

Lab5: data recovery and extraction

For this lab we will learn about how to acquire data from the computer when the files have been deleted and how to retrieve information based on the recovery data. However, before we get into the acquisition of data and data recovery, we have to have a basic understanding of how data is stored in the computer and what happens when the user deletes the data from the computer.

For a computer to save anything in the hard drive, first it must reserve the spot for the items in the hard drive, after then it will create a reference for the users to interact with that items, and as long as the reference for that particular items exist the reservation spot will always belong to that items and that is how most computer treat saving a file. So what happens when you delete the files? When you delete the files from your computer, it generally only removed the reference of the items from the user to hard drive, and because of how hard drives treat reservation spots, when you delete the file not only does it remove the reference it will also remove the spot reservation for that files as well and during the next iteration of saving on the hard drive, that spot will be overwrite with entirely new data, and that is how the operating system treat the files saving to hard drive. However, because of the reservation system, when the files have been removed, it still exists in the drive for some time and the master files table still has the content available on the it tables. And by using some special tools we can recover all the files that have been deleted as we will see today's lab.

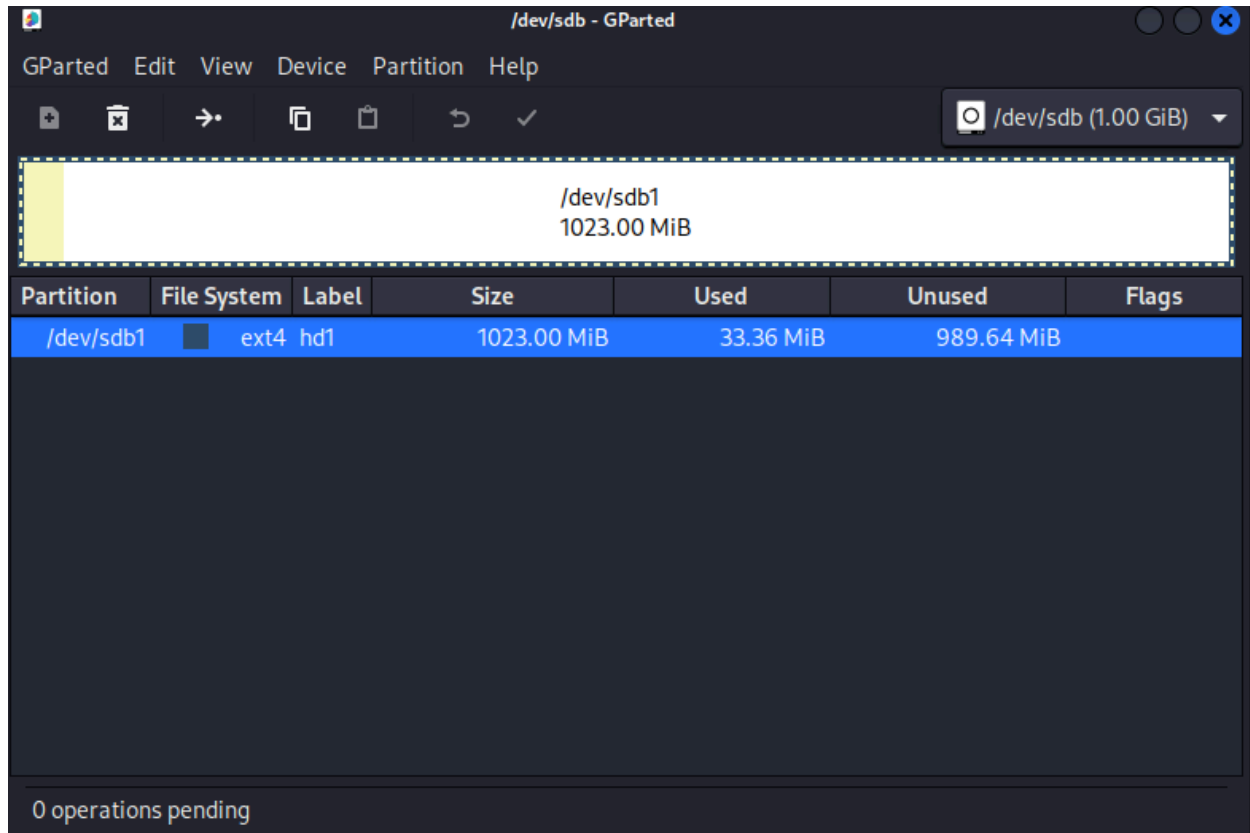
First a review the available hard disk drive:

```
(kali㉿kali)-[~]
$ sudo lshw -class volume -short
[sudo] password for kali:
H/W path          Device          Class          Description
-----
/0/100/d/0/1      /dev/sda1       volume         24GiB EXT4 volume
/0/100/d/0/2      /dev/sda2       volume         975MiB Extended partition
/0/100/d/0/2/5    /dev/sda5       volume         975MiB Linux swap volume
/0/100/d/1/1      /dev/sdb1       volume         1023MiB EXT4 volume

(kali㉿kali)-[~]
$ sudo lshw -class disk -short
H/W path          Device          Class          Description
-----
/0/100/1.1/0.0.0  /dev/cdrom      disk           CD-ROM
/0/100/d/0        /dev/sda        disk           26GB VBOX HARDDISK
/0/100/d/1        /dev/sdb        disk           1073MB VBOX HARDDISK
```

(in this code, we using the command lshw to check the available disk currently recognize in the system)

We run this command i the terminal: `sudo gparted` to opened a partition application



(this should be the application that opens up, however if this is not the case when you have more than one drive, you can select the drive on the top right to the one you want to partition.)(So in order to partition the drive you select the drive, click on the device on the toolbar, select the new partition table and just leave everything at it for now and click on ADD, when done click the check mark in the toolbar and click apply all.) After this step you should have a partition drive ready to be used.

After create the partition drive you might want to change it name and mount it

```
(kali㉿kali)-[~]  
$ sudo tune2fs -L /dev/sdb1  
tune2fs 1.47.0 (5-Feb-2023)  
Usage: tune2fs [-c max_mounts_count] [-e errors_behavior] [-f] [-g group]  
       [-i interval[d|m|w]] [-j] [-J journal_options] [-l]  
       [-m reserved_blocks_percent] [-o [^]mount_options[, ... ]]  
       [-r reserved_blocks_count] [-u user] [-C mount_count]  
       [-L volume_label] [-M last_mounted_dir]  
       [-O [^]feature[, ... ]] [-Q quota_options]  
       [-E extended-option[, ... ]] [-T last_check_time] [-U UUID]  
       [-I new_inode_size] [-z undo_file] device
```

(this display the however as i already rename the drive it will not work)

```
(kali㉿kali)-[~]  
$ sudo tune2fs -L alforensics1g /dev/sdb1  
tune2fs 1.47.0 (5-Feb-2023)
```

(this code will rename the drive to alforensics1g, however after you run this code you will need to reboot the system for the change to be apply)

Run this code in the terminal: reboot

```
# reboot the system  
kali㉿kali)-[~] reboot
```

(this will reboot the whole system)

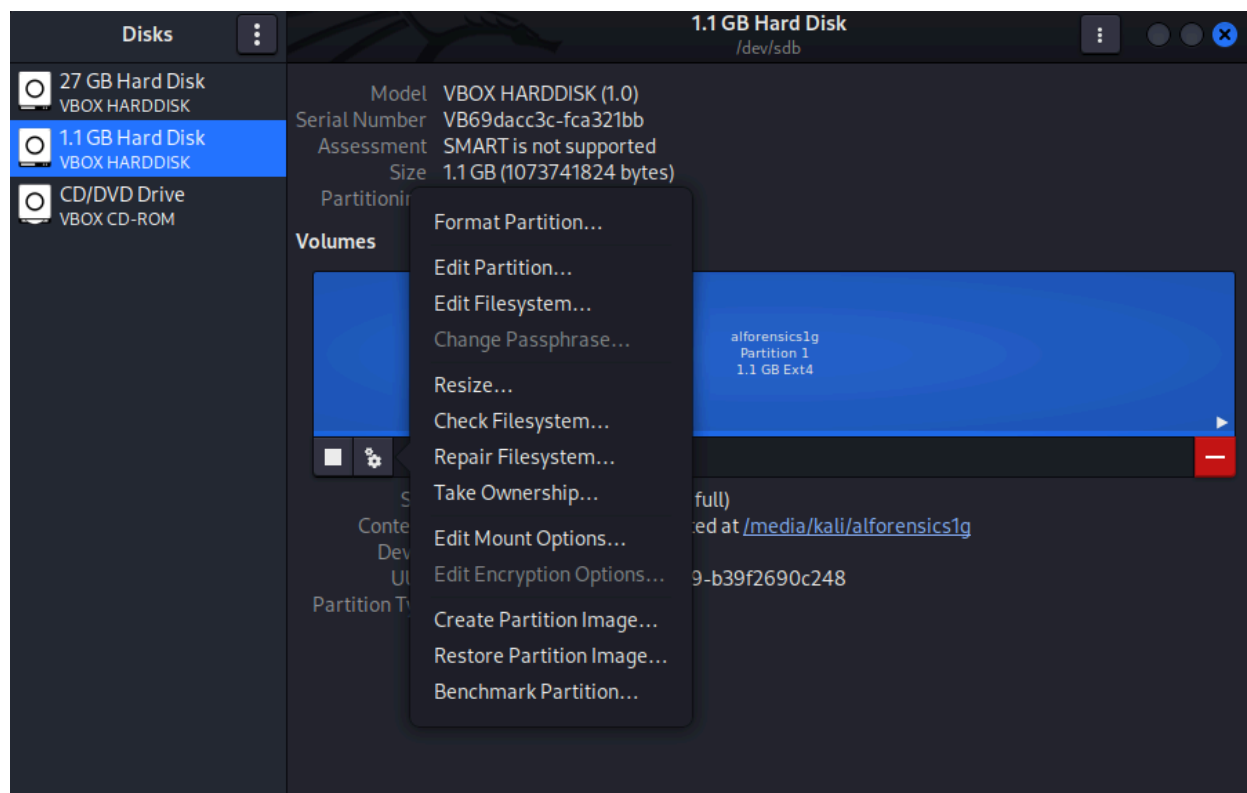
After the reboot and mounted the drive this is what you will get

```
(kali㉿kali)-[~]  
$ df  
Filesystem      1K-blocks    Used Available Use% Mounted on  
udev             964252         0    964252   0% /dev  
tmpfs            201208        1028    200180   1% /run  
/dev/sda1       24640544 18368076  4995440  79% /  
tmpfs            1006028         0    1006028   0% /dev/shm  
tmpfs             5120          0         5120   0% /run/lock  
tmpfs            201204         116    201088   1% /run/user/1000  
/dev/sdb1       1013420         24    944636   1% /media/kali/alforensics1g
```

Another function that help avoiding disk writing error

```
(kali㉿kali)-[~]  
$ sudo apt-get install gnome-disk-utility
```

(this will install the gnome, which lets you take ownership of of the partition so that it can minimize the write to disk error)



Next we sanitize the drive before copy or moving content to it

```
(kali㉿kali)-[~/Downloads]
└─$ sudo dd if=/dev/random of=/dev/sdb1 bs=1M status=progress
1062207488 bytes (1.1 GB, 1013 MiB) copied, 12 s, 88.4 MB/s
dd: error writing '/dev/sdb1': No space left on device
1024+0 records in
1023+0 records out
1072693248 bytes (1.1 GB, 1023 MiB) copied, 12.194 s, 88.0 MB/s
```

(what we are doing in this is wiping the partition.)

(code: call the method dd function(if=) generate random values and and output it in (of=) sdb1 with the max bytes of 1M (bs=1M) with display the status when it run(status=progress))

Now that you has wipe the drive we gonna copy a bunch of zero in to that drive

```
(kali㉿kali)-[~/Downloads]
└─$ sudo dd if=/dev/zero of=/dev/sdb1 bs=1M
dd: error writing '/dev/sdb1': No space left on device
1024+0 records in
1023+0 records out
1072693248 bytes (1.1 GB, 1023 MiB) copied, 20.0377 s, 53.5 MB/s
```

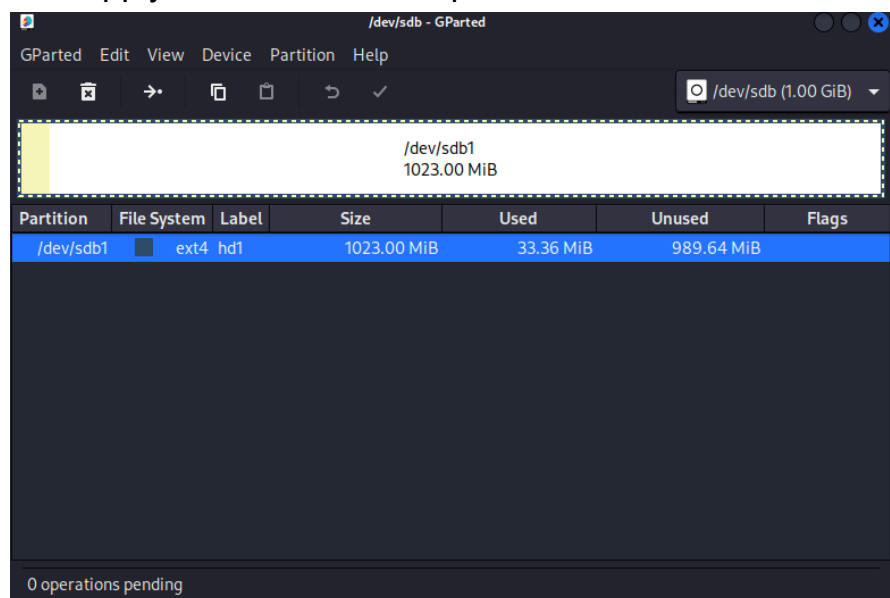
(code : method dd function(if=/dev/zero) generate zero values and put it in the drive(of=/dev/sdb1) with the maximum bytes of 1M(bs=1M)

Here is another way to wipe the content of the drive/partition, you can wipe it by pattern.

```
(kali㉿kali)-[~/Downloads]
$ sudo dcfldd pattern=AAAA of=/dev/sdb1 bs=1M status=progress
768 blocks (768Mb) written.dcfldd:: No space left on device
```

(code: method dcfldd(Department of Defense Computer Forensics Lab) this responsible for wiping the content, look for this pattern in the partition/drive (pattern=AAAA) from/ output sdb1 (of=/dev/sdb1) with the max bytes size of 1M(bs=1M) show process when run(status=progress)) After this code done running the content in the partition/drive what have the matching pattern of AAAA will be remove.

For the next part we will need to remove the current partition and create a new one. For that just follow the step above for how to create a new partition. Som important note you will need to delete the current partition in order to create a new one, so when you select the partition right click and select delete, after that click apply and create a new partition afterward.



Now we move to file recovery

Take whatever files you have that are not important and move it into the partition drive. You can use the command `sudo mv [files name] [target destination]` to

move the files or if you want to move them all at one then use `sudo mv [target destination] [files 1][files 2]` this should work , also remember to remove [] because this is for demo purpose. ex(`mv sample.zip /media/kali/a1forensics1g` or `mv /media/kali/a1forensics1g sample.zip sample2.zip`)

```
(kali㉿kali)-[/media/kali/alforensics1g]
$ ls
101  MICC-F220  MICC-F220.zip  lost+found  sb1
```

(just a little note if you want to unzip the files just run this `unzip sample.zip`, this will unzip the file in the current directory)

(Code : (ls) list the files that currently exist in the directory.)

Next move to the folder MICC-F220 by: `cd MICC-F220`

```
(kali㉿kali)-[/media/kali/alforensics1g/MICC-F220]
$ ls -l | grep .jpg | wc -l
220
```

(this code will count how many jpg are current in that directory.)

(code: (ls -l | grep.jpg| wc -l) list the all the jpg file and past that list to count(wc -l) and return the count of how many in the directory)

```
(kali㉿kali)-[/media/kali/alforensics1g/MICC-F220]
$ sudo rm *.jpg
[sudo] password for kali:

(kali㉿kali)-[/media/kali/alforensics1g/MICC-F220]
$ ls -l | grep .jpg | wc -l
0
```

(in this we remove all the jpg files and then check to see how many jpg are exist after the remove, and it should return 0)

(code: (rm) this is a remove function (*.jpg) this mean select all jpg files)

```
(kali㉿kali)-[/media/kali/alforensics1g/MICC-F220]
$ cd ../101

(kali㉿kali)-[/media/kali/alforensics1g/101]
$ ls -l | grep .jpg | wc -l
7
```

(we do the same thing for this folder check how many jpg)

```
(kali㉿kali)-[/media/kali/alforensics1g/101]
$ sudo rm *.jpg

(kali㉿kali)-[/media/kali/alforensics1g/101]
$ ls -l | grep .jpg | wc -l
0
```

(and we remove all of the jpg)

Now we want to check how many files that still in the folder/directory after the removal of all jpg files

```
(kali㉿kali)-[/media/kali/alforensics1g/101]
$ ls -l | wc -l
974
```

Now for the recovery: create a folder to store the recover file and move to it

```
(kali㉿kali)-[/media/kali/alforensics1g/101]
$ sudo mkdir jpegrecovery && cd jpegrecovery

(kali㉿kali)-[/media/kali/alforensics1g/101/jpegrecovery]
$
```

(code: (mkdir) make a new directory (&&) and (cd) move to)
First make sure the new folder is empty.

```
(kali㉿kali)-[/media/kali/alforensics1g/101/jpegrecovery]
$ ls -l
total 0
```

Now we will need to the tool for recovery run this

```
(kali㉿kali)-[/media/kali/alforensics1g/101/jpegrecovery]
$ sudo apt-get install recoverjpeg -y
```

```
(kali㉿kali)-[/media/kali/alforensics1g]
$ sudo recoverjpeg /dev/sdb1 -o ./101/jpegrecovery
Restored 228 pictures
```

(now remember move back to the main folder that contain the recovery container
and run the method recoverjpeg ([what location do you want to recover from])
/dev/sdb1 and (-o=the output) output it in ./101/jpegrecovery)

```
(kali㉿kali)-[/media/kali/alforensics1g]
$ ls -l ./101/jpegrecovery/*.jpg | wc -l
228
```

(Now run a check of how many file are in the recovery folder that are jpg)

That is one way you can recover all the deleted jpg files using recoverjpeg tools.
Next we're gonna use foremost tools to recover even more data.

Before any of that you have to get the tools first if you don't have it

```
kali㉿kali)-[ /media/kali/a1forensics1g] sudo apt-get install foremost -y
```

Now remove all the folders in the current partition/drive. There are two ways of doing this, the first one is to open the drive as root and delete them all or do it by command like this.

```
(kali㉿kali)-[/media/kali/alforensics1g]
$ sudo rm -r *
```

(right here i run the remove command (-r *) recursively meaning that it will run and run until all files are delete.)

Next create an image file, this is where most of the recovery methods are taking information from.

```
(kali㉿kali)-[/media/kali/alforensics1g]
$ cd ~ && mkdir evidencesdb1
```

(go back to the main directory(kali) and and make a new directory name evidencesdb1)

```
(kali㉿kali)-[~]
$ sudo dd if=/dev/sdb1 of=./evidencesdb1/sdb1image.dd hash=sha1 hashlog=./evidencesdb1/hashlog.log
32512 blocks (1016Mb) written.
32736+0 records in
32736+0 records out

(kali㉿kali)-[~]
$ ls evidencesdb1
hashlog.log  sdb1image.dd

(kali㉿kali)-[~]
$ cat ./evidencesdb1/hashlog.log

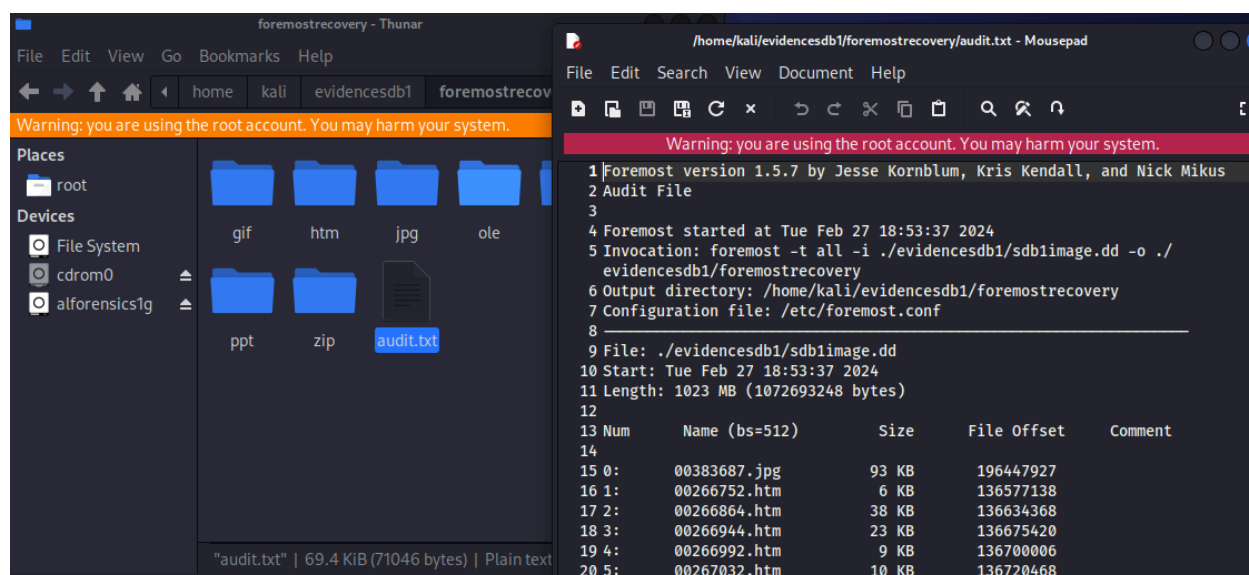
Total (sha1): ff54ae9e9b7ee59317243694c660dc9de9f8870c
```


(code: call the method dcflddd with the input location (if=/dev/sdb1) and the output (of=./evidencesdb1/sdb1image.dd) after that past the information to hash function (sha1) and log it in (hashlog=./evidencesdb1/hashlog.log) this will create two files in the folders, one is the hash files and one is the image files of the drive.)

```
(kali@kali)-[~]  
$ sudo foremost -t all -i ./evidencesdb1/sdb1image.dd -o ./evidencesdb1/foremostrecovery
```

(the code run as follow:
call the method foremost and for all items in the drive image output it in
foremostrecovery folder)

And this is the result



(all the files that has being delete on the drive now has been recover and place in their respective folders)

Next we look at another tool for recover name scalpel Tool

This should function the same as the foremost but with the exception that you have a choice to pick what you want to recover.

But first install

```
(kali@kali)-[~]  
$ sudo apt-get install scalpel -y
```

```
(kali㉿kali)-[~]
$ sudo scalpel -o ./evidencesdb1/scalpelrecovery2/ ./evidencesdb1/sdb1image.dd
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/home/kali/evidencesdb1/sdb1image.dd"

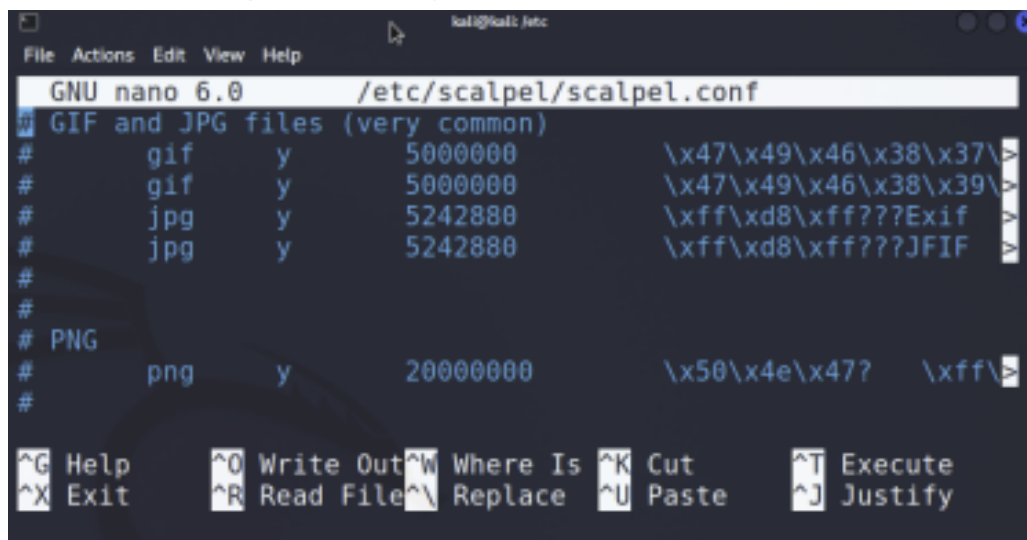
ERROR: The configuration file didn't specify any file types to carve.
(If you're using the default configuration file, you'll have to
uncomment some of the file types.)

See /etc/scalpel/scalpel.conf.
```

(in this screenshot this error happened because of the lack of files type you want to recover from the command)

You will have to go to the path that contains the scalpel.conf and uncomment the file type you want to get.

(route= go to the home folder, files system , and follow the path (etc/scalpel) you will see the scalpel.conf file.)



```
GNU nano 6.0 /etc/scalpel/scalpel.conf
# GIF and JPG files (very common)
# gif y 5000000 \x47\x49\x46\x38\x37\x14
# gif y 5000000 \x47\x49\x46\x38\x39\x14
# jpg y 5242880 \xff\xd8\xff???Exif
# jpg y 5242880 \xff\xd8\xff???JFIF
#
#
# PNG
# png y 20000000 \x50\x4e\x47? \xff\
#
```

(it should look something like this, just uncomment the files type you want to get and then run the command again, now it should just work and all the files will be outputted in scalpelrecovery2)

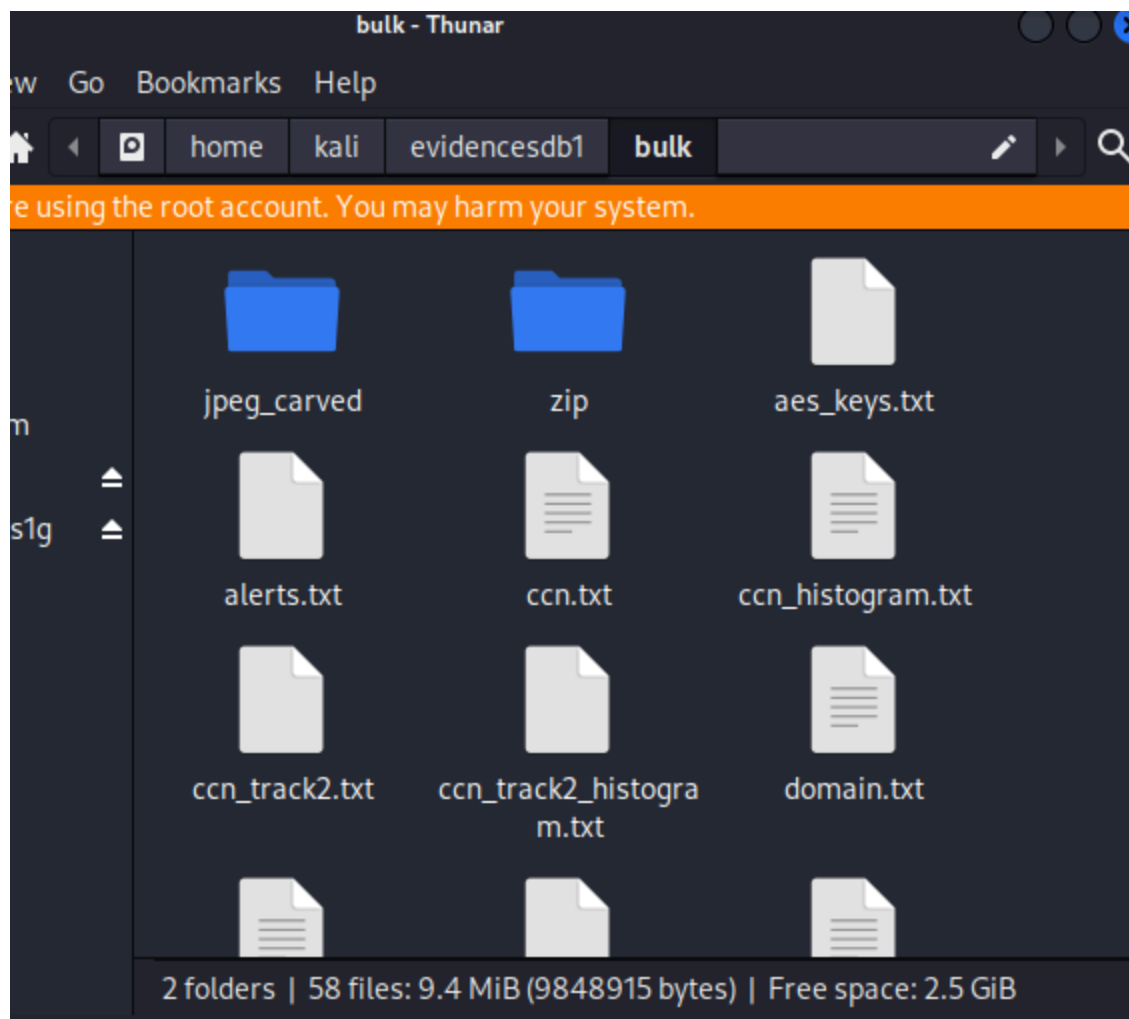
Finally bulk data extraction.

```
(kali@kali)-[~]  
$ sudo bulk_extractor -o ./evidencesdb1/bulk ./evidencesdb1/sdb1image.dd  
mkdir "./evidencesdb1/bulk"  
bulk_extractor version: 2.0.3  
Input file: "./evidencesdb1/sdb1image.dd"  
Output directory: "./evidencesdb1/bulk"  
Disk Size: 1072693248
```

(this will then extract more Information in addition to files, and it including email addresses, encryption keys, domain names, credit card numbers, among others, can also be stored on the drive based on the image file.)

The output:

```
Phase 2. Shutting down scanners  
Computing final histograms and shutting down...  
Phase 3. Generating stats and printing final usage information  
All Threads Finished!  
Elapsed time: 183.9 sec.  
Total MB processed: 1072  
Overall performance: 5.833 MBytes/sec 2.916 (MBytes/sec/thread)  
sbufs created: 3689690  
sbufs unaccounted: 0  
Time producer spent waiting for scanners to process data: 0:02:38 (158.86 seconds)  
Time consumer scanners spent waiting for data from producer: 0:00:00 (0.00 seconds)  
Average time each consumer spent waiting for data from producer: 0:00:00 (0.00 seconds)  
*** More time spent waiting for workers. You need a faster CPU or more cores for improved performance.  
Total email features found: 3664
```



So in conclusion there are many tools that are out there for you to recover your data but selecting the best one for the jobs is the most important. However, there is one thing to note, not all data can be recovered, some may not even be recoverable so work with caution when you handle data.

Resource

Info on what happen when delete the file

<https://www.aptosolutions.com/blog/when-does-deleting-a-file-not-delete-it>

Tools use

Gnome-disk-utility: for formatting partition of the disk

Foremost : data recovery tool

Scalpel : data recovery tool

Some images where from lab5