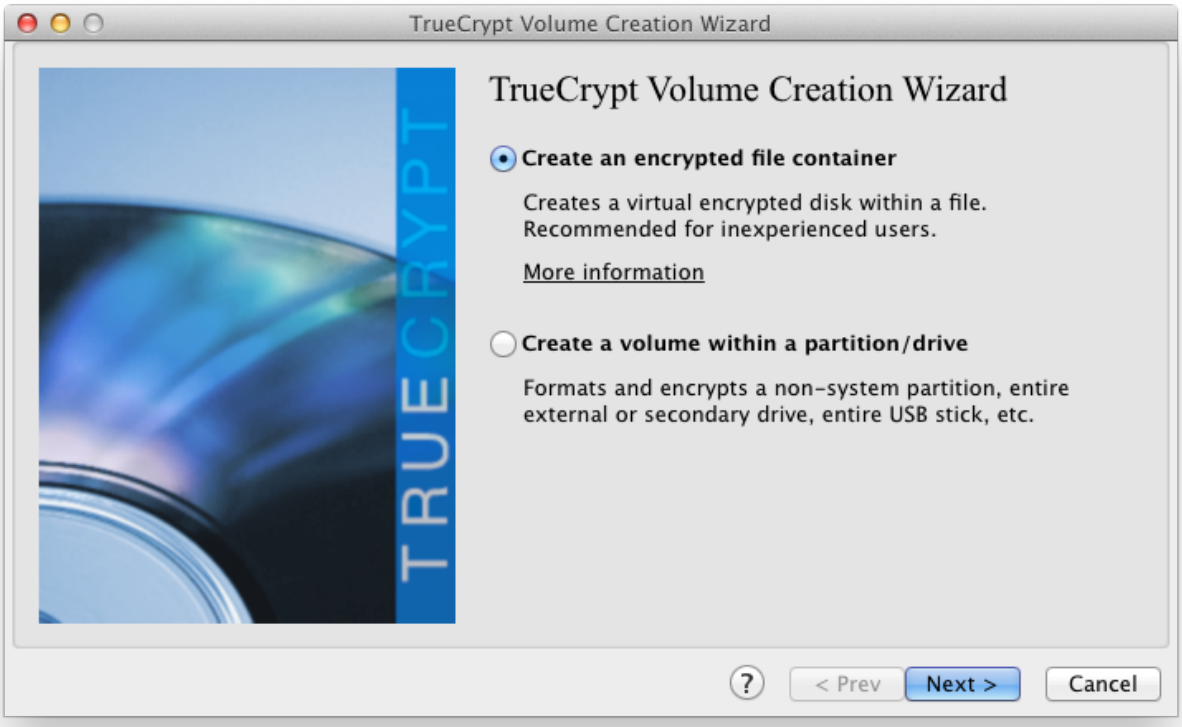
Backing-up your most valuable Data

In this previous post you found instructions, how to setup a USB-stick to contain an additional hidden encrypted partition to store valuable data on. Here you learn how to use your secured USB-stick and backing-up your most valuable data, based on a simple rsync script.

Step 1: Protect my local Data: Yes or No?

The first question is, whether you consider your local data on your PC / Mac to be secured enough to prevent unauthorized access or not. Since we are using laptops which are known to be portable, we consider the data to be unsafe. If you are positive, that no unauthorized user can access your computer, make sure all your valuable data is stored in a specific folder and proceed to step 2 of this tutorial, otherwise read on.

The aim of this step is to create a new local encrypted filecontainer which lateron can be mounted as a local encrypted drive. This container has to be big enough to fit on your USB-stick and to contain your valuable data. It must be slightly smaller or equal the space on the hidden USB-partition created before. To to this, follow the steps of our previous post, but instead of creating a volume within a partition/drive, choose the option 'create encrypted file container'.



Then choose 'Standard TrueCrypt volume' (unless you are really paranoid and want to have a

fake drive which would be exposed by mounting the file with another password, not unveilling the secret data but rather showing some uninteresting or fake-secret content you don't care to present to any alice as well as bob).

Now select the volume location. Make sure, your (loca) harddrive provides enough space to fit another big file in the size of your hidden USB-Stick partition, prepared in the other post. Then repeat the steps as described under 'Encryption Options'.

After having finished this step, you should have three newly created devices on your desktop:

- one small unencrypted drive on your USB-stick (visible to anyone plugging in the stick)
- one larger hidden and encrypted drive on your USB-stick
- one large encrypted drive in a file on your harddrive

Step 2: Create your rsync-Script

In this step we want to create a simple rsync script which copies the data from your local location to the stick. Everytime when running the script, all your local data found under a given directory will be synchronized to your USB-stick. All changes applied to your stick will be overridden, data is only synchronized in one direction from PC / Mac to USB-stick.

Determine your top source folder
If you decided to store your valuable files locally in an encrypted filecontainer, you will have to mount it previously to run the script. Within TrueCrypt, select the filecontainer on your local harddrive, select a free slot from the volume-list, click the 'Mount'-button and enter the password/select the keyfile. After having successfully mounted your filecontainer, you'll see a new drive icon on your desktop and your *top source folder* would be something like

```
'/Volumes/SOURCE_SEC_DATA/'
```

given SOURCE_SEC_DATA was the devicename you assigned to your filecontainer. Otherwise, if you did decide against encrypting you local files, you'll simply have a predefined folder, whose content you want to have recursively copied to the secured USB-stick. Your *top source folder* would then be something like

```
'/Users/UserName/PrivateData/'
```

given *UserName* is your name and *PrivateData* the name of the folder in your user-home where you have moved all your valuable data into.

Determine your top destination folder

Our destination folder will be the top-level of our mounted hidden partition on our USB-stick, which we have already prepared in the previous post. Within TrueCrypt, select the partition on your USB-stick connected, select a free slot from the volume-list, click the 'Mount'-button and enter the password/select the keyfile. After having successfully mounted your hidden partition, you'll see a new drive icon on your desktop and your *top destination folder* would be something like

```
'/Volumes/DEST_SEC_DATA/'
```

given SEC_DATA_STICK is the devicename you assigned to your device contained in the hidden partition on your USB-stick.

Write your shell script
With the preparation steps from the last section, your shell script should look something like:

The --delete option tells rsync to delete any file on the destination folder (on your USB-stick), which have previously been removed from your source folder. If you do not want to have files removed from your USB-stick, remove the '--delete' section from the statement. **Attention: Be careful to provide the rsync - parameters in the correct order and always check your script against a set of dummy files prior to run it for the first time.**

Make your script runnable
Store your script on your desktop with a name like 'doSomeThing.command'. **From the commandline run**

Congrats! Now you can see the script on your desktop and can rename it or add a nice icon to it. After clicking your icon, all delta are synched from your source-folder to your destination-folder.