

CS 208

Wed, 18 Oct 2023

#3  $\text{function1}(\overset{\text{rdi}}{*a}, \overset{\text{rsi}}{*b})$   
 is a NULL? b?

testq %rdi, %rdi

sete %al



ZF = 1 if rdi == 0  
 = 0 otherwise

if prev. result == 0 (ie. ZF=1)

Set %al = 1

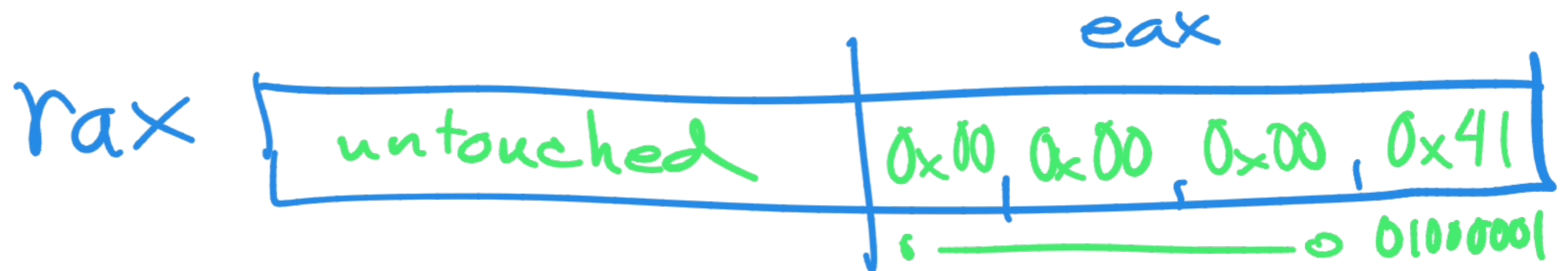
al = { if (a == 0) al = 1  
 else al = 0 } OR { if (b == 0) al = 1  
 else al = 0 }

function (char \*a, char \*b)

if (a == NULL || b == NULL)  
 bail.

mov z bl ← dest is 4 bytes  
move a byte

mov z bl \$0x41, %eax



fill the rest of the  
dest w/ 0's

movzbl (%rsi), %eax

rsi contains an address

go to that address, +

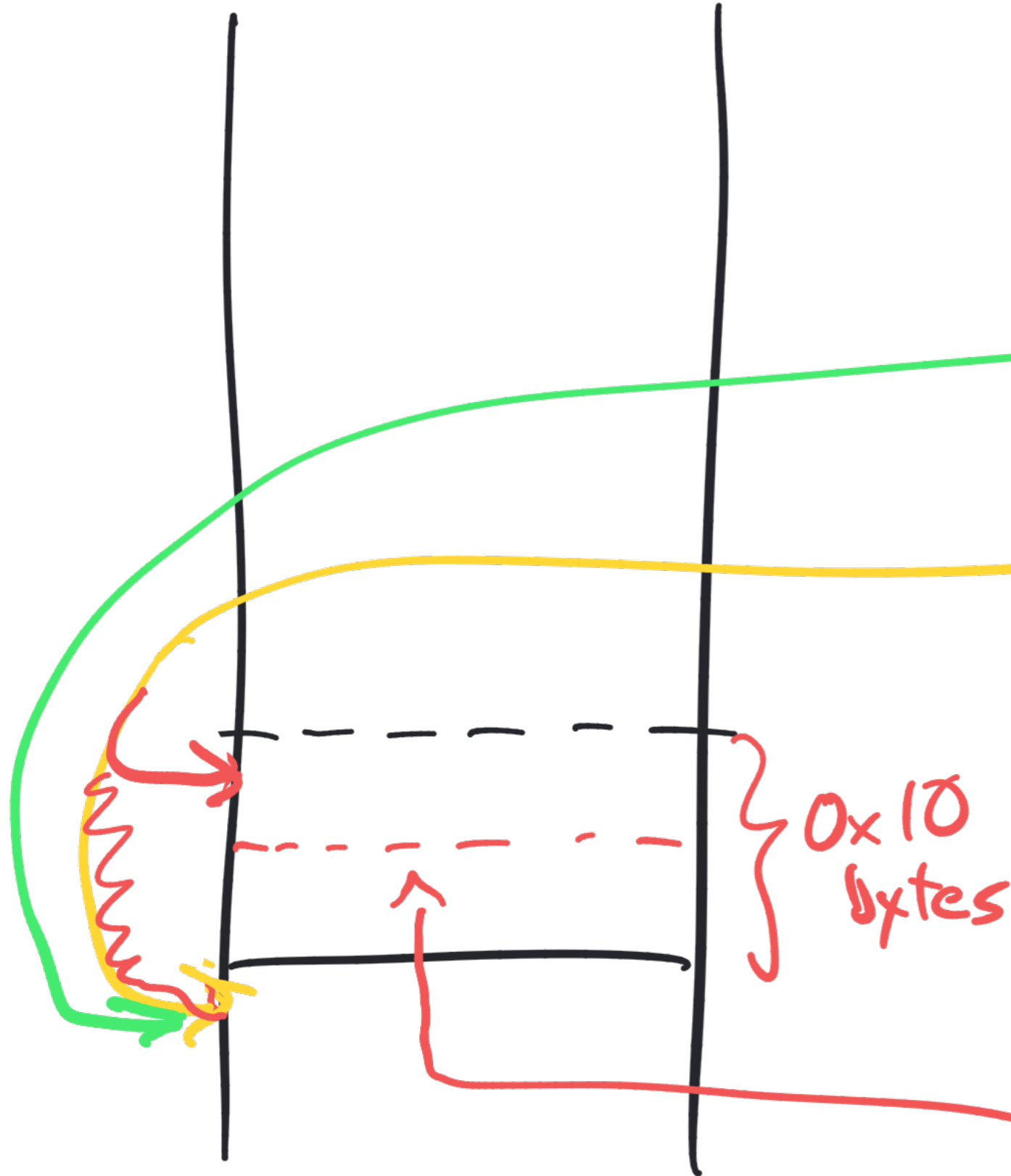
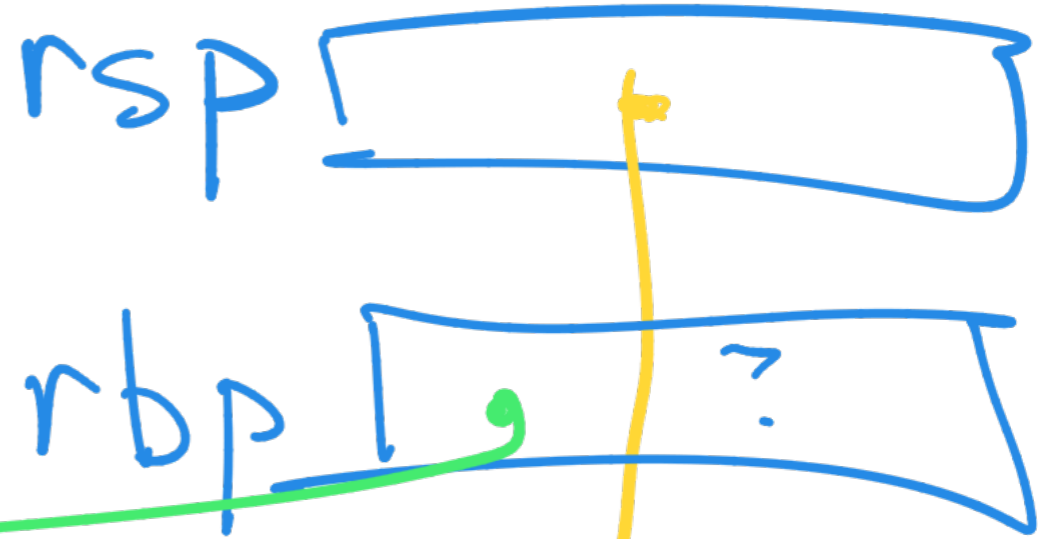
grab 1 byte

do the movzbl thing

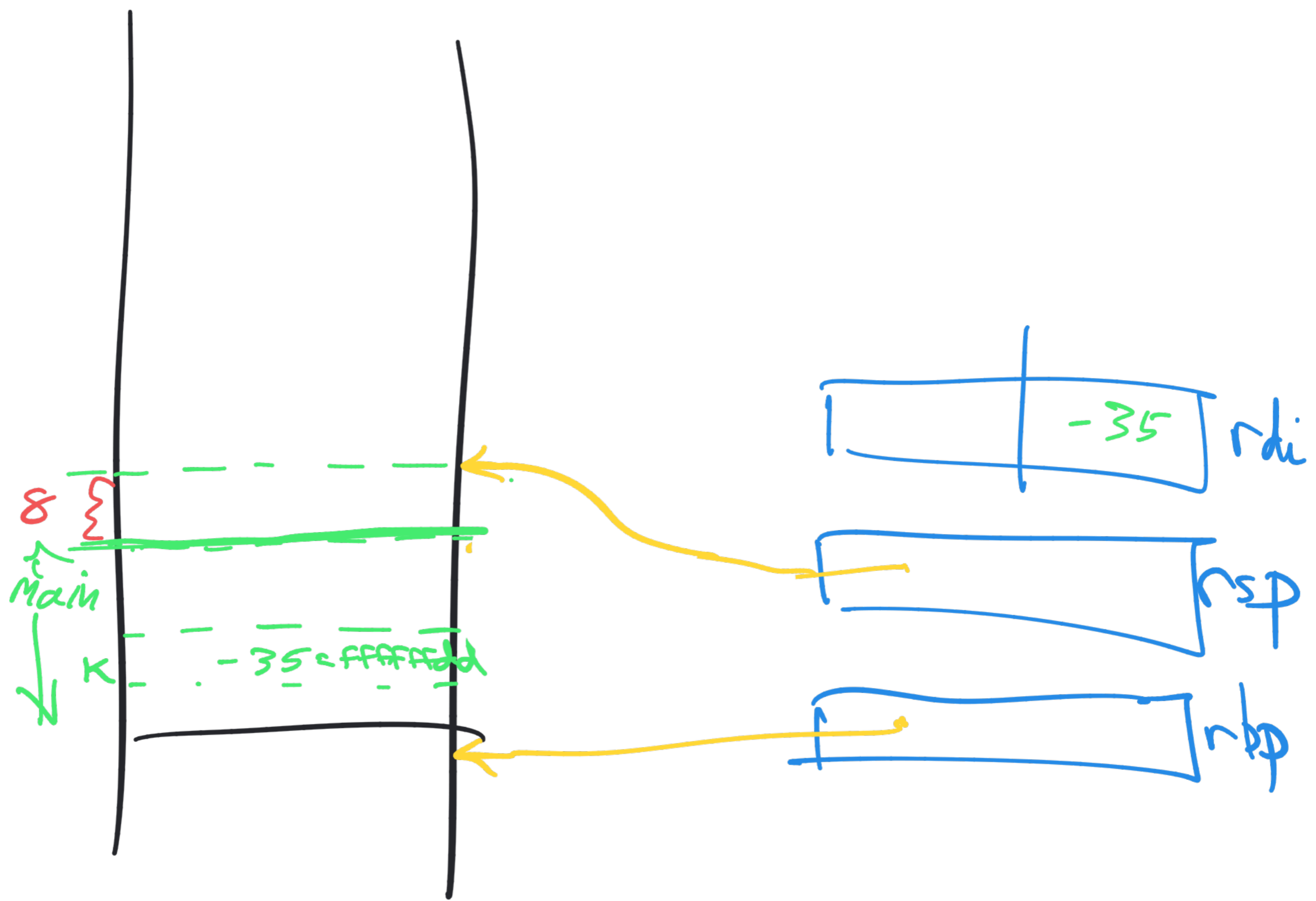
w/ that byte

Mem

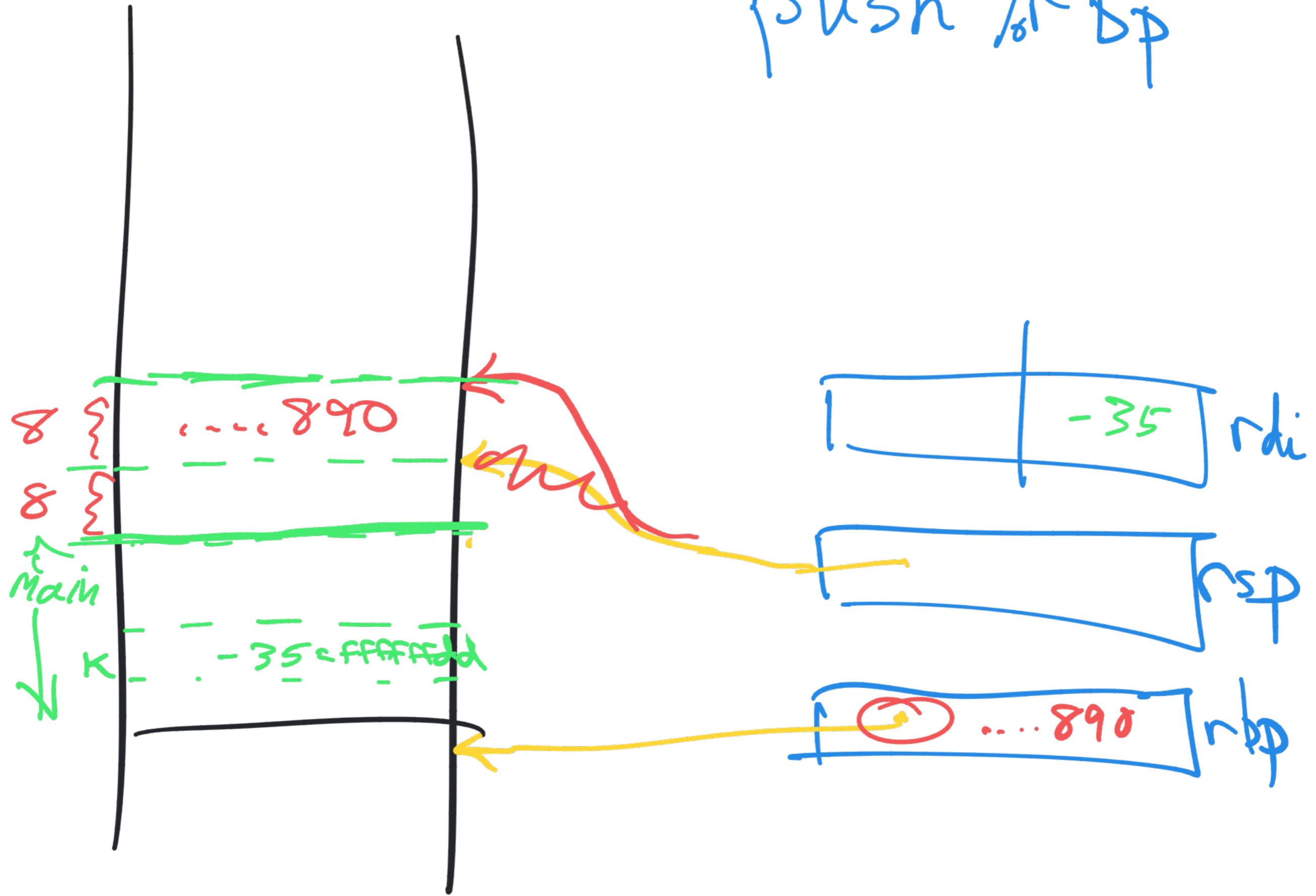
"stack pointer"



```
mov %rbp, %rsp  
sub $0x10, %rsp  
mov -35, [-8(%rbp)]
```



push  $\uparrow$  bp





push %rbp  
mov %rsp, %rbp

