

Module 2: VeraCrypt

Objectives

- Understand how to use VeraCrypt to encrypt a drive
- Understand how to use the plausible deniability function to encrypt a hidden volume inside another regular volume

Tasks

Task 0. Set up the environment.

1. (Recommended) Prepare a Windows 10 virtual machine
You can download a free premade Windows 10 virtual machine at <https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>
The virtual machine will expire after 90 days. The password is Passw0rd!
You can choose whichever VM platform you would like.

Virtual Machines

Test IE11 and Microsoft Edge Legacy using free Windows 10 virtual machines you download and manage locally

Select a download

Virtual Machines

MSEdge on Win10 (x64) Stable 1809

Choose a VM platform:

VirtualBox

Download .zip >

ⓘ Before installing, please note:

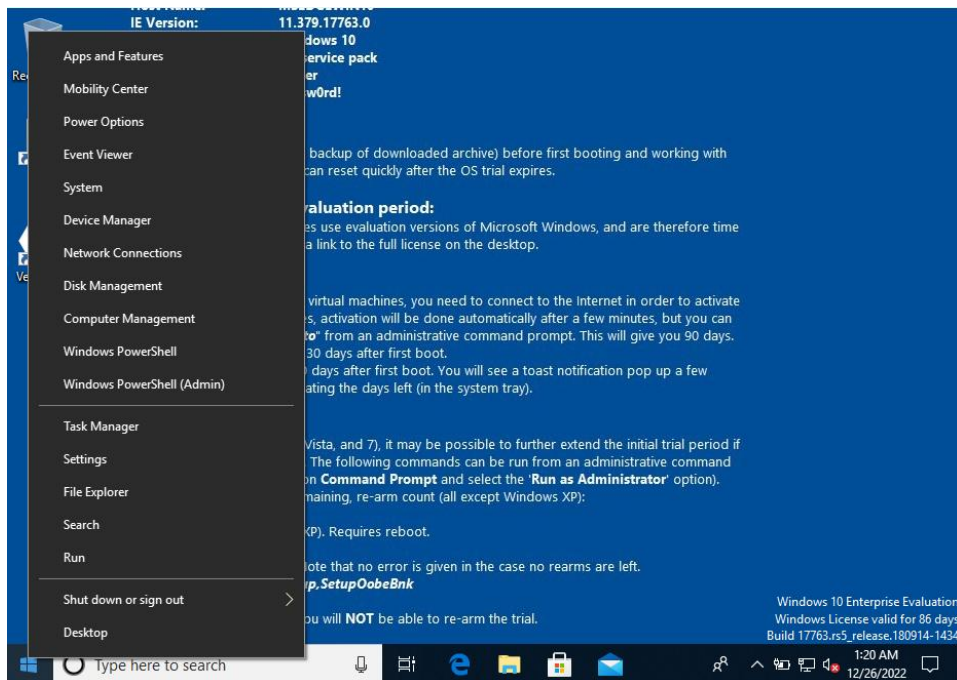
These virtual machines expire after 90 days. We recommend setting a snapshot when you first install the virtual machine which you can roll back to later. Mac users will need to use a tool that supports zip64, like [The Unarchiver](#), to unzip the files.
The password to your VM is "Passw0rd!"

2. Prepare a USB

Note: If you are using VirtualBox, you can download GuestAdditions and the extension pack to be able to use a physical USB.

If you have a physical USB, you can skip straight to Task 1.

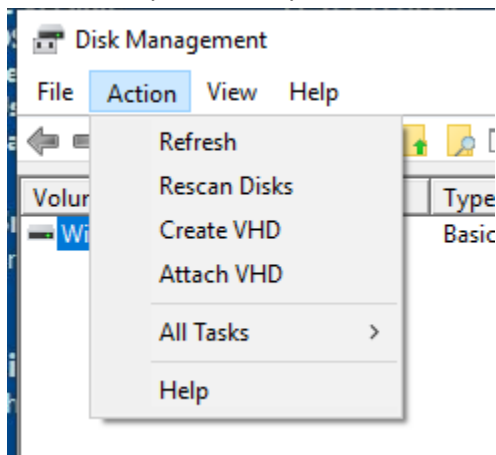
Here is how to create a virtual USB:



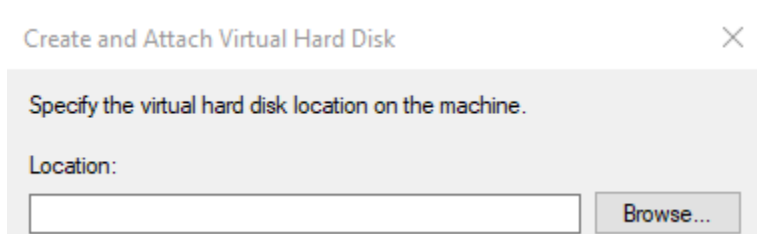
-Right click the windows icon on the bottom left of the screen and click “Disk Management”

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
Windows 10 (C:)	Simple	Basic	NTFS	Healthy (S...	40.00 GB	20.93 GB	52 %

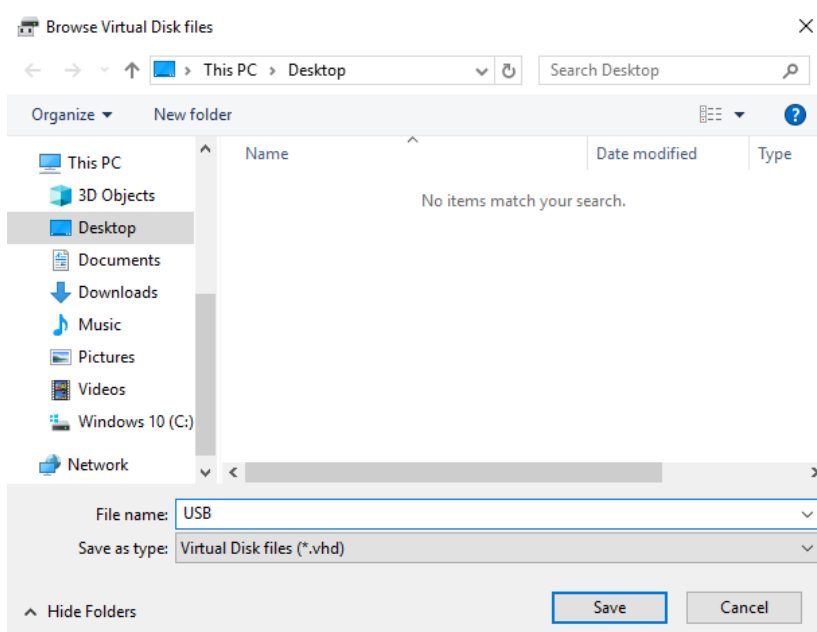
-Make sure your main system is selected



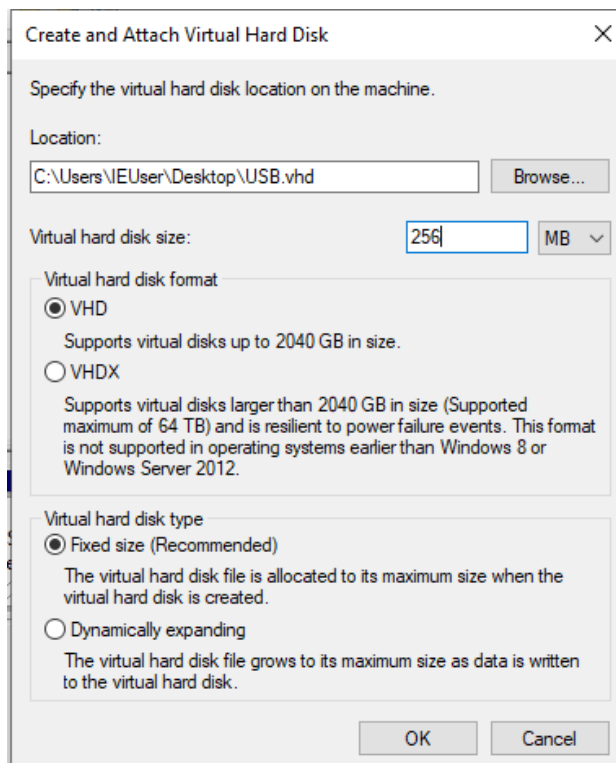
-Click the Action tab and click “Create VHD”



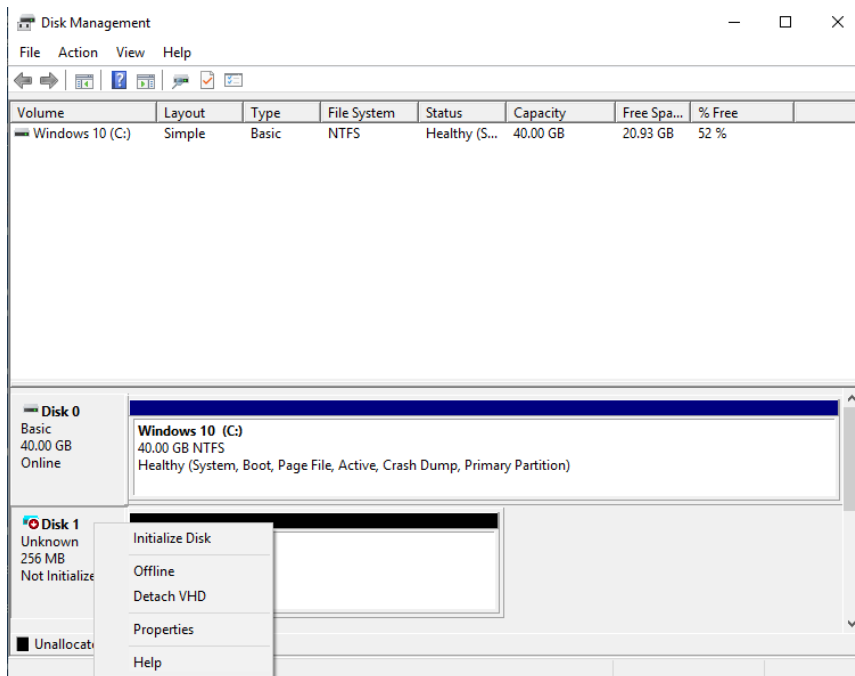
-Click Browse



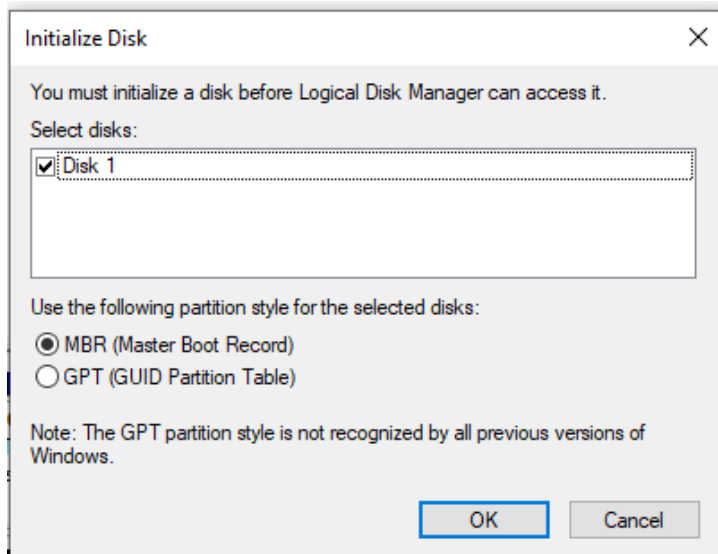
-Navigate to where you would like to save your virtual USB and name your USB. When you are done click “Save”



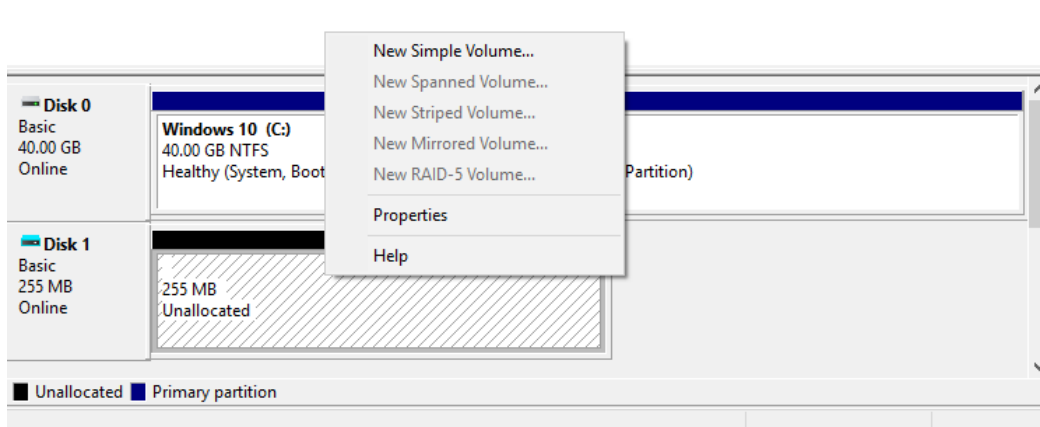
-Type the size you want your virtual hard disk to be and then click “OK” at the very bottom



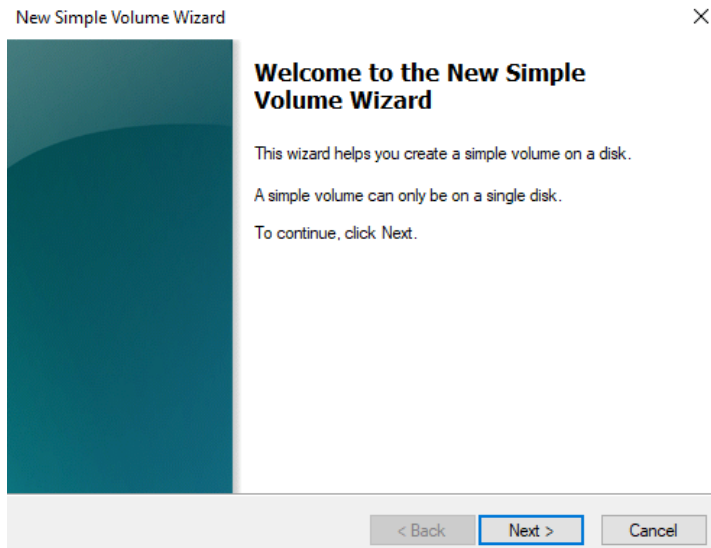
-You should now see the new USB on the bottom of the window. Right click it and click “Initialize Disk”



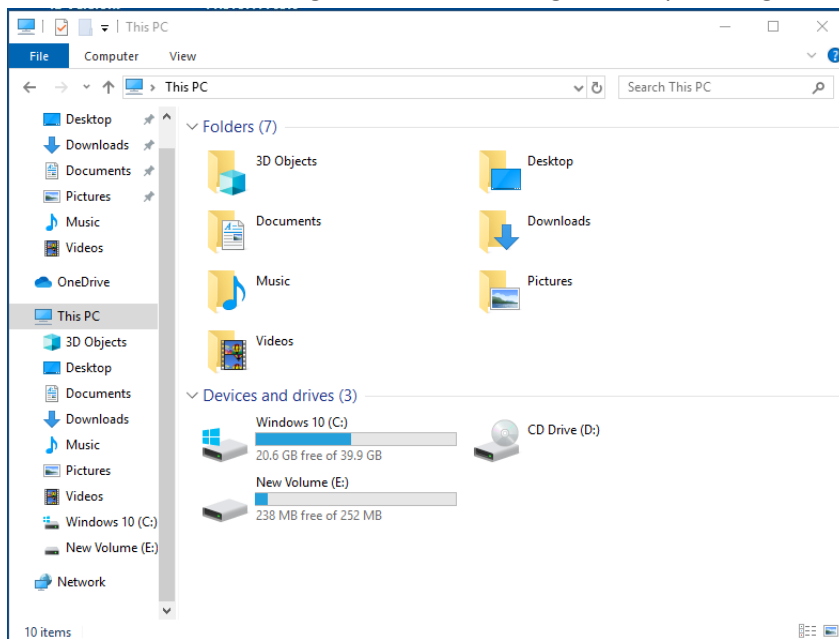
-Click OK



-Right click the unallocated space and click “New Simple Volume...”



-You do not need to change the default settings, so keep clicking next until you reach the end and Finish.



-You should now be able to see your virtual USB in the File Explorer.

Task 1. Install VeraCrypt

1. Install VeraCrypt at <https://www.veracrypt.fr/en/Downloads.html>



[Home](#) [Source Code](#) [Downloads](#) [Documentation](#) [Donate](#) [Forums](#)

Note to publishers: If you intend to host our files on your server, please instead consider linking to this page. It will help us prevent spreading of obsolete versions, which we believe is critical when security software is concerned. Thank you.

[Supported versions of operating systems](#)

PGP Public Key: https://www.idr.fr/VeraCrypt/VeraCrypt_PGP_public_key.asc (ID=0x680D16DE, Fingerprint=5069A233D55A0EEB174A5FC3821ACD02680D16DE)

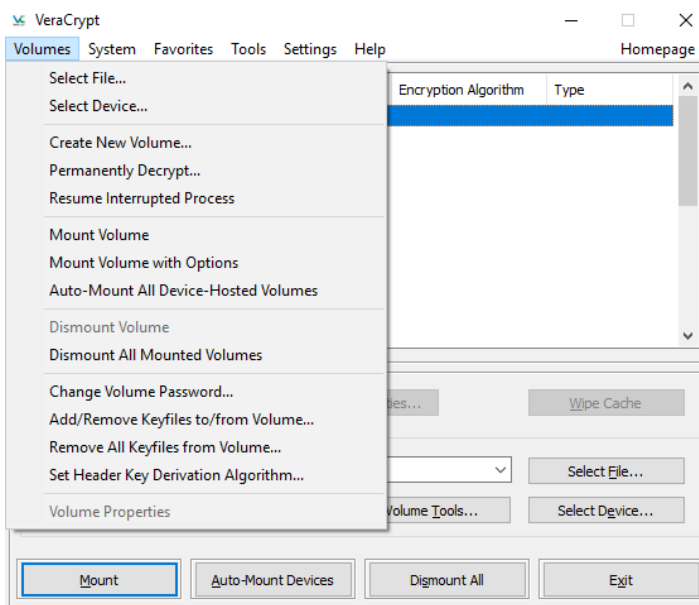
Bleeding edge builds based on latest source code are available at <https://sourceforge.net/projects/veracrypt/files/VeraCrypt%20Nightly%20Builds/>.

Latest Stable Release - 1.25.9 (Saturday February 19, 2022)

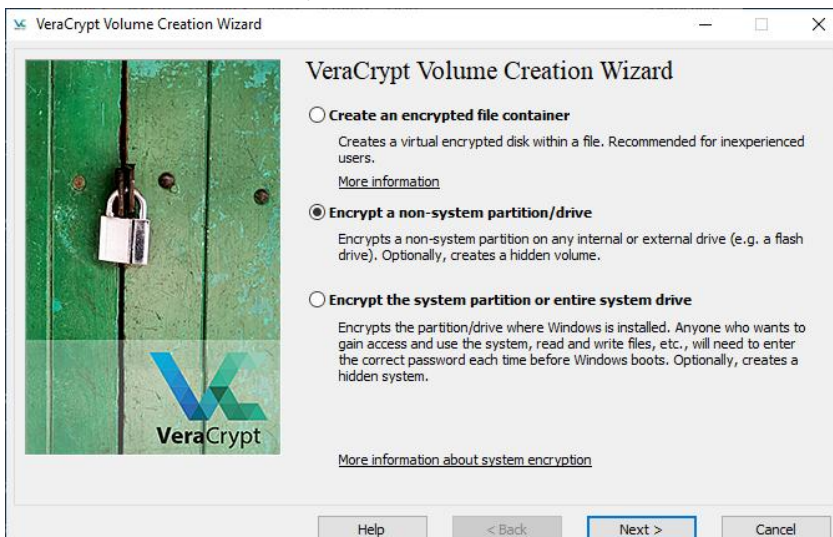
- Windows:**
 - EXE Installer: [VeraCrypt Setup 1.25.9.exe](#) (21.1 MB) (PGP Signature)
 - MSI Installer (64-bit) for Windows 10 and later: [VeraCrypt_Setup_x64_1.25.9.msi](#) (29 MB) (PGP Signature)
 - Portable version: [VeraCrypt Portable 1.25.9.exe](#) (20.9 MB) (PGP Signature)
 - Debugging Symbols: [VeraCrypt_1.25.9_Windows_Symbols.zip](#) (18.4 MB) (PGP Signature)
- macOS:**
 - macOS Mavericks 10.9 and later: [VeraCrypt_1.25.9.dmg](#) (11.7 MB) (PGP Signature)
 - [OSXFUSE](#) 3.10 or newer must be installed.
- Linux:**
 - Generic Installers: [veracrypt-1.25.9-setup.tar.bz2](#) (41.5 MB) (PGP Signature)
 - Linux Legacy installer for 32-bit CPU with no SSE2: [veracrypt-1.25.9-x86-legacy-setup.tar.bz2](#) (13.8 MB) (PGP Signature)
 - Debian/Ubuntu packages:
 - Debian 11:
 - GUI: [veracrypt-1.25.9-Debian-11-amd64.deb](#) (PGP Signature)
 - Console: [veracrypt-console-1.25.9-Debian-11-amd64.deb](#) (PGP Signature)

Task 2. Create the hidden drive using VeraCrypt

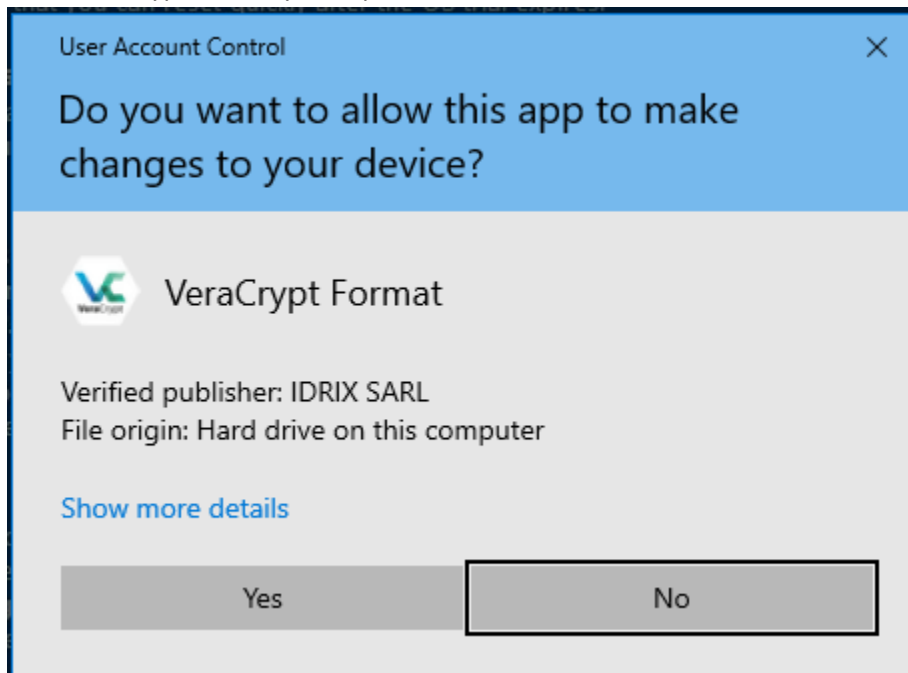
1. Open VeraCrypt



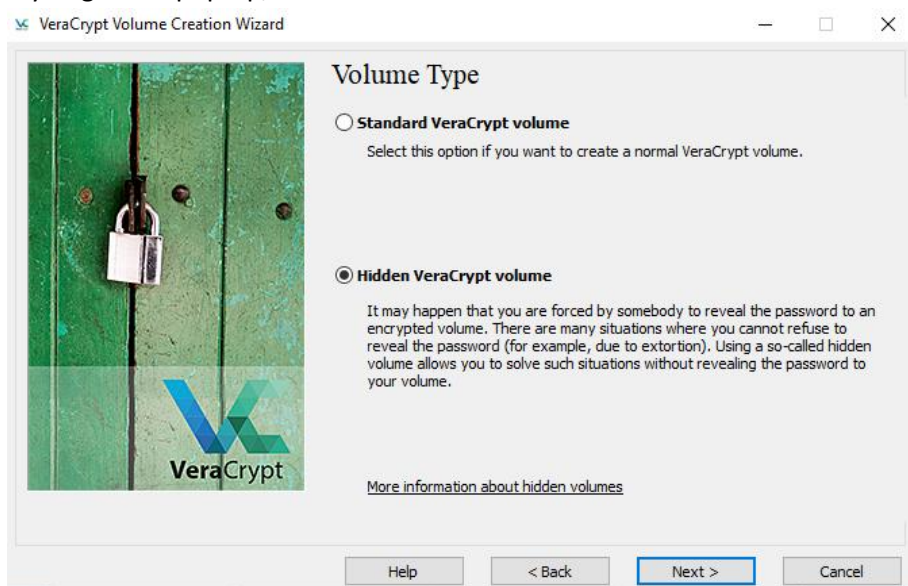
2. Under the “Volumes” tab, click “Create a New Volume”



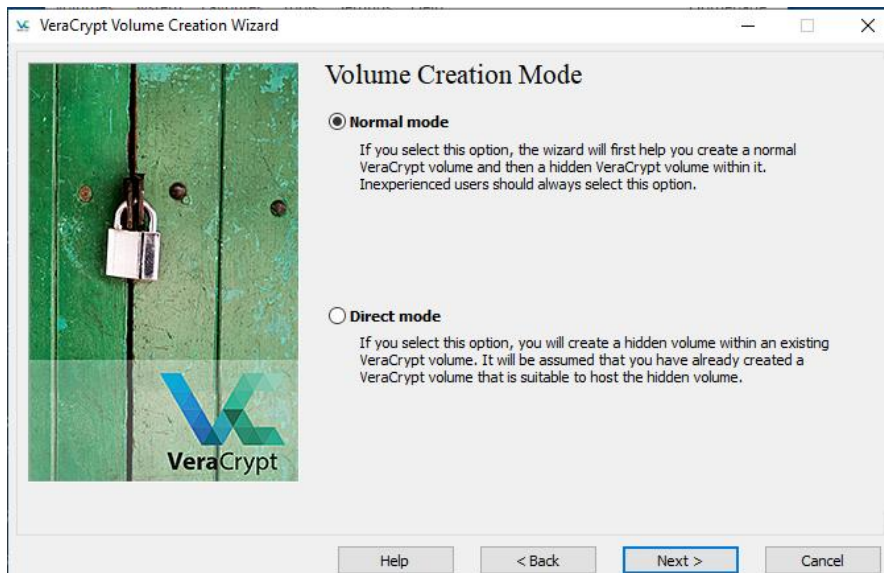
3. Select "Encrypt a non-system partition/drive" and click "Next >"



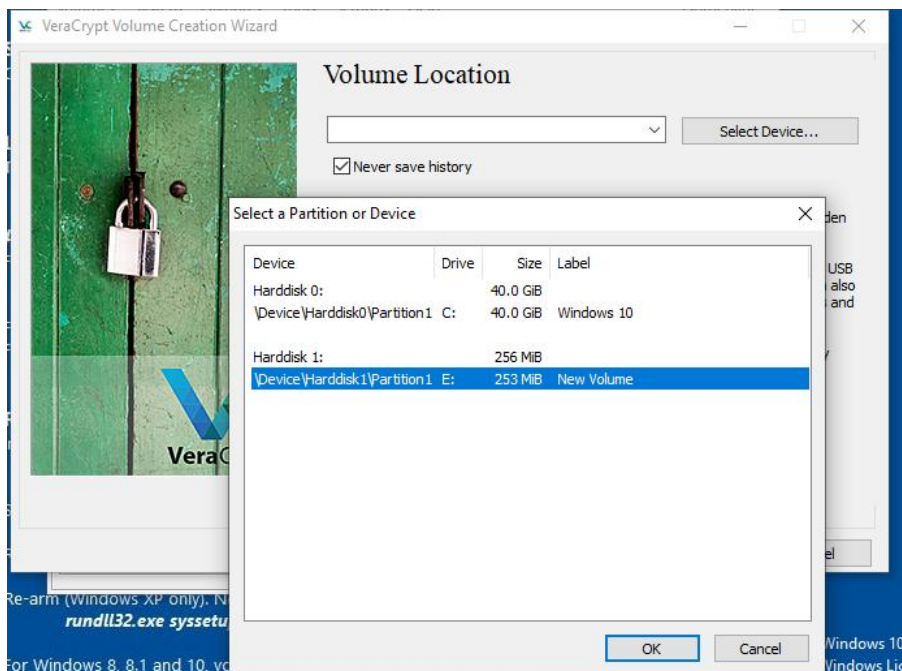
4. If you get this pop-up, click Yes



5. Select "Hidden VeraCrypt volume" and click "Next >"

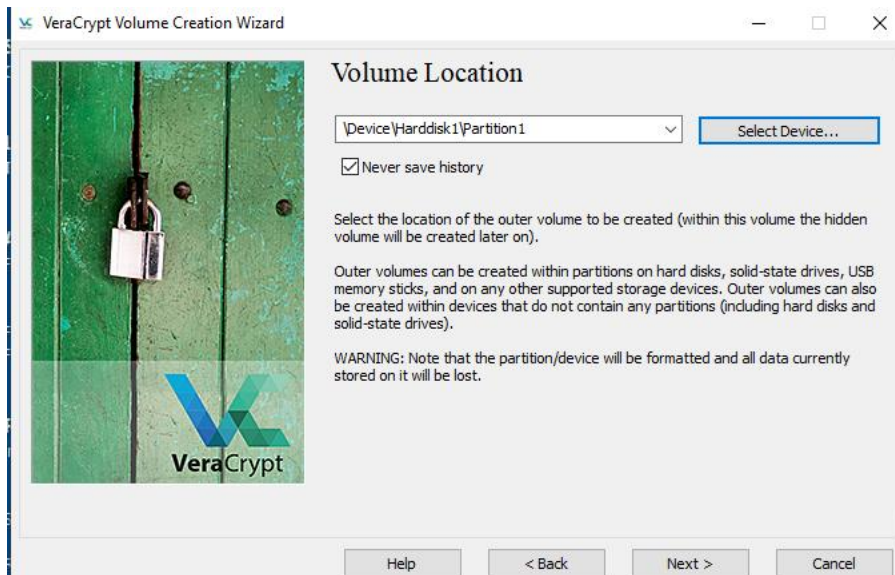


6. Select "Normal mode" and click "Next >"

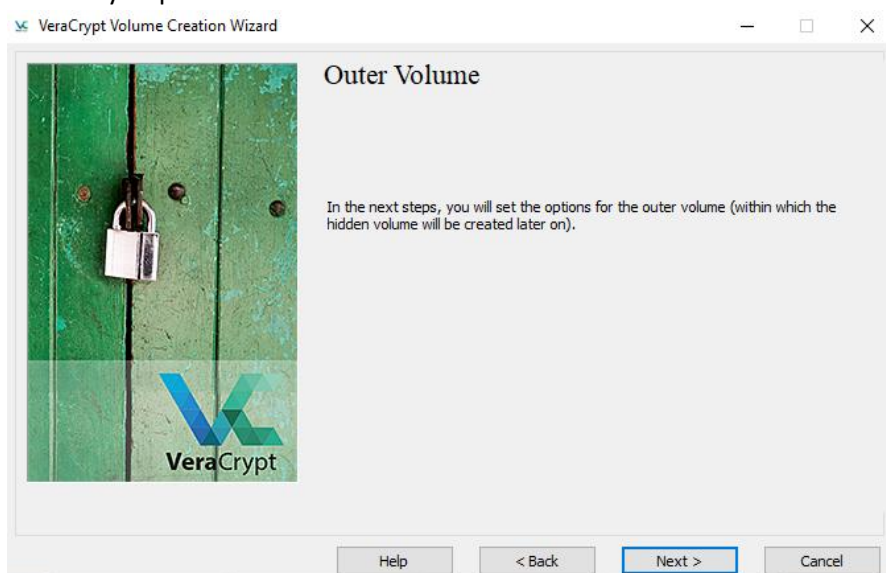


7. Click "Select Device..." and select your USB drive then click "OK".

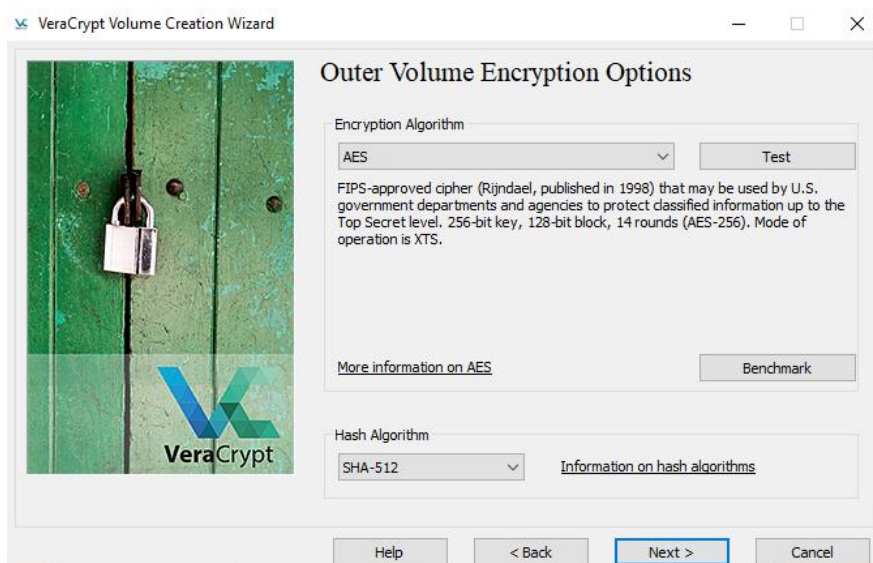
NOTE: BE CAREFUL TO SELECT THE RIGHT USB DRIVE OR YOU WILL LOSE THE DATA ON YOUR DRIVE



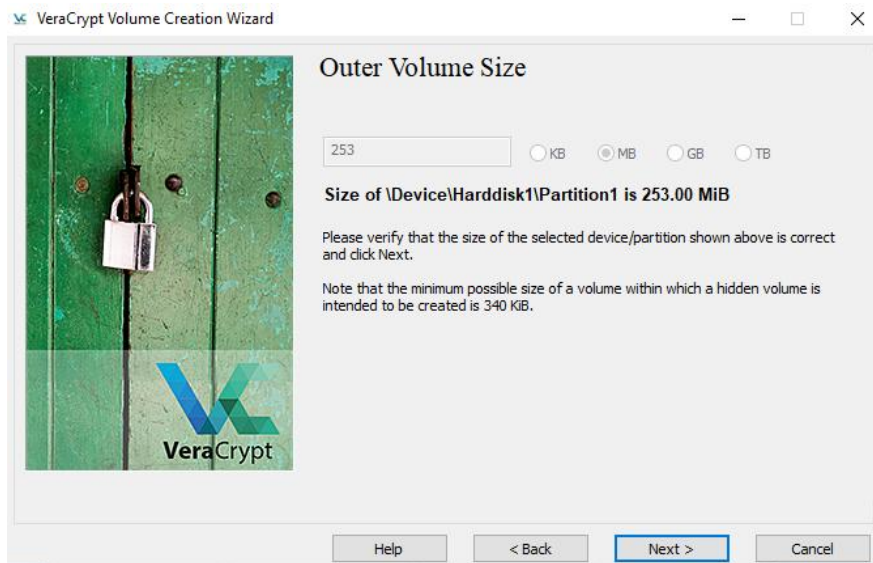
8. Read and make sure you understand the warning, then click “Next >” when you are ready to proceed



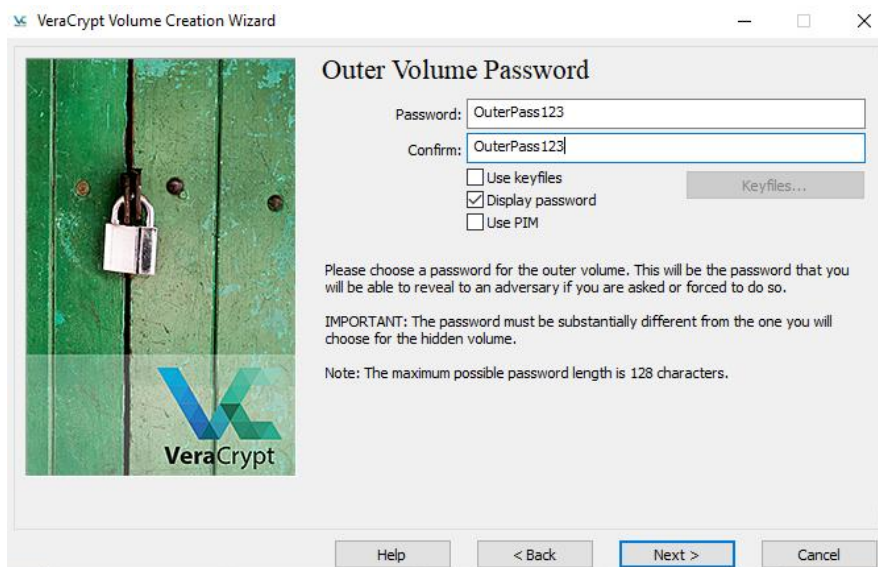
9. Click “Next >”



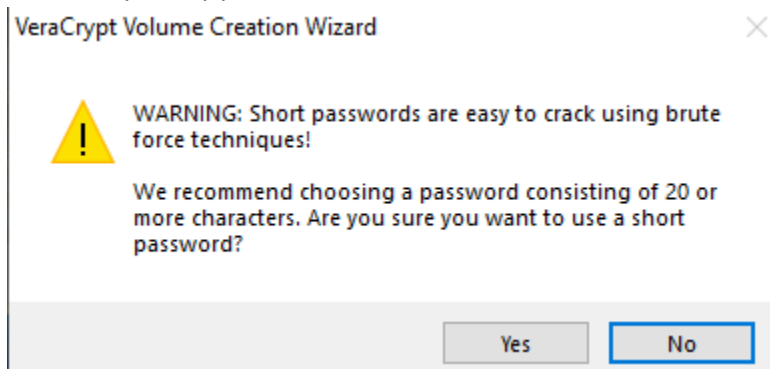
10. You may select whichever algorithms you would like. In this demonstration we are keeping the default settings. Once you have decided, click “Next >”



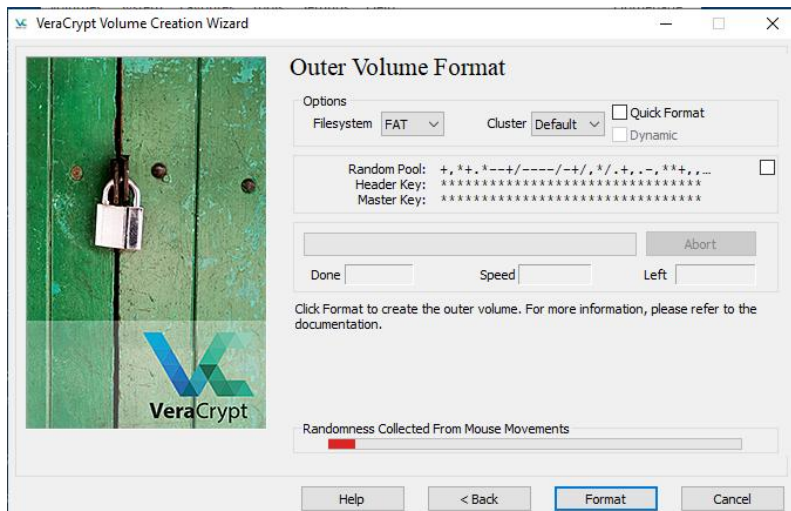
11. Click "Next >"



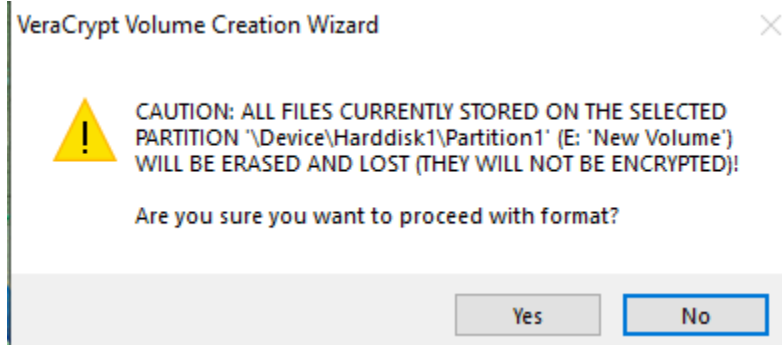
12. Create any decoy password then click "Next >"



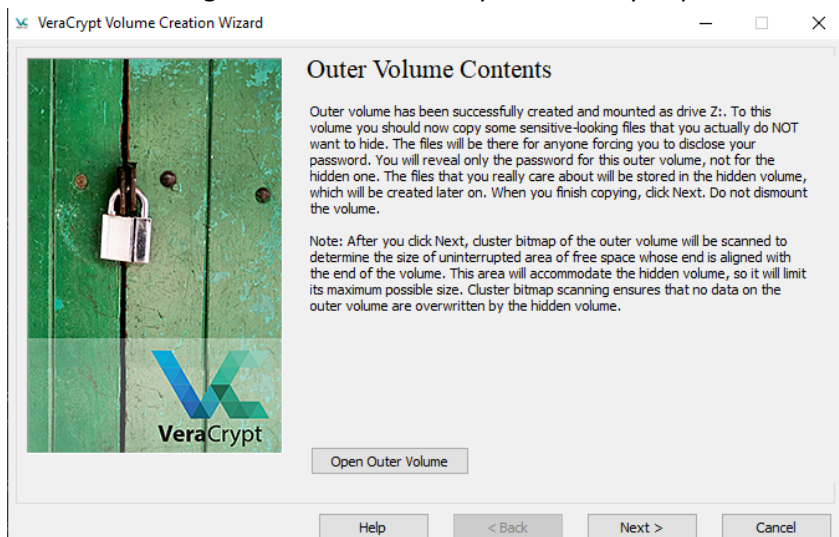
13. If you receive this message, you can click Yes.



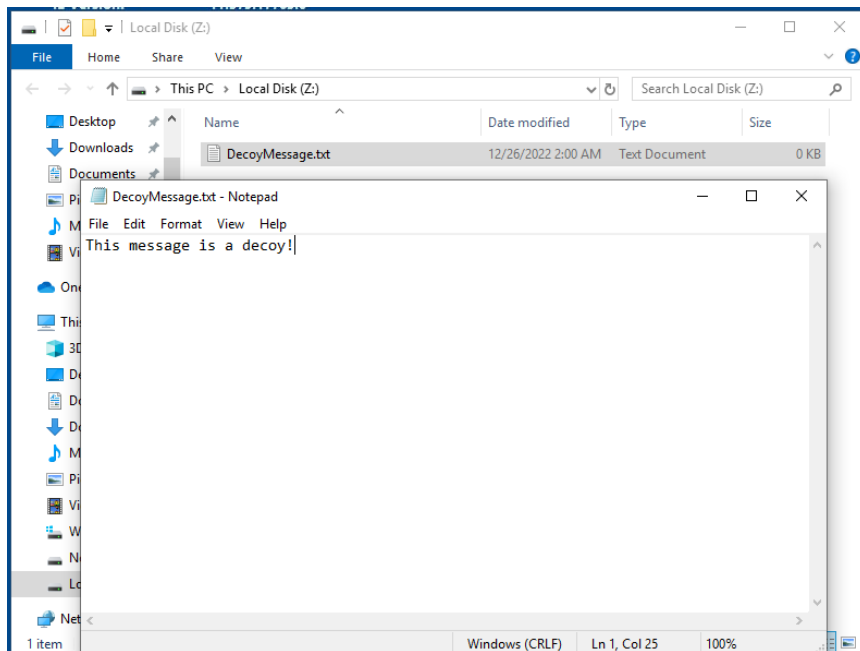
14. Move your mouse around until the gauge is full. Once it is full, click “Format”



15. Read the warning and click “Yes” when you are ready to proceed

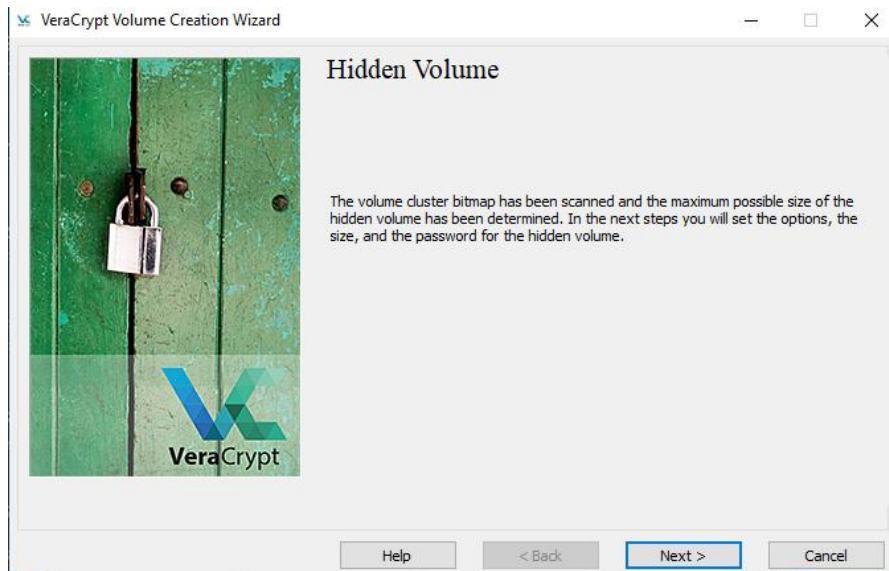


16. Click “Open Outer Volume” to open the hidden storage

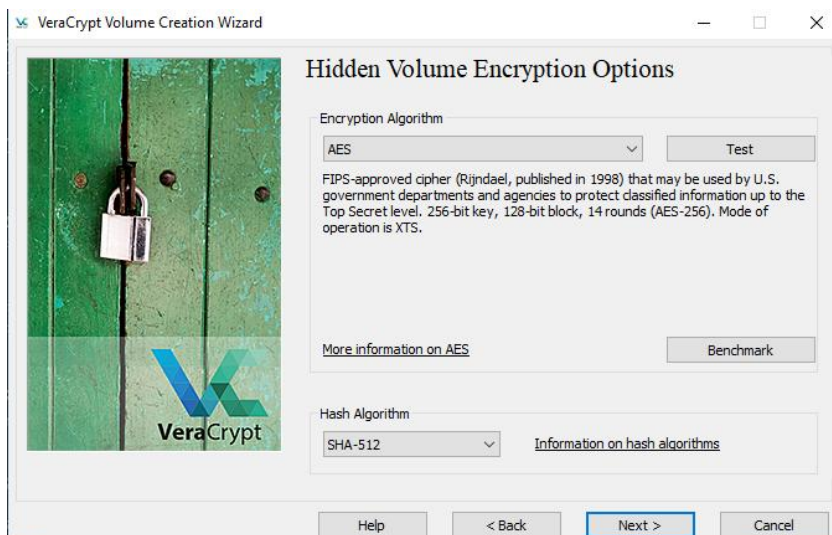


17. Save or create any decoy file. When you are done click “Next >” in VeraCrypt

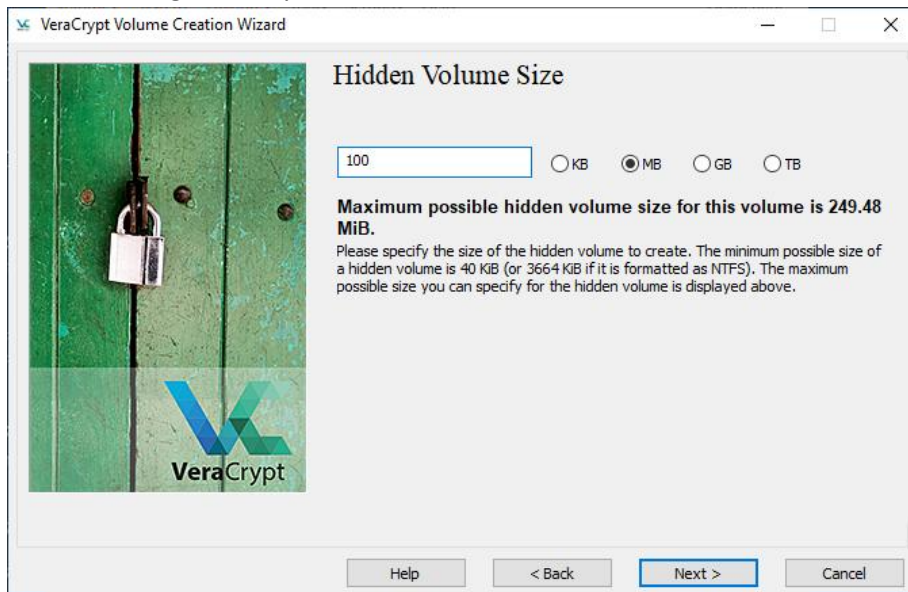
Task 3. Create the main hidden drive



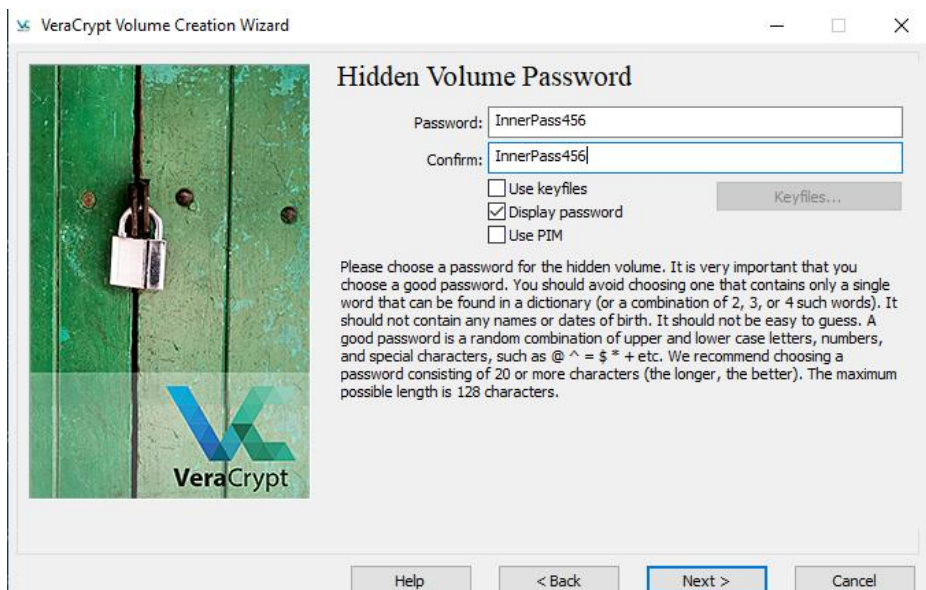
1. Click “Next >”



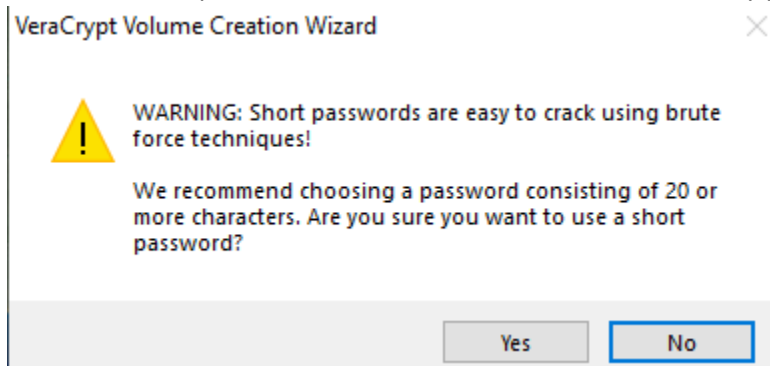
2. Choose the algorithms you would like and click “Next >”



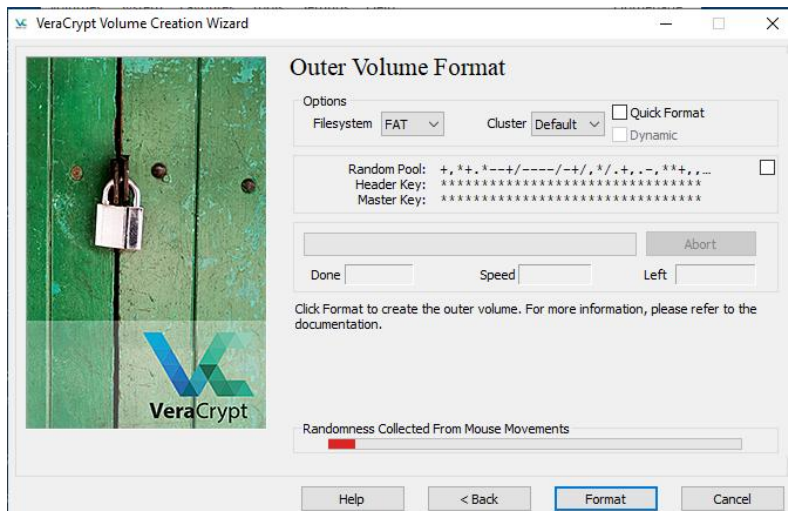
3. Type a number smaller than the maximum possible volume size then click “Next >”



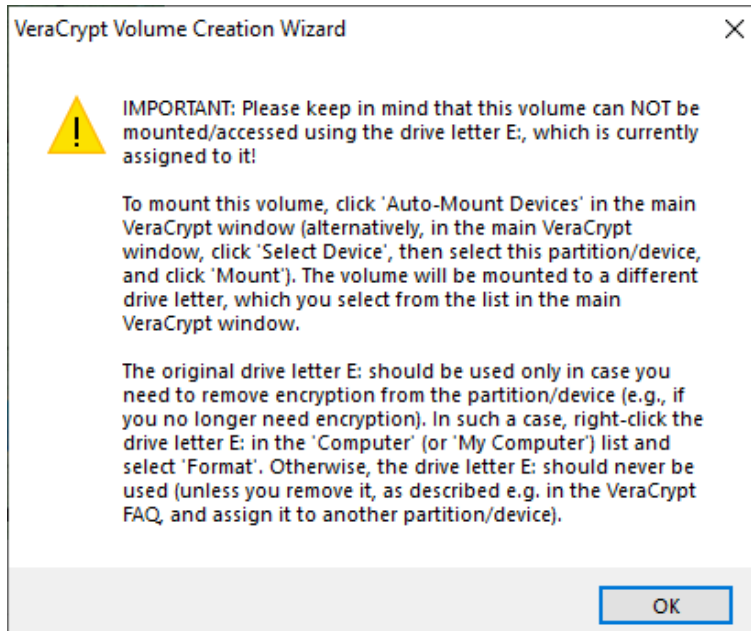
4. Create a secure password, it MUST be different from the decoy password



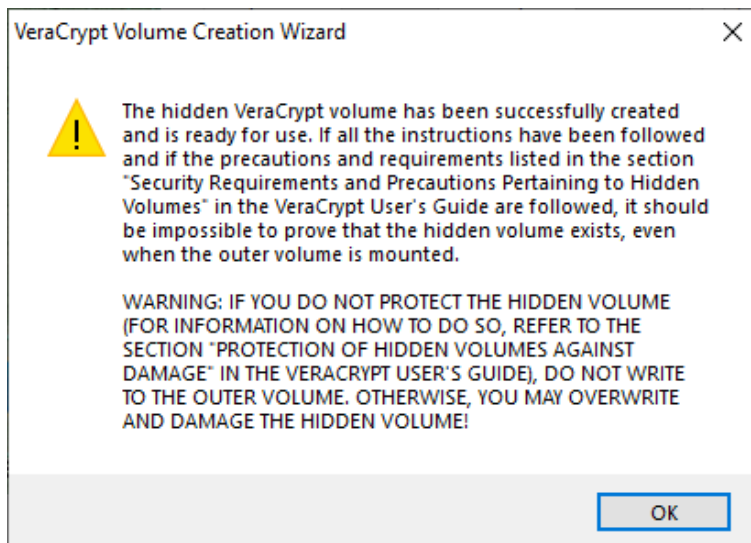
5. If you receive this message, you can click Yes.



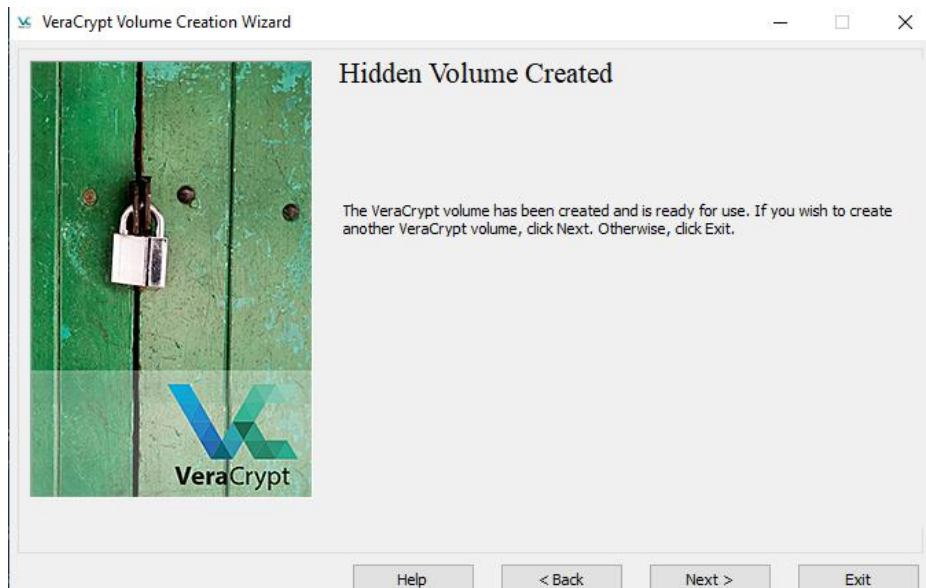
6. Move your mouse around until the gauge is full. Once it is full, click “Format”



7. Click “OK”

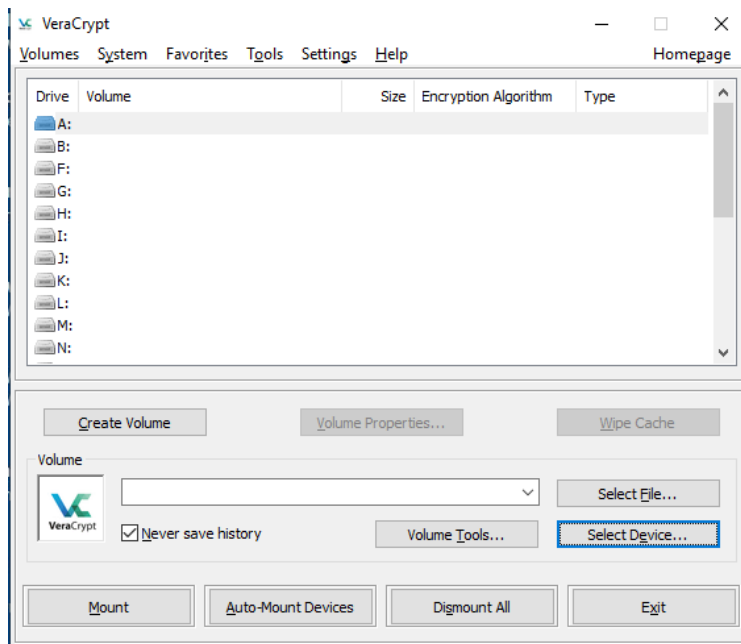


8. Click “OK”

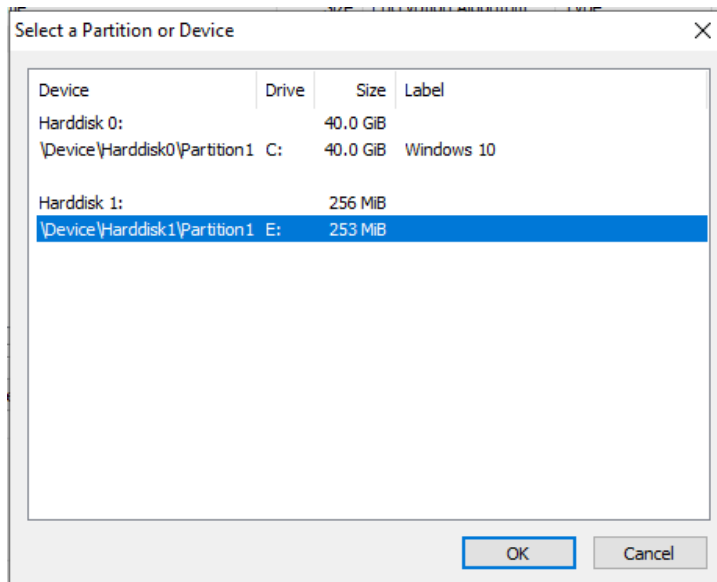


9. Click "Exit"

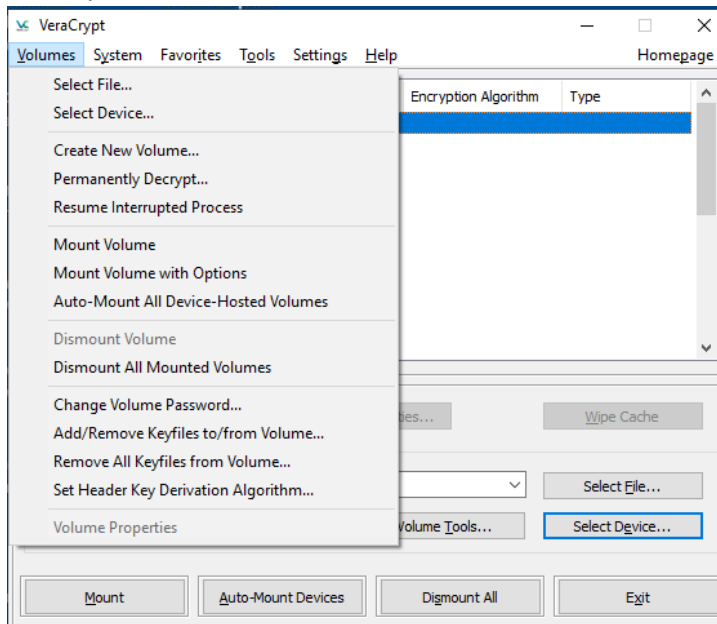
Task 4. Mount the drive.



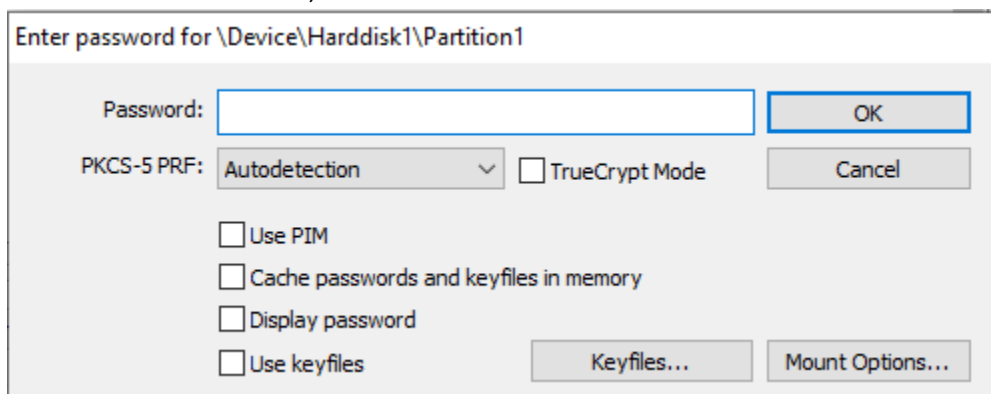
1. Select any drive (in this demonstration, we have selected A:), then click "Select Device..." on the bottom



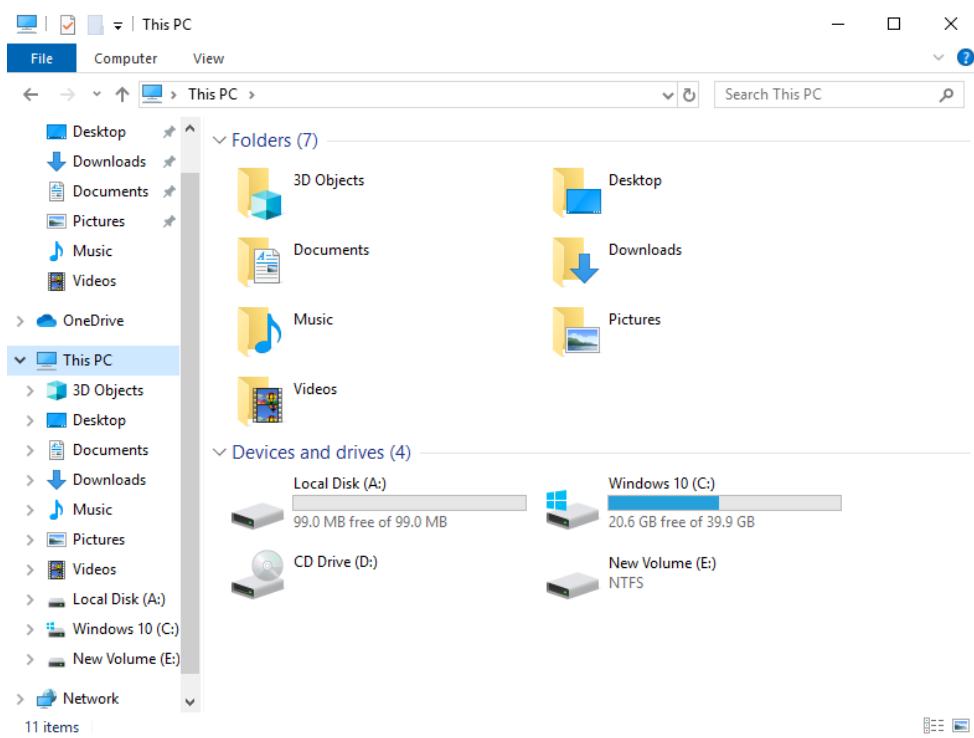
2. Select your USB then click “OK”



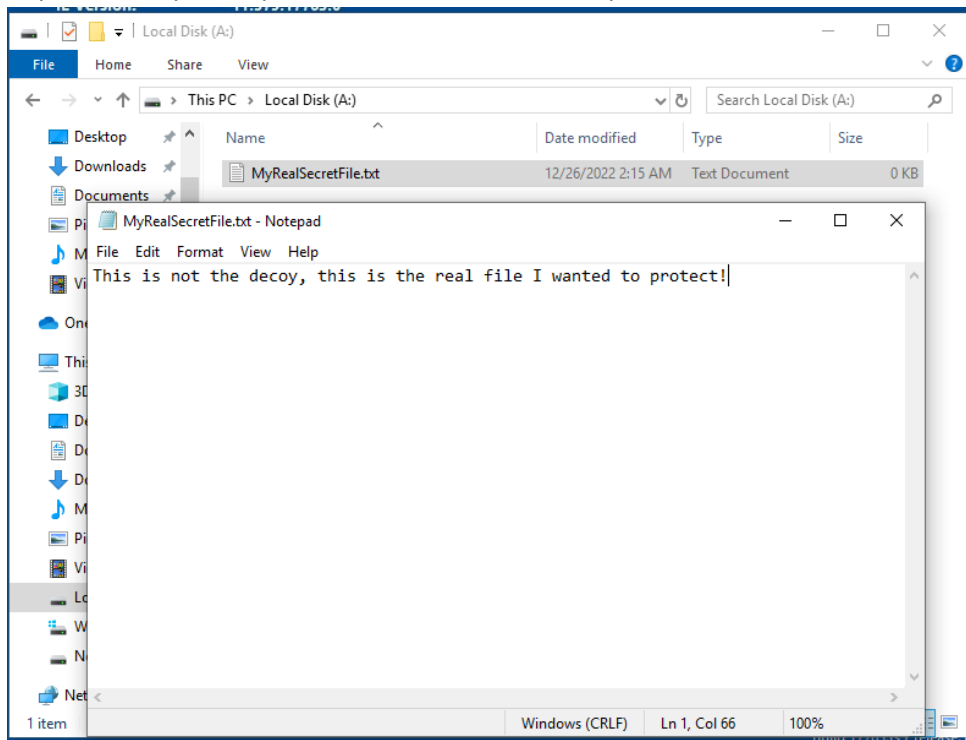
3. Under the “Volumes” tab, click “Mount Volume”



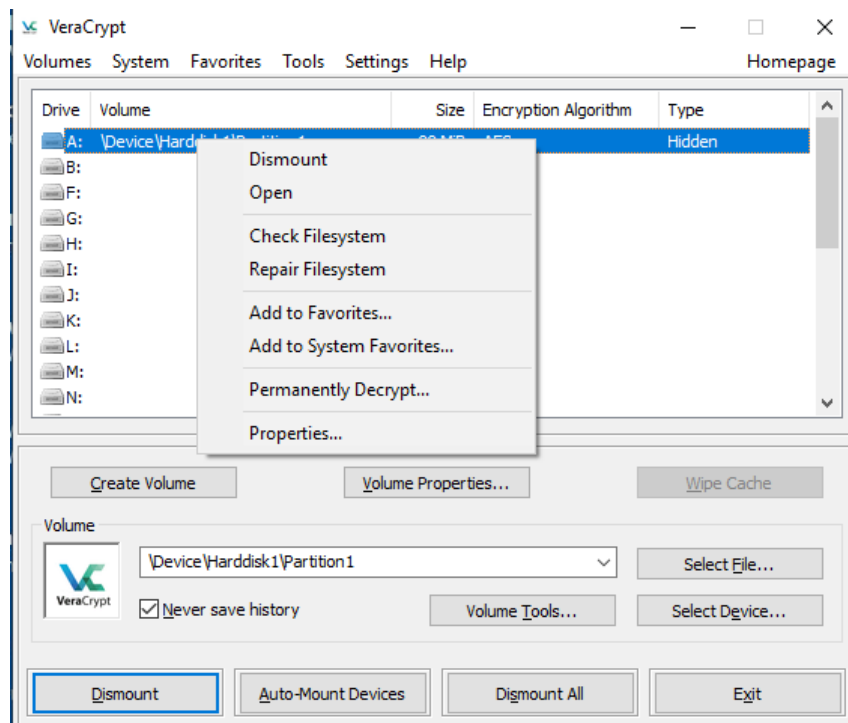
4. Enter your decoy password to mount your hidden decoy drive. Enter your inner password to mount your main hidden drive.



5. In your File Explorer, you should now see the newly mounted drive



6. In your main hidden drive, save any file that is different from your decoy file.



7. To navigate between the two drives, right click the Volume and click “Dismount”. Now you can repeat step 13 to access the other drive.

Questions:

1. In what type of situation would you need to create a hidden volume? How does this relate to plausible deniability?
2. Which volume should decoy files be placed in?
3. List at least 3 tips for creating a good password.
4. If one were to follow all the precautions and requirements listed in the VeraCrypt User's Guide, would it be possible to prove the hidden volume exists?
5. What does cluster bitmap scanning do and what does it ensure?