Using Foremost to Recover Deleted Files

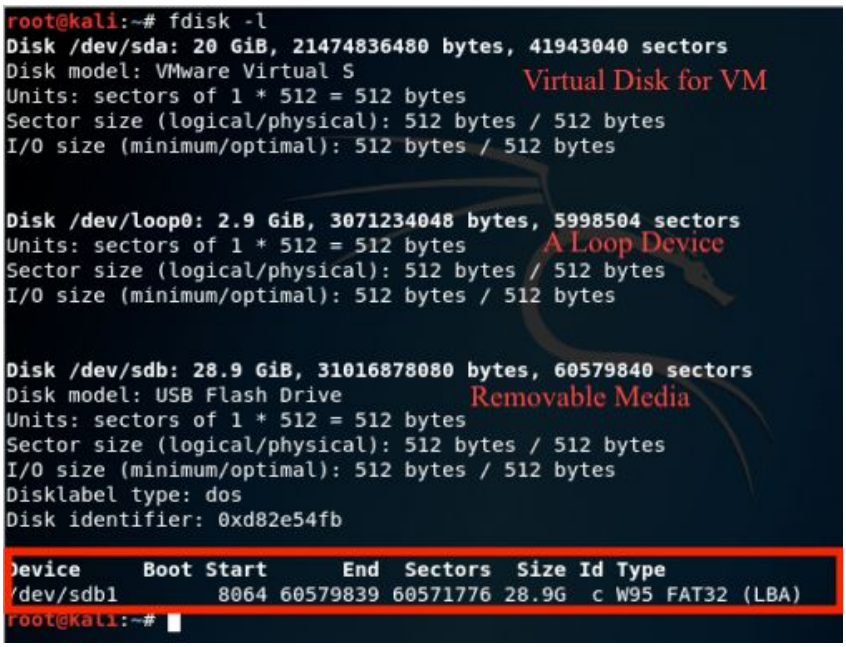
Adithya Bhaskara

Foremost 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`



3. Run `'foremost -h'` to get all the arguments foremost can take

```
root@kali:~# foremost -h
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w-d] [-t <type>] [-s <blocks>] [-k <size>]
        [-b <size>] [-c <file>] [-o <dir>] [-i <file]

-V  - display copyright information and exit
-t  - specify file type.  (-t jpeg,pdf ...)
-d  - turn on indirect block detection (for UNIX file-systems)
-i  - specify input file (default is stdin)
-a  - Write all headers, perform no error detection (corrupted files)
-w  - Only write the audit file, do not write any detected files to the disk
-o  - set output directory (defaults to output)
-c  - set configuration file to use (defaults to foremost.conf)
-q  - enables quick mode. Search are performed on 512 byte boundaries.
-Q  - enables quiet mode. Suppress output messages.
-v  - verbose mode. Logs all messages to screen
root@kali:~#
```

   a. Let's look for all files, output to /root/Desktop/Recovered_Files, specify the input from `/dev/sdb1` and enable verbose mode so we can see what is happening.
4. Run foremost with all desired arguments, in this case, `'foremost -t all -v -i /dev/sdb1 -o /root/Desktop/Recovered_Files'`
5. Run `'less /root/Desktop/Recovered_Files/audit.txt'` to view audit logs after completion.

```
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Thu Jul 25 07:00:59 2019
Invocation: foremost -t all -v -i /dev/sdb1 -o /root/Desktop/Recovered_Files
Output directory: /root/Desktop/Recovered_Files
Configuration file: /etc/foremost.conf
------------------------------------------------------------------
File: /dev/sdb1
Start: Thu Jul 25 07:00:59 2019
Length: 28 GB (31012749312 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00057504.gif          9 KB        29442048        (300 x 210)
1:      00058656.gif          6 KB        30031872        (300 x 210)
2:      00060512.gif          9 KB        30982144        (300 x 210)
3:      00060544.gif          6 KB        30998528        (300 x 210)
4:      00060576.gif          9 KB        31014912        (300 x 210)
5:      00060608.gif          6 KB        31031296        (300 x 210)
6:      00060640.gif          9 KB        31047680        (300 x 210)
7:      00060672.gif          6 KB        31064064        (300 x 210)
8:      00111425.gif          9 KB        57049600        (300 x 210)
9:      00112577.gif          6 KB        57639424        (300 x 210)
10:     00166241.gif          9 KB        85115392        (300 x 210)
11:     00167393.gif          6 KB        85705216        (300 x 210)
12:     00059200.ole          5 MB        30310400
/root/Desktop/Recovered_Files/audit.txt
```

6. Peruse the output directory for any deleted files.

```
root@kali:/# cd /root/Desktop/Recovered_Files/
root@kali:~/Desktop/Recovered_Files# ls
audit.txt  gif  jpg  ole  pdf  png  zip
root@kali:~/Desktop/Recovered_Files#
```

FOREMOST GUIDE