

phase - 6.1

%r14	ee420
%r13	ee418
%r12	ee410
%rbp	ee408
%rbx	ee400
0xb03320	ee3f8
0xb03310	ee3f0
0xb03300	ee3e8
0xb032f0	ee3e0
0xb032e0	ee3d8
0xb032d0	ee3d0
0	ee3c8
6 5	ee3c0
4 3	ee3b8
2 1	ee3b0

小
↑
0x1bb ←
0x1dd ←
~~0xb032f0~~ ←
0x263 ←
0x39c ←
0xa8 ←
0x14c ←
大

443 ④
477 ③
691 ②
924 ①
168 ⑥
332 ⑤

$\%r13 = \%rsp$
 $\%r14 = \%rsp$
 $\%r12d = 0$
 $\%rbp = \%r13 = \%rsp$
 $\%eax = \cancel{(\%r13)} = \%rsp$ 第4数
 $\%eax = \%eax - 1 = 5$
 $\%r12d = \%r12d + 1 = 1$
 $\%ebx = \%r12d = 1$
 $\%rax = 1$
 $\%eax = \cancel{(\%rsp + 4 \%rax)} = 5 \rightarrow$ 第2数
 $(\%rbp + 0) - \%eax$
 第4数 \neq 第2数
 $\%ebx = \%ebx + 1 = 2$
 $\%ebx - 5$
 $\%rax = 2$

$\%rsi = \%rsp + 0x18 = ee3c8$
 $\%rax = \%r14 = ee3b0$
 $\%ecx = 7$
 $\%edx = \%ecx = 7$
 $\%edx = \%edx - \cancel{(\%rax)} =$
 $\cancel{(\%rax)} = \%edx = 1$
 $\%rax = \%rax + 4 = ee3b4$ 2数
 $\%rax - \%rsi$
 $\%ecx = \%rsp + \%rsi = ee3b0 + 0$ 3数
 $\cancel{(\%rax + \%rsp + 2 \%rsi)} = \%rdx$
 $\cancel{(0x20 + \%rsp + 2 \%rsi)} =$
 $\%rsi = \%rsi + 4 = 4$
 $\%ecx = \%rsp + \%rsi =$ 3数

6 5 4 3 2 1
 ↓
 7-6 7-5
 1 5 4 3 2 1
 2 — 477
 1 — 3320 — 443
 3 — 3360 — 691
 5 — 3200 — 168
 4 — 32f0 — 924
 6 — 32d0 — 332

6 4 5 3 1 2
 6 4 3 2 1 0
 10 6 3 1 0
 10 11 7 4 2 1
 4321 65

$\%eax = 1$
 $\%rdx = \cancel{(\%rdx + 0x8)} = 0xb032e0$
 $\%rbx = \cancel{(\%rsp + 0x20)} = 0xb032d0$
 $\%rax = \%rsp + 0x28 = ee3d8$
 $\%rsi = \%rsp + 0x50 = ee400$
 $\%rcx = \%rbx = 0xb032d0$
 $\%rdx = \cancel{(\%rax)} = 0xb032e0$

phase - b. 2

$$*(\%rbx + 0x8) = *(0x6032d8) = \%rdi = 0x6032e0$$

$$\%ebp = 5$$

$$\%rax = *(\%rbx + 8) = *(0x6032d8) = 0x6032e0$$

$$\%eax = *(\%rax) = \underline{0xa8}$$

$$*(\%rbx) \underset{14c}{\geq} \%eax \underset{a8}$$

$$\%rbx = *(\%rbx + 8) = 0x6032e0$$

$$\%ebp = \%ebp - 1 = 4$$