

[HOME](#)[THE FORUM](#)[SUBSCRIBE!](#)[VIDEOS](#)[WRITE FOR US](#)[PRIVACY](#)[TERMS](#)

Disk Management

How to do data recovery from hard drive

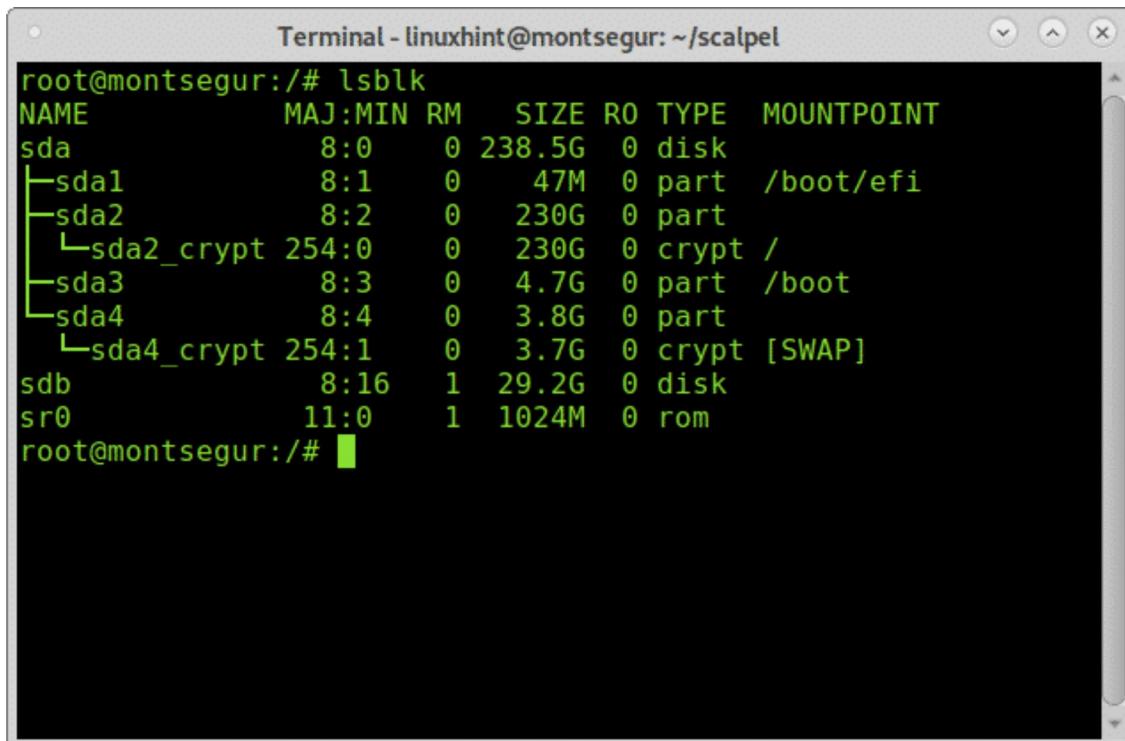
1 week ago • by Ivan Vanney

This tutorial shows how to recover data from storage devices in Linux. In this case the data will be recovered from a SanDisk USB pendrive of 32 GB, yet the process shown in this tutorial is the same as for a regular hard disk. This tutorial will focus on two of the most popular file carving tools, Foremost and PhotoRect, both described in the [File Carving Tools](#) article. Both of them will be explained from the installation process on Debian 10 Buster to data recovery.

Data Recovery From Hard Drive with Foremost:

To begin lets see the connected storage devices by using the command ***lsblk***, on the console run:

```
# lsblk
```



A screenshot of a terminal window titled "Terminal - linuxhint@montsegur: ~/scalpel". The window displays the output of the "lsblk" command. The output shows the following disk information:

NAME	MAJ:MIN	RM	SIZE	R0	TYPE	MOUNTPOINT
sda	8:0	0	238.5G	0	disk	
└─sda1	8:1	0	47M	0	part	/boot/efi
└─sda2	8:2	0	230G	0	part	
└─sda2_crypt	254:0	0	230G	0	crypt	/
└─sda3	8:3	0	4.7G	0	part	/boot
└─sda4	8:4	0	3.8G	0	part	
└─sda4_crypt	254:1	0	3.7G	0	crypt	[SWAP]
sdb	8:16	1	29.2G	0	disk	
sr0	11:0	1	1024M	0	rom	

The terminal prompt is "root@montsegur:~#".



Lsblk will show all available storage devices and partitions, including swap and optical devices, in this case I want the sdb device.

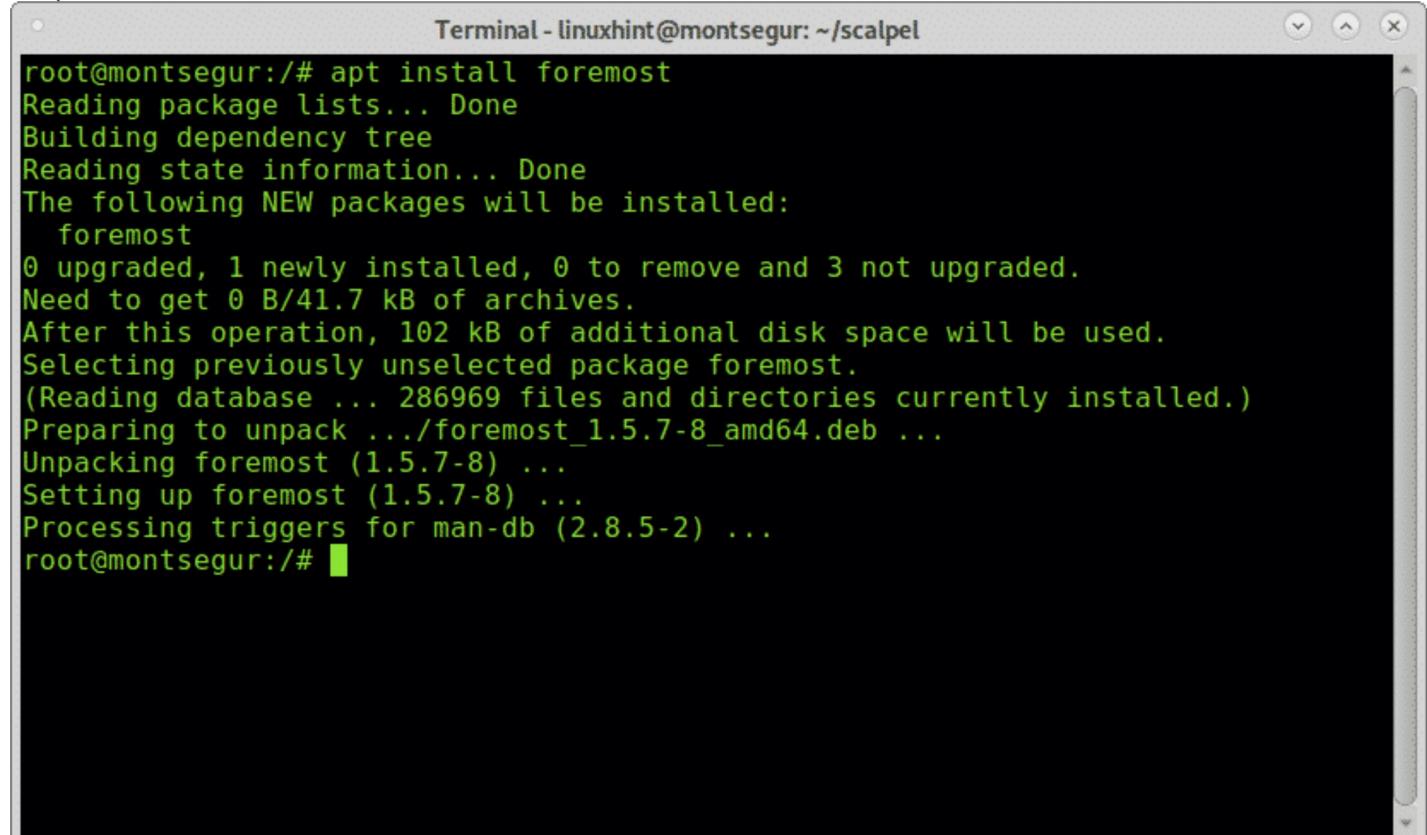
Note: to learn more on the lsblk command read [How to List all Linux Disk Devices](#).

As you can see the 32 GB USB pendrive was called **sdb** and that's the device I'll work on.

Data Recovery from USB drive with Foremost:

To begin data recovery from a USB drive start by installing Foremost using the APT package manager on Debian or based Linux distributions by running:

```
# apt install foremost
```

A screenshot of a terminal window titled "Terminal - linuxhint@montsegur: ~/scalpel". The window shows the output of the apt install foremost command. It starts with "root@montsegur:/# apt install foremost", followed by the package manager's processing steps: "Reading package lists... Done", "Building dependency tree", "Reading state information... Done", and "The following NEW packages will be installed: foremost". It then shows the download and unpacking process: "0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.", "Need to get 0 B/41.7 kB of archives.", "After this operation, 102 kB of additional disk space will be used.", "Selecting previously unselected package foremost.", "(Reading database ... 286969 files and directories currently installed.)", "Preparing to unpack .../foremost_1.5.7-8_amd64.deb ...", "Unpacking foremost (1.5.7-8) ...", "Setting up foremost (1.5.7-8) ...", and "Processing triggers for man-db (2.8.5-2) ...". The command concludes with "root@montsegur:/#".

Once installed you can display the man page to check all available options:



```
# man foremost
```

Terminal - linuxhint@montsegur: ~/scalpel

FOREMOST(8) System Manager's Manual **FOREMOST(8)**

NAME

foremost - Recover files using their headers, footers, and data structures

SYNOPSIS

```
foremost [-h] [-V] [-d] [-vqwQT] [-b <blocksize>] [-o <dir>] [-t <type>] [-s <num>] [-i <file>]
```

BUILTIN FORMATS

Recover files from a disk image based on file types specified by the user using the **-t** switch.

- jpg** Support for the JFIF and Exif formats including implementations used in modern digital cameras.
- gif**
- png**
- bmp** Support for windows bmp format.

Manual page **foremost(8)** line 1 (press h for help or q to quit)

From the man page we understand the flag **-i** is to determine an input file, from which Foremost will start working. It is usually aimed to work with images such as these produced by tools like dd or Encase. To launch Foremost in the simplest way without additional flags run the following command replacing /sdb for the device ID you want to recover data from.

Run:

```
# foremost -i /dev/sdb
```

Where **sdb** put the correct device.

Once executed the carving process will look like:

Terminal - linuxhint@montsegur: ~/scalpel

```
00D666A,A60160/{0b6666666666}0D6669w=005k898,IR666666666666{660          0@p666 0d666T0[-666M0`y0`6X,603cVM0|0-NKE0f26664KeU00{0666+0j0^0
0|0oNc0:0iT80q0|F65600Sp c0I666@ 66k86F60!666M66 666 Y0qr@A2'6c+6X|'P
0)66苔66;66ya660c0hN066a=C0'W'66s9]66n66d696 ]-6[664L60U6666K668L]66C6648=2:66?966766666]c6666;UP
vLundat=jsloader/resource/gre/modules/services-sync/status.js@Y0o6666;667^0$#
    nIX#
0Zs6666w?0,_s-u66WG66666},K0J66HhZ66R6o6CB666G\6V6H6JU66666-g0]6i
    666666B66斐 667x-66;eS66666FF,0,6uA^X%6T0/[166m6k6x6s66Q((<w0<J67666p6
0/0dH6E66Rq0A 6666 = 0-60666-Neh666'66]66666!{66(A66GM666666To?@66B6HCV66 66" py6w ?p6
foundata=jsloader/resource/gre/modules/services-sync/telemetry.js@<ip'0=6F0eY0/a<66a666,6X6k,6 68#4xfZ666!0cI'00!Eb0s66663me66666[61666
    a76666W66666,{z{Z666T666-6[66{_,EQZ]66KY6n6M77e/6>6m@{U66j6YR 66F66\66Z66h66,666^0<66466666-666;n6K=666666666K/0
66D:66U666{66616F666}6Y66j6S666u+j61df696t66LGX6
    66|666z
    66.6+6W66616
```



```

,0@0F0p 00v03h0000
SU-00[bb]0\{000000\0~900u00z0~C7[BC0d,q70001=X0000Z60000v0p+0
07'N<0r?b&00C00kp[04\n60n0T20n0T0n0T30015
      S0c0Sw$sp0     0C0010;G0=0{06L0000
      S000S01X00_0000uV0`0w0:0+000R_0+1u00`j30000T'0000U00SK100Y
A000(H0)0
000V00000009g000=j0..900000000vv00iw0;0;vkt/]0001000=00000Yk0[E0y#00=0u00B)m0NH500000010 0000=v60g0C0hd#00
0q+000|00U00000;0:5K000 00000YC00000)0.00i00Z00Z0w0000000>H0^0{01=0000]000L030010uv0uv0000aS0Y7`0-000%W
2000f0vj0]0Z00D00.0n0{0o00000g:/Y<00000/0000
    7^000Bh^h0?0v0000}x=00cx00z00`0|U0K00[00000K0X000CG000{l000
Yc04R0500*U000*0<0N0f0Z)bp0,000000[000Jd0W!0H0Vh00`00..3000M000000vK00000f=7p00Y0j0w|00cg0T)00L0001P>^0o
foundat=jsloader/resource/gre/modules/sessionstore/Utils.jsm0W0oU00>0}/m.*!0t00Y
0E;30:0       000e0d<00A0e^0:
b00..-0!000v0ff000*00IH06
0"00/0I0       00*hb0 00H00-030sgf(w0K0dM(0;000y0108n00x00000(00000
*****
root@montsegur:/#

```

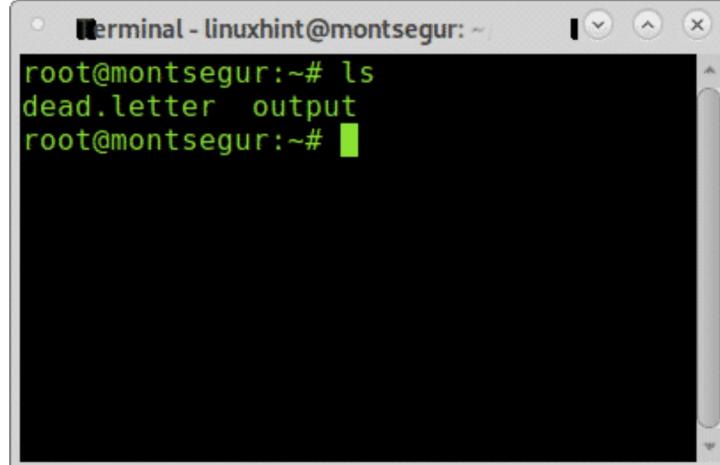
▷ X



Note: you can also specify partitions like for example /dev/sdb1.

When the process ends run **ls** to confirm the creation of a new directory called **output**:

ls



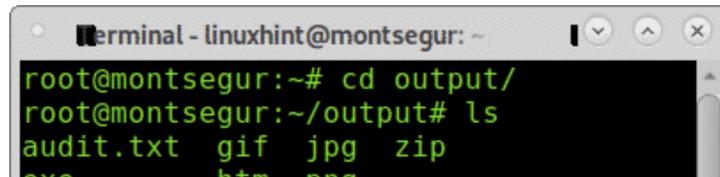
```

Terminal - linuxhint@montsegur: ~
root@montsegur:~# ls
dead.letter  output
root@montsegur:~#

```

As you can see the directory **output** exists, to see the recovered files enter it using the command **cd** (Change Directory) and then run **ls**:

cd output
ls



```

Terminal - linuxhint@montsegur: ~
root@montsegur:~# cd output/
root@montsegur:~/output# ls
audit.txt  gif  jpg  zip
exe        htm  png

```

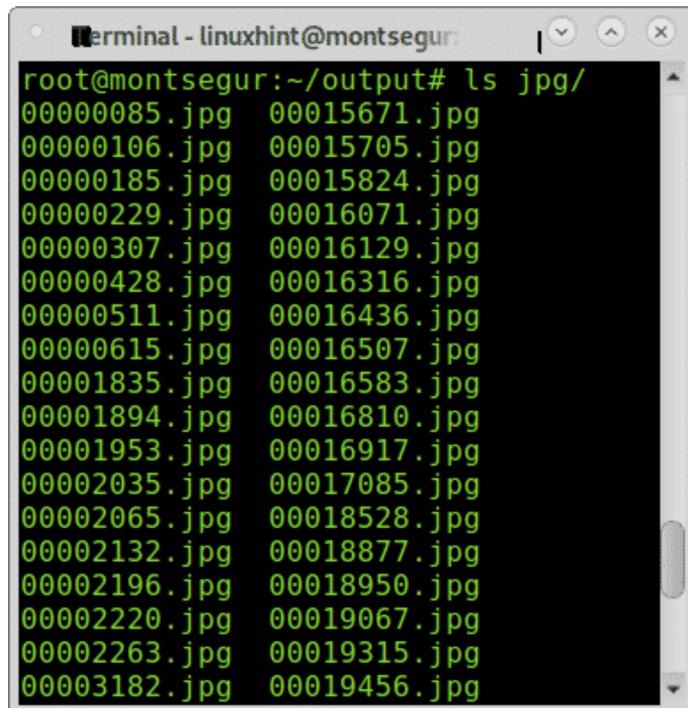


Inside you'll see directories for all file types Foremost managed to recover, additionally you'll see a file called audit.txt with a report on carved files.

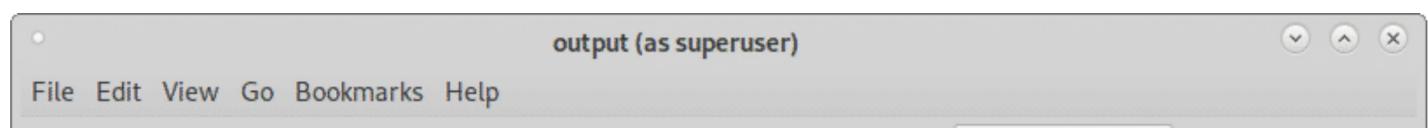


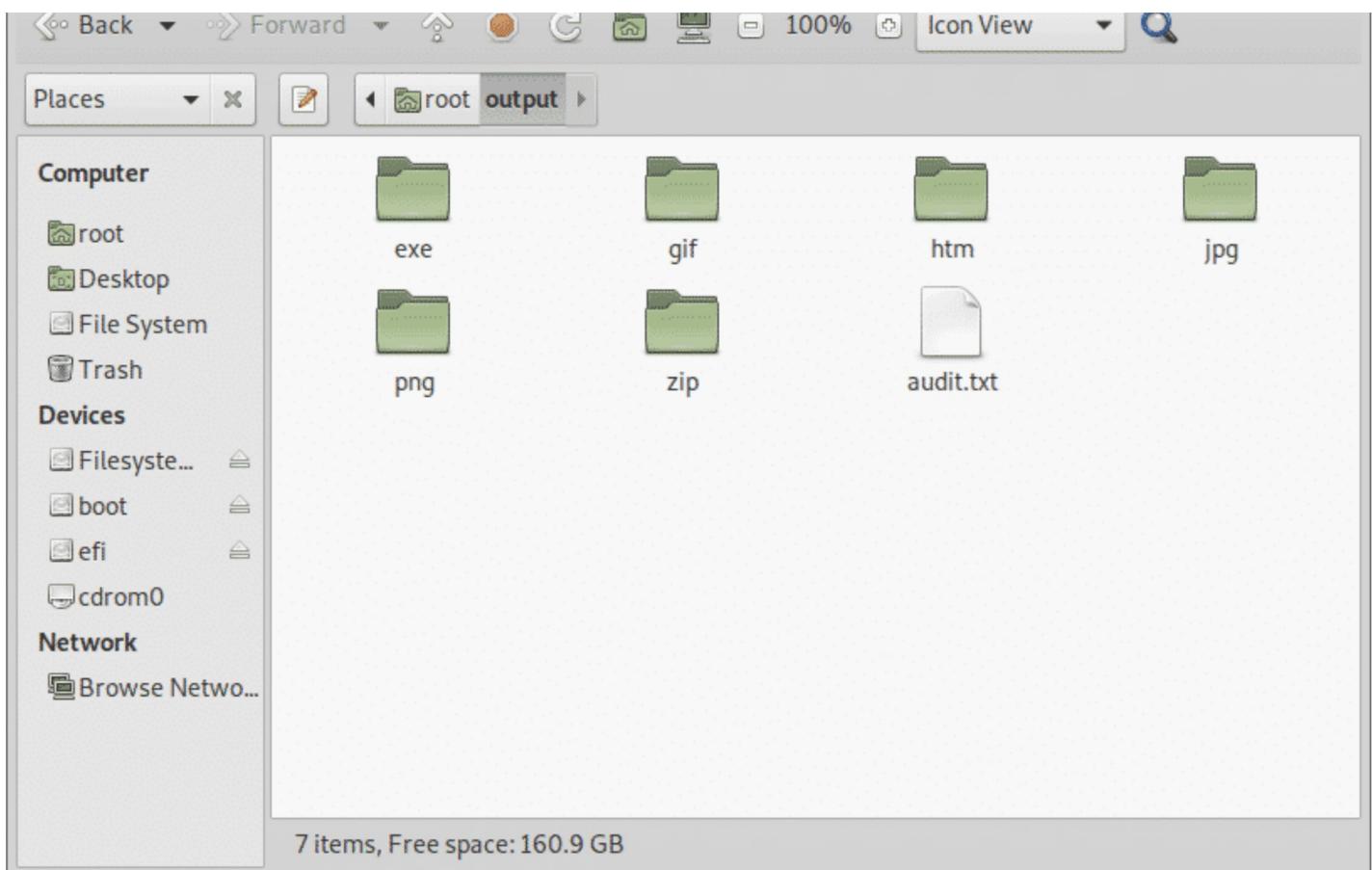
You can check what files were found inside each directory by running `ls <directory>`:

```
# ls jpg/
```



You can also browse all recovered files through a graphical file manager:





Data Recovery From Hard Drive with PhotoRec:

PhotoRec is together with Foremost the most popular file carving or data recovery tool both for professional forensics and domestic use. While Foremost does a smarter recovery showing a faster performance, PhotoRec's brute force shows better results when carving files. This section shows how to carry out data recovery from hard drive using PhotoRec.

To begin on Debian and based Linux distributions install photorec by running:

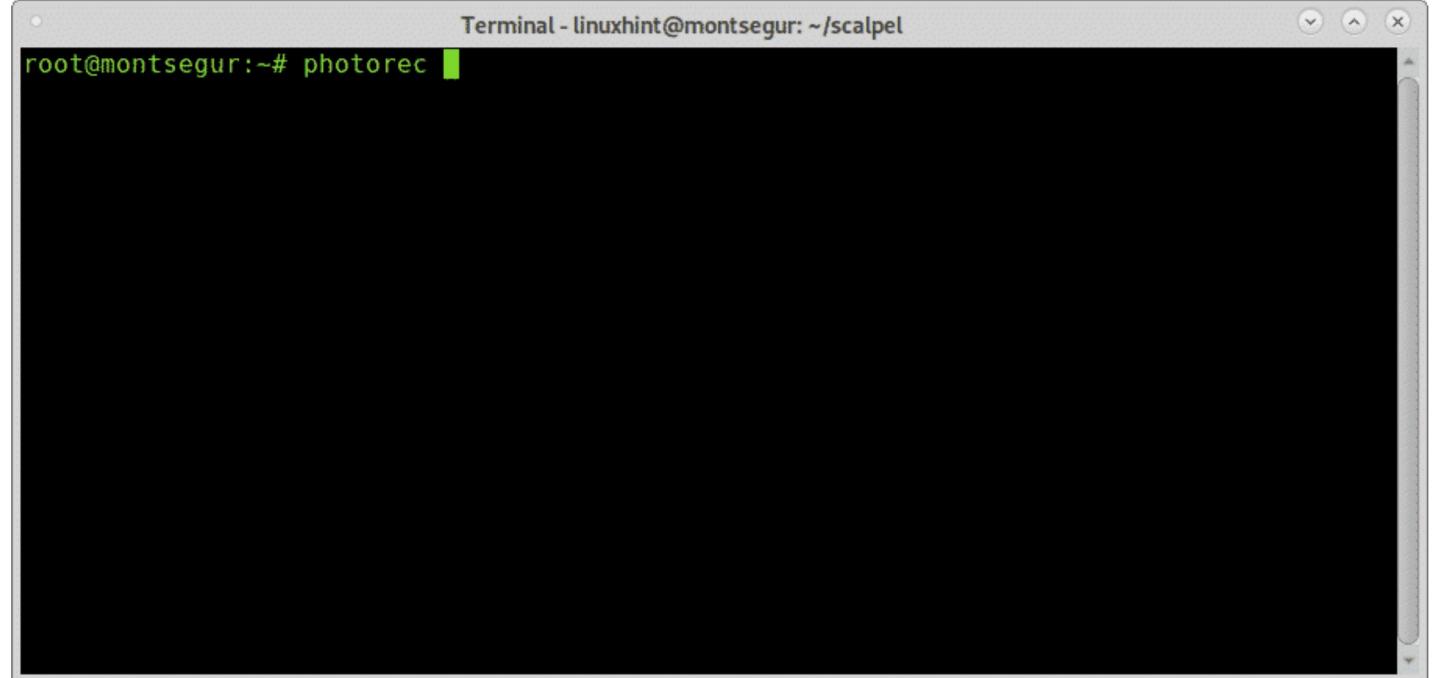
```
# apt install testdisk
```

```
Terminal - linuxhint@montsegur: ~/scalpel
root@montsegur:~# apt install testdisk
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  testdisk
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 388 kB of archives.
After this operation, 1,371 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian buster/main amd64 testdisk amd64 7.0-3+b4 [388 kB]
Fetched 388 kB in 0s (1,577 kB/s)
Selecting previously unselected package testdisk.
(Reading database ... 286977 files and directories currently installed.)
Preparing to unpack .../testdisk_7.0-3+b4_amd64.deb ...
Unpacking testdisk (7.0-3+b4) ...
Setting up testdisk (7.0-3+b4) ...
Processing triggers for man-db (2.8.5-2) ...
root@montsegur:~#
```

PhotoRec man page is almost empty, Photorec is pretty simple to use and only needs to be executed, a didactic friendly interface similar to the one of CFDISK will show up to guide you during the whole process.

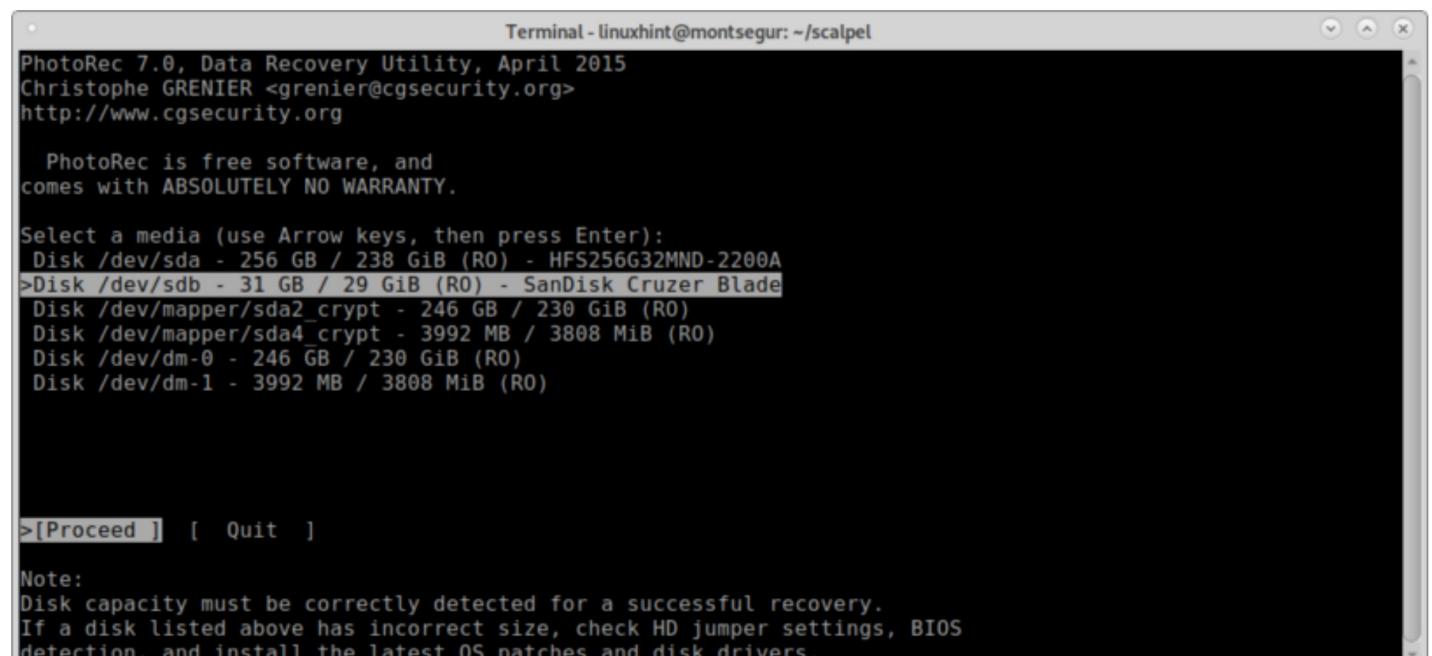
Once installed run it by calling the program:

```
# photorec
```



Remember to run PhotoRec with enough permissions to access the device to be carved.

On the first screen you need to select the source disk or image from which PhotoRec needs to recover the data. In this case I'm selecting the device /dev/sdb as shown in the image below:



In this step you need to select the partition from which you want to recover the data. If partitions aren't found and listed before proceeding with a search using the keyboard arrows move to **File Opt** to explore the available options as shown in the image below:

Terminal - linuxhint@montsegur: ~/scalpel

```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdb - 31 GB / 29 GiB (R0) - SanDisk Cruzer Blade

      Partition          Start          End    Size in sectors
> P Unknown              0            1  29879   63  32    61194240

[ Search ] [Options] >[File Opt] [ Quit ]
                         Modify file options
```

As you can see within **File Opt** you can increase the result accuracy you want by specifying the type of files you are looking for. Select the type of files you want and then press **b** to continue, or **Quit** to go back.

Terminal - linuxhint@montsegur: ~/scalpel

```
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

PhotoRec will try to locate the following files

>[X] custom Own custom signatures
[X] 1cd Russian Finance 1C:Enterprise 8
[X] 3dm Rhino / openNURBS
[X] 7z 7zip archive file
[X] DB
[X] a Unix Archive/Debian package
[X] abr Adobe Brush
[X] acb Adobe Color Book
[X] accdb Access Data Base
[X] ace ACE archive
[X] ab MAC Address Book
[X] ado Adobe Duotone Options
[X] ahn Ahnenblatt
[X] aif Audio Interchange File Format
[X] all Cubase Song file: .all
Next
Press s to disable all file families, b to save the settings
>[ Quit ]                                Return to main menu
```

Once back in the previous screen select **Search** and press Enter to continue to begin the data recovery process.

```

Terminal - linuxhint@montsegur: ~/scalpel
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdb - 31 GB / 29 GiB (RO) - SanDisk Cruzer Blade

Partition Start End Size in sectors
> P Unknown 0 0 1 29879 63 32 61194240

>[ Search ] [Options] [File Opt] [ Quit ]
Start file recovery

```

At this stage Foremost will ask what type of filesystem the device has or used to have, in this case it was FAT or NTFS, select the proper filesystem, even if it's currently broken and press **ENTER**.

```

Terminal - linuxhint@montsegur: ~/scalpel
PhotoRec 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

P Unknown 0 0 1 29879 63 32 61194240

To recover lost files, PhotoRec need to know the filesystem type where the
file were stored:
[ ext2/ext3 ] ext2/ext3/ext4 filesystem
>[ Other ] FAT/NTFS/HFS+/ReiserFS/...

```

Finally PhotoRec will ask where you want to save the files, I just left the Desktop but you can create a dedicated folder for it, after choosing the destination press **C** to continue.

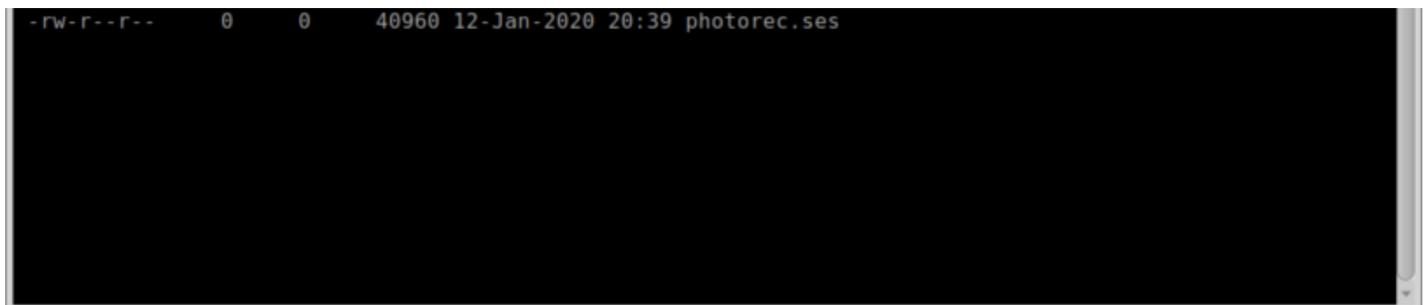
```

Terminal - linuxhint@montsegur: ~/scalpel
PhotoRec 7.0, Data Recovery Utility, April 2015

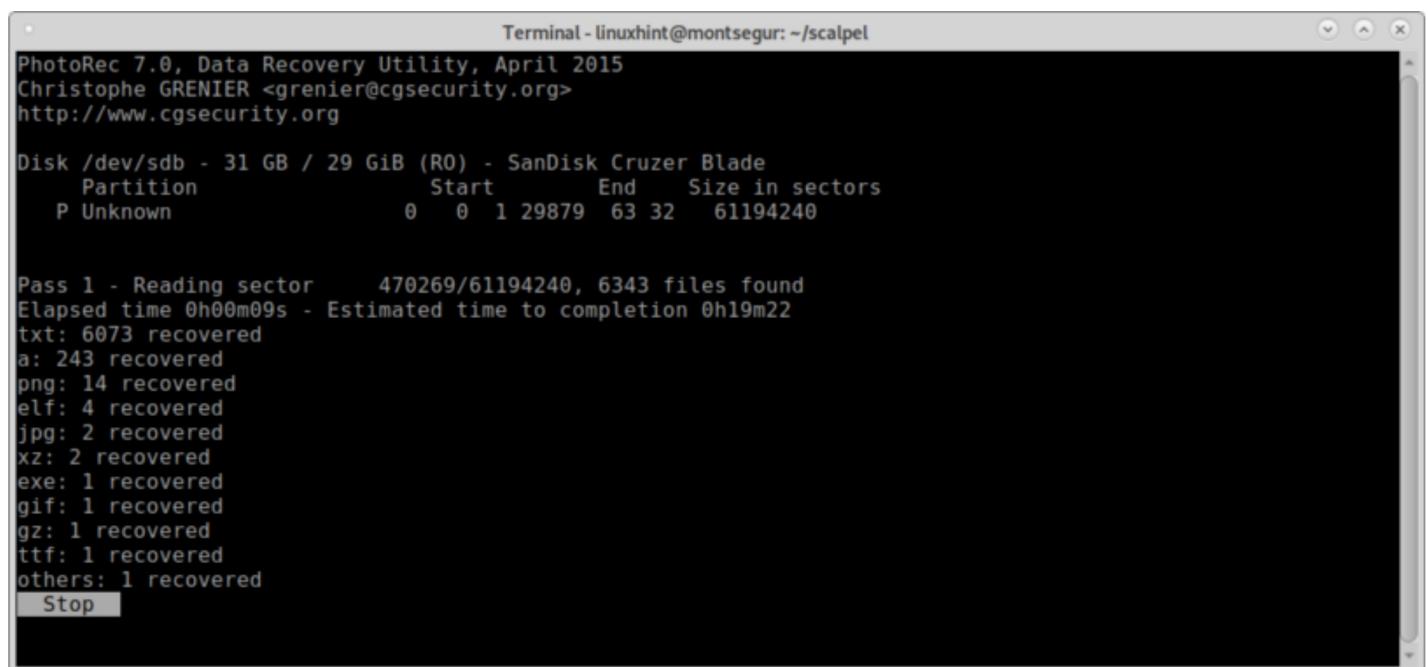
Please select a destination to save the recovered files.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit

Directory /root
drwx----- 0 0 4096 12-Jan-2020 20:39 .
drwxr-xr-x 0 0 4096 12-Jan-2020 19:36 ..
>drwxr-xr-x 0 0 4096 12-Jan-2020 20:15 Desktop
drwxr-xr-- 0 0 4096 12-Jan-2020 20:13 output
-rw----- 0 0 138 2-Jan-2020 22:40 dead.letter

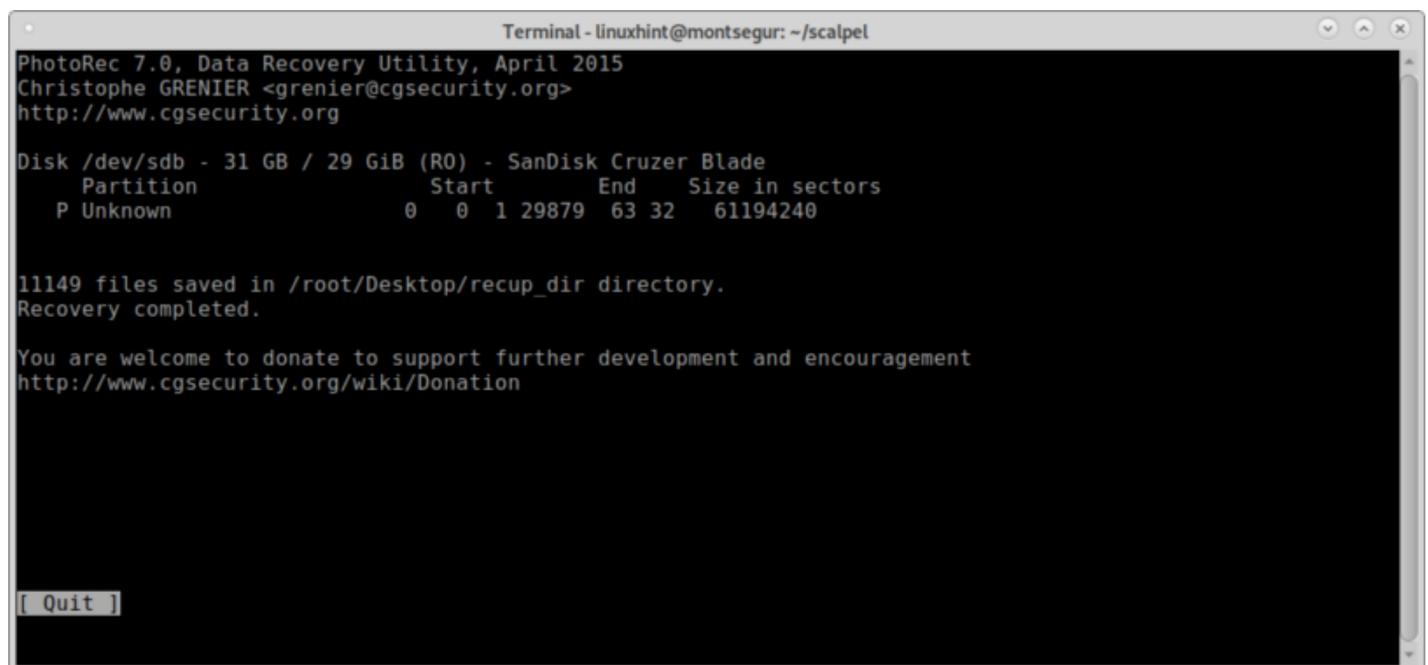
```



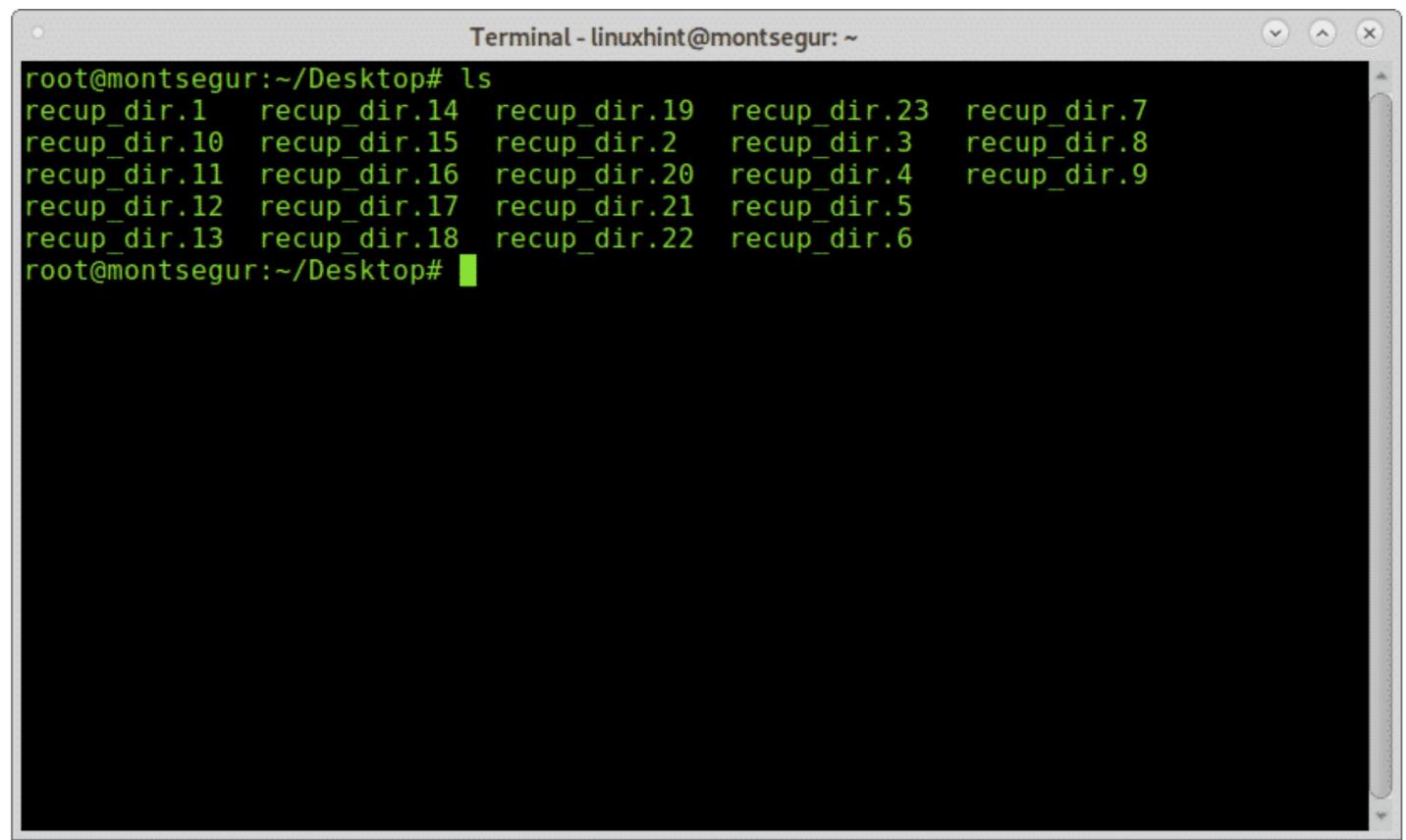
The process will start and may last some minutes or hours depending on the size.



At the end of the process PhotoRect will notify the creation of a directory with the recovered files, in this case `recup_dir*` inside the Desktop previously selected as destination.

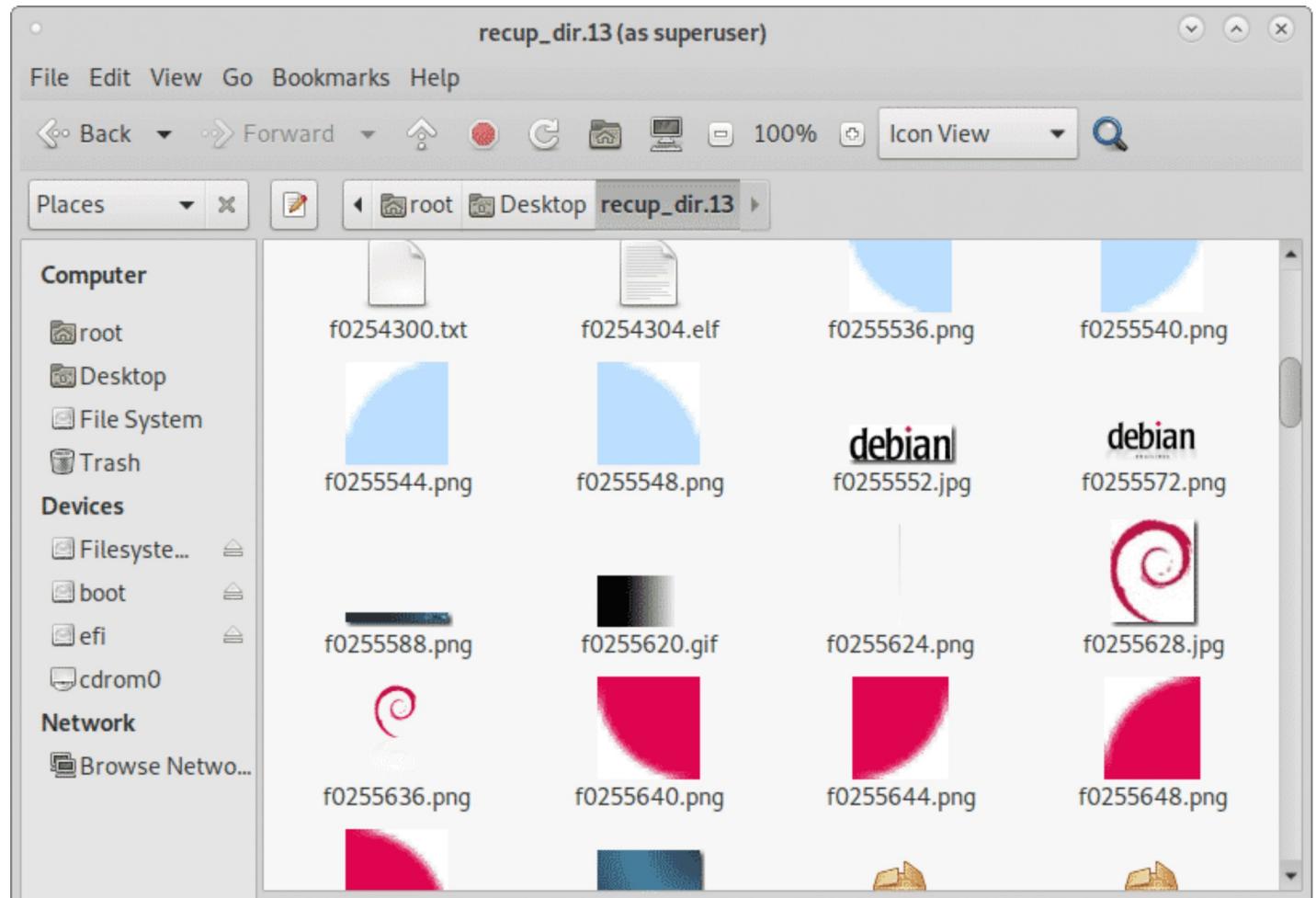


Like with Foremost you can list all files from the console:



```
Terminal - linuxhint@montsegur: ~
root@montsegur:~/Desktop# ls
recup_dir.1   recuper_dir.14  recuper_dir.19  recuper_dir.23  recuper_dir.7
recup_dir.10  recuper_dir.15  recuper_dir.2   recuper_dir.3   recuper_dir.8
recup_dir.11  recuper_dir.16  recuper_dir.20  recuper_dir.4   recuper_dir.9
recup_dir.12  recuper_dir.17  recuper_dir.21  recuper_dir.5
recup_dir.13  recuper_dir.18  recuper_dir.22  recuper_dir.6
root@montsegur:~/Desktop#
```

Or you can browse files using your preferred graphical file manager:



500 items, Free space: 145.7 GB

Conclusion on data recovery from hard drive with PhotoRec and Foremost:

Both tools lead the file carving market, both tools allow to recover any type of files, Foremost supports carving *jpg*, *gif*, *png*, *bmp*, *avi*, *exe*, *mpg*, *wav*, *riff*, *wmv*, *mov*, *pdf*, *ole*, *doc*, *zip*, *rar*, *htm*, and *cpp* and more. Both tools are compatible with disk images like dd or for Encase. While PhotoRec relays on brute force providing a deeper carving, Foremost focuses on block headers and footers working faster. Both tools are included in the most popular forensic suites and OS distributions such as Deft/Deft Zero live or CAINE which were described at https://linuxhint.com/live_forensics_tools/.

Using PhotoRec or Foremost brings the possibility to apply high level forensics tools even for domestic use, the mentioned tools have not complex flags and options to add the launching them.

I hope you found this tutorial on How to Data Recovery from Hard Drive useful. Keep following LinuxHint for more tips and updates on Linux and networking.

ABOUT THE AUTHOR



Ivan Vanney

Ivan Vanney has over 2 years as writer for LinuxHint, he is co-founder of the freelance services marketplace GIGopen.com where he works as a sysadmin.

[View all posts](#)

**1669 Holenbeck Ave, #2-244, Sunnyvale,
CA 94087
editor@linuxhint.com**

[Update Privacy Preferences](#)

AN ELITE CAFEMEDIA PUBLISHER