Deleted Data Recovery Mechanism For IOT Devices

M.Kankara, M.Padebettu, M.Kulkarni, A.Gokhale

April 23rd, 2023

Turnitin Plagiarism Score:
7% - from Internet Sources and Publications
14% - from previously submitted Project Proposal dated 17th March, 2023.

Table of Contents

List of Figures

1. Abstract

As Internet of Things (IoT) devices become more widespread in our daily lives, the necessity for data recovery techniques that can successfully retrieve lost or deleted data grows. The project in question aims to develop a method for recovering deleted data from Internet of Things devices. The creation of hardware and software tools to recover erased data from sensors, wearables, and other connected Internet of Things devices is the suggested remedy. The project will start with a thorough examination of the methods for data recovery that are already in use, as well as the standard data storage platforms used in IoT devices. It will be possible to recover erased data from a variety of devices and storage systems thanks to a recovery solution that is built on the findings of this research. The suggested approach uses cutting-edge methods to recover erased files from hard drives, USB drives, and memory cards, among other types of storage devices. Amongst other tools and techniques, the project will include data carving, memory analysis, and file carving. The project's importance comes from its capability to help forensic investigators recover important data that may have been erased intentionally or unintentionally. It serves as an important tool for digital forensics because it can be used to gather data for criminal investigations. A functional mechanism for recovering deleted data will be available to forensic investigators as a result of this study. The efficiency of various data recovery methods and technologies will be demonstrated, establishing the foundation for further research in the area of digital forensics.

2. Introduction

The Internet of Things (IoT) has quickly become more widespread and is now considered an essential component of our day-to-day lives. The amount of data produced by Internet of Things devices has increased at an exponential rate over the past few years as their use has increased across a variety of industries, including the healthcare industry, the transportation industry, and the manufacturing industry. Because of the sensitive nature of this data and the possibility that it could be lost or stolen, concerns have been raised about the safety and privacy of devices connected to the internet of things (IoT).

One of the most significant challenges associated with ensuring the safety of Internet of Things devices is the inability to restore data that has been accidentally or purposefully removed from those devices. At the moment, Internet of Things devices do not have efficient data recovery mechanisms, which can lead to significant data loss and compromise the devices' ability to perform their intended functions.

This project intends to address this issue by developing a mechanism for recovering deleted data on Internet of Things devices. This mechanism will be able to recover deleted data from a wide variety of data storage systems and devices. In order to recover data that has been accidentally deleted from sensors, wearables, and other connected devices, the proposed solution will involve the development of software and hardware solutions.

In order to recover deleted data from a variety of storage devices, the project will investigate various data recovery strategies and tools. Some examples of these strategies and tools include data carving, file carving, and memory analysis. The objective of this project is to develop a method that is robust and reliable for recovering deleted data from Internet of Things devices. This method will assist in protecting the security and privacy of sensitive data generated by these devices. We will be able to improve the functionality and security of IoT devices if we create a mechanism for recovering data that has been deleted from those devices. This will make these devices more reliable for both individuals and businesses. The process of searching a storage device for remnants of deleted files is referred to as "carving" files. This piece of software will extract these fragments and then put them back together into a whole file. Memory analysis is the process of analyzing the memory of a computer in order to locate and recover data that was previously deleted.

Recovering data that was deleted prior to it being written to a storage device can be accomplished with the help of this method. The process of "data carving" involves searching for recurring patterns within the information held on a storage device. This method is helpful in situations where it would be difficult to recover data using more traditional methods, such as when the file system has become corrupted and deleted files need to be recovered. Hex editors are one of the tools that can be used in a deleted data recovery mechanism. Other tools that can be used in this mechanism include forensic analysis tools, disk imaging tools, and hex editors. The kind of storage device, the degree to which data was lost, and the intricacy of the investigation all play a role in the choice of recovery tools that are implemented in a mechanism for erasing data and retrieving it later.

3.Background

The amount of data produced by these devices has grown exponentially along with the Internet of Things (IoT) industry's rapid expansion. The Internet of Things (IoT) is a network of small computing devices that can collect, process, and transmit data. These gadgets can be put to use in a variety of settings, including manufacturing, transportation, and the medical field.

However, as the use of these devices has grown, concerns over security and privacy have also grown. These devices produce sensitive data that can include sensitive personal information like biometric data, financial information, and location data. If this information ends up in the wrong hands, it might be used maliciously for things like fraud, identity theft, and cyberattacks.

Delete sensitive data once it is no longer required is one of the common ways to protect it. However, merely deleting data does not guarantee that it is permanently lost. The data can still be recovered with the aid of cutting-edge methods and tools. The privacy and security of sensitive data produced by IoT devices are seriously jeopardized by this.

As a result, IoT devices need a deleted data recovery mechanism that can effectively and securely recover deleted data. A mechanism like this can be used to recover crucial data that may have been accidentally or intentionally deleted. It is an important tool for digital forensics because it can be used to gather data for legal investigations.

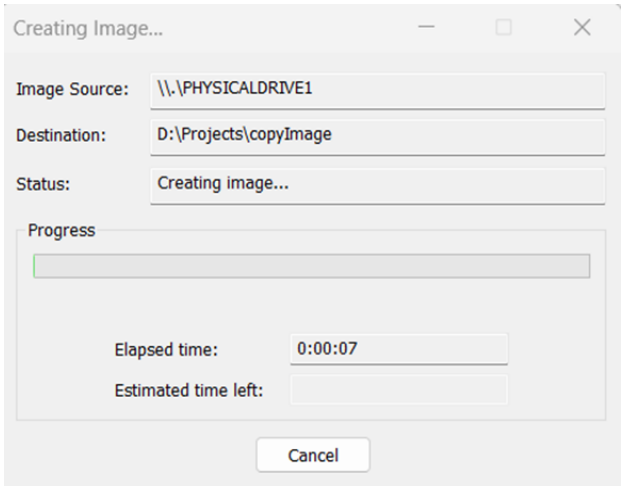
4. Methods

Performing data carving, file carving, and memory analysis on a flash drive requires forensic analysis tools and techniques. Here are the general steps that the team followed:

We made use of two softwares: Autopsy and Scalpel

1. Autopsy

Obtain a forensic image of the flash drive: Before performing any analysis on the flash drive, it is important to create a forensic image of the drive. This will ensure that the original data on the drive is preserved and can be used as evidence if required.



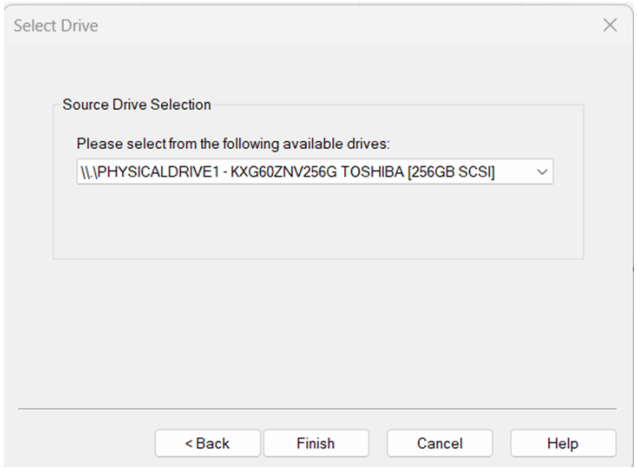


Figure 1 and 2

The above picture shows the name of the storage device to be selected for creating the data source and making a forensic image of it.

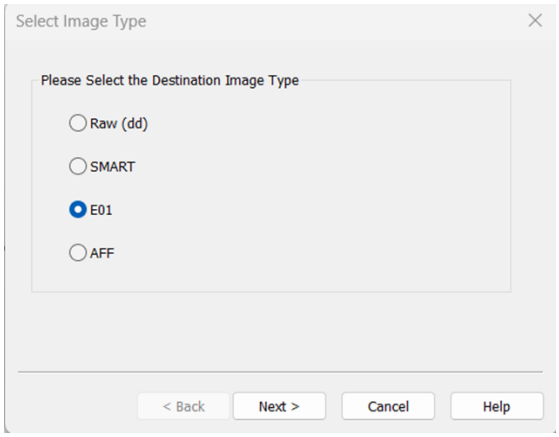


Figure 3

The above picture asks you to choose the destination image type.

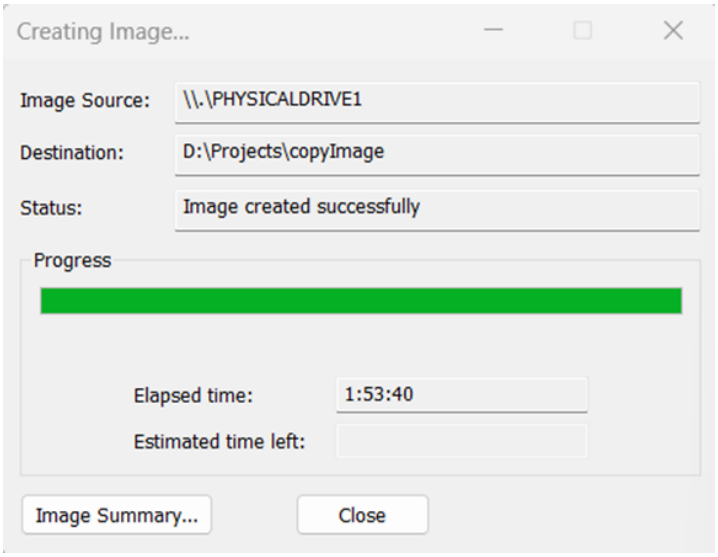


Figure 4

The above picture shows the progress of the forensic image.

We used a software write blocker. Before connecting the flash drive to the forensic workstation, it is important to use a write blocker. This is a device that ensures that no data can be written to the drive during the imaging process, which helps to maintain the integrity of the original data. Write blockers can be hardware or software-based, and there are many options available.

We then created a forensic image. This will create a bit-by-bit copy of the drive, including all data, metadata, and deleted files.

After the image was created, it is important to verify its integrity. This can be done using tools such as md5sum or sha256sum, which calculate a hash value for the image. We compared the hash value of the image to the hash value of the original drive to ensure that the image is an exact copy. The tool autopsy had an option to verify the image while creating it.

Figure 5

Once the image is verified, it was stored in a secure location. This may be on a separate drive or on a network storage device. We saved it on the computer we are working on. It is important to keep the image in a safe and secure location to prevent any accidental modification or loss.

We then analyzed the image for deleted or hidden files. Using the “keyword search” button, we looked for files with extensions - .jpg, .png, .pdf, .txt.

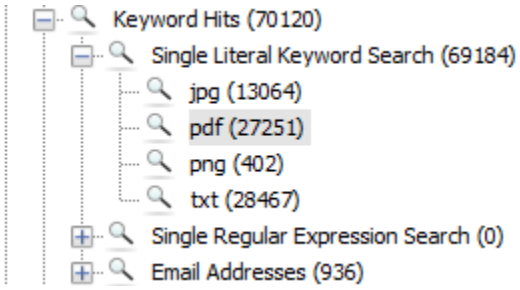


Figure 6

There were numerous deleted files found. These files included wallpapers, flight tickets, python files, and some personal photos.

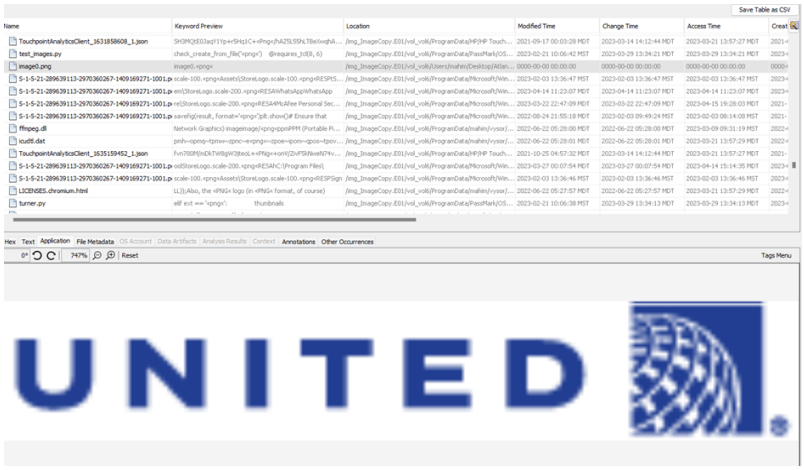


Figure 7

The above image shows the files recovered from ‘keyword search”. One image which was recovered was the logo of the United Airlines, which shows that there might be a possibility that the user might have had international flight bookings.

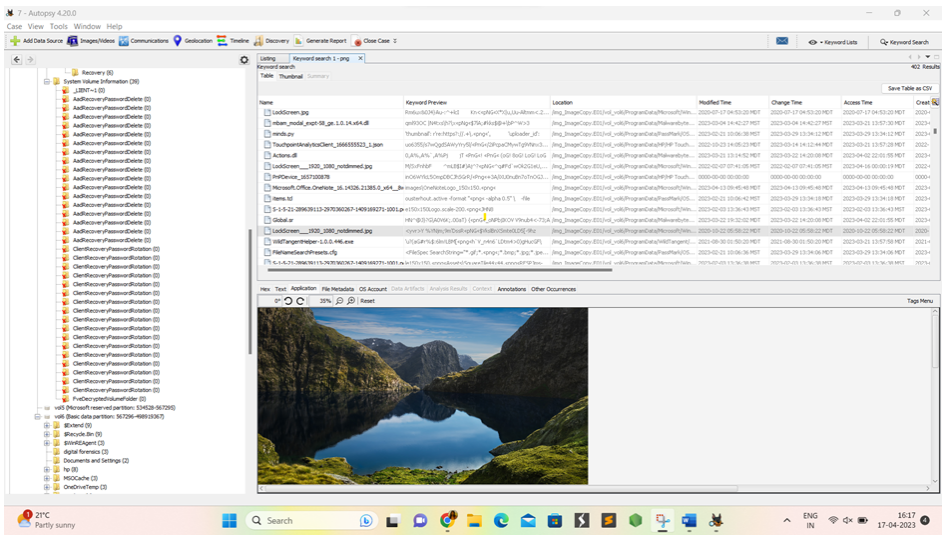


Figure 8

The above pictures show some wallpapers which were recovered.

2. Foremost

In the following steps we will be performing Digital Fingerprint, Data Carving & Data recovery of deleted files using Foremost on a Linux machine. Foremost is a digital forensics tool that is used to recover files based on their headers, footers, and data structures.

After successfully retrieving a flash drive of any IOT device, the forensic investigator must first ensure that the we must create a hash of a drive before conducting a digital forensics investigation. This is vital as it ensures the integrity and authenticity of the evidence collected during the investigation.

In the following subsequent screenshots we see that after installing the Foremost tool on our Ubuntu Linux machine we first check use the "*fdisk -l*" command to list the partitions on a storage device in a Linux system.

As shown in the screenshot below we have identified our drive consisting of deleted files and will now have to use the tool for data recovery.

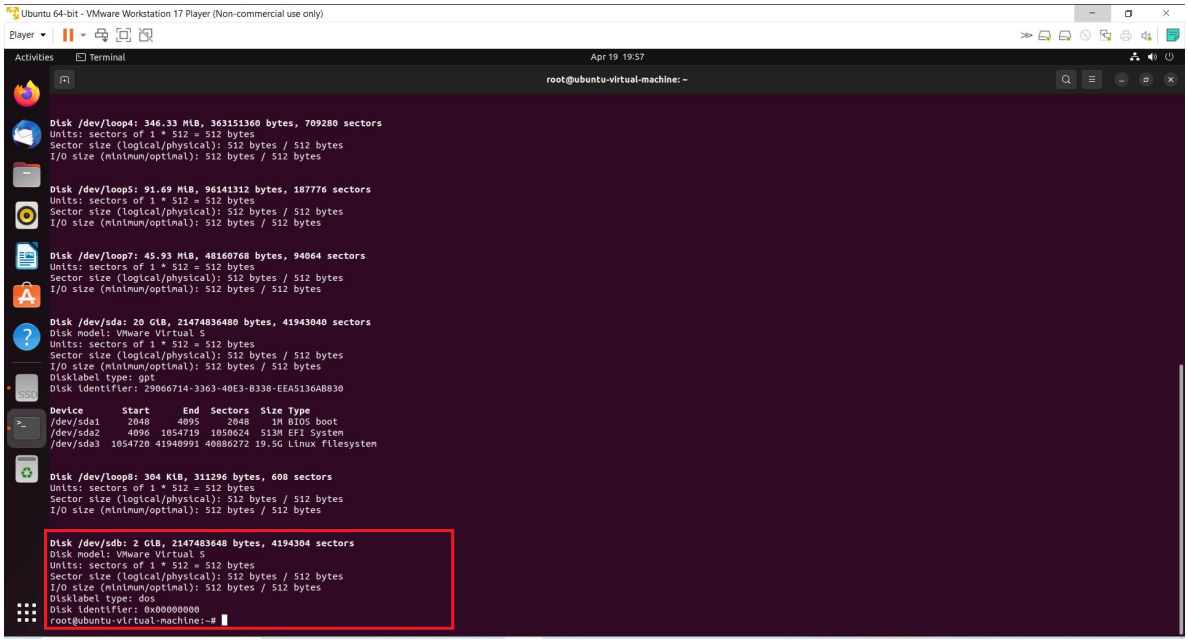


Figure 9

Having identified our drive to scan, we will now proceed with running the Foremost tool as shown below.

On running the command "foremost -h" we are provided with the following options. Foremost supports a number of file types, including .jpg, .gif, .png, .bmp, .avi, .mpg,

.wav, .mov, .pdf, .doc, .zip, and.mp4 as we see below before when using the man foremost command

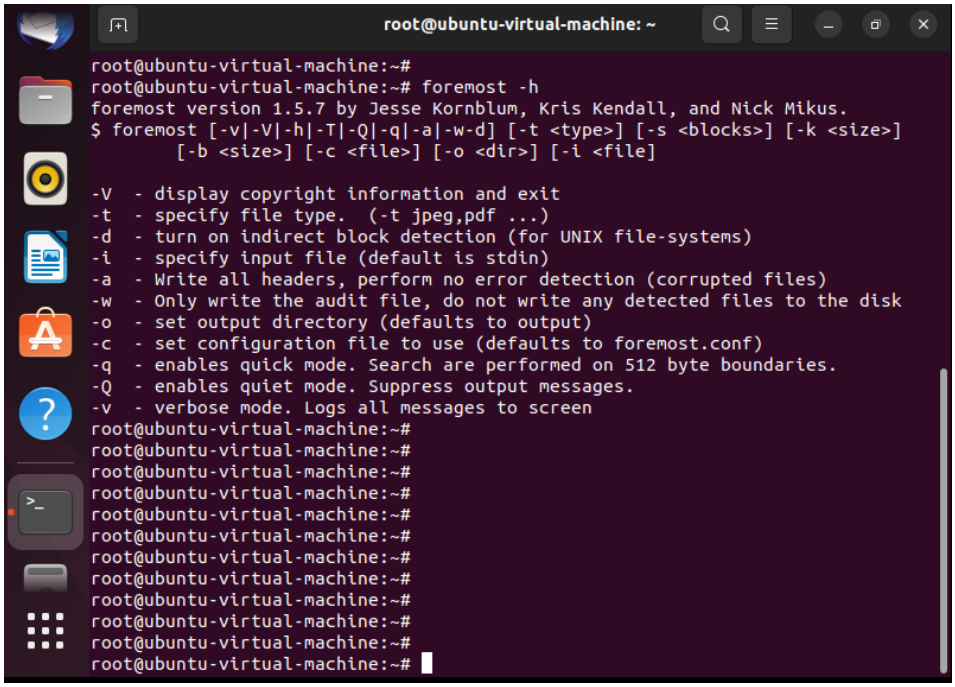


Figure 10

In the next step we will create a hash of the drive that we intend to scan, maintaining the integrity of the digital evidence collected during a forensic investigation and is a standard practice in the field of digital forensics. In the example shown in the screenshots the storage that we will be analyzing is /dev/sdb and we will create a hash of the drive. The hash value created is in the form of MD5.

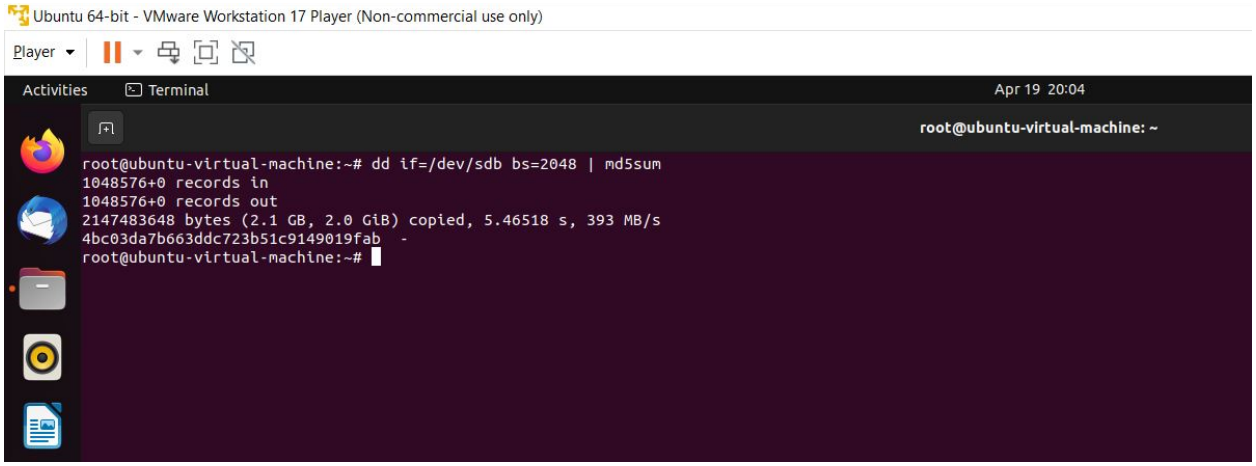


Figure 11

Having obtained the hash value of the drive, we proceed with creation of a image of the partition using the following commands and copy the image to desired location-

"*dd if=/dev/sdb of=/home/ubuntu/Desktop/Test/test.img bs=2048*"

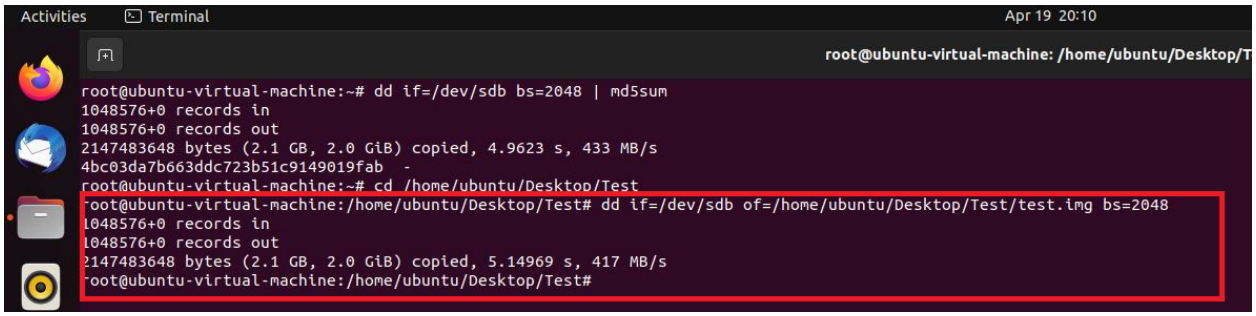


Figure 12

To validate that the authenticity of the image we must compare the hash values, this shows us that the contents of the partition has not been tampered. Comparing the hash values of the two we find the following.

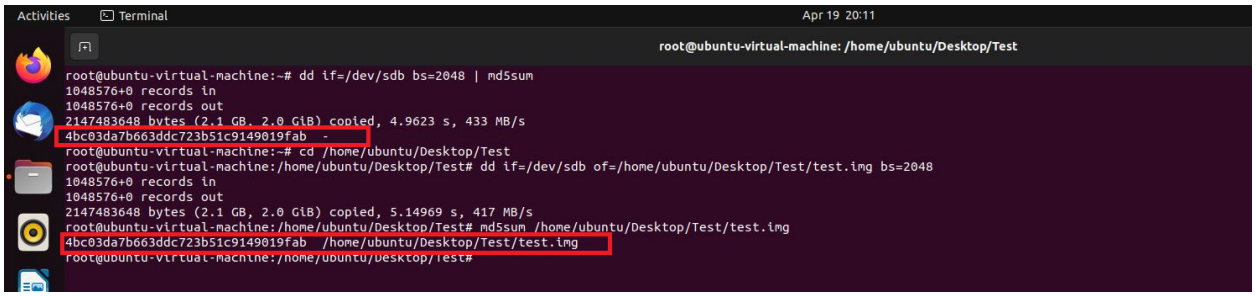


Figure 13

This indicates that the hash values are not tampered and that we created a digital copy of the partition that we intend to scan. After creating the .img file we will now use the Foremost tool to scan our .img file. Before triggering the scan we must make sure that we review the foremost.conf file such that we can customize its behavior and file recovery capabilities. The file is used to specify the tool's many settings, such as the file types that will be recovered, the output directory, and the largest file that may be recovered.

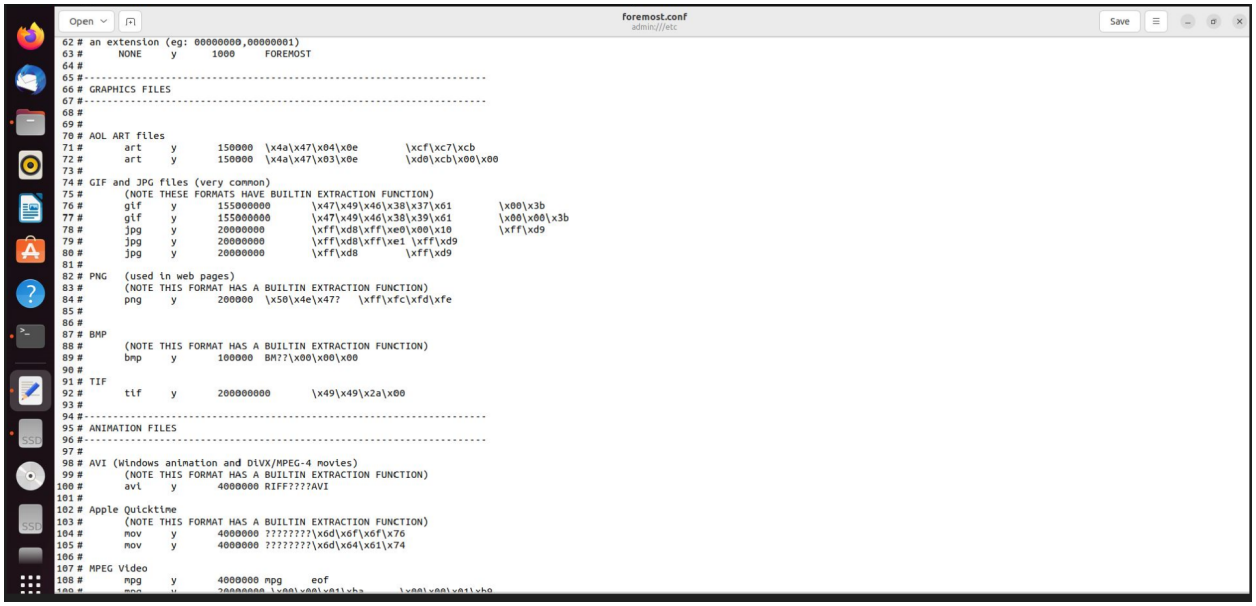


Figure 14

In the next step, we will proceed with scanning our drive using the following command→

"***sudo foremost -i test.img***".

We can further modify our command such that we are able to scan the storage device's binary data for specific file signatures or headers and then extract the data associated with those files. Some sample commands are as follows:

- To search for PDF Files : "***foremost -i /dev/sdb -o /output/directory -t pdf***"
- To search and skip files larger than 20MB : "***foremost -i /dev/sdb -o /output/directory -s 20m***"
- To search for ZIP files with custom header signature : "***foremost -i /dev/sdb -o /output/directory -c custom.zip:/FF/FF/FF/FF/***"

On running the command we will now see on the console that the tool starts to run the scan based on the configurations and arguments passed on the commands.

```
root@ubuntu-virtual-machine:/home/ubuntu/Desktop/Test# cd /home/ubuntu/Desktop/Test
root@ubuntu-virtual-machine:/home/ubuntu/Desktop/Test# ls
test.img
root@ubuntu-virtual-machine:/home/ubuntu/Desktop/Test# sudo foremost -i test.img
Processing: test.img
|foundat=_rels/.rels ◆(◆
*******************|
root@ubuntu-virtual-machine:/home/ubuntu/Desktop/Test#
```

Figure 15

The -i option tells foremost to scan the specified input device, which in this case is test.img which is a device file that represents a block device, such as a hard drive or a

USB flash drive. Recovered files are saved to the output directory given by the -o option or the default output directory.

On Navigating to the appropriate folder we see that the recovered files that were discovered during the scan are located in the output folder that is created when you run the foremost command. Based on the categories of files they contain, the recovered files are arranged in subfolders.

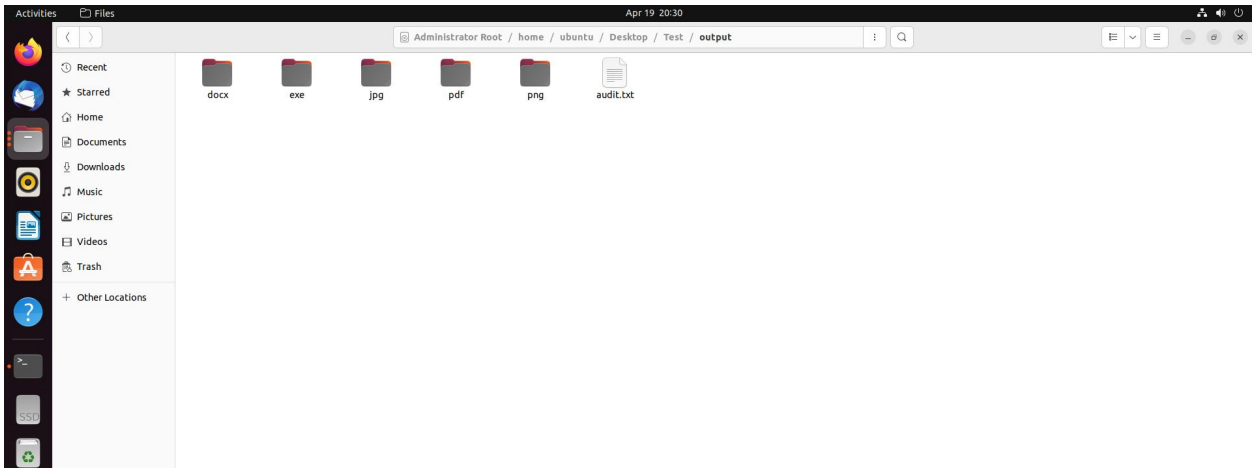


Figure 16

After successfully scanning, foremost will create folders and subfolders for all different types of extensions. A folder called pdf will be created in the output folder and the file will be saved there if first recovers a PDF file with the name example.pdf.

A log file that contains a summary of the outcomes of the data recovery scan is created first in the output folder and is called audit.txt. It includes details about the quantity of files discovered, the categories of data recovered, and any scanning mistakes. In the following scenario we see that after the scan we are able to get several recovered files that the tool was able to recover files from storage of the Ring Doorbell device. By using the File Carving techniques the tool was able to recover deleted or lost files from the storage device by searching for file headers and footers.

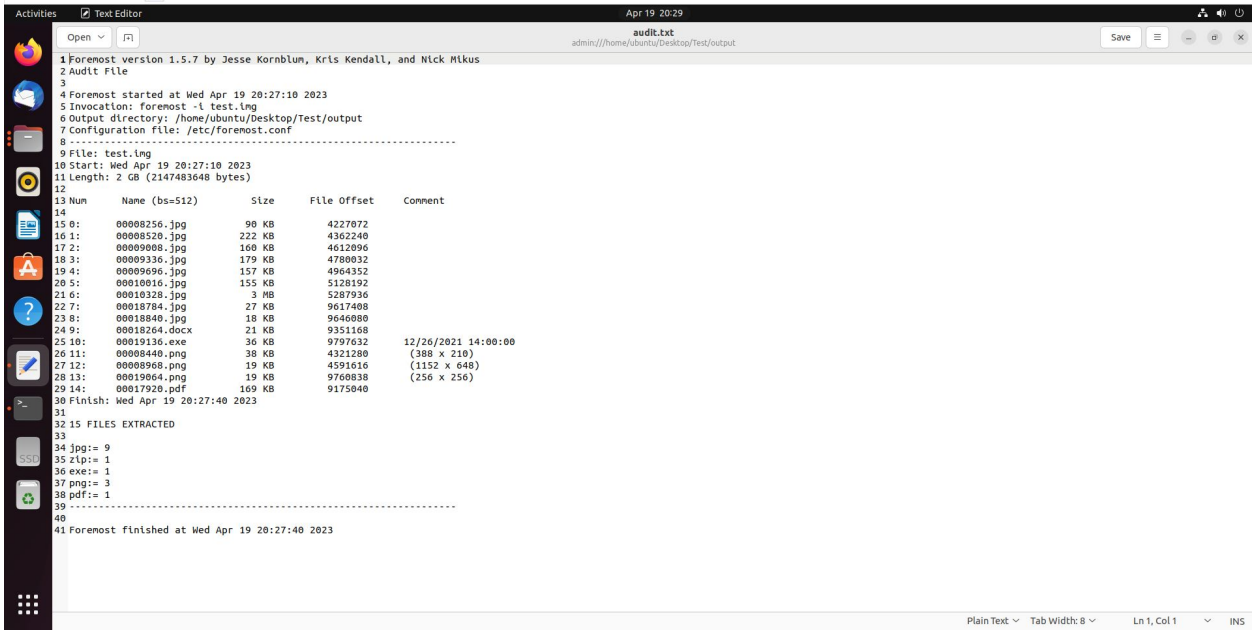


Figure 17

The above image shows the types of files that were recovered after the scan, this indicates that the software was able to recover the lost data. The .txt file contains detailed information such as:

- Recovery statistics
- File details
- Total number of files recovered
- Error messages

5. Conclusion

The need to protect the security and privacy of the data produced by IoT devices grows as we move toward a more connected world thanks to their widespread use. A dependable and effective data recovery mechanism is necessary because these devices are increasingly being used to store sensitive data.

In order to recover deleted data from a variety of different IoT devices and storage systems, the proposed solution in this project makes use of cutting-edge techniques and tools, including file carving, memory analysis, and data carving. Wearable technology, smart home technology, industrial IoT technology, among other IoT devices, can all use these techniques.

Forensic investigators can recover crucial data that may have been deleted accidentally or on purpose by developing a working deleted data recovery mechanism. This mechanism is useful for digital forensics because it can be used to gather evidence in

criminal investigations. The mechanism can be especially helpful in situations where data may have been removed in order to hide wrongdoing or restrict access to sensitive data.

The project highlights the significance of creating efficient data recovery mechanisms for IoT devices and lays the groundwork for future research in the field of digital forensics. To ensure the security and privacy of the data produced by IoT devices as their use expands, it is crucial to stay current with the most recent developments in data recovery techniques and tools.

6. References

[1] "Top 10 Best Free Data Recovery Software of 2022" by TechPout - https://www.techpout.com/best-free-data-recovery-software/

[2] "How to Recover Deleted Files in Windows" by How-To Geek - https://www.howtogeek.com/169344/how-to-recover-a-deleted-file-the-ultimate-guide/

[3] "Best Data Recovery Software for Mac of 2022" by Techsviewer - https://techsviewer.com/best-data-recovery-software-for-mac/

[4] "The Ultimate Guide to Data Recovery: How to Recover Lost Files and Deleted Data" by EaseUS - https://www.easeus.com/datarecoverywizard/recover-deleted-files.htm

[5] "5 Common Causes of Data Loss and How to Prevent Them" by Norton - https://us.norton.com/internetsecurity-emerging-threats-5-common-causes-of-data-loss-and-how-to-prevent-them.html

[6] "How Does Data Recovery Work? A Beginner's Guide" by Prosoft Engineering - https://www.prosofteng.com/blog/how-does-data-recovery-work-a-beginners-guide/

[7] "10 Mistakes to Avoid When Recovering Lost Data" by Techradar - https://www.techradar.com/how-to/10-mistakes-to-avoid-when-recovering-lost-data

[8] "The Importance of Backing Up Your Data" by PCMag - https://www.pcmag.com/how-to/the-importance-of-backing-up-your-data

[9] "How to Recover Deleted Files from External Hard Drive on Mac" by Stellar Data Recovery -

https://www.stellarinfo.com/blog/recover-deleted-files-from-external-hard-drive-on-mac/

[10] "Deleted Files Recovery from Recycle Bin and Cloud Storage" by MiniTool - https://www.minitool.com/data-recovery/deleted-files-recovery.html

Appendix A

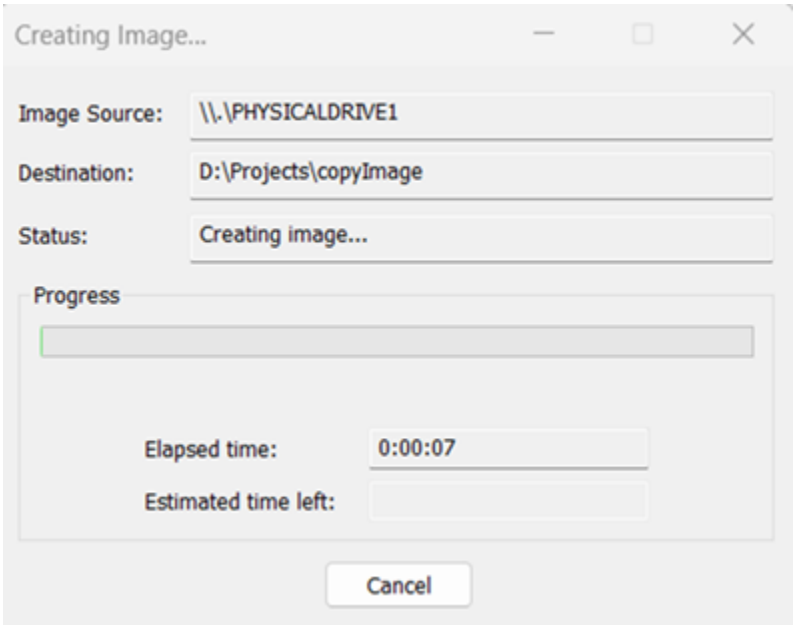


Figure 1: Creating a forensic image

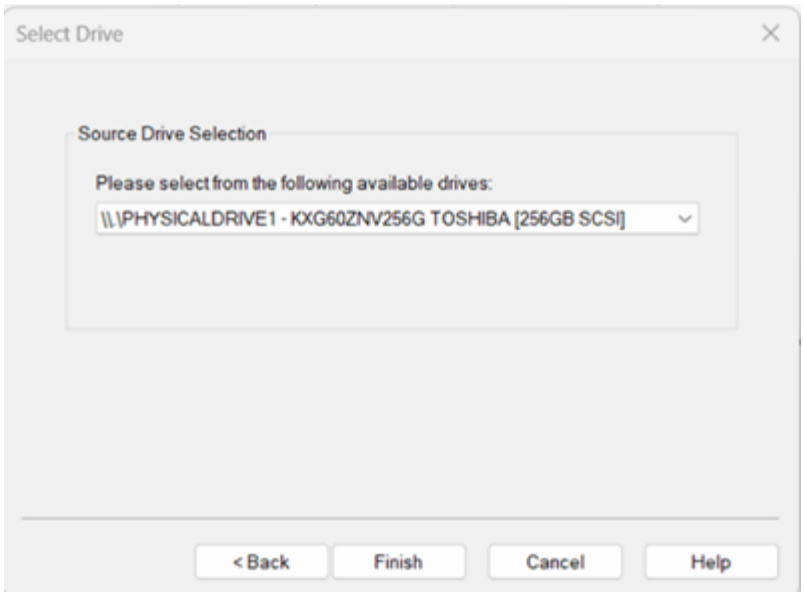


Figure 2: Storage device to be selected

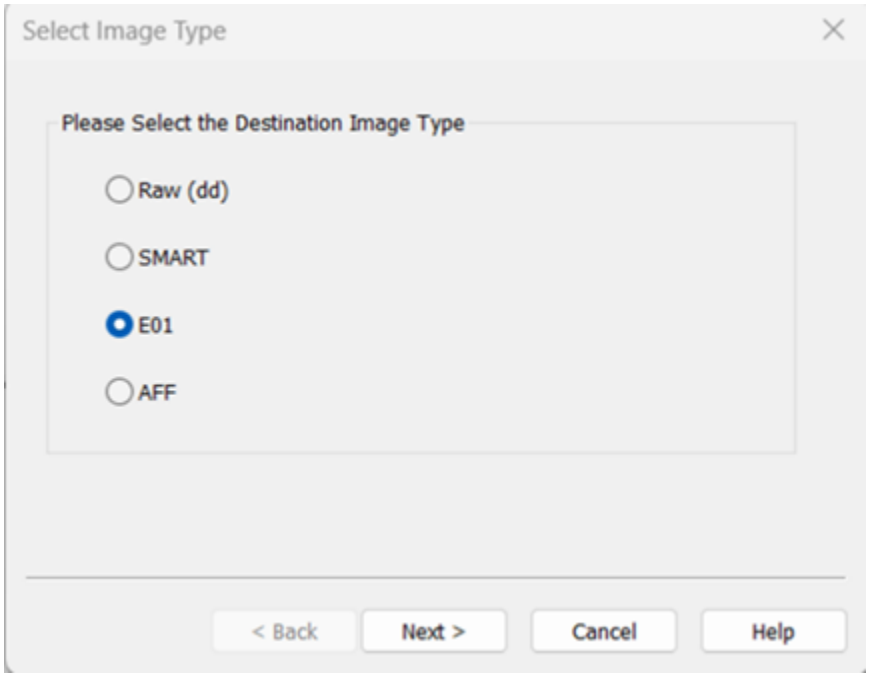


Figure 3: Destination image type

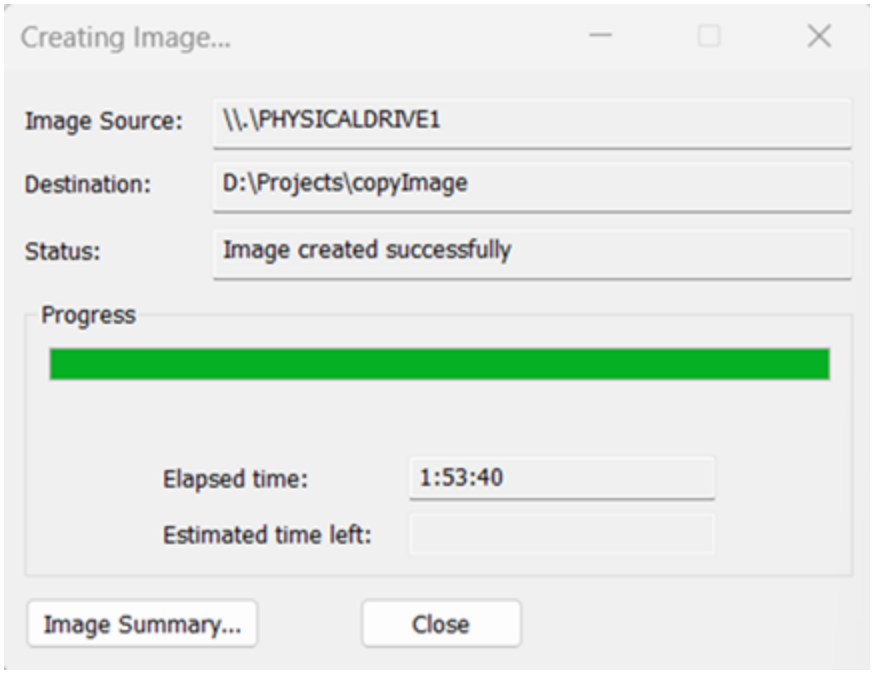


Figure 4: Forensic image created

Figure 5: Image Verification

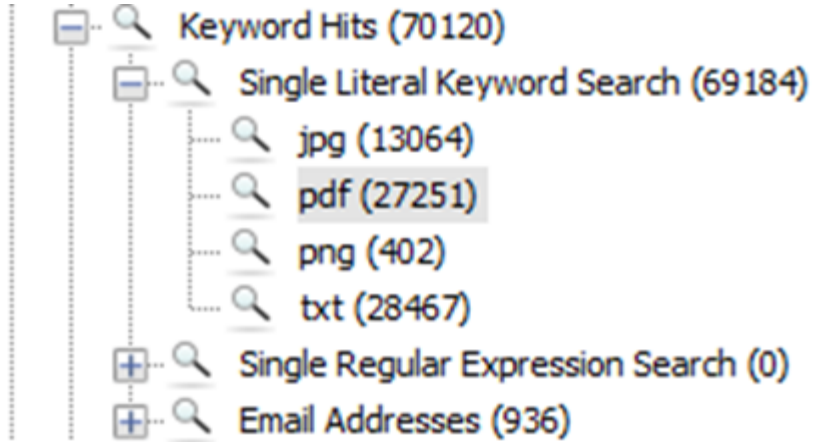


Figure 6: Numerous deleted files found

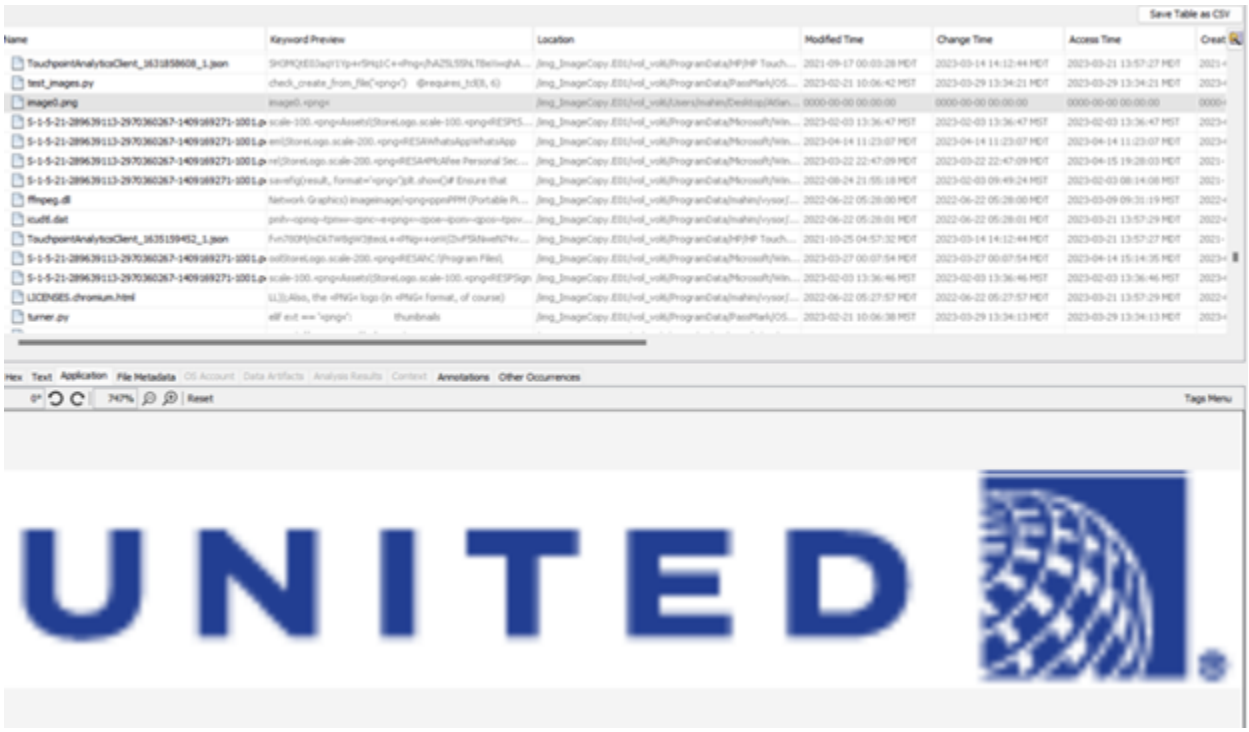


Figure 7: Files recovered from ‘keyword search”

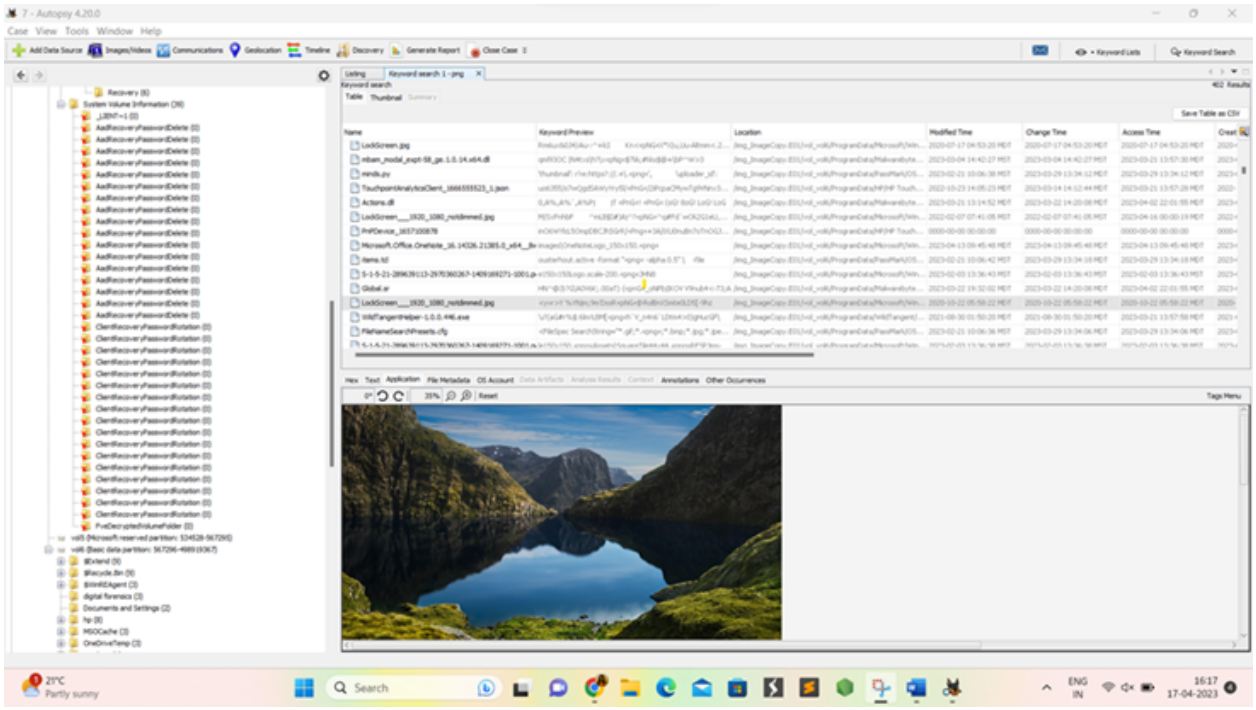


Figure 8: Wallpapers which were recovered

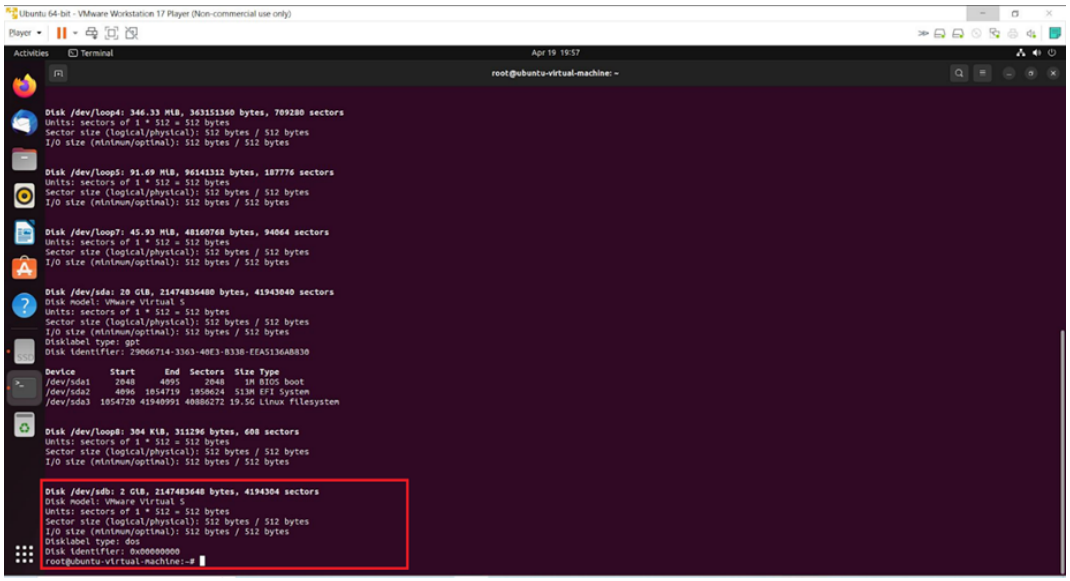


Figure 9

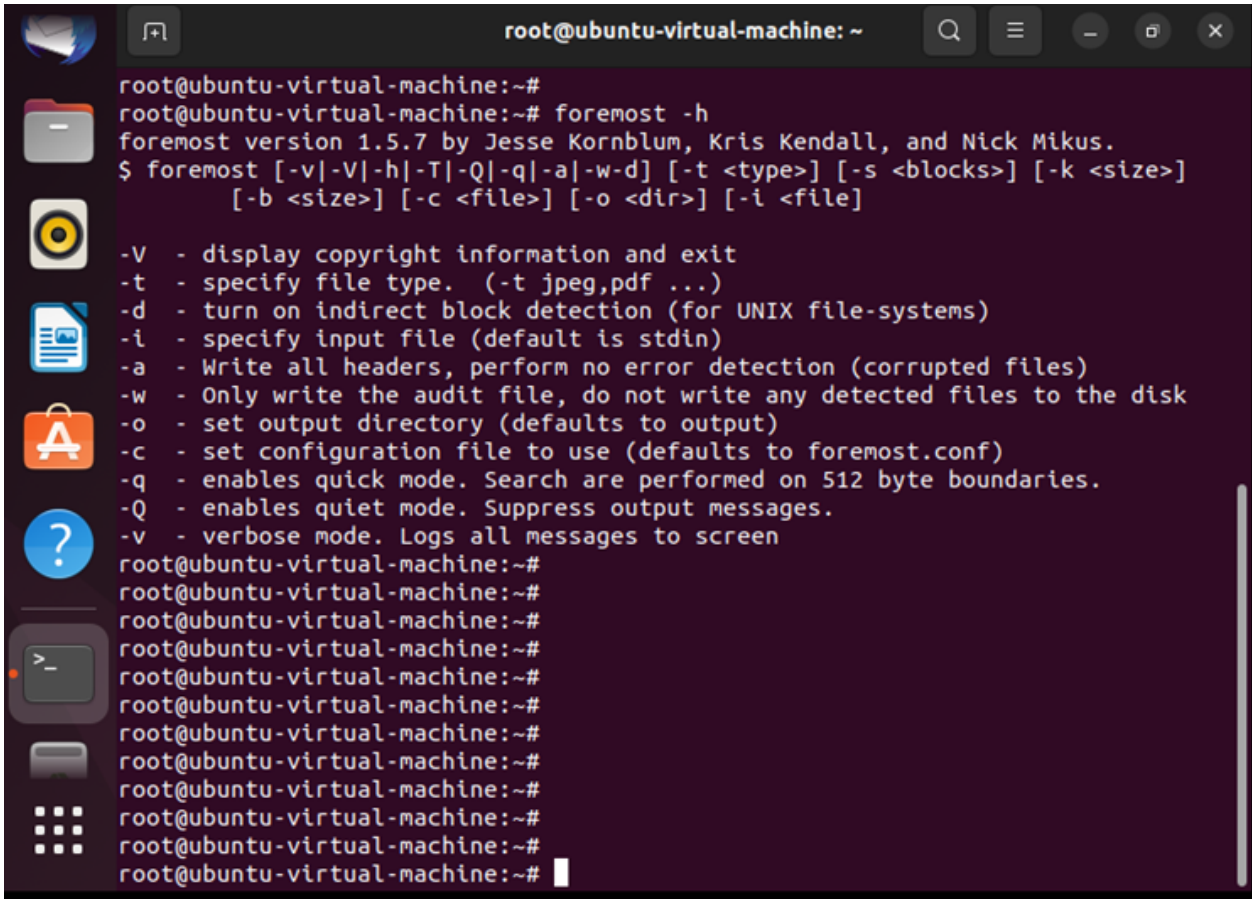


Figure 10: Creation of a hash of the drive

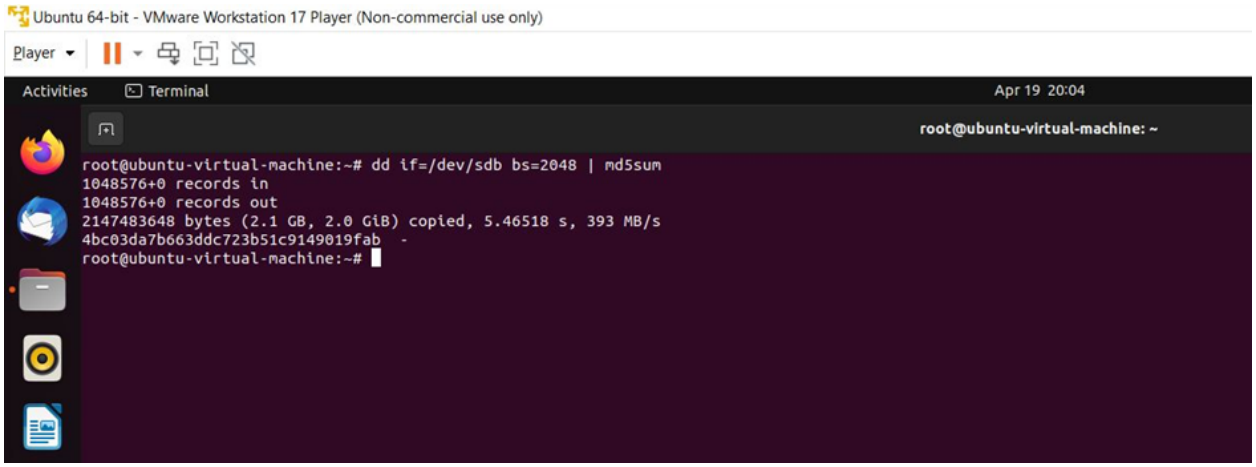


Figure 11: Creation of an image

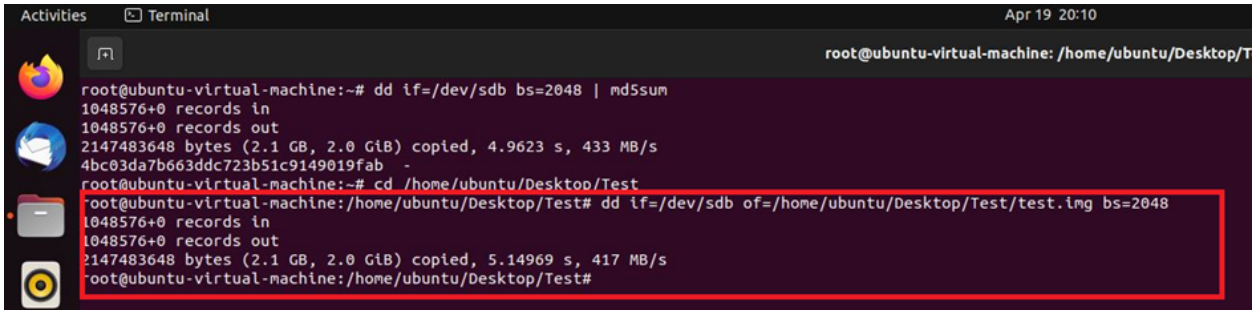


Figure 12: Contents of the partition has not been tampered

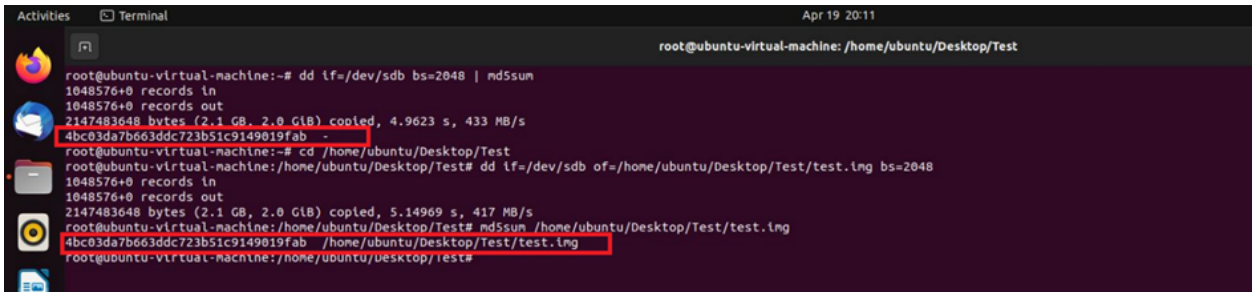


Figure 13: Non tampered hash values and creation of a digital copy

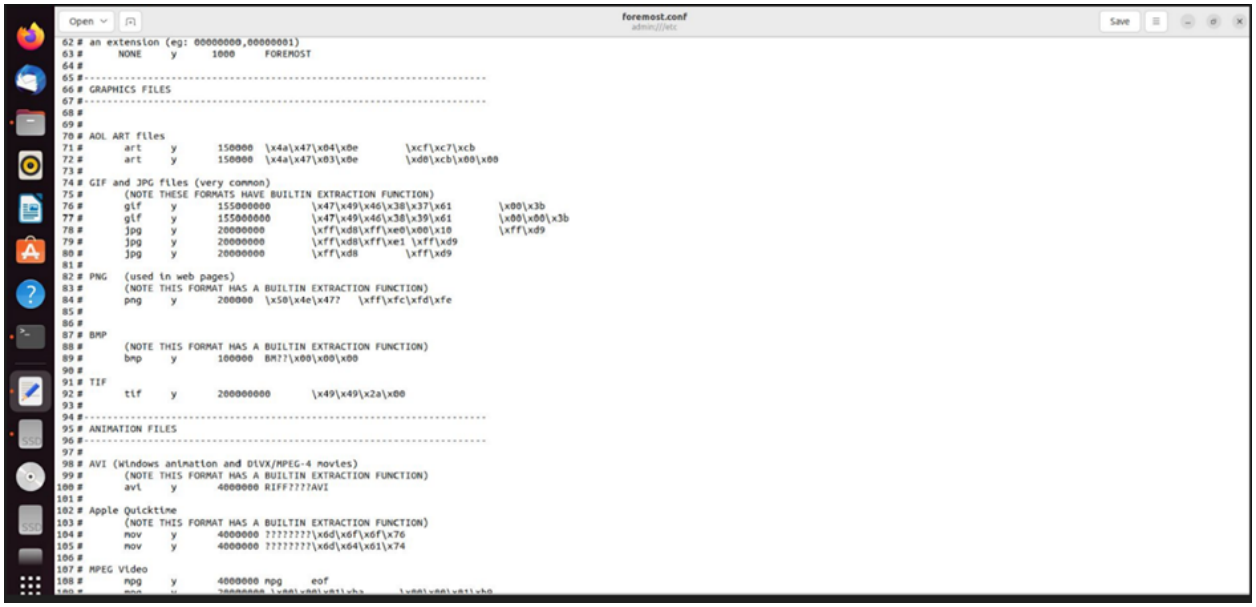


Figure 14

```
root@ubuntu-virtual-machine:/home/ubuntu/Desktop/Test# cd /home/ubuntu/Desktop/Test
root@ubuntu-virtual-machine:/home/ubuntu/Desktop/Test# ls
test.img
root@ubuntu-virtual-machine:/home/ubuntu/Desktop/Test# sudo foremost -i test.img
Processing: test.img
|foundat=_rels/.rels ◆(◆
**********|
root@ubuntu-virtual-machine:/home/ubuntu/Desktop/Test#
```

Figure 15: The -i option tells foremost to scan the specified input device

Figure 16: Foremost will create folders and subfolders

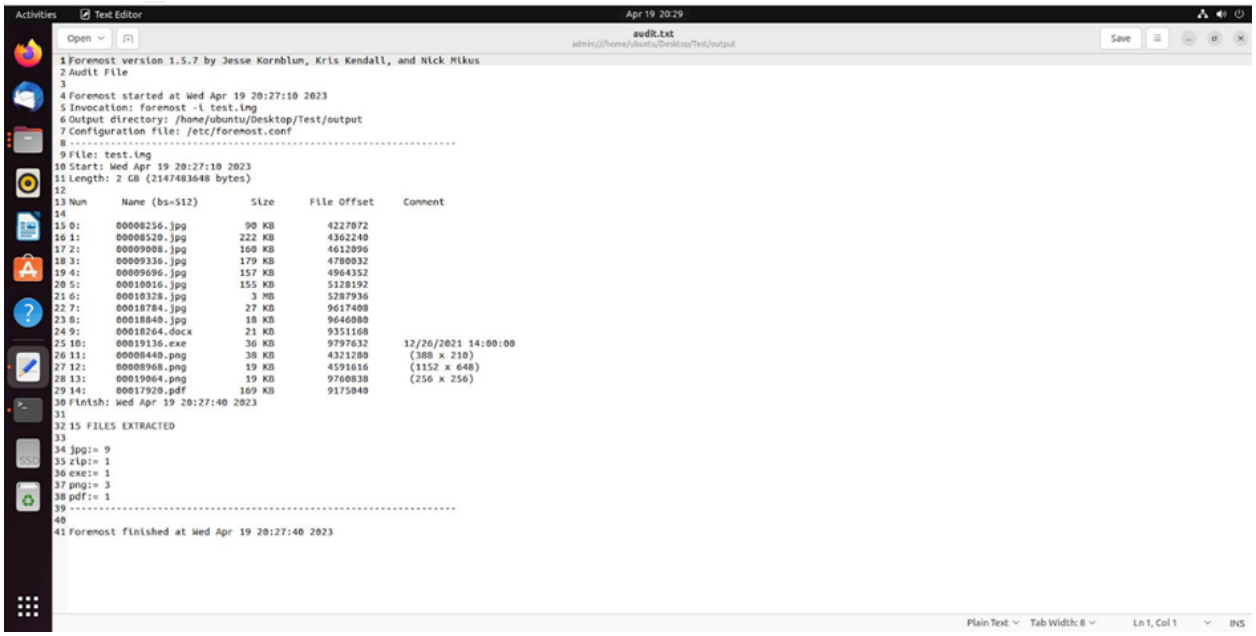


Figure 17: Types of files that were recovered