

# 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.

```
(kali@kali)-[~]
$ sudo fdisk -l
Disk /dev/sda: 80.09 GiB, 86000000000 bytes, 167968750 sectors
Disk model: VBox HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x1a92f870

Device Boot Start End Sectors Size Id Type
/dev/sda1 * 2048 167968749 167966702 80.1G 83 Linux

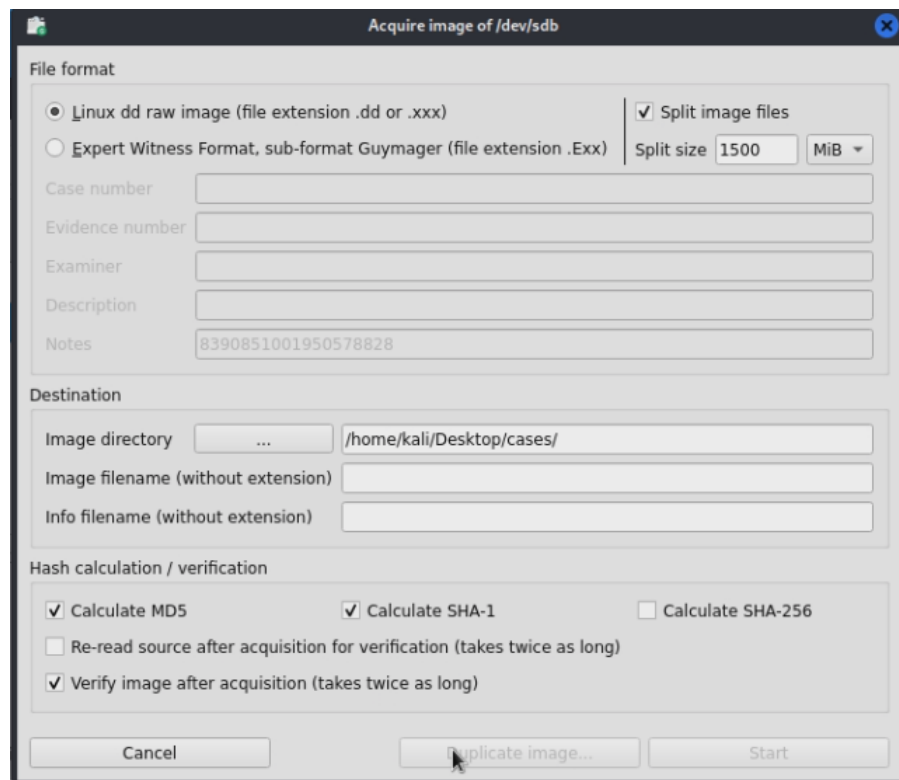
Disk /dev/sdb: 7.5 GiB, 8053063680 bytes, 15728640 sectors
Disk model: Sparta
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 09EC39E3-7643-4B33-8187-1F9052646144

Device Start End Sectors Size Type
/dev/sdb1 2048 15728606 15726559 7.5G Microsoft basic data
```

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.

The screenshot shows the GUYMAGER 0.8.13 application window. The 'Devices' tab is active, displaying a table of detected devices. The device /dev/sdb (Sparta) is currently in a 'Running' state, with 14% progress shown. Below the table, detailed acquisition statistics are provided. At the bottom, a progress bar indicates that the acquisition of /dev/sdb is now 'Finished - Verified & ok' at 100%.

Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]	Time remaining
/dev/sda	VBOX_HARDDISK	Idle	86.0GB	unknown				
/dev/sdb	Sparta	Running	8.1GB	unknown	0	14%	9.07	00:24:10

Size: 8,053,063,680 bytes (7.50GiB / 8.05GB)  
Sector size: 512  
Image file: /home/kali/Desktop/cases/001.dd  
Info file: /home/kali/Desktop/cases/001.info  
Current speed: 8.13 MB/s  
Started: 22. November 12:40:17 (00:04:03)  
Hash calculation: MD5 and SHA-1  
Source verification: off  
Image verification: on  
Overall speed (all acquisitions): 8.13 MB/s

ID	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Time remaining
8390851001950578828	/dev/sdb	Sparta	Finished - Verified & ok	8.1GB	unknown	0	100%	18.24

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

The screenshot shows a file manager window titled 'cases'. The left sidebar displays a tree view of the file system, with 'kali' and 'Desktop' selected. The main pane shows the contents of the 'cases' folder, which includes six image files (001.000 to 001.005) and one information file (001.info). The status bar at the bottom indicates that there are 7 files totaling 7.5 GiB, with 45.5 GiB of free space available.

File Edit View Go Help

← → ↑ ↓ Home kali Desktop cases

Places

- Computer
- kali
- Desktop
- Trash
- Documents
- Music
- Pictures
- Videos
- Downloads

Devices

- File System
- W10X64\_6X1\_

Network

- Browse Network

001.000 001.001 001.002 001.003 001.004 001.005

001.info

7 files: 7.5 GiB (8,053,069,336 bytes), Free space: 45.5 GiB

001.info file contains information about the acquisition done.

```
~/Desktop/cases/001.info [Read Only] - Mousepad
File Edit Search View Document Help
1
2 GUYMAGER ACQUISITION INFO FILE
3
4
5 Guymager
6
7
8 Version      : 0.8.13-1
9 Version timestamp : 2021-08-13-12.57.42 UTC
10 Compiled with  : gcc 10.2.1 20210110
11 libewf version  : 20140807 (not used as Guymager is configured to use its own EWF module)
12 libguytools version: 2.1.0
13 Host name      : kali
14 Domain name    : (none)
15 System         : Linux kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07)
16 x86_64
17
18 Device information
19
20 Command executed: bash -c "search=`basename /dev/sdb`: H..t P.....d A..a de.....d" && dmesg | grep -A3
"$search" || echo "No kernel HPA messages for /dev/sdb"
21 Information returned:
22
23 No kernel HPA messages for /dev/sdb
24
25 Command executed: bash -c "smartctl -s on /dev/sdb ; smartctl -a /dev/sdb"
26 Information returned:
27
28 smartctl 7.3 2022-02-28 r5338 [x86_64-linux-5.18.0-kali5-amd64] (local build)
29 Copyright (C) 2002-22, Bruce Allen, Christian Franke, www.smartmontools.org
```

Compare MD5 and SHA1 hashes with the hashes of images.

```
MD5 hash      : 6e11b6a478cdabeedd2aac1538ae0868
MD5 hash verified source : --
MD5 hash verified image  : 6e11b6a478cdabeedd2aac1538ae0868
SHA1 hash     : 5a0f9fa4a84ae6c83f87731e490b84254d00c1f1
SHA1 hash verified source : --
SHA1 hash verified image  : 5a0f9fa4a84ae6c83f87731e490b84254d00c1f1
SHA256 hash   : --
SHA256 hash verified source: --
SHA256 hash verified image : --
Image verification OK. The image contains exactly the data that was written.
```