



# Curso de Ciberseguridad

## Análisis Forense en Windows

Análisis Forense Informático



¿Qué es el Análisis Forense Digital o Digital Forensics?	3
Análisis Forense de Respuesta a Incidentes .....	3
Análisis Forense Pericial .....	4
Principio de Intercambio de Locard .....	5
Metodología Actual de Análisis Forense .....	6
ISO27037: Fase de Identificación .....	7
ISO27037: Fase de Recopilación o Recolección .....	7
ISO27037: Fase de Adquisición .....	8
ISO27037: Fase de Preservación .....	10
ISO27037: Fase de Cadena de Custodia .....	10
Tipos de Evidencias	12
Discos duros .....	12
Discos de estados solido .....	17
Pendrives / Tarjetas de memoria .....	18
Tipos de Adquisiciones	21
Adquisiciones Lógicas .....	21
Adquisiciones Físicas .....	22
Adquisición de ficheros o carpetas .....	23
Tipos de Imagen Forense	24
Formato Bruto o RAW Images .....	24
Formato Encase 6 (E01) - Expert Witness Format .....	26
Encase 7 evidence file images (Ex01) .....	28
AFF: advanced forensic format .....	29
AccessData Custom Content Image (AD1) .....	29
Tipos de herramientas de Adquisición	30
Clonadoras o duplicadoras .....	30
Bloqueadores por hardware .....	31
Bloqueadores por software .....	32
¿Qué herramientas podremos utilizar con un PC doméstico para realizar la adquisición? .....	32
Verificación del hash de una imagen forense	45
Adquisición de discos SSD	47
Adquisición de artefactos forenses en sistemas encendidos	48
Adquisición de memoria RAM .....	49
Detección de Cifrado .....	53
Análisis y extracción de artefactos .....	54

## ¿QUÉ ES EL ANÁLISIS FORENSE DIGITAL O DIGITAL FORENSICS?

Disciplina que se ocupa de **IDENTIFICAR, ASEGURAR, ANALIZAR, EXTRAER** y **PRESENTAR** pruebas generadas electrónicamente y guardadas en medios electrónico, utilizando una serie de procedimientos técnicos y operativos, con el objetivo de que sean aceptadas en un proceso legal, si fuese necesario.



### ANÁLISIS FORENSE DE RESPUESTA A INCIDENTES

Para hacer forense de respuesta a incidentes se necesita contacto con la dirección de la organización para que pueda tomar decisiones y éstas, serán muchas de ellas de negocio.

- ◆ Incidente en Curso
- ◆ Interactuar
- ◆ Cambiante
- ◆ Resolver el incidente

¿Qué hacer durante un forense de respuesta a incidentes? Obviamente la propia identificación es la clave del éxito para la contención y erradicación del incidente.

---

CICLO DE VIDA DE RESPUESTA A INCIDENTES

La fase de **identificación** es una de las fases más críticas, ya que entra en juego las capacidades de Análisis Forense para identificar si realmente es un incidente o no. ¿Qué objetivos tenemos?

- ◆ Identificar el compromiso, es decir, como se ha producido el incidente.
- ◆ Identificar si se ha ejecutado algo, es decir, búsqueda de ejecución de aplicaciones o malware.
- ◆ Identificar si en el sistema, se ha conseguido persistencia, es decir, hay algún mecanismo o tarea que se ejecute en background y permita a los atacantes conseguir su propósito.
- ◆ Identificar los movimientos laterales, es decir, si han saltado de un ordenador a otro.

---

ANÁLISIS FORENSE PERICIAL

Tiene como objetivo responder ¿Cómo? ¿Cuándo? ¿Dónde? ¿Porqué?

- ◆ Incidente pasado



- ◆ Analizar restos
- ◆ Repetible
- ◆ Documentar

El informe será presentado como medio de prueba para un proceso judicial y el objeto vendrá determinado por las necesidades del departamento legal o cliente que necesita los servicios análisis forense.

Cuando un asesino deja salpicaduras de sangre en la pared, no lo hace para que el investigador de CSI pueda reconstruir con exactitud lo que ha sucedido, sino como efecto secundario de lo que hace.

- ◆ En Análisis Forense sucede lo mismo.
- ◆ Es necesario conocer esos “efectos secundarios”, cómo estudiarlos, y qué fiabilidad tienen.

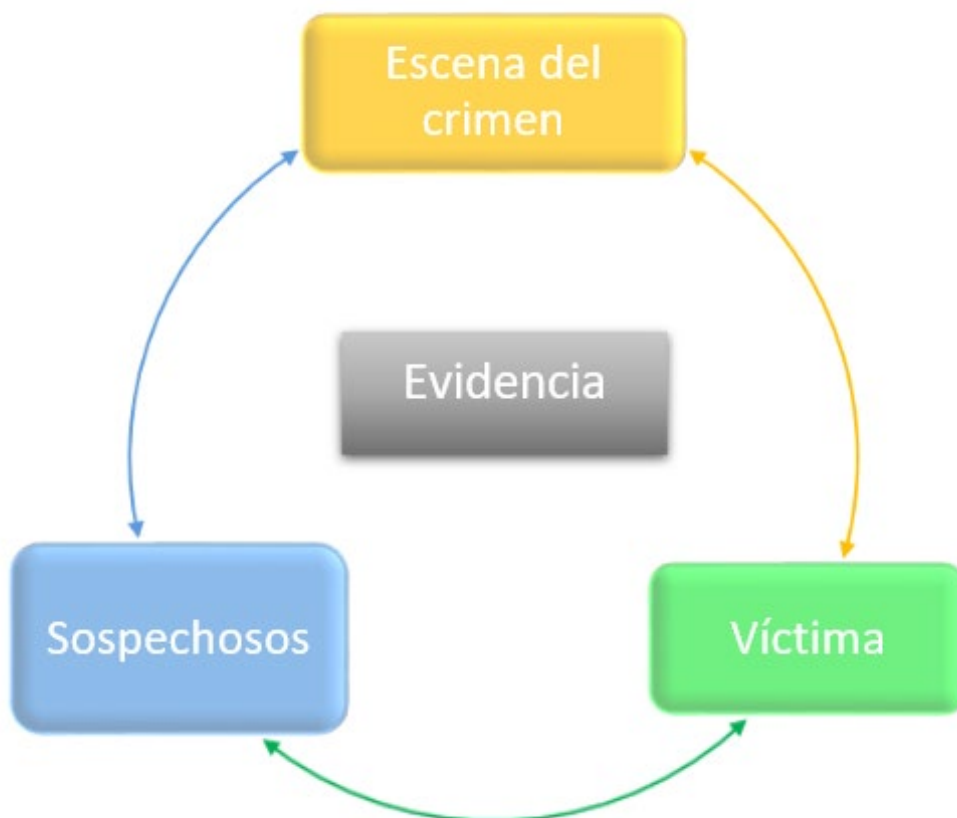
En esto es en lo que se basa el Análisis Forense.

---

#### PRINCIPIO DE INTERCAMBIO DE LOCARD

Siempre que dos objetos entran en contacto, transfieren parte del material que incorporan al otro objeto

QUANTIKA<sup>14</sup>





Este principio se puede aplicar de la misma manera al Análisis Forense, como por ejemplo cuando insertamos un dispositivo USB extraíble sobre un computador. En este caso el dispositivo USB dejaría una huella sobre el computador. Sería labor del investigador analizar el tipo de huella:

- Fecha de inserción
- Apertura de Ficheros
- Posibles Carpetas
- Marca y modelo del dispositivo USB extraíble
- Número de serie del dispositivo USB extraíble.

---

## METODOLOGÍA ACTUAL DE ANÁLISIS FORENSE

Dependerá mucho de la legislación vigente, que aplique a cada país, pero sino aplicase ningún tipo obligatoriedad, es recomendable, siempre que se pueda seguir una guía de buenas prácticas o estándar, en cuanto a la metodología:

- ◆ RFC 3227 Guidelines for Evidence Collection and Archiving (año 2002)
- ◆ ISO27037 Guidelines for identification, collection, acquisition, and preservation of digital evidence (año 2016)
- ◆ NIST 800-66 Guide to Integrating Forensics Techniques into Incident Response (2008)

Vamos a utilizar la ISO27037 como base de las técnicas y métodos que aplicaremos para la gestión de evidencias respecto a la identificación, recopilación, adquisición y preservación de evidencias digitales junto a la cadena de custodia.

La ISO27037 está principalmente focalizada a la realización de un Forense Pericial, donde es probable que el informe realizado sea presentado ante la corte o juzgados.

Muchas veces, un Análisis Forense de Respuesta a Incidentes, puede llegar a convertirse en un Análisis Forense Pericial, dado que el análisis forense realizado en la fase de identificación del ciclo de vida de un incidente ha identificado que se ha producido un perjuicio para la organización o compañía, y se quieren depurar responsabilidades. Es por esto por lo que el análisis deberá conocer esta metodología y aplicar sus fases, cuando correspondan.

La ISO27037 describe que la evidencia digital es frágil por naturaleza y qué podría ser alterada, manipulada o destruida a través de una gestión incorrecta. El analista forense que gestione las evidencias digitales debe ser competente para identificar, gestionar los riesgos y consecuencias de posibles procedimientos a seguir, cuando lidian con evidencias digitales. El analista forense necesita seguir procedimientos correctos para asegurar que se mantiene la integridad y la fiabilidad de la posible evidencia digital. Las reglas fundamentales, en la gestión de fuentes de posibles evidencias digitales son:

- ◆ Minimizar la gestión de la evidencia original o de la posible evidencia digital.
- ◆ Justificar cualquier cambio y documentar las acciones realizadas (para que un experto pueda formar una opinión sobre la fiabilidad).
- ◆ Cumplir con la regulación local en cuanto a gestión de evidencias.
- ◆ El analista forense no debe tomar decisiones más allá de su competencia.



---

## ISO27037: FASE DE IDENTIFICACIÓN

Las evidencias digitales se pueden presentar de manera física y lógica. La forma física incluye la representación de datos dentro de un dispositivo tangible. La forma lógica de una evidencia digital se refiere a la representación virtual de la información dentro de un dispositivo tangible.

El proceso de identificación involucra realizar un reconocimiento y documentación de posibles evidencias digitales. El proceso de identificación debería identificar el medio de almacenamiento digital y de los dispositivos de procesamiento, que pueden contener posibles evidencias digitales relevantes para el incidente. Esta fase también incluye, un proceso para priorizar la recopilación de evidencias basados en su volatilidad. La volatilidad de la información debe ser identificada para asegurar el correcto orden de recopilación y adquisición; minimizando el daño en las posibles evidencias digitales. El analista forense debería ser consciente de que no todos los tipos de almacenamiento pueden ser identificados y localizados. Por ejemplo: el almacenamiento en la nube.

El analista forense debería llevar a cabo sistemáticamente, una búsqueda exhaustiva de los elementos que puedan contener evidencias digitales, incluyendo diferentes tipos de dispositivos digitales que puedan tener posibles evidencias digitales y pueden ser fácilmente ignorados.

---

## ISO27037: FASE DE RECOPIACIÓN O RECOLECCIÓN

Una vez que los dispositivos digitales que podrían contener evidencias digitales son identificados, el personal forense debe decidir si recopilar o adquirir en los siguientes pasos. Hay un número de factores de decisión para esto y está basado en las circunstancias.

La recopilación es un paso en el proceso de gestión de evidencias digitales, donde los dispositivos que posiblemente contenga evidencias digitales son obtenidos. Estos dispositivos deben ser movidos de localización original a un laboratorio o a otro entorno controlado para más tarde realizar la adquisición y el análisis. Las posibles evidencias digitales pueden existir en al menos dos posibles estados: cuando el sistema está encendido o cuando el sistema está apagado. Cada estado necesita ser tratado de una manera diferente y distintas herramientas son utilizadas, dependiendo del estado.

**Equipo Encendido:**

- Obtención de datos volátiles
- Verificación de sistemas de cifrado (Veracrypt, BitLocker, Luks, Filevault)
- Documentar todos los pasos realizados para minimizar el impacto

**Equipo Apagado:**

- Si está encendido nunca apagar de forma ordenada -> tirar del cable
- Adquisición física

El proceso de recopilación incluye la documentación del proceso completo y también el empaquetado de los dispositivos antes del transporte. Es importante para analista forense que recopile cualquier material que podría estar relacionado con la posible evidencia digital, como, por ejemplo: contraseñas, cables de alimentación, etc. Las posibles evidencias digitales se pueden dañar sino se tiene en cuenta los cuidados necesarios para el transporte.

El analista forense debe adoptar el mejor método de recopilación posible, basado en la situación, coste y tiempo; y siempre documentando la decisión tomada en caso de usar un método en particular.

---

## ISO27037: FASE DE ADQUISICIÓN

El proceso de adquisición produce una imagen de la fuente original (por ejemplo, de un disco duro junto con su partición y los archivos contenidos dentro de la partición) siendo necesario documentar los pasos realizados para realizar dicha imagen. El analista forense deberá adoptar un método de adquisición apropiado basado en la situación, coste y tiempo, y nuevamente debe documentar la decisión de usar un método en particular o herramienta.

El método de adquisición usado debería producir una imagen copia de la fuente original o de la posible evidencia digital o del dispositivo digital. Tanto la fuente original como la imagen copia deberían ser verificada con una función de verificación demostrada, que sea aceptable por el individuo o persona que utilice dicha evidencia. La fuente original y cada imagen copia de la fuente original, deben de producir la misma función de verificación. (Si se utilizan funciones de verificación criptográficas, tales como SHA256, ambas deben producir el mismo hash).

Cada imagen copia, copia forense o imagen forense, debe ser verificada como copia de la fuente original. Habrá casos donde el proceso de verificación no se pueda realizar, por ejemplo, cuando el sistema está funcionando, cuando la fuente original tenga errores, cuando la fuente original sea un disco de estado sólido con el TRIM activado o cuando haya una limitación de tiempo. Si la imagen copia no puede ser verificada, este hecho debe ser documentado y justificado. Siempre que se pueda, se debe realizar una imagen copia, donde se obtendrá el espacio libre y el espacio utilizado.





Podría haber casos en el cual no sea factible o esté permitido hacer una imagen copia de la evidencia original, como cuando esta sea muy grande. En estos casos, el analista forense puede realizar una adquisición lógica, de la información específica o de directorios. Este tipo de adquisición, generalmente se realiza a nivel de sistema de archivos. Durante una adquisición lógica, solo los archivos visibles, es decir, los no borrados serán copiados. Los ficheros borrados y el espacio libre no serán copiados. Este método es muy útil a realizar sobre sistemas críticos que no pueden ser apagados. Las adquisiciones pueden presenciales o remotas. En función de cómo se encuentre fuente original o dispositivo se podrán realizar distintos tipos de adquisición.

La evidencia original debe mantenerse inalterable, siempre que se pueda y el estado de la técnica lo permita. Si fuese necesario ejecutar algo sobre el sistema, para que este permita realizar la adquisición, se deberá documentar todos los pasos realizados y plasmarlos en el informe. Este tipo de conducta de ejecutar algo sobre el sistema se produce en la adquisición denominada Triage.





---

## ISO27037: FASE DE PRESERVACIÓN

Las posibles evidencias digitales deben ser preservadas para asegurar su utilidad en la investigación. Es importante proteger la integridad de la evidencia. El proceso de preservación como dice el propio nombre debe preservar las posibles evidencias digitales y los dispositivos que las contengan, de posibles manipulaciones o modificaciones. El proceso de preservación debe ser iniciado y mantenido a lo largo de gestión de las evidencias empezando desde la fase de identificación. Se podrán utilizar funciones resumen criptográficas para verificar su no alterabilidad. También se debe tener en cuenta el espacio a utilizar, donde debiese tener las medidas de seguridad necesarias, así como un control de acceso al mismo.

---

## ISO27037: FASE DE CADENA DE CUSTODIA

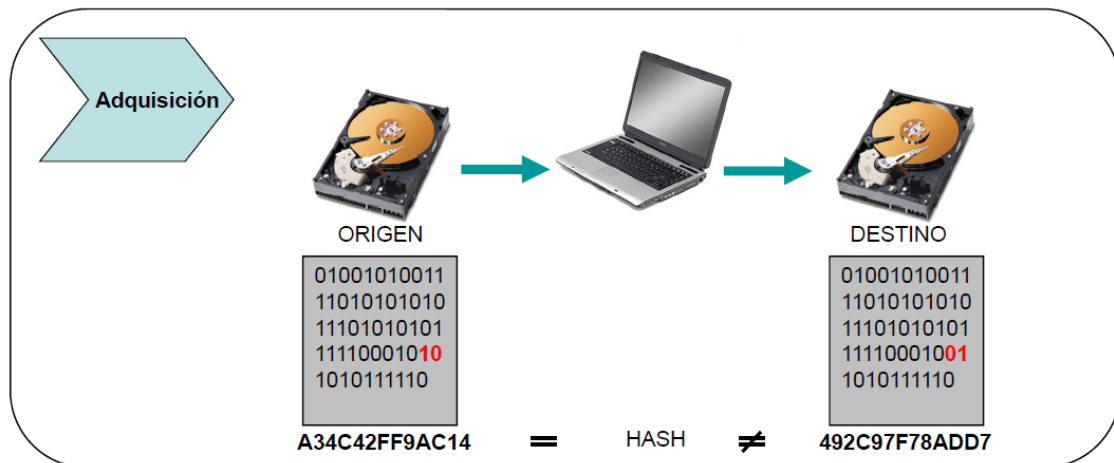
El registro de cadena de custodia es un documento que identifica la cronología de localización y gestión de la posible evidencia digital. Para cumplimentar este registro, típicamente, traza la historia del dispositivo en tiempo, por la persona que lo recibe, persona que lo entrega, y el motivo de la entrega. Esta fase empieza cuando se recibe el sistema para analizar.

El registro de cadena de custodia es un documento o documentos que detallan quien es el responsable de la gestión de dicha evidencia en un periodo de tiempo determinado. El propósito de mantener la cadena de custodia es saber en un tiempo concreto, donde estaba y quien lo gestionaba. El registro de cadena de custodia debería llevar la siguiente información como mínimo:

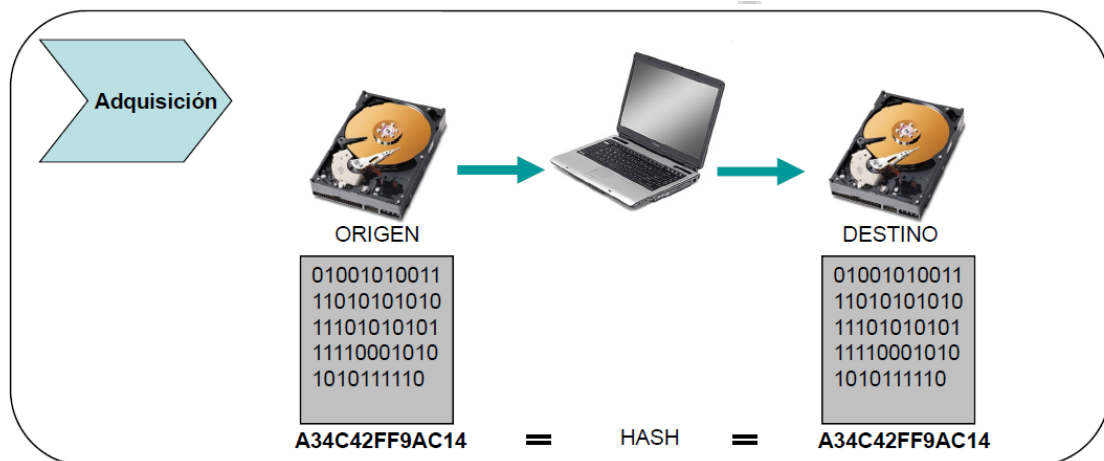
- ◆ Identificador único de la evidencia
- ◆ Quien accedió a la evidencia detallando tiempo y sitio donde se accedió.
- ◆ Quien chequeó si la evidencia estaba fuera o dentro de las instalaciones de preservación y que ocurrió.
- ◆ El motivo de que la evidencia saliese (caso y propósito) y la autoridad si fuese.

La cadena de custodia debe ser mantenida a lo largo de la vida de la evidencia y preservada durante cierto periodo de tiempo después de finalizar el caso. Este periodo puede ser establecido en concordancia de las leyes locales y debe ser establecido desde el momento de la adquisición. Un método para verificar si la cadena de custodia se mantiene es mediante los hashes de adquisición.

Podemos tener dos cadenas de custodia: una para la evidencia y otra para la copia/imagen forense.



En la imagen superior vemos que, si se calcula el hash de la evidencia origen y el hash del disco clonado y se verifica, vemos que no coincide.



En la imagen superior vemos que, si se calcula el hash de la evidencia origen y el hash del disco clonado y se verifica, vemos que si coincide.

El procedimiento natural para este tipo de custodia es realizar una adquisición de la evidencia original y que genere dos copias forenses. La evidencia original se custodia y no se trabaja con ella. La primera imagen forense es la utilizada para trabajar con ella y la segunda se almacena como backup por si fallase la primera.



## TIPOS DE EVIDENCIAS

Las evidencias se pueden encontrar en cualquier tipo de almacenamiento que sea susceptible de almacenar información. Al estar este curso focalizado en Windows, podremos encontrarlo en sistemas escritorio, servidores, portátiles y tabletas. Estos sistemas disponen de los siguientes dispositivos físicos donde almacenar la información.

- ◆ Discos duros
- ◆ Discos de estado sólido o SSD
- ◆ Dispositivos de almacenamiento extraíble: tarjetas flash, pendrives

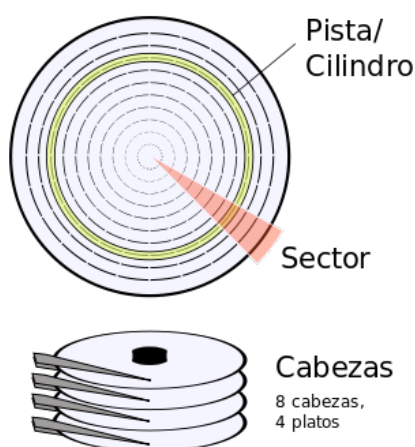
### DISCOS DUROS

Los hay de distintos factores de forma:

- ◆ 8 pulgadas: 241,3×117,5×362 mm
- ◆ 3,5 pulgadas: 101,6×25,4×146 mm
- ◆ 2,5 pulgadas: 69,85×9,5-15×100 mm
- ◆ 1,8 pulgadas: 54×8×71 mm
- ◆ 1 pulgadas: 42,8×5×36,4 mm
- ◆ 0,85 pulgadas: 24×5×32 mm



El disco duro está formado por los siguientes elementos:



- ◆ Plato: cada uno de los discos que hay dentro de la unidad de disco duro.
- ◆ Cara: cada uno de los dos lados de un plato.
- ◆ Cabezal: número de cabeza o cabezal por cada cara.
- ◆ Pista: una circunferencia dentro de una cara; la pista cero (0) está en el borde exterior.
- ◆ Cilindro: conjunto de varias pistas; son todas las circunferencias que están alineadas verticalmente (una de cada cara).
- ◆ Sector: cada una de las divisiones de una pista. El tamaño del sector no es fijo, siendo el estándar actual 512 bytes. Es la unidad mínima de información a nivel de disco.



El primer sistema de direccionamiento que se usó fue el Cilindro-Cabezal-Sector (Cylinder-Head-Sector, CHS), ya que con estos tres valores se puede situar un dato cualquiera del disco.

Actualmente se usa direccionamiento de bloques lógicos (Logical Block Addressing, LBA), que consiste en dividir el disco entero en sectores y asignar a cada uno un único número.

Los discos duros pueden tener de los siguientes conectores:

- ◆ USB
- ◆ SATA
- ◆ SAS
- ◆ SCSI
- ◆ IDE

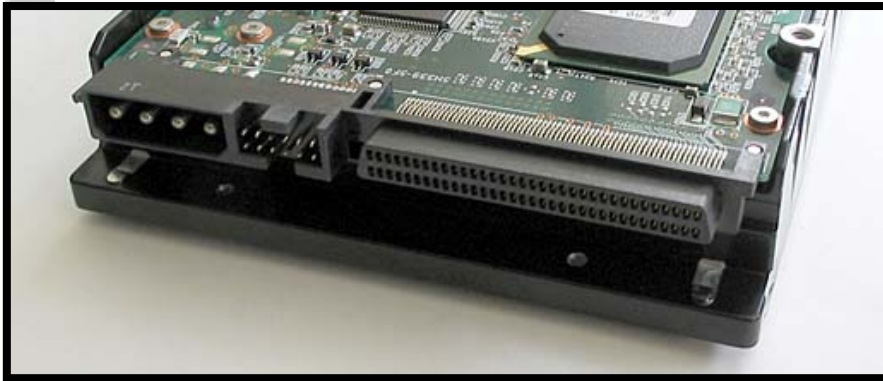
Conector SATA



USB Hard Disk



SCSI Hard Disk



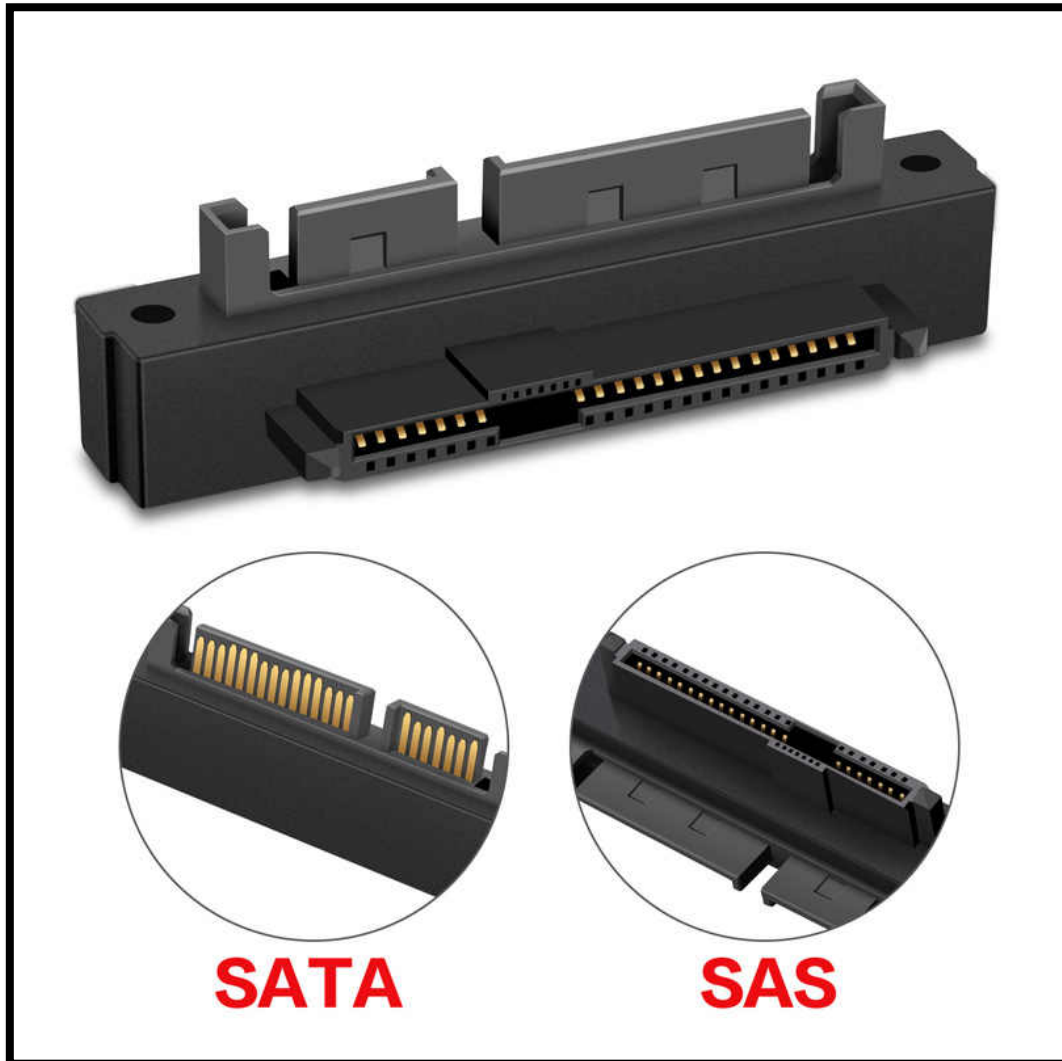
IDE Hard Disk



# QUANTIKA<sup>14</sup>



## Conector SAS







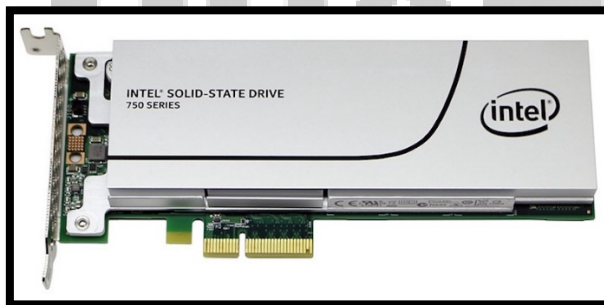
## DISCOS DE ESTADOS SOLIDO

- SATA SSD
- PCIe
- M.2 sobre PCIe (NVMe) o SATA M.2

### Dispositivos M.2



### PCIe



### SATA SSD



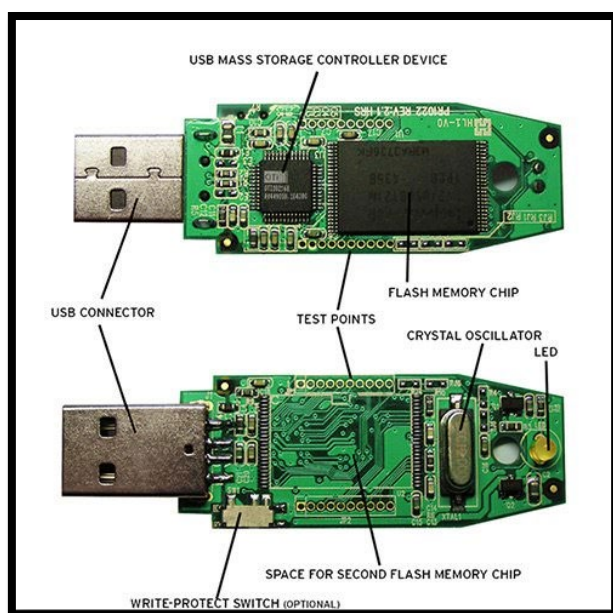
### Pendrives / Tarjetas de memoria

Los pendrives, tarjetas de memoria o cualquier dispositivo de almacenamiento extraíble que su almacenamiento sea en una memoria flash, pueden contener información relevante para la investigación forense. Como veremos más adelante, estos tipos de dispositivos necesitarán un sistema de archivos para guardar la información. Para las tarjetas de memoria, la mayoría de las veces será necesario utilizar un lector de tarjetas que nos permita leer su contenido.

### Pendrive USB



### Pendrive USB abierto



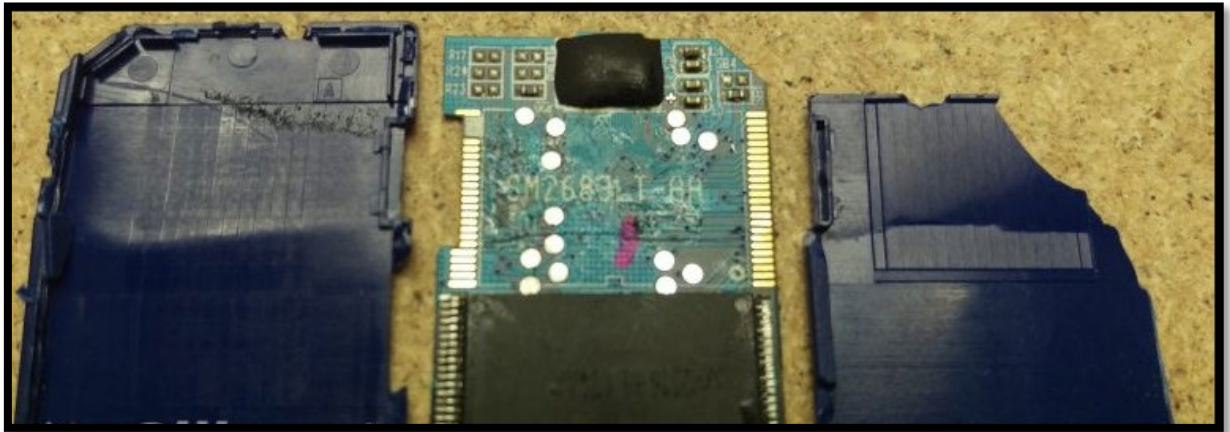
# QUANTIKA<sup>14</sup>



Distintos tipos de tarjetas de memoria



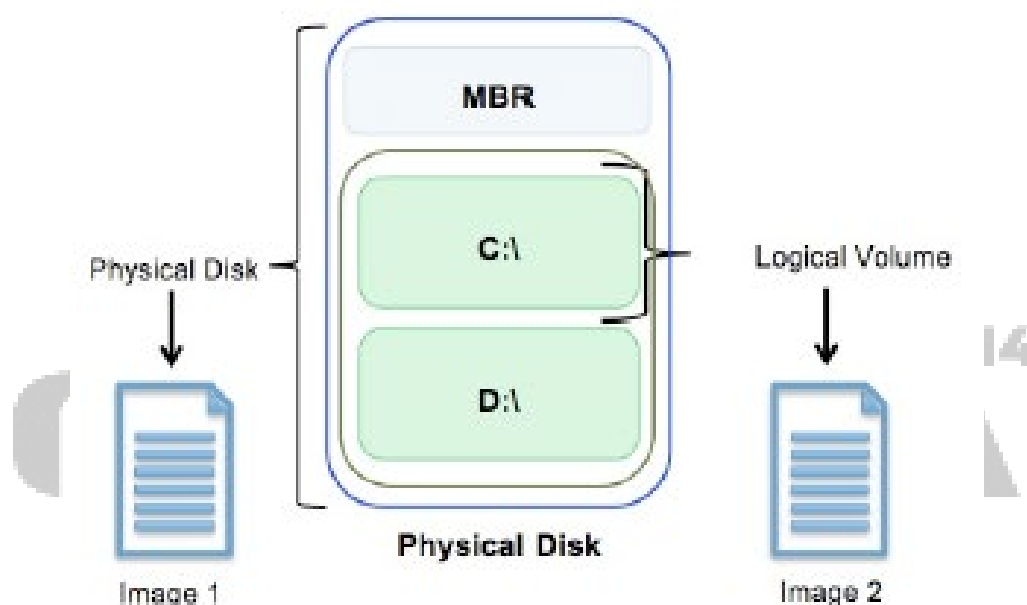
Tarjeta SD Card abierta



## TIPOS DE ADQUISICIONES

### ADQUISICIONES LÓGICAS

Este tipo de adquisición tiene como objetivo realizar una copia bit a bit de la partición o volumen lógico. Al realizar una copia bit a bit de todo el volumen, obtendrá la parte visible (carpetas y ficheros) y la parte no visible (espacio libre). En este caso según la imagen inferior, para hacer la adquisición lógica de las particiones, primeramente, se debe realizar sobre la partición C y seguidamente sobre la partición D. Es muy común realizarla con el sistema apagado o post mortem. Este tipo de adquisición está muy orientado a generar una imagen forense, como veremos en la parte de adquisiciones físicas.



El almacenamiento mostrado en la imagen superior contiene el Master Boot Record y dos particiones con sus sistemas de archivos.



---

## ADQUISICIONES FÍSICAS

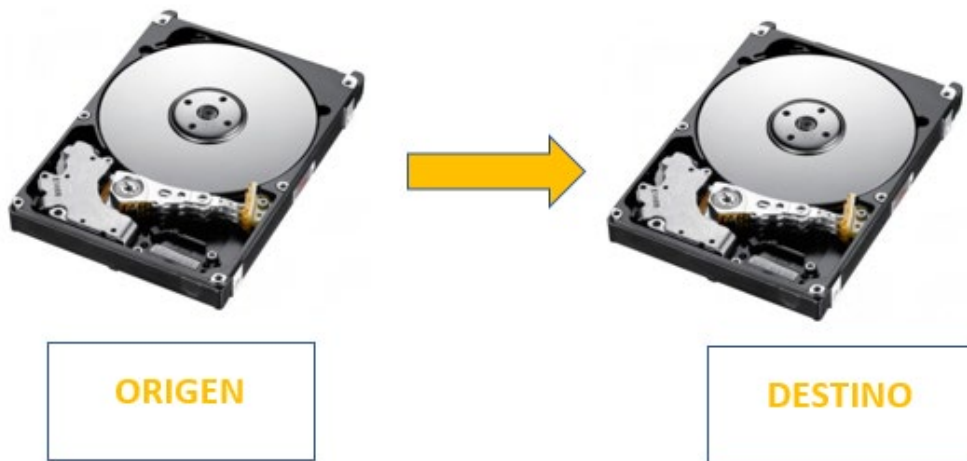
Cuando se realiza una adquisición física, se obtiene una imagen forense de todo el dispositivo, incluyendo las particiones (por ejemplo, las particiones C y D de un sistema Windows) junto con sus espacios libres y el sector de arranque que contenga. Es muy común realizarla con el sistema apagado o post mortem.

Dentro de las adquisiciones físicas podemos encontrar dos tipos:

---

### CLONADO DE DISCO

Para realizar este tipo de adquisición física, el disco destino debe ser del mismo tamaño que el origen, ya que se va a realizar una copia bit a bit de todos los sectores del mismo. Si no fuese del mismo tamaño, cuando se produzca la verificación mediante hashes criptográficos, la verificación fallará.



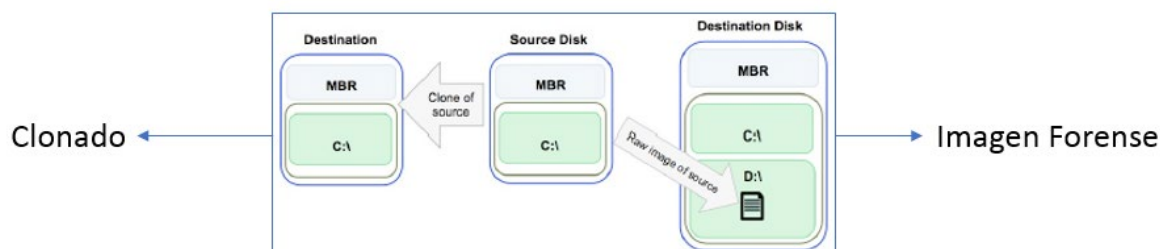
---

### IMAGEN FORENSE

Se clona el contenido del dispositivo a un fichero con formato. Los formatos forenses tienen una serie de limitaciones que podemos resumir:

- Formatos propietarios
- Formatos de archivo simple, son muy grandes al no estar comprimidos, además no suelen disponer de las opciones de cifrado ni firmado y no incorporan el almacenamiento de metadatos.

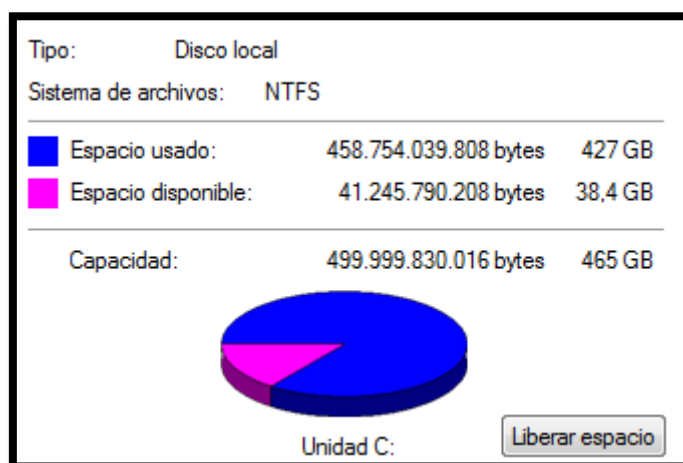
Un clonado es una duplicación de disco y una adquisición a imagen es un clonado de la información del disco que es escrita a un fichero, tal y como se puede ver en la imagen inferior.



## ADQUISICIÓN DE FICHEROS O CARPETAS

A veces se suele llamar también adquisición lógica de ficheros o triaje. No incluye el espacio libre pero sí ciertos metadatos del sistema de archivos. El espacio libre depende de la cantidad de información que estemos utilizando en el sistema de archivos.

### Espacio Libre



Es muy común realizarla con el sistema encendido o Live. Si la adquisición se produce sobre un sistema Live o encendido, estaríamos contaminando la evidencia, ya que se están ejecutando procesos para realizar dicha adquisición.

La contaminación, es decir, la ejecución del programa sobre la máquina se debe documentar concienzudamente, y siempre dicha herramienta debe haberse probado en un entorno de pruebas para verificar su comportamiento y la huella dejada en el sistema.



## TIPOS DE IMAGEN FORENSE

Casi todos los formatos de imagen forense suelen estar orientados a copias bit-a-bit del espacio de almacenamiento utilizado. En la actualidad existen los siguientes tipos de imagen forense, más importantes:

- ◆ RAW (Extensión .001 o .dd)
- ◆ EnCase 6 (Extensión. E01)
- ◆ EnCase 7 (Extensión. Ex01)
- ◆ AFF
- ◆ AccessData Custom Content Image (Extensión. AD1)

---

### FORMATO BRUTO O RAW IMAGES



Una imagen RAW solo contiene la información de la evidencia original, es decir solamente los datos. La imagen superior identifica el fichero imagen creado.

Este tipo de formato es una copia bit a bit de la evidencia original. Se suele acompañar de un fichero de texto donde están los metadatos de la imagen (hash de adquisición y verificación, fecha de adquisición).

```
my_image_set.001  
my_image_set.002  
my_image_set.003  
my_image_set.004  
my_image_set.txt
```

Raw standard naming convention  
uses the suffix **nnn**

En la imagen superior podemos ver la imagen forense creada. Este caso dicha imagen ha sido troceada en varios ficheros, siendo el primer fichero el que tiene la extensión 001. El fichero TXT contiene los metadatos del proceso de adquisición.



Ejemplo de fichero de Metadatos:

```
Created By AccessData® FTK® Imager 4.2.0.13

Case Information:
Acquired using: ADI4.2.0.13
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:

-----

Information for C:\Pruebas\imagen_pendrive:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 488
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 7,839,744
[Physical Drive Information]
Drive Model: JetFlash Transcend 4GB USB Device
Drive Serial Number: E1X7
Drive Interface Type: USB
Removable drive: True
Source data size: 3828 MB
Sector count: 7839744

Computed Hashes]
MD5 checksum: 08c3b88571687043cf7c4e57eb12fa87
SHA1 checksum: 4c6a9875a6e1dfb9cebb7055acle0fa775d2ee22

Image Information:
Acquisition started: Wed Oct 10 09:10:52 2018
Acquisition finished: Wed Oct 10 09:15:36 2018
Segment list:
C:\Pruebas\imagen_pendrive.001

Image Verification Results:
Verification started: Wed Oct 10 09:15:36 2018
Verification finished: Wed Oct 10 09:16:06 2018
MD5 checksum: 08c3b88571687043cf7c4e57eb12fa87 : verified
SHA1 checksum: 4c6a9875a6e1dfb9cebb7055acle0fa775d2ee22 : verified
```

La imagen anterior se corresponde con los metadatos generados por la herramienta FTK Imager donde podemos localizar cinco secciones:

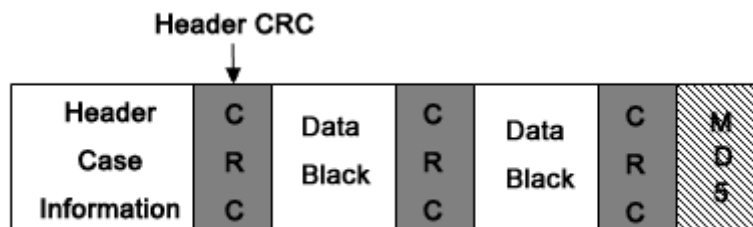
- ◆ Información del caso
- ◆ Información del dispositivo
- ◆ Hashes calculados del dispositivo
- ◆ TimeStamps o marcas de tiempo, de cuando se realizó la adquisición
- ◆ Verificación de los hashes

## FORMATO ENCASE 6 (E01) - EXPERT WITNESS FORMAT

El formato E01 o formato testigo, genera un fichero imagen donde contiene la información y los metadatos en el mismo fichero.



Si analizamos el fichero E01 en profundidad podemos identificar que está formado de la siguiente manera:



El fichero E01 contiene header y footer que contiene metadatos sobre la imagen. E01 dispone de cálculo de integridad del fichero mediante CRC.

Los metadatos incluyen, el tipo de dispositivo, versión del programa que ha generado la imagen forense, timestamps, y hashes criptográficos MD5 ó SHA1. Por defecto E01 utiliza compresión a nivel de bloque utilizando el algoritmo zlib.

Al igual que en el formato RAW, podemos trocear la imagen creada en distintos ficheros E01, E02, E03.

```

my_image_set.E01
my_image_set.E02
my_image_set.E03
my_image_set.E04
my_image_set.txt
  
```

EnCase standard naming convention uses the suffix **Enn**

También es muy común cuando se utiliza este tipo de formato, encontrar los metadatos en un fichero TXT, aparte de que ya van dentro del mismo fichero.

```
Created By AccessData® FTK® Imager 4.3.0.18

Case Information:
Acquired using: ADI4.3.0.18
Case Number: Evidencia Examen Final
Evidence Number:
Unique Description:
Examiner: Juan Manuel Martinez alcala
Notes: Curso Forense Basico en Windows

-----

Information for C:\Imagen_Examen_Final:

Physical Evidentiary Item (Source) Information:
[Device Info]
  Source Type: Physical
[Drive Geometry]
  Bytes per Sector: 512
  Sector Count: 52.428.800
[Image]
  Image Type: Raw (dd)
  Source data size: 25600 MB
  Sector count: 52428800

[Computed Hashes]
MD5 checksum: 87f1c087ec037cc4dc7db1842e31006c
SHA1 checksum: 3300924d4fad73e55146beeebab23696b2ed4968

Image Information:
Acquisition started: Wed Jul 22 23:33:18 2020
Acquisition finished: Wed Jul 22 23:36:57 2020
Segment list:
  C:\Imagen_Examen_Final.E01
```

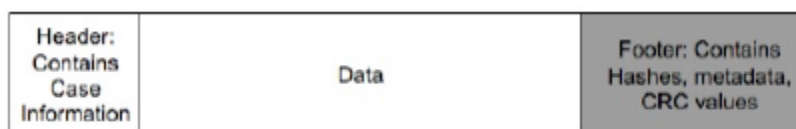
En la imagen superior vemos que falta la zona de verificación. Esto quiere decir, que solo se calcularon los hashes del dispositivo, pero no se verificó si el cálculo fue correcto o no. Al ver esta información, el analista forense debería realizar el cálculo.

Si abriésemos la imagen E01 con un editor hexadecimal, veríamos que los tres primeros bytes contienen las letras “EVF”. Como veremos más adelante, estos serán los magic numbers o signatures de un fichero.

Windows10_target.E01																
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	45	56	46	09	0D	0A	FF	00	01	01	00	00	00	68	65	61
00000010	64	65	72	00	00	00	00	00	00	00	00	00	00	BA	00	00
00000020	00	00	00	00	00	AD	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000050	00	00	00	00	00	D1	03	CF	F0	78	DA	33	E4	CA	4D	CC
00000060	CC	E3	4A	E6	CC	E3	4C	E4	4C	E5	2C	E1	4C	2C	E3	CC
00000070	2F	E3	CC	E5	2C	E5	2C	E0	2C	E2	F2	CC	48	4C	CE	F6
00000080	49	4C	2A	56	F0	09	71	E1	24	97	E7	E8	E2	69	AC	67
00000090	A2	67	AC	67	CC	19	9E	99	97	92	5F	5E	AC	60	CE	69
000000A0	64	60	68	A1	60	68	A0	60	01	84	C6	E6	0A	A6	C6	58
000000B0	44	0C	38	D3	B8	00	95	A2	2A	55	68	65	61	64	65	72
000000C0	00	00	00	00	00	00	00	00	00	00	67	01	00	00	00	00
000000D0	00	00	AD	00	00	00	00	00	00	00	00	00	00	00	00	00
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000100	00	00	7F	03	DE	DE	78	DA	33	E4	CA	4D	CC	CC	E3	4A
00000110	E6	CC	E3	4C	E4	4C	E5	2C	E1	4C	2C	E3	CC	2F	E3	CC
00000120	E5	2C	E5	2C	E0	2C	E2	F2	CC	48	4C	CE	F6	49	4C	2A
00000130	56	F0	09	71	E1	24	97	E7	E8	E2	69	AC	67	A2	67	AC
00000140	67	CC	19	9E	99	97	92	5F	5E	AC	60	CE	69	64	60	68
00000150	A1	60	68	A0	60	01	84	C6	E6	0A	A6	C6	58	44	0C	38
00000160	D3	B8	00	95	A2	2A	55	64	69	73	6B	00	00	00	00	00
00000170	00	00	00	00	00	00	00	CF	05	00	00	00	00	00	00	68
00000180	04	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	EC
000001B0	02	67	B8	01	00	00	00	00	00	1E	00	40	00	00	00	00
000001C0	02	00	00	00	00	80	07	00	00	00	00	00	00	00	00	00
000001D0	00	00	00	00	00	00	00	03	00	00	00	00	00	00	00	00

## ENCASE 7 EVIDENCE FILE IMAGES (EX01)

El formato Encase 7 es otro formato testigo, que a diferencia de la versión 6, utiliza un algoritmo distinto de compresión bzip en lugar de zlib y los CRCs son escritos al final del fichero en lugar de después de cada bloque de datos.



---

## AFF: ADVANCED FORENSIC FORMAT

Formato abierto, interpretado por herramientas como FTK Imager o Autopsy. Dispone de las siguientes características:

- ◆ Soporte de compresión, cifrado y firma digital
- ◆ Soporte de almacenado en varios ficheros
- ◆ Guarda metadatos extensibles

Métodos de almacenado en AFF:

- ◆ AFF: este método es por defecto y genera un fichero que contiene la evidencia y los metadatos.
- ◆ AFD: fichero con metadatos y la evidencia en varios ficheros adicionales.
- ◆ AFM: evidencia en un fichero y metadatos en otro fichero.

La nueva versión de este formato es la AFF4 y su referencia <http://www2.aff4.org/>

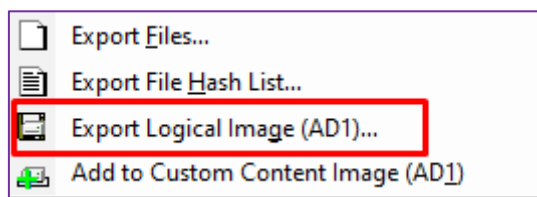
En la actualidad programas como X-Ways Forensics, o Magnet Axiom soportan este tipo de imagen forense, e incluso la versión gratuita de Evimetry, Evimetry Community:

<https://evimetry.com/evimetry-community/>

---

## ACCESSDATA CUSTOM CONTENT IMAGE (AD1)

Es un formato propietario de Access Data y tiene como fuente de evidencia siempre debe ser un el contenido de carpeta. Como tal solo contendrá los ficheros, no incluirá ningún metadato del sistema de archivos, ni ficheros borrados ni el espacio libre. Es útil para crear un contenedor de una carpeta.





## TIPOS DE HERRAMIENTAS DE ADQUISICIÓN

Durante la fase de adquisición debemos garantizar que la evidencia original se mantiene inalterable, es decir, que una vez vayamos a realizar la adquisición, este procedimiento debe intentar no modificar la información contenida en ella. ¿qué podemos utilizar?

### CLONADORAS O DUPLICADORAS

Las clonadoras o duplicadoras, son elementos hardware que realizan adquisiciones de evidencias. Disponen de bloqueadores de escritura internos. Este método suele ser más rápido que la utilización un bloqueador de escritura junto con un PC.



En la imagen anterior vemos a la izquierda conectada la evidencia original y la derecha los destinos de la adquisición. Puede ser que se realice un clonado o imagen forense. Disponen también de un puerto USB auxiliar donde se guarda el log de toda la operación realizada y de los metadatos de la adquisición. Si se utiliza la opción de imagen forense, también guardará los metadatos asociados en un fichero TXT en el disco destinatario.



## BLOQUEADORES POR HARDWARE

Dispositivo hardware que se conecta sobre el dispositivo para evitar cualquier escritura. En la imagen inferior, se ha desconectado el disco duro del sistema, por lo que se estaría realizando una adquisición post mortem.



El bloqueador hardware se pone entre el PC que realizará la adquisición y el disco duro. El proceso de realizar la copia bit a bit la realizará el software instalado en el pc. En la imagen de la figura se observa que el bloqueador está conectado por USB al PC, y luego mediante IDE al disco duro. Hay multitud de tipos de bloqueadores:

- ◆ USB
- ◆ SATA
- ◆ IDE
- ◆ SAS
- ◆ Firewire
- ◆ PCIe





---

## BLOQUEADORES POR SOFTWARE

Los bloqueadores por software lo que hacen es que, a nivel del sistema operativo impidan que se puedan escribir datos sobre la evidencia conectada.

¿Cómo podríamos realizarlo?

Si vamos a utilizar un PC con sistema Windows como base para realizar la adquisición, sería necesario modificar el registro de Windows para que active el bloqueo de escritura mediante USB, es decir, Windows solo permite realizar mediante la modificación de su registro el bloqueo de escritura de dispositivos que sean conectados mediante USB.

Esta operación siempre hay que realizarla antes de conectar la evidencia original. Los pasos los podemos encontrar aquí:

<https://www.fagforge.com/windows/windows-10/enable-write-protection-usb-devices-windows-10/>

Si vamos a utilizar un PC con sistema Linux como base para realizar la adquisición, o recomendable es utilizar una distribución que no monte los sistemas de archivos que haya dentro de la evidencia original.

Conectaríamos nuestra evidencia sabiendo que no va a ser montada y adicionalmente lanzaríamos el siguiente comando para cerciorarnos de que NUNCA escrito nada el dispositivo

```
blockdev --setro /dev/sdX
```

Donde X será el dispositivo que queremos evitar que se produzca una modificación. Más información sobre este método:

<https://github.com/msuhanov/Linux-write-blocker>

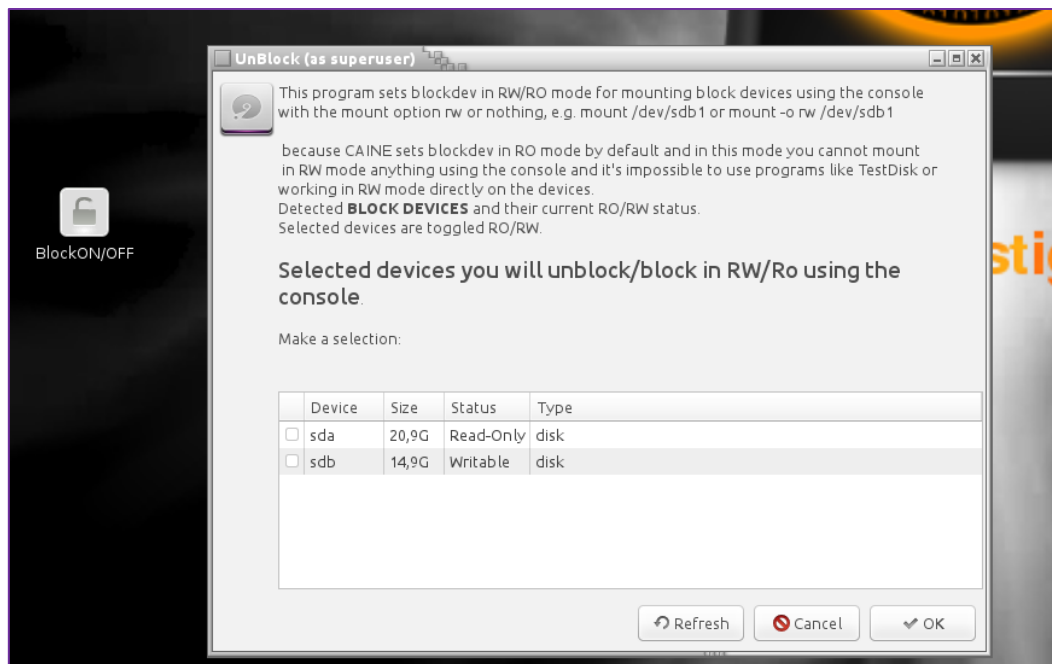
---

## ¿QUÉ HERRAMIENTAS PODREMOS UTILIZAR CON UN PC DOMÉSTICO PARA REALIZAR LA ADQUISICIÓN?

**Caine** es una distribución basada en Linux, que la podemos instalar sobre un PC e ir conectando sobre él mismo las evidencias extraídas previamente, que necesitemos realizar la adquisición. Dispone del módulo de protección de escritura y por defecto no monta ninguna unidad, que no sea la suya propia.

El modo de funcionamiento de este PC con Caine, sería como el de una duplicadora.

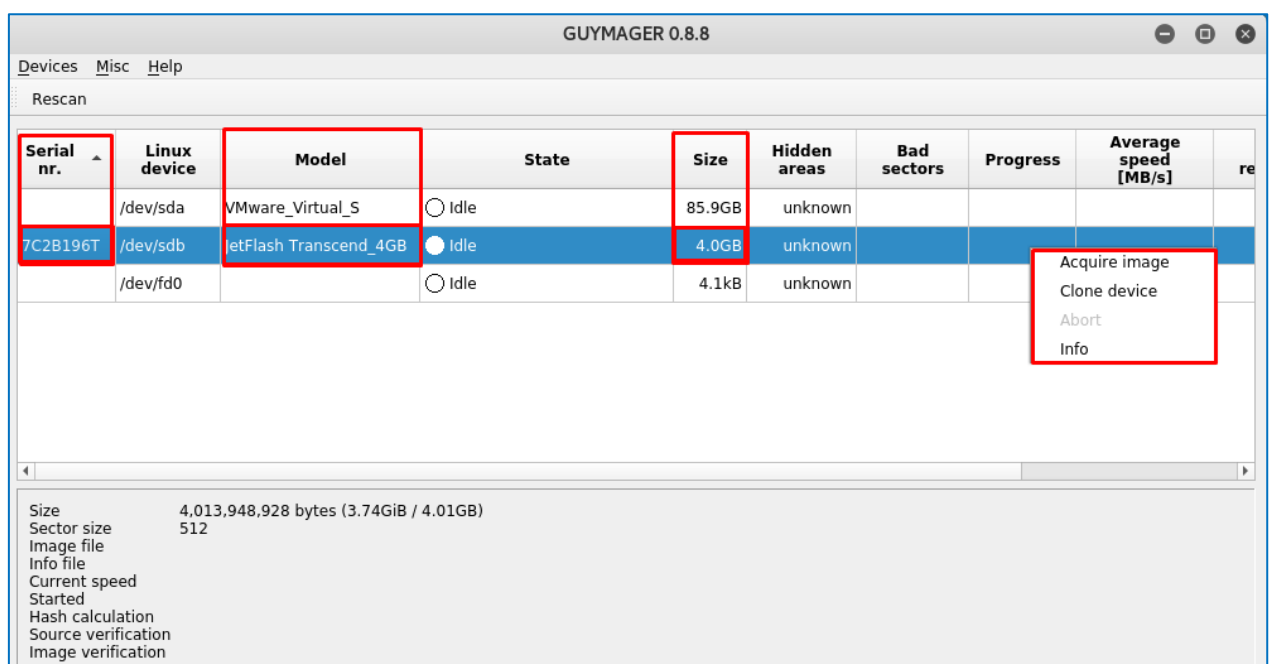




En la imagen anterior se puede observar cómo sobre el dispositivo sda no se puede escribir mientras sobre el dispositivo sdb sí. Para cambiar el dispositivo sdb, bastaría con seleccionarlo y darle a OK, para que cambie a su estado.

El funcionamiento de la herramienta solo permite cambiar de un estado a otro.

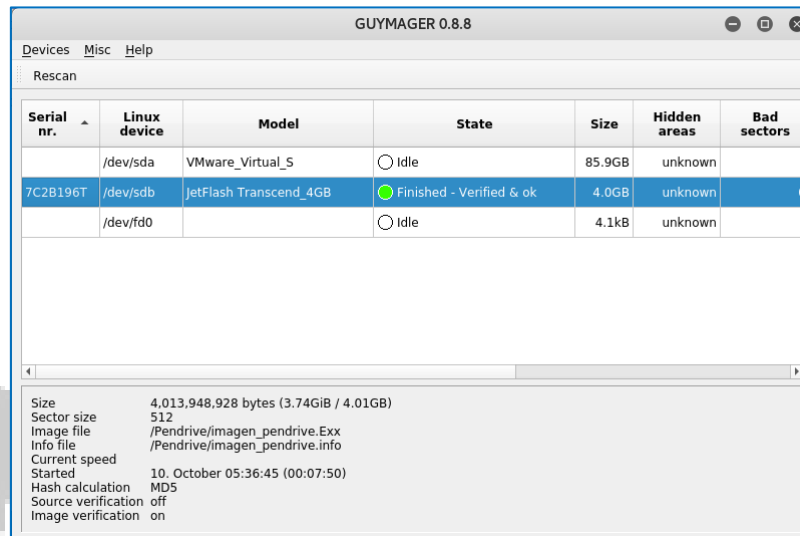
Dentro de Caine encontramos la herramienta GUYMAGER, que nos permitirá seleccionar el tipo de adquisición a realizar y sobre que dispositivos. Dispone de las opciones de hash de adquisición y verificación.



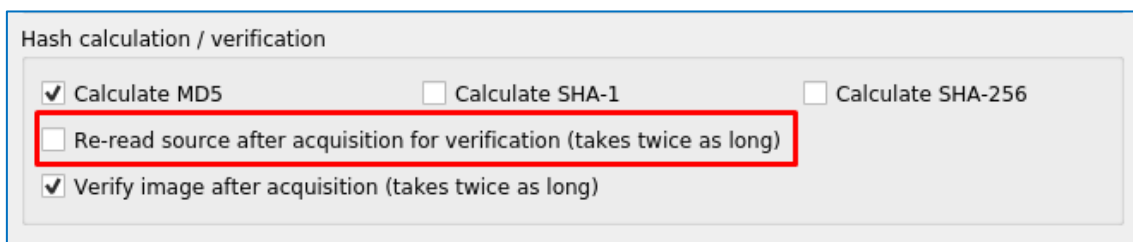
En la imagen anterior se ha conectado un pendrive sobre Caine y se ha arrancado GUYMAGER. Hay que saber identificar cual es la evidencia que vayamos adquirir, ya que la herramienta nos muestra todos los posibles dispositivos conectados, inclusive los del propio PC. En este caso, como queremos adquirir un pendrive, lo identificaríamos mediante el modelo, tamaño y número de serie. Pulsando botón derecho sobre el dispositivo, nos daría las dos opciones para realizar la adquisición.

*\*Ver video: 001/ MÓD. 1 - Adquisición Pendrive*

Una vez terminado el proceso se mostrará en el apartado de estado "Finished" en verde.






Durante la fase de adquisición se mostraron las siguientes opciones:



- ◆ Hashes MD5, SHA1, SHA256: hashes criptográficos que garantizarán la cadena de custodia de evidencia y de las imágenes forenses.
- ◆ Verify image after acquisition: verifica el fichero de creado
- ◆ La opción marcada en rojo es verificar por segunda vez el hash de la evidencia. Es decir, vuelve a releer la evidencia para volver a calcular el hash y así poder compararlo con el hash de la imagen forense. Si es marcado, este segundo proceso de verificación no se realiza.

Si vamos a la carpeta donde guardamos la imagen, obtendremos los siguientes ficheros:

Name	Size	Modified
 imagen_pendrive.E01	2.1 GB	05:40
 imagen_pendrive.E02	1.9 GB	05:44
 imagen_pendrive.info	7.2 kB	05:44

El fichero con extensión .info serían los metadatos que ha generado GUYMAGER:

```
Linux device      : /dev/sdb
Device size      : 4013948928 (4.0GB)
Format           : Expert Witness Format, sub-format Guymager - file extension is .Exx
Image meta data
  Case number     : 001
  Evidence number : Pendrive-A001
  Examiner        : Analista Forense
  Description      : Prueba de adquisición Pendrive
  Notes           : 7C2B196T
Image path and file name: /Pendrive/imagen_pendrive.Exx
Info path and file name: /Pendrive/imagen_pendrive.info
Hash calculation  : MD5
Source verification : off
Image verification : on

No bad sectors encountered during acquisition.
State: Finished successfully

MD5 hash           : 08c3b88571687043cf7c4e57eb12fa87
MD5 hash verified source : --
MD5 hash verified image : 08c3b88571687043cf7c4e57eb12fa87
SHA1 hash          : --
SHA1 hash verified source : --
SHA1 hash verified image : --
SHA256 hash        : --
SHA256 hash verified source: --
SHA256 hash verified image : --
Image verification OK. The image contains exactly the data that was written.
```

**Caine también lo podemos utilizar sobre un sistema, el cual no podamos extraer su disco de almacenamiento interno, y utilizar el propio hardware para ejecutar CAINE en memoria RAM. Ejecutando en memoria RAM, no modificaríamos el contenido del disco.**

Caine viene en formato ISO, por lo que es misión del analista forense grabarla en un pendrive o DVD. Para pasarlo a pendrive mirar el siguiente enlace: <https://rufus.akeo.ie/>

A continuación, se deberá configurar la BIOS o UEFI para que pueda arrancar desde este DVD o Pendrive. Es muy importante que este proceso se realice correctamente, de lo contrario arrancará el sistema operativo natural del sistema.

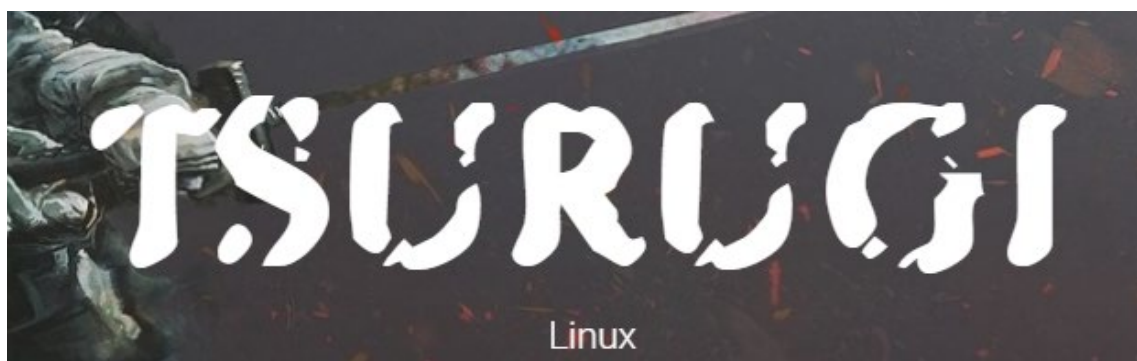
*\*Ver Video: 002/ MÓD. 1 - Adquisición CAINE Equipo*



Una vez terminado el proceso de adquisición debemos, desmontar las unidades externas, que fueron utilizadas para guardar la imagen forense.

```
caine@caine: ~  
File Edit View Search Terminal Help  
caine@caine:~$ sudo umount --force /puntomontaje/
```

Otra distribución muy parecida a Caine, es TSURUGI: <https://tsurugi-linux.org/>



Dispone de dos distribuciones Linux y un pack de herramientas forenses para muy interesante:

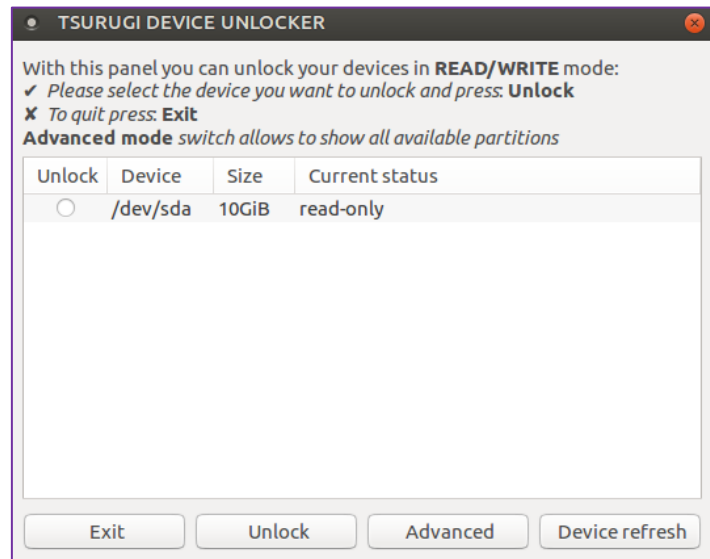
- ◆ Tsurugi Linux – Lab: suite Linux con todas las herramientas forenses
- ◆ Tsurugi Acquire: Live de 32bits para ser boteada desde Pendrive
- ◆ Bento Tools: suite de herramientas para análisis de sistemas Windows, Linux y MacOS

**Tsurugi Acquire** nos permitirá disponer de un entorno compatible para realización de la adquisición, sobre el mismo equipo o sobre dispositivos externos conectados.



QUANTIKA<sup>14</sup>

Tsurugi Acquire también dispone de un bloqueador por software como Caine, llamado Tsurugi device unlocker:



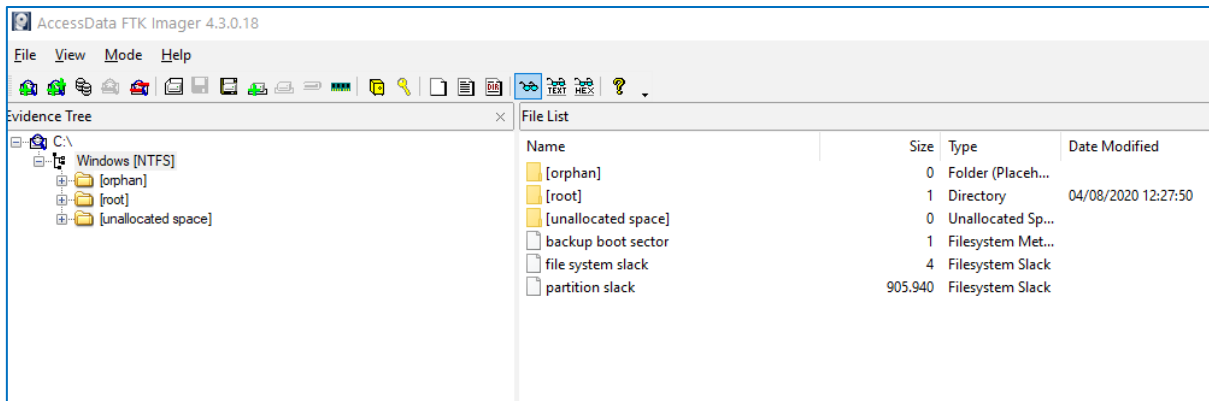
El bloqueador que vemos en la imagen superior nos permitirá desbloquear/unlock un dispositivo de almacenamiento para guardar información, en concreto para la imagen forense. Y finalmente Tsurugi Acquire dispone de Guymager como software principal para realizar adquisiciones.

**FTK Imager** es otra herramienta que funciona sobre sistemas operativos Windows. No dispone de bloqueador integrado de escritura como Caine. Por lo que es labor del analista forense utilizar algún método para bloquear la escritura, ya sea por software o por hardware.

Si vamos a bloquear la escritura, esto indica que solamente podremos utilizar elementos externos que estén conectados al PC sobre el que se va a ejecutar FTK Imager.

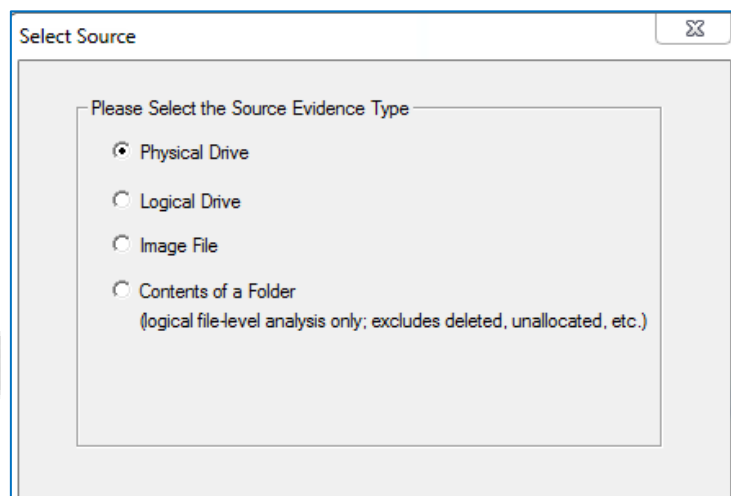
Sino bloqueásemos la escritura, estaríamos en la situación de que vamos a ejecutar FTK Imager sobre un sistema encendido o sistema Live para realizar:

- ◆ Adquisición lógica de ficheros: extraer solo ciertas carpetas o ficheros
- ◆ Adquisición lógica: muy útil para casos donde el dispositivo de almacenamiento donde está el sistema operativo disponga de algún tipo de cifrado.
- ◆ Adquisición física: si el dispositivo no se pudiese apagar por ser un sistema crítico, y no dispone de cifrado en su almacenamiento, es muy recomendable utilizar esta opción.



FTK Imager dispone de multitud de opciones, pero solamente vamos a trabajar con las siguientes:

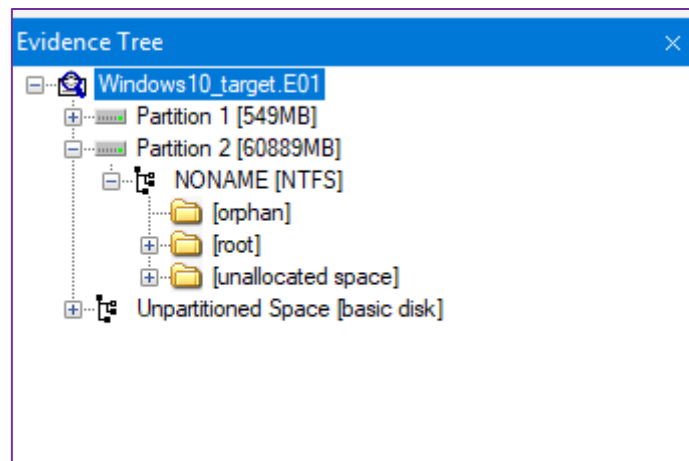
a) File -> Add Evidence Item (Añadir una Evidencia)



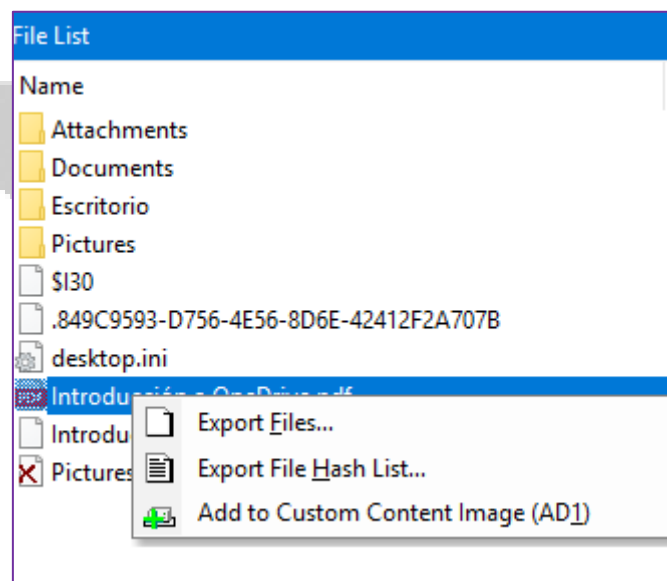
El objetivo de añadir una evidencia es para tener el contenido de esta y extraer ficheros/ carpetas para ser analizados. Este tipo de análisis se le llama, análisis post-mortem.

- ◆ Physical Drive: dispositivo físico conectado al PC. Puede estar conectado por cualquier protocolo ya sea SATA, IDE, USB.
- ◆ Logical Drive: volúmenes lógicos conectados al pc, es decir, que particiones es capaz de ver FTK imager de los dispositivos físicos.
- ◆ Image File: añadir una imagen forense para examinarla. Este será uno de los métodos que utilizaremos frecuentemente.
- ◆ Contenido de un directorio: añadir una carpeta en concreto.

Una vez añadida podemos ir navegando sobre la estructura de carpetas, sin ninguna restricción de permisos:

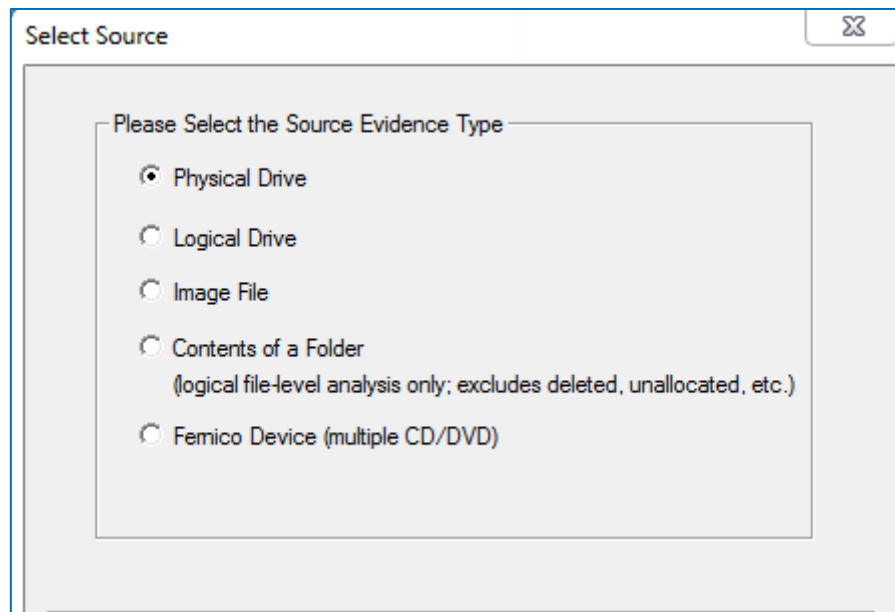


Para extraer un fichero de la imagen forense, bastaría con seleccionar el fichero o carpeta y darle al botón derecho: "Export Files"



a) Create Disk Image - Crear una imagen forense

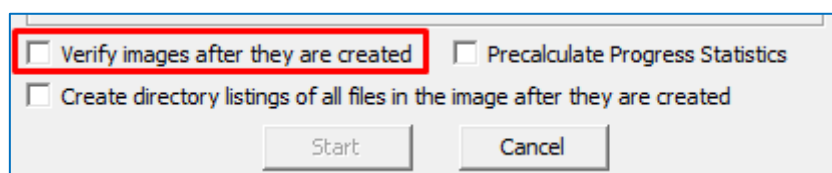




Nos va a permitir crear una imagen forense a partir de las siguientes fuentes de información:

- ◆ Physical Drive: dispositivo físico conectado al PC. Puede estar conectado por cualquier protocolo ya sea SATA, IDE, USB. Realizaría una adquisición física.
- ◆ Logical Drive: volúmenes lógicos conectados al pc, es decir, que particiones es capaz de ver FTK imager de los dispositivos físicos. Realizaría una adquisición lógica.
- ◆ Image File: utilizar como fuente una imagen forense para convertirla a otro formato.
- ◆ Contenido de un directorio: realizaría una adquisición lógica de ficheros y carpetas.

La opción de verificación de hashes de FTK Imager es la siguiente:

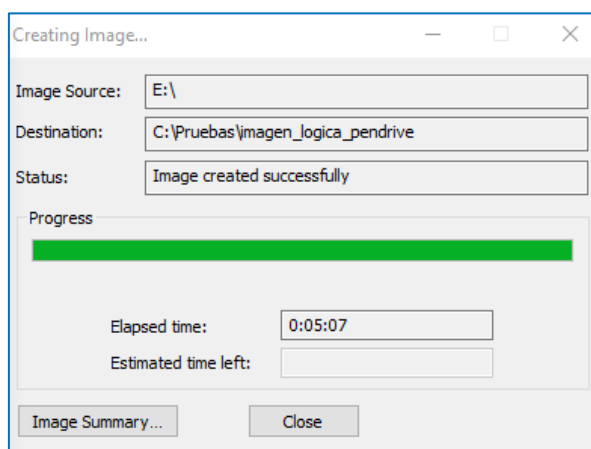


La opción marcada en rojo verifica el hash de la imagen forense contra el dispositivo o evidencia. Es decir, una vez que termine el proceso de adquisición, calcula el hash del fichero, y lo verifica con la lectura que ha ido haciendo progresivamente sobre la evidencia, realizando la verificación. Es práctica habitual marcar esta opción, para tener un match completo.

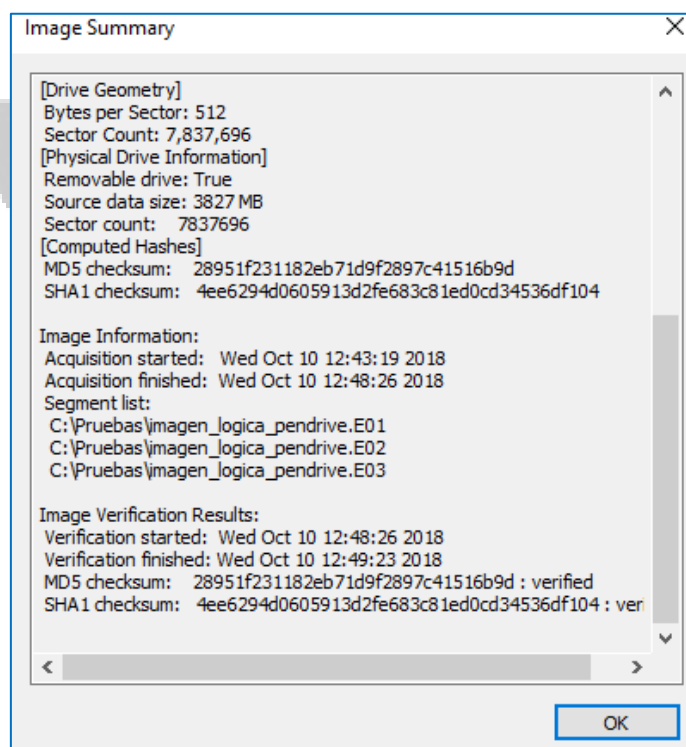
*\*Ver Video: 003/ MÓD. 1 - Adquisición Física Pendrive*

*\*Ver Video: 004/ MÓD. 1 - Adquisición Lógica Pendrive*

Una vez terminada la creación de la imagen forense nos aparecerá la siguiente pantalla:



Si pinchamos en “Image Summary” podremos ver información del proceso de creación de imagen forense.



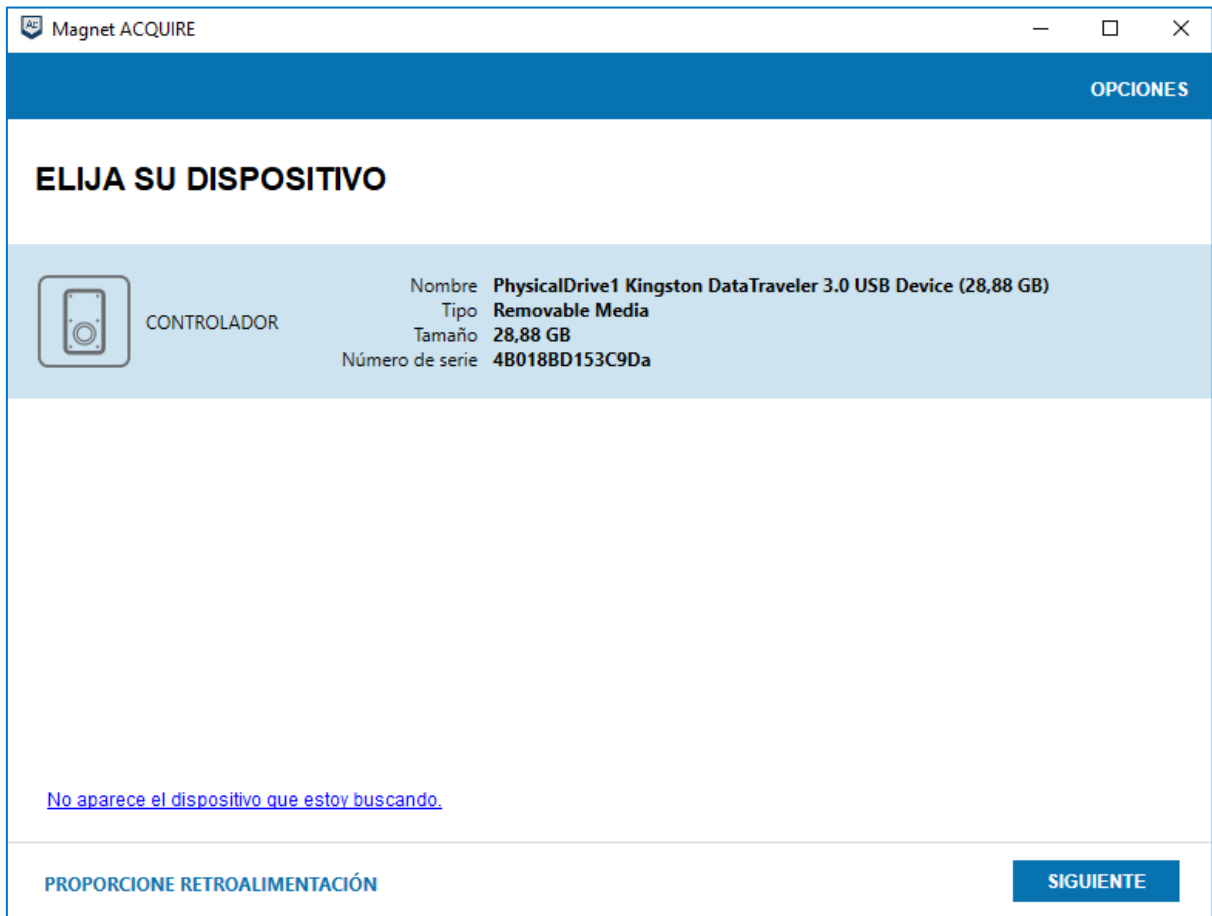
Esta información es la misma que se guarda como metadatos en los ficheros TXT. En los videos anteriores se ha utilizado un equipo Windows como medio de adquisición, por lo que se debe usar un bloqueador de escritura hardware o si se va a adquirir por USB, modificar el registro como se comentado anteriormente. Esto evitará que se puede escribir cualquier fichero/carpeta.



## Magnet Acquire

[Magnet Acquire](#) es una herramienta gratuita de Magnet Forensics que nos permitirá realizar adquisiciones de tanto de dispositivos de almacenamiento como de Smartphones.

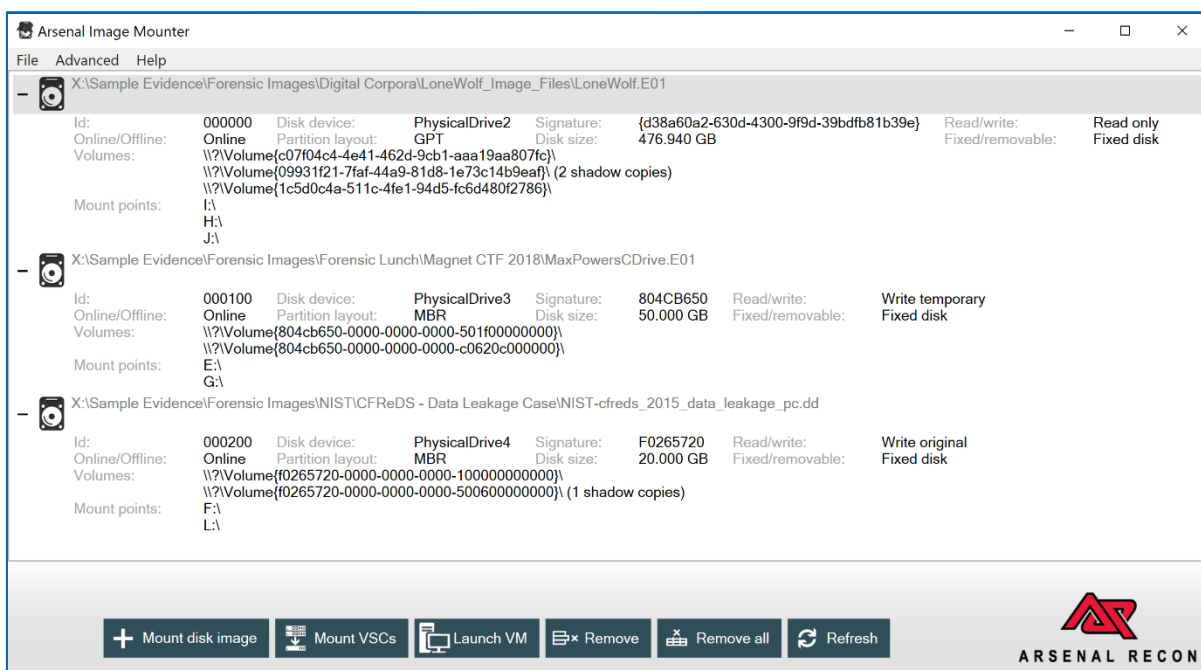
- ◆ Computadores y Smartphones: podremos adquirir smartphones, tabletas y también ordenadores portátiles, ordenadores de sobremesa y dispositivos extraíbles. Siempre se deberá utilizar un bloqueo de escritura.
- ◆ iOS y Android: podremos realizar una extracción rápida de dispositivos iOS y Android para obtener una imagen física de los dispositivos Android que estén rooteados o el sistema de archivos completo de un dispositivo iOS que este con jailbreak.



*\*Ver video 005/MÓD. 1 – Utilización Magnet Acquire*

## Arsenal Image Mounter

[Arsenal Image Mounter](#) es una herramienta de pago que tiene la funcionalidad gratuita para montar imágenes forenses, es decir, la imagen forense quedaría conectada como si el mismo disco de almacenamiento que contenía la información de la imagen forense, estuviese conectado al sistema operativo. Como veremos más adelante, podremos utilizar esta herramienta para poder acceder a las Shadows Copies.



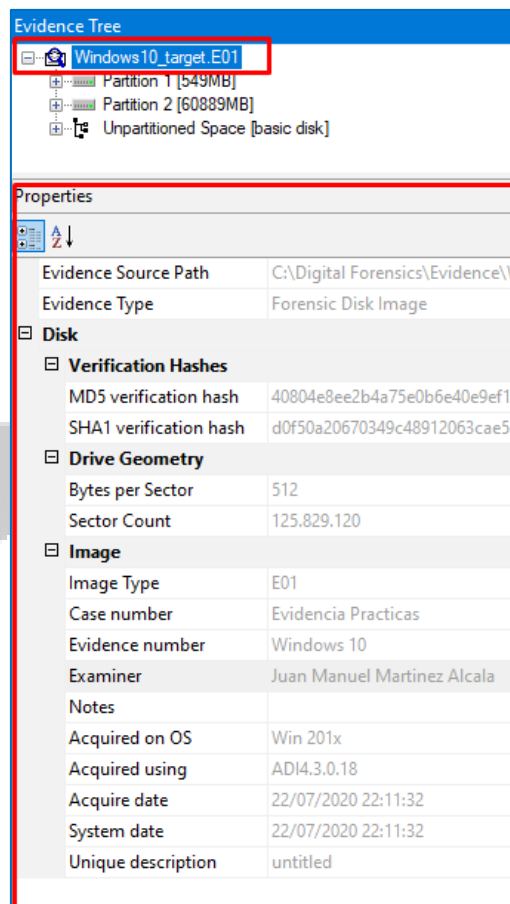
Esta herramienta también nos permitiría montar una imagen forense que estuviese cifrada con Bitlocker , para posteriormente montarla utilizando el propio sistema operativo.

*\*Ver vídeo: 006/ MÓD. 1 – Utilización Arsenal Image Mounter*

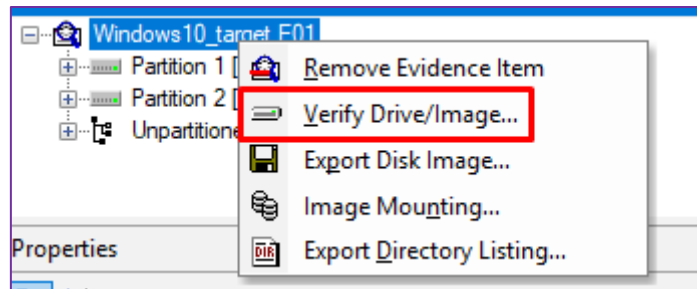
## VERIFICACIÓN DEL HASH DE UNA IMAGEN FORENSE

Muchas veces, podemos recibir directamente la imagen forense para nosotros realizar la investigación sin haber sido las personas que han realizado la adquisición. Es labor primordial verificar que la imagen que nos entregan coincide su HASH con el que nos entregan o encontramos el fichero de metadatos o en la cabecera las imágenes en formato testigo.

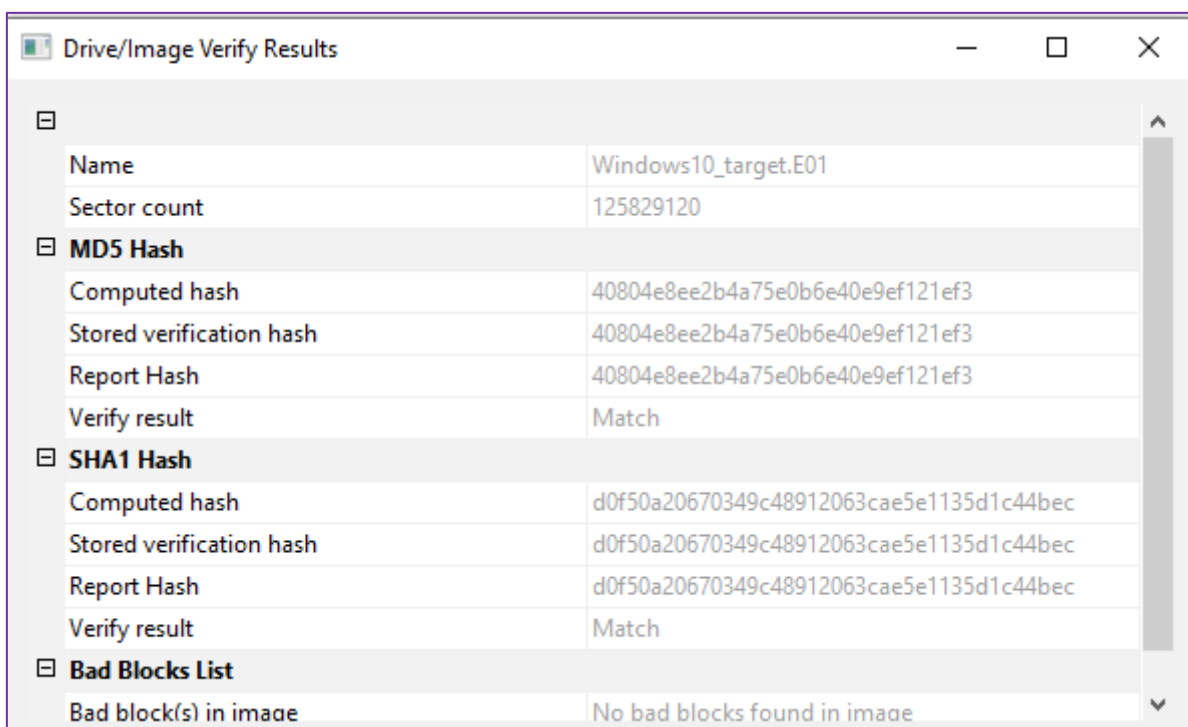
Para ello vamos a utilizar Access Data FTK Imager, añadiendo la imagen al programa y quedando la evidencia de la siguiente manera:



En la ventana de “properties” veremos los metadatos de la imagen forense E01 y para verificarlo, solo bastaría con pulsar sobre la imagen Windows10\_target. E01 con el botón derecho y darle “Verify Drive/Image”

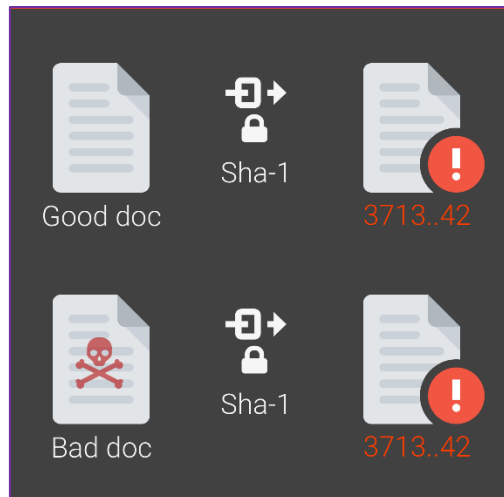


Este proceso calculará el hash de la imagen forense E01 y lo comparará con sus metadatos. También funciona con imágenes en RAW, siempre y cuando el fichero txt se encuentre en mismo directorio de la imagen RAW.



Finalmente aparecerá una ventana como la imagen anterior donde se puede identificar el calculo de los hashes junto con sus verificaciones.

Hoy en día, se sabe tanto que los hashes criptográficos MD5 y SHA1 han sido rotos, es decir, que se consiguió que dos flujos de datos totalmente distintos diesen el mismo hash.



Es decir, se pudo calcular como en la imagen anterior, un documento con un contenido (Good doc) y otro documento con otro contenido (Bad doc) sus hashes SHA1 y ambos dieron el mismo código hash SHA1.

Debido a que muchos programas forenses e incluso el propio formato E01 utiliza este tipo de hashes criptográficos, es recomendable, siempre que se pueda utilizar otro tipo de formato u programa que funcione con SHA256. Sino se pudiese utilizar, se debe justificar de manera exhaustiva el porqué de la utilización de MD5 y SHA1.

## ADQUISICIÓN DE DISCOS SSD

Todos los procesos que hemos visto de adquisición son 100% aplicables para cualquier dispositivo de almacenamiento y siempre que se pueda poner un bloqueador por software o por hardware. Los discos de estado sólido o SSD tienen las siguientes características que les hace especiales a la hora de hacer una adquisición:

- ◆ **Wear Leveling:** se utiliza para incrementar la vida del dispositivo de manera que la información es movida a otras celdas para que todas reciban el mismo número de escrituras. No exista slack space debido a esta característica.
- ◆ **TRIM:** los sistemas operativos Windows 7/8/10 y Windows 2012/2016/2019 disponen de capacidad de ejecutar este “comando” sobre los discos SSD, con el objetivo de mejorar la velocidad y el tiempo de vida del dispositivo. Su funcionamiento se basa en que cuando un fichero es borrado, la operación TRIM sobre el disco es solicitada por el sistema operativo, y el disco lo elimina definitivamente. Es un recolector de basura, de manera que limpia el espacio libre. Lo suele realizar una vez a semana para equipos Win7-Win10. El comando TRIM también es solicitado cuando desde Windows se realizan operaciones de particionado y a nivel del sistema de archivos como dar formato. No existe desfragmentación en este tipo de discos y en la mayoría de RAIDs no se dispone del comando TRIM.

**¿Cuál es mejor método para realizar una adquisición de un disco SSD sabiendo estas características y con la posibilidad de qué en la fase de adquisición el hash no coincida?**

Basado en el estudio realizado en este enlace:

<https://www.forensicfocus.com/articles/forensic-acquisition-of-solid-state-drives-with-open-source-tools/>

Se recomienda:

- ◆ Qué el dispositivo sea hashado en la fase de recopilación o recolección, es decir, en el lugar donde se encuentre el sistema y siempre que sea conectado como un dispositivo externo. Esto es debido al tiempo en el que se ejecuta ese comando TRIM. Por lo que es recomendable apagar el sistema y no tirar del cable.
- ◆ Sino fuese posible extraer el dispositivo de almacenamiento del sistema, se debe apagar el sistema y bootear una distribución como CAINE/Tsuguri que no monte el sistema de archivos.
- ◆ En el caso de que no se pueda apagar el sistema, se deberá realizar una adquisición con el equipo encendido.

Para los tres casos sería posible realizar una adquisición física o lógica a nivel de partición y para el triaje no existiría ningún tipo de problema.

## Adquisición de artefactos forenses en sistemas encendidos

Como hemos visto anteriormente, este proceso de adquisición en sistemas live o encendidos, puede ser el no recomendado judicialmente ya que se utilizan los recursos propios del sistema para analizar, es decir, se ejecutan sobre el propio sistema.

Hay que diferenciar que utilizar los propios recursos del sistema para adquirir, como vimos con Caine/Tsuguri y todo se ejecutaba sobre memoria RAM es totalmente diferente a utilizar los propios recursos del sistema para adquirir e incluso analizar.

Aprovechando que tenemos el sistema encendido para realizar análisis, como veremos también podemos realizar la adquisición o verificación de ciertos artefactos.

Es un método agresivo de realizar un análisis forense. Es válido, siempre y cuando se documente exhaustivamente y se justifique el uso de este tipo de método.

La definición de artefacto forense se puede definir como un fichero o conjunto de ficheros, rutas de acceso, configuraciones y registros, que una vez analizado mediante la técnica o programa apropiado pueden terminar cierta actividad. Suelen contener información relevante la investigación.

¿Qué podemos hacer sobre un sistema Live o encendido, del cual tenemos las credenciales de acceso para ejecutar programas?

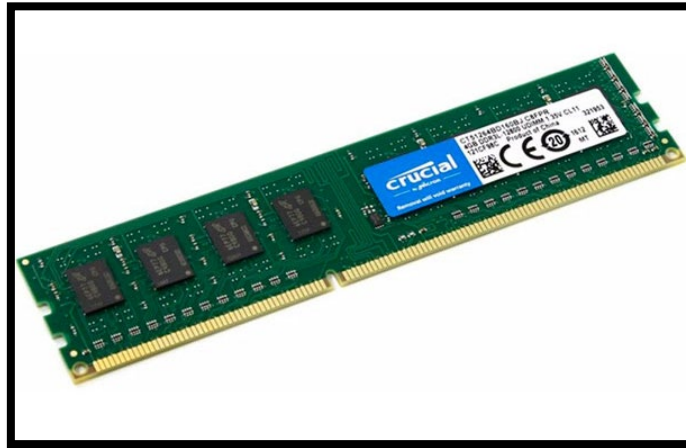
- ◆ Adquisición de memoria RAM
- ◆ Identificación de Cifrado
- ◆ Análisis y extracción de Artefactos





## ADQUISICIÓN DE MEMORIA RAM

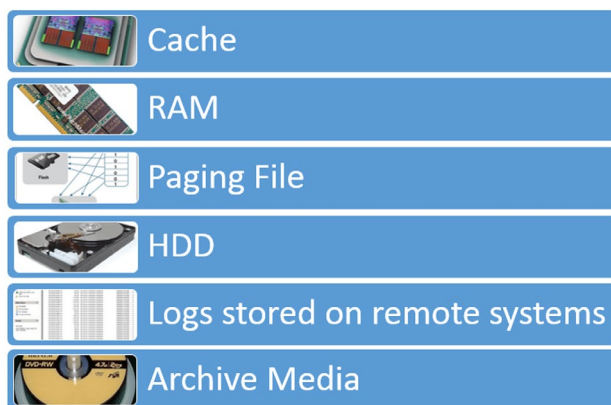
La adquisición de memoria RAM se ha convertido en uno de los mayores cambios en el campo del digital forensics. Hoy en día existe muchas conversaciones respecto a que se debe hacer para responder un incidente cuando el equipo está encendido. Fuerzas y cuerpos de seguridad del estado enseñan a sus agentes que tirar el cable del equipo sería lo ideal. Otros recomiendan adquirir y documentar toda la información volátil, incluyendo la memoria RAM, antes de apagar el sistema.



Los incident responders y las empresas de peritajes forenses no son conscientes de la cantidad de información que puede haber cuando se llega a la escena. Con el incremento de sistemas de cifrado, el tirar del cable, ha hecho que para las empresas de peritajes no tengan nada que investigar, ya que pierden las claves de cifrado, a no ser que se extraigan las claves previamente o sean proporcionadas por el administrador de sistemas.

Como regla general para responder a un incidente donde hay información digital, se debe preservar toda la información posible de la misma manera que fue encontrada cuando se produjo la adquisición de evidencias. La mayor prioridad debería ser capturar toda la información volátil.

La información volátil se refiere a la información que desaparece o es destruida una vez, el sistema es apagado. Típicamente se refiere a la memoria RAM. La información volátil son también las conexiones de red, las aplicaciones que están ejecutándose, puertos abiertos. La mayoría de esta información tiene un valor importante para determinar o refutar, por ejemplo, si alguien se ha conectado remotamente sobre el sistema para monitorizarlo



La adquisición de memoria RAM se realiza con el sistema encendido y con permisos de administrador. Hoy en día no existe método para bloquear la escritura en memoria. Esto podría indicar que al ejecutar el programa de adquisición de memoria RAM, podríamos estar introduciendo cambios en el sistema y ¿se podría invalidar nuestra prueba?

Para responder a esta pregunta, es obligatorio documentar todas las acciones y cambios que vayan a ser realizados sobre el sistema. Como medida adicional, las herramientas que vayan a ser ejecutadas sobre el sistema live, deben ser probadas con anterioridad en sistemas de prueba para verificar su correcto funcionamiento.

**¿Qué hay en la memoria y por qué debe ser adquirida?**



En la memoria están todos los procesos, archivos, directorios y otra información que podría estar. Esta información se puede utilizar obtener, por ejemplo, comandos ejecutados por un individuo. También se podría descubrir viejos e-mails o websites por las que haya navegado. Se podría encontrar restos de procesos que hayan finalizado y probablemente, lo más importante, passwords relacionado con el cifrado y de otros programas.

Mas especialmente:

- ◆ Lista de procesos en ejecución
- ◆ Puertos TCP/UDP Abiertos
- ◆ Historial de navegación privado
- ◆ Ficheros mapeados en memoria
- ◆ Detección de rootkits
- ◆ Información oculta: claves de cifrado, etc
- ◆ Cachés: passwords, clipboards, SAM database



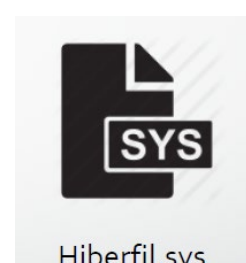
Con el crecimiento del uso del cifrados sobre los sistemas y particularmente sobre los discos de almacenamiento, aplicaciones como Windows BitLocker, PGP y TrueCrypt, se utilizan para cifrar por lo que se ha vuelto más importante el hecho de adquirir memoria RAM y los datos volátiles.

#### Herramientas basadas en Software:

- ◆ FTK Imager
- ◆ [Magnet Forensics Ram Capture](#)
- ◆ [Belkasoft Live Ram Capturer](#)
- ◆ DumpIT
- ◆ WinPmem

Para sistemas que están apagados o post mortem:

- ◆ Fichero de hibernación (también lo podemos encontrar en las shadow copies) -> C:\hiberfil.sys
- ◆ Page File (C:\pagefile.sys)
- ◆ Memory Dumps(C:\Windows\memory.dmp)

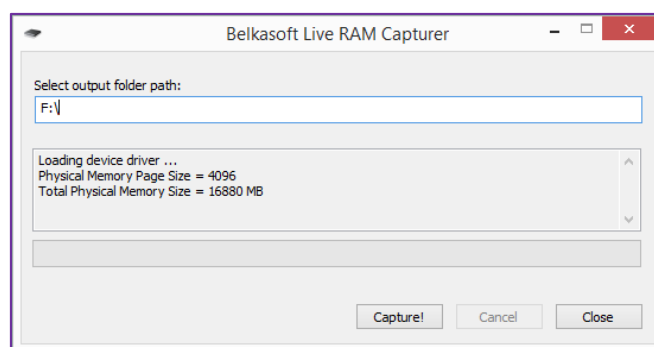


Las herramientas de adquisición cargan un controlador para obtener acceso a la memoria y después leer todo el contenido y guardarlo en un fichero. Hay varias cosas de las que se debe ser consciente con este tipo de enfoque.

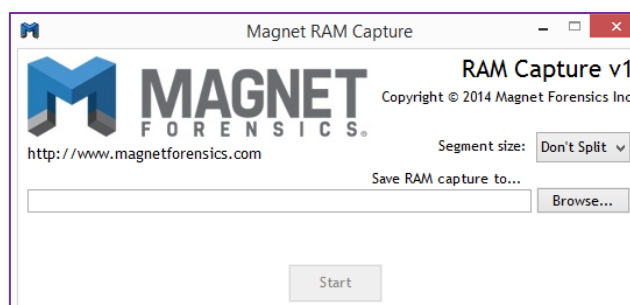
Para aquellos alumnos que tengan experiencia en la búsqueda de malware, se podría identificar que usar un driver para acceder a la memoria es bastante similar a lo que puede llegar a hacer un malware.

Durante la ejecución de estas herramientas podríamos encontrar fallos en el sistema, debido a las aplicaciones que protegen como el Antivirus o un Host Intrusión Prevention software (HIPS). En los sistemas Windows de 64 bits, todos los drivers deben estar firmados digitalmente.

### Belkasoft RAM Capturer



### Magnet RAM Capture



## DETECCIÓN DE CIFRADO

Muchas veces es necesario conocer si el equipo que vayamos a realizar la adquisición dispone de algún cifrado que cuando vayamos a tirar del cable o apagar, ya no podamos disponer de las claves de cifrado

Gracias a la herramienta de Magnet Forensics, [Magnet Encrypted Disk Detector](http://www.magnetforensics.com) podemos identificar a primera vista si el equipo sobre el que se va a realizar la adquisición dispone de alguna partición cifrada.

Verifica:

- ◆ TrueCrypt,
- ◆ PGP
- ◆ Safeboot
- ◆ Bitlocker
- ◆ Veracrypt

```
Encrypted Disk Detector v2.2.0
Copyright (c) 2009-2017 Magnet Forensics Inc.
http://www.magnetforensics.com

* Checking physical drives on system... *

PhysicalDrive0, Partition 1 --- OEM ID: NTFS
PhysicalDrive0, Partition 2 --- OEM ID: NTFS
PhysicalDrive1, Partition 1 --- OEM ID: MSDOS5.0
PhysicalDrive1, Partition 1 --- Volume label: NO NAME

* Completed checking physical drives on system. *

* Now checking logical volumes on system... *

Drive C: is located on PhysicalDrive0, Partition #2.
Drive D: is a CD-ROM/DVD device (#0).
Drive E: is located on PhysicalDrive1, Partition #1.

* Completed checking logical volumes on system. *

* Running Secondary Bitlocker Check... *

* Completed Secondary Bitlocker Check... *

* Checking for running processes... *
```

Importante:

- ◆ Si obtenemos que el equipo está cifrado, se debe realizar una adquisición de ficheros y carpetas - TRIAJE.
- ◆ Si se dispone de claves de cifrado para realizar el descifrado post mortem, no haría falta realizar este paso.

## ANÁLISIS Y EXTRACCIÓN DE ARTEFACTOS

Como hemos comentado anteriormente, se puede dar la situación donde sea necesario ejecutar sobre la propia evidencia herramientas que nos permitan analizar y extraer artefactos forenses.

El Triage es una técnica donde se ejecuta una herramienta sobre un sistema encendido y se realiza una adquisición de ciertos ficheros en concreto, que contienen información relevante para la investigación e incluso dichos ficheros, son analizados sobre el propio computador.

Una de las herramientas más fáciles de utilizar y potentes, debido a la poca huella que deja en la evidencia es KAPE de Eric Zimmerman: <https://ericzimmerman.github.io/>

Dispone de capacidad para procesar las Shadows Copies y subir los resultados a un SFTP, Amazon o Azure.

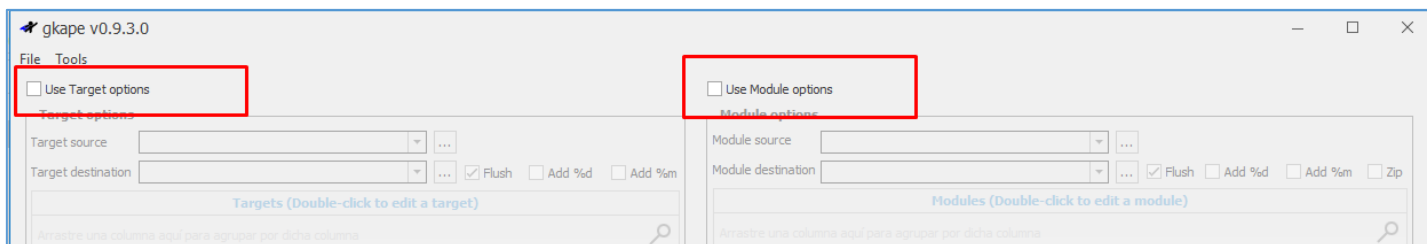
Documentation	File Folder
Modules	File Folder
Targets	File Folder
gkape.exe	53.7 MB Application
kape.exe	2.96 MB Application

Kape solo funciona con sistemas Windows y dispone de dos binarios importantes:

- ◆ gkape.exe – con interfaz gráfica
- ◆ Kape.exe - sin interfaz gráfica

Lo bueno es que se puede “cocinar” el comando final en Gkape.exe para que luego sea utilizado en kape.exe

Si lanzamos Gkape.exe podemos obtener dos secciones bien diferenciadas:



- ◆ Target Options: todas las opciones relacionadas con los ficheros que van a ser adquiridos en un sistema Windows.
- ◆ Module Options: todas las opciones con el procesado de los ficheros que son adquiridos en el Target Options y posibles comandos a lanzar sobre el sistema Windows.
- ◆

### Target Options

- ◆ Target source: se debe indicar la partición que contiene el sistema operativo Windows, normalmente C.
- ◆ Target Destination: donde se van a guardar los ficheros que sean extraídos

También se le puede indicar sobre el target Destination, que borre su contenido (Flush), que añada el día en que realiza la adquisición (%d) y el nombre del computador en que se realiza la adquisición (%m)

☒ Flush ☐ Add %d ☐ Add %m

La lista de Targets, son listas precargadas con las rutas a los ficheros o carpetas que debe adquirir:

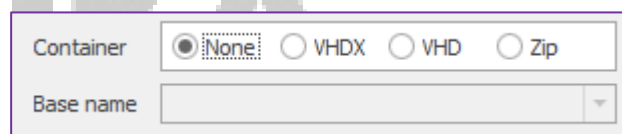
Targets (Double-click to edit a target)				
Arrastre una columna aquí para agrupar por dicha columna				
	Selected	Name	Folder	Description
	<input checked="" type="checkbox"/>	C	C	C
	<input type="checkbox"/>	!BasicCollection	Targets	Basic Collection
	<input checked="" type="checkbox"/>	!SANS_Triage	Targets	SANS Triage Collection.
	<input type="checkbox"/>	\$Boot	Windows	\$Boot
	<input type="checkbox"/>	\$J	Windows	\$J
	<input type="checkbox"/>	\$LogFile	Windows	\$LogFile
	<input type="checkbox"/>	\$MFT	Windows	\$MFT
	<input type="checkbox"/>	\$SDS	Windows	\$SDS
	<input type="checkbox"/>	\$T	Windows	\$T

Si se hace doble click sobre una lista se puede verificar cual serían los objetivos:

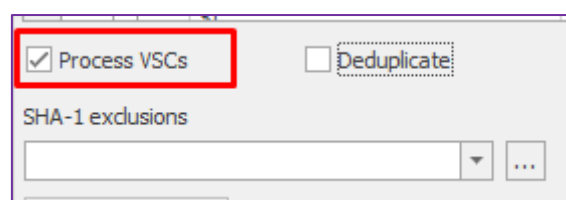


Se puede seleccionar el tipo de contenedor como se guardarán los ficheros adquiridos y que nombre tendrán:

- ◆ Contenedor VHDX: en formato de disco de máquina virtual y
- ◆ Contenedor VHD: en formato de disco de máquina virtual
- ◆ Contenedor ZIP: solamente en ZIP
- ◆ Base Name: nombre base para los contenedores anteriores



Kape permita procesar las Shadows Copies, de tal manera que la lista de targets será aplicada también aquí, para obtener versiones anteriores de los ficheros:



La opción Deduplicate, permite calcular el Hash de los ficheros encontrados en las shadows copies y obtener ficheros únicos, es decir, que, si tienen distinto hash, los copiará, sino no serán copiados.

Kape permite que los contenedores que contienen los ficheros creados, incluyendo los ficheros de las shadows copies sean transferidos cuando terminen a:

- ◆ Servidor SFTP
- ◆ Amazon AWS
- ◆ Azure Storage



Para ello se deben de insertar las credenciales apropiadas de los servidores.

Se recomienda al investigador que verifique las listas de los targets para sus necesidades, sino dejar marcada SANS\_Triage.

Selected	Name	Folder	Description
<input checked="" type="checkbox"/>	RBC	RBC	RBC
<input type="checkbox"/>	!BasicCollection	Targets	Basic Collection
<input checked="" type="checkbox"/>	!SANS_Triage	Targets	SANS Triage Collection.
<input type="checkbox"/>	\$Boot	Windows	\$Boot
<input type="checkbox"/>	\$J	Windows	\$J
<input type="checkbox"/>	\$LogFile	Windows	\$LogFile
<input type="checkbox"/>	\$MFT	Windows	\$MFT

### Module Options

- ◆ Module source: si se deja en blanco será utilizado el destino guardado en el target destination, es decir, trabajara con los ficheros adquiridos.
- ◆ Module destination: donde se guarda el análisis sobre los ficheros o sobre el sistema operativo Windows.

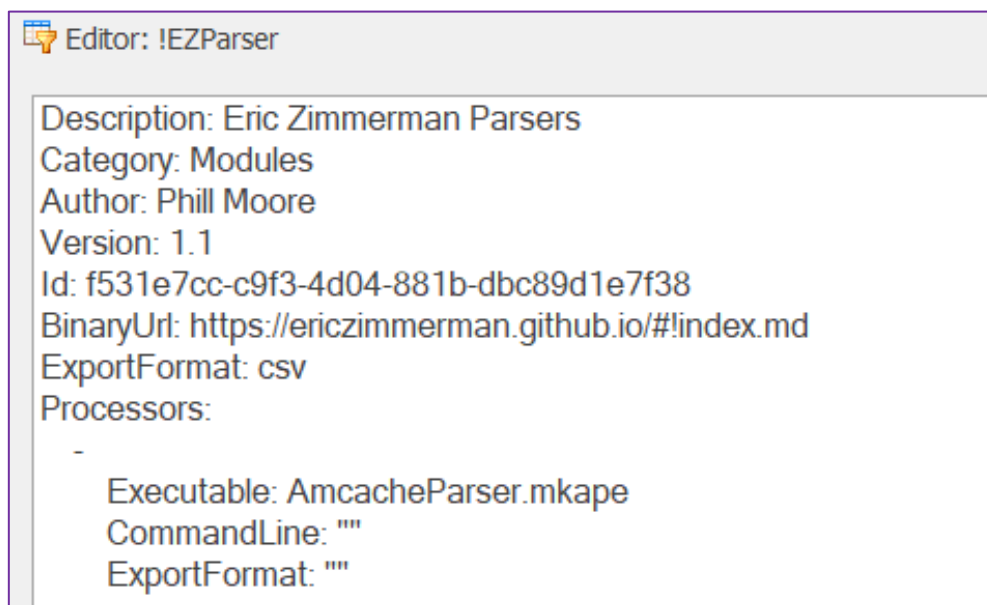
Se le puede indicar que el module destination, si hay algo previamente, que lo borre (flush), que le añada el día en que es analizado (%d), el nombre del computador en que se realizan las acciones (%m) y que los resultados los guarde en un fichero ZIP.

☒ Flush ☐ Add %d ☐ Add %m ☐ Zip

¿Qué operaciones de análisis se pueden hacer de todos los ficheros obtenidos previamente? Pues nuevamente existen operaciones precargadas llamadas “Modules”

Selected	Name	Folder	Category	Description
<input checked="" type="checkbox"/>	RBC	RBC	RBC	RBC
<input type="checkbox"/>	!EZParser	Modules	Modules	Eric Zimmerman Parsers
<input type="checkbox"/>	AmcacheParser	ProgramExecution	ProgramExecution	AmcacheParser: extr...
<input type="checkbox"/>	Apache_Access_Log	Misc	Webservers	LogParser Apache Ac...
<input type="checkbox"/>	AppCompatCacheParser	ProgramExecution	ProgramExecution	AppCompatCachePar...
<input type="checkbox"/>	ApplicationFullEventLogView	EventLogs	EventLogs	Parses Application ev...
<input type="checkbox"/>	ARPCache	LiveResponse	LiveResponse	ARPCache
<input type="checkbox"/>	autoruns	LiveResponse	LiveResponse	Autoruns reports Exp...
<input type="checkbox"/>	bitlocker-key	LiveResponse	VolumeInformation	Collect BitLocker reco...

Es tipo de módulos deberán ser analizados por el investigador para verificar cuál es de su interés. Se puede ver el funcionamiento de cada uno haciendo doble click:

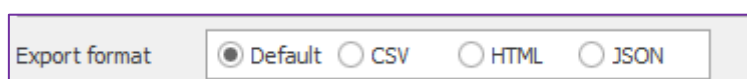


Aprovechando que los módulos, también pueden ser utilizados para ejecutar comandos sobre la máquina o computador, seleccionaríamos:

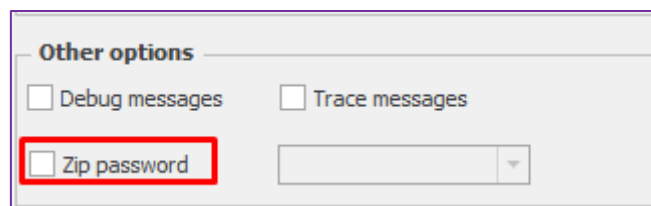
- ◆ Bitlocker-key: si hubiese bitlocker, su clave sería extraída
- ◆ EDD: detectaría el Bitlocker si lo hubiese y otros tipos de cifrado como TrueCrypt, Veracrypt
- ◆ WinPmem: extracción de memoria RAM del equipo

...	Name	Folder	Category	Description
<input checked="" type="checkbox"/>	ABC	ABC	ABC	ABC
<input checked="" type="checkbox"/>	bitlocker-key	LiveResponse	VolumeInform...	Collect BitLocker recovery key for a volume
<input checked="" type="checkbox"/>	EDD	LiveResponse	LiveResponse	Checks the local physical drives on a system for TrueCrypt, PGP,
<input checked="" type="checkbox"/>	WinPmem	LiveResponse	Memory	WinPmem Memory Dump

También se puede seleccionar el formato de salida de los resultados del análisis, es decir, si un módulo debe generar un fichero, en qué formato debe generarlo:



Y para darle confidencialidad a los datos de los análisis obtenidos del sistema, se pudiese establecer una contraseña al fichero ZIP:



Y finalmente podríamos ver el comando que ha sido generado con todas las opciones marcadas en el último recuadro:

```
Current command line
\kape.exe --tsource C: --tdest C:\Users\usuario\Desktop\Kape\destino --target ISANS_Triage --vss --vhd DEMO_KAPE --msource C:\ --mdest C:\Users\usuario\Desktop\Kape\destino --module bitlocker-key,EDD,WinPmem --mvars Unidad:C: --gui
```

Con esta configuración habríamos adquirido los ficheros importantes de Windows, según la lista SANS\_Triage, habríamos obtenido la clave de BitLocker si tuviese BitLocker y también la memoria RAM del equipo.

*\*Ver Video: 007/MÓD. 1 - KAPE*

Se recomienda que siempre que sea posible, seguir estos 5 pasos:

