

**Computer Security**

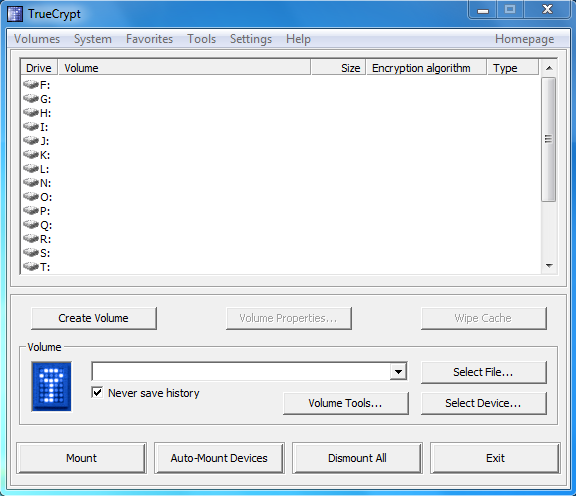
**Tutorial 4:**

**Part 1: TrueCrypt**

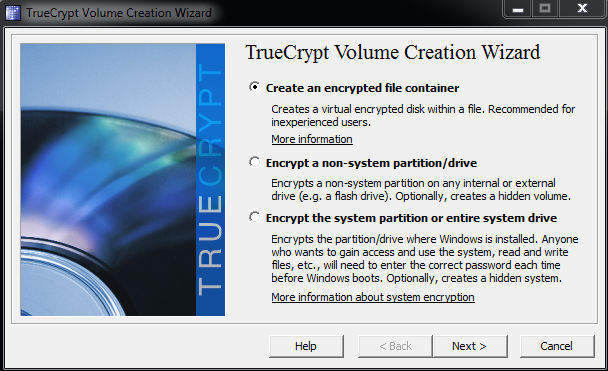
In this activity you will be using the freely available, open source program TrueCrypt to encrypt files thus ensuring their *confidentiality*. It is vitally important that you use TrueCrypt on a test machine as there is always the possibility of files being lost or a system being inaccessible. You use this tool at your own risk.

Please note that TrueCrypt is no longer considered secure by its developers. However, the program is still beneficial as a learning activity. The TrueCrypt installation file is available on Blackboard within this module. However, if you are undertaking this activity in a lab on-campus then the software should already be pre-installed and accessible from within the Windows Start Menu.

Navigate to the TrueCrypt program in your Windows Start Menu. Once you run the TrueCrypt program you will be presented with the screen shown below.



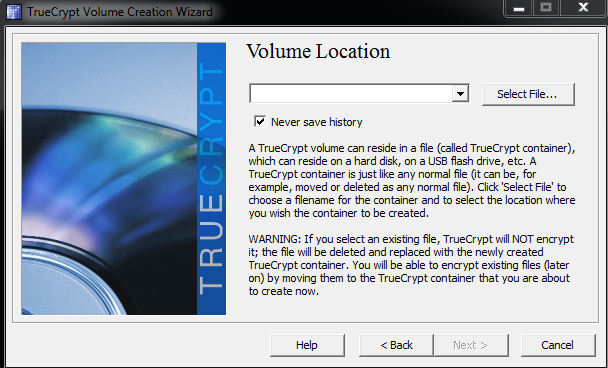
Click on the Volumes menu button in the top left hand corner followed by Create New Volume.



As per the image above, you will notice that TrueCrypt provides three means by which you can encrypt a specific section of the hard disk. Using the documentation provided with TrueCrypt you should familiarise yourself with the different forms of encryption that can be utilised. This will significantly benefit you in this unit. The option that we will be selecting as a part of this activity is the *Create an encrypted file container*.

1. What is an encrypted file container?
2. How does the encrypted file container function?
3. How does the encrypted file container differ from encrypting an entire system partition?

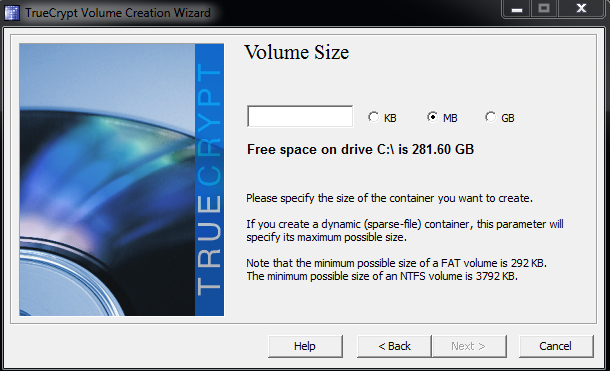
You should be presented with the option of choosing a Standard or Hidden TrueCrypt volume. We will be creating a Standard TrueCrypt volume for this activity, however you should familiarise yourself with the difference when using a hidden volume.



TrueCrypt will ask you to select a *Volume Location*, clicking the Select File button you should navigate to a specific location on your computer (preferably your desktop). Next, you should provide a name to your container file. In this instance you may call it *encrypt* or *test*. You will then be provided with a series of options to select an Encryption Algorithm and Hash Algorithm.

You should use this opportunity to go through the algorithms available and briefly read through the algorithm notes provided by TrueCrypt. This will provide you with the foundation information for the subsequent week three and week four lectures in this unit which will be covered.

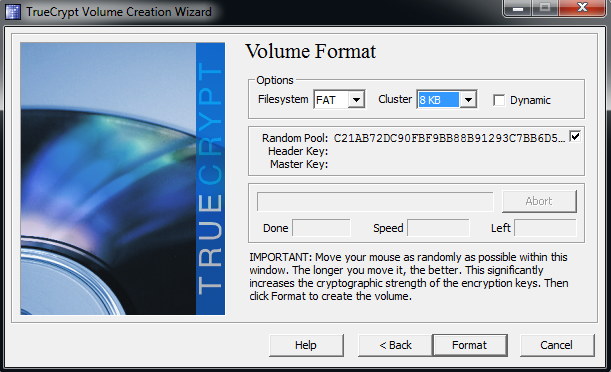
Having selected an Encryption Algorithm and Hash Algorithm of your choice (it will make no difference in this activity as to which one you have selected), you will then be prompted to select a Volume Size as per the image below. You may create a Volume Size as large or small as you like, but for this activity lets create a 100MB volume.



Once you have progressed through the Volume Size selection, TrueCrypt will prompt you to create and confirm a password which will be used to secure your encrypted container file. You may choose any password for this activity as we are just experimenting with this encryption program but in an ideal situation you would want to choose a password which is very strong.

1. Are you using symmetric or asymmetric encryption? This may not seem obvious at first, so it is recommended that you jump onto the World Wide Web and do a quick search of the differences between symmetric and asymmetric encryption. Once you know the answer, continue the activity. We will be covering these topics in the following two weeks so this will provide you with some useful background information for class.

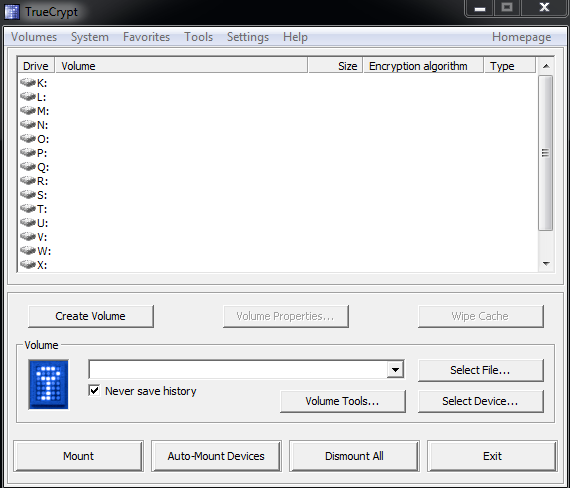
TrueCrypt will then display the Volume Format option. You will see that there are different Filesystem and Cluster options. These will be covered throughout the semester but you are being exposed to these now. Select the FAT file system and a 8KB cluster size and when you are ready click Format. Once the process finishes click through the remaining options and close the program.



All we have done so far is created an encrypted container file. No files have been encrypted as of yet, and so we have not ensured the confidentiality of any files, *yet.* Navigate to the location where you have created the container file. Note the size and location of the container file.

Next we need to actually use the encrypted container file to encrypt some documents. Assuming as per the last instruction that you have completely closed down TrueCrypt, you will need to run TrueCrypt again. However, this time you need to run the TrueCrypt.exe executable.

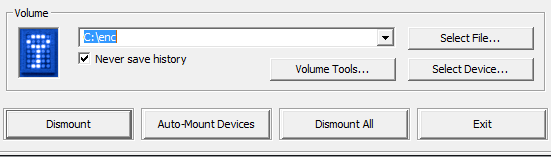
Once you run TrueCrypt.exe (remember you extracted all the files into a folder on your desktop) you should be presented with a window similar to what is presented below. First click the Select File... button and find the container file that you created. The location and container file name should be displayed just next to the key logo. Next click on a drive letter (i.e. K: or L: or T: etc.) and then click the Mount button, you should be prompted for a password. Type in the password that you used when you created the container file.



Once the container file has been mounted successfully, you will then be able to access the container file as though it was a physical drive connected to the computer. Using My Computer, Computer or Windows Explorer you should see a drive which is 100MB in size (assuming you created a 100MB volume as per the previous instruction).

From here on you can drag and drop, delete and copy files you would like to encrypt into the drive (container file) as if it were a hard disk, USB drive etc. Whilst the container file is mounted, the contents of the container file is decrypted. This means that anyone or anything that has access to your computer could potentially access your confidential files.

Assuming you have completed using the files that were decrypted, you may want to encrypt the files so that an unauthorised party cannot access them. Make sure no files are still copying to the container file (drive). Once you are comfortable that files are not being copied click the Dismount button. You may be prompted to force a dismount in which case you should agree. You can then take your file container and move it from disk to disk or onto a USB stick, or you may simply delete it.



1. What happens to the drive (in My Computer, Computer or Windows Explorer) when it is dismounted?
2. After you copied files into the encrypted file container, did the size of the container change?
   1. What was the reason behind this?
3. If you delete the encrypted file container what will happen to the files inside?

**Part 2: Questions**

1. Eve has an antenna that can pick up Alice's encrypted cell phone conversations. What type of attack is Eve employing?
2. Eve has given a bunch of messages to Alice for her to sign using the RSA signature scheme, which Alice does without looking at the messages and without using a one-way hash function.

These messages are cipher text that Eve constructed to help her figure out Alice's RSA private key. What kind of attack is Eve using here?

1. Eve has bet Bob that she can figure out the AES secret key he shares with Alice if he will simply encrypt 20 messages for Eve using that key.

For some unknown reason, Bob agrees. Eve gives him 20 messages, which he then encrypts and emails back to Eve. What kind of attack is Eve using here?

1. What are the next four numbers in the pseudo-random number generator 3x +2 mod 11, starting from 5?
2. What is 7120 mod 143?
3. What is the plaintext for the following cipher text, which was encrypted using a simple substitution cipher:

CJBT COZ NPON ZJV FTTK TWRTUYTFGT NJ DTN O XJL. Y COZ ZJV CPJVIK DTN O XJL MYUCN.