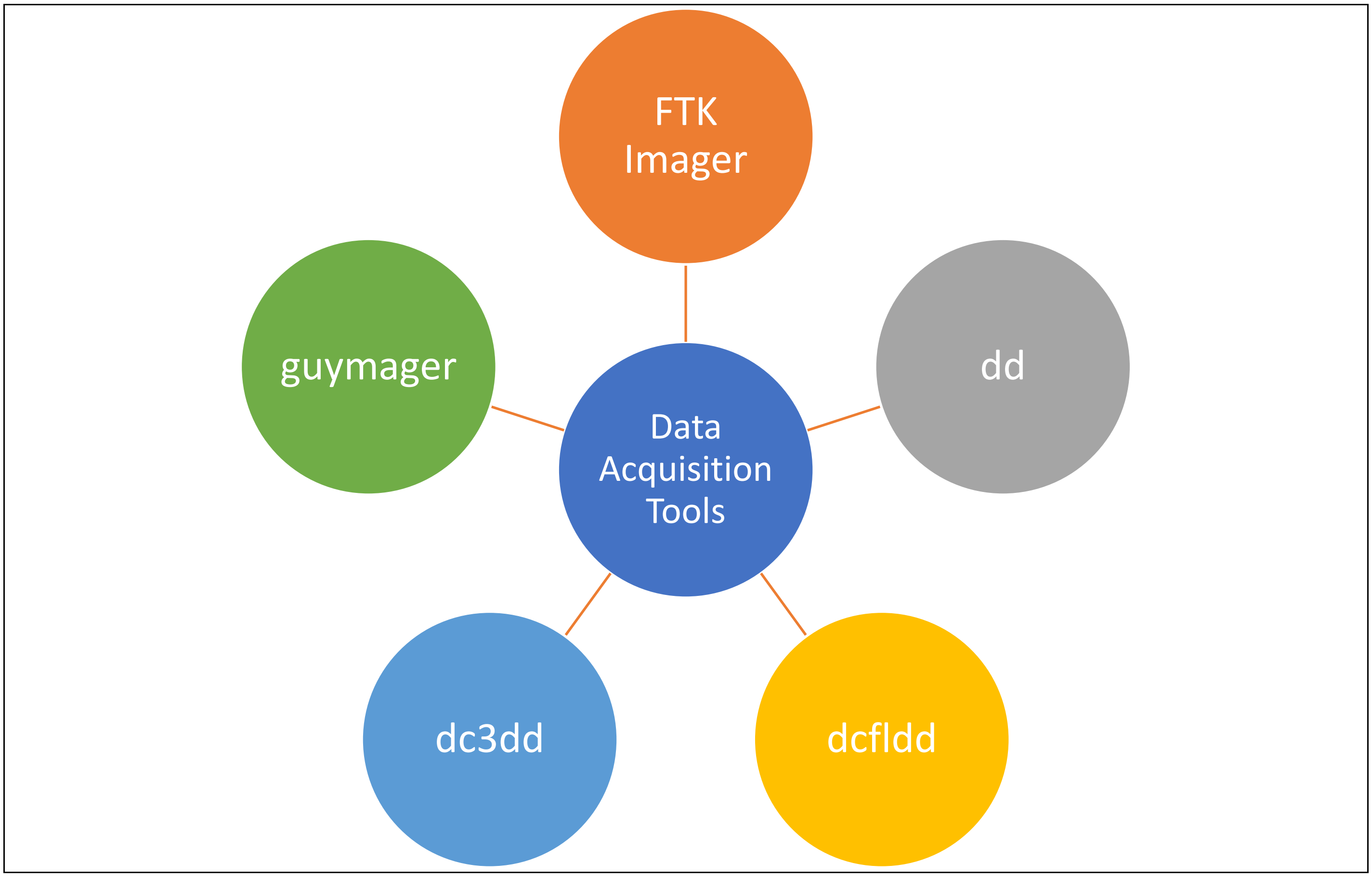
Cyber Law and Forensics (CS402)

Lab Assignment 2

U19CS012

1.) Collecting evidence from a Turned Off system.



A.) FTK Imager

Steps:-

1.) File -> Create Disk Image -> Physical Drive -> Select Your Drive -> Finish -> Add -> File Format (E01 (Recommended) / Raw(dd) / SMART / AFF)

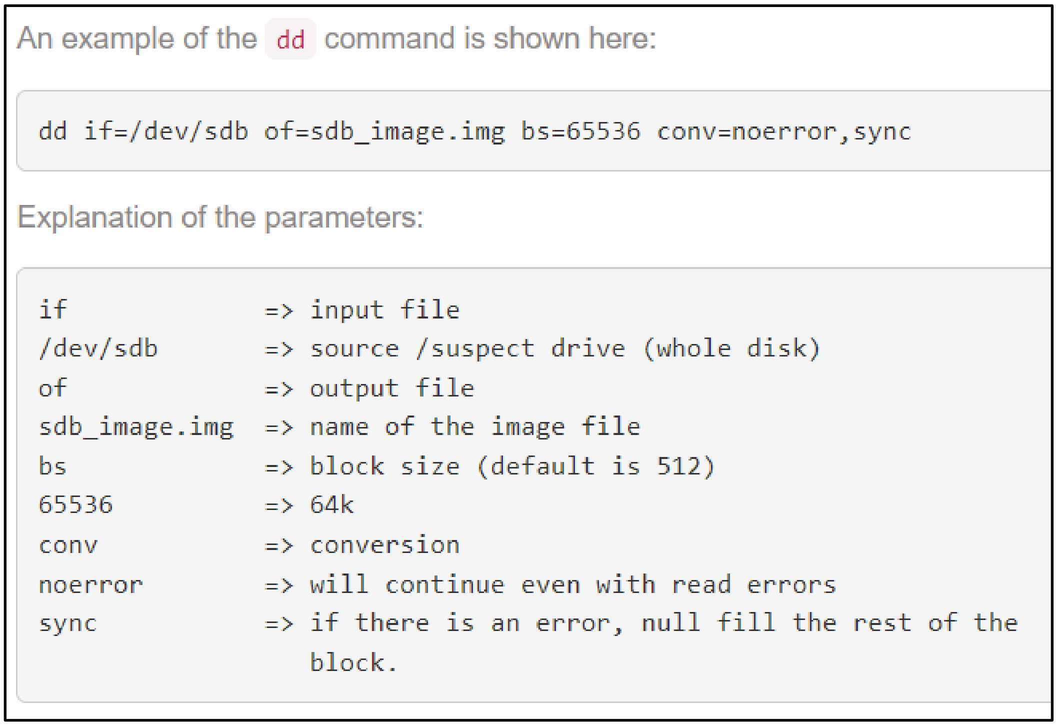
Steps Followed using Blog.

Screenshot

B.) dd Command

Acquiring Data with "**dd**" in Linux

- ✓ dd -> "data dump"
- ✓ creates a bit-by-bit copy of a physical drive without mounting the drive first



An example of the `dd` command is shown here:

```
dd if=/dev/sdb of=sdb_image.img bs=65536 conv=noerror,sync
```

Explanation of the parameters:

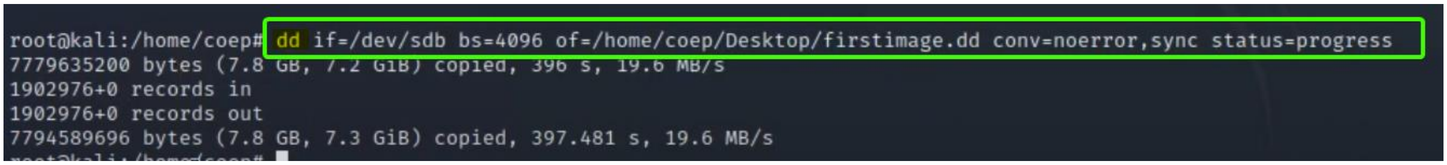
```
if             => input file
/dev/sdb       => source /suspect drive (whole disk)
of             => output file
sdb_image.img  => name of the image file
bs             => block size (default is 512)
65536          => 64k
conv           => conversion
noerror        => will continue even with read errors
sync           => if there is an error, null fill the rest of the
                  block.
```

status=progress -> to show the progress of imaging.

Important Points to Note:-

- ➢ **dd** does not create an MD5 hash.
- ➢ Don't reverse if with of. You might lose all the data on the suspect drive!

<u>Screenshot</u>



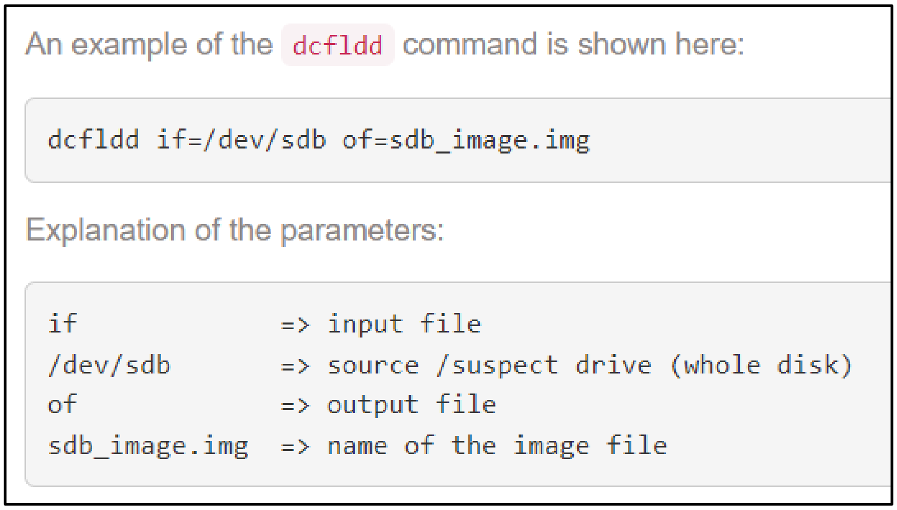
```
root@kali:/home/coep# dd if=/dev/sdb bs=4096 of=/home/coep/Desktop/firstimage.dd conv=noerror,sync status=progress
7779635200 bytes (7.8 GB, 7.2 GiB) copied, 396 s, 19.6 MB/s
1902976+0 records in
1902976+0 records out
7794589696 bytes (7.8 GB, 7.3 GiB) copied, 397.481 s, 19.6 MB/s
root@kali:/home/coep# █
```

C.) dcfldd Command

Dcfldd -> Defense Computer Forensics Laboratory (DCFL) "dd"

"dcfldd" offers the following options:

- ✓ Log errors to an output file for analysis and review
- ✓ Various hashing options MD5, SHA-1, SHA-256, etc
- ✓ Indicating the acquisition progress
- ✓ Split image file into segmented volumes
- ✓ Verify acquired data with the original source



An example of the `dcfldd` command is shown here:

```
dcfldd if=/dev/sdb of=sdb_image.img
```

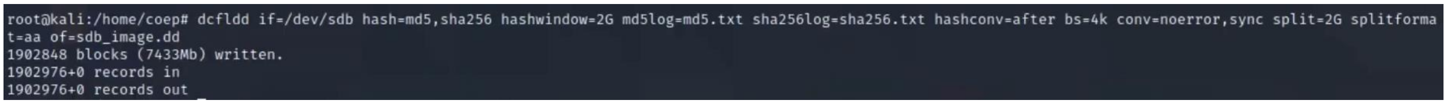
Explanation of the parameters:

```
if             => input file
/dev/sdb       => source /suspect drive (whole disk)
of             => output file
sdb_image.img  => name of the image file
```

Important Note:

dcfldd can enter an **infinite loop** when a faulty sector is encountered on the source drive, thus writing to the image over and over again until there is no free space left.

Screenshot

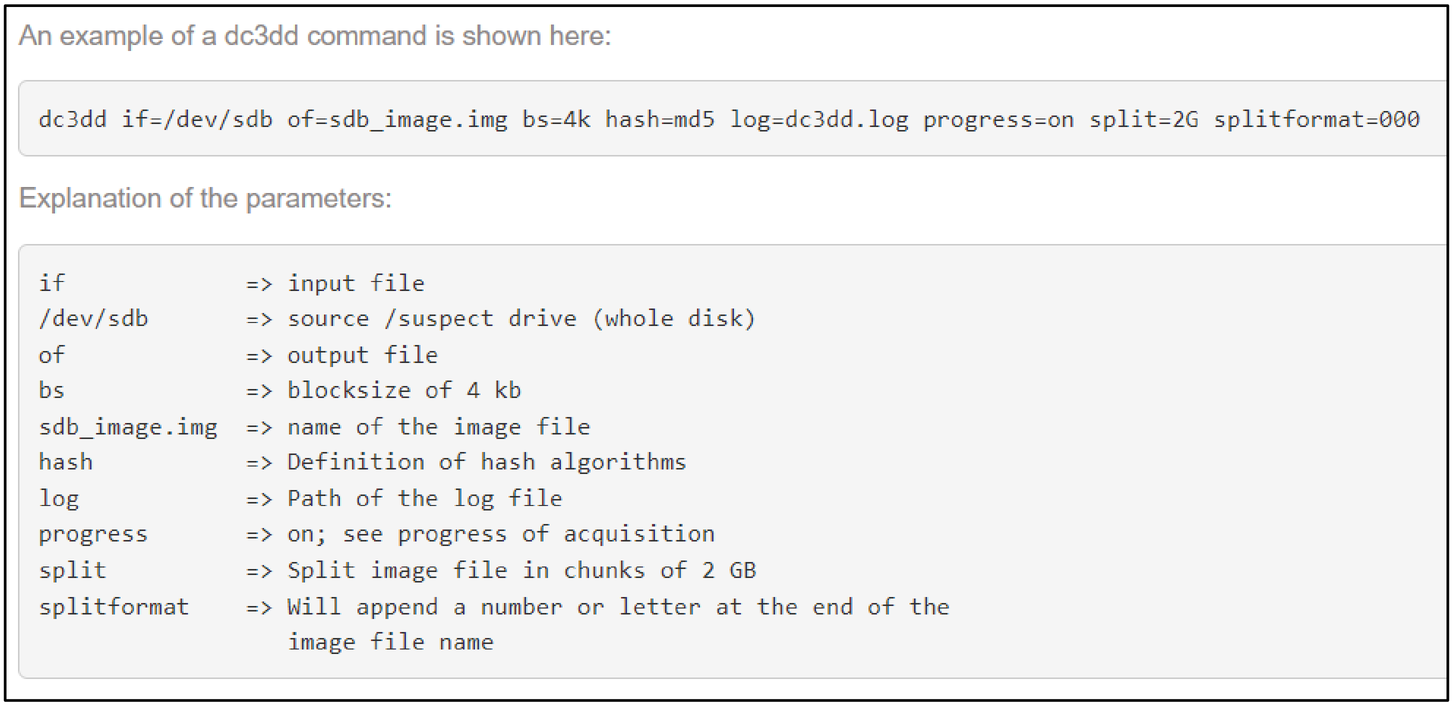


```
root@kali:/home/coep# dcfldd if=/dev/sdb hash=md5,sha256 hashwindow=2G md5log=md5.txt sha256log=sha256.txt hashconv=after bs=4k conv=noerror,sync split=2G splitforma
t=aa of=sdb_image.dd
1902848 blocks (7433Mb) written.
1902976+0 records in
1902976+0 records out _
```

D.) dc3dd Command

dc3dd -> DoD Cyber Crime Center dd

dc3dd will be updated every time GNU dd is updated und is therefore not affected by any bugs of an old dd version.



An example of a dc3dd command is shown here:

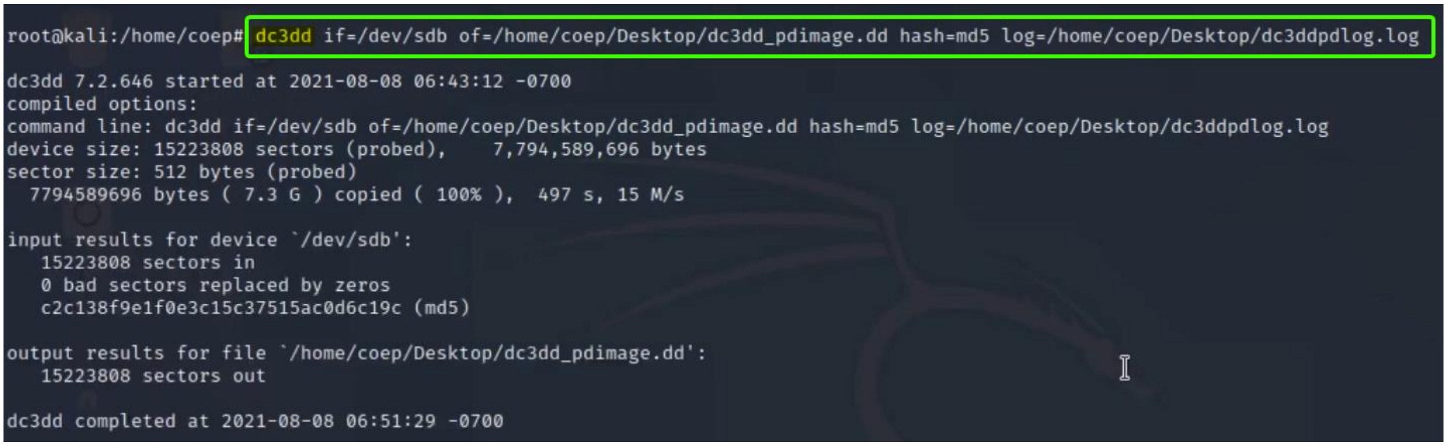
```
dc3dd if=/dev/sdb of=sdb_image.img bs=4k hash=md5 log=dc3dd.log progress=on split=2G splitformat=000
```

Explanation of the parameters:

```
if            => input file
/dev/sdb      => source /suspect drive (whole disk)
of            => output file
bs            => blocksize of 4 kb
sdb_image.img => name of the image file
hash          => Definition of hash algorithms
log           => Path of the log file
progress      => on; see progress of acquisition
split         => Split image file in chunks of 2 GB
splitformat   => Will append a number or letter at the end of the
                 image file name
```

Reference Blog Link.

Screenshot



```
root@kali:/home/coep# dc3dd if=/dev/sdb of=/home/coep/Desktop/dc3dd_pdimage.dd hash=md5 log=/home/coep/Desktop/dc3ddpdlog.log

dc3dd 7.2.646 started at 2021-08-08 06:43:12 -0700
compiled options:
command line: dc3dd if=/dev/sdb of=/home/coep/Desktop/dc3dd_pdimage.dd hash=md5 log=/home/coep/Desktop/dc3ddpdlog.log
device size: 15223808 sectors (probed),    7,794,589,696 bytes
sector size: 512 bytes (probed)
  7794589696 bytes ( 7.3 G ) copied ( 100% ),  497 s, 15 M/s

input results for device `/dev/sdb':
   15223808 sectors in
   0 bad sectors replaced by zeros
   c2c138f9e1f0e3c15c37515ac0d6c19c (md5)

output results for file `/home/coep/Desktop/dc3dd_pdimage.dd':
   15223808 sectors out

dc3dd completed at 2021-08-08 06:51:29 -0700
```

- **dd**

—> already installed

- **dcfldd** (Defense Computer Forensics Lab)

—> sudo apt-get install dcfldd

—> fork of dd

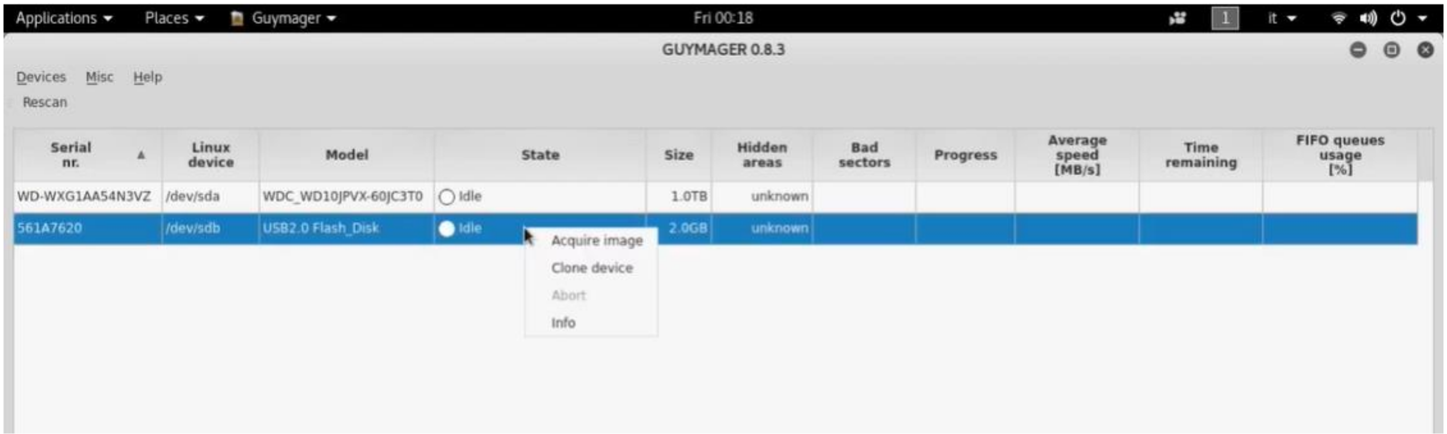
• **dc3dd** (Defense Cyber Crime Center)

—> sudo apt-get install dc3dd

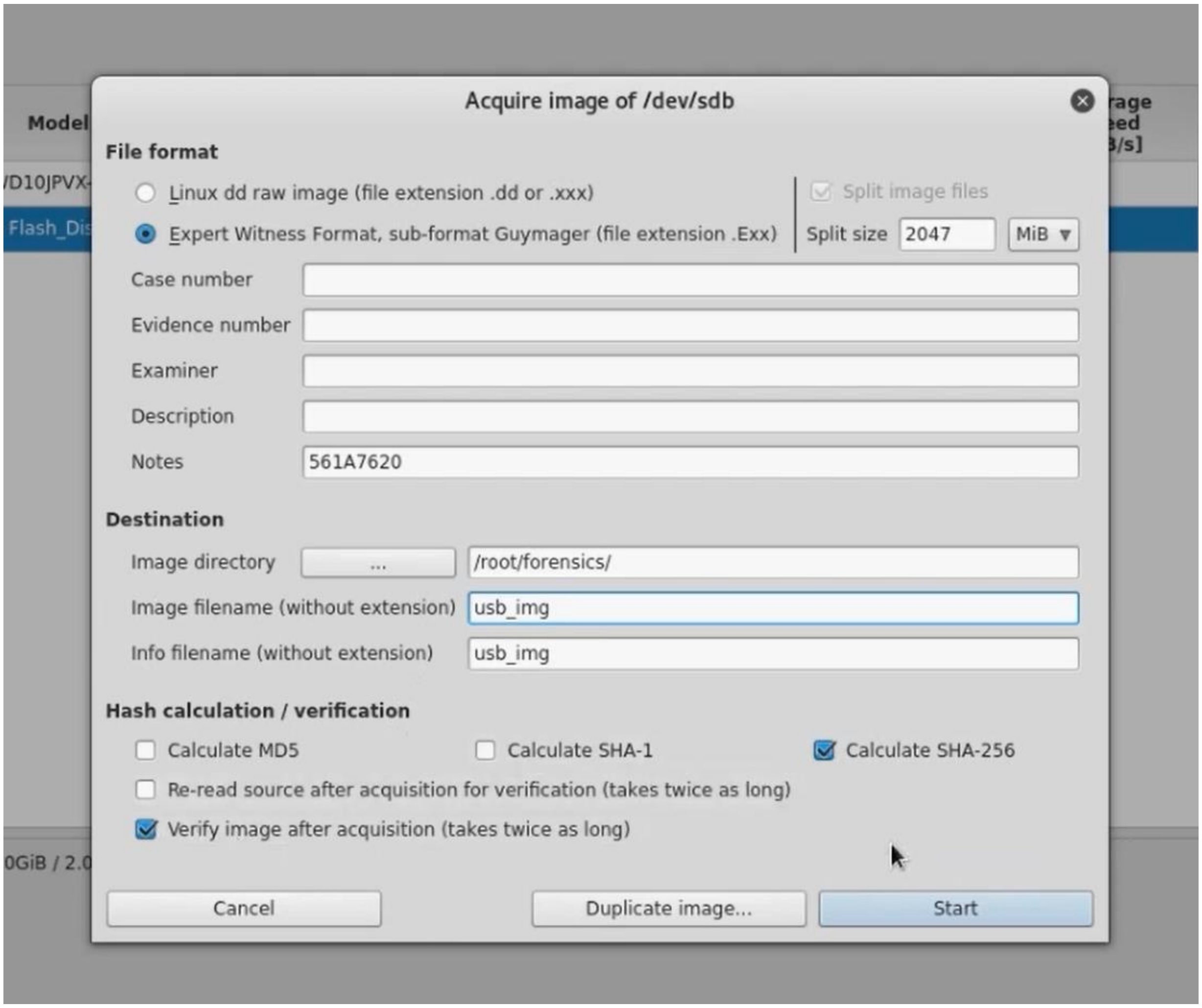
—> uses dd, adds cababilities

E.) Guymager

✓ Guymager is a GUI program based on the Qt libraries that run only on Linux
✓ It supports raw dd and EWF image formats
✓ It includes case management functionalities
✓



Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]	Time remaining	FIFO queues usage [%]
WD-WXG1AA54N3VZ	/dev/sda	WDC_WD10JPVX-60JC3T0	○ Idle	1.0TB	unknown					
561A7620	/dev/sdb	USB2.0 Flash_Disk	● Idle	2.0GB	unknown					



File format

○ Linux dd raw image (file extension .dd or .xxx)

● Expert Witness Format, sub-format Guymager (file extension .Exx)

☑ Split image files

Split size: 2047 MiB

Case number:

Evidence number:

Examiner:

Description:

Notes: 561A7620

Destination

Image directory: /root/forensics/

Image filename (without extension): usb_img

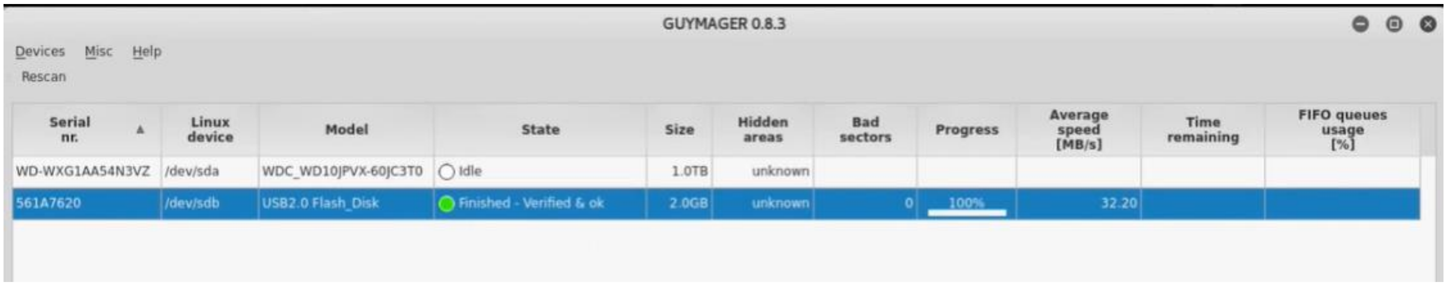
Info filename (without extension): usb_img

Hash calculation / verification

□ Calculate MD5 □ Calculate SHA-1 ☑ Calculate SHA-256

□ Re-read source after acquisition for verification (takes twice as long)

☑ Verify image after acquisition (takes twice as long)



Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]	Time remaining	FIFO queues usage [%]
WD-WXG1AA54N3VZ	/dev/sda	WDC_WD10JPVX-60JC3T0	○ Idle	1.0TB	unknown					
561A7620	/dev/sdb	USB2.0 Flash_Disk	● Finished - Verified & ok	2.0GB	unknown	0	100%	32.20		

SUBMITTED BY: U19CS012

BHAGYA VINOD RANA