```
Source Dest Src,Dest C Analog

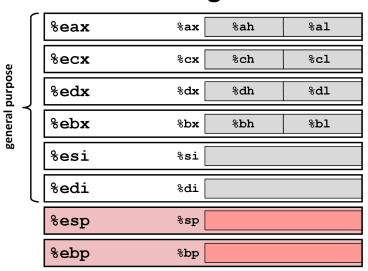
| Imm | Reg | movq $0x4, %rax | temp = 0x4; |
| Mem | movq $-147, (%rax) | *p = -147; |
| Reg | Reg | movq %rax, %rdx | temp2 = temp1; |
| Mem | movq %rax, (%rdx) | *p = temp; |
| Mem | Reg | movq (%rax), %rdx | temp = *p; |
```

## x86-64 Integer Registers

Sei irebisi
%eax
%ebx
%ecx
%edx
%esi
%edi
%esp
%ebp

%r8	%r8d
%r9	%r9d
%r10	%r10d
%r11	%r11d
%r12	%r12d
%r13	%r13d
%r14	%r14d
%r15	%r15d

## **IA32 Registers**



## 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

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

[[reinman@lnxsrv06 ~/code]\$ gdb a.out
GNU gdb (GDB) Red Hat Enterprise Linux 7.6.1-12
Copyright (C) 2013 Free Software Foundation, In
License GPLv3+: GNU GPL version 3 or later <htt< td=""></htt<>
This is free software: you are free to change a
There is NO WARRANTY, to the extent permitted b
and "show warranty" for details.
This GDB was configured as "x86_64-redhat-linux
For bug reporting instructions, please see:
<http: bugs="" gdb="" software="" www.gnu.org=""></http:>
Reading symbols from /w/fac.3/cs/reinman/code/a
[(gdb) break *0x4005af
Breakpoint 1 at 0x4005af
((gdb) run 42 7

[(gdb) i r				
rax	0x7	7		
rbx	0x7fffff	ffe1a8	140737488347	560
rcx	0x0	0		
rdx	0xa	10		
rsi	0x0	0		
rdi	0x1999999	99999999	99 1844	674407:
rbp	0x0	0x0		
rsp	0x7ffffff	ffe0b0	0x7fffffffe0	b0
r8	0x7ffff7c	dd5060	140737351864	416
r9	0x7ffffff	ffe4a2	140737488348	322
r10	0x7	7		
r11	0x0	0		
r12	0x400490	4195472		
r13	0x7fffff	ffe1a0	140737488347	552
r14	0x0	0		
r15	0x0	0		
rip	0x4005af	0x4005a	f <main+50></main+50>	

000000000004005	57d <main>:</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></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></strtol@plt>
4005af:	8b 54 24	0c	mov	0xc(%rsp),%edx
4005b3:	8d 54 82	01	lea	<pre>0x1(%rdx,%rax,4),%edx</pre>
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></printf@plt>
4005d2:	8b 44 24	0c	mov	0xc(%rsp),%eax
4005d6:	48 83 c4	10	add	\$0x10,%rsp
4005da:	5b		pop	%rbx
4005db:	с3		retq	
4005dc:	0f 1f 40	00	nopl	0x0(%rax)

```
000000000040057d <main>:
                                                 40057d:
                                                               53
                                                                                        push
                                                                                               %rbx
                                                 40057e:
                                                               48 83 ec 10
                                                                                        sub
                                                                                                $0x10,%rsp
                                                 400582:
                                                               48 89 f3
                                                                                        mov
                                                                                               %rsi,%rbx
                                                                                                0x8(%rsi),%rdi
                                                 400585:
                                                               48 8b 7e 08
                                                                                        mov
(gdb) i r
                                                 400589:
                                                               ba 0a 00 00 00
                                                                                                $0xa,%edx
                                                                                        mov
rax
              0x7
                                                 40058e:
                                                               be 00 00 00 00
rbx
              0x7ffffffffe1a8
                                                                                                $0x0,%esi
                             140737488347560
                                                                                        mov
                                                                                               400480 <strtol@plt>
rcx
              0x0
                                                 400593:
                                                               e8 e8 fe ff ff
                                                                                        callq
rdx
              0xa
                      10
                                                 400598:
                                                               89 44 24 0c
                                                                                               %eax,0xc(%rsp)
                                                                                        mov
rsi
              0x0
                                                 40059c:
                                                               48 8b 7b 10
                                                                                                0x10(%rbx),%rdi
                                                                                        mov
rdi
              0x199999999999999
                                     1844674407
                                                 4005a0:
                                                               ba 0a 00 00 00
                                                                                                $0xa,%edx
                                                                                        mov
rbp
              0x0
                      0x0
                                                 4005a5:
                                                                                                $0x0,%esi
                                                               be 00 00 00 00
                                                                                        mov
rsp
              0x7fffffffe0b0
                              0x7fffffffe0b0
                                                                                        callq
                                                                                               400480 <strtol@plt>
                                                 4005aa:
                                                               e8 d1 fe ff ff
r8
              0x7ffff7dd5060
                             140737351864416
                                                               8b 54 24 0c
                                                                                                0xc(%rsp),%edx
                                                 4005af:
                                                                                        mov
r9
              0x7fffffffe4a2
                             140737488348322
                                                 4005b3:
                                                               8d 54 82 01
                                                                                        lea
                                                                                                0x1(%rdx,%rax,4),%edx
r10
              0x7
                      7
r11
                                                 4005b7:
                                                               89 54 24 0c
                                                                                               %edx,0xc(%rsp)
              0x0
                                                                                        mov
              0x400490 4195472
r12
                                                 4005bb:
                                                               0f bf d2
                                                                                        movswl %dx,%edx
r13
              0x7fffffffe1a0
                             140737488347552
                                                 4005be:
                                                               48 8d 74 24 10
                                                                                                0x10(%rsp),%rsi
                                                                                        lea
r14
              0x0
                      0
                                                                                               $0x400670,%edi
                                                 4005c3:
                                                               bf 70 06 40 00
                                                                                        mov
r15
              0x0
                                                 4005c8:
                                                               b8 00 00 00 00
                                                                                                $0x0,%eax
                                                                                        mov
rip
              0x4005af 0x4005af <main+50>
                                                               e8 7e fe ff ff
                                                                                               400450 <printf@plt>
                                                 4005cd:
                                                                                        calla
                                                 4005d2:
                                                               8b 44 24 0c
                                                                                                0xc(%rsp),%eax
                                                                                        mov
                                                               48 83 c4 10
                                                 4005d6:
                                                                                                $0x10,%rsp
                                                                                        add
                                                 4005da:
                                                               5b
                                                                                               %rbx
                                                                                        pop
(gdb) x/32xb 0x7fffffffe0b0
0x7fffffffe0b0: 0xa0
                                           0xff
                                                      0xff
                                                                 0xff
                                                                            0x7f
                                                                                       0x00
                                                                                                  0x00
                                0xe1
0x7fffffffe0b8: 0x00
                                0x00
                                           0x00
                                                      0x00
                                                                 0x2a
                                                                            0x00
                                                                                       0x00
                                                                                                  0x00
0x7fffffffe0c0: 0x00
                                           0x00
                                                      0x00
                                                                                       0x00
                                0x00
                                                                 0x00
                                                                            0x00
                                                                                                  0x00
0x7fffffffe0c8: 0x55
                                0xf5
                                                                 0xff
                                                                            0x7f
                                                                                       0x00
                                           0xa2
                                                      0xf7
                                                                                                  0x00
```

rax	0x7	7	
rbx		ffffe1a8	140737488347560
rcx	0x0	0	
rdx	0x2a	42	
rsi	0x0	0	
rdi	0x1999	99999999	999 1844674
rbp	0x0	0×0	
rsp	0x7fff	ffffe0b0	0x7fffffffe0b0
r8	0x7fff	f7dd5060	140737351864416
r9	0x7fff	ffffe4a2	140737488348322
r10	0x7	7	
r11	0x0	0	
r12	0x4004	90 419547	2
r13	0x7fff	ffffe1a0	140737488347552
r14	0x0	0	
r15	0x0	0	
rip	0x4005	b3 0x4005	b3 <main+54></main+54>

	00000000000400	57d <main< th=""><th>&gt;:</th><th></th><th></th><th></th></main<>	>:			
	40057d:	53			push	%rbx
	40057e:	48 83 6	ec 10		sub	\$0x10,%rsp
	400582:	48 89 1	f3		mov	%rsi,%rbx
	400585:	48 8b 7	7e 08		mov	0x8(%rsi),%rdi
37488347560	400589:	ba 0a (	90 00	00	mov	\$0xa,%edx
	40058e:	be 00 (	90 00	00	mov	\$0x0,%esi
	400593:	e8 e8 1	fe ff	ff	callq	400480 <strtol@plt></strtol@plt>
	400598:	89 44 2	24 0c		mov	%eax,0xc(%rsp)
1844674	40059c:	48 8b 7	7b 10		mov	0x10(%rbx),%rdi
	4005a0:	ba 0a 6	90 00	00	mov	\$0xa,%edx
ffffffe0b0	4005a5:	be 00 (	90 00	00	mov	\$0x0,%esi
37351864416	4005aa:	e8 d1 1	fe ff	ff	callq	400480 <strtol@plt></strtol@plt>
37488348322	4005af:	8b 54 2	24 0c		mov	0xc(%rsp),%edx
	4005b3:	8d 54 8	32 01		lea	<pre>0x1(%rdx,%rax,4),%edx</pre>
	4005b7:	89 54 2	24 0c		mov	%edx,0xc(%rsp)
37488347552	4005bb:	0f bf d	12		movswl	%dx,%edx
3/40034/332	4005be:	48 8d 7	74 24	10	lea	0x10(%rsp),%rsi
	4005c3:	bf 70 (	96 40	00	mov	\$0x400670,%edi
in+54>	4005c8:	b8 00 6		00	mov	\$0x0,%eax
2111041	4005cd:	e8 7e 1		ff	callq	400450 <printf@plt></printf@plt>
	4005d2:	8b 44 2	24 0c		mov	0xc(%rsp),%eax
	4005d6:	48 83 0	c4 <b>10</b>		add	\$0x10,%rsp
	4005da:	5b			pop	%rbx
	4005db:	сЗ			retq	
	4005dc:	0f 1f 4	40 00		nopl	0x0(%rax)

(gdb) si				000000000004005	7d <mai< th=""><th>n&gt;:</th><th></th><th></th><th></th></mai<>	n>:			
				40057d:	53			push	%rbx
0x00000000000400	05D/ 1n ma	ain ()		40057e:	48 83	ec 1	0	sub	\$0x10,%rsp
[(gdb) i r				400582:	48 89	f3		mov	%rsi,%rbx
rax	0x7	7		400585:	48 8b			mov	0x8(%rsi),%rdi
rbx	0x7ffffff	ffe1a8	140737	400589:		<i>00 0</i>		mov	\$0xa,%edx
rcx	0x0	0		40058e:	be 00			mov	\$0x0,%esi
rdx	0x47	71		400593:		fe f		callq	400480 <strtol@plt></strtol@plt>
rsi	0x47	0		400598:	89 44			mov	%eax,0xc(%rsp)
	0x1999999		^	40059c:	48 8b			mov	0x10(%rbx),%rdi
rdi			9	4005a0:		00 0		mov	\$0xa,%edx
rbp	0x0	0x0		4005a5:	be 00			mov	\$0x0,%esi
rsp	0x7fffff		0x7fff	4005aa:		fe f		callq	400480 <strtol@plt></strtol@plt>
r8	0x7ffff7d	dd5060	140737	4005af: 4005b3:	8b 54 8d 54			mov lea	<pre>0xc(%rsp),%edx 0x1(%rdx,%rax,4),%edx</pre>
r9	0x7ffffff	ffe4a2	140737	4005b3: 4005b7:	89 54			mov	%edx,0xc(%rsp)
r10	0x7	7		4005b7:	0f bf		C		%dx,%edx
r11	0x0	0		4005bb:	48 8d		4 10	lea	0x10(%rsp),%rsi
r12	0x400490			4005c3:	bf 70			mov	\$0x400670,%edi
			1/0707	4005c8:	b8 00			mov	\$0x0,%eax
r13	0x7ffffff		140737	4005cd:	e8 7e			callq	400450 <printf@plt></printf@plt>
r14	0x0	0		4005d2:	8b 44			mov	0xc(%rsp),%eax
r15	0x0	0		4005d6:	48 83	c4 1	9	add	\$0x10,%rsp
rip	0x4005b7	0x4005b7	<main< td=""><td>4005da:</td><td>5b</td><td></td><td></td><td>pop</td><td>%rbx</td></main<>	4005da:	5b			pop	%rbx
(gdb) x/32xb	0x7fffff	ffe0b0							
0x7fffffffe0b	0: 0xa0	0xe1	0x-	ff 0xff	0x	ff	0x7f	0x00	0x06 <sup>''</sup>
0x7fffffffe0b	8: 0x00	0x00	0x6	00×0 0×00	0x	2a	0x00	0x00	0x06
0x7fffffffe0c	0: 0x00	0x00	0x6	00×0 0×00	0x	00	0x00	0x00	0x06
0x7fffffffe0c	8: 0x55	0xf5	0xa	a2 0xf7	0x	ff	0x7f	0x00	0x06

			000000000004	0057d <mair< th=""><th>n&gt;:</th><th></th><th></th><th></th><th></th></mair<>	n>:				
(gdb) si			40057d:	53		push	%rbx		
0×000000000	004005bb in main ()		40057e:	48 83	ec 10	sub	\$0x10,	%rsp	
(gdb) i r			400582:	48 89	f3	mov	%rsi,%	rbx	
rax	0x7 7		400585:	48 8b	7e 08	mov	0x8(%r	si),%rdi	
rbx	0x7fffffffe1a8	140737488	400589:		00 00 00	mov	\$0xa,%		
rcx	0x0 0		40058e:		00 00 00	mov	\$0x0,%		
rdx	0x47 71		400593:		fe ff ff	call		<pre><strtol@p< pre=""></strtol@p<></pre>	1t>
rsi	0x0 0		400598:		24 0c	mov		xc(%rsp)	
rdi	0x199999999999	999 1	40059c:	48 8b		mov		rbx),%rdi	
	0x1,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	777 <u>I</u> (	4005a0:		00 00 00	mov	\$0xa,%		
rbp		0.75555	4005a5:		00 00 00	mov	\$0x0,%		
rsp	0x7fffffffe0b0	0x7ffffff	4005aa:		fe ff ff	call		<pre><strtol@p< pre=""></strtol@p<></pre>	lt>
r8	0x7ffff7dd5060	140737351	4005af:		24 0c	mov		sp),%edx	
r9	0x7fffffffe4a2	140737488	4005b3:		82 01	lea		dx,%rax,4)	,%edx
r10	0x7 7		4005b7:	89 54		mov		xc(%rsp)	
r11	0×0 0		4005bb:	0f bf			wl %dx,%e		
r12	0x400490 419547	2	4005be:		74 24 10	lea		rsp),%rsi	
r13	0x7fffffffe1a0	140737488	4005c3:		06 40 00	mov		670,%edi	
r14	0x0 0		4005c8:		00 00 00	mov	\$0x0,%		7.4.
r15	0x0 0		4005cd:		fe ff ff	call		<pre><pre><pre><pre></pre></pre></pre></pre>	Tt>
rip	0x4005bb 0x4005	bb <main+62< td=""><td>4005d2:</td><td></td><td>24 0c</td><td>mov</td><td></td><td>sp),%eax</td><td></td></main+62<>	4005d2:		24 0c	mov		sp),%eax	
p			4005d6: 4005da:	48 83 5b	C4 10	add	\$0x10, %rbx	%rsp	
(gdb	) x/32xb 0x7ffff	fffe0b0	4иизна :	<u> </u>			%/UX		
0x7f	ffffffe0b0: 0xa0	0xe1	0xff	0xff	0xff	0x7f	0x00	0x00	
0x7f	ffffffe0b8: 0x00	0×00	0x00	0x00	0x47	0x00	0x00	0x00	
0x7f	ffffffe0c0: 0x00	0×00	0x00	0x00	0x00	0×00	0x00	0x00	
0x7f	ffffffe0c8: 0x55	0xf5	0xa2	0xf7	0xff	0x7f	0x00	0x00	

		0000000000400	J/u \IIIaii/.	
		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
[(gdb) si		400589:	ba 0a 00 00 00	mov \$0xa,%edx
_	05be in main ()	40058e:	be 00 00 00 00	mov \$0x0,%esi
(gdb) i r	JOBE III IIIIIII ()	400593:	e8 e8 fe ff ff	callq 400480 <strtol@plt></strtol@plt>
rax	0x7 7	400598:	89 44 24 0c	mov %eax,0xc(%rsp)
rbx	0x7fffffffe1a8 14073748834756	40059c:	48 8b 7b 10	mov 0x10(%rbx),%rdi
rcx	0x0 0	4005a0:	ba 0a 00 00 00	mov \$0xa,%edx
rdx	0x47 71	4005a5:	be 00 00 00 00	mov \$0x0,%esi
rsi	0x0 0	4005aa:	e8 d1 fe ff ff	callq 400480 <strtol@plt></strtol@plt>
rdi	0x1999999999999999999999999999999999999	4005af:	8b 54 24 0c	mov 0xc(%rsp),%edx
rbp	0x0 0x0	4005b3:	8d 54 82 <b>0</b> 1	lea 0x1(%rdx,%rax,4),%edx
rsp	0x7fffffffe0b0 0x7fffffffe0b0	4005b7:	89 54 24 0c	mov %edx,0xc(%rsp)
r8	0x7ffff7dd5060 14073735186441	4005bb:	0f bf d2	movswl %dx,%edx
r9	0x7fffffffe4a2 14073748834832	4005be:	48 8d 74 24 10	lea 0x10(%rsp),%rsi
r10	0x7 7	4005c3:	bf 70 06 40 00	mov \$0x400670,%edi
r11	0x0 0	4005c8:	b8 00 00 00 00	mov \$0x0,%eax
r12	0x400490 4195472	4005cd:	e8 7e fe ff ff	callq 400450 <printf@plt></printf@plt>
r13	0x7fffffffe1a0 14073748834755	4005d2:	8b 44 24 0c	mov 0xc(%rsp),%eax
r14	0x0 0	4005d6:	48 83 c4 10	add \$0x10,%rsp
r15	0x0 0	4005da:	5b	pop %rbx
rip	0x4005be 0x4005be <main+65></main+65>	4005db:	c3	retq
		4005dc:	0f 1f 40 00	nopl 0x0(%rax)

000000000040057d <main>:

		4005/d:	53	pusn	%
(gdb) si		40057e:	48 83 ec 10	sub	\$
	4005c3 in main ()	400582:	48 89 f3	mov	%
	4005C3 III IIIaIII ()	400585:	48 8b 7e 08	mov	0
[(gdb) i r		400589:	ba 0a 00 00 00	mov	\$
rax	0x7 7	40058e:	be 00 00 00 00	mov	\$
rbx	0x7fffffffe1a8 14073748834	400593:	e8 e8 fe ff ff	callq	4
rcx	0x0 0	400598:	89 44 24 0c	mov	%
rdx	0x47 71	40059c:	48 8b 7b 10	mov	0
rsi	0x7fffffffe0c0 14073748834	4005a0:	ba 0a 00 00 00	mov	\$
rdi	0x199999999999999 184	4005a5:	be 00 00 00 00	mov	\$
rbp	0x0 0x0	4005aa:	e8 d1 fe ff ff	callq	4
rsp	0x7fffffffe0b0 0x7fffffffe	4005af:	8b 54 24 0c	mov	0
r8	0x7ffff7dd5060 14073735186	4005b3:	8d 54 82 01	lea	0
r9	0x7ffffffffe4a2 14073748834	4005b7:	89 54 24 0c	mov	%
r10	0x7 7	4005bb:	0f bf d2	movswl	%
r11	0x0 0	4005be:	48 8d 74 24 10	lea	0
r12	0x400490 4195472	4005c3:	bf 70 06 40 00	mov	\$
r13	0x7ffffffffe1a0 14073748834	4005c8:	b8 00 00 00 00	mov	\$
r14	0x0 0	4005cd:	e8 7e fe ff ff	callq	4
r15	0x0 0	4005d2:	8b 44 24 0c	mov	0
rip	0x4005c3 0x4005c3 <main+70></main+70>	4005d6:	48 83 c4 10	add	\$
		4005da:	5b	pop	%

	00000000000400	57d <ma< th=""><th>in&gt;:</th><th></th><th></th><th></th><th></th></ma<>	in>:				
	40057d:	53				push	%rbx
	40057e:	48 8	33 ec	10		sub	\$0x10,%rsp
	400582:	48 8	89 f3			mov	%rsi,%rbx
	400585:	48 8	3b 7e	80		mov	0x8(%rsi),%rdi
	400589:	ba 0	a 00	00	00	mov	\$0xa,%edx
,	40058e:	be 0	00	00	00	mov	\$0x0,%esi
34	400593:	e8 e	8 fe	ff	ff	callq	400480 <strtol@plt></strtol@plt>
	400598:	89 4	4 24	0c		mov	<pre>%eax,0xc(%rsp)</pre>
	40059c:	48 8	3b 7b	10		mov	0x10(%rbx),%rdi
34	1000401	ba 0	a 00	00	00	mov	\$0xa,%edx
34	4005a5:	be 0	00	00	00	mov	\$0x0,%esi
	4005aa:	e8 d	l1 fe	ff	ff	callq	400480 <strtol@plt></strtol@plt>
Ēе	4005af:	8b 5	4 24	0c		mov	0xc(%rsp),%edx
36	4005b3:	8d 5	4 82	01		lea	<pre>0x1(%rdx,%rax,4),%edx</pre>
34	4005b7:	89 5	4 24	0c		mov	<pre>%edx,0xc(%rsp)</pre>
	4005bb:	0f b	of d2			movswl	%dx,%edx
	4005be:	48 8	3d 74	24	10	lea	0x10(%rsp),%rsi
	4005c3:	bf 7	0 06	40	00	mov	\$0x400670,%edi
34	4005c8:	b8 0	00	00	00	mov	\$0x0,%eax
	4005cd:	e8 7	'e fe	ff	ff	callq	400450 <printf@plt></printf@plt>
	4005d2:		4 24			mov	0xc(%rsp),%eax
	4005d6:	48 8	33 c4	10		add	\$0x10,%rsp
	4005da:	5b				pop	%rbx
	4005db:	сЗ				retq	
	4005dc:	0f 1	f 40	00		nopl	0x0(%rax)

```
000000000040057d <main>:
                                               40057d:
                                                             53
                                                                                    push
                                                                                           %rbx
(qdb) si
                                               40057e:
                                                             48 83 ec 10
                                                                                           $0x10,%rsp
                                                                                    sub
                                                            48 89 f3
                                               400582:
                                                                                           %rsi,%rbx
                                                                                    mov
0x000000000004005c8 in main ()
                                                                                           0x8(%rsi),%rdi
                                               400585:
                                                             48 8b 7e 08
                                                                                    mov
(gdb) i r
                                                             ba 0a 00 00 00
                                               400589:
                                                                                           $0xa,%edx
                                                                                    mov
                               7
                   0x7
                                               40058e:
                                                            be 00 00 00 00
                                                                                           $0x0,%esi
rax
                                                                                    mov
                                                            e8 e8 fe ff ff
                                                                                           400480 <strtol@plt>
                                               400593:
                                                                                    callq
                   0x7fffffffe1a8
rbx
                                         146
                                                                                           %eax, 0xc(%rsp)
                                               400598:
                                                             89 44 24 0c
                                                                                    mov
                   0x0
                               0
rcx
                                               40059c:
                                                             48 8b 7b 10
                                                                                           0x10(%rbx),%rdi
                                                                                    mov
rdx
                   0x47
                               71
                                               4005a0:
                                                             ba 0a 00 00 00
                                                                                           $0xa,%edx
                                                                                    mov
                                                                                           $0x0,%esi
                                               4005a5:
                                                             be 00 00 00 00
                                                                                    mov
rsi
                   0x7fffffffe0c0
                                         146
                                                                                           400480 <strtol@plt>
                                               4005aa:
                                                             e8 d1 fe ff ff
                                                                                    callq
rdi
                   0x400670 4195952
                                                             8b 54 24 0c
                                               4005af:
                                                                                    mov
                                                                                           0xc(%rsp),%edx
rbp
                   0x0
                               0x0
                                                                                           0x1(%rdx,%rax,4),%edx
                                               4005b3:
                                                             8d 54 82 01
                                                                                    lea
                                               4005b7:
                                                             89 54 24 0c
                                                                                           %edx,0xc(%rsp)
                   0x7fffffffe0b0
                                                                                    mov
rsp
                                         0x7
                                               4005bb:
                                                             0f bf d2
                                                                                    movswl %dx,%edx
                   0x7ffff7dd5060
r8
                                         146
                                               4005be:
                                                             48 8d 74 24 10
                                                                                           0x10(%rsp),%rsi
                                                                                    lea
r9
                   0x7fffffffe4a2
                                         146
                                               4005c3:
                                                                                           $0x400670,%edi
                                                             bf 70 06 40 00
                                                                                    mov
                                               4005c8:
                                                             b8 00 00 00 00
                                                                                           $0x0,%eax
r10
                   0x7
                               7
                                                                                    mov
                                                                                           400450 <printf@plt>
                                                             e8 7e fe ff ff
                                               4005cd:
                                                                                    calla
r11
                   0x0
                               0
                                               4005d2:
                                                             8b 44 24 0c
                                                                                           0xc(%rsp),%eax
                                                                                    mov
r12
                   0x400490 4195472
                                                            48 83 c4 10
                                               4005d6:
                                                                                           $0x10,%rsp
                                                                                    add
r13
                   0x7fffffffe1a0
                                         146
                                               4005da:
                                                             5b
                                                                                           %rbx
                                                                                    pop
                                               4005db:
                                                             сЗ
                                                                                    retq
r14
                   0x0
                               0
                                                            0f 1f 40 00
                                                                                           0x0(%rax)
                                               4005dc:
                                                                                    nopl
r15
                   0x0
                               0
                   0x4005c8 0x4005c8 <main+75>
rip
```

(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	

## **ASCII Table**

Dec	Hex	0ct	Char	Dec	Hex	0ct	Char	Dec	Hex	0ct	Char	Dec	Hex	0ct	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	В	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	1	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(	72	48	110	Н	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	В	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	1
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	0	111	6F	157	0
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	Т	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	Υ	121	79	171	У
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	

00000000000400	57d /main>:			
40057d:	53		push %rt	nv.
40057a:	48 83 ec	10		(10,%rsp
400582:	48 89 f3			si,%rbx
400585:		98		3(%rsi),%rdi
400589:		00 00		ka,%edx
40058e:		00 00		(0,%esi
400593:		ff ff		0480 <strtol@plt></strtol@plt>
400598:		Øc		ax,0xc(%rsp)
40059c:		10		L0(%rbx),%rdi
4005a0:		00 00		ka,%edx
4005a5:	be 00 00	00 00		k0,%esi
4005aa:	e8 d1 fe	ff ff	callq 400	0480 <strtol@plt></strtol@plt>
4005af:	8b 54 24	0c		c(%rsp),%edx
4005b3:	8d 54 82	01	lea 0x1	L(%rdx,%rax,4),%edx
4005b7:	89 54 24	0c		dx,0xc(%rsp)
4005bb:	0f bf d2		movswl %d>	k,%edx
4005be:	48 8d 74	24 10	lea 0x1	L0(%rsp),%rsi
4005c3:	bf 70 06	40 00	mov \$0>	k400670,%edi
4005c8:	b8 00 00	00 00	mov \$0>	<0,%eax
4005cd:	e8 7e fe	ff ff	callq 400	0450 <printf@plt></printf@plt>
4005d2:	8b 44 24	0c	mov 0x0	c(%rsp),%eax
4005d6:	48 83 c4	10	add \$0>	<10,%rsp
4005da:	5b		pop %rk	ΣX
4005db:	с3		retq	
4005dc:	0f 1f 40	00	nopl 0x0	0(%rax)

```
(gdb) c
c
Continuing.
7fffffffe0c0 47
```

00000000000400	57d <main></main>			
40057d:	53		push	%rbx
40057e:	48 83 e	10	sub	\$0x10,%rsp
400582:	48 89 f3	3	mov	%rsi,%rbx
400585:	48 8b 7	e 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 f	e ff ff	callq	400480 <strtol@plt></strtol@plt>
400598:	89 44 24	+ 0c	mov	%eax,0xc(%rsp)
40059c:	48 8b 7l	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 f	ff ff	callq	400480 <strtol@plt></strtol@plt>
4005af:	8b 54 24	+ 0c	mov	0xc(%rsp),%edx
4005b3:	8d 54 82	2 01	lea	<pre>0x1(%rdx,%rax,4),%edx</pre>
4005b7:	89 54 24	+ 0c	mov	%edx,0xc(%rsp)
4005bb:	0f bf di	2	movswl	%dx,%edx
4005be:	48 8d 74	4 24 10	lea	0x10(%rsp),%rsi
4005c3:	bf 70 0	40 00	mov	\$0x400670,%edi
4005c8:	b8 00 00	00 00	mov	\$0x0,%eax
4005cd:	e8 7e fe	e ff ff	callq	400450 <printf@plt></printf@plt>
4005d2:	8b 44 24	+ 0c	mov	0xc(%rsp),%eax
4005d6:	48 83 c	10	add	\$0x10,%rsp
4005da:	5b		рор	%rbx
4005db:	c3		retq	
4005dc:	0f 1f 40	00	nopl	0x0(%rax)