Condition Codes (Implicit Setting)

Single bit registers

```
CECF Carry Flag (for unsigned) SF Sign Flag (for signed)
```

OF Overflow Flag (for signed)

Implicitly set (think of it as side effect) by arithmetic operations

```
Example: addq Src,Dest ↔ t = a+b

CF set if carry out from most significant bit (unsigned overflow)

ZF set if t == 0

SF set if t < 0 (as signed)

OF set if two's-complement (signed) overflow
```

(a>0 && b>0 && t<0) || (a<0 && b<0 && t>=0)

Not set by leaq instruction

Condition Codes (Explicit Setting: Compare)

- Explicit Setting by Compare Instruction
 - cmpq Src2, Src1
 - cmpq b,a like computing a-b without setting destination
 - **©CF set** if carry out from most significant bit (used for unsigned comparisons)
 - 2ZF set if a == b
 - **QSF set** if (a-b) < 0 (as signed)
 - **©OF set** if two's-complement (signed) overflow

 (a>0 && b<0 && (a-b)<0) || (a<0 && b>0 && (a-b)>0)

Condition Codes (Explicit Setting: Test)

- Explicit Setting by Test instruction
 - 2testq Src2, Src1
 - ②testq b,a like computing a&b without setting destination
 - Sets condition codes based on value of Src1 & Src2
 - Useful to have one of the operands be a mask
 - **QZF set** when a&b == 0
 - **SF** set when a&b < 0

| jX | Condition | Description |
|-----|---------------|---------------------------|
| jmp | 1 | Unconditional |
| je | ZF | Equal / Zero |
| jne | ~ZF | Not Equal / Not Zero |
| js | SF | Negative |
| jns | ~SF | Nonnegative |
| jg | ~(SF^OF) &~ZF | Greater (Signed) |
| jge | ~(SF^OF) | Greater or Equal (Signed) |
| jl | (SF^OF) | Less (Signed) |
| jle | (SF^OF) ZF | Less or Equal (Signed) |
| ja | ~CF&~ZF | Above (unsigned) |
| jb | CF | Below (unsigned) |

```
int main( int argc, const char* argv[] )
 int i,j,a,k;
  char *label;
  a=atoi(argv[1]);
  i=atoi(argv[2]);
  j=atoi(argv[3]);
  fprintf(stderr, "START\n");
  for (k=0; k<i; k++)</pre>
    fprintf(stderr,".");
 if (j>10)
    label="Blue";
 else
    label="Gold";
  switch(a){
  case 100:
   i++;
   j++;
    break;
  case 102:
   i+=2;
    j+=2;
    break;
```

```
case 103:
    i++;
case 104:
    j+=2;
    break;

case 106:
    i+=2;
    j++;
    break;

default:
    i=0;
    j=0;
}

fprintf (stderr, "%s! i:%d j:%d\n", label, i,j);
}
```

```
int main( int argc, const char* argv[] )
{
  int i,j,a,k;
  char *label;

a=atoi(argv[1]);
  i=atoi(argv[2]);
  j=atoi(argv[3]);

fprintf(stderr, "START\n");
```

[(gdb) break *0x4005be Breakpoint 1 at 0x4005be [(gdb) run

```
[(gdb) i r
rax
               0x4
rbx
               0x0
rcx
               0x7ffff7dd51c0
                                140737351864768
rdx
               0x6
rsi
               0x1
rdi
               0x4007ea 4196330
rbp
                        0x3
               0x7fffffffdfd0
rsp
                                0x7fffffffdfd0
r8
               0x7ffff7dd5060
                                140737351864416
r9
                                140737488348174
               0x7fffffffe40e
r10
               0x4
r11
               0x0
                        0
r12
               0x3
                        3
r13
               0x66
                        102
r14
               0x4
                        4
r15
               0x0
rip
               0x4005be 0x4005be <main+94>
```

| 000000000400560 <main>:</main> | | | | | | | | |
|--------------------------------|------|-------|----|----|----|----|-------|----------------------------------|
| 400560: | 41 5 | 56 | | | | | push | %r14 |
| 400562: | ba 0 | 9a 00 | 00 | 00 | | | mov | \$0xa,%edx |
| 400567: | 41 5 | 55 | | | | | push | %r13 |
| 400569: | 41 5 | 54 | | | | | push | %r12 |
| 40056b: | 55 | | | | | | push | %rbp |
| 40056c: | 53 | | | | | | push | %rbx |
| 40056d: | 48 8 | 3b 7e | 80 | | | | mov | 0x8(%rsi),%rdi |
| 400571: | 48 8 | 39 f3 | | | | | mov | %rsi,%rbx |
| 400574: | 31 f | f6 | | | | | xor | %esi,%esi |
| 400576: | e8 c | 5 ff | ff | ff | | | callq | 400540 <strtol@plt></strtol@plt> |
| 40057b: | 48 8 | 3b 7b | 10 | | | | mov | 0x10(%rbx),%rdi |
| 40057f: | 31 f | f6 | | | | | xor | %esi,%esi |
| 400581: | ba 0 | 00 a | 00 | 00 | | | mov | \$0xa,%edx |
| 400586: | 49 8 | 39 c5 | | | | | mov | %rax,%r13 |
| 400589: | e8 b | o2 ff | ff | ff | | | callq | 400540 <strtol@plt></strtol@plt> |
| 40058e: | 48 8 | 3b 7b | 18 | | | | mov | 0x18(%rbx),%rdi |
| 400592: | 31 f | f6 | | | | | xor | %esi,%esi |
| 400594: | ba 0 | 00 a | 00 | 00 | | | mov | \$0xa,%edx |
| 400599: | 49 8 | 39 c4 | | | | | mov | %rax,%r12 |
| 40059c: | 89 c | :5 | | | | | mov | %eax,%ebp |
| 40059e: | 31 c | db | | | | | xor | %ebx,%ebx |
| 4005a0: | e8 9 | b ff | ff | ff | | | callq | 400540 <strtol@plt></strtol@plt> |
| 4005a5: | 48 8 | 3b 0d | а4 | 0a | 20 | 00 | mov | 0x200aa4(%rip),%rcx |
| 4005ac: | ba 0 | 96 00 | 00 | 00 | | | mov | \$0x6,%edx |
| 4005b1: | | 91 00 | 00 | 00 | | | mov | \$0x1,%esi |
| 4005b6: | bf e | ea 07 | 40 | 00 | | | mov | \$0x4007ea,%edi |
| 4005bb: | 49 8 | 39 c6 | | | | | mov | %rax,%r14 |
| 4005be: | e8 8 | 3d ff | ff | ff | | | callq | 400550 <fwrite@plt></fwrite@plt> |

```
fprintf(stderr, "START\n");

for (k=0; k<i; k++)
  fprintf(stderr,".");

if (j>10)
  label="Blue";
else
  label="Gold";
```

4005be:

[(gdb) break *0x4005be Breakpoint 1 at 0x4005be [(gdb) run 102 3 4

| (gdb) i r | | | |
|-----------|----------|---------|-----------------------|
| rax | 0x4 | 4 | |
| rbx | 0x0 | 0 | |
| rcx | 0x7ffff7 | dd51c0 | 140737351864768 |
| rdx | 0x6 | 6 | |
| rsi | 0x1 | 1 | |
| rdi | 0x4007ea | 4196330 | |
| rbp | 0x3 | 0x3 | |
| rsp | 0x7fffff | ffdfd0 | 0x7fffffffdfd0 |
| r8 | 0x7ffff7 | dd5060 | 140737351864416 |
| r9 | 0x7fffff | ffe40e | 140737488348174 |
| r10 | 0x4 | 4 | |
| r11 | 0x0 | 0 | |
| r12 | 0x3 | 3 | |
| r13 | 0x66 | 102 | |
| r14 | 0x4 | 4 | |
| r15 | 0x0 | 0 | |
| rip | 0x4005be | 0x4005b | e <main+94></main+94> |

| 400006. | 60 | ou | | | | | | Саттч | 400000 /IMITCEGhTC> |
|---------|----|----|----|----|----|----|----|-------|--------------------------------|
| 4005c3: | 45 | 85 | e4 | | | | | test | %r12d,%r12d |
| 4005c6: | 7e | 20 | | | | | | jle | 4005e8 <main+0x88></main+0x88> |
| 4005c8: | 0f | 1f | 84 | 00 | 00 | 00 | 00 | nopl | 0x0(%rax,%rax,1) |
| 4005cf: | 00 | | | | | | | | |
| 4005d0: | 48 | 8b | 35 | 79 | 0a | 20 | 00 | mov | 0x200a79(%rip),%rsi |
| 4005d7: | bf | 2e | 00 | 00 | 00 | | | mov | \$0x2e,%edi |
| 4005dc: | 83 | сЗ | 01 | | | | | add | \$0x1,%ebx |
| 4005df: | е8 | 1c | ff | ff | ff | | | callq | 400500 <fputc@plt></fputc@plt> |
| 4005e4: | 39 | eb | | | | | | cmp | %ebp,%ebx |
| 4005e6: | 7c | e8 | | | | | | jl | 4005d0 <main+0x70></main+0x70> |
| 4005e8: | 41 | 83 | fe | 0b | | | | cmp | \$0xb,%r14d |
| 4005ec: | ba | е0 | 07 | 40 | 00 | | | mov | \$0x4007e0,%edx |
| 4005f1: | b8 | е5 | 07 | 40 | 00 | | | mov | \$0x4007e5,%eax |
| 4005f6: | 48 | 0f | 4c | d0 | | | | cmovl | %rax,%rdx |
| 4005fa: | 41 | 83 | ed | 64 | | | | sub | \$0x64,%r13d |
| 4005fe: | 41 | 83 | fd | 96 | | | | cmp | \$0x6,%r13d |
| 400602: | 77 | 4f | | | | | | ja | 400653 <main+0xf3></main+0xf3> |
| 400604: | 42 | ff | 24 | ed | 80 | 80 | 40 | jmpq | *0x400808(,%r13,8) |
| | | | | | | | | | |

calld 400550 <fwriteOplt>

```
fprintf(stderr, "START\n");
                                                          2testq Src2, Src1
   for (k=0; k<i; k++)</pre>
                                                             27F set when a &b == 0
     fprintf(stderr,".");
                                                             SF set when a&b < 0
   if (j>10)
     label="Blue";
   else
                                             jle
                                                           (SF^OF) | ZF
                                                                                      Less or Equal (Signed)
     label="Gold";
                                                                  e8 8d ff ff ff
                                                                                                 400550 <fwrite@plt>
                                                    4005be:
                                                                                          callq
(gdb) break *0x4005be
                                                    4005c3:
                                                                  45 85 e4
                                                                                          test
                                                                                                 %r12d,%r12d
Breakpoint 1 at 0x4005be
                                                    4005c6:
                                                                  7e 20
                                                                                          ile
                                                                                                 4005e8 <main+0x88>
(gdb) run 102 3 4
                                                    4005c8:
                                                                                                 0x0(%rax,%rax,1)
                                                                  0f 1f 84 00 00 00 00
                                                                                          nopl
                          Decimal Hex Char
                                                    4005cf:
                                                                  00
                           32
                                     20
                                           [SPACE]
(adb) i r
                                                    4005d0:
                                                                  48 8b 35 79 0a 20 00
                                                                                                 0x200a79(%rip),%rsi
                                                                                          mov
                           33
                                     21
rax
            0x4
                                                                                                 $0x2e,%edi
                                                    4005d7:
                                                                  bf 2e 00 00 00
                                                                                          mov
rbx
                           34
                                     22
            0x0
                                                    4005dc:
                                                                  83 c3 01
                                                                                                 $0x1,%ebx
                                                                                          add
            0x7ffff7dd51c0
rcx
                           35
                                     23
                                                                  e8 1c ff ff ff
                                                                                                 400500 <fputc@plt>
rdx
            0x6
                                                    4005df:
                                                                                          calla
                           36
                                     24
rsi
            0x1
                                                    4005e4:
                           37
                                     25
                                                                  39 eb
                                                                                                 %ebp,%ebx
                                                                                          cmp
rdi
            0x4007ea 4196330
                           38
                                     26
                                                    4005e6:
                                                                  7c e8
                                                                                          il
                                                                                                 4005d0 <main+0x70>
rbp
            0x3
                   0x3
                           39
                                     27
                                                    4005e8:
                                                                  41 83 fe 0b
                                                                                                 $0xb,%r14d
            0x7fffffffdfd0
                                                                                          cmp
rsp
                           40
                                     28
r8
            0x7ffff7dd5060
                                                    4005ec:
                                                                  ba e0 07 40 00
                                                                                                 $0x4007e0,%edx
                                                                                          mov
                           41
                                     29
r9
            0x7fffffffe40e
                                                    4005f1:
                                                                  b8 e5 07 40 00
                                                                                                 $0x4007e5, %eax
                                                                                          mov
r10
                           42
                                     2A
            0x4
                                                    4005f6:
                                                                  48 0f 4c d0
                                                                                          cmovl %rax,%rdx
r11
                           43
            0x0
                                     2B
                                                    4005fa:
                                                                  41 83 ed 64
                                                                                                 $0x64,%r13d
                                                                                          sub
r12
            0x3
                           44
                                     2C
r13
            0x66
                   102
                                                   4005fe:
                                                                  41 83 fd 06
                                                                                                 $0x6,%r13d
                           45
                                                                                          amo
                                     2D
r14
            0x4
                           46
                                     2E
                                                    400602:
                                                                  77 4f
                                                                                          iа
                                                                                                 400653 <main+0xf3>
r15
            0x0
                                     2F
                                                                  42 ff 24 ed 08 08 40
                                                                                          impq
                                                    400604:
                                                                                                 *0x400808(,%r13,8)
            0x4005be 0x4005be
```

```
fprintf(stderr, "START\n");

for (k=0; k<i; k++)
  fprintf(stderr,".");

if (j>10)
  label="Blue";
else
  label="Gold";
```

```
[(gdb) break *0x4005f6
Breakpoint 2 at 0x4005f6
[(gdb) c
Continuing.
START
...
Breakpoint 2, 0x0000000004005f6 in main () (gdb)
```

```
[(gdb) break *0x4005be
Breakpoint 1 at 0x4005be
[(gdb) run 102 3 4
```

```
(adb) i r
rax
               0x4
rbx
               0x0
                        0
               0x7ffff7dd51c0
rcx
                                 140737351864768
rdx
               0x6
rsi
               0x1
rdi
               0x4007ea 4196330
rbp
               0x3
                        0x3
               0x7fffffffdfd0
                                 0x7fffffffdfd0
rsp
r8
               0x7ffff7dd5060
                                140737351864416
r9
               0x7fffffffe40e
                                140737488348174
r10
               0x4
r11
               0x0
r12
               0x3
r13
                        102
               0x66
r14
               0x4
r15
               0x0
               0x4005be 0x4005be <main+94>
```

```
e8 8d ff ff ff
                                              400550 <fwrite@plt>
4005be:
                                       calla
4005c3:
              45 85 e4
                                       test
                                              %r12d,%r12d
                                              4005e8 <main+0x88>
4005c6:
              7e 20
                                       ile
4005c8:
              0f 1f 84 00 00 00 00
                                              0x0(%rax,%rax,1)
                                       nopl
4005cf:
              00
                                              0x200a79(%rip),%rsi
4005d0:
              48 8b 35 79 0a 20 00
                                       mov
                                              $0x2e,%edi
4005d7:
              bf 2e 00 00 00
                                       mov
4005dc:
              83 c3 01
                                              $0x1,%ebx
                                       add
4005df:
              e8 1c ff ff ff
                                       callq 400500 <fputc@plt>
4005e4:
              39 eb
                                       cmp
                                              %ebp,%ebx
4005e6:
              7c e8
                                       il
                                              4005d0 <main+0x70>
4005e8:
              41 83 fe 0b
                                              $0xb,%r14d
                                       cmp
4005ec:
              ba e0 07 40 00
                                              $0x4007e0,%edx
                                       mov
4005f1:
              b8 e5 07 40 00
                                              $0x4007e5,%eax
                                       mov
4005f6:
              48 0f 4c d0
                                       cmovl %rax,%rdx
4005fa:
              41 83 ed 64
                                              $0x64,%r13d
                                       sub
              41 83 fd 06
                                              $0x6,%r13d
4005fe:
                                       cmp
400602:
              77 4f
                                       iа
                                              400653 <main+0xf3>
              42 ff 24 ed 08 08 40
400604:
                                       pami
                                              *0x400808(,%r13,8)
```

```
[(gdb) i r
                                                              (qdb) break *0x4005f6
rax
               0x4007e5 4196325
                                                               Breakpoint 2 at 0x4005f6
rbx
               0x3
                        3
                                                               (gdb) c
rcx
               0x7ffff7afca00
                                140737348880896
rdx
               0x4007e0 4196320
                                                               Continuing.
rsi
               0x7ffff7dd69f0
                                140737351870960
                                                               START
rdi
               0x2
                        2
rbp
               0x3
                        0x3
               0x7fffffffdfd0
                                0x7fffffffdfd0
rsp
                                                               Breakpoint 2, 0x0000000004005f6 in main ()
r8
               0x2e
                        46
                                                               (gdb)
r9
               0x7ffff7fce740
                                140737353934656
r10
               0x7ffffffdb90
                                140737488346000
r11
               0x246
                        582
r12
               0x3
                        3
                                                                      e8 8d ff ff ff
                                                                                                       400550 <fwrite@plt>
                                                       4005be:
                                                                                               calla
r13
               0x66
                        102
                                                                      45 85 e4
                                                       4005c3:
                                                                                               test
                                                                                                       %r12d,%r12d
r14
               0x4
                        4
                                                       4005c6:
                                                                      7e 20
                                                                                               ile
                                                                                                       4005e8 <main+0x88>
r15
                        0
               0x0
                                                       4005c8:
                                                                      0f 1f 84 00 00 00 00
                                                                                                       0x0(%rax,%rax,1)
                                                                                               nopl
rip
               0x4005f6 0x4005f6 <main+150>
                                                       4005cf:
                                                                      00
(adb) i r
                                                                                                       0x200a79(%rip),%rsi
                                                       4005d0:
                                                                      48 8b 35 79 0a 20 00
                                                                                               mov
             0x4
rax
                                                                                                       $0x2e,%edi
                                                       4005d7:
                                                                      bf 2e 00 00 00
                                                                                               mov
rbx
             0x0
                    0
                                                       4005dc:
                                                                      83 c3 01
                                                                                               add
                                                                                                       $0x1,%ebx
             0x7ffff7dd51c0
rcx
                           140737351864768
                                                       4005df:
                                                                      e8 1c ff ff ff
                                                                                                      400500 <fputc@plt>
rdx
             0x6
                                                                                               callo
rsi
             0x1
                                                       4005e4:
                                                                      39 eb
                                                                                               cmp
                                                                                                       %ebp,%ebx
rdi
             0x4007ea 4196330
                                                       4005e6:
                                                                      7c e8
                                                                                               il
                                                                                                       4005d0 <main+0x70>
rbp
                    0x3
             0x3
                                                       4005e8:
                                                                      41 83 fe 0b
                                                                                                       $0xb,%r14d
                                                                                               cmp
             0x7fffffffdfd0
                           0x7fffffffdfd0
rsp
r8
             0x7ffff7dd5060
                           140737351864416
                                                       4005ec:
                                                                      ba e0 07 40 00
                                                                                                       $0x4007e0,%edx
                                                                                               mov
r9
             0x7fffffffe40e
                           140737488348174
                                                       4005f1:
                                                                      b8 e5 07 40 00
                                                                                                       $0x4007e5, %eax
                                                                                               mov
r10
             0x4
                                                                                               cmovl %rax,%rdx
                                                       4005f6:
                                                                      48 0f 4c d0
r11
             0x0
                                                       4005fa:
                                                                      41 83 ed 64
                                                                                                       $0x64,%r13d
                                                                                               sub
r12
             0x3
r13
                    102
             0x66
                                                                                                       $0x6,%r13d
                                                       4005fe:
                                                                      41 83 fd 06
                                                                                               amo
r14
             0x4
                                                       400602:
                                                                      77 4f
                                                                                               iа
                                                                                                       400653 <main+0xf3>
r15
             0x0
                    0
                                                                      42 ff 24 ed 08 08 40
                                                       400604:
                                                                                               pami
                                                                                                       *0x400808(,%r13,8)
             0x4005be 0x4005be <main+94>
```

```
(gdb) break *0x4005f6
(gdb) i r
rax
              0x4007e5 4196325
                                                           Breaknoint 2 at 0v/005f6
rbx
              0x3 3 (gdb) si
0x7ffff7afd
rcx
              0 \times 4007 = 0.41 0 \times 000000000004005 fa in main ()
rdx
              0x7ffff7dd6(qdb) i r
rsi
rdi
              0x2
                                             0x4007e5 4196325
                      <sub>0x</sub> rax
rbp
              0x3
              0x7fffffffc rbx
                                                          3
                                             0x3
rsp
                                                                                             04005f6 in main ()
r8
              0x2e
                                             0x7ffff7afca00
                                                                    140737348880896
                         rcx
r9
              0x7ffff7fce
              0x7ffffffffd rdx
                                             0x4007e5 4196325
r10
                      58 rsi
r11
              0x246
                                             0x7ffff7dd69f0
                                                                    140737351870960
r12
              0x3
                                                                                                400550 <fwrite@plt>
                                             0x2
                                                          2
                      1e rdi
r13
              0x66
                                                                                                 %r12d,%r12d
r14
              0x4
                         rbp
                                             0x3
                                                          0x3
                                                                                                 4005e8 <main+0x88>
r15
              0x0
                                                                                                0x0(%rax,%rax,1)
                                             0x7fffffffdfd0
                                                                    0x7fffffffdfd0
              0x4005f6 0x rsp
rip
                                             0x2e
                                                          46
                         r8
(qdb) i r
                                                                                                0x200a79(%rip),%rsi
            0x4
rax
                         r9
                                             0x7ffff7fce740
                                                                    140737353934656
                                                                                                 $0x2e,%edi
rbx
            0x0
                                                                                                $0x1,%ebx
            0x7ffff7dd51c0
                                             0x7fffffffdb90
                                                                    140737488346000
rcx
                         r10
                                                                                             q 400500 <fputc@plt>
rdx
            0x6
                         r11
                                             0x246
                                                         582
rsi
            0x1
                                                                                                 %ebp,%ebx
rdi
            0x4007ea 4196330
                         r12
                                                         3
                                             0x3
                                                                                                 4005d0 <main+0x70>
rbp
                   0x3
            0x3
                                                                                                 $0xb,%r14d
            0x7fffffffdfd0
rsp
                         r13
                                             0x66
                                                         102
r8
            0x7ffff7dd5060
                                                                                                 $0x4007e0,%edx
                        r14
                                             0x4
                                                         4
r9
            0x7fffffffe40e
                                                                                                 $0x4007e5, %eax
r10
            0x4
                                                                                             1 %rax,%rdx
                         r15
                                                          0
                                             0x0
r11
            0x0
                                                                                                $0x64,%r13d
r12
            0x3
                         rip
                                             0x4005fa 0x4005fa <main+154>
r13
                   102
            0x66
                                                                                                 $0x6,%r13d
r14
            0x4
                                                   400602:
                                                                 77 4f
                                                                                          iа
                                                                                                 400653 <main+0xf3>
r15
            0x0
                                                                 42 ff 24 ed 08 08 40
                                                   400604:
                                                                                          pami
                                                                                                 *0x400808(,%r13,8)
            0x4005be 0x4005be <main+94>
```

```
switch(a){
case 100:
  i++;
  j++;
  break;
case 102:
  i+=2;
  j+=2;
  break;
case 103:
  i++;
case 104:
  i+=2;
  break;
case 106:
 i+=2;
  j++;
  break;
default:
 i=0;
  j=0;
fprintf (stderr, "%s! i:%d j:%d\n", label, i,j);
```

```
48 0f 4c d0
4005f6:
                                              %rax,%rdx
                                        cmovl
4005fa:
              41 83 ed 64
                                        sub
                                               $0x64,%r13d
4005fe:
              41 83 fd 06
                                               $0x6,%r13d
                                        cmp
400602:
              77 4f
                                        ja
                                               400653 <main+0xf3>
400604:
                                               *0x400808(,%r13,8)
              42 ff 24 ed 08 08 40
                                        jmpq
40060b:
              00
40060c:
                                               0x1(%r12),%ebp
              41 8d 6c 24 01
                                        lea
400611:
              45 8d 46 02
                                               0x2(%r14),%r8d
                                        lea
400615:
              5b
                                               %rbx
                                       pop
              89 e9
400616:
                                               %ebp,%ecx
                                       mov
400618:
              48 8b 3d 31 0a 20 00
                                               0x200a31(%rip),%rdi
                                       mov
40061f:
                                               $0x4007f1,%esi
              be f1 07 40 00
                                       mov
400624:
              5d
                                               %rbp
                                       pop
400625:
              41 5c
                                               %r12
                                        pop
400627:
              41 5d
                                               %r13
                                       pop
400629:
              41 5e
                                               %r14
                                        pop
40062b:
                                               %eax,%eax
              31 c0
                                        xor
40062d:
                                               400520 <fprintf@plt>
              e9 ee fe ff ff
                                        jmpq
400632:
              41 8d 6c 24 02
                                               0x2(%r12),%ebp
                                        lea
400637:
              45 8d 46 01
                                               0x1(%r14),%r8d
                                       lea
40063b:
              eb d8
                                        jmp
                                               400615 <main+0xb5>
40063d:
              41 8d 6c 24 01
                                        lea
                                               0x1(%r12),%ebp
400642:
              45 8d 46 01
                                               0x1(%r14),%r8d
                                        lea
400646:
                                               400615 <main+0xb5>
              eb cd
                                        qmj
400648:
              41 8d 6c 24 02
                                               0x2(%r12),%ebp
                                        lea
40064d:
              45 8d 46 02
                                               0x2(%r14),%r8d
                                       lea
400651:
                                               400615 <main+0xb5>
              eb c2
                                        jmp
400653:
              45 31 c0
                                               %r8d,%r8d
                                        xor
400656:
              31 ed
                                               %ebp,%ebp
                                        xor
                                               400615 <main+0xb5>
400658:
              eb bb
                                        jmp
```

```
4005f6:
                                                                48 0f 4c d0
                                                                                                %rax,%rdx
                                                                                         cmovl
switch(a){
                                                 4005fa:
                                                                41 83 ed 64
                                                                                         sub
                                                                                                $0x64,%r13d
                                                 4005fe:
                                                                41 83 fd 06
                                                                                                $0x6,%r13d
                                                                                         cmp
case 100:
                                                                                         jа
                                                                                                400653 <main+0xf3>
  i++;
                         (adb) si
                                                                                   40
                                                                                                *0x400808(,%r13,8)
                                                                                         jmpq
  j++;
                        0x00000000004005fe in main ()
  break;
                         (qdb) i r
                                                                                                0x1(%r12),%ebp
                                                                                         lea
                                        0x4007e5 4196325
                        rax
                                                                                                0x2(%r14),%r8d
                                                                                         lea
case 102:
                        rbx
                                        0x3
                                                  3
                                                                                                %rbx
                                                                                         pop
  i+=2;
                                        0x7ffff7afca00
                                                           140737348880896
                        rcx
                                                                                                %ebp,%ecx
                                                                                         mov
  j+=2;
                                        0x4007e5 4196325
                                                                                   00
                        rdx
                                                                                                0x200a31(%rip),%rdi
                                                                                         mov
  break;
                        rsi
                                        0x7ffff7dd69f0
                                                                                                $0x4007f1,%esi
                                                           140737351870960
                                                                                         mov
case 103:
                        rdi
                                        0x2
                                                                                                %rbp
                                                                                         pop
  i++;
                        rbp
                                                  0x3
                                                                                                %r12
                                        0x3
                                                                                         pop
case 104:
                                        0x7fffffffdfd0
                                                           0x7fffffffdfd0
                        rsp
                                                                                         pop
                                                                                                %r13
  i+=2;
                                                                                                %r14
                        r8
                                        0x2e
                                                  46
                                                                                         pop
  break;
                        r9
                                        0x7ffff7fce740
                                                                                                %eax,%eax
                                                           140737353934656
                                                                                         xor
                                                                                                400520 <fprintf@plt>
                        r10
                                        0x7fffffffdb90
                                                                                         jmpq
                                                           140737488346000
case 106:
                                                                                                0x2(%r12),%ebp
                                                                                         lea
                        r11
                                        0x246
                                                  582
  i+=2;
                                                                                         lea
                                                                                                0x1(%r14),%r8d
                        r12
                                        0x3
                                                  3
 j++;
                                                                                         jmp
                                                                                                400615 <main+0xb5>
                        r13
                                        0x2
                                                  2
  break;
                                                                                                0x1(%r12),%ebp
                                                                                         lea
                        r14
                                                  4
                                        0x4
                                                                                         lea
                                                                                                0x1(%r14),%r8d
default:
                        r15
                                        0x0
                                                                                         jmp
                                                                                                400615 <main+0xb5>
  i=0;
                        rip
                                        0x4005fe 0x4005fe <main+158>
                                                                                                0x2(%r12),%ebp
                                                                                         lea
  j=0;
                                                 40064d:
                                                                45 8d 46 02
                                                                                         lea
                                                                                                0x2(%r14),%r8d
                                                 400651:
                                                                eb c2
                                                                                         jmp
                                                                                                400615 <main+0xb5>
                                                                45 31 c0
                                                                                                %r8d,%r8d
fprintf (stderr, "%s! i:%d j:%d\n", label, i,j);
                                                 400653:
                                                                                         xor
                                                 400656:
                                                                31 ed
                                                                                         xor
                                                                                                %ebp,%ebp
                                                 400658:
                                                                                                400615 <main+0xb5>
                                                                                         jmp
                                                                eb bb
```

```
48 0f 4c d0
                                              4005f6:
                                                                                   cmovl
                                                                                         %rax,%rdx
switch(a){
                                              4005fa:
                                                           41 83 ed 64
                                                                                   sub
                                                                                          $0x64,%r13d
                                              4005fe:
                                                           41 83 fd 06
                                                                                          $0x6,%r13d
                                                                                   cmp
case 100:
                                              400602:
                                                           77 4f
                                                                                   ja
                                                                                          400653 <main+0xf3>
  i++;
                                              400604:
                                                                                          *0x400808(,%r13,8)
                                                           42 ff 24 ed 08 08 40
                                                                                   jmpq
  j++;
                                              40060b:
                                                           00
  break;
                                              40060c:
                                                                                          0x1(%r12),%ebp
                                                           41 8d 6c 24 01
                                                                                   lea
                                              400611:
                                                           45 8d 46 02
                                                                                          0x2(%r14),%r8d
                                                                                   lea
case 102:
                                              400615:
                                                           5b
                                                                                          %rbx
                                                                                   pop
  i+=2;
                                                           89 e9
                                              400616:
                                                                                          %ebp,%ecx
                                                                                   mov
  j+=2;
                                              400618:
                                                           48 8b 3d 31 0a 20 00
                                                                                          0x200a31(%rip),%rdi
                                                                                   mov
  break;
                                              40061f:
                                                           be f1 07 40 00
                                                                                          $0x4007f1,%esi
                                                                                   mov
case 103:
                                              400624:
                                                           5d
                                                                                          %rbp
                                                                                   pop
 i++;
                                              400625:
                                                           41 5c
                                                                                          %r12
                                                                                   pop
case 104:
               (gdb) x/96xb 0x400808
  i+=2;
  break;
               0x400808:
                                   0x3d
                                             0x06
                                                      0x40
                                                                0x00
                                                                          0x00
                                                                                    0x00
                                                                                             0x00
                                                                                                       0x00
                0x400810:
                                   0x53
                                             0x06
                                                      0x40
                                                                0x00
                                                                          0x00
                                                                                    0x00
                                                                                             0x00
                                                                                                       0x00
case 106:
                0x400818:
                                             0x06
                                                      0x40
                                                                0x00
                                                                          0x00
                                                                                                       0x00
                                   0x48
                                                                                    0x00
                                                                                             0x00
 i+=2;
  j++;
                0x400820:
                                   0x0c
                                             0x06
                                                      0x40
                                                                0x00
                                                                          0x00
                                                                                    0x00
                                                                                             0x00
                                                                                                       0x00
 break;
                0x400828:
                                                      0x40
                                                                0x00
                                                                                                       0x00
                                   0x11
                                             0x06
                                                                          0x00
                                                                                    0x00
                                                                                             0x00
                0x400830:
                                   0x53
                                             0x06
                                                      0x40
                                                                0x00
                                                                          0x00
                                                                                    0x00
                                                                                             0x00
                                                                                                       0x00
default:
 i=0;
                0x400838:
                                                      0x40
                                                                0x00
                                                                          0x00
                                                                                                       0x00
                                   0x32
                                             0x06
                                                                                    0x00
                                                                                             0x00
 j=0;
                0x400840:
                                   0x01
                                             0x1b
                                                      0x03
                                                                0x3b
                                                                          0x34
                                                                                    0x00
                                                                                             0x00
                                                                                                       0x00
                0x400848:
                                   0x05
                                             0x00
                                                      0x00
                                                                0x00
                                                                          0xb0
                                                                                    0xfc
                                                                                             0xff
                                                                                                       0xff
                0x400850:
                                   0x80
                                             0x00
                                                      0x00
                                                                0x00
                                                                          0x20
                                                                                    0xfd
                                                                                             0xff
                                                                                                       0xff
fprintf (stderr,
                0x400858:
                                             0x00
                                                      0x00
                                                                0x00
                                                                          0x1a
                                                                                    0xfe
                                                                                             0xff
                                                                                                       0xff
                                   0xa8
                0x400860:
                                   0x50
                                             0x00
                                                      0x00
                                                                0x00
                                                                          0x10
                                                                                    0xff
                                                                                             0xff
                                                                                                       0xff
```

```
48 0f 4c d0
                                                    4005f6:
                                                                                                    %rax,%rdx
switch(a){
                                                                                             cmovl
             (gdb) x/96xb 0x400808
                                                   4005fa:
                                                                   41 83 ed 64
                                                                                                     $0x64,%r13d
                                                                                             sub
             0x400808:
                             0x3d
                                    0x06
                                            0x40
                                                    4005fe:
                                                                   41 83 fd 06
                                                                                                     $0x6,%r13d
                                                                                             cmp
case 100:
             0x400810:
                             0x53
                                    0x06
                                            0x40
                                                   400602:
                                                                   77 4f
                                                                                             ja
                                                                                                     400653 <main+0xf3>
             0x400818:
                             0x48
                                    0x06
                                            0x40
  i++;
                                                                                                     *0x400808(,%r13,8)
             0x400820:
                                                   400604:
                                                                   42 ff 24 ed 08 08 40
                             0x0c
                                     0x06
                                            0x40
                                                                                             jmpq
  j++;
             0x400828:
                             0x11
                                    0x06
                                            0x40
                                                   40060b:
                                                                   00
  break;
             0x400830:
                             0x53
                                    0x06
                                            0x40
                                                   40060c:
                                                                                                     0x1(%r12),%ebp
                                                                   41 8d 6c 24 01
                                                                                             lea
             0x400838:
                             0x32
                                    0x06
                                            0x40
                                                   400611:
                                                                   45 8d 46 02
                                                                                                     0x2(%r14),%r8d
                                                                                             lea
case 102:
             0x400840:
                             0x01
                                    0x1b
                                            0x03
                                                    400615:
                                                                   5b
                                                                                                     %rbx
                                                                                             pop
  i+=2;
             0x400848:
                             0x05
                                     0x00
                                            0x00
                                                                  89 e9
                                                    400616:
                                                                                                     %ebp,%ecx
                                                                                             mov
  j+=2;
             0x400850:
                             0x80
                                    0x00
                                            0x00
                                                   400618:
                                                                                                     0x200a31(%rip),%rdi
                                                                   48 8b 3d 31 0a 20 00
                                                                                             mov
             0x400858:
  break;
                             0xa8
                                    0x00
                                            0x00
                                                    40061f:
                                                                  be f1 07 40 00
                                                                                                     $0x4007f1,%esi
                                                                                             mov
             0x400860:
                             0x50
                                    0x00
                                            0x00
case 103:
                                                    400624:
                                                                   5d
                                                                                                     %rbp
                                                                                             pop
  i++;
                                                    400625:
                                                                   41 5c
                                                                                                     %r12
                                                                                             pop
case 104:
                                                    400627:
                                                                   41 5d
                                                                                                     %r13
                                                                                             pop
  i+=2;
                                                    400629:
                                                                   41 5e
                                                                                                     %r14
                                                                                             pop
  break;
                                                    40062b:
                                                                                                     %eax,%eax
                                                                   31 c0
                                                                                             xor
                                                   40062d:
                                                                   e9 ee fe ff ff
                                                                                                     400520 <fprintf@plt>
                                                                                             jmpq
case 106:
                                                    400632:
                                                                   41 8d 6c 24 02
                                                                                                     0x2(%r12),%ebp
                                                                                             lea
  i+=2;
                                                    400637:
                                                                   45 8d 46 01
                                                                                                     0x1(%r14),%r8d
                                                                                             lea
  j++;
                                                    40063b:
                                                                   eb d8
                                                                                             jmp
                                                                                                     400615 <main+0xb5>
  break;
                                                    40063d:
                                                                   41 8d 6c 24 01
                                                                                             lea
                                                                                                     0x1(%r12),%ebp
                                                    400642:
                                                                   45 8d 46 01
                                                                                                     0x1(%r14),%r8d
                                                                                             lea
default:
                                                                                                     400615 <main+0xb5>
                                                    400646:
                                                                   eb cd
                                                                                             qmj
  i=0;
                                                    400648:
                                                                   41 8d 6c 24 02
                                                                                             lea
                                                                                                     0x2(%r12),%ebp
  j=0;
                                                                                                     0x2(%r14),%r8d
                                                    40064d:
                                                                   45 8d 46 02
                                                                                             lea
                                                   400651:
                                                                                                     400615 <main+0xb5>
                                                                   eb c2
                                                                                             jmp
fprintf (stderr, "%s! i:%d j:%d\n", label, i,j);
                                                   400653:
                                                                   45 31 c0
                                                                                                     %r8d,%r8d
                                                                                             xor
                                                    400656:
                                                                   31 ed
                                                                                                     %ebp,%ebp
                                                                                             xor
                                                   400658:
                                                                                                     400615 <main+0xb5>
                                                                   eb bb
                                                                                             jmp
```

```
/005f6 ·
                                                                   48 0f 4c d0
                                                                                                    %rax,%rdx
switch(a){
                                                                                             cmovl
                   (gdb) i r
                                                                  41 83 ed 64
                                                                                             sub
                                                                                                    $0x64,%r13d
                                  0x4007e5 4196325
                   rax
                                                                  41 83 fd 06
                                                                                                    $0x6,%r13d
                                                                                             cmp
case 100:
                                 0x3
                   rbx
                                                                   77 4f
                                                                                             ja
                                                                                                    400653 <main+0xf3>
  i++;
                                 0x7ffff7afca00
                                                  140737348880896
                   rcx
                                                                   42 ff 24 ed 08 08 40
                                                                                                    *0x400808(,%r13,8)
                                                                                             jmpq
  j++;
                   rdx
                                 0x4007e5 4196325
  break;
                   rsi
                                 0x7ffff7dd69f0
                                                  140737351870960
                                                                                                    0x1(%r12),%ebp
                                                                   41 8d 6c 24 01
                                                                                             lea
                   rdi
                                 0x2
                                          2
                                                                  45 8d 46 02
                                                                                                    0x2(%r14),%r8d
                   rbp
                                 0x3
                                          0x3
                                                                                             lea
case 102:
                   rsp
                                 0x7fffffffdfd0
                                                  0x7fffffffdfd0
                                                                   5b
                                                                                                    %rbx
                                                                                             pop
  i+=2;
                   r8
                                 0x2e
                                          46
                                                                  89 e9
                                                                                                    %ebp,%ecx
                                                                                             mov
  j+=2;
                   r9
                                 0x7ffff7fce740
                                                  140737353934656
                                                                   48 8b 3d 31 0a 20 00
                                                                                                    0x200a31(%rip),%rdi
                                                                                             mov
  break;
                   r10
                                 0x7fffffffdb90
                                                  140737488346000
                                                                  be f1 07 40 00
                                                                                                    $0x4007f1,%esi
                                                                                             mov
                   r11
                                 0x246
                                          582
case 103:
                                                                  5d
                                                                                                    %rbp
                                                                                             pop
                   r12
                                 0x3
                                          3
  i++;
                                                                  41 5c
                                                                                                    %r12
                   r13
                                 0x2
                                          2
                                                                                             pop
case 104:
                                                                  41 5d
                   r14
                                 0x4
                                          4
                                                                                                    %r13
                                                                                             pop
  i+=2;
                   r15
                                 0x0
                                                                   41 5e
                                                                                                    %r14
                                                                                             pop
  break;
                   rip
                                  0x400648 0x400648 <main+232>
                                                                  31 c0
                                                                                                    %eax,%eax
                                                                                             xor
                                                                   e9 ee fe ff ff
                                                   40062d:
                                                                                                    400520 <fprintf@plt>
                                                                                             jmpq
case 106:
                                                   400632:
                                                                   41 8d 6c 24 02
                                                                                             lea
                                                                                                    0x2(%r12),%ebp
 i+=2;
                                                   400637:
                                                                   45 8d 46 01
                                                                                                    0x1(%r14),%r8d
                                                                                             lea
  j++;
                                                   40063b:
                                                                   eb d8
                                                                                                    400615 <main+0xb5>
                                                                                             jmp
  break;
                                                   40063d:
                                                                   41 8d 6c 24 01
                                                                                             lea
                                                                                                    0x1(%r12),%ebp
                                                   400642:
                                                                   45 8d 46 01
                                                                                                    0x1(%r14),%r8d
                                                                                             lea
default:
                                                   400646:
                                                                                                    400615 <main+0xb5>
                                                                   eb cd
                                                                                             qmj
 i=0;
                                                   400648:
                                                                   41 8d 6c 24 02
                                                                                                    0x2(%r12),%ebp
                                                                                             lea
  j=0;
                                                   40064d:
                                                                   45 8d 46 02
                                                                                                    0x2(%r14),%r8d
                                                                                             lea
                                                   400651:
                                                                                                    400615 <main+0xb5>
                                                                   eb c2
                                                                                             jmp
fprintf (stderr, "%s! i:%d j:%d\n", label, i,j);
                                                   400653:
                                                                   45 31 c0
                                                                                                    %r8d,%r8d
                                                                                             xor
                                                   400656:
                                                                   31 ed
                                                                                                    %ebp,%ebp
                                                                                             xor
                                                   400658:
                                                                   eb bb
                                                                                                    400615 <main+0xb5>
                                                                                             jmp
```

```
4005f6:
                                                                     48 0f 4c d0
                                                                                                        %rax,%rdx
switch
                                                                                                 cmovl
        (gdb) i r
                                                      4005fa:
                                                                     41 83 ed 64
                                                                                                sub
                                                                                                        $0x64,%r13d
        rax
                     0x4007e5 4196325
                                                      4005fe:
                                                                     41 83 fd 06
                                                                                                        $0x6,%r13d
                                                                                                cmp
case 1
        rbx
                     0x3
                                                      400602:
                                                                     77 4f
                                                                                                ja
                                                                                                        400653 <main+0xf3>
  i++;
                     0x7ffff7afca00
        rcx
                                    140737348880896
                                                     400604:
                                                                                                        *0x400808(,%r13,8)
                                                                     42 ff 24 ed 08 08 40
                                                                                                jmpq
  j++;
        rdx
                     0x4007e5 4196325
        rsi
                     0x7ffff7dd69f0
                                    140737351870960
                                                      40060b:
                                                                     00
  brea
        rdi
                     0x2
                             2
                                                                                                        0x1(%r12),%ebp
                                                      40060c:
                                                                     41 8d 6c 24 01
                                                                                                lea
        rbp
                     0x5
                             0x5
                                                     400611:
                                                                     45 8d 46 02
                                                                                                        0x2(%r14),%r8d
                                                                                                lea
        rsp
                     0x7fffffffdfd0
                                    0x7fffffffdfd0
case 1
                                                     400615:
        r8
                     0x6
                                                                     5b
                                                                                                        %rbx
                                                                                                pop
  i+=2
        r9
                     0x7ffff7fce740
                                    140737353934656
                                                                     89 e9
                                                      400616:
                                                                                                        %ebp,%ecx
                                                                                                mov
  j+=2
        r10
                     0x7fffffffdb90
                                    140737488346000
                                                     400618:
                                                                     48 8b 3d 31 0a 20 00
                                                                                                        0x200a31(%rip),%rdi
                                                                                                mov
        r11
  brea
                     0x246
                             582
                                                      40061f:
                                                                     be f1 07 40 00
                                                                                                        $0x4007f1,%esi
        r12
                     0x3
                             3
                                                                                                mov
case 10
        r13
                     0x2
                                                     400624:
                                                                     5d
                                                                                                        %rbp
                                                                                                pop
  i++;
        r14
                     0x4
                                                     400625:
                                                                     41 5c
                                                                                                        %r12
                                                                                                pop
        r15
                     0x0
case 10
                                                      400627:
                                                                     41 5d
                                                                                                        %r13
                                                                                                pop
                     0x400615 0x400615 <main+181>
        rip
  i+=2;
                                                      400629:
                                                                     41 5e
                                                                                                        %r14
                                                                                                pop
  break;
                                                     40062b:
                                                                                                        %eax,%eax
                                                                     31 c0
                                                                                                xor
                                                     40062d:
                                                                     e9 ee fe ff ff
                                                                                                        400520 <fprintf@plt>
                                                                                                jmpq
case 106:
                                                     400632:
                                                                     41 8d 6c 24 02
                                                                                                lea
                                                                                                        0x2(%r12),%ebp
  i+=2;
                                                     400637:
                                                                     45 8d 46 01
                                                                                                        0x1(%r14),%r8d
                                                                                                lea
  j++;
                                                     40063b:
                                                                     eb d8
                                                                                                jmp
                                                                                                        400615 <main+0xb5>
  break;
                                                     40063d:
                                                                     41 8d 6c 24 01
                                                                                                lea
                                                                                                        0x1(%r12),%ebp
                                                     400642:
                                                                     45 8d 46 01
                                                                                                        0x1(%r14),%r8d
                                                                                                lea
default:
                                                     400646:
                                                                                                        400615 <main+0xb5>
                                                                     eb cd
                                                                                                qmj
  i=0;
                                                     400648:
                                                                     41 8d 6c 24 02
                                                                                                        0x2(%r12),%ebp
                                                                                                lea
  j=0;
                                                     40064d:
                                                                     45 8d 46 02
                                                                                                        0x2(%r14),%r8d
                                                                                                lea
                                                     400651:
                                                                                                        400615 <main+0xb5>
                                                                     eb c2
                                                                                                jmp
fprintf (stderr, "%s! i:%d j:%d\n", label, i,j);
                                                     400653:
                                                                     45 31 c0
                                                                                                        %r8d,%r8d
                                                                                                xor
                                                     400656:
                                                                     31 ed
                                                                                                        %ebp,%ebp
                                                                                                xor
                                                     400658:
                                                                                                        400615 <main+0xb5>
                                                                     eb bb
                                                                                                jmp
```

Gold! i:5 j:6