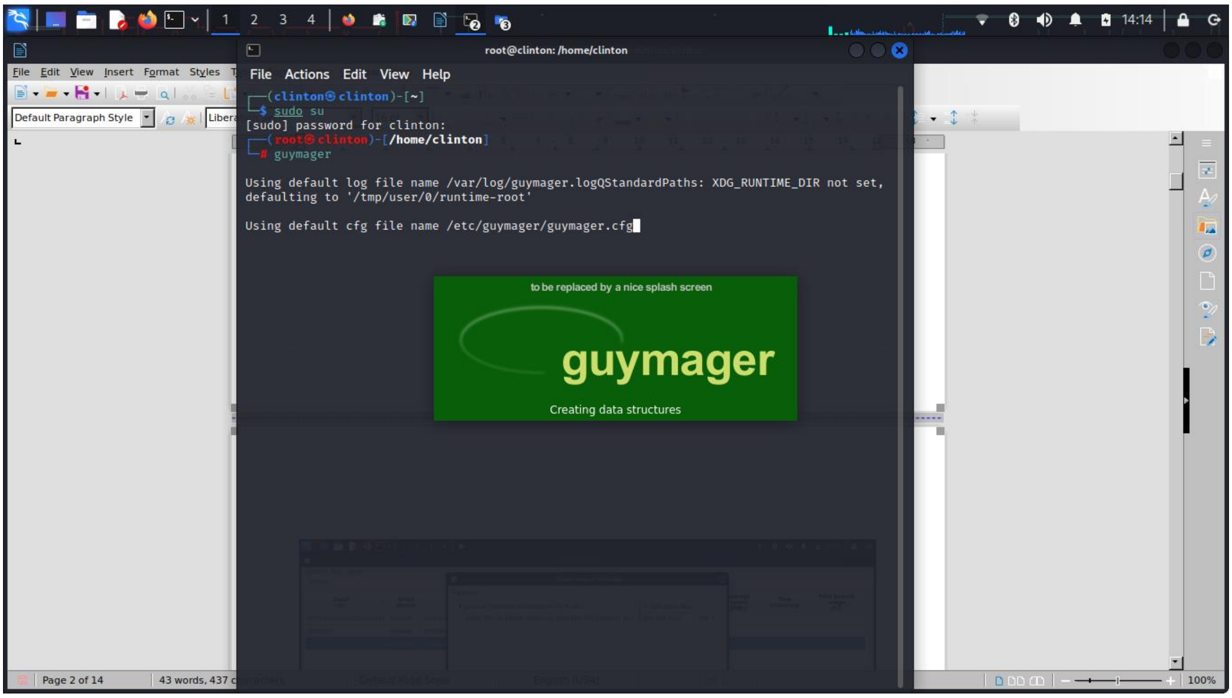
1} GUYMAGER

Guymager is a forensic disk imaging tool used primarily for creating a bit-for-bit copy of storage devices such as hard drives, USB drives, and other digital storage media. It's popular in the field of digital forensics for its simplicity and reliability when handling data preservation tasks.

In the following project I will provide step by step on how to use the tool for forensics investigations.

i) Steps for Using Guymager:

: Ensure that the software is installed on a forensic workstation running a supported operating system (usually Linux). Start by typing guymager on the terminal.

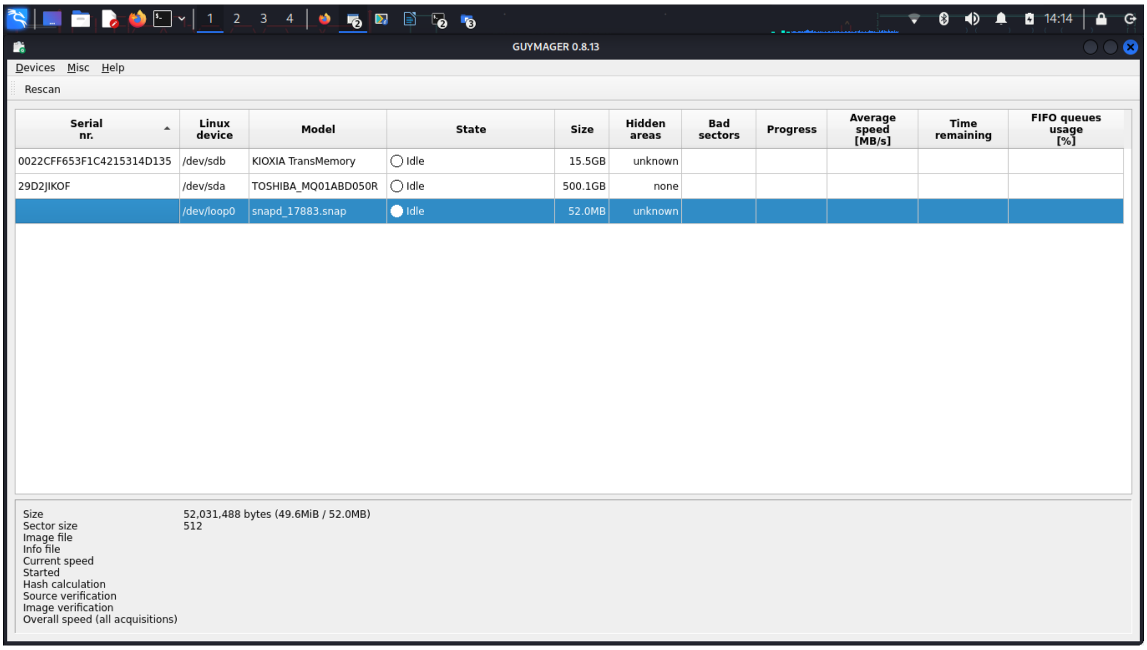


```
┌──(clinton㉿clinton)-[~]
└─$ sudo su
[sudo] password for clinton:
┌──(root㉿clinton)-[/home/clinton]
└─# guymager

Using default log file name /var/log/guymager.logQStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/user/0/runtime-root'

Using default cfg file name /etc/guymager/guymager.cfg
```

root@clinton: /home/clinton
File Actions Edit View Help
to be replaced by a nice splash screen
guymager
Creating data structures
14:14
Default Paragraph Style
Page 2 of 14
43 words, 437
100%

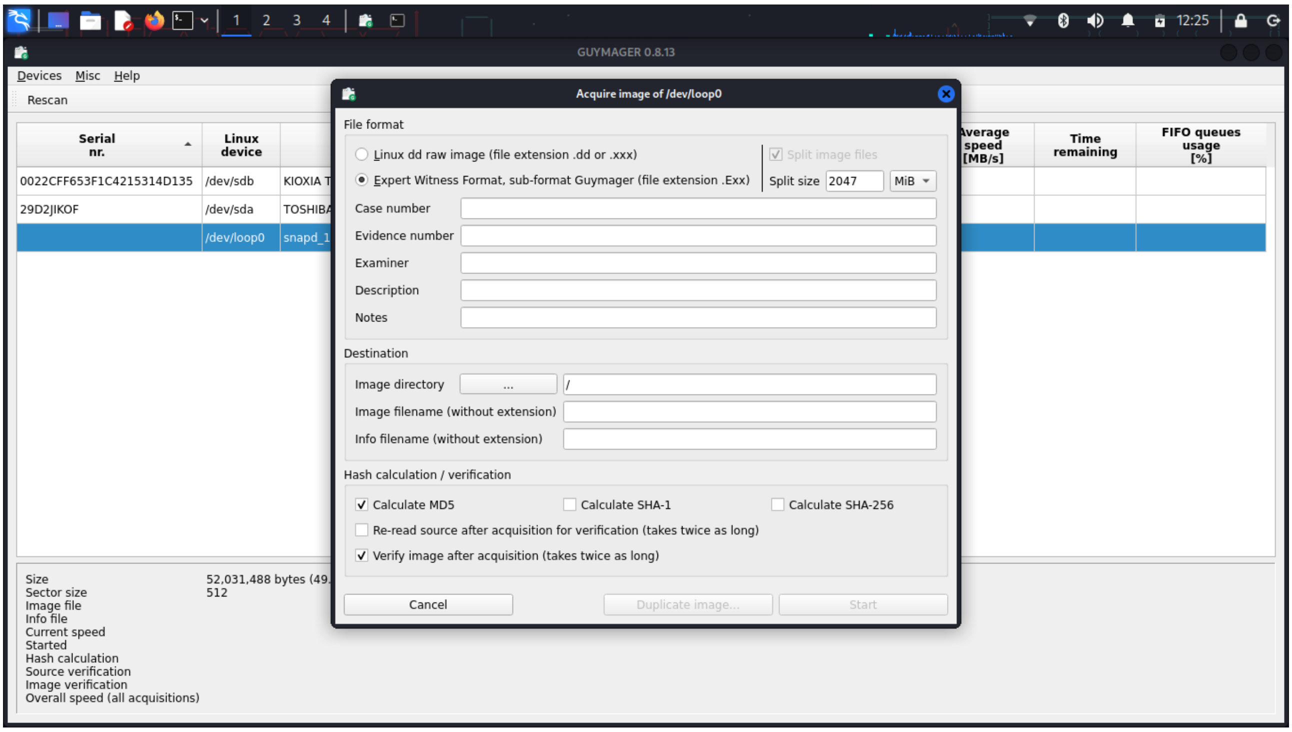
Select the Source Disk: After launching Guymager, you would select the physical disk or partition that you wish to create an image of.

Choose the Output Format: Decide on the format for the image (e.g., E01, raw, etc.).



Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]	Time remaining	FIFO queues usage [%]
0022CFF653F1C4215314D135	/dev/sdb	KIOXIA TransMemory	○ Idle	15.5GB	unknown					
29D2JIKOF	/dev/sda	TOSHIBA_MQ01ABD050R	○ Idle	500.1GB	none					
	/dev/loop0	snapd_17883.snap	● Idle	52.0MB	unknown					

Size	52,031,488 bytes (49.6MiB / 52.0MB)
Sector size	512
Image file	
Info file	
Current speed	
Started	
Hash calculation	
Source verification	
Image verification	
Overall speed (all acquisitions)	



Serial nr.	Linux device		Average speed [MB/s]	Time remaining	FIFO queues usage [%]
0022CFF653F1C4215314D135	/dev/sdb	KIOXIA T			
29D2JIKOF	/dev/sda	TOSHIBA			
	/dev/loop0	snapd_1			

Size	52,031,488 bytes (49.
Sector size	512
Image file	
Info file	
Current speed	
Started	
Hash calculation	
Source verification	
Image verification	
Overall speed (all acquisitions)	

Acquire image of /dev/loop0

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

Destination

Image directory ... /

Image filename (without extension)

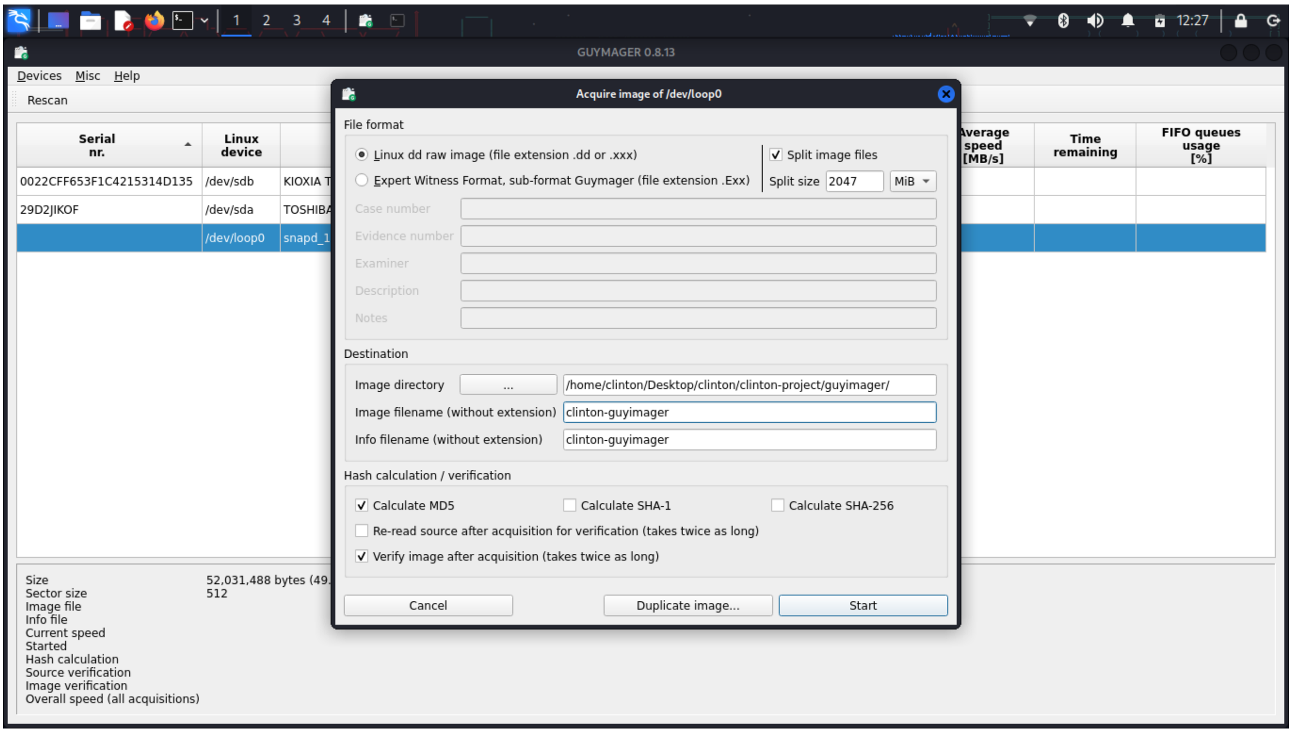
Info filename (without extension)

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) choose the destination of the image and begin Imaging: Start the imaging process. Guymager will create a bit-for-bit copy of the selected disk.



Serial nr.	Linux device		Average speed [MB/s]	Time remaining	FIFO queues usage [%]
0022CFF653F1C4215314D135	/dev/sdb	KIOXIA T			
29D2JIKOF	/dev/sda	TOSHIBA			
	/dev/loop0	snapd_1			

Size 52,031,488 bytes (49.
Sector size 512
Image file
Info file
Current speed
Started
Hash calculation
Source verification
Image verification
Overall speed (all acquisitions)

Acquire image of /dev/loop0

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

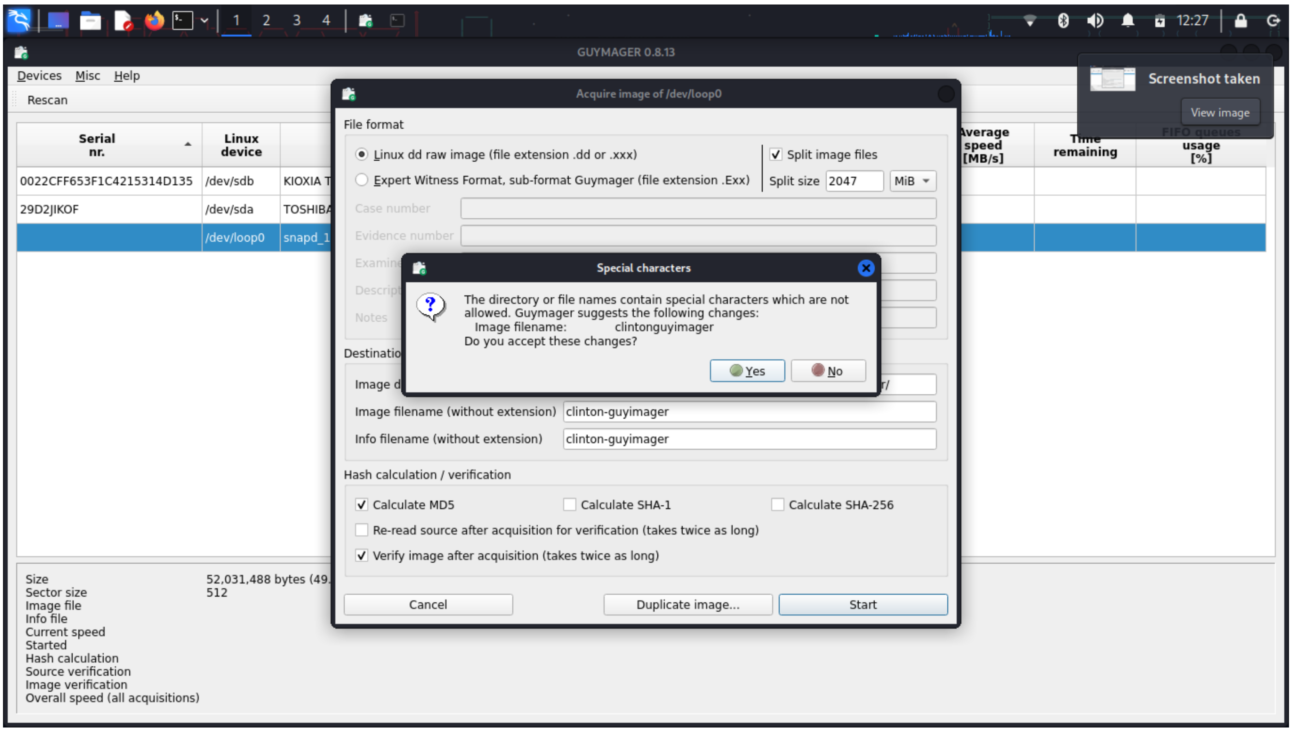
Destination

Image directory ... /home/clinton/Desktop/clinton/clinton-project/guyimager/
Image filename (without extension) clinton-guyimager
Info filename (without extension) clinton-guyimager

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)

Verify the Image: After the image is created, use the built-in verification tool to check for data integrity.



GUYMAGER 0.8.13

Acquire image of /dev/loop0

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

Special characters

The directory or file names contain special characters which are not allowed. Guymager suggests the following changes:
Image filename: clintonguyimager
Do you accept these changes?

Yes No

Image filename (without extension) clinton-guyimager

Info filename (without extension) clinton-guyimager

Hash calculation / verification

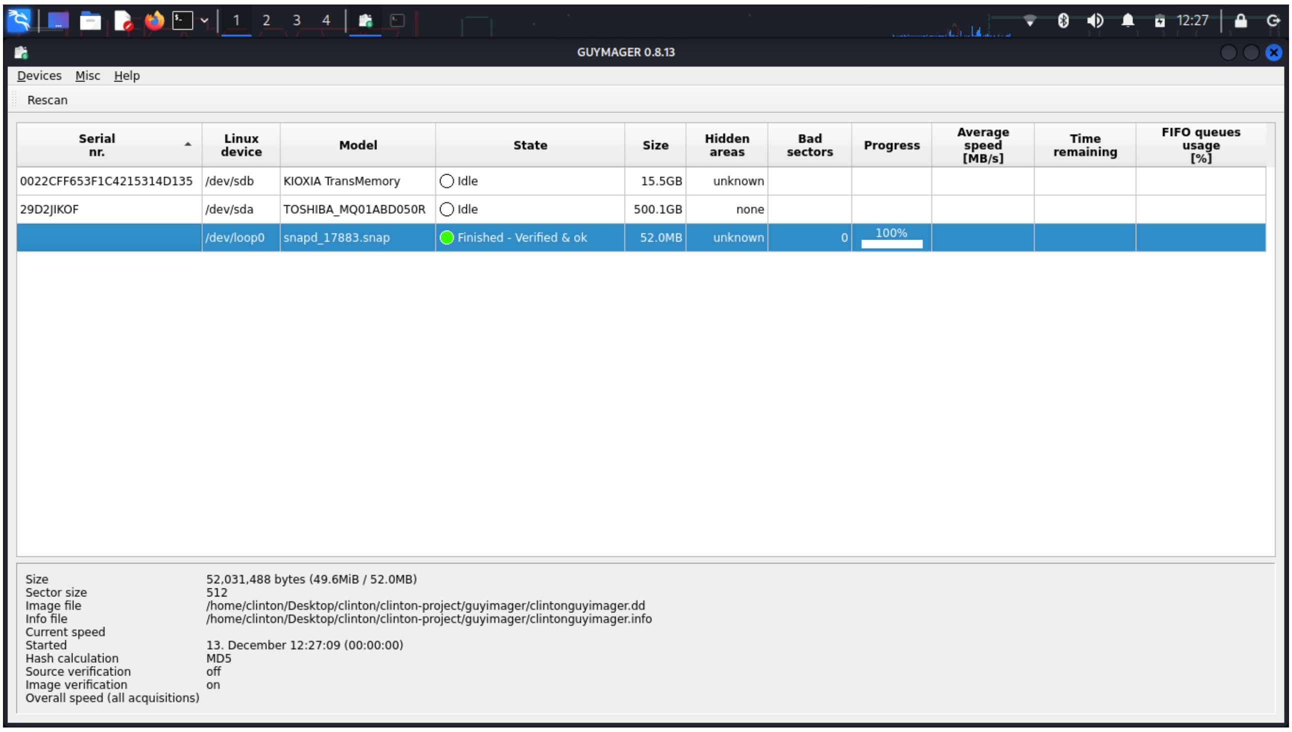
☑ Calculate MD5 □ Calculate SHA-1 □ Calculate SHA-256

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

☑ Verify image after acquisition (takes twice as long)

Cancel Duplicate image... Start

```
Size                            52,031,488 bytes (49.
Sector size                     512
Image file
Info file
Current speed
Started
Hash calculation
Source verification
Image verification
Overall speed (all acquisitions)
```

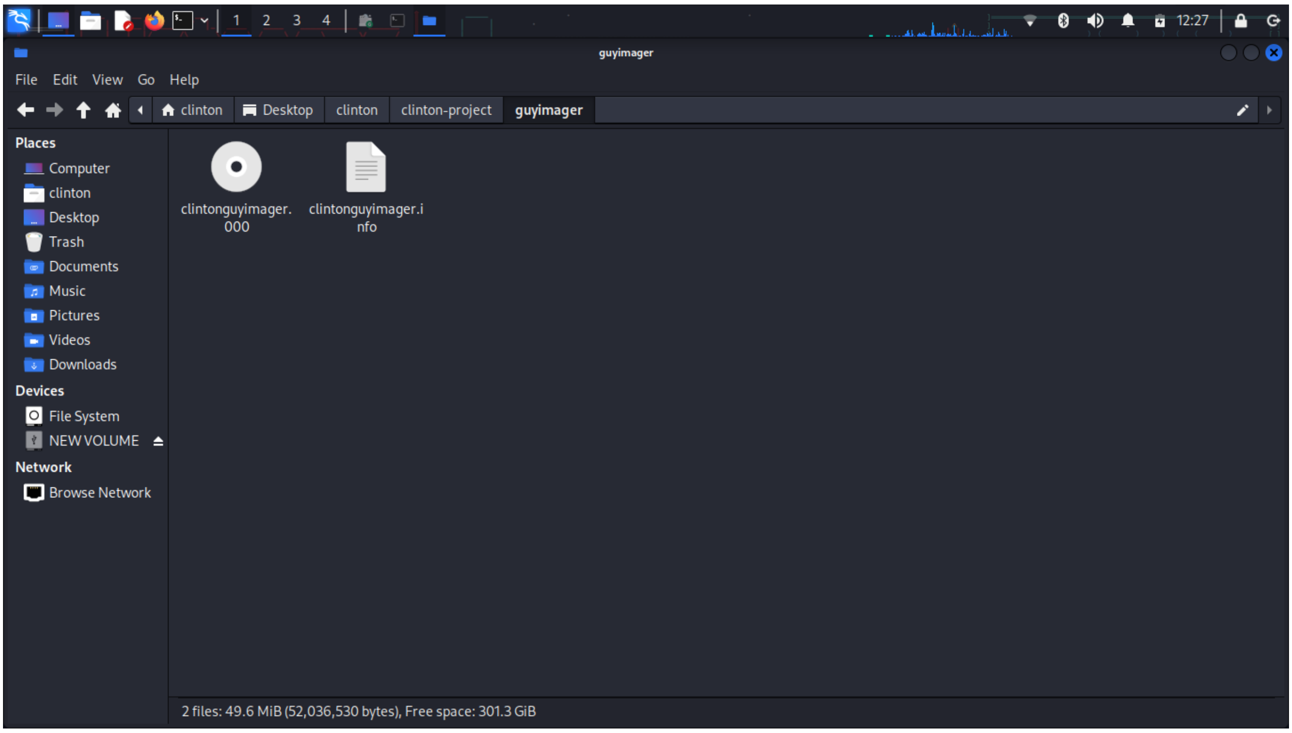


GUYMAGER 0.8.13

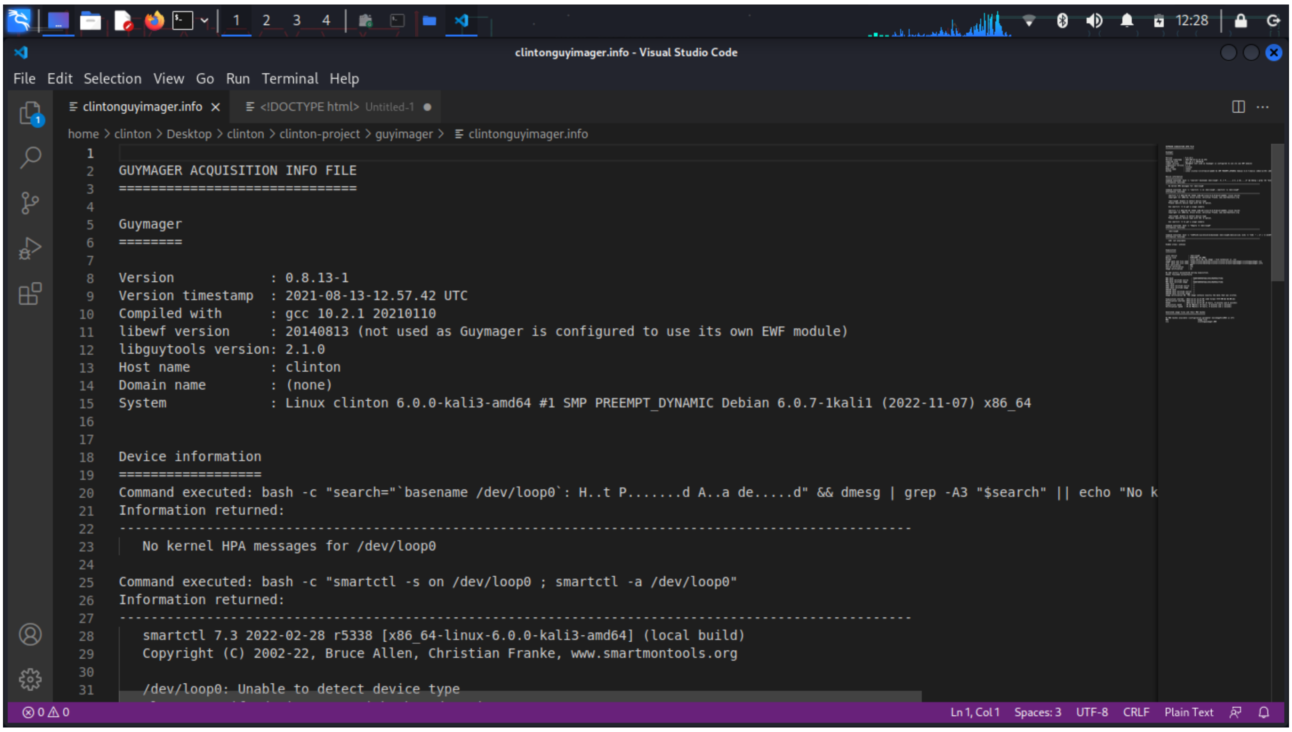
Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Average speed [MB/s]	Time remaining	FIFO queues usage [%]
0022CFF653F1C4215314D135	/dev/sdb	KIOXIA TransMemory	○ Idle	15.5GB	unknown					
29D2JIKOF	/dev/sda	TOSHIBA_MQ01ABD050R	○ Idle	500.1GB	none					
	/dev/loop0	snapd_17883.snap	● Finished - Verified & ok	52.0MB	unknown	0	100%			

```
Size                            52,031,488 bytes (49.6MiB / 52.0MB)
Sector size                     512
Image file                      /home/clinton/Desktop/clinton/clinton-project/guyimager/clintonguyimager.dd
Info file                       /home/clinton/Desktop/clinton/clinton-project/guyimager/clintonguyimager.info
Current speed
Started                         13. December 12:27:09 (00:00:00)
Hash calculation                MD5
Source verification             off
Image verification              on
Overall speed (all acquisitions)
```

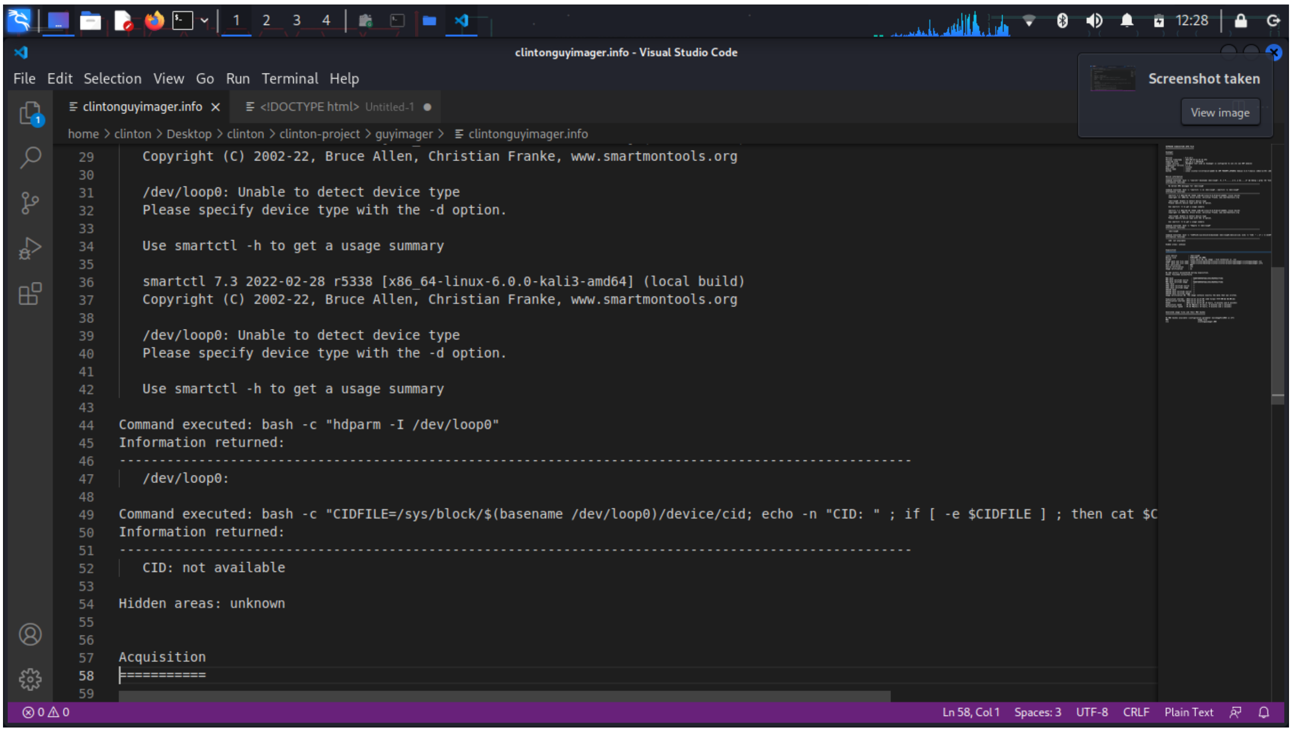
Navigate to the destination of the file that you chose and view the image.



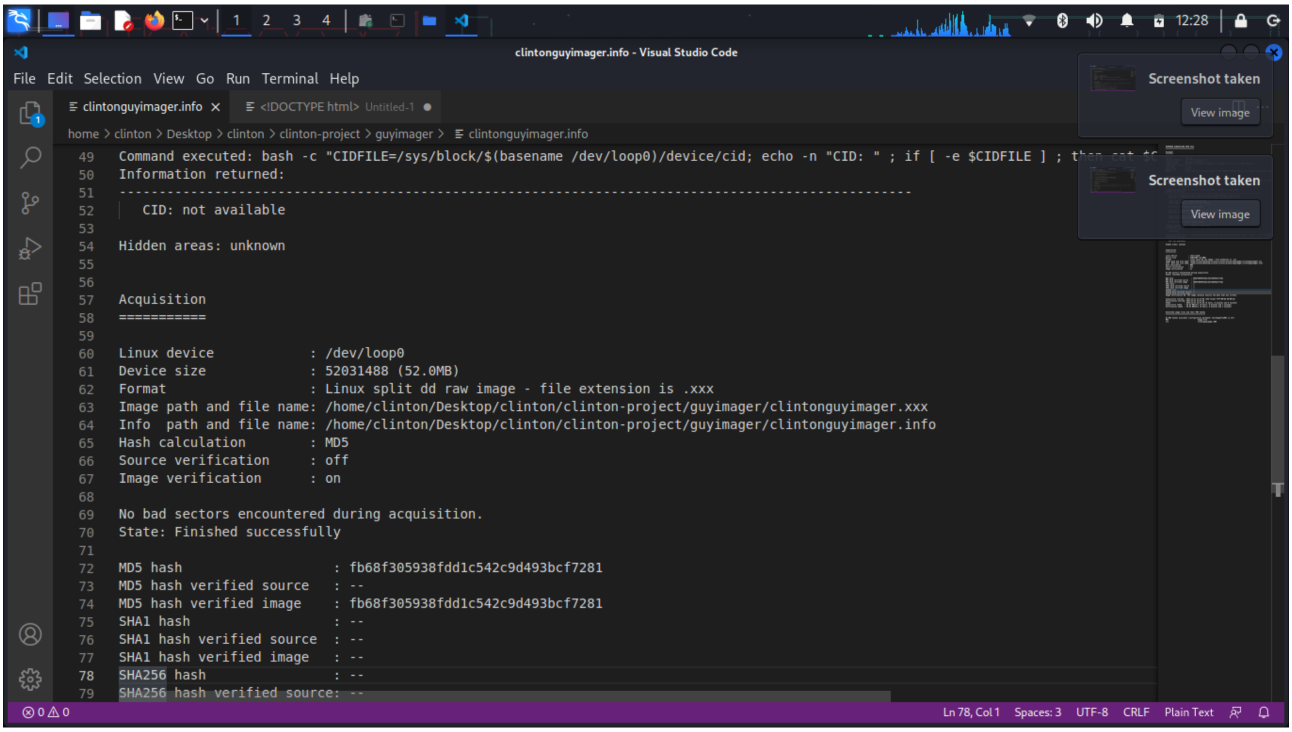
2 files: 49.6 MiB (52,036,530 bytes), Free space: 301.3 GiB


clintonguyimager.info - Visual Studio Code
File
Edit
Selection
View
Go
Run
Terminal
Help
clintonguyimager.info
<!DOCTYPE html> Untitled-1
home > clinton > Desktop > clinton > clinton-project > guyimager > clintonguyimager.info
Ln 1, Col 1
Spaces: 3
UTF-8
CRLF
Plain Text
12:28

```

GUYMAGER ACQUISITION INFO FILE
==============================

Guymager
========

Version              : 0.8.13-1
Version timestamp    : 2021-08-13-12.57.42 UTC
Compiled with        : gcc 10.2.1 20210110
libewf version       : 20140813 (not used as Guymager is configured to use its own EWF module)
libguytools version: 2.1.0
Host name            : clinton
Domain name          : (none)
System               : Linux clinton 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) x86_64


Device information
==================
Command executed: bash -c "search="`basename /dev/loop0`: H..t P.......d A..a de.....d" && dmesg | grep -A3 "$search" || echo "No k
Information returned:
----------------------------------------------------------------------------------------------------
   No kernel HPA messages for /dev/loop0

Command executed: bash -c "smartctl -s on /dev/loop0 ; smartctl -a /dev/loop0"
Information returned:
----------------------------------------------------------------------------------------------------
   smartctl 7.3 2022-02-28 r5338 [x86_64-linux-6.0.0-kali3-amd64] (local build)
   Copyright (C) 2002-22, Bruce Allen, Christian Franke, www.smartmontools.org

   /dev/loop0: Unable to detect device type
```


clintonguyimager.info - Visual Studio Code
File Edit Selection View Go Run Terminal Help
clintonguyimager.info
<!DOCTYPE html> Untitled-1
home > clinton > Desktop > clinton > clinton-project > guyimager > clintonguyimager.info
Screenshot taken
View image
12:28
Ln 58, Col 1 Spaces: 3 UTF-8 CRLF Plain Text

```
    Copyright (C) 2002-22, Bruce Allen, Christian Franke, www.smartmontools.org

    /dev/loop0: Unable to detect device type
    Please specify device type with the -d option.

    Use smartctl -h to get a usage summary

    smartctl 7.3 2022-02-28 r5338 [x86_64-linux-6.0.0-kali3-amd64] (local build)
    Copyright (C) 2002-22, Bruce Allen, Christian Franke, www.smartmontools.org

    /dev/loop0: Unable to detect device type
    Please specify device type with the -d option.

    Use smartctl -h to get a usage summary

Command executed: bash -c "hdparm -I /dev/loop0"
Information returned:
----------------------------------------------------------------------------------------------------
   /dev/loop0:

Command executed: bash -c "CIDFILE=/sys/block/$(basename /dev/loop0)/device/cid; echo -n "CID: " ; if [ -e $CIDFILE ] ; then cat $C
Information returned:
----------------------------------------------------------------------------------------------------
   CID: not available

Hidden areas: unknown


Acquisition
===========
```


clintonguyimager.info - Visual Studio Code
File Edit Selection View Go Run Terminal Help
clintonguyimager.info
<!DOCTYPE html> Untitled-1
home > clinton > Desktop > clinton > clinton-project > guyimager > clintonguyimager.info
Screenshot taken
View image
Screenshot taken
View image
12:28
Ln 78, Col 1 Spaces: 3 UTF-8 CRLF Plain Text

```
Command executed: bash -c "CIDFILE=/sys/block/$(basename /dev/loop0)/device/cid; echo -n "CID: " ; if [ -e $CIDFILE ] ; then cat $C
Information returned:
----------------------------------------------------------------------------------------------------
   CID: not available

Hidden areas: unknown


Acquisition
===========

Linux device            : /dev/loop0
Device size             : 52031488 (52.0MB)
Format                  : Linux split dd raw image - file extension is .xxx
Image path and file name: /home/clinton/Desktop/clinton/clinton-project/guyimager/clintonguyimager.xxx
Info  path and file name: /home/clinton/Desktop/clinton/clinton-project/guyimager/clintonguyimager.info
Hash calculation        : MD5
Source verification     : off
Image verification      : on

No bad sectors encountered during acquisition.
State: Finished successfully

MD5 hash                   : fb68f305938fdd1c542c9d493bcf7281
MD5 hash verified source   : --
MD5 hash verified image    : fb68f305938fdd1c542c9d493bcf7281
SHA1 hash                  : --
SHA1 hash verified source  : --
SHA1 hash verified image   : --
SHA256 hash                : --
SHA256 hash verified source: --
```

Key Features:

Disk Imaging:

Guymager creates exact disk images (also known as forensic images) that preserve the integrity of the data for analysis. This is crucial in forensic investigations where maintaining the authenticity of the data is essential.

Multiple Formats:

It supports multiple disk image formats, including raw (dd), E01 (EnCase), and AFF (Advanced Forensic Format). These formats are widely accepted in the forensic community.

Verification:

After creating the disk image, Guymager can verify the image against the source drive to ensure that no data was lost or altered during the imaging process. This is crucial for maintaining evidence integrity in legal proceedings.

User-Friendly Interface:

Guymager has a graphical user interface (GUI), which makes it easier for forensic professionals to use compared to command-line tools. It is available for Linux and supports most file systems, including FAT, NTFS, and EXT.

Open Source:

Guymager is free and open-source, making it accessible to both professional and educational users.

Use Case in Forensics:

Data Acquisition:

When a forensic investigator is called to collect evidence from a computer or storage device, Guymager is often used to create a bit-for-bit copy of the storage medium. This allows them to examine the data without altering the original device.

Court Admissibility:

Using tools like Guymager ensures that the data collection process adheres to legal standards, helping ensure the evidence can be presented in court without challenges to its integrity.