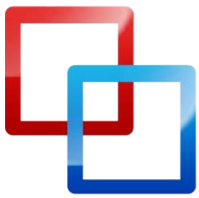

makeuseof.com
presents
Lock Down:
Secure your files
with TrueCrypt
By Lachlan Roy



makeuseof.com

LOCKDOWN: SECURE YOUR FILES WITH TRUECRYPT

By: Lachlan Roy
http://lachlanroy.com

Edited by: Justin Pot
Cover Photo: Kristy Pargeter via Shutterstock

Table of Contents

Introduction

Your laptop has been stolen.

You left it there for just a second and there were plenty of people around, but you came back and it was gone. It takes a moment to sink in.

It's *gone*.

First comes the initial shock, then the disbelief. Maybe I just put it down by the chair so that it was out of the way… Nope. It's not there either. It's been taken.

"Damn", you think. "I'm not getting *that* back." But it's not that bad. It was an old laptop, faithful but due for retirement.

But then it hits you.

My email account.

My bank details.

My personal details, and the details of all my friends and family.

The financial reports for my business.

The pictures of my family.

I've got them all backed up, but that's not the problem here. They're out there in the wild, now. Who knows where they could end up and who could see them? Who knows how that information could be exploited? What am I going to do?

The world shrinks around you as you realise the enormity of what has just happened. If only you'd encrypted your data.

What is encryption?

Encryption is the process of protecting data by using an algorithm to scramble it. The data is unintelligible, undetectable, unreadable and irretrievable unless a key is used to reverse the encryption, or *decrypt,* the data.

Encryption is used all the time, often without you even realising it. Whenever you buy something online and make a transaction, all your details are heavily encrypted until they reach the other end, making sure that no third party could be listening in. If you use instant messaging programs it is possible to create an encryption tunnel to ensure that only you and the person you're talking to can see the messages.

In this manual we'll be talking about *local file encryption* – that is, encrypting files on a hard drive (or encrypting the entire hard drive; more on that later). The files are safe as long as they are kept in the encrypted area.

What do I need encryption for?

If you have files that you don't want (or can't afford) anyone else to see, then you have a use for file encryption. Its entire purpose is to keep files hidden and safe.

Advantages of encryption

The biggest advantage of encrypting your files is the knowledge that your data will be safe if your computer is stolen. As soon as your computer is turned off you'll know that all your files are inaccessible, and may in fact be locked earlier depending on the type and level of encryption that you use (more on that later).

When you sell your computer (or dispose of it by other means), it's always a good idea to make sure that your data is securely erased to prevent the recovery of deleted files by whoever comes across the computer next.

The great thing about data encryption is that, without the key for decryption, the data appears as random noise. Unless the person happens to know the decryption key (which is highly unlikely), you might as well have already securely erased the drive.

Disadvantages of encryption

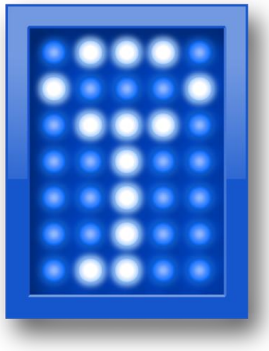
Unfortunately, encryption's strength is also its weakness. Encryption is great at keeping people without the decryption key out. The problem: if you've forgotten the password that includes you too. Once that data is encrypted and you lose the key you might as well have securely deleted the files, and you're not getting them back.

While it's nowhere as dire as losing the files forever, another disadvantage of encryption is that you will lose some read/write performance when working with

encrypted files (that is, opening files, saving them and/or moving them around). While this decrease is imperceptible when working with a few small files, working with thousands of tiny files or a few really big ones will take significantly longer as each file is decrypted before it can be used.

Thankfully, TrueCrypt supports parallelization (splitting data between the multiple cores of most recent processors), which means that in even these circumstances the drops in performance are minimized.

What is TrueCrypt?



TrueCrypt is a free, cross-platform program (meaning that it works in Windows, Mac OS X and Linux distributions including Ubuntu) that you can use to encrypt your data. It is classified as 'On The Fly Encryption' (OTFE) software, which basically means that it encrypts and decrypts files as you access and modify them and that all files within the area of encryption are available as soon as you enter the key.

Different types of encryption

There are three main types of encryption, each with a different level of technical difficulty to implement and with its own advantages and disadvantages. We'll be taking a look at each of them and eventually finding out how to set each one up.

Virtual encrypted disk

The virtual encrypted disk (VED) is the quickest and easiest type of encryption to set up. It works by creating a file of a specified size that can then be mounted. Basically, it acts just like an external hard drive. When you unmount the VED the files inside are invisible – only the VED file itself is visible and appears as random data when analysed at the hardware level.

Using a virtual encrypted disk has a couple of downsides. The first is that, because the file is its own discrete file that is stored in a folder like any other file, it can be quite conspicuous and stand out easily. It is also easy to accidentally delete the file and all the files in it. However, being a separate file also has the advantage that it can be moved around easily.

The other main disadvantage of a virtual encryption disk is that you must choose how large you want it to be when you create the file. This file cannot be resized easily and takes up the entire amount of space straight away, which can be troublesome if you make it too big or too small to begin with. Too large, and you'll

be wasting hard drive space; too small, and you'll run out of room when you go to store more documents.
If you're using Windows it's possible to create a *dynamic* VED; that is, one that starts small and only increases in size as you add files to it. However, a dynamic VED is much slower than a standard one, is no longer cross-platform and is a lot easier to detect than it would be otherwise.

Partition/drive encryption

Partition/drive encryption covers an entire drive (or one of its partitions, if your drive happens to be divided up). It's a little more complicated to set up than a VED, but it has its own rewards. For example, as the encryption covers the entire hard drive it is arguably less conspicuous while casually browsing files, and it is a lot harder to accidentally delete your important files. You also don't need to worry about the size of a virtual drive, as the entire partition is encrypted.

The big downfall of encrypting the entire drive is that it takes a very long time to set up, mainly because TrueCrypt has to create random data and write it to the entire hard drive. The other thing to bear in mind is that because you're encrypting the whole drive you won't be able to use any of it without the key. If you lose your password then you won't be able to use the drive without losing *everything*.

System encryption

The last main form of encryption goes one step further than encrypting your data – it encrypts the entire operating system and all the data on that partition with it, requiring you to enter your password before you get to the operating system (this is known as *pre-boot authentication*). However, this particular type of encryption through TrueCrypt is only compatible with Windows. Never fear, though! Mac OS X and most Linux distributions have some form of system encryption built in to the operating system itself, so they just require you to turn it on in the system preferences.

System encryption is the most secure, but it also has the most at stake. If you lose your password, you'll not only lose access to your encrypted data, but to your applications and the rest of your computer, too. This is fine if you have another operating system on a separate drive or partition to fall back on (or if you have a Linux Live CD), but if you don't you'll be stuck without your computer. Either way you'll be forced to erase everything on the drive and reinstall everything from scratch.

This isn't a problem so long as you write down your password in a couple of places so that you don't forget it, but it's definitely worth bearing in mind.

The other thing to take into account is that encrypting the operating system is by far the most complex encryption type so will take a lot longer than the others to set up and is more likely to have something go wrong. This would most likely entail the TrueCrypt Boot Loader (which comes up before you boot Windows and is where you

enter your password to decrypt the system) becoming damaged and failing to load (and locking you out of the system).
With this in mind TrueCrypt requires you to create a rescue disc that you can use to decrypt your installation in case something goes wrong.

Which type of encryption is best for me?

The vast majority of users will want to use either the virtual encrypted disk or encrypt a whole drive or partition. Which one is "better" depends on how much you want to encrypt. If you only have a couple of GB or less of sensitive data there's little point in encrypting an entire drive, especially as it makes it a lot harder to move the encrypted data around.

There are very few scenarios in which encrypting the entire operating system is the recommended choice, considering the number of things that could go wrong and the consequences if the password is lost. If you're working with data sensitive enough to require the entire operating system to be encrypted then the chances are you aren't setting it up yourself.

To summarise: you're probably best off using a virtual encrypted disk unless you either have a lot of sensitive data or a very small drive/partition, in which case you might as well encrypt the whole thing.

Installing and Using TrueCrypt

Downloading TrueCrypt

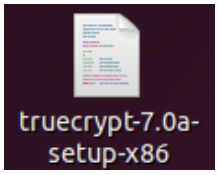
The first thing you'll want to do is go to the TrueCrypt download page at http://www.truecrypt.org/downloads, and choose the download for the operating system that you're using.

Each platform has a slightly different installer. For Windows you download an .exe file that is the actual installer. For OS X you download a .dmg image file that you *mount* to reveal the installer file (which is a .pkg file). For Linux you need to choose either the 32-bit or 64-bit version (if you don't know what this is, download the 32-bit one). This will download a .tar.gz file (which is just like a .zip file) which contains the installer file which you can extract and then run.

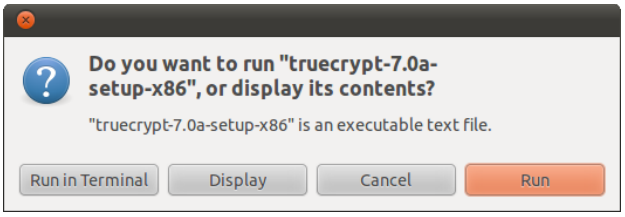
Installing TrueCrypt

The process of installing TrueCrypt is very similar for Windows and OS X and is just a case of following the instructions on each screen. It's just like installing any other application, so you shouldn't have any problems.

If you're using Linux then the process is a little different, but it is still very straightforward. Once you've extracted the installer somewhere (your desktop, for example), you'll see this:

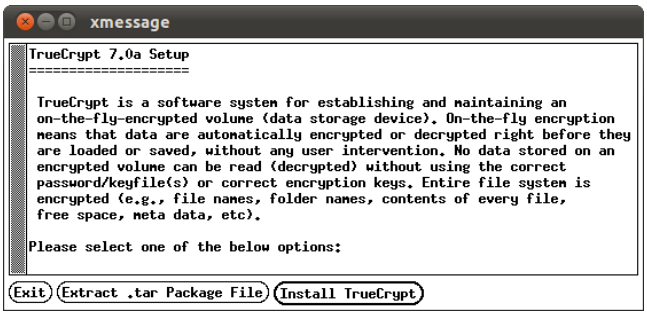


When you double click on it, you'll be met with this dialog box:

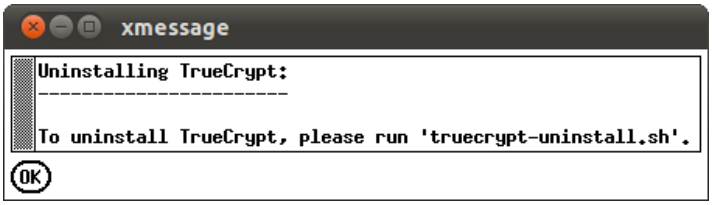


Obviously you want to run it, so click on "Run".

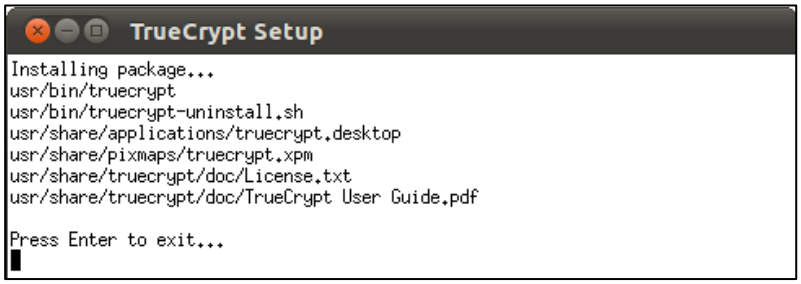
After that you'll be met with a black and white installer that looks like this:



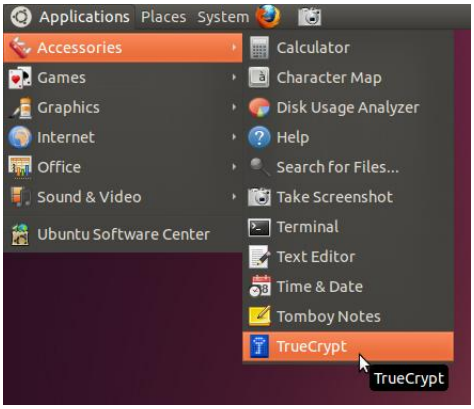
Just follow the prompts as you would with a normal installer. The only thing that needs mentioning is that you'll see this and probably get confused for a second:



Relax, it's not uninstalling the program as soon as you've installed it! That's just telling you what you need to do if you want to uninstall TrueCrypt later. Click okay and then you'll see this, which shows that you've installed TrueCrypt properly:

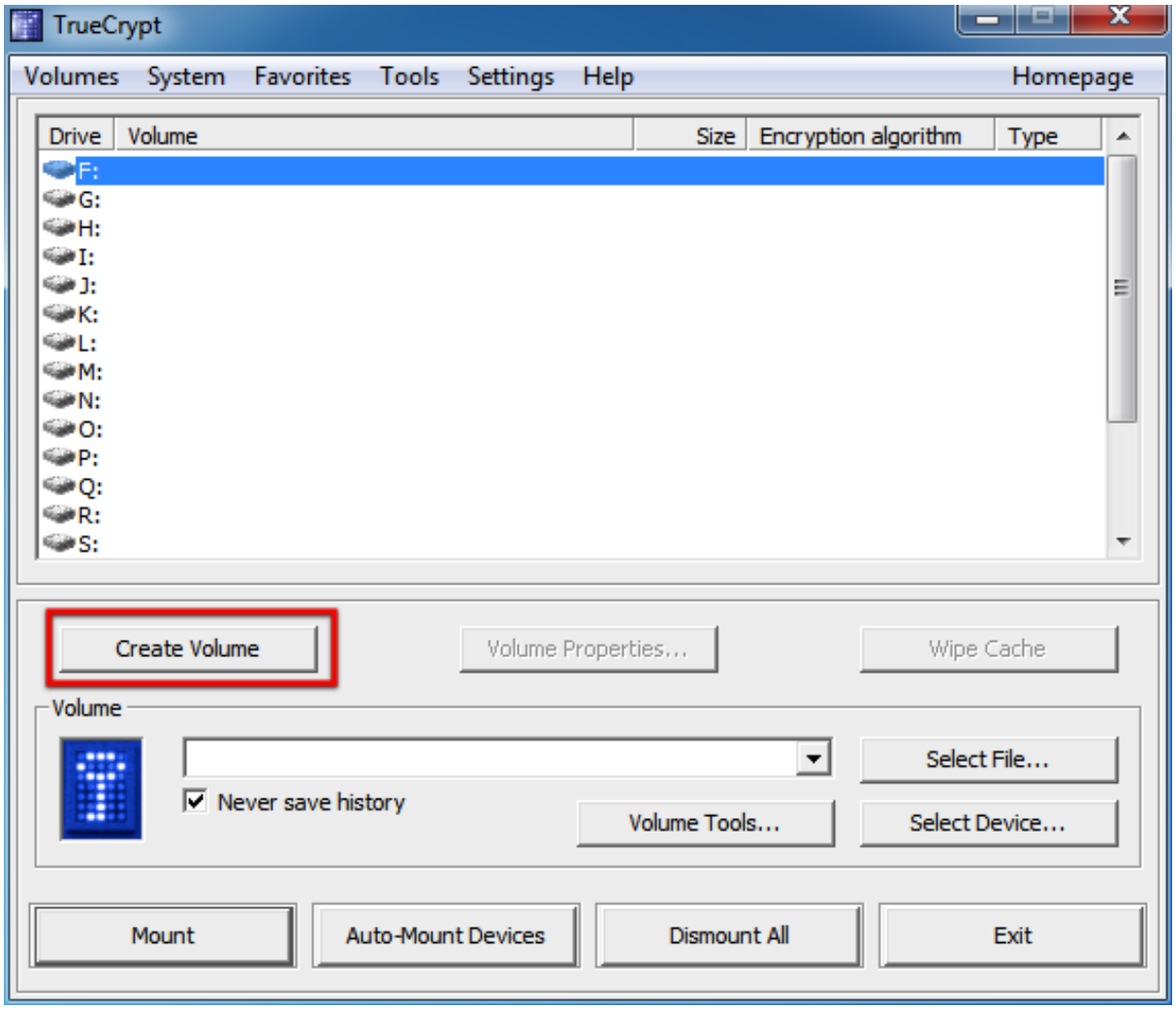


That's it! You can find TrueCrypt in the Applications menu under Accessories:



Creating a virtual encrypted disk

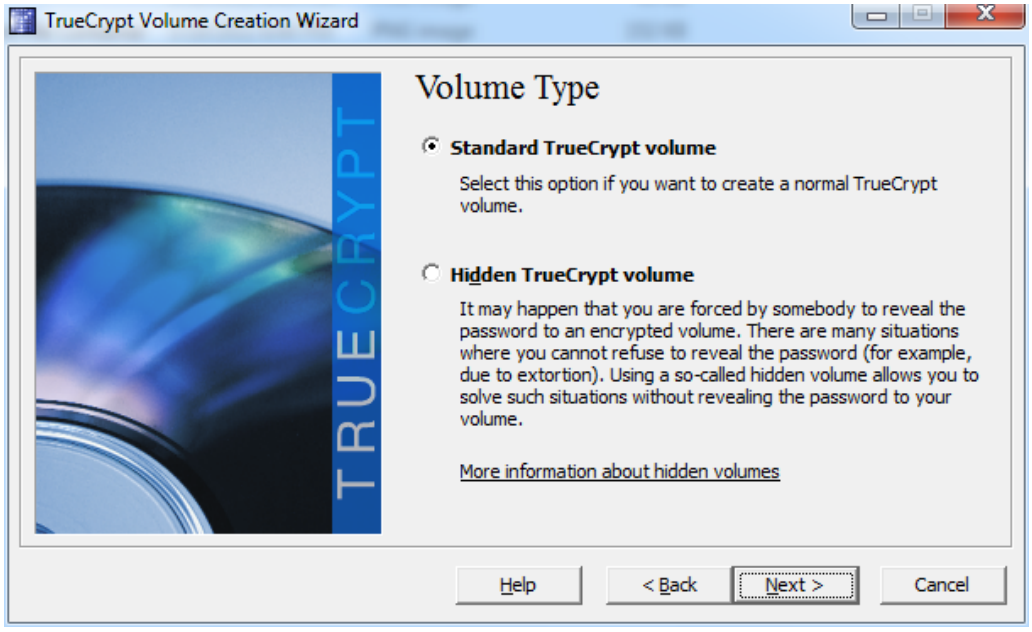
Regardless of what platform you're using, when you open up TrueCrypt for the first time you'll see this window (although in Ubuntu and Mac OS X the drives are simply numbers and not drive letters like they are here):



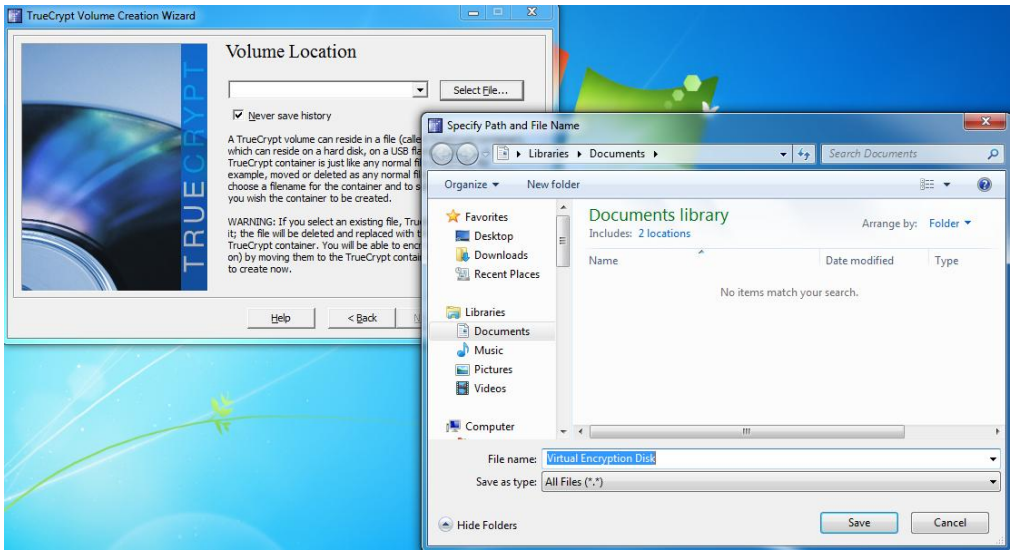
The first thing we want to do is create a new Virtual Encryption Disk, so we'll click on "Create Volume". This will start the TrueCrypt Volume Creation Wizard, which will guide us through the steps we need to create the VED.

The wizard looks like this:

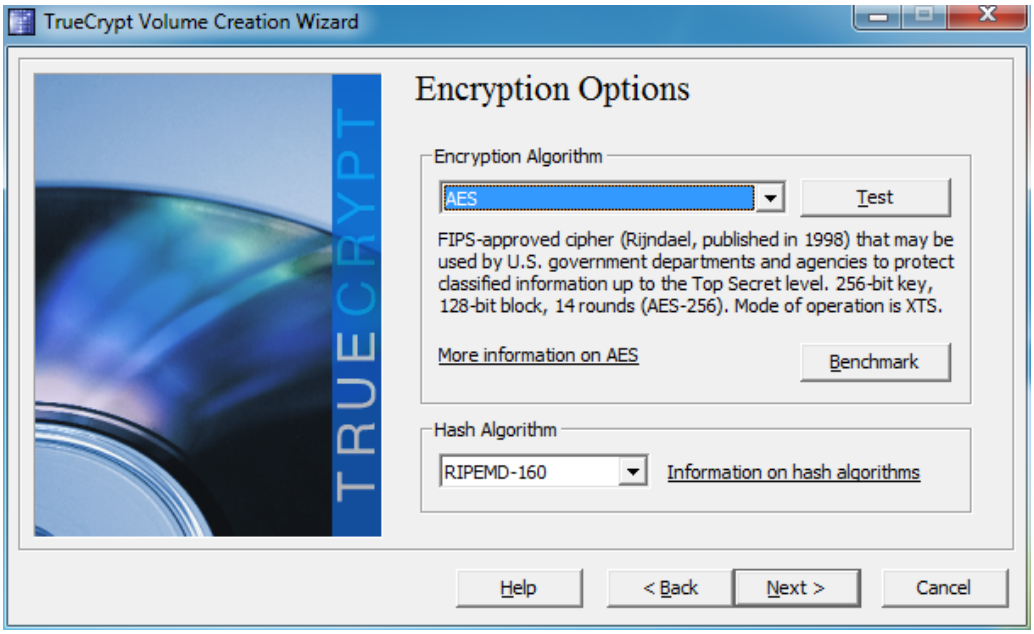
We want to create an encrypted file container, so we'll select this option and then click on "Next". Then we'll make sure that "Standard Truecrypt volume" is selected and then click on "Next" again.



It is possible to create a hidden TrueCrypt volume but there are very few reasons why you would want to make one (that is, unless you're likely to be subject to extortion for the files you're hiding!). If you want to know more you can read the documentation for hidden volumes on the TrueCrypt website.



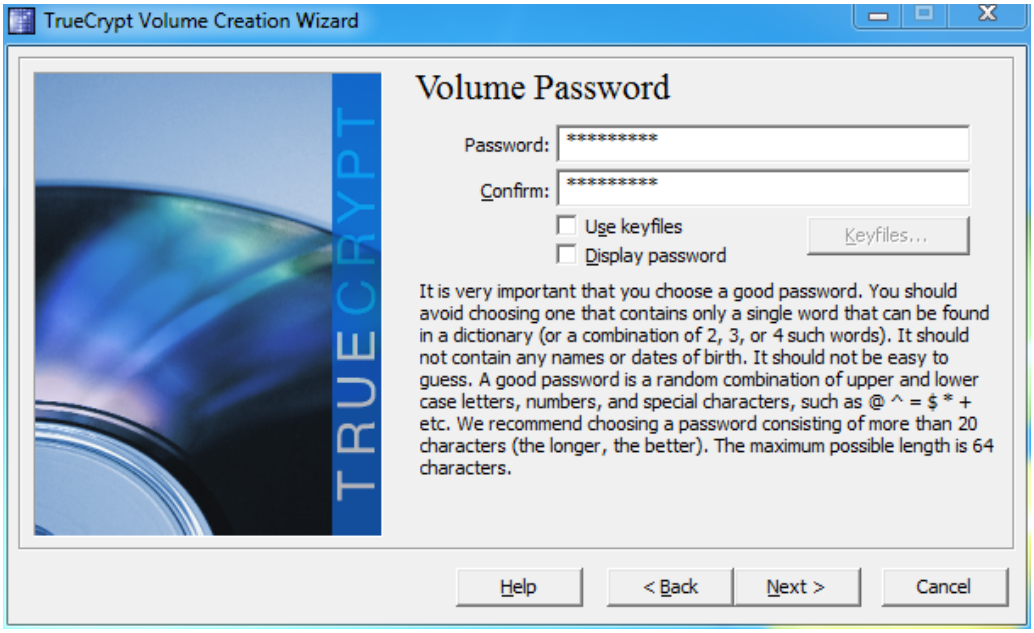
Next we're asked to select a location and a name for the VED. Here I've called it "Virtual Encryption Disk" and just stored it in the "My Documents" folder. Then it's time to click "Next" again!



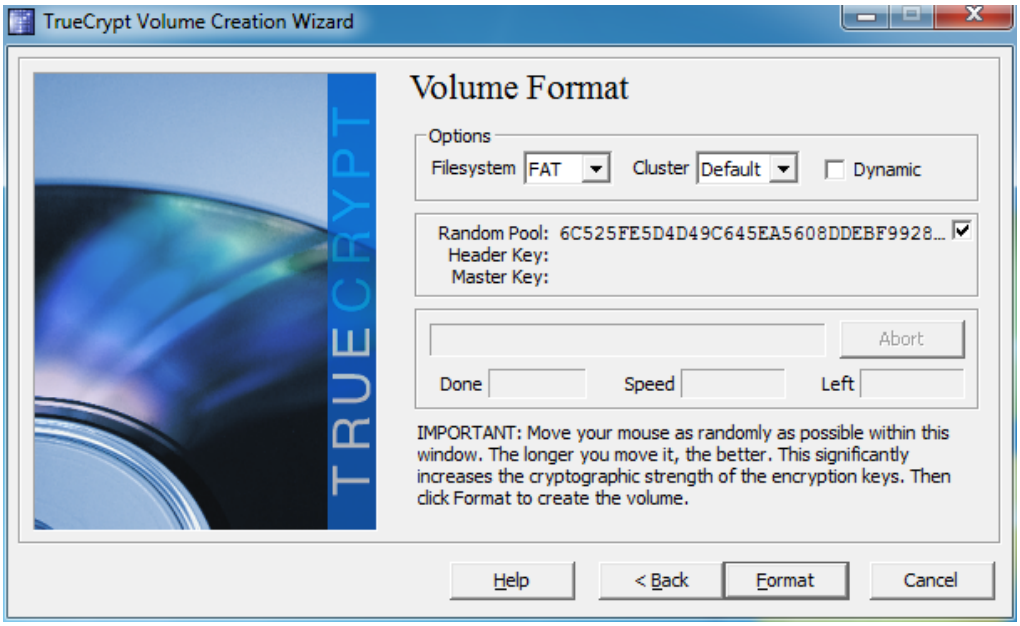
We don't need to worry about any of the encryption options – even the defaults are plenty secure enough for our needs! The defaults should be "AES" and "RIPEMD-160" for the respective drop down menus, but it doesn't really matter either way. To the next step!

Now we're going to choose how much space we want to allocate to our VED. I've chosen to give 250MB to this one:

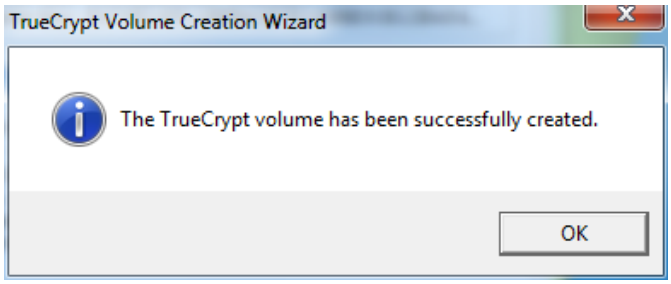
After clicking on "Next" yet again, it's time to choose the password for our VED. The length our password needs to be depends on how secure we need to be, but we need to be able to remember it! I've chosen a 9 character complex password (more on that later), which should be more than secure enough for the data that I'll be storing in it.



An error will pop up if the password is less than 20 characters long; don't worry about it, and just continue. Onwards!



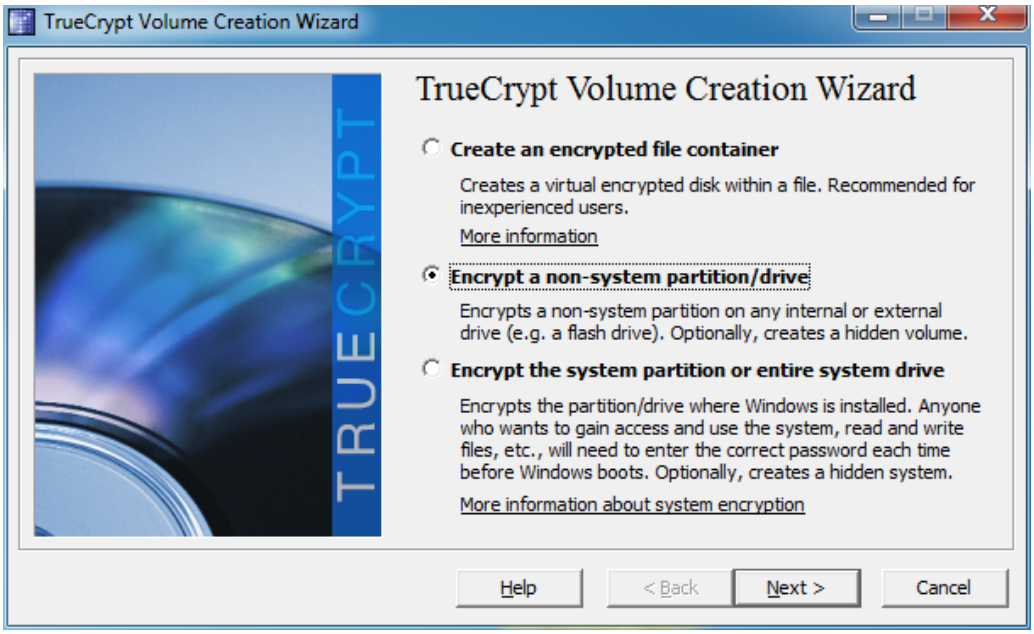
The next screen is where we format the volume and generate the encryption keys for the VED. TrueCrypt uses the movement of our mouse to help increase the cryptographic strength of the keys, so make sure to move your mouse randomly over the window for a while before clicking on "Format". When it's finished you'll see this dialog box pop up:



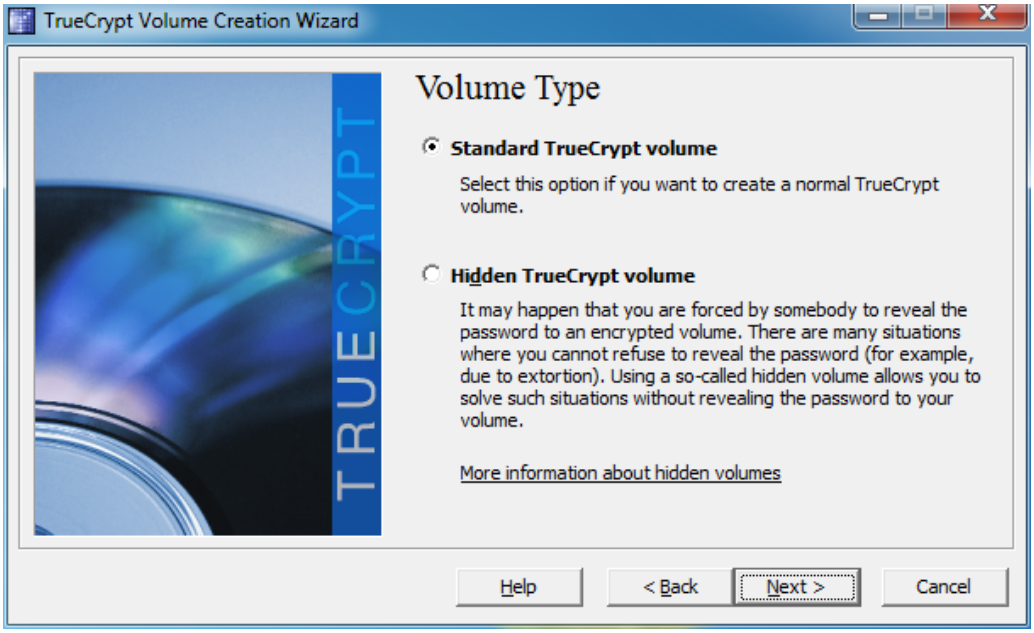
That's it! Your VED is ready to go. The next step is to mount it, but we'll talk about that a bit later on.

Encrypting a drive or partition

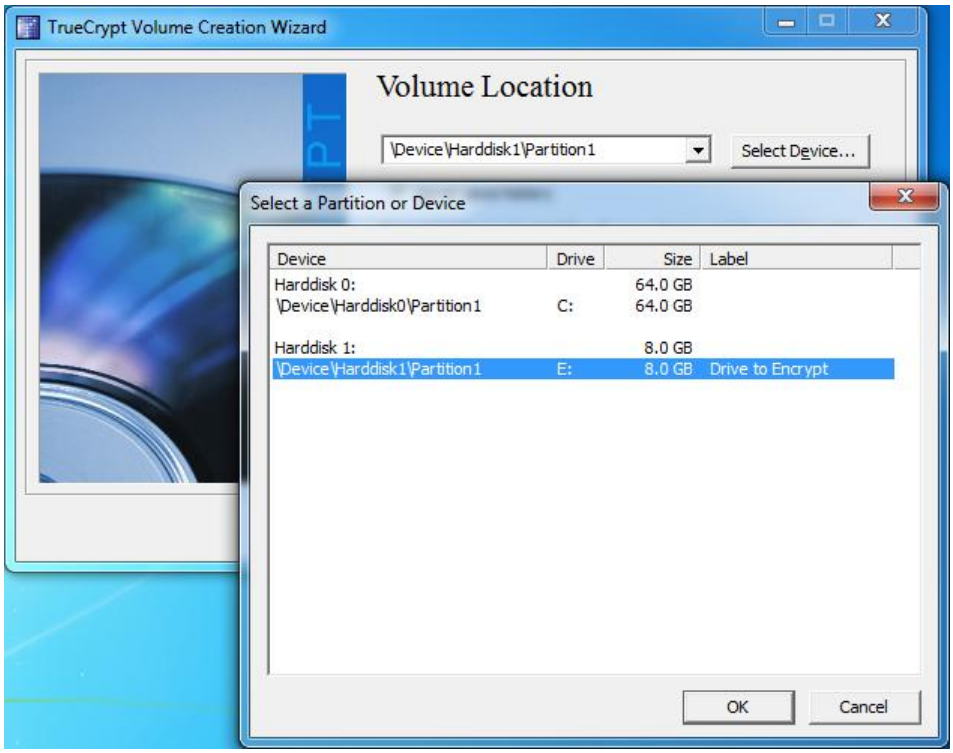
Just like creating a VED, the first step is to click on "New Volume" in the main TrueCrypt window. However, instead of selecting "Create an encrypted file container", we'll be selecting "Encrypt a non-system partition/drive" before clicking on the "Next" button.



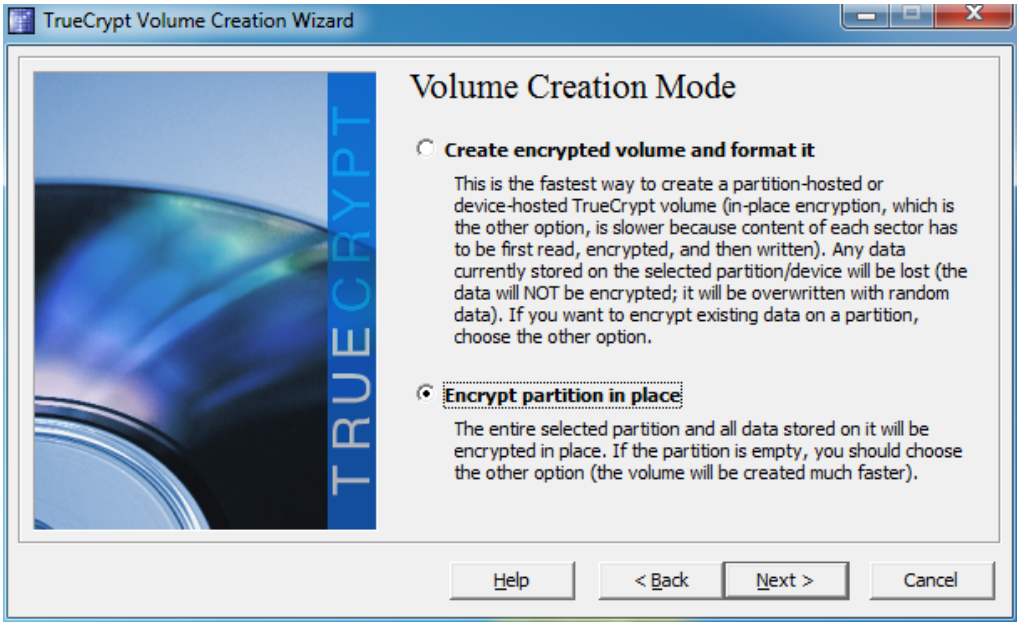
While it's possible to create a hidden volume, we'll just be making a standard encrypted volume this time. Make sure "Standard TrueCrypt volume" is selected and then click on "Next" again.



Now we need to choose the partition that we wish to format. I have a virtual drive that I created for this example, so I'll select that:

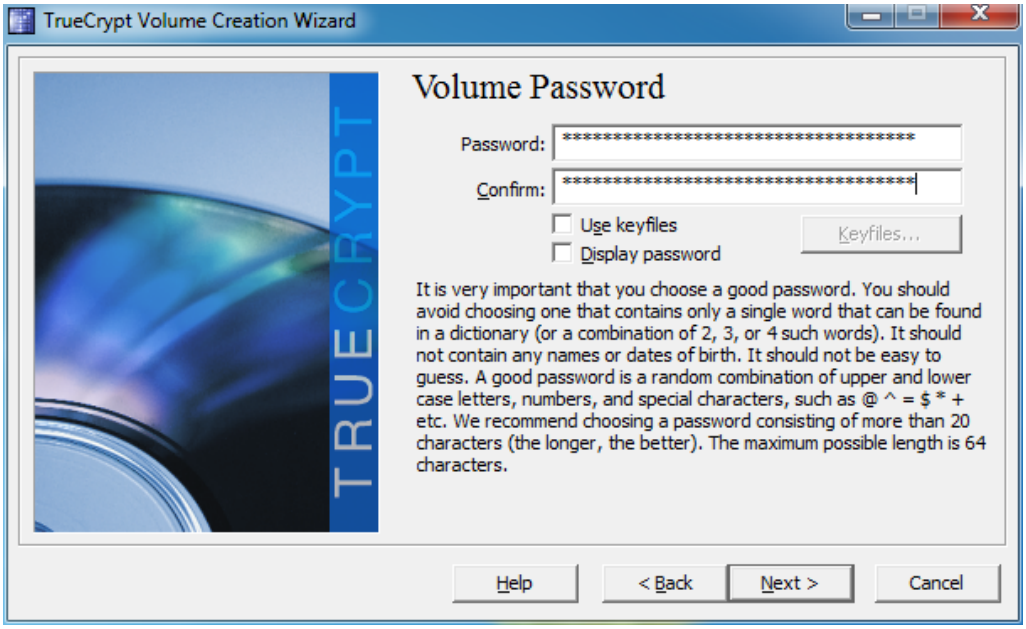


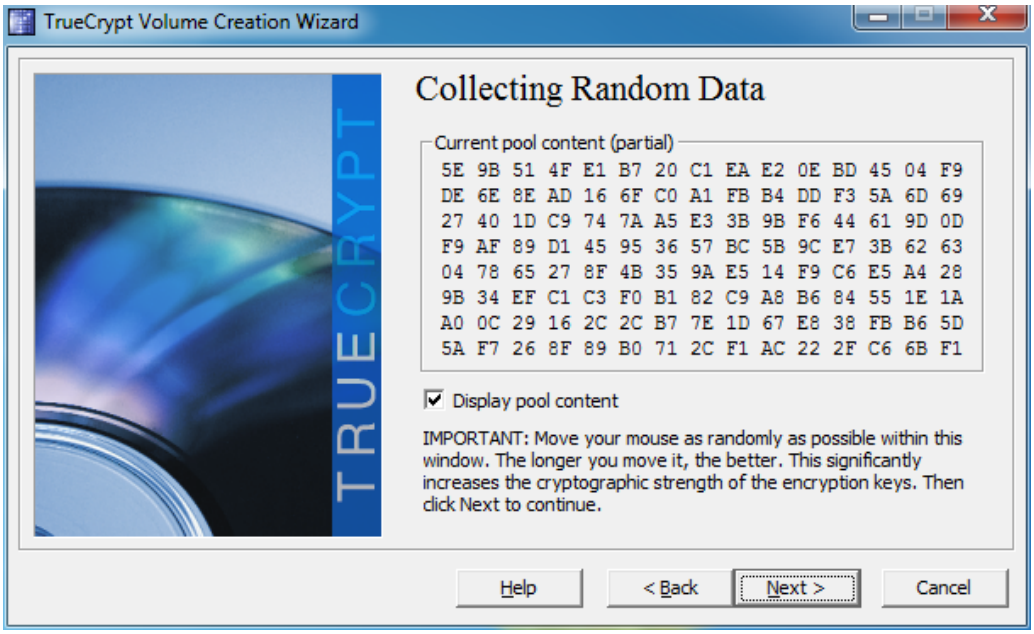
After that we need to choose how we create the volume. This basically boils down to whether you already have data on the drive that you want to encrypt or whether it's been freshly made. I've already got some files on this partition, so I've selected the "Encrypt partition in place" option.



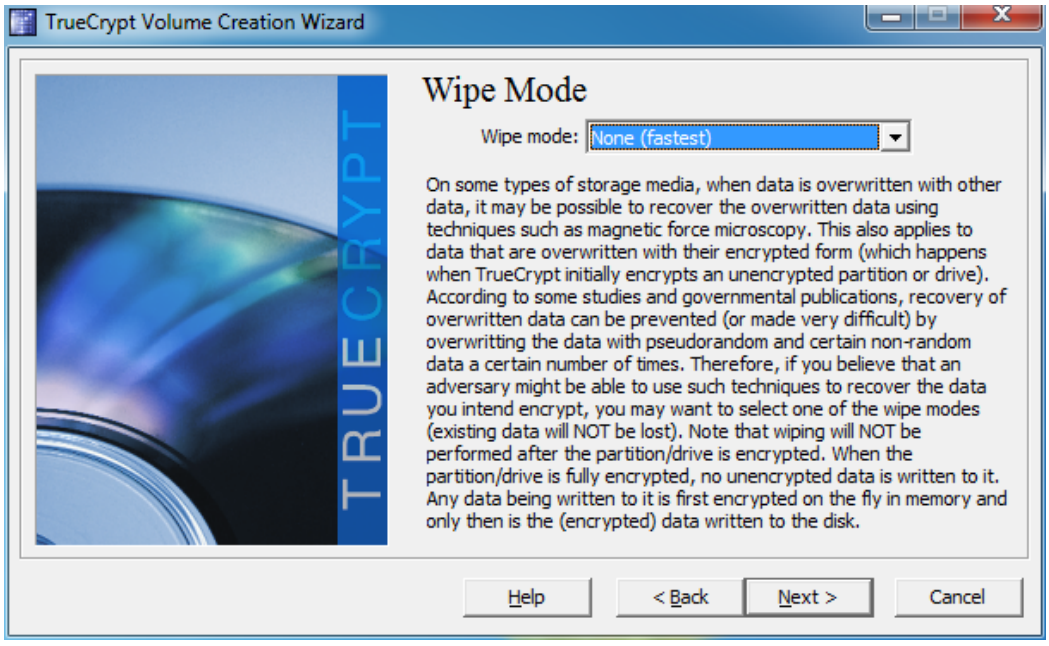
Next up is to choose the encryption options. Just like with the VED we don't really need to change any of these settings since they'll be more than secure enough for what we're using them for. Just click "Next" to move on.

Now it's time to choose a new password. Again, there's no point in having a ridiculously long password if you can't remember it (more on that in the 'Selecting good passwords' section below). Once you've entered and confirmed a password, click on "Next" again.





Here we're generating the keys for the encryption. Moving the mouse randomly in the window makes the keys stronger, so make sure to do that before clicking "Next"!

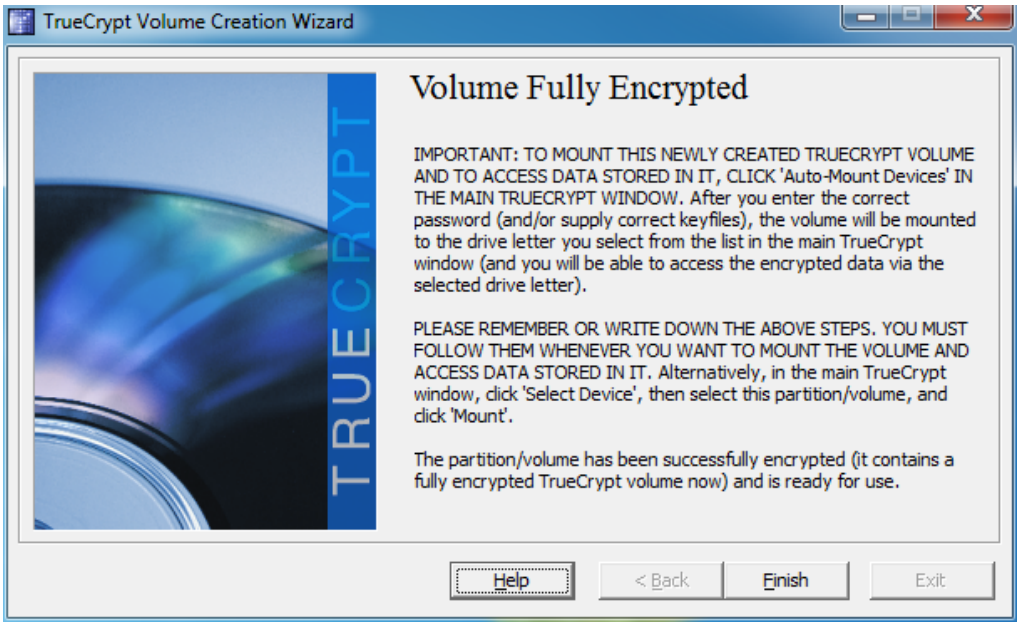


If there's data that you've deleted from the drive that you want to be unrecoverable, you'll want to choose a wipe mode that overwrites the raw data. In this case there's nothing to overwrite so I'll choose the option with no overwriting, but if there's data you want to hide then you'll probably want to choose the 3-pass option. There are also 7-pass and 35-pass options but these would take far too long to be worthwhile.

Now we're up to the final stage – just hit "Encrypt"! You'll get a dialog box that reminds you that you won't be able to access the data at all until the entire drive has finished encrypting. There's also a warning that if your computer shuts down for any reason without giving it a chance to pause then you'll almost certainly corrupt some of the data that you're copying over (if you are). Even if you're not, you'll also have to start the encryption process again from scratch.

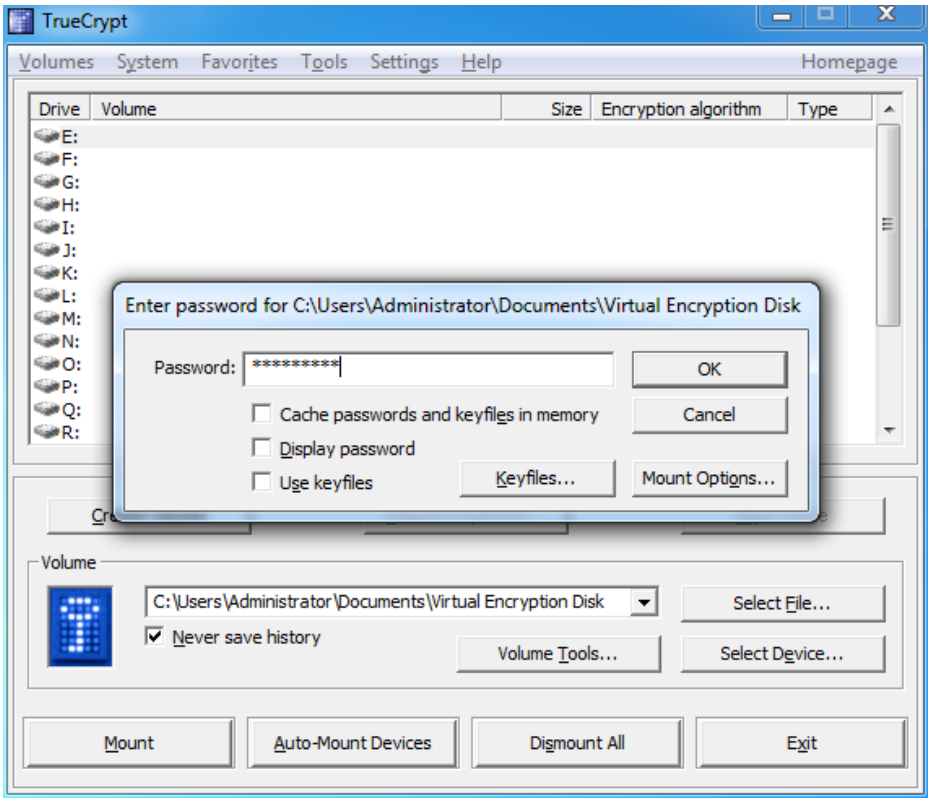
Go get a cup of coffee – this is going to take a while. Once you've finished encrypting the drive you'll have a few more dialog boxes pop up to give you some important instructions with regard to mounting the drive.

Once you've taken those on board, you'll be greeted with the last window:



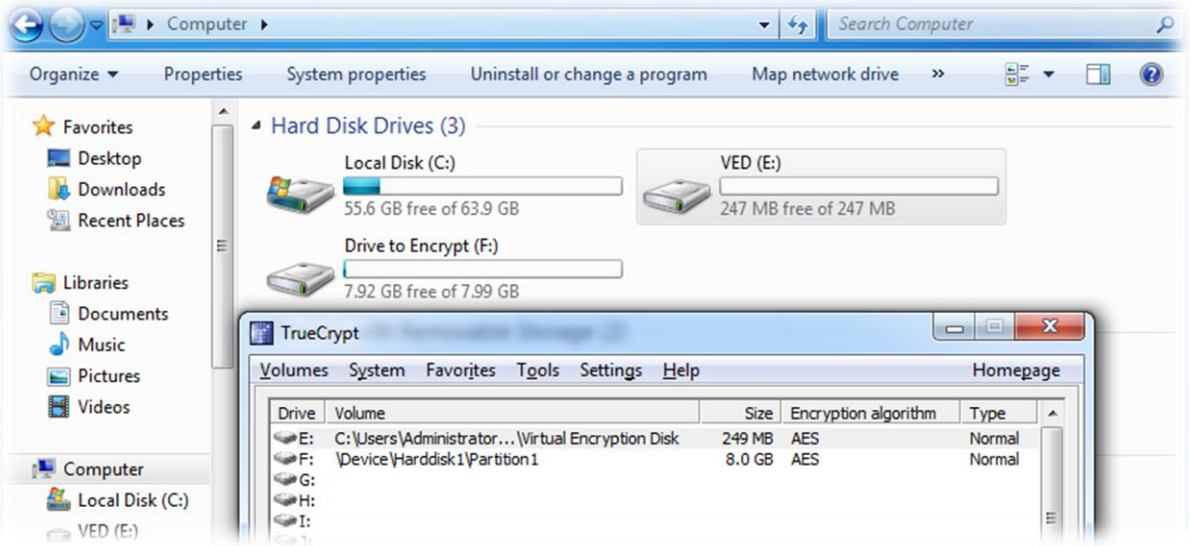
Mounting and dismounting encrypted disks

Mounting an encrypted disk is fairly straightforward. First we'll look at mounting a VED. In the main window we'll click on "Select File…" and select the VED that we created earlier. We're then asked to enter the password for the archive. It'll look a little like this:



That's it! Once we enter the password and click "OK", the drive will be mounted and will look just like any other hard drive:

Mounting an encrypted partition is even easier – all we need to do is click on "Auto-Mount Devices" at the bottom of the window, which will give us a dialog box to enter in the password of the encrypted partition. When we click "OK" it'll be mounted as a drive in the same way as the VED:



When you're finished working with the files, just go back to the main TrueCrypt window and click on "Dismount All".

Other Good Security Habits

Selecting good passwords

It's very important that you choose good passwords to keep everything secure. There are a few things to keep in mind when selecting passwords to use.
The first thing may seem obvious, but it needs to be said: make sure you use different passwords for everything! It doesn't matter how secure your password is; if you use the same password for everything and somebody manages to learn it, they'll have access to your entire digital life. That's not fun.

Secondly, your password actually needs to *be* secure. Setting your password as "password" or the name of your cat may be easy to remember, but they're also the first things that somebody trying to access your data is going to try.

A good password is one that is easy to remember but hard to guess or crack. This means that you can one of two routes:

- Go for a really, really long password. For example, the password "`TheRainInSpainStaysMainlyInThePlain`" is 35 characters long – long enough that no hacker is going to be able to figure it out and trying to crack it by brute force (using a computer to go through all the possible combinations) would take far too long. The only problem is that some websites or programs may set a limit to how many characters you can use.
- Go for a complex password. These should still contain at least 8 characters but includes upper and lower case characters, numbers and symbols to make the number of possible combinations for a shorter password much larger. "`nES+=3ux`" is an example of a complex password.

I personally prefer the complex route, as it's faster to type. "But Lachlan!" I hear you say, "How am I ever going to come up with a random password with symbols and numbers in it, let alone remember it?"

When I need a new password I'll usually come up with a sentence that is easy to remember, for example "All for one and one for all". Then I'll take the first letter of each word – "`afoaofa`". Right now it's not a complex password, but we'll get there.

Next we can change the "a" for "and" to an "&" sign. This gives us "`afo&ofa`". Now we need a number or two. The number 4 looks like an upper case "A", so we can change one of them out, and we can change the word "one" for "1". Doing that we end up with "`afo&1f4`". Starting to look better, isn't it?
If we make the first "a" a capital (like at the start of sentence), and add in a couple of punctuation marks at the start and end of the password we end up with

something like "`!Afo&1f4?`". Have fun trying to crack that! It's still pretty easy to remember, though:

`All for one and one for all → !Afo&1f4?`

If you're not feeling particularly creative you can always use an online password generator; I've personally found pctools.com's password generator to be the best. Regardless of what password you use or how you come up with it, it's a good idea to test the strength of your password; passwordmeter.com is great for that.

Locking your computer and logging out of services

It goes without saying that a password is pointless if it's not being used. Your computer may be protected by an awesome password that stops people from logging in. But what happens if you log in and then walk away for your computer for a while? Anybody could sit down and get at any of your files (unless you've got them in a virtual encrypted disk, that is!)

The quick and easy solution to this is to lock your computer whenever you leave it and go elsewhere. If you use Windows you can press the "Windows" key + L to lock your screen; if you're using Ubuntu, you can press "Ctrl"+"Alt"+L.
If you're using a Mac there's no keyboard shortcut, but it's still possible to lock your screen. There are a couple of ways you can do this:

Screensaver Lock

Simply go to System Preferences, click on "Security", then select the first option: "Require password after sleep or screen saver begins". You can select a period of time before the password is required ranging from an immediate lock up to 4 hours. If you want to lock the screen quickly you can then set one of your "hot corners" to start your screensaver. The setting for this is under "Exposé" in System Preferences.

Login Window

Alternatively, you can go to System Preferences and then click on "Accounts". Next, select "Login Options" towards the bottom of the window and select "Show fast user switching menu". This puts an icon or your username in the menu bar. You can click on this and then click on "Login Window…" to lock your screen.

You can also set the screen to lock after coming out of the screensaver on the other operating systems – the option is usually under the screensaver settings.
This is all well and good if you're using your own computer, but what if you're using a friend's computer, or a public one?

Just make sure that you don't tell the browser to remember any of your passwords and that you log out when you're finished. That way there's no chance that somebody can get access to your data without you knowing about it!

Conclusion

Your laptop has been stolen.

You left it there for just a second and there were plenty of people around, but you came back and it was gone. It takes a moment to sink in.

It's *gone*.

First comes the initial shock, then the disbelief. Maybe I just put it down by the chair so that it was out of the way… Nope. It's not there either. It's been taken.

"Damn", you think. "I'm not getting *that* back." But it's not that bad. It was an old laptop, faithful but due for retirement.

But then it hits you.

My email account.

My bank details.

My personal details, and the details of all my friends and family.

The financial reports for my business.

The pictures of my family.

I've got them all backed up, but that's not the problem here. They're out there in the wild, now. Who knows where they could end up and who could see them? Who knows how that information could be exploited?

But hang on a second. All my business files are in a virtual encrypted disk and the rest is on the second partition that I encrypted, and I locked my screen before I put it down. Even if they do manage to get past my 15 character complex password, they're not going to be able to get at my personal data.

I guess it's not so bad after all.

Thank goodness I encrypted my data!

Did you like this PDF Guide? Then why not visit MakeUseOf.com for daily posts on cool websites, free software and internet tips.

If you want more great guides like this, why not **subscribe to MakeUseOf and receive instant access to 20+ PDF Guides** like this one covering wide range of topics. Moreover, you will be able to download free Cheat Sheets, Free Giveaways and other cool things.

Subscribe to MakeUseOf : http://www.makeuseof.com/join

MakeUseOf Links:

Home:	http://www.makeuseof.com
MakeUseOf Directory:	http://www.makeuseof.com/dir
MakeUseOf Answers:	http://www.makeuseof.com/answers
Geeky Fun:	http://www.makeuseof.com/tech-fun
PDF Guides:	http://www.makeuseof.com/pages/
Tech Deals:	http://www.makeuseof.com/pages/hot-tech-deals

Follow MakeUseOf:

RSS Feed:	http://feedproxy.google.com/Makeuseof
Newsletter:	http://www.makeuseof.com/join
Facebook:	http://www.facebook.com/makeuseof
Twitter:	http://www.twitter.com/Makeuseof

Download Other MakeUseOf PDF Guides!

Like us to download: http://www.facebook.com/makeuseof