Forensic acquisition in linux using Guymager

Muhammad Zain-ul-abideen

201002

Digital Forensics

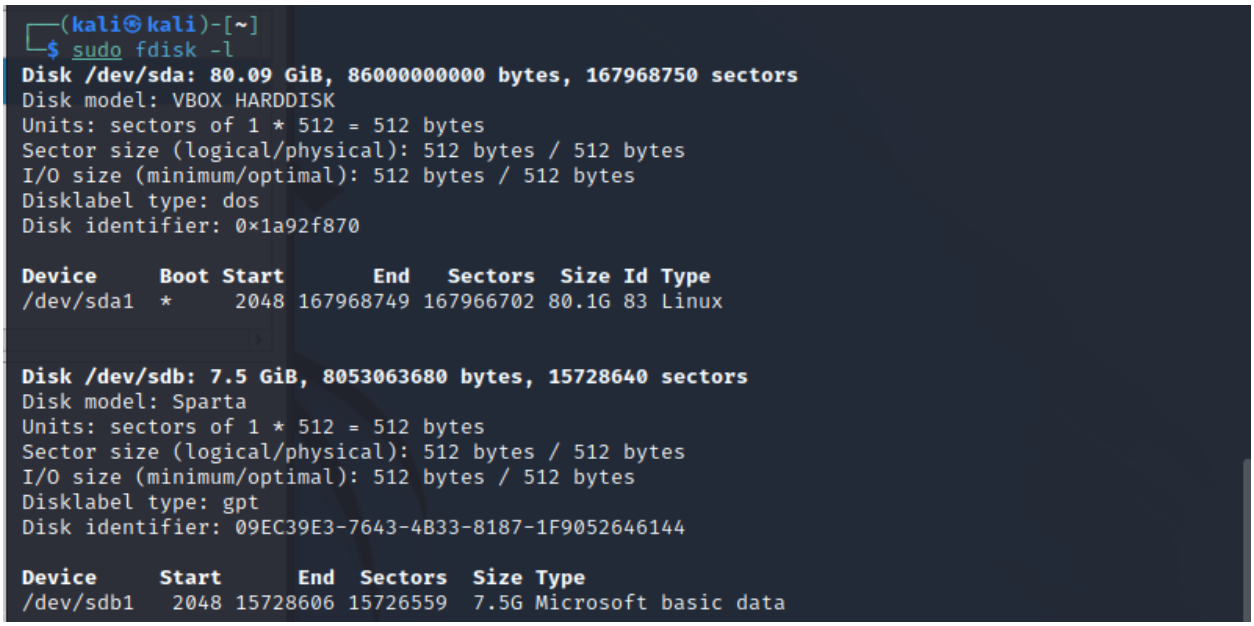
Guymager

It is a free forensic imager for media acquisition. Its main features are:

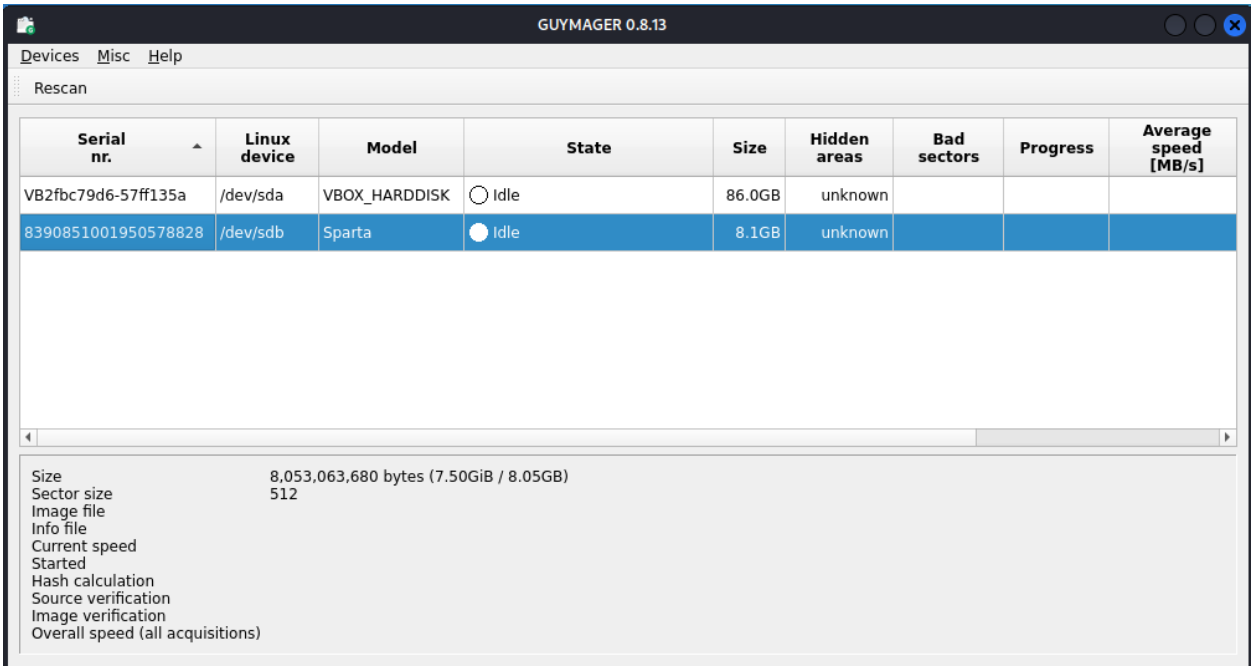
- Easy user interface in different languages
- Runs under Linux
- Really fast, due to multi-threaded, pipelined design and multi-threaded data compression
- Makes full usage of multi-processor machines
- Generates flat (dd), EWF (E01) and AFF images, supports disk cloning
- Free of charges, completely open source

Explanations:

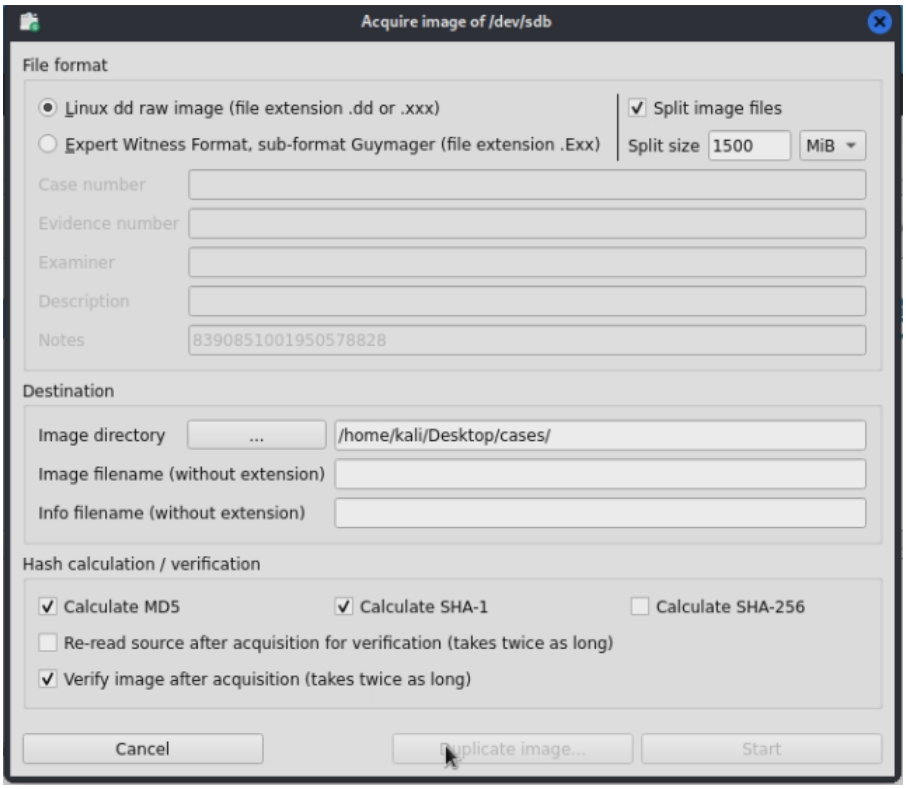
- The connected storage devices are listed in the upper part. New devices can be connected at any time - press the rescan button for displaying them.
- The devices marked with light red color are local hard disks. They cannot be acquired, thus preventing from acquiring the wrong disks. Local hard disks are recognised by their serial numbers which can be entered in the configuration file.
- The lower part shows more detailed info about the acquisition currently selected by the blue cursor.



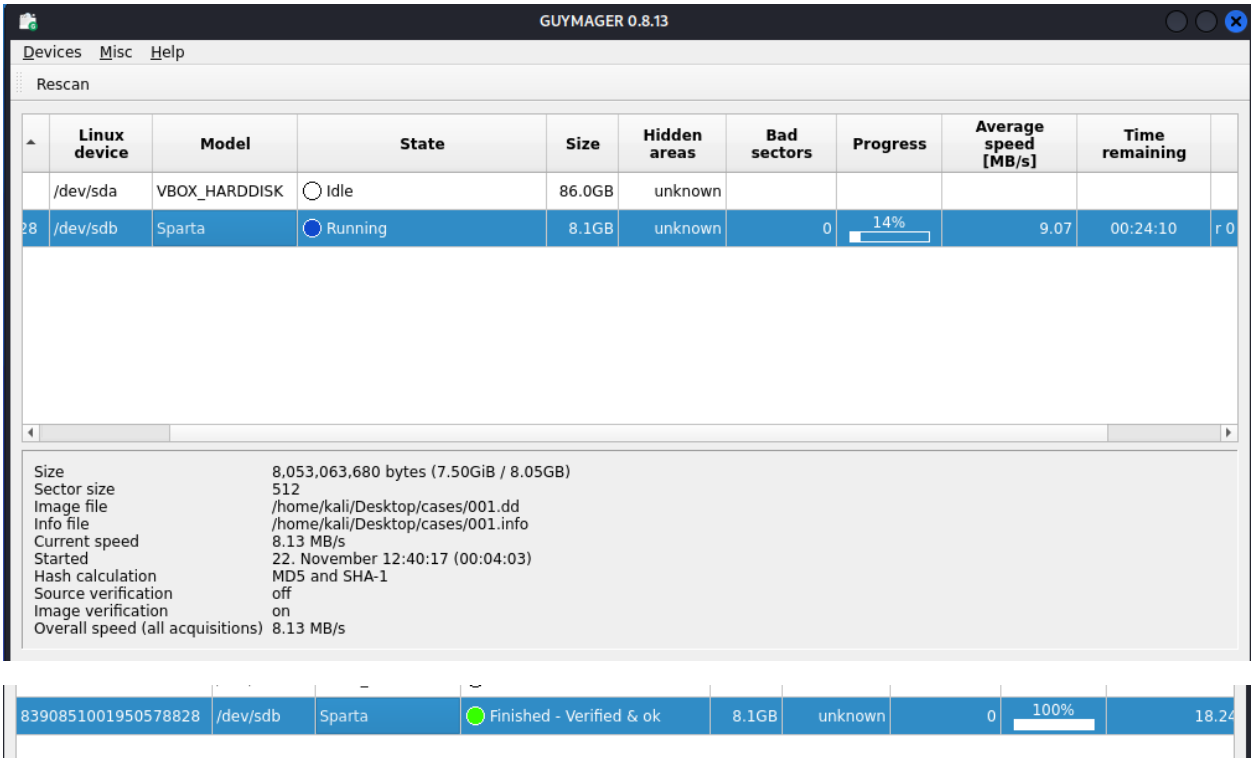
Check if the USB is connected. Here I have taken a 32GB USB drive and partitioned it into two smaller parts. Click on acquire image option.



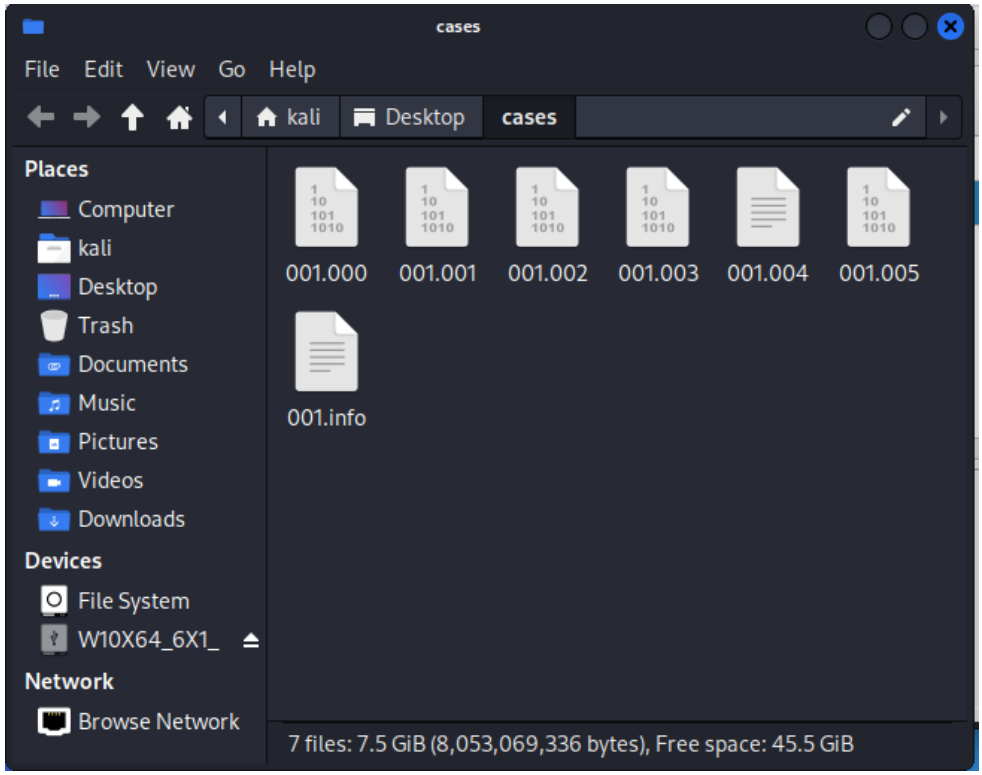
Choose the following options for image acquisition. Split into 1500MB image files and calculate both MD5 and SHA1 hashes for verification.



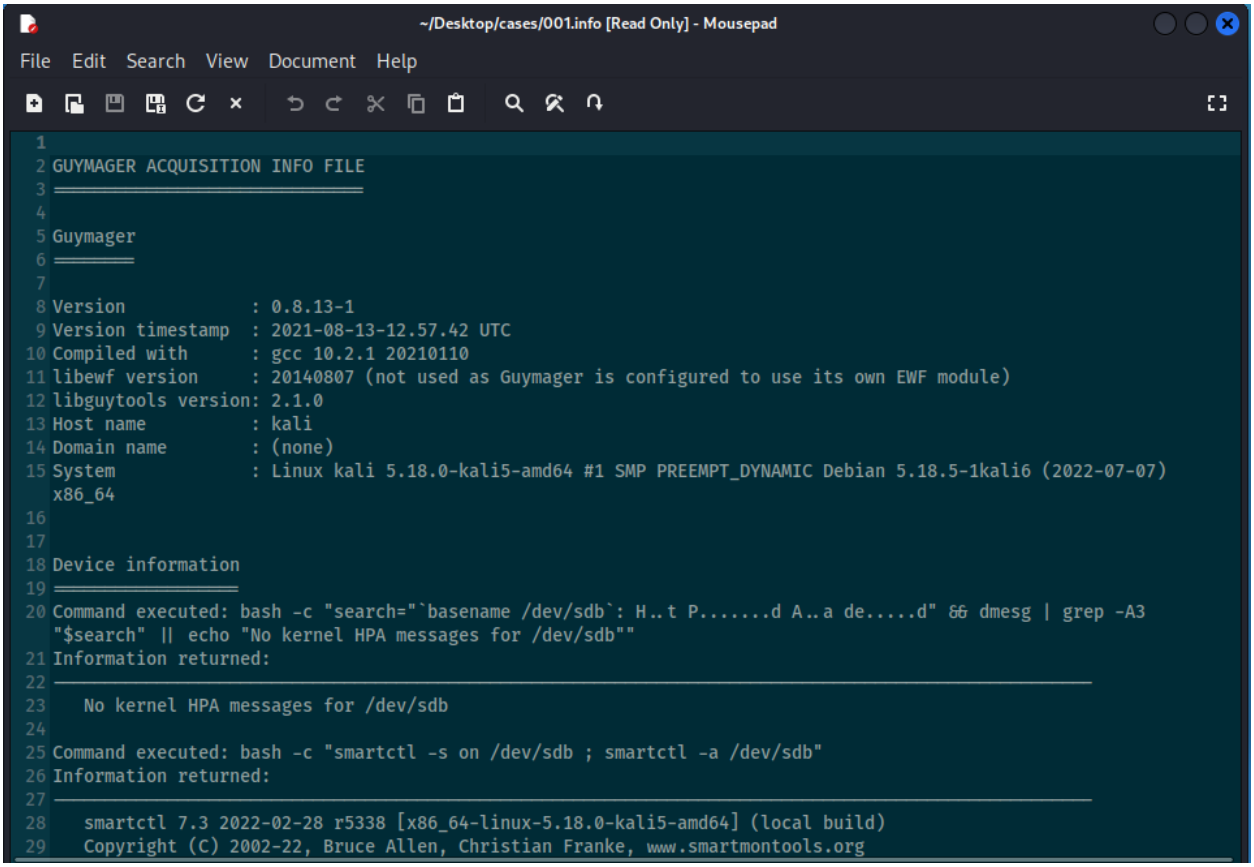
It will take some time for image acquisition and then added time for image verification.



Opening the folder where the image files are saved, we get this:



001.info file contains information about the acquisition done.



Compare MD5 and SHA1 hashes with the hashes of images.