Trinity Lutheran College

Documentation Encryption Strategies

Introduction

This instruction document is for use by anyone who wishes to save digital files in a secure manner to avoid theft or misuse, by keeping it secret from anyone who you do not authorize. It uses the program called TrueCrypt. TrueCrypt is an encryption program which allows you to encrypt on-the-fly volume.

Programs

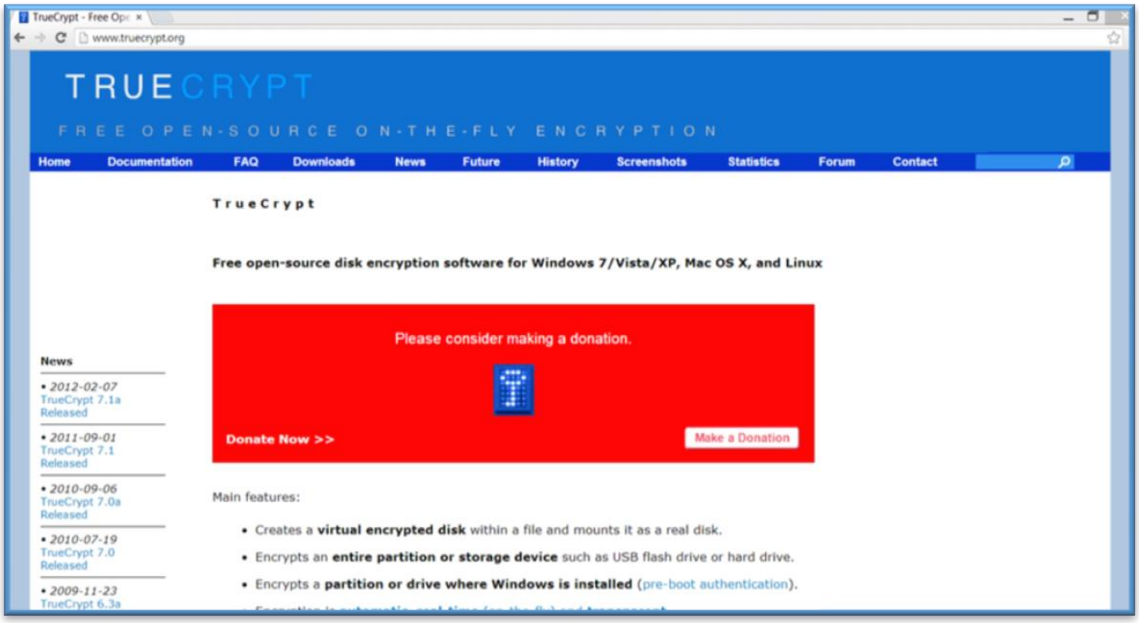
The following instructions use the following programs.

- TrueCrypt

Installing and Using Program

Step 1: Download TrueCrypt

To sign up, all you need to do is download the program. The TrueCrypt program can be found at TrueCrypt.org. It is a free download.



TrueCrypt

Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux

Please consider making a donation.

News

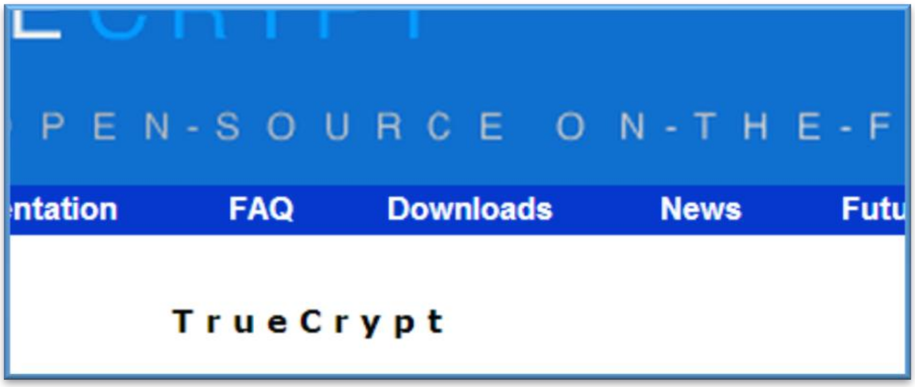
- 2012-02-07 TrueCrypt 7.1a Released
- 2011-09-01 TrueCrypt 7.1 Released
- 2010-09-06 TrueCrypt 7.0a Released
- 2010-07-19 TrueCrypt 7.0 Released
- 2009-11-23 TrueCrypt 6.3a

Main features:

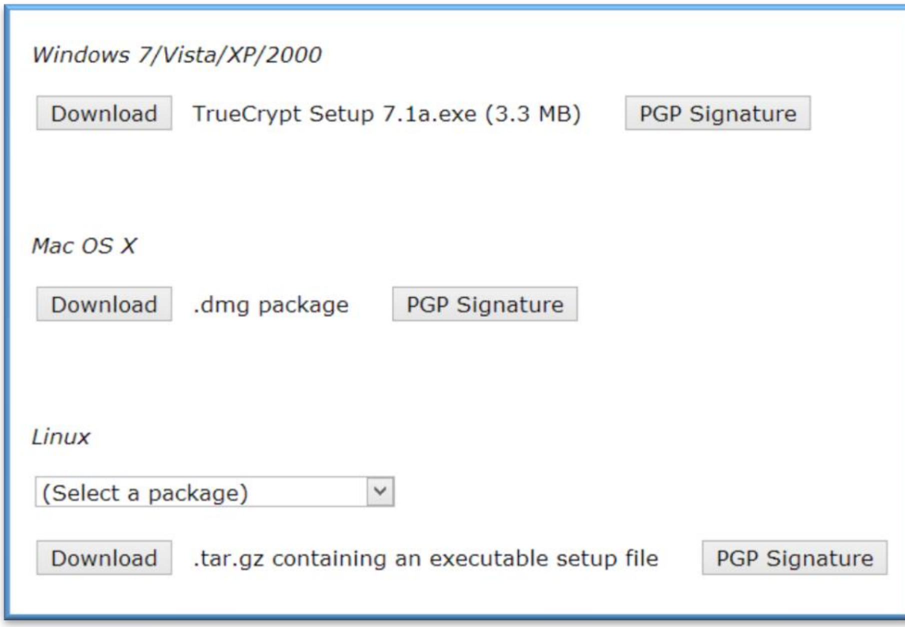
- Creates a **virtual encrypted disk** within a file and mounts it as a real disk.
- Encrypts an **entire partition or storage device** such as USB flash drive or hard drive.
- Encrypts a **partition or drive where Windows is installed** (pre-boot authentication).

Figure 1: TrueCrypt.org Webpage

1. Click on "Downloads" in the blue bar at the top



2. The link will take you to a selection of operating systems. Truecrypt works on both PC and MAC. Choose the option that best matches your computer, and click on download. (Figure 2)



Windows 7/Vista/XP/2000

Download TrueCrypt Setup 7.1a.exe (3.3 MB) PGP Signature

Mac OS X

Download .dmg package PGP Signature

Linux

(Select a package)

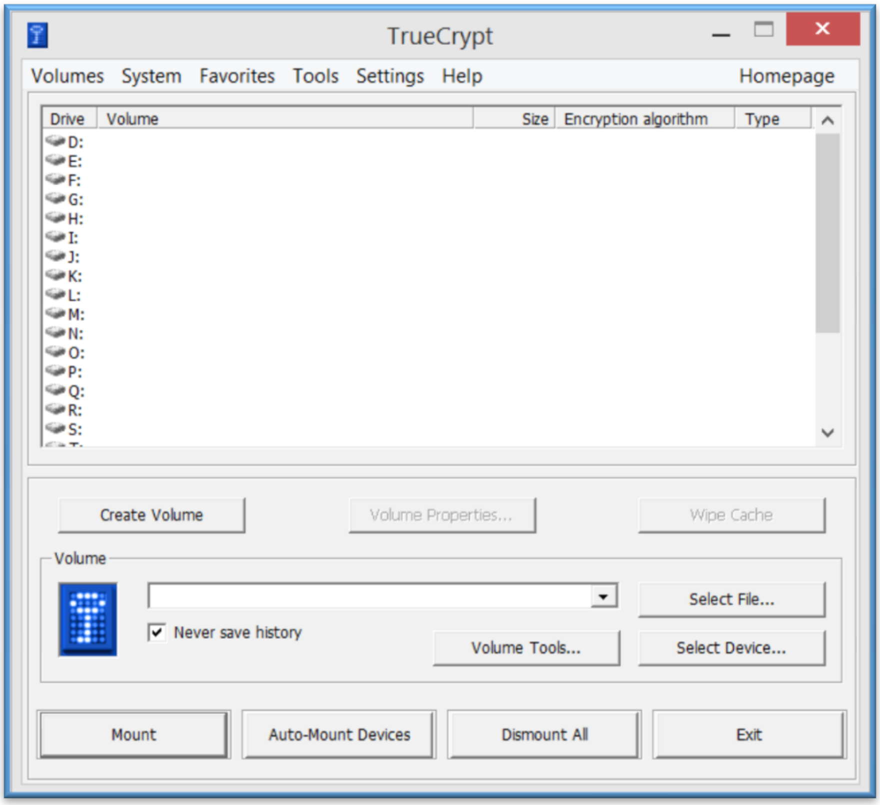
Download .tar.gz containing an executable setup file PGP Signature

Figure 2: Operating System Options

3. Install the program following standard operating system procedures.

Step 2: Creating your first secured file

The first time you use TrueCrypt you will need to create your file.

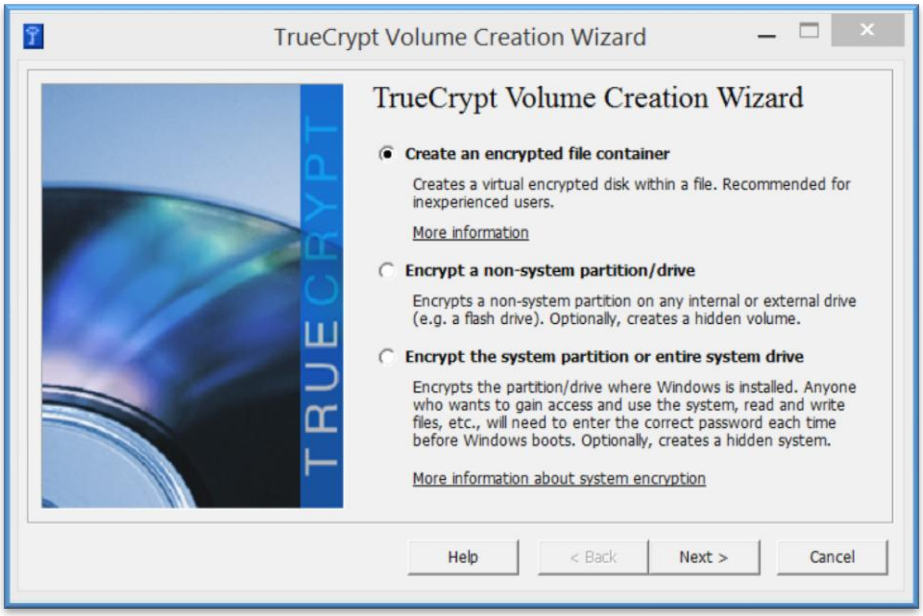


Drive	Volume	Size	Encryption algorithm	Type
D:				
E:				
F:				
G:				
H:				
I:				
J:				
K:				
L:				
M:				
N:				
O:				
P:				
Q:				
R:				
S:				

☑ Never save history

Figure 3: TrueCrypt Opening Page

1. For this example we are going to create a file in “My Documents” and encrypt that.
    a. Click on “Create Volume”.



TrueCrypt Volume Creation Wizard

● Create an encrypted file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

○ Encrypt a non-system partition/drive

Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

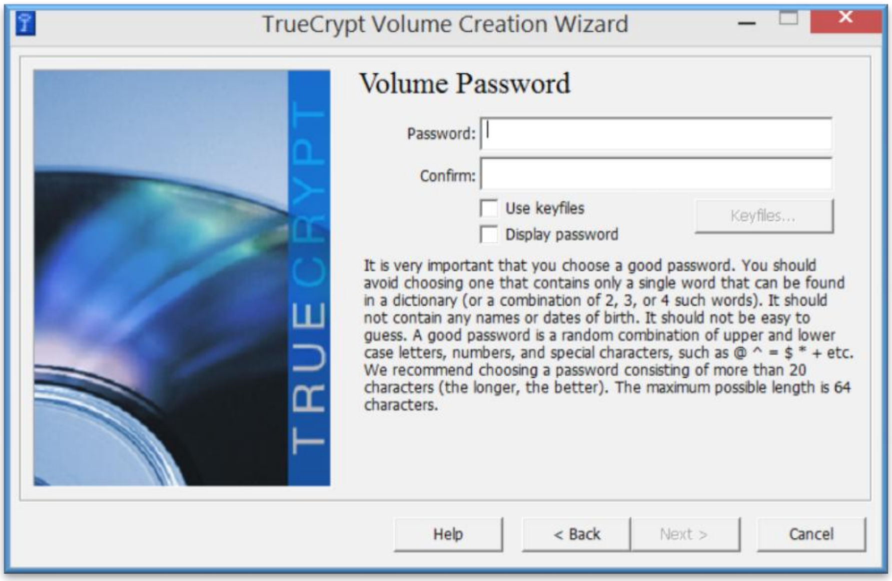
○ Encrypt the system partition or entire system drive

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

More information about system encryption

Figure 4: Volume Creation Wizard

2. Select ‘Create an encrypted file container’ and click ‘Next’.
3. Select ‘Standard TrueCrypt volume’ and click ‘Next’.
4. Choose a location on your computer to store the file. “My Documents” is a fine location. Give the file name. For this example SecureFile will be used.
5. Leave the default options for ‘Encryption Options’.
6. Next it asks for the size of the volume. For this example I will use 40 MB. Type in 40 and make sure that MB is selected, and press ‘Next’.



Volume Password

Password:

Confirm:

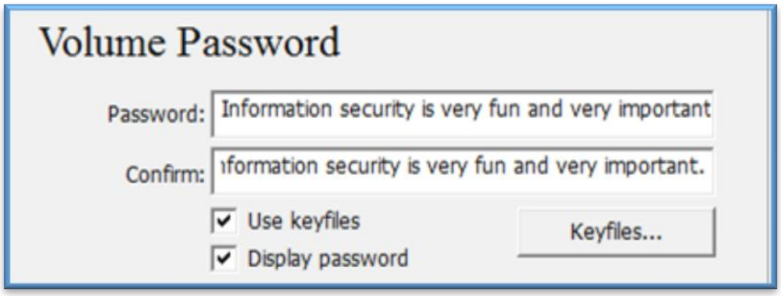
□ Use keyfiles

□ Display password

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.

7. Now for the password!

a. Make sure the passphrase is very long. It can be up to 64 characters in length. Go ahead and select “Use Keyfiles” as well.
b. This example uses:
    i. Information security is very fun and very important.
    ii.



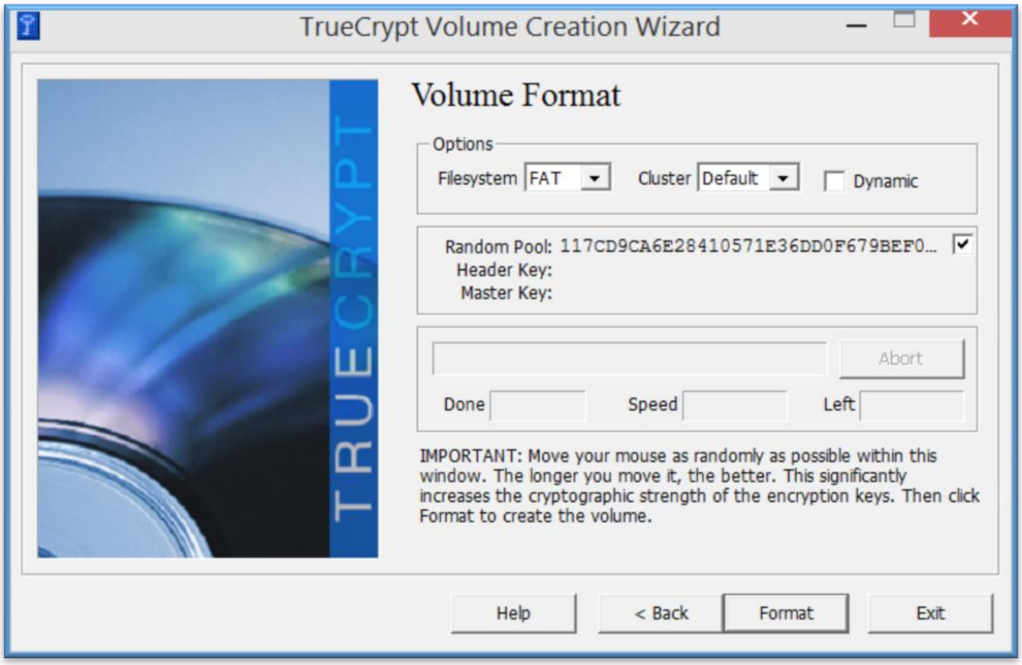
Volume Password

Password: Information security is very fun and very important

Confirm: ıformation security is very fun and very important.

☑ Use keyfiles

☑ Display password



TrueCrypt Volume Creation Wizard

Volume Format

Options

Filesystem FAT Cluster Default □ Dynamic

Random Pool: 117CD9CA6E28410571E36DD0F679BEF0... ☑
Header Key:
Master Key:

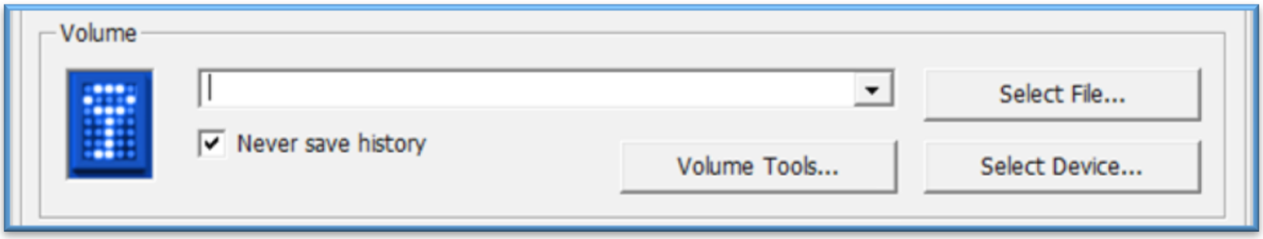
Done Speed Left

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

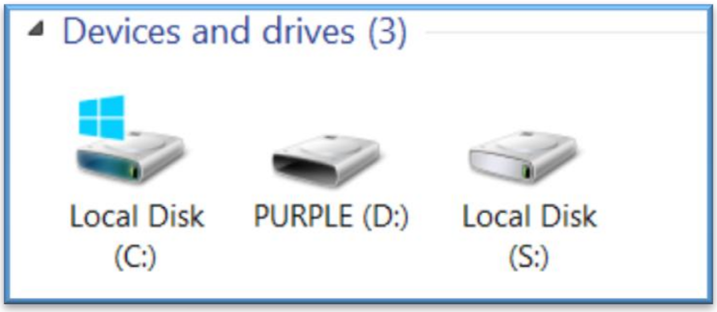
c. Press Format.
d. You should be taken to a confirmation page.
e. Congratulations! You now have a secure file!

Step 3: Mount the file.

1. Back the main program screen, open your file by clicking “Select File…” and finding the file in the location where it was saved.



2. Highlight the drive letter above where you want the file saved and click “Mount”.
3. You will be prompted for the password. Type the password exactly as it was created. No not select Keyfile at this time. If it was correct your file will be mounted to a drive.
4. Press Exit.



5. Your file is created! In this case it is the S-Drive.
6. Use it just as you would any other drive.

Step 4: Closing the TrueCrypt session.

1. When you finished with the files, open the TrueCrypt program and select ‘Dismount All’. This will secure the file from attack.

Limits To TrueCrypt

Storage limits

On Windows XP/2003, TrueCrypt does not support encrypting an entire system drive that contains extended (logical) partitions. You can encrypt an entire system drive provided that it contains only primary partitions.

What does a novice computer user need to understand to use it?

If you are a novice computer user you will want to have a basic understanding of what encrypting is.

Known Issues

The company Elcomsoft has provided a software tool that can decrypt true-crypt containers. When the containers are accessed on the computer the decryption passwords are kept in the computer's operating memory. All the software needs is a memory dump from the computer, this can be achieved by either a firewall attack or using forensic tools. The software then searches the memory dump for the encryption and decryption keys. The best way to avoid this kind of security breach is to make sure, when the encrypted files are finished being written on the containers are demounted and the computer is shut down. The keys can only be found in the memory dump if the containers are mounted at the time of attack.

The articles referenced for this are:

- http://news.techworld.com/security/3418189/bitlocker-pgp-and-truecrypt-encryption-weakened-by-new-attack-tool/
- http://www.informationweek.com/security/encryption/forensic-tool-cracks-bitlocker-pgp-truec/240145127

Encryption Basics

- Encryption is the conversion of data into a form called a ciphertext ,that can not be easily understood by the unauthorized people.
- Computer Encryption is based on the science of cryptography which has been in used as long humans have wanted to keep information secret.
- Decryption is the process of converting data back to its original form ,so it can be understood
  - The biggest users of cryptography where the governments and military Encryption /Decryption is old as the art of communication. In wartime, a cipher, often and incorrectly called a code, can be employed to keep the enemy from obtaining the contents of the transmission, technically a code is a means of

representing a signal without the intent of keeping it a secret examples Morse code and AscII .

- Simple ciphers include the substitution of letters for numbers , the rotation of letters in the alphabet, and scrambling of voice signals by inventing sideband frequencies More complex ciphers work according to sophisticated computer algorithms.
- Algorithms are a program for the means of a small procedure that solves a recurrent problem.
    - The Greek historian ,Plutarch wrote Spartan generals who sent and received sensitive messages using a scytale a thin cylinder made out of wood the general would wrap a piece of parchment from the cylinder around the scytale and write the message along the length ,when someone would remove the paper from the cylinder ,the writing appeared to be jumbled of nonsense but if the other general receiving the parchment has a scytale of similar size he could wrap the paper around it and easily read the intended message.
    - The Greeks were the first to use deciphers they could decode any message the other sent to make other more difficult to decipher, they could arrange the letters inside the grid in any combination most forms of cryptography in use these days rely on computers.
- Also deciphers are better known today as algorithms which guides for encryption they provide a way to craft the message and gives certain range of possible combination.
- To make computer do anything you have to write a code or computer program you have to tell the computer or computer program you have to tell the computer step by step exactly what you want it to do. The computer executes the command, following each step mechanically, to accomplish their goal that is a computer algorithms. The algorithm is the technique used to get the job done.
- **How do the key files work?**

Conclusion

We believe that TrueCrypt will solve your security needs.

Make sure to save your work and demount the container before shutting down every time.