DIGITAL FORENSIC ASSIGNMENT #3

Submitted By: Muhsin Ali Shah

Submission To: Sir Faizyab Khan

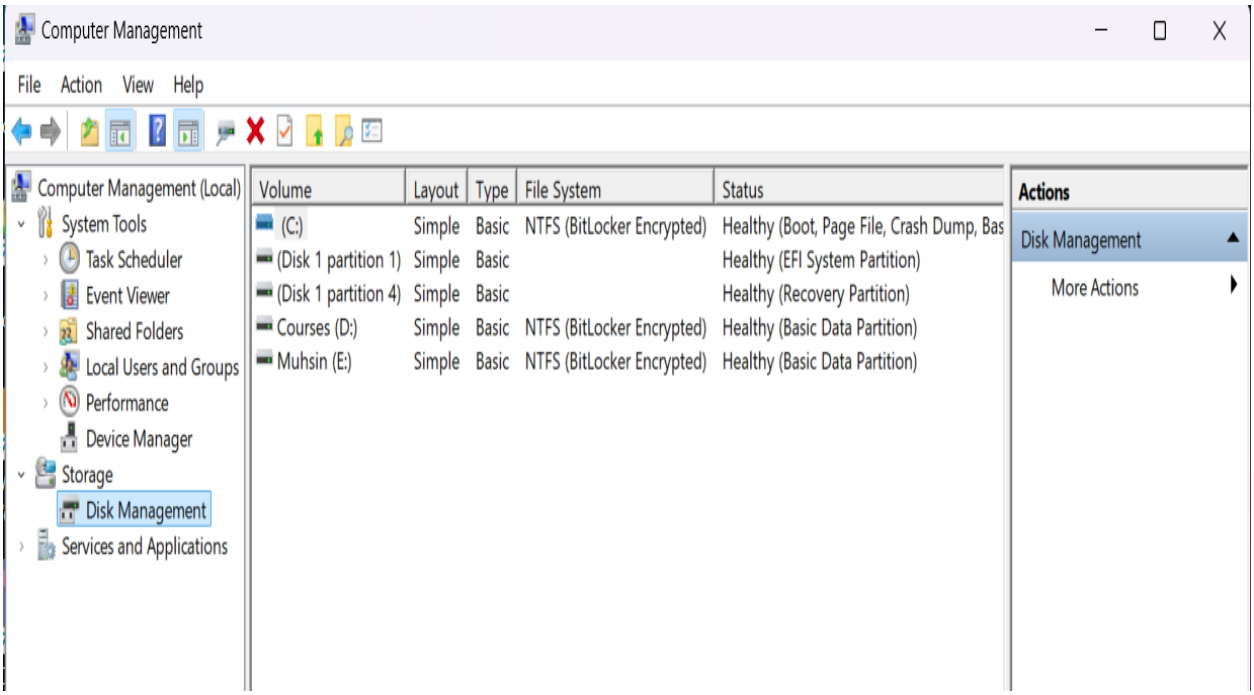
File Systems (File formats) and their applications and dependencies on OS also write a short report on how you made the image of the evidence.

Introduction:

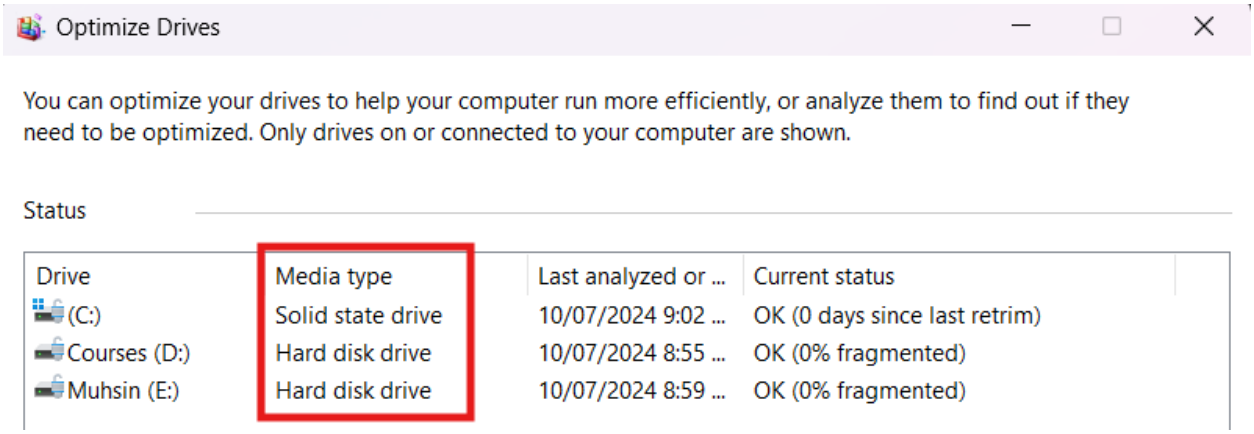
Files system is a method in which any operating system is used to store data. Different system can have different methods and structures such as Linux and windows can have different formats of saving or storing data and its system structure can be changed from each other.

Some of the well known file systems are **FAT32 , NTFS , HFS & EXT.**

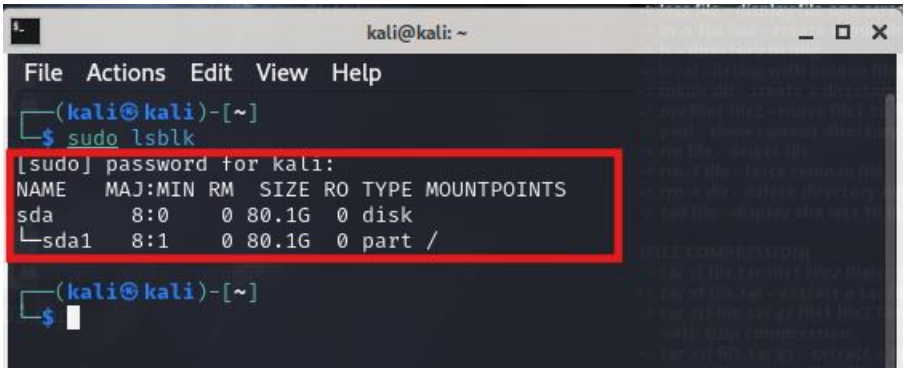
An Example of a ***File System*** *:*



*Another Example to look for filetypes is we can see it through **disk defragmentation** to know about the **hard drive** and **SSD** we are using in our system.*

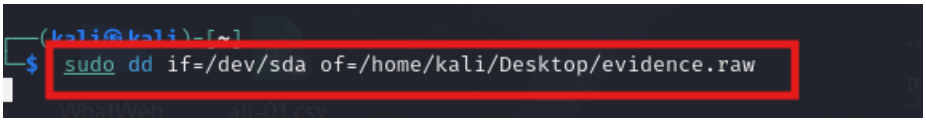


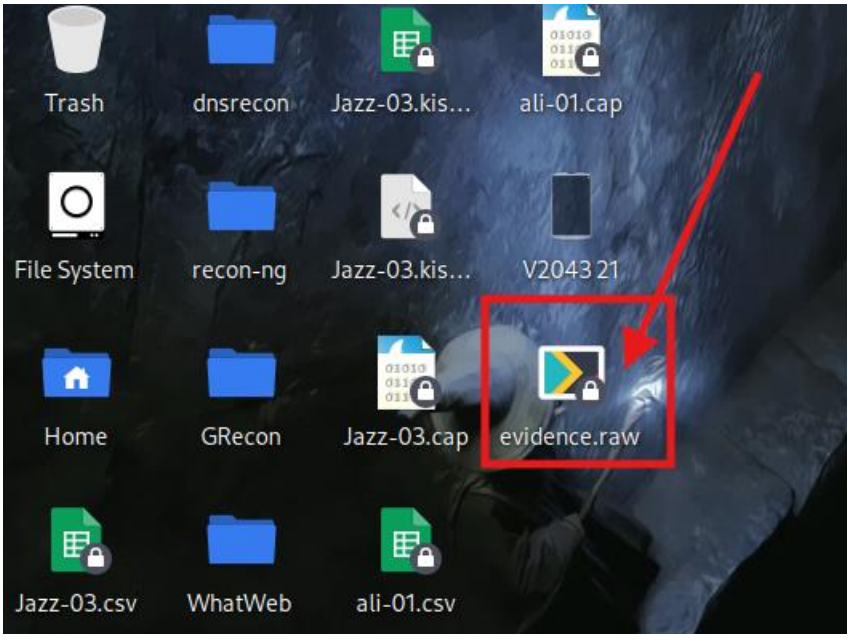
*These are an example for looking file system in **Windows.** Now we will try to look in command line of kalil linux.*



Generating copy of evidence:

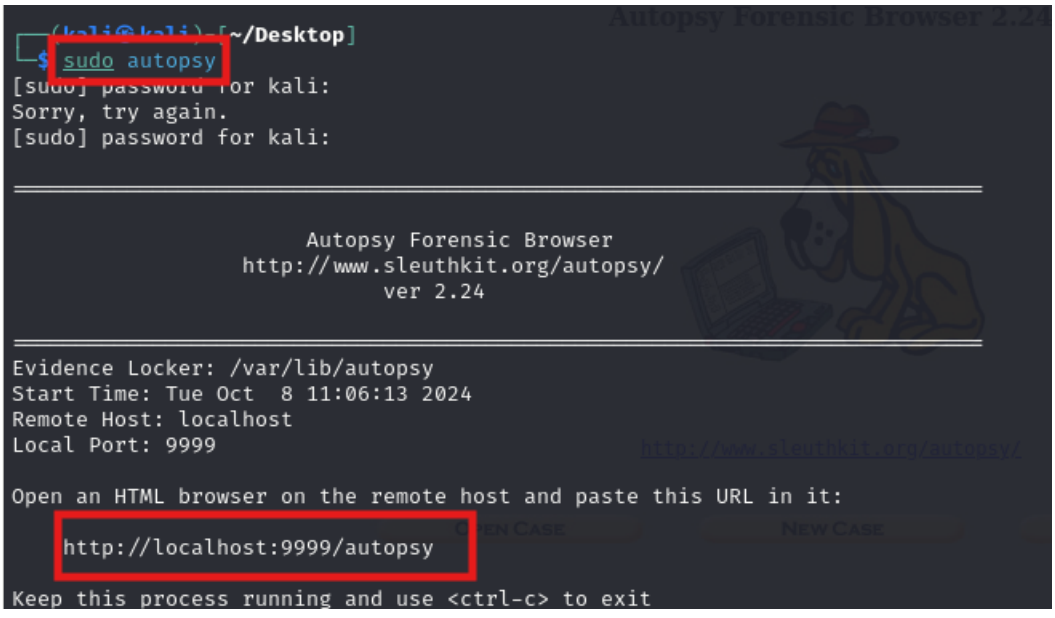
We can generate evidence of a file in simple steps by executing dd if=/dev/sda of=/home/kali/Desktop/evidence.raw. by this we are copying file system as a copy evidence to our Desktop as evidence.raw.





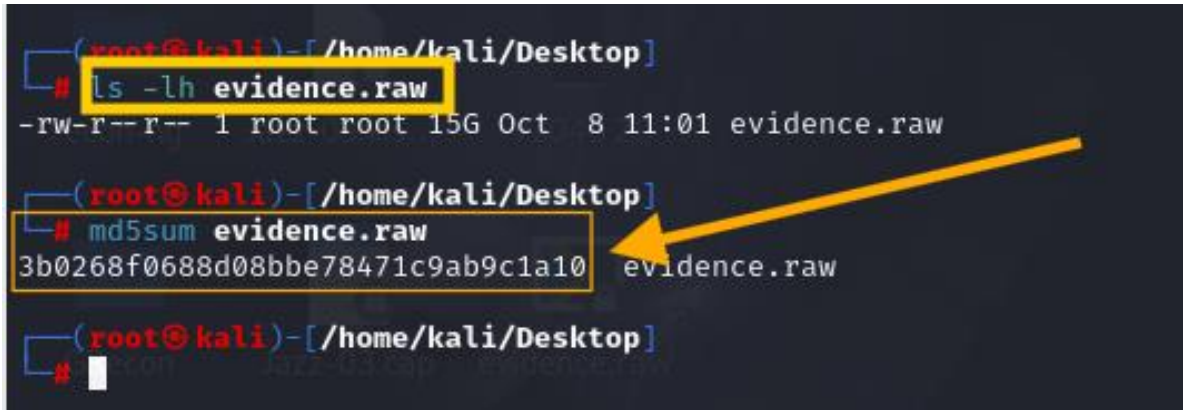
By such we can connect **usb** and if we want to create any image of data present in usb we can create them in a blink of an eye. It must be 16gb or 8gb usb of which we will be creating img.

For Further analysis we can use autopsy in Linux:



Generating hash of our Filesystem:

We Can simply generate hash of our img we created by entering md5sum and then filename.



This is our hash key **3b0268f0688d08bbe78471c9ab9c1a10**

Write a short report on how you made the image of the evidence.

In this process, I have generated an image of evidence from a USB drive using a few simple command-line steps. By the way I have attached all practical steps before this short report.

Report in some points as conducted above.

Connecting USB and Verify Detection:

First, I attached the USB drive to the system and verified its connection using the CLI (command-line interface). This is usually done by executing **lsblk** or **fdisk -l** to confirm the correct device name, such as /dev/sda.

Create the Evidence Image:

After identifying the USB drive, I created an image of the USB file system using the dd command. The command used was:

Enter dd if=/dev/sda of=/home/kali/Desktop/evidence.raw in cli

Explanation:

if=/dev/sda: Specifies the input file, which is the USB drive.

of=/home/kali/Desktop/evidence.raw: Specifies the output file, which is the evidence image saved on the desktop.

This command cloned the entire USB drive into an image file (evidence.raw) on the system's desktop.

Generating Hash for Integrity:

To ensure the integrity of the evidence, I generated a hash of the image file using the md5sum command:

md5sum evidence.raw

This creates an MD5 hash of the image, which can be used later to verify that the image has not been altered or tampered with.

The entire process ensures that the evidence is captured accurately from the USB drive, and the hash adds an extra layer of security by validating the integrity of the image file.

Result of Hash:

This was our hash key **3b0268f0688d08bbe78471c9ab9c1a10**