

	Source	Dest	Src, Dest	C Analog
movq	<i>Imm</i>	<i>Reg</i>	movq \$0x4, %rax	temp = 0x4;
		<i>Mem</i>	movq \$-147, (%rax)	*p = -147;
	<i>Reg</i>	<i>Reg</i>	movq %rax, %rdx	temp2 = temp1;
		<i>Mem</i>	movq %rax, (%rdx)	*p = temp;
	<i>Mem</i>	<i>Reg</i>	movq (%rax), %rdx	temp = *p;

x86-64 Integer Registers

%rax	%eax	%r8	%r8d
%rbx	%ebx	%r9	%r9d
%rcx	%ecx	%r10	%r10d
%rdx	%edx	%r11	%r11d
%rsi	%esi	%r12	%r12d
%rdi	%edi	%r13	%r13d
%rsp	%esp	%r14	%r14d
%rbp	%ebp	%r15	%r15d

IA32 Registers

general purpose	%eax	%ax	%ah	%al
	%ecx	%cx	%ch	%cl
	%edx	%dx	%dh	%dl
	%ebx	%bx	%bh	%bl
	%esi	%si		
	%edi	%di		
	%esp	%sp		
	%ebp	%bp		

D(Rb,Ri,S)

Mem[Reg[Rb]+S*Reg[Ri]+ D]

- ⌚ D: Constant “displacement” 1, 2, or 4 bytes
- ⌚ Rb: Base register: Any of 16 integer registers
- ⌚ Ri: Index register: Any, except for **%rsp**
- ⌚ S: Scale: 1, 2, 4, or 8 (*why these numbers?*)

```

#include <stdlib.h>
#include <stdio.h>

int main( int argc, const char* argv[] )
{
    int x,y;

    short z;
    int *ptr;

    x=atoi(argv[1]);
    y=atoi(argv[2]);

    ptr=&x;

    (*ptr)++;
    ptr++;

    x+=y*4;
    z=x;

    printf("%lx %x\n",ptr,z);

    return x;
}

```

```

000000000040057d <main>:
40057d: 53                push    %rbx
40057e: 48 83 ec 10       sub     $0x10,%rsp
400582: 48 89 f3          mov     %rsi,%rbx
400585: 48 8b 7e 08       mov     0x8(%rsi),%rdi
400589: ba 0a 00 00 00    mov     $0xa,%edx
40058e: be 00 00 00 00    mov     $0x0,%esi
400593: e8 e8 fe ff ff   callq  400480 <strtol@plt>
400598: 89 44 24 0c       mov     %eax,0xc(%rsp)
40059c: 48 8b 7b 10       mov     0x10(%rbx),%rdi
4005a0: ba 0a 00 00 00    mov     $0xa,%edx
4005a5: be 00 00 00 00    mov     $0x0,%esi
4005aa: e8 d1 fe ff ff   callq  400480 <strtol@plt>
4005af: 8b 54 24 0c       mov     0xc(%rsp),%edx
4005b3: 8d 54 82 01       lea     0x1(%rdx,%rax,4),%edx
4005b7: 89 54 24 0c       mov     %edx,0xc(%rsp)
4005bb: 0f bf d2          movswl  %dx,%edx
4005be: 48 8d 74 24 10    lea     0x10(%rsp),%rsi
4005c3: bf 70 06 40 00    mov     $0x400670,%edi
4005c8: b8 00 00 00 00    mov     $0x0,%eax
4005cd: e8 7e fe ff ff   callq  400450 <printf@plt>
4005d2: 8b 44 24 0c       mov     0xc(%rsp),%eax
4005d6: 48 83 c4 10       add     $0x10,%rsp
4005da: 5b               pop     %rbx
4005db: c3               retq
4005dc: 0f 1f 40 00       nopl    0x0(%rax)

```

```
[reinman@lnxsr06 ~/code]$ gdb a.out
GNU gdb (GDB) Red Hat Enterprise Linux 7.6.1-12
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://www.gnu.org/licenses/gpl.html>
This is free software: you are free to change a copy of the program.
There is NO WARRANTY, to the extent permitted by law.
This GDB was configured as "x86_64-redhat-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /w/fac.3/cs/reinman/code/a.out...
(gdb) break *0x4005af
Breakpoint 1 at 0x4005af
(gdb) run 42 7
```

```
(gdb) i r
rax            0x7          7
rbx            0x7fffffff1a8    140737488347560
rcx            0x0           0
rdx            0xa          10
rsi            0x0           0
rdi            0x1999999999999999    18446744073709551615
rbp            0x0           0
rsp            0x7fffffff0b0    0x7fffffff0b0
r8             0x7ffff7dd5060    140737351864416
r9             0x7fffffff4a2    140737488348322
r10            0x7          7
r11            0x0           0
r12            0x400490 4195472
r13            0x7fffffff1a0    140737488347552
r14            0x0           0
r15            0x0           0
rip            0x4005af 0x4005af <main+50>
```

```
000000000040057d <main>:
40057d: 53                      push    %rbx
40057e: 48 83 ec 10             sub     $0x10,%rsp
400582: 48 89 f3                mov     %rsi,%rbx
400585: 48 8b 7e 08             mov     0x8(%rsi),%rdi
400589: ba 0a 00 00 00          mov     $0xa,%edx
40058e: be 00 00 00 00          mov     $0x0,%esi
400593: e8 e8 fe ff ff          callq   400480 <strtol@plt>
400598: 89 44 24 0c             mov     %eax,0xc(%rsp)
40059c: 48 8b 7b 10             mov     0x10(%rbx),%rdi
4005a0: ba 0a 00 00 00          mov     $0xa,%edx
4005a5: be 00 00 00 00          mov     $0x0,%esi
4005aa: e8 d1 fe ff ff          callq   400480 <strtol@plt>
4005af: 8b 54 24 0c             mov     0xc(%rsp),%edx
4005b3: 8d 54 82 01             lea     0x1(%rdx,%rax,4),%edx
4005b7: 89 54 24 0c             mov     %edx,0xc(%rsp)
4005bb: 0f bf d2                movswl  %dx,%edx
4005be: 48 8d 74 24 10          lea     0x10(%rsp),%rsi
4005c3: bf 70 06 40 00          mov     $0x400670,%edi
4005c8: b8 00 00 00 00          mov     $0x0,%eax
4005cd: e8 7e fe ff ff          callq   400450 <printf@plt>
4005d2: 8b 44 24 0c             mov     0xc(%rsp),%eax
4005d6: 48 83 c4 10             add     $0x10,%rsp
4005da: 5b                      pop     %rbx
4005db: c3                      retq
4005dc: 0f 1f 40 00             nopl    0x0(%rax)
```

```
(gdb) i r
rax      0x7      7
rbx      0x7fffffff1a8    140737488347560
rcx      0x0      0
rdx      0xa      10
rsi      0x0      0
rdi      0x1999999999999999    18446744073709551615
rbp      0x0      0x0
rsp      0x7fffffff0b0    0x7fffffff0b0
r8       0x7ffff7dd5060    140737351864416
r9       0x7fffffff4a2    140737488348322
r10      0x7      7
r11      0x0      0
r12      0x400490 4195472
r13      0x7fffffff1a0    140737488347552
r14      0x0      0
r15      0x0      0
rip      0x4005af 0x4005af <main+50>
```

```
00000000040057d <main>:
40057d: 53                push    %rbx
40057e: 48 83 ec 10       sub     $0x10,%rsp
400582: 48 89 f3          mov     %rsi,%rbx
400585: 48 8b 7e 08       mov     0x8(%rsi),%rdi
400589: ba 0a 00 00 00    mov     $0xa,%edx
40058e: be 00 00 00 00    mov     $0x0,%esi
400593: e8 e8 fe ff ff    callq   400480 <strtol@plt>
400598: 89 44 24 0c       mov     %eax,0xc(%rsp)
40059c: 48 8b 7b 10       mov     0x10(%rbx),%rdi
4005a0: ba 0a 00 00 00    mov     $0xa,%edx
4005a5: be 00 00 00 00    mov     $0x0,%esi
4005aa: e8 d1 fe ff ff    callq   400480 <strtol@plt>
4005af: 8b 54 24 0c       mov     0xc(%rsp),%edx
4005b3: 8d 54 82 01       lea     0x1(%rdx,%rax,4),%edx
4005b7: 89 54 24 0c       mov     %edx,0xc(%rsp)
4005bb: 0f bf d2          movswl  %dx,%edx
4005be: 48 8d 74 24 10    lea     0x10(%rsp),%rsi
4005c3: bf 70 06 40 00    mov     $0x400670,%edi
4005c8: b8 00 00 00 00    mov     $0x0,%eax
4005cd: e8 7e fe ff ff    callq   400450 <printf@plt>
4005d2: 8b 44 24 0c       mov     0xc(%rsp),%eax
4005d6: 48 83 c4 10       add     $0x10,%rsp
4005da: 5b                pop     %rbx
```

```
(gdb) x/32xb 0x7fffffff0b0
0x7fffffff0b0: 0xa0    0xe1    0xff    0xff    0xff    0x7f    0x00    0x00
0x7fffffff0b8: 0x00    0x00    0x00    0x00    0x2a    0x00    0x00    0x00
0x7fffffff0c0: 0x00    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffff0c8: 0x55    0xf5    0xa2    0xf7    0xff    0x7f    0x00    0x00
```

```

(gdb) si
0x00000000004005b3 in main ()
(gdb) i r
rax          0x7          7
rbx          0x7fffffff1a8    140737488347560
rcx          0x0          0
rdx          0x2a         42
rsi          0x0          0
rdi          0x1999999999999999 1844674
rbp          0x0          0x0
rsp          0x7fffffff0b0    0x7fffffff0b0
r8           0x7ffff7dd5060    140737351864416
r9           0x7fffffff4a2    140737488348322
r10          0x7          7
r11          0x0          0
r12          0x400490 4195472
r13          0x7fffffff1a0    140737488347552
r14          0x0          0
r15          0x0          0
rip          0x4005b3 0x4005b3 <main+54>

```

```

000000000040057d <main>:
40057d: 53                push    %rbx
40057e: 48 83 ec 10       sub     $0x10,%rsp
400582: 48 89 f3          mov     %rsi,%rbx
400585: 48 8b 7e 08       mov     0x8(%rsi),%rdi
400589: ba 0a 00 00 00    mov     $0xa,%edx
40058e: be 00 00 00 00    mov     $0x0,%esi
400593: e8 e8 fe ff ff    callq   400480 <strtol@plt>
400598: 89 44 24 0c       mov     %eax,0xc(%rsp)
40059c: 48 8b 7b 10       mov     0x10(%rbx),%rdi
4005a0: ba 0a 00 00 00    mov     $0xa,%edx
4005a5: be 00 00 00 00    mov     $0x0,%esi
4005aa: e8 d1 fe ff ff    callq   400480 <strtol@plt>
4005af: 8b 54 24 0c       mov     0xc(%rsp),%edx
4005b3: 8d 54 82 01       lea     0x1(%rdx,%rax,4),%edx
4005b7: 89 54 24 0c       mov     %edx,0xc(%rsp)
4005bb: 0f bf d2          movswl  %dx,%edx
4005be: 48 8d 74 24 10    lea     0x10(%rsp),%rsi
4005c3: bf 70 06 40 00    mov     $0x400670,%edi
4005c8: b8 00 00 00 00    mov     $0x0,%eax
4005cd: e8 7e fe ff ff    callq   400450 <printf@plt>
4005d2: 8b 44 24 0c       mov     0xc(%rsp),%eax
4005d6: 48 83 c4 10       add     $0x10,%rsp
4005da: 5b              pop     %rbx
4005db: c3              retq
4005dc: 0f 1f 40 00       nopl    0x0(%rax)

```



```
(gdb) si
0x0000000004005b7 in main ()
```

```
(gdb) i r
```

```
rax      0x7      7
rbx      0x7fffffffef1a8    140737
rcx      0x0      0
rdx      0x47      71
rsi      0x0      0
rdi      0x1999999999999999
rbp      0x0      0x0
rsp      0x7fffffffef0b0    0x7fff
r8       0x7ffff7dd5060    140737
r9       0x7fffffffef4a2    140737
r10      0x7      7
r11      0x0      0
r12      0x400490 4195472
r13      0x7fffffffef1a0    140737
r14      0x0      0
r15      0x0      0
rip      0x4005b7 0x4005b7 <main>
```

```
00000000040057d <main>:
```

```
40057d: 53                push    %rbx
40057e: 48 83 ec 10       sub     $0x10,%rsp
400582: 48 89 f3          mov     %rsi,%rbx
400585: 48 8b 7e 08       mov     0x8(%rsi),%rdi
400589: ba 0a 00 00 00    mov     $0xa,%edx
40058e: be 00 00 00 00    mov     $0x0,%esi
400593: e8 e8 fe ff ff   callq  400480 <strtol@plt>
400598: 89 44 24 0c       mov     %eax,0xc(%rsp)
40059c: 48 8b 7b 10       mov     0x10(%rbx),%rdi
4005a0: ba 0a 00 00 00    mov     $0xa,%edx
4005a5: be 00 00 00 00    mov     $0x0,%esi
4005aa: e8 d1 fe ff ff   callq  400480 <strtol@plt>
4005af: 8b 54 24 0c       mov     0xc(%rsp),%edx
4005b3: 8d 54 82 01       lea     0x1(%rdx,%rax,4),%edx
4005b7: 89 54 24 0c       mov     %edx,0xc(%rsp)
4005bb: 0f bf d2          movswl  %dx,%edx
4005be: 48 8d 74 24 10    lea     0x10(%rsp),%rsi
4005c3: bf 70 06 40 00    mov     $0x400670,%edi
4005c8: b8 00 00 00 00    mov     $0x0,%eax
4005cd: e8 7e fe ff ff   callq  400450 <printf@plt>
4005d2: 8b 44 24 0c       mov     0xc(%rsp),%eax
4005d6: 48 83 c4 10       add     $0x10,%rsp
4005da: 5b                pop     %rbx
```

```
(gdb) x/32xb 0x7fffffffef0b0
```

```
0x7fffffffef0b0: 0xa0    0xe1    0xff    0xff    0xff    0x7f    0x00    0x00
0x7fffffffef0b8: 0x00    0x00    0x00    0x00    0x2a    0x00    0x00    0x00
0x7fffffffef0c0: 0x00    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffef0c8: 0x55    0xf5    0xa2    0xf7    0xff    0x7f    0x00    0x00
```

```

(gdb) si
0x0000000004005bb in main ()
(gdb) i r
rax                0x7          7
rbx                0x7fffffff1a8    140737488
rcx                0x0            0
rdx                0x47           71
rsi                0x0            0
rdi                0x1999999999999999 1
rbp                0x0            0x0
rsp                0x7fffffff0b0    0x7fffffff
r8                 0x7ffff7dd5060    140737351
r9                 0x7fffffff4a2    140737488
r10                0x7            7
r11                0x0            0
r12                0x400490 4195472
r13                0x7fffffff1a0    140737488
r14                0x0            0
r15                0x0            0
rip                0x4005bb 0x4005bb <main+62>

```

00000000040057d <main>:

```

40057d: 53                push    %rbx
40057e: 48 83 ec 10       sub     $0x10,%rsp
400582: 48 89 f3          mov     %rsi,%rbx
400585: 48 8b 7e 08       mov     0x8(%rsi),%rdi
400589: ba 0a 00 00 00    mov     $0xa,%edx
40058e: be 00 00 00 00    mov     $0x0,%esi
400593: e8 e8 fe ff ff    callq   400480 <strtol@plt>
400598: 89 44 24 0c       mov     %eax,0xc(%rsp)
40059c: 48 8b 7b 10       mov     0x10(%rbx),%rdi
4005a0: ba 0a 00 00 00    mov     $0xa,%edx
4005a5: be 00 00 00 00    mov     $0x0,%esi
4005aa: e8 d1 fe ff ff    callq   400480 <strtol@plt>
4005af: 8b 54 24 0c       mov     0xc(%rsp),%edx
4005b3: 8d 54 82 01       lea     0x1(%rdx,%rax,4),%edx
4005b7: 89 54 24 0c       mov     %edx,0xc(%rsp)
4005bb: 0f bf d2          movswl  %dx,%edx
4005be: 48 8d 74 24 10    lea     0x10(%rsp),%rsi
4005c3: bf 70 06 40 00    mov     $0x400670,%edi
4005c8: b8 00 00 00 00    mov     $0x0,%eax
4005cd: e8 7e fe ff ff    callq   400450 <printf@plt>
4005d2: 8b 44 24 0c       mov     0xc(%rsp),%eax
4005d6: 48 83 c4 10       add     $0x10,%rsp
4005da: 5b                pop     %rbx

```

(gdb) x/32xb 0x7fffffff0b0

```

0x7fffffff0b0: 0xa0    0xe1    0xff    0xff    0xff    0x7f    0x00    0x00
0x7fffffff0b8: 0x00    0x00    0x00    0x00    0x47    0x00    0x00    0x00
0x7fffffff0c0: 0x00    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffff0c8: 0x55    0xf5    0xa2    0xf7    0xff    0x7f    0x00    0x00

```



```

(gdb) si
0x0000000004005be in main ()
(gdb) i r
rax            0x7          7
rbx            0x7fffffff1a8    14073748834756
rcx            0x0            0
rdx            0x47           71
rsi            0x0            0
rdi            0x1999999999999999 184467
rbp            0x0            0x0
rsp            0x7fffffff0b0    0x7fffffff0b0
r8             0x7ffff7dd5060    14073735186441
r9             0x7fffffff4a2    14073748834832
r10            0x7            7
r11            0x0            0
r12            0x400490 4195472
r13            0x7fffffff1a0    14073748834755
r14            0x0            0
r15            0x0            0
rip            0x4005be 0x4005be <main+65>

```

```

00000000040057d <main>:
40057d:      53                push    %rbx
40057e:      48 83 ec 10       sub     $0x10,%rsp
400582:      48 89 f3          mov     %rsi,%rbx
400585:      48 8b 7e 08       mov     0x8(%rsi),%rdi
400589:      ba 0a 00 00 00    mov     $0xa,%edx
40058e:      be 00 00 00 00    mov     $0x0,%esi
400593:      e8 e8 fe ff ff    callq   400480 <strtol@plt>
400598:      89 44 24 0c       mov     %eax,0xc(%rsp)
40059c:      48 8b 7b 10       mov     0x10(%rbx),%rdi
4005a0:      ba 0a 00 00 00    mov     $0xa,%edx
4005a5:      be 00 00 00 00    mov     $0x0,%esi
4005aa:      e8 d1 fe ff ff    callq   400480 <strtol@plt>
4005af:      8b 54 24 0c       mov     0xc(%rsp),%edx
4005b3:      8d 54 82 01       lea     0x1(%rdx,%rax,4),%edx
4005b7:      89 54 24 0c       mov     %edx,0xc(%rsp)
4005bb:      0f bf d2          movswl  %dx,%edx
4005be:      48 8d 74 24 10    lea     0x10(%rsp),%rsi
4005c3:      bf 70 06 40 00    mov     $0x400670,%edi
4005c8:      b8 00 00 00 00    mov     $0x0,%eax
4005cd:      e8 7e fe ff ff    callq   400450 <printf@plt>
4005d2:      8b 44 24 0c       mov     0xc(%rsp),%eax
4005d6:      48 83 c4 10       add     $0x10,%rsp
4005da:      5b                pop     %rbx
4005db:      c3                retq
4005dc:      0f 1f 40 00       nopl    0x0(%rax)

```

```

(gdb) si
0x00000000004005c3 in main ()
(gdb) i r
rax          0x7          7
rbx          0x7fffffff1a8    14073748834
rcx          0x0           0
rdx          0x47          71
rsi          0x7fffffff0c0    14073748834
rdi          0x1999999999999999 184
rbp          0x0           0x0
rsp          0x7fffffff0b0    0x7fffffff
r8           0x7ffff7dd5060    14073735186
r9           0x7fffffff4a2    14073748834
r10          0x7          7
r11          0x0           0
r12          0x400490 4195472
r13          0x7fffffff1a0    14073748834
r14          0x0           0
r15          0x0           0
rip          0x4005c3 0x4005c3 <main+70>

```

```

000000000040057d <main>:
40057d: 53                push    %rbx
40057e: 48 83 ec 10       sub     $0x10,%rsp
400582: 48 89 f3          mov     %rsi,%rbx
400585: 48 8b 7e 08       mov     0x8(%rsi),%rdi
400589: ba 0a 00 00 00    mov     $0xa,%edx
40058e: be 00 00 00 00    mov     $0x0,%esi
400593: e8 e8 fe ff ff    callq   400480 <strtol@plt>
400598: 89 44 24 0c       mov     %eax,0xc(%rsp)
40059c: 48 8b 7b 10       mov     0x10(%rbx),%rdi
4005a0: ba 0a 00 00 00    mov     $0xa,%edx
4005a5: be 00 00 00 00    mov     $0x0,%esi
4005aa: e8 d1 fe ff ff    callq   400480 <strtol@plt>
4005af: 8b 54 24 0c       mov     0xc(%rsp),%edx
4005b3: 8d 54 82 01       lea     0x1(%rdx,%rax,4),%edx
4005b7: 89 54 24 0c       mov     %edx,0xc(%rsp)
4005bb: 0f bf d2          movswl  %dx,%edx
4005be: 48 8d 74 24 10    lea     0x10(%rsp),%rsi
4005c3: bf 70 06 40 00    mov     $0x400670,%edi
4005c8: b8 00 00 00 00    mov     $0x0,%eax
4005cd: e8 7e fe ff ff    callq   400450 <printf@plt>
4005d2: 8b 44 24 0c       mov     0xc(%rsp),%eax
4005d6: 48 83 c4 10       add     $0x10,%rsp
4005da: 5b               pop     %rbx
4005db: c3               retq
4005dc: 0f 1f 40 00       nopl    0x0(%rax)

```

```
(gdb) si
0x0000000004005c8 in main ()
```

```
(gdb) i r
```

rax	0x7	7	
rbx	0x7fffffff	e1a8	140
rcx	0x0	0	
rdx	0x47	71	
rsi	0x7fffffff	e0c0	140
rdi	0x400670	4195952	
rbp	0x0	0x0	
rsp	0x7fffffff	e0b0	0x7
r8	0x7fffff	7dd5060	140
r9	0x7fffffff	e4a2	140
r10	0x7	7	
r11	0x0	0	
r12	0x400490	4195472	
r13	0x7fffffff	e1a0	140
r14	0x0	0	
r15	0x0	0	
rip	0x4005c8	0x4005c8	<main+75>

```
00000000040057d <main>:
```

40057d:	53	push	%rbx
40057e:	48 83 ec 10	sub	\$0x10,%rsp
400582:	48 89 f3	mov	%rsi,%rbx
400585:	48 8b 7e 08	mov	0x8(%rsi),%rdi
400589:	ba 0a 00 00 00	mov	\$0xa,%edx
40058e:	be 00 00 00 00	mov	\$0x0,%esi
400593:	e8 e8 fe ff ff	callq	400480 <strtol@plt>
400598:	89 44 24 0c	mov	%eax,0xc(%rsp)
40059c:	48 8b 7b 10	mov	0x10(%rbx),%rdi
4005a0:	ba 0a 00 00 00	mov	\$0xa,%edx
4005a5:	be 00 00 00 00	mov	\$0x0,%esi
4005aa:	e8 d1 fe ff ff	callq	400480 <strtol@plt>
4005af:	8b 54 24 0c	mov	0xc(%rsp),%edx
4005b3:	8d 54 82 01	lea	0x1(%rdx,%rax,4),%edx
4005b7:	89 54 24 0c	mov	%edx,0xc(%rsp)
4005bb:	0f bf d2	movswl	%dx,%edx
4005be:	48 8d 74 24 10	lea	0x10(%rsp),%rsi
4005c3:	bf 70 06 40 00	mov	\$0x400670,%edi
4005c8:	b8 00 00 00 00	mov	\$0x0,%eax
4005cd:	e8 7e fe ff ff	callq	400450 <printf@plt>
4005d2:	8b 44 24 0c	mov	0xc(%rsp),%eax
4005d6:	48 83 c4 10	add	\$0x10,%rsp
4005da:	5b	pop	%rbx
4005db:	c3	retq	
4005dc:	0f 1f 40 00	nopl	0x0(%rax)

```
(gdb) x/32bx 0x400670
```

```
0x400670:      0x25      0x6c      0x78      0x20      0x25      0x78      0x0a      0x00
0x400678:      0x01      0x1b      0x03      0x3b      0x34      0x00      0x00      0x00
0x400680:      0x05      0x00      0x00      0x00      0xc8      0xfd      0xff      0xff
0x400688:      0x80      0x00      0x00      0x00      0x18      0xfe      0xff      0xff
```

Contents of section .rodata:

```
400660 01000200 00000000 00000000 00000000 .....
400670 256c7820 25780a00          %lx %x..
```

ASCII Table

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	\$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(72	48	110	H	104	68	150	h
9	9	11		41	29	51)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	o
16	10	20		48	30	60	0	80	50	120	P	112	70	160	p
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	r
19	13	23		51	33	63	3	83	53	123	S	115	73	163	s
20	14	24		52	34	64	4	84	54	124	T	116	74	164	t
21	15	25		53	35	65	5	85	55	125	U	117	75	165	u
22	16	26		54	36	66	6	86	56	126	V	118	76	166	v
23	17	27		55	37	67	7	87	57	127	W	119	77	167	w
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	z
27	1B	33		59	3B	73	;	91	5B	133	[123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	
29	1D	35		61	3D	75	=	93	5D	135]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	

```
00000000040057d <main>:
40057d:      53                      push   %rbx
40057e:      48 83 ec 10             sub    $0x10,%rsp
400582:      48 89 f3                mov    %rsi,%rbx
400585:      48 8b 7e 08             mov    0x8(%rsi),%rdi
400589:      ba 0a 00 00 00         mov    $0xa,%edx
40058e:      be 00 00 00 00         mov    $0x0,%esi
400593:      e8 e8 fe ff ff         callq  400480 <strtol@plt>
400598:      89 44 24 0c             mov    %eax,0xc(%rsp)
40059c:      48 8b 7b 10             mov    0x10(%rbx),%rdi
4005a0:      ba 0a 00 00 00         mov    $0xa,%edx
4005a5:      be 00 00 00 00         mov    $0x0,%esi
4005aa:      e8 d1 fe ff ff         callq  400480 <strtol@plt>
4005af:      8b 54 24 0c             mov    0xc(%rsp),%edx
4005b3:      8d 54 82 01             lea    0x1(%rdx,%rax,4),%edx
4005b7:      89 54 24 0c             mov    %edx,0xc(%rsp)
4005bb:      0f bf d2                movswl %dx,%edx
4005be:      48 8d 74 24 10          lea    0x10(%rsp),%rsi
4005c3:      bf 70 06 40 00         mov    $0x400670,%edi
4005c8:      b8 00 00 00 00         mov    $0x0,%eax
4005cd:      e8 7e fe ff ff         callq  400450 <printf@plt>
4005d2:      8b 44 24 0c             mov    0xc(%rsp),%eax
4005d6:      48 83 c4 10             add    $0x10,%rsp
4005da:      5b                      pop     %rbx
4005db:      c3                      retq
4005dc:      0f 1f 40 00             nopl   0x0(%rax)
```

```
(gdb) c
c
Continuing.
7fffffffef0c0 47
```

```
00000000040057d <main>:
40057d: 53                                push    %rbx
40057e: 48 83 ec 10                       sub     $0x10,%rsp
400582: 48 89 f3                          mov     %rsi,%rbx
400585: 48 8b 7e 08                       mov     0x8(%rsi),%rdi
400589: ba 0a 00 00 00                   mov     $0xa,%edx
40058e: be 00 00 00 00                   mov     $0x0,%esi
400593: e8 e8 fe ff ff                   callq   400480 <strtol@plt>
400598: 89 44 24 0c                       mov     %eax,0xc(%rsp)
40059c: 48 8b 7b 10                       mov     0x10(%rbx),%rdi
4005a0: ba 0a 00 00 00                   mov     $0xa,%edx
4005a5: be 00 00 00 00                   mov     $0x0,%esi
4005aa: e8 d1 fe ff ff                   callq   400480 <strtol@plt>
4005af: 8b 54 24 0c                       mov     0xc(%rsp),%edx
4005b3: 8d 54 82 01                       lea     0x1(%rdx,%rax,4),%edx
4005b7: 89 54 24 0c                       mov     %edx,0xc(%rsp)
4005bb: 0f bf d2                          movswl  %dx,%edx
4005be: 48 8d 74 24 10                   lea     0x10(%rsp),%rsi
4005c3: bf 70 06 40 00                   mov     $0x400670,%edi
4005c8: b8 00 00 00 00                   mov     $0x0,%eax
4005cd: e8 7e fe ff ff                   callq   400450 <printf@plt>
4005d2: 8b 44 24 0c                       mov     0xc(%rsp),%eax
4005d6: 48 83 c4 10                       add     $0x10,%rsp
4005da: 5b                                pop     %rbx
4005db: c3                                retq
4005dc: 0f 1f 40 00                       nopl    0x0(%rax)
```