

# Non-Identifiable Encryption of Flash Drives



- Anti Forensics

How to Encrypt a device in a way which makes it seem as if it was securely overridden.

# What?



In this tutorial I will show you step by step how to securely encrypt your flash drives in a way which has no headers so it is impossible to crack just with your Flash Drive; This will make your Flash Drive seem as if it has been filled with random data.

# Why?



Why? You may ask...

Well its kind of simple, say you have some very very bad and incriminating files that could put you away for life.

Now would you use TrueCrypt? Sure you could but the way that TrueCrypt stores the keys to decrypt its data makes it possible to grab the header and just attempt to crack that until you find the identifiers I think FF-Key-FF or something like that.

# Why Cont...



Ok so maybe Ill just use the DM-Crypt/luks Encryption that comes with Ubuntu. Won't that protect me? No if you look in the device with a hexeditor you will see the LUKS header, along with the hashes of your passwords/keys. So someone could just attempt to crack your hash.

Also neither of those options allow for in-place encryption so you don't have to copy any files onto your computer. Just hope that you do not lose power because that may lead to power loss.

# Why Cont...



Ok so what can we do? Well we can use CryptSetup to make a mapping with a layer of encryption...

Ok so again, say you have those bad bad files and don't want to have to get rid of them.

You do this and everything in the drive looks random and can not be proven to be encrypted.

So a forensics person takes your flash drive and puts it into their Computer(more than likely Windows lol) and uses a program to look for strings or deleted files

# Why Cont...

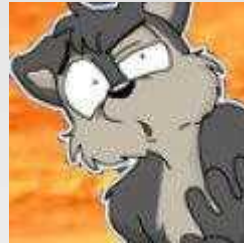


Which there are none because we will be encryption all data in place so it will take all the old data like deleted files and encrypting them.

So no matter what they do to look at the drive its self they will get no information from it.

The only real danger with my method is that you will have to use sudo... When you use a sudo command a log is kept in your log files, which if you want you can shred and then you will be safe.

# Tutorial





Allright you got this far so lets get down to the commands and protecting your data.

Lets open up a Terminal (Ctrl+Alt+T).

Now we need to figure out what the device is called /dev/sdb, /dev/sdc, etc.

```
sudo fdisk -l
```

Find your device, for me it is /dev/sdb

Now we need to make sure that the partition is not mounted.

```
sudo umount /dev/sdb1
```

Once your Flash Drive is unmounted we can start to encrypt everything that was on it.



Ok so at this point your flash drive is in your computer, and is not mounted so we can read/write data to it freely.

Now Lets encrypt everything lol...

```
sudo cryptsetup -c aes-cbc-essiv:sha256 -h whirlpoo -y create FD /dev/sdb1
```

Now you need to choose a strong password that someone would not be able to guess.

Now you need to type in this code to transfer the original data to the encrypted device.

```
sudo dd if=/dev/sdb1 of=/dev/mapper/FD bs=1M
```

Now let dd run and once it is finished you should test it out to see if you can mount the encrypted device.



Lets change into our Desktop...  
`cd ~/Desktop/`

Lets make a test directory...  
`mkdir tmp`

Mount out encrypted Device...  
`sudo mount /dev/mapper/FD tmp`

Now in your computer go to the tmp folder that is on your desktop and inside of it you should see the files that were in the old partition.

If you want added security to make the device even more secure...  
`cd tmp`

Repeat this command and when it finishes change the of by one like AAAAA  
AAAAB AAAAC etc  
`dd if=/dev/urandom of=AAAAA bs=1M count=100`

Untill the device or full, if yopu get to a point of where there under 100MB of free space change the 100 to what ever lol.



Once all the free space is gone delete those AAA files.  
Now you can unmount the encrypted device.

```
Cd ..  
sudo umount tmp  
rmdir tmp
```

Now lets close the encrypted device.  
sudo cryptsetup remove FD

And finally eject the device.  
sudo eject /dev/sdb

Woot now our device is ready lol... Now all you have to do to access the data on your partition is to repeat the steps to mount it so...

```
sudo cryptsetup -c aes-cbc-essiv:sha256 -h whirlpool -y create FD /dev/sdb1  
mkdir tmp  
sudo mount /dev/mapper/FD tmp
```

Then to close it out again...  
sudo umount tmp  
sudo cryptsetup remove FD  
sudo eject /dev/sdb

# Non-Identifiable Encryption of Flash Drives



The End

By KenTheFurry

Email: [KenTheFurry@gmail.com](mailto:KenTheFurry@gmail.com)

GPG Key: 068ACDD2