CompTIA Security+® Lab Series

Lab 16: Importance of Data Security - Securing Data Using Encryption Software

CompTIA Security+® Domain 4 - Application, Data and Host Security

Objective 4.3: Explain the importance of data security

Document Version: 2013-08-02

Organization: Moraine Valley Community College
Author: Jesse Varsalone

The original works of this document were funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) at Moraine Valley Community College (MVCC).

Contents

Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

During this lab, students will install and use TrueCrypt. TrueCrypt is a type of disk encryption software for use with the Windows, Mac, and Linux operating systems.

This lab includes the following tasks:

1 - Installing TrueCrypt
2 - Creating a TrueCrypt Container
3 - Opening and Viewing Data within a TrueCrypt Container

Objective: Explain the importance of data security

Data needs to be protected by businesses and government agencies. When data theft occurs, companies and organizations can lose money, credibility and customers. There have been several high profile cases mentioned in the media where a laptop was lost or stolen and a large number of individuals had their social security numbers compromised. Using disk encryption software can help protect sensitive data on desktops, laptops and mobile devices.

TrueCrypt – TrueCrypt is a free, open source, disk encryption software for use with the Windows, Mac, and Linux operating systems. TrueCrypt can encrypt the operating system drive, a data drive, or a file container within a partition.

BitLocker – Included with the Enterprise and Ultimate versions of Windows Vista and Windows 7, BitLocker offers full volume Encryption. BitLocker can be utilized with either a Trusted Platform Module (TPM) chip or a USB key at startup.

FileVault 2 – Starting with Mac OS X 7 (Lion), FileVault version 2 was included with the operating system. It will encrypt the full disk, not just the user's home folder.

FileVault – Included with Mac OS X version 3 (Panther) through version 6 (Snow Leopard). FileVault only encrypts the user's home folder when activated for the user.

DMCrypt –Used to encrypt devices on the Linux operating system.

Pod Topology

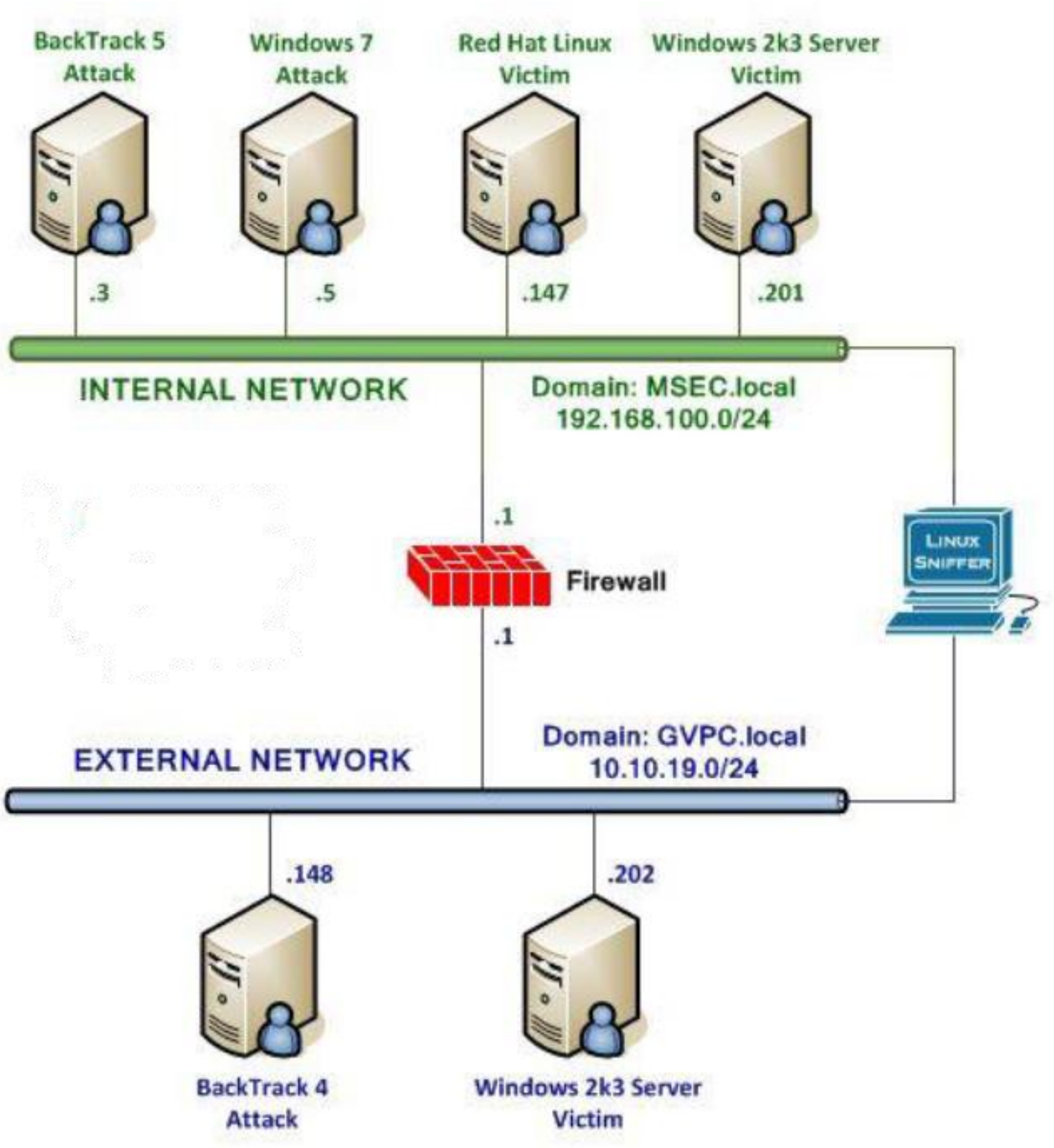


Figure 1: Topology

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

Log in to the following virtual machines before starting the tasks in this lab:

Windows 7 Internal Attack Machine	192.168.100.5
Windows 7 student password	password

Windows 7 Internal Attack Login:

1. Click on the Windows 7 Internal Attack icon on the topology.
2. Enter the username, **student** (verify the username with your instructor).
3. Type in the password, **password** and hit enter to log in (verify the password with your instructor).

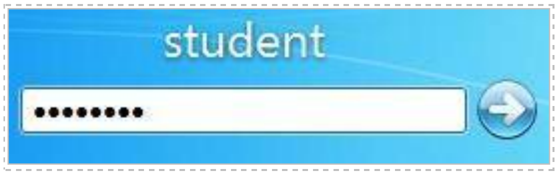


Figure 2: Windows 7 login

If prompted to Set Network Location, select "Work network" and then click "Close". Click to reboot the Windows 7 machine when prompted.

1 Installing TrueCrypt

TrueCrypt is free software that works on Windows, Mac OS X, and Linux operating systems. It can be downloaded from http://www.truecrypt.org/. After installing TrueCrypt, a user can:

- Mount TrueCrypt Volumes
- Create TrueCrypt Volumes
- Encrypt their Operating System Drive
- Encrypt a Data Drive

1.1 TrueCrypt Installation

To install TrueCrypt on your system, perform the following tasks:

1. On the Windows 7 system, double-click on the **TrueCrypt Setup 7.1a** file on your desktop.

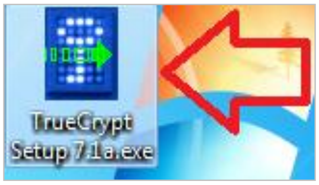
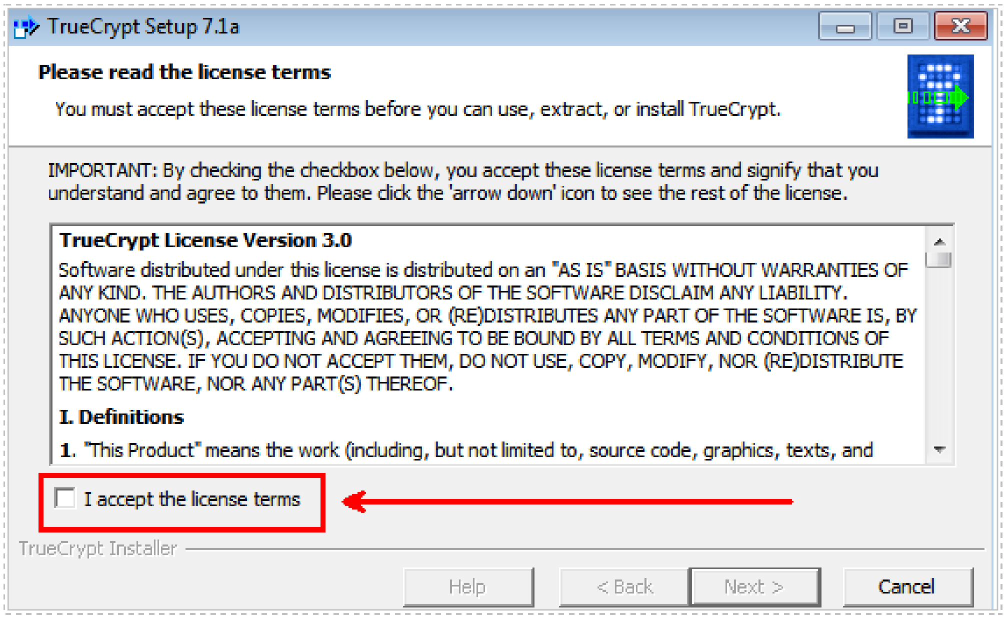


Figure 3: The TrueCrypt Installation Package

2. Click **I accept the license terms** and click **Next**.



Please read the license terms

You must accept these license terms before you can use, extract, or install TrueCrypt.

IMPORTANT: By checking the checkbox below, you accept these license terms and signify that you understand and agree to them. Please click the 'arrow down' icon to see the rest of the license.

TrueCrypt License Version 3.0

Software distributed under this license is distributed on an "AS IS" BASIS WITHOUT WARRANTIES OF ANY KIND. THE AUTHORS AND DISTRIBUTORS OF THE SOFTWARE DISCLAIM ANY LIABILITY. ANYONE WHO USES, COPIES, MODIFIES, OR (RE)DISTRIBUTES ANY PART OF THE SOFTWARE IS, BY SUCH ACTION(S), ACCEPTING AND AGREEING TO BE BOUND BY ALL TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT ACCEPT THEM, DO NOT USE, COPY, MODIFY, NOR (RE)DISTRIBUTE THE SOFTWARE, NOR ANY PART(S) THEREOF.

I. Definitions

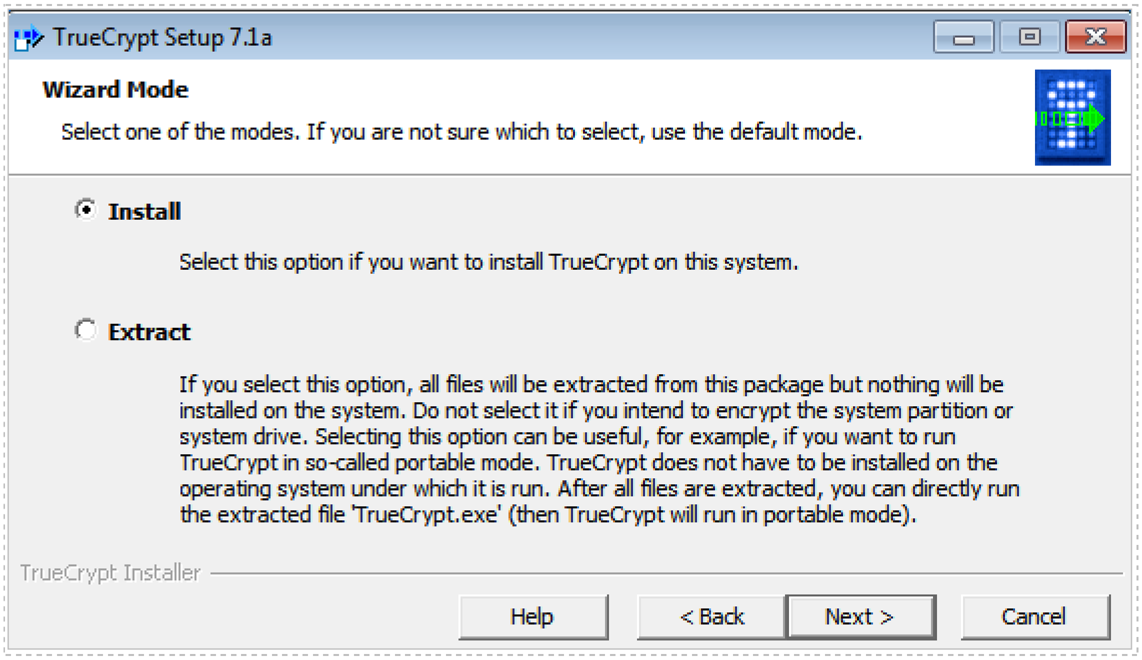
1. "This Product" means the work (including, but not limited to, source code, graphics, texts, and

☐ I accept the license terms

Figure 4: Accepting the License Agreement

You can either install TrueCrypt or extract the files and run the executable. This would be convenient if the user wanted to use the program without installing it.

3. Select **Install** to install TrueCrypt and click the **Next** button.



Wizard Mode

Select one of the modes. If you are not sure which to select, use the default mode.

● **Install**

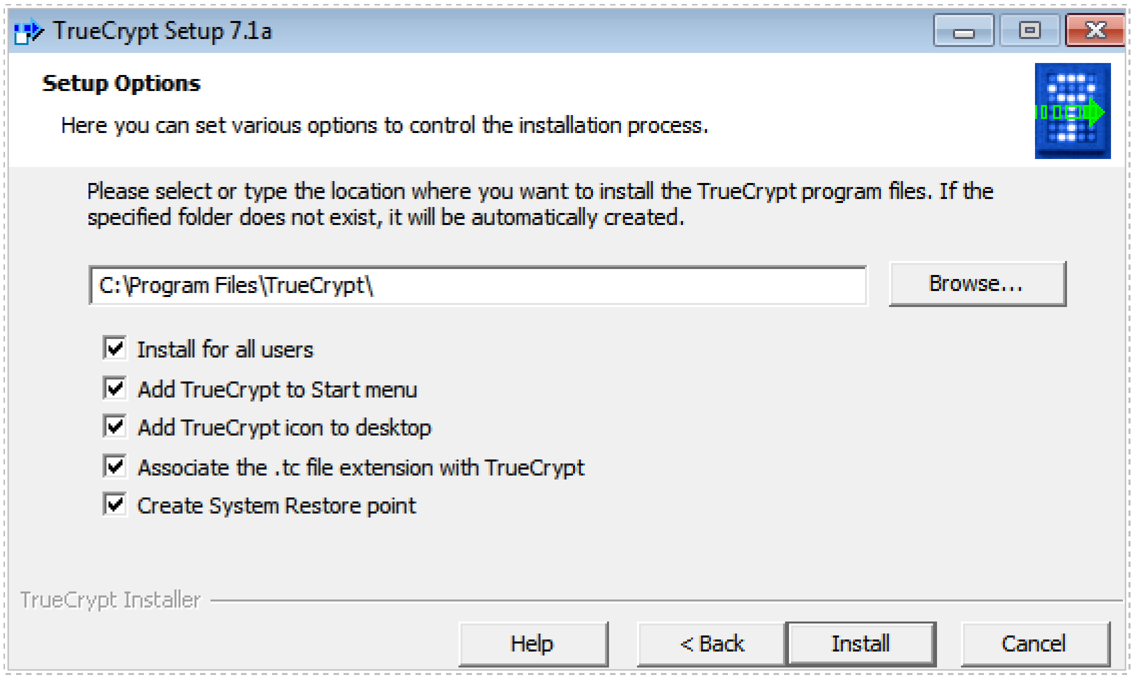
Select this option if you want to install TrueCrypt on this system.

○ **Extract**

If you select this option, all files will be extracted from this package but nothing will be installed on the system. Do not select it if you intend to encrypt the system partition or system drive. Selecting this option can be useful, for example, if you want to run TrueCrypt in so-called portable mode. TrueCrypt does not have to be installed on the operating system under which it is run. After all files are extracted, you can directly run the extracted file 'TrueCrypt.exe' (then TrueCrypt will run in portable mode).

Figure 5: Installing TrueCrypt to the Hard Disk

4. Accept the default installation path and click the **Install** button.



Setup Options

Here you can set various options to control the installation process.

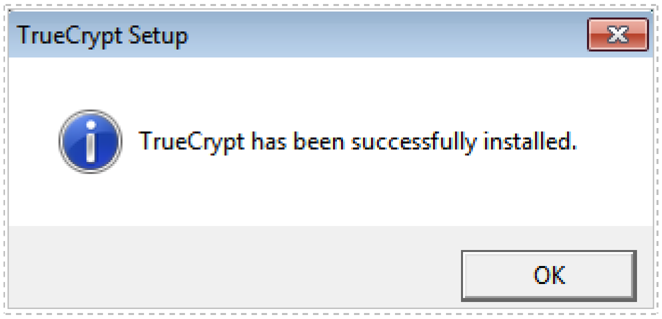
Please select or type the location where you want to install the TrueCrypt program files. If the specified folder does not exist, it will be automatically created.

C:\Program Files\TrueCrypt\

☑ Install for all users
☑ Add TrueCrypt to Start menu
☑ Add TrueCrypt icon to desktop
☑ Associate the .tc file extension with TrueCrypt
☑ Create System Restore point

Figure 6: Accepting the Default Installation Path

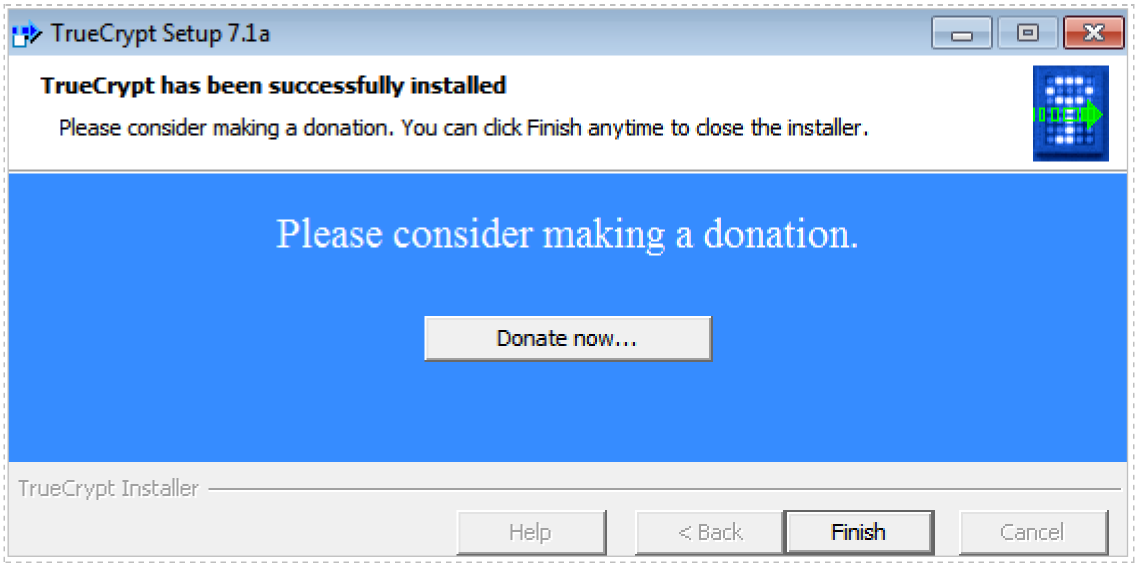
5. You should receive a message indicating *TrueCrypt was successfully installed*.



TrueCrypt has been successfully installed.

Figure 7: TrueCrypt Installed Successfully

6. Click **Finish** to close the installer.



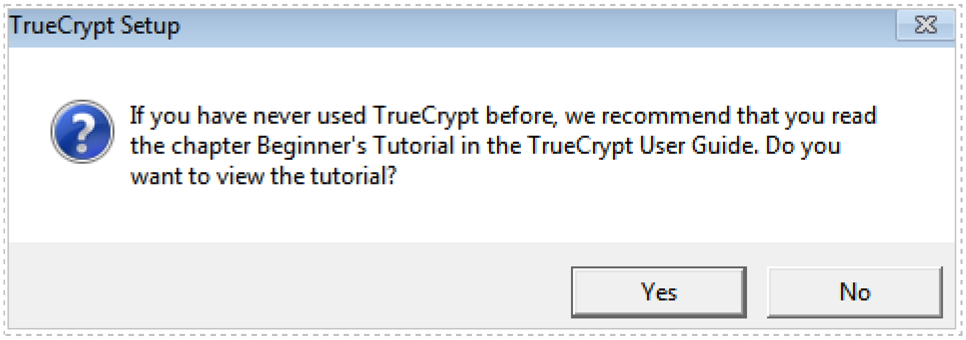
TrueCrypt has been successfully installed

Please consider making a donation. You can click Finish anytime to close the installer.

Please consider making a donation.

Figure 8: Click Finish to Close the Installer

7. Click **No** to bypass the tutorial. If you choose to view the tutorial, you would need a PDF viewer in order to read the file.



If you have never used TrueCrypt before, we recommend that you read the chapter Beginner's Tutorial in the TrueCrypt User Guide. Do you want to view the tutorial?

Figure 9: View Tutorial

You will now be at the TrueCrypt screen where volumes can be created and mounted. Notice the TrueCrypt icon in the bottom right hand corner of the screen, which indicates that TrueCrypt is in use on the system.

If TrueCrypt does not open after installation, click on the TrueCrypt shortcut to display the TrueCrypt interface shown in the figure below.

8. Click **Exit** to leave the TrueCrypt program.

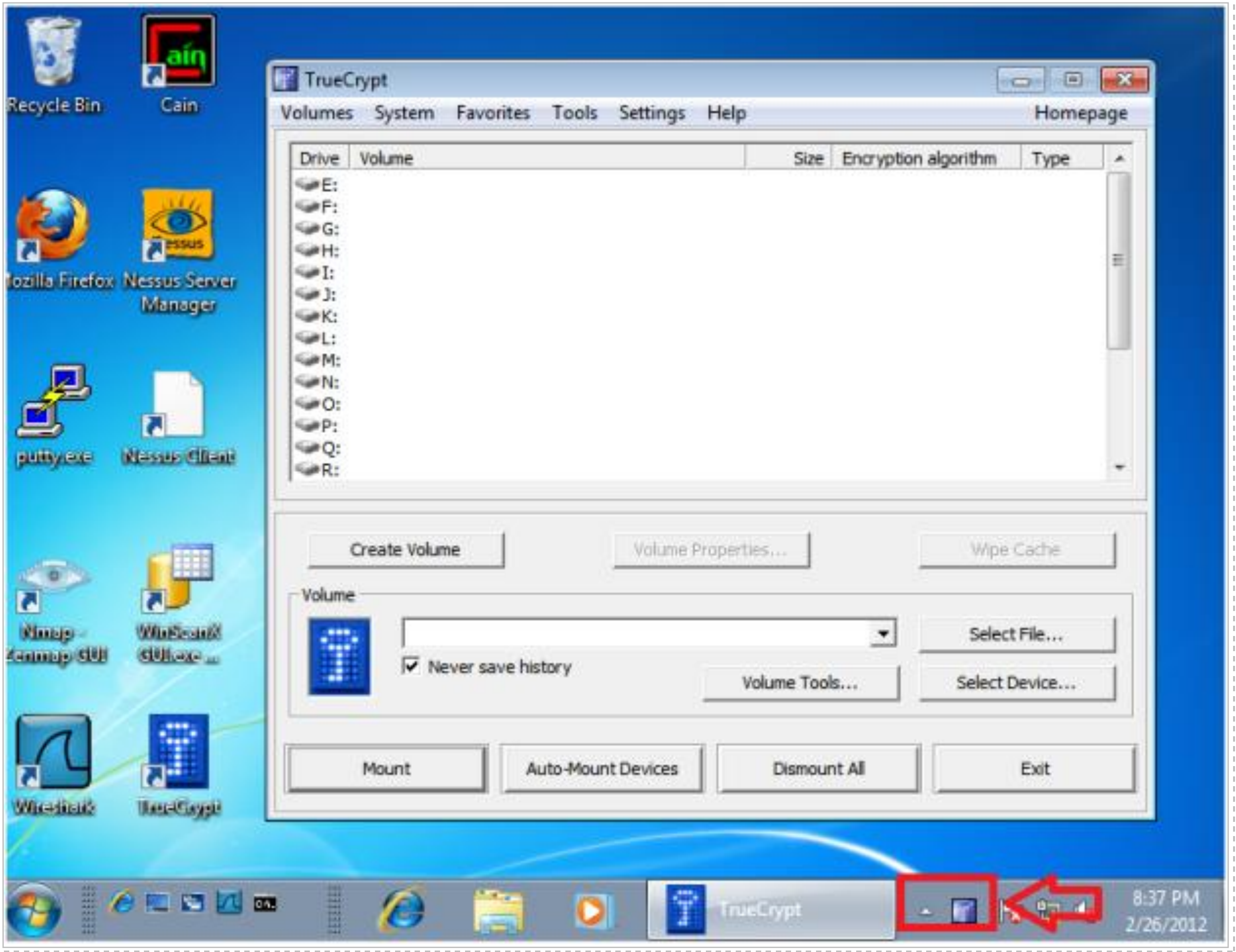


Figure 10: TrueCrypt Icon in Right Corner of Taskbar

1.2 Conclusion

There are many different disk encryption software packages that can be used to protect your data. Microsoft offers BitLocker, but it only works with certain higher end editions of their operating system, such as Enterprise and Ultimate. If you are a Mac user, you can use FileVault. However, FileVault 1 only functions on Mac OS X, and it only encrypts the user’s home folder. TrueCrypt is free to use and can be used on Windows, Mac, and Linux operating systems. TrueCrypt can encrypt both volumes and containers.

1.3 Discussion Questions

1. Is it necessary to install TrueCrypt in order to use it?
2. On what operating systems can you use TrueCrypt?
3. How can you tell if TrueCrypt is in use?
4. Can you encrypt your operating system drive with TrueCrypt?

2 Creating a TrueCrypt Container

In order to store data in a protected area, a TrueCrypt container must be created. You can create the container using a blank text file.

2.1 Creating a Container

1. Right-click on the Desktop and select **New**, then select **Text Document**.

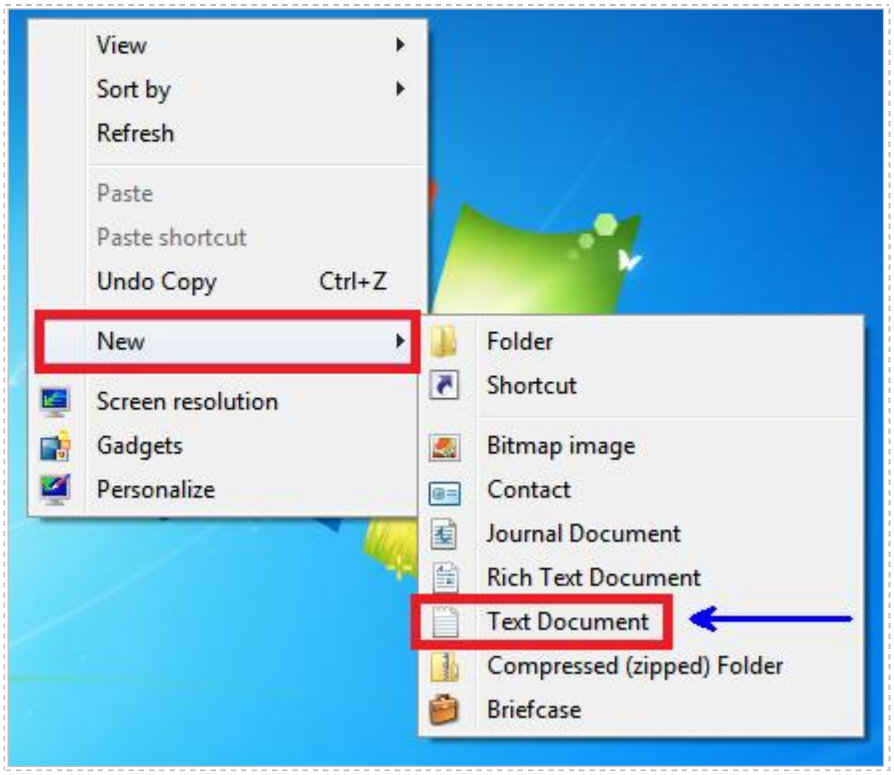


Figure 11: Creating a New Text Document

2. Name the text document **securityplus.txt**. Use a blank document for a TrueCrypt container because anything in the text file will be overwritten.

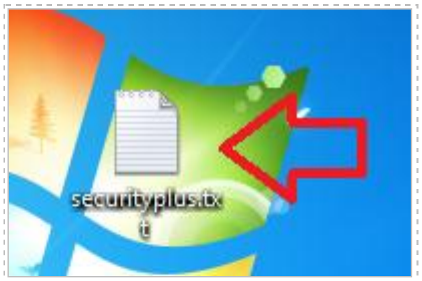
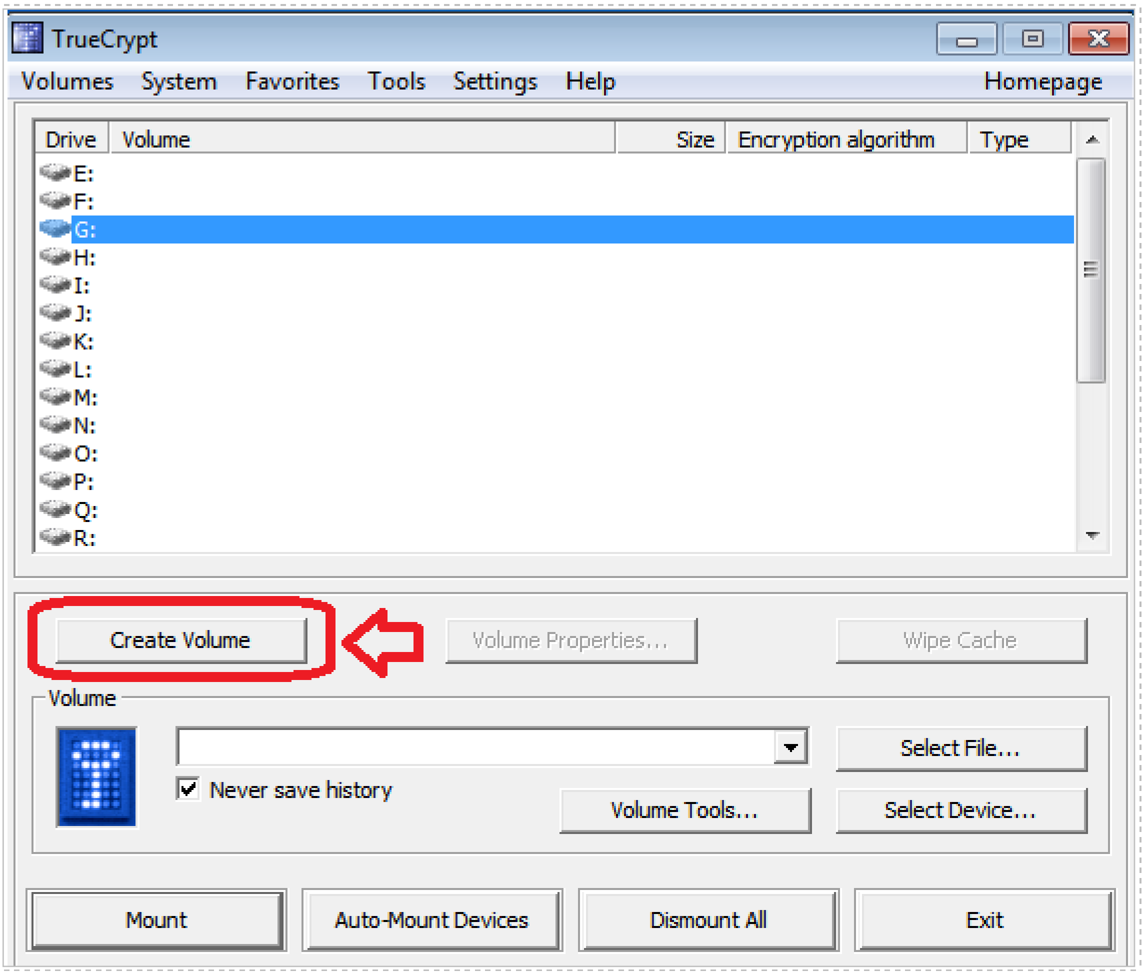


Figure 12: The Text File that will be the TrueCrypt Container

3. Double-click on the shortcut **TrueCrypt** icon on your desktop. Click **Create Volume**.



☑ Never save history

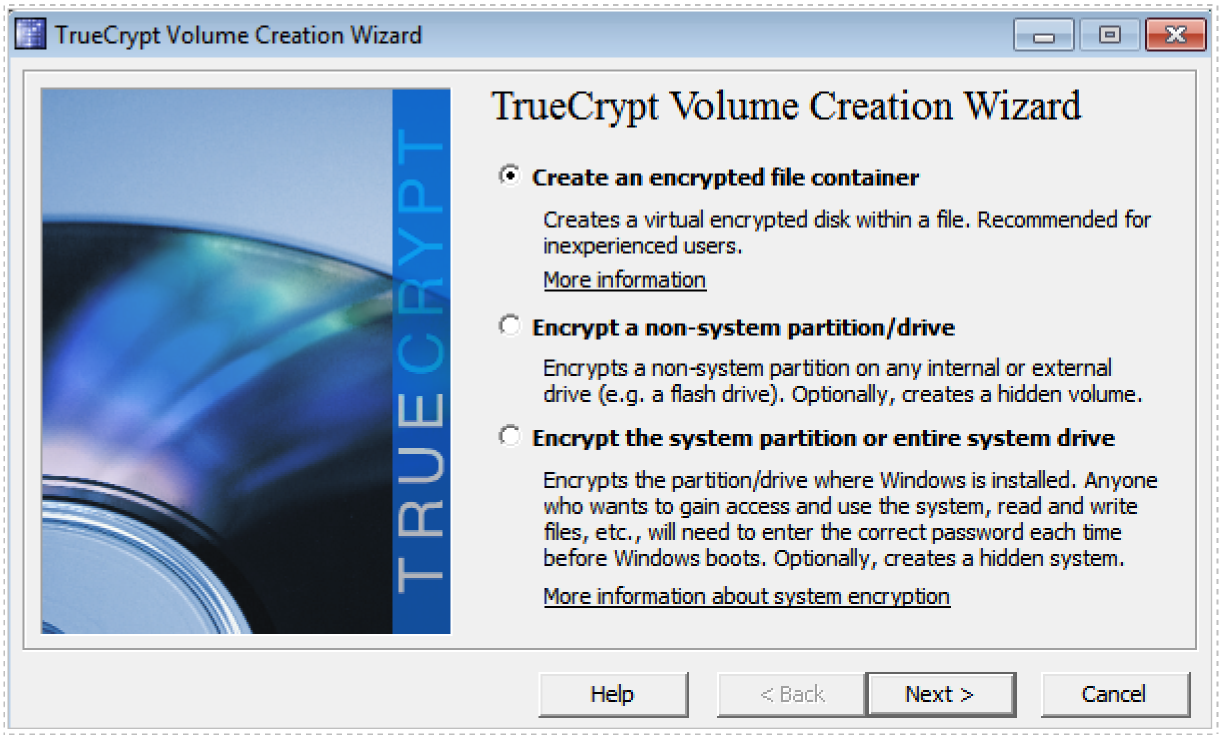
Figure 13: The Volume Creation Process in TrueCrypt

With TrueCrypt, you can:

- Create an encrypted file container
- Encrypt a non-system partition/drive
- Encrypt the system partition or entire system drive

If you encrypt the system partition, you will need to burn a recovery CD.

4. Select Create **an encrypted file container** and click **Next**.



TrueCrypt Volume Creation Wizard

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.

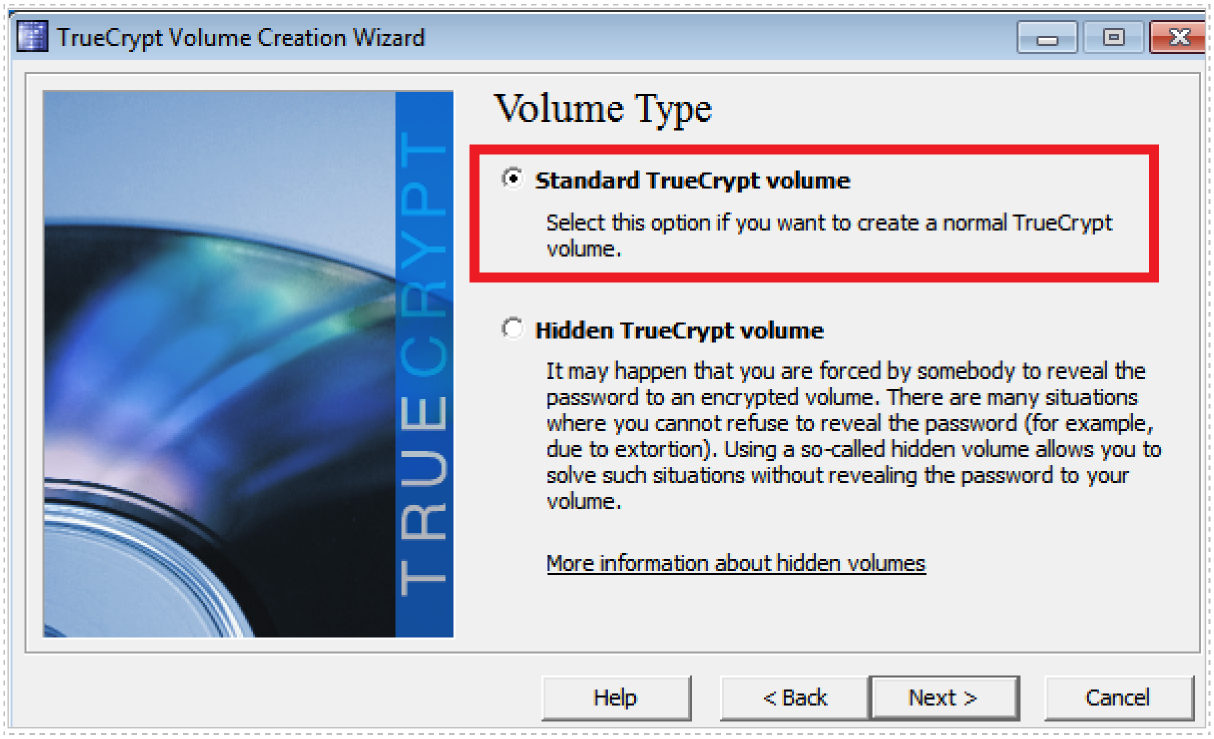
○ **Encrypt the system partition or entire system drive**

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 14: Create an encrypted file container

5. Select **Standard TrueCrypt volume** and click **Next**.



TrueCrypt Volume Creation Wizard

Volume Type

● **Standard TrueCrypt volume**

Select this option if you want to create a normal TrueCrypt volume.

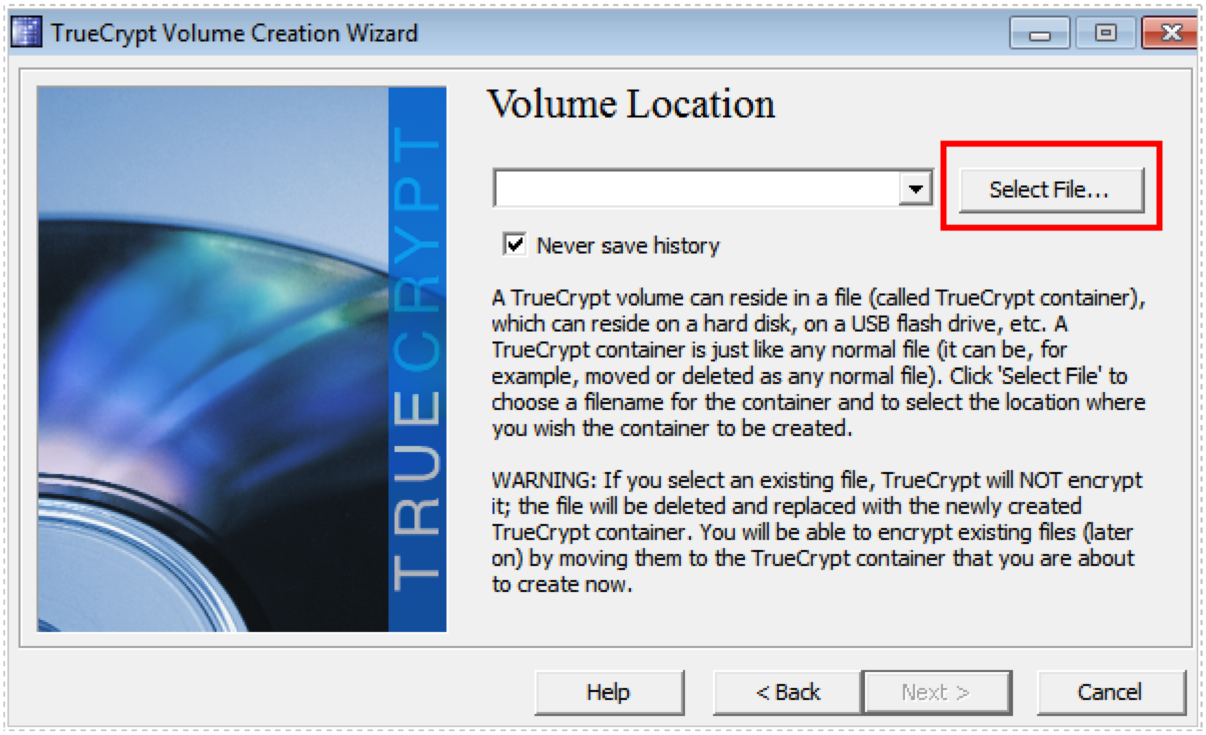
○ **Hidden TrueCrypt volume**

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

More information about hidden volumes

Figure 15: Standard TrueCrypt volume

6. Click the **Select File** button at the Volume Location screen.



Volume Location

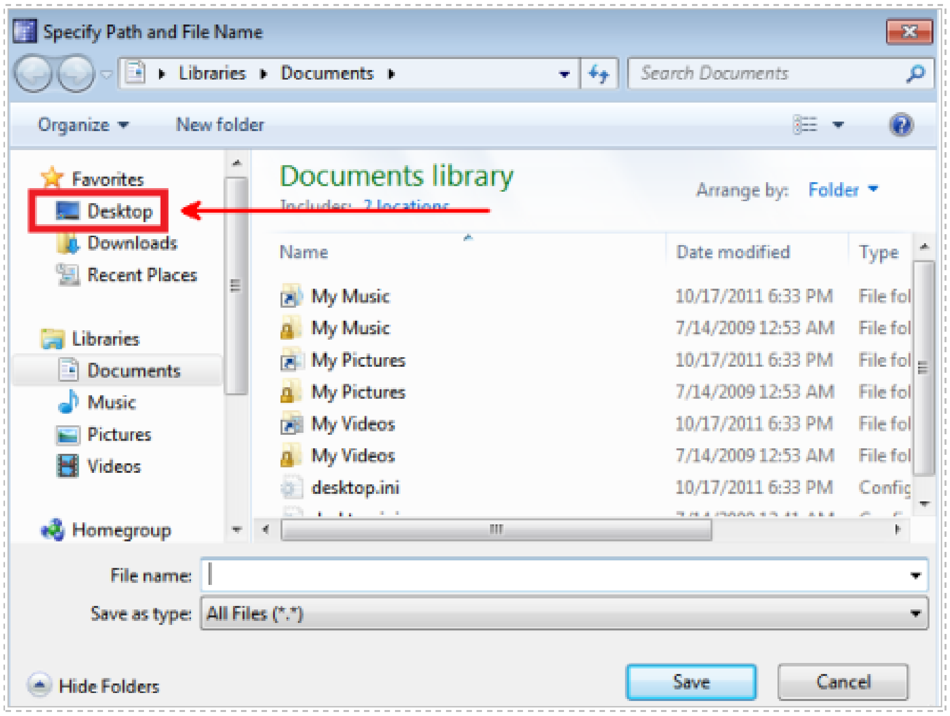
☑ Never save history

A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

Figure 16: Volume Location Screen

7. Click the **Desktop** link on the Left side of Windows Explorer screen.



Documents library

Includes: 2 locations

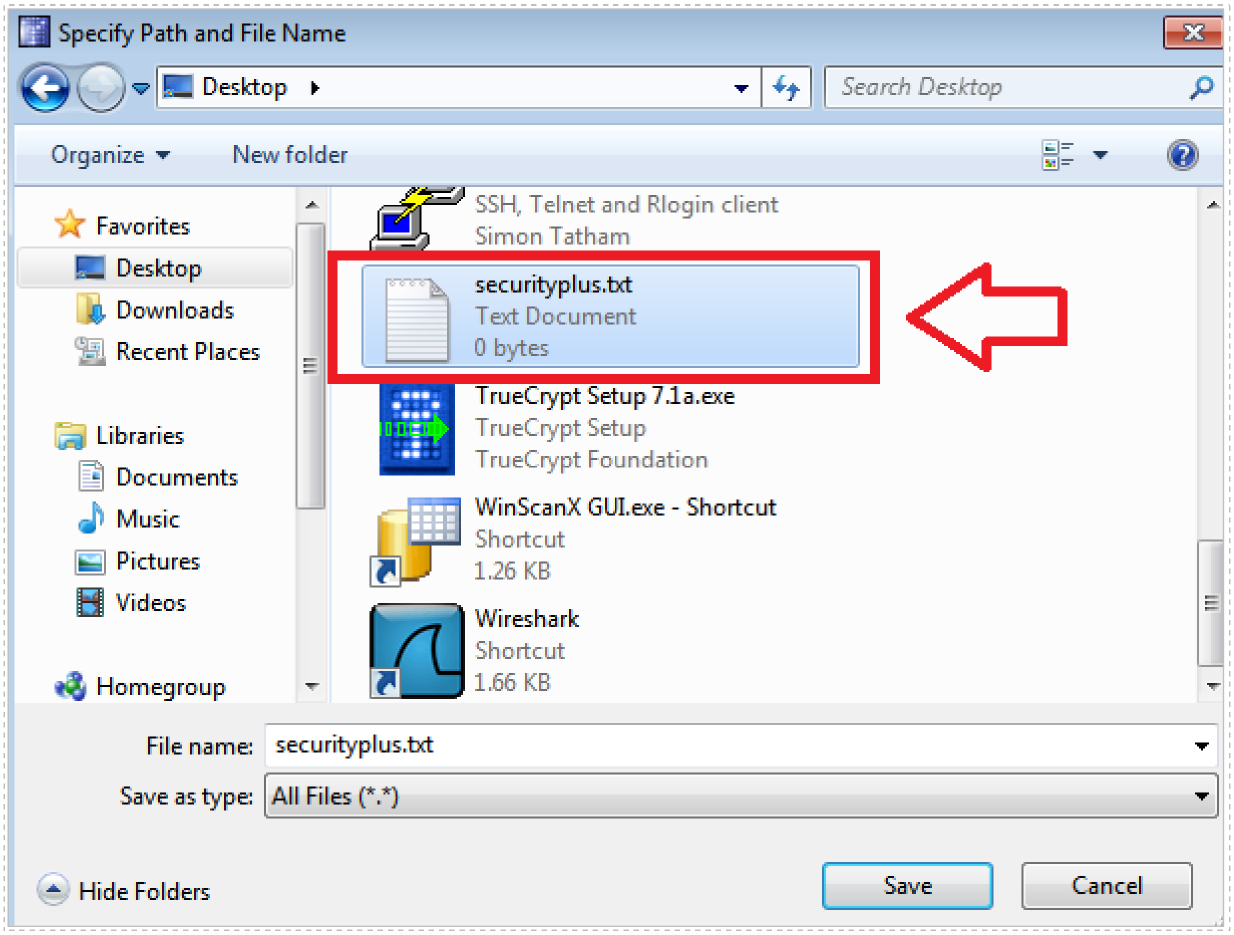
Name	Date modified	Type
My Music	10/17/2011 6:33 PM	File fol
My Music	7/14/2009 12:53 AM	File fol
My Pictures	10/17/2011 6:33 PM	File fol
My Pictures	7/14/2009 12:53 AM	File fol
My Videos	10/17/2011 6:33 PM	File fol
My Videos	7/14/2009 12:53 AM	File fol
desktop.ini	10/17/2011 6:33 PM	Config

File name:

Save as type: All Files (*.*)

Figure 17: Navigating to the Text File Location

8. Double-click on the **securityplus.txt** file on the Desktop.



File name: securityplus.txt

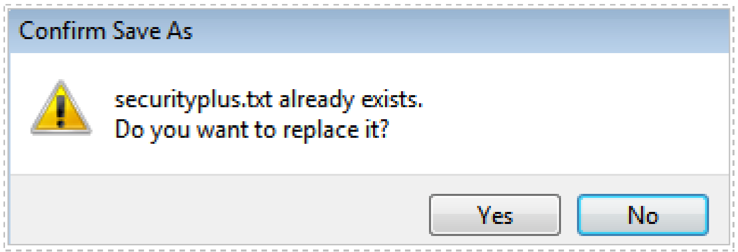
Save as type: All Files (*.*)

Figure 18: Selecting the Text File

At this point, you will be asked if you want to replace the text file.

It is important to select the blank text file you recently created, in order to avoid inadvertently deleting some other text file, which could contain important information. Once **Yes** it clicked, information in the text file is destroyed.

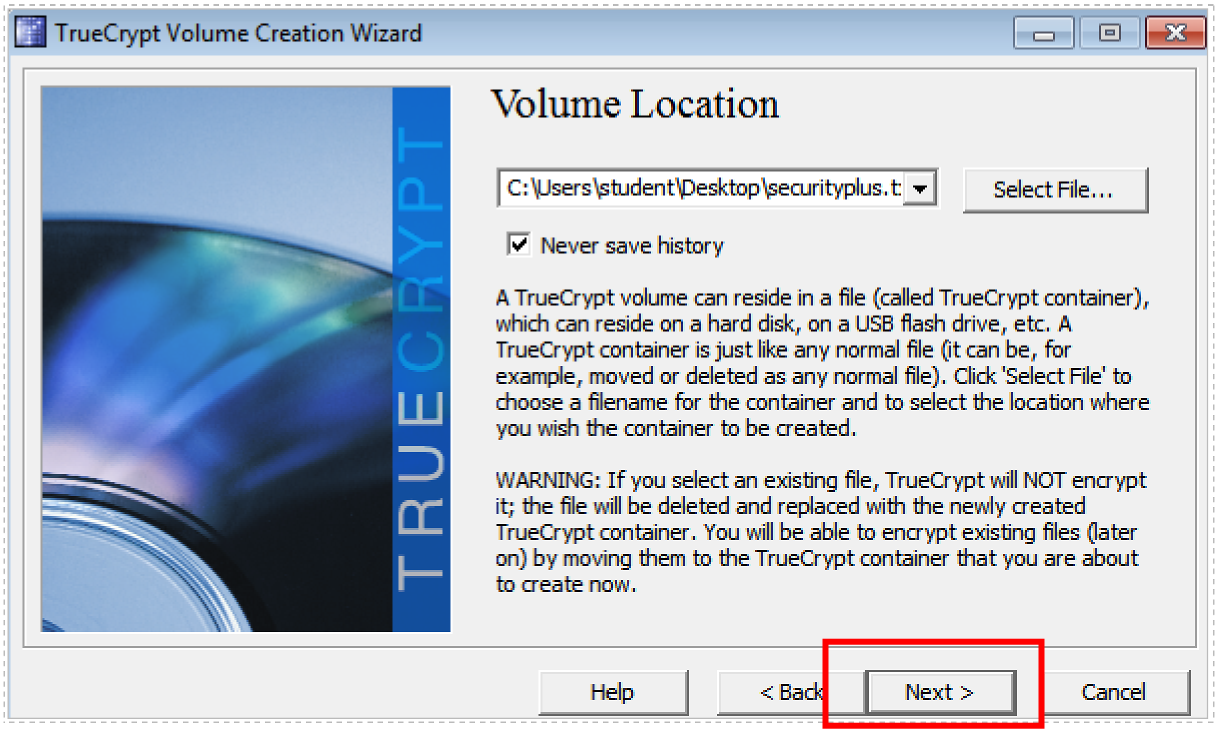
9. Click **Yes** to replace the text file



securityplus.txt already exists.
Do you want to replace it?

Figure 19: Click Yes to Replace the Text File

10. Click **Next** at the Volume Location Screen after **securityplus.txt** is selected.



Volume Location

C:\Users\student\Desktop\securityplus.t

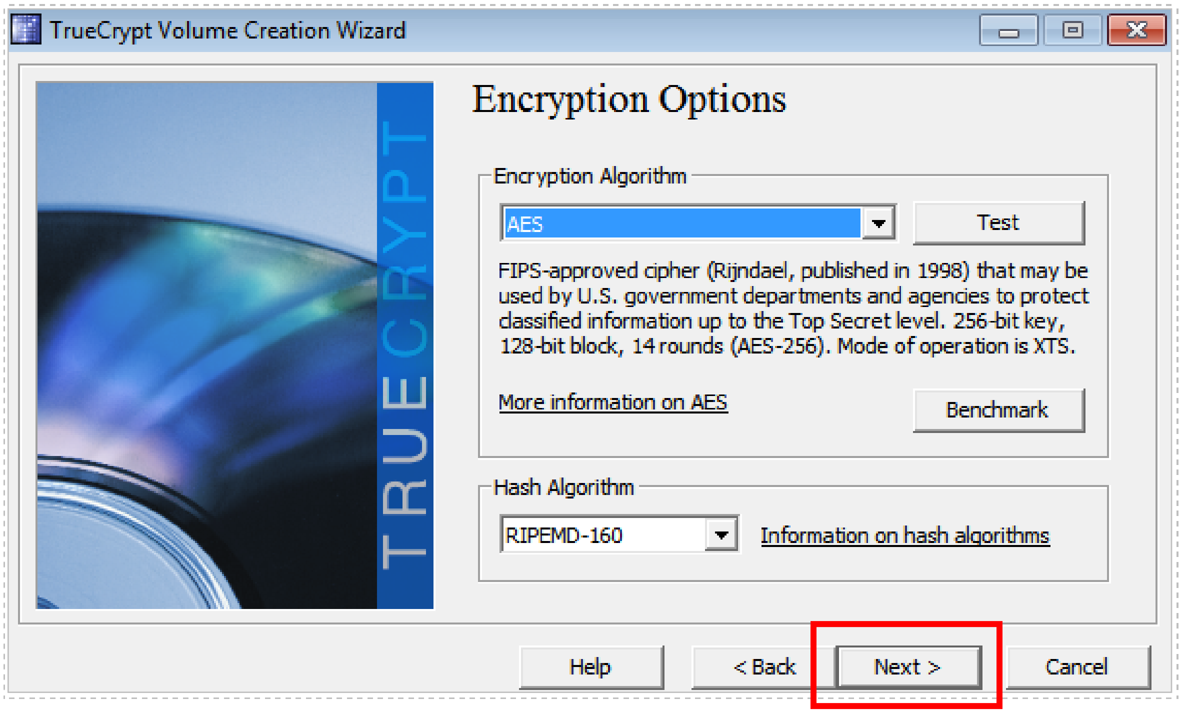
☑ Never save history

A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

Figure 20: Volume Location Screen

11. At the Encryption Options, accept the default Encryption Algorithm of **AES**; however, others can also be selected. Click the **Next** button.



Encryption Options

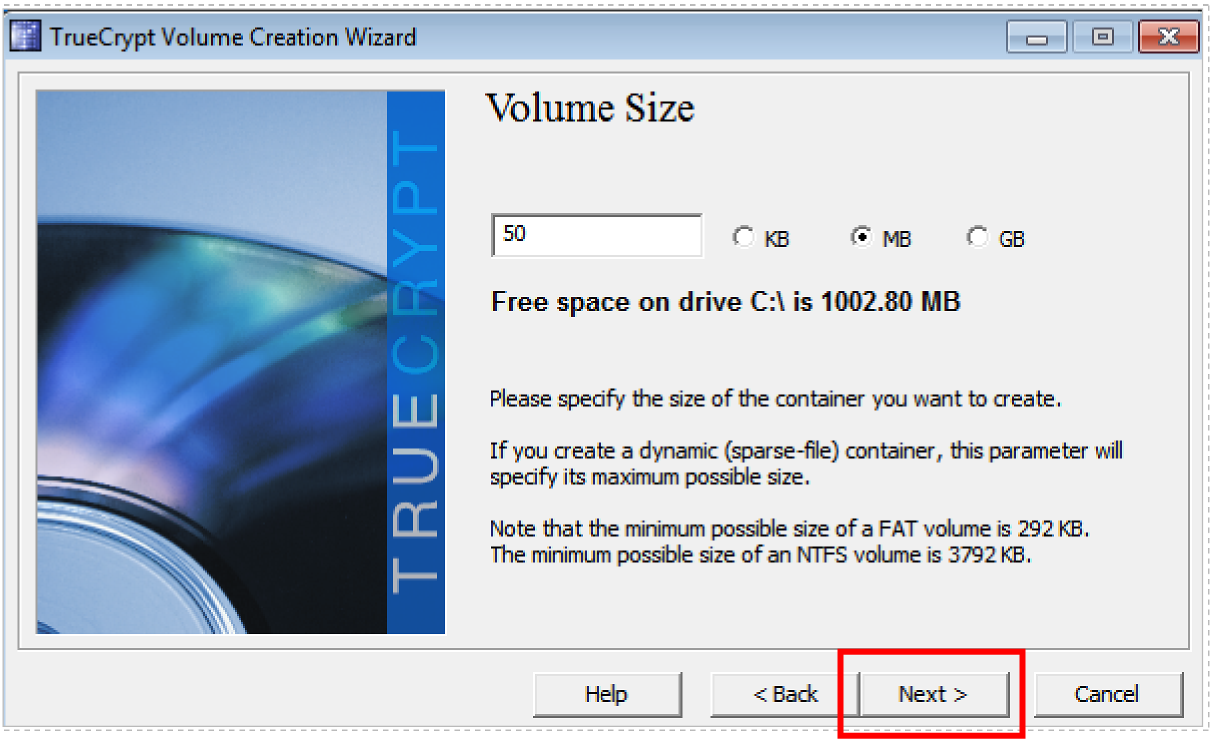
Encryption Algorithm: AES

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

Hash Algorithm: RIPEMD-160

Figure 21: Encryption Options

12. For the Volume Size, type **50**. Verify **MB** is selected and click **Next**.



Volume Size

50 ○ KB ● MB ○ GB

Free space on drive C:\ is 1002.80 MB

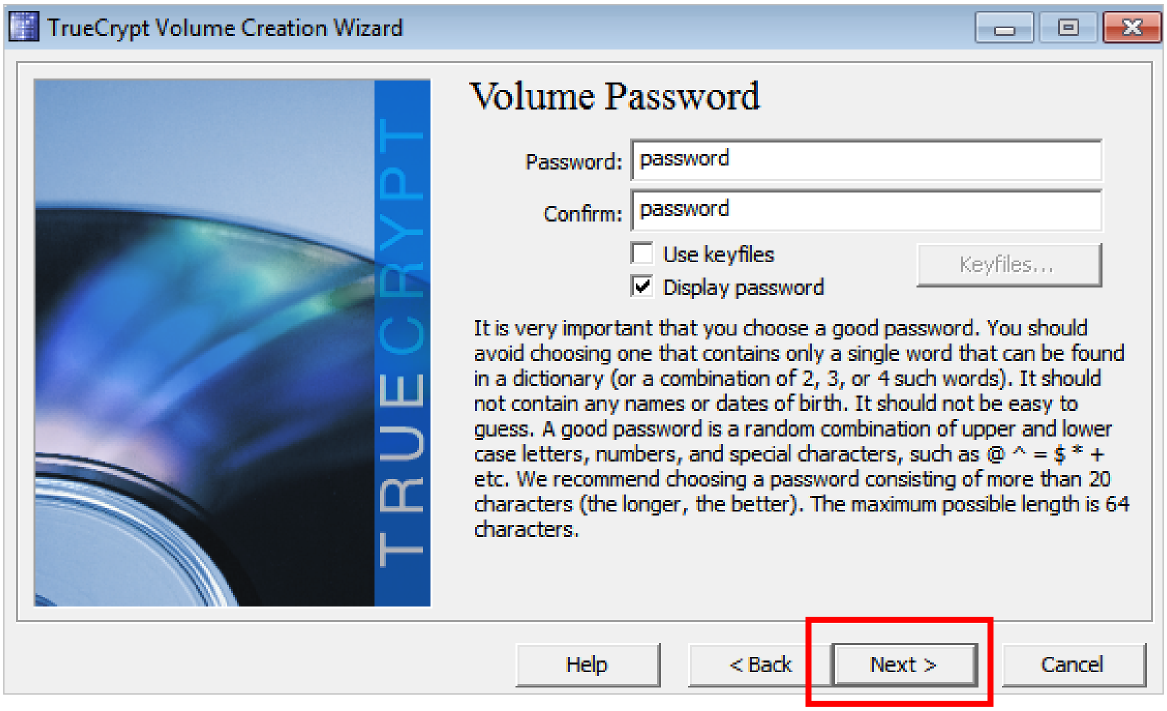
Please specify the size of the container you want to create.

If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.

Note that the minimum possible size of a FAT volume is 292 KB. The minimum possible size of an NTFS volume is 3792 KB.

Figure 22: Volume Size Screen

13. For the password, type **password** and confirm the password of **password**. Click **Next**.



Volume Password

Password: password

Confirm: password

□ Use keyfiles

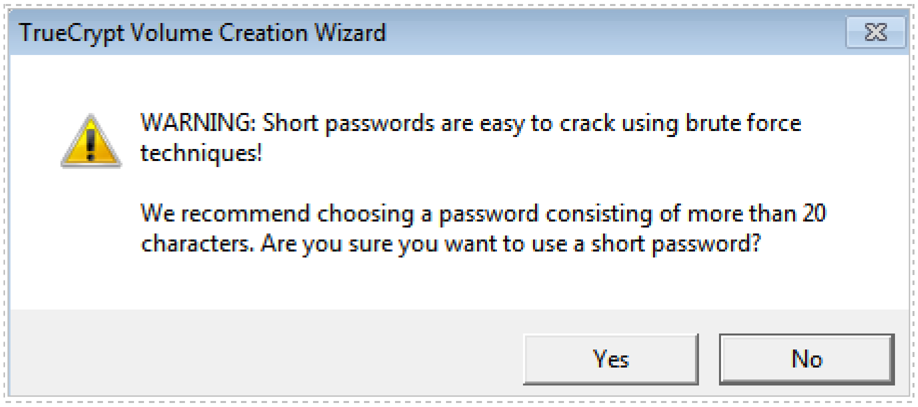
☑ Display password

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.

Figure 23: Setting the Volume Password

TrueCrypt asks for a password that is a minimum of 20 characters. You can use a shorter password, but it is not advised. Use uppercase, lowercase, and special characters to make a stronger password for any production use of TrueCrypt.

14. Click **Yes** to the warning about the short password (of password).

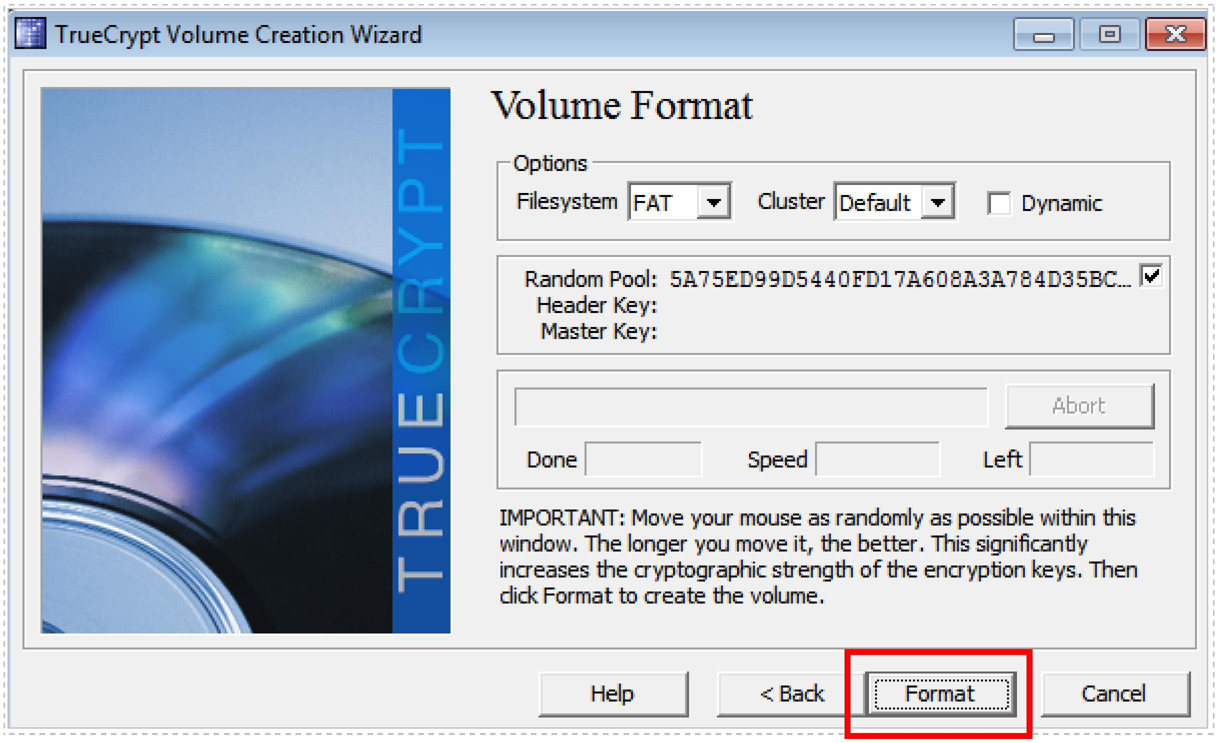

TrueCrypt Volume Creation Wizard

WARNING: Short passwords are easy to crack using brute force techniques!

We recommend choosing a password consisting of more than 20 characters. Are you sure you want to use a short password?

Figure 24: Short Password Warning

15. Accept the default for the File System and click **Format**.


TrueCrypt Volume Creation Wizard

Volume Format

Options

Filesystem FAT Cluster Default □ Dynamic

Random Pool: 5A75ED99D5440FD17A608A3A784D35BC... ☑
Header Key:
Master Key:

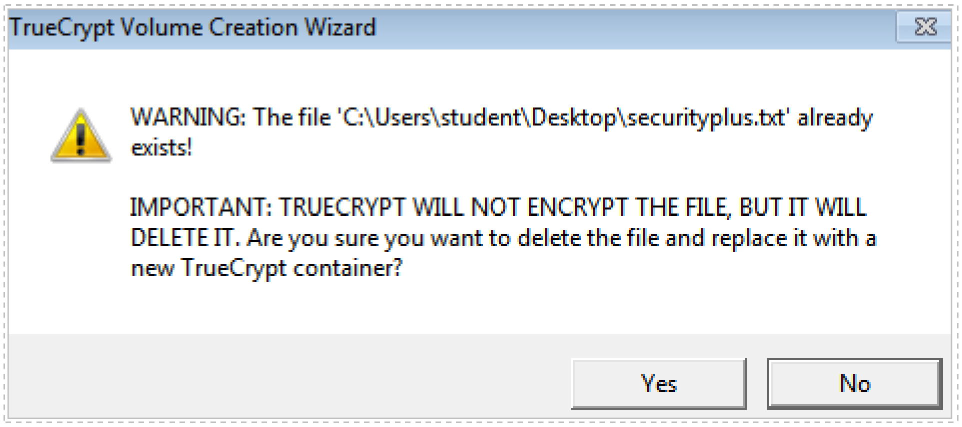
Done Speed Left

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.

Figure 25: Volume Format Screen of TrueCrypt

A file 4 GB or larger cannot be stored on a FAT volume. If you have files larger than 4 GB, use an NTFS file system instead of using a FAT file system.

16. Click **Yes** to replace the blank text file with a TrueCrypt container.



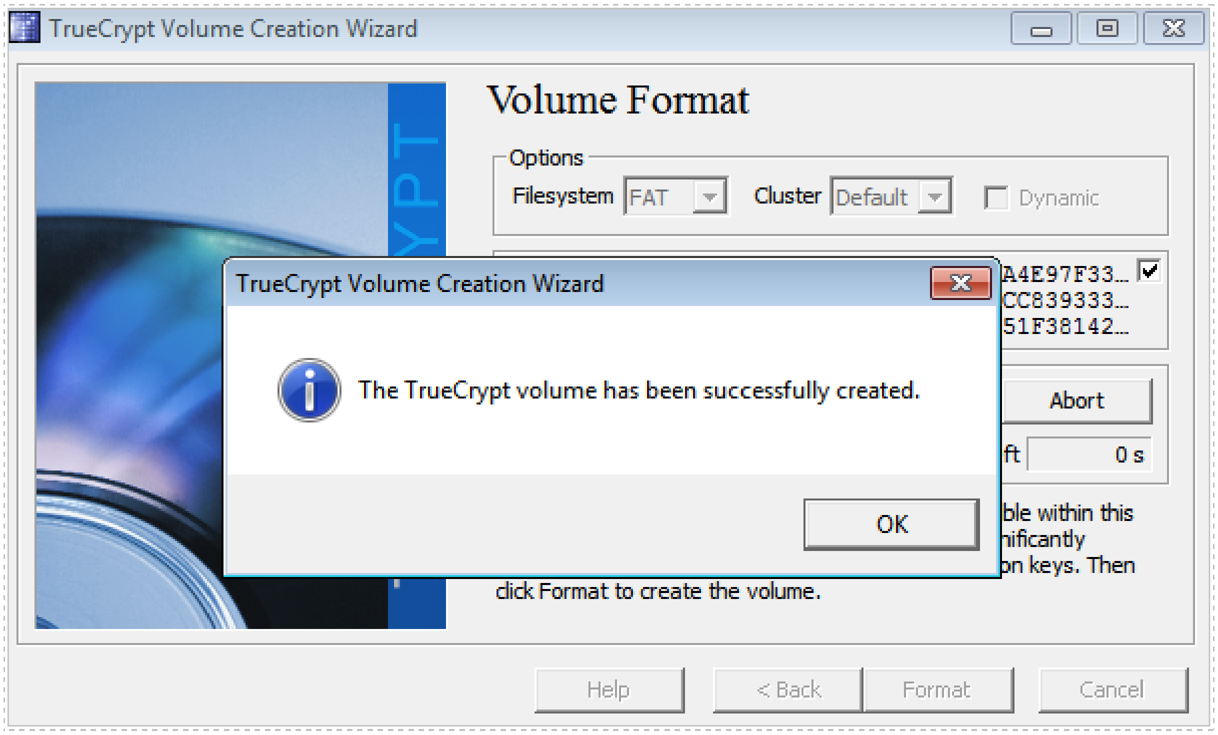
TrueCrypt Volume Creation Wizard

WARNING: The file 'C:\Users\student\Desktop\securityplus.txt' already exists!

IMPORTANT: TRUECRYPT WILL NOT ENCRYPT THE FILE, BUT IT WILL DELETE IT. Are you sure you want to delete the file and replace it with a new TrueCrypt container?

Figure 26: File Deletion Warning

17. Click **OK** in response to the message that *the TrueCrypt volume was successfully created*.



TrueCrypt Volume Creation Wizard

Volume Format

Options

Filesystem FAT

Cluster Default

☐ Dynamic

A4E97F33... ☑
CC839333...
51F38142...

ft 0 s

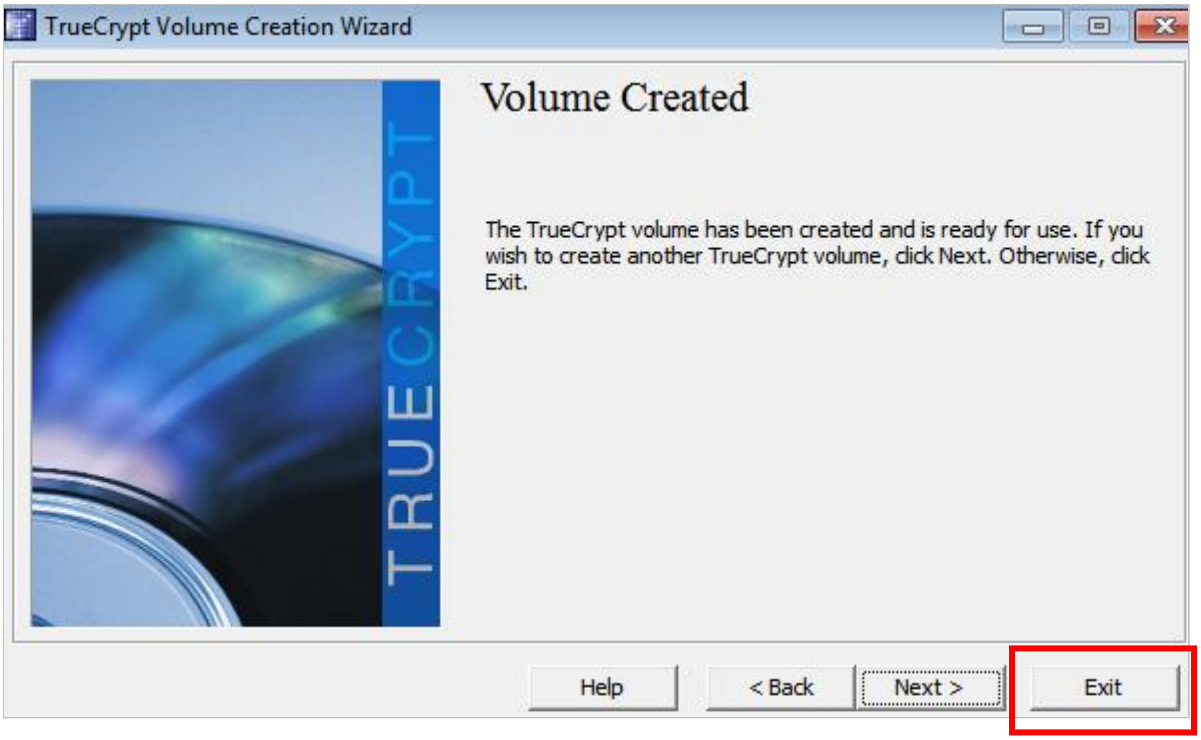
ble within this
hificantly
on keys. Then
click Format to create the volume.

TrueCrypt Volume Creation Wizard

The TrueCrypt volume has been successfully created.

Figure 27: Volume Successfully Created Message

18. Click **Exit** at the Volume Creating Wizard Screen to exit the TrueCrypt program.



Volume Created

The TrueCrypt volume has been created and is ready for use. If you wish to create another TrueCrypt volume, click Next. Otherwise, click Exit.

Figure 28: Exiting TrueCrypt

2.2 Conclusion

Creating an encrypted file container is done by creating a blank text file, and then selecting that blank text file during the file container creation process.

2.3 Discussion Questions

1. What are the two types of volumes TrueCrypt can create?
2. What will you need to do if you encrypt the system partition or drive?
3. What is the default encryption algorithm used within TrueCrypt?
4. What might make you decide you want to format your TrueCrypt container with the NTFS file system?

3 Opening and Viewing Data within a TrueCrypt Container

In this section, you will open your newly created TrueCrypt container, store files on it, and unmount the volume. Only a user with the password will be able to mount the volume and view the information stored on the encrypted file container.

3.1 Using the TrueCrypt Container

In order to protect your data, you will need to know how to mount and unmount your TrueCrypt volume. In order to mount the volume, provide the correct password.

1. Double-click on the **TrueCrypt** icon on your desktop.

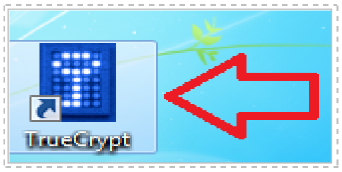


Figure 29: Opening TrueCrypt

2. Click the **Select File** radio button so your TrueCrypt container can be located.

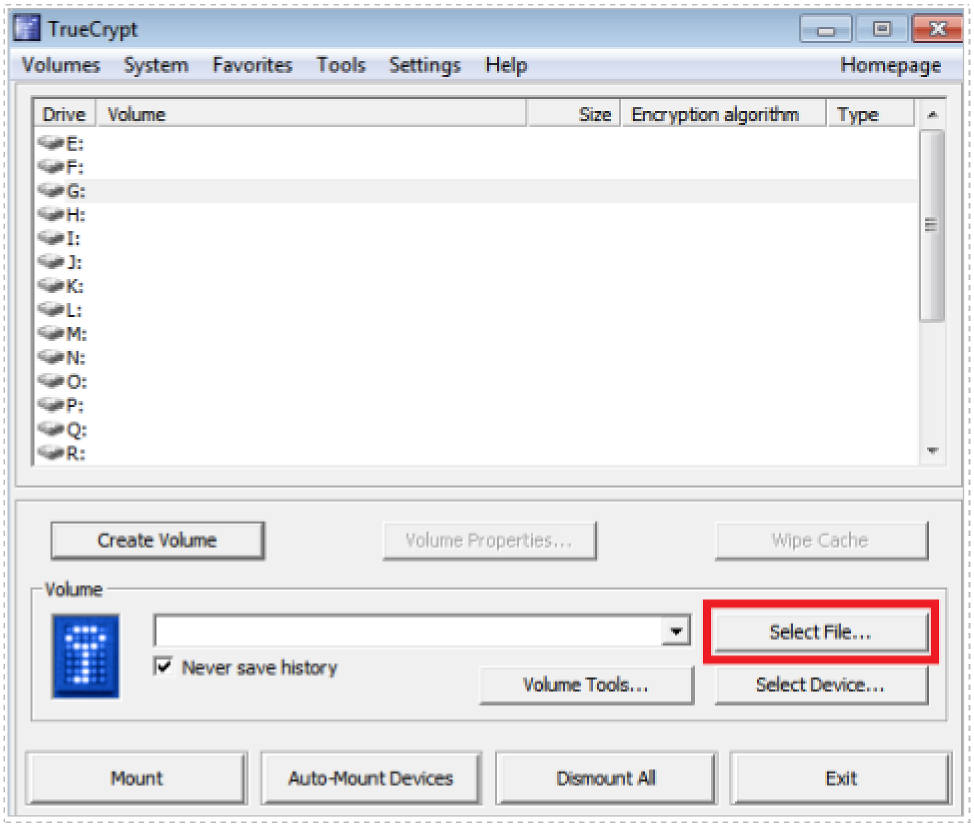
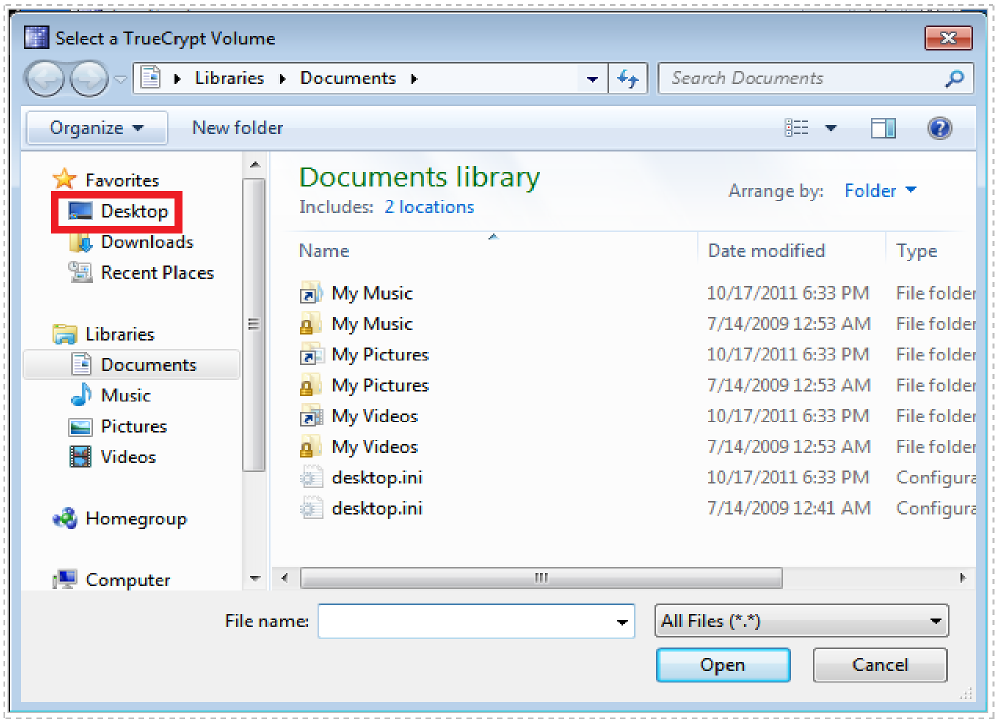


Figure 30: Selecting the TrueCrypt File

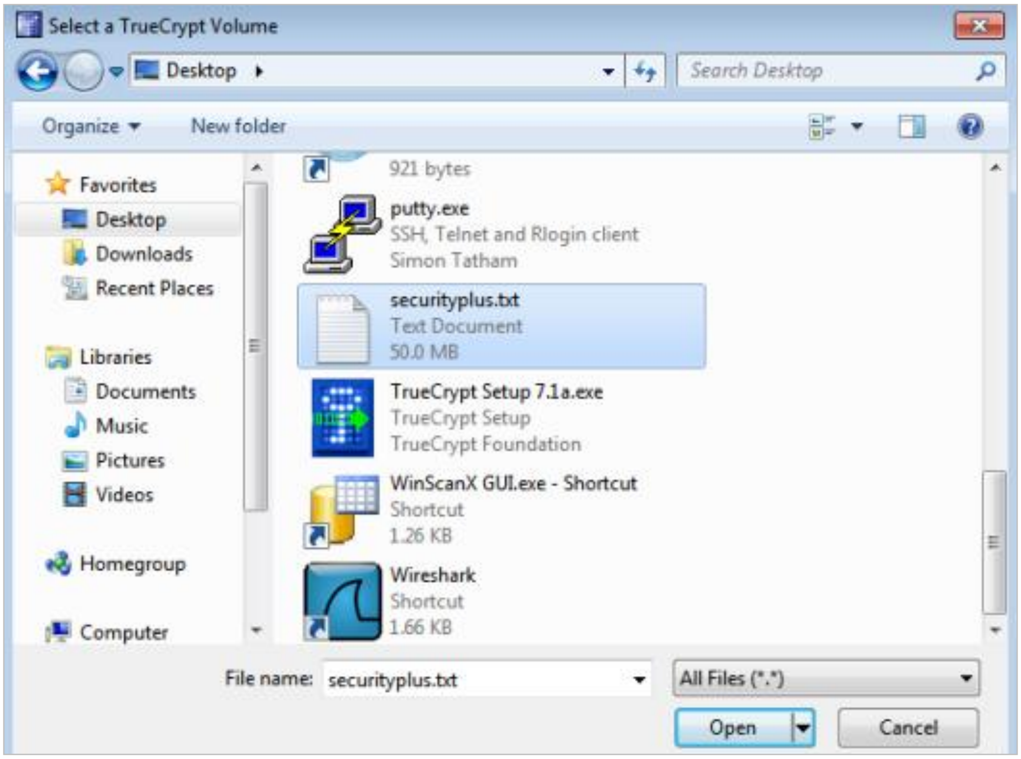
3. Click the **Desktop** link on the left side of Windows Explorer screen.



Name	Date modified	Type
My Music	10/17/2011 6:33 PM	File folder
My Music	7/14/2009 12:53 AM	File folder
My Pictures	10/17/2011 6:33 PM	File folder
My Pictures	7/14/2009 12:53 AM	File folder
My Videos	10/17/2011 6:33 PM	File folder
My Videos	7/14/2009 12:53 AM	File folder
desktop.ini	10/17/2011 6:33 PM	Configura
desktop.ini	7/14/2009 12:41 AM	Configura

Figure 31: Navigating to the Text File Location

4. Double-click on the **securityplus**.txt file on the desktop.



921 bytes

putty.exe
SSH, Telnet and Rlogin client
Simon Tatham

securityplus.txt
Text Document
50.0 MB

TrueCrypt Setup 7.1a.exe
TrueCrypt Setup
TrueCrypt Foundation

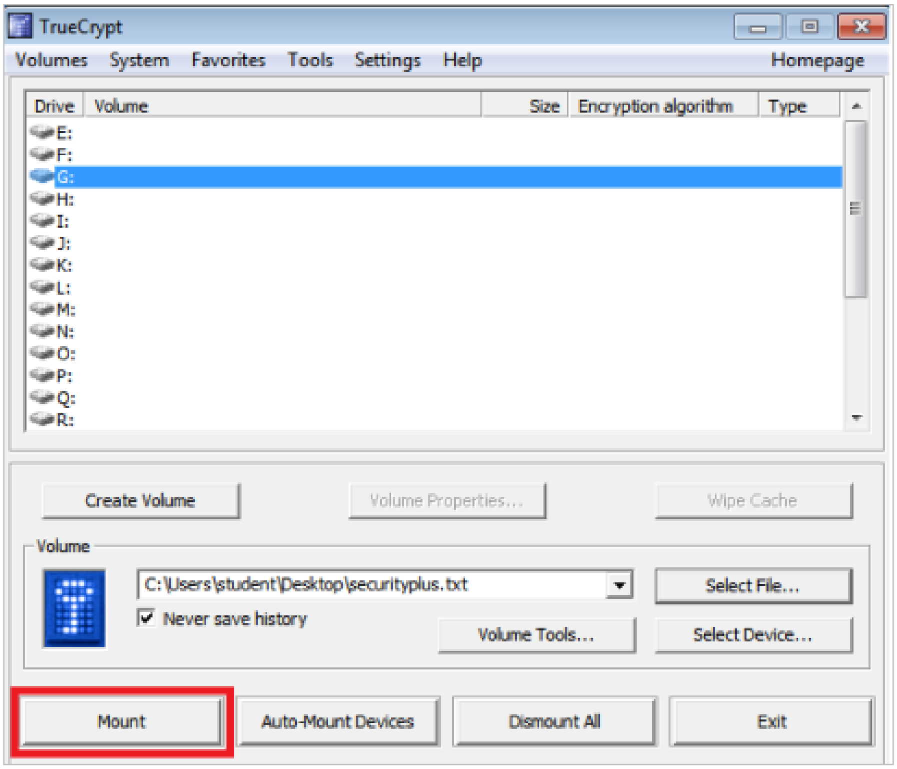
WinScanX GUI.exe - Shortcut
Shortcut
1.26 KB

Wireshark
Shortcut
1.66 KB

File name: securityplus.txt

Figure 32: Selecting the Text File

5. Click on any available drive letter, and then click the **Mount** radio button.

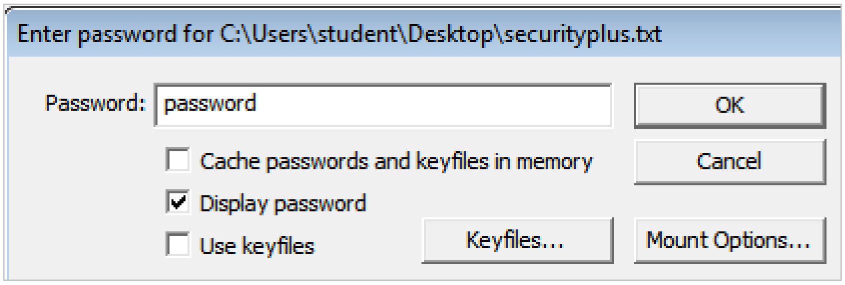

TrueCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption algorithm Type
E: F: G: H: I: J: K: L: M: N: O: P: Q: R:
Create Volume
Volume Properties...
Wipe Cache
Select File...
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

Volume: C:\Users\student\Desktop\securityplus.txt

☑ Never save history

Figure 33: Mounting the Container

6. Enter **password** for the password, then click the **OK** button.


Enter password for C:\Users\student\Desktop\securityplus.txt

Password: password

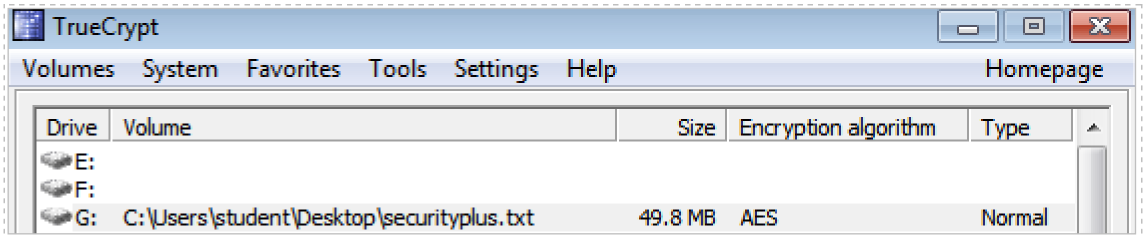
☐ Cache passwords and keyfiles in memory

☑ Display password

☐ Use keyfiles

Figure 34: Entering the Password for the Volume

If the drive is successfully mounted, it will be listed in the TrueCrypt window.



Drive	Volume	Size	Encryption algorithm	Type
E:				
F:				
G:	C:\Users\student\Desktop\securityplus.txt	49.8 MB	AES	Normal

Figure 35: The Volume is Successfully Mounted

7. Click on the **Start** button, and click on **Computer**.

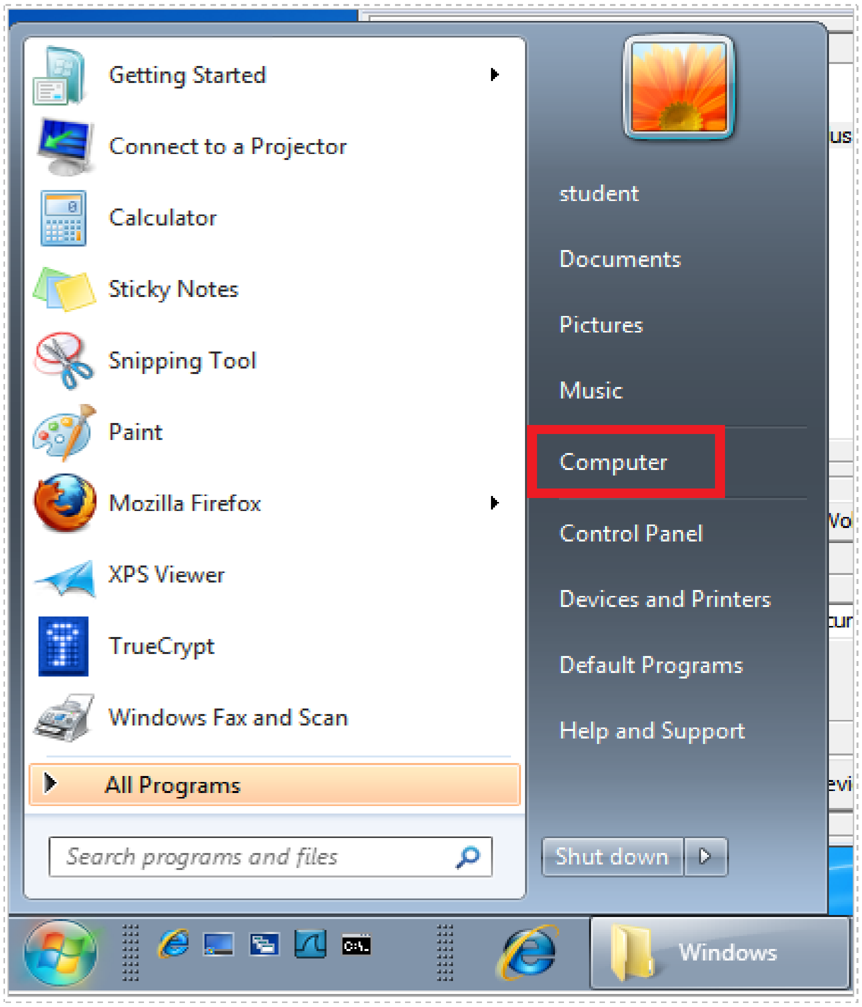


Figure 36: Clicking on Computer from the Start Button

Your TrueCrypt volume is displayed as a logical drive on your system. Items can be stored there. After it is unmounted, no one will be able to see the files stored within the container unless they successfully mount the volume with the correct password.

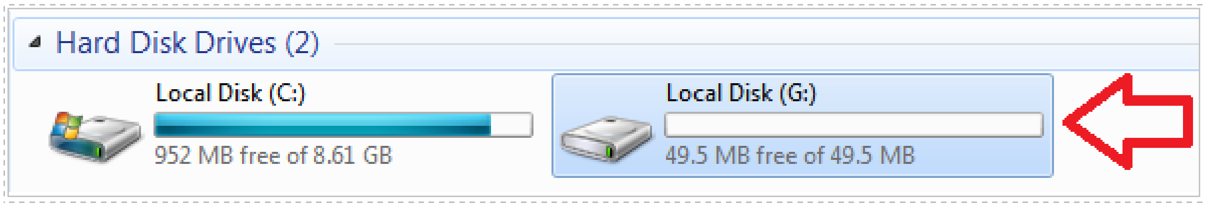


Figure 37: The TrueCrypt Volume is Displayed

8. Navigate to **Local Disk C:>Windows>Web>Wallpaper>Architecture.** Use the **CTRL-A** keys to copy all of the files within the Architecture folder.

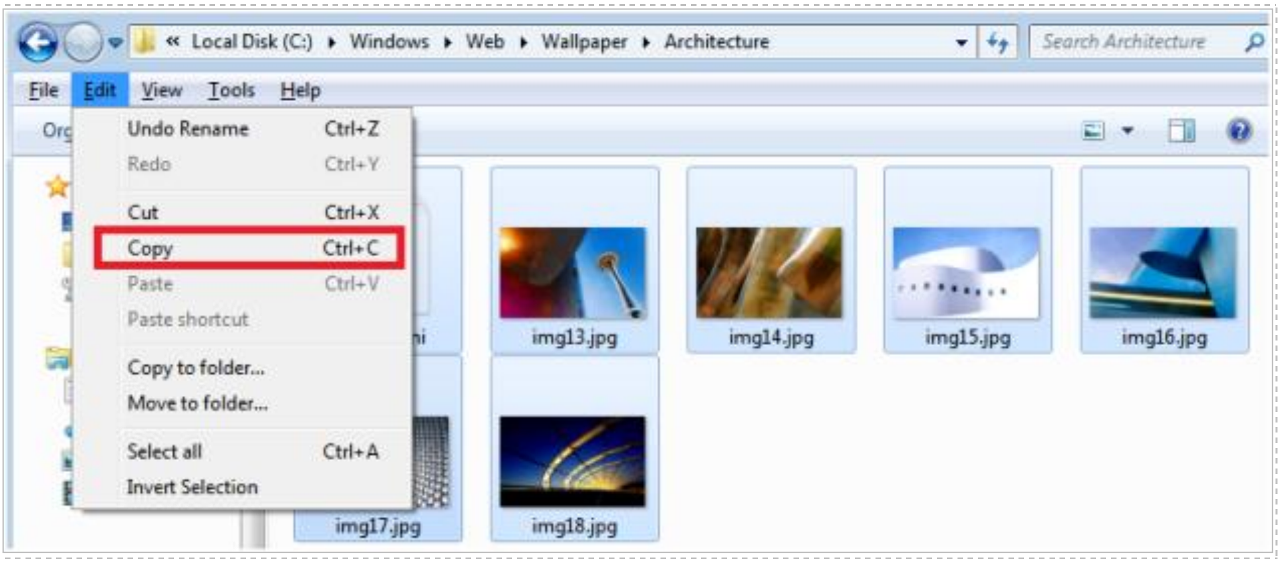


Figure 38: Copying the Picture Files

9. Click on **Start** and select **Computer**. Double-click on the TrueCrypt Volume. Use **Control + V** to paste all of the items from the folder into the TrueCrypt container.

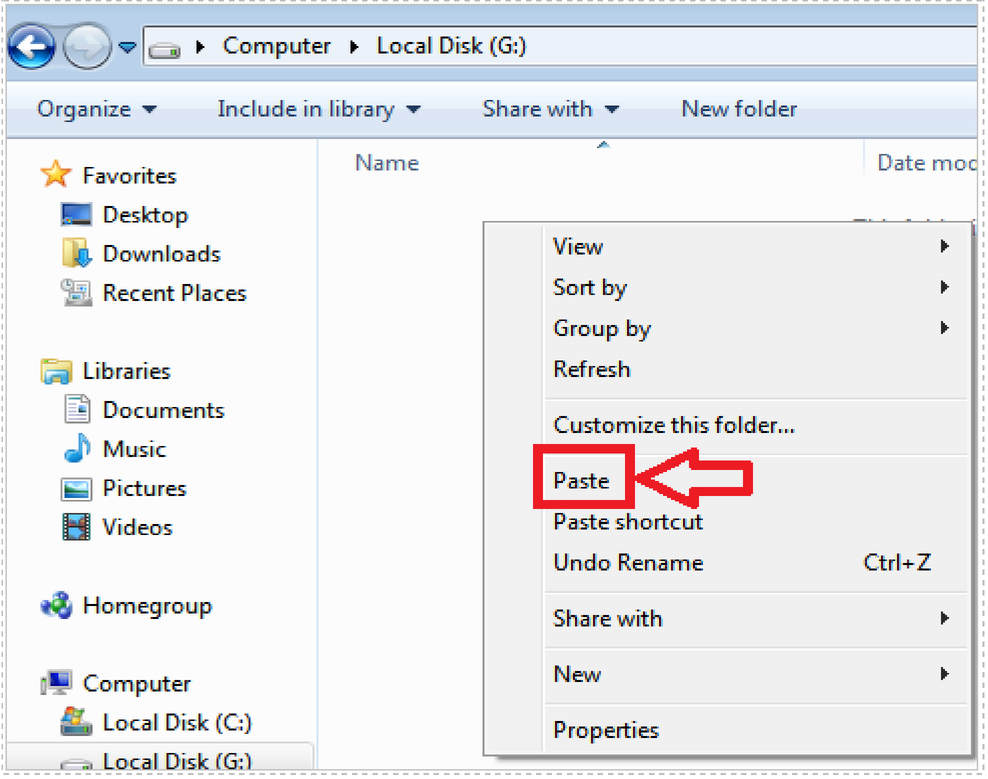
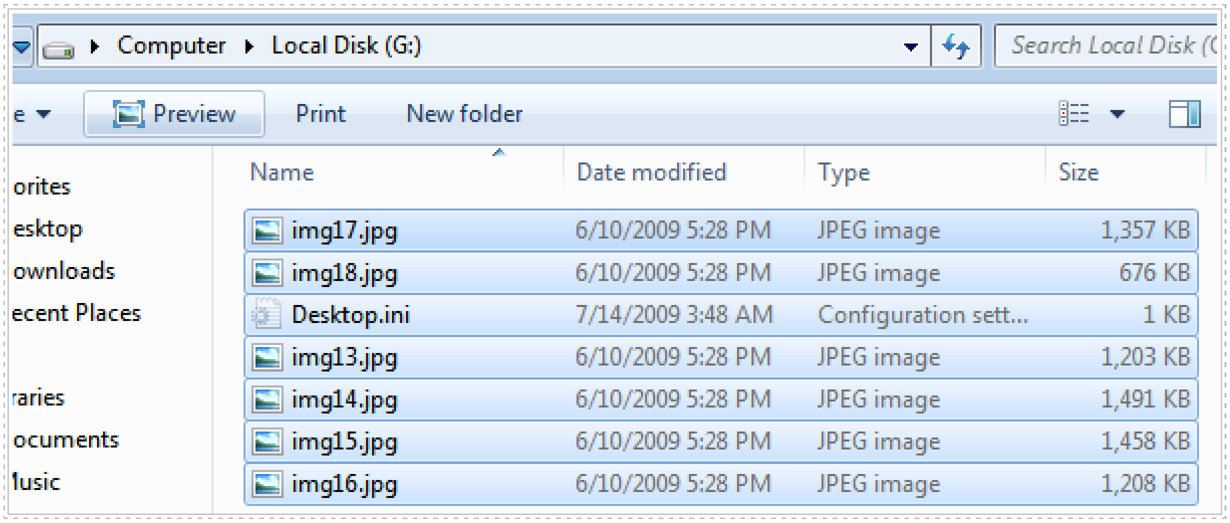


Figure 39: Pasting the files within the TrueCrypt Volume

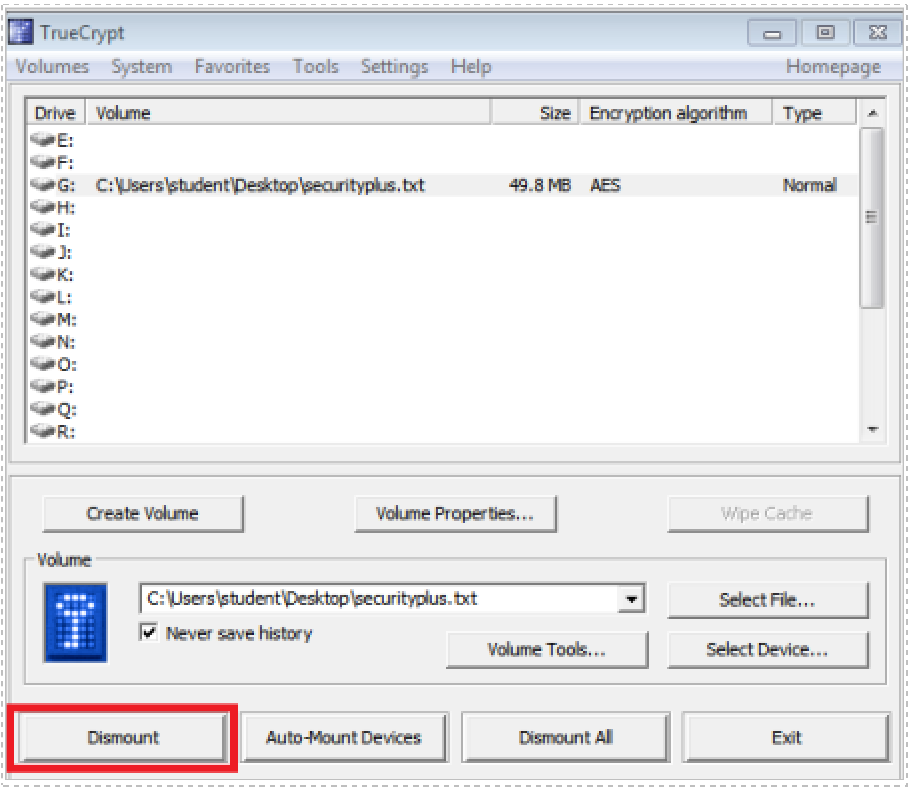
The files should now all be in the TrueCrypt container.



Name	Date modified	Type	Size
img17.jpg	6/10/2009 5:28 PM	JPEG image	1,357 KB
img18.jpg	6/10/2009 5:28 PM	JPEG image	676 KB
Desktop.ini	7/14/2009 3:48 AM	Configuration sett...	1 KB
img13.jpg	6/10/2009 5:28 PM	JPEG image	1,203 KB
img14.jpg	6/10/2009 5:28 PM	JPEG image	1,491 KB
img15.jpg	6/10/2009 5:28 PM	JPEG image	1,458 KB
img16.jpg	6/10/2009 5:28 PM	JPEG image	1,208 KB

Figure 40: The files within the TrueCrypt Volume

10. Click **Dismount** to unmount the volume. The only way someone will be able to view those files is if they mount the volume with the correct password.



Drive	Volume	Size	Encryption algorithm	Type
E:				
F:				
G:	C:\Users\student\Desktop\securityplus.txt	49.8 MB	AES	Normal
H:				
I:				
J:				
K:				
L:				
M:				
N:				
O:				
P:				
Q:				
R:				

Volume: C:\Users\student\Desktop\securityplus.txt

☑ Never save history

Figure 41: Dismounting the TrueCrypt Volume

11. Complete the task by closing all open windows.

3.2 Conclusion

Once an encrypted file container is created with TrueCrypt, it must be located, and then mounted. In order to mount the drive successfully, you must provide the correct password. Data can then be stored on the drive. When you are finished using the drive, and want to prevent others from seeing the content within it, dismount the volume.

3.3 Discussion Questions

1. What drive letter can be used when mounting a TrueCrypt volume?
2. How is a TrueCrypt volume displayed after it is mounted?
3. After mounting, how do you prevent individuals from viewing the content?
4. What two things do you need to successfully mount a TrueCrypt volume?

References

1. TrueCrypt:
   http://www.truecrypt.org/

2. BitLocker:
   http://technet.microsoft.com/en-us/library/cc766295(v=ws.10).aspx

3. FileVault 2:
   http://support.apple.com/kb/HT4790?viewlocale=en_US&locale=en_US

4. FileVault:
   http://docs.info.apple.com/article.html?path=Mac/10.4/en/mh1906.html

5. DM-Crypt:
   http://www.saout.de/misc/dm-crypt/