**CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING (C-DAC),**

**THIRUVANANTHAPURAM, KERALA**

**A PROJECT REPORT ON**

**“File Recovery and Data Carving Using Foremost Tool”**

**SUBMITTED TOWARDS THE**

# PG-DCSF March 2024

**BY**

**Group Number – 06**

|  |  |
| --- | --- |
| **RACHEL SHARMA** | **PRN: 240360940026** |
| **RAJDEEP DIVEKAR** | **PRN: 240360940027** |
| **ROSHANI MADANKAR** | **PRN: 240360940028** |
| **SAKSHI PAGARE** | **PRN: 240360940029** |
| **SANDESH KAMBLE** | **PRN: 240360940030** |

**Under The Guidance Of**

## Mr. Jayaram Peggam Dr. Jayaram Peggam

**( Centre Co- Ordinator) (Project Guide)**

**TABLE OF CONTENTS**

**Topic Page No**

**Abstract……………………………………………………….03**

**Objective……………………………………………………....04**

**Certificate……………………………………………………..05**

**Introduction…………………………………………………..06**

**Features of Foremost Tool…………………………………...08**

**Installation of Foremost Tool……………………………....10**

**Foremost to recover deleted files…………………………..11**

**Add support for a specific file type………………………..17**

**Conclusion…………………………………………………..18**

# ABSTRACT

Foremost is an exceptional, versatile, and powerful digital forensics and data recovery tool that has revolutionized the way investigators and enthusiasts approach data extraction and analysis. With its advanced capabilities, Foremost has become the go-to solution for extracting critical information from a wide range of digital devices, including computers, laptops, and mobile devices. Developed by a team of experts, it has been meticulously crafted to cater to the diverse needs of the digital forensics community.

One of the key strengths of Foremost lies in its intelligent file identification and recovery mechanism. The tool expertly analyzes disk images and raw data sources, identifying files based on their unique signatures, headers, footers, and even internal data structures. This sophisticated approach ensures that even fragmented or partially damaged files can be accurately recovered, providing investigators with a complete picture of the data.

The versatility of Foremost is further showcased through its extensive support for various file formats. From multimedia files to compressed archives and documents, Foremost can extract and recover a vast array of file types, making it applicable to numerous investigation scenarios. This flexibility ensures that no matter the nature of the data, Foremost provides a reliable and efficient solution.

In addition to its core functionality, Foremost offers a range of advanced features that enhance its usability and effectiveness. The tool provides a verbose mode, offering detailed output for comprehensive analysis, and allows users to specify file types for recovery, enabling focused and efficient investigations. With the ability to customize carving parameters, investigators can tailor their searches to specific research requirements, optimizing the data recovery process.

.

In conclusion, Foremost is an indispensable tool in the digital forensics arsenal, offering unparalleled versatility, functionality, and ease of use. Its advanced file recovery capabilities, extensive file format support, and customizable features make it a powerful ally in extracting critical information from digital devices. With its open-source nature fostering continuous improvement and collaboration, Foremost remains at the forefront of digital forensics and data recovery, empowering investigators and enthusiasts alike to uncover the truth hidden within digital data.

**OBJECTIVE**

The objective of Foremost is to provide a versatile, powerful, and accessible digital forensics and data recovery tool that empowers investigators and enthusiasts to extract critical information from a wide range of digital devices. Foremost aims to revolutionize data extraction and analysis by offering advanced file recovery capabilities, extensive file format support, and customizable features, ensuring efficient and focused investigations. With its intuitive interface and open-source nature, Foremost strives to lower the barrier to entry into the world of digital forensics, making it a go-to resource for anyone seeking to uncover valuable insights from digital devices

CERTIFICATE

THIS IS CERTIFY THAT,

|  |  |
| --- | --- |
| RACHEL SHARMA | PRN: 240360940026 |
| RAJDEEP DIVEKAR | PRN: 240360940027 |
| ROSHANI MADANKAR | PRN: 240360940028 |
| SAKSHI PAGARE | PRN: 240360940029 |
| SANDESH KAMBLE | PRN: 240360940030 |

Have Satisfactory completed the project work Entitled, **“File Recovery and Data Carving Using Foremost Tool”** to Centre for Advanced Computing in the partial fulfilment of the requirement of Post-Graduate Diploma (PG-Diploma), is a record of project work carried out by them under my guidance and supervision. The matter presented in this project report has not been submitted either in part of full to any University or Institute for award of any degree.

## Mr. Jayram Peggam Dr.Hiron Bose

### (Centre Co-Ordinator) (Project Guide)

**INTRODUCTION**

In the realm of digital forensics, the ability to extract and analyze data from various sources is paramount. As digital devices become increasingly integral to our daily lives, so does the need for comprehensive tools to uncover the secrets they hold. This is where Foremost steps in—a revolutionary data recovery and forensic analysis tool that has transformed the way we approach digital investigations. Developed by a team of dedicated experts, Foremost offers a powerful, versatile, and accessible solution for extracting critical information from the depths of digital storage.

The digital world presents unique challenges and opportunities when it comes to data recovery and forensics. With the ever-evolving landscape of file systems, storage media, and data structures, investigators need a dynamic and adaptable tool. Foremost rises to this challenge, providing an innovative approach to data extraction that goes beyond traditional methods. With its advanced capabilities, Foremost empowers users to delve deep into the intricacies of digital devices, uncovering hidden insights and revealing valuable evidence.

What sets Foremost apart is its intelligent and sophisticated design. The tool has been meticulously crafted to identify and recover files based on their unique signatures, headers, and footers, ensuring accurate and reliable results. This signature-based recovery method allows Foremost to excel in extracting specific file types, even from fragmented or partially damaged data sources. With its advanced algorithms and data parsing techniques, Foremost offers a new level of precision and efficiency to the field of digital forensics.

The versatility of Foremost is another key advantage. Recognizing the diverse nature of digital investigations, the tool has been developed to support a broad range of file formats and media types. From multimedia files to compressed archives and documents, Foremost can handle a vast array of data, making it applicable to numerous scenarios. Whether it's examining a suspect's hard drive or recovering crucial evidence from a mobile device, Foremost provides a flexible and adaptable solution, ensuring investigators have the necessary tools for any situation.

Usability and accessibility have been central considerations in the development of Foremost. The tool boasts an intuitive and user-friendly interface, making it accessible to a wide range of users, from novice enthusiasts to seasoned professionals. Clear documentation, comprehensive tutorials, and a supportive community further enhance the user experience, providing guidance and ensuring that anyone can leverage the power of Foremost effectively. This focus on usability lowers the barrier to entry into the world of digital forensics, encouraging exploration and fostering a community of passionate investigators.

Open-source collaboration is at the heart of Foremost's development philosophy. By making the source code readily available, Foremost invites contributions and improvements from the wider community. This collaborative approach has fostered a vibrant ecosystem, with developers and enthusiasts alike contributing their expertise to enhance the tool's capabilities. The open-source nature also ensures transparency and trust, allowing users to verify the integrity and security of the software. This collaborative spirit has not only improved Foremost but has also inspired and influenced the development of other digital forensics tools, raising the bar for the entire community.

Foremost has had a significant impact on the field of digital forensics, setting new standards for data recovery and analysis. Its effectiveness and reliability have been proven in numerous real-world investigations, contributing to the resolution of complex cases and the advancement of forensic techniques. The insights and evidence uncovered through Foremost have played a pivotal role in shaping the strategies and methodologies employed by digital forensics professionals, solidifying its place as a cornerstone technology in their arsenal.

In conclusion, Foremost is an exceptional digital forensics and data recovery tool that has revolutionized data extraction and analysis. With its advanced file recovery capabilities, extensive file format support, and customizable features, Foremost provides investigators and enthusiasts with a powerful and versatile solution. Its intuitive interface and open-source nature make it accessible and collaborative, fostering a community dedicated to uncovering the truth hidden within digital devices. As digital forensics continues to evolve, Foremost remains at the forefront, empowering users to tackle the challenges and opportunities of the digital world with confidence and expertise.

**FEATURES OF FOREMOST TOOL**

The Foremost tool is a powerful and versatile digital forensics and data recovery utility with a range of impressive features:

* File Recovery and Data Carving: Foremost excels in recovering lost or deleted files from various storage media, including disk images and physical disks. It can extract specific file types based on their headers, footers, and internal data structures, even if the metadata is lost or damaged.
* Support for Various File Systems: Foremost supports a wide range of file systems, such as FAT, NTFS, and ext2/ext3/ext4, making it compatible with different operating systems and storage devices.
* Customization of Carving Parameters: Users can customize carving parameters to tailor the tool to their specific needs. This includes specifying file signatures, search methods, and collection of information about recovered files, allowing for focused and efficient investigations.
* Open-Source and Collaborative: Foremost is developed as an open-source program, fostering a collaborative environment. This allows users to review, modify, and contribute to the source code, encouraging continuous improvement and innovation.
* Integration with Kali Linux: When integrated with Kali Linux, a popular operating system for penetration testing and forensic analysis, Foremost becomes an indispensable tool for digital investigators.
* User-Friendly Interface: Foremost offers an intuitive and user-friendly interface, making it accessible to users of all experience levels. Clear documentation and community support further enhance its usability.
* Verbose Mode: The tool provides a verbose mode, offering detailed output during the recovery process. This feature aids in comprehensive analysis and provides valuable insights into the recovered data.
* Support for Image Files: Foremost can work directly on image files generated by various tools, such as dd, Safeback, and Encase, allowing for non-destructive analysis and recovery.
* Command Line Flexibility: Foremost can be operated through command-line switches, providing flexibility and advanced options for users who prefer a command-line interface.
* Efficiency and Speed: Foremost is designed for efficiency and speed, making it a go-to choice for quick data recovery operations. Its advanced algorithms optimize the recovery process, saving valuable time for investigators.
* Community and Support: Foremost has an active community of users and developers who provide support, share insights, and contribute to the tool's ongoing improvement. This community aspect ensures that users can readily access guidance and benefit from the collective experience.

These features make Foremost a powerful and versatile tool for digital forensics and data recovery, suitable for professionals and enthusiasts alike. Its combination of functionality, ease of use, and adaptability has established it as a trusted utility in the field of digital investigations.

**INSTALLATION OF FOREMOST TOOL**

Foremost is a Linux program used to recover files based on their headers and footers. It can be installed on Linux by following these steps:

1. Open a terminal.
2. Use the package manager for your Linux distribution to install Foremost. For Debian/Ubuntu/Linux Mint, the command is:

**sudo apt install foremost**

For other distributions, you may need to use a different package manager, such as DNF:

**sudo dnf install foremost**

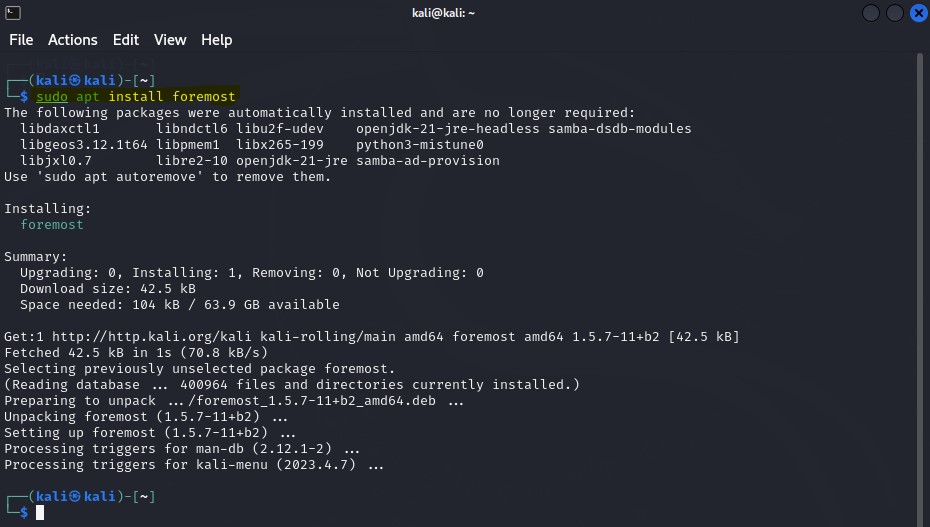


Fig 5.1 Installation of Foremost tool

**FOREMOST TO RECOVER DELETED FILES**

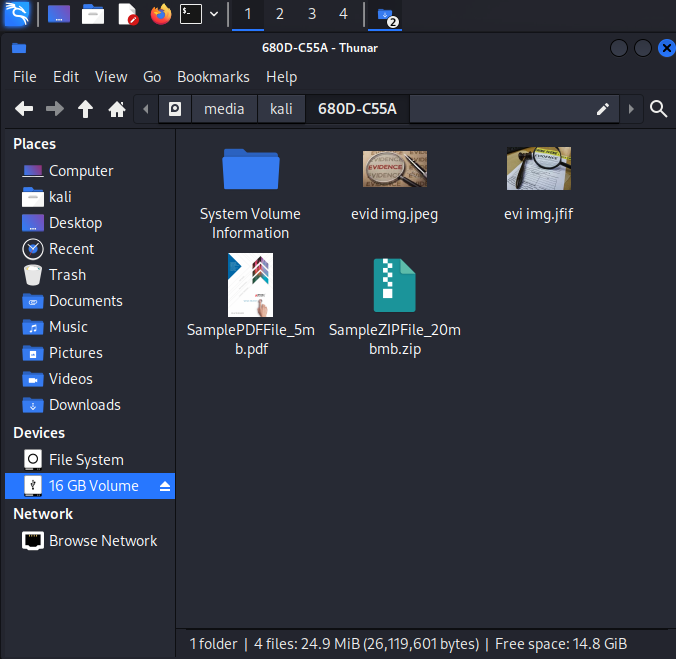


Fig 6.1 Files in Pen drive

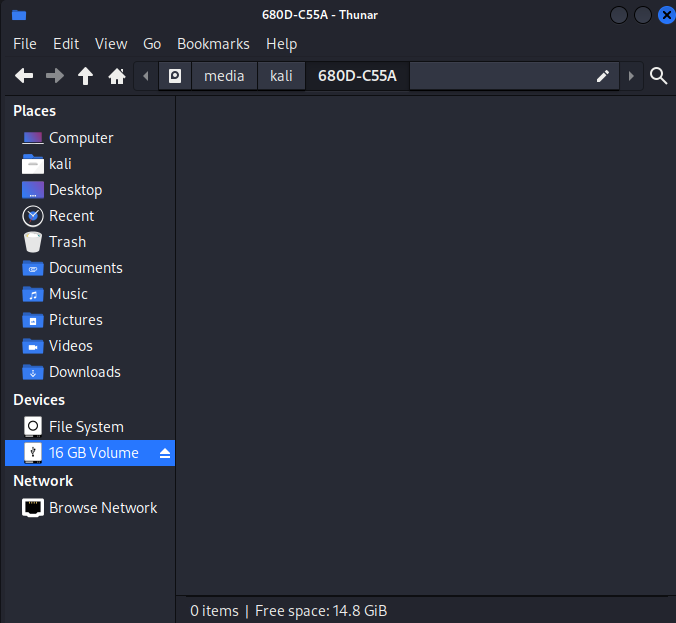


Fig 6.2 Deleting Files in Pen drive

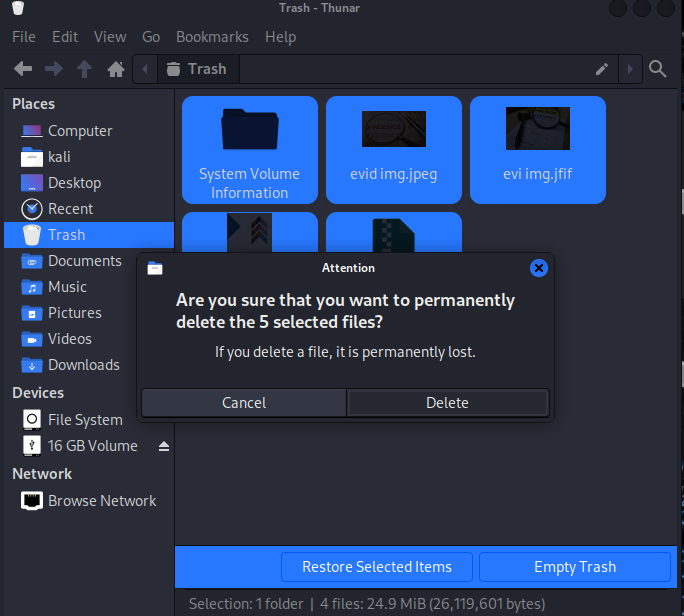


Fig 6.3 Permanently Deleting files in Pendrive

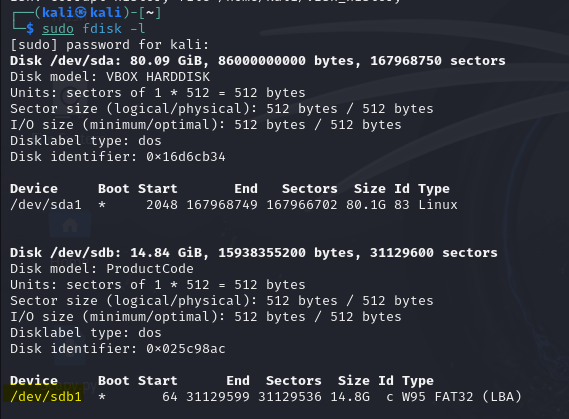
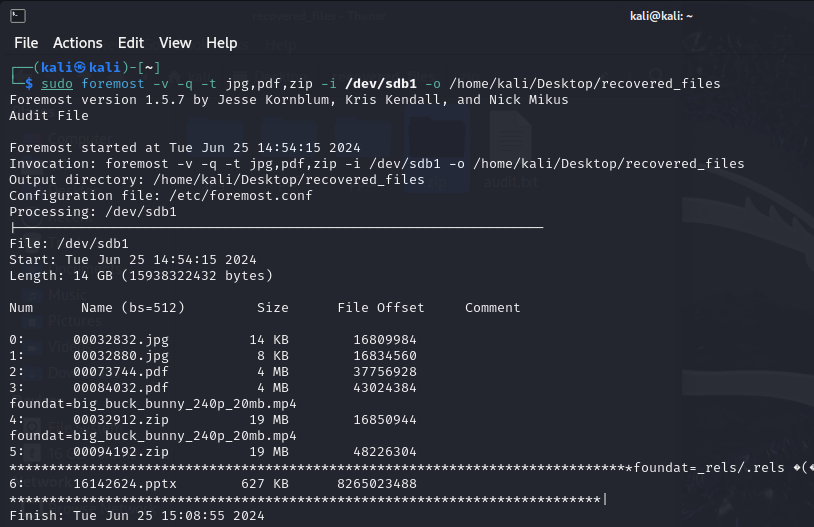


Fig 6.4 list partition tables and detailed information about storage devices



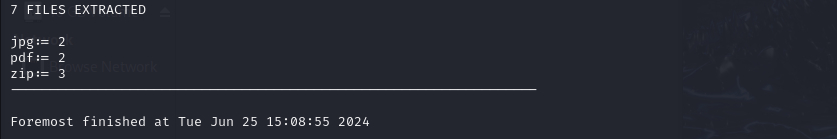


Fig 6.5 Use of foremost tool

Identify the device or partition from which you want to recover files.

For example, if you want to recover files from a USB drive mounted at /media/usbdrive, you need to know the device path of that drive.

Run Foremost with the appropriate options. The basic syntax is as follows: foremost [options] -i <input\_device> -o <output\_directory>

[options]: Various options can be specified, such as -t to specify a specific file type or -v for verbose output.

-i <input\_device>: Specify the input device or partition from which you want to recover files. Replace <input\_device> with the path to the device, such as /dev/sda1 or /media/usbdrive.

-o <output\_directory>: Specify the directory where you want Foremost to save the recovered files. Replace <output\_directory> with the desired path, such as

/home/recovery/.

Wait for Foremost to scan the specified device or partition. Depending on the size of the device and the number of files, this process can take some time.

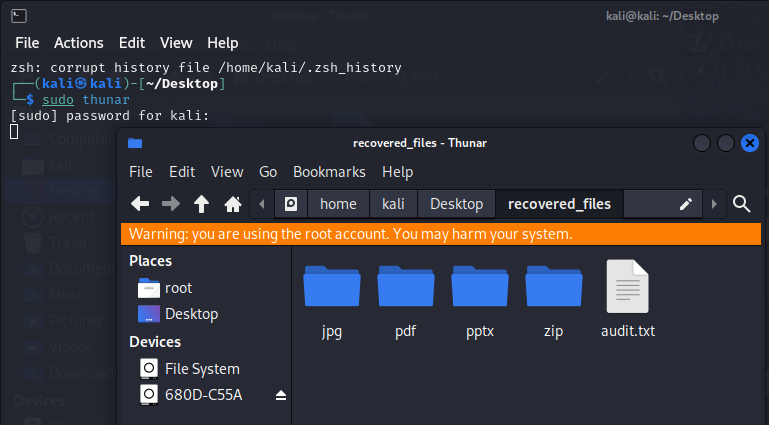


Fig 6.6 reconstruction of files on the base of their headers, footers and data structures, without relying on filesystem metadata

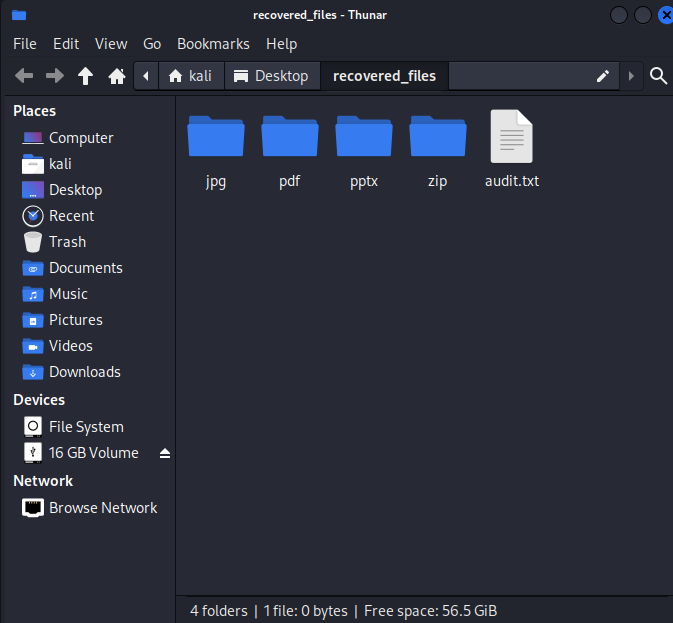


Fig 6.7 Recovered Files Types

Once the scan is complete, navigate to the specified output directory to find the recovered files. Foremost creates subdirectories based on the file types it has identified.

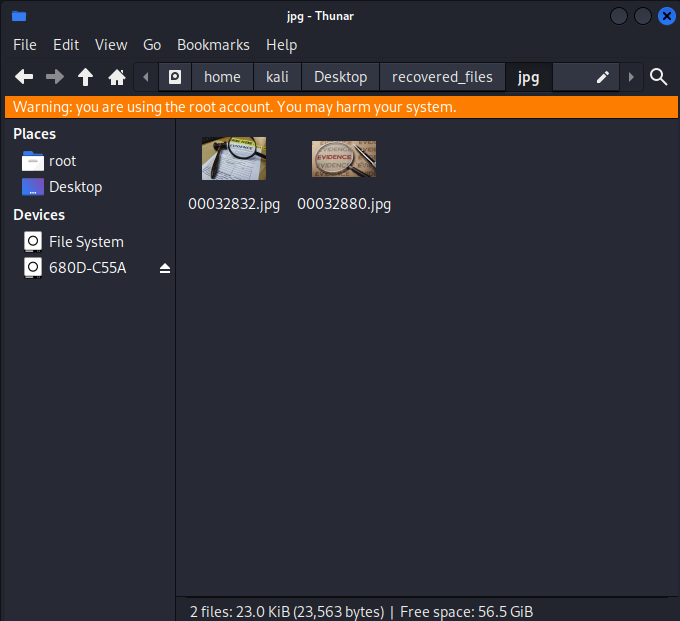


Fig 6.8 Recovered JPG Files

Examine the recovered files

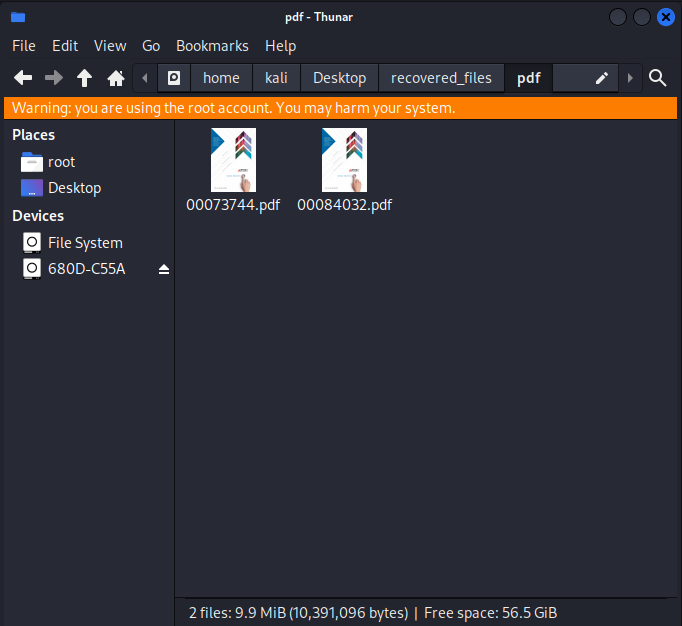


Fig 6.9 Recovered PDF Files

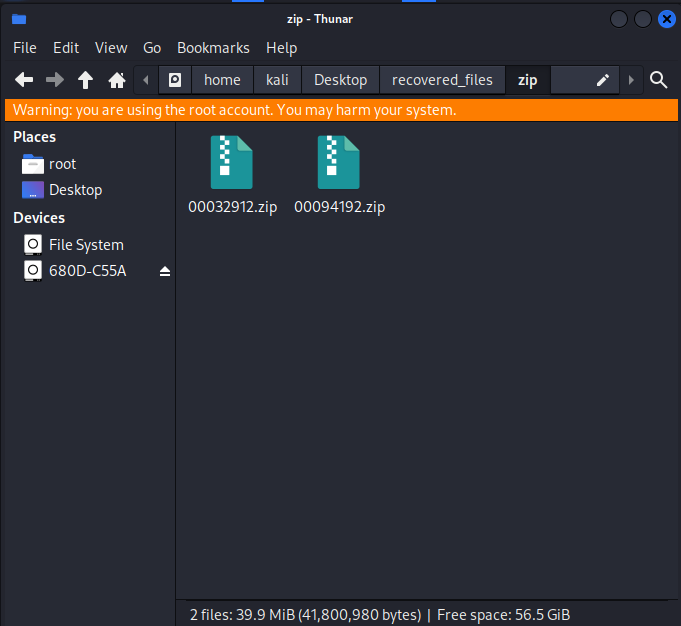


Fig 6.10 Recovered ZIP Files

**ADD SUPPORT FOR A SPECIFIC FILE TYPE**

To add support for a specific file type in Foremost, you can follow these steps:

1. **Understand Foremost's configuration file:** Foremost uses a configuration file to specify file formats that are not natively supported by the program. The default configuration file is typically located at /etc/foremost.conf.
2. **Open the configuration file:** Use a text editor with root or administrative privileges to open the configuration file.

For example: sudo nano /etc/foremost.conf

1. **Edit the configuration file:** Inside the configuration file, you will find commented examples showing the syntax for adding new file types. Uncomment or add a new entry for the file type you want to add.
2. **Specify the file type details:** For each file type, you need to provide specific details such as the file extension, header, and footer information.

For your custom image format, provide the following details:

* file extension: The unique file extension associated with your custom image format.
* MIME type: The MIME type or media type that represents your image format.
* header: The specific byte sequence that identifies the start of your image files.
* footer: The specific byte sequence that identifies the end of your image files.

1. **Save and close the configuration file:** After making the necessary additions or modifications, save the configuration file and exit the text editor.
2. **Test the new file type support:** Run Foremost with the -t option to specify the new file type and verify that it is recognized and processed correctly.
3. **Verify the recovered files:** After running Foremost with the new file type, check the output directory to find the recovered files of the specified type. By default, Foremost creates a directory named after the file type where it places the recovered files.

**CONCLUSION**

In conclusion, Foremost is an exceptional digital forensics and data recovery tool that offers a comprehensive solution for extracting valuable information from digital devices. With its advanced file recovery capabilities, extensive file format support, and customizable features, it empowers investigators and enthusiasts alike to tackle data extraction and analysis effectively. Foremost provides a versatile and accessible platform, enabling users to uncover critical insights from various digital sources. Its sophisticated algorithms and data parsing techniques ensure accurate and reliable results, even in complex scenarios involving fragmented or damaged files.

Moreover, Foremost's open-source nature has fostered a collaborative community that continuously improves and enhances the tool's capabilities. The availability of its source code encourages contributions, innovation, and transparency, benefiting users worldwide. With its combination of powerful functionality, ease of use, and adaptability, Foremost has established itself as a trusted and indispensable utility in the field of digital forensics. By revolutionizing data recovery and analysis, Foremost continues to play a pivotal role in shaping the strategies and successes of digital investigations, both now and in the future.