Какво е това сектор, клъстър : <https://en.wikipedia.org/wiki/Disk_sector>

Файловете се разделят на клъстъри. Размера на клъстъра се определя при форматиране и варира от 1 sector (512Bytes) до 128 sectors (64KB). В някои случаи минималното е 8 sectors.

==================================================================

Начално зареждане за Windows 10:

BIOS:

* POST (Power On self Test)
* POST Beep Codes
* Bootstrap – търси кое е активното устройство зададено от настройките в BIOS (boot device priority). Може да бъде форсиран с някой клавиш според дъното (примерно F12) за директно влизане в Boot Menu за избор на устройство.

Ако активното устройство е HDD или SSD

* MBR или GPT (GUID Partition Table)

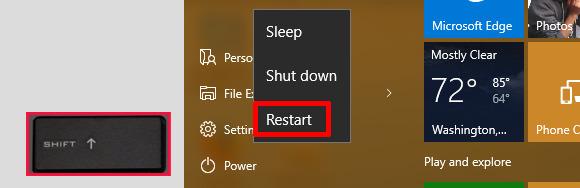
Порчита го и търси файл за качване в RAM и служи за зареждане на OS. За win10 това е файлът bootmgr (Boot Manager). Зарежда файловата система (NTFS – от по новите версии). Първоначално bootmgr проверява за хибернация или за заспиване на ОС. Ако е така извиква winresume.exe

Ако не - монтира дяла BCD(Boot Configuration Data) (за MBR) или EFI (за UEFI Unified Extensible Firmware Interface BIOS със GPT). Този дял е създаден при инсталацията и е с размер 100MB. Съдържа информация за други имиджи (указатели към други ОС). От EFI bootmgr конструира Boot-Selection Menu за избор на OS, ако е само един не конструира нищо.

* Потребителя избира ОС.
* //Тук се превключва в 64 битов режим
* Bootmgr зарежда и предава контрола на winload.exe
* winload.exe зарежда NTOSKRNL.EXE (ядрото на ОС) и HAL.DLL (**"Hardware Abstraction Layer DLL**), boot drivers и системните регистри
* NTOSKRNL.EXE се стартира в две фази :
  + Самоинициализация, стартира видео драйвера (появява се логото), стартира дебъгера и след това:
  + Инициализира системата (зарежда драйверите) и старитра Windows Session Manager->
    - Зарежда виртуалната памет
    - Останалата част от регистрите
    - Services and controller app
    - Client server Runtime Process – управлява работата на win приложенията
    - Windows Logon application: ->
      * За влизане и излизане от системата
      * И при равилно логване се старита Local Security Authority Process – поддържа цялата сигурност в системата
        + Зарежда се Desctop и Auto Run

======================================================================

Влизане в Safe Mode за Windows 10



1. Click or tap the *Start* button*,* and then the *Power* button*.* Hold down the **Shift** key when you select *Restart.*
2. In the resulting, full-screen menu , select *Troubleshoot>Advanced options>Startup Settings.*
3. In the Startup Settings screen, tap the *Restart* button. The PC will reboot, and bring you to a Startup Settings screen*.*
4. Use the arrow keys on your keyboard to select *Enable Safe Mode* or *Enable Safe Mode with Networking*.

Note: If the system can't load the necessary configuration more than two times, the system will direct the display to Windows RE(Recovery environment).

=================================================================

Разделяне на дялове:

За MBR са възможни до 4 primary partitions или 3 primary + 1 extended (също primary) дял, който съдържа произволен брой логически дялове. Ограничението на MBR е до 2TB за дял.

За windows броя на дяловете формално се ограничава до 26 (въпреки че е заобиколимо), според броя на буквите в азбуката, които се дават за имена на отделните дялове.

За инсталациите се изискват primary дялове (например за Win , файлът bootmgr трябва да е на primary дял).

Спецификацията EFI предлага GUID Partition Table (GPT) която се поддържа от всички съвременни ОС. GPT e широко използван за HDD и SSD дискове и е част от стандарта UEFI.

Максималния брой дялове за GPT e 128.

Демонстрация на разделяне на дялове от Computer Management -> Disk Management

(This Ps -> Manage)

==============================================

Windows Registry

Йерархична база данни за всички конфигурационни настройки и опции на windows. Организирана е чрез два типа основни елементи: Keys и Values. Ключовете съдържат обекти близки до директориите, докато параметрите са подобни на файловете. Ключовете могат да съдържат параметри и подключове. Параметрите имат имена и стойност.

За редактиране на регистрите се използват подходящи програми като

Regedit.exe (от Run -> regedit)

Regedt32.exe (от Run -> regdt32)

За win 10 и с двете команди се отваря пограмата Registry Editor.

Регистрите са организирани йерархично чрез 5 главни ключа с префикс HKEY. “H” идва от hive (кошер).

HKEY\_CLASSES\_ROOT (HKCR) - Съдържа информация за регистрираните данни от приложения, като например файлови асоциации.

HKEY\_CURRENT\_USER (HKCU) - Съдържа настройки за текущият потребител на системата. Този ключ се съдържа в ключа HKU

HKEY\_LOCAL\_MACHINE (HKLM) – Това е най-големия ключ и съдържа настройки, отнасящи се за локалният компютър, както за хардуера, така и за софтуера.

HKEY\_USERS (HKU) - Съдържа съответстващи на HKEY\_CURRENT\_USER ключове, но за всички налични потребители на системата.

HKEY\_CURRENT\_CONFIG (HKCC) - Съдържа информация, събрана по време на работата на операционната система. Информацията се обновява при при всяко зареждане на операционната система.

----

Примери:

Разглеждаме ключа:

[HKEY\_CURRENT\_USER\Control Panel\Desktop]

* и параметрите CursorBlinkRate, MenuShowDelay, Wallpaper

[HKEY\_CURRENT\_USER\Control Panel\Mouse]

* някои от параметрите там.
* "MouseHoverTime" – колко време да се изчака за popup

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control]

* "WaitToKillServiceTimeout"

Може да проментм стойността на MenuShowDelay

Ако искаме да се стартира програма (например калкулатора) от Startup:

Отиваме в ключа:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

В полето в дясно -> [десен бутон] -> New

Разглеждаме какви варианти има. Избираме string value с име Calc

Два пъти на параметъра и слагаме Value Data: calc.exe

//calc.exe е програма от win компонентите и е с глобално име, за другите програми трябва да се посочи пълния път.

Ако искаме само за текущия потребител може да се окаже само в ключа:

HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Програмите от startup могат да се забранят от Task Manager -> Startup

От Регистрите на посочения ключ ги затриваме изцяло.

===================================================

Файлови системи:

Какво е файлова система и за какво всъщност служи?

Разглеждаме файловата система NTFS (New Technologies File Sysytem).

https://technet.microsoft.com/en-us/library/cc781134(v=ws.10).aspx

Тази файлова система е много по-сложна от предшественика FAT. Едно от многото ограничения на FAT (например 32) е максималния размер за дял (също и за файл), който може да адресира. В случая е 2^32 бита или приблизително 4GB.

NTFS е с коренно различна структура и подържа допълнително компресия, криптиране, журнал (дневник), могат да се правят твърди и символни връзки (чрез mklink – ако е инсталирано). Всеки NTFS дял (partititon) съдържа файлове, директории, bitmaps и други структури от данни. Всеки дял е организиран като линейна последователност от блокове (клъстъри) които имат фиксиран размер и се определят при форматиране (от 512B – 64KB). Повечето NTFS дискове използват 4KB клъстъри, като компромис между голям блок (за ефективен трансфер) и малък блок (за намаляване на вътрешната фрагментация).

Основната структура от данни за един NTFS дял е MFT (Master File Table), която е линейна последователност от записи с фиксиран размер (1KB). Всеки MFT запис описва един файл или директория. Той съдържа името (255 unicode знака), файловите атрибути , дата на последно модифициране, както и списък с адресите на всички блокове. Ако файла е изключително голям се използват няколко записа от MFT. Един файл може да нараства до максимум 2^48 записа. MFT файла може да се разположи където е необходимо по самия дял и има възможност за заобикаляне на дефектиралите сектори.

Първите 16 записа от MFT са резервирани за NTFS метафайлове, чийто имена започват с $. Ето кратко описание за по-важните файлове:

$MFT – описва къде къде се намира MFT файла, т.е. самия себе си и съдържа информация за блоковете за да може системата да го открие. Windows се нуждае само от първия блок, а той се намира в boot блока при форматиране с NTFS.

$MFTMirr – копие на първите няколко записа от $MFT – обикновено 4. Те са критични и се ползват в случай, че $MFT е нечетим.

$LogFile – съдържа системния дневник или transaction log на всички действия – добавяне или изтриване на директория, промяна на атрибути и други . Този файл се ползва за възстановяване (faster recovery) на файловата система при крашване и заради него тя се нарича журнална.

$AttrDef – съдържа дефиниции за атрибутите.

. – това е кореновата директория

$Boot – съдържа информация (bootstrap code) за къде се намира файлът BootMgr. Това е и първия клъстър от дяла.

$BadClus – съдържа информация за всички клъстъри, които са маркирани, че имат лоши сектори .

-------

NTFS може да използва компресиране на файлове. За целта се използва модификация на Лемпел-Зиф алгоритъма – LZNT1.

---------

NTFS може да криптира файлове.

----------

За да може други ОС да четат дялове форматирани с NTFS се използва драйвера NTFS-3G.

Максималния размер за един дял зависи от partition таблицата и от размера на един клъстър. Ако се използва MBR ограничението е до 2TB. За по-глеми дялове трябва да се използва GPT, като при него ограничението е от конкретните ОС и обикновено е до 256TB (засега). За буутване от GPT дял се изисква UEFI и 64-битова поддръжка.

-----

За да се определи размера на клсътъра използваме следната команда в Command Prompt (Admin):

fsutil fsinfo ntfsinfo C:

Това е посочено в Bytes per cluster

-----------------

Тъй като в процеса на работа и най вече от променяне по файловете, по диска се появяват фрагменти. Т.е. частите на файловете са разпръснати и при отваряне ОС трябва да ги сглобява всеки път. Затова е удачно това да бъде оптимизирано.

Control Panel -> Administrative tools -> Defragment and Optimize Drives -> Optimize (но зависи от състоянието на диска ще отнеме различно време).

Също от administrative tools може да се използва Disk Cleanup

---------------------

File Auditing:

https://www.youtube.com/watch?v=ZAudZvgZ1aE

==================================================

System Restore - НЕ

System Backup - НЕ

==================================================

Hirens Boot USB -НЕ, последната версия е от 2013

==================================================

Computer Forensics

==================================================

Multiple desctops

==================================================

Stream Video – win 10

==================================================

Restore files with File History - НЕ

==================================================

Mount - монтиране на файлови системи. Десен бутон на някой .iso файл -> mount, вместо използване на програми като Magic Disk, Alcohol и др.

==================================================

Mozilla Firefox -> New Private Window

За скриване на локализацията (т.е. анонимност) може да се използва връзка с Tor Browser.

https://en.wikipedia.org/wiki/Tor\_(anonymity\_network)

==================================================

Live USB с Linux

Програма Rufus

https://www.ubuntu.com/download/desktop/create-a-usb-stick-on-windows

===================================================