Profesor

Constantino Malagón

Seguridad Informática

Imágenes forenses

Universidad Francisco de Vitoria UFV Madrid

Grado en Ingeniería Informática
Escuela Politécnica Superior

Imagen forense

Universidad Francisco de Vitoria UFV Madrid

- La obtención de una imagen forense consiste en copiar todo el contenido de un disco duro (o cualquier medio de almacenamiento), sector por sector, en otro dispositivo de almacenamiento o **fichero de imagen** para luego analizarlo.
- Se genera a su vez una firma hash de los bits leídos durante el proceso.
- Con ello se obtiene una **copia exacta** a bajo nivel de todo el contenido del disco duro además de certificar su contenido con una firma **hash**.

Imagen forense

- La firma hash crea una cadena de números y caracteres mediante la aplicación de una función matemática unívoca a los bits leídos del disco duro y que ahora están presentes en la imagen.
- Este número tiene una dependencia del contenido evaluado por el algoritmo permitiendo que si se produjera un cambio en los datos, el numero HASH cambiaría.
- Por ello la firma hash permite certificar que el contenido del disco duro no se ha visto alterado durante la intervención del perito informático ni con posterioridad por ninguna otra persona.

Preparación

- 1) Agregamos un disco duro a la máquina virtual: /dev/sdb
- 2)Creamos tres particiones, una primaria y dos lógicas
  - Primaria: ext4
  - Lógica 1: fat32
  - Lógica 2: ntfs
- 3) Montarlas agregándolas en /etcfstab en los siguientes puntos de montaje
  - Primaria: /mnt/PRI_ext4
  - Lógica 1: /mnt/LO_fat32
  - Lógica 2: /mnt/LO_ntfs

Herramientas

Universidad Francisco de Vitoria UFV Madrid

- Hay muchas herramientas pero vamos a centrarnos en dos que se suelen usar en Linux: dfcldd y dc3dd.
- Las dos están preinstaladas en Kali

Herramientas

Universidad Francisco de Vitoria UFV Madrid

- Herramienta 1: dc3dd
- Hacemos primero fdisk –l para ver qué particiones tenemos.
- Hay que saber muy bien:
  - ¿Qué es una partición?
  - ¿Qué tipos de particiones hay?
  - ¿Cómo se nombran los discos duros en Linux?
  - ¿Cómo se nombran las particiones en Linux?

Herramientas

- Herramienta 1: dc3dd
- Para hacer una imagen de la partición /dev/sdb2 hacer:
  - dc3dd if=/dev/sdb2 of=/tmp/0002.dd
- if -> input file
- of -> output file
- El /tmp dice que el fichero lo guarde ahí. Puedo cambiar esa ruta

Herramientas

- ¿Cuánto ocupa este fichero imagen?
- Para ver cuánto ocupa:
  - du –h /tmp
  - También ls –lh /tmp (o en donde lo haya guardado)
- Ojo que habrá que tener un disco con suficiente espacio para almacenar este fichero imagen
- Es recomendable que este disco duro destino esté cifrado

Herramientas

- Si queremos añadir un hash y que guarde un log con éste y la salida:
  - dc3dd if=/dev/sdb2 of=0002.dd hash=sha256 log=/tmp/sdb1.log
- En este caso usaríamos el algoritmo sha256 para generar el hash
- Pueden usarse md5, sha1, sha256 ó sha512

Herramientas

- A medida que se realiza la imagen, también se calcula el hash del disco de origen en paralelo.
- Luego, una vez que termina el proceso de copiar los datos, se calcula el hash para la salida (imagen), y se contrasta contra el de origen (partición).

Herramientas

- Herramienta 2: dfcldd
- Para hacer una imagen de la partición /dev/sdb1 hacer:
  - dcfldd if=/dev/sdb1 of=/tmp/0001.dd (se hace en un fichero, la extensión da igual, pero es común usar la extension .dd o .iso)

Herramientas

- Si queremos añadir un hash y que guarde un log con éste y la salida:
  - dcfldd if=/dev/sdb2 of=0002.dd hash=md5 hashlog=/tmp/sdb1.log
- En este caso usaríamos el algoritmo md5 para generar el hash

Herramientas

- La comparación de los hash de entrada contra los de salida no es realizada en forma automática como lo hacía dc3dd.
- Para realizar esta verificación se debe ejecutar otra vez dcfldd con otras opciones, o utilizar otra herramienta como md5sum

Herramientas

- Para ello me voy al directorio donde he almacenado las imágenes (/tmp en nuestro caso) y ejecuto:
  - cd /tmp
  - md5sum 000*.dd > hash
- Mediante la orden diff puedo compararlos
  - Mejor hacer una copia de los ficheros de log (el creado por dcfldd y por md5sum) y llevarlos al mismo directorio (por ejemplo al /tmp)
  - Editarlos y borrar todo lo que no sean los hash en estos ficheros
  - diff hash sdb1.log

Herramientas

- Como podemos ver la salida de dcfldd es mucho más simple que la de dc3dd, ofreciendo menos información del proceso.
- Además la velocidad de copia es más lenta

Herramientas

- Las dos herramientas anteriores son versiones mejoradas de una herramienta clásica de copia en Linux llamada dd
- La sintaxis es la misma
  - dd if=/dev/sdb2 of=0002.dd
- Esta herramienta dd se utiliza mucho para hacer backups, mientras que las otras dos se utilizan más en análisis forense

Herramientas

- **Herramienta 3:** FTK imager
- Es una herramienta comercial aunque gratuita
- La version para Windows es gráfica mientras que la version para Linux es para el shell
- Podemos crear las imágenes y cargar imágenes ya hechas desde las otras dos herramientas anteriores para su análisis
- Para descargarla buscar FTK imager en Google. Necesitaremos registrarnos para descargarla

Herramientas

- Una de sus características más importantes es que se puede comprimir el fichero imagen
- Esto en teoría sería un poco más lento, pero esto está optimizado y la diferencia no es muy grande
- Podemos obtener una imagen de 4 GB de una partición de 10 GB

Preparación de la creación de la imagen

Universidad Francisco de Vitoria UFV Madrid

- Vamos a ver ahora la parte práctica
- ¿Cómo haríamos este proceso en un caso real?
- Tenemos que distinguir entre varios escenarios

Preparación de la creación de la imagen

Universidad Francisco de Vitoria UFV Madrid

- 1) El equipo que estamos analizando o encontramos encendido
- En este caso, no queremos que la información que está en el disco se modifique, por lo que si apagáramos la misma de forma normal, las aplicaciones y el sistema operativo escribirían en el disco al cerrarse.
- Y encima el contenido de la memoria RAM se eliminaría
- Ya veremos que esto también lo analizaremos

Preparación de la creación de la imagen

Universidad Francisco de Vitoria UFV Madrid

- De igual forma, si instaláramos alguna aplicación también estaríamos modificando el estado del mismo.
- No ocurriría esto si arrancamos con un USB Live de Kali por ejemplo o ForLex (http://www.forlex.it)

Preparación de la creación de la imagen

Universidad Francisco de Vitoria UFV Madrid

- 2) El equipo que estamos analizando está apagado
- Tenemos dos opciones: se puede realizar la imagen del disco sin desarmar el equipo, o extraer el disco duro.
- En el primer caso, debemos tomar todas las precauciones necesarias para que en ningún momento arranque el sistema que se encuentra instalado en el disco.

Preparación de la creación de la imagen

Universidad Francisco de Vitoria UFV Madrid

- Para ello, podemos utilizar como antes alguna de varias distribuciones de Linux en su versión Live (como Kali o ForLex), que cuentan con diversas aplicaciones forenses ya instaladas y listas para ser usadas.
- Además, los discos son montados en modo de sólo lectura (opción ro en /etc/fstab), y cualquier medio extraíble que sea insertado, no se montará automáticamente (opción auto en /etc/fstab).

Preparación de la creación de la imagen

Universidad Francisco de Vitoria UFV Madrid

- En el caso de que decidamos extraer físicamente el disco del equipo en el que se encuentra, podemos realizar la imagen conectando el disco a otro equipo nuestro, o a dispositivos como duplicadores forenses, que realizan el proceso a una alta velocidad.

Preparación de la creación de la imagen

Universidad Francisco de Vitoria UFV Madrid

- Si utilizamos un equipo externo, deberemos conectar el disco a adquirir, y la imagen podrá ser almacenada en el disco local o en otro disco cifrado, por ejemplo.

Preparación de la creación de la imagen

Universidad Francisco de Vitoria UFV Madrid

Preparación de la creación de la imagen

Universidad Francisco de Vitoria UFV Madrid

- Hay varias aplicaciones que cifran discos duros como TrueCrypt o VeraCrypt (https://linuxconfig.org/how-to-install-veracrypt-on-kali-Linux).
- El propio Windows lo hace siempre y cuando la partición esté formateada con NTFS