

¿QUÉ ES HELIX?

Ing. Gustavo Presman, EnCE - CCE

gustavo@presman.com.ar

Preparado especialmente para la comunidad de [Segu-Info](#)

Hace pocas semanas se liberó la nueva versión de este Live CD: [Helix 3 2.0](#), clásico de la comunidad forense informática. En esta nota explico que es Helix y por qué se encuentra tan bien posicionado entre los peritos e investigadores forenses informáticos de todo el mundo.

Helix 3, tal su nombre (y no la versión) del producto, hace referencia a que el mismo cubre los tres flancos de la investigación informática: Descubrimiento electrónico, respuesta a Incidentes e Informática forense.

Ha sido desarrollado por la empresa e-fense y desde su sitio web se puede descargar el producto, el manual del mismo y acceder a los foros de intercambio: <http://www.e-fense.com/helix/>

Helix es de distribución gratuita aunque pueden adquirirlo en un CD estampado, con el manual impreso y una remera alusiva en el mismo sitio. El contrato de adhesión señala expresamente que no puede ser vendido.

Entre las principales características de Helix que lo han hecho muy popular en el ambiente forense informático sobresalen dos:

- Helix es una distribución de Linux “Forense”, es decir que al ser cargado en una computadora, garantiza la no escritura en ninguno de los medios magnéticos de manera automática.
- Helix viene precargado con gran cantidad de utilidades para la adquisición y el análisis de evidencia en el ambiente nativo de Linux, tanto como para Windows.

La utilidad principal de análisis forense incluida en Helix es Autopsy, la interfase gráfica (browser) que facilita el uso de TSK (The Sleuth Kit) una suite de línea de comando muy conocida en el ambiente.

Personalmente creo que a pesar de las limitaciones del Autopsy frente a otros toolkits forenses comerciales y a lo cuestionado que el mismo resulta en cortes de todo el mundo, es una excelente herramienta para entrenamiento en procedimientos forenses informáticos y para la ejecución de las pruebas de concepto que un investigador forense informático debe realizar dentro de las reglas de mejores prácticas a fin de validar los procedimientos y las herramientas por las utilizadas.

¿Qué trae esta nueva versión?

La versión liberada el 15 septiembre de 2008 es la Helix 2008R1 (2.0) y su característica distintiva respecto de la versión anterior (1.9) es que ha dejado de basarse en la distribución Knoppix para pasar ahora a la distribución Ubuntu en la versión 2.0, esto permite utilizar Helix en computadoras Macintosh basadas en procesadores PPC, lo cual no era posible en Helix 1.9.

Entre las principales utilidades incluidas en el “lado Linux”, todas ellas con licencia de uso gratuito, se destacan:

- **autopsy**: Interfase gráfica pa utilizar TSK
- **foremost** :Utilidad para “ data carving” que permite hacer búsquedas por firmas
- **Linen** : Permite la adquisición de evidencia en formato Encase
- **aimage** : Utilidad para hacer imágenes forenses
- **md5deep** : Calculador de Hashes MD5, SHA-1, SHA-256, Tiger y Whirlpool
- **readpst** : Conversor de archivos pst a mbox
- **Vinetto** : Para analizar archivos Thumbs .db
- **dc3dd** : Versión modificada del dd para uso forense
- **gkhash** : Utilidad para hacer análisis de Hashes

Helix también puede utilizarse bajo sistemas operativos Windows y al acceder al “lado Windows” las principales herramientas, cuyo nombre describe su uso, son:

- **FTK Imager** : Herramienta para adquisición y conversión de archivos de evidencia
- **Lists USB Devices**
- **Remote Desktop Password Recovery**
- **Outlook PST Password Recovery**
- **Mail Password Recovery**
- **IE History View**
- **IE Cookies View**
- **IE Cache View**
- **WirelessKeyView**
- **Winen RAM imager**

Obtención de Imágenes forenses empleando Helix

Frecuentemente el investigador forense informático deberá arrancar el sistema a analizar con Helix a fin de realizar una imagen forense de alguno de los medios contenidos en ese sistema, para ello desde la consola de administrador se utilizarán los comandos necesarios para montar el disco de destino que es aquel donde la imagen forense será depositada. Aquí **se debe prestar especial atención de no cometer ningún error** sobre el disco origen, es decir aquel del que queremos obtener la evidencia, evitando aplicar cualquier comando que pudiera escribir sobre el mismo, de manera de no alterar su contenido y evitar una posterior discusión judicial sobre la validez de la evidencia aportada.

Para ayudar en la sintaxis de los comandos más frecuentes para la preparación de los medios magnéticos, previo a la adquisición de la imagen forense, he preparado una guía que contiene la sintaxis Linux de las tareas más frecuentes en la preparación de los medios, para la utilización de **dd**, **adepto**, **linen** o la herramienta de adquisición forense de su preferencia entre las numerosas con que cuenta Helix.

TAREAS BÁSICAS PREVIAS A LA ADQUISICIÓN DE EVIDENCIA EN LINUX

Ing. Gustavo Presman, EnCE - CCE

gustavo@presman.com.ar

Preparado especialmente para la comunidad de [Segu-Info](#)

*Todos los comandos se refieren **hdx**, pero deberá se utilizar **sdx** para unidades SCSI, SATA ó Externas USB/FW.*

Ver tabla de partición

`fdisk -l`

Calcular el Hash

`md5sum /dev/hdx` Del disco

`md5sum /mnt/destino/archivo` Del archivo de evidencia

Uso del DMA en los discos

`hdparm -d1 /dev/hdx` Activa el DMA

`hdparm -d0 /dev/hdx` Desactiva el DMA

Hacer un wipe del disco

PRESTAR ATENCION AL DISCO DESTINO DE ESTE COMANDO

`time dd if=/dev/zero of=/dev/hdx bs=64k` Con `dd`

`time dcfldd pattern=00 of=/dev/hdx bs=64k` Con `dcfldd`

`time` : indicará la duración estimada de la operación

`if` : archivo de entrada

`of` : archivo salida

`bs`: tamaño del bloque

`pattern`: patrón a grabar

Particionar un disco

ESTA ES UNA UTILIDAD DE MENU

Pasos a seguir :

`fdisk /dev/hdx`

`m [help]`

`n [new partition]`

`p [primary]`

`1 [1-4]`

`1st cylinder [enter]`

`Last Cylinder [enter]`

`t [change partition]`

`1 [1-4]`

c [fat32 LBA]

w [write partition section out]

Particionar un disco

mkdosfs -F 32 -n Evidencia /dev/hdxy

F 32: Instala File System FAT32

n : nombre del volumen

hdxy : unidad lógica a formatear (p/ej hdb2)

Crear un punto de montaje

mkdir /destino

destino: nombre de la carpeta

Montar un volumen

mount /dev/hdxy /destino Si el volumen es FAT

mount /dev/hdxy /destino -t ntfs-3g Si el volumen es NTFS