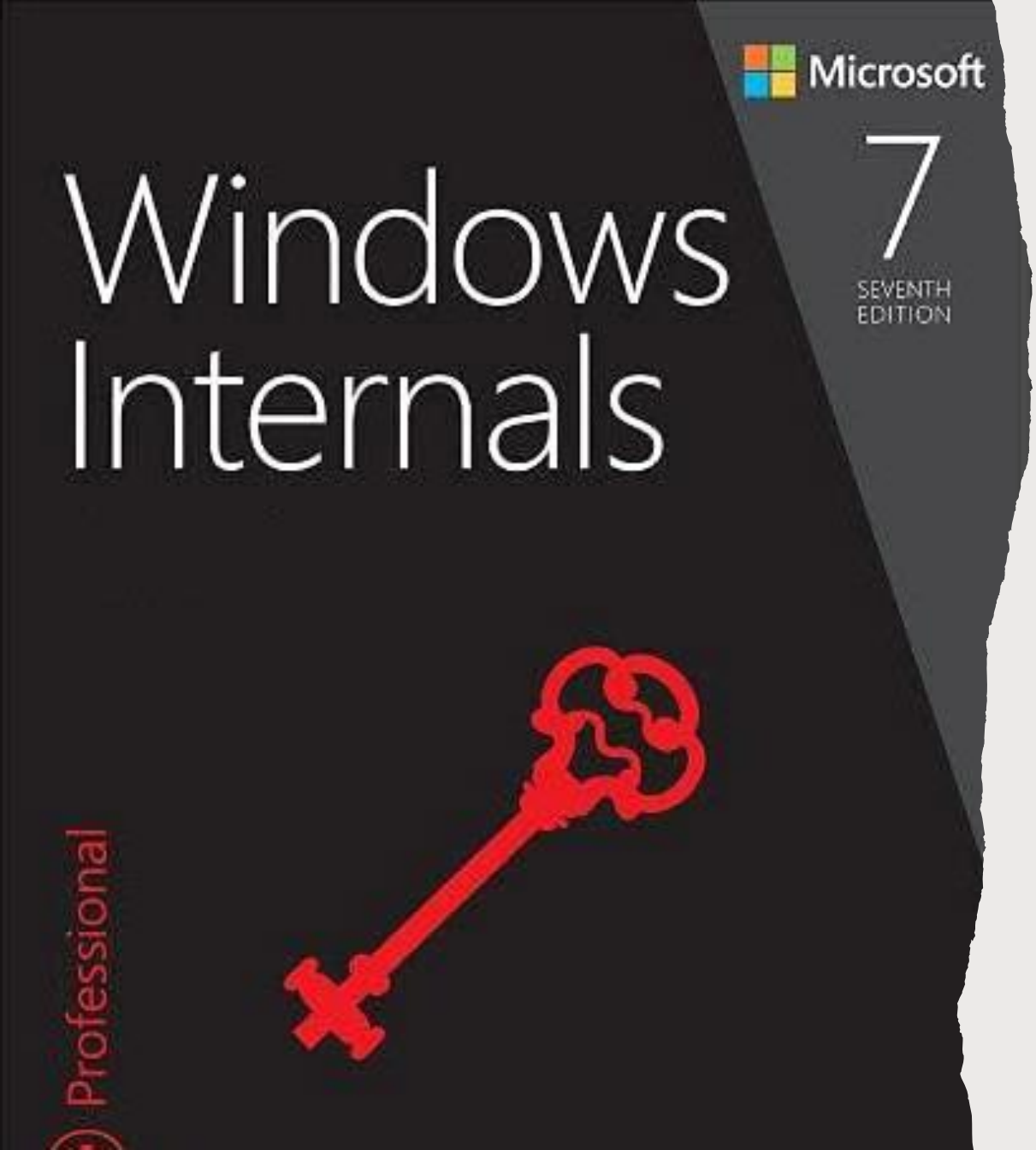
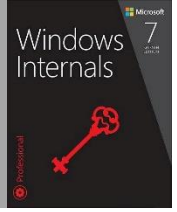


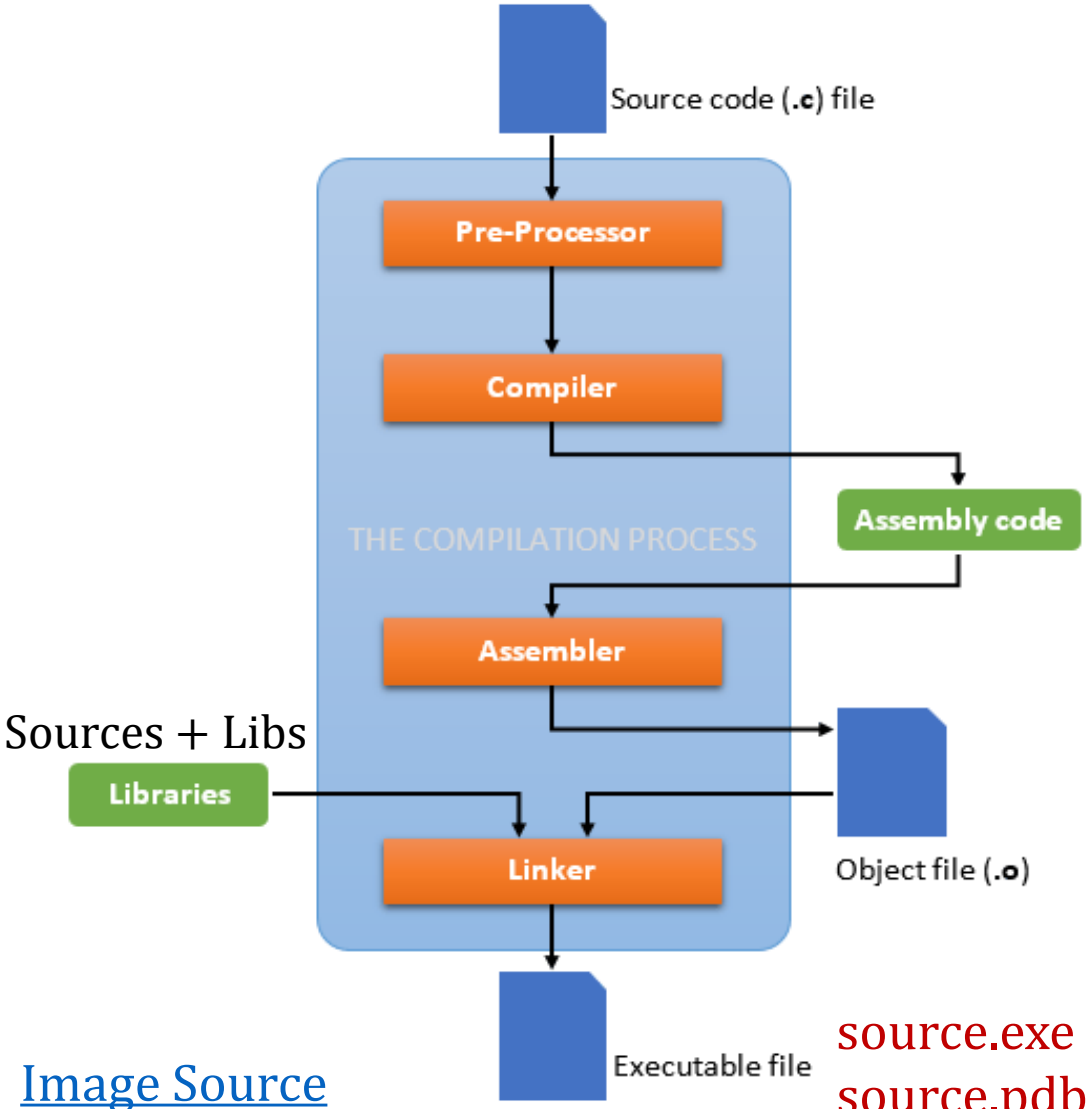
02)Debugging

Chapter Topics



- Program Compilation & Execution
- Assembly Review (x86, x64)
- Visual Studio Debugging
- Introducing Windows Debuggers
- How to use WinDbg [Preview]
- Calling Conventions (x86, x64)
- Live Kernel Debugging
- Examining Windows Structures
- HyperDbg Introduction

Compilation Stages



source.cpp

source.i

source.asm or source.cod

source.obj

source.exe
source.pdb

[Image Source]

Portable Executable Structure

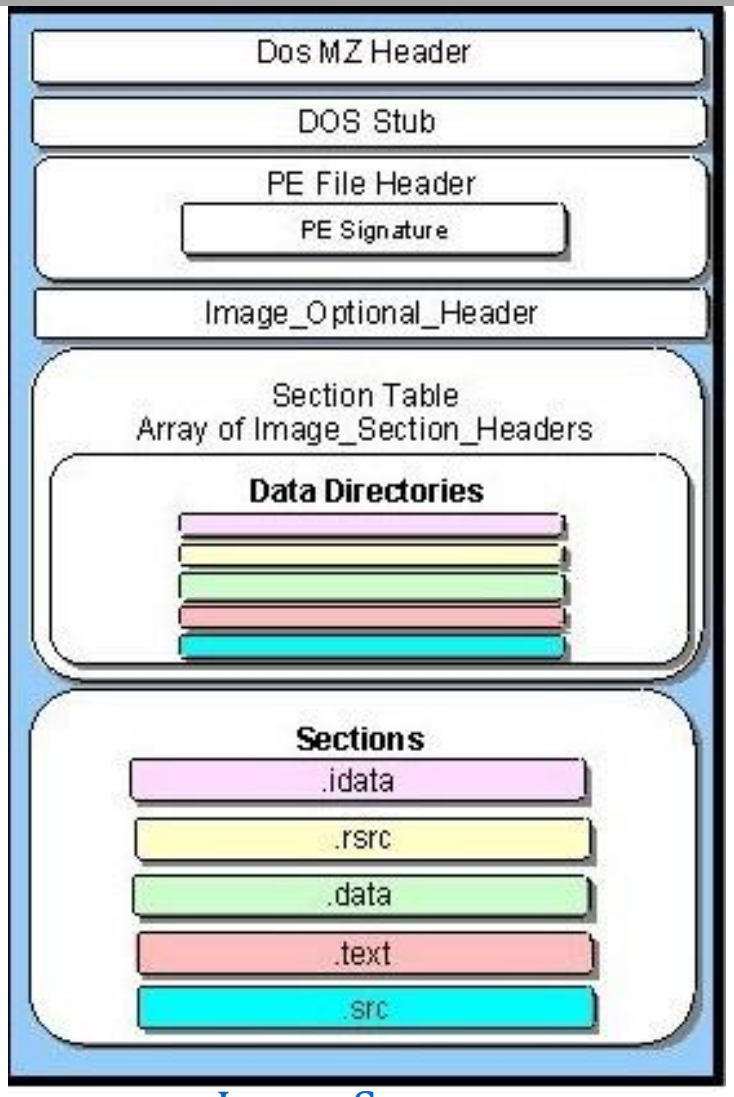
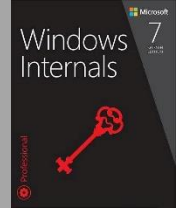
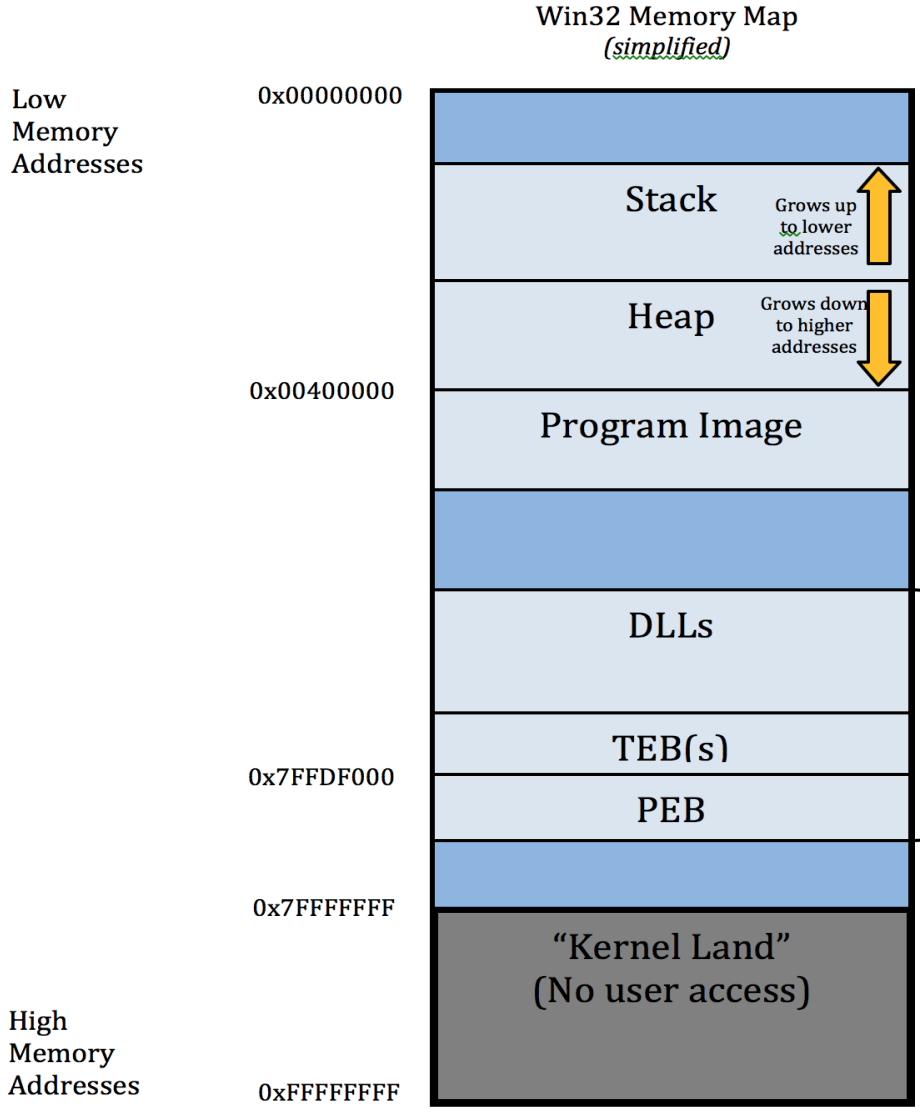


Image Source

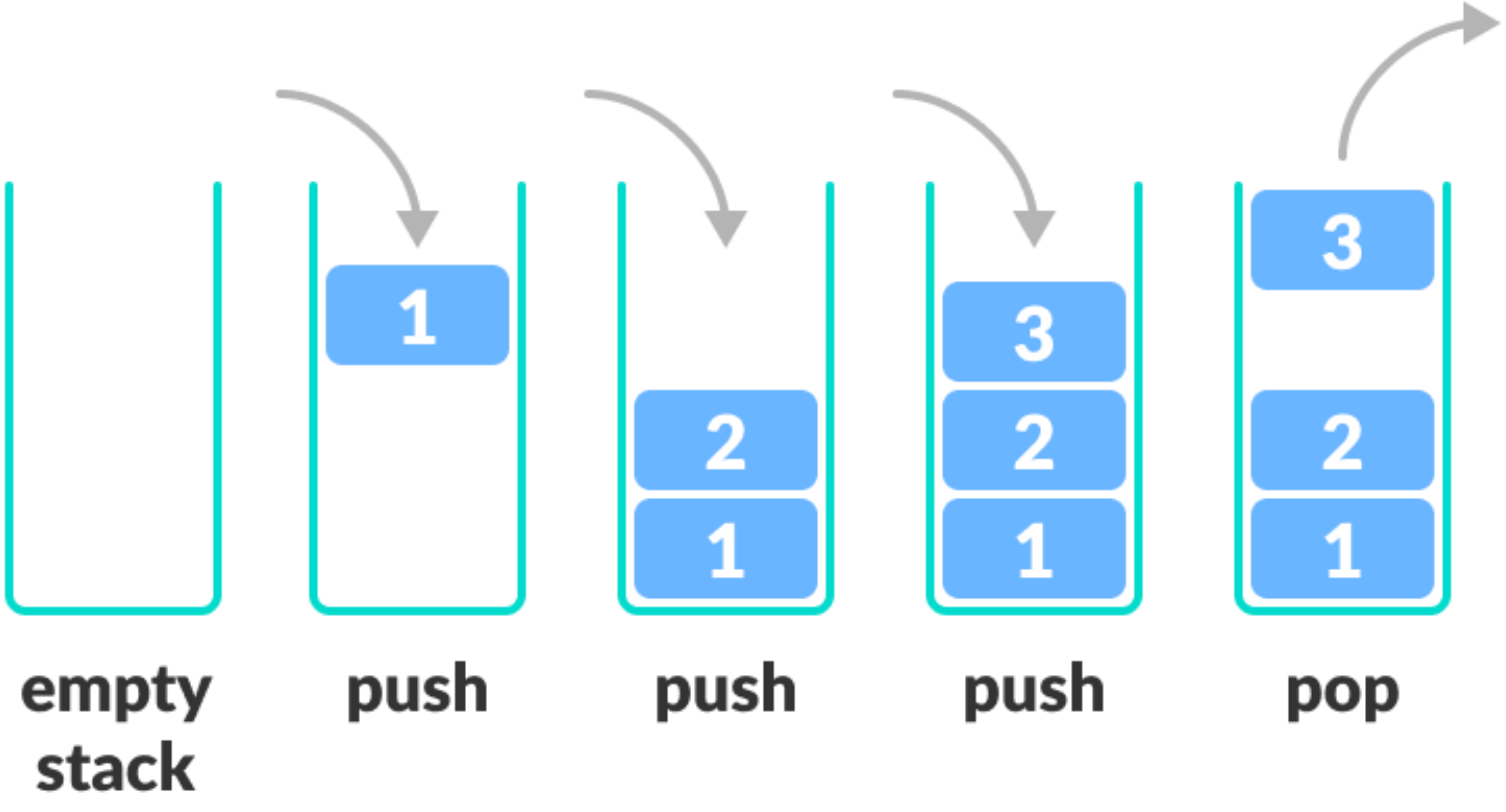
Windows Process Layout





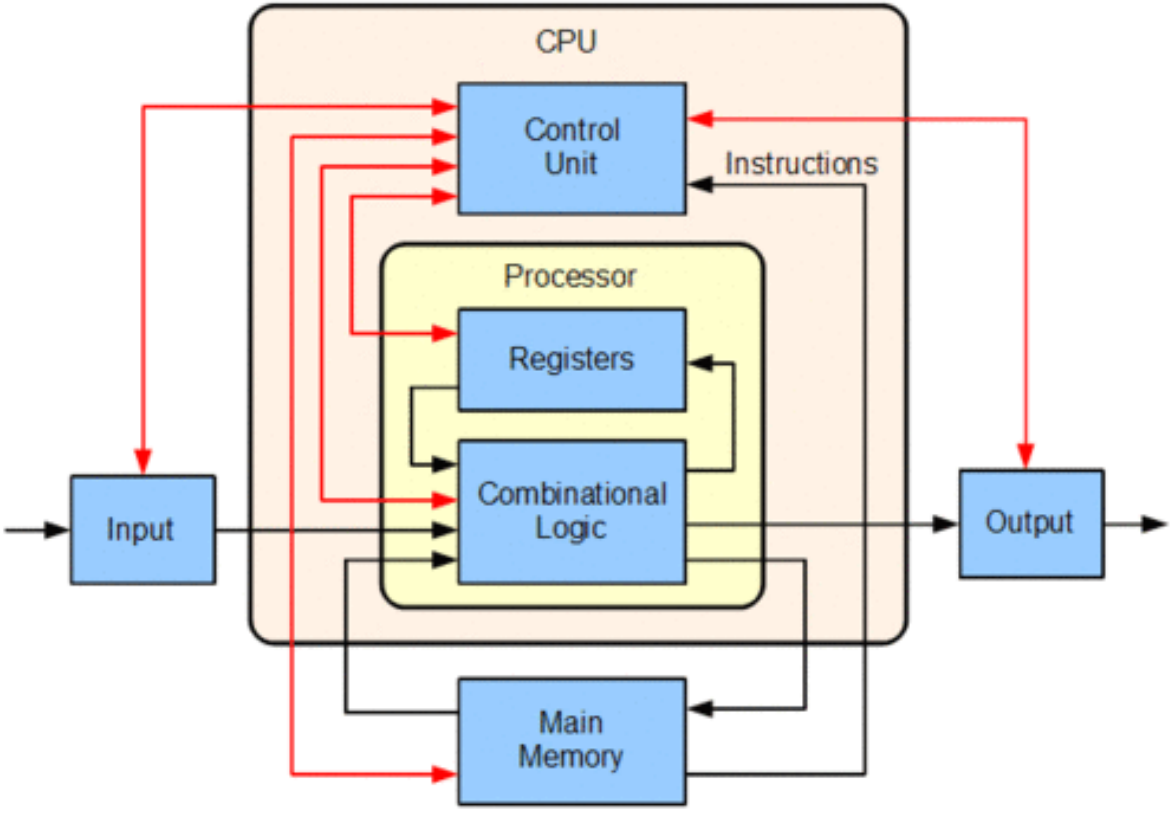
[Image Source]

Stack Structure



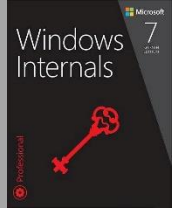
[Image Source]

Computer Architecture



[Image Source]

x86 Registers

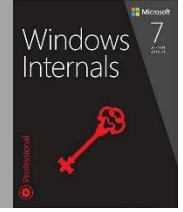


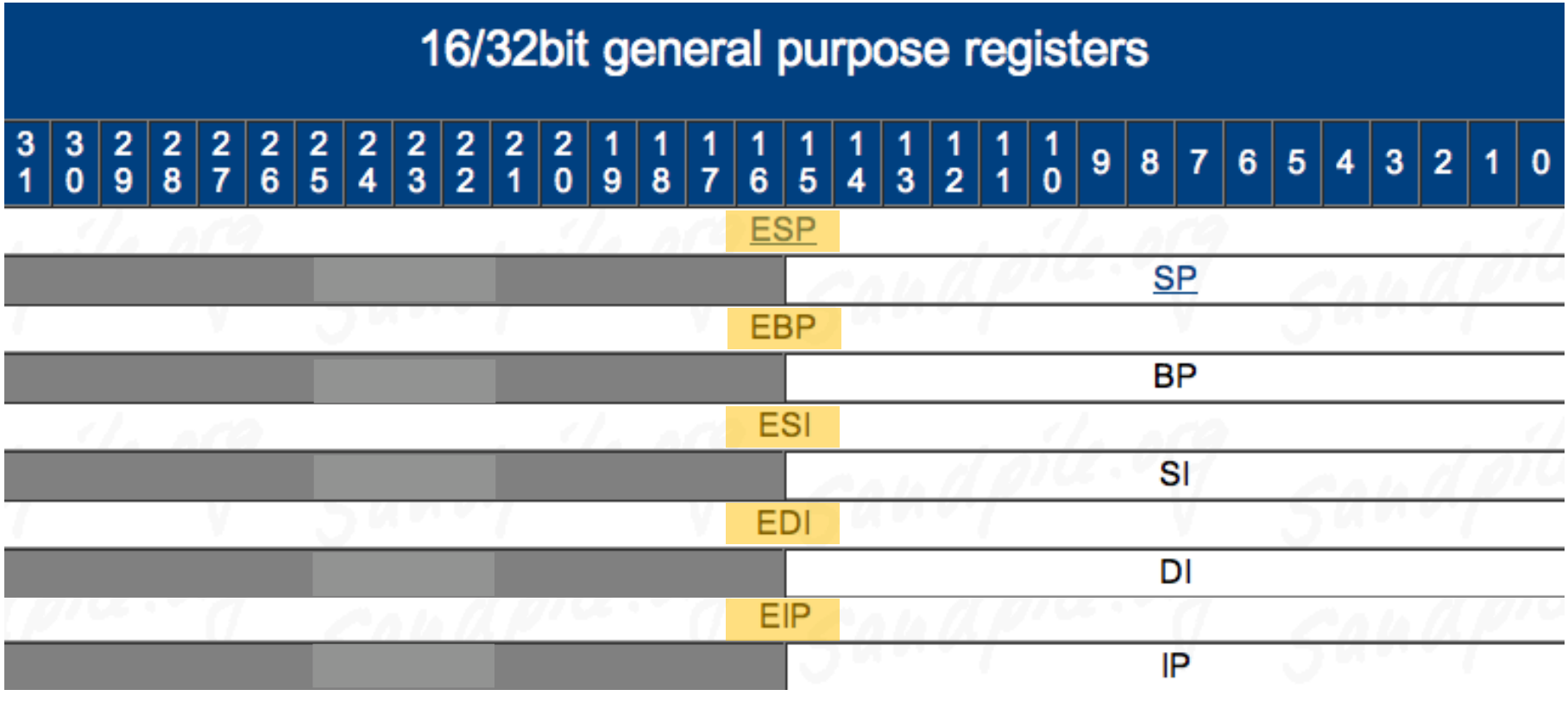
8/16/32bit general purpose registers

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
EAX																															
																AX															
																			AH									AL			
ECX																															
																CX															
																			CH									CL			
EDX																															
																DX															
																			DH									DL			
EBX																															
																BX															
																			BH									BL			

[Image Source]

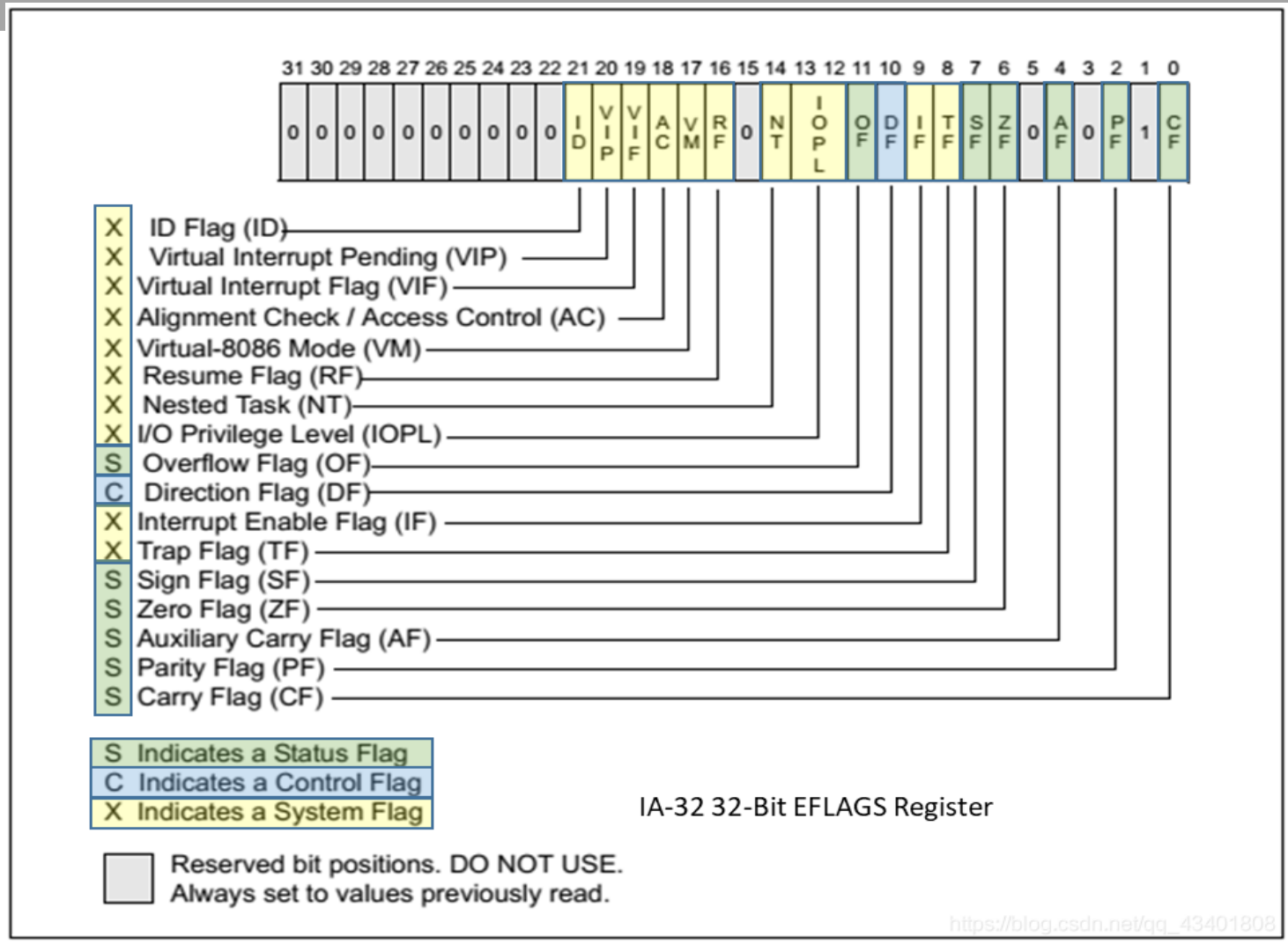
x86 Registers





[Image Source]

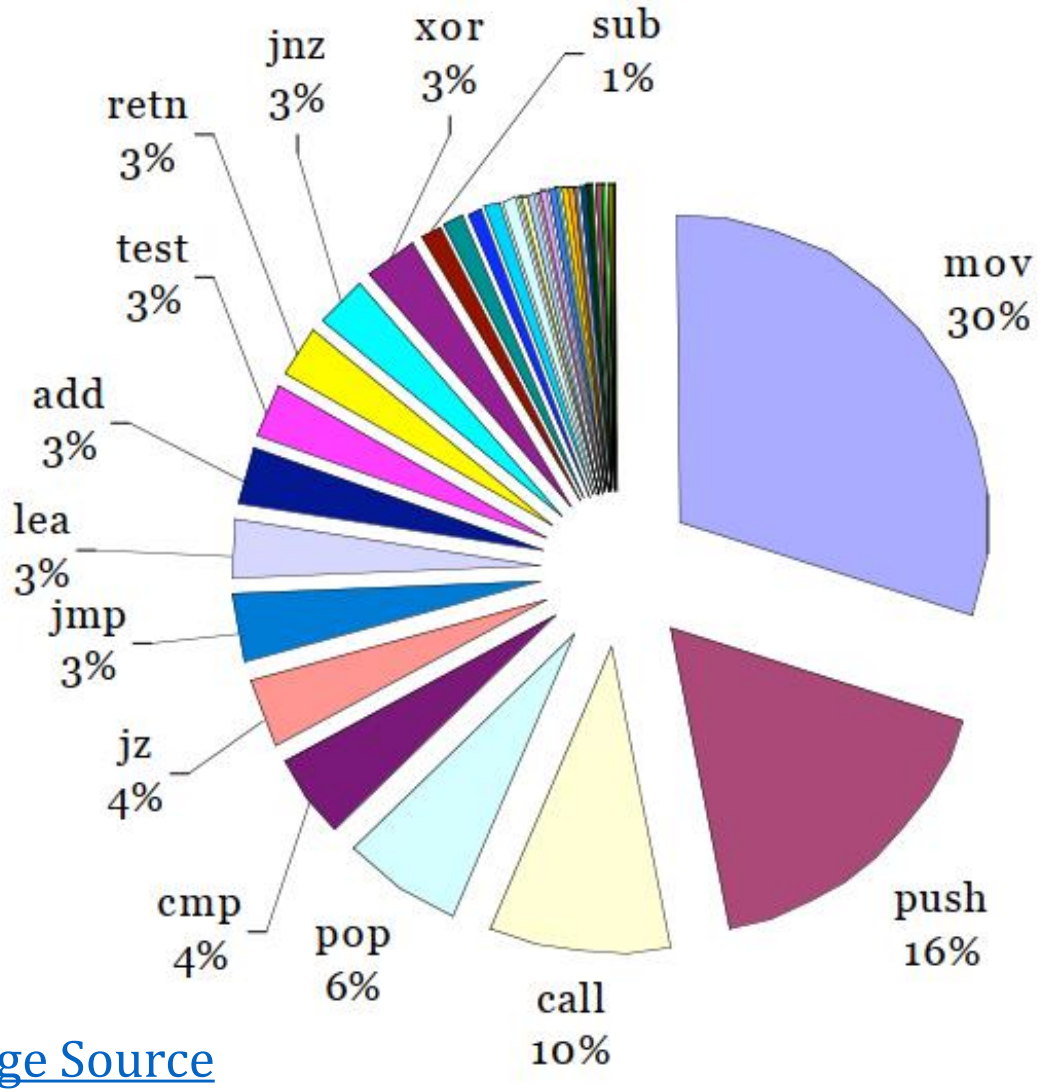
EFLAGS Register



IA-32 32-Bit EFLAGS Register

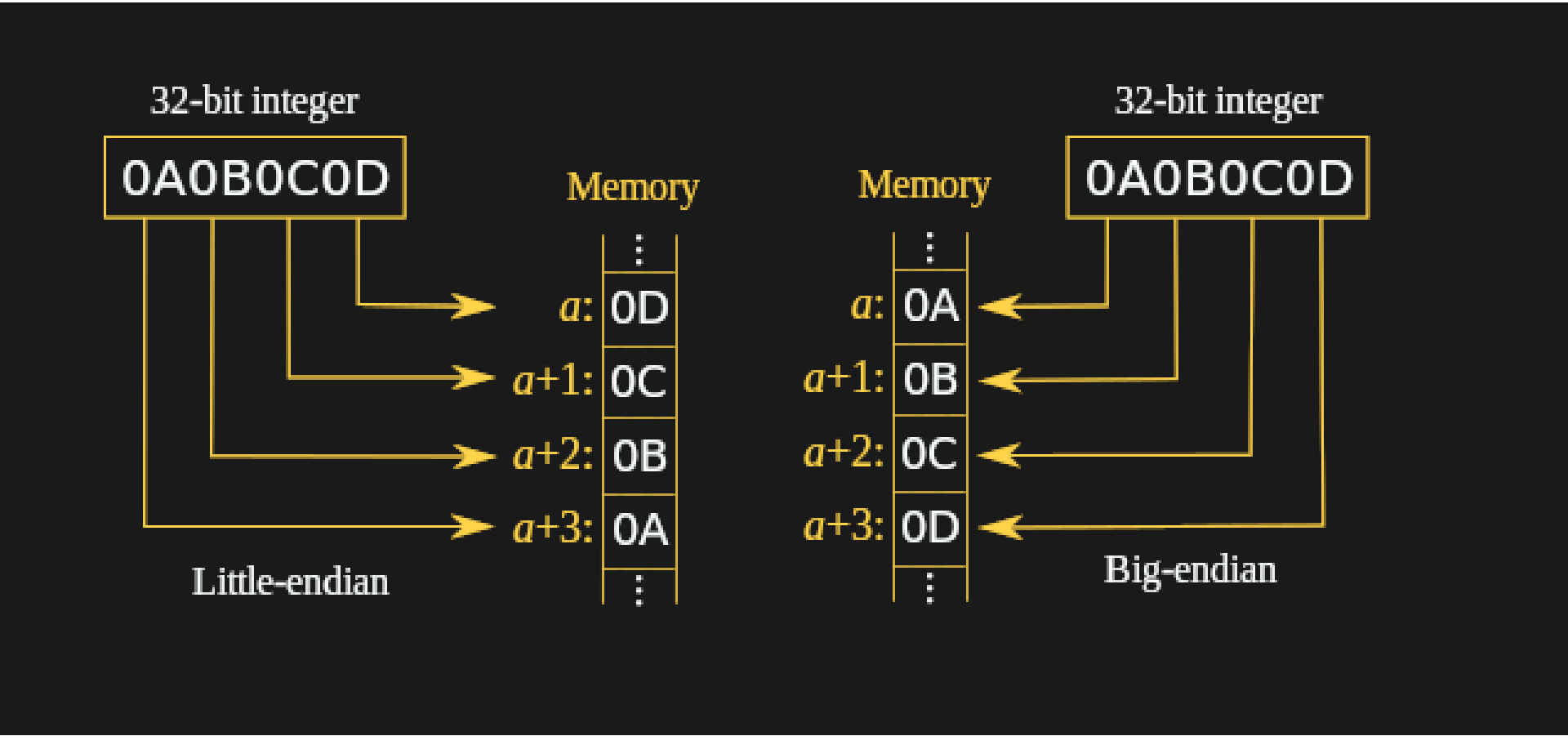
[Image Source]

90% of Assembly Codes



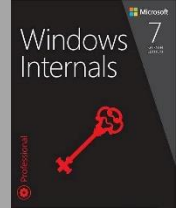
[Image Source]

Endianness

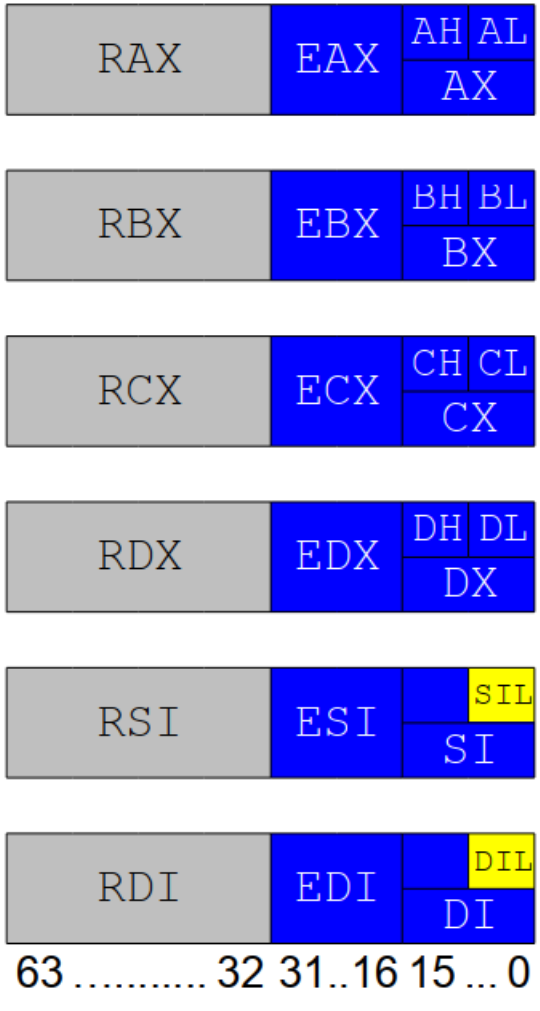


[Image Source]

x64 Registers

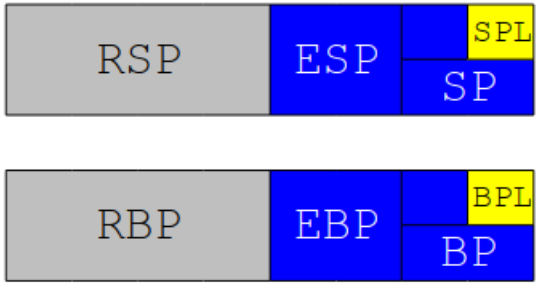


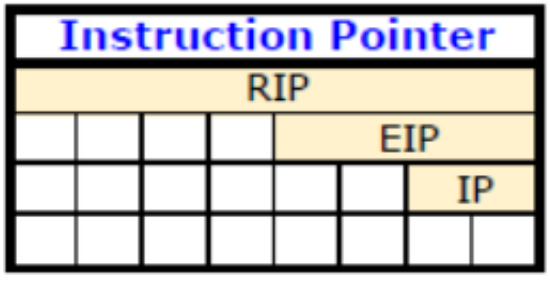
General-purpose regs:



Source

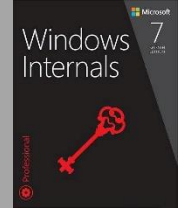
Stack management:



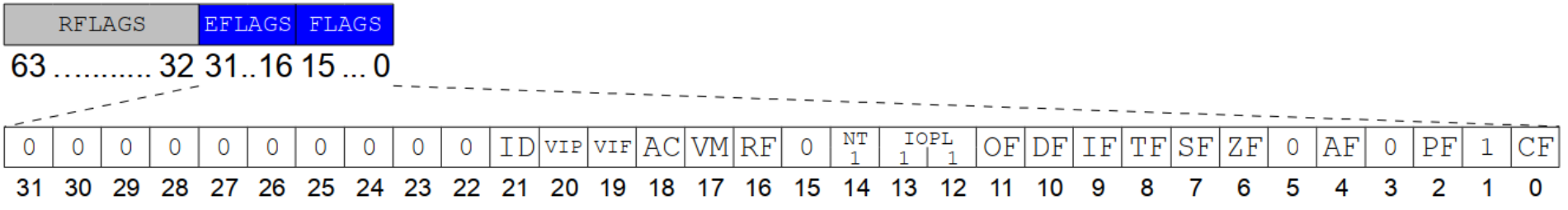


Source

x64 Registers



Flags register:



64-bit mode registers: