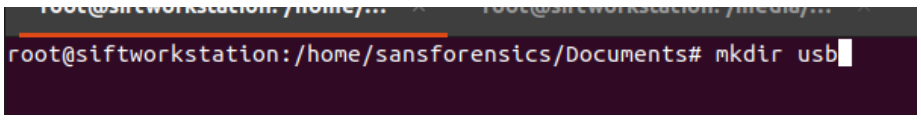
NGEE ANN POLYTECHNIC

School of InfoComm Technology ict Taking IT Higher

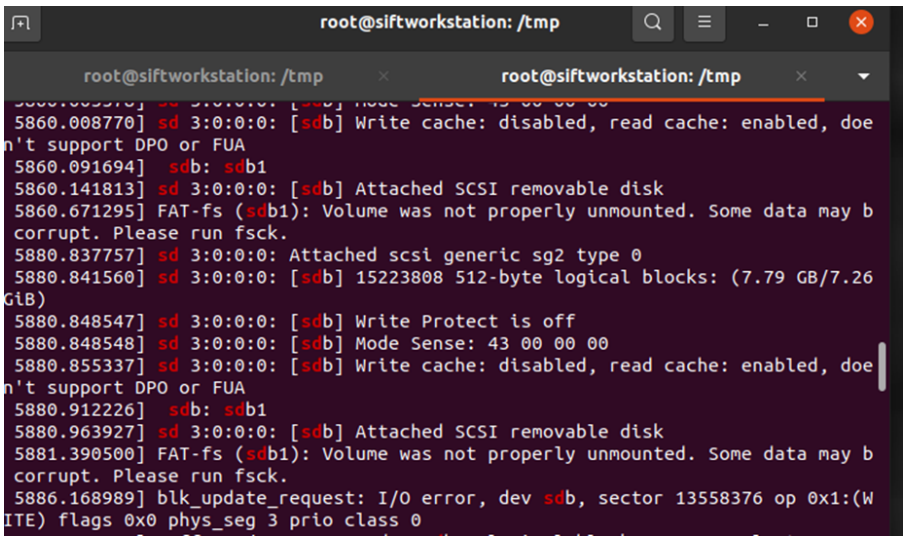
dcfldd - Latest version 1.3.4-1

1.



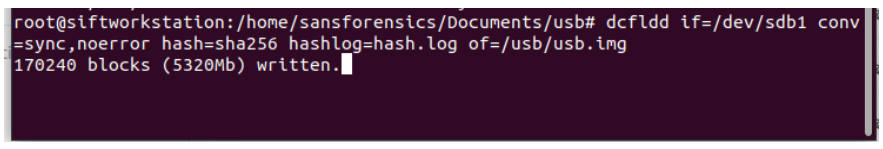
First create a folder to stroage the image files.

2.



Using the command “dmesg | grep” sd this command will focus on an SD drive
the picture above shows that sdb1 is an FAT-fs it the drive name

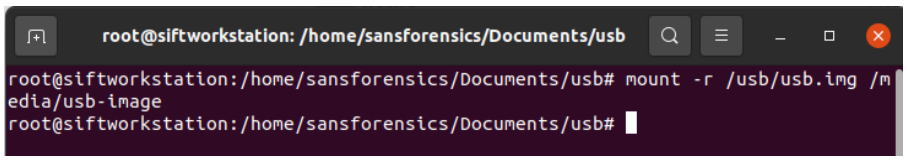
3.



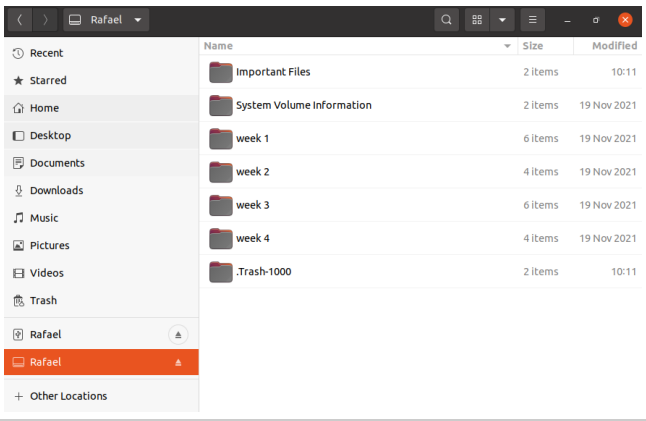
Now I'm aware of the drive's name. I can generate an image of the drive without modifying the actual drive. Imaging is the process of duplicating bits by bits of the original drive; depending on the size of the hdd, this procedure may take a long time.

dcfldd if=/dev/sdb1 conv=sync,noerror hash=sha256 hashlog=hash.log of=/usb/usb.img of=/usb/usb.img of=/usb/usb.img of=/usb/usb.img of=/usb/usb.img of=/usb/usb.img of=/usb

4.

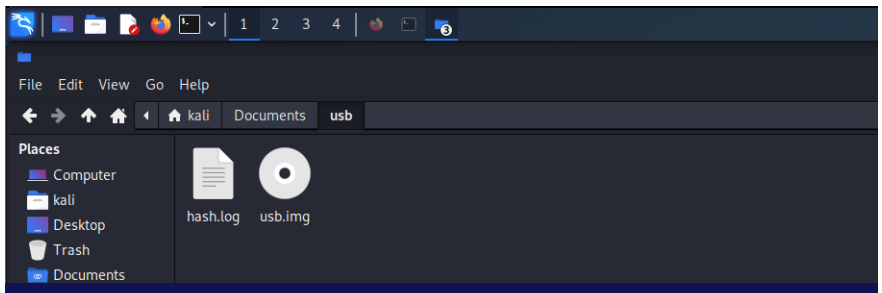


Once I finish creating the image i can mount the .img file in the media folder.
The image below shows the mounted .img



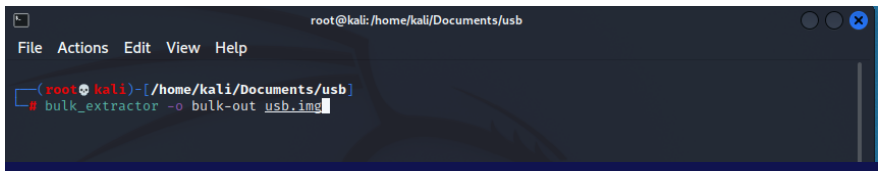
Bulk-Extractor

1.



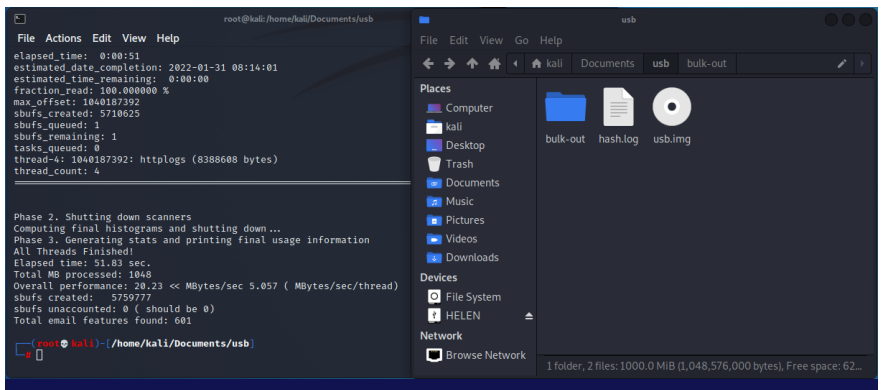
Copy and paste the image file created using dcfldd to somewhere accesible and easy to remember

2.



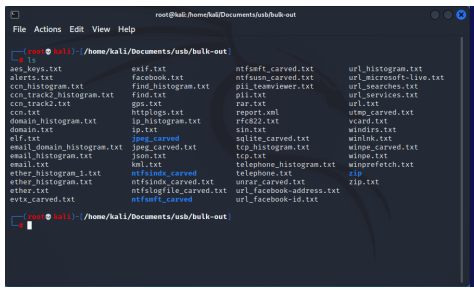
Open terminal and cd to the directory where the .img is stored in, and run the command
“bulk_extractor -o bulk-out usb.img”

3.



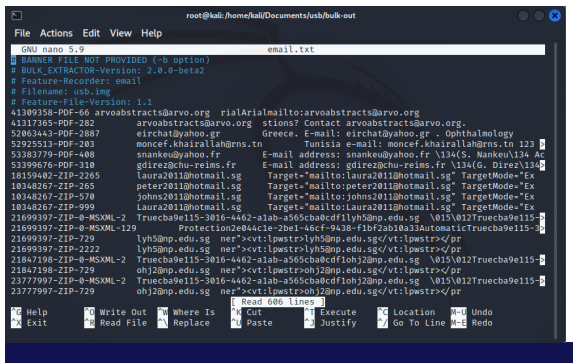
once the the command finish running, there will be a output folder in the folder where the .img is stored

4.



The image on the left shows the output and it categorized the data accordingly

5.



For example, running the command "nano email.txt" will display all of the email addresses saved in the.img file, eliminating the need for the user to go through the file one by one. Same goes for different information such as credit card number.

Contact Information
Rafael Kamil
S10192797@connect.np.edu.sg
Muhammad Azzi Izzuan Bin Azahar
S10189579@connect.np.edu.sg