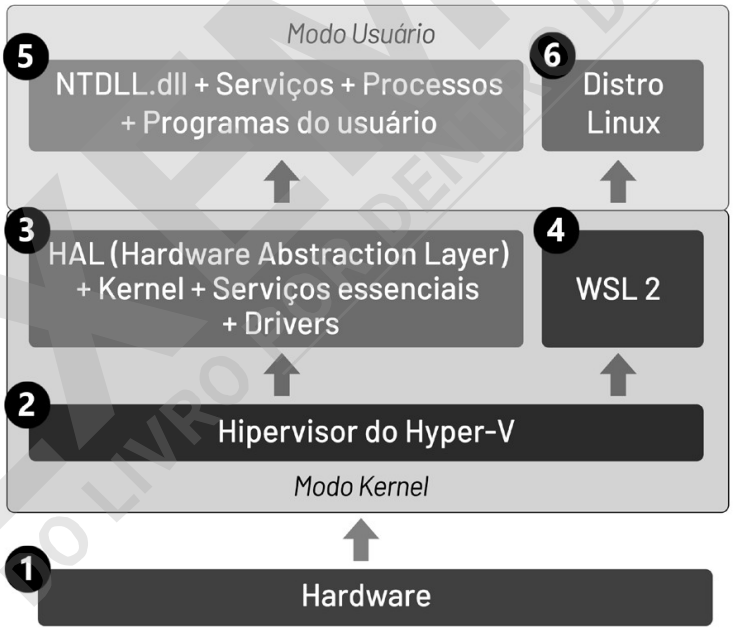
Sumário

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

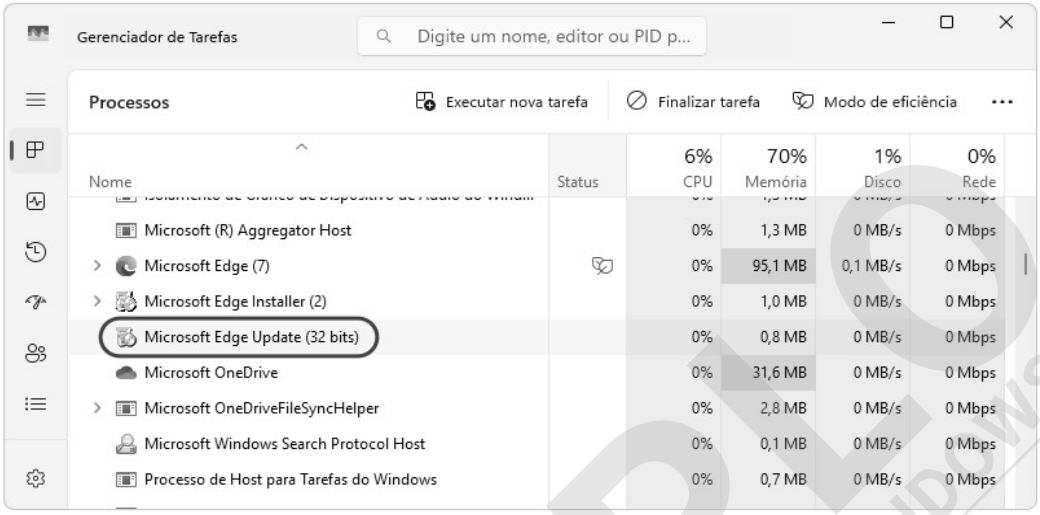
O **WDDM** *(Windows Display Driver Model)* é a arquitetura de driver de vídeo utilizada pelo Windows para gerenciar gráficos e a exibição na tela. Introduzido no Windows Vista em 2006, o WDDM substituiu o antigo XDDM (Windows XP Display Driver Model), tornando incompatíveis os drivers desenvolvidos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

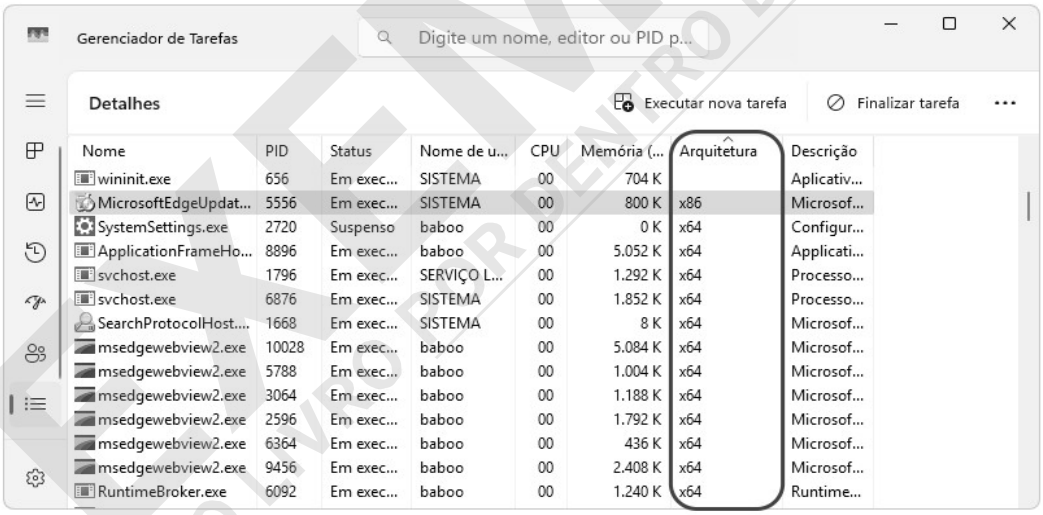
- **Gerenciamento de Memória de Vídeo**, pois o WDDM gerencia a memória de vídeo de forma mais eficiente, permitindo que a GPU e o sistema operacional compartilhem recursos de memória de maneira otimizada.

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:

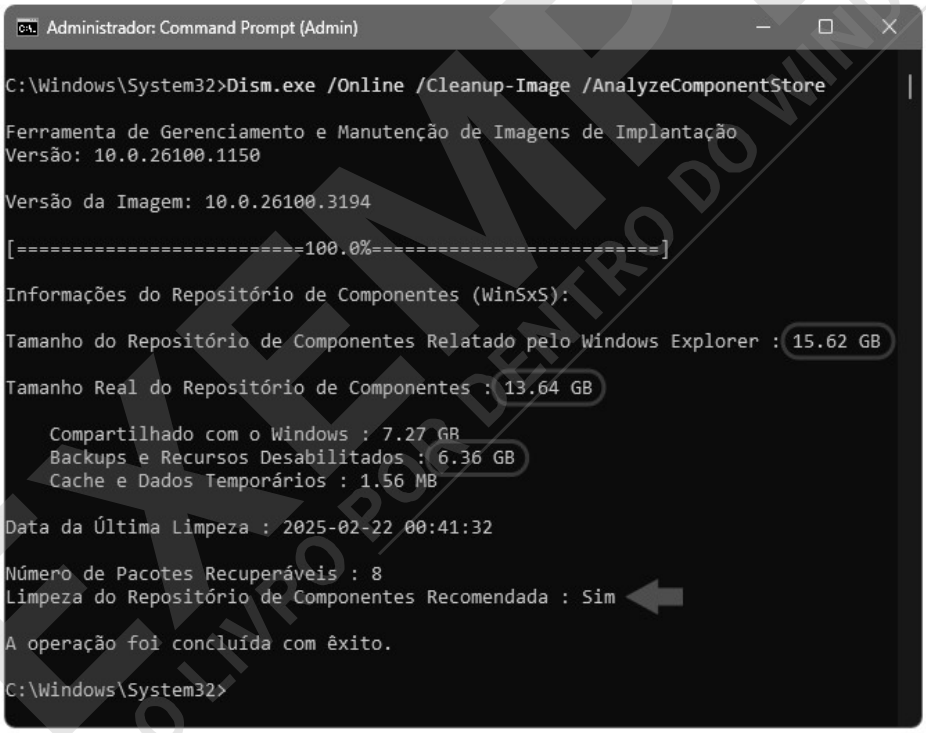


Se criarmos um hard link para o arquivo `dx12ultra.dll`, ambos os jogos compartilharão o mesmo arquivo físico, economizando espaço:

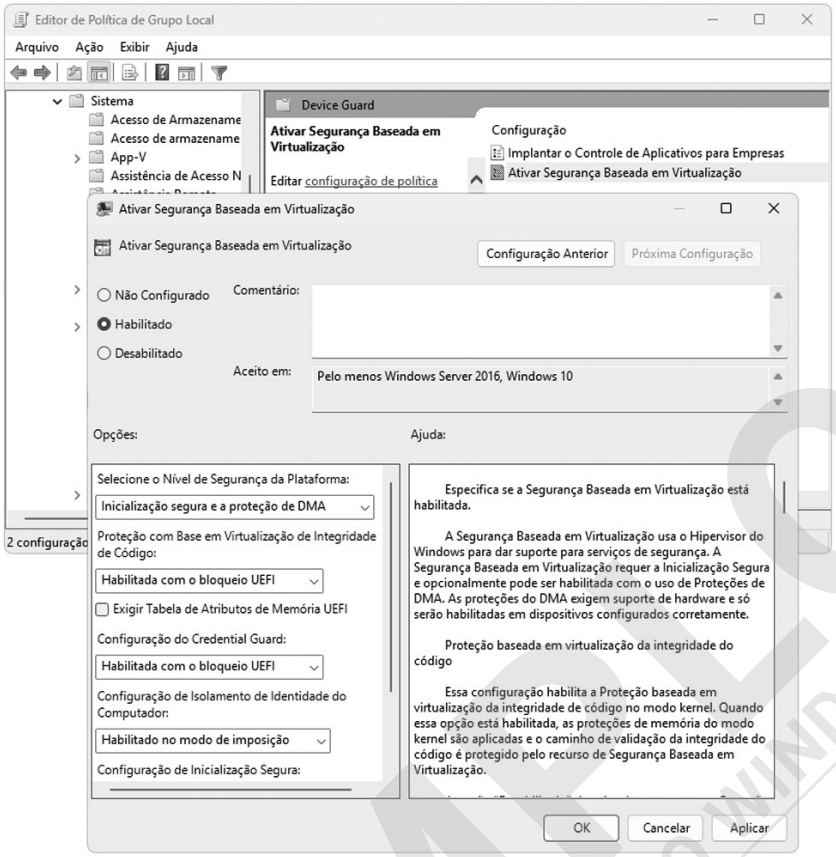
```
fsutil hardlink create "C:\JogoA\dx12ultra.dll" "C:\Windows\System32\dx12ultra.dll"
fsutil hardlink create "C:\JogoB\dx12ultra.dll" "C:\Windows\System32\dx12ultra.dll"
```

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:



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.



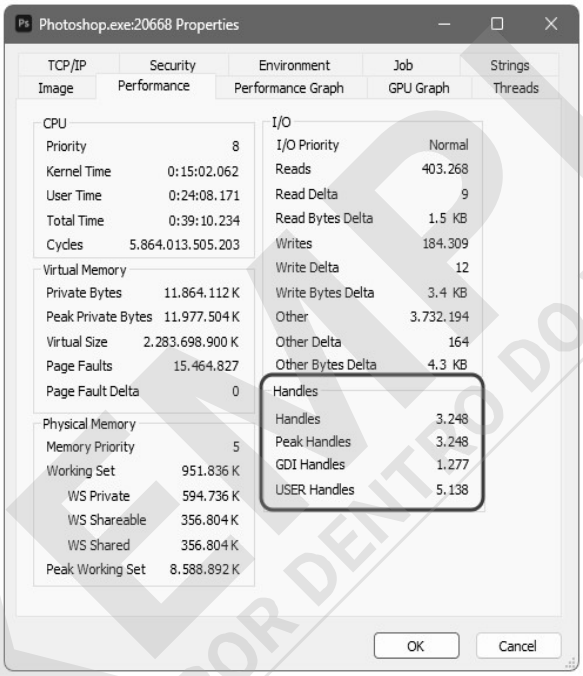
O WDCG utiliza a VBS e o Hyper-V para criar um ambiente isolado chamado **Virtual Secure Mode (VSM)**, onde as credenciais são armazenadas e gerenciadas de forma segura, longe do sistema operacional principal. O **LSA** *(Local Security Authority)* é um componente crucial que gerencia a autenticação 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.

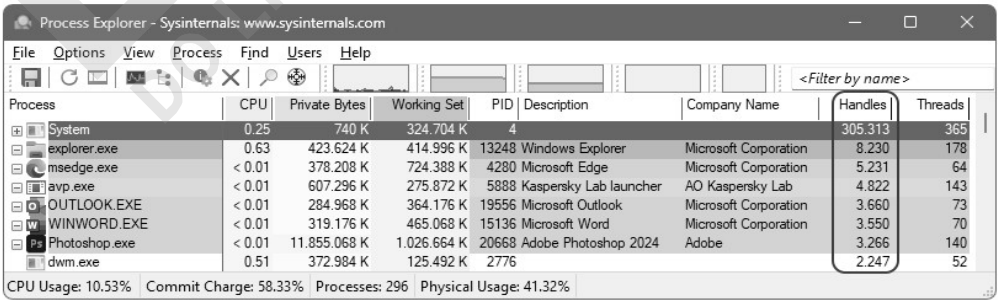
Área Restrita do Windows *(Windows Sandbox)*, abordada no Capítulo 14, permite executar softwares e arquivos potencialmente perigosos ou não confiáveis em um ambiente virtual temporário totalmente isolado, descartando-o automaticamente após o uso e protegendo o computador principal contra ameaças e contaminação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



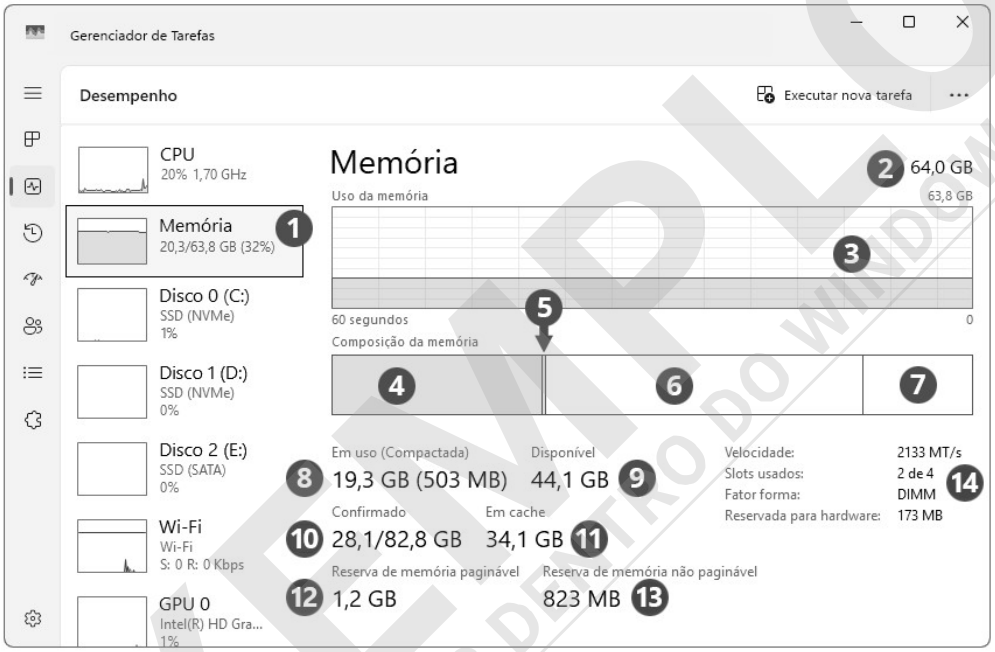
Geralmente o processo **System** (detalhado no Capítulo 24) é o maior responsável pela quantidade de Identificadores:



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.

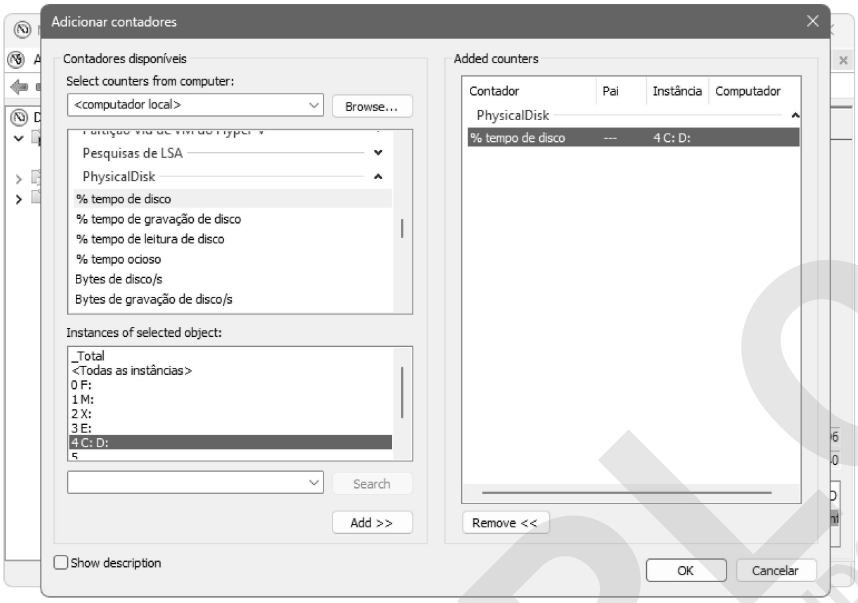
2: Total: de memória RAM instalada.

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**).

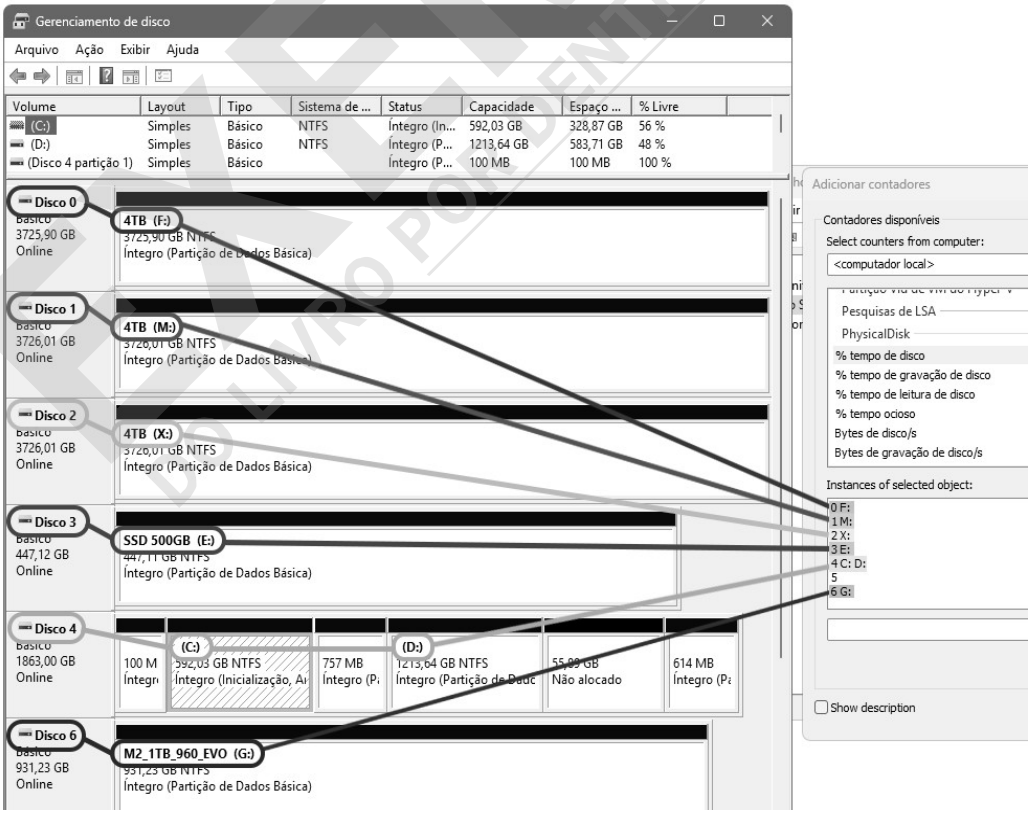
4: Memória em Uso mostra visualmente a quantidade de memória física utilizada pelos programas, processos, drivers e sistema operacional. O valor é mostrado no item **8**.

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 selecionar 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 aplicar 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