phase_4

313233343536

ee428
ee424
ee420
ee41C
ee418
ee414
ee410
ee40C
ee408 — } func4
ee404
ee400

13   31
$=$
→ return 3.

$\%rsp+8$

11 11 → return 1.
10 01 → return 5

8 16 → return 1
8 21 → return 1
8 20 → return 1
8 19 →   1
   18
   17 →   1

8 8 →   1

1+2(rax) → rax.

ecx = edi.
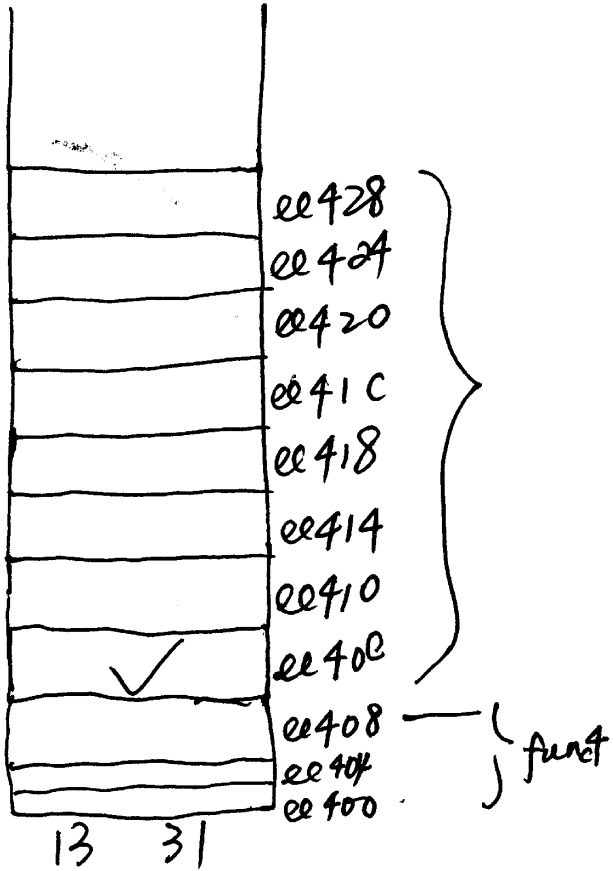
$\%rcx = \%rsp + 0xC = 0xee41C$
$\%rdx = \%rsp + 0x8 = 0xee418$
$\%esi = 0x4025cf$
$*(\%rsp + 0x8) - \$0xe$
$\%edx = \$0xe = 14$
$\%esi = 0$
$\%edi = *(\%rsp + 8) = 13$

$\%eax = \%edx = 14$ →0
$\%eax = \%eax - \%esi = 14$
$\%ecx = \%eax = 14$
$\%ecx = \%ecx >> 31 = 0$ 符号位
$\%eax = \%eax + \%ecx = 14$ 加符号位
$\%eax = \%eax >> 1 = \%eax/2 = 7$
$\%ecx = \%rax + \%rsi = 7$

$\%ecx - \%edi ?$

$\%eax = 0$
$\%ecx - \%edi ?$

$\%esi = \%rcx + 1 = 8$

$\%eax = 14 - 8 = 6$
$\%eax = 6/2 = 3$
$\%ecx = \%rax + \%rsi = 3 + 8 = 11$

$\%eax = 0$ $\%rsi = 12$

1   0 1 0 1
16 8 4 2 1
0   1 0 0 0 0 0 0.
1   0 1 0 0

$6 \times 6 = 36 + 5 = 41$