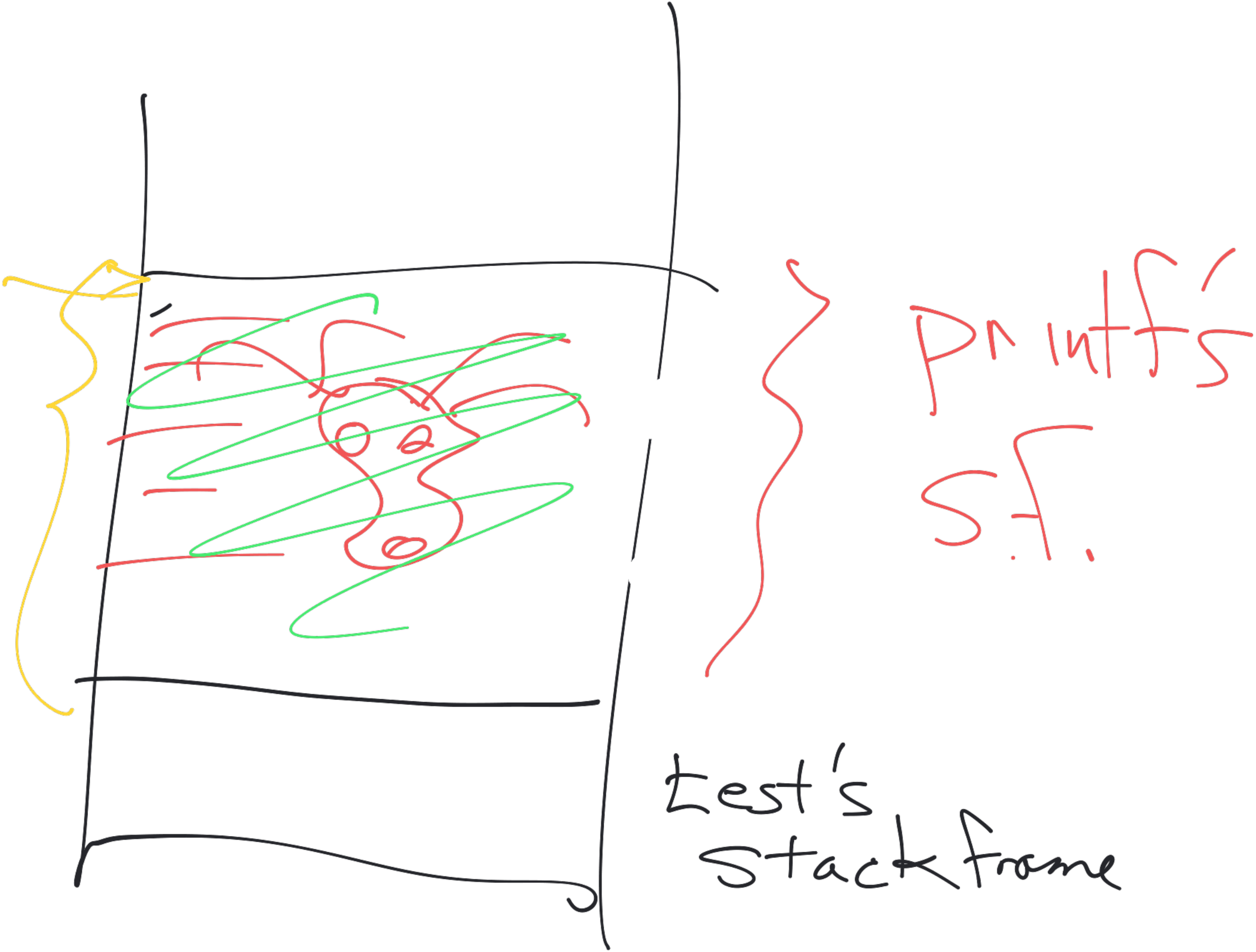
CS 208

Wed

2 March 2022


printf's
S.F.
test's
stackframe

0x28

0x28

getInt

test

Call a function

- Put parameters where the fn expects them
  (common: rdi, rsi, ..)
  (too big? stack)
- callq
  - pushes return addr on stack
  - rsp = rsp - 8
  - jump to function

Function f just got called

- subtract from rsp to make stack frame for local vars
- push regs f plans to use, so we can save their values

Return from function

- pop the used registers so orig values are back
- add to rsp to "tear down" the stack frame
- put return value where the caller expects it (commonly: rax)
- retq — pop return addr (rsp = rsp + 8) + jump there