

Sumário

INTRODUÇÃO.....	9
Dedicatória.....	11
CAPÍTULO 1: Sobre o autor	13
❖ Aurélio "Baboo"	13
COMDEX.....	14
Internet + site BABOO.....	15
DEFCON + Fórum do BABOO.....	16
MVP (Most Valuable Professional)	18
Windows Server.....	19
BABOO se torna Estudo de Caso da Microsoft.....	20
Cursos do BABOO	20
CAPÍTULO 2: Windows, Arquitetura, Segurança, Copilot, IA, OneCore e Rust	23
❖ Windows.....	23
Windows 10 não foi a última versão do Windows.....	23
❖ Arquitetura do Windows.....	25
Windows 11.....	35
❖ Segurança no Windows 11	36
❖ COPILOT	42
❖ Inteligência Artificial (IA) no Windows 11	42
❖ OneCore	51
❖ RUST.....	52
CAPÍTULO 3: BIOS, UEFI, Firmware e CFU	55
❖ BIOS.....	55
❖ UEFI: a evolução do BIOS	56
Windows mais seguro com UEFI.....	57
Mas o que é DBX?	58
❖ Firmware: o cérebro dos seus dispositivos.....	61
❖ CFU (Component Firmware Update)	62
CAPÍTULO 4: CPU e NPU	63

❖ CPU.....	63
x86, x64, 16 bits, 32 bits e 64 bits	65
SSE e AVX.....	66
Big.LITTLE.....	68
Evolução das CPUs.....	69
❖ NPU	71
Diferenças entre CPU, GPU e NPU.....	71
❖ Windows 11 ARM	72
CAPÍTULO 5: GPU	73
❖ GPU	73
Drivers.....	74
DirectX.....	76
WDDM.....	78
CAPÍTULO 6: RAM	81
❖ RAM	81
Tipos de RAM	83
Como o Windows interage com a RAM	85
CAPÍTULO 7: HD, SSD e SSHD	93
❖ HD	93
❖ SSD	94
OP (Over Provisioning).....	95
TBW	96
❖ SSHD (disco híbrido)	98
Como o Windows interage com o HD, SSD e SSHD?	98
Windows Server 2025 e SSD NVMe	102
Fragmentação	102
Por que a desfragmentação deixa o Windows mais rápido?.....	104
Dicas importantes sobre desfragmentação.....	105
CAPÍTULO 8: FAT, NTFS e ReFS.....	109
❖ FAT	109
❖ NTFS.....	110
❖ ReFS.....	114
ReFS no Windows Server 2025	116

Como o Windows interage com FAT, NTFS e ReFS.....	117
CAPÍTULO 9: MBR, GPT e BCD	119
❖ MBR.....	119
❖ GPT	122
❖ BCD	124
CAPÍTULO 10: Edições do Windows 11 e Windows Server 2025, WOW64	127
❖ Edições do Windows 11 e Windows Server 2025	127
❖ Edições do Windows 11	128
❖ Edições do Windows Server 2025	130
❖ WOW64.....	131
Como saber se um programa está rodando sob WOW64?	133
CAPÍTULO 11: Kernel e Drivers	135
❖ Kernel do Windows	135
Anéis de privilégio	139
❖ Drivers	140
Driver DCH	145
Princípios de Design DCH	145
Principais Características dos Drivers DCH:	146
❖ ID de Hardware.....	147
❖ ARQUIVOS .INF.....	150
Como o Windows encontra o driver correto de um dispositivo?	151
Mudanças após Windows 10 versão 2004	152
Drivers com data de 2006	154
Atualização de drivers	154
CAPÍTULO 12: Serviços, Arquivos DLL e SYS, SID e Sysprep.....	157
❖ Serviços.....	157
Serviços não deixam o Windows mais lento	159
❖ Arquivos .DLL.....	161
Problemas Comuns Relacionados às DLLs.....	163
❖ DLL HELL.....	164
WinSXS e Hard Link.....	165
❖ Arquivos .SYS	167
❖ SID e Syprep.....	169

CAPÍTULO 13: Subsistema do Windows e WSL 2	173
❖ Subsistema do Windows	173
❖ WSL 2	173
Melhorias do WSL 2 no Windows 11 em relação ao Windows 10:	174
❖ Distros Linux	177
CAPÍTULO 14: Hipervisor, Virtualização, Hyper-V, VBS e Área Restrita	179
❖ Hipervisor	179
❖ Virtualização	180
❖ Hyper-V	181
Segurança no Hyper-V	184
❖ VBS	185
❖ Área Restrita do Windows (Windows Sandbox)	189
CAPÍTULO 15: BitLocker	193
❖ BitLocker	193
Métodos de autenticação	195
Habilitando o BitLocker em computadores sem chip TPM	195
Ataques contra o BitLocker	196
Criptografia de Dispositivo x BitLocker	197
CAPÍTULO 16: Processos, Threads e Identificadores	199
❖ Processos	199
❖ Threads	200
❖ Identificadores	204
CAPÍTULO 17: Prioridade e Afinidade	207
❖ Prioridade	207
❖ Afinidade	210
CAPÍTULO 18: Registro do Windows	213
❖ Registro	213
Regedit, Reg e Regini	214
Arquivos e Estrutura hierárquica	215
Otimização ou Limpeza do Registro	217
Backup e Restauração do Registro	219
CAPÍTULO 19: Visualizador de Eventos e ID de Evento	221

❖ Visualizador de Eventos	221
❖ ID de Evento (ID Event)	223
CAPÍTULO 20: Tela Azul da Morte (BSOD).....	229
❖ Tela Azul da Morte (BSOD)	229
O que acontece no momento da Tela Azul da Morte?	230
Códigos de Parada mais comuns.....	231
Motivos da Tela Azul da Morte	232
Como saber qual processo ou driver causou a Tela Azul da Morte	234
CAPÍTULO 21: Gerenciador de Tarefas.....	237
❖ Gerenciador de Tarefas.....	237
Processos	239
Desempenho: CPU.....	241
Desempenho: Memória	243
Desempenho: Disco	246
HD100	248
Desempenho: Ethernet, Wi-Fi e Bluetooth.....	249
Desempenho: GPU	252
Estados de Energia	255
CAPÍTULO 22: Monitor de Recursos.....	257
❖ Monitor de Recursos.....	257
Visão Geral	257
CPU	258
Memória.....	260
Como saber quem está acessando uma determinada pasta?	260
Disco.....	262
Rede.....	263
CAPÍTULO 23: Monitor de Desempenho (PerfMon)	265
❖ Monitor de Desempenho (PerfMon)	265
Exemplo de monitoramento do arquivo de paginação e Photoshop	267
CAPÍTULO 24: Pastas e Processos do Windows.....	273
❖ Pastas do Windows.....	273
Pasta dos usuários.....	274

Desinstalação manual de programas	276
❖ Processos do Windows.....	278
CAPÍTULO 25: Dados de Diagnóstico (Telemetria)	285
❖ Dados de Diagnóstico (Telemetria)	285
ID de Hardware.....	290
Visualizador de Dados de Diagnóstico	291
Privacidade.....	292
CAPÍTULO 26: Windows Update	295
❖ Windows Update.....	295
Atualizações do Microsoft Defender	296
Perigos ao desativar o Windows Update	297
Como o Windows Update funciona.....	299
Windows Update em funcionamento	303
Falha na instalação	305
KIR (Known Issue Rollback)	308
Hotpatch no Windows 11.....	308

A primeira melhoria anunciada pela Microsoft é a nova funcionalidade **Recuperação Rápida da Máquina** (*Quick Machine Recovery*) que está sendo implementada no Windows 11:



A imagem abaixo resume a arquitetura do Windows 11:



1. Hardware

A arquitetura do Windows é projetada para funcionar em uma variedade de **hardware**, desde dispositivos móveis até servidores de alto desempenho. O hardware desempenha um papel crucial na execução do sistema operacional, e a arquitetura do

imagens, efeitos gráficos e decodificação de vídeos puderam ser aceleradas diretamente na CPU, reduzindo a carga da GPU, como por exemplo a decodificação de vídeos em MPEG-4, H.264 e VP9, e a suavização de imagens e filtragem de texturas em gráficos 3D.

Os jogos modernos dependem de cálculos rápidos para movimentação de objetos, simulações físicas e efeitos gráficos, e o SSE permitiu a execução desses cálculos de forma mais eficiente, como no cálculo de colisões em *engines* como Unreal Engine e Unity, e simulação de fluidos e partículas em animações e efeitos especiais. Embora as GPUs sejam otimizadas para cálculos gráficos e AI, a CPU com SSE ainda é fundamental para algumas tarefas, como pré-processamento de dados antes de enviá-los para a GPU, execução de física de jogos que não pode ser delegada à GPU e o gerenciamento de threads e execução de IA em jogos modernos. Em jogos, a CPU com SSE processa lógica de jogo, simulações físicas e animações básicas, enquanto a GPU renderiza gráficos, calcula shaders e efeitos de iluminação.

Muitos softwares aproveitam tanto a CPU (SSE/AVX) quanto a GPU para maximizar o desempenho:

- **Adobe Premiere e DaVinci Resolve** (edição de vídeo), onde a SSE acelera decodificação e a GPU processa efeitos visuais
- **AutoCAD e SolidWorks** (modelagem 3D), com a SSE acelerando cálculos vetoriais enquanto a GPU renderiza os gráficos
- **TensorFlow e PyTorch** (Inteligência Artificial), com a SSE ajudando no pré-processamento, enquanto a GPU treina redes neurais

Um dos requisitos do Windows 11 é que o processador tenha **SSE 4.2** e a **instrução POPCNT (Population Count)** – algo que não deve ser problemático, pois essas funcionalidades estão incorporadas nos processadores desde 2008. A instrução **POPCNT (Population Count)**, introduzida no **SSE4.2** é necessária para agilizar tarefas que envolvam compressão de dados e criptografia, além do Windows 11 fazer uso intensivo da **SIMD** para acelerar cálculos em segundo plano e recursos como segurança baseada em virtualização (VBS).

As otimizações **SIMD (Single Instruction, Multiple Data)** permitem que uma única instrução processe múltiplos dados simultaneamente, aumentando muito o



Embora os jogos mais recentes sejam desenvolvidos para aproveitar o DirectX 12, títulos antigos não recebem atualizações para utilizá-lo, pois isso exigiria reescrever o código-fonte desses jogos, algo que muitas empresas não consideram viável economicamente.



No início de 2025 a Microsoft publicou um artigo sobre **renderização neural no DirectX**, que usa Inteligência Artificial e Aprendizado de Máquina (Machine Learning) para alterar como os gráficos são gerados, em colaboração com as empresas AMD, Intel, NVIDIA e Qualcomm.

WDDM

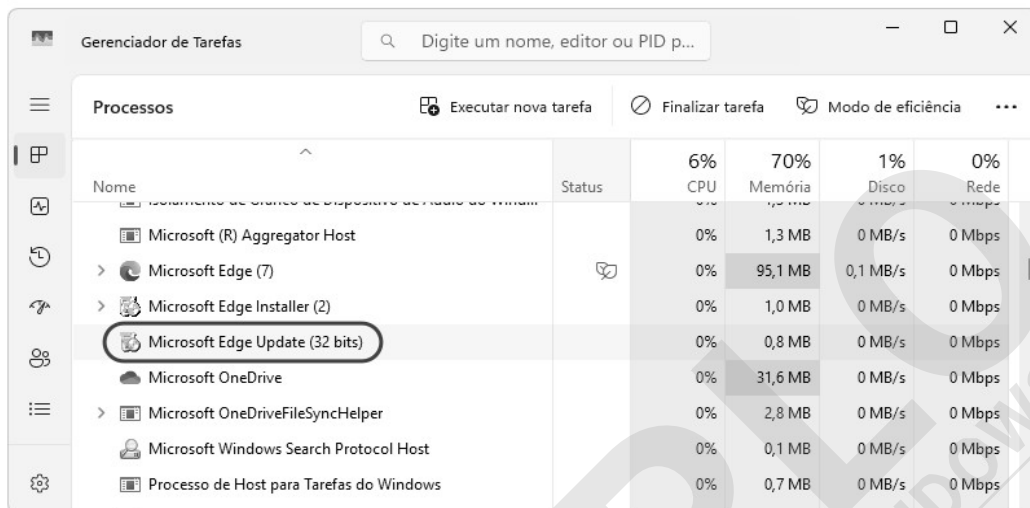
O **WDDM** (*Windows Display Driver Model*) é a arquitetura de driver de vídeo utilizada pelo Windows para gerenciar gráficos e a exibição na tela. Introduzido no Windows Vista em 2006, o WDDM substituiu o antigo XDDM (*Windows XP Display Driver Model*), tornando incompatíveis os drivers desenvolvidos para o Windows XP com o novo sistema operacional.

O WDDM trouxe uma série de melhorias significativas em termos de estabilidade, desempenho e funcionalidades gráficas:

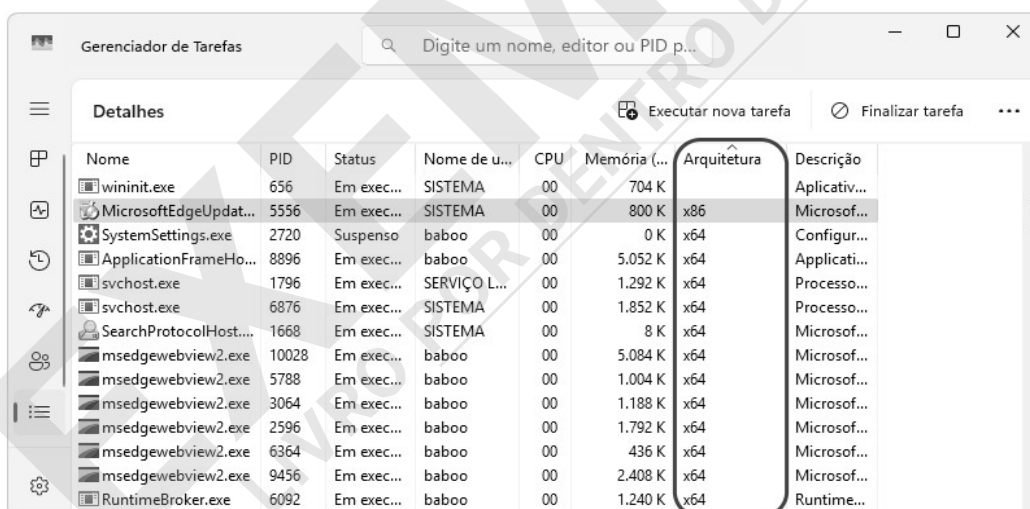
- **Gerenciamento de Memória de Vídeo**, pois o WDDM gerencia a memória de vídeo de forma mais eficiente, permitindo que a GPU e o sistema operacional compartilhem recursos de memória de maneira otimizada.

Como saber se um programa está rodando sob WOW64?

Programas 32 bits sendo executados sob WOW64 aparecem com “(32 bits)” no final do nome dele no Gerenciador de Tarefas:



Além disso, na aba Detalhes você sabe qual é a arquitetura (x86 ou x64) de cada processo em execução:



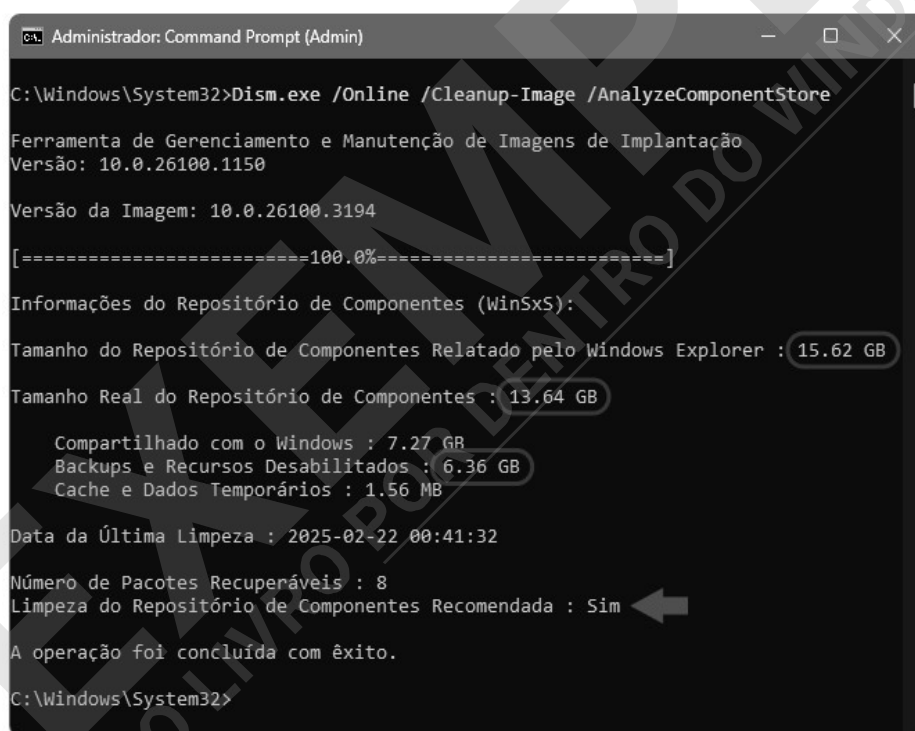
Se criarmos um hard link para o arquivo dx12ultra.dll, ambos os jogos compartilharão o mesmo arquivo físico, economizando espaço:

```
fsutil hardlink create "C:\JogoA\dx12ultra.dll" "C:\Windows\System32\dx12ultra.dll"
```

```
fsutil hardlink create "C:\JogoB\dx12ultra.dll" "C:\Windows\System32\dx12ultra.dll"
```

Com isso, os dois jogos acessam o mesmo arquivo físico em C:\Windows\System32\dx12ultra.dll, mas cada um acredita que a DLL está dentro da sua pasta.

O WinSXS utiliza vários hard links, então ao visualizar os arquivos e pastas existentes em C:\Windows\WinSXS, muitos deles não estão ali, pois na realidade estão em outras pastas. Se você quer saber o tamanho correto da pasta WinSXS, basta executar o comando `dism /online /cleanup-image /analyzecomponentstore` e analisar o resultado, como mostrado nesta imagem:



```
Administrador: Command Prompt (Admin)

C:\Windows\System32>Dism.exe /Online /Cleanup-Image /AnalyzeComponentStore

Ferramenta de Gerenciamento e Manutenção de Imagens de Implantação
Versão: 10.0.26100.1150

Versão da Imagem: 10.0.26100.3194

[=====100.0%=====]

Informações do Repositório de Componentes (WinSxS):

Tamanho do Repositório de Componentes Relatado pelo Windows Explorer : 15.62 GB

Tamanho Real do Repositório de Componentes : 13.64 GB

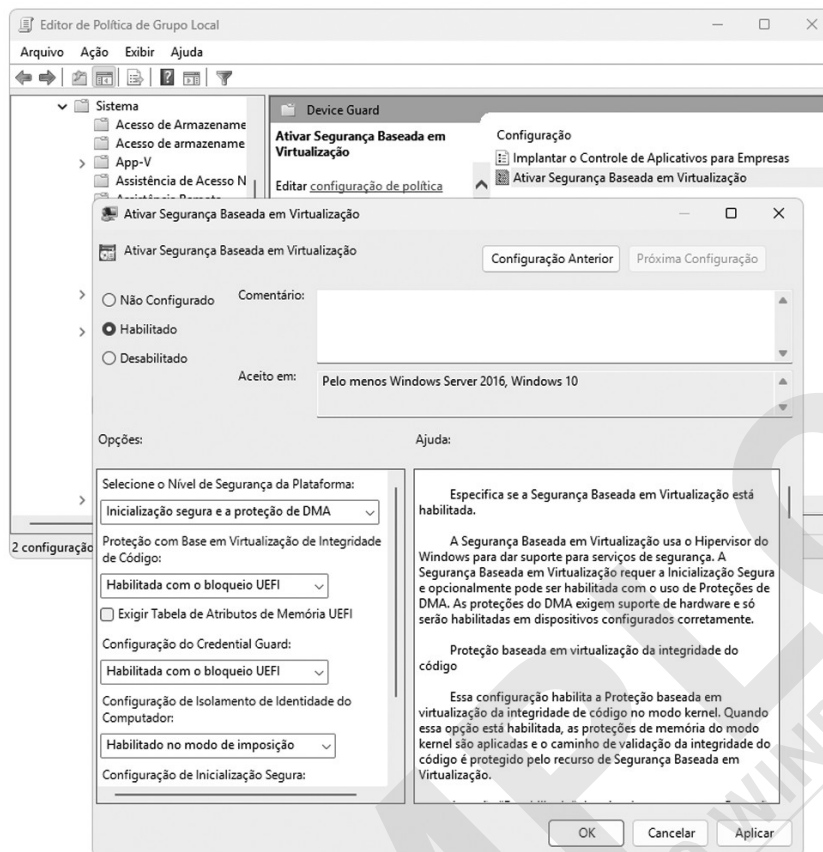
    Compartilhado com o Windows : 7.27 GB
    Backups e Recursos Desabilitados : 6.36 GB
    Cache e Dados Temporários : 1.56 MB

Data da Última Limpeza : 2025-02-22 00:41:32

Número de Pacotes Recuperáveis : 8
Limpeza do Repositório de Componentes Recomendada : Sim ←
A operação foi concluída com êxito.

C:\Windows\System32>
```

O resultado acima mostra que o Explorador de Arquivos considera que a pasta WinSXS tem **15,62 GB**, embora o tamanho real (sem os hard links) seja **13,64 GB**, sendo que **6,36 GB** são referentes a backups e recursos desabilitados. A **seta** mostra que o próprio Windows recomenda a limpeza da pasta WinSXS para remover versões antigas de componentes que não são mais necessárias, ajudando a reduzir o tamanho do repositório e liberar espaço em disco.



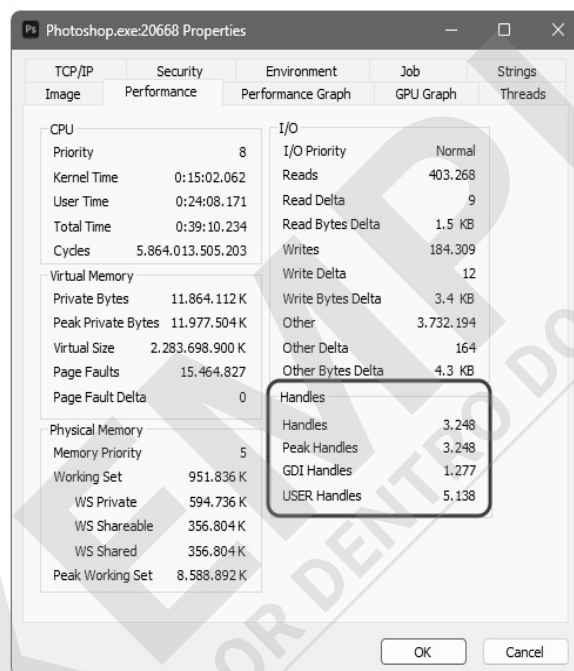
O WDCG utiliza a VBS e o Hyper-V para criar um ambiente isolado chamado **Virtual Secure Mode (VSM)**, onde as credenciais são armazenadas e gerenciadas de forma segura, longe do sistema operacional principal. O **LSA (Local Security Authority)** é um componente crucial que gerencia a autenticação de usuários e a aplicação de políticas de segurança no sistema, e ele tradicionalmente é executado como parte do processo do sistema operacional, mas com a introdução do **Isolated LSA**, ele foi movido para um processo separado (`lsaiso.exe`) para aumentar a segurança do sistema. Ele utiliza o TPM para garantir a integridade do ambiente virtualizado e proteger as chaves de criptografia utilizadas.

Windows Defender Application Guard (WDAG) foi descontinuado no Windows 11 versão 24H2. Ele executava o navegador Edge e aplicações potencialmente perigosas em um contêiner isolado por virtualização, garantindo que sites ou aplicativos suspeitos não pudessem comprometer o sistema principal.

Área Restrita do Windows (Windows Sandbox), abordada no Capítulo 14, permite executar softwares e arquivos potencialmente perigosos ou não confiáveis em um ambiente virtual temporário totalmente isolado, descartando-o automaticamente após o uso e protegendo o computador principal contra ameaças e contaminação por malware.

- **Identificadores de GDI (GDI handles)** são identificadores usados para gerenciar recursos gráficos no Windows, como fontes, bitmaps e objetos de desenho utilizados pelo GDI (Graphics Device Interface, a camada gráfica do Windows) que permite a renderização de elementos visuais.
- **Identificadores do Usuário (User Handles)** incluem recursos como janelas, menus, cursores e ícones, que são fundamentais para a interação do usuário com o sistema operacional e aplicativos

O **Process Explorer** da Microsoft (Sysinternals) mostra mais detalhes de cada tipo de Identificador:



Geralmente o processo **System** (detalhado no Capítulo 24) é o maior responsável pela quantidade de Identificadores:

The screenshot shows the Process Explorer window with the following data:

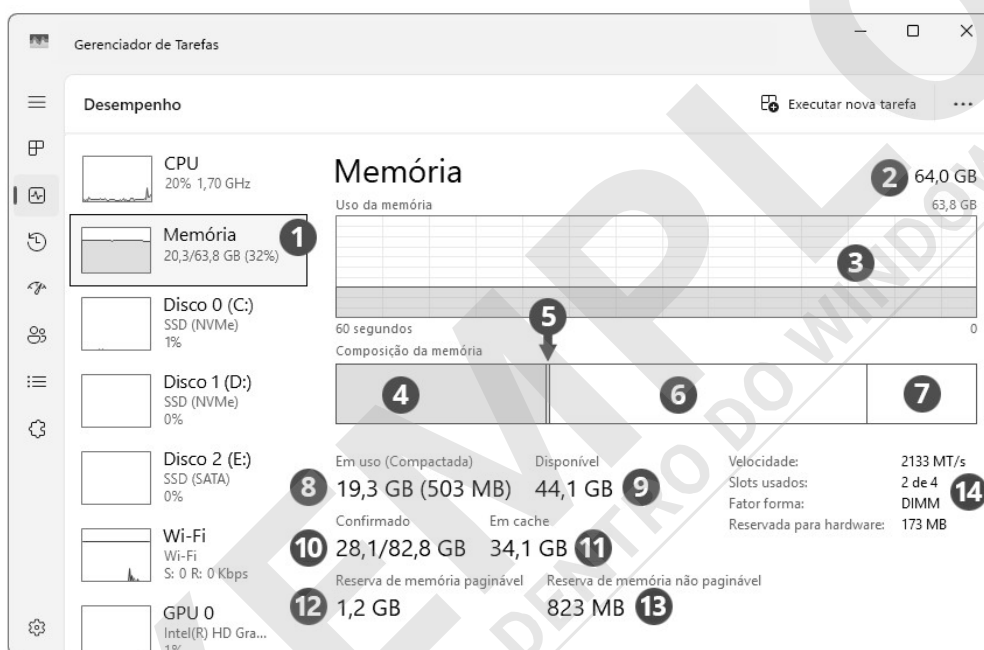
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Handles	Threads
System	0.25	740 K	324,704 K	4			305,313	365
explorer.exe	0.63	423,624 K	414,996 K	13248	Windows Explorer	Microsoft Corporation	8,230	178
msedge.exe	< 0.01	378,208 K	724,388 K	4280	Microsoft Edge	Microsoft Corporation	5,231	64
avp.exe	< 0.01	607,296 K	275,872 K	5888	Kaspersky Lab launcher	AO Kaspersky Lab	4,822	143
OUTLOOK.EXE	< 0.01	284,968 K	364,176 K	19556	Microsoft Outlook	Microsoft Corporation	3,660	73
WINWORD.EXE	< 0.01	319,176 K	465,068 K	15136	Microsoft Word	Microsoft Corporation	3,550	70
Photoshop.exe	< 0.01	11,855,068 K	1,026,664 K	20668	Adobe Photoshop 2024	Adobe	3,266	140
dwm.exe	0.51	372,984 K	125,492 K	2776			2,247	52

At the bottom of the window, the status bar shows: CPU Usage: 10.53%, Commit Charge: 58.33%, Processes: 296, Physical Usage: 41.32%.

de cache mais distante do núcleo da CPU, mas ainda mais rápido do que a memória RAM e o que possui a maior capacidade de armazenamento entre os três níveis de cache.

Desempenho: Memória

O gráfico de **memória RAM** é bastante incompreendido pelo excesso de informações mostradas que podem confundir o usuário. O Windows trabalha com quatro tipo de memórias: em uso, modificada, em espera e livre+zerada.



1: Memória indica a quantidade de uso atual da RAM, o total de RAM disponível e a porcentagem de uso em relação ao total.

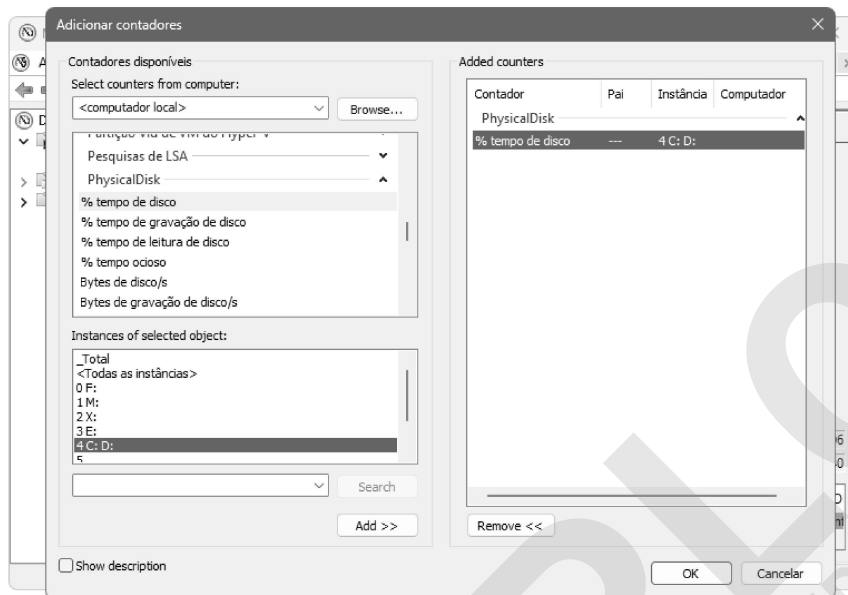
2: Total: de memória RAM instalada.

3: Gráficos mostra visualmente a utilização da memória RAM nos últimos 60 segundos, onde o valor máximo é o total da memória RAM instalada (64 GB no exemplo acima) menos a memória RAM reservada para o hardware (173 MB mostrado no item 14).

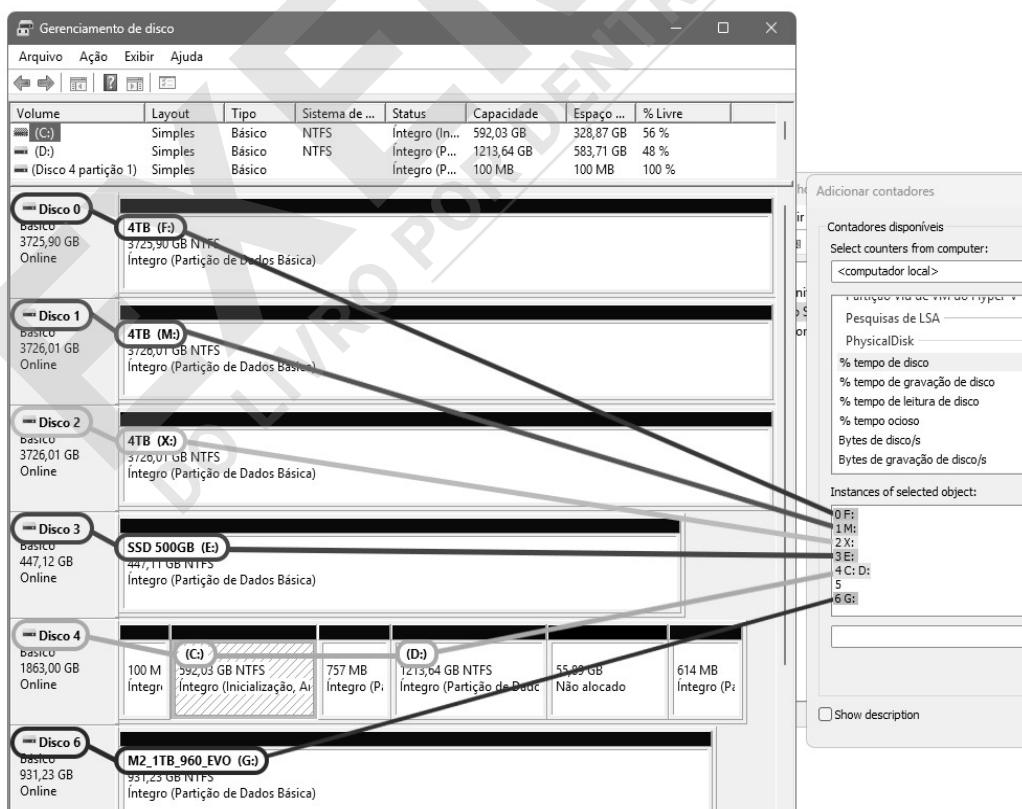
4: Memória em Uso mostra visualmente a quantidade de memória física utilizada pelos programas, processos, drivers e sistema operacional. O valor é mostrado no item 8.

5: Memória Modificada é a quantidade de memória que foi alterada pelos aplicativos e processos em execução, mas ainda não foi gravada no disco rígido. Exemplo: você

Ao seleccionar o disco desejado e clicar em **Adicionar**, o contador passará a ser exibido no gráfico principal:



Para confirmar qual disco ou partição você deseja monitorar, abra primeiro o Gerenciamento de Disco do Windows e compare as informações exibidas com aquelas mostradas no PerfMon. Você verá que todos os dispositivos de armazenamento e suas partições são listados ali, facilitando a identificação:



Com os arquivos já baixados, o sistema entra na fase de instalação. O Windows Update inicia a aplicação dos pacotes, utilizando o **NTFS Transacional**, que permite reverter qualquer modificação no caso de falhas durante a instalação.

Cada atualização é processada individualmente, garantindo que dependências sejam respeitadas e que possíveis conflitos sejam resolvidos antes da aplicação. Algumas atualizações podem ser instaladas imediatamente em segundo plano, enquanto outras exigem uma reinicialização do sistema para substituir arquivos críticos que estão em uso.

A instalação das atualizações envolve alguns processos. Entre eles estão o `TIWorker.exe`, que gerencia e aplica atualizações, `msiexec.exe` (Windows Installer) que instala programas e aplicativos, e `TrustedInstaller.exe`, que gerencia os componentes que serão atualizados.

Durante a execução desses processos, é normal aumentar por vários minutos o consumo de CPU, RAM e disco, voltando aos níveis normais assim que a instalação das atualizações for finalizada.

Com o lançamento da versão **24H2 do Windows 11**, a Microsoft implementou otimizações significativas no processo de atualização. Essas melhorias resultam em tempos de instalação até 45% mais rápidos, redução de até 25% no uso da CPU durante as atualizações mensais e diminuição de quase 40% no tempo de reinicialização em alguns sistemas. Essas otimizações foram alcançadas por meio do processamento paralelo de componentes, uso escalável da RAM do sistema e cache otimizado para atualização de componentes.

Caso uma atualização necessite de reinicialização, o Windows Update avisa o usuário. Quando o computador é reiniciado, ele entra em um modo de manutenção, onde as atualizações são finalizadas antes da inicialização completa do sistema. Esse processo é auxiliado pelo **WinRE** (*Ambiente de Recuperação do Windows*), que pode restaurar automaticamente o sistema para um estado anterior caso algo dê errado durante a aplicação das atualizações.

Após o carregamento do sistema operacional, o Windows Update realiza em segundo plano uma verificação pós-instalação para garantir que as atualizações foram aplicadas corretamente, analisando diversos parâmetros de funcionamento e