

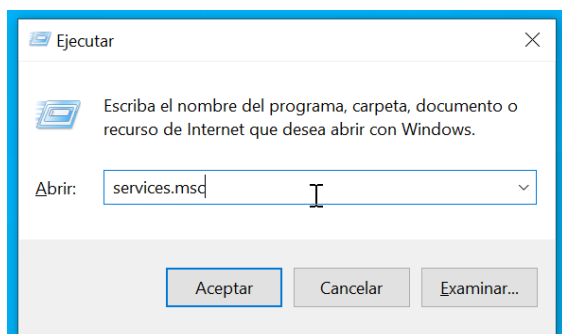
## Practica 2

# Shadow Copy

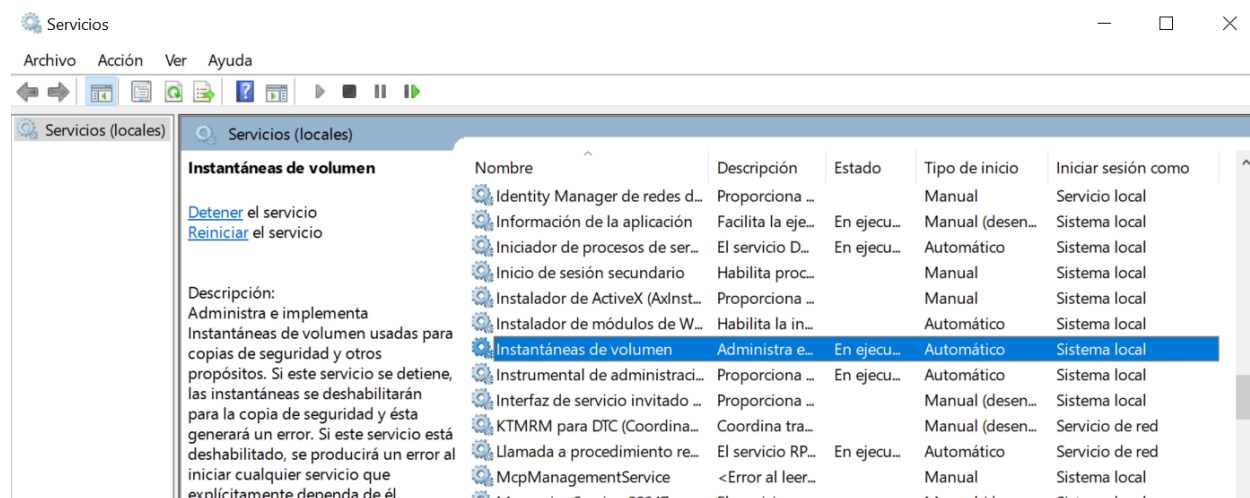
En esta práctica, nos enfocaremos en los puntos de restauración de Windows, también conocidos como **'Shadow Copy'**. Para comenzar, agregaremos un disco a nuestro sistema Windows 10 con un tamaño igual o superior al del sistema actual.

Para iniciar el trabajo con los puntos de restauración, primero activaremos este servicio. Para hacerlo, presionamos **'Win + R'**, ingresamos **'services.msc'** y ejecutamos el comando.

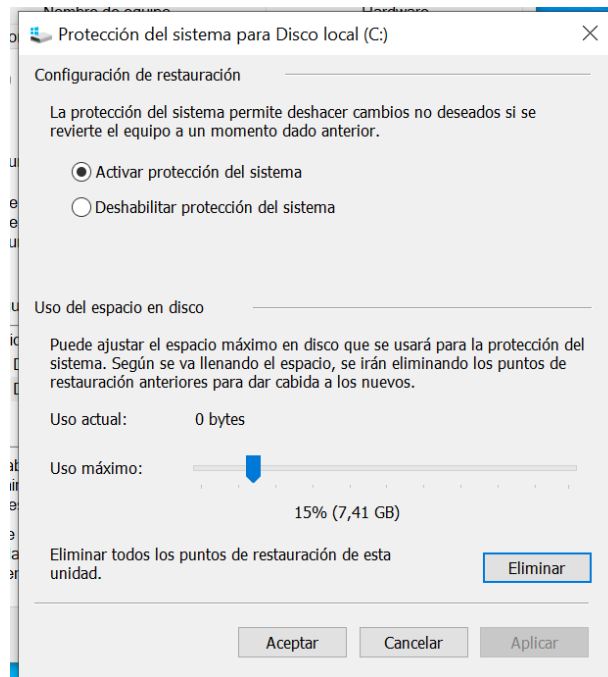
<b>Disco 0</b> Básico 50,00 GB En pantalla	<b>Reservado para e</b> 50 MB NTFS Correcto (Sistema,	<b>(C:)</b> 49,42 GB NTFS Correcto (Arranque
<b>Disco 1</b> Básico 55,00 GB En pantalla	<b>(E:)</b> 55,00 GB NTFS Correcto (Partición primaria)	



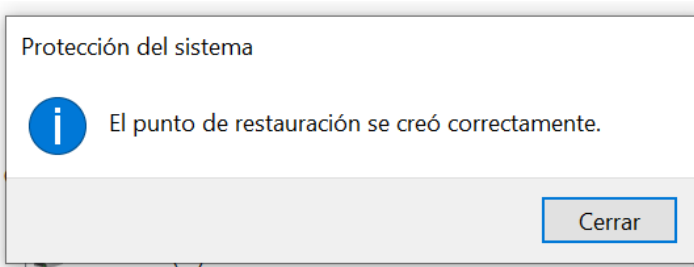
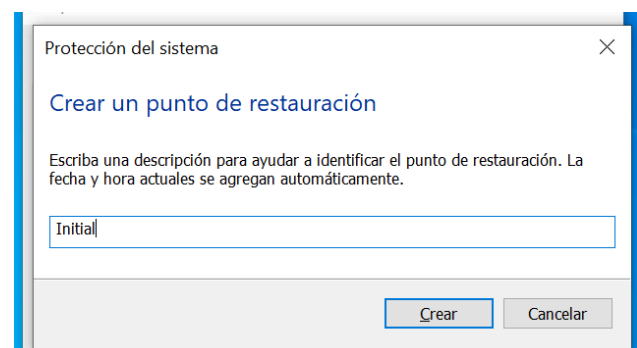
Se abrirá una ventana donde deberemos buscar **'Instantáneas de volumen'** y asegurarnos de que esté en estado de ejecución, con el tipo de inicio configurado como automático



Una vez completado este paso, procedemos a buscar '**Crear punto de restauración**' y configuramos la protección del sistema. En este punto, es suficiente asignar un 5% o 10% del tamaño de nuestro disco para la protección.



Ahora que hemos habilitado el botón '**Crear**', podemos generar instantáneas. En este caso, procederé a crear un par de ellas



Puedes verificar la configuración de los puntos de restauración desde la ventana de comandos de Windows utilizando el comando '**vssadmin list shadowstorage**'.

```
C:\> Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.2965]
(c) Microsoft Corporation. Todos los derechos reservados.

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

Asociación de almacenamiento de instantáneas
Para el volumen: (C:)\?\Volume{4bef3153-0000-0000-0000-300300000000}\
Volumen de almacenamiento de instantáneas: (C:)\?\Volume{4bef3153-0000-0000-0000-300300000000}\
Espacio de almacenamiento de instantáneas usado: 42,4 MB (0%)
Espacio asignado para el almacenamiento de instantáneas: 352 MB (0%)
Espacio máximo de almacenamiento de instantáneas: 7,41 GB (15%)
```

Al ir a '**Crear puntos de restauración > Restaurar**', podremos revisar los puntos de restauración que hemos creado.

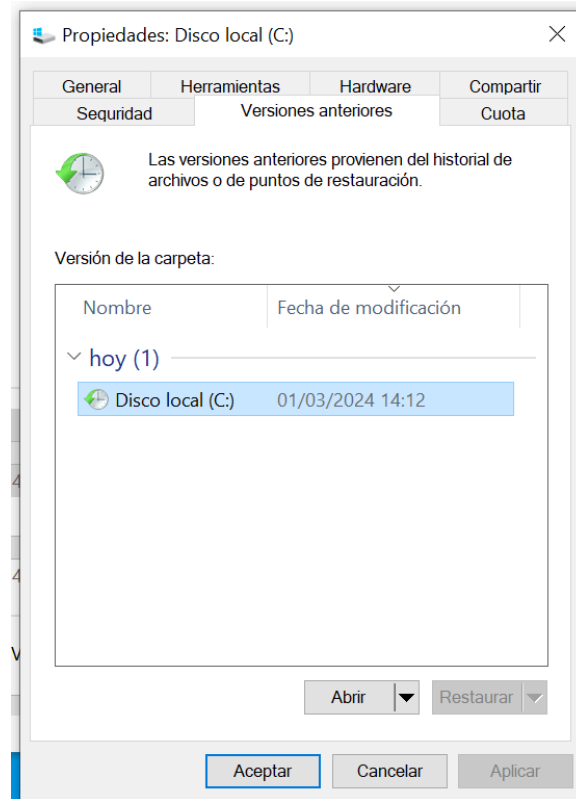
Restaurar sistema

Restaurar el equipo al estado anterior al evento seleccionado

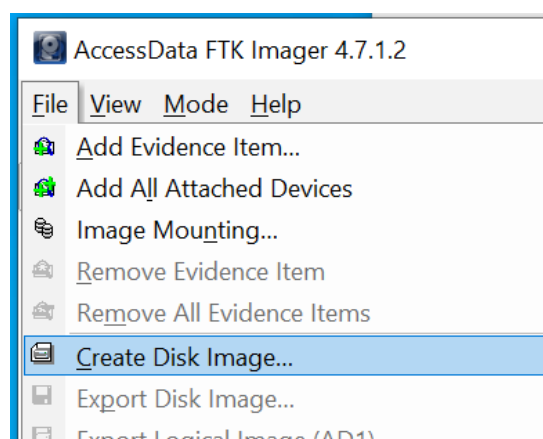
Zona horaria actual: Hora estándar romance

Fecha y hora	Descripción	Tipo
01/03/2024 14:05:42	Install VLC Media Player	Manual
01/03/2024 13:58:54	Install Chrome	Manual
01/03/2024 13:47:00	Install Firefox	Manual
01/03/2024 13:27:41	Initial	Manual

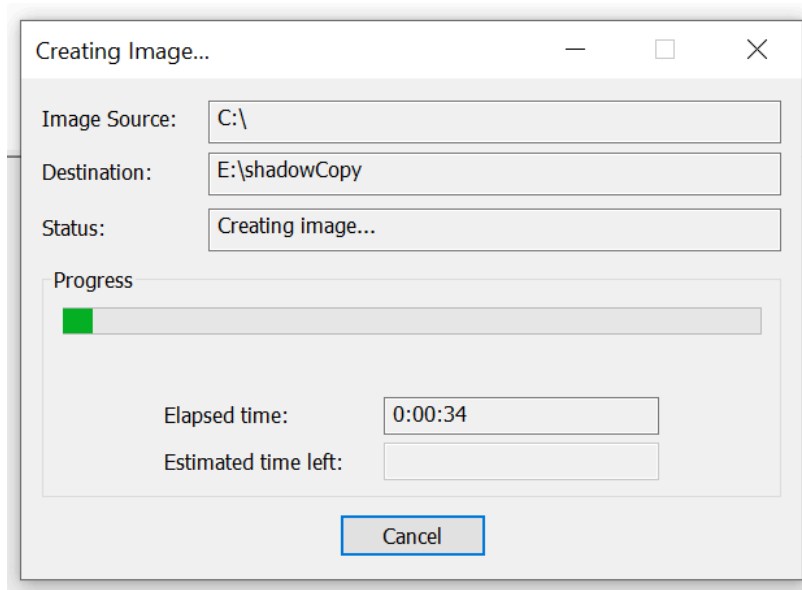
Al ir a '**Equipo > Menú contextual en el volumen > Propiedades > Versiones anteriores**', podrás verificar las versiones anteriores del sistema.





Ahora, procederemos a crear una imagen del disco que incluirá estos puntos de restauración y la guardaremos en el disco que agregamos inicialmente. Para llevar a cabo esta tarea, utilizaremos FTK Imager, yendo a '**File > Create Disk Image**'.





Proseguimos con los mismos pasos que hemos aplicado en prácticas anteriores para la creación de la imagen.

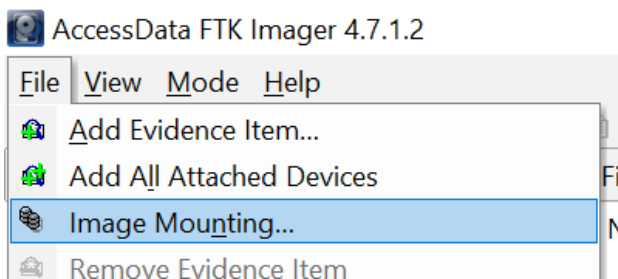


Finalmente obtendremos la imagen del sistema.

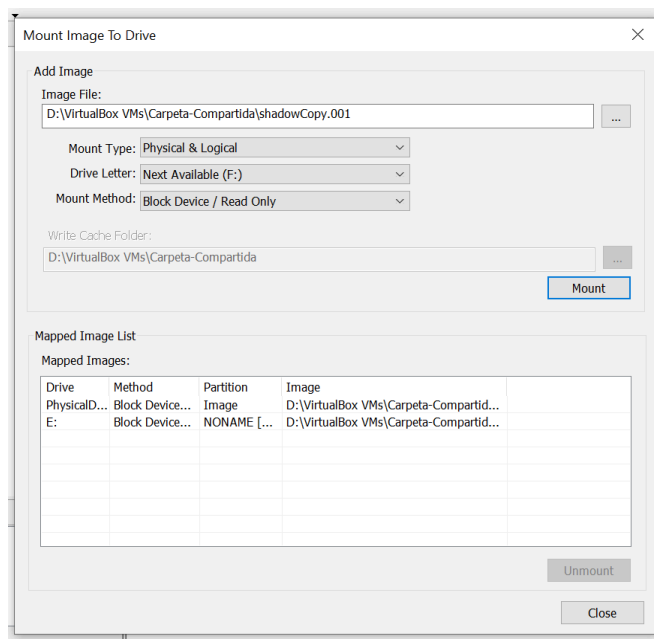
equipo > Disco local (E:)   Buscar en Disco local (E:)

Nombre	Fecha de modificación	Tipo	Tamaño
 shadowCopy.001	05/03/2024 22:28	Archivo 001	51.826.055 KB
 shadowCopy.001	05/03/2024 22:37	Documento de texto	2 KB

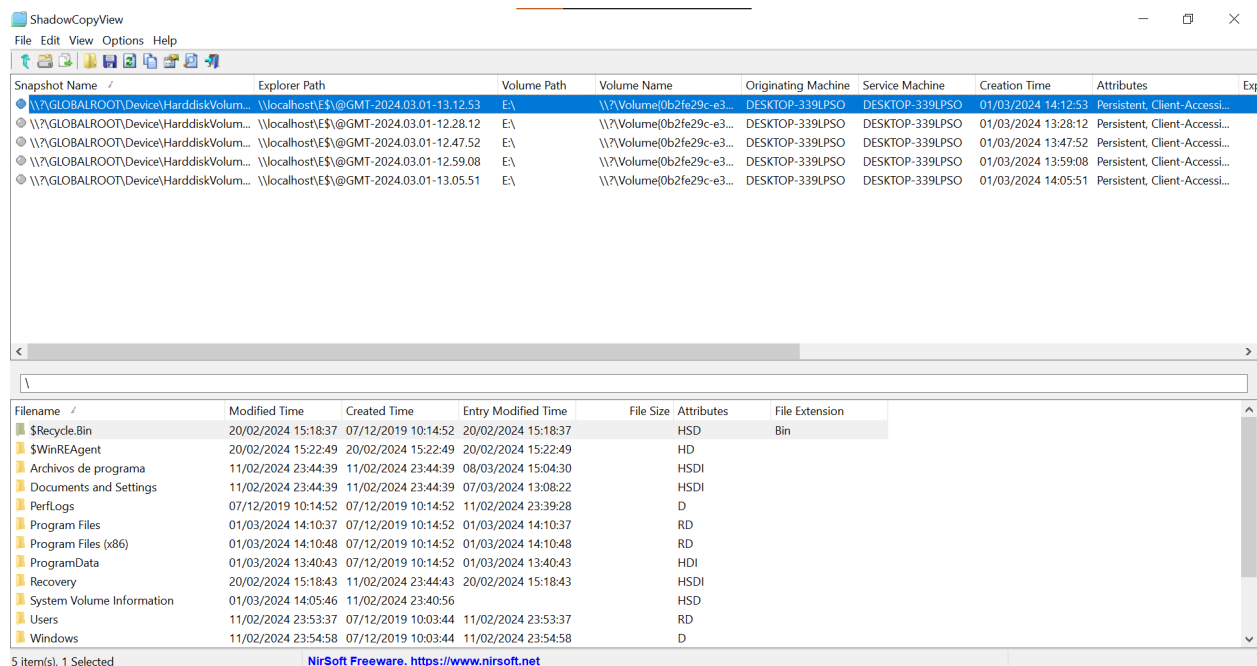
A continuación, suponiendo que hayamos trasladado este disco con las evidencias a otro ordenador, también podemos utilizar FTK Imager para montar las evidencias en nuestro propio sistema y así trabajar con la información adquirida. Para hacerlo, nos dirigimos a '**File > Image Mounting**'.



Se abrirá una ventana en la que debemos seleccionar la adquisición extraída y hacer clic en **'Mount'**.



Finalmente, podemos utilizar **'ShadowCopyView'** para visualizar y realizar una exhaustiva investigación forense de estos puntos de restauración.



Observamos que en este punto de restauración seleccionado, a diferencia del primero mostrado en la primera imagen, se incluyen directorios de programas instalados como '**Google Chrome**', '**Mozilla Firefox**' y '**VLC Media Player**'.

ShadowCopyView

File Edit View Options Help

Snapshot Name	Explorer Path	Volume Path	Volume Name	Orig
\\?\GLOBALROOT\Device\HarddiskVolum...	\\localhost\E\$\@GMT-2024.03.01-13.12.53	E:\	\\?\Volume{0b2fe29c-e3...	DES
\\?\GLOBALROOT\Device\HarddiskVolum...	\\localhost\E\$\@GMT-2024.03.01-12.28.12	E:\	\\?\Volume{0b2fe29c-e3...	DES
\\?\GLOBALROOT\Device\HarddiskVolum...	\\localhost\E\$\@GMT-2024.03.01-12.47.52	E:\	\\?\Volume{0b2fe29c-e3...	DES
\\?\GLOBALROOT\Device\HarddiskVolum...	\\localhost\E\$\@GMT-2024.03.01-12.59.08	E:\	\\?\Volume{0b2fe29c-e3...	DES
\\?\GLOBALROOT\Device\HarddiskVolum...	\\localhost\E\$\@GMT-2024.03.01-13.05.51	E:\	\\?\Volume{0b2fe29c-e3...	DES

<

\Program Files

Filename	Modified Time	Created Time	Entry Modified Time	File Size	Attributes
Archivos comunes	11/02/2024 23:44:39	11/02/2024 23:44:39	07/03/2024 12:57:09		HSDI
Common Files	07/12/2019 10:31:10	07/12/2019 10:14:52	11/02/2024 23:39:28		D
Google	01/03/2024 13:57:28	01/03/2024 13:57:28	01/03/2024 13:57:28		D
Internet Explorer	05/05/2023 14:24:22	07/12/2019 10:14:52	11/02/2024 23:39:28		D
Microsoft Update Health Tools	20/02/2024 15:22:33	20/02/2024 15:22:33	20/02/2024 15:22:33		D
ModifiableWindowsApps	07/12/2019 10:14:52	07/12/2019 10:14:52	11/02/2024 23:39:28		D
Mozilla Firefox	01/03/2024 13:40:45	01/03/2024 13:36:30	01/03/2024 13:40:45		D
Oracle	11/02/2024 23:52:41	11/02/2024 23:52:41	11/02/2024 23:52:41		D
RUXIM	20/02/2024 15:18:51	20/02/2024 15:18:50	20/02/2024 15:18:51		D
Uninstall Information	11/02/2024 23:41:31	11/02/2024 23:41:31	11/02/2024 23:41:31		HD
Windows Defender	12/02/2024 11:14:10	07/12/2019 10:14:52	12/02/2024 11:14:10		D
Windows Defender Advanced Threa...	05/05/2023 14:24:22	07/12/2019 15:58:17	11/02/2024 23:39:28		D