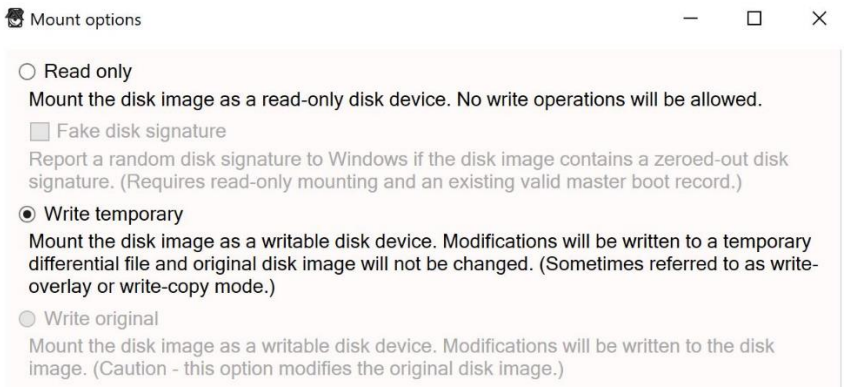
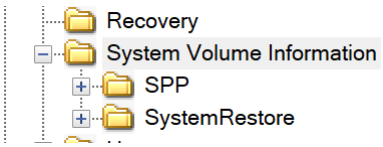
Exploring Volume Shadow (VSS) snapshots

(For the following, I used the Win10 Lone Wolf scenario .E0x image on a Win 10(v1809 build 17754.1) PC)

First we mount the image with Arsenal Image Mounter (with the write-temporary option):



The Image in this case was assigned drive letter F: by Windows.
If we open the Logical Volume (F:) in FTK imager, and expand the 'System Volume Information' folder:



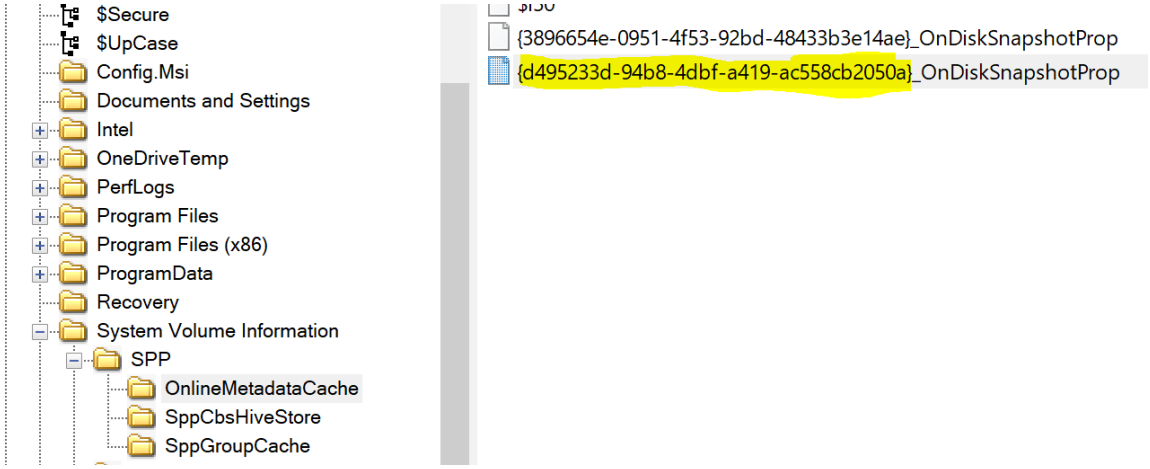
We can see that there are two snapshots:

Name	Size	Type
SPP	1	Directory
SystemRestore	1	Directory
IndexerVolumeGuid	1	Regular File
MountPointManagerRemoteDatabase	0	Regular File
tracking.log	20	Regular File
Wcifs.md	1	Regular File
WPSettings.dat	1	Regular File
{3808876b-c176-4e48-b7ae-04046e6cc752}	64	Regular File
{3869c289-31b8-11e8-9b12-ecf4bb487fed}{3808876b-c176-4e48-b7ae-04046e6cc752}	1.408.592	Regular File
{d4a32c4c-37d0-11e8-9b15-28e347017777}{3808876b-c176-4e48-b7ae-04046e6cc752}	884.736	Regular File

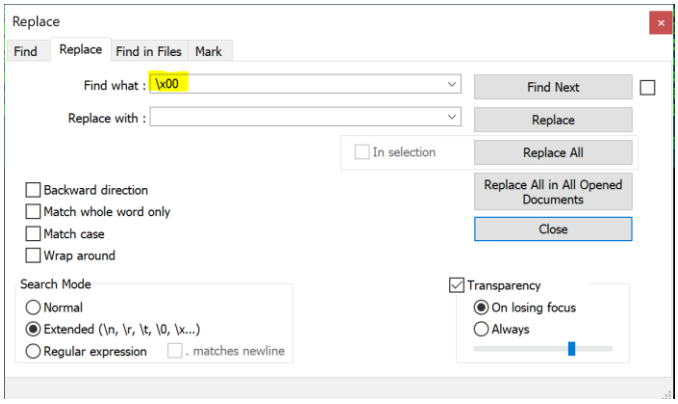
Running the 'vssadmin list shadows' command in an elevated command prompt gives:

```
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {3896654e-0951-4f53-92bd-48433b3e14ae}
   Contained 1 shadow copies at creation time: 27 Mar 18 12:22:37 pm
      Shadow Copy ID: {4fc85291-ebac-4113-aeb5-590de0ae9b66}
         Original Volume: (F:)\\?\Volume{09931f21-7faf-44a9-81d8-1e73c14b9eaf}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3
         Originating Machine: DESKTOP-PM6C56D
         Service Machine: DESKTOP-PM6C56D
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessibleWriters
         Attributes: Persistent, Client-accessible, No auto release, Differential, Auto recovered

Contents of shadow copy set ID: {d495233d-94b8-4dbf-a419-ac558cb2050a}
   Contained 1 shadow copies at creation time: 04 Apr 18 9:32:10 am
      Shadow Copy ID: {2b03870e-d9f3-410d-8699-53d49e76fd25}
         Original Volume: (F:)\\?\Volume{09931f21-7faf-44a9-81d8-1e73c14b9eaf}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4
         Originating Machine: DESKTOP-PM6C56D
         Service Machine: DESKTOP-PM6C56D
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessibleWriters
         Attributes: Persistent, Client-accessible, No auto release, Differential, Auto recovered
```

Where does vssadmin get all these information from? From the 'System Volume Information\SPP\OnlineMetadataCache' folder:



If we open the "{d495233d-94b8-4dbf-a419-ac558cb2050a}_OnDiskSnapshotProp" file in Notepad++ and trim the NULL characters (replace \x00),



we can see some interesting information, like the PC name, Workgroup\Domain name, the Volume GUID & drive letter, as well as included & excluded folders:

□ αj YϋG²Γ<ï&μ+€¬†—> MMMM =#•ΤΈ”ΩM¤ ¬U□²
½.T¤ήΛΣ π μ Π†»F—c'ΨβE¤ $ 8 I Scheduled Checkpoint
C:\Windows\ DESKTOP-PM6C56D

WORKGROUP +σΩ
A†™ST□vú% DMIO:ID:!“—•©D□Ψ-sAK□— 22\\?\Volume{09931f21-7faf-44a9-81d8-1e73c14b9eaf}\ C:\ Evχ N)€A—jü• (0 , 22\\?\Volume{09931f21-7faf-44a9-81d8-1e73c14b9eaf}\ 4 (C:)< @ D H L P T X \ ` d h ++Backup and Sync from Google 3.40.8921.5350 Box Sync 4.0.7900.0--Dell Touchpad 10.1207.101.103 Dropbox 46.4.65 Google Chrome 65.0.3325.18144 Microsoft Office 365 ProPlus - en-us 16.0.8431.2236&&NVIDIA 3D Vision Driver 376.54 376.54%%NVIDIA Graphics Driver 376.54 376.54++NVIDIA HD Audio Driver 1.3.34.17 1.3.34.17 NVIDIA nView 148.03 148.03!!S3 Browser version 7.6.9 7.6.9.0,,Vulkan Run Time Libraries 1.0.26.0 1.0.26.0 p t x | € „ □ □ □ ” □ □ ¤ ¨ ¬ ° ′ Έ Ό ΐ Δ Θ Μ Π Τ Ψ ά ϋ δ θ μ π τ ψ ό ComSpec--%SystemRoot%\system32\cmd.exe OS

Windows_NT Pathll%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\ PATHEXT66.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC PROCESSOR_ARCHITECTURE AMD64

PSModulePath^^%ProgramFiles%\WindowsPowerShell\Modules;%SystemRoot%\system32\WindowsPowerShell\v1.0\Modules TEMP %SystemRoot%\TEMP TMP %SystemRoot%\TEMP USERNAME SYSTEM windir

%SystemRoot% NUMBER_OF_PROCESSORS 4 PROCESSOR_LEVEL 6 PROCESSOR_IDENTIFIER33Intel64 Family 6 Model 58 Stepping 9, GenuineIntel PROCESSOR_REVISION 3a09 Default %SystemDrive%\Users\Default ProfilesDirectory %SystemDrive%\Users\ProgramData %SystemDrive%\ProgramData Public %SystemDrive%\Users\Public

ProgramFiles C:\Program Files

We can run the VolumeSnapshot.ps1 PowerShell script to get the events from the ‘Microsoft-Windows-VolumeSnapshot-Driver/Operational.evtx’ log:

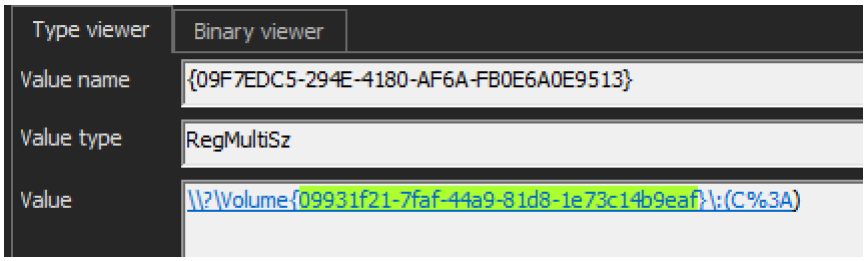
Target Volume GUID	Source File
{09931f21-7faf-44a9-81d8-1e73c14b9eaf}	1
{09931f21-7faf-44a9-81d8-1e73c14b9eaf}	{3869c289-31b8-11e8-9b12-ecf4bb487fed}
{09931f21-7faf-44a9-81d8-1e73c14b9eaf}	{3869c289-31b8-11e8-9b12-ecf4bb487fed}
{09931f21-7faf-44a9-81d8-1e73c14b9eaf}	{3869c289-31b8-11e8-9b12-ecf4bb487fed}
{09931f21-7faf-44a9-81d8-1e73c14b9eaf}	0x1
{09931f21-7faf-44a9-81d8-1e73c14b9eaf}	0x1

So what do these Snapshot filenames in the 'System Volume Information' folder seen above mean?

The **first part** of the filename (same as the 'Source File' from the evtx log) is the Volume GUID.

Target Volume GUID : {09931f21-7faf-44a9-81d8-1e73c14b9eaf}
Source File : {3869c289-31b8-11e8-9b12-ecf4bb487fed}

Looking at the SOFTWARE hive at '\Microsoft\Windows NT\CurrentVersion\SPP\Clients'
We find the drive letter of the volume with this GUID:

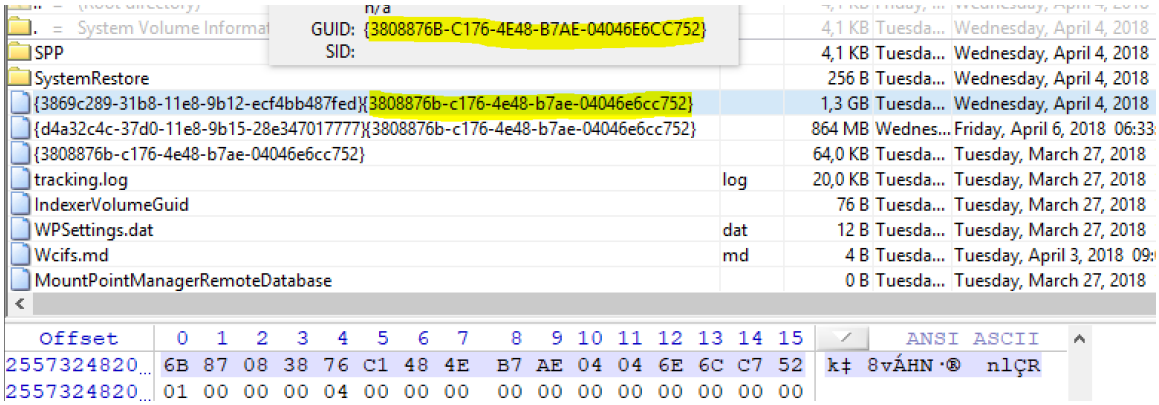


Which is **C:**

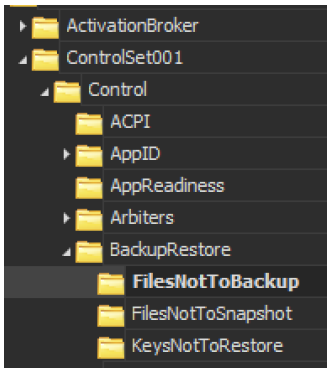
```
57 39 071 &#57; 9
58 3A 072 &#58; :
59 3B 073 &#59; ;
```

(http://www.asciitable.com/)

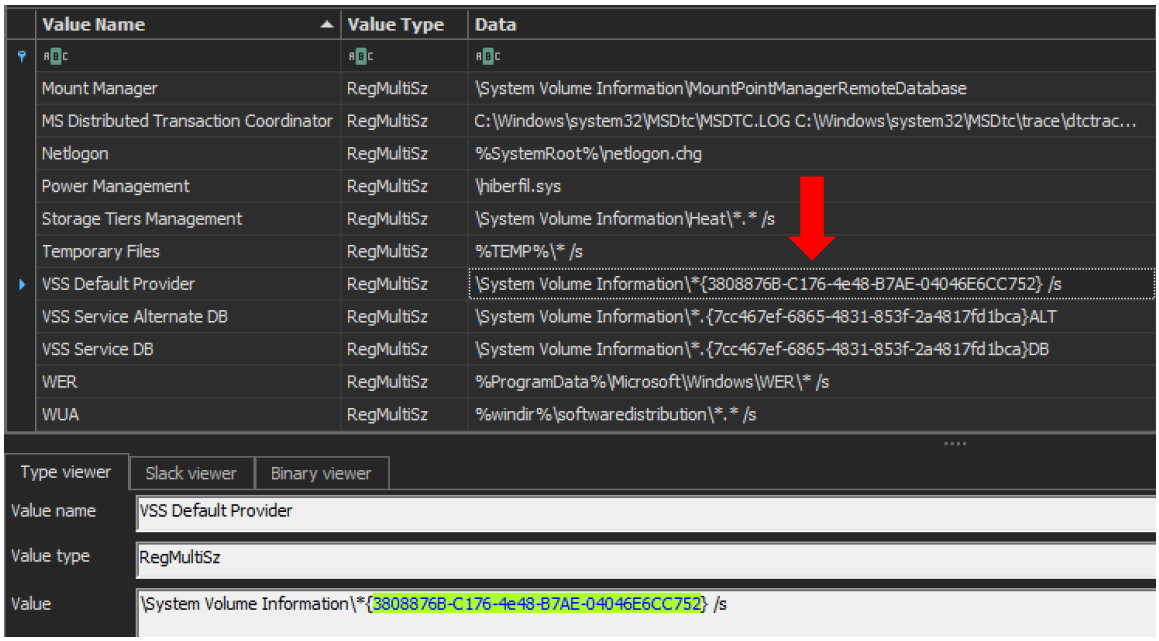
The **second part** of the filename is the Snapshot Provider GUID *(Provider: 'Microsoft Software Shadow Copy provider 1.0')*



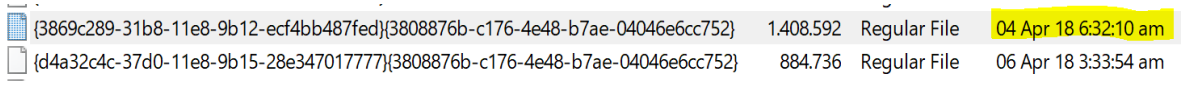
as seen at the SYSTEM hive at the value:



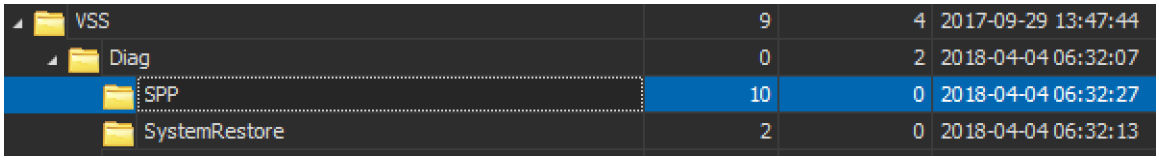
"\ControlSet001\Control\BackupRestore\FilesNotToBackup\VSS Default Provider"



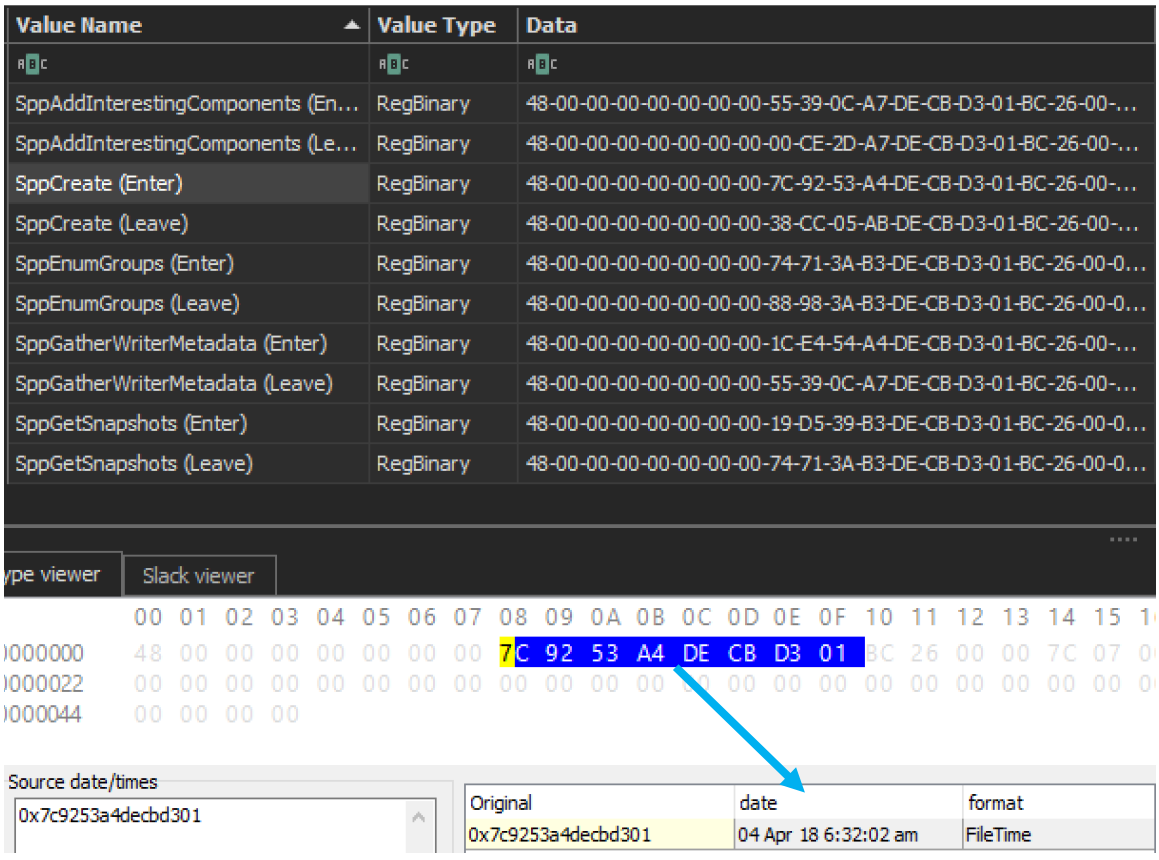
IF we look at the dates of the Snapshot files in the ‘System Volume Information’ folder:



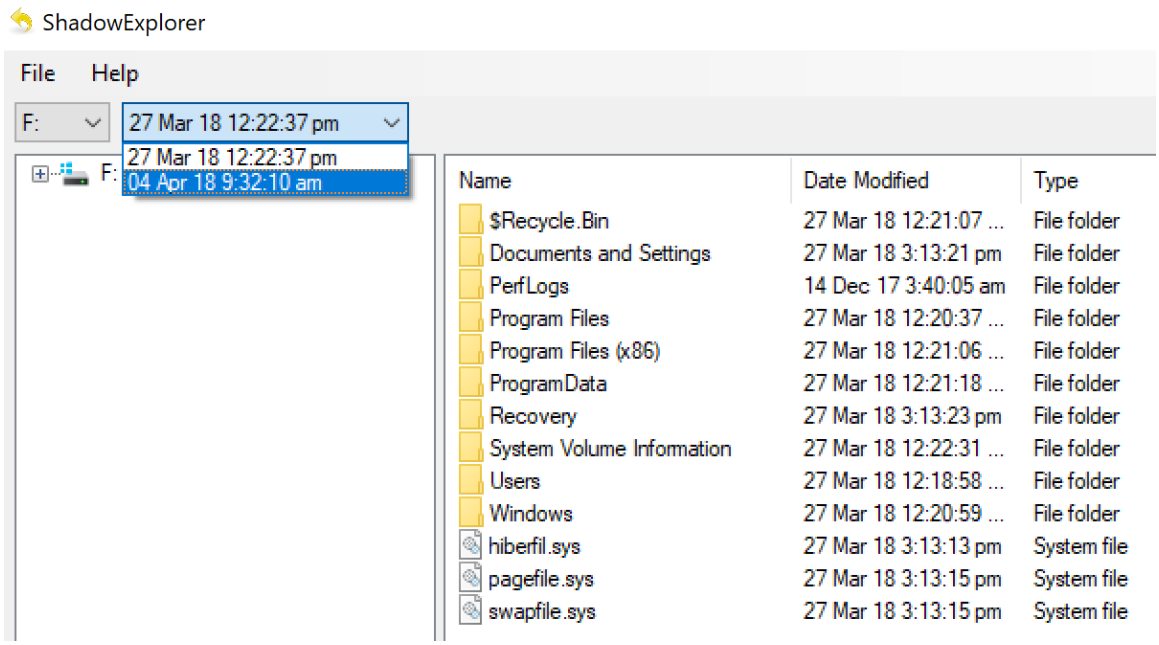
at the SYSTEM hive at "ControlSet001\Services\VSS\Diag\SPP"



“SppCreate (Enter)” value:



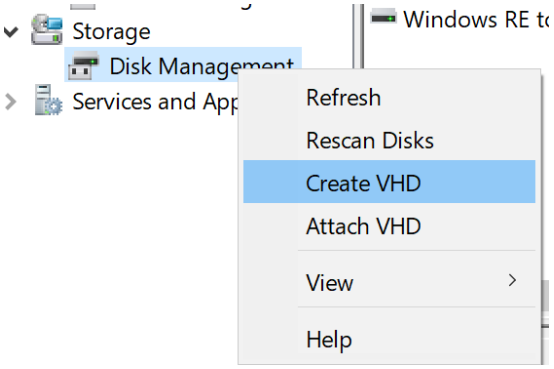
and the Snapshots with ShadowExplorer:
(Time displayed in ShadowExplorer is my localtime: GMT+3)



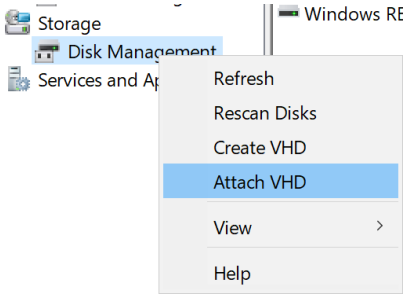
We see that the dates/times match with a few seconds difference.

Now let's save the Snapshot to a VHDx file.

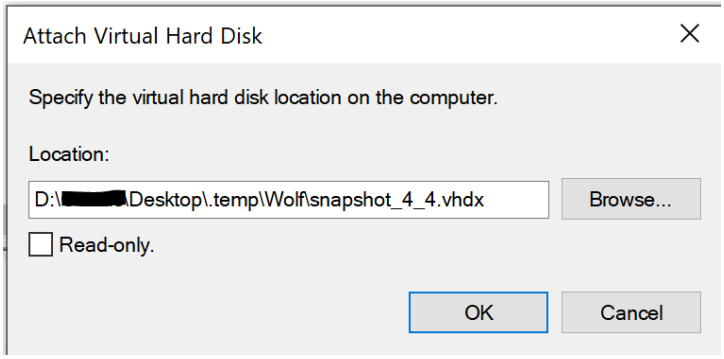
In Windows Disk Management we right click on Disk Management and select Create VHD:



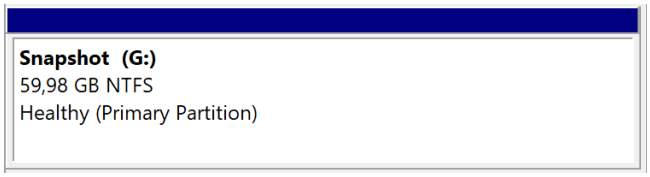
and create a dynamic VHD(X) file. Again we right click on Disk Management and select the 'Attach VHD' option this time:



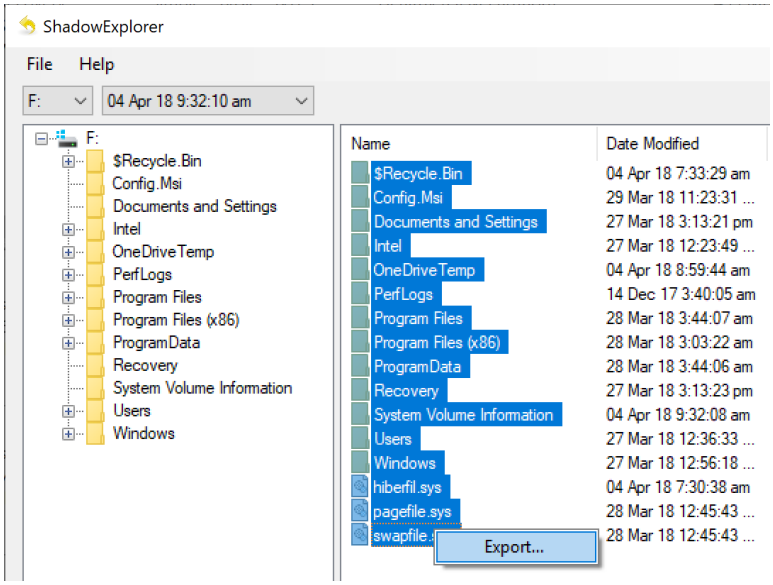
and select the previously created vhdx



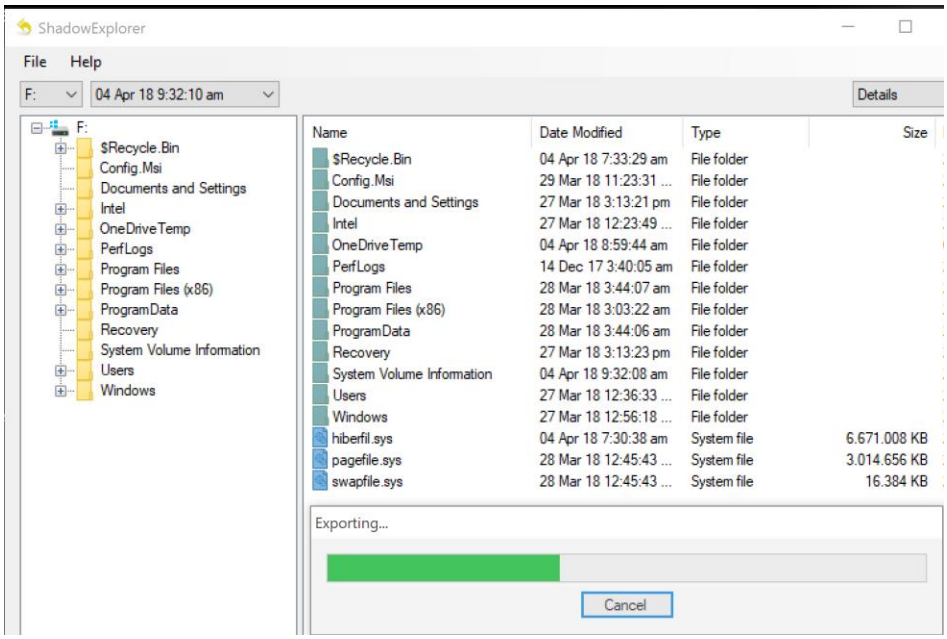
Now with the vhdx attached (read-write), initialized and formatted (60Gb) as with any normal Hard Disk:



We proceeded to export the Snapshot to this new drive G:. by selecting all the files/folders in ShadowExplorer and right clicked on Export:

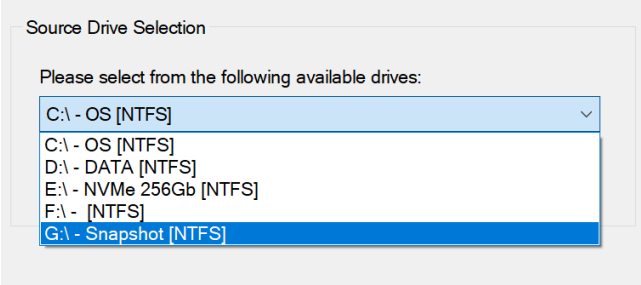


And select drive G: as the destination.

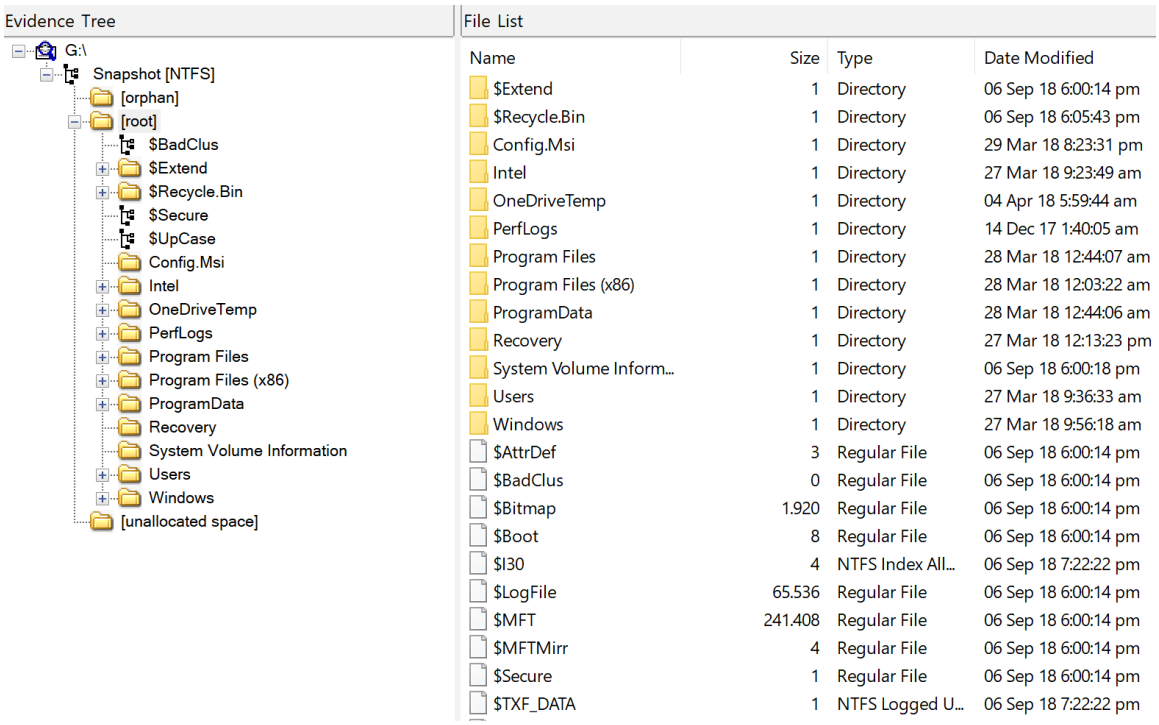


Sometime later in the day.. the export finishes, so we detach the VHDX file, and re-attach it as read-only this time.

If we open now the G: drive with FTK Imager:



We can explore the contents of the Snapshot



or create an .E01/raw image of the G: drive.

·_