CS107, Lecture 14
Assembly: The Runtime Stack

Reading: B&O 3.7

Learning Goals

- Learn what %rip represents and how it is updated.
- Learn how assembly calls functions and manages stack frames.
- Learn the rules of register use when calling functions.

Plan For Today

- The Instruction Pointer (%rip)
- Calling Functions
  - The Stack
  - Passing Control
  - Passing Data
  - Local Storage
- **Break:** Announcements
- Register Restrictions
- Pulling it all together: recursion example

Plan For Today

- The Instruction Pointer (%rip)
- Calling Functions
  - The Stack
  - Passing Control
  - Passing Data
  - Local Storage
- **Break:** Announcements
- Register Restrictions
- Pulling it all together: recursion example

%rip

- **%rip** is a special register that points to the instruction currently executing.
- **Let's dive deeper into how %rip works, and how jumps modify it**.

%rip

```
00000000004004ed <loop>:
4004ed: 55                      push
4004ee: 48 89 e5                mov
4004f1: c7 45 fc 00 00 00 00    movl
4004f8: 83 45 fc 01             addl
4004fc: eb fa                   jmp
```

%rip

```
00000000004004ed <loop>:
4004ed: 55                      push
4004ee: 48 89 e5                mov
4004f1: c7 45 fc 00 00 00 00    movl
4004f8: 83 45 fc 01             addl
4004fc: eb fa                   jmp
```

%rip

```
0000000004004ed <loop>:
4004ed: 55                          push
4004ee: 48 89 e5                    mov
4004f1: c7 45 fc 00 00 00 00        movl
4004f8: 83 45 fc 01                 addl
4004fc: eb fa                       jmp
```

%rip

```
00000000004004ed <loop>:
4004ed: 55                      push
4004ee: 48 89 e5                mov
4004f1: c7 45 fc 00 00 00 00    movl
4004f8: 83 45 fc 01             addl
4004fc: eb fa                   jmp
```

%rip

```
00000000004004ed <loop>:
4004ed: 55                            push
4004ee: 48 89 e5                      mov
4004f1: c7 45 fc 00 00 00 00          movl
4004f8: 83 45 fc 01                   addl
4004fc: eb fa                         jmp
```

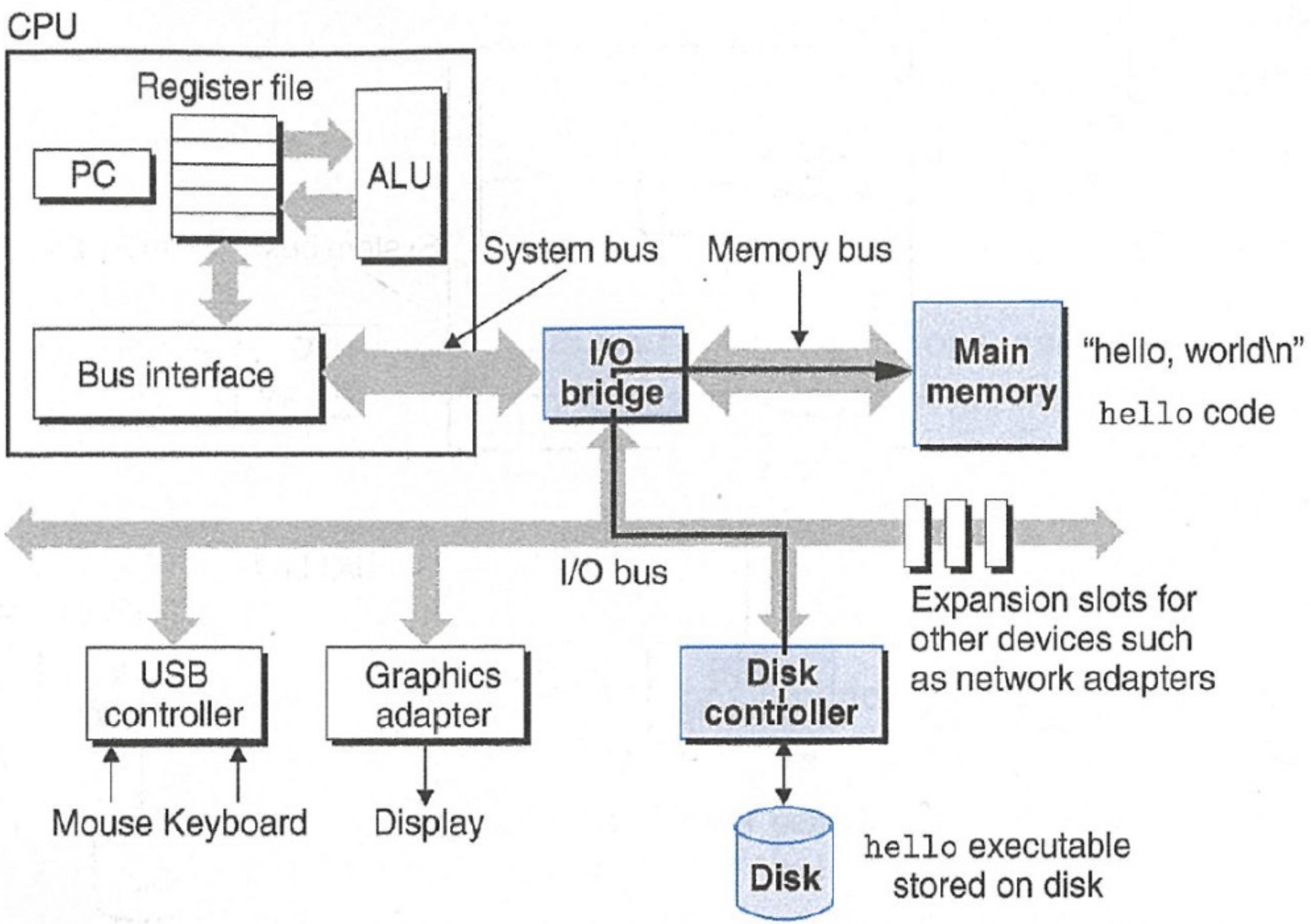
%rip

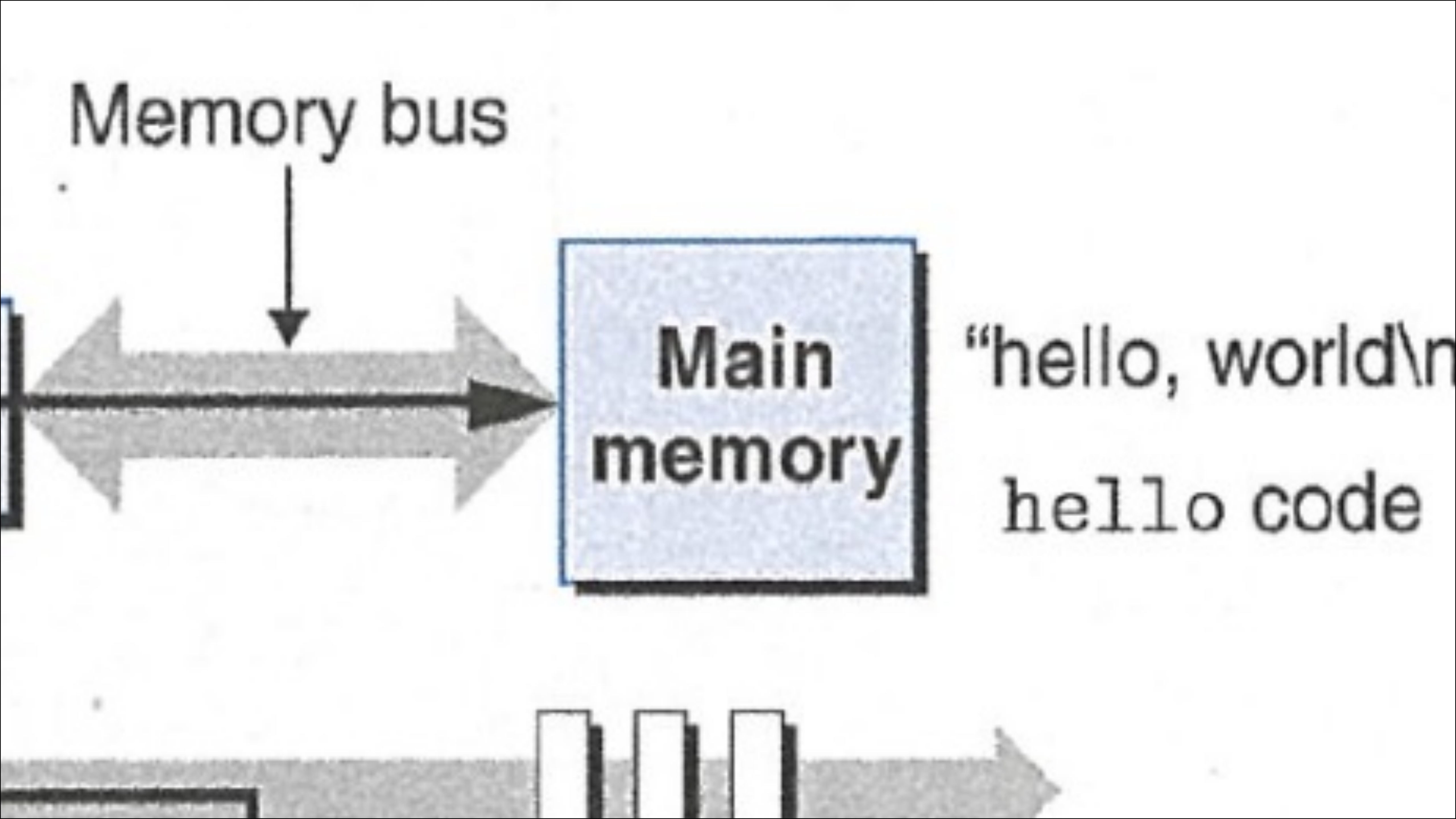
```
00000000004004ed <loop>:
4004ed: 55                               push
4004ee: 48 89 e5                         mov
4004f1: c7 45 fc 00 00 00 00             movl
4004f8: 83 45 fc 01                      addl
4004fc: eb fa                            jmp
```

%rip

```
00000000004004ed <loop>:
4004ed: 55                              push
4004ee: 48 89 e5                        mov
4004f1: c7 45 fc 00 00 00 00            movl
4004f8: 83 45 fc 01                     addl
4004fc: eb fa                           jmp
```

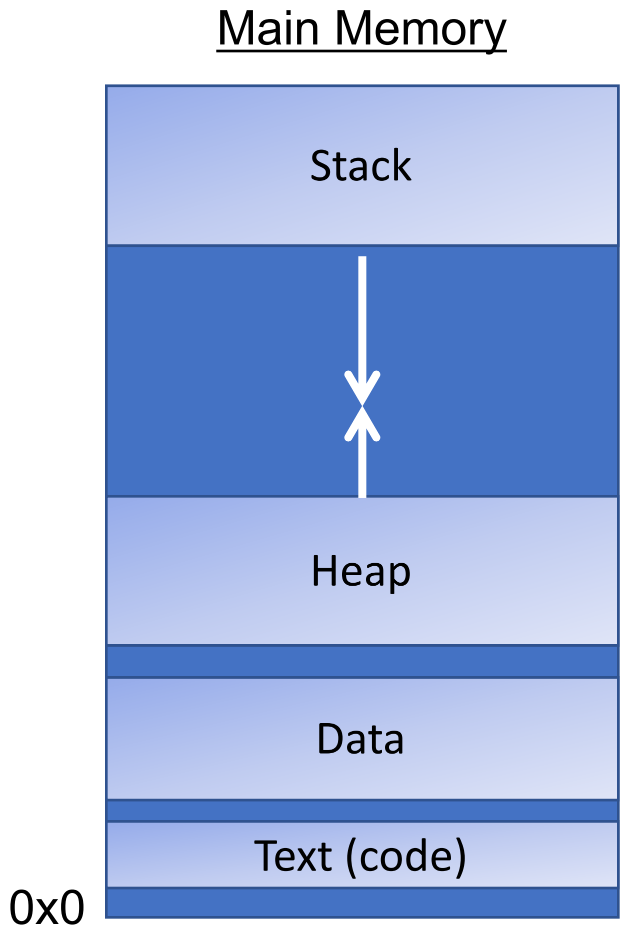
Instructions Are Just Bytes!



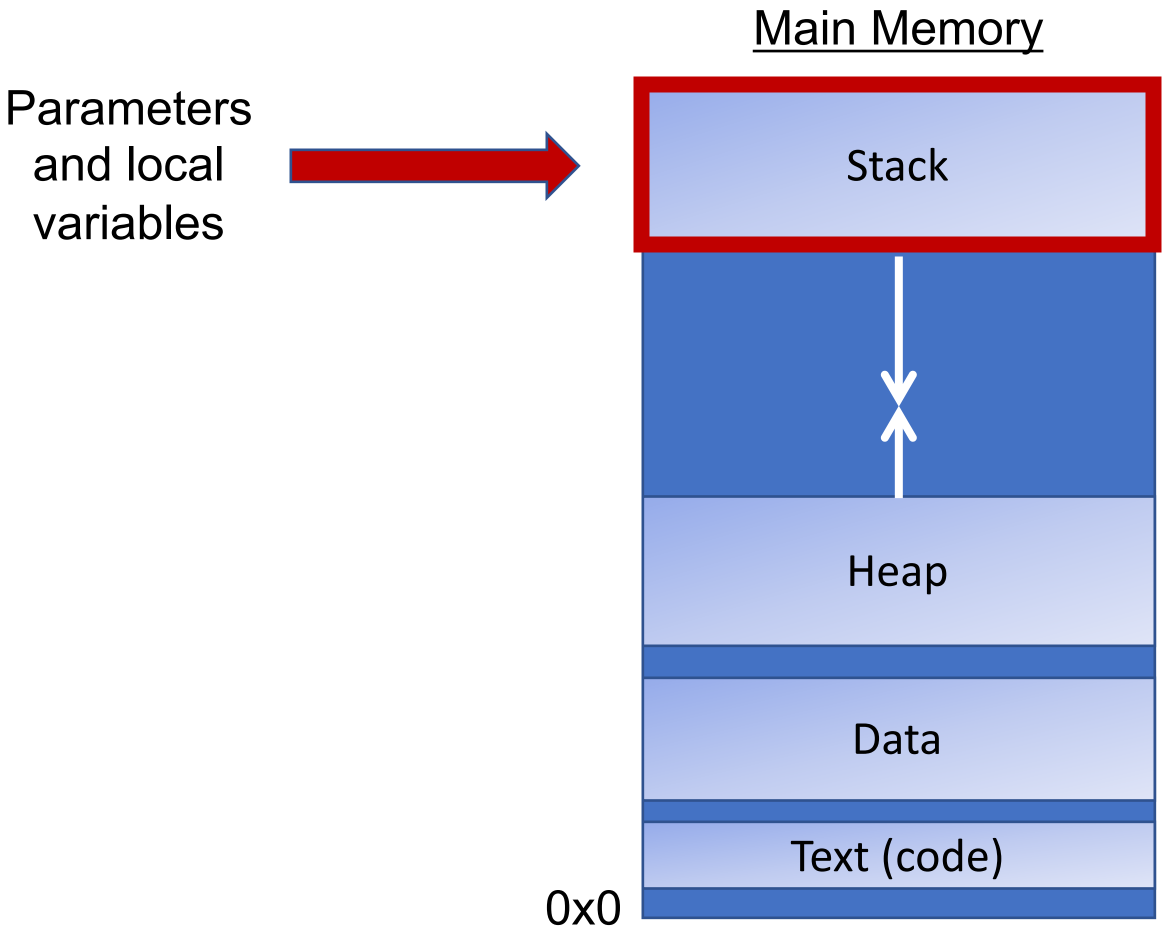


Memory bus
Main memory
"hello, world\n
hello code

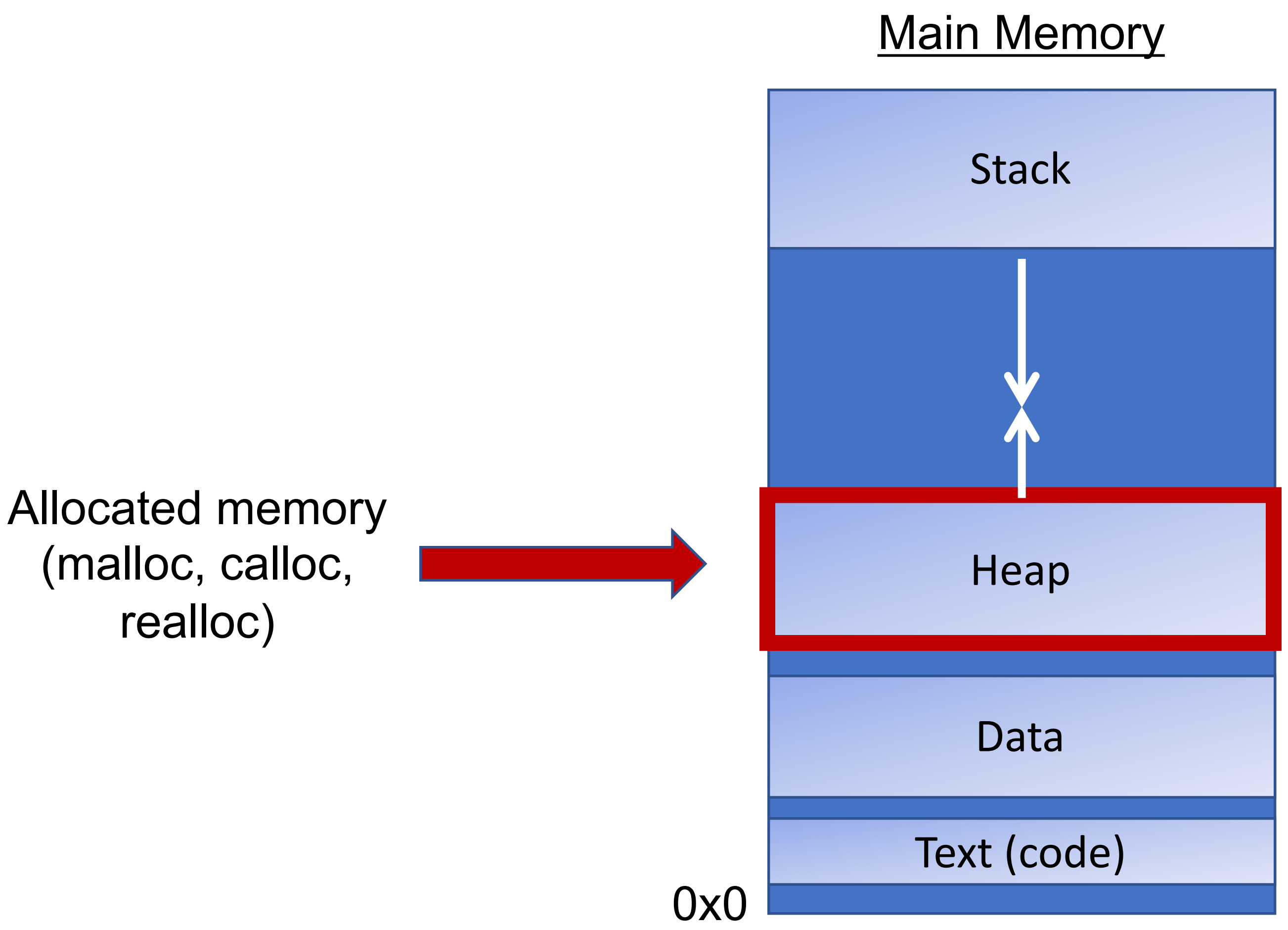
Instructions Are Just Bytes!



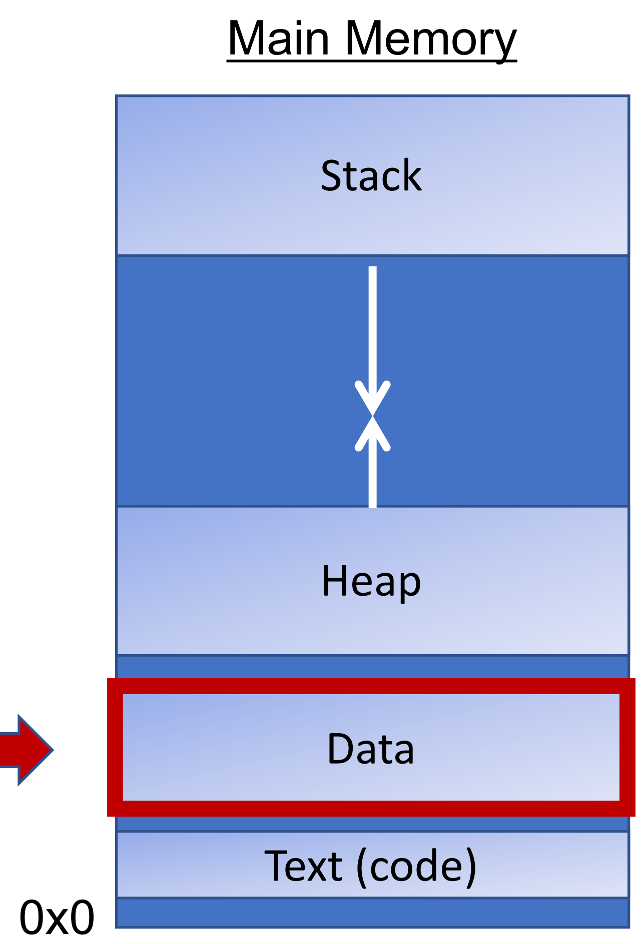
Instructions Are Just Bytes!



Instructions Are Just Bytes!

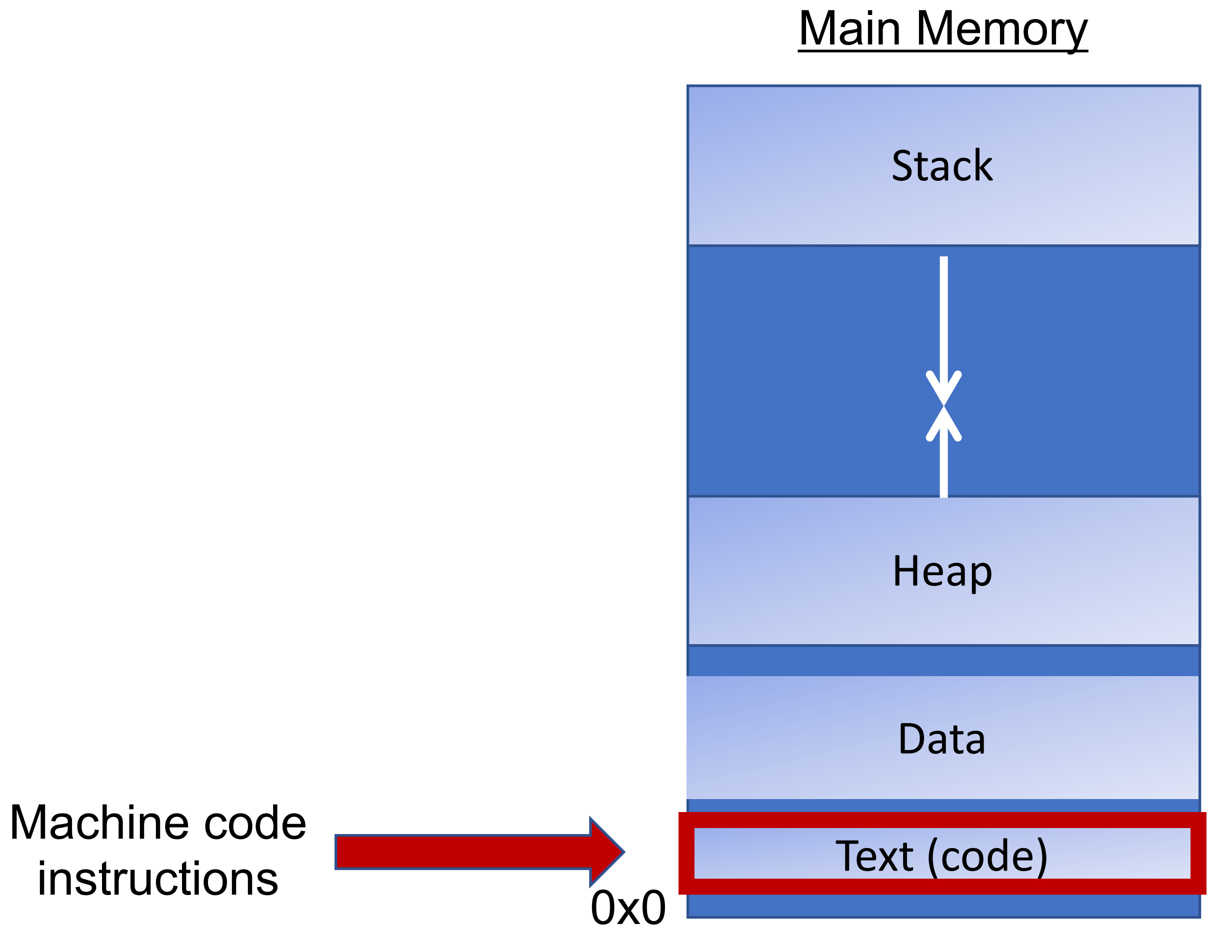


Instructions Are Just Bytes!



Global variables (boo!), static variables and string literals

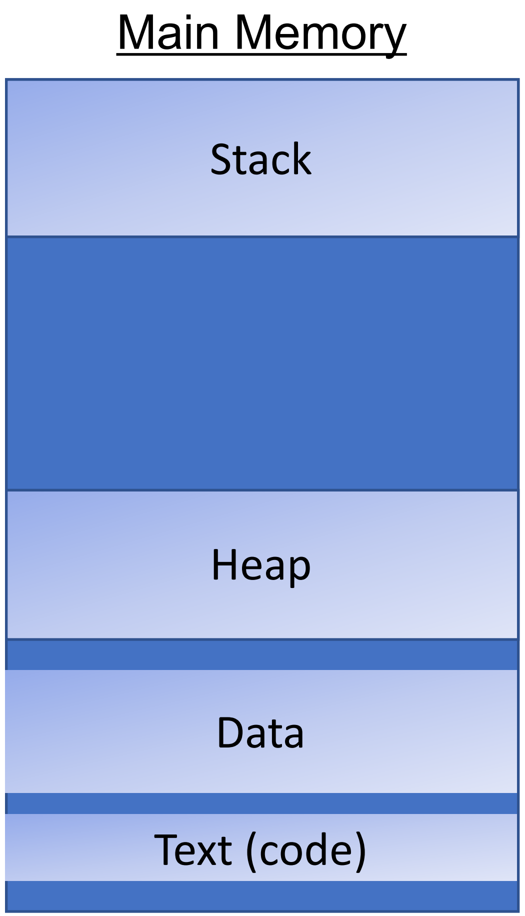
Instructions Are Just Bytes!



%ri

```
00000000004004ed <loop>:
4004ed: 55                      push
4004ee: 48 89 e5                mov
4004f1: c7 45 fc 00 00 00 00    movl
4004f8: 83 45 fc 01             addl
4004fc: eb fa                   jmp
```

4004fd	fa
4004fc	eb
4004fb	01
4004fa	fc
4004f9	45
4004f8	83
4004f7	00
4004f6	00
4004f5	00
4004f4	00
4004f3	fc
4004f2	45
4004f1	c7
4004f0	e5
4004ef	89
4004ee	48
4004ed	55



%rip

```
00000000004004ed <loop>:
4004ed: 55                       push
4004ee: 48 89 e5                 mov
4004f1: c7 45 fc 00 00 00 00     movl
4004f8: 83 45 fc 01              addl
4004fc: eb fa                    jmp
```

4004fd	fa
4004fc	eb
4004fb	01
4004fa	fc
4004f9	45
4004f8	83
4004f7	00
4004f6	00
4004f5	00
4004f4	00
4004f3	fc
4004f2	45
4004f1	c7
4004f0	e5
4004ef	89
4004ee	48
4004ed	55

%rip

```
00000000004004ed <loop>:
4004ed: 55                      push
4004ee: 48 89 e5                mov
4004f1: c7 45 fc 00 00 00 00    movl
4004f8: 83 45 fc 01             addl
4004fc: eb fa                   jmp
```

0x4004ed

%rip

4004fd	fa
4004fc	eb
4004fb	01
4004fa	fc
4004f9	45
4004f8	83
4004f7	00
4004f6	00
4004f5	00
4004f4	00
4004f3	fc
4004f2	45
4004f1	c7
4004f0	e5
4004ef	89
4004ee	48
4004ed	55

%rip

```
00000000004004ed <loop>:
4004ed: 55                           push
4004ee: 48 89 e5                     mov
4004f1: c7 45 fc 00 00 00 00         movl
4004f8: 83 45 fc 01                  addl
4004fc: eb fa                        jmp
```

4004fd	fa
4004fc	eb
4004fb	01
4004fa	fc
4004f9	45
4004f8	83
4004f7	00
4004f6	00
4004f5	00
4004f4	00
4004f3	fc
4004f2	45
4004f1	c7
4004f0	e5
4004ef	89
4004ee	48
4004ed	55

0x4004ee

%rip

%rip

```
00000000004004ed <loop>:
4004ed: 55                        push
4004ee: 48 89 e5                  mov
4004f1: c7 45 fc 00 00 00 00      movl
4004f8: 83 45 fc 01               addl
4004fc: eb fa                     jmp
```

4004fd	fa
4004fc	eb
4004fb	01
4004fa	fc
4004f9	45
4004f8	83
4004f7	00
4004f6	00
4004f5	00
4004f4	00
4004f3	fc
4004f2	45
4004f1	c7
4004f0	e5
4004ef	89
4004ee	48
4004ed	55

0x4004f1

%rip

%rip

```
00000000004004ed <loop>:
4004ed: 55                          push
4004ee: 48 89 e5                    mov
4004f1: c7 45 fc 00 00 00 00        movl
4004f8: 83 45 fc 01                 addl
4004fc: eb fa                       jmp
```

4004fd	fa
4004fc	eb
4004fb	01
4004fa	fc
4004f9	45
4004f8	83
4004f7	00
4004f6	00
4004f5	00
4004f4	00
4004f3	fc
4004f2	45
4004f1	c7
4004f0	e5
4004ef	89
4004ee	48
4004ed	55

0x4004f8

%rip

%rip

```
00000000004004ed <loop>:
4004ed: 55                    push
4004ee: 48 89 e5              mov
4004f1: c7 45 fc 00 00 00 00  movl
4004f8: 83 45 fc 01           addl
4004fc: eb fa                 jmp
```

0x4004fc

%rip

4004fd	fa
4004fc	eb
4004fb	01
4004fa	fc
4004f9	45
4004f8	83
4004f7	00
4004f6	00
4004f5	00
4004f4	00
4004f3	fc
4004f2	45
4004f1	c7
4004f0	e5
4004ef	89
4004ee	48
4004ed	55

%rip

```
00000000004004ed <loop>:
4004ed: 55                         push
400                                   v
400                                   vl
400                                   dl
400                                   p
```

Special hardware is responsible for setting %rip's value to the next instruction.

› it does %rip += size of current instruction (in bytes)

4004fd	fa
4004fc	eb
4004fb	01
4004fa	fc
4004f9	45
4004f8	83
4004f7	00
4004f6	00
4004f5	00
4004f4	00
4004f3	fc
4004f2	45
4004f1	c7
4004f0	e5
4004ef	89
4004ee	48
4004ed	55

0x4004fc

%rip

%rip

```
void loop() {
    int i = 0;
    while (i < 100) {
        i++;
    }
}
```

```
0x400570 <+0>:  b8 00 00 00 00 mov $0x0,%eax
0x400575 <+5>:  eb 03          jmp 0x40057a <loop+10>
0x400577 <+7>:  83 c0 01       add $0x1,%eax
0x40057a <+10>: 83 f8 63       cmp $0x63,%eax
0x40057d <+13>: 73 f8          jle 0x400577 <loop+7>
0x40057f <+15>: f3 c3          repz retq
```

%rip

```
void loop() {
    int i = 0;
    while (i < 100) {
        i++;
    }
}
```

```
0x400570 <+0>:  b8 00 00 00 00 mov $0x0,%eax
0x400575 <+5>:  eb 03          jmp 0x40057a <loop+10>
0x400577 <+7>:  83 c0 01       add $0x1,%eax
0x40057a <+10>: 83 f8 63       cmp $0x63,%eax
0x40057d <+13>: 73 f8          jle 0x400577 <loop+7>
0x40057f <+15>: f3 c3          repz retq
```

These are 0-based offsets in bytes for each instruction relative to the start of this function.

%rip

```
void loop() {
    int i = 0;
    while (i < 100) {
        i++;
    }
}
```

```
0x400570 <+0>:  b8 00 00 00 00 mov $0x0,%eax
0x400575 <+5>:  eb 03          jmp 0x40057a <loop+10>
0x400577 <+7>:  83 c0 01       add $0x1,%eax
0x40057a <+10>: 83 f8 63       cmp $0x63,%eax
0x40057d <+13>: 73 f8          jle 0x400577 <loop+7>
0x40057f <+15>: f3 c3          repz retq
```

These are bytes for the machine code instructions. Instructions are variable length.

%rip

```c
void loop() {
    int i = 0;
    while (i < 100) {
        i++;
    }
}
```

```
0x400570 <+0>:  b8 00 00 00 00 mov $0x0,%eax
0x400575 <+5>:  eb 03          jmp 0x40057a <loop+10>
0x400577 <+7>:  83 c0 01       add $0x1,%eax
0x40057a <+10>: 83 f8 63       cmp $0x63,%eax
0x40057d <+13>: 73 f8          jle 0x400577 <loop+7>
0x40057f <+15>: f3 c3          repz retq
```

%rip

```
0x400570 <+0>:   b8 00 00 00 00 mov $0x0,%eax
0x400575 <+5>:   eb 03          jmp 0x40057a <loop+10>
0x400577 <+7>:   83 c0 01       add $0x1,%eax
0x40057a <+10>: 83 f8 63       cmp $0x63,%eax
0x40057d <+13>: 73 f8          jle 0x400577 <loop+7>
0x40057f <+15>: f3 c3          repz retq
```

%rip

```
0x400570 <+0>:   b8 00 00 00 00 mov $0x0,%eax
0x400575 <+5>:   eb 03          jmp 0x40057a <loop+10>
0x400577 <+7>:   83 c0 01       add $0x1,%eax
0x40057a <+10>:  83 f8 63       cmp $0x63,%eax
0x40057d <+13>:  73 f8          jle 0x400577 <loop+7>
0x40057f <+15>:  f3 c3          repz retq
```

0xeb means **jmp**.

%rip

```
0x400570 <+0>:   b8 00 00 00 00 mov $0x0,%eax
0x400575 <+5>:   eb 03          jmp 0x40057a <loop+10>
0x400577 <+7>:   83 c0 01       add $0x1,%eax
0x40057a <+10>:  83 f8 63       cmp $0x63,%eax
0x40057d <+13>:  73 f8          jle 0x400577 <loop+7>
0x40057f <+15>:  f3 c3          repz retq
```

0x03 is the number of instruction bytes to jump relative to %rip.

With no jump, %rip would advance to the next line. This **jmp** says to then go **3** bytes further!

%rip

```
0x400570 <+0>:   b8 00 00 00 00 mov $0x0,%eax
0x400575 <+5>:   eb 03          jmp 0x40057a <loop+10>
0x400577 <+7>:   83 c0 01       add $0x1,%eax
0x40057a <+10>:  83 f8 63       cmp $0x63,%eax
0x40057d <+13>:  73 f8          jle 0x400577 <loop+7>
0x40057f <+15>:  f3 c3          repz retq
```

0x03 is the number of instruction bytes to jump relative to %rip.

With no jump, %rip would advance to the next line. This **jmp** says to then go **3** bytes further!

%rip

```
0x400570 <+0>:  b8 00 00 00 00 mov $0x0,%eax
0x400575 <+5>:  eb 03          jmp 0x40057a <loop+10>
0x400577 <+7>:  83 c0 01       add $0x1,%eax
0x40057a <+10>: 83 f8 63       cmp $0x63,%eax
0x40057d <+13>: 73 f8          jle 0x400577 <loop+7>
0x40057f <+15>: f3 c3          repz retq
```

0x73 means **jle**.

%rip

```
0x400570 <+0>:  b8 00 00 00 00 mov $0x0,%eax
0x400575 <+5>:  eb 03          jmp 0x40057a <loop+10>
0x400577 <+7>:  83 c0 01       add $0x1,%eax
0x40057a <+10>: 83 f8 63       cmp $0x63,%eax
0x40057d <+13>: 73 f8          jle 0x400577 <loop+7>
0x40057f <+15>: f3 c3          repz retq
```

0xf8 is the number of instruction bytes to jump relative to %rip. This is -8 (in two's complement!).

With no jump, %rip would advance to the next line. This **jmp** says to then go **8** bytes back!

%rip

```
0x400570 <+0>:   b8 00 00 00 00 mov $0x0,%eax
0x400575 <+5>:   eb 03          jmp 0x40057a <loop+10>
0x400577 <+7>:   83 c0 01       add $0x1,%eax
0x40057a <+10>:  83 f8 63       cmp $0x63,%eax
0x40057d <+13>:  73 f8          jle 0x400577 <loop+7>
0x40057f <+15>:  f3 c3          repz retq
```

0xf8 is the number of instruction bytes to jump relative to %rip. This is -8 (in two's complement!).

With no jump, %rip would advance to the next line. This **jmp** says to then go **8** bytes back!

Summary: Instruction Pointer

- Machine code instructions live in main memory, just like stack and heap data.
- %rip is a register that stores a number (an address) of the currently executing instruction. It marks where we currently are in the program's instructions.
- To advance to the next instruction, special hardware adds the size of the current instruction in bytes.
- **jmp** instructions work by adjusting %rip by a specified amount.

Plan For Today

- The Instruction Pointer (%rip)
- Calling Functions
  - The Stack
  - Passing Control
  - Passing Data
  - Local Storage
- **Break:** Announcements
- Register Restrictions
- Pulling it all together: recursion example

How do we call functions in assembly?

Calling Functions In Assembly

To call a function in assembly, we must do a few things:

- **Pass Control** – %rip must be adjusted to execute the callee's instructions, and then resume the caller's instructions afterwards.
- **Pass Data** – we must pass any parameters and receive any return value.
- **Manage Memory** – we must handle any space needs of the callee on the stack.

How does assembly interact with the stack?

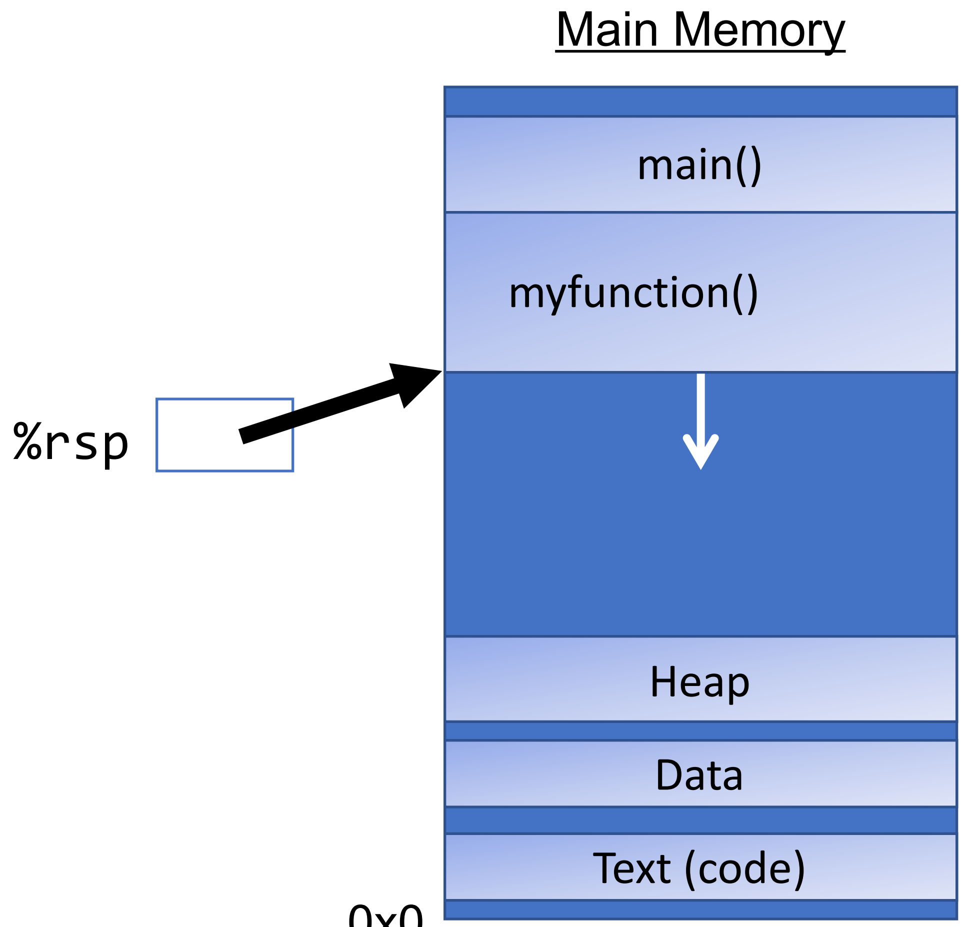
Terminology: **caller** function calls the **callee** function.

Plan For Today

- The Instruction Pointer (%rip)
- Calling Functions
  - The Stack
  - Passing Control
  - Passing Data
  - Local Storage
- **Break:** Announcements
- Register Restrictions
- Pulling it all together: recursion example

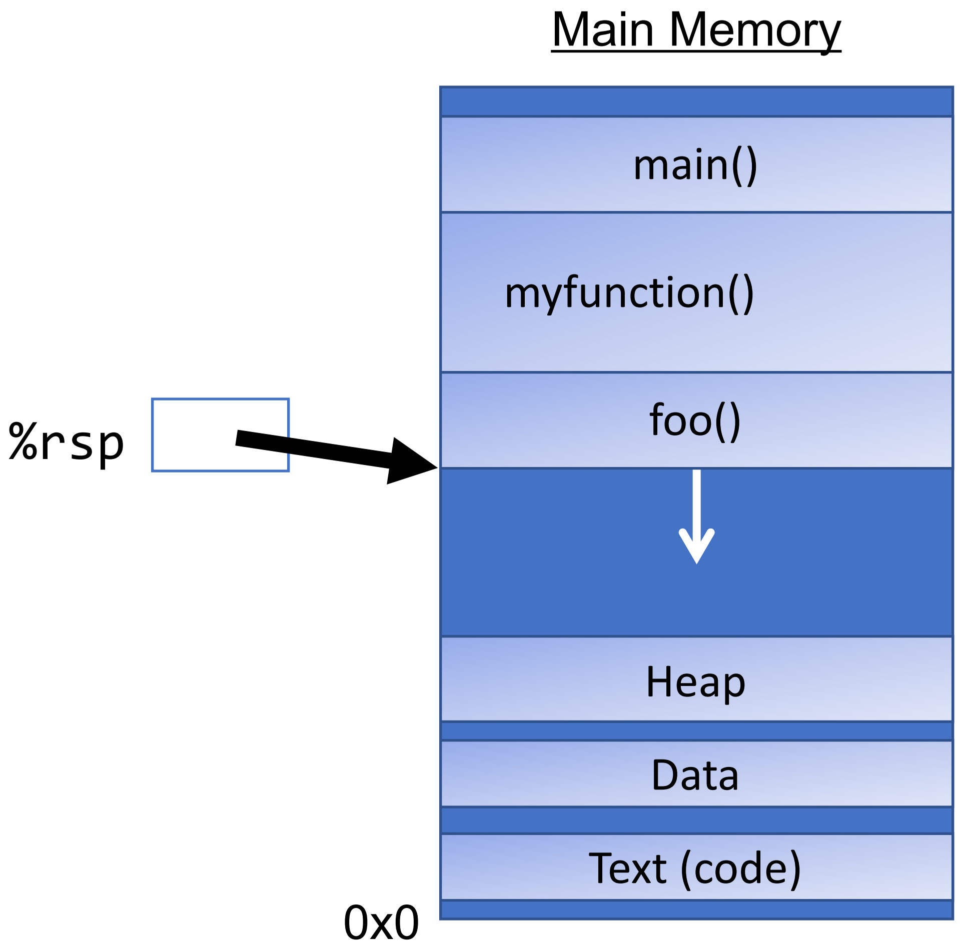
%rip

- **%rsp** is a special register that stores the address of the current "top" of the stack (the bottom in our diagrams, since the stack grows downwards).



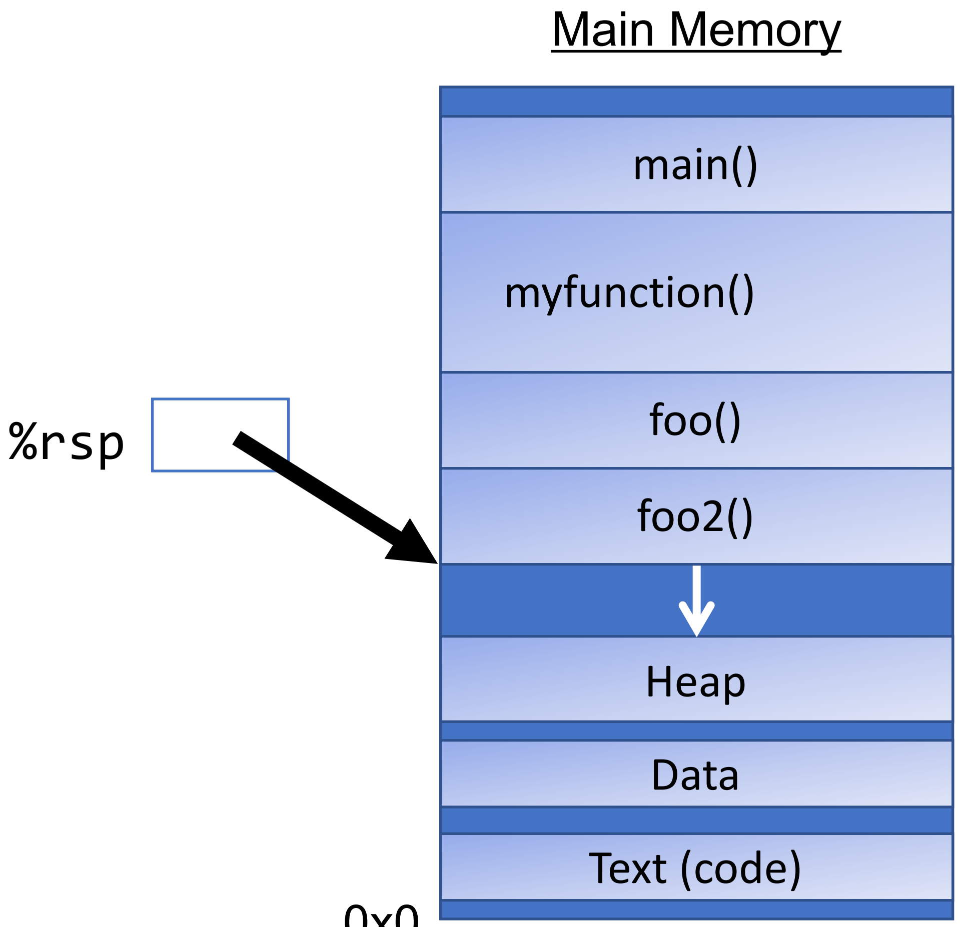
%rip

- **%rsp** is a special register that stores the address of the current "top" of the stack (the bottom in our diagrams, since the stack grows downwards).



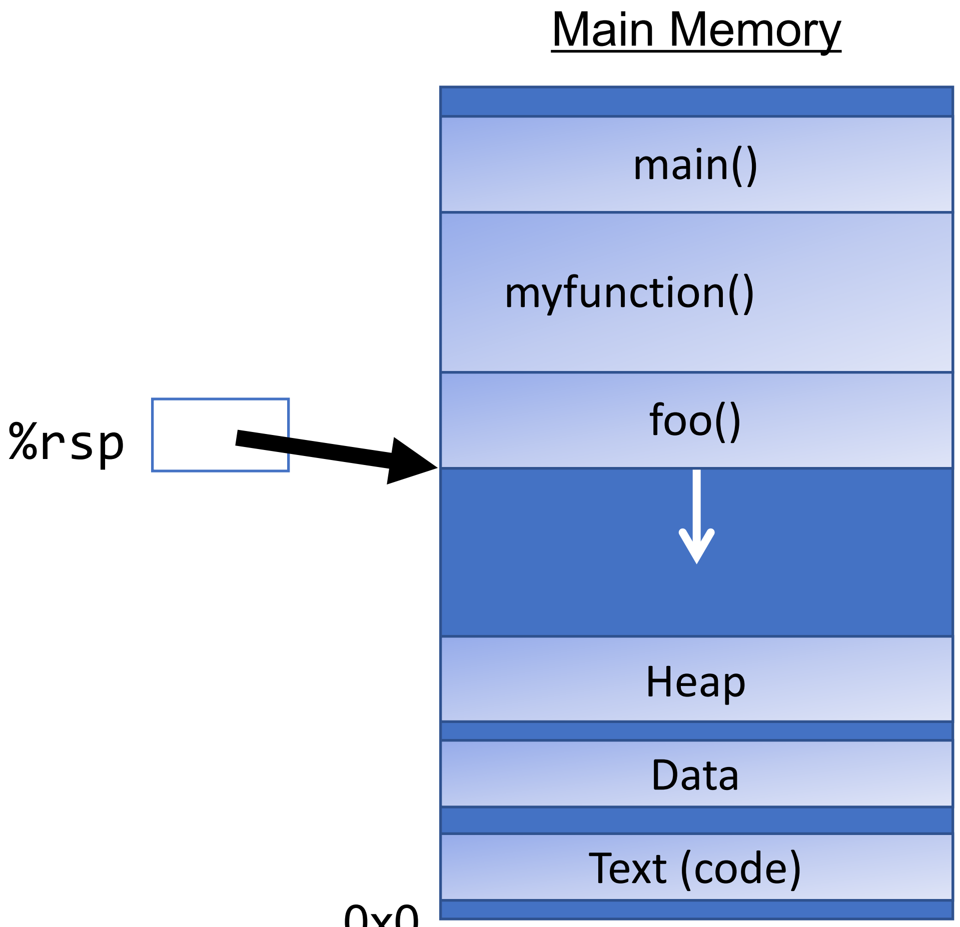
%rip

- **%rsp** is a special register that stores the address of the current "top" of the stack (the bottom in our diagrams, since the stack grows downwards).



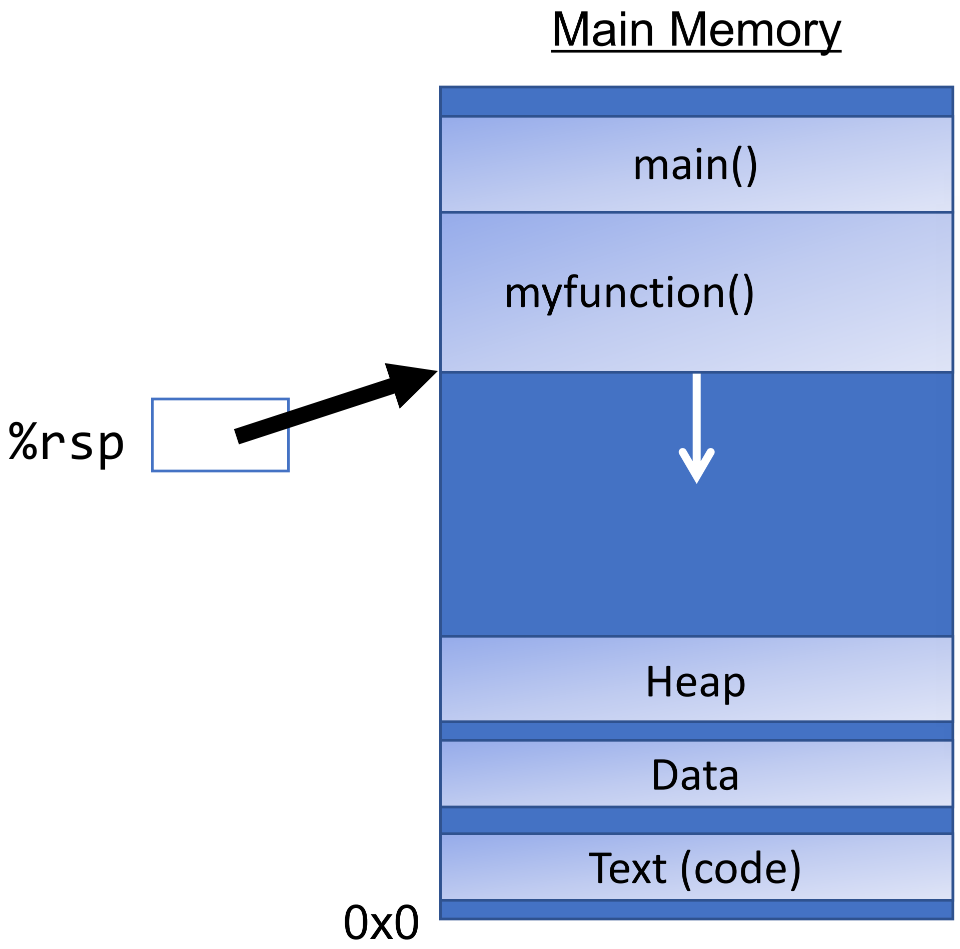
%rip

- **%rsp** is a special register that stores the address of the current "top" of the stack (the bottom in our diagrams, since the stack grows downwards).



%rip

- **%rsp** is a special register that stores the address of the current "top" of the stack (the bottom in our diagrams, since the stack grows downwards).



Key idea: %rsp must point to the same place before and after a function is called, since stack frames go away when a function finishes.

push

- The **push** instruction pushes the data at the specified source onto the top of the stack, adjusting **%rsp** accordingly.

Instruction	Effect
`pushq S`	`R[%rsp] ⟵ R[%rsp] - 8;` `M[R[%rsp]] ⟵ S`

push

- The **push** instruction pushes the data at the specified source onto the top of the stack, adjusting **%rsp** accordingly.

Instruction	Effect
`pushq S`	`R[%rsp] ⟵ R[%rsp] - 8;` `M[R[%rsp]] ⟵ S`

push

- The **push** instruction pushes the data at the specified source onto the top of the stack, adjusting **%rsp** accordingly.

Instruction	Effect
`pushq S`	`R[%rsp] ⟵ R[%rsp] - 8;` `M[R[%rsp]] ⟵ S`

push

- The **push** instruction pushes the data at the specified source onto the top of the stack, adjusting **%rsp** accordingly.

Instruction	Effect
`pushq S`	`R[%rsp] ⟵ R[%rsp] - 8;` `M[R[%rsp]] ⟵ S`

- This behavior is equivalent to the following, but pushq is a shorter instruction:

```
subq $8, %rsp
movq  S, (%rsp)
```

- Sometimes, you'll see instructions just explicitly decrement the stack pointer to make room for future data.

pop

- The **pop** instruction pops the topmost data from the stack and stores it in the specified destination, adjusting **%rsp** accordingly.

Instruction	Effect
`popq D`	`D ⟵ M[R[%rsp]]` `R[%rsp] ⟵ R[%rsp] + 8;`

- **Note**: this *does not* remove/clear out the data! It just increments %rsp to indicate the next push can overwrite that location.

pop

- The **pop** instruction pops the topmost data from the stack and stores it in the specified destination, adjusting **%rsp** accordingly.

Instruction	Effect
`popq D`	`D ⟵ M[R[%rsp]]` `R[%rsp] ⟵ R[%rsp] + 8;`

- This behavior is equivalent to the following, but popq is a shorter instruction:

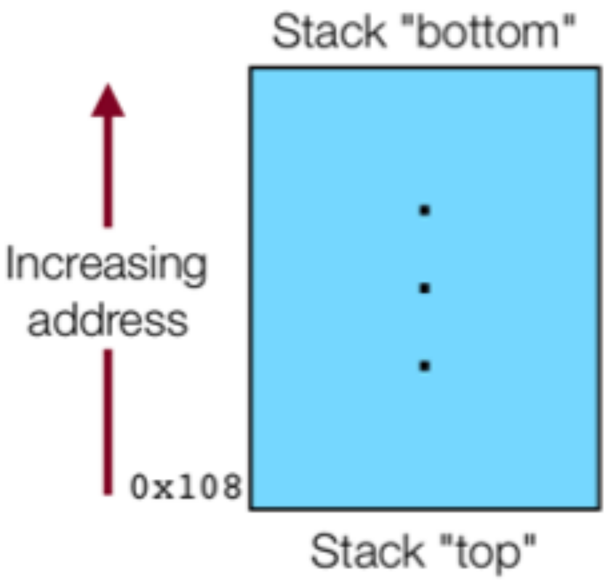
```
movq (%rsp), D
addq $8, %rsp
```

- Sometimes, you'll see instructions just explicitly increment the stack pointer to pop data.

Pushing onto the Stack

- Example:

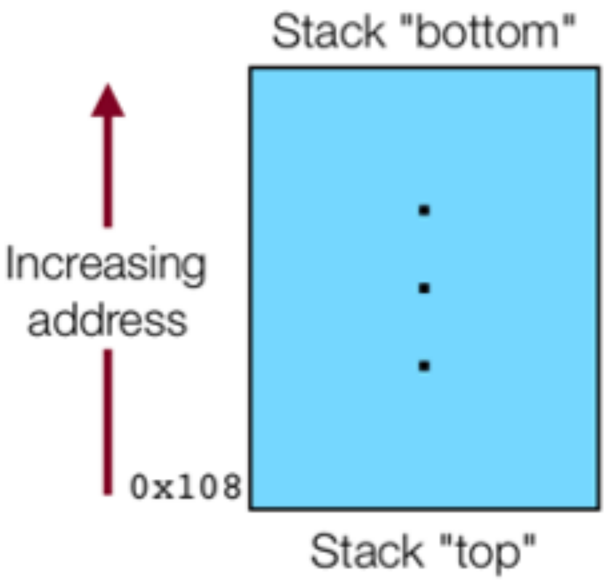
Initially	
%rax	0x123
%rdx	0
%rsp	0x108



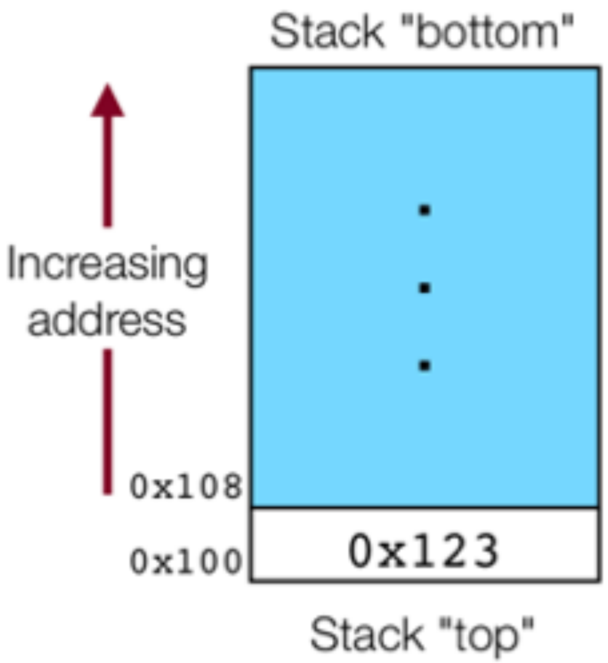
Pushing onto the Stack

- Example:

Initially	
%rax	0x123
%rdx	0
%rsp	0x108



pushq %rax	
%rax	0x123
%rdx	0
%rsp	0x100



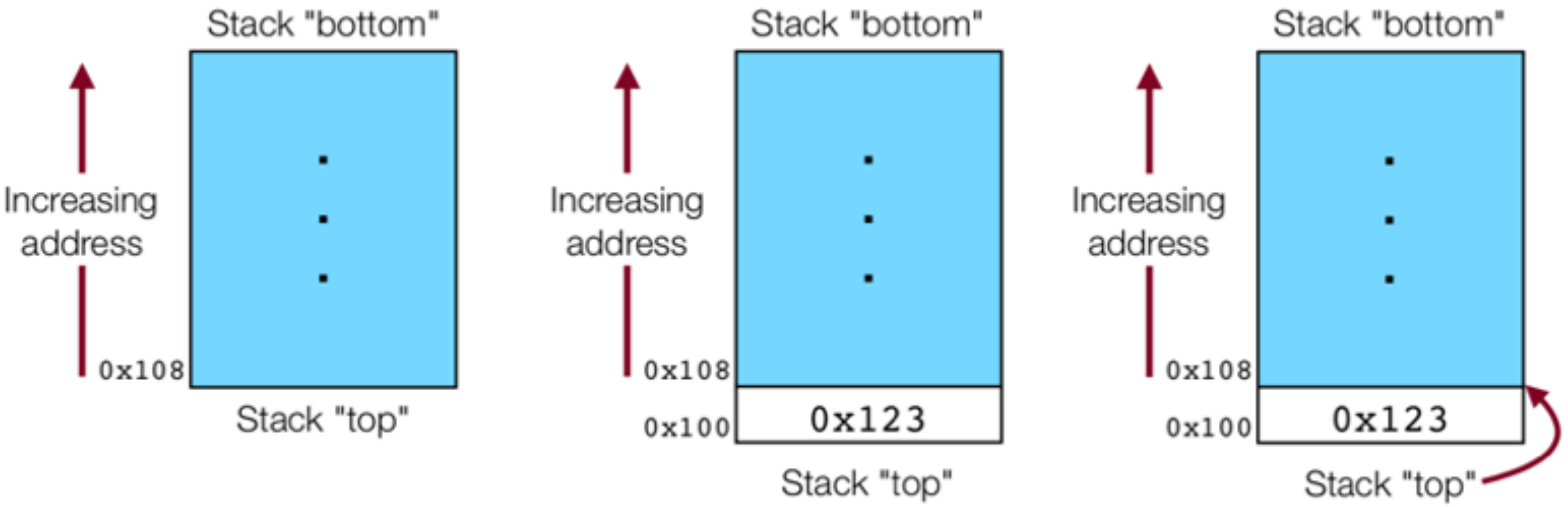
Pushing onto the Stack

- Example:

Initially	
%rax	0x123
%rdx	0
%rsp	0x108

pushq %rax	
%rax	0x123
%rdx	0
%rsp	0x100

popq %rdx	
%rax	0x123
%rdx	0x123
%rsp	0x108



Calling Functions In Assembly

To call a function in assembly, we must do a few things:

- **Pass Control** – %rip must be adjusted to execute the callee's instructions, and then resume the caller's instructions afterwards.
- **Pass Data** – we must pass any parameters and receive any return value.
- **Manage Memory** – we must handle any space needs of the callee on the stack.

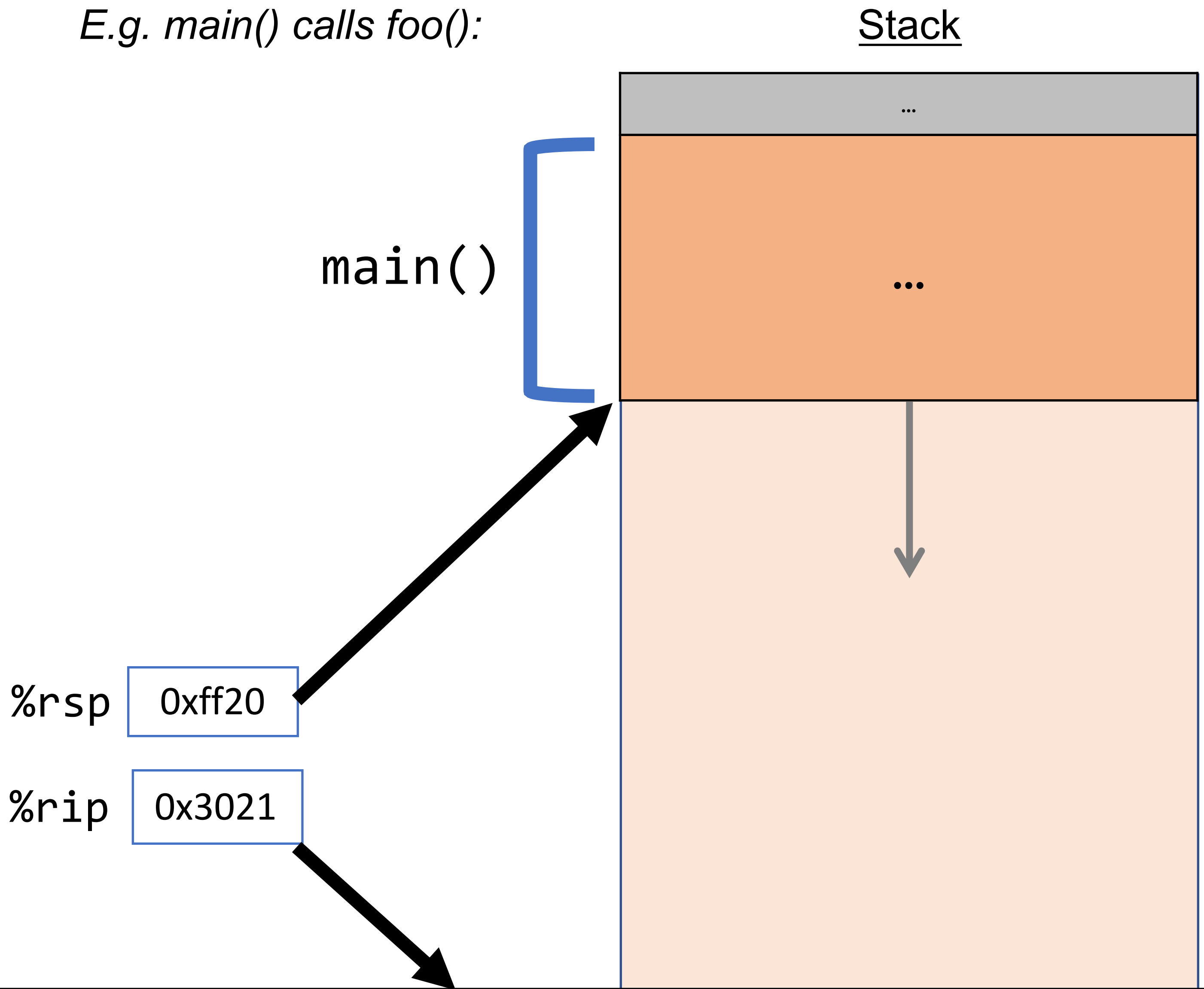
Terminology: **caller** function calls the **callee** function.

Plan For Today

- The Instruction Pointer (%rip)
- Calling Functions
  - The Stack
  - Passing Control
  - Passing Data
  - Local Storage
- **Break:** Announcements
- Register Restrictions
- Pulling it all together: recursion example

Remembering Where We Left Off

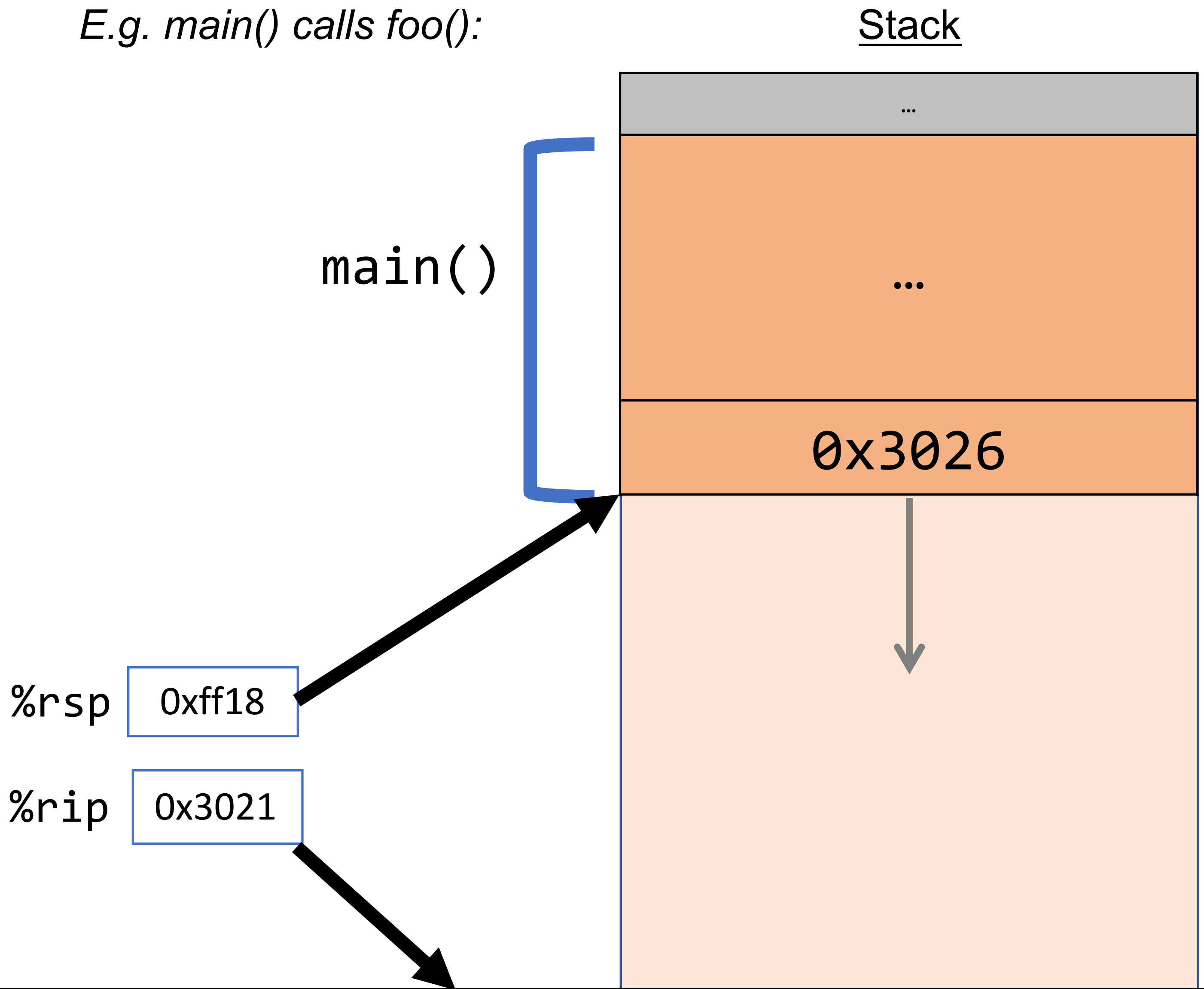
- **Problem:** %rip points to the currently executing instruction. To call a function, we must remember the *next* caller instruction to resume at after.
- **Solution:** push the current value of %rip onto the stack. Then call the function. When it is finished, put this value back into %rip and continue executing.



Remembering Where We Left Off

- **Problem:** %rip points to the currently executing instruction. To call a function, we must remember the *next* caller instruction to resume at after.
- **Solution:** push the current value of %rip onto the stack. Then call the function. When it is finished, put this value back into %rip and continue executing.

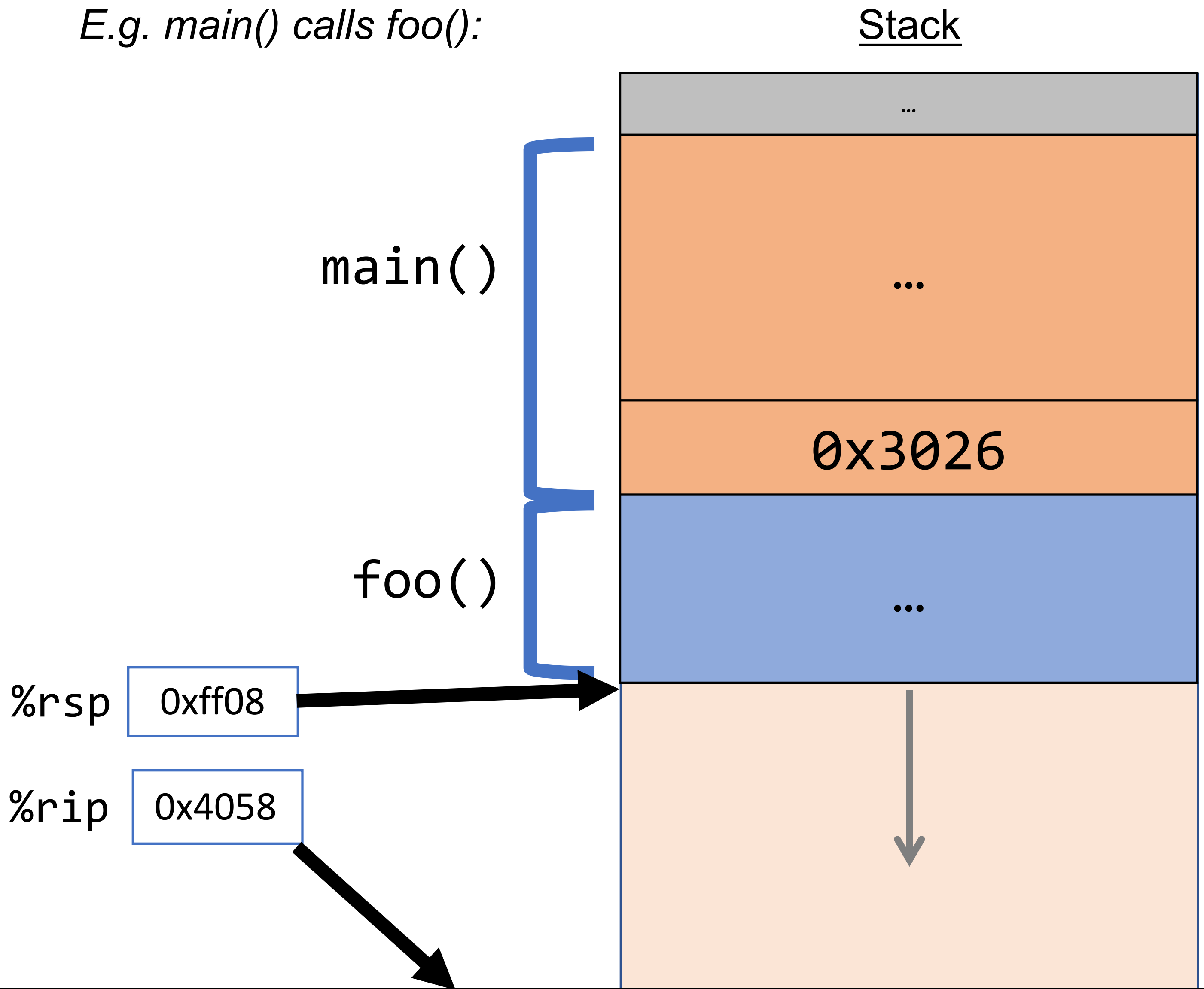
E.g. main() calls foo():



Remembering Where We Left Off

- **Problem:** %rip points to the currently executing instruction. To call a function, we must remember the *next* caller instruction to resume at after.
- **Solution:** push the current value of %rip onto the stack. Then call the function. When it is finished, put this value back into %rip and continue executing.

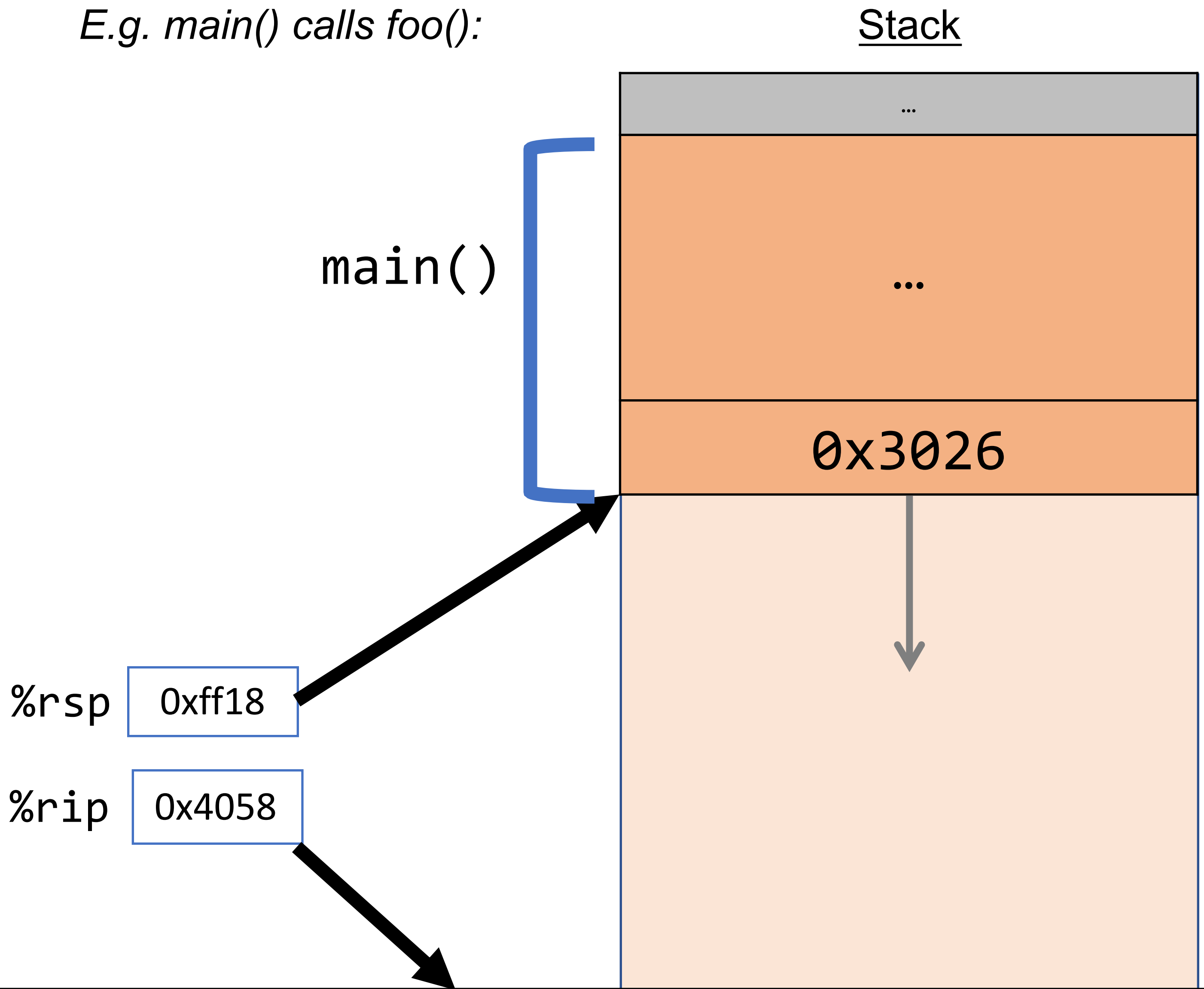
E.g. main() calls foo():



Remembering Where We Left Off

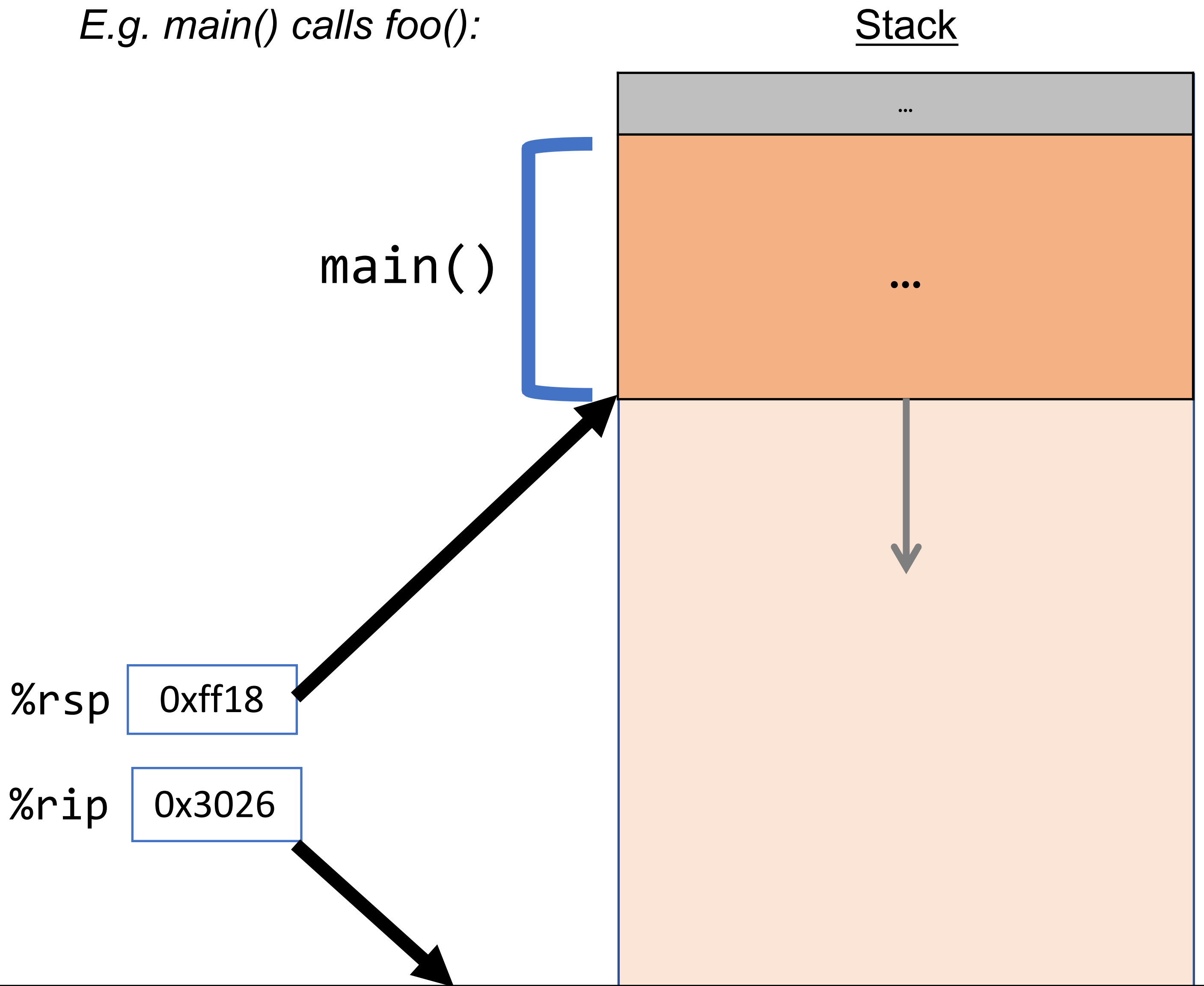
- **Problem:** %rip points to the currently executing instruction. To call a function, we must remember the *next* caller instruction to resume at after.
- **Solution:** push the current value of %rip onto the stack. Then call the function. When it is finished, put this value back into %rip and continue executing.

E.g. main() calls foo():



Remembering Where We Left Off

- **Problem:** %rip points to the currently executing instruction. To call a function, we must remember the *next* caller instruction to resume at after.
- **Solution:** push the current value of %rip onto the stack. Then call the function. When it is finished, put this value back into %rip and continue executing.



Call And Return

The **call** instruction pushes the value of %rip onto the stack and sets %rip to point to the beginning of the specified function's instructions.

```
call Label
call *Operand
```

The **ret** instruction pops the value of %rip from the stack and stores it in %rip.

```
ret
```

The stored %rip value for a function is called its **return address.** It is the address of the instruction at which to resume the function's execution. (not to be confused with **return value**, which is the value returned from a function).

Calling Functions In Assembly

To call a function in assembly, we must do a few things:

- **Pass Control** – %rip must be adjusted to execute the function being called and then resume the caller function afterwards.
- **Pass Data** – we must pass any parameters and receive any return value.
- **Manage Memory** – we must handle any space needs of the callee on the stack.

Terminology: **caller** function calls the **callee** function.

Plan For Today

- The Instruction Pointer (%rip)
- Calling Functions
  - The Stack
  - Passing Control
  - Passing Data
  - Local Storage
- **Break:** Announcements
- Register Restrictions
- Pulling it all together: recursion example

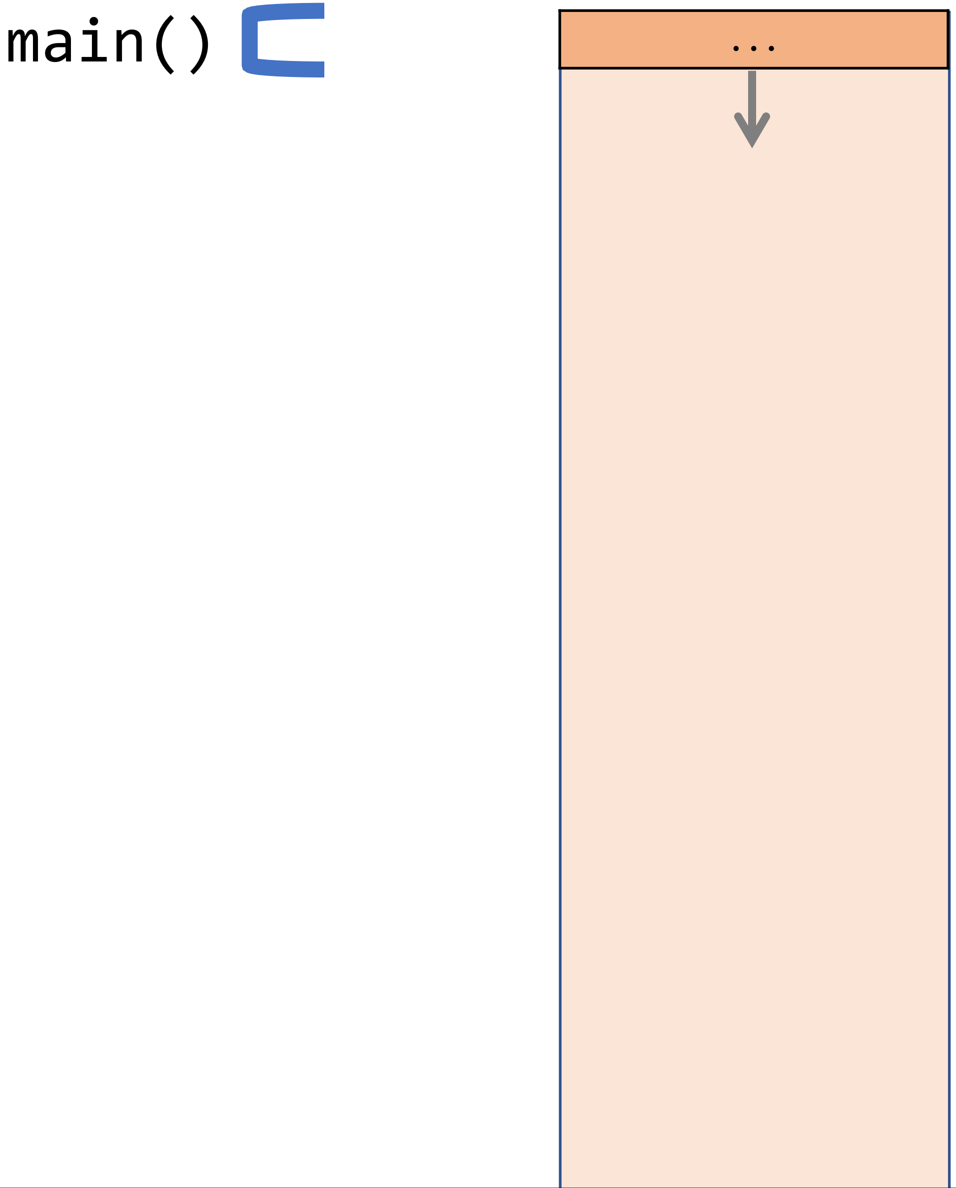
Parameters and Return

- There are special registers that store parameters and the return value.
- To call a function, we must put any parameters we are passing into the correct registers. (%rdi, %rsi, %rdx, %rcx, %r8, %r9, in that order)
- Parameters beyond the first 6 are put on the stack.
- If the caller expects a return value, it looks in %rax after the callee completes.

Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
             int v1, int v2, int v3, int v4) {
    …
}
```

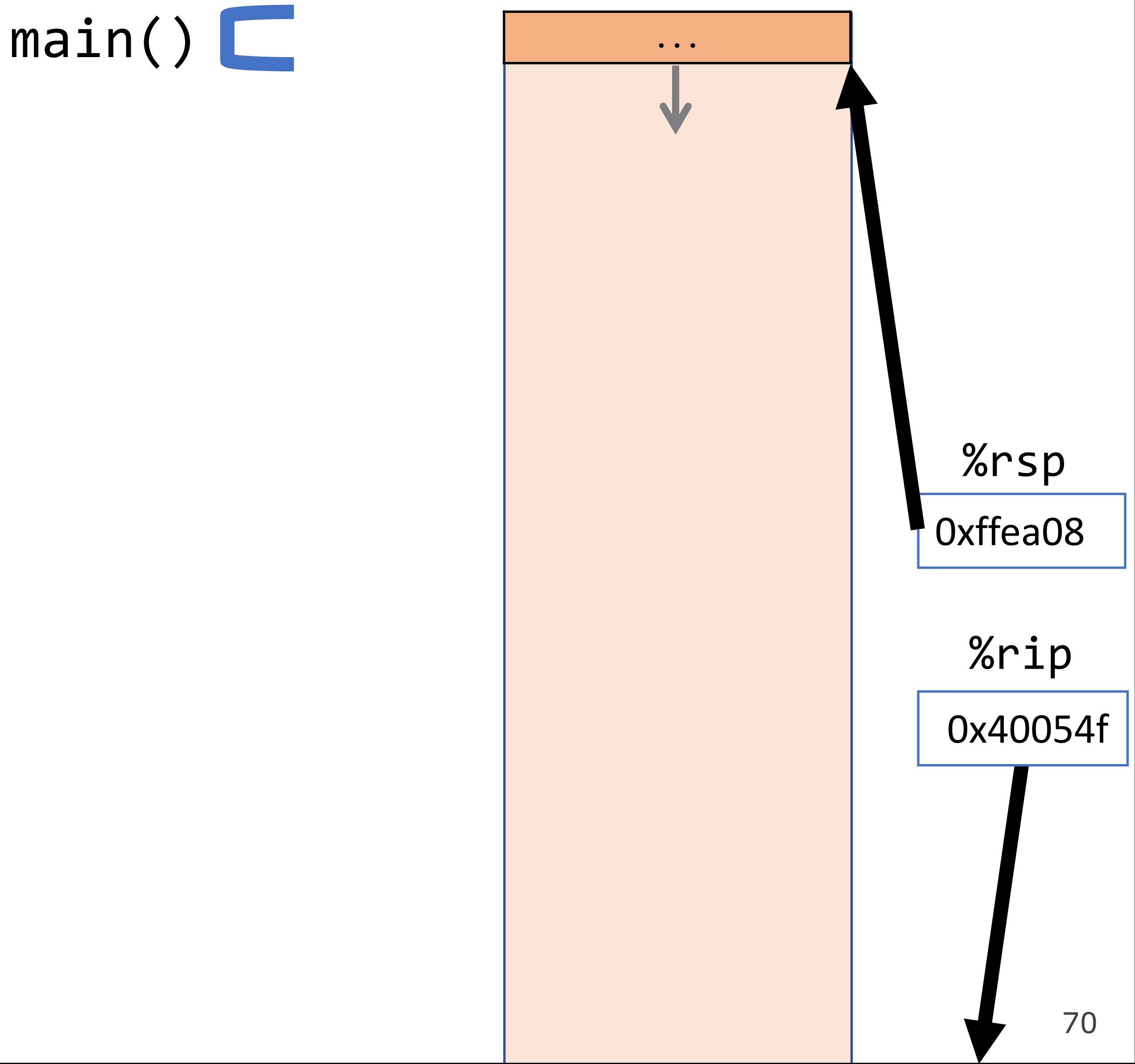


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x40054f <+0>:     sub    $0x18,%rsp
0x400553 <+4>:     movl   $0x1,0xc(%rsp)
0x40055b <+12>:    movl   $0x2,0x8(%rsp)
0x400563 <+20>:    movl   $0x3,0x4(%rsp)
0x40056b <+28>:    movl   $0x4,(%rsp)
```

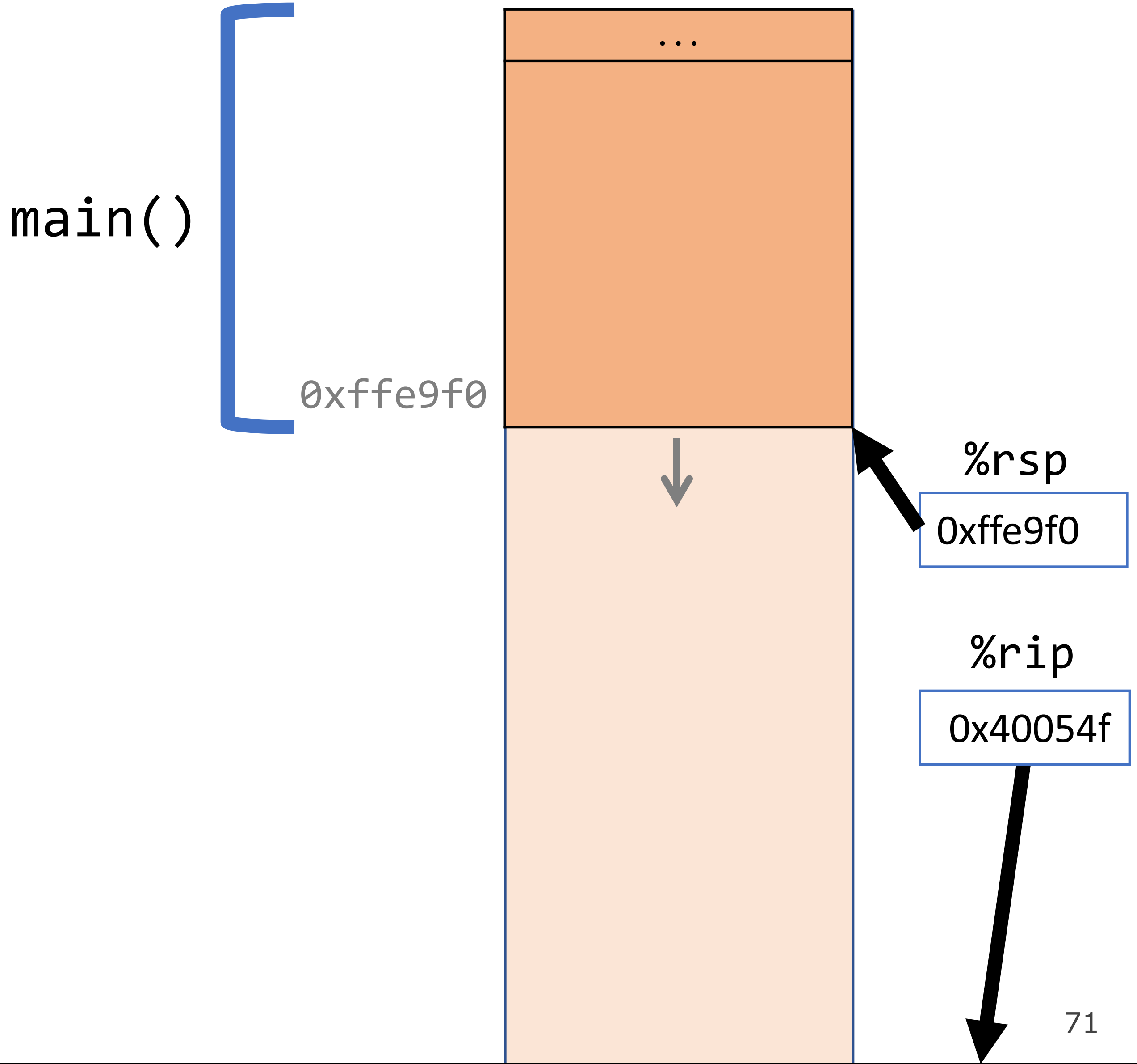


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x40054f <+0>:    sub    $0x18,%rsp
0x400553 <+4>:    movl   $0x1,0xc(%rsp)
0x40055b <+12>:   movl   $0x2,0x8(%rsp)
0x400563 <+20>:   movl   $0x3,0x4(%rsp)
0x40056b <+28>:   movl   $0x4,(%rsp)
```

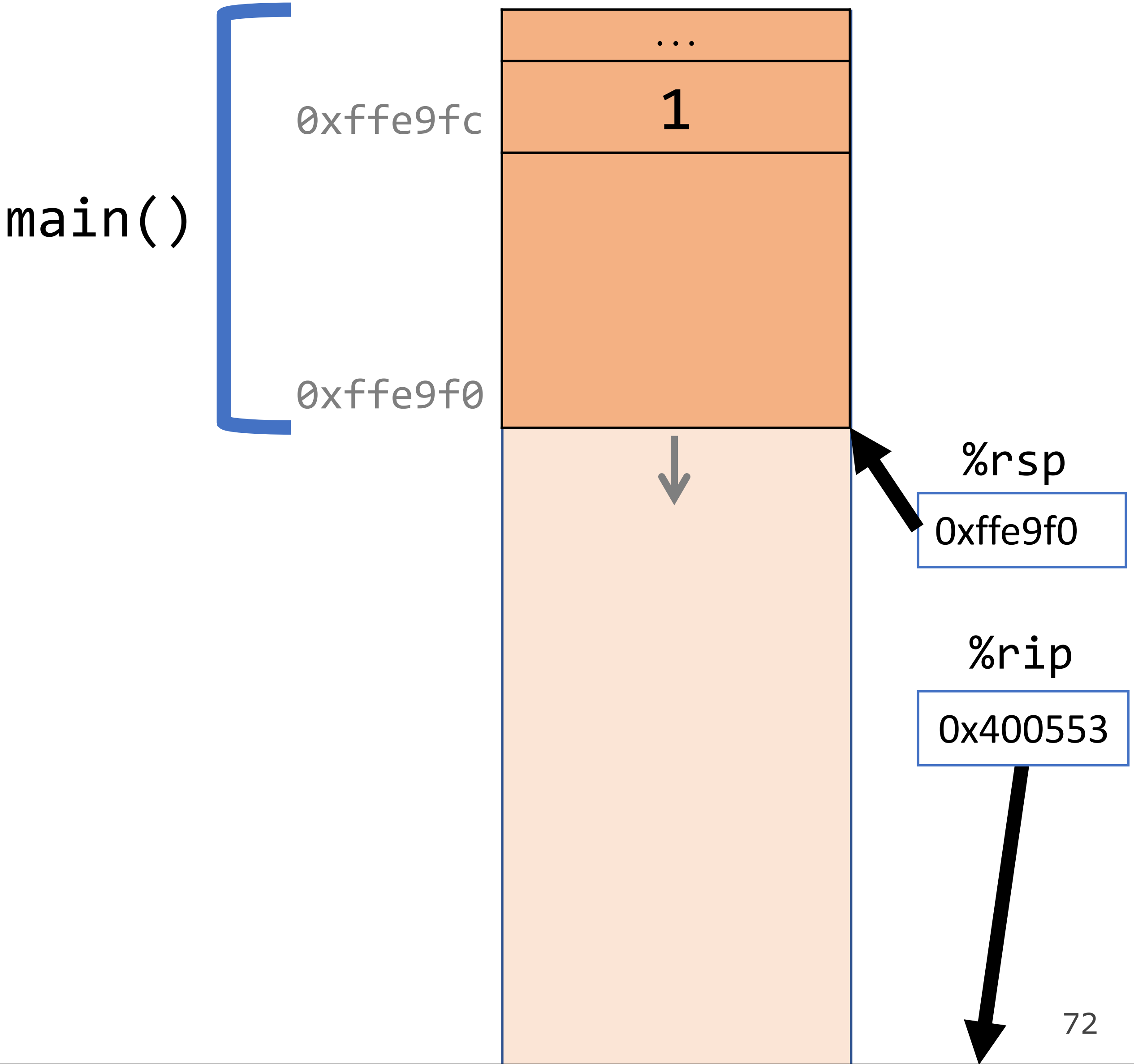


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x40054f <+0>:     sub     $0x18,%rsp
0x400553 <+4>:     movl    $0x1,0xc(%rsp)
0x40055b <+12>:    movl    $0x2,0x8(%rsp)
0x400563 <+20>:    movl    $0x3,0x4(%rsp)
0x40056b <+28>:    movl    $0x4,(%rsp)
```

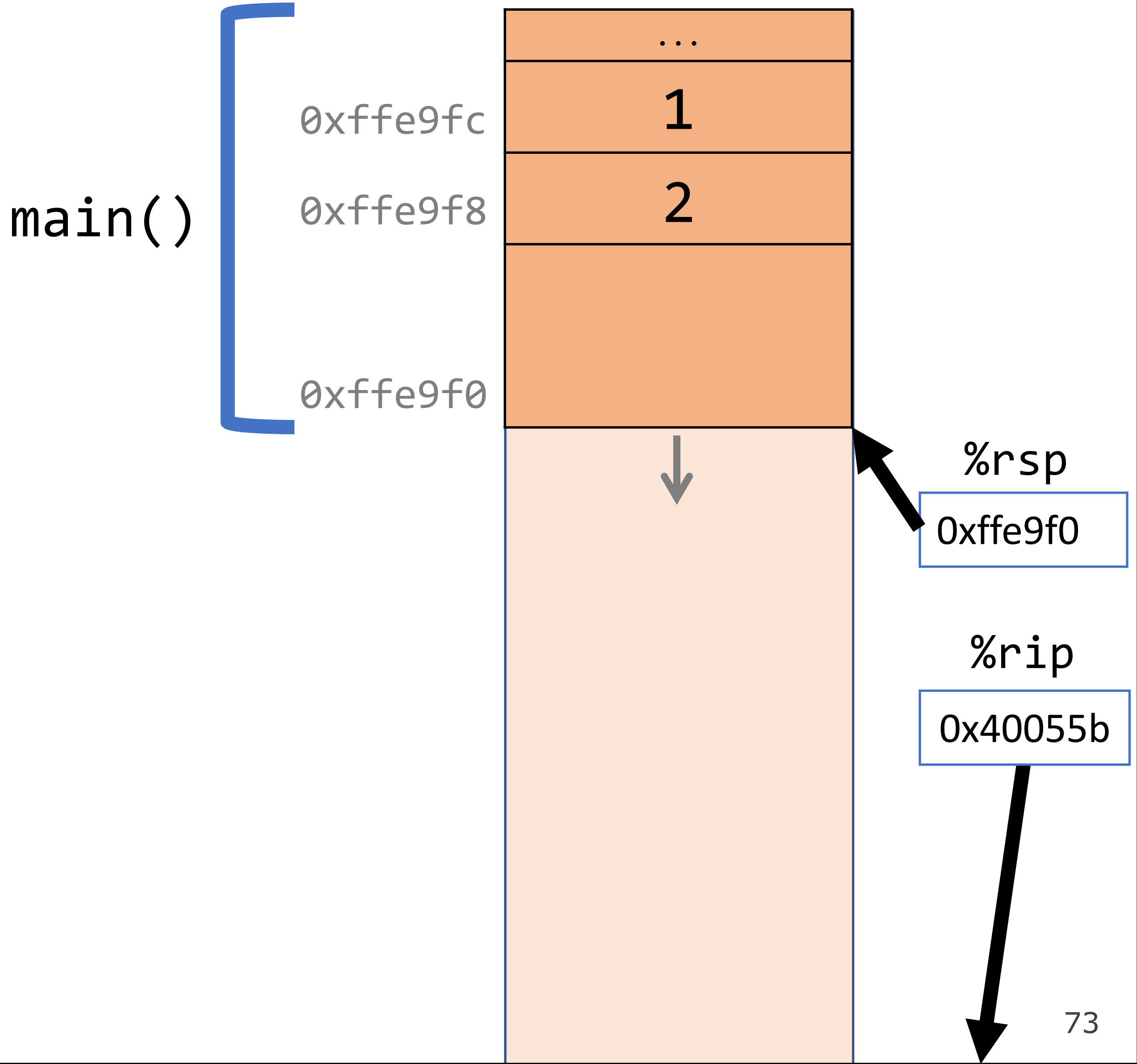


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x40054f <+0>:     sub    $0x18,%rsp
0x400553 <+4>:     movl   $0x1,0xc(%rsp)
0x40055b <+12>:    movl   $0x2,0x8(%rsp)
0x400563 <+20>:    movl   $0x3,0x4(%rsp)
0x40056b <+28>:    movl   $0x4,(%rsp)
```

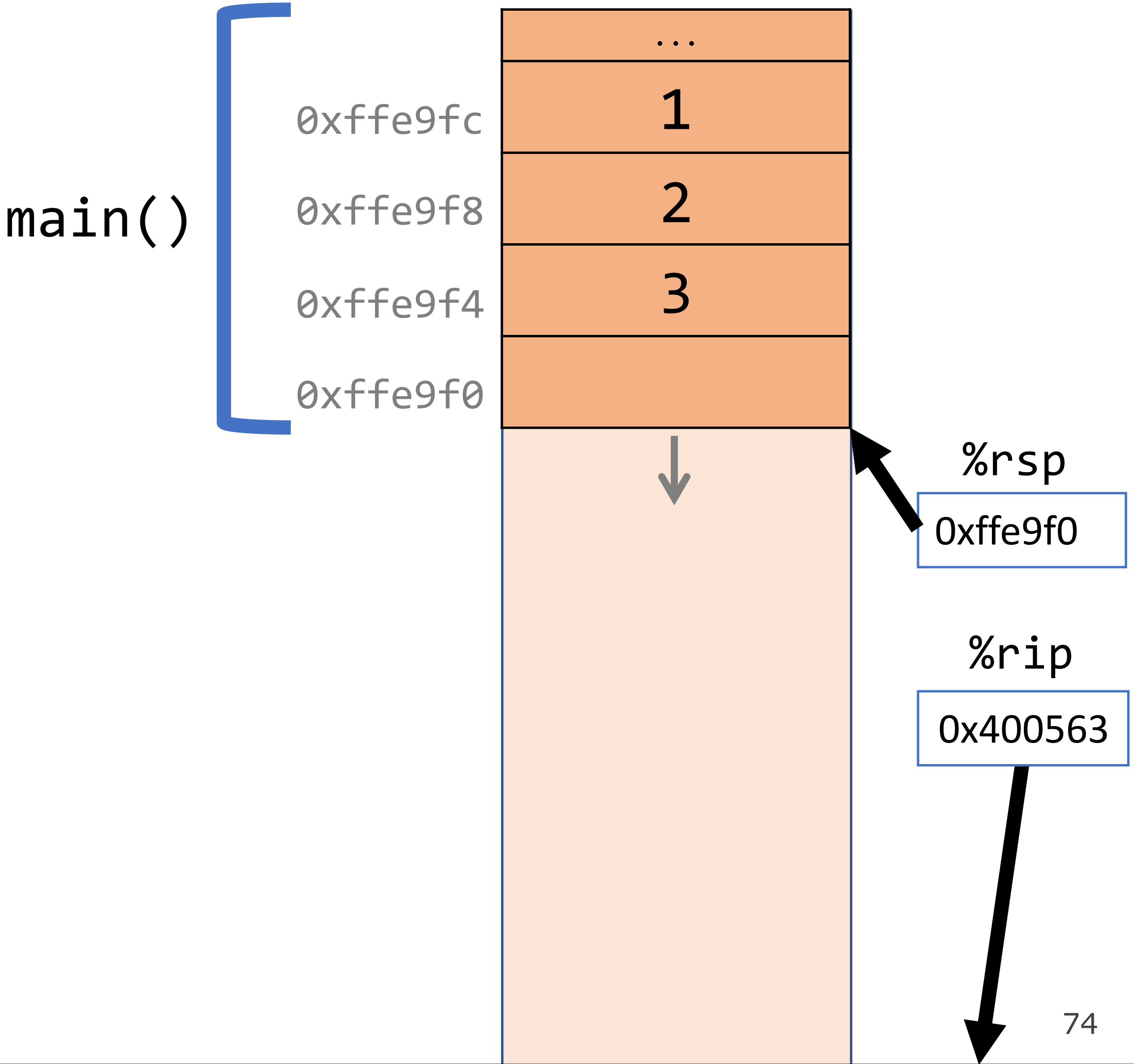


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x400553 <+4>:    movl   $0x1,0xc(%rsp)
0x40055b <+12>:   movl   $0x2,0x8(%rsp)
0x400563 <+20>:   movl   $0x3,0x4(%rsp)
0x40056b <+28>:   movl   $0x4,(%rsp)
0x400572 <+35>:   pushq  $0x4
```

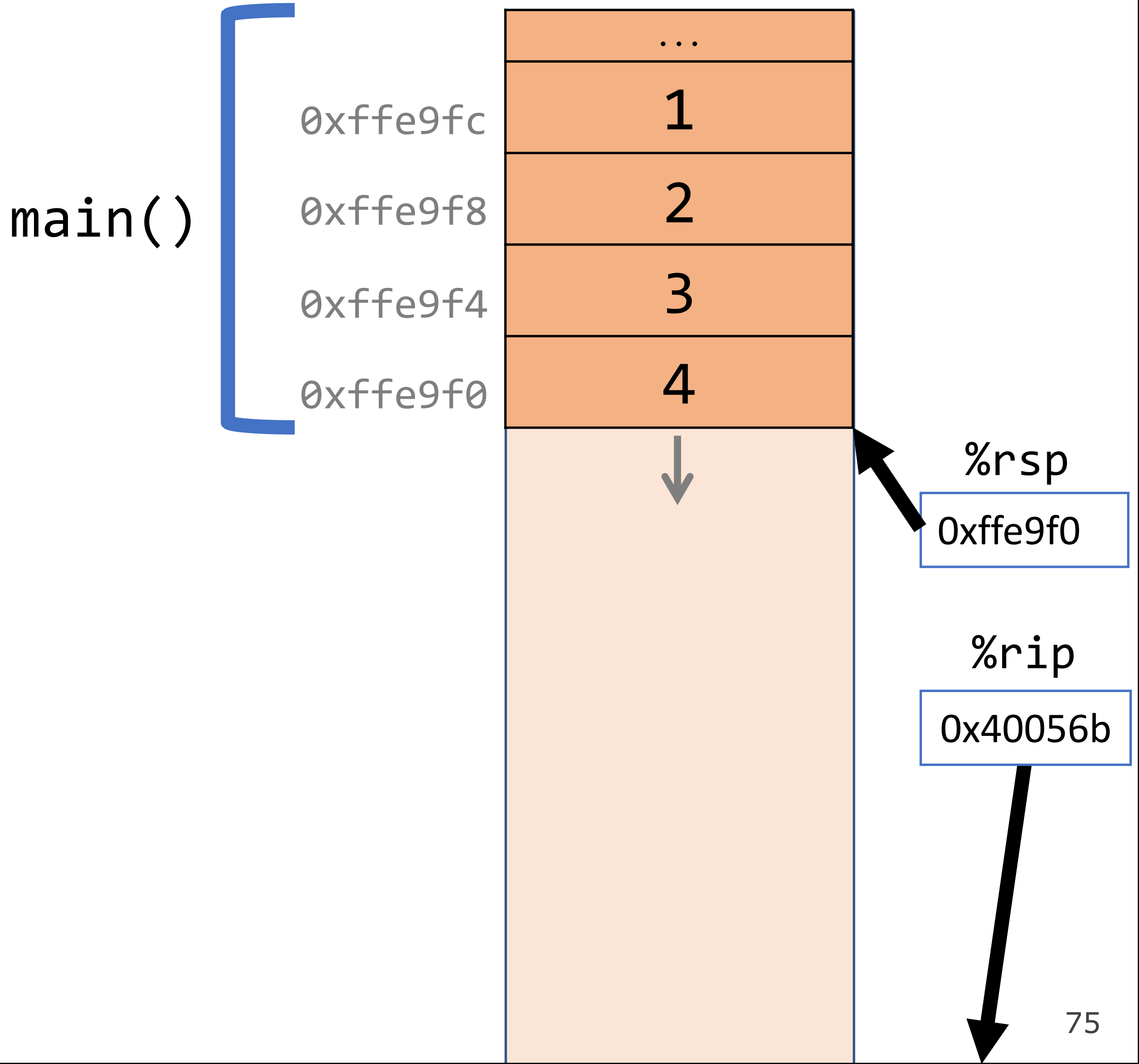


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x40055b <+12>:   movl    $0x2,0x8(%rsp)
0x400563 <+20>:   movl    $0x3,0x4(%rsp)
0x40056b <+28>:   movl    $0x4,(%rsp)
0x400572 <+35>:   pushq   $0x4
0x400574 <+37>:   pushq   $0x3
```

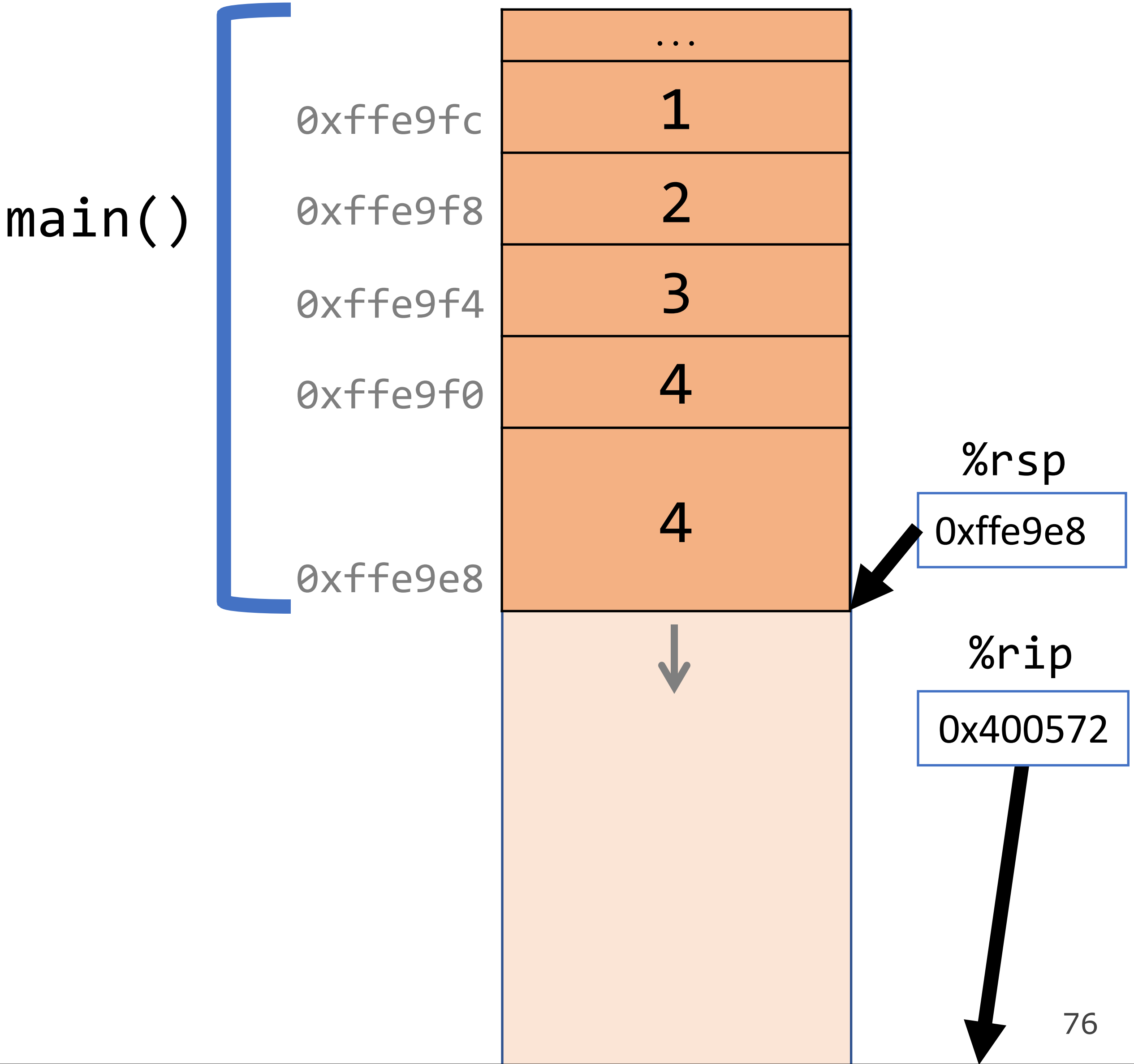


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
             int v1, int v2, int v3, int v4) {
    …
}
```

```
0x400563 <+20>:    movl   $0x3,0x4(%rsp)
0x40056b <+28>:    movl   $0x4,(%rsp)
0x400572 <+35>:    pushq  $0x4
0x400574 <+37>:    pushq  $0x3
0x400576 <+39>:    mov    $0x2,%r9d
```

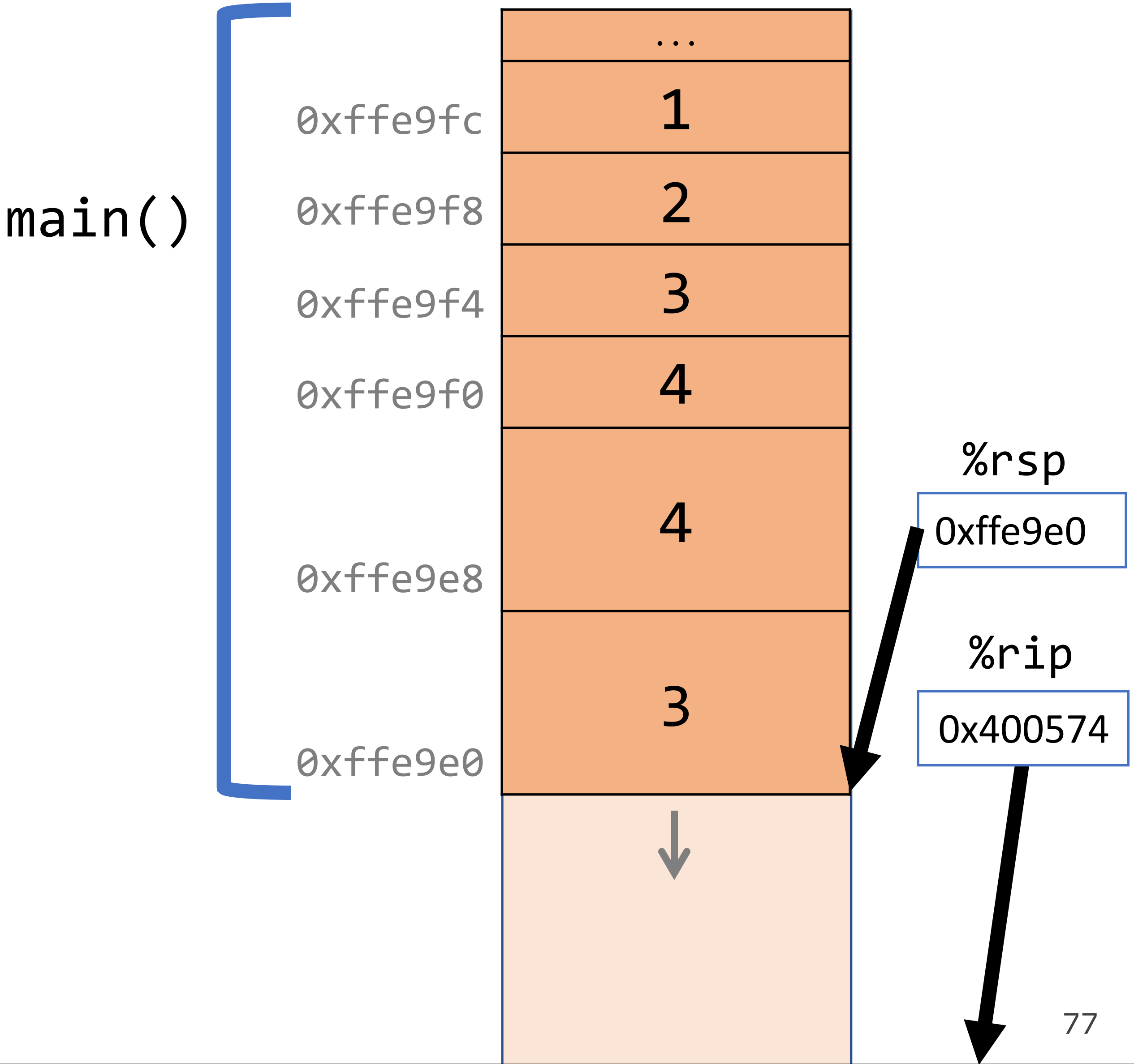


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x40056b <+28>:   movl   $0x4,(%rsp)
0x400572 <+35>:   pushq  $0x4
0x400574 <+37>:   pushq  $0x3
0x400576 <+39>:   mov    $0x2,%r9d
0x40057c <+45>:   mov    $0x1,%r8d
```

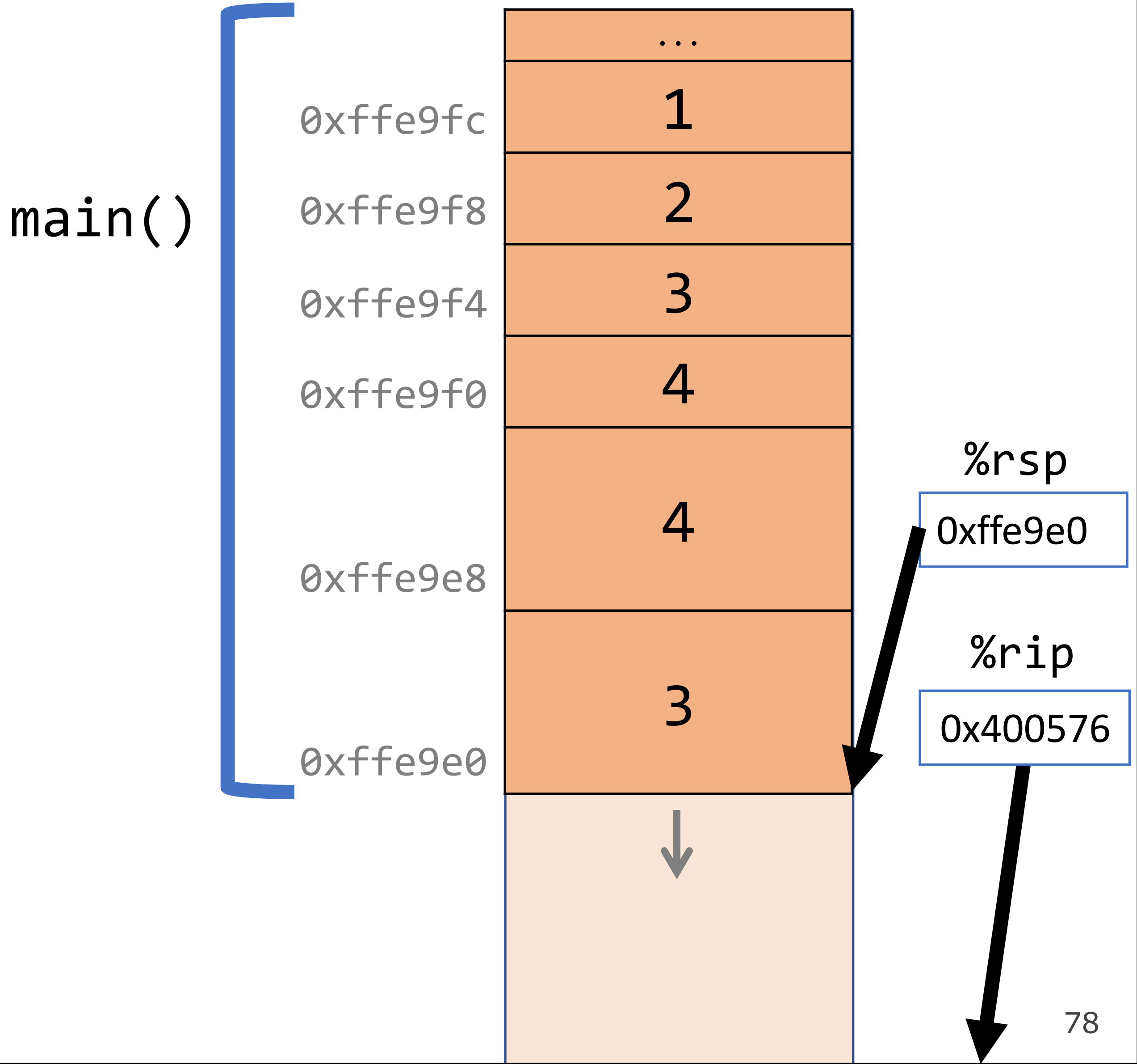


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x400572 <+35>:    pushq   $0x4
0x400574 <+37>:    pushq   $0x3
0x400576 <+39>:    mov     $0x2,%r9d
0x40057c <+45>:    mov     $0x1,%r8d
0x400582 <+51>:    lea     0x10(%rsp),%rcx
```

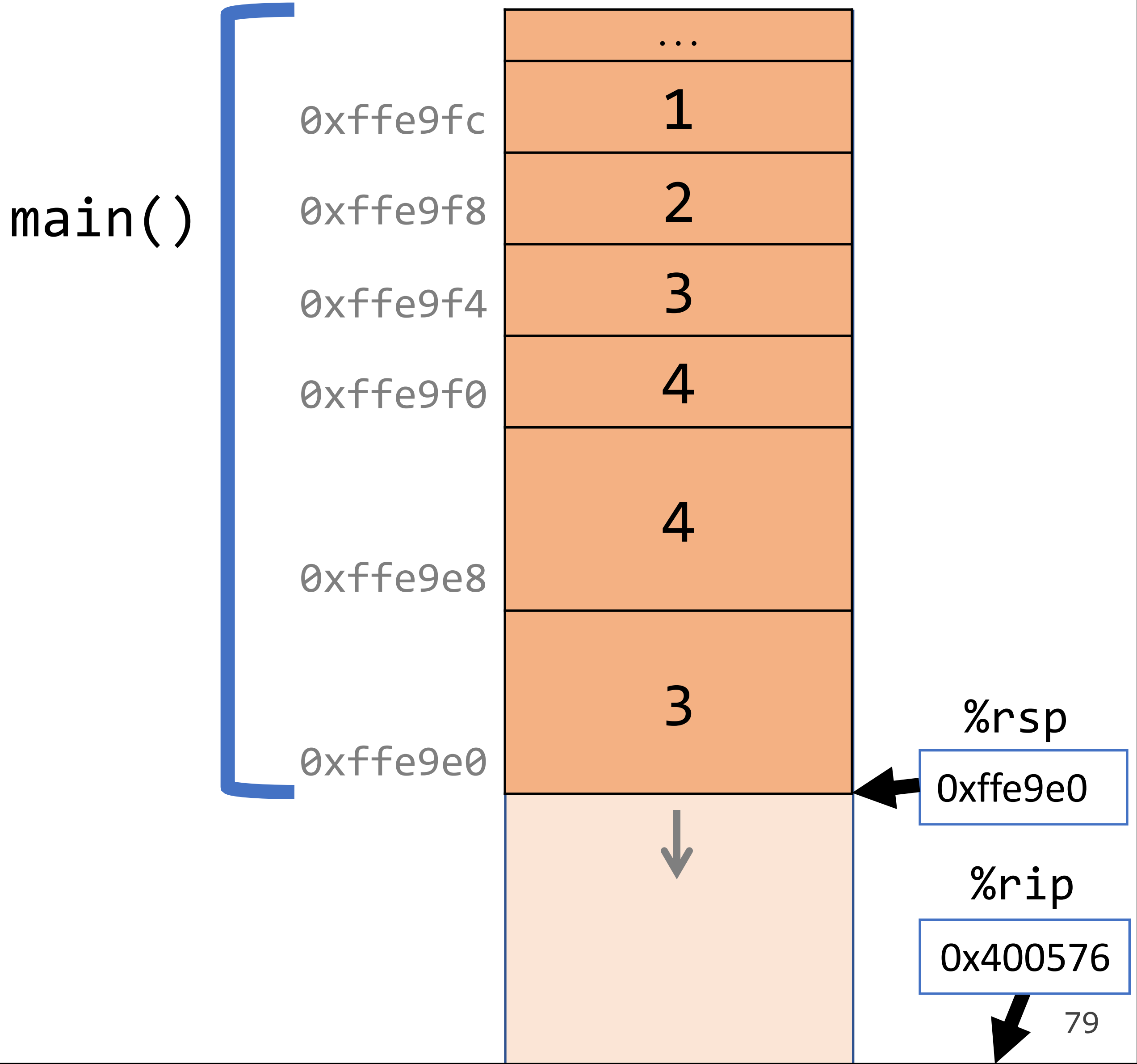


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x400572 <+35>:   pushq  $0x4
0x400574 <+37>:   pushq  $0x3
0x400576 <+39>:   mov    $0x2,%r9d
0x40057c <+45>:   mov    $0x1,%r8d
0x400582 <+51>:   lea    0x10(%rsp),%rcx
```

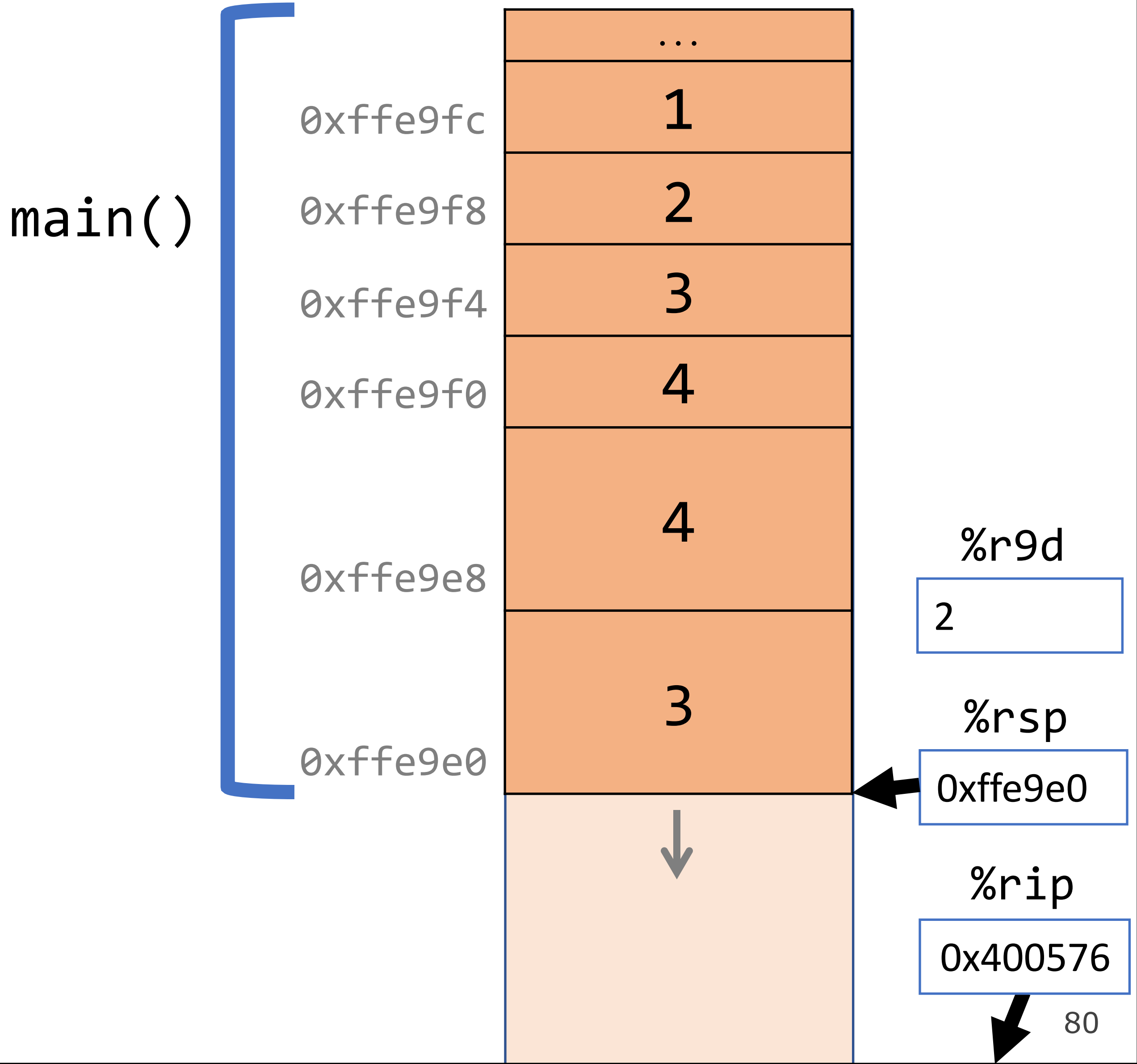


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x400572 <+35>:   pushq   $0x4
0x400574 <+37>:   pushq   $0x3
0x400576 <+39>:   mov     $0x2,%r9d
0x40057c <+45>:   mov     $0x1,%r8d
0x400582 <+51>:   lea     0x10(%rsp),%rcx
```

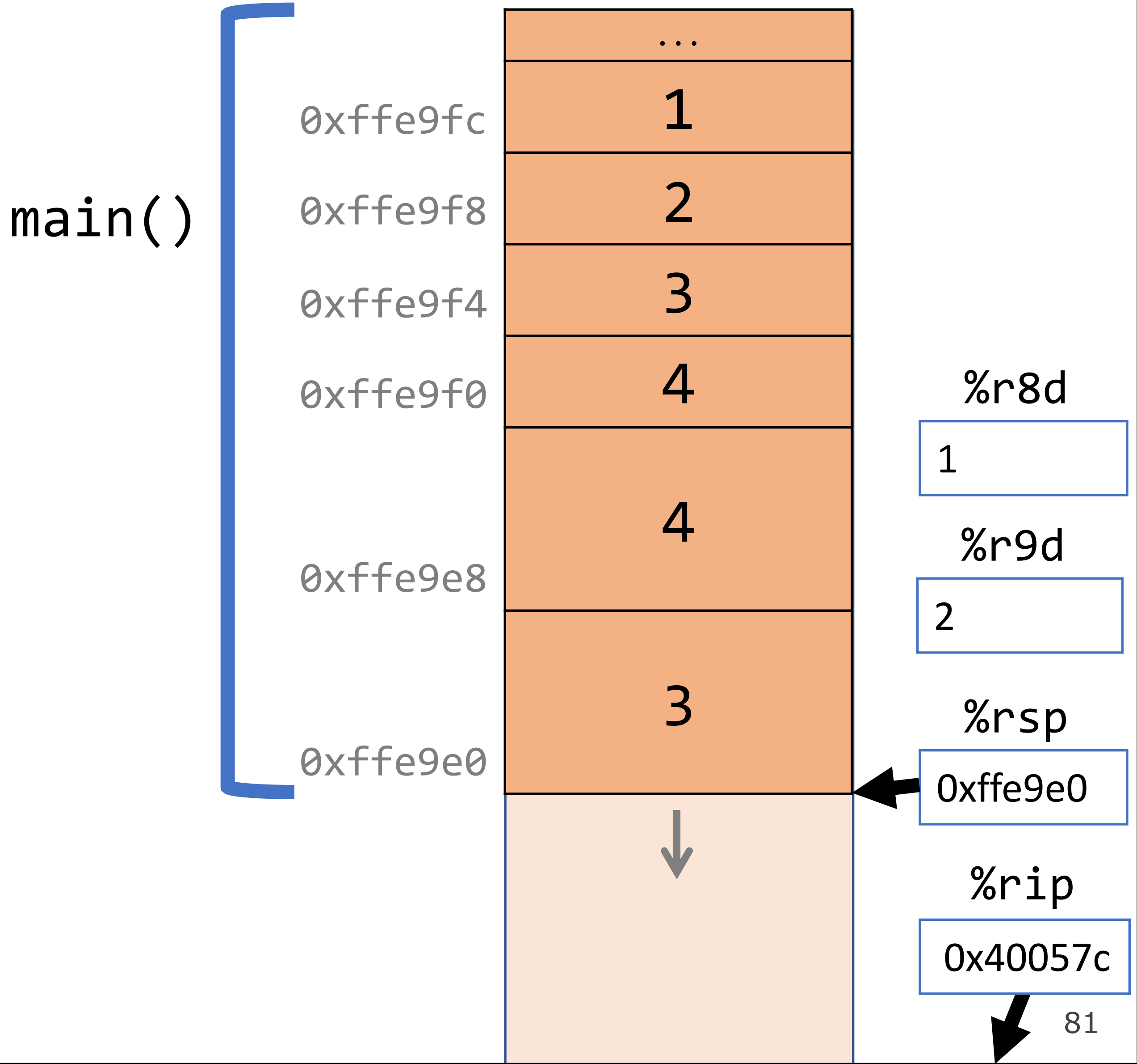


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
             int v1, int v2, int v3, int v4) {
    …
}
```

```
0x400574 <+37>:    pushq   $0x3
0x400576 <+39>:    mov     $0x2,%r9d
0x40057c <+45>:    mov     $0x1,%r8d
0x400582 <+51>:    lea     0x10(%rsp),%rcx
0x400587 <+56>:    lea     0x14(%rsp),%rdx
```

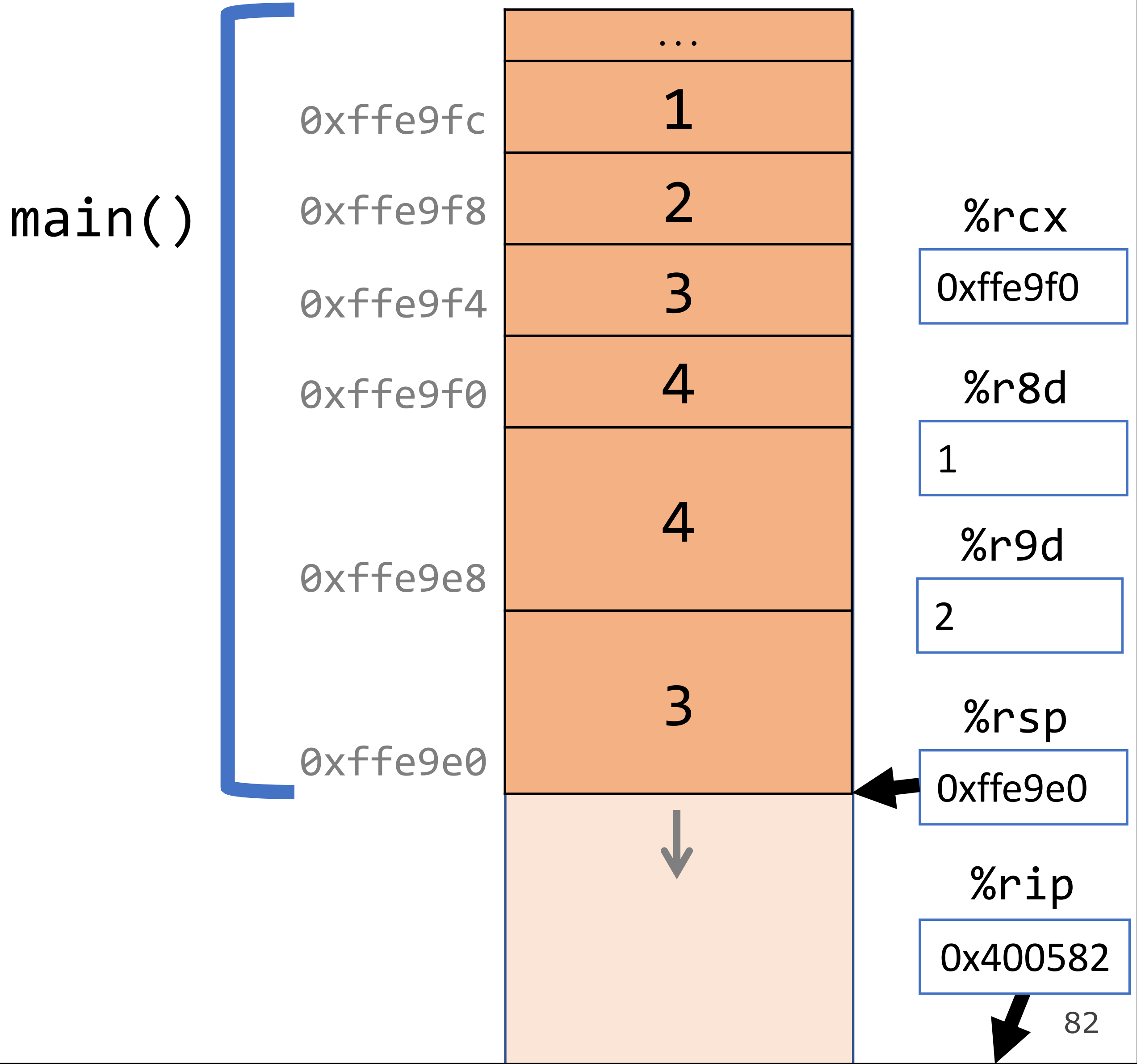


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x400576 <+39>:    mov    $0x2,%r9d
0x40057c <+45>:    mov    $0x1,%r8d
0x400582 <+51>:    lea    0x10(%rsp),%rcx
0x400587 <+56>:    lea    0x14(%rsp),%rdx
0x40058c <+61>:    lea    0x18(%rsp),%rsi
```

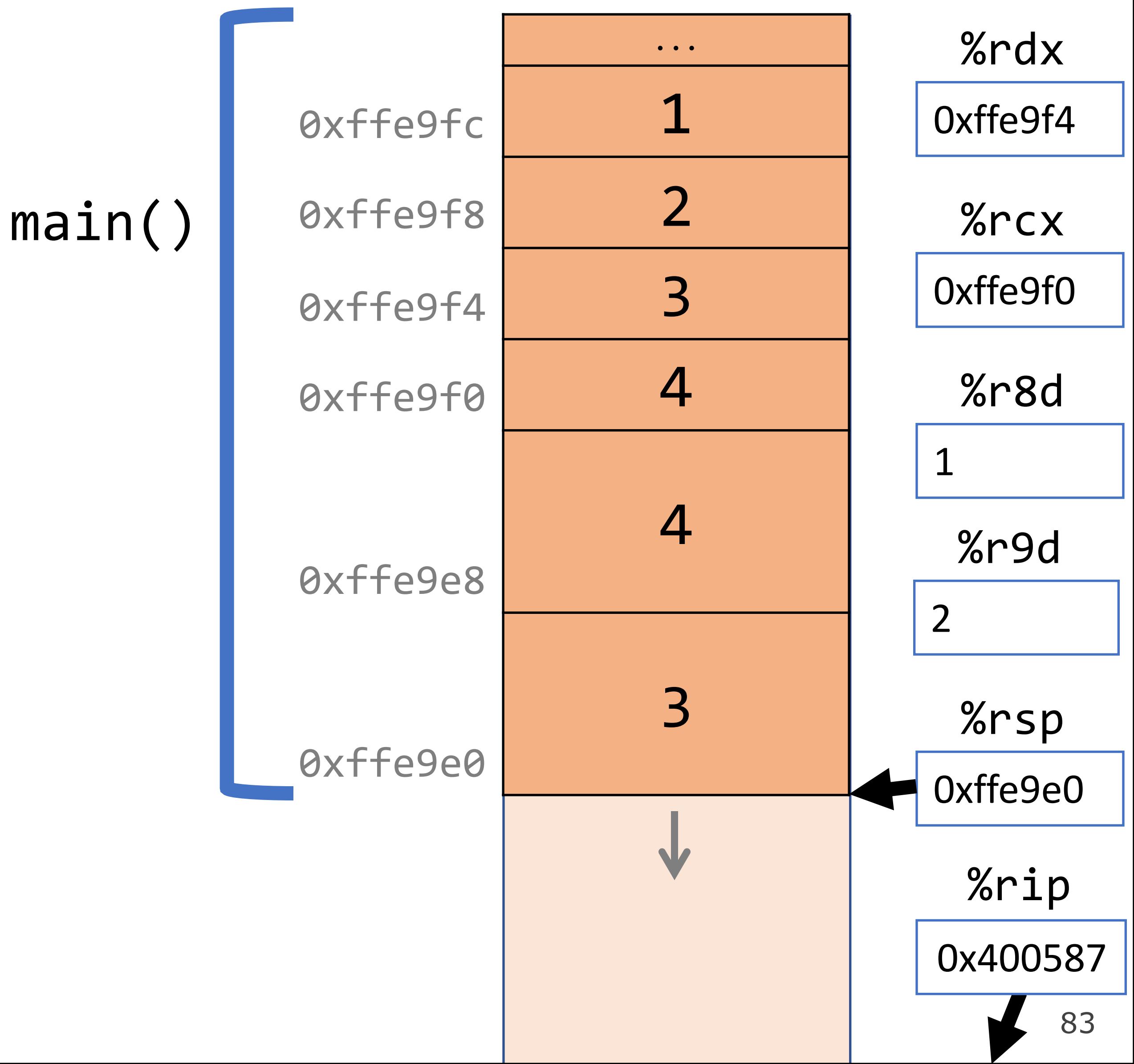


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x40057c <+45>:    mov    $0x1,%r8d
0x400582 <+51>:    lea    0x10(%rsp),%rcx
0x400587 <+56>:    lea    0x14(%rsp),%rdx
0x40058c <+61>:    lea    0x18(%rsp),%rsi
0x400591 <+66>:    lea    0x1c(%rsp),%rdi
```

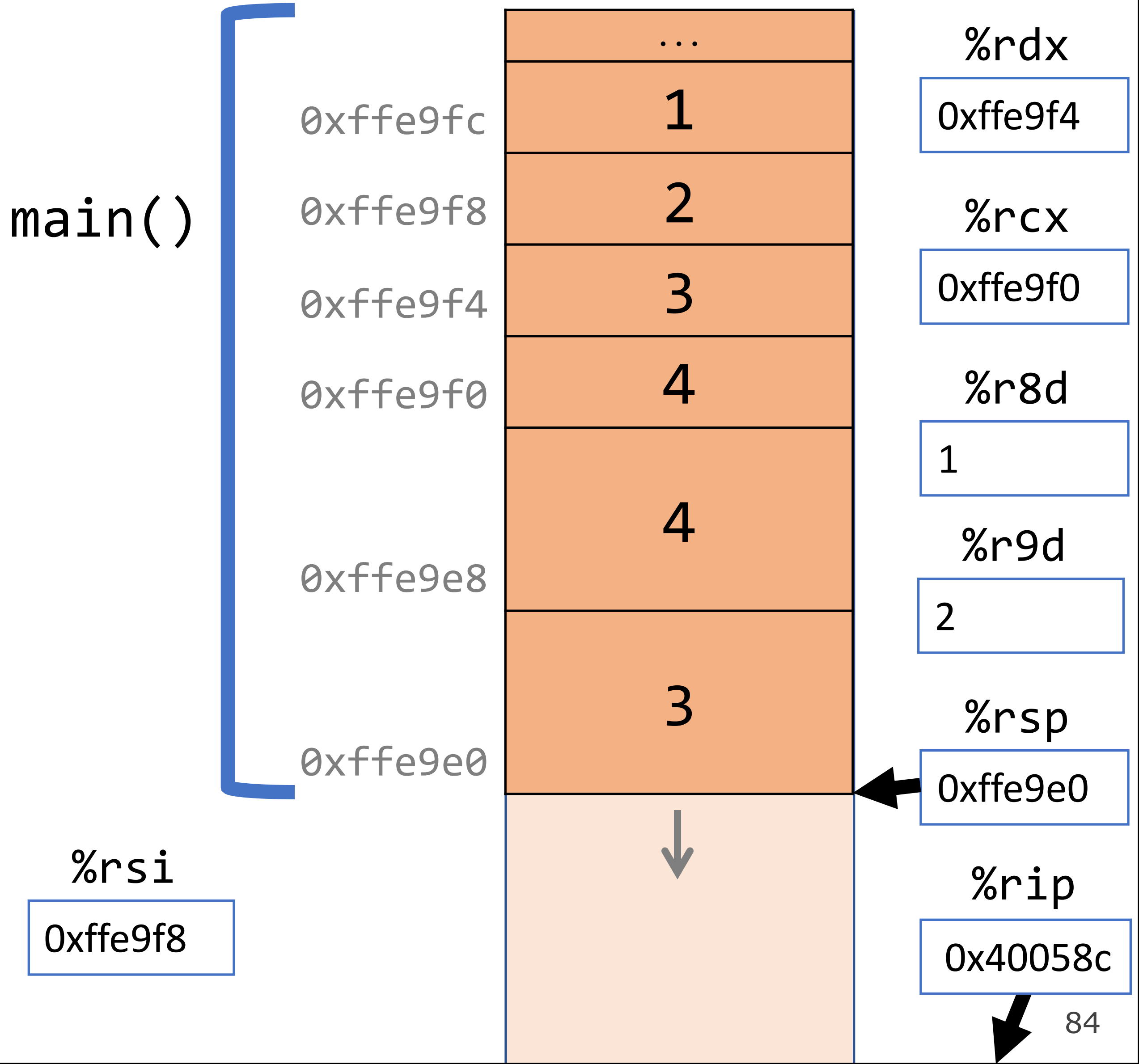


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
             int v1, int v2, int v3, int v4) {
    …
}
```

```
0x400582 <+51>:    lea    0x10(%rsp),%rcx
0x400587 <+56>:    lea    0x14(%rsp),%rdx
0x40058c <+61>:    lea    0x18(%rsp),%rsi
0x400591 <+66>:    lea    0x1c(%rsp),%rdi
0x400596 <+71>:    callq  0x400546 <func>
```

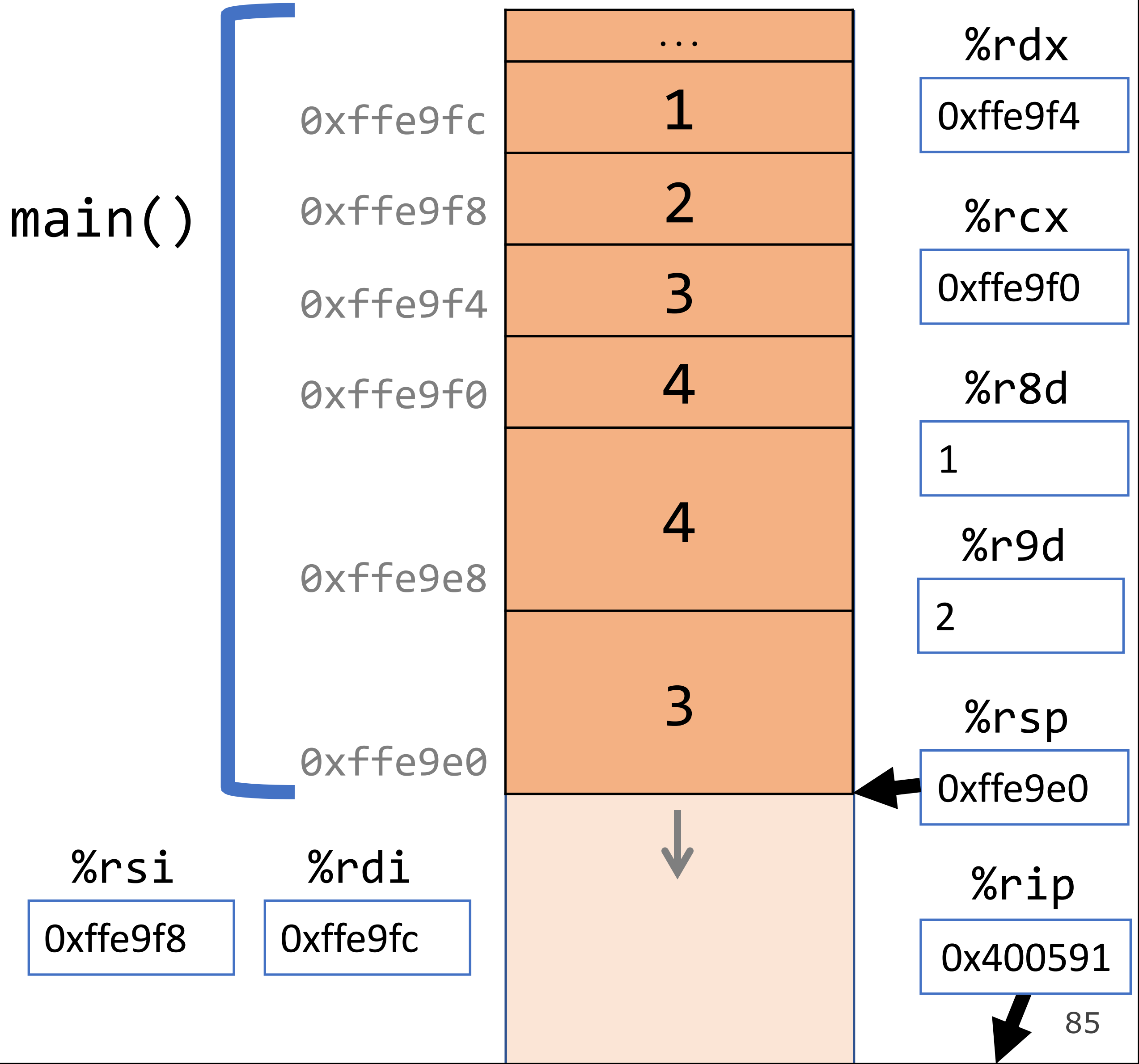


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x400587 <+56>:   lea    0x14(%rsp),%rdx
0x40058c <+61>:   lea    0x18(%rsp),%rsi
0x400591 <+66>:   lea    0x1c(%rsp),%rdi
0x400596 <+71>:   callq  0x400546 <func>
0x40059b <+76>:   add    $0x10,%rsp
```

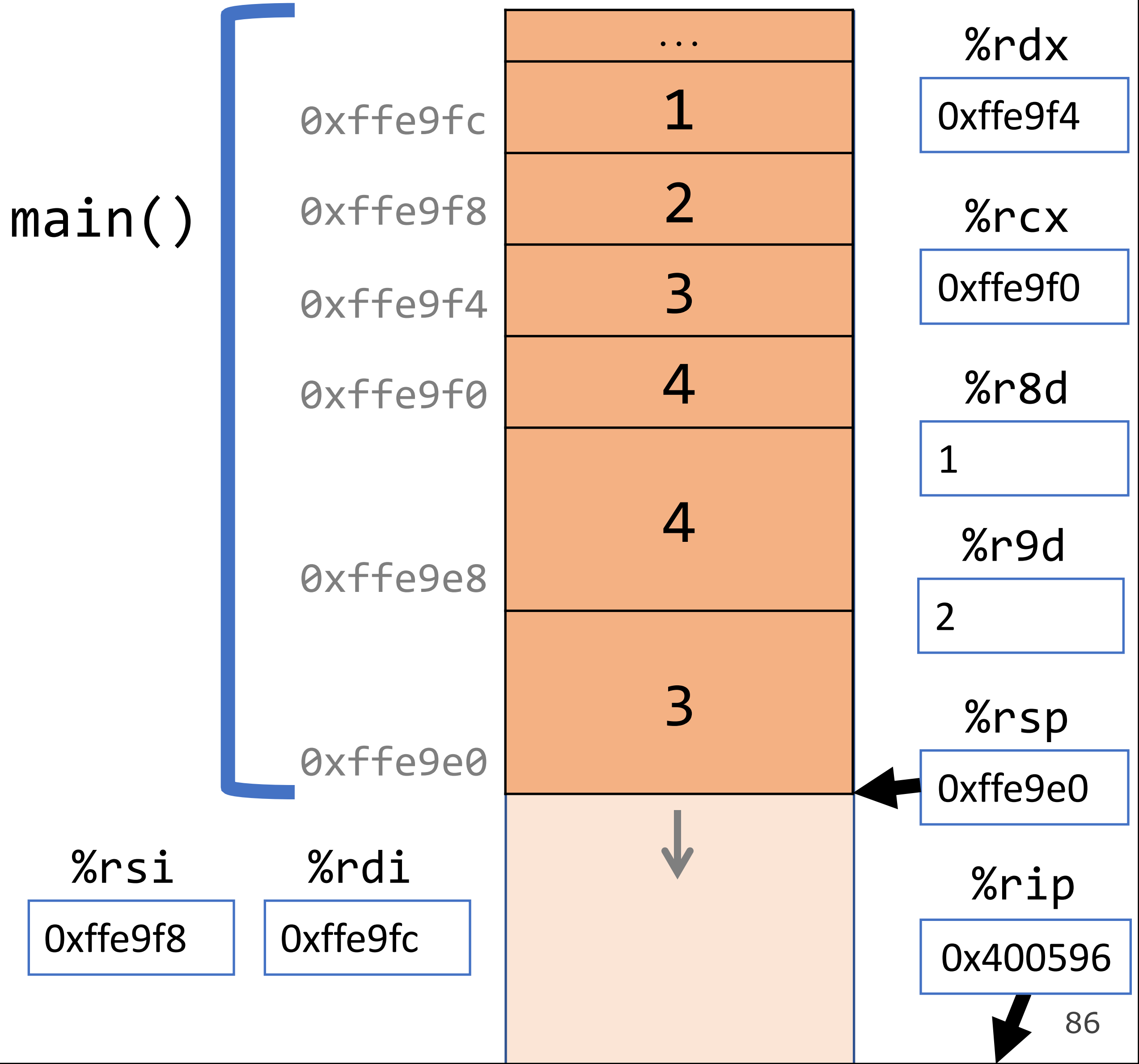


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x40058c <+61>:    lea    0x18(%rsp),%rsi
0x400591 <+66>:    lea    0x1c(%rsp),%rdi
0x400596 <+71>:    callq  0x400546 <func>
0x40059b <+76>:    add    $0x10,%rsp
…
```

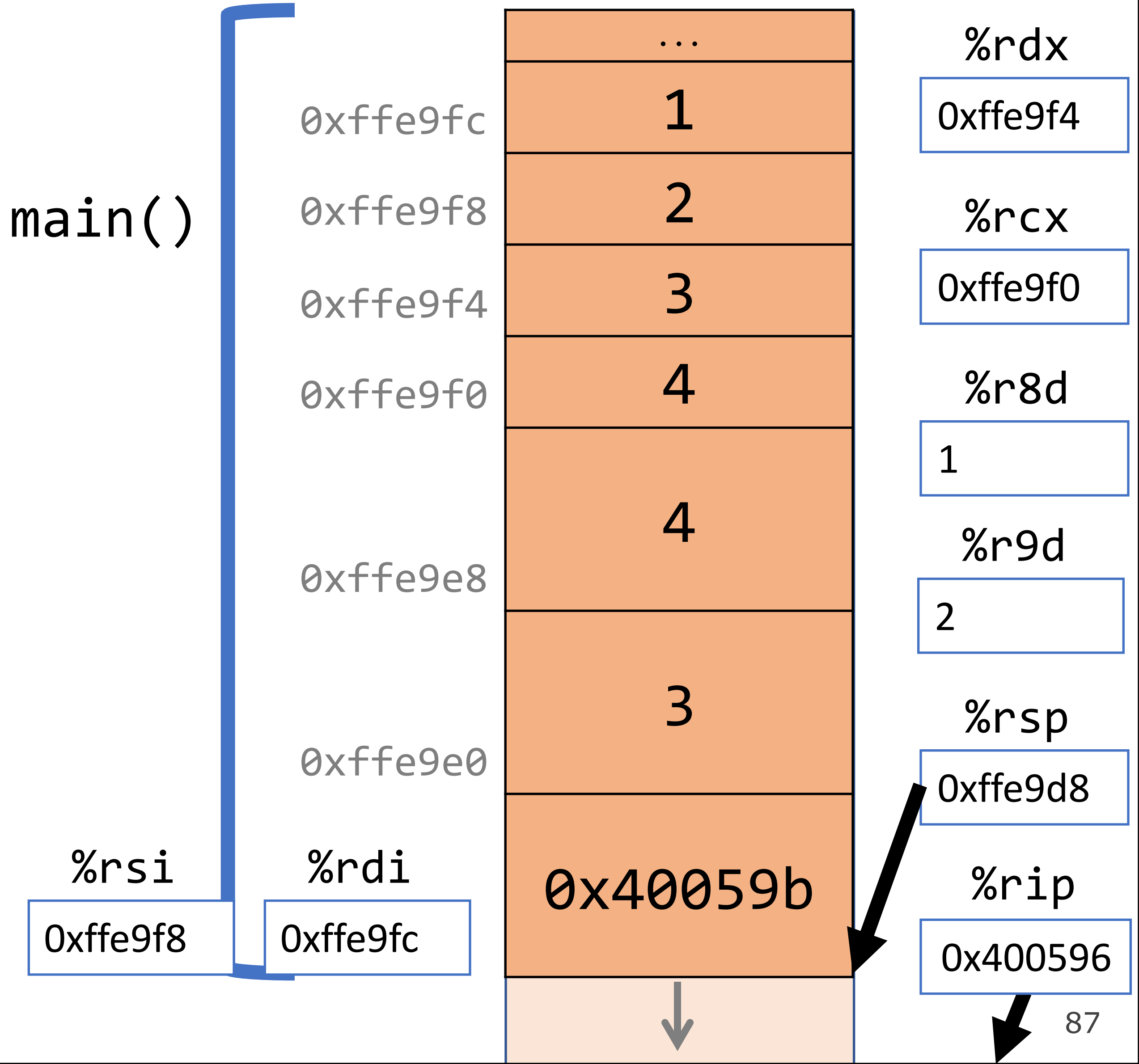


Parameters and Return

```
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x40058c <+61>:    lea    0x18(%rsp),%rsi
0x400591 <+66>:    lea    0x1c(%rsp),%rdi
0x400596 <+71>:    callq  0x400546 <func>
0x40059b <+76>:    add    $0x10,%rsp
…
```

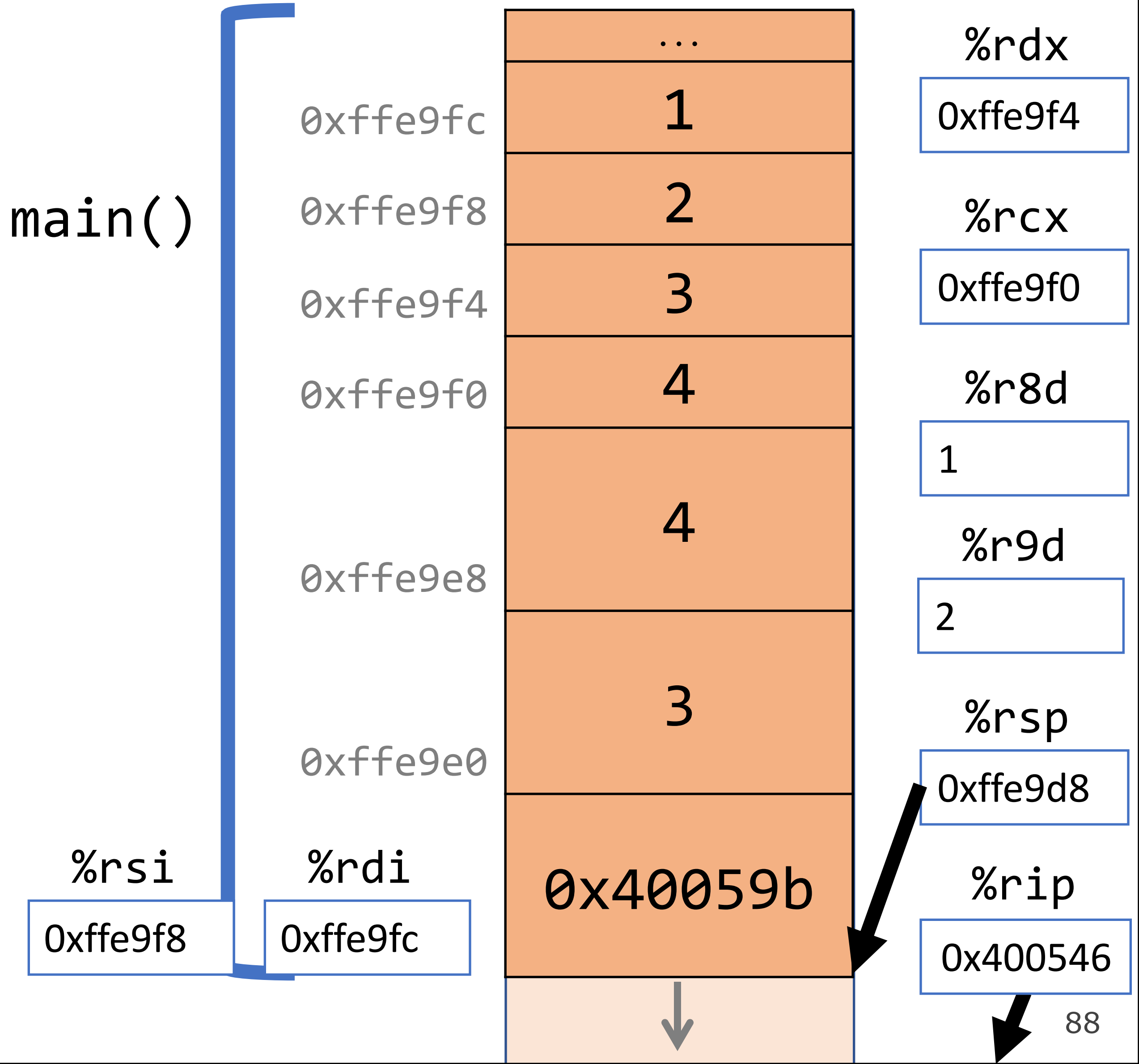


Parameters and Return

```c
int main(int argc, char *argv[]) {
    int i1 = 1;
    int i2 = 2;
    int i3 = 3;
    int i4 = 4;
    int result = func(&i1, &i2, &i3, &i4,
                      i1, i2, i3, i4);
    …
}

int func(int *p1, int *p2, int *p3, int *p4,
         int v1, int v2, int v3, int v4) {
    …
}
```

```
0x40058c <+61>:    lea    0x18(%rsp),%rsi
0x400591 <+66>:    lea    0x1c(%rsp),%rdi
0x400596 <+71>:    callq  0x400546 <func>
0x40059b <+76>:    add    $0x10,%rsp
…
```



Calling Functions In Assembly

To call a function in assembly, we must do a few things:

- **Pass Control** – %rip must be adjusted to execute the function being called and then resume the caller function afterwards.
- **Pass Data** – we must pass any parameters and receive any return value.
- **Manage Memory** – we must handle any space needs of the callee on the stack.

Terminology: **caller** function calls the **callee** function.

Plan For Today

- The Instruction Pointer (%rip)
- Calling Functions
  - The Stack
  - Passing Control
  - Passing Data
  - Local Storage
- **Break:** Announcements
- Register Restrictions
- Pulling it all together: recursion example

Local Storage

- So far, we've often seen local variables stored directly in registers, rather than on the stack as we'd expect. This is for optimization reasons.
- There are **three** common reasons that local data must be in memory:
  - We've run out of registers
  - The '&' operator is used on it, so we must generate an address for it
  - They are arrays or structs (need to use address arithmetic)

Local Storage

```c
 long swap_add(long *xp, long *yp) {
    long x = *xp;
    long y = *yp;
    *xp = y;
    *yp = x;
    return x + y;
}

long caller() {
    long arg1 = 534;
    long arg2 = 1057;
    long sum = swap_add(&arg1, &arg2);
    long diff = arg1 - arg2;
    return sum * diff;
}
```

```
caller:
    subq $16, %rsp          // 16 bytes for stack frame
    movq $534, (%rsp)       // store 534 in arg1
    movq $1057, 8(%rsp)     // store 1057 in arg2
    leaq 8(%rsp), %rsi      // compute &arg2 as second arg
    movq %rsp, %rdi         // compute &arg1 as first arg
    call swap_add           // call swap_add(&arg1, &arg2)
    movq (%rsp),%rdx        // get arg1
    subq 8(%rsp), %rdx      // compute diff = arg1 - arg2
    imulq %rdx, %rax        // compute sum * diff
    addq $16, %rsp          // deallocate stack frame
    ret                     // return and restore %rip
```

Plan For Today

- The Instruction Pointer (%rip)
- Calling Functions
  - The Stack
  - Passing Control
  - Passing Data
  - Local Storage
- **Break:** Announcements
- Register Restrictions
- Pulling it all together: recursion example

Plan For Today

- No lecture Friday
- None! Let's take a breather ☺

Plan For Today

- The Instruction Pointer (%rip)
- Calling Functions
  - The Stack
  - Passing Control
  - Passing Data
  - Local Storage
- **Break:** Announcements
- Register Restrictions
- Pulling it all together: recursion example

Register Restrictions

- There is only one copy of registers for all programs and instructions.
- Therefore, there are some rules that callers and callees must follow when using registers so they do not interfere with one another.
- There are two types of registers: **caller-owned** and **callee-owned**

Register Restrictions

Caller Owned

- If a callee wants to use this, they must *save* the existing value and *restore* it back into the register after they are done.
- If a caller wants to use this, they can store values there during function calls and can assume that the values will be preserved.

Callee-Owned

- If a callee wants to use this, they can do so without worrying about overwriting data. They do not need to save the existing value.
- If a caller wants to use this, they must be careful when calling a function, as that function may overwrite the contents! They may want to *save* the existing value and *restore* it back into the register after the function call.

Register Restrictions

```
long P(long x, long y) {
    long u = Q(y);
    long v = Q(x);
    return u + v;
}
```

long P(long x, long y), x in %rdi, y in %rsi:

```
push %rbp
push %rbx
mov %rdi,%rbp
mov %rsi,%rdi
callq 40056d <Q(long)>
mov %rax,%rbx
mov %rbp,%rdi
callq 40056d <Q(long)>
add %rbx,%rax
pop %rbx
pop %rbp
retq
```

Register Restrictions

```
long P(long x, long y) {
    long u = Q(y);
    long v = Q(x);
    return u + v;
}
```

long P(long x, long y), x in %rdi, y in %rsi:

```
push %rbp
push %rbx
mov %rdi,%rbp
mov %rsi,%rdi
callq 40056d <Q(long)>
mov %rax,%rbx
mov %rbp,%rdi
callq 40056d <Q(long)>
add %rbx,%rax
pop %rbx
pop %rbp
retq
```

Register Restrictions

```
long P(long x, long y) {
    long u = Q(y);
    long v = Q(x);
    return u + v;
}
```

long P(long x, long y), x in %rdi, y in %rsi:

```
push %rbp
push %rbx
mov %rdi,%rbp
mov %rsi,%rdi
callq 40056d <Q(long)>
mov %rax,%rbx
mov %rbp,%rdi
callq 40056d <Q(long)>
add %rbx,%rax
pop %rbx
pop %rbp
retq
```

Plan For Today

- The Instruction Pointer (%rip)
- Calling Functions
  - The Stack
  - Passing Control
  - Passing Data
  - Local Storage
- **Break:** Announcements
- Register Restrictions
- Pulling it all together: recursion example

Example: Recursion

- Let's take a look at an example of recursion at the assembly level.
- We'll put to use everything we've learned about registers, the stack, function calls, parameters, and assembly instructions!
- We'll also see how helpful GDB can be when tracing through assembly.

Recap

- The Instruction Pointer (%rip)
- Calling Functions
  - The Stack
  - Passing Control
  - Passing Data
  - Local Storage
- **Break:** Announcements
- Register Restrictions
- Pulling it all together: recursion example

That's it for assembly! **Next time:** managing the heap