Worcester Polytechnic Institute
Department of Computer Science

Module 2: VeraCrypt

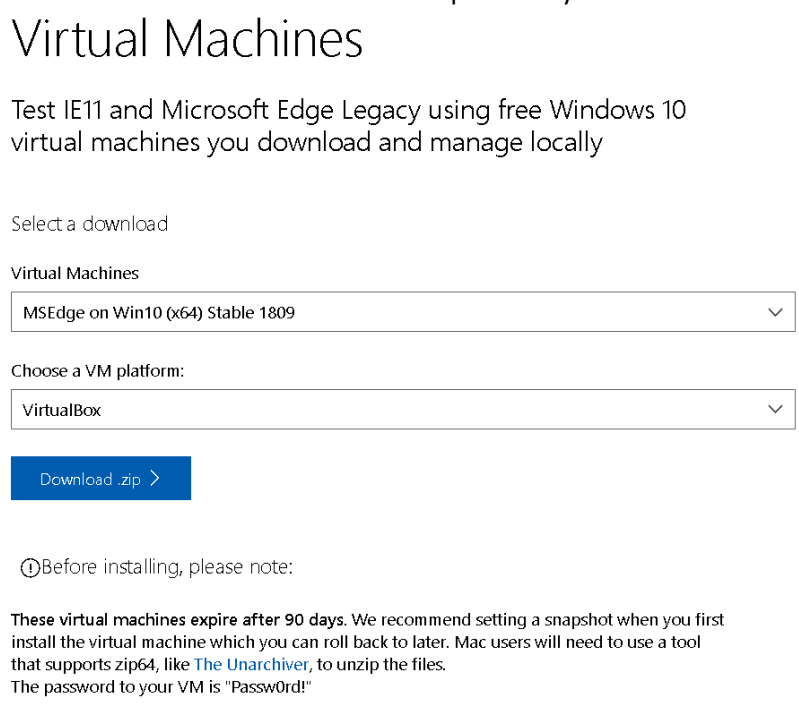
Objectives

- 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.

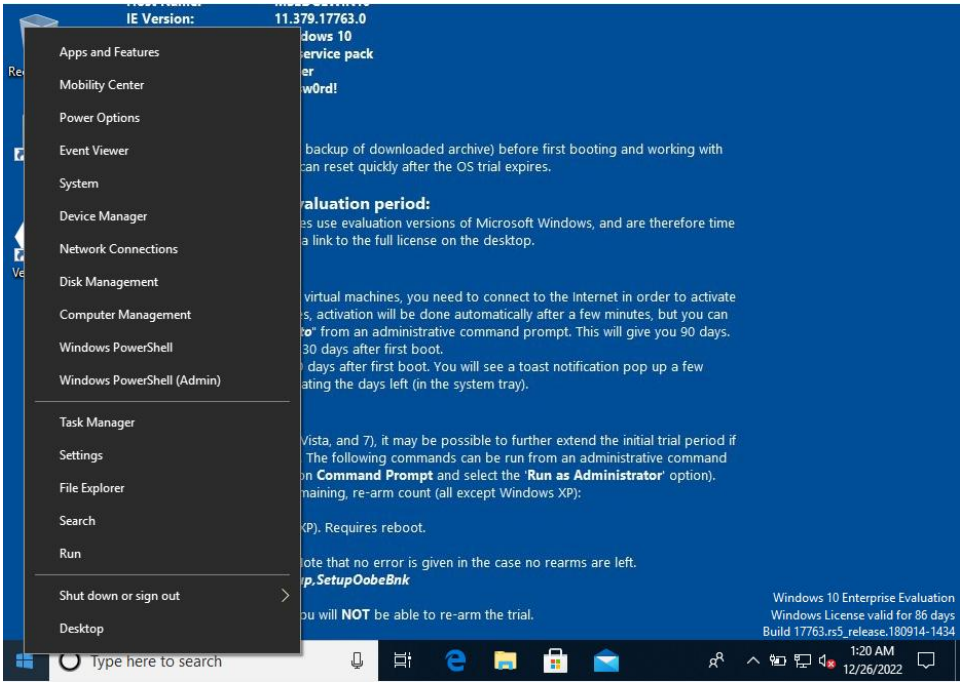


2. Prepare a USB

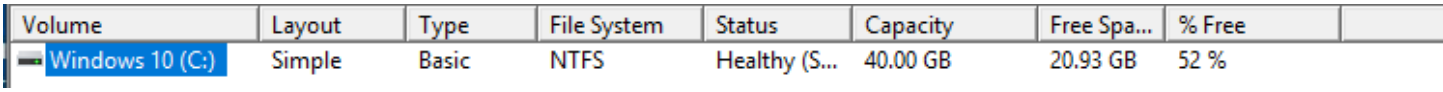
Note: If you are using VirtualBox, you can download GuestAdditions and the extension pack to be able to use a physical USB.

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

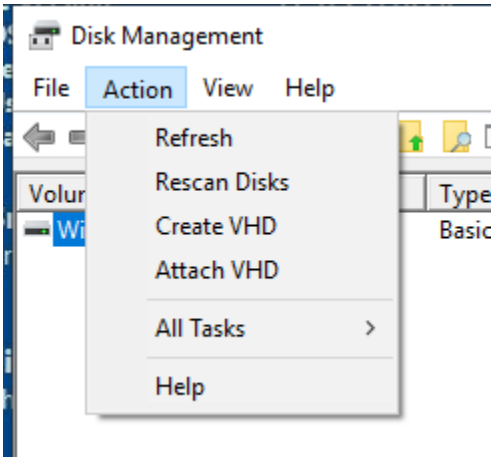
Here is how to create a virtual USB:



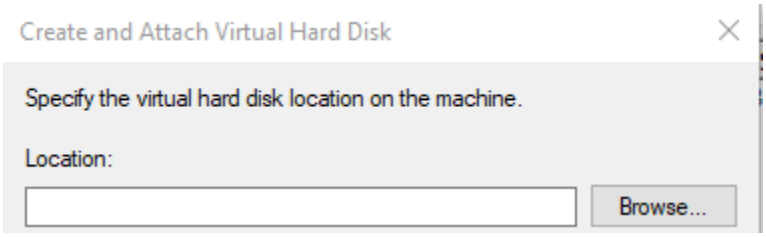
-Right click the windows icon on the bottom left of the screen and click “Disk Management”



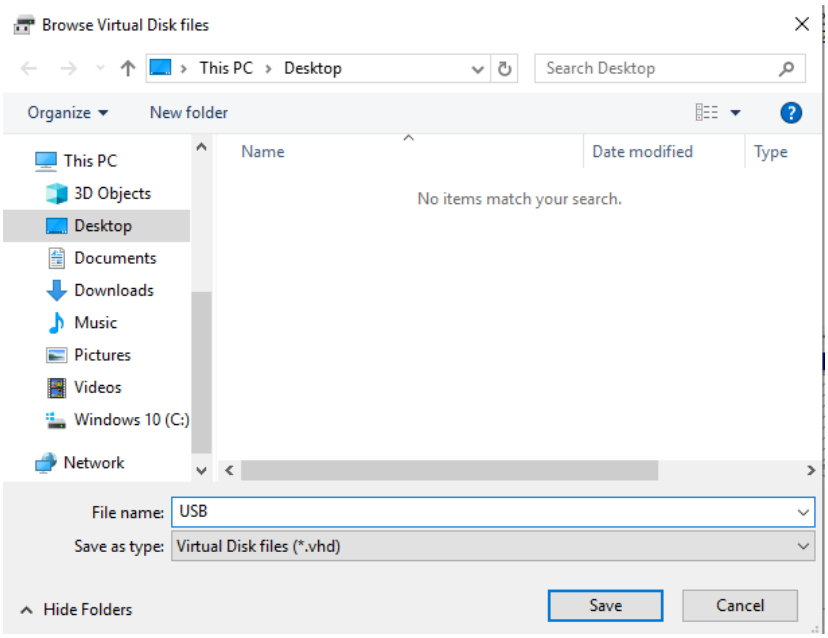
-Make sure your main system is selected



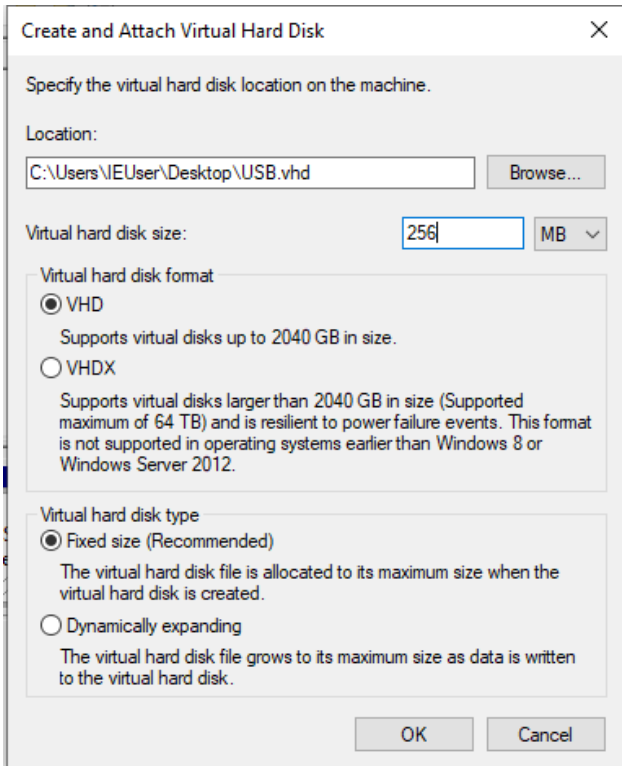
-Click the Action tab and click “Create VHD”



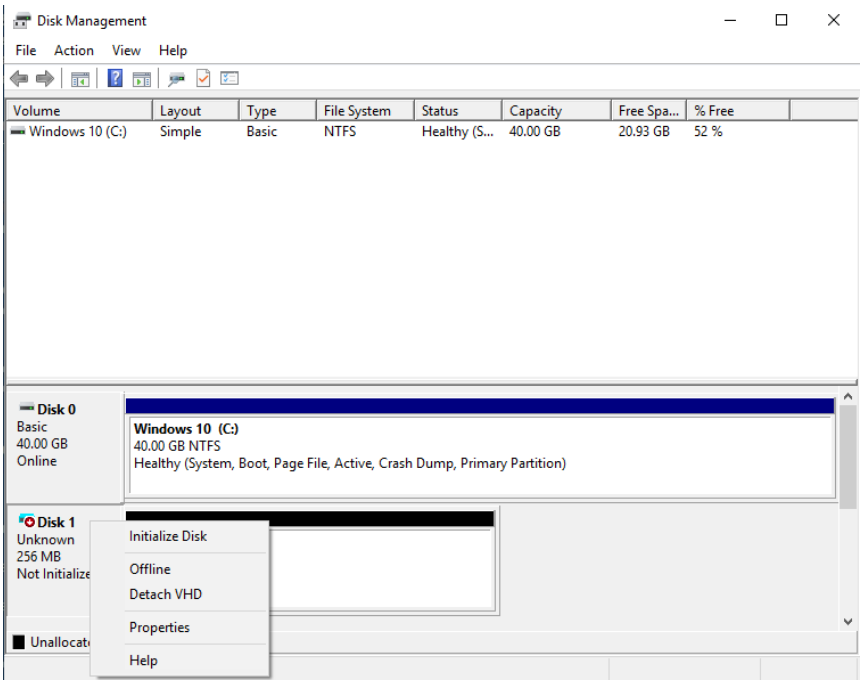
-Click Browse



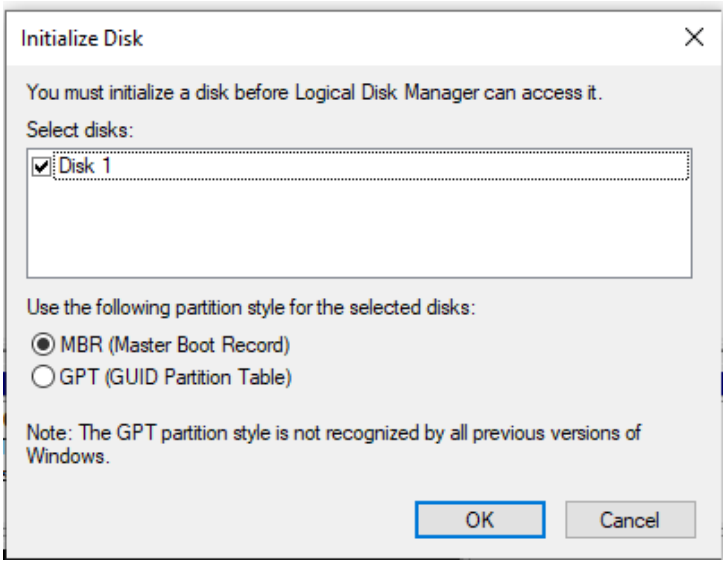
-Navigate to where you would like to save your virtual USB and name your USB. When you are done click "Save"



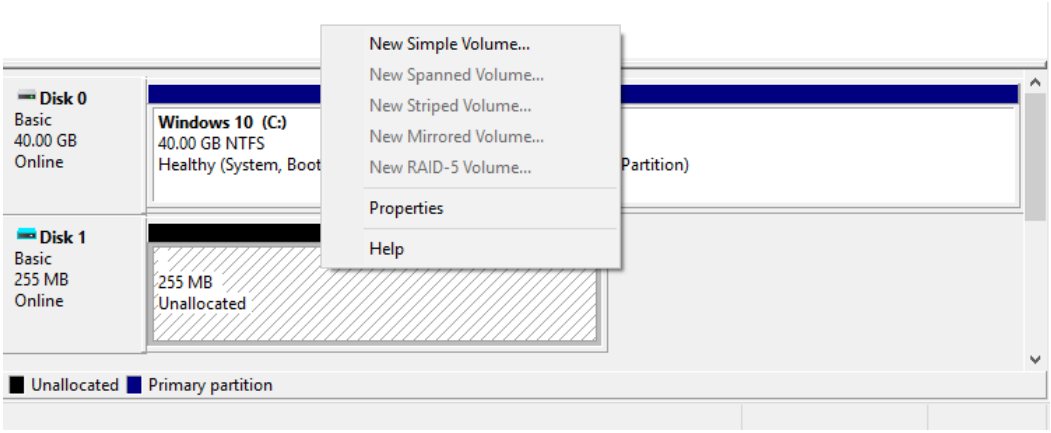
-Type the size you want your virtual hard disk to be and then click "OK" at the very bottom



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

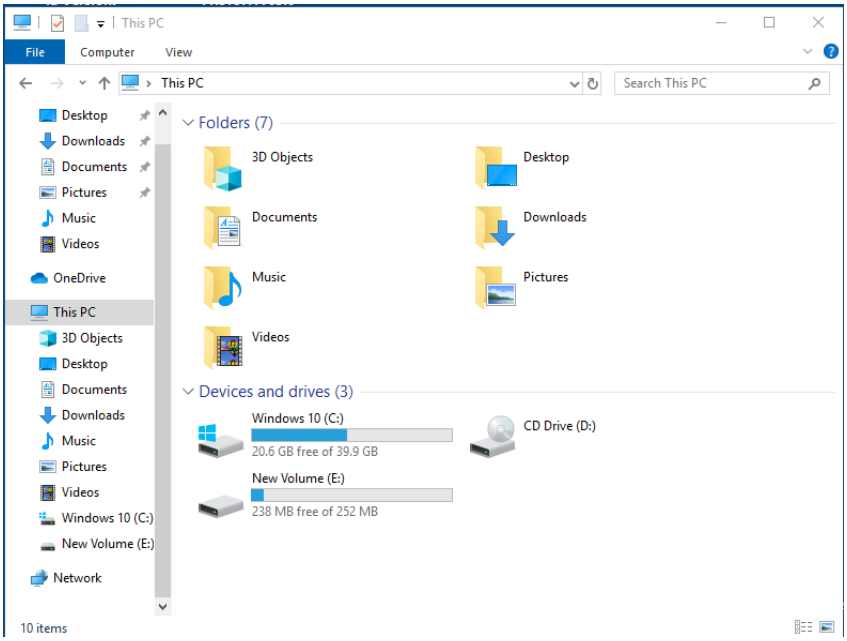


-Click OK



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

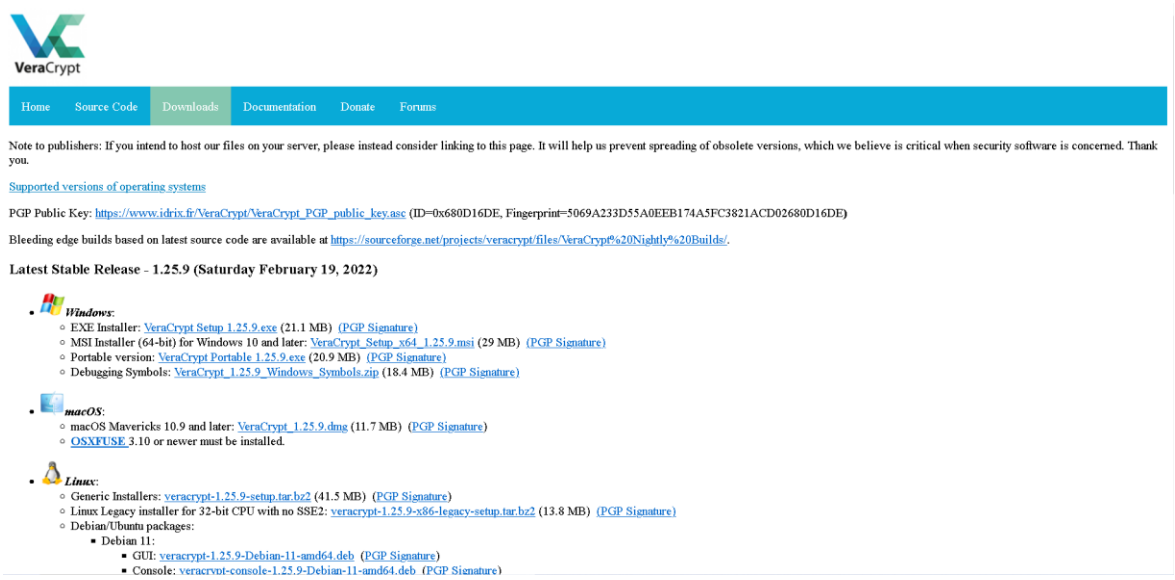
-You do not need to change the default settings, so keep clicking next until you reach the end and Finish.



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

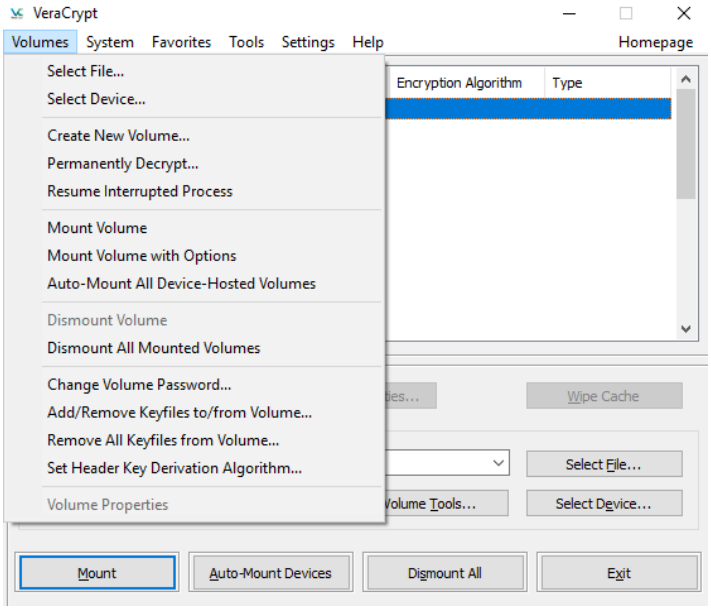
Task 1. Install VeraCrypt

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

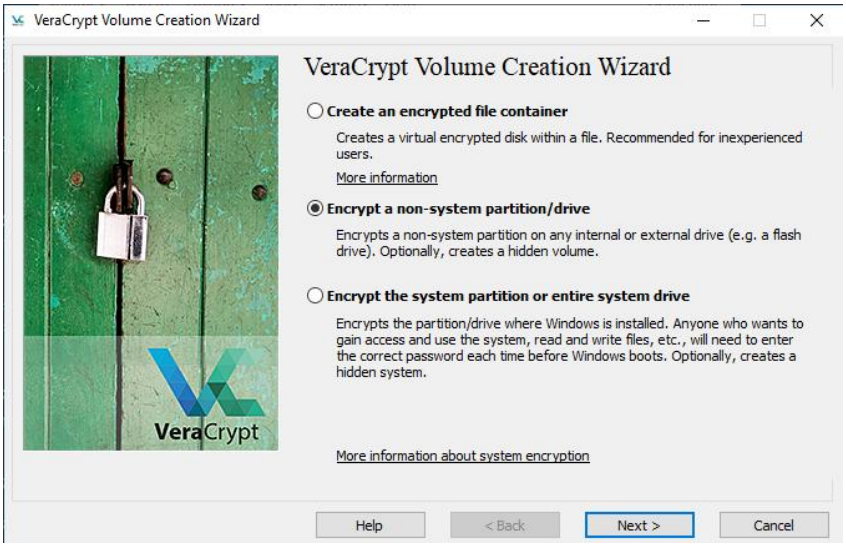


Task 2. Create the hidden drive using VeraCrypt

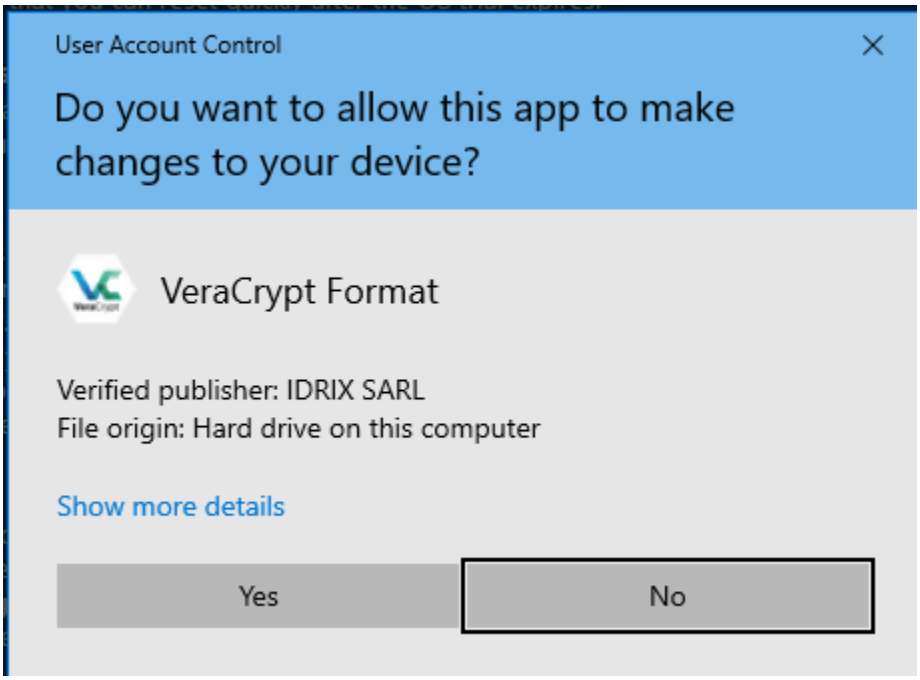
1. Open VeraCrypt



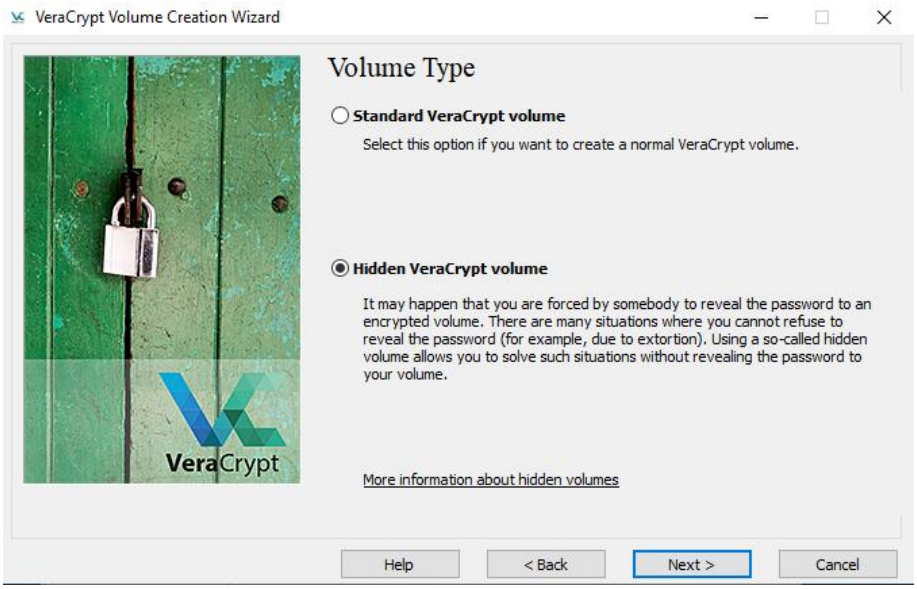
2. Under the “Volumes” tab, click “Create a New Volume”



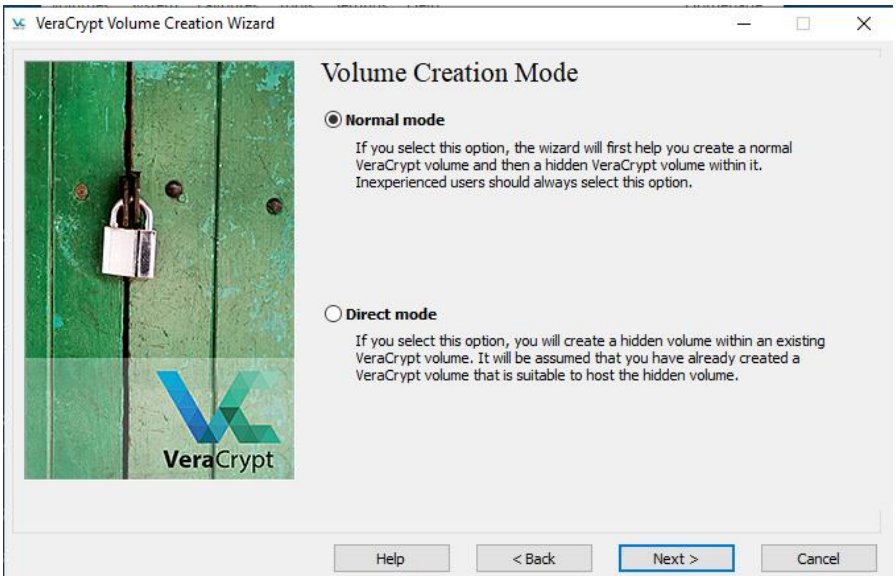
3. Select “Encrypt a non-system partition/drive” and click “Next >”



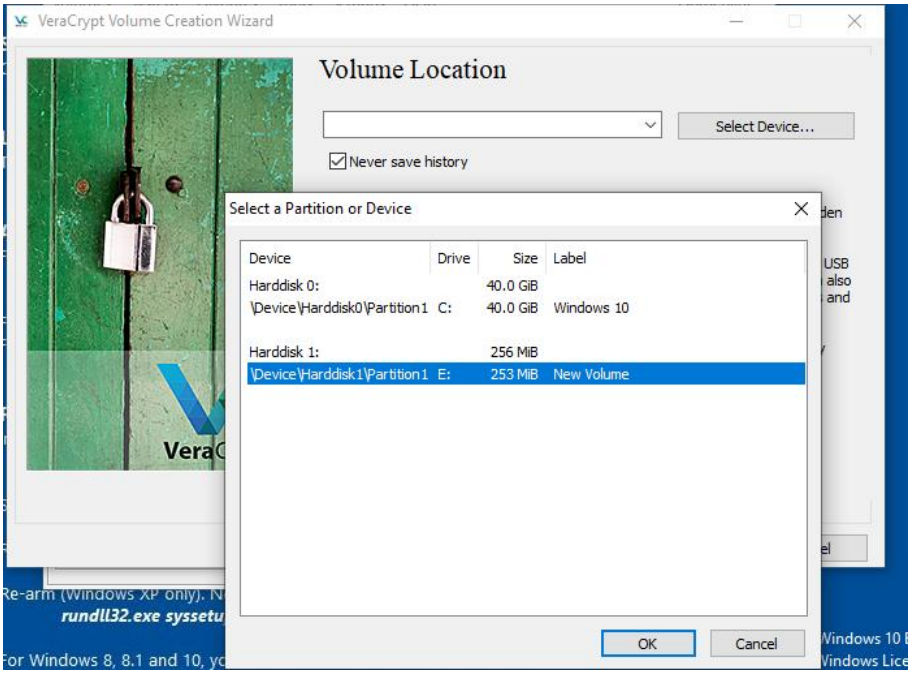
4. If you get this pop-up, click Yes



5. Select “Hidden VeraCrypt volume” and click “Next >”

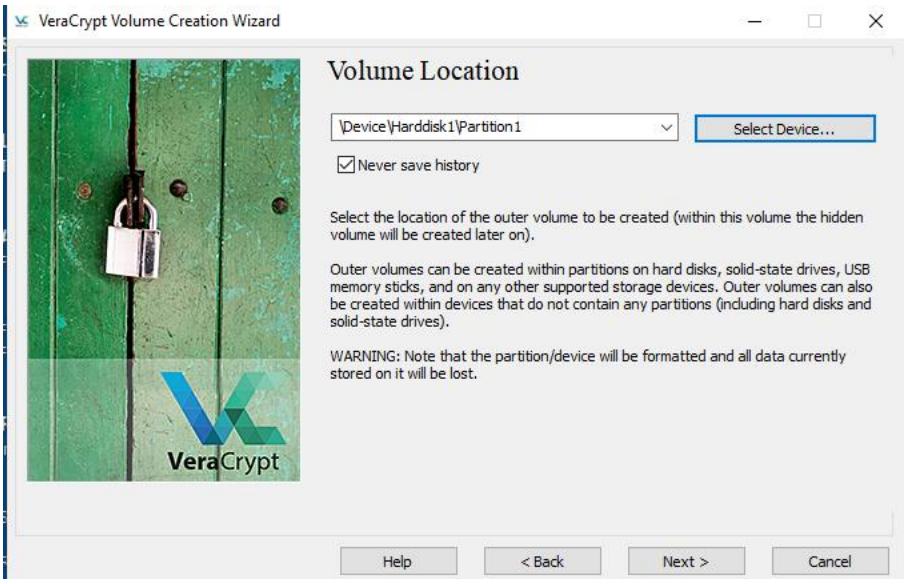


6. Select “Normal mode” and click “Next >”

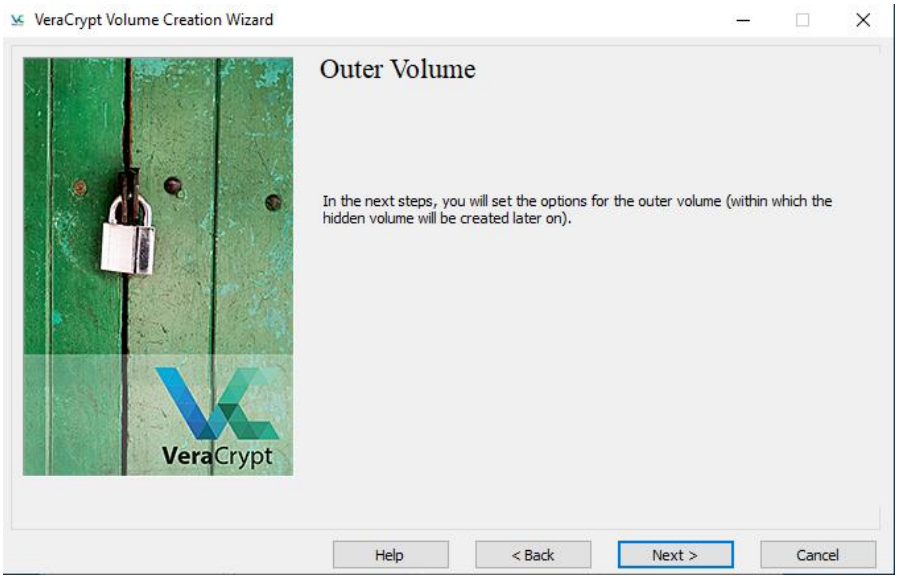


7. Click “Select Device…” and select your USB drive then click “OK”.

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

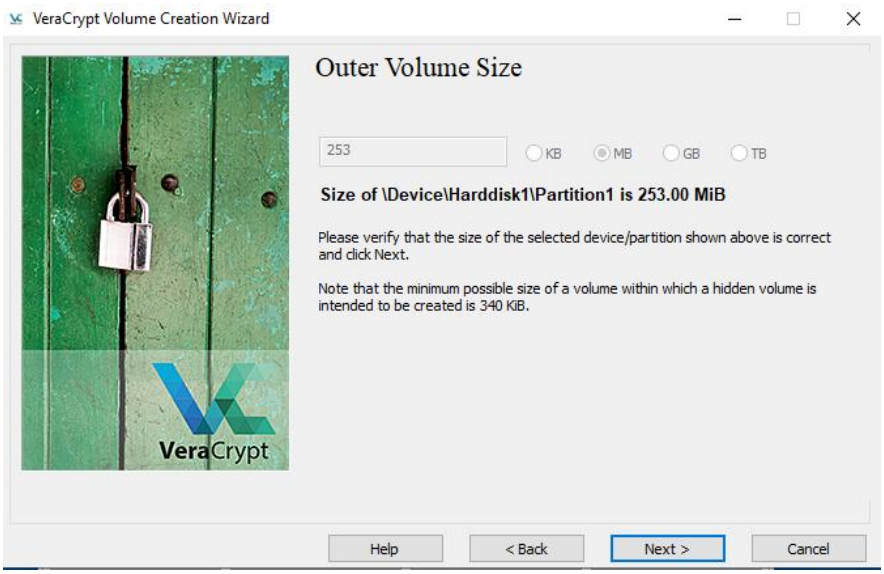


8. Read and make sure you understand the warning, then click “Next >” when you are ready to proceed

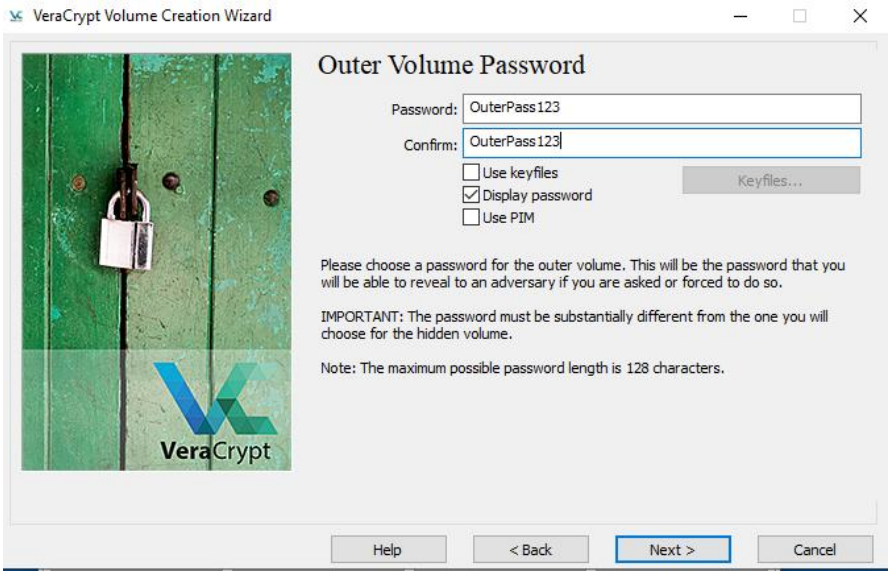


9. Click “Next >”

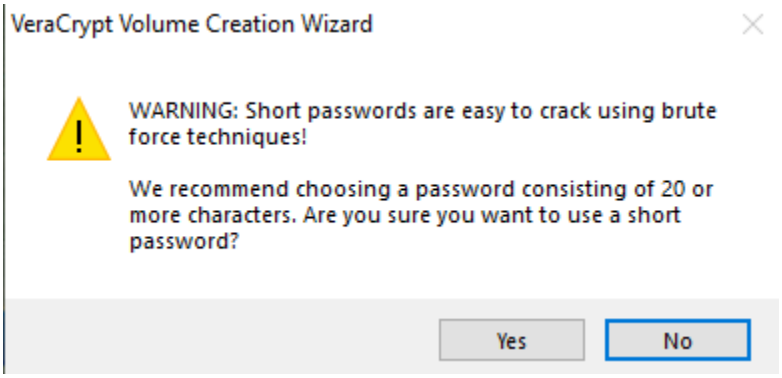
10. You may select whichever algorithms you would like. In this demonstration we are keeping the default settings. Once you have decided, click “Next >”



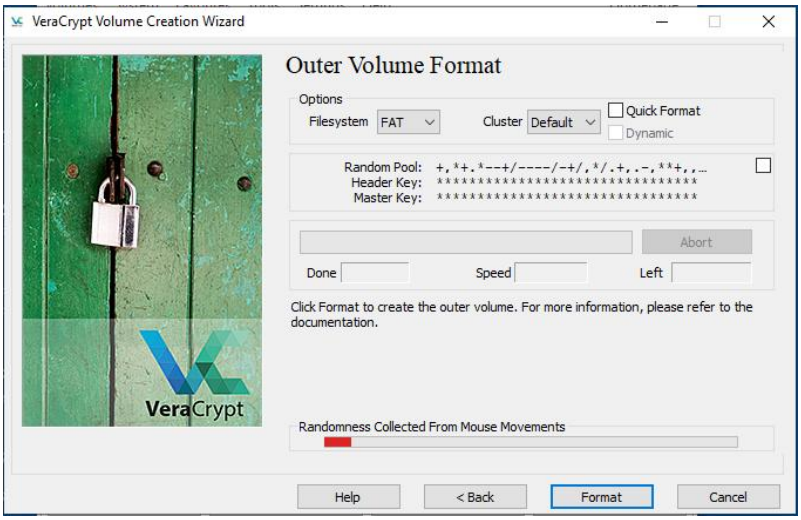
11. Click “Next >”



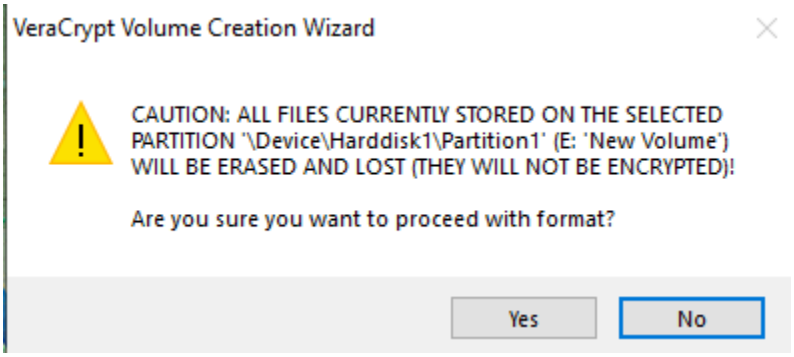
12. Create any decoy password then click “Next >”



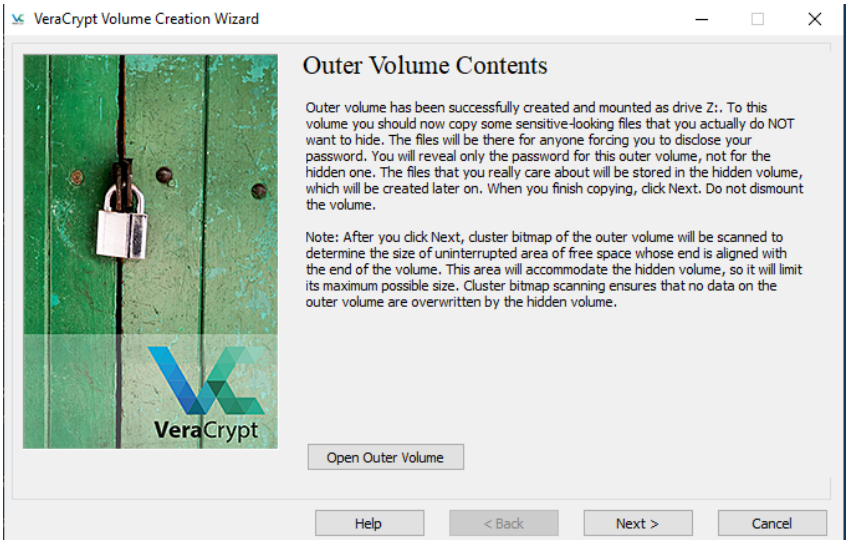
13. If you receive this message, you can click Yes.



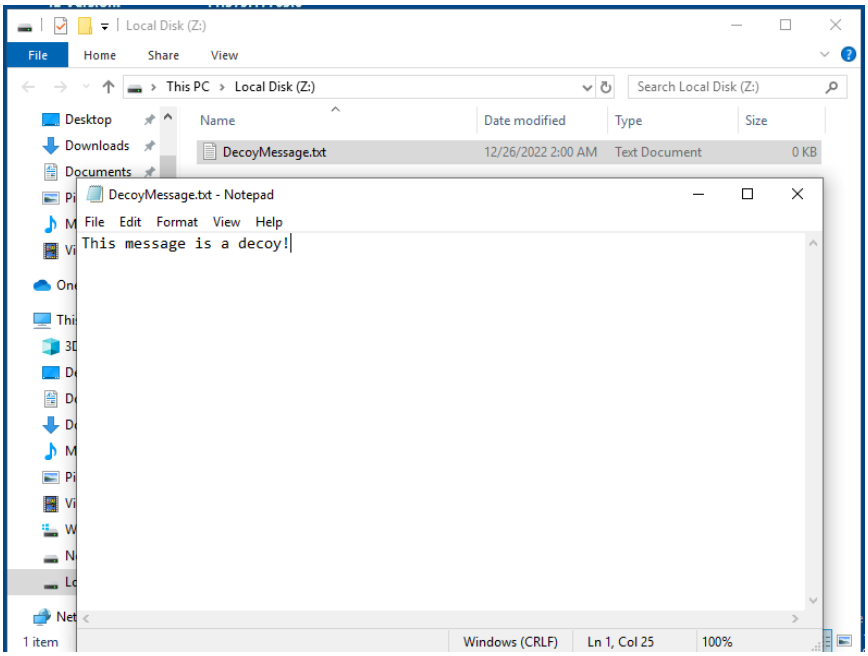
14. Move your mouse around until the gauge is full. Once it is full, click “Format”



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

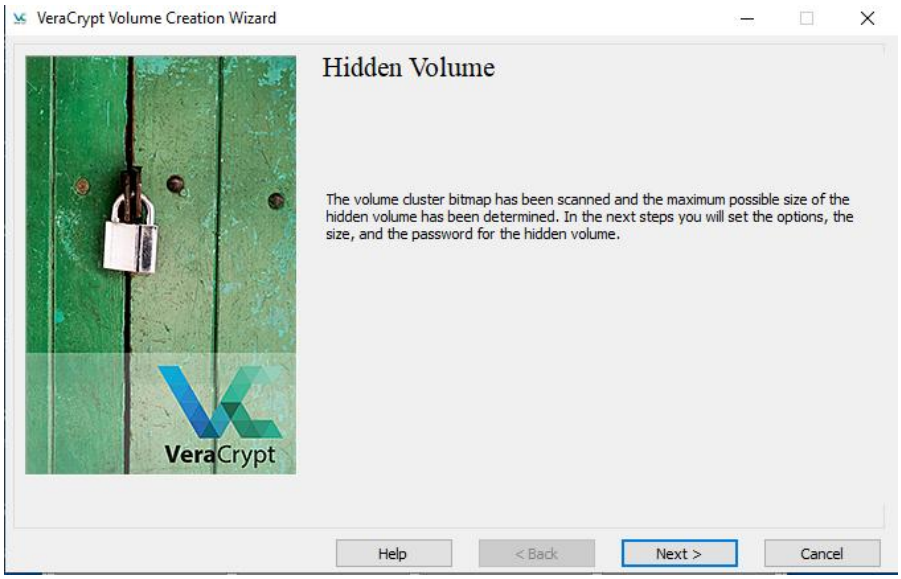


16. Click “Open Outer Volume” to open the hidden storage



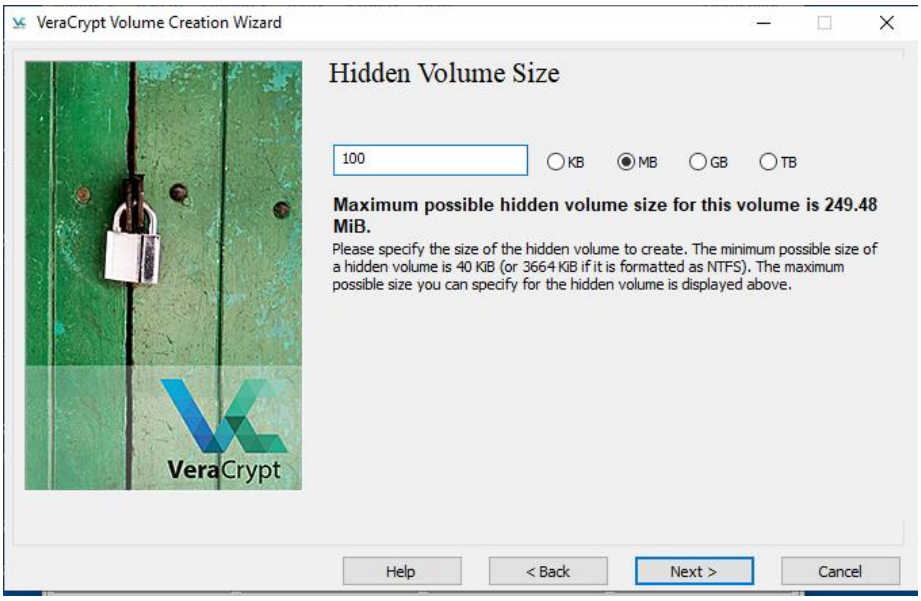
17. Save or create any decoy file. When you are done click “Next >” in VeraCrypt

Task 3. Create the main hidden drive

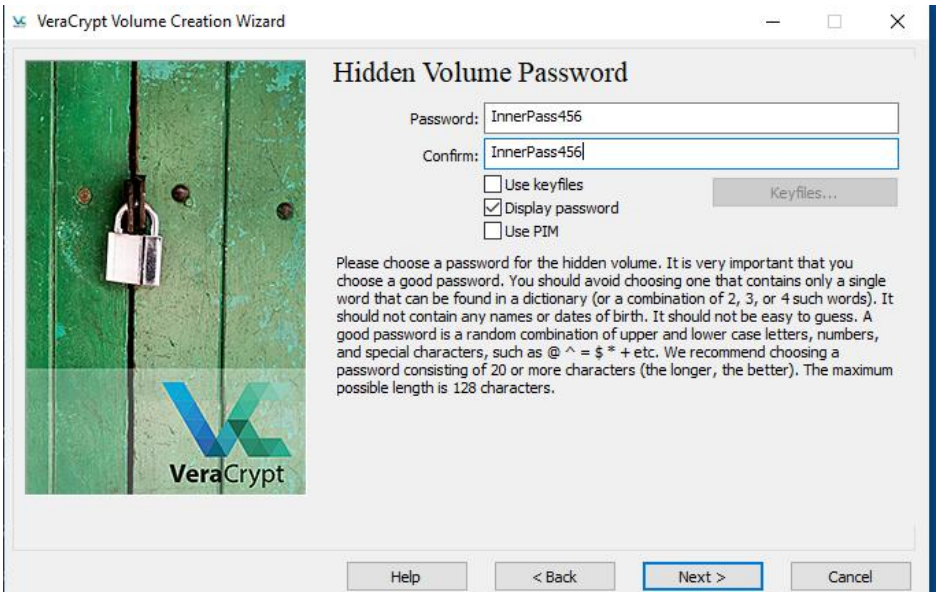


1. Click “Next >”

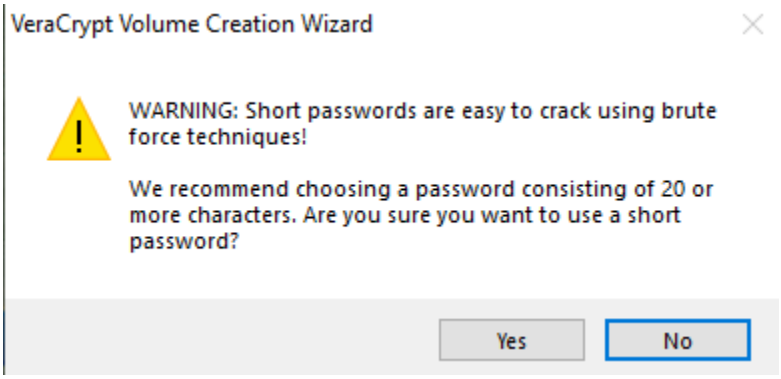
2. Choose the algorithms you would like and click “Next >”



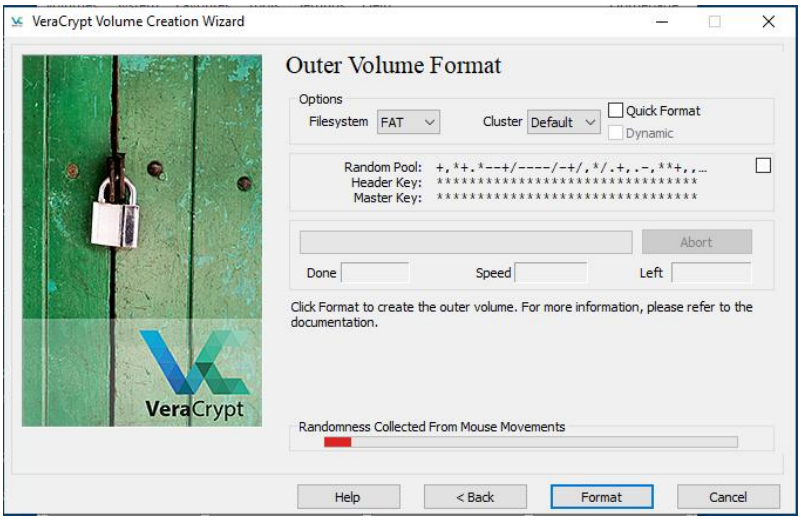
3. Type a number smaller than the maximum possible volume size then click “Next >”



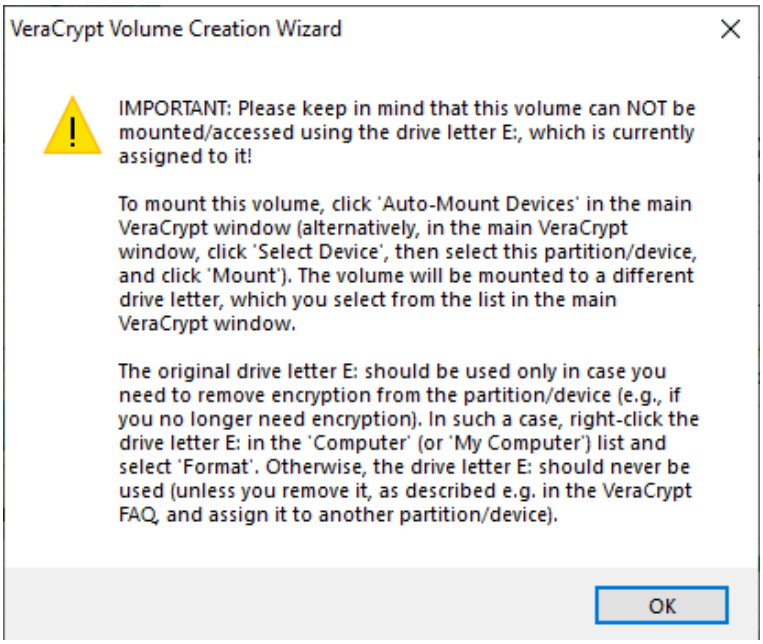
4. Create a secure password, it MUST be different from the decoy password



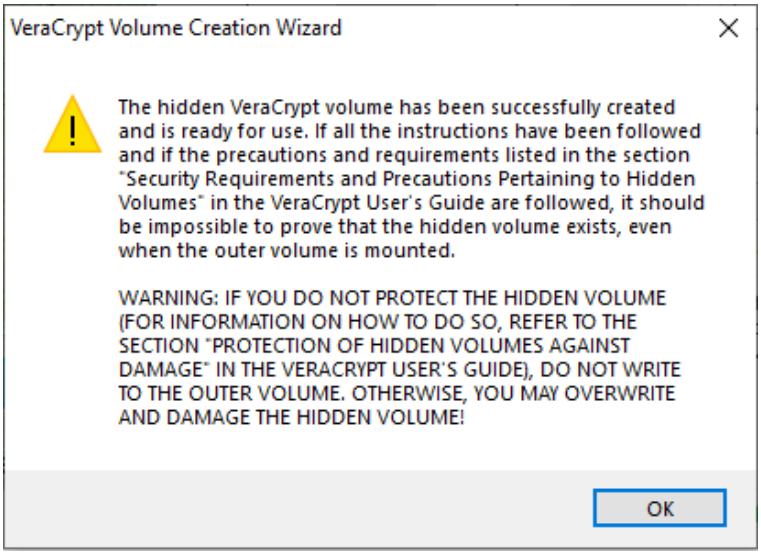
5. If you receive this message, you can click Yes.



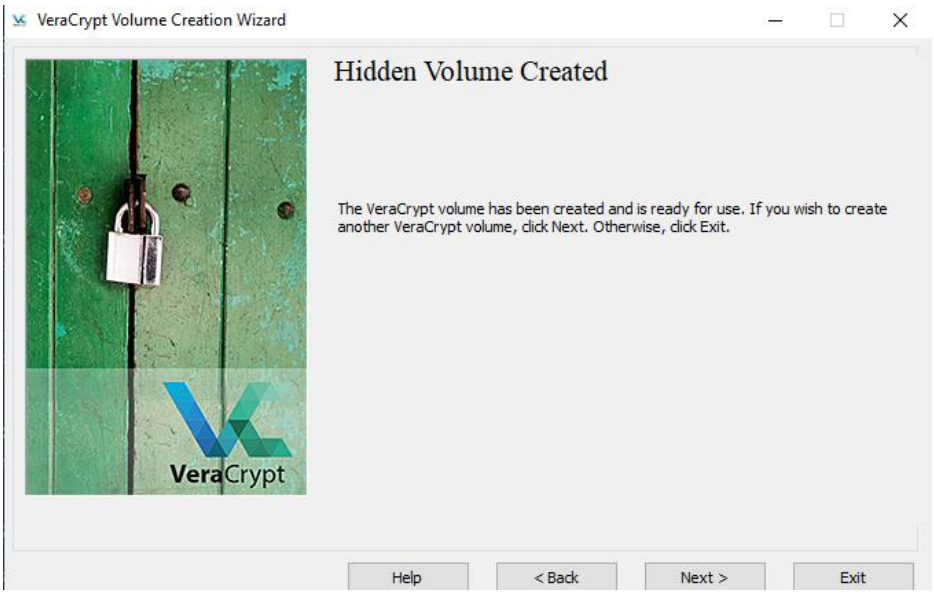
6. Move your mouse around until the gauge is full. Once it is full, click “Format”



7. Click “OK”

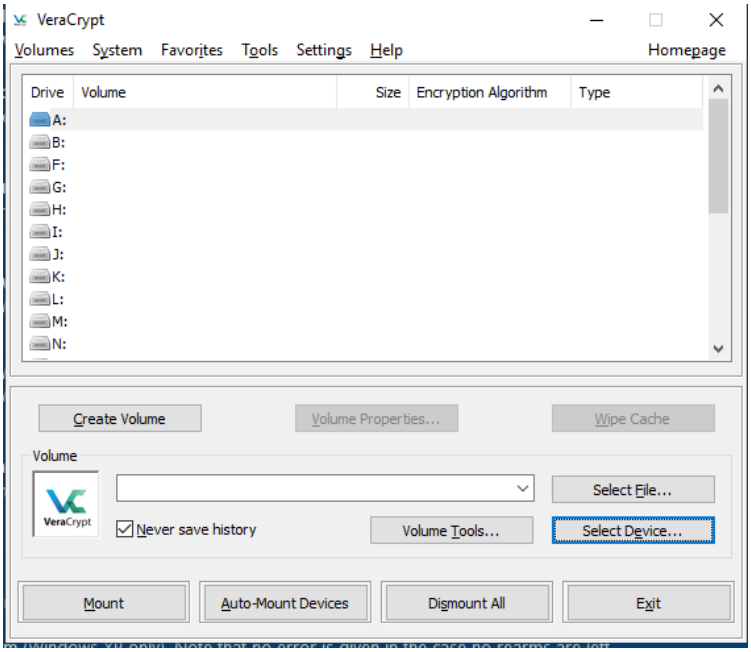


8. Click “OK”

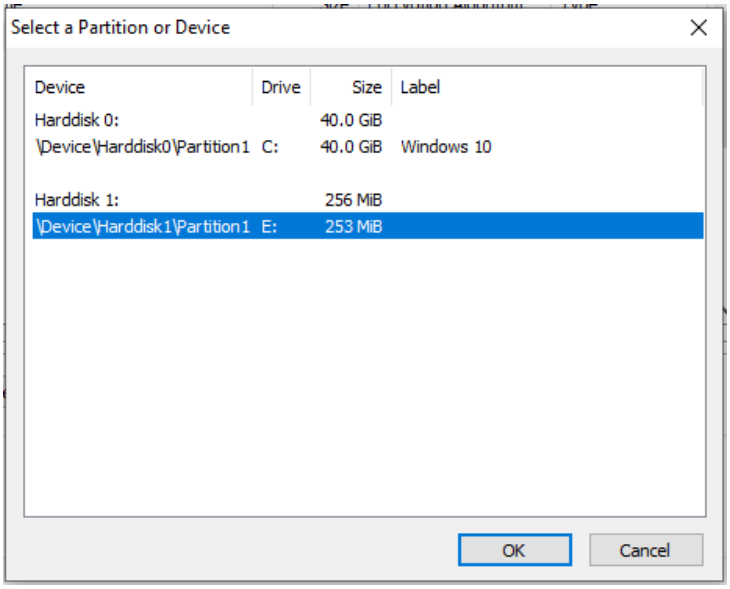


9. Click “Exit”

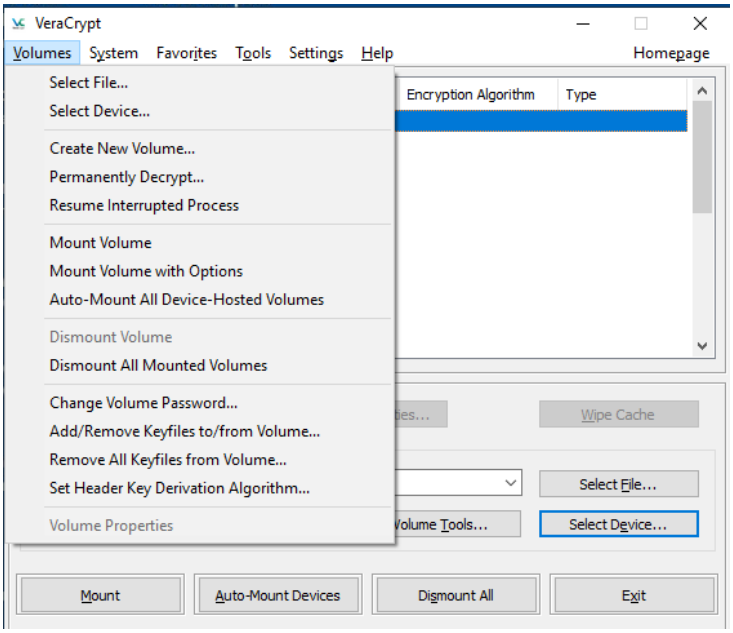
Task 4. Mount the drive.



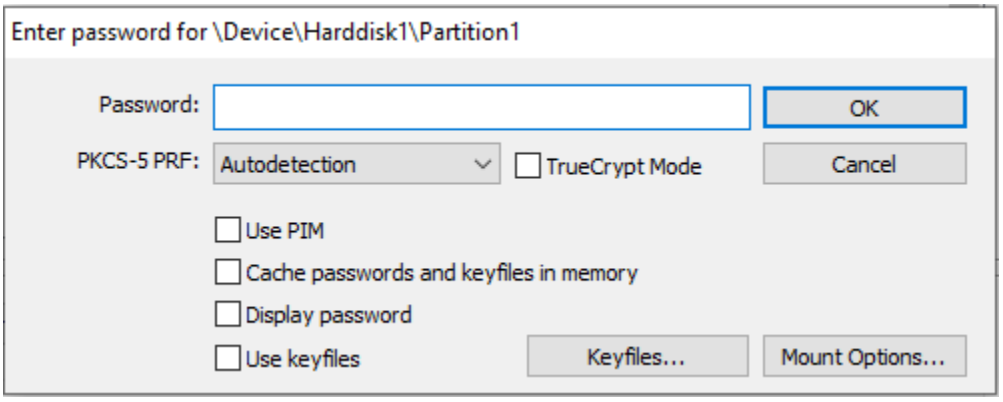
1. Select any drive (in this demonstration, we have selected A:), then click “Select Device…” on the bottom



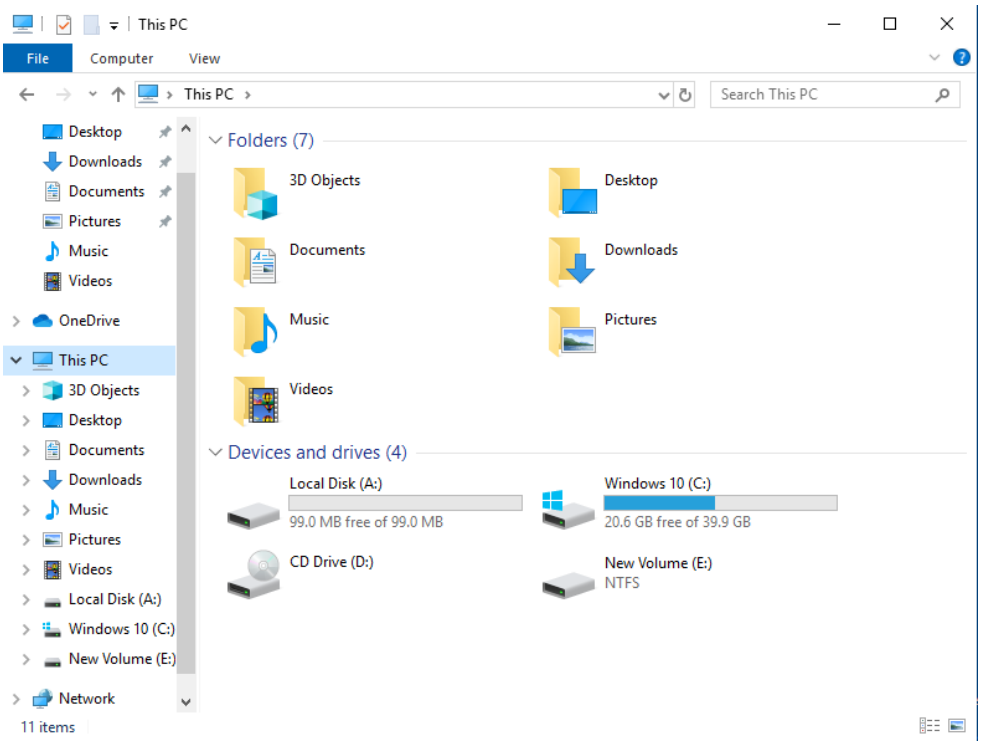
2. Select your USB then click “OK”



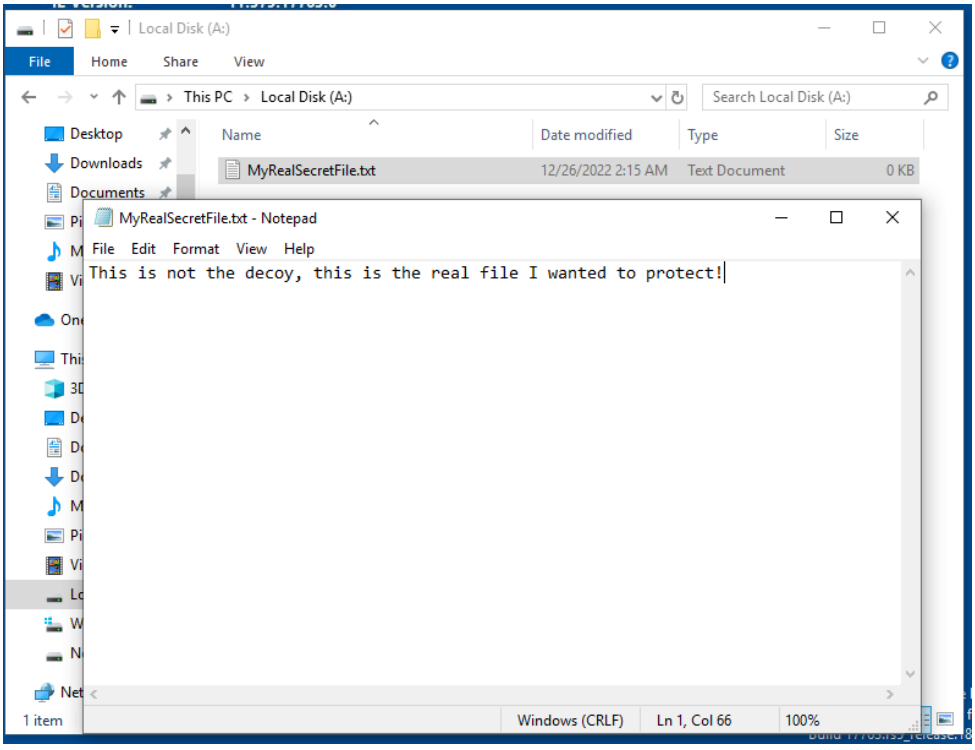
3. Under the “Volumes” tab, click “Mount Volume”



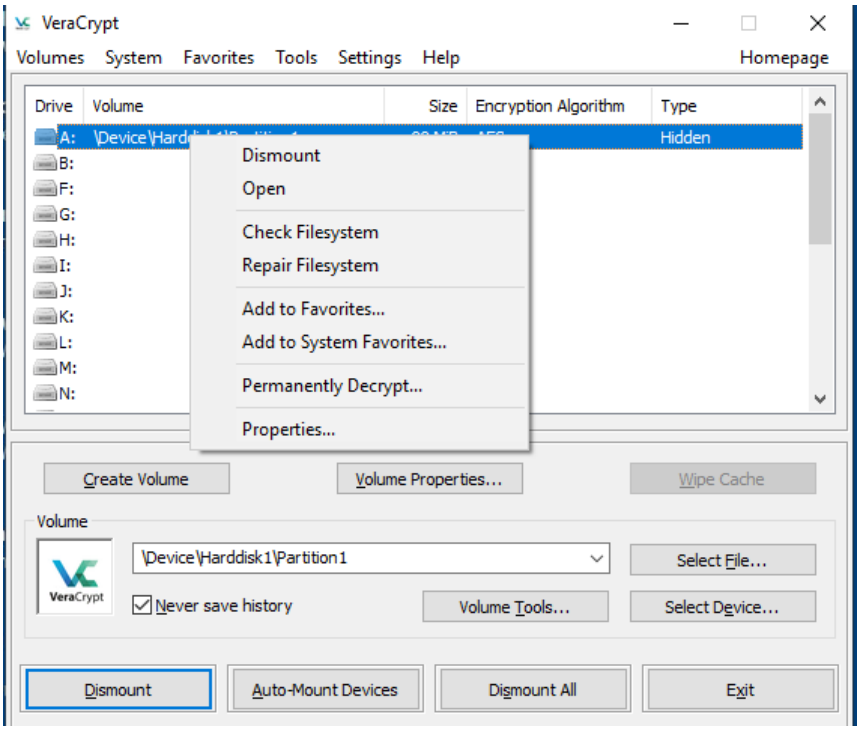
4. Enter your decoy password to mount your hidden decoy drive. Enter your inner password to mount your main hidden drive.



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?