

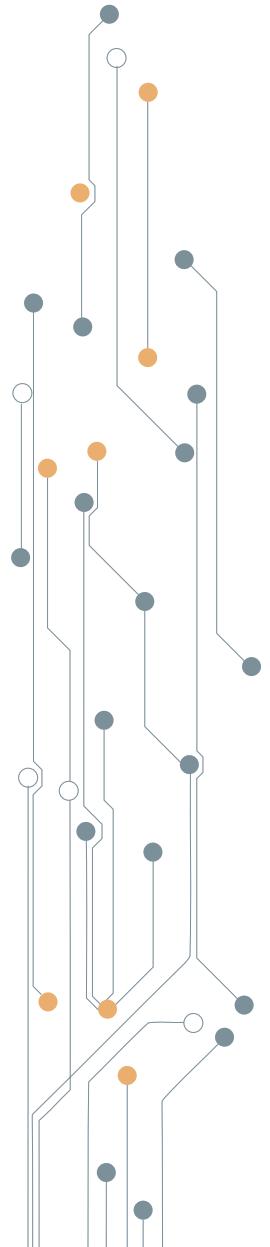


Adquisición de evidencias.  
Clonación. Integridad

Telefónica

EDUCACIÓN DIGITAL

# Índice



- 1 | Metodología básica
- 1.1 | Diferencias entre Live Response Acquisition y Traditional Acquisition
- 2 | Traditional Acquisition
- 3 | Live Response Acquisition
- 4 | Adquisición en entorno Windows

3  
6  
8  
11  
14

# 1. Metodología básica

Hay dos preguntas que todo investigador debe hacerse: realizar el análisis en un equipo apagado (*Traditional Acquisition*) o realizar el análisis en vivo con el equipo en funcionamiento (*Live Response Acquisition*). En ambos casos se seguiría una metodología básica, consistente en:

- Adquirir la evidencia sin alterar o dañar el original.
- Autenticar que la evidencia recuperada es la misma que la que se obtuvo del original.
- Analizar los datos sin modificarlos.

La práctica forense actual más utilizada es realizar la adquisición en una máquina apagada para obtener una imagen del disco duro (*Traditional Acquisition*). Esta técnica puede dañar o alterar datos, así como que el sistema esté un tiempo inactivo y consecuentemente pérdida de ingresos para las empresas. Una técnica más reciente, la adquisición forense en vivo (*Live Response Acquisition*), surgió para limitar algunos de los problemas causados por la adquisición

forense de sistemas apagados. Esta técnica permite realizar una imagen intacta de una máquina en vivo, es decir, una máquina que está funcionando obteniendo información de la memoria RAM o de la red del sistema.

Los investigadores no siempre pueden realizar el análisis forense en un sistema apagado con éxito en el que obtener suficientes pruebas, por lo que se desarrollan técnicas de adquisición forense en vivo, como la adquisición de la memoria RAM, del sistema de red, etc.

A pesar de las numerosas ventajas de la adquisición forense en vivo, da lugar a nuevas dificultades técnicas y legales en la que hay que convencer al tribunal de que la imagen adquirida forense es una copia exacta sin cambios de la original. Obligatorio si el método de adquisición es el tradicional, pero más complicado probar en la adquisición forense en vivo. En la actualidad, no existe un método aceptado de hacer adquisiciones en vivo y la investigación tradicional es necesaria.



Dependiendo del modo de adquisición, el acceso al dispositivo en el que obtener las evidencias puede ser:

- Apagar el equipo mediante el botón de alimentación (*Traditional Acquisition*).
- Apagar el equipo siguiendo el procedimiento de apagado normal (*Traditional Acquisition*).
- Mantener el sistema en funcionamiento (*Live Response Acquisition*).

Independientemente del método de adquisición que se utilice, lo primero que se debe realizar es aislar tanto el sistema como los datos relevantes para prevenir la alteración de otros sistemas, lo que reduce el riesgo de un fallo en cascada de la organización, y la congelación del estado del sistema afectado, conservando una imagen exacta.

Se debe recopilar información entrevistando a los administradores de sistemas y otros usuarios que hayan tenido contacto con el sistema afectado, aunque no siempre es posible, debido a que puede ser una investigación encubierta, planeada y ejecutada para ocultar la identidad de su autor. Hay que tratar de reunir toda la información sobre el sistema antes de iniciar el proceso de adquisición, como contraseñas, ya que puede ahorrar tiempo y esfuerzo.

Una vez que el sistema está completamente aislado, se debe recoger toda la información posible no técnica, como horarios de los usuarios que acceden al sistema, con lo que se puede crear una línea de tiempo que nos lleven a la sospecha del delito cometido.

Durante la adquisición y análisis forense, es posible escribir en la unidad con la evidencia accidentalmente. Dado que esto daría lugar a la no admisión de las pruebas en un juicio, el investigador debe tener cuidado de no poner en peligro la evidencia. La forma más fácil de asegurar es usar un bloqueador de escritura.



Un bloqueador de escritura permite a un sistema leer datos de un disco duro externo al mismo tiempo que evita que cualquier comando de escritura realice una modificación no autorizada o formatee la unidad. Con este bloqueador se evita escribir a través de la interfaz del disco duro.

Hay dos tipos de bloqueadores de escritura:

- Por software, el cuál sustituye a una interfaz de acceso al disco duro en un equipo con discos duros externos y bloquea cualquier comando que podría modificar un disco duro.
- Por hardware, es un dispositivo de hardware que se conecta físicamente al sistema informático. Su principal objetivo es interceptar y bloquear cualquier comando de modificación antes de alcanzar el dispositivo de almacenamiento.

Como comentábamos anteriormente, es muy importante para preservar las evidencias crear copias a los efectos de análisis.

Después de la adquisición física es necesario documentar el incidente y todas las acciones llevadas a cabo por los investigadores mediante la cadena de custodia.

A lo largo de proceso, las evidencias y los dispositivos adquiridos deben tenerse documentados. La cadena de custodia comienza en el momento en que el investigador forense entra en la escena del crimen, y continúa hasta el juicio, si lo hay, dando validez y solidez de las evidencias forenses del caso.

Una posible definición sería "*Una cadena de custodia es el proceso de validación de cómo cualquier tipo de evidencia ha sido recogida, seguida y protegida en su camino a un juicio*". Básicamente es tener todo documentado y bien identificado para, en el caso de que haya una modificación pueda ser identificada en tiempo y formas.

La evidencia tiene que ser transportada desde la escena del crimen al laboratorio forense para completar el proceso de adquisición. En el laboratorio, las pruebas deben de almacenarse de forma segura.

Hay que tomar ciertas precauciones para asegurarse de que la evidencia llega sin ningún daño o alteración. Utilizando envases sin electricidad estática donde introducir las evidencias, el último investigador debe sellar el paquete y firmar el sello. Si alguien no autorizado intenta abrir el paquete, el sello se rompería y se estropearía la firma, invalidando la prueba. Cada vez que alguien necesite acceder a los datos, el paquete debe ser puesto en un nuevo paquete, y el nuevo paquete debe ser sellado y firmado. Algunos casos judiciales se posponen, inevitablemente, varias veces, y pueden extenderse varios años. Por lo que se hace necesario controlar el deterioro de las evidencias.



## 1.1 | Diferencias entre Live Response Acquisition y Traditional Acquisition

A continuación, comentamos algunas de las diferencias y ventajas entre la adquisición en vivo (*Live Response Acquisition*) y la adquisición de un sistema apagado (*Traditional Acquisition*).

La probabilidad de que los investigadores modifiquen los datos de una evidencia es muy grande. Se deben tomar suficientes precauciones para asegurarse de que el ordenador no permita ninguna modificación durante el proceso de copia, del original o la imagen copiada, del disco duro original.

Una característica que distingue entre la adquisición forense de un sistema en vivo o apagado es que en un sistema apagado no se pueden adquirir los datos volátiles. Una vez que el sistema está apagado, la máquina pierde toda la información de la memoria volátil de la memoria RAM.

Hay una serie de limitaciones y problemas asociados en la adquisición de un sistema apagado (*Traditional Acquisition*) como vemos a continuación:

- Uso cada vez más frecuente de la criptografía. Aunque se tenga la imagen completa bit a bit, en crudo o raw, del disco duro del sistema sospechoso, ésta puede estar cifrada y sin ningún valor práctico, ya que la unidad sólo puede ser descifrada con una contraseña única. El cifrado de todo el disco no se limita únicamente a los criminales, ya que también es una técnica utilizada en algunos sistemas operativos.

- Adquisición de los datos de red, como puertos, conexiones establecidas, ... Este tipo de información es volátil y se pierde en el caso de que se desconecte el ordenador.
- Todos los datos deben ser recogidos y examinados como evidencias. Sin embargo, actualmente se dispone de sistemas con grandes capacidades de almacenamiento por lo que esa cantidad de información debe ser analizada, requiriendo mucho tiempo. Los archivos de registro también tienden a aumentar de tamaño y dimensión, lo que complica la investigación.
- Falta de procedimientos estandarizados en los que se recopilan datos sin valor que consumen un tiempo innecesario.
- Muchas restricciones prácticas (equipos en empresas en las que no se puede disponer exclusivamente de los equipos por estar en uso constantemente) y legales (restricción de los métodos en los que los investigadores forenses pueden obtener los datos).
- Es importante que los investigadores estén equipados con herramientas y mecanismos validados que puedan realizar la adquisición correcta y validada para que los datos obtenidos se puedan ver como evidencia y admisibles en un juicio.
- El análisis de un sistema apagado no es el método indicado para la adquisición de datos volátiles como la memoria RAM.

Debido a todo esto, la adquisición forense en vivo puede ser una alternativa mejor ya que permite acceder a una variedad de información de gran valor que se habría perdido en el análisis forense tradicional. Sin embargo, en la práctica trae consigo sus propias limitaciones, especialmente con respecto a las implicaciones legales.

El análisis en vivo (*Live Response Acquisition*) permite a los investigadores forenses recuperar información volátil específica de la configuración de red del sistema sospechoso, así como la memoria RAM. Esta información puede ser muy valiosa para la persecución de un delincuente.

Por lo tanto, es posible ver el desarrollo del análisis de la adquisición en vivo como una mejora frente a los métodos tradicionales o de un sistema apagado.

Un apunte es que la adquisición forense en vivo limita la cantidad de datos recogidos. A menudo, los investigadores analizan grandes partes del sistema, pero sólo se almacenan los elementos relevantes o principales.

Aunque la adquisición en vivo aborda la mayoría de los problemas asociados con la adquisición tradicional, provoca problemas adicionales:

- Variedad en la configuración de equipos. Aunque hay muchos componentes y aspectos comunes, se pueden compilar los sistemas de varias formas, por lo que el investigador forense debe asegurar que tiene un conocimiento suficiente de la amplia variedad de sistemas de hardware, software y sistemas operativos.

- La modificación de los datos durante el proceso de adquisición y la dependencia en el sistema operativo del sistema sospechoso son dos de las preocupaciones más importantes. Si se alteran los datos, los tribunales podrían rechazar las evidencias. Parte de la adquisición en vivo ejecuta código en la CPU del sistema sospechoso. Esto puede alterar los datos en los registros de la CPU, la memoria RAM o el disco duro.
- La modificación más pequeña de una imagen puede causar un problema. Del mismo modo, la memoria volátil no representa un único punto en el tiempo, sino más bien un vistazo de un momento. Cuando se adquieren datos volátiles, los investigadores no siempre pueden utilizar bloqueadores de escritura, ni existe siempre una comparación hash de los datos originales.
- Otro problema en la obtención de evidencias de red en redes no seguras, es la autenticidad y fiabilidad. Los kits de herramientas anti-forenses también están ampliamente disponibles, y pueden obstruir la obtención de pruebas a partir de fuentes de red en vivo. Es posible escribir un programa que destruya la evidencia cuando el sistema operativo detecte un programa de adquisición forense. Este tipo de programas son desarrollados por individuos u organizaciones que quieren entorpecer las investigaciones forenses, y su objetivo es eliminar todas las evidencias incriminatorias en el sistema de la víctima. Algunos de estos programas son Evidence Eliminator, The Defiler's Toolkit, Diskzapper, CryptoMite, Tracks Eraser Pro e Invisible Secrets. Las herramientas anti-forenses trabajan en una variedad de plataformas, y realizan una serie de funciones diferentes.
- En algunos casos se recopilan una cantidad limitada de información. Esto no siempre puede constituir una representación completa del sistema afectado original, y puede ser interpretado como una posible alteración de los datos.

## 2. Traditional Acquisition

El análisis de adquisición de un sistema apagado, a menudo se denomina método digital tradicional o Traditional Acquisition. La adquisición en un sistema apagado implica quitar la corriente eléctrica en un sistema sospechoso, evitando que cualquier proceso malicioso se ejecute en el sistema y elimine datos del sistema. Se crea una instantánea de los archivos swap y más información del sistema tal y como se encontraba por última vez.

Una definición formal es "*el análisis realizado en un ordenador apagado*". Por lo general, hay cuatro etapas en el análisis tradicional:

- La recolección de evidencias se realiza en el lugar del incidente y se basa en la búsqueda y adquisición de información de una manera válida a efectos legales. Las principales acciones son la duplicación de discos forense y la recogida de pruebas al azar, tales como CDs, entrevistas personales, ...

- El examen se basa en una investigación automática y manual de los datos adquiridos. Esta etapa tiene como objetivo identificar y extraer los datos pertinentes al caso específico, e incluye el análisis del sistema de archivos y la extracción de las evidencias.
- El análisis es el proceso de utilización de los datos, identificados de alguna manera, para demostrar las acciones realizadas en el equipo por uno o más individuos. Esta etapa consiste en la navegación, la consulta y la correlación de datos existentes.
- La notificación es la última etapa en la que se informa de la información recopilada de una forma escrita mediante los informes técnicos y ejecutivos.

En el proceso de copia forense, con la suficiente formación y el software forense adecuado, los investigadores pueden copiar la imagen del disco duro, con los sectores no asignados, el espacio slack, perdido o desperdiciado, y los metadatos de los archivos. Esto se hace generalmente mediante la copia del disco duro bit a bit o en crudo o raw.



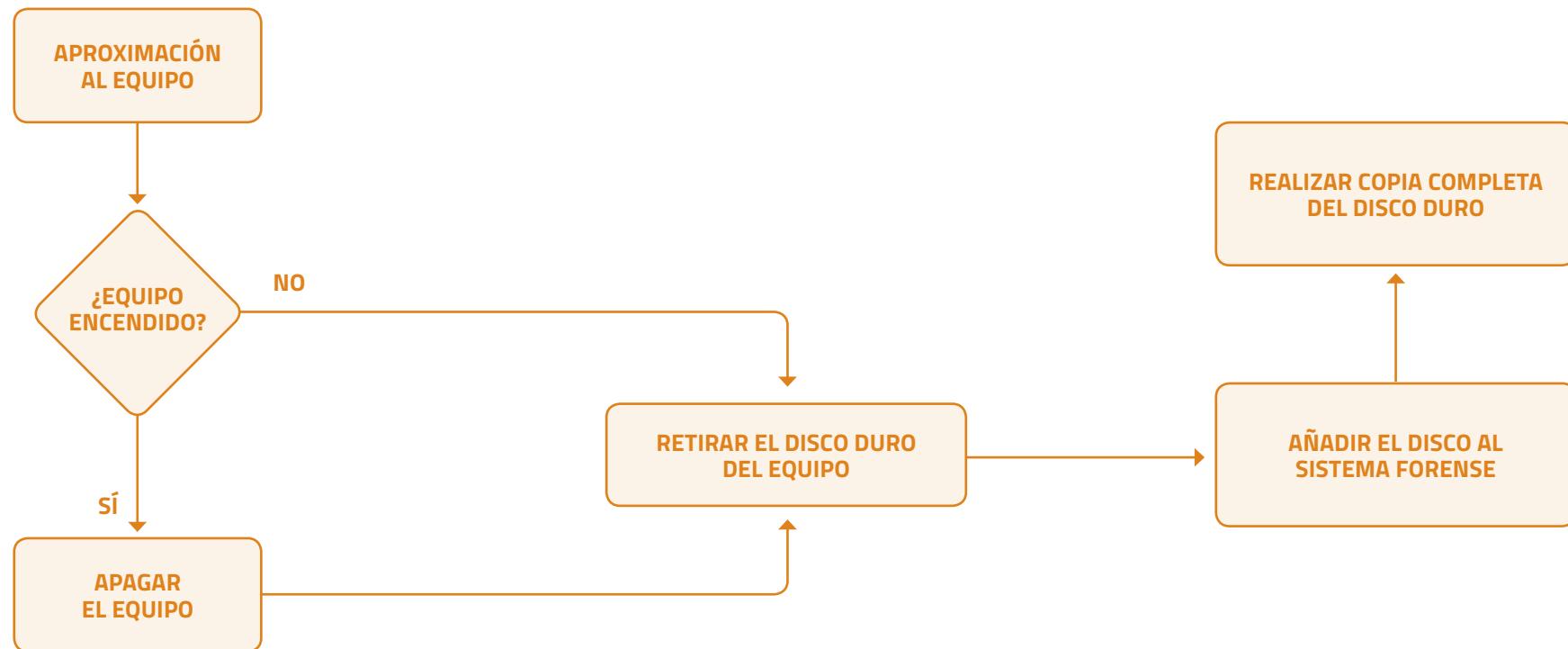


Imagen 2 Esquema Traditional Response Acquisition

El esquema anterior ilustra el proceso forense. El investigador forense llega por primera vez al equipo y determina si está encendido o apagado. Si el ordenador está encendido, se puede realizar el apagado abrupto o el procedimiento habitual de apagado del sistema, pero la recomendación sería un apagado abrupto del mismo. Una vez que el equipo está apagado, el investigador retira físicamente el disco duro del sistema, lo añade como una unidad externa a un sistema forense y copia su contenido. El investigador

toma las precauciones necesarias para garantizar que no haya modificación de datos. Dependiendo de la situación específica, el investigador puede devolver el disco duro al sistema original, o meterla en una bolsa antiestática como evidencia.

Durante muchos años, la adquisición forense tradicional (*Traditional Acquisition*) ha sido el único medio para llevar a cabo adquisiciones forenses. Es un procedimiento sencillo de seguir.

## Ejemplo de adquisición física de una máquina apagada

A continuación, vamos a realizar un ejemplo de una posible adquisición física de un sistema comprometido mediante el método tradicional.

1. Si se encuentra apagada la máquina pasar al siguiente punto. Si se decide apagar la máquina, realizarlo de las dos maneras disponibles, o bien desconectando el cable de corriente o bien mediante el apagado normal del sistema.
2. Extraemos las unidades de las que realizar la imagen, en nuestro caso el disco duro.
3. Si se dispone de jumper en la unidad 'read-only' utilizarla o bien utilizar un bloqueador por hardware/software, para no modificar los datos que hay en la unidad en el original.
4. Conectarlo a la estación forense.
5. Previamente borrar a bajo nivel el disco que contendrá la imagen mediante 'dd'

```
dd if=/dev/zero of=/dev/sda
```

6. Realizar una copia bit a bit con 'dd' al disco externo limpio

```
dd if=/dev/sda of=/dev/sdb
```

7. Calcular los hashes del original y copia para garantizar su integridad y autenticidad.
8. En caso de disponer de clonadoras hardware, se evitaría el tener que realizar los pasos anteriores ya que realizan todo de una vez, bloqueando la escritura en el disco origen.

## Ejemplo de adquisición a través de la red de una máquina apagada

En este ejemplo realizaremos la adquisición de un disco a través de red. Para ello realizaremos los siguientes pasos:

1. Extraemos las unidades de las que realizar la imagen, en nuestro caso el disco duro, si es necesario.
2. Si se dispone de jumper en la unidad 'read-only' utilizarla o bien utilizar un bloqueador por hardware/software, para no modificar los datos que hay en la unidad en el original.
3. Mientras en la estación forense lanzar los comandos que nos permiten realizar la adquisición por red, en nuestro caso mediante netcat:

```
nc -l -p 5000 > disk1.dd
```

4. Iniciar la máquina a analizar con una distribución LiveCD de Linux (p.ej. Deft) y ejecutar los comandos que nos permiten enviar la copia bit a bit de la unidad por red al equipo forense:

```
dd if=/dev/sda | nc 192.168.0.1 5000
```

5. Calcular los hashes del original y copia para garantizar su integridad y autenticidad.

### 3. Live Response Acquisition

El método de adquisición forense en vivo (*Live Response Acquisition*) es similar al método de adquisición forense tradicional. Se desarrolló en respuesta a las deficiencias de las técnicas de adquisición forenses tradicionales, teniendo en cuenta la conservación de datos volátiles como la RAM o los datos de red, y una contramedida para los archivos cifrados que se pueden encontrar en un sistema encendido.

La filosofía es la misma, en la que ambos métodos necesitan asegurarse de que la imagen adquirida se mantenga sin cambios, sin alteraciones. La secuencia de pasos es la misma (recopilación, examen, análisis, informes). Los investigadores, sin embargo, deben adaptar el funcionamiento interno de las etapas para permitir la adquisición en vivo del sistema.

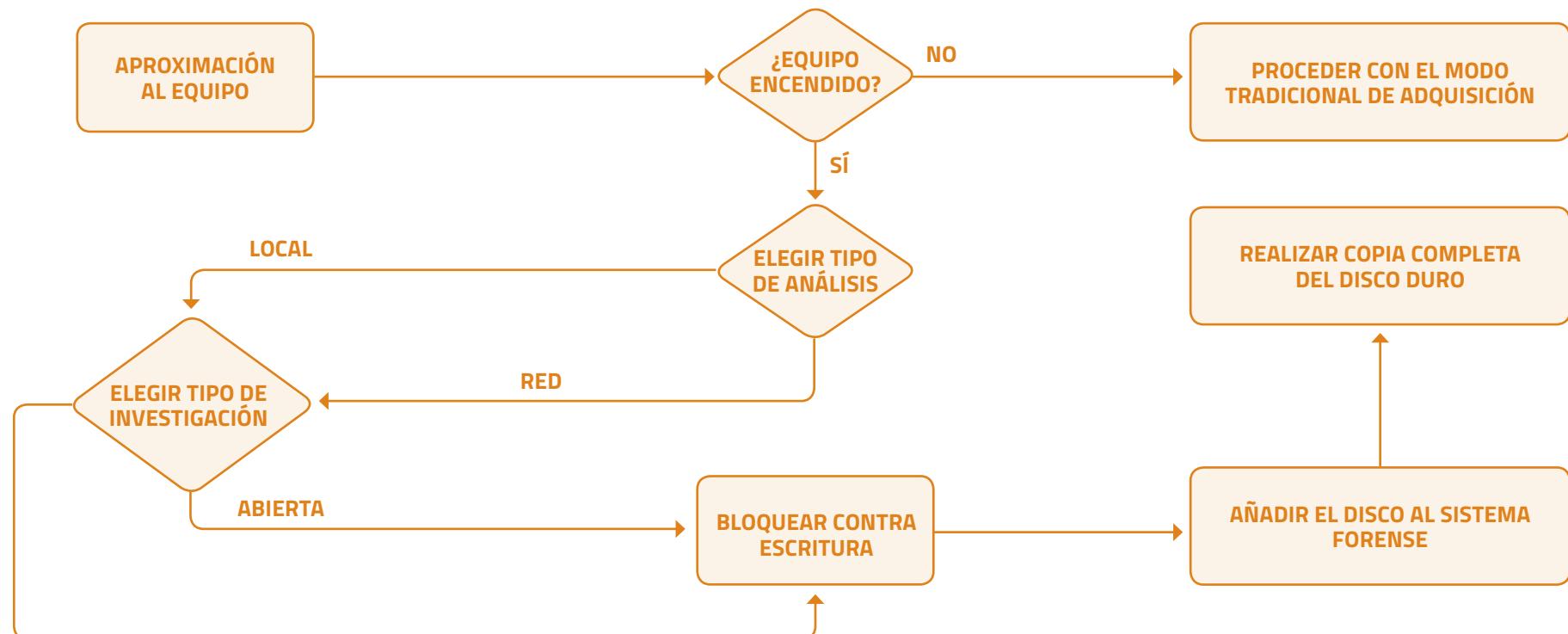


Imagen 3 Esquema Live Response Acquisition

El esquema anterior presenta las acciones del investigador forense durante la adquisición en vivo. El investigador forense llega por primera vez al equipo y determina si está encendido o apagado. Si el ordenador está apagado, continúa con el procedimiento de adquisición forense de un sistema apagado o tradicional. Si el ordenador está encendido, el investigador necesita primero seleccionar si los datos se copiarán a nivel local, o a través de la red. Además, tiene que decidir si la investigación se llevará a cabo de manera abierta o encubierta. A continuación, el investigador conecta un sistema bloqueador de escritura, ya sea por hardware o basado en software, tanto a la máquina sospechosa como a la unidad externa al sistema forense, para copiar el contenido de la máquina sospechosa. Por supuesto, una investigación forense en vivo es mucho más fácil si se ha iniciado la sesión en la cuenta que tiene derechos administrativos. Sin embargo, en caso de que la cuenta actual no tenga derechos administrativos, la funcionalidad del usuario con la que el investigador puede trabajar depende de los derechos asignados a la cuenta actual y el software instalado. Se pueden dar una gran cantidad de escenarios posibles.

Además, durante la investigación forense, es necesario determinar si la cuenta se encuentra en un entorno real o virtual. En esencia, los diferentes entornos requieren el mismo método de investigación. Sin embargo, si se ha iniciado la sesión de la cuenta en una máquina virtual, el investigador tiene que hacer un análisis más detallado para adquirir tanto la imagen del sistema de la máquina real, como la de las posibles máquinas virtuales ubicadas en la máquina real.

Puede ser difícil de detectar si el investigador forense accede a un entorno informático real, o una máquina virtual. Para ello existe una serie de técnicas que pueden indicar si un sistema es real o virtual, la técnica más sencilla es la búsqueda de:

- Notas de los derechos de autor o cadenas de los proveedores en varios archivos.
- Los controladores de hardware específicos de las máquinas virtuales.
- BIOS específica de las máquinas virtuales.
- Direcciones MAC específicas de las máquinas virtuales.
- Herramientas de las máquinas virtuales instaladas.
- La virtualización por hardware.

Estos indicios pueden ser más bien poco fiable ya que son fáciles de modificar. Un método de búsqueda más fiable es ver las características de hardware. En el caso de las máquinas virtuales de Microsoft, un claro indicador es que la placa está fabricada por "Microsoft Corporation". DEVCON, una versión de línea de comandos del Administrador de dispositivos, es útil en la detección del hardware que se encuentra en el sistema, identificando cualquier hardware de la máquina virtual, en algunos casos los discos IDE se denominan "HD virtual".

Una técnica más fiable es la instalación de detectores de máquinas virtuales teniendo en cuenta que este software puede tener un impacto negativo sobre la solidez de la evidencia forense. Algunas de estas herramientas son Red Pill, Jerry, ScoopyNG y VMware Virtual Machine Detector.

## Ejemplo de adquisición física de una máquina encendida

A continuación, vamos a realizar un ejemplo de una posible adquisición física de un sistema en vivo comprometido mediante el método tradicional.

1. Podríamos utilizar 'dd' para realizar una copia bit a bit, tanto para sistemas Windows como Unix/Linux.
2. Para Windows puede ser más cómodo usar frameworks como OSForensics / FTK Imager, EnCase,... ya que permiten realizar además la imagen de los elementos más volátiles, así como calcular hashes y con un montón de utilidades de análisis y gestión.
3. Calcular los hashes para garantizar su integridad y autenticidad.

## Ejemplo de adquisición a través de la red de una máquina encendida

A continuación, realizaremos la adquisición a través de la red de una máquina encendida. Como hemos visto anteriormente no es la opción más recomendable ya que el sistema operativo no es fiable y el sistema de ficheros no está en un estado 'estable'. Pero si no tenemos más remedio como comentamos en los puntos anteriores realizaremos los siguientes pasos:

1. En la estación forense lanzaremos los comandos que nos permiten realizar la adquisición por red, en nuestro caso mediante netcat:

```
nc -l -p 5000 > disk1.dd
```

2. En la máquina a analizar, ejecutar 'dd' desde un CD/USB limpio:

```
dd if=\\.\PhysicalDrive0 bs=2k | nc -w 3 192.168.0.1 5000
```

3. Para la captura de la memoria podríamos utilizar alguno de los métodos vistos en el ejemplo de adquisición física de una máquina encendida. Hay distribuciones que nos permiten enviar por red las capturas como Helix 3 (Live CD orientado al Incident Response)



Imagen 4 Helix 3 - Adquisición de memoria

4. Calcular los hashes del original y copia para garantizar su integridad y autenticidad.

## 4. Adquisición en entorno Windows

Los datos volátiles de Windows nos darán información acerca de los usuarios existentes, las conexiones establecidas, datos en memoria y servicios en marcha. Para recuperar esos datos volátiles es necesario utilizar herramientas especiales, ya sean herramientas nativas o no nativas del sistema operativo. La pérdida de este tipo de información podría complicar el proceso de análisis forense y por consiguiente la investigación llevada a cabo. Por lo que como indica el *RFC 3227*, se tienen que llevar a cabo la toma de evidencias de más volátil a menos volátil.

Se debe tener en cuenta varias cosas antes de empezar:

- Realizar varias copias de la información del disco para no trabajar nunca sobre la información original. Realizar varias copias es fundamental por si se nos daña una de las copias poder siempre volver a realizar una copia de la copia. Por ello se recomienda realizar 2 copias del disco original, primero una copia del disco original y después una copia de la copia.

- Almacenar en un lugar seguro y a salvo para no contaminar ni alterar la información y así guardar su integridad y autenticidad.
- Establecerse la cadena de custodia para el manejo de las evidencias.

Podemos utilizar las herramientas nativas del sistema operativo y comandos que nos darán información importante sobre la configuración y el estado del sistema como *ipconfig* y *route*. Además, también podemos utilizar las herramientas no nativas especializadas para el diagnóstico de sistemas Windows como la *Suite Sysinternals* de Microsoft.

Primeramente, vamos a obtener uno de los elementos volátiles más importantes como son las conexiones abiertas del sistema, ya que estas conexiones se pierden al apagar el equipo.

Herramientas nativas de Windows para visualizar las conexiones abiertas podemos utilizar *Netstat* (Puertos y conexiones abiertas), *Nbtstat* (Conexiones de NetBIOS), *Net* (Recursos compartidos), *Route* (Configuración de la red) e *Ipconfig* (Interfaces de red).



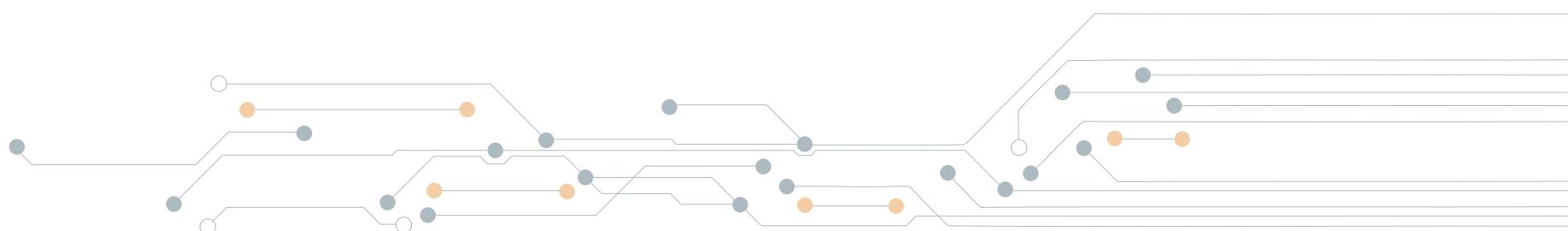
Para ello abrimos una consola de Windows mediante C:\Windows\System32\cmd.exe y lanzamos los siguientes comandos para ver:

- Puertos y conexiones abiertos: *netstat -a*

```
C:\Documents and Settings\admin>netstat -a
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    winxp-9d4ad0906:epmap  winxp-9d4ad0906:0      LISTENING
  TCP    winxp-9d4ad0906:microsoft-ds  winxp-9d4ad0906:0      LISTENING
  TCP    winxp-9d4ad0906:1028   winxp-9d4ad0906:0      LISTENING
  TCP    winxp-9d4ad0906:netbios-ssn  winxp-9d4ad0906:0      LISTENING
  UDP    winxp-9d4ad0906:microsoft-ds  *:*
  UDP    winxp-9d4ad0906:isakmp   *:*
  UDP    winxp-9d4ad0906:4500    *:*
  UDP    winxp-9d4ad0906:ntp     *:*
  UDP    winxp-9d4ad0906:1900    *:*
  UDP    winxp-9d4ad0906:ntp     *:*
  UDP    winxp-9d4ad0906:netbios-ns  *:*
  UDP    winxp-9d4ad0906:netbios-dgm  *:*
  UDP    winxp-9d4ad0906:1900    *:*
```

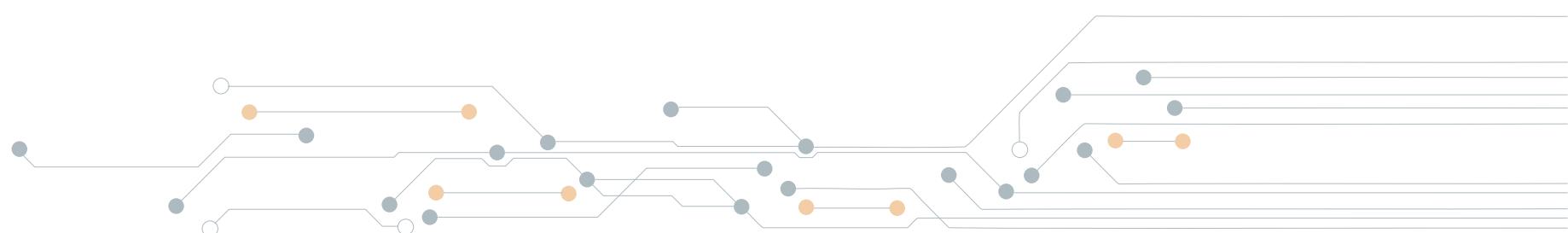
Imagen 5 Puertos y conexiones abiertos



- Tráfico por proceso: `netstat -b`

c:\Users\Raul>netstat -b			
Conexiones activas			
Proto	Dirección local	Dirección remota	Estado
TCP	127.0.0.1:443 [vmware-hostd.exe]	down:53208	ESTABLISHED
TCP	127.0.0.1:443 [vmware-hostd.exe]	down:64160	ESTABLISHED
TCP	127.0.0.1:5354 [mDNSResponder.exe]	down:49156	ESTABLISHED
TCP	127.0.0.1:5354 [mDNSResponder.exe]	down:49157	ESTABLISHED
TCP	127.0.0.1:49156 [AppleMobileDeviceService.exe]	down:5354	ESTABLISHED
TCP	127.0.0.1:49157 [AppleMobileDeviceService.exe]	down:5354	ESTABLISHED
TCP	127.0.0.1:52001 [BtvStack.exe]	down:55737	ESTABLISHED
TCP	127.0.0.1:52001 [BtvStack.exe]	down:55738	ESTABLISHED
TCP	127.0.0.1:52001 [BtvStack.exe]	down:55739	ESTABLISHED
TCP	127.0.0.1:52001 [BtvStack.exe]	down:55740	ESTABLISHED
TCP	127.0.0.1:53208 [vmware.exe]	down:https	ESTABLISHED
TCP	127.0.0.1:53209 [vmware.exe]	down:53210	ESTABLISHED
TCP	127.0.0.1:53210 [vmware.exe]	down:53209	ESTABLISHED

Imagen 6 Tráfico por proceso



- Estadísticas de conexiones: *netstat -es*

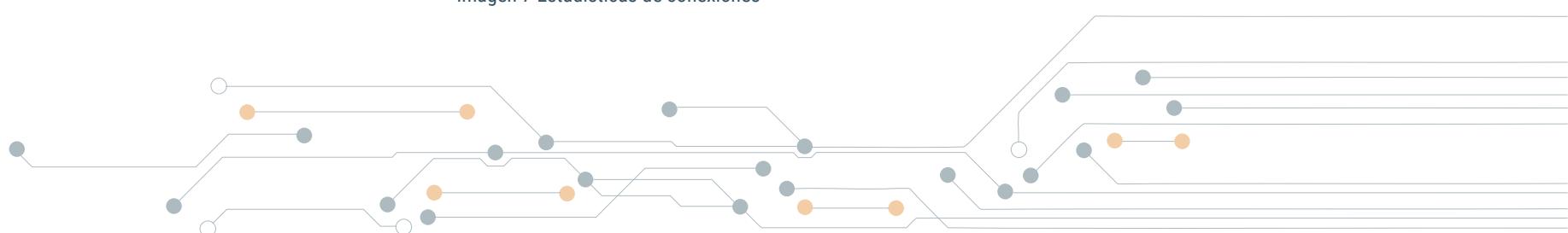
```
C:\Documents and Settings\admin>netstat -es
Interface Statistics

                                Received          Sent
Bytes                      1657787          8547
Unicast packets            20386           39
Non-unicast packets        46             37
Discards                   0              0
Errors                     0              0
Unknown protocols          0              0

IPv4 Statistics

Packets Received           = 20426
Received Header Errors     = 0
Received Address Errors    = 3
Datagrams Forwarded        = 0
Unknown Protocols Received = 0
Received Packets Discarded = 20387
Received Packets Delivered = 39
Output Requests             = 71
Routing Discards            = 0
Discarded Output Packets   = 0
Output Packet No Route     = 0
Reassembly Required         = 0
Reassembly Successful       = 0
Reassembly Failures        = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created           = 0
```

Imagen 7 Estadísticas de conexiones



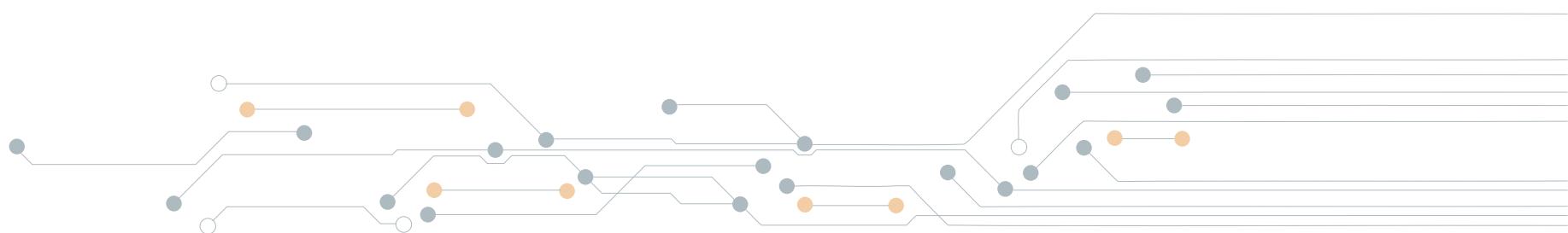
- Conexiones de NetBIOS: *nbtstat -r*

```
C:\Documents and Settings\admin>netstat -r

Route Table
=====
Interface List
0x1 ...00 0c 29 c4 44 a7 .... MS TCP Loopback interface
0x2 ...00 0c 29 c4 44 a7 .... AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
0x10004 ...08 3e 8e 85 33 34 ..... Bluetooth Device <Personal Area Network>
=====

Active Routes:
Network Destination      Netmask          Gateway        Interface Metric
          0.0.0.0          0.0.0.0    192.168.10.2  192.168.10.162    10
          127.0.0.0         255.0.0.0   127.0.0.1     127.0.0.1       1
          192.168.10.0     255.255.255.0 192.168.10.162  192.168.10.162    10
          192.168.10.162   255.255.255.255 127.0.0.1     127.0.0.1       10
          192.168.10.255   255.255.255.255 192.168.10.162  192.168.10.162    10
          224.0.0.0          240.0.0.0   192.168.10.162  192.168.10.162    10
          255.255.255.255  255.255.255.255 192.168.10.162           10004       1
          255.255.255.255  255.255.255.255 192.168.10.162  192.168.10.162       1
Default Gateway:        192.168.10.2
=====
Persistent Routes:
  None
```

Imagen 8 Conexiones de NetBIOS



- Caché de NetBIOS: *nbtstat -c*

```
C:\Documents and Settings\admin>nbtstat /c

Local Area Connection:
Node IpAddress: [192.168.10.162] Scope Id: []
    No names in cache

Bluetooth Network Connection:
Node IpAddress: [0.0.0.0] Scope Id: []
    No names in cache
```

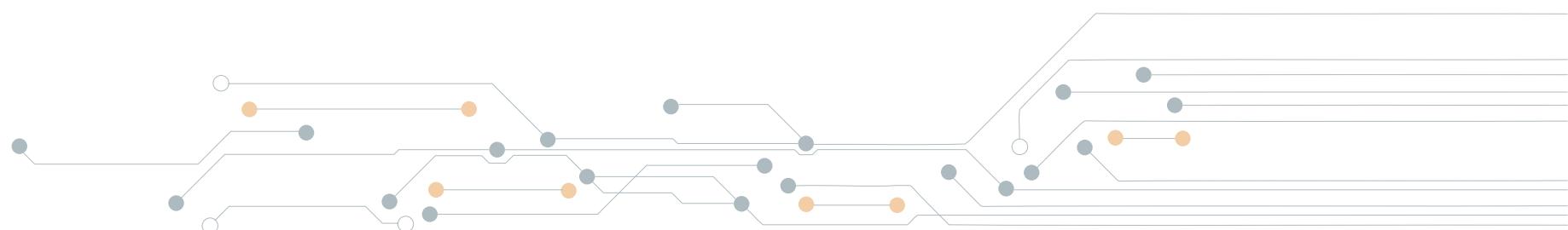
Imagen 9 Caché de NetBIOS



- Configuración de la red: *route PRINT*

```
C:\Documents and Settings\admin>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...0c 29 c4 44 a7 .... AMD PCNET Family PCI Ethernet Adapter - Packet S
cheduler Miniport
0x10004 ...08 3e 8e 85 33 34 ..... Bluetooth Device <Personal Area Network>
=====
Active Routes:
Network Destination      Netmask          Gateway        Interface Metric
          0.0.0.0        0.0.0.0    192.168.10.2  192.168.10.162    10
          127.0.0.0       255.0.0.0   127.0.0.1    127.0.0.1       1
         192.168.10.0    255.255.255.0  192.168.10.162  192.168.10.162    10
        192.168.10.162    255.255.255.255   127.0.0.1    127.0.0.1    10
        192.168.10.255    255.255.255.255  192.168.10.162  192.168.10.162    10
          224.0.0.0        240.0.0.0  192.168.10.162  192.168.10.162    10
      255.255.255.255    255.255.255.255  192.168.10.162           10004       1
      255.255.255.255    255.255.255.255  192.168.10.162  192.168.10.162       1
Default Gateway:        192.168.10.2
=====
Persistent Routes:
  None
```

Imagen 10 Configuración de la red



- Interfaces de red: *ipconfig /all*

```
C:\Documents and Settings\admin>ipconfig /all

Windows IP Configuration

Host Name . . . . . : winxp-9d4ad0906
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . : localdomain

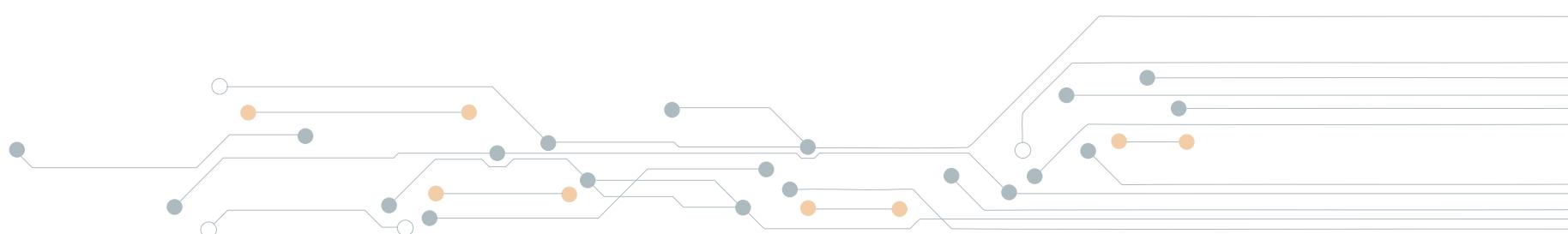
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . . . : localdomain
Description . . . . . : VMware Accelerated AMD PCNet Adapter
Physical Address. . . . . : 00-0C-29-C4-44-A7
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IP Address. . . . . : 192.168.10.162
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.2
DHCP Server . . . . . : 192.168.10.254
DNS Servers . . . . . : 192.168.10.2
Primary WINS Server . . . . . : 192.168.10.2
Lease Obtained. . . . . : Monday, June 20, 2016 7:51:08 AM
Lease Expires . . . . . : Monday, June 20, 2016 8:21:08 AM

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . . . . . : Media disconnected
Description . . . . . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . . . . . : 08-3E-8E-85-33-34
```

Imagen 11 Interfaces de red



- Recursos compartidos: *net SHARE*

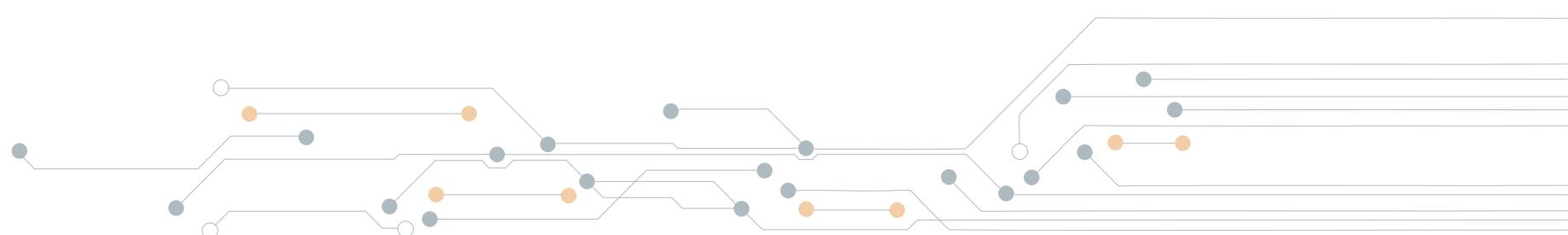
C:\Documents and Settings\admin>net share		
Share name	Resource	Remark
IPC\$		Remote IPC
ADMIN\$	C:\WINDOWS	Remote Admin
C\$	C:\	Default share
E\$	E:\	Default share
The command completed successfully.		

Imagen 12 Recursos compartidos

Toda esta información sería interesante redireccionarla a un documento de texto mediante la redirección >> ubicándolo en una unidad externa y así tener esa información para su posterior análisis.

Otro de los elementos volátiles interesantes serían los usuarios activos. Existen herramientas nativas de Windows para visualizar los usuarios, así como otras herramientas que extraen el hash de la contraseña e incluso en texto plano si es posible.

Para este proceso utilizaremos herramientas nativas como *Nbtstat* (Usuarios de NetBIOS) Y *Net* (Usuarios de recursos compartidos), así como la utilización de la suite *Sysinternals* descargable de <https://technet.microsoft.com/es-es/sysinternals/bb842062>.



- Usuarios de NetBIOS: *nbtstat -n*

```
C:\Documents and Settings\admin>nbtstat -n

Local Area Connection:
NodeIpAddress: [192.168.10.162] Scope Id: []

NetBIOS Local Name Table

Name          Type      Status
-----        -----
WINXP-9D4AD0906<00>  UNIQUE   Registered
MIGRUPO       <00>    GROUP    Registered
WINXP-9D4AD0906<20>  UNIQUE   Registered

Bluetooth Network Connection:
NodeIpAddress: [0.0.0.0] Scope Id: []

No names in cache
```

Imagen 13 Usuarios de NetBIOS

- Usuarios de recursos compartidos: *net USERS*

```
C:\Documents and Settings\admin>net users

User accounts for \\WINXP-9D4AD0906

admin           Administrator           Guest
HelpAssistant  SUPPORT_388945a0
The command completed successfully.
```

Imagen 14 Usuarios de recursos compartidos

- Usuarios locales y remotos: [ruta donde esté sysinternals]/PsLoggedon.exe

```
C:\Documents and Settings\admin\SysinternalsSuite>PsLoggedon
PsLoggedon v1.34 - See who's logged on
Copyright <C> 2000-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
  6/20/2016 7:51:09 AM      WINXP-9D4AD0906\admin

No one is logged on via resource shares.
```

Imagen 15 Usuarios locales y remotos

- SID de usuarios: [ruta donde esté sysinternals]/PsGetsid.exe

```
C:\Documents and Settings\admin\SysinternalsSuite>PsGetsid
PsGetSid v1.44 - Translates SIDs to names and vice versa
Copyright <C> 1999-2008 Mark Russinovich
Sysinternals - www.sysinternals.com

SID for \\WINXP-9D4AD0906:
S-1-5-21-57989841-1580818891-1801674531
```

Imagen 16 SID de usuarios

Toda esta información sería interesante redireccionarla a un documento de texto mediante la redirección >> ubicándolo en una unidad externa y así tener esa información para su posterior análisis.

Además, los servicios en ejecución pueden aportar mucha información acerca de conexiones maliciosas, y sobre todo para análisis de malware. Es imprescindible analizarlos antes de apagar el equipo.

Podremos utilizar las herramientas externas de la Suite Sysinternals con la que obtener los servicios en ejecución y procesos activos y los eventos del sistema.

Para ello abrimos una consola de Windows C:\Windows\System32\cmd.exe y obtenemos la información correspondiente a:

- Servicios en ejecución: [ruta donde esté sysinternals]/PsService.exe

```
Provides performance library information from WMI HiPerf providers.
    TYPE          : 10 WIN32_OWN_PROCESS
    STATE         : 1 STOPPED
                  <NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN>
    WIN32_EXIT_CODE : 1077 <0x435>
    SERVICE_EXIT_CODE : 0 <0x0>
    CHECKPOINT    : 0x0
    WAIT_HINT     : 0 ms

SERVICE_NAME: wscsvc
DISPLAY_NAME: Security Center
Monitors system security settings and configurations.
    TYPE          : 20 WIN32_SHARE_PROCESS
    STATE         : 4 RUNNING
                  <STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN>
    WIN32_EXIT_CODE : 0 <0x0>
    SERVICE_EXIT_CODE : 0 <0x0>
    CHECKPOINT    : 0x0
    WAIT_HINT     : 0 ms

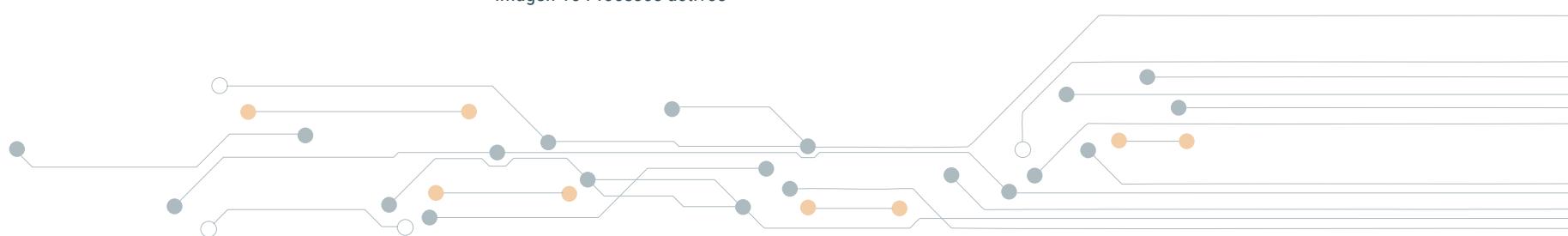
SERVICE_NAME: wuauserv
DISPLAY_NAME: Automatic Updates
Enables the download and installation of Windows updates. If this service is disabled, this computer will not be able to use the Automatic Updates feature or the Windows Update Web site.
    TYPE          : 20 WIN32_SHARE_PROCESS
    STATE         : 4 RUNNING
                  <STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN>
    WIN32_EXIT_CODE : 0 <0x0>
    SERVICE_EXIT_CODE : 0 <0x0>
    CHECKPOINT    : 0x0
    WAIT_HINT     : 0 ms
```

Imagen 17 Servicios en ejecución

- Procesos activos: [ruta donde esté sysinternals]/PsList.exe

Process information for WINXP-9D4AD0906:								
Name	Pid	Pri	Thd	Hnd	Priv	CPU Time	Elapsed Time	
Idle	0	0	1	0	0	0:09:27.406	0:00:00.000	
System	4	8	58	318	0	0:00:10.421	0:00:00.000	
smss	508	11	3	19	172	0:00:00.015	0:10:38.056	
csrss	660	13	10	459	1716	0:00:04.875	0:10:34.947	
winlogon	684	13	18	525	6820	0:00:03.343	0:10:34.478	
services	728	9	16	294	1780	0:00:02.546	0:10:34.103	
lsass	748	9	24	363	4008	0:00:01.093	0:10:34.041	
umacthlp	904	8	1	25	608	0:00:00.031	0:10:33.478	
svchost	920	8	17	210	3096	0:00:00.156	0:10:33.369	
svchost	968	8	10	285	1884	0:00:00.421	0:10:33.135	
svchost	1112	8	86	1472	13960	0:00:03.843	0:10:32.806	
svchost	1380	8	7	83	1340	0:00:00.187	0:10:29.978	
svchost	1392	8	11	181	1596	0:00:00.093	0:10:29.869	
explorer	1700	8	12	363	9324	0:00:02.156	0:10:28.556	
spoolsv	1796	8	12	143	4324	0:00:00.171	0:10:27.931	
rundll32	2016	8	4	75	2296	0:00:00.062	0:10:25.478	
vmtoolsd	2024	8	6	142	8576	0:00:03.937	0:10:25.463	
ctfmon	2040	8	1	87	920	0:00:00.093	0:10:25.369	
svchost	392	8	4	106	1308	0:00:00.031	0:10:11.963	
svchost	428	8	6	104	2296	0:00:00.046	0:10:11.869	
UGAuthService	628	8	2	60	6312	0:00:00.218	0:10:11.572	
vmtoolsd	1208	13	8	275	11384	0:00:00.968	0:10:03.713	
smiprvse	1556	8	13	255	3580	0:00:02.015	0:10:02.619	
alg	596	8	6	106	1180	0:00:00.078	0:10:00.963	
wscntfy	1268	8	1	37	580	0:00:00.031	0:10:00.556	
wuauctl	1100	8	4	112	2224	0:00:00.093	0:09:01.397	
cmd	1316	8	1	33	2024	0:00:00.140	0:07:11.436	
chrome	1708	8	32	849	67204	0:00:12.640	0:02:41.730	
chrome	1440	8	8	48	1856	0:00:00.062	0:02:41.652	
chrome	1056	8	10	189	50036	0:00:05.609	0:02:33.323	
pslist	3588	13	2	93	1196	0:00:00.093	0:00:02.265	

Imagen 18 Procesos activos



- Eventos del sistema: [ruta donde esté sysinternals]/PsLoglist.exe

```
[008] Setup
  Type: ERROR
  Computer: WINXP-9D4AD0906
  Time: 6/3/2016 9:56:36 AM ID: 60055
Windows Setup encountered non-fatal errors during installation. Please check the
setuperr.log found in your Windows directory for more information.

[007] HTTP
  Type: INFORMATION
  Computer: WINXP-9D4AD0906
  Time: 6/3/2016 9:53:59 AM ID: 15007
Reservation for namespace identified by URL prefix http://*:2869/ was successful-
ly added.

[006] Workstation
  Type: INFORMATION
  Computer: WINXP-9D4AD0906
  Time: 6/3/2016 9:52:48 AM ID: 3268
This computer has been successfully joined to workgroup 'MIGRUPO'.

[005] EventLog
  Type: INFORMATION
  Computer: WINXP-9D4AD0906
  Time: 6/3/2016 9:51:09 AM ID: 6011
The NetBIOS name and DNS host name of this machine have been changed from MACHIN-
ENAME to WINXP-9D4AD0906.
```

Imagen 19 Eventos del sistema



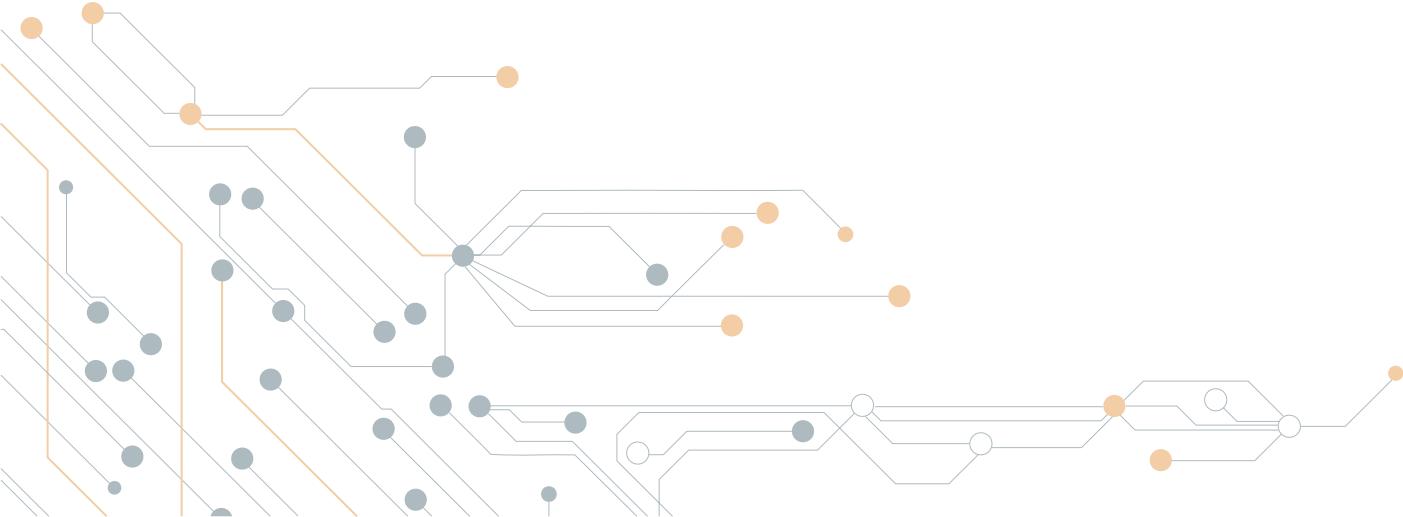
Toda esta información sería interesante redireccionarla a un documento de texto mediante la redirección >> ubicándolo en una unidad externa y así tener esa información para su posterior análisis.

Una recopilación de comandos que permiten obtener más información interesante que se podría recopilar, ya sea utilizando herramientas nativas de windows como herramientas especializadas, es la que a continuación se lista:

- Fecha y Hora del sistema: `date /t & time /t` (tanto al principio de la investigación como a la finalización del proceso)

```
C:\Documents and Settings\admin\SysinternalsSuite>date /t & time /t  
Mon 06/20/2016  
08:02 AM
```

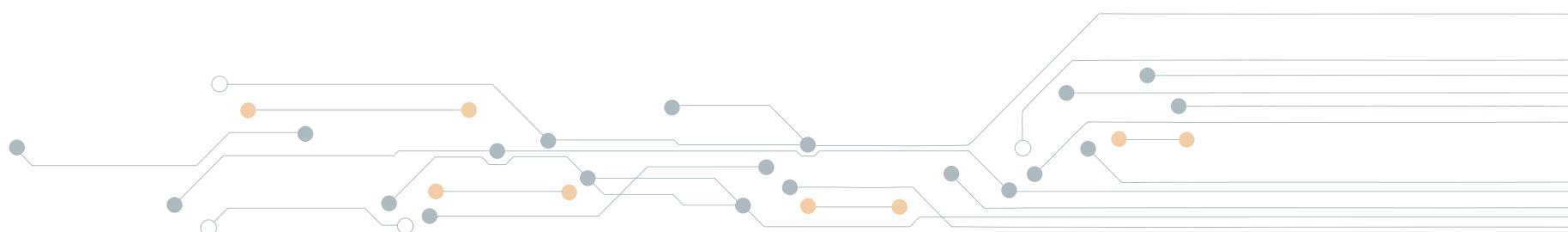
Imagen 20 Fecha y Hora del sistema



- Información del sistema: *systeminfo*

```
C:\Documents and Settings\admin\SysinternalsSuite>systeminfo
Host Name:          WINXP-9D4AD0906
OS Name:           Microsoft Windows XP Professional
OS Version:        5.1.2600 Service Pack 3 Build 2600
OS Manufacturer:   Microsoft Corporation
OS Configuration:  Standalone Workstation
OS Build Type:    Uniprocessor Free
Registered Owner:  WinXP
Registered Organization:
Product ID:        76487-640-5536995-23670
Original Install Date: 6/3/2016, 9:56:30 AM
System Up Time:    0 Days, 0 Hours, 11 Minutes, 52 Seconds
System Manufacturer: VMware, Inc.
System Model:      VMware Virtual Platform
System type:       X86-based PC
Processor(s):
  1 Processor(s) Installed.
  [01]: x86 Family 6 Model 58 Stepping 9 GenuineIntel
  1696 Mhz
  BIOS Version:     INTEL - 6040000
  Windows Directory: C:\WINDOWS
  System Directory:  C:\WINDOWS\system32
  Boot Device:      \Device\HarddiskVolume2
  System Locale:    en-us;English (United States)
  Input Locale:     en-us;English (United States)
  Time Zone:        <GMT-08:00> Pacific Time (US & Canada)
  Total Physical Memory: 2,047 MB
  Available Physical Memory: 1,616 MB
  Virtual Memory: Max Size: 2,048 MB
  Virtual Memory: Available: 2,004 MB
  Virtual Memory: In Use: 44 MB
  Page File Location(s): C:\pagefile.sys
  Domain:           MIGRUP0
  Logon Server:     \\WINXP-9D4AD0906
  Hotfix(s):
    386 Hotfix(s) Installed.
    [01]: File 1
    [02]: File 1
```

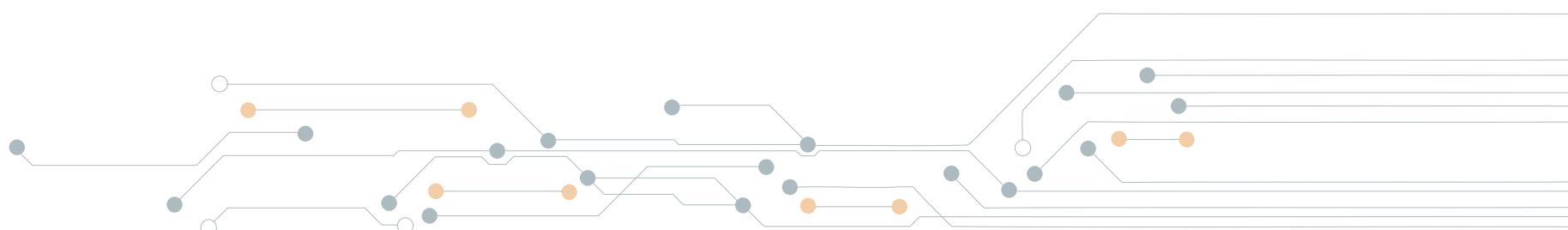
Imagen 21 Información del sistema



- Información Tcp/Ip: `ipconfig /all`
- Las conexiones abiertas y puertos en espera, con PID asociado: `netstat -an`
- La información del sistema (hardware, software, hotfixes, versiones, etc.): `psinfo -shd`
- La lista de los procesos: `pslist -t`
- La lista de tareas programadas: `at` o `schtasks`
- Los usuarios logados y hora de logon: `psloggedon`
- Volcado de los log de eventos: `psloglist`
- La información de servicios de sistema: `psservice`
- Las conexiones netbios/smb: `net use`, `net accounts`, `net session`, `net share`, `net user`
- La lista de DLLs cargadas en el sistema: `listdlls`

chrome.exe pid: 1708		
Command line: "C:\Program Files\Google\Chrome\Application\chrome.exe"		
Base	Size	Path
0x00400000	0xdc000	chrome.exe
0x7c900000	0xb2000	ntdll.dll
0x7c800000	0xf6000	kernel32.dll
0x01c20000	0x23000	chrome_elf.dll
0x77dd0000	0x9b000	ADVAPI32.dll
0x77e70000	0x93000	RPCRT4.dll
0x77fe0000	0x11000	Secur32.dll
0x4d4f0000	0x59000	WINHTTP.dll
0x77c10000	0x58000	msvcrt.dll
0x77f60000	0x76000	SHLWAPI.dll
0x77f10000	0x49000	GDI32.dll
0x7e410000	0x91000	USER32.dll
0x77c00000	0x8000	VERSION.dll
0x76b40000	0x2d000	WINMM.dll
0x769c0000	0xb4000	USERENV.dll
0x76f50000	0x8000	WTSAPI32.dll
0x76360000	0x10000	WINSTA.dll
0x5b860000	0x56000	NETAPI32.dll
0x76390000	0x1d000	IMM32.DLL
0x7c9c0000	0x818000	SHELL32.dll
0x773d0000	0x103000	comct132.dll
0x01c50000	0x2216000	chrome.dll
0x74d90000	0x6b000	USP10.dll
0x26hf0000	0xh000	PSAPI.DLL

Imagen 22 DLLs cargadas en el sistema



- La lista de ficheros (.exe, .dll) no firmados: `sigcheck -u -e c:\windows`

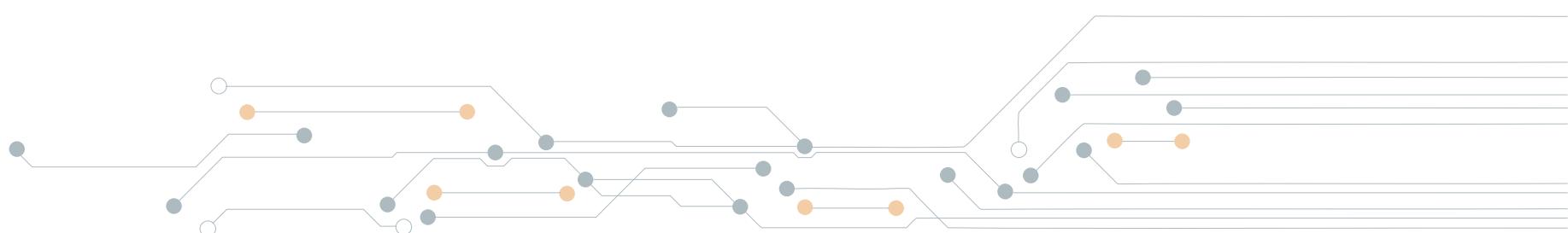
```
c:\Users\Raul\SysinternalsSuite>sigcheck -u -e c:\windows
Sigcheck v2.51 - File version and signature viewer
Copyright (C) 2004-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\windows\SECOH-QAD.dll:
    Verified: Unsigned
    Link date: 19:48 24/01/2014
    Publisher: n/a
    Company: n/a
    Description: n/a
    Product: n/a
    Prod version: n/a
    File version: n/a
    MachineType: 64-bit

c:\windows\SECOH-QAD.exe:
    Verified: Unsigned
    Link date: 19:48 24/01/2014
    Publisher: n/a
    Company: n/a
    Description: n/a
    Product: n/a
    Prod version: n/a
    File version: n/a
    MachineType: 64-bit

c:\windows\unins000.exe:
    Verified: Unsigned
    Link date: 16:16 20/12/2011
    Publisher: n/a
    Company: n/a
    Description: Setup/Uninstall
    Product: n/a
    Prod version: n/a
    File version: 51.1052.0.0
    MachineType: 32-bit
```

Imagen 23 Ficheros no firmados



- La lista de ficheros con alternate data streams (ads): *streams -s c:\*
- Las sesiones actuales y procesos por sesión: *logonsessions -p*
- La tabla de caché ARP: *arp -a*
- Los eventos de logon correctos y fallidos: *ntlast*

```
C:\Documents and Settings\admin>ntlast
- No Records - Check to see if auditing is on
```

Imagen 24 Eventos de logon correctos y fallidos

- La tabla de enrutado IP: *route print*
- Los elementos de autoejecución: *autorunsc*

Autoruns [WINXP-904AD0906\administrator] - Sysinternals: www.sysinternals.com					
File		Entry		Options	
User		Help			
Autorun Entry	Description	Publisher	Image Path	Timestamp	
HKEY\Software\Microsoft\Windows\CurrentVersion\Run				6/20/2016 7:	
VMware User ...	VMware Tools Core Service	VMware, Inc.	c:\program files\vmware\.../v...	10/18/2015 1	
HKEY\Software\Microsoft\Active Setup\Installed Components				6/20/2016 7:	
Address Book 6	Outlook Express Setup Libr..	Microsoft Corporation	c:\program files\outlook.ex...	4/13/2008 11	
Google Chrome	Google Chrome Installer	Google Inc.	c:\program files\google\chr...	4/5/2016 4:2	
Microsoft Office...	Outlook Express Setup Libr..	Microsoft Corporation	c:\program files\outlook.ex...	4/13/2008 11	
HKEY\Software\Microsoft\Internet Explorer\Desktop\Components				6/3/2016 9:5	
0				File not found: About.Home	
HKEY\Software\Classes\ShellEx\ContextMenuHandlers				6/3/2016 11:	
WinRAR	WinRAR shell extension	Alexander Roshal	c:\program files\winrar\.../w...	2/3/2016 12:	
HKEY\Software\Classes\Folder\ShellEx\ContextMenuHandlers				6/3/2016 11:	
WinRAR	WinRAR shell extension	Alexander Roshal	c:\program files\winrar\.../w...	2/3/2016 12:	
HKEY\Software\Classes\Folder\ShellEx\DragDropHandlers				6/3/2016 11:	
WinRAR	WinRAR shell extension	Alexander Roshal	c:\program files\winrar\.../w...	2/3/2016 12:	
Task Scheduler					
GoogleUpdate...	Google Installer	Google Inc.	c:\program files\google\up...	1/9/2016 5:0	
GoogleUpdate...	Google Installer	Google Inc.	c:\program files\google\up...	1/9/2016 5:0	
HKEY\System\CurrentControlSet\Services				6/20/2016 8:	
gupdate	Keeps your Google software up-to-date	Google Inc.	c:\program files\google\up...	1/9/2016 5:0	
quardate	Keeps your Google software up-to-date	Google Inc.	c:\program files\google\up...	1/9/2016 5:0	
TPLAutoConnSvc	ThePrint component for printer sharing	Confado AG	c:\program files\vmware\.../v...	1/8/2015 8:0	
TPVCGateway	ThePrint component that receives print jobs from the printer sharing service	Confado AG	c:\program files\vmware\.../v...	10/29/2014 6	
VGAAuthService	Alias Manager and Ticket Service	VMware, Inc.	c:\program files\vmware\.../v...	10/14/2015 1	
VMT tools	Provides support for synchronizing VMs	VMware, Inc.	c:\program files\vmware\.../v...	10/18/2015 1	
VMware Physi...	Enables support for running virtual machines	VMware, Inc.	c:\program files\vmware\.../v...	10/18/2015 1	

Imagen 25 Elementos de autoejecución

- La información sobre volúmenes, mount points, filesystem, etc.: *volume\_dump*

```
C:\Documents and Settings\admin\fau-1.4.0.2464\fau-1.4.0.2464\x86\volume_dump.exe
Forensic Acquisition Utilities, 1.4.1.2464
Volume Dump Utility, 1.4.1.2464
Copyright (C) 2002-2013 GMG Systems, Inc.

Command Line: volume_dump.exe
Microsoft Windows XP 5.1.2600 Uniprocessor Free(Service Pack 3, 2600.xpsp_sp3_qFE.101209-1646)
6/20/2016 15:19:36 PM <UTC>
6/20/2016 8:19:36 AM <local time>
Current User: WINXP-9D4AD9\administrator
Current Locale: English_United States.437
User Default Locale Language: 0x0409

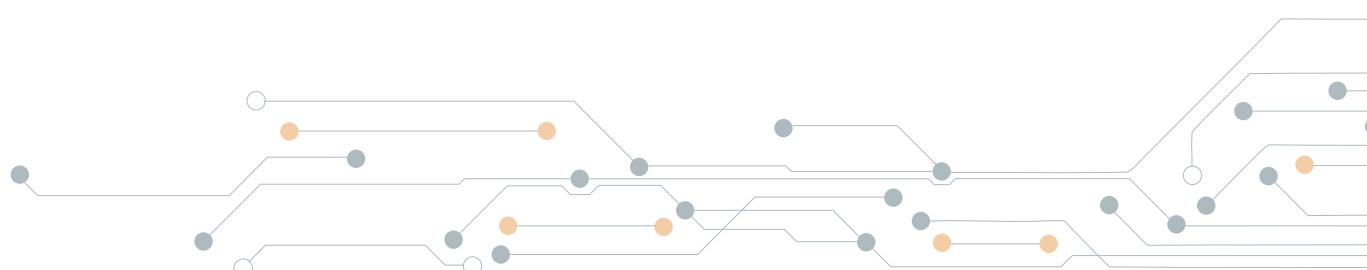
The Windows Firewall Firewall is active with exceptions.

Volume Name: \\?\Volume{02fea846-29b8-11e6-8a3a-083e8e853334}
Device: \Device\HarddiskVolume1
Volume Label: copia
Mount Points:
    E:\
Drive Type: Fixed
Volume Serial Number: d8cd-1dd4
Maximum Component Length: 255

Volume Characteristics:
    File system preserves case
    File system supports case sensitive file names
    File system supports Unicode file names
    File system preserves and supports persistent ACL's
    File system supports file level compression
    File system supports named streams
    File system supports encryption
    File system supports object identifiers
    File system supports reparse points
    File system supports sparse files
    File system supports quotas

File System: NTFS
Mounted: Yes
Clustered: No
```

Imagen 26 Información sobre volúmenes, mount points, filesystem, etc



- Los hashes (nthash/lmhash) de cuentas locales: *pwdump2*

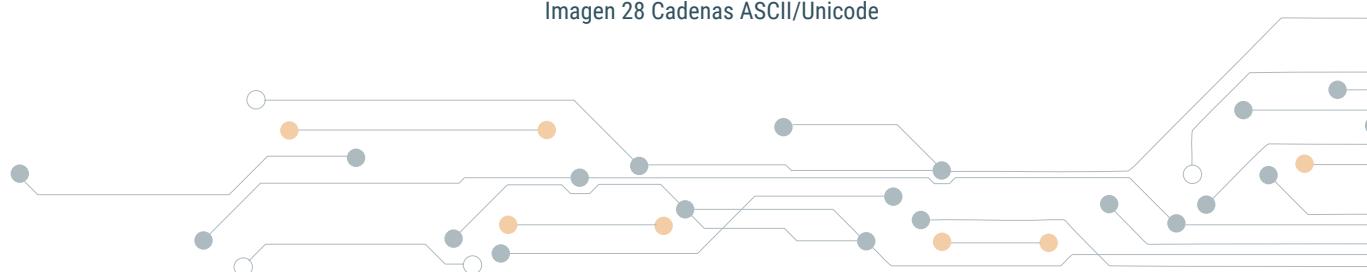
```
C:\>tools>pwdump2
Administrador:500:0182bd0bd4444bf8aad3b435b51404ee:328727b81ca05805a68ef26acb252
039:::
Invitado:501:aad3b435b51404eeeaad3b435b51404ee:31d6cfe0d16ae931b73e59d7e0c089c0:::
:
SUPPORT_388945a0:1001:aad3b435b51404eeeaad3b435b51404ee:114a2bb20d53cdc637e0ac81e
c07b797:::
```

Imagen 27 Hashes

- Las cadenas ASCII/Unicode en los ficheros: *strings*

```
c:\Users\Raul\SysinternalsSuite>strings * | findstr /i password
c:\Users\Raul\SysinternalsSuite\accesschk.exe: \pard\fi-357\li357\sb120\sai20\tx360\b\fs20 3.\tab SEN
t capture \ldblquote process state\rdblquote information, files saved by Sysinternals tools may incl
passwords, paths to files accessed, and paths to registry accessed). By using this software, you ackn
lly identifiable or other sensitive information provided to Microsoft or any other party through your
c:\Users\Raul\SysinternalsSuite\accesschk.exe: information, files saved by Sysinternals tools may in
passwords, paths to files accessed, and paths to registry accessed). By using this software, you ackn
lly identifiable or other sensitive information provided to Microsoft or any other party through your
c:\Users\Raul\SysinternalsSuite\accesschk.exe: \pard\fi-357\li357\sb120\sai20\tx360\b\fs20 3.\tab SEN
t capture \ldblquote process state\rdblquote information, files saved by Sysinternals tools may incl
passwords, paths to files accessed, and paths to registry accessed). By using this software, you ackn
lly identifiable or other sensitive information provided to Microsoft or any other party through your
c:\Users\Raul\SysinternalsSuite\accesschk.exe: information, files saved by Sysinternals tools may in
passwords, paths to files accessed, and paths to registry accessed). By using this software, you ackn
lly identifiable or other sensitive information provided to Microsoft or any other party through your
c:\Users\Raul\SysinternalsSuite\AccessEnum.exe: {\edmins5}\{\nofpages\}\{\nofwords1030\}\{\nofchars5872\}\
build_version\proptype30\staticval 2.6\{\propname db_charger_document_reference\proptype3\staticv
c:\Users\Raul\SysinternalsSuite\ADExplorer.exe: Password Error
c:\Users\Raul\SysinternalsSuite\ADExplorer.exe: The passwords do not match.
c:\Users\Raul\SysinternalsSuite\ADExplorer.exe: Password Error
c:\Users\Raul\SysinternalsSuite\ADExplorer.exe: badPasswordTime
c:\Users\Raul\SysinternalsSuite\ADExplorer.exe: USERPASSWORD
c:\Users\Raul\SysinternalsSuite\ADExplorer.exe: USERPASSWORD
```

Imagen 28 Cadenas ASCII/Unicode



También podríamos utilizar alguna herramienta gráfica para obtener cierta información relevante, como:

- Detecta rootkits en modo usermode o kernelmode: *rootkit revealer*

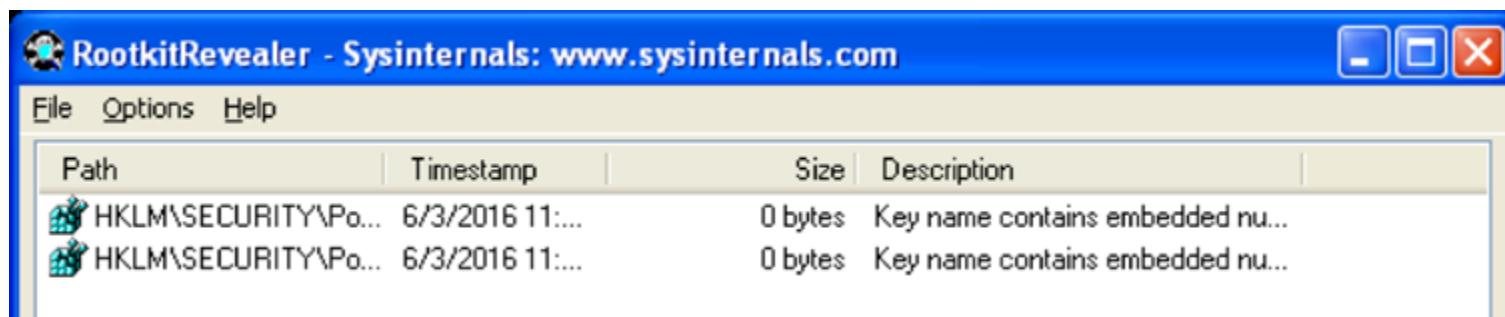
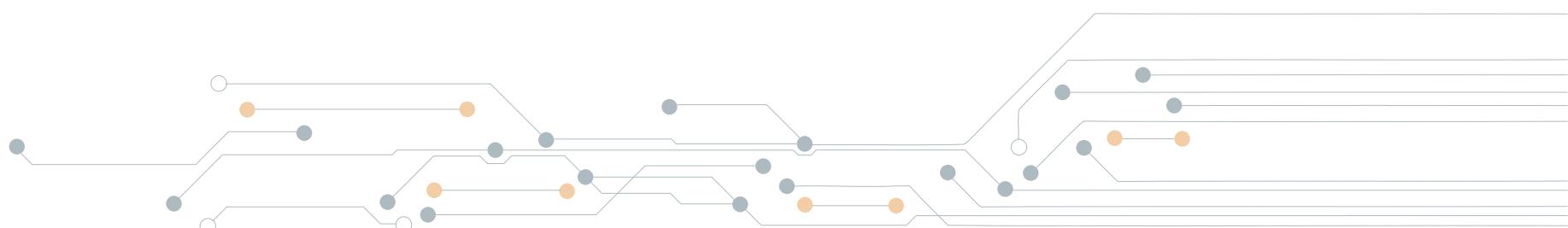


Imagen 29 Rootkits

Podemos descargarla de <https://technet.microsoft.com/en-us/sysinternals/rootkitrevealer.aspx>



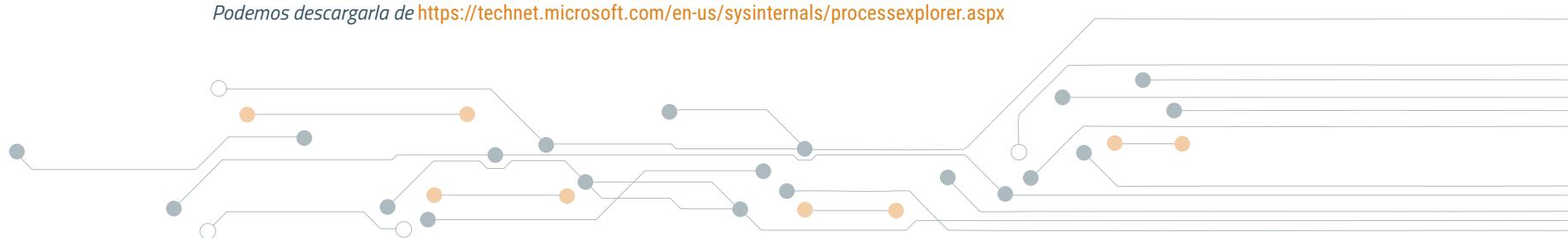
- La información útil sobre procesos, librerías que usan, recursos accedidos, conexiones de red, etc.: *procexp* y *procmon*

**Process Explorer - Sysinternals: www.sysinternals.com [WINXP-9D4AD0906\admin]**

Process	CPU	Private Bytes	Working Set	PID	Description	Compa
System Idle Process	100.00	0 K	28 K	0		
System	< 0.01	0 K	236 K	4		
Interrupts		0 K	0 K		n/a Hardware Interrupts and DPCs	
smss.exe		172 K	428 K	508	Windows NT Session Mana... Microsoft	
csrss.exe		1,780 K	3,716 K	660	Client Server Runtime Process Microsoft	
winlogon.exe		6,444 K	4,972 K	684	Windows NT Logon Applicat... Microsoft	
services.exe		1,820 K	3,812 K	728	Services and Controller app Microsoft	
vmacthl.exe		608 K	2,572 K	904	VMware Activation Helper VMware	
svchost.exe		3,096 K	5,024 K	920	Generic Host Process for Wi... Microsoft	
wmprvse.exe		3,860 K	8,988 K	1556	WMI Microsoft	
wmprvse.exe		2,416 K	4,984 K	3152	WMI Microsoft	
svchost.exe		1,928 K	4,696 K	968	Generic Host Process for Wi... Microsoft	
svchost.exe		17,928 K	27,584 K	1112	Generic Host Process for Wi... Microsoft	
wscnfy.exe		580 K	2,520 K	1268	Windows Security Center No... Microsoft	
wuauctl.exe		2,208 K	4,108 K	1100	Windows Update Microsoft	
svchost.exe		1,336 K	3,696 K	1380	Generic Host Process for Wi... Microsoft	
svchost.exe		1,596 K	4,180 K	1392	Generic Host Process for Wi... Microsoft	
spoolsv.exe		4,244 K	6,816 K	1796	Spooler SubSystem App Microsoft	
svchost.exe		1,332 K	3,820 K	392	Generic Host Process for Wi... Microsoft	
svchost.exe		2,248 K	3,556 K	428	Generic Host Process for Wi... Microsoft	
VGAAuthService.exe		6,312 K	9,216 K	628	VMware Guest Authenticatio... VMware	
vmtoolsd.exe		11,388 K	14,572 K	1208	VMware Tools Core Service VMware	
alg.exe		1,164 K	3,628 K	596	Application Layer Gateway S... Microsoft	
lsass.exe		4,028 K	6,580 K	748	LSA Shell (Export Version) Microsoft	

Imagen 30 Procesos

Podemos descargarla de <https://technet.microsoft.com/en-us/sysinternals/processexplorer.aspx>



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time... Process Name PID Operation Path Result Detail

Time...	Process Name	PID	Operation	Path	Result	Detail
8:13:1...	lsass.exe	748	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access
8:13:1...	lsass.exe	748	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access
8:13:1...	lsass.exe	748	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(\D...	BUFFER OVERFL...	Length: 12
8:13:1...	lsass.exe	748	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
8:13:1...	lsass.exe	748	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access
8:13:1...	lsass.exe	748	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(\D...	SUCCESS	Type: REG_I
8:13:1...	lsass.exe	748	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
8:13:1...	lsass.exe	748	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access
8:13:1...	lsass.exe	748	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access
8:13:1...	lsass.exe	748	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(\D...	BUFFER OVERFL...	Length: 12
8:13:1...	lsass.exe	748	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
8:13:1...	lsass.exe	748	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access
8:13:1...	lsass.exe	748	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(\D...	SUCCESS	Type: REG_I
8:13:1...	lsass.exe	748	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	

Imagen 31 Monitor de procesos



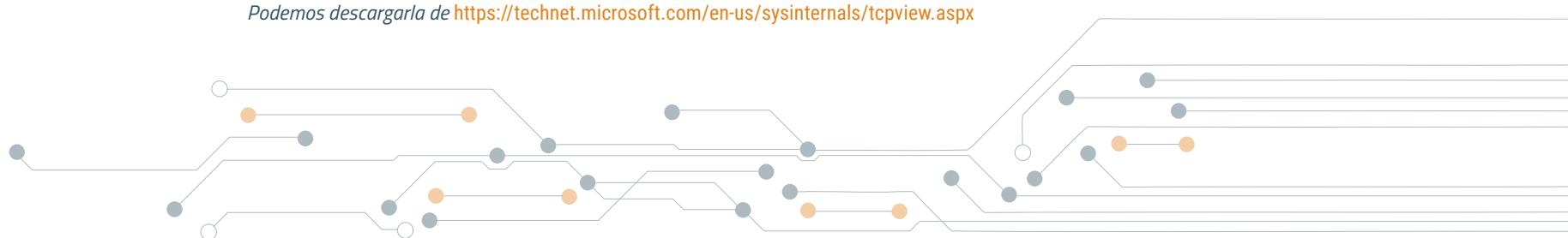
- Las conexiones de red y aplicaciones asociadas: *tcpview*

**TCPView - Sysinternals: www.sysinternals.com**

Proc...	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
alg.exe	596	TCP	winxp-9d4ad0906	1028	winxp-9d4ad0906	0
chrome.exe	1708	TCP	winxp-9d4ad0906...	1139	mad01s25-in-f206...	http
chrome.exe	1708	TCP	winxp-9d4ad0906...	1120	40.dc.c0ad.ip4.sta...	http
chrome.exe	1708	TCP	winxp-9d4ad0906...	1095	a104-126-71-174...	http
chrome.exe	1708	TCP	winxp-9d4ad0906...	1099	a104-126-71-174...	http
chrome.exe	1708	TCP	winxp-9d4ad0906...	1140	mad01s25-in-f206...	http
chrome.exe	1708	TCP	winxp-9d4ad0906...	1107	185.43.181.32	http
chrome.exe	1708	TCP	winxp-9d4ad0906...	1100	104.126.86.66	http
chrome.exe	1708	TCP	winxp-9d4ad0906...	1115	95.101.109.2	https
chrome.exe	1708	TCP	winxp-9d4ad0906...	1093	a104-126-71-174...	http
chrome.exe	1708	TCP	winxp-9d4ad0906...	1137	185.43.181.33	http
chrome.exe	1708	TCP	winxp-9d4ad0906...	1161	2.17.44.168	http
chrome.exe	1708	TCP	winxp-9d4ad0906...	1119	40.dc.c0ad.ip4.sta...	http
chrome.exe	1708	TCP	winxp-9d4ad0906...	1094	a104-126-71-174...	http
lsass.exe	748	UDP	winxp-9d4ad0906	isakmp	*	*
lsass.exe	748	UDP	winxp-9d4ad0906	4500	*	*
svchost.exe	968	TCP	winxp-9d4ad0906	epmap	winxp-9d4ad0906	0
svchost.exe	1392	UDP	winxp-9d4ad0906...	1900	*	*
svchost.exe	1112	UDP	winxp-9d4ad0906	nntp	*	*
svchost.exe	1112	UDP	winxp-9d4ad0906...	nntp	*	*
svchost.exe	1392	UDP	winxp-9d4ad0906	1900	*	*
System	4	TCP	winxp-9d4ad0906...	netbios-ssn	winxp-9d4ad0906	0
System	4	TCP	winxp-9d4ad0906	microsoft-ds	winxp-9d4ad0906	0
System	4	UDP	winxp-9d4ad0906...	netbios-ns	*	*
System	4	UDP	winxp-9d4ad0906...	netbios-dgm	*	*
System	4	UDP	winxp-9d4ad0906	microsoft-ds	*	*

Imagen 32 Conexiones de red

Podemos descargarla de <https://technet.microsoft.com/en-us/sysinternals/tcpview.aspx>



Muy importante recordar que hay que realizar el hash siempre de toda evidencia adquirida.

Algunos de los nombres de dispositivos en Windows que tenemos que tener claros para trabajar con sistemas Windows, son los siguientes:

\.\	Local machine
\.\C:	C: volume
\.\D:	D: volume
\.\PhysicalDrive0	First physical disk
\.\PhysicalDrive1	Second physical disk
\.\CdRom0	First CD-Rom
\.\Floppy0	First floppy disk
\.\PhysicalMemory	Physical memory

El volcado de memoria es el proceso más importante y crítico ya que en la memoria se almacenan muchas evidencias que podrían ser importantes para el proceso de investigación. Como hemos visto anteriormente entre ellas están las conexiones establecidas, los procesos en ejecución, contraseñas de volúmenes cifrados, etc. Para realizar el volcado de memoria hay que realizarlo de una forma correcta, ya que podría invalidar el proceso.

Debemos realizar el volcado de la memoria, tanto de la física, la memoria real del sistema, como de la virtual, en sistemas Windows el archivo pagefile.sys. La memoria virtual es una técnica de gestión de la memoria que permite que el sistema operativo disponga, tanto para el software de usuario como para sí mismo, de mayor cantidad de memoria que esté disponible físicamente.

Disponemos de multitud de herramientas que se utilizan para realizar el volcado de memoria: Una de ellas es mediante Dumpl o MoonSols Windows Memory Toolkit, que es una herramienta para tomar muestras de la memoria RAM. Se ejecuta con solo un clic y se recomienda lanzar la aplicación desde un recurso externo.

```
DumpIt - v1.3.2.20110401 - One click memory dumper
Copyright <c> 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright <c> 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size:          1073741824 bytes (< 1024 Mb>
Free space size:            7792447488 bytes (< 7431 Mb>
* Destination = \??\E:\USER-PC-20140512-063419.rau
--> Are you sure you want to continue? [y/n] y
+ Processing... Success.
```

Imagen 33 Dumpl - Adquisición de memoria

Obien mediante OSForensics que es una herramienta de investigación digital que le permite extraer datos forenses o descubrir información oculta de una computadora. Ofrece una variedad de características de búsquedas avanzadas que le permiten descubrir las actividades realizadas en el equipo o en Internet, archivos borrados, contraseñas almacenadas y otras informaciones forenses.

Para el volcado de Memoria podemos ir a Memory Viewer → Dump Physical Memory

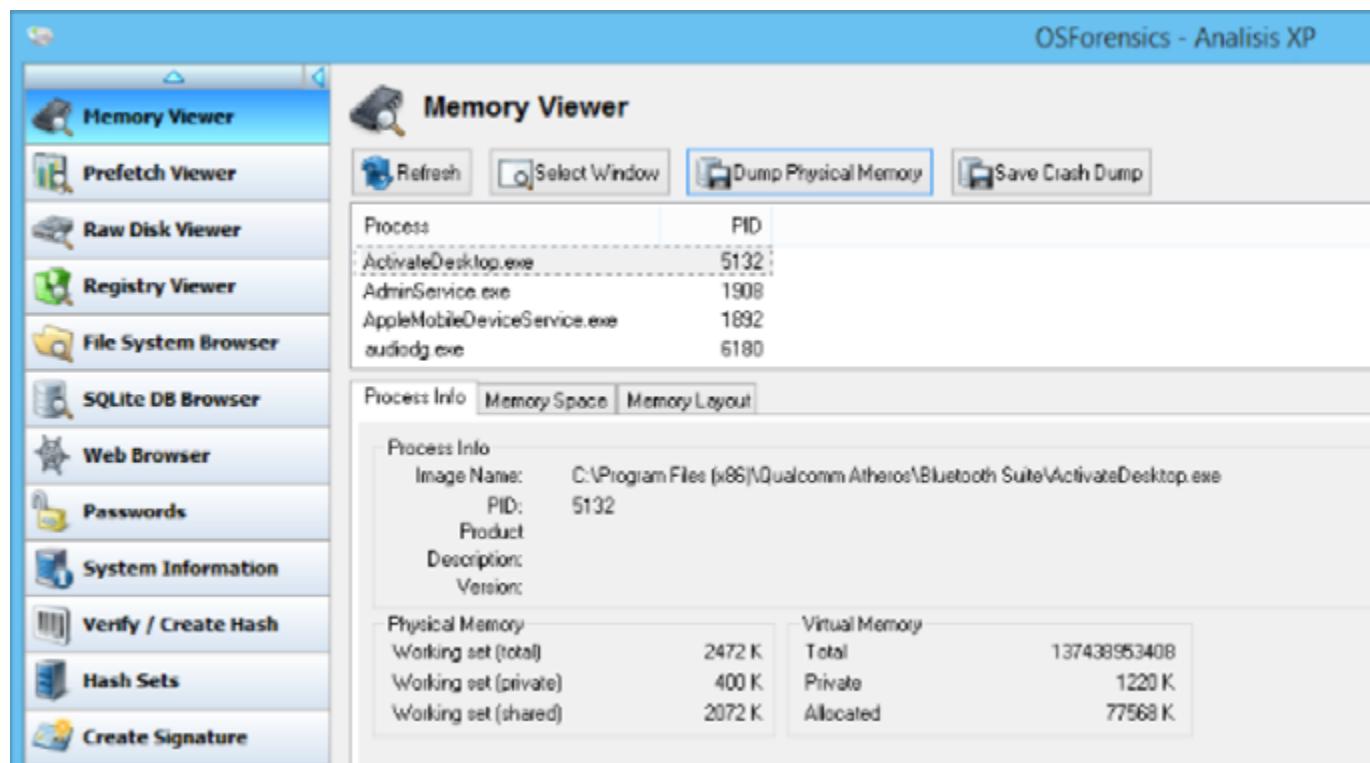
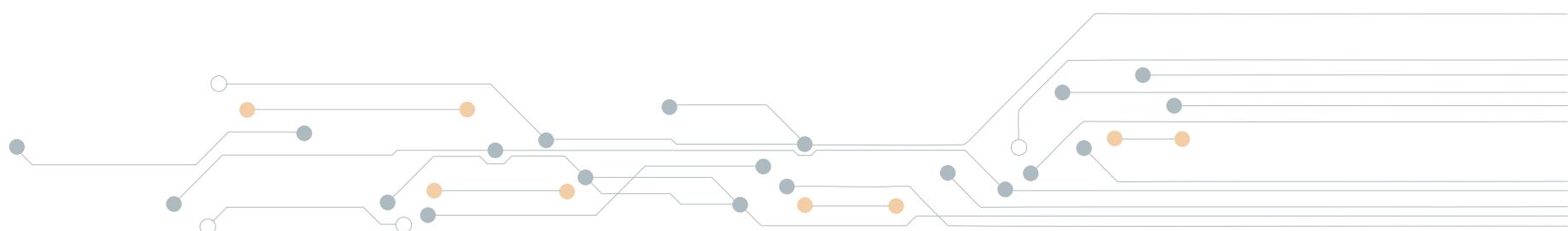


Imagen 34 OSForensics - Adquisición de memoria



También podemos realizar el volcado mediante alguna distribución orientada a análisis forense como Caine. Para ello introducimos el Live CD en la unidad y al abrir dicha unidad ejecutamos WIN-UFO

Ultimate Forensics Outflow, con lo que nos desplazamos a la opción:  
Volcado de Memoria → Viewers → FTK Imager → Capture Memory

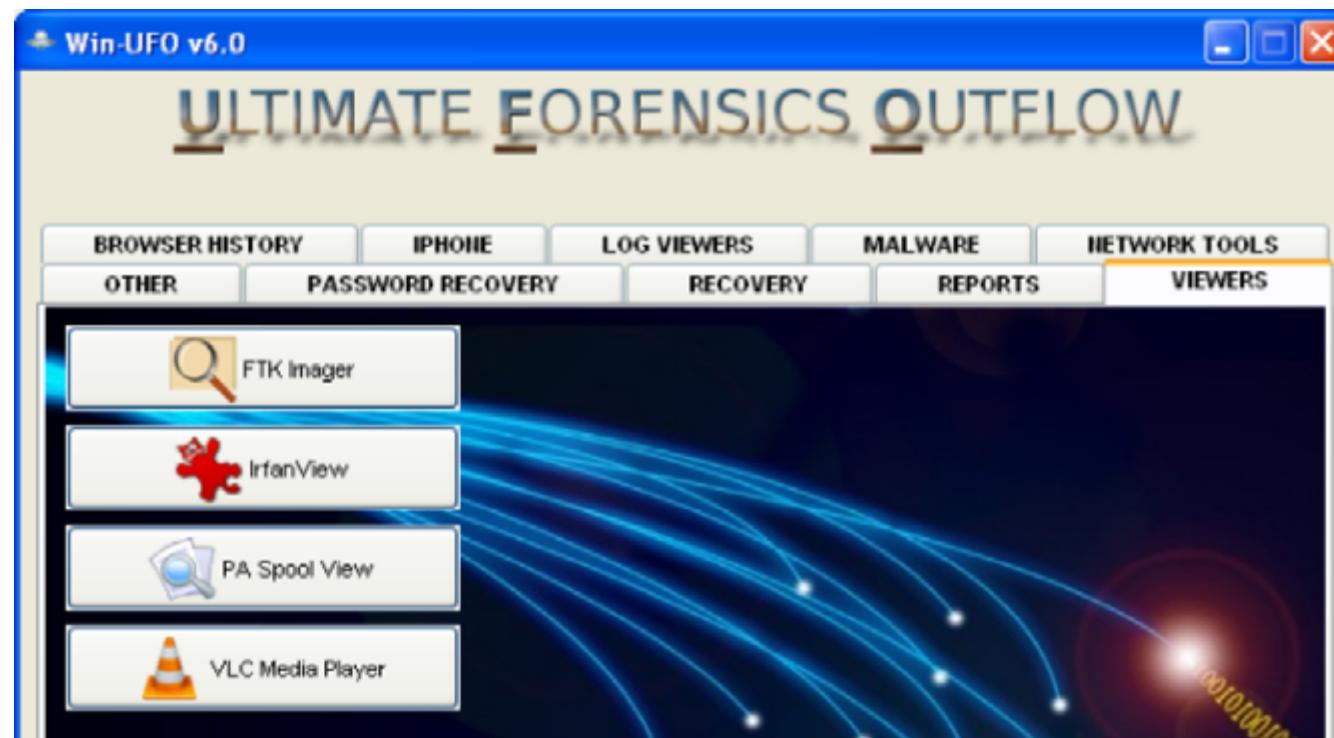
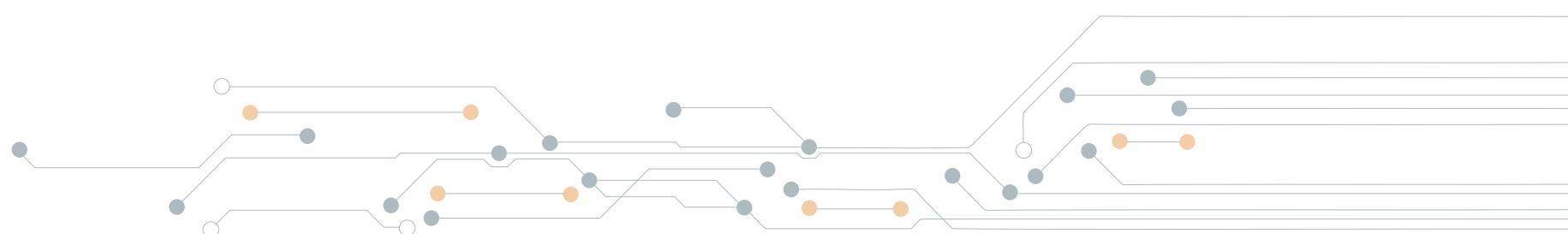


Imagen 35 WIN-UFO Caine



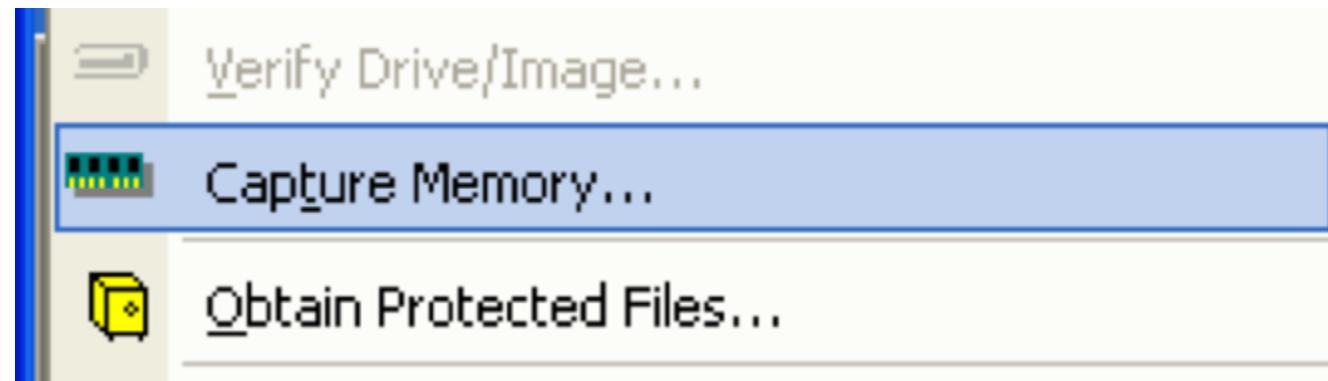
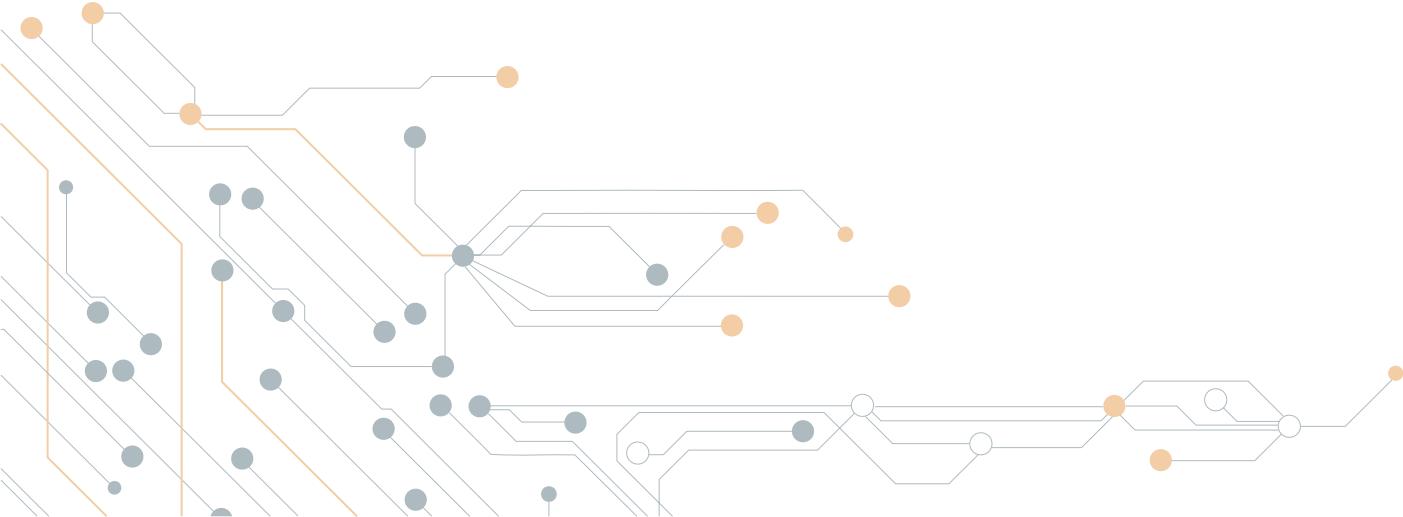


Imagen 36 FTK Imager - Volcado de memoria

Muy importante siempre es almacenar los volcados en las unidades externas habilitadas para ello del sistema.

A continuación, veremos otra manera de obtener la memoria física mediante un “crash dump” o BOSD (Blue Screen Of Death), que es el fallo del sistema cuando no puede recuperarse generando un fichero

que puede ser un volcado parcial o completo de la memoria física, para su posterior análisis. Se puede provocar mediante herramientas como NotMyFault, pero dependerá de la investigación que se lleva en marcha, pero siempre teniendo en cuenta el orden de adquisición de las distintas evidencias.



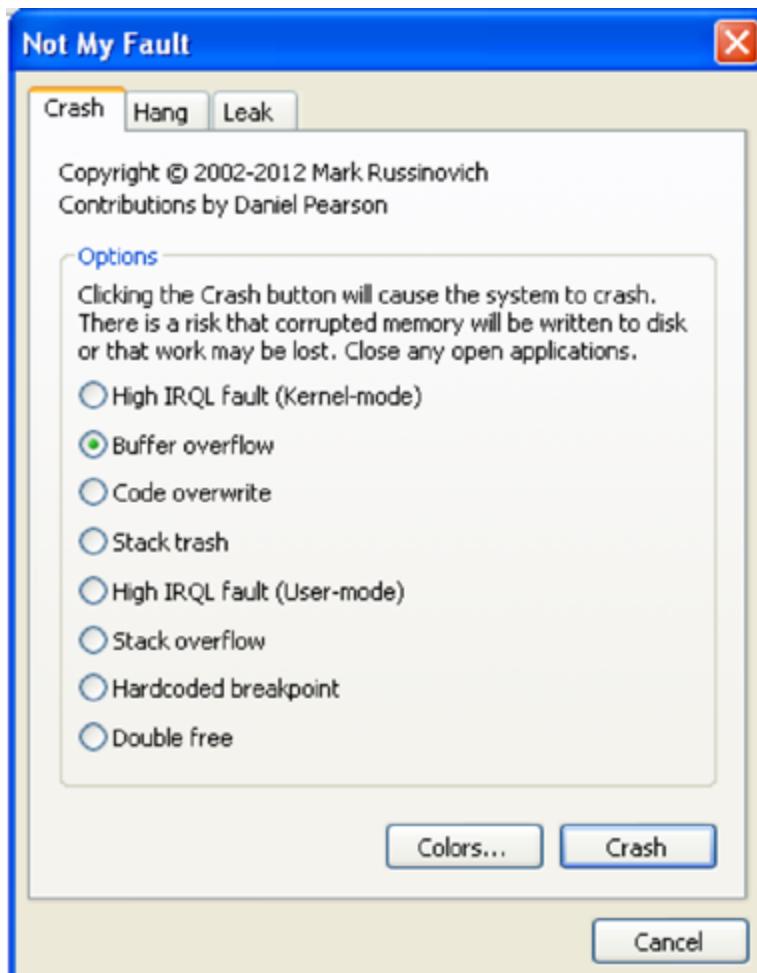
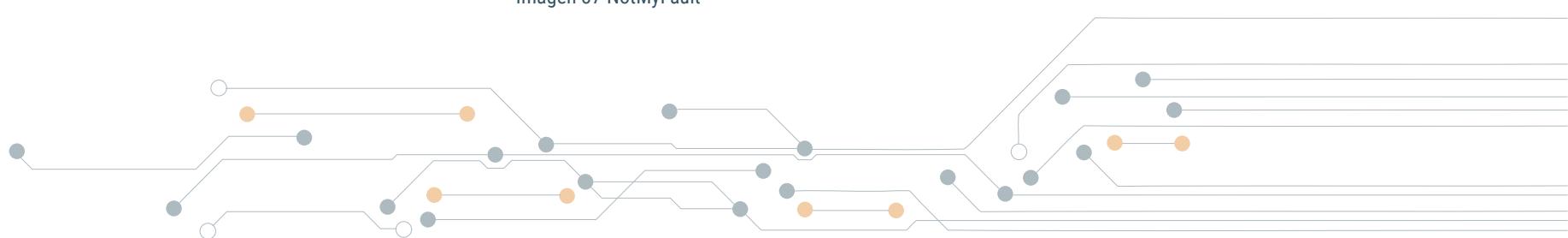


Imagen 37 NotMyFault



A problem has been detected and windows has been shut down to prevent damage to your computer.

DRIVER\_IRQL\_NOT\_LESS\_OR\_EQUAL

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup options, and then select Safe Mode.

Technical information:

\*\*\* STOP: 0x000000D1 (0xE2ABC3F8,0x00000002,0x00000000,0xBAE565AB)

\*\*\* myfault.sys - Address BAE565AB base at BAE56000, Datestamp 4f806ca0

Beginning dump of physical memory  
Physical memory dump complete.  
Contact your system administrator or technical support group for further assistance.

Imagen 38 BOSD (Blue Screen Of Death)



Una vez obtenido el volcado de memoria se ha de realizar el hash del archivo obtenido. En Windows, tenemos distintas herramientas que permiten obtener distintos hashes de un fichero, como son: HashMyFiles o HashCalc

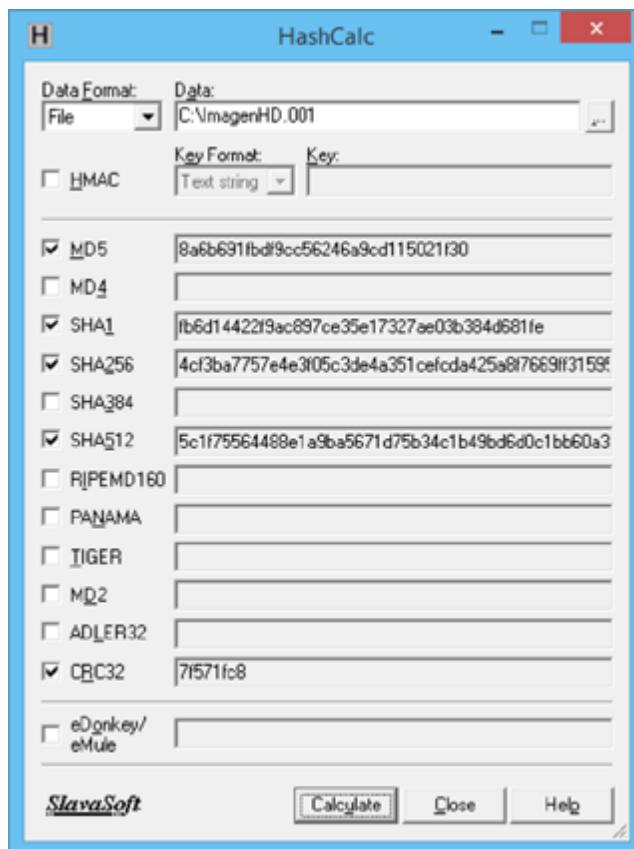


Imagen 39 HashCalc - Cálculo de hashes

Para la adquisición de la memoria virtual, se puede realizar de dos formas: o través de herramientas específicas como FTKImager o como posteriormente realizaremos un volcado de disco completo, en ese volcado de disco también se copia el archivo pagefile.sys que como hemos visto anteriormente corresponde con la memoria virtual.

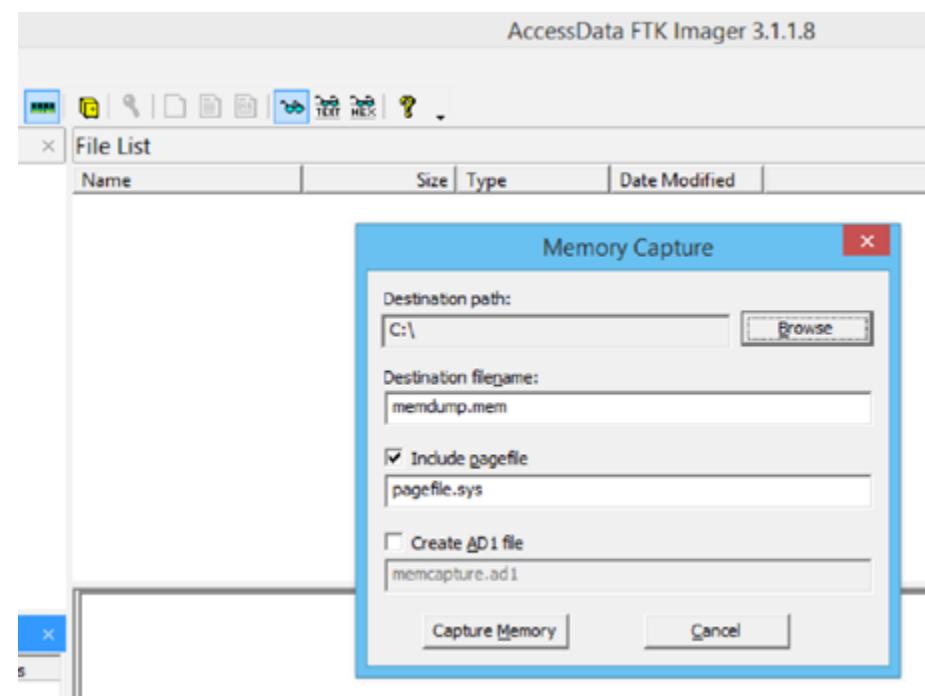


Imagen 40 FTK Imager - Volcado pagefile.sys

Otra forma de poder realizar el volcado de memoria es mediante la herramienta ManTech Memory DD (mdd) la cual se encarga de generar un volcado de la memoria física del sistema y almacenarla en un fichero binario en crudo o raw.

```
C:\>dd_1.3.exe -o imagen.ing
-> mdd
-> ManTech Physical Memory Dump Utility
  Copyright <C> 2008 ManTech Security & Mission Assurance
-> This program comes with ABSOLUTELY NO WARRANTY: for details use option `--help'.
  This is free software, and you are welcome to redistribute it
  under certain conditions; use option `--c' for details.
-> Dumping 2047.48 MB of physical memory to file 'imagen.ing'.

524156 map operations succeeded (1.00)
0 map operations failed

took 68 seconds to write
MD5 is: 7fb2cc94d6f38a9bd535a70dbefa5400
```

Imagen 41 ManTech Memory DD (mdd)

Una vez realizado el volcado de memoria, con la herramienta que mejor se adapte al incidente en concreto, se procedería a analizar el volcado con herramientas como Yara o Volatility, entre otras, para la búsqueda de las evidencias que nos ayuden en nuestra investigación.

Una vez recopilada la información volátil mediante las herramientas vistas anteriormente pasaremos a la recolección de la información no volátil mediante un volcado de disco.

Debido al volumen de los discos el proceso podría llevarnos mucho tiempo e incluso la utilización de muchos recursos, veremos varias formas de poder realizar la adquisición o volcado de discos.

La copia bit a bit de disco es un método rápido y que permite realizar tantas copias como se necesiten. Podemos utilizar varias herramientas como FTK Imager, OSForensics, WinDD, Clonezilla,....

FTK Imager, ya sea en su versión gráfica o en línea de comandos, software de AccessData es una herramienta para realizar copias y visualización previa de datos, la cual permite una evaluación rápida de la evidencia. También puede crear copias iguales (imágenes forenses) sin realizar cambios en la evidencia original.

Mediante la herramienta gráfica seleccionaríamos la opción de "Create Disk Image" y seguiríamos los pasos siguientes:

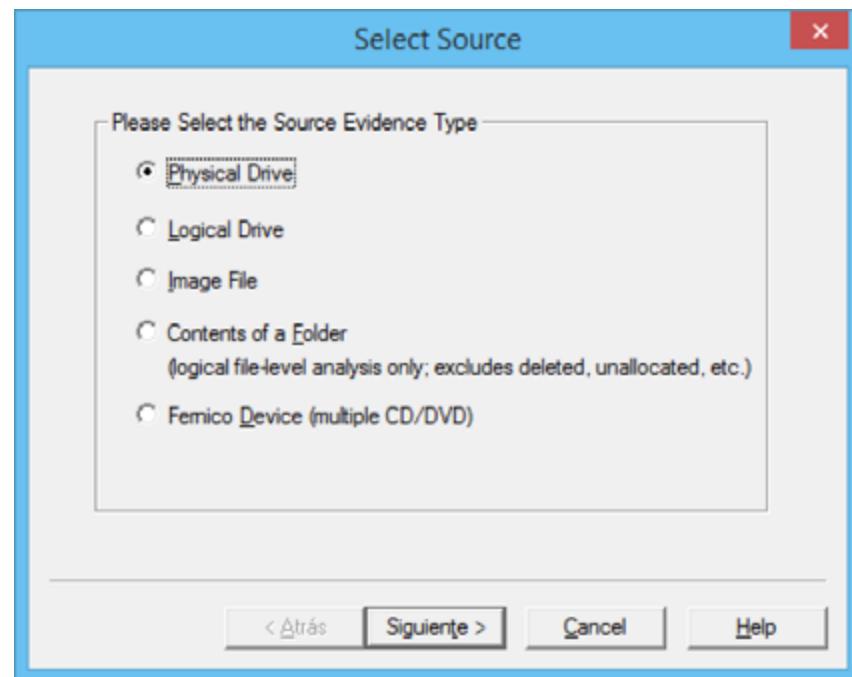


Imagen 42 FTK Imager - Volcado disco – Select Source

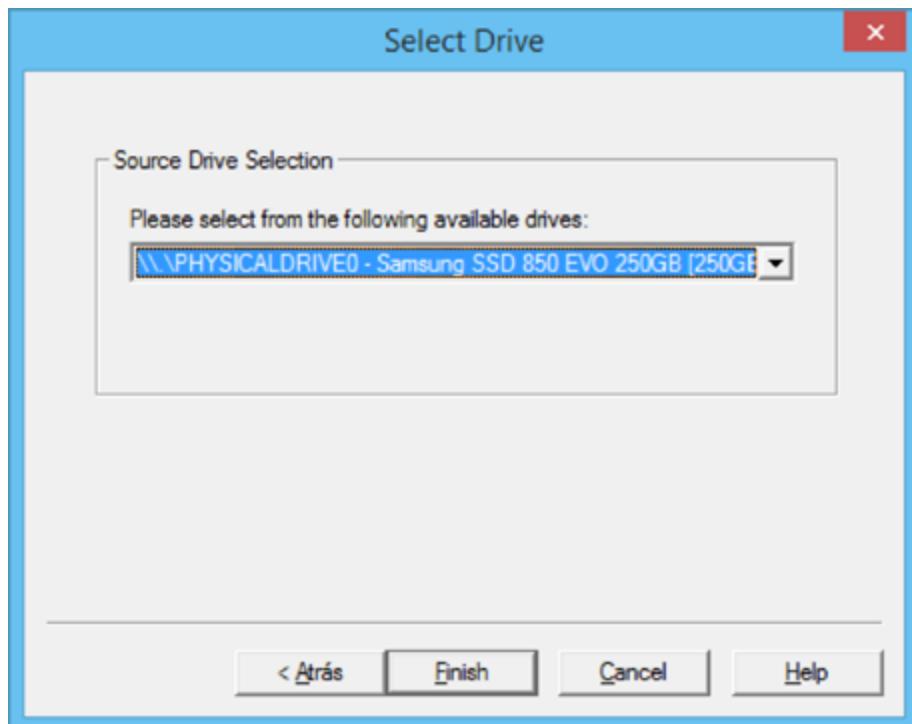


Imagen 43 FTK Imager - Volcado disco – Select Drive

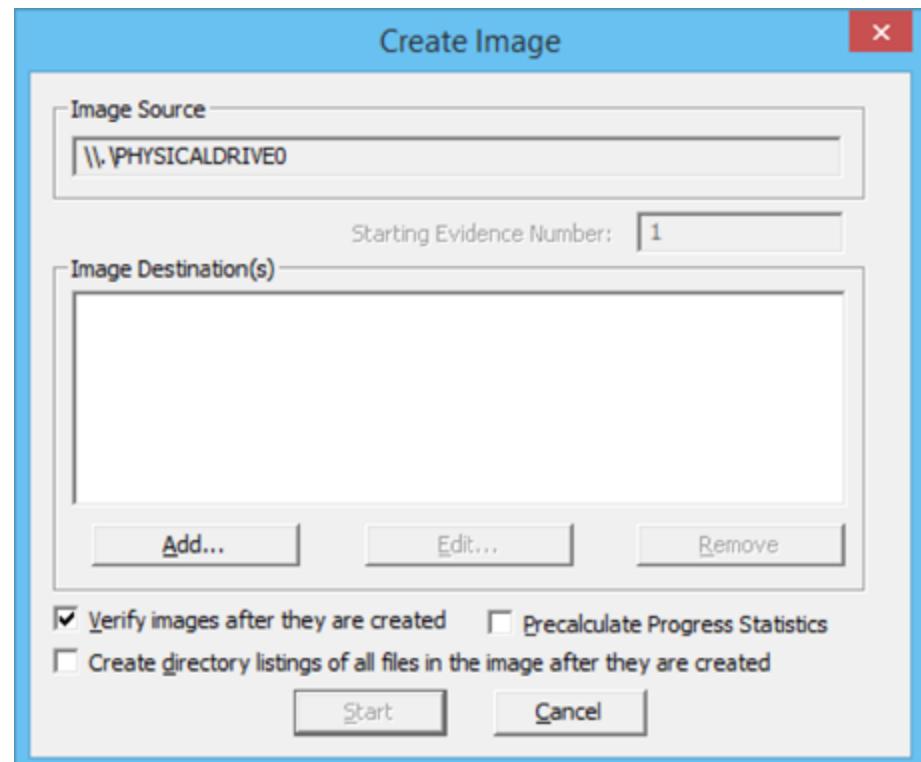


Imagen 44 FTK Imager - Volcado disco – Create Image

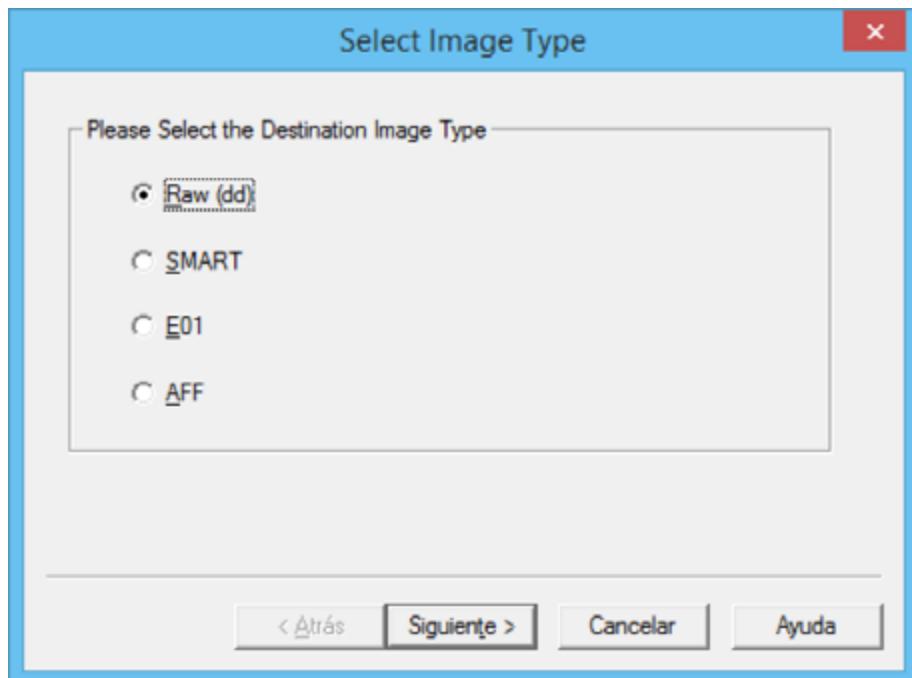


Imagen 45 FTK Imager - Volcado disco – Select Image Type

The dialog box has a blue header bar with the title "Evidence Item Information". It contains five input fields with labels: "Case Number" (value 1), "Evidence Number" (value 25), "Unique Description" (empty), "Examiner" (value Raul), and "Notes" (empty). At the bottom are buttons for "< Atrás", "Siguiente >", "Cancel", and "Help".

Imagen 46 FTK Imager - Volcado disco - Evidence Item Information



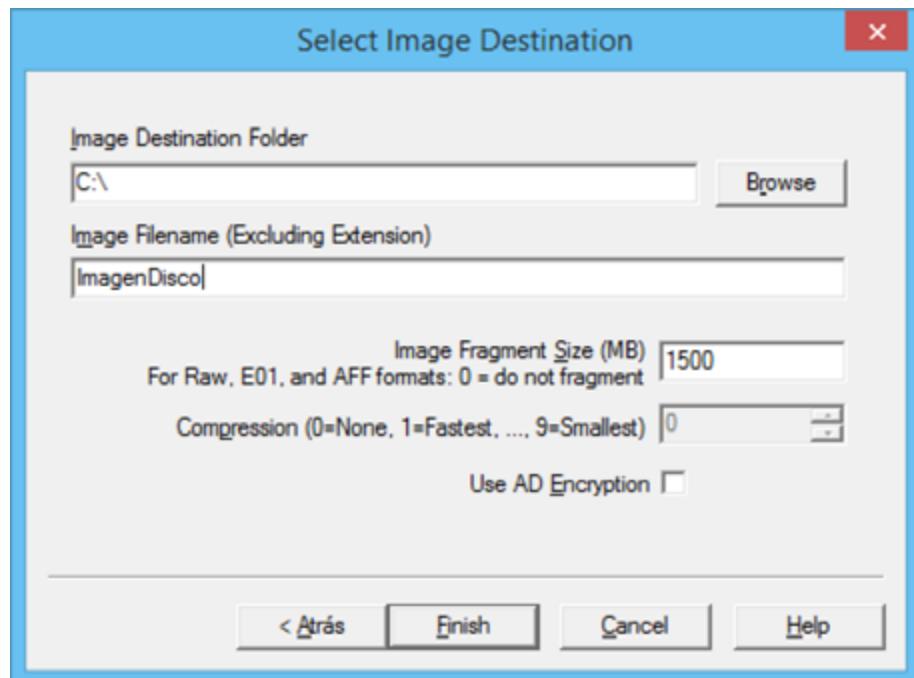


Imagen 47 FTK Imager - Volcado disco - Select Image Destination

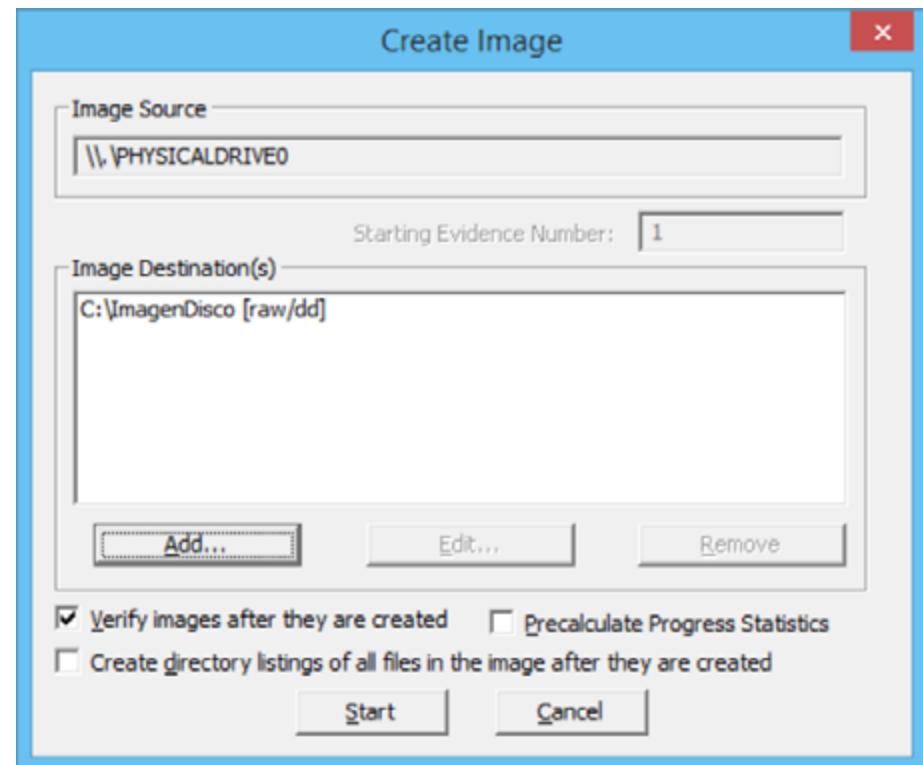
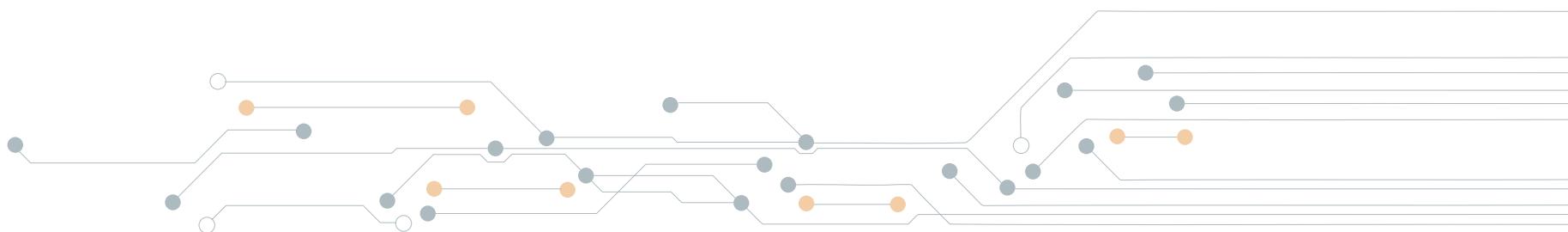


Imagen 48 FTK Imager - Volcado disco - Start



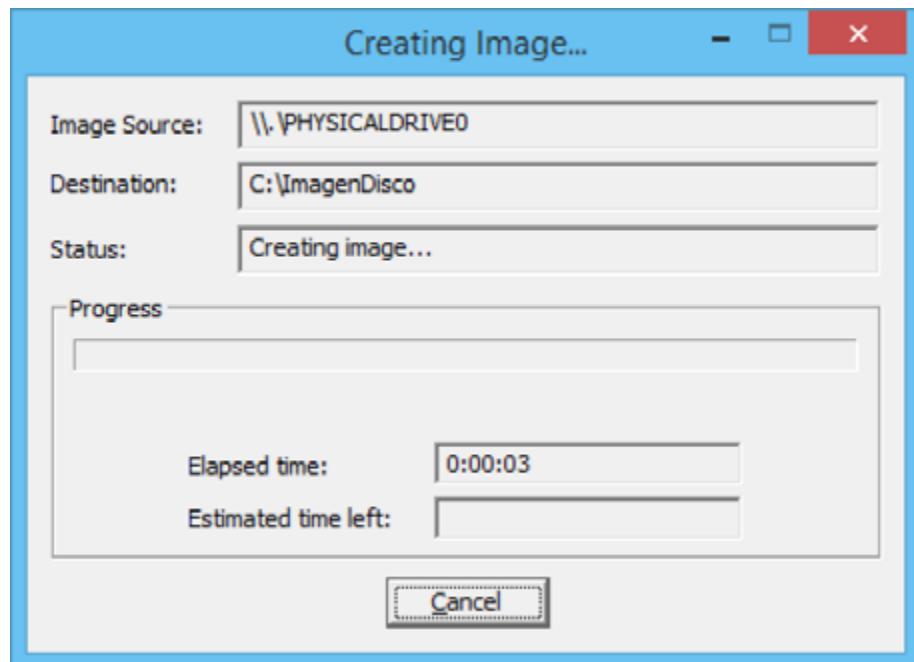
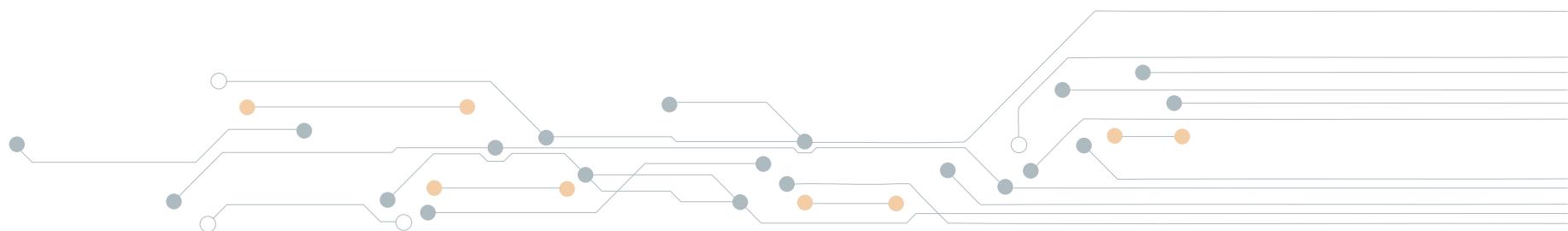


Imagen 49 FTK Imager - Volcado disco - Creating image



Para realizar la imagen desde la línea de comandos escribimos la siguiente instrucción, con la que realizaríamos la imagen del disco físico 0 en la unidad F y verificaría el proceso.

```
ftkimager.exe \\.\PHYSICALDRIVE0 f:\ImagenHD --verify
```

```
c:\Users\Raul\ftkimager>ftkimager.exe \\.\PHYSICALDRIVE0 c:\ImagenHD --verify
AccessData FTK Imager v3.1.1 CLI <Aug 20 2012>
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.

Creating image...
90,00 / 238475,18 MB (45,00 MB/sec) - 1:28:17 left
```

Imagen 50 FTK Imager - Línea de comandos

Con la siguiente instrucción realizaríamos un listado de las unidades disponibles:

```
ftkimager.exe --list-drives
```

```
c:\Users\Raul\ftkimager>ftkimager --list-drives
AccessData FTK Imager v3.1.1 CLI <Aug 20 2012>
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.

\\.\PHYSICALDRIVE0 - Samsung SSD 850 EVO 250GB [250GB IDE]
```

Imagen 51 FTK Imager - Línea de comandos - Listado Unidades



Otra forma de poder realizar el volcado de la imagen de disco sería con el framework OSForensics. Seleccionaremos "Drive Imaging". Seleccionar la unidad o partición de la que realizar la copia, además

del destino de la imagen, siempre en una unidad externa al sistema y formateada a bajo nivel (todo a 0).

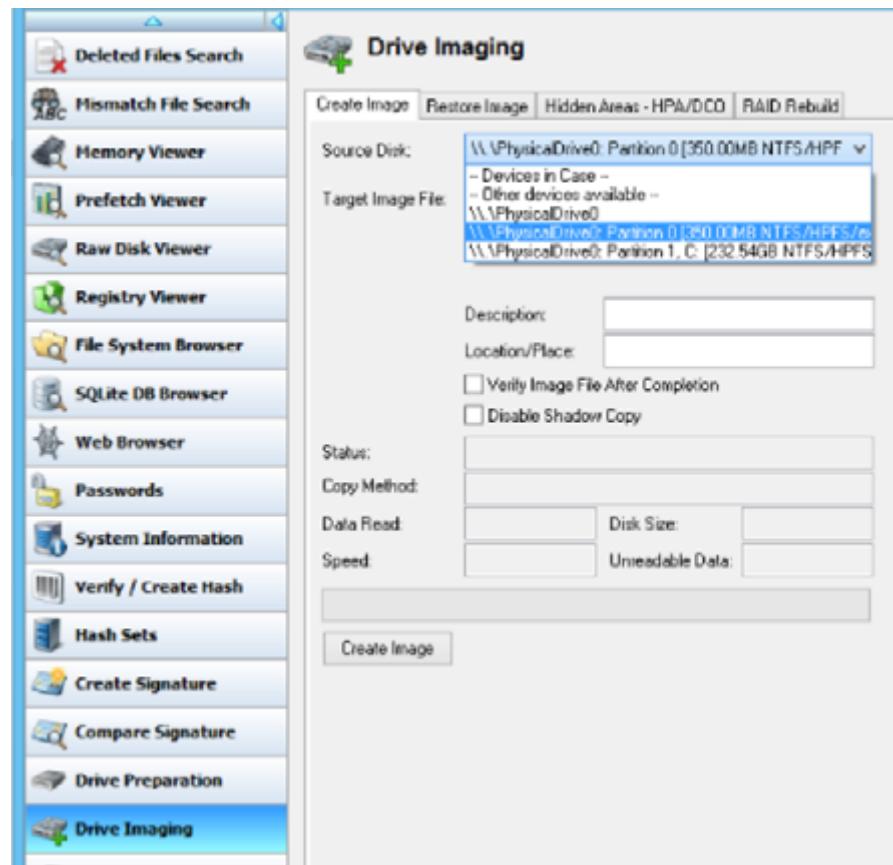


Imagen 52 OSForensics - Volcado de disco - Source Disk

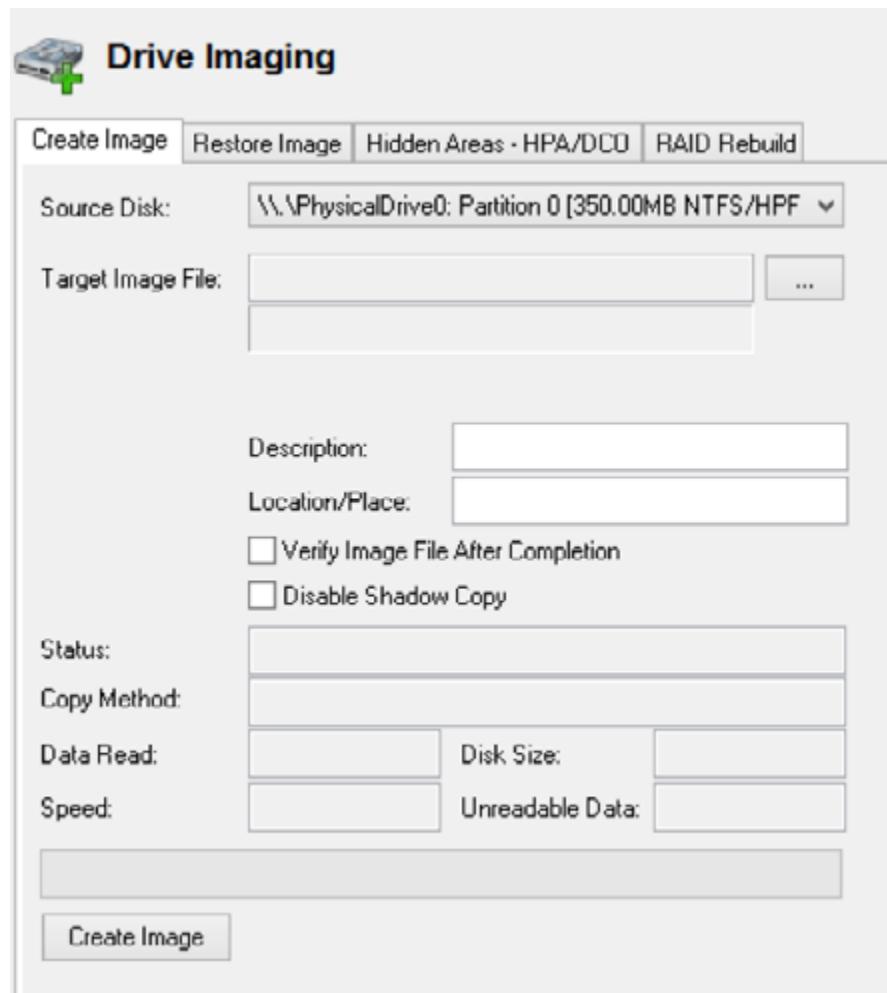


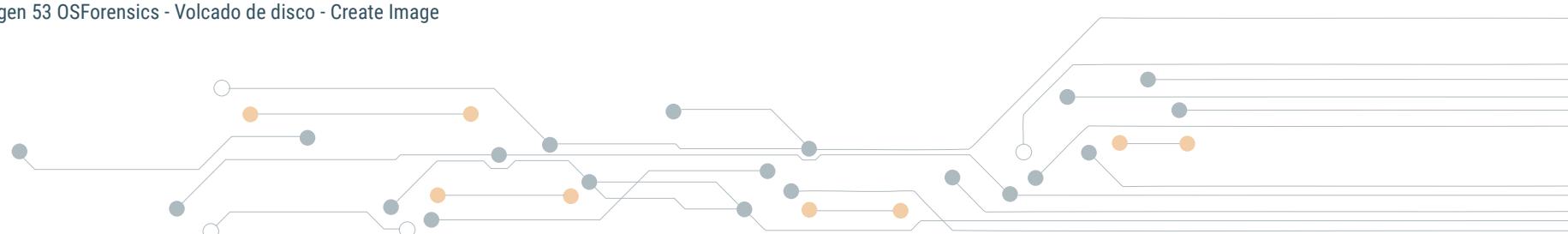
Imagen 53 OSForensics - Volcado de disco - Create Image

Los discos SSD no funcionan de la misma manera que los discos tradicionales. Los fabricantes crearon el comando TRIM para alargar la vida útil de los SSD informando qué celdas ya no están en uso al controlador, notificando al recolector de basura que el contenido de esas celdas y las prepare para futuras operaciones de escritura. No es posible evitar el proceso de recolección de basura en el caso de que el comando TRIM esté activado ya que un disco SSD únicamente con tener corriente iniciará dicho proceso de manera automática.

Si un usuario elimina un archivo y TRIM está activado la evidencia desaparecerá. Esto afecta a la hora de calcular el hash, el cual puede ser distinto cada vez, porque el proceso que desencadena el comando TRIM se ejecuta en un segundo plano y aunque aparentemente no haya sufrido ninguna modificación, en realidad sí que ha habido cambios.

Existen multitud de herramientas que permiten realizar la copia, volcado o imagen de los discos. Hemos visto algunas, pero sería interesante que se investigue y trabaje con varias, ya que dependiendo del incidente sería conveniente utilizar una herramienta u otra.

Muy importante, siempre, es realizar el cálculo de hashes de cualquier evidencia obtenida para garantizar la autenticidad e integridad de la misma, rellenando en su caso el documento de la cadena de custodia correspondiente.



Telefónica EDUCACIÓN DIGITAL