Condition Codes (Implicit Setting)

- **Single bit registers**
  - **CF** Carry Flag (for unsigned) **SF** Sign Flag (for signed)
  - **ZF** Zero Flag **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)
  - **ZF set** if **`a == b`**
  - **SF 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)`

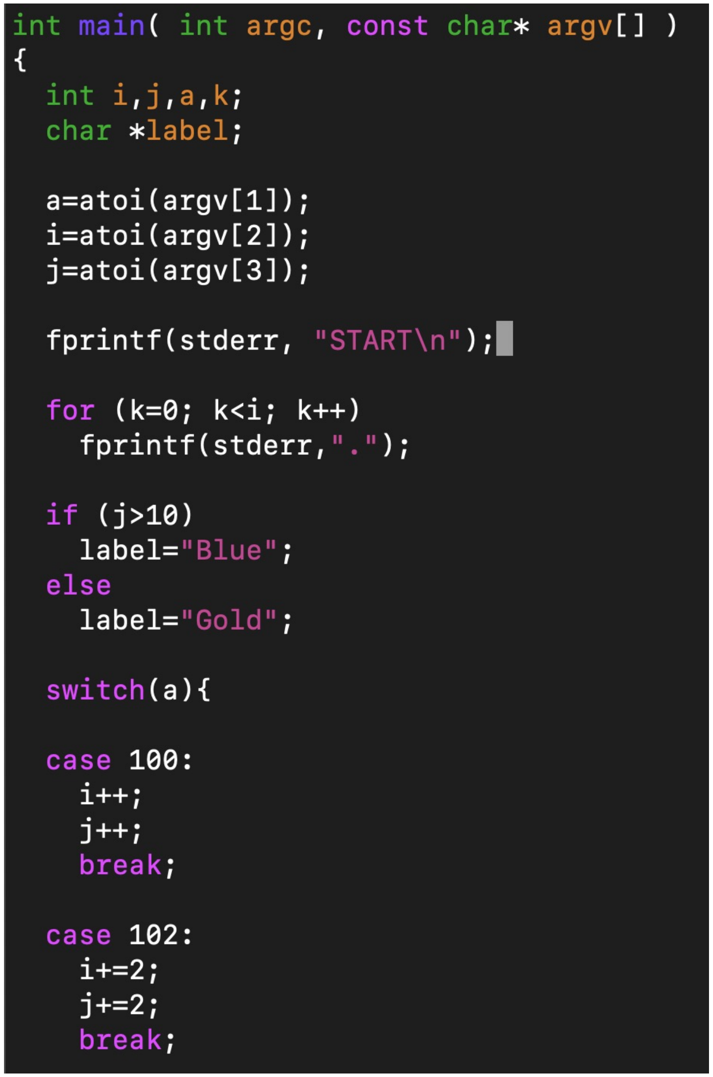
Condition Codes (Explicit Setting: Test)

- **Explicit Setting by Test instruction**
  - `testq` *Src2*, *Src1*
    - `testq b,a` like computing `a&b` without setting destination

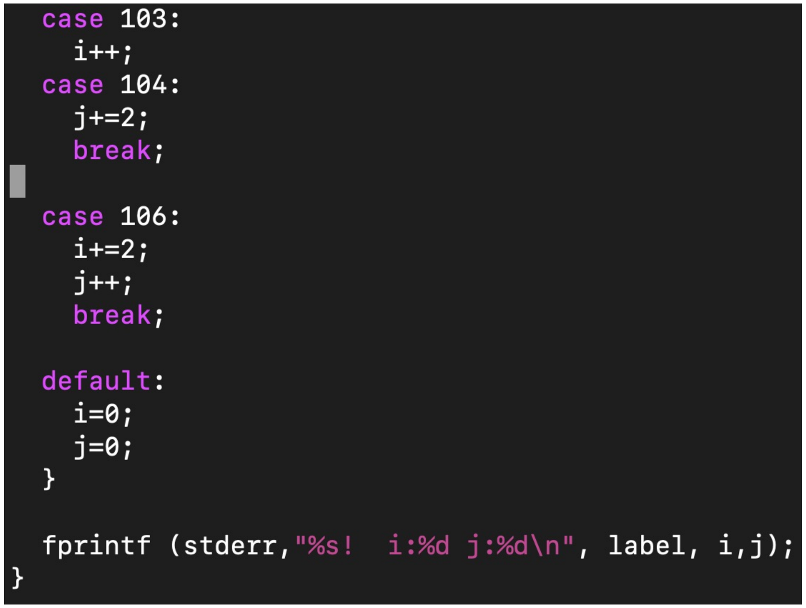
  - Sets condition codes based on value of *Src1* & *Src2*
  - Useful to have one of the operands be a mask

  - **ZF set** when `a&b == 0`
  - **SF set** when `a&b < 0`

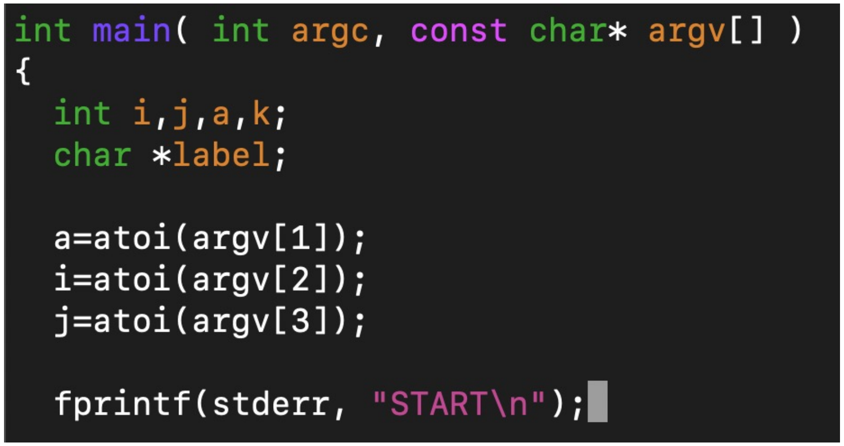
jX	Condition	Description
jmp	1	Unconditional
je	ZF	Equal / Zero
jne	~ZF	Not Equal / Not Zero
js	SF	Negative
jns	~SF	Nonnegative
jg	~(SF^OF)&~ZF	Greater (Signed)
jge	~(SF^OF)	Greater or Equal (Signed)
jl	(SF^OF)	Less (Signed)
jle	(SF^OF)|ZF	Less or Equal (Signed)
ja	~CF&~ZF	Above (unsigned)
jb	CF	Below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



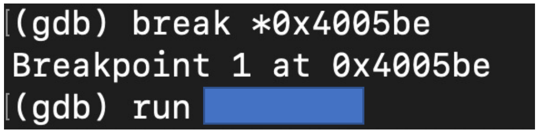
```c
int main( int argc, const char* argv[] )
{
  int i,j,a,k;
  char *label;

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

  fprintf(stderr, "START\n");

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

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

  switch(a){

  case 100:
    i++;
    j++;
    break;

  case 102:
    i+=2;
    j+=2;
    break;
```



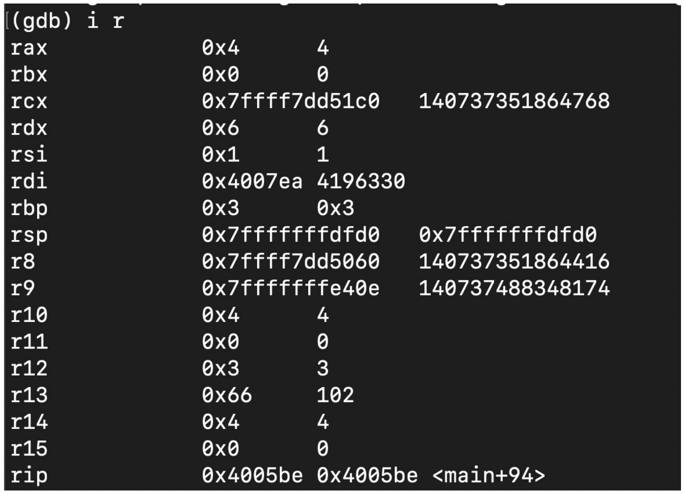
```c
  case 103:
    i++;
  case 104:
    j+=2;
    break;

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

  default:
    i=0;
    j=0;
  }

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



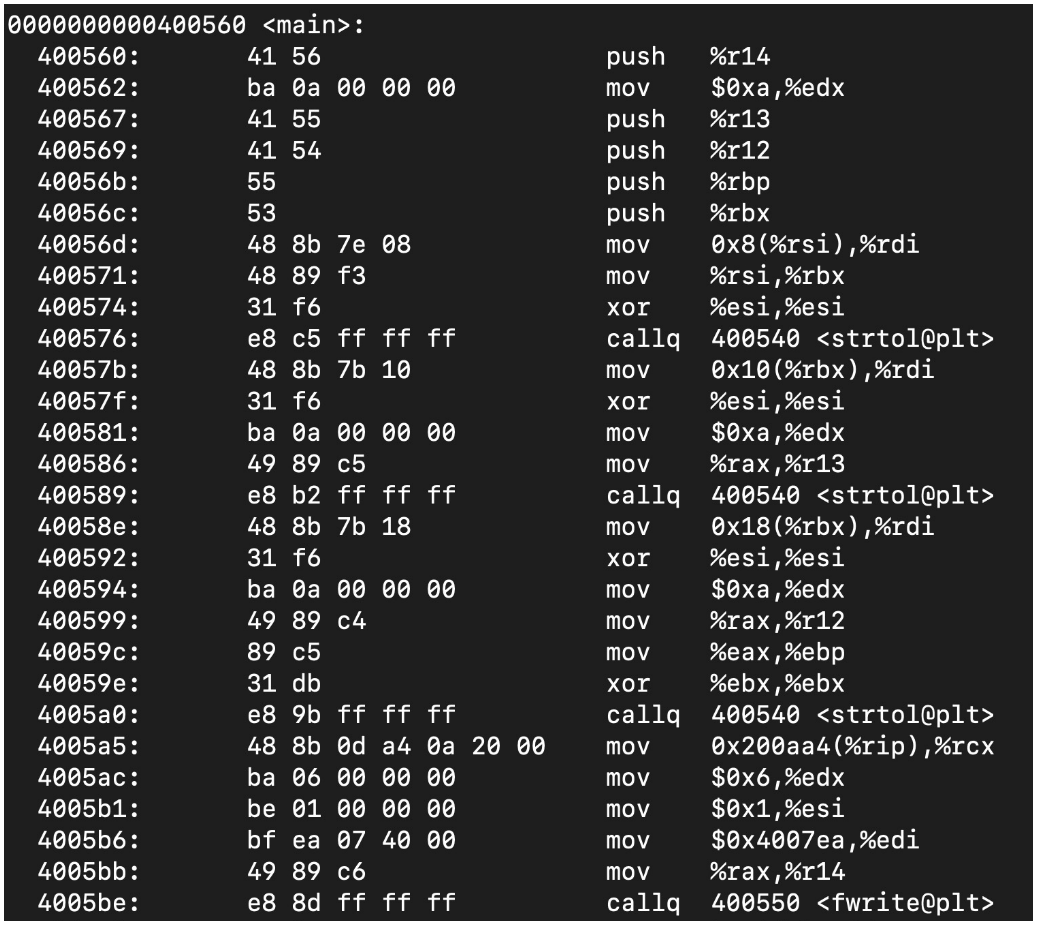
```c
int main( int argc, const char* argv[] )
{
  int i,j,a,k;
  char *label;

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

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



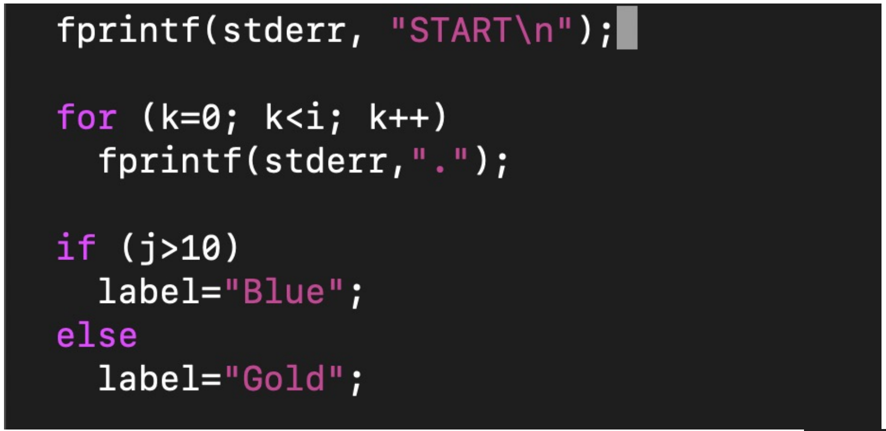
```
(gdb) break *0x4005be
Breakpoint 1 at 0x4005be
(gdb) run [redacted]
```



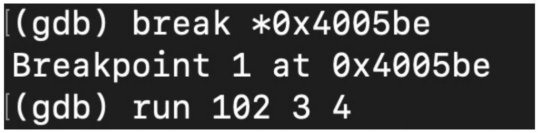
```
(gdb) i r
rax            0x4      4
rbx            0x0      0
rcx            0x7ffff7dd51c0   140737351864768
rdx            0x6      6
rsi            0x1      1
rdi            0x4007ea 4196330
rbp            0x3      0x3
rsp            0x7fffffffdfd0   0x7fffffffdfd0
r8             0x7ffff7dd5060   140737351864416
r9             0x7ffffffe40e    140737488348174
r10            0x4      4
r11            0x0      0
r12            0x3      3
r13            0x66     102
r14            0x4      4
r15            0x0      0
rip            0x4005be 0x4005be <main+94>
```



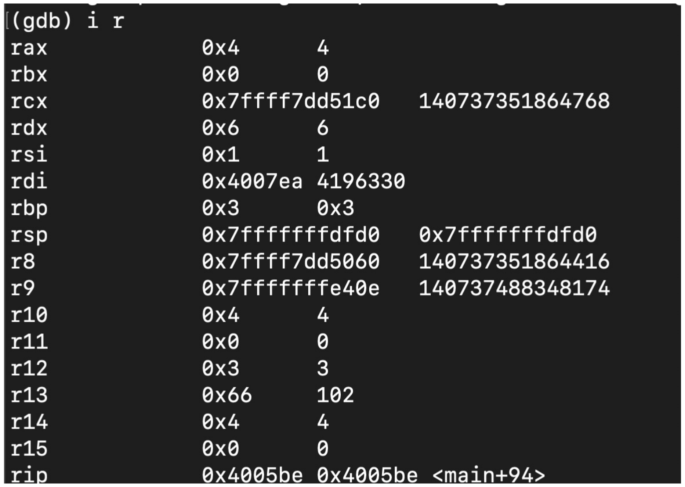
```
0000000000400560 <main>:
  400560:       41 56                   push   %r14
  400562:       ba 0a 00 00 00          mov    $0xa,%edx
  400567:       41 55                   push   %r13
  400569:       41 54                   push   %r12
  40056b:       55                      push   %rbp
  40056c:       53                      push   %rbx
  40056d:       48 8b 7e 08             mov    0x8(%rsi),%rdi
  400571:       48 89 f3                mov    %rsi,%rbx
  400574:       31 f6                   xor    %esi,%esi
  400576:       e8 c5 ff ff ff          callq  400540 <strtol@plt>
  40057b:       48 8b 7b 10             mov    0x10(%rbx),%rdi
  40057f:       31 f6                   xor    %esi,%esi
  400581:       ba 0a 00 00 00          mov    $0xa,%edx
  400586:       49 89 c5                mov    %rax,%r13
  400589:       e8 b2 ff ff ff          callq  400540 <strtol@plt>
  40058e:       48 8b 7b 18             mov    0x18(%rbx),%rdi
  400592:       31 f6                   xor    %esi,%esi
  400594:       ba 0a 00 00 00          mov    $0xa,%edx
  400599:       49 89 c4                mov    %rax,%r12
  40059c:       89 c5                   mov    %eax,%ebp
  40059e:       31 db                   xor    %ebx,%ebx
  4005a0:       e8 9b ff ff ff          callq  400540 <strtol@plt>
  4005a5:       48 8b 0d a4 0a 20 00    mov    0x200aa4(%rip),%rcx
  4005ac:       ba 06 00 00 00          mov    $0x6,%edx
  4005b1:       be 01 00 00 00          mov    $0x1,%esi
  4005b6:       bf ea 07 40 00          mov    $0x4007ea,%edi
  4005bb:       49 89 c6                mov    %rax,%r14
  4005be:       e8 8d ff ff ff          callq  400550 <fwrite@plt>
```



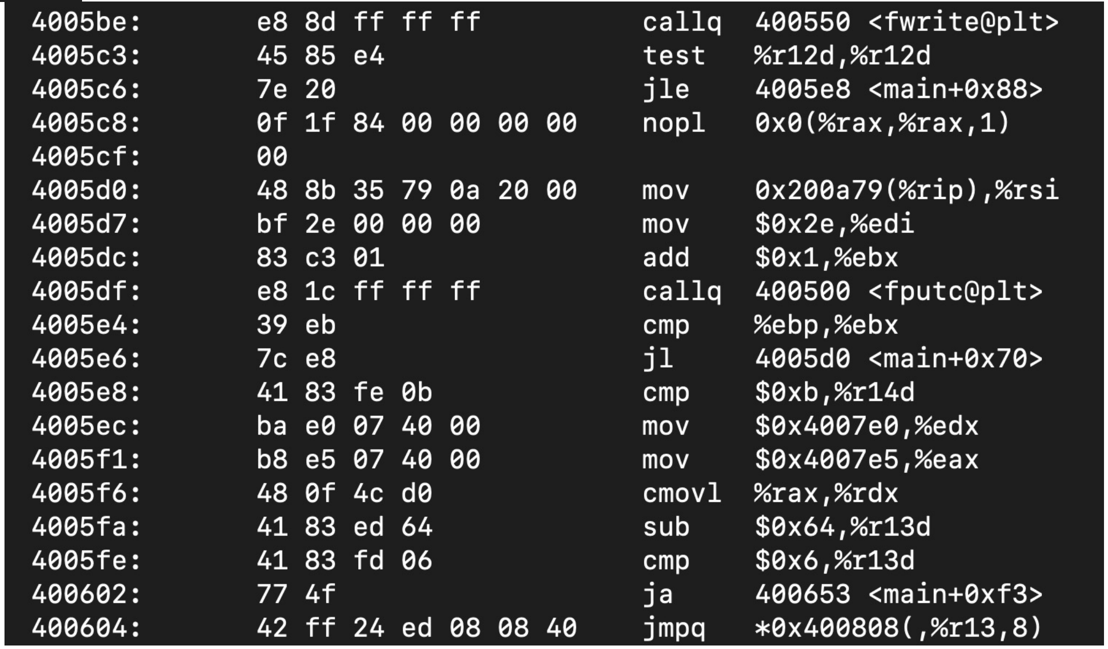
```
  fprintf(stderr, "START\n");

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

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



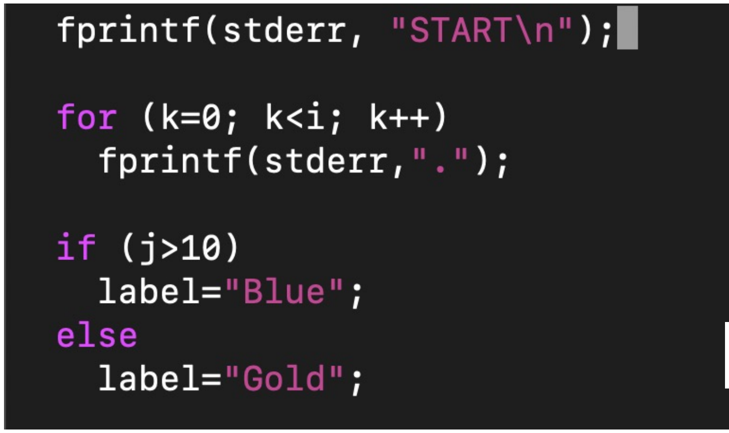
```
(gdb) break *0x4005be
Breakpoint 1 at 0x4005be
(gdb) run 102 3 4
```



```
(gdb) i r
rax            0x4      4
rbx            0x0      0
rcx            0x7ffff7dd51c0   140737351864768
rdx            0x6      6
rsi            0x1      1
rdi            0x4007ea 4196330
rbp            0x3      0x3
rsp            0x7fffffffdfd0   0x7fffffffdfd0
r8             0x7ffff7dd5060   140737351864416
r9             0x7ffffffe40e    140737488348174
r10            0x4      4
r11            0x0      0
r12            0x3      3
r13            0x66     102
r14            0x4      4
r15            0x0      0
rip            0x4005be 0x4005be <main+94>
```



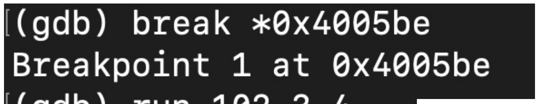
```
4005be:     e8 8d ff ff ff          callq  400550 <fwrite@plt>
4005c3:     45 85 e4                test   %r12d,%r12d
4005c6:     7e 20                   jle    4005e8 <main+0x88>
4005c8:     0f 1f 84 00 00 00 00    nopl   0x0(%rax,%rax,1)
4005cf:     00
4005d0:     48 8b 35 79 0a 20 00    mov  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



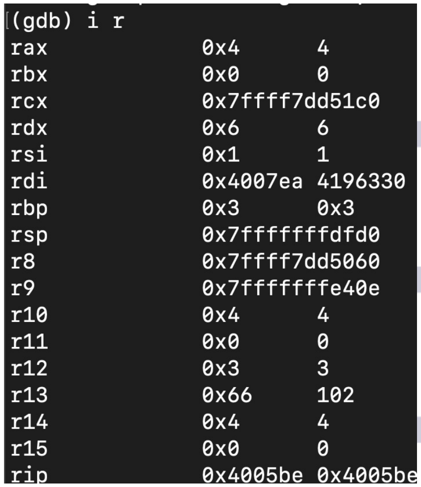
```
  fprintf(stderr, "START\n");

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

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

- **testq** *Src2, Src1*
  - **ZF set** when **a&b == 0**
  - **SF set** when **a&b < 0**

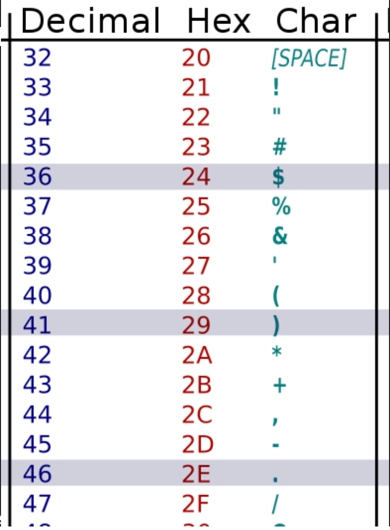
`jle`	`(SF^OF)|ZF`	**Less or Equal (Signed)**



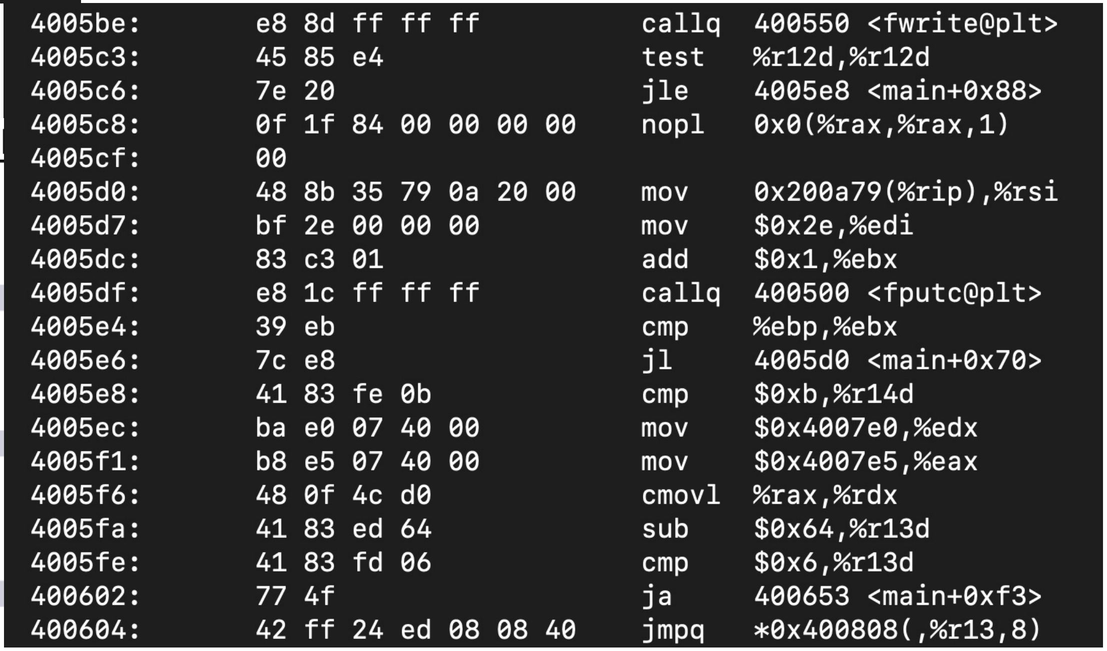
```
(gdb) break *0x4005be
Breakpoint 1 at 0x4005be
(gdb) run 102 3 4
```



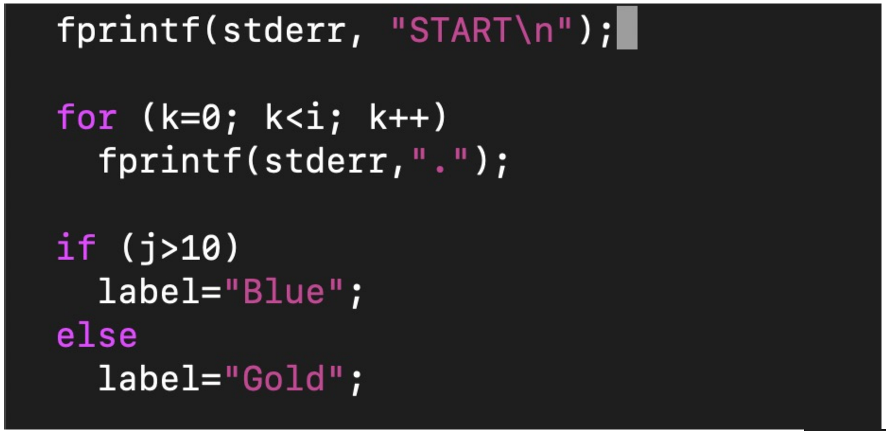
```
(gdb) i r
rax            0x4      4
rbx            0x0      0
rcx            0x7ffff7dd51c0
rdx            0x6      6
rsi            0x1      1
rdi            0x4007ea 4196330
rbp            0x3      0x3
rsp            0x7fffffffdfd0
r8             0x7ffff7dd5060
r9             0x7ffffffe40e
r10            0x4      4
r11            0x0      0
r12            0x3      3
r13            0x66     102
r14            0x4      4
r15            0x0      0
rip            0x4005be 0x4005be
```



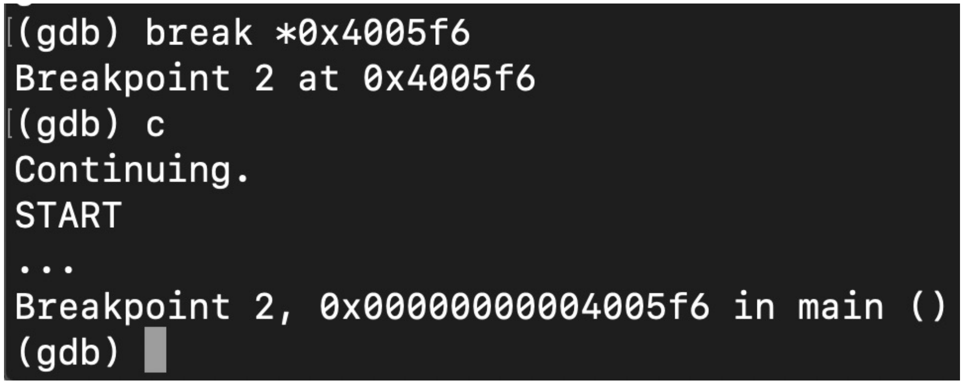
Decimal	Hex	Char
32	20	*[SPACE]*
33	21	!
34	22	"
35	23	#
36	24	$
37	25	%
38	26	&
39	27	'
40	28	(
41	29	)
42	2A	*
43	2B	+
44	2C	,
45	2D	-
46	2E	.
47	2F	/



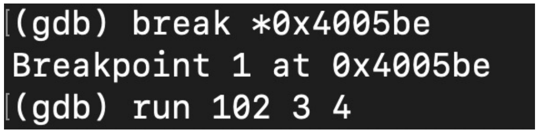
```
4005be:    e8 8d ff ff ff          callq  400550 <fwrite@plt>
4005c3:    45 85 e4                test   %r12d,%r12d
4005c6:    7e 20                   jle    4005e8 <main+0x88>
4005c8:    0f 1f 84 00 00 00 00    nopl   0x0(%rax,%rax,1)
4005cf:    00
4005d0:    48 8b 35 79 0a 20 00    mov    0x200a79(%rip),%rsi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



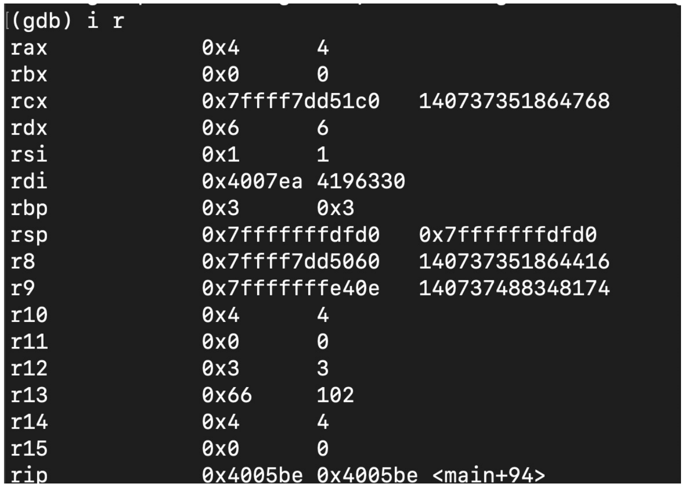
```
  fprintf(stderr, "START\n");

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

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



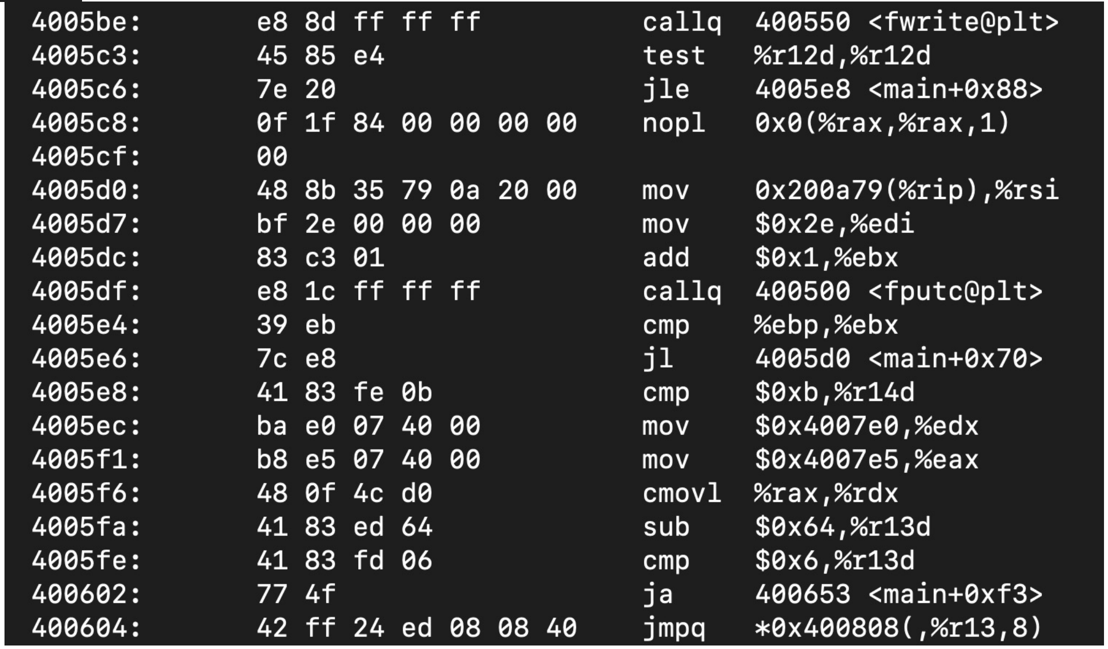
```
(gdb) break *0x4005f6
Breakpoint 2 at 0x4005f6
(gdb) c
Continuing.
START
...
Breakpoint 2, 0x00000000004005f6 in main ()
(gdb)
```



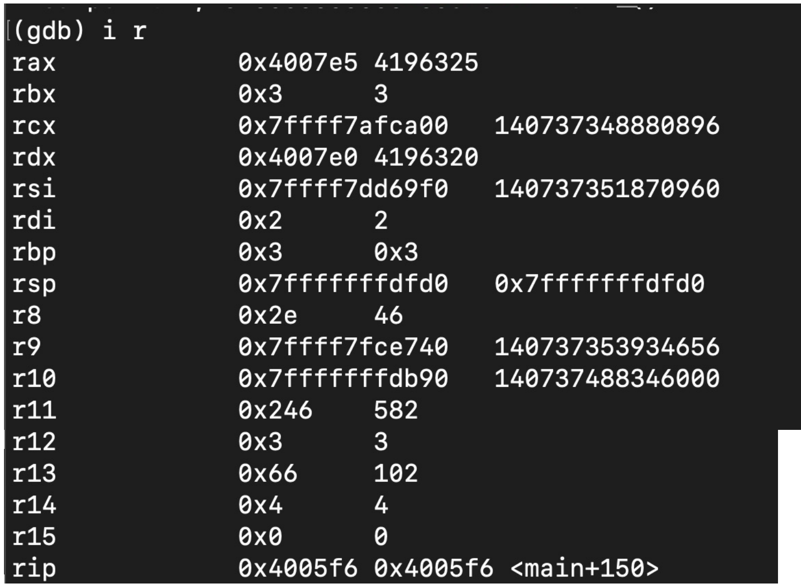
```
(gdb) break *0x4005be
Breakpoint 1 at 0x4005be
(gdb) run 102 3 4
```



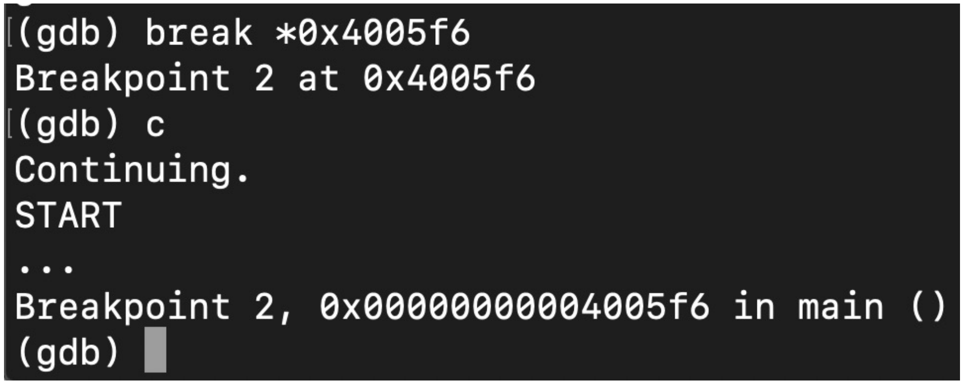
```
(gdb) i r
rax            0x4      4
rbx            0x0      0
rcx            0x7ffff7dd51c0   140737351864768
rdx            0x6      6
rsi            0x1      1
rdi            0x4007ea 4196330
rbp            0x3      0x3
rsp            0x7fffffffdfd0   0x7fffffffdfd0
r8             0x7ffff7dd5060   140737351864416
r9             0x7ffffffe40e    140737488348174
r10            0x4      4
r11            0x0      0
r12            0x3      3
r13            0x66     102
r14            0x4      4
r15            0x0      0
rip            0x4005be 0x4005be <main+94>
```



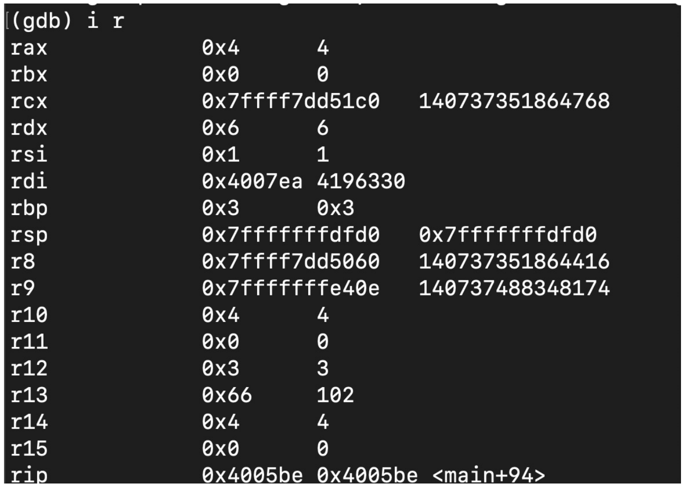
```
4005be:       e8 8d ff ff ff          callq  400550 <fwrite@plt>
4005c3:       45 85 e4                test   %r12d,%r12d
4005c6:       7e 20                   jle    4005e8 <main+0x88>
4005c8:       0f 1f 84 00 00 00 00    nopl   0x0(%rax,%rax,1)
4005cf:       00
4005d0:       48 8b 35 79 0a 20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



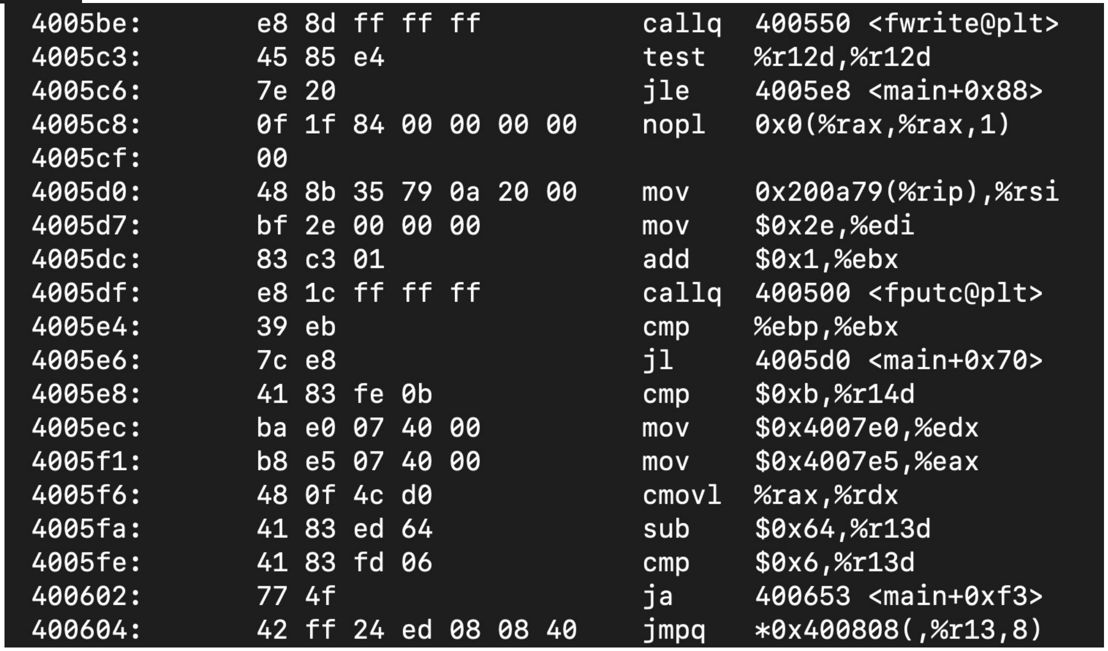
```
(gdb) i r
rax            0x4007e5 4196325
rbx            0x3      3
rcx            0x7ffff7afca00   140737348880896
rdx            0x4007e0 4196320
rsi            0x7ffff7dd69f0   140737351870960
rdi            0x2      2
rbp            0x3      0x3
rsp            0x7fffffffdfd0   0x7fffffffdfd0
r8             0x2e     46
r9             0x7ffff7fce740   140737353934656
r10            0x7fffffffdb90   140737488346000
r11            0x246    582
r12            0x3      3
r13            0x66     102
r14            0x4      4
r15            0x0      0
rip            0x4005f6 0x4005f6 <main+150>
```



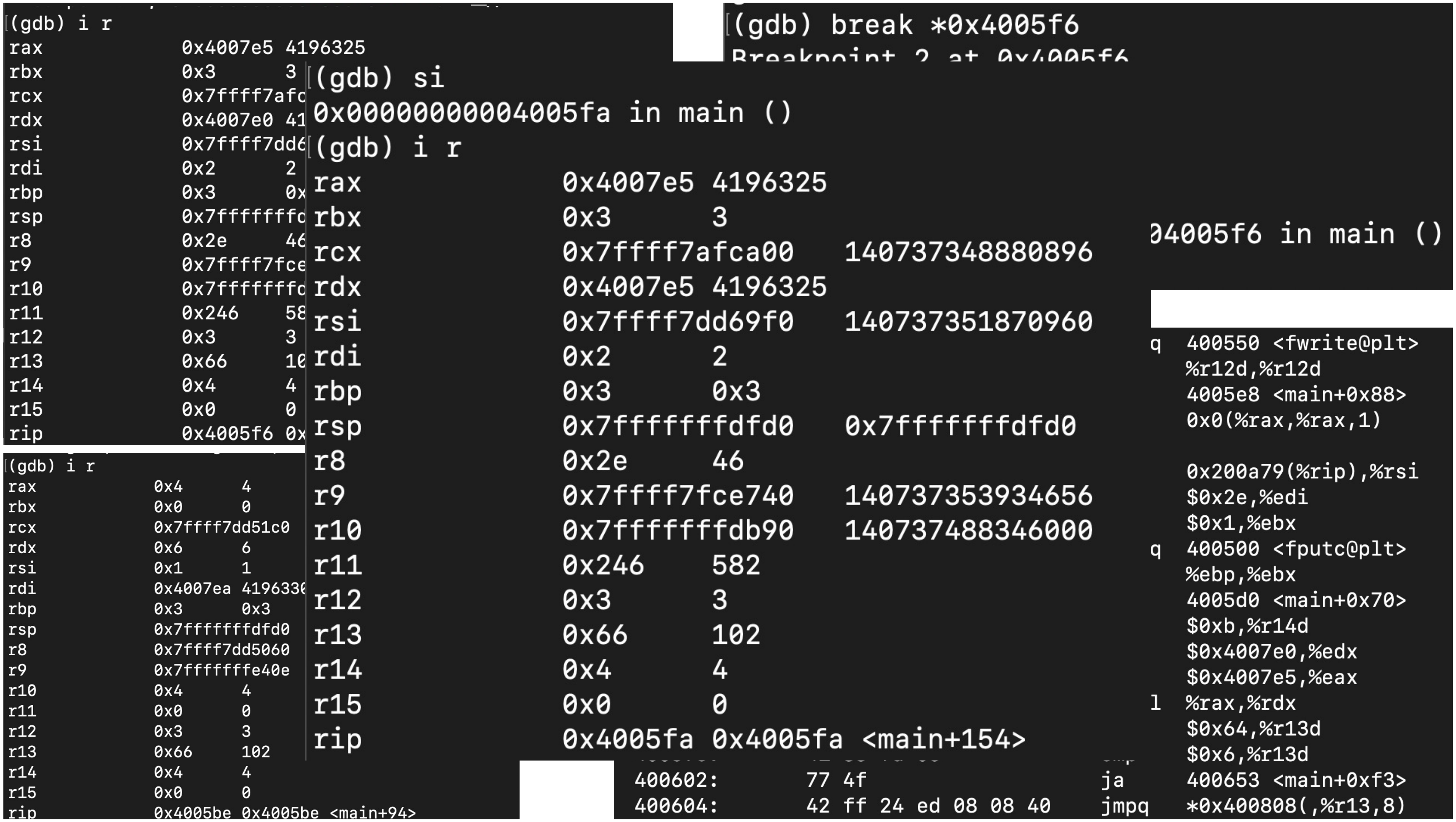
```
(gdb) break *0x4005f6
Breakpoint 2 at 0x4005f6
(gdb) c
Continuing.
START
...
Breakpoint 2, 0x00000000004005f6 in main ()
(gdb)
```



```
(gdb) i r
rax            0x4      4
rbx            0x0      0
rcx            0x7ffff7dd51c0   140737351864768
rdx            0x6      6
rsi            0x1      1
rdi            0x4007ea 4196330
rbp            0x3      0x3
rsp            0x7fffffffdfd0   0x7fffffffdfd0
r8             0x7ffff7dd5060   140737351864416
r9             0x7fffffffe40e   140737488348174
r10            0x4      4
r11            0x0      0
r12            0x3      3
r13            0x66     102
r14            0x4      4
r15            0x0      0
rip            0x4005be 0x4005be <main+94>
```



```
4005be:	e8 8d ff ff ff       	callq  400550 <fwrite@plt>
4005c3:	45 85 e4             	test   %r12d,%r12d
4005c6:	7e 20                	jle    4005e8 <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 c3 01             	add    $0x1,%ebx
4005df:	e8 1c ff ff ff       	callq  400500 <fputc@plt>
4005e4:	39 eb                	cmp    %ebp,%ebx
4005e6:	7c e8                	jl     4005d0 <main+0x70>
4005e8:	41 83 fe 0b          	cmp    $0xb,%r14d
4005ec:	ba e0 07 40 00       	mov    $0x4007e0,%edx
4005f1:	b8 e5 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 06          	cmp    $0x6,%r13d
400602:	77 4f                	ja     400653 <main+0xf3>
400604:	42 ff 24 ed 08 08 40 	jmpq   *0x400808(,%r13,8)
```



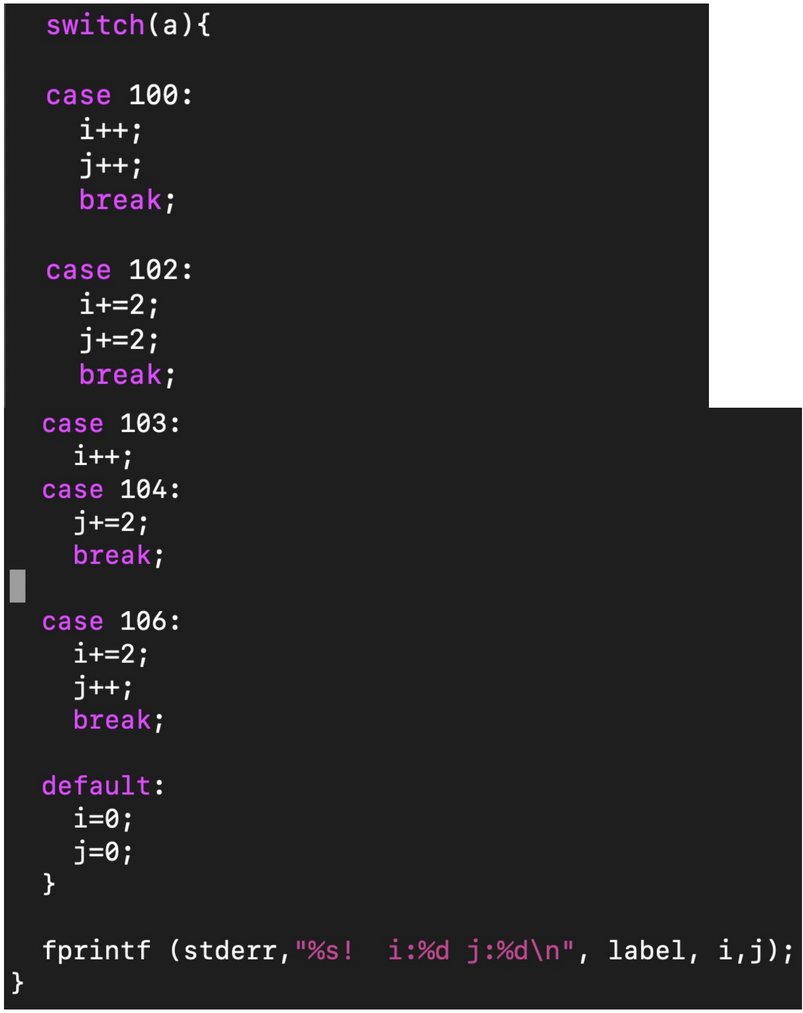
```
(gdb) i r
rax            0x4007e5 4196325
rbx            0x3      3
rcx            0x7ffff7afc
rdx            0x4007e0 41
rsi            0x7ffff7dd6
rdi            0x2      2
rbp            0x3      0x
rsp            0x7fffffffd
r8             0x2e     46
r9             0x7ffff7fce
r10            0x7fffffffd
r11            0x246    58
r12            0x3      3
r13            0x66     10
r14            0x4      4
r15            0x0      0
rip            0x4005f6 0x
```

```
(gdb) i r
rax            0x4      4
rbx            0x0      0
rcx            0x7ffff7dd51c0
rdx            0x6      6
rsi            0x1      1
rdi            0x4007ea 419633
rbp            0x3      0x3
rsp            0x7fffffffdfd0
r8             0x7ffff7dd5060
r9             0x7fffffffe40e
r10            0x4      4
r11            0x0      0
r12            0x3      3
r13            0x66     102
r14            0x4      4
r15            0x0      0
rip            0x4005be 0x4005be <main+94>
```

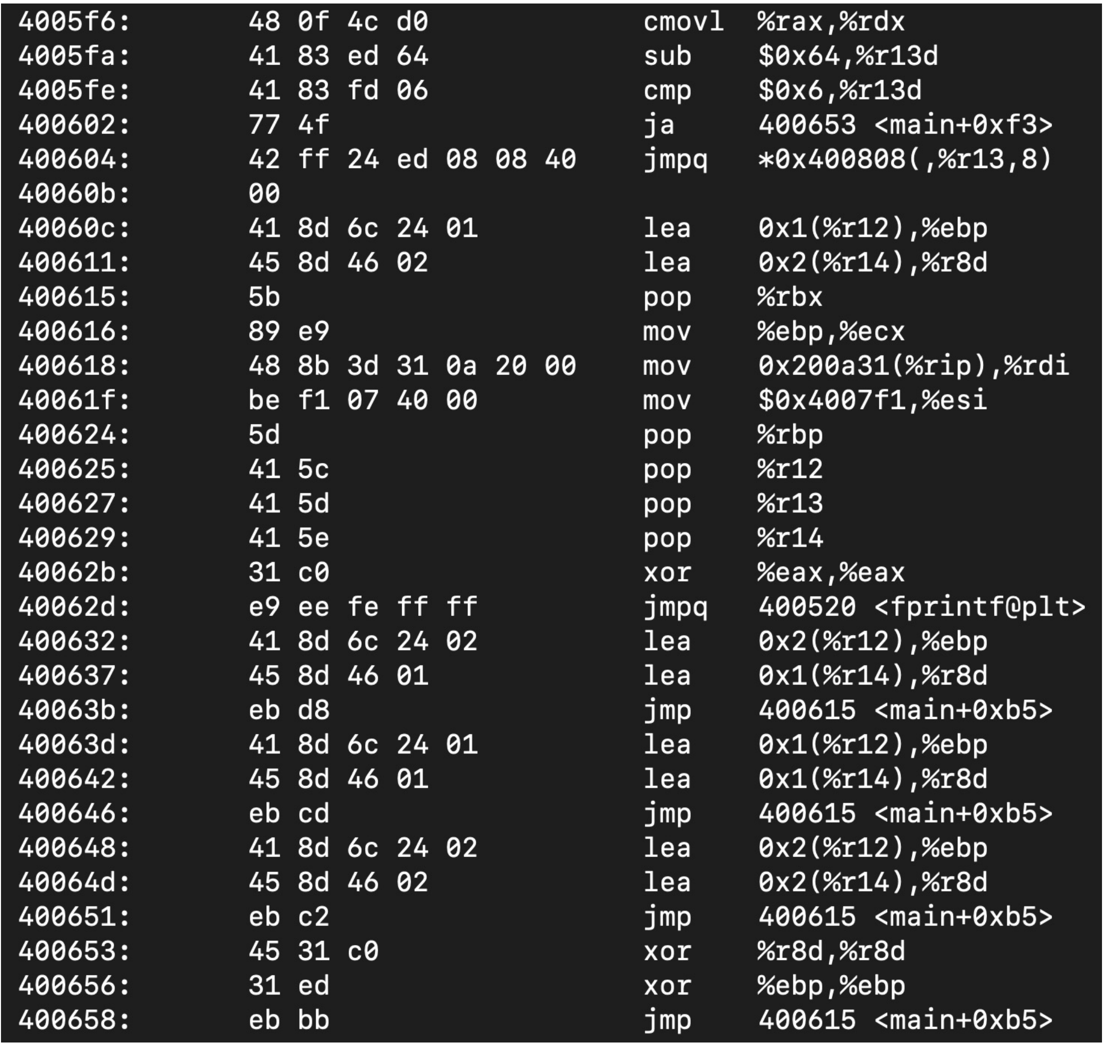
```
(gdb) si
0x00000000004005fa in main ()
(gdb) i r
rax            0x4007e5 4196325
rbx            0x3      3
rcx            0x7ffff7afca00   140737348880896
rdx            0x4007e5 4196325
rsi            0x7ffff7dd69f0   140737351870960
rdi            0x2      2
rbp            0x3      0x3
rsp            0x7fffffffdfd0   0x7fffffffdfd0
r8             0x2e     46
r9             0x7ffff7fce740   140737353934656
r10            0x7fffffffdb90   140737488346000
r11            0x246    582
r12            0x3      3
r13            0x66     102
r14            0x4      4
r15            0x0      0
rip            0x4005fa 0x4005fa <main+154>
```

```
(gdb) break *0x4005f6
Breakpoint 2 at 0x4005f6

04005f6 in main ()
```

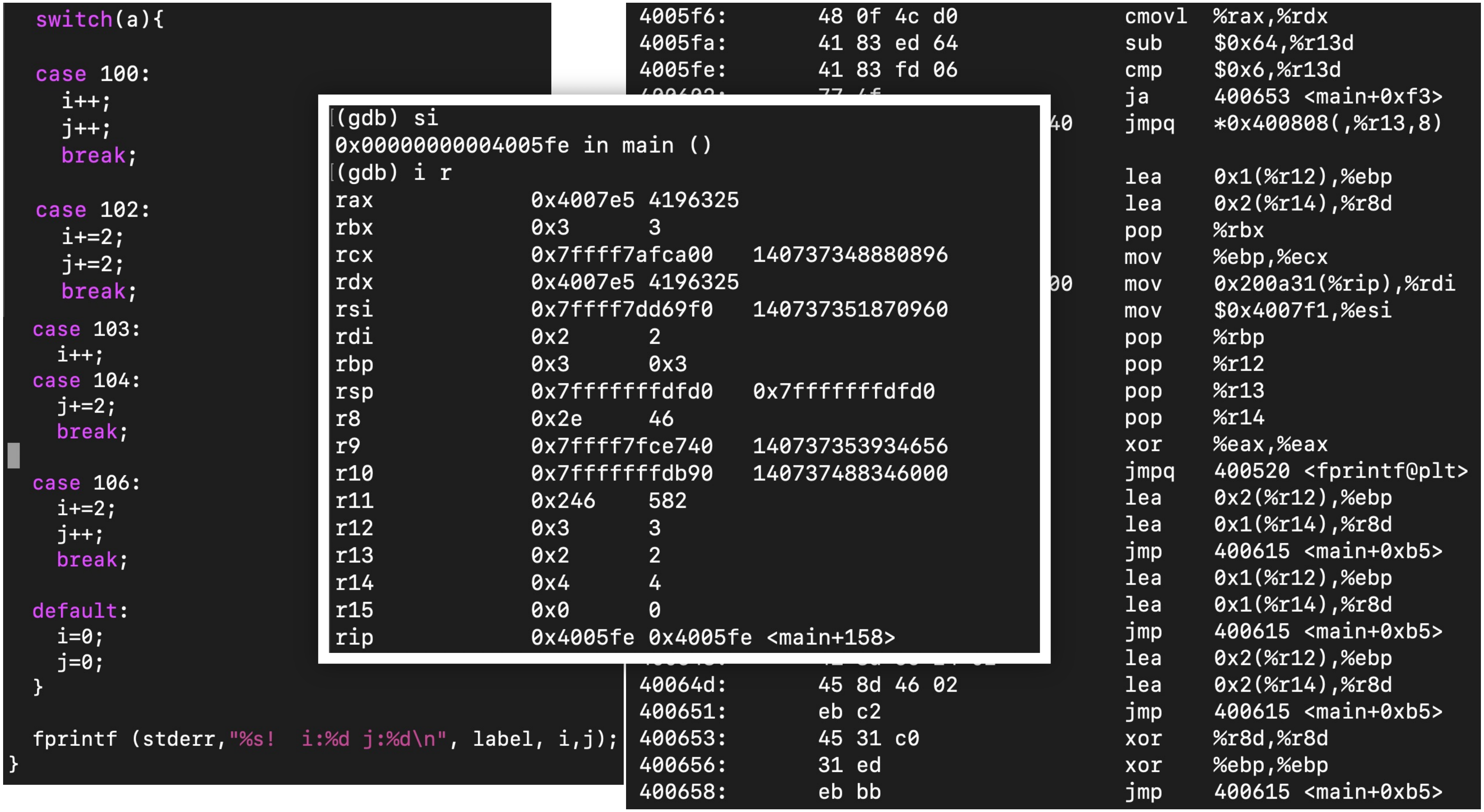
```
q   400550 <fwrite@plt>
    %r12d,%r12d
    4005e8 <main+0x88>
    0x0(%rax,%rax,1)

    0x200a79(%rip),%rsi
    $0x2e,%edi
    $0x1,%ebx
q   400500 <fputc@plt>
    %ebp,%ebx
    4005d0 <main+0x70>
    $0xb,%r14d
    $0x4007e0,%edx
    $0x4007e5,%eax
l   %rax,%rdx
    $0x64,%r13d
    $0x6,%r13d
400602:      77 4f                  ja     400653 <main+0xf3>
400604:      42 ff 24 ed 08 08 40   jmpq   *0x400808(,%r13,8)
```



```
  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);
}
```



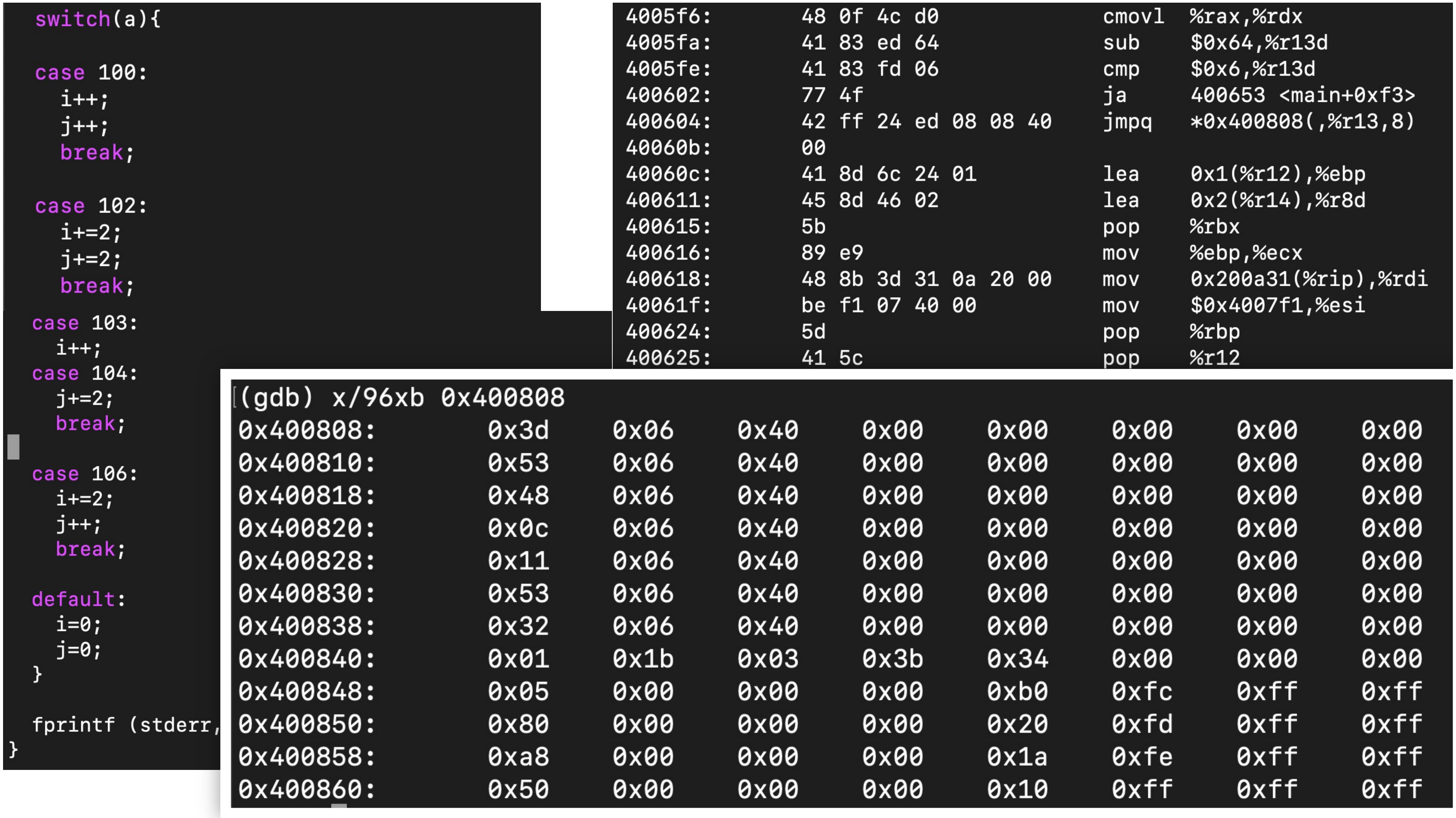
```
4005f6:        48 0f 4c d0                 cmovl  %rax,%rdx
4005fa:        41 83 ed 64                 sub    $0x64,%r13d
4005fe:        41 83 fd 06                 cmp    $0x6,%r13d
400602:        77 4f                       ja     400653 <main+0xf3>
400604:        42 ff 24 ed 08 08 40        jmpq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



```
  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);
}
```

```
(gdb) si
0x00000000004005fe in main ()
(gdb) i r
rax            0x4007e5 4196325
rbx            0x3      3
rcx            0x7ffff7afca00   140737348880896
rdx            0x4007e5 4196325
rsi            0x7ffff7dd69f0   140737351870960
rdi            0x2      2
rbp            0x3      0x3
rsp            0x7fffffffdfd0   0x7fffffffdfd0
r8             0x2e     46
r9             0x7ffff7fce740   140737353934656
r10            0x7fffffffdb90   140737488346000
r11            0x246    582
r12            0x3      3
r13            0x2      2
r14            0x4      4
r15            0x0      0
rip            0x4005fe 0x4005fe <main+158>
```

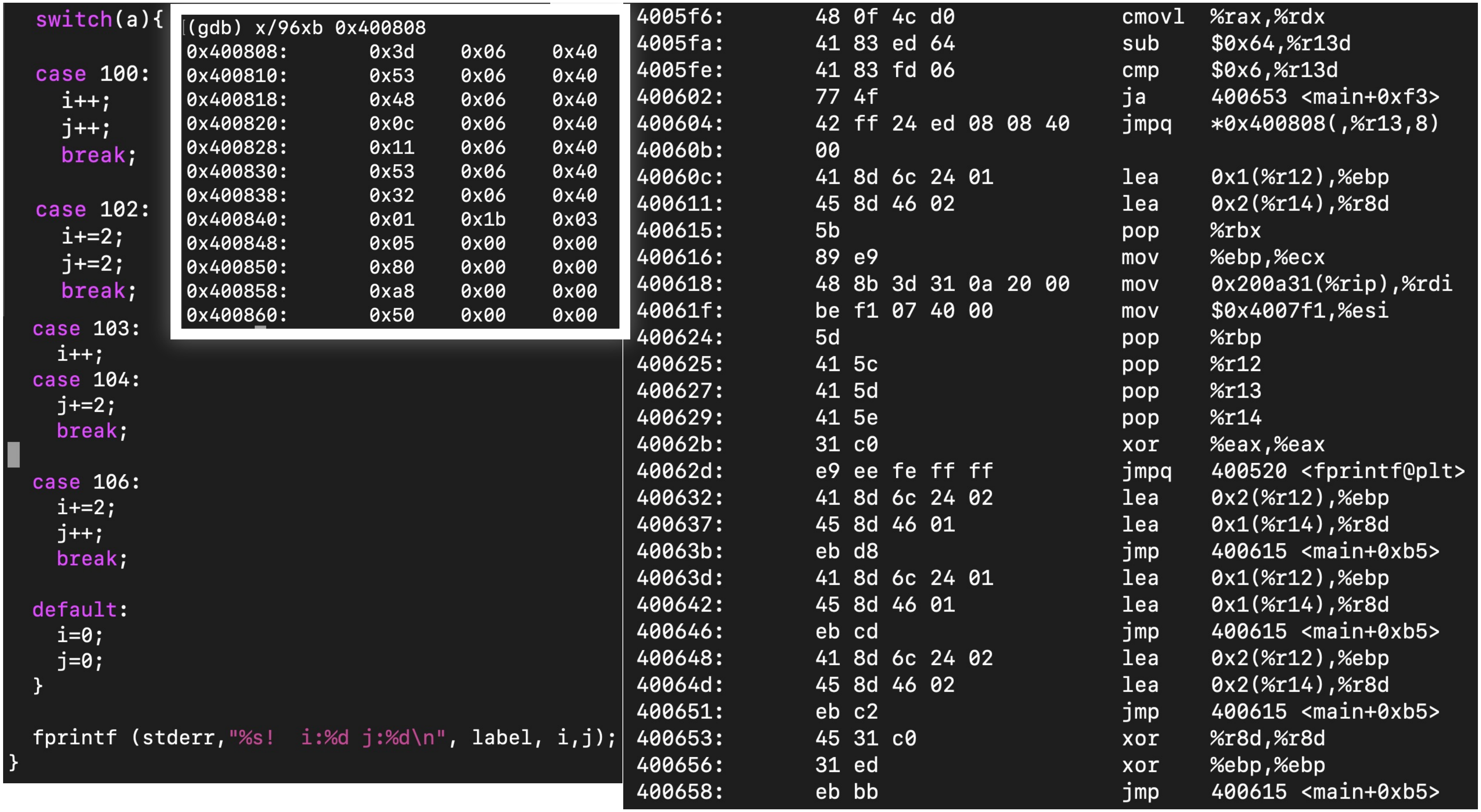
```
4005f6:      48 0f 4c d0             cmovl  %rax,%rdx
4005fa:      41 83 ed 64             sub    $0x64,%r13d
4005fe:      41 83 fd 06             cmp    $0x6,%r13d
                                     ja     400653 <main+0xf3>
                                     jmpq   *0x400808(,%r13,8)

                                     lea    0x1(%r12),%ebp
                                     lea    0x2(%r14),%r8d
                                     pop    %rbx
                                     mov    %ebp,%ecx
                                     mov    0x200a31(%rip),%rdi
                                     mov    $0x4007f1,%esi
                                     pop    %rbp
                                     pop    %r12
                                     pop    %r13
                                     pop    %r14
                                     xor    %eax,%eax
                                     jmpq   400520 <fprintf@plt>
                                     lea    0x2(%r12),%ebp
                                     lea    0x1(%r14),%r8d
                                     jmp    400615 <main+0xb5>
                                     lea    0x1(%r12),%ebp
                                     lea    0x1(%r14),%r8d
                                     jmp    400615 <main+0xb5>
                                     lea    0x2(%r12),%ebp
40064d:      45 8d 46 02             lea    0x2(%r14),%r8d
400651:      eb c2                   jmp    400615 <main+0xb5>
400653:      45 31 c0                xor    %r8d,%r8d
400656:      31 ed                   xor    %ebp,%ebp
400658:      eb bb                   jmp    400615 <main+0xb5>
```



```
  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,
}
```

```
4005f6:       48 0f 4c d0             cmovl  %rax,%rdx
4005fa:       41 83 ed 64             sub    $0x64,%r13d
4005fe:       41 83 fd 06             cmp    $0x6,%r13d
400602:       77 4f                   ja     400653 <main+0xf3>
400604:       42 ff 24 ed 08 08 40    jmpq   *0x400808(,%r13,8)
40060b:       00
40060c:       41 8d 6c 24 01          lea    0x1(%r12),%ebp
400611:       45 8d 46 02             lea    0x2(%r14),%r8d
400615:       5b                      pop    %rbx
400616:       89 e9                   mov    %ebp,%ecx
400618:       48 8b 3d 31 0a 20 00    mov    0x200a31(%rip),%rdi
40061f:       be f1 07 40 00          mov    $0x4007f1,%esi
400624:       5d                      pop    %rbp
400625:       41 5c                   pop    %r12
```

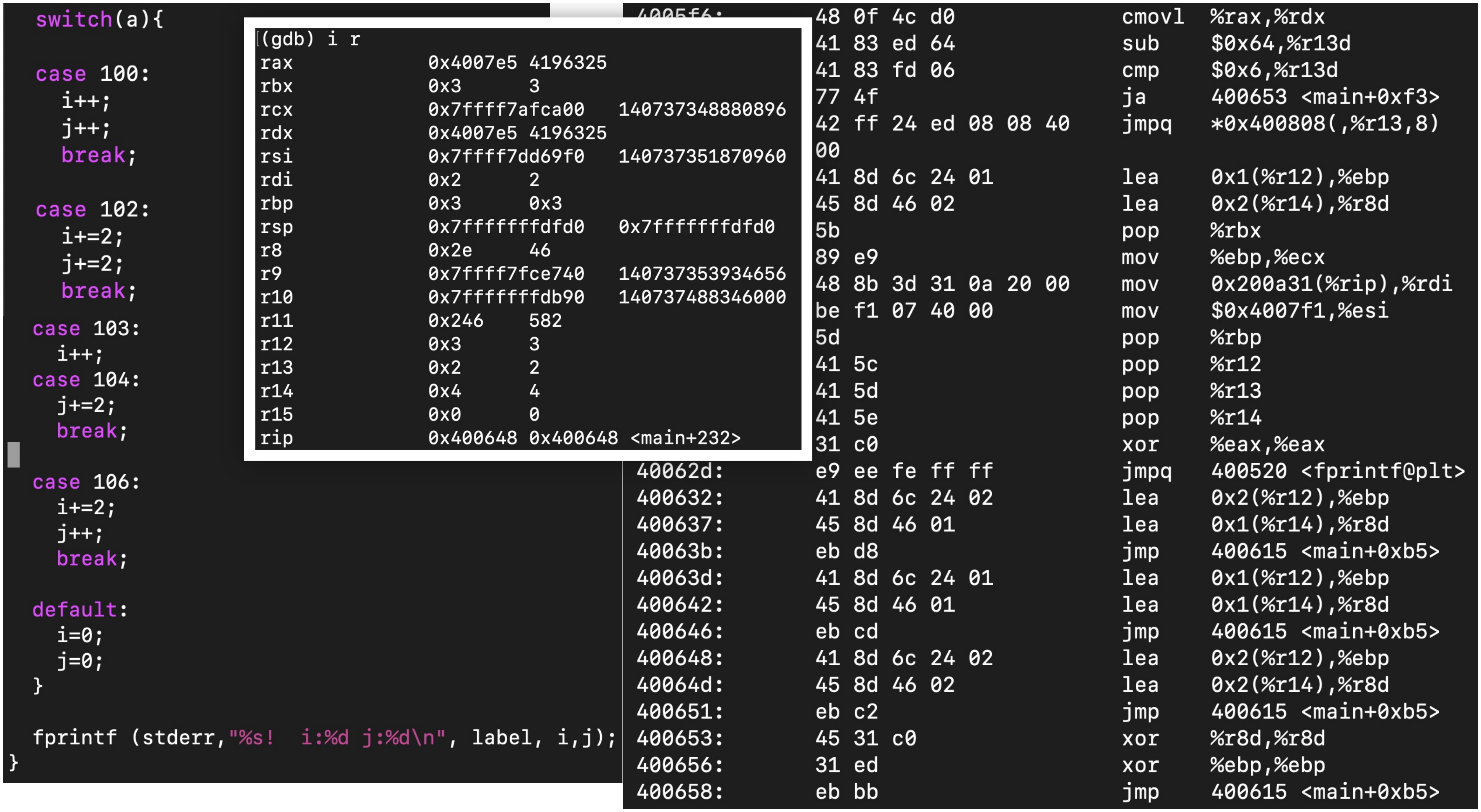
```
(gdb) x/96xb 0x400808
0x400808:       0x3d    0x06    0x40    0x00    0x00    0x00    0x00    0x00
0x400810:       0x53    0x06    0x40    0x00    0x00    0x00    0x00    0x00
0x400818:       0x48    0x06    0x40    0x00    0x00    0x00    0x00    0x00
0x400820:       0x0c    0x06    0x40    0x00    0x00    0x00    0x00    0x00
0x400828:       0x11    0x06    0x40    0x00    0x00    0x00    0x00    0x00
0x400830:       0x53    0x06    0x40    0x00    0x00    0x00    0x00    0x00
0x400838:       0x32    0x06    0x40    0x00    0x00    0x00    0x00    0x00
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
0x400858:       0xa8    0x00    0x00    0x00    0x1a    0xfe    0xff    0xff
0x400860:       0x50    0x00    0x00    0x00    0x10    0xff    0xff    0xff
```



```
  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);
}
```

```
(gdb) x/96xb 0x400808
0x400808:       0x3d    0x06    0x40
0x400810:       0x53    0x06    0x40
0x400818:       0x48    0x06    0x40
0x400820:       0x0c    0x06    0x40
0x400828:       0x11    0x06    0x40
0x400830:       0x53    0x06    0x40
0x400838:       0x32    0x06    0x40
0x400840:       0x01    0x1b    0x03
0x400848:       0x05    0x00    0x00
0x400850:       0x80    0x00    0x00
0x400858:       0xa8    0x00    0x00
0x400860:       0x50    0x00    0x00
```

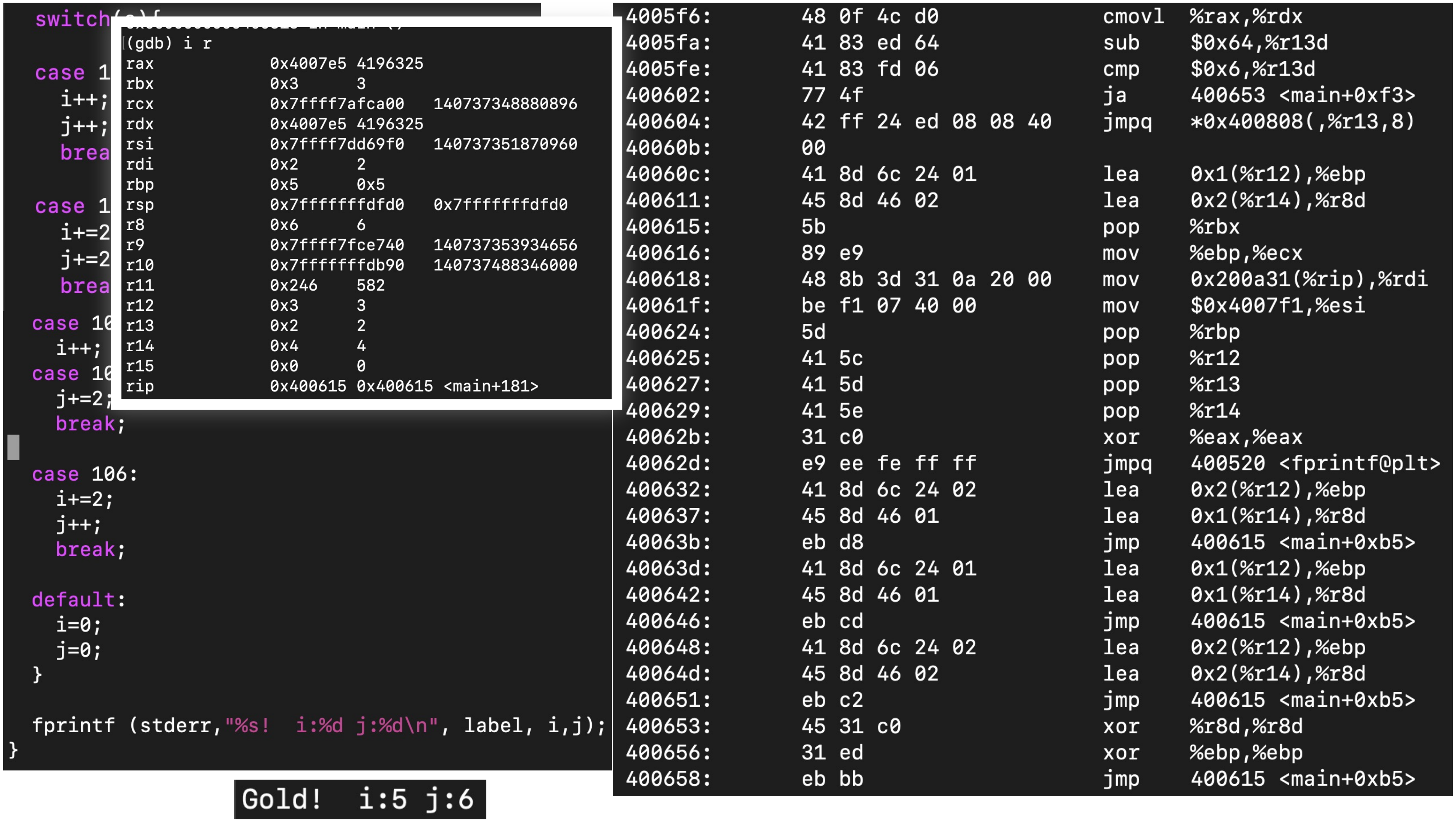
```
4005f6:     48 0f 4c d0              cmovl  %rax,%rdx
4005fa:     41 83 ed 64              sub    $0x64,%r13d
4005fe:     41 83 fd 06              cmp    $0x6,%r13d
400602:     77 4f                    ja     400653 <main+0xf3>
400604:     42 ff 24 ed 08 08 40     jmpq   *0x400808(,%r13,8)
40060b: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



```
  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);
}
```

```
(gdb) i r
rax            0x4007e5 4196325
rbx            0x3      3
rcx            0x7ffff7afca00   140737348880896
rdx            0x4007e5 4196325
rsi            0x7ffff7dd69f0   140737351870960
rdi            0x2      2
rbp            0x3      0x3
rsp            0x7fffffffdfd0   0x7fffffffdfd0
r8             0x2e     46
r9             0x7ffff7fce740   140737353934656
r10            0x7fffffffdb90   140737488346000
r11            0x246    582
r12            0x3      3
r13            0x2      2
r14            0x4      4
r15            0x0      0
rip            0x400648 0x400648 <main+232>
```

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



```
  switch(c){

  case 1
    i++;
    j++;
    brea

  case 1
    i+=2
    j+=2
    brea
  case 10
    i++;
  case 10
    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);
}
```

```
(gdb) i r
rax            0x4007e5 4196325
rbx            0x3      3
rcx            0x7ffff7afca00   140737348880896
rdx            0x4007e5 4196325
rsi            0x7ffff7dd69f0   140737351870960
rdi            0x2      2
rbp            0x5      0x5
rsp            0x7fffffffdfd0   0x7fffffffdfd0
r8             0x6      6
r9             0x7ffff7fce740   140737353934656
r10            0x7fffffffdb90   140737488346000
r11            0x246    582
r12            0x3      3
r13            0x2      2
r14            0x4      4
r15            0x0      0
rip            0x400615 0x400615 <main+181>
```

```
Gold!  i:5 j:6
```

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