DOCENTE: Ing. Pablo A. Rodriguez Romeo

MATERIA: Computer Forensics

EKOPARTY
HACKADEMY

Hola!

SOY Pablo Rodriguez Romeo

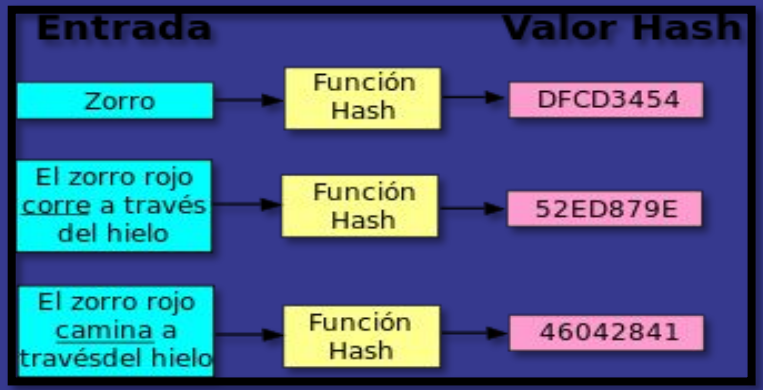
I am here because I love to give presentations.

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

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.

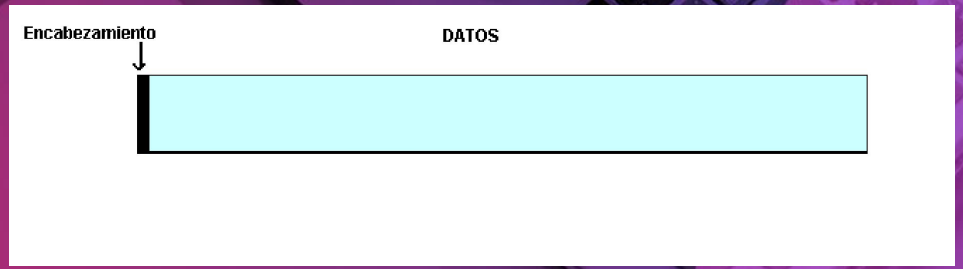
Se refiere a la evidencia almacenada en la memoria RAM o en algun cache que normalmente se pierde al perder la energía.

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)

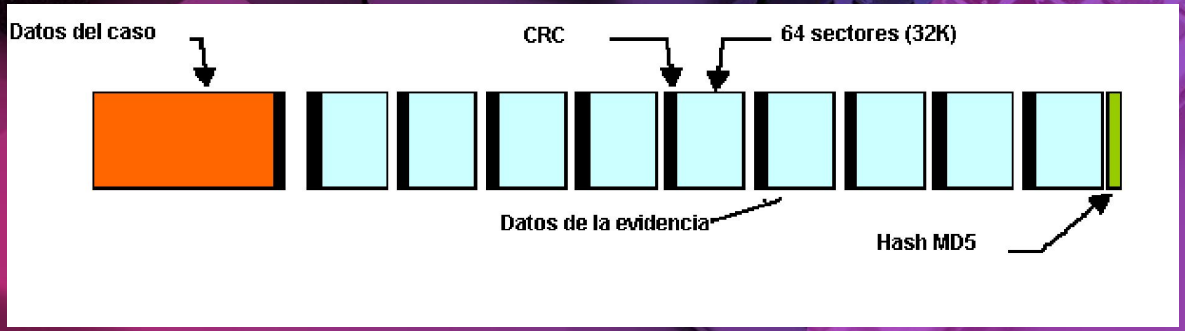
Formato de evidencia “dd”

- 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



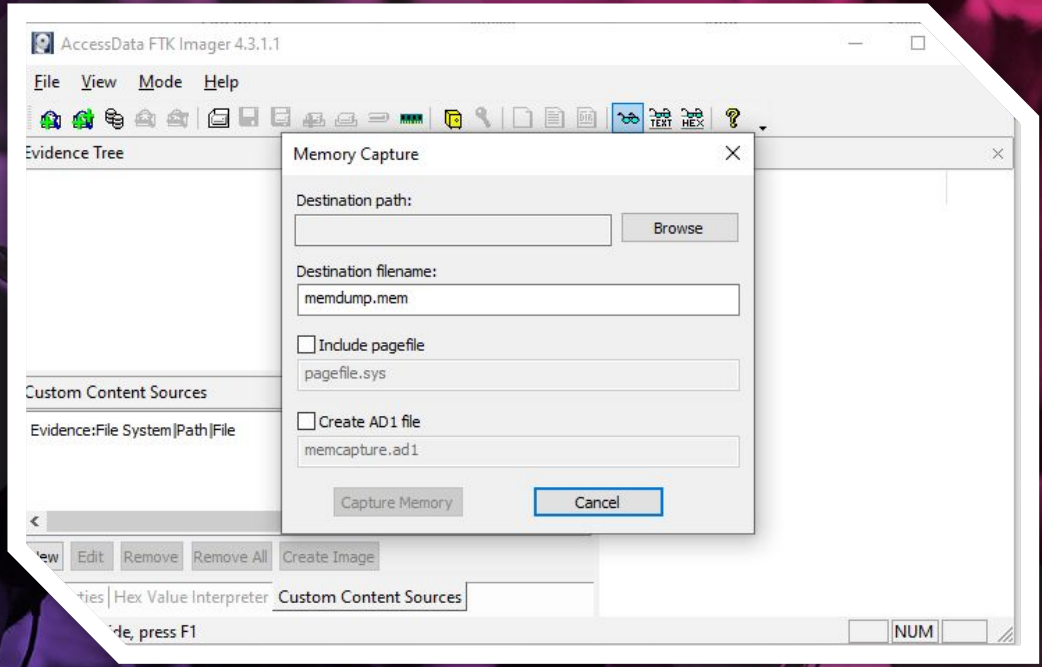
Documentación

EKOPARTY HACKADEMY

Preservación de la Prueba

Capture imagen lo más precisa posible del sistema

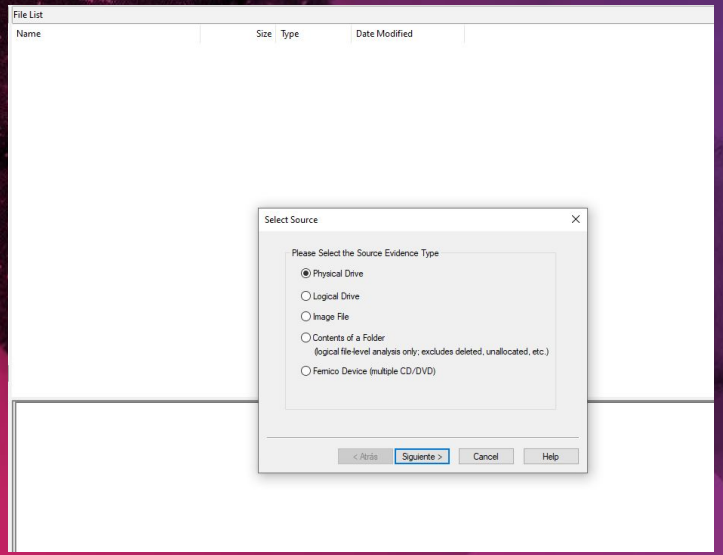
Memoria Ram



Hacer pruebe en vivo

EKOPARTY HACKADEMY

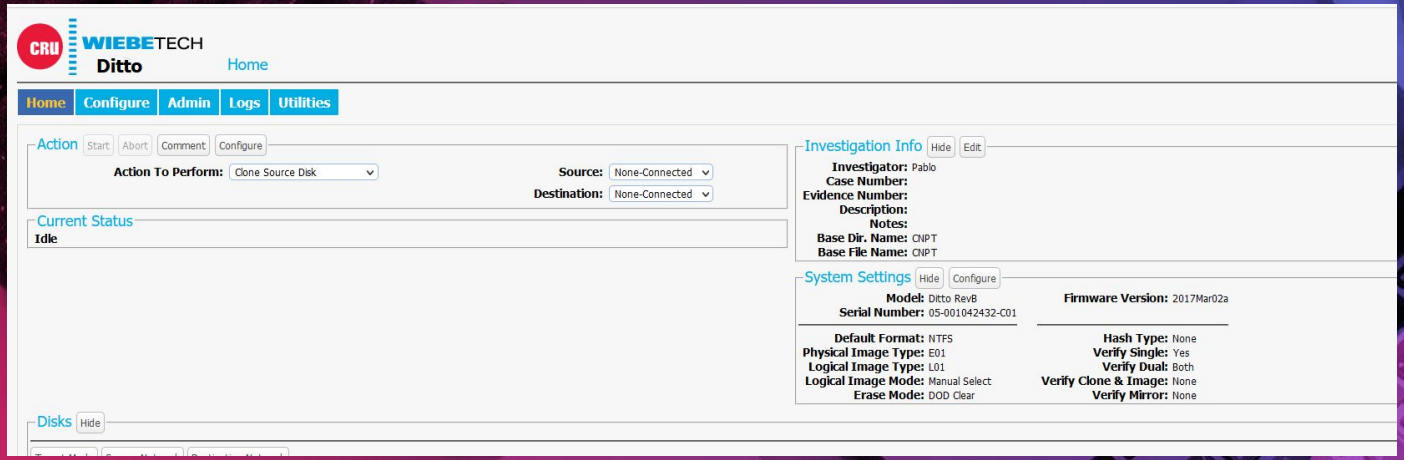
Preservación de la Prueba con soft



Hacer pruebe en vivo

EKOPARTY HACKADEMY

Preservación de la Prueba con hard



Hacer pruebe en vivo

EKOPARTY HACKADEMY

Preservación de la Prueba - Apple

¿Qué información se puede pedir?

Datos de registro de los dispositivos
Records de servicios al cliente
Uso de iTunes
Transacciones on-line
Transacciones en locales oficiales y representantes
Tarjeta de crédito
Acceso a iCloud
iOS Activación de dispositivos

Datos de contacto:

1 - Se debe completar el siguiente formulario:

Microsoft Word - gle-inforequest.docx (apple.com)

EKOPARTY HACKADEMY

Preservación de la Prueba - Apple

Enviarlo a por correo electrónico oficial a la casilla:

lawenforcement@apple.com

Para tramitar el congelamiento y conservación de una cuenta, es por 90 días y ampliable por otros 90 días más completando nuevamente el formulario y enviarlo a la casilla: **subpoenas@apple.com**

Tener en cuenta:

Apple notificará a sus clientes y/o usuarios cuando se busque la información de su cuenta de Apple en respuesta a una solicitud legal válida de Gobiernos y/o Fuerzas de la Ley, excepto cuando la solicitud legal válida explicite la prohibición de notificar

EKOPARTY HACKADEMY

Preservación de la Prueba – Facebook – Instagram

Confeccionar oficio dirigido a

Facebook Security, Law Enforcement Response Team
Señor Gerente de Facebook Inc.
1601 Willow Road
Menlo Park, CA 94025

Nombre de la autoridad que realiza la solicitud, dirección de correo electrónico oficial y un número de teléfono de contacto directo.
- Dirección de correo electrónico del usuario, número de identificación de usuario (http://www.facebook.com/profile.php?id=1000000XXXX) o nombre de usuario del perfil de Facebook (http://www.facebook.com/username)

Hacer pruebe en vivo

EKOPARTY HACKADEMY

Preservación de la Prueba – Google

Confeccionar oficio dirigido a

Google Inc.
1600 Amphitheatre Parkway
Mountain View, California 94043
United States

Para solicitar información referida a direcciones IP, registros de conexión y/o datos sobre el suscriptor de una cuenta y fecha de creación de la misma incluir:

- Datos de la Causa.
- Autoridad judicial que solicita la información

EKOPARTY HACKADEMY

Resumiendo

Gracias