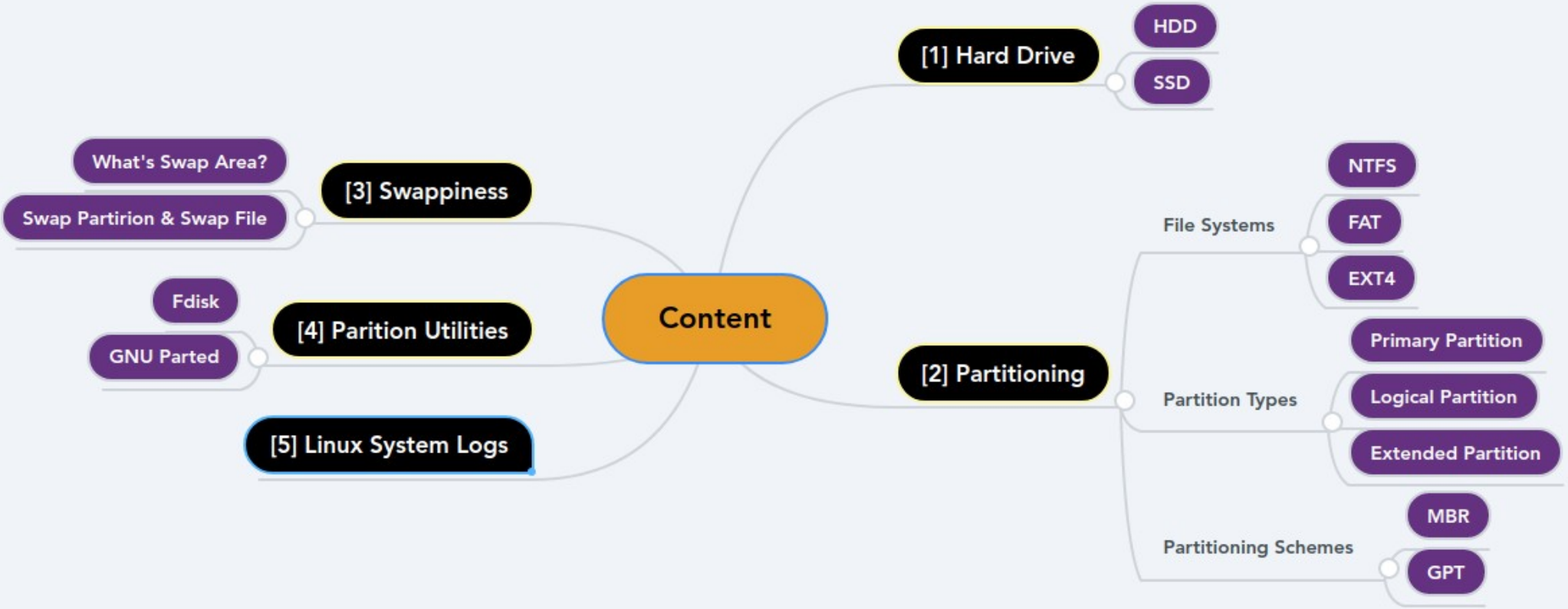
Partitions and Linux System Logs

Prepared by : Abanoub Asaad

Content


Content
[1] Hard Drive
HDD
SSD
[2] Partitioning
File Systems
NTFS
FAT
EXT4
Partition Types
Primary Partition
Logical Partition
Extended Partition
Partitioning Schemes
MBR
GPT
[3] Swappiness
What's Swap Area?
Swap Partirion & Swap File
[4] Parition Utilities
Fdisk
GNU Parted
[5] Linux System Logs

Hard Drive

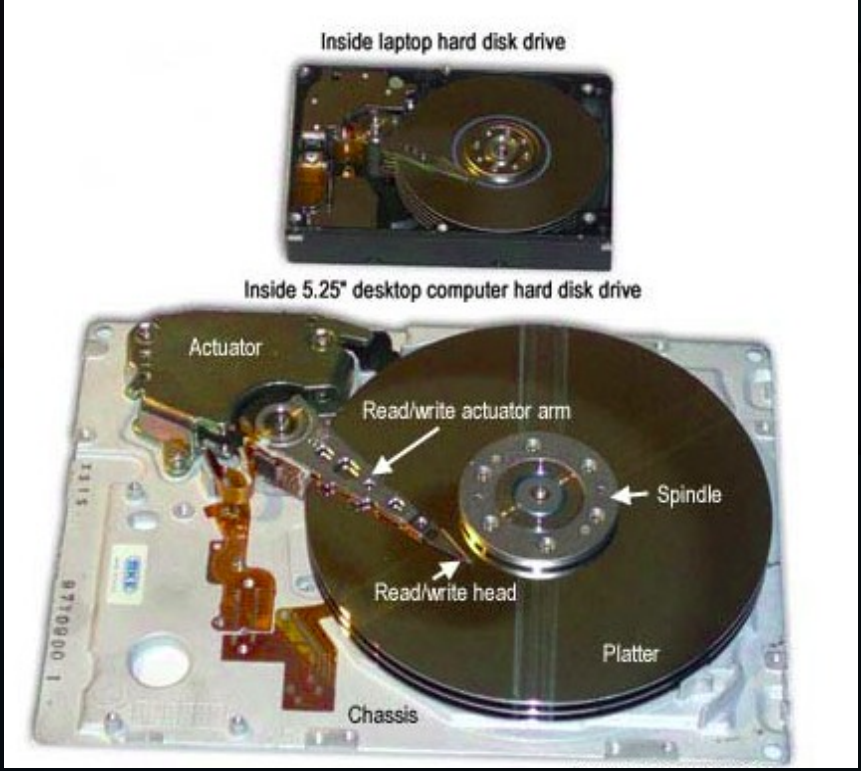
- It is a Non Volatile Storage

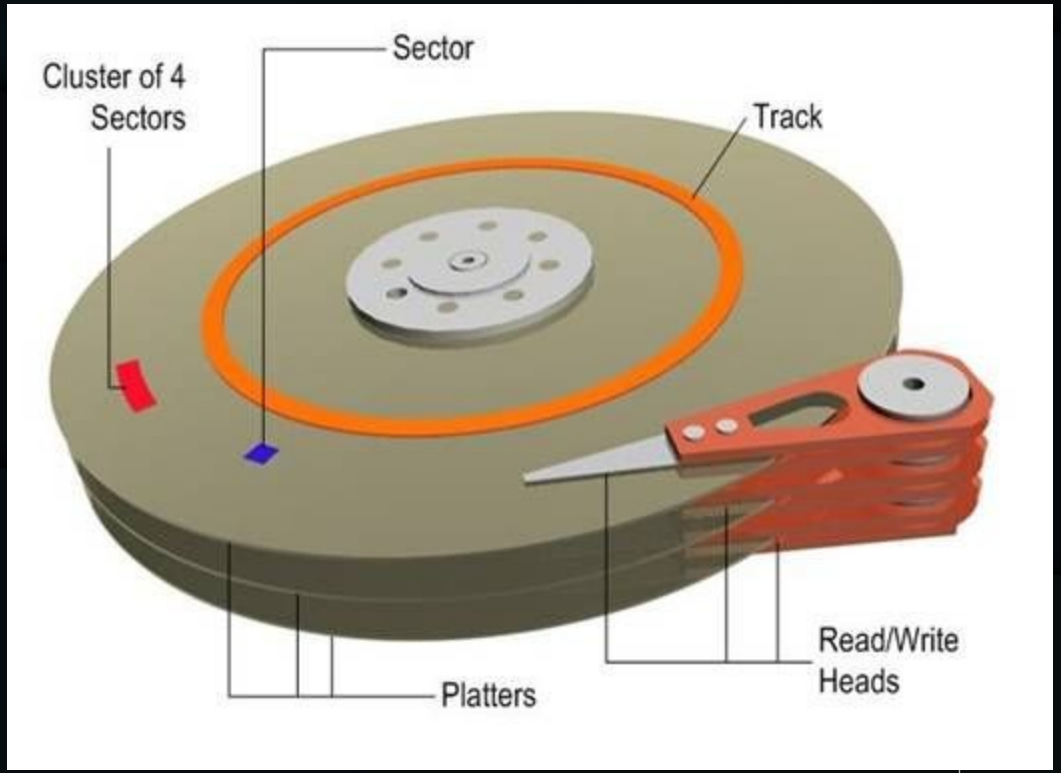
- There’s 2 types of Hard Drive :

1- HDD
2- SSD

1- HDD (Hard Disk Drive)

– Components



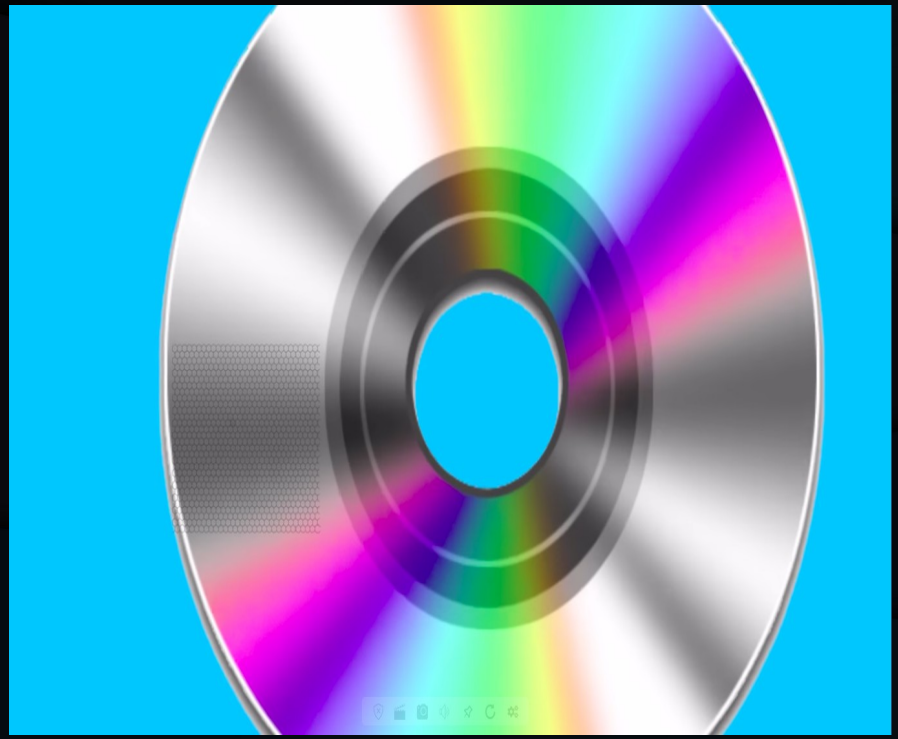


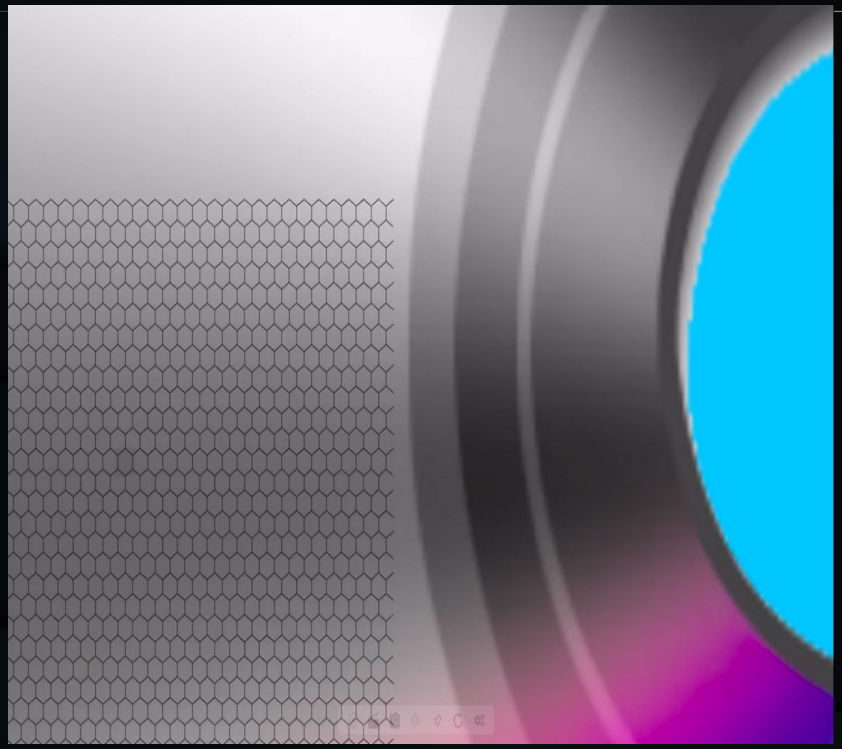
How data is stored in HDD ?

- We’re all know that data is stored with 0’s or 1’s

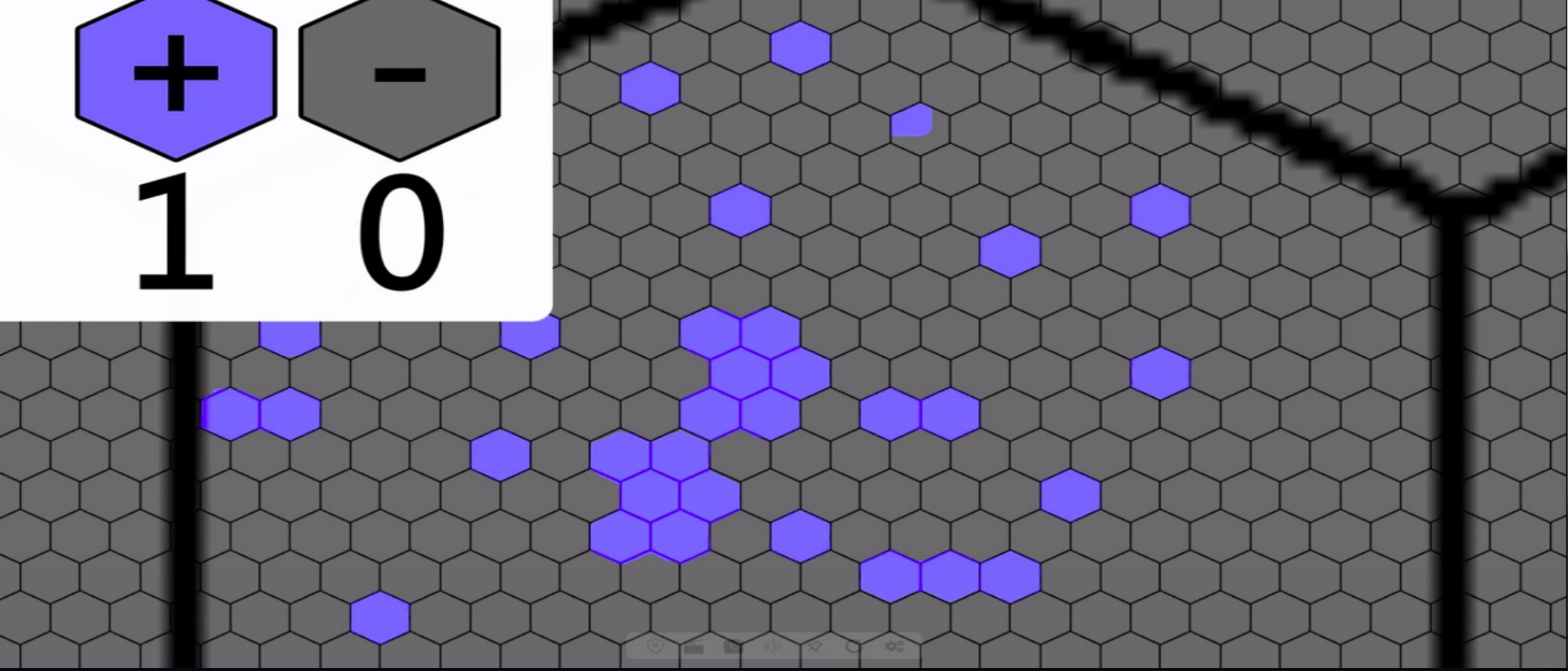
SO How data is stored in the Hard Drive ?

Using Magnets

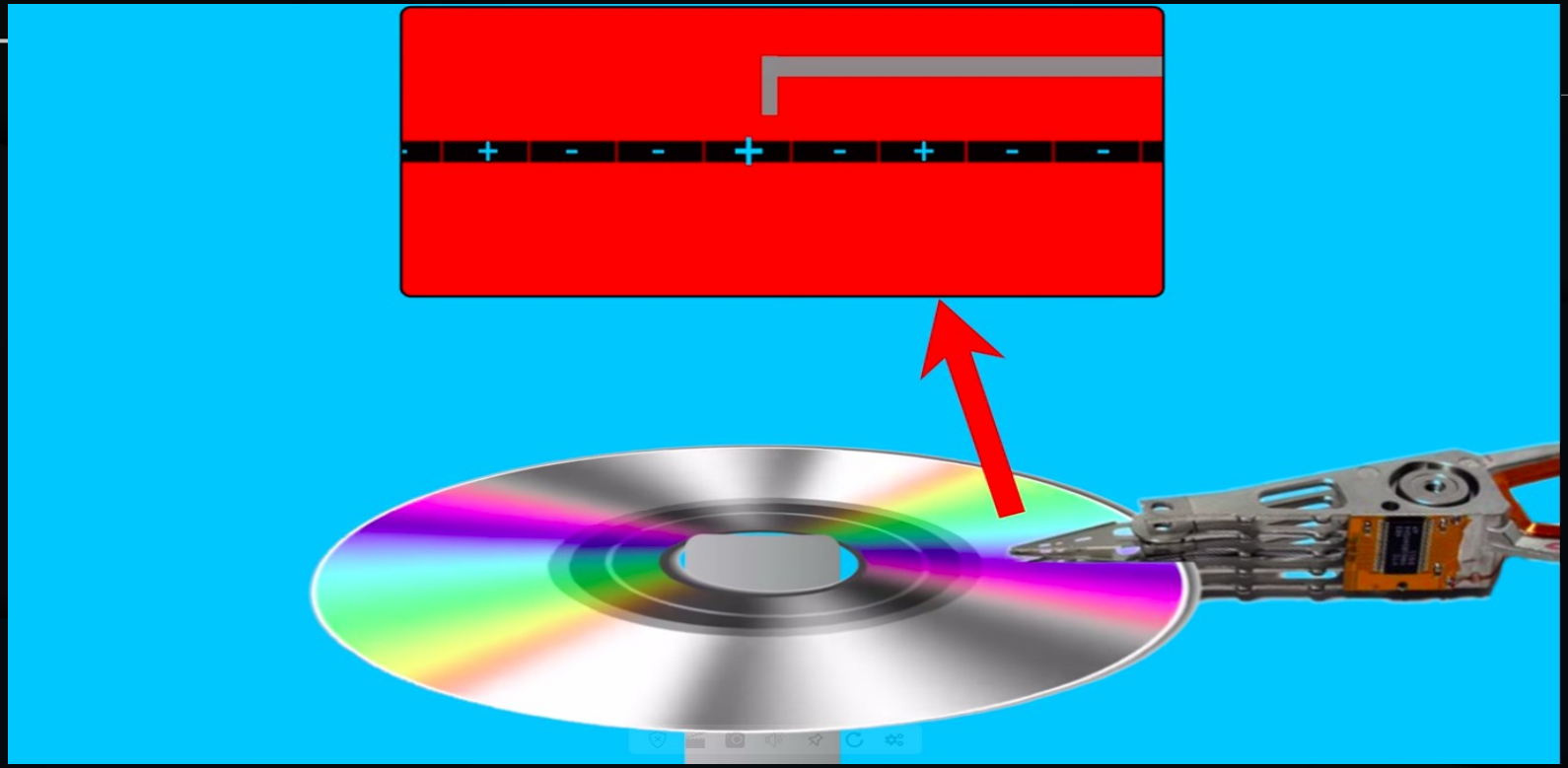




The platter (disk) contains ferromagnetic material



- Single region represents a single digit of binary
- Actuator arm : sends magnetic charges to the disk



There’s two methods what deals with data :

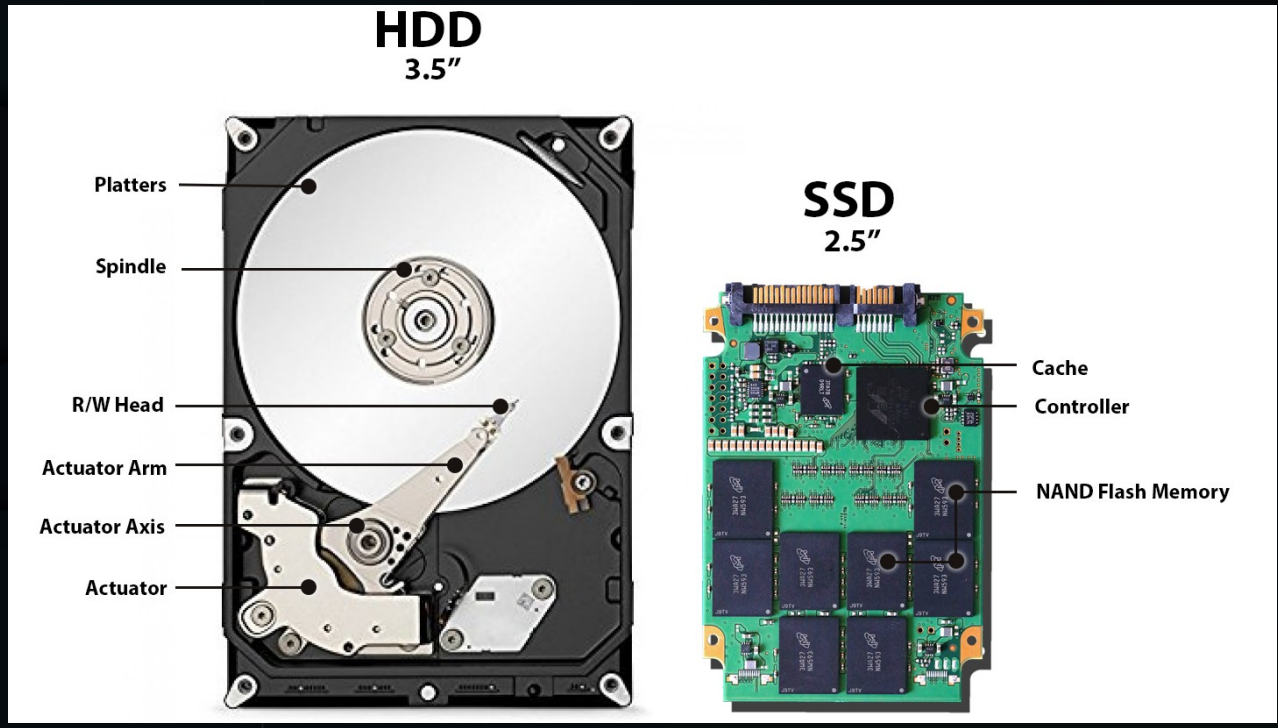
1- Writing Data

2- Reading Data.

2- SSD (Solid State Drive)

- Components

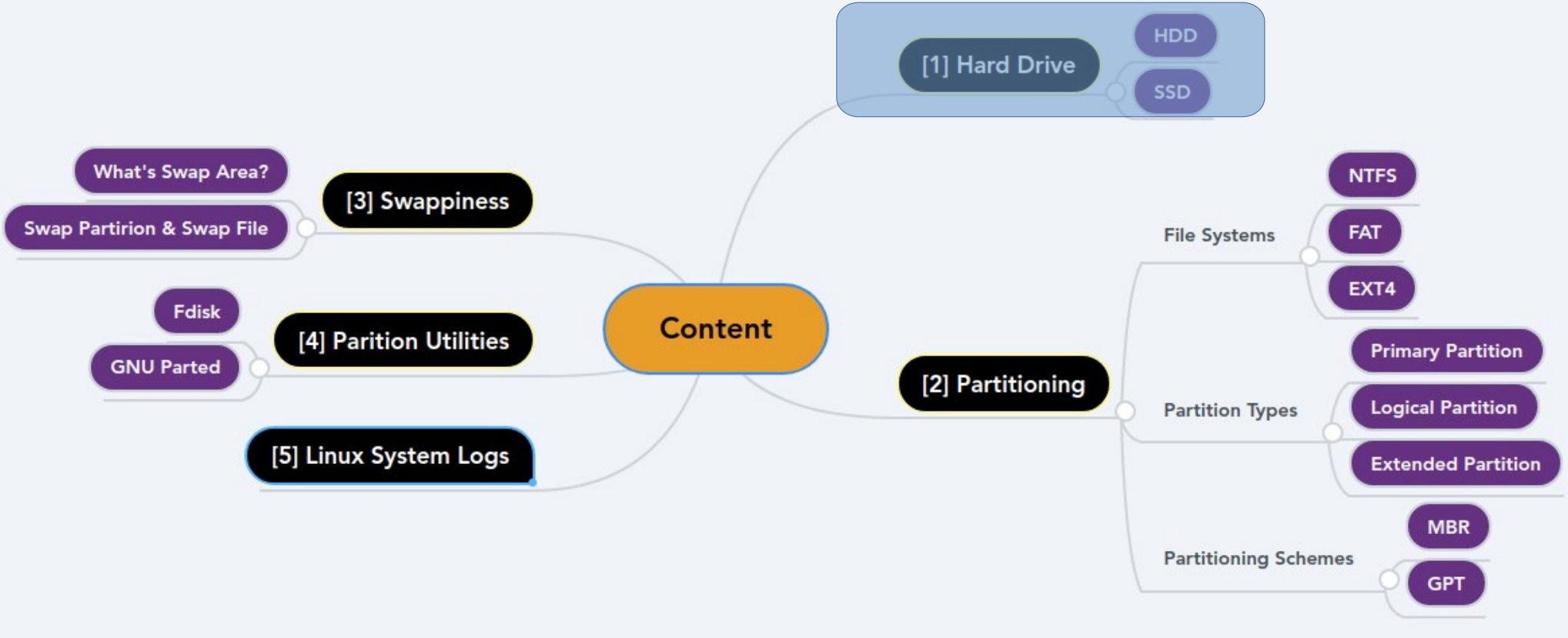
1- Cache
2- Controller
3- NAND Flash Memory



SSD has no moving parts

Why Photoshop speed in SSD is faster than HDD ?!

Content


Content
[1] Hard Drive
HDD
SSD
[2] Partitioning
File Systems
NTFS
FAT
EXT4
Partition Types
Primary Partition
Logical Partition
Extended Partition
Partitioning Schemes
MBR
GPT
[3] Swappiness
What's Swap Area?
Swap Partirion & Swap File
[4] Parition Utilities
Fdisk
GNU Parted
[5] Linux System Logs

Partitioning

- A hard disk can be divided into several partitions.

- Advantages of Partitioning :
  - 1- Organizing personal data
  - 2- Multiple operating systems
  - 3- More efficient disk space management.

File System

- Definition : is a process that manages how data is stored or accessed in the hard drive.
- Types :
  - ➔ FAT12, FAT16 & FAT32
  - ➔ NTFS
  - ➔ ExFAT
  - ➔ Ext2, Ext3 & Ext4
  - ➔ HFS, HFS+ & APFS
  - ➔ Linux-Swap will be explained later :)

– FAT12, FAT16 & FAT32

- FAT “File Allocation Table”
- Each has an increasing number of clusters, maximum file and volume sizes.
- FAT32 is the most popular one and so suitable for flash drive.

	Max file size	Max volume size
FAT12	32MB (8KB clusters)*	32MB (8KB clusters)*
FAT16	2GB/4GB**	16GB (256KB clusters)**
FAT32	4GB	32GB (Windows format) 2TB (other OS) 16TB (theoretical)

– NTFS

- NTFS “New Technology File System”
- It’s introduced in 1993 to overcome the limitations of FAT32
- It’s the most popular windows file system
- Unlike FAT32, NTFS supports permissions and encryption.

Disadvantages :

- By default NTFS volumes are read-only in Mac OS and in older Linux distros.

– ExFAT

- ExFAT “Extended File Allocation Table”
- It’s a file system introduced by Microsoft
- It’s optimized for flash memory such as USB and SD cards that larger than 32 GB.

– EXT2, EXT3 & EXT4

- In 1992, ext “extended file system” was launched for Linux
- In 1993, ext2 was released
- In 2001, ext3 was released
- In 2008, ext4 became the Linux default FS.

- Disadvantages :
  - Neither Windows or Mac OS supports ext2, ext3 or ext4.

– HFS, HFS+ & APFS

- In 1985, HFS “Hierarchical File System” was launched for Mac OS
- In 1998, HFS+ was released
- In 2017, APFS “Apple File System” is launched

- Disadvantages :
  - Neither Windows nor Linux supports HFS, HFS+ or APFS.

In the current time , What’s the suitable file system to use in Windows, Linux, Mac OS and USB drivers ?!

– Partition Types

- Primary Partition
  - is the partition where Windows OS and other data can be stored. You can only boot from a primary partition
- Logical Partition
  - is the partition that can any other data that not related to the boot
- Extended Partition
  - is a special type of primary partition but is created by a different way.

((Conversion))

– Partitioning Schemes

MBR	GPT
Stands for “Master Boot Record”	Stands for “GUID Partition Table”
Can contain up to 4 primary partitions	Can contain up to 128 primary partitions
Can access up to 2 Terabyte	Can access more than 2 Terabyte “has no limit”
Used with Old BIOS (Legacy Boot) & UEFI sometimes	Used with UEFI

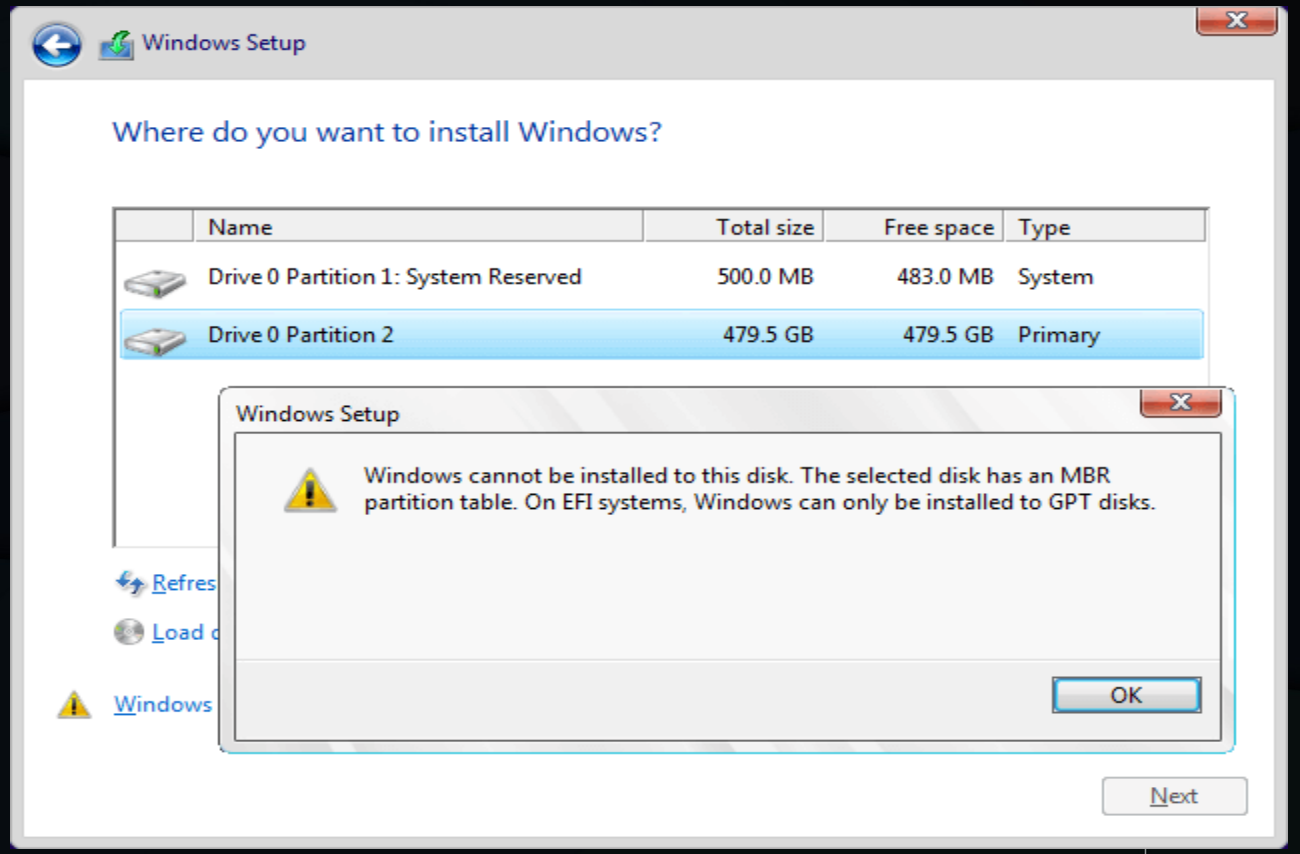
GPT is the most preferred partitioning schemes for hard disks.

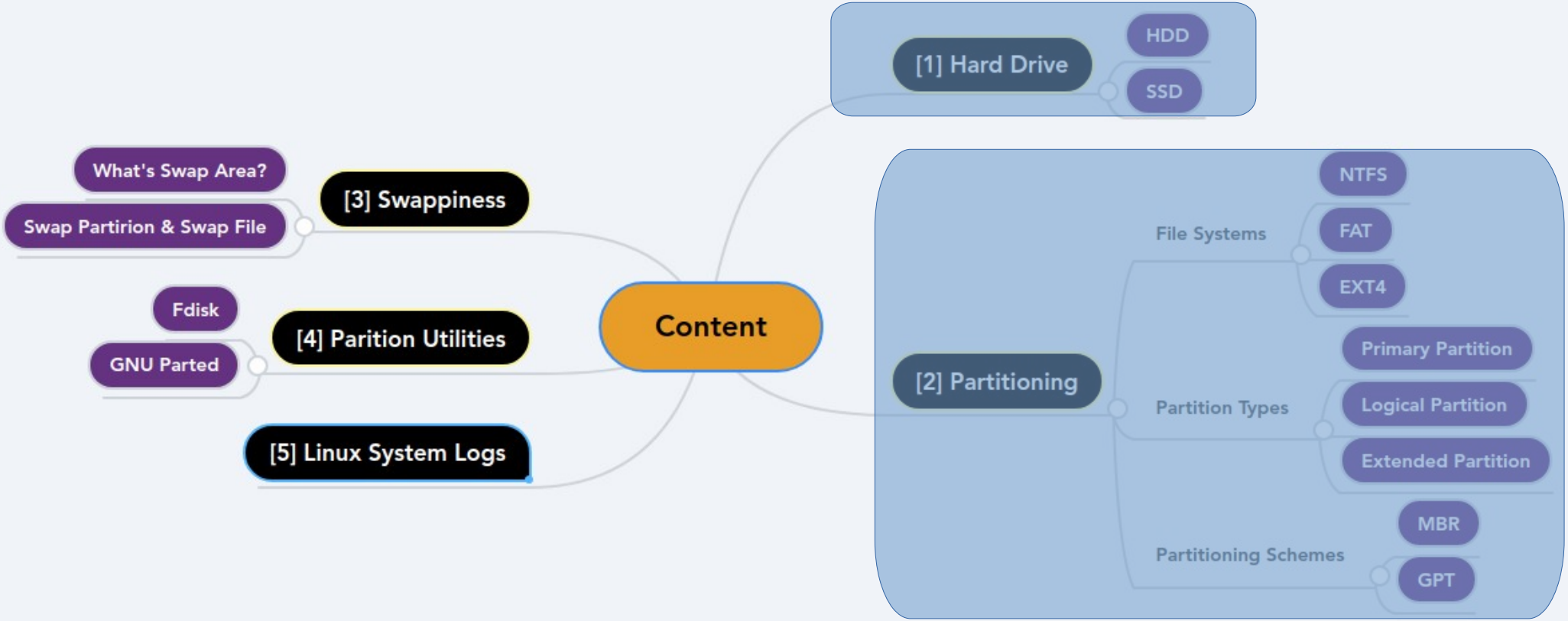
((Conversion))

Interactive Question

Have anyone faced this problem ?

How to solve it ?



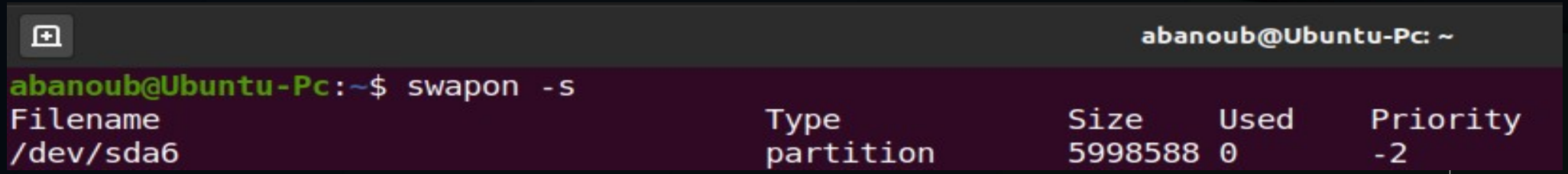

Content
[1] Hard Drive
HDD
SSD
[2] Partitioning
File Systems
NTFS
FAT
EXT4
Partition Types
Primary Partition
Logical Partition
Extended Partition
Partitioning Schemes
MBR
GPT
[3] Swappiness
What's Swap Area?
Swap Partirion & Swap File
[4] Parition Utilities
Fdisk
GNU Parted
[5] Linux System Logs

– Swappiness

- is a technique where data in RAM is written to a special location on your hard disk - either a swap partition or a swap file to free up RAM.
- Swap area is the extension of the RAM
- Swap Space :
  - ➔ Swap Partition :
    - is not easy to change and has fixed size
  - ➔ Swap File
    - You can change the size of the file any time easily.

- Advantages :
  - ➔ Swappiness saves you from crashes
- Disadvantages :
  - ➔ Swap space is much slower than RAM

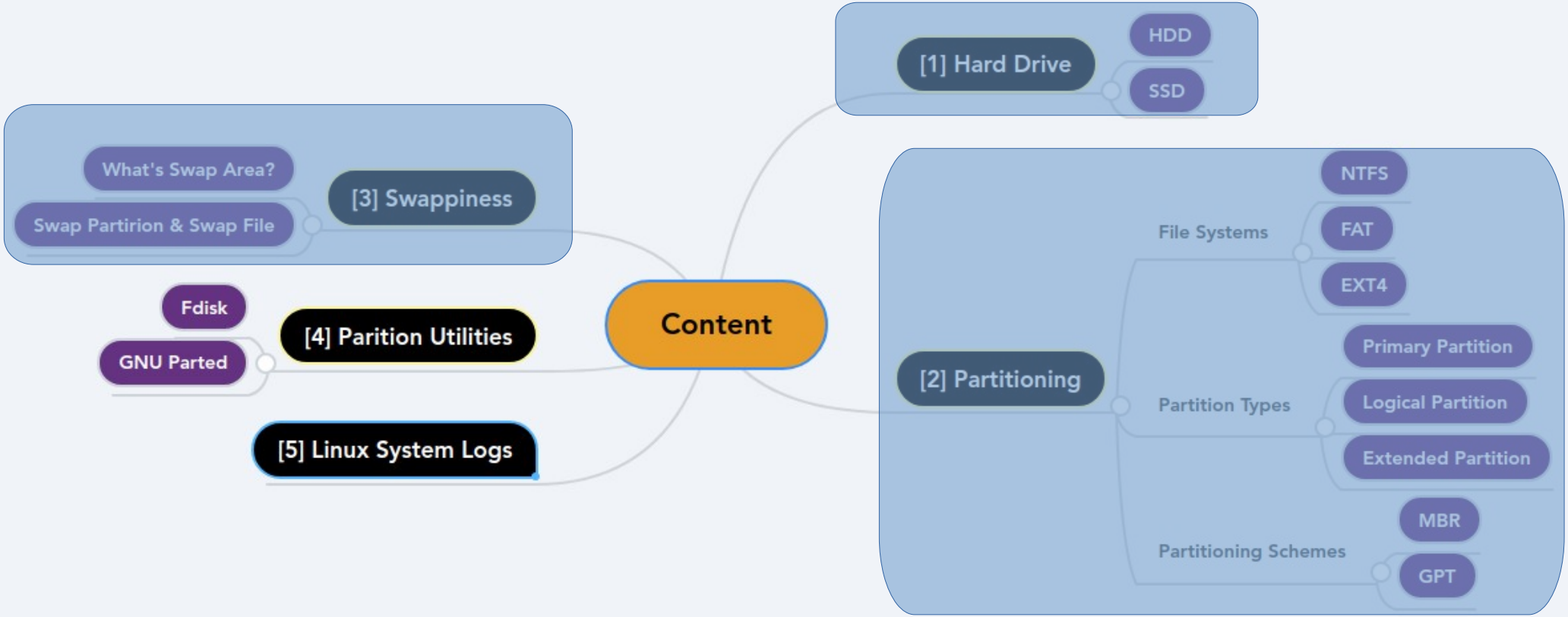
To display information about the swap partition



– What is the right amount of swap space?

Amount of system RAM	Recommended swap space
less than 2 GB	2 times the amount of RAM
2 GB - 8 GB	Equal to the amount of RAM
8 GB - 64 GB	0.5 times the amount of RAM

Let’s continue :)


Content
[1] Hard Drive
HDD
SSD
[2] Partitioning
File Systems
NTFS
FAT
EXT4
Partition Types
Primary Partition
Logical Partition
Extended Partition
Partitioning Schemes
MBR
GPT
[3] Swappiness
What's Swap Area?
Swap Partirion & Swap File
[4] Parition Utilities
Fdisk
GNU Parted
[5] Linux System Logs

– Partition Utilities

- are used as a software to manage the hard disk and its partitions
- are like Disk Management in Windows
- Types :
  - Fdisk
  - GNU Parted

1 - Fdisk

- It is a simple text-based partitioning utility
- It exists for both Windows and Linux
- You can use the fdisk utility in Linux to view, create, modify or edit partitions

To use fdisk in Linux :

- Be a super user
- Type this command : fdisk /dev/sda

Screenshot of fdisk in Linux

Running fdisk in Windows

1- Run cmd as an administrator

2- type this command : diskpart

2 – GNU Parted

- It is a simple text-based partitioning utility
- It’s a text-based partitioning utility manages the hard
- disk
- There’s a GUI-version of that software
- To use GNU Parted in Linux :

➢ Be a super user

➢ Type this command : parted /dev/sda

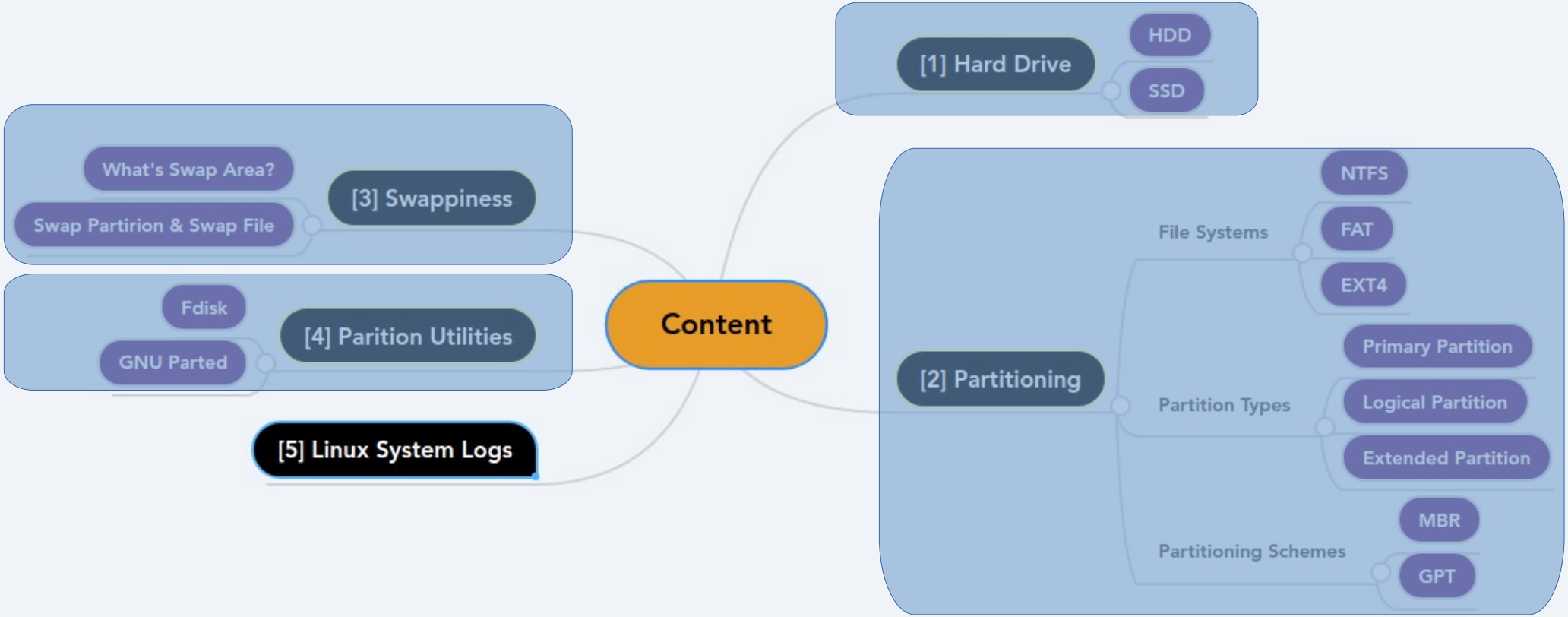
Screenshot of GNU Parted in Linux

```
root@Ubuntu-Pc:~# parted /dev/sda
GNU Parted 3.3
Using /dev/sda
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) print
Model: ATA WDC WD10SPZX-24Z (scsi)
Disk /dev/sda: 1000GB
Sector size (logical/physical): 512B/4096B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type      File system     Flags
 1      1049kB  608MB   607MB   primary   ntfs            boot
 2      608MB   215GB   214GB   primary   ntfs
 3      215GB   1000GB  785GB   extended                  lba
 5      215GB   317GB   102GB   logical   ext4
 6      317GB   323GB   6143MB  logical   linux-swap(v1)
 7      323GB   678GB   354GB   logical   ntfs
 8      678GB   1000GB  323GB   logical   ntfs

(parted)
```

Parted	Fdisk, Sfdisk
Create GPT partition table	Create DOS partition table (MBR)
Address up to 8ZB	Format up to 2TB -> 16TB
128 partition or more	Only 16 partitions
Two copies of partition table are saved (At the beginning & end of the disk)	Only one copy of partition table is stored

- So Parted is really good to use
- To view partition table :

  sudo fdisk -l or sudo parted -l


Content
[1] Hard Drive
HDD
SSD
[2] Partitioning
File Systems
NTFS
FAT
EXT4
Partition Types
Primary Partition
Logical Partition
Extended Partition
Partitioning Schemes
MBR
GPT
[3] Swappiness
What's Swap Area?
Swap Partirion & Swap File
[4] Parition Utilities
Fdisk
GNU Parted
[5] Linux System Logs

– Linux System Logs

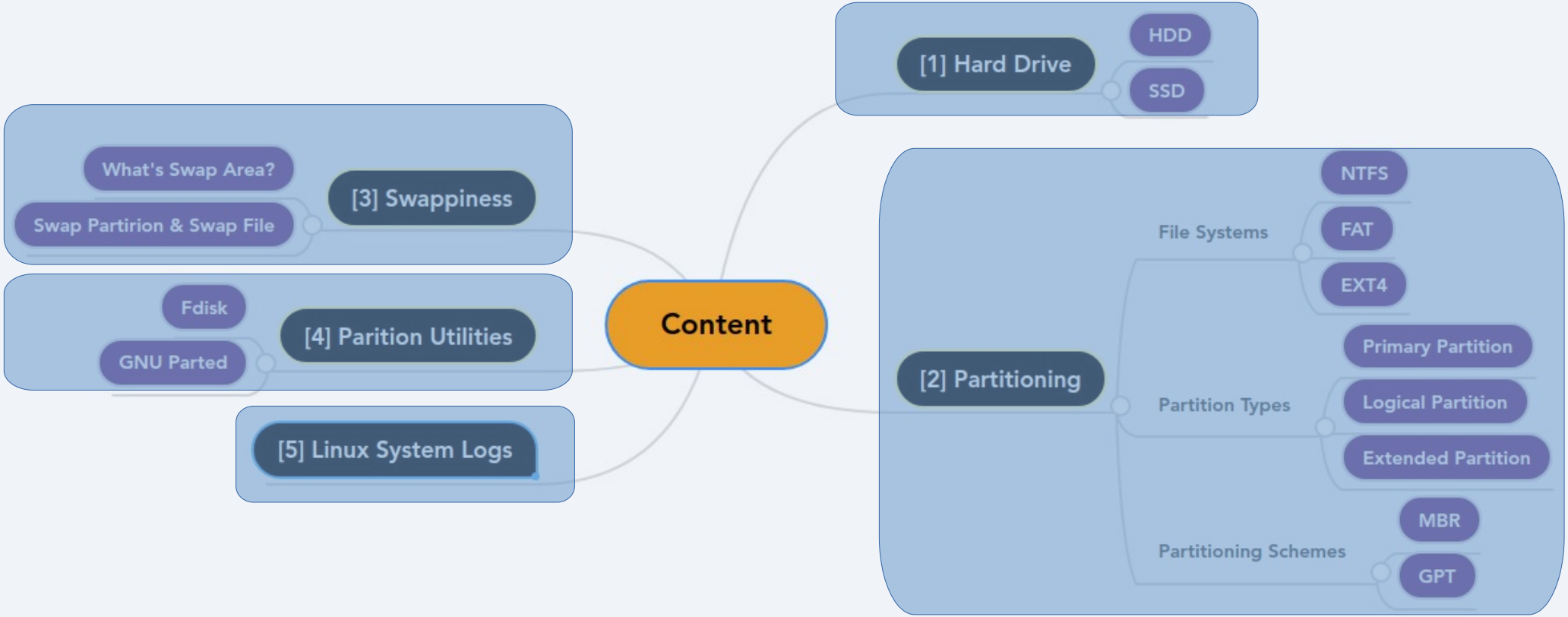
- Log entries are like footprints
- A log file : is a file contains entries with information about some past event
- Most logs files are in plain text
- Most logs files reside in the /var/log directory and the other log files in /var/run
- Log analysis is important in Troubleshooting
- Troubleshooting is a form of problem solving

– Log Files

Path	Importance
/var/log/messages **In some distros** /var/log/syslog	Shows messages related to the system
/var/log/dmesg	Shows messages from hardware devices and drivers
/var/log/secure	Shows messages related to authentication messages
/var/log/auth.log	Shows messages related to System authorization
/var/log/kern.log	Shows kernel messages
/var/log/cron	This log file records information on cron jobs

– Log Files cont..

Path	Importance
/var/log/boot.log	Contains messages generated during the boot
/var/log/daemon.log	Contain messages from processes running in the background
/var/log/apt	record activities of pakcage managers for apt (for Debian and Ubuntu)
/var/log/dpkg.log	record activities of pakcage managers for dpkg
/var/log/yum.log	record activities of pakcage managers for yum (for)
/var/log/wtmp /var/log/btmp /var/run/utmp	Contain login records file


Content
[1] Hard Drive
HDD
SSD
[2] Partitioning
File Systems
NTFS
FAT
EXT4
Partition Types
Primary Partition
Logical Partition
Extended Partition
Partitioning Schemes
MBR
GPT
[3] Swappiness
What's Swap Area?
Swap Partirion & Swap File
[4] Parition Utilities
Fdisk
GNU Parted
[5] Linux System Logs

It’s DONE :)