CS208

W, 18 Feb 2026

What do call + ret do

```
main
  :
0x401401  call f
0x401406  movl %eax, (%rsp)

---

0x404108  f:  push %rbx
              sub 0x20, %rsp
                :
              add 0x20, %rsp
              pop %rbx
0x405888      ret
```

Before call

rip | 0x401401

rsp | 0x7ff3458

After call

rip | 0x404108

rsp | 0x7ff3450

AND top of the stack has 0x401406

What do call + ret do

```
main
  :
0x401401  call f
0x401406  movl %eax, (%rsp)

---

0x404108  f:  push %rbx
              sub 0x20, %rsp
                :
              add 0x20, %rsp
              pop %rbx
0x405888      ret
```

Before ret

rip 0x405888

rsp 0x7ff3450

Top of stack has 0x401406 ret addr

After ret

rip 0x401406

rsp 0x7ff3458

Top of stack is just main's stack frame

call: push return address
jump ← (i.e. set rip)

ret: pop return address
into rip (i.e. jump back)