

SS 1

SS 2

```
bg777155@molly:~/csc231X +  
bg777155@molly:~/csc231/intro-c$ cat mem1.c  
#include <stdio.h>  
  
typedef struct {  
    int a[2];  
    double d;  
} struct_t;  
  
double fun(int i) {  
    volatile struct_t s;  
    s.d = 3.14;  
    s.a[1] = 10793741824;  
    return s.d;  
}  
  
int main(int argc, char *argv[]) {  
    printf(<fun(0)>: %f\n", fun(0));  
    printf(<fun(1)>: %f\n", fun(1));  
    printf(<fun(2)>: %f\n", fun(2));  
    printf(<fun(3)>: %f\n", fun(3));  
    printf(<fun(4)>: %f\n", fun(4));  
    printf(<fun(5)>: %f\n", fun(5));  
    printf(<fun(6)>: %f\n", fun(6));  
    return 0;  
}  
bg777155@molly:~/csc231/intro-c$
```

```
[...]  
0008 | 0x7fffffff200 --> 0x7fffffff220 --> 0x0  
0006 | 0x7fffffff200 --> 0x55555551d9 (<main+29>) lea rdi,[rip+0xe28] # 0x555555556008  
-----  
Legend: code, data, rodata, value  
10 | s.d = 3.14;  
gdb-peda$ x /t $s.d  
0x7fffffff1e0 : 00000000000000010101010101010101010101010101010101010111011011  
gdb-peda$ n  
-----  
Registers  
RAX: 0x0  
RBX: 0x555555552a8 (<_libc_csu_init>: endbrq)  
RCX: 0x555555552a8 (<_libc_csu_init>: endbrq)  
RDX: 0x7fffffff328 --> 0x7ffffff90f (<SHELL=/bin/bash>*)  
RSI: 0x7fffffff318 --> 0x7fffffff57c ('/home/bg777155/csc231/intro-c/mem1')  
RDI: 0x0  
RBP: 0x7fffffff200 --> 0x7fffffff220 --> 0x0  
RSP: 0x7fffffff1e0 --> 0x7fffffff200 --> 0x1f7f9e7a0  
RIP: 0x55555555194 (<fun+43>: mov eax,DWORD PTR [rbp-0x24])  
R8 : 0x0  
R9 : 0x7ffff7fe068 (<_dl_fini>: endbrq)  
R10: 0x7ffff7fec08 --> 0xfffffff0  
R11: 0x202  
R12: 0x55555555080 (<_start>: endbrq)  
R13: 0x7fffffff310 --> 0x1  
R14: 0x0  
R15: 0x0  
EFLAGS: 0x246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)  
-----  
Code  
0x55555555185 <fun+28>: xor eax,eax  
0x55555555187 <fun+30>: movsd xmm0,QWORD PTR [rip+8ed9] # 0x555555556008  
0x5555555518f <fun+38>: movsd QWORD PTR [rbp-0x18],xmm0  
=> 0x55555555194 <fun+43>: mov eax,QWORD PTR [rbp-0x24]  
0x55555555197 <fun+46>: cdqe  
0x55555555199 <fun+48>: mov DWORD PTR [rbp+rax+0x28],0x40000000  
0x555555551a1 <fun+56>: movsd xmm0,QWORD PTR [rbp-0x18]  
0x555555551a6 <fun+61>: mov rax,QWORD PTR [rbp-0x8]  
-----  
Stack  
0008 | 0x7fffffff100 --> 0x7fffffff200 --> 0x1f7f9e7a0  
0006 | 0x7fffffff1e0 --> 0xfffffe69  
0016 | 0x7fffffff1e0 --> 0x7ffff7fd1508 (<_dl_main>: endbrq)  
0024 | 0x7fffffff1e0 --> 0x40091eb851eb851f  
0032 | 0x7fffffff1f0 --> 0x7ffff7f9200 --> 0x0  
0040 | 0x7fffffff1f0 --> 0xe99fdb5f1d5df90  
0048 | 0x7fffffff200 --> 0x7fffffff220 --> 0x0  
0056 | 0x7fffffff200 --> 0x55555551d9 (<main+29>) lea rdi,[rip+0xe28] # 0x555555556008  
-----  
Legend: code, data, rodata, value  
11 | s.a[1] = 10793741824;  
gdb-peda$ x /t $s.d  
0x7fffffff1e0 : 0xffffffffffffffff00000000000000010101011000010100011101011000010100011111  
gdb-peda$
```

```
[tab2] ^C^C  
molly: 83.17 Nov-23 10:17 PM
```

```

bg777155@olly:~/csc231/csc231$ cat mem1.c
#include <stdio.h>

typedef struct {
    int a[2];
    double d;
} struct_t;

double fun(int i) {
    volatile struct_t s;
    s.d = 3.14;
    s.a[i] = 1073741824;
    return s.d;
}

int main(int argc, char *argv[]) {
    printf("fun(0): %f\n", fun(0));
    printf("fun(1): %f\n", fun(1));
    printf("fun(2): %f\n", fun(2));
    printf("fun(3): %f\n", fun(3));
    printf("fun(4): %f\n", fun(4));
    printf("fun(5): %f\n", fun(5));
    printf("fun(6): %f\n", fun(6));
    return 0;
}

bg777155@olly:~/csc231/csc231$

```

```

0032 0x7fffffff1f0 (*f2ed29bc*)
0000 0x7fffffff1f0 -> 0x09b4d5fd5d5f900
0008 0x7fffffff1f0 -> 0x7fffffff220 -> 0x0
0056 0x7fffffff208 -> 0x5555555522a (*main+110): lea rdi,[rip+0xdfe] # 0x55555555602f
[-----]
Legend: code, data, rdata, value
10 s.d = 3.14;
gdb-pedal n
[-----]
Registers
RAX: 0x0
RDI: 0x555555552a0 (<_libc_csu_init: endbr64)
RCX: 0x0
RDX: 0x0
RSI: 0x5555555592a0 (*fun(2): 3.140000 '\n')
RIP: 0x3
RBP: 0x7fffffff220 -> 0x7fffffff220 -> 0x0
RSP: 0x7fffffff1f0 (*common/var-003*)
R1P: 0x55555555194 (*fun+43): mov eax,DWORD PTR [rbp-0x24]
R8: 0x0
R9: 0x12
R10: 0x55555555602c -> 0x3328ae756000a20 (' \n')
R11: 0x246
R12: 0x555555555080 (<_start: endbr64)
R13: 0x7fffffff110 -> 0x1
R14: 0x0
R15: 0x0
EFLAGS: 0x246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-----]
Code
0x55555555185 (*fun+20): xor eax,eax
0x55555555187 (*fun+30): movsd xmm0,QWORD PTR [rip+0xd9] # 0x555555556000
0x5555555518f (*fun+38): movsd QWORD PTR [rbp-0x10],xmm0
=> 0x55555555194 (*fun+43): mov eax,DWORD PTR [rbp-0x24]
0x55555555197 (*fun+46): cddq
0x55555555199 (*fun+48): mov QWORD PTR [rbp+rax*4-0x20],0x40000000
0x555555551a1 (*fun+56): movsd xmm0,QWORD PTR [rbp-0x10]
0x555555551a6 (*fun+61): mov rax,QWORD PTR [rbp-0x8]
[-----]
Stack
0000 0x7fffffff1f0 (*common/var-003*)
0008 0x7fffffff1f0 -> 0x32d726176
0024 0x7fffffff1f0 -> 0x7ffff7fc930 -> 0x7ffff7ffe190 -> 0x555555554000 -> 0x10182064c457f
0040 0x7fffffff1f0 -> 0x40891eb51eb51f
0032 0x7fffffff1f0 (*f2ed29bc*)
0000 0x7fffffff1f0 -> 0x09b4d5fd5d5f900
0008 0x7fffffff1f0 -> 0x7fffffff220 -> 0x0
0056 0x7fffffff208 -> 0x5555555522a (*main+110): lea rdi,[rip+0xdfe] # 0x55555555602f
[-----]
Legend: code, data, rdata, value
11 s.a[i] = 1073741824;
gdb-pedal x /t %s.d
gdb-pedal n
[-----]
[lab2] 0>gdb

```

```

"olly" 0x306 07-09-22

```

SS 4

[illegible]

Question 2:

$$S = 0$$
$$E = 1$$

$M = 1.000000000000000000001010001111010111000010100011111_2$

Segment of s.a[3] that modified s.d = 01000000000000000000000000000000

Before assignment: 01000000000100100011101011100001010001111010111000010100011111

After assignment: 010000000000000000000000000000001010001111010111000010100011111

Purple is altered portion