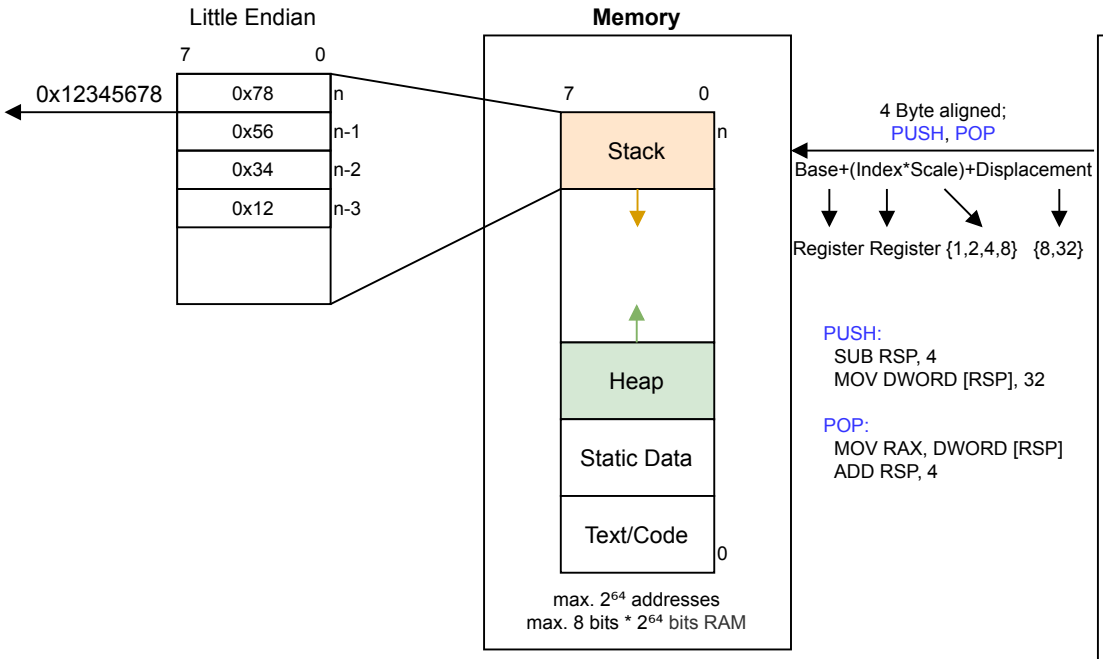
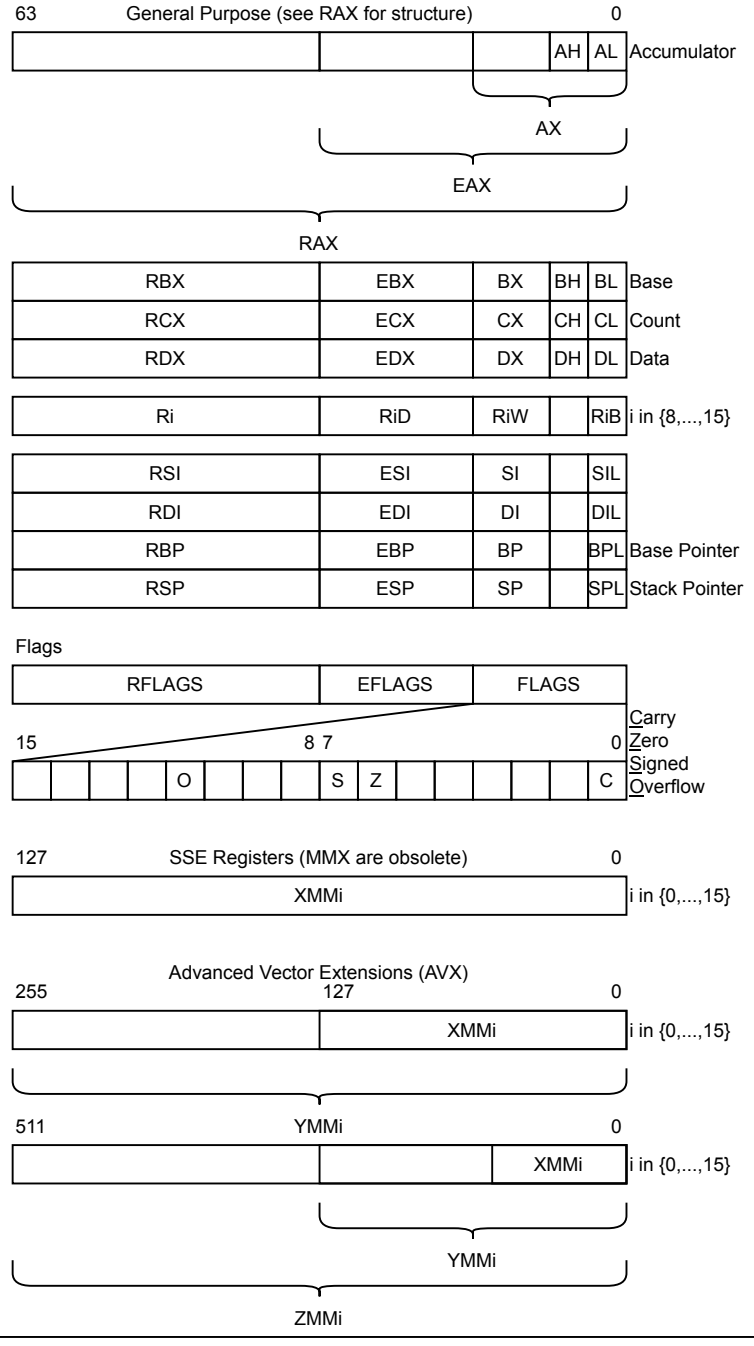
x64 Cheatsheet

by Ludwig Kratzl





Calling Conventions

Argument 1	RDI	Caller-saved
Argument 2	RSI	Caller-saved
Argument 3	RDX	Caller-saved
Argument 4	RCX	Caller-saved
Argument 5	R8	Caller-saved
Argument 6	R9	Caller-saved
Return Value	RAX	Caller-saved

Calling Conventions (floating point)

Argument 1-8	XMM0-7	Caller-saved

Callee/Caller-saved registers

RBX	Callee-saved
RBP	Callee-saved
RSP	Callee-saved
R10,R12	Caller-saved
R12-15	Callee-saved

7th argument on stack (64 Bit arguments/variables)

...	
RBP + 16	8th parameter
RBP + 8	7th parameter
RBP (old)	
RBP - 8	local variable 1
RBP - 16	local variable 2
...	

Words and sizes (NASM)

BYTE	DB	RESB	8 bits
WORD	DW	RESW	16 bits
DWORD	DD	RESD	32 bits
QWORD	DQ	RESQ	64 bits
OWORD	DO	RESO	128 bits
YWORD	DY	RESY	256 bits
ZWORD	DZ	RESZ	512 bits