🔍 Exploring 6 Free Forensic Tools in Kali Linux

In the world of digital forensics, understanding tools conceptually is important—but knowing how to use them in real-life scenarios is what truly builds competence. This write-up isn't just a theoretical overview. Instead, it offers a hands-on walkthrough of six powerful, open-source Linux forensic tools, showing exactly how they were applied in practical forensic cases.

From acquiring disk images of USB drives to recovering deleted multimedia files, each tool covered here—Guymager, Autopsy, Foremost, dcfldd, Scalpel, and FTK Imager—was used in a real lab scenario. The document includes step-by-step use cases, storage paths, image types, and recovery results to give you a clear picture of how these tools perform in actual investigations.

Whether you're a student, forensic analyst, or cybersecurity enthusiast, this guide provides practical insights you can apply in your own forensic workflow.

Let's dive in. 🚀

1. 💻 Guymager – High-Speed GUI Forensic Imaging Tool

Guymager is a fast and efficient disk imager with a simple GUI, ideal for preserving digital evidence without altering the source.

🔹 **Key Features:**

- GUI-based, beginner-friendly interface
- Supports **raw (.dd)**, **EWF**, and **AFF** formats
- Multithreaded imaging with parallel compression
- Supports **MD5**, **SHA-1**, **SHA-256** hashing
- Detailed logging for chain-of-custody documentation

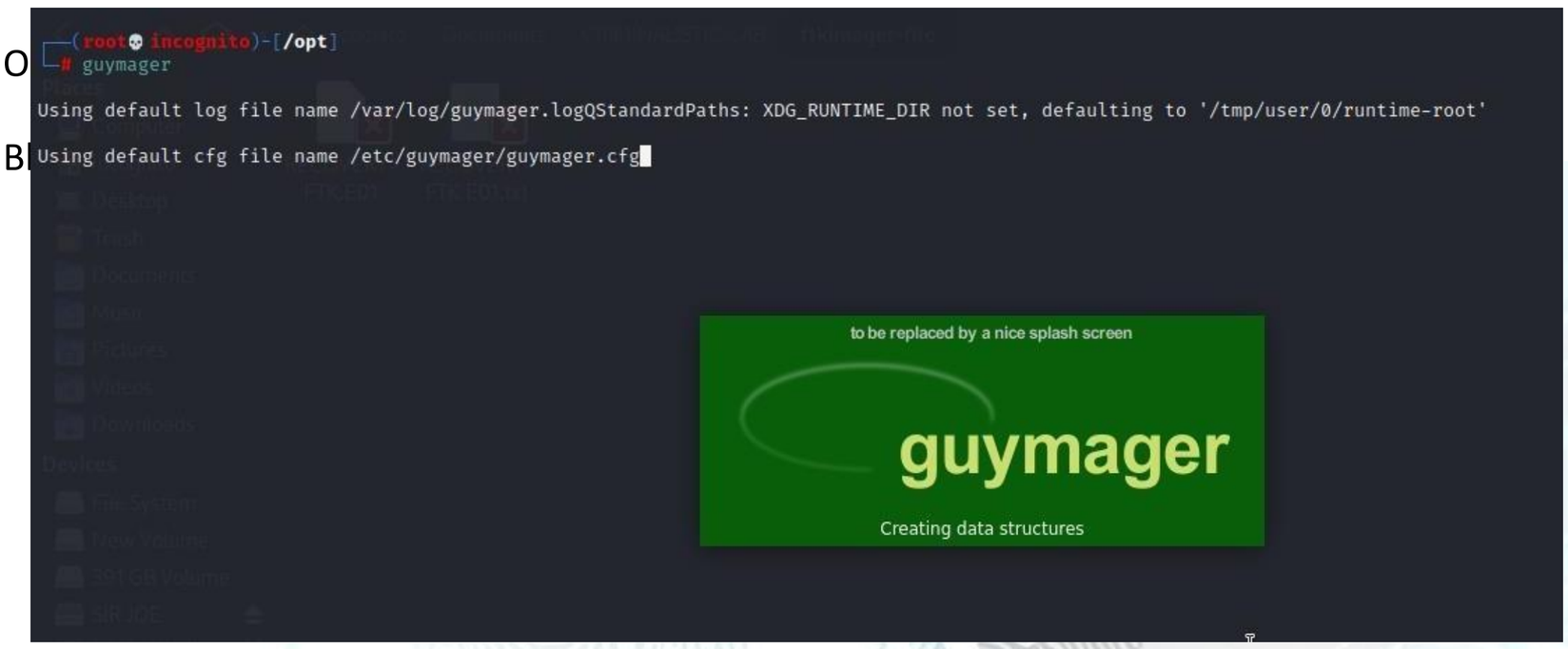
📎 More on Guymager

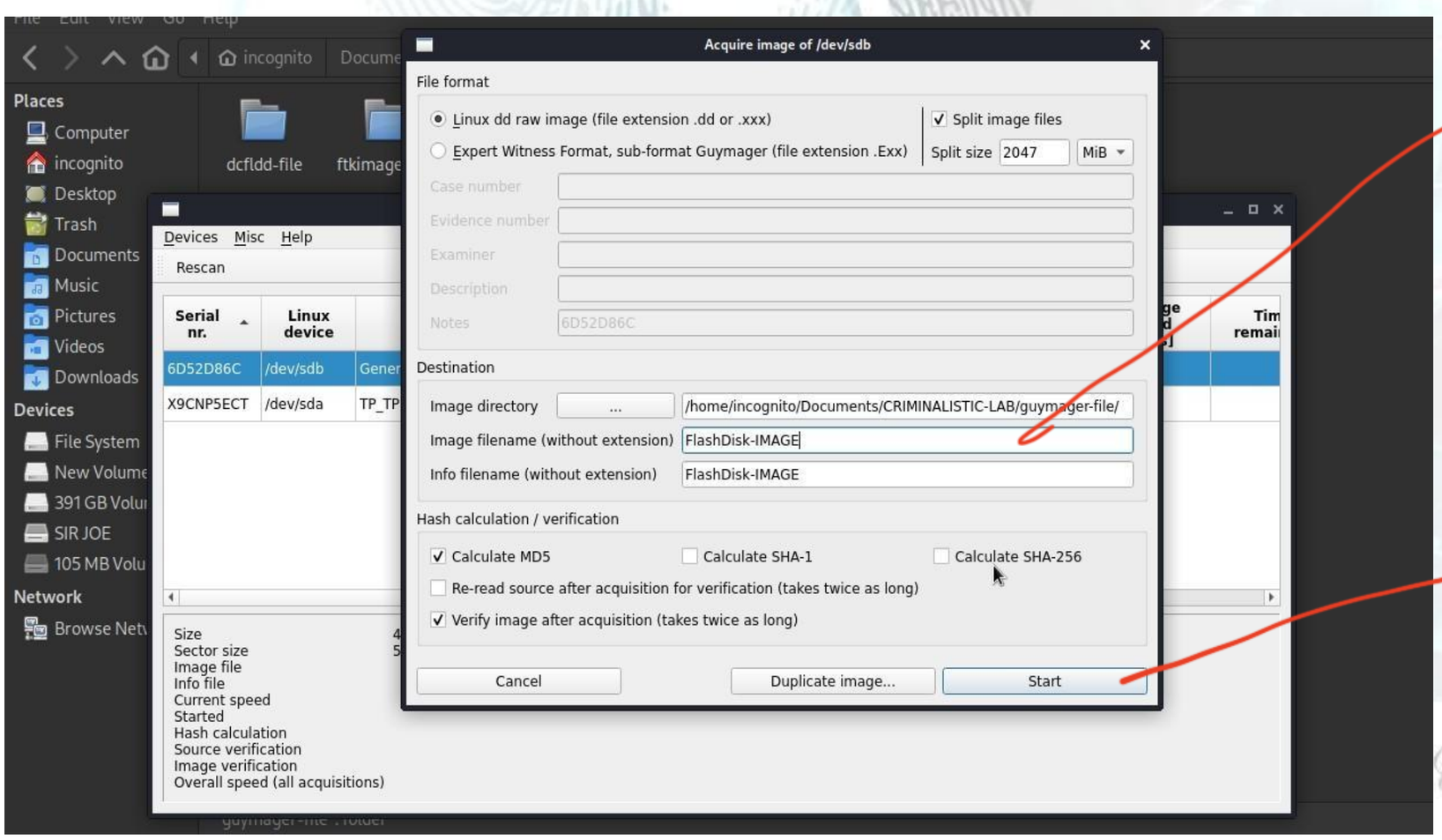
Eudine Oyier

Usage Highlight

I used Guymager to acquire a forensic image of a **4GB USB flash drive**, stored at:
/home/incognito/Documents/CRIMINALISTIC-LAB/guymager-file/ → images name

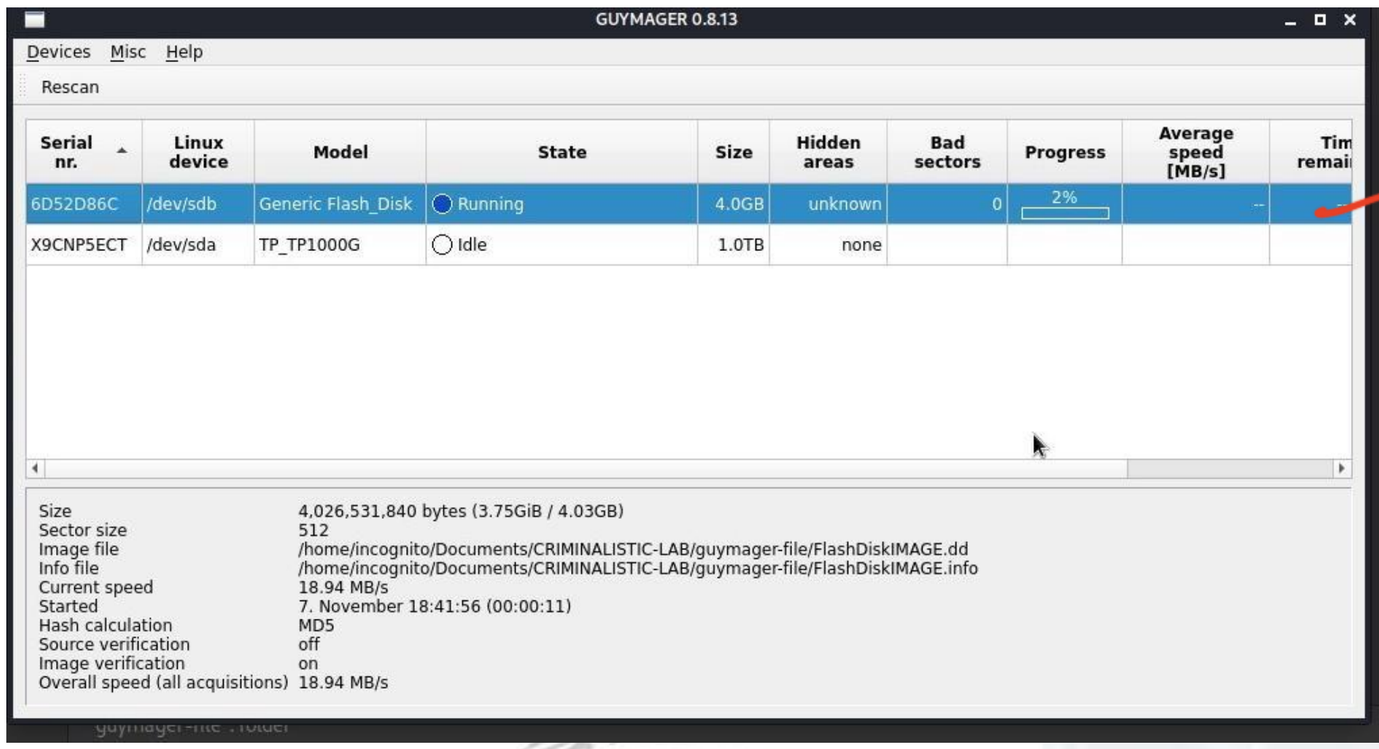
- Image format: **Raw (.dd)**
- O
- B



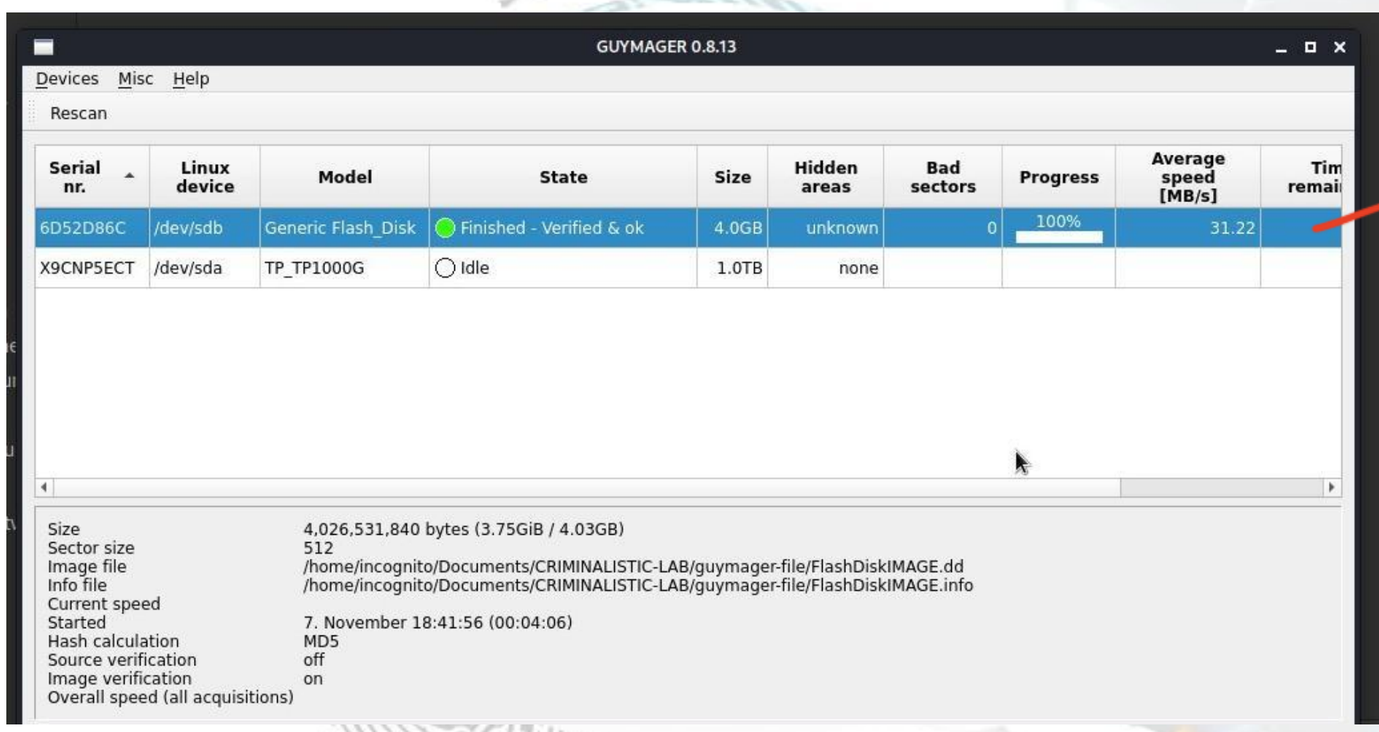


1 image name

2

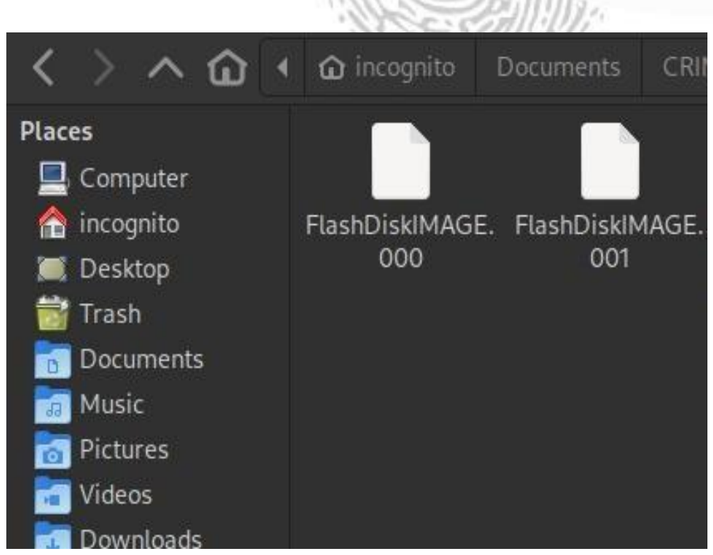


3 select drive



4 Finished

check storage location.



2. G Autopsy – Advanced Forensic Analysis Suite

Screenshot: Autopsy showing recovered deleted files]

Autopsy is a full-featured forensic browser, providing GUI access to file systems, user activity, timelines, and deleted data—powered under the hood by Sleuth Kit.

Key Features:

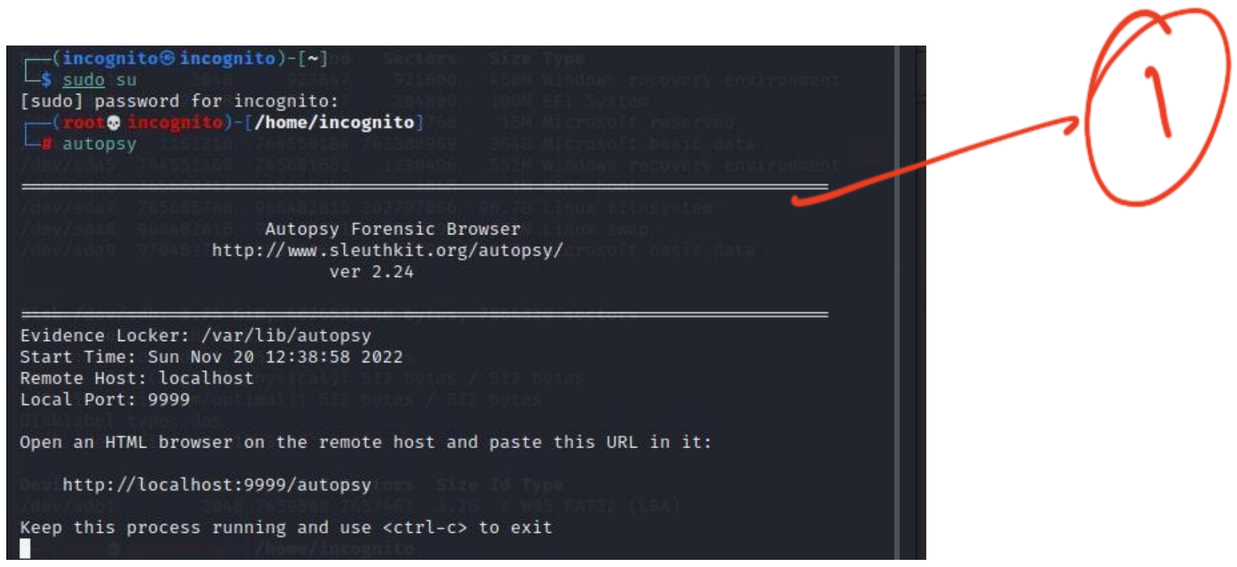
- GUI-based web application for deep analysis
- Supports .img, .dd, .e01, .vmdk, .vhd images
- File system support: **NTFS, FAT, exFAT, ext4, HFS+**
- Deleted file recovery, multimedia preview, keyword search

GitHub – Autopsy/SleuthKit

Usage Highlight

I used Autopsy to analyze a .dd image created by Guymager. It allowed me to:

- **Recover and export deleted files**
- **View media content** using external players
- Analyze user activity and file metadata



Create A New Case

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

mycase1

2. **Description:** An optional, one line description of this case.

my criminal case

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. Eudine Oyier
b.
c.
d.
e.
f.
g.
h.
i.
j.

New Case | Cancel | Help

2

Case: mycase1
Host: host2

Add a New Image

1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/home/incognito/Documents/CRIMINALISTIC-LAB/

2. **Type**
Please select if this image file is for a disk or a single partition.

Disk | Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

Symlink | Copy | Move

Next

Cancel | Help

3 location of disk images

we will use images acquired above by GUYMAGER

Case: mycase1

Add a New Host

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

host2

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

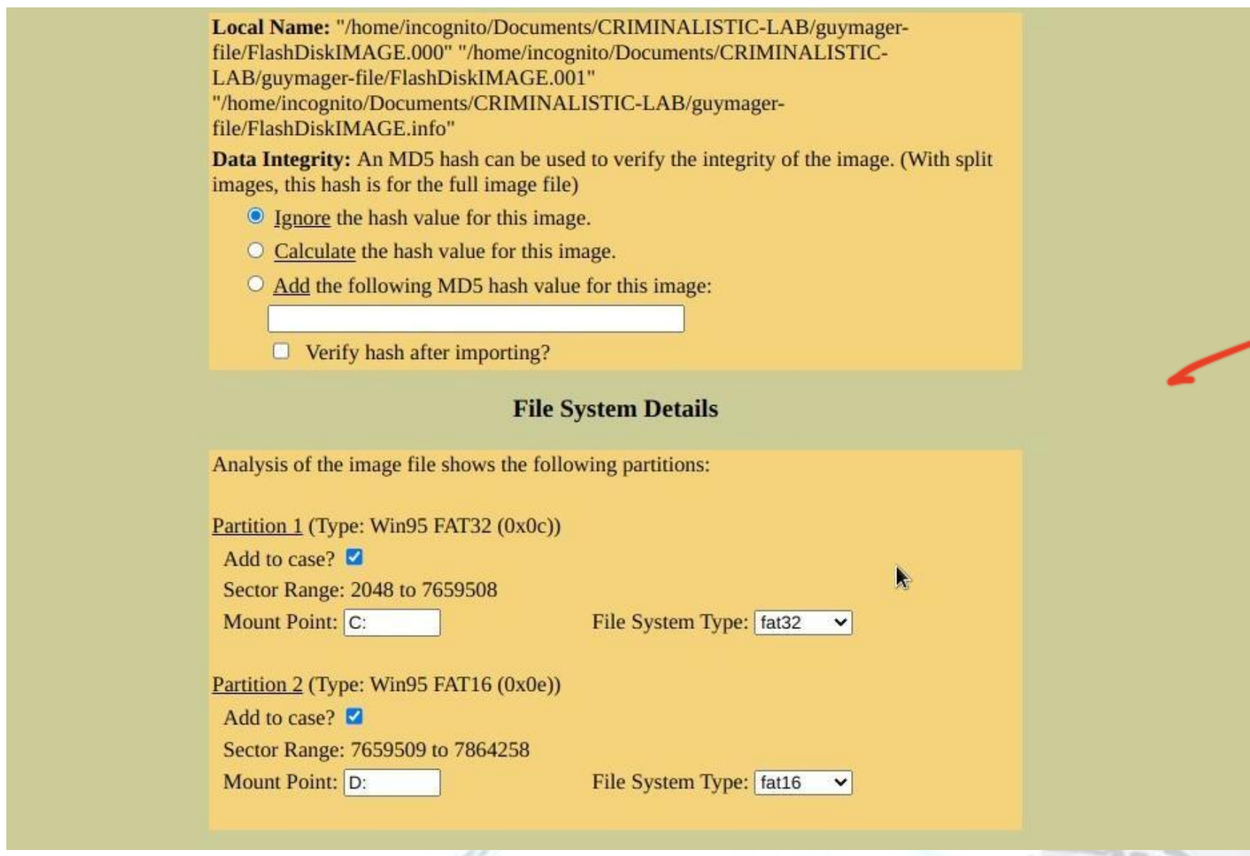
0

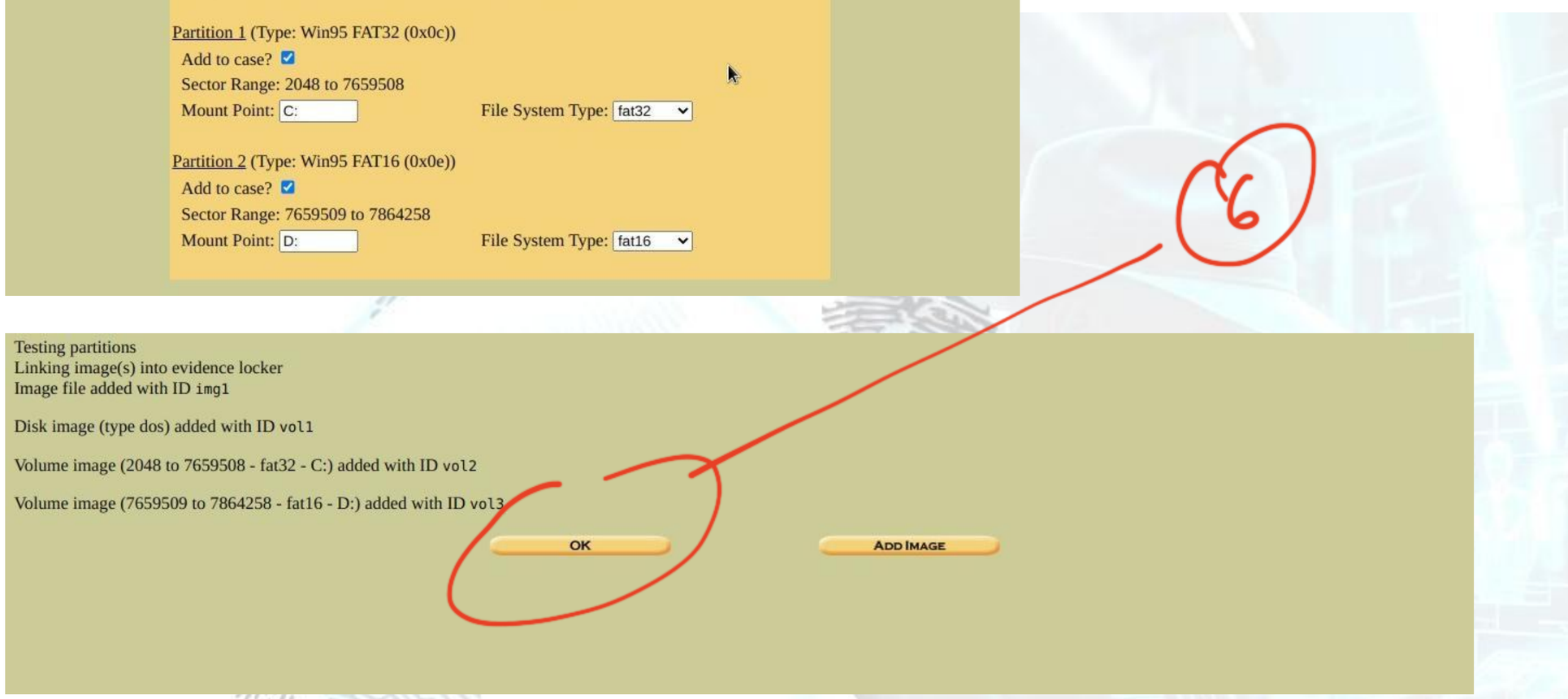
5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

Add Host | Cancel | Help

4


Local Name: "/home/incognito/Documents/CRIMINALISTIC-LAB/guymager-file/FlashDiskIMAGE.000" "/home/incognito/Documents/CRIMINALISTIC-LAB/guymager-file/FlashDiskIMAGE.001" "/home/incognito/Documents/CRIMINALISTIC-LAB/guymager-file/FlashDiskIMAGE.info"
Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)
Ignore the hash value for this image.
Calculate the hash value for this image.
Add the following MD5 hash value for this image:
Verify hash after importing?
File System Details
Analysis of the image file shows the following partitions:
Partition 1 (Type: Win95 FAT32 (0x0c))
Add to case?
Sector Range: 2048 to 7659508
Mount Point: C:
File System Type: fat32
Partition 2 (Type: Win95 FAT16 (0x0e))
Add to case?
Sector Range: 7659509 to 7864258
Mount Point: D:
File System Type: fat16
5


Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1
Disk image (type dos) added with ID vol1
Volume image (2048 to 7659508 - fat32 - C:) added with ID vol2
Volume image (7659509 to 7864258 - fat16 - D:) added with ID vol3
OK
ADD IMAGE
6

Case: mycase1
Host: host2
Select a volume to analyze or add a new image file.
CASE GALLERY
HOST GALLERY
HOST MANAGER
mount name fs type
disk FlashDiskIMAGE.000-disk raw details
C:/ FlashDiskIMAGE.000-2048-7659508 fat32 details
D:/ FlashDiskIMAGE.000-7659509-7864258 fat16 details
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER
7

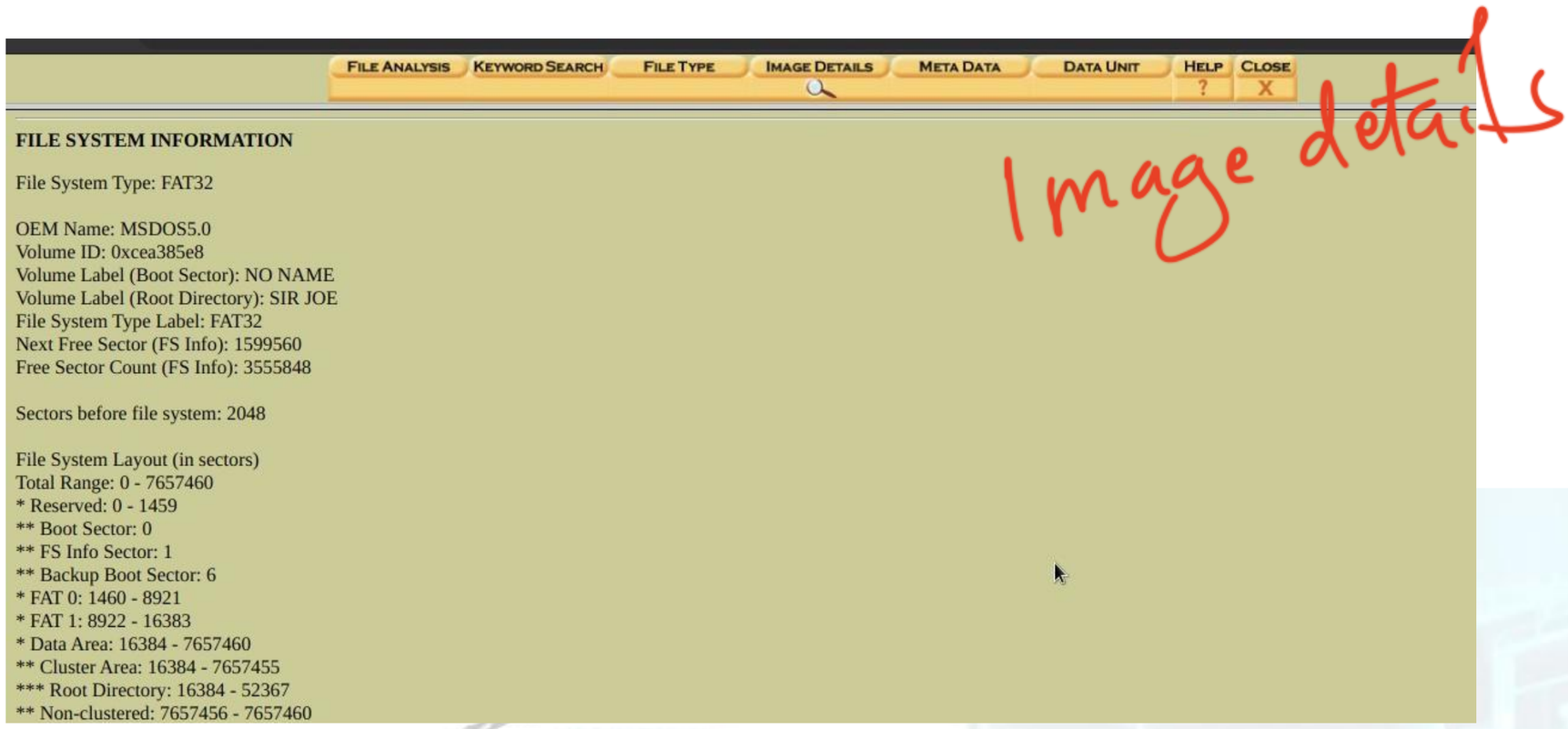
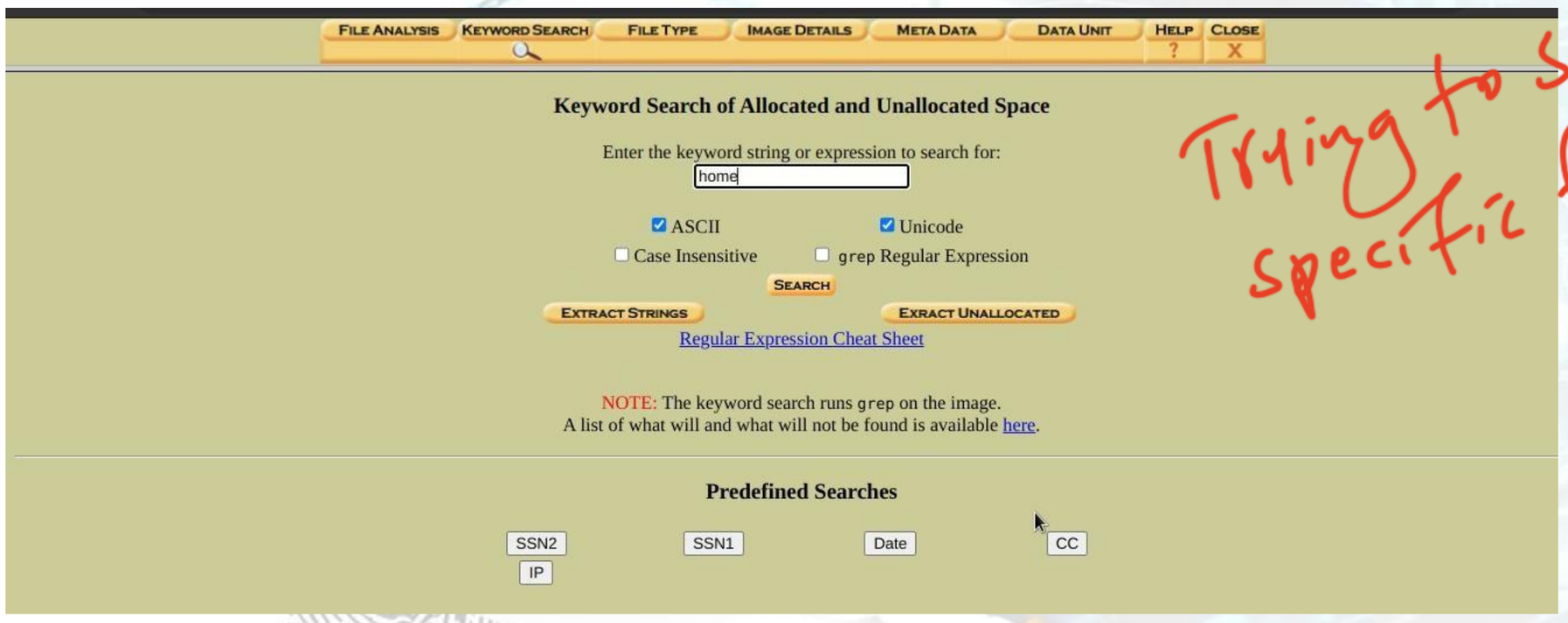
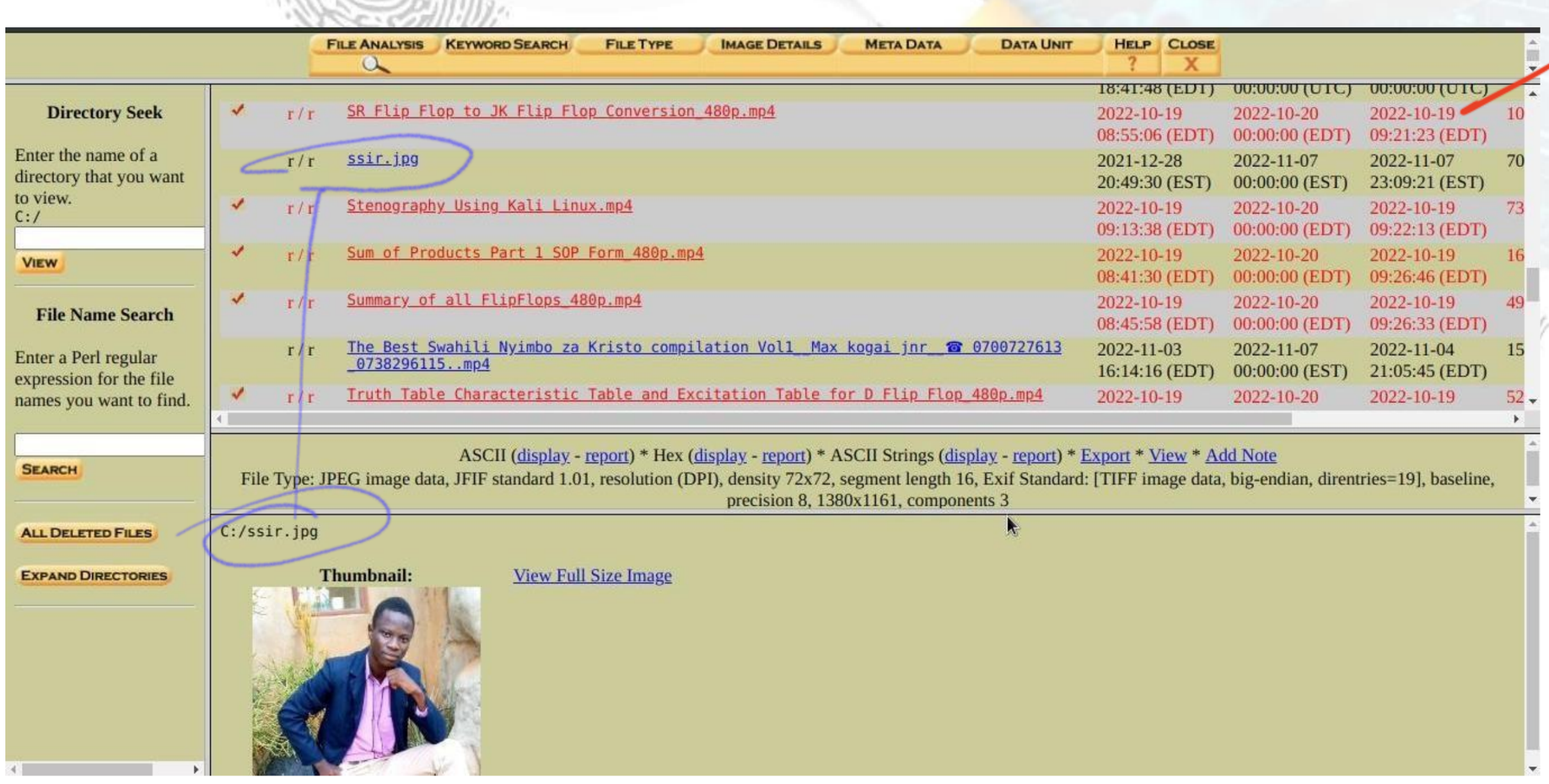


Image details



Trying to search specific file



8 Analyze

3. 🔍 Foremost – CLI-Based Deleted File Recovery

Foremost is a CLI-based forensic tool designed to recover deleted files based on signature carving (headers/footers).

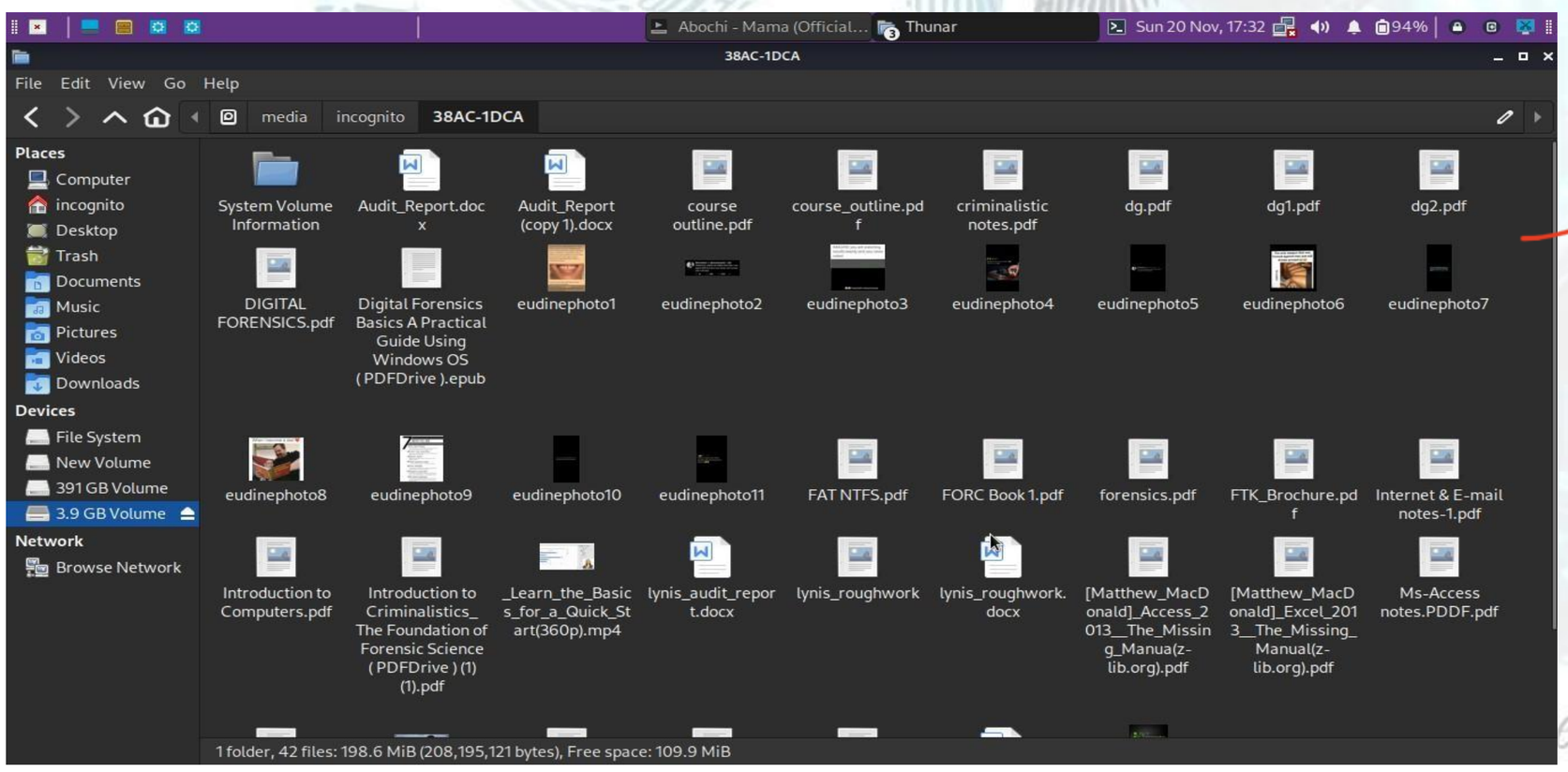
◆ **Key Features:**

- ✓ Recovers files based on binary signatures
- ✓ CLI-based and lightweight
- ✓ Works on raw images or live disk devices
- ✓ Filesystem-independent

Usage Highlight

I used Foremost to carve all .jpg files from the flash disk image.

- ✓ Original visible photos: **12**
- ✓ Recovered: **270 .jpg files** (including previously deleted ones)



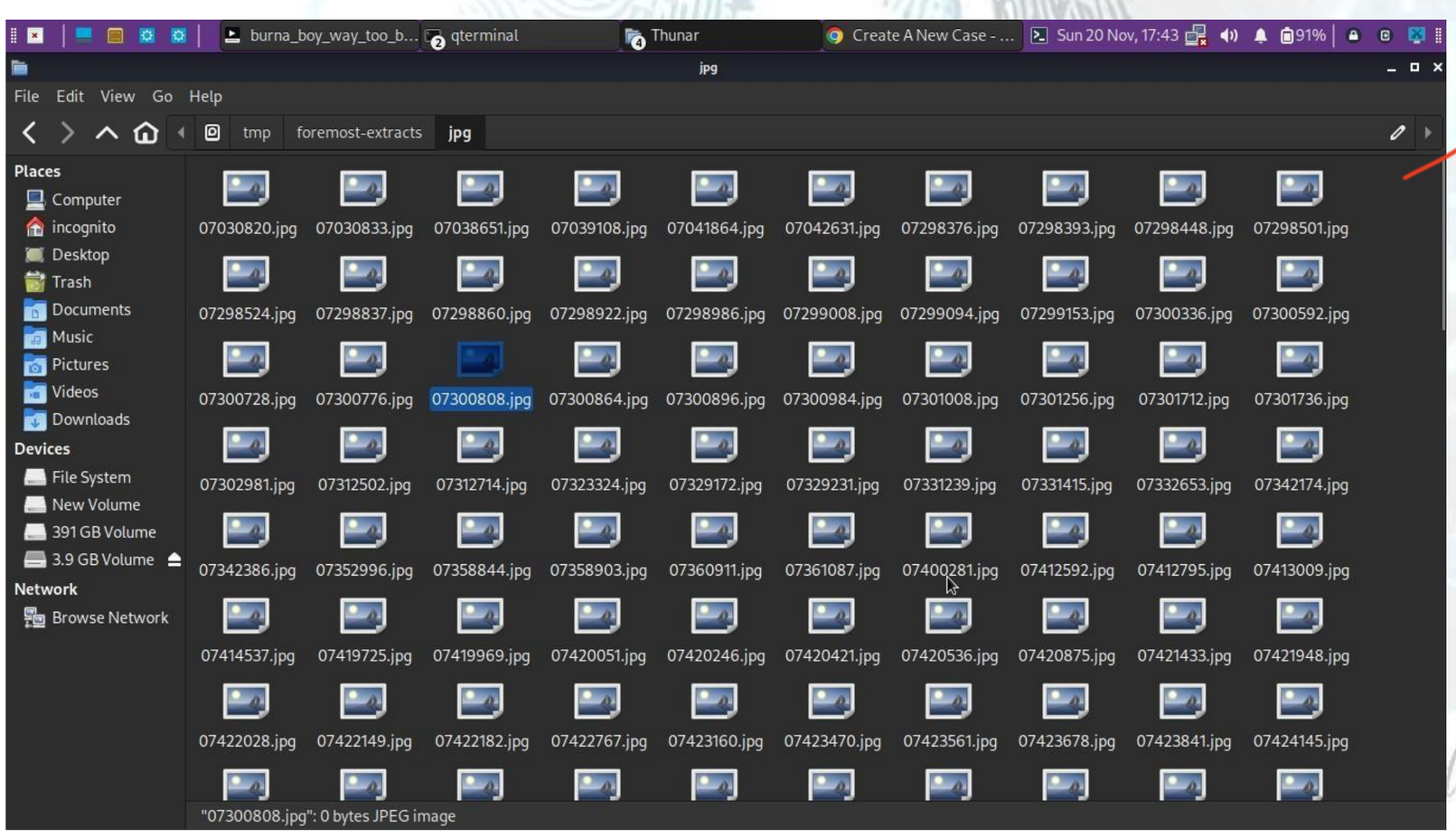
contents of USB used

```
┌──(root💀 incognito)-[/home/incognito]
└─# foremost -t jpg -i /dev/sdb1 -v -o /tmp/foremost-extracts/
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Sun Nov 20 12:36:46 2022
Invocation: foremost -t jpg -i /dev/sdb1 -v -o /tmp/foremost-extracts/
Output directory: /tmp/foremost-extracts
Configuration file: /etc/foremost.conf
Processing: /dev/sdb1
|------------------------------------------------------------------
File: /dev/sdb1
Start: Sun Nov 20 12:36:46 2022
Length: 3 GB (3920620032 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

*
```

① command used.

Use:
* fdisk -l
* df

To list storage drives in a linux system and choose the drive to analyze.



② jpg files recovered as defined above.

other filetypes can also be defined

4. dcfldd – Enhanced Forensic Disk Cloner

dcfldd is a forensic-ready variant of dd, created by the U.S. Department of Defense for secure, verifiable imaging.

Key Features:

- Real-time hashing (MD5, SHA1)
- Progress bar for imaging
- Verifies output matches source
- Supports wiping and multi-output

Guide to dcfldd

Usage Highlight

I used dcfldd to create a disk image of the same 4GB USB drive.

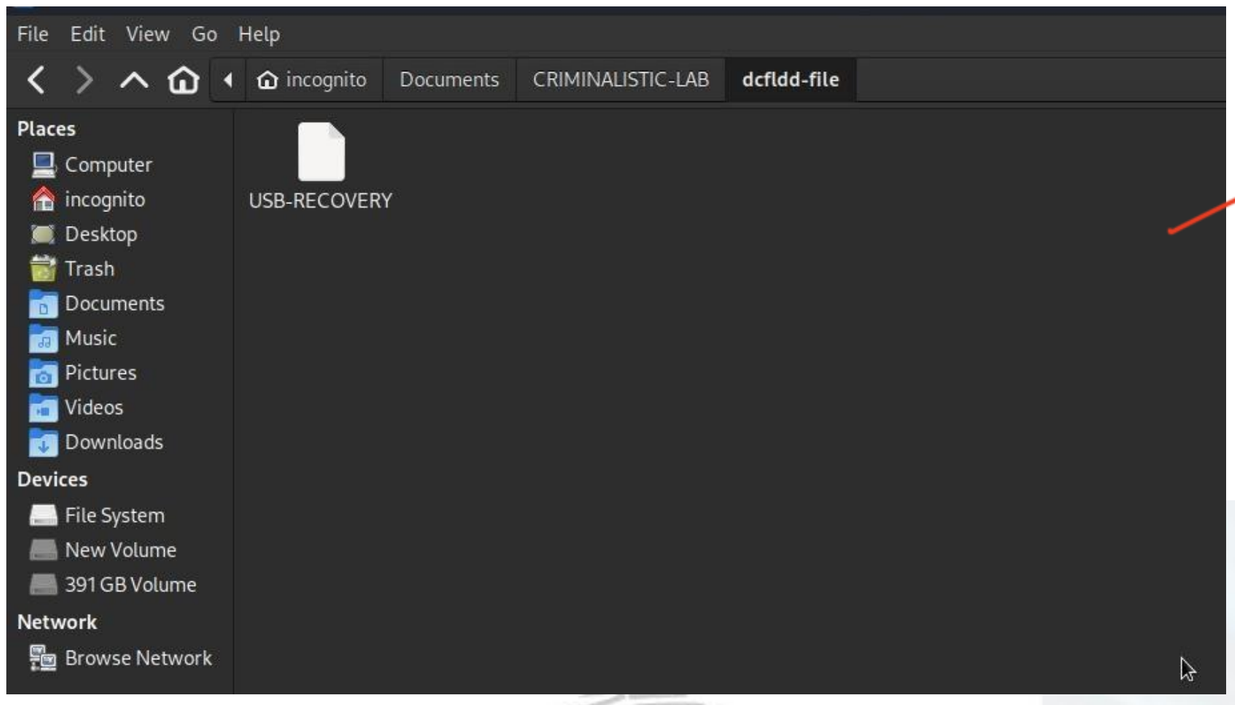
- Image stored at: /home/incognito/Documents/CRIMINALISTIC-LAB/dcfldd-file/
- Image named: USB-RECOVERY
- This image was later analyzed using Scalpel

```
┌──(incognito㉿incognito)-[~]
└─$ sudo su
[sudo] password for incognito:
┌──(root💀incognito)-[/home/incognito]
└─# df
Filesystem     1K-blocks      Used Available Use% Mounted on
udev             1933452         0   1933452   0% /dev
tmpfs             394192      1624    392568   1% /run
/dev/sda7       99220616  39449128  54685180  42% /
tmpfs            1970944         0   1970944   0% /dev/shm
tmpfs               5120         0      5120   0% /run/lock
tmpfs             394188        88    394100   1% /run/user/1000
/dev/sda9      491518972 379076012 112442960  78% /media/incognito/New Volume
/dev/sda4      381694484 187992580 193701904  50% /media/incognito/78E61B03E61AC0F4
/dev/sdb1        3820536   2042612   1777924  54% /media/incognito/SIR JOE
```

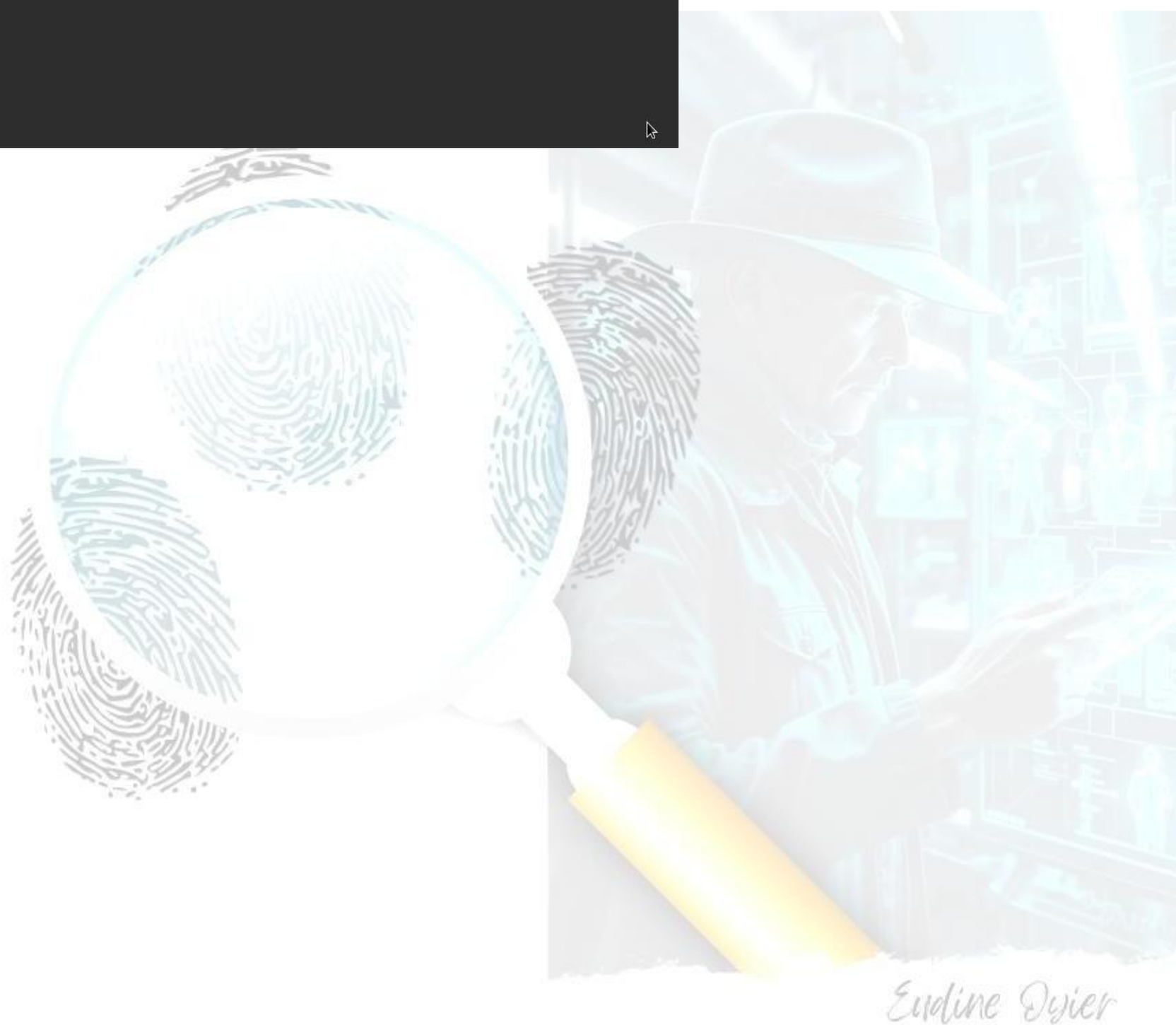
① list drives

```
┌──(root💀incognito)-[/home/incognito]
└─# dcfldd if=/dev/sdb1 of=/home/incognito/Documents/CRIMINALISTIC-LAB/dcfldd-file/USB-RECOVERY
119552 blocks (3736Mb) written.
119647+1 records in
119647+1 records out

┌──(root💀incognito)-[/home/incognito]
└─#
```

② command to create image.



③ Image created



5. ⚡ Scalpel – High-Speed File Carving Tool

Scalpel is a fast and configurable file carver derived from Foremost, with better performance and file carving flexibility.

◆ Key Features:

- Recovers files using header/footer signatures
- Works on raw images or partitions
- File system agnostic: **NTFS, ext4, exFAT, FAT32, XFS**, etc.
- Configurable search via scalpel.conf

Usage Highlight

Using the USB-RECOVERY image from dcfldd, Scalpel recovered:

- Files with .jpg, .png, and .gif extensions
- Output stored at: /home/incognito/Documents/RECOVER1/scalpel

Scalpel configuration file location.

1

```
┌──(incognito㉿incognito)-[~/Documents/CRIMINALISTIC-LAB/ftkimager-file]
└─$ sudo man scalpel
[sudo] password for incognito:

┌──(incognito㉿incognito)-[~/Documents/CRIMINALISTIC-LAB/ftkimager-file]
└─$ whatis scalpel
scalpel (1)          - Recover files using a header/footer database

┌──(incognito㉿incognito)-[~/Documents/CRIMINALISTIC-LAB/ftkimager-file]
└─$ whereis scalpel
scalpel: /usr/bin/scalpel /etc/scalpel /usr/share/man/man1/scalpel.1.gz

┌──(incognito㉿incognito)-[~/Documents/CRIMINALISTIC-LAB/ftkimager-file]
└─$ cd /etc/scalpel

┌──(incognito㉿incognito)-[/etc/scalpel]
└─$ ls
scalpel.conf

┌──(incognito㉿incognito)-[/etc/scalpel]
└─$ sudo gedit scalpel.conf
```

Eudine Oyier

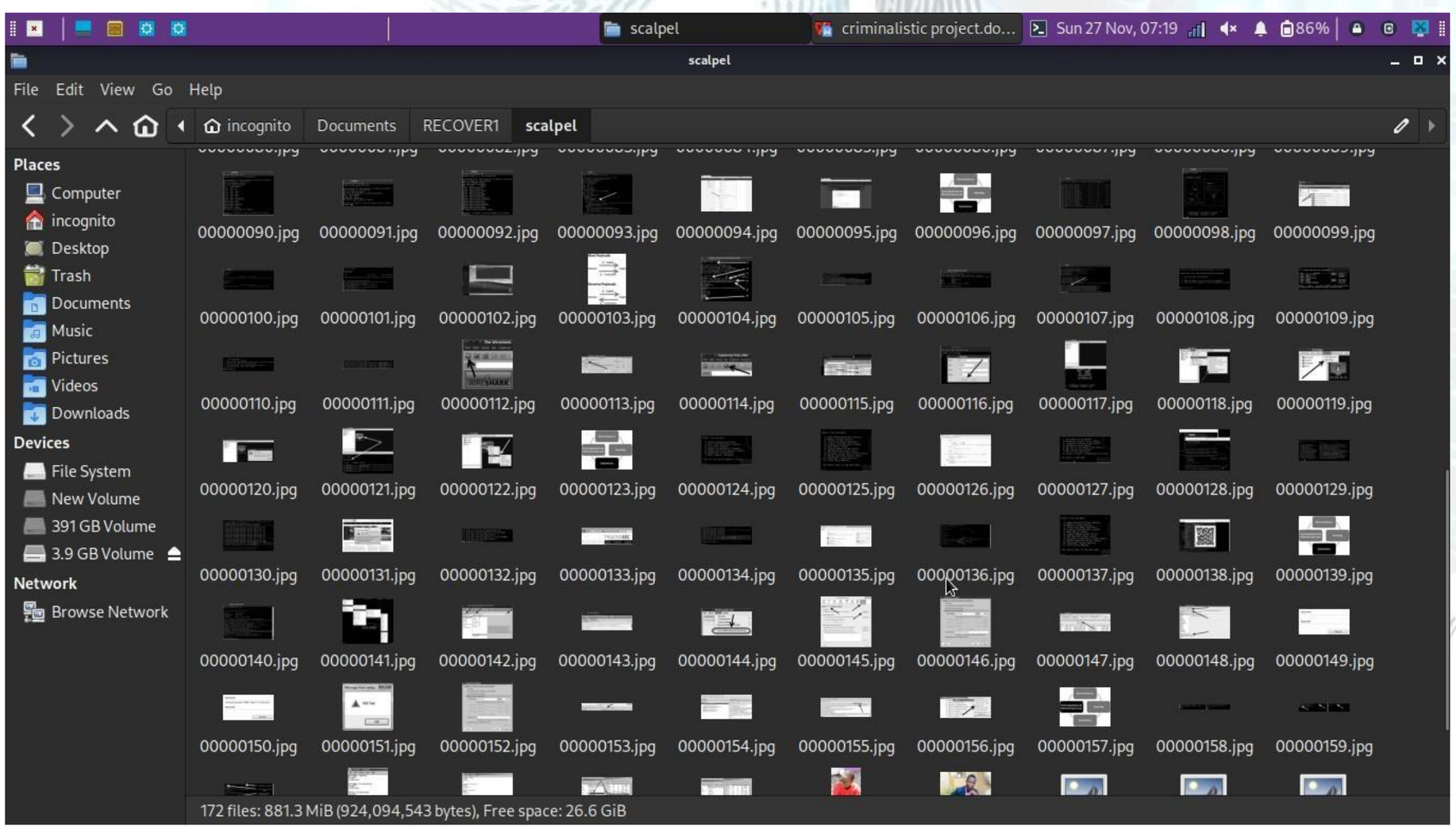
```
#       NONE    y       1000    FOREMOST
#
#-----------------------------------------------------------------
# GRAPHICS FILES
#-----------------------------------------------------------------
#
#
# AOL ART files
#       art     y       150000  \x4a\x47\x04\x0e        \xcf\xc7\xcb
#       art     y       150000  \x4a\x47\x03\x0e        \xd0\xcb\x00\x00
#
# GIF and JPG files (very common)
        gif     y       5000000         \x47\x49\x46\x38\x37\x61        \x00\x3b
        gif     y       5000000         \x47\x49\x46\x38\x39\x61        \x00\x3b
        jpg     y       5242880         \xff\xd8\xff???Exif             \xff\xd9        REVERSE
        jpg     y       5242880         \xff\xd8\xff???JFIF             \xff\xd9        REVERSE
#
#
# PNG
        png     y       20000000        \x50\x4e\x47?   \xff\xfc\xfd\xfe
#
#
# BMP   (used by MSWindows, use only if you have reason to think there are
#       BMP files worth digging for. This often kicks back a lot of false
#       positives
#
#       bmp     y       100000  BM??\x00\x00\x00
#
# TIFF
#       tif     y       200000000       \x49\x49\x2a\x00
# TIFF
#       tif     y       200000000       \x4D\x4D\x00\x2A
#
```

2

Uncomment
- gif
- jpg
- png

```
┌──(incognito㉿incognito)-[~]
└─$ sudo su
[sudo] password for incognito:
┌──(root💀incognito)-[/home/incognito]
└─# scalpel -o /home/incognito/Documents/RECOVER1/scalpel USB-RECOVERY -O -v
```

3 command to recover images.



6. 📄 FTK Imager – Disk Imaging & Quick Analysis Tool

FTK Imager is a forensic classic for creating drive images and previewing file content without altering the original media.

🔹 **Key Features:**

- Create images in **raw**, **E01**, and **AFF** formats
- View disk content and file metadata
- Export specific files or folders for further analysis
- Simple, reliable, and widely used

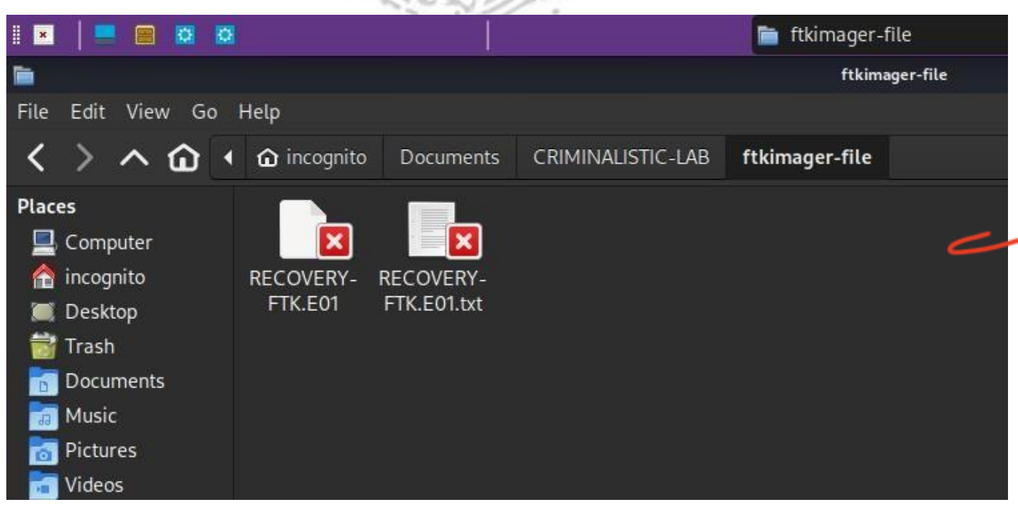
🟩 **Usage Highlight**

I used FTK Imager to create forensic images of drives in a structured lab scenario. It's especially useful for **previewing drive content before full analysis**.

① list drives

```
┌──(root💀 incognito)-[/opt]
└─# ftkimager --list-drives
AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.

/dev/sda - TP TP1000G                          [1000GB]
/dev/sdb

┌──(root💀 incognito)-[/opt]
└─# ftkimager /dev/sdb /home/incognito/Documents/CRIMINALISTIC-LAB/ftkimager-file/RECOVERY-FTK --e01 --compress 9 --case-number 001 --evidence-number EVIDENCE1 --descr
iption my-first-ftkimage-usage --examiner Eudine --notes 'this is a dd forensic image of a 4gb flash drive'
AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.

Creating image ...
Image creation complete.

┌──(root💀 incognito)-[/opt]
└─#
```

② create image



③ The images.

Eudine Oyier

Summary and Conclusion

Tool	Category	Interface	Windows Version	Key Capabilities
Guymager	Imaging	GUI	+	High-speed imaging, supports EWF/AFF/raw, multithreaded, hashing (MD5/SHA1/SHA256).
Autopsy	Analysis	GUI (Web)		File system analysis, integrates Sleuth Kit, supports many image types and VMs.
Sleuth Kit	Analysis	CLI		Core forensic analysis library powering Autopsy, supports FAT, NTFS, EXT, HFS+.
dcfldd	Imaging	CLI	+	Forensic dd variant with hashing, disk wiping, multi-output, and progress bar.
Foremost	Analysis	CLI	(via	File recovery from images or devices using headers/footers; supports multiple formats.
Scalpel	Analysis	CLI	(via port)	Fast file carver, improved version of Foremost, works on raw/images/partitions.
FTK Imager	Imaging & Analysis	GUI & CLI		Disk imaging and previewing tool, supports EWF, raw, and mounting image files.

Whether you're imaging a drive, recovering deleted files, or tracing user activity—these tools form the foundation of **open-source forensic practice**. This exercise reminded me that **powerful, reliable investigations don't always require expensive commercial software**.

ÇNB: **This is done in Linux Operating System.**

Eudine Oyier