1} GUYMAGER

- Guymager is a free, open-source forensic imaging tool it is designed for Linux systems (though it can run under other environments with proper dependencies).
- Used by digital forensic investigators to create bit-by-bit forensic images of storage devices.
- Developed with a graphical user interface (GUI), making it user-friendly compared to command-line-only tools like `dd`.

Purpose

- Acquire forensically sound images of hard drives, SSDs, USB flash drives, memory cards, etc.
- Ensure integrity with hashing (MD5, SHA-1, SHA-256).
- Provide documentation and logging of the acquisition process.
- Support investigators in incident response, forensic analysis, and evidence preservation.

Key Features

Imaging

- Creates bitstream images (exact sector-by-sector copies).
- Supports multiple image formats:
    - E01 (EnCase format) – industry standard, supports metadata and compression.
    - dd/raw – simple bit-by-bit copy without compression.
    - AFF (Advanced Forensic Format) – supports compression and metadata.
- Can split images into segments for easier storage/transfer.

Hashing & Verification

- Calculates MD5, SHA-1, SHA-256 checksums during acquisition.
- Verifies hash of source and image to ensure data integrity.
- Generates detailed acquisition logs.

Performance

- Very fast imaging due to multi-threading.
- Supports on-the-fly compression for image files.
- Efficient handling of damaged sectors (can skip or retry).

User Interface

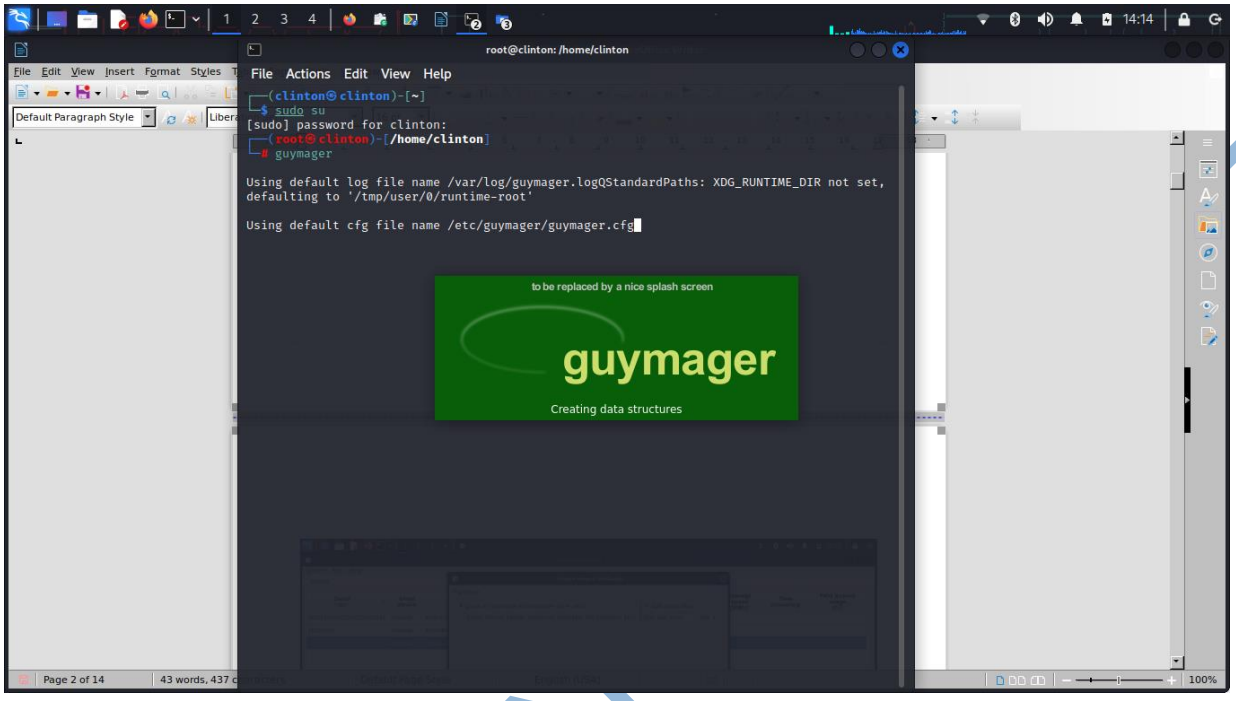
- Graphical interface makes it easy to use.
- Displays connected storage devices with details:
    - Model

- Serial number
- Size
- Sector count

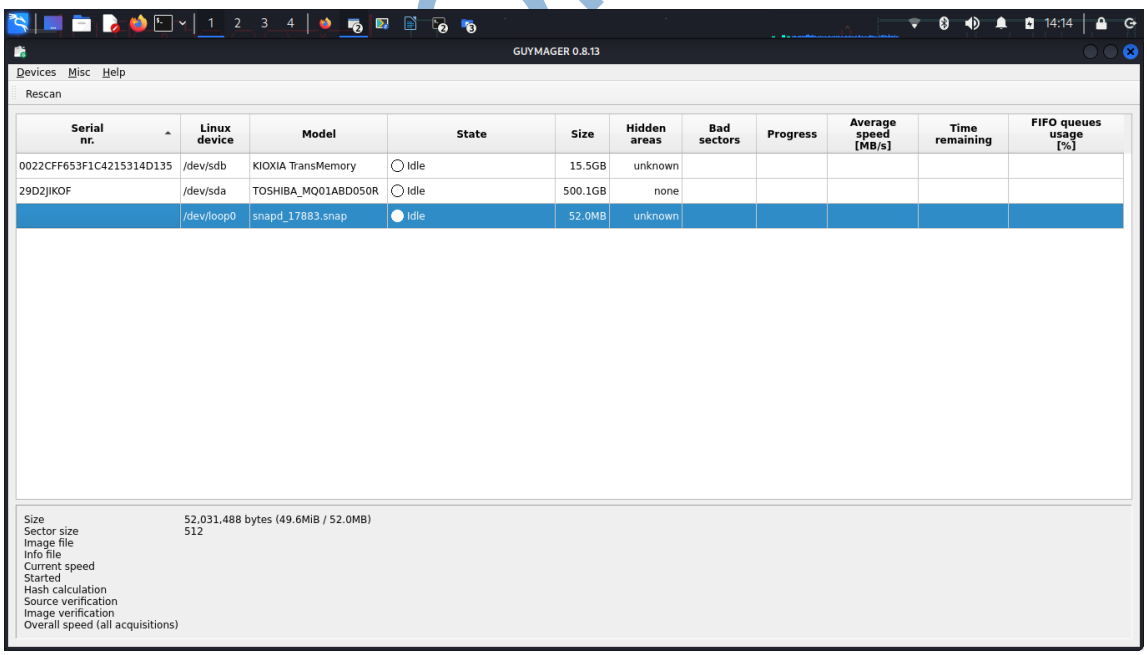
- Allows easy selection of destination folder, format, and hash options.

Workflow

i)START

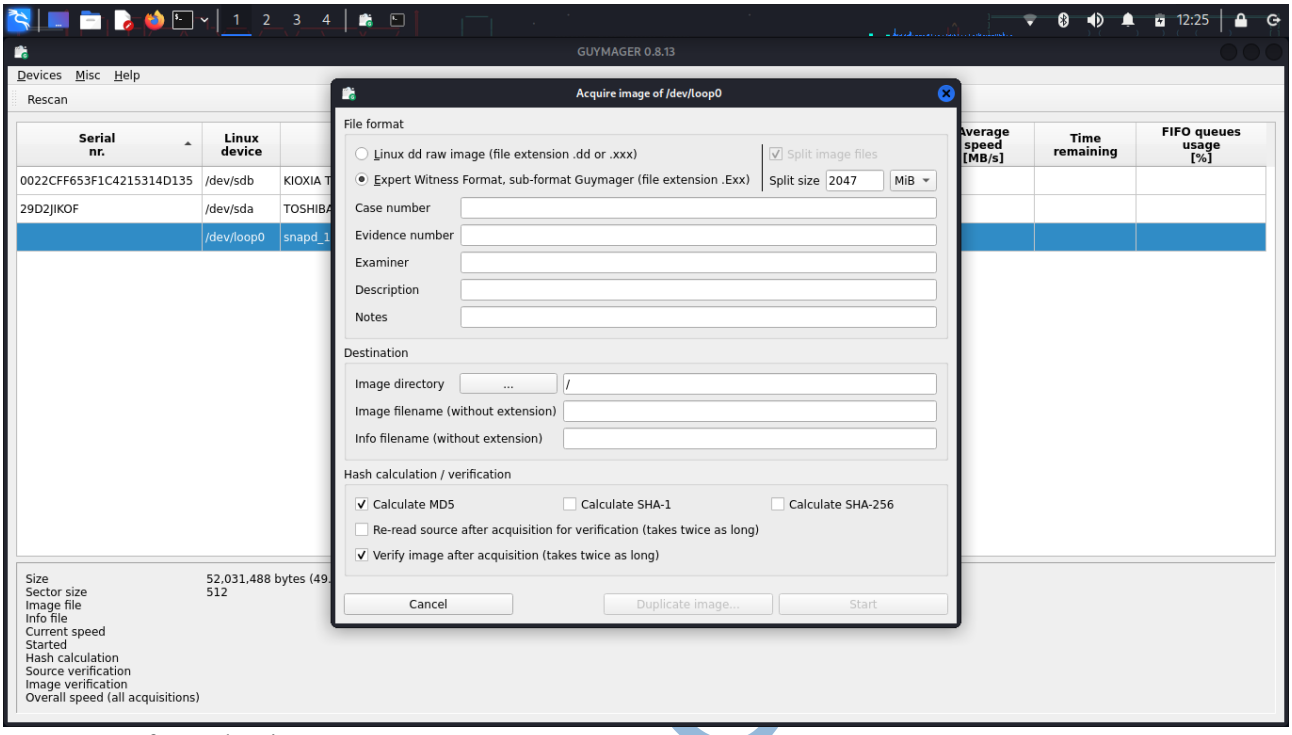


Shows the main interface when Guymager is launched.



• It shows all connected storage devices (e.g., hard disks, USB drives) are displayed with details such as size, model, and serial number. Investigators can select which device to acquire an image from.

- In order to provides a read-only view to avoid tampering with original evidence.

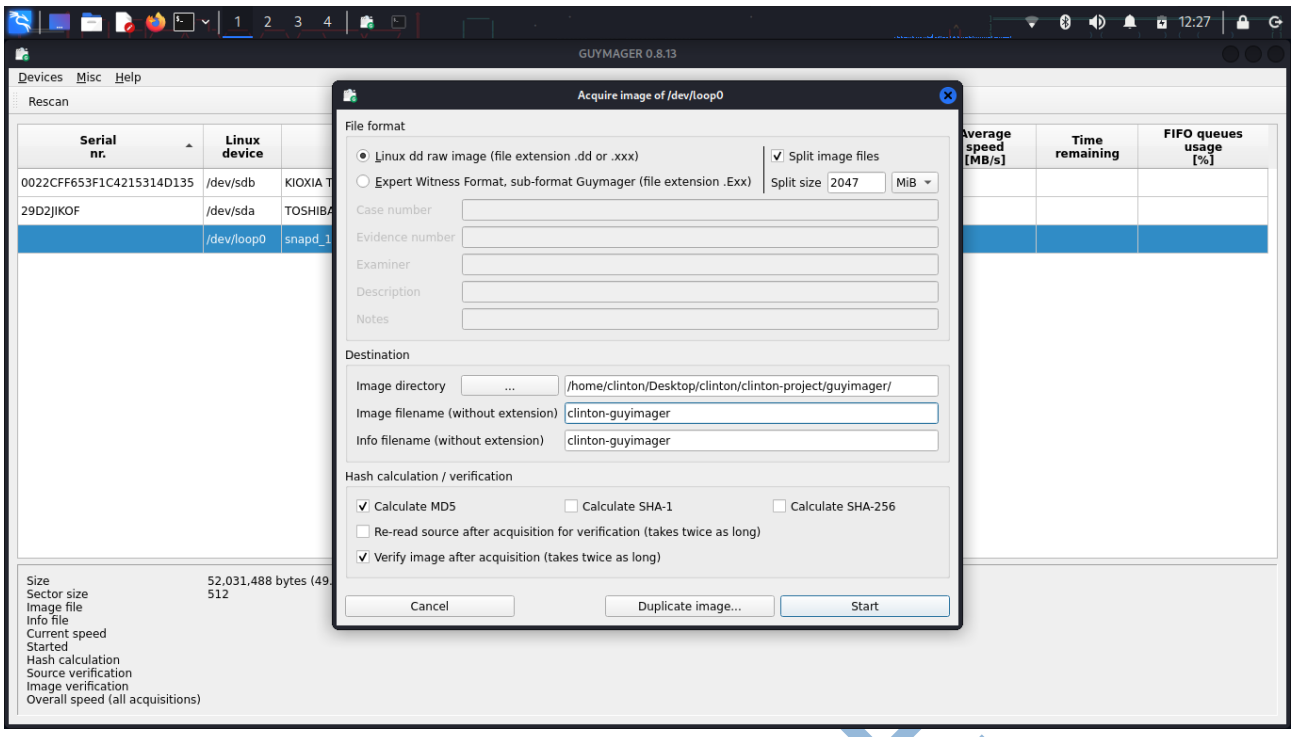


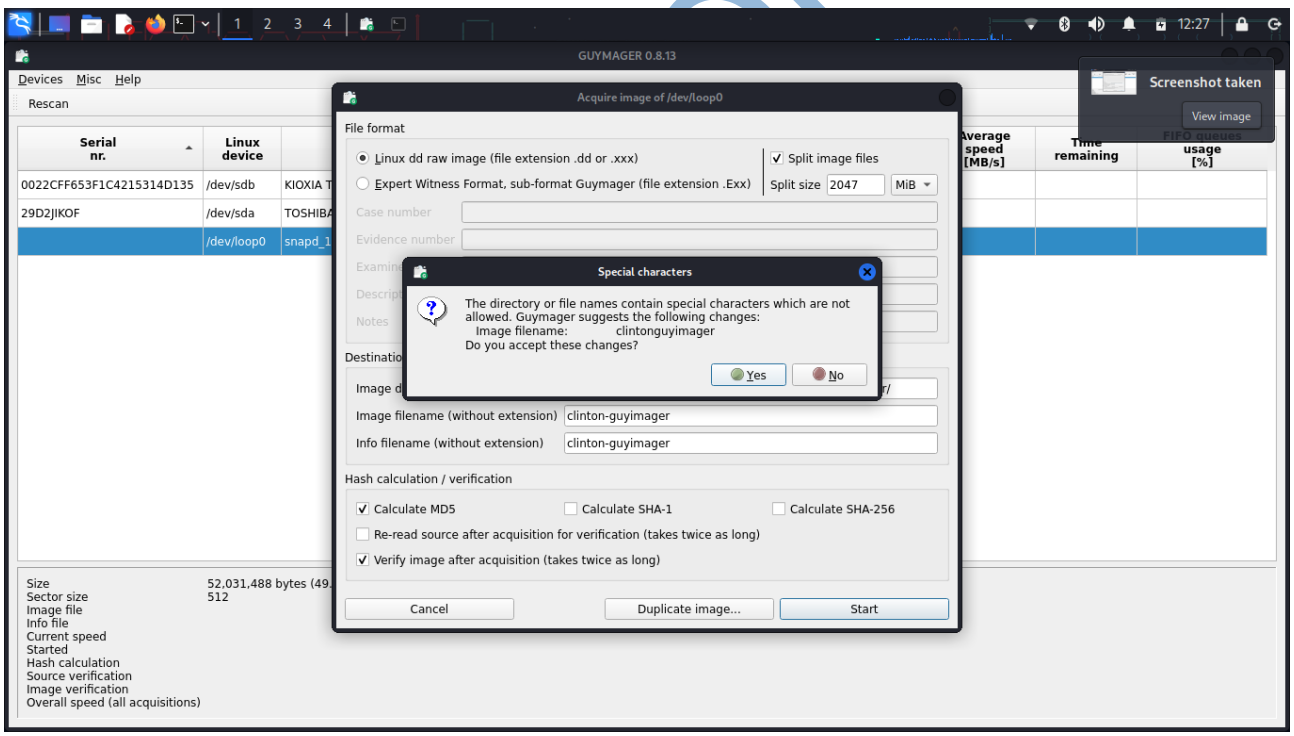
Appears after selecting *"Acquire Image"*.

Shows fields to enter details such as:

- Case number, examiner name, evidence number.
- Destination path for storing the forensic image.
- Choice of image format (e.g., E01, AFF, RAW).

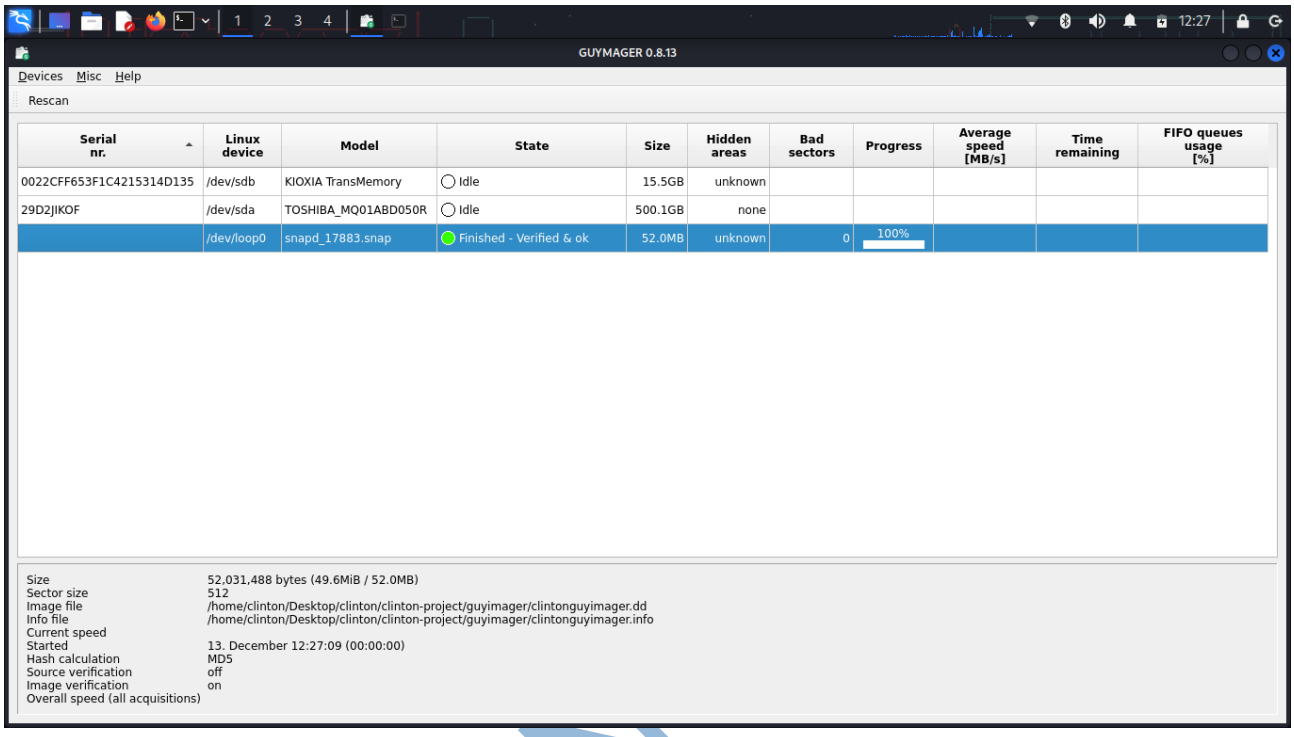
This ensures proper documentation and chain of custody during imaging.

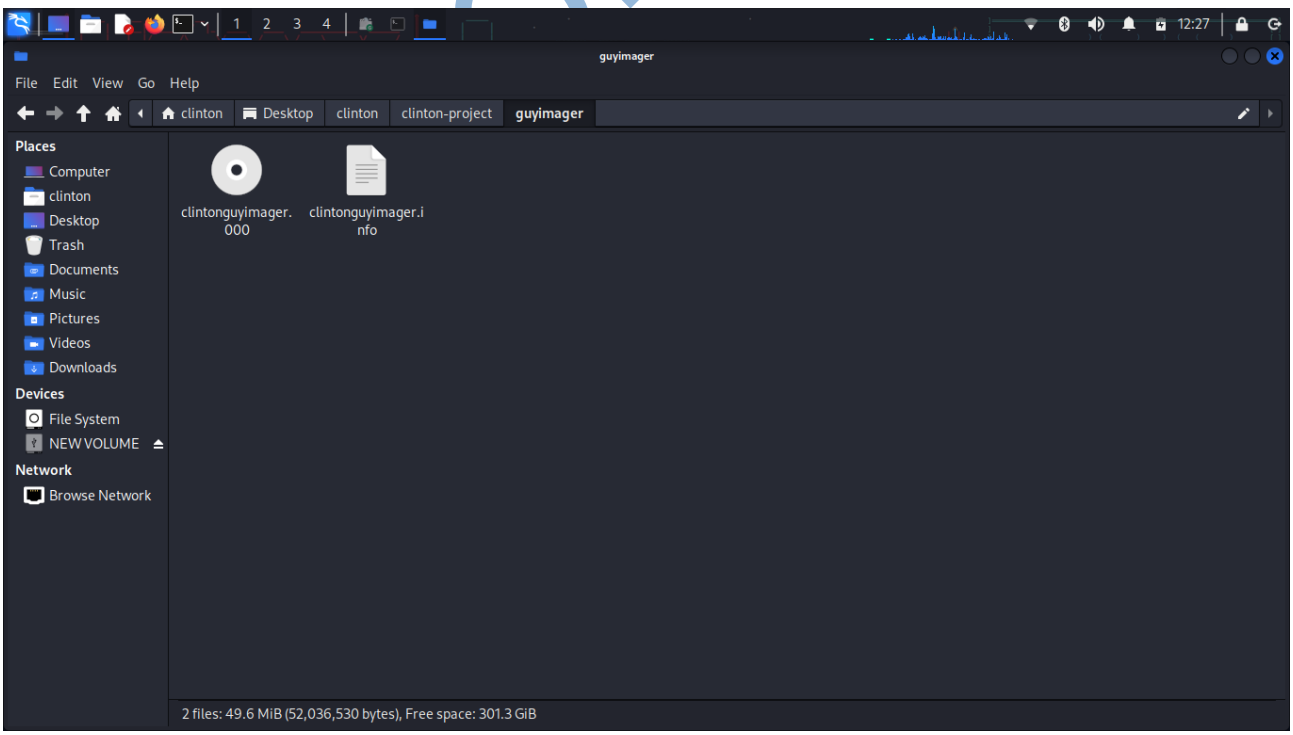

GUYMAGER 0.8.13
Devices Misc Help
Rescan
Serial nr.
Linux device
0022CFF653F1C4215314D135 /dev/sdb
29D2JIKOF /dev/sda
/dev/loop0
Average speed [MB/s]
Time remaining
FIFO queues usage [%]
Acquire image of /dev/loop0
File format
Linux dd raw image (file extension .dd or .xxx)
Expert Witness Format, sub-format 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)
Cancel
Duplicate image...
Start
Size
Sector size
Image file
Info file
Current speed
Started
Hash calculation
Source verification
Image verification
Overall speed (all acquisitions)


GUYMAGER 0.8.13
Screenshot taken
View image
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
Cancel
Duplicate image...
Start

Imaging in Progress

- Shows real-time statistics like:
    - Data copied, estimated time remaining, and transfer speed.
    - Hash calculation (e.g., MD5, SHA1) for integrity verification.
- This confirms that the evidence is being copied without alteration.





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

```
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
```

Ln 1, Col 1 Spaces: 3 UTF-8 CRLF Plain Text

clintonguyimager.info - Visual Studio Code

File Edit Selection View Go Run Terminal Help

Screenshot taken

View image

clintonguyimager.info | <!DOCTYPE html> Untitled-1

home > clinton > Desktop > clinton > clinton-project > guyimager > clintonguyimager.info

```
   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
===========
```

Ln 58, Col 1 Spaces: 3 UTF-8 CRLF Plain Text

clintonguyimager.info - Visual Studio Code

File Edit Selection View Go Run Terminal Help

Screenshot taken

View image

Screenshot taken

View image

clintonguyimager.info | <!DOCTYPE html> Untitled-1

home > clinton > Desktop > clinton > clinton-project > guyimager > clintonguyimager.info

```
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: --
```

Ln 78, Col 1 Spaces: 3 UTF-8 CRLF Plain Text

- Shows the final report after imaging is complete.

- Includes details such as:

    - Device information (model, size, serial).
    - Hash values generated before and after imaging (ensures authenticity).
    - Log of the acquisition process.

- This provides documentation to prove the evidence image is an exact, untampered copy.