DOCENTE: Ing. Pablo A. Rodriguez Romeo

MATERIA: Computer Forensics

EKOPARTY
HACKADEMY

Hola!

SOY Pablo Rodriguez Romeo

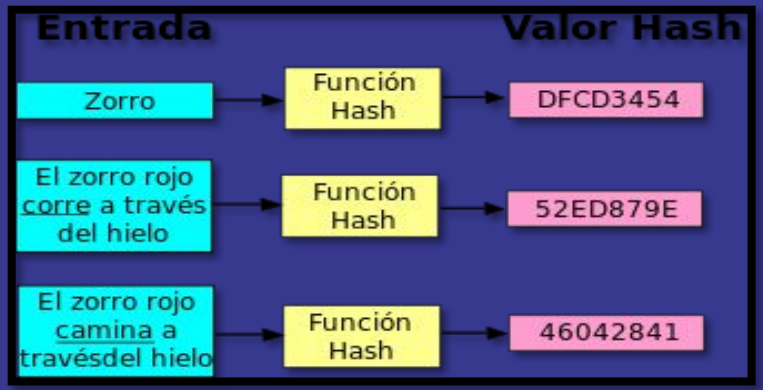
I am here because I love to give presentations.

You can find me at @username

Extracción y preservación de evidencia digital de almacenamiento

Hash o funciones resumen

Es una función que tiene como entrado, un conjunto de datos y como salida un numero finito, al cambiar el conjunto de datos de entrada el numero finito de salida cambia



EKOPARTY HACKADEMY

NOCIONES BÁSICAS

Informática Forense

Es la ciencia de adquirir, preservar y presentar los datos que han sido procesados almacenados electrónicamente y/o trafican en la red.

La prueba Digital

Se podría definir que la prueba digital es todo dato no tangible resguardado en algún tipo de dispositivo de almacenamiento magnético o electrónico

EKOPARTY HACKADEMY

NOCIONES BÁSICAS

Características de la prueba digital:

Prueba Constante - Prueba Volátil

Ser muy Frágil:

Tiene la gran posibilidad de ser eliminada o modificada con facilidad.

Ser reproducible:

Tiene la gran posibilidad de ser copiada sin rastros.

Ser anónima:

No se puede saber con exactitud si realmente lo que se extrajo pertenece a un individuo en particular.

NOCIONES BÁSICAS

LA PRUEBA DIGITAL

Evidencia Constante:

Es el tipo de evidencia más buscada en los análisis forenses.

Se refiere a la evidencia almacenada en un dispositivo magnético u óptico que se mantiene preservada después de perder la energía.

Evidencia Volátil:

Es el tipo de evidencia más difícil de obtener.

Se refiere a la evidencia almacenada en la memoria RAM o en algun cache que normalmente se pierde al perder la energía.

NOCIONES BÁSICAS

Dispositivos con Prueba digital

Computadora de escritorio o portátil

Hardware de Red

Servidor

Teléfono celular

Identificadores de llamadas

“GPS”

Cámaras, videos

Memoria “flash”

Pendrives

Discos Rígidos

Tablets

Reproductores de mp3

NOCIONES BÁSICAS

Dispositivos con EVIDENCIA digital

Etapas Forense

Adquisición: Acceso al objeto de estudio

Preservación: Conservar el objeto

Obtención: Análisis y búsqueda

Adquisición de la prueba

- Acceso durante Allanamientos
- Procedimientos Notariales
- Resguardado por la autoridad policial

Fuentes de prueba Digital

Los Medios de Almacenamiento (Sistemas)

Los Dispositivos de Comunicación (Redes y sistemas de transmisión de información)

Fuentes de Evidencia

Básicamente se confía en los Registros y restos de información recuperados de un Sistema comprometido en la Escena del Crimen.
Necesitamos saber :
- Dónde está la prueba
- Qué significa la prueba
- Como obtenerla y resguardarla (adquirirla y preservarla)

La prueba obtenida en violación de cualquier procedimiento técnico-legales es INADMISIBLE (prueba nula)
…y todas las conclusiones que obtenga a partir de esta Evidencia!!!

Preservación de la prueba

- Cadena de Custodia
- Obtención de Imágenes digitales
- Utilización de software que duplique bit a bit
- Validación de las copias mediante un algoritmo matemático (hash)

MODOS DE ADQUISICION

Aspectos a tener en cuenta para elegir el modo de adquisición

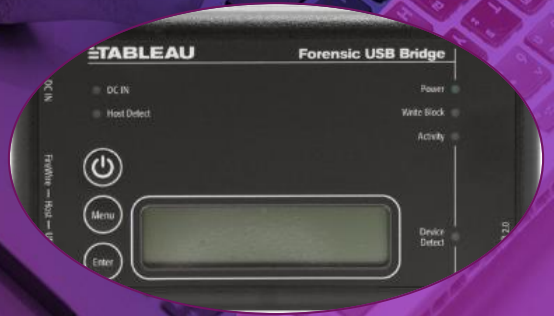
- Lugar
- Posibilidad de exceso al almacenamiento
- Tiempo disponible
- Espacio de almacenamiento

ADQUISICION POR METODO DIRECTO

Es el más rápido pero requiere de un bloqueador de escritura (Write blocker) o un OS (DOS-Linux) modificado

Pasos a seguir :
1- Extraer medio de almacenamiento sospechoso
2- Montar disco en el dispositivo de adquisición
3- Adquirir imagen
4- Verificar el hash

Equipos que bloquean la escritura

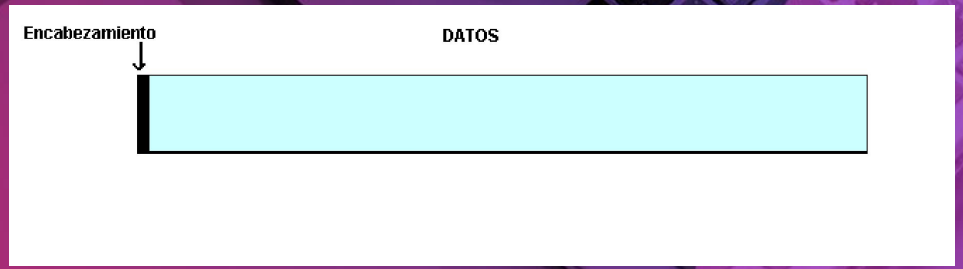


Equipos copian y bloquean la escritura

Equipos copian y bloquean la escritura

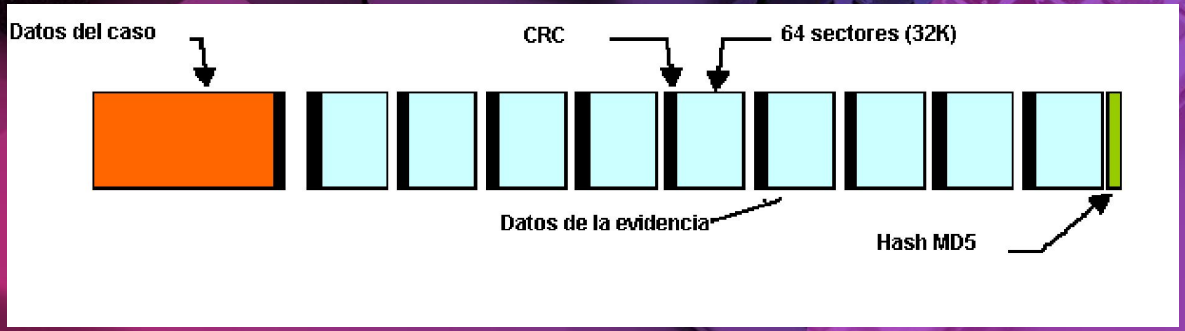
Formato de evidencia “dd”

- Simple de utilizar
- Split externo
- Hash externo
- Compresión externa
- Sin checksum
- Sin límite de tamaño



Formato de evidencia “Encase”

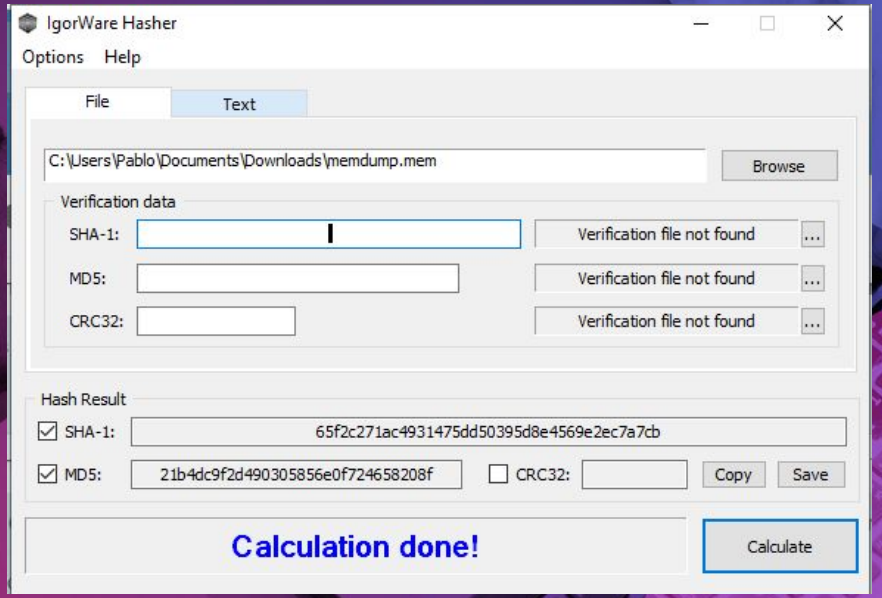
- Simple de utilizar
- Split y compresión nativa
- Hash incluido en el encabezado
- Checksum ajustable /granularidad
- Límite de tamaño
- Soporte password de adquisición



Documentación

EKOPARTY HACKADEMY

Preservación de la Prueba



Gracias