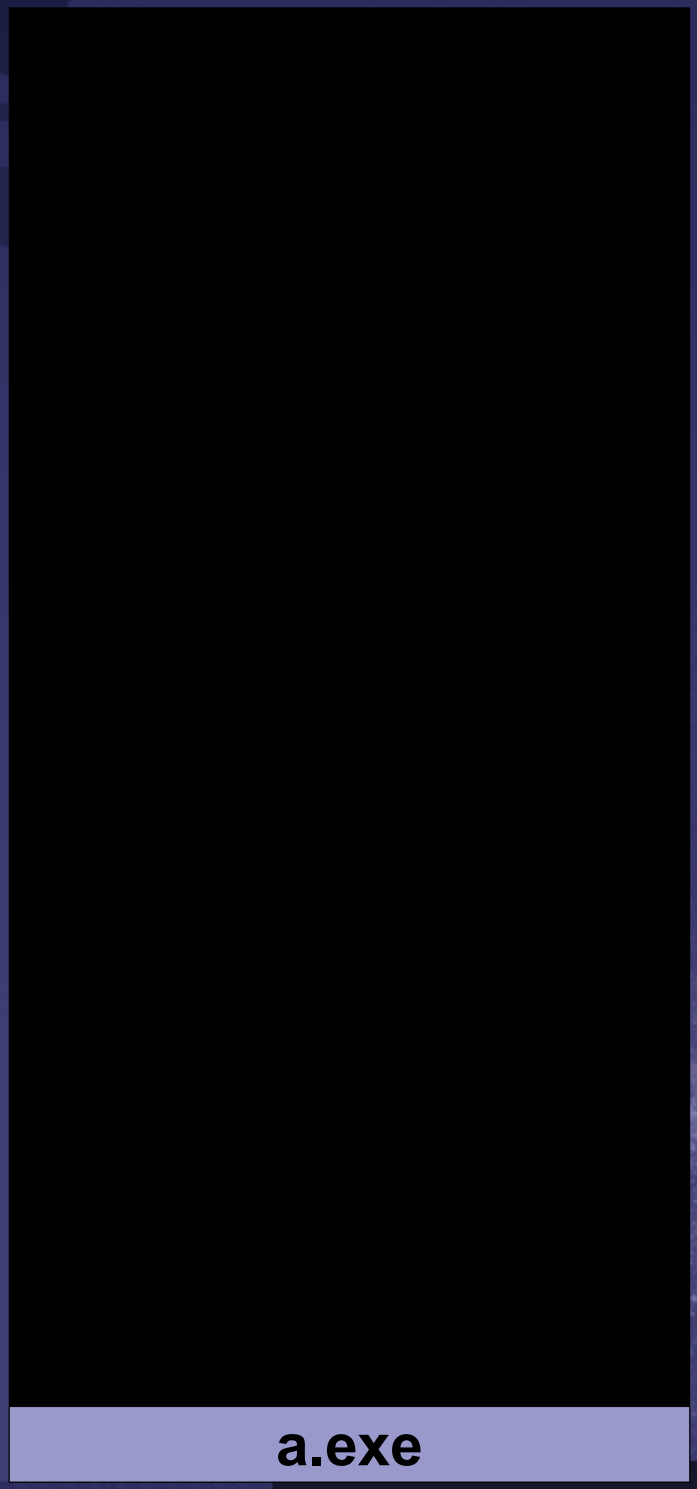
ReverseCraft

by gynvael.coldwind//vx

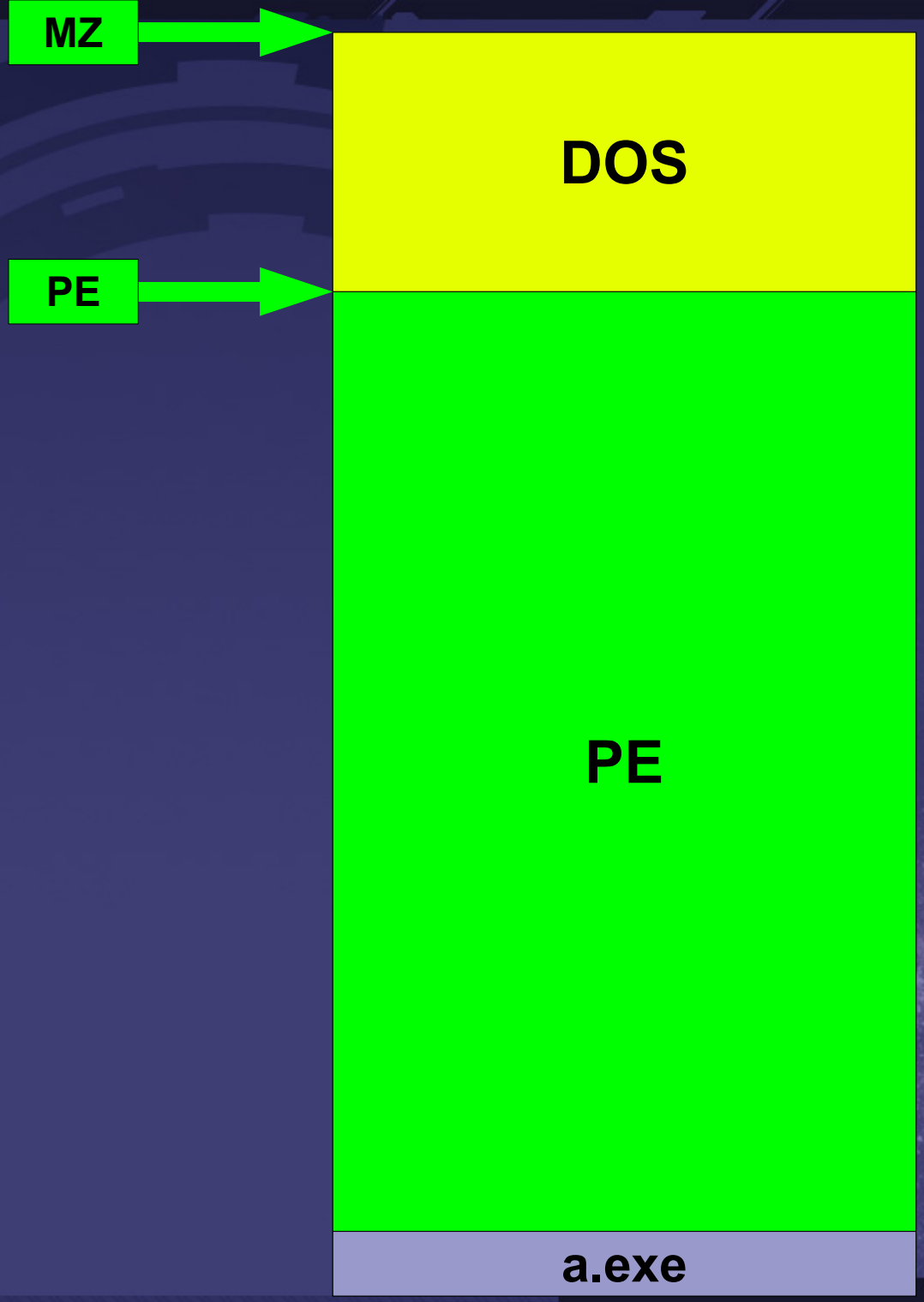
002 – Podstawy budowy plików PE

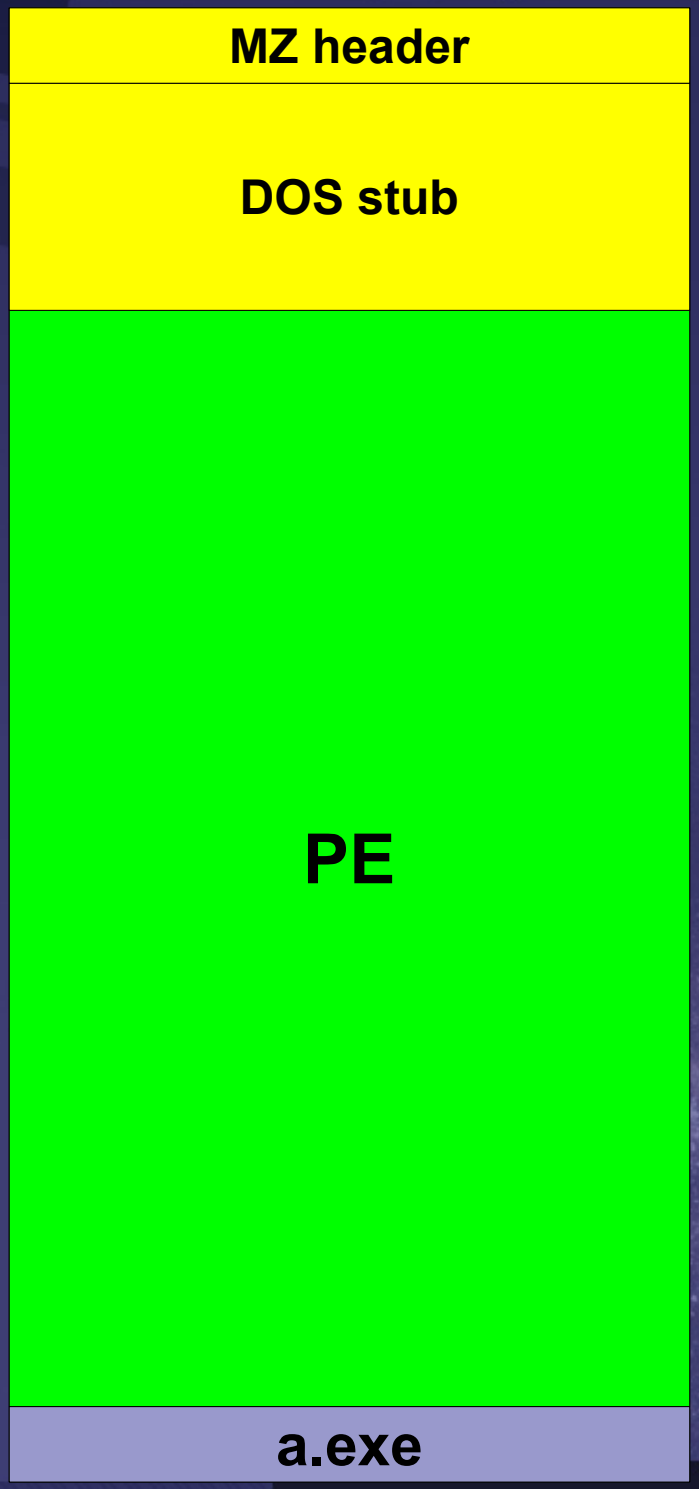
Strony projektu:

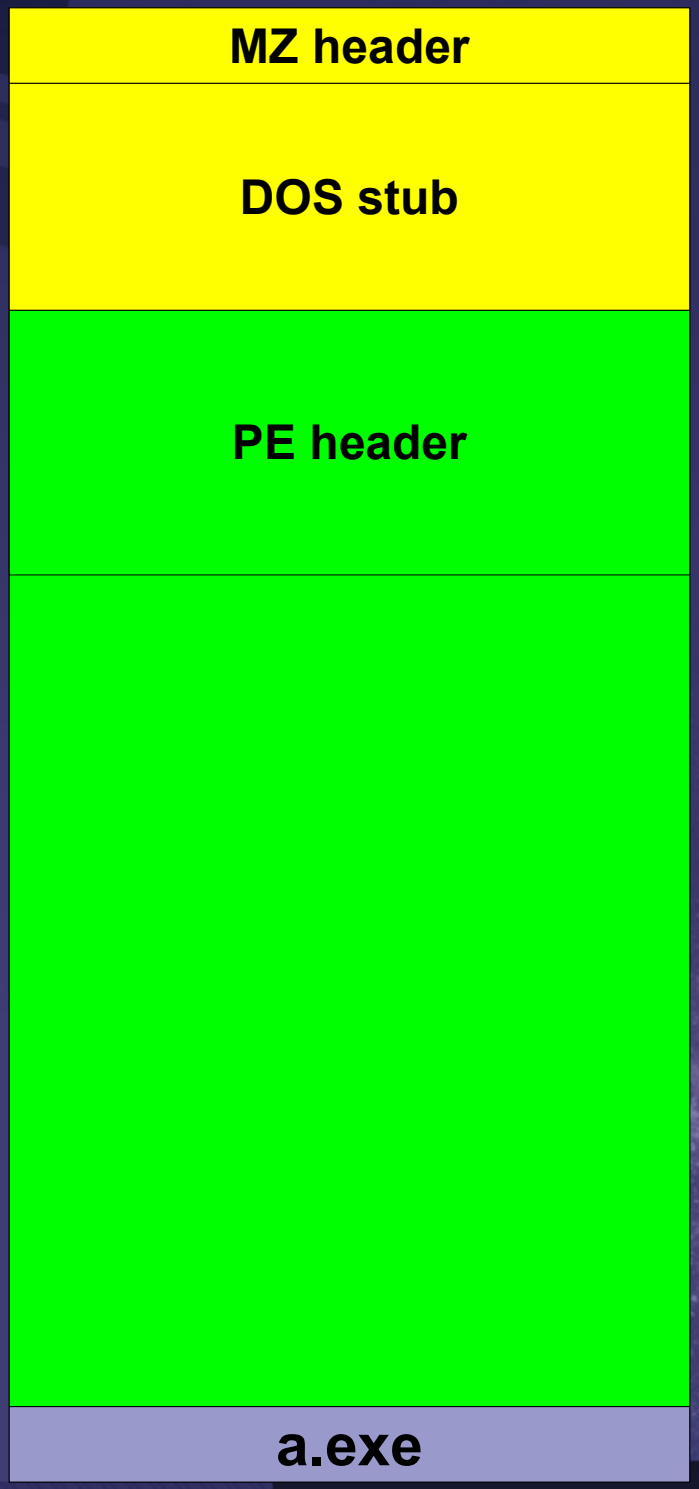
http://re.coldwind.pl/
http://www.uw-team.org/

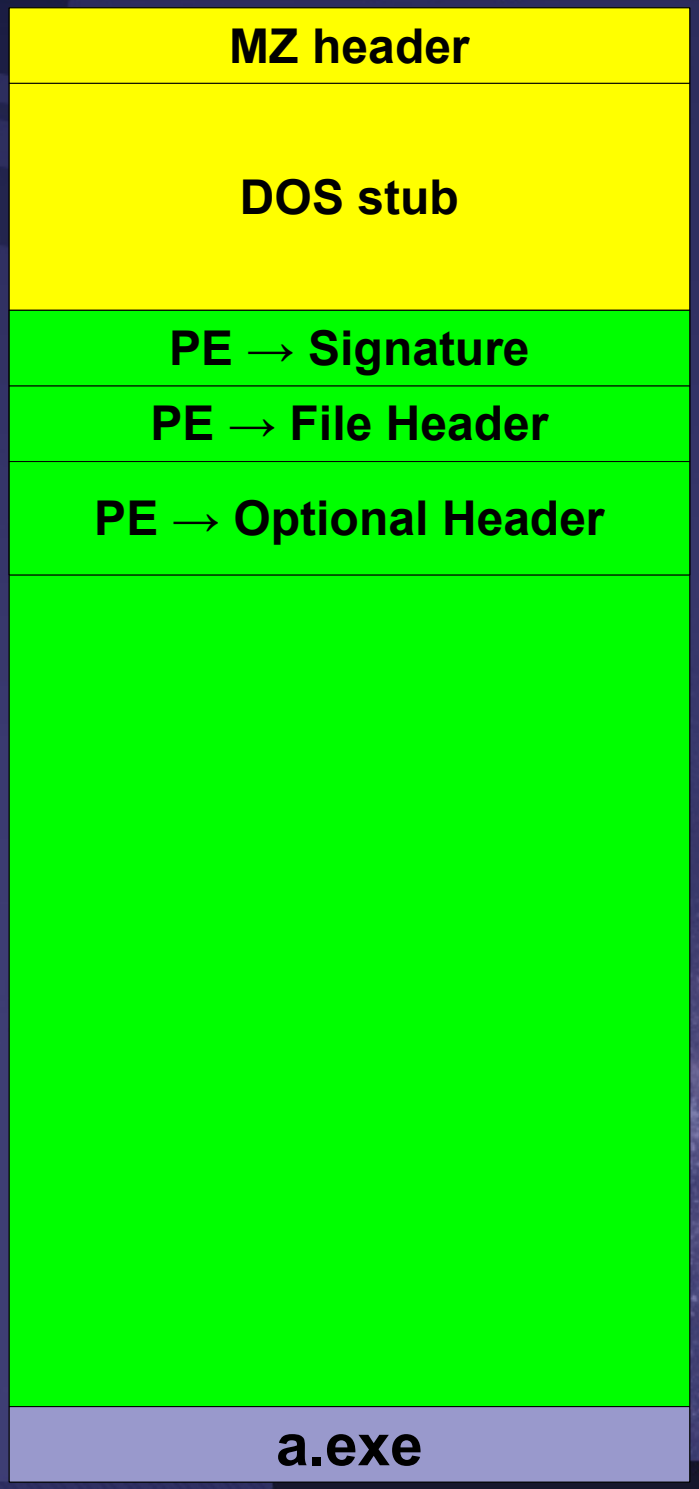


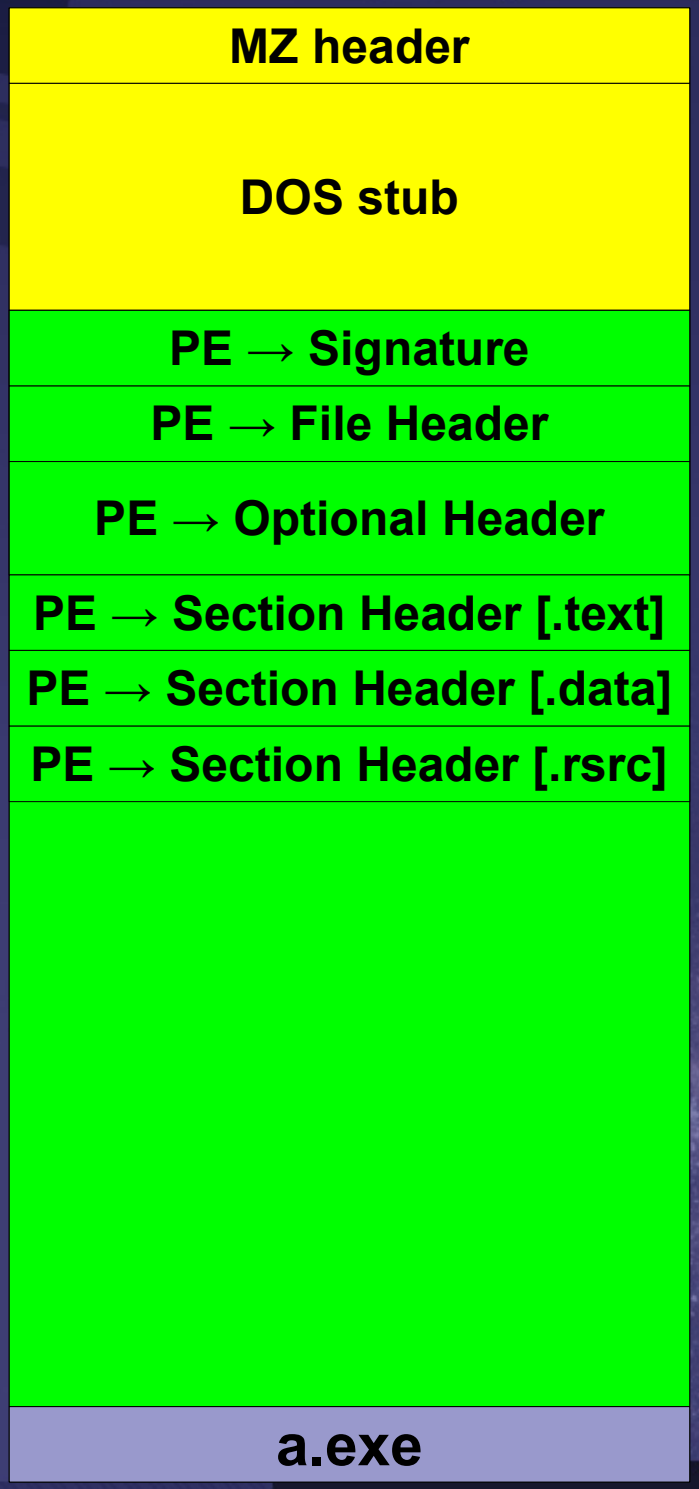
a.exe

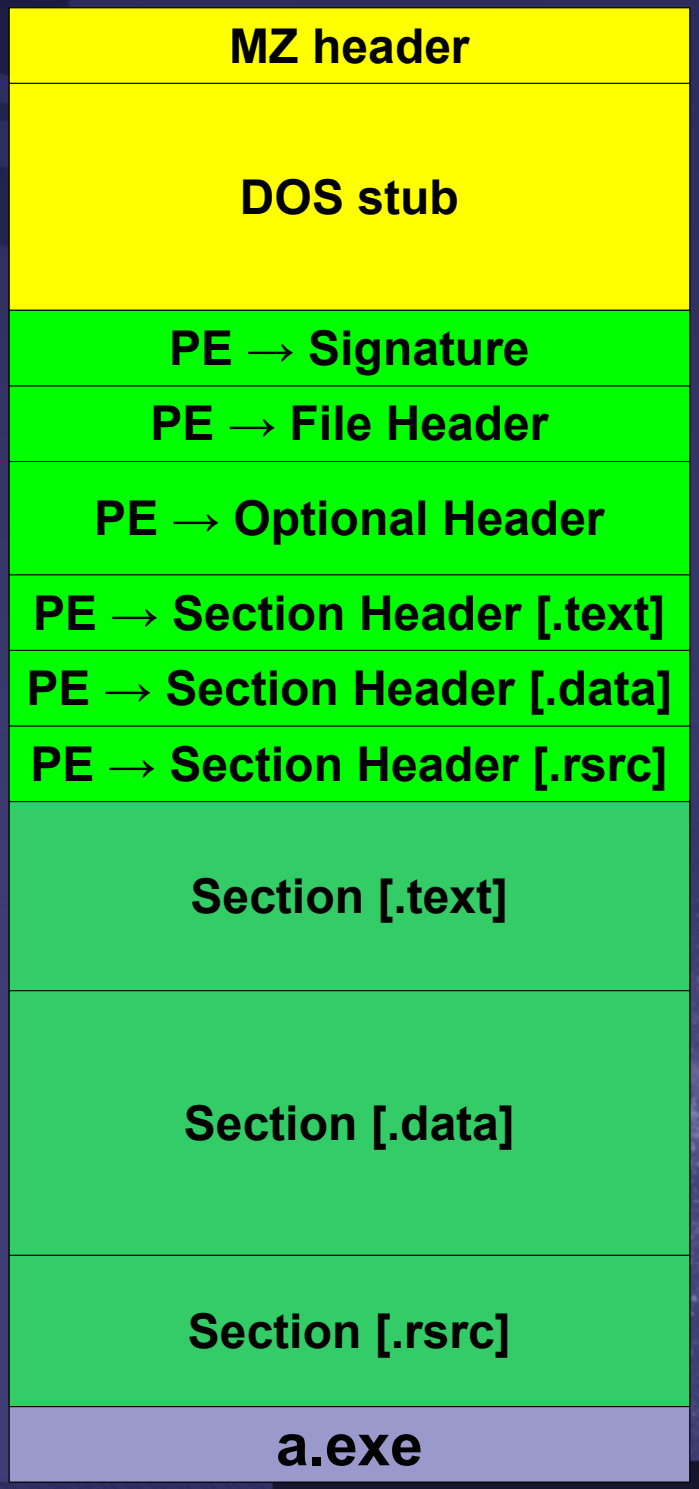

MZ
PE
DOS
PE
a.exe

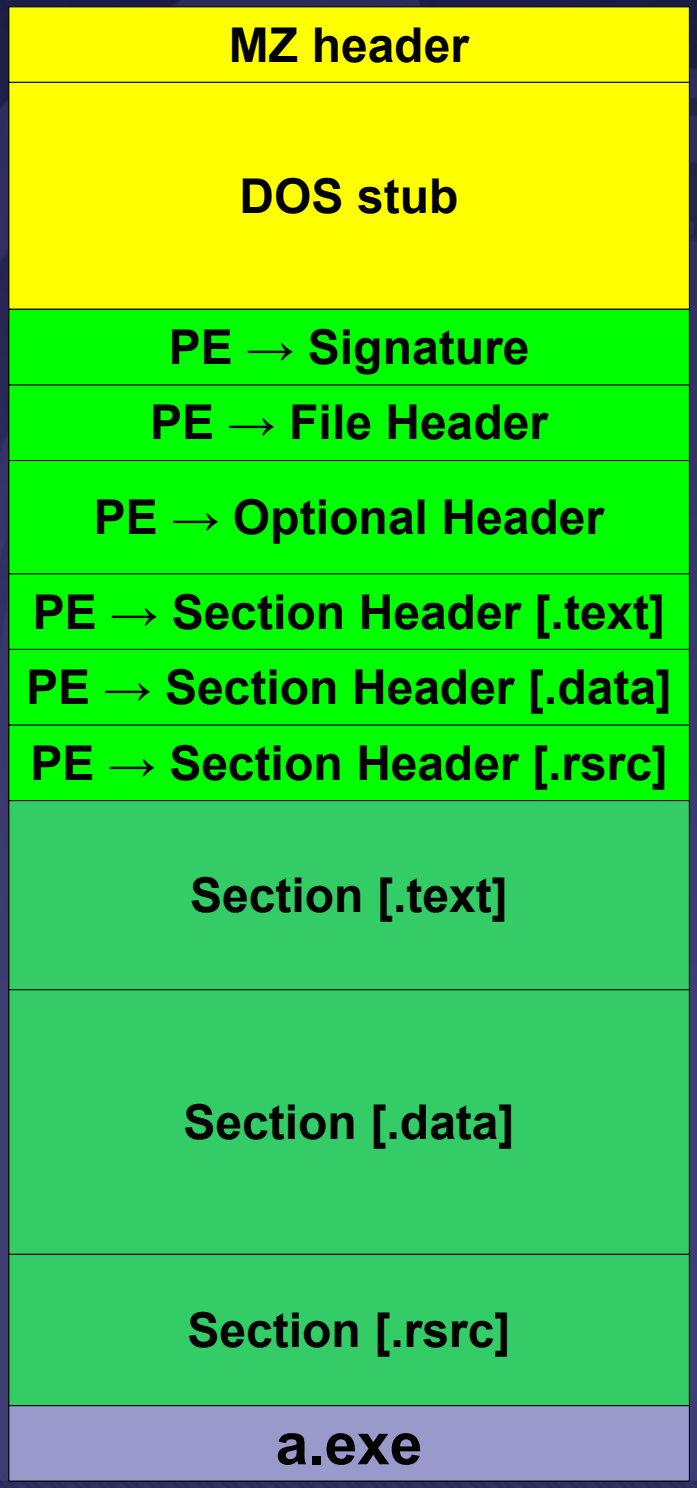

MZ header
DOS stub
PE
a.exe

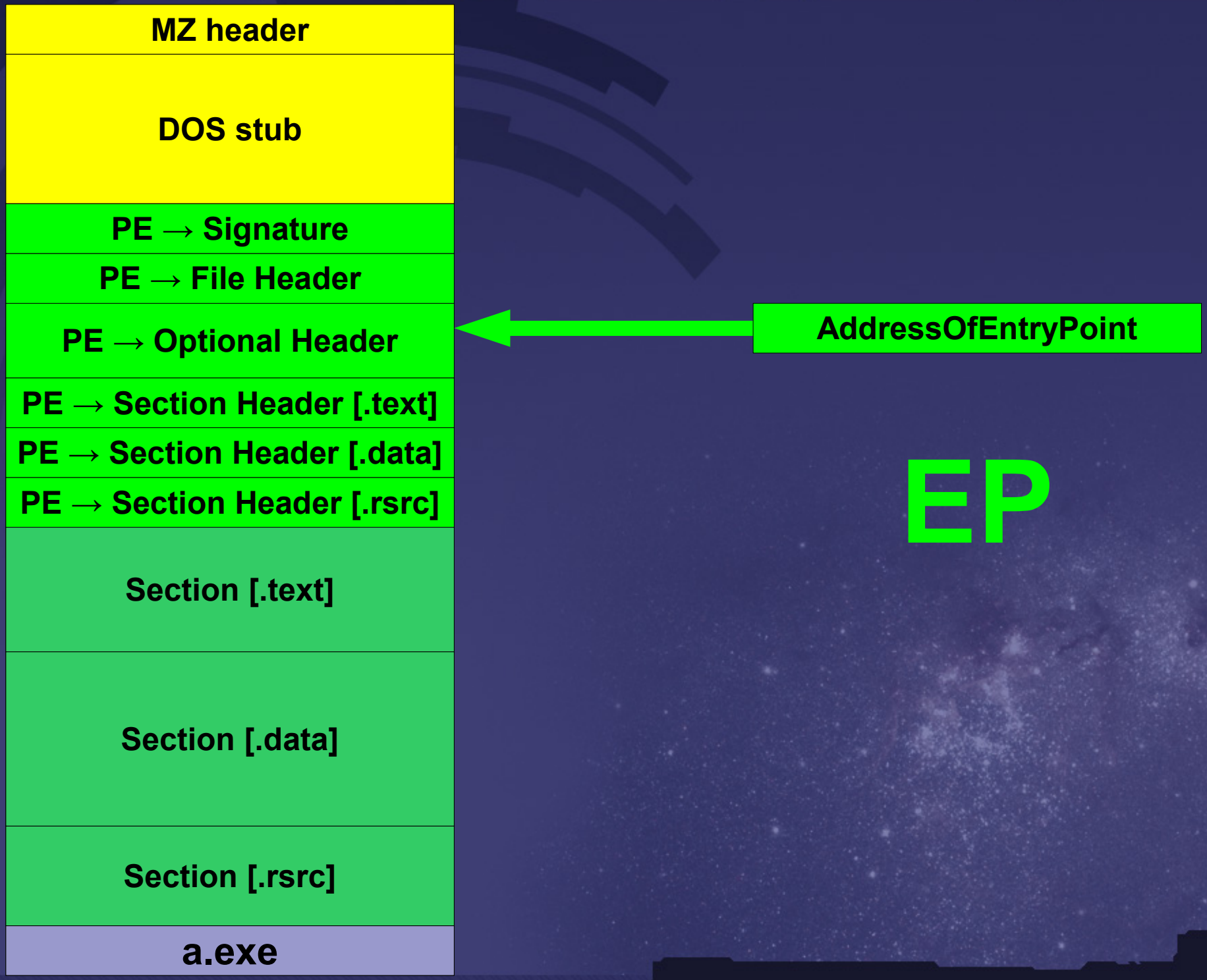

MZ header
DOS stub
PE header
a.exe

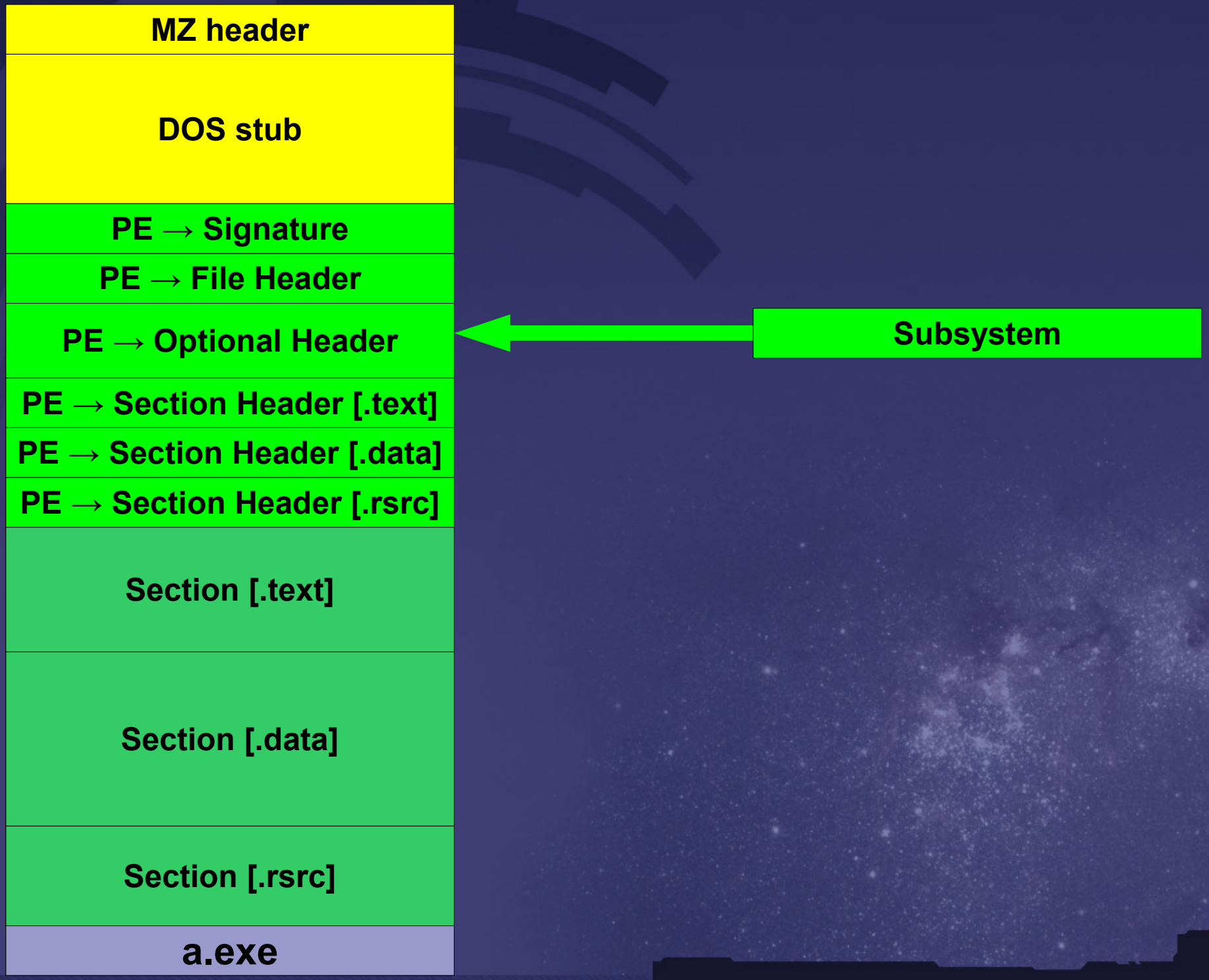

MZ header
DOS stub
PE → Signature
PE → File Header
PE → Optional Header
a.exe


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

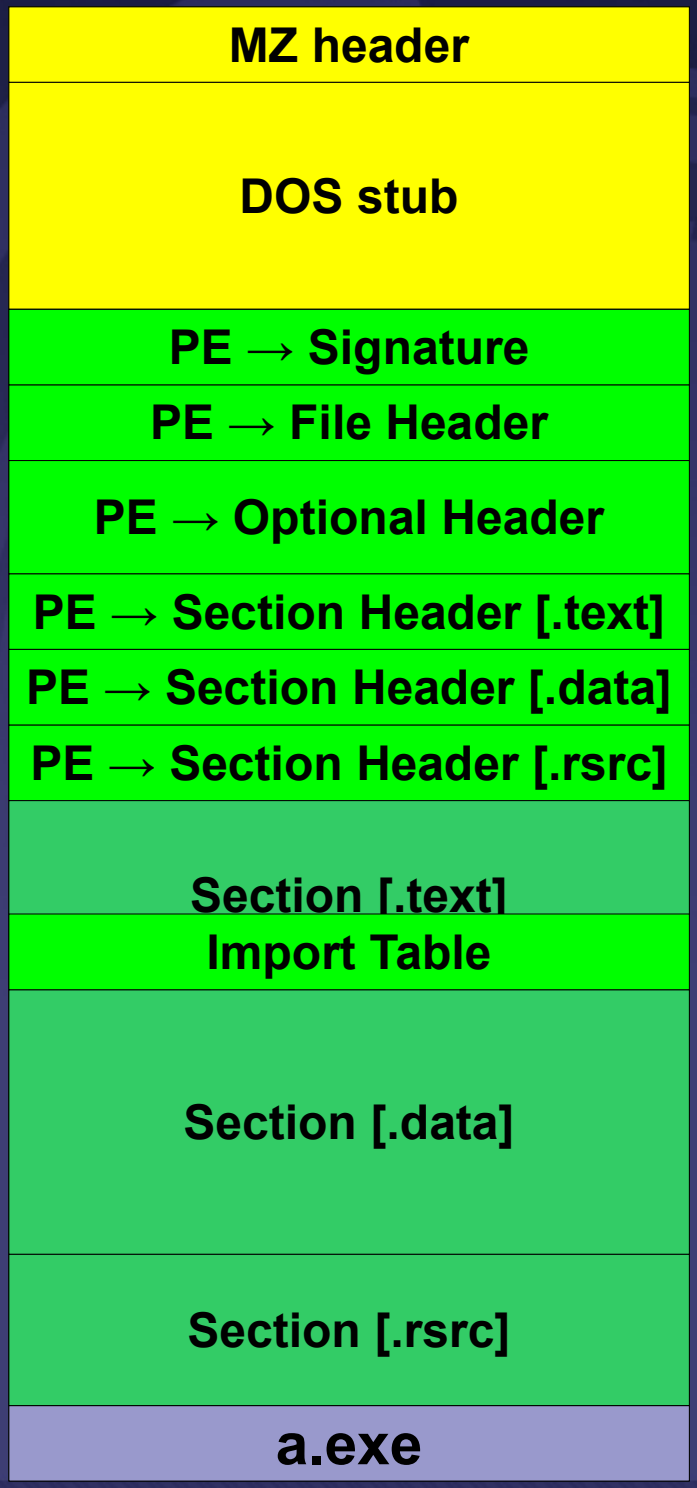

MZ header
DOS stub
PE → Signature
PE → File Header
PE → Optional Header
PE → Section Header [.text]
PE → Section Header [.data]
PE → Section Header [.rsrc]
Section [.text]
Section [.data]
Section [.rsrc]
a.exe
AddressOfEntryPoint
EP

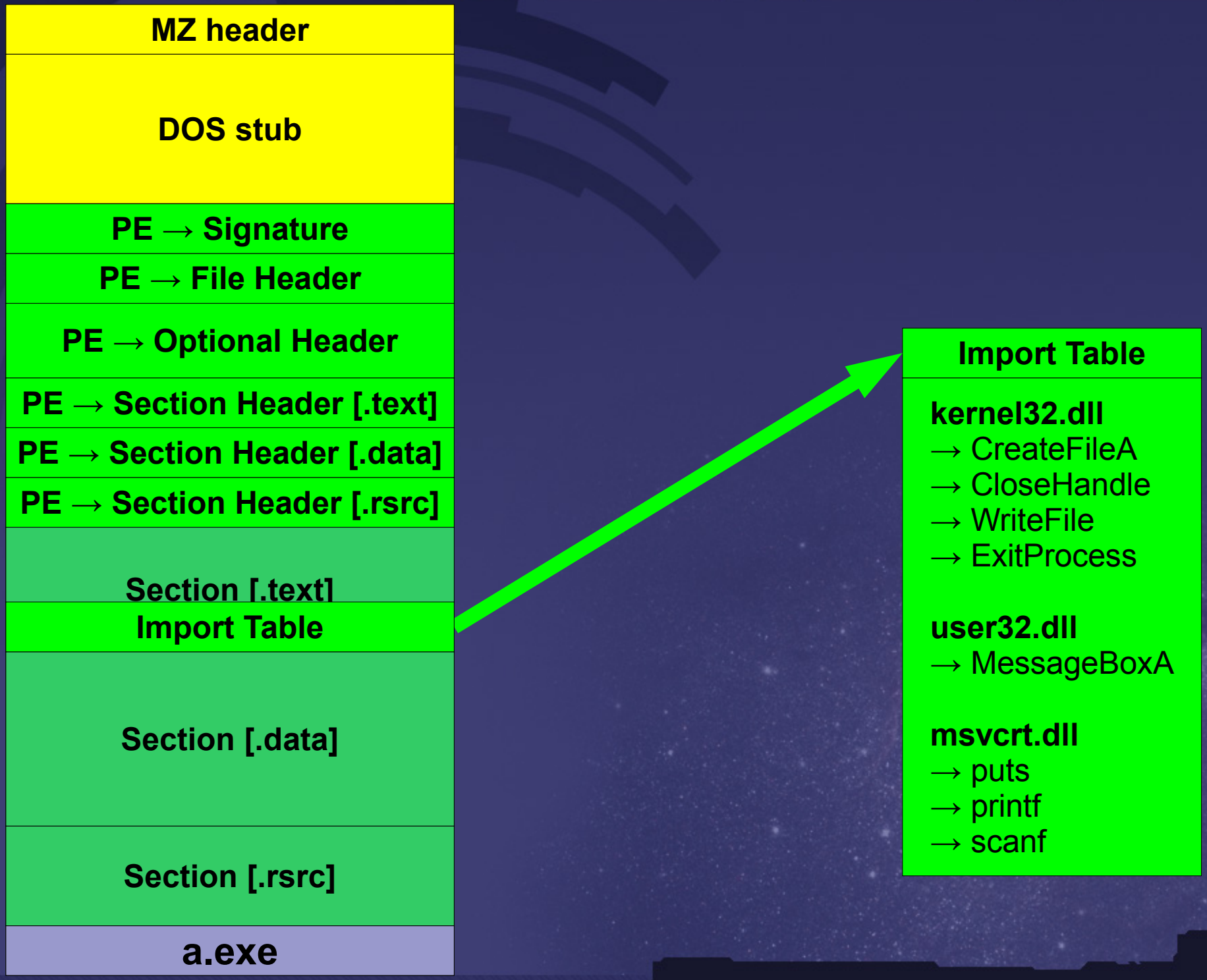

MZ header
DOS stub
PE → Signature
PE → File Header
PE → Optional Header
PE → Section Header [.text]
PE → Section Header [.data]
PE → Section Header [.rsrc]
Section [.text]
Section [.data]
Section [.rsrc]
a.exe
Subsystem

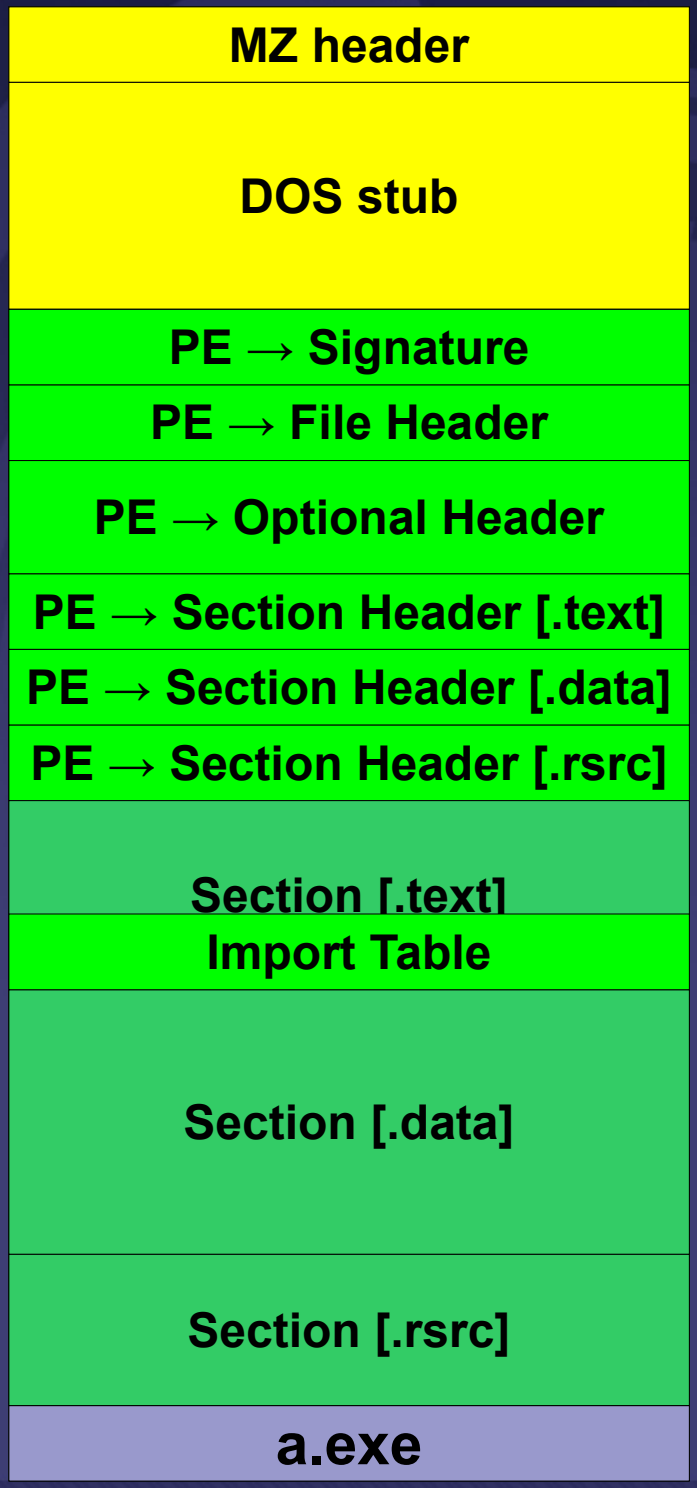

MZ header
DOS stub
PE → Signature
PE → File Header
PE → Optional Header
PE → Section Header [.text]
PE → Section Header [.data]
PE → Section Header [.rsrc]
Section [.text]
Section [.data]
Section [.rsrc]
a.exe
Data Directory


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]
Section [.data]
Section [.rsrc]
a.exe
Data Directory
0 EXPORT
1 IMPORT
2 RESOURCE
3 EXCEPTION
4 SECURITY
5 BASERELOC
6 DEBUG
7 COPYRIGHT lub
ARCHITECTURE
8 GLOBALPTR
9 TLS
10 LOAD_CONFIG
11 BOUND_IMPORT
12 IAT
13 DELAY_IMPORT
14 COM_DESCRIPTOR


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 Directory
0 EXPORT
1 IMPORT
2 RESOURCE
3 EXCEPTION
4 SECURITY
5 BASERELOC
6 DEBUG
7 COPYRIGHT lub
ARCHITECTURE
8 GLOBALPTR
9 TLS
10 LOAD_CONFIG
11 BOUND_IMPORT
12 IAT
13 DELAY_IMPORT
14 COM_DESCRIPTOR


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
Import Table
kernel32.dll
→ CreateFileA
→ CloseHandle
→ WriteFile
→ ExitProcess
user32.dll
→ MessageBoxA
msvcrt.dll
→ puts
→ printf
→ scanf


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

Dziękuje za uwagę :)

Strony projektu:

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