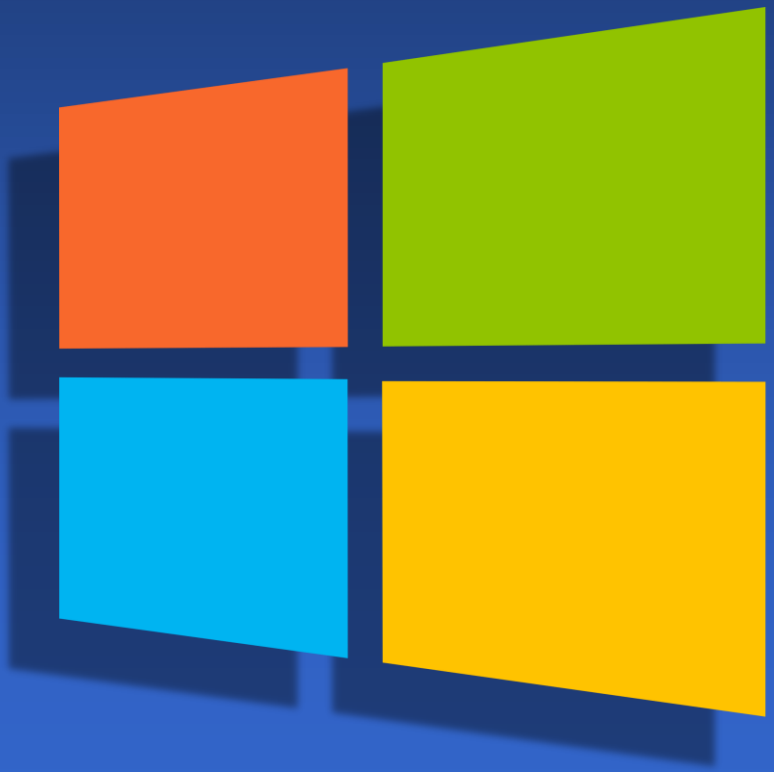
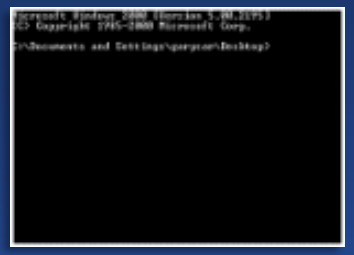
Use & Admin Windows
Survival Kit – 2 STORAGE



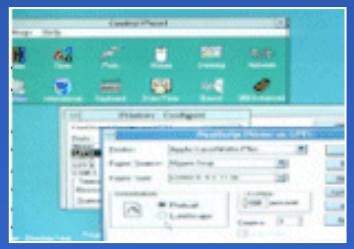
2 - Storage

Windows file system

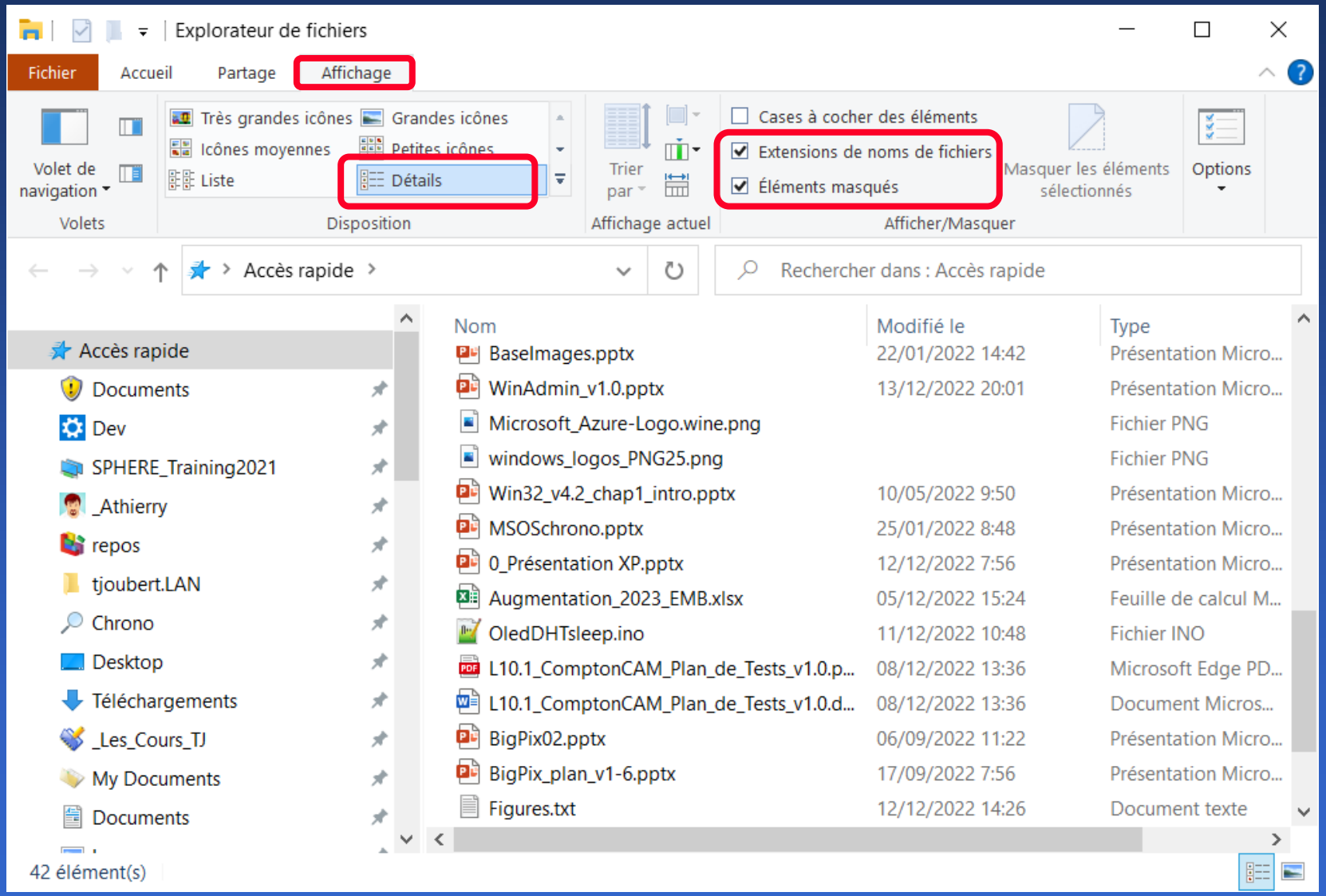
- Inherited from DOS (!Unix)
  - Not case sensitive
    - `foo.exe ~ FOO.EXE ~ Foo.exe`
  - Volume letter prefix (`C:`, `D:` etc.)
  - Separator symbol = `\`
  - 3 letters extensions `.EXE .JPG .HTM etc.`
  - Script files `.BAT` (execute !..)
  - Command line interface (`DIR`, `XCOPY`, `CD` ...)



- Windows evolutions
  - Long file names *(including spaces)*
  - Standard extensions `.JPEG .HTML`
  - Huge files (> 2Gb)



Explorer



Files

- **User data**
  - Images
  - Sounds
  - Documents
  - Downloads

```
C:\users\username
      \Pictures
      \Music
      \Documents
      \Downloads
```

- **User applications**
  - 32-bits
  - 64-bits

```
C:\
      \Program Files (x86)
      \Program Files
```

- **System apps & data**
  - Configuration
  - Programs, etc.

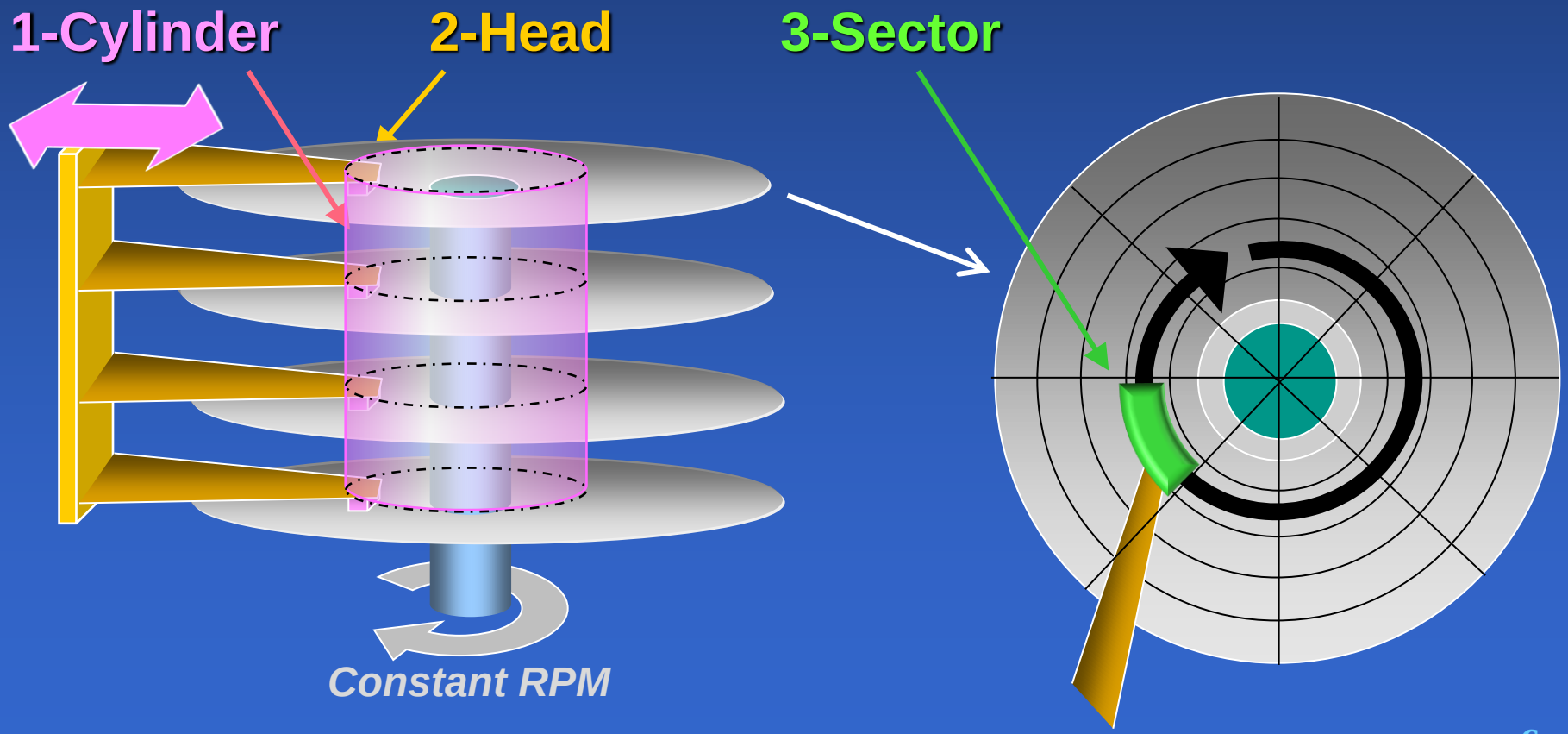
```
C:\Windows
      \System32
```

- **Shortcut**
  - Access to a file

```
C:\users\username\Desktop
                      \cmd.lnk
```

Hard Drive structure

- Magentic surface
  - One HEAD per magnetic surface
  - Read/Write unit is a SECTOR
  - C-H-S referential of each sector

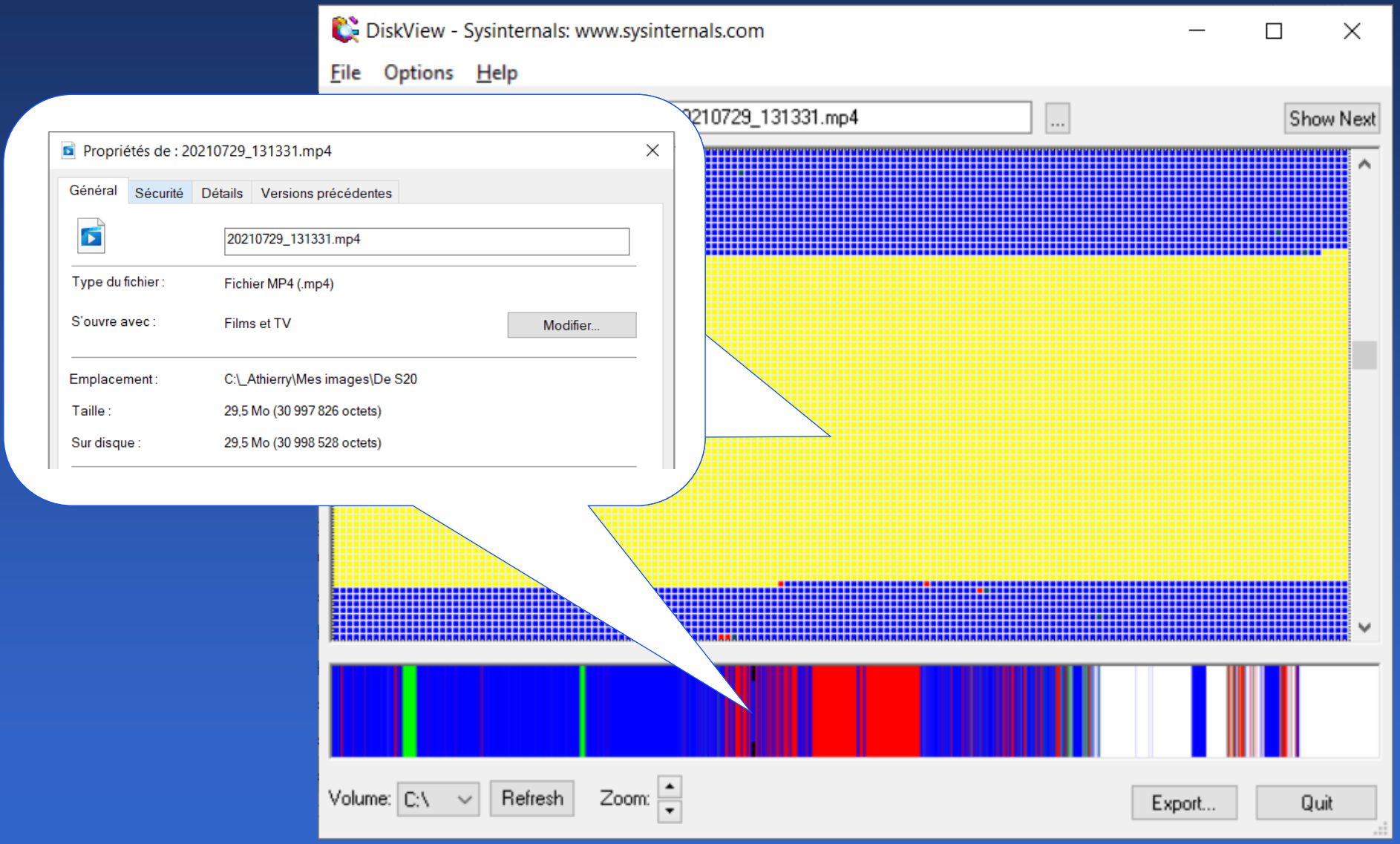


FLASH storages

- All have sectors

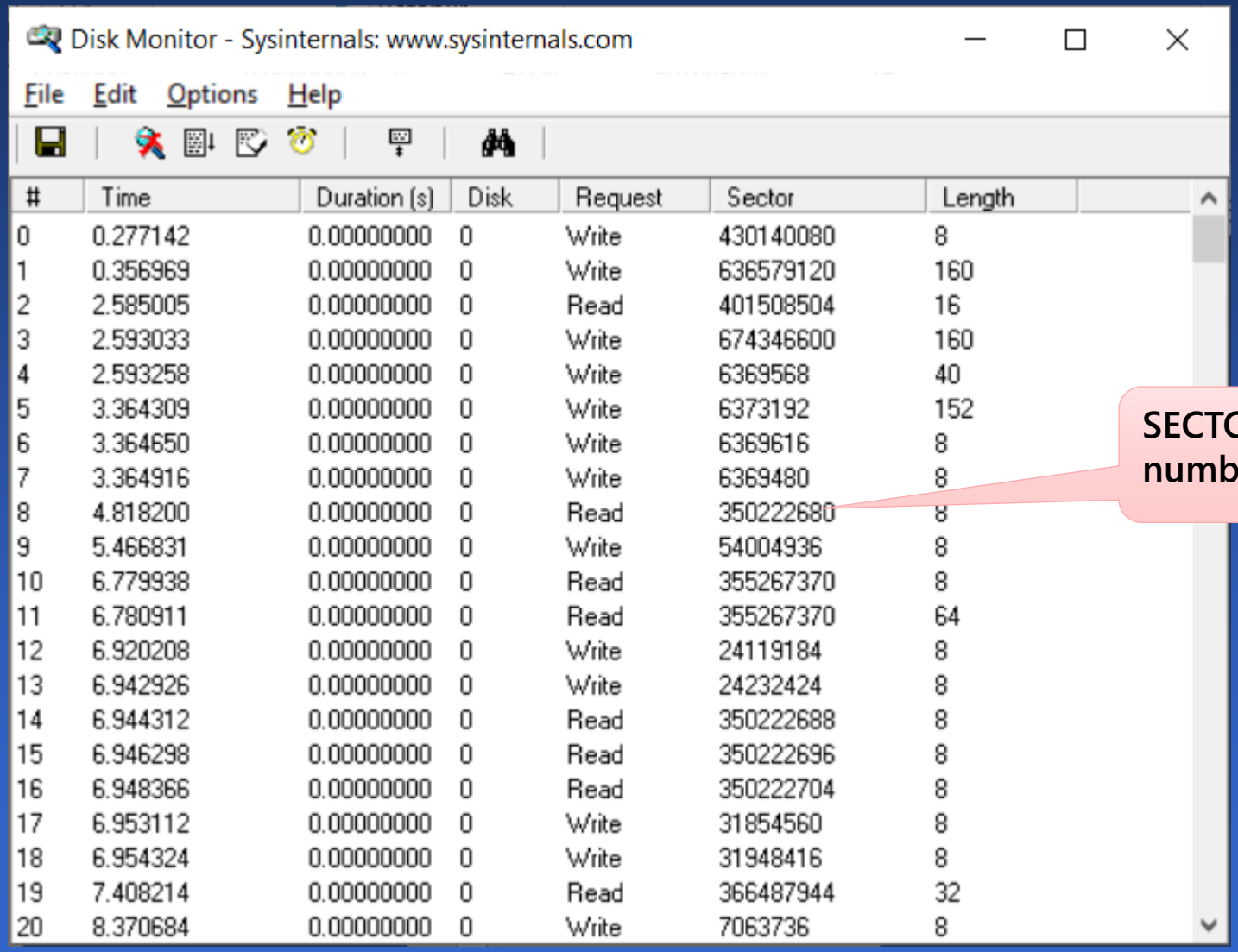
Windows Sysinternals

DiskView = Storage sectors



Windows Sysinternals

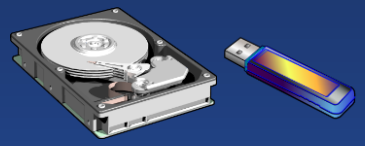
DiskMon = sector operations



#	Time	Duration (s)	Disk	Request	Sector	Length
0	0.277142	0.00000000	0	Write	430140080	8
1	0.356969	0.00000000	0	Write	636579120	160
2	2.585005	0.00000000	0	Read	401508504	16
3	2.593033	0.00000000	0	Write	674346600	160
4	2.593258	0.00000000	0	Write	6369568	40
5	3.364309	0.00000000	0	Write	6373192	152
6	3.364650	0.00000000	0	Write	6369616	8
7	3.364916	0.00000000	0	Write	6369480	8
8	4.818200	0.00000000	0	Read	350222680	8
9	5.466831	0.00000000	0	Write	54004936	8
10	6.779938	0.00000000	0	Read	355267370	8
11	6.780911	0.00000000	0	Read	355267370	64
12	6.920208	0.00000000	0	Write	24119184	8
13	6.942926	0.00000000	0	Write	24232424	8
14	6.944312	0.00000000	0	Read	350222688	8
15	6.946298	0.00000000	0	Read	350222696	8
16	6.948366	0.00000000	0	Read	350222704	8
17	6.953112	0.00000000	0	Write	31854560	8
18	6.954324	0.00000000	0	Write	31948416	8
19	7.408214	0.00000000	0	Read	366487944	32
20	8.370684	0.00000000	0	Write	7063736	8

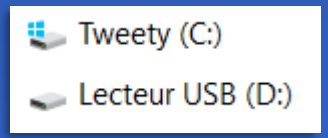
Storage structure

- Storage peripherial = DISK
  - HDD, SSD, USB storage
  - Network drive



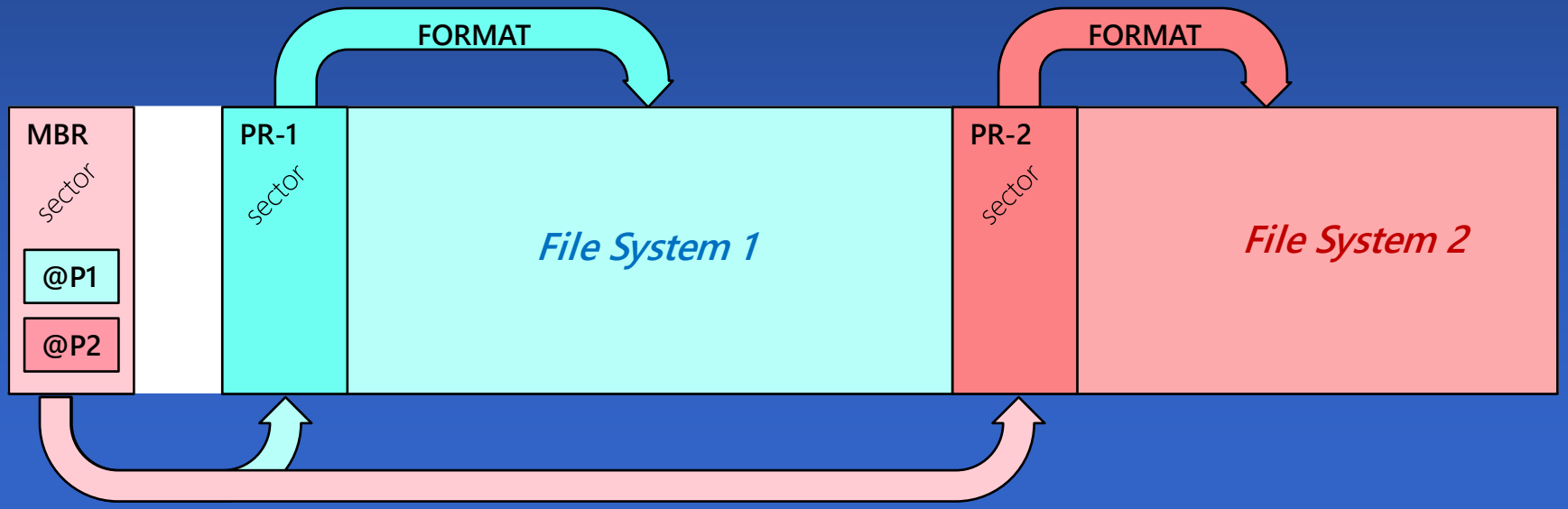
- Storage subdivision = PARTITION
  - Logical structure
  - One partition = One file system (Fat32, NTFS)

- External view = VOLUME
  - One partition may be assigned a Volume-letter
  - No letter means « hidden partition »



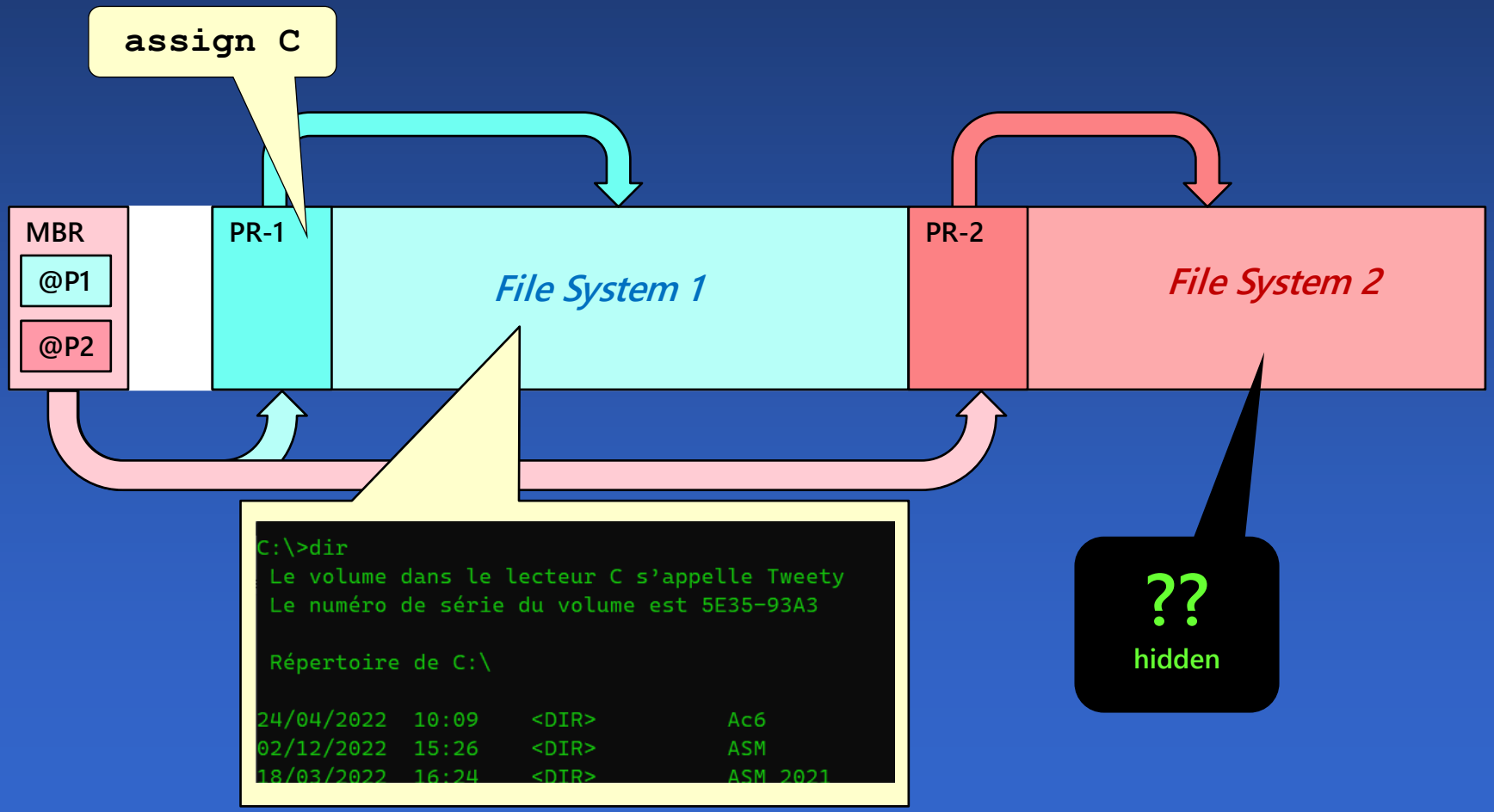
Strorage space partitionning

- Dedicated entry sectors
  - Master Boot Record = Disk entry sector
  - Partition Record = Partition entry sector
- Format
  - Partition's file allocation policy *(NTFS, FAT32…)*



Partitions & Volumes

- Volume = Partition with assigned letter C, D etc.
  - No letter = partition is hidden

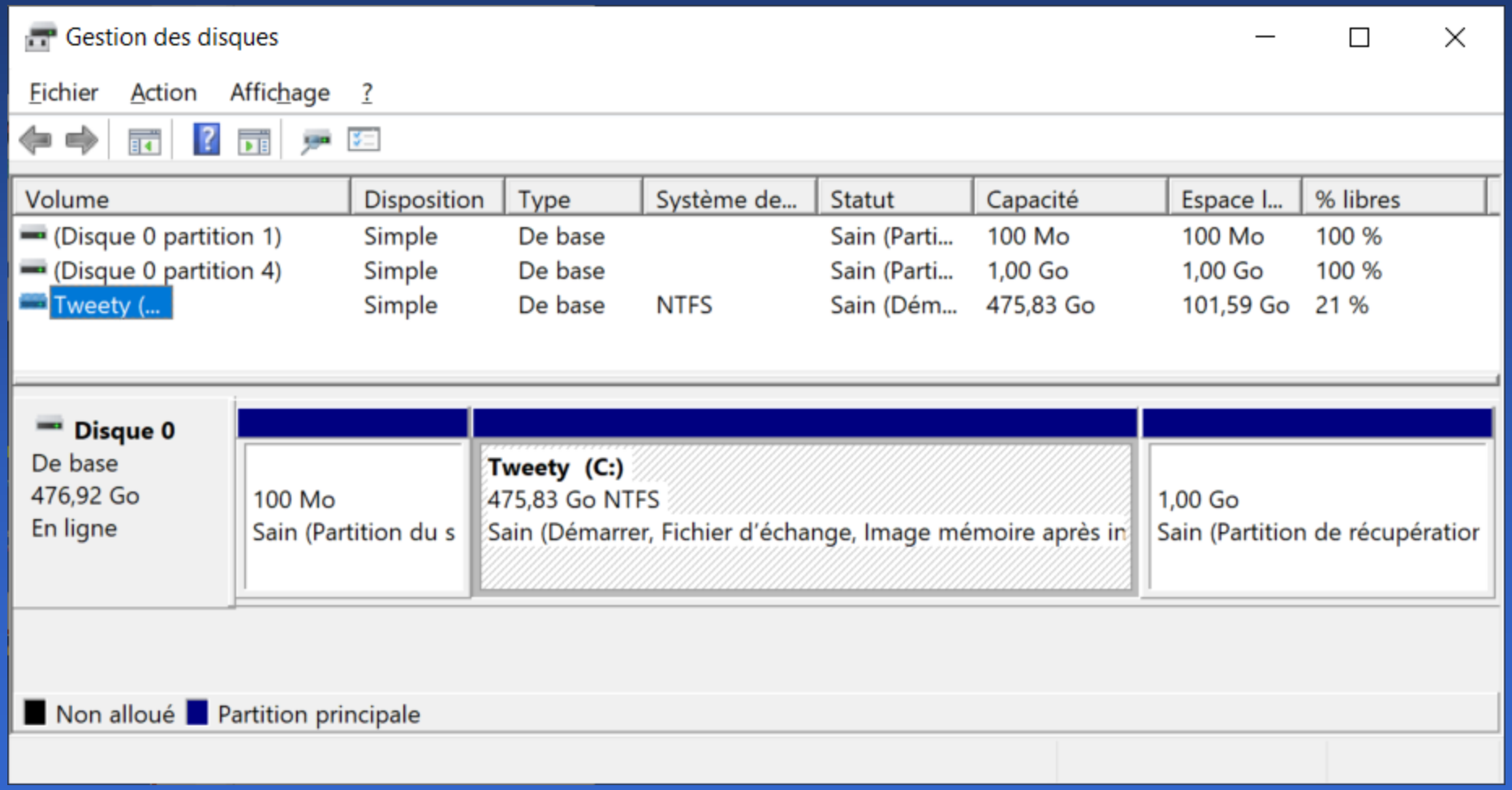


Windows supported file systems

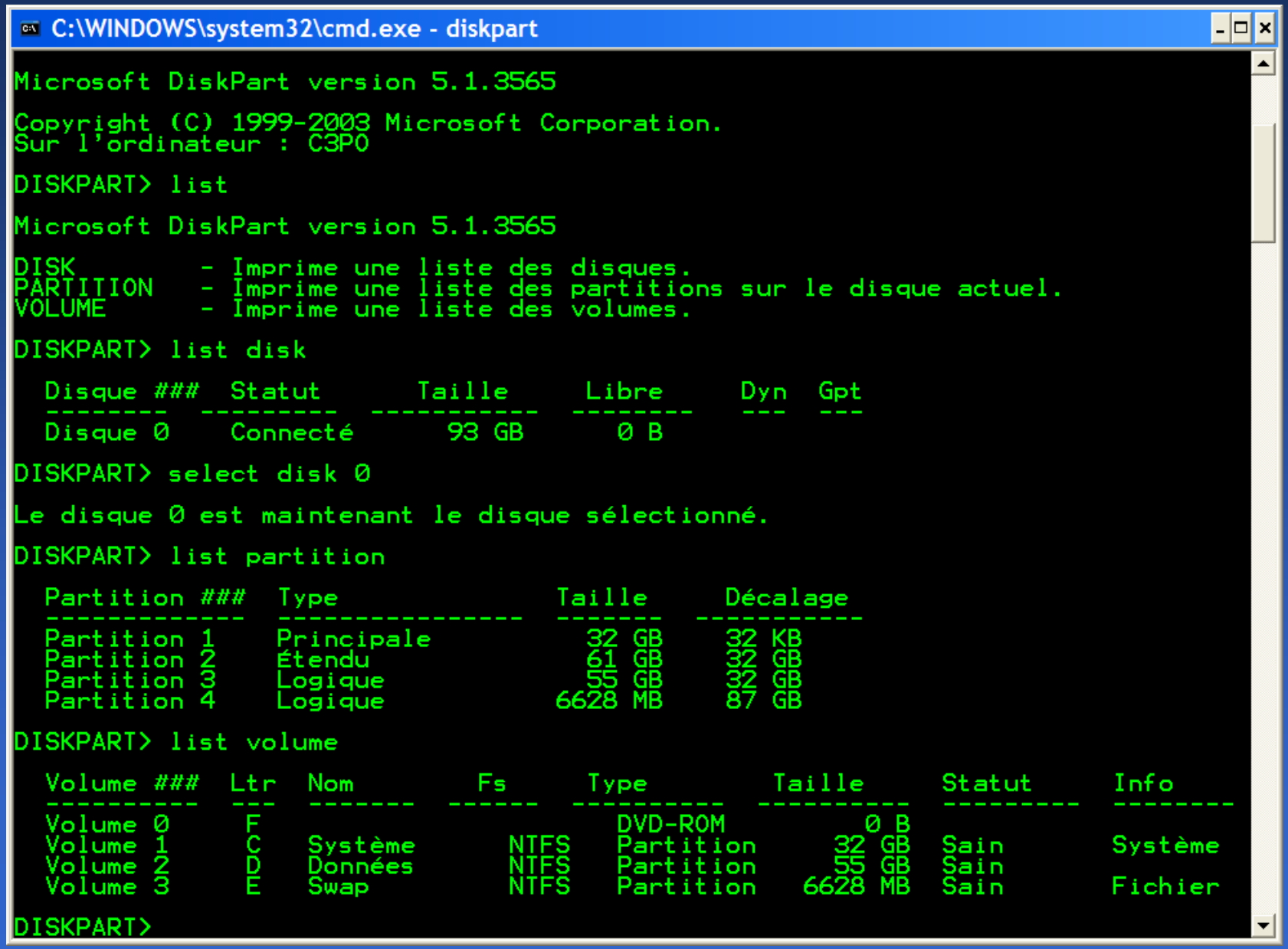
- Fat32
  - Inherited from DOS *(1977)*
  - Limited & Produces fragmentation
  - May be converted to NTFS → `convert D: /fs:NTFS`
  - Cross-system compatible
  - Optimal format for SD cards (wear leveling)
- NTFS
  - Win-NT native file system *(1993)*
  - User permissions
  - Compression allowed
  - AUTO-defragment
- Ext4
  - Through WSL2 *(C: cannot be Ext4)*

Storage management

- DISKMGMT.msc



DISKPART tool



DISKPART scripting

- Launch `DISKPART /S SCRIPT.S`

SCRIPT.S

```
rem == SCRIPT.S ==
rem    Create partitions for a UEFI/GPT-based PC.
rem    Adjust the partition sizes to fit the drive
select disk 0
clean
convert gpt
rem == 1. System partition =========================
create partition efi size=100
rem    ** NOTE: For Advanced Format 4Kn drives,
rem                change this value to size = 260 **
format quick fs=fat32 label="System"
assign letter="S"
rem == 2. Microsoft Reserved (MSR) partition =======
create partition msr size=16
rem == 3. Windows partition ========================
rem ==    a. Create the Windows partition ==========
create partition primary
rem ==    c. Prepare the Windows partition =========
format quick fs=ntfs label="Windows"
assign letter="W"
list volume
exit
```

Windows setup will modify volume letters

Windows Sysinternals

ProcMon → File monitor

Process Monitor - Sysinternals: www.sysinternals.com

Time o...	Process Name	PID	Operation	Path	Result	Detail
12:03:12...	MsMpEng.exe	5028	UnlockFileSingle	C:\ProgramData\Microsoft\Windows Defender\Scans\mpengine...	SUCCESS	Offset: 124, Length: 1
12:03:12...	msedge.exe	4692	CloseFile	C:\Users\tjoubert.LAN\AppData\Local\Microsoft\Edge\User Dat...	SUCCESS	
12:03:12...	msedge.exe	4692	FileSystemControl	C:\Users\tjoubert.LAN\AppData\Local\Microsoft\Edge\User Dat...	SUCCESS	Control: FSCTL_WRITE_USN_CLOSE_RECORI
12:03:12...	msedge.exe	4692	CloseFile	C:\Users\tjoubert.LAN\AppData\Local\Microsoft\Edge\User Dat...	SUCCESS	
12:03:12...	MsMpEng.exe	5028	LockFile	C:\ProgramData\Microsoft\Windows Defender\Scans\mpengine...	SUCCESS	Exclusive: False, Offset: 124, Length: 1, Fail Imme
12:03:12...	msedge.exe	4692	CreateFile	C:\Users\tjoubert.LAN\AppData\Local\Microsoft\Edge\User Dat...	SUCCESS	Desired Access: Read Attributes, Delete, Dispos
12:03:12...	MsMpEng.exe	5028	UnlockFileSingle	C:\ProgramData\Microsoft\Windows Defender\Scans\mpengine...	SUCCESS	Offset: 124, Length: 1
12:03:12...	msedge.exe	4692	QueryAttributeTagF...	C:\Users\tjoubert.LAN\AppData\Local\Microsoft\Edge\User Dat...	SUCCESS	Attributes: A, ReparseTag: 0x0
12:03:12...	msedge.exe	4692	SetDispositionInfor...	C:\Users\tjoubert.LAN\AppData\Local\Microsoft\Edge\User Dat...	SUCCESS	Flags: FILE_DISPOSITION_DELETE, FILE_DISF
12:03:12...	msedge.exe	4692	CloseFile	C:\Users\tjoubert.LAN\AppData\Local\Microsoft\Edge\User Dat...	SUCCESS	
12:03:12...	Teams.exe	12772	ReadFile	C:\Users\tjoubert.LAN\AppData\Local\Microsoft\Teams\current\...	SUCCESS	Offset: 136 095 744, Length: 16 384, I/O Flags: Nor
12:03:12...	Teams.exe	12772	ReadFile	C:\Users\tjoubert.LAN\AppData\Local\Microsoft\Teams\current\...	SUCCESS	Offset: 136 067 072, Length: 16 384, I/O Flags: Nor
12:03:12...	Teams.exe	12772	ReadFile	C:\Users\tjoubert.LAN\AppData\Local\Microsoft\Teams\current\...	SUCCESS	Offset: 136 030 208, Length: 16 384, I/O Flags: Nor
12:03:12...	Teams.exe	12772	ReadFile	C:\Users\tjoubert.LAN\AppData\Local\Microsoft\Teams\current\...	SUCCESS	Offset: 135 948 288, Length: 16 384, I/O Flags: Nor
12:03:12...	Teams.exe	12772	ReadFile	C:\Users\tjoubert.LAN\AppData\Local\Microsoft\Teams\current\...	SUCCESS	Offset: 135 964 672, Length: 12 288, I/O Flags: Nor
12:03:12...	Teams.exe	12772	ReadFile	C:\Users\tjoubert.LAN\AppData\Local\Microsoft\Teams\current\...	SUCCESS	Offset: 135 739 392, Length: 4 096, I/O Flags: Non-
12:03:13...	SearchIndexer...	9136	FileSystemControl	C:	SUCCESS	Control: FSCTL_READ_USN_JOURNAL
12:03:13...	SearchIndexer...	9136	FileSystemControl	C:	SUCCESS	Control: FSCTL_READ_USN_JOURNAL
12:03:13...	MsMpEng.exe	5028	CreateFile	C:\Windows\System32\svchost.exe	SUCCESS	Desired Access: Read Attributes, Synchronize, D
12:03:13...	MsMpEng.exe	5028	QueryInformationVo...	C:\Windows\System32\svchost.exe	BUFFER OV...	VolumeCreationTime: 17/08/2020 03:57:56, Volur
12:03:13...	MsMpEng.exe	5028	QueryAllInformation...	C:\Windows\System32\svchost.exe	BUFFER OV...	CreationTime: 14/07/2022 13:17:24, LastAccessT
12:03:13...	MsMpEng.exe	5028	QueryInformationVo...	C:\Windows\System32\svchost.exe	BUFFER OV...	VolumeCreationTime: 17/08/2020 03:57:56, Volur
12:03:13...	MsMpEng.exe	5028	QueryAllInformation...	C:\Windows\System32\svchost.exe	BUFFER OV...	CreationTime: 14/07/2022 13:17:24, LastAccessT
12:03:13...	MsMpEng.exe	5028	FileSystemControl	C:\Windows\System32\svchost.exe	SUCCESS	Control: FSCTL_READ_FILE_USN_DATA
12:03:13...	MsMpEng.exe	5028	QueryIdInformation	C:\Windows\System32\svchost.exe	SUCCESS	
12:03:13...	MsMpEng.exe	5028	CloseFile	C:\Windows\System32\svchost.exe	SUCCESS	
12:03:16...	MsMpEng.exe	5028	LockFile	C:\ProgramData\Microsoft\Windows Defender\Scans\mpengine...	SUCCESS	Exclusive: False, Offset: 124, Length: 1, Fail Imme
12:03:16...	MsMpEng.exe	5028	UnlockFileSingle	C:\ProgramData\Microsoft\Windows Defender\Scans\mpengine...	SUCCESS	Offset: 124, Length: 1
12:03:16...	MsMpEng.exe	5028	LockFile	C:\ProgramData\Microsoft\Windows Defender\Scans\mpengine...	SUCCESS	Exclusive: False, Offset: 124, Length: 1, Fail Imme
12:03:16...	MsMpEng.exe	5028	UnlockFileSingle	C:\ProgramData\Microsoft\Windows Defender\Scans\mpengine...	SUCCESS	Offset: 124, Length: 1
12:03:16...	MsMpEng.exe	5028	LockFile	C:\ProgramData\Microsoft\Windows Defender\Scans\mpengine...	SUCCESS	Exclusive: False, Offset: 124, Length: 1, Fail Imme
12:03:16...	MsMpEng.exe	5028	UnlockFileSingle	C:\ProgramData\Microsoft\Windows Defender\Scans\mpengine...	SUCCESS	Offset: 124, Length: 1

Showing 15 596 of 484 419 events (3.%)

Backed by virtual memory