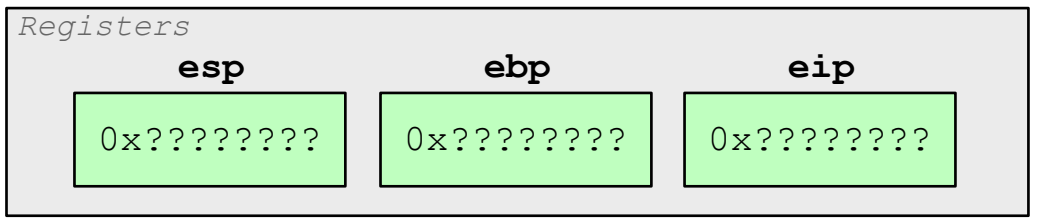
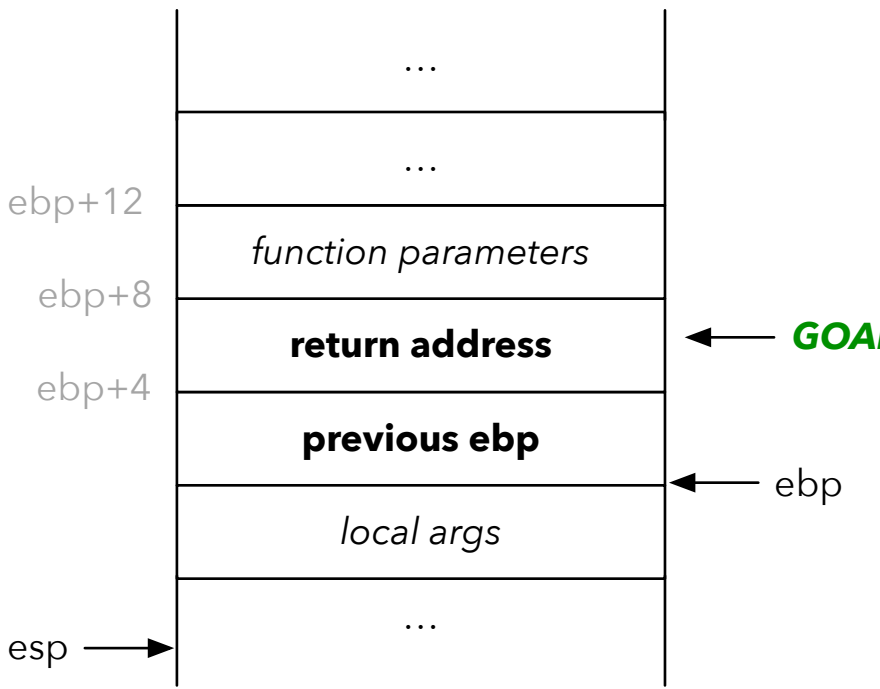
[Step 0]
The anatomy of a stack frame (high-level)

Assumes 32-bit system



← ***interesting registers…***
esp = stack pointer
ebp = frame pointer
eip = instruction pointer *(a.k.a. "program counter" or "pc")*



GOAL: *Overwrite return address – jump to arbitray code (e.g., code in libc)*