

R V COLLEGE OF ENGINEERING

Name: HASIFA A S USN: 1RV18IS016 Dept/Lab: ISE/CSDF Expt No.: 06 a
Date: 10/12/2021 Title: FORENSICS TOOLS

a. FOREMOST

INTRODUCTION

Foremost is a digital forensic application that is used to recover lost or deleted files. It can be used to recover the files from hard disks, memory cards, USBs or any other type of storage devices. It is a console program for carving files based on its headers, footers and internal data structure. This process is commonly referred to as data carving.

Data carving, also known as file carving, is the forensic technique of reassembling files from raw data fragments when no filesystem metadata is available. It is a common procedure when performing data recovery, after a storage device failure, for instance. This tool can be used

- For personal use to recover deleted files that are accidentally deleted.
- Or by law enforcement agencies to recover files from a criminal's storage device, that might be formatted.

Objectives - To recover permanently deleted files from a storage device.

EXECUTION STEPS

1. Installing Foremost from a package

Command - *sudo apt install foremost*

2. Basic Structure

Syntax - *foremost [options] [USB_path]*

Example cases

1. Select the connected USB device in your Kali machine,
Devices -> USB -> Connected Mass Storage device
2. To know the path of the connected USB device,
Command - *fdisk -l*

```
(root@kali)-[/home/kali]
# fdisk -l

Disk /dev/sda: 80 GiB, 85899345920 bytes, 167772160 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xe7875fa7

Device      Boot    Start        End    Sectors    Size Id Type
/dev/sda1   *        2048    165771263    165769216    79G 83 Linux
/dev/sda2                165773310    167770111    1996802    975M  5 Extended
/dev/sda5                165773312    167770111    1996800    975M 82 Linux swap / Solaris
```

```

Disk /dev/sdb: 29.81 GiB, 32010928128 bytes, 62521344 sectors
Disk model: Cruzer Blade
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00000000

```

3. Copy the path of the USB device - `/dev/sda1`
4. The main options available for foremost tool are -
 - a. **-t** - to specify the **type** of file to recover
 - i. To recover a single file type
Command - `foremost -t jpg`
 - ii. To recover multiple file types
Command - `foremost -t jpg,pdf, exe`
 - iii. To recover all file types
Command - `foremost -t all`
 - b. **-q** - to enable **quick** mode
 - c. **-v** - to enable **verbose** mode. It prints the details of the files that are being recovered
 - d. **-Q** - to enable **quiet** mode, no information will be printed on the terminal
 - e. **-i** - to specify **disk location**
 - f. **-o** - to specify **output location**. The place where the recovered files will be stored. By default, its "output" folder.
5. To receiver all files with verbose and quick mode
Command - `foremost -v -q -t gif -i /dev/sda1 -o filee`

```

(root@kali)-[/home/kali/filee/gif]
# foremost -v -q -t gif -i /dev/sda1 -o filee
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Fri Dec 10 04:02:50 2021
Invocation: foremost -v -q -t gif -i /dev/sda1 -o filee
Output directory: /home/kali/.local/share/Trash/files/filee/gif/filee
Configuration file: /etc/foremost.conf
Processing: /dev/sda1
|
File: /dev/sda1
Start: Fri Dec 10 04:02:50 2021
Length: 79 GB (84873838592 bytes)

Num      Name (bs=512)      Size      File Offset      Comment
*****0:  02424576.gif      41 KB      1241382912      (309 x 432)

```

6. Results -

```
(root@kali) ~ - [ /home/kali/filee/gif ]
ls
02424576.gif 105363328.gif 159649768.gif 159651664.gif 159652032.gif 159652656.gif 159652992.gif 17076592.gif 25566048.gif 33935360.gif 33938848.gif
08788584.gif 105363344.gif 159649784.gif 159651680.gif 159652048.gif 159652672.gif 159653008.gif 21248696.gif 25566208.gif 33935440.gif 33938880.gif
08788648.gif 105363376.gif 159651312.gif 159651696.gif 159652064.gif 159652688.gif 159653024.gif 21267344.gif 25572160.gif 33935456.gif 33938888.gif
08788664.gif 105438464.gif 159651328.gif 159651712.gif 159652080.gif 159652704.gif 159653040.gif 25449432.gif 25572744.gif 33935464.gif 33938896.gif
08788816.gif 12945424.gif 159651344.gif 159651728.gif 159652384.gif 159652720.gif 159653056.gif 25449440.gif 25572816.gif 33935472.gif 33938912.gif
105212856.gif 12945432.gif 159651360.gif 159651744.gif 159652400.gif 159652736.gif 159653072.gif 25449448.gif 25572840.gif 33935480.gif 33938920.gif
105336864.gif 142934640.gif 159651400.gif 159651760.gif 159652416.gif 159652752.gif 159653088.gif 25449472.gif 25573968.gif 33938432.gif 33938928.gif
105362608.gif 143366368.gif 159651440.gif 159651776.gif 159652432.gif 159652768.gif 159653104.gif 25449536.gif 25573992.gif 33938504.gif 33938936.gif
105362640.gif 143366400.gif 159651456.gif 159651784.gif 159652448.gif 159652784.gif 159653120.gif 25449544.gif 25574040.gif 33938512.gif 33938944.gif
105362656.gif 143366416.gif 159651472.gif 159651800.gif 159652464.gif 159652800.gif 159653136.gif 25449552.gif 25574064.gif 33938520.gif 33938952.gif
105362688.gif 143366432.gif 159651488.gif 159651824.gif 159652480.gif 159652816.gif 159653152.gif 25449560.gif 25574080.gif 33938528.gif 33938960.gif
105362704.gif 143366448.gif 159651504.gif 159651840.gif 159652496.gif 159652832.gif 159653168.gif 25449568.gif 25574096.gif 33938536.gif 33938968.gif
105362736.gif 159621389.gif 159651520.gif 159651856.gif 159652512.gif 159652848.gif 159653184.gif 25449576.gif 25574112.gif 33938544.gif 33938976.gif
105362752.gif 159649632.gif 159651536.gif 159651872.gif 159652528.gif 159652864.gif 159653192.gif 25449584.gif 25574128.gif 33938552.gif 33938984.gif
105362800.gif 159649648.gif 159651552.gif 159651888.gif 159652544.gif 159652880.gif 159653200.gif 25449592.gif 25574144.gif 33938560.gif 33938992.gif
105362808.gif 159649664.gif 159651568.gif 159651904.gif 159652560.gif 159652896.gif 159653208.gif 25449600.gif 25574160.gif 33938568.gif 33939000.gif
105362872.gif 159649680.gif 159651584.gif 159651920.gif 159652576.gif 159652912.gif 159653216.gif 25449608.gif 25574176.gif 33938576.gif 33939008.gif
105362904.gif 159649696.gif 159651600.gif 159651936.gif 159652592.gif 159652928.gif 162103296.gif 25555408.gif 33932400.gif 33938584.gif 33939016.gif
105363216.gif 159649712.gif 159651616.gif 159651952.gif 159652608.gif 159652944.gif 17067920.gif 25563440.gif 33932416.gif 33938592.gif 33939024.gif
105363248.gif 159649728.gif 159651632.gif 159652000.gif 159652624.gif 159652960.gif 17067928.gif 25565888.gif 33932424.gif 33938600.gif 33939032.gif
105363296.gif 159649752.gif 159651648.gif 159652016.gif 159652640.gif 159652976.gif 17067944.gif 25565952.gif 33932432.gif 33938608.gif 33939040.gif
```

CONCLUSION

1. It is an extremely useful tool for file recovery.
2. Although written for law enforcement use, it is freely available and can be used as a general data recovery tool.
3. The limitations of this tool are
 - a. Slow processing
 - b. Cannot process files bigger than 2GB

REFERENCES

1. Foremost - <https://forensicswiki.xyz/wiki/index.php?title=Foremost>
2. Foremost - Recover files using their headers, footers, and data structures - <http://manpages.ubuntu.com/manpages/bionic/man8/foremost.8.html>
3. Recovering deleted files using Foremost - <https://www.section.io/engineering-education/recover-deleted-files-with-foremost/>