Análisis Forense Informático

Análisis Forense Informático

Mario Guerra Soto

Ra-Ma®

La ley prohíbe
fotocopiar este libro

Análisis Forense Informático

Editado por:
RA-MA Editorial
Calle Jarama, 3A, Polígono Industrial Igarsa
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: *editorial@ra-ma.com*
Internet: *www.ra-ma.es* y *www.ra-ma.com*
ISBN: 978-84-1897-124-2
Depósito legal: M-26476-2021
Maquetación: Antonio García Tomé
Diseño de portada: Antonio García Tomé
Filmación e impresión: Safekat
Impreso en España en octubre de 2021

A mi familia,
de la que escribir este libro
me ha privado tanto tiempo.

ÍNDICE

ACERCA DEL AUTOR

Mario Guerra Soto es Ingeniero de Telecomunicación por la Universidad de Cantabria (UC). Durante siete años trabajó en el Mando Conjunto de Ciberdefensa como DFIR, *threat hunter*, analista de ciberinteligencia, y analista de *malware*. Es Máster en Seguridad de Tecnologías de Información y Comunicación por la Universitat Oberta de Catalunya (UOC), y Máster en Análisis de Evidencias Digitales y Lucha contra el Cibercrimen por la Universidad Autónoma de Madrid (UAM). Dispone de las certificaciones en ciberseguridad GCFA, GCTI, GREM, CEH, CHFI, CND, CCPA, CASA y KAPE. Además, ha realizado otros cursos relacionados con la ciberseguridad, como el de Cyber Security Professional por la NATO School of Oberammergau, y el Curso de Especialidades Criptológicas por el Centro Criptológico Nacional (CCN). Ha colaborado como ponente en diferentes CON nacionales como RootedCON, Cybercamp, C1b3rwall, IntelCon, Hackron y TACS. Colabora como docente en el programa de postgrado de la UAM y de la Universidad de Salamanca (USAL).

1

INTRODUCCIÓN A FORENSE DIGITAL

1.1 CONCEPTOS BÁSICOS

1.1.1 Definición de forense digital

La Ciencia Forense juega un papel fundamental en las investigaciones criminales. Debe entenderse como una aproximación multidisciplinar que permite juntar todo tipo de evidencias en una investigación. Normalmente, durante el transcurso de una investigación, deberán aplicarse los principios y metodologías de diferentes disciplinas científicas para la presentación de evidencias ante un tribunal.

En 1910, el francés Edmond Locard establece el primer laboratorio forense policial en Lyon. Pasa además a la historia de la ciencia forense por enunciar el denominado **Principio de Locard** "*Todo contacto deja una huella*". Es decir, que la presencia del autor de los hechos en la escena del crimen conlleva una transferencia de evidencias, pues el criminal deja rastros en la escena del crimen, pero también lleva consigo evidencias que demuestran su presencia en dicho lugar. Dicho de otra forma, las acciones físicas dejan evidencias físicas en el mundo físico; las acciones digitales dejan evidencias digitales en el mundo digital.

Actualmente, entre las diferentes ramas de la Ciencia Forense destacan: Toxicología, Psicología, Podología, Patología, Odontología, Lingüística, Geología, Entomología, Ingeniería, Análisis de ADN, Botánica, Arqueología, Antropología, Balística y Digital.

Podría definirse Forense Digital como la disciplina que combina elementos legales, informáticos y de telecomunicaciones para obtener y analizar evidencias

digitales (Ej. Ordenadores, tráfico de red, dispositivos de almacenamiento, teléfonos móviles, *smartphones*, *wearables*) de modo que sean admisibles ante un tribunal. Si bien a primera vista su principal aplicación sería la investigación de cibercrímenes, el nivel de digitalización de la sociedad moderna provoca que, en la mayoría de los casos, sea necesario el análisis de una o más evidencias digitales.

A su vez, Forense Digital puede subdividirse en diferentes ramas: forense de ordenadores, análisis forense de información, forense de bases de datos, forense de red, forense de dispositivos móviles y forense de vídeo/audio.

Uno de los aspectos más complejos de las investigaciones forenses digitales consiste en determinar el papel que desempeña el dispositivo en el incidente objeto de estudio. En general, los dos roles que puede adoptar el dispositivo son:

- La herramienta empleada para realizar la acción objeto de estudio, es decir, el *arma del crimen*.
- El objetivo de la acción objeto de estudio, es decir, el *cadáver*.

Un ejemplo que permite ilustrar la clasificación anterior sería un escenario en el que un agente malicioso consigue tomar el control del equipo de un usuario de una organización. El atacante podría utilizar ese equipo bajo su control para intentar acceder a un servidor de ficheros dentro de dicha organización y exfiltrar información (entiéndase por exfiltrar la extracción ilícita de información sin conocimiento de su legítimo propietario). En este escenario, el equipo controlado por el atacante es la herramienta, mientras que el servidor es el objetivo. No obstante, si el atacante hubiese exfiltrado información del equipo corporativo bajo su control, este equipo sería a la vez la herramienta y el objetivo del ataque.

El dispositivo debe ser considerado la escena del crimen digital, pues contiene las evidencias digitales que permitirán al investigador forense digital determinar cuándo (*When*) y cómo (*How*) el ataque tuvo lugar. Adicionalmente, podrían obtenerse evidencias que demostraran quién (*Who*), qué (*What*), dónde (*Where*) y por qué (*Why*) realizó el ataque. Las famosas 5WH a obtener en toda investigación forense.

En forense digital, separar la parte legal de la parte técnica puede ser en ocasiones complicado. Los avances técnicos alteran los tipos de evidencia que pueden ser obtenidos; las modificaciones en las leyes afectan el modo en el que las evidencias pueden ser obtenidas y si esas evidencias serán admisibles ante un tribunal.

El reconocimiento de la importancia de las investigaciones forenses digitales tiene su primer hito con la creación en 1984 por el FBI del CART (*Computer Analysis and Response Team*).

La capacidad de determinar con prontitud el impacto de un ataque, la identidad del atacante y sus posibles objetivos son una muestra de los beneficios aportados a una organización por la disciplina de forense digital. Otros beneficios adicionales serían el mantenimiento del estado operacional de sistemas informáticos y redes, además de poder facilitar a las FCSE (Fuerzas y Cuerpos de Seguridad del Estado) la información necesaria de las actividades maliciosas llevadas a cabo por empleados maliciosos haciendo uso de los equipos y redes corporativas.

Existe cierta controversia a la hora de determinar qué es un cibercrimen. En general, suele considerarse que una actividad delictiva es un cibercrimen cuando solo pueda cometerse empleando ordenadores o comunicaciones digitales. Es decir, acceso ilegal a sistemas informáticos, distribución de *malware*, manipulación de aplicaciones informáticas, fraude en apuestas ilegales, ataques DoS (*Denial of Service*), *webjacking*, contrabando de identidades digitales y uso ilegal de equipos de telecomunicaciones contra dispositivos en red (Ej. *Eavesdropping*, creación de identidades digitales fraudulentas).

Por un lado, el atacante podría haber utilizado el dispositivo como herramienta para la comisión del delito (Ej. Acceder a un sistema remoto, envío de mensajería digital, videoconferencia). Por otro, el dispositivo pudiera ser el objetivo del ataque (exfiltración, modificación o borrado de información). Por tanto, el dispositivo será la escena del crimen en la cual hay que preservar las evidencias (Ej. Archivos de *log*, aplicaciones instaladas, línea temporal de actividades). Algunas de estas evidencias (Ej. Memoria RAM, tablas ARP, conexiones de red) tendrán un elevado grado de volatilidad (es decir, que su grado de permanencia con respecto del tiempo es limitada), debiendo ser por tanto obtenidas con la mayor presteza posible o desaparecerían. En cambio, otras evidencias (Ej. Archivos en disco duro, soporte óptico) tendrán un grado de volatilidad menor o, dicho de otro modo, su grado de persistencia será mayor.

Resulta por tanto necesario dentro de una organización que exista un equipo con las capacidades técnicas y recursos necesarios para poder hacer frente a un incidente concreto. La seguridad informática puede ser vista como un triángulo donde uno de sus lados lo constituye la detección y respuesta a intrusiones, siendo sus otros dos lados el análisis de vulnerabilidades y las investigaciones informáticas.

La detección de intrusiones, el análisis de vulnerabilidades y las investigaciones informáticas están directamente relacionadas con diferentes controles de seguridad que pueden ser implementados en una organización. El análisis de vulnerabilidades identifica los fallos a corregir o mitigar; la detección y respuesta a intrusiones representan controles de investigación y compensación; y las investigaciones intentan analizar el origen y establecer los pertinentes controles preventivos.

1.1.2 Investigaciones corporativas e investigaciones criminales

Existen dos tipos de investigaciones en el ámbito forense digital:

- **Investigaciones criminales**. Son aquellas que tienen lugar dentro del ámbito de un delito (civil o penal). Las consecuencias legales para los autores pueden ser económicas y/o pena de prisión, según el delito cometido.

- **Investigaciones corporativas**. Son aquellas que persiguen la violación de la política corporativa. Ejemplos de violación de la política corporativa serían acceder a sitios de apuestas deportivas o con contenido pornográfico utilizando los recursos de la red corporativa. Algunas investigaciones corporativas pueden derivar en investigaciones criminales (Ej. Distribución de pornografía infantil o exfiltración de propiedad intelectual desde el ordenador corporativo). Las consecuencias legales de las investigaciones corporativas pueden conllevar el despido y/o resarcimiento económico a alguna de las partes.

Dado que algunas investigaciones corporativas pudieran desembocar en investigaciones criminales, resulta una buena estrategia implicar a los equipos legales y de recursos humanos de la corporación desde el comienzo de la investigación.

Es importante señalar que hay que estar autorizado para llevar a cabo una investigación forense digital. La autoridad responsable de autorizar una investigación varía en función de la naturaleza de la investigación. Para las investigaciones criminales, será necesario disponer de una orden judicial. Para las investigaciones corporativas, tendrá que estar regulado previamente el ámbito de la investigación por el departamento legal y de recursos humanos.

Un investigador forense digital actuará como experto en los procesos de detección y obtención de evidencias, garantizará el mantenimiento de la cadena de custodia de la evidencia, analizará la evidencia y presentará los resultados de la investigación.

El rol del investigador forense digital se solapa con el del respondedor de incidentes. Pese a que se utilizan las mismas herramientas en ambos roles, el objetivo de ambos es muy diferente, y cada actividad tiene su propio conjunto de procesos y procedimientos.

1.1.3 Diferencias entre E-Discovery y forense digital

Se entiende por *E-Discovery* (*Electronic Discovery*) el proceso que implica la recogida, preparación, revisión, interpretación y presentación de documentos electrónicos procedentes de soportes de almacenamiento en litigios civiles.

E-Discovery	Forense digital
Litigios civiles	Investigaciones criminales
No implica datos eliminados	Pueden recuperarse datos eliminados
Centrado en los datos del espacio asignado del soporte de almacenamiento	Incluye los datos presentes en el espacio asignado y en el espacio no asignado.
Recuperación de datos limitada	Búsqueda de datos sin límite
Testimonio basado en hechos	Testimonio basado en la experiencia del forense

Tabla 1. Diferencias entre E-Discovery y forense digital.

1.1.4 Definición de evidencia digital

A medida que fueron apareciendo un mayor número de dispositivos (Ej. *Smartphones*, tabletas, ordenadores portátiles, *netbooks*, reproductores de audio) que hacían uso de las comunicaciones digitales, el término forense digital fue aumentando su popularidad al resultar más preciso para definir el amplio abanico de dispositivos que puede abarcar una investigación forense digital.

La información digital se representa mediante una serie de dígitos binarios (‘*1*’ y ‘*0*’), generalmente referenciados como bits; 4 bits conforman un *nibble* (útil por ejemplo para representar la información en base hexadecimal, con valores de *0* a *F*); 8 bits conforman un byte. Estos bits son únicamente inteligibles para el ser humano cuando se establece un formato sobre la información y se interpreta la información bajo las reglas de esa estructura. Si se intenta visualizar un archivo binario en código ASCII, obtendremos que algunos de sus bytes son representables (tienen un valor correspondiente dentro de la tabla de caracteres ASCII) y otros no. Cualquier tipo de información puede representarse digitalmente: audio, vídeo, texto, imágenes y aplicaciones informáticas. Toda esta información puede ser transmitida y almacenada en un conjunto de bytes denominado archivo o fichero.

Se conoce como investigación digital al examen realizado sobre una evidencia digital motivado por la relación existente entre el dispositivo del que se obtuvo la evidencia digital con el incidente objeto de estudio. La investigación se

lleva a cabo desarrollando una hipótesis de lo ocurrido y buscando evidencias que puedan refutar dicha hipótesis.

Evidencia digital es un objeto digital que contiene información fiable que apoya o refuta una hipótesis. Esta definición de evidencia refleja su utilización en investigaciones científicas.

Desde un punto de vista legal, una evidencia digital (o electrónica) es cualquier información probatoria almacenada o transmitida en formato digital que cualquiera de las partes presenta como prueba ante un tribunal.

Por tanto, una investigación forense digital es un proceso que utiliza la ciencia y la tecnología para analizar los objetos digitales obtenidos, desarrollando hipótesis y comprobando teorías para ser llevadas ante un tribunal, pudiendo contestar a las preguntas referentes a lo ocurrido.

Las investigaciones forenses digitales son un subconjunto de las investigaciones digitales, a las cuales se las aplica un conjunto restrictivo de normas motivadas por el propio proceso forense. Ambas investigaciones utilizan objetos digitales, pero difieren en el modo de utilizarlos.

El DFIR deberá tener cuidado en la obtención, procesado y almacenamiento de objetos digitales. Salvo que se esté completamente seguro de que la evidencia no va a ser utilizada ante un tribunal, resulta conveniente extremar las precauciones con las evidencias digitales, de modo que el investigador no acometa ninguna acción que anule la validez de la evidencia ante un tribunal. En muchas ocasiones, lo que comienza como una simple investigación corporativa de un incidente, termina convirtiéndose en una investigación criminal.

El National Justice Institute de EE.UU. publicó en noviembre de 2009 un documento referencia, "*Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders*". Este documento lista 14 categorías diferentes de crimen y 60 tipos diferentes de crímenes electrónicos y evidencias digitales. En general, si es un dispositivo electrónico que pueda almacenar información, entonces es una potencial fuente de evidencias.

1.1.5 Principios internacionales de evidencia digital

El crecimiento del número de dispositivos electrónicos existentes durante los años 90 hizo necesario la elaboración de estándares internacionales para facilitar la comunicación y compartición de información, además de estandarizar los procedimientos.

La IOCE (*International Organization on Computer Evidence*) se creó en 1995 para desarrollar estándares internacionales relativos a evidencias digitales. En su guía de 2002, titulada "*Guidelines of Best Practice in the Forensic Examination of Digital Technology*", se sustituye el concepto de evidencia informática por el de evidencia digital. Esta guía cubre un amplio espectro de buenas prácticas para implementar una capacidad forense, incluyendo equipamiento, formación y necesidades organizacionales.

1.1.6 Registros generados y registros almacenados por un ordenador

El Departamento de Justicia de los EE.UU. define como registros generados por ordenador aquellos generados por una aplicación informática en ejecución, mientras que se define como registros almacenados por ordenador aquellos registros o archivos que contienen información generada por un agente humano.

Registros generados por ordenador

En general, los registros almacenados en un ordenador se consideran evidencias "de oídas" (*hearsay*). En los países anglosajones, este término hace referencia al informe que un testigo aporta sobre las palabras pronunciadas por un tercero, siendo poco frecuente que sean aceptadas ante un tribunal. En cambio, cada vez es mayor la aceptación de los registros generados por ordenador (Ej. *Registro de Windows*, *Eventos de Windows*), especialmente si constituyen parte de la actividad habitual del negocio de la organización. Es decir, que si la organización recopila de forma sistemática la actividad de los dispositivos (Ej. Archivos de *log* de navegación de los usuarios) del entorno corporativo, la probabilidad de que sean aceptados ante un tribunal será mayor.

Conviene reseñar que los archivos de *log* adquiridos de manera adicional pueden no ser admitidos ante un tribunal. Un ejemplo sería cuando, ante la sospecha de que se está llevando a cabo actividad maliciosa desde un dispositivo del entorno corporativo, se decide realizar un volcado completo del tráfico de red, cuando normalmente solo se registran las URL accedidas por los usuarios. No obstante, si el incremento de los archivos de *log* estuviese tipificado previamente dentro del procedimiento de respuesta a incidentes de la organización, aumentarían las probabilidades de que la evidencia resultase admisible ante un tribunal.

Los registros generados por ordenador deben ser autenticados. La autenticidad (identificación) de ese registro generado por ordenador puede ser establecida mediante testimonio del individuo que creó o configuró la creación de ese archivo (Ej. El administrador del sistema). No obstante, para saber si el software

que generó el registro es o no de confianza, suele ser de ayuda el demostrar que el registro generado por ese software es utilizado a nivel interno de la corporación como entrada de otro proceso durante el funcionamiento normal del negocio. De este modo, demostrar la fiabilidad del software que generó el registro aumentará las probabilidades de admisión ante un tribunal de un registro obtenido fuera del funcionamiento normal del negocio.

1.1.7 Cadena de custodia

La cadena de custodia contribuye a garantizar la autenticidad de los registros generados por ordenador. Una cadena de custodia es un registro documental de quién estaba en posesión y control de una determinada evidencia en cada momento, hasta que dicha evidencia es presentada ante un tribunal. Existen documentos estándar para estos formularios de cadena de custodia. En general, la información principal que deben recoger estos formularios es la fecha y hora de transferencia, quién hizo la entrega, quién la recepción y el motivo de la transferencia de la evidencia.

La cadena de custodia es una parte significativa de toda la cadena de evidencia. Un formulario de cadena de evidencia incluye la búsqueda, recogida y catalogación de una evidencia una vez que ha sido obtenida. El formulario generalmente incluye información como número de caso, fecha de obtención de la evidencia, lugar de obtención y la lista y números de objetos de esta evidencia. Esto permite realizar el seguimiento de una evidencia en particular dentro del sistema judicial.

1.1.8 Recopilación de evidencias digitales

Recopilación de evidencias "en vivo" (*live*)

La recopilación de datos se realiza con el dispositivo encendido, y su sistema operativo, servicios y herramientas en ejecución. Es decir, el investigador estará *logueado* en el sistema, ya sea utilizando su consola local, su GUI o mediante software de acceso remoto, y la recopilación se realizará mientras están siendo utilizados los recursos del propio sistema objeto de la investigación (Ej. Memoria RAM, conexiones de red).

El normal funcionamiento del sistema operativo irá modificando rápidamente el contenido de los registros del procesador (datos necesarios para la ejecución de los programas) y los datos presentes en la memoria RAM (Ej. Procesos en ejecución, conexiones de red abiertas, contraseñas de usuario, archivos en uso). Adicionalmente,

si el sistema operativo se reiniciase o el dispositivo se apagase, esta información se perderá, de ahí que se considere altamente volátil.

Por tanto, la recopilación de datos altamente volátiles será equivalente a una "fotografía" (*snapshot*) del instante en el cual se produjo la recopilación de evidencias, pudiendo variar los resultados de manera notoria dependiendo del instante en el cual se realice la captura. Estos datos serán de especial importancia cuando el objeto de la investigación es determinar la presencia de actividad potencialmente maliciosa en el sistema, pero también pueden permitir recopilar credenciales que habiliten el acceso a potenciales fuentes de evidencias (Ej. Perfiles del usuario en redes sociales, correo electrónico web, almacenamiento en la nube, volúmenes cifrados).

No obstante, cuando en una investigación la recopilación de evidencias se realiza "en vivo", las propias acciones llevadas a cabo por el investigador (Ej. Ejecución de una herramienta de volcado de memoria RAM desde la consola del sistema operativo) contaminarán el escenario, debiendo ser pertinentemente documentadas como apoyo para la posterior fase de análisis de las evidencias.

Recopilación de evidencias "en muerto" (*dead*)

Este tipo recopilación de evidencias se realiza cuando el dispositivo objeto de la investigación se encuentra inicialmente apagado o resulta absolutamente necesario apagarlo para proceder a la extracción de los datos de sus soportes de almacenamiento. También hace referencia a la copia o clonado de soportes de almacenamiento externos (Ej. Memorias USB, discos externos USB, soportes de almacenamiento ópticos) que no estuviesen conectados a un dispositivo encendido cuando se fuese a proceder a la recopilación de evidencias.

En determinados escenarios, será posible extraer los soportes de almacenamiento internos del dispositivo objeto de la investigación y proceder a su copia bit a bit (clonado), garantizando de esta manera la integridad del proceso de recopilación de evidencias, puesto que al no estar *logueado* el investigador en el sistema operativo del dispositivo, no contaminará con sus acciones "el escenario".

En cambio, en otros escenarios, será necesario realizar la extracción del contenido de los soportes de almacenamiento del dispositivo empleando sus propios recursos hardware (Ej. BIOS, Procesador, memoria RAM, puerto USB, teclado, ratón), pero utilizando para el arranque un dispositivo externo (Ej. Memoria USB, un dispositivo óptico) con sistema operativo en modo *live*. De este modo, no se ejecutaría el sistema operativo instalado en los soportes de almacenamiento del dispositivo objetivo, evitándose la contaminación de sus evidencias.

No obstante, la recopilación de evidencias "en muerto" únicamente permitirá obtener evidencias presentes en el almacenamiento persistente (baja volatilidad) del dispositivo.

Aproximaciones para la recopilación de evidencias

La recogida de evidencias puede realizarse conforme a dos posibles aproximaciones:

- Respuesta a incidentes orientada a la continuidad del negocio. Prevalece la contención, erradicación y vuelta al normal funcionamiento de los sistemas para minimizar el impacto económico, aunque las acciones adoptadas puedan invalidar las evidencias obtenidas sobre la autoría del ataque o impedir la recopilación de evidencias que permitan determinar una potencial autoría.
- Investigación forense digital. Prevalece la detección, extracción forense y posterior análisis de las evidencias, preservando su integridad y manteniendo la debida cadena de custodia, de manera que pudieran ser posteriormente presentadas, si llegase a ser necesario, ante un tribunal.

Principios generales para la recopilación forense de evidencias digitales

Las guías de la IOCE destacan los siguientes principios generales para recopilación forense de evidencias digitales:

1. Los laboratorios forenses de los países del G8 deben cumplir los siguientes principios generales:
   a. Las reglas generales de las evidencias deben ser aplicadas a todos los dispositivos digitales.
   b. Cuando se recoge una evidencia digital, las acciones llevadas a cabo para recoger dicha evidencia digital no deben modificar la evidencia.
   c. Cuando sea necesario que una persona acceda a la información original de la evidencia, esa persona deberá tener la formación necesaria para dicho propósito.
   d. Toda actividad relacionada con la obtención, acceso, almacenamiento o transferencia de evidencias digitales debe estar completamente documentada, preservada y disponible para su revisión.
   e. Un individuo es responsable de lo acaecido en las evidencias digitales bajo su posesión.

2. Toda actividad relacionada con la recogida, proceso examinador y presentación de acceso a la evidencia, almacenamiento o transferencia de evidencia digital debe estar documentado, preservado y disponible para su revisión.

3. La responsabilidad de mantener el valor de las evidencias es de carácter individual, no corporativo. Si un individuo asume la responsabilidad de un objeto firmando el registro de acceso, es responsable de todo lo que ocurra con dicho objeto desde ese momento y hasta que sea devuelto a su punto de almacenamiento o formalmente transferido a otro individuo.

1.1.9 El método científico

La recogida de evidencias digitales sigue el denominado método científico, es decir, comprobar nuestras hipótesis de cómo y por qué sucedió un determinado evento. Básicamente, el método científico requiere:

1. Definir/aceptar una pregunta. Recoger información y evidencias.

2. Formular una hipótesis de lo sucedido.

3. Comprobar la hipótesis experimentalmente y recoger la información de una manera reproducible.

4. Analizar la información.

5. Obtener unas conclusiones, las cuales apoyarán o refutarán la hipótesis original. Si la información y las conclusiones del investigador no apoyan la tesis, debe volverse al punto 2.

6. Comunicar los resultados (presentación de informe).

Las evidencias pueden ser de dos tipos:

- **Inculpatorias**. Aquellas que tienden a demostrar que el acusado es culpable o tenía intención criminal, y apoyan la hipótesis inicial del investigador sobre lo que podría haber ocurrido.

- **Exculpatorias**. Aquellas que tienden a demostrar que el acusado no realizó las acciones por las que se le acusa, refutando por tanto la hipótesis inicial del investigador.

No obstante, conviene reseñar que la ausencia de evidencias inculpatorias no significa necesariamente que la hipótesis inicial realizada por el investigador sea errónea.

1.1.10 Mejor evidencia

Cuando se presenta una evidencia ante un tribunal, se requiere presentar la *mejor evidencia* (*best evidence*). Se entiende como mejor evidencia cualquier salida legible por el ojo humano si refleja fielmente la información.

Se aplica el concepto de mejor evidencia cuando una de las partes quiere que se admita como evidencia los contenidos de un documento ante un tribunal, pero el documento original no está disponible. En este caso, la parte que presenta la evidencia deberá presentar una justificación razonable para justificar su ausencia. Si está justificación es aceptada, entonces se permitirá a la parte utilizar una evidencia secundaria para probar los contenidos del documento para que finalmente sea admitido como evidencia.

El concepto de mejor evidencia se aplica en forense digital para evidencias como el del volcado de memoria RAM del ordenador del sospechoso. En este ejemplo, la mejor evidencia sería el contenido de la memoria en el momento de su captura. La imposibilidad de presentar el contenido de la memoria en ese momento concreto habilita que pueda presentarse como evidencia secundaria el volcado de la memoria RAM. De modo similar, la presentación del listado de conexiones de red sería admitida como evidencia secundaria porque, cuando un dispositivo se apaga, se finalizan las conexiones de red establecidas.

En algunas ocasiones, presentar la evidencia original no resulta práctico. Sirvan como ejemplos un *rack* de servidores *blade* o un conjunto de cabinas de bandejas de discos en una SAN (*Storage Array Network*). Dado que la recogida de estos dispositivos físicos no resulta práctica, e impactaría en la continuidad de negocio de la organización, normalmente ser realizará una copia forense de ese dispositivo. Se entiende por copia forense a una copia bit a bit del contenido del dispositivo. En ocasiones, la recogida de datos se limitará a aquellos de interés para la organización, pues en escenarios como la recogida de datos de una SAN, no resulta práctico copiar TB de información almacenada cuando el interés se centra en una única carpeta del soporte de almacenamiento.

1.1.11 Antiforense digital

El peor error que puede cometer un DFIR es subestimar a su adversario. Quizás el mejor punto de partida a la hora de acometer una investigación forense digital sea asumir que el atacante es más inteligente que el investigador, que tiene mejor equipamiento y que ha tenido más tiempo y paciencia para preparar el ataque del que tendrá el investigador forense digital para obtener y analizar las evidencias disponibles. Como en el ajedrez, no hay que depender del movimiento erróneo del oponente, pero sí hay que estar atento para aprovecharlo al máximo si se produce.

Se conoce como antiforense digital al conjunto de métodos y herramientas utilizadas para destruir u ofuscar objetos digitales de modo que no puedan ser empleados como evidencias digitales. Entre estas técnicas destacan el cifrado, la esteganografía, la compresión, el empaquetado, compresión y cifrado, la modificación de los metadatos de un archivo (Ej. *MAC time*), borrado de ficheros, ocultación de sistemas de ficheros (Ej. Empleando *TrueCrypt*).

El resultado de utilizar estas técnicas puede conllevar que no queden evidencias de la existencia del archivo, que el archivo existiese pero que fuera borrado de manera segura, o que el archivo exista pero que el contenido no se encuentre accesible.

1.2 GESTIÓN DE UN CASO FORENSE DIGITAL

1.2.1 Introducción

El jefe del departamento forense digital debe establecer un procedimiento que sirva de guía a los investigadores para la gestión de los casos encomendados. Antes de proceder con un caso, el jefe del departamento debe asegurarse de que todas las acciones que se vayan a acometer se adecúen a la legislación nacional y/o internacional vigente. Así, debe siempre existir un permiso (Ej. Orden judicial) que garantice el procesado de la evidencia. La finalidad de llevar a cabo una investigación forense digital es utilizar las evidencias disponibles para demostrar o refutar unos hechos, de ahí la importancia de que las evidencias digitales sean obtenidas conforme con la legislación vigente. Durante toda la gestión del caso, deberá garantizarse que la evidencia electrónica resulta admisible y el informe forense aceptable ante un tribunal.

Suelen considerarse siete etapas en la gestión de un caso forense digital: recibir la petición; registrar el caso; registrar la prueba documental (*exhibit*); fotografiar la prueba documental; ejecutar el análisis; devolver la prueba documental; cerrar el caso.

1.2.2 Recepción de la petición

El flujo de trabajo en el laboratorio forense digital (DFL, *Digital Forensics Laboratory*) comienza con la recepción de una petición formal (Ej. Carta, correo electrónico, burofax). La información suministrada en la petición formal debe incluir una descripción del caso, detalles de la evidencia electrónica, el objetivo del caso y, probablemente, adjuntará una orden judicial si se trata de un laboratorio de las FCSE.

El jefe del laboratorio revisará la petición y determinará si el caso es factible en base a los siguientes criterios:

- El caso entra dentro del ámbito forense digital, es decir, la evidencia es electrónica y no de otro tipo (Ej. Huellas dactilares, muestra de ADN).
- Métodos y herramientas disponibles.
- Personal disponible para llevar a cabo el caso.
- Se cumplen los requisitos legales para llevar a cabo la investigación.

El jefe del laboratorio responderá formalmente a la petición tanto si la respuesta fuese en sentido afirmativo como negativo. En caso afirmativo, el jefe del laboratorio coordinará con el peticionario (*requestor*) una fecha para la recepción de la evidencia electrónica.

1.2.3 Registro de un caso

Aceptado el caso, el peticionario hará entrega de la evidencia electrónica. El personal del laboratorio generará un número de caso único para ese caso, y rellenará un formulario de registro, como el ejemplo de la Ilustración 1. Este documento deberá ser firmado tanto por el peticionario como por un representante del laboratorio forense digital que recepciona la evidencia.

Requesting Agency Information	
Name:	Department/Unit:
Job Title:	Agency:
Tel Number:	Requestor Case Number:
Email:	DFL Case Number: fill in by DFL

Case Information
Case Background: Describe the background of the case that may help DFL with the analysis
Case Specific Request: List all keywords or analysis scope here

Terms and Conditions
1 Selection of Method: DFL shall select the best available method to conduct digital forensics analysis.
2 Statement of Confidential: DFL ensures that any information supplied by Requestor and any information gathered from the work performed will be treated with STRICTEST CONFIDENCE.
3 Damage or Loss of Profit: DFL shall not be held liable for any damaged exhibit or loss of profit caused by the Requestor in connection to the work performed. DFL,however, shall take reasonable precautions, care and steps in preserving the integrity of evidence at all times.
4 Abandoned or Unclaim Exhibit: Exhibit unclaimed or abandoned at DFL's location in excess of 30 days after communication has been made with the Requestor will be disposed of at DFL's discretion. DFL will not be responsible for exhibit left in its possession beyond 30 days. DFL, however,will inform the Requestor prior to disposing the exhibit.

Requestor	DFL
I have read, understood and agreed to the Terms and Conditions. Sign here Date :	Sign here Name: Date :

Ilustración 1. Ejemplo de formulario de registro de evidencias. Fuente: Interpol.

Para poder examinar de manera efectiva las evidencias electrónicas recibidas, los investigadores necesitan disponer por parte del peticionario de una petición clara y precisa de la información que desea obtener de la prueba documental. Debido a la gran cantidad de información que almacenan los dispositivos y la diversidad de tipos de datos existentes (Ej. Documentos, vídeos, llamadas, mensajería, datos de monitorización de salud, ubicaciones), resultará muy difícil proporcionar al peticionario una respuesta adecuada a sus necesidades de información si no se ha proporcionado previamente una petición clara y específica. Esta petición permitirá al investigador planificar los métodos y herramientas que debe emplear para procesar la evidencia.

1.2.4 Registro de la prueba documental

Cuando se recibe una evidencia digital o, en el caso general, una prueba documental, es importante que su envoltorio se encuentre convenientemente cerrado y sellado antes de ser transferida al laboratorio forense digital para garantizar la integridad de la cadena de la evidencia. Adicionalmente, para eliminar cualquier duda razonable sobre la integridad de la evidencia, tanto el peticionario como el examinador deben ser capaces de demostrar que no hubo acceso de terceros a la evidencia durante su proceso de transferencia.

Cada evidencia digital que llegue al laboratorio debe ser registrada y asignada una codificación única visible que será añadida al formulario de registro de la evidencia. Este documento incluirá cada uno de los elementos en los que puede dividirse la evidencia digital, utilizando una nomenclatura que permita relacionar fácilmente cada uno de los elementos con la evidencia digital completa. A modo de ejemplo:

20210622-TM01	Smartphone
20210622-TM01-Smartphone01	Terminal
20210622-TM01-SIM01	Tarjeta SIM
20210622-TM01-microSD01	Tarjeta microSD

Cuando se recibe la evidencia, deberá anotarse en el formulario cualquier imperfección apreciable a simple vista (Ej. La pantalla del dispositivo está rota). El formulario debe ser firmado tanto por el peticionario como por el examinador. Es recomendable almacenar una copia digital del documento en la carpeta del sistema de ficheros asignada al caso, por si se estropeara el documento original en papel.

Una vez realizada la transferencia de la evidencia digital, comienza la custodia de la evidencia por parte del laboratorio. Normalmente, la evidencia será almacenada en la sala de almacenaje de evidencias o depositada en la caja fuerte hasta que pueda ser procesada por el personal de laboratorio.

Section A: Exhibit Receive

No	DFL Exhibit Label	Manufacturer	Capacity	Description Include any defects of the item here	Serial Number

Requestor	DFL
Sender of the exhibit sign here Name: Date:	Sign here Name: Date:

Section B: Exhibit Return

I have agreed that DFL has returned all the exhibits listed in Section A to me. Upon signing the above column, both parties agreed that the work has completed and the case is signed off.

Requestor	DFL
Sender of the exhibit sign here Name: Date:	Sign here Name: Date:

Ilustración 2. Ejemplo de formulario de registro de una evidencia. Fuente: Interpol.

1.2.5 Fotografiar la prueba documental

Se fotografiará una prueba documental tanto para registrar el estado de la evidencia digital en el momento de su recepción como para poder identificar la prueba posteriormente. Se recomienda tomar tanto fotografías que proporcionen una visión general como otras que proporcionen una visión más detallada (Ej. La etiqueta de identificación de un disco duro, la etiqueta que identifica el modelo y número de serie de un ordenador portátil). Las fotos realizadas serán añadidas a la carpeta del sistema de ficheros del caso.

La obtención de fotografías de la evidencia digital es especialmente recomendable en aquellos casos en los que la evidencia digital original debe ser devuelta al peticionario tras la copia forense de sus datos (Ej. Un disco duro, un teléfono móvil).

1.2.6 Análisis de la prueba documental

El análisis de la evidencia digital se realizará conforme al modelo de análisis establecido en el laboratorio. Durante este proceso, el analista deberá mantener comunicación con el peticionario y transmitirle cualquier desviación o limitación que pudiera surgir durante la ejecución del análisis de la evidencia. La experiencia del analista suele facilitar la fluidez de información con el peticionario.

1.2.7 Devolución de la prueba documental

Una vez que se ha completado el análisis, el laboratorio contactará con el peticionario para devolverle la evidencia digital. Normalmente, el laboratorio devolverá la evidencia junto con una copia del informe elaborado a partir de su análisis. Antes de devolver la prueba documental, esta será sellada convenientemente, indicándose en una etiqueta el analista que procedió a su sellado, junto con la fecha y hora de esta acción.

1.2.8 Cierre del caso

El proceso se completa cuando el peticionario retira la evidencia digital, procediéndose al cierre del caso. Para poder cerrar el caso, tanto el peticionario como el jefe del laboratorio deben estar conformes con el alcance del trabajo realizado y el contenido del informe, formalizándose normalmente esta conformidad con la firma de un documento. A modo de ejemplo, la firma de la sección B de la Ilustración 2

por ambas partes serviría como conformidad con la completitud del trabajo llevado a cabo por el laboratorio.

En ocasiones, el analista que realizó la investigación acudirá ante un tribunal a prestar testimonio experto de los resultados presentados en el informe. El analista será notificado convenientemente en caso de resultar necesaria su comparecencia ante el tribunal.

1.3 PROCEDIMIENTO DE INVESTIGACIÓN

1.3.1 Importancia del procedimiento investigador

Independientemente de que se esté realizando una investigación forense digital con el rol de investigador forense digital (DFI, *Digital Forensics Investigator*), con el rol de respuesta a incidentes (IR, *Incident Responder*), o con una figura híbrida entre ambos, DFIR (*Digital Forensics and Incident Responder*), es necesario seguir un procedimiento. El procedimiento y la formación del investigador son fundamentales para alcanzar el objetivo final de la investigación.

Un procedimiento correctamente diseñado indica al investigador qué debe hacer en primer lugar, los pasos siguientes a seguir, cuándo dar por terminada cada fase y qué es necesario para pasar a la siguiente fase. Una vez completada la investigación, el procedimiento sirve como *checklist* para garantizar que se han realizado todas las tareas y que se ha generado la documentación apropiada para cada paso.

1.3.2 Pasos previos a la preparación de la investigación

Antes de comenzar una investigación hay que realizar ciertas actividades. Entre ellas se encuentran comprobar que se dispone del material necesario, repasar la legislación y/o políticas corporativas vigentes, asegurarse de disponer de la autorización necesaria de las autoridades pertinentes, bien sea de una orden judicial o del departamento legal de la corporación (según corresponda). Por último, comprobar nuevamente que el kit de herramientas forenses está listo y preparado para desplegar.

Comprobar el material forense digital

Resulta una buena práctica el reponer todos los elementos consumibles utilizados durante una investigación a la conclusión de esta. De este modo, se simplifica la tarea de preparar un posterior despliegue.

Otra buena práctica es el borrado forense de todo medio reutilizable empleado durante la investigación.

Actualmente, disponer de un entorno concreto de trabajo (la eterna duda de elegir entre una plataforma *Microsoft Windows*, una distribución Linux orientada a forense o *macOS*) resulta menos traumático debido a la facilidad de disponer de entornos de virtualización muy maduros (Ej. *Oracle VirtualBox*, *QEMU*, *VMware Workstation*, *VMware Fusion*, *Parallels Desktop*, *Microsoft Hyper-V* o *Citrix XenDesktop*), que permiten crear máquinas virtuales de diferentes sistemas operativos, lo que aumenta la versatilidad de la plataforma de análisis forense digital.

Por tanto, resulta clave el invertir buena parte del recurso económico en una potente plataforma forense digital (ya sea en configuración *workstation* o portátil), equipada con un procesador potente que permita virtualización hardware, la mayor cantidad posible de memoria RAM y espacio en disco duro suficiente para instalar aplicaciones y guardar temporalmente copias (insistir en trabajar con copias, nunca con la evidencia digital original) de las evidencias digitales de la investigación en curso. Si el presupuesto lo permitiera, instalar una o más tarjetas gráficas de gama alta (las de *gamer* en configuración SLI son una opción muy recomendable) para cuando haya que acometer ataques de fuerza bruta mediante *GPU cracking*. En el caso de las *workstation*, resulta interesante disponer de salida de monitor dual, pues permite al analista procesar varias evidencias digitales al mismo tiempo.

Para el *kit* de recogida de evidencias resulta también interesante disponer de diferentes sistemas operativos *live* y una variedad de herramientas que permitan obtener evidencias digitales en diferentes escenarios. En forense digital resulta muy difícil, por no decir imposible, encontrar una herramienta universal que valga para todos los escenarios posibles.

Además, es necesario disponer de un entorno de trabajo que permita almacenar y garantizar la integridad de las evidencias digitales.

Revisión de leyes y políticas corporativas en vigor

El DFIR necesita conocer las leyes que afectan el modo en el que realiza la recogida de evidencias para poder llevar a cabo sus investigaciones forenses digitales. En el caso de las investigaciones corporativas, además de las leyes en vigor que pudieran aplicarse, es necesario conocer las políticas corporativas aplicables.

Notificar a las autoridades y obtener los permisos pertinentes

La responsabilidad principal de un DFIR es elevar un informe relatando los hechos de la investigación a una instancia superior de la manera más clara y precisa posible. En general, el destinatario del informe no será personal técnico, debiendo por tanto el investigador elaborar el informe de manera que sea comprensible para el lego en la materia, adjuntando al informe un anexo donde se detallen los aspectos técnicos de la investigación.

En la mayoría de los escenarios, el DFIR deberá notificar o solicitar una autorización a una entidad superior como paso previo al comienzo de la investigación. En el caso de las investigaciones criminales, esta autorización vendrá dada mediante una orden judicial. En el caso de las investigaciones corporativas, esta autorización podrá ser una autorización marco otorgado a la unidad forense dentro del entorno corporativo o, por el contrario, la autorización realizarse de manera concreta para cada incidente, dependiendo de la importancia del incidente como para asignarle recursos de la unidad forense.

Independientemente del tipo de investigación, el DFIR debe asegurarse de que los niveles adecuados de dirección de la organización han aprobado sus actividades y el alcance de la investigación. No hay que olvidar que sobrepasar el marco de la investigación puede conllevar la anulación de la evidencia o incluso la suspensión del caso.

Material mínimo recomendado para un DFIR

El Departamento de Justicia de EE.UU. recomienda que el kit básico de trabajo de un DFIR incluya: cámara fotográfica y de vídeo; cajas; cuadernos de notas; guantes; registros de evidencias; cinta de evidencias; bolsas de papel para evidencias; pegatinas de evidencias; etiquetas; cinta de escenario del crimen; bolsas anti-ESD (*Electrostatic Discharge*); rotuladores permanentes, kit de herramientas no magnetizadas, material para apantallar electromagnéticamente un dispositivo; soportes DVD y CD vírgenes; material extra (Ej. Memorias USB, pegatinas, soportes ópticos).

Especialmente cuando el marco de la investigación incluya el decomiso de un dispositivo móvil, es necesario utilizar bolsas de Faraday o papel de aluminio envolviendo el dispositivo para evitar que este se conecte a una red inalámbrica (ya sea WiFi o de datos de telefonía móvil), debido a que muchos dispositivos permiten de fábrica como medida de seguridad el borrado remoto de la información almacenada en el dispositivo.

Ilustración 3. Ejemplo de bolsa de Faraday del fabricante Paraben.

1.3.3 Preparación de la investigación

Tras la notificación al departamento forense digital de un caso, suele ser habitual establecer una breve entrevista (oral o escrita) con el notificador (en el caso de que haya sido notificado a través del nivel de respuesta a incidentes) o el usuario del equipo (si es colaborativo con la investigación) para intentar establecer las 5WH de la investigación en curso:

- **Quién** (*Who*). ¿Quién es el gestor del incidente? ¿Existe un identificador para el incidente?
- **Qué** (*What*). ¿Qué ha ocurrido?
- **Cuándo** (*When*). ¿Cuándo es necesaria la presencia del DFIR?
- **Dónde** (*Where*). ¿Dónde se encuentra la escena del incidente localizada? Jurisdicción aplicable.

- **Por qué** (*Why*). ¿La investigación es abierta o encubierta? ¿Es corporativa o criminal?
- **Cómo** (*How*). ¿Qué dispositivos van a ser decomisados? ¿Cuánto trabajo va a llevar el incidente?

Antes de proceder a capturar las evidencias, es necesario desarrollar un análisis del caso, es decir, crear un plan previo. El DFIR deberá desarrollar una hipótesis previa a partir de las respuestas a las preguntas anteriores y su experiencia previa en la materia. Por ejemplo, hay que tener en consideración la pericia técnica del sospechoso, especialmente ante aquellos con conocimientos suficientes como para haber preparado medidas antiforenses para tratar de impedir su identificación.

En caso de tratarse de una investigación criminal será necesario solicitar una orden judicial. Dicha orden deberá incluir detalladamente el alcance de la investigación y los dispositivos incluidos en la misma.

Una de las primeras tareas que debe acometer el DFIR al llegar al escenario donde se encuentran los dispositivos de los cuales se obtendrán las evidencias digitales es asegurarse de que las evidencias digitales están correctamente preservadas y hacer un croquis en papel del escenario como respaldo físico de las fotos y/o vídeos que se tomen en el escenario. De esta forma se mitiga la posibilidad de que el DFIR pierda la composición del lugar por un eventual accidente que afectara a su cámara.

Un DFIR necesita tener la imaginación de un *hacker* y las capacidades organizativas y atención a los detalles de las que disponen los auditores del Tribunal de Cuentas.

Se asignará un número de caso (siguiendo un estándar de generación de números identificativos, como incluir la fecha en formato *aaaammdd* y el número del caso del día, *xxx*, quedando por tanto el caso identificado como *aaaammddxxx*), un nombre de investigador y todas aquellas etiquetas necesarias para identificar la evidencia recogida.

Debe establecerse una diferencia entre la información recogida como parte de la gestión del caso y las notas tomadas por el DFIR durante su investigación. En general, las notas escritas por el DFIR contendrán algo más que hechos, resultando de gran ayuda posteriormente durante la investigación.

La integridad del escenario debe ser preservada, generalmente empleando cinta para escenario del crimen y garantizando que los dispositivos digitales sean manipulados de manera apropiada. En caso de colaborar en una investigación con las FCSE deberá el DFIR identificarse como tal ante ellos.

El DFIR deberá:

- Anotar todos los dispositivos que encuentre en la escena, su estado y ubicación.
- Fotografiar todos estos dispositivos para determinar su ubicación en el local y su estado (apagado; encendido, y lo que se ve en pantalla).
- Etiquetar unívocamente dichos dispositivos y sus conexiones.
- Fotografiar nuevamente toda la escena con los dispositivos y conexiones etiquetadas.

Por cada dispositivo que se encuentre encendido, el DFIR deberá anotar y capturar una imagen de las aplicaciones en ejecución. Si la pantalla del dispositivo no muestra información pese a encontrarse este encendido, se puede desplazar el dispositivo puntero (Ej. Ratón, *touchpad*) para quitar el protector de pantalla o hacer que el dispositivo salga del estado de suspensión.

1.3.4 Recopilación de evidencias digitales

Cualquiera que sea la evidencia digital que el DFIR pretende obtener del escenario debe ser en concordancia con la legislación vigente y/o las políticas corporativas existentes, empleando para ello procedimientos forenses seguros que garanticen la integridad del procedimiento de obtención de evidencias digitales.

En el caso de encontrarse el DFIR en el escenario con dispositivos no previstos (Ej. Memoria USB sobre la mesa) inicialmente durante la fase de planificación, deberá tener en cuenta que durante el transcurso de una investigación criminal necesitará en la mayoría de los casos una extensión de la orden judicial existente para que se incluya dentro del alcance de la investigación dichos dispositivos imprevistos.

Resulta una buena práctica examinar el escenario en busca de notas, *Post-it*, cuadernos (son lugares habituales donde podrían estar anotadas credenciales de usuario a distintos sistemas), dispositivos de almacenamiento ópticos (pudieran contener material multimedia constitutivo de delito o copias de seguridad del sistema o de la información del usuario), etc.

Incluso en escenarios domésticos, el DFIR deberá identificar la electrónica de red local existente (Ej. *Switches*, puntos de acceso inalámbricos) y dispositivos móviles. Además, otros dispositivos, como impresoras, pueden tener en caché información de los últimos documentos impresos.

Adicionalmente, el DFIR buscará aquellos dispositivos que deberían encontrarse en el escenario de la investigación pero que no se encuentran presentes (Ej. Se encuentra el manual de un dispositivo electrónico que no se encuentra en el escenario).

La doctrina legal del "fruto del árbol envenenado" (*fruit of the poisonous tree*) es una derivación de la doctrina de las reglas de exclusión consistente en la desestimación de cualquier medio probatorio obtenido empleando vías ilegítimas. No obstante, la doctrina del fruto del árbol envenenado no se refiere únicamente a las pruebas obtenidas de manera ilícita, sino que extiende sus efectos a cualquier prueba que directa o indirectamente y por cualquier nexo esté viciada, arrastrando sus efectos a todas aquellas pruebas relacionadas y derivadas. Es decir, mientras que las reglas de exclusión desestiman cualquier medio probatorio obtenido ilegalmente, con la doctrina del fruto del árbol envenenado se extienden sus efectos a todos aquellos medios que por alguna razón o nexo estén relacionados de manera directa o indirecta con la primera prueba viciada.

Un ejemplo sería la obtención de evidencias digitales del domicilio de un sospechoso sin disponer de la pertinente orden judicial. Estas evidencias se convertirían automáticamente en ilegítimas y, por tanto, su radical nulidad, conllevando que todas aquellas otras evidencias directamente relacionadas y derivadas en el procedimiento seguido fuesen también nulas de pleno derecho.

Otros ejemplos serían los supuestos de obtención de evidencias vulnerando el derecho a la intimidad, el secreto de las comunicaciones o la inviolabilidad del domicilio del sospechoso.

No obstante, esta doctrina está sujeta a cuatro excepciones y una evidencia envenenada será admitida ante el tribunal si:

- Fue descubierta en parte como resultado de una fuente independiente no envenenada.
- Habría sido descubierta inevitablemente pese a la fuente envenenada.
- La cadena de causalidad entere la acción ilegal y la fuente envenenada se encuentra muy atenuada.
- Excepción de la buena fe (*good-faith exception*). Esta excepción permite que las evidencias recopiladas violando los derechos de privacidad protegidos por la Cuarta Enmienda de la Constitución de los EE.UU. puedan ser admitidas ante un tribunal siempre que los agentes de la autoridad actuasen de buena fe, es decir, careciendo de motivo para dudar de la legalidad de la orden de registro utilizada.

1.3.5 Preservación de las evidencias

A la hora de obtener la evidencia el DFIR siempre debe recordar que el objetivo es preservar la evidencia. Por tanto, estas deben almacenarse en contenedores de almacenamiento apropiados y debidamente etiquetados (Ej. Bolsas de Faraday, bolsas anti ESD), comenzando así su cadena de evidencia.

Cada vez que una evidencia digital cambie de manos, este cambio deberá ser correctamente reflejado tanto en la cadena de custodia como en la cadena de evidencia. El correcto mantenimiento de estos dos formularios resultará vital para poder presentar la evidencia ante un tribunal, pues en caso contrario, se cuestionará su integridad.

1.3.6 Análisis de las evidencias

En el caso general, para garantizar la integridad de la evidencia original es necesario trabajar con una copia de la evidencia, y solo en casos excepcionales con el original (Ej. *Smartphone* encendido del que se quiera obtener información de oportunidad).

La copia debe ser realizada en un entorno medioambiental que garantice que el original no va a ser dañado (Ej. Cambios bruscos en condiciones de humedad, gradiente térmico). La copia debe ser segura desde un punto de vista forense, es decir, debe representar una copia exacta del original (copia bit a bit). El modo de demostrar que se realizó una copia segura es obtener el valor resumen (*hash*) de ambas evidencias (el original y la copia) y compararlos. Preferiblemente el valor resumen empleado será uno que garantice bajas colisiones (Ej. SHA-2).

Existen diferentes modos de analizar una evidencia digital. Por ejemplo, si la evidencia a analizar fuese un disco duro, un análisis físico realizaría sus búsquedas a nivel hexadecimal en los bloques del disco; en cambio, un análisis lógico examinaría la información a nivel sistema de ficheros.

Los análisis físicos permiten obtener información que no se encuentra accesible al realizar análisis lógicos. Por ejemplo, permite realizar búsquedas de palabras clave a través de los bloques físicos del disco, extraer archivos del disco empleando la técnica conocida como *carving*, y recuperar espacio libre en el disco. Un análisis lógico resulta muy útil a la hora de recuperar información del disco como el nombre, tamaño, tipo (Ej. PDF, JPG, EXE) y otros metadatos almacenados relativos al estado del sistema de ficheros (Ej. *Slack space*, espacio no asignado).

Una clasificación habitual de las diferentes formas en las que un DFIR puede analizar una evidencia digital es la siguiente:

- **Análisis temporal**. Determina la actividad a nivel de archivo ocurrida en el dispositivo en una determinada horquilla temporal, examinando diferentes archivos de eventos del sistema para correlar las actividades del sistema de ficheros con otras actividades.
- **Análisis de información oculta**. Busca información oculta ya sea en el sistema de ficheros o en partes del disco normalmente inaccesibles al acceso estándar del sistema de ficheros.
- **Análisis de aplicaciones y archivos**. Busca en el contenido de archivos, relaciona archivos con aplicaciones y actividad de aplicaciones con la creación y eliminación de archivos.
- **Análisis de propiedad y posesión**. Ayuda a identificar actividades relacionadas con la actividad de una determinada cuenta de usuario (Ej. Eliminado de archivos, modificación o intentos de cambiar el propietario de un archivo particular).

Normalmente, durante el transcurso de una investigación, se utilizarán varios o todos de estos modos de análisis para intentar contestar las 5WH.

Es importante señalar que, si durante el curso de una investigación criminal, se descubrieran evidencias de otra actividad criminal diferente, debería pararse inmediatamente el análisis y obtener la autorización pertinente para poder proseguir con esa línea de investigación (o transferirla, si fuera pertinente).

1.3.7 Presentación de informes de la investigación

Una vez completado el análisis de las evidencias, y en ocasiones durante el propio análisis, será necesario presentar un informe escrito con las conclusiones del análisis. Dependiendo del estado del avance de las investigaciones, se tratará de un informe preliminar o un informe final de la investigación. El informe final de la investigación será más completo, abarcando todas las evidencias recogidas y analizadas durante el caso; mientras que un informe preliminar únicamente hará referencia a las evidencias analizadas hasta la presentación de dicho informe preliminar.

A la hora de elaborar un informe, resulta de gran ayuda ir documentando cada paso del proceso de la investigación, pues reduce el tiempo necesario para elaborar el informe y evita omitir pasos que pudieran resultar de importancia a la hora de justificar el proceso investigativo.

La prioridad para el DFIR a la hora de redactar el informe será conocer la audiencia objetivo (destinatarios) del informe, especialmente si su perfil no es técnico. El informe debe ser una presentación sistemática, concienzuda e imparcial de los hechos averiguados durante la investigación.

1.3.8 Presentación de informes de la investigación ante un tribunal

En el caso de que el DFIR actúe como perito de parte ante un tribunal, es probable que tenga que presentar declaración ante dicho tribunal exponiendo las conclusiones del informe. Es muy probable también que la otra parte presente un contra análisis de la/s evidencia/s digitales, intentando ofrecer "otra visión de la misma realidad" o buscando argumentos para invalidar las evidencias presentadas (Ej. no se mantuvo toda la cadena de custodia o alegar que las evidencias pudieron ser de algún modo fabricadas o manipuladas).

1.3.9 Cierre del caso

Una vez que se da por concluida una investigación relacionada con un caso, se ha presentado el pertinente informe, e incluso se ha declarado ante un tribunal, no hay que dar por sentado que no se tendrá más relación con dicho caso.

En primer lugar, y especialmente en aquellos casos en los que se declara ante un tribunal, pueden existir servidumbres vinculadas a la confidencialidad de las investigaciones.

Resulta también de gran importancia para el DFIR realizar un análisis retrospectivo del caso y del modo en el que se llevó a cabo la investigación para obtener unas "lecciones aprendidas" del mismo. Una buena dosis de autocrítica permitirá ser más efectivo en casos futuros, especialmente cuando se detecten carencias (Ej. Material, formativas) durante el proceso de la investigación.

Finalmente, y como se comentó anteriormente, deben ser repuestos todos los materiales consumibles utilizados y sanitizar los dispositivos de almacenamiento empleados del kit forense del DFIR.

1.4 RAMAS DE LAS INVESTIGACIONES FORENSES DIGITALES

1.4.1 Introducción

Los aspectos técnicos de una investigación forense digital pueden subdividirse en varias ramas, conforme al tipo de dispositivo digital implicado en la investigación. Así, suele distinguirse entre forense de ordenadores (*computer forensics*), forense de dispositivos móviles (*mobile device forensics*), forense de red (*network forensics*) y análisis de *malware* (*malware forensics*).

1.4.2 Forense de ordenadores

Comprende la obtención y el análisis de evidencias físicas o lógicas encontradas en el hardware, sistemas operativos, sistemas de ficheros e información almacenada de servidores, equipos sobremesa, ordenadores portátiles y tabletas (*Microsoft Windows* y *Windows RT*). Según el sistema operativo del dispositivo a analizar suele subdividirse en:

- **Forense de *Windows* (*Windows forensics*)**. Comprende el análisis forense digital de aquellos equipos en los que se ejecutan sistemas operativos de Microsoft, tanto destinados al usuario (*Windows XP*, *Vista*, *7*, *8* y *10*) como a servidores (*Server 2003*, *2008*, *2012*, *2016* y *2019*). Debido a que en la actualidad los sistemas operativos de Microsoft son los más extendidos especialmente a nivel de usuario final, esta rama suele ser la que engloba el mayor número de casos de análisis en la mayoría de los entornos de trabajo.

- **Forense de Linux/UNIX (*Linux forensics*)**. La elevada cuota de mercado de sistemas operativos Linux/UNIX en servidores dedicados a prestar servicios en la nube (Ej. *Web hosting*) hace que la importancia de esta rama sea mayor en entornos empresariales.

- **Forense de *macOS* (*Mac forensics*)**. El porcentaje de equipos con este sistema operativo ha incrementado en los últimos años especialmente en entornos domésticos y orientados a la creación multimedia. Pese a tratarse de un sistema operativo UNIX modificado, debido a sus muchas peculiaridades se le considera una rama independiente de la anterior.

Según el tipo de datos almacenado, la información a analizar se clasifica en:

- **Datos no estructurados**. Comprende el análisis de la información presente en archivos de *log*, mensajería (Ej. Correos electrónicos, mensajería instantánea), documentos de texto y sitios web (E. *Blogs* y *microblogging*, redes sociales, *YouTube*).
- **Datos estructurados (*Forensic data analysis*)**. Comprende el análisis forense de información estructurada. Es decir, la información almacenada en bases de datos relacionales (Ej. Registros financieros, información logística), hojas de cálculo y credenciales de acceso a los sistemas. El análisis de esta información suele estar relacionado con crímenes de tipo financiero o análisis de intrusión. Su objetivo es descubrir y analizar patrones de actividades fraudulentas.
- **Contenido multimedia (*Forensic* v*ideo analysis*)**. Comprende el examen científico, comparación y/o evaluación de contenido multimedia digital (audio, fotografía y/o vídeo) con fines legales.
- ***Big Data* (*Big Data analytics*)**. Se conoce como *Big Data* la combinación de cualquier tipo de información, ya sea estructurada, no estructurada o contenido multimedia. Este tipo de información resulta compleja de analizar por su velocidad de generación/tránsito, volumen y variedad de datos implicados, además de la diversidad de las fuentes origen. La localización de estas fuentes conlleva consideraciones transnacionales y el análisis de información proveniente de mensajería instantánea, correos electrónicos, etc. Tiene implicaciones de privacidad de datos.

1.4.3 Forense de dispositivos móviles

Comprende la obtención y el análisis de evidencias físicas o lógicas encontradas en teléfonos móviles, agendas electrónicas, *e-books*, *smartphones*, *wearables* (Ej. *Smartwatches*, *fit bands*), tabletas y dispositivos de geolocalización (Ej. Navegadores GPS manuales, vehiculares) y *drones*. Para ello debe disponerse, por un lado, de la capacidad de extracción física y/o lógica de evidencias digitales (memoria RAM y del almacenamiento interno y externo) del mayor espectro posible de sistemas operativos y sus diferentes versiones (Ej. *Symbian OS*, *Google Android*, *Apple iOS*, *BlackBerry OS*, *Tizen*). Por otro lado, debe disponerse de una herramienta software para el análisis de estas evidencias digitales, la cual debe ser capaz de leer los sistemas de ficheros del mayor espectro posible de sistemas operativos móviles, analizar los datos procedentes de la agenda de contactos (y la relación de éstos con el usuario del dispositivo), calendario, registro de llamadas, mensajería (Ej. Correo electrónico, SMS/MMS, *WhatsApp*, *Line*, *Telegram*, *Skype*), histórico de navegación

web, redes sociales (Ej. *Facebook*, *Google+*) y *microblogging* (*Twitter*), contenido multimedia (Ej. Fotografías, vídeos), información de localización y *geotags*, recuperación de archivos borrados, *trip-logs* de dispositivos de geolocalización, detectar la presencia de *malware* en el dispositivo, etc. englobadas en lo que se conoce como *Internet artifacts*.

1.4.4 Forense de red

Orientado a la monitorización y el análisis del tráfico de las redes de datos con objeto de obtener información, adquirir pruebas legales o detectar una intrusión en la red. Al tratarse de información dinámica y volátil, la investigación debe tener un carácter proactivo.

1.4.5 Análisis de malware

De aplicación en todas las ramas anteriores. Comprende las actividades de ingeniería inversa necesarias para detectar la presencia de *malware* en un dispositivo, conocer su funcionamiento, evaluar los daños potenciales y/o producidos y determinar su autoría. Las aproximaciones más habituales son: análisis estático de *malware*, análisis dinámico de *malware*, y análisis *post-mortem*.

Análisis estático de *malware*

El análisis del código malicioso se lleva a cabo sin ejecutarlo. Las herramientas más empleadas son desensambladores, decompiladores, analizadores de código fuente, etc.

En aplicaciones con una cantidad de líneas de código reducida, permite conocer a priori su comportamiento en condiciones diferentes a las habituales, pues se pueden examinar fragmentos de dicha aplicación que normalmente no se ejecutarían.

Análisis dinámico de *malware*

El estudio de la muestra se realiza durante su ejecución. Las herramientas más empleadas en este tipo de análisis son *sandboxes* (entornos virtuales confinados donde se puede ejecutar y observar el comportamiento de muestras concretas de código malicioso), *debuggers*, trazadores de llamadas de función, analizadores lógicos, emuladores, capturadores de tráfico (*sniffers*) de red, y analizadores de protocolos de red.

La principal ventaja que proporciona este tipo de análisis es que, dependiendo de la muestra objeto de estudio, puede ofrecer una caracterización rápida y precisa. Su principal inconveniente es que el resultado del análisis sólo recogerá aquellas características de la muestra observadas directamente, pudiendo quedar parte de sus funciones adicionales ocultas. Esto es debido a que resulta complejo conseguir una ejecución controlada de todas las posibles rutas que puede seguir el flujo del código.

Además, esta aproximación permite el análisis completo del ciclo de vida del *malware* si se habilita en el entorno de estudio la conectividad de red. De este modo, el analista podría intentar seguir el rastro de los ciberataques a través de sus múltiples fases y diferentes vectores.

Análisis *post-mortem*

Este tipo de análisis se basa en el estudio del comportamiento de la muestra a partir de los artefactos generados en el sistema durante su ejecución. Este tipo de análisis suele ser el llevado a cabo tras un incidente de seguridad.

Ejemplos de actividades llevadas a cabo en este tipo de análisis serían la comprobación de los archivos de *log* de los accesos al sistema, modificaciones en el contenido de archivos o en los patrones de acceso a dichos archivos, archivos eliminados, información escrita en el espacio *swap* del sistema operativo, información *exfiltrada*, trazas de información todavía presentes en la memoria, etc.

La principal desventaja de este tipo de análisis es su total dependencia del grado de volatilidad de los diferentes artefactos forenses generados por la muestra y de la posible aplicación de medidas antiforenses por el atacante.

1.5 EL LABORATORIO FORENSE DIGITAL

1.5.1 Generalidades

Un laboratorio de análisis forense digital es el local donde el analista forense digital realiza sus investigaciones, almacena de forma segura las evidencias físicas y digitales y realiza la mayor parte de su trabajo. Por tanto, el laboratorio debe disponer tanto del espacio suficiente para ubicar los equipos de los puestos de trabajo de los analistas como de capacidad para almacenar de forma segura las evidencias hardware/software obtenidas hasta su destrucción una vez concluido su ciclo de vida.

Las instalaciones y el control de accesos al laboratorio deben garantizar que los analistas puedan llevar a cabo sus pesquisas sin exponer la integridad de la cadena de custodia de las evidencias que almacenan y analizan.

El laboratorio deberá diseñarse siguiendo los criterios de eficiencia de material y personal para poder desempeñar el amplio abanico de casos que puedan plantearse en los cuales haya que obtener y analizar evidencias digitales.

Por tanto, a la hora de diseñar el laboratorio se tendrán en cuenta tanto la disponibilidad presupuestaria como el tiempo necesario para la adquisición de nuevas capacidades o la acometida de actualizaciones para seguir el ritmo de los cambios tecnológicos.

1.5.2 Emplazamiento del laboratorio

A continuación, se enumeran algunos de los principales factores que deben ser tenidos en consideración a la hora de seleccionar la ubicación del laboratorio forense digital:

- Disponer de potencia eléctrica suficiente para operar los dispositivos necesarios. Considerar la necesidad de equipamiento adicional para garantizar el suministro eléctrico (Ej. Generadores de respaldo, SAI).
- Si el laboratorio se encuentra en un nivel del edificio superior a la planta baja, determinar si sería necesario disponer de un ascensor/montacargas para facilitar el transporte de grandes cantidades de evidencias electrónicas.
- Determinar el nivel de seguridad del edificio y del laboratorio, de modo que se pueda garantizar la seguridad física de los datos almacenados y de los investigadores.
- Determinar la resistencia de paredes, techos y suelos para resistir a daños físicos o medioambientales.
- Determinar el riesgo de inundaciones, incendios, desastres naturales y malestar social.
- Tomar las medidas de seguridad necesarias para minimizar los riesgos ante posibles ataques de grupos organizados motivados en la destrucción de las evidencias almacenadas.

- Determinar la capacidad de refrigeración disponible para garantizar el adecuado funcionamiento de los equipos en todas las épocas del año, aumentándola si fuera necesario.

1.5.3 Seguridad física del laboratorio

El laboratorio forense digital deberá garantizar la seguridad de las evidencias electrónicas custodiadas, del personal que trabaja en él, y del material que utiliza para trabajar. Entre las principales capacidades de seguridad física, deben ser tenidas en consideración las siguientes:

- Sistema de vigilancia. El sistema de vigilancia se utiliza para monitorizar las instalaciones frente accesos no autorizados. Deberá seleccionarse la mejor ubicación posible de las cámaras y un nivel de resolución de lente que garantice un nivel de seguridad máxima, siempre dentro del presupuesto.

- Control de accesos. El control de accesos se implementará, en función del presupuesto, empleando cerraduras y llaves, teclados electrónicos, tarjetas smartcard y/o controles biométricos.

- Sistema de control de incendios. El laboratorio debe disponer de un sistema de detección y extinción de incendios. El agente extintor seleccionado no debe provocar daños sobre el personal, el equipamiento o las evidencias electrónicas almacenadas.

- Protección de puertas, ventanas y paredes. De considerarse necesario, las ventanas deberán ser reforzadas con barrotes para prevenir accesos desde el exterior. Si el laboratorio tuviera paredes y/o ventanas de vidrio, deberán adoptarse medidas para que la información sensible no pueda ser vista desde el exterior.

- Provisionar las tomas de corriente necesarias. Deben instalarse suficientes tomas de corriente, fusibles y diferenciales para garantizar el normal funcionamiento y evitar picos de corriente eléctrica que pudieran producir un incendio.

- Suelo antiestático. La disposición de un suelo antiestático reduce el riesgo de posibles descargas electrostáticas que pidieran afectar a los empleados, el equipamiento o las evidencias digitales.

- Sistema de inhibidores radioeléctricos. Se recomienda la instalación de un sistema de bloqueo de señales de red (Ej. Jaula de Faraday, Inhibidor

de frecuencias). Un inhibidor de frecuencias bloqueará cualquier señal de red, evitando así la posibilidad de que las evidencias digitales puedan verse alteradas o eliminadas. Esto es de especial relevancia en el caso de teléfonos móviles, *smartphones*, *wearables*, tabletas, ordenadores portátiles, etc. pues disponen de diferentes interfaces de red (Ej. 2G/3G/4G/5G, WiFi, Bluetooth, NFC). Deberá verificarse que el inhibidor de frecuencias no interfiera con otros sistemas del entorno.

- Sistema de refrigeración. Los dispositivos de trabajo del laboratorio generarán calor cuando son operados. Como el sobrecalentamiento puede provocar la pérdida de datos y daños en los equipos, deberá instalarse un sistema de refrigeración que permita controlar la temperatura del laboratorio. Además, deberá controlarse la temperatura de la sala de almacenamiento de evidencias y, si hubiere, la sala de servidores o el CPD.

- Almacenamiento de respaldo en una ubicación diferente. Cuando se dispone de servidores para el almacenamiento de datos, una buena práctica es realizar una copia de seguridad de esos datos en un servidor ubicado en otro emplazamiento alejado del laboratorio. De este modo, si se produjese un incendio o un desastre natural (Ej. Terremoto, riada), el almacenamiento de respaldo permitiría recuperar los datos. La disposición de un centro de almacenamiento de respaldo debe formar parte del plan de recuperación ante desastres (DRP, *Disaster Recovery Plan*) de la organización.

- Almacenamiento de datos a largo plazo. Tras su análisis las evidencias digitales deben almacenarse de modo que puedan ser posteriormente recuperadas y/o nuevamente analizadas con posterioridad como parte de un procedimiento judicial. El tiempo de almacenamiento de las evidencias digitales debe adecuarse a la normativa nacional donde se encuentre el laboratorio.

1.5.4 Tamaño y disposición del laboratorio

Los requisitos mínimos imprescindibles para trabajar en el laboratorio serán disponer de mesas y sillas para que los DFIR puedan llevar a cabo sus investigaciones. Adicionalmente, es deseable disponer de una mesa o tablero de grandes dimensiones donde depositar las evidencias para su registro, etiquetado, duplicado y precintado. Las evidencias digitales normalmente se almacenarán en un armario ignífugo, y las copias en papel de los informes forenses, en un archivador.

Si el volumen de evidencias digitales a procesar es elevado, frecuentemente se opta por desarrollar actividades específicas de manera separada para evitar tanto la contaminación cruzada como la pérdida de evidencias (Ej. Reservar un área para la recepción de evidencias).

En caso de necesitarse un servidor con una cabina de discos para almacenar las evidencias digitales, este se encontrará en el propio laboratorio o, de ser posible, en una sala dedicada debidamente securizada.

El acceso al laboratorio estará restringido, de modo que únicamente pueda acceder al laboratorio el personal conveniente habilitado.

Se reservará un área para el procesado y la clonación de evidencias digitales. Debe estar separada de la estación de trabajo del analista y próxima a la sala de almacenamiento de evidencias para minimizar su manipulación. No obstante, en laboratorios donde el espacio sea reducido, podrá optarse por utilizar una estación de trabajo forense con capacidad integrada de clonado de soportes de almacenamiento y un NAS para el almacenamiento de las copias de las evidencias digitales.

Ilustración 4. Ejemplo de estación de trabajo forense. Fuente: Sumuri.

Si se dispone de espacio suficiente, se habilitará una sala de reuniones y un despacho para el jefe del laboratorio.

Habitualmente, el laboratorio dispondrá de su propia LAN aislada, o una VLAN dedicada, reduciendo así el riesgo de infección proveniente de otras subredes o VLAN de la organización. Además, deberá disponer de una conexión a Internet sin filtrar, de modo que los analistas de *malware* puedan interactuar con la infraestructura IT empleada por los operadores de la campaña a la que pertenece la muestra de *malware* objeto de estudio. Esta LAN/VLAN forense deberá dotarse de ciertas medidas de seguridad y un sistema básico de almacenamiento de archivos de *log* de eventos de red y capacidad de detección de intrusiones.

1.5.5 Normativa aplicable a un laboratorio forense digital

La normativa *UNE-EN ISO/IEC 17025:2005* "*Evaluación de la conformidad. Requisitos generales para la competencia de los laboratorios de ensayo y calibración*" establece en España los requisitos que deben cumplir los laboratorios de ensayo y calibración, siendo su principal objetivo la acreditación de la competencia de las entidades de ensayo y calibración.

Esta normativa es aplicada por los laboratorios de ensayo y calibración con objeto de demostrar que son técnicamente competentes y de que son capaces de producir resultados técnicamente válidos.

El transporte de evidencias almacenadas en dispositivos electrónicos, en tanto en cuanto no exista una legislación nacional o Directiva de la UE al respecto, se realizará en bolsas de Faraday, conforme a las directrices establecidas por la Corte Suprema de los EE.UU.

La cabina de flujo laminar para manipulación de dispositivos electrónicos deberá ser *Clase 100*, conforme a la normativa *Fed. Std. 209* y *BS 5295*.

1.5.6 Departamentos dentro del laboratorio forense digital

El amplio abanico de evidencias hardware/software a obtener y analizar y la específica preparación técnica que conlleva cada una de las ramas de las investigaciones forenses digitales invitan a dividir el laboratorio en departamentos, debiendo cubrirse cada uno de ellos por un analista especializado en la respectiva rama en el mejor escenario de plantilla posible.

Por tanto, un laboratorio podría estar constituido en los siguientes departamentos:

- **Forense de ordenadores**. Orientado a la obtención y análisis de evidencias procedentes de equipos (Ej. Servidores, terminales de usuario, ordenadores portátiles) y los datos almacenados en ellos. La obtención de datos del dispositivo a analizar puede implicar la recuperación física de dicho dispositivo.

- **Forense de dispositivos móviles**. Orientado a la obtención y análisis de evidencias procedentes de dispositivos móviles (Ej. Teléfonos móviles, *smartphones*, *wearables*) y de geolocalización y de los datos almacenados en ellos.

- **Forense de red**. Orientado al análisis masivo del tráfico de red de un entorno corporativo para determinar el origen y actividades acaecidas (Ej. Espionaje de las comunicaciones, control remoto de equipos, exfiltración, modificación o destrucción de información) durante un incidente de ciberseguridad.

- **Forense de *malware***. Orientado al análisis de dispositivos y software potencialmente maliciosos para determinar su origen, comportamiento y efectos potenciales en los sistemas TIC (Ej. Espionaje de las comunicaciones, control remoto de equipos, exfiltración, modificación o destrucción de información).

1.6 EVIDENCIAS DIGITALES

1.6.1 Introducción

Para poder ser utilizadas ante un tribunal, las evidencias digitales requieren ser objeto 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 que el DFIR realice una labor previa de localización de estas, para poder ser posteriormente analizadas conforme a una metodología forense.

A nivel nacional, puede recomendarse seguir la metodología expuesta en la *UNE 71506* "*Metodología para el análisis forense de las evidencias electrónicas*", de julio de 2013 (o sus posibles actualizaciones posteriores). Esta norma ha sido elaborada por el Comité Técnico *AEN/CTN 71* "*Tecnología de la Información*".

En esta norma se detalla una metodología para la obtención de resultados válidos en un procesado forense de las evidencias digitales. De esta forma, se pretende dar cumplida respuesta a la problemática causada por infracciones legales e incidentes informáticos acaecidos en entornos corporativos, ya que la obtención de evidencias digitales fiables y robustas ayuda a atribuir correctamente dichos hechos, pudiendo discernir si su causa tuvo como origen un carácter intencional o negligente por parte del usuario. Con dicha información se pretende conseguir ubicar de forma acertada los instrumentos, acciones, fines y demás parámetros concernientes a dichas conductas.

La información que puede ser investigada abarca el almacenamiento interno del dispositivo, la encontrada en los sistemas distribuidos y la ubicada en entornos virtuales, siempre y cuando esta información a analizar esté perfectamente localizada y ubicada en un espacio físico (*Where*).

1.6.2 Objeto y campo de aplicación

La *UNE 71506* tiene por objeto establecer una metodología para la preservación, adquisición, documentación, análisis y presentación de evidencias digitales.

Su ámbito de aplicación abarca cualquier organización con independencia de su actividad o tamaño. Además, este tipo de normas sirven de referencia tanto a los equipos de respuesta a incidentes y seguridad (IR Team, *Incident Responder Team*) como a los DFIR.

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

1.6.3 Términos y definiciones

La Norma *UNE 71505-1* "*Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales*" define como **evidencia digital** cada uno de los datos digitales recogidos en la escena de interés susceptibles de ser analizados con una metodología forense. Por su parte, una **muestra** es la parte representativa o significativa de una evidencia.

Se entiende por **información original** el conjunto organizado de datos que mantiene su integridad desde el inicio hasta el final del archivo o soporte informático que los contiene.

Se define como **cadena de custodia** el procedimiento de trazabilidad controlado que se aplica a las evidencias, desde el momento de su adquisición hasta su análisis y presentación final (ciclo de vida de la evidencia), el cual tiene como fin no alterar la integridad y autenticidad de estas, asegurando en todo este proceso que los datos originales no son alterados.

Se entiende por **clonado** el proceso de copia, realizada a bajo nivel y firmada digitalmente (mediante un algoritmo de resumen como MD5, SHA-1 o SHA-2), 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.

Una **imagen forense** es el producto de realizar un proceso de clonado de cualquier evidencia digital en un formato de archivo (Ej. RAW), sin tener en cuenta el soporte que la contiene.

El **entorno de análisis forense digital** es el lugar físico aislado del resto de actividades de la empresa u organismo donde se analiza la información digital, y que está dotado de los medios técnicos necesarios para poder llevar a cabo los trabajos forenses digitales. Dependiendo de la entidad de la organización, suele asociarse con la idea de laboratorio forense digital.

Un **informe pericial forense digital** es el documento donde se recoge y expone por escrito todas las tareas realizadas durante las diferentes fases del análisis forense digital, así como las tesis elaboradas a partir de las conclusiones extraídas durante la investigación en base a las evidencias encontradas.

Se entiende por **metadato** la información que describe el contenido de un dato. Los metadatos han cobrado gran relevancia debido la extensión del uso de Internet, por surgir la necesidad de utilizar los metadatos para la clasificación de la enorme cantidad de datos. Además, los metadatos pueden ayudar en la realización de búsquedas. Por ejemplo, si buscamos un artículo sobre vehículos, este dato tendrá sus correspondiente metadatos clave adjuntos, como cuatro ruedas, motor, etc. Otros ejemplos de usos de metadatos son las *metatags* en HTML, es decir, etiquetas con información sobre el propio documento web (Ej. Autor, editor, codificación); información en el propio sistema de ficheros (Ej. FAT, FAT32, NTFS, ext4, HFS); clasificaciones de contenido multimedia (fotografía, audio o vídeo).

Una **prueba electrónica** es la demostración en un procedimiento judicial de los hechos que fundamentan la aplicación de requerimientos formales, procesales y/o legales.

El ***Registro*** del sistema operativo es un conjunto de datos que almacena la información y configuraciones de todo el hardware, software, usuarios y preferencias. Por su parte, un **sistema de ficheros** recoge la organización lógica del almacenamiento de un dispositivo.

El concepto de **trazabilidad** hace referencia a la propiedad de la información de ser rastreada o reconstruida hasta su origen.

Se entiende por **virtualización** la emulación del funcionamiento del hardware, sistema operativo y aplicaciones de un dispositivo físico.

En general, se consideran como **artefactos volátiles** aquellos que se pierden al apagar o reiniciar el dispositivo objeto de la adquisición de evidencias. El orden de la adquisición de evidencias digitales en un sistema encendido viene determinado por el **orden de volatilidad** (*order of volatility*), que es el inverso de la persistencia, debiendo iniciarse el proceso con la recogida de los datos más volátiles (los menos persistentes) y finalizar con los menos volátiles (más persistentes). Puede tomarse como referencia el orden de volatilidad reflejado en la Tabla 2:

Orden de volatilidad	Artefacto	Modificación
Extrema volatilidad	Registros y caché del procesador.	Inferior a microsegundos.
Ultra volátil	Memoria RAM.	Microsegundos.
Muy volátil	Red (Ej. Tablas de enrutamiento, caché ARP).	Milisegundos.
Volátil	Tabla de procesos en ejecución, estadísticas del *kernel* del sistema operativo.	Segundos.
Volátil	Tráfico de red.	Segundos.
Volátil	Archivos temporales del sistema de ficheros.	Segundos.
No-Volátil	Sistema de ficheros del almacenamiento del dispositivo.	Minutos.
Estable	Configuración física, topología de red física.	Necesaria acción humana.
Estable	Cintas, disquetes, memorias USB, soportes ópticos (Ej. CD, DVD).	Años.

Tabla 2. Orden de volatilidad de las evidencias digitales.

Adicionalmente, el personal responsable de la recopilación de evidencias deberá tener en cuenta otros factores como: la efectividad, entendida como la probabilidad de que un dispositivo contenga información útil para la investigación; el nivel de esfuerzo, o recursos empleados para recopilar las evidencias, especialmente el tiempo necesario para extraer la evidencia (Ej. Extraer toda la información almacenada en una cabina de discos); la compatibilidad, o tiempo necesario para lograr los prerrequisitos para extraer las evidencias de un dispositivo; el nivel de pericia del propio personal para llevar a cabo la tarea; la alimentación del dispositivo (Ej. Batería restante, posibles caídas de tensión), por si se considera oportuno utilizar baterías externas para mantener el dispositivo encendido; la conectividad, pues los dispositivos conectados a redes cableadas o inalámbricas pueden ser manipulados remotamente para destruir las evidencias en almacenadas en ellos; o la aplicación de otras medidas antiforenses cuya intención sea denegar la extracción o destruir las evidencias.

1.6.4 Preservación de la evidencia

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 debe tener en cuenta los siguientes principios a la hora de interactuar con las evidencias digitales 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 estas de manera intencionada (*tampering*), o por los efectos de descargas electrostáticas, campos electromagnéticos o la conexión accidental a redes inalámbricas.

- El personal técnico encargado de una primera respuesta sobre las evidencias objeto de estudio debe poner especial cuidado en su almacenamiento en soportes adecuados para, además de garantizar esta integridad, poder preservar posibles evidencias físicas (Ej. Huellas dactilares, tejidos celulares, fluidos corporales) presentes en los soportes digitales.

- El 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 (Ej. Bolsas de Faraday) 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 por 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.

1.7 ADQUISICIÓN DE EVIDENCIAS DIGITALES

1.7.1 Inteligencia digital y recolección de evidencias de un escenario

La inteligencia digital y la recopilación de evidencias, como parte de la explotación de información disponible en un escenario, representan una nueva aproximación del método de procesar información de modelos de la amenaza móviles, sociales, virtuales y colaborativos.

Conforme a la publicación del Ejército de los EE.UU. *ATP 3-90.15 "Site Exploitation"* de 2015, la explotación de información de un escenario está compuesta por explotación táctica (*tactical exploitation*) y explotación técnica (*technical exploitation*).

Se entiende por explotación táctica el conjunto de actividades desarrolladas en un escenario o sus proximidades. Estas actividades permitirán detectar, recopilar y procesar el material de forma efectiva. La explotación del material recopilado permitirá contestar los requisitos de información y facilitar nuevas operaciones.

Por su parte, se entiende por explotación técnica el conjunto de actividades llevadas a cabo en entornos seguros (Ej. Un laboratorio forense en las dependencias de las FCSE) y con capacidades de procesado avanzadas.

Esta publicación también describe la utilización de procedimientos forenses para que las tareas de identificación y recolección de evidencias apoyen las fases de análisis y difusión de información del ciclo de *targeting* F3EAD (*Find*, *Fix*, *Finish*, *Exploit*, *Analyze*, *Disseminate*).

Ilustración 5. Ciclo F3EAD. Fuente: CCDCoE.

A medida que evolucionan las capacidades de explotación táctica de un escenario, el personal responsable de la recopilación de evidencias debe a su vez mejorar sus capacidades técnicas sobre el terreno, entre las que se encontrarían:

- Técnicas de búsqueda.
- Biometría.
- Forense.
- Explotación de documentos y soportes de información (Ej. Citas de vídeo, DVD, discos duros).

Desde un punto de vista del ciclo de *targeting*, los soportes de información digitales encontrados en un escenario son fuentes potenciales de evidencias que ofrecerán actividad C2 (*Command and Control*) con nodos de las redes del adversario (*proxies*). Si se realiza un interrogatorio a táctico concienzudo a los detenidos, podrían obtenerse pistas que condujeran a la atribución de cuentas en redes sociales desde las cuales se llevan actividades encubiertas de C2. Una operación de vigilancia de la ubicación de los *proxies* podría generar nueva inteligencia y nuevas intervenciones

en diferentes escenarios, lo que a su vez proporcionará nuevas evidencias y más inteligencia.

La explotación de información de un escenario está compuesta por las siguientes cinco actividades fundamentales:

- Detección.
- Recolección.
- Procesado.
- Análisis
- Difusión.

Estas actividades proporcionan la metodología que deberá adoptarse durante la recolección de soportes de información y de dispositivos electrónicos de telefonía móvil en el escenario.

1.7.2 Retos de la recogida de evidencias digitales

Cada vez es mayor el número de escenarios en los cuales deben intervenirse equipos electrónicos y soportes de información digital por su relevancia para una investigación en curso, o para explotar la información almacenada en ellos. Estos dispositivos y soportes de almacenamiento deberán ser adecuadamente identificados, conservados y asegurados para poder ser explotados o utilizados durante un proceso legal.

La información digital es inherentemente volátil debido a la complejidad de su estructura y la fragilidad del almacenamiento en la que se encuentra. La corrupción de unos pocos bits de información puede inhabilitar la correcta extracción del resto de la información almacenada. Además, para no contravenir la normativa de admisibilidad ante un tribunal, las evidencias digitales tendrán que ser presentadas de manera conveniente.

Cuando se manipulan evidencias digitales deben aplicarse los siguientes procedimientos forenses:

- Recolectar, securizar, y transportar las evidencias digitales de tal forma que no puedan ser alteradas.
- Las evidencias digitales deberán ser procesadas únicamente por personal cualificado para realizar esa tarea.
- Todas las tareas llevadas a cabo durante la incautación, transporte y almacenamiento de evidencias digitales deberán ser correctamente documentadas, almacenadas y encontrarse disponibles para su revisión.

El personal que recopila evidencias deberá detectar con rapidez y precisión todas las potenciales fuentes de evidencias (Ej. Contenido de la memoria RAM, tráfico de red, soporte de almacenamiento) y priorizar adecuadamente el orden de recopilación de evidencias conforme a su potencial criticidad y a su orden de volatilidad. Una vez recopiladas las evidencias, deberá garantizarse su integridad a lo largo del ciclo de vida de la evidencia.

1.7.3 Triaje de evidencias en un escenario

El personal responsable de la recopilación de evidencias en un escenario debe seguir un conjunto de principios que faciliten la búsqueda e incautación de información digital y dispositivos electrónicos. El CCDCoE (NATO *Cooperative Cyber Defence Centre of Excellence*) propone las siguientes fases, si bien el orden o el lugar para llevarse algunas de ellas quedarán al criterio del personal responsable de la recopilación de evidencias en el escenario. A modo de ejemplo, podría priorizarse la recopilación de evidencias volátiles sobre la documentación si se considera que la información de interés podría encontrarse en riesgo de no poder ser obtenida si se demora la acción.

Reconocimiento (*scan*)

- Examen visual del escenario para identificar todos los dispositivos electrónicos y soportes de almacenamiento existentes (Ej. Ordenadores sobremesa, ordenadores portátiles, servidores, soluciones RAID de almacenamiento, NAS inalámbricos, reproductores de música, memorias USB, discos duros externos, CD/DVD/Blue-Ray, teléfonos móviles, *tablets*, *wearables*, dispositivos GPS, videoconsolas, televisiones inteligentes, impresoras). Deberá tenerse en cuenta la posible aplicación de medidas antiforenses para ocultar dispositivos y/o soportes de almacenamiento (Ej. Numerosos objetos comunes sirven para ocultar memorias USB, como navajas suizas u objetos de *merchandising*).
- Examinar el área en busca de la presencia de redes cableadas y/o inalámbricas. Utilizar la información obtenida para descubrir otros dispositivos actualmente conectados, u otros que podrían estar temporalmente desconectados o apagados. En ocasiones, los dispositivos detectados podrían encontrarse ocultos a la vista. En el caso de las redes cableadas, bastará con seguir cada cable desde la boca del switch al dispositivo. En el caso de las redes inalámbricas, el límite de propagación de la señal limitará el área en la cual se encuentra el dispositivo. Deberá tenerse en cuenta la posible aplicación de medidas antiforenses para crear redes falsas.

Identificación (*identify*)

- Identificar los dispositivos electrónicos, los soportes de almacenamiento, la electrónica de red y los conectores.
- Identificar los dispositivos que se encuentran conectados a alguna red, ya sea interna o externa.
- Examinar los dispositivos en busca de cualquier posible daño físico.
- Identificar posibles trampas, *kill switches* o cualquier otro tipo de dispositivo que pueda representar una técnica antiforense. En determinados escenarios, no deberá descartarse la posible presencia de bombas trampa (*booby-traps*) con la intención de atentar contra la integridad física del personal de FCSE o FAS.

Documentar (*document*)

- Registrar documentalmente cualquier tipo de daño físico apreciable en los dispositivos o soportes de almacenamiento.
- Documentar gráficamente (Ej. Vídeo, fotografía) el escenario del cual se recogen los dispositivos y soportes de almacenamiento. Del mismo modo, deberá también documentarse las partes frontal y trasera de los dispositivos que serán incautados, anotando cualquier evidencia física (Ej. Conectores, cables, *dongles*, soportes de almacenamiento) antes de ser retirados.
- Se limitará la interacción con los dispositivos, salvo que esta esté previamente planificada.
- Utilizar etiquetas que incluyan las credenciales del personal que realizó la recogida de evidencias (Ej. Número identificativo, iniciales), marcando adicionalmente los dispositivos con cinta de evidencias para su correcta identificación visual.
- Generar listados del contenido de cada contenedor empleado para transportar las evidencias y sellarlos convenientemente con cinta de evidencias siempre que sea posible.
- Documentar gráficamente todas las actividades llevadas a cabo y mantener la cadena de custodia.

Securizar (*secure*)

- Preservar cualquier material impreso o evidencia en papel.
- Determinar si los dispositivos se encuentran apagados o encendidos. Cuando se encuentren encendidos, la pantalla podría contener información de interés, debiendo entonces ser documentado gráficamente. En caso contrario, deberá tratar de identificarse luces o sonidos que indiquen la presencia de dispositivos encendidos.
- Intentar acceder al contenido de datos con un alto índice de volatilidad. En ocasiones, podrían haberse empleado técnicas antiforenses para evitar el volcado del contenido de la memoria RAM del dispositivo.
- Apagar los dispositivos únicamente si es estrictamente necesario (Ej. Extracción de los soportes de almacenamiento de un ordenador) y anotar la fecha y hora de su apagado.
- Preservar la integridad de los dispositivos electrónicos y los soportes de almacenamiento incautados transportándolos en cajas rugerizadas, bolsas de Faraday, bolsas antiestáticas o paños de algodón.

Mantener la presencia (*sustain*)

- En determinados escenarios, la acción principal consistirá en la instalación de software en los dispositivos que permita controlar la actividad de su usuario sin su conocimiento.
- Utilizar la conexión a Internet del dispositivo o crear un canal de comunicación temporal para extraer los datos de interés almacenados en los dispositivos digitales.
- Emplear redes inalámbricas y otras tecnologías de comunicación acordes al escenario.

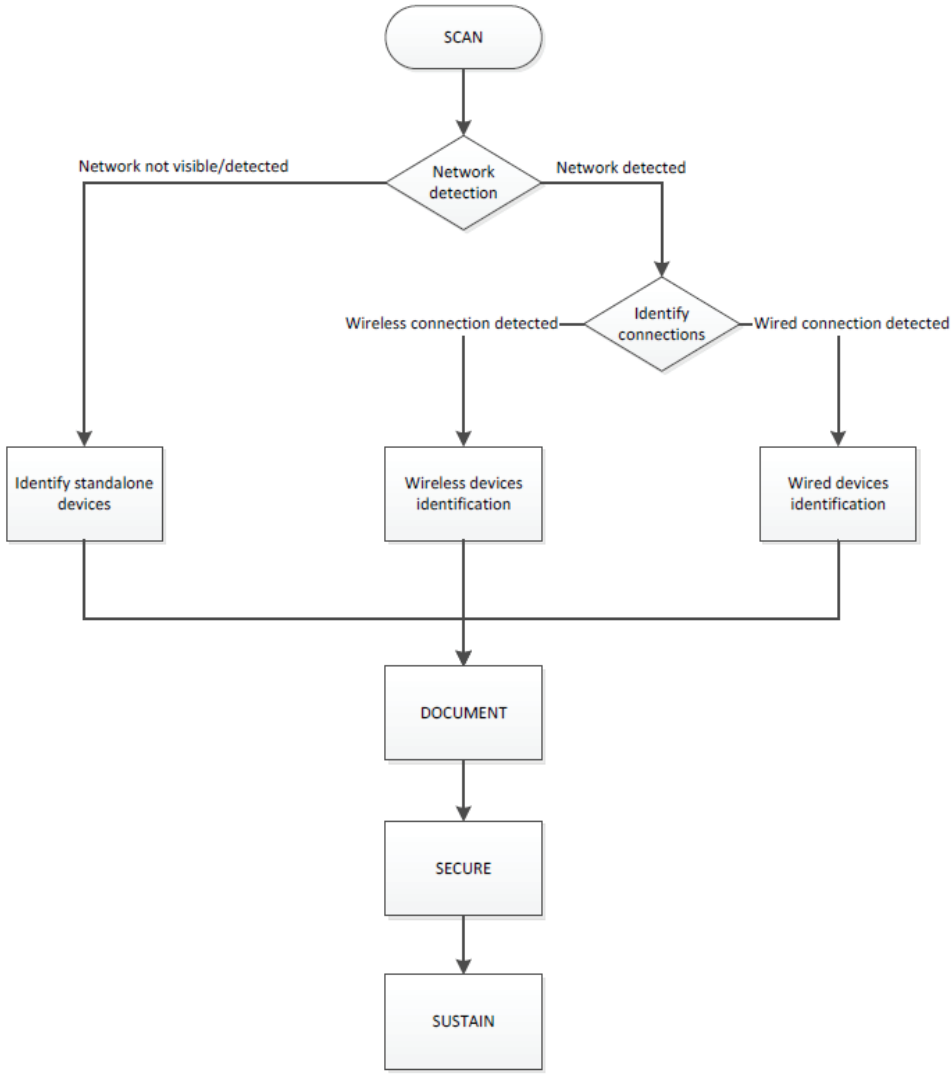

Ilustración 6. Recolección de evidencias digitales. Fuente: CCDCoE.

El organigrama de recolección de evidencias digitales representado en la Ilustración 6 puede ser ampliado en caso de detectarse medidas antiforenses a otro como el representado en el organigrama de la Ilustración 7.

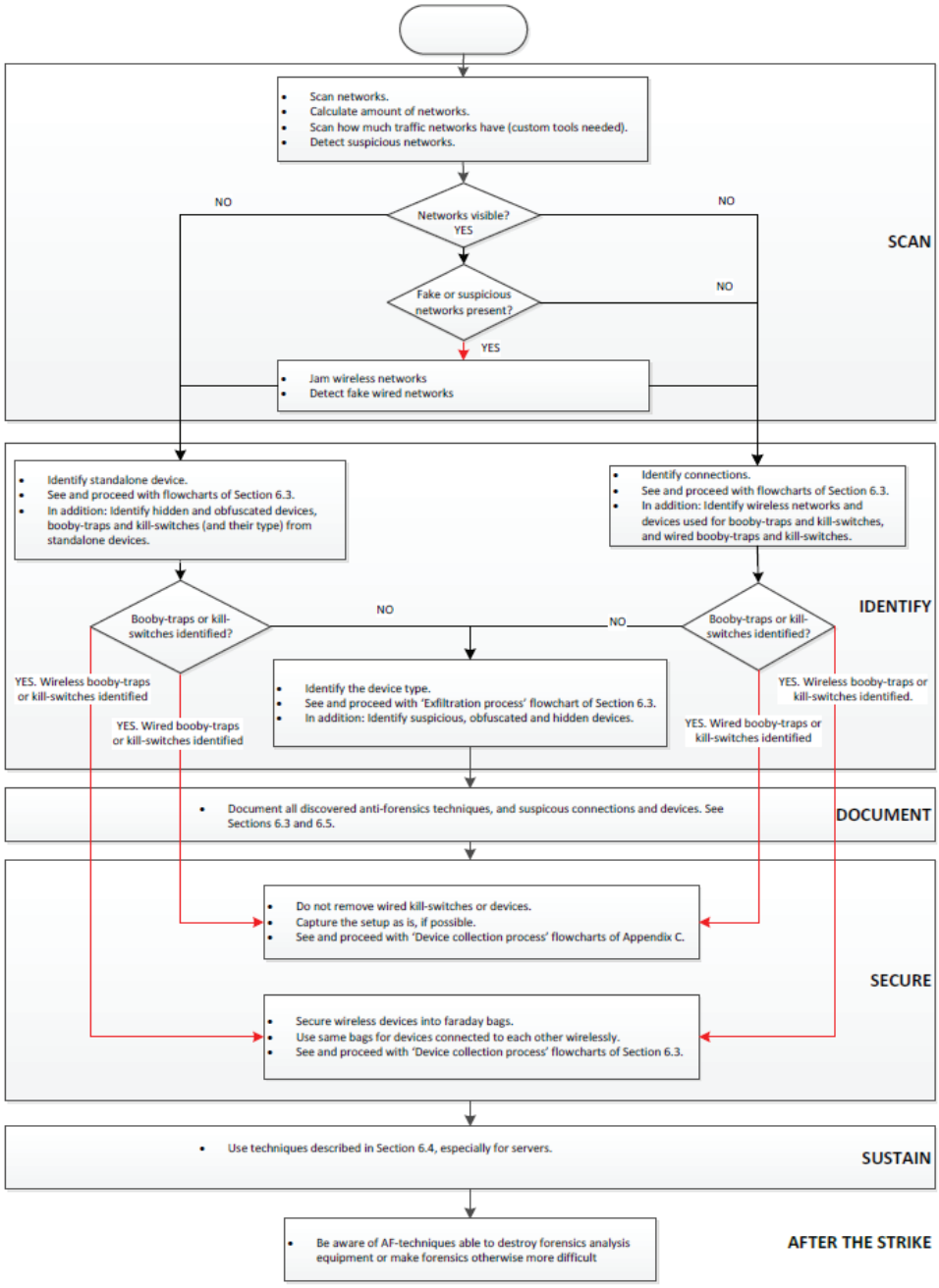

Ilustración 7. Recolección de evidencias digitales en escenarios donde se aplican medidas antiforenses. Fuente: CCDCoE.

1.7.4 Proceso de adquisición de evidencias digitales

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

- Un clonado forense;
- La realización de imágenes completas o lógicas de la información de interés.

A tal fin, se debe seguir un procedimiento documentado por cada organización, 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:

- La adquisición de información de dispositivos apagados (*muertos*);
- La adquisición de información de dispositivos encendidos (*live*), donde la aplicación de métodos intrusivos, aunque sean mínimos, puede comprometer de algún modo la integridad de la información original a investigar.

En el caso de que la organización no contase en el emplazamiento con un equipo de adquisición de evidencias especializado, es recomendable que el equipo de adquisición actuando como primer escalón de respuesta cuente con al menos con dos personas y que se asista, en su caso, de otro personal técnico especializado.

En todo caso, los técnicos que vayan a realizar la adquisición de evidencias digitales deben estar previamente debidamente autorizados por la organización propietaria del sistema. En el caso de personal externalizado, 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 organización.

En todos los casos, para asegurar la independencia de las actuaciones forenses, se recomienda la presencia de un fedatario público (Ej. Secretario judicial, notario) o de terceros independientes (Ej. Delegados sindicales, peritos terceros) que den fe de este proceso. En determinadas investigaciones corporativas, la adquisición de evidencias digitales tendrá que realizarse en presencia del propio usuario del dispositivo (y quizás este pueda requerir la presencia de un abogado de parte durante el proceso, o el ya mencionado representante sindical, o ambos). Se recomienda

también, siempre que sea posible, realizar la grabación en vídeo (con *timestamp*) de todo el proceso de recogida y clasificación de evidencias.

El personal encargado de la adquisición de evidencias digitales debe seguir un procedimiento de adquisición documentado y aprobado previamente, utilizando además herramientas de hardware y software reconocidas en el ámbito forense (a ser posible, certificadas por un organismo de reconocido prestigio, como el Departamento de Justicia de los EE.UU.), 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.

Es recomendable que el personal técnico encargado de efectuar la adquisición de la información almacenada en los distintos equipos y dispositivos objeto de investigación sea previamente informado y conozca la política de seguridad que posee la organización, especialmente en lo relativo a los cuatro aspectos siguientes:

- **Control de acceso a dispositivos**. Permite acceder a los dispositivos con los privilegios necesarios. El personal de la organización no sólo tiene que acceder al local donde se ubica el dispositivo, sino autenticarse para poder acceder al propio dispositivo (o a un entorno en red desde dicho dispositivo), ya sea empleando un único factor de autenticación (Ej. usuario/contraseña, factor biométrico, *token* RFID) o uno múltiple (Ej. *token* RFID+ PIN, factor biométrico+ PIN).

- **Existencia de un registro de eventos**. Es buena práctica de seguridad lógica que las organizaciones que dispongan de registro de eventos lo centralicen con todas aquellas operaciones que se determinen conforme a sus políticas de seguridad.

- **Calendario de auditorías**. Conocimiento del plan de auditorías internas y externas periódicas que garanticen que la seguridad de la información de la organización no se encuentra comprometida con la tecnología vigente en ese momento.

- Conocimiento del sistema de gestión y control de las copias de seguridad de los datos, así como saber la ubicación de los soportes donde se lleva a cabo.

Si el lugar del incidente está delimitado físicamente, el personal técnico 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 dispositivos ubicados en dicho lugar.

2. Identificar al administrador de los distintos sistemas IT, caso de tener que solicitarse su soporte 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 de las evidencias comprometidas. Si el dispositivo está encendido, conviene obtener grabación en vídeo, realizar fotografías y/o anotar por escrito lo que se visualiza en la pantalla del dispositivo.

4. Buscar en el entorno que rodea al dispositivo cualquier tipo de nota manuscrita o impresa que pudiera estar asociada a credenciales de acceso a los dispositivos (Ej. *Post-it*, agendas personales, un archivo de texto en el escritorio del sistema operativo) y manuales técnicos de los dispositivos involucrados.

5. Siempre que sea posible, documentar mediante grabación en vídeo y/o fotografiar la escena de interés, anotando detalladamente la posición original de los distintos equipos con el cableado correspondiente y sus periféricos (Ej. Módem, impresoras, *routers*, cámaras del circuito CCTV que pudieran encontrarse en el local), 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 donde se analizarán las evidencias.

6. Etiquetar convenientemente todos los dispositivos y el cableado asociado con las evidencias de interés. Las etiquetas deben colocarse en lugares no relacionados con elementos mecánicos de los dispositivos, de manera que queden visibles sus números de serie u otros datos de relevancia para su correcta identificación.

7. Localizar todos los dispositivos inalámbricos que permitan conectividad radioeléctrica en la zona, tanto los públicamente visibles (Ej. En WiFi, emiten en abierto su SSID) como los que operan ocultando su identificador, determinando la banda de frecuencias y canales empleados. Si la escena lo recomienda, deben activarse equipos que inhiban a la misma de interferencias radioeléctricas externas (*jammers*).

8. Prestar especial atención para no desconectar las fuentes de alimentación cuando las evidencias estén almacenadas en soportes volátiles (Ej.

Memoria RAM, conexión de red). En el caso de equipos dependientes de baterías (Ej. Tabletas, teléfonos móviles, ordenadores portátiles), se deben mantener, en la medida de lo posible (el equipo de recogida de evidencias deberá disponer del kit más amplio posible de conectores para maximizar la gama de dispositivos compatibles), 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 (Ej. Un soporte óptico en el lector óptico, una tarjeta SD en el lector de tarjetas de memoria).

Igualmente, conviene no desvincular los soportes digitales de almacenamiento (Ej. Cintas de grabación, cintas de datos, discos duros) de los equipos en los que operan (Ej. Audiodiscos, sistemas CCTV) pues, en muchos casos, dichos soportes vienen asociados al equipo correspondiente. En caso de tener que realizar 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 que estuvieran conectados a una 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 (Ej. NAS) y distribuidos (Ej. Almacenamiento *en la nube* ofrecido por un proveedor de servicios, como *Dropbox*, *Google Drive*, *Microsoft OneDrive*).

1.7.5 Dispositivos apagados

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

- Antes de comenzar el proceso de clonado forense (copia bit a bit, es decir, una copia íntegra de los datos del sistema de almacenamiento del dispositivo original) de la evidencia, el soporte de almacenamiento destino debe ser sometido a un proceso de borrado seguro y estar dentro de su ciclo de vida útil. Dicho soporte debe estar libre de cualquier tipo de información previa. Idealmente, y en aquellas corporaciones con mayores recursos económicos, será un dispositivo de almacenamiento "a estrenar" (es decir, que desde su fabricación hasta su utilización para el clonado forense no haya sido utilizado).

- Utilizar *write blockers* (dispositivos que manipulan la evidencia original en modo solo lectura), evitando que se puedan producir modificaciones en ella durante el proceso de clonado forense.
- Efectuar un resumen digital (*hash*) de la información contenida en el soporte de almacenamiento original de forma simultánea al proceso de clonado u obtención de la imagen a bajo nivel, utilizando uno o varios algoritmos resumen que garantice una baja colisión (Ej. SHA-1, SHA-2).
- Efectuar el cálculo del valor del *hash* de la información contenida en el soporte destino donde se realizó el clonado forense utilizando los mismos algoritmos de resumen empleados con la evidencia original.
- Comprobar que los valores de los *hashes* obtenidos de la evidencia original y de la copia forense coinciden, lo cual garantiza la integridad de los datos almacenados en la copia forense. Esta integridad de la información almacenada en la copia forense permitiría realizar a partir de ella posteriores copias forenses o imágenes siguiendo el procedimiento descrito.

Finalizado el proceso anterior, los soportes de información originales deberán volver a ser precintados junto con los equipos donde se encontraban instalados, quedando igualmente almacenados en el recinto o área dedicados expresamente para tal fin.

Extracción de evidencias de dispositivos móviles apagados

En el caso concreto de los dispositivos de telefonía móvil, *phablets*, tabletas y *wearables* con conectividad a través de redes de telefonía móvil, etc., se debe proceder además a la extracción de la información almacenada en la tarjeta SIM (Ej. Contactos, SMS) 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 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 debe realizarse un *hash* de su contenido para así garantizar la no alteración de los datos extraídos, caso de tener que efectuar más copias o imágenes de éstos.

1.7.6 Dispositivos encendidos

La obtención de evidencias forenses digitales de dispositivos encendidos, o "en vivo" (*live*), comprende el conjunto de acciones a llevar a cabo en aquellos dispositivos que se encuentran en funcionamiento en el momento de su intervención por el equipo de primera respuesta.

La principal ventaja de este escenario con respecto al escenario de obtención de evidencias de dispositivos apagados es la posibilidad de obtención de información de carácter volátil (es decir, no persistente), la cual desaparece con el apagado o el reinicio del dispositivo.

Otra de las principales ventajas de este método de análisis forense es precisamente su pequeño impacto en la operatividad del sistema (Ej. no existe tiempo de caída del sistema; esta característica es de especial importancia a la hora de extraer información de sistemas críticos) durante el proceso de obtención de evidencias digitales.

La adquisición de evidencias en este caso debe realizarse desde el propio sistema operativo en ejecución del dispositivo, intentando minimizar al máximo la alteración o impacto en el sistema, con vistas a su análisis posterior, pudiendo entonces emplearse la metodología utilizada con los dispositivos apagados.

Esta cualidad puede ser especialmente 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 la adquisición de evidencias debe documentar perfectamente todos los procesos efectuados.
- Estas técnicas no permiten su reproducibilidad. Es decir, el contenido de la memoria es dinámico, los archivos temporales, el registro del sistema operativo, etc. Las capturas de evidencia en vivo son equiparables a *fotografías* del estado del sistema en el momento que se realiza la adquisición de las evidencias. Por tanto, la validez de los resultados obtenidos ante un tribunal dependería en gran parte de la correcta justificación en el informe pericial.

- El informe 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 utilizando dispositivos hardware adecuados, o vía software, activando comandos perfectamente conocidos (Ej. *Scripts* validados para los procesos de obtención de la organización), caso del acceso a los datos de la evidencia a través de un entorno remoto.

En estos casos, el cálculo del valor del *hash* es dinámico. Según el instante temporal en que se efectúe el cálculo del resumen, se obtendrá un resultado diferente. No obstante, es una buena práctica generar el *hash* de la evidencia digital generada, pues permite identificar de forma única la evidencia, garantizando así la posibilidad de contrastar la integridad de cualquier copia que se realice de la evidencia digital adquirida con posterioridad.

El responsable técnico de la obtención de evidencias deberá prestar especial atención ante la posible presencia en el dispositivo de medidas antiforenses (Ej. Esteganografía, discos con cifrado *full-disk*), y/o en las investigaciones donde el dispositivo a investigar pudiera existir una infección por *malware*.

El responsable técnico de la obtención de evidencias deberá utilizar su propio kit de herramientas del sistema (versión portable, a ser posible) para soslayar una posible contaminación de la adquisición de evidencias si se hiciese uso de las propias herramientas instaladas en el sistema operativo del dispositivo a analizar en el caso de que se encontrase comprometido por algún tipo de *malware*.

Extracción de evidencias "en vivo" de dispositivos móviles

Por su parte, la adquisición de evidencias en vivo procedentes de dispositivos móviles se ve afectada por la peculiaridad de estos dispositivos de poder interactuar con redes inalámbricas (Ej. WiFi, *Bluetooth*) y/o de telefonía móvil (Ej. GSM, 3G, 4G). Por este motivo, los dispositivos móviles deben ser protegidos o aislados electromagnéticamente de la manera pertinente (Ej. Bolsa de Faraday, jaula de Faraday) para garantizar que durante su manipulación no puedan conectarse utilizando sus interfaces de red a las citadas redes. De esta forma se evita que una manipulación accidental por parte del equipo de obtención de evidencias o maliciosa en remoto por parte del propietario del dispositivo (o el agente malicioso que lo controla a través de un servidor de mando y control) pueda dañar o destruir la información almacenada en el dispositivo.

Una buena praxis de obtención de evidencias de dispositivos móviles encendidos consiste en seguir las recomendaciones siguientes:

- Realizar un proceso de copia o clonado de las partes accesibles de la tarjeta SIM original, empleando para ello un lector de tarjetas con su software específico, y se debe proceder seguidamente a introducir esta tarjeta clon en el dispositivo móvil. Reseñar que la tarjeta clon carece de las claves de acceso a la red de telefonía móvil de la tarjeta SIM original. Esto impide que el dispositivo móvil se conecte a dicha red, evitando así tener que procesar las evidencias en el interior de una jaula de Faraday (elevado coste y tecnológicamente complejo de construir) o entorno de similares características.
- Arrancar el dispositivo móvil con la tarjeta clon insertada y realizar una copia a bajo nivel, conocida también como extracción física, de los datos en la memoria o memorias internas del dispositivo móvil.

No obstante, existen casos en los cuales las herramientas hardware/software específicas para forense de dispositivos móviles no soportan la copia física del modelo concreto objeto de la investigación.

Como primera alternativa, algunos de esos dispositivos permiten realizar una extracción lógica (copia del sistema de ficheros del dispositivo móvil). La extracción lógica no permite obtener la misma información que la extracción física, no pudiendo por ejemplo realizar *carving* de información perdida o eliminada (accidental o intencionadamente) o acceder al espacio no utilizado de la memoria del dispositivo.

Existe también la posibilidad de 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 un software de análisis de datos capaz de interpretar el volcado realizado.

Además, en aquellos escenarios en los cuales no se pueda proceder a una extracción física (porque no lo soporta el equipo del DFIR) o lógica (Ej. No se encuentra activada la opción ADB en el dispositivo móvil con sistema operativo *Android*) de la información, existen dos alternativas:

- Reflejar en el informe forense digital la información visualizada en la pantalla del dispositivo móvil. En este caso, se recomienda encarecidamente grabar en soporte audiovisual todo el proceso de obtención de evidencias para adjuntarlo como prueba pericial.
- Extraer la información del dispositivo empleando técnicas de manipulación de su hardware (Ej. JTAG/*Chip-off*).

Una vez finalizado la adquisición de evidencias del dispositivo móvil, los miembros del equipo de obtención de evidencias no deben introducir ni la batería ni la tarjeta SIM original en el dispositivo a fin de impedir la alteración del archivo de localización (LOCI, *LOCation Information*) de la SIM, unido a la modificación del listado de llamadas almacenadas.

Una vez realizado el volcado de la información de las diferentes memorias (Ej. NAND, microSD) debe generarse su valor resumen para garantizar la integridad de los datos extraídos.

1.7.7 Obtención de evidencias de activos empresariales

En ocasiones, el DFIR se enfrentará a escenarios donde la evidencia de la investigación se encuentra almacenada en un sistema de información masiva centralizado (Ej. RAID, SAN, NAS). En la mayoría de estos casos, no es plausible realizar un duplicado completo de la fuente original debido al gigantesco volumen de datos o la complejidad de la configuración del almacenamiento.

El DFIR debe determinar dónde reside la información relevante y elaborar un plan adecuado de obtención para crear una copia lógica únicamente de esta información. Herramientas corporativas como *Guidance EnCase* o *AccessData FTK* disponen de características que permiten copiar y almacenar copias lógicas de archivos en contenedores propietarios. El proceso de copia y los contenedores resultantes preservan los metadatos originales de cada archivo fuente e incluyen un resumen para poder comprobar la integridad de los datos en el futuro.

Si el sistema de almacenamiento de datos es pequeño o de tamaño moderado, el DFIR puede disponer de tiempo y recursos para completar el duplicado completo. No obstante, algunos sistemas de almacenamiento utilizan métodos propietarios para almacenar la información y gestionar el soporte de almacenamiento. Esto podría llegar a impedir al DFIR reconstruir con posterioridad los duplicados a un estado operativo.

Por este motivo, si el DFIR conoce la información que es relevante, puede ser mejor solución realizar una imagen en vivo del volumen montado o crear copias lógicas de los archivos. En cambio, si no está seguro de qué información es relevante, o si se tiene un control continuado sobre el sistema de almacenamiento, el DFIR puede optar por crear imágenes completas a nivel físico del soporte de almacenamiento e intentar crear un reensamblado que resulte operativo. Esta aproximación provocará que la unidad de almacenamiento esté fuera de servicio durante un periodo prolongado de tiempo.

1.7.8 Sistemas virtualizados

Actualmente, es frecuente que al analizar el DFIR el contenido de un dispositivo detecte la presencia de información almacenada en soportes de almacenamiento virtual dentro de entornos virtualizados.

En los entornos virtualizados, el hardware, software y aplicaciones de un dispositivo (en su conjunto, la máquina virtualizada es conocida como *guest* o *virtual machine*) es emulada dentro de un dispositivo físico conocido como *host* utilizando sus recursos hardware disponibles (procesador, memoria RAM y espacio físico del dispositivo de almacenamiento). Dependiendo de sus recursos hardware, un mismo *host* puede ejecutar concurrentemente varios dispositivos virtualizados.

Este tipo de entornos virtualizados están cada vez más extendidos, pudiendo actualmente encontrarse tanto en un dispositivo doméstico como en un dispositivo de un entorno corporativo 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 archivos (configuración del hardware del equipo, memoria RAM, y uno o más espacios de almacenamiento en disco virtuales). Desde el punto de vista del sistema *host*, estos espacios de almacenamiento virtualizados se corresponderán con uno o varios archivos. Dependiendo del hipervisor, sus extensiones serán *.vhd*, *.vmd*, *.img*, etc.

Cuando el equipo de obtención de evidencias se enfrenta a un escenario virtualizado, debe recoger:

- Los archivos almacenados en el *host* correspondientes al soporte de almacenamiento virtual de los sistemas *guest*, es decir, copiar los archivos apropiados de este entorno.
- De encontrarse en estado de suspensión las máquinas virtuales, el volcado de la parte de la memoria RAM del *host* utilizada por la máquina virtual. Este volcado se analizará posteriormente de forma similar al volcado de una memoria RAM física.

El DFIR debe recordar documentar la fuente de la evidencia digital, el valor resumen y el resto de los detalles, como en cualquier otra investigación. Este sistema resulta especialmente eficiente para capturar la imagen forense de un servidor.

En este ámbito, una vez obtenidos todos los archivos de configuración del entorno virtualizado, el DFIR podrá reproducir el entorno original del equipo virtualizado para proceder a su análisis forense.

1.7.9 Extracción de evidencias mediante manipulación hardware

JTAG

JTAG (*Joint Test Action Group*) es un estándar industrial para la verificación de diseños y comprobar el correcto funcionamiento de las PCB (*Printed Circuit Board*) tras su fabricación. Es la denominación más utilizada para la norma *IEEE 1149.1* "*Standard Test Access Port and Boundary-Scan Architecture*" de 1990. En 1994 se agregó un suplemento que contiene una descripción de BSDL (*Boundary Scan Description Language*).

Pese a que fue diseñado originalmente para comprobar las PCB, actualmente también es utilizado para la comprobación de submódulos de IC (*Integrated Circuit*) y depurar aplicaciones embebidas. La mayoría de los procesadores modernos soportan JTAG cuando tienen suficientes pines. Dispositivos electrónicos como los smartphones solo disponen de este tipo de interfaces de depuración.

Desde el punto de vista forense, se conoce como **forense de JTAG** (JTAG *forensics*) al proceso de adquisición de evidencias que implica la conexión al TAP (*Test Access Port*) estándar de un dispositivo. Esta conexión se realiza utilizando soldador, *molex* o *jig* y una *JTAG Box* que permita transmitir órdenes al procesador para adquirir un volcado completo en crudo de los datos almacenados en el chip de memoria.

Esta técnica está considerada como no destructiva. El riesgo de modificar los datos almacenados es mínimo y no requiere desoldar el chip de memoria.

Esta técnica tiene también ciertos inconvenientes. En primer lugar, el proceso de obtención de la imagen puede resultar lento. Además, no todos los dispositivos móviles disponen de interfaz JTAG, de ahí que se desarrollase una tecnología de pruebas denominada *boundary scan*. En ocasiones, puede resultar complejo encontrar el puerto de pruebas de acceso.

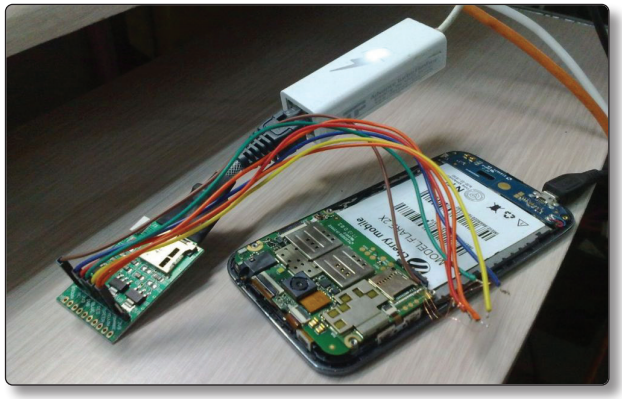

Ilustración 8. Ejemplo de JTAG para la obtención de datos de un dispositivo móvil.
Fuente: Digital Forensics Corp.

En segundo lugar, la extracción de datos debe realizarse conociendo el procesador y circuitos de memoria del dispositivo del cual pretende extraer los datos y cómo se encuentran conectados al bus del sistema. En aquellos escenarios en los cuales la interfaz JTAG no se encuentra accesible desde el exterior, deben identificarse cuáles son los puntos de prueba de la PCB y determinar la correspondencia de estos puntos con cada una de las diferentes señales. Debe conocerse además cuál es el voltaje correcto que evite dañar físicamente la memoria (lo que obviamente supondría la pérdida de los datos en ella almacenada) y el protocolo que debe ser utilizado para poder leer el contenido de la memoria.

Modo EDL

Los procesadores del fabricante Qualcomm disponen de una característica denominada modo EDL (*Emergency Download*) que consiste en un modo de arranque alternativo al *bootloader* primario. El modo EDL permite realizar un volcado completo de los datos de los chips de memoria de un dispositivo (*full dump*), desbloquearlo (*unbricking*) o volcar un contenido en su memoria (*flashing*). Esta técnica está limitada por el modelo de dispositivo y por la versión de parches de seguridad de su sistema operativo.

Ilustración 9. Ejemplo de cable EDL para dispositivos del fabricante Xiaomi. Fuente: DHgate.

Existen tres métodos diferentes para intentar establecer el modo EDL en un dispositivo, y ninguno de ellos funciona en todos los dispositivos. En algunos modelos, basta con utilizar un cable especial, en otros casos, hay que desmontar el dispositivo y manipular pines de JTAG. En los dispositivos con sistema operativo

Android, si el dispositivo se encuentra desbloqueado, puede utilizarse ADB (*Android Debug Bridge*) para reiniciarlo en modo EDL.

El método más sencillo suele ser utilizar un cable EDL. Este cable dispone de un botón que permite cortocircuitar los pines de datos adecuados forzando al dispositivo a establecer el modo EDL. Una vez que se encuentra establecido el modo EDL, puede llevarse a cabo el volcado de memoria conocido como extracción física.

En aquellos escenarios en los cuales el cable no permite establecer el dispositivo en modo EDL, puede cortocircuitarse el pin CMD de los puertos de test para indicar al dispositivo que se reinicie en modo EDL.

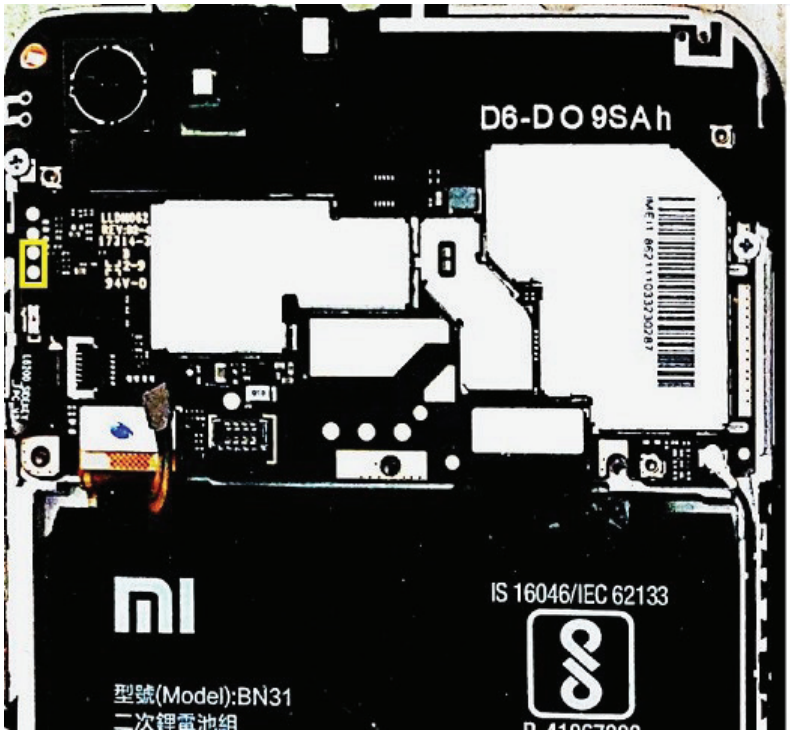

Ilustración 10. Ejemplo de los puertos que deben ser cortocircuitados para establecer el modo EDL en un dispositivo Xiaomi Note 5A. Fuente: Magnet Forensics.

Una vez que se abre el dispositivo y se identifican los puertos de test necesarios, pueden cortocircuitarse empleando pinzas de electrónica u otro objeto metálico mientras que se inserta el cable USB en el dispositivo. No obstante, ni todos los dispositivos disponen de puertos de test JTAG ni la técnica funciona con todos los dispositivos.

En aquellos escenarios en los que se encuentra habilitado en el dispositivo el modo ADB (es decir, el dispositivo se encuentra encendido, desbloqueado y establecido el modo de depuración USB) puede establecerse el modo EDL mediante el comando *adb* de *Android Studio*:

```
adb reboot edl
```

Chip-off

Se conoce como **forense de *chip-off*** (*chip-off forensics*) o desoldado forense (*forensic desoldering*) a un conjunto de técnicas de adquisición de evidencias consistente en el desoldado de un chip de memoria no volátil del dispositivo móvil objeto de la investigación y su posterior conexión a lector de este tipo de memorias.

Ilustración 11. Ejemplo de lector de chips eMMC y eMCP para técnicas chip-off. Fuente: Amazon.

Debido al calor del proceso de desoldado puede resultar dañado el chip, lo que supondría la pérdida de los datos en él almacenados. Por este motivo, suele considerarse la última alternativa de extracción de datos a adoptar. Además, requiere disponer de un laboratorio dotado de material específico de coste relativamente elevado y de personal altamente experimentado en estas técnicas.

Ilustración 12. Ejemplo de banco de trabajo para realizar JTAG, chip-off e ISP. Fuente: TeelTechnologies.

ISP

Se conoce como ISP (*In-System Programming*) a la técnica de conexión a un chip de memoria *flash* del tipo eMMC (*Embedded Multimedia Card*) o eMCP (*Embedded Multi-chip Package*) para realizar un volcado completo de la memoria de un dispositivo sin tener que extraer el chip o destruir el dispositivo. Este tipo de memorias son las más utilizadas actualmente en los dispositivos móviles.

No obstante, y dado que la identificación de los TAP conectados al chip se realiza utilizando un multímetro, en ausencia de documentación previa del dispositivo del que debe realizarse el volcado de memoria, será necesario disponer de otro dispositivo idéntico que pueda ser destruido durante el proceso de descubrimiento de los TAP.

2

SOPORTES DE ALMACENAMIENTO Y SISTEMAS DE FICHEROS

2.1 INTRODUCCIÓN

Brian Carrier es uno de los más prestigiosos autores en forense digital y programador de la conocida herramienta de análisis forense de código abierto *Autopsy*. Su libro *File System Forensic Analysis* sobre análisis forense del sistema de ficheros, pese a haber sido publicado en el año 2005, es referencia habitual en multitud de cursos forenses por la granularidad de detalle alcanzada en su exposición sobre el análisis forense de información persistente.

Carrier establece en varios niveles de abstracción el análisis de un soporte de almacenamiento convencional:

- **Análisis físico de medios**, aplicado sobre los sectores de datos.
- **Análisis de volúmenes**, aplicado sobre los volúmenes del disco.
- **Análisis del sistema de ficheros**, aplicado sobre los archivos de un determinado volumen.
- **Análisis de aplicaciones**.

Un DFIR debe comprender la organización del almacenamiento persistente, desde el nivel físico del funcionamiento del disco hasta el sistema de ficheros, para poder comprender la manera en la que se puede ocultar información en el disco y no ser accesible desde la interfaz del sistema de ficheros.