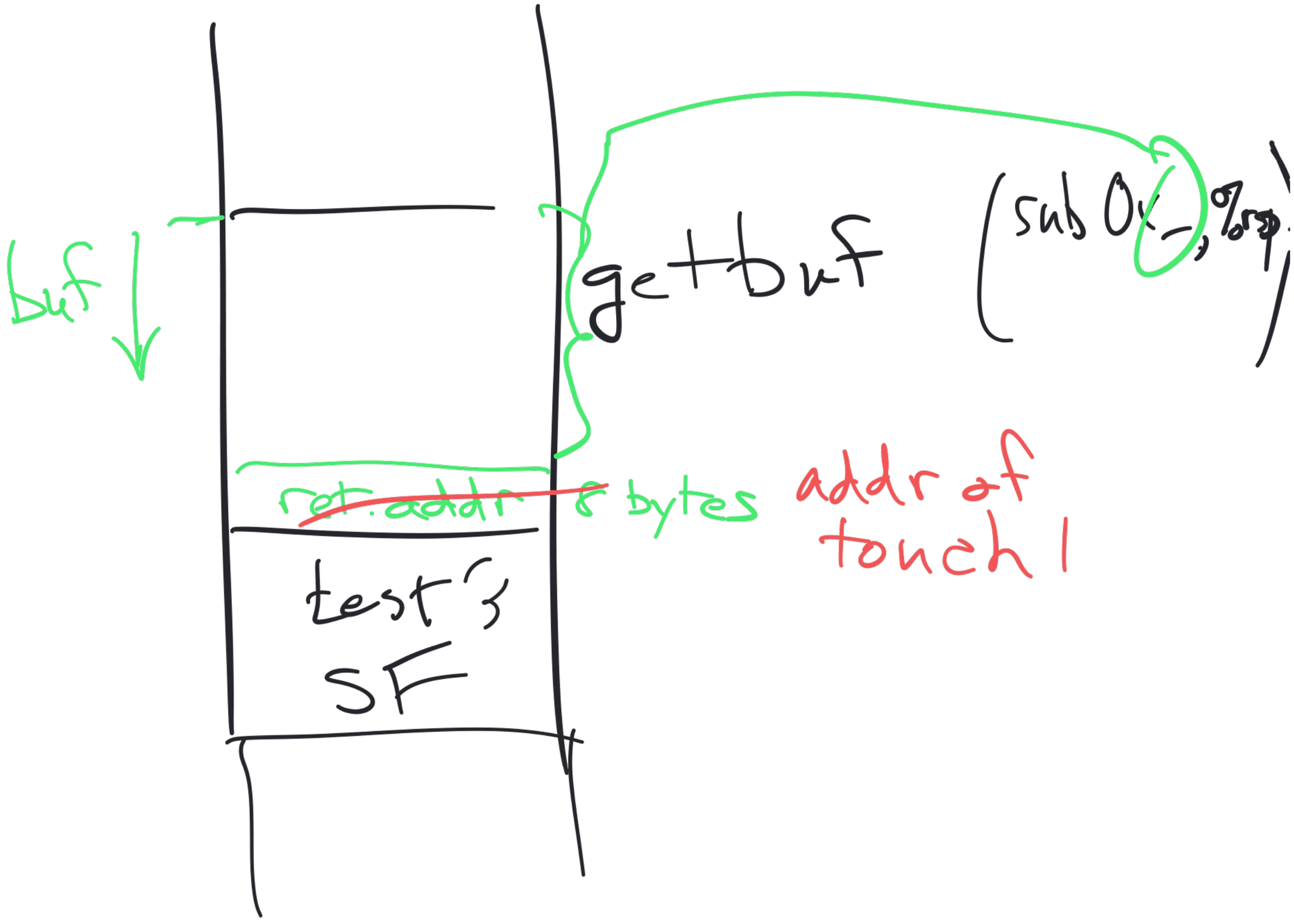
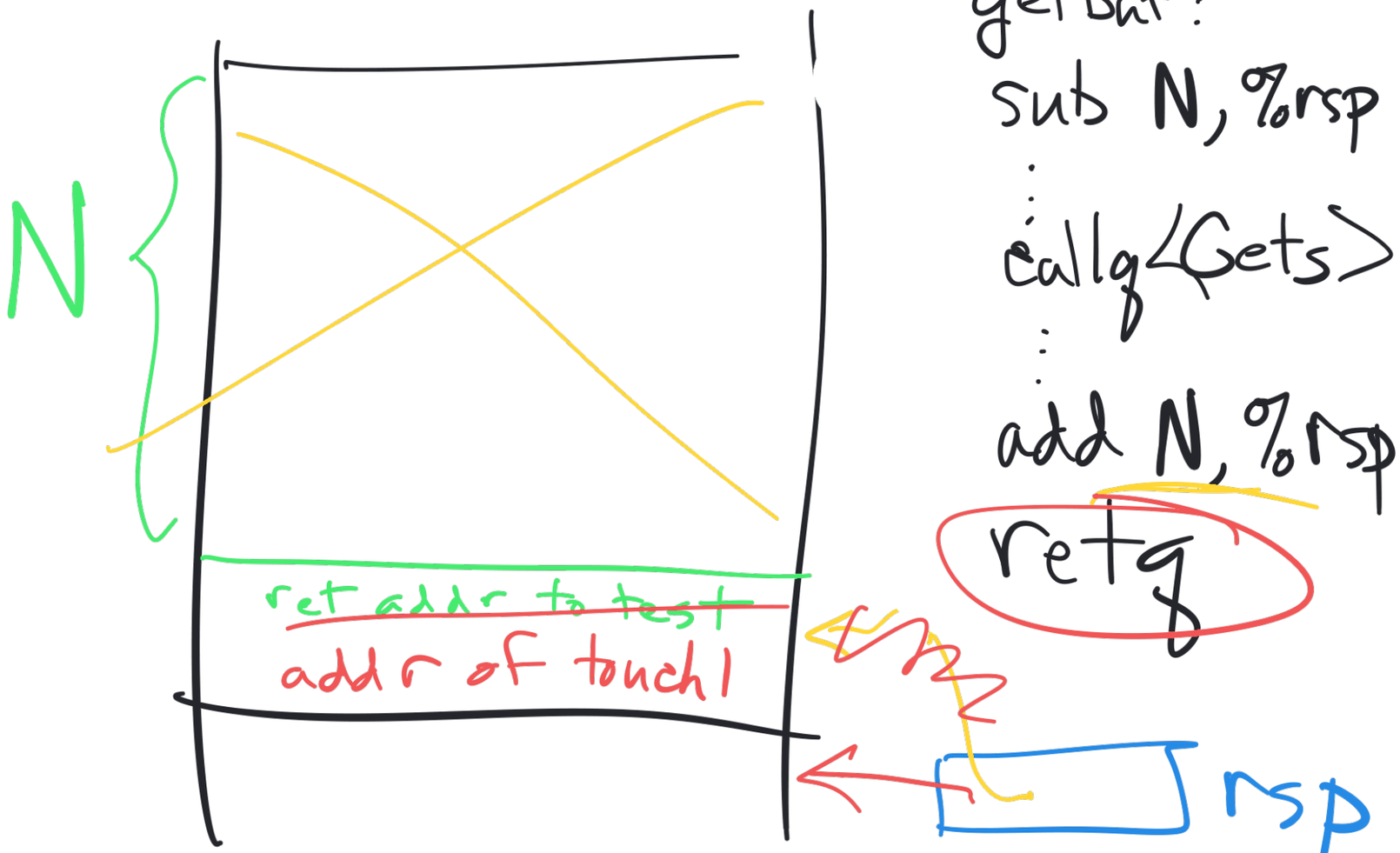
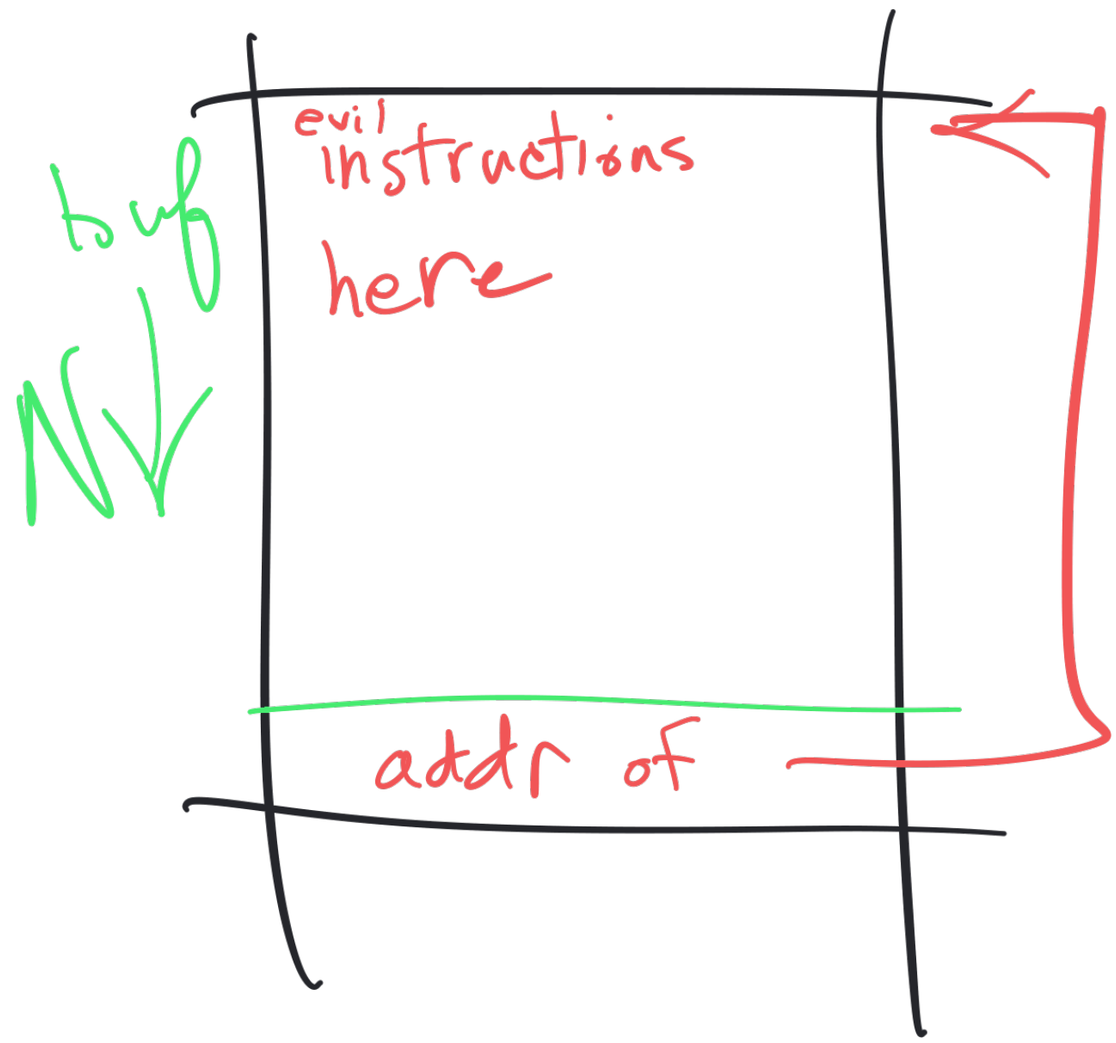
# CS 208

Mon, 27 Feb 2023


buf
getbuf
(sub 0x_, %rsp)
ret. addr
8 bytes
addr of touch1
test's
SF



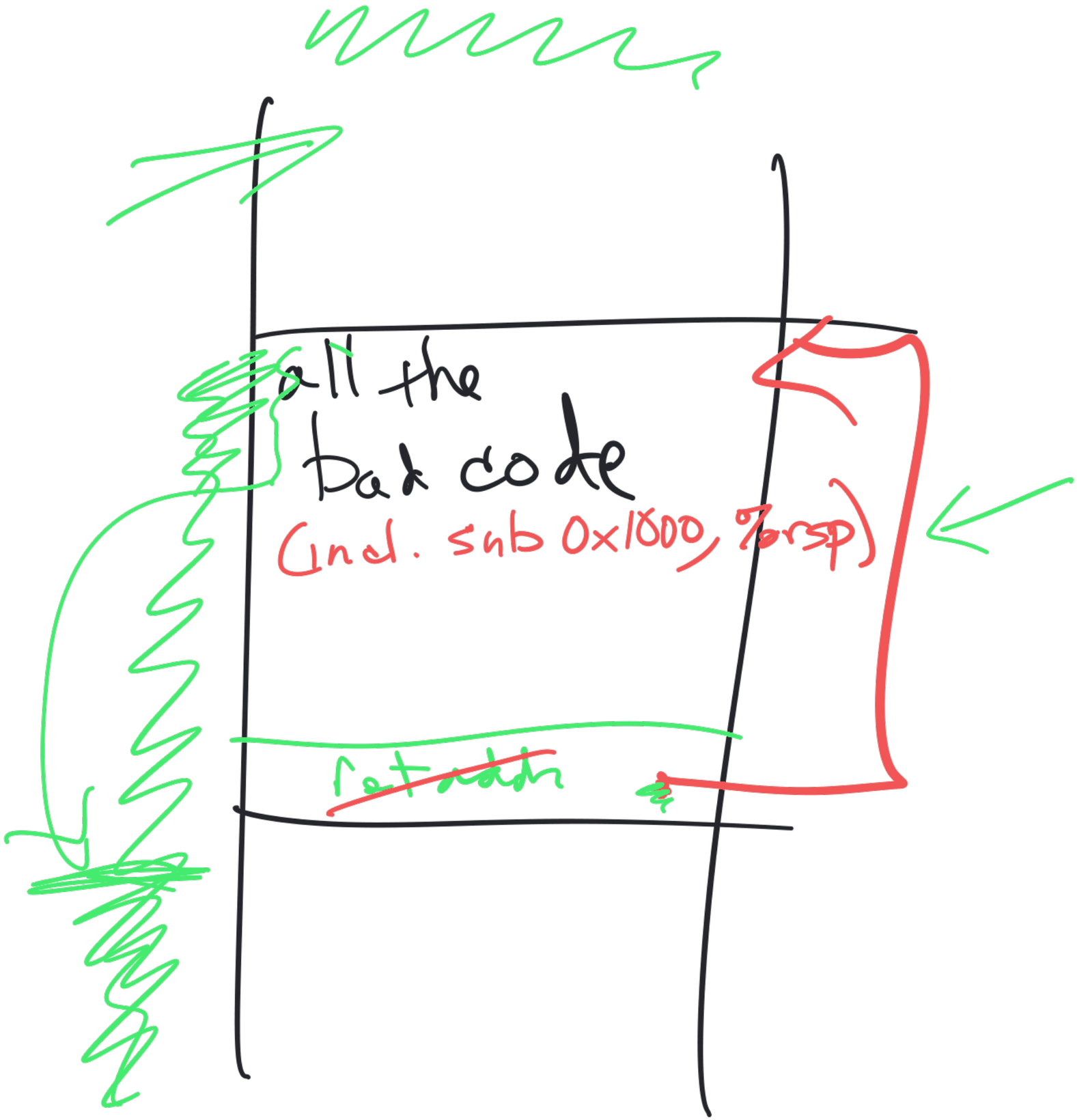

retq ① Grab 8-byte address rsp is pointing to
② Jmp there
③ Add 8 to rsp




Useful technique in evil instructions

① push target address

② retq


all the
bad code
(ind. sub 0x1000, %rsp)
ret addr