1. %rsp %esi = $0x402720

$0x402720

Joy shared with others are more enjoyed.

1. $0x402a21 %d %d %d %d %d %d

1 2 4 8 16 32

3、

$0x402776 %d %c %d

Ja 无符号，第一个大于第二个跳转(后面的为第一个)

Je 相等时跳转

Jg 有符号，第一个大于第二个跳转

第一个要为有符号数>2

第二个要为无符号数<7 %rsp16 0-7

0x402790 0 0x67 103 g 587

0x402798 1 0x65 101 e 687

0x4027A0 2 0x69 105 i 942

0x4027A8 3 0x6d 109 m 0x1a9 425

0x4027B0 4 0x72 114 r 0xbd 189

0x4027B8 5 0x73 115 s 0x34d 845

0x4027C0 6 0x66 102 f 0x266 614

0x4027C8 7 0x6a 106 j 0x368 872

4、

[cmp 是一个汇编指令，用于比较两个操作数的值。它将第一个操作数减去第二个操作数，并根据结果设置条件码寄存器的值。如果第一个操作数小于第二个操作数，则条件码寄存器的符号标志位（SF）为 1；如果两个操作数相等，则零标志位（ZF）为 1；如果结果溢出，则溢出标志位（OF）为 1。](https://www.testing.com/tests/comprehensive-metabolic-panel-cmp/" \t "_blank)

%eax = 2

[jbe 是一个条件跳转指令，它会根据条件码寄存器的值来决定是否跳转到指定的地址。如果 ZF 的值为 1 或 CF 的值为 1，则会跳转到指定地址，否则不会跳转 1](https://www.springer.com/journal/10551" \t "https://www.bing.com/_blank).

(%rsp) = 0xe

%edx = 0xe

%esi = 0

%edi = 0xe

%eax = 0xe

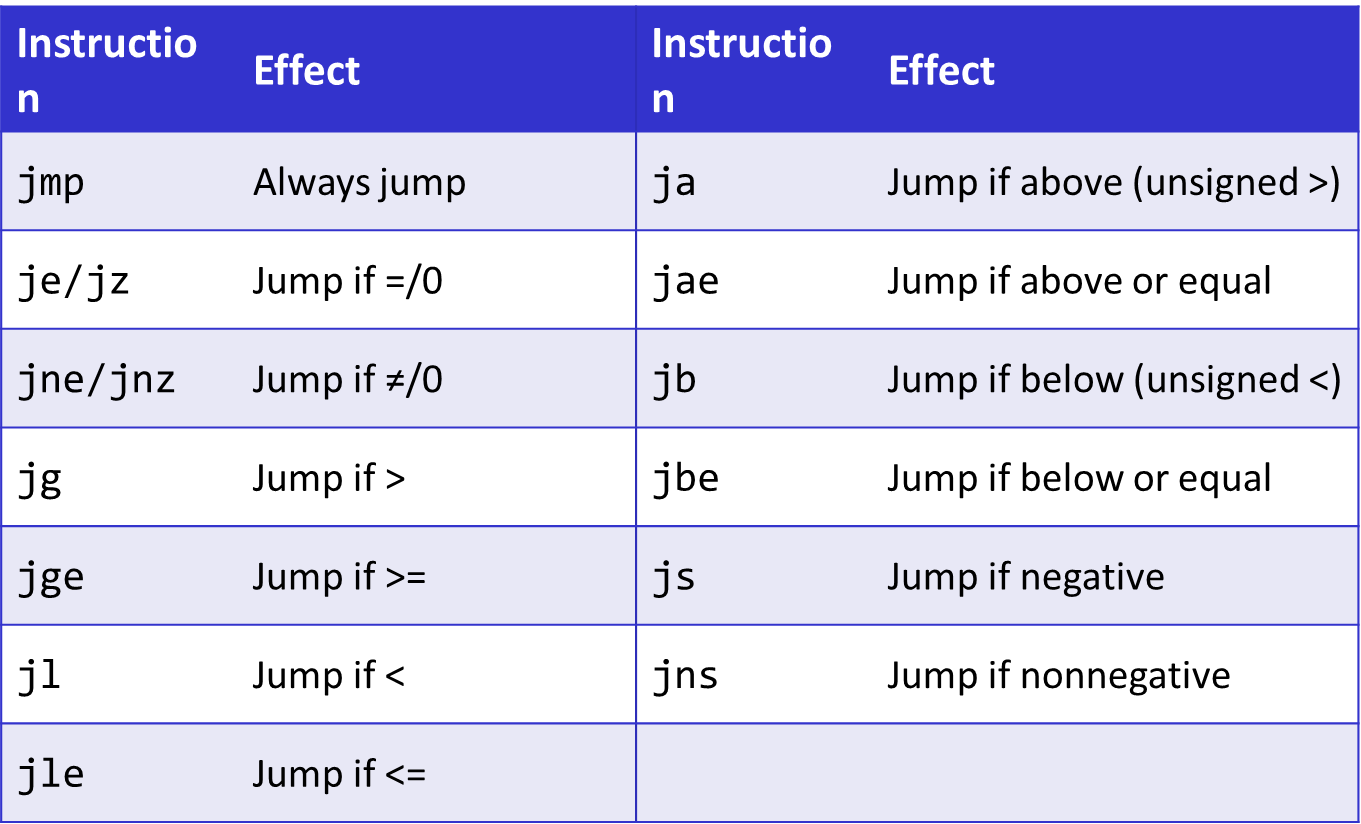
%ecx逻辑右移31位 0

%eax = 7

%ecx = 7

$0x402a2d %d %d

8 1(要递归一次使%rax为0，然后执行加一,最后才能避开爆炸判断



5、

$0x40277f “oilers”

0x4027d0 “maduiersnfotvbyl” 10 4 15 5 6 7

1010 j 0100 （d） 1111（o） 0101 （e） 0110 （f）0111 (g)

6、

0x6042f0 <node1>: 0x39a 0x1 0x604300 <node2> 0x0

0x604300 <node2>: 0x8d 0x2 0x604310 <node3> 0x0

0x604310 <node3>: 0x1e5 0x3 0x604320 <node4> 0x0

0x604320 <node4>: 0x10c 0x4 0x604330 <node5> 0x0

0x604330 <node5>: 0x1f1 0x5 0x604340 <node6> 0x0

0x604340 <node6>: 0x3ac 0x6 0x0 0x0

0x8d (2)< 0x10c(4) < 0x1e5(3) < 0x1f1(5) < 0x39a(1) < 0x3ac(6)

6 1 5 3 4 2

7、

0x402a77: "%d %d %s"

(gdb) x/s 0x402a80

0x402a80: "DrEvil" //输入%d %d %s 即可进入秘密炸弹，炸弹四后输入即可

(gdb) x/s 0x4028d8

0x4028d8: "Curses, you've found the secret phase!"

(gdb) x/s 0x402900

0x402900: "But finding it and solving it are quite different..."

(gdb) x/s 0x402938

0x402938: "Congratulations! You've defused the bomb!"

(gdb) x/s 0x402968

0x402968: "Your instructor has been notified and will verify your solution."

二叉树

1、Forget the memories, continue to be life, miss, just pass by.

2、

第31位为0

A[m]+i=A[m+1]

1 2 4 7 11 16 21

0 1 3 6 10 15 21也行

3、

3(28) 0x67(23) 0xe4(24)

3 0x67 228 0xe4 103

所以答案为3 g 228

...

4、w0 <= 14

W3 = w2 - w1 = 12

W3 = w3 + w3>>31 = w3 ; w3 = w1 + w3>1 = 6

14 7（暴力求解）

5、

W1 = a[i];

X4 = 0x5400

W3 = 66

0x4026a8 <array.4328>: 0x02 0x00 0x00 0x00 0x0a 0x00 0x00 0x00

0x4026b0 <array.4328+8>: 0x06 0x00 0x00 0x00 0x01 0x00 0x00 0x00

0x4026b8 <array.4328+16>: 0x0c 0x00 0x00 0x00 0x10 0x00 0x00 0x00

0x4026c0 <array.4328+24>: 0x09 0x00 0x00 0x00 0x03 0x00 0x00 0x00

0x4026c8 <array.4328+32>: 0x04 0x00 0x00 0x00 0x07 0x00 0x00 0x00

0x4026d0 <array.4328+40>: 0x0e 0x00 0x00 0x00 0x05 0x00 0x00 0x00

0x4026d8 <array.4328+48>: 0x0b 0x00 0x00 0x00 0x08 0x00 0x00 0x00

0x4026e0 <array.4328+56>: 0x0f 0x00 0x00 0x00 0x0d 0x00 0x00 0x00

6 + 12 + 9 + 14 + 11 + 14

偏移量 8 16 24 40 48 40

2 4 6 10 12 10

0010 0100 0110 1010 1100 1010

B D F J L J

6、

0x420110 <node1>: 0x1000003a4 0x420288 <node2> 1

(gdb) x/2 0x420288

0x420288 <node2>: 0x2000003a2 0x420298 <node3> 2

(gdb) x/2 0x420298

0x420298 <node3>: 0x3000000d0 0x4202a8 <node4> 6

(gdb) x/2 0x4202a8

0x4202a8 <node4>: 0x400000144 0x4202b8 <node5> 5

(gdb) x/2 0x4202b8

0x4202b8 <node5>: 0x500000196 0x4202c8 <node6> 4

(gdb) x/2 0x4202c8

0x4202c8 <node6>: 0x600000370 0x0 3

1 2 6 5 4 3

7、

(gdb) x/s 0x402980

0x402980: "DrEvil"

0x24 or 0x8