a639f1e561b6dca4ce6f

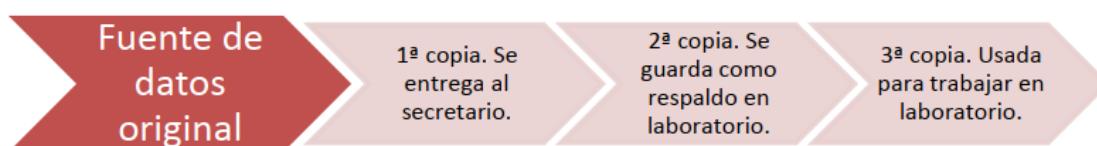
Resumen (MD5)

Correcto:	1 de 1 archivo	Illegible:	0 de 1 archivo
Incorrecto:	0 de 1 archivo	Pendiente:	0 de 1 archivo

[Salir](#)

Cálculo de la función HASH de un archivo con la herramienta HashCheck para Windows.

- c) **Con la primera copia realizada y comprobada procedemos a realizar una segunda copia sobre la primera.** En este caso también se comprobará que el contenido es idéntico mediante el mismo proceso descrito anteriormente. Teniendo ambas copias entregaremos la primera al secretario judicial o notario responsable del caso y nos quedaremos con la segunda para poder trabajar. La segunda copia será nuestra copia de respaldo en todo momento en el laboratorio y no será para trabajar directamente con ella en ningún caso.
- d) Para realizar el análisis se deberá realizar una tercera copia, comprobar su integridad y trabajar sobre ella, de tal modo que en caso de cualquier desastre o alteración de los datos siempre tengamos la segunda copia exacta al original de donde poder volver a realizar otra copia para analizar.



### 3.1.3 Preservación de evidencias.

Una mala preservación de las evidencias, un mal uso o una mala manipulación pueden **invalidar toda la investigación** que se lleva a cabo delante de un tribunal, este es un factor muy importante que se va repitiendo a lo largo de toda la metodología.

**La cadena de custodia** es el procedimiento controlado aplicable a las evidencias relacionadas con el suceso, desde el momento en que se encuentran en la escena hasta su análisis en el laboratorio. La finalidad de la cadena de custodia es evitar cualquier tipo de manipulación y tener un control absoluto sobre todos los elementos incautados, quién los ha manipulado, cómo lo ha realizado, por qué los ha manipulado, para qué lo ha hecho y cuándo ha tenido lugar dicha manipulación.

Es importante realizar todas las anotaciones descritas en la fase de identificación de las evidencias para que esta fase sea aún más sólida. Con todos los elementos documentados será mucho más fácil tener un control de todas las evidencias que disponemos y poder realizar una traza de todas las pruebas adquiridas.

Mientras los dispositivos estén en el laboratorio y no se estén manipulando es importante tenerlos embalados con etiquetas informativas que contengan al menos datos como un identificador único para cada elemento, nombre del técnico responsable del material, la descripción del mismo. También es relevante el propietario del mismo y en qué lugar fue confiscado, así como fecha y hora del evento. Finalmente se podrán anotar otras observaciones que puedan resultar útiles para los investigadores y que aporten cualquier otro dato.

En función de la naturaleza de los equipos confiscados habrá que tomar una serie de cuidados adicionales. En caso de discos ópticos o magnéticos, por ejemplo discos duros, CD, cintas de copias de seguridad o similares, estos se deberán proteger contra electricidad

estática y se guardarán en bolsas antiestáticas para evitar pérdida o daño en los datos contenidos. Se procederá de la misma forma con placas electrónicas que pudieren verse afectadas por descargas de electricidad estática o sean sensibles a la manipulación.

Además se tendrá en cuenta de proteger los bienes para el transporte desde el lugar de los hechos hasta el laboratorio con los medios necesarios para evitar golpes o proteger de caídas fortuitas.

El lugar de almacenamiento también debe reunir unas mínimas condiciones de seguridad, no sólo de acceso físico a las evidencias, sino también ambientales. No se podrán almacenar dispositivos electrónicos en sitios húmedos o con temperaturas extremas o con exceso de polvo y suciedad.

La documentación de la cadena de custodia deberá contener también todos los lugares por donde ha pasado la evidencia y quién ha realizado su transporte y su acceso.

### 3.2 Análisis.

La fase de análisis no termina hasta que no se puede determinar qué o quién causó el incidente, cómo lo hizo, qué afectación ha tenido en el sistema, etc. Es decir, es el núcleo duro de la investigación y tiene que concluir con el máximo de información posible para poder proceder a elaborar unos informes con todo el suceso bien documentado.

Antes de empezar el análisis, es importante recordar unas premisas básicas que todo investigador debe tener presente en el momento de enfrentarse al incidente. Como ya se ha

explicado nunca se debe trabajar con datos originales y se debe respetar cada una de las leyes vigentes en la jurisdicción donde se lleve a cabo la investigación. Los resultados que se obtengan de todo el proceso han de ser verificables y reproducibles, así que en cualquier

momento debemos poder montar un entorno donde reproducir la investigación y mostrarlo a

quién lo requiera. Es importante también disponer de una documentación adicional con información de diversa índole, por ejemplo:

- Sistema operativo del sistema.
- Programas instalados en el equipo.
- Hardware, accesorios y periféricos que forman parte del sistema.
- Datos relativos a la conectividad del equipo:
  - Si dispone de firewall, ya sea físico o lógico.
  - Si el equipo se encuentra en zonas de red especiales, por ejemplo, DMZ.
  - Si tiene conexión a Internet o utiliza proxies.
- Datos generales de configuración que puedan ser de interés para el investigador para ayudar en la tarea.

Para ayudar al desarrollo de esta fase del análisis forense podemos centrarnos en varias subfases o puntos importantes que generalmente siempre deben realizarse. Cabe recordar que no existe ningún proceso estándar que ayude a la investigación y habrá que estudiar cada caso por separado teniendo en cuenta las diversas particularidades que nos podamos

encontrar. **No será lo mismo analizar un equipo con sistema operativo Windows o con Linux.**

Tampoco será lo mismo un caso de intrusión en el correo electrónico de alguien o un ataque de denegación de servicio a una institución. De igual forma no actuaremos con los mismos pasos en un caso de instalación de un malware que destruya información de una ubicación de disco o un malware que envíe todo lo que se teclea en un equipo.

En todo caso, se pueden destacar varios pasos, que habrá que adaptar en cada caso:

- Preparar un entorno de trabajo adaptado a las necesidades del incidente.
- Reconstruir una línea temporal con los hechos sucedidos.
- Determinar qué procedimiento se llevó a cabo por parte del atacante.
- Identificar el autor o autores de los hechos.
- Evaluar el impacto causado y si es posible la recuperación del sistema.

### *3.2.1 Preparar un entorno de trabajo*

Antes de empezar el análisis propiamente, se debe preparar un entorno para dicho análisis. Es el momento de decidir si se va a hacer un análisis en caliente o en frío.

En caso de un **análisis en caliente** se hará la investigación sobre los discos originales, lo que conlleva ciertos riesgos. Hay que tomar la precaución de poner el disco en modo sólo lectura, esta opción sólo está disponible en sistemas operativos Linux pero no en Windows.

Si se opta por esta opción hay que operar con sumo cuidado pues cualquier error puede ser fatal y dar al traste con todo el proceso, invalidando las pruebas.

Si se opta por un **análisis en frío**, lo más sencillo es **preparar una máquina virtual** con el mismo sistema operativo del equipo afectado y montar una imagen del disco. Para ello, previamente habremos creado la imagen a partir de las copias que se hicieron para el análisis. En este caso podremos trabajar con la imagen, ejecutar archivos y realizar otras tareas sin tanto cuidado, pues siempre cabe la opción de volver a montar la imagen desde cero en caso de problemas.

La opción del análisis en frío resulta muy atractiva pues en caso de malwares se podrán ejecutar sin miedo, reproducir lo que ocurre y desmontar la imagen sin que la copia original resulte afectada. De este modo tal vez se pueda ir un poco más allá en la investigación y ser un poco más agresivo.

Existen varios programas gratuitos para crear y gestionar máquinas virtuales, por ejemplo, Oracle VM VirtualBox, que ofrecen muy buenas prestaciones.

### 3.2.2 Creación de la línea temporal

Sea cual sea el tipo de análisis que se va a llevar a cabo, **el primer paso suele ser crear una línea temporal dónde ubicar los acontecimientos** que han tenido lugar en el equipo desde su primera instalación.

Para crear la línea temporal, **lo más sencillo es referirnos a los tiempos MACD** de los archivos, es decir, las fechas de modificación, acceso, cambio y borrado, en los casos que aplique. Es importante, como ya se ha indicado en alguna ocasión tener en cuenta los husos horarios y que la fecha y hora del sistema no tienen porqué coincidir con los reales. Este dato es muy importante para poder dar crédito a las pruebas y a la investigación en general.

Para empezar, lo mejor es determinar la fecha de instalación del sistema operativo, para ello

se puede buscar en los datos de registro. Además la mayoría de ficheros del sistema compartirán esa fecha. A partir de aquí puede ser interesante ver qué usuarios se crearon al principio, para ver si hay discrepancias o usuarios fuera de lo común en últimos instantes del equipo. Para ver esta información también es útil acudir al registro del sistema operativo.

Teniendo ya los datos iniciales del sistema, ahora se puede proceder a buscar más información en los ficheros que se ven “a simple vista”. Lo importante es localizar qué programas fueron los últimos en ser instalados y qué cambios repercutieron en el sistema.

Lo más habitual es que estos programas no se instalen en los lugares habituales, sino que se localicen en rutas poco habituales, por ejemplo en archivos temporales o mezclados con los archivos y librerías del sistema operativo. Aquí se puede ir creando la línea temporal con esos datos.

Alternativamente es útil pensar que no todos los archivos están a la vista. Se puede encontrar información en archivos normales, pero también en temporales, ocultos, borrados o usando técnicas como la esteganografía, no se puede obviar ninguna posibilidad.

Habitualmente los sistemas operativos ofrecen la opción de visualizar los archivos ocultos y también las extensiones. Es útil activar estas opciones para detectar posibles elementos ocultos y extensiones poco habituales que nos resulten extrañas.

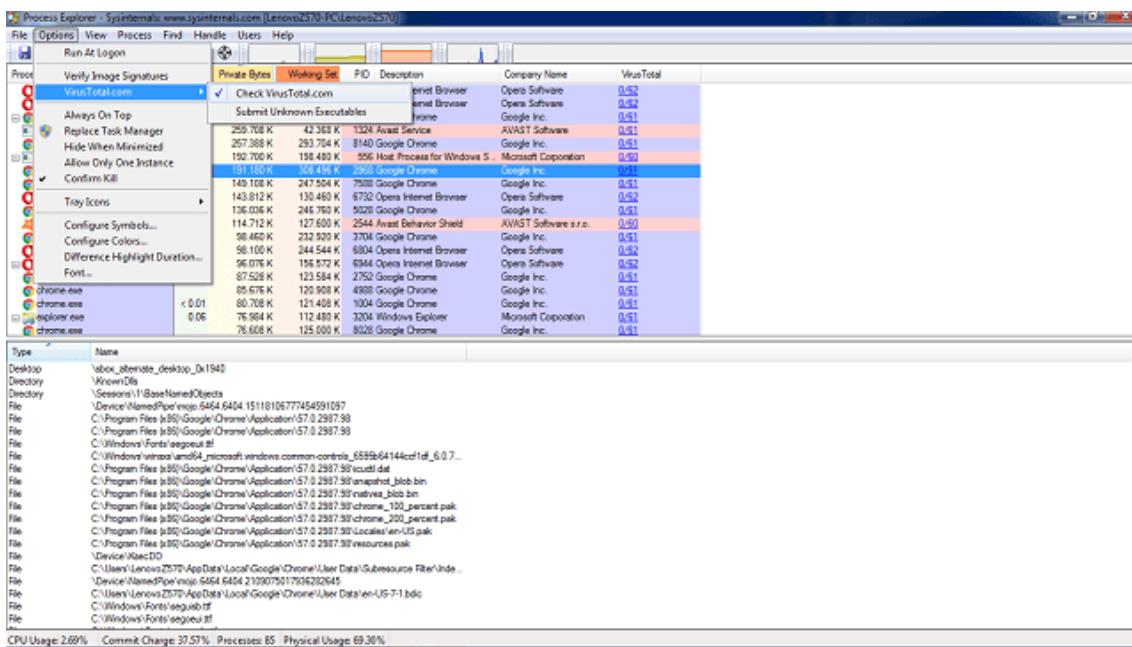
Para los archivos borrados se utilizaran programas especiales capaces de recuperar aquellos datos que se hayan eliminado del disco pero sobre los cuales aún no se haya sobrescrito nada. Es posible que el atacante elimine archivos o registros varios en afán de esconder lo que ha ocurrido, si estos no han sido sobrescritos se podrán recuperar y se podrán situar en la línea temporal relacionándolos con el conjunto de sucesos. Para recuperar información oculta mediante esteganografía también se deberán usar programas concretos. Es posible que el atacante ocultara información sobre otros archivos, tales como imágenes o audio para enviarlos posteriormente o tenerlos almacenados sin llamar la atención. Habitualmente hallaremos más información en ubicaciones ocultas que en los lugares más habituales.

Con todos estos datos se debería poder crear un esbozo de los puntos clave en el tiempo tales como la instalación del sistema, el borrado de determinados archivos, la instalación de los últimos programas, etcétera.

### 3.2.3 Determinar cómo se actuó

Para determinar cómo se actuó es importante llevar a cabo una **investigación sobre la memoria del equipo**. Es interesante realizar un volcado de memoria para la obtención de cierta información. Con programas destinados a tal fin podremos ver que procesos se están ejecutando en el momento concreto y también aquellos que hayan sido ocultados para no levantar sospechas. Con esta información podremos saber qué ejecutables inician los procesos en ejecución y qué librerías se ven involucradas. Llegados aquí se puede proceder a realizar volcados de los ejecutables y de dichas librerías para poder analizar si contienen cadenas sospechosas o si, por lo contrario, son archivos legítimos. Sabiendo los procesos que se ejecutan y su naturaleza podemos obtener pistas de cómo se actuó para comprometer al equipo.

A menudo nos deberemos fijar en procesos en ejecución aparentemente inofensivos, habituales y legítimos en los sistemas operativos. No es extraño que determinados procesos con fines malintencionados se camuflen con procesos legítimos. Para ello deberemos observar que muchas veces estos se encuentran sin un proceso padre, cuando lo más habitual es que dependan de otros. En otras ocasiones simplemente se camuflan con nombres muy parecidos a otros para pasar desapercibidos.



#### El programa Process Explorer en funcionamiento

Ciertos programas también nos darán información sobre las cadenas del ejecutable en cuestión. Con ellas podremos ver si mutan su contenido cuando se ejecutan en memoria y cuál es su contenido. En ocasiones, cierta información de las cadenas nos puede dar pistas muy valiosas, como por ejemplo, cadenas dónde encontrar logs, o enlaces a direcciones de Internet. También nos puede dar pistas sobre el tipo de malware al que nos enfrentamos. Si por ejemplo encontramos cadenas con alfabetos o teclas concretas del teclado, es probable que nos encontremos ante un keylogger.

Finalmente, otra práctica interesante para determinar cómo se actuó es leer la secuencia de comandos escrita por consola. Para ello procederemos con el volcado de memoria y podremos obtener dicha información. De este modo podremos leer que comandos se hicieron por consola y sabremos si se ejecutó algún proceso de este modo. Debemos excluir nuestras propias instrucciones pues seguramente aparecerán los comandos del volcado de

memoria que se hicieron en su momento.

### *3.2.4 Identificar a los autores*

Para poder realizar una identificación del autor o autores del incidente, otra información importante que nos puede dar el volcado de memoria son las **conexiones de red abiertas** y las que están preparadas para enviar o recibir datos. Con esto podremos relacionar el posible origen del ataque buscando datos como la **dirección IP** en Internet.

Hay que actuar con prudencia puesto que en ocasiones se utilizan técnicas para distribuir los ataques o falsear la dirección IP. Hay que ser crítico con la información que se obtiene y contrastarla correctamente. No siempre se obtendrá la respuesta al primer intento y posiblemente en ocasiones sea muy difícil averiguar el origen de un incidente.

Es interesante recapacitar en los distintos perfiles de atacantes que se pueden dar hoy día en este ámbito para intentar mimetizarse y entender quién pudo ser el autor.

- Por un lado podemos **encontrar organizaciones y criminales que actúan por motivaciones económicas**. Su finalidad es robar cierta información, ya sea empresarial o personal, para una vez obtenida venderla o sacar un rendimiento oneroso de la información.
- Por otro lado está **quien sólo busca acceder a sistemas por mero prestigio** y reconocimiento en su ambiente cibernético. Accediendo a sistemas mal configurados y publicando datos que prueben su fechoría incrementará su notoriedad y se dará a conocer más en las redes.

En este punto es importante analizar dos vertientes. En caso que se esté realizando un peritaje con fines inculpatorios, o sea, judiciales, se deberá intentar resolver quién es el autor o al menos aportar pistas fiables para que otros investigadores puedan llevar a cabo otras investigaciones de otros ámbitos.

En cambio, si es con fines correctivos lo más interesante seguramente será obviar esta fase y proceder con el estudio del impacto causado y estudiar las mejoras que se pueden implantar para evitar episodios similares.

### *3.2.5 Impacto causado*

El impacto causado se puede calcular en base a distintos factores y no hay un método único para su cálculo, ni una fórmula que nos dé un importe económico. Aun así para estos cálculos puede servir ayudarse de métodos como **BIA (Business Impact Analysis)** que determinan el impacto de ciertos eventos ayudando a valorar los daños económicamente.

A la larga cualquier incidente ocurrido devengará en unos gastos económicos que habrá que cuantificar en función de los ítems afectados tras el suceso. En ocasiones el coste económico resultará de tener que reemplazar una máquina o dispositivo que ha quedado inservible tras un ataque o bien las horas de empleado de tener que reinstalar el sistema. En este caso, el cálculo no supone mayor dificultad y se resuelve fácilmente.

En otras ocasiones, por ejemplo, los daños pueden deberse al robo de una información de secreto industrial en el que habrá que cuantificar no sólo qué supone reponer el sistema sino, a la larga, en qué se verá afectada la empresa. Los datos robados pueden ser para

publicar cierta información sobre la empresa y poner en la opinión pública datos con intenciones de crear mala imagen, lo cual supone un daño incalculable y muy elevado.

El impacto no sólo se puede calcular en base económica. Como ya se ha comentado al inicio de esta sección también existen otros factores, es el caso del **tiempo de inactividad**. Si el incidente ha supuesto paralizar la producción de una planta automatizada de fabricación esto supone muchas horas en que la producción es nula, por lo tanto no se trabajará.

Evidentemente, a la larga también supondrá un problema económico pues no se podrán servir los pedidos pendientes de los clientes. Si la paralización afecta a una oficina, tal vez no se pare la producción de bienes pero sí el trabajo de los empleados que verán retrasado todo su trabajo.

### *3.3 Redacción de informes y Presentación*

La última fase de un análisis forense queda para redactar los informes que documenten los antecedentes del evento, todo el trabajo realizado, el método seguido y las conclusiones e impacto que se ha derivado de todo el incidente.

Para ello se redactarán dos informes, a saber, **el informe técnico y el ejecutivo**. En esencia en ambos informes se explican los mismos hechos pero varía su enfoque y el grado de detalle con que se expone el asunto.

En **el informe ejecutivo** se usará un **lenguaje claro y sin tecnicismos**, se debe evitar usar terminología propia de la ciencia e ingeniería y expresiones confusas para gente no ducha en el tema. Hay que pensar que **el público lector de estos informes serán jueces y gerentes** que seguramente estén poco relacionados con el tema y además tengan poco tiempo para dedicarle. Se les debe facilitar la tarea al máximo.

En **el informe técnico**, por el contrario, **el público final será técnico y con conocimientos de la materia** que se expone. Aquí se detallarán todos los procesos, los programas utilizados, las técnicas, etcétera. Debemos crear un documento que pueda servir de guía para repetir todo el proceso que se ha realizado en caso necesario.

# CAPÍTULO 4

---

## Requisitos de la investigación forense

---

### *4.1 Aceptabilidad*

Las herramientas y métodos del investigador deberán ser conocidos y aceptados por los profesionales de su sector. Lo ideal sería que otros investigadores hubieran trabajado previamente con determinados procedimientos y existan informes positivos sobre la eficacia de los mismos.

### *4.2 Integridad*

Las pruebas no deben sufrir alteraciones de ningún tipo. Generalmente el medio-disco duro, pendrive o CD/DVD- se precinta después de haber obtenido tres copias cuyos hashes han de coincidir. Con una de ellas llevará a cabo su análisis el investigador. Otra se guardará como respaldo, y la tercera será puesta a disposición de la parte contraria para que esta pueda realizar sus propias averiguaciones, manifestar su posición al respecto o elaborar un contrainforme.

### *4.3 Credibilidad*

Todo lo que se haga debe ser demostrable. El investigador debe acreditar un conocimiento adecuado de sus herramientas para poder explicar de manera plausible lo que consigue de ellas.

#### *4.4 Relación causa-efecto*

Aunque no es cometido del investigador extraer conclusiones de ningún tipo sobre culpabilidad o responsabilidades de las personas que intervienen en los hechos, los métodos empleados por aquél deben hacer posible una explicación de los acontecimientos en términos de causa-efecto.

#### *4.5 Carácter repetible*

Este requisito se explica por sí mismo. Sean cuales fueren los métodos de trabajo empleados o la persona que realiza la investigación, los mismos datos de entrada deberán producir los mismos resultados.

#### *4.6 Documentación*

Cada paso dado por el investigador deberá disponer de una descripción detallada y exacta, al objeto de que los informes no puedan ser impugnados por culpa de ambigüedades o negligencias de ningún tipo. Especial cuidado deberá tenerse a la hora de documentar la cadena de custodia que es la parte más sensible de todo el proceso y la que con más facilidad podrá atacar la parte contraria en caso de localizar la menor irregularidad.

# CAPÍTULO 5

---

## Valoración jurídica de la prueba digital

---

### *5.1 Interés legal de la prueba*

En el ámbito jurídico, al cual va destinada la evidencia, no se rige por la mentalidad lineal del ingeniero, sino por las complejas categorías del derecho. El destino de toda prueba digital es ser expuesta ante los tribunales, y su solvencia jurídica dependerá de las circunstancias en que haya sido obtenida.

### *5.2 Prueba física y prueba personal*

Pruebas físicas no en sentido literal, sino en el de la validez jurídica de las mismas pueden ser discos duros, archivos de registro, informes periciales o huellas dactilares. Esta evidencia es llevada al proceso por personas que tienen que explicarlas y hacer valer su carácter probatorio en relación con los hechos juzgados.

“Por sí misma la prueba física, es decir, el objeto evidencial hallado en el lugar de los hechos, no demuestra nada”

Haber encontrado huellas dactilares en el arma homicida no implica que quien las dejó cometiera el crimen necesariamente. También cabe pensar que tuvo el arma en sus manos en un momento anterior, para limpiarla o darle grasa. Por el contrario el verdadero agresor podría haber usado unos guantes para disparar. Del mismo modo hallar archivos de pornografía infantil en una computadora no inculpa automáticamente a su propietario.

La fuerza probatoria no se manifiesta hasta que intervienen las personas que hallaron la evidencia o aquellas que han de explicarla en relación con los hechos que se juzgan.

Existen por lo tanto una estrecha relación entre la **prueba física** (disco duro, archivo de registro, mensaje de correo electrónico, volcado de memoria, fotografía digital) y la **prueba personal** (intervención del investigador forense ante el juez). El carácter probatorio de

una evidencia, ya sea electrónica o de cualquier otro tipo, depende de la cualificación profesional.

### *5.3 Cualificación del investigador forense*

La presentación de los elementos de evidencia y los métodos utilizados en la consecución de aquellos van a ser comprobados por el tribunal minuciosamente. Pierde credibilidad quien aporta pruebas de forma inadecuada, realizando afirmaciones rebatibles o divagando acerca de la evidencia y sus posibles significados.

“Si el investigador no realiza bien su trabajo la prueba puede quedar invalidada en el proceso”

### *5.4 La adquisición: fase crucial*

Es en la obtención de los elementos de evidencia donde las buenas prácticas han de observarse con mayor rigor. El punto de partida de la investigación forense lo constituye la imagen a bajo nivel mediante flujo de bits obtenida a partir del soporte de datos. Conviene recordar que no estamos recuperando una tesis doctoral perdida por un profesor universitario a consecuencia de un fallo en el disco duro, ni las fotos de las vacaciones que se nos borraron accidentalmente por culpa de un virus.

Estamos a punto de tomar parte en un proceso que puede tener graves consecuencias cuando lo que se juzga son responsabilidades penales.

La pericia técnica no es suficiente. **De lo que se trata es de preservar elementos de evidencia, asegurar una cadena de custodia y realizar duplicados exactos resistentes a las sumas de verificación y alegatos de la parte contraria.**

# CAPÍTULO 6

---

## Más información

---

### 6.1 Webgrafía

#### 6.1.1 SANS: Evidence acquisition

SANS es una organización especializada en seguridad informática, con unos artículos muy apreciados en el ámbito de la informática forense. Dentro de la categoría «Digital Forensics and Incident Response » encontraréis todo lo relacionado con la adquisición de evidencias digitales.

- <https://www.sans.org/blog/?focus-area=digital-forensics>

#### 6.1.2 Básica

- Altheide, Cory and Harlan Carvey. (2011). *Digital Forensics with Open Source Tools* (pp. 1-8). Science Direct.
- Brezinski, D., y Killalea, T. (2002). [Guidelines for Evidence Collection and Archiving](#)
- Bulbula, H. I., H. Guclu Yavuzcanb, and Mesut Ozel. (2013). Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM). *Forensic Science International*, Vol. 233(1-3), 244-256.
- Casey, Eoghan, Monique Ferraro, and Lam Nguyen. (2009). Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence. *Journal of Forensic Sciences*, Vol. 54(6), 1353-1364.
- Henry, P. (2009). [Best Practices. In Digital Evidence Collection](#).
- ISACA. (2015). [Overview of Digital Forensics](#).

- Karie, Nickson M. and H. S. Venter (2015). Taxonomy of Challenges for Digital Forensics. *Journal of Forensic Sciences*, Vol.60(4), 885-893.
- Maras, Marie-Helen. (2014). *Computer Forensics: Cybercriminals, Laws, and Evidence*. Jones and Bartlett.
- Myers, Matthew and Marcus Rogers. (2007). Digital Forensics: Meeting the Challenges of Scientific Evidence. Advances in Digital Forensics: IFIP International Conference on Digital Forensics (pp. 43-50).
- Rousset, Vassil, Candace Quates, and Robert Martel. (2013). Real-time digital forensics and triage. *Digital Investigation* Vol. 10(2), 158-167.
- Sammons, John. (2017). *Digital forensics*, 2st edition. Elsevier.

### 6.1.3 Avanzada

- Alavrez, Karolina and Masooda Bashir. (2015). Exploring the Effectiveness of Digital Forensics Tools on the Sony PlayStation Vita. In: Joshua I. James and Frank Breitinger, eds. *7th International Conference on Digital forensics and Cyber Crime, Selected Conference Papers* (Seoul, South Korea, 6-8 October 2015).
- Antwi-Boasiako, Albert and Hein Venter. (2017). A Model for Digital Evidence Admissibility Assessment. In: G. Peterson and S. Shenoi. (eds.). *Advances in Digital Forensics* (pp. 23-38). Springer.
- Barmpatsalou, Konstantia, Dimitrios Damopoulos, Georgios Kambourakis, and Vasilios Katos. (2013). A critical review of 7 years of Mobile Device Forensics. *Digital Investigation*, Vol. 10(4), 323-349.
- Burke, Paul and Philip Craiger. (2007). Forensic Analysis of Xbox Consoles. *Advances in Digital Forensics III: IFIP International Conference on Digital Forensics* (pp. 269-280).
- Eden, Peter, Andrew Blyth, Pete Burnap, Yulia Cherdantseva, Kevin Jones, High Soulsby, and Kristin Stoddart. (2015). A Cyber Forensic Taxonomy for SCADA Systems in Critical Infrastructure. *10th International Conference, Critical Information Infrastructure Security (CRITIS)*, Berlin, Germany (pp. 27-39).
- Joshi, R. C. and Pilli, Emmanuel S. (2016). *Fundamentals of Network Forensics: A Research Perspective*. Springer.
- Pieterse, Heloise and Martin Olivier. (2014). *Smartphones as Distributed Witnesses for Digital Forensics*. *Advances in Digital Forensics X: IFIP International Conference on Digital Forensics* (pp. 237-251).
- Quick, Darren and Kim-Kwang Raymond Choo. (2017). Pervasive social networking forensics: Intelligence and evidence from mobile device extracts. *Journal of Network and Computer Applications*, Vol. 86, 24-33.
- Sommer, Peter. (2018). Accrediting digital forensics. *Digital Investigation*, Vol. 25, 116-120.
- Suleman, Khan, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Muhammad Shiraz, and Iftikhar Ahmad. (2016). Network forensics: Review, taxonomy, and open challenges. *Journal of Network and Computer Applications* 66, 214-235.

- UK Crown Prosecution Service. (n.d.). [Cybercrime - prosecution guidance](#)

#### 6.1.4 Referencias

- Alba, Manuel. (2014). Order out of chaos: technology, intermediation, trust, and reliability as the basis for the recognition of legal effects in electronic transactions. *Creighton Law Review*, Vol. 47, 387-521.
- Altimari, Dave. (2018). All Evidence Turned Over As Fitbit Murder Case Moves Toward Trial. *Hartford Courant*, 20 July 2018.
- Antwi-Boasiako, Albert and Hein Venter. (2017). A Model for Digital Evidence Admissibility Assessment. G. Peterson and S. Shenoi. (eds.). *Advances in Digital Forensics* (pp. 23-38). Springer.
- Baryamureeba, Venansius and Florence Tushabe. (2004). [The Enhanced Digital Investigation Process Model](#). *Proceedings of the Digital Forensic Research Conference (DFRWS)* (Baltimore, Maryland, 11-13 August 2004).
- Bazin, Philippe. (2008). [An Outline of the French Law on Digital Evidence](#). *Digital Evidence and Electronic Signature Law Review*, Vol. 5, 179-182.
- Biasiotti, Maria Angela, Jeanne Pia Mifsud Bonnici, Joe Cannataci (eds.) (2018). *Handling and Exchanging Electronic Evidence Across Europe*. Springer.
- Brunton, Finn and Helen Nissenbaum. (2016). *Obfuscation: A User's Guide for Privacy and Protest*. MIT Press.
- Carrier, Brian and Eugene H. Spafford. (2003). [Getting Physical with the Investigative Process](#). *International Journal of Digital Evidence*, Vol. 2(2).
- Casey, Eoghan, Monique Ferraro, and Lam Nguyen. (2009). Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence. *Journal of Forensic Sciences*, Vol. 54(6), 1353-1364.
- Caviglione, Luca, Steffen Wendzel, and Wojciech Mazurczyk. (2017). The Future of Digital Forensics: Challenges and the Road Ahead. *IEEE Security & Privacy*, Vol. 15(6), 12-17.
- Conlan, Kevin, Ibrahim Baggili, and Frank Breitinger. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Digital Investigation* Vol. 18, 66-75.
- Conrad, Scott, Greg Dorn and Philip Craiger. (2010). [Forensic analysis of a Playstation 3 console](#). *Advances in Digital Forensics VI: IFIP International Conference on Digital Forensics* (pp. 65-76).
- De La Torre, Gonzalo, Paul Rad, and Kim-Kwang Raymond Choo. (2018). Driverless vehicle security: Challenges and future research opportunities. *Future Generation Computer Systems*, available online 11 January 2018.
- Du, Xiaoyu, Nhien-An Le-Khac, and Mark Scanlon. (2017). [Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service](#). *16th European Conference on Cyber Warfare and Security* (Dublin, Ireland, June 2017).

- Duranti, Lucciana and Corrine Rogers. (2012). Trust in digital records: an increasingly cloudy legal area. *Computer Law & Security Review*, Vol. 28(5), 522-531.
- Goode, Steven. (2009). The admissibility of electronic evidence. *The Review of Litigation*, Vol. 29, 1-64.
- Kasper, Agnes and Eneli Lauritis. (2016). Challenges in Collecting Digital Evidence: A Legal Perspective. In Tanel Kerikmae and Addi Rull. *The Future of Law and eTechnologies*. Springer.
- Kent, Karen, Suzanne Chevalier, Timothy Grance, and Hung Dang. (2006). **SP 800-86. Guide to Integrating Forensic Techniques into Incident Response**. National Institute of Standards and Technology.
- Le-Khac, Nhien-An, Daniel Jacobs, John Nijhoff, Karsten Bertens, Kim-Kwang, and Raymond Choo. (2018). Smart vehicle forensics: Challenges and case study. *Future Generation Computer Systems*, available online 7 June 2018.
- Liskiewicz, Maciej, Rudiger Reischuk, and Ulrich Wolfel. (2017). Security levels in steganography - Insecurity does not imply detectability. *Theoretical Computer Science* Vol. 692(5), 25-45.
- Maras, M.-H. (2014). *Computer Forensics: Cybercriminals, Laws and Evidence* (2nd edition). Jones and Bartlett.
- Maras, Marie-Helen. (2017). Social Media Platforms: Targeting the «Found Space» of Terrorists. *Journal of Internet Law*, 21(2), 3-9.
- Maras, Marie-Helen and Miranda, Michelle D. (2014). Forensic Science. In J. Backhaus (Ed.). *Encyclopedia of Law and Economics*. Springer.
- Maras, Marie-Helen and Alexandrou, Alex. (2018). Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos. *International Journal of Evidence and Proof*, published online 28 October 2018.
- Maras, Marie-Helen and Wandt, Adam. (2018). IoT Data Collection and Analytics. Presentation for FBI, DHS, and Secret Service agents and members of the National Cyber-Forensics & Training Alliance, at John Jay College of Criminal Justice, City University of New York (2 May 2018).
- McKemmish, Rodney. (2008). **When is digital evidence forensically sound? Advances in Digital Forensics IV: IFIP International Conference on Digital Forensics** (pp. 3-15).
- Palmer, G. (2001). **DFRWS Technical Report: A Road Map for Digital Forensic Research**. *Digital Forensic Research Workshop*. Utica, New York.
- Parkinson, M. J. and Matthew G. McKay. (2016). **The Evolution of Vehicle Forensics**. *The Expert Witness*, 31 May 2016.
- Read, Huw, Elizabeth Thomas, Iain Sutherland, Konstantinos Xynos and Mikhaila Burgess. (2016). A forensic methodology for analyzing Nintendo 3DS devices. *Advances in Digital Forensics XII: IFIP International Conference on Digital Forensics* (pp. 127-143).
- Reith, Mark, Clint Carr, and Gregg Gunsch. (2002). An Examination of Digital Forensics Models. *International Journal of Digital Evidence*, Vol. 1(3).

- Shanmugam, Karthikeyan, Roger Powell and Tom Owens. (2011). An Approach for Validation of Digital Anti-Forensic Evidence. *Information Security Journal: A Global Perspective* 20(4-5), 219-230.
- Valijarevic, Aleksandar and Hein S. Venter. (2015). A Comprehensive and Harmonized Digital Forensic Investigation Process Model. *Journal of Forensic Sciences*, Vol. 60(6), 1467-1483.
- UK Association of Police Chiefs. (2012). [ACPO Good Practice Guide for Digital Evidence](#).
- U.S. National Institute of Justice. (2008). [Electronic Crime Scene Investigation: A Guide for First Responders](#), Second Edition.
- U.S. National Institute of Standards and Technology. [Computer Forensics Tool Testing Program](#)