norma española

UNE 71506

Julio 2013

TÍTULO

Tecnologías de la Información (TI)

Metodología para el análisis forense de las evidencias electrónicas

Information Technologies (IT). Methodology for the digital evidences forensic analysis.

Technologies de l'information. Méthodologie pour analyse médico-légale de la preuve numérique.

CORRESPONDENCIA

OBSERVACIONES

ANTECEDENTES

Esta norma ha sido elaborada por el comité técnico AEN/CTN 71 *Tecnología de la información* cuya Secretaría desempeña AMETIC.

Editada e impresa por AENOR
Depósito legal: M 20322:2013

LAS OBSERVACIONES A ESTE DOCUMENTO HAN DE DIRIGIRSE A:

AENOR Asociación Española de Normalización y Certificación

Génova, 6
28004 MADRID-España

info@aenor.es
www.aenor.es

Tel.: 902 102 201
Fax: 913 104 032

23 Páginas

ÍNDICE

Página

0 INTRODUCCIÓN

Las evidencias electrónicas requieren de un análisis forense detallado que confirme la existencia de un incidente, las causas que lo originaron, así como sus consecuencias. Para ello, se requiere una labor previa de localización de las mismas, para posteriormente, ser analizadas con una metodología forense como la que aquí se presenta.

En esta norma se detalla la metodología necesaria para obtener resultados válidos en un procesado forense de las evidencias electrónicas. Una evidencia electrónica puede ser cualquier evidencia física como son el ordenador, los periféricos, la salida visual del monitor, la evidencia impresa, los registros informáticos, etc.

Se pretende que esta norma dé cumplida respuesta a la problemática causada por infracciones legales e incidentes informáticos en las distintas empresas y entidades, ya que la obtención de evidencias electrónicas fiables y robustas ayuda a atribuir correctamente dichos hechos, pudiendo discernir si su causa tiene como origen un carácter intencional o negligente. Con dicha información se consigue ubicar de forma acertada los instrumentos, acciones, fines y demás parámetros concernientes a dichas conductas.

La información a estudiar por esta norma incluirá, unida a la propia de los sistemas dotados de un único repositorio de almacenamiento, la encontrada en los sistemas distribuidos, así como la ubicada en entornos virtuales, siempre y cuando esta información a analizar esté perfectamente localizada y ubicada en un espacio físico donde se encuentran los datos en formato digital.

1 OBJETO Y CAMPO DE APLICACIÓN

La presente norma tiene por objeto establecer una metodología para la preservación, adquisición, documentación análisis y presentación de evidencias electrónicas.

La presente norma es de aplicación a cualquier organización con independencia de su actividad o tamaño, así como a cualquier profesional competente en este ámbito.

El presente documento se dirige especialmente a los equipos de respuesta a incidentes y seguridad, así como al personal técnico que trabaje en laboratorios o entornos de análisis forense de evidencias electrónicas.

La presente norma se ha elaborado para definir el proceso de análisis forense dentro del ciclo de gestión de las evidencias electrónicas, complementando todos aquellos otros procesos que conforman dicho sistema de gestión de las evidencias electrónicas, según se describe en las partes de la Norma UNE 71505.

No se consideran dentro del campo de aplicación de esta norma la generación, gestión, seguridad, conservación y/o almacenamiento de la evidencia electrónica antes de la adquisición, aspectos a los que se refieren las Normas UNE 71505.

No es tampoco objeto de esta norma la validación y/o acreditación de laboratorios forenses ni la homologación de *software* o equipos relacionados.

2 NORMAS PARA CONSULTA

Los documentos que se citan a continuación son indispensables para la aplicación de esta norma. Únicamente es aplicable la edición de aquellos documentos que aparecen con fecha de publicación. Por el contrario, se aplicará la última edición (incluyendo cualquier modificación que existiera) de aquellos documentos que se encuentran referenciados sin fecha.

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

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

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

UNE 197001:2011 *Criterios generales para la elaboración de informes y dictámenes periciales.*

CEN/Guide 14 *Common policy guidance for addressing standardisation on qualification of professions and personnel*.

3 ESTRUCTURA DE LA NORMA

Esta norma se estructura en los siguientes capítulos y anexos:

- El capítulo 5 se refiere a la preservación de las evidencias originales garantizando su inalterabilidad, lo cual permite igualmente la reproducibilidad de los estudios a efectuar sobre ellas. En consecuencia, todo análisis forense de la información digital exige preservar las evidencias originales para que éstas no pierdan en ningún momento su validez legal. Esta preservación conlleva el almacenamiento de las evidencias electrónicas originales en soportes y lugares estancos o aislados que eviten las interferencias externas que puedan modificarlas.

- El capítulo 6 se refiere a la adquisición de las evidencias, distinguiendo entre el tratamiento de la información obtenida en sistemas apagados y la obtenida en sistemas encendidos. Es decir, las evidencias electrónicas sobre las que se realizará el pertinente análisis forense pueden tener su origen en datos estáticos de sistemas apagados, datos en tránsito de sistemas en funcionamiento, datos volátiles, datos de sistemas embebidos, así como datos de grandes sistemas, dispositivos móviles y redes, pudiendo estar toda la información a analizar ubicada en un único lugar o en varios repositorios físicos.

- El capítulo 7 se refiere a la documentación, con la finalidad de garantizar la cadena de custodia y la trazabilidad de las evidencias objeto de análisis forense, a través de la implantación de un sistema de gestión documental, que registre todos los procesos que se efectúan sobre dichas evidencias digitales, bien sean originales o copias o clonados de éstas.

- El capítulo 8 se dedica al análisis propiamente dicho de la información de interés de las distintas evidencias digitales objeto de estudio.

- El capítulo 9 se refiere a la presentación de los resultados obtenidos a la autoridad judicial o entidad que solicita este informe pericial.

Esta norma tiene tres anexos, uno normativo (anexo A- Modelo de informe pericial) y dos informativos (anexo B- Competencias para el análisis forense de las evidencias electrónicas y el anexo C-Equipamiento para el análisis forense de las evidencias electrónicas).

4 TÉRMINOS Y DEFINICIONES

Para los fines de este documento, se aplican los términos y definiciones incluidos en la Norma UNE 71505-1 además de los siguientes:

4.1 evidencia:
Cada uno de los datos digitales recogidos en la escena de interés susceptibles de ser analizados con una metodología forense.

4.2 muestra:
Parte representativa o significativa de una evidencia.

4.3 información original:
Conjunto organizado de datos que mantiene su integridad desde el inicio hasta el final del fichero o soporte informático que los contiene.

4.4 cadena de custodia:
Procedimiento de trazabilidad controlado que se aplica a las evidencias, desde su adquisición hasta su análisis y presentación final, el cual tiene como fin no alterar la integridad y autenticidad de las mismas, asegurando en todo este proceso que los datos originales no son alterados.

4.5 clonado:
Proceso de copia, a bajo nivel y firmada digitalmente, de la información original por el cual se traslada ésta a un nuevo soporte de almacenamiento digital, preservando la inalterabilidad de la información en el sistema o soporte de origen y asegurando la identidad total entre aquella y la extraída.

4.6 imagen forense:
Es el producto de realizar un clonado de cualquier evidencia electrónica en un formato de fichero, sin tener en cuenta el soporte que la contiene.

4.7 entorno de análisis forense:
Lugar físico aislado del resto de actividades de la empresa u organismo donde se analiza la información electrónica, dotado de medios técnicos para los trabajos forenses asociados a las nuevas tecnologías.

4.8 informe pericial:
Documento donde se recogen todas las tareas realizadas en las diferentes fases del análisis forense, así como las conclusiones extraídas en base a los hallazgos encontrados.

4.9 metadato:
Información que describe el contenido de un dato.

4.10 prueba electrónica:
Es la demostración en un procedimiento judicial de los hechos que fundamentan la aplicación de requerimientos formales, procesales y/o legales.

4.11 registro:
Conjunto de datos que almacena la información y configuraciones de todo el *hardware*, *software*, usuarios y preferencias de un sistema de información.

4.12 sistema de ficheros:
Organización lógica de un dispositivo.

4.13 trazabilidad:
Propiedad de la información de ser rastreada o reconstruida hasta su origen.

4.14 virtualización:
Método consistente en la simulación del funcionamiento de una máquina física con su sistema operativo.

5 ABREVIATURAS

ADN: Ácido DesoxirriboNucleico

BIOS: Sistema básico de encendido/apagado (*Basic Input/Output System*)

CCTV: Circuito cerrado de televisión (*Closed Circuit Television*)

CD: Disco compacto (*Compact Disc*)

DCO: Capa de configuración de dispositivo *(Device Configuration Overlays)*

FS: Sistema de ficheros (*File System)*

FSFSHPA: Áreas ocultas de almacenamiento *(Host Protected Areas)*

ICCID: Identificador de tarjeta con circuitos integrados *(Integrated Circuit Card ID)*

IP: Protocolo de Internet (*Internet Protocol*)

LOCI: Archivo de localización (*Localization Information File*)

MAC: Control de acceso del medio (*Media Access Control*)

MFT: Tabla maestra de archivos (*Master File Table*)

PIN: Número de identificador personal (*Personal Identification Number)*

PUK: Clave personal de desbloqueo (*Personal Unlocking Key*)

RAID: Conjunto redundante de discos independientes *(Redundant Array of Independent Disks)*

RAM: Memoria de acceso aleatorio *(Random-access memory)*

SIM: Módulo de identificación del suscriptor (*Subscriber Identity Module*)

URL: Localizador de recursos uniforme (*Uniform Resource Locator*)

VLAN: Red de área local virtual (*Virtual Local Area Network*)

6 PRESERVACIÓN

El análisis de la información digital exige preservar las evidencias originales para que éstas no pierdan en ningún momento su validez y confiabilidad, garantizando también la reproducibilidad de los estudios efectuados por cualquier entorno de análisis forense o laboratorio designado para su análisis, caso de existir contraanálisis o contrapericias sobre esta misma información.

Toda organización o entorno empresarial debe tener en cuenta los siguientes principios a la hora de interactuar con las evidencias electrónicas a las cuales se les pueda realizar un análisis forense:

– poseer protocolos detallados que aseguren la integridad de las evidencias objeto del estudio forense, de tal forma que se evite la manipulación de las mismas por los efectos de la modificación intencionada "*tampering",* descargas electrostáticas, campos magnéticos o la conexión accidental a redes inalámbricas;

– igualmente, los técnicos encargados de una primera respuesta sobre las evidencias objeto de estudio, deben poner especial cuidado en almacenar éstas en soportes adecuados, para además de garantizar esta integridad, poder preservar otras evidencias ajenas a las nuevas tecnologías presentes en los soportes digitales, como son, huellas, restos orgánicos asociados con el ADN o partículas diversas;

– este personal técnico debe manipular las evidencias con la indumentaria adecuada, especialmente adaptada para evitar descargas electrostáticas, así como ser conscientes de que no deberían portar equipos que puedan crear señales de radiofrecuencia y alterar el espectro radioeléctrico de la escena de interés, lo cual lleva en ocasiones a la necesidad de utilizar soportes estancos o aislados que eviten las interferencias externas que puedan modificar los datos originales.

Simultáneamente a los principios de actuación anteriores, el personal técnico encargado de la preservación de las evidencias electrónicas debería llevar a cabo las siguientes pautas:

– proceder a precintar y sellar en soportes adecuados todas las evidencias encontradas, hasta que se active su análisis por los peritos o especialistas designados para dicho cometido dentro del laboratorio o entorno de análisis forense, poniendo especial atención en los dispositivos que requieran estar alimentados por una fuente de energía externa;

– todas las evidencias o muestras a analizar, y hasta que se finalice la pericia correspondiente, se deben almacenar en un lugar seguro dedicado a tal fin, siempre y cuando los medios así lo permitan, y en ausencia de dicho lugar, en una caja fuerte en el mismo entorno de trabajo.

7 ADQUISICIÓN

Es un principio ineludible del mundo forense de las nuevas tecnologías trabajar con imágenes, copias o clonados a bajo nivel de los datos originales.

El proceso de adquisición o captura forense de las evidencias, debe incluir, según los casos:

– un clonado forense; o

– la realización de imágenes completas o lógicas de la información de interés.

A tal fin, se debe seguir un procedimiento documentado por cada organización o empresa, de tal forma que se asegure que es reproducible y repetible.

Para la adquisición forense de los datos de interés almacenados en los distintos soportes digitales se distinguen en esta norma dos situaciones:

a) la adquisición de información de sistemas apagados;

b) la adquisición de información de sistemas encendidos, donde el aplicar métodos intrusivos, aunque sean mínimos, puede comprometen en algún estadio la integridad de la información original a estudiar.

En el caso de que la organización no contase con un equipo de adquisición especializado, se recomienda que el equipo de adquisición que actúe como primer escalón de respuesta cuente al menos con dos personas y que se asista, en su caso, de otro personal técnico especializado. En todo caso, los técnicos que van a realizar la adquisición deben estar debidamente autorizados por la organización propietaria del sistema. En el caso de técnicos externos debe existir un contrato de servicio previamente firmado entre las partes, y en el caso de técnicos internos o en plantilla de la empresa, éstos deben disponer de una autorización escrita por una persona autorizada por la organización, que deje constancia de que los técnicos involucrados en la adquisición actúan por cuenta y mandato de la respectiva organización.

En todos los casos, para asegurar la independencia de las actuaciones forenses, se recomienda la presencia de un fedatario público (secretario judicial, notario, etc.) o de terceros independientes (delegados sindicales, peritos terceros, etc.) que den fe de este proceso.

El personal encargado de la adquisición debe seguir un procedimiento de adquisición documentado y debe utilizar herramientas de *hardware* y *software* reconocidas en el ámbito forense, dejando constancia documental o telemática, a su vez, de los pasos básicos realizados y la metodología seguida en dicha adquisición, que deben ir acompañados del correspondiente historial temporal, asegurando así la cadena de custodia.

De manera previa, es conveniente que el personal técnico encargado de efectuar la adquisición de la información almacenada en los distintos equipos y dispositivos objeto de estudio, sea informado y conozca la política de seguridad que posee la organización o empresa, especialmente en lo relativo a los cuatro aspectos que se detallan seguidamente:

1 Sobre el control de acceso a las máquinas y dispositivos. Este control de accesos permite acceder a las máquinas con los privilegios necesarios. El personal laboral no sólo tiene que acceder al edificio y oficina o habitación donde está el equipo, sino a la máquina física mediante el uso de una combinación de un nombre de usuario y contraseña, o mediante la utilización de otros sistemas de seguridad más robustos (huellas digitales, certificados, tarjetas criptográficas, etc.).

2 Existencia o no de un registro de eventos. Es buena práctica que las organizaciones que dispongan de registro de eventos lo centralicen con todas aquellas operaciones que se determinen conforme a sus políticas de seguridad.

3 Conocimiento del plan de auditorías periódicas que garanticen que la seguridad de los datos de la organización no están comprometidos con la tecnología vigente en ese momento.

4 Conocimiento del sistema de gestión y control de las copias de los datos, así como saber dónde se ubican físicamente los soportes donde se lleva a cabo.

Si el lugar del incidente está delimitado físicamente, el personal técnico reseñado debe adoptar, como mínimo, las siguientes precauciones antes de proceder a la correcta adquisición forense de la información o datos de interés:

1 Aislar la escena de personas no autorizadas, alejando a todos los operarios de los correspondientes ordenadores ubicados en dicho lugar.

2 Identificar al administrador de los distintos sistemas y comunicaciones, caso de que tenga que pedir su apoyo técnico.

3 Si el dispositivo está encendido, no apagarlo y si está apagado, no encenderlo, como medida preventiva hasta que se decida qué tipo de adquisición se llevará a cabo en las evidencias comprometidas. Si el dispositivo está encendido, conviene obtener fotografías o dejar constancia visual y escrita de lo que se visualiza en la pantalla.

4 Buscar en dicho entorno todo tipo de notas asociadas a las palabras de paso y al PIN de acceso a los equipos o ficheros, diarios y manuales técnicos de los equipos involucrados.

5 Fotografiar y grabar en vídeo la escena de interés, anotando detalladamente la posición original de los distintos equipos con el cableado correspondiente y sus periféricos (módem, impresoras, routers, cámaras de grabación activas, etc.), haciendo especial mención a los puertos o salidas estándar a las que se encontraban conectados, con vistas a una posible reconstrucción posterior en el laboratorio o entorno forense que analizará las evidencias.

6 Etiquetar convenientemente todos los dispositivos y el cableado asociado con las evidencias de interés. Las etiquetas se deben colocar en lugares no relacionados con elementos mecánicos de los dispositivos, no ocultando números de serie u otros datos de importancia.

7 Localizar todos los equipos inalámbricos instalados, tanto los visibles como los ocultos, determinando los modos de comunicación que usan éstos. Si la escena lo recomienda, deben activarse equipos que inhiban a la misma de interferencias radioeléctricas externas.

8 Prestar especial atención para no desconectar las fuentes de alimentación cuando las evidencias estén almacenadas en soportes volátiles. En el caso de equipos dependientes de baterías, se deben mantener, en lo posible, en perfecto estado de carga.

9 En los distintos dispositivos digitales, conviene revisar todos los sistemas multimedia incorporados a los mismos, por si hubiese algún dispositivo adicional de almacenamiento digital introducido en ellos.

Igualmente, conviene no separar los soportes digitales de almacenamiento de los equipos en los que están ubicados, especialmente en los sistemas de videograbación o sistemas cerrados de televisión (CCTV) y ordenadores portátiles, pues en muchos casos dichos soportes vienen asociados al equipo correspondiente, de tal forma que al activar un análisis forense de la información de los datos en ellos almacenados, es preciso efectuar este proceso únicamente en el equipo contenedor, y no en otro de similares características o serie ubicado en el laboratorio o entorno forense.

En los sistemas configurados en red cableada o inalámbrica, el personal técnico debe determinar dónde se encuentra el lugar de almacenamiento de la información de interés, discriminando entre almacenamientos homogéneos y distribuidos.

7.1 Sistemas apagados

En el proceso de adquisición de la información almacenada en un sistema apagado se deben seguir unas recomendaciones básicas, como son las siguientes:

– de forma previa, el disco duro o soporte que va a guardar el clonado forense o copia íntegra de los datos originales debe ser sometido a un borrado seguro y estar dentro de su vida útil. Dicho soporte debe estar libre de información previa, para lo cual debe ser testeado de forma segura;

– comprobado dicho extremo, y para garantizar la no alteración de los datos originales durante su proceso de adquisición, se deben usar dispositivos bloqueadores que eviten la escritura de ningún dato adicional a los ya almacenados en el disco o soporte físico original;

– igualmente, se debe efectuar un resumen digital ("*hash*") de la información contenida en el disco duro o soporte original de forma simultánea al proceso de clonado u obtención de la imagen a bajo nivel, usando herramientas *hardware* o *software* contrastadas en el ámbito forense;

– y finalmente, al concluir con los procesos anteriores, se debe proceder a efectuar un nuevo resumen digital ("*hash)*" de la información contenida en el disco o soporte copia obtenido, comprobando que el resumen digital previo y posterior coinciden, lo cual garantiza la integridad de los datos almacenados en el disco original y los obtenidos en las sucesivas copias o imágenes que se elaboren de la información de partida.

Posteriormente y finalizado el proceso detallado anteriormente, los discos o soportes originales se deben volver a precintar y sellar junto con los equipos donde iban instalados, quedando igualmente almacenados en el recinto o área dedicado expresamente para tal fin.

7.1.1 Dispositivos móviles

Un caso particular dentro de estos sistemas apagados son los dispositivos móviles. En este apartado se debe incluir el estudio y extracción de la información contenida en la tarjeta SIM, si la portan y siempre y cuando se disponga del número PIN o PUK correspondiente. Si no es así, se debe solicitar el número PUK de la operadora de telefonía propietaria de la tarjeta a través de la correspondiente autorización judicial tomando como referencia el número ICCID de dicha tarjeta SIM.

También existe información en el terminal móvil, para lo cual se debe proceder a efectuar una copia a bajo nivel de los datos obrantes en la memoria o memorias internas del dispositivo móvil como puedan ser los archivos de audio, imágenes, etc.

De toda la información extraída de la tarjeta SIM y de las memorias del terminal móvil se debe realizar un resumen digital ("*hash*") de su contenido mediante un algoritmo criptográfico, para así garantizar la no alteración de los datos extraídos, caso de tener que efectuar más copias o imágenes de éstos.

7.2 Sistemas encendidos

El análisis forense de estos sistemas se refiere a los equipos en funcionamiento ("*Live Forensics")*, en los cuales se reconoce el valor de la información volátil existente principalmente en la memoria RAM del dispositivo, de tal forma que ésta se pierde al apagar el equipo. Para evitar este hecho, se debe proceder a la adquisición de la información desde el propio sistema en funcionamiento con una mínima alteración o impacto, con vistas a su análisis posterior, siguiendo entonces la metodología utilizada en los sistemas apagados.

Una de las principales ventajas de este análisis es que requiere poco o ningún tiempo de inactividad del sistema, lo cual es importante según el entorno del cual haya que obtener la información de interés, a la par de que permite recuperar información que únicamente está disponible en la memoria RAM o volátil.

Para intentar asegurar la validez forense de estas evidencias, dejando claro que toda adquisición de un sistema en funcionamiento conlleva el uso de técnicas intrusivas, se deberían seguir las siguientes recomendaciones:

– el personal técnico encargado de esta tarea debe documentar, más si cabe, perfectamente todos los procesos efectuados;

– también debe tener claro que estas técnicas no permiten su reproducibilidad. Por tanto, la validez de los resultados obtenidos depende en gran medida de cómo se justifiquen en el informe pericial correspondiente a entregar a la autoridad judicial o entidad que encargó dicho estudio;

– en este informe se debe detallar la metodología seguida para la adquisición efectuada en los sistemas en funcionamiento, así como si se ha minimizado al máximo dicho efecto intrusivo usando dispositivos *hardware* adecuados, o vía *software*, activando comandos perfectamente conocidos, caso del acceso a los datos de la evidencia a través de un entorno remoto.

En estos casos, el resumen digital ("*hash*") es dinámico. Según el instante temporal en que se efectúe se obtendrá uno distinto. Si bien, un resumen digital ("*hash*") de la información volcada va a permitir, como en los dispositivos apagados, identificar de forma única la misma, garantizando así la posibilidad de contrastar la integridad de cualquier copia que se haga del archivo con la imagen de la información obtenida en un determinado momento. Su uso en sistemas encendidos no debería afectar a su posible valor legal;

– los datos en un sistema encendido tienen un determinado orden de volatilidad que determina la permanencia de esta información disponible para su adquisición, debiendo iniciar este proceso con la recogida de los datos más volátiles y finalizar con los menos volátiles. En general, el grado de volatilidad posee dos niveles;

– la información de la memoria, particiones y archivos de intercambio ("*swap"*), procesos de red y procesos del sistema en ejecución, los cuales son los más volátiles y se pierden al reiniciar o apagar el equipo;

– la información de los sistemas de ficheros y los datos existentes en los sectores de los dispositivos de bloques, los cuales son los menos volátiles;

– se debería tener especial cuidado ante la presencia de discos cifrados o ficheros que exijan palabras de paso para su acceso, así como ante el estudio de *software* dañino o malicioso ("malware") diverso, en cuyo caso, unos correctos procedimientos forenses para la adquisición de la memoria volátil es fundamental para obtener, según los casos, la información en ellos almacenados o para averiguar el tipo de *software* malicioso de que se trate.

7.2.1 Dispositivos móviles

Por la peculiaridad de estos dispositivos de poder interactuar con redes inalámbricas, los dispositivos móviles deben ser protegidos o aislados debidamente a fin de evitar su entrada en contacto con las citadas redes y así evitar la manipulación accidental de los datos en ellos almacenados, impidiendo de esta forma que se produzca el cambio de los ficheros internos con los datos de su posición y celda de radiocomunicaciones.

Una metodología de análisis a seguir con estos dispositivos móviles encendidos debe ser la siguiente:

– previo al análisis de los datos obrantes en el terminal móvil, se debería realizar un proceso de copia o clonado de las partes accesibles de la tarjeta SIM original usando un lector de tarjetas con su *software* específico, y se debe proceder seguidamente a introducir esta tarjeta clon en el terminal móvil. Se reseña que la tarjeta clon al carecer de las claves de acceso a la red inalámbrica de la tarjeta SIM original, impide que este sistema móvil se conecte a dicha red, evitando así tener que procesar las evidencias en el interior de una cámara de Faraday o sistema de similares características;

– posteriormente, una vez arrancado el terminal móvil junto con la tarjeta clon en él insertada, se debe proceder a efectuar una copia a bajo nivel de los datos obrantes en la memoria o memorias internas del dispositivo móvil;

– en el caso de que las herramientas específicas forenses para este fin no soporten algún modelo de dispositivo móvil o no se disponga del cableado adecuado de comunicaciones, se puede optar por la opción de trasladar literalmente al informe pericial la información que se lea en la pantalla visual del mismo, caso de que posea esa posibilidad, o bien, se puede proceder como en el caso de los sistemas apagados. Es decir, se debe extraer la información directamente de la memoria del dispositivo utilizando para ello dispositivos *hardware*, para posteriormente emplear el *software* correspondiente que permita interpretar en claro los datos almacenados en ellas.

Una vez finalizado el análisis de los datos de interés del dispositivo móvil, no se debe introducir ni la batería ni la tarjeta SIM original en el dispositivo, a fin de impedir, caso de su encendido accidental, la alteración del archivo de localización (LOCI) de la SIM, unido a la modificación del listado de llamadas almacenadas.

De toda la información extraída de las memorias del terminal móvil se debe realizar un resumen digital ("*hash*") de su contenido mediante un algoritmo criptográfico, para así garantizar la no alteración de los datos extraídos, caso de tener que efectuar más copias o imágenes de éstos.

7.2.2 Entornos virtualizados

En los entornos virtualizados un equipo físico o varios, están recreados de forma simulada dentro de una máquina física utilizando sus recursos disponibles. En este equipo están en funcionamiento a la vez todos ellos como si se tratará de varios equipos físicos individuales.

Este entorno virtualizado se puede encontrar en un equipo local o en un entorno empresarial y la tecnología utilizada puede implementar una virtualización completa o parcial dependiendo del *hardware* del equipo o del *software* utilizado. Cada una de estas máquinas virtuales consta de varios ficheros, como son el de configuración del *hardware* del equipo, el utilizado para la memoria, y un disco o varios discos duros físicos o virtuales. En este último caso, se corresponderán con varios archivos de imagen de los mismos (extensiones *.vhd, *.vmd, *.img, etc.) que se encuentran en alguno de los dispositivos o sistemas de almacenamiento que tiene disponible el equipo donde se implementa el entorno virtualizado.

Lo que se debe capturar con herramientas forenses es lo siguiente:

– los discos duros virtuales, es decir, copiar los archivos apropiados de este entorno;

– igualmente si se suspende el equipo virtual, se podría obtener un volcado de la parte de la memoria RAM utilizada por el mismo en un archivo, que posteriormente se debe analizar de forma similar al volcado real de la memoria física.

En este ámbito, una vez obtenidos todos los ficheros de configuración de la máquina virtual y los discos virtuales utilizados, se podrá reproducir el mismo entorno original del equipo virtualizado para su análisis forense.

8 DOCUMENTACIÓN

Todo análisis forense requiere un control de calidad de la entrada de las evidencias o muestras forenses al entorno de análisis que va a efectuar su estudio, el cual conlleva implícito la trazabilidad de la cadena de custodia de las mismas.

En este análisis tiene una importancia relevante la planificación íntegra de la metodología a utilizar y la secuencia en que se deben ejecutar los procesos que permitirán la recogida de las evidencias y su posterior análisis.

A tal fin, se debe documentar el procedimiento realizado desde el momento en que se inicia el análisis hasta su finalización, indicando los procesos y herramientas utilizadas así como el momento en que se ejecutaron cada uno de ellos, siguiendo una secuencia temporal claramente definida. Debe elaborarse un registro y éste debe ser auditable.

En consecuencia, la trazabilidad y la propia cadena de custodia de las evidencias electrónicas debe tener implementado un sistema de gestión documental donde se reflejen todos los pasos llevados a cabo por el personal técnico dedicado a estas funciones dentro de una organización. Este sistema debe ser implantado en formato electrónico o en papel, y el mismo debe recoger desde el proceso inicial de adquisición de la evidencia objeto de estudio hasta la finalización de la pericial correspondiente a través de la redacción del informe pericial preceptivo a enviar al organismo o entidad solicitante.

Esta gestión documental, a modo de registro de eventos auditable de la cadena de custodia, conlleva la confección de una serie de documentos o formularios que deben confeccionarse, ya sea a un nivel más genérico del entorno de trabajo o bien a un nivel más concreto, por el personal que realiza el propio análisis forense.

La gestión documental de la cadena de custodia debe incluir, entre otros, los siguientes documentos:

- un documento de recepción de evidencias/muestras electrónicas. Mediante este registro, se lleva el control de entrada de peticiones del análisis, así como de las evidencias a estudiar;

- un registro de la documentación recibida. Los documentos que deben acompañar a una evidencia digital pueden ser los siguientes:

  - descripción de las evidencias electrónicas,

  - reseña de la cadena de custodia hasta la llegada de las mismas al entorno de análisis forense,

  - estudios solicitados en dicho análisis,

  - permisos necesarios para la realización de los estudios solicitados,

- registro de reseña de las evidencias electrónicas. Este documento describe de forma detallada y completa tanto la evidencia digital como el estado en el que se encuentra en el momento de la recepción;

- registro del tratamiento inicial: Se debe detallar el proceso de volcado forense de datos o la realización de la imagen correspondiente;

- registro de situación de evidencias/muestras. Este documento debe reflejar las operaciones llevadas a cabo sobre una evidencia digital, dónde se realizan estas operaciones, por quién y el momento temporal en que se efectúan;

- registro de tareas del análisis inicial;

- registro de tareas del análisis de datos definitivo con la expresión temporal de los distintos procesos que se lleven a cabo, así como de la ubicación temporal de la evidencia si se paraliza temporalmente el estudio de la misma.

9 ANÁLISIS

Entre los procesos y tareas presentados en este capítulo, se deben detallar aquellos que tienen como fin dar respuesta a preguntas relacionadas con el tiempo de intrusión, su origen, lista de sistemas afectados, métodos de intrusión usados, así como la lista de activos alterados y/o accedidos, y cualquier otra actividad realizada en las evidencias objeto de estudio. De igual modo, se debe dar una orientación sobre aquellos aspectos relacionados con los requisitos a cumplir por parte del personal técnico, equipos y documentación en general a tratar. En cualquier caso, todos estos procesos y tareas aquí presentadas se muestran para ser realizadas de forma metódica, auditable, repetible y defendible.

En líneas generales, el análisis de las evidencias digitales debe conllevar la realización de las siguientes acciones y procesos:

Las siguientes son las acciones previas que se deben tener en cuenta en el análisis de las evidencias electrónicas al llegar las mismas a un entorno o laboratorio forense:

1 comprobar que el objeto y alcance de lo que se precisa estudiar está dentro de la competencia de dicho laboratorio o entorno forense;

2 estudiar la documentación adjunta a las evidencias electrónicas para componer un mapa contextual de las mismas, estableciéndose las relaciones que pudiera haber entre las distintas evidencias electrónicas entre sí y de éstas con los distintos actores que están implicados en el hecho que se participa en las cuestiones planteadas para su estudio;

3 supervisar la cadena de custodia previa hasta la llegada de las evidencias o muestras al entorno de análisis forense, dando respuesta a las preguntas de qué, quién, dónde y cuándo se tomaron éstas. Igualmente, se debe comprobar quién fue el responsable y dónde estuvieron almacenadas hasta su llegada al lugar de análisis;

4 solicitar las autorizaciones necesarias, según la legislación vigente a nivel nacional, para el estudio completo de lo solicitado;

5 comprobar que las evidencias no están deterioradas y son susceptibles de su estudio forense;

6 durante este proceso de reseña es posible que aparezcan nuevas evidencias que no habían sido contempladas en un principio durante la toma u obtención de las mismas allí donde estaban ubicadas originariamente, como puede ser la aparición en los distintos dispositivos lectores/grabadores de los equipos informáticos, de tarjetas de memoria, CD, disquetes, etc., en cuyo caso debe iniciarse nuevamente la reseña de éstas, generándose un nuevo proceso de gestión, custodia y trazabilidad de estas evidencias según la Norma UNE 71505. Se debe notificar de forma oportuna la existencia de las mismas a quién solicitó el análisis del resto, requiriendo los permisos correspondientes para su estudio, en caso de ser necesario;

7 especificar la hora de la BIOS del equipo informático donde van instalados los distintos discos duros o soportes digitales que contienen la información de interés, a los efectos de poder ser comparada con la fecha del momento en que se active el análisis forense de la información;

8 se recomienda tener establecidos unos criterios de prioridades.

9.1 Recuperación de los ficheros borrados

Este proceso, cuando se pueda efectuar, consiste en la localización de las entradas de archivos o carpetas borradas en las estructuras de localización de ficheros (tablas tipo FS, MFT, etc.) u otras similares, dependiendo de donde se ubiquen éstos.

Es decir, se debe efectuar una recuperación parcial o total de la información borrada existente en los distintos soportes de almacenamiento, unido a una recuperación de los datos ubicados en las áreas o espacio del disco sin asignar actualmente por el sistema y en el espacio del disco sin utilizar, así como la obtención de las carpetas y archivos "huérfanos" contenidos dentro de los distintos ficheros, de los que se ha perdido su vinculación.

Igualmente, este proceso consiste en una búsqueda, a través de sus cabeceras, de archivos completos o fragmentos de éstos existentes en los dispositivos de almacenamiento.

A los efectos de asegurar la trazabilidad de toda la información recuperada, se debe determinar claramente en el informe pericial que se elabore, de dónde se ha extraído la misma y el método usado para dicha recuperación.

9.2 Estudio de las particiones y sistemas de archivos

Este proceso consiste en el estudio de las diversas estructuras de los contenedores de almacenamiento de los dispositivos (particiones, volúmenes físicos, sistemas RAID, etc.), en los que se puedan encontrar diferentes volúmenes lógicos que contienen los sistemas de archivos. Cada una de estas estructuras pueden ser diferentes según el tipo de sistema de particionado utilizado.

Este proceso también debe incluir entre sus tareas básicas las siguientes:

– una enumeración de los contenedores o de las particiones actuales y de las que hubieran podido existir anteriormente;

– así mismo, se deben identificar las zonas o espacios de disco ocultos, como las HPA, DCO u otras que pudiera haber según la tecnología del fabricante;

– también se debe realizar la identificación de los distintos sistemas de archivos que pudiera haber en los contenedores o en las particiones, con la identificación del contenedor que almacena el sistema operativo de inicio y tipo de arranque o selector multiarranque;

– se deben identificar los sistemas de archivos de los discos compactos, en especial, se deben identificar las distintas pistas de las sesiones de grabación que pueden existir en los diferentes formatos de estos medios, así como la identificación de los archivos cifrados y/o protegidos con contraseña, unido a la localización de los volúmenes o discos cifrados;

– finalmente, se debe proceder al montaje de archivos contenedores de otros, como pueden ser los comprimidos, compuestos, empaquetados, verificando las cabeceras de los distintos formatos de archivos y sus resúmenes digitales.

En el caso del análisis de la memoria RAM, se debe estudiar, para un momento temporal concreto, los procesos activos, los ficheros abiertos, los puertos y tomas de corriente activas, así como, entre otros datos de interés, las distintas claves de acceso a los programas o volúmenes cifrados del soporte de almacenamiento físico correspondiente.

9.3 Estudio del sistema operativo

Este proceso consiste en el estudio del sistema o sistemas operativos instalados en los volúmenes lógicos de los dispositivos de almacenamiento, la actividad de los usuarios existentes en el mismo y su política de seguridad.

Dicho proceso debe englobar distintos pasos, como son los siguientes:

– la identificación del sistema operativo principal del equipo y su localización;

– la identificación del sistema o sistemas operativos utilizados, su fecha de instalación, así como sus revisiones o actualizaciones;

– la identificación de los distintos usuarios con sus privilegios y permisos dentro del sistema operativo;

– las fechas de último acceso al equipo de cada uno de ellos y su política de seguridad;

– la identificación de los dispositivos de *hardware* y de *software* reconocidos por el sistema o que pudieran haber estado instalados anteriormente.

9.4 Estudio de la seguridad implementada

Este proceso tiene por finalidad estudiar si las evidencias electrónicas remitidas para su estudio han sido comprometidas. Existen distintos grados de vulnerabilidad de las evidencias electrónicas objeto de análisis, bien por métodos de intrusión, modificación, eliminación y sustracción de la información almacenada en los soportes originales.

Se debe identificar el *software* malicioso (virus, troyanos, etc.) que pudiera existir en las distintas particiones identificadas, evaluando el grado de intrusión en el sistema informático y qué archivos se han visto comprometidos, identificando de qué modo.

9.5 Análisis detallado de los datos obtenidos

Incluye el análisis detallado de las evidencias electrónicas, aprovechando todos los análisis previos ya especificados. Para ello se debe utilizar *software* contrastado en el ámbito forense. Igualmente, este análisis se debe ajustar estrictamente a las cuestiones planteadas por el organismo o entidad que solicita el estudio forense.

Este análisis conlleva la realización al mismo tiempo de una clasificación de los datos, así como opcionalmente de un proceso previo de indexado de los mismos, el cual agilizará posteriormente las distintas búsquedas de los indicios a encontrar en los soportes digitales, utilizando para ello distintas palabras clave o códigos alfanuméricos preparados al efecto. Es conveniente reflejar las palabras o criterios de búsqueda implementados para efectuar este indexado.

En este proceso de indexado se deben aislar los archivos en los que no se puede observar a priori el texto que contienen en claro, como por ejemplo, los archivos comprimidos, pues su información quedaría sin indexar. Una vez tratados, se deben añadir al proceso general de indexación. Este proceso también permite descartar del análisis detallado posterior de los datos digitales, los ficheros que pertenecen a aplicaciones comerciales instaladas en el soporte de almacenamiento digital.

Un análisis forense detallado de las evidencias electrónicas, sin ánimo de ser exhaustivos, debe contemplar los siguientes estudios:

1 Determinación de información del sistema: *hardware* instalado y reconocido por el sistema operativo, fecha, hora y usuario de la última actividad del sistema, datos de la configuración regional, etc.

2 Estudio de los dispositivos físicos conectados en algún momento al equipo informático: agendas personales digitales, teléfonos móviles, lápices de memoria, impresoras, escáneres, equipos multifunción, cámaras fotográficas y de vídeo, tarjetas de memoria y otras unidades de almacenamiento externo.

3 Estudio del escritorio o pantalla principal de visualización y su papelera de reciclaje.

4 Las conexiones de red y las tarjetas instaladas con identificación de la MAC, además de los protocolos usados y direcciones IP.

5 Estudio de las comunicaciones habidas desde el equipo informático.

6 Estudio del registro del sistema y registros ("*logs"*) de auditoría del propio sistema operativo.

7 Información contenida en los espacios no asignados en las particiones y en el espacio físico no ocupado por los archivos lógicos, entre el cual se incluyen las áreas o espacio del disco sin asignar actualmente por el sistema.

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

9 Análisis de la cola de impresión.

10 Visualizar los enlaces a archivos, así como los archivos accedidos de forma reciente.

11 Estudio de las carpetas de los distintos usuarios.

12 Estudio de las aplicaciones instaladas relativas a programación, grabación y tratamiento de imágenes, procesamiento de audio, imagen y vídeo, *software* de uso contable y de gestión económica, programas ofimáticos, etc.

13 Estudio de los metadatos, cuando sean de interés.

14 Análisis de aplicaciones de virtualización, con el fin de determinar los soportes virtuales creados y su configuración.

15 Estudio de las bases de datos instaladas y sus sistemas gestores.

16 Estudio de *software* de cifrado y los ficheros y particiones cifradas, así como la posibilidad de que el mismo venga implementado en el sistema operativo.

17 Estudio de la navegación por Internet, con determinación de las "*cookies*" y análisis de la distintas carpetas que presenten historial de navegabilidad en dicha red.

18 Análisis de los correos electrónicos y correos vía web.

NOTA No se entra en esta norma a debatir los condicionamientos legales que exige el análisis forense de los correos electrónicos.

19 Análisis de los registros de mensajería instantánea y conversaciones (conocidas como "*chats"*), junto con las listas de contactos.

10 PRESENTACIÓN

El análisis forense realizado se debe materializar en un informe pericial, el cual debe compaginar los términos técnicos con un lenguaje de fácil comprensión dirigido al organismo o entidad que solicitó dicho estudio, en la idea de que el público objetivo del mismo no tiene por qué ser personal técnico ni entender en profundidad de las nuevas tecnologías.

A los efectos de esta norma el término de "informe pericial" se considera equivalente al término de "informe técnico-forense".

Para la confección de la parte general del mismo, se tendrá en cuenta la Norma UNE 197001, con la particularidad de que en este caso, su contenido versa sobre aspectos técnicos propios de las tecnologías de la información.

Una vez redactado el informe pericial correspondiente, se deben remitir al organismo solicitante del estudio los equipos y soportes digitales estudiados, yendo éstos acompañados del correspondiente recibo o documento de control de evidencias. Dicho recibo, debidamente cumplimentado, debe devolverse al organismo u empresa que lo emite, una vez haya llegado el informe y las muestras objeto de estudio al organismo o entidad que lo solicitó, dando así por finalizado la trazabilidad y el proceso de custodia de las evidencias objeto del análisis forense.

ANEXO A (Informativo)

MODELO DE INFORME PERICIAL

Tomando como referencia el modelo de informe propuesto por la Norma UNE 197001, en el apartado relativo al cuerpo del informe, deben incluirse los siguientes apartados:

1.- Asunto

Se deben especificar los estudios solicitados, identificación del entorno de análisis forense o en su caso, laboratorio que emite el informe y los datos identificativos de forma nominal de los peritos que han efectuado el análisis de los distintos soportes digitales, reseñando igualmente la fecha de inicio y fin de estos estudios.

2.- Evidencias/muestras recibidas

Se deben reseñar todas las muestras objeto de análisis, las cuales se deben visualizar en un anexo fotográfico o videográfico que debe acompañar al cuerpo del informe en un anexo.

3.- Resolución o estudios efectuados sobre las evidencias/muestras

Constituye el cuerpo del informe pericial propiamente dicho. Aquí se deben incluir todos los análisis previos descritos en esta norma así como en detalle, el apartado correspondiente al análisis de los datos, reflejándose, por tanto, los siguientes subapartados:

1 Descripción del proceso de clonado bit a bit de la información original o procedimiento seguido para obtener los datos copia que han servido para el estudio de las evidencias correspondientes.

2 Análisis de las particiones y sistemas de ficheros.

3 Proceso de recuperación de archivos borrados, si ha lugar.

4 Estudio del sistema operativo y usuarios del mismo.

5 Estudio de la seguridad implementada.

6 Análisis detallado e individualizado, para cada soporte digital, de los indicios encontrados de interés de las distintas evidencias electrónicas. Se deben reseñar a lo largo de este análisis, en los anexos correspondientes, los indicios encontrados perfectamente clasificados, con sus rutas de ubicación en los soportes originales.

4.- Situación final de las evidencias/muestras

Una vez finalizados los estudios reflejados en el apartado anterior, se debe especificar el destino final que se dará a las evidencias una vez concluido su análisis, reseñando para todas ellas el medio utilizado para la puesta a disposición del organismo o entidad solicitante de esta pericial.

5.- Conclusiones finales

Se deben extractar las principales conclusiones que se determinen de los estudios efectuados sobre las evidencias electrónicas. Los resultados del informe pericial deben de responder a las expectativas de quien lo solicitó, siendo claros y concisos. Para ello se debe usar un lenguaje llano sin tecnicismos ni ambigüedades.

6.- Anexos del informe

Toda la información de interés se debe adjuntar en los correspondientes anexos, bien en formato papel o en formato electrónico. En este último caso, a los soportes con los datos de interés se les debe realizar un resumen digital o "hash" para garantizar la no alterabilidad de los mismos para su puesta a disposición del organismo o entidad que lo solicita.

Finalmente, el informe pericial debe ser firmado por los peritos y otros responsables del entorno de análisis forense que lo emite, según el plan de calidad instaurado en el mismo, o bien, se puede firmar digitalmente por los mismos actores anteriores, procediéndose ahora a su remisión final al organismo o entidad que lo ha solicitado.

ANEXO B (Informativo)

COMPETENCIAS PARA EL ANÁLISIS FORENSE DE LAS EVIDENCIAS ELECTRÓNICAS

Independientemente de que en una organización o entidad exista o no una política de calidad, el personal técnico dedicado a estos cometidos debería poseer unos requisitos mínimos globalmente aceptados en el ámbito forense relacionado con las evidencias electrónicas.

Este Anexo orienta de forma genérica sobre las competencias con que ha de contar el personal involucrado en las diversas fases del análisis forense, ya que la integridad y autenticidad de las evidencias electrónicas encontradas depende en gran manera de su labor. De este modo se establecen una serie de pautas a seguir, de cara a afianzar un proceso de cualificación sobre los candidatos que han de desarrollar alguna tarea en el ámbito del análisis forense relacionado con las nuevas tecnologías. Estas recomendaciones se amplían en la Guía "*CEN/Guide 14 Common policy guidance for addressing standardisation on qualification of professions and personnel*".

En primer lugar se ha diferenciar claramente el significado entre conocimientos y competencias, refiriéndose el primero a la asimilación de información a través de cualquier acción formativa, y el segundo a la habilidad demostrada para aplicar ese conocimiento en la resolución de tareas y problemas específicos. De igual modo, se ha de atender a la legislación existente en cada país respecto de los diplomas y/o certificados existentes en su sistema educativo. El ámbito de estas recomendaciones es aplicable para todos aquellos que desarrollan, ofrecen y buscan una actividad profesional en este ámbito, así como aquellos que evalúan las competencias y/o requieren de una cualificación.

A continuación se indican las diferentes categorías de competencias que se deberían considerar:

– **Técnicas:**

  - Conocimiento de la legislación vigente en lo concerniente a la relevancia digital de las evidencias forenses y de cómo éstas han de estar tratadas en todo su ciclo de vida para no perder validez.
  - Conocimiento del *software* y *hardware* forense existente en la industria actual.
  - Entrenamiento adecuado en labores de manejo de la evidencia digital.
  - Conocimientos en labores de identificación de la información forense.
  - Conocimientos de los diversos sistemas de ficheros existentes.
  - Conocimientos sobre los métodos existentes de extracción de contraseñas.
  - Conocimientos sobre los diferentes elementos de Internet que pueden ser almacenados en un sistema.
  - Conocimientos sobre las distintas técnicas y herramientas usadas en el fraude informático.
  - Conocimientos sobre los principales métodos usados por los intrusos informáticos.

– **Profesionales:**

  - Experiencia previa en las tareas a desempeñar en las diferentes fases del análisis forense.
  - Formación continua en el ámbito forense.

– **Personales:**

  - Honestidad, discreción y cumplimiento del oportuno código de práctica profesional.

- Espíritu crítico e independiente, de mente abierta para tomar en consideración diferentes opiniones y puntos de vista.
- Perseverancia, autodisciplina, con capacidad de aprendizaje y adaptación a nuevos escenarios.
- Capacidad de observación, análisis y extracción de conclusiones basadas en el razonamiento y análisis lógico.
- Capacidad de describir situaciones y fenómenos complejos en términos comprensibles.

ANEXO C (Informativo)

EQUIPAMIENTO PARA EL ANÁLISIS FORENSE DE LAS EVIDENCIAS ELECTRÓNICAS

Todo entorno o laboratorio forense que se reconozca con las competencias descritas en esta norma debe contar con *hardware* y *software* reconocido por la comunidad forense internacional para dichos fines. La no existencia de una normalización a nivel mundial en este aspecto no entra en contradicción con la necesidad de cumplir para ambos aspectos con las recomendaciones genéricas reseñadas en este anexo, las cuales son las que se siguen básicamente en todos los laboratorios o entornos forenses de reconocido prestigio dentro del análisis de las evidencias electrónicas asociadas a las tecnologías de la información.

***Hardware* forense:**

Este *hardware* puede estar integrado básicamente, por dispositivos electrónicos que permitan las siguientes funcionalidades:

- Efectuar un duplicado forense con el que obtener capturas/adquisiciones de un clon forense o imagen fiel de los datos originales, tanto en un entorno forense como en el lugar de trabajo donde ocurrió el incidente. Dichos elementos han de permitir acceder de igual modo a cualquier área protegida, siendo capaces de operar también sobre dispositivos de memoria u otros elementos de almacenamiento digital de datos.
- Acceder a los distintos soportes magnéticos sin alterar su contenido.
- Permitir extraer datos de los dispositivos móviles.
- Opcionalmente, contar con aceleradores *hardware* para la recuperación de contraseñas.
- Estar dotados de sistemas de bloqueo de escritura sobre los soportes originales.

***Software* forense:**

El *software* forense que se utilice debería, como mínimo, permitir las siguientes funcionalidades:

- Efectuar una captura exacta de los datos hallados en el dispositivo o medio bajo estudio.
- Generar resúmenes digitales ("*hash*") de dichas imágenes o clonados forenses, pudiendo así mantener la validez legal de los datos para su uso en procedimientos judiciales.
- Indexar por tipos de documentos y procesos para obtener una base de datos con todos los elementos de análisis fácil de operar.
- Tener la posibilidad de obtener informes forenses de diversa precisión, con los que presentar la información hallada ante cualquier autoridad legal o gerencia que lo solicite.
- Parametrizar la granularidad de la adquisición.
- Recuperar archivos y carpetas eliminadas.
- Recuperar particiones, pudiendo reconstruir la estructura de los volúmenes.
- Analizar los archivos de registro y configuración de los dispositivos *hardware* bajo estudio.
- Analizar los resúmenes digitales ("*hash*") existentes.
- Analizar las firmas de archivos.

- Tener la posibilidad de realizar búsquedas en el espacio de disco no asignado.
- Generar listados detallados de archivos, carpetas y direcciones URL junto con las fechas y horas de visita a las mismas.
- Poder reconstruir los artefactos de Internet, siendo los principales los relacionados con la navegación web, el correo electrónico, las herramientas de intercambio de ficheros y la mensajería instantánea.
- Recuperar los archivos de registros ("*logs*") de seguridad y las trazas de los paquetes de red.

AENOR Asociación Española de Normalización y Certificación

Génova, 6
28004 MADRID-España

info@aenor.es
www.aenor.es

Tel.: 902 102 201
Fax: 913 104 032