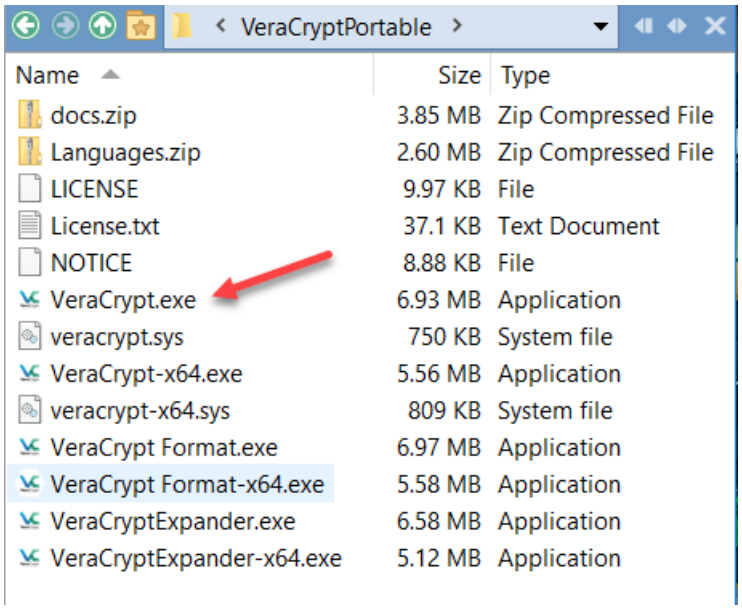
How to Use VeraCrypt to Encrypt your Medical Data

TimeAcct Information Systems
2018/05/28

It is VERY important to encrypt any data you send to TimeAcct Information Systems! We will not accept data that is not encrypted!!

There are two ways of running VeraCrypt. The first is to install it on your PC – the second is to run it without installing it (portable). On the hard drive (or in the email we send you) there is directory named VeraCyptInstaller and another called VeraCryptPortable. In the VeraCryptInstaller directory there is a file for fully installing VeraCrypt – called VeraCryptSetup.exe. It is used to fully install VeraCrypt on your computer. This is useful if you want to encrypt your entire hard drive. However, if you just want to encrypt a few files on a hard drive – you can use the VeraCrypt.exe application in the VeraCryptPortable directory.

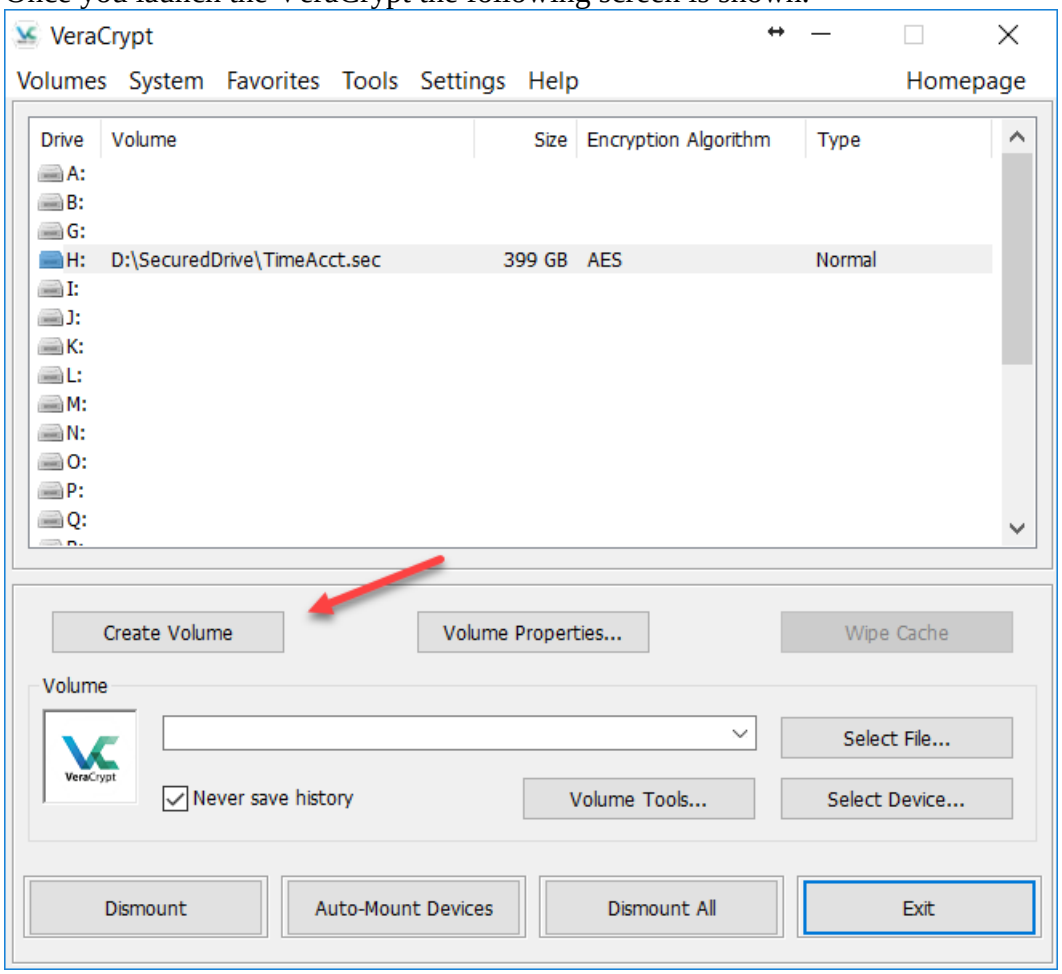


This is what we will do to ship your medical data to TimeAcct Information Systems for the extraction/conversion process.

We will use this program to create an Encrypted container file that we will then 'mount' as another drive letter. Anything you then copy to that drive letter will be automatically encrypted.

Starting True Crypt

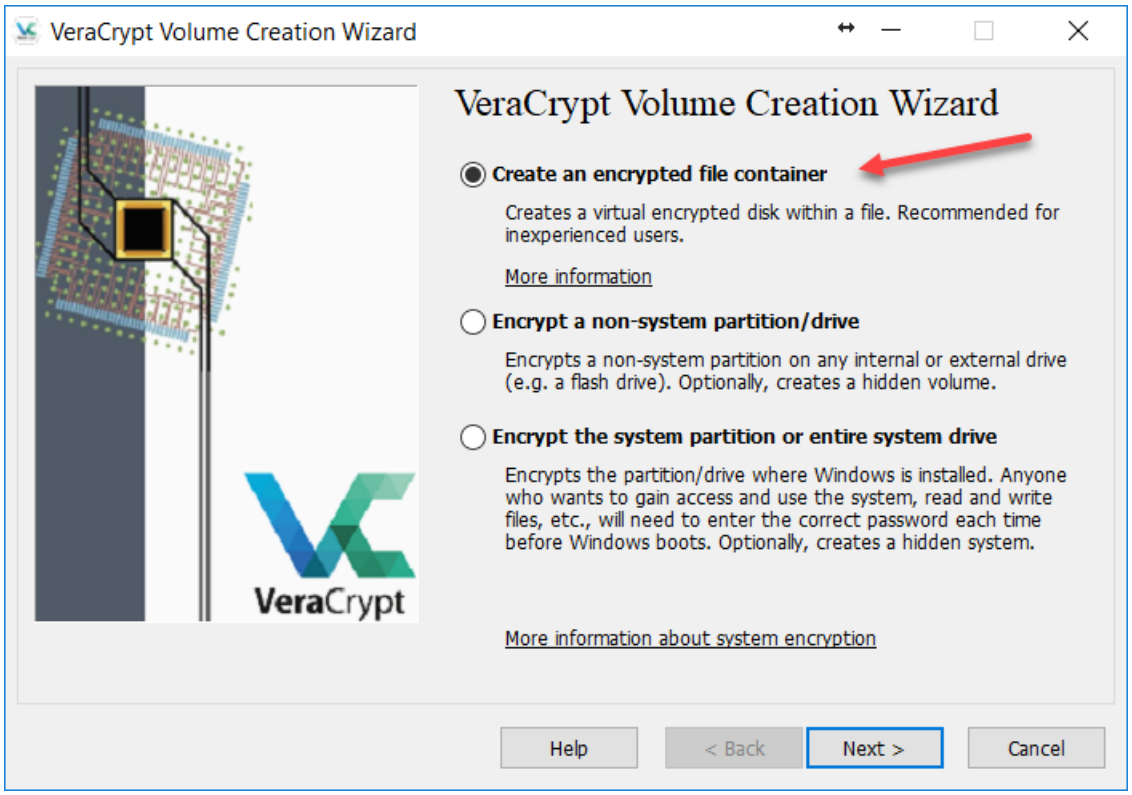
Once you launch the VeraCrypt the following screen is shown.



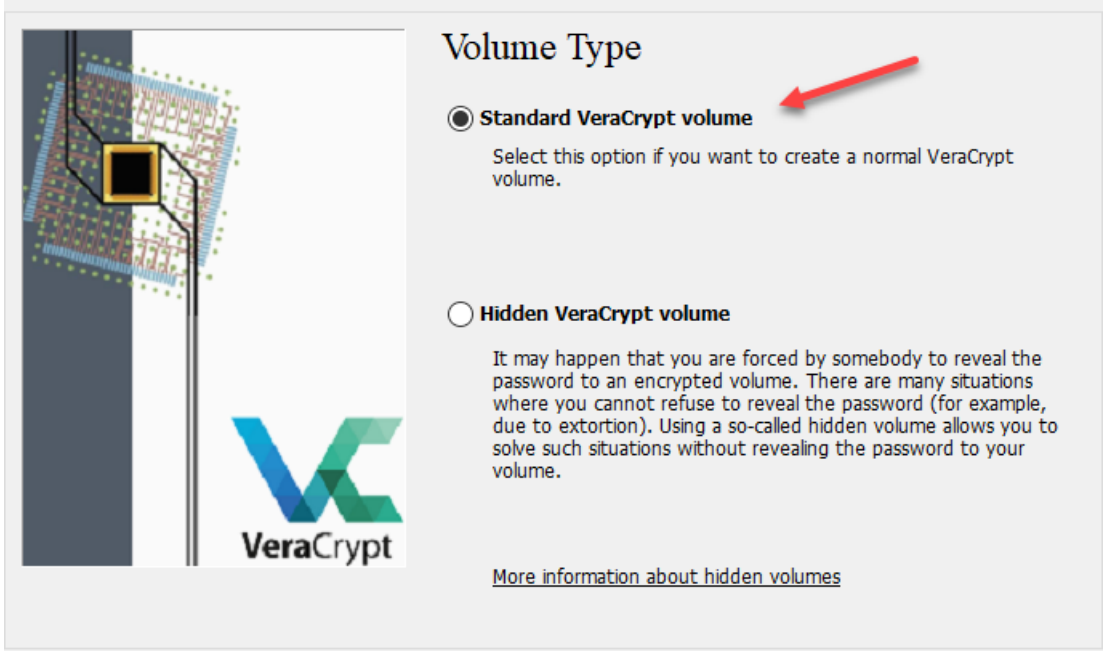
From here we will create an encrypted file container – and then ‘mount’ it to a drive letter.

Creating an Encrypted Volume (Container File)

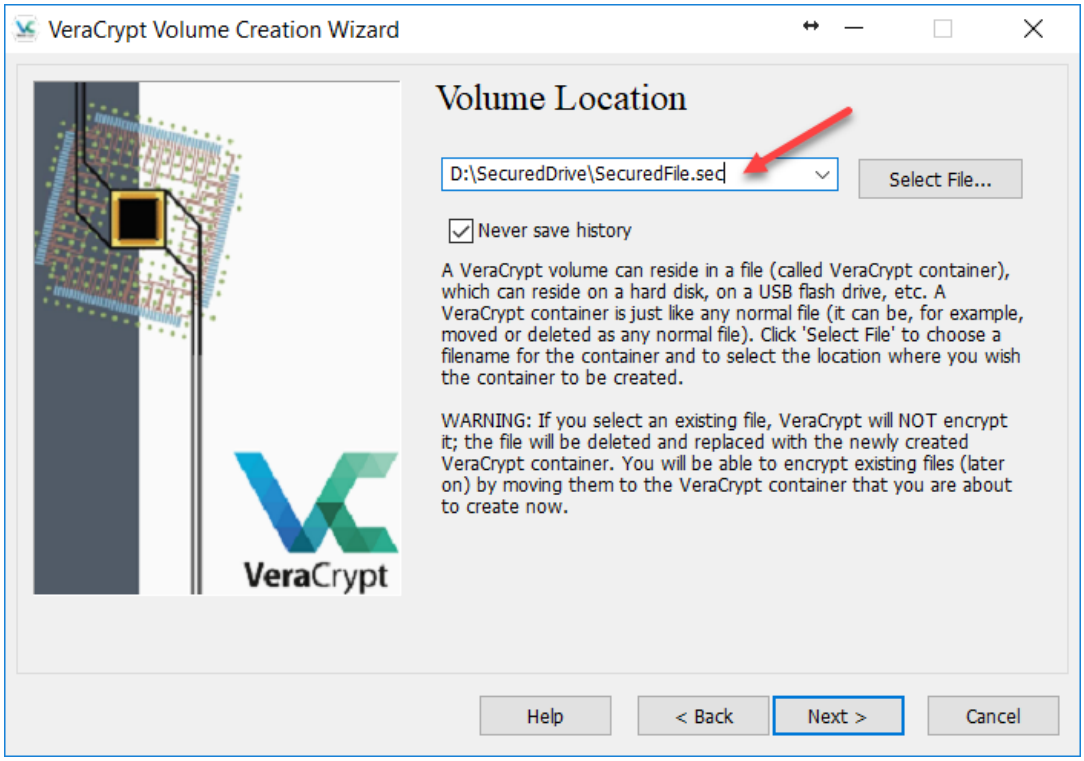
To create the volume – click on the "Create Volume" button. This will present the following screen – where you should select "Create an Encrypted File Container" button. Then Click the Next button.



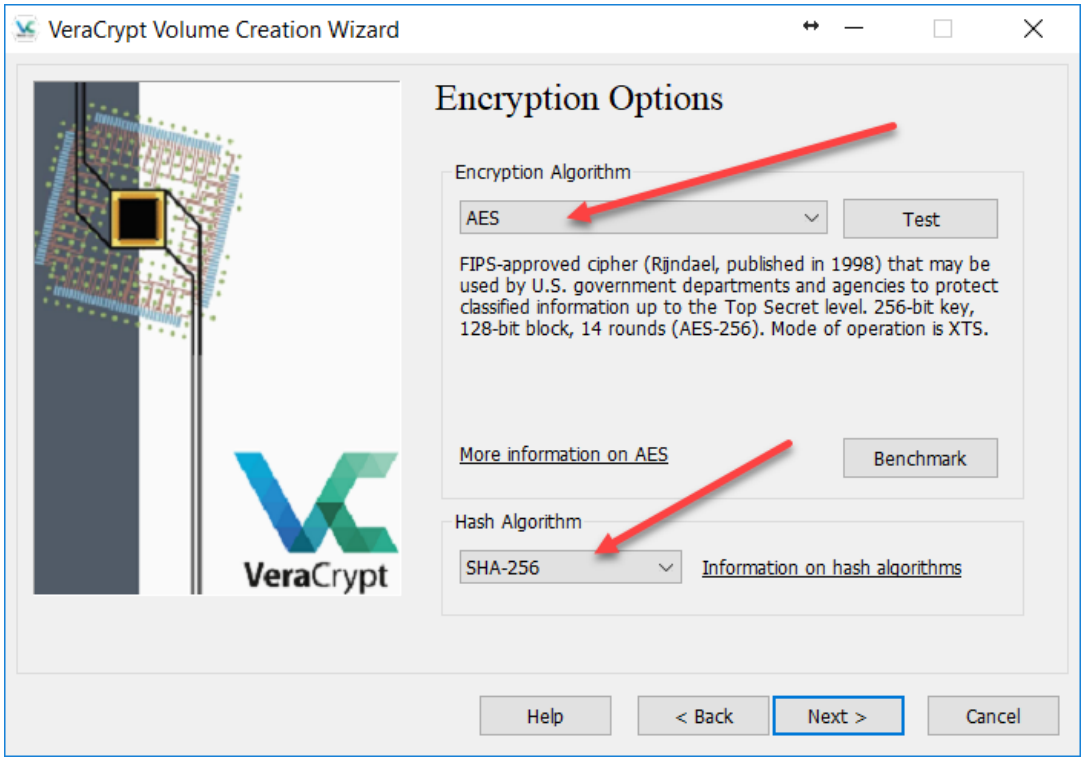
On this screen – you need to select the "Standard VeraCrypt Volume" radio button. Click the Next button.



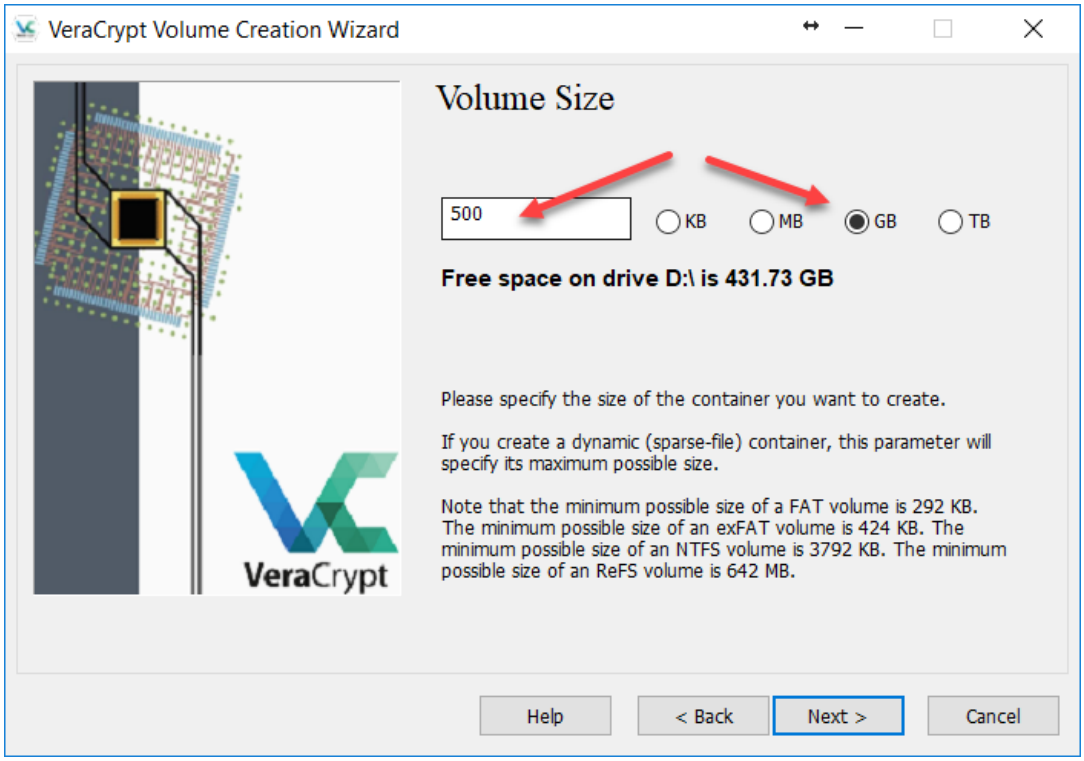
On the next screen – you enter the file you want to create. This file should be stored on the hard drive you want to copy the data to. You can call it anything you like – but a descriptive file name is best. That way in the future you will know what it is. Unlike other files – this will not have any relation to VeraCrypt – so that if the file is not well named you will not know what it is for.
We suggest using something like your clinic name and date – with a .Sec extension. So the name might be like
Medicenters20100121.sec



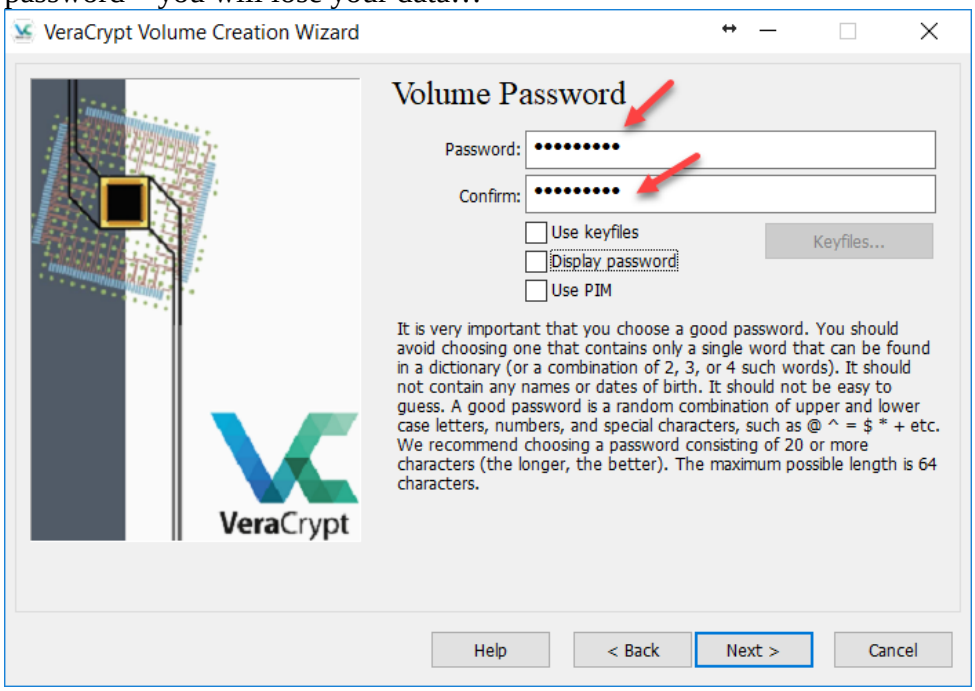
On the next screen you need to choose the encryption options. Here we want to make sure that Encryption Algorithm is set to AES – and the Hash Algorithm is set to SHA-512 or SHA-256. This is what is used by the NSA.



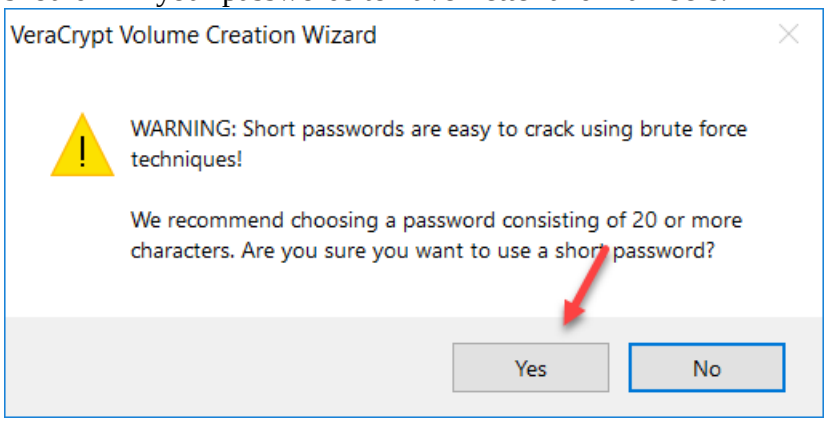
On the next screen – you set the Size of the encrypted area. Here you should set it large enough to hold three times the size of the data you are sending to TimeAcct Information Systems – and then add a little bit. A safe bet is to just set it to 500GB – as shown in the image. Basically at the end of the conversion process – the drive will have to contain the original data, the extracted data and possibly an export (i.e. COPD or CDS).



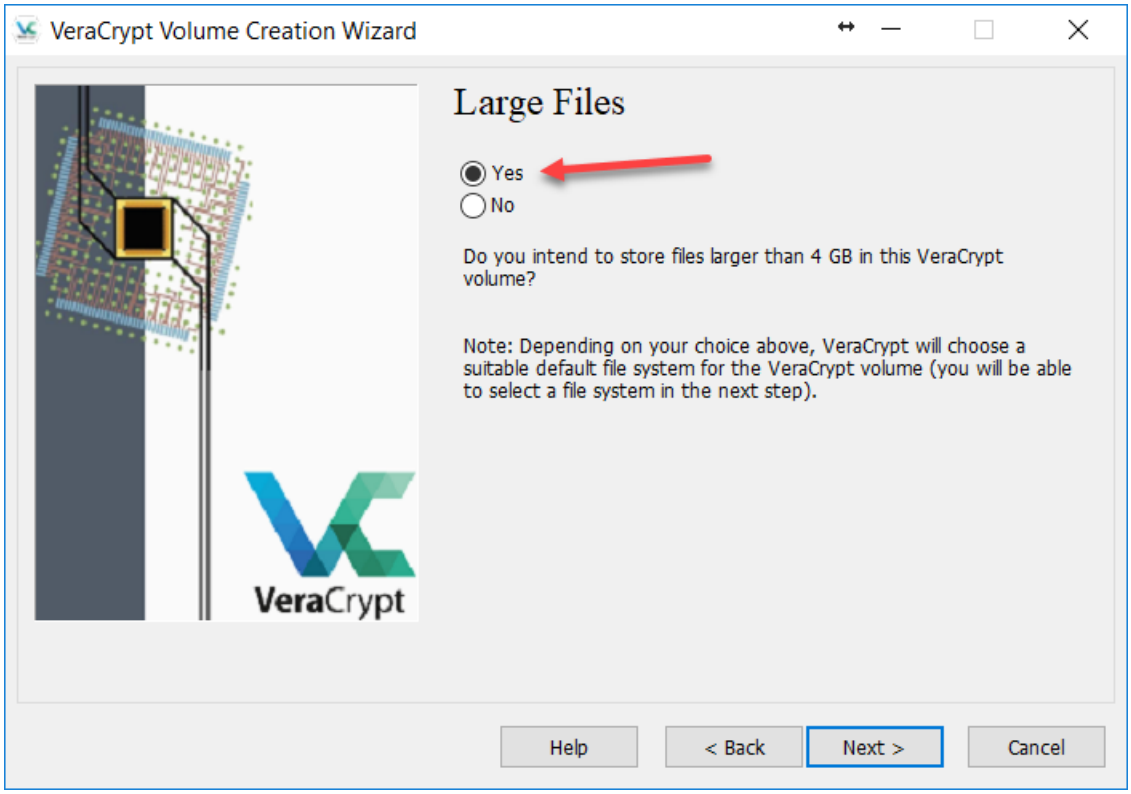
On this screen you will have to enter the password that will be used to secure the encryption. Here you will have to enter it twice. And then – IMMEDIATELY – write it down somewhere. You will need to know and remember this password – or you will have no way to retrieve your data. This cannot be stressed enough – if you lose that password – you will lose your data!!!



In some cases – your password will be too short. This is displayed for anything less than 20 characters. You should mix your passwords to have Letter and Numbers.

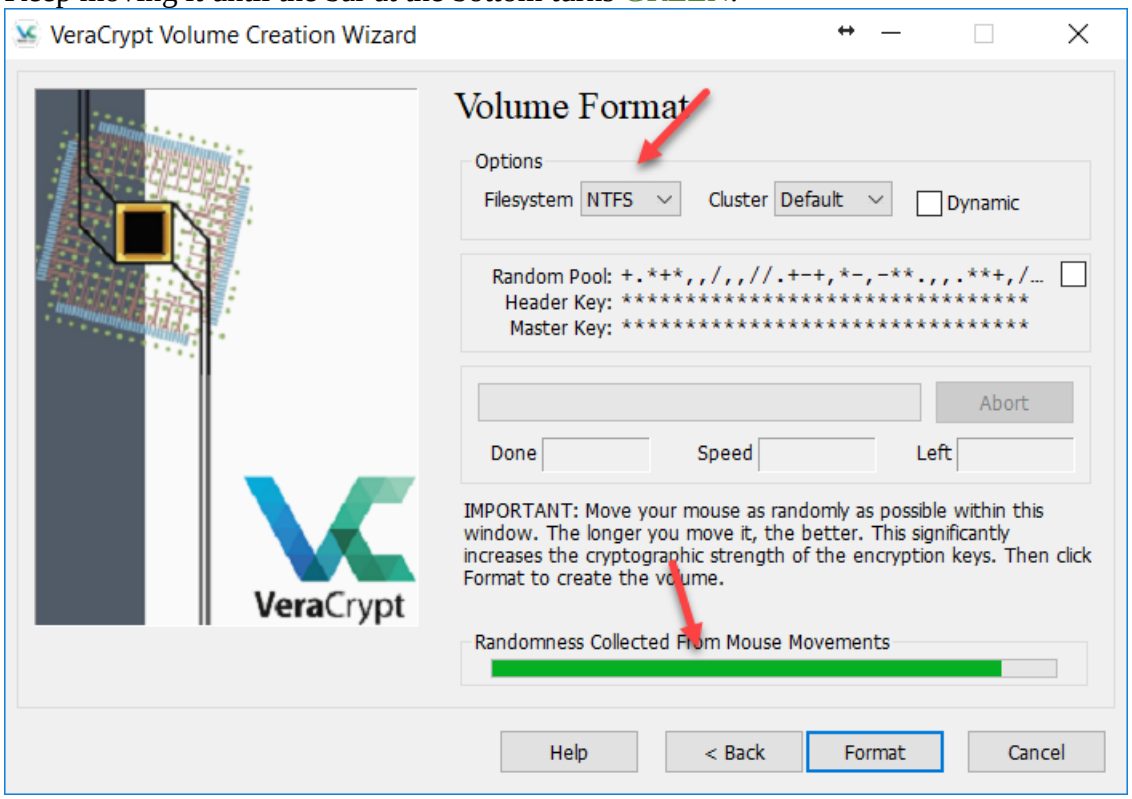


The next screen to be shown will be asking whether you will be storing large files on this volume or not. Please choose YES.

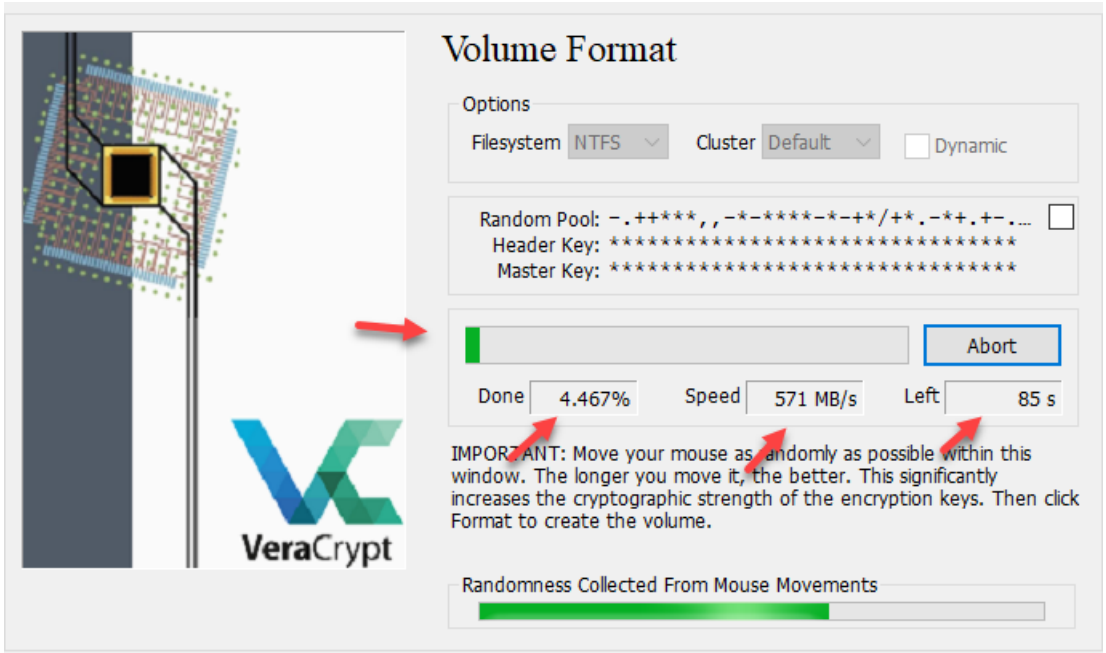


On the next screen you tell VeraCrypt what type of format you want the drive to be formatted in. For most cases we suggest using NTFS for our data conversion purposes. This will allow you to easily handle large files (> 4GB).

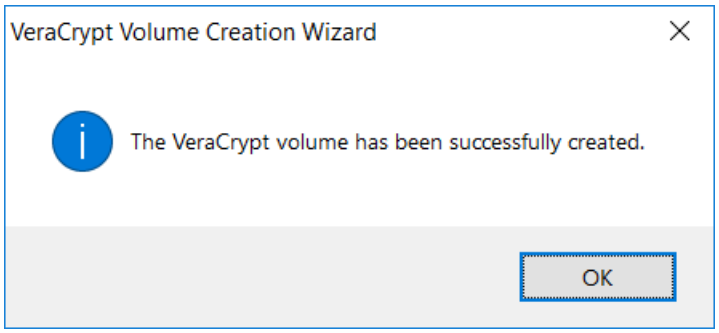
As well – the program wants you to move your mouse around the screen to generate the best encryption possible. Keep moving it until the bar at the bottom turns GREEN.



When you are ready – hit the Format button – and the creation of the volume begins. Here you will see progress as to how much is done, the speed at which is being encrypted – and how much time is left. The bigger the drive – the longer the process will take.



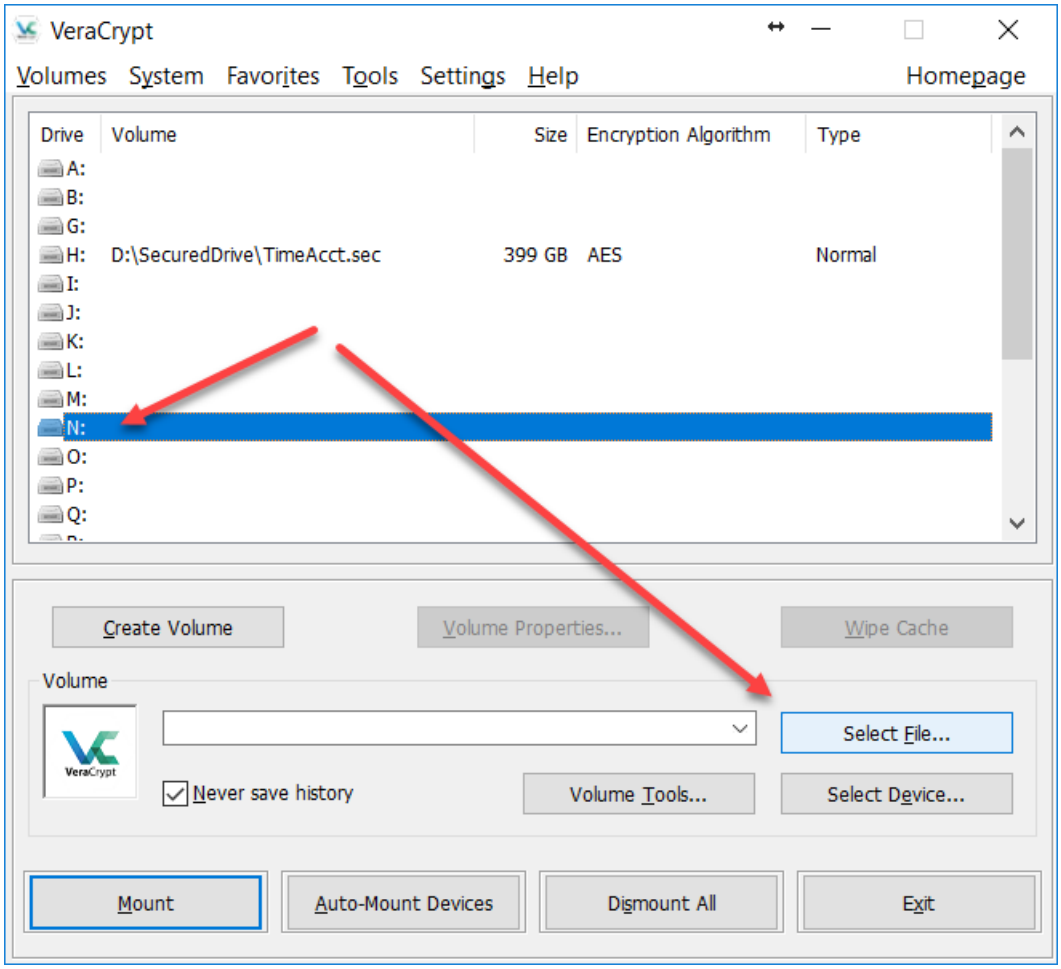
When the process completes – you may be prompted to allow the program VeraCrypt to make changes to your computer. This is the standard User Control prompt. When the process is complete – you will see the following message…



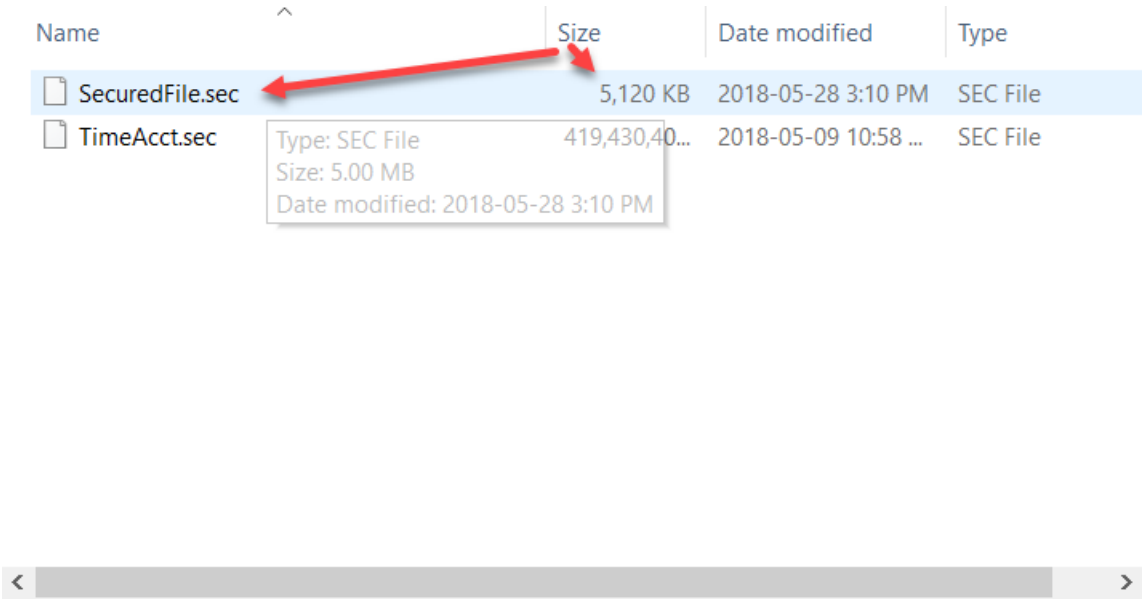
Mounting an Encrypted File

Now that we have an encrypted container (file) created – we have to 'Mount' it to make it usable.

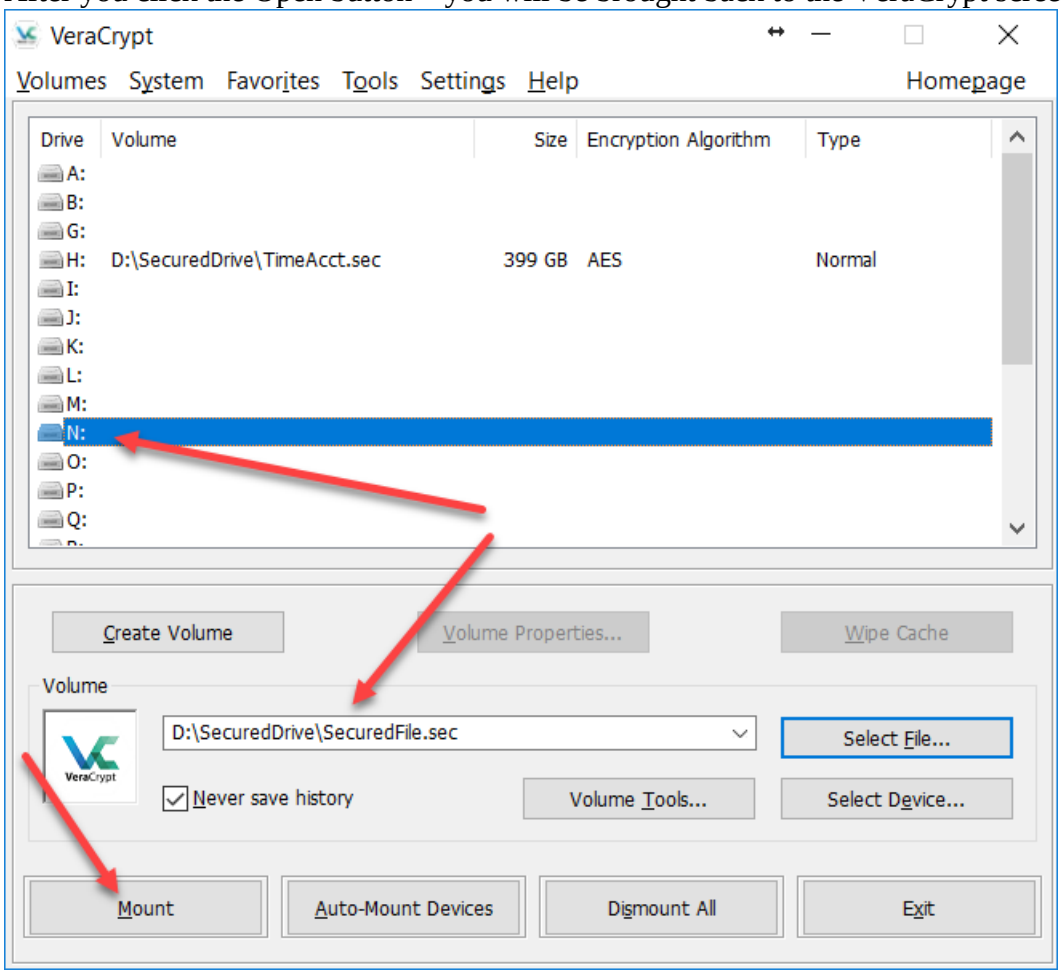
So – launch VeraCrypt as we did in the steps above. Here we want to select what drive letter we want to use – and then click the 'Select File' button.



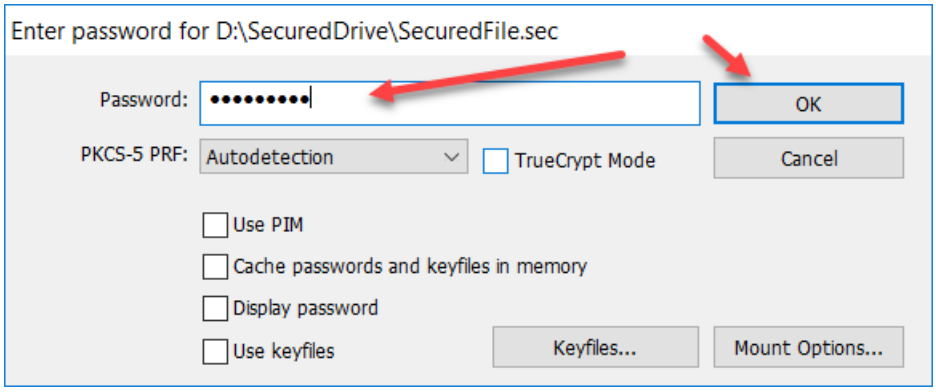
When you click the Select File button – the standard Windows file selection window appears. Navigate to your external drive and select the encrypted file you created above. In our example – it is called SecuredFile.sec. Note that in interest of speed – we only created this encrypted file to be 5MB in size – not the 50 GB in the example. However, you can also see in this directory we have a 420GB secured file.



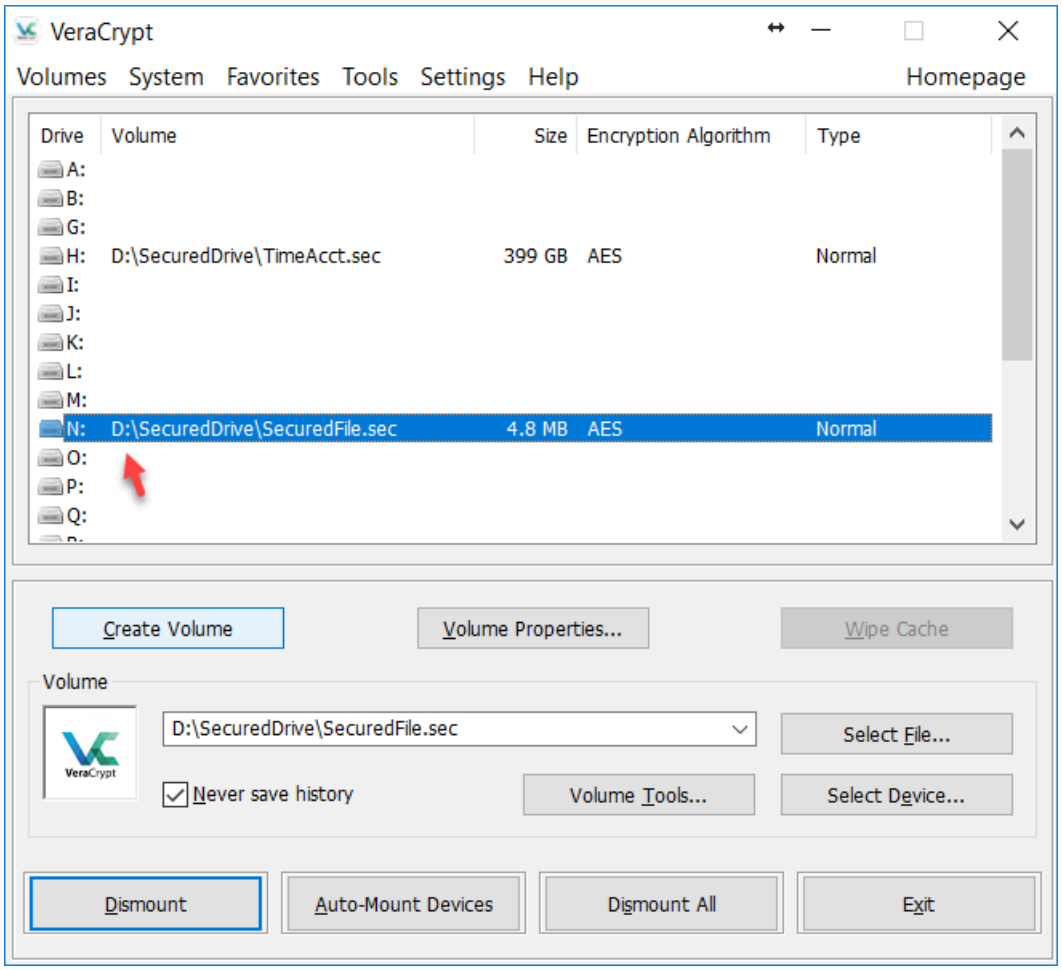
After you click the Open button – you will be brought back to the VeraCrypt screen – click on the Mount button.



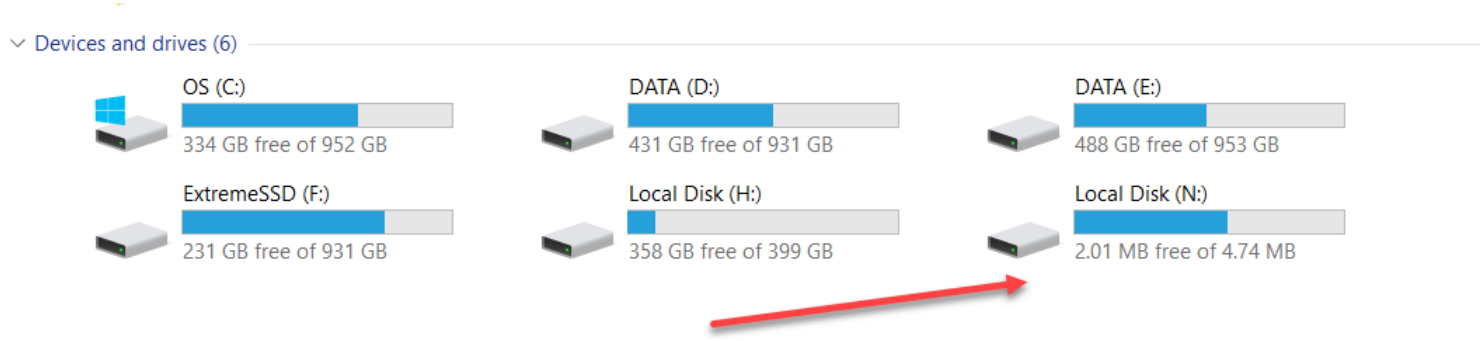
When you click on the Mount button – you will be prompted for the password. Enter it in – and click the OK button. REMEMBER – without the password – you have no way to access the encrypted archive – and your data will forever be unavailable.



You are once more brought back to the VeraCrypt screen – only now – your file is mounted to the drive letter you had selected!!



When you open up explorer – you can see that you now have a Drive N. It acts just like any other Windows drive. You can create directories and files in it. Now – copy the data you want to send to TimeAcct Information Systems – to this drive. When you done – you can remove the drive letter link – by clicking on the Dismount button



You will need to send the password to TimeAcct Information Systems. The best way is either by email or by phone. DO NOT Ship it with the drive!!