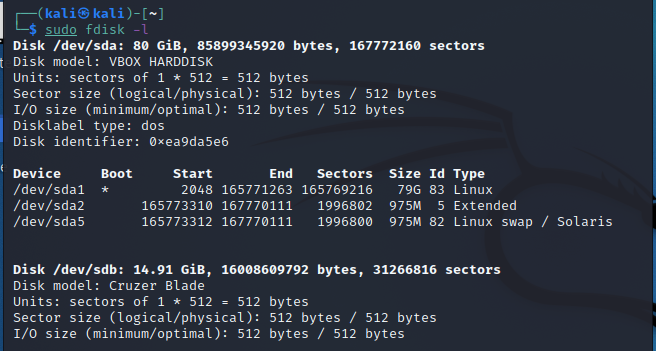
**Task-1**

**Drives and Partition in Linux**

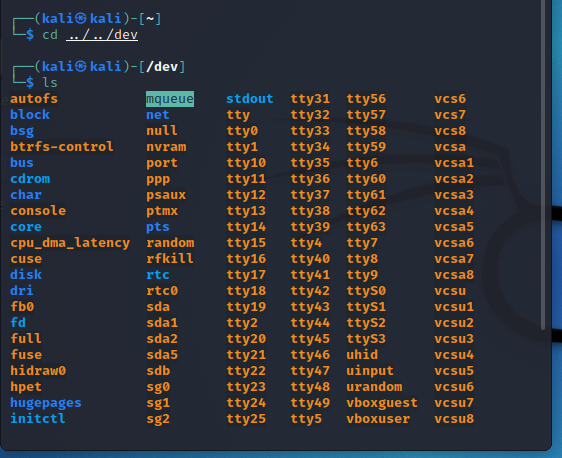
First, we are going to analyze and gather information about our disk

Using command “**sudo fdisk -l**”

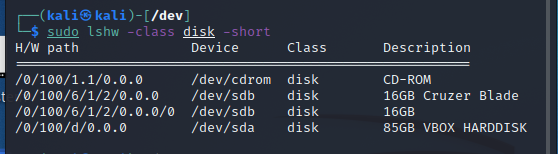


Getting information about the list devices and drives recognized by our machine

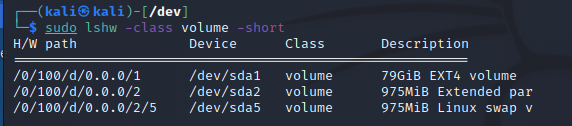
Analyzing **/dev** directory



Hardware Disk information



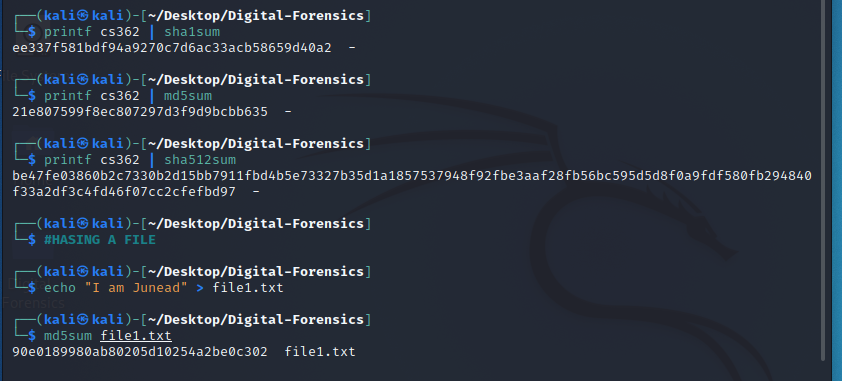
Hardware Volume information



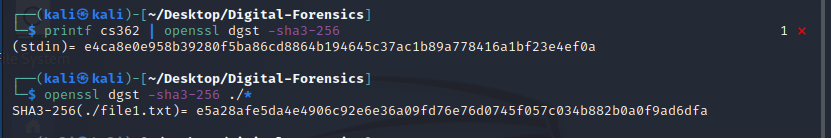
**Task-2**

**Linux Hashing Commands**

Learning about hashing commands



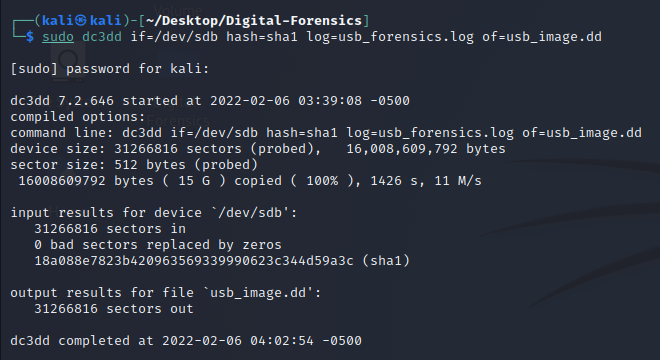
Using openssl to use hashing command sha3



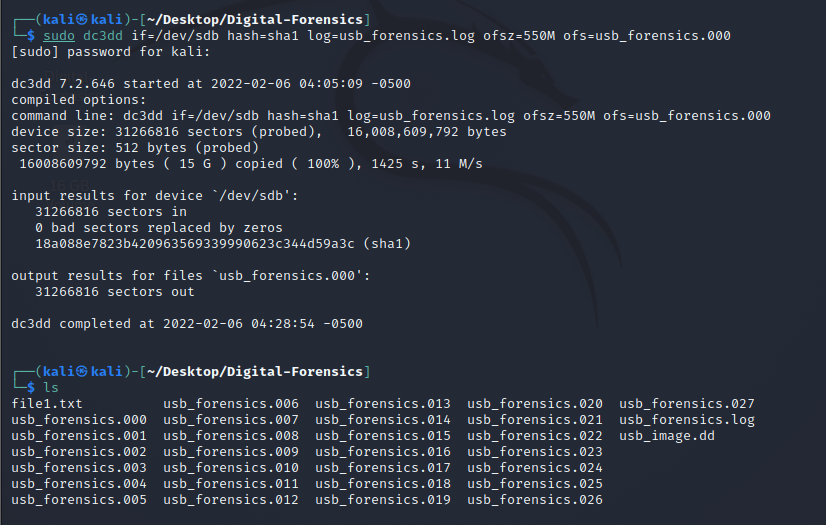
**Task-3**

**Acquisition using dc3dd and dd Commands**

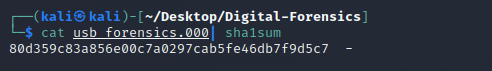
Creating raw-image of USB



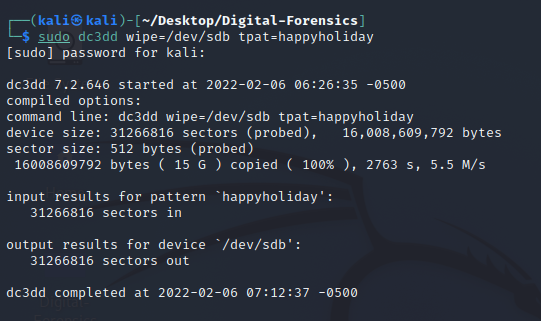
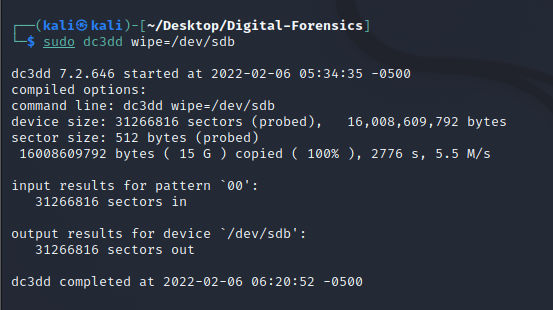
Splitting the files of the created image



Computing hash function

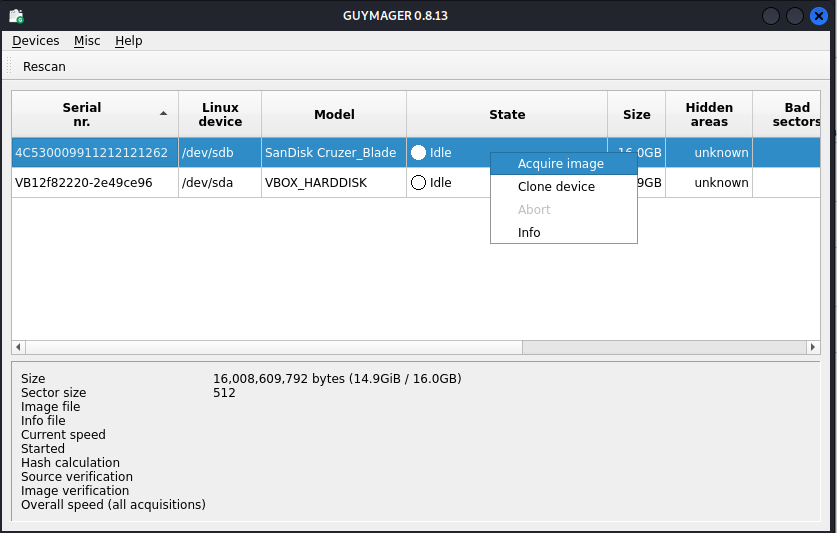


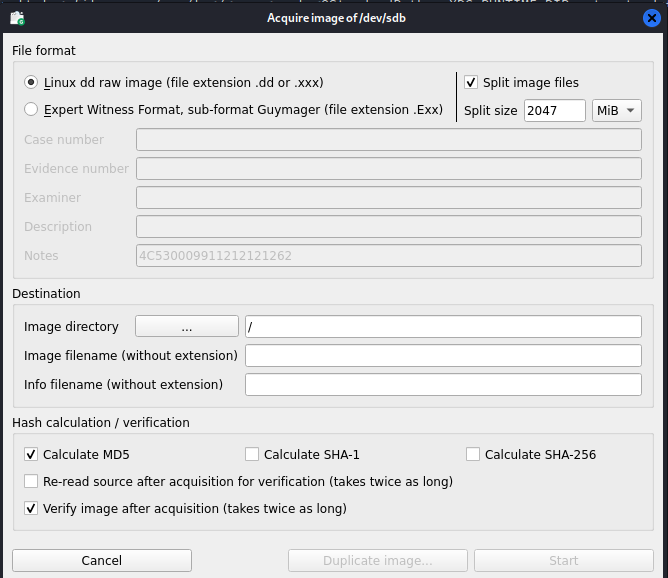
Avoid recovery of deleted files



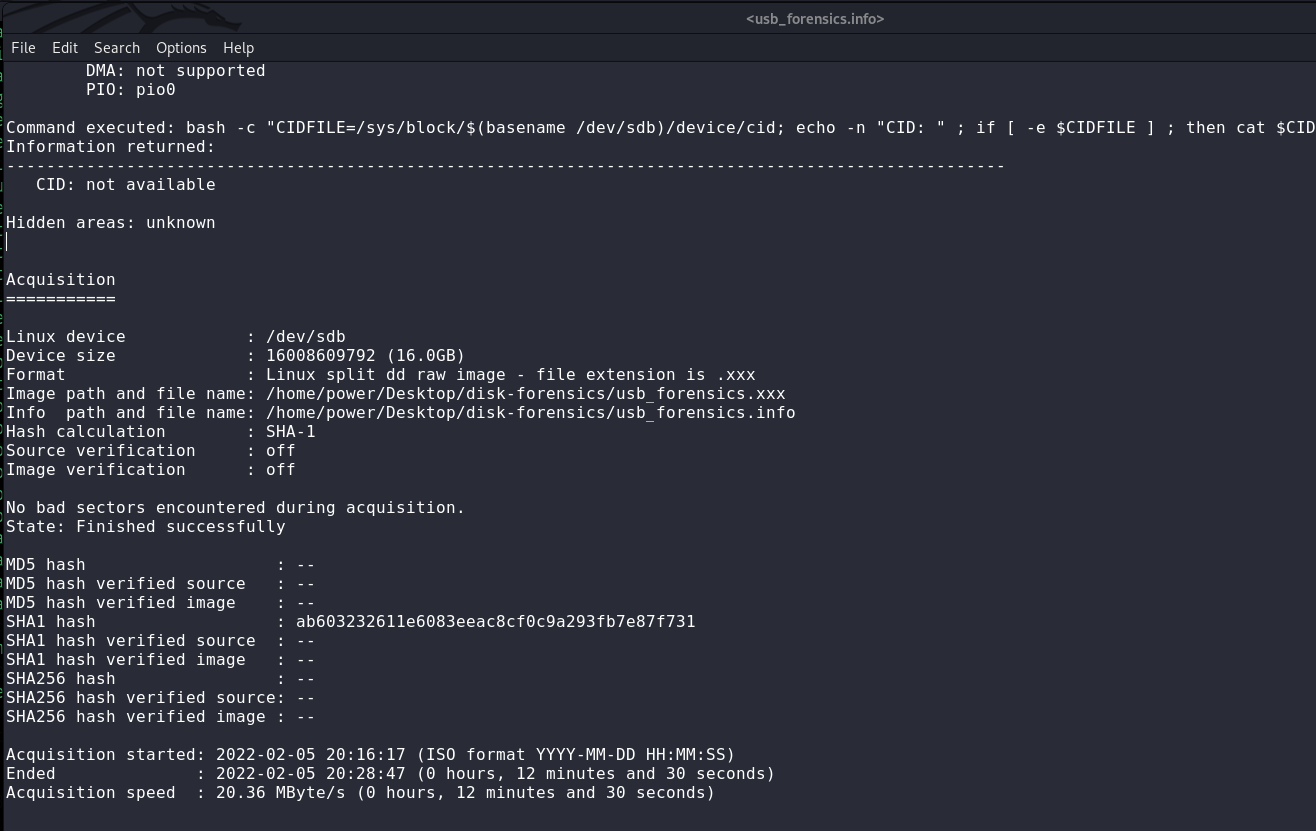
**Task-4**

**Image Acquisition using Guymager**



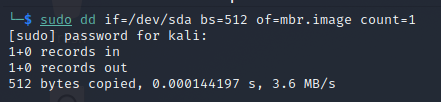


This is a graphical method of acquiring an image

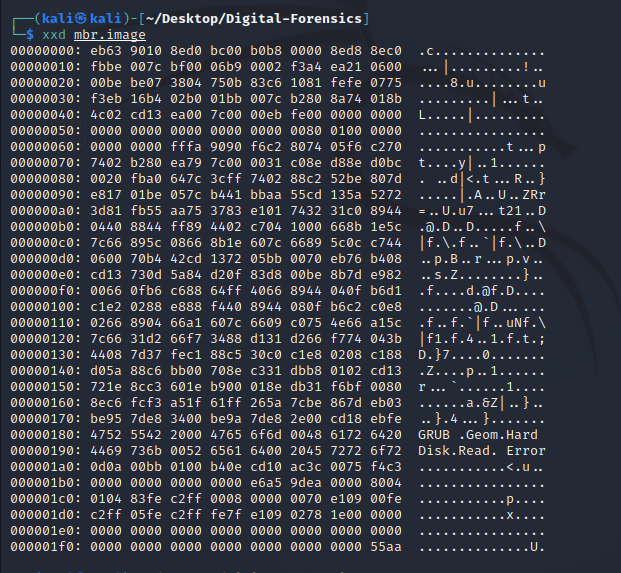


**Task-5**

**Retrieve the Master Boot Record (MBR) using the dd Command**



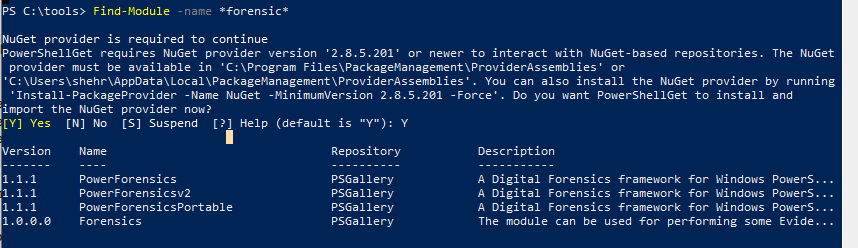
Reading mbr.image file in hex format

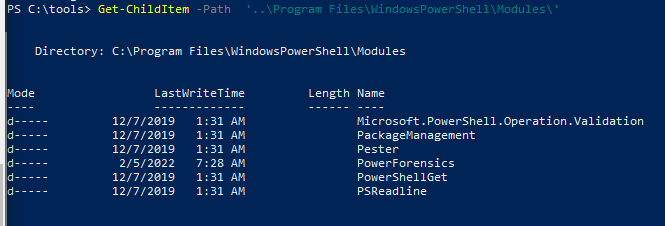


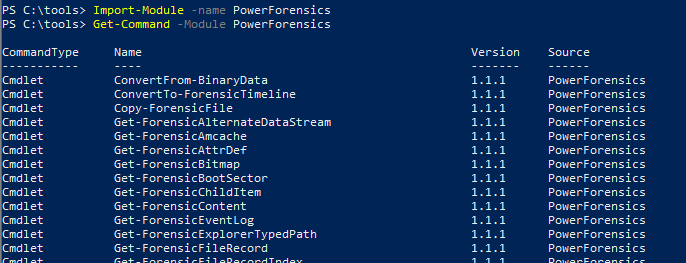
**Task-6**

**Windows Disk Investigation with PowerShell Cmdlets**

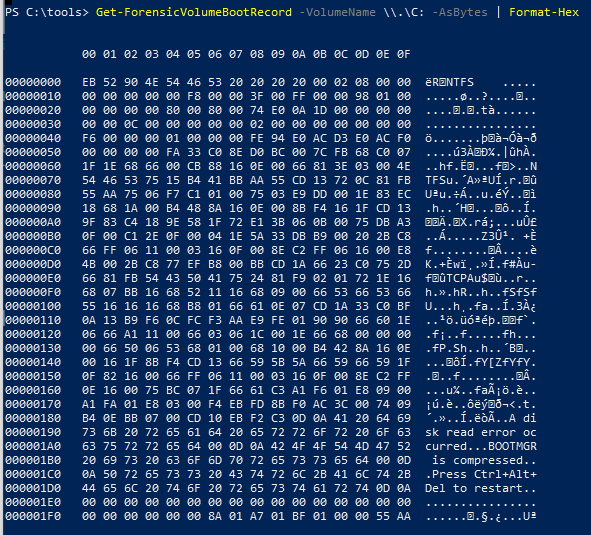
Now we are using windows PowerShell to install forensics tool and look at the details of the image

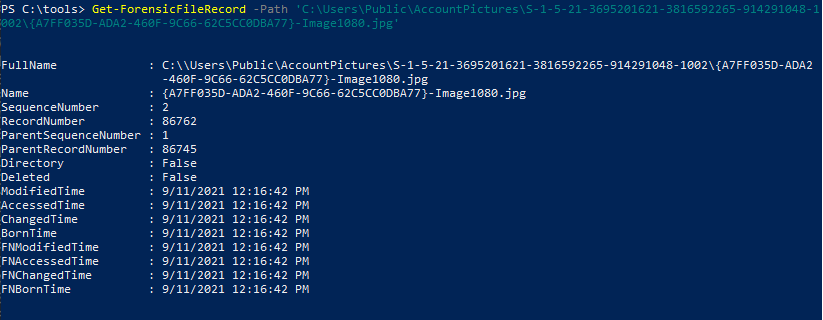






Checking master boot record of the volume C disk





**Summary**

This whole lab was about Disk Forensics. We have learned how to view information about the storage devices that are fitted in our system. We also did practical on how to use hashing commands and get hash of any text or file. Then we learned to create a raw image of a disk and also to avoid recovery of deleted files. We learned to use guymager software that is gui based software. We have also read the MBR (Master Record Boot) of our disk. At last, we have used Windows PowerShell to do Windows Disk Investigation.

**🡨END🡪**