
VIII SEMANA DA COMPUTAÇÃO
E TECNOLOGIA

Execução de Código Debaixo dos Panos

Wanderley Caloni

Caloni: definição

```
auto caloni = 0; ///@todo dunno
```

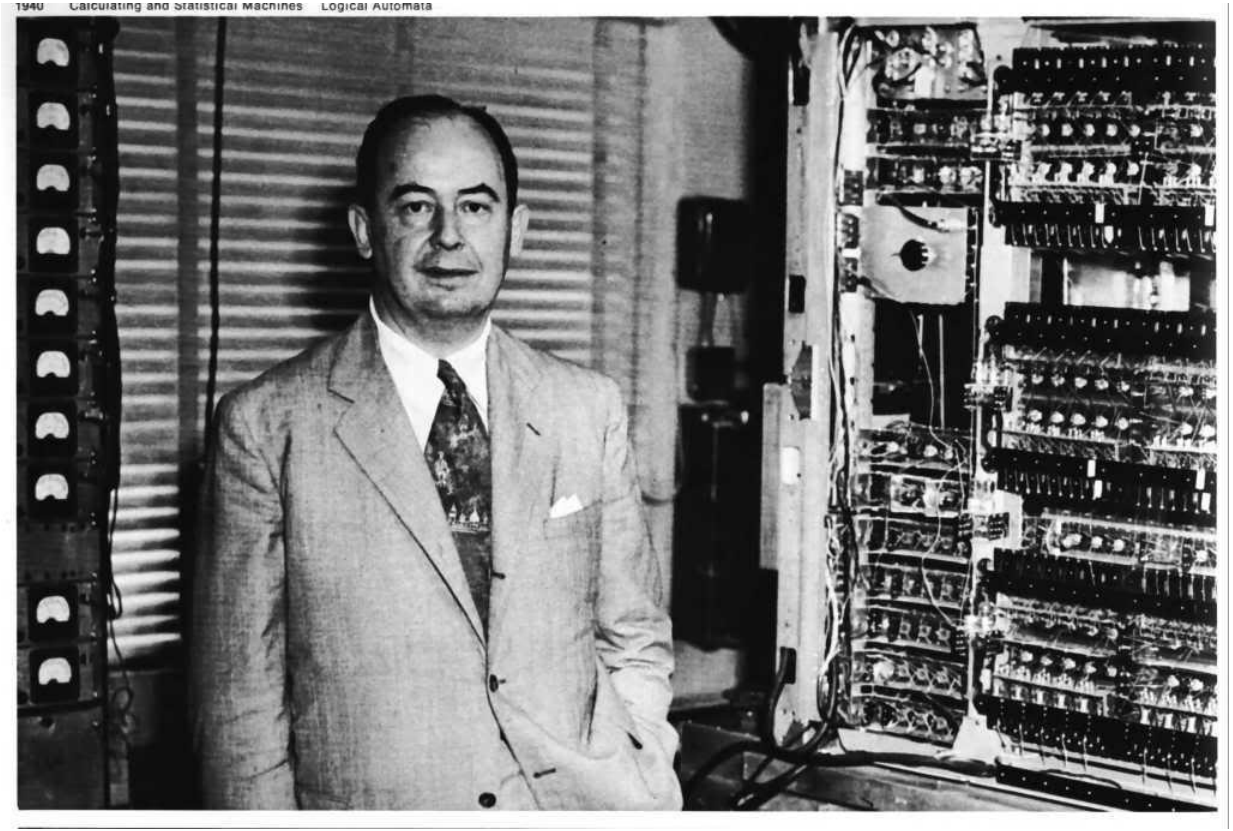
Wanderley Caloni

Dev CCPP, Microsoft MVP and Personal CCF (Capitalista que Curte Filmes).

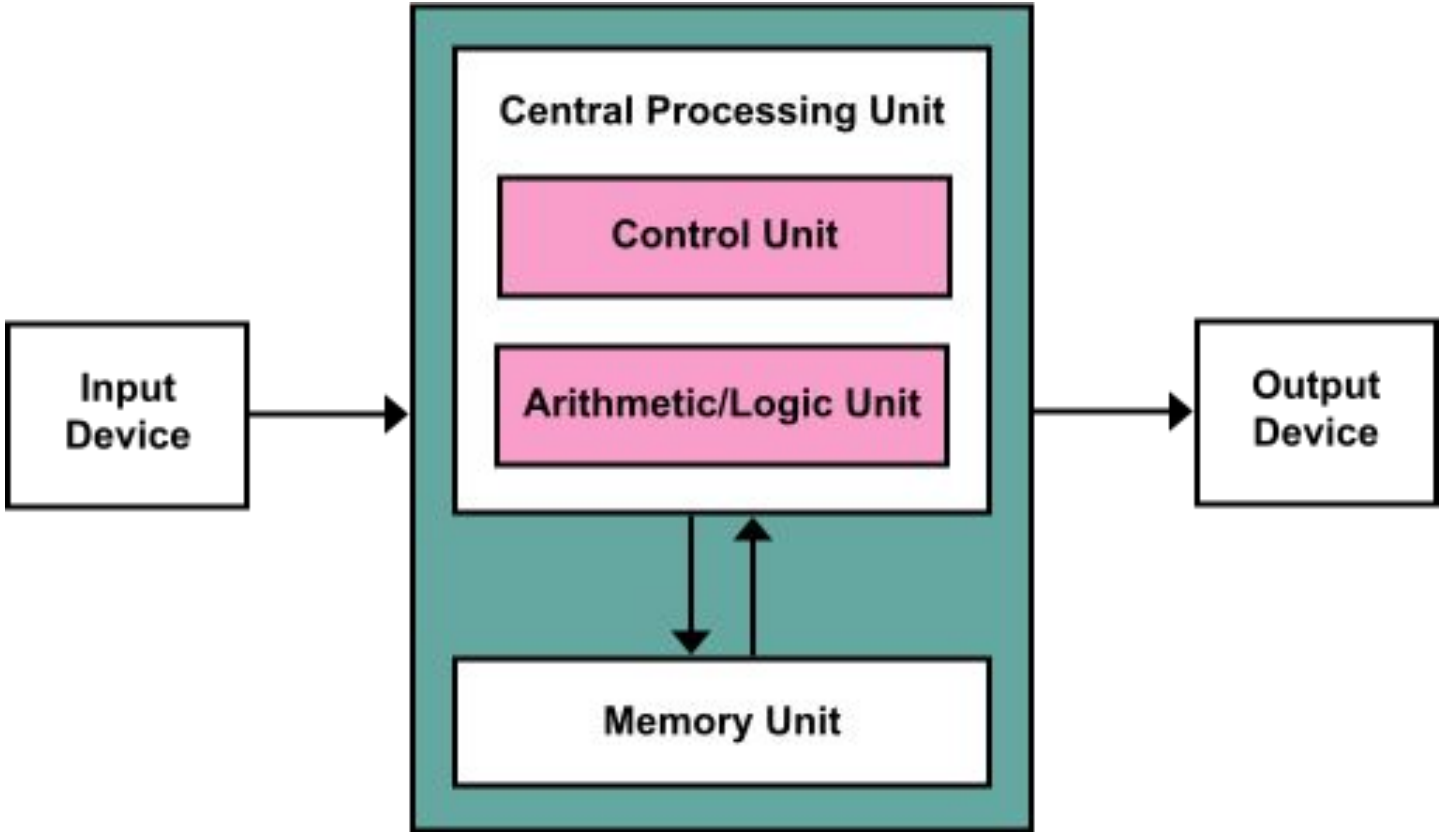
Fonte: www.caloni.com.br

Fonte: www.caloni.com.br/about

B1TFORGE



John... Von Neunmman... Newman... Neo!

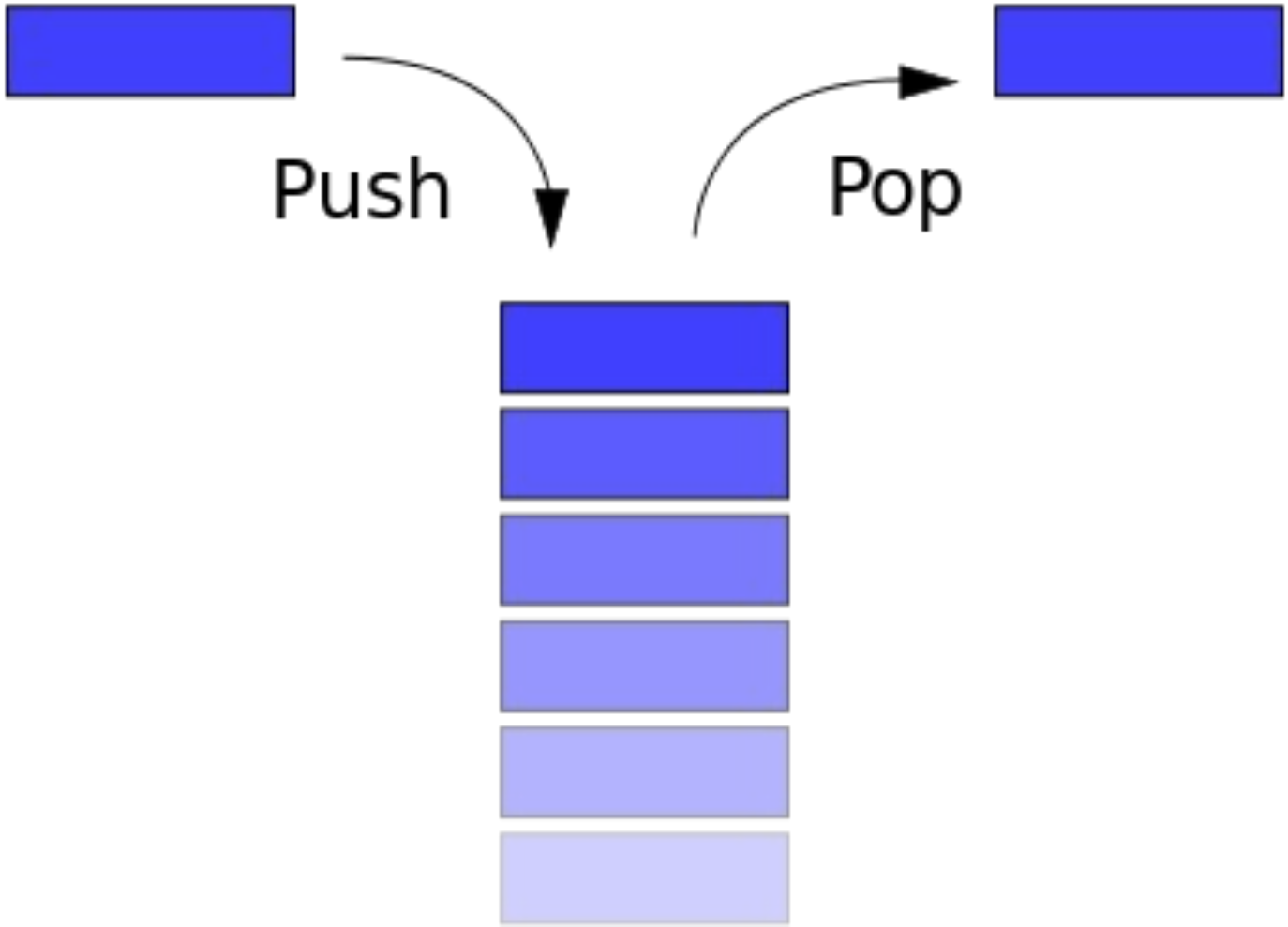


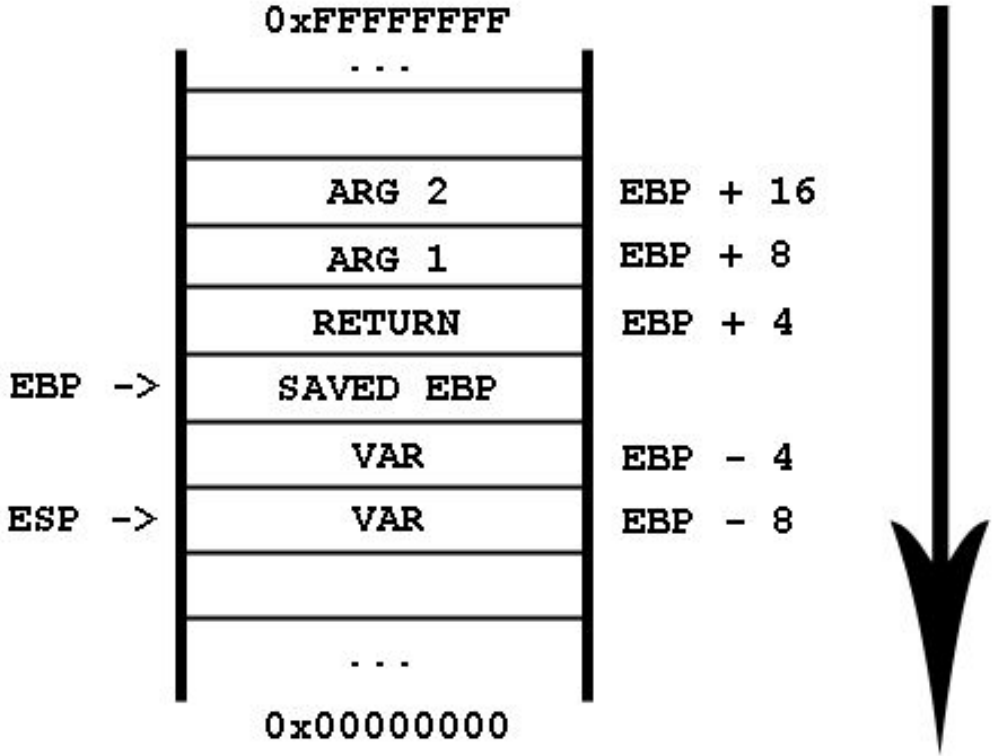
Neumann Architecture (a.k.a. The Matrix)

Self-modifying code [edit]

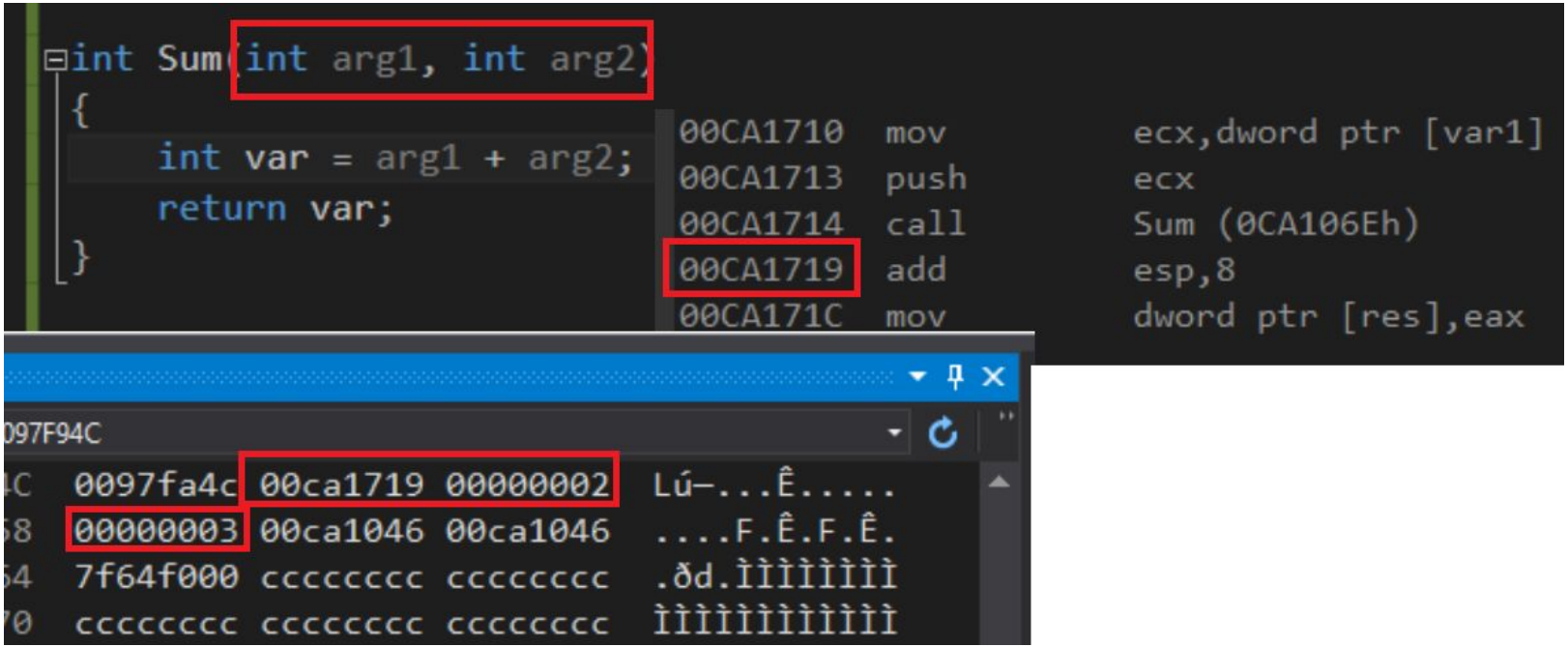
Aside from the von Neumann bottleneck, program modifications can be quite harmful, either by accident or design. In some simple stored-program computer designs, a malfunctioning program can damage itself, other programs, or the operating system, possibly leading to a computer crash. Memory protection and other forms of access control can usually protect against both accidental and malicious program modification.

Neumann Architecture (a.k.a. The Matrix)


Push
Pop

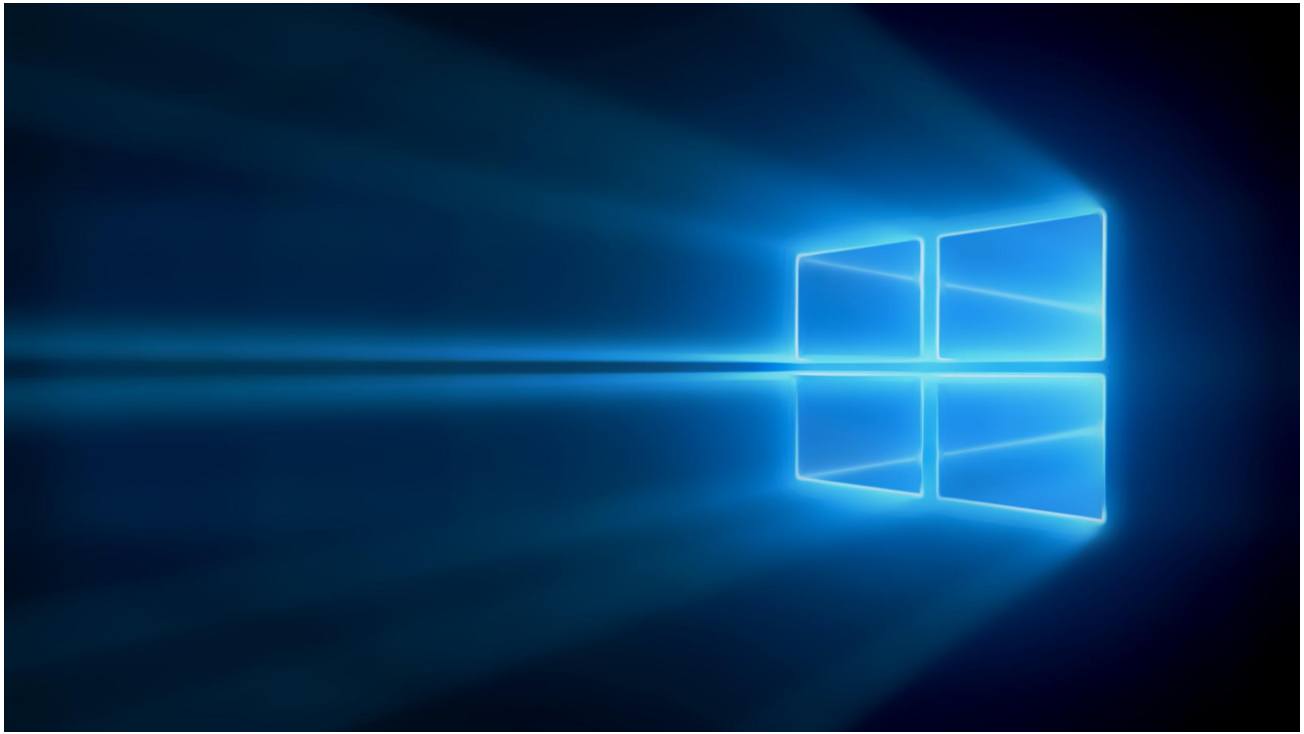

0xFFFFFFFF
...
ARG 2
EBP + 16
ARG 1
EBP + 8
RETURN
EBP + 4
EBP ->
SAVED EBP
VAR
EBP - 4
ESP ->
VAR
EBP - 8
...
0x00000000

Stack x86

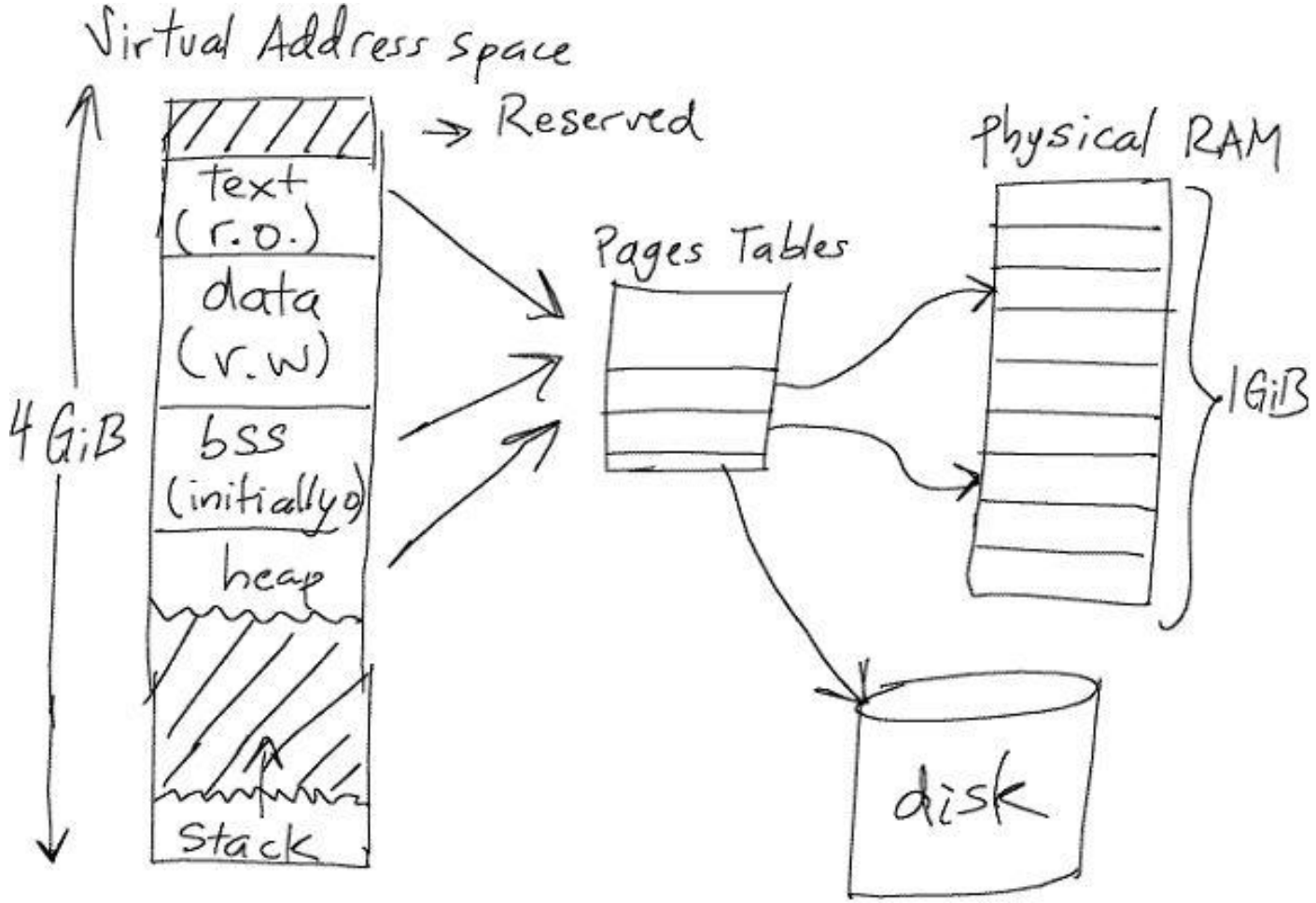

int Sum(int arg1, int arg2)
{
int var = arg1 + arg2;
return var;
}
00CA1710 mov ecx,dword ptr [var1]
00CA1713 push ecx
00CA1714 call Sum (0CA106Eh)
00CA1719 add esp,8
00CA171C mov dword ptr [res],eax
097F94C
0097fa4c 00ca1719 00000002 Lú–...Ê.....
00000003 00ca1046 00ca1046 ....F.Ê.F.Ê.
7f64f000 cccccccc cccccccc .ðd.ÌÌÌÌÌÌÌ
cccccccc cccccccc cccccccc ÌÌÌÌÌÌÌÌÌÌÌÌ

Stack x86

Is for dummies only



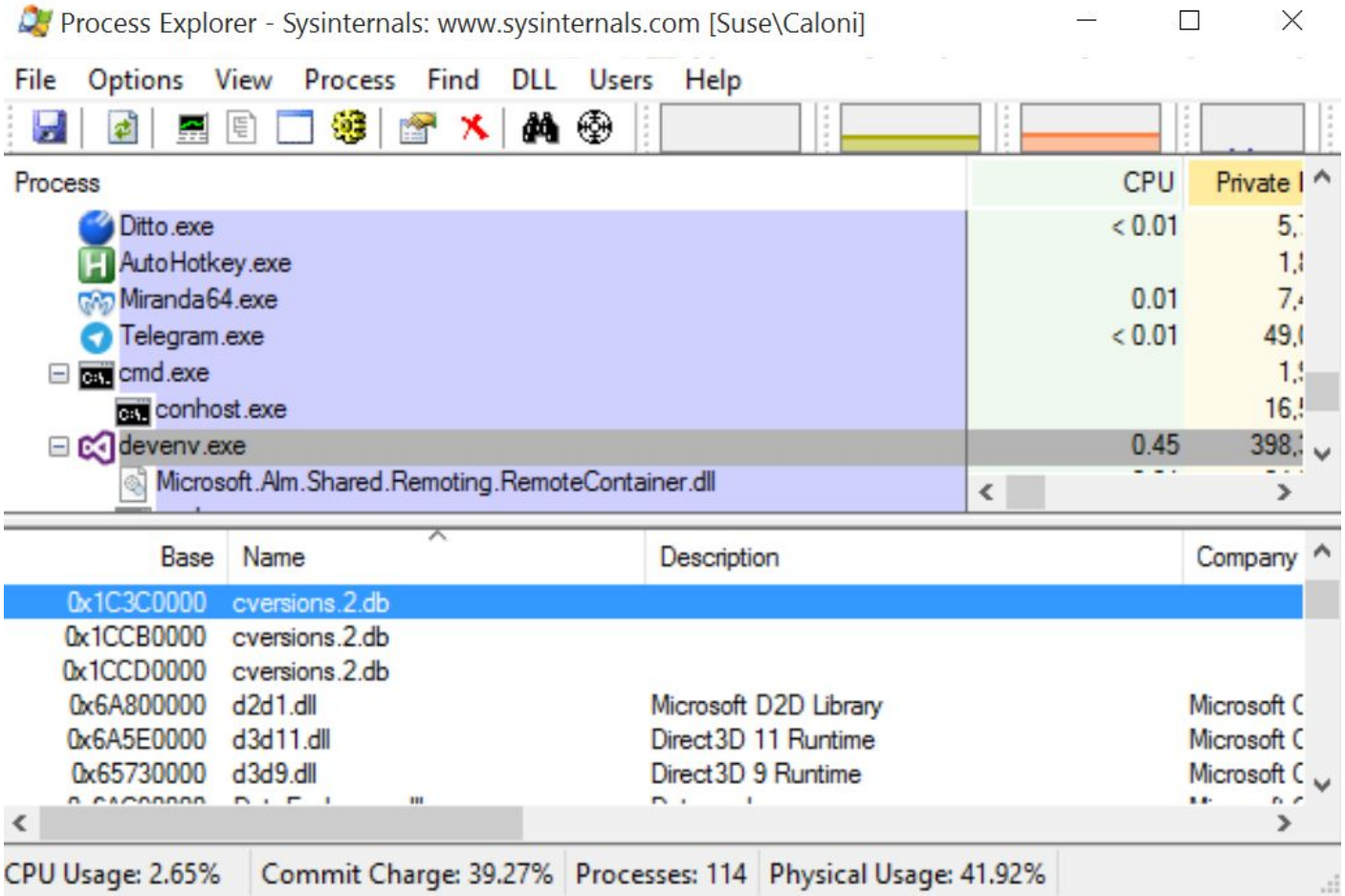
Talking about dummies...


Virtual Address space
Reserved
Physical RAM
text
(r.o.)
data
(r.w)
bss
(initially 0)
heap
Stack
4 GiB
Pages Tables
1 GiB
disk

Partes obscuras

Favor ler readme.md do projeto no GitHub [1]

[1] https://github.com/Caloni/StackOverflow


Process Explorer - Sysinternals: www.sysinternals.com [Suse\Caloni]
File Options View Process Find DLL Users Help
Process
CPU
Private
Ditto.exe
< 0.01
AutoHotkey.exe
Miranda64.exe
0.01
Telegram.exe
< 0.01
cmd.exe
conhost.exe
devenv.exe
0.45
Microsoft.Alm.Shared.Remoting.RemoteContainer.dll
Base
Name
Description
Company
0x1C3C0000 cversions.2.db
0x1CCB0000 cversions.2.db
0x1CCD0000 cversions.2.db
0x6A800000 d2d1.dll
Microsoft D2D Library
0x6A5E0000 d3d11.dll
Direct3D 11 Runtime
0x65730000 d3d9.dll
Direct3D 9 Runtime
CPU Usage: 2.65%
Commit Charge: 39.27%
Processes: 114
Physical Usage: 41.92%

B1TFORGE