(gdb) run

Starting program: /home/cs-student/Downloads/a.out

Breakpoint 1, main () at examine\_stack.c:41

41      int result = freshman (month, day, year);

(gdb) disas main

Dump of assembler code for function main:

  0x08048564 <+0>:    push   %ebp

  0x08048565 <+1>:    mov %esp,%ebp

  0x08048567 <+3>:    and $0xfffffff0,%esp

  0x0804856a <+6>:    sub $0x20,%esp

  0x0804856d <+9>:    movl   $0x7dc,0x10(%esp)

  0x08048575 <+17>:    movl   $0xc,0x14(%esp)

  0x0804857d <+25>:    movl   $0x19,0x18(%esp)

=> 0x08048585 <+33>:    mov 0x10(%esp),%eax

  0x08048589 <+37>:    mov %eax,0x8(%esp)

  0x0804858d <+41>:    mov 0x18(%esp),%eax

  0x08048591 <+45>:    mov %eax,0x4(%esp)

  0x08048595 <+49>:    mov 0x14(%esp),%eax

  0x08048599 <+53>:    mov %eax,(%esp)

  0x0804859c <+56>:    call   0x80484f2 <freshman>

  0x080485a1 <+61>:    mov %eax,0x1c(%esp)

  0x080485a5 <+65>:    movl   $0x0,(%esp)

  0x080485ac <+72>:    call   0x8048350 <exit@plt>

End of assembler dump.

(gdb) p $ebp

$1 = (void \*) 0xffffd6f8

(gdb) x/32xw $esp

0xffffd6d0:    0x00000001    0xffffd794    0xffffd79c    0xf7e4c19d

0xffffd6e0:    0x000007dc    0x0000000c    0x00000019    0xf7fc0000

0xffffd6f0:    0x080485c0    0x00000000    0x00000000    0xf7e32ad3

0xffffd700:    0x00000001    0xffffd794    0xffffd79c    0xf7feacca

0xffffd710:    0x00000001    0xffffd794    0xffffd734    0x0804a018

0xffffd720:    0x0804822c    0xf7fc0000    0x00000000    0x00000000

0xffffd730:    0x00000000    0x8bace869    0xb257cc79    0x00000000

0xffffd740:    0x00000000    0x00000000    0x00000001    0x08048370

(gdb) continue

Continuing.

Breakpoint 2, freshman (a=12, b=25, c=2012) at examine\_stack.c:29

29      sophomore (a + b, c);

(gdb) disas freshman

Dump of assembler code for function freshman:

  0x080484f2 <+0>:    push   %ebp

  0x080484f3 <+1>:    mov %esp,%ebp

  0x080484f5 <+3>:    sub $0x48,%esp

  0x080484f8 <+6>:    mov %gs:0x14,%eax

  0x080484fe <+12>:    mov %eax,-0xc(%ebp)

  0x08048501 <+15>:    xor %eax,%eax

  0x08048503 <+17>:    movl   $0x616c6548,-0x2a(%ebp)

  0x0804850a <+24>:    movl   $0x206e616d,-0x26(%ebp)

  0x08048511 <+31>:    movl   $0x6c6c6148,-0x22(%ebp)

  0x08048518 <+38>:    movl   $0x73,-0x1e(%ebp)

  0x0804851f <+45>:    movl   $0x0,-0x1a(%ebp)

  0x08048526 <+52>:    movl   $0x0,-0x16(%ebp)

  0x0804852d <+59>:    movl   $0x0,-0x12(%ebp)

  0x08048534 <+66>:    movw   $0x0,-0xe(%ebp)

=> 0x0804853a <+72>:    mov 0xc(%ebp),%eax

  0x0804853d <+75>:    mov 0x8(%ebp),%edx

  0x08048540 <+78>:    add %eax,%edx

  0x08048542 <+80>:    mov 0x10(%ebp),%eax

  0x08048545 <+83>:    mov %eax,0x4(%esp)

  0x08048549 <+87>:    mov %edx,(%esp)

  0x0804854c <+90>:    call   0x80484d2 <sophomore>

  0x08048551 <+95>:    mov -0xc(%ebp),%ecx

  0x08048554 <+98>:    xor %gs:0x14,%ecx

  0x0804855b <+105>:    je 0x8048562 <freshman+112>

  0x0804855d <+107>:    call   0x8048330 <\_\_stack\_chk\_fail@plt>

  0x08048562 <+112>:    leave

  0x08048563 <+113>:    ret

End of assembler dump.

(gdb) p $ebp

$2 = (void \*) 0xffffd6c8

(gdb) x/32xw $esp

0xffffd680:    0xffffd734    0xffffd6a8    0xffffd6a0    0x0804825c

0xffffd690:    0xf7ffd938    0x00000000    0x000000c2    0x6548d716

0xffffd6a0:    0x616d616c    0x6148206e    0x00736c6c    0x00000000

0xffffd6b0:    0x00000000    0x00000000    0x00000000    0x8e7e1600

0xffffd6c0:    0xffffd8c0    0x0000002f    0xffffd6f8    0x080485a1

0xffffd6d0:    0x0000000c    0x00000019    0x000007dc    0xf7e4c19d

0xffffd6e0:    0x000007dc    0x0000000c    0x00000019    0xf7fc0000

0xffffd6f0:    0x080485c0    0x00000000    0x00000000    0xf7e32ad3

(gdb) c

Continuing.

Breakpoint 3, sophomore (a=37, b=2012) at examine\_stack.c:23

23      junior (b, &tiny);

(gdb) disas sophomore

Dump of assembler code for function sophomore:

  0x080484d2 <+0>:    push   %ebp

  0x080484d3 <+1>:    mov %esp,%ebp

  0x080484d5 <+3>:    sub $0x28,%esp

  0x080484d8 <+6>:    movw   $0x8,-0xa(%ebp)

=> 0x080484de <+12>:    lea -0xa(%ebp),%eax

  0x080484e1 <+15>:    mov %eax,0x4(%esp)

  0x080484e5 <+19>:    mov 0xc(%ebp),%eax

  0x080484e8 <+22>:    mov %eax,(%esp)

  0x080484eb <+25>:    call   0x8048481 <junior>

  0x080484f0 <+30>:    leave

  0x080484f1 <+31>:    ret

End of assembler dump.

(gdb) p $ebp

$3 = (void \*) 0xffffd678

(gdb) x/32xw $esp

0xffffd650:    0x00000001    0x00000000    0x00000001    0xf7ffd938

0xffffd660:    0x00000000    0x00000000    0x00000000    0x00080000

0xffffd670:    0x00000003    0x00000009    0xffffd6c8    0x08048551

0xffffd680:    0x00000025    0x000007dc    0xffffd6a0    0x0804825c

0xffffd690:    0xf7ffd938    0x00000000    0x000000c2    0x6548d716

0xffffd6a0:    0x616d616c    0x6148206e    0x00736c6c    0x00000000

0xffffd6b0:    0x00000000    0x00000000    0x00000000    0x8e7e1600

0xffffd6c0:    0xffffd8c0    0x0000002f    0xffffd6f8    0x080485a1

(gdb) c

Continuing.

Breakpoint 4, junior (x=2012, y=0xffffd66e) at examine\_stack.c:16

16      senior (x, 2);

(gdb) disas junior

Dump of assembler code for function junior:

  0x08048481 <+0>:    push   %ebp

  0x08048482 <+1>:    mov %esp,%ebp

  0x08048484 <+3>:    sub $0x28,%esp

  0x08048487 <+6>:    mov 0xc(%ebp),%eax

  0x0804848a <+9>:    mov %eax,-0x1c(%ebp)

  0x0804848d <+12>:    mov %gs:0x14,%eax

  0x08048493 <+18>:    mov %eax,-0xc(%ebp)

  0x08048496 <+21>:    xor %eax,%eax

  0x08048498 <+23>:    movl   $0x67756f63,-0x16(%ebp)

  0x0804849f <+30>:    movl   $0x737261,-0x12(%ebp)

  0x080484a6 <+37>:    movw   $0x0,-0xe(%ebp)

=> 0x080484ac <+43>:    movl   $0x2,0x4(%esp)

  0x080484b4 <+51>:    mov 0x8(%ebp),%eax

  0x080484b7 <+54>:    mov %eax,(%esp)

  0x080484ba <+57>:    call   0x804846d <senior>

  0x080484bf <+62>:    mov -0xc(%ebp),%edx

  0x080484c2 <+65>:    xor %gs:0x14,%edx

  0x080484c9 <+72>:    je 0x80484d0 <junior+79>

  0x080484cb <+74>:    call   0x8048330 <\_\_stack\_chk\_fail@plt>

  0x080484d0 <+79>:    leave

  0x080484d1 <+80>:    ret

End of assembler dump.

(gdb) p $ebp

$4 = (void \*) 0xffffd648

(gdb) x/32xw $esp

0xffffd620:    0x00000000    0xf7ffd000    0xffffd734    0xffffd66e

0xffffd630:    0x6f63d6f0    0x72616775    0x00000073    0x8e7e1600

0xffffd640:    0xffffd6a8    0xf7ffda94    0xffffd678    0x080484f0

0xffffd650:    0x000007dc    0xffffd66e    0x00000001    0xf7ffd938

0xffffd660:    0x00000000    0x00000000    0x00000000    0x00080000

0xffffd670:    0x00000003    0x00000009    0xffffd6c8    0x08048551

0xffffd680:    0x00000025    0x000007dc    0xffffd6a0    0x0804825c

0xffffd690:    0xf7ffd938    0x00000000    0x000000c2    0x6548d716

(gdb) c

Continuing.

Breakpoint 5, senior (a=2012, b=2) at examine\_stack.c:9

9      return 12;

(gdb) disas senior

Dump of assembler code for function senior:

  0x0804846d <+0>:    push   %ebp

  0x0804846e <+1>:    mov %esp,%ebp

  0x08048470 <+3>:    sub $0x10,%esp

  0x08048473 <+6>:    movl   $0x7530,-0x4(%ebp)

=> 0x0804847a <+13>:    mov $0xc,%eax

  0x0804847f <+18>:    leave

  0x08048480 <+19>:    ret

End of assembler dump.

(gdb) p $ebp

$5 = (void \*) 0xffffd618

(gdb) x/32xw $esp

0xffffd608:    0x0804825c    0xf7e26474    0x0804820c    0x00007530

0xffffd618:    0xffffd648    0x080484bf    0x000007dc    0x00000002

0xffffd628:    0xffffd734    0xffffd66e    0x6f63d6f0    0x72616775

0xffffd638:    0x00000073    0x8e7e1600    0xffffd6a8    0xf7ffda94

0xffffd648:    0xffffd678    0x080484f0    0x000007dc    0xffffd66e

0xffffd658:    0x00000001    0xf7ffd938    0x00000000    0x00000000

0xffffd668:    0x00000000    0x00080000    0x00000003    0x00000009

0xffffd678:    0xffffd6c8    0x08048551    0x00000025    0x000007dc

(gdb)