LAB Manual

PART A

(PART A : TO BE REFFERED BY STUDENTS)

**Experiment No.**

**A.1 Aim:**

To Perform Forensic Analysis of deleted files.

**A.2 Prerequisite:**

Data recovery, Digital Forensic, kali Linux

**A.3 Outcome:**

**After successful completion of this experiment students will be able to**

1. Appreciate foremost as a forensic tool to recover the data.

2. Explorer kali Linux as penetration testing Operating system.

**A.4 Theory:**

**Virtual Machine:** With a virtual machine, the sandbox is isolated from the underlying physical hardware but has access to the installed operating system. Virtualized environment. Usually, a sandbox is on a virtual machine so that it has no access to physical resources but can access virtualized hardware.

**Kali Linux:** Kali Linux is a Debian -derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security.

**Forensic:** Digital forensics is a branch of forensic science encompassing the recovery, investigation, examination, and analysis of material found in digital devices, often in relation to mobile devices and computer crime.

**Foremost**is a digital forensic application that is used to recover lost or deleted files. Foremost can recover the files for hard disk, memory card, pen drive, and another mode of memory devices easily. It can also work on the image files that are being generated by any other Application. It is a free command-line tool that is pre-installed in Kali Linux. This tool comes pre-installed in Kali Linux. Foremost is an especially useful software that is used to recover the deleted files, if some files are deleted accidentally or in any case files are deleted. You can recover the deleted files from foremost only if the data in the device is not overridden, which means after deleting the files no more data is added to the storage device because in that case data may be overridden and the chances of recovery also get reduced and data must get corrupted.

**Installing the Foremost Tool:**

Use the following command to install this tool in any Debian based Linux Operating System or in any other Operating System using the APT package manager.

sudo apt install foremost

Use the following command to install this tool using dnf package manager

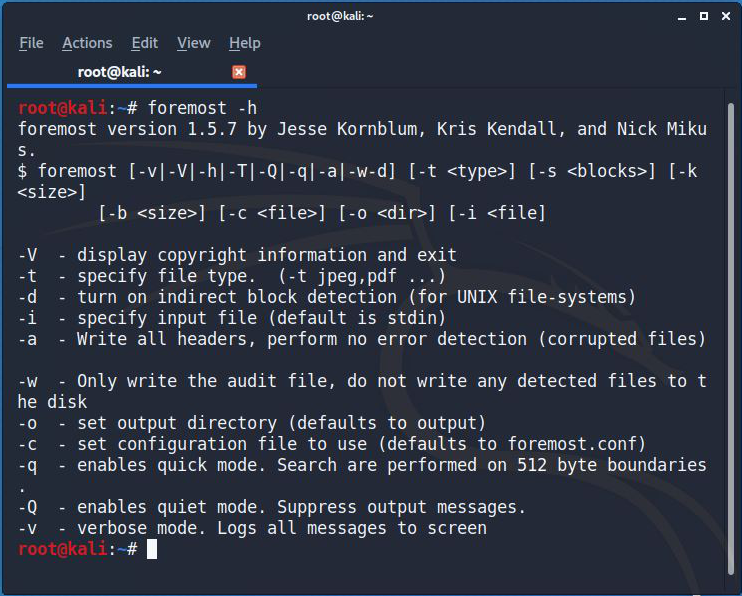
sudo dnf install foremost

Use the following command to install this tool using Pacman package manager or in Arch Linux.

sudo pacman -S foremost

**Syntax:**

foremost [options]

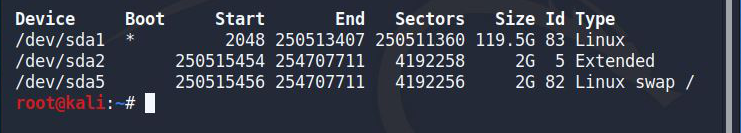


Here you can check the options available and their functions. Let us now see how to recover deleted files using foremost:

**Recovering from USB/Hard Disk:**

* Connect the External memory storage with the system.
* First, you need to know the path of your external memory device, for that use the command

fdisk -l



* After copying the device path, now we must recover the files from that device.

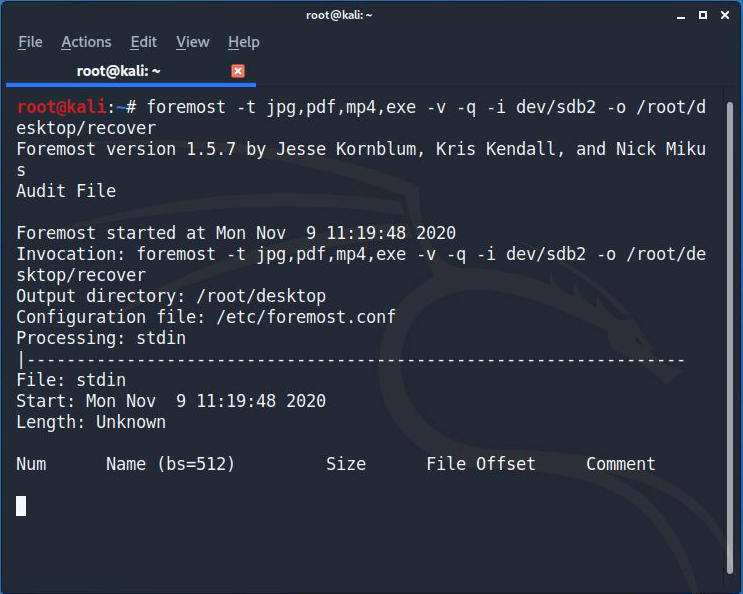
Use the options available by the “foremost -h” command.

**For example**:

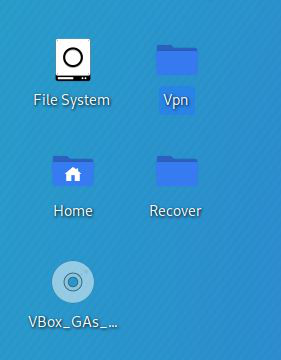
foremost -t jpg,pdf,mp4,exe -v -q -i /dev/sdb2 -o /root/desktop/recover

Here uses this command to recover the data from the device.

* **-t**: It is the type of files we want to recover. Here I want to recover jpg, pdf,mp4, and exe files.
* **-q**: It is a quick scan for the device
* **-i**: It means the input as in this case external memory.
* **-o**: It is the output folder, where to save the recovered files.



Hereafter running this command, all the files will be saved in the folder name as mentioned. Here you can see the folder recover on desktop and all the files will be stored here.



PART B

(PART B : TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)***

|  |  |
| --- | --- |
| Roll. No. A022 | Name: Kartik Padave |
| Class: B.Tech | Batch: 1 |
| Date of Experiment: | Date of Submission: |
| Grade: | |

**B.1 Software installation issues faced:**

**B.2 Input and Output:**

***(Paste your program input and output in following format, If there is error then paste the specific error in the output part. In case of error with due permission of the faculty extension can be given to submit the error free code with output at the right time of time. Students will be graded accordingly.)***

**Input and Output**

1. Bulk\_extractor -h

A screenshot of a computer

Description automatically generated with medium confidence

1. bulk\_extractor -o bulk\_output terry-work-usb-2009-12-11.E01

Text

Description automatically generated

1. ls -l

Text

Description automatically generated with medium confidence

1. ls -l bulk output

Text

Description automatically generated with medium confidence

Graphical user interface, text

Description automatically generated

**B.3 Observations and learning:**

***(Students are expected to comment on the output obtained with clear observations and learning for each task/ sub part assigned)***

bulk\_extractor is a wonderful tool that carves data and finds useful information, such as email addresses, visited URLs, Facebook URLs, credit card numbers, and a variety of other information.

**B.4 Conclusion:**

*(****Students must write the conclusion as per the attainment of individual outcome listed above and learning/observation noted in section B.3)***

**Questions of Curiosity**

***(To be answered by student based on the practical performed and learning/observations)***

Q1: what are open source and proprietary forensic tools for multimedia recovery?

1. Autopsy

Autopsy is a GUI-based open-source digital forensic program to analyze hard drives and smart phones effectively. Thousands of users use autopsy worldwide to investigate what happened in the computer.

1. Encrypted Disk Detector

Encrypted Disk Detector can be helpful to check encrypted physical drives. It supports TrueCrypt, PGP, Bitlocker, Safeboot encrypted volumes.

1. Wireshark

Wireshark is a network capture and analyzer tool to see what is happening in your network. Wireshark will be handy to investigate network related incident.4. Magnet RAM Capture. You can use Magnet RAM to capture the physical memory of a computer and analyze artifacts in memory. It supports Windows operating system.

1. Network Miner

An interesting network forensic analyzer for Windows, Linux & MAC OS X to detect OS, hostname, sessions, and open ports through packet sniffing or by PCAP file. Network Miner provide extracted artifacts in an intuitive user interface.6. NMAP