Sanjana Asrani **Lab 02**
D17B/01/Batch B **Forensic Tools**

AIM:

Explore forensics tools in Kali Linux for acquiring, analyzing and duplicating data: dd, dcfldd

THEORY:

The objective of this digital forensics experiment is to explore and understand the usage of forensics tools in Kali Linux, specifically focusing on data acquisition, analysis, and duplication using the dd (disk dump) and dcfldd (enhanced version of dd) tools. The experiment will cover the process of acquiring data from a source drive, analyzing the acquired data, and duplicating it to another storage device.

Introduction to dd and dcfldd:

dd is a command-line tool used for copying and converting files and is commonly used in digital forensics
for disk imaging.
dcfldd is an enhanced version of dd with additional features such as on-the-fly hashing and status output.

Steps :
1. Creating an Empty USB Storage Device:
Start by connecting a USB storage device to the Kali Linux system.
Identify the device using the fdisk-l command.
Create a new partition on the USB device using fdisk.
Format the partition with a file system, for example, here using sanj_df02_data.vmdk (vdi or vhd can be used too)

2. Data Acquisition using dd:
Identify the source drive (e.g., a suspect drive) using fdisk-l.
Use the dd command to create a forensic image of the source drive:
dd if=/dev/sdX of=/path/to/output/image.dd bs=4M
if: Input file (source drive).
of: Output file (forensic image).
bs: Block size for copying.
status: Display progress during the operation.

3. Data Acquisition using dcfldd :
Alternatively, use dcfldd for acquisition with additional features like hashing:

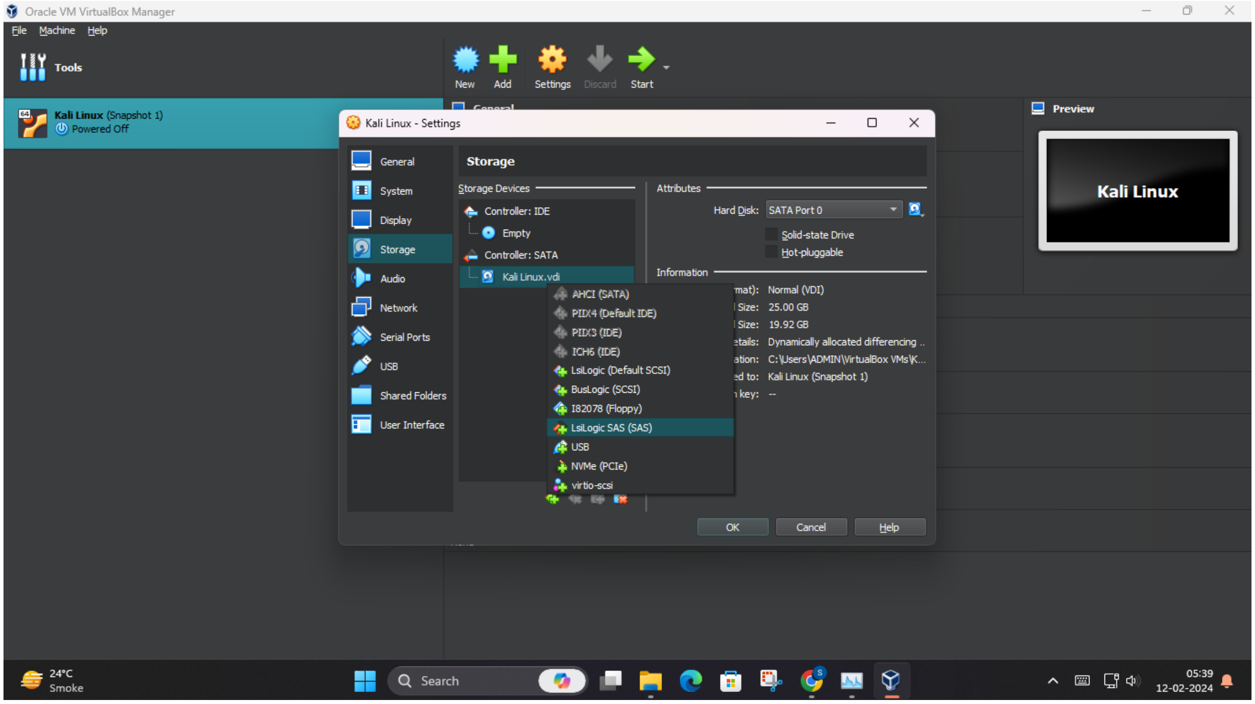
```
dcfldd if=/dev/sdX of=/path/to/output/image.dd hash=md5,sha256 bs=4M
```

4. Verification of Data Integrity:
Verify the integrity of the duplicated data by comparing hash values generated during the acquisition and duplication stages.

5. Documentation and Reporting:
Document all steps, commands used, and any findings during the experiment.
Generate a detailed report summarizing the entire process and any forensic artifacts discovered

STEPS:

Download the .vmdk file if using vbox (or a vdi)



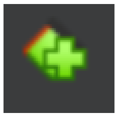
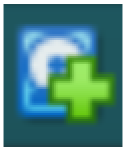
Kali Linux (Snapshot 1)
Powered Off

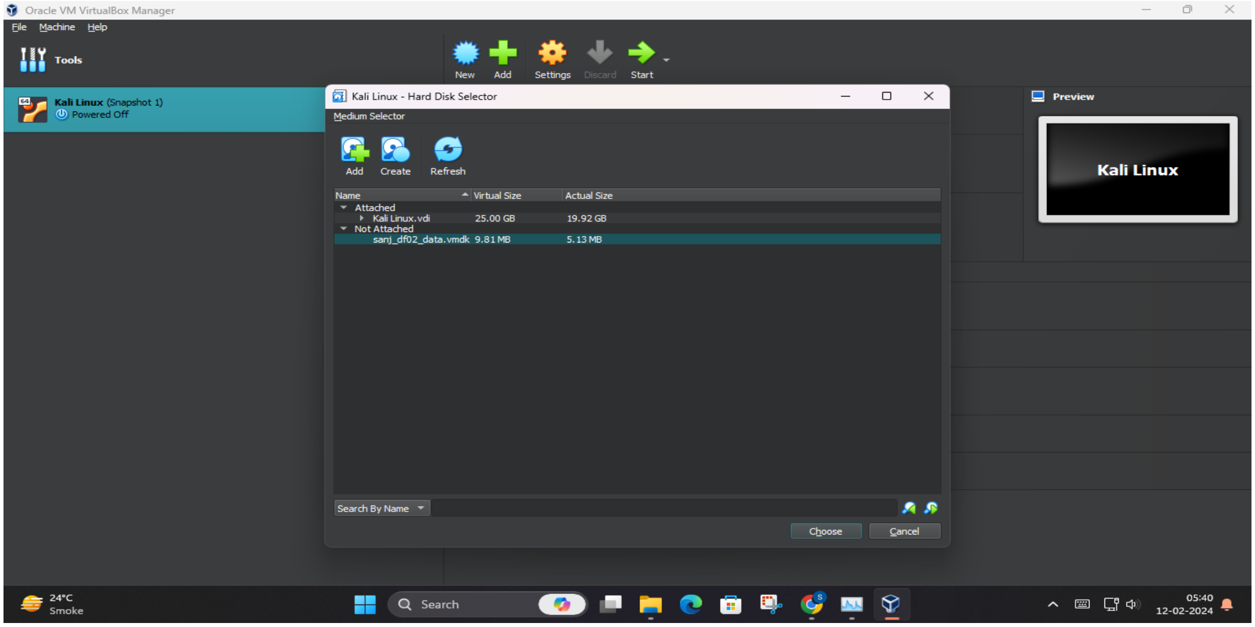
Storage

Storage Devices
Controller: IDE
Empty
Controller: SATA
Kali Linux.vdi

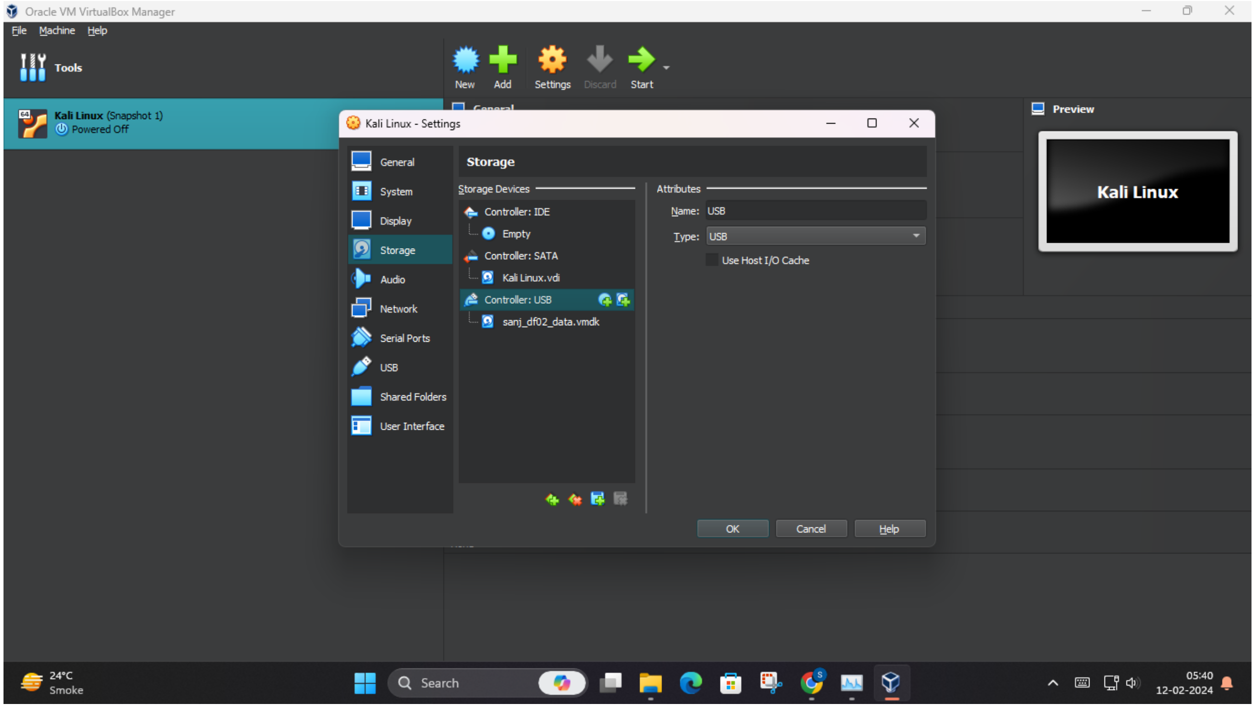
Attributes
Hard Disk: SATA Port 0
□ Solid-state Drive
□ Hot-pluggable

Information
mat): Normal (VDI)
Size: 25.00 GB
Size: 19.92 GB
etails: Dynamically allocated differencing ..
ation: C:\Users\ADMIN\VirtualBox VMs\K...
ed to: Kali Linux (Snapshot 1)
key: --

When the machine is off, go to storage settings  click on USB, Click on the add hard drive btn, select hard disk. and add storage: 
Add a storage (You can also create one), Choose it.



Name	Virtual Size	Actual Size
Attached		
Kali Linux.vdi	25.00 GB	19.92 GB
Not Attached		
sanj_df02_data.vmdk	9.81 MB	5.13 MB



Storage

Storage Devices
- Controller: IDE
  - Empty
- Controller: SATA
  - Kali Linux.vdi
- Controller: USB
  - sanj_df02_data.vmdk

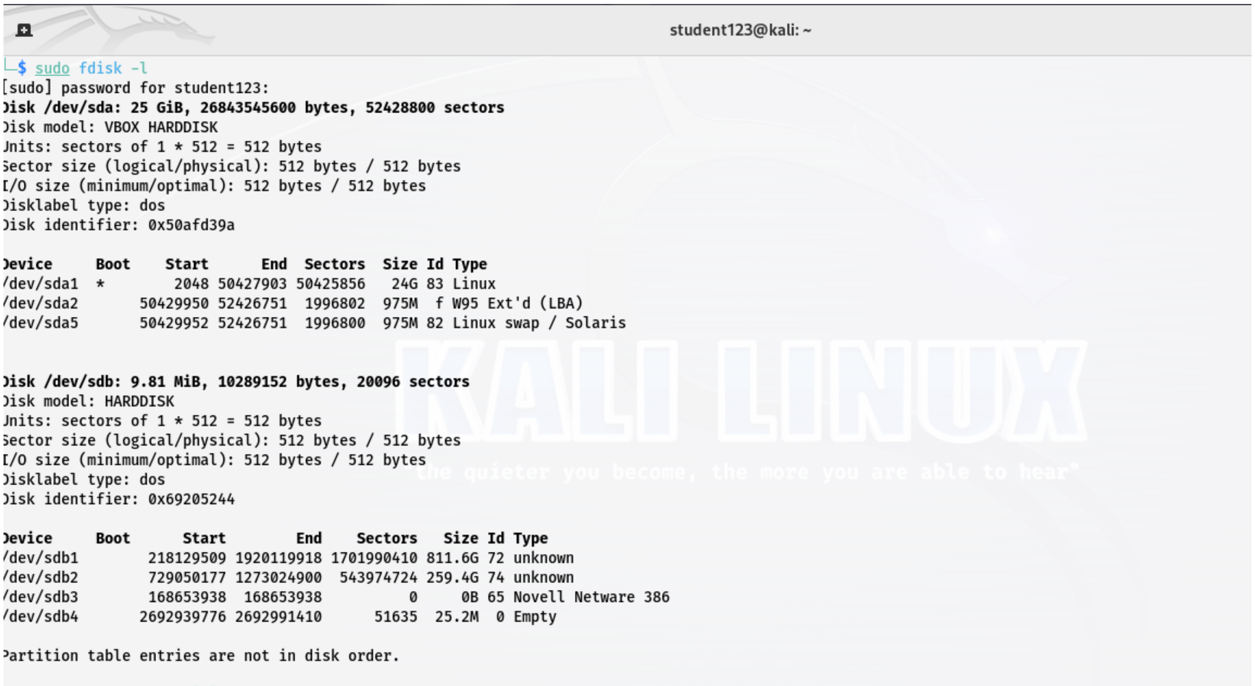
Attributes
Name: USB
Type: USB
□ Use Host I/O Cache

(if these options are disabled, probably your machine state has been saved. Discard it and retry)
Start the machine and open terminal:

Cmds:
(if not using root user, put sudo in front of the cmds, student123 pswd: student)

1. fdisk -l

Tells you what hard drives are attached to your computer

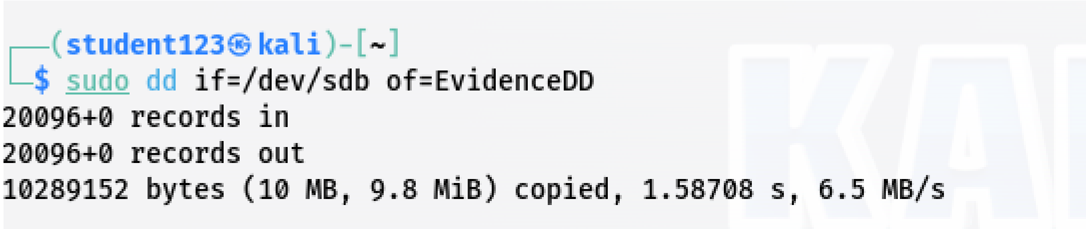


student123@kali: ~

```
└─$ sudo fdisk -l
[sudo] password for student123:
)isk /dev/sda: 25 GiB, 26843545600 bytes, 52428800 sectors
)isk model: VBOX HARDDISK
Jnits: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
)isklabel type: dos
)isk identifier: 0x50afd39a

)evice     Boot    Start      End  Sectors  Size Id Type
/dev/sda1  *        2048 50427903 50425856   24G 83 Linux
/dev/sda2       50429950 52426751  1996802  975M  f W95 Ext'd (LBA)
/dev/sda5       50429952 52426751  1996800  975M 82 Linux swap / Solaris


)isk /dev/sdb: 9.81 MiB, 10289152 bytes, 20096 sectors
)isk model: HARDDISK
Jnits: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
)isklabel type: dos
)isk identifier: 0x69205244

)evice     Boot      Start        End    Sectors   Size Id Type
/dev/sdb1        218129509 1920119918 1701990410 811.6G 72 unknown
/dev/sdb2        729050177 1273024900  543974724 259.4G 74 unknown
/dev/sdb3        168653938  168653938          0     0B 65 Novell Netware 386
/dev/sdb4       2692939776 2692991410      51635  25.2M  0 Empty

Partition table entries are not in disk order.
```

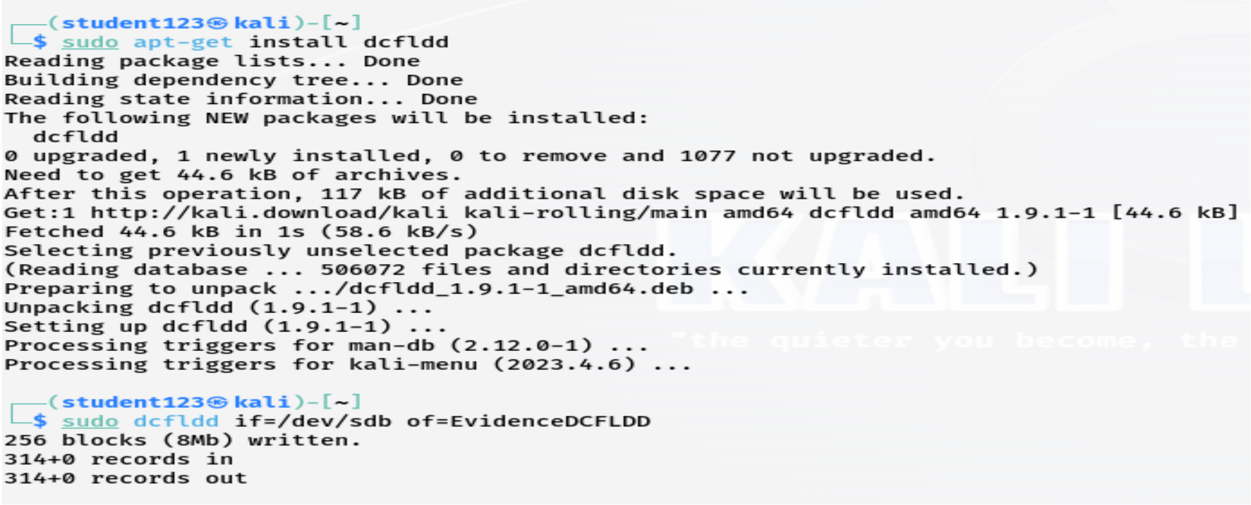
2. dd if=/dev/sdb of=EvidenceDD

Create a copy of the file using the dd command

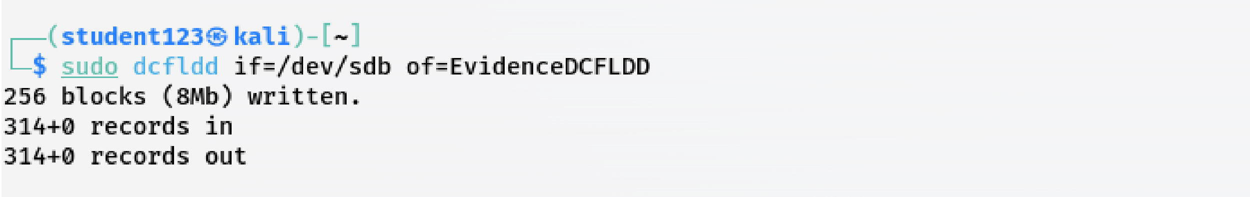


```
┌──(student123㉿kali)-[~]
└─$ sudo dd if=/dev/sdb of=EvidenceDD
20096+0 records in
20096+0 records out
10289152 bytes (10 MB, 9.8 MiB) copied, 1.58708 s, 6.5 MB/s
```

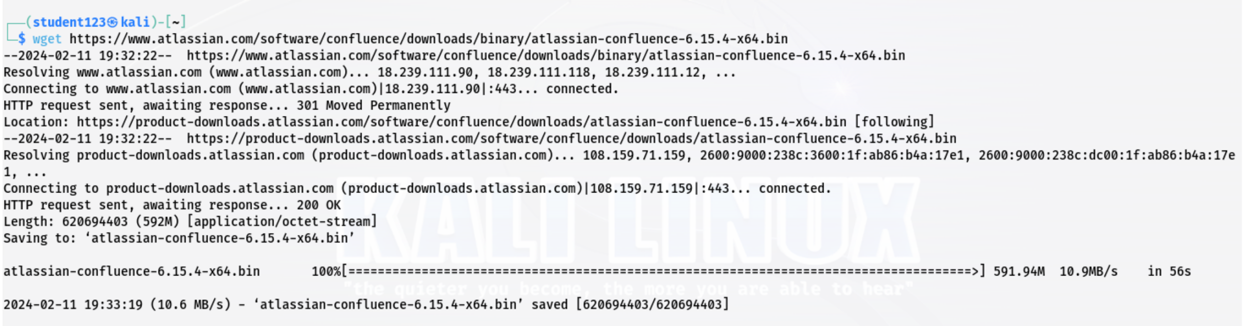
3. dd if=/dev/sdb | md5sum
4. dd if=/dev/sdb of=EvidenceDD
   md5sum EvidenceDD
5. sudo apt install dcfldd
   dcfldd if=/dev/sdb of=EvidenceDCFLDD



```
┌──(student123㉿kali)-[~]
└─$ sudo apt-get install dcfldd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  dcfldd
0 upgraded, 1 newly installed, 0 to remove and 1077 not upgraded.
Need to get 44.6 kB of archives.
After this operation, 117 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 dcfldd amd64 1.9.1-1 [44.6 kB]
Fetched 44.6 kB in 1s (58.6 kB/s)
Selecting previously unselected package dcfldd.
(Reading database ... 506072 files and directories currently installed.)
Preparing to unpack .../dcfldd_1.9.1-1_amd64.deb ...
Unpacking dcfldd (1.9.1-1) ...
Setting up dcfldd (1.9.1-1) ...
Processing triggers for man-db (2.12.0-1) ...
Processing triggers for kali-menu (2023.4.6) ...

┌──(student123㉿kali)-[~]
└─$ sudo dcfldd if=/dev/sdb of=EvidenceDCFLDD
256 blocks (8Mb) written.
314+0 records in
314+0 records out
```

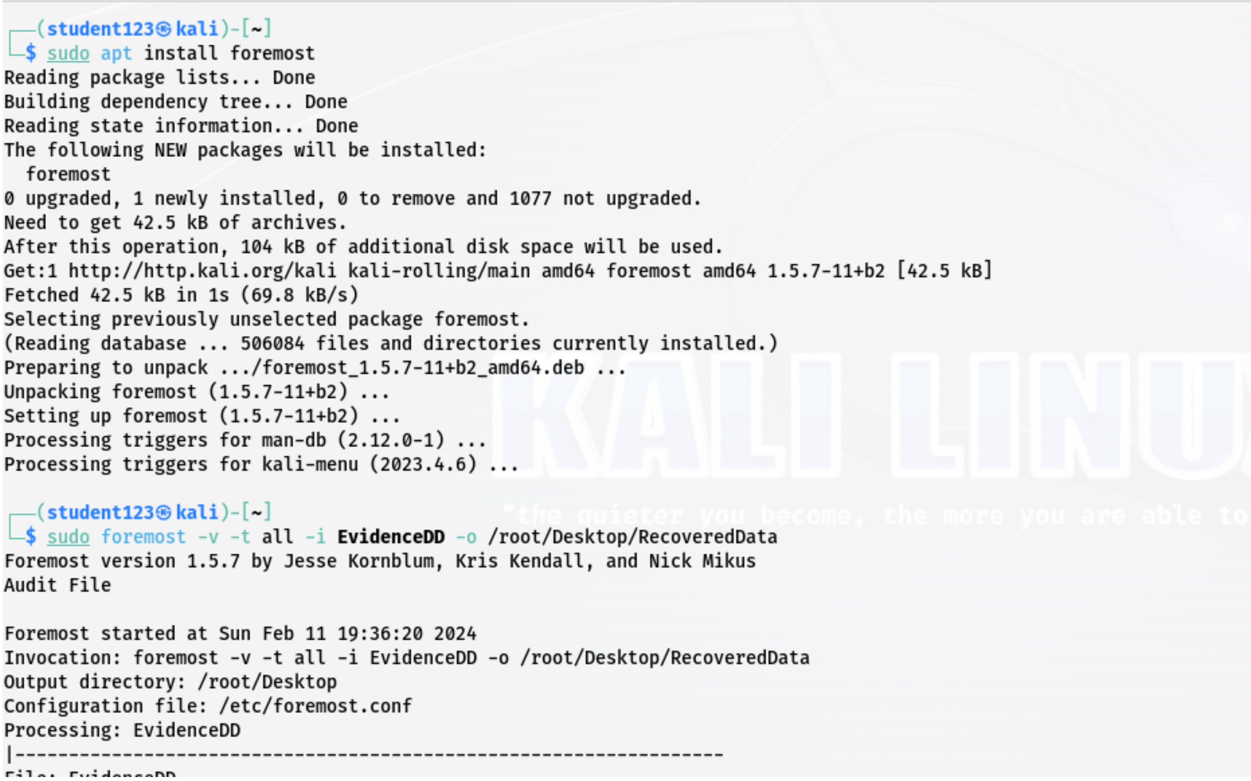


```
┌──(student123㉿kali)-[~]
└─$ sudo dcfldd if=/dev/sdb of=EvidenceDCFLDD
256 blocks (8Mb) written.
314+0 records in
314+0 records out
```

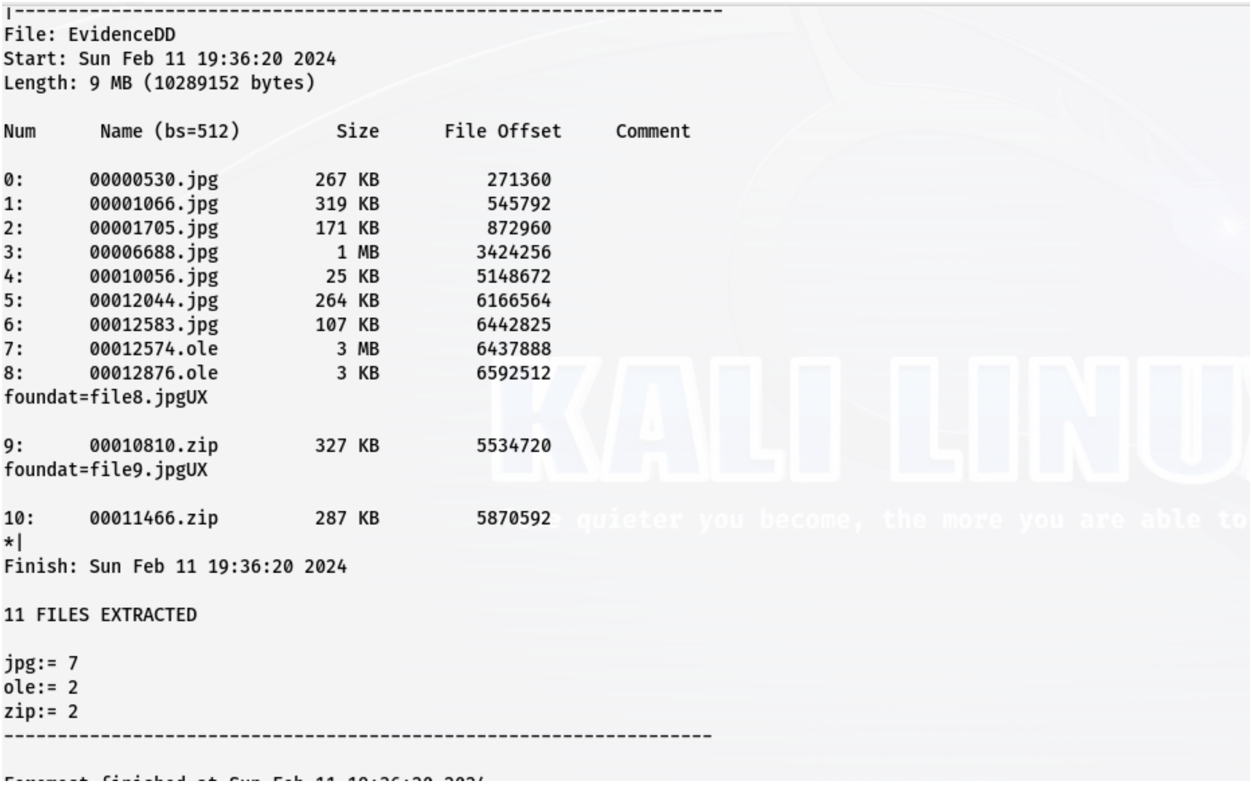


```
┌──(student123㉿kali)-[~]
└─$ wget https://www.atlassian.com/software/confluence/downloads/binary/atlassian-confluence-6.15.4-x64.bin
--2024-02-11 19:32:22--  https://www.atlassian.com/software/confluence/downloads/binary/atlassian-confluence-6.15.4-x64.bin
Resolving www.atlassian.com (www.atlassian.com)... 18.239.111.90, 18.239.111.118, 18.239.111.12, ...
Connecting to www.atlassian.com (www.atlassian.com)|18.239.111.90|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://product-downloads.atlassian.com/software/confluence/downloads/atlassian-confluence-6.15.4-x64.bin [following]
--2024-02-11 19:32:22--  https://product-downloads.atlassian.com/software/confluence/downloads/atlassian-confluence-6.15.4-x64.bin
Resolving product-downloads.atlassian.com (product-downloads.atlassian.com)... 108.159.71.159, 2600:9000:238c:3600:1f:ab86:b4a:17e1, 2600:9000:238c:dc00:1f:ab86:b4a:17e
1, ...
Connecting to product-downloads.atlassian.com (product-downloads.atlassian.com)|108.159.71.159|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 620694403 (592M) [application/octet-stream]
Saving to: ‘atlassian-confluence-6.15.4-x64.bin’

atlassian-confluence-6.15.4-x64.bin       100%[==========================================================================>] 591.94M  10.9MB/s    in 56s

2024-02-11 19:33:19 (10.6 MB/s) - ‘atlassian-confluence-6.15.4-x64.bin’ saved [620694403/620694403]
```

6. sudo apt update
   sudo apt install foremost
   foremost -v -t all -i EvidenceDD -o /root/Desktop/RecoveredData



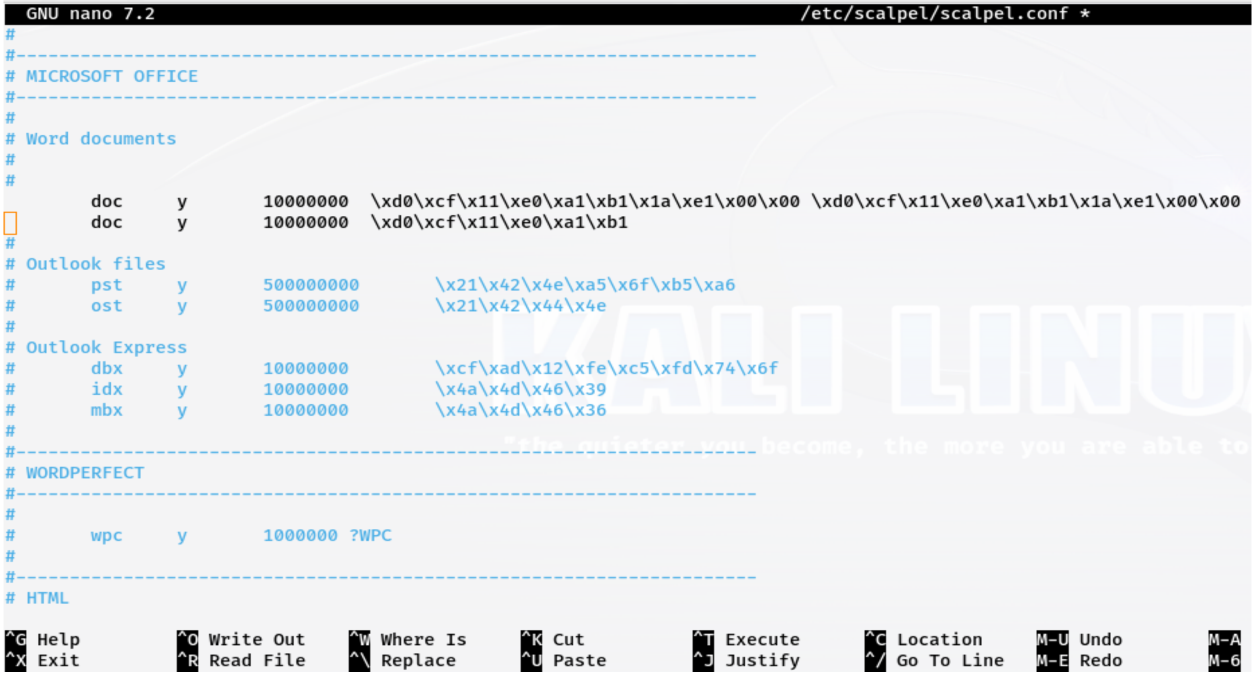
```
┌──(student123㉿kali)-[~]
└─$ sudo apt install foremost
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  foremost
0 upgraded, 1 newly installed, 0 to remove and 1077 not upgraded.
Need to get 42.5 kB of archives.
After this operation, 104 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 foremost amd64 1.5.7-11+b2 [42.5 kB]
Fetched 42.5 kB in 1s (69.8 kB/s)
Selecting previously unselected package foremost.
(Reading database ... 506084 files and directories currently installed.)
Preparing to unpack .../foremost_1.5.7-11+b2_amd64.deb ...
Unpacking foremost (1.5.7-11+b2) ...
Setting up foremost (1.5.7-11+b2) ...
Processing triggers for man-db (2.12.0-1) ...
Processing triggers for kali-menu (2023.4.6) ...

┌──(student123㉿kali)-[~]
└─$ sudo foremost -v -t all -i EvidenceDD -o /root/Desktop/RecoveredData
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Sun Feb 11 19:36:20 2024
Invocation: foremost -v -t all -i EvidenceDD -o /root/Desktop/RecoveredData
Output directory: /root/Desktop
Configuration file: /etc/foremost.conf
Processing: EvidenceDD
|----------------------------------------------------------------
File: EvidenceDD
```



```
|----------------------------------------------------------------------
File: EvidenceDD
Start: Sun Feb 11 19:36:20 2024
Length: 9 MB (10289152 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00000530.jpg         267 KB          271360
1:      00001066.jpg         319 KB          545792
2:      00001705.jpg         171 KB          872960
3:      00006688.jpg           1 MB         3424256
4:      00010056.jpg          25 KB         5148672
5:      00012044.jpg         264 KB         6166564
6:      00012583.jpg         107 KB         6442825
7:      00012574.ole           3 MB         6437888
8:      00012876.ole           3 KB         6592512
foundat=file8.jpgUX

9:      00010810.zip         327 KB         5534720
foundat=file9.jpgUX

10:     00011466.zip         287 KB         5870592
*|
Finish: Sun Feb 11 19:36:20 2024

11 FILES EXTRACTED

jpg:= 7
ole:= 2
zip:= 2
------------------------------------------------------------------

Foremost finished at Sun Feb 11 19:36:20 2024
```

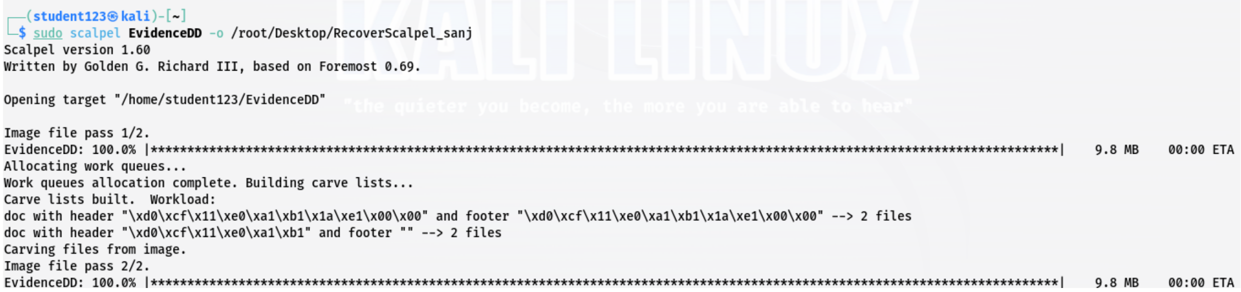
7. Nano /etc/foremost.conf

Uncomment some file types in the configuration file for those files to be recovered by foremost (you can just find where word doc is written and uncomment it.)

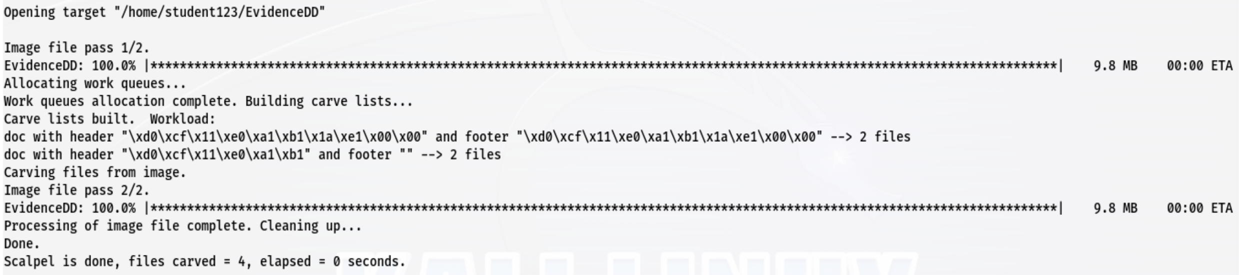


```
  GNU nano 7.2                                                           /etc/scalpel/scalpel.conf *
#
#---------------------------------------------------------------------
# MICROSOFT OFFICE
#---------------------------------------------------------------------
#
# Word documents
#
#
        doc     y       10000000  \xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00 \xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00
        doc     y       10000000  \xd0\xcf\x11\xe0\xa1\xb1
#
# Outlook files
#       pst     y       500000000       \x21\x42\x4e\xa5\x6f\xb5\xa6
#       ost     y       500000000       \x21\x42\x44\x4e
#
# Outlook Express
#       dbx     y       10000000        \xcf\xad\x12\xfe\xc5\xfd\x74\x6f
#       idx     y       10000000        \x4a\x4d\x46\x39
#       mbx     y       10000000        \x4a\x4d\x46\x36
#
#---------------------------------------------------------------------
# WORDPERFECT
#---------------------------------------------------------------------
#
#       wpc     y       1000000 ?WPC
#
#---------------------------------------------------------------------
# HTML
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6
```

8. Recovery using Scalpel
sudo scalpel EvidenceDD -o /root/Desktop/RecoverScalpel_sanj



```
┌──(student123㉿kali)-[~]
└─$ sudo scalpel EvidenceDD -o /root/Desktop/RecoverScalpel_sanj
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/home/student123/EvidenceDD"

Image file pass 1/2.
EvidenceDD: 100.0% |*************************************************************************************************************************|    9.8 MB    00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
doc with header "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" and footer "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" --> 2 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1" and footer "" --> 2 files
Carving files from image.
Image file pass 2/2.
EvidenceDD: 100.0% |*************************************************************************************************************************|    9.8 MB    00:00 ETA
```



```
Opening target "/home/student123/EvidenceDD"

Image file pass 1/2.
EvidenceDD: 100.0% |*************************************************************************************************************************|    9.8 MB    00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
doc with header "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" and footer "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" --> 2 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1" and footer "" --> 2 files
Carving files from image.
Image file pass 2/2.
EvidenceDD: 100.0% |*************************************************************************************************************************|    9.8 MB    00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 4, elapsed = 0 seconds.
```

ls to see the folder contents.

CONCLUSION:

____

____

____.