Writing Assignment 2
How to Encrypt Files on Ubuntu Using TrueCrypt

Motivation

It is often useful to store sensitive information on your computer. For example, you might store your credit card number on your computer for online shopping. However, if you do not protect this data, anyone with access to your computer can see it. You can guard against this threat by encrypting your sensitive files so that only you can view them.

Overview

This tutorial will teach you how to use TrueCrypt, an open-source encryption program. TrueCrypt creates *encrypted volumes*, which are containers that store the files you want to protect. The tutorial has **5 steps** and should take no more than **10 minutes** to complete. After completing these steps, you should be able to encrypt and decrypt files on your computer using TrueCrypt.

Audience

This tutorial is for Ubuntu users who want to encrypt files on their computer. Audience members should be familiar with the Gnome desktop environment. Users should be experienced enough to perform basic tasks such as browsing for files, copying files from one location to another, and starting applications from the Ubuntu main menu.

Requirements

For this tutorial, you must use the **Gnome desktop** environment for **Ubuntu Linux**. You will need **Internet access**, as well as a modern **web browser**, such as Mozilla Firefox or Google Chrome, to navigate the Internet and download files.

Caution

You may lose your files if you do not follow the steps carefully. If you forget an encryption password, you may never be able to decrypt your files. Decrypting a file without knowing the correct password is incredibly difficult!

Step 1: Download and Install TrueCrypt

This step outlines how to install TrueCrypt on your computer.

- In a web browser, go to **http://www.truecrypt.org/downloads**.

- Scroll to the Linux section. Use the drop-down menu to select the 32- or 64-bit **Standard** package (shown in *Figure 1*), depending on your system. If you do not know whether your computer is 64-bit, download the 32-bit version. Click the **Download** button below the drop-down menu to start downloading.
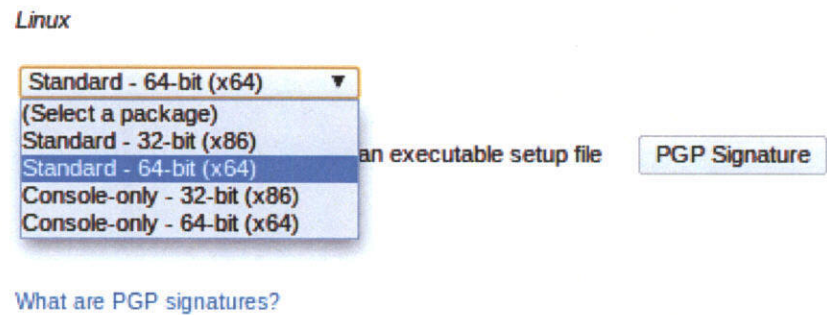

Figure 1: Downloading the correct installer

- Right-click the downloaded file and select **Extract Here** in the context menu. An installer with a name like "**truecrypt-7.0a-setup-x64**" should appear in the same folder. The name of the file depends on the version number and whether you downloaded the 64- or 32-bit version.

- Run the installer, then click the **Install TrueCrypt** button.

- Accept the license terms by clicking the button outlined in *Figure 2*. A confirmation window should appear.
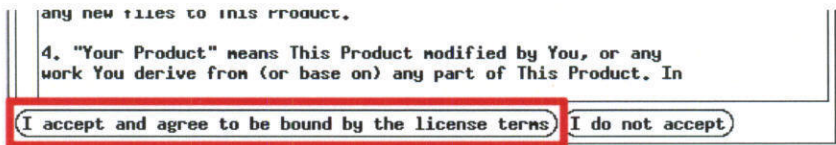

Figure 2: TrueCrypt terms and conditions

- In the confirmation window, click **OK**. If prompted, enter the administrator password. When the installation finishes, press Enter to close the installer window.

- Proceed to **Step 2**, where you will launch TrueCrypt and start creating an encrypted volume.

Step 2: Launch the Volume Creation Wizard

This step details how to launch TrueCrypt and start the volume creation wizard. This wizard lets you create encrypted volumes.

- In the Ubuntu main menu, navigate to **Accessories > TrueCrypt** and click the TrueCrypt launcher. The TrueCrypt main menu (*Figure 3*) should open in a new window.

  Note: If TrueCrypt does not start, go back to **Step 1**. If you downloaded the 32-bit installer before, try downloading the 64-bit version instead, and vise versa.
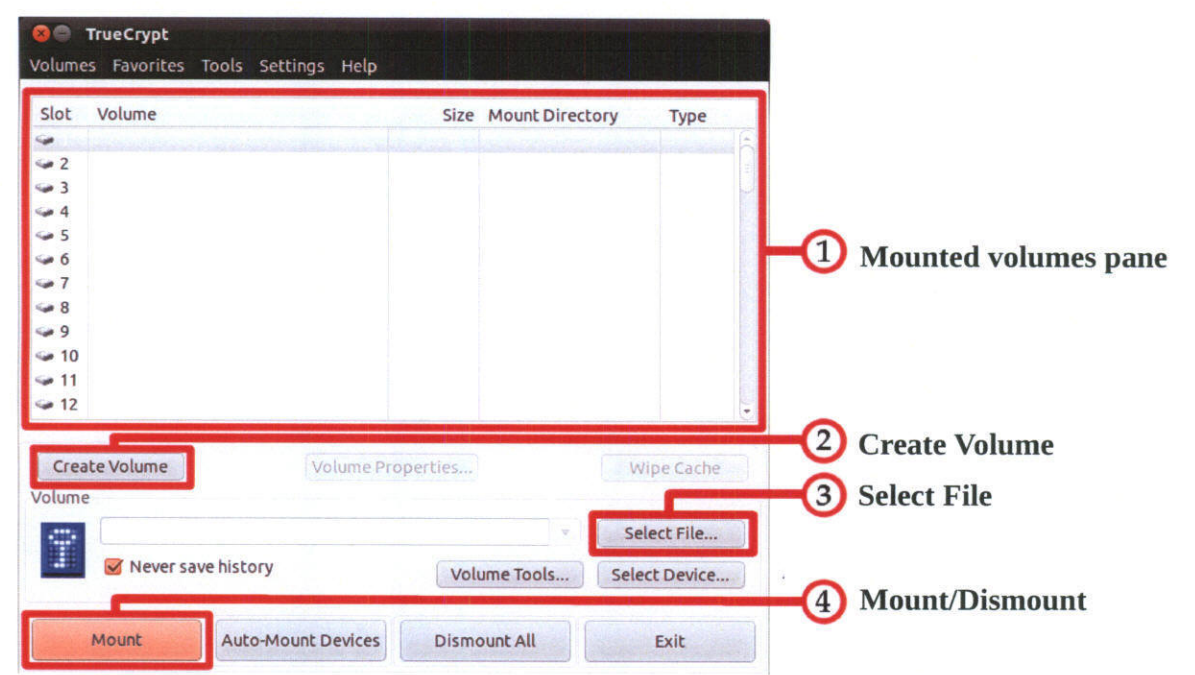

Figure 3: TrueCrypt main menu

- Click **Create Volume** (labeled **2** in *Figure 3*). The TrueCrypt Volume Creation Wizard should appear in a new window.

- Proceed to **Step 3**, where you will specify the settings of the encrypted volume you want to create.

3

Step 3: Create an Encrypted Volume

This step explains how to use the default settings to create an encrypted volume. You can choose different settings if you wish.

- In the lower-right corner of the wizard, click the **Next** button twice, to use the default settings.

- Click **Select File**, as seen in *Figure 4*. Browse to the location where the volume should be stored and enter a name for the volume. *Figure 4* shows the wizard after choosing a location. Click **Next** to continue.

    Caution: TrueCrypt will delete any file whose name matches the name you give in this step, so do not select a file that you want to encrypt. **Step 5** shows how to encrypt a specific file.
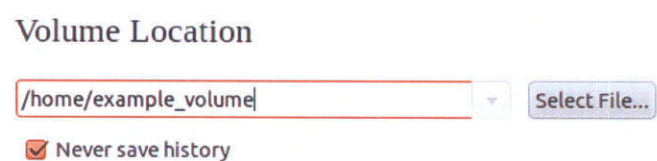
Volume Location

/home/example_volume   ▾   Select File...

☑ Never save history

Figure 4: Setting the location

- Click **Next** to accept the default encryption algorithm.

- Enter the size of the encrypted volume. TrueCrypt will tell you the largest and smallest possible size of the volume. Make sure the size you enter is large enough to store the files you want to encrypt. Click **Next** when you are done.

- Enter and confirm a password to use with this volume, as in *Figure 5*. You will use this password to decrypt the volume, so choose a strong password. Click **Next** to continue.

    Note: If you enter a weak password, TrueCrypt will display a warning message. Click **OK** to close this warning.

Volume Password

Password: ••••••••••••••••

Confirm password: ••••••••••••••••

Figure 5: Choosing a password

- Click **Next** to accept the default filesystem type.

- Click **Format**. If prompted, enter the administrator password. A confirmation dialog will appear if the volume is created successfully. Click **OK** to close the dialog, then click **Exit** to close the wizard.

- Proceed to **Step 4**, where you will mount the encrypted volume.

Step 4: Mount the Encrypted Volume

This step shows you how to mount the encrypted volume on your computer. Mounting a volume decrypts it and lets you view and change its contents.

- In the **mounted volumes pane** (labeled **1** in *Figure 3*), click an empty slot where you would like to mount the volume.

- Click **Select File** (labeled **3** in *Figure 3*). Browse to the volume you created and open it. The name in the main menu should match the name from **Step 3**, as in *Figure 6*.
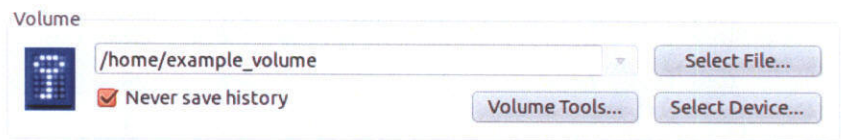

Figure 6: Browsing for a volume to mount

- Click **Mount** (labeled **4** in *Figure 3*). If prompted, enter the administrator password.

- Enter the password from **Step 3**, then click **OK**. If the mount is successful, the name of the volume should appear in the **mounted volumes pane**, as in *Figure 7*. In addition, the **Mount** button should turn into the **Dismount** button.

Figure 7: Mounted volumes pane

- Proceed to **Step 5**, where you will add files to the mounted volume.

Step 5: Encrypt Your Files

This step outlines how to add files from your computer to the mounted volume, and then encrypt the volume.

- Double-click the volume on the **mounted volumes pane** (*Figure 7*). A window with a title like "**truecrypt1**" should open.

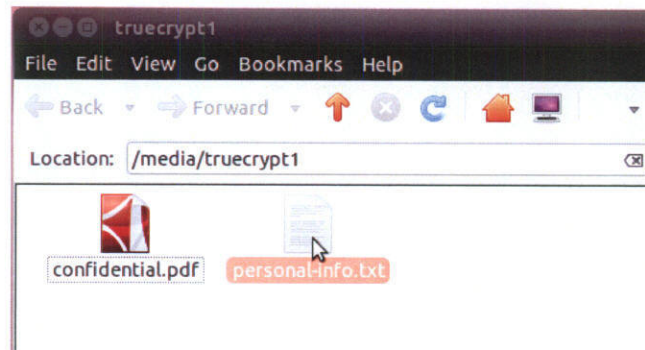- Copy the files you want to encrypt into that window, as in *Figure 8*.

Figure 8: Copying files into the volume

- Click **Dismount** (labeled **4** in *Figure 3*). The volume should disappear from the mounted volumes pane, and the window titled like "**truecrypt1**" should close.

TrueCrypt will encrypt the volume as soon as you dismount it. In order to view or modify anything in the encrypted volume, you will need to mount it again using the correct password, as in **Step 4**.