

Disassembling a 32-bit Windows Program

Register	Value	Register	Value
eax		ebp	0x7ffec
ebx		esp	0x7ff20
ecx		esi	
edx		edi	
xmm0			

Start Address	End Address	Contents
0x7fff4	0x7fff7	
0x7fff0	0x7fff3	
0x7ffec	0x7ffef	<i>old ebp</i>
...
0x7ff24	0x7ff27	
0x7ff20	0x7ff23	
0x7ff1c	0x7ff1f	
0x7ff18	0x7ff1b	
0x7ff14	0x7ff17	
0x7ff10	0x7ff13	
0x7ff0c	0x7ff0f	
0x7ff08	0x7ff0b	
0x7ff04	0x7ff07	
0x7ff00	0x7ff03	
0x7fefc	0x7fefb	
0x7fef8	0x7fefb	
0x7fef4	0x7fef7	

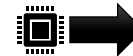
```
int main() {  
    printf("%f\n", end_speed(50.0, .75, 12, 0xdeadb));  
    return 0;  
}
```



main:

```
    push    ebp  
    mov     ebp, esp
```

...



```
    push    0x0  
    push    0xdeadb  
    sub     esp, 0x8  
    movsd   xmm0, QWORD PTR ds:0x417b68  
    movsd   QWORD PTR [esp], xmm0  
    sub     esp, 0x8  
    movsd   xmm0, QWORD PTR ds:0x417b38  
    movsd   QWORD PTR [esp], xmm0  
    sub     esp, 0x8  
    movsd   xmm0, QWORD PTR ds:0x417b78  
    movsd   QWORD PTR [esp], xmm0  
    call    0x411136
```