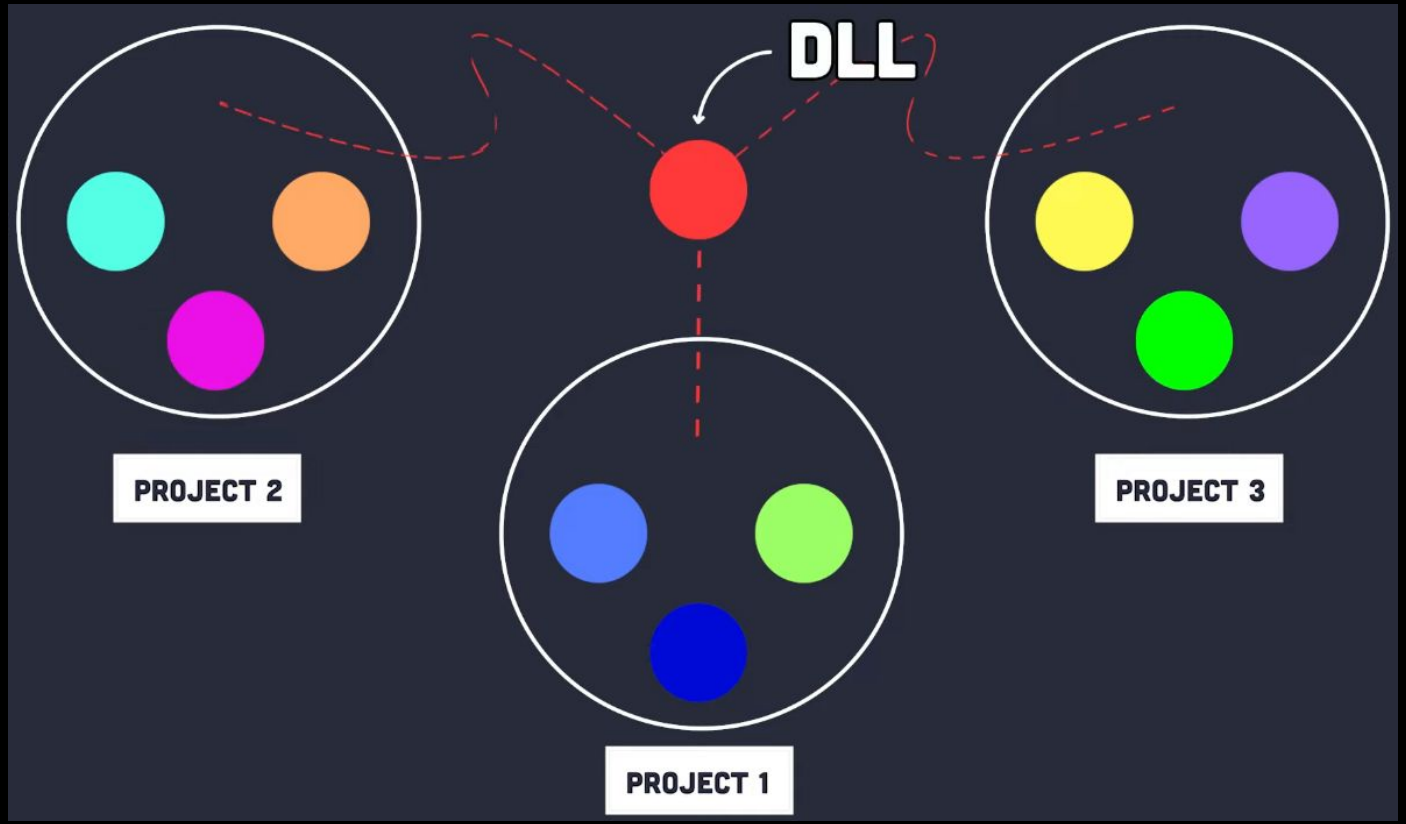
DLL Injection


GANESH
O que são DLLs?

O que são DLLs?

- Dynamic Link Library (Biblioteca de Link Dinâmico)
- Contém código, dados ou recursos (ícones, imagens)
- Acesso compartilhado
- No passado, solução para falta de memória (evita duplicação)
- É um PE (Portable Executable, permite execução)
- Apenas para Windows

O que são DLLs?



O que são DLLs?


GANESH
APIs do Windows

APIs do Windows

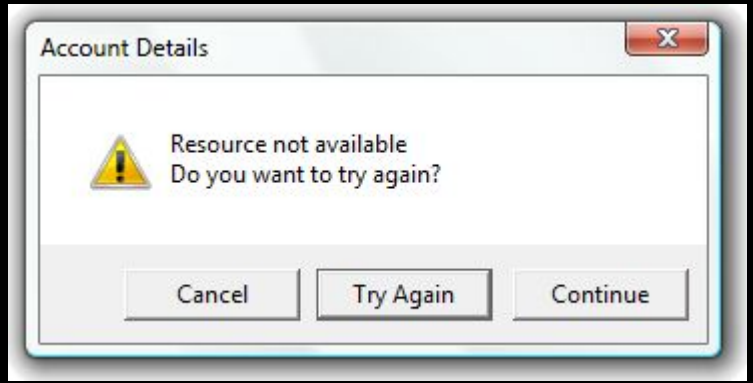
- Conjunto de funções que facilitam uso dos recursos do SO
- Apps não possuem acesso direto a processador/memória, deve ser feito via APIs

GANESH

APIs do Windows

```c
#include <windows.h>

int main(void) {
    MessageBox(
        NULL,
        (LPCWSTR)L"Resource not available\nDo you want to try again?",
        (LPCWSTR)L"Account Details",
        MB_ICONWARNING | MB_CANCELTRYCONTINUE | MB_DEFBUTTON2
    );
}
```



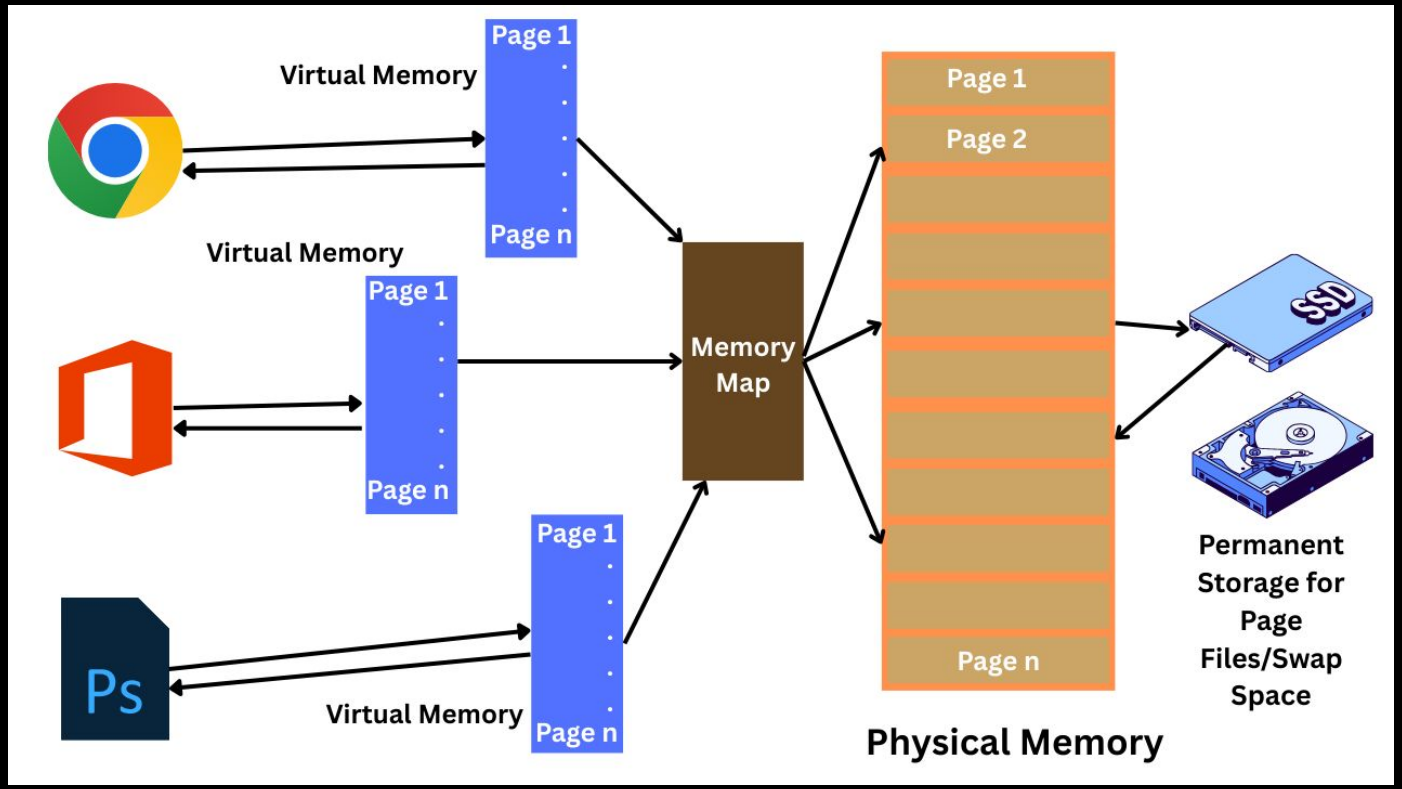

GANESH
Memória Virtual

Memória Virtual

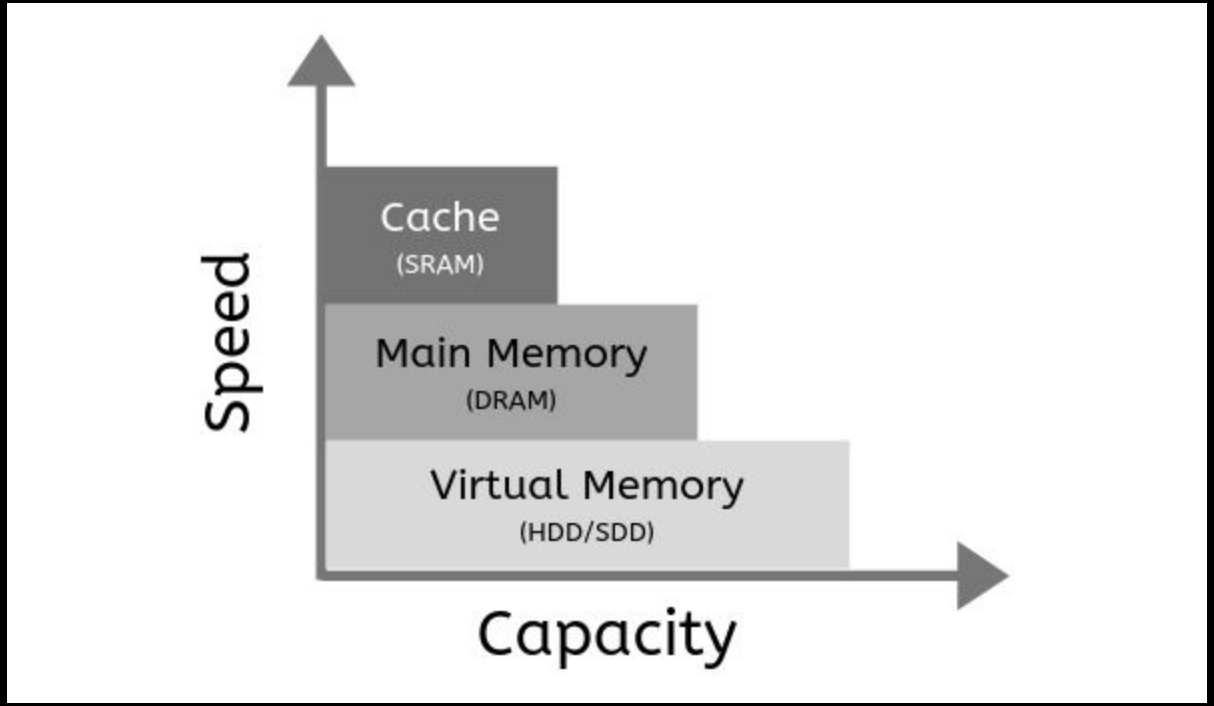
GANESH

- Técnica que permite executar programas que precisam de mais memória do que o disponível
- Gerenciado pelo SO
- Dados na RAM que não são usados com frequência são jogados temporariamente no HD/SSD, como arquivos de paginação (pagefile.sys)
- Arquivos de paginação são gerenciados como (memória a mais), e recuperados/armazenados conforme necessidade
- A memória virtual contém tanto RAM quanto HD/SSD

Memória Virtual



Memória Virtual

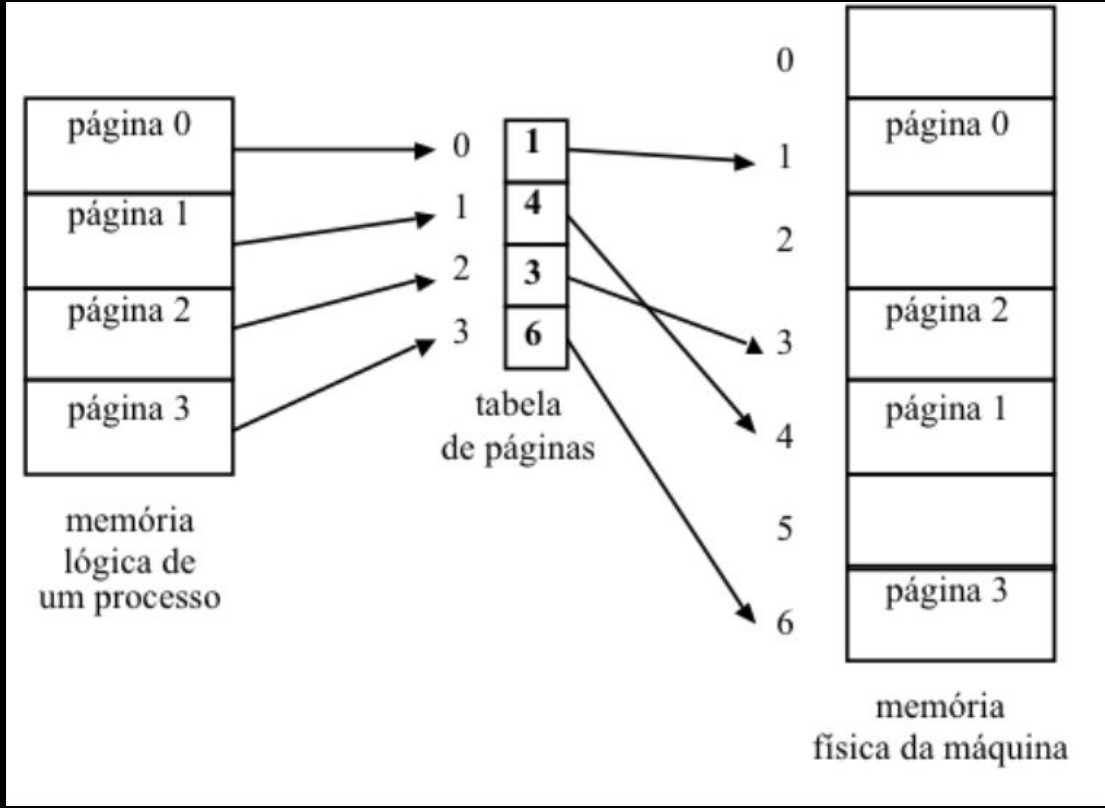


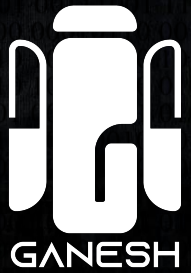

GANESH
Paginação

Paginação

- Técnica de gerenciamento de memória
- Memória dividida em pedaços do mesmo tamanho (cerca de 4Kb), tanto na RAM (frames) quanto na memória virtual (páginas)
- Programa não precisa ser encaixado na RAM, está espalhado
- Cada processo tem sua própria tabela de páginas (mapa de páginas e frames). Assim, um processo não pode acessar memória de outro processo

Memória Virtual





Process Address Space

Process Address Space

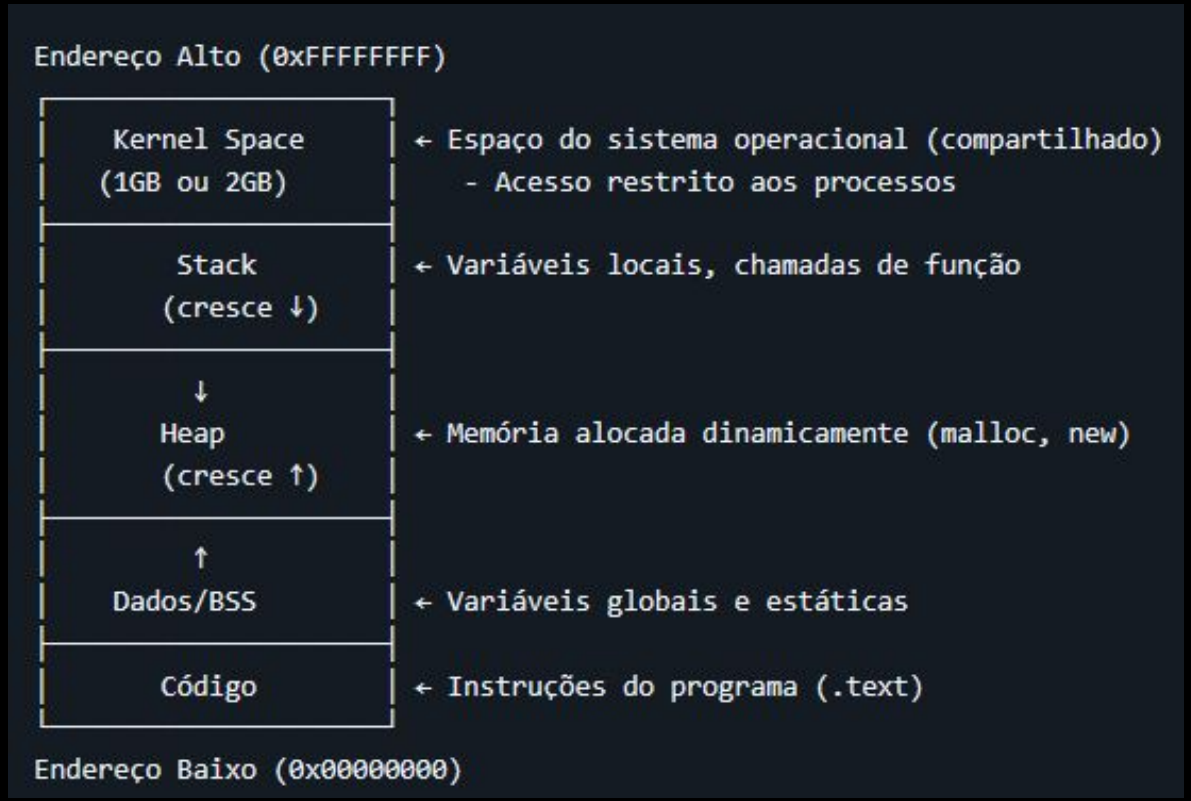
- Região de memória virtual alocada para cada processo rodando na máquina
- Windows implementa isolamento por padrão. Processos podem apenas acessar seu próprio espaço de memória.

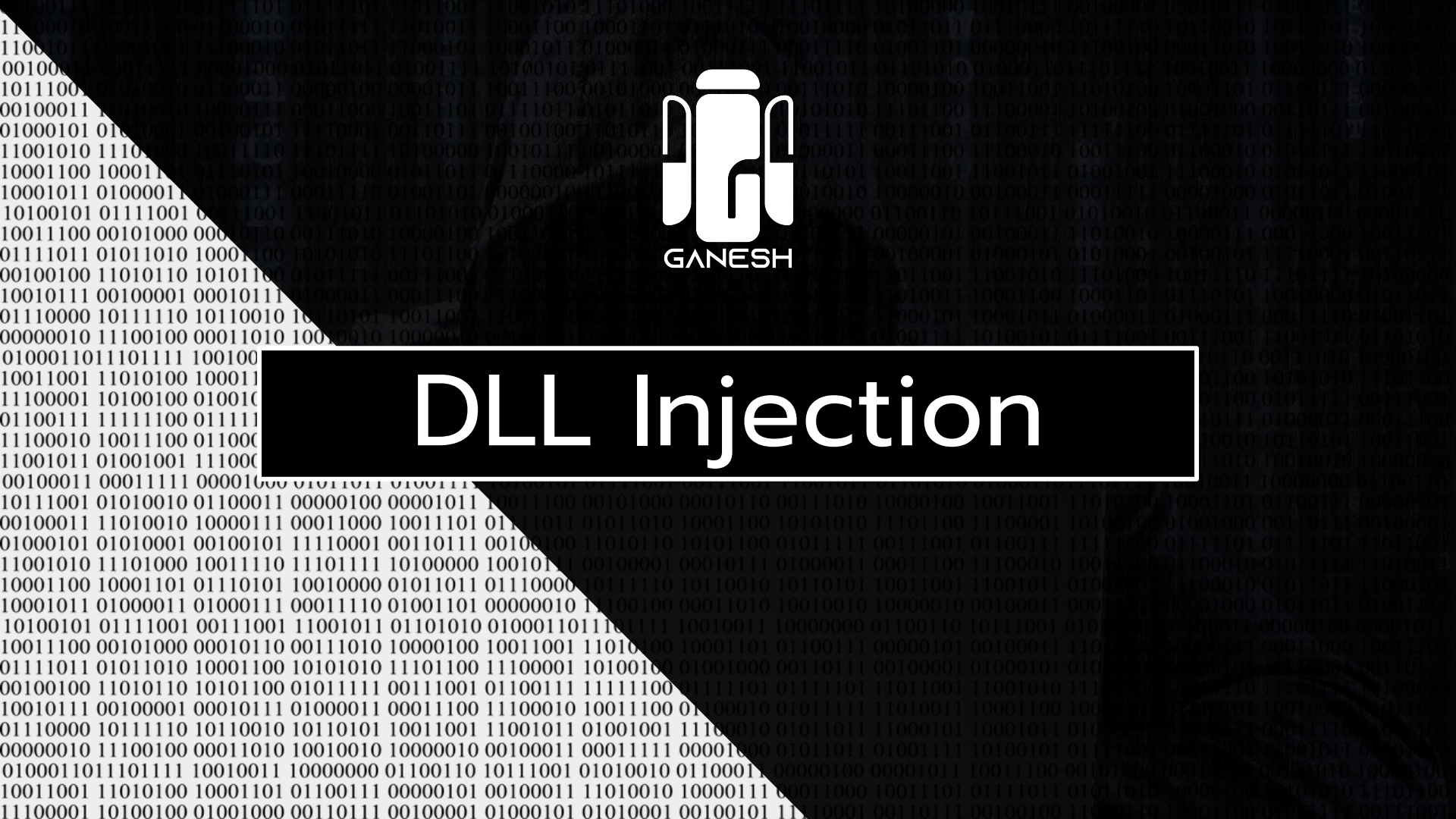
Process Address Space

GANESH

Processo A (Word):	Processo B (Excel):	Memória Física (RAM):
0x00000000-0x0000FFFF	0x00000000-0x0000FFFF	Processo A - Página 0
0x00010000-0x0001FFFF	0x00010000-0x0001FFFF	Processo B - Página 0
0x00020000-0x0002FFFF	0x00020000-0x0002FFFF	Processo A - Página 1
...	...	Processo B - Página 1
0x7FFFFFFF-0xFFFFFFFF	0x7FFFFFFF-0xFFFFFFFF	...

Process Address Space

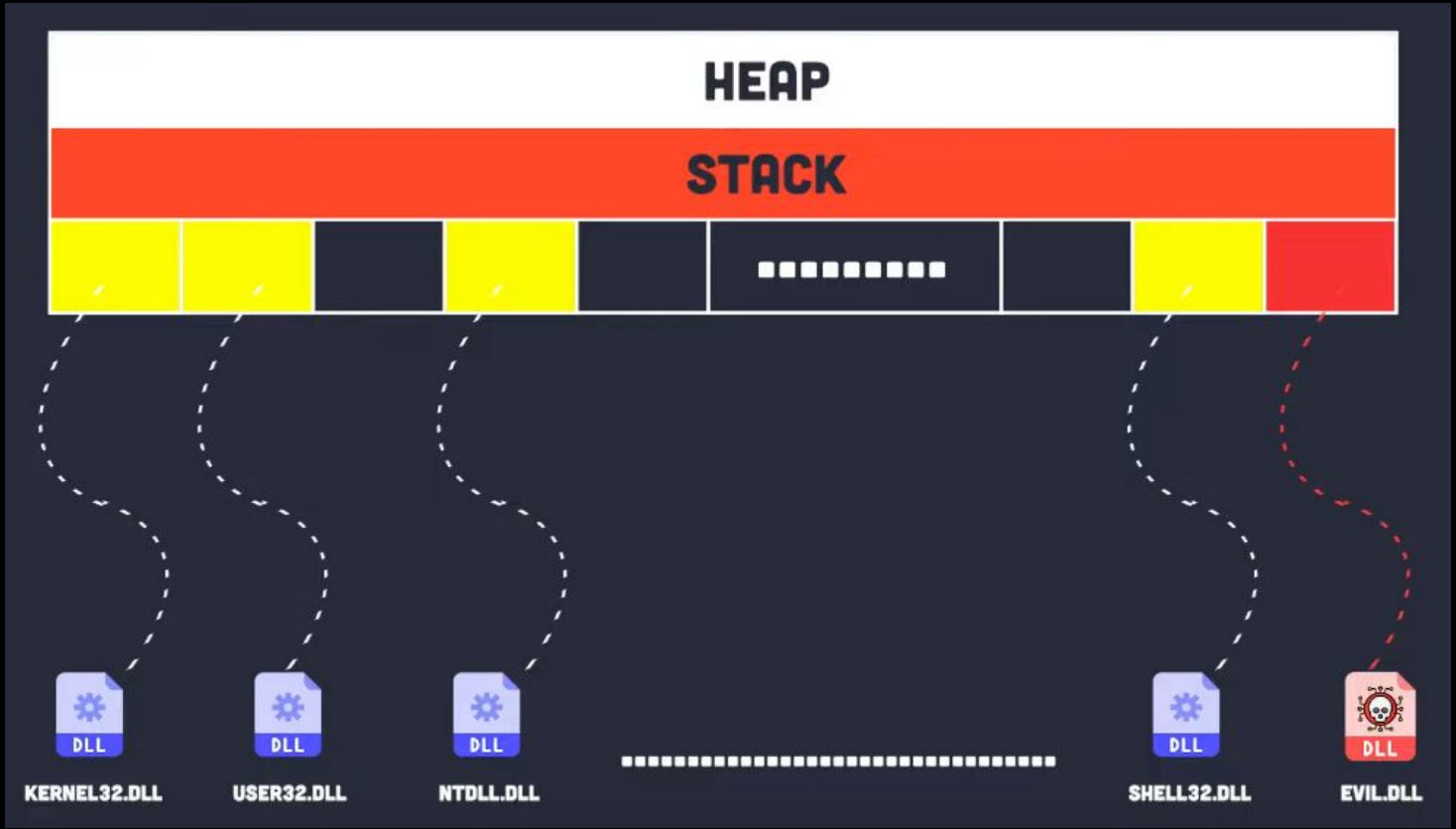



GANESH
DLL Injection

DLL Injection

- Método de injeção de código, onde um processo (injetor) manipula outro processo ativo para carregar uma DLL dentro dele
- DLL injetada ganha acesso completo ao espaço de memória do processo alvo, inclusive a recursos e privilégios
- É difícil de detectar, consegue evadir antivírus, não é notado pelo usuário, herda os privilégios do processo alvo, e pode ler dados da região de memória do processo alvo (como cookies, senhas, tokens de sessão)

DLL Injection



GANESH

Grupo de Extensão em Segurança da Informação

ICMC USP SÃO CARLOS

@ganeshICMC @ganeshicmc

Contato:

ganesh@icmc.usp.br

https://ganesh.icmc.usp.br