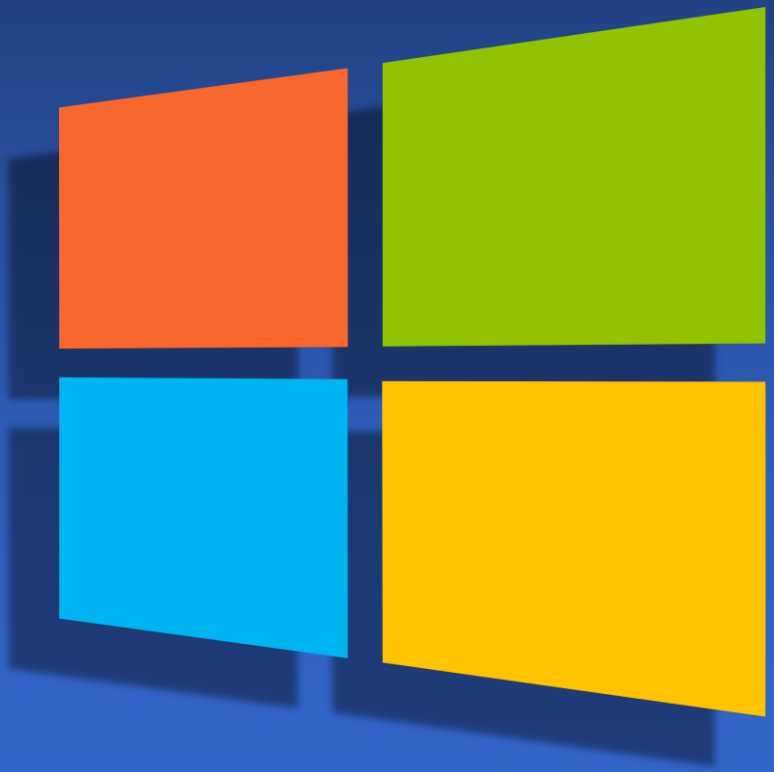
Use & Admin Windows
Survival Kit – 4 RUNTIME



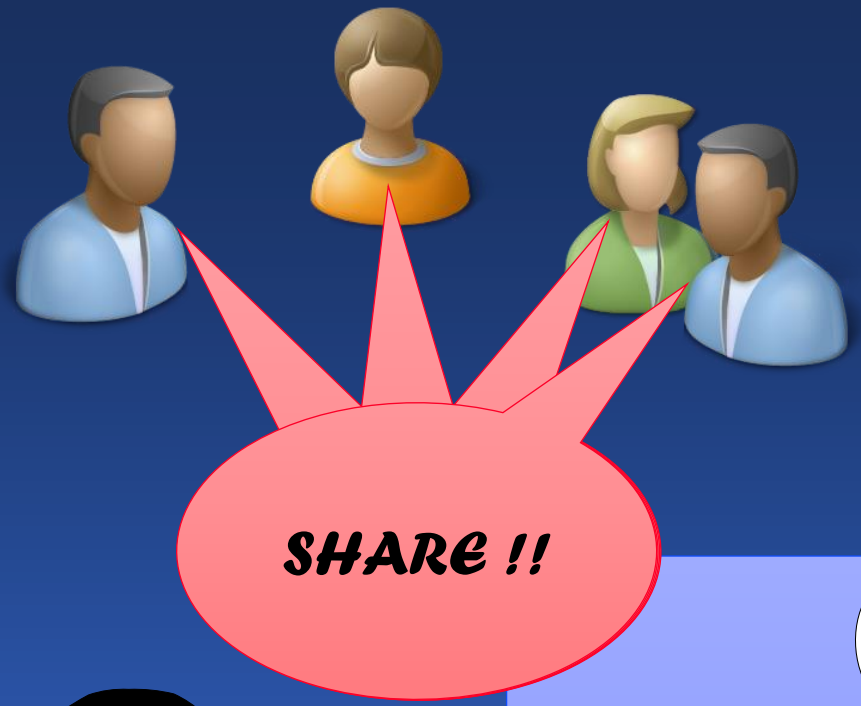
© Thierry Joubert 2024

Windows Processes

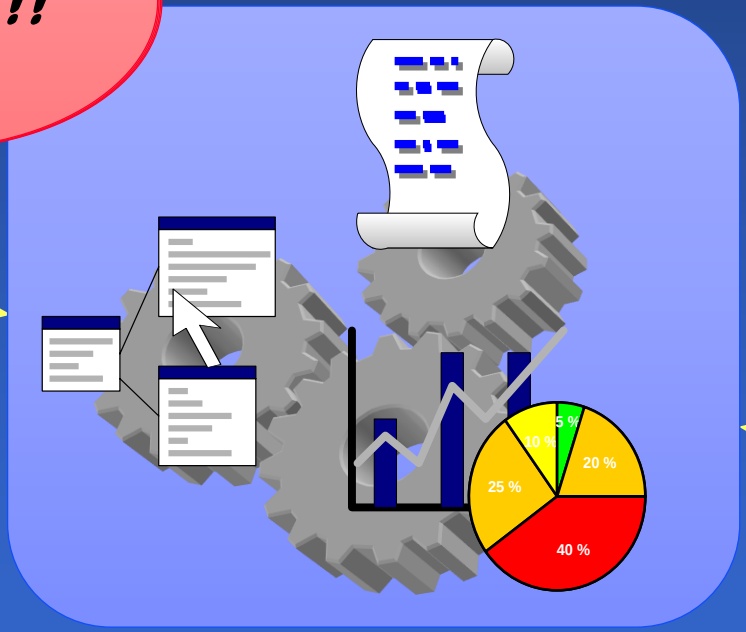
Applications & Services

© Thierry Joubert 2024

OS ?



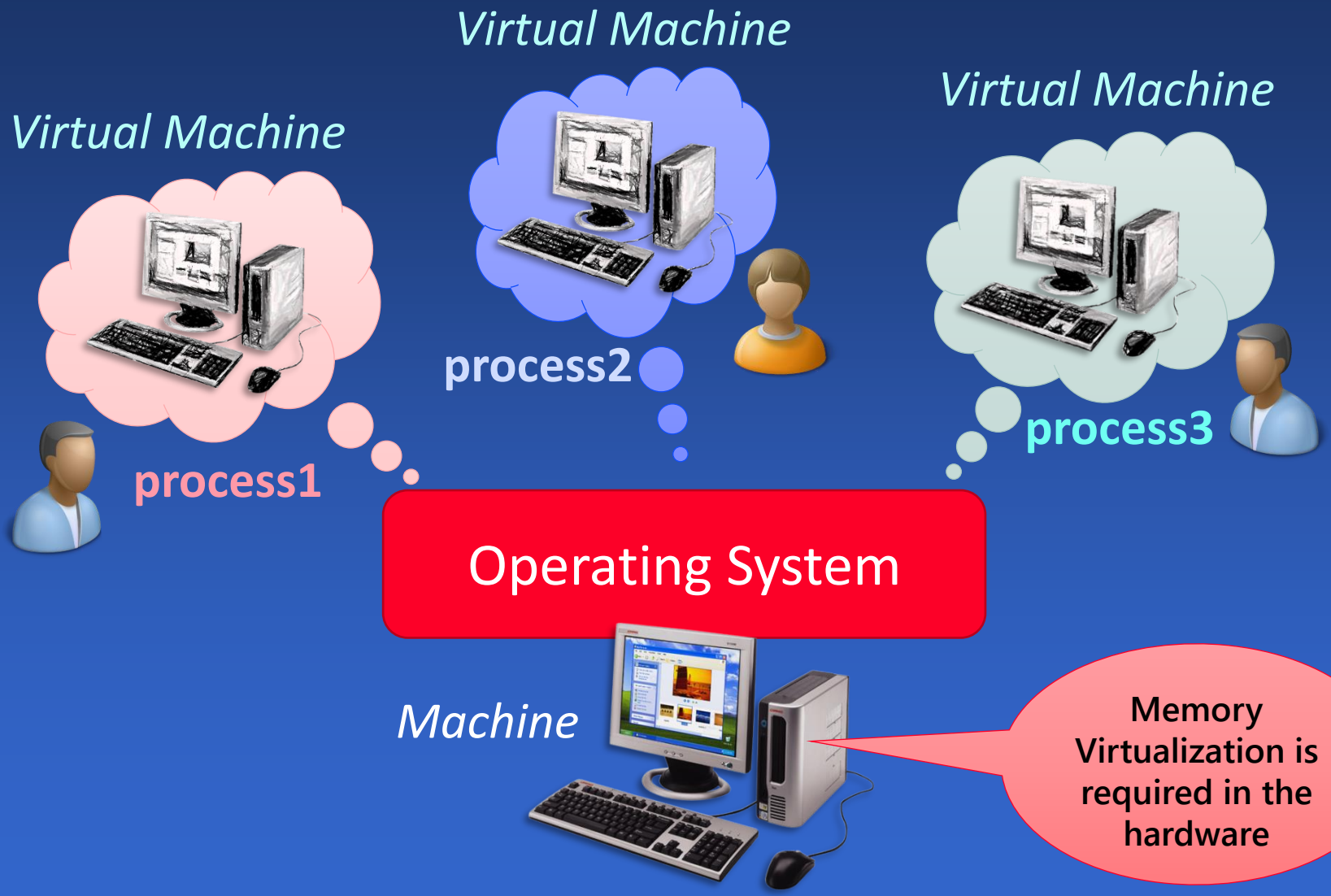
User



Hardware

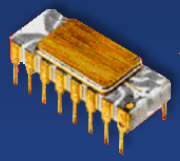
© Thierry Joubert 2024

Sharing the hardware

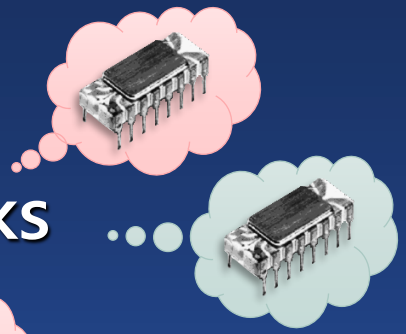


© Thierry Joubert 2024

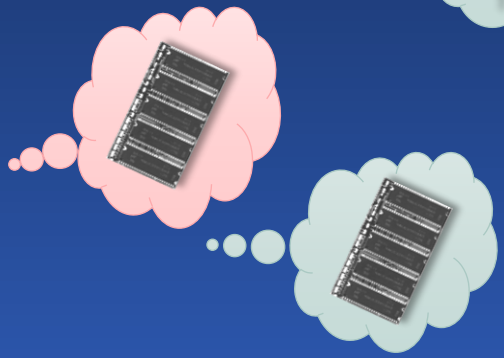
Role of the OS



Virtual CPU → Schedule tasks



Virtual RAM → MMU



Virtual I/O → Driver management

- File system
- Byte streams
- User interface

© Thierry Joubert 2024

OS Layers

User environment

TTY shell

GUI shell

Developer environment

System API (LIBC, POSIX, Win32 …)

OOP framework (JAVA, .NET …)

Services

Virtualized I/O

Persistence → HDD, SSD, File System …

IPC → pipes, sockets …

Peripherials & Stacks → Serial, USB, Ethernet …

Drivers

Memory

MMU → processus → protection

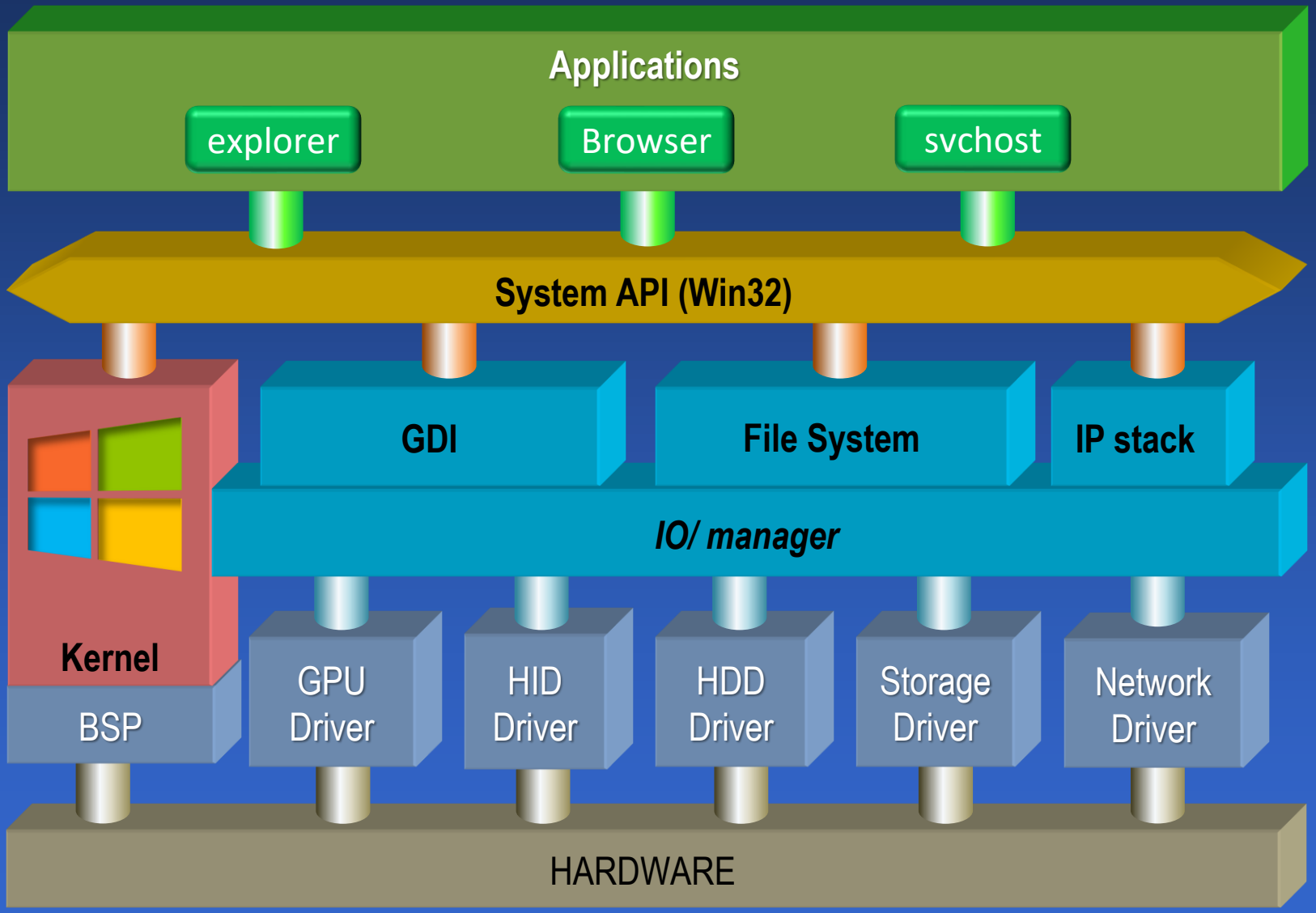
Execution

Scheduler→ thread → synchronization

Kernel

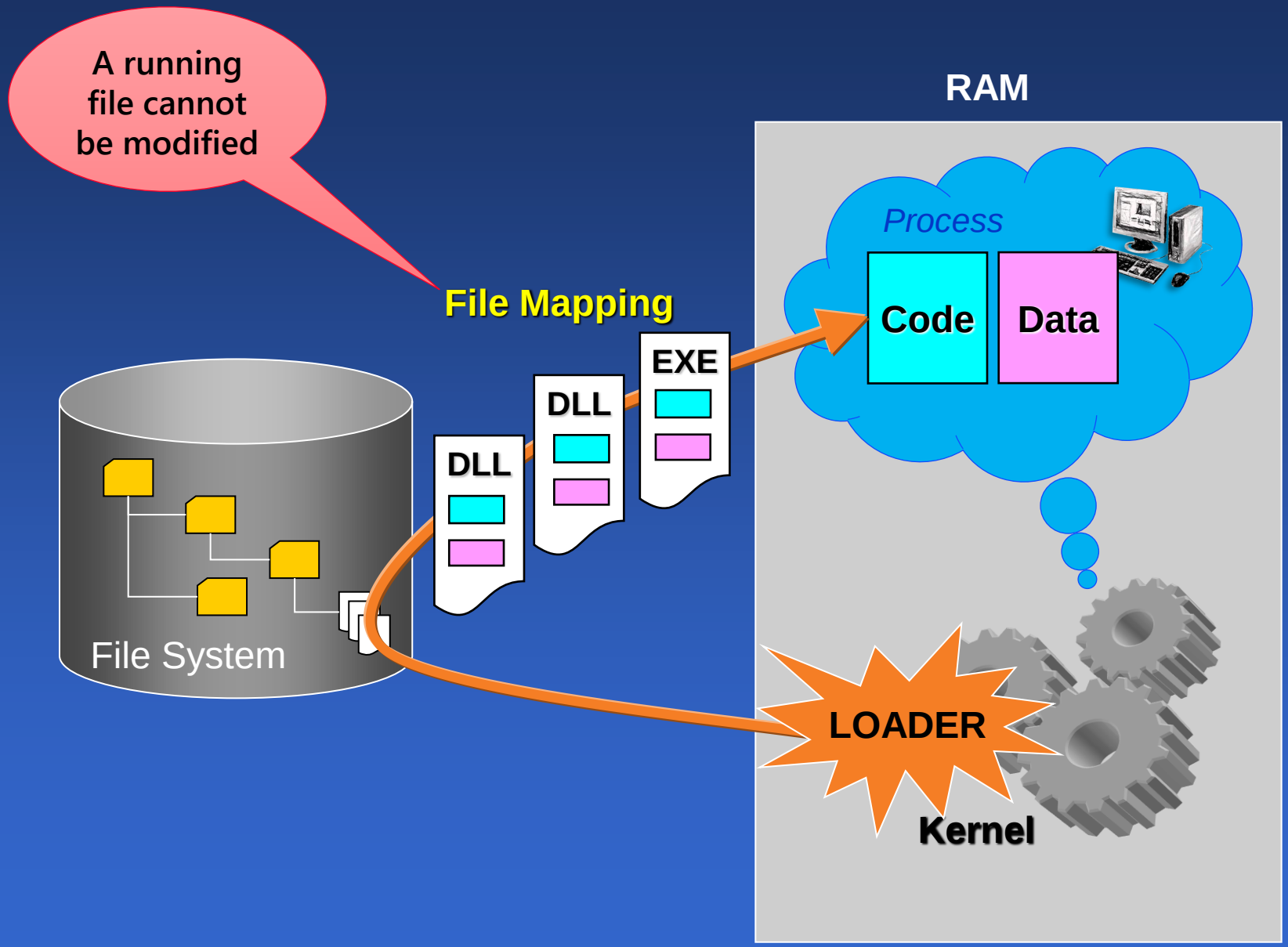
© Thierry Joubert 2024

OS logical organization



© Thierry Joubert 2024

Executable files EXE & DLL

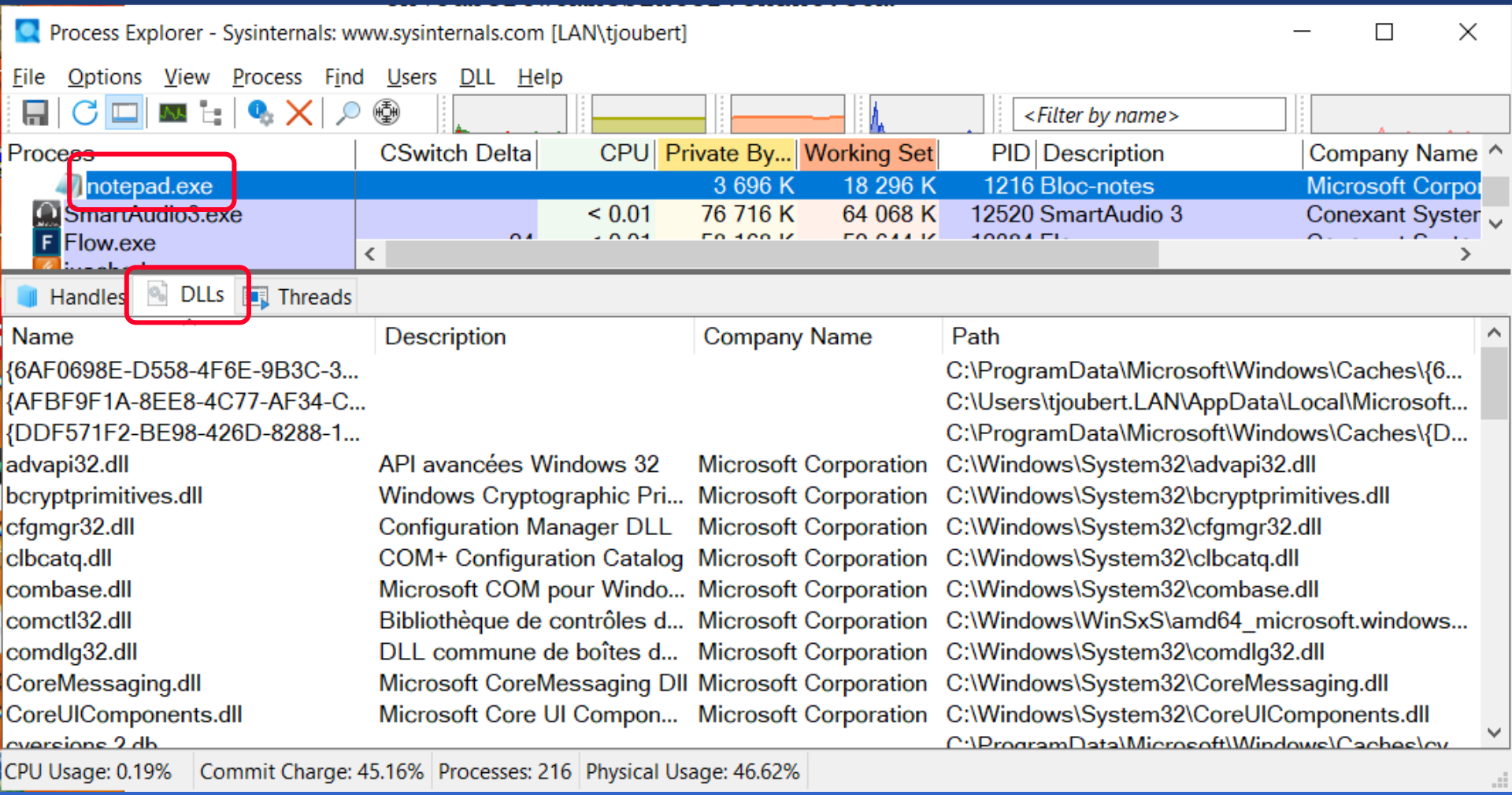


© Thierry Joubert 2024

Windows Sysinternals

Module DLLs

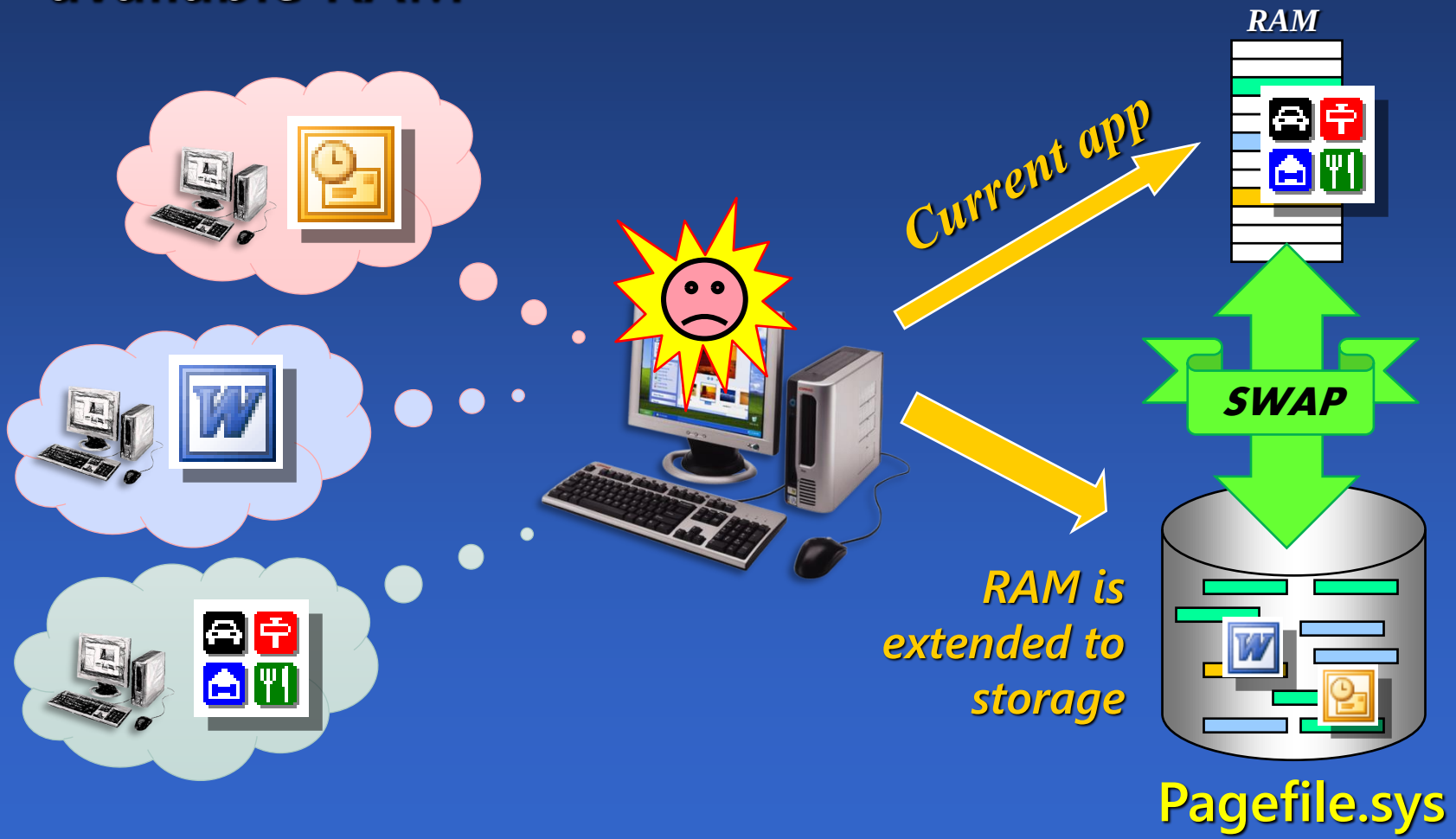
- Explore NOTEPAD with ProcExp



© Thierry Joubert 2024

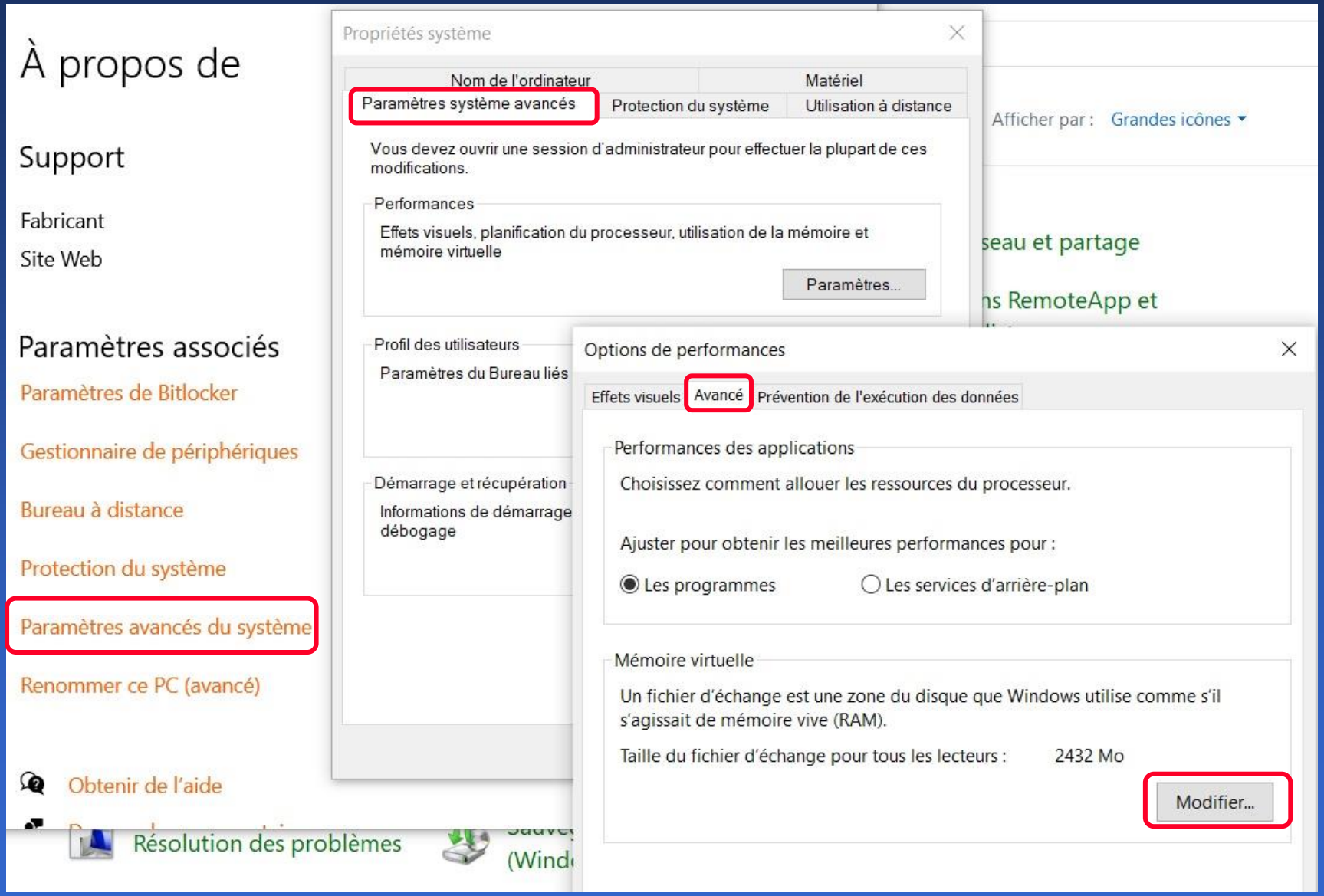
Virtual Memory & Swap

- Applications may use more memory than the available RAM



© Thierry Joubert 2024

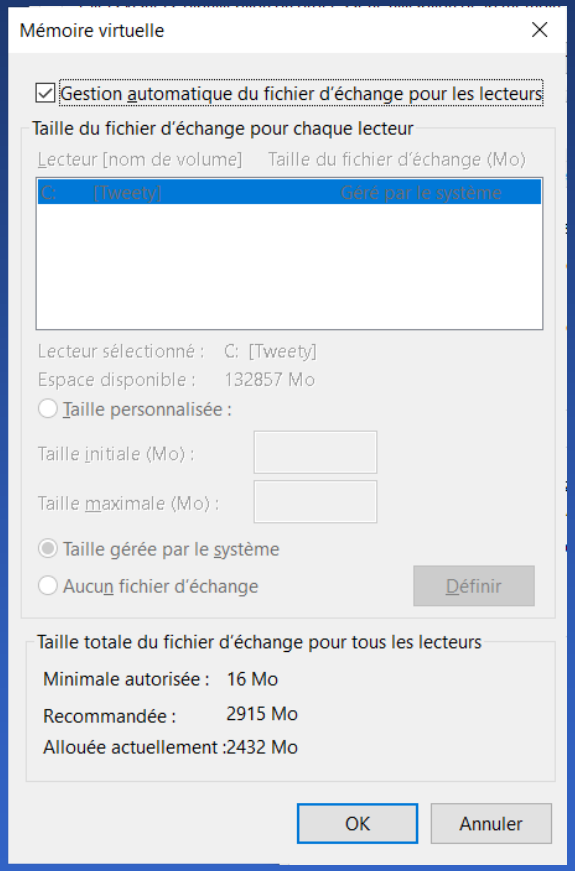
Swap parameters



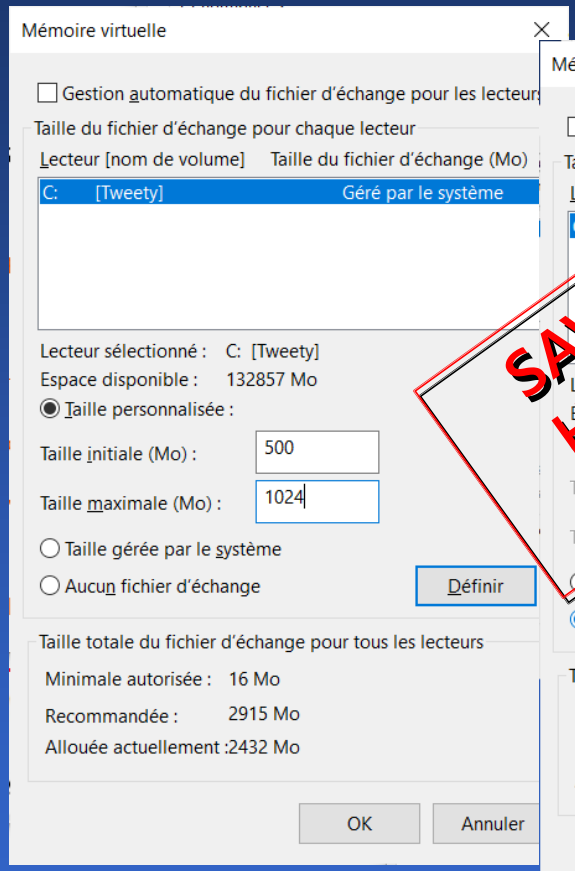
© Thierry Joubert 2024

Swap options

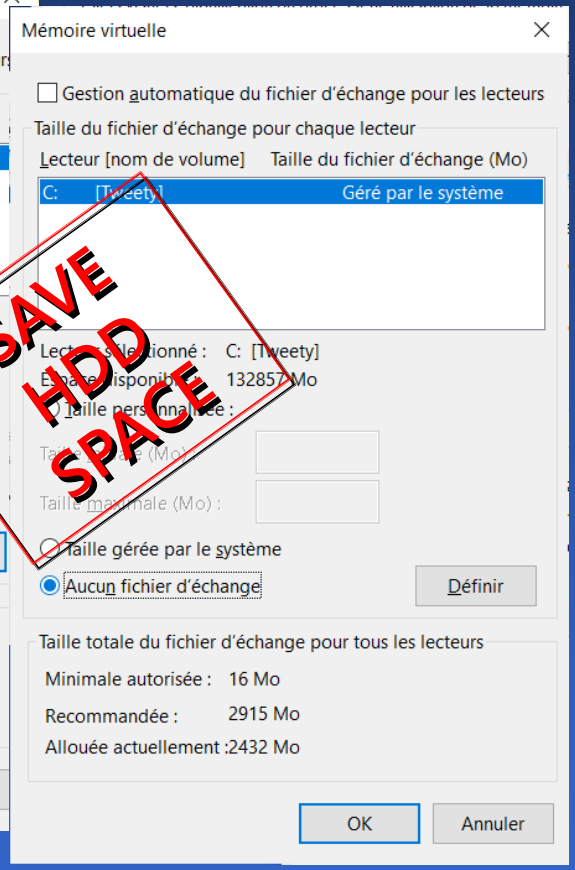
AUTO SWAP (default)



DEDICATED SWAP



NO SWAP

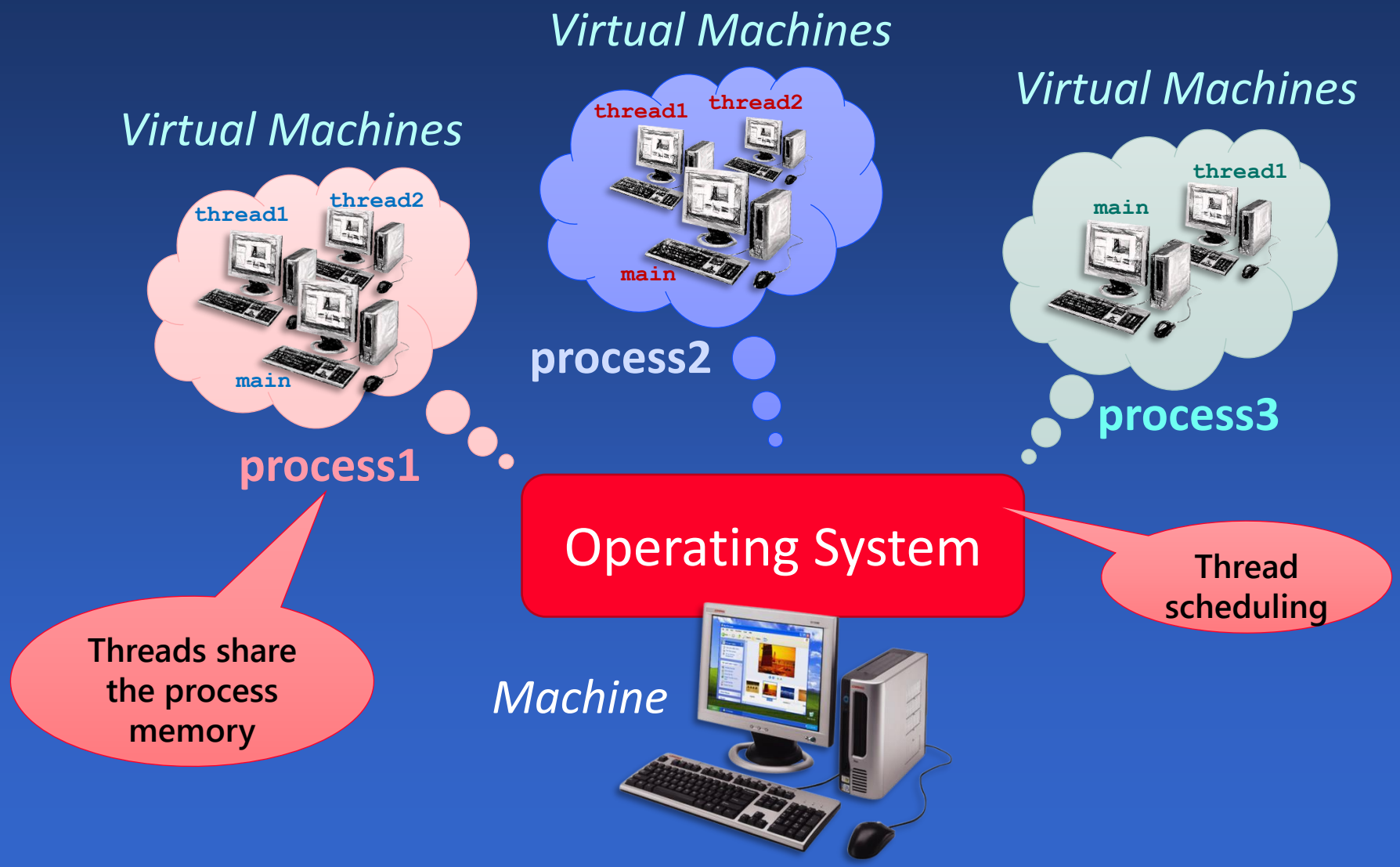


SAVE HDD SPACE

Reboot is required

© Thierry Joubert 2024

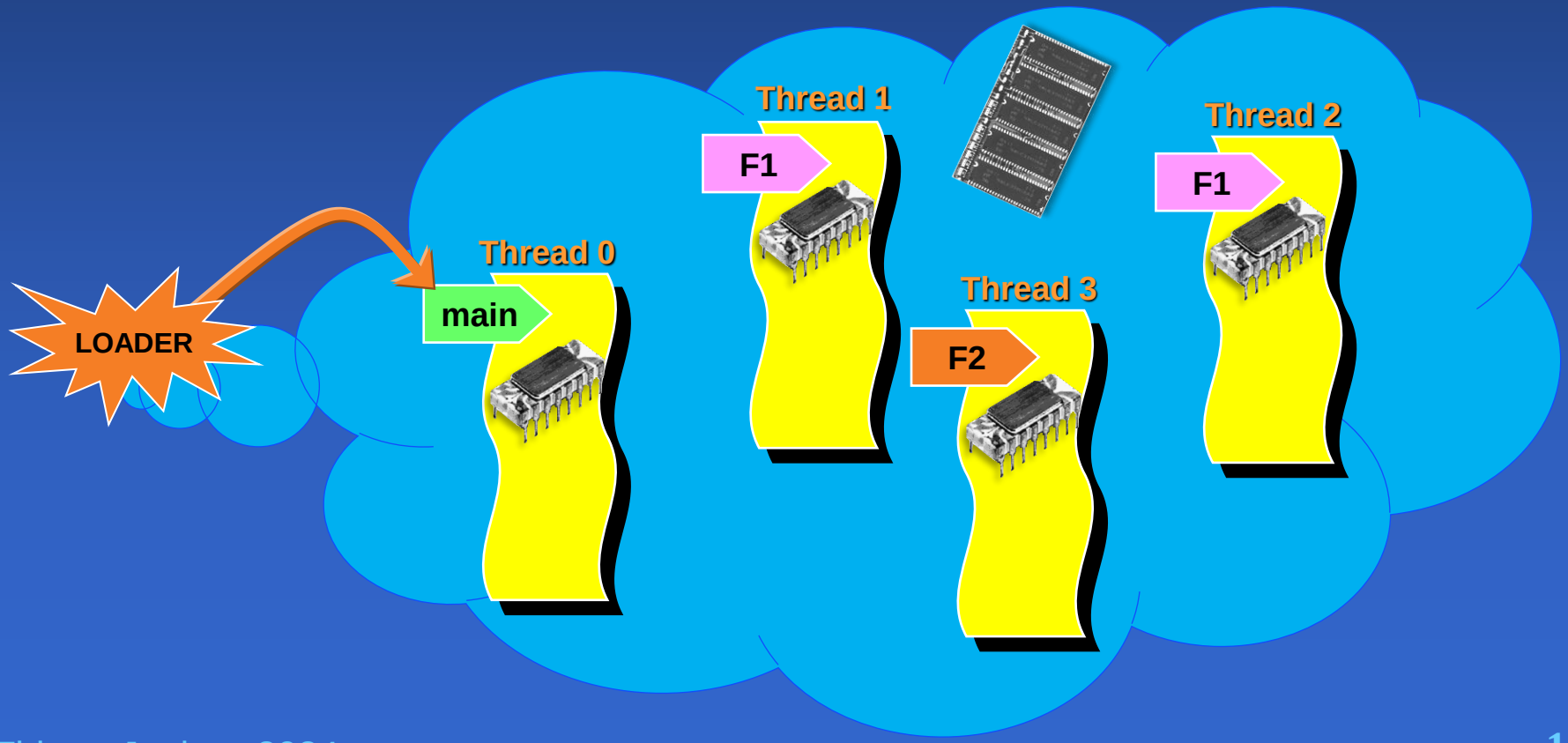
Next step = Threads



© Thierry Joubert 2024

Multi-threading

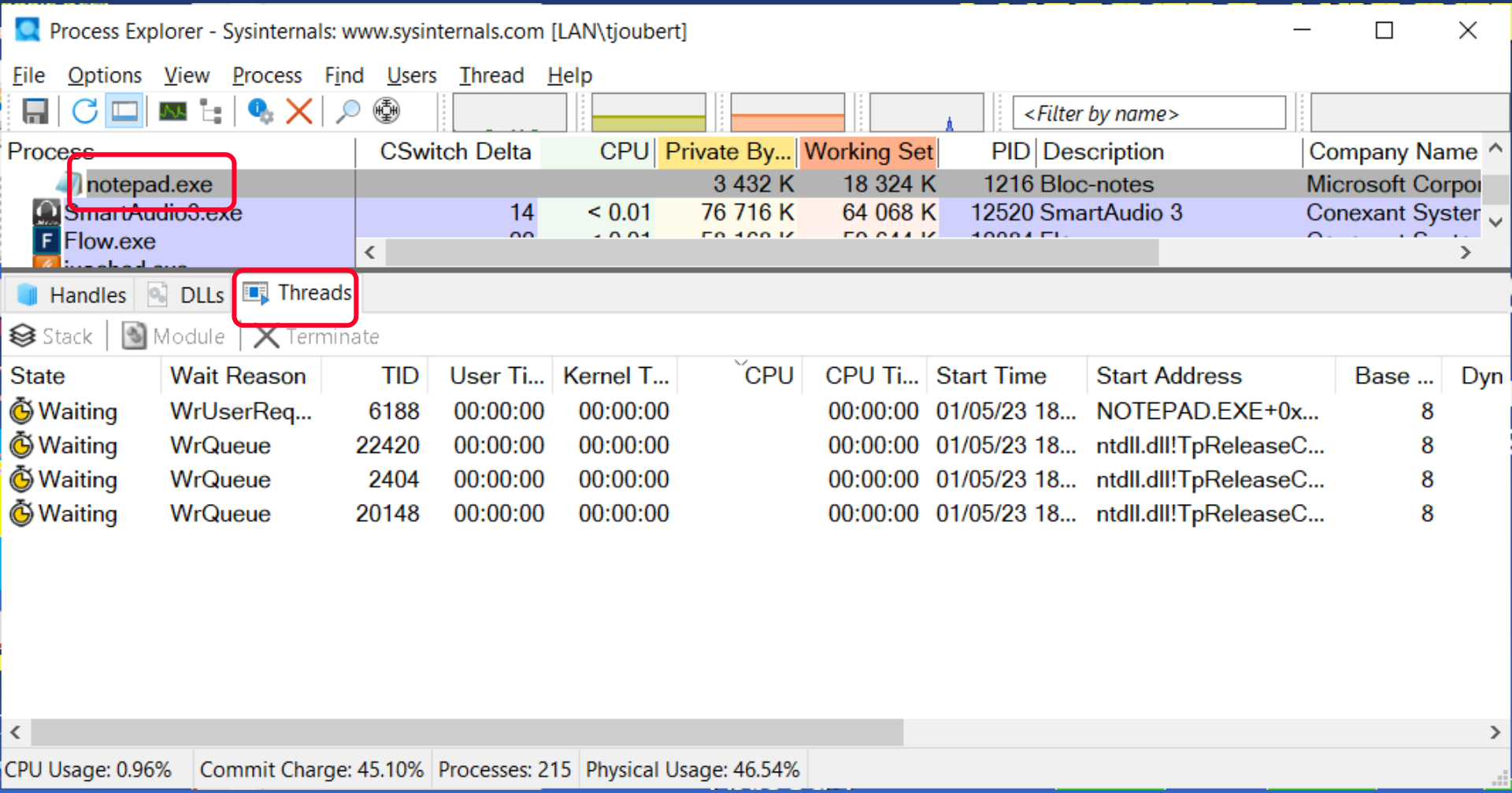
- Applications may have several threads
  - Thread0 runs the `main`
  - Others Threads run dedicated code
  - Each thread has its own STACK
  - All threads share the same memory space (BSS, HEAP)



© Thierry Joubert 2024

Module Threads

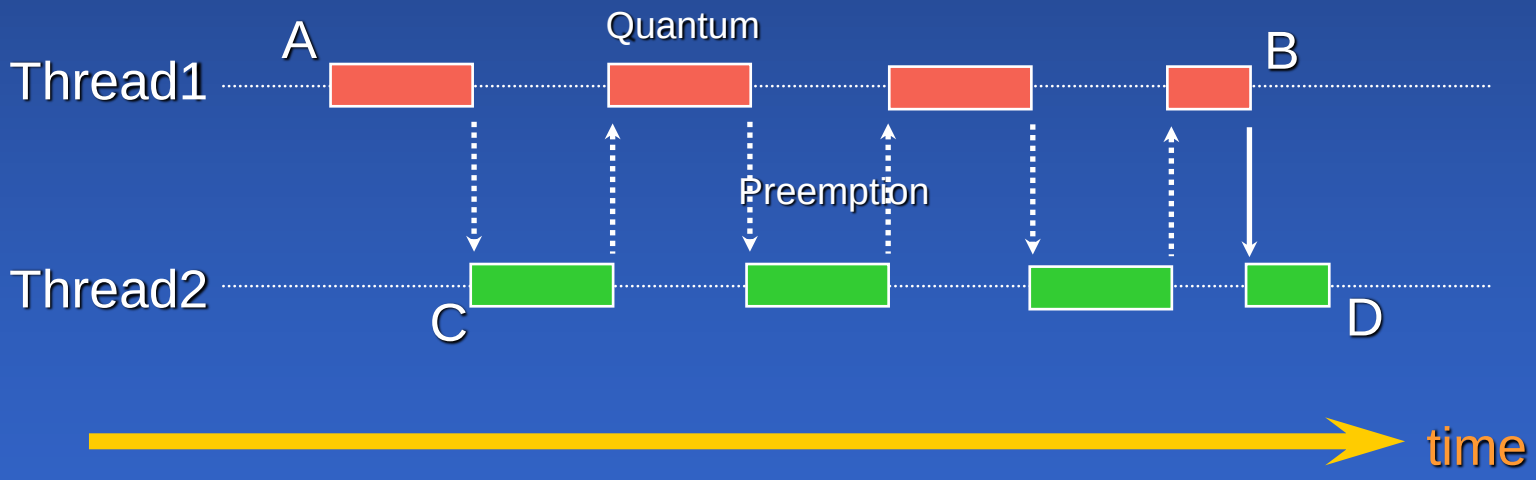
- Explore NOTEPAD with ProcExp



© Thierry Joubert 2024

CPU distribution

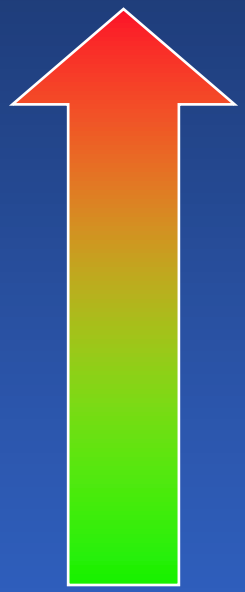
- Windows is a preemptive OS
  - The highest priority thread always runs
  - Two threads with equal priorities run in "quantums«
  - Two threads may run in parallel in case of multicore



© Thierry Joubert 2024

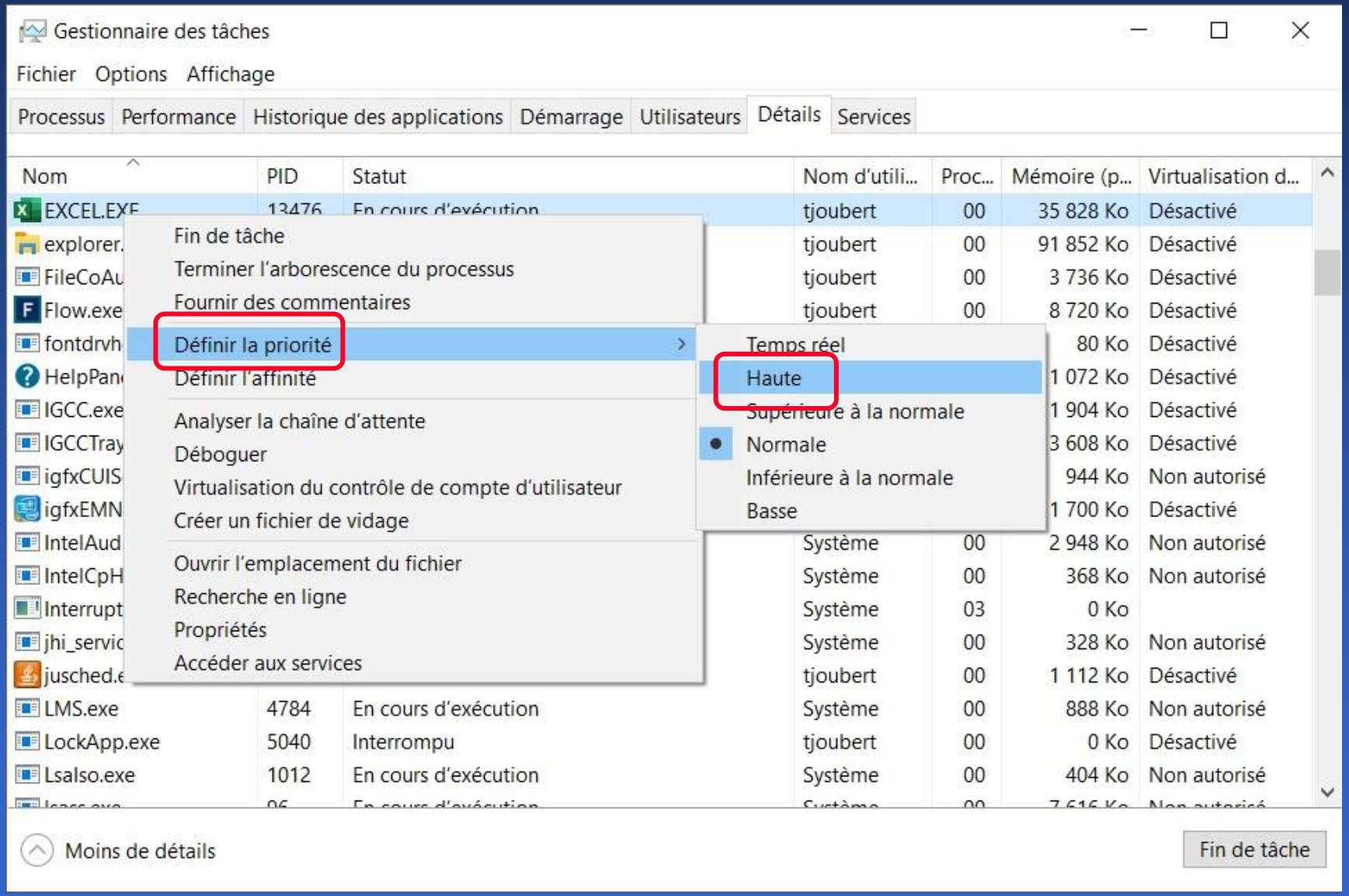
Process priorities

- Windows has 6 priority levels for processes
  - REAL TIME
  - HIGH
  - ABOVE_NORMAL
  - NORMAL
  - BELOW_NORMAL
  - IDLE



© Thierry Joubert 2024

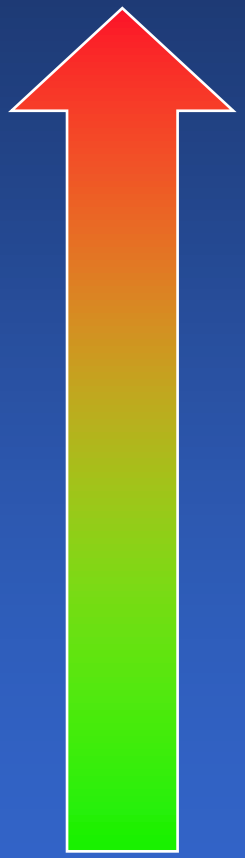
Change a process priority



© Thierry Joubert 2024

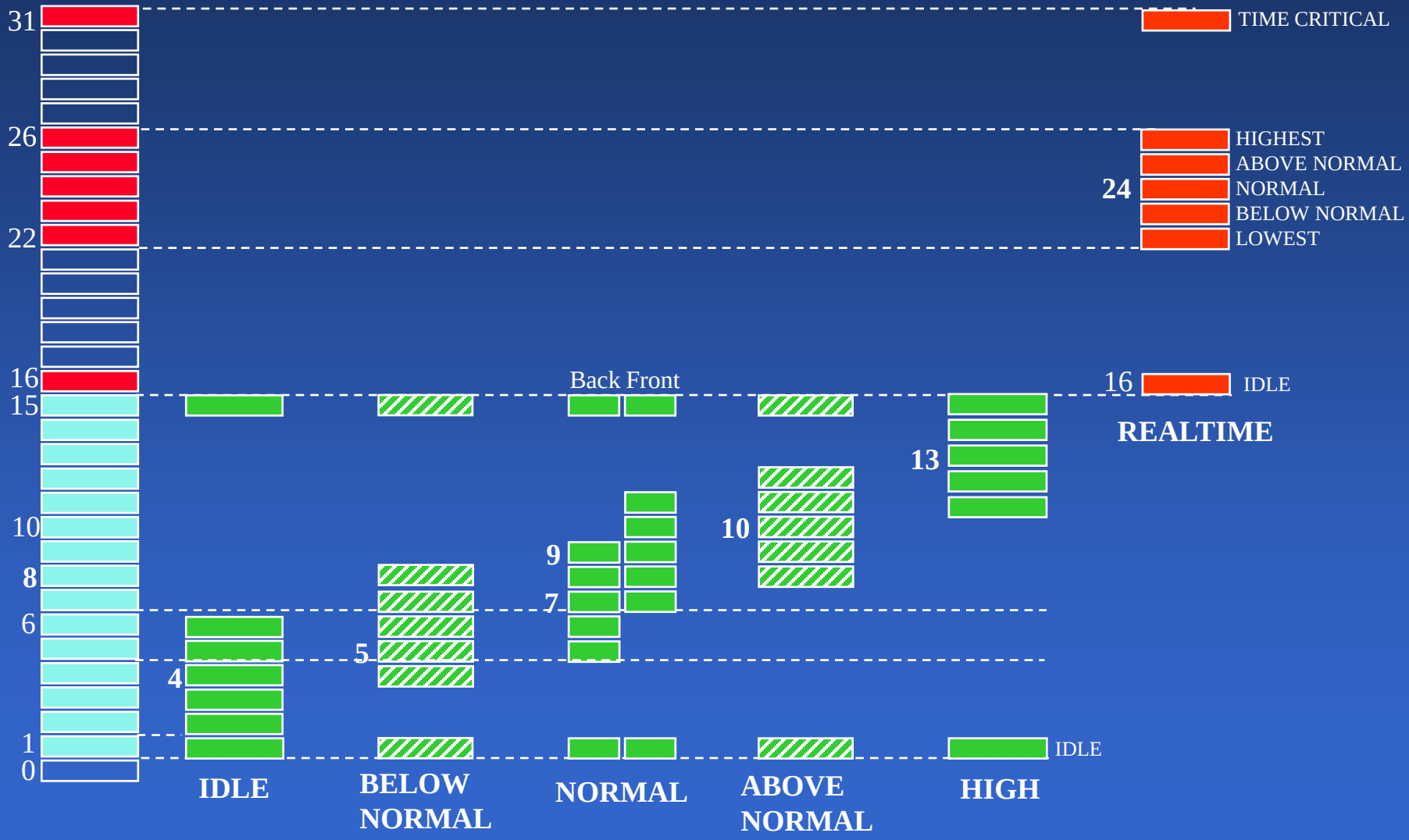
Thread priorities

- Windows has 7 priority levels for threads
  - THREAD_PRIORITY_TIME_CRITICAL (15 or 31)
  - THREAD_PRIORITY_HIGHEST (+2)
  - THREAD_PRIORITY_ABOVE_NORMAL (+1)
  - THREAD_PRIORITY_NORMAL (default)
  - THREAD_PRIORITY_BELOW_NORMAL (-1)
  - THREAD_PRIORITY_LOWEST (-2)
  - THREAD_PRIORITY_IDLE (1 or 16)



© Thierry Joubert 2024

Runtime priority map



© Thierry Joubert 2024

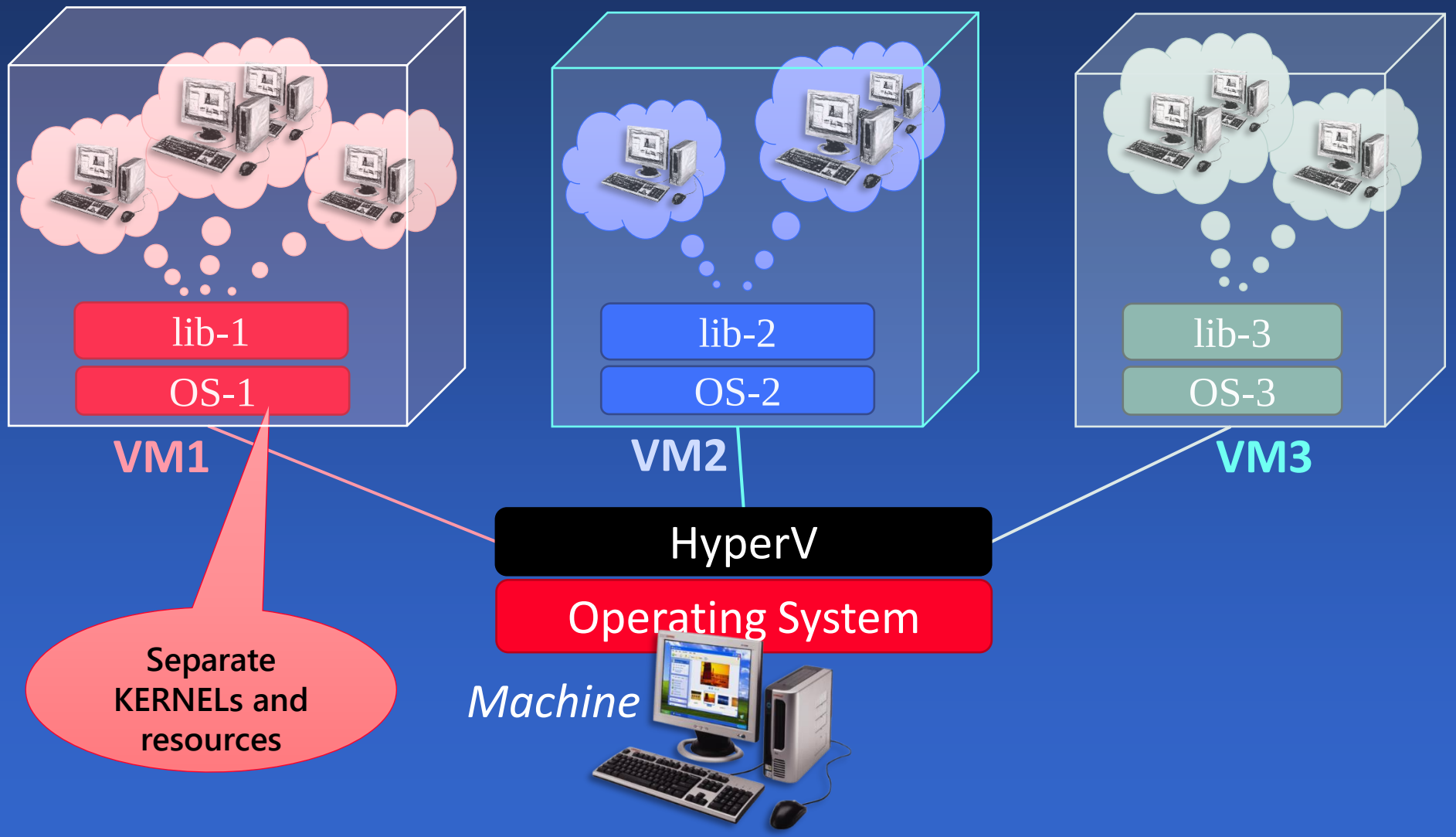
20

Beyond Processes

Hypervisor

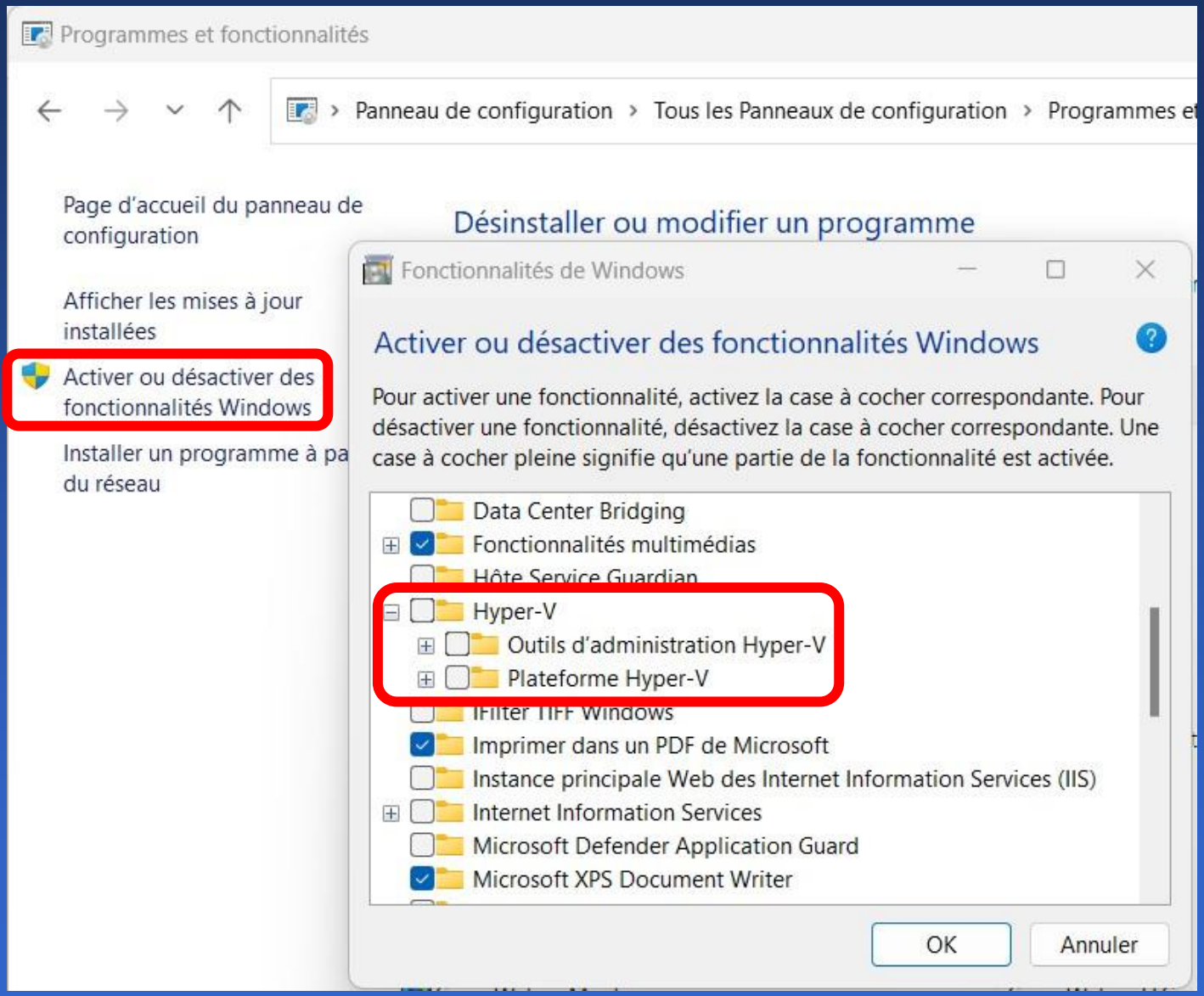
© Thierry Joubert 2024

Many OSes = HyperV



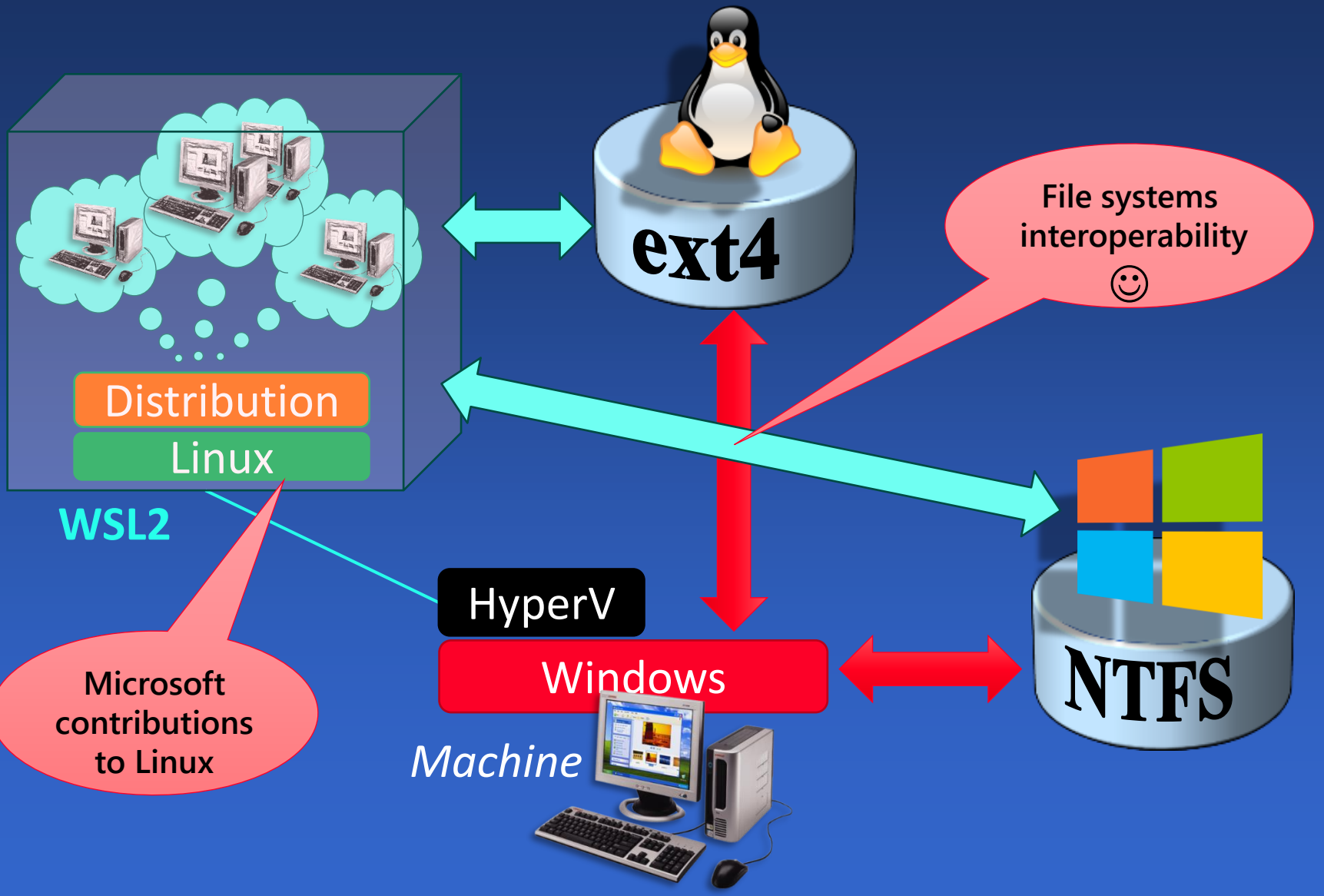
© Thierry Joubert 2024

Activate HyperV in Control Panel



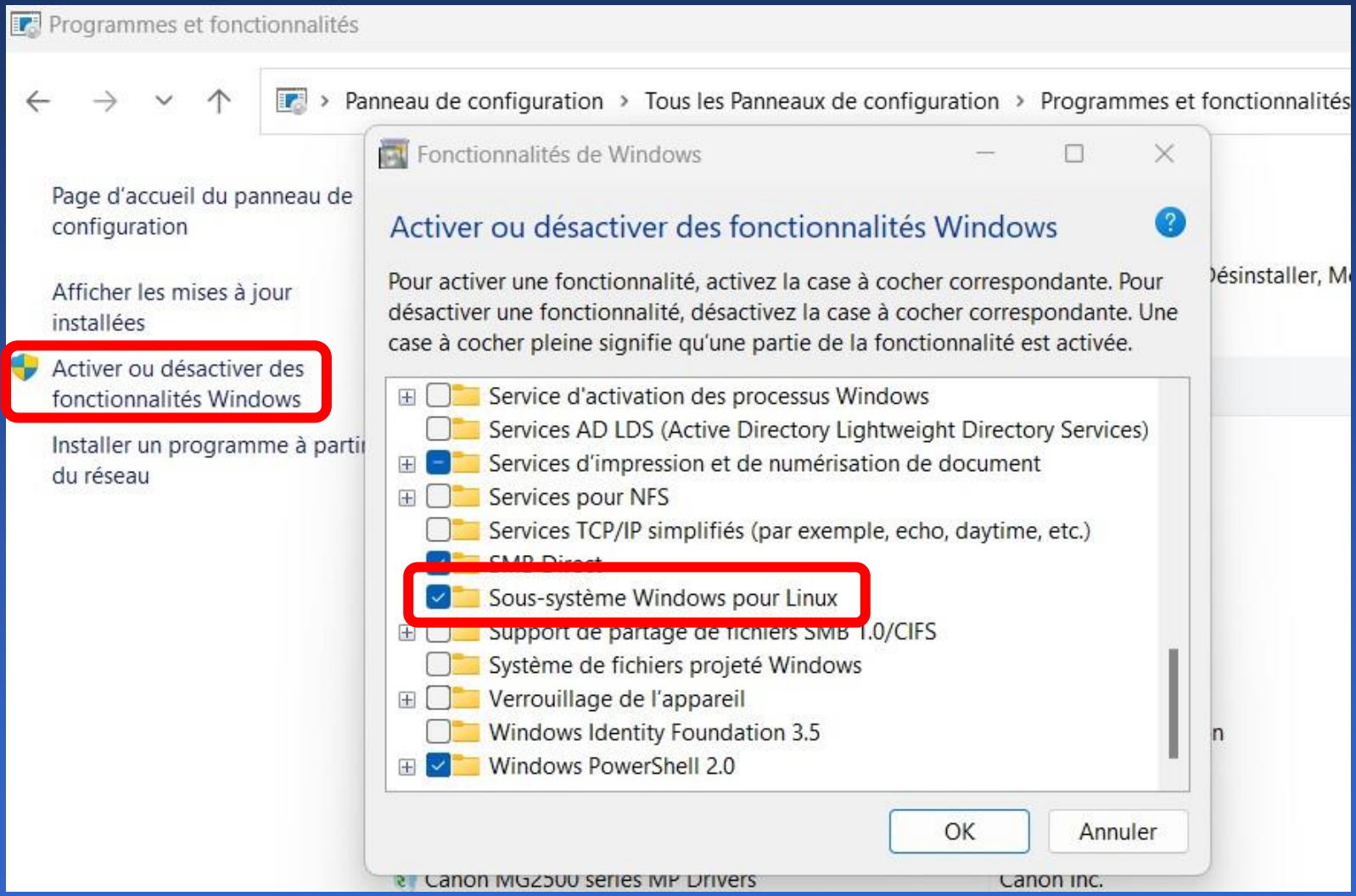
© Thierry Joubert 2024

A native HyperV VM = WSL2



© Thierry Joubert 2024

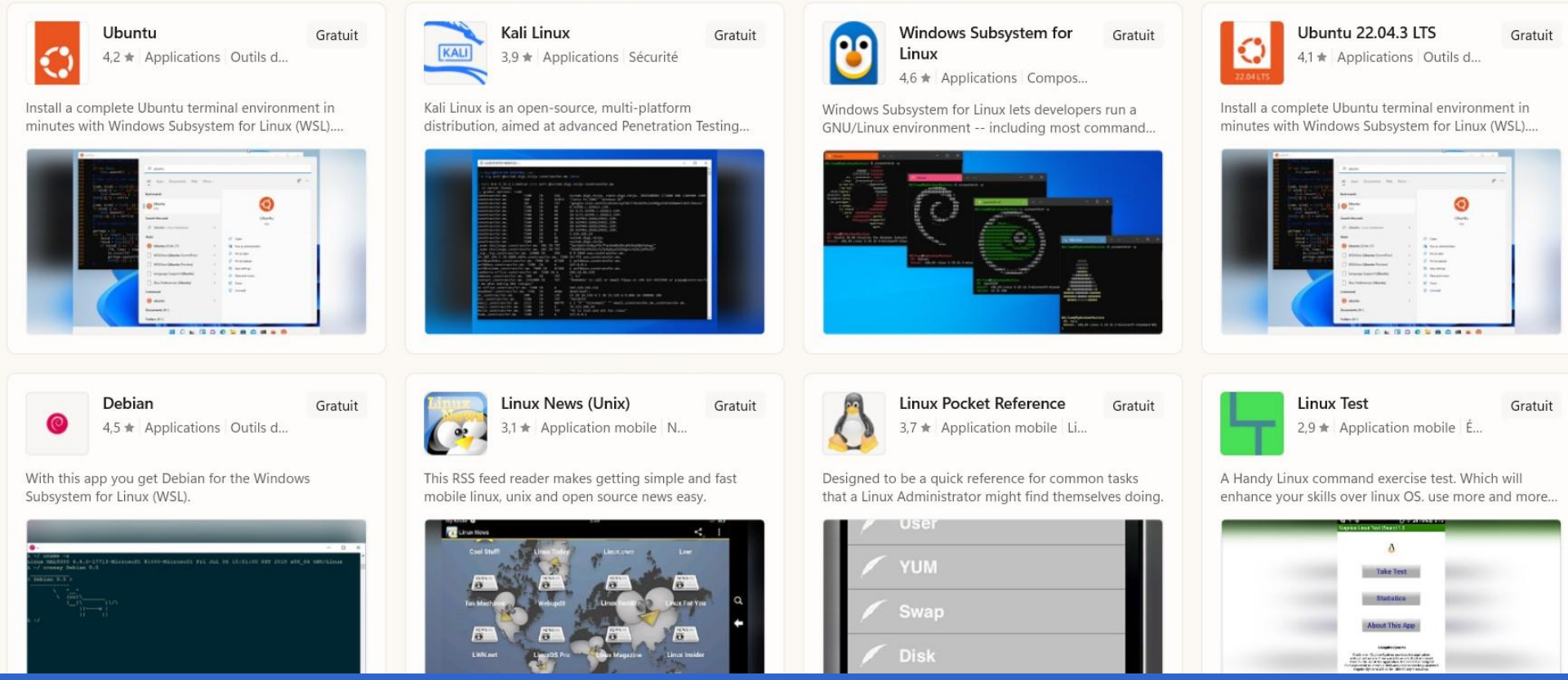
Activate WSL2 in control panel



© Thierry Joubert 2024

Install a distribution

- Native WSL2 is limited to the Kernel
  - Complete system services are in a “distribution”
  - Many flavors available in the Windows Store



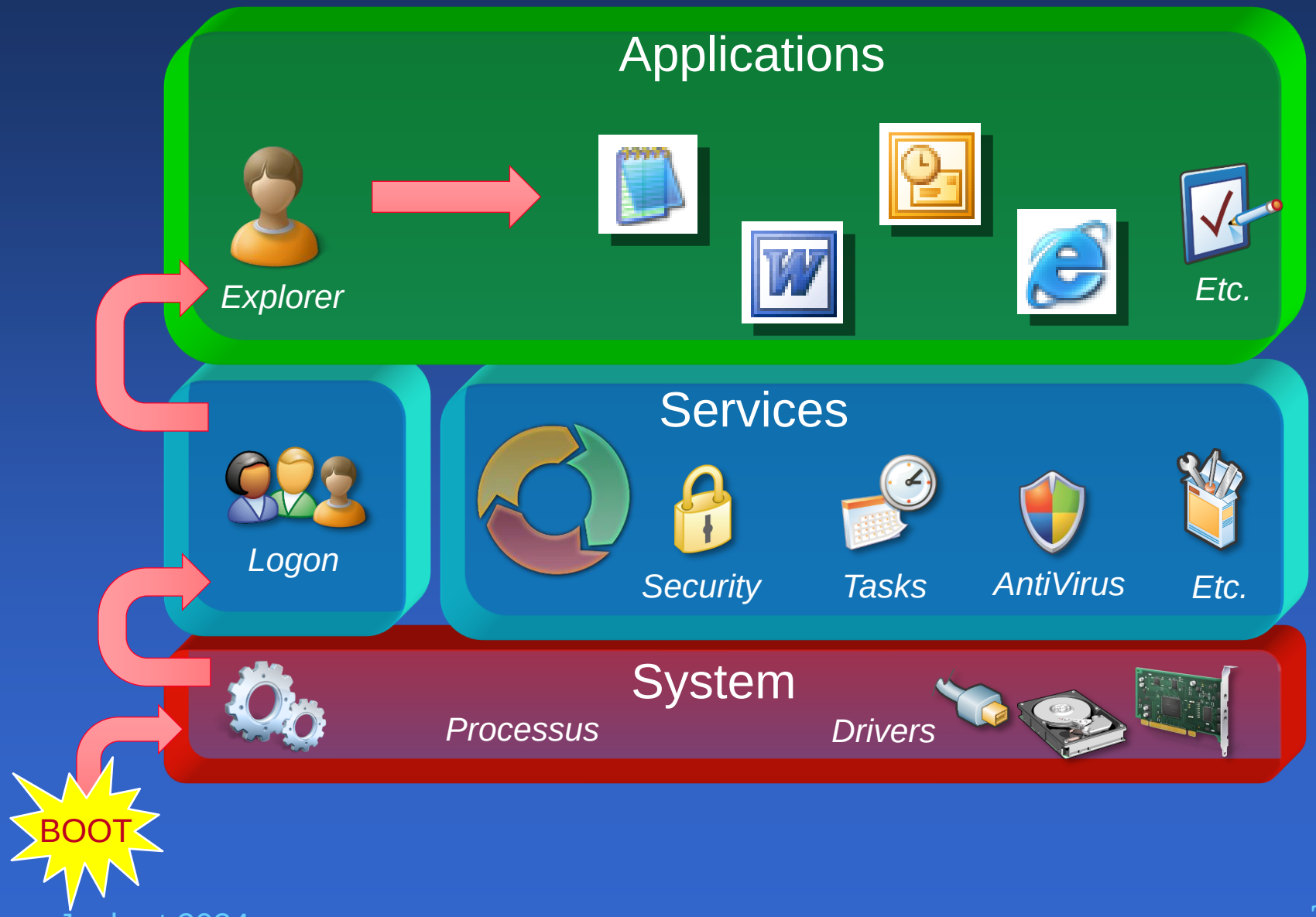
© Thierry Joubert 2024

Windows Services

Background activities

© Thierry Joubert 2024

Software layers



© Thierry Joubert 2024

Services processus

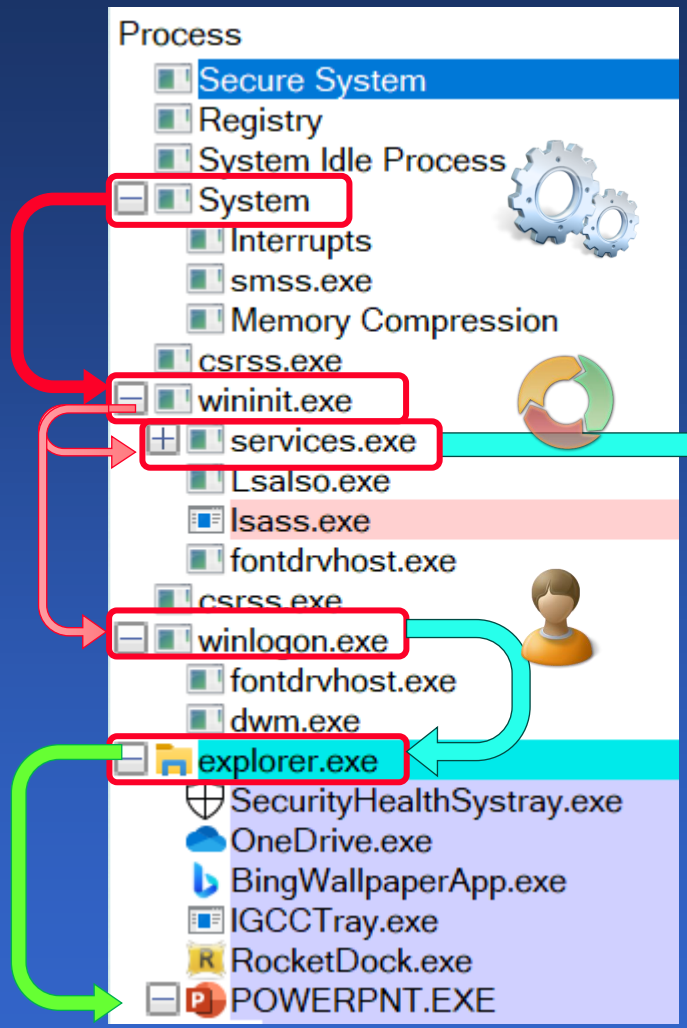
- Run before logon
  - Use system identities
- Run in the background
  - Cannot display windows of any type
  - Print in a system log (event viewer)
  - May display icons in the SYSTRAY

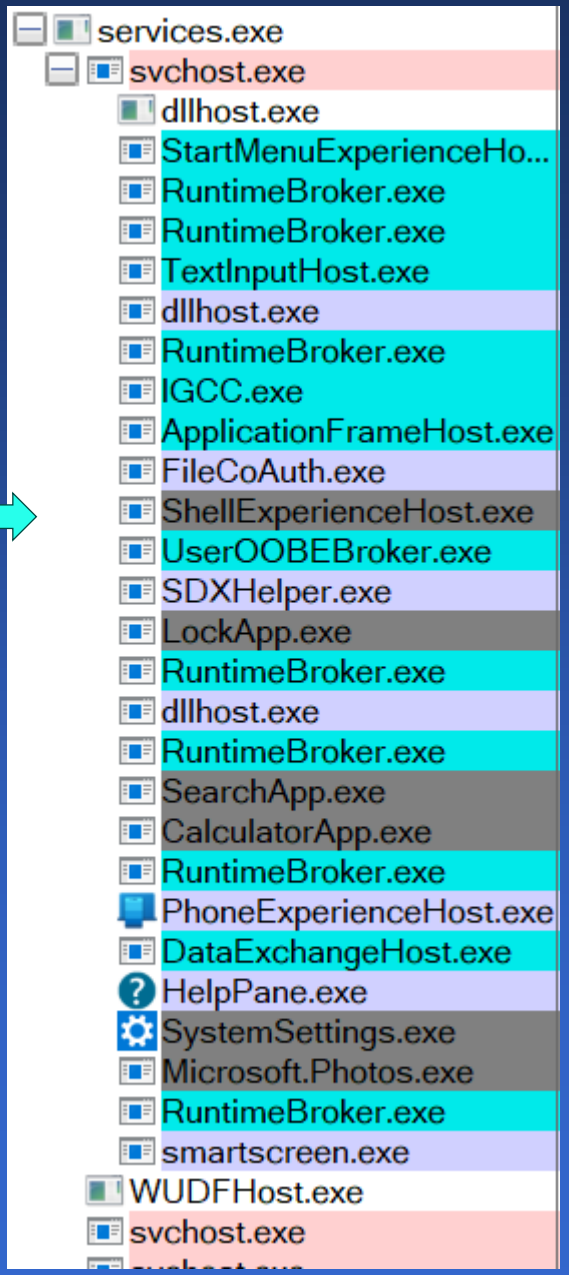
- Are controlled by the logged user
  - START
  - STOP
  - PAUSE

© Thierry Joubert 2024

Windows Sysinternals

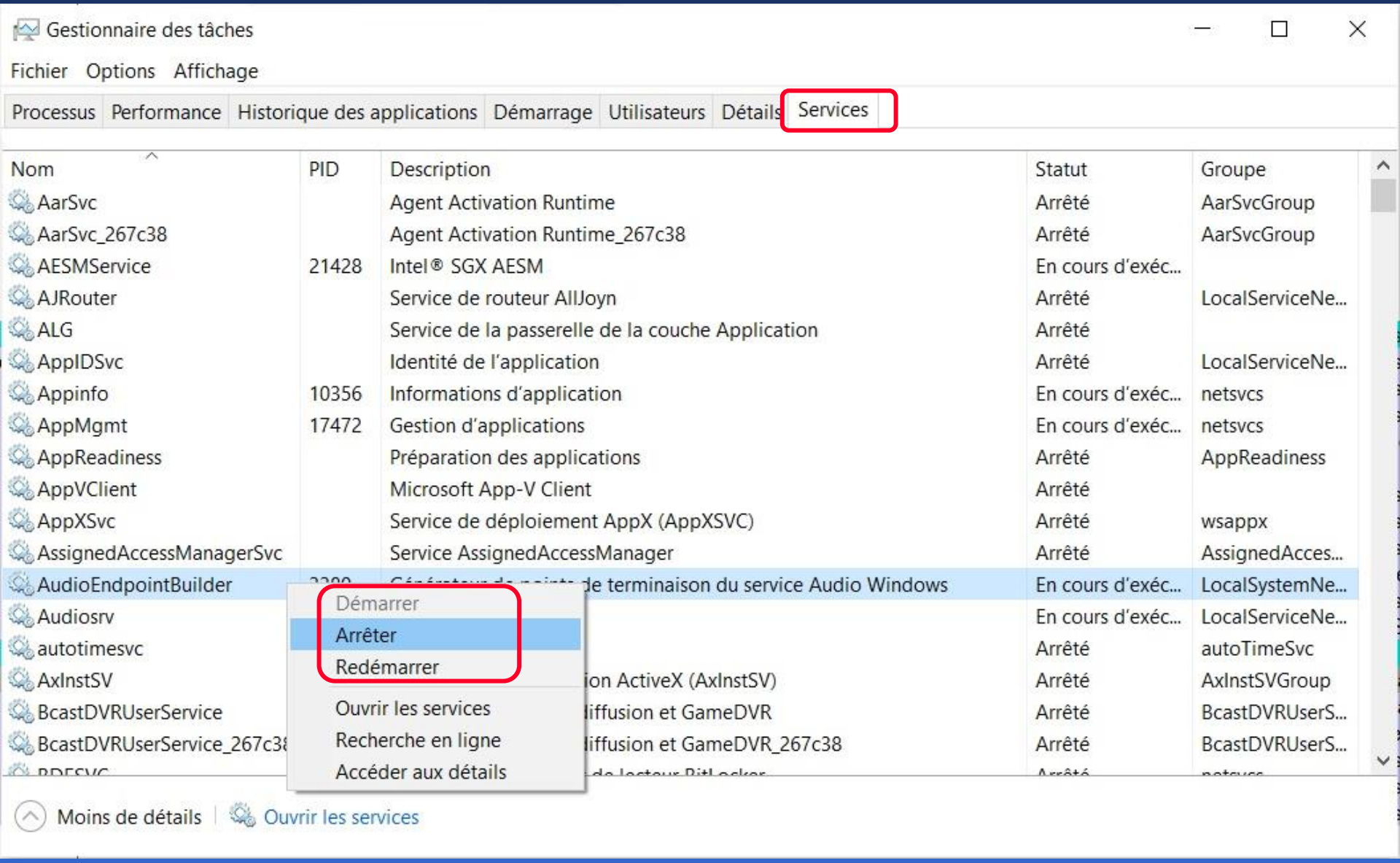
Process hierarchy





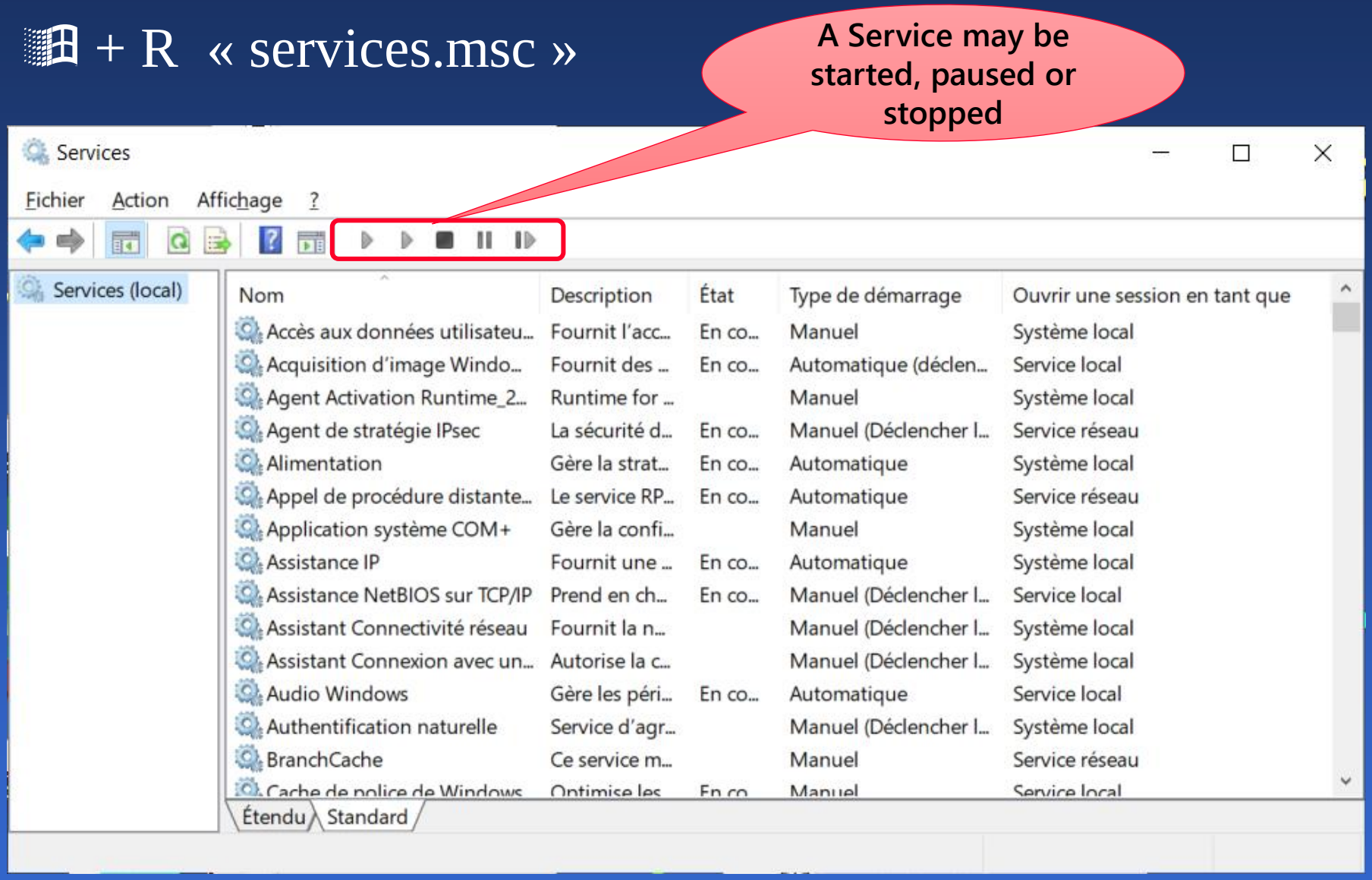
© Thierry Joubert 2024

Services in the Task Manager



Services console

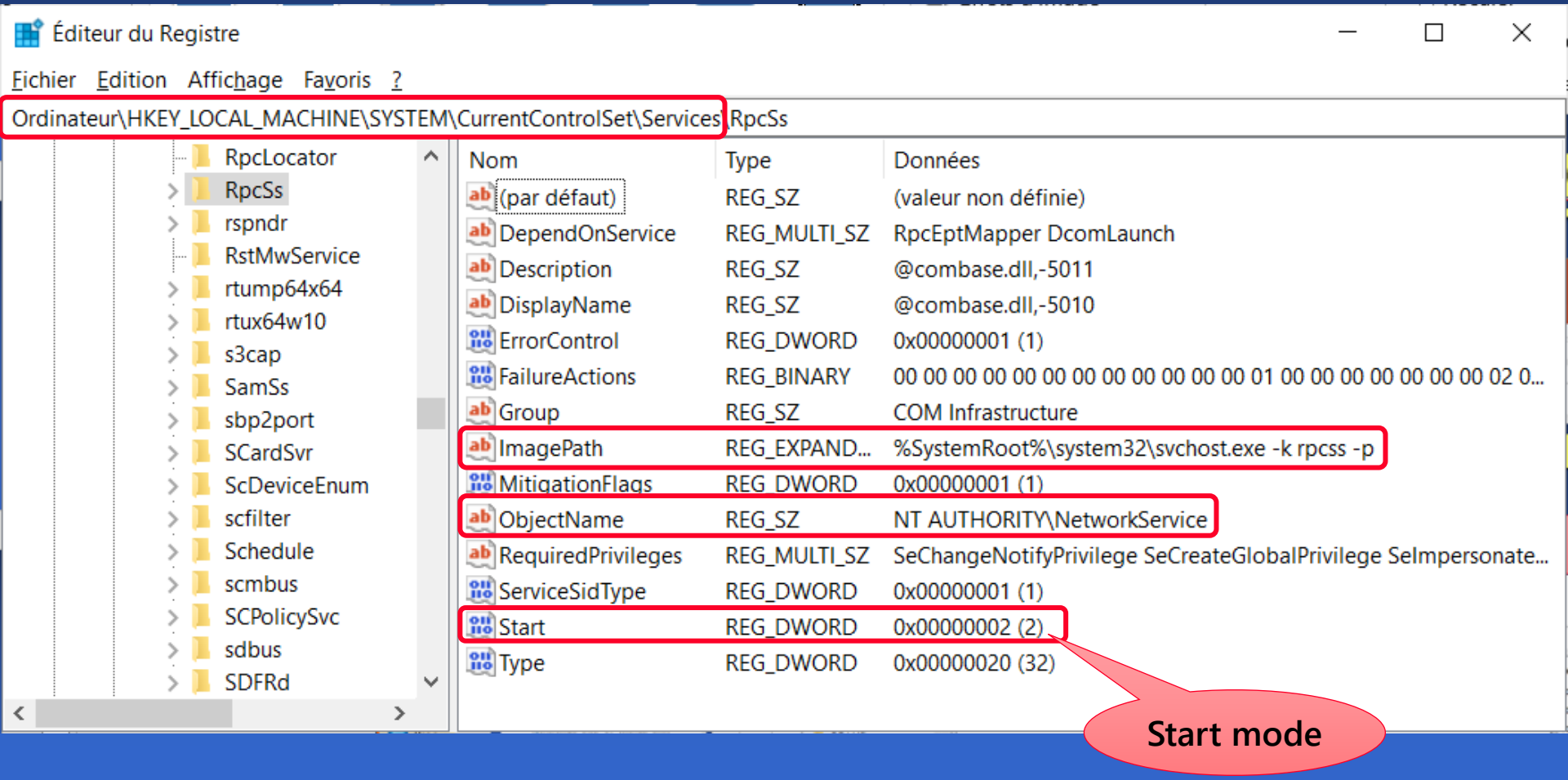
⊞ + R « services.msc »



© Thierry Joubert 2024

Services in the registry

HKLM/SYSTEM/CurrentControlSet/Services



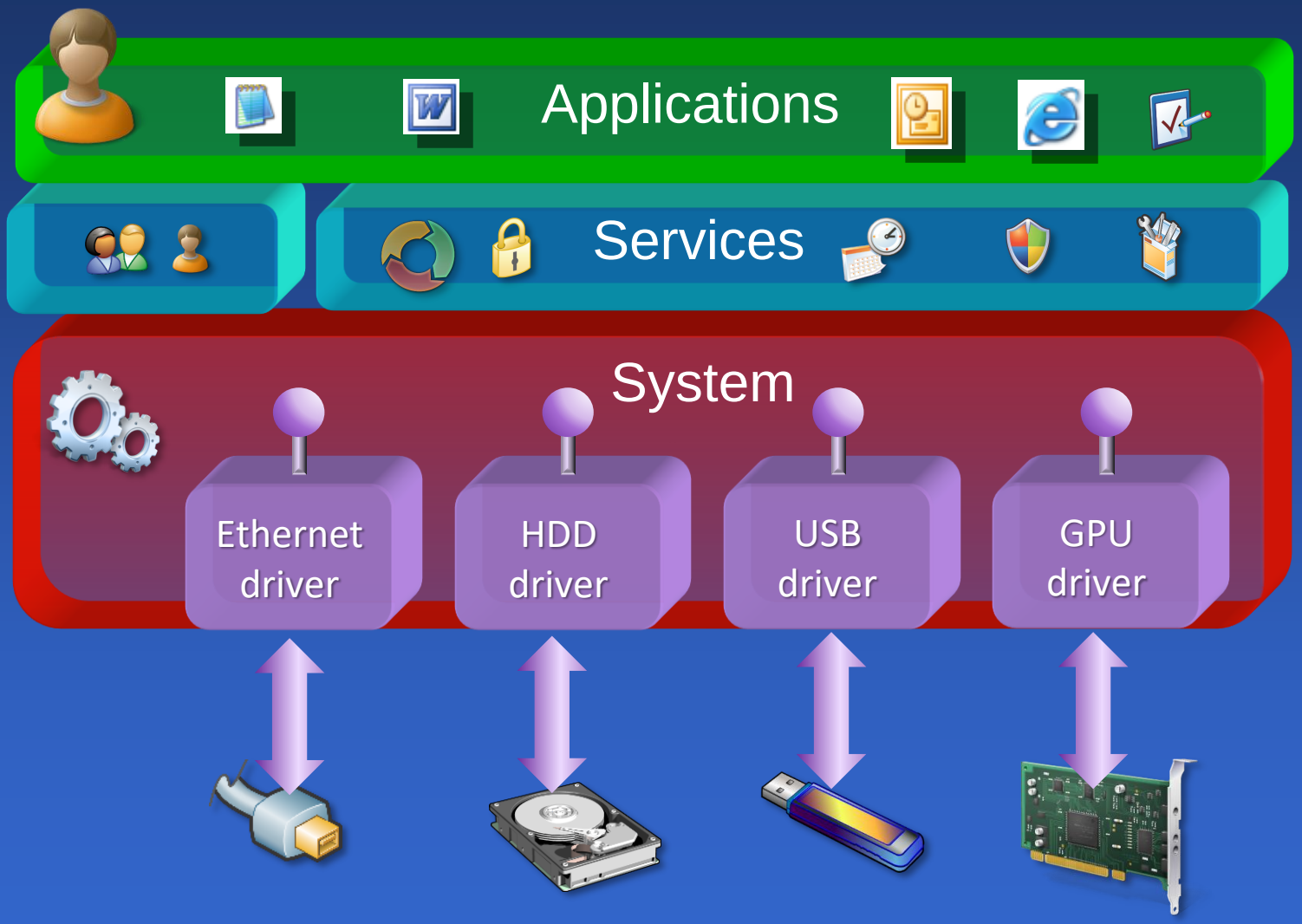
© Thierry Joubert 2024

Windows Drivers

Harware control

© Thierry Joubert 2024

Low level Software layers



© Thierry Joubert 2024

Windows Drivers

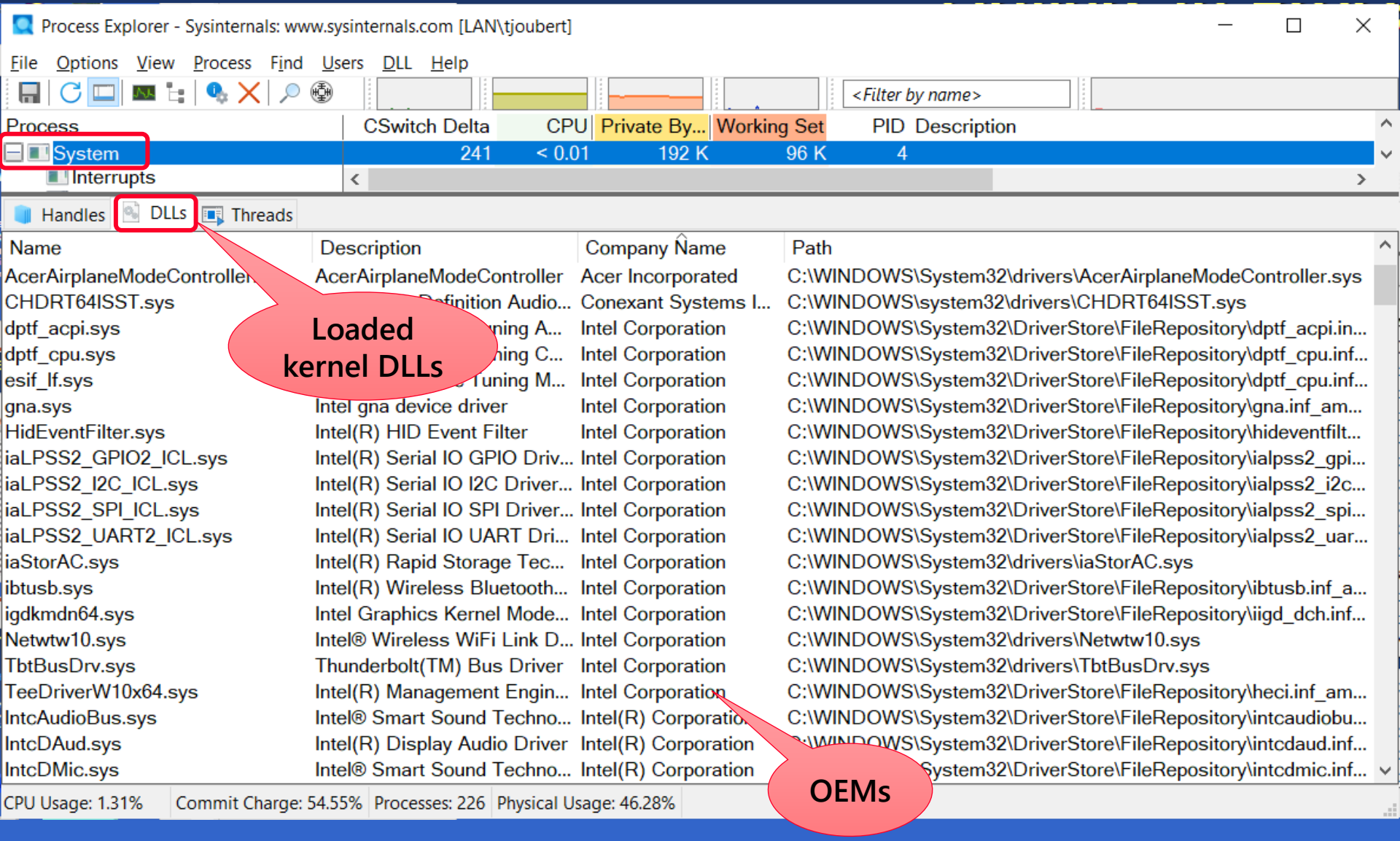
- Plug-in Kernel modules
  - Dynamic link modules *(DLL structure)*
  - Loaded by the Kernel *(.SYS extension)*
  - Run at Kernel level *(Intel ring 0 = privileged)*

- OEM software
  - Link with Kernel libraries
  - Dedicated IDE (Win DDK)
  - Third party kernel module may be a Threat
    - BUGS → MS driver certification process
    - VIRUS → MS driver signing process

© Thierry Joubert 2024

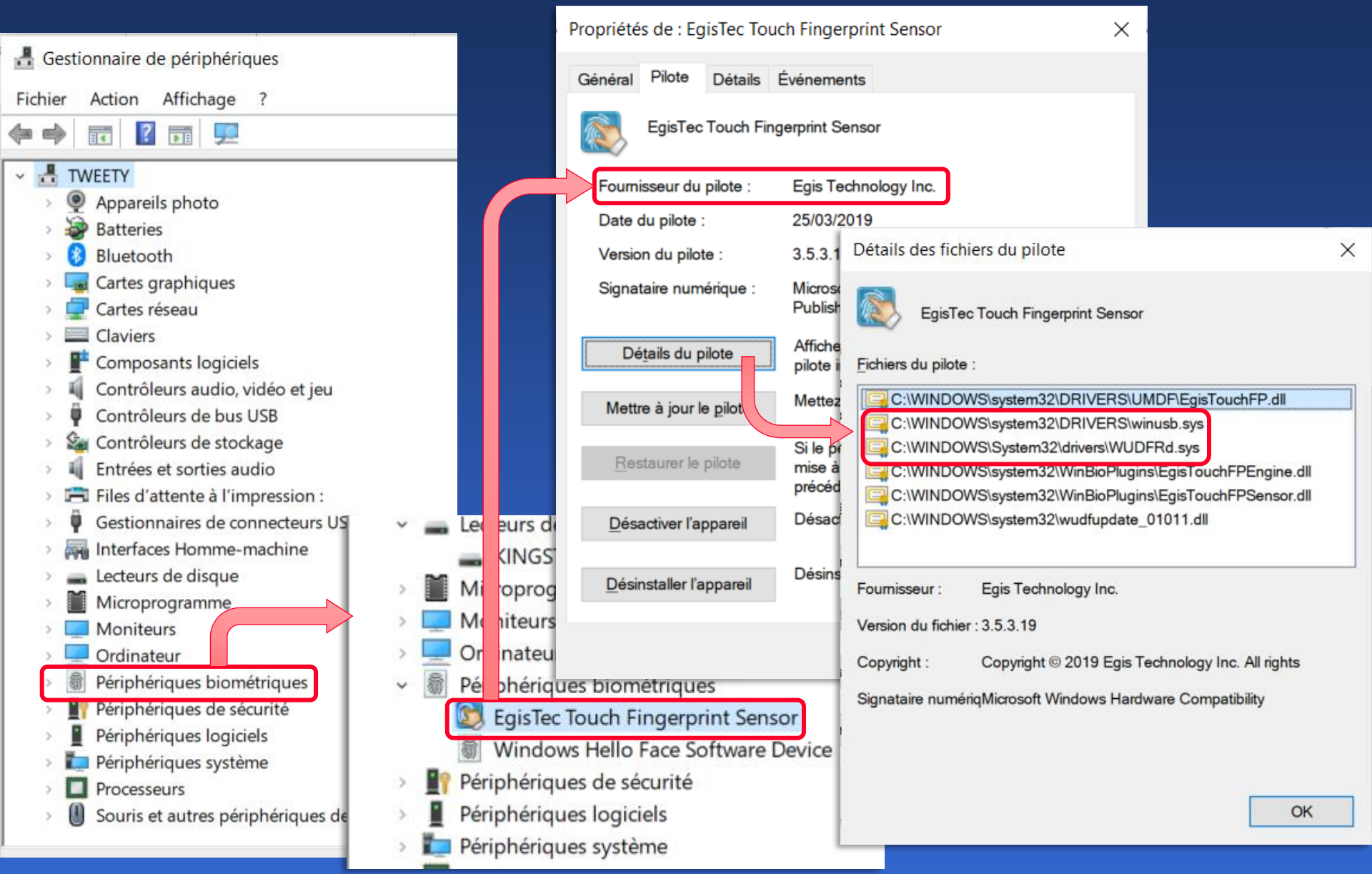
Windows Sysinternals

Drivers in Procexp



© Thierry Joubert 2024

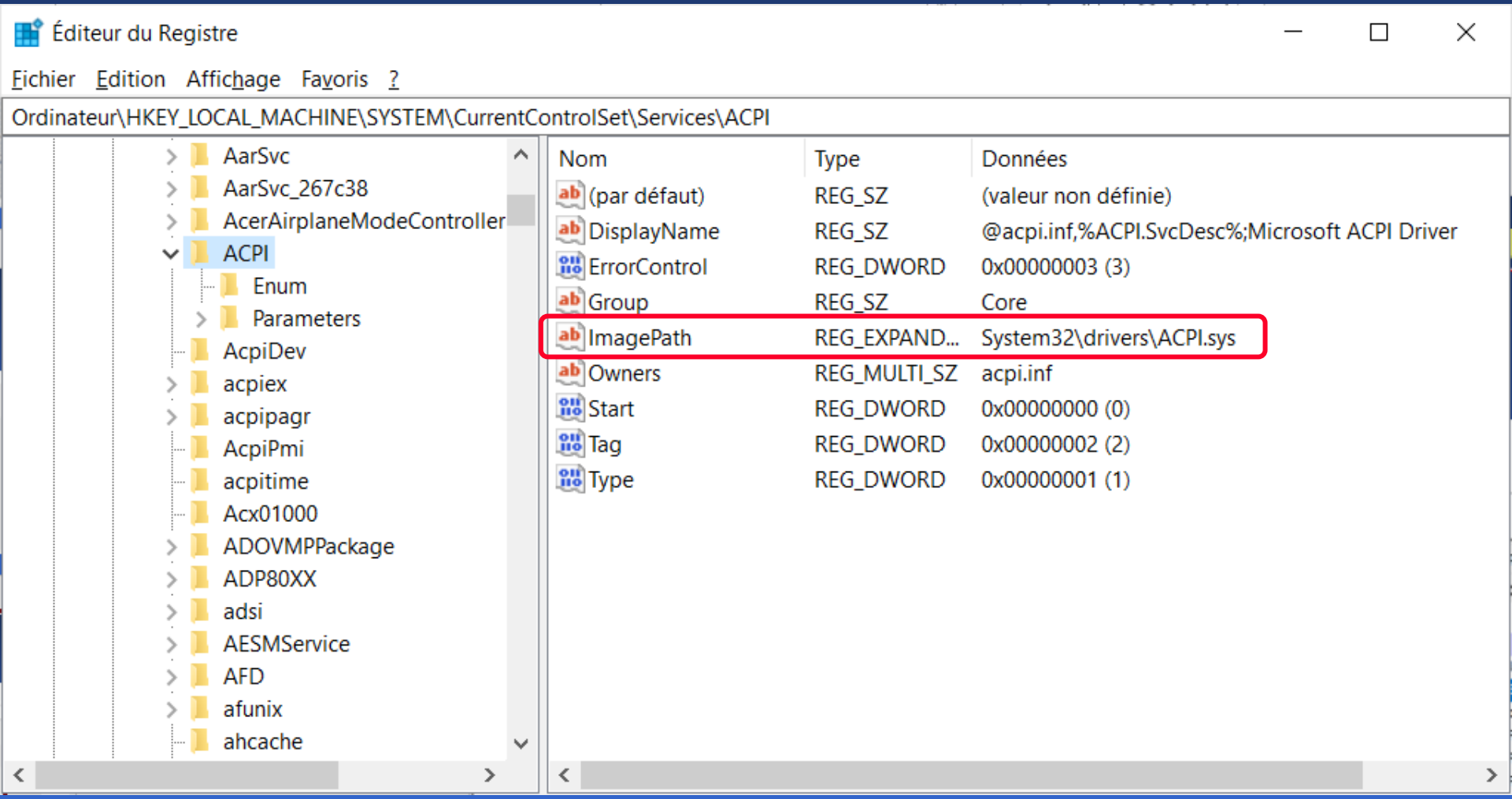
drivers in Computer Management



© Thierry Joubert 2024

Drivers in the Registry

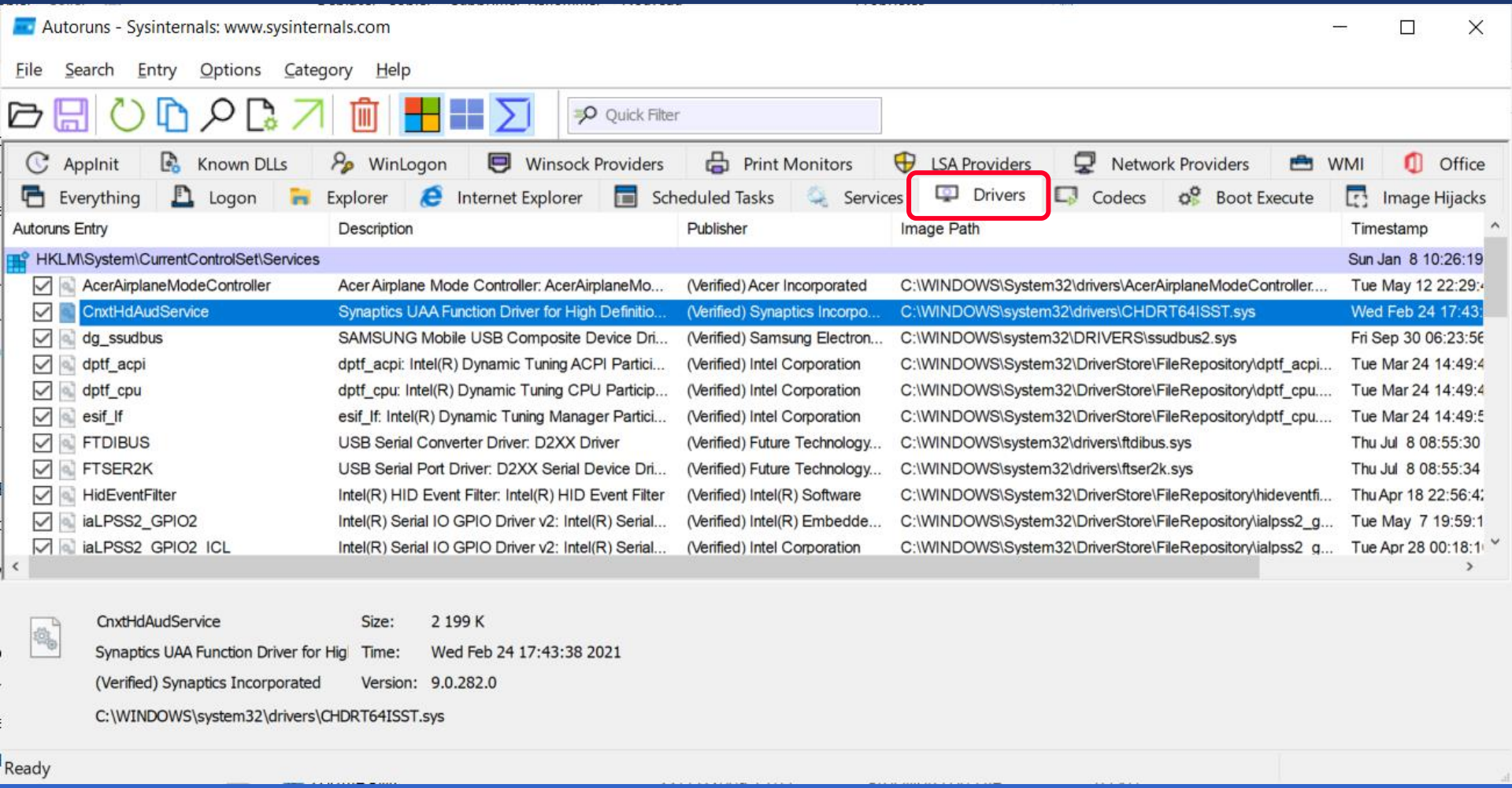
HKLM/SYSTEM/CurrentControlSet/Services



© Thierry Joubert 2024

Windows Sysinternals

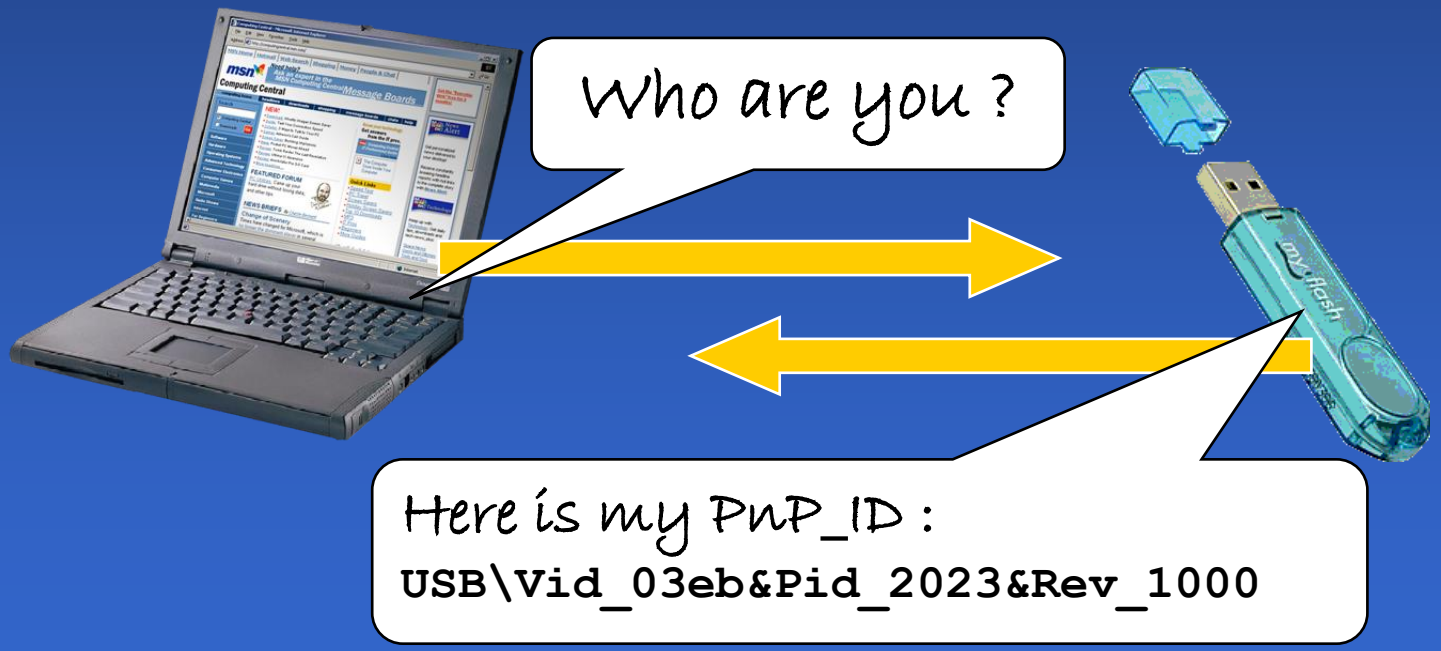
Drivers in Autoruns



© Thierry Joubert 2024

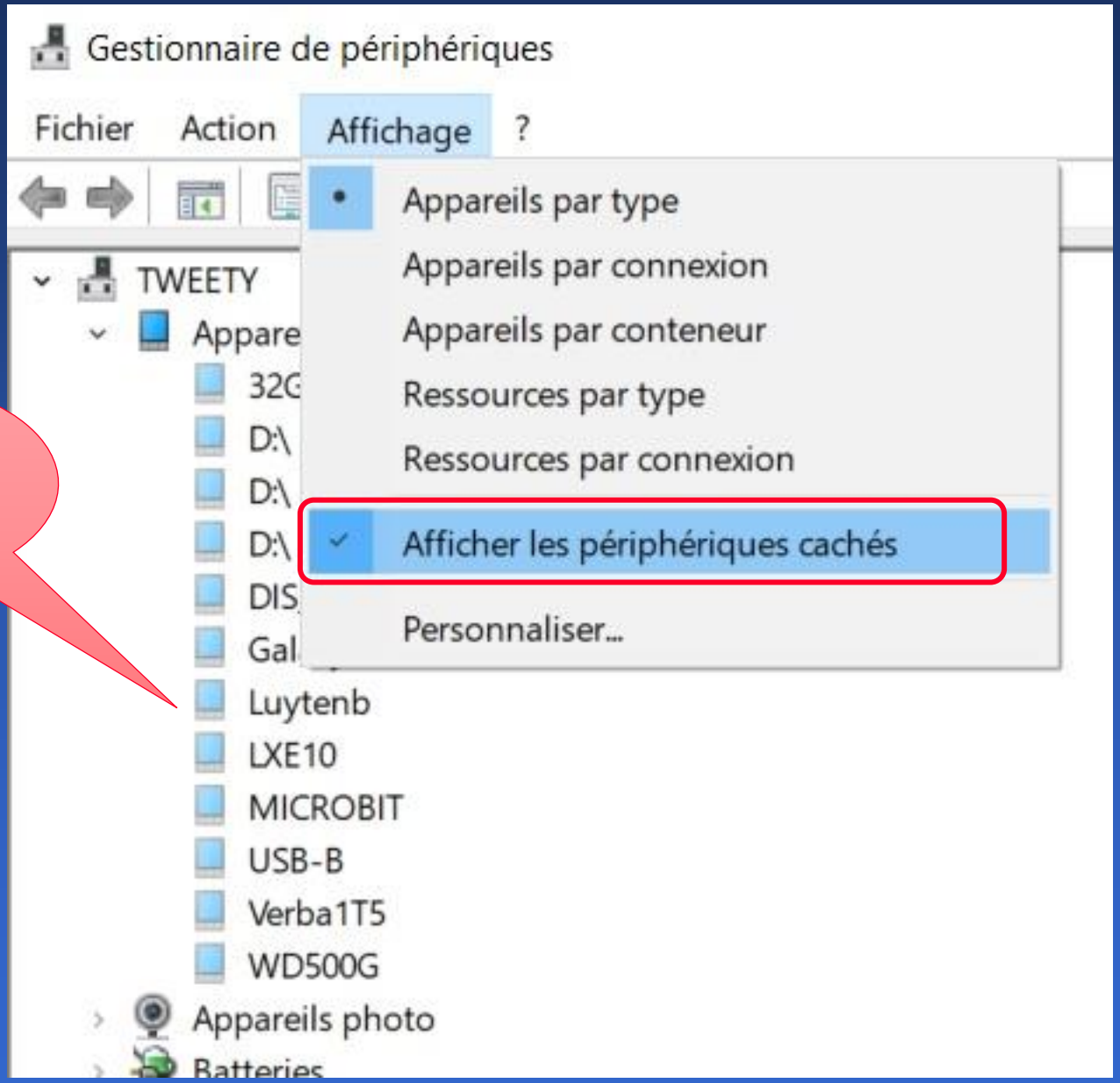
Hardware unique IDs

- Hardware query
  - Fixed devices (PCI …) in HKLM/HARDWARE
  - Runtime Query protocol for Plug&Play devices
- Each device type has a UNIQUE ID



© Thierry Joubert 2024

Known Plug&Play devices



USB keys
Phones
Etc.

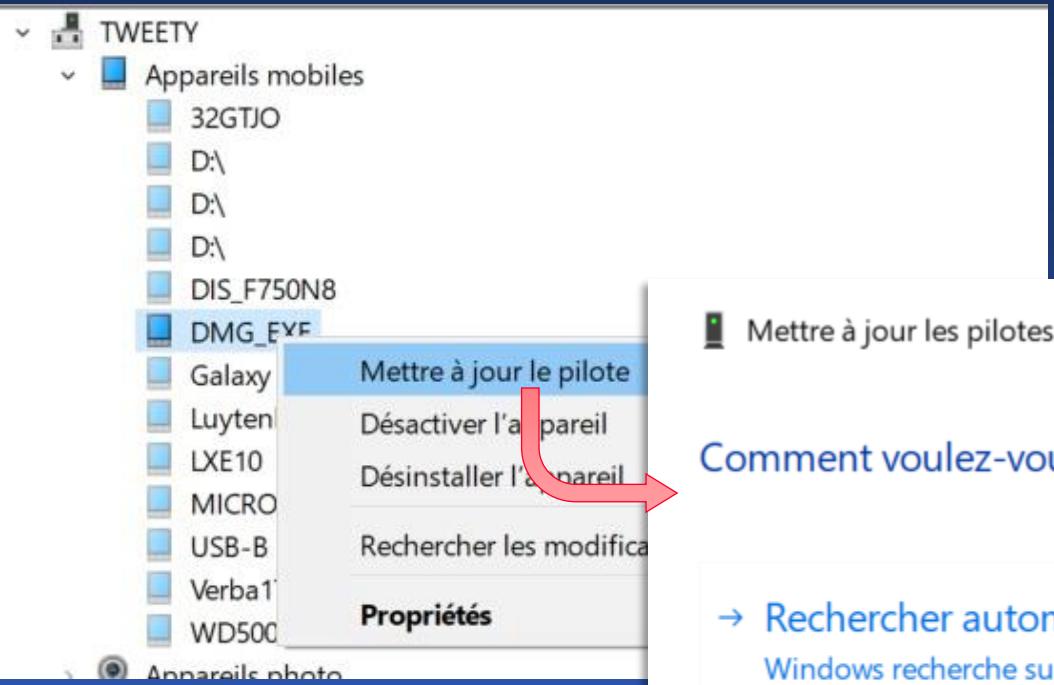
© Thierry Joubert 2024

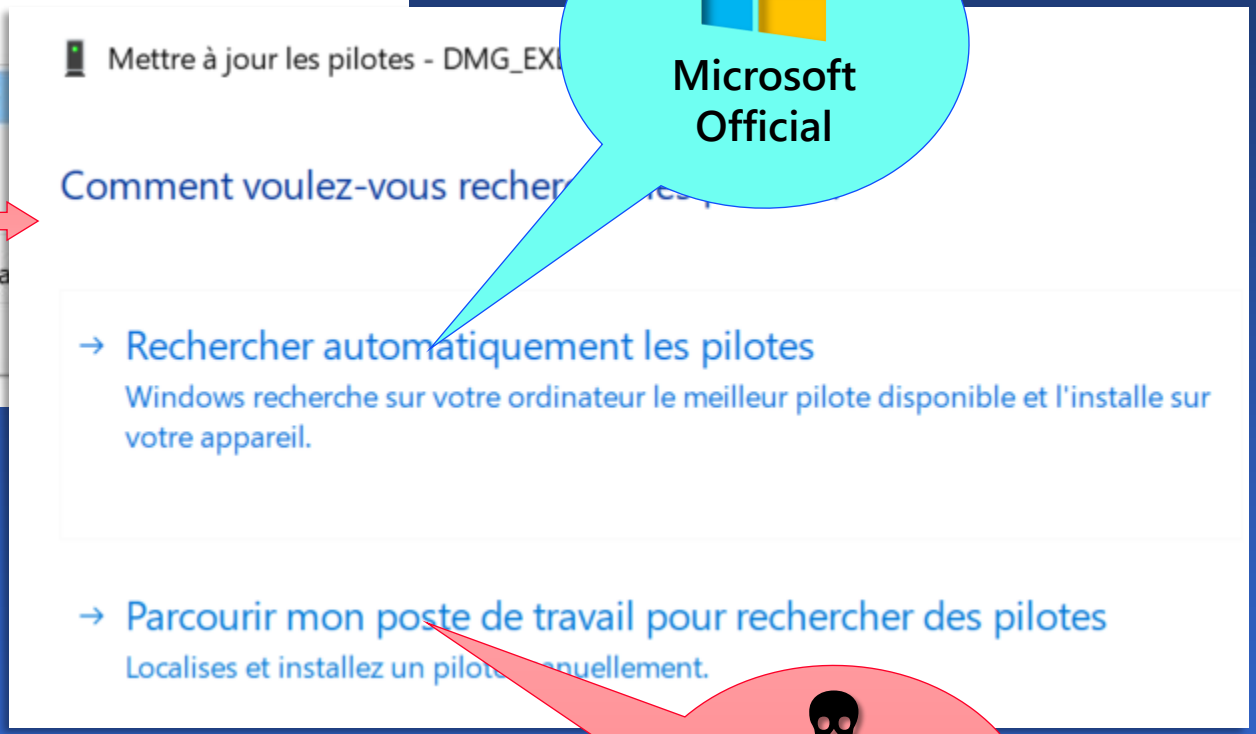
Driver update & Install sources

- Microsoft official repository
  - Contains WindowsUpdate & OEM Drivers
  - MSFT certified OEM drivers
    - Bug free
    - Valid signature
  - This MUST always be your first try
- OEM official Web repository
  - Installers (setup.exe, etc.)
  - Driver packages (.zip files)
  - This is only a second choice… for « weak » OEMs
- Drivers HoneyPots *(top Search results)*
  - Malware, Spamware Inc.
  - Keep away - unless you REALLY know what you do!

© Thierry Joubert 2024

Driver manual installation



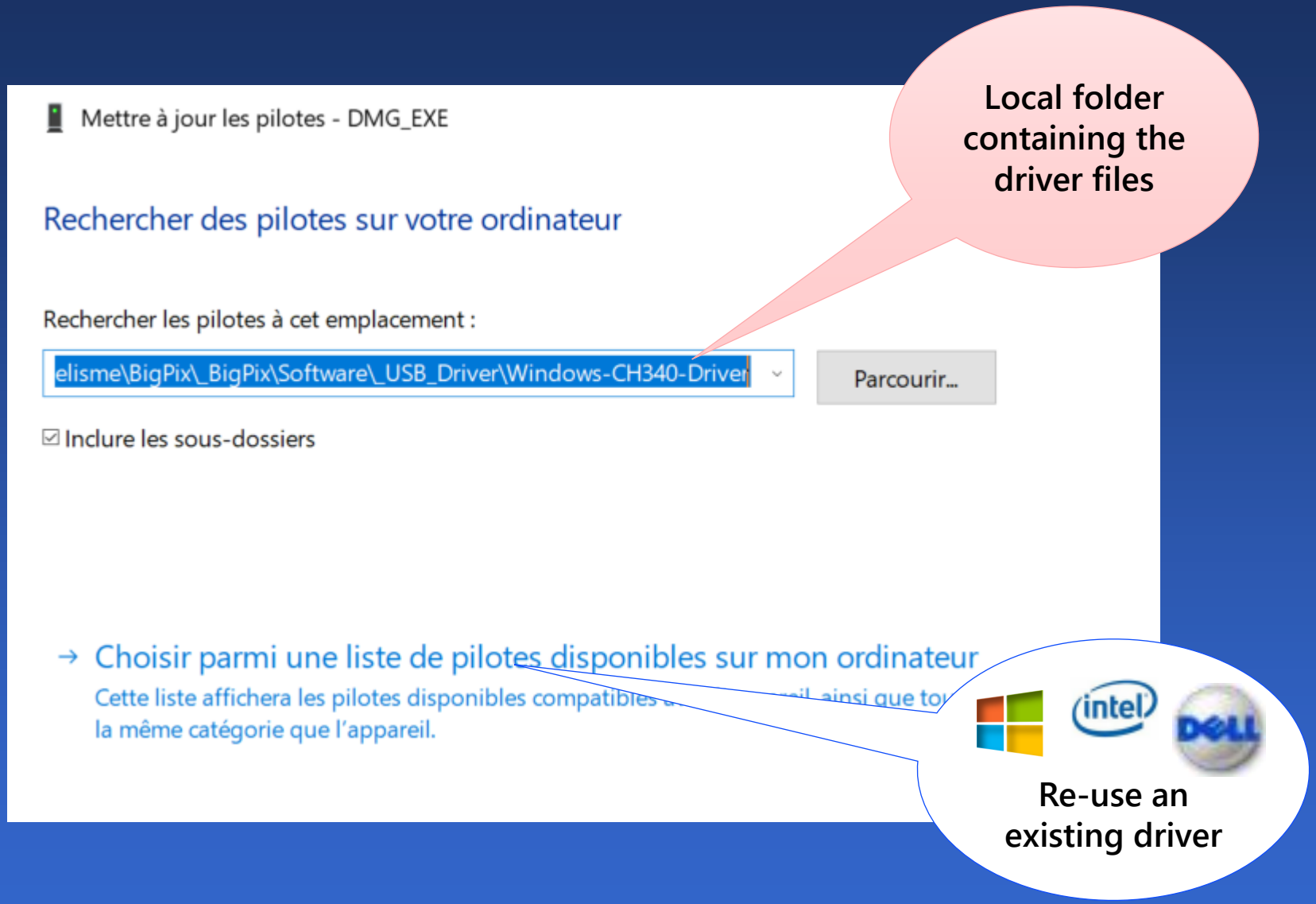


Microsoft Official

Potential road to HELL

© Thierry Joubert 2024

Install an OEM driver



© Thierry Joubert 2024

Files of an OEM Driver

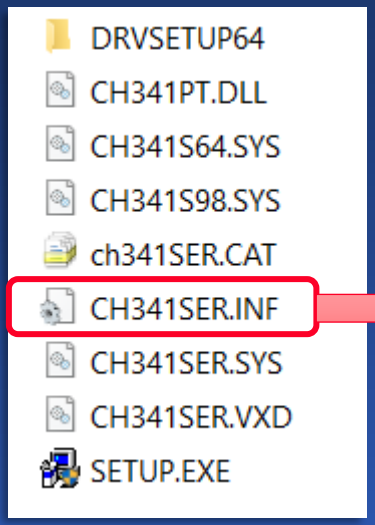
- OEM installation script → `.inf`
  - Go to `/Windows/inf`
  - `Manufacturer` section = Hardware_ID

```
%USB\VID_1194&PID_0004.DeviceDesc%=FB11USB.Dev, USB\VID_1194&PID_0004
```

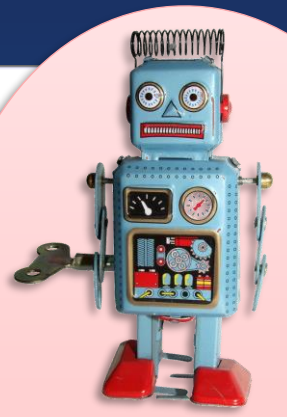
  - `AddReg` section = Registry actions
  - `CopyFiles` section = Files copy
- Kernel DLL → `.sys`
  - Go to `/Windows/System32/drivers`
- User code → `.exe, .dll, .cpl`
  - Go to `/Windows/System32`

© Thierry Joubert 2024

Example of OEM driver



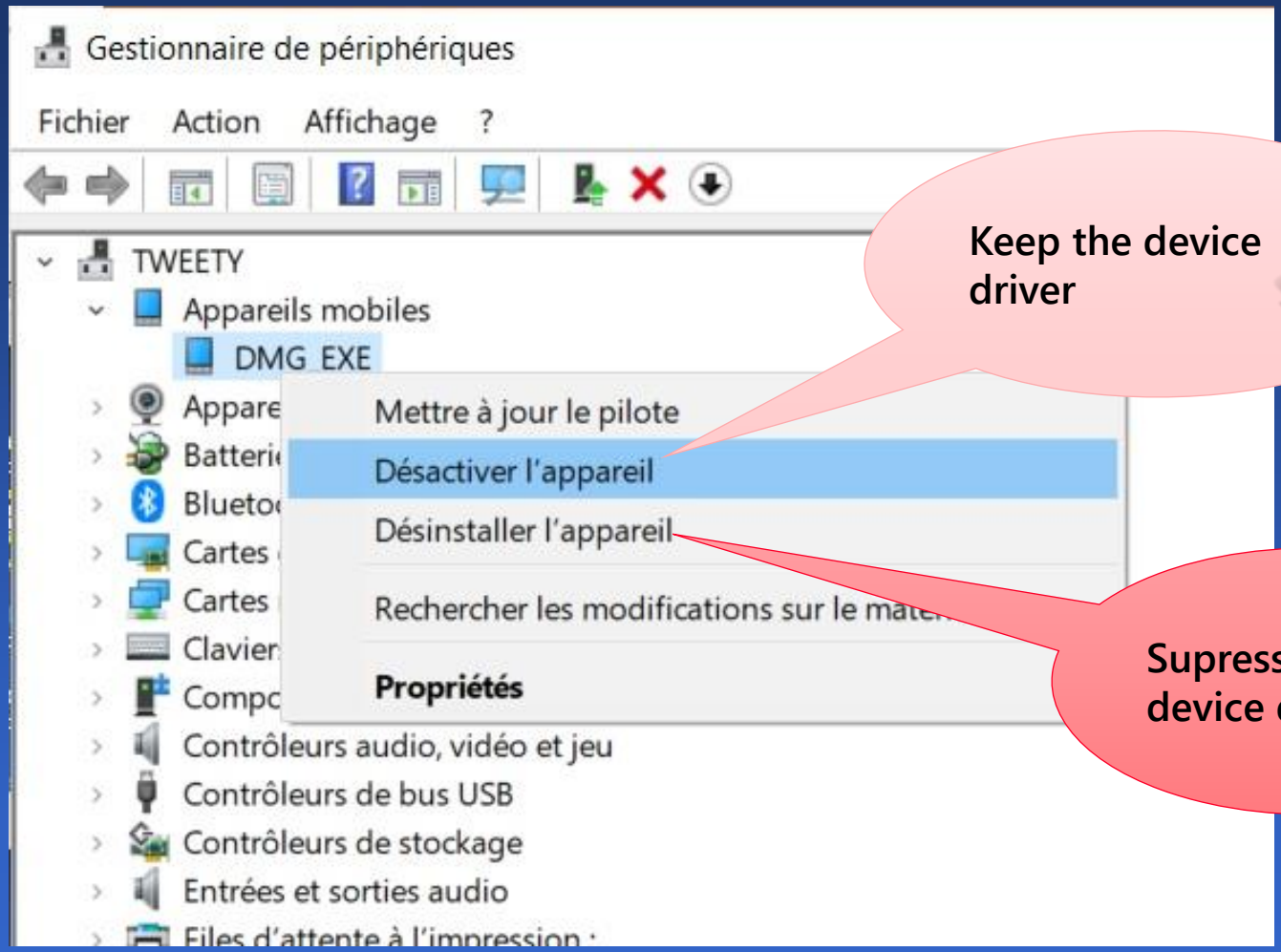

```
; CH341SER.INF
; Driver for CH341 (USB=>SERIAL chi
; WDM&VXD for Windows 98/Me/2000/XP                    /64b
; Copyright (C) W.ch 2001-2014
;

[Version]
Signature = "$Chicago$"
Class     = Ports
ClassGuid = {4D36E978-E325-11CE-BFC1                   }
Provider  = %WinChipHead%
DriverVer = 08/08/2014, 3.4.2014.0
CatalogFile = CH341SER.CAT

[ControlFlags]
ExcludeFromSelect = USB\VID_1A86&PID_7523
ExcludeFromSelect = USB\VID_1A86&PID_5523
ExcludeFromSelect = USB\VID_4348&PID_5523
ExcludeFromSelect = USB\VID_4348&PID_5523&REV_0250
ExcludeFromSelect = USBSERPORT\SER5523
ExcludeFromSelect = CH341PORT\SER5523

[Manufacturer]
%WinChipHead% = WinChipHead,NT,NTamd64,NTia64
```



OEM P&P IDs

© Thierry Joubert 2024

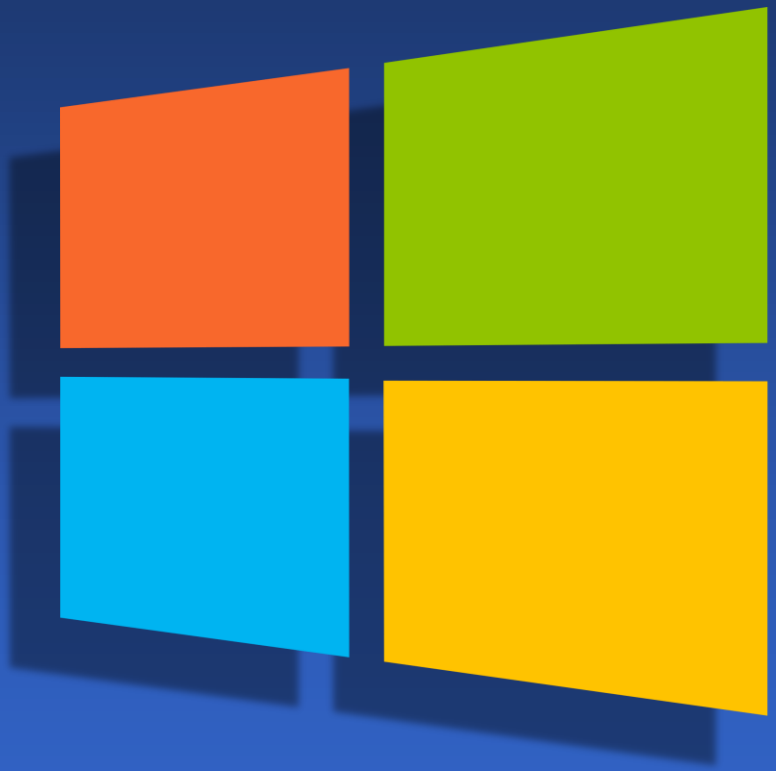
Device control



Keep the device driver

Supress the device driver

© Thierry Joubert 2024



© Thierry Joubert 2024