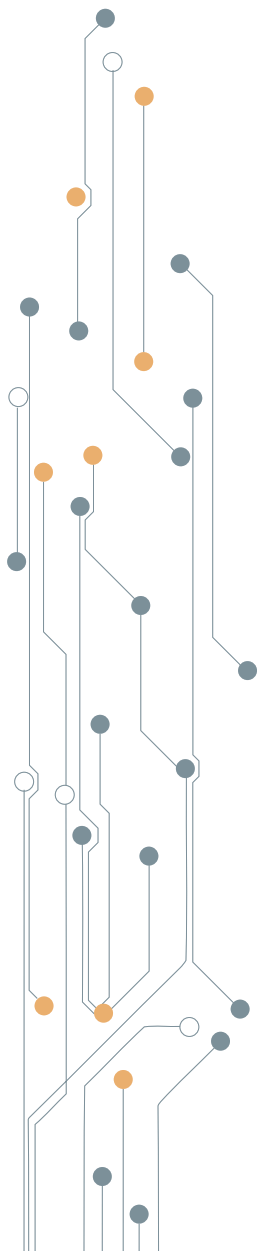




Gestión y análisis de logs de Windows

Índice



1 | Gestión y análisis de logs deWindows

3

1. Gestión y análisis de logs de Windows

En temas anteriores ya hemos visto cómo se gestiona y se analiza algunos de los logs más importantes de Windows, a continuación, mostramos una lista de logs a tener en cuenta a la hora de realizar un análisis forense, a completar de los vistos.

```
%WINDIR%\setupact.log
```

Información sobre las acciones llevadas a cabo durante la instalación. Obtenemos fechas de instalación, propiedades de programas instalados, rutas de acceso, copias legales, discos de instalación...

```
%WINDIR%\setuperr.log
```

Información sobre los errores producidos durante la instalación. Obtenemos fallos de programas, rutas de red inaccesibles, rutas a volcados de memoria...

```
%WINDIR%\WindowsUpdate.log
```

Información de transacción sobre la actualización del sistema y las aplicaciones. Obtenemos tipos de hotfix instalados, fechas de instalación, elementos por actualizar...

```
%WINDIR%\Debug\mrt.log
```

Información sobre la eliminación de software malintencionado de Windows. Obtenemos fechas, versión del motor, firmas y resumen de actividad.

```
%WINDIR%\security\logs\scecomp.old
```

Información sobre los componentes de Windows que no han podido ser instalados. Obtenemos DLL's no registradas, fechas, intentos de escritura, rutas de acceso...

```
%WINDIR%\SoftwareDistribution\ReportingEvents.log
```

Información de los eventos relacionados con el proceso de actualización. Obtenemos agentes de instalación, descargas incompletas o finalizadas, fechas, tipos de paquetes, rutas...

```
%WINDIR%\Logs\CBS\CBS.log
```

Información sobre los ficheros pertenecientes a 'Windows Resource Protection' y que no se han podido restaurar. Obtenemos el proveedor de almacenamiento, PID de procesos, fechas, rutas...

```
%AppData%\Local\Microsoft\Websetup (Windows 8)
```

Información sobre la fase de instalación web de Windows 8. Obtenemos URLs de acceso, fases de instalación, fechas de creación, paquetes de programas...

```
%AppData%\setupapi.log
```

Información de las unidades, services pack y hotfixes instalados. Obtenemos las unidades locales y extraíbles, programas de instalación, programas instalados, actualizaciones de seguridad, reconocimiento de dispositivos conectados...

```
%SYSTEMROOT%\$Windows.~BT\Sources\Panther\*.log.xml  
%WINDIR%\PANTHER\*.log.xml
```

Información de las acciones, errores y estructuras de SID cuando se realiza el proceso de actualización desde versión anterior de Windows. Obtenemos fechas, rutas, errores, medio de instalación, dispositivos, versiones, reinicio, dispositivos PnP...

```
%WINDIR%\INF\setupapi.dev.log
```

Información sobre las unidades Plug and Play y la instalación de drivers. Obtenemos la versión del SO, Kernel, Service Pack, arquitectura, modo de inicio, fechas, rutas, lista de drivers, dispositivos conectados, dispositivos iniciados o parados...

```
%WINDIR%\INF\setupapi.app.log
```

Información del registro de instalación de las aplicaciones. Obtenemos fechas, rutas, sistema operativo, versiones, ficheros, firma digital, dispositivos...

```
%WINDIR%\Performance\Winsat\winsat.log
```

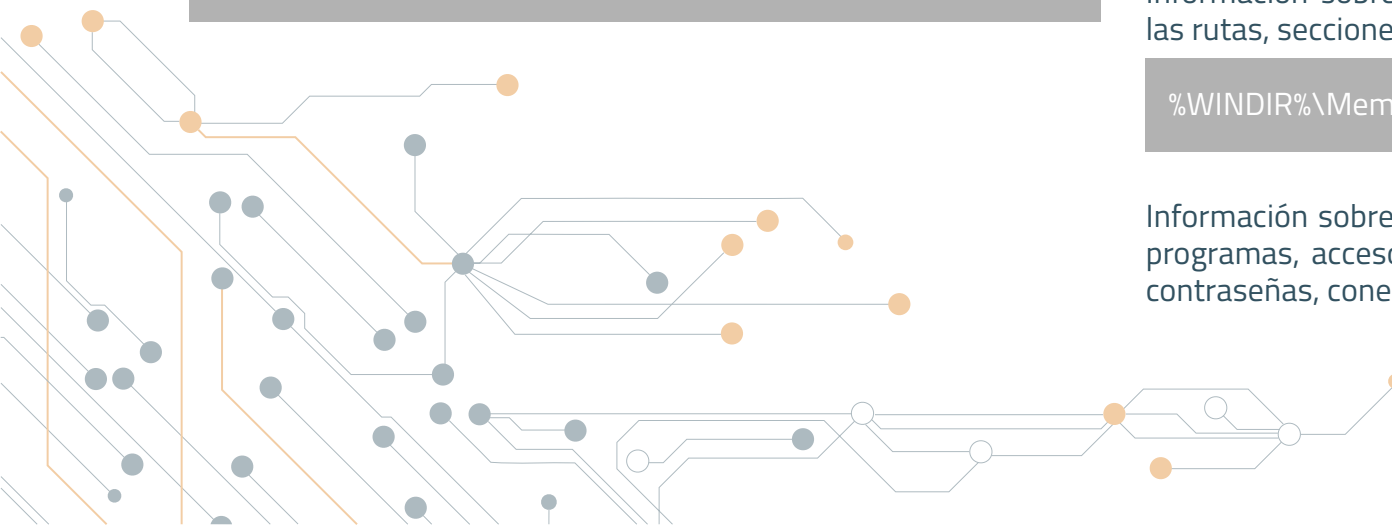
Información sobre las trazas de utilización de la aplicación WINSAT que miden el rendimiento del sistema. Obtenemos las fechas, valores sobre la tarjeta gráfica, CPU, velocidades, puertos USB...

```
*.INI
```

Información sobre las configuraciones de programas. Obtenemos las rutas, secciones, parámetros de usuarios...

```
%WINDIR%\Memory.dmp
```

Información sobre los volcados de memoria. Obtenemos las rutas, programas, accesos, direcciones de memoria, listado de usuarios, contraseñas, conexiones...



Volume Shadow Copy

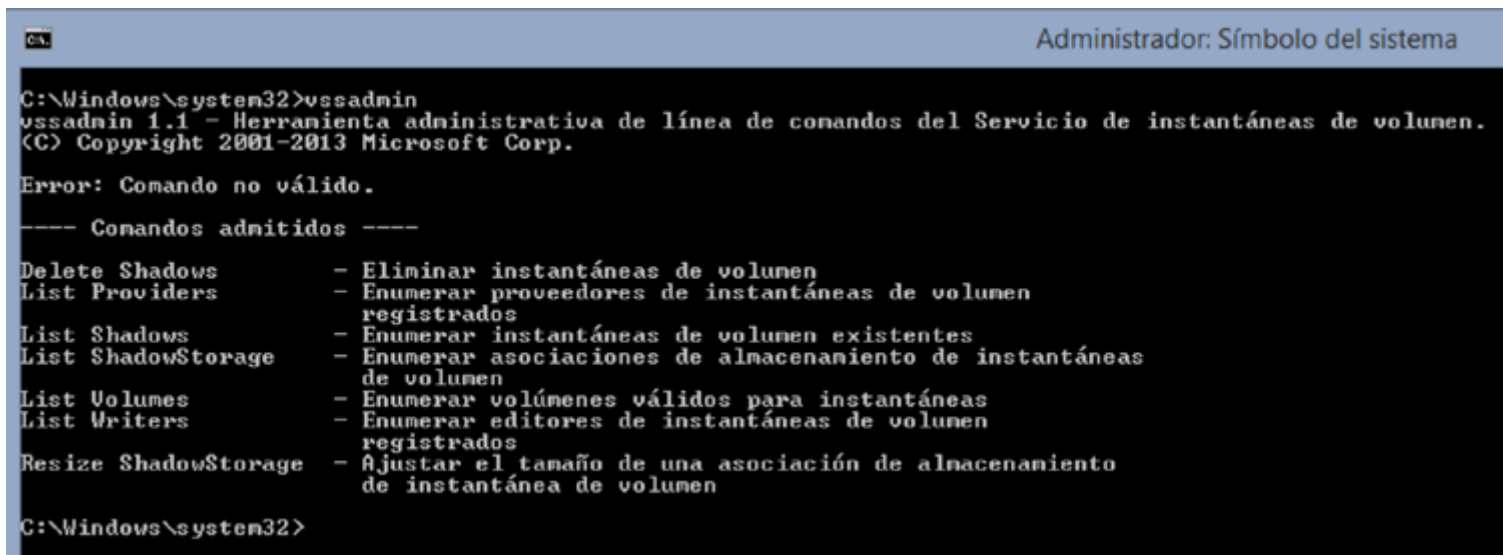
Es el servicio que permite crear copias de seguridad cada cierto tiempo de nuestra computadora, y así, poder restaurar el sistema en caso de fallo general o en caso de que el usuario decida. En Windows se le conoce como “punto de restauración del sistema”.

VSC crea copias ocultas de cada uno de los bloques de 16k que recibe una variación y/o cambio de estado en la partición NTFS del disco duro. Este servicio realiza las copias de seguridad ocultas cada vez que ocurre una variación en el sistema como fruto de la instalación y/o actualización de un software / aplicación. Por defecto, en la mayoría de Windows Volume Shadow Copy se encuentra activo y funcionando por defecto. Esto en parte se debe a que se tiene activado el sistema de protección del Sistema, o lo que es lo mismo, el servicio de “creación de puntos de restauración”.

Podríamos utilizar los volúmenes (VSC) para ocultar elementos malware en el sistema, acceder a los archivos protegidos del sistema operativo y encontrar archivos antiguos, que fueron eliminados hace tiempo.

Existen varias formas de poder manejar los VSC, a través de herramientas por consola o terminal, o mediante interfaces gráficas que facilitan el uso de estos volúmenes.

- *vssadmin*: herramienta administrativa del Servicio de Volume Shadow Snapshots (VSS), que permite administrar dichos volúmenes. Con el comando *vssadmin list shadows* muestra las instantáneas realizadas.



```
C:\Windows\system32>vssadmin
vssadmin 1.1 - Herramienta administrativa de línea de comandos del Servicio de instantáneas de volumen.
(C) Copyright 2001-2013 Microsoft Corp.

Error: Comando no válido.

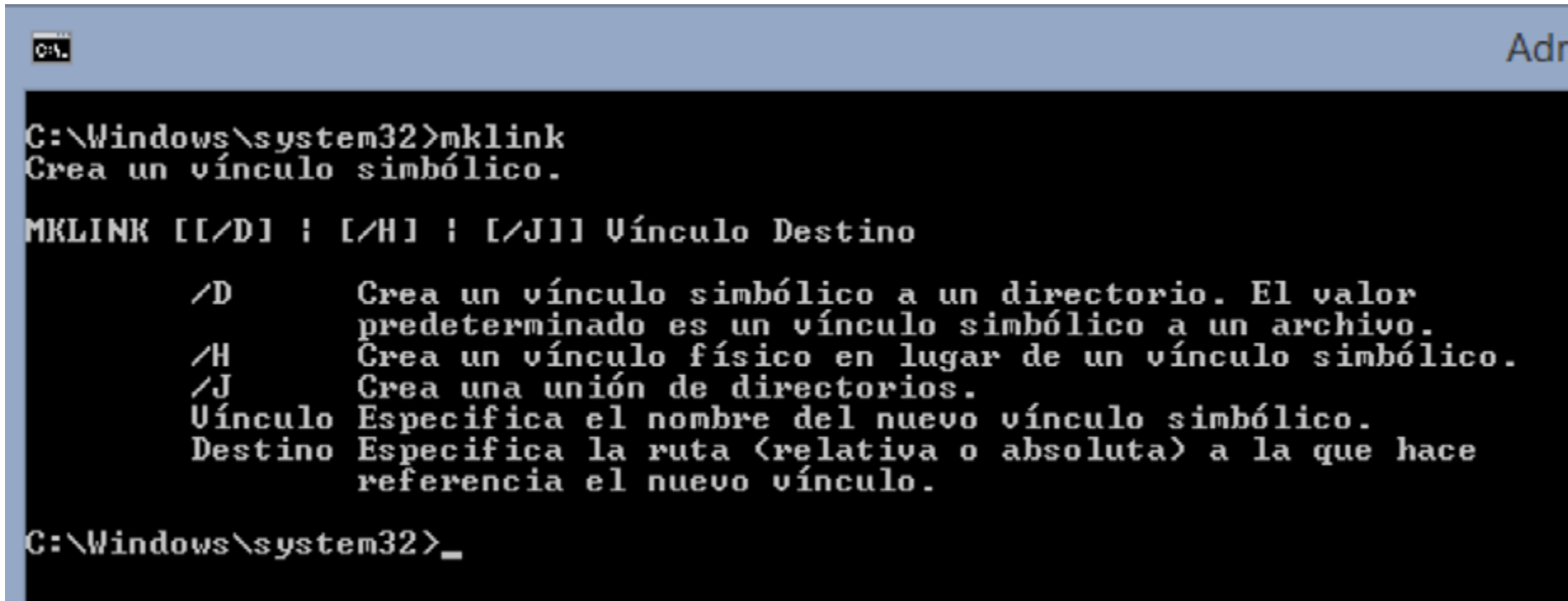
---- Comandos admitidos ----

Delete Shadows      - Eliminar instantáneas de volumen
List Providers      - Enumerar proveedores de instantáneas de volumen
                    registrados
List Shadows         - Enumerar instantáneas de volumen existentes
List ShadowStorage   - Enumerar asociaciones de almacenamiento de instantáneas
                    de volumen
List Volumes         - Enumerar volúmenes válidos para instantáneas
List Writers         - Enumerar editores de instantáneas de volumen
                    registrados
Resize ShadowStorage - Ajustar el tamaño de una asociación de almacenamiento
                    de instantánea de volumen

C:\Windows\system32>
```

Imagen 98 vssadmin

- *mklink*: se utiliza para crear un vínculo simbólico con un volumen VSC.



```

C:\Windows\system32>mklink
Crea un vínculo simbólico.

MKLINK [[/D] : [/H] : [/J]] Vínculo Destino

    /D      Crea un vínculo simbólico a un directorio. El valor
             predeterminado es un vínculo simbólico a un archivo.
    /H      Crea un vínculo físico en lugar de un vínculo simbólico.
    /J      Crea una unión de directorios.
    Vínculo Especifica el nombre del nuevo vínculo simbólico.
    Destino Especifica la ruta <relativa o absoluta> a la que hace
             referencia el nuevo vínculo.

C:\Windows\system32>_
  
```

Imagen 99 mklink

Una vez se ha creado un enlace simbólico al volumen oculto en cuestión, se tiene pleno acceso al contenido almacenado en él, pudiendo realizar todo tipo de acciones.

Existen otras herramientas que permiten navegar de forma gráfica por los volúmenes ocultos (VSC) como pueden ser The Sleuth Kit (Autopsy) o VSC Toolset.

VSC Toolset, permite identificar los volúmenes existentes, y navegar por el sistema de ficheros de dichos volúmenes a través de una interfaz gráfica muy intuitiva. Para poder trabajar se necesitan permisos de administrador.

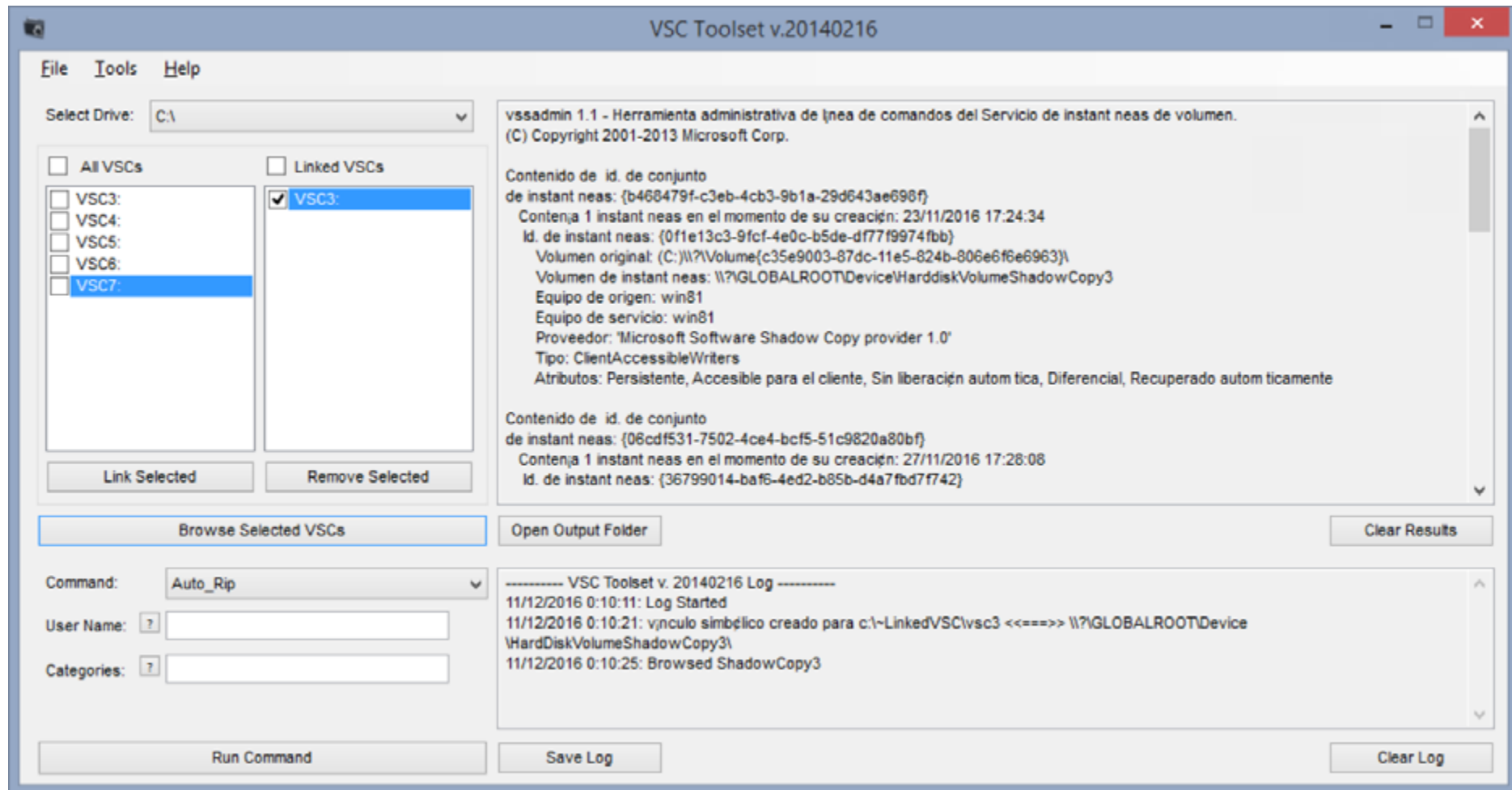
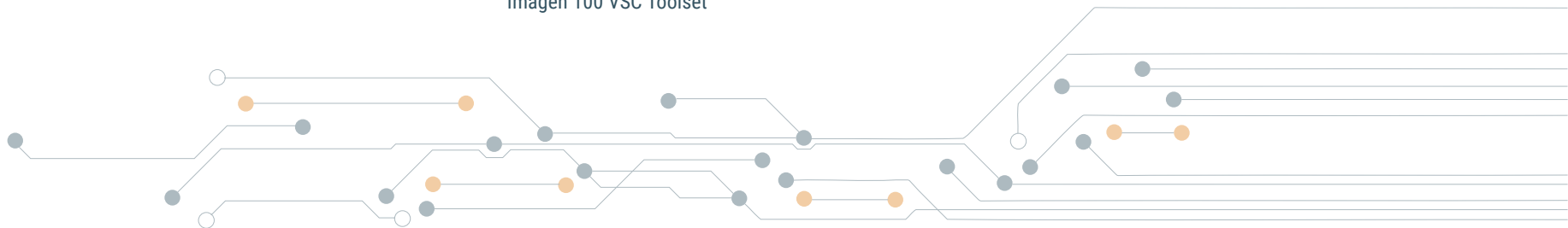


Imagen 100 VSC Toolset



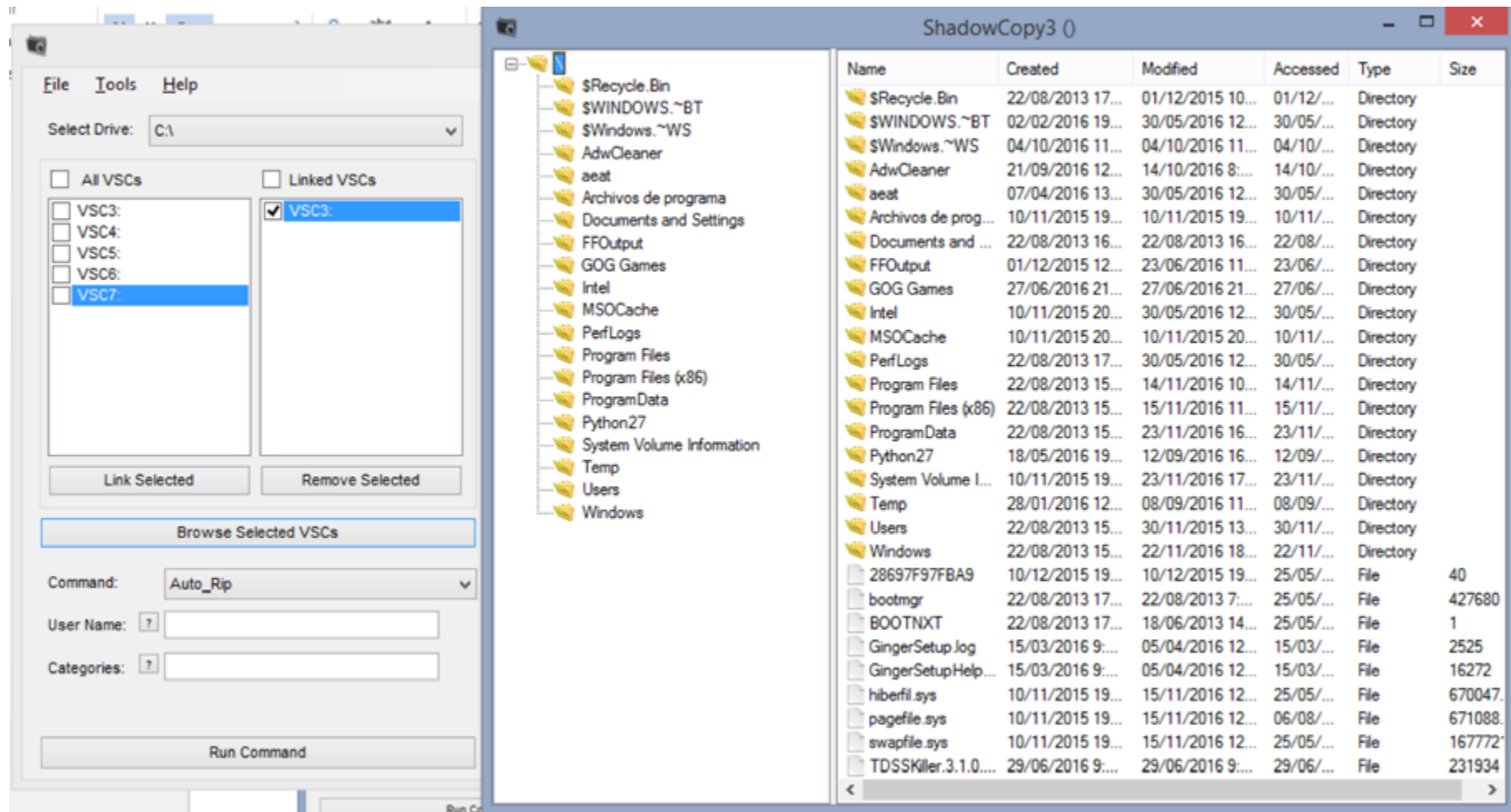
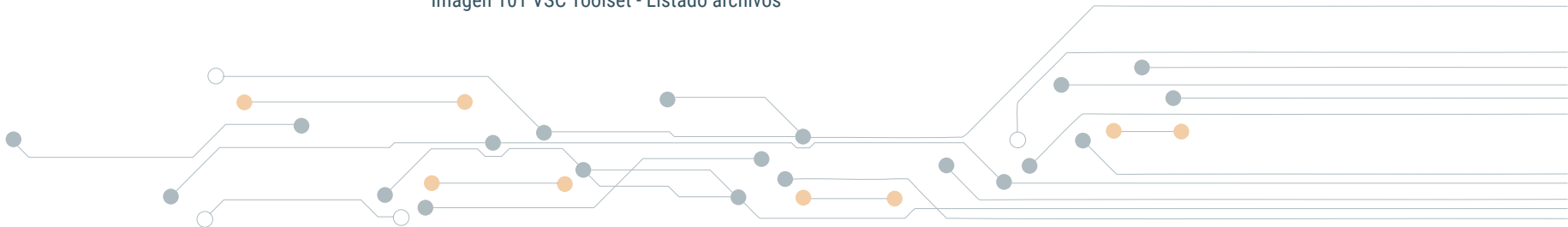


Imagen 101 VSC Toolset - Listado archivos



Telefonica EDUCACIÓN DIGITAL