EXPERIMENT NO: 04

Explore forensics tools in kali linux for acquiring, analyzing and duplicating data.

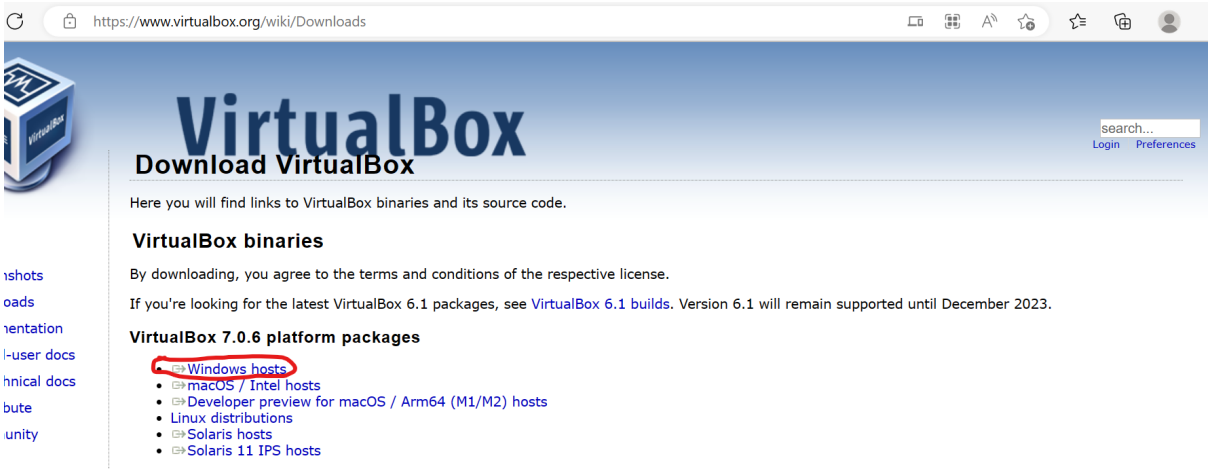
- **dd**
- **dcfldd**

AIM : To Explore forensics tools in kali linux for acquiring, analyzing and duplicating data.

THEORY :

Installation guide for VirtualBox and Kali Linux:

1. Download Virtual Box
https://www.virtualbox.org/wiki/Downloads

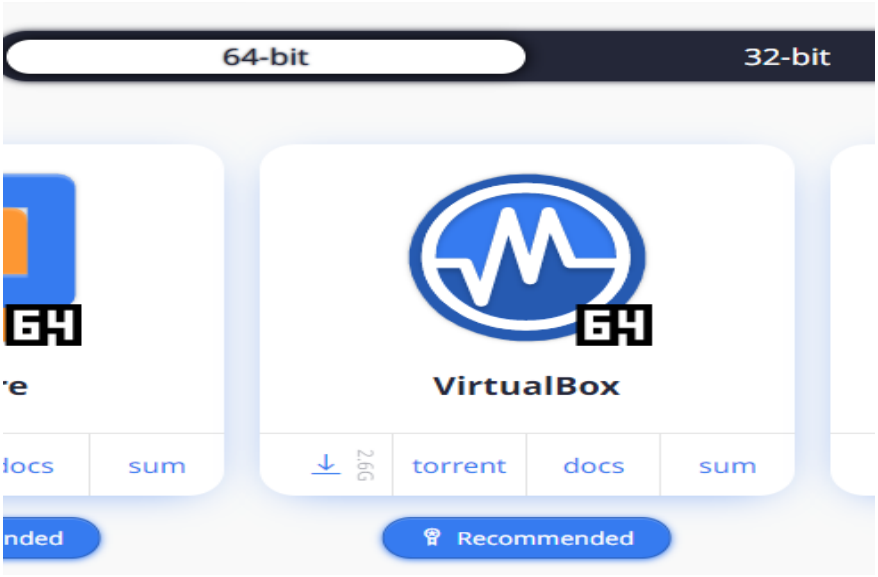


Download the highlighted version

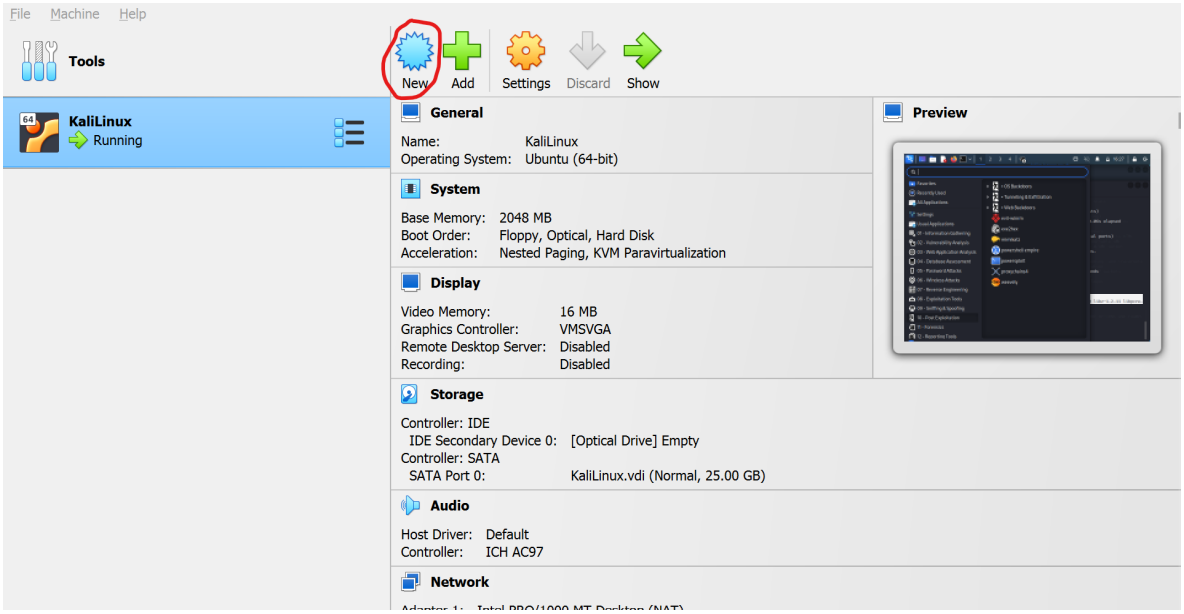
2. Follow the installation steps

3. Download Kali

https://www.kali.org/get-kali/#kali-virtual-machines



4. Go to Virtual box



5. Click on New, enter the name of the machine without spaces, select the ISO image that you downloaded and then click on next and follow the steps.

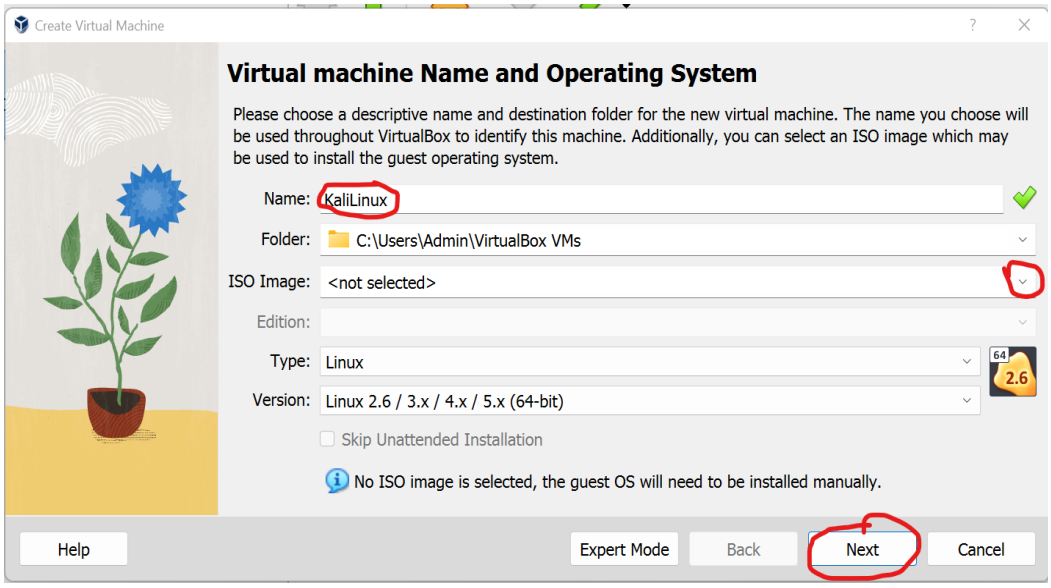


Image acquisition using DD:

DD file is the image file created out of dd commands. It is a powerful and simple command-line that is used to create disk images, copy files, etc. of hard drives on Unix or Linux Operating System.

The utility is inbuilt and installed in Linux or Unix OS to create raw images of drives, folders, files, etc. for forensic purposes. Users can create the output file either in .img or .dd file or other file formats by specifying the file type at the **"of"** part.

dd command- data duplication:

sudo apt get update

Create a file inside a folder and try to copy

dd if=/home/vaishali/test2 of=/home/kali/test1.img

Few more commands

Following the dd command example, the UNIX device name of the source hard disk is /dev/hda, and device name of the target hard disk is /dev/hdb.

 # dd if=/dev/sda of=/dev/sdb

If there are any errors, the above command will fail. If you give the parameter *"conv=noerror"* then it will continue to copy if there are read errors.

Input file and output file should be mentioned very carefully. Just in case, you mention source

device in the target and vice versa, you might loss all your data.

To copy, hard drive to hard drive using dd command given below, sync option allows you to copy everything using synchronized I/O.

 # dd if=/dev/sda of=/dev/sdb conv=noerror, sync

To back up a Partition:

You can use the device name of a partition in the input file, and in the output either you can specify your target path or image file as shown in the dd command.

 # dd if=/dev/hda1 of=~/partition.img

To create an image of a Hard Disk:

Instead of taking a backup of the hard disk, you can create an image file of the hard disk and save it in other storage devices. There are many advantages of backing up your data to a disk image, one being the ease of use. This method is typically faster than other types of backups, enabling you to quickly restore data following an unexpected catastrophe.It creates the image of a hard disk /dev/hda.

 # dd if=/dev/hda of=~/hdadisk.img

dcfldd

Sudo apt-get update

Sudo apt install dcfldd

dcfldd if=/home/vaishali/test2 of=/home/kali/test2.img

dc3dd

Sudo apt-get update

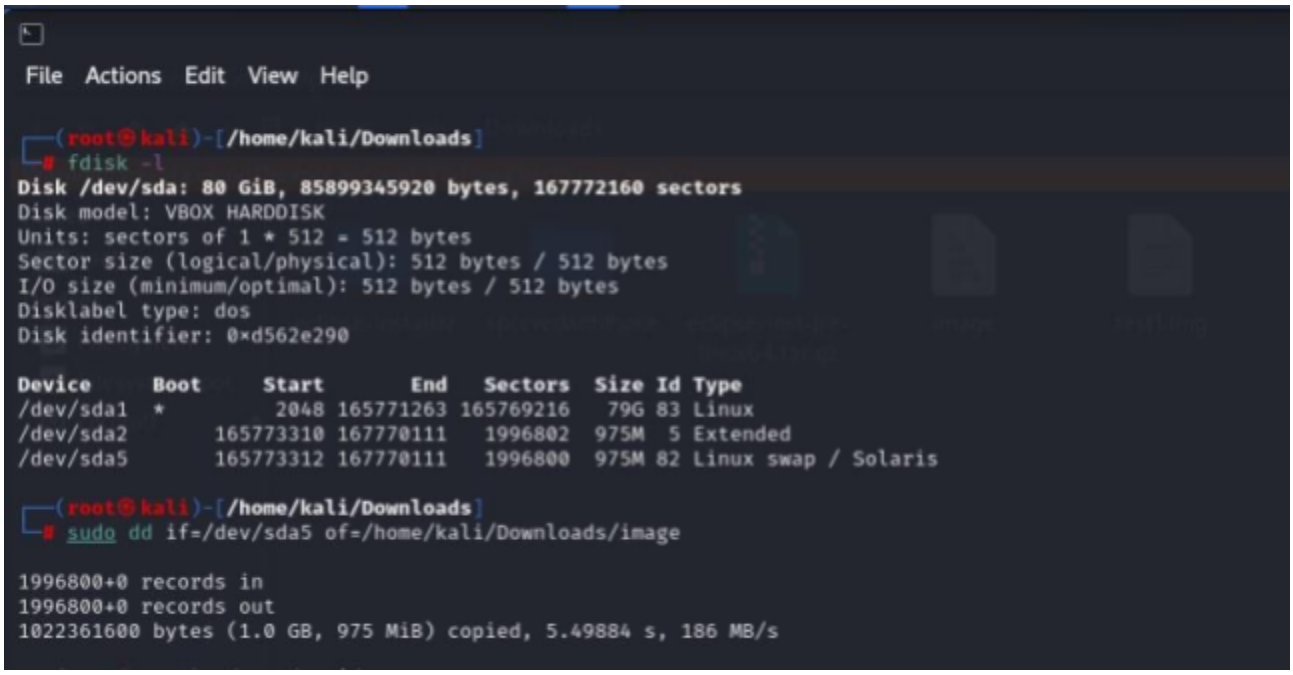
Sudo apt install dc3dd

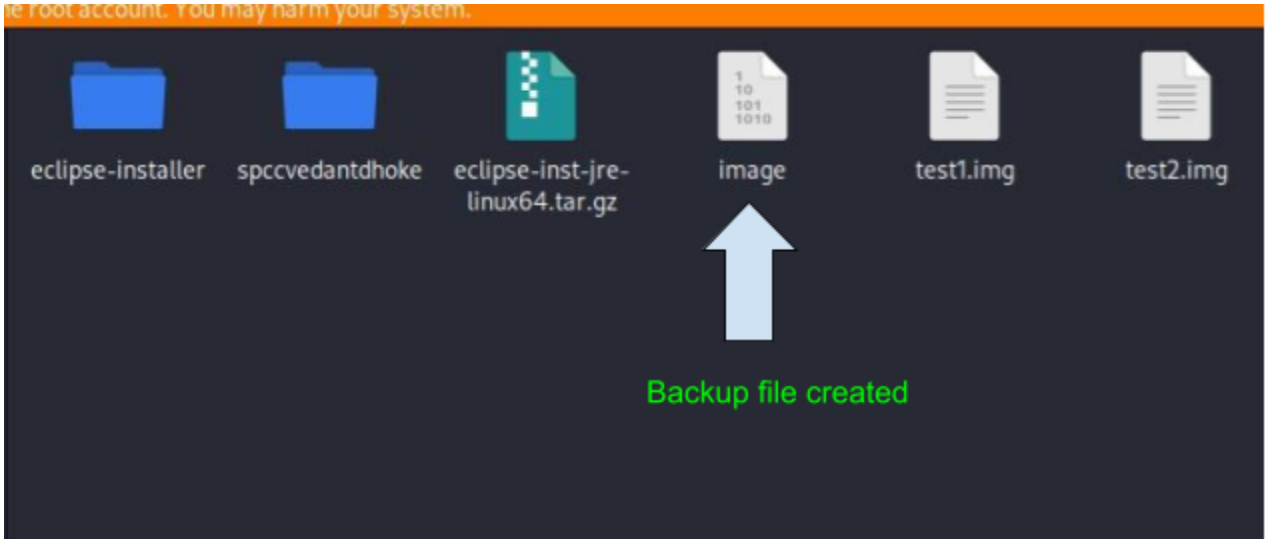
dc3dd if=/home/vaishali/test2 of=/home/kali/test3.img

Output:

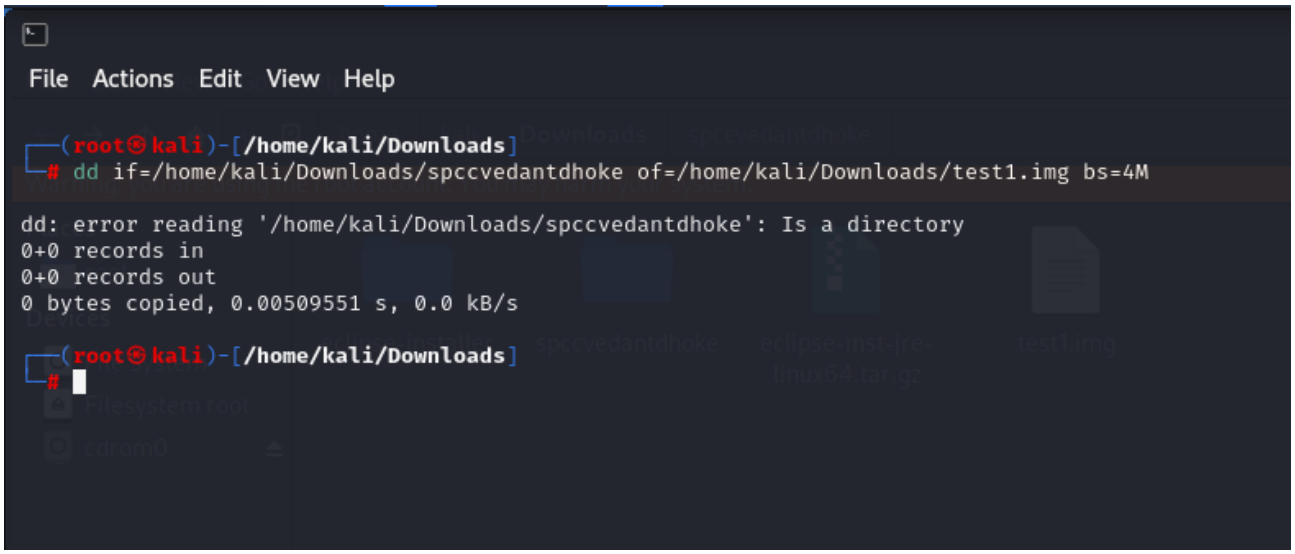
dd command

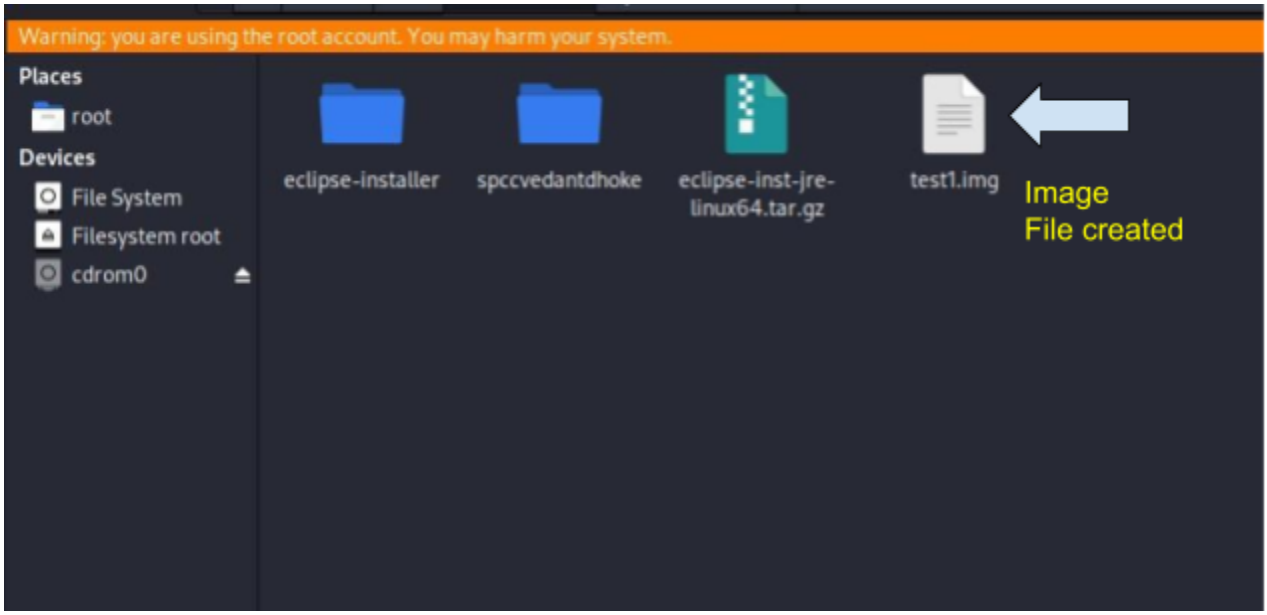
1. **Backup a Partition**



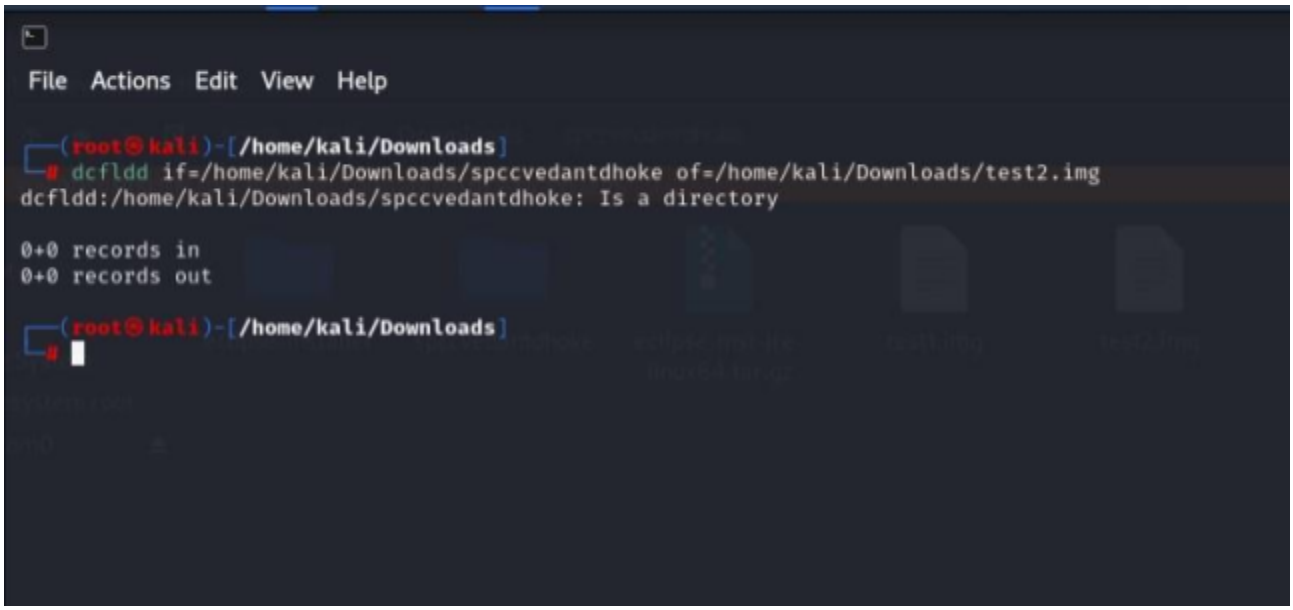


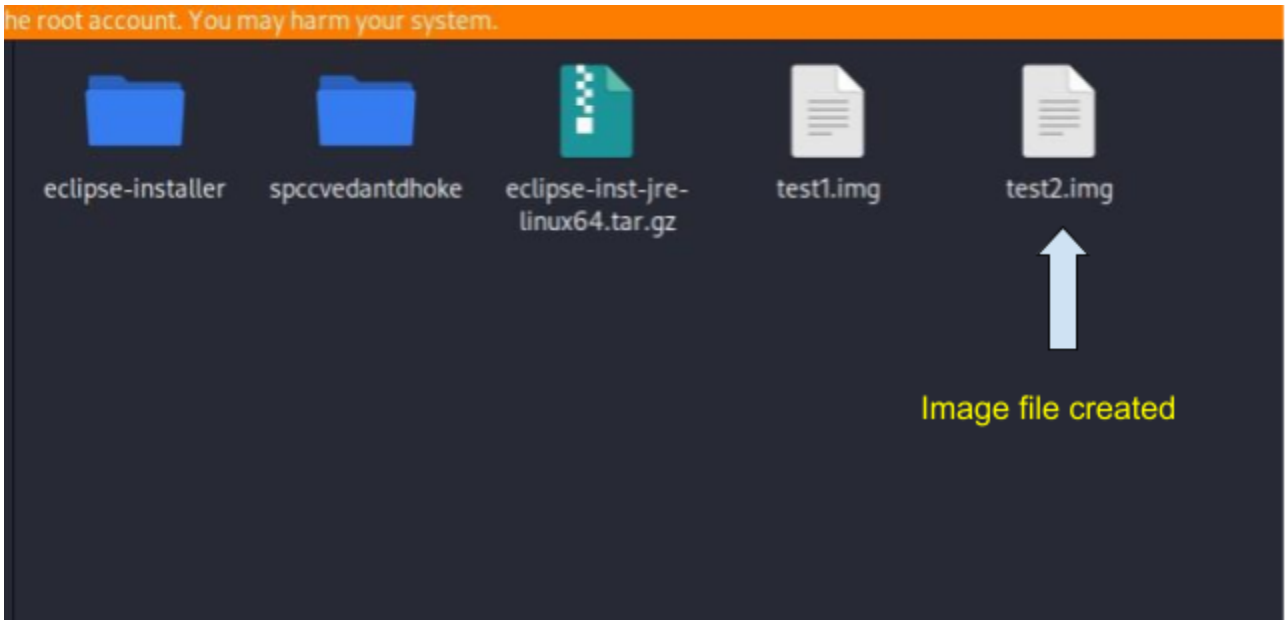
2. Creating an image(Data Duplication)





dcfldd command





Conclusion: In conclusion, dd and dcfldd are both powerful command-line tools used for copying and converting data. Both tools are widely used in Linux and other Unix-like operating systems for various purposes, such as creating backups, cloning drives, and creating disk images.These tools are powerful and can cause serious damage if used incorrectly.