1. (论述题, 50分)

已知函数funct的C语言代码如下：

1    int funct(void)  {

2        int x, y;

3        scanf("%x %x",  &x, &y);

4        return x - y;  
5     }

函数funct对应的汇编代码如下：

1    funct:

2      pushl      %ebp

3      movl      %esp, %ebp

4      subl        $40,  %esp

5      leal         -8(%ebp),  %eax

6      movl      %eax, 8(%esp)

7      leal         -4(%ebp),  %eax

8      movl      %eax, 4(%esp)

9      movl       $.LC0,  (%esp)

10     call         scanf

11     movl       -4(%ebp),  %eax

12     subl        -8(%ebp),  %eax

13     leave

14      ret

假设函数funct开始执行时R[esp]=0xbc00 0020，R[ebp]=0xbc00 0030，执行第10行call指令后，scanf从标准输入读入的值为0x16和0x100，指向字符串"%x %x”的指针为0x0804c000。

回答下列问题或完成下列任务。

（1）执行第3、10和13行的指令后，寄存器EBP中的内容分别是什么？

（2）执行第3、10和13行的指令后，寄存器ESP中的内容分别是什么？

（3）局部变量x和y所在的存储单元的地址分别是什么？

（4）画出执行第10行指令后funct的栈帧，指出栈帧中的内容及其地址。

(1)

        3:R[ebp]=0xbc00001c    10:R[ebp]=0xbc00001c    13:R[ebp]=0xbc000030

(2)

        3:R[esp]=0xbc00001c     10:R[esp]=0xbbfffff4    13:R[esp]=0xbbfffffo

(3)

        x:0xbc000018    y:0xbc0000014

(4）

图片包含 图示

描述已自动生成

2. (论述题, 50分)

已知两个C语言源程序（教材194页上图4.9），其main函数源代码对应的main.o中.text节和.rel.text节的内容如下所示，其中.text节有一处需要重定位。假定链接后main函数代码起始地址是0x8048386，紧跟在main后的是swap函数的代码，且首地址按4字节边界对齐。要求给出main.o的.text节中需要重定位的符号名、相对于.text节起始位置的位移、所在指令行号、重定位类型、重定位前的内容、重定位后的内容，并给出重定位值的计算过程。

|  |
| --- |
| 1  Disassembly of section .text:  2  00000000 <main>:  3      0:55                    push  %ebp  4      1:89 e5                  mov   %esp, %ebp  5      3:83 e4 f0                and   $0xfffffff0, %esp  6      6:e8 fc ff ff ff            call   7 <main+0x7>  7      7: R\_386\_PC32 swap  8      b:b8 00 00 00 00            mov   $0x0, %eax  9     10:c9                    leave  10     11:c3                   ret |

