


```
Terminal — ssh — 80x24
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /homes/iws/rs/351_TA/linux_tut/small_programs/hi...(no debu
gging symbols found)...done.
(gdb) break main
Breakpoint 1 at 0x4004c8
(gdb) run
Starting program: /homes/iws/rs/351_TA/linux_tut/small_programs/hi

Breakpoint 1, 0x000000004004c8 in main ()
Missing separate debuginfos, use: debuginfo-install glibc-2.14-5.x86_64
(gdb) disas ←
Dump of assembler code for function main:
   0x000000004004c4 <+0>:   push   %rbp
   0x000000004004c5 <+1>:   mov    %rsp,%rbp
=> 0x000000004004c8 <+4>:   mov    $0x4005e8,%eax
   0x000000004004cd <+9>:   mov    %rax,%rdi
   0x000000004004d0 <+12>:  mov    $0x0,%eax
   0x000000004004d5 <+17>:  callq 0x4003b8 <printf@plt>
   0x000000004004da <+22>:  mov    $0x0,%eax
   0x000000004004df <+27>:  pop   %rbp
   0x000000004004e0 <+28>:  retq

End of assembler dump.
(gdb) █
```

```
Terminal — ssh — 80x24
Continuing.

Breakpoint 3, 0x000000004004cd in main ()
(gdb) disas
Dump of assembler code for function main:
   0x000000004004c4 <+0>:   push   %rbp
   0x000000004004c5 <+1>:   mov    %rsp,%rbp
   0x000000004004c8 <+4>:   mov    $0x4005e8,%eax
=> 0x000000004004cd <+9>:   mov    %rax,%rdi
   0x000000004004d0 <+12>:  mov    $0x0,%eax
   0x000000004004d5 <+17>:  callq 0x4003b8 <printf@plt>
   0x000000004004da <+22>:  mov    $0x0,%eax
   0x000000004004df <+27>:  pop   %rbp
   0x000000004004e0 <+28>:  retq

End of assembler dump.
(gdb) stepi ←
0x000000004004d0 in main ()
(gdb) p /x $eax ←
$2 = 0x4005e8
(gdb) x /s $eax
0x4005e8 <_dso_handle+8>: "hello, world!" ←
(gdb) x /s $rdi
0x4005e8 <_dso_handle+8>: "hello, world!" ←
(gdb) █
```

```
Terminal — ssh — 80x24
File Edit Options Buffers Tools C Help
#include <stdio.h>

void hello() {
    printf("hello again!\n");
}

void hello2(int target) {
    printf("hello, %d\n", target);
}

int main() {
    printf("hello, world!\n");
    hello();
    hello2(351);
    return 0;
}

-UU-:----F1 hello.c All L1 (C/l Abbrev)-----
For information about GNU Emacs and the GNU system, type C-h C-a.
```

```
Terminal — ssh — 80x24
0x000000000400555 <+29>: callq 0x400514 @hello2>
0x00000000040055a <+34>: mov $0x0,%eax
0x00000000040055f <+39>: pop %rbp
0x000000000400560 <+40>: retq
End of assembler dump.
(gdb) stepi
0x000000000400541 in main ()
(gdb) disas
Dump of assembler code for function main:
0x000000000400538 <+0>: push %rbp
0x000000000400539 <+1>: mov %rsp,%rbp
0x00000000040053c <+4>: mov $0x400680,%edi
=> 0x000000000400541 <+9>: callq 0x400400 @puts@plt>
0x000000000400546 <+14>: mov $0x0,%eax
0x00000000040054b <+19>: callq 0x400504 @hello>
0x000000000400550 <+24>: mov $0x15f,%edi
0x000000000400555 <+29>: callq 0x400514 @hello2>
0x00000000040055a <+34>: mov $0x0,%eax
0x00000000040055f <+39>: pop %rbp
0x000000000400560 <+40>: retq
End of assembler dump.
(gdb) x /s $edi
0x400680 <__dso_handle+32>: "hello, world!"
(gdb)
```

```
Terminal — ssh — 80x24
(gdb) stepi
0x00000000400541 in main ()
(gdb) disas
Dump of assembler code for function main:
   0x00000000400538 <+0>:   push   %rbp
   0x00000000400539 <+1>:   mov    %rsp,%rbp
   0x0000000040053c <+4>:   mov    $0x400680,%edi
=>  0x00000000400541 <+9>:   callq 0x400400 <puts@plt>
   0x00000000400546 <+14>:  mov    $0x0,%eax
   0x0000000040054b <+19>:  callq 0x400504 <hello>
   0x00000000400550 <+24>:  mov    $0x15f,%edi
   0x00000000400555 <+29>:  callq 0x400514 <hello2>
   0x0000000040055a <+34>:  mov    $0x0,%eax
   0x0000000040055f <+39>:  pop   %rbp
   0x00000000400560 <+40>:  retq

End of assembler dump.
(gdb) break *0x0000000040054b
Breakpoint 2 at 0x40054b
(gdb) info breakpoints
Num   Type             Disp Enb Address          What
  1    breakpoint       keep y   0x0000000040053c <main+4>
      breakpoint already hit 1 time
  2    breakpoint       keep y   0x0000000040054b <main+19>
(gdb)
```

```
Terminal — ssh — 80x24
0x00000000400504 in hello ()
(gdb) disas
Dump of assembler code for function hello:
=>  0x00000000400504 <+0>:   push   %rbp
   0x00000000400505 <+1>:   mov    %rsp,%rbp
   0x00000000400508 <+4>:   mov    $0x400668,%edi
   0x0000000040050d <+9>:   callq 0x400400 <puts@plt>
   0x00000000400512 <+14>:  pop   %rbp
   0x00000000400513 <+15>:  retq

End of assembler dump.
(gdb) stepi 2
0x00000000400508 in hello ()
(gdb) disas
Dump of assembler code for function hello:
   0x00000000400504 <+0>:   push   %rbp
   0x00000000400505 <+1>:   mov    %rsp,%rbp
=>  0x00000000400508 <+4>:   mov    $0x400668,%edi
   0x0000000040050d <+9>:   callq 0x400400 <puts@plt>
   0x00000000400512 <+14>:  pop   %rbp
   0x00000000400513 <+15>:  retq

End of assembler dump.
(gdb) x /s 0x400668
0x400668 <_dso_handle+8>:  "hello again!"
(gdb)
```

```
Terminal — ssh — 80x24
0x00000000040051f <+11>:  mov    $0x400675,%eax
0x000000000400524 <+16>:  mov    -0x4(%rbp),%edx
0x000000000400527 <+19>:  mov    %edx,%esi
0x000000000400529 <+21>:  mov    %rax,%rdi
0x00000000040052c <+24>:  mov    $0x0,%eax
=> 0x000000000400531 <+29>:  callq 0x4003f0 <printf@plt>
0x000000000400536 <+34>:  leaveq
0x000000000400537 <+35>:  retq

End of assembler dump.
(gdb) info registers
rax            0x0            0
rbx            0x0            0
rcx            0x3d9c6d30f0    264617406704
rdx            0x15f         351
rsi            0x15f         351
rdi            0x400675    4195957
rbp            0x7fffffff3e0     0x7fffffff3e0
rsp            0x7fffffff3d0     0x7fffffff3d0
r8             0x7ffff7ffc000    140737354121216
r9             0xc             12
r10            0x22             34
r11            0x246            582
r12            0x400420    4195360
r13            0x7fffffff4d0     140737488348368
```

```
Terminal — ssh — 80x24
rsi            0x15f         351
rdi            0x400675    4195957
rbp            0x7fffffff3e0     0x7fffffff3e0
rsp            0x7fffffff3d0     0x7fffffff3d0
r8             0x7ffff7ffc000    140737354121216
r9             0xc             12
r10            0x22             34
r11            0x246            582
r12            0x400420    4195360
r13            0x7fffffff4d0     140737488348368
r14            0x0             0
r15            0x0             0
rip            0x400531    0x400531  -hello2+29>
eflags        0x202         [ IF ]
cs             0x33             51
ss             0x2b             43
ds             0x0             0
es             0x0             0
fs             0x0             0
---Type <return> to continue, or q <return> to quit---
gs            0x0             0
(gdb) x /s 0x400675
0x400675 <_dso_handle+21>:  "hello, %d\n"
(gdb)
```