

**Digital Forensics Lab**

**Cyber Security Department**

CYL-2002

Fall 2024

Lab #04

Instructor:

Ubaid Ullah

Fahad Waheed

# Forensics Image File Formats:

Forensic image file formats play a crucial role in digital forensic investigations, as they capture and store the data from digital devices in a forensically sound manner. These file formats preserve the integrity of the original evidence and allow investigators to analyze and examine the data without altering or damaging it. There are several commonly used forensic image file formats, each with its own unique characteristics and applications. Here are descriptions of some of the major formats:

**Raw (dd):** Raw format, often referred to as "dd" (disk dump), is a bit-by-bit copy of a storage device. It includes all data sectors, including empty space, deleted files, and file system metadata. Raw images are popular for their completeness and versatility. They are useful when the investigator needs to perform in-depth analysis, data carving, or data recovery.

**Advanced Forensic Format (AFF):** AFF is a flexible and extensible forensic image format. It supports various compression methods, encryption, and metadata. AFF files can store multiple images within a single file, making it easier to manage different data sources in one container. It allows for efficient data transfer, reduces storage requirements, and supports advanced forensic features.

**EnCase Evidence File Format (E01):** Developed by Guidance Software, the E01 format is widely used in digital investigations. It creates a segmented file that contains an exact replica of the original storage device, maintaining its integrity. E01 files support compression and encryption, and they can store multiple images or segments. E01 is compatible with EnCase software and other forensic tools.

**Forensic Disk Image (Forensic Imager, FTK Imager): These** are proprietary image formats used by popular forensic software tools like Forensic Imager and FTK Imager. They capture the contents of a storage device and preserve it in a forensically sound manner. These formats often support compression, encryption, and metadata. Forensic image formats from specific software tools are useful when working with those tools extensively.

**Virtual Hard Disk (VHD/VMDK):** VHD and VMDK are virtual disk image formats commonly used in virtualization environments. In digital forensics, these formats find application when investigating virtual machines or analyzing virtualized systems. They contain the contents of virtual hard drives and can be mounted within virtualization software for examination and analysis.

**Portable Case (P2C):** P2C is a forensic image format designed for mobile devices. It captures the data from mobile phones, tablets, or other portable devices. P2C files store the device's file system, including operating system files, user data, and metadata. These formats are essential for mobile forensic investigations, allowing for data recovery, analysis of messages, call logs, and other device-specific artifacts.

# File System Types:

## FAT File System:

FAT or File Allocation Table is a file system used by operating systems for locating files on a disk. Due to fragmentation, files may be scattered around and divided into sections. FAT system keeps a track of all parts of the file. FAT has existed as a file system since the advent of personal computers.

**Features**

* File Name
  + FAT system in MS DOS allows file names of 8 characters only
  + FAT file system in Windows supports long file name, with full file path being as long as 255 characters
  + File name should start with alphanumeric characters
  + File names can have any character except “/ = [],? ^“”
  + File names can have more than one period and spaces. Characters that come after the last period in full file name are considered as the file extension.
* FAT file system does not support folder and local security. This means users logged into a computer locally will gain complete access to folders and files that lie in FAT partitions.
* It provides fast access to files. The rate depends upon the size of partition, file size, type of file and number of files in the folder.

## FAT 32 File System:

This is an advanced version of the FAT File system and can be used on drives ranging from 512 MB to 2 TB.

**Features**

* It is more storage-efficient and supports up to 2TB of size
* Provides a better usage of disk space
* Easier access of files in partitions less than 500 MB or greater than 2GB in size

## NTFS File System:

The NTFS File System stands for New Technology File System.

**Features**

* Naming
  + File name can be as long as 255 characters
  + File names can have any character other than / “ :\*
  + They are not case sensitive
* It provides folder and file security. This is done by passing on NTFS permission to files and folders. Security works at local as well as network level. Every file and folder in the list has an Access Control List that includes the users, security identifier, and the access privileges that are granted to the users.
* Files and partition sizes are larger in NTFS than those of FAT. An NTFS partition can be of a size as large as 16 Exabytes, but practically it is limited to 2TB. File size can range from 4GB to 64 GB.
* It provides up to 50% file compression
* It is a reliable and recoverable file system which makes use of transaction logs for updating files and folders automatically.
* It provides bad-cluster mapping. This means that it can detect bad clusters or erroneous space in the disk, retrieve the data in those clusters, and then store it in another space. To avoid further data storage in those areas, bad clusters are marked for errors.

## EXT File Systems:

Extended file system (EXT), Second Extended file system (EXT2) and Third Extended file system (EXT3) are designed and implemented on Linux. The EXT is an old file system that was used in pioneer Linux systems. EXT2 is probably one of the most widely used Linux file systems. EXT 3 also includes same features as EXT 2, but also includes journaling.

Here we will talk about the most used EXT2. With the optimizations in kernel code, it provides robustness along with good performance whilst providing standard and advanced Unix file features.

**Features**

* Supports standard file types in Unix i.e. regular files, device special files, directories, symbolic links
* Can manage file systems created on huge partitions. Originally, file system size was restricted to 2 GB, but with recent work in VFS layer, this limit has now increased to 4 TB.
* Reserves about 5 percent of blocks for administrator usage, thus allowing the admins to recover from situations of overfilled processes.
* Allows for secure deletion of files. Once data is deleted, the space is overwritten with random data to prevent malicious users from gaining access to the previous data.

# Sleuth Kit

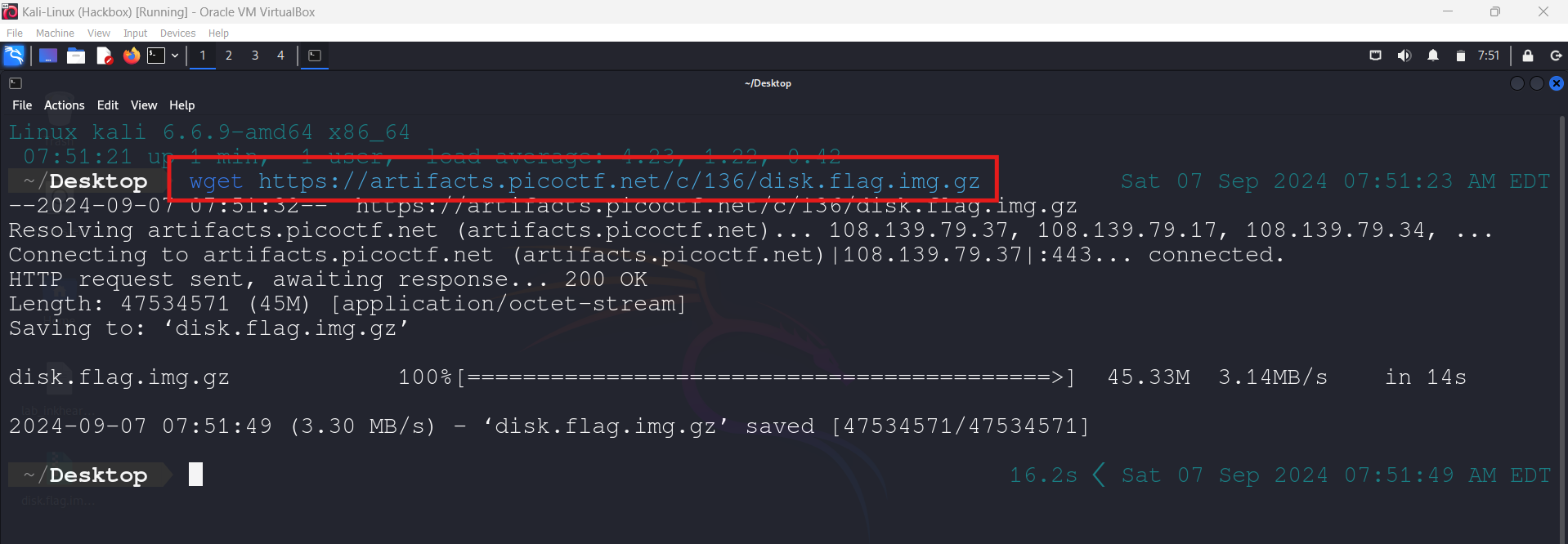
The [Sleuth Kit](https://www.sleuthkit.org/) is an open-source toolset that provides a collection of command-line tools for digital forensics. It supports file system analysis, disk imaging, and keyword searching across various operating systems. It is a library and collection of command line tools that allow you to investigate disk images. The core functionality of TSK allows you to analyze volume and file system data. The library can be incorporated into larger digital forensics tools and the command line tools can be directly used to find evidence.<https://www.kali.org/tools/sleuthkit/>

**Download Practice File**: <https://artifacts.picoctf.net/c/136/disk.flag.img.gz>

**Challenge Description:** Download the file and find the flag.

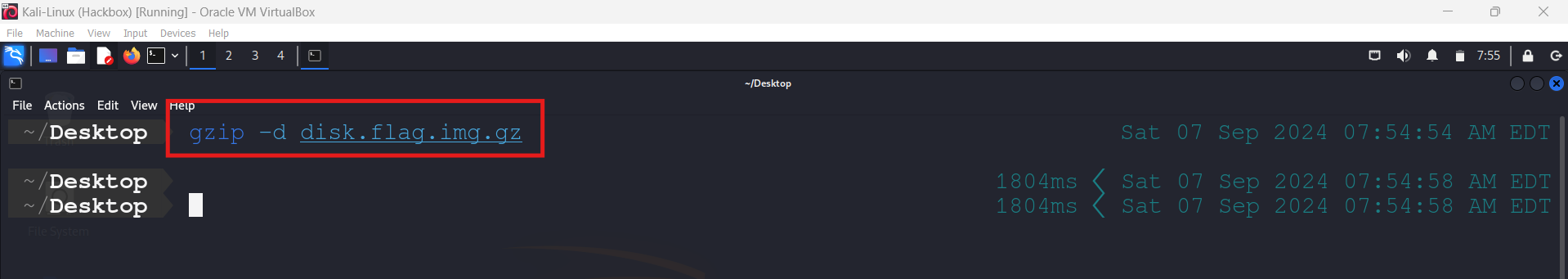
The challenge file is an image file, we can download the image file using the command:

wget <https://artifacts.picoctf.net/c/136/disk.flag.img.gz>



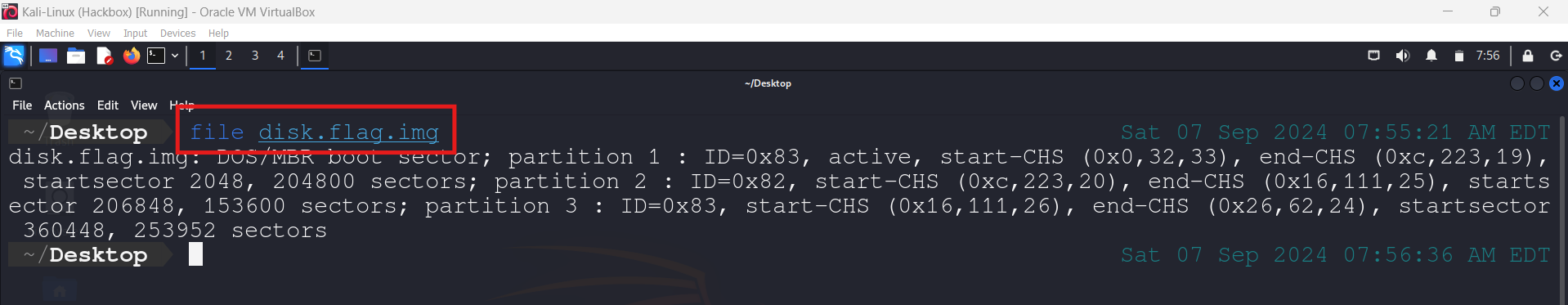
Now to extract the archive we can use gzip:

gzip -d disk.flag.img.gz



To check file type we can used the file utility:

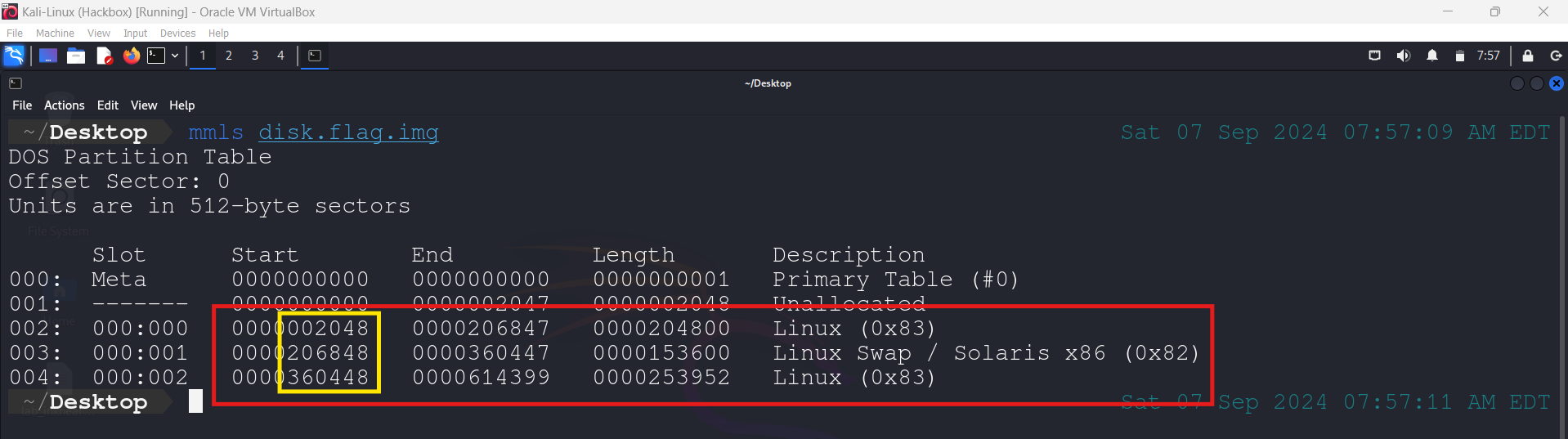
file disk.flag.img



Now we need to determine the layout of the partition table with mmls. This will provide us with the offset address for each partition in the image file.

mmls disk.flag.img

The starting offsets are 2048, 206848 and 360448 respectively as highlighted in the screenshot below.

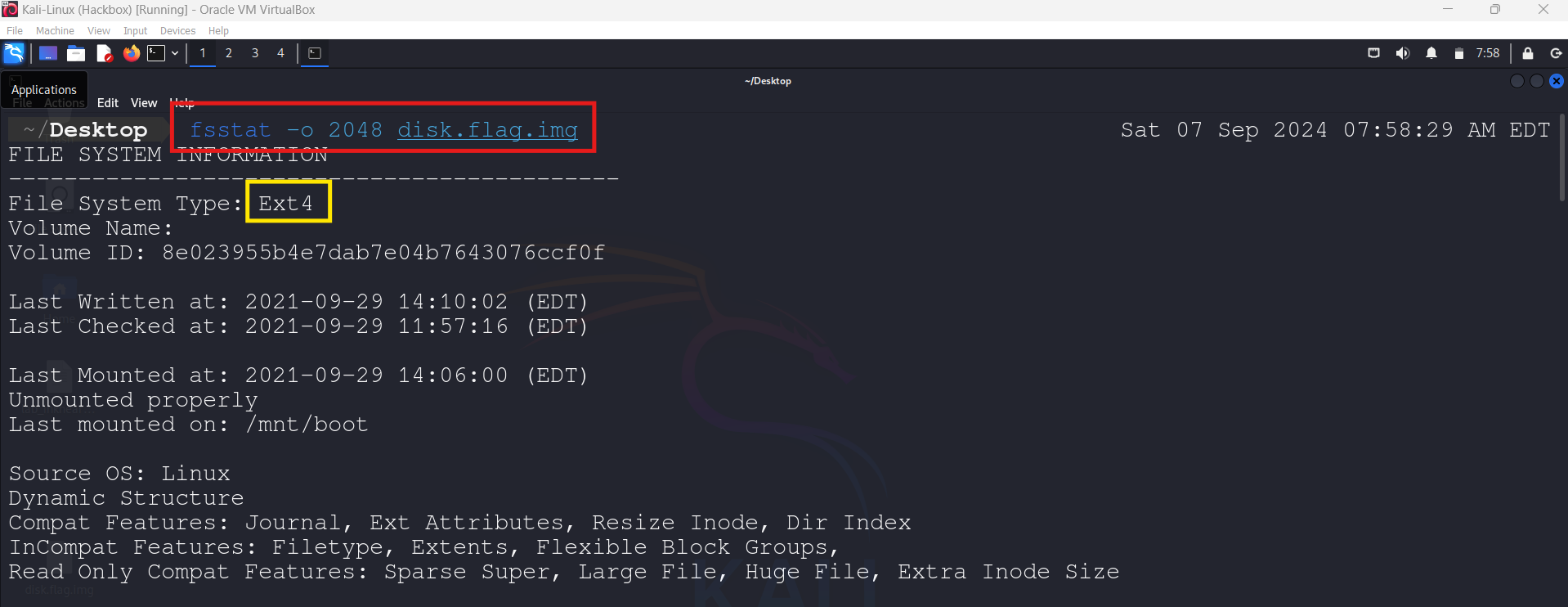


Now that we have the partition information, we can determine what kind of file system is used on the image. We can used fsstat:

fsstat -o 2048 disk.flag.img

*In the above command 2048 is starting offset of Linux (0x83)*

As we can see in the screenshot below that the file system type is **EXT4**.



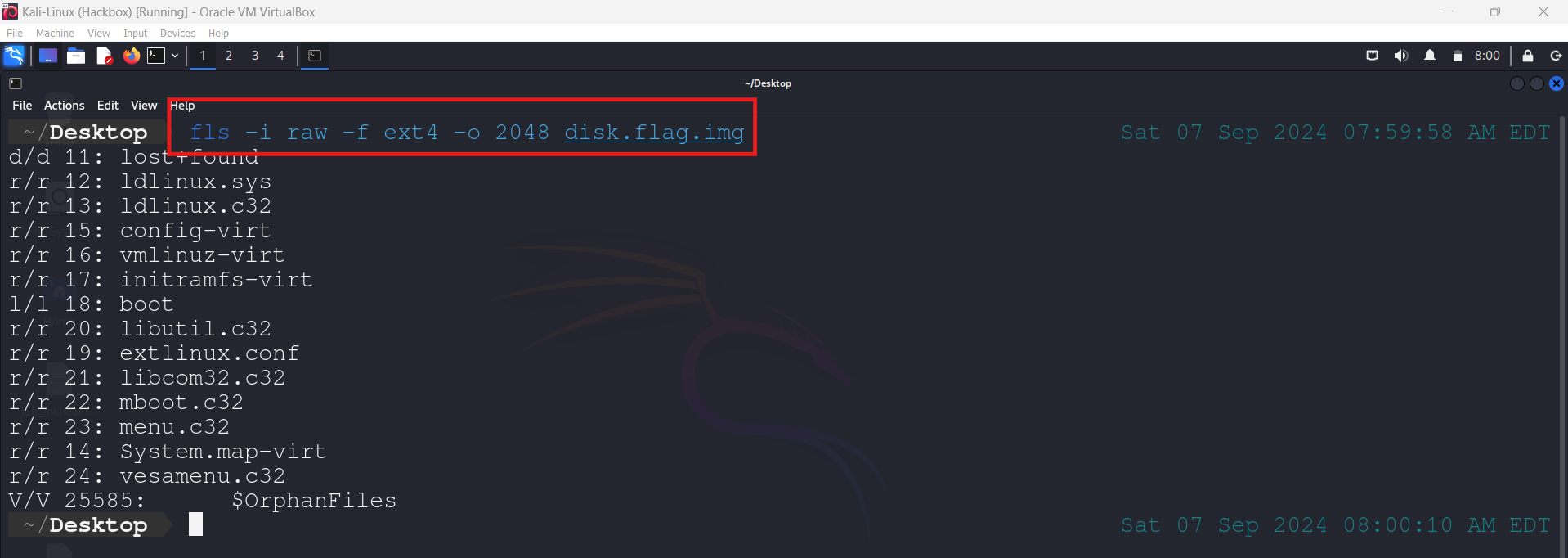
Next we use fls to list the file and directory names in each partition.

fls -i raw -f ext4 -o 2048 disk.flag.img

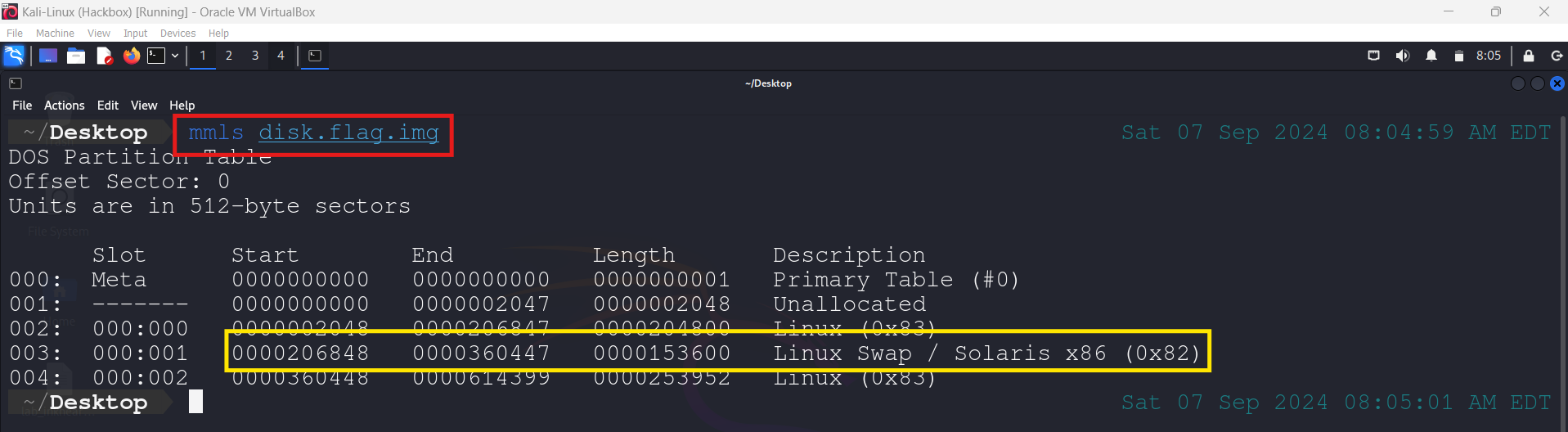
*-i is the image type*

*-f is the file system type*

There wasn’t much that seemed of interest on the first partition now we need to perform the same for second and third partition.



mmls disk.flag.img



fsstat -o 260848 disk.flag.img

The second partition in this case is Linux Swap space we can skip it for now and move to third partition.

A screen shot of a computer

Description automatically generated

mmls disk.flag.img

A screenshot of a computer

Description automatically generated

fsstat -o 360448 disk.flag.img

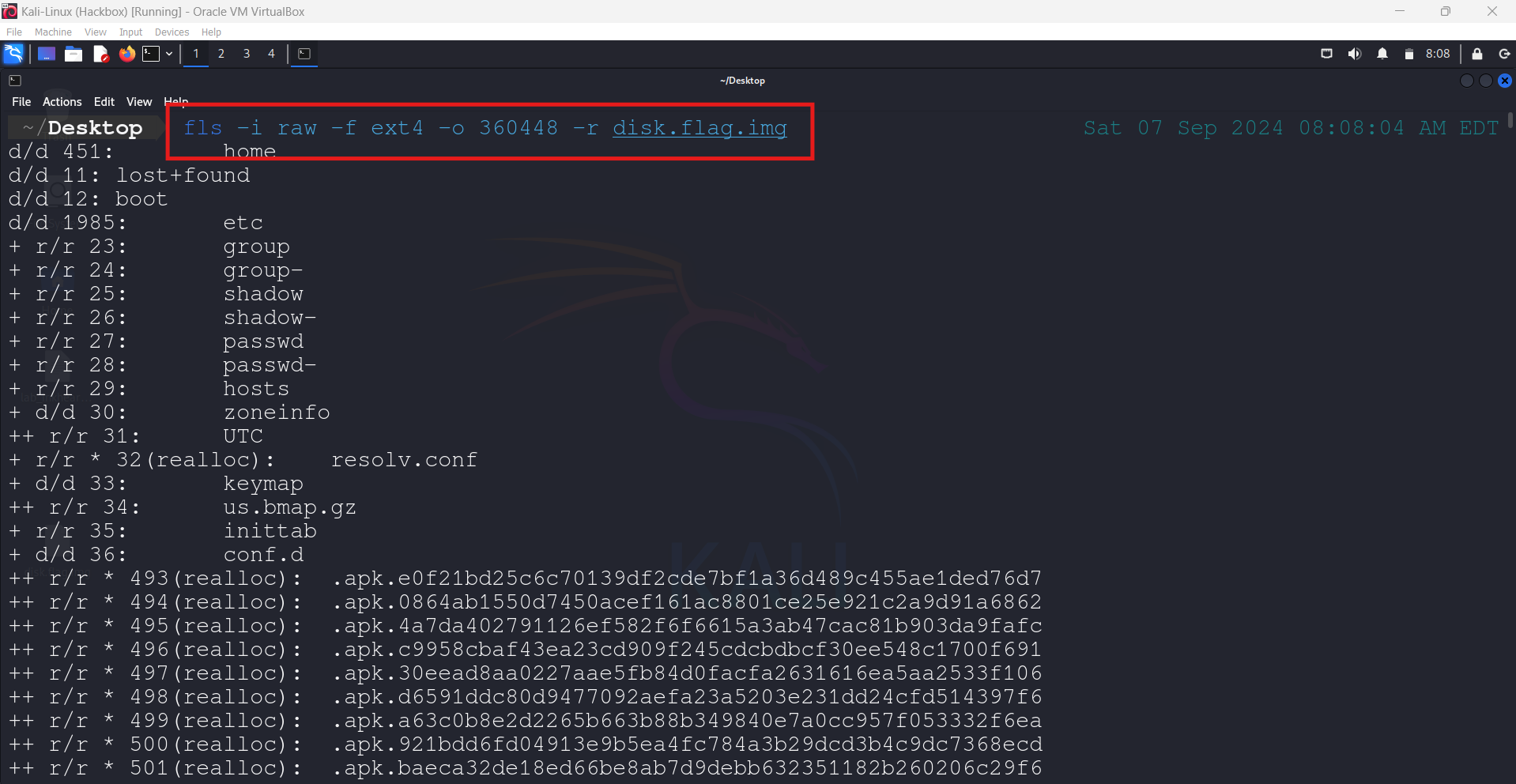
As we can see in the screenshot below that the file system type is **EXT4**.

A screenshot of a computer

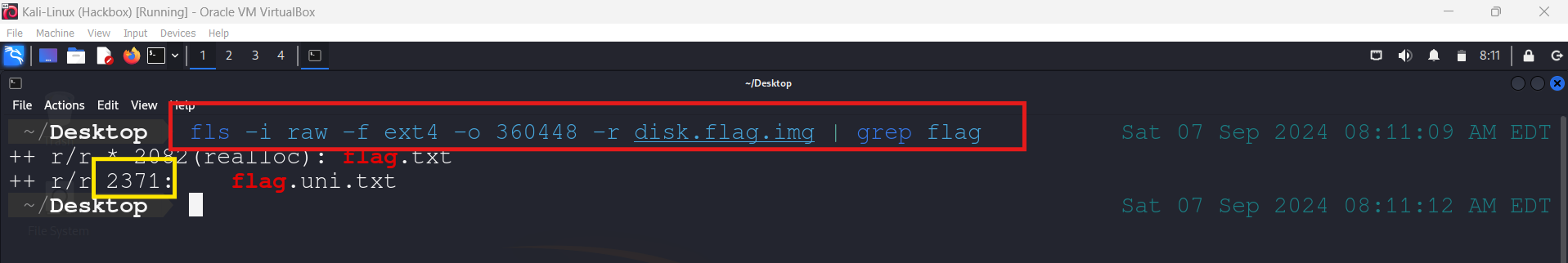
Description automatically generated

fls -i raw -f ext4 -o 360448 disk.flag.img

We run fls on the third one, we get a lot of content back as shown in the screenshot below:

 fls -i raw -f ext4 -o 360448 disk.flag.img | grep flag

As there were a lot of files so we can search for flag keyword using grep. The first result is interesting, because it found a file in unallocated space called “flag.txt” and we know this because of the asterisk next to the inode number *(highlighted in yellow)* (r/r \*). The r stands for regular file and realloc means that the metadata structure is in an allocated state still, but the file is deleted.



We can use icat to print the contents of these files to the terminal. The digits (2371) at the end of the command are the inode numbers associated with the files.

icat -i raw -f ext4 -o 360448 disk.flag.img 2371

A screen shot of a computer

Description automatically generated

**Reference Material:** <https://hackernoon.com/getting-started-with-digital-forensics-using-the-sleuth-kit-c34a3wkg>

# Tasks:

Naming Convention: i22xxxx\_Lab04.pdf

For this practical you should consider yourself to be a Forensic Analyst with a private company that carries out work on behalf of your local Police Service. You should study the scenario below and then carry out your forensic examination as instructed.

## Scenario:

*You are assisting in the investigation of a suspect named Tony Smith, who is alleged to be involved in passing forged cheques and bank drafts using the pseudonym Michael, Mike, or Mickey McNugget. Smith has been arrested in England, where it is believed, he had gone to meet up with his partner in crime, who is named Roger Jones and from whom he buys counterfeit cheque books. His laptop has been seized and examined in England. The forensic examiner has reported that the laptop is encrypted with Symantec Whole Disk encryption and Smith has refused to provide the password. The investigating officer has been to Smith’s home but only a USB device was found.*

The USB device has been imaged by a technician in your company and the image files are available for examination inside Evidence.zip file. You should carry out a forensic examination and submit a forensic report on your findings.

The report should include screenshots and explanation for every single step you followed for all the questions. Use the tools and techniques from the previous labs.

1. What is the Image File Format? (e.g., RAW, AFD, etc.)
2. What is the Volume Serial Number and Volume Name?
3. What is the File System Type? (e.g., FAT, EXT, etc.)
4. How many partitions are there?
5. Name the file with a mismatched extension. Hint: Hexed.it and Gary are close friends who share a lot with me.
6. Use Cipher Identifier if you encounter any encoded text, such as "kHrkn Bqqzon."
7. What is the password for the Password-Protected PDF?

*The password for Password-Protected PDF is “Catchme”, we’ll go through the process of finding this password in MFT Analysis Lab -> Lab 05.*

1. What are the contents of the Password-Protected PDF? Does it relate to the investigation?
2. Write a conclusion based on the investigation above.

# References:

<https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-media-file-system-forensics/>