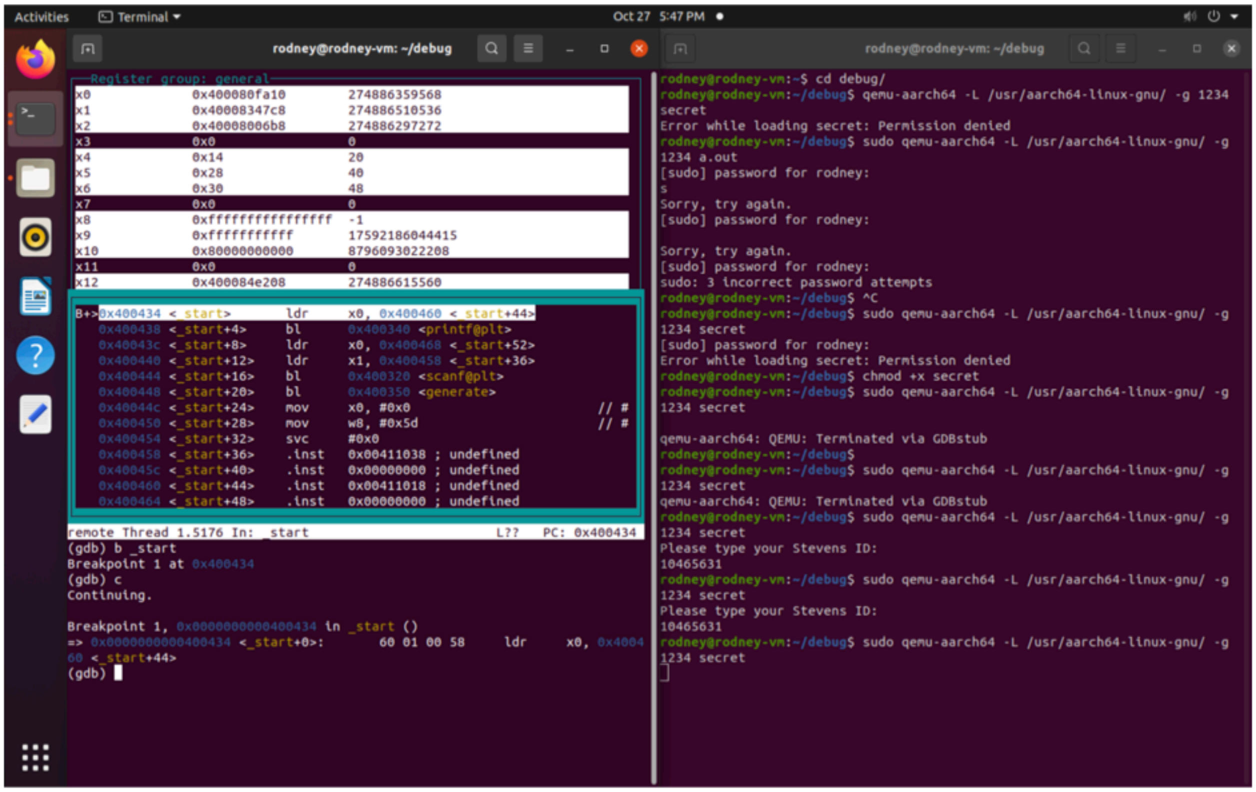
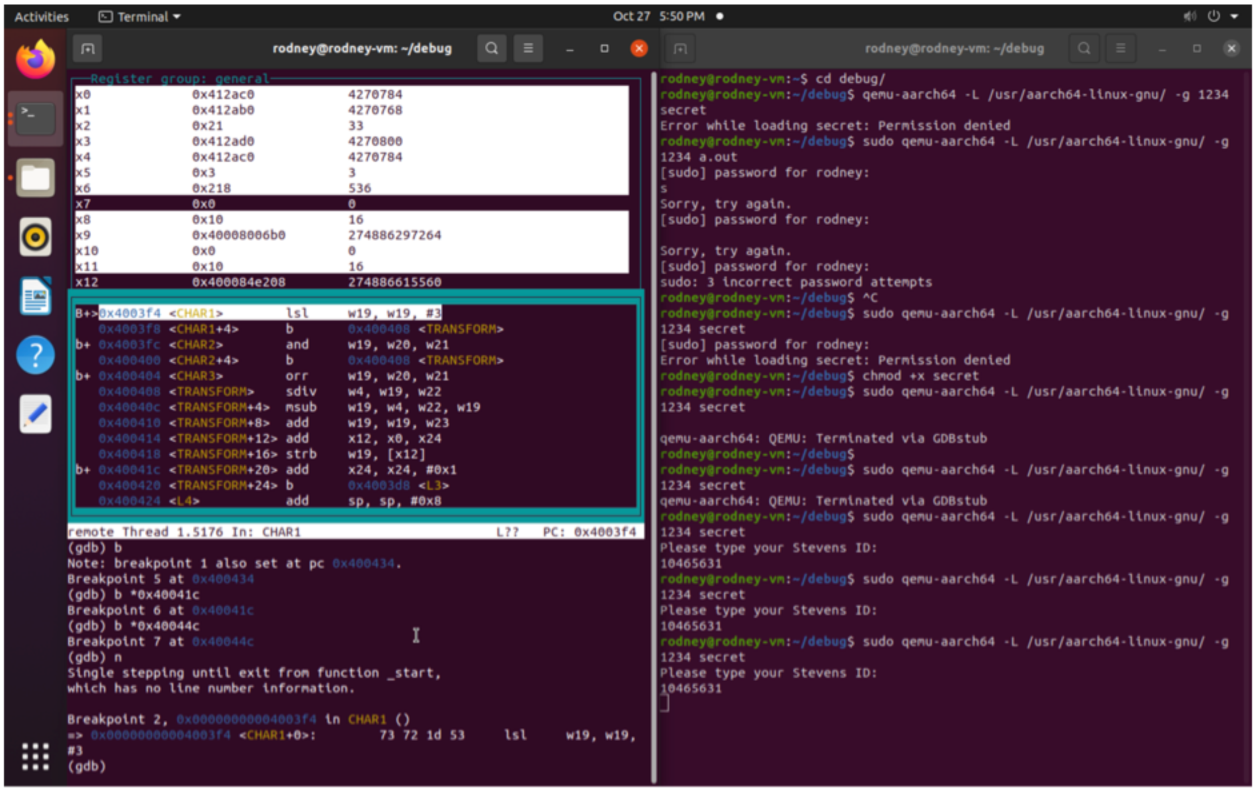
Rodney Wotton
Student ID: 10465631
Shudong Hao
3 Character Secret String “p!/”

In order to find the unique strings that were generated from my Stevens ID, I used breakpoints to find where the registers were storing the string and commands to print out the list that they added it to. I put breakpoints on CHAR1, 2, and 3 as well as one on the TRANSFORM line (0x40041c) that adds each string to the list after each iteration. When observing these three functions and the registers that change with them, I was able to identify that the singular character addresses were stored in x12 and the full character string was stored in x0. After the program was done, I was able to print out 3 character bites of x0 using the command x/3cb $x0, giving me “p”, “!”, and “/”



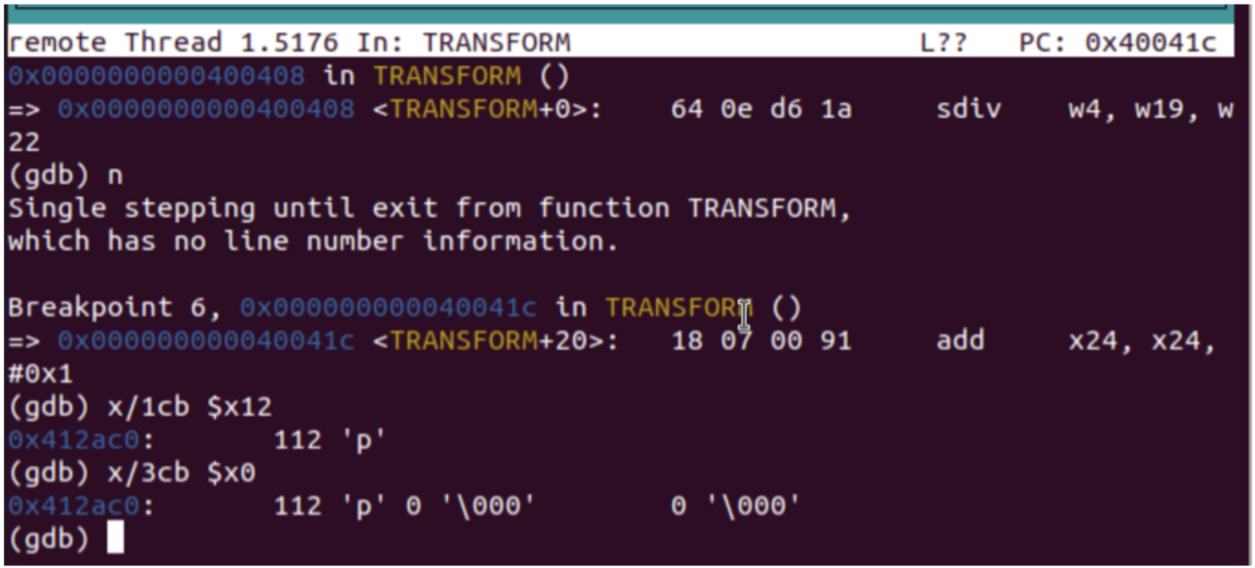
```
-Register group: general-
x0             0x400080fa10        274886359568
x1             0x40008347c8        274886510536
x2             0x40008006b8        274886297272
x3             0x0                 0
x4             0x14                20
x5             0x28                40
x6             0x30                48
x7             0x0                 0
x8             0xffffffffffffffff  -1
x9             0xffffffffff        17592186044415
x10            0x80000000000       8796093022208
x11            0x0                 0
x12            0x400084e208        274886615560

B+>0x400434 <_start>         ldr     x0, 0x400460 <_start+44>
   0x400438 <_start+4>       bl      0x400340 <printf@plt>
   0x40043c <_start+8>       ldr     x0, 0x400468 <_start+52>
   0x400440 <_start+12>      ldr     x1, 0x400458 <_start+36>
   0x400444 <_start+16>      bl      0x400320 <scanf@plt>
   0x400448 <_start+20>      bl      0x400350 <generate>
   0x40044c <_start+24>      mov     x0, #0x0                              // #
   0x400450 <_start+28>      mov     w8, #0x5d                             // #
   0x400454 <_start+32>      svc     #0x0
   0x400458 <_start+36>      .inst   0x00411038 ; undefined
   0x40045c <_start+40>      .inst   0x00000000 ; undefined
   0x400460 <_start+44>      .inst   0x00411018 ; undefined
   0x400464 <_start+48>      .inst   0x00000000 ; undefined

remote Thread 1.5176 In: _start                              L??   PC: 0x400434
(gdb) b _start
Breakpoint 1 at 0x400434
(gdb) c
Continuing.

Breakpoint 1, 0x0000000000400434 in _start ()
=> 0x0000000000400434 <_start+0>:       60 01 00 58     ldr     x0, 0x4004
60 <_start+44>
(gdb) 
```

```
rodney@rodney-vm:~$ cd debug/
rodney@rodney-vm:~/debug$ qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g 1234
secret
Error while loading secret: Permission denied
rodney@rodney-vm:~/debug$ sudo qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g
1234 a.out
[sudo] password for rodney:
s
Sorry, try again.
[sudo] password for rodney:

Sorry, try again.
[sudo] password for rodney:
sudo: 3 incorrect password attempts
rodney@rodney-vm:~/debug$ ^C
rodney@rodney-vm:~/debug$ sudo qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g
1234 secret
[sudo] password for rodney:
Error while loading secret: Permission denied
rodney@rodney-vm:~/debug$ chmod +x secret
rodney@rodney-vm:~/debug$ sudo qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g
1234 secret

qemu-aarch64: QEMU: Terminated via GDBstub
rodney@rodney-vm:~/debug$
rodney@rodney-vm:~/debug$ sudo qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g
1234 secret
qemu-aarch64: QEMU: Terminated via GDBstub
rodney@rodney-vm:~/debug$ sudo qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g
1234 secret
Please type your Stevens ID:
10465631
rodney@rodney-vm:~/debug$ sudo qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g
1234 secret
Please type your Stevens ID:
10465631
rodney@rodney-vm:~/debug$ sudo qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g
1234 secret
```

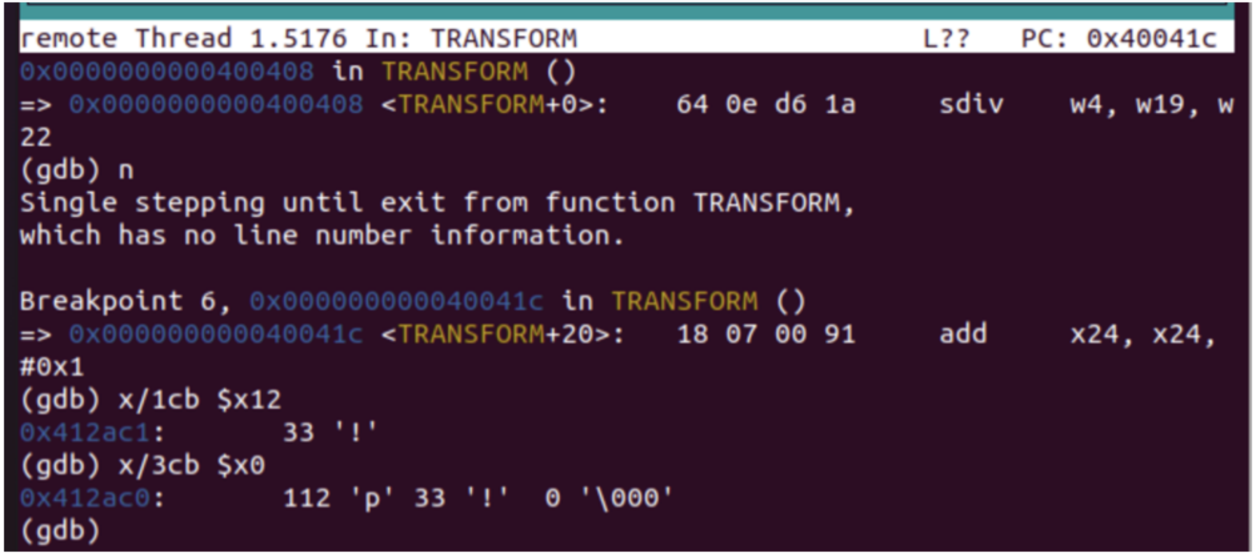


```
Register group: general
x0             0x412ac0            4270784
x1             0x412ab0            4270768
x2             0x21                33
x3             0x412ad0            4270800
x4             0x412ac0            4270784
x5             0x3                 3
x6             0x218               536
x7             0x0                 0
x8             0x10                16
x9             0x40008006b0        274886297264
x10            0x0                 0
x11            0x10                16
x12            0x400084e208        274886615560

B+>0x4003f4 <CHAR1>           lsl     w19, w19, #3
   0x4003f8 <CHAR1+4>         b       0x400408 <TRANSFORM>
b+ 0x4003fc <CHAR2>           and     w19, w20, w21
   0x400400 <CHAR2+4>         b       0x400408 <TRANSFORM>
b+ 0x400404 <CHAR3>           orr     w19, w20, w21
   0x400408 <TRANSFORM>       sdiv    w4, w19, w22
   0x40040c <TRANSFORM+4>     msub    w19, w4, w22, w19
   0x400410 <TRANSFORM+8>     add     w19, w19, w23
   0x400414 <TRANSFORM+12>    add     x12, x0, x24
   0x400418 <TRANSFORM+16>    strb    w19, [x12]
b+ 0x40041c <TRANSFORM+20>    add     x24, x24, #0x1
   0x400420 <TRANSFORM+24>    b       0x4003d8 <L3>
   0x400424 <L4>              add     sp, sp, #0x8
remote Thread 1.5176 In: CHAR1                          L??   PC: 0x4003f4
(gdb) b
Note: breakpoint 1 also set at pc 0x400434.
Breakpoint 5 at 0x400434
(gdb) b *0x40041c
Breakpoint 6 at 0x40041c
(gdb) b *0x40044c
Breakpoint 7 at 0x40044c
(gdb) n
Single stepping until exit from function _start,
which has no line number information.

Breakpoint 2, 0x00000000004003f4 in CHAR1 ()
=> 0x00000000004003f4 <CHAR1+0>:        73 72 1d 53     lsl     w19, w19,
#3
(gdb)
```

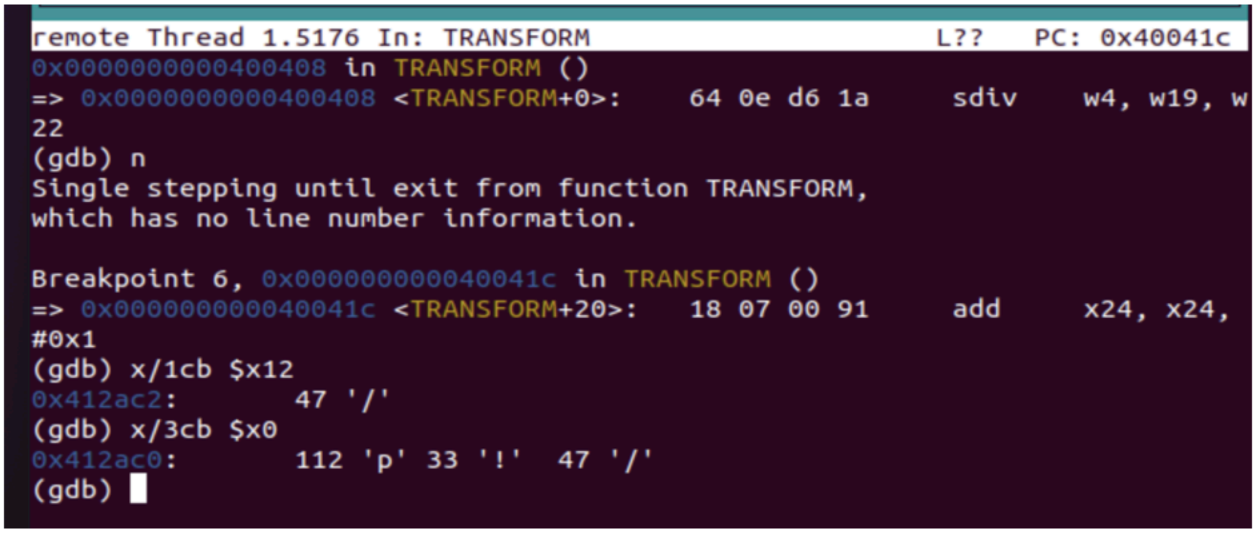
```
rodney@rodney-vm:~$ cd debug/
rodney@rodney-vm:~/debug$ qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g 1234
secret
Error while loading secret: Permission denied
rodney@rodney-vm:~/debug$ sudo qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g
1234 a.out
[sudo] password for rodney:
s
Sorry, try again.
[sudo] password for rodney:

Sorry, try again.
[sudo] password for rodney:
sudo: 3 incorrect password attempts
rodney@rodney-vm:~/debug$ ^C
rodney@rodney-vm:~/debug$ sudo qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g
1234 secret
[sudo] password for rodney:
Error while loading secret: Permission denied
rodney@rodney-vm:~/debug$ chmod +x secret
rodney@rodney-vm:~/debug$ sudo qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g
1234 secret

qemu-aarch64: QEMU: Terminated via GDBstub
rodney@rodney-vm:~/debug$
rodney@rodney-vm:~/debug$ sudo qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g
1234 secret
qemu-aarch64: QEMU: Terminated via GDBstub
rodney@rodney-vm:~/debug$ sudo qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g
1234 secret
Please type your Stevens ID:
10465631
rodney@rodney-vm:~/debug$ sudo qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g
1234 secret
Please type your Stevens ID:
10465631
rodney@rodney-vm:~/debug$ sudo qemu-aarch64 -L /usr/aarch64-linux-gnu/ -g
1234 secret
Please type your Stevens ID:
10465631
```



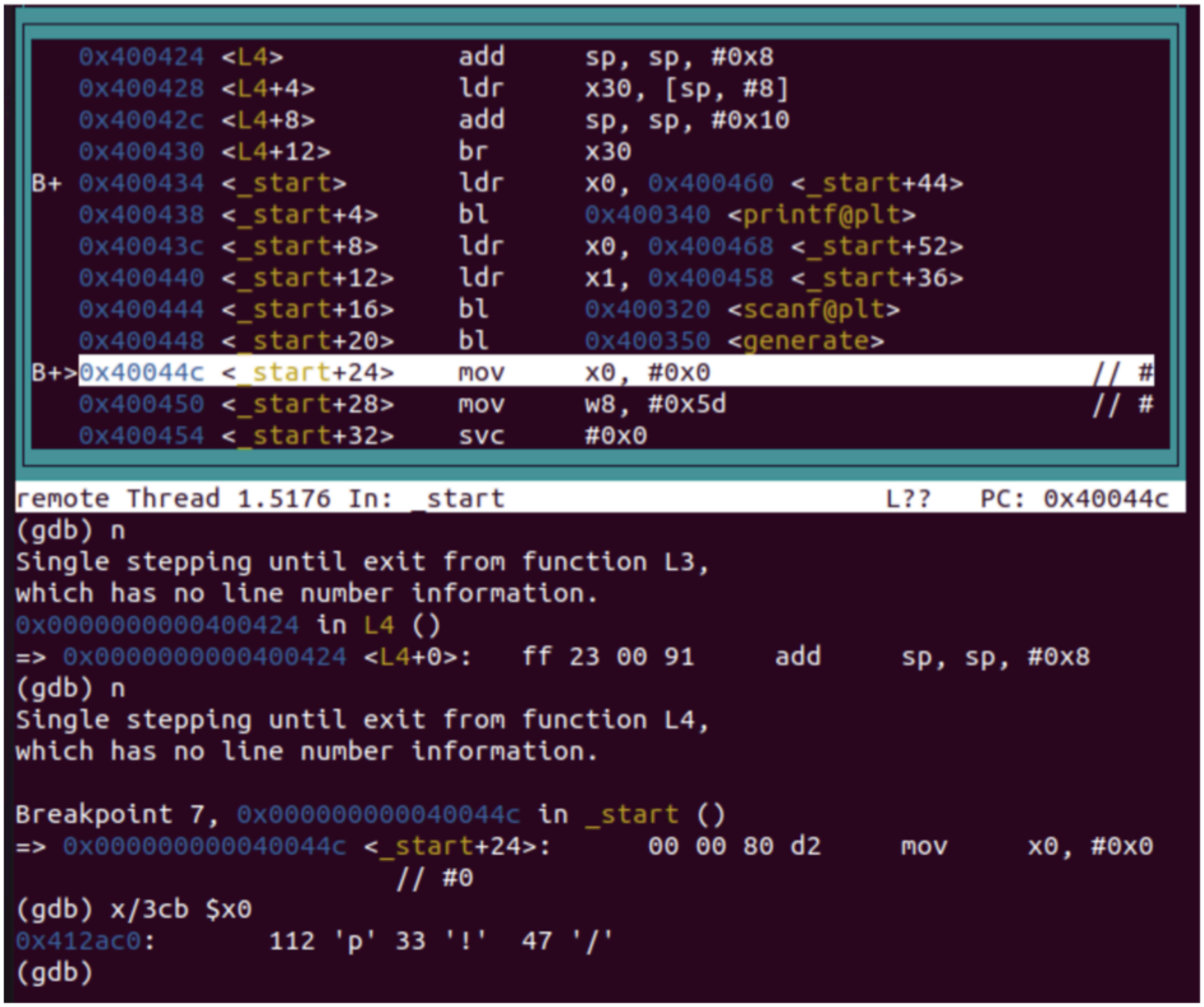
```
remote Thread 1.5176 In: TRANSFORM                    L??   PC: 0x40041c
0x0000000000400408 in TRANSFORM ()
=> 0x0000000000400408 <TRANSFORM+0>:    64 0e d6 1a     sdiv    w4, w19, w
22
(gdb) n
Single stepping until exit from function TRANSFORM,
which has no line number information.

Breakpoint 6, 0x000000000040041c in TRANSFORM ()
=> 0x000000000040041c <TRANSFORM+20>:   18 07 00 91     add     x24, x24,
#0x1
(gdb) x/1cb $x12
0x412ac0:       112 'p'
(gdb) x/3cb $x0
0x412ac0:       112 'p' 0 '\000'        0 '\000'
(gdb)
```



```
remote Thread 1.5176 In: TRANSFORM                    L??   PC: 0x40041c
0x0000000000400408 in TRANSFORM ()
=> 0x0000000000400408 <TRANSFORM+0>:    64 0e d6 1a     sdiv    w4, w19, w
22
(gdb) n
Single stepping until exit from function TRANSFORM,
which has no line number information.

Breakpoint 6, 0x000000000040041c in TRANSFORM ()
=> 0x000000000040041c <TRANSFORM+20>:   18 07 00 91     add     x24, x24,
#0x1
(gdb) x/1cb $x12
0x412ac1:       33 '!'
(gdb) x/3cb $x0
0x412ac0:       112 'p' 33 '!'  0 '\000'
(gdb)
```



```
remote Thread 1.5176 In: TRANSFORM                         L??   PC: 0x40041c
0x0000000000400408 in TRANSFORM ()
=> 0x0000000000400408 <TRANSFORM+0>:    64 0e d6 1a     sdiv    w4, w19, w
22
(gdb) n
Single stepping until exit from function TRANSFORM,
which has no line number information.

Breakpoint 6, 0x000000000040041c in TRANSFORM ()
=> 0x000000000040041c <TRANSFORM+20>:   18 07 00 91     add     x24, x24,
#0x1
(gdb) x/1cb $x12
0x412ac2:       47 '/'
(gdb) x/3cb $x0
0x412ac0:       112 'p' 33 '!'  47 '/'
(gdb) █
```



```
   0x400424 <L4>            add     sp, sp, #0x8
   0x400428 <L4+4>          ldr     x30, [sp, #8]
   0x40042c <L4+8>          add     sp, sp, #0x10
   0x400430 <L4+12>         br      x30
B+ 0x400434 <_start>        ldr     x0, 0x400460 <_start+44>
   0x400438 <_start+4>      bl      0x400340 <printf@plt>
   0x40043c <_start+8>      ldr     x0, 0x400468 <_start+52>
   0x400440 <_start+12>     ldr     x1, 0x400458 <_start+36>
   0x400444 <_start+16>     bl      0x400320 <scanf@plt>
   0x400448 <_start+20>     bl      0x400350 <generate>
B+>0x40044c <_start+24>     mov     x0, #0x0                           // #
   0x400450 <_start+28>     mov     w8, #0x5d                          // #
   0x400454 <_start+32>     svc     #0x0

remote Thread 1.5176 In: _start                            L??   PC: 0x40044c
(gdb) n
Single stepping until exit from function L3,
which has no line number information.
0x0000000000400424 in L4 ()
=> 0x0000000000400424 <L4+0>:   ff 23 00 91     add     sp, sp, #0x8
(gdb) n
Single stepping until exit from function L4,
which has no line number information.

Breakpoint 7, 0x000000000040044c in _start ()
=> 0x000000000040044c <_start+24>:      00 00 80 d2     mov     x0, #0x0
                        // #0
(gdb) x/3cb $x0
0x412ac0:       112 'p' 33 '!'  47 '/'
(gdb)
```