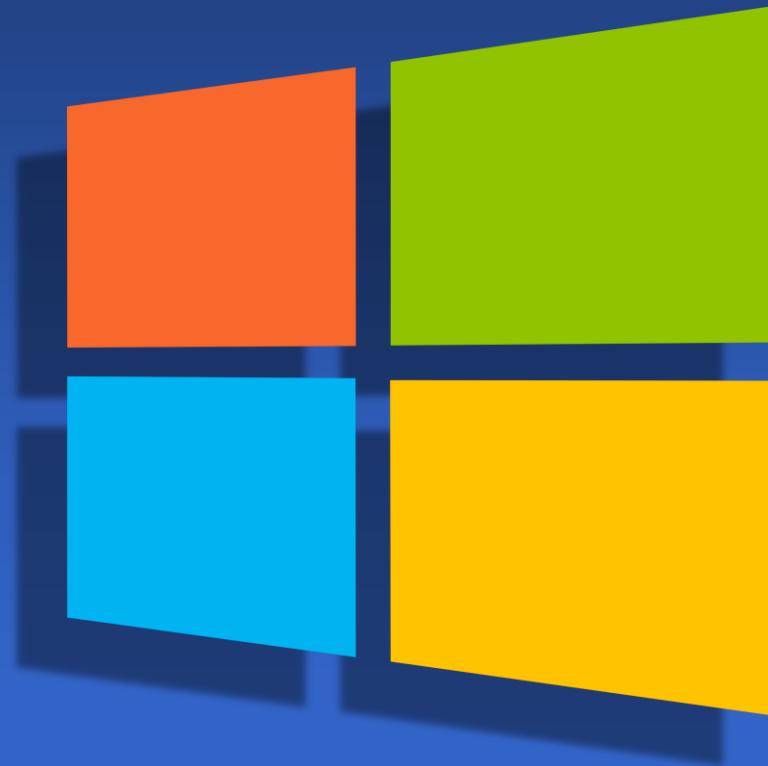


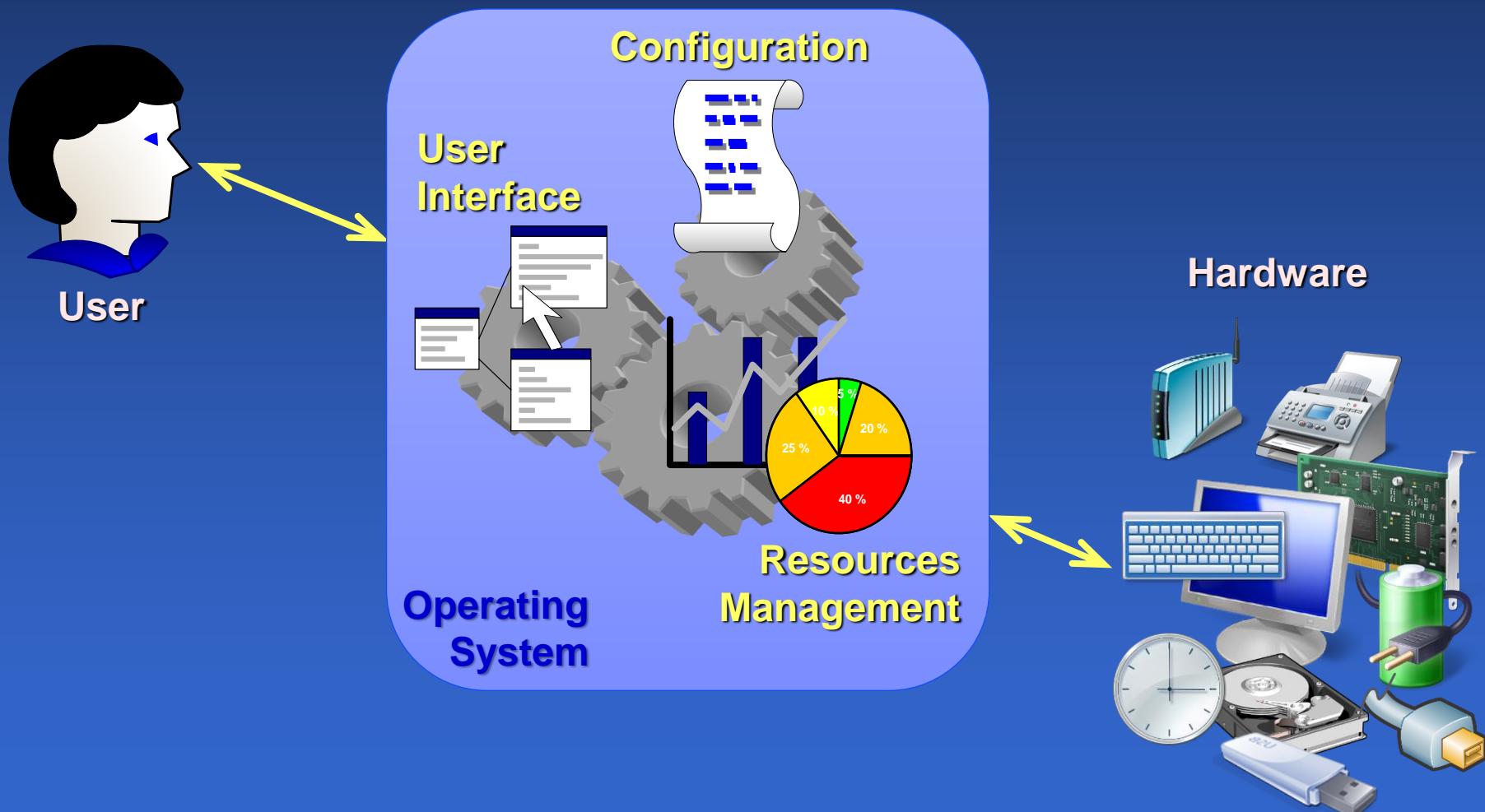
# Use & Admin Windows

## Survival Kit – 1 WINDOWS ??



# Introduction

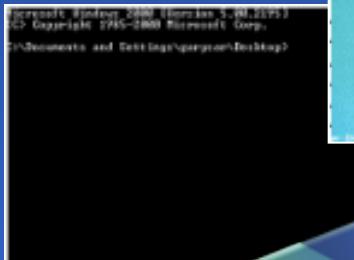
# OS ?



# 40 years of Personnal Computing



1981  
*CLI*



DOS  
UNIX

1990  
*GUI*



X-11  
Windows  
Macintosh

1995  
*Web*



Netscape  
IIS – IE  
javascript

2000  
*Mobility*



Google  
Android  
.net, js



2010  
*Cloud*



AWS  
Azure  
iOS

# Hardware changes



1981

- Keyboard
- RAM 64 Kb
- Screen (25x80 char)
- Floppy 180 Kb
- Serial 9 600 bps

x(1)  
x(250 000)  
x(3 000)  
x(5 600 000)  
x(520 000)



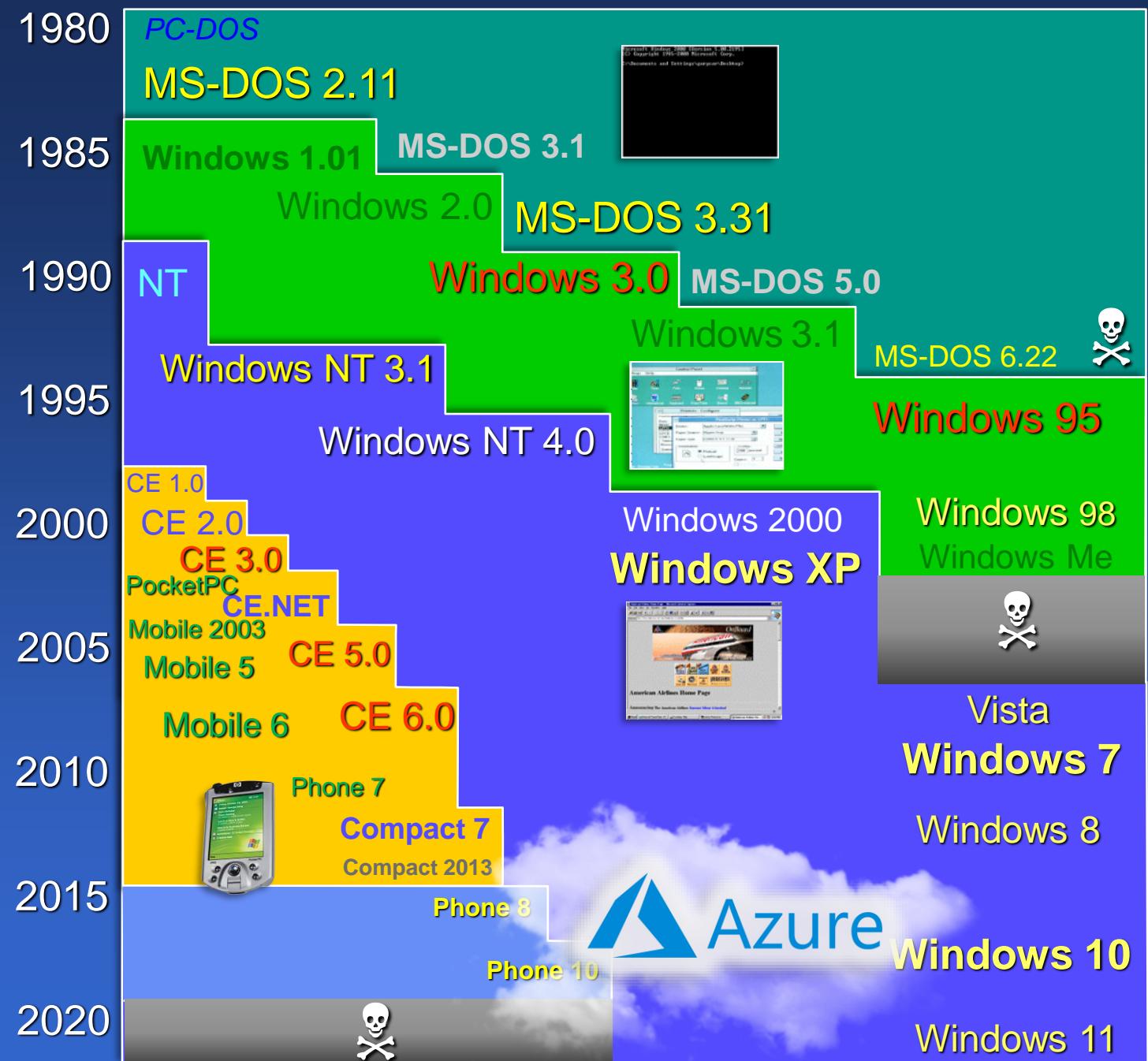
2023

- Keyboard + Mouse
- RAM 16 000 000 Kb
- Screen (1920x1080 pixels)
- SSD 1 000 000 000 Kb
- USB-3.0 5 000 000 000 bps
- Network (PAN/LAN/WAN)
- Camera/Sound
- Battery (ACPI)

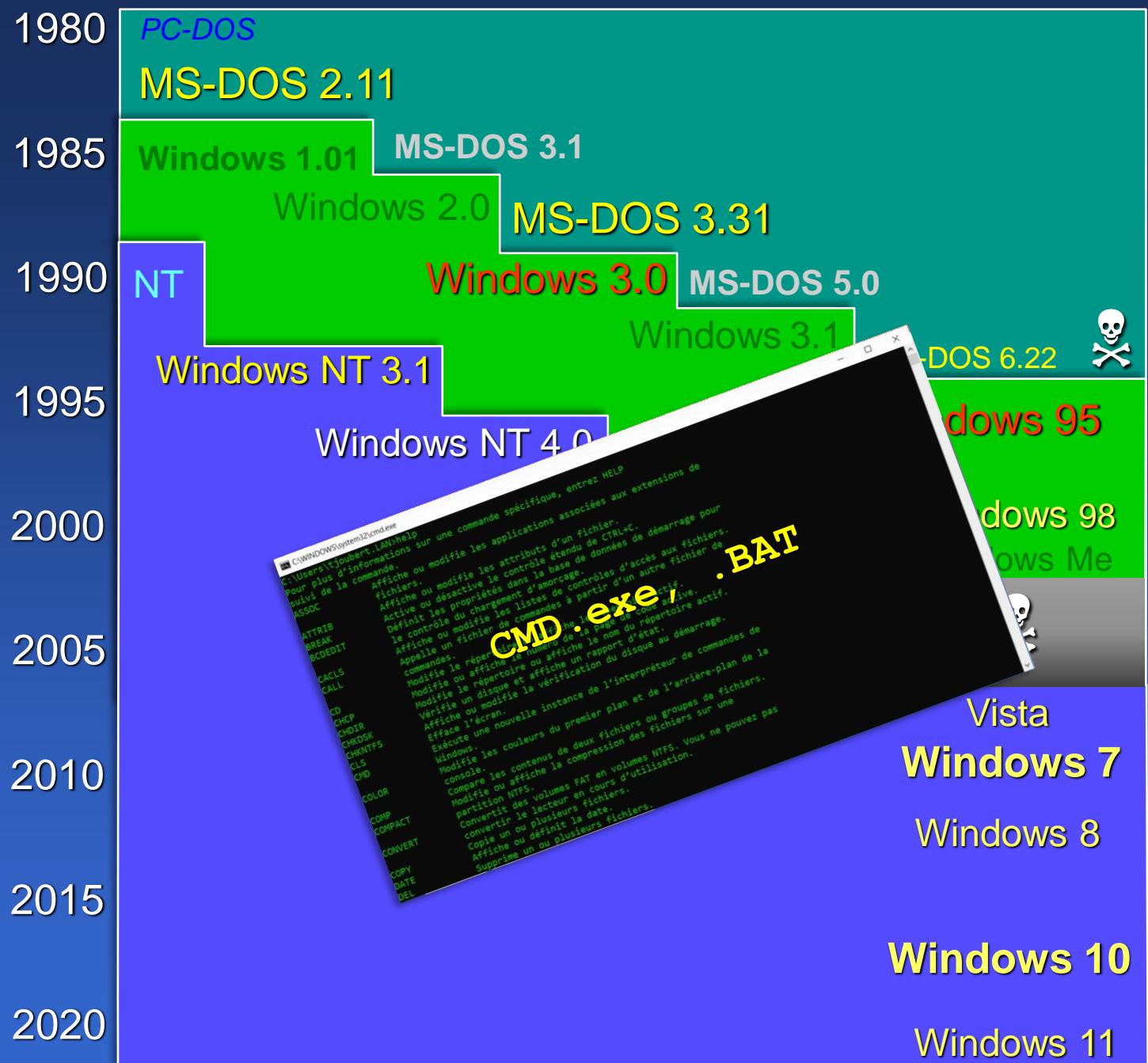
*Desktop Productivity*

*+ Mobile Connected Experience*

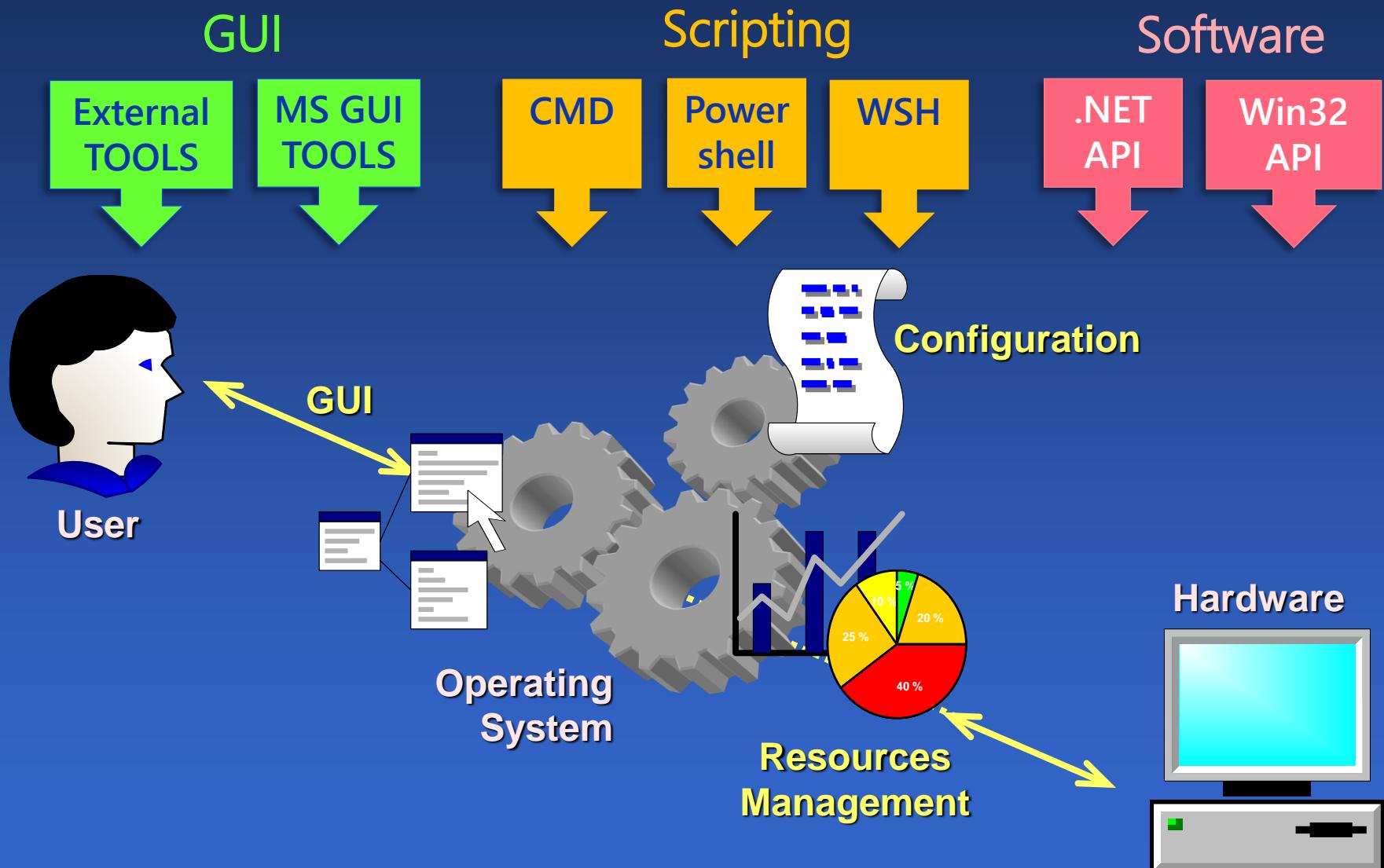
# MS OS



# One Survivor



# OS control levels



# Useful shortcuts

- ◆  + R → run
- ◆  + E → explorer
- ◆  + P → display
- ◆  + L → lock session
- ◆  + U → utilities
- ◆  + D → desktop
- ◆ Alt + PrntScr → captures current windows
- ◆ Alt + Tab → switch applications
- ◆ Ctrl+Alt+Del → Supervisor screen >*TaskMgr.exe*

# CLI – check MS license

◆  + R → CMD

◆ CD \Windows\System32

◆ cscript slmgr.vbs /dlv

Version du service de licences logicielles : 10.0.22621.1105

Nom : Windows(R), Professional edition

Description : Windows(R) Operating System, OEM\_DM channel

ID d'activation :

ID d'application

PID étendu :

Canal de la clé de produit (Product Key) : OEM:DM

Identificateur d'installation :

URL de licence d'utilisation : <https://activation-v2.sls.microsoft.com/S>

URL de validation : <https://validation-v2.sls.microsoft.com/SLWGA/slwg>

Clé de produit partielle :

État de la licence : avec licence

Nombre de réinitialisations de Windows restant : 1001

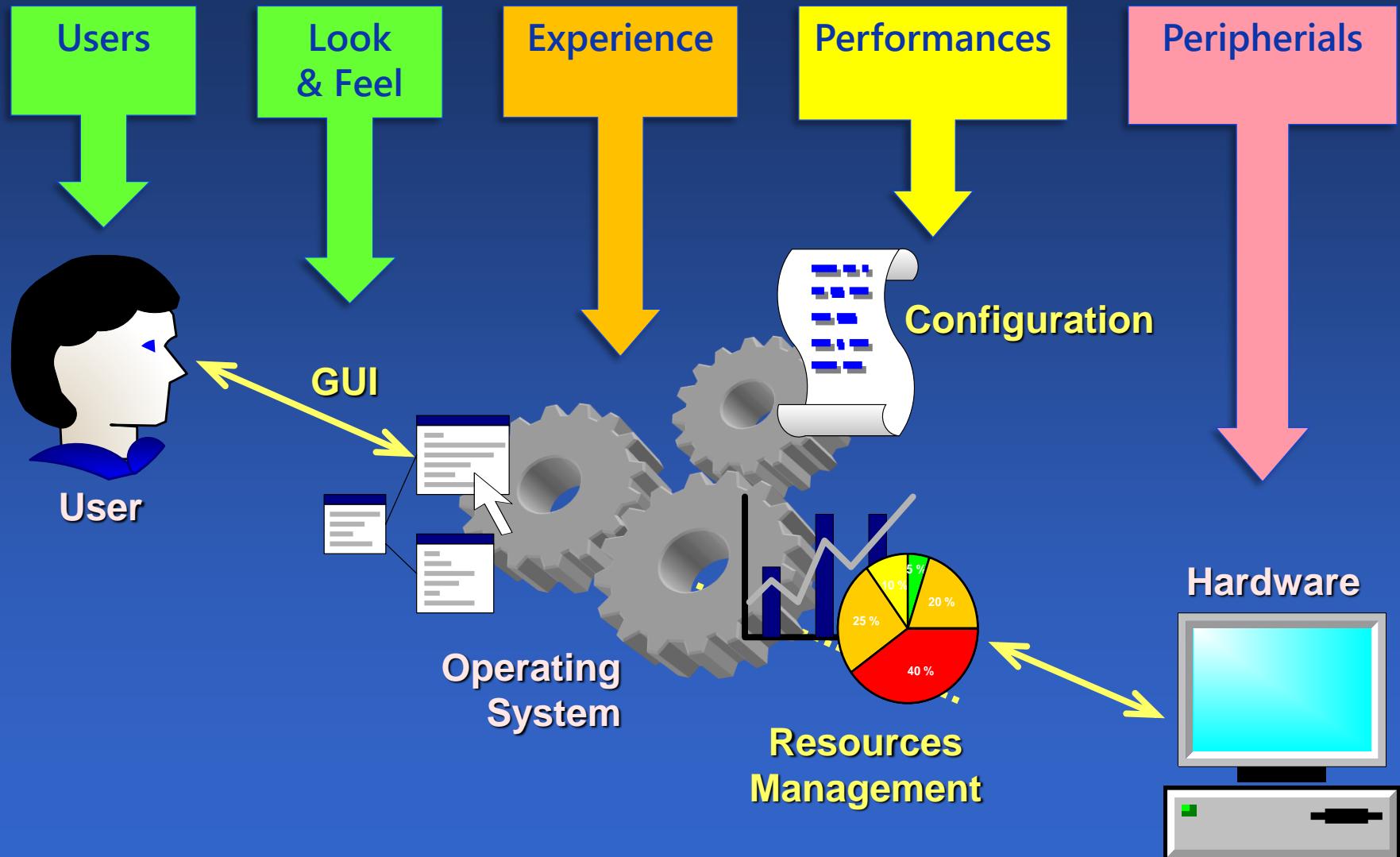
Nombre de réinitialisations de la référence (SKU) restant : 1001

Heure approuvée : 11/02/2023 07:58:27

## MS GUI tools

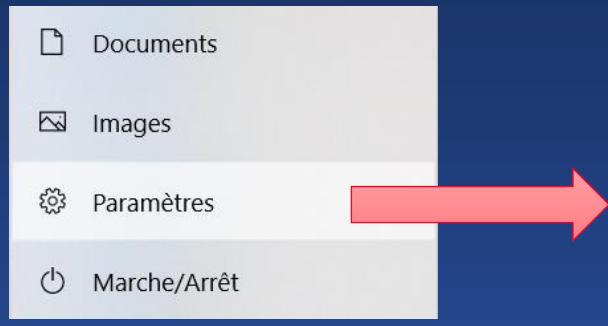
# OS control

# OS control targets



# Windows Parameters

## Start Menu



### Paramètres Windows

Rechercher un paramètre

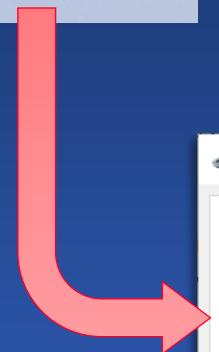
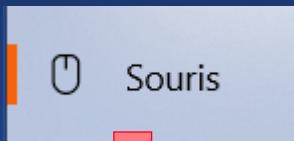
Système Affichage, son, notifications, alimentation	Pérophériques Bluetooth, imprimantes, souris	Téléphone Associer votre téléphone Android ou votre iPhone
Réseau et Internet Wi-Fi, mode Avion, VPN	Personnalisation Arrière-plan, écran de verrouillage, couleurs	Applications Désinstaller, valeurs par défaut, fonctionnalités facultatives
Comptes Comptes, e-mail, synchronisation, travail, autres utilisateurs	Heure et langue Voix, région, date	Jeux Xbox Game Bar, captures, Mode Jeu
Options d'ergonomie Narrateur, loupe, contraste élevé	Rechercher Rechercher mes fichiers, autorisations	Confidentialité Emplacement, caméra, microphone
Mise à jour et sécurité Windows Update, récupération, sauvegarde		

Win + U

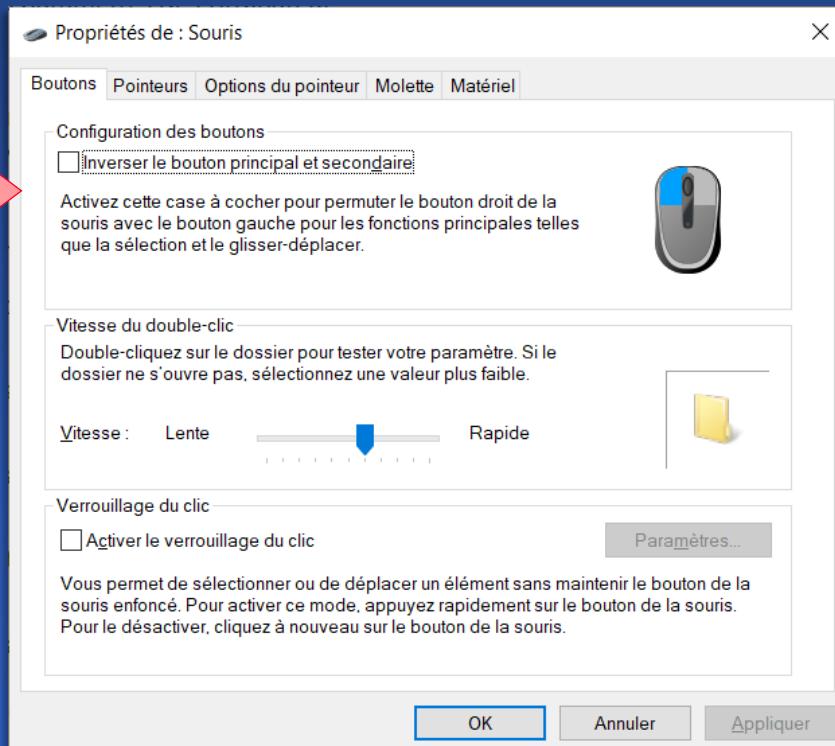
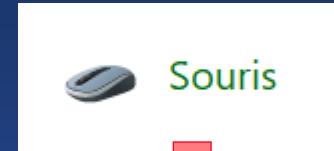


# Parameters vs Control

## Parameters

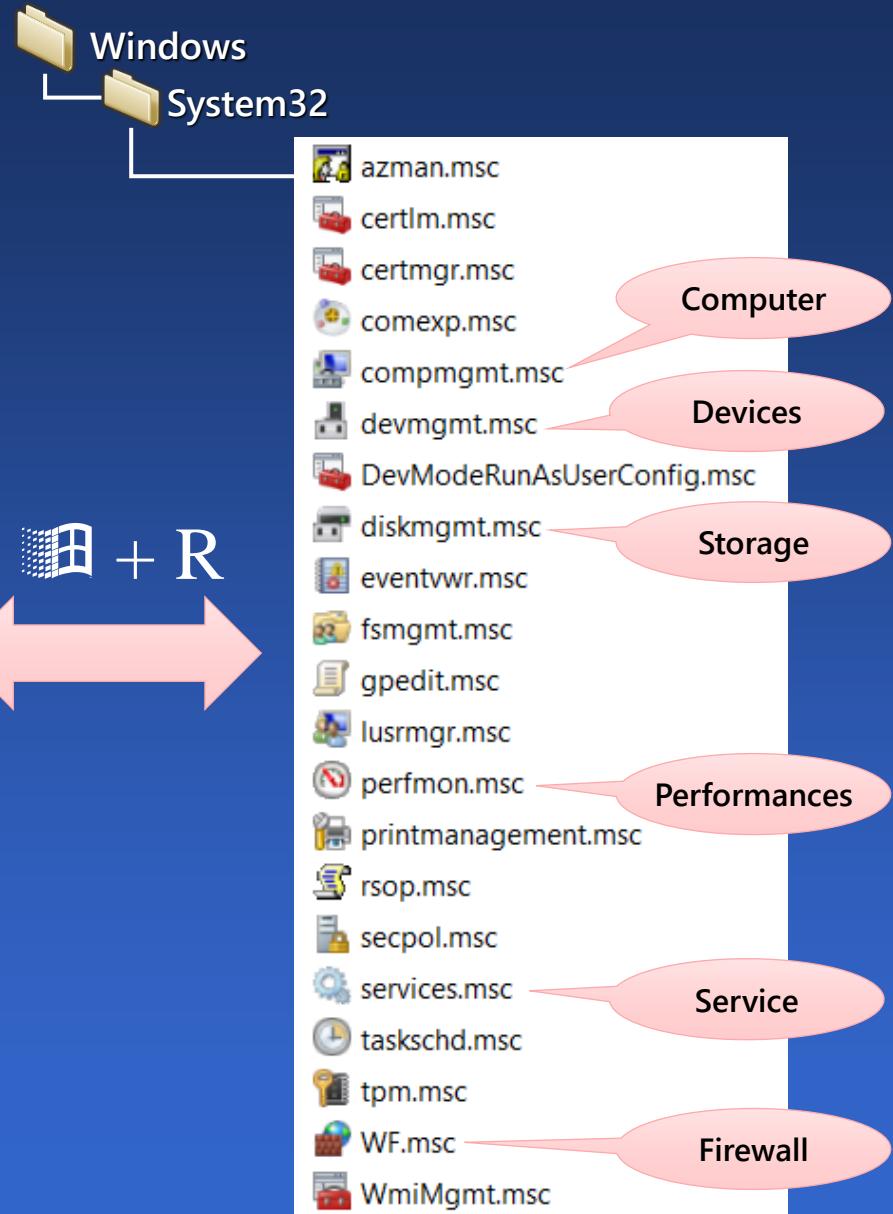
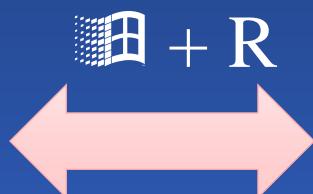


## Control Panel



# Computer Management

## ◆ From Explorer menu



## ◆ Management console

- **MMC .EXE**

# Control panel

Windows + R control

The screenshot shows the Windows Control Panel interface. At the top, there's a navigation bar with back, forward, search, and refresh buttons. Below it, a title bar says "Tous les Panneaux de configuration". The main area is titled "Ajuster les paramètres de l'ordinateur" and has a "Afficher par : Grandes icônes" dropdown. The control panel is organized into four columns of icons:

Icon	Label	Icon	Label	Icon	Label	Icon	Label
	Barre des tâches et navigation		Centre de mobilité Windows		Centre de synchronisation		Centre Réseau et partage
	Chiffrement de lecteur BitLocker		Clavier		Comptes d'utilisateurs		Connexions RemoteApp et Bureau à dist...
	Date et heure		Dossiers de travail		Espaces de stockage		Exécution automatique
	Gestion des couleurs		Gestionnaire de périphériques		Gestionnaire d'identification		Historique des fichiers
	Java		Mail (Microsoft Outlook) (32 bits)		Options d'alimentation		Options d'ergonomie
	Options d'indexation		Options de l'Explorateur de fichiers		Options Internet		Outils d'administration
	Paramètres du Tablet PC		Pare-feu Windows Defender		Périphériques et imprimantes		Polices
	Programmes et fonctionnalités		Programmes par défaut		Reconnaissance vocale		Récupération
	Région		Résolution des problèmes		Sauvegarder et restaurer (Windows 7)		Sécurité et maintenance
	Son		Souris		Stylet et fonction tactile		Système
	Téléphone et modem						

# Behind the control panel



appwiz.cpl
bthprops.cpl
desk.cpl
Firewall.cpl
hdwwiz.cpl
inetcpl.cpl
intl.cpl
irprops.cpl
joy.cpl
main.cpl
mmsys.cpl
ncpa.cpl
powercfg.cpl
sysdm.cpl
TabletPC.cpl
telephon.cpl
timedate.cpl
wscui.cpl

Extensible

# System tools

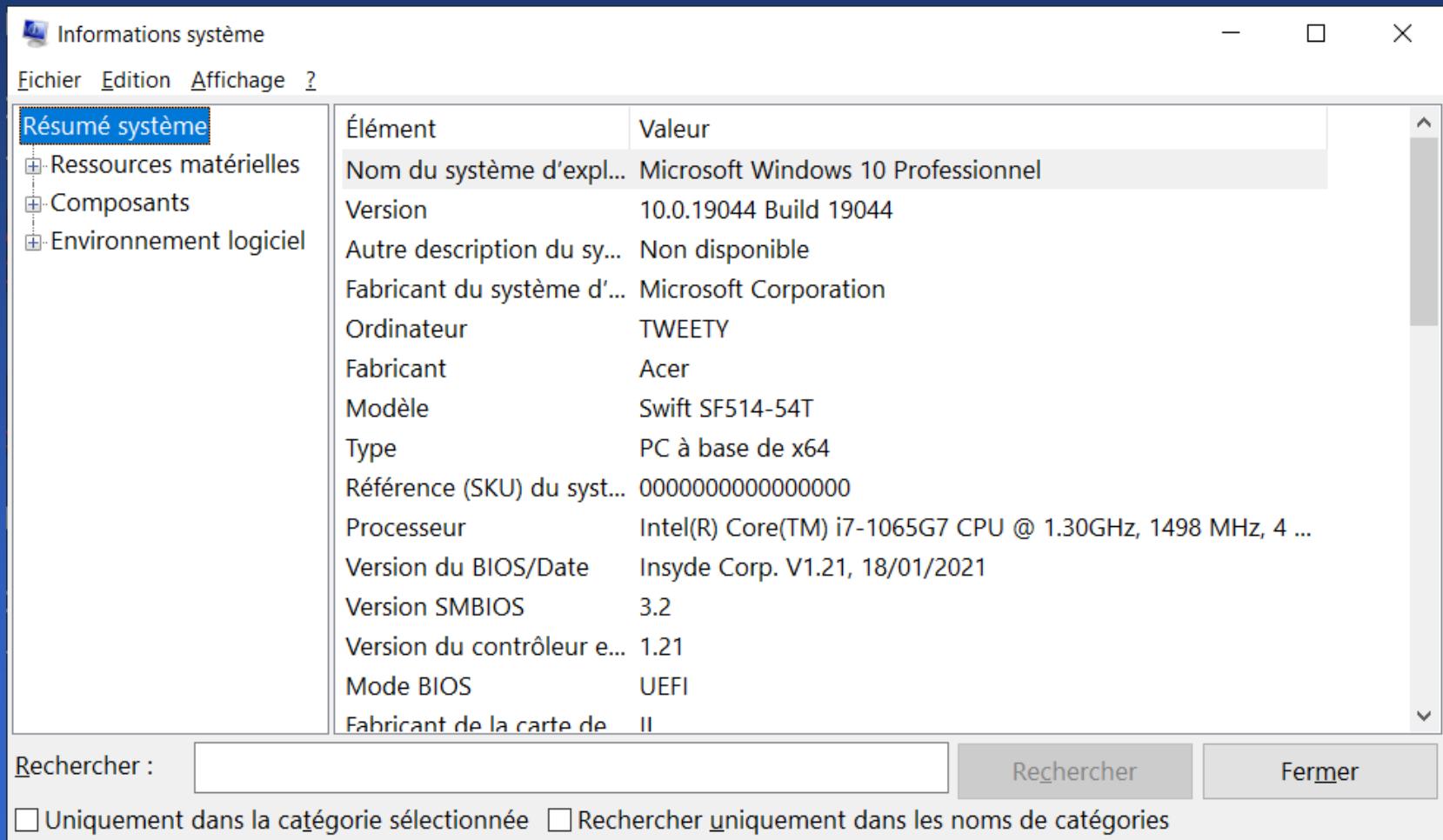
## ◆ Windows Admin Tools

- MMC snap-ins
- Local tools
  - Defrag.
  - Disk cleanup

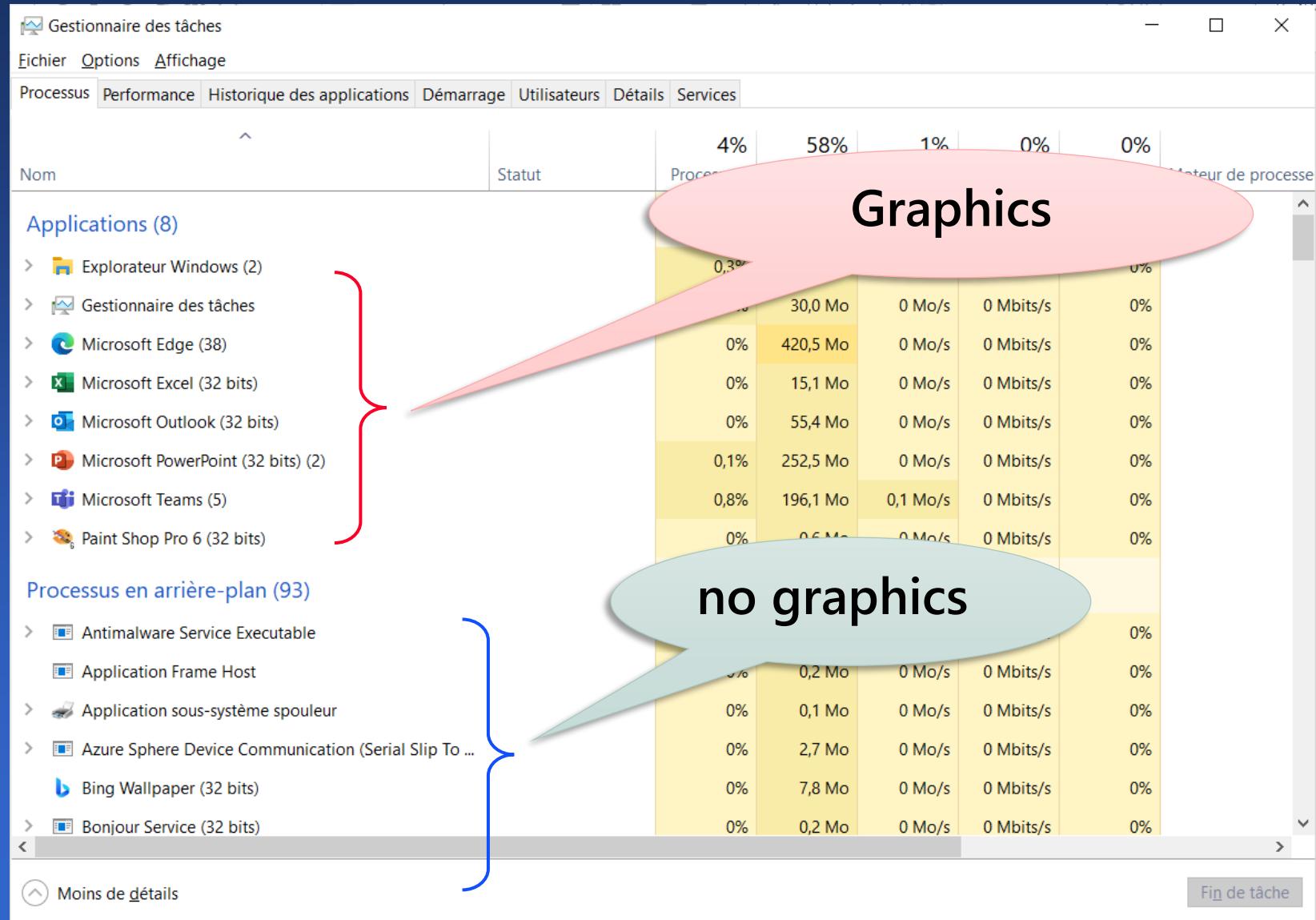


# Hard & Soft summary

## ◆ Launch MSinfo32.exe



# Task manager



# Sysinternals Suite

Article • 11/28/2022 • 2 minutes to read • 8 contributors

By Mark Russinovich

Updated: November 28, 2022

[Download Sysinternals Suite](#) (44.7 MB)

[Download Sysinternals Suite for Nano Server](#) (8.8 MB)

[Download Sysinternals Suite for ARM64](#) (13.1 MB)

[Install Sysinternals Suite from the Microsoft Store](#)

# External tools

## GUI and CLI

# Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [LAN\tjoubert]

File Options View Process Find Users DLL Help

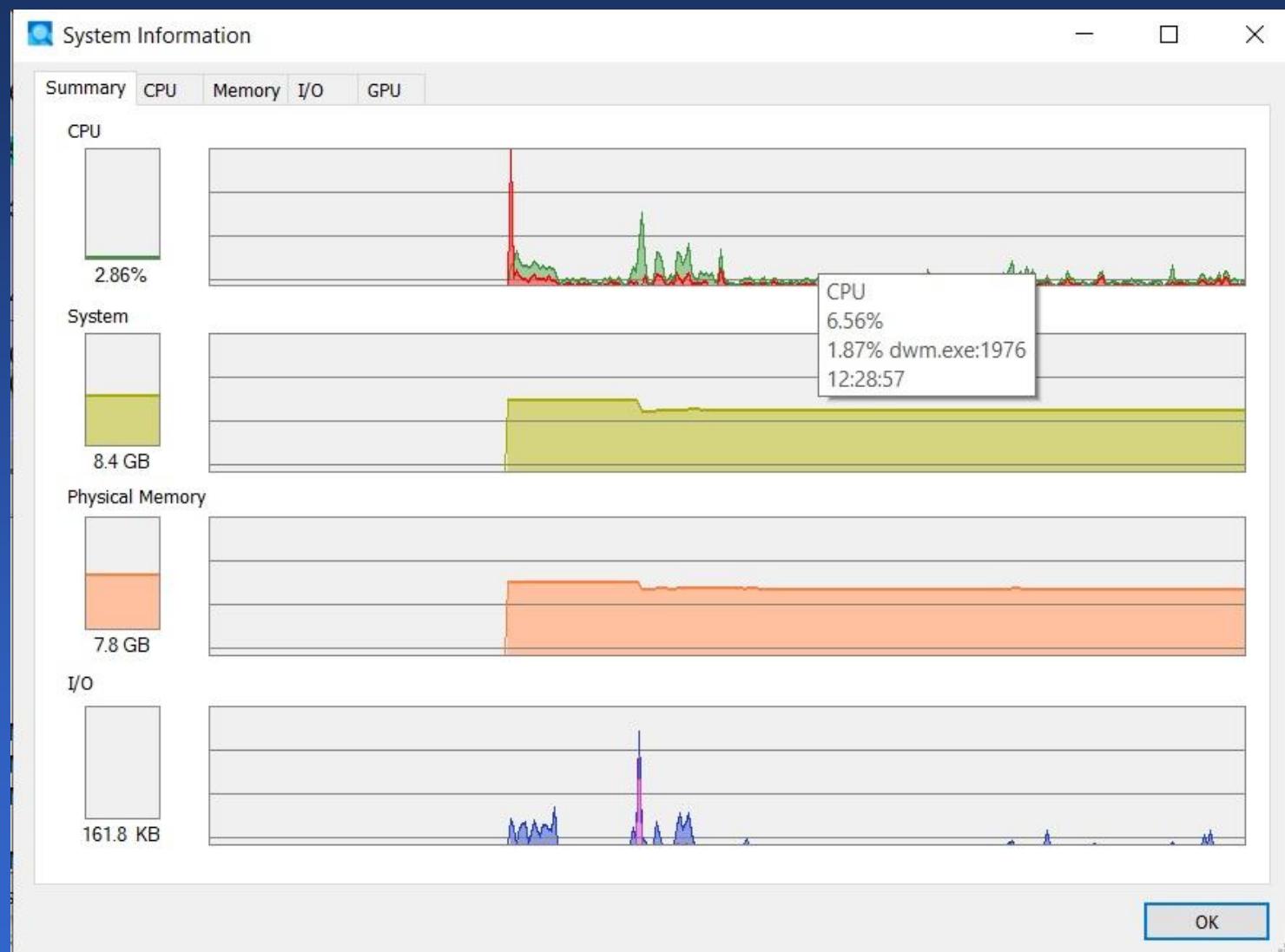
Process	CSwitch Delta	CPU	Private By...	Working Set	PID	Description	Company Name
System Idle Process	2 423	92.87	60 K	8 K	0		
System	262	< 0.01	192 K	152 K	4		
csrss.exe			2 456 K	4 928 K	696		
wininit.exe			1 464 K	5 648 K	844		
csrss.exe	30	< 0.01	3 152 K	5 816 K	852		
winlogon.exe			2 788 K	11 204 K	952		
explorer.exe	3	< 0.01	162 272 K	227 508 K	4620 Explorateur Windows	Microsoft Corporation	
SecurityHealthSystray....			1 948 K	8 952 K	10428 Windows Security notif...	Microsoft Corporation	
OneDrive.exe			41 584 K	73 716 K	1720 Microsoft OneDrive	Microsoft Corporation	
BingWallpaperApp.exe			35 176 K	68 044 K	12704 Bing Wallpaper	Microsoft Corporation	
IGCCTray.exe			49 192 K	55 276 K	13120 IGCCTray	Intel Corporation	
RocketDock.exe	2	< 0.01	6 376 K	25 176 K	1376		
OUTLOOK.EXE	4	< 0.01	187 584 K	242 236 K	1872 Microsoft Outlook	Microsoft Corporation	
WINWORD.EXE	21	< 0.01	71 104 K	113 360 K	11036 Microsoft Word	Microsoft Corporation	
POWERPNT.EXE	22	< 0.01	289 436 K	327 884 K	18684 Microsoft PowerPoint	Microsoft Corporation	
cmd.exe			2 716 K	4 232 K	17160		
conhost.exe			11 212 K	15 420 K	19172		
diskpart.exe			1 296 K	6 600 K	2972		
Windows Terminal.exe	1	< 0.01	47 760 K	70 018 K	16224		
powershell.exe							

Handles DLLs Threads

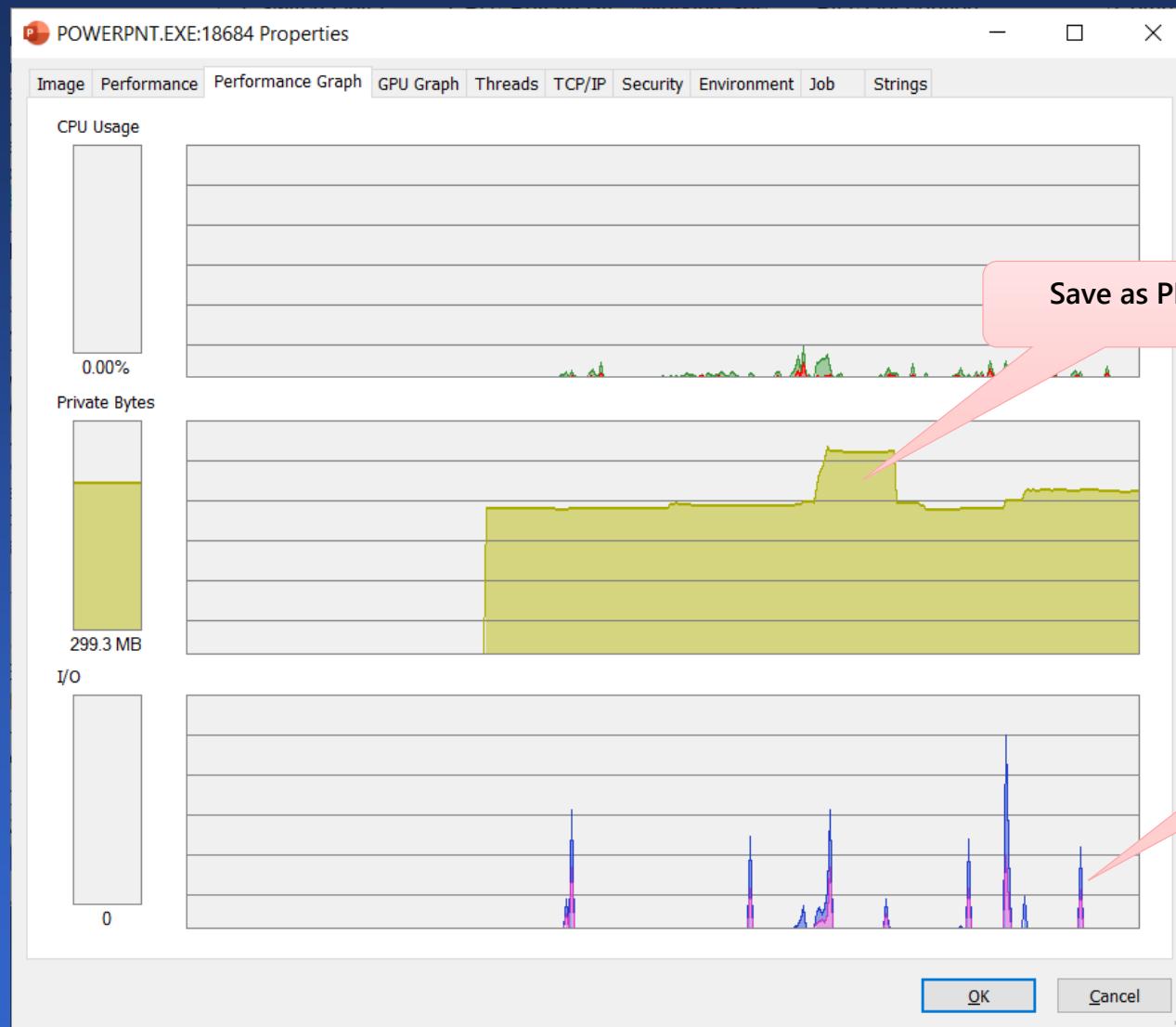
Name	Description	Company Name	Path
{6AF0698E-D55...			C:\ProgramData\Microsoft\Windows\Caches\{6...
{AFBF9F1A-8E...			C:\Users\tjoubert.LAN\AppData\Local\Microsoft...
{DDF571F2-BE...			C:\ProgramData\Microsoft\Windows\Caches\{D...
~FontCache-Fo...			C:\Windows\ServiceProfiles\LocalService\AppData\FontCache\FontCache-Fo...
~FontCache-S-1...			C:\Windows\ServiceProfiles\LocalService\AppData\FontCache\FontCache-S-1...
advapi32.dll	Advanced Windows 32 Bas...	Microsoft Corporation	C:\Windows\SysWOW64\advapi32.dll

CPU Usage: 6.87% Commit Charge: 46.42% Processes: 227 Physical Usage: 50.01%

# Proceexp - System load



# Procexp - Process load



# ProcMon – Process activity

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o... Process Name PID Operation Path Result Detail

Time o...	Process Name	PID	Operation	Path	Result	Detail
12:46:14...	Teams.exe	13012	Thread Create		SUCCESS	Thread ID: 21088
12:46:15...	RuntimeBroker.exe	11892	Thread Create		SUCCESS	Thread ID: 15540
12:46:15...	SmartAudio3.exe	12312	Thread Exit		SUCCESS	Thread ID: 14728, User Time: 0.0000000, Kernel Time: 0.0000000
12:46:15...	SmartAudio3.exe	12312	Thread Create		SUCCESS	Thread ID: 4020
12:46:15...	svchost.exe	1864	Thread Create		SUCCESS	Thread ID: 15424
12:46:15...	svchost.exe	1864	Thread Create		SUCCESS	Thread ID: 1880
12:46:15...	svchost.exe	1864	Thread Create		SUCCESS	Thread ID: 15108
12:46:15...	F Flow.exe	2060	Thread Create		SUCCESS	Thread ID: 21168
12:46:16...	svchost.exe	3304	Thread Create		SUCCESS	Thread ID: 10916
12:46:16...	svchost.exe	3272	Thread Create		SUCCESS	Thread ID: 16208
12:46:16...	SmartAudio3.exe	12312	Thread Exit		SUCCESS	Thread ID: 4020, User Time: 0.0000000, Kernel Time: 0.0000000
12:46:17...	svchost.exe	8056	Thread Create		SUCCESS	Thread ID: 19448
12:46:17...	svchost.exe	3304	Thread Create		SUCCESS	Thread ID: 14636
12:46:17...	svchost.exe	5376	Thread Create		SUCCESS	Thread ID: 18148
12:46:17...	svchost.exe	17544	Thread Exit		SUCCESS	Thread ID: 12940, User Time: 0.0000000, Kernel Time: 0.0000000
12:46:17...	svchost.exe	17544	Thread Exit		SUCCESS	Thread ID: 6856, User Time: 0.0312500, Kernel Time: 0.0156250
12:46:17...	F Flow.exe	2060	Thread Exit		SUCCESS	Thread ID: 21168, User Time: 0.0000000, Kernel Time: 0.0000000
12:46:17...	SmartAudio3.exe	12312	Thread Create		SUCCESS	Thread ID: 16244
12:46:17...	splwow64.exe	19704	Thread Exit		SUCCESS	Thread ID: 18576, User Time: 0.0625000, Kernel Time: 0.0156250
12:46:17...	splwow64.exe	19704	Thread Exit		SUCCESS	Thread ID: 3600, User Time: 0.0000000, Kernel Time: 0.0000000
12:46:18...	OneApp.IGCC.WinSer...	4608	Thread Exit		SUCCESS	Thread ID: 12788, User Time: 0.0000000, Kernel Time: 0.0000000
12:46:19...	SmartAudio3.exe	12312	Thread Exit		SUCCESS	Thread ID: 16244, User Time: 0.0000000, Kernel Time: 0.0000000
12:46:19...	SmartAudio3.exe	12312	Thread Create		SUCCESS	Thread ID: 18536
12:46:20...	svchost.exe	7532	Thread Exit		SUCCESS	Thread ID: 14680, User Time: 0.0000000, Kernel Time: 0.0000000
12:46:20...	Explorer.EXE	4620	Thread Exit		SUCCESS	Thread ID: 13876, User Time: 0.0468750, Kernel Time: 0.0312500
12:46:20...	OUTLOOK.EXE	1872	Thread Create		SUCCESS	Thread ID: 12324
12:46:20...	F Flow.exe	2060	Thread Create		SUCCESS	Thread ID: 4356
12:46:20...	SmartAudio3.exe	12312	Thread Exit		SUCCESS	Thread ID: 18536, User Time: 0.0000000, Kernel Time: 0.0000000
12:46:21...	SmartAudio3.exe	12312	Thread Create		SUCCESS	Thread ID: 2836
12:46:21...	msedge.exe	2940	Thread Exit		SUCCESS	Thread ID: 15384, User Time: 0.0000000, Kernel Time: 0.0000000
12:46:22...	Teams.exe	11464	Thread Create		SUCCESS	Thread ID: 20704
12:46:22...	F Flow.exe	2060	Thread Exit		SUCCESS	Thread ID: 4356, User Time: 0.0000000, Kernel Time: 0.0000000
12:46:22...	svchost.exe	16060	Thread Create		SUCCESS	Thread ID: 11716