CURSO DE ESPECIALIACIÓN
CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Análisis Forense Informático

Unidad 2. Identificación, preservación y adquisición de evidencias

Índice

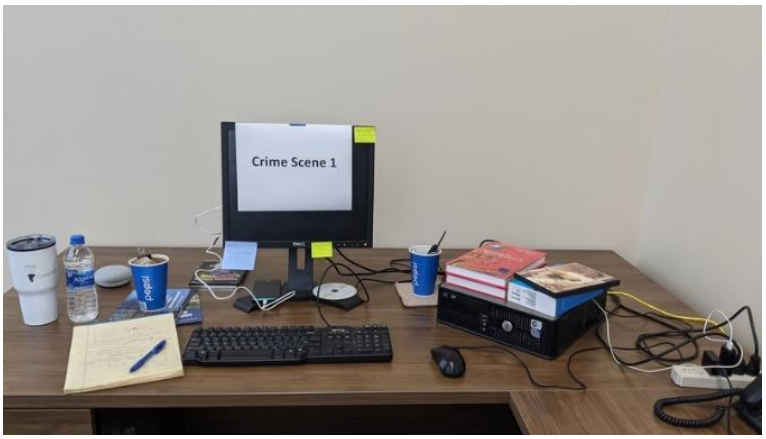
1 Introducción.

Como vimos en la unidad anterior, el proceso forense sigue estos pasos de la imagen. A continuación veremos los 3 primeros pasos de la metodología forense un poco más en detalle.

2 Identificación del escenario.

En este primer estadio del proceso debemos:

- **Acotar el entorno** en el que se ha producido el incidente. A continuación, debemos recopilar y documentar (entre otras cosas):
    - Tipo de evidencia involucrada.
    - Sistemas operativos y software involucrados.
    - Formato de los sistemas de ficheros.
    - Localización física de la evidencia (hacer fotografías).



    - Motivo de la recogida de pruebas (caso, sospecha, …).
- Para esta tarea, es muy importante:
    - Ser o tener **profesionales** con conocimientos adecuados.
    - Disponer de un **laboratorio forense**.
    - Disponer de **materiales apropiados** para recoger y procesar las evidencias.

2.1 Evaluación de las evidencias.

Una **evidencia digital** es una **pieza de información digital** guardada o transmitida entre uno o varios sistemas de información y que se puede utilizar como **prueba en un proceso judicial**.

La evidencia digital debe ser evaluada respecto al alcance de cada caso:

- Revisar la **autorización legal** si es necesaria, como por ejemplo necesitar una orden de registro hecha por un juez.
- Valorar con el investigador principal que se puede o no descubrir mediante la realización del forense.

- Estudiar la posibilidad de obtener otras evidencias:
    - Por ejemplo: Envío de una **orden de preservación de datos de tráfico de red** a un ISP.
- Considerar la **relevancia de los periféricos** en el caso:
    - Por ejemplo: Robo o fraude: tarjetas de crédito en blanco, papel de cheques, impresoras, escáneres, etc.
    - Dispositivos externos extraíbles, almacenamiento en la nube, etc.
- Determinar si hay **información adicional** al caso:
    - Por ejemplo: Cuentas de correo, ISP, usuarios, configuración de red, etc

3 PRESERVACIÓN

La metodología de recolección y preservación de las evidencias implica documentar exhaustivamente los siguientes puntos:

- El escenario: fotografías, notas...
- El método de obtención de la evidencia: método y herramientas de extracción
- La cadena de custodia: crear los documentos y anexar a las evidencias
- El hardware y la configuración del sistema
- La hora y fecha del sistema
- Las fechas y horas clave de los sucesos (**línea de tiempo**)

3.1 La escena del incidente o crimen.

Las siguientes acciones se realizan habitualmente mientras investigamos en la escena del crimen o incidente:

- Identificar el número y tipo de equipos
- Determinar si hay una **red presente**
- **Entrevistar** al **administrador de sistemas y usuarios** para obtener información por ejemplo de quién puede acceder a qué.
- Identificar y documentar los **tipos y volúmenes de datos**, incluyendo medios extraíbles
- Identificar **áreas de almacenamiento externo**
- Identificar **software propietario**.

3.2 Cadena de custodia.

La **cadena de custodia** de una prueba se define como:

> Procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos. Tiene por finalidad **no viciar el manejo que se haga de las evidencias y así evitar alteraciones, sustituciones, contaminaciones o destrucciones**.

Se necesita un documento que asegure la **integridad de la evidencia** como prueba ante procesos judiciales. El primer paso deberá ser:

- la realización de una **adquisición** de esta **ante fedatario público (notario o secretario judicial)**
- la evidencia original no puede ser accedida, en ningún momento, por el perito informático.
- En ese momento, se data la evidencia.

Así, **cada evidencia precisa de un documento de cadena de custodia**. **El documento** de cadena de custodia **debe estar siempre donde esté la evidencia**:

- La evidencia debe estar **inequívocamente identificada** (quién, cuándo, dónde se ha recogido)
- Es necesaria información sobre **quién custodia la evidencia** (quién, cuándo, dónde, cuánto tiempo, cómo se guarda)
- Se debe registrar la información sobre **cada cambio de custodia** (fecha, hora, personal involucrado, tiempo que ha durado, número de envío, etc.)

Modelo de documento de cadena de custodia

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____Location of Seizure: _____

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

(NIST National Institute of Standards and Technology)

https://www.nist.gov/document/sample-chain-custody-formdocx

Explicación extendida sobre el documento de custodia:

- https://peritoinformatico.es/cadena-de-custodia-peritaje-informatico/
- https://peritoinformaticocolegiado.es/blog/cadena-de-custodia-en-el-peritaje-informatico/

Ejemplo real : "Los peritos confirman la manipulación del disco duro de Déborah Fernández" – https://www.diariodepontevedra.es/articulo/vigo/peritos-confirman-manipulacion-disco-duro-deborah-fernandez/20220526203826120264 5.html

4 Adquisición de datos

Para realizar la adquisición de los datos debemos seguir las siguientes indicaciones:

- Localizar la evidencia (determinar qué dispositivos deben adquirirse).
- Asegurar el escenario, para que nadie acceda.
- Descubrir datos relevantes.
- Tener en cuenta el **orden de volatilidad**.
- Recoger la evidencia.
- Recuperación de información borrada u oculta.
- Duplicar la evidencia (copia binaria bit a bit).
- Preparar la cadena de custodia.

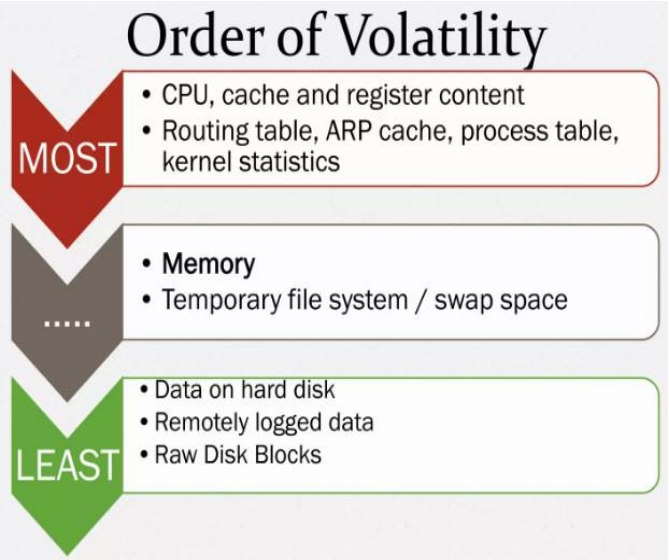
Existen directrices para recuperar evidencias (entre ellas **RFC 3227**)

https://www.incibe-cert.es/blog/rfc3227

4.1 Orden de volatilidad.

Se trata del orden en que haremos la adquisición de evidencias:

- Atendemos a qué evidencias desaparecen antes que las demás.
- Hay que respetar siempre este orden en la adquisición para evitar que desaparezcan las evidencias o las contaminamos involuntariamente.



Según las diferentes guías de recolección y archivo de evidencias electrónicas, podemos determinar que el orden de volatilidad es (De más volátil a menos volátil): **RFC3227** https://datatracker.ietf.org/doc/html/rfc3227 - https://www.incibe-cert.es/blog/rfc3227

La siguiente tabla clarifica algo más el orden de volatilidad:

Orden de volatilidad	Artefacto	Modificación
Extremadamente volátil	Registros y caché del procesador	Inferior a microsegundos
Ultra volátil	Memoria RAM	Microsegundos
Volátil	Tabla de procesos en ejecución, estadísticas del kernel, tráfico de red, archivos temporales del sistema de ficheros	Segundos
No volátil	Sistema de ficheros	Minutos
Persistente	Configuración física, topología de red	Acción humana necesaria
Persistente	Configuración física, topología de red	Años

Algunos **ejemplos de datos volátiles importantes** son:

- Zona horaria del equipo.
- Fecha y hora del equipo
- Análisis de red (conexiones establecidas, etc.)
- Volcado de memoria RAM
- Histórico del intérprete de comandos (history en Linux, por ejemplo)
- Pagefile.sys e hiberfile.sys (Windows).
- Árbol de directorios y ficheros en memoria.
- Historial de internet (en memoria)
- Carpetas compartidas (actualmente abiertas)
- Usuarios que han iniciado sesión y listado de cuentas
- Procesos activos
- Servicios en ejecución
- Dispositivos compartidos
- Actividad remota
- Volúmenes cifrados abiertos (por ejemplo Veracrypt).

En este momento, la pregunta del millón sería:

¿Se debe apagar una máquina para hacer la adquisición? Pues depende del caso. De entrada, NO.

- Antes se tendía a apagar la máquina inmediatamente y se perdía la oportunidad de obtener datos valiosos en vivo.
- Actualmente, se evalúa primero si la máquina debe apagarse antes de "estirar el cable".

4.2 Documento propuesto para la adquisición.

Durante la adquisición de cada evidencia debemos rellenar un documento donde anotar la información de cada elemento. Por ejemplo, podríamos usar el siguiente documento propuesto:

Formulario adquisición evidencia digital.xlsx

4.3 OFF-LINE vs LIVE en la adquisición de evidencias.

Como ya se ha comentado, tenemos básicamente **dos posibilidades para adquirir las evidencias**:

- **Modo "Live"** (en caliente, con la máquina encendida)
- **Modo "Offline"** (en frío, con la máquina apagada). Se conoce como "estirar del cable".

Para poder tomar alguna decisión sobre esto, siempre hay que tener presente:

- No siempre es posible recolectar datos volátiles. Depende de las circunstancias.
- Si se encuentra un **proceso destructivo en marcha**, se recomienda detenerla inmediatamente.
- Si se encuentra una **conexión remota que pone en marcha el proceso destructivo**, hay que documentar la conexión, cerrarla y adquirir la RAM para analizar el malware.
- Si el **atacante está conectado remotamente** accediendo a datos, hay que pensar si queremos mantenerla mientras capturamos la RAM o detenerla.

Modo "Online" o "Live" (en caliente)

Se hace cuando no se puede apagar el equipo, por ejemplo:

- El equipo utiliza encriptación de disco y no se tiene acceso a las claves necesarias para descifrar.
- Se debe mantener el servicio en funcionamiento por motivos de negocio.
- No se quiere apagar el equipo no modificar el comportamiento de un proceso malicioso, etc.

ATENCIÓN: Este tipo de adquisición puede provocar cambios debido al uso normal del equipo (último acceso a archivos, eventos producidos y entradas de logs nuevas).

Hay que documentar el momento en que se empieza la adquisición para poder descartar estos elementos provocados por el proceso de adquisición.

Modo "Offline" o "Dead" (en frío)

Se hace **con el equipo apagado**. Evita cambios debido al uso normal del equipo, como por ejemplo las marcas de tiempo (MAC) de los archivos (marcas de tiempo), alta de eventos y actualización de los logs.

- Implica apagar el equipo, extraer el disco y colocarlo en una estación forense.
- Utilizar algún elemento hardware/software para bloquear las escrituras (**sólo lectura**) antes de crear la imagen.

4.4 Tipos de copia.

Cuando hacemos copias de dispositivos de almacenamiento, se pueden aplicar dos estrategias:

Copia binaria o Bit a bit

Se copian todos los bloques del dispositivo a un fichero imagen, con formato RAW, E01, encase, etc. Esta copia ignora el sistema de archivos de origen ya que a posteriori se cargará la imagen para el análisis con alguna herramienta adecuada que comprenda el sistema de archivos. Ejemplos:

- copia con dd
- FTK Imager
- Guymager

La copia binaria:

- Siempre ocupa más espacio y tarda mucho más en hacerse.
- Permite recuperar datos en zonas del disco no asignados, ya que se copien todos los bloques del disco.
- No se modifican los metadatos del sistema de archivos.
- Es la opción preferida si se dispone del tiempo suficiente.

ATENCIÓN: También se puede hacer una copia binaria de dispositivo físico a un dispositivo físico idéntico con clonadoras de discos (método con hardware).

Formatos de ficheros de imagen

Algunos ejemplos de formato de del fichero de imagen destino son:

RAW (DD)

Es básicamente una copia bit a bit de los datos RAW del disco o del volumen almacenado en uno solo o múltiples ficheros:

- **No hay metadatos almacenados** en los ficheros de imagen.
- La mayoría de las herramientas crean un fichero de texto separado que contiene todos los detalles relativos al fichero de imagen, incluidos los detalles del hardware/software usado, los detalles de la fuente y el destino y los valores del hash.
- La principal ventaja del formato de imagen RAW es el hecho de que los ficheros solo contienen datos de origen no modificados, nada más. Esto significa que **casi todas las herramientas soportan imágenes en bruto**. Incluso herramientas no forenses.
- El principal **inconveniente** del formato de imagen RAW **es la falta de metadatos**. Sin el fichero de texto no hay manera de determinar la fuente de la imagen.
- Tampoco tiene **ninguna forma de compresión** de manera que **las imágenes son tan grandes como la unidad de origen**, aunque sólo se hayan utilizado unos pocos GB.
- Las imágenes RAW también se llaman a veces imágenes dd, ya que **el formato de imagen RAW tiene su origen en la herramienta dd**.

E01

Ficheros de evidencia de la herramienta forense EnCase. Es, junto con las imágenes RAW, el formato de imagen más utilizado. Su nombre es debido a su extensión, E01.

- Contiene una copia física binaria almacenada en uno solo o varios ficheros enriquecidos con metadatos.
- Estos **metadatos incluyen información de casos**, nombre del examinador, notas, sumas de verificación y un hash MD5.
- La principal **ventaja** de este formato de fichero es la **compresión, la protección por contraseña y la suma de verificación por fichero** (checksum).
- El principal inconveniente de este formato de fichero es el hecho de que es un **formato cerrado no documentado.**
- Aunque la mayoría de las herramientas forenses admiten este formato de fichero, no es compatible con otras herramientas no forenses.

SMART

El formato de imagen SMART es utilizado principalmente por la herramienta SMART para Linux.

- La imagen se almacena en un único o múltiples ficheros, cada uno con metadatos.
- Este formato de imagen ya no se utiliza prácticamente.

AFF

El **Advanced Forensics Format** es un formato abierto para el almacenamiento de imágenes forenses.

- Su objetivo es ofrecer un formato de imagen de disco que no esté ligado a software propietario.
- Este formato de imagen prácticamente está en desuso.

Copia lógica

Se copian los ficheros del disco en función del sistema de archivos del dispositivo. Es necesaria una herramienta de adquisición que pueda trabajar con el sistema de archivos del dispositivo.

- Se copian los archivos seleccionados o todos los posibles en función del tiempo del que disponemos. En caso de tener poco tiempo, hacemos el triaje de los ficheros más importantes.
- **No se copian las zonas no asignadas del disco**.
- No se podrá hacer cualquier proceso sobre el espacio no asignado a ficheros, como por ejemplo "carving"
- No se podrá buscar en el "slack space"
- Ni buscar en el espacio que puede quedar entre particiones
- Ni buscar a los sectores marcados como defectuosos, etc.

Ejemplos: se usan herramientas como cp, tar, cpio, dump, restore, o herramientas de triaje.

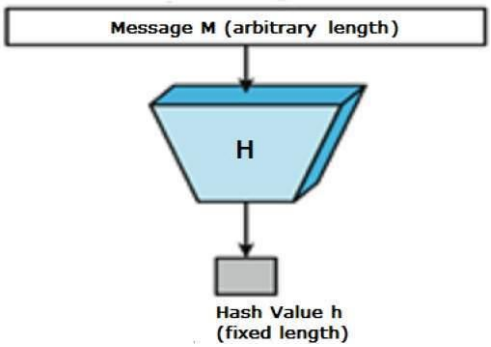
ATENCIÓN: estas herramientas no se pueden usar en forense sin usar parámetros que eviten la modificación de los MAC's de los archivos.
Por defecto, cuando se hace una **copia de un fichero en otro dispositivo, el propietario, fecha y hora, derechos, etc. se actualizan a las actuales en el dispositivo de salida**.

Únicamente aplicaremos esta técnica cuando:

- **No tenemos acceso al dispositivo físico** para extraerlo, por ejemplo, cuando trabajamos en la nube.
- **No podemos extraer el dispositivo debido a que está siendo utilizado**, por ejemplo si queremos copiar el directorio personal de un solo usuario a un disco de red.
- **En este caso el tiempo suele ser limitado**. Aplicaremos un proceso de selección.

4.5 Integridad de las evidencias.

¿Cómo podemos asegurar que las evidencias no se han alterado? **La solución es usar funciones criptográficas de resumen** (hashing).



Las funciones hash toman como entrada una secuencia **de datos de cualquier tamaño** y generan una salida de un tamaño concreto (por ejemplo 128 bits). Su objetivo es que para una entrada concreta, su resultado siempre sea el mismo (determinista).

En criptografía existen algoritmos de hashing para los que teóricamente sus resultados son siempre distintos, es decir, que no hay dos entradas de datos distintas que resulten en el mismo hash (**dicho suceso se denomina colisión**).

Para asegurar la integridad de las evidencias, es necesario **calcular siempre el valor de hash de la copia de trabajo** de las evidencias y compararlo con el valor de hash que se calculó en el momento de la adquisición.

- El hash es una **función de cifrado de un solo sentido** (no es reversible y por lo tanto no se puede recuperar la información original a partir del hash).
- Con un método cifrado concreto, por ejemplo, MD5, **siempre se genera un hash con el mismo número de bits**, independientemente del tamaño de los datos de entrada.
- Debe ser un **algoritmo libre de colisiones**.
    - Esto quiere decir que en la práctica es imposible generar un documento que tenga el mismo hash que otro documento dado.
    - Si es posible que dos o más documentos generen el mismo hash, pero no es posible saber a priori con cuales ocurrirá.

Funciones de hash más usadas:

- MD5
- Secure Hash Algorithm (SHA) del NIST
    - SHA-1
    - SHA-2
    - SHA-3

Ejemplo: Calculo de hash desde consola:

```
$ sha256sum pfSense-CE-2.6.0-RELEASE-amd64.iso
f6520bb14a5e690c6533e4e8fbf4a48d2967f3bc35a713e716b9c64317a13f23  pfSense-CE-2.6.0-RELEASE-amd64.iso
```

ATENCIÓN: MD5 y SHA1 se consideran hash inseguros (se puede generar un hash concreto a partir de un fichero preparado).
Al ser funciones hash mucho más rápidas, lo que se hace es calcular ambas y usarlas en conjunto.
Por ejemplo FTK Imager usa MD5 y SHA1 simultáneamente.

Utilidad del hash

Principalmente lo utilizamos el hash en tres situaciones:

- **Instruir las evidencias**: verificar que la evidencia está intacta y no ha sido cambiada (por errores, etc).
- **Hacer un análisis de hash:** comparar el hash de las evidencias con uno o más hash de ficheros típicos "buenos" o "malos". Por ejemplo:
  - Comparar con ficheros típicos de Windows en un sistema "limpio".
  - Compara con hashs de ficheros que contienen malware
- **Verificar positivamente que un archivo ha sido alterado** (por ejemplo por un malware).

4.6 Buenas prácticas de adquisición de evidencias.

La adquisición de la evidencia digital debe producirse de tal manera que ésta sea preservada. Hay que tener en cuenta:

- Documentar el **hardware/software (comandos) utilizados**. Abrir el ordenador con cuidado para **tener acceso físico a los discos**
- **Proteger las evidencias** de electricidad estática y campos magnéticos (bolsas antiestáticas y cajas de Faraday).
- **Documentar la adquisición y realizarla ante testigos** (si puede ser un notario o fedatario público, mejor).
- **Identificar los dispositivos de almacenamiento** (internos o externos) que es necesario adquirir.
  - Documentar los **dispositivos de almacenamiento internos y la configuración hardware** del equipo
  - Registrar el **estado del disco** (marca, modelo, geometría, interfaz, etc.)
  - Indicar los **componentes internos del equipo**, como tarjetas de sonido, gráficas, de red, etc.
- **Comprobar si el disco está encriptado** antes de apagar el equipo. Se recomienda en este caso adquirir en caliente, por si no tenemos la clave de descifrado.
- **Desconectar los dispositivos de almacenamiento** para prevenir la destrucción o alteración de los datos.
- Realizar la adquisición utilizando **el equipo del examinador**. Hay excepciones, como sistemas RAID, portátiles, hardware propietario, etc.
- Es aconsejable **el uso de dispositivos de protección de escritura** para evitar modificar el disco original.
- El **disco destino debe estar "limpio"** en términos forenses:
  - Disco nuevo recién estrenado
  - Disco utilizado pero formateado con sobreescritura indicando el procedimiento en el informe (método de wipe).
- Es recomendable crear un valor conocido de la evidencia original antes de adquirirla (**Cálculo de un hash del disco, p.ej. MD5 y SHA1**)
- Adquirir la evidencia **utilizando software o hardware testeado** y verificar la adquisición.

    - Realizarla **bit a bit** para que contenga los ficheros borrados (para hacer "carving") y los "file slack" (espacio del clúster no aprovechado).
    - **Comparación del hash** original respecto al de la copia
- **Cifrar las imágenes forenses** para garantizar la confidencialidad y establecer la cadena de custodia correcta para la imagen.
- Investigar **siempre sobre las copias**, nunca sobre el original.
    - La adquisición sólo se hará una vez, del dispositivo original. Éste se guardará y no se tocará más.
    - Hay que tener un máster del que obtener copias. El máster una vez obtenido, lo guardamos como copia base.
    - A partir de este máster hacer copias de trabajo, comprobando el hash.

4.7 Análisis de las evidencias.

A la hora de trabajar con una evidencia, siempre debe hacerse con una **copia de los datos originales** para no afectar a su integridad.

¿Cómo se analizan estas evidencias? A rasgos generales, se pueden diferenciar dos tipos de análisis:

- **Análisis físico:** se analiza el propio medio de almacenamiento y/o sus datos, sin atender a ningún formato.
- **Análisis lógico:** se analizan los datos según el formato de estos.

Ejemplo de análisis de una evidencia del tipo disco duro:

- **Análisis físico**: búsqueda de valores hexadecimales en los bloques del disco.
- **Análisis lógico:** búsqueda de directorios/archivos en el sistema de ficheros.

A un nivel más detallado, se pueden diferenciar los siguientes tipos de análisis:

- **Análisis temporal:** a nivel de archivo se determina la actividad y localización temporal de estos.
- **Análisis de información oculta:** búsqueda de información oculta tanto a nivel físico como lógico.
- **Análisis de aplicaciones y archivos:** búsqueda en los propios datos de los archivos.
- **Análisis de propiedad y posesión:** identificación de actividades relacionadas con una cuenta de usuario.

Durante la investigación, será necesaria la utilización de algunos (o todos) estos tipos, con el objetivo de responder a las **5W1H**.

La regla de las 5W1H pretende, al investigador forense, determinar determinar cuándo (**When**) y cómo (**How**) el ataque tuvo lugar. Además, es posible obtener evidencias que puedan demostrar quién (Who), qué (**What**), dónde (Where) y por qué (**Why**).

El objetivo es establecer una relación entre la escena del crimen, la víctima y el sospechoso. Para ello nos servimos de las evidencias.

4.8 Requisitos de las herramientas de adquisición de evidencias.

Necesitamos perfilar los requisitos de las herramientas, sobre todo si la adquisición va a ser en caliente. Es necesario tener preparado un dispositivo que se cargará en modo sólo lectura (lo más fácil sería un CD o DVD) con las herramientas necesarias:

- Hay que tener en cuenta el **sistema operativo** donde se hará la adquisición. Herramientas para **examinar procesos**. Por ejemplo 'ps' de linux.
- Programas **para examinar el estado**, por ejemplo 'showrev', 'ifconfig', 'netstat', 'arp'... de linux.
- Programa para **hacer copia bit a bit**, por ejemplo 'dd' de linux.
- Programas para generar **checksums i hash** como 'sha1sum', 'dd' con cálculo de hash, 'SafeBack', 'pgp'...
- Programas para generar **imágenes del core** y para examinarlas, por ejemplo 'gcore', 'gdb'...
- Scripts por **automatizar la recogida de evidencias**
    - por ejemplo The Sleuth Kit® (TSK), https://www.sleuthkit.org/
    - FastIR Artifacts
        - https://medium.com/@Sekoia_team/introducing-fastir-artifacts-66f1d43fcac5
        - https://github.com/OWNsecurity/fastir_artifacts

Como se puede observar, necesitamos herramientas muy variadas (seguro que algunas que no mencionadas se os ocurren), pero en general es muy importante **poder demostrar que las herramientas son confiables y lícitas**. Existe un proyecto para sistematizar las pruebas del software forense en el NIST (National Institute of Standards and Technology) de los EE. UU.

Más información: Computer Forensics Tool Testing Program (CFTT) (https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt).
Hay una lista de herramientas testadas por el NIST aquí: https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical

Herramientas adicionales

Orientadas a la preservación de evidencias

- **Bloqueo lógico de escritura** en los discos originales
- **Soporte de formatos** RAW, Encase EWF, AFF, etc.
- Trazabilidad (**cadena de custodia**)
- Cálculo de **hashs** criptográficos

Orientadas a la reducción de datos y captura rápida (triaje)

- Detección de **firmas de ficheros**
- **Filtros avanzados** y motor de búsqueda
- **Extracción de ficheros** claves y registros del sistema.

Orientadas a la reconstrucción de volúmenes y sistemas de ficheros

- Detección y **montaje** de particiones
- Soporte de formato VMDK (Virtual Machine Disk)
- Apoyo de FAT12/16/32 (USB)
- Soporte de NTFS con ADS https://es.wikipedia.org/wiki/Alternate_Data_Streams y compresión (Windows)
- Soporte de HFS, HFS+ y HFSX (OS X, iPhone)
- Soporte de Ext2/3/4 (GNU Linux, Android)

Orientadas al análisis multimedia

- Visualización de **galerías de fotografías**
- Extracción de **miniaturas de vídeos**
- Extracción de **metadato exIF** (Exchangeable image file format)

Orientadas al análisis de artefactos Windows

- Ficheros LNK (Acceso directo)
- Ficheros Prefetch (precarga de aplicaciones)
- Registro de Windows
- Buzones PST (Outlook)

Orientadas al análisis de memoria

- Volatility Framework
- Reconstrucción gráfica de procesos: pstree, psxview
- Información de procesos: procdump

Orientadas al análisis de documentos

- Visualizadores dedicados: PDF, Texto, Web, etc.
- Extracción de metadatos, texto e imágenes en documentos ofimáticos.

5 Herramientas populares para DFIR (Digital Forensics Incident Response).

A modo de ejemplo, aquí tenéis las herramientas DFIR que suele utilizar un profesional.

https://www.youtube.com/watch?v=-xGfzCT6TUQ

índice para poder consultar alguna herramienta concreta:

- 00:00 - Intro
- 01:42 - Windows Subsystem for Linux (WSL) 2 03:18 - Windows Terminal
- 04:39 - Sysinternals Suite
- 05:31 - Microsoft PowerToys
- 06:20 - DCode

- 07:04 - FTK Imager
- 07:31 - PST Walker
- 08:53 - Arsenal Image Mounter
- 09:35 - Hibernation Recon
- 10:05 - Kroll Artifact Parser and Extractor (KAPE)
- 10:42 - NirSoft Tools
- 11:49 - X-Ways Forensics
- 12:19 - Eric Zimmerman Tools
- 14:09 - Chainsaw
- 14:21 - INDXRipper
- 14:26 - RegRipper
- 15:09 - balenaEtcher
- 15:49 - Sysinternals Suite (RDCMan)
- 17:12 - Visual Studio Code

6 Herramientas de adquisición de evidencias.

A continuación, se detallan las herramientas más populares para realizar la adquisición de evidencias:

6.1 Distribuciones live de linux.

- **Paladin** - https://sumuri.com/software/paladin/ - PALADIN (64 bits) es una distribución de Linux "en vivo" modifica da, basada en Ubuntu, que simplifica diversas tareas forenses con solidez forense mediante PALADIN Toolbox. PALADIN fue diseñada para ser ligera y compatible con sistemas de 64 bits.

- **PALADIN LTS** es una solución completa para triaje, imágenes, análisis e informes que contiene más de cien aplicaciones forenses de código abierto, disponibles en nuestro directorio de herramientas forenses. https://sumuri.com/product/paladin-lts/

- **Tsurugi Acquire Live - 32 bits**: Tsurugi Acquire es una versión ligera y optimizada de Tsurugi Linux [LAB], diseñada para proporcionar las herramientas básicas necesarias para arrancar un PC y adquirir dispositivos de almacenamiento masivo.
    - Se instala un pequeño subconjunto de herramientas para reducir el tamaño de la ISO. Su objetivo principal es que resida fácilmente en la RAM, sea rápido al arrancar y sea compatible con tantas arquitecturas como sea posible.
    - Esta distribución de Linux se basa en Debian 10 con un kernel 5.11.6 parcheado de 32 bits para mayor compatibilidad y fácil ejecución en dispositivos antiguos.

- Incorpora un sistema de detección de resolución de pantalla para adaptar automáticamente el tamaño de los iconos y menús en pantallas Retina y 4K.
- Además, es posible colocar la imagen completa en la RAM, lo que permite al usuario extraer la memoria USB/DVDROM tras el arranque y usar el sistema a alta velocidad, ahorrando un puerto USB o el lector/grabador óptico.

- **Tsurugi Linux** es un proyecto DFIR de código abierto que es y será totalmente gratuito, independiente y sin la participación de ninguna marca comercial. https://tsurugi-linux.org/index.php

  - Tsurugi es una distribución de Linux altamente personalizada, diseñada para respaldar sus investigaciones DFIR, análisis de malware y actividades OSINT (Inteligencia de Código Abierto).
  - Esta distribución incluye las últimas versiones de las herramientas más conocidas necesarias para realizar una investigación forense o de respuesta a incidentes exhaustiva, además de varias características especiales como el bloqueo de escritura en dispositivos a nivel de kernel, una sección dedicada al análisis de Visión Artificial, un selector de perfiles OSINT y mucho más que puede descubrir en su documentación.
  - El sistema operativo de 64 bits se basa en la versión "Ubuntu 22.04.3 LTS" (Long Time Support) para tener siempre un sistema actualizado y estable con más herramientas compatibles.
  - El kernel personalizado se basa en la versión 6.9.3, que implementa numerosos controladores y funciones nuevos.
  - Puedes usar Tsurugi Linux [LAB] en modo en vivo, pero su objetivo principal es instalarse y convertirse en tu laboratorio forense predeterminado.

- **SIFT** https://www.sans.org/tools/sift-workstation/ La estación de trabajo SIFT es una colección de herramientas forenses y de respuesta a incidentes gratuitas y de código abierto, diseñadas para realizar análisis forenses digitales detallados en diversos entornos. Es compatible con cualquier conjunto actual de herramientas forenses y de respuesta a incidentes. SIFT demuestra que se pueden lograr capacidades avanzadas de respuesta a incidentes y técnicas forenses digitales exhaustivas utilizando herramientas de código abierto de vanguardia, disponibles gratuitamente y actualizadas con frecuencia.

SIFT

- **CAINE** https://www.caine-live.net/page5/page5.html CAINE (Computer Aided INvestigative Environment) es una distribución italiana de GNU/Linux en vivo creada como un proyecto de análisis forense digital. CAINE ofrece un entorno forense completo, organizado para integrar herramientas de software existentes como módulos y proporcionar una interfaz gráfica intuitiva.

- **OSFClone** (Passmark soft) es una solución gratuita y autoarranque que permite crear o clonar imágenes de disco sin procesar exactas (FAT, NTFS, Ext) de forma rápida e independiente del sistema operativo instalado. Además de las imágenes de disco sin procesar, OSFClone también admite la creación de imágenes de unidades en el formato abierto Advanced Forensics Format (AFF), un formato abierto y extensible para almacenar imágenes de disco y metadatos asociados, y en el formato Expert Witness Compression Format (EWF). Un estándar abierto permite a los investigadores utilizar de forma rápida y eficiente sus herramientas preferidas para el análisis de unidades. https://www.osforensics.com/tools/create-disk-images.html

- **BackBox** https://linux.backbox.org/ Linux es una distribución de Linux orientada a pruebas de penetración y evaluación de seguridad que ofrece un conjunto de herramientas de análisis de redes y sistemas. Incluye algunas de las herramientas de seguridad y análisis más conocidas y utilizadas, con el objetivo de alcanzar una amplia gama de objetivos, que abarcan desde el análisis de aplicaciones web hasta el análisis de redes, pruebas de estrés, rastreo, evaluación de vulnerabilidades, análisis forense informático, aplicaciones automotrices y explotación. Se ha construido sobre el sistema central Ubuntu pero está totalmente personalizado, diseñado para ser una de las mejores distribuciones en pruebas de penetración y seguridad y más.

6.2 Herramientas opensource basadas en dd

- **dd**: clásico comando de linux
- **dcfldd**: https://www.kali.org/tools/dcfldd/ Desarrollado por el U.S. Department of Defense computer forensics lab:
    - Proporciona la opción de generar hash de los datos transmitidos
    - Tiene una barra de progreso que muestra cuántos datos se han enviado Registro de errores a un fichero de salida para el análisis
- **dc3dd:** https://www.kali.org/tools/dc3dd/ dc3dd es una versión mejorada de GNU dd con características añadidas para forense digital.
    - Cálculo de hash mientras se hace la copia (on the fly): md5, sha-1, sha-256 y sha-512. posibilidad de escribir sectores con errores en el fichero de salida.
    - Envía los errores al log de errores (error log).
    - Esterilización (wipe) del dispositivo usando un patrón.
    - Informe de progreso.
    - Posibilidad de dividir la salida.

- **ddrescue**: https://www.kali.org/tools/ddrescue/
    - Como las anteriores y además no se detiene cuando estás copiando de un disco con errores. Tiene muchas opciones avanzadas.

6.3 Otras herramientas

Herramientas opensource

Guymager: https://guymager.sourceforge.io/ https://www.kali.org/tools/guymager/

Guymager es un generador de imágenes forenses gratuito para la adquisición de evidencias. Sus principales características son:

- Interfaz de usuario sencilla en diferentes idiomas. Funciona en Linux.
- Muy rápido gracias a su diseño multiproceso y segmentado, y a su compresión de datos multiproceso. Aprovecha al máximo los equipos multiprocesador.
- Genera imágenes planas (dd), EWF (E01) y AFF, y admite la clonación de discos. Gratuito y completamente de código abierto. Contenido en las distros CAINE, TSURUGI, BACKBOX, KALI, GRML, ForLEx, SANS SIFT (Vmware image), BitCurator (Live CD and VirtualBox image)

Herramientas propietarias en Windows

- **FTK Imager** (gratuita)
- **OS Forensics** (Passmark soft) - https://www.osforensics.com/download.html OSForensics™ ofrece una de las maneras más rápidas y eficaces de localizar archivos en un ordenador Windows. Puede buscar por nombre de archivo, tamaño, fecha de creación y modificación, entre otros criterios.
- **X-Ways Imager** https://www.x-ways.net/imager/index-m.html

Montaje de imágenes

- **OSFMount** (software de Passmark) permite montar archivos de imagen de disco locales (copias bit a bit de un disco completo o una partición) en Windows como un disco físico o una letra de unidad lógica. - https://www.osforensics.com/tools/mount-disk-images.html
- **Arsenal Image Mounter**: Muchas soluciones de montaje de imágenes de disco basadas en Windows® montan el contenido de las imágenes de disco como recursos compartidos o particiones, en lugar de discos completos (también conocidos como discos físicos o reales), lo que limita su utilidad para profesionales de la informática forense y otros profesionales. Arsenal Image Mounter monta el contenido de las imágenes de disco como discos completos en Windows, lo que

permite a los usuarios beneficiarse de funciones específicas de cada disco, como la integración con el Administrador de discos, el lanzamiento de máquinas virtuales (y la posterior omisión de la autenticación de Windows y DPAPI), la gestión de volúmenes protegidos por BitLocker, el montaje de instantáneas de volumen y más. https://arsenalrecon.com/products/arsenal-image-mounter

7 Documentación y presentación.

Una vez analizadas las evidencias (o incluso durante el análisis – **informe preliminar**) es necesaria la elaboración de un informe en el que se expongan las conclusiones del análisis.

Para ello, es necesario (además de gran utilidad) ir documentando cada paso realizado durante la investigación. De este modo, se facilita que otros analistas forenses puedan realizar los mismos pasos y llegar a las mismas conclusiones (contra peritaje).

A la hora de redactar el informe es vital conocer el **público objetivo** al que irá dirigido. No es lo mismo un informe dirigido a otros analistas forenses que estará plagado de tecnicismos que uno dirigido a un tribunal no técnico.

En cualquiera de los casos, **el informe** debe ser **concienzudo, sistemático e imparcial** respecto a los hechos concluidos durante la investigación.

Es posible también que un investigador forense sea citado para declarar ante un tribunal, exponiendo las conclusiones del informe.

La parte contraria tratará de exponer un contra análisis de las evidencias, intentando ofrecer otra visión de la realidad o buscando argumentos que invaliden las evidencias presentadas (por ejemplo cadena de custodia fallida, evidencias creadas/manipuladas, etc).

7.1 Después la investigación

Una vez se da por finalizada la investigación no hay que dar por hecho que no va a haber más relaciones con el caso. Dependiendo de la situación, **puede ser necesaria la preservación de las evidencias de la investigación durante un tiempo determinado**.

Respecto a lo personal, una buena práctica es realizar una **retrospección del trabajo realizado:** lecciones aprendidas, en qué puntos se puede mejorar y ser más eficiente, etcétera. De este modo se mejorará para los casos futuros.

En cuanto a lo material, han de reponerse los materiales consumibles utilizados y sanear los dispositivos de almacenamiento y otras herramientas empleadas.

8 Normativa.

- **ISO/IEC 27037:2012** Normativa para la identificación, recolección, adquisición y conservación, de evidencias digitales - https://peritosinformaticos.es/iso-iec-270372012-perito-informatico/
- **ISO/IEC 27042:2015**. Normativa para el análisis e interpretación de evidencias digitales - https://peritosinformaticos.es/iso-27042-perito-informatico/
- **UNE 71505/2013**. Sistema de Gestión de Evidencias Electrónicas - https://peritosinformaticos.es/une-71505/
    - **UNE 71505/2013-1**. Sistema de Gestión de Evidencias Electrónicas Parte 1: Vocabulario y principios generales. - https://peritosinformaticos.es/une-71505-perito-informatico-3/
    - **UNE 71505/2013-2**. Buenas prácticas en la gestión de las evidencias electrónicas - https://peritosinformaticos.es/une-71505-perito-informatico/
    - **UNE 71505/2013-3**. Formatos y mecanismos técnicos - https://peritosinformaticos.es/une- 71505-perito-informatico-2/
- **UNE 71506/2013**. Metodología para el análisis forense de las evidencias electrónicas. - https://peritosinformaticos.es/une-71506-perito-informatico/
- **UNE 197010/2015**. Normas Generales para la elaboración de informes y dictámenes periciales sobre TIC. - https://peritosinformaticos.es/une-197010-perito-informatico/

9 Referencias.

- Forensics 101: What is a forensic image? - https://www.raedts.biz/forensics/forensics-101-forensic-image/
- Sep 2024 When Speed Matters: Optimizing Disk Imaging - https://blog.elcomsoft.com/2024/09/when-speed-matters-optimizing-disk-imaging/