


Executable Before/After Relocation

00000000 <main>:

```
. . .
e: 83 ec 04      sub    $0x4,%esp
11: e8 fc ff ff ff call   12 <main+0x12>
      12: R_386_PC32 swap
16: 83 c4 04      add    $0x4,%esp
. . .
```

-4(수행시의 PC 보정값)



08048380 <main>:

```
. . .
804838e: 83 ec 04      sub    $0x4,%esp
8048391: e8 ?? ?? ?? ?? call   80503b0 <swap>
8048396: 83 c4 04      add    $0x4,%esp
. . .
```

(1) Call swap()을 수행할때의 PC의 값은 ?


(2) swap() 의 주소가 080503b0 라고 하면 relocation이 끝나서 ?? ?? ?? ?? 에 들어갈 값을 계산하시오.

Before Relocation (.text) swap.o

0000000000000000 <swap>:

```
0: 55                push    %rbp
1: 48 89 e5          mov     %rsp,%rbp
4: 48 c7 05 00 00 00 00  movq    $0x0,0x0(%rip)    # f <swap+0xf>
                          7: R_386_PC32          bufp1   -0x8
b: 00 00 00 00
                          b: R_386_32 buf+0x4
f: 48 8b 05 00 00 00 00  mov     0x0(%rip),%rax    # 16 <swap+0x16>
                          12: R_386_PC32          bufp0   -0x4
16: 8b 00            mov     (%rax),%eax
18: 89 45 fc          mov     %eax,-0x4(%rbp)
1b: 48 8b 05 00 00 00 00  mov     0x0(%rip),%rax    # 22 <swap+0x22>
                          1e: R_386_PC32          bufp0   -0x4
22: 48 8b 15 00 00 00 00  mov     0x0(%rip),%rdx    # 29 <swap+0x29>
                          25: R_386_PC32          bufp1   -0x4
29: 8b 12            mov     (%rdx),%edx
2b: 89 10            mov     %edx,(%rax)
2d: 48 8b 05 00 00 00 00  mov     0x0(%rip),%rax    # 34 <swap+0x34>
                          30: R_386_PC32          bufp1   -0x4
34: 8b 55 fc          mov     -0x4(%rbp),%edx
37: 89 10            mov     %edx,(%rax)
39: 5d              pop     %rbp
3a: c3              retq
```

(수행시의 PC 보정값)



Swap – Before Relocation

```
0000000000000000 <swap>:
 0:  55                push    %rbp
 1:  48 89 e5          mov     %rsp,%rbp
 4:  48 c7 05 00 00 00 00  movq    $0x0,0x0(%rip)    # f <swap+0xf>
                               7: R_386_PC32          bufp1 -0x8
 b:  00 00 00 00
                               b: R_386_32S buf+0x4
 f:  48 8b 05 00 00 00 00  mov     0x0(%rip),%rax    # 16 <swap+0x16>
```

Swap – After Relocation

```
0000000000400502 <swap>:
400502:  55                push    %rbp
400503:  48 89 e5          mov     %rsp,%rbp
400506:  48 c7 05 ?? ?? ?? ??  movq    $0x60103c,???????(%rip) #600040 <bufp1>
40050d:  3c 10 60 00
400511:  ...                (next instruction)
```

Disassembly of section .bss:

0000000000600040 <bufp1>:

PC-relative Address:

(3) movq를 수행할 시점의 PC는 ? (4) ?? ?? ?? ?? 에 들어갈 주소값을 구하시오.