UNIVERSIDAD AGRARIA DEL ECUADOR
FACULTAD DE CIENCIAS AGRARIAS
CARRERA: INGENIERIA EN CIENCIAS DE LA COMPUTACIÓN
ASIGNATURA: SEGURIDAD INFORMÁTICA

TRABAJO DE INVESTIGACIÓN:

¿QUÉ ES UNA COPIA DIGITAL FORENSE?
¿CÓMO OBTENER UNA COPIA DIGITAL FORENSE?
¿PARA QUÉ SIRVE UNA COPIA DIGITAL FORENSE?
¿FUNCIONALIDADES DE LOS HASH EN LAS COPIAS DIGITALES FORENSES?

DOCENTE:
ING. ENRIQUE FERRUZOLA.

ESTUDIANTE:
ARTURO FRANCESCO NEGREIROS SAMANEZ.

¿Qué es una copia digital forense?

La copia digital forense es una replica digitalizada de la información o evidencia digital que está siendo procesada, con la finalidad de no alterar la misma de la fuente original. La evidencia digital se puede definir como cualquier información probatoria o almacenada o transmitida en forma digital que una parte de un caso judicial puede usar en un juicio.

Estas pruebas se pueden encontrar en distintos dispositivos de almacenamiento o transmisión, pudiendo ser discos rígidos, cintas de respaldo, distintos tipos de tarjetas de memoria de teléfonos celulares, computadoras o cualquier terminal tecnológica.

¿Cómo obtener una copia digital forense?

Para obtener una copia digital forense, primero se debe determinar que dispositivos de almacenamiento o transmisicón están vinculados en algún incidente. Luego de que el/los dispositivos sean elegidos, ejecutar las herramientas del caso para la clonación de digital para posterior análisis; las herramientas más elegidas en estos casos, trabajando en un entorno basado en Unix tales como: dd, dc3dd, dcfldd; cabe recalcar que estas herramientas se las puede ejecutar desde la terminal de comandos agregando los parámetros para hacer la clonación; por ejemplo:

arturo@arturo:~$ sudo dd if=/dev/sdc1/ of=~/Desktop/usbCloned/image.img bs=4M

Dónde **dd** es el comando que nos permite hacer el proceso de clonación bit a bit, “**if**” el dispositivo que queremos clonar, “**of**” hacia donde vamos a enviar la imagen clonada y “**bs**” lee y escribe bytes.

¿Para qué sirve una copia digital forense?

Poder tener una copia exacta de un disco permite al investigador acceder al sistema de archivos e inspeccionar las cuentas de usuario existente, los documentos asociados a un usuario, y los programas instalados, entre otras cosas. Adicional es posible realizar la recuperación de archivos borrados o datos especiales en partes del disco.

¿Funcionalidades de los hash en las copias digitales forenses?

Partiendo del *¿Cómo es posible verificar que la imagen creada a partir de una copia digital es un duplicado exacto del dispositivo de almacenamiento original conteniendo la evidencia?* Esto lo podemos responder con un valor único llamado “Hash”. El Hash es un valor único generado por un algoritmo criptográfico, los valores hash son utilizados en una diversidad de maneras incluyendo la integridad de la evidencia criptográfica; son común mente asociados a una huella digital si al menos se hiciera un cambio en un solo bit en el dispositivo de almacenamiento generaría un hash diferente.

Bibliografías.

http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/informatica_forence.htm

http://www.reydes.com/d/?q=Los_Hashes_en_el_Ambito_del_Forense_Digital

https://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-de-informacion/#:~:text=2013%20%2D%2001%3A41PM-,El%20an%C3%A1lisis%20forense%20digital%20se%20corresponde%20con%20un%20conjunto%20de,el%20estado%20de%20los%20mismos.&text=introducir%C3%A1%20el%20tema%2C-,El%20an%C3%A1lisis%20forense%20digital%20se%20corresponde%20con%20un%20conjunto%20de,el%20estado%20de%20los%20mismos.

https://www.cyberciti.biz/faq/linux-copy-clone-usb-stick-including-partitions/

https://tools.kali.org/forensics/dc3dd