```c
int func2 (int a, long b, short c, long d, long e, long f, long g, long h)
{
  return a+b-c+d+e+f+g+h;
}

int func1 (int x, long y, short z)
{
  x*=256;
  y*=18;
  z*=2;
  return func2(x,y,z,y,y,y,y,y);
}

int func0 (void)
{
  int a;
  int i,j,k;

  i=rand();
  j=rand();
  k=rand();

  a=func1(i,j,k)*256;

  return a;
}

int main( int argc, const char* argv[] )
{
  return func0();
}
```

```
000000000040054e <main>:
  40054e:       48 83 ec 08             sub    $0x8,%rsp
  400552:       e8 b7 ff ff ff          callq  40050e <func0>
  400557:       48 83 c4 08             add    $0x8,%rsp
  40055b:       c3                      retq
  40055c:       90                      nop
  40055d:       90                      nop
  40055e:       90                      nop
  40055f:       90                      nop
```

```
000000000040050e <func0>:
  40050e:       48 89 5c 24 f0          mov    %rbx,-0x10(%rsp)
  400513:       48 89 6c 24 f8          mov    %rbp,-0x8(%rsp)
  400518:       48 83 ec 18             sub    $0x18,%rsp
  40051c:       e8 a7 fe ff ff          callq  4003c8 <rand@plt>
  400521:       89 c5                   mov    %eax,%ebp
  400523:       e8 a0 fe ff ff          callq  4003c8 <rand@plt>
  400528:       89 c3                   mov    %eax,%ebx
  40052a:       e8 99 fe ff ff          callq  4003c8 <rand@plt>
  40052f:       0f bf d0                movswl %ax,%edx
  400532:       48 63 f3                movslq %ebx,%rsi
  400535:       89 ef                   mov    %ebp,%edi
  400537:       e8 a3 ff ff ff          callq  4004df <func1>
  40053c:       c1 e0 08                shl    $0x8,%eax
  40053f:       48 8b 5c 24 08          mov    0x8(%rsp),%rbx
  400544:       48 8b 6c 24 10          mov    0x10(%rsp),%rbp
  400549:       48 83 c4 18             add    $0x18,%rsp
  40054d:       c3                      retq
```

```
00000000004004c4 <func2>:
  4004c4:       8d 34 37                lea    (%rdi,%rsi,1),%esi
  4004c7:       01 ce                   add    %ecx,%esi
  4004c9:       0f bf d2                movswl %dx,%edx
  4004cc:       29 d6                   sub    %edx,%esi
  4004ce:       44 01 c6                add    %r8d,%esi
  4004d1:       44 01 ce                add    %r9d,%esi
  4004d4:       89 f0                   mov    %esi,%eax
  4004d6:       03 44 24 08             add    0x8(%rsp),%eax
  4004da:       03 44 24 10             add    0x10(%rsp),%eax
  4004de:       c3                      retq

00000000004004df <func1>:
  4004df:       48 83 ec 10             sub    $0x10,%rsp
  4004e3:       48 8d 34 f6             lea    (%rsi,%rsi,8),%rsi
  4004e7:       48 01 f6                add    %rsi,%rsi
  4004ea:       01 d2                   add    %edx,%edx
  4004ec:       0f bf d2                movswl %dx,%edx
  4004ef:       c1 e7 08                shl    $0x8,%edi
  4004f2:       48 89 74 24 08          mov    %rsi,0x8(%rsp)
  4004f7:       48 89 34 24             mov    %rsi,(%rsp)
  4004fb:       49 89 f1                mov    %rsi,%r9
  4004fe:       49 89 f0                mov    %rsi,%r8
  400501:       48 89 f1                mov    %rsi,%rcx
  400504:       e8 bb ff ff ff          callq  4004c4 <func2>
  400509:       48 83 c4 10             add    $0x10,%rsp
  40050d:       c3                      retq
```

```
(gdb) break *0x4004de
Breakpoint 1 at 0x4004de
(gdb) run
Starting program: /w/fac.3/cs/reinman/code/a.out

Breakpoint 1, 0x00000000004004de in func2 ()
Missing separate debuginfos, use: debuginfo-install glibc-2.12-1.209.el6_9.2.x86_64
(gdb) backtrace
#0  0x00000000004004de in func2 ()
#1  0x0000000000400509 in func1 ()
#2  0x000000000040053c in func0 ()
#3  0x0000000000400557 in main ()
(gdb) i r
rax            0xd7384db6       3610791350
rbx            0x327b23c6       846930886
rcx            0x38ca883ec      15244755948
rdx            0x30d2   12498
rsi            0xbde745de       3186050526
rdi            0x8b456700       2336581376
rbp            0x6b8b4567       0x6b8b4567
rsp            0x7fffffffe130   0x7fffffffe130
r8             0x38ca883ec      15244755948
r9             0x38ca883ec      15244755948
r10            0x7fffffffded0   140737488346832
r11            0x3366436840     220759025728
r12            0x4003e0 4195296
r13            0x7fffffffe250   140737488347728
r14            0x0      0
r15            0x0      0
rip            0x4004de 0x4004de <func2+26>
```

```
(gdb) x/256xb 0x7fffffffe130
0x7fffffffe130: 0x09    0x05    0x40    0x00    0x00    0x00    0x00    0x00
0x7fffffffe138: 0xec    0x83    0xa8    0x8c    0x03    0x00    0x00    0x00
0x7fffffffe140: 0xec    0x83    0xa8    0x8c    0x03    0x00    0x00    0x00
0x7fffffffe148: 0x3c    0x05    0x40    0x00    0x00    0x00    0x00    0x00
0x7fffffffe150: 0x00    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffe158: 0x00    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffe160: 0x00    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffe168: 0x57    0x05    0x40    0x00    0x00    0x00    0x00    0x00
```

func1:

```
400504:  callq  4004c4 <func2>
400509:  add    $0x10,%rsp
```

```
r8             0x38ca883ec
r9             0x38ca883ec
```

func0:

```
400537:  callq  4004df <func1>
40053c:  shl    $0x8,%eax
40053f:  mov    0x8(%rsp),%rbx
400544:  mov    0x10(%rsp),%rbp
400549:  add    $0x18,%rsp
40054d:  retq
```