- We can point the RIP (x64 bit instruction pointer register) to a location that contains a micro instruction that we want to execute followed by a ***RET***

```
f7 c7 07 00 00 00        test $0x00000007, %edi
0f 95 45 c3              setnzb -61(%ebp)
```

Byte Shift

[redacted]

[redacted]

[redacted]

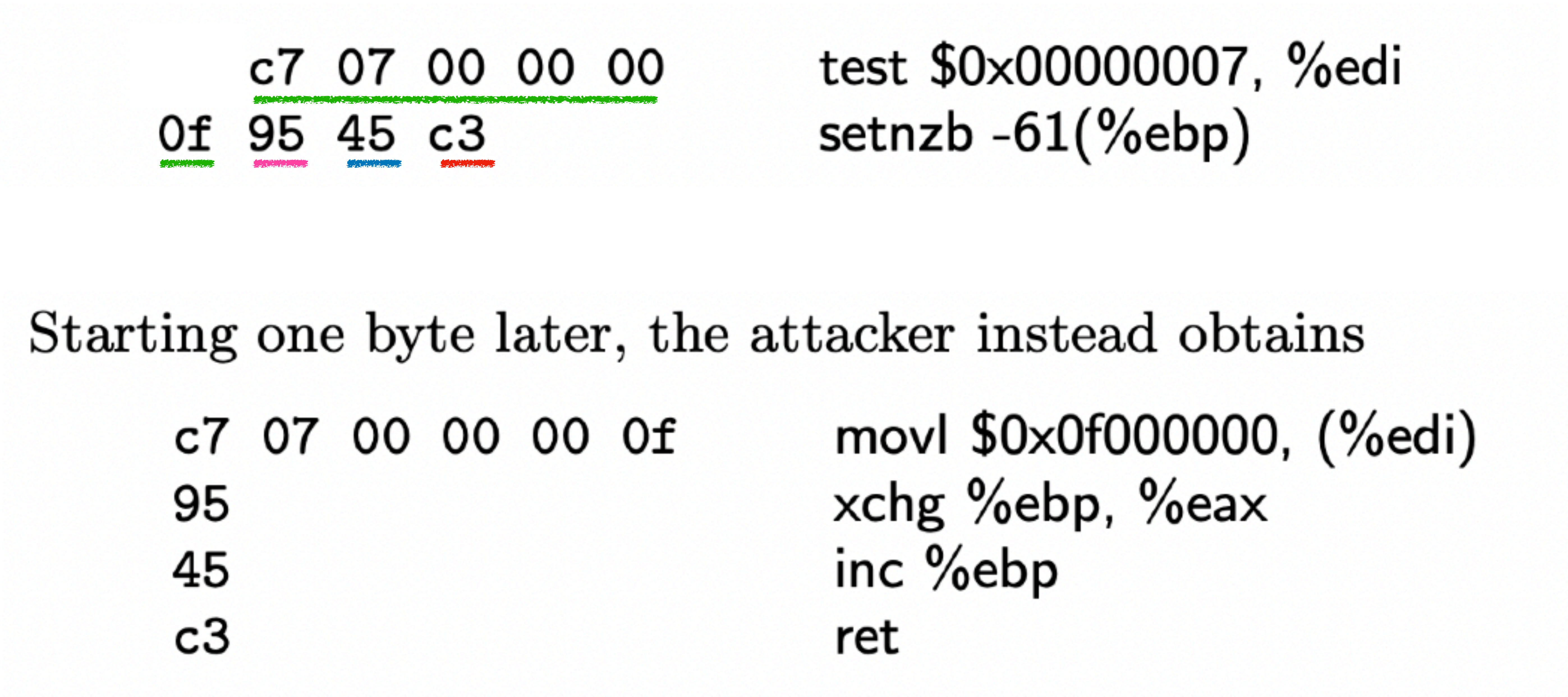
[redacted]

Starting one byte later, the attacker instead obtains

```
c7 07 00 00 00 0f        movl $0x0f000000, (%edi)
95                       xchg %ebp, %eax
45                       inc %ebp
c3                       ret
```

Byte Shift

- We can point the RIP (x64 bit instruction pointer register) to a location that contains a micro instruction that we want to execute followed by a ***RET***



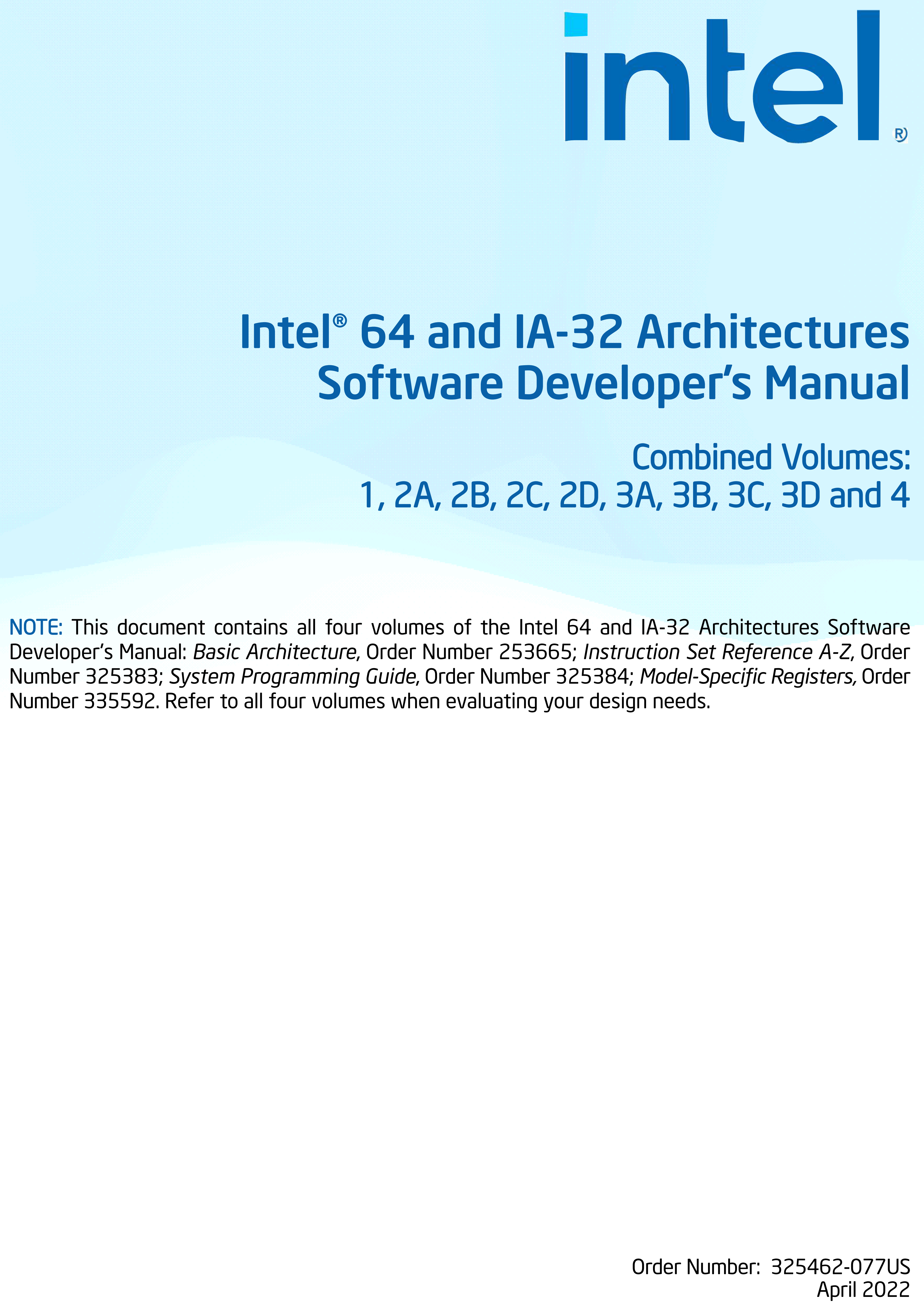
```
   c7 07 00 00 00      test $0x00000007, %edi
0f 95 45 c3            setnzb -61(%ebp)
```

Starting one byte later, the attacker instead obtains

```
c7 07 00 00 00 0f      movl $0x0f000000, (%edi)
95                     xchg %ebp, %eax
45                     inc %ebp
c3                     ret
```

CISC is Complex for a reason

- Intel x86 (32+64) has over 2000 instructions [1]
- They maintain a 4000+ page manual for IA-32 Arch.



Intel® 64 and IA-32 Architectures Software Developer's Manual

Combined Volumes:
1, 2A, 2B, 2C, 2D, 3A, 3B, 3C, 3D and 4

NOTE: This document contains all four volumes of the Intel 64 and IA-32 Architectures Software Developer's Manual: *Basic Architecture*, Order Number 253665; *Instruction Set Reference A-Z*, Order Number 325383; *System Programming Guide*, Order Number 325384; *Model-Specific Registers*, Order Number 335592. Refer to all four volumes when evaluating your design needs.

Order Number: 325462-077US
April 2022

[1] https://stefanheule.com/blog/how-many-x86-64-instructions-are-there-anyway/