# GNU/Linux Administration - Bug #409

## Recovering Files From A LUKS and eCryptfs Encrypted Filesystem

07/07/2014 12:34 PM - Daniel Curtis

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 07/07/2014 |
| **Priority:** | Immediate | **Due date:** | |
| **Assignee:** | Daniel Curtis | **% Done:** | 100% |
| **Category:** | | **Estimated time:** | 8.00 hours |
| **Target version:** | | **Spent time:** | 8.00 hours |

**Description**

I've encountered a problem where I have lost my USB booloader used to boot into my primary OS; which consists of two LUKS encrypted partitions, one for / and one for /home. Not only were the partitions encrypted, but also the user folders via ecryptfs. Luckily, I was not ultra-paranoid and only used a passphrase with LUKS and not a passphrase/keyfile combination. To begin I booted into a live ubuntu environment and dropped into a root shell:

```
sudo su
```

## Open and mount the LUKS containers

- First open up the LUKS encrypted partitions:

  ```
  cryptsetup luksOpen /dev/sda5 root
  cryptsetup luksOpen /dev/sda6 home
  ```

  NOTE: This will prompt for a passphrase. Recovering the passphrase is beyond the scope of this guide.

- Next, mount the mapped partitions:

  ```
  mount /dev/mapper/root /mnt
  mount /dev/mapper/home /mnt/home
  ```

- Mount the device, process, and system mountpoints:

  ```
  mount --bind /dev /mnt/dev
  mount --bind /sys /mnt/sys
  mount --bind /proc /mnt/proc
  ```

## Mount the Read-Only eCryptfs

Now that I had access to both my root and home partitions, I needed to recover my personal files. These were encrypted using ecryptfs, and it just so happens there is a tool just for recovering ecryptfs partition.

- From the root terminal, run the recovery command:

  ```
  ecryptfs-recover-private
  ```

  This will prompt a few questions including the login passphase of the user's directory that recovery is ran on. Once the recovery is complete, a read-only version will be available.

## Transfer the files to another machine

Now that I had access to my files, I used rsync to backup my files to another machine:

```
cd /tmp/ecrypt.63f8g4
rsync -avh --progress -n . -e ssh user@backup.example.com:/path/to/backup/folder
```

NOTE: Make sure to remove the -n flag to remove the 'dry-run' option.

## Resources

- http://citizen428.net/blog/2011/10/17/fixing-grub-on-a-luks-encrypted-disk
- https://help.ubuntu.com/12.04/serverguide/ecryptfs.html
- https://help.ubuntu.com/community/EncryptedPrivateDirectory

### History

**#1 - 07/07/2014 02:09 PM - Daniel Curtis**

*- Description updated*

**#2 - 07/08/2014 08:30 AM - Daniel Curtis**

*- Description updated*

*- Status changed from New to Resolved*

*- % Done changed from 30 to 100*

**#3 - 08/15/2014 03:02 PM - Daniel Curtis**

*- Status changed from Resolved to Closed*