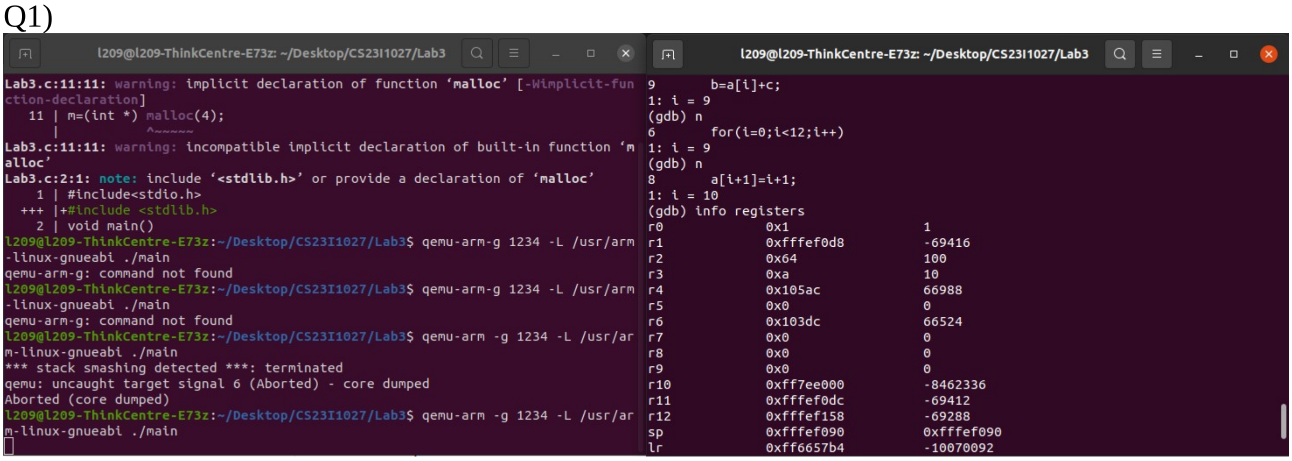
Q1)

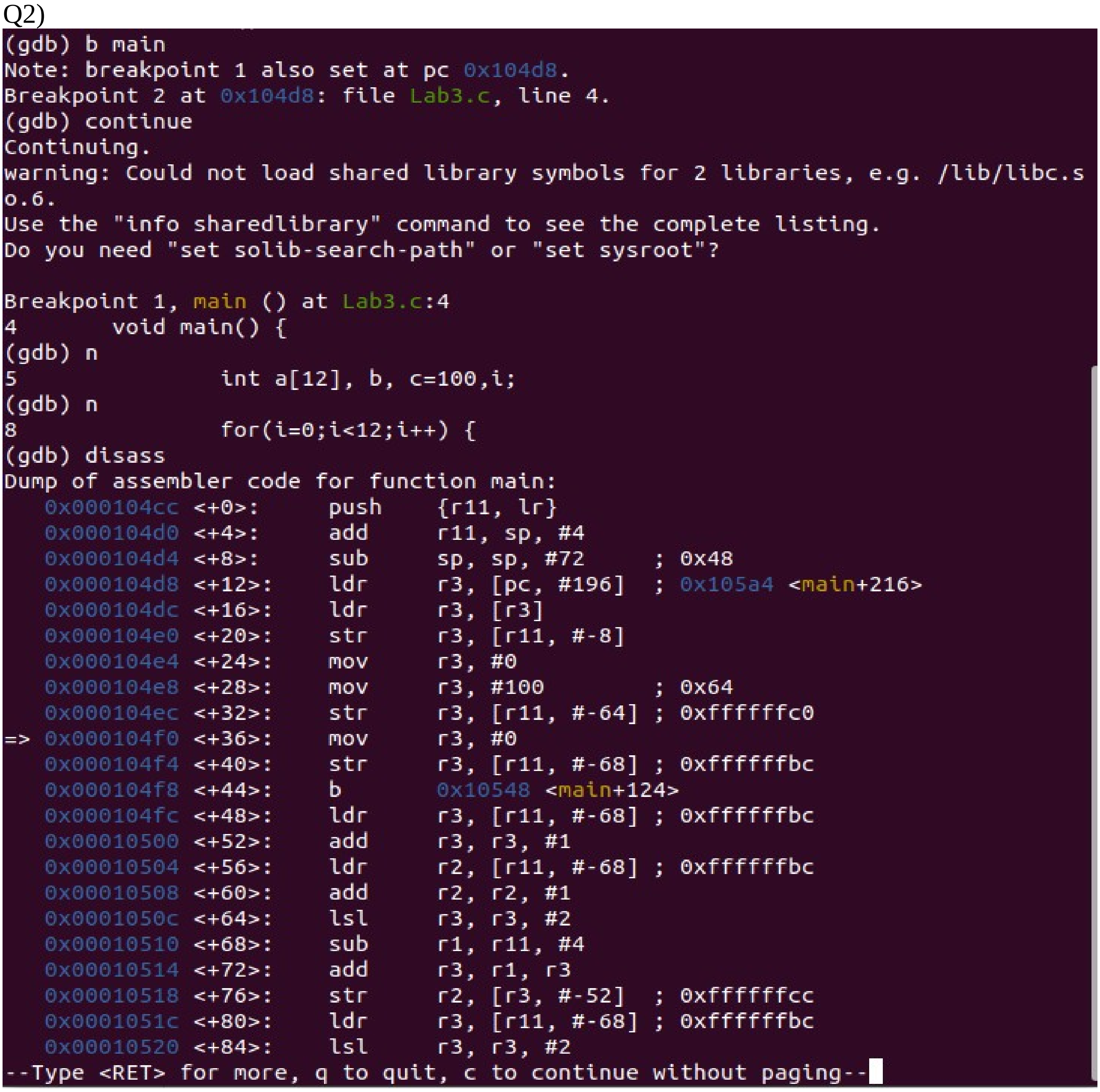

l209@l209-ThinkCentre-E73z: ~/Desktop/CS23I1027/Lab3
l209@l209-ThinkCentre-E73z: ~/Desktop/CS23I1027/Lab3

```
Lab3.c:11:11: warning: implicit declaration of function ‘malloc’ [-Wimplicit-fun
ction-declaration]
   11 | m=(int *) malloc(4);
      |           ^~~~~~
Lab3.c:11:11: warning: incompatible implicit declaration of built-in function ‘m
alloc’
Lab3.c:2:1: note: include ‘<stdlib.h>’ or provide a declaration of ‘malloc’
    1 | #include<stdio.h>
  +++ |+#include <stdlib.h>
    2 | void main()
l209@l209-ThinkCentre-E73z:~/Desktop/CS23I1027/Lab3$ qemu-arm-g 1234 -L /usr/arm
-linux-gnueabi ./main
qemu-arm-g: command not found
l209@l209-ThinkCentre-E73z:~/Desktop/CS23I1027/Lab3$ qemu-arm-g 1234 -L /usr/arm
-linux-gnueabi ./main
qemu-arm-g: command not found
l209@l209-ThinkCentre-E73z:~/Desktop/CS23I1027/Lab3$ qemu-arm -g 1234 -L /usr/ar
m-linux-gnueabi ./main
*** stack smashing detected ***: terminated
qemu: uncaught target signal 6 (Aborted) - core dumped
Aborted (core dumped)
l209@l209-ThinkCentre-E73z:~/Desktop/CS23I1027/Lab3$ qemu-arm -g 1234 -L /usr/ar
m-linux-gnueabi ./main
```

```
9         b=a[i]+c;
1: i = 9
(gdb) n
6         for(i=0;i<12;i++)
1: i = 9
(gdb) n
8         a[i+1]=i+1;
1: i = 10
(gdb) info registers
r0             0x1                 1
r1             0xfffef0d8          -69416
r2             0x64                100
r3             0xa                 10
r4             0x105ac             66988
r5             0x0                 0
r6             0x103dc             66524
r7             0x0                 0
r8             0x0                 0
r9             0x0                 0
r10            0xff7ee000          -8462336
r11            0xfffef0dc          -69412
r12            0xfffef158          -69288
sp             0xfffef090          0xfffef090
lr             0xff6657b4          -10070092
```

r5 = 0

Q2)



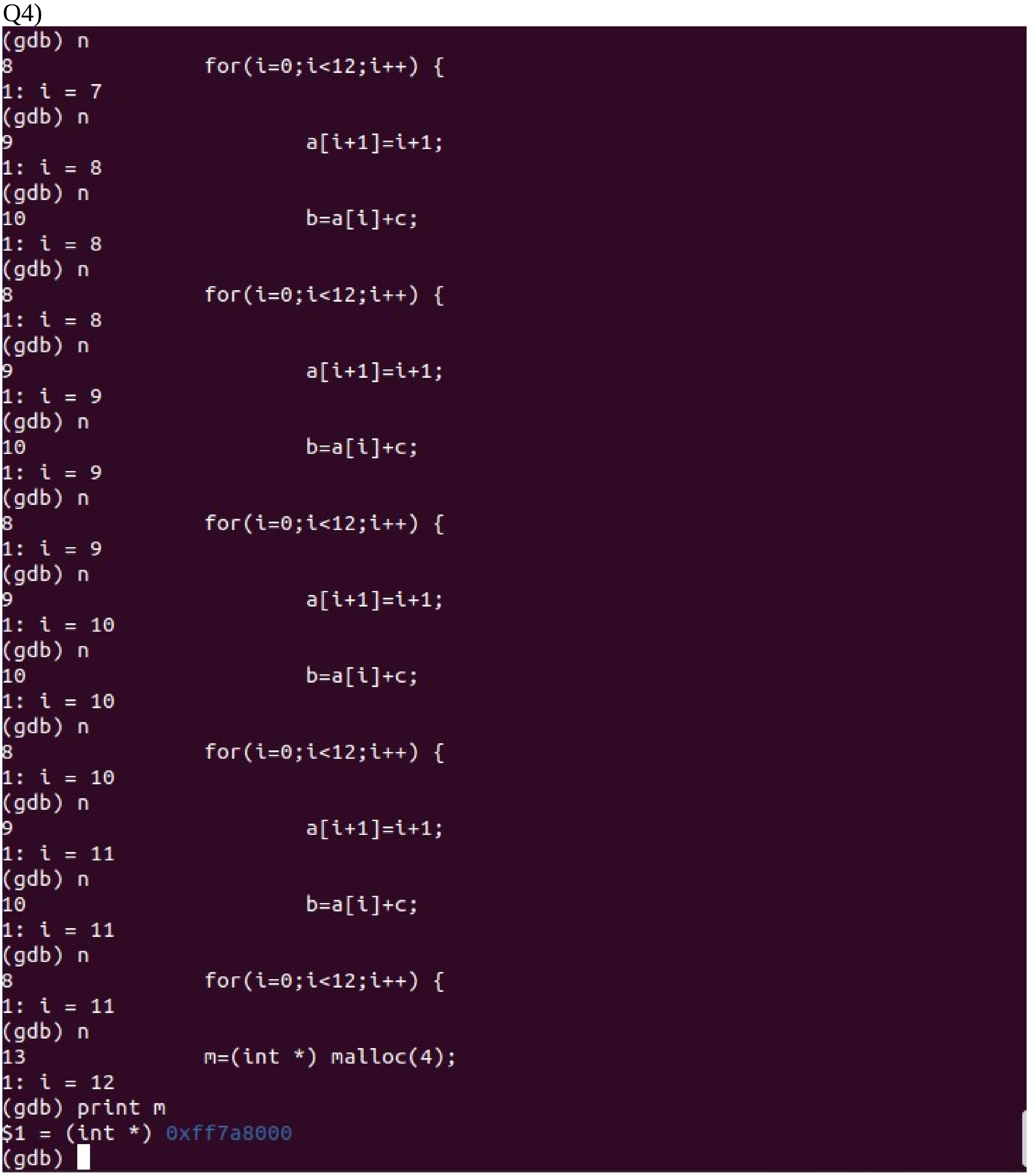
```
(gdb) b main
Note: breakpoint 1 also set at pc 0x104d8.
Breakpoint 2 at 0x104d8: file Lab3.c, line 4.
(gdb) continue
Continuing.
warning: Could not load shared library symbols for 2 libraries, e.g. /lib/libc.s
o.6.
Use the "info sharedlibrary" command to see the complete listing.
Do you need "set solib-search-path" or "set sysroot"?

Breakpoint 1, main () at Lab3.c:4
4         void main() {
(gdb) n
5                 int a[12], b, c=100,i;
(gdb) n
8                 for(i=0;i<12;i++) {
(gdb) disass
Dump of assembler code for function main:
   0x000104cc <+0>:     push    {r11, lr}
   0x000104d0 <+4>:     add     r11, sp, #4
   0x000104d4 <+8>:     sub     sp, sp, #72     ; 0x48
   0x000104d8 <+12>:    ldr     r3, [pc, #196]  ; 0x105a4 <main+216>
   0x000104dc <+16>:    ldr     r3, [r3]
   0x000104e0 <+20>:    str     r3, [r11, #-8]
   0x000104e4 <+24>:    mov     r3, #0
   0x000104e8 <+28>:    mov     r3, #100        ; 0x64
   0x000104ec <+32>:    str     r3, [r11, #-64] ; 0xffffffc0
=> 0x000104f0 <+36>:    mov     r3, #0
   0x000104f4 <+40>:    str     r3, [r11, #-68] ; 0xffffffbc
   0x000104f8 <+44>:    b       0x10548 <main+124>
   0x000104fc <+48>:    ldr     r3, [r11, #-68] ; 0xffffffbc
   0x00010500 <+52>:    add     r3, r3, #1
   0x00010504 <+56>:    ldr     r2, [r11, #-68] ; 0xffffffbc
   0x00010508 <+60>:    add     r2, r2, #1
   0x0001050c <+64>:    lsl     r3, r3, #2
   0x00010510 <+68>:    sub     r1, r11, #4
   0x00010514 <+72>:    add     r3, r1, r3
   0x00010518 <+76>:    str     r2, [r3, #-52]  ; 0xffffffcc
   0x0001051c <+80>:    ldr     r3, [r11, #-68] ; 0xffffffbc
   0x00010520 <+84>:    lsl     r3, r3, #2
--Type <RET> for more, q to quit, c to continue without paging--
```

Stack is accessed 3 times, in 0x000104d0 frame and 0x000104d4 frame.
Once in addition, Once in Accessing while subtracting and once while subtracting itself.

Q3)
Since it is using malloc, Heap memory is being accessed.

Q4)



```
(gdb) n
8               for(i=0;i<12;i++) {
1: i = 7
(gdb) n
9                       a[i+1]=i+1;
1: i = 8
(gdb) n
10                      b=a[i]+c;
1: i = 8
(gdb) n
8               for(i=0;i<12;i++) {
1: i = 8
(gdb) n
9                       a[i+1]=i+1;
1: i = 9
(gdb) n
10                      b=a[i]+c;
1: i = 9
(gdb) n
8               for(i=0;i<12;i++) {
1: i = 9
(gdb) n
9                       a[i+1]=i+1;
1: i = 10
(gdb) n
10                      b=a[i]+c;
1: i = 10
(gdb) n
8               for(i=0;i<12;i++) {
1: i = 10
(gdb) n
9                       a[i+1]=i+1;
1: i = 11
(gdb) n
10                      b=a[i]+c;
1: i = 11
(gdb) n
8               for(i=0;i<12;i++) {
1: i = 11
(gdb) n
13              m=(int *) malloc(4);
1: i = 12
(gdb) print m
$1 = (int *) 0xff7a8000
(gdb) 
```

If the value is NULL, the allocation failed. Here it is not NULL.
(gdb) break malloc
watch *m
print m
info locals