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: 0×e7875fa7

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*

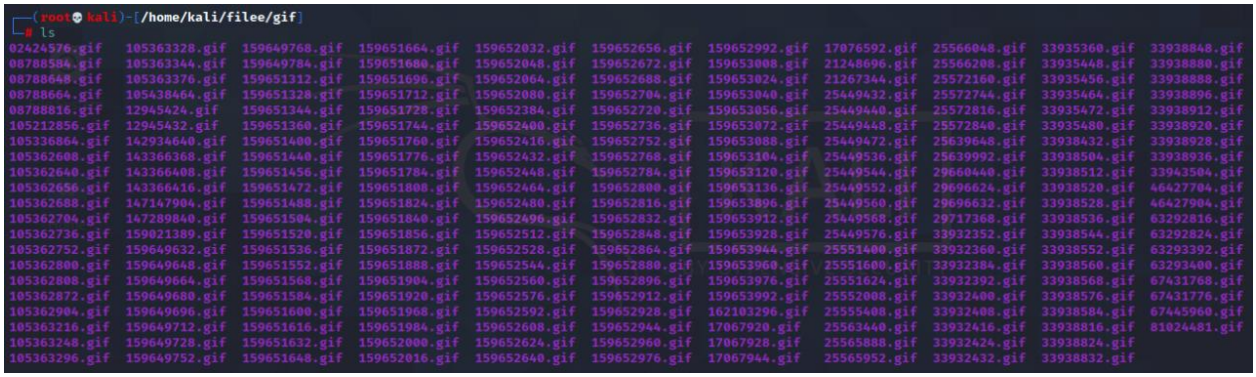
```
┌──(root💀kali)-[/home/kali/filee/gif]
└─# foremost -v -q -t gif -i /dev/sda1 -o filee
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

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 -



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/