

***Your document should have the following information:***

1. Name: Jennifer Paparelli
2. Date: March 21, 2012
3. Assignment #6a Instructional Blog
4. URL of Instructional Blog:

Content for the instructional blog (images plus actual text so that we can review and comment using Track Changes)

Screenshots of the instructional blog on your Interactive Resume

**NOTE:** Name the file: Lastname\_FirstInitial\_Assign#6.docx

<http://www.webcitation.org/query?url=g1.globo.com/English/noticia/2010/06/not-even-fbi-can-de-crypt-files-daniel-dantas.html>

## **ENCRIPTING A USB DRIVE WITH TRUECRYPT**

Use Easy Bib and make a bibliography

### **Intended audience**

Anyone at any skill level looking for their information on a USB stick to be safe.

### **How Does This Work?**

TrueCrypt creates and maintains on-the-fly encryption to any drive (cd, DVD, hard drive, USB). The files are automatically encrypted when the user clicks save. Files are automatically decrypted when you open them.

In order to work with your files, you must mount (connect) the drive. This is for safety, if you shut down or restart your computer, the drive will unmount, (disconnect) even if it is still plugged in. To use them, you must mount the drive. After you have mounted the drive, you are able to use the decrypted data on the drive (volume) by entering your password. Without the correct password, data cannot be read.

### **In order to encrypt a USB stick, you will need:**

- A USB stick
- A Macintosh or Windows computer
- TrueCrypt program installed to your computer (<http://www.truecrypt.org/downloads>)

## Things to think about before you encrypt your drive:

### *Would you like to encrypt the entire USB drive or just one folder?*

Encrypting the entire drive will mean you need TrueCrypt installed on every machine you wish to view the files on. Benefit: if you lost your USB drive, no one can view your files without your password AND the program installed.

Encrypting only a folder requires you to have TrueCrypt installed and your password to view files in that folder. Benefit: you can still use the other files/folders on the USB on any machine without TrueCrypt, but if you lose the USB stick, only files in the encrypted folder are protected, any not in the folder are public.

### *Be careful not to lose existing data.*

Backup your data currently on the drive to your desktop. Create a folder on your desktop; you can leave it as untitled. Drag all the items from the flash drive into the folder on the desktop.

### *Do you want a hidden volume?*

A hidden volume is a TrueCrypt volume (inner) created in another TrueCrypt (outer) volume. When you mount the outer volume, it is impossible to know if there is a hidden (inner) volume within the free space on any drive encrypted by TrueCrypt.

When a volume (outer) is created, any blank space left is filled with random data, because of this, even a dismounted hidden volume is not seen because it looks the same as the random data.

## Tutorial

Step 1: Download TrueCrypt; open the program TrueCrypt from Start, Programs

Step 2: The wizard appears, Select, Create Volume

Step 3: You have a decision; you can encrypt the entire drive, or choose to encrypt a container (folder). *Be warned, if you encrypt the entire thing, it will reformat your drive and you will lose everything.* This is why we backed it up to your desktop to be copied back after encryption is complete.

- After encrypting the entire drive, you will need to download TrueCrypt on every computer you plan to use this drive on. It's easy to do.
- Once you decide, click next.

Step 4: Volume type, select standard and then next

Step 5: Volume Location, select file, select the flash drive

Step 6: Skip, you did this in Step 5

Step 7: Select next if your flash drive is in the drop down box

Step 8: Encryption options. I chose Twofish and SHA-512.

Step 9: Volume Size. I encrypted my entire drive, which is 2.2 Gigs.

- Go for the max rounded to the nearest whole number. For mine, I entered 2.

Step 10: Create a password you will remember. Using \*@#.\$ and uppercase letters makes it harder for them to crack. As does a 20 character password. Then select next.

Step 11: Formats. FAT32 is good for Windows, the drop down allows for Mac also.

- Click format. This takes a few minutes.
- Once it is complete, it will pop up a box, click okay.

Step 12: Volume created comes up, click exit.

Step 13: Now you need to mount the drive.

- Choose any letter and select by clicking on it.

Step 14: Select file

Step 15: Find the flash drive (probably on your desktop or in my computer), select open

Step 16: click Mount

Step 17: Enter your password

Step 18: Click okay

Step 19: Click exit

Step 20: Open the flash drive from your desktop or in my computer and drag the files from the unnamed folder you copied everything into back to the flash drive.

## **Working With Your Encrypted USB Stick**

*\*Remember: To use this drive on other computers: you must have TrueCrypt installed.*

Mounting:

Unmounting:

Problems? <mailto:jep10f@my.fsu.edu>Contact me</>

Resources and advanced data encryption: [www.truecrypt.org](http://www.truecrypt.org)