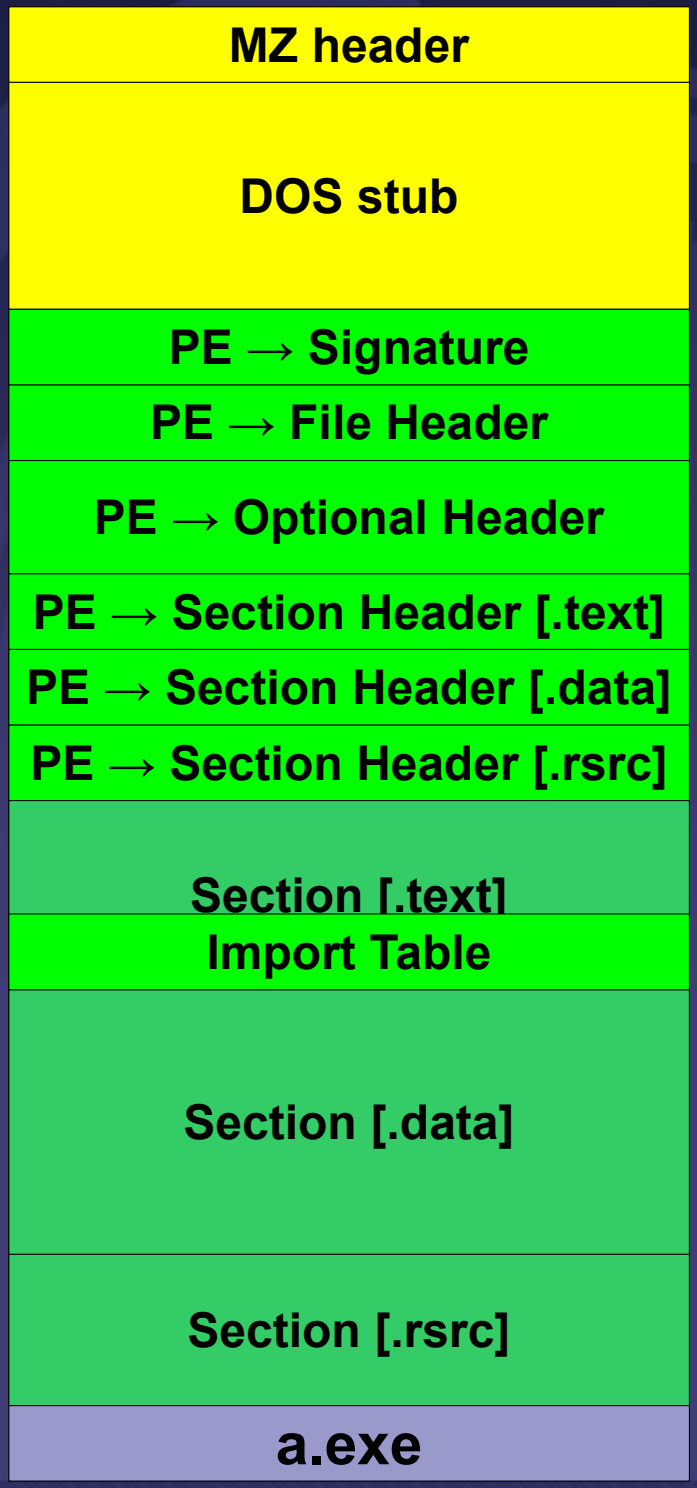
ReverseCraft

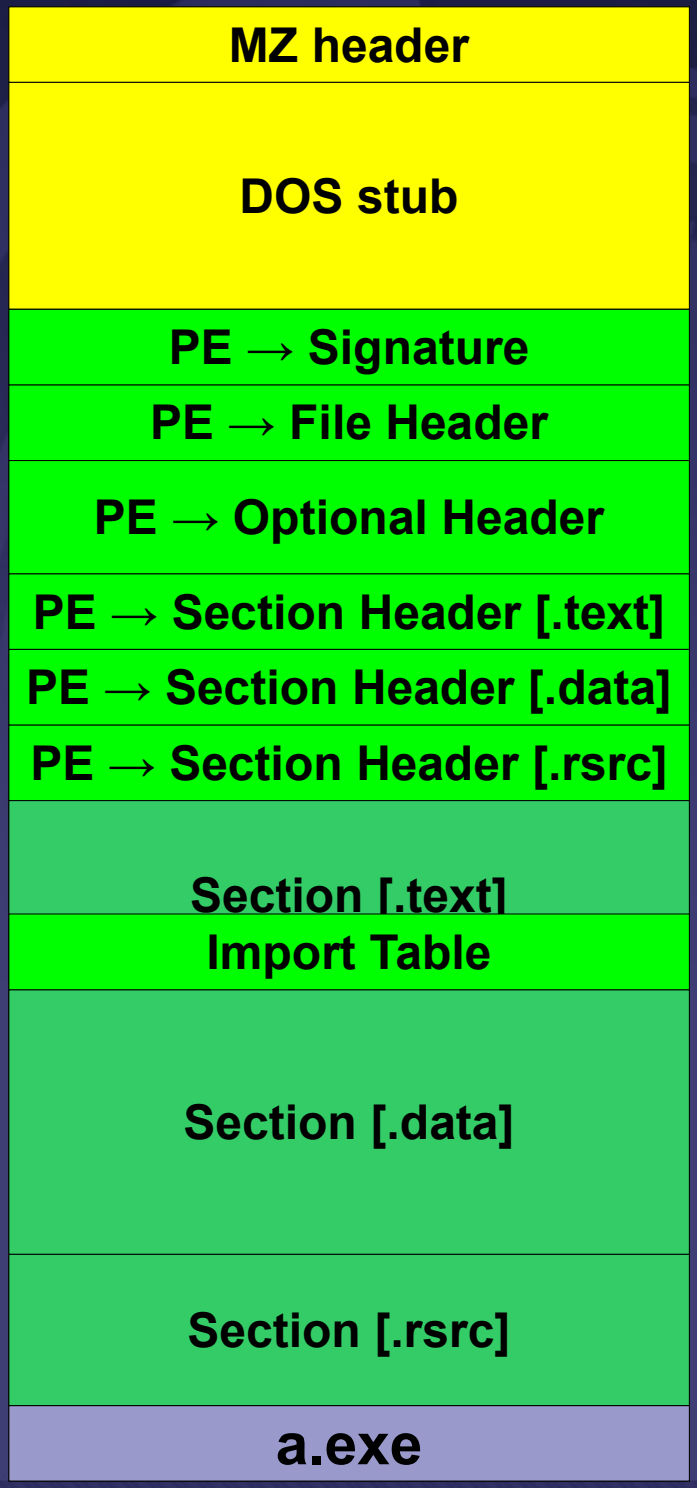
by gynvael.coldwind//vx

003 – Pamięć, proces i PE

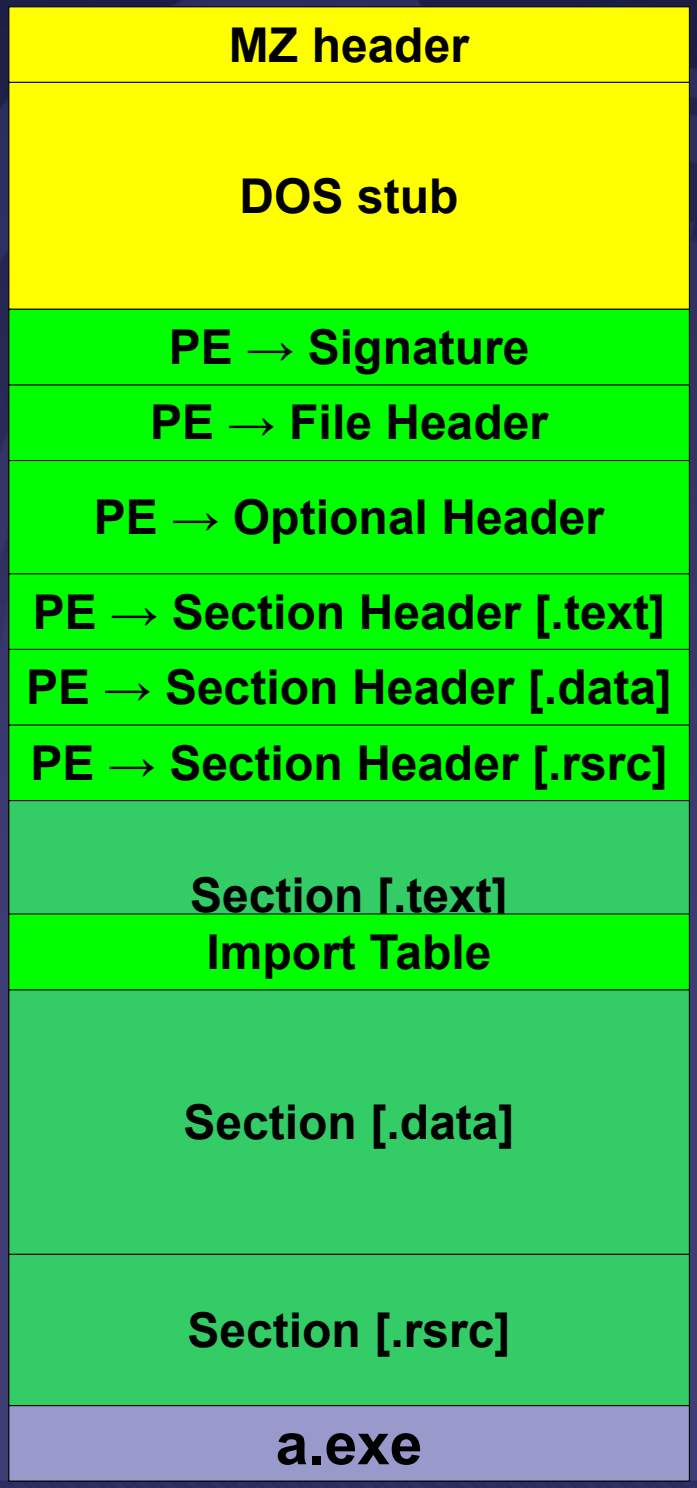
Strony projektu:

http://re.coldwind.pl/
http://www.uw-team.org/

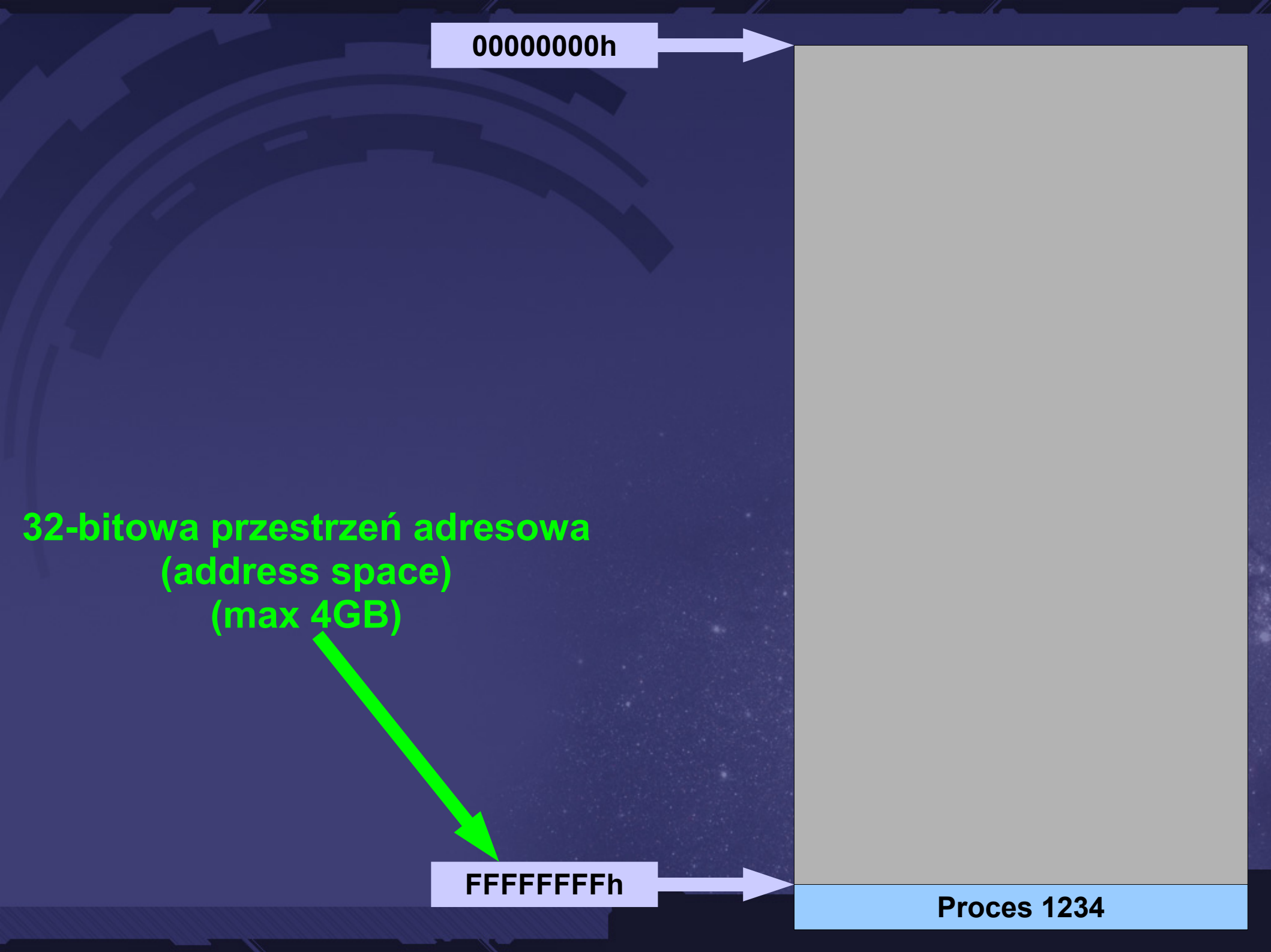

MZ header
DOS stub
PE → Signature
PE → File Header
PE → Optional Header
PE → Section Header [.text]
PE → Section Header [.data]
PE → Section Header [.rsrc]
Section [.text]
Import Table
Section [.data]
Section [.rsrc]
a.exe


MZ header
DOS stub
PE → Signature
PE → File Header
PE → Optional Header
PE → Section Header [.text]
PE → Section Header [.data]
PE → Section Header [.rsrc]
Section [.text]
Import Table
Section [.data]
Section [.rsrc]
a.exe

Proces 1234


MZ header
DOS stub
PE → Signature
PE → File Header
PE → Optional Header
PE → Section Header [.text]
PE → Section Header [.data]
PE → Section Header [.rsrc]
Section [.text]
Import Table
Section [.data]
Section [.rsrc]
a.exe

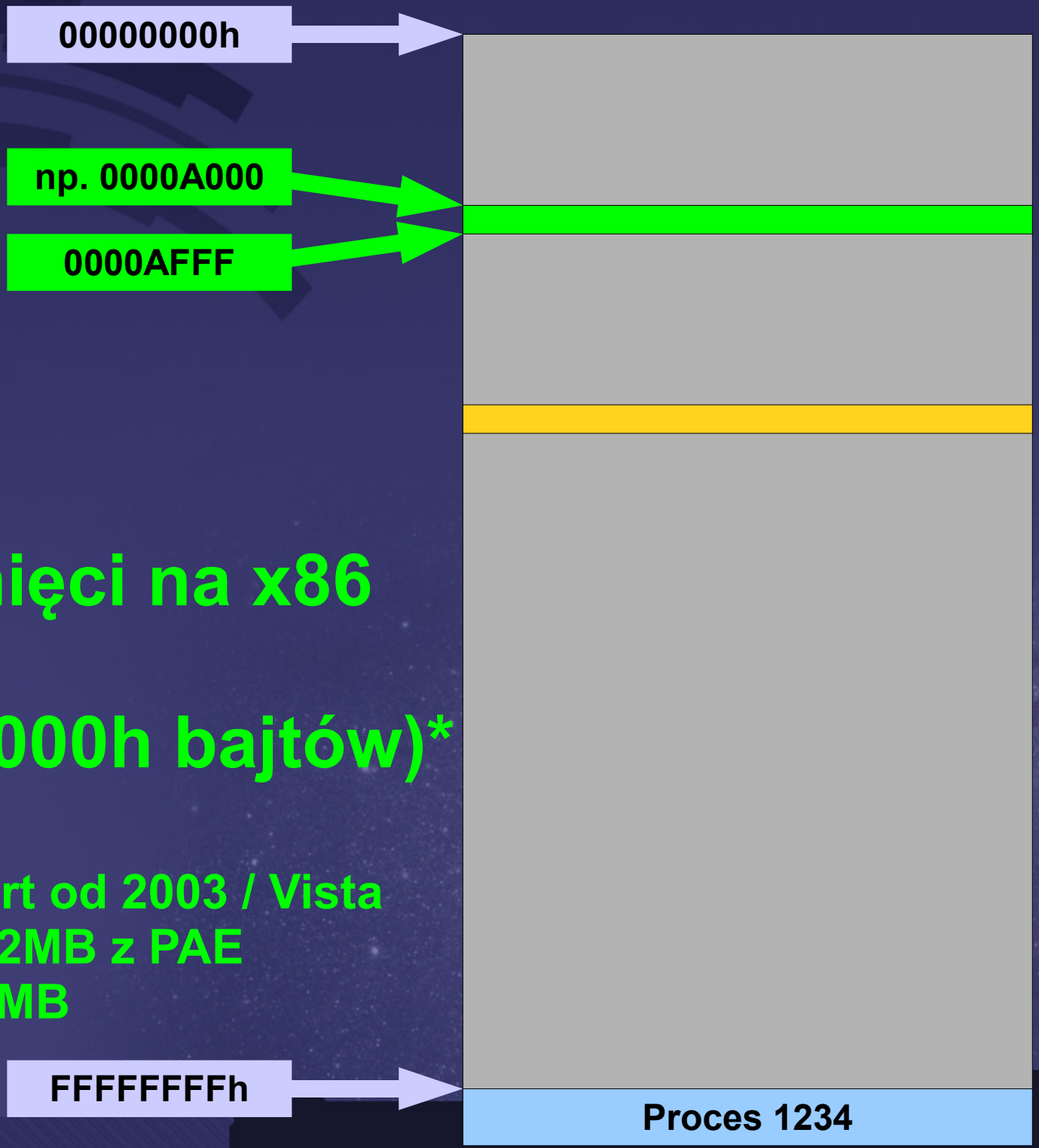

PROCESS
VIRTUAL
SPACE
Proces 1234


00000000h
32-bitowa przestrzeń adresowa
(address space)
(max 4GB)
FFFFFFFFh
Proces 1234

„Zamapowana” strona

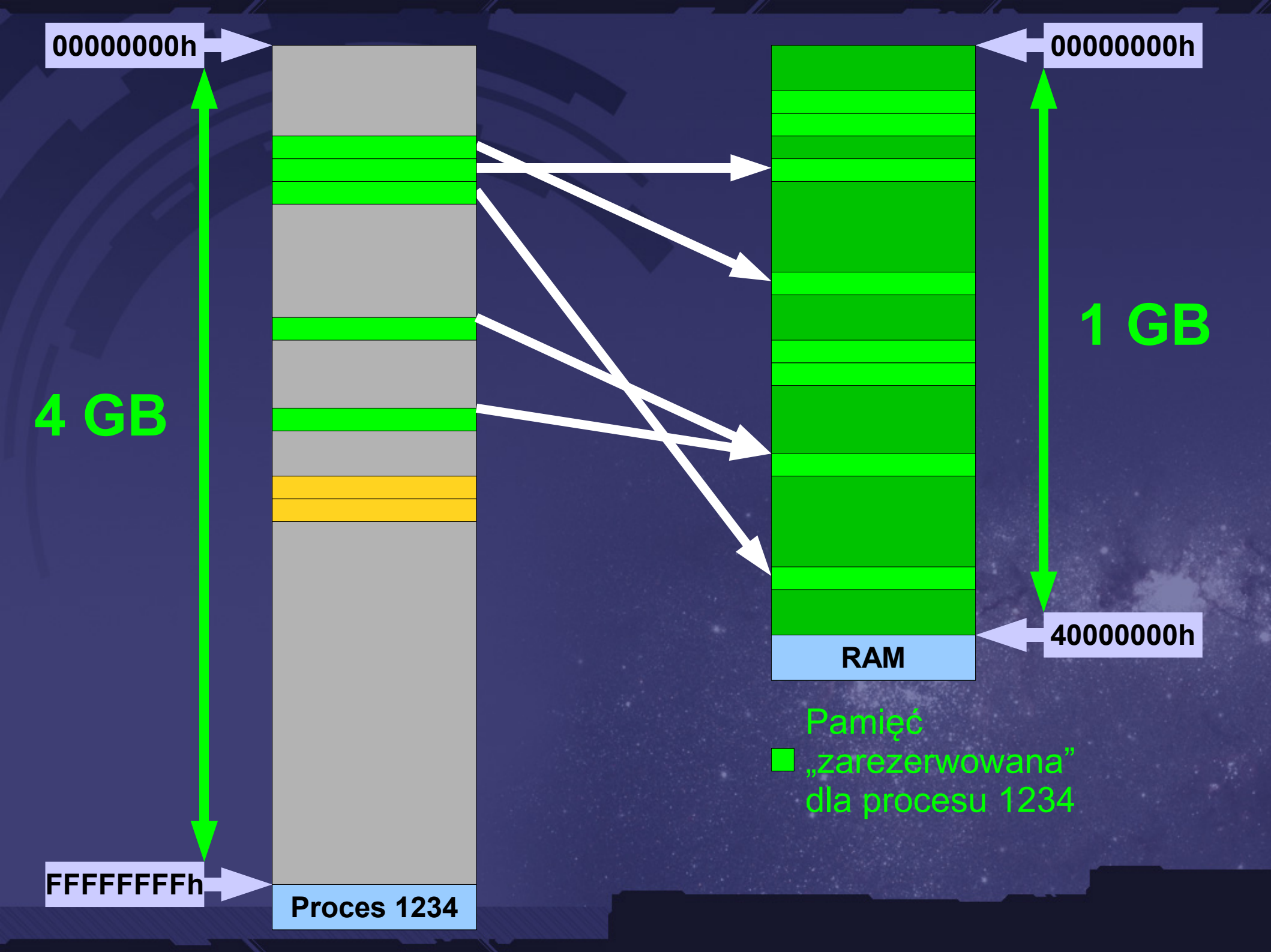
Strona nieistniejąca

Strona zarezerwowana



1 strona pamięci na x86 to 4096 bajtów (1000h bajtów)*

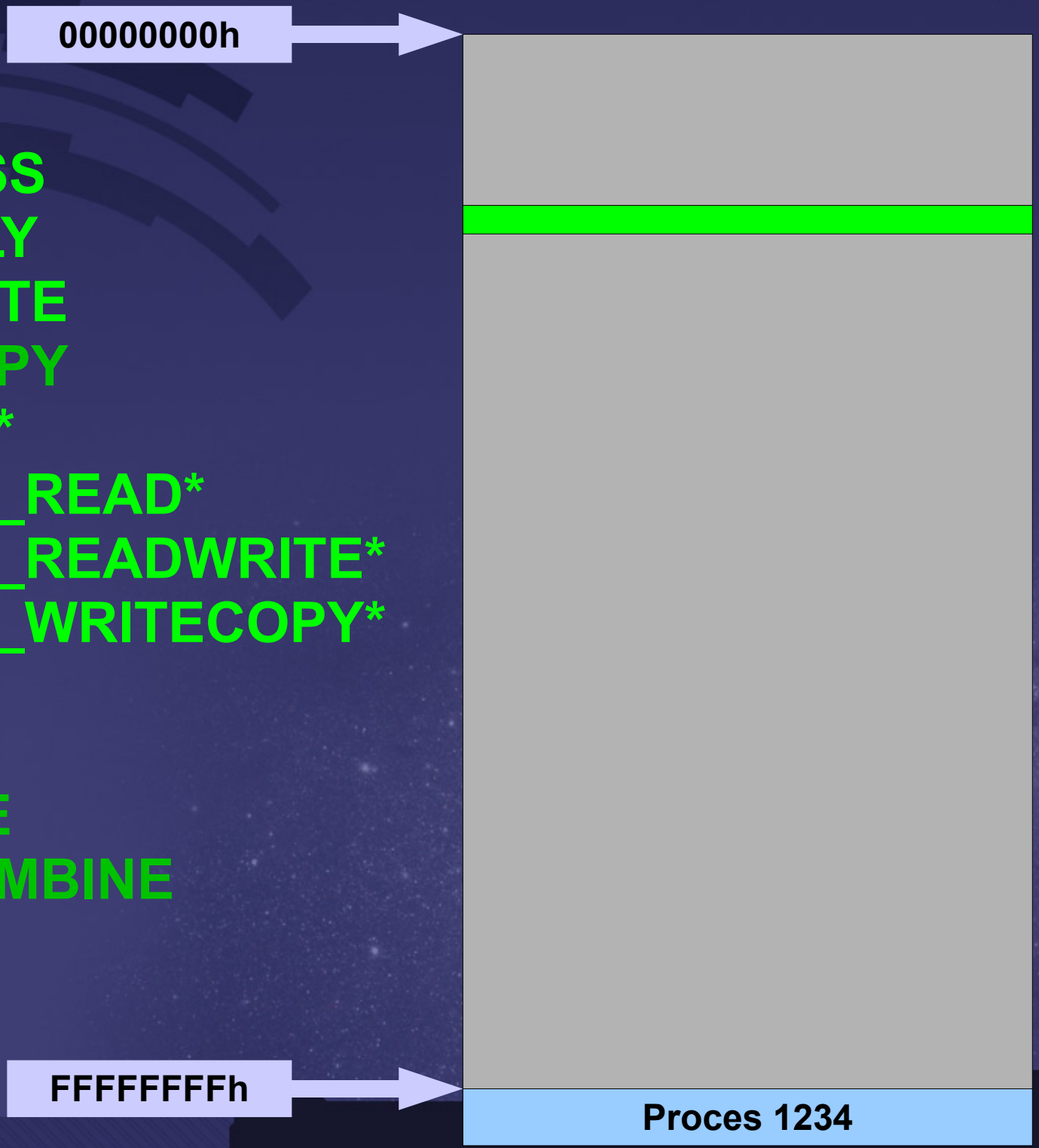
*** Large Page Support od 2003 / Vista**
x86: 4MB lub 2MB z PAE
x64: 2MB

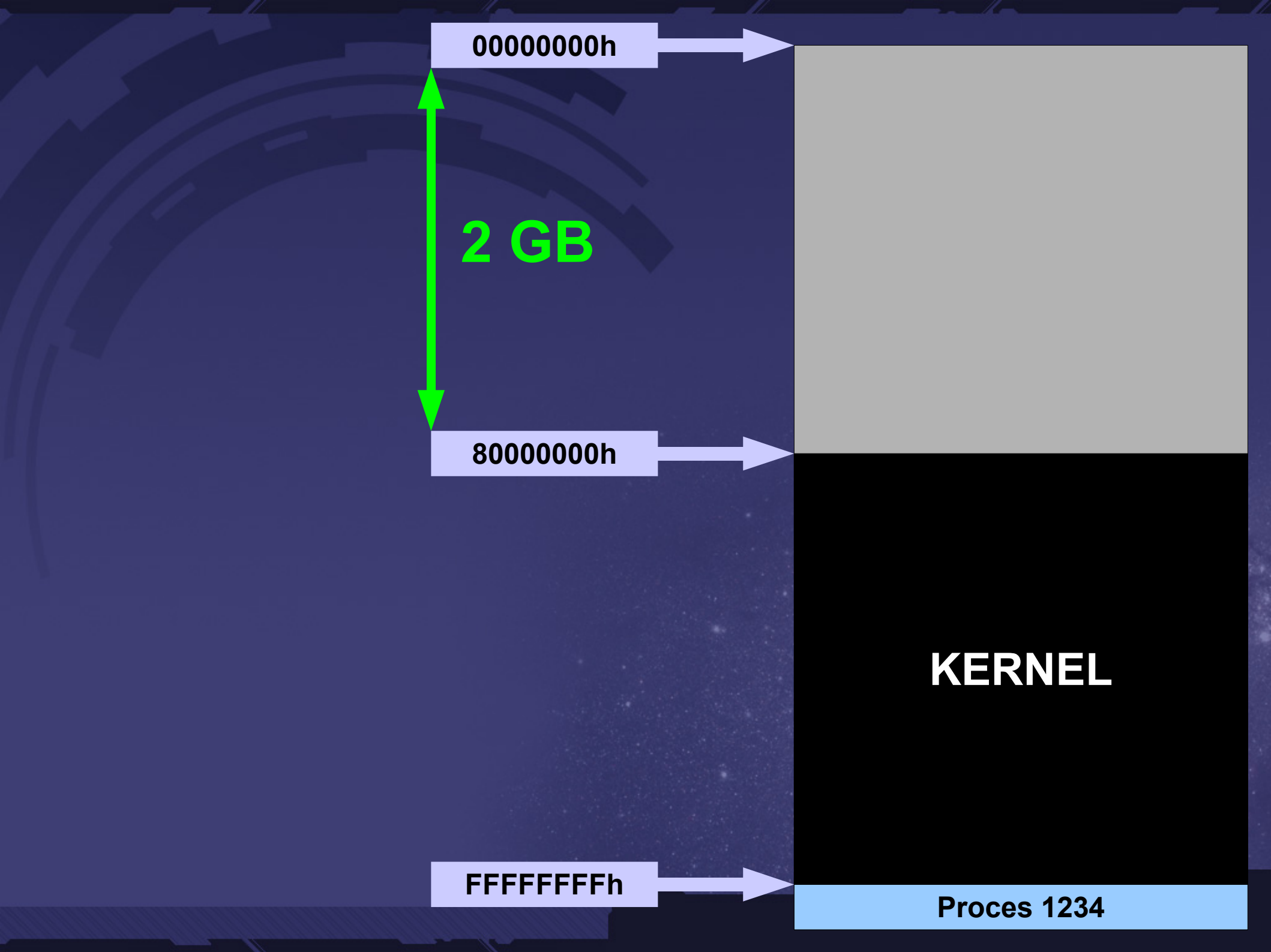

00000000h
FFFFFFFFh
4 GB
Proces 1234
00000000h
40000000h
1 GB
RAM
Pamięć
„zarezerwowana”
dla procesu 1234

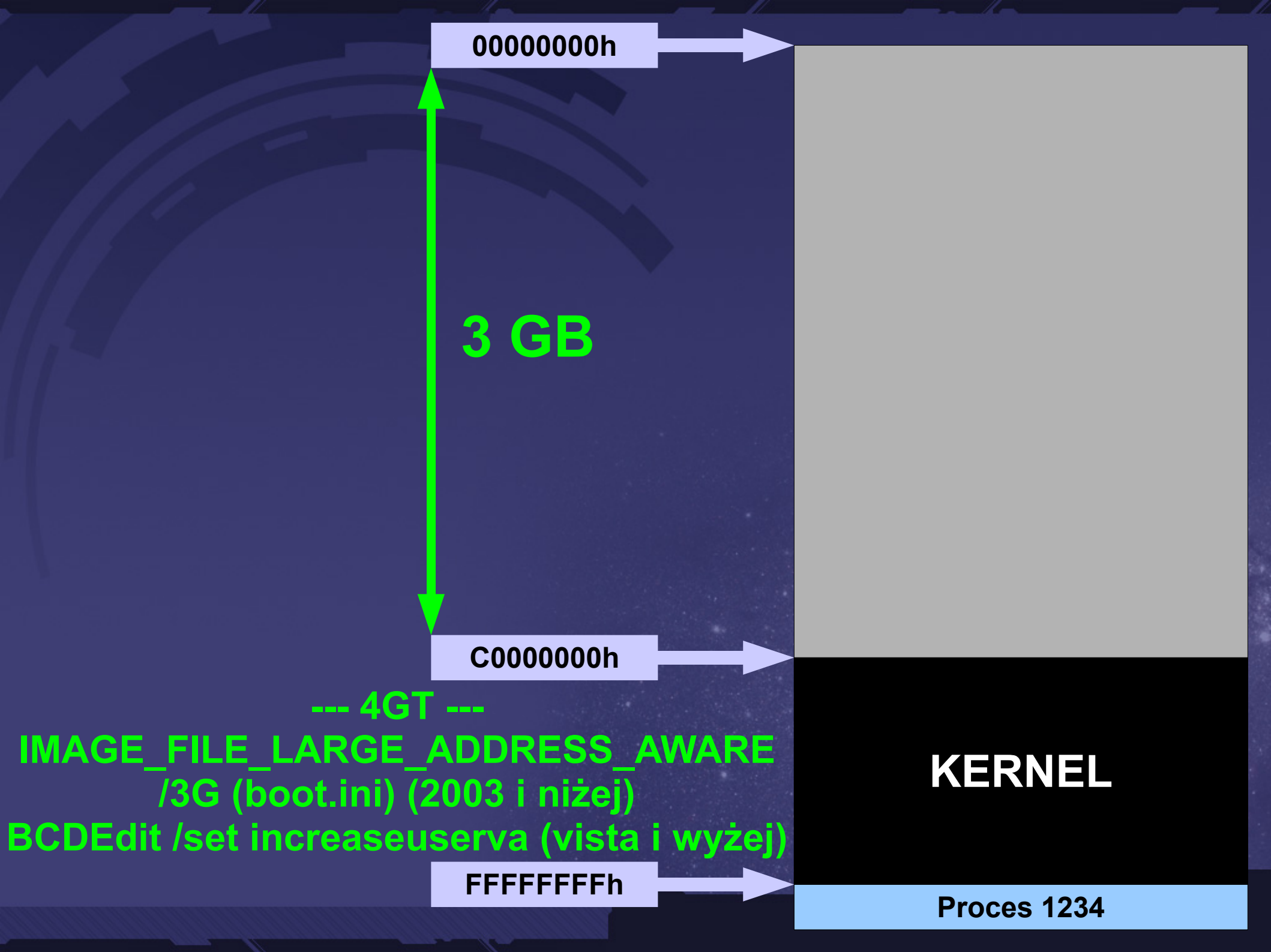
PAGE_NOACCESS
PAGE_READONLY
PAGE_READWRITE
PAGE_WRITECOPY
PAGE_EXECUTE*
PAGE_EXECUTE_READ*
PAGE_EXECUTE_READWRITE*
PAGE_EXECUTE_WRITECOPY*

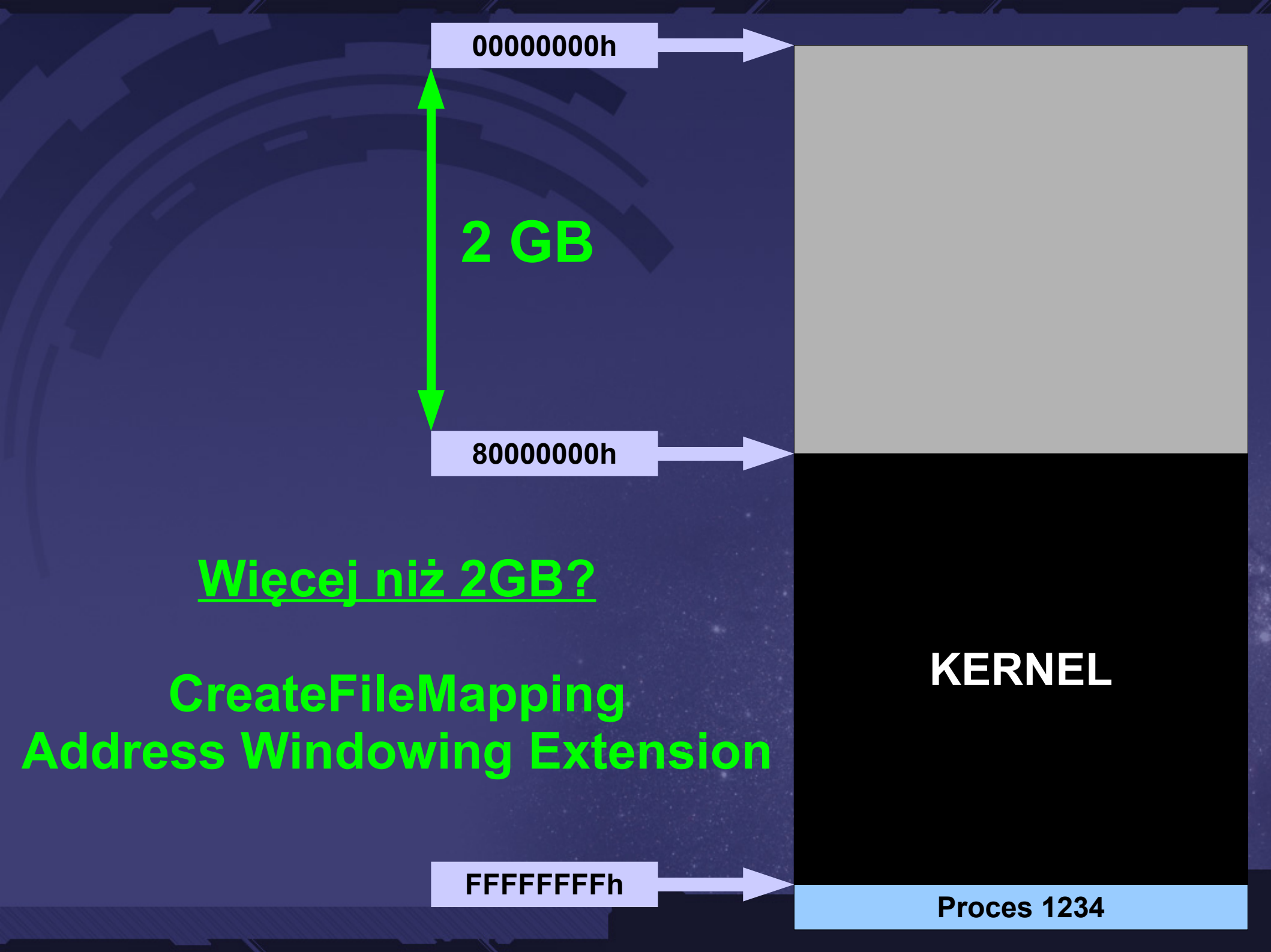
PAGE_GUARD
PAGE_NOCACHE
PAGE_WRITECOMBINE

* DEP, XD, NX



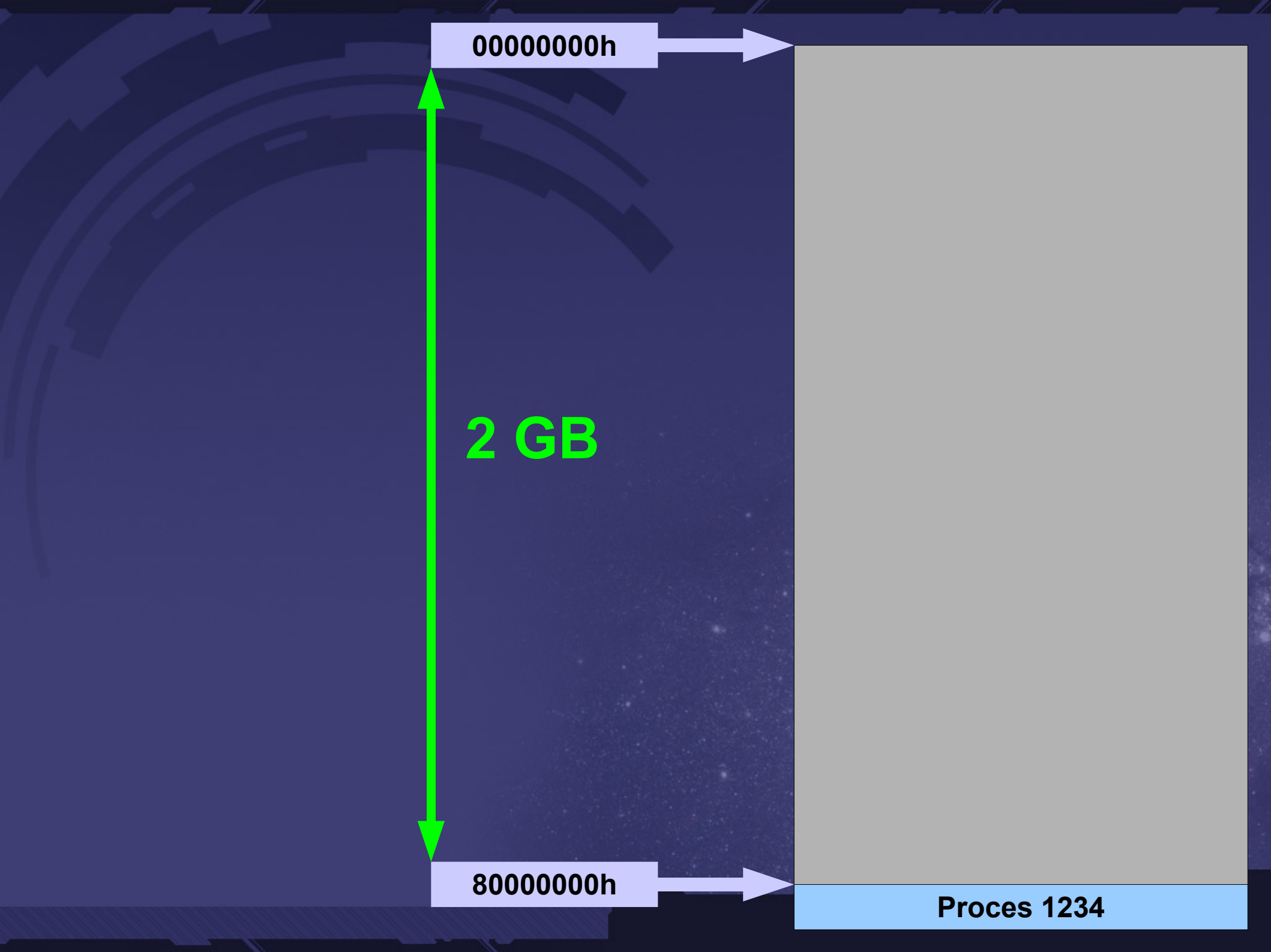

00000000h
2 GB
80000000h
KERNEL
FFFFFFFFh
Proces 1234


00000000h
3 GB
C0000000h
--- 4GT ---
IMAGE_FILE_LARGE_ADDRESS_AWARE
/3G (boot.ini) (2003 i niżej)
BCDEdit /set increaseuserva (vista i wyżej)
FFFFFFFFh
KERNEL
Proces 1234



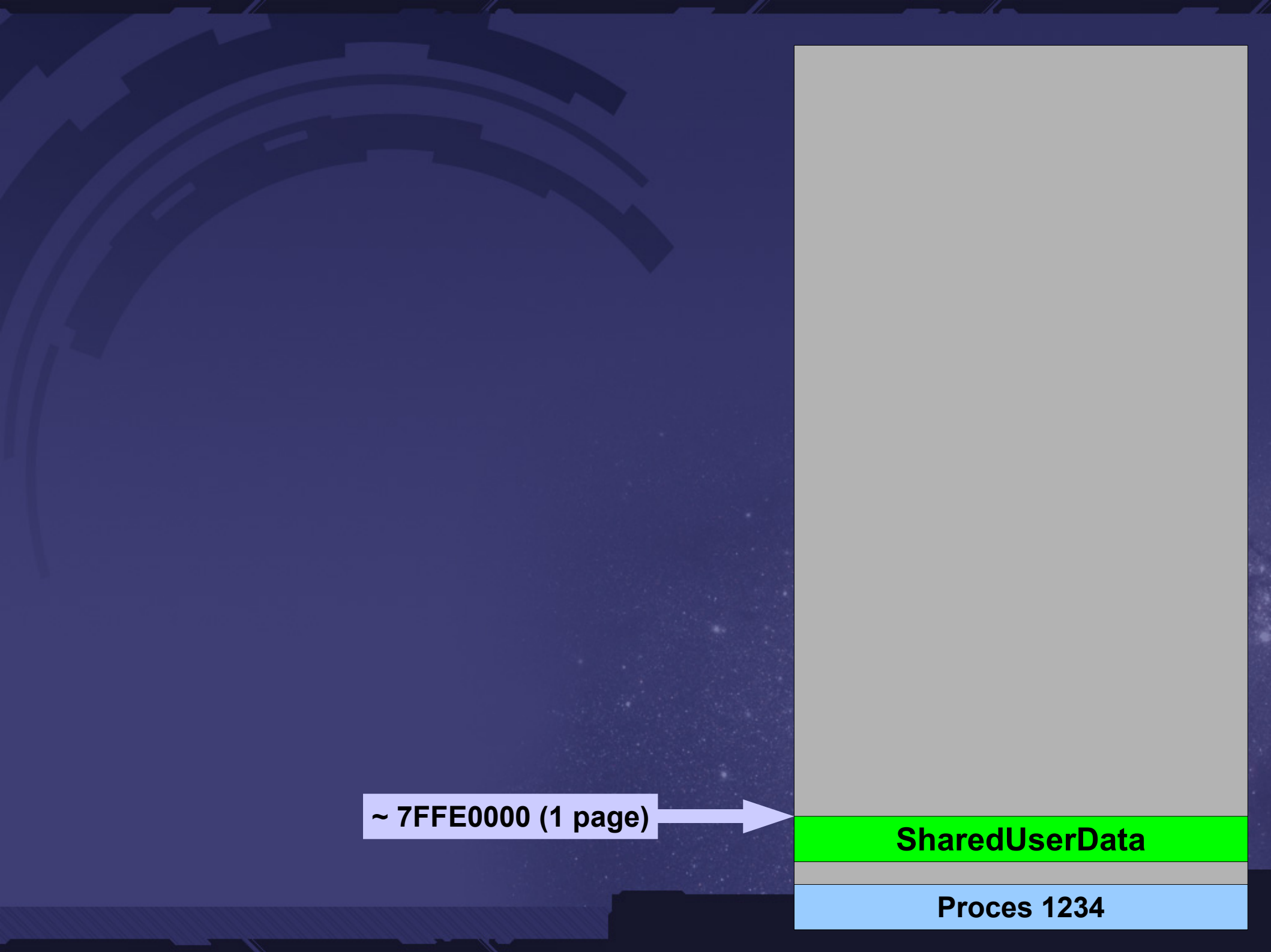
Więcej niż 2GB?

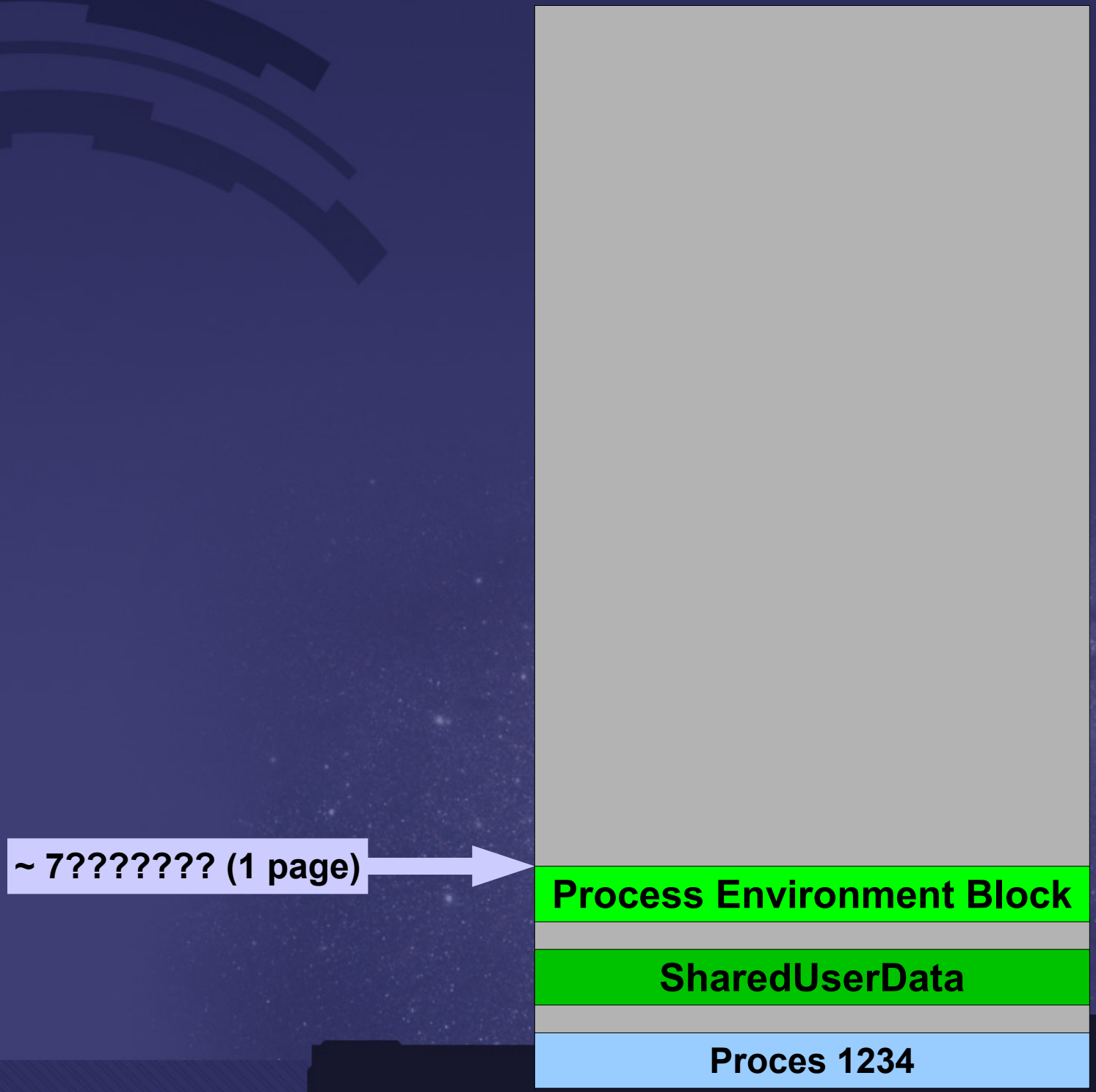
CreateFileMapping
Address Windowing Extension

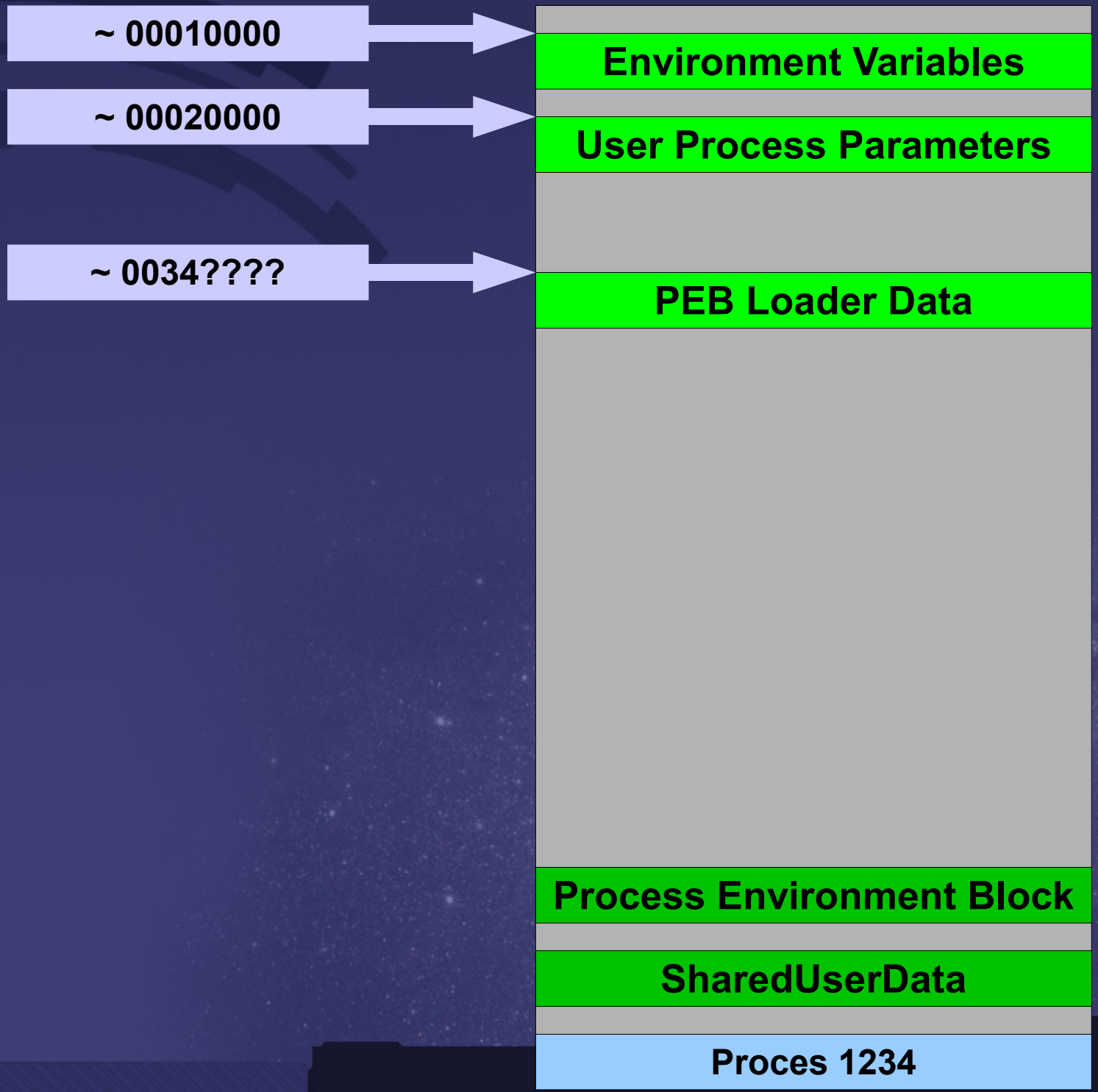

00000000h
2 GB
80000000h
Proces 1234

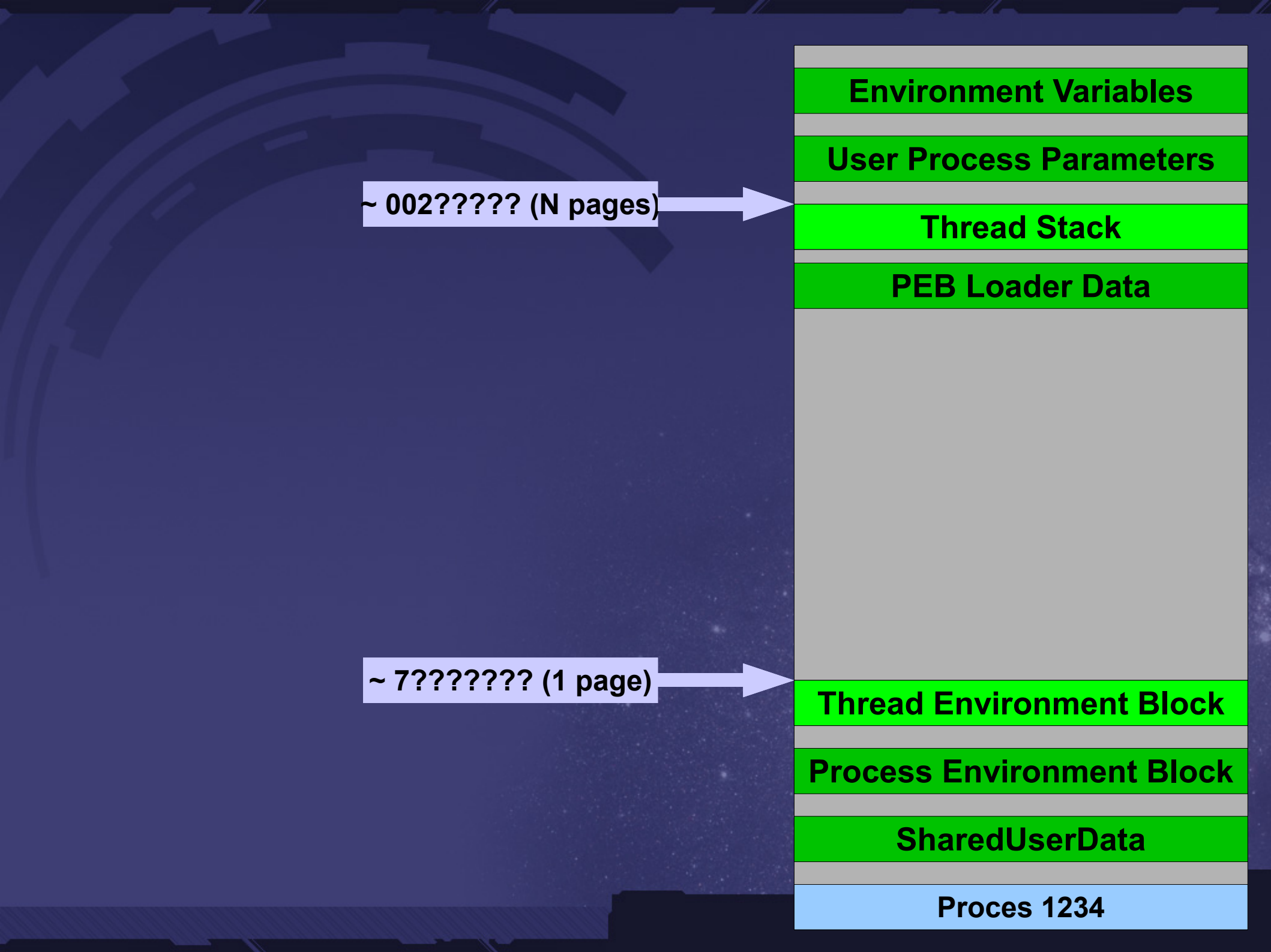
PROCESS VIRTUAL SPACE

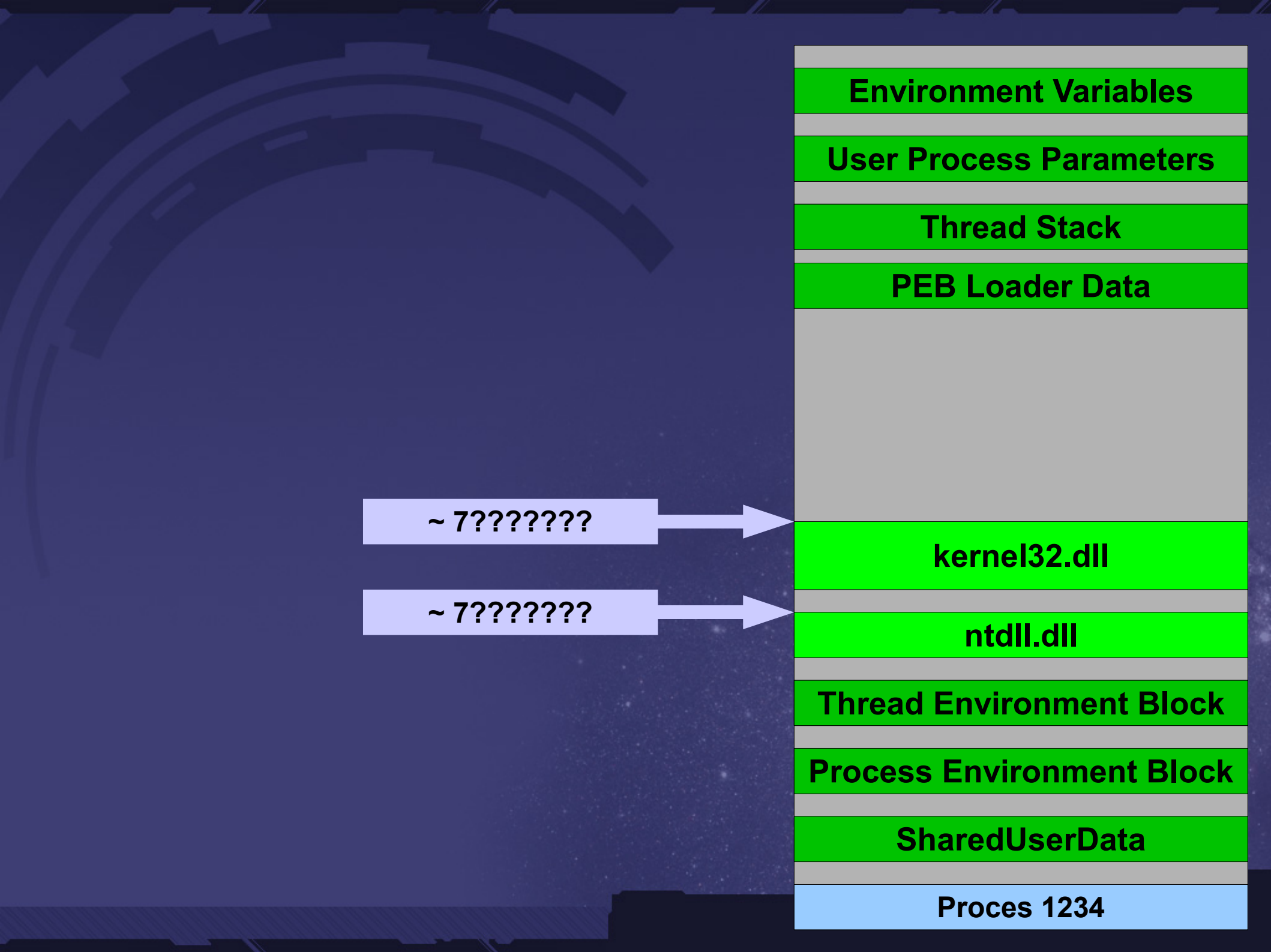
Proces 1234

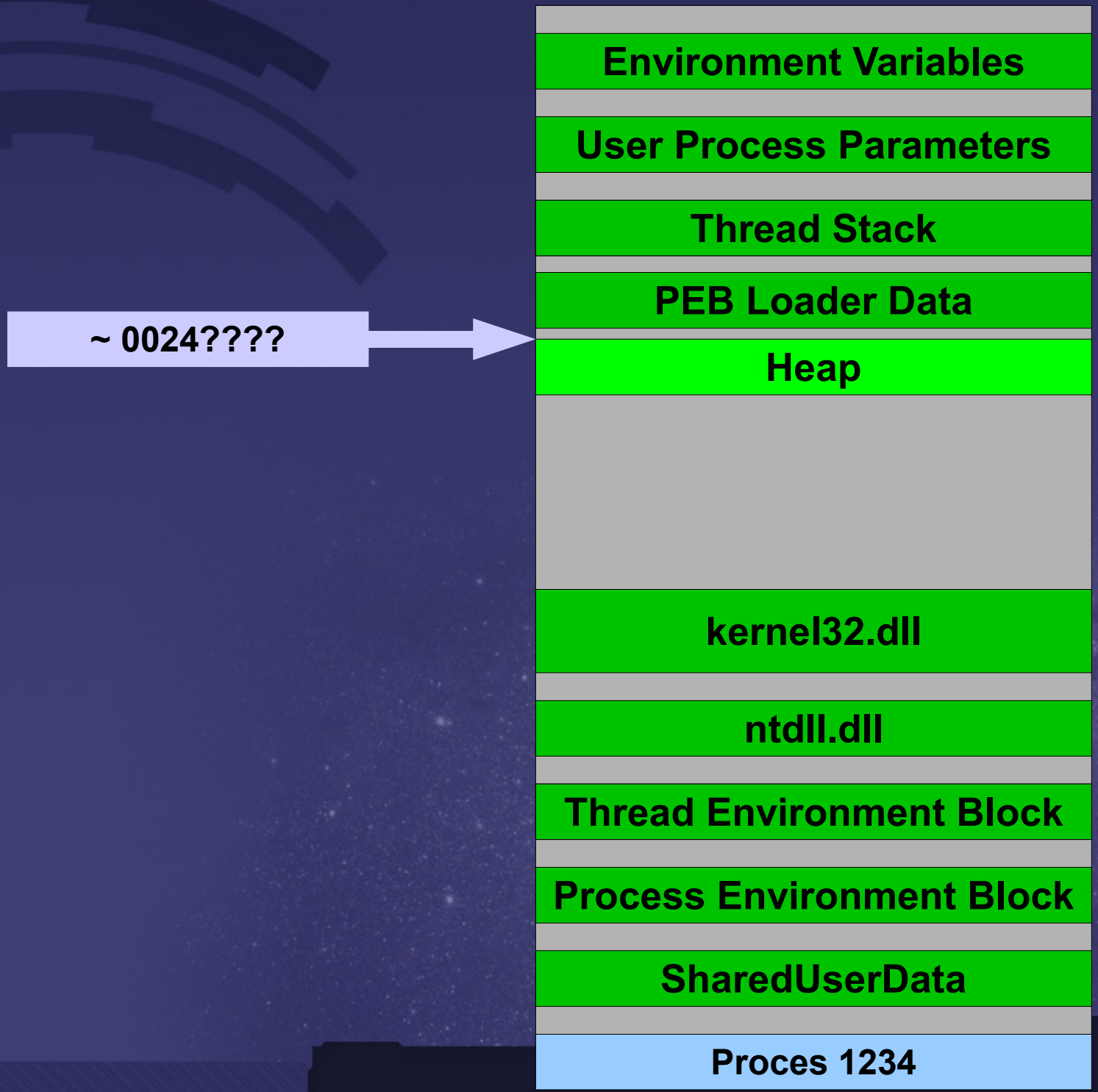

~ 7FFE0000 (1 page)
SharedUserData
Proces 1234


~ 7??????? (1 page)
Process Environment Block
SharedUserData
Proces 1234


~ 00010000
~ 00020000
~ 0034????
Environment Variables
User Process Parameters
PEB Loader Data
Process Environment Block
SharedUserData
Proces 1234


Environment Variables
User Process Parameters
~ 002????? (N pages)
Thread Stack
PEB Loader Data
~ 7??????? (1 page)
Thread Environment Block
Process Environment Block
SharedUserData
Proces 1234


Environment Variables
User Process Parameters
Thread Stack
PEB Loader Data
~ 7???????
kernel32.dll
~ 7???????
ntdll.dll
Thread Environment Block
Process Environment Block
SharedUserData
Proces 1234


~ 0024????
Environment Variables
User Process Parameters
Thread Stack
PEB Loader Data
Heap
kernel32.dll
ntdll.dll
Thread Environment Block
Process Environment Block
SharedUserData
Proces 1234


MZ header
DOS stub
PE → Signature
PE → File Header
PE → Optional Header
PE → Section Header [.text]
PE → Section Header [.data]
PE → Section Header [.rsrc]
Section [.text]
Import Table
Section [.data]
Section [.rsrc]
a.exe
Environment Variables
User Process Parameters
Thread Stack
PEB Loader Data
Heap
kernel32.dll
ntdll.dll
Thread Environment Block
Process Environment Block
SharedUserData
Proces 1234

VA – (Linear) Virtual Address

np. PE.OptionalHeader.ImageBase 0x00400000 lub 0x01000000

VA – (Linear) Virtual Address
np. PE.OptionalHeader.ImageBase
0x00400000 lub 0x01000000

RVA – Relative Virtual Address
np. PE.SectionHeader[.text].VirtualAddress

RVA → VA: VA(RVA) = ImageBase + RVA
VA → RVA: RVA(VA) = VA – ImageBase

To jest ImageBase modułu do którego dane RVA się odnosi!

RAW lub Offset – File Offset

np.

PE.SectionHeader[.text].PointerToRawData

RVA → RAW:

1. Znajdź sekcję w której RVA się zawiera:

RVA >= Sec.VirtualAddress &&

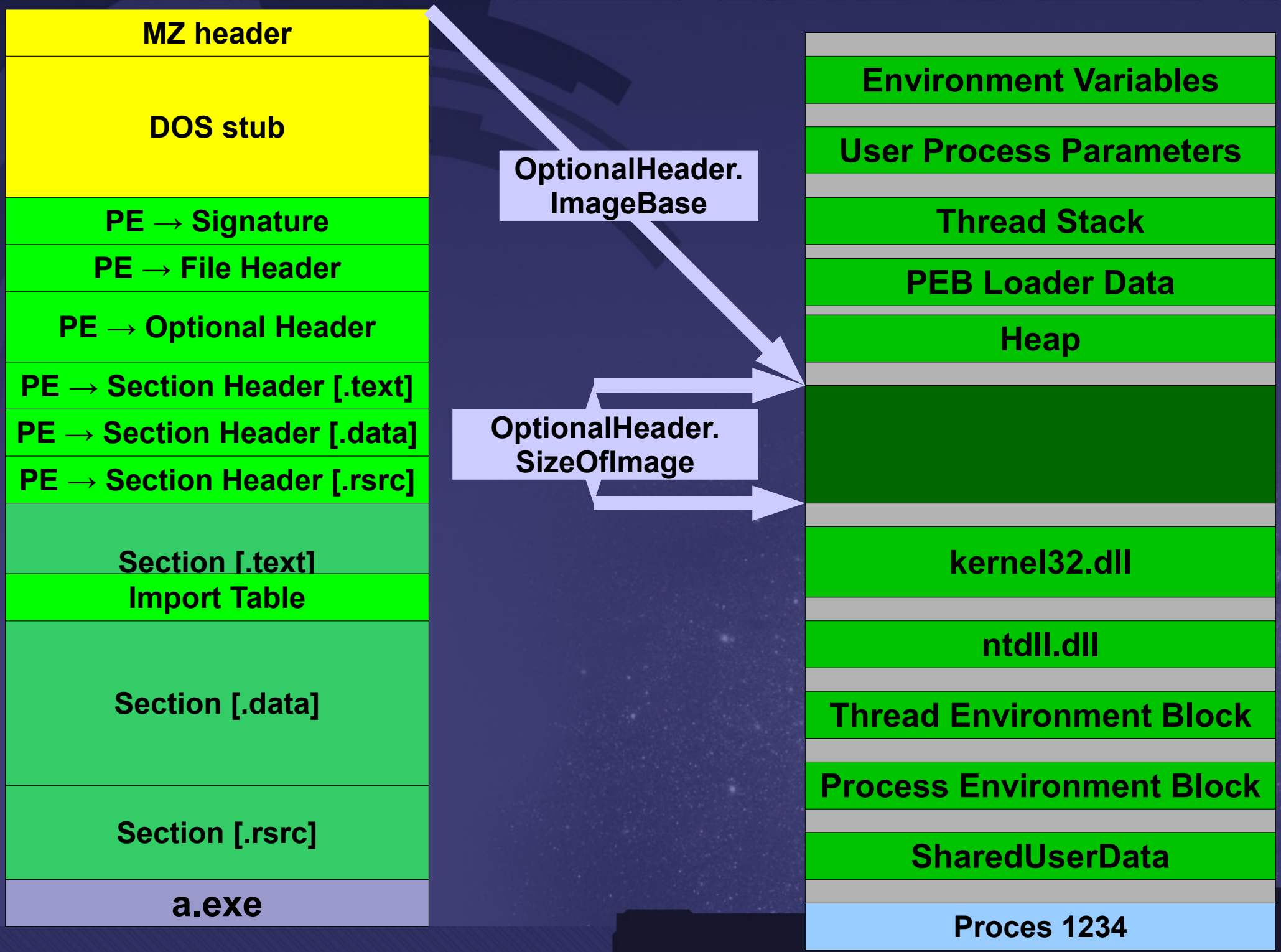
RVA < Sec.VirtualAddress +

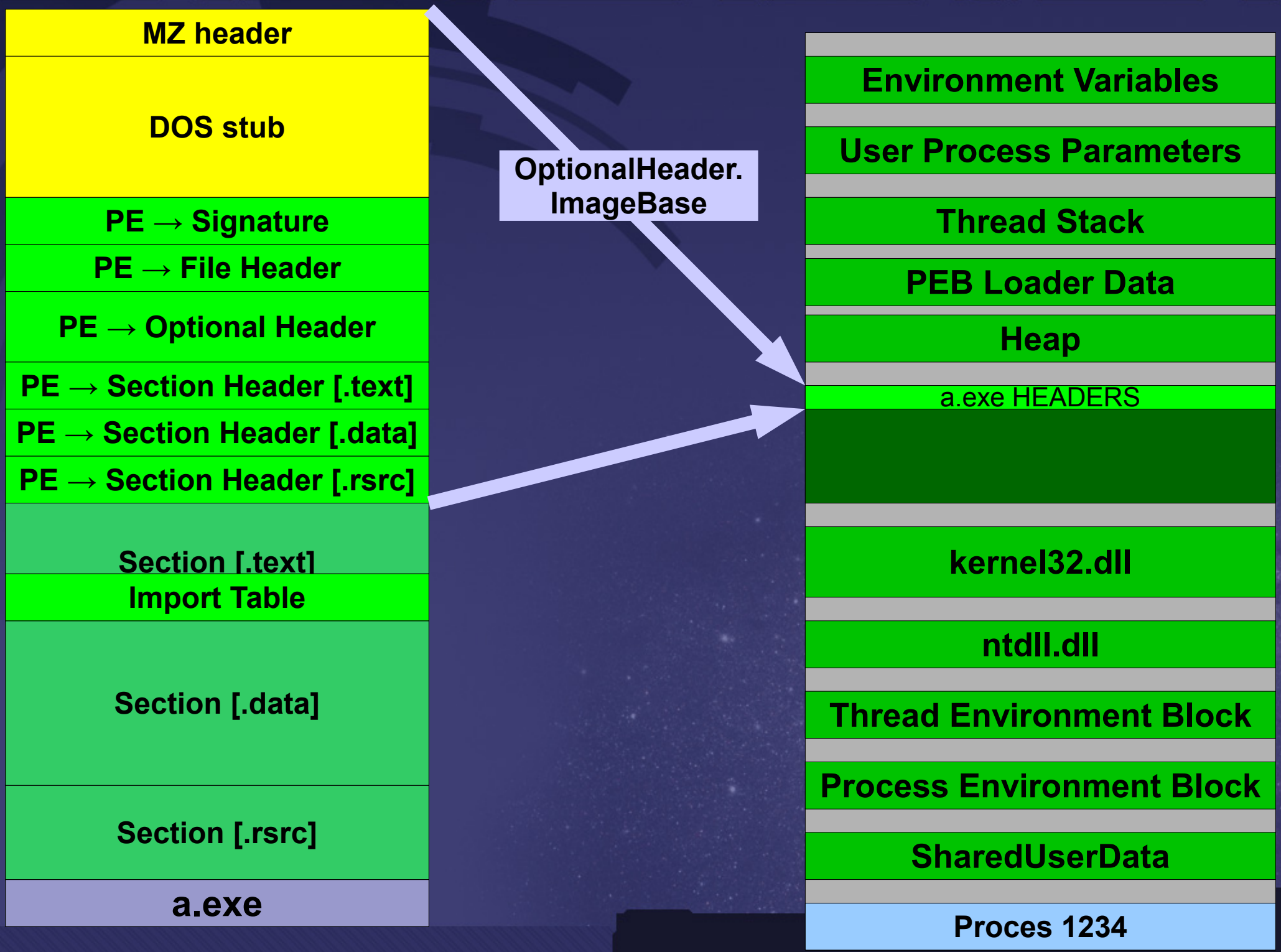
Sec.Misc.VirtualSize

2. Oblicz:

RAW(RVA) = RVA – Sec.VirtualAddress +

Sec.PointerToRawData

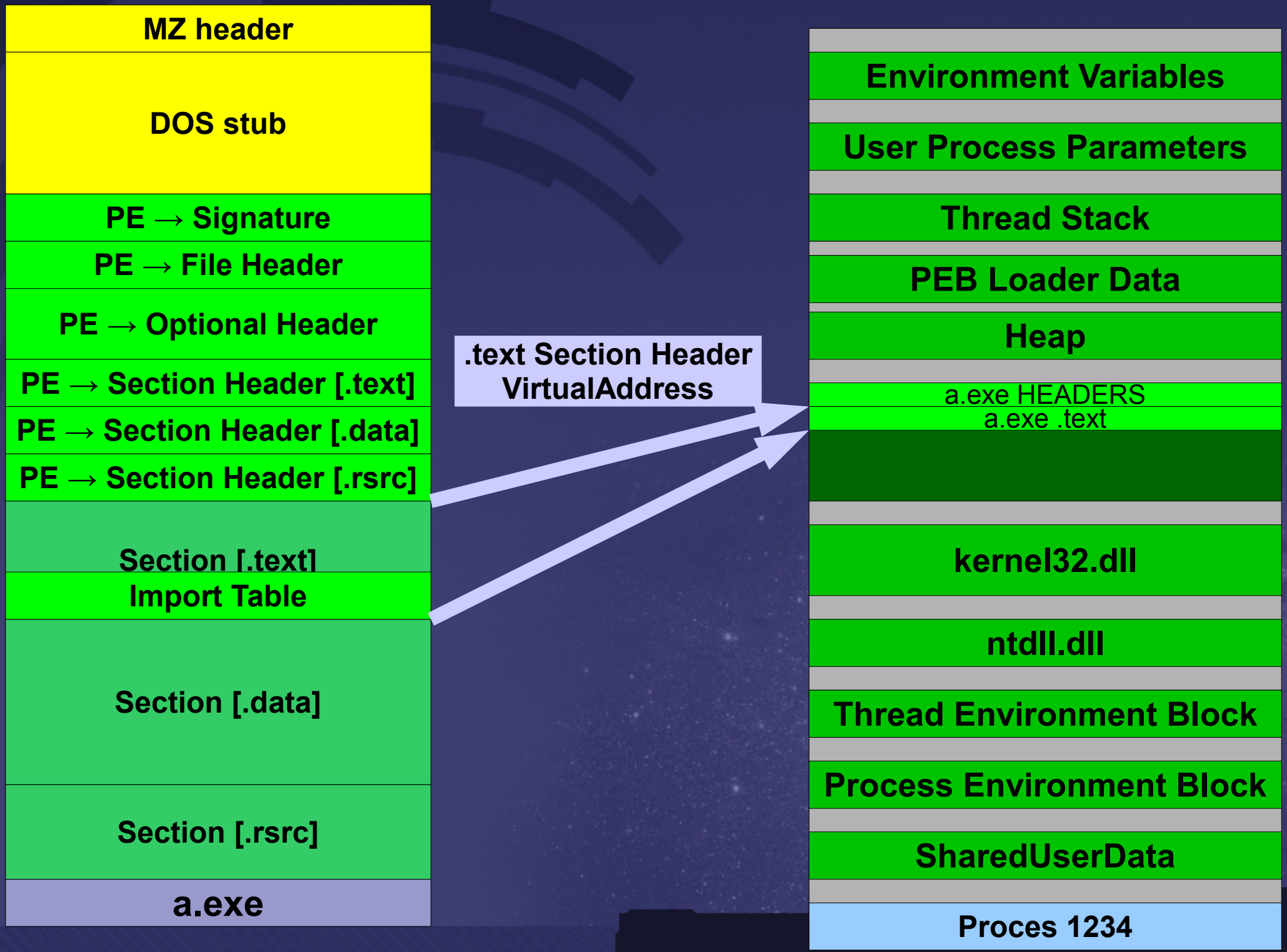

MZ header
DOS stub
PE → Signature
PE → File Header
PE → Optional Header
PE → Section Header [.text]
PE → Section Header [.data]
PE → Section Header [.rsrc]
Section [.text]
Import Table
Section [.data]
Section [.rsrc]
a.exe
OptionalHeader.
ImageBase
OptionalHeader.
SizeOfImage
Environment Variables
User Process Parameters
Thread Stack
PEB Loader Data
Heap
kernel32.dll
ntdll.dll
Thread Environment Block
Process Environment Block
SharedUserData
Proces 1234

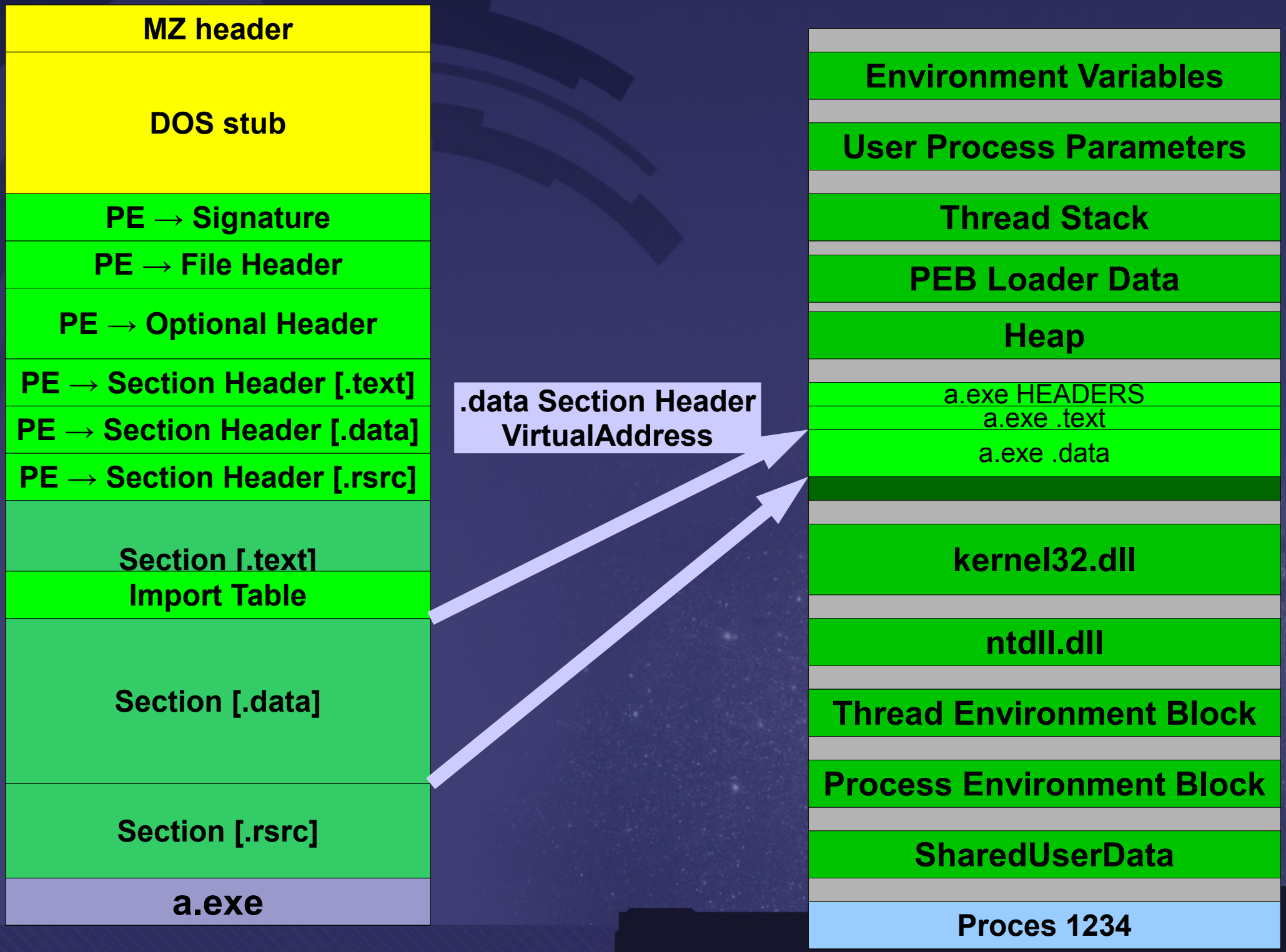

MZ header
DOS stub
PE → Signature
PE → File Header
PE → Optional Header
PE → Section Header [.text]
PE → Section Header [.data]
PE → Section Header [.rsrc]
Section [.text]
Import Table
Section [.data]
Section [.rsrc]
a.exe
OptionalHeader.
ImageBase
Environment Variables
User Process Parameters
Thread Stack
PEB Loader Data
Heap
a.exe HEADERS
kernel32.dll
ntdll.dll
Thread Environment Block
Process Environment Block
SharedUserData
Proces 1234

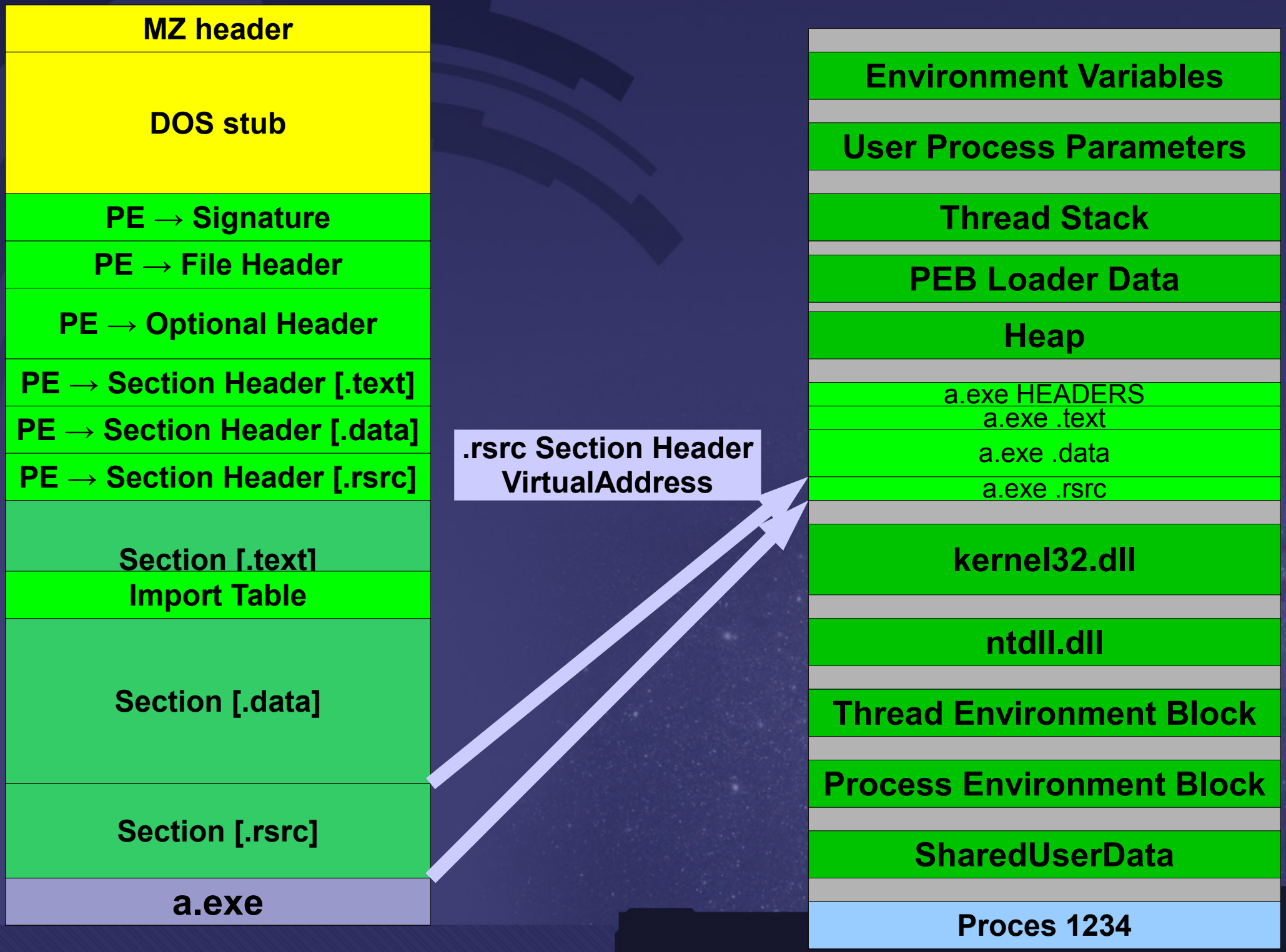
IMAGE_SECTION_HEADER

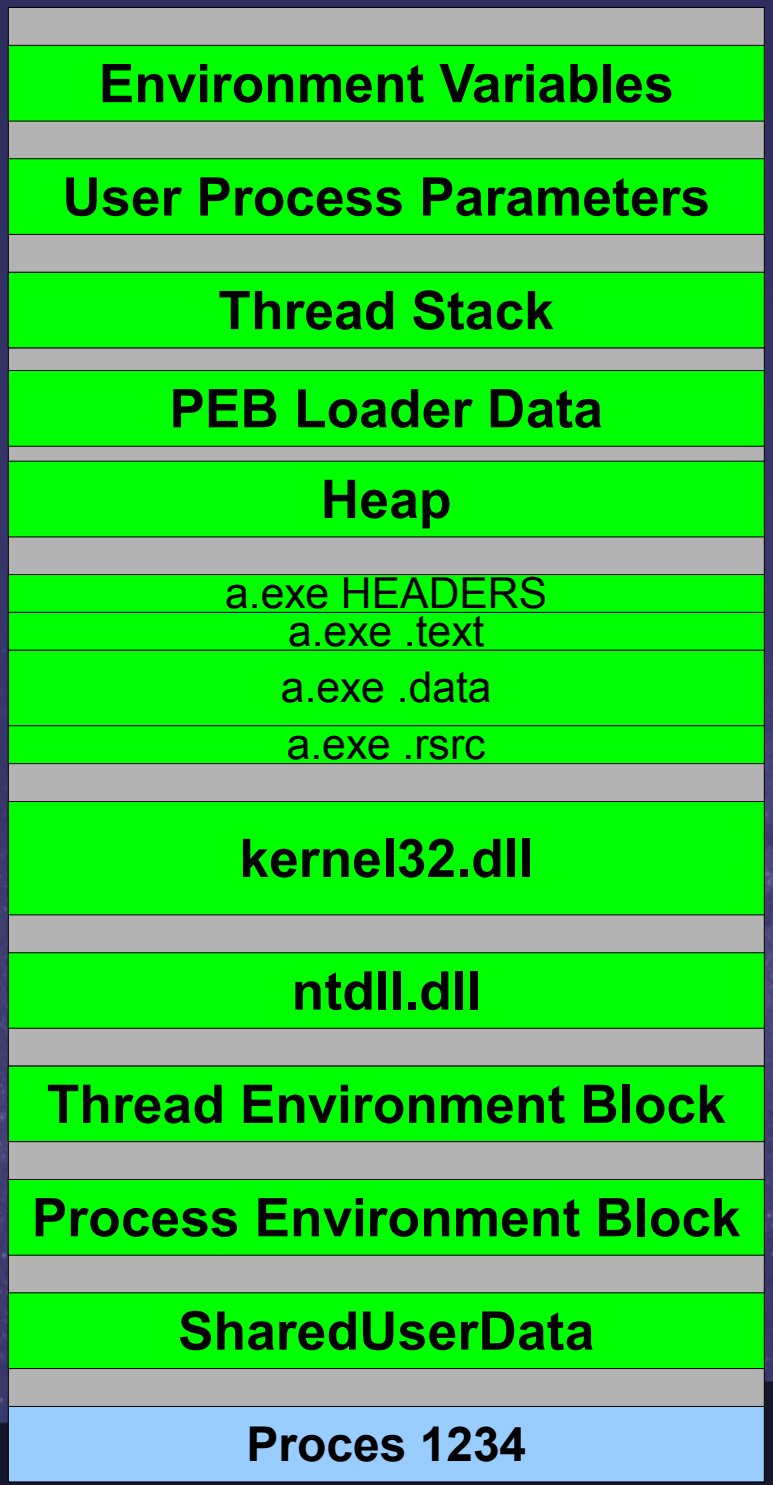
RAW	RVA
PointerToRawData SizeOfRawData	VirtualAddress Misc.VirtualSize
Align to:	**Align to:**
FileAlignment np. 200h	SectionAlignment np. 1000h

SizeOfRawData ??? Misc.VirtualSize


MZ header
DOS stub
PE → Signature
PE → File Header
PE → Optional Header
PE → Section Header [.text]
PE → Section Header [.data]
PE → Section Header [.rsrc]
Section [.text]
Import Table
Section [.data]
Section [.rsrc]
a.exe
.text Section Header
VirtualAddress
Environment Variables
User Process Parameters
Thread Stack
PEB Loader Data
Heap
a.exe HEADERS
a.exe .text
kernel32.dll
ntdll.dll
Thread Environment Block
Process Environment Block
SharedUserData
Proces 1234


MZ header
DOS stub
PE → Signature
PE → File Header
PE → Optional Header
PE → Section Header [.text]
PE → Section Header [.data]
PE → Section Header [.rsrc]
Section [.text]
Import Table
Section [.data]
Section [.rsrc]
a.exe
.data Section Header
VirtualAddress
Environment Variables
User Process Parameters
Thread Stack
PEB Loader Data
Heap
a.exe HEADERS
a.exe .text
a.exe .data
kernel32.dll
ntdll.dll
Thread Environment Block
Process Environment Block
SharedUserData
Proces 1234


MZ header
DOS stub
PE → Signature
PE → File Header
PE → Optional Header
PE → Section Header [.text]
PE → Section Header [.data]
PE → Section Header [.rsrc]
Section [.text]
Import Table
Section [.data]
Section [.rsrc]
a.exe
.rsrc Section Header
VirtualAddress
Environment Variables
User Process Parameters
Thread Stack
PEB Loader Data
Heap
a.exe HEADERS
a.exe .text
a.exe .data
a.exe .rsrc
kernel32.dll
ntdll.dll
Thread Environment Block
Process Environment Block
SharedUserData
Proces 1234


Environment Variables
User Process Parameters
Thread Stack
PEB Loader Data
Heap
a.exe HEADERS
a.exe .text
a.exe .data
a.exe .rsrc
kernel32.dll
ntdll.dll
Thread Environment Block
Process Environment Block
SharedUserData
Proces 1234

Dziękuje za uwagę :)

Strony projektu:

http://re.coldwind.pl/
http://www.uw-team.org/