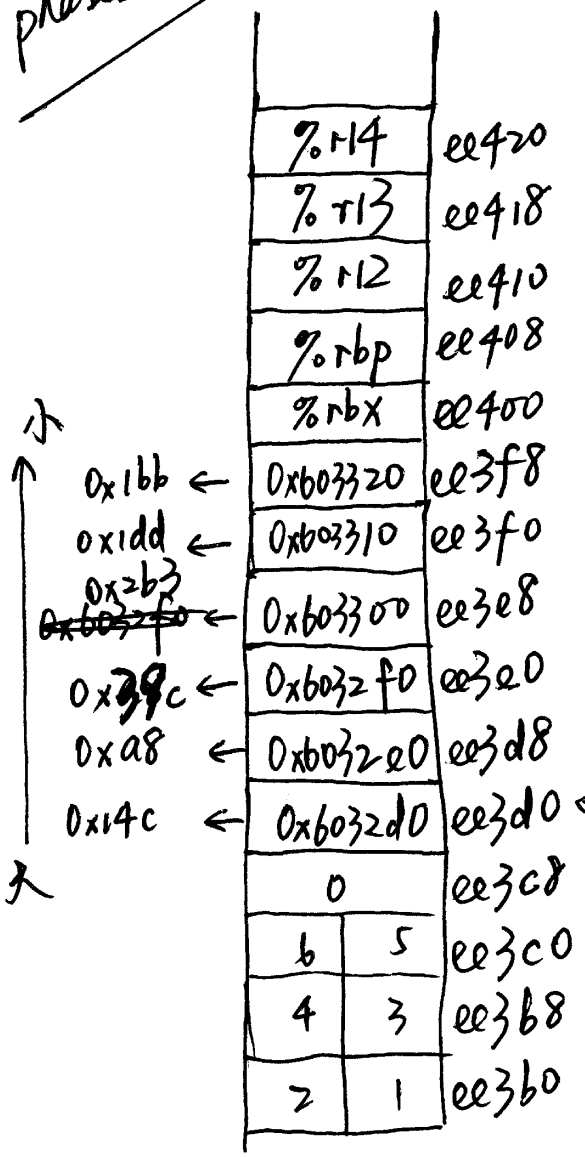
phase_6.1



%r13 = %rsp
%rsi = %rsp
%r14 = %rsp
%r12d = 0
%rbp = %r13 = %rsp
%eax = *(%r13) = %rsp 第一个数

%eax = %eax - 1 = 5
%r12d = %r12d + 1 = 1
%ebx = %r12d = 1

443 ④ ③ %ebx = %r12d = 1
477 ③ ④ %rax = 1
691 ② ⑤ %eax = *(%rsp + 4*%rax) = 5 → 第2个
824 ① ⑥ *(%rbp + 0) - %eax
168 ⑥ ① 第6个 ≠ 第2个
332 ⑤ ② %ebx = %ebx + 1 = 2
%ebx - 5

%rax = 2

%rsi = %rsp + 0x18 = ee3c8
%rax = %r14 = ee3b0
%ecx = 7
%edx = %ecx = 7
%edx = %edx - *(%rax) = 7 - 1
*(%rax) = %edx = 1
%rax = %rax + 4 = ee3b4 · 2个
%rax - %rsi

%ecx = %rsp + *%rsi = ee3b0 + 0 - 1个
(0x20 + %rsp + 2%rsi) = %rdx
*(0x20 + 3b0 + 2*0)
%rsi = %rsi + 4 = 4
%ecx = %rsp + %rsi = 3个

%eax = 1
%rdx = *(%rdx + 0x8) = 0xb032e0

%rbx = *(%rsp + 0x20) = 0xb032d0
%rax = %rsp + 0x28 = ee3d8
%rsi = %rsp + 0x50 = ee400
%rcx = %rbx = 0xb032d0
%rdx = *(%rax) = 0xb03200

6 5 4 3 2 1
↓
7-6 7-5
1 5 4 3 2 1

2 — 477
1 — 3320 — 443
3 — 3300 — 691
5 — 3200 — 168
4 — 32f0 — 824
6 — 32d0 — 332

6 4 5 3 1 2

6 4 3 2 1 0
1 0 6 3 1 0
1 0 7 4 2 1

4 3 2 1 6 5

phase-6.2

*(%rcx+0x8) = *(0x6032d8) = %rdx = 0x6032e0

%ebp = 5

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

%eax = *(%rax) = 0xa8

*(%rbx) ≥ %eax

14c a8

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

%ebp = %ebp - 1 = 4