

Using RecoverJpeg to Recover Deleted JPGs

Adithya Bhaskara

RecoverJpeg is a built-in tool in Kali Linux that allows the user to recover deleted files in many different file formats.

For Removable Media

1. Run `\fdisk -l` in the terminal, this will list all disks connected to the operating system
 - a. This includes the virtual hard disk and any other removable media (USB Sticks, CDs, SD Cards, etc.)
2. Look for the device of the removable disk. In this case, it is `/dev/sdb1`

```
root@kali:~# fdisk -l
Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Virtual Disk for VM

Disk /dev/loop0: 2.9 GiB, 3071234048 bytes, 5998504 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
A Loop Device

Disk /dev/sdb: 28.9 GiB, 31016878080 bytes, 60579840 sectors
Disk model: USB Flash Drive
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Removable Media
Disklabel type: dos
Disk identifier: 0xd82e54fb

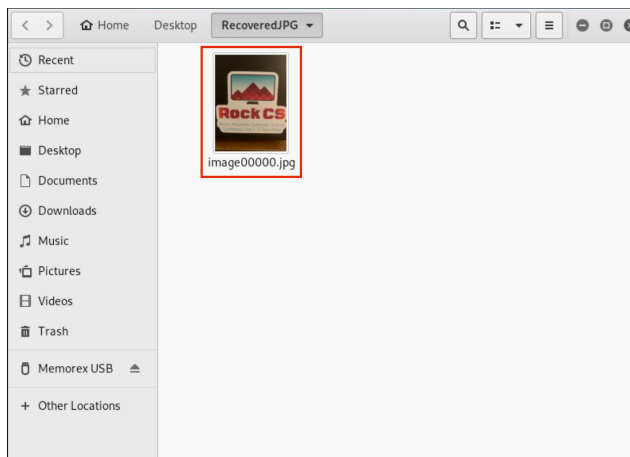
Device      Boot Start      End  Sectors  Size Id Type
/dev/sdb1   8064 60579839 60571776 28.9G  c W95 FAT32 (LBA)
root@kali:~#
```

3. Create a new directory in `/root/Desktop` called 'RecoveredJPG':
 - a. `\mkdir /root/Desktop/RecoveredJPG'`

4. Run `recoverjpeg -h` to get all the arguments foremost can take

```
root@kali:~# recoverjpeg -h
Usage: recoverjpeg [options] file|device
Options:
  -b blocksize  Block size in bytes (default: 512)
  -d format     Directory format string in printf syntax
  -f format     File format string in printf syntax
  -h           This help message
  -i index     Initial picture index
  -m maxsize   Max jpeg file size in bytes (default: 6m)
  -o directory Restore jpeg files into this directory
  -q           Be quiet
  -r readsize  Size of disk reads in bytes (default: 128m)
  -s cutoff   Minimal file size in bytes to restore
  -S skipsize  Size to skip at the beginning
  -v           Be verbose
  -V           Display version and exit
root@kali:~#
```

- a. Lets run `recoverjpeg` with input from `/dev/sdb1`, lets set the output directory to `/root/Desktop/RecoveredJPG`
5. Run `recoverjpeg` with all desired arguments, in this case, `recoverjpeg /dev/sdb1 -o /root/Desktop/RecoveredJPG`
6. Navigate to `/root/Desktop/RecoveredJPG` to see the files. You may use the GUI to view them. This may also be refreshed as the process continues



FOREMOST GUIDE
