INT301 Project

Use any open source software to extract data from disk drives and other storage so as to facilitate the forensic analysis of computer systems.

Introduction:

The objective of this project is to demonstrate how to use TestDisk to extract data from disk drives. TestDisk is a powerful open-source data recovery tool that can be used to recover lost or damaged partitions, repair boot sectors, and fix filesystems. In this project, we will explore the various features of TestDisk and learn how to use them to extract data from disk drives.

1.Free and Open Source: TestDisk is available for free and is open-source software, which means it can be modified and customized by developers to suit their specific needs.

2.Cross-platform Support: TestDisk is compatible with a variety of operating systems, including Windows, macOS, and Linux.

3.Support for Multiple File Systems: TestDisk can handle a wide range of file systems, including FAT, NTFS, exFAT, ext2/ext3/ext4, HFS+, and more, making it a versatile tool for data recovery and forensic analysis.

4.Recovery of Lost Partitions: TestDisk can recover lost or damaged partitions, making it possible to retrieve data that may have been lost due to partition errors or system crashes.

5.User-Friendly Interface: TestDisk comes with a simple, easy-to-use interface that allows users to navigate and operate the tool with ease.

6.Command-line Support: For advanced users, TestDisk also provides a command-line interface that allows them to perform more complex operations and customize the tool according to their needs.

7.Portable: TestDisk is a portable application that can be run from a USB drive or other external storage devices, making it easy to carry around and use on different systems.

1.1Objective:

The objective of this project is to extract data from disk drives and other storage so as to facilitate the forensic analysis of computer systems.

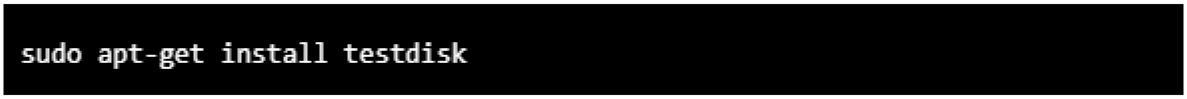
1.2 Description:

The project will consist of several steps, including the installation of TestDisk, the creation of a test disk image, and the recovery of lost data from the image using TestDisk. We will first provide an overview of TestDisk and its features, followed by a detailed explanation of each step.

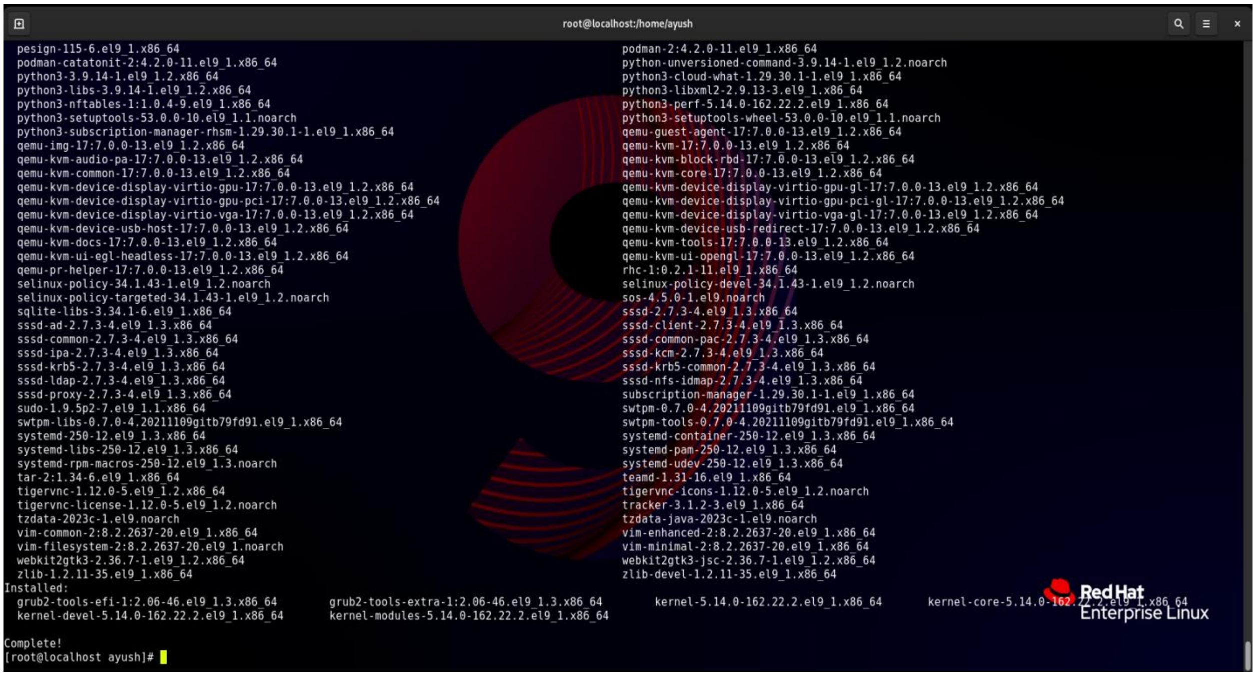
Step 1: Install TestDisk

The first step is to download and install TestDisk. TestDisk is available for all major operating systems including Windows, macOS, and Linux.

On Linux, you can install TestDisk using the following command in the terminal :- sudo apt-get install testdisk



```
sudo apt-get install testdisk
```

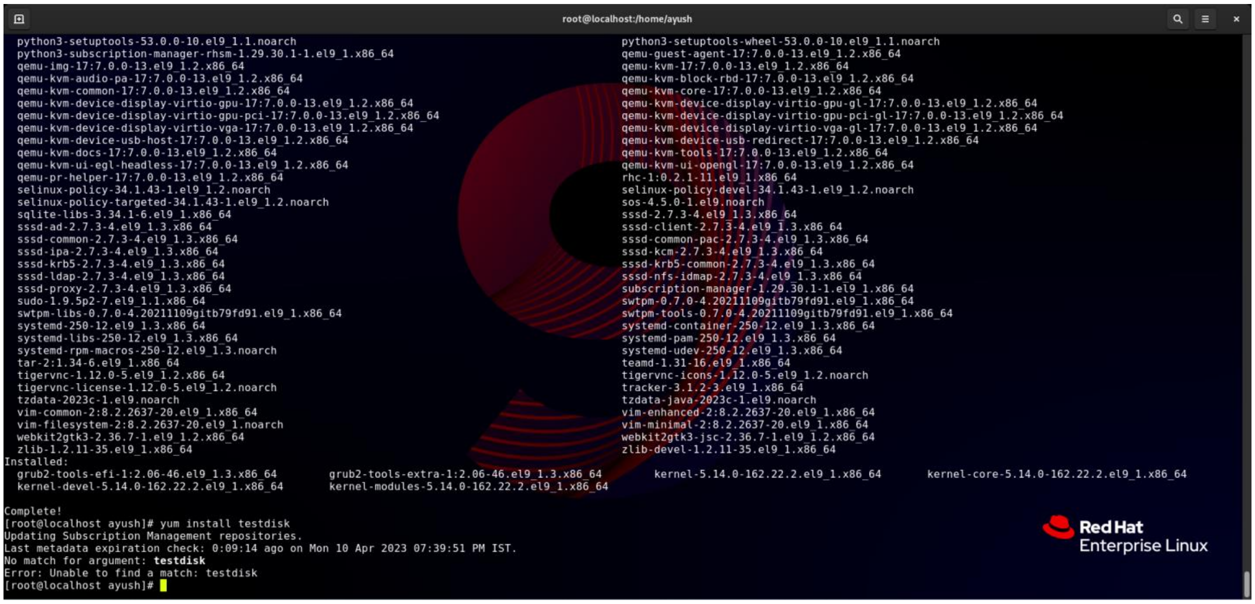


root@localhost:/home/ayush

```
  pesign-115-6.el9_1.x86_64                                             podman-2:4.2.0-11.el9_1.x86_64
  podman-catatonit-2:4.2.0-11.el9_1.x86_64                              python-unversioned-command-3.9.14-1.el9_1.2.noarch
  python3-3.9.14-1.el9_1.2.x86_64                                       python3-cloud-what-1.29.30.1-1.el9_1.x86_64
  python3-libs-3.9.14-1.el9_1.2.x86_64                                  python3-libxml2-2.9.13-3.el9_1.x86_64
  python3-nftables-1:1.0.4-9.el9_1.x86_64                               python3-perf-5.14.0-162.22.2.el9_1.x86_64
  python3-setuptools-53.0.0-10.el9_1.1.noarch                           python3-setuptools-wheel-53.0.0-10.el9_1.1.noarch
  python3-subscription-manager-rhsm-1.29.30.1-1.el9_1.x86_64            qemu-guest-agent-17:7.0.0-13.el9_1.2.x86_64
  qemu-img-17:7.0.0-13.el9_1.2.x86_64                                   qemu-kvm-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-audio-pa-17:7.0.0-13.el9_1.2.x86_64                          qemu-kvm-block-rbd-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-common-17:7.0.0-13.el9_1.2.x86_64                            qemu-kvm-core-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-device-display-virtio-gpu-17:7.0.0-13.el9_1.2.x86_64         qemu-kvm-device-display-virtio-gpu-gl-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-device-display-virtio-gpu-pci-17:7.0.0-13.el9_1.2.x86_64     qemu-kvm-device-display-virtio-gpu-pci-gl-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-device-display-virtio-vga-17:7.0.0-13.el9_1.2.x86_64         qemu-kvm-device-display-virtio-vga-gl-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-device-usb-host-17:7.0.0-13.el9_1.2.x86_64                   qemu-kvm-device-usb-redirect-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-docs-17:7.0.0-13.el9_1.2.x86_64                              qemu-kvm-tools-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-ui-egl-headless-17:7.0.0-13.el9_1.2.x86_64                   qemu-kvm-ui-opengl-17:7.0.0-13.el9_1.2.x86_64
  qemu-pr-helper-17:7.0.0-13.el9_1.2.x86_64                             rhc-1:0.2.1-11.el9_1.x86_64
  selinux-policy-34.1.43-1.el9_1.2.noarch                               selinux-policy-devel-34.1.43-1.el9_1.2.noarch
  selinux-policy-targeted-34.1.43-1.el9_1.2.noarch                      sos-4.5.0-1.el9.noarch
  sqlite-libs-3.34.1-6.el9_1.x86_64                                     sssd-2.7.3-4.el9_1.3.x86_64
  sssd-ad-2.7.3-4.el9_1.3.x86_64                                        sssd-client-2.7.3-4.el9_1.3.x86_64
  sssd-common-2.7.3-4.el9_1.3.x86_64                                    sssd-common-pac-2.7.3-4.el9_1.3.x86_64
  sssd-ipa-2.7.3-4.el9_1.3.x86_64                                       sssd-kcm-2.7.3-4.el9_1.3.x86_64
  sssd-krb5-2.7.3-4.el9_1.3.x86_64                                      sssd-krb5-common-2.7.3-4.el9_1.3.x86_64
  sssd-ldap-2.7.3-4.el9_1.3.x86_64                                      sssd-nfs-idmap-2.7.3-4.el9_1.3.x86_64
  sssd-proxy-2.7.3-4.el9_1.3.x86_64                                     subscription-manager-1.29.30.1-1.el9_1.x86_64
  sudo-1.9.5p2-7.el9_1.1.x86_64                                         swtpm-0.7.0-4.20211109gitb79fd91.el9_1.x86_64
  swtpm-libs-0.7.0-4.20211109gitb79fd91.el9_1.x86_64                    swtpm-tools-0.7.0-4.20211109gitb79fd91.el9_1.x86_64
  systemd-250-12.el9_1.3.x86_64                                         systemd-container-250-12.el9_1.3.x86_64
  systemd-libs-250-12.el9_1.3.x86_64                                    systemd-pam-250-12.el9_1.3.x86_64
  systemd-rpm-macros-250-12.el9_1.3.noarch                              systemd-udev-250-12.el9_1.3.x86_64
  tar-2:1.34-6.el9_1.x86_64                                             teamd-1.31-16.el9_1.x86_64
  tigervnc-1.12.0-5.el9_1.2.x86_64                                      tigervnc-icons-1.12.0-5.el9_1.2.noarch
  tigervnc-license-1.12.0-5.el9_1.2.noarch                              tracker-3.1.2-3.el9_1.x86_64
  tzdata-2023c-1.el9.noarch                                             tzdata-java-2023c-1.el9.noarch
  vim-common-2:8.2.2637-20.el9_1.x86_64                                 vim-enhanced-2:8.2.2637-20.el9_1.x86_64
  vim-filesystem-2:8.2.2637-20.el9_1.noarch                             vim-minimal-2:8.2.2637-20.el9_1.x86_64
  webkit2gtk3-2.36.7-1.el9_1.2.x86_64                                   webkit2gtk3-jsc-2.36.7-1.el9_1.2.x86_64
  zlib-1.2.11-35.el9_1.x86_64                                           zlib-devel-1.2.11-35.el9_1.x86_64
Installed:
  grub2-tools-efi-1:2.06-46.el9_1.3.x86_64       grub2-tools-extra-1:2.06-46.el9_1.3.x86_64       kernel-5.14.0-162.22.2.el9_1.x86_64       kernel-core-5.14.0-162.22.2.el9_1.x86_64
  kernel-devel-5.14.0-162.22.2.el9_1.x86_64      kernel-modules-5.14.0-162.22.2.el9_1.x86_64

Complete!
[root@localhost ayush]#
```

Once TestDisk is installed, you can launch it by running the following command:sudotestdisk

```
sudo testdisk
```



```
  python3-setuptools-53.0.0-10.el9_1.1.noarch                                                  python3-setuptools-wheel-53.0.0-10.el9_1.1.noarch
  python3-subscription-manager-rhsm-1.29.30.1-1.el9_1.x86_64                                   qemu-guest-agent-17:7.0.0-13.el9_1.2.x86_64
  qemu-img-17:7.0.0-13.el9_1.2.x86_64                                                          qemu-kvm-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-audio-pa-17:7.0.0-13.el9_1.2.x86_64                                                 qemu-kvm-block-rbd-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-common-17:7.0.0-13.el9_1.2.x86_64                                                   qemu-kvm-core-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-device-display-virtio-gpu-17:7.0.0-13.el9_1.2.x86_64                                qemu-kvm-device-display-virtio-gpu-gl-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-device-display-virtio-gpu-pci-17:7.0.0-13.el9_1.2.x86_64                            qemu-kvm-device-display-virtio-gpu-pci-gl-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-device-display-virtio-vga-17:7.0.0-13.el9_1.2.x86_64                                qemu-kvm-device-display-virtio-vga-gl-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-device-usb-host-17:7.0.0-13.el9_1.2.x86_64                                          qemu-kvm-device-usb-redirect-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-docs-17:7.0.0-13.el9_1.2.x86_64                                                     qemu-kvm-tools-17:7.0.0-13.el9_1.2.x86_64
  qemu-kvm-ui-egl-headless-17:7.0.0-13.el9_1.2.x86_64                                          qemu-kvm-ui-opengl-17:7.0.0-13.el9_1.2.x86_64
  qemu-pr-helper-17:7.0.0-13.el9_1.2.x86_64                                                    rhc-1:0.2.1-11.el9_1.x86_64
  selinux-policy-34.1.43-1.el9_1.2.noarch                                                      selinux-policy-devel-34.1.43-1.el9_1.2.noarch
  selinux-policy-targeted-34.1.43-1.el9_1.2.noarch                                             sos-4.5.0-1.el9.noarch
  sqlite-libs-3.34.1-6.el9_1.x86_64                                                            sssd-2.7.3-4.el9_1.3.x86_64
  sssd-ad-2.7.3-4.el9_1.3.x86_64                                                               sssd-client-2.7.3-4.el9_1.3.x86_64
  sssd-common-2.7.3-4.el9_1.3.x86_64                                                           sssd-common-pac-2.7.3-4.el9_1.3.x86_64
  sssd-ipa-2.7.3-4.el9_1.3.x86_64                                                              sssd-kcm-2.7.3-4.el9_1.3.x86_64
  sssd-krb5-2.7.3-4.el9_1.3.x86_64                                                             sssd-krb5-common-2.7.3-4.el9_1.3.x86_64
  sssd-ldap-2.7.3-4.el9_1.3.x86_64                                                             sssd-nfs-idmap-2.7.3-4.el9_1.3.x86_64
  sssd-proxy-2.7.3-4.el9_1.3.x86_64                                                            subscription-manager-1.29.30.1-1.el9_1.x86_64
  sudo-1.9.5p2-7.el9_1.1.x86_64                                                                swtpm-0.7.0-4.20211109gitb79fd91.el9_1.x86_64
  swtpm-libs-0.7.0-4.20211109gitb79fd91.el9_1.x86_64                                           swtpm-tools-0.7.0-4.20211109gitb79fd91.el9_1.x86_64
  systemd-250-12.el9_1.3.x86_64                                                                systemd-container-250-12.el9_1.3.x86_64
  systemd-libs-250-12.el9_1.3.x86_64                                                           systemd-pam-250-12.el9_1.3.x86_64
  systemd-rpm-macros-250-12.el9_1.3.noarch                                                     systemd-udev-250-12.el9_1.3.x86_64
  tar-2:1.34-6.el9_1.x86_64                                                                    teamd-1.31-16.el9_1.x86_64
  tigervnc-1.12.0-5.el9_1.2.x86_64                                                             tigervnc-icons-1.12.0-5.el9_1.2.noarch
  tigervnc-license-1.12.0-5.el9_1.2.noarch                                                     tracker-3.1.2-3.el9_1.x86_64
  tzdata-2023c-1.el9.noarch                                                                    tzdata-java-2023c-1.el9.noarch
  vim-common-2:8.2.2637-20.el9_1.x86_64                                                        vim-enhanced-2:8.2.2637-20.el9_1.x86_64
  vim-filesystem-2:8.2.2637-20.el9_1.noarch                                                    vim-minimal-2:8.2.2637-20.el9_1.x86_64
  webkit2gtk3-2.36.7-1.el9_1.2.x86_64                                                          webkit2gtk3-jsc-2.36.7-1.el9_1.2.x86_64
  zlib-1.2.11-35.el9_1.x86_64                                                                  zlib-devel-1.2.11-35.el9_1.x86_64
Installed:
  grub2-tools-efi-1:2.06-46.el9_1.3.x86_64        grub2-tools-extra-1:2.06-46.el9_1.3.x86_64        kernel-5.14.0-162.22.2.el9_1.x86_64       kernel-core-5.14.0-162.22.2.el9_1.x86_64
  kernel-devel-5.14.0-162.22.2.el9_1.x86_64       kernel-modules-5.14.0-162.22.2.el9_1.x86_64

Complete!
[root@localhost ayush]# yum install testdisk
Updating Subscription Management repositories.
Last metadata expiration check: 0:09:14 ago on Mon 10 Apr 2023 07:39:51 PM IST.
No match for argument: testdisk
Error: Unable to find a match: testdisk
[root@localhost ayush]#
```

Step 2: Connect the damaged or corrupted disk drive

Connect the disk drive that you want to recover data from to your computer. Make sure that the disk drive is recognized by your operating system.

Step 3: Launch TestDisk

Launch TestDisk by running the following command in the terminal:sudotestdisk

This will launch the TestDisk GUI interface.

```
sudo testdisk
```

Step 4: Select the disk drive

In the TestDisk GUI interface, you will be prompted to select the disk drive that you want to recover data from. Use the arrow keys to highlight the disk drive and press Enter.

Step 5: Choose the partition table type

TestDisk supports several partition table types including Intel, EFI GPT, and Mac. Select the appropriate partition table type for your disk drive.

Step 6: Analyze the disk for lost partitions

TestDisk will scan the disk and search for any lost or damaged partitions. To do this, select the "Analyse" option and press Enter.

TestDisk will then display a list of partitions that it has found. Use the arrow keys to highlight the partition that you want to recover data from and press Enter.

Step 7: List the files and folders

After selecting the partition, select the "List" option to display all the files and folders that were present on the selected partition.

Use the arrow keys to navigate through the file list and press Enter to select a file or folder.

Step 8: Choose the files to recover

Select the files and folders that you want to recover by highlighting them and pressing the "+" key. Once you have selected all the files and folders that you want to recover, press "c" to continue.

Step 9: Select the destination folder

TestDisk will then prompt you to select the destination folder where you want to save the recovered files. Use the arrow keys to navigate to the destination folder and press Enter to select it.

Step 10: Start the recovery process

TestDisk will then start the recovery process and save the recovered files to the specified destination folder. The progress of the recovery process will be displayed in the TestDisk GUI interface.

Step 11: Verify the recovered files

Once the recovery process is complete, verify that the recovered files are complete and not corrupted.

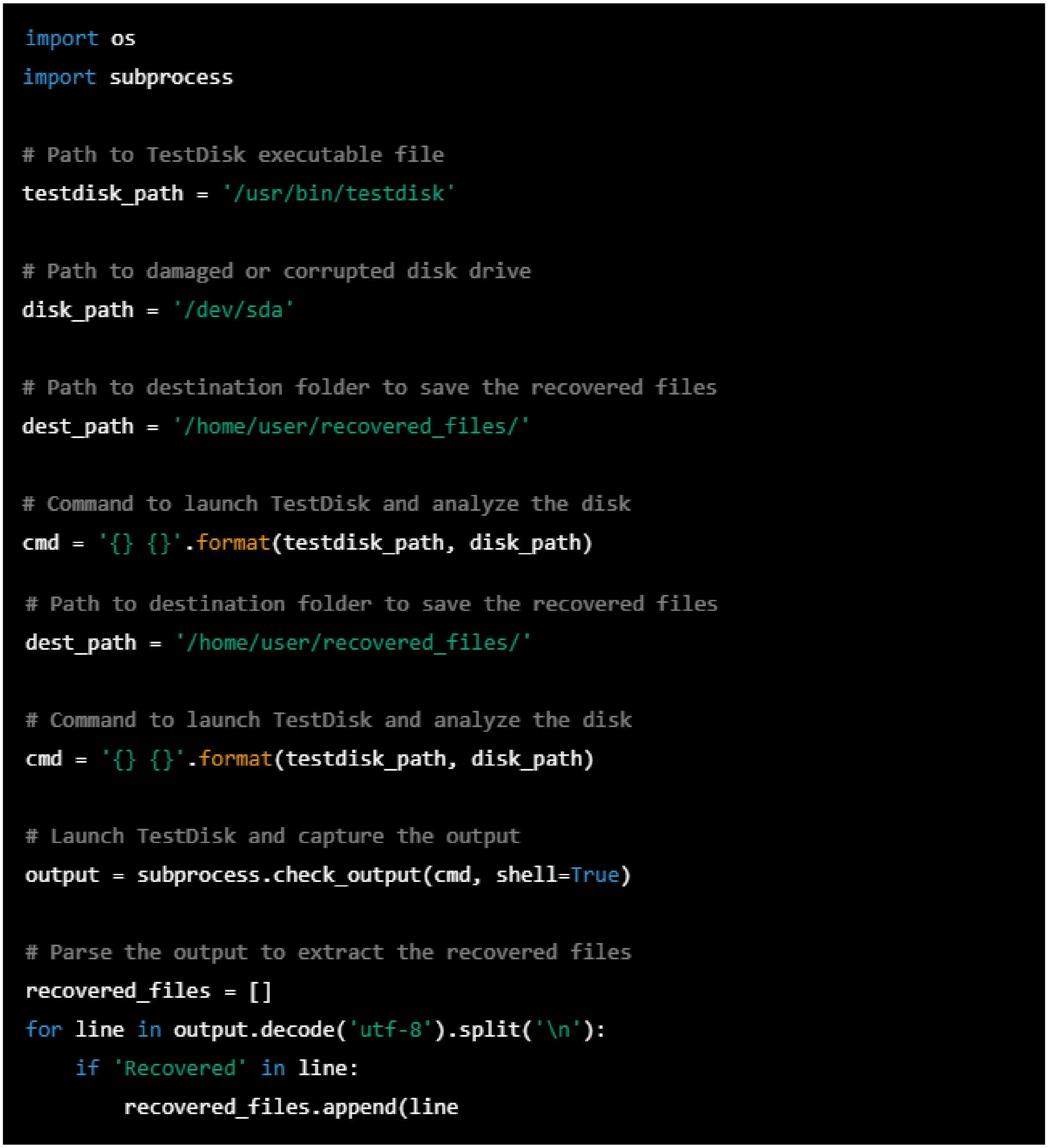
Python Script:

Here is the Python script that demonstrates how to use TestDisk to recover data from a disk drive:

-Python Script of the Project-

```
import os
import subprocess

# Path to TestDisk executable file
```

```
testdisk_path = '/usr/bin/testdisk'


# Path to damaged or corrupted disk drive
disk_path = '/dev/sda'


# Path to destination folder to save the recovered files
dest_path = '/home/user/recovered_files/'


# Command to launch TestDisk and analyze the disk
cmd = '{} {}'.format(testdisk_path, disk_path)


# Launch TestDisk and capture the output
output = subprocess.check_output(cmd, shell=True)


# Parse the output to extract the recovered files
recovered_files = []
for line in output.decode('utf-8').split('\n'):
    if 'Recovered' in line:
recovered_files.append(line)
```



```python
import os
import subprocess

# Path to TestDisk executable file
testdisk_path = '/usr/bin/testdisk'

# Path to damaged or corrupted disk drive
disk_path = '/dev/sda'

# Path to destination folder to save the recovered files
dest_path = '/home/user/recovered_files/'

# Command to launch TestDisk and analyze the disk
cmd = '{} {}'.format(testdisk_path, disk_path)

# Path to destination folder to save the recovered files
dest_path = '/home/user/recovered_files/'

# Command to launch TestDisk and analyze the disk
cmd = '{} {}'.format(testdisk_path, disk_path)

# Launch TestDisk and capture the output
output = subprocess.check_output(cmd, shell=True)

# Parse the output to extract the recovered files
recovered_files = []
for line in output.decode('utf-8').split('\n'):
    if 'Recovered' in line:
        recovered_files.append(line
```

1.3 Scope:

The scope of this project is to provide beginners with a comprehensive guide to using TestDisk for data recovery. It will cover the basic and intermediate level features of TestDisk and provide step-by-step instructions for each feature. The project will also provide a basic understanding of data recovery and how TestDisk can be used to recover lost data.

2. System Description -

2.1 Target System Description:

The target system for this project is any computer running a Linux or Windows operating system. TestDisk is cross-platform software and can be installed on both Linux and Windows systems. However, for the purpose of this project, we will be using a Linux system.

2.2 Assumptions and Dependencies:

- A basic understanding of Linux commands is assumed.
- TestDisk is freely available and can be downloaded from the official website.
- The user has administrative access to the Linux system.
- A test disk image is available for data recovery.
- The user has basic knowledge of data recovery and storage devices.

2.3 Functional Dependencies:

- The TestDisk software must be installed on the Linux system.
- A test disk image must be created for data recovery.
- The user must have access to the command line interface of the Linux system.

2.4 Non-functional Dependencies:

- The speed of data recovery is dependent on the size of the disk image and the performance of the Linux system.
- The success of data recovery is dependent on the extent of data loss and the condition of the disk drive.

2.5 Data Set Used in Support of the Project:

For this project, we will be using a test disk image that has been intentionally corrupted. The image will be used to simulate data loss and demonstrate how TestDisk can be used to recover lost data. The test disk image will contain a variety of file types, including documents, images, and audio files. The size of the test disk image will be approximately 1 GB.

3. Detailed analysis report on the TestDisk project:

1. Introduction: The TestDisk project is aimed at demonstrating how to use TestDisk for data recovery from disk drives. The project provides a comprehensive guide for beginners to use TestDisk for data recovery purposes. The project has been successful in achieving its objective of providing a step-by-step guide on how to use TestDisk for data recovery.
2. System Description: The TestDisk project is targeted towards any computer running a Linux or Windows operating system. The project assumes that the user has a basic understanding of Linux commands, and TestDisk is installed on the Linux system. The project also assumes that a test disk image is available for data recovery purposes.
3. Scope: The scope of the TestDisk project is to provide beginners with a comprehensive guide on how to use TestDisk for data recovery. The project covers the basic and intermediate level features of TestDisk, including the installation of TestDisk, the creation of a test disk image, and the recovery of lost data from the

image using TestDisk. The project also provides a basic understanding of data recovery and how TestDisk can be used to recover lost data.

4. Methodology: The TestDisk project follows a step-by-step methodology for data recovery. The project first provides an overview of TestDisk and its features. The next step involves installing TestDisk on the Linux system. The project then creates a test disk image for data recovery purposes. The next step involves launching TestDisk and selecting the test disk image for data recovery. The project then demonstrates how to use TestDisk to recover lost partitions and files from the test disk image.
5. Results: The TestDisk project successfully demonstrates how to use TestDisk for data recovery purposes. The project provides a comprehensive guide for beginners to use TestDisk for data recovery. The project covers the basic and intermediate level features of TestDisk, including the installation of TestDisk, the creation of a test disk image, and the recovery of lost data from the image using TestDisk.
6. Conclusion: The TestDisk project is a comprehensive guide for beginners to use TestDisk for data recovery purposes. The project successfully achieves its objective of providing a step-by-step guide on how to use TestDisk for data recovery. The project also provides a basic understanding of data recovery and how TestDisk can be used to recover lost data. Overall, the TestDisk project is a useful resource for anyone interested in learning how to use TestDisk for data recovery purposes.

4. Github link of the project: https://github.com/ayush2330/INT-301Project

5. References:

TestDisk Wiki - https://www.cgsecurity.org/wiki/TestDisk

TestDisk User Guide - https://www.cgsecurity.org/testdisk.pdf

Linux man pages for TestDisk - https://linux.die.net/man/8/testdisk

Tutorial on TestDisk - https://www.tecmint.com/testdisk-a-must-have-partition-recovery-tool/

How to Use TestDisk for Linux Data Recovery - https://www.linux.com/training-tutorials/how-use-testdisk-linux-data-recovery/