BitLocker: Encrypt containers instead of entire drives

TrueCrypt had a really nifty feature that allowed the user to encrypt only certain containers instead of entire drives. BitLocker does not. Or does it? In this short tutorial I'm going to show you how to (by using some sneaky and mischievous built-in disk management trickery) "fool" BitLocker into encrypting only what you want and even hide it from prying eyes.

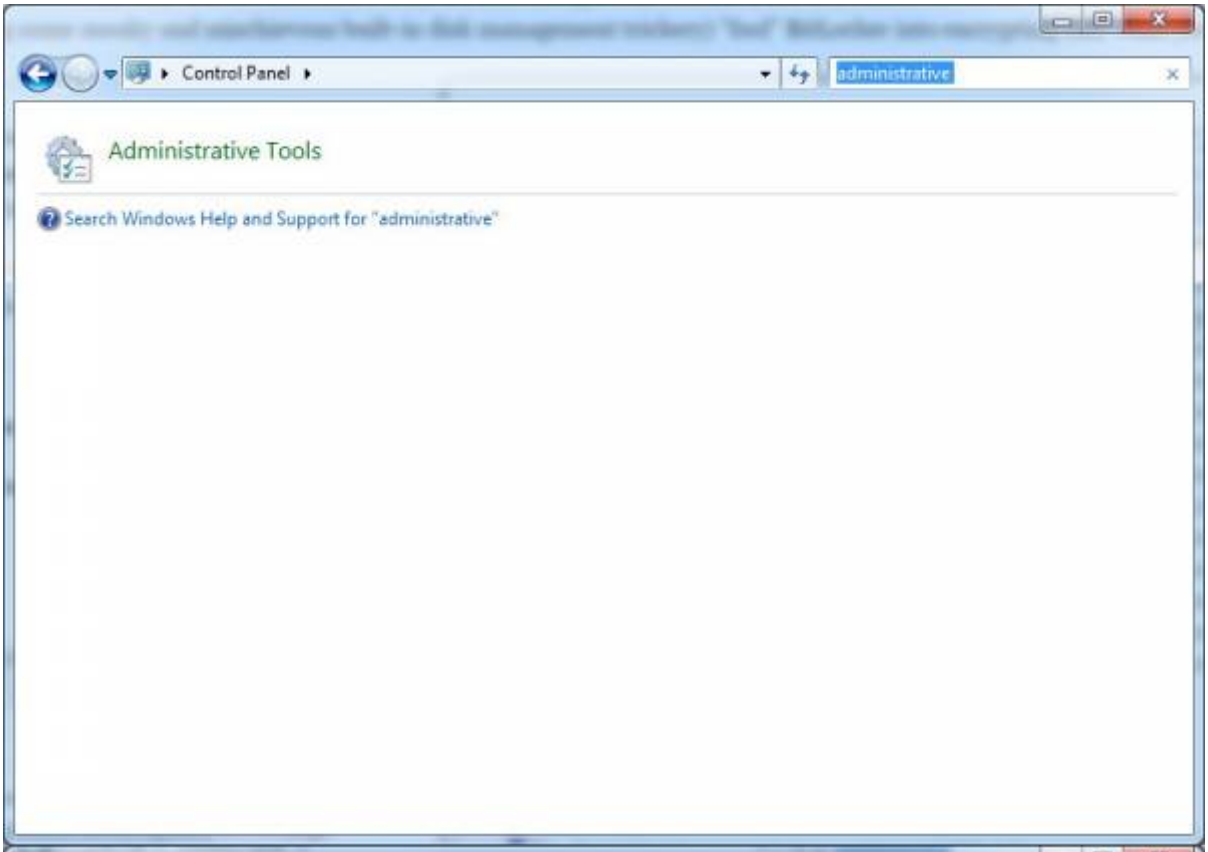
Before we begin do note that you can only pull this off with certain versions of Windows that actually support BitLocker functionality and those are **Windows 7 Ultimate/Windows 8/8.1 Professional and Enterprise**. Now that that's sorted we will also assume that you already have some level of experience with BitLocker (basically that you know how to lock a drive will be sufficient) because we shall be mostly concentrating our efforts on how to create a container that will then be encrypted by BL.

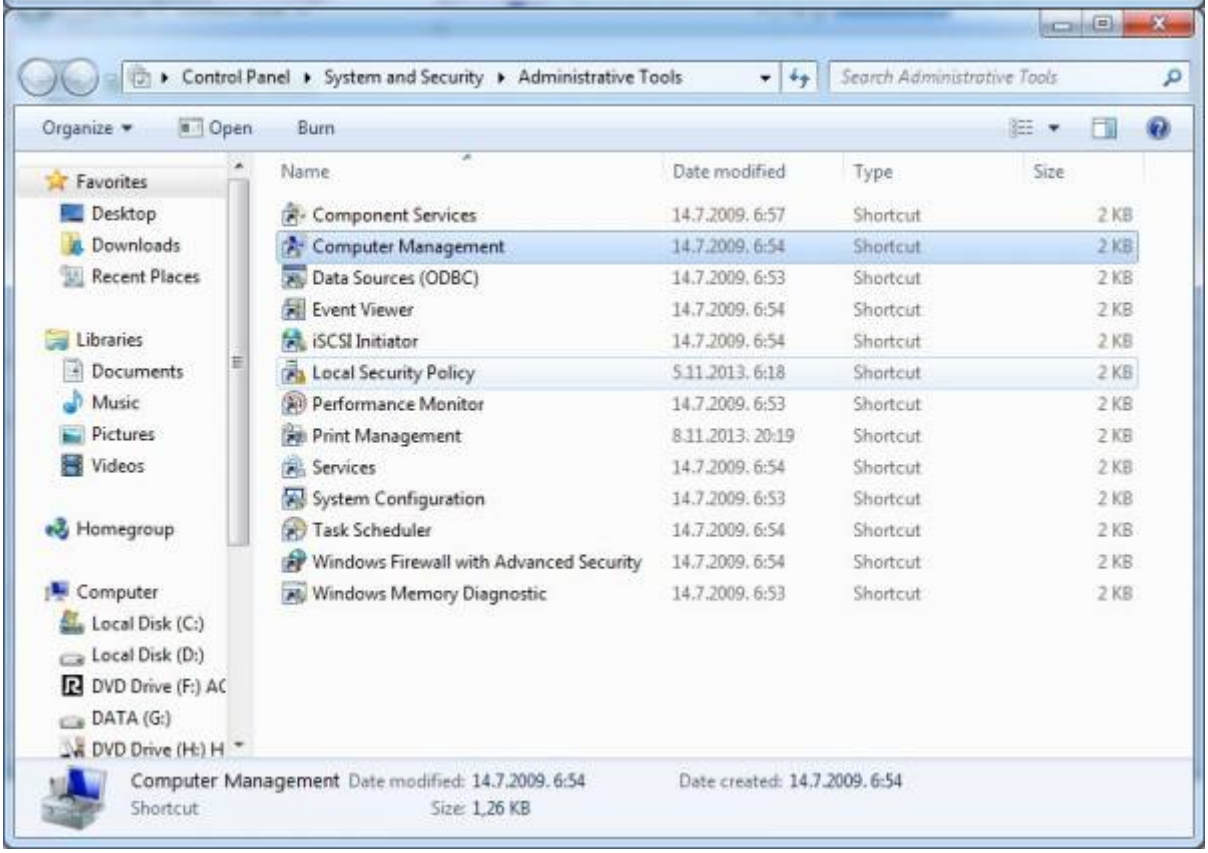
The Question: How to make BitLocker encrypt only what we want and not an entire drive? The Answer: Simple – give it a drive. Just make it virtual. Yes my dears, we can bamboozle BitLocker into thinking it's doing it's job with a VHD, which in turn allows for enough flexibility to only actually ever encrypt that what needs to be encrypted.

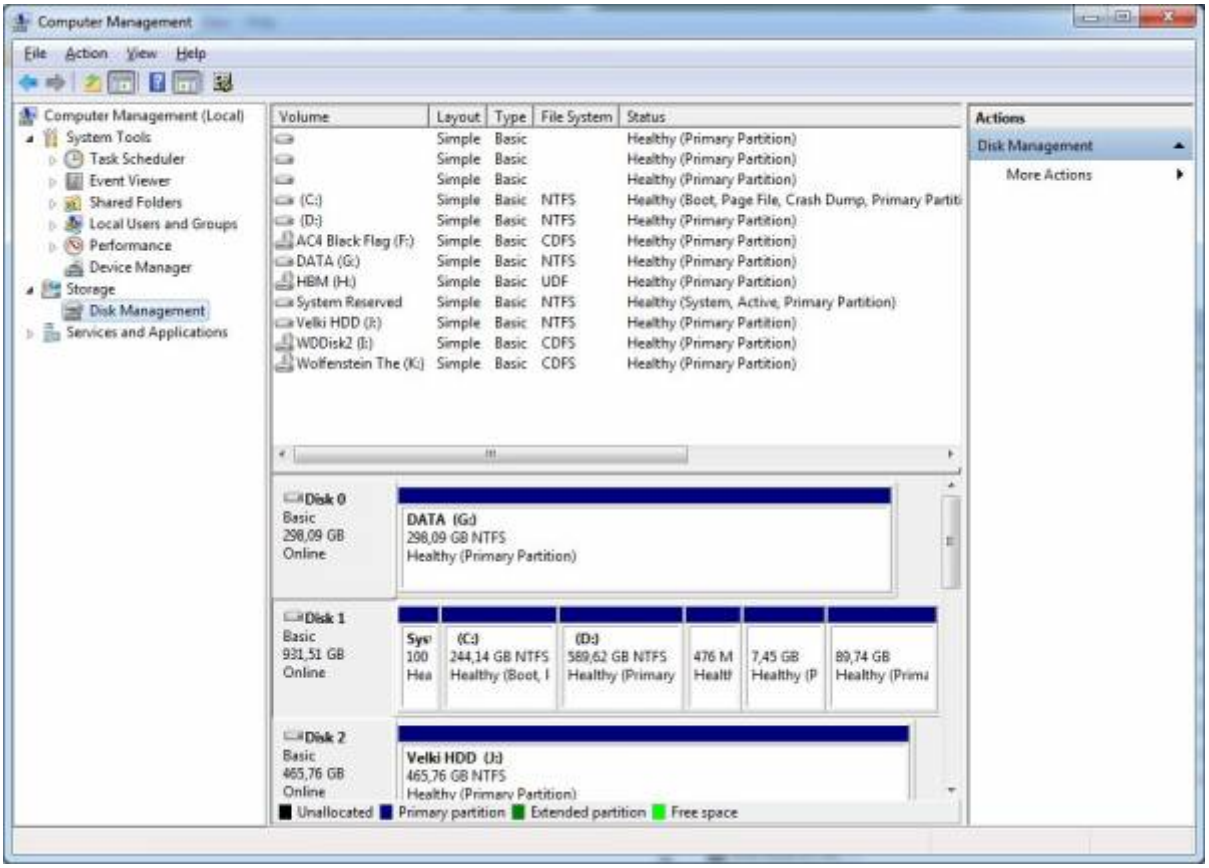
Let's start!

Create a VHD

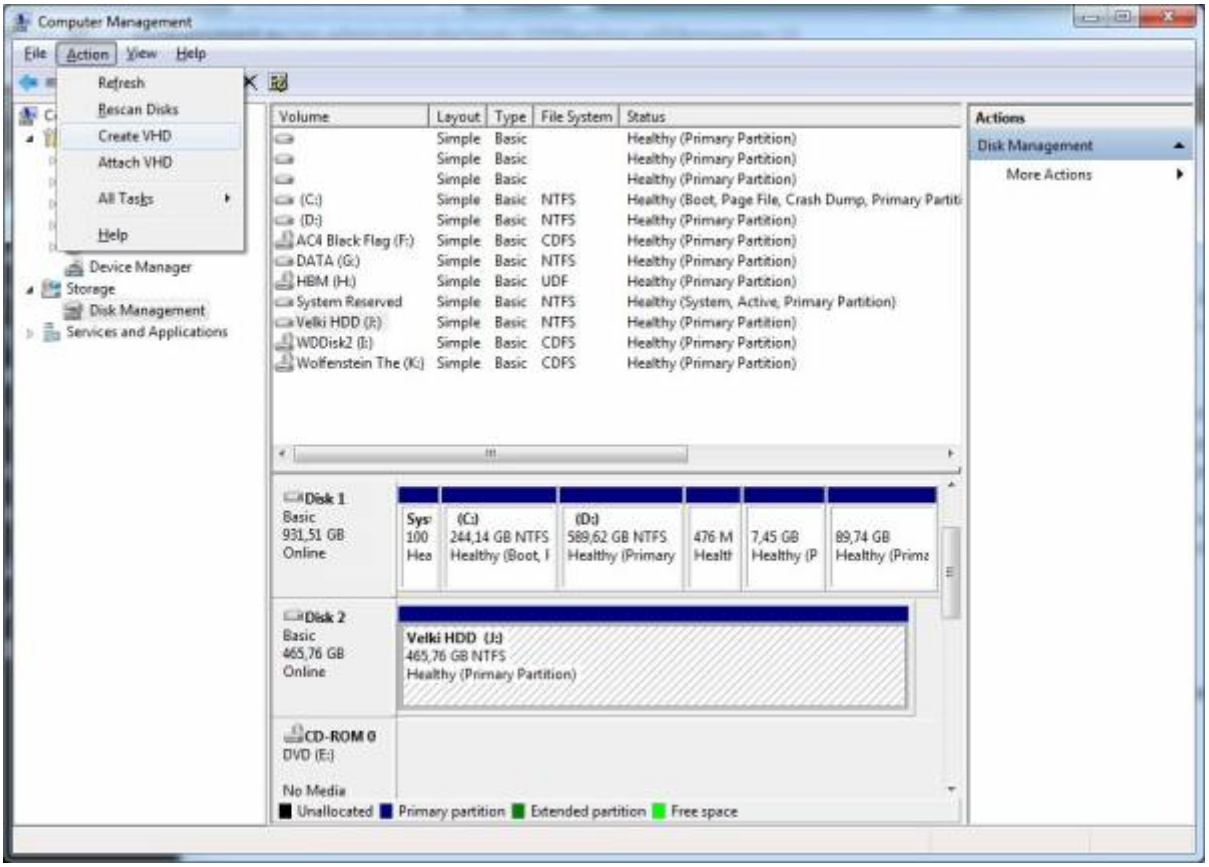
- Go to **Control Panel → Administrative Tools → Computer Management**. In the Computer Management pane on the left, under the **"Storage"** node select **"Disk Management"**.


Control Panel
administrative
Administrative Tools
Search Windows Help and Support for "administrative"


Control Panel ▸ System and Security ▸ Administrative Tools
Search Administrative Tools
Organize
Open
Burn
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
Local Disk (D:)
DVD Drive (F:) AC
DATA (G:)
DVD Drive (H:) H
Name
Date modified
Type
Size
Component Services 14.7.2009. 6:57 Shortcut 2 KB
Computer Management 14.7.2009. 6:54 Shortcut 2 KB
Data Sources (ODBC) 14.7.2009. 6:53 Shortcut 2 KB
Event Viewer 14.7.2009. 6:54 Shortcut 2 KB
iSCSI Initiator 14.7.2009. 6:54 Shortcut 2 KB
Local Security Policy 5.11.2013. 6:18 Shortcut 2 KB
Performance Monitor 14.7.2009. 6:53 Shortcut 2 KB
Print Management 8.11.2013. 20:19 Shortcut 2 KB
Services 14.7.2009. 6:54 Shortcut 2 KB
System Configuration 14.7.2009. 6:53 Shortcut 2 KB
Task Scheduler 14.7.2009. 6:54 Shortcut 2 KB
Windows Firewall with Advanced Security 14.7.2009. 6:54 Shortcut 2 KB
Windows Memory Diagnostic 14.7.2009. 6:53 Shortcut 2 KB
Computer Management Date modified: 14.7.2009. 6:54 Date created: 14.7.2009. 6:54
Shortcut Size: 1,26 KB

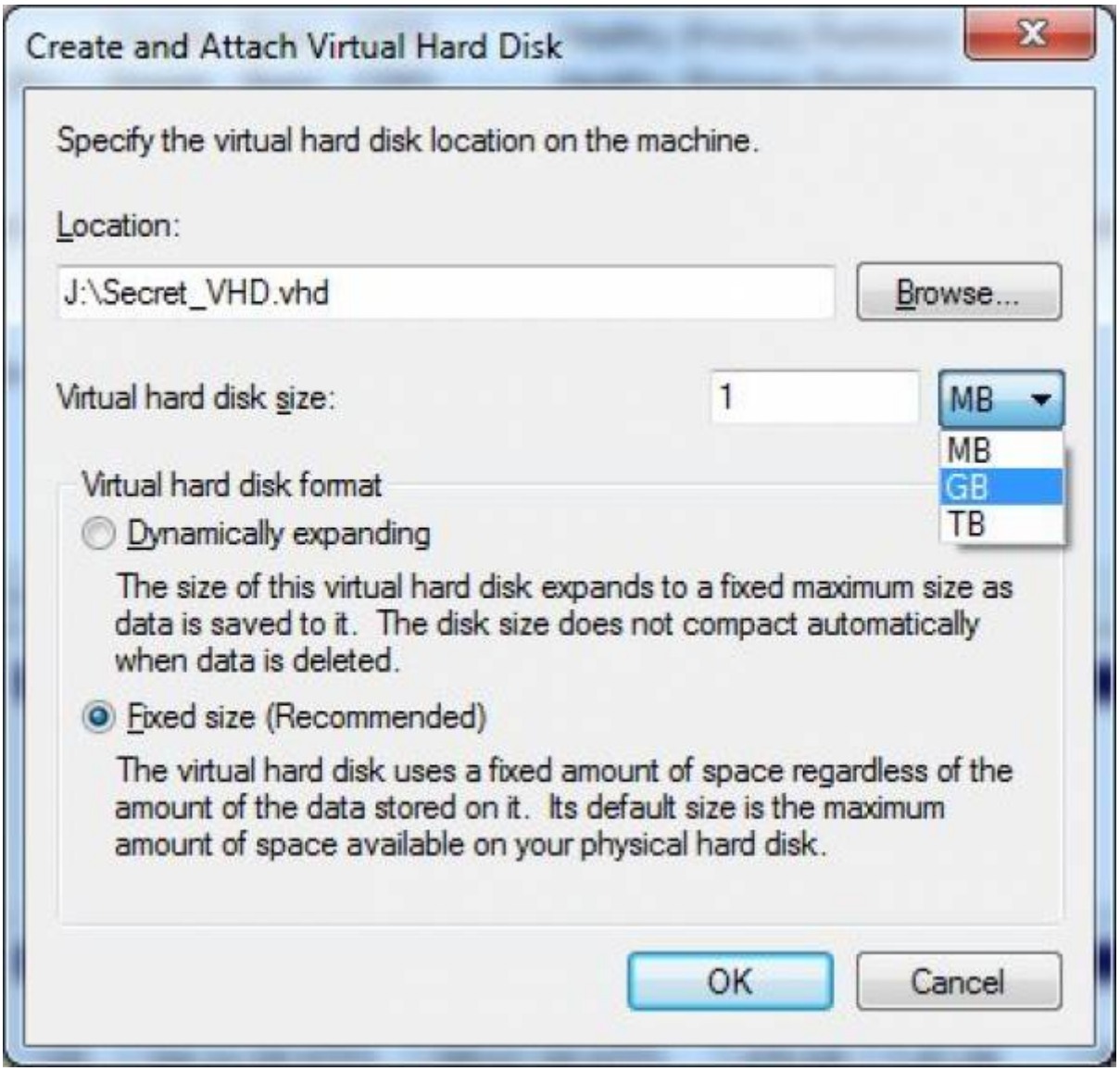


- From Disk Management select a drive (I'll select **Disk 2** for this demonstration) by clicking on it. Go to the **"Action"** menu and select **"Create VHD"** from the drop-down menu.

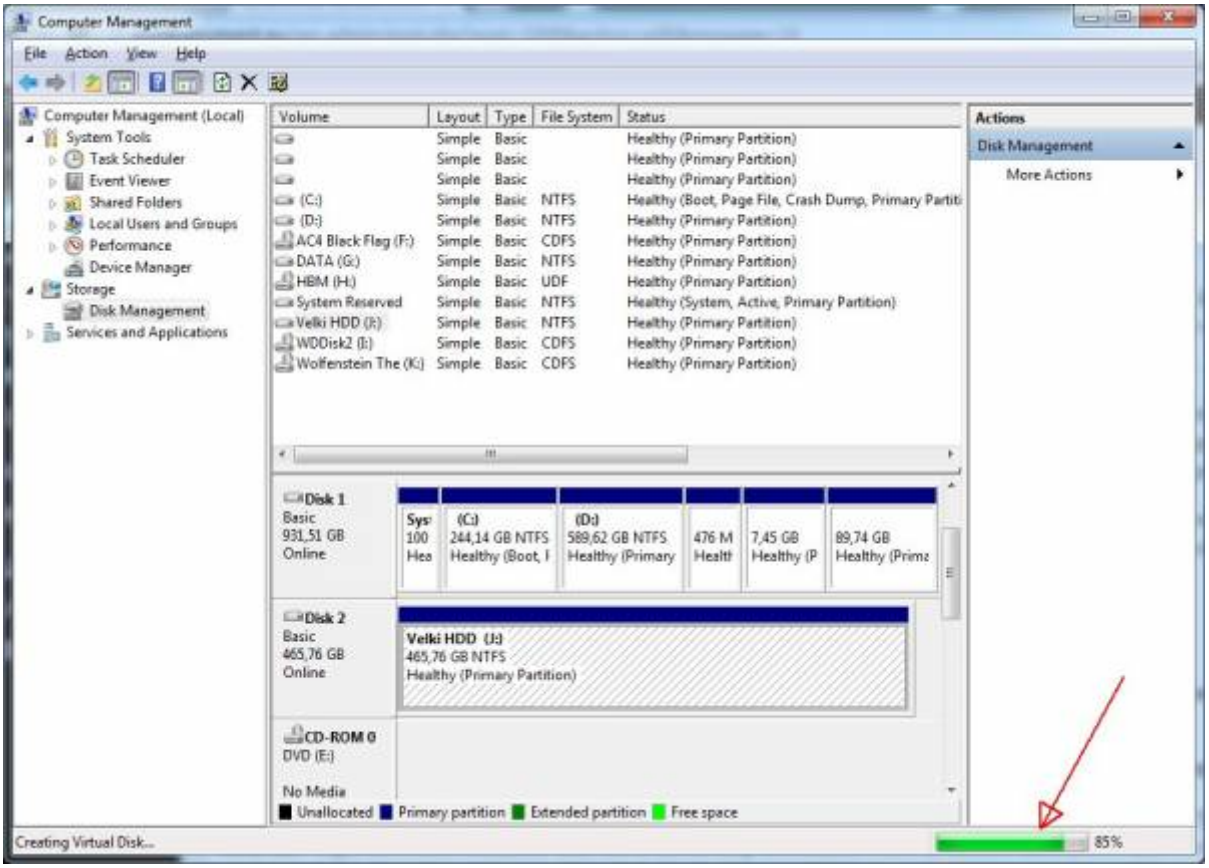


- In the "Create and Attach Virtual Hard Disk" dialog box under **"Location"** select a destination where your VHD will be stored by clicking on the **"Browse"** button. In the **"Virtual hard disk**

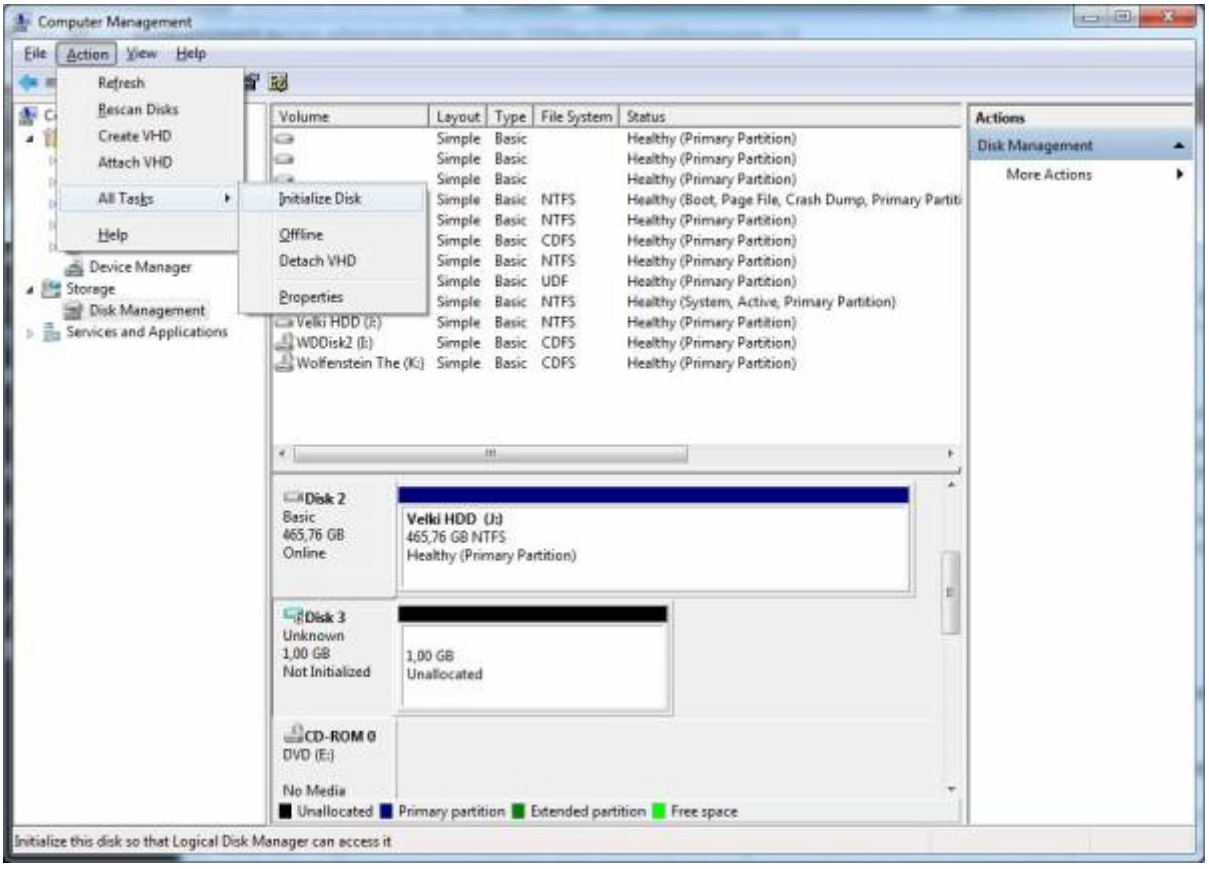
size” input field enter a numeric value and from the drop-down menu select the desired units (I’ll set mine to 1 GB). Leave your VHD as **“Fixed size”** and confirm all setting by clicking on the **“OK”** button.

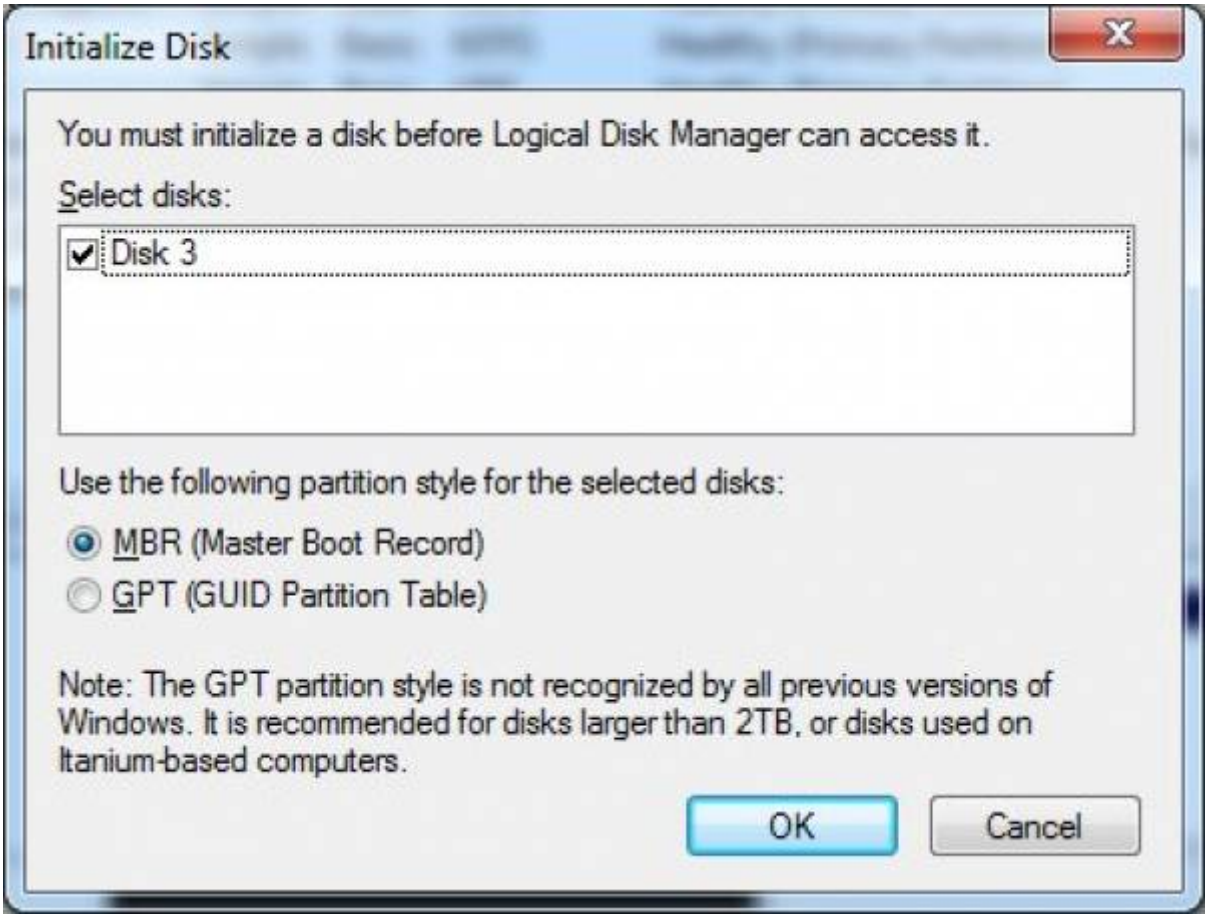


- Now wait for the VHD to be created (note the progress bar to the lower right of the Disk Management console window).

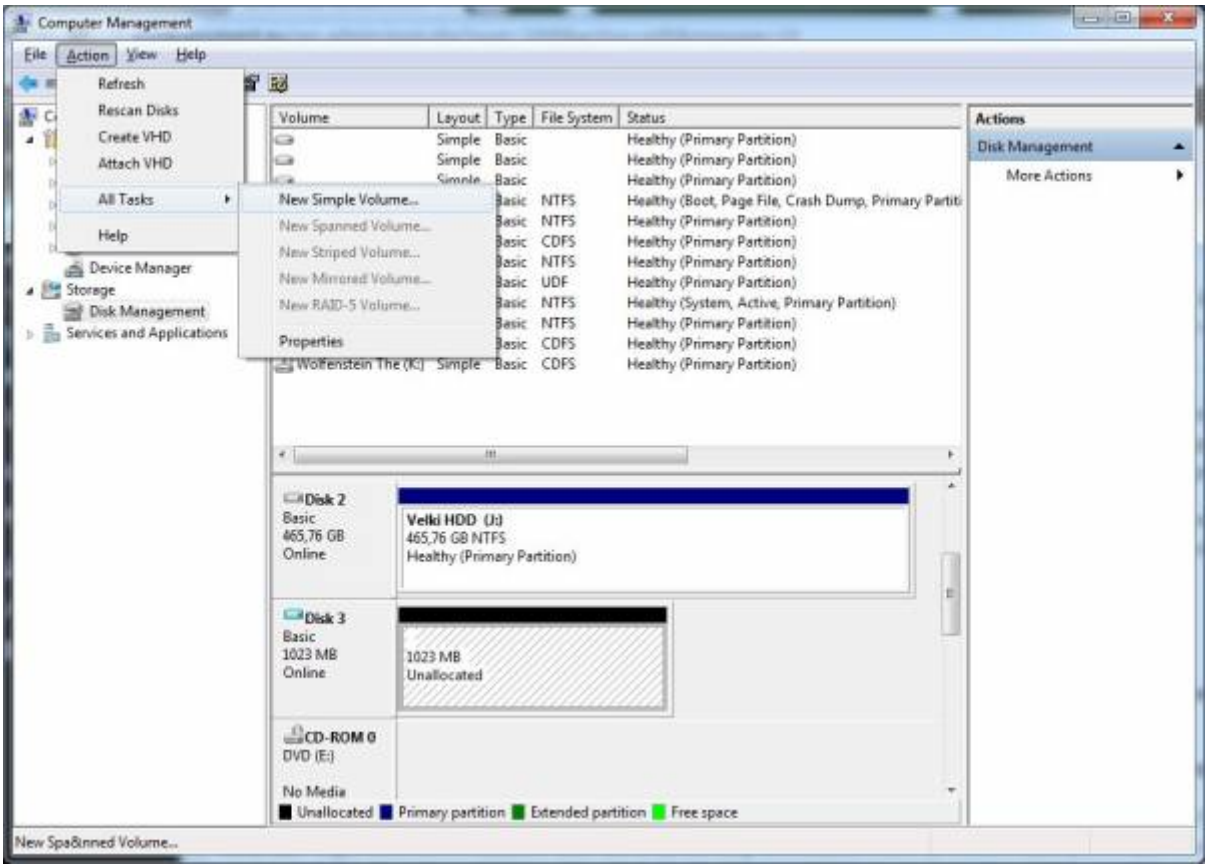


- Once the new drive is created it can be seen as a **“Disk X”** (where X is the drive number under which Windows created the VHD – in my case its **“Disk 3”**) in the Disk Management console window. Now select it by clicking on it and go to **Action → All Tasks → Initialize Disk**. In the **“Initialize Disk”** dialog box confirm by clicking on the **“OK”** button that you indeed wish to initialize the disk.

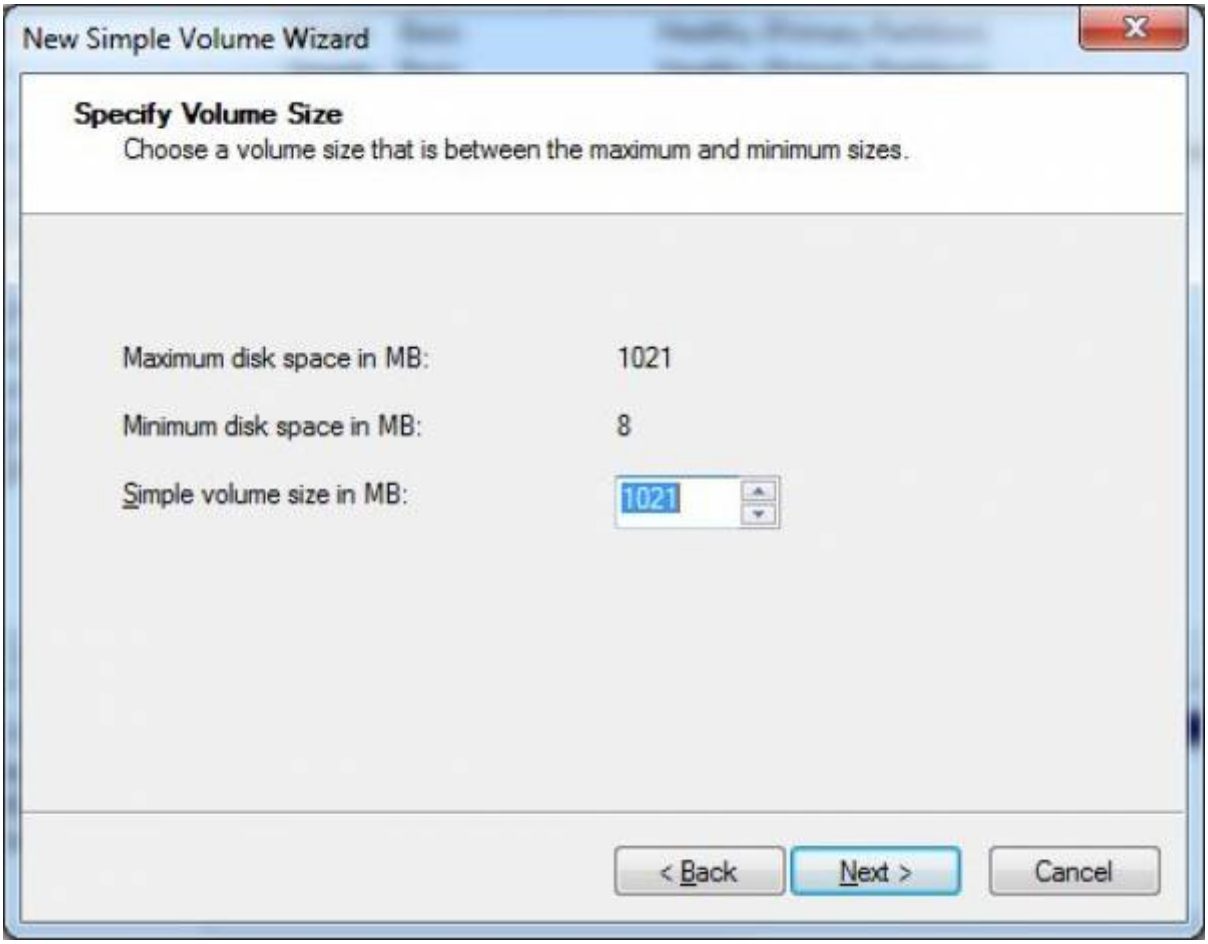




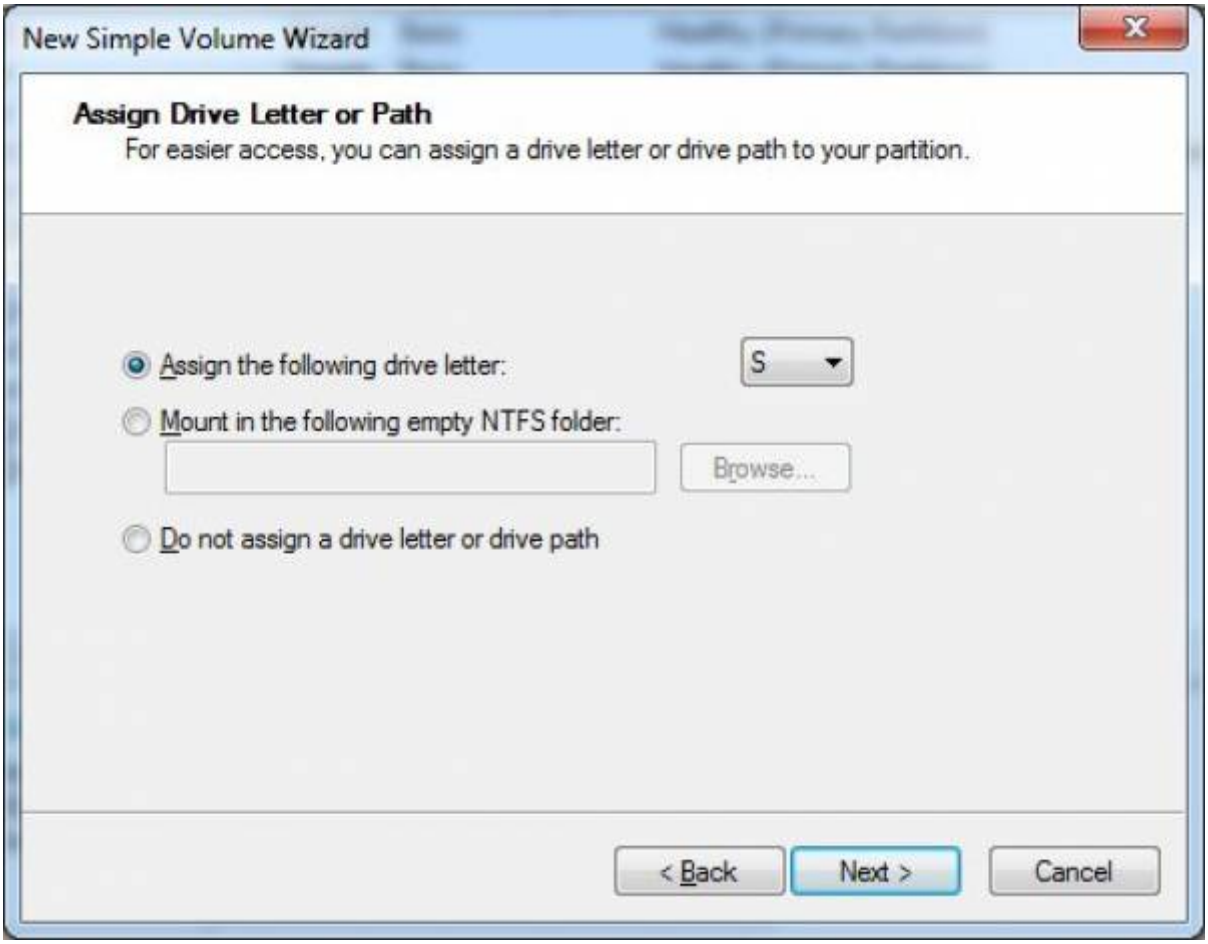
- Select the volume frame of the newly initialized disk and go to **Action → All Tasks → New Simple Volume**.



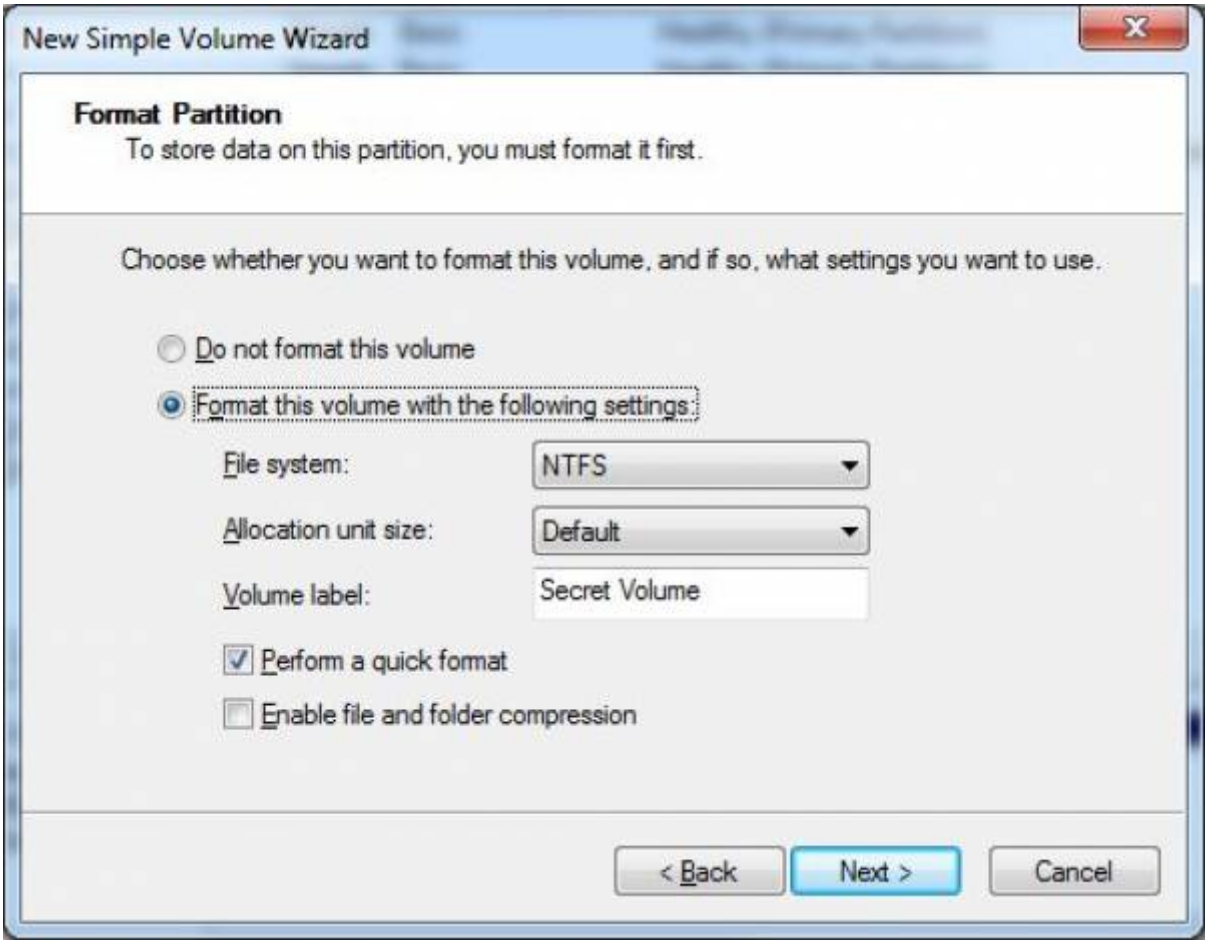
- Click the **“Next”** button on the **“New Simple Volume Wizard”** welcome screen and on the second screen of the Wizard specify the size of the volume.



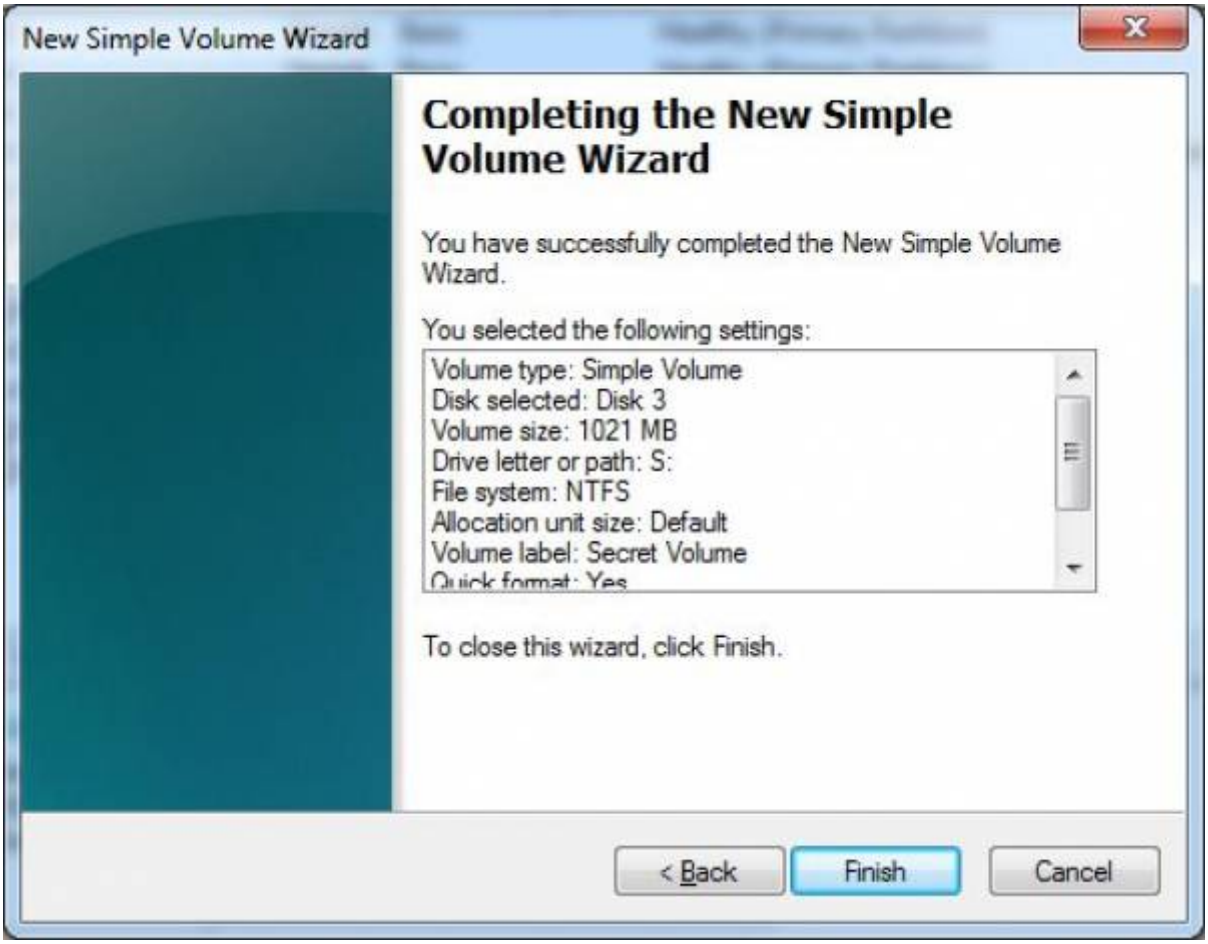
- In the following specify the drive letter (I'll use S for 'secret' in this case).



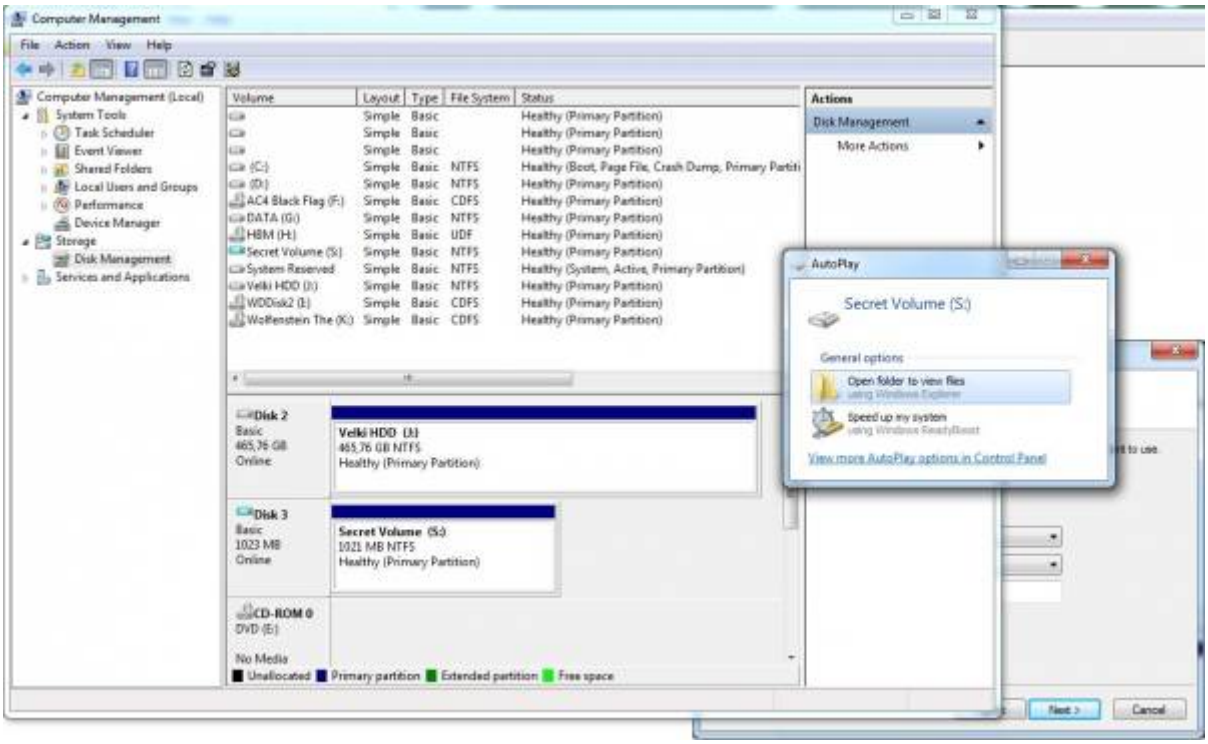
- Set formatting options for the volume and give it a name (let’s call it Secret Volume… obviously).



- Confirm all settings and click on the **“Finish”** button.

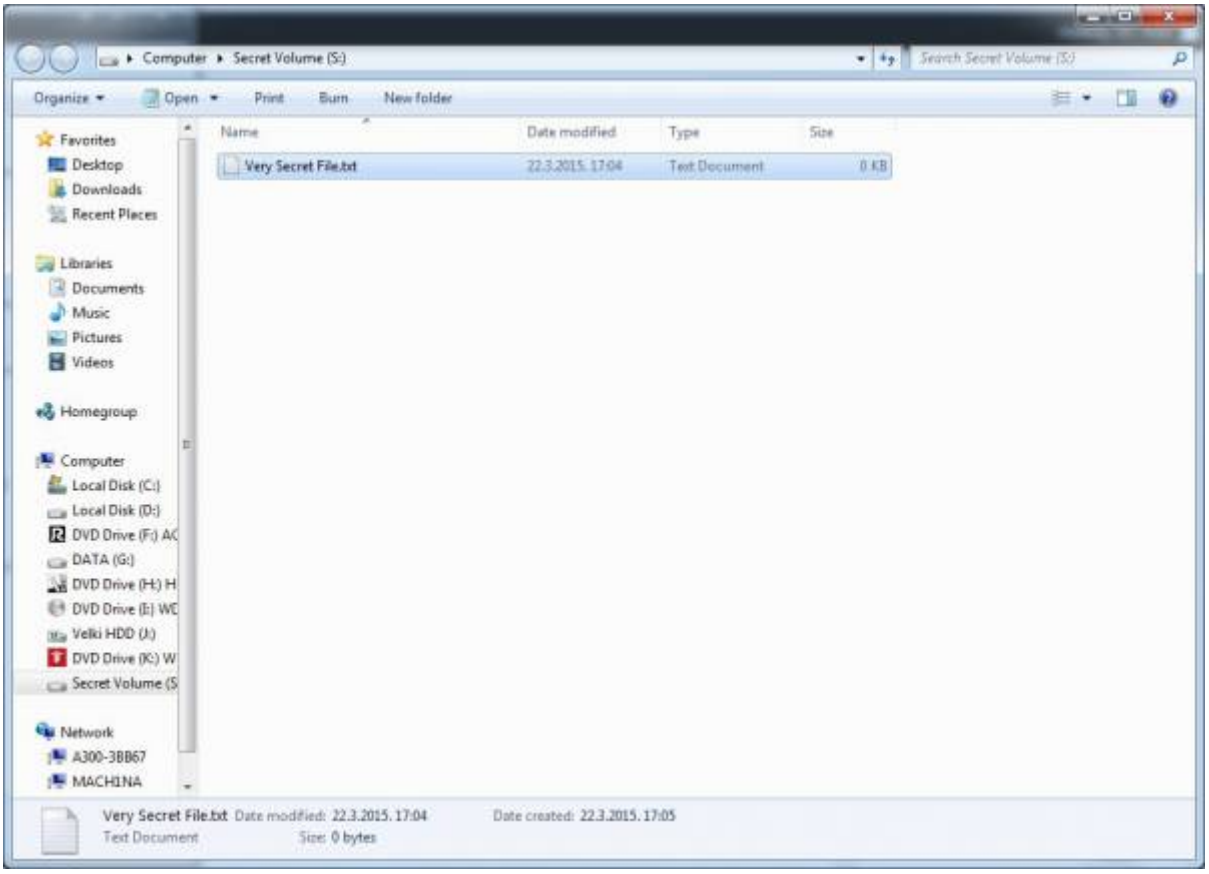


- Once done you can observe the newly created Volume in the Disk Management console and you should also get an **“AutoPlay”** dialog offering to open the volume folder. Go ahead and open it because we ought to copy something on it (for instance something we would like to encrypt).



Copy the data and encrypt the VHD

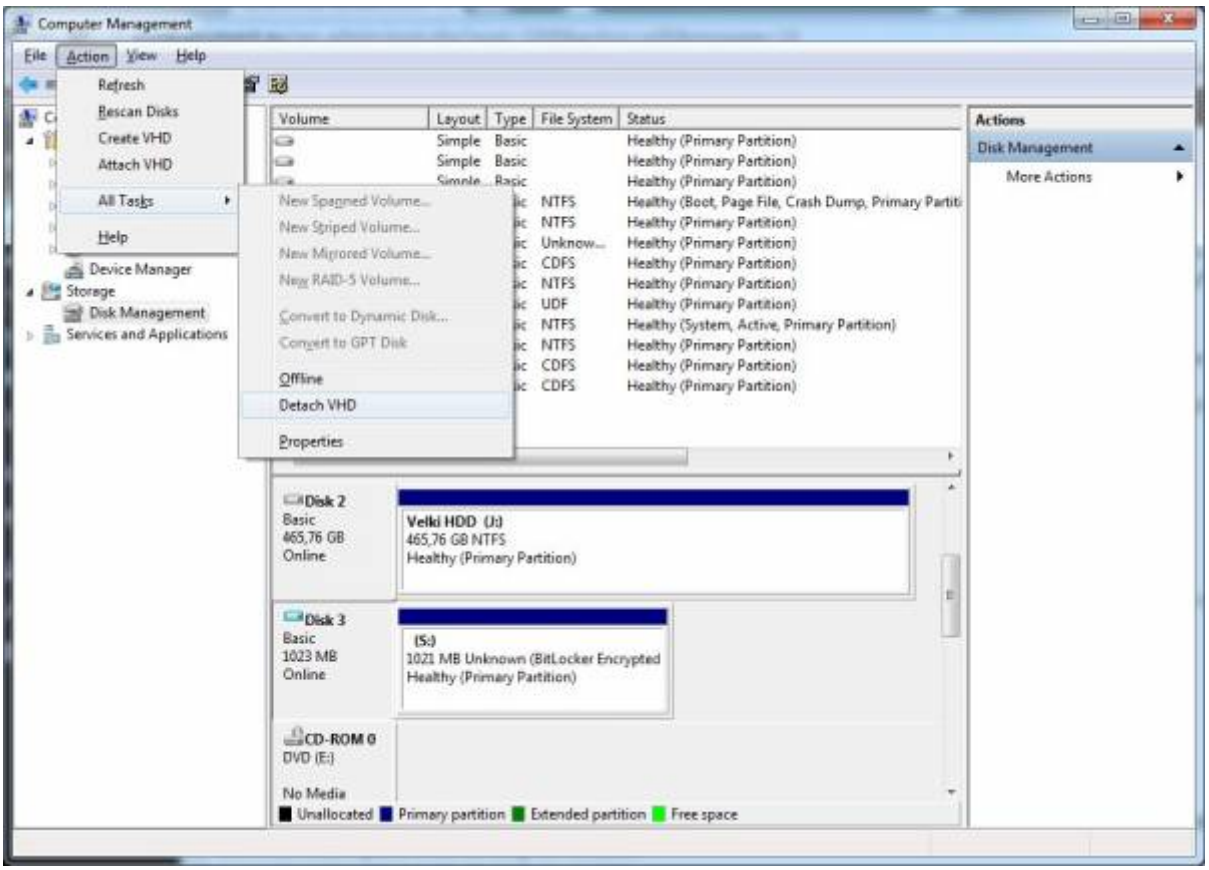
- Once you've opened the new volume in Windows Explorer copy what you'd like to encrypt to it.



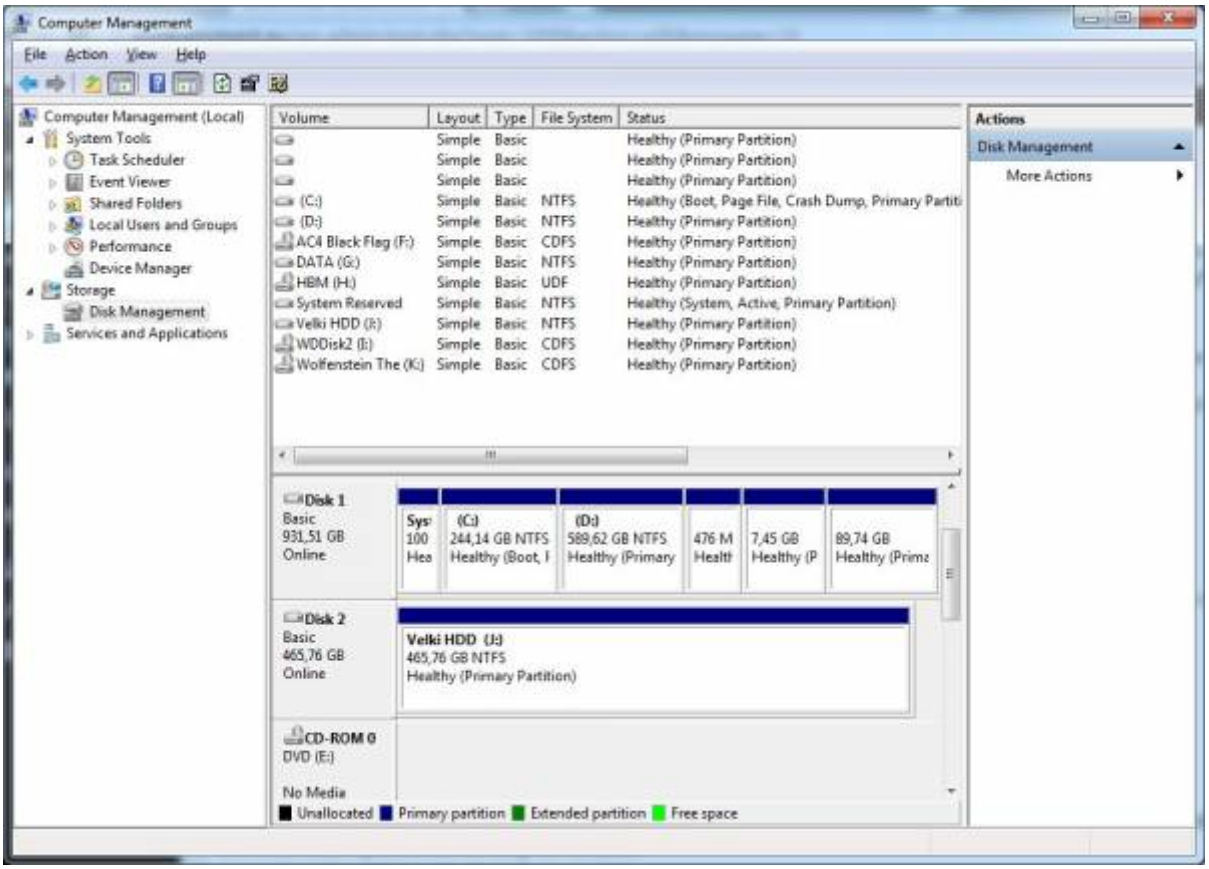
- Now from Windows Explorer select the drive that you'd like to encrypt and u can run **BitLocker** by either going to **File → Turn on BitLocker** or right click on the drive itself and select the same option from the drop-down menu.

“Hide” your newly encrypted data

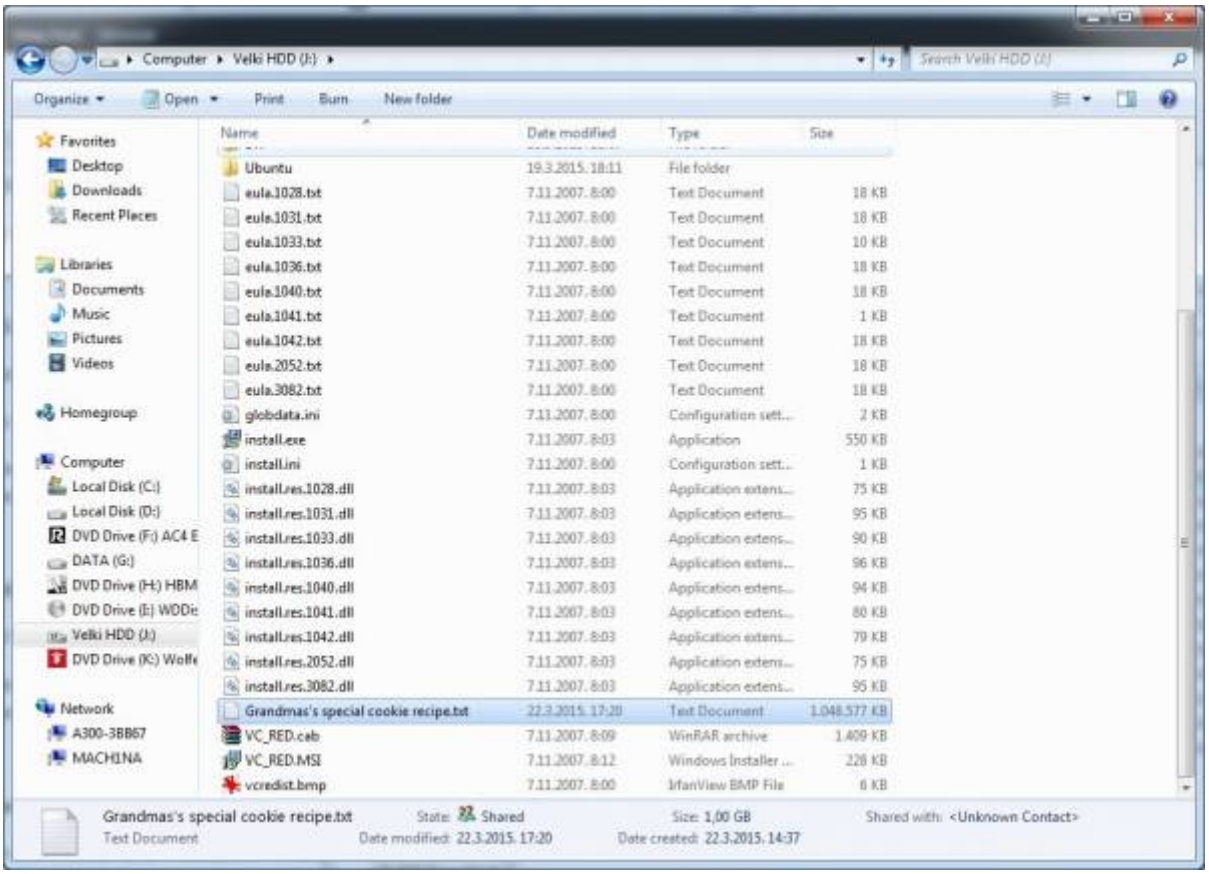
- To secure our valuable data even further we can now “hide” our VHD by taking it offline and detaching it, so go to Disk Management console once more and select the encrypted VHD. Go to **Action → All Tasks → Detach VHD** or right click on the volume and select the same option from the drop-down menu. Confirm the physical VHD file location by clicking the OK button from the **“Detach Virtual Hard Disk”** dialog box.



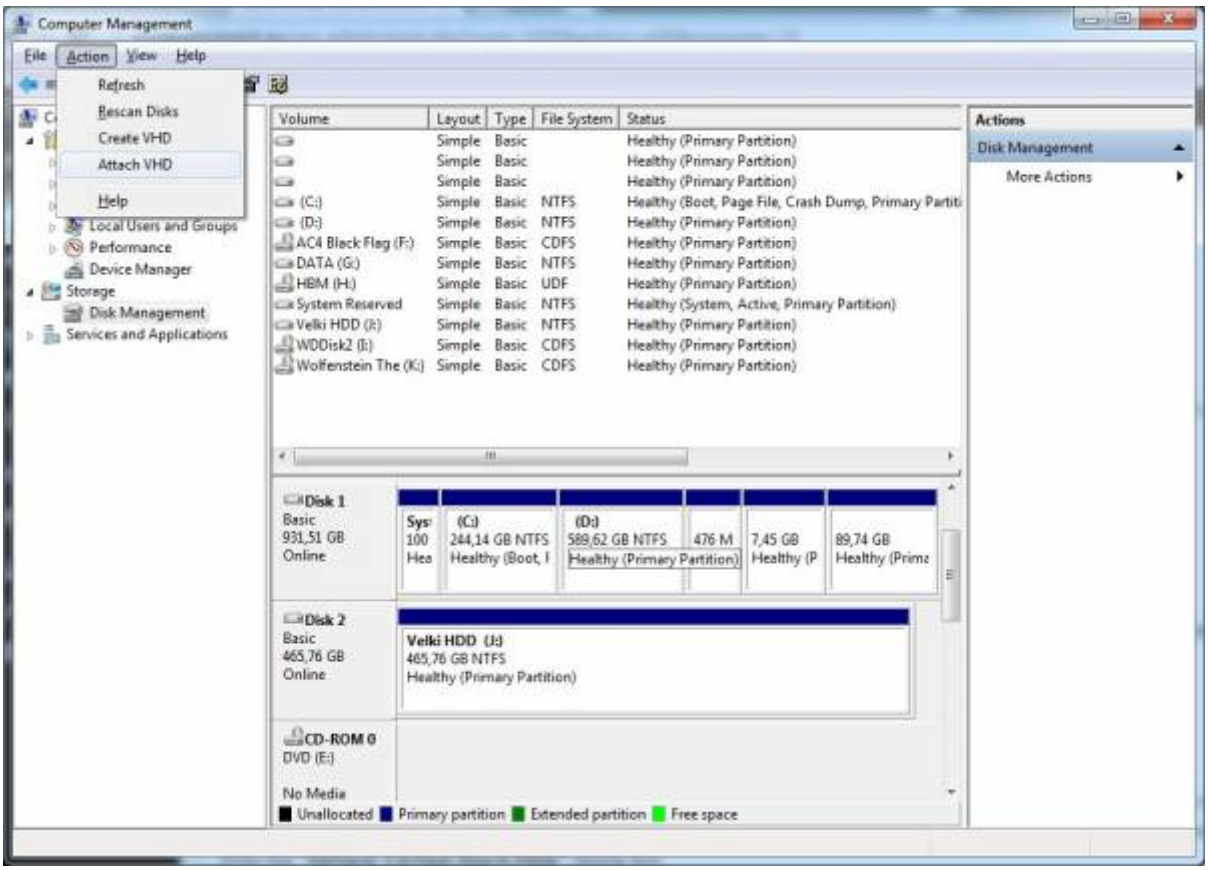
- Hey Presto! No more VHD. You can confirm that the drive was successfully detached by examining the drives list in the Disk Management console where now you should be unable to find the detached drive. Now your encrypted VHD is just another file on your computers physical hard drive.



- To make the ruse even more convincing (although I'd recommend not making a habit out of this because it can lead to data corruption and other issues when latter reattaching the VHD back where it belongs) you can now rename our Secret_VHD.vhd to – say – Grandma's special cookie recipe.txt. Now do keep in mind that the size of the file itself remains unchanged so come up with a naming convention and a file type extension that make the file size credible. You can also move the encrypted data to a more suitable location. So if you've opted for a file name in the lines of let's say Grimm_S04E02.mp4, you should probably keep it in the same folder where you keep the rest of your Grimm Season 4 episodes (ok, ok – i know you got the picture by now, so sorry if I'm being a bit overzealous).



- To restore your data you should reattach the VHD back but remember to first rename it back to what it was originally called (in our case Secret_VHD.vhd). When you've renamed the file (no need to return it in the same exact location on the physical disk where it was originally created) go to the Disk Management Console and then select **Action → Attach VHD**.



- Browse for the VHD file and confirm with **“OK”** once You’ve found and selected it.

- When the VHD is attached the BitLocker unlock window automatically pops up. From here you can choose to do one of the following:
  - Unlock the drive upon attaching it by inputting the drive unlock password and confirming with “OK” or;
  - Keep the drive attached and visible (though not readable) but locked by simply clicking on the “Cancel” button in the BitLocker dialog window.

And we're done. I know it looks like allot if you've never done this kinda thing before but believe me – it's quick and easy once you get the hang of it, and what's more important: it'll keep your data safe in a more flexible and reliable way then thus far.

From:
https://wiki.plecko.hr/ - **Eureka Moment**

Permanent link:
https://wiki.plecko.hr/doku.php?id=windows:client_os:bitlocker_containers

Last update: **2019/10/31 09:06**