





Practice: Disassembling a 64-bit Function Call Idiom

Given the information presented here about a **64-bit ELF** program paused as it is about to execute the instruction labeled by  , complete the chart and identify the contents of register `xmm0` when the program reaches the instruction labeled by  . Reference information about the calling conventions for the System V (Linux) ABI can be found here: https://wiki.osdev.org/System_V_ABI#x86-64. The reference for the semantics of x86-64 instructions can be found here: <https://cdrdv2-public.intel.com/774492/325383-sdm-vol-2abcd.pdf>.

Registers

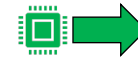
Register	Value	Register	Value
rax		rbp	0x7ff50
rbx		rsp	0x7ff20
rcx		rsi	
rdx		rdi	
xmm0		xmm1	


Stack Memory

Start Address	End Address	Contents
0x7ff30	0x7ff37	
0x7ff28	0x7ff2f	
0x7ff20	0x7ff27	
0x7ff18	0x7ff1f	
0x7ff10	0x7ff17	
0x7ff08	0x7ff0f	
0x7ff00	0x7ff07	
0x7fef8	0x7fef7	
0x7fee0	0x7fee7	
0x7fee8	0x7feef	
0x7fee0	0x7fee7	
0x7fed8	0x7fedf	

Program

```
401110: push    rbp
401111: mov     rbp, rsp
401114: mov     DWORD PTR [rbp-0x4], edi
401117: movsd   QWORD PTR [rbp-0x10], xmm0
40111c: cvtsi2sd xmm0, DWORD PTR [rbp-0x4]
401121: mulsd   xmm0, QWORD PTR [rbp-0x10]
401126: pop     rbp
401127: ret
```



```
...
401130: push    rbp
401131: mov     rbp, rsp
401134: sub     rsp, 0x10
401138: mov     DWORD PTR [rbp-0x4], 0x0
40113f: mov     edi, 0x5
401144: movsd   xmm0, QWORD PTR [rip+0xec4]
40114c: call    401110
 401151: movsd   QWORD PTR [rbp-0x10], xmm0
```

On-Disk Data (in hexdump -C format)

```
00001ff0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00002000  01 00 02 00 00 00 00 00 00 00 00 00 00 31 40     |.....1@|
00002010  01 1b 03 3b 34 00 00 00 05 00 00 00 10 f0 ff ff   |...;4.....|
00002020  68 00 00 00 20 f0 ff ff 90 00 00 00 30 f0 ff ff   |h... ..0...|
```

ELF Header Information

There are 33 section headers, starting at offset 0x5c48:

Section Headers:

[Nr]	Name	Type	Address	Offset
	Size	EntSize	Flags Link Info Align	
[14]	.rodata	PROGBITS	0000000000402000	00002000
	0000000000000018	0000000000000000	A 0 0	8