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](https://www.hackingdream.net/2018/06/cloning-disk-without-tampering-drive-using-ftk-imager-forensic-investigation.html).

**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

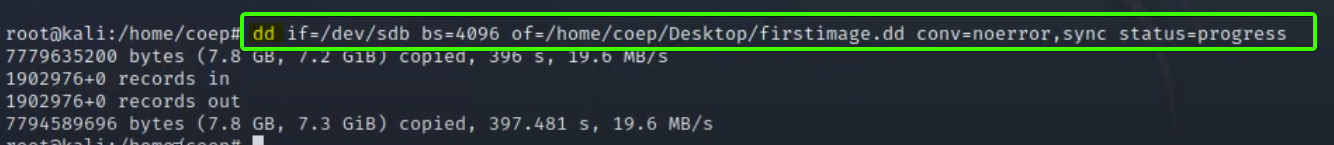


status=progress -> to show the progress of imaging.

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!

**Screenshot**

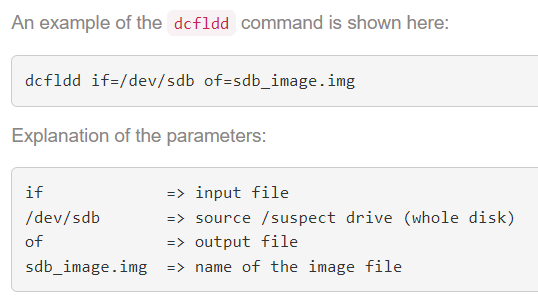


C.) dcfldd Command

Dcfldd -> Defense Computer Forensics Laboratory (DCFL) “dd”

“dcfldd” offers the following options:

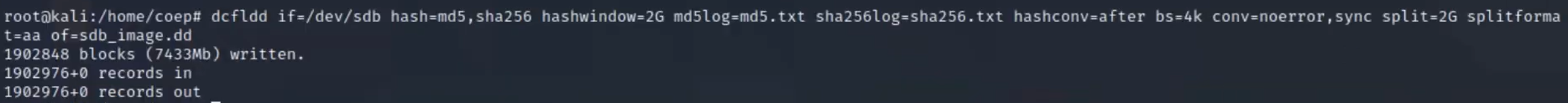
* Log errors to an output file for analysis and review
* Various hashing options MD5, SHA-1, SHA-256, etc
* Indicating the acquisition progress
* Split image file into segmented volumes
* Verify acquired data with the original source



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.

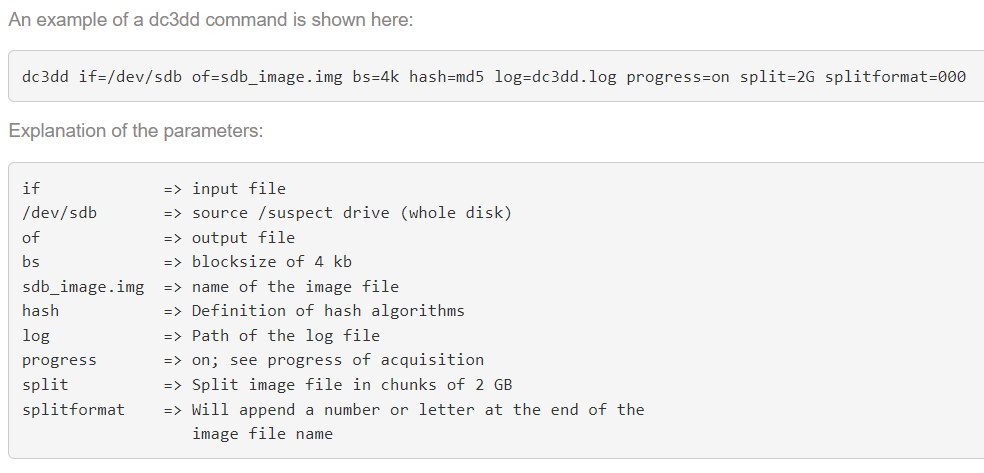
**Screenshot**



D.) dc3dd Command

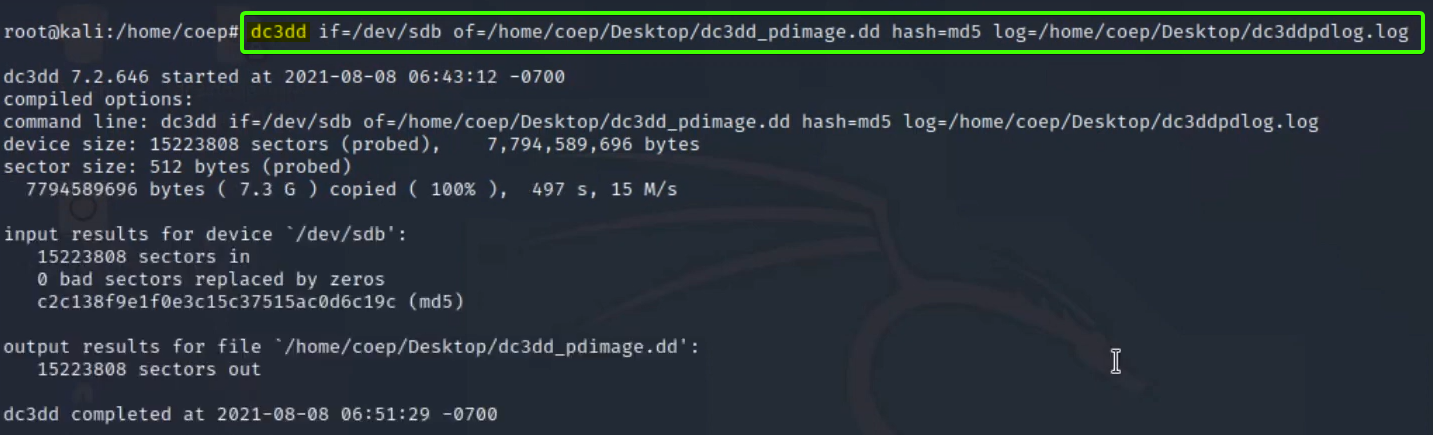
dc3dd -> DoD Cyber Crime Center dd

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



Reference Blog [Link](http://www.cyber-forensics.ch/acquiring-data-with-dd-dcfldd-dc3dd/).

**Screenshot**



• **dd**

—> already installed

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

—> sudo apt-get install dcfldd

—> fork of dd

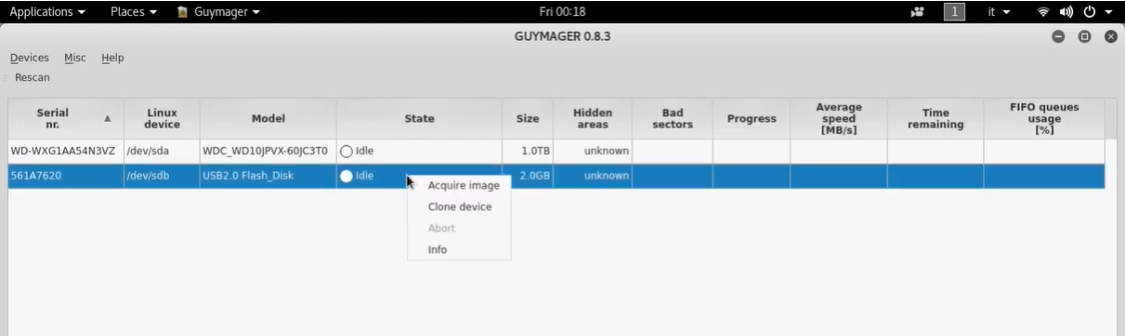
• **dc3dd** (Defense Cyber Crime Center)

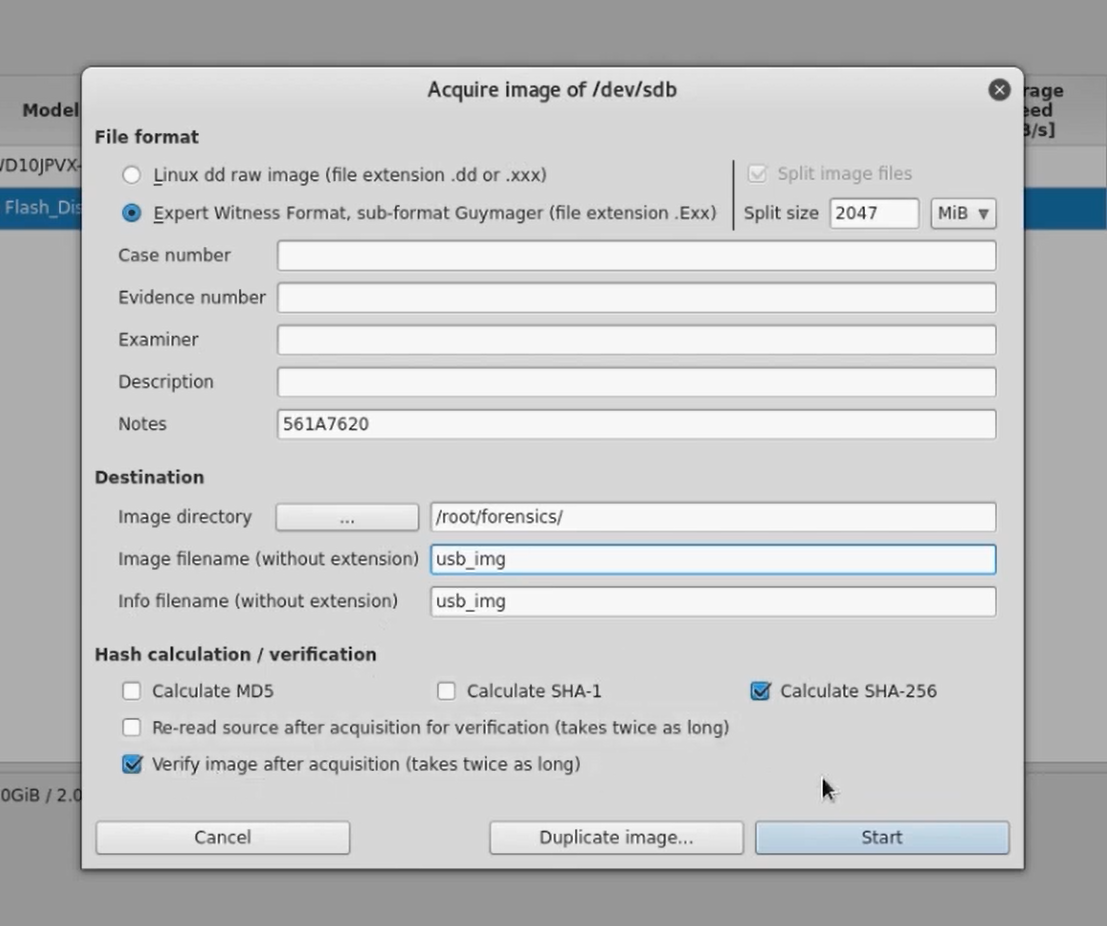
—> sudo apt-get install dc3dd

—> 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







**SUBMITTED BY**: U19CS012

BHAGYA VINOD RANA