**Homework 1**

System Programming (12506)

2017029807 성창호

**Q.** gdb에서 x/24x $esp 명령어 통해 출력된 결과와 출력된 스택 영역 데이터의 의미를 기술하라.

**\* Print Result :**

(gdb) br \* 0x0010000c

Breakpoint 1 at 0x10000c

(gdb) c

Continuing.

The target architecture is assumed to be i386

=> 0x10000c: mov %cr4,%eax

Thread 1 hit Breakpoint 1, 0x0010000c in ?? ()

(gdb) info reg

eax 0x0 0

ecx 0x0 0

edx 0x1f0 496

ebx 0x10074 65652

esp 0x7bcc 0x7bcc

ebp 0x7bf8 0x7bf8

esi 0x10074 65652

edi 0x0 0

eip 0x10000c 0x10000c

eflags 0x46 [ PF ZF ]

cs 0x8 8

ss 0x10 16

ds 0x10 16

es 0x10 16

fs 0x0 0

gs 0x0 0

(gdb) x/24x $esp

0x7bcc: 0x00007db7 0x00000000 0x00000000 0x00000000

0x7bdc: 0x00000000 0x00000000 0x00000000 0x00000000

0x7bec: 0x00000000 0x00000000 0x00000000 0x00000000

0x7bfc: 0x00007c4d 0x8ec031fa 0x8ec08ed8 0xa864e4d0

0x7c0c: 0xb0fa7502 0xe464e6d1 0x7502a864 0xe6dfb0fa

0x7c1c: 0x16010f60 0x200f7c78 0xc88366c0 0xc0220f01

**A.** 현재 0x001000c에 breakpoint를 걸어 놓고 스택 영역을 보면, 처음에는 스택 영역이 비어 있다가\_start, 즉 kernel의 entry까지 실행시키면, 0x7bcc에 0x00007db7가 들어있는 것을 볼 수 있다. 이는 bootmain 안에 있는 함수인 entry의 eip 주소가 들어있는 것이다. 그리고 0x7bfc 부분부터 채워져 있는 데이터들은 bootmain을 실행시키기 위한 주소 값들로 보여진다. 즉, call bootmain이 실행되는 곳까지 프로그램을 진행시키고 스택 영역을 보았을 때에는 0x7bfc부터 보여질 것이며 bootmain의 주소인 0x00007c4d부터 데이터가 채워져 있을 것이다.