# 注解：

# 第七章：栈帧

EBP的作用：当程序运行时，ESP的值会随时变化，所以需要在调用函数时用栈帧去保存函数起始地址，作为基准点。所以在函数调用过程中，第一条指令基本上都是PUSH EBP（55），函数RET之前会POP EBP（5D）

1. 生成栈帧（EBP）的代码有两行

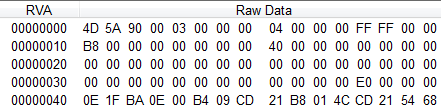
PUSH EBP

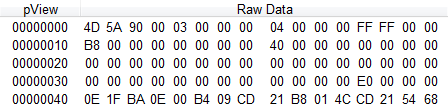
MOV EBP， ESP

# 第13章：PE文件结构

DOS头部是PE文件的前64个字节，偏移为00000000——0000003F。

这里的偏移指offset，由于第一个节区imagebase = 0，所以offset 和RVA相等。





DOS头最后8个字节是NT头的偏移，这里是000000E0，小端地址表示法。

IAT的偏移在Image\_potional\_header中。

