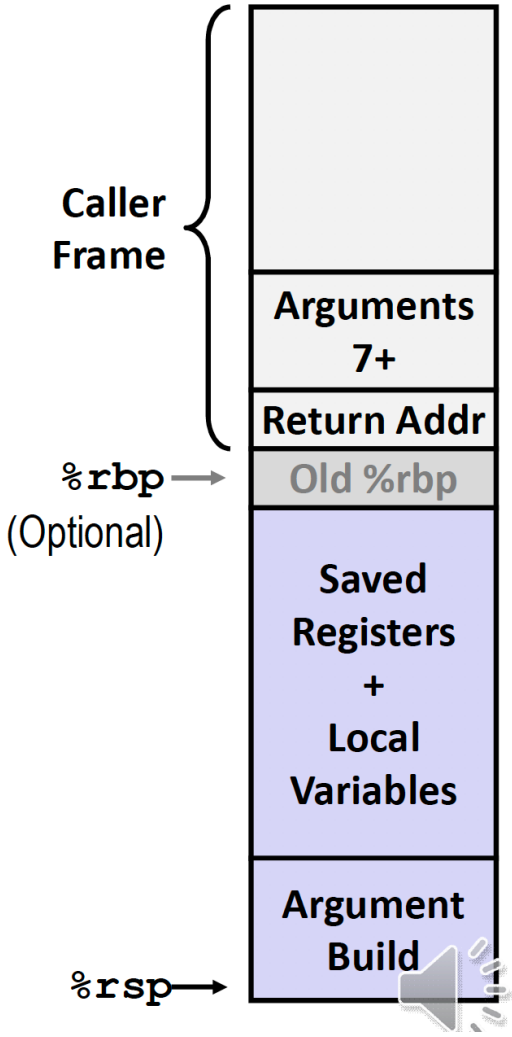
Registers

- First 6 arguments

%rdi
%rsi
%rdx
%rcx
%r8
%r9

- Return value

%rax



```c
unsigned int factorial (unsigned int x)
{
  if (x==0)
    return 0;
  else
    if (x==1)
      return 1;
    else
      return x*factorial(x-1);
}

int main( int argc, const char* argv[] )
{
  int x;
  x=atoi(argv[1]);

  printf("%d %d\n", x, factorial(x));

  return 1;

}
```

```c
unsigned int factorial (unsigned int x)
{
  if (x==0)
    return 0;
  else
    if (x==1)
      return 1;
    else
      return x*factorial(x-1);
}

int main( int argc, const char* argv[] )
{
  int x;
  x=atoi(argv[1]);

  printf("%d %d\n", x, factorial(x));

  return 1;

}
```

```
000000000040059d <main>:
  40059d:       53                      push   %rbx
  40059e:       48 8b 7e 08             mov    0x8(%rsi),%rdi
  4005a2:       ba 0a 00 00 00          mov    $0xa,%edx
  4005a7:       be 00 00 00 00          mov    $0x0,%esi
  4005ac:       e8 cf fe ff ff          callq  400480 <strtol@plt>
  4005b1:       48 89 c3                mov    %rax,%rbx
  4005b4:       89 c7                   mov    %eax,%edi
  4005b6:       e8 c2 ff ff ff          callq  40057d <factorial>
  4005bb:       89 c2                   mov    %eax,%edx
  4005bd:       89 de                   mov    %ebx,%esi
  4005bf:       bf 70 06 40 00          mov    $0x400670,%edi
  4005c4:       b8 00 00 00 00          mov    $0x0,%eax
  4005c9:       e8 82 fe ff ff          callq  400450 <printf@plt>
  4005ce:       b8 01 00 00 00          mov    $0x1,%eax
  4005d3:       5b                      pop    %rbx
  4005d4:       c3                      retq
  4005d5:       66 2e 0f 1f 84 00 00    nopw   %cs:0x0(%rax,%rax,1)
  4005dc:       00 00 00
  4005df:       90                      nop
```

```
000000000040057d <factorial>:
  40057d:       53                      push   %rbx
  40057e:       89 fb                   mov    %edi,%ebx
  400580:       b8 00 00 00 00          mov    $0x0,%eax
  400585:       85 ff                   test   %edi,%edi
  400587:       74 12                   je     40059b <factorial+0x1e>
  400589:       b0 01                   mov    $0x1,%al
  40058b:       83 ff 01                cmp    $0x1,%edi
  40058e:       74 0b                   je     40059b <factorial+0x1e>
  400590:       8d 7f ff                lea    -0x1(%rdi),%edi
  400593:       e8 e5 ff ff ff          callq  40057d <factorial>
  400598:       0f af c3                imul   %ebx,%eax
  40059b:       5b                      pop    %rbx
  40059c:       c3                      retq
```

```
(gdb) break *0x4005b6
Breakpoint 1 at 0x4005b6
(gdb) run
```

```
(gdb) i r
rax            0x4      4
rbx            0x4      4
rcx            0x0      0
rdx            0xa      10
rsi            0x0      0
rdi            0x4      4
rbp            0x0      0x0
rsp            0x7fffffffe000   0x7fffffffe000
r8             0x7ffff7dd5060   140737351864416
r9             0x7fffffffe40d   140737488348173
r10            0x4      4
r11            0x0      0
r12            0x400490 4195472
r13            0x7fffffffe0e0   140737488347360
r14            0x0      0
r15            0x0      0
rip            0x4005b6 0x4005b6 <main+25>
```

```
000000000040059d <main>:
  40059d:       53                      push   %rbx
  40059e:       48 8b 7e 08             mov    0x8(%rsi),%rdi
  4005a2:       ba 0a 00 00 00          mov    $0xa,%edx
  4005a7:       be 00 00 00 00          mov    $0x0,%esi
  4005ac:       e8 cf fe ff ff          callq  400480 <strtol@plt>
  4005b1:       48 89 c3                mov    %rax,%rbx
  4005b4:       89 c7                   mov    %eax,%edi
  4005b6:       e8 c2 ff ff ff          callq  40057d <factorial>
  4005bb:       89 c2                   mov    %eax,%edx
  4005bd:       89 de                   mov    %ebx,%esi
  4005bf:       bf 70 06 40 00          mov    $0x400670,%edi
  4005c4:       b8 00 00 00 00          mov    $0x0,%eax
  4005c9:       e8 82 fe ff ff          callq  400450 <printf@plt>
  4005ce:       b8 01 00 00 00          mov    $0x1,%eax
  4005d3:       5b                      pop    %rbx
  4005d4:       c3                      retq
  4005d5:       66 2e 0f 1f 84 00 00    nopw   %cs:0x0(%rax,%rax,1)
  4005dc:       00 00 00
  4005df:       90                      nop
```

```
(gdb) x/32bx $rsp
0x7fffffffe000: 0x00    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffe008: 0x55    0xf5    0xa2    0xf7    0xff    0x7f    0x00    0x00
0x7fffffffe010: 0x00    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffe018: 0xe8    0xe0    0xff    0xff    0xff    0x7f    0x00    0x00
```

```
(gdb) i r
rax            0x4      4
rbx            0x4      4
rcx            0x0      0
rdx            0xa      10
rsi            0x0      0
rdi            0x4      4
rbp            0x0      0x0
rsp            0x7fffffffdff8   0x7fffffffdff8
r8             0x7ffff7dd5060   140737351864416
r9             0x7fffffffe40d   140737488348173
r10            0x4      4
r11            0x0      0
r12            0x400490 4195472
r13            0x7fffffffe0e0   140737488347360
r14            0x0      0
r15            0x0      0
rip            0x40057d 0x40057d <factorial>
```

```
000000000040059d <main>:
  40059d:       53                      push   %rbx
  40059e:       48 8b 7e 08             mov    0x8(%rsi),%rdi
  4005a2:       ba 0a 00 00 00          mov    $0xa,%edx
  4005a7:       be 00 00 00 00          mov    $0x0,%esi
  4005ac:       e8 cf fe ff ff          callq  400480 <strtol@plt>
  4005b1:       48 89 c3                mov    %rax,%rbx
  4005b4:       89 c7                   mov    %eax,%edi
  4005b6:       e8 c2 ff ff ff          callq  40057d <factorial>
  4005bb:       89 c2                   mov    %eax,%edx
```

```
000000000040057d <factorial>:
  40057d:       53                      push   %rbx
  40057e:       89 fb                   mov    %edi,%ebx
  400580:       b8 00 00 00 00          mov    $0x0,%eax
  400585:       85 ff                   test   %edi,%edi
  400587:       74 12                   je     40059b <factorial+0x1e>
  400589:       b0 01                   mov    $0x1,%al
  40058b:       83 ff 01                cmp    $0x1,%edi
  40058e:       74 0b                   je     40059b <factorial+0x1e>
  400590:       8d 7f ff                lea    -0x1(%rdi),%edi
  400593:       e8 e5 ff ff ff          callq  40057d <factorial>
  400598:       0f af c3                imul   %ebx,%eax
  40059b:       5b                      pop    %rbx
  40059c:       c3                      retq
```

```
(gdb) x/32bx $rsp
0x7fffffffdff8: 0xbb    0x05    0x40    0x00    0x00    0x00    0x00    0x00
0x7fffffffe000: 0x00    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffe008: 0x55    0xf5    0xa2    0xf7    0xff    0x7f    0x00    0x00
0x7fffffffe010: 0x00    0x00    0x00    0x00    0x00    0x00    0x00    0x00
```

```
(gdb) break *0x40059b
Breakpoint 3 at 0x40059b
```

```
(gdb) c
Continuing.

Breakpoint 3, 0x000000000040059b in factorial ()
```

```
(gdb) i r
rax            0x1      1
rbx            0x1      1
rcx            0x0      0
rdx            0xa      10
rsi            0x0      0
rdi            0x1      1
rbp            0x0      0x0
rsp            0x7fffffffdfc0   0x7fffffffdfc0
r8             0x7ffff7dd5060   140737351864416
r9             0x7fffffffe40d   140737488348173
r10            0x4      4
r11            0x0      0
r12            0x400490 4195472
r13            0x7fffffffe0e0   140737488347360
r14            0x0      0
r15            0x0      0
rip            0x40059b 0x40059b <factorial+30>
```

```
000000000040059d <main>:
  40059d:       53                      push   %rbx
  40059e:       48 8b 7e 08             mov    0x8(%rsi),%rdi
  4005a2:       ba 0a 00 00 00          mov    $0xa,%edx
  4005a7:       be 00 00 00 00          mov    $0x0,%esi
  4005ac:       e8 cf fe ff ff          callq  400480 <strtol@plt>
  4005b1:       48 89 c3                mov    %rax,%rbx
  4005b4:       89 c7                   mov    %eax,%edi
  4005b6:       e8 c2 ff ff ff          callq  40057d <factorial>
  4005bb:       89 c2                   mov    %eax,%edx
```

```
000000000040057d <factorial>:
  40057d:       53                      push   %rbx
  40057e:       89 fb                   mov    %edi,%ebx
  400580:       b8 00 00 00 00          mov    $0x0,%eax
  400585:       85 ff                   test   %edi,%edi
  400587:       74 12                   je     40059b <factorial+0x1e>
  400589:       b0 01                   mov    $0x1,%al
  40058b:       83 ff 01                cmp    $0x1,%edi
  40058e:       74 0b                   je     40059b <factorial+0x1e>
  400590:       8d 7f ff                lea    -0x1(%rdi),%edi
  400593:       e8 e5 ff ff ff          callq  40057d <factorial>
  400598:       0f af c3                imul   %ebx,%eax
  40059b:       5b                      pop    %rbx
  40059c:       c3                      retq
```

```
(gdb) x/128bx $rsp
0x7fffffffdfc0: 0x02    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffdfc8: 0x98    0x05    0x40    0x00    0x00    0x00    0x00    0x00
0x7fffffffdfd0: 0x03    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffdfd8: 0x98    0x05    0x40    0x00    0x00    0x00    0x00    0x00
0x7fffffffdfe0: 0x04    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffdfe8: 0x98    0x05    0x40    0x00    0x00    0x00    0x00    0x00
0x7fffffffdff0: 0x04    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffdff8: 0xbb    0x05    0x40    0x00    0x00    0x00    0x00    0x00
```

```
(gdb) c
Continuing.

Breakpoint 3, 0x000000000040059b in factorial ()
(gdb) i r
rax            0x2      2
rbx            0x2      2
rcx            0x0      0
rdx            0xa      10
rsi            0x0      0
rdi            0x1      1
rbp            0x0      0x0
rsp            0x7fffffffdfd0   0x7fffffffdfd0
r8             0x7ffff7dd5060   140737351864416
r9             0x7fffffffe40d   140737488348173
r10            0x4      4
r11            0x0      0
r12            0x400490 4195472
r13            0x7fffffffe0e0   140737488347360
r14            0x0      0
r15            0x0      0
rip            0x40059b 0x40059b <factorial+30>
```

```
000000000040059d <main>:
  40059d:       53                      push   %rbx
  40059e:       48 8b 7e 08             mov    0x8(%rsi),%rdi
  4005a2:       ba 0a 00 00 00          mov    $0xa,%edx
  4005a7:       be 00 00 00 00          mov    $0x0,%esi
  4005ac:       e8 cf fe ff ff          callq  400480 <strtol@plt>
  4005b1:       48 89 c3                mov    %rax,%rbx
  4005b4:       89 c7                   mov    %eax,%edi
  4005b6:       e8 c2 ff ff ff          callq  40057d <factorial>
  4005bb:       89 c2                   mov    %eax,%edx
```

```
000000000040057d <factorial>:
  40057d:       53                      push   %rbx
  40057e:       89 fb                   mov    %edi,%ebx
  400580:       b8 00 00 00 00          mov    $0x0,%eax
  400585:       85 ff                   test   %edi,%edi
  400587:       74 12                   je     40059b <factorial+0x1e>
  400589:       b0 01                   mov    $0x1,%al
  40058b:       83 ff 01                cmp    $0x1,%edi
  40058e:       74 0b                   je     40059b <factorial+0x1e>
  400590:       8d 7f ff                lea    -0x1(%rdi),%edi
  400593:       e8 e5 ff ff ff          callq  40057d <factorial>
  400598:       0f af c3                imul   %ebx,%eax
  40059b:       5b                      pop    %rbx
  40059c:       c3                      retq
```

```
(gdb) x/128bx $rsp
0x7fffffffdfd0: 0x03    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffdfd8: 0x98    0x05    0x40    0x00    0x00    0x00    0x00    0x00
0x7fffffffdfe0: 0x04    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffdfe8: 0x98    0x05    0x40    0x00    0x00    0x00    0x00    0x00
0x7fffffffdff0: 0x04    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffdff8: 0xbb    0x05    0x40    0x00    0x00    0x00    0x00    0x00
```

```
(gdb) c
Continuing.

Breakpoint 3, 0x000000000040059b in factorial ()
(gdb) i r
rax            0x6      6
rbx            0x3      3
rcx            0x0      0
rdx            0xa      10
rsi            0x0      0
rdi            0x1      1
rbp            0x0      0x0
rsp            0x7fffffffdfe0   0x7fffffffdfe0
r8             0x7ffff7dd5060   140737351864416
r9             0x7fffffffe40d   140737488348173
r10            0x4      4
r11            0x0      0
r12            0x400490 4195472
r13            0x7fffffffe0e0   140737488347360
r14            0x0      0
r15            0x0      0
rip            0x40059b 0x40059b <factorial+30>
```

```
000000000040059d <main>:
  40059d:       53                      push   %rbx
  40059e:       48 8b 7e 08             mov    0x8(%rsi),%rdi
  4005a2:       ba 0a 00 00 00          mov    $0xa,%edx
  4005a7:       be 00 00 00 00          mov    $0x0,%esi
  4005ac:       e8 cf fe ff ff          callq  400480 <strtol@plt>
  4005b1:       48 89 c3                mov    %rax,%rbx
  4005b4:       89 c7                   mov    %eax,%edi
  4005b6:       e8 c2 ff ff ff          callq  40057d <factorial>
  4005bb:       89 c2                   mov    %eax,%edx
```

```
000000000040057d <factorial>:
  40057d:       53                      push   %rbx
  40057e:       89 fb                   mov    %edi,%ebx
  400580:       b8 00 00 00 00          mov    $0x0,%eax
  400585:       85 ff                   test   %edi,%edi
  400587:       74 12                   je     40059b <factorial+0x1e>
  400589:       b0 01                   mov    $0x1,%al
  40058b:       83 ff 01                cmp    $0x1,%edi
  40058e:       74 0b                   je     40059b <factorial+0x1e>
  400590:       8d 7f ff                lea    -0x1(%rdi),%edi
  400593:       e8 e5 ff ff ff          callq  40057d <factorial>
  400598:       0f af c3                imul   %ebx,%eax
  40059b:       5b                      pop    %rbx
  40059c:       c3                      retq
```

```
(gdb) x/128bx $rsp
0x7fffffffdfe0: 0x04    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffdfe8: 0x98    0x05    0x40    0x00    0x00    0x00    0x00    0x00
0x7fffffffdff0: 0x04    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffdff8: 0xbb    0x05    0x40    0x00    0x00    0x00    0x00    0x00
```

```
(gdb) c
Continuing.

Breakpoint 3, 0x000000000040059b in factorial ()
(gdb) i r
rax            0x18     24
rbx            0x4      4
rcx            0x0      0
rdx            0xa      10
rsi            0x0      0
rdi            0x1      1
rbp            0x0      0x0
rsp            0x7fffffffdff0   0x7fffffffdff0
r8             0x7ffff7dd5060   140737351864416
r9             0x7fffffffe40d   140737488348173
r10            0x4      4
r11            0x0      0
r12            0x400490 4195472
r13            0x7fffffffe0e0   140737488347360
r14            0x0      0
r15            0x0      0
rip            0x40059b 0x40059b <factorial+30>
```

```
000000000040059d <main>:
  40059d:       53                      push   %rbx
  40059e:       48 8b 7e 08             mov    0x8(%rsi),%rdi
  4005a2:       ba 0a 00 00 00          mov    $0xa,%edx
  4005a7:       be 00 00 00 00          mov    $0x0,%esi
  4005ac:       e8 cf fe ff ff          callq  400480 <strtol@plt>
  4005b1:       48 89 c3                mov    %rax,%rbx
  4005b4:       89 c7                   mov    %eax,%edi
  4005b6:       e8 c2 ff ff ff          callq  40057d <factorial>
  4005bb:       89 c2                   mov    %eax,%edx
```

```
000000000040057d <factorial>:
  40057d:       53                      push   %rbx
  40057e:       89 fb                   mov    %edi,%ebx
  400580:       b8 00 00 00 00          mov    $0x0,%eax
  400585:       85 ff                   test   %edi,%edi
  400587:       74 12                   je     40059b <factorial+0x1e>
  400589:       b0 01                   mov    $0x1,%al
  40058b:       83 ff 01                cmp    $0x1,%edi
  40058e:       74 0b                   je     40059b <factorial+0x1e>
  400590:       8d 7f ff                lea    -0x1(%rdi),%edi
  400593:       e8 e5 ff ff ff          callq  40057d <factorial>
  400598:       0f af c3                imul   %ebx,%eax
  40059b:       5b                      pop    %rbx
  40059c:       c3                      retq
```

```
(gdb) x/128bx $rsp
0x7fffffffdff0: 0x04    0x00    0x00    0x00    0x00    0x00    0x00    0x00
0x7fffffffdff8: 0xbb    0x05    0x40    0x00    0x00    0x00    0x00    0x00
```

```c
unsigned int factorial (unsigned int x)
{
  if (x==0)
    return 0;
  else
    if (x==1)
      return 1;
    else
      return x*factorial(x-1);
}

int main( int argc, const char* argv[] )
{
  int x;
  x=atoi(argv[1]);

  printf("%d %d\n", x, factorial(x));

  return 1;

}
```

```
0000000000400490 <main>:
  400490:       48 83 ec 08             sub    $0x8,%rsp
  400494:       48 8b 7e 08             mov    0x8(%rsi),%rdi
  400498:       ba 0a 00 00 00          mov    $0xa,%edx
  40049d:       31 f6                   xor    %esi,%esi
  40049f:       e8 dc ff ff ff          callq  400480 <strtol@plt>
  4004a4:       85 c0                   test   %eax,%eax
  4004a6:       74 49                   je     4004f1 <main+0x61>
  4004a8:       83 f8 01                cmp    $0x1,%eax
  4004ab:       74 4b                   je     4004f8 <main+0x68>
  4004ad:       89 c1                   mov    %eax,%ecx
  4004af:       ba 01 00 00 00          mov    $0x1,%edx
  4004b4:       eb 0f                   jmp    4004c5 <main+0x35>
  4004b6:       66 2e 0f 1f 84 00 00    nopw   %cs:0x0(%rax,%rax,1)
  4004bd:       00 00 00
  4004c0:       83 f9 01                cmp    $0x1,%ecx
  4004c3:       74 25                   je     4004ea <main+0x5a>
  4004c5:       0f af d1                imul   %ecx,%edx
  4004c8:       83 e9 01                sub    $0x1,%ecx
  4004cb:       75 f3                   jne    4004c0 <main+0x30>
  4004cd:       31 c9                   xor    %ecx,%ecx
  4004cf:       0f af d1                imul   %ecx,%edx
  4004d2:       89 c6                   mov    %eax,%esi
  4004d4:       bf b0 06 40 00          mov    $0x4006b0,%edi
  4004d9:       31 c0                   xor    %eax,%eax
  4004db:       e8 70 ff ff ff          callq  400450 <printf@plt>
  4004e0:       b8 01 00 00 00          mov    $0x1,%eax
  4004e5:       48 83 c4 08             add    $0x8,%rsp
  4004e9:       c3                      retq
  4004ea:       b9 01 00 00 00          mov    $0x1,%ecx
  4004ef:       eb de                   jmp    4004cf <main+0x3f>
  4004f1:       ba 01 00 00 00          mov    $0x1,%edx
  4004f6:       eb d5                   jmp    4004cd <main+0x3d>
  4004f8:       ba 01 00 00 00          mov    $0x1,%edx
  4004fd:       b9 01 00 00 00          mov    $0x1,%ecx
  400502:       eb cb                   jmp    4004cf <main+0x3f>
```