RV COLLEGE OF ENGINEERING

Name: Dhanush M **USN**: 1RV18IS011 **Dept/Lab**: ISE/CSDF **Expt. No.**: 6a
Date: 08/12/2021 **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.

❖ Foremost was created in March 2001 to duplicate the functionality of the DOS program ***CarvThis*** for use on the Linux platform by Special Agents Kris Kendall and Jesse Kornblum of the U.S. Air Force Office of Special Investigations.

❖ In 2005, the program was modified by Nick Mikus, a research associate at the Naval Postgraduate School's Center for Information Systems Security Studies and Research as part of his master's thesis. These modifications included improvements to accuracy and extraction rate of this tool.

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

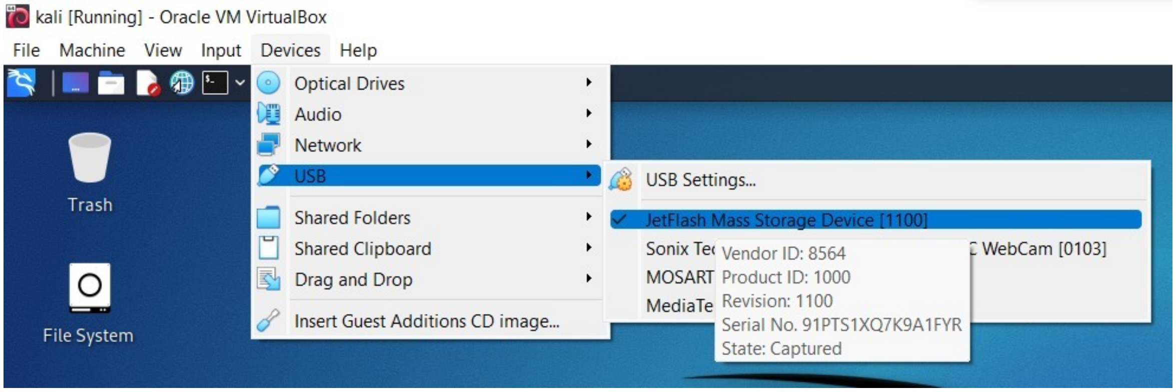
Installation

If foremost is not listed in or installed on your version of Kali Linux, install it by typing the command

```
# sudo apt-get install foremost
```

Execution Steps

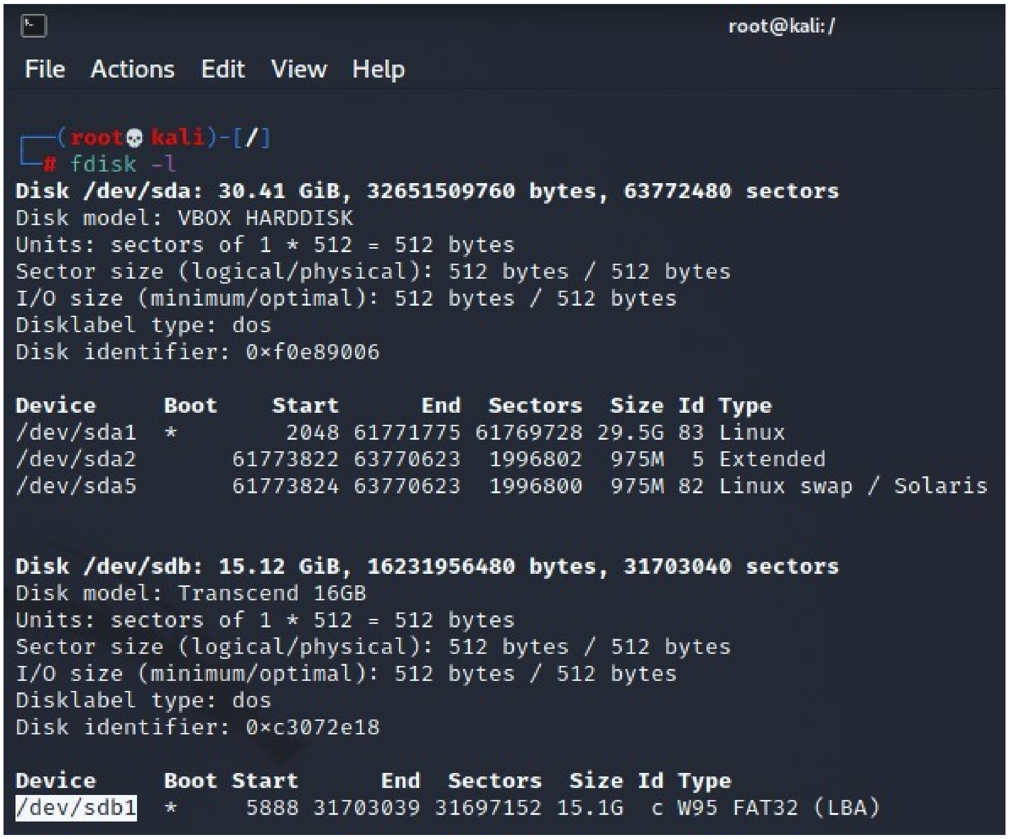
- Connect your usb device to your laptop/desktop
- Select Devices->USB->JetFlash Mass Storage Device to connect the usb to kali machine


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Optical Drives
Audio
Network
USB
Shared Folders
Shared Clipboard
Drag and Drop
Insert Guest Additions CD image...
USB Settings...
JetFlash Mass Storage Device [1100]
Sonix Tec
MOSART
MediaTe
WebCam [0103]

Vendor ID: 8564
Product ID: 1000
Revision: 1100
Serial No. 91PTS1XQ7K9A1FYR
State: Captured

- To know the path of the USB device, use the command

```
# fdisk -l
```



```
┌──(root💀kali)-[/]
└─# fdisk -l
Disk /dev/sda: 30.41 GiB, 32651509760 bytes, 63772480 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: 0xf0e89006

Device     Boot    Start      End  Sectors  Size Id Type
/dev/sda1  *        2048 61771775 61769728 29.5G 83 Linux
/dev/sda2       61773822 63770623  1996802  975M  5 Extended
/dev/sda5       61773824 63770623  1996800  975M 82 Linux swap / Solaris


Disk /dev/sdb: 15.12 GiB, 16231956480 bytes, 31703040 sectors
Disk model: Transcend 16GB
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: 0xc3072e18

Device     Boot Start      End  Sectors  Size Id Type
/dev/sdb1  *     5888 31703039 31697152 15.1G  c W95 FAT32 (LBA)
```

- Copy the path of the USB disk - `/dev/sdb1`

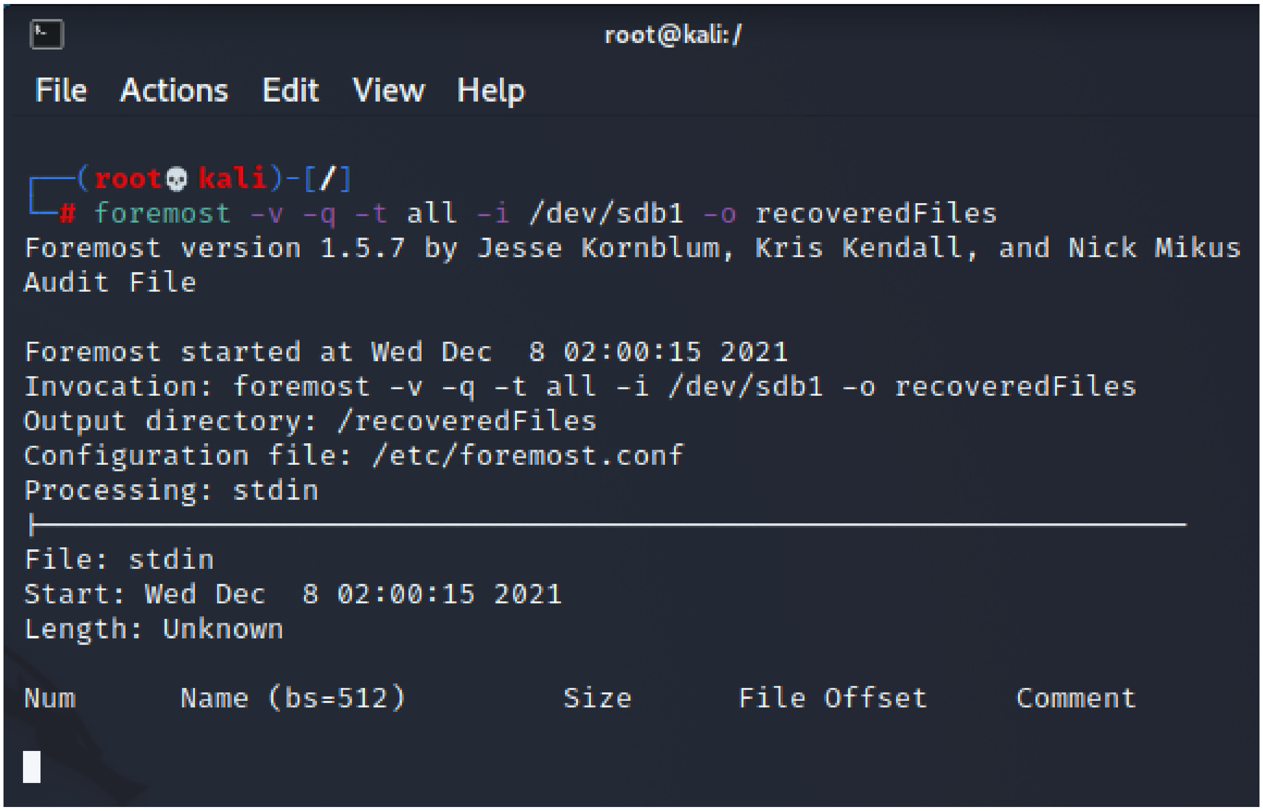
- The main options available with foremost tool are
  - **-t**: to specify the ***type*** of file to recover
    - To recover a single file type: `foremost -t jpg`
    - To recover multiple file types: `foremost -t jpg,pdf,exe`

      (no space after commas)

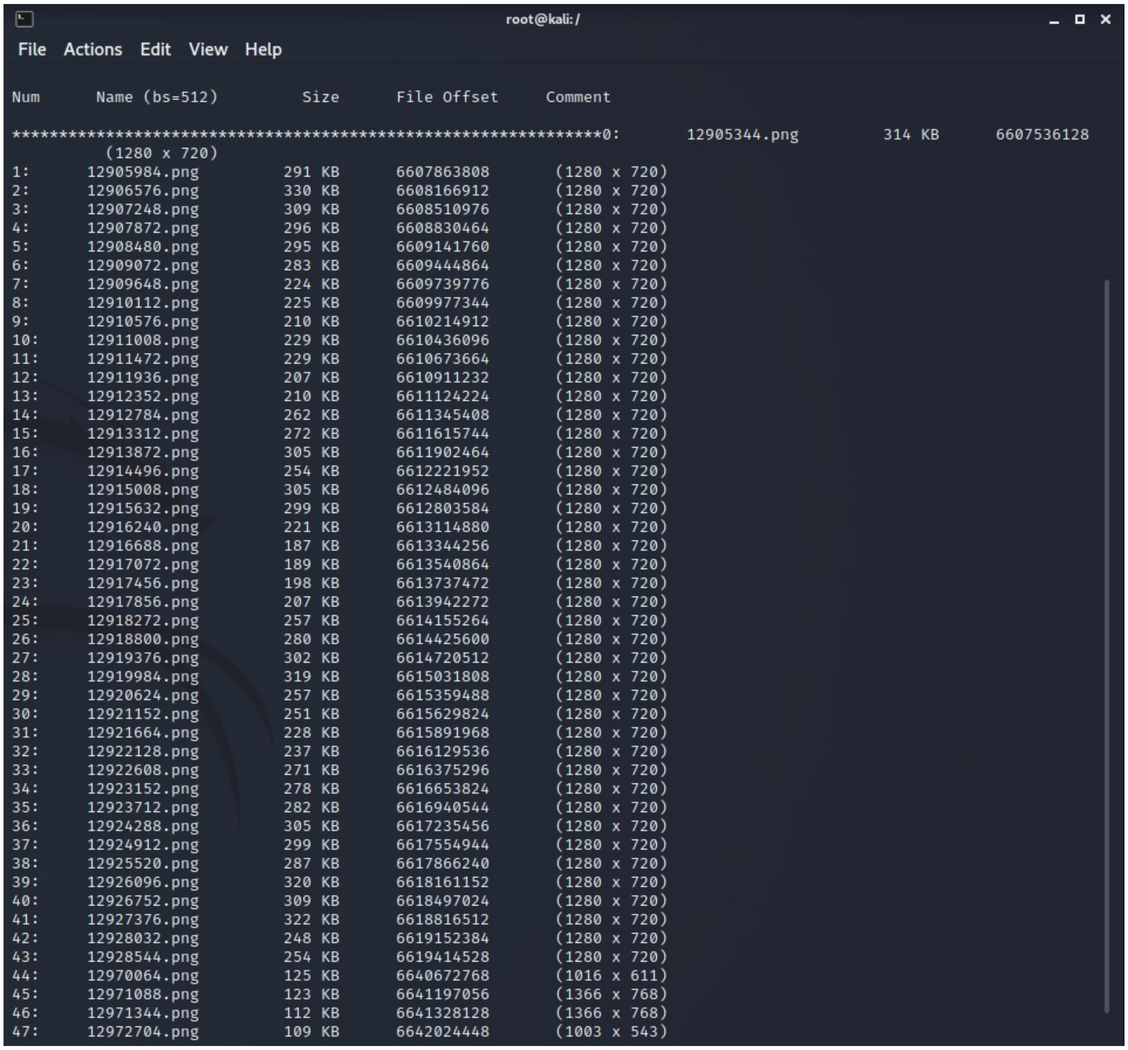
    - To recover all file types: `foremost -t all`
  - **-q**: to enable ***quick*** mode
  - **-v**: to enable ***verbose*** mode. It prints the details of the files that are being recovered
  - **-Q**: to enable ***quiet*** mode, no information will be printed on the terminal.
  - **-i**: to specify ***disk location*** (in this case `/dev/sdb1`)
  - **-o**: to specify ***output location***. The place where the recovered files will be stored. (By default, "output" folder)

- To recover all files (with verbose and quick mode) run the command

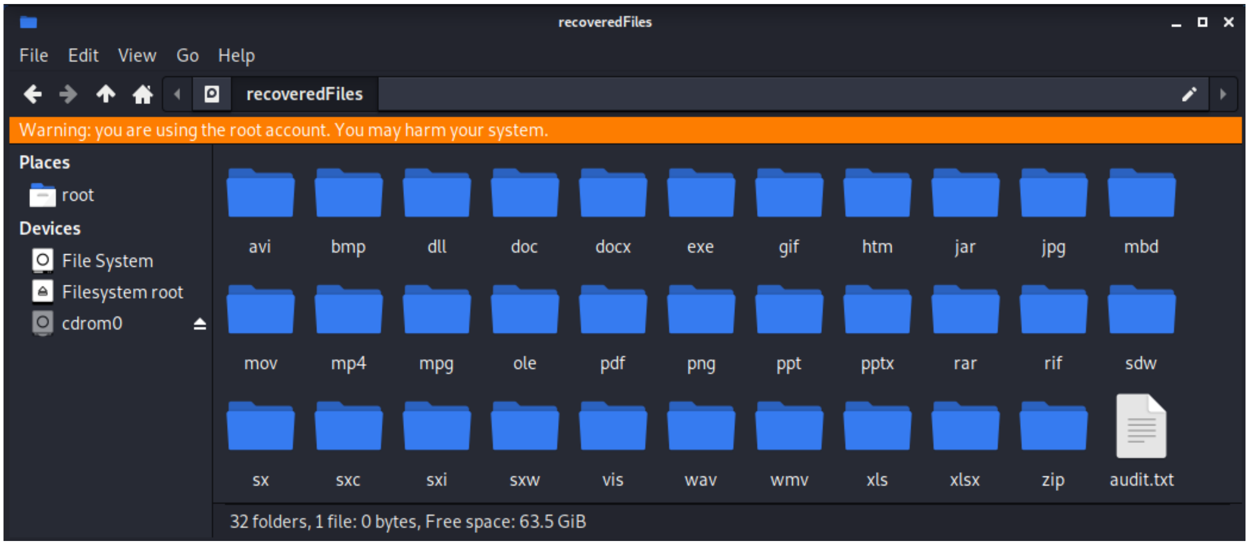
```
# foremost -v -q -t all -i /dev/sdb1 -o recoveredFiles
```



```
┌──(root💀kali)-[/]
└─# foremost -v -q -t all -i /dev/sdb1 -o recoveredFiles
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Wed Dec  8 02:00:15 2021
Invocation: foremost -v -q -t all -i /dev/sdb1 -o recoveredFiles
Output directory: /recoveredFiles
Configuration file: /etc/foremost.conf
Processing: stdin
|----------------------------------------------------------------
File: stdin
Start: Wed Dec  8 02:00:15 2021
Length: Unknown

Num      Name (bs=512)        Size       File Offset     Comment

█
```



```
Num      Name (bs=512)         Size      File Offset     Comment

***************************************************************0:     12905344.png        314 KB      6607536128
          (1280 x 720)
1:       12905984.png          291 KB     6607863808      (1280 x 720)
2:       12906576.png          330 KB     6608166912      (1280 x 720)
3:       12907248.png          309 KB     6608510976      (1280 x 720)
4:       12907872.png          296 KB     6608830464      (1280 x 720)
5:       12908480.png          295 KB     6609141760      (1280 x 720)
6:       12909072.png          283 KB     6609444864      (1280 x 720)
7:       12909648.png          224 KB     6609739776      (1280 x 720)
8:       12910112.png          225 KB     6609977344      (1280 x 720)
9:       12910576.png          210 KB     6610214912      (1280 x 720)
10:      12911008.png          229 KB     6610436096      (1280 x 720)
11:      12911472.png          229 KB     6610673664      (1280 x 720)
12:      12911936.png          207 KB     6610911232      (1280 x 720)
13:      12912352.png          210 KB     6611124224      (1280 x 720)
14:      12912784.png          262 KB     6611345408      (1280 x 720)
15:      12913312.png          272 KB     6611615744      (1280 x 720)
16:      12913872.png          305 KB     6611902464      (1280 x 720)
17:      12914496.png          254 KB     6612221952      (1280 x 720)
18:      12915008.png          305 KB     6612484096      (1280 x 720)
19:      12915632.png          299 KB     6612803584      (1280 x 720)
20:      12916240.png          221 KB     6613114880      (1280 x 720)
21:      12916688.png          187 KB     6613344256      (1280 x 720)
22:      12917072.png          189 KB     6613540864      (1280 x 720)
23:      12917456.png          198 KB     6613737472      (1280 x 720)
24:      12917856.png          207 KB     6613942272      (1280 x 720)
25:      12918272.png          257 KB     6614155264      (1280 x 720)
26:      12918800.png          280 KB     6614425600      (1280 x 720)
27:      12919376.png          302 KB     6614720512      (1280 x 720)
28:      12919984.png          319 KB     6615031808      (1280 x 720)
29:      12920624.png          257 KB     6615359488      (1280 x 720)
30:      12921152.png          251 KB     6615629824      (1280 x 720)
31:      12921664.png          228 KB     6615891968      (1280 x 720)
32:      12922128.png          237 KB     6616129536      (1280 x 720)
33:      12922608.png          271 KB     6616375296      (1280 x 720)
34:      12923152.png          278 KB     6616653824      (1280 x 720)
35:      12923712.png          282 KB     6616940544      (1280 x 720)
36:      12924288.png          305 KB     6617235456      (1280 x 720)
37:      12924912.png          299 KB     6617554944      (1280 x 720)
38:      12925520.png          287 KB     6617866240      (1280 x 720)
39:      12926096.png          320 KB     6618161152      (1280 x 720)
40:      12926752.png          309 KB     6618497024      (1280 x 720)
41:      12927376.png          322 KB     6618816512      (1280 x 720)
42:      12928032.png          248 KB     6619152384      (1280 x 720)
43:      12928544.png          254 KB     6619414528      (1280 x 720)
44:      12970064.png          125 KB     6640672768      (1016 x 611)
45:      12971088.png          123 KB     6641197056      (1366 x 768)
46:      12971344.png          112 KB     6641328128      (1366 x 768)
47:      12972704.png          109 KB     6642024448      (1003 x 543)
```



Warning: you are using the root account. You may harm your system.

32 folders, 1 file: 0 bytes, Free space: 63.5 GiB

Conclusion

- ❖ It is an extremely useful tool for file recovery.
- ❖ Although written for law enforcement use, it is freely available and can be used as a general data recovery tool.
- ❖ The limitations of this tool are
  - Slow processing
  - 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/