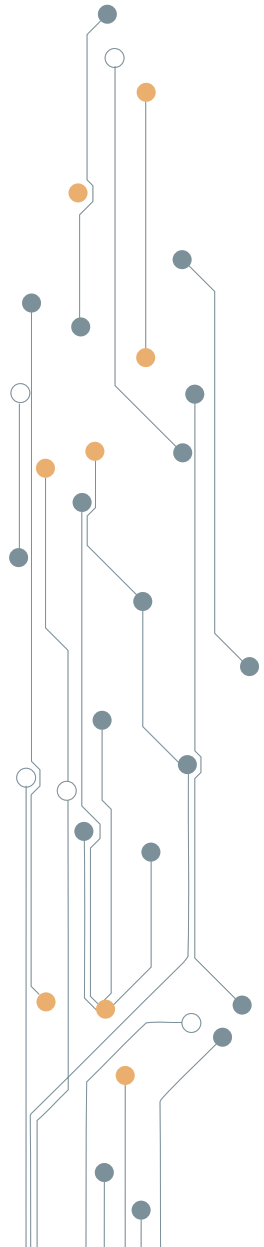
Introducción al análisis forense de sistemas informáticos

Telefónica EDUCACIÓN DIGITAL

Índice



1. Análisis forense de sistemas. Introducción al análisis forense

La informática forense es un procedimiento que debe ir guiado por unas buenas prácticas. Los distintos sistemas operativos pueden ser objeto de un análisis forense para poder deducir qué ha sucedido.

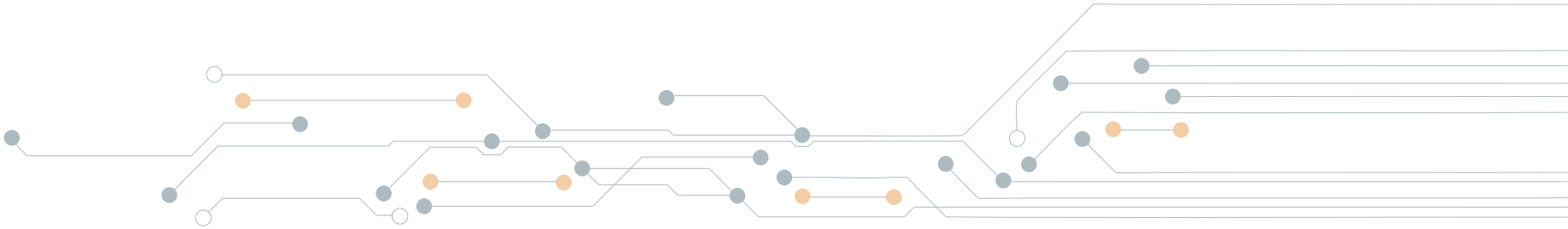
Es fundamental disponer de los conceptos básicos para poder llevar a cabo el proceso forense con éxito. En algunas fases del análisis forense existen similitudes entre los diferentes sistemas operativos que los dispositivos pueden tener, como por ejemplo la fase de adquisición, la cual no difiere en gran medida de uno a otro. Incluso el tratamiento de la memoria RAM, en algunos casos, puede ser llevado a cabo con las mismas herramientas.

Existe una gran cantidad de definiciones para indicar qué es el análisis forense. En el ámbito en el que nos encontramos diremos que es un proceso de estudio exhaustivo de un sistema, pudiendo ser este Linux, Windows, OS X, Android, iOS, ... De este sistema se desea conocer su historia.

En muchas ocasiones es importante saber por qué se realiza un análisis forense. En este punto, un agente, el cual puede ser una empresa, un particular, una entidad, sospecha o tiene la certeza de que ha sido víctima de una intrusión, un ataque, en general un incidente. Desde este sistema se ha podido realizar una acción maliciosa, o en este sistema se ha llevado a cabo una acción maliciosa que se desea estudiar.

El objetivo del análisis forense, independientemente del sistema operativo, es obtener evidencias o en su defecto indicios que puedan clarificar qué es lo que ha sucedido. En otros libros podemos encontrar otras preguntas que el análisis forense debe facilitar y contestar:

- Deducción de lo sucedido.
- Qué ha permitido llegar a ello.
- Qué acciones han sido consecuencias de ello.



Lo que se debe tener claro que no debe ser respondido por un análisis forense, por lo consiguiente por un analista o perito forense es qué podemos hacer para evitar que lo ocurrido vuelva a suceder.

Toda investigación requiere de la búsqueda y captura de evidencias digitales. Se puede definir como evidencia digital a toda aquella información electrónica que puede aportar algún dato para la resolución forense durante el proceso. A continuación, se enumeran algunos ejemplos de evidencias que pueden ser utilizados o necesarias en el proceso:

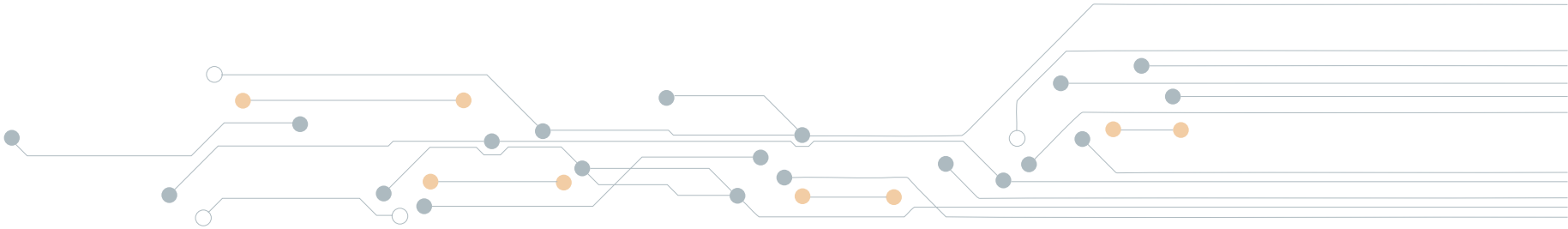
- Fecha del último acceso a un fichero ofimático o a una aplicación.
- Un intento de elevación de privilegio en el sistema a través de sudoers. Por ejemplo, este intento de acceso se registra cómo "<user> is not in the sudoers file. This incident will be reported". En función del sistema Linux se puede encontrar el log en /var/log/secure (Fedora) o en /var/log/auth.log (Debian).
- Una cookie de navegación web a través de Mozilla Firefox almacenada en un disco duro.
- La imagen de un disco duro o pendrive. Se podría ver como un conjunto o ecosistema de evidencias.

El estudio del mayor número de evidencias encontradas en un sistema Linux dará información concreta y verificable. Es cierto que muchos pasos en el análisis forense a sistemas Linux llevan la misma parte o base teórica que a otros sistemas. Las particularidades de herramientas, técnicas o propiedades de sistemas de ficheros o memoria RAM son las que diferencian el forense a un sistema y a otros.

Por supuesto, y tal y como se habrá aprendido en otros ámbitos, es de gran importancia que sean recogidas todas las evidencias posibles y que éstas sean tratadas y analizadas de manera responsable no perturbando el contenido que almacenan.

Las evidencias digitales pueden quedar invalidadas en los siguientes casos:

- Aquellas que no puedan demostrarse como no manipuladas.
- Aquellas que vulneren normativas de seguridad de la empresa.
- Aquellas que vulneren la intimidad o revelen información personal.



En el momento que se pueda poner en duda la integridad de una evidencia, pasará a ser invalidada. Las otras afirmaciones pueden tener algunos casos donde puedan ser debatibles, aunque en la mayoría de los casos se asumirá que puedan ser invalidadas.

Una vez definido el análisis forense, haber definido qué es una evidencia digital y haberlas ejemplificado, debemos preguntarnos: ¿dónde se aplica el análisis forense? A continuación, se enumeran escenarios reales donde se puede aplicar un análisis forense:

- Fraudes.
- Casos civiles.
- Delitos informáticos.
- Conflictividad corporativa o laboral.

...

A la orden del día se pueden encontrar diferentes escenarios donde se precisa llevar a cabo un análisis forense sobre un sistema, sobre una red, sobre un servicio concreto, ... A continuación, se enumeran algunos ejemplos que pueden resultar de interés:

- **Accesos no autorizados al sistema.** El usuario consigue acceder al sistema Linux, al cual no debería poder acceder. Este tipo de ataques pueden afectar a la confidencialidad e integridad de la información y activos de la empresa.
- **Incidente de ejecución de código malicioso.** Existe un malware ejecutándose en el sistema Linux. Con este tipo de software se puede dar acceso o destruir información de un sistema. Este tipo de ataques pueden afectar a la confidencialidad e integridad de la información y activos de la empresa.
- **Interrupción o denegación del servicio.** El objetivo de un atacante o grupo de atacantes es el de saturar o interrumpir la ejecución de un servicio determinado. Por ejemplo, una organización tiene una serie de servidores Apache ejecutándose sobre máquinas Linux y a través del uso de una Botnet se satura mediante ataque SYN Flood las conexiones de dichas máquinas. Este tipo de ataques pueden afectar sobre la imagen corporativa y sobre la continuidad de negocio de la propia empresa.
- **Utilización no autorizada de un servicio.** El usuario puede hacer uso de un servicio, sin estar autorizado para ello. Una mala configuración de permisos, por ejemplo, en sudoers podría permitirlo. La evaluación del log en este caso podría ser importante.

Por último, antes de pasar al contenido de la RFC 3227 se debe tener en cuenta aspectos que pueden ser de utilidad en una investigación:

- Método y/o técnicas utilizadas por el atacante para lograr entra en el sistema Linux.
- Actividades ilícitas realizadas por el intruso.
- Alcance e implicaciones de dichas actividades.
- Software malicioso instalado en el sistema.
- Otras actividades.

1.1 | RFC 3227: Recolección y manejo de evidencias

La RFC 3227 es un documento que recoge las recomendaciones sobre las pautas que un analista o perito forense debe seguir en el instante de llevar a cabo la recolección de evidencias de un sistema. Lógicamente, eso es aplicable a la recogida de evidencias de un sistema Linux, el cual es el que nos interesa en este tema. En otras palabras, el documento se centra en los aspectos que son de interés en los procesos de análisis forense.

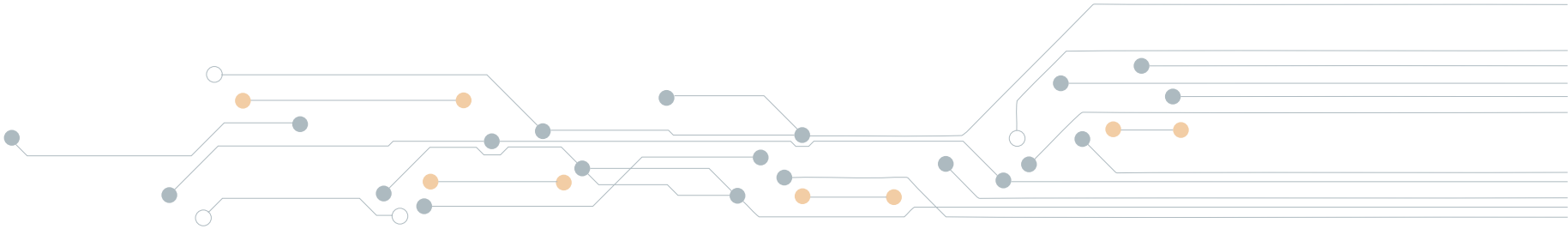
El documento recoge toda la problemática global que lleva asociado la realización de un proceso forense riguroso y útil. Es decir, un proceso forense que no pueda ser echado para atrás por ningún juez.

El análisis forense, según se enmarca en la RFC 3227, debe ser tratado como un proyecto delicado. En primer lugar, se deben cumplir unos prerrequisitos. Sin el cumplimiento de estos prerrequisitos el analista no podrá tener éxito. Esto es lo que se denomina como principios para la recolección de evidencias.

La RFC engloba la importancia del orden de volatilidad. No todo tiene el mismo orden de volatilidad, por lo que las evidencias deben ser recogidas en función de éste. No es lo mismo la información que se almacena en un DVD que la caché ARP. En otras palabras, el tiempo de vida de dicha evidencia es mayor en un DVD, mientras que la caché ARP puede ser del orden de segundos.

En el documento de recomendaciones y buenas prácticas se indican acciones a evitar. A continuación, se enumeran algunos ejemplos importantes de acciones a evitar:

- Acciones que invaliden un proceso forense. Por ejemplo, la manipulación de alguna evidencia. Su integridad es algo fundamental.
- Precaución para que la evidencia siga pura. Esto está relacionado con la sentencia anterior.
- Consideraciones relativas a la privacidad de los datos de los propios usuarios.
- Pueden existir datos sujetos a otras leyes. Por ejemplo, los datos personales que se encuentren en el disco pueden estar sujetas a la LOPD.



La recogida de información de manera pura es uno de los objetivos principales de la RFC 3227. La necesidad de conseguir la no pérdida de información, siempre que sea posible, es algo fundamental. Una simple ejecución de una aplicación sobre un entorno de evidencias puede provocar que algo de información sea eliminado o modificado en otro lugar. Esto provocaría la invalidez de una o varias evidencias, por lo que se debe controlar en todo momento por el analista o perito forense.

La transparencia para la recogida de evidencias es fundamental. La utilización de herramientas que se sepa cómo actúan y qué está ejecutando por debajo es fundamental. En ningún momento se puede utilizar herramientas que no sepamos cómo funcionan o que están ejecutando. Esto podría poner en riesgo la validez de las evidencias. También por este hecho es fundamental, una vez adquirida, por ejemplo, la imagen de un disco, trabajar siempre sobre la copia.

Se propone una metodología para llevar a cabo el almacenamiento de evidencias. Hay que almacenarlas en sitios de confianza y con vida suficiente para que pase un posible juicio. Es de vital importancia que las evidencias se encuentren bajo la custodia del analista y se encuentren protegidas en todo momento. En otras palabras, en todo momento se debe poder contrastar quién entrega la información y quién es el responsable de la custodia de ella. Esto debe ser realizado así hasta que la pruebe o evidencia se utilice.

En el documento de la RFC 3227 se indica explícitamente que la captura de una imagen de un sistema debe ser tan exacta como se pueda llevar a cabo. Por supuesto, se debe evitar trabajar sobre el propio sistema que se debe estudiar. Se deben realizar al menos 2 copias del sistema original.

Además, se debe tener en cuenta que almacenar toda la información posible de la investigación, siempre que se realice de forma correcta es fundamental. La información periférica de situaciones que ayuden a entender mejor el incidente puede ayudar al perito o analista forense a mejorar el rendimiento del proceso.

Por último, el documento refleja que las evidencias y su proceso de recolección debe ir en función de la volatilidad, el cual se ha tratado anteriormente. A continuación, se enumeran una serie de ejemplos a modo de orden:

- Registros del microprocesador, cachés. Difícil captura de ellos y una vida muy corta.
- Tabla de enrutamiento, caché ARP, tabla de procesos que se ejecutan en el sistema, estadísticas del sistema operativo, ...
- Información almacenada en la memoria RAM. Este medio sigue siendo de gran volatilidad y una corta vida. La captura de la memoria RAM puede suponer la modificación del entorno Linux, por lo que se debe valorar mucho cuando es necesario realizar dicha captura.
- Recolección y evaluación de archivos temporales. Estos archivos existirán en el sistema de archivos, en muchas ocasiones.
- Ficheros almacenados en discos.
- Datos de monitorización del sistema, por ejemplo, los eventos de inicio de sesión, de conexión a un servicio, de la elevación de privilegios, ...

1.2 | Fases de un análisis forense

En diferentes medios se pueden encontrar diferentes definiciones sobre las fases de un análisis forense. Desde el punto de vista más general se pueden enumerar y definir 4 fases bien diferenciadas. A continuación, se enumeran las diferentes fases identificadas en un proceso forense:

- **Evaluación.**
- **Adquisición.**
- **Análisis.**
- **Reporte o generación de informes.**

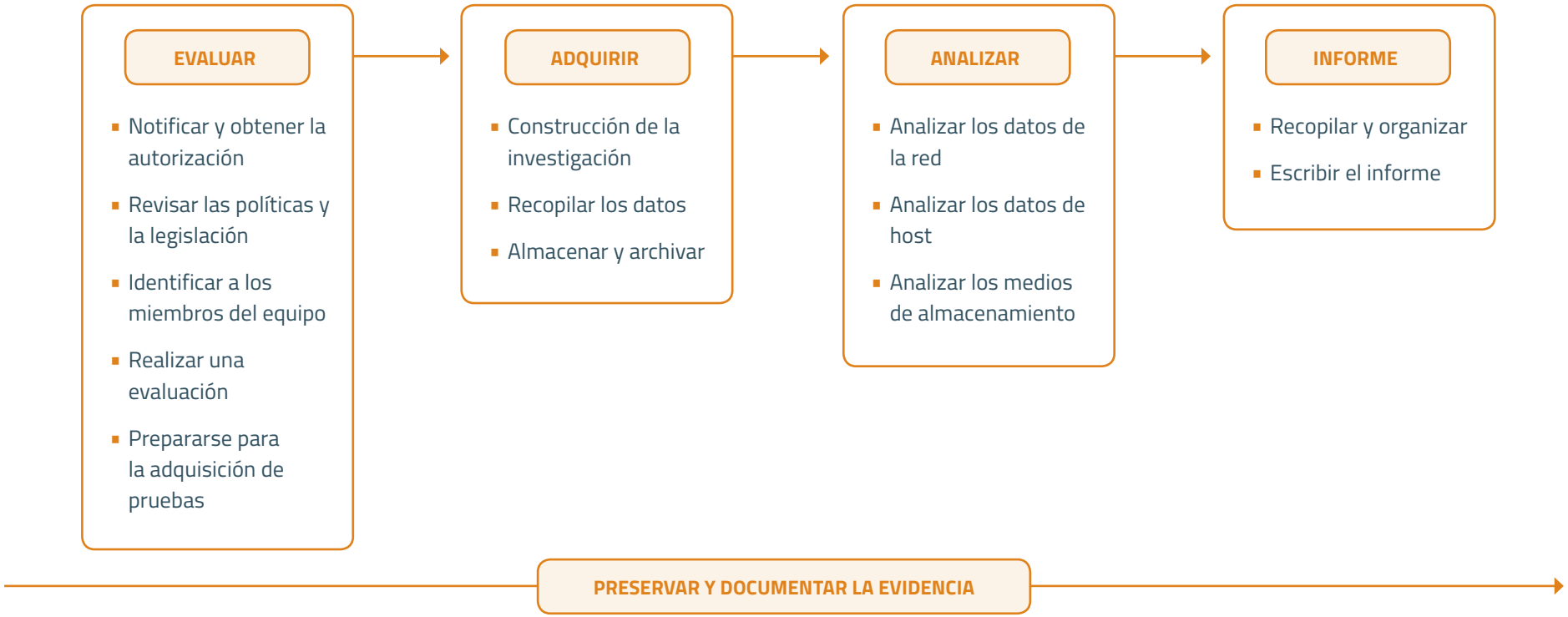


Imagen 1 Fases del análisis Forense

La **evaluación** es la primera fase a llevar a cabo en un proceso forense. Aunque este aspecto queda lejos del ámbito técnico de los temas que se tratarán en adelante, es interesante conocerlos. La preparación para la adquisición de pruebas es un paso vital. Hay que revisar toda la información que se tiene sobre el caso que se debe investigar e intentar resolver.

La **fase de adquisición** permite obtener las evidencias para su almacenamiento. Por ejemplo, en dicha fase se pueden obtener copias de la información que se sospecha puede estar relacionado con el incidente que concierne al perito o analista. En esta fase se realiza la copia de la información, evitando modificar cualquier tipo de dato, tal y como enuncia la RFC 3227. Siempre se deben realizar copias a bajo nivel, utilizando para ello hardware especializado, como son las clonadoras, o software especializado. Sobre esta fase en los sistemas Linux se tratará en el siguiente tema, dónde se podrá estudiar en detalle y mediante ejemplos prácticos.

Cómo indica Juan Luis García Rambla en la obra "*Un forense llevado a juicio*", se debe rotular con la fecha, hora y huso horario la muestra obtenida. Además, ésta debe ser aislada en un recipiente para protegerla, tal y como se puede visualizar en la imagen anterior almacenar y archivar. Por último, se pueden anexar a la prueba obtenida una fotografía con el objetivo de plasmar el estado de equipos y los diferentes componentes electrónicos.

La adquisición debe respetar la regla fundamental de la volatilidad, tal y como reflejaba el documento RFC 3227. El analista puede encontrar un sistema encendido del cual se puede obtener diversas pruebas antes de llevar a cabo el apagado del sistema. Si, por el contrario, el caso comienza con un sistema apagado, la adquisición comenzará en un punto de volatilidad distinto.

En la **fase de análisis** se llevan a cabo una serie de pruebas con el objetivo de poder dar respuestas al incidente por el que el analista se encuentra en esta investigación. En función del tipo de forense y ámbito de trabajo se llevarán a cabo distintas pruebas. También depende de lo que se intente demostrar con el análisis forense. En otras palabras, en esta fase el analista profundizará y evaluará las pruebas recogidas en la fase anterior con el objetivo de poder encontrar evidencias que den respuesta de cara a un juicio. En los siguientes temas se podrá estudiar ejemplos de este tipo de fase, junto a la utilización de distintas herramientas.

Por último, se encuentra la **fase de reporte o generación de informes**. La documentación en el proceso forense es una situación que debe darse de manera continua a lo largo de todo el proceso. Esta última fase debe ser la puesta en común de todo lo anotado y aportar el formato adecuado para poder presentar lo realizado a la persona que lo solicite. Se debe intentar dar énfasis a las cuestiones críticas y relevantes anunciadas en la fase de evaluación. Se debe indicar y adjuntar toda información obtenida, reflejando una relación entre pruebas obtenidas y tareas realizadas. Esto es importante, ya que se debe asegurar que otro analista o perito pueda repetir el proceso y llegar a las mismas conclusiones.

Generalmente se debe entregar un informe ejecutivo en el que se muestra lo más importante de forma resumida. En este tipo de informe se debe reflejar lo más importante, sin entrar en detalles técnicos. En otras palabras, este informe debe ser claro y conciso. Por otro lado, debe existir un informe técnico. Éste es una exposición detallada de todo el proceso llevado a cabo reflejando todas las pruebas y conclusiones obtenidas desde el punto de vista técnico.

1.3 | Tipos de forense

El análisis forense, en muchas ocasiones, depende del ámbito del incidente que se esté tratando. Para poder obtener ciertas evidencias también se puede necesitar realizar distintos tipos de forense. En este apartado se pretende hacer una clasificación de los tipos de análisis forense que se pueden llevar a cabo. Lo importante es entender que para resolver o poder dar respuestas a través de evidencias se pueden necesitar distintos tipos de análisis como los que se pueden englobar en este apartado.

Es cierto que el análisis forense es un proceso con procedimiento en un alto grado. Hay que tener en cuenta que hay parte del forense que se escapa del procedimiento como es la experiencia del analista o el conocimiento que éste tiene sobre una tecnología o sistema concreto. Todos los tipos de forense que se indican en este apartado pueden ser ejercidos sobre sistemas Linux o, por ejemplo, sobre el sistema de archivos característico de estos sistemas, que también se pueden encontrar en plataformas móviles.

A continuación, se muestra una tabla dónde se reflejan distintos **tipos de forense**. Algunos tipos presentados pueden ser parte de otros forenses más concretos, por ejemplo, en forense de un disco puede englobar al forense de malware. La clasificación que se presenta también intenta reflejar distintos tipos de incidentes, los más comunes, por lo que muchas veces se considera un tipo de forense.

- **Malware:** se lleva a cabo un análisis de un sistema en busca de un tipo de software malicioso. Generalmente se intenta dar respuestas a qué malware es, qué ha estado realizando y dónde se encuentra la conexión desde dónde se recibe las órdenes o dónde se extrae información.
- **RAM:** este análisis forense es crítico. La memoria RAM es uno de los elementos más volátiles de los ordenadores. La modificación es casi instantánea, por lo que se incurre en una violación del estado del dispositivo, y por lo tanto posiblemente de las pruebas. En este tipo de análisis se intenta identificar el estado actual de un sistema en el momento en el que incidente ocurre. La información que puede ser extraída de la memoria es mucha, por lo que se detallará en un tema aparte.
- **Red:** las conexiones de los sistemas es algo fundamental y ante un incidente es la vía para comunicarse con, por ejemplo, un malware, el atacante. A través de la red circula todo lo que entra y sale del sistema hacia Internet o la propia red interna. El análisis forense de red intenta dar respuestas mediante capturas de red qué ha ocurrido, quién está comunicando o extrayendo información, cómo lo está haciendo y hacia dónde lo está haciendo.
- **Dispositivos móviles:** el análisis forense a dispositivos móviles sigue los principios del análisis forense clásico, ya que al final son ordenadores. Tiene matices debido a la naturaleza de dichos dispositivos. Se debe tener en cuenta una serie de matices.
- **Disco:** en la mayoría de incidentes hay que hacer una copia de disco del sistema afectado por el incidente. Por ejemplo, el análisis forense de la RAM puede ser un complemento a un análisis de un sistema a través del disco.

Telefónica EDUCACIÓN DIGITAL