

Beginner's Tutorial for TrueCrypt

(Ubuntu 6.06 Version)

Author: Kenway Ng
kenway@cmu.edu

TABLE OF CONTENT

I.	Introduction	page 3
II.	Obtaining TrueCrypt.....	page 4
III.	Installing TrueCrypt.....	page 6
IV.	Creating TrueCrypt Volume.....	page 9
V.	Using TrueCrypt.....	page 13

I. Introduction

Welcome to the exciting (or not) world of cryptography. As our lives become more dependent on computers and the Internet, we leave a lot of personal/business, and sensitive data on our computers. It can be our banking records, client's information, email messages or our grocery list. Our computers have become a repository of information and juicy targets for a lot of criminals that commit identity theft. Having access your computer can easily be done remotely through the Internet nowadays. With the surge in Internet attacks, and bugs on your operating system and software being exploited, your computer is like an open vault.

A good first step in safekeeping your data is to encrypt it. In this Step-by-Step guide, we'll introduce TrueCrypt, an encryption software. In addition, the guide will walk you through a simple scenario which shows you how to obtain TrueCrypt v4.3, install it on Ubuntu 6.06, create TrueCrypt volumes, and how to keep your data safe.

TrueCrypt is a free open source on the fly encryption software. (On the fly means that all decryption is done within the memory and no decrypted data is written to the hard drive.) It works for many operating systems, including Windows and Linux (ie: Ubuntu 6.06). TrueCrypt works in two ways. It creates a TrueCrypt encrypted volume on your hard drive, which is basically a file, or it can encrypt entire hard disk partition or USB memory stick, but the latter topic is out of the scope of this guide. (Please refer to www.truecrypt.org for more information on how to encrypt an entire hard disk partition.) After TrueCrypt creates the encrypted volume - it can be mounted for anyone to use. No data stored on an encrypted volume can be read (decrypted) without using the correct password. Everything is encrypted including file names, folder names, contents of every file, free space, meta data, etc. In short, a TrueCrypt volume behaves like a real physical drive. You can imagine yourself moving your sensitive files to that volume(another hard drive). To have access to that volume, you'll need a password. All the data that resides on the volume is encrypted and no one can read it without the right password.

II. Obtaining TrueCrypt

1. Before we can start using TrueCrypt we need to obtain the software first. Open a browser and go to www.truecrypt.org/downloads.php to download the source code. (See Figure 1.)

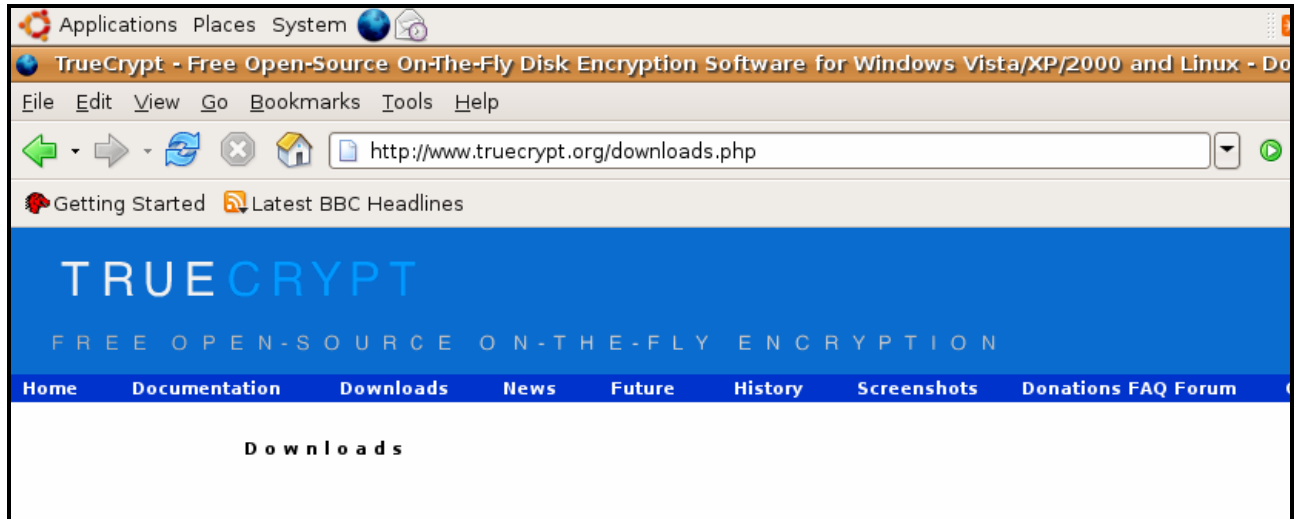


Figure 1

2. From the drop down menu – select Ubuntu 6.06 x86 and click on download. (See Figure 2.)

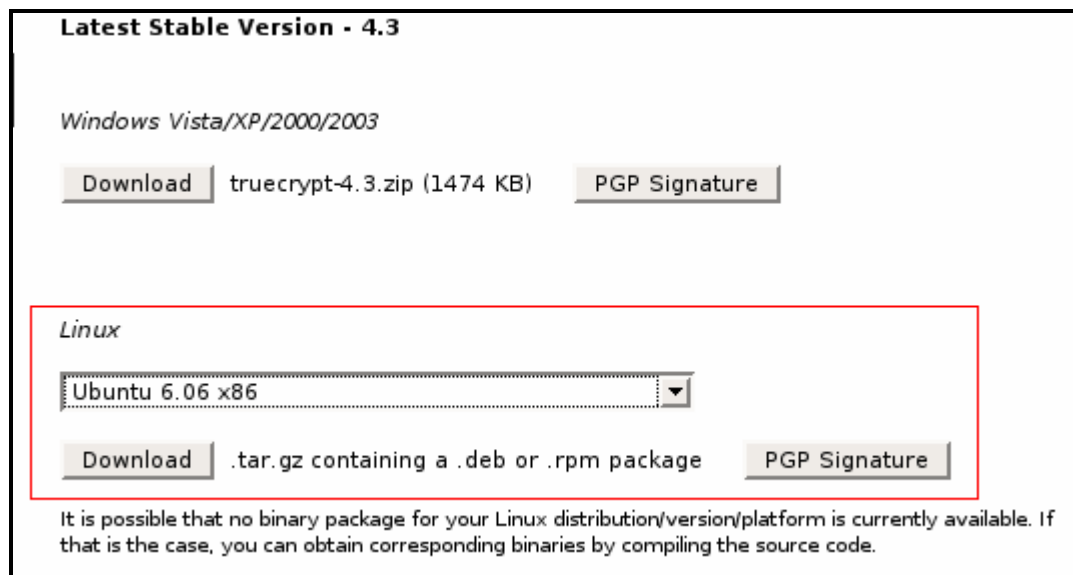


Figure 2

3. Save the file to your desktop. (See Figure 3.) You will notice there is a new file on your Desktop named “truecrypt-4.3-ubuntu-6.06-x86.tar.gz .” (See Figure 4.) Proceed to the next section on how to install TrueCrypt.

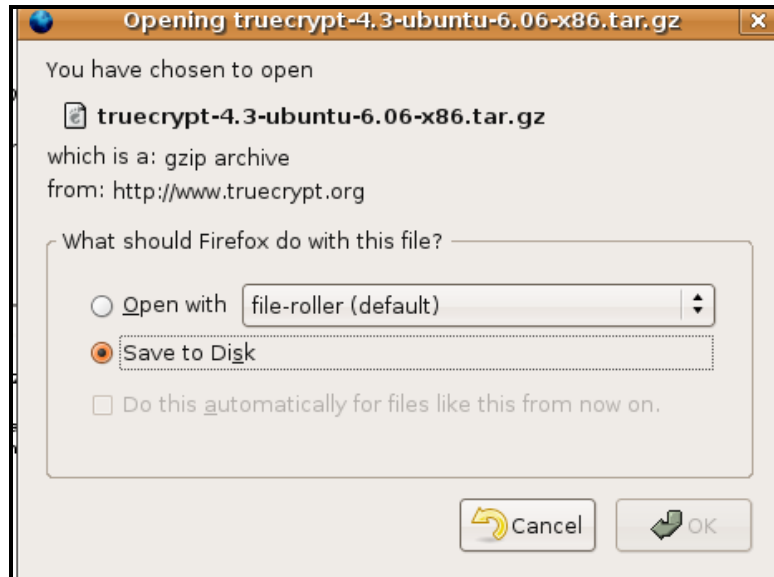


Figure 3

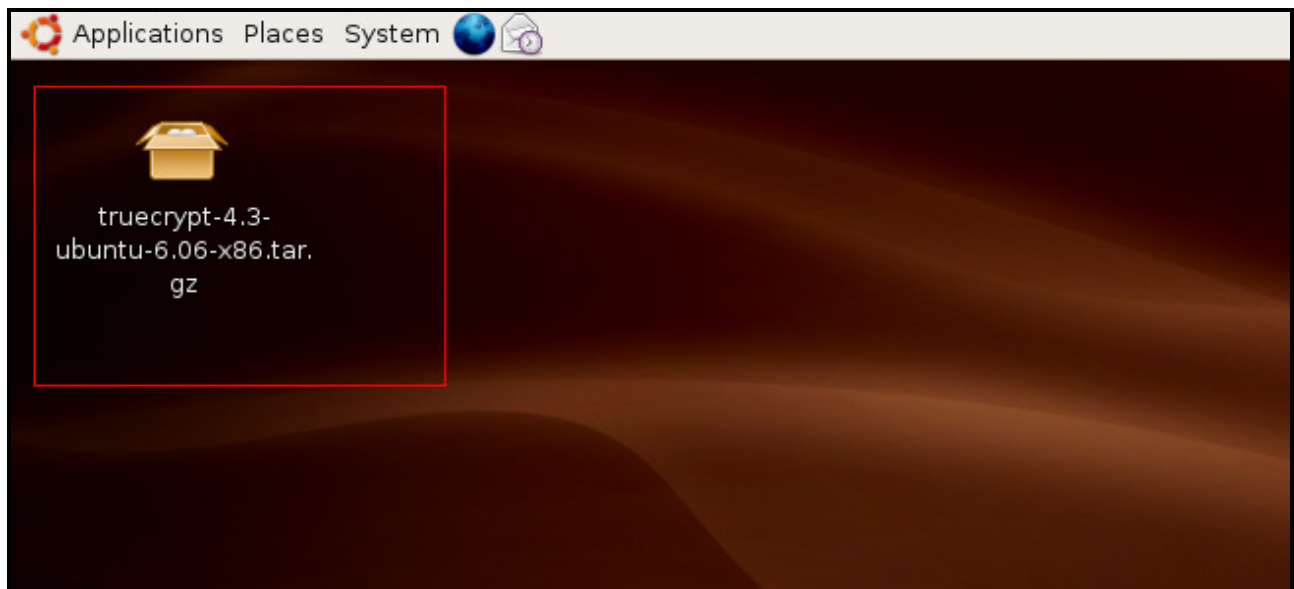


Figure 4

III. Installing TrueCrypt

4. Now that you downloaded TrueCrypt, you'll need to install the program before you can use its services. Launch a terminal screen and go to your Desktop directory.

```
% cd /home/username/Desktop
```

(Replace username with your username.)

Note: The % character at the beginning of these command boxes represents a shell prompt. You should not type the % character!

5. Decompress and extract TrueCrypt .deb file by entering the following command:

```
% tar -zxvf truecrypt-4.3-ubuntu-6.06-x86.tar.gz
```

6. You will notice that a new folder, "truecrypt-4.3", is created on your Desktop. Change your directory to that folder and install TrueCrypt. You'll need root access to install TrueCrypt. Type your password when prompted.

```
% cd truecrypt-4.3/  
% sudo dpkg -i /root/Tools/truecrypt_4.2-0_i386.deb
```

7. If your screen is similar to Figure 4, you have installed TrueCrypt. (See Figure 5.)

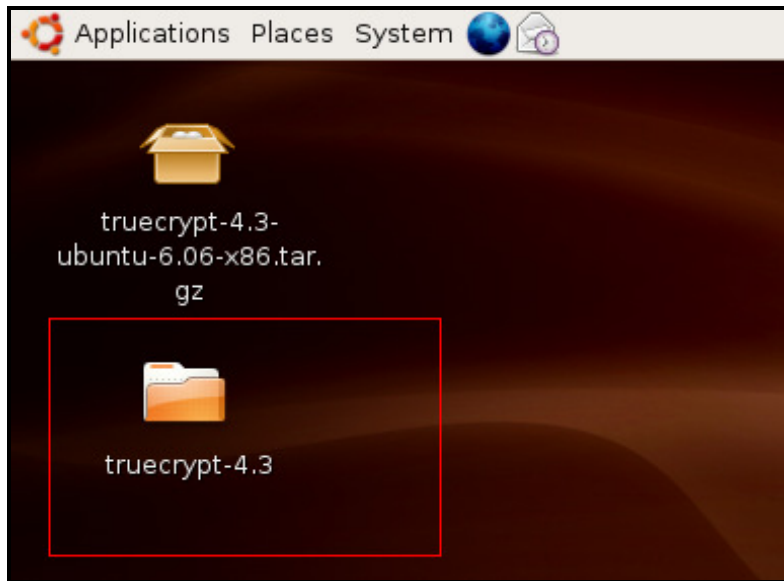
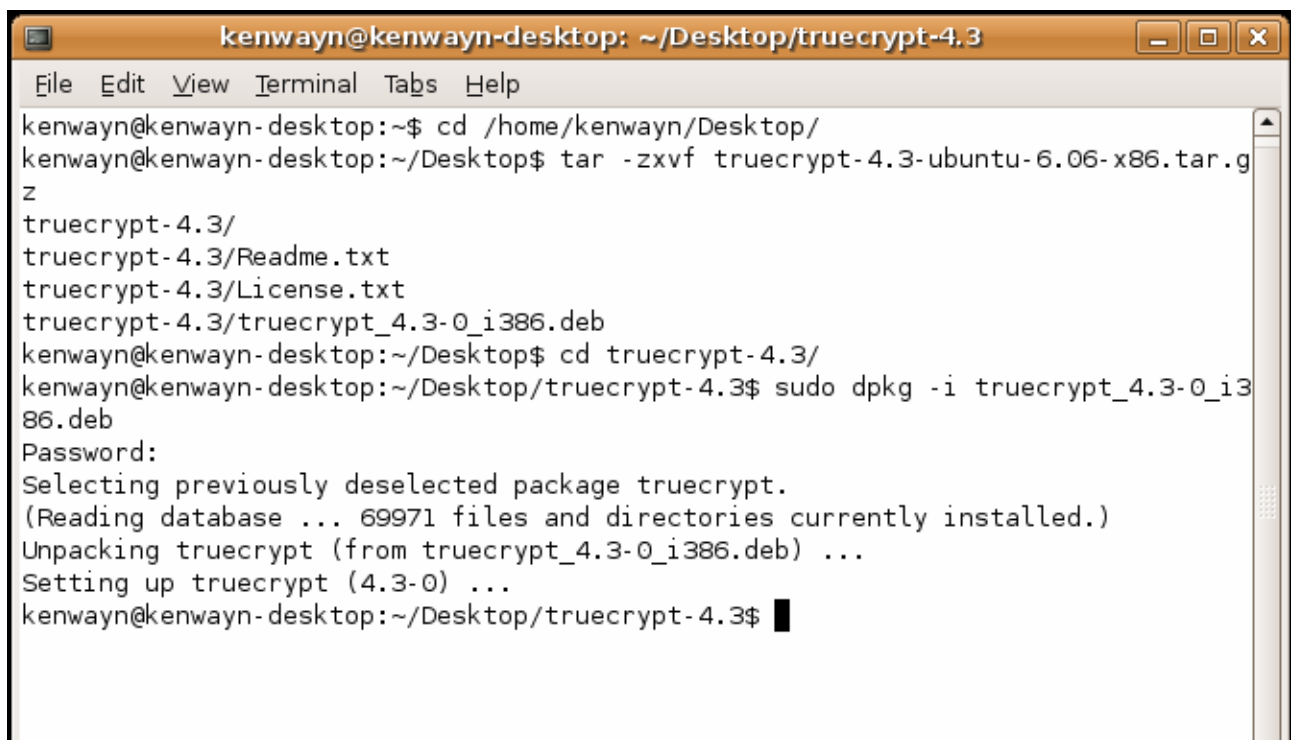


Figure 5

8. In addition, check the path where TrueCrypt is installed by typing:

```
% which truecrypt
```

The path should be /usr/bin/truecrypt. TrueCrypt is now installed and ready to create encrypted volumes. (See Figure 6 for output of my terminal.)

A terminal window titled "kenwayn@kenwayn-desktop: ~/Desktop/truecrypt-4.3" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the following commands and output:

```
kenwayn@kenwayn-desktop:~$ cd /home/kenwayn/Desktop/  
kenwayn@kenwayn-desktop:~/Desktop$ tar -zxvf truecrypt-4.3-ubuntu-6.06-x86.tar.gz  
truecrypt-4.3/  
truecrypt-4.3/Readme.txt  
truecrypt-4.3/License.txt  
truecrypt-4.3/truecrypt_4.3-0_i386.deb  
kenwayn@kenwayn-desktop:~/Desktop$ cd truecrypt-4.3/  
kenwayn@kenwayn-desktop:~/Desktop/truecrypt-4.3$ sudo dpkg -i truecrypt_4.3-0_i386.deb  
Password:  
Selecting previously deselected package truecrypt.  
(Reading database ... 69971 files and directories currently installed.)  
Unpacking truecrypt (from truecrypt_4.3-0_i386.deb) ...  
Setting up truecrypt (4.3-0) ...  
kenwayn@kenwayn-desktop:~/Desktop/truecrypt-4.3$
```

Figure 6

IV. Creating TrueCrypt Volumes

9. Go back to your home directory. Now begin creating a TrueCrypt volume. To get started, type:

```
% cd ~  
% truecrypt -c
```

10. Enter '1' to select a Normal volume type.

Note that the alternate option, 'Hidden', creates a hidden encrypted volume inside a normal (decoy) encrypted volume, where you would not write data after the hidden volume's creation. This feature is useful for extremely sensitive data or for users who may have to surrender their keys due to legal reasons or torture. The hidden volume is undetectable within the normal volume without the hidden volume key. However, if data is written to the normal volume, there is a chance that data in the hidden volume will be corrupted. For this reason, it is probably a good idea to use normal volumes for backup data. For more information, see:

<http://www.truecrypt.org/hiddenvolume.php>

11. For the file or device name, enter `pc.tc` for your first TrueCrypt volume. (You can create the file anywhere, just enter the full path. Ie: By entering `/home/kenwayn/Desktop/pc.tc`, I created the volume on my desktop.)
12. Press [Enter] to accept the default file system.
13. TrueCrypt will ask for the size of your encrypted volume. Before selecting the size, keep in mind that the size of the true crypt volume cannot be changed after you created it. For my example, enter '250M' when asked to specify the volume size.
14. TrueCrypt allows you to decide which hash algorithm and encryption method you want to use. You can read more about the different algorithm on www.truecrypt.org. The default choices will suffice. Press [Enter] twice to accept the default hash algorithm (RIPEMD-160) and the default encryption algorithm (AES).

15. When asked to enter a password for the new volume, enter 'tartans'. Re-enter the password to confirm it.
16. Press [Enter] to not use a key file. A key file is another alternative method used to decrypt your TrueCrypt volume. It is analogous to a key used to open a door. Instead of providing a password, you can provide a key file instead. (Or you can elect to have the volume to required both password and key file to achieve two-factor authentication.)
17. Before creating the encrypted volume – True Crypt would need to collect random data from the user. Enter 'y' to confirm that your mouse is connected to your computer.
18. Move the mouse in a random order until the counter reaches 100%. If you have selected no to the previous question – type randomly until the counter reaches 100%.
19. A “Volume Created” message will appear shortly to alert the user that the encrypted volume is ready to be use. See Figure 7-10 for installation screen shots.

```
kenwayn@kenwayn-desktop: ~  
File Edit View Terminal Tabs Help  
Selecting previously deselected package truecrypt.  
(Reading database ... 69971 files and directories currently installed.)  
Unpacking truecrypt (from truecrypt_4.3-0_i386.deb) ...  
Setting up truecrypt (4.3-0) ...  
kenwayn@kenwayn-desktop:~/Desktop/truecrypt-4.3$ which truecrypt  
/usr/bin/truecrypt  
kenwayn@kenwayn-desktop:~/Desktop/truecrypt-4.3$ cd ~  
kenwayn@kenwayn-desktop:~$ truecrypt truecrypt -c  
Volume type:  
 1) Normal  
 2) Hidden  
Select [1]: 1  
  
Enter file or device path for new volume: pc.tc  
Filesystem:  
 1) FAT  
 2) None  
Select [1]:  
  
Enter volume size (bytes - size/sizeK/sizeM/sizeG): 250M  
  
Hash algorithm:  
 1) RIPEMD-160  
 2) SHA-1  
 3) Whirlpool  
Select [1]:
```

Figure 7

```
kenwayn@kenwayn-desktop: ~  
File Edit View Terminal Tabs Help  
Select [1]:  
  
Enter volume size (bytes - size/sizeK/sizeM/sizeG): 250M  
  
Hash algorithm:  
 1) RIPEMD-160  
 2) SHA-1  
 3) Whirlpool  
Select [1]:  
  
Encryption algorithm:  
 1) AES  
 2) Blowfish  
 3) CAST5  
 4) Serpent  
 5) Triple DES  
 6) Twofish  
 7) AES-Twofish  
 8) AES-Twofish-Serpent  
 9) Serpent-AES  
10) Serpent-Twofish-AES  
11) Twofish-Serpent  
Select [1]:  
  
Enter password for new volume 'pc.tc':  
Re-enter password:
```

Figure 8

```
kenwayn@kenwayn-desktop: ~
File Edit View Terminal Tabs Help
Select [1]:

Enter volume size (bytes - size/sizeK/sizeM/sizeG): 250M

Hash algorithm:
 1) RIPEMD-160
 2) SHA-1
 3) Whirlpool
Select [1]:

Encryption algorithm:
 1) AES
 2) Blowfish
 3) CAST5
 4) Serpent
 5) Triple DES
 6) Twofish
 7) AES-Twofish
 8) AES-Twofish-Serpent
 9) Serpent-AES
10) Serpent-Twofish-AES
11) Twofish-Serpent
Select [1]:

Enter password for new volume 'pc.tc':
Re-enter password:
```

Figure 9

```
kenwayn@kenwayn-desktop: ~
File Edit View Terminal Tabs Help
 3) CAST5
 4) Serpent
 5) Triple DES
 6) Twofish
 7) AES-Twofish
 8) AES-Twofish-Serpent
 9) Serpent-AES
10) Serpent-Twofish-AES
11) Twofish-Serpent
Select [1]:

Enter password for new volume 'pc.tc':
Re-enter password:

Enter keyfile path [none]:

TrueCrypt will now collect random data.

Is your mouse connected directly to computer where TrueCrypt is running? [
y

Please move the mouse randomly until the required amount of data is captur
Mouse data captured: 100%

Done: 249.56 MB Speed: 8.33 MB/s Left: 0:00:00
Volume created.
kenwayn@kenwayn-desktop:~$ █
```

Figure 10

V. Using TrueCrypt

20. Mount the encrypted volume by supplying the path to the volume and the mount point.
(Ie: `%truecrypt /path/to/created/volume /mnt/mountpoint`)

We would mount the volume to `/mnt/pc`. To do so, we need to first create the directory and then mount the volume to that directory.

Enter the following commands:

```
%sudo mkdir /mnt/tc
%truecrypt -u pc.tc /mnt/tc
```

Enter 'tartans' as the password when mounting the encrypted volume.

21. You can now move sensitive files to `/mnt/tc` or create new files under `/mnt/tc`. Every file under `/mnt/tc` would be encrypted.
22. Enter the following commands to create a new file named sensitivefile.

```
% cd /mnt/tc
% cat > sensitivefile
```

Type "this is sensitive data" follow by control-d.

23. Type the following command to view the file:

```
%more sensitivefile
```

24. Unmount the truecrypt container when you no longer need access to the files in the volume. Once the encrypted volume is unmounted no one can access the

sensitivefile you just created in that volume (or any files in that volume) unless they know the password.

Leave the encrypted volume and dismount the truecrypt volume by typing:

```
% cd ~  
% truecrypt -d
```

This command dismounts all truecrypt volumes – if you want to be specific type use: “truecrypt -d /path/to/truecrypt/volume.” ***Remember, you cannot dismount the volume, if you are still using it. (ie: Your terminal is still in that encrypted volume). You will get an error similar to Figure 11.



```
kenwayn@kenwayn-desktop:/mnt/tc$ truecrypt -d  
umount: /mnt/tc: device is busy  
umount: /mnt/tc: device is busy  
Cannot dismount /dev/mapper/truecrypt0  
kenwayn@kenwayn-desktop:/mnt/tc$ cd ~  
kenwayn@kenwayn-desktop:~$ truecrypt -d  
kenwayn@kenwayn-desktop:~$ █
```

Figure 11