6669 Criptografía y Seguridad Informática

Informática Forense

¿Qué es la Informática?

Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras

¿Que son las Ciencias Forenses?

Es la aplicación de prácticas científicas dentro del proceso legal

¿Qué es la Informática Forense?

La Informática Forense es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal".

Principio de intercambio de Locard

“Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto”.

Edmond Locard

Identificar

Es introducirnos en el momento, el entorno, la causa y el activo informático al cual hay que realizarle forense.

Tendremos distintas metodologías para las distintas situaciones que nos surjan.

Preservar

En la preservación de los artefactos que vayamos adquiriendo durante el proceso es esencial mantener la integridad de los mismos.

De otro modo se estaría contaminando la evidencia y la misma no tendría valor alguno.

Analizar

El análisis será nuestro próximo paso dentro de nuestro proceso forense, en donde a partir de lo adquirido llegaremos a conclusiones que harán a la causa.

Presentar

Por último, se encuentra la acción de presentar, el armado del Informe Pericial o simplemente un Informe.

Este siempre tiene que tener el vocabulario necesario para su comprensión por las personas que vayan a hacer lectura del mismo.

Roles

- ✔ Consultor técnico
- ✔ Perito de parte
- ✔ Perito de oficio

Perito de Parte o Consultor Técnico

Tanto el Perito de Parte como el Consultor Técnico abogan en favor de unas de las partes del pleito.

En donde, poniendo en juego sus conocimientos, podrán afirmar o rebatir lo expresado en el Informe Pericial del Perito de Oficio.

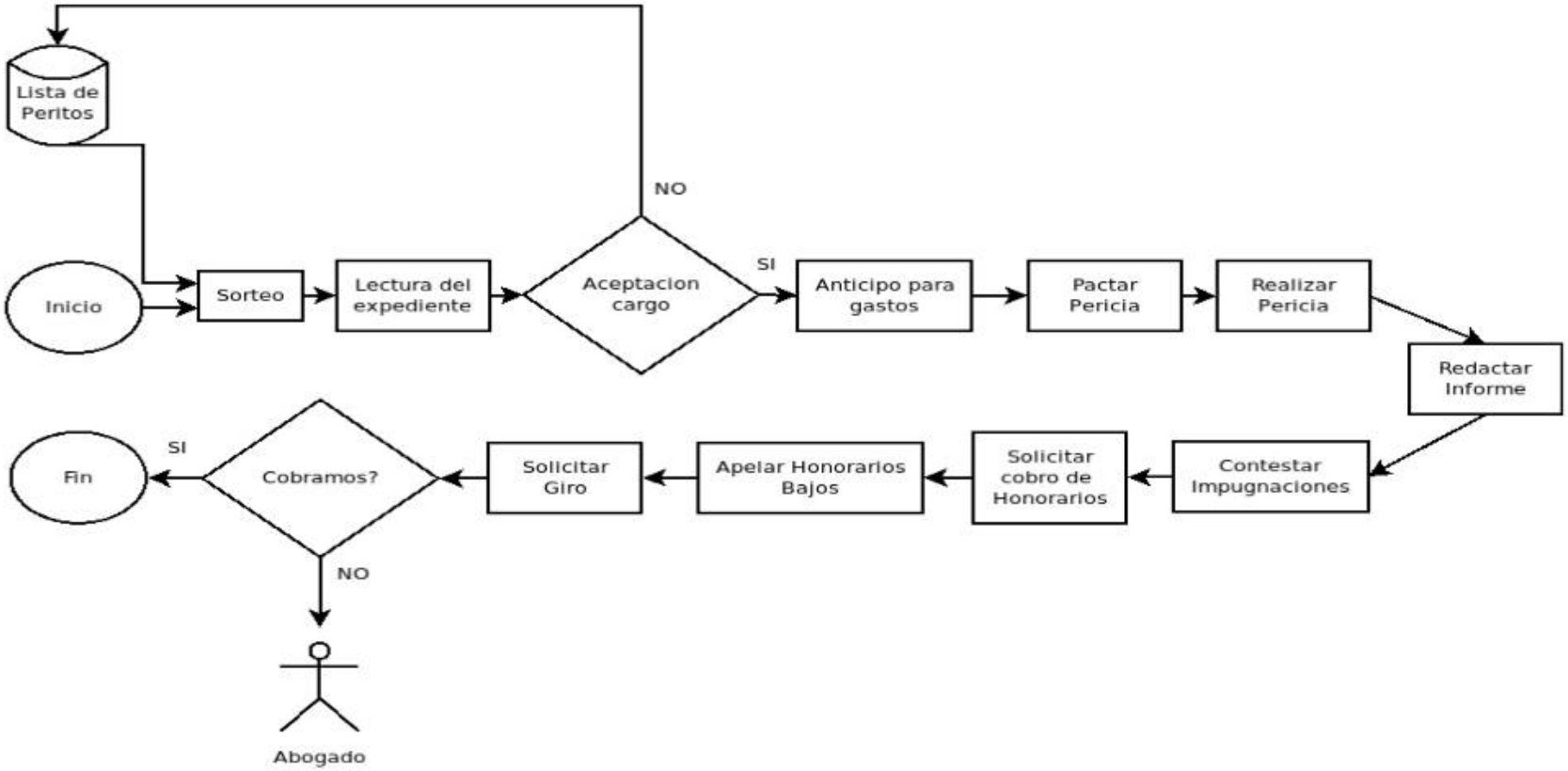
Perito de Oficio

Tal como vimos al momento de definir la acción de presentar, los Jueces no conocen sobre todas las disciplinas y es por ello que suelen solicitar a los especialistas su participación cuando la requieren.

Entonces, se realiza un sorteo para que algún especialista inscripto para actuar en el fuero que corresponde la causa sea designado como Perito de Oficio.

El Perito de Oficio, es el especialista que, como me gusta llamarlo, es la mano informática del Juez.

Proceso del Perito de Oficio



Artefactos

Objetos obtenidos sobre el proceso de adquisición forense.





Prueba digital vs evidencia digital

Denominamos prueba digital a todo aquel elemento digital que se emplea con el fin de demostrar la veracidad o falsedad de un hecho.

La evidencia digital se entiende como todo aquel elemento digital que permite establecer, de manera clara, la relación entre dos elementos.

Criptografía

- ✔ Simétrica
- ✔ Asimétrica
- ✔ HASH

La importancia de HASH

Este algoritmo va a tener un gran valor en cuestiones forenses, ya que, con el mismo podremos asegurar la integridad de los artefactos desde el momento de la adquisición hasta el momento de la entrega del Informe Pericial.

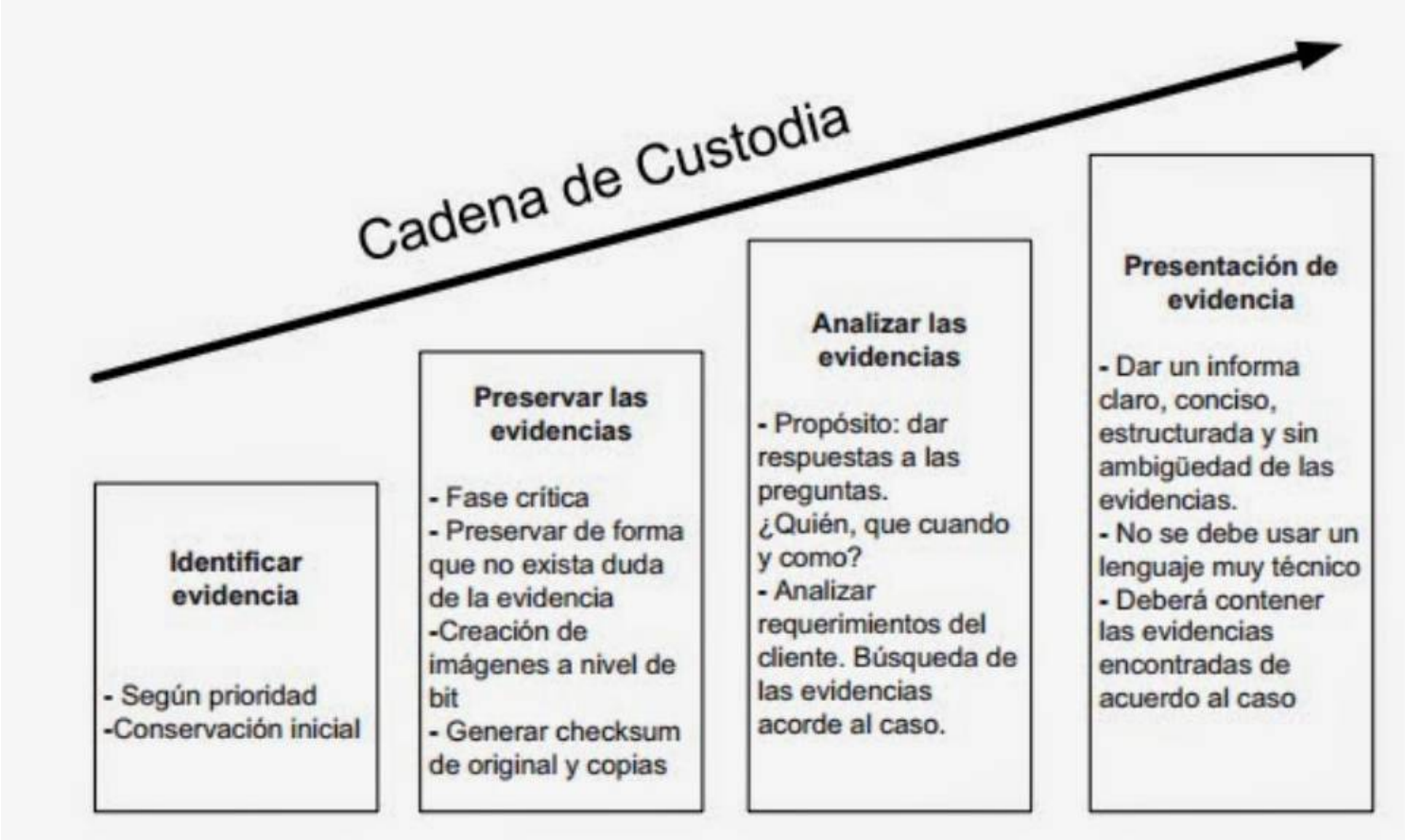
En la actualidad hay algoritmos que se encuentran rotos, por lo cual se recomienda no utilizarse, entre ellos se hallan: MD5 y SHA1. Es recomendable el uso de SHA256 y SHA512.

Cadena de custodia

Es la manera en que se asegura la NO alteración de los artefactos recolectados desde su adquisición hasta la presentación de la evidencia.

La cadena de custodia es el conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de los objetos o muestras que pueden ser fuente de prueba de hechos criminales (preservación total de su eficacia procesal).

Cadena de custodia



Triage

Es un procedimiento que se toma prestado de la medicina, mediante el cual se evalúa rápidamente el estado de varios pacientes para establecer la prioridad y orden en que deben ser atendidos.
En el ámbito de la informática forense, el triage es un análisis rápido que se realiza sobre un equipo para determinar si contiene evidencia o indicios que puedan ser de utilidad para una investigación. De esta forma se puede examinar rápidamente un conjunto de equipos y determinar su importancia para la investigación en curso.

Adquisición

En el campo de la Informática Forense, uno de los puntos más importantes es la recolección de la evidencia, también conocido como Adquisición Forense, ya que, si al momento de tomar la evidencia no se toman los recaudos correspondientes puede echarse a perder todo el análisis posterior.
Es muy importante recalcar este punto debido a que la alteración de la evidencia llevará a la invalidez de toda la investigación.
Un punto a considerar al momento de realizar las copias bit a bit es que necesitaremos de tiempo, ya que, es un proceso que suele demandar varias horas.

Tipos de adquisiciones

Adquisición física

Se entiende por adquisición física a la adquisición forense de la capacidad absoluta de un medio de almacenamiento.

Adquisición lógica

En el caso de la adquisición lógica, se adquiere por volúmen lógico, por partición. Esto quiere decir que si nuestro disco es de 1TB pero dentro tenemos una partición de 100GB podríamos únicamente realizar la copia bit a bit solo de esos 100GB.

Tipos de adquisiciones

Adquisición directa

Se llama Adquisición Directa cuando se extrae el medio de almacenamiento y se conecta al equipo de analista forense con el fin de realizar su copia bit a bit.

Adquisición indirecta

En el caso de la adquisición Indirecta a la adquisición forense realizada por medio de un SW utilizando la red como medio de transmisión para almacenar la copia en un equipo remoto.

Tipos de adquisiciones

Adquisición por hardware

Como supondrán, en este caso nos referimos a realizar la adquisición por un dispositivo que se encuentra diseñado para realizar copias forenses. Los mismos, por lo general, traen un bloqueador de escritura para evitar contaminar la evidencia.

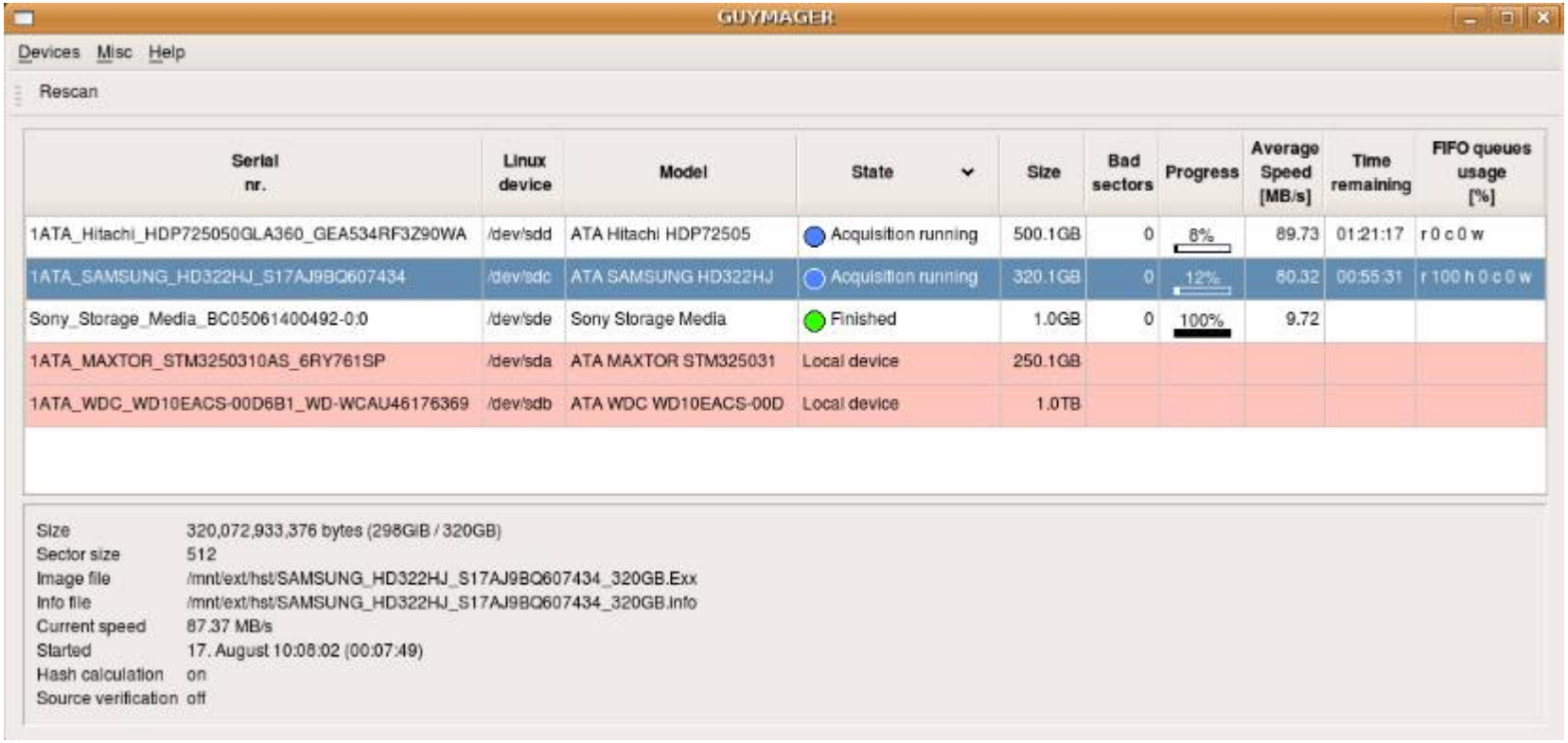
Adquisición por Software

En este caso, se utilizará para realizar la adquisición software confeccionado para llevar a cabo la copia bit a bit. En este caso, tenemos que preocuparnos de que el disco no se monte con permisos de escritura, ya que, si esto sucede estaríamos contaminando la evidencia.

GUYMAGER

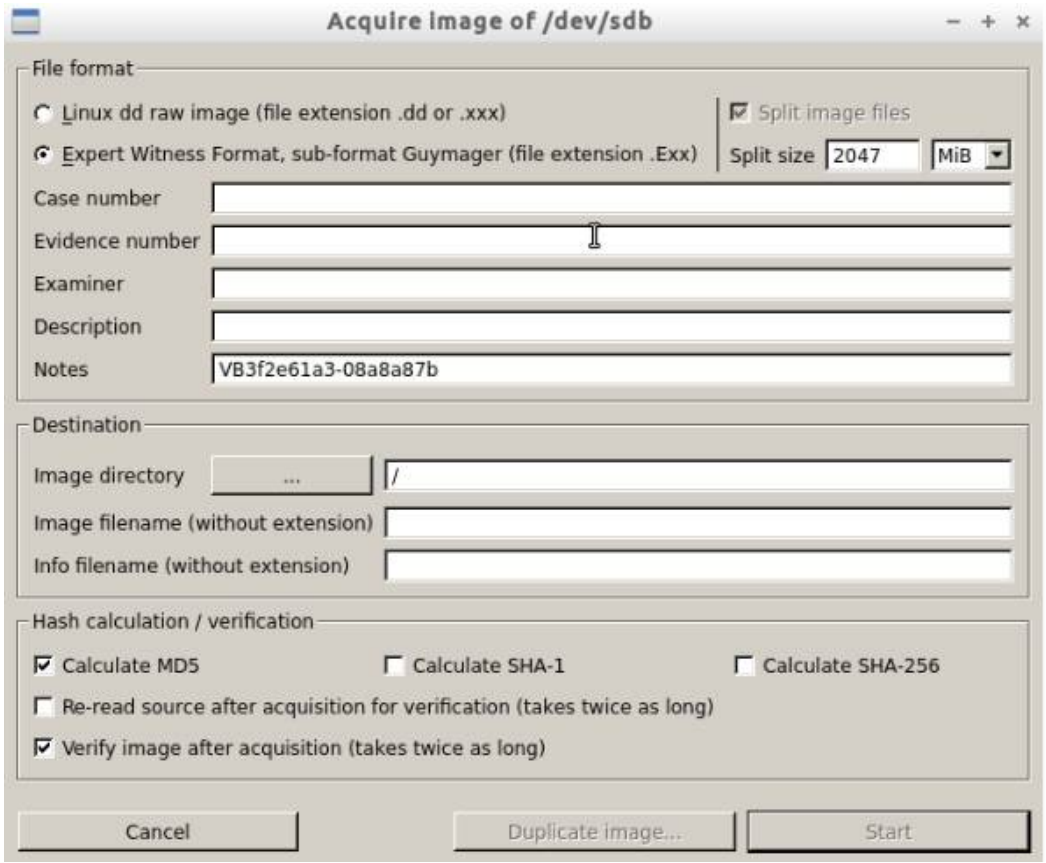
Es una alternativa a dd y ewfacquire, posee interfaz gráfica bastante intuitiva y permite la salida tanto en formato RAW como en EWF. RAW es el formato crudo, del mismo modo que realiza dd, para ser más preciso, utiliza dd para realizar la adquisición. Permite particionar archivos por tamaño y también nos genera un log muy completo con el proceso que realiza.

GUYMAGER


GUYMAGER
Devices Misc Help
Rescan
Serial nr.
Linux device
Model
State
Size
Bad sectors
Progress
Average Speed [MB/s]
Time remaining
FIFO queues usage [%]
1ATA_Hitachi_HDP725050GLA360_GEA534RF3Z90WA /dev/sdd ATA Hitachi HDP72505 Acquisition running 500.1GB 0 8% 89.73 01:21:17 r 0 c 0 w
1ATA_SAMSUNG_HD322HJ_S17AJ9BQ607434 /dev/sdc ATA SAMSUNG HD322HJ Acquisition running 320.1GB 0 12% 80.32 00:55:31 r 100 h 0 c 0 w
Sony_Storage_Media_BC05061400492-0:0 /dev/sde Sony Storage Media Finished 1.0GB 0 100% 9.72
1ATA_MAXTOR_STM3250310AS_6RY761SP /dev/sda ATA MAXTOR STM325031 Local device 250.1GB
1ATA_WDC_WD10EACS-00D6B1_WD-WCAU46176369 /dev/sdb ATA WDC WD10EACS-00D Local device 1.0TB
Size 320,072,933,376 bytes (298GiB / 320GB)
Sector size 512
Image file /mnt/ext/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.Exx
Info file /mnt/ext/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.info
Current speed 87.37 MB/s
Started 17. August 10:08:02 (00:07:49)
Hash calculation on
Source verification off

Informática Forense - Preservación

GUYMAGER



Autopsy

Autopsy es una interfaz gráfica de las herramienta por línea de comando para investigación digital contenidas en Sleuth Kit. Puede analizar discos de Windows y Linux (NTFS, FAT, UFS1/2, ext2/3)

Tanto Autopsy como Sleuth Kit son open source y corre sobre plataformas Windows y Linux.

Autopsy

Permite realizar las siguientes acciones:

- ✔ Listado de archivos
- ✔ Contenido de archivos
- ✔ HASH
- ✔ Timeline
- ✔ Búsquedas por palabras clave
- ✔ Análisis de Metadata
- ✔ Detalles de imagen

Informática Forense

Autopsy