Nulltack
Purple team bootcamp

Digital Forensics & Disk Acquisition

Prepared By:
Kazim Ali Obad

Supervisor:
Anmar Mohammed
Mohammed baqer

Contents

1: Disk Acquisition & Live Imaging

1. Introduction to Disk Acquisition

The whole idea behind acquisition similar to triage is that it should be done on a live running system. Of course, the ideal scenario is to power off the machine, pull the hard drive, and connect it externally. But when we can't do that, we do a live acquisition.

What is Acquisition?

Acquisition means taking a byte-for-byte copy of the data (resources) from a storage device.It can be a full Physical Hard Disk (the entire drive) or a Logical Drive (a specific partition, e.g., C:, D:).

The difference: Physical = the entire hard disk; Logical = one partition on that disk.

2. FTK Imager (Windows)

The most widely used tool for creating forensic images on Windows is FTK Imager. It is made by AccessData. Think of it as a very feature-rich research center tool.

2.1 What FTK Imager Can Do

- Produce multiple image formats: Raw, E01, Smart, AFF
- Compress the captured image (reduce file size)
- Hash verification: compute and verify hashes of the disk
- Support multiple acquisition types: physical drive, logical drive, image file, or folder/content

2.2 Acquisition Types in FTK Imager

Type	What It Captures	Use Case	Notes
Physical Drive	The entire hard disk, byte by byte	Full disk acquisition	Includes all partitions, unallocated space
Logical Drive	A single partition (e.g., C: or D:)	Partition-level acquisition	Smaller than full disk image
Image File	Converts one image format to another	Format conversion (e.g., .E01 to another format)	Used when you already have an existing forensic image
Folder / Content	Selected files and folders only	Custom image of specific content	Creates a custom image from selected files/directories

2.3 Image Formats in FTK Imager

When creating a disk image, FTK Imager asks you to choose the output format.

Here is a breakdown of all available formats:

Format	Full Name	Status	Key Feature
Raw	Bit-for-bit copy (dd-style)	Widely used	Pure binary copy; no metadata stored inside the file
Smart	Linux Expert Witness / SMART format	Obsolete	Legacy format considered deprecated today
E01	Expert Witness Format (EnCase)	Most popular	Stores metadata (case info, examiner name, MD5 hash) alongside the image; supports compression and notes
AFF	Advanced Forensic Format (Open Source)	Rarely used	Open source; designed for zero-knowledge image format — metadata not visible to the user

RECOMMENDATION: ***Always Use E01***

The E01 format is the most recommended and widely supported across forensic environments.

It stores case metadata, supports compression, allows notes, and is accepted by nearly all forensic tools.

AFF is open source but rarely used in practice. Raw is fine but stores no metadata inside the image itself.

2.4 Step-by-Step: Creating a Disk Image with FTK Imager

Before you open FTK Imager, make sure you have created a Write Blocker device first. This ensures the hardware write blocker is in place so nothing gets written to the source disk.

- Go to File > Create Disk Image
- Select the source type: Physical Drive, Logical Drive, Image File, or Folder/Content
- Choose the source disk (e.g., the physical hard drive you want to image)
- Click Next — FTK will show you the Image Source and Image Destination fields
- Set the Image Destination — always save to an external drive (USB, external HDD, etc.)

Note : *Always Save to External Drive , Always save the acquired image to an external drive — whether USB or external HDD.*

Never save the image back onto the same drive you are acquiring from.

This is an absolute rule in forensics.

2.5 Image Destination Settings

When configuring the image destination, you will need to fill in the following fields:

Field	Description / Example
Case Number	Tracking number for the investigation case (e.g., 001)
Evidence Number	Identifier for this specific piece of evidence
Description	Free-text note — e.g., 'Windows OS belonging to suspect'
Examiner Name	Your name or the analyst's name performing the acquisition
Notes	Any additional information about the acquisition
Destination Folder	Where to save the image file — always an external drive
File Name	Name for the output image file (e.g., 001.E01)
Image Fragment Size	Split output into multiple files of this size (e.g., 1500 MB per file). Set to 0 to keep as one file.
Compression Level	0 = No compression (fastest); 9 = Maximum compression (smallest size)

2.6 Verify and Finalize

- After clicking Finish, FTK will start the acquisition process
- Enable "Verify image after creation" — this computes hashes of the original disk and the resulting image, then compares them to confirm integrity
- Optional: "Create directory listing" — generates a text file listing all files captured (slightly slower)

WHY HASH VERIFICATION MATTERS ?

Hash verification computes hashes of both the original disk and the acquired image. If both hashes match, the image is a perfect, tamper-free copy.

This is critical for chain of custody and court admissibility.

3. Disk Acquisition on Linux

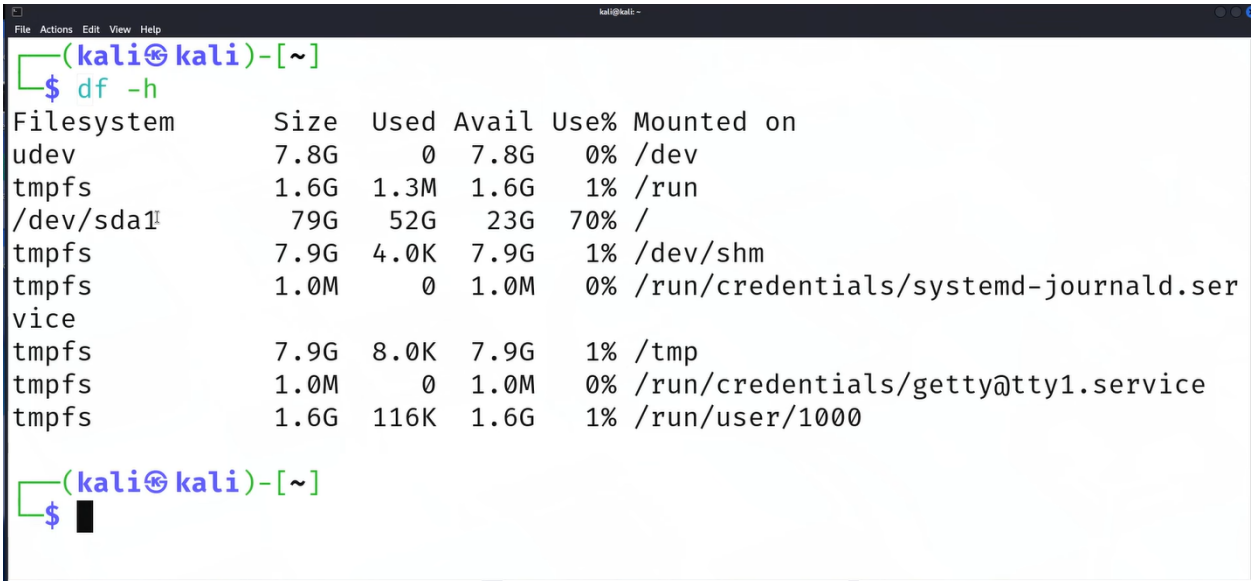
On Linux, we have several tools available. We will cover the two most important ones: dd and dcfldd.

3.1 The dd Command

dd is a built-in Linux utility — think of it as the Linux equivalent of FTK Imager. It produces a byte-for-byte copy of a drive, and it outputs in Raw format.

Before running dd, you need to identify your disks. Use the following command to list all drives:

```
df -h
```

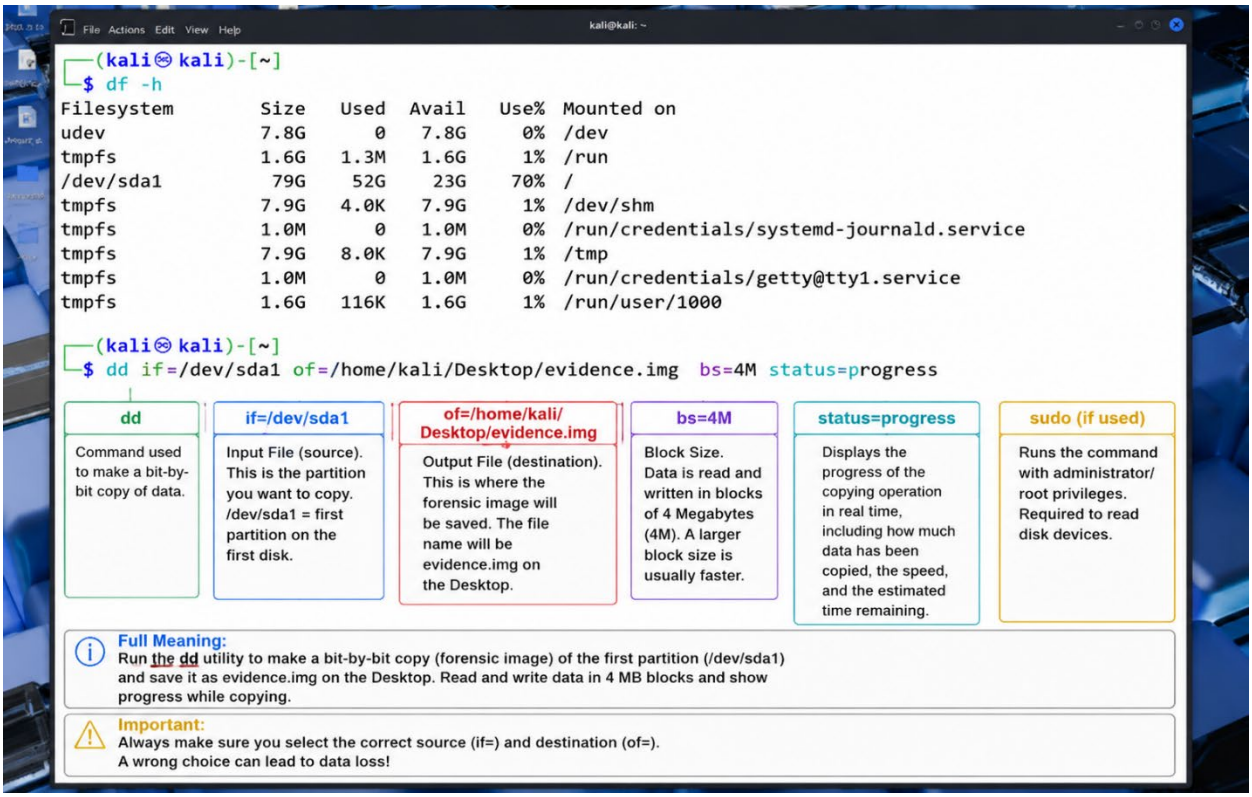


This shows all mounted disks both physical and logical. Once you know which disk you want to acquire, the basic dd syntax is:

NOTE: *Save Output to External Drive*

As always, save the output (if=) to an external drive, not back to the same disk.

```
sudo dd if=/dev/sda1 of=/home/kali/Desktop/evidence.img bs=4M status=progress
```



3.2 dcfldd — The Department of Defense Version

dcfldd was created by the United States Department of Defense. It is essentially dd but with additional forensic features:

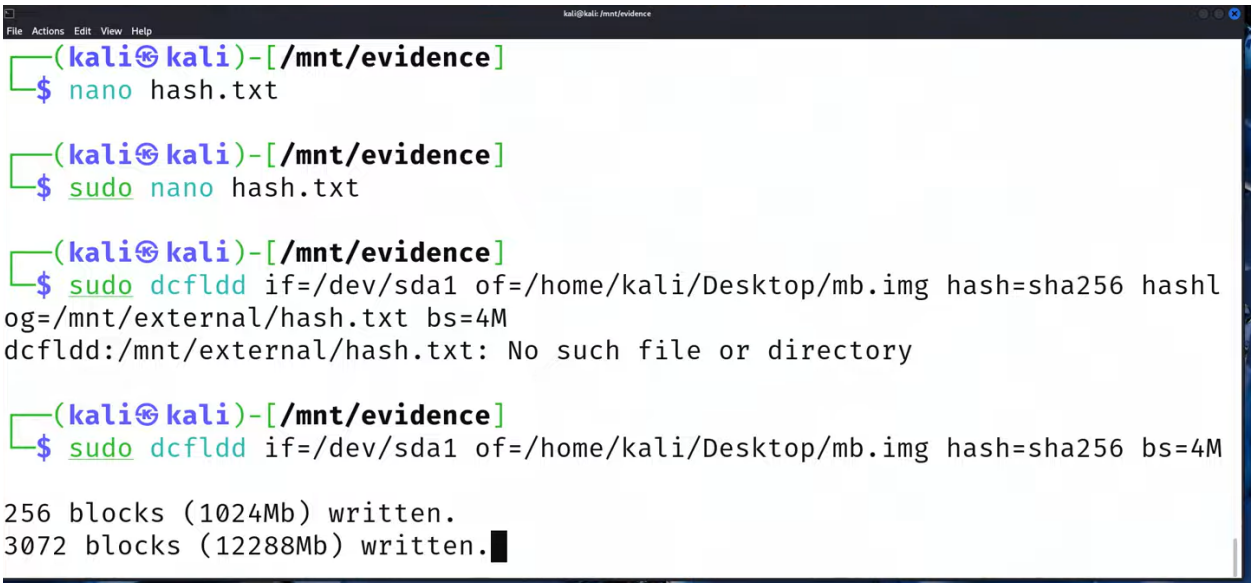
- Automatic hash computation during acquisition
- Real-time progress display
- Splitting output into multiple files (segmented output)

The process is straightforward, and the command structure is very similar to dd.

3.3 dcfldd — Full Command Example

Here is a full dcfldd command with all important options:

```
dcfldd if=/dev/sda of=/mnt/external/evidence.img bs=4M
      hash=md5 hashlog=/mnt/external/evidence.hashlog
```




```
# if       = source disk
# of       = output image file destination
# bs       = block size (4M recommended)
# hash     = hashing algorithm (e.g., md5, sha256)
# hashlog  = file to save hash log output
```

Note: The hash log file must exist before you run the command, or you must create the destination folder first:

```
mkdir /mnt/external/evidence_folder

# Then run dcfldd pointing of= and hashlog= inside this folder
```

4. Image Mounting

After acquiring a forensic image, the next step is often to mount it so you can access and analyze the files inside. This is called image mounting.

Think of it this way: when you plug in a USB drive on your laptop, Windows or Linux automatically shows it as a new drive (e.g., E: or /mnt/usb). Mounting does the same thing it makes your forensic image appear as a readable drive/partition in the operating system so you can browse and work with its contents.

4.1 Why Mount an Image?

- Browse and access the files and folders inside the image
- Run an antivirus scan on the captured partition
- View logs and forensic artifacts within the image
- Copy specific files out for further analysis
- Use various forensic tools directly on the mounted image

4.2 Arsenal Image Mounter (Windows)

On Windows, we use Arsenal Image Mounter for this task. The key feature that makes it forensically sound is Write Temporary Mode.

Write Temporary Mode

The Problem: When you normally mount a forensic image, any action opening a file, running a tool, or even background OS processes will write changes to the image and modify it. Why This Matters: Modifying the original evidence is a chain-of-custody violation.

The Solution: *Arsenal Image Mounter uses* ***Write Temporary Mode****. How It Works:* ***It creates a functional overlay layer on top*** *of the original image.*

- The original image is NEVER touched.

- All writes go to a temporary location.
- You can work freely and safely without any risk to the evidence.
- When you are done, all changes are discarded and the image returns to its original state.

Think of it like a sandbox or a protective copy for your evidence.

4.3 Linux File System Challenge When Mounting

A common challenge during mounting is file system compatibility. For example:

- Linux only natively understands Linux file systems (e.g., ext4)
- If your forensic image is from a Windows machine (NTFS), Linux cannot read it natively without extra support

The solutions are:

- Use Arsenal Image Mounter on Windows (has built-in support for multiple file systems)
- Use FTK Imager (also supports various file systems)
- Use a specific Linux module or tool that adds NTFS support

This is especially important when you are investigating a Linux server but working from a Windows forensic workstation or vice versa. If you are cross-platform and encounter an unreadable drive, the image will appear as an unreadable partition until you use the right tool.

NOTE : *In most cases, the recommended approach is to extract the EXT4 file system and work with it that way.*

This is one of the known limitations you may encounter when mounting Linux images on Windows and vice versa.

Windows Disk Forensics

5. Introduction to Windows Forensics

After collecting our evidence, we move to the next phase: forensic analysis. we will focus on Windows disk forensics specifically "Disk Forensics 6" (DF6).

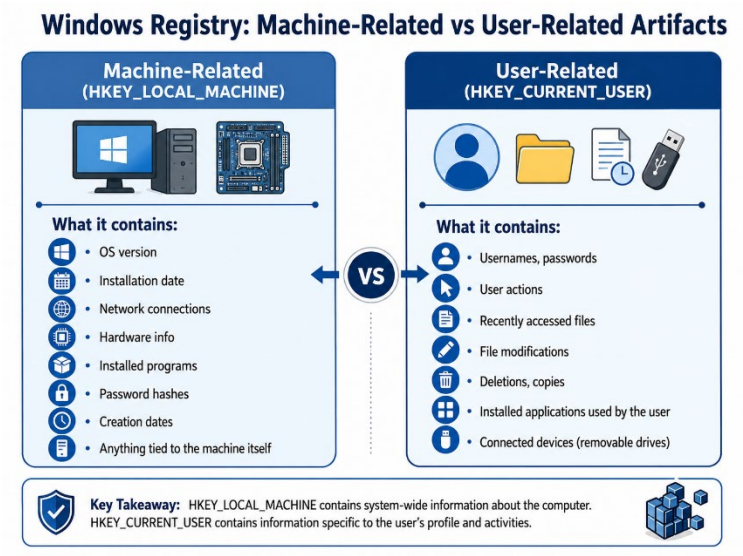
Why Windows? Because Windows desktops and laptops represent roughly 87% of the market. So the vast majority of your forensic investigations will be on Windows machines.

KEY INSIGHT: Why Windows Forensics is Powerful

- Windows is a complex system and that complexity produces a rich set of forensic artifacts.
- Every artifact reveals specific information about what happened on the machine.
- As a forensic analyst, you need to know WHERE to look otherwise you will waste enormous amounts of time.

6. The Two Categories of Windows Artifacts

Windows forensic artifacts fall into two broad categories: Machine-Related and User-Related. You see this same two-way split reflected in the Windows Registry itself.



6.1 Machine-Related Artifacts

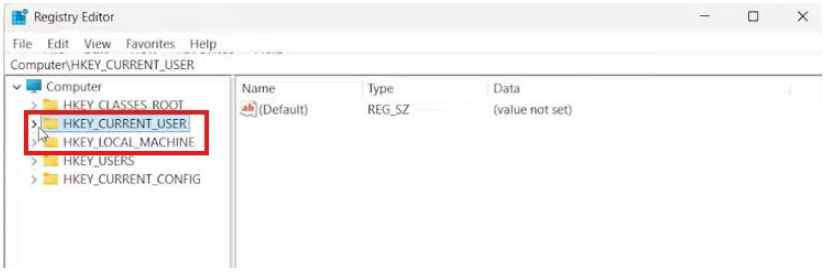
These artifacts are associated with the machine itself, not any specific user. They include:

- Operating System version and build information
- OS installation date and time
- Network connection history and IP addresses
- Hostname
- Password hashes and creation dates
- Installed programs

6.2 User-Related Artifacts

These artifacts are tied to individual user accounts on the machine. They include:

- Username and password files
- Actions performed by the user
- File access history (recently opened files)
- File modification, deletion, and copy history
- Applications installed or used by the user
- Connected removable devices (USB drives, etc.) including drive letter assigned and file names



7. Multiple Evidence Sources for the Same Artifact

An important principle in Windows forensics is that there is rarely just one place to find a piece of information. Most artifacts have multiple sources you can cross-reference.

For example, if you want to find the Windows installation date and time, you have two options:

- The Registry look up the installation timestamp key
- The Event Log find the relevant event entry

There is no single standard method. Every analyst has a different approach and order they prefer to work in. As long as you understand the core concepts of Windows forensics, you can follow your own investigation path.

NOTE *"Different analysts have different approaches different alpha answers."*

The important thing is that you understand the core concepts and can navigate them. Once you understand the process, you can work from any starting point.

8. Windows Event Logs

Windows Event Logs are special files that record everything that happens on the system. They are one of the most valuable sources of forensic evidence.

8.1 The Three Main Event Log Categories

Log Category	What It Records
System	Operating system events OS-level activity, driver failures, service starts/stops
Application	Application-level events any application running on the machine logs here
Security	Security events login successes, login failures, account access attempts

8.2 Security Log — Login Events

The Security log is particularly important for tracking user authentication. Login success and login failure events are both recorded here.

IMPORTANT: Audit Policy Configuration

- To get useful data from the Security log, audit policies must be configured first.
- Organizations like the CIS (Center for Internet Security) publish standard audit policy baselines.
- Always audit your policies without proper configuration, the Security log may not record what you need.
- Use Group Policy to configure audit settings across the environment.