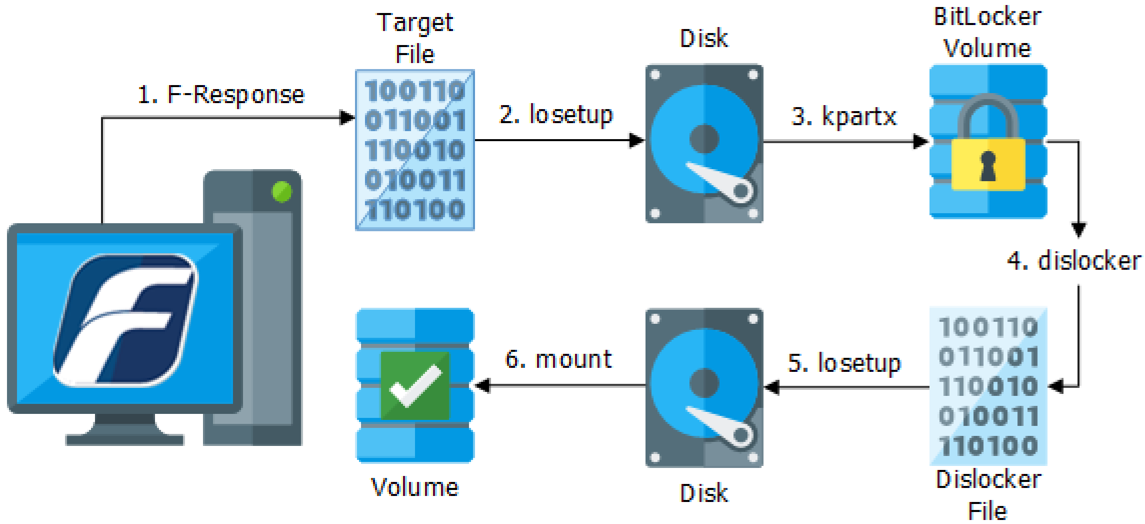
Mount a BitLocker Volume on Linux

Overview

Step 1: Mount the Disk containing the BitLocker Volume 1
Step 2: Mount the Target File 2
Step 3: Mount the BitLocker Volume 2
Step 4: Mount the BitLocker Volume with Dislocker 2
Step 5: Mount the Dislocker File 3



Step 1: Mount the Disk containing the BitLocker Volume

Mount the disk containing the BitLocker volume with the F-Response Management Console or Accelerator. A target file representing the disk will be created on the mount path.

```
$ fr_exa cache
name,platform,url,version
"x64-win10-sub","Windows 10","192.168.1.64:3262/sub","7.0.4.4"
$ fr_exa cache -s x64-win10-sub
name,block_size,block_count,pid,mount_path
"disk-1","512","10485760","0",""
"disk-2","512","10485760","0",""
"vol-C","512","82857984","0",""
"pmem","4096","524288","0",""
"disk-0","512","83886080","0",""
$ fr_exa mount -s x64-win10-sub -t disk-1 -m ~/Desktop -d
F-Response Linux Examiner 7.0.4.4
Copyright F-Response, All Rights Reserved
```

```
Connected to subject 192.168.1.64:3262/sub.
Connected to target disk-1.
Exported target on /home/jching/Desktop/x64-win10-sub/disk-1.
Examiner worker is online and running in  the background.
Exclude -d,--daemon on command line to run in foreground.
```

Step 2: Mount the Target File

Mount the target file on a loopback device, such as /dev/loop0. The loopback device presents the target file as a block device. And the block device provides an interface for disk utilities and forensic tools.

```
$ sudo losetup /dev/loop0 x64-win10-sub/disk-1/disk-1
$ sudo losetup -a
/dev/loop0: [0041]:2 (/home/jching/Desktop/x64-win10-sub/disk-1/disk-1)
```

Step 3: Mount the BitLocker Volume

Find the BitLocker Volume by dumping the partition table with a disk utility or forensic tool, i.e. fdisk or mmls.

```
$ mmls /dev/loop0
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0010481663   0010479616   NTFS / exFAT (0x07)
003:  -------   0010481664   0010485759   0000004096   Unallocated
```

Mount the block device using kpartx. kpartx presents the BitLocker volume as a block device, i.e. /dev/mapper/loop0p1.

```
$ sudo kpartx -a /dev/loop0
$ sudo kpartx -l /dev/loop0
loop0p1 : 0 10479616 /dev/loop0 2048
```

Step 4: Mount the BitLocker Volume with Dislocker

Mount the BitLocker volume using dislocker. dislocker presents the volume as a dislocker file.

```
$ mkdir unlockbt
$ sudo dislocker -V /dev/mapper/loop0p1 -p680724-390104-007722-262328-351186-
340417-246906-306724 unlockbt
$ sudo ls -l unlockbt
total 0
-rw-rw-rw- 1 root root 5365562880 Dec 31  1969 dislocker-file
```

Step 5: Mount the Dislocker File

Mount the dislocker file on another loopback device, such as /dev/loop1. Then mount the loopback device to present the filesystem.

```
$ sudo losetup /dev/loop1 unlockbt/dislocker-file
$ mkdir vole
$ sudo mount -o ro /dev/loop1 vole
$ ls -l vole
total 8
drwxrwxrwx 1 root root    0 Jun 28  2017 $RECYCLE.BIN
drwxrwxrwx 1 root root 4096 Jan 12 12:47 System Volume Information
drwxrwxrwx 1 root root 4096 Jun 28  2017 TestingDataset
```