

Jack Harrington
 October 26, 2021
 CS-382

Lab 8: Debugging Assembly

```
jack@jack-VirtualBox:~/CS-382/DebugAssembly$ qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g 1239 secret
Please type your Stevens ID:
10463675
```

```
Register group: general
x0      0x412ac0      4270784
x1      0x412ab0      4270768
x2      0x21          33
x3      0x412ad0      4270800
x4      0x0           0
x5      0x3           3
x6      0x218         536
x7      0x0           0
x8      0x10          16
x9      0x4000800140   274886295872
x10     0x0           0
x11     0x10          16
x12     0x412ac2      4270786

0x400394 <L2+20>      ldrb    w20, [sp, #6]
0x400398 <L2+24>      ldrb    w21, [sp]
0x40039c <L2+28>      add     w20, w20, w21
0x4003a0 <L2+32>      ldrb    w21, [sp, #4]
0x4003a4 <L2+36>      ldrb    w22, [sp, #1]
0x4003a8 <L2+40>      ldrb    w23, [sp, #2]
0x4003ac <L2+44>      add     w21, w21, w22
0x4003b0 <L2+48>      add     w21, w21, w23
0x4003b4 <L2+52>      mov     x0, #0x3           // #3
0x4003b8 <L2+56>      sub     sp, sp, #0x1
0x4003bc <L2+60>      str     x30, [sp]
0x4003c0 <L2+64>      bl     0x400330 <malloc@plt>
0x4003c4 <L2+68>      ldr     x30, [sp]

Remote Thread 1.3078 In: L3                                L??  PC: 0x4003d8
Breakpoint 6, 0x00000000004003d8 in L3 ()
(gdb) c
Continuing.

Breakpoint 6, 0x00000000004003d8 in L3 ()
(gdb) c
Continuing.

Breakpoint 6, 0x00000000004003d8 in L3 ()
(gdb) x/s 0x412ac0
0x412ac0:      "!7"
(gdb)
```

Steps to Finding the String: I set breakpoints at each new branch in the command: L1, L2, L3. Then continued until each of the loops were broken out of. This is when I recognized the value of X0 had changed and I wrote out the command 'x/s 0x412ac0'. This gave me the string in the memory address listed above. The following output was observed: '!7'.