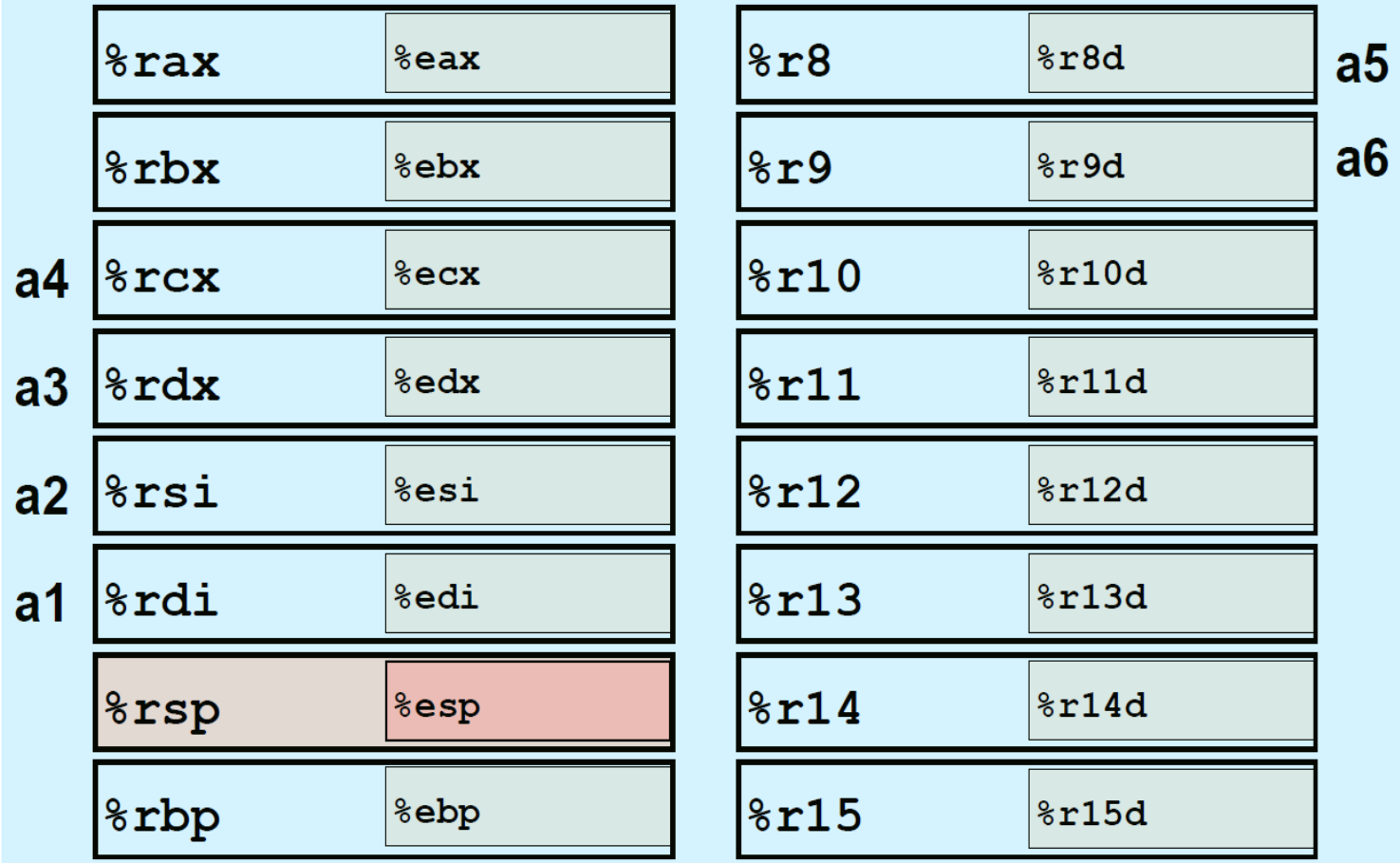
Week2

x86-64 General-Purpose Registers



– Extend existing registers to 64 bits. Add 8 new ones.

32-bit code for swap

```
void swap(int *xp, int *yp)
{
  int t0 = *xp;
  int t1 = *yp;
  *xp = t1;
  *yp = t0;
}
```

```
swap:
   pushl  %ebp
   movl   %esp,%ebp
   pushl  %ebx

   movl   8(%ebp), %edx
   movl   12(%ebp), %ecx
   movl   (%edx), %ebx
   movl   (%ecx), %eax
   movl   %eax, (%edx)
   movl   %ebx, (%ecx)

   popl   %ebx
   popl   %ebp
   ret
```

Set Up

Body

Finish

64-bit code for swap

```
void swap(int *xp, int *yp)
{
  int t0 = *xp;
  int t1 = *yp;
  *xp = t1;
  *yp = t0;
}
```

```
swap:
                                    } Set Up
   movl   (%rdi), %edx
   movl   (%rsi), %eax
   movl   %eax, (%rdi)              } Body
   movl   %edx, (%rsi)
                                    } Finish
   ret
```

Object Code

```
int sum(int a, int b) {
    return(a+b);
}
```

```
<sum>:
        55          push   %ebp
        89 e5       mov    %esp,%ebp
        8b 45 0c    mov    0xc(%ebp),%eax
        03 45 08    add    0x8(%ebp),%eax
        5d          pop    %ebp
        c3          ret
```

Code for `sum`

```
0x401040 <sum>:
    0x55
    0x89
    0xe5
    0x8b
    0x45
    0x0c
    0x03
    0x45
    0x08
    0x5d
    0xc3
```

- Total of 11 bytes
- Each instruction: 1, 2, or 3 bytes
- Starts at address `0x401040`

Disassembling Object Code

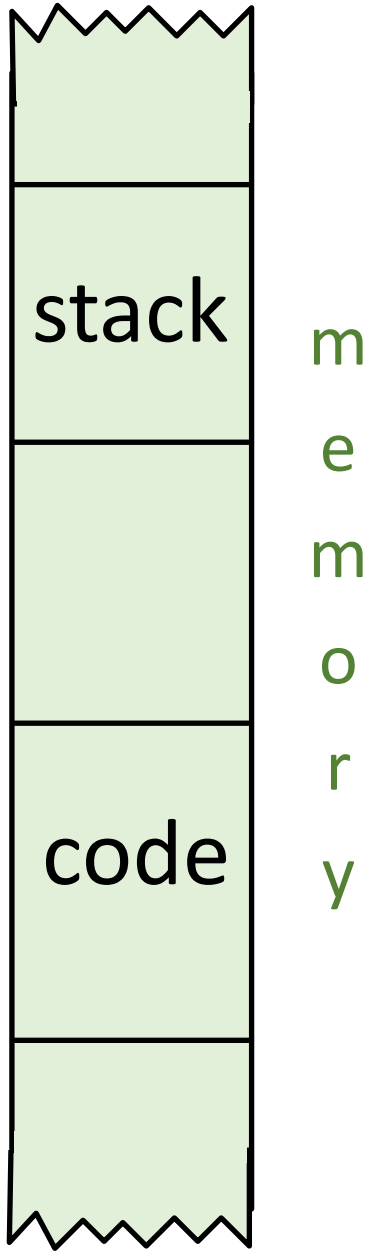
- **Disassembler**
  - **`objdump -d <file>`**
    - **useful tool for examining object code**
    - **can be run on either executable or object (.o) file**

Today

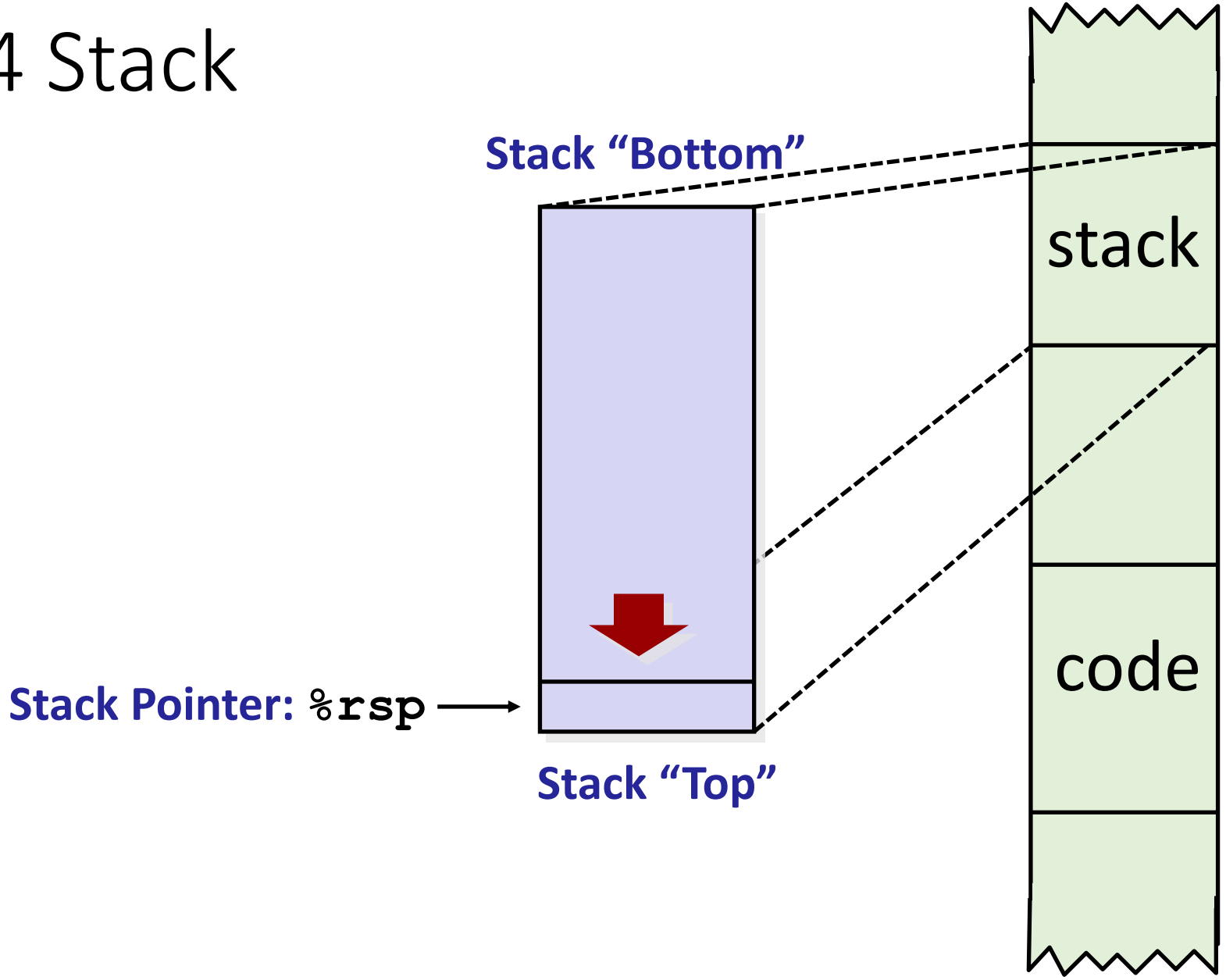
- Procedures
  - **Mechanisms**
  - **Stack Structure**
  - **Calling Conventions**
    - **Passing control**
    - **Passing data**
    - **Managing local data**
  - **Illustration of Recursion**

x86-64 Stack

- Region of memory managed with stack discipline
  - Memory viewed as array of bytes.
  - Different regions have different purposes.

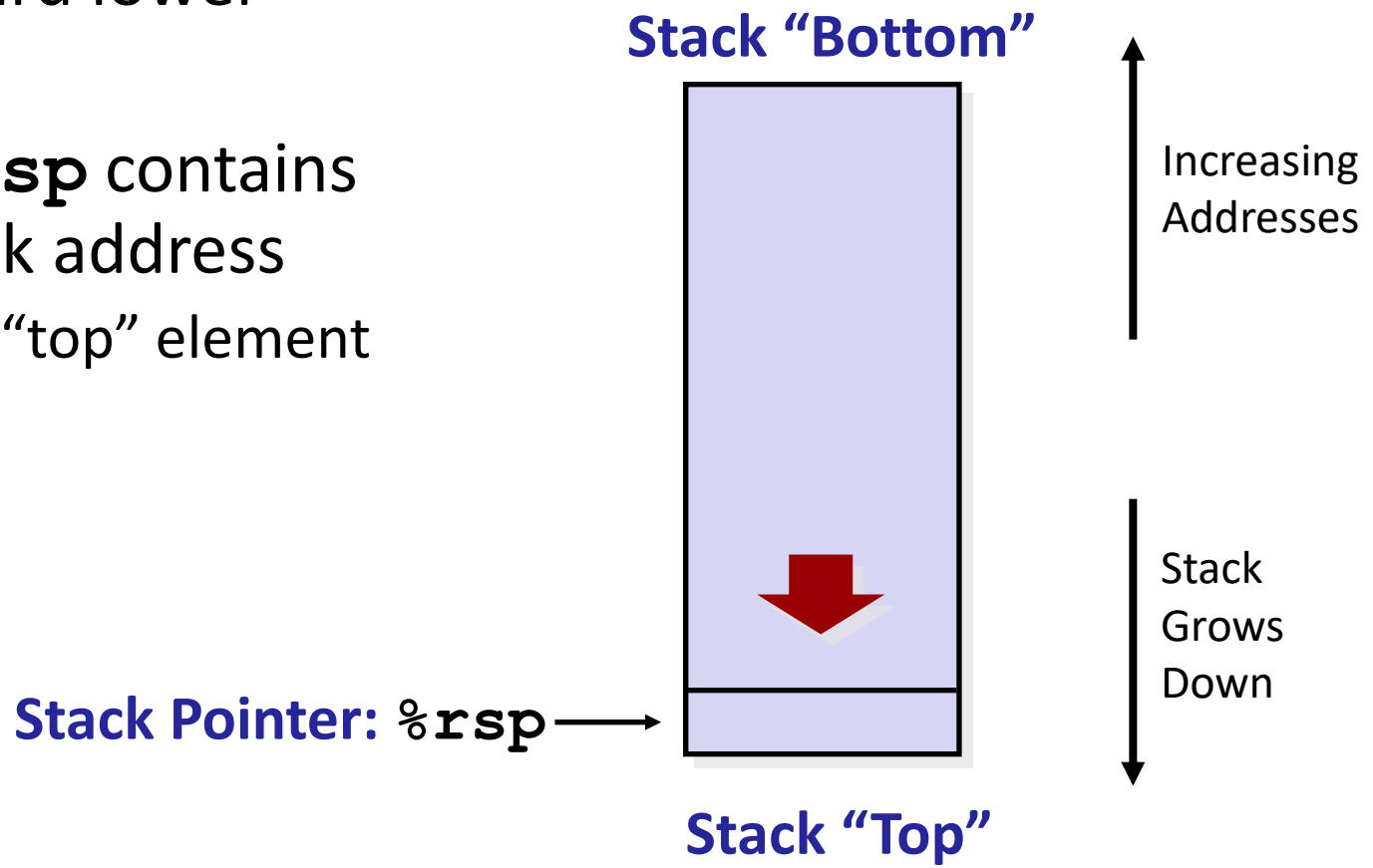


x86-64 Stack



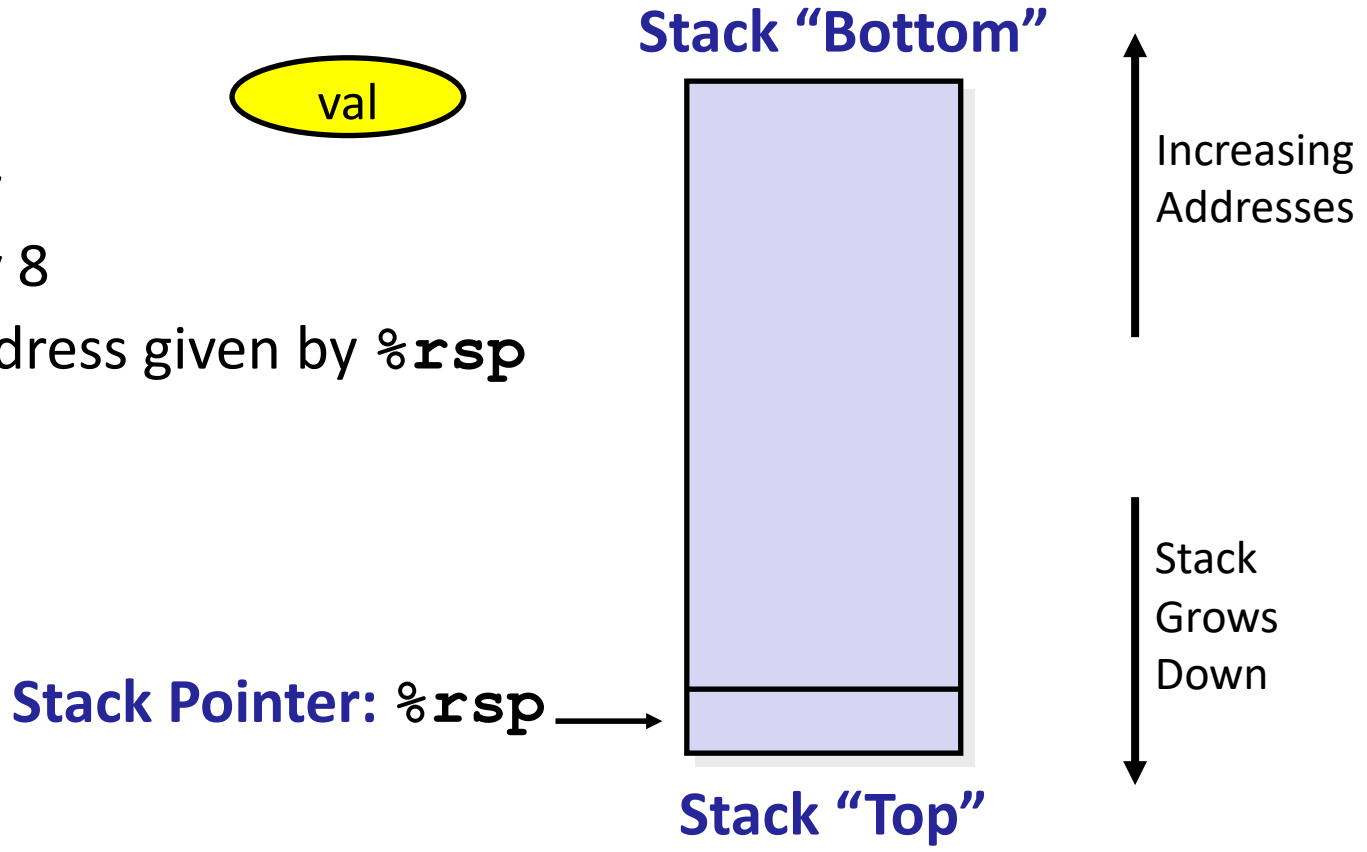
x86-64 Stack

- Grows toward lower addresses
- Register `%rsp` contains lowest stack address
  - address of "top" element



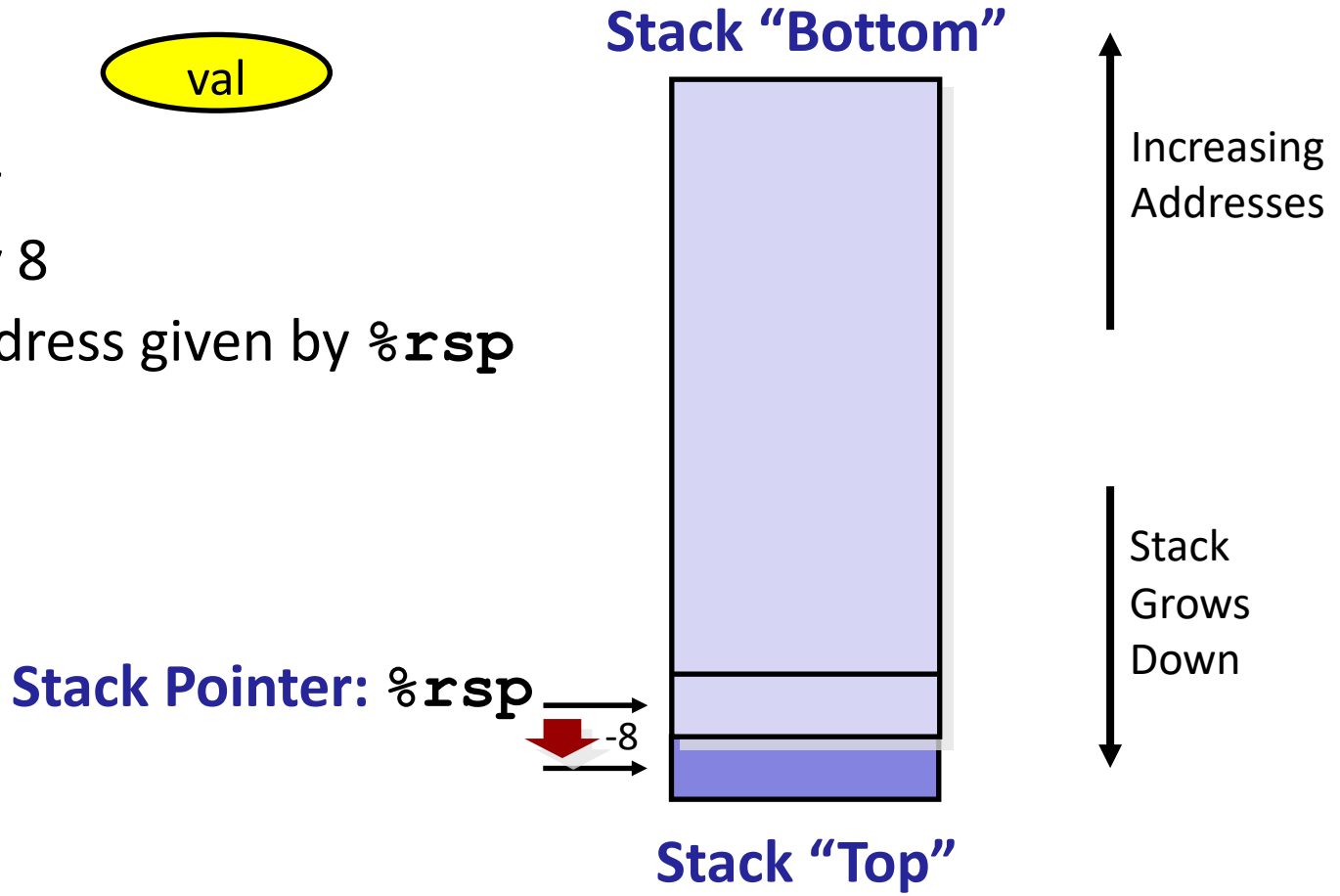
x86-64 Stack: Push

- **`pushq` *Src***
  - Fetch operand at *Src*
  - Decrement **`%rsp`** by 8
  - Write operand at address given by **`%rsp`**



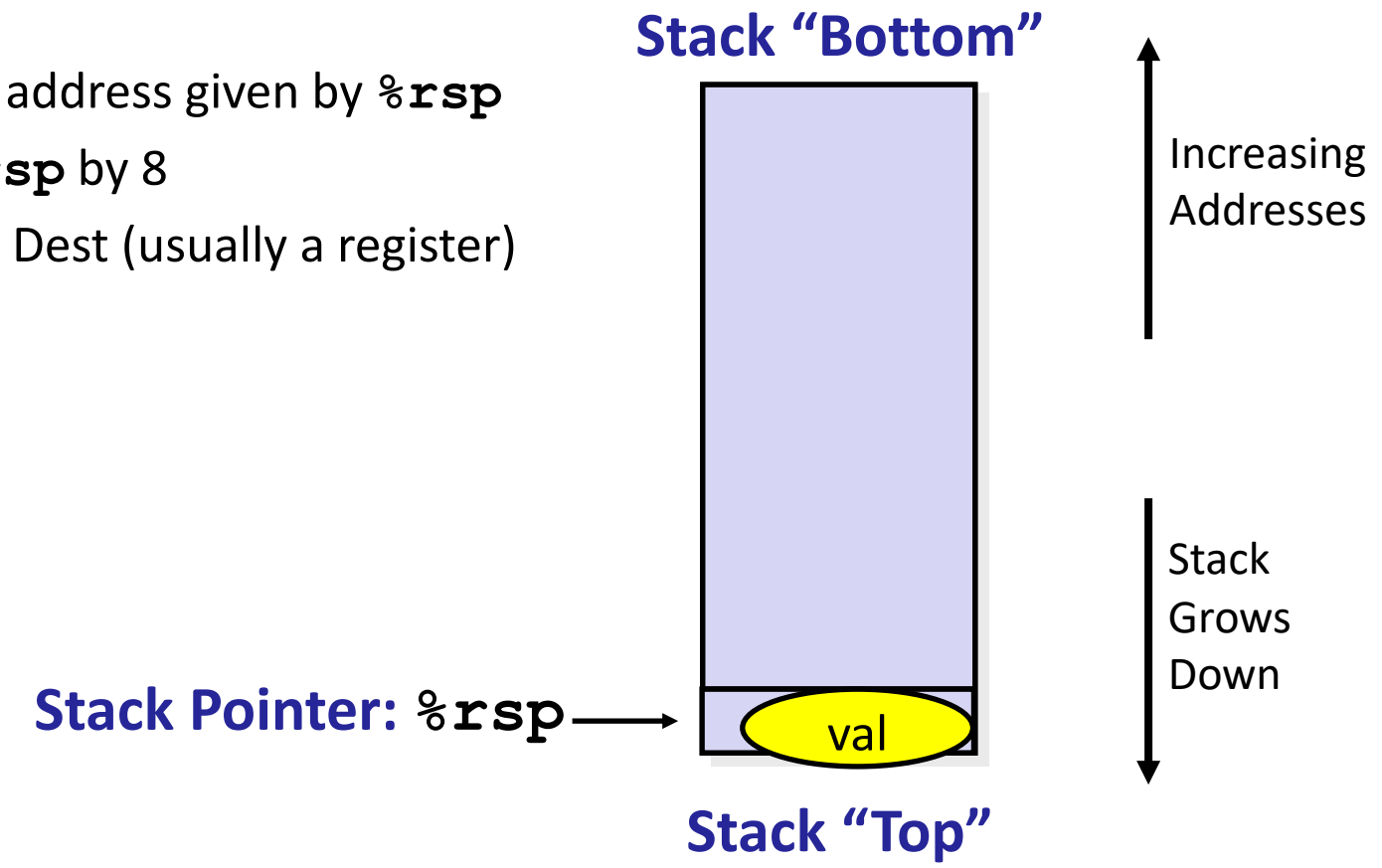
x86-64 Stack: Push

- **`pushq` *Src***
  - Fetch operand at *Src*
  - Decrement **`%rsp`** by 8
  - Write operand at address given by **`%rsp`**



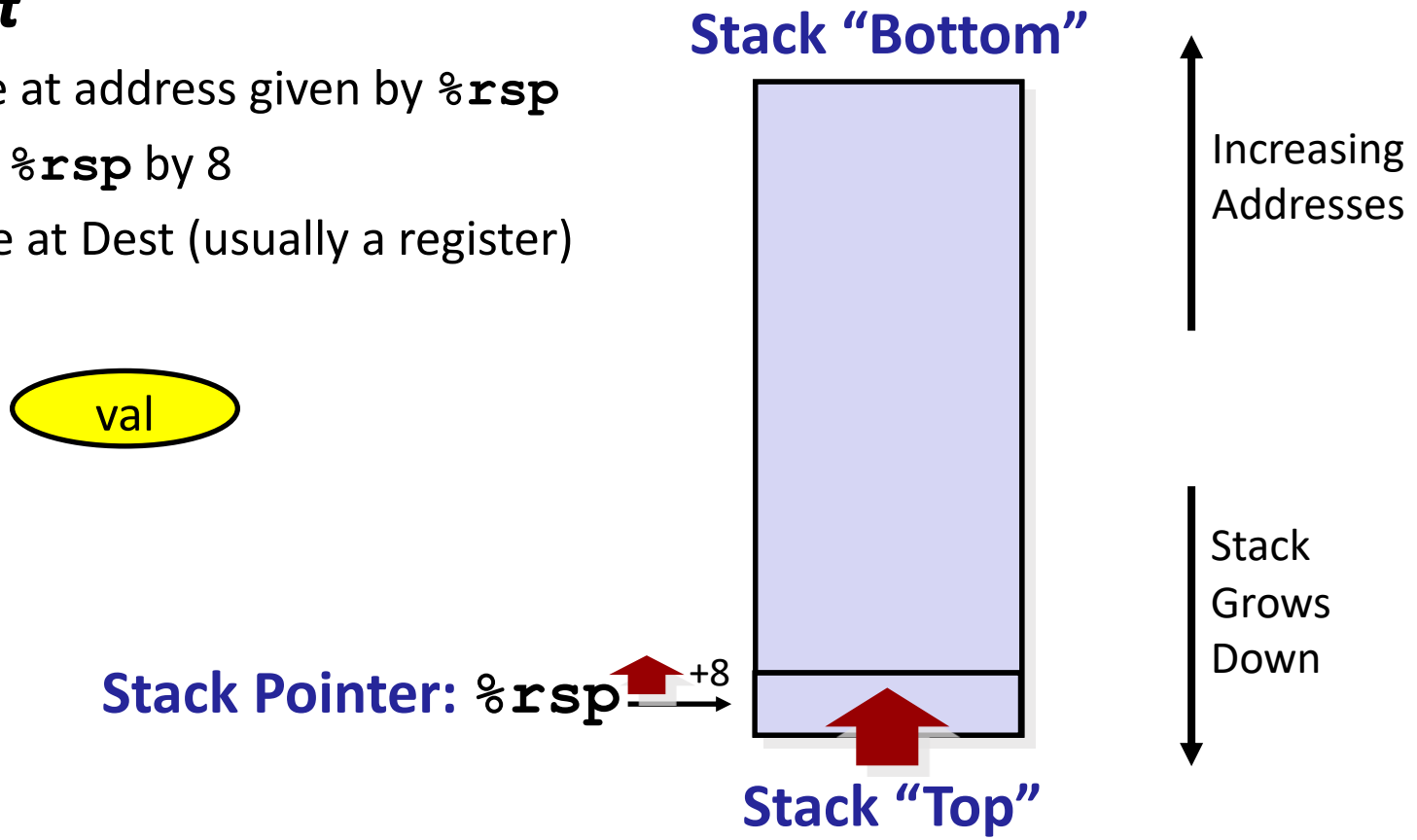
x86-64 Stack: Pop

- **`popq` *Dest***
  - Read value at address given by **`%rsp`**
  - Increment **`%rsp`** by 8
  - Store value at Dest (usually a register)



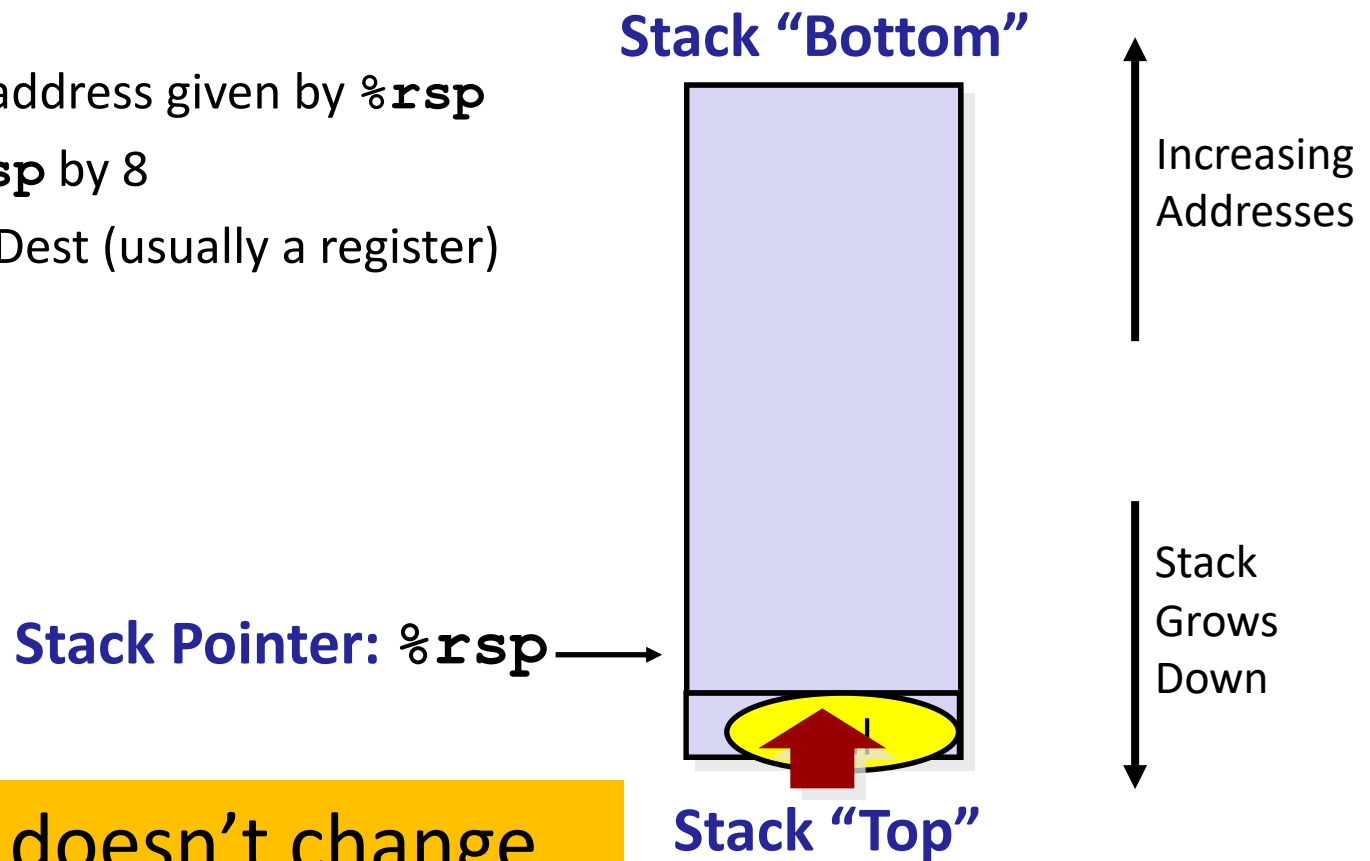
x86-64 Stack: Pop

- **`popq` *Dest***
  - Read value at address given by **`%rsp`**
  - Increment **`%rsp`** by 8
  - Store value at Dest (usually a register)



x86-64 Stack: Pop

- **`popq` *Dest***
  - Read value at address given by **`%rsp`**
  - Increment **`%rsp`** by 8
  - Store value at Dest (usually a register)



(The memory doesn't change, only the value of **`%rsp`**)

Today

- Procedures
  - **Mechanisms**
  - **Stack Structure**
  - **Calling Conventions**
    - **Passing control**
    - **Passing data**
    - **Managing local data**
  - **Illustration of Recursion**

Code Examples

```
void multstore(long x, long y, long *dest)
{
    long t = mult2(x, y);
    *dest = t;
}
```

```
0000000000400540 <multstore>:
  400540: push   %rbx                # Save %rbx
  400541: mov    %rdx,%rbx           # Save dest
  400544: callq  400550 <mult2>      # mult2(x,y)
  400549: mov    %rax,(%rbx)         # Save at dest
  40054c: pop    %rbx                # Restore %rbx
  40054d: retq                       # Return
```

```
long mult2(long a, long b)
{
  long s = a * b;
  return s;
}
```

```
0000000000400550 <mult2>:
  400550:  mov    %rdi,%rax          # a
  400553:  imul   %rsi,%rax          # a * b
  400557:  retq                      # Return
```

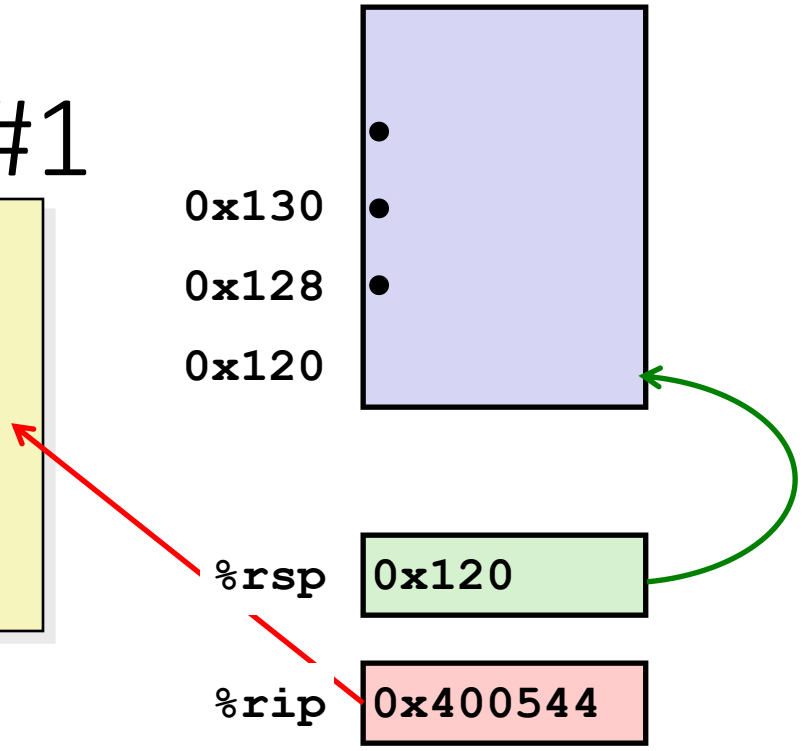
Procedure Control Flow

- Use stack to support procedure call and return
- Procedure call: **`call label`**
  - Push return address on stack
  - Jump to ***label***
- Return address:
  - Address of the next instruction right after call
- Procedure return: **`ret`**
  - Pop address from stack
  - Jump to address

Control Flow Example #1

```
0000000000400540 <multstore>:
  •
  •
  400544: callq  400550 <mult2>
  400549: mov    %rax,(%rbx)
  •
  •
```

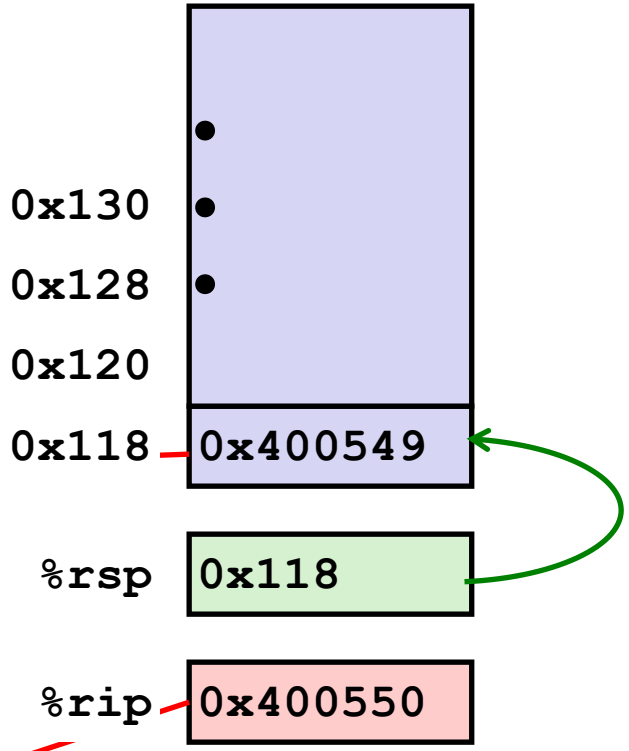
```
0000000000400550 <mult2>:
  400550:  mov    %rdi,%rax
  •
  •
  400557:  retq
```



Control Flow Example #2

```
0000000000400540 <multstore>:
  •
  •
  400544: callq  400550 <mult2>
  400549: mov    %rax,(%rbx)
  •
  •
  •
```

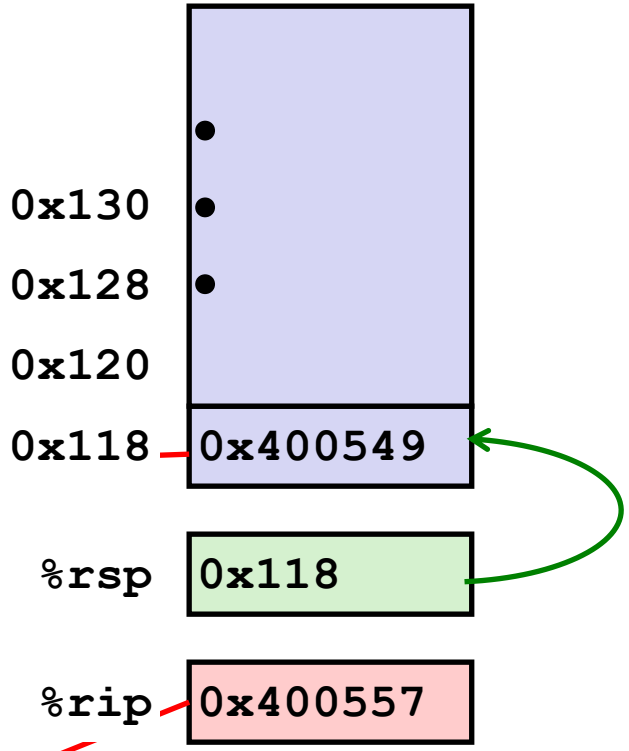
```
0000000000400550 <mult2>:
  400550:  mov    %rdi,%rax
  •
  •
  400557:  retq
```



Control Flow Example #3

```
0000000000400540 <multstore>:
  •
  •
  400544: callq  400550 <mult2>
  400549: mov    %rax,(%rbx)
  •
  •
  •
```

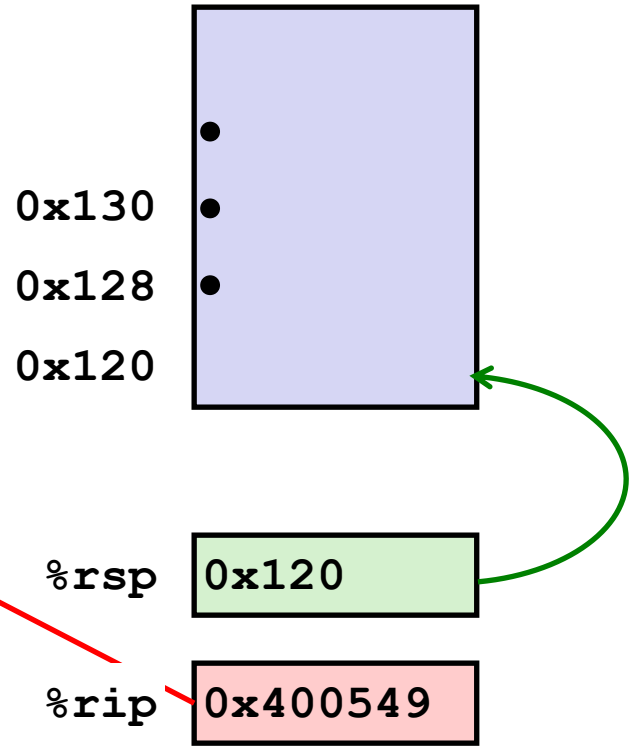
```
0000000000400550 <mult2>:
  400550:  mov    %rdi,%rax
  •
  •
  400557:  retq
```



Control Flow Example #4

```
0000000000400540 <multstore>:
  •
  •
  400544: callq  400550 <mult2>
  400549: mov    %rax,(%rbx)
  •
  •
```

```
0000000000400550 <mult2>:
  400550:  mov    %rdi,%rax
  •
  •
  400557:  retq
```



Today

- Procedures
  - **Mechanisms**
  - **tack Structure**
  - **Calling Conventions**
    - **Passing control**
    - **Passing data**
    - **Managing local data**
  - **Illustrations of Recursion & Pointers**

Procedure Data Flow

Registers

- First 6 arguments

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

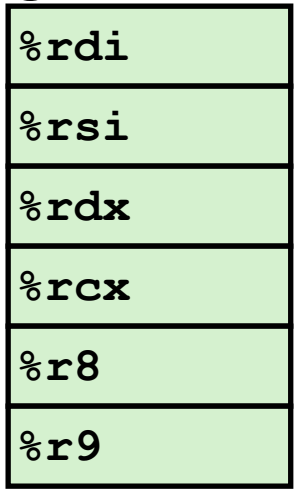
- Return value

`%rax`

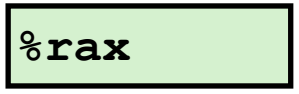
Procedure Data Flow

Registers

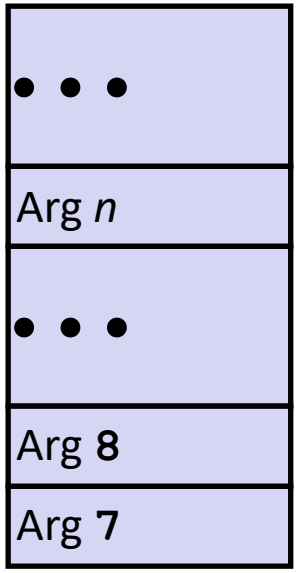
- First 6 arguments



- Return value



Stack



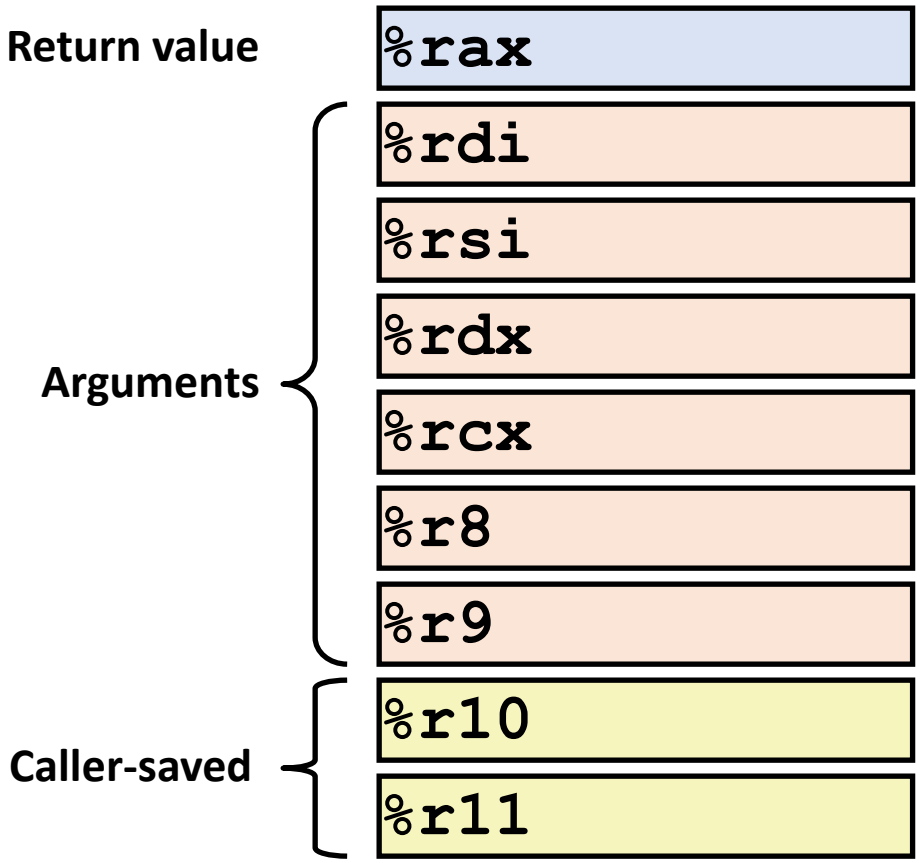
- Only allocate stack space when needed

Register Saving Conventions

- Conventions
  - ***"Caller Saved"***
    - Caller saves temporary values in its frame before the call
      - push %rax
    - Caller restores them in its frame after the call
      - pop %rax
  - ***"Callee Saved"***
    - Callee saves temporary values in its frame before using
    - Callee restores them before returning to caller

x86-64 Linux Register Usage #1

- **`%rax`**
  - Return value
  - Also caller-saved
  - Can be modified by procedure
- **`%rdi`**, …, **`%r9`**
  - Arguments
  - Also caller-saved
  - Can be modified by procedure
- **`%r10`**, **`%r11`**
  - Caller-saved
  - Can be modified by procedure



x86-64 Linux Register Usage #2

- **`%rbx`**, **`%r12`**, **`%r13`**, **`%r14`**
  - Callee-saved
  - Callee must save & restore
- **`%rbp`**
  - Callee-saved
  - Callee must save & restore
  - May be used as frame pointer
- **`%rsp`**
  - Special form of callee save
  - Restored to original value upon exit from procedure