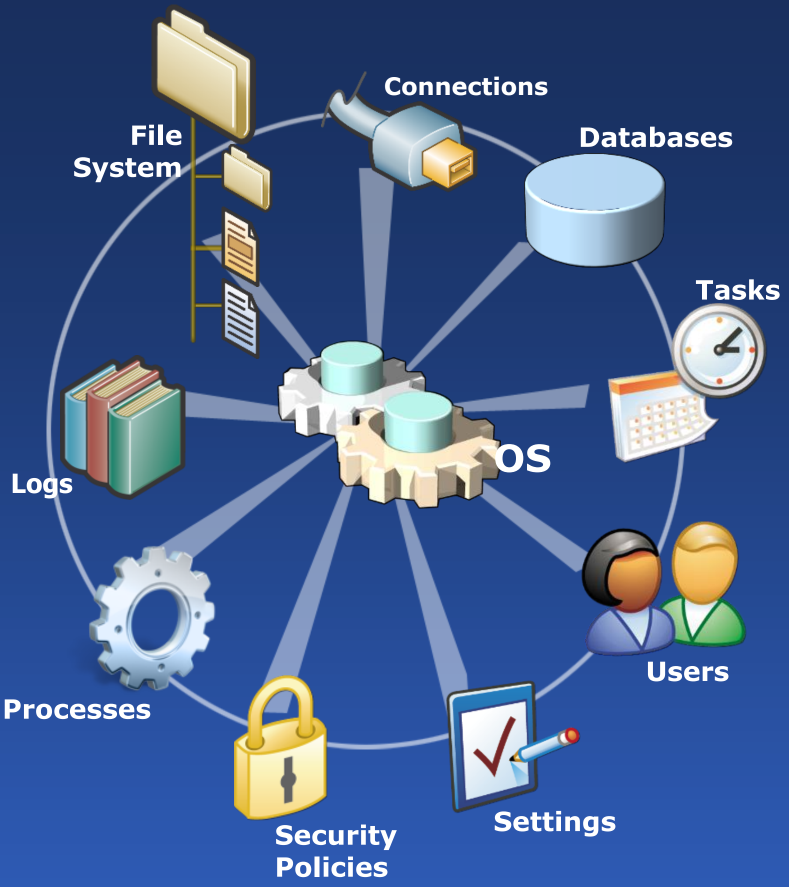
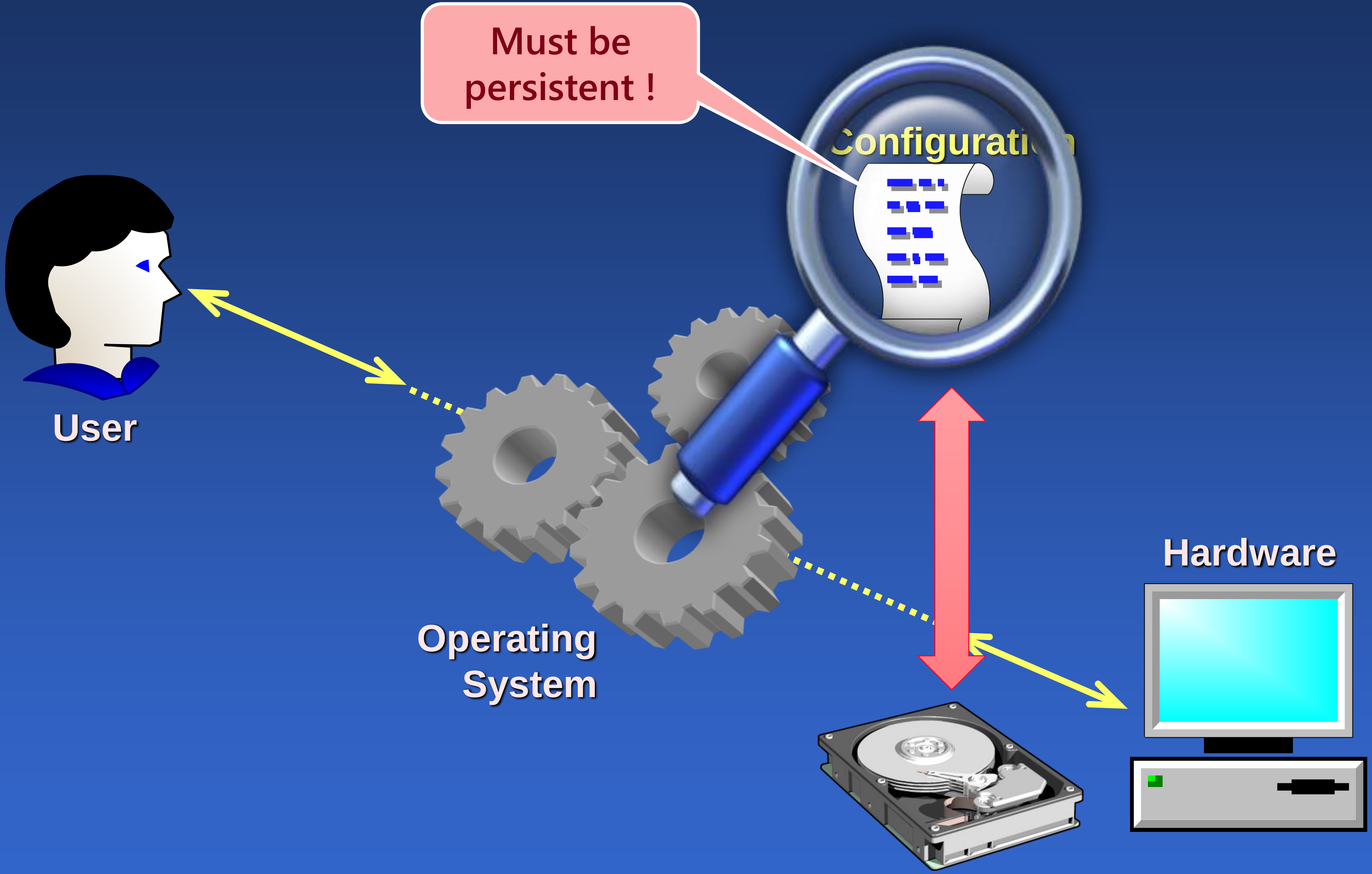
Use & Admin Windows
Survival Kit – 3 REGISTRY



System parameters

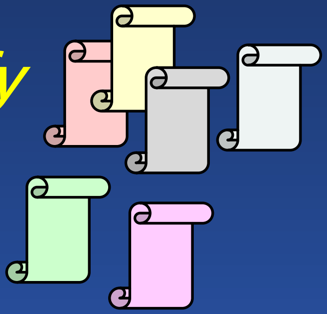
The Registry

Configuration

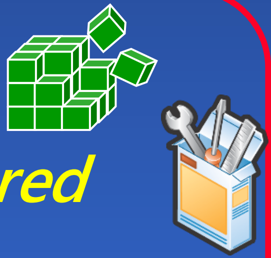


Configuration persitence

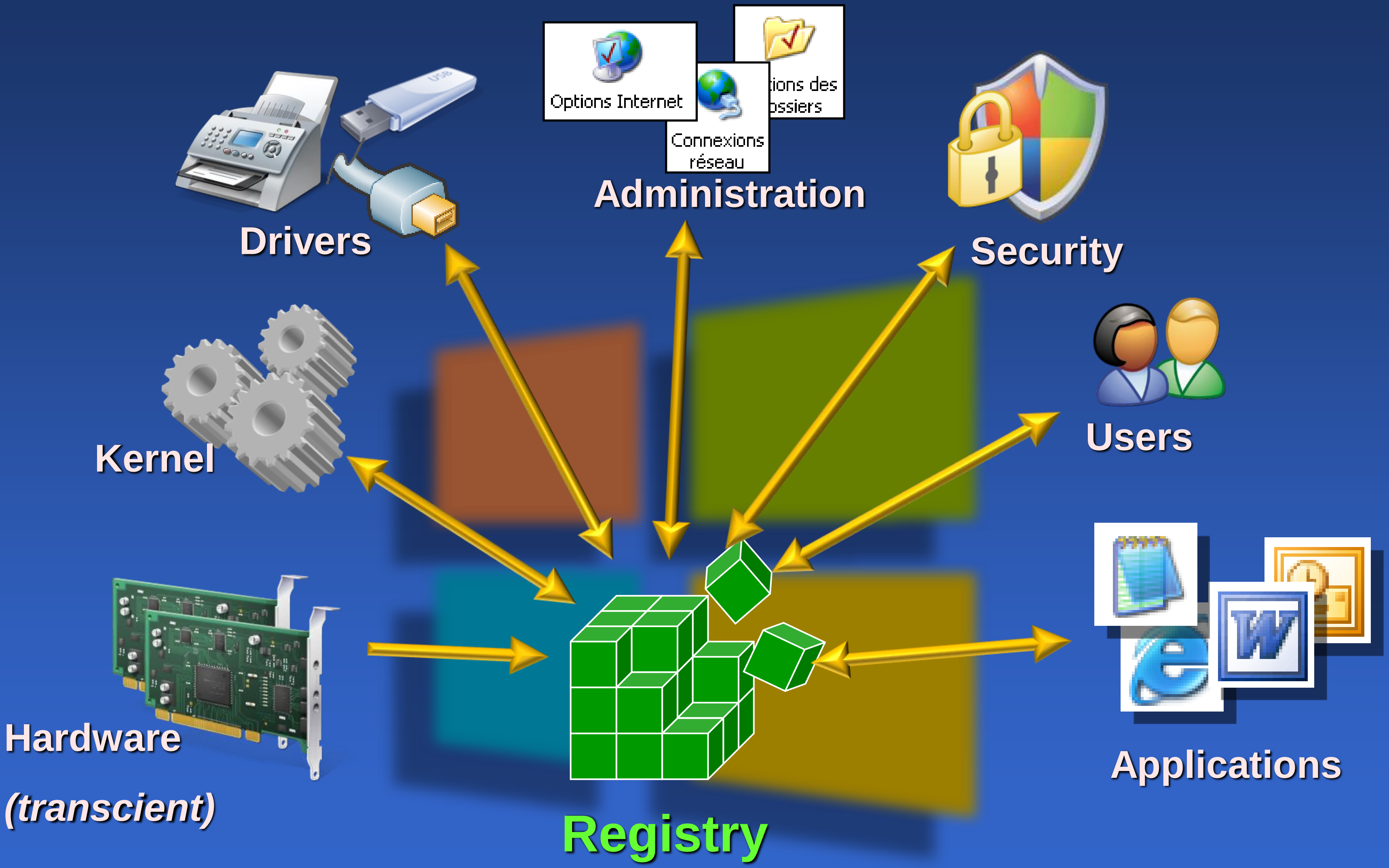
- ◆ UNIX choice → CONFIGURATION FILES
  - Dedicated text files → *Easy to consult/modify*
  - Permissions at the file level
  - Many different locations/names/formats
  - No automatic backup



- ◆ Windows choice → REGISTRY DATABASE
  - A unique binary database → *Tool or API is required*
  - Permissions at the parameter level
  - Centralized location
  - Automatic backup

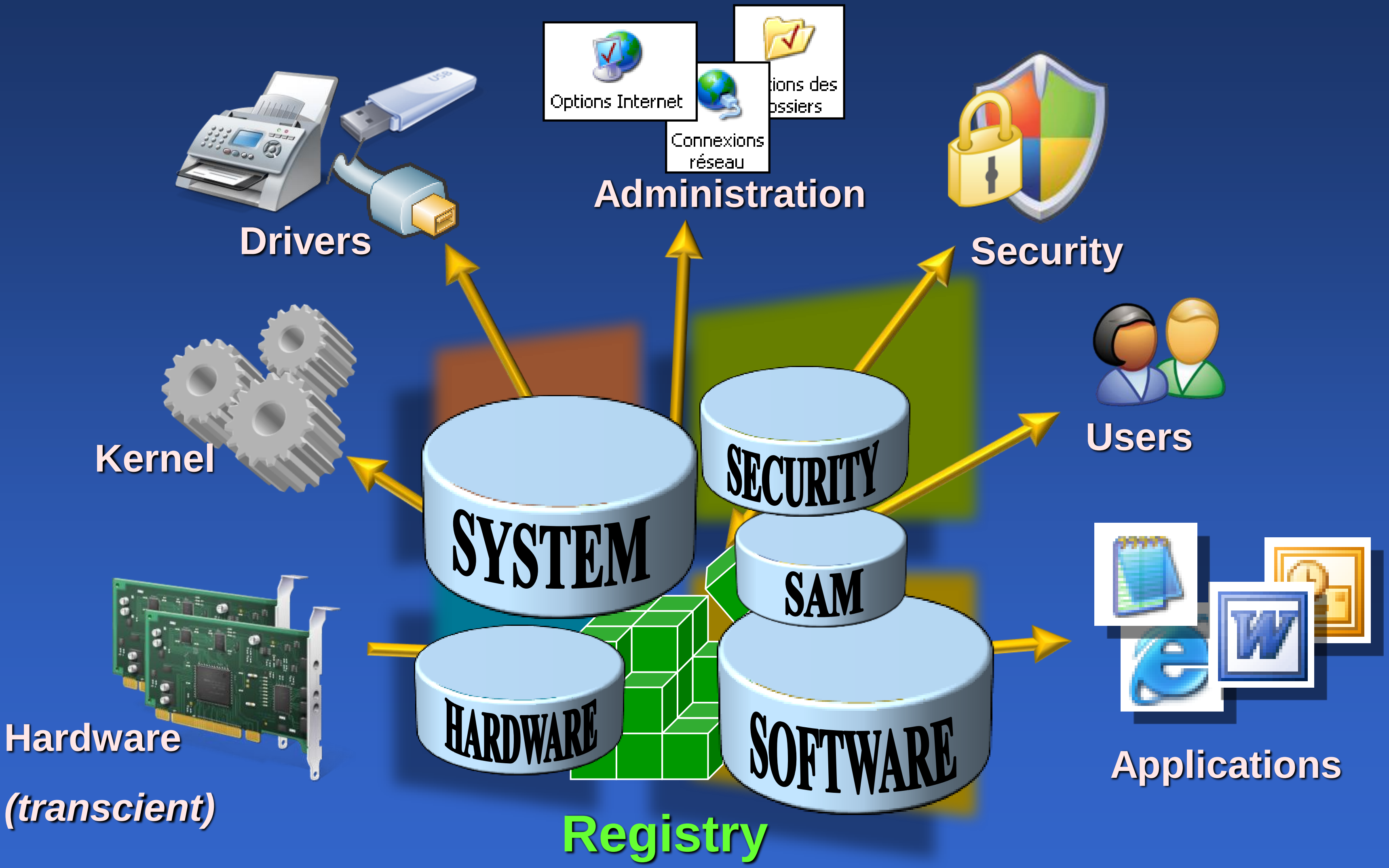


Registry Database



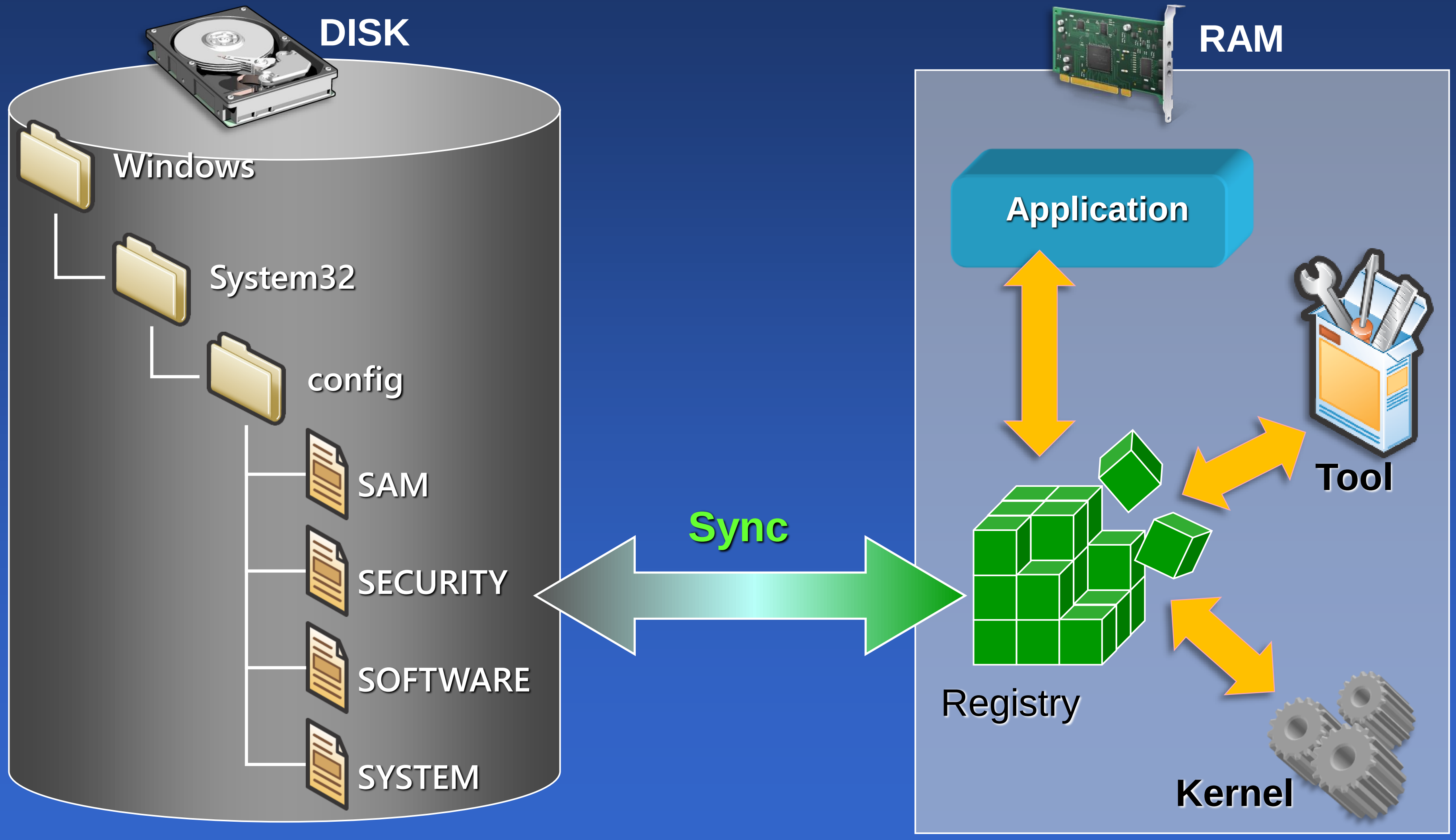
© Thierry Joubert 2022

Registry Hives *(stores)*

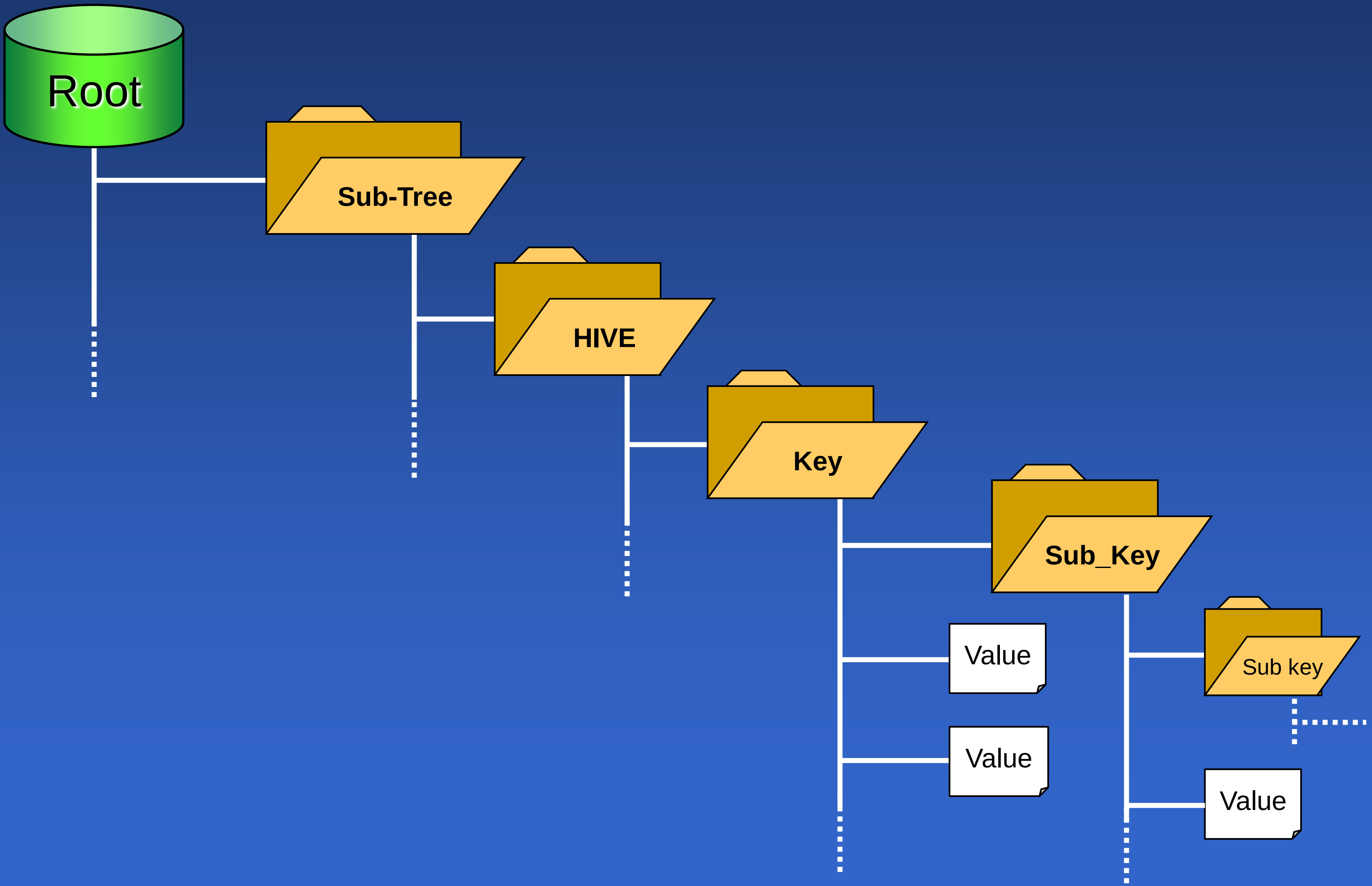


Registry at runtime

- Memory mapping

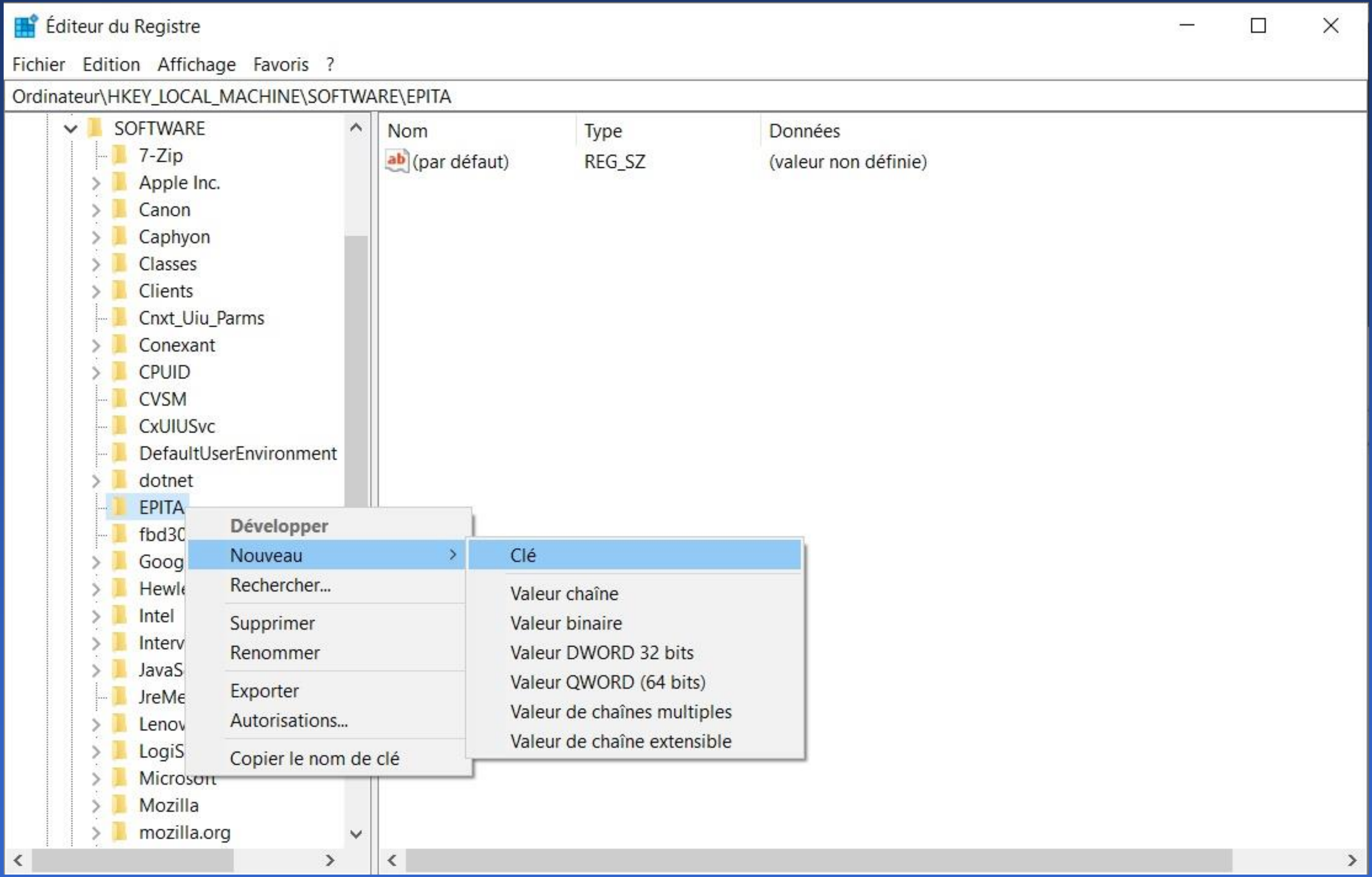


Registry organization



Registry tool

- Regedit → Browse & Edit the registry

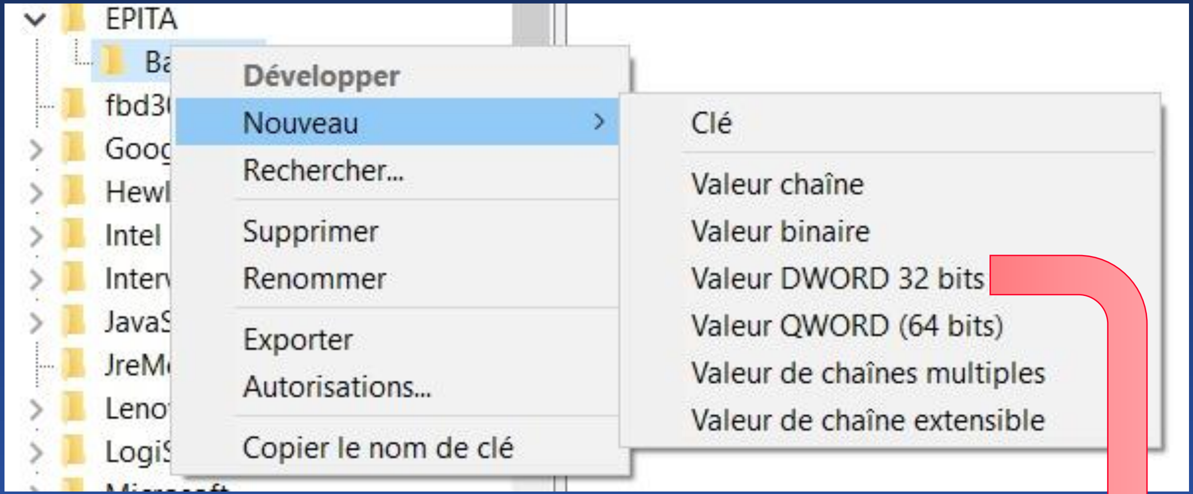


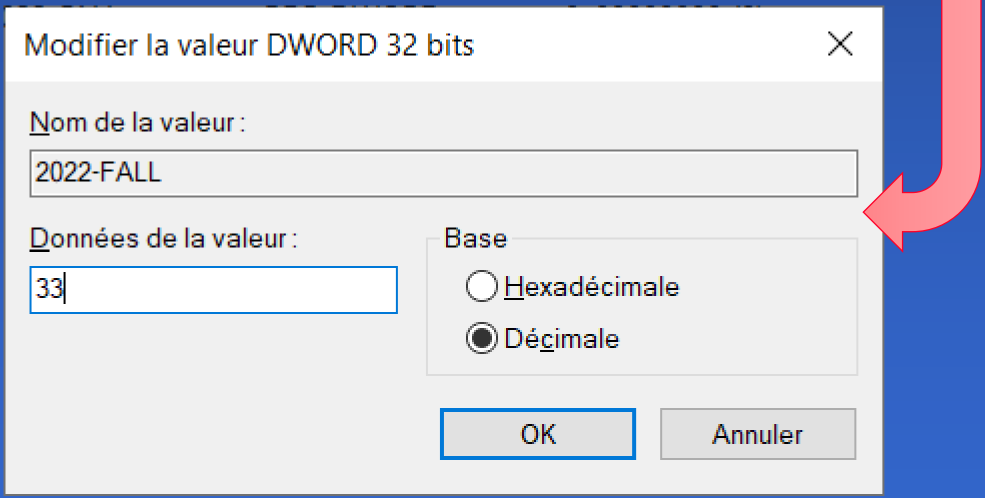
Ordinateur\HKEY_LOCAL_MACHINE\SOFTWARE\EPITA

Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)

Registry Values

- Value types:
  - String
  - Binary
  - Int32
  - Int64
  - String array
  - Resizable String





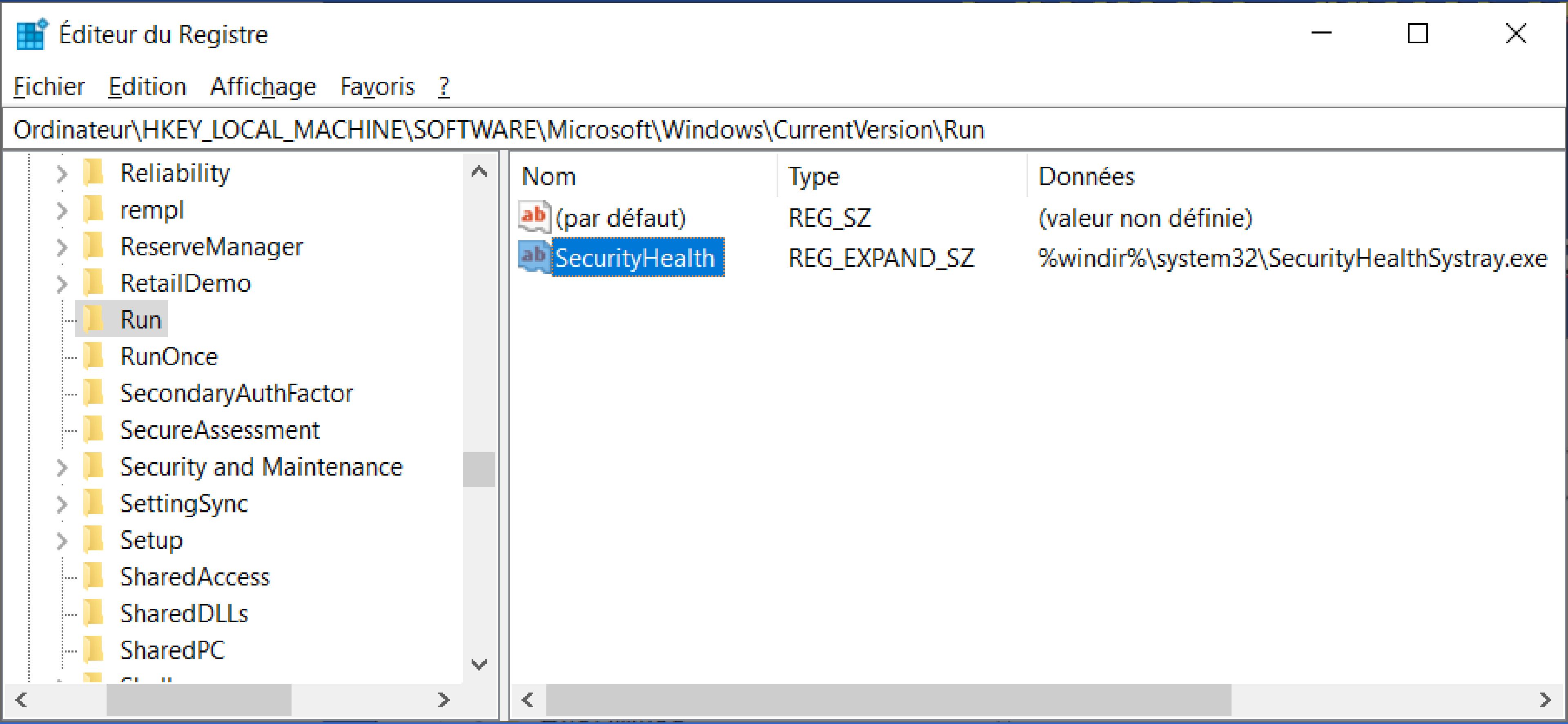
Nom de la valeur : 2022-FALL

Données de la valeur : 33

Base
○ Hexadécimale
● Décimale

Example : Startup Applications

- HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/Run
  - Seek for malware…



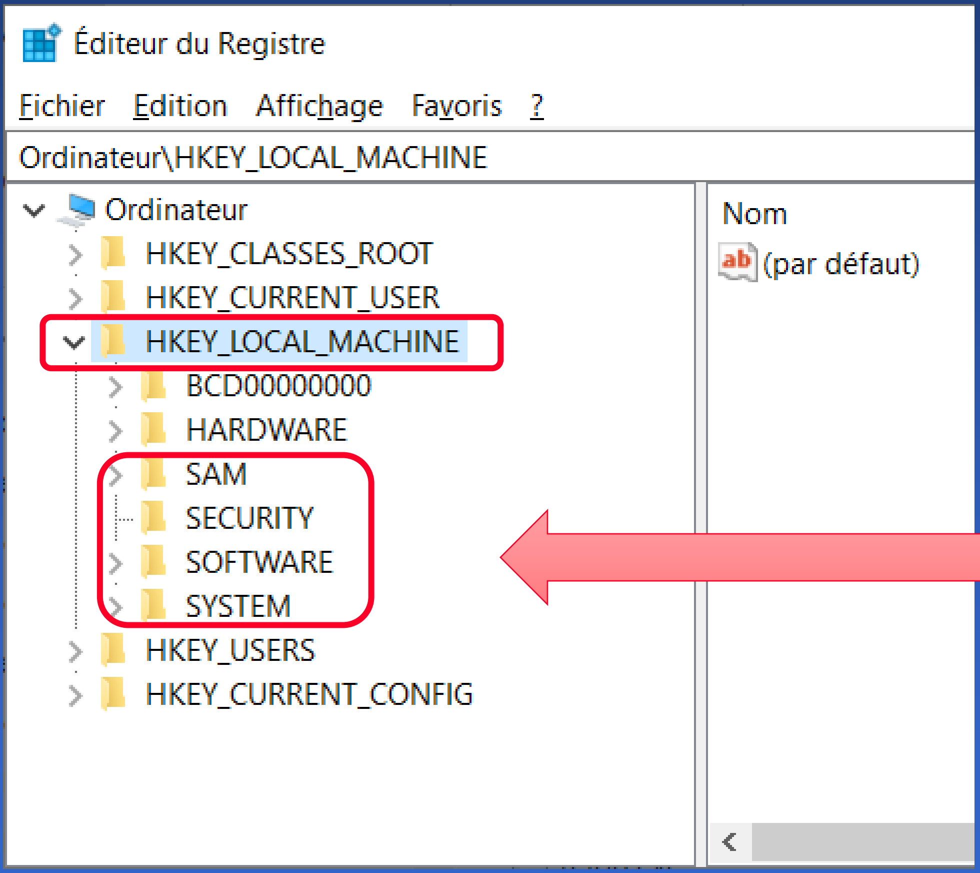
Ordinateur\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- Reliability
- rempl
- ReserveManager
- RetailDemo
- Run
- RunOnce
- SecondaryAuthFactor
- SecureAssessment
- Security and Maintenance
- SettingSync
- Setup
- SharedAccess
- SharedDLLs
- SharedPC

Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe

General sub-tree = HKLM

- ◆ The HKLM sub-tree → system hives

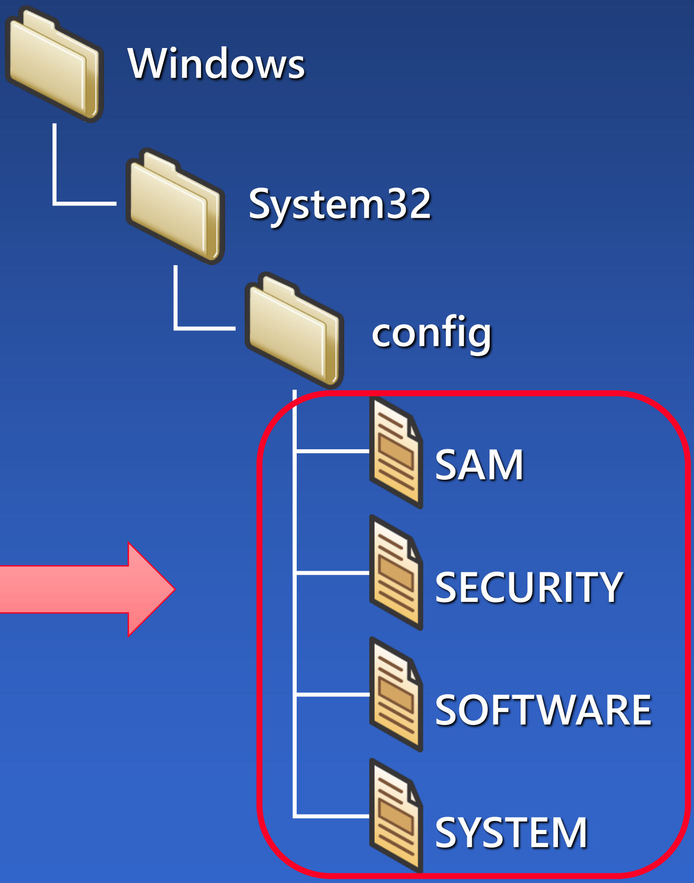


Éditeur du Registre

Ordinateur\HKEY_LOCAL_MACHINE

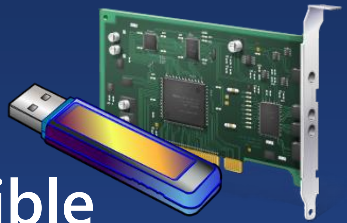
```
Ordinateur
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    BCD00000000
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
  HKEY_USERS
  HKEY_CURRENT_CONFIG
```

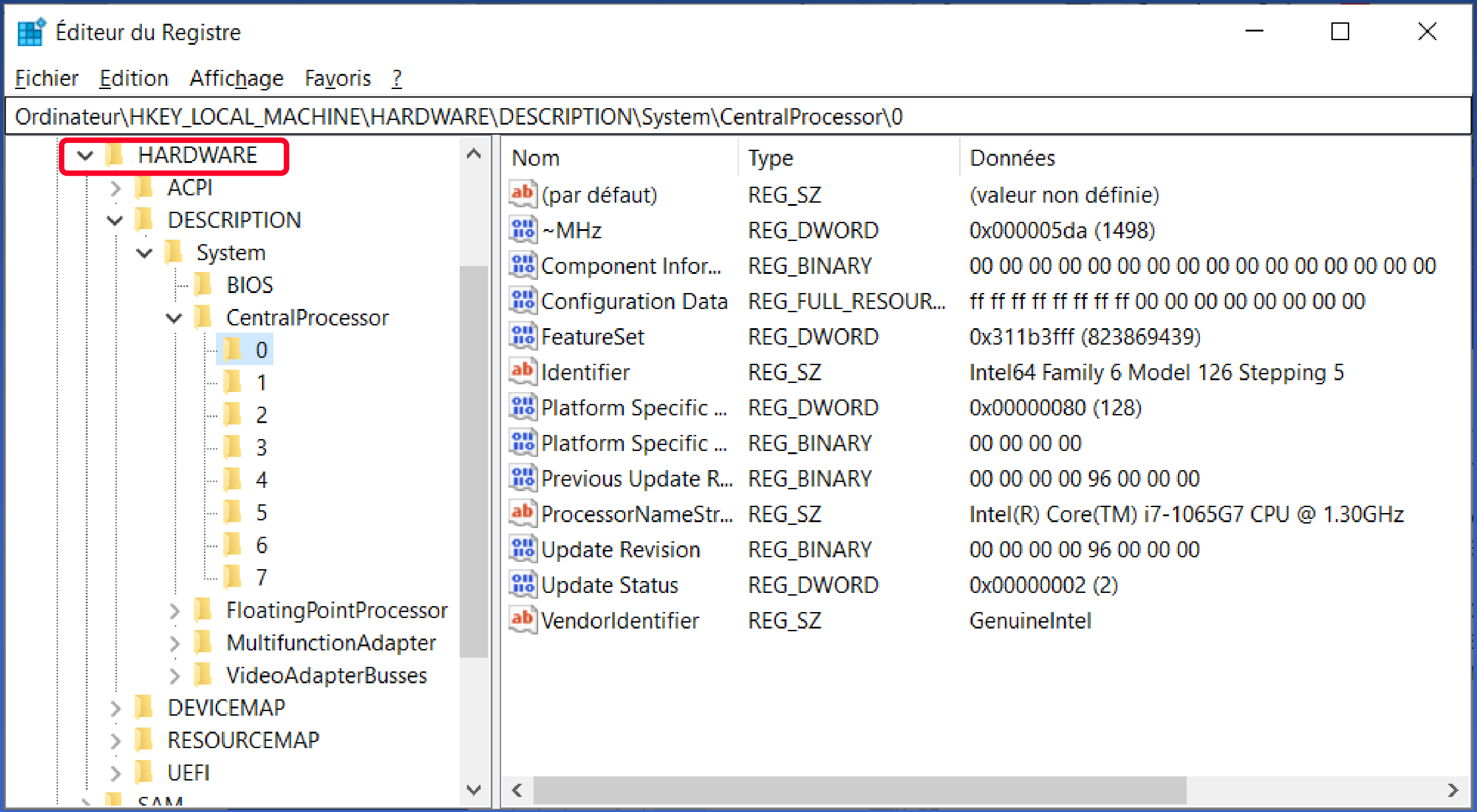
Nom
(par défaut)



HARDWARE sub-tree

- HARDWARE is re-built at each boot
  - PCI & USB bus are Plug & Play
  - Wrong hardware configuration is not possible





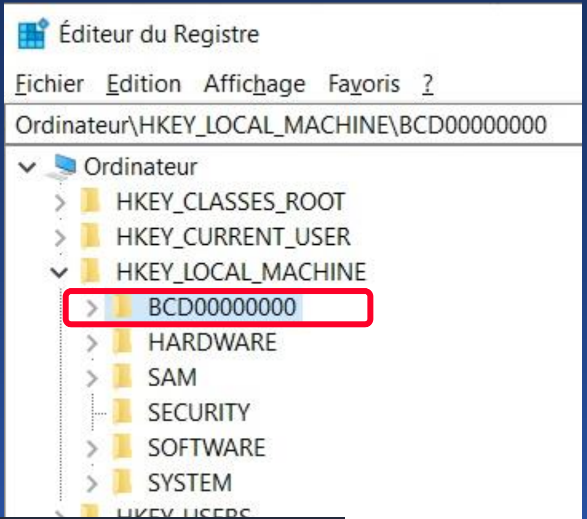
Ordinateur\HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0

- HARDWARE
  - ACPI
  - DESCRIPTION
    - System
      - BIOS
      - CentralProcessor
        - 0
        - 1
        - 2
        - 3
        - 4
        - 5
        - 6
        - 7
      - FloatingPointProcessor
      - MultifunctionAdapter
      - VideoAdapterBusses
  - DEVICEMAP
  - RESOURCEMAP
  - UEFI
- SAM

Nom	Type	Données
ab (par défaut)	REG_SZ	(valeur non définie)
~MHz	REG_DWORD	0x000005da (1498)
Component Infor...	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Configuration Data	REG_FULL_RESOUR...	ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00
FeatureSet	REG_DWORD	0x311b3fff (823869439)
ab Identifier	REG_SZ	Intel64 Family 6 Model 126 Stepping 5
Platform Specific ...	REG_DWORD	0x00000080 (128)
Platform Specific ...	REG_BINARY	00 00 00 00
Previous Update R...	REG_BINARY	00 00 00 00 96 00 00 00
ab ProcessorNameStr...	REG_SZ	Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz
Update Revision	REG_BINARY	00 00 00 00 96 00 00 00
Update Status	REG_DWORD	0x00000002 (2)
ab VendorIdentifier	REG_SZ	GenuineIntel

BCD sub-tree

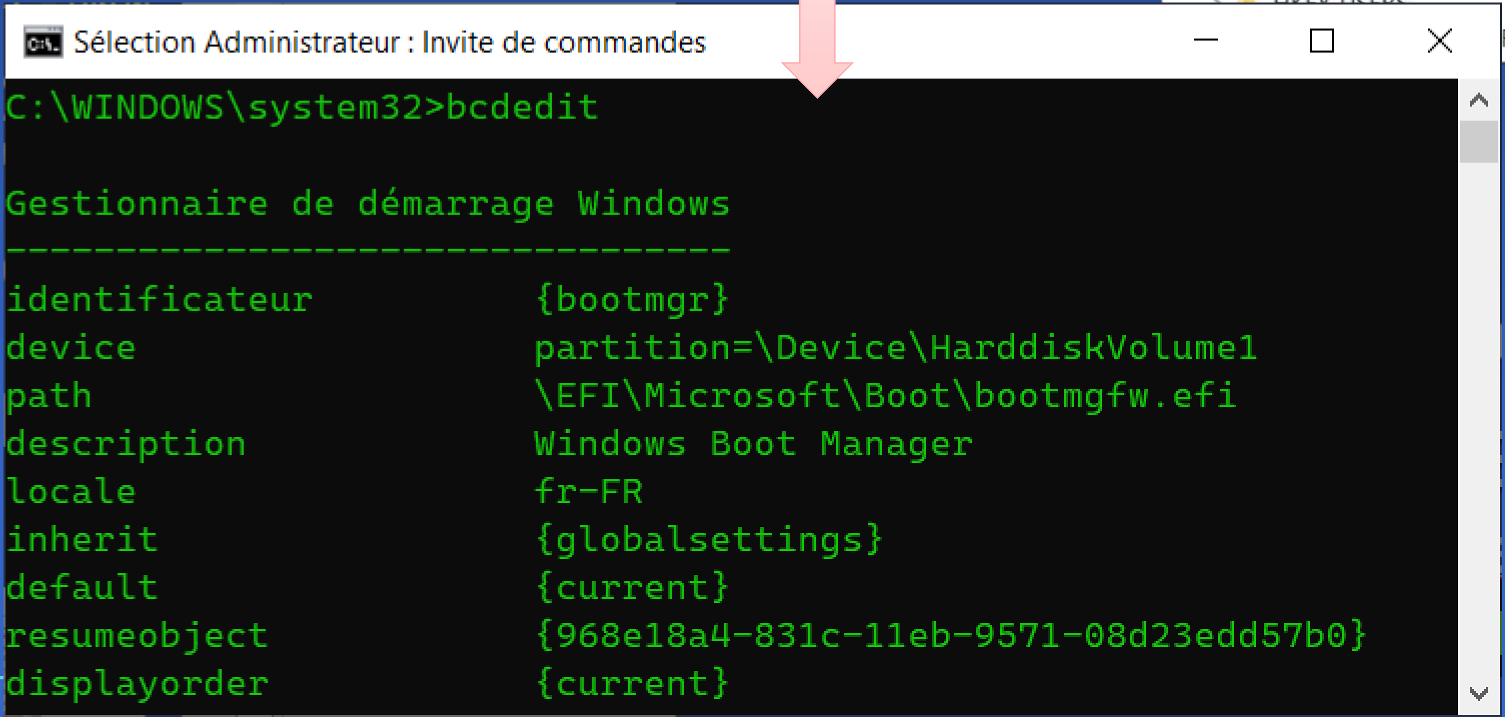
- ◆ Boot Configuration
  - Multi-boot
  - System restore
- ◆ A dedicated HIVE
  - Stored in a hidden partition
  - Modify with `bcdedit.exe`



Éditeur du Registre

Ordinateur\HKEY_LOCAL_MACHINE\BCD00000000

- Ordinateur
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
    - BCD00000000
    - HARDWARE
    - SAM
    - SECURITY
    - SOFTWARE
    - SYSTEM
  - HKEY_USERS
  - FIG



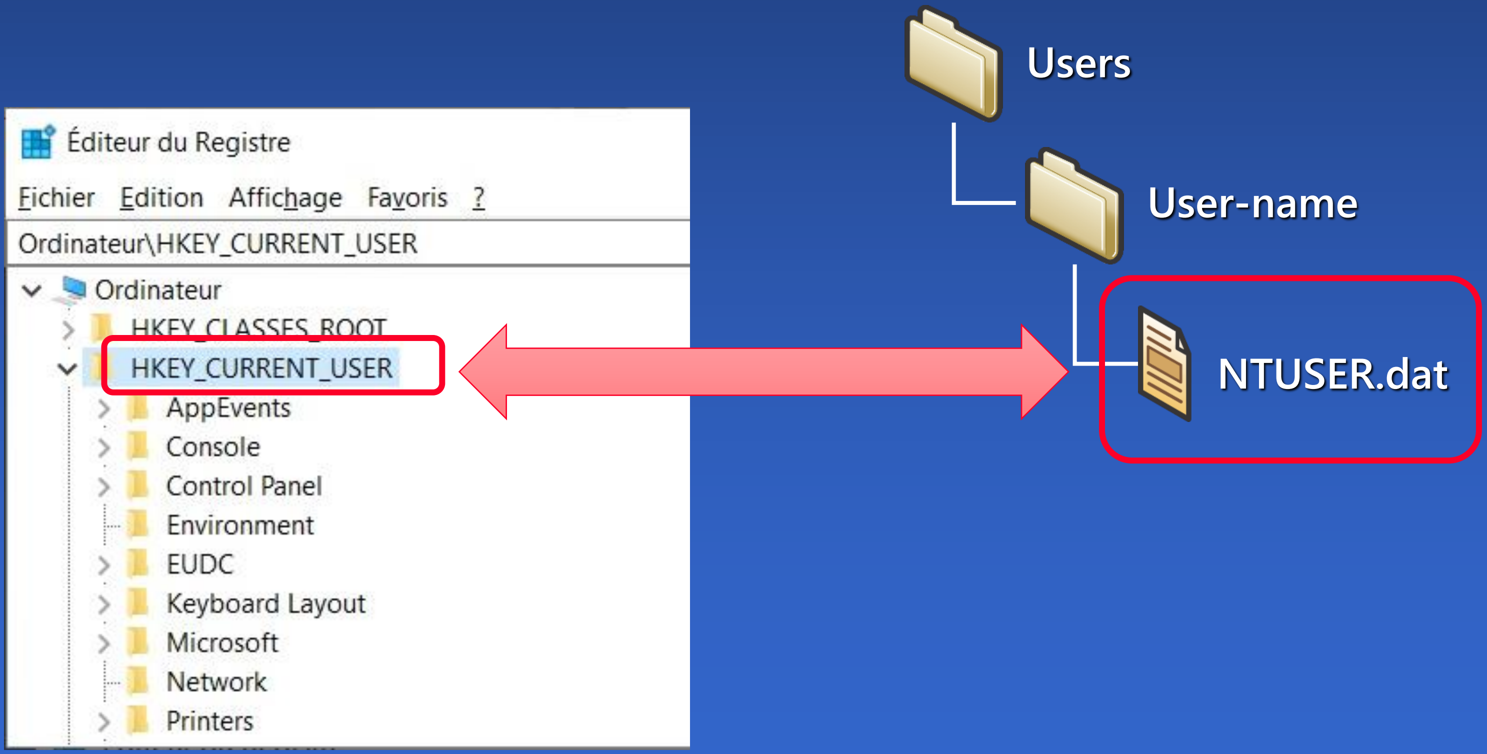
Sélection Administrateur : Invite de commandes

```
C:\WINDOWS\system32>bcdedit

Gestionnaire de démarrage Windows
---------------------------------
identificateur          {bootmgr}
device                  partition=\Device\HarddiskVolume1
path                    \EFI\Microsoft\Boot\bootmgfw.efi
description             Windows Boot Manager
locale                  fr-FR
inherit                 {globalsettings}
default                 {current}
resumeobject            {968e18a4-831c-11eb-9571-08d23edd57b0}
displayorder            {current}
```

USER sub-tree = HKCU

- The HKCU sub-tree → User hive
  - Dedicated user parameters



Éditeur du Registre

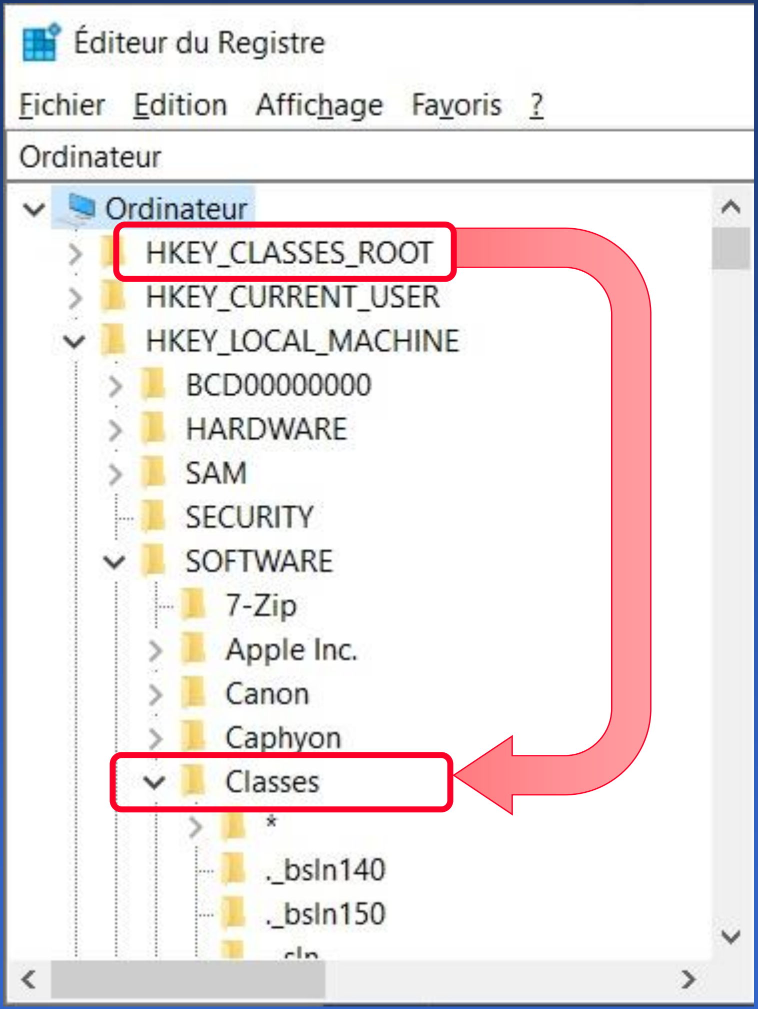
Fichier Edition Affichage Favoris ?

Ordinateur\HKEY_CURRENT_USER

- Ordinateur
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
    - AppEvents
    - Console
    - Control Panel
    - Environment
    - EUDC
    - Keyboard Layout
    - Microsoft
    - Network
    - Printers

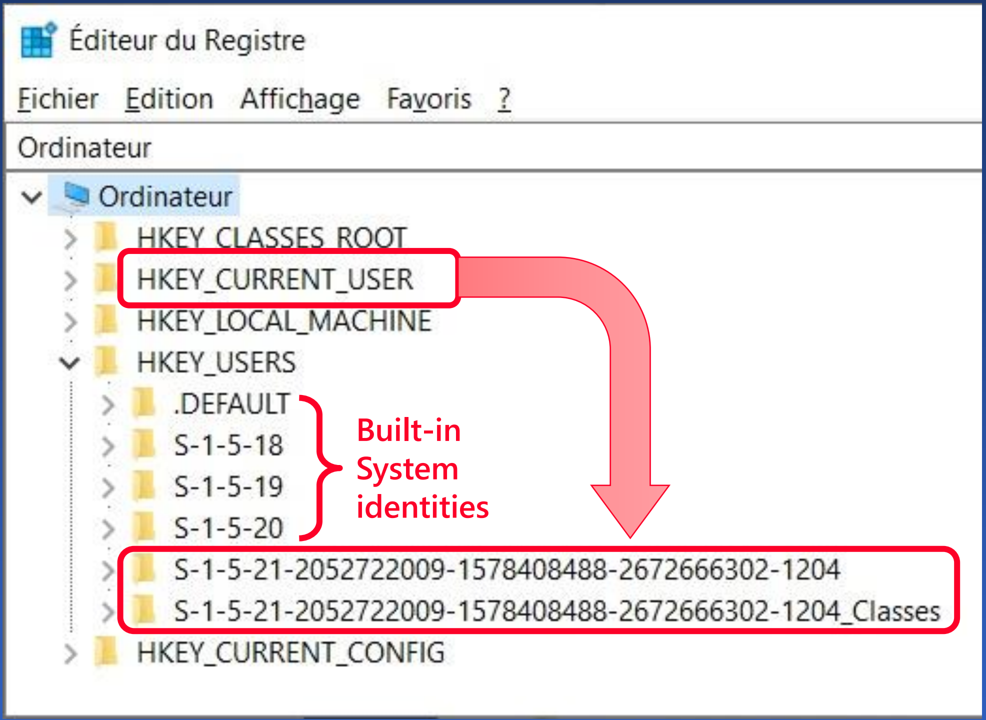
Registry aliases - 1

HKCR sub-tree



Ordinateur
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
  - BCD00000000
  - HARDWARE
  - SAM
  - SECURITY
  - SOFTWARE
    - 7-Zip
    - Apple Inc.
    - Canon
    - Caphyon
    - Classes
      - *
      - ._bsln140
      - ._bsln150
      - .cln

HKCU sub-tree

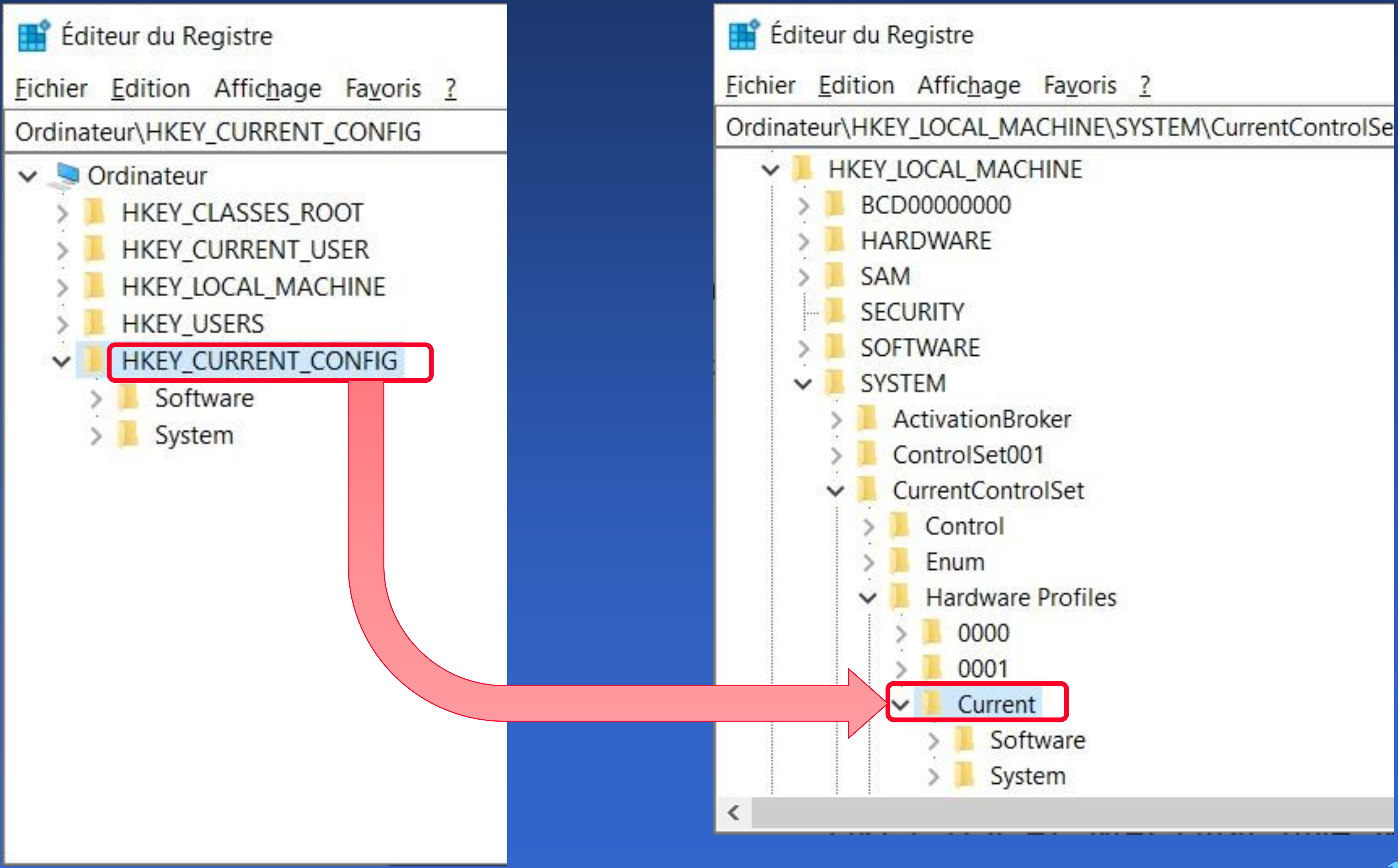


Ordinateur
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
  - .DEFAULT
  - S-1-5-18
  - S-1-5-19
  - S-1-5-20
  - S-1-5-21-2052722009-1578408488-2672666302-1204
  - S-1-5-21-2052722009-1578408488-2672666302-1204_Classes
- HKEY_CURRENT_CONFIG

Built-in System identities

Registry aliases - 2

HKCC sub-tree


Éditeur du Registre
Fichier Edition Affichage Favoris ?

Ordinateur\HKEY_CURRENT_CONFIG

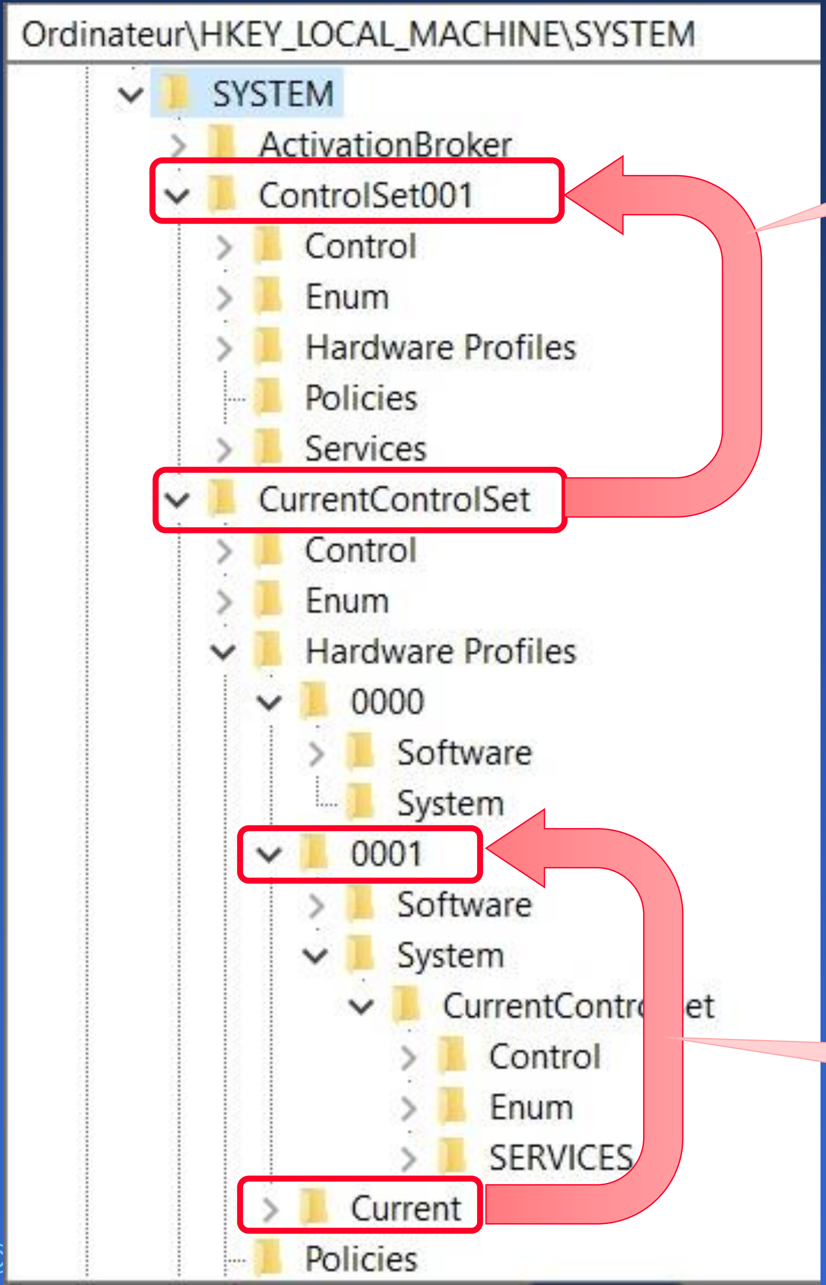
- Ordinateur
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
  - HKEY_USERS
  - HKEY_CURRENT_CONFIG
    - Software
    - System

Éditeur du Registre
Fichier Edition Affichage Favoris ?

Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSe

- HKEY_LOCAL_MACHINE
  - BCD00000000
  - HARDWARE
  - SAM
  - SECURITY
  - SOFTWARE
  - SYSTEM
    - ActivationBroker
    - ControlSet001
    - CurrentControlSet
      - Control
      - Enum
      - Hardware Profiles
        - 0000
        - 0001
        - Current
          - Software
          - System

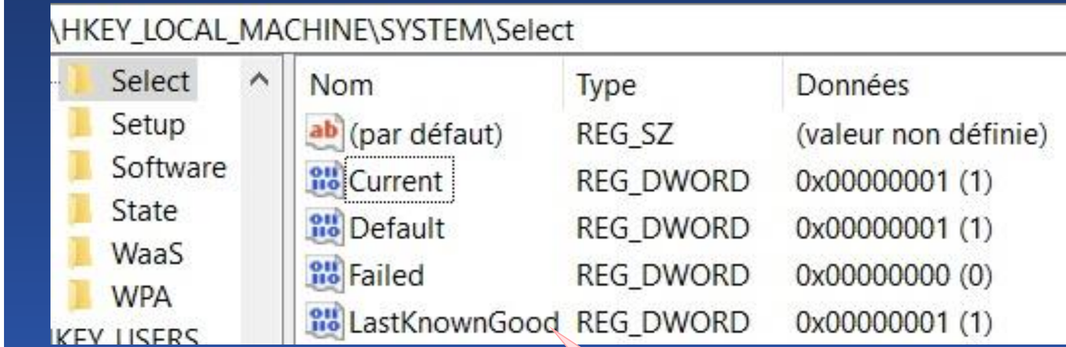
Registry aliases - 3



Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM

```
SYSTEM
    ActivationBroker
    ControlSet001
        Control
        Enum
        Hardware Profiles
        Policies
        Services
    CurrentControlSet
        Control
        Enum
        Hardware Profiles
            0000
                Software
                System
            0001
                Software
                System
                    CurrentContr    et
                        Control
                        Enum
                        SERVICES
            Current
        Policies
```

Current runtime status *(Default)*



\HKEY_LOCAL_MACHINE\SYSTEM\Select

```
Select
Setup
Software
State
WaaS
WPA
KEY_USERS
```

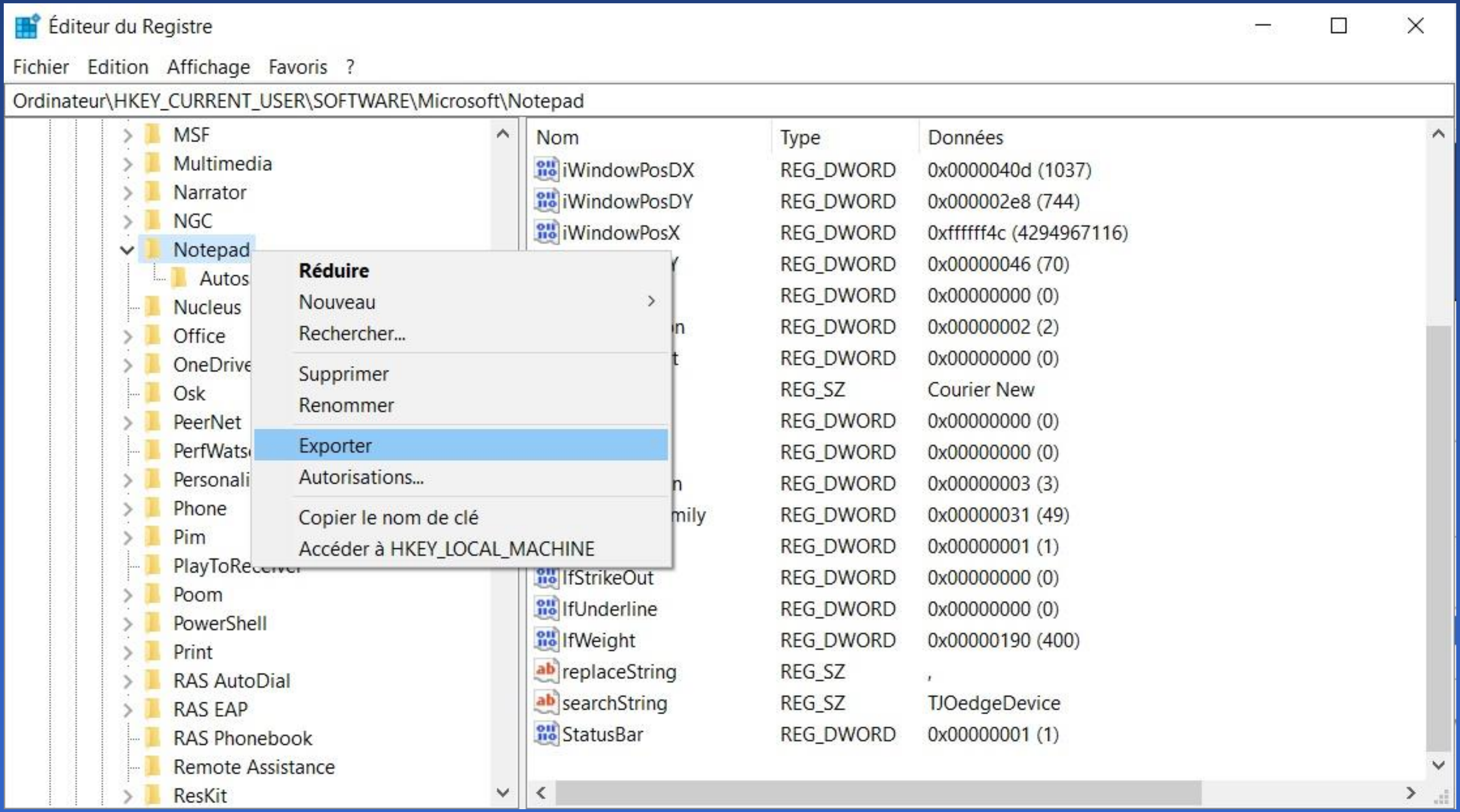
Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000001 (1)

Backup

Current hardware status

Registry Import / Export

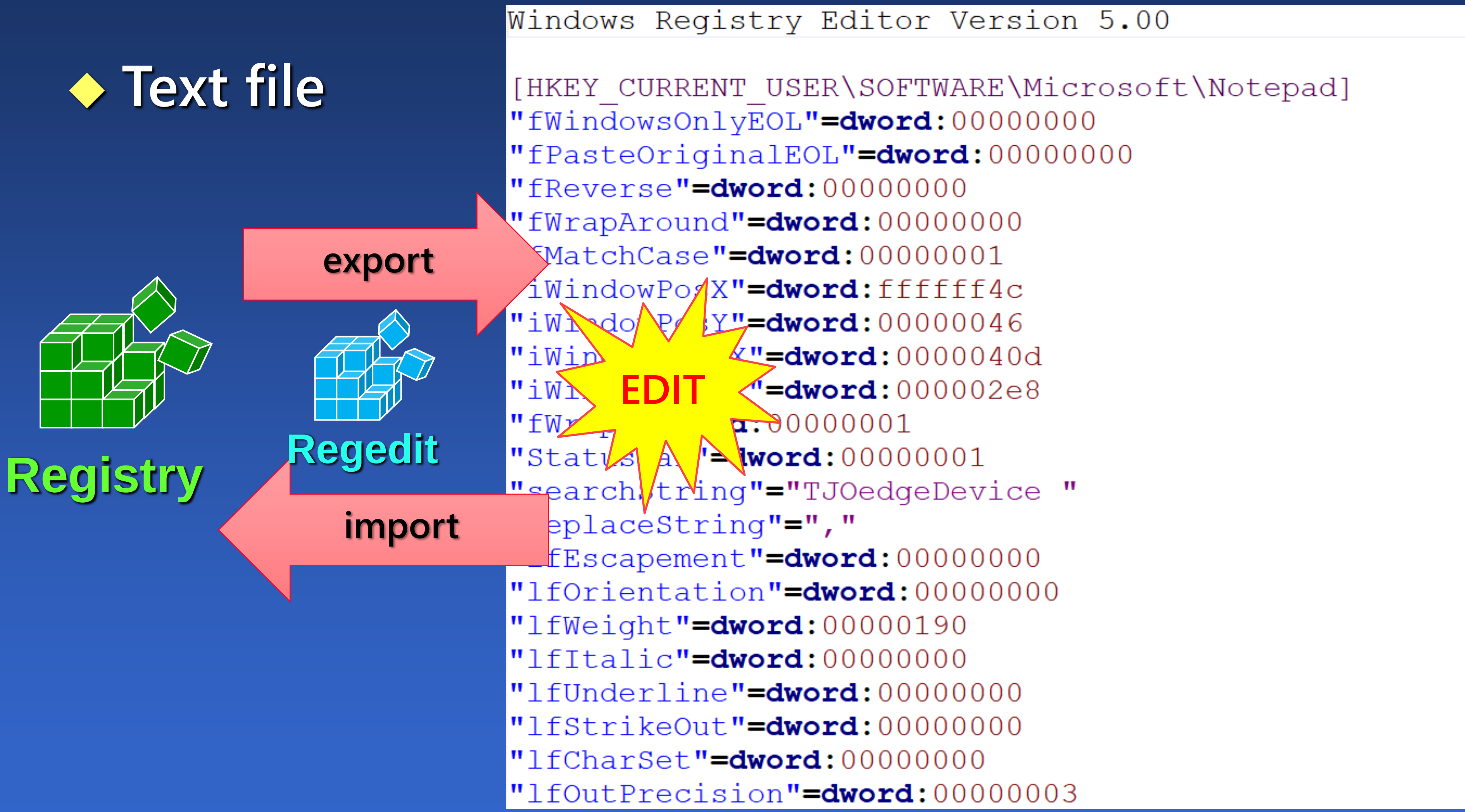
- .REG files
  - Exported by REGEDIT



Nom	Type	Données
iWindowPosDX	REG_DWORD	0x0000040d (1037)
iWindowPosDY	REG_DWORD	0x000002e8 (744)
iWindowPosX	REG_DWORD	0xffffff4c (4294967116)
Y	REG_DWORD	0x00000046 (70)
	REG_DWORD	0x00000000 (0)
n	REG_DWORD	0x00000002 (2)
t	REG_DWORD	0x00000000 (0)
	REG_SZ	Courier New
	REG_DWORD	0x00000000 (0)
	REG_DWORD	0x00000000 (0)
n	REG_DWORD	0x00000003 (3)
mily	REG_DWORD	0x00000031 (49)
	REG_DWORD	0x00000001 (1)
lfStrikeOut	REG_DWORD	0x00000000 (0)
lfUnderline	REG_DWORD	0x00000000 (0)
lfWeight	REG_DWORD	0x00000190 (400)
replaceString	REG_SZ	,
searchString	REG_SZ	TJOedgeDevice
StatusBar	REG_DWORD	0x00000001 (1)

.REG files

- Text file

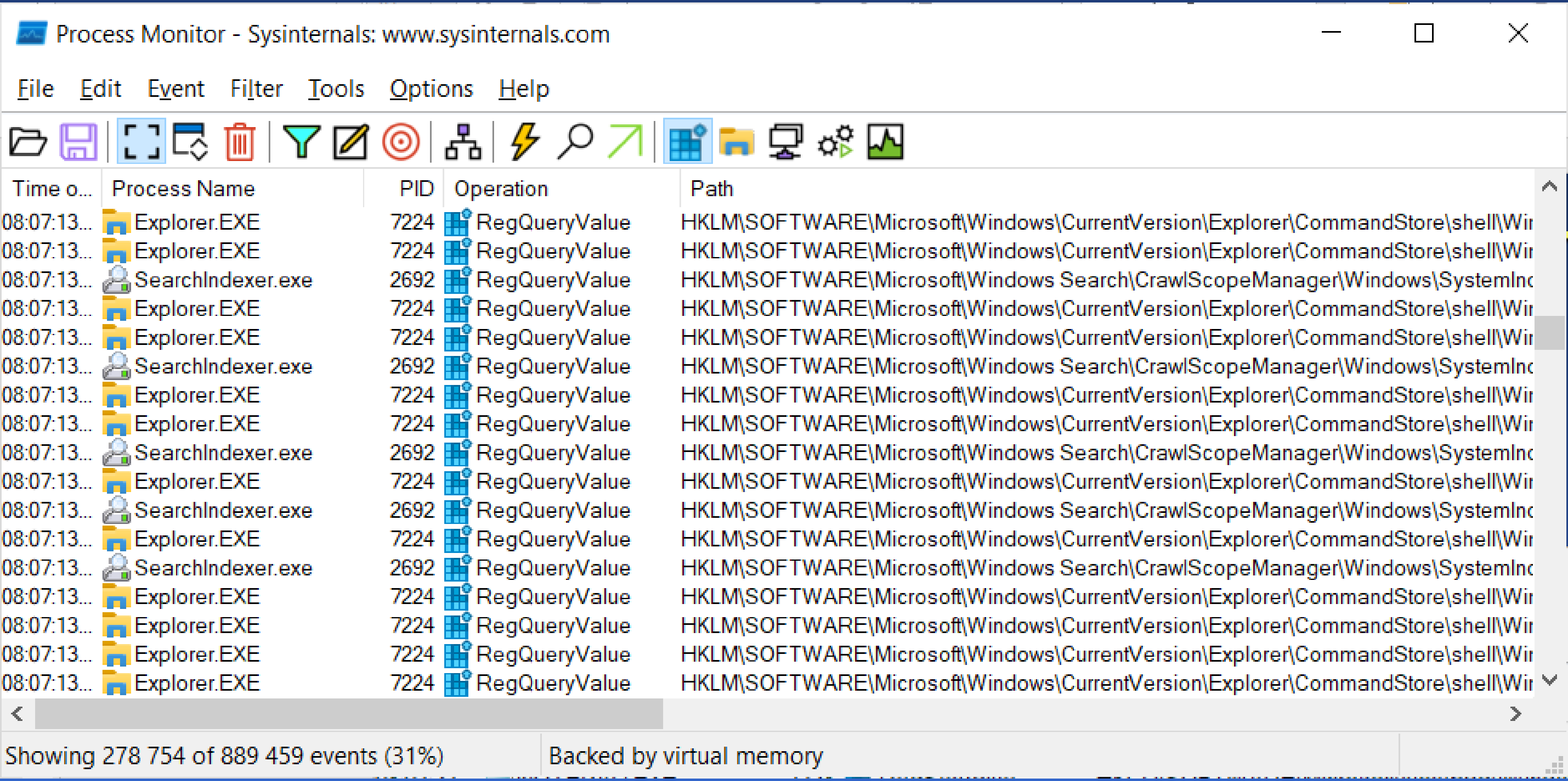


```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Notepad]
"fWindowsOnlyEOL"=dword:00000000
"fPasteOriginalEOL"=dword:00000000
"fReverse"=dword:00000000
"fWrapAround"=dword:00000000
"fMatchCase"=dword:00000001
"iWindowPosX"=dword:ffffff4c
"iWindowPosY"=dword:00000046
"iWindowPosDX"=dword:0000040d
"iWindowPosDY"=dword:000002e8
"fWrap"=dword:00000001
"StatusBar"=dword:00000001
"searchString"="TJOedgeDevice "
"replaceString"=","
"lfEscapement"=dword:00000000
"lfOrientation"=dword:00000000
"lfWeight"=dword:00000190
"lfItalic"=dword:00000000
"lfUnderline"=dword:00000000
"lfStrikeOut"=dword:00000000
"lfCharSet"=dword:00000000
"lfOutPrecision"=dword:00000003
```

Procmon - Registry

- Tracks Registry activity



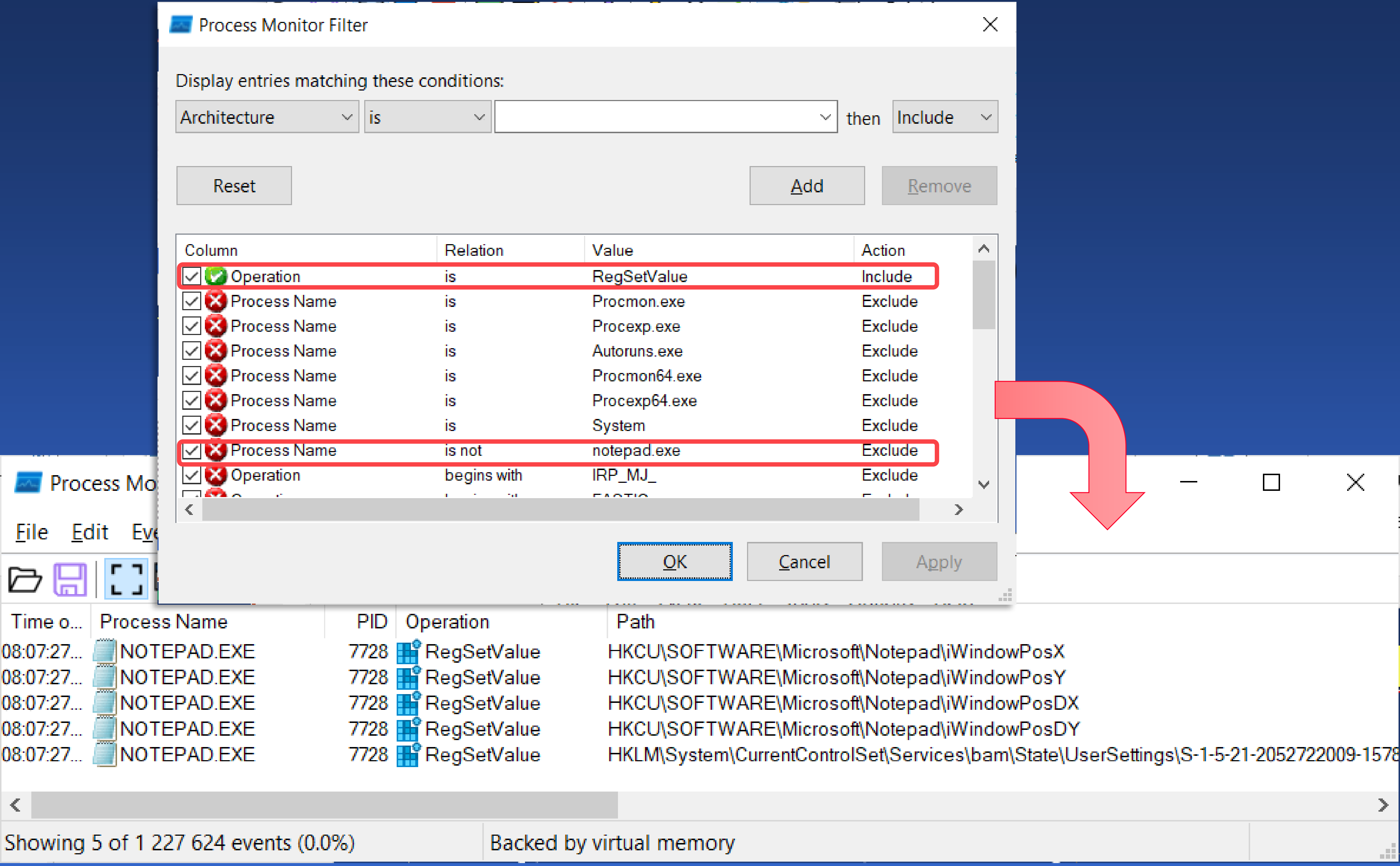
Process Monitor - Sysinternals: www.sysinternals.com

Time o...	Process Name	PID	Operation	Path
08:07:13...	Explorer.EXE	7224	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CommandStore\shell\Wi
08:07:13...	Explorer.EXE	7224	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CommandStore\shell\Wi
08:07:13...	SearchIndexer.exe	2692	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows Search\CrawlScopeManager\Windows\SystemInd
08:07:13...	Explorer.EXE	7224	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CommandStore\shell\Wi
08:07:13...	Explorer.EXE	7224	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CommandStore\shell\Wi
08:07:13...	SearchIndexer.exe	2692	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows Search\CrawlScopeManager\Windows\SystemInd
08:07:13...	Explorer.EXE	7224	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CommandStore\shell\Wi
08:07:13...	Explorer.EXE	7224	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CommandStore\shell\Wi
08:07:13...	SearchIndexer.exe	2692	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows Search\CrawlScopeManager\Windows\SystemInd
08:07:13...	Explorer.EXE	7224	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CommandStore\shell\Wi
08:07:13...	SearchIndexer.exe	2692	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows Search\CrawlScopeManager\Windows\SystemInd
08:07:13...	Explorer.EXE	7224	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CommandStore\shell\Wi
08:07:13...	SearchIndexer.exe	2692	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows Search\CrawlScopeManager\Windows\SystemInd
08:07:13...	Explorer.EXE	7224	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CommandStore\shell\Wi
08:07:13...	Explorer.EXE	7224	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CommandStore\shell\Wi
08:07:13...	Explorer.EXE	7224	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CommandStore\shell\Wi
08:07:13...	Explorer.EXE	7224	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CommandStore\shell\Wi

Showing 278 754 of 889 459 events (31%)   Backed by virtual memory

Windows Sysinternals

Procmon registry filters



Process Monitor Filter

Display entries matching these conditions:

Architecture | is | | then Include

	Column	Relation	Value	Action
☑ ✓	Operation	is	RegSetValue	Include
☑ ☒	Process Name	is	Procmon.exe	Exclude
☑ ☒	Process Name	is	Procexp.exe	Exclude
☑ ☒	Process Name	is	Autoruns.exe	Exclude
☑ ☒	Process Name	is	Procmon64.exe	Exclude
☑ ☒	Process Name	is	Procexp64.exe	Exclude
☑ ☒	Process Name	is	System	Exclude
☑ ☒	Process Name	is not	notepad.exe	Exclude
☑ ☒	Operation	begins with	IRP_MJ_	Exclude

Time o...	Process Name	PID	Operation	Path
08:07:27...	NOTEPAD.EXE	7728	RegSetValue	HKCU\SOFTWARE\Microsoft\Notepad\iWindowPosX
08:07:27...	NOTEPAD.EXE	7728	RegSetValue	HKCU\SOFTWARE\Microsoft\Notepad\iWindowPosY
08:07:27...	NOTEPAD.EXE	7728	RegSetValue	HKCU\SOFTWARE\Microsoft\Notepad\iWindowPosDX
08:07:27...	NOTEPAD.EXE	7728	RegSetValue	HKCU\SOFTWARE\Microsoft\Notepad\iWindowPosDY
08:07:27...	NOTEPAD.EXE	7728	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2052722009-1578

Showing 5 of 1 227 624 events (0.0%) | Backed by virtual memory