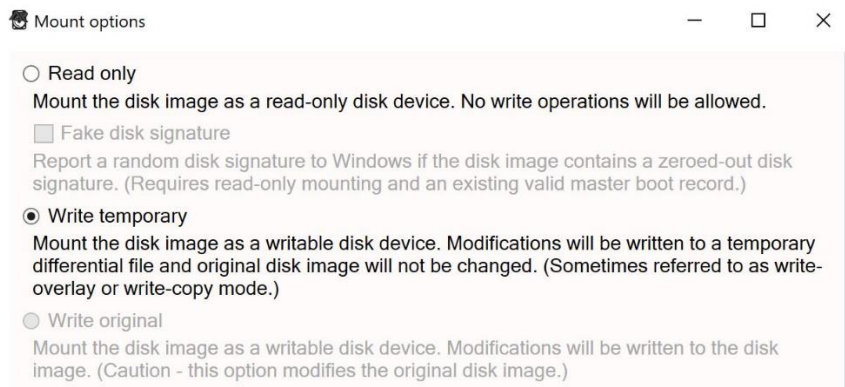


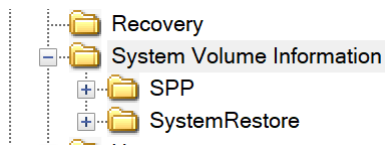
# Exploring Volume Shadow (VSS) snapshots

(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.

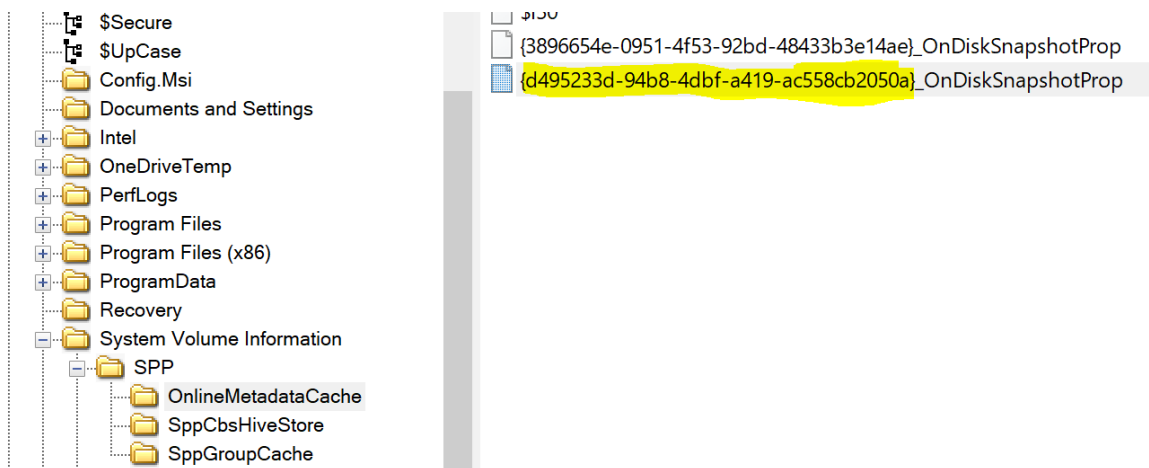
C:\WINDOWS\system32>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

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

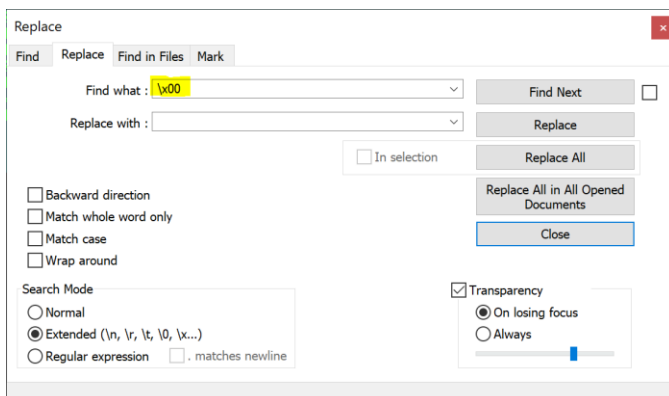
Contents of shadow copy set ID: {d495233d-94b8-4dbf-a419-ac558cb2050a}
  Contained 1 shadow copies at creation time: 04 Apr 18 9:32:10 am
  Shadow Copy ID: {2b03870e-d9f3-410d-8699-53d49e76fd25}
    Original Volume: (F:)\\?\Volume{09931f21-7faf-44a9-81d8-1e73c14b9eaf}\
    Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4
    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:

Ⓜ aj YÜG²Γ<ï&μ+€-†—> M M M M =#•TE''ΩMα -UⓂ²  
½.ΤάήΛΣ π μ Π†»F—c'ψβεα \$ 8 I Scheduled Checkpoint  
C:\Windows\ DESKTOP-PM6C56D

**WORKGROUP** +σΩ  
A+™ST@vú% DMIO:ID:!—"•©DΨ-sAK⊖— 22\\?Volume{09931f21-7faf-44a9-81d8-1e73c14b9eaf}\\ C:\ Evx 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 | € „ ? ? ? " ? ? ¤ ¯ ~ ° ´ ´ ¸ Ò Ì Δ Θ Μ Π Τ Ψ á ü δ θ μ π τ ψ ó ComSpec--%SystemRoot%\system32\cmd.exe OS

```
Windows_NT Path\\%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\Win
dowsPowerShell\v1.0\Modules  TEMP  %SystemRoot%\TEMP  TMP  %SystemRoot%\TEMP
  USERNAME  SYSTEM  windir
```

```
%SystemRoot%    NUMBER_OF_PROCESSORS    4    PROCESSOR_LEVEL    6    PROCESSOR_IDENT
IFIER33Intel64 Family 6 Model 58 Stepping 9,
GenuineIntel    PROCESSOR_REVISION    3a09    Default    %SystemDrive%\Users\Default    Profil
esDirectory    %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:

Type viewer	Binary viewer
Value name	{09F7EDC5-294E-4180-AF6A-FB0E6A0E9513}
Value type	RegMultiSz
Value	\\?Volume{09931f21-7faf-44a9-81d8-1e73c14b9eaf}\:(C%3A)

Which is C:

```

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

```

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

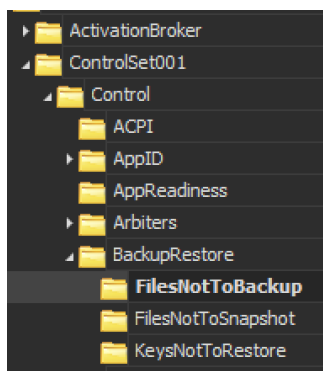
The **second part** of the filename is the Snapshot Provider GUID (Provider: 'Microsoft Software Shadow Copy provider 1.0')

System Volume Information	GUID: {3808876B-C176-4E48-B7AE-04046E6CC752}	4,1 KB	Tuesda...	Wednesday, April 4, 2018
SPP	SID:	4,1 KB	Tuesda...	Wednesday, April 4, 2018
SystemRestore		256 B	Tuesda...	Wednesday, April 4, 2018
{3869c289-31b8-11e8-9b12-ecf4bb487fed}{3808876b-c176-4e48-b7ae-04046e6cc752}		1,3 GB	Tuesda...	Wednesday, April 4, 2018
{d4a32c4c-37d0-11e8-9b15-28e347017777}{3808876b-c176-4e48-b7ae-04046e6cc752}		864 MB	Wednes...	Friday, April 6, 2018 06:33
{3808876b-c176-4e48-b7ae-04046e6cc752}		64,0 KB	Tuesda...	Tuesday, March 27, 2018
tracking.log	log	20,0 KB	Tuesda...	Tuesday, March 27, 2018
IndexerVolumeGuid		76 B	Tuesda...	Tuesday, March 27, 2018
WPSettings.dat	dat	12 B	Tuesda...	Tuesday, March 27, 2018
Wcifs.md	md	4 B	Tuesda...	Tuesday, April 3, 2018 09:
MountPointManagerRemoteDatabase		0 B	Tuesda...	Tuesday, March 27, 2018

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		ANSI	ASCII
2557324820...	6B	87	08	38	76	C1	48	4E	B7	AE	04	04	6E	6C	C7	52		k†	8vÁHN ·® nlÇR
2557324820...	01	00	00	00	04	00	00	00	00	00	00	00	00	00	00	00			

as seen at the SYSTEM hive at the value:



“\ControlSet001\Control\BackupRestore\FilesNotToBackup\VSS Default Provider”

Value Name	Value Type	Data
Mount Manager	RegMultiSz	\System Volume Information\MountPointManagerRemoteDatabase
MS Distributed Transaction Coordinator	RegMultiSz	C:\Windows\system32\MSDtc\MSDTC.LOG C:\Windows\system32\MSDtc\trace\dtctrac...
Netlogon	RegMultiSz	%SystemRoot%\netlogon.chg
Power Management	RegMultiSz	\hiberfil.sys
Storage Tiers Management	RegMultiSz	\System Volume Information\Heat\*. */s
Temporary Files	RegMultiSz	%TEMP%\* */s
VSS Default Provider	RegMultiSz	\System Volume Information\*{3808876B-C176-4e48-B7AE-04046E6CC752} /s
VSS Service Alternate DB	RegMultiSz	\System Volume Information\*.{7cc467ef-6865-4831-853f-2a4817fd1bca}ALT
VSS Service DB	RegMultiSz	\System Volume Information\*.{7cc467ef-6865-4831-853f-2a4817fd1bca}DB
WER	RegMultiSz	%ProgramData%\Microsoft\Windows\WER\* */s
WUA	RegMultiSz	%windir%\softwaredistribution\* */s

Type viewer	Slack viewer	Binary viewer
Value name	VSS Default Provider	
Value type	RegMultiSz	
Value	\System Volume Information\*{3808876B-C176-4e48-B7AE-04046E6CC752} /s	

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

{3869c289-31b8-11e8-9b12-ecf4bb487fed}{3808876b-c176-4e48-b7ae-04046e6cc752}	1,408,592	Regular File	04 Apr 18 6:32:10 am
{d4a32c4c-37d0-11e8-9b15-28e347017777}{3808876b-c176-4e48-b7ae-04046e6cc752}	884,736	Regular File	06 Apr 18 3:33:54 am

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

VSS	9	4	2017-09-29 13:47:44
Diag	0	2	2018-04-04 06:32:07
SPP	10	0	2018-04-04 06:32:27
SystemRestore	2	0	2018-04-04 06:32:13

“SppCreate (Enter)” value:

Value Name	Value Type	Data
SppAddInterestingComponents (Enter...)	RegBinary	48-00-00-00-00-00-00-55-39-0C-A7-DE-CB-D3-01-BC-26-00-...
SppAddInterestingComponents (Le...)	RegBinary	48-00-00-00-00-00-00-CE-2D-A7-DE-CB-D3-01-BC-26-00-...
SppCreate (Enter)	RegBinary	48-00-00-00-00-00-00-7C-92-53-A4-DE-CB-D3-01-BC-26-00-...
SppCreate (Leave)	RegBinary	48-00-00-00-00-00-00-38-CC-05-AB-DE-CB-D3-01-BC-26-00-...
SppEnumGroups (Enter)	RegBinary	48-00-00-00-00-00-00-74-71-3A-B3-DE-CB-D3-01-BC-26-00-0...
SppEnumGroups (Leave)	RegBinary	48-00-00-00-00-00-00-88-98-3A-B3-DE-CB-D3-01-BC-26-00-0...
SppGatherWriterMetadata (Enter)	RegBinary	48-00-00-00-00-00-00-1C-E4-54-A4-DE-CB-D3-01-BC-26-00-...
SppGatherWriterMetadata (Leave)	RegBinary	48-00-00-00-00-00-00-55-39-0C-A7-DE-CB-D3-01-BC-26-00-...
SppGetSnapshots (Enter)	RegBinary	48-00-00-00-00-00-00-19-D5-39-B3-DE-CB-D3-01-BC-26-00-0...
SppGetSnapshots (Leave)	RegBinary	48-00-00-00-00-00-00-74-71-3A-B3-DE-CB-D3-01-BC-26-00-0...

type viewer

Slack viewer

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16

000000 48 00 00 00 00 00 00 00 7C 92 53 A4 DE CB D3 01 BC 26 00 00 7C 07 00

000022 00

000044 00 00 00 00

Source date/times

0x7c9253a4decdbd301

Original

0x7c9253a4decdbd301

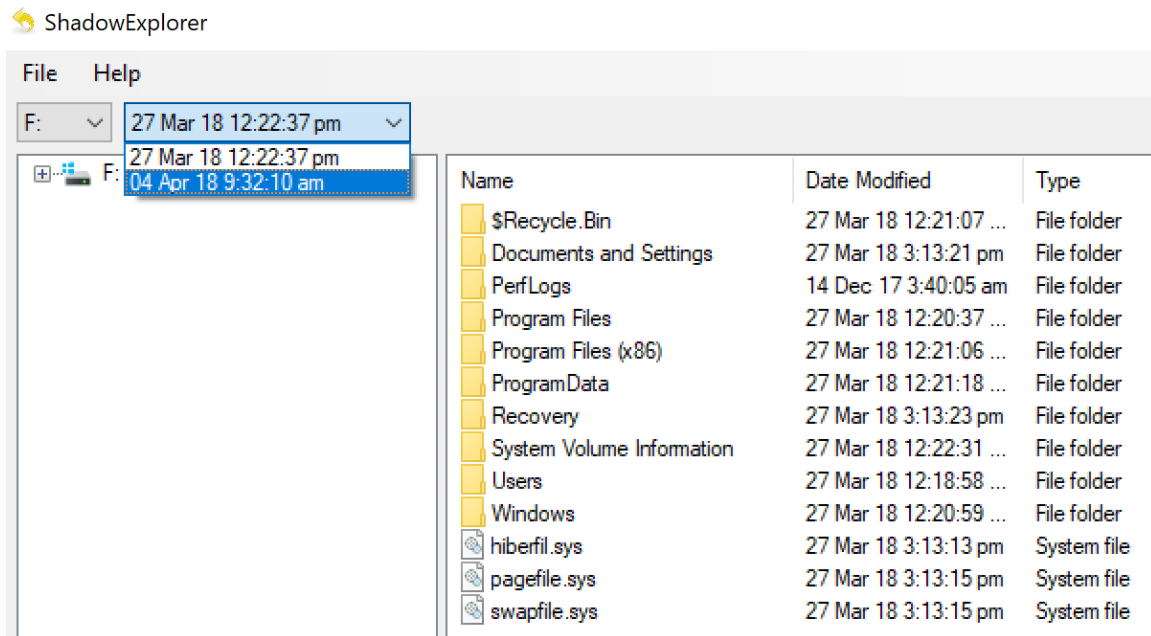
date

04 Apr 18 6:32:02 am

format

FileTime

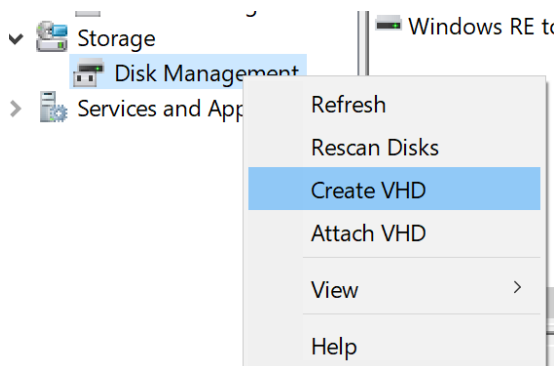
and the Snapshots with [ShadowExplorer](#):  
(Time displayed in ShadowExplorer is my localtime: GMT+3)



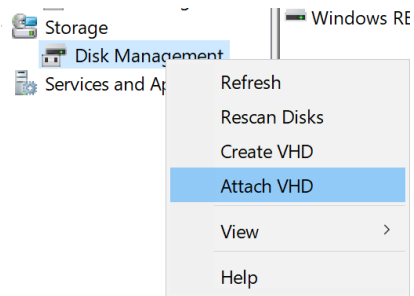
We see that the dates/times match with a few seconds difference.

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

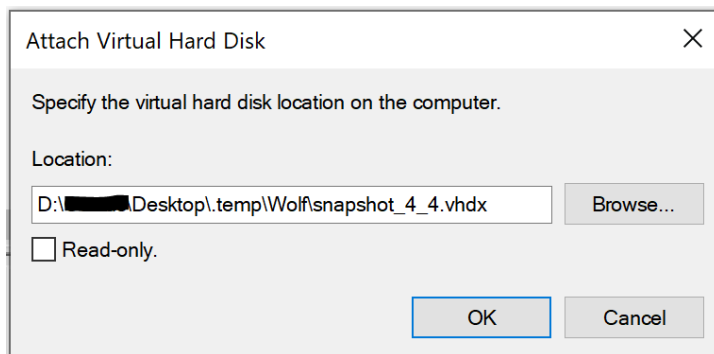
In Windows Disk Management we right click on Disk Management and select Create VHD:



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 vhd

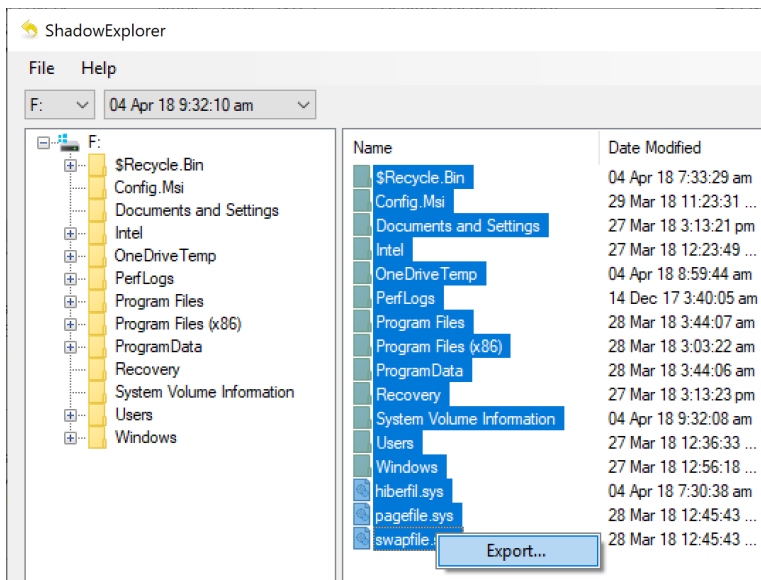


Now with the vhdx attached (read-write), initialized and formatted (60Gb) as with any normal Hard Disk:

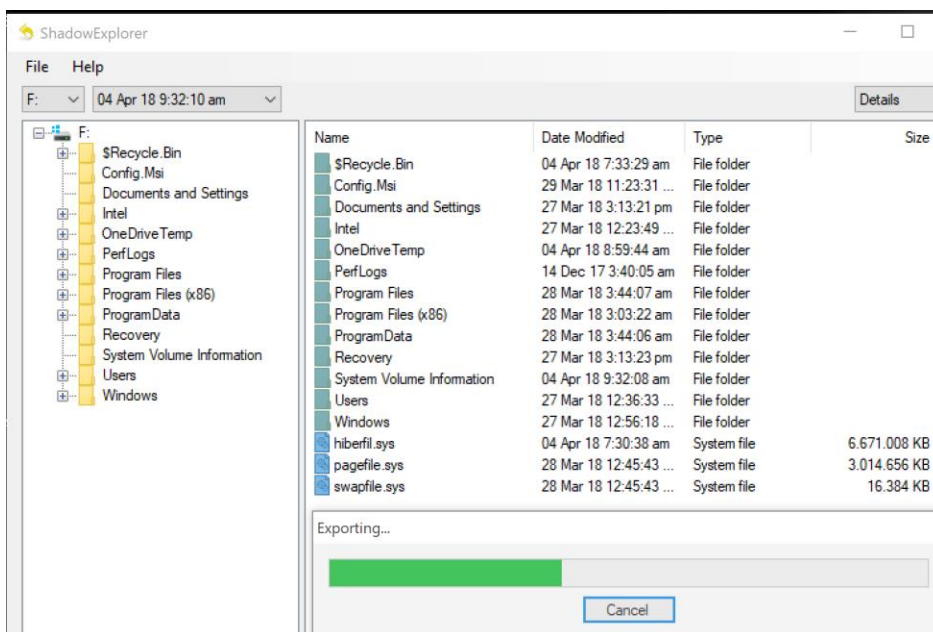


We proceeded to export the Snapshot to this new drive G:. by selecting all the files/folders in ShadowExplorer and right clicked on Export:



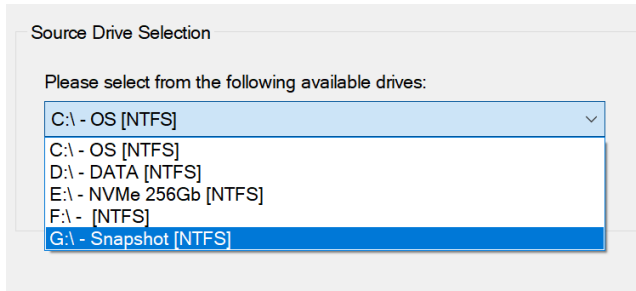


And select drive G: as the destination.



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

Evidence Tree		File List			
G:\		Name	Size	Type	Date Modified
Snapshot [NTFS]		\$Extend	1	Directory	06 Sep 18 6:00:14 pm
[orphan]		\$Recycle.Bin	1	Directory	06 Sep 18 6:05:43 pm
[root]		Config.Msi	1	Directory	29 Mar 18 8:23:31 pm
\$BadClus		Intel	1	Directory	27 Mar 18 9:23:49 am
\$Extend		OneDriveTemp	1	Directory	04 Apr 18 5:59:44 am
\$Recycle.Bin		PerfLogs	1	Directory	14 Dec 17 1:40:05 am
\$Secure		Program Files	1	Directory	28 Mar 18 12:44:07 am
\$UpCase		Program Files (x86)	1	Directory	28 Mar 18 12:03:22 am
Config.Msi		ProgramData	1	Directory	28 Mar 18 12:44:06 am
Intel		Recovery	1	Directory	27 Mar 18 12:13:23 pm
OneDriveTemp		System Volume Inform...	1	Directory	06 Sep 18 6:00:18 pm
PerfLogs		Users	1	Directory	27 Mar 18 9:36:33 am
Program Files		Windows	1	Directory	27 Mar 18 9:56:18 am
Program Files (x86)		\$AttrDef	3	Regular File	06 Sep 18 6:00:14 pm
ProgramData		\$BadClus	0	Regular File	06 Sep 18 6:00:14 pm
Recovery		\$Bitmap	1.920	Regular File	06 Sep 18 6:00:14 pm
System Volume Information		\$Boot	8	Regular File	06 Sep 18 6:00:14 pm
Users		\$I30	4	NTFS Index All...	06 Sep 18 7:22:22 pm
Windows		\$LogFile	65.536	Regular File	06 Sep 18 6:00:14 pm
[unallocated space]		\$MFT	241.408	Regular File	06 Sep 18 6:00:14 pm
		\$MFTMirr	4	Regular File	06 Sep 18 6:00:14 pm
		\$Secure	1	Regular File	06 Sep 18 6:00:14 pm
		\$TXF_DATA	1	NTFS Logged U...	06 Sep 18 7:22:22 pm

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

.\_