MÓDULO 1
TEMA 11: PROCEDIEMIENTO DE CLONADO

PROCEDIMIENTO DE CLONADO

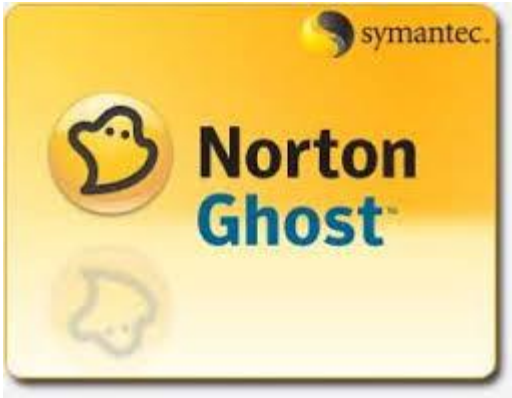
El clonado forense de discos duros se realiza a fin de **certificar y mantener la cadena de custodia de las evidencias digitales** contenidas en el dispositivo.

La **clonación forense** de los **discos duros** consiste en copiar todo el contenido de un **disco duro**, bit a bit, en otro dispositivo de almacenamiento o fichero de imagen obteniendo la firma hash de los bits leídos durante el proceso.

PROCEDIMIENTO DE CLONADO

Una de las labores en la informática forense que tenemos que realizar de acuerdo a las fases es hacer una copia de seguridad de la evidencia para eso existen herramientas software y hardware en el mercado de que nos ayudan con esta labor.

fillezilla



PROCEDIMIENTO DE CLONADO

En la parte Hardware un dispositivo que nos puede ayudar mucho es la duplicadora de discos , aunque un inconveniente es que tenemos que desmontar la unidad de disco para hacer la operación de duplicado , algunas de sus características son:

Skip Error: Al utilizar nuestro anterior producto, si hay un error de sector en el disco, se debe detener la copia. Sin embargo, este producto en el momento de ocurrido el error, se saltará en un punto de error y continuar copiando.

PROCEDIMIENTO DE CLONADO

Pantalla LCD: Como está equipado con pantalla LCD, puede confirmar la situación de funcionamiento de un vistazo. La conveniencia de la operación es el mejor nivel!

Interfaz SATA amigable : Dos conectores S-ATA se construyen en el cuerpo principal en ambos lados Aplicaciones clave (como un conector HDD externo)

PROCEDIMIENTO DE CLONADO

comparación y **comprobación de disco:** Capacidad Comparativa rápida para identificar las diferencias entre los dos discos duros conectados. y verificar fácilmente dos unidades de disco duro una vez al mismo tiempo.

Capacidad de combinación: Dos discos duros pueden ser utilizados como una gran unidad de disco duro de alta capacidad, Escribe en los datos en ambos discos duros de una vez al mismo tiempo para fines de respaldo.(Esto no es RAID)

PROCEDIMIENTO DE CLONADO

PROCEDIMIENTO DE CLONADO

El primer problema al que deberá enfrentarse un informático forense, una vez realizado el clonado, es el del cálculo de estas funciones. Ejemplo práctico: Un forense se ha desplazado a un despacho Notarial (con todos sus accesorios), para efectuar un clonado de un disco duro. Después tendrá que efectuar la práctica forense, una vez recolectada la evidencia. Lo primero que tiene que hacer es preservar el original, no contaminarlo

PROCEDIMIENTO DE CLONADO

Por lo general un perito informático dispone de una máquina clonadora por hardware, que permite la copia bit a bit de los dispositivos, sin necesidad de conectarlos a un equipo informático. Cuando se hace una copia “bit a bit”, mediante una clonadora de hardware, se garantiza la autenticidad y exactitud de la misma, pero si se quiere calcular el HASH (existen algunas clonadoras -generalmente caras-, que permiten calcularlo).

PROCEDIMIENTO DE CLONADO

Bloquear escritura de los dispositivos conectados a USB en Windows 7 Para poder bloquear estos puertos contra escritura será preciso entrar en el archivo de registro, con la utilidad “RegEdit”, antes de conectar los discos duros sobre los que hay que calcular el Hash. Ya en el regedit, navegamos hasta llegar a la clave

PROCEDIMIENTO DE CLONADO

Qué es la creación de imágenes forenses:

Las imágenes se obtienen mediante un método que no altera, en ninguna manera, dato alguno del disco que está siendo duplicado.

- El duplicado debe contener una copia de cada bit, byte, y sector del disco original.
- El duplicado no contendrá ningún dato distinto a caracteres de relleno (para designar áreas dañadas del medio), además de los datos copiados del disco original.
- Preciso, verificable, reproducible.

BLOQUEADORES FÍSICOS DE ESCRITURA

Qué son? –

- ✓ Dispositivos físicos que impiden la escritura al disco analizado como prueba.
- ✓ Constituyen el MEJOR método de creación de imágenes

EN QUÉ SITUACIONES NOS PODRÍAMOS ENCONTRAR?

- Situación 1: Podemos realizar la adquisición en frío, apagando la máquina usando un duplicador de disco hardware
- Situación 3: Por criticidad de la máquina afectada, la adquisición se tendrá que realizar en caliente, es decir, sin apagar la máquina
- Situación 2: Podemos realizar la adquisición en frío, apagando la máquina usando un LiveCD

SITUACIÒN 1

Personalmente, la situación 1, en la que se puede apagar la máquina y es posible el desensamblaje de los discos duros para copiarlos mediante un dispositivo de hardware, es la más limpia y profesional de todas, siendo la forma en que menos contaminaríamos la evidencia.

A pesar que la situación 1 es la recomendada, la adquisición mediante software es igualmente correcta y aceptada en litigios dónde se presenta la prueba como evidencia electrónica. Por ello, en éste post nos basaremos en analizar en detalle la situación 2 y 3. Veamos.

SITUACIÒN 2

En este caso, nos encontraríamos ante una máquina que sí puede ser apagada y reiniciada mediante un Live CD, como por ejemplo **ad-quiere** , mediante el cual podemos hacer uso de la utilidad DD. En esta situación disponemos de dos alternativas para realizar la adquisición, como son:

1.Por rojo

1.Mediante dispositivo de almacenamiento externo

SITUACIÒN 2

Dichas alternativas quedan ilustradas en las siguientes figuras mediante un ejemplo de prueba de concepto:

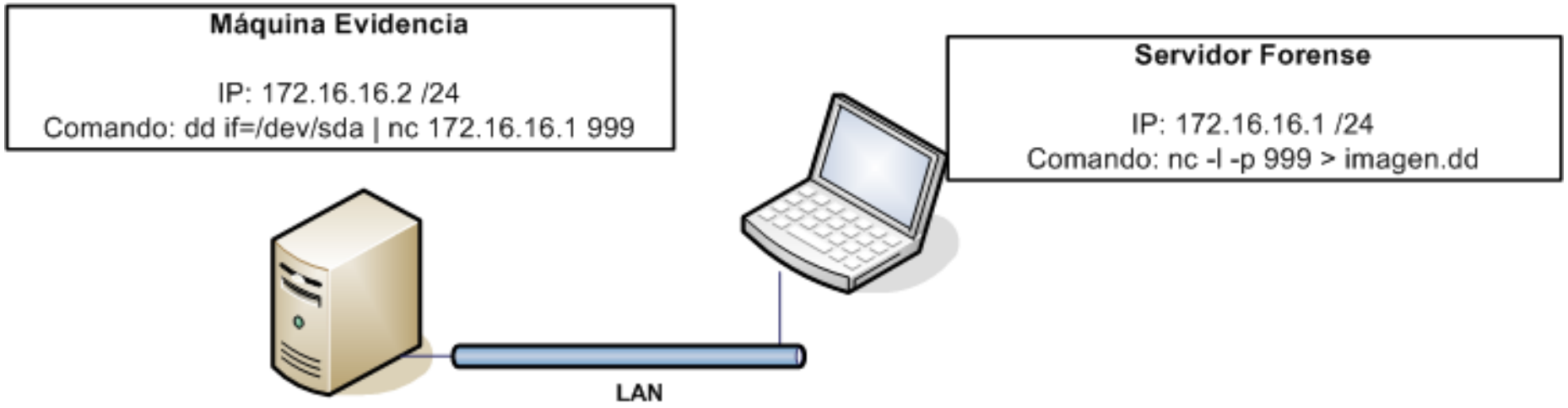


Figura 1. Adquisición del disco en un entorno Windows con un medio de almacenamiento a través de red, enviando los datos desde la Máquina Evidencia hacia la máquina Servidor Forense.

SITUACIÒN 2

Dichas alternativas quedan ilustradas en las siguientes figuras mediante un ejemplo de prueba de concepto:

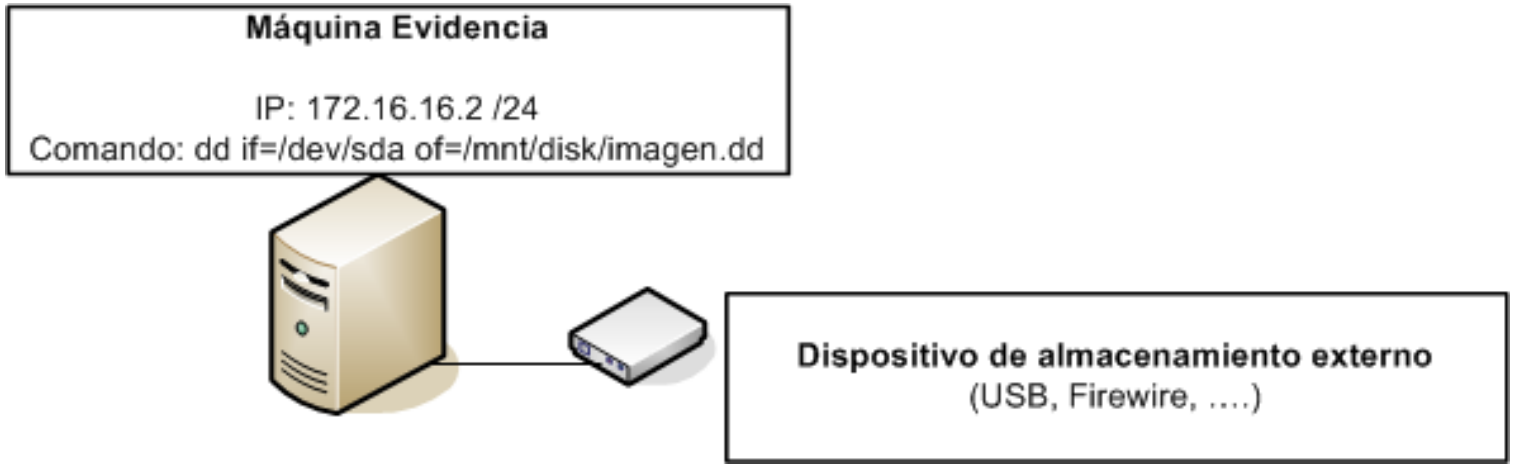


Figura 2. Adquisición mediante un dispositivo de almacenamiento externo conectado directamente en la Máquina Evidencia.

SITUACIÒN 3

Nos podemos encontrar un caso en que debamos realizar una adquisición forense en una máquina (típicamente un servidor corporativo) tan crítica que no pueda ser apagada de ninguna manera. De modo que nuestro modo de operación deberá ser:

- ✓ Insertaremos un CD Rom de herramientas de adquisición en la unidad (siendo esta la manera menos intrusiva).

- ✓ El CD Rom deberá contener todas las herramientas y librerías que vayamos a necesitar para realizar la adquisición. De esta manera, no ejecutaremos ningún tipo de comando del sistema.

SITUACIÒN 3

- ✓ Mediante las herramientas disponibles en el CD, si procede, vamos a obtener información volátil y por orden de volatilidad como son procesos, memoria, estado de red, etc.

Realizaremos la copia del disco duro evidencia mediante DD

En este caso, la sintaxis de ejecución de comandos no variará, salvo que debemos asegurarnos, para no afectar a la evidencia, que estamos ejecutando las herramientas del CD Rom y no las nativas del sistema. Véanse las siguientes imágenes como ejemplo de cómo ejecutaríamos los comandos en entornos Windows y UNIX:

SITUACIÒN 3

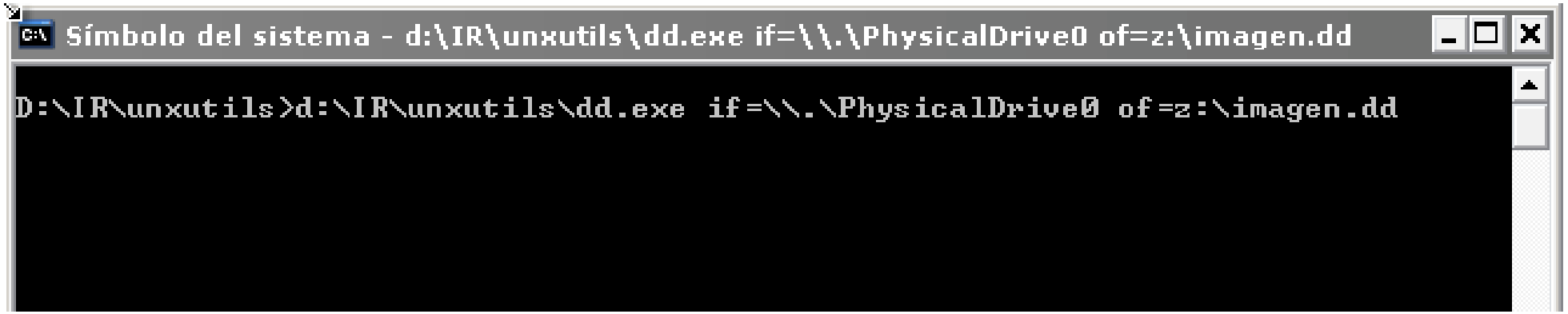


Figura 3. Adquisición del disco en un entorno Windows con un medio de almacenamiento externo

SITUACIÒN 3

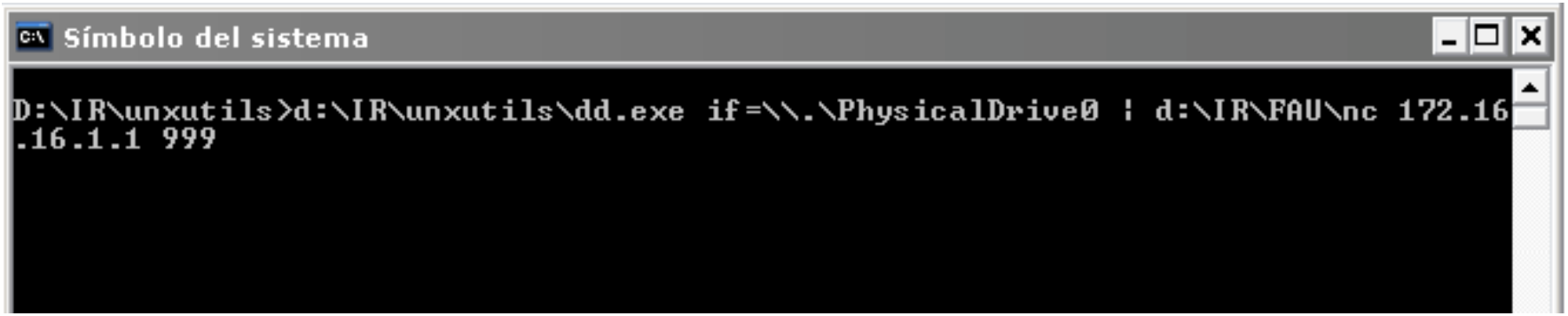


Figura 4. Adquisición del disco en un entorno Windows con un medio de almacenamiento a través de red utilizando Netcat

SITUACIÒN 3

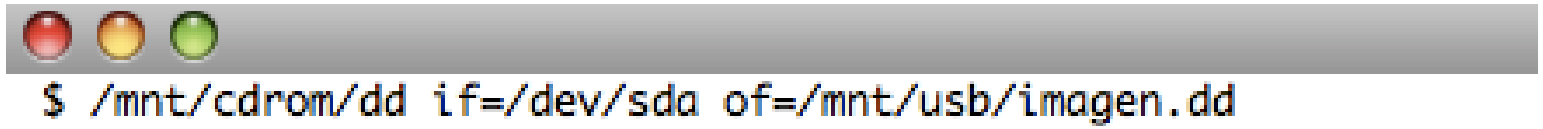


figura 5. Adquisición del disco en un entorno UNIX con un medio de almacenamiento externo

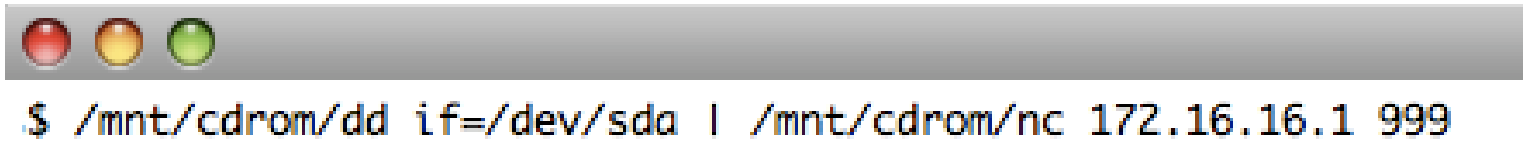


Figura 6. Adquisición del disco en un entorno UNIX con un medio de almacenamiento a través de red utilizando Netcat