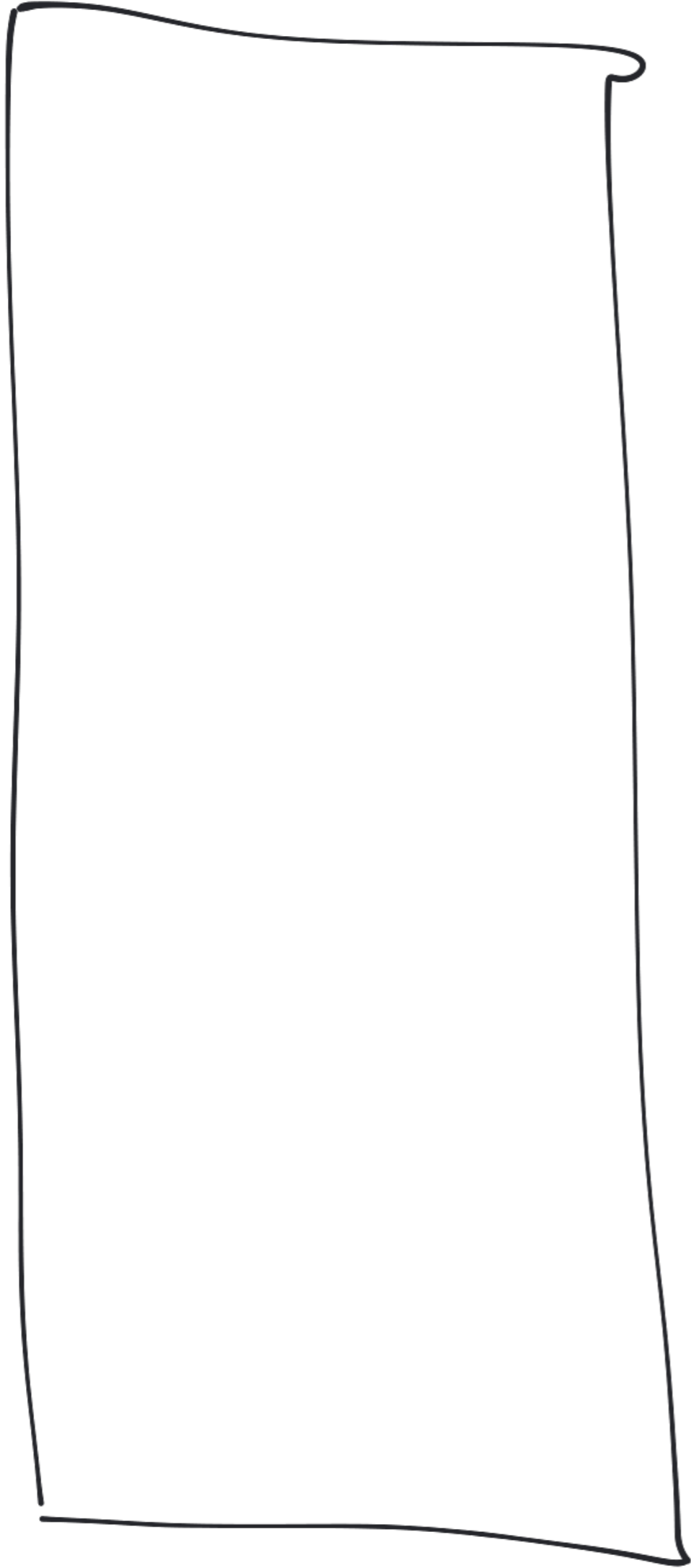


CS 2008

Wednesday

26 Jan 2022

0



$2^{64} - 1$

Where are
my local vars?

Where is my
code?

malloc'd mem?

"Hello"

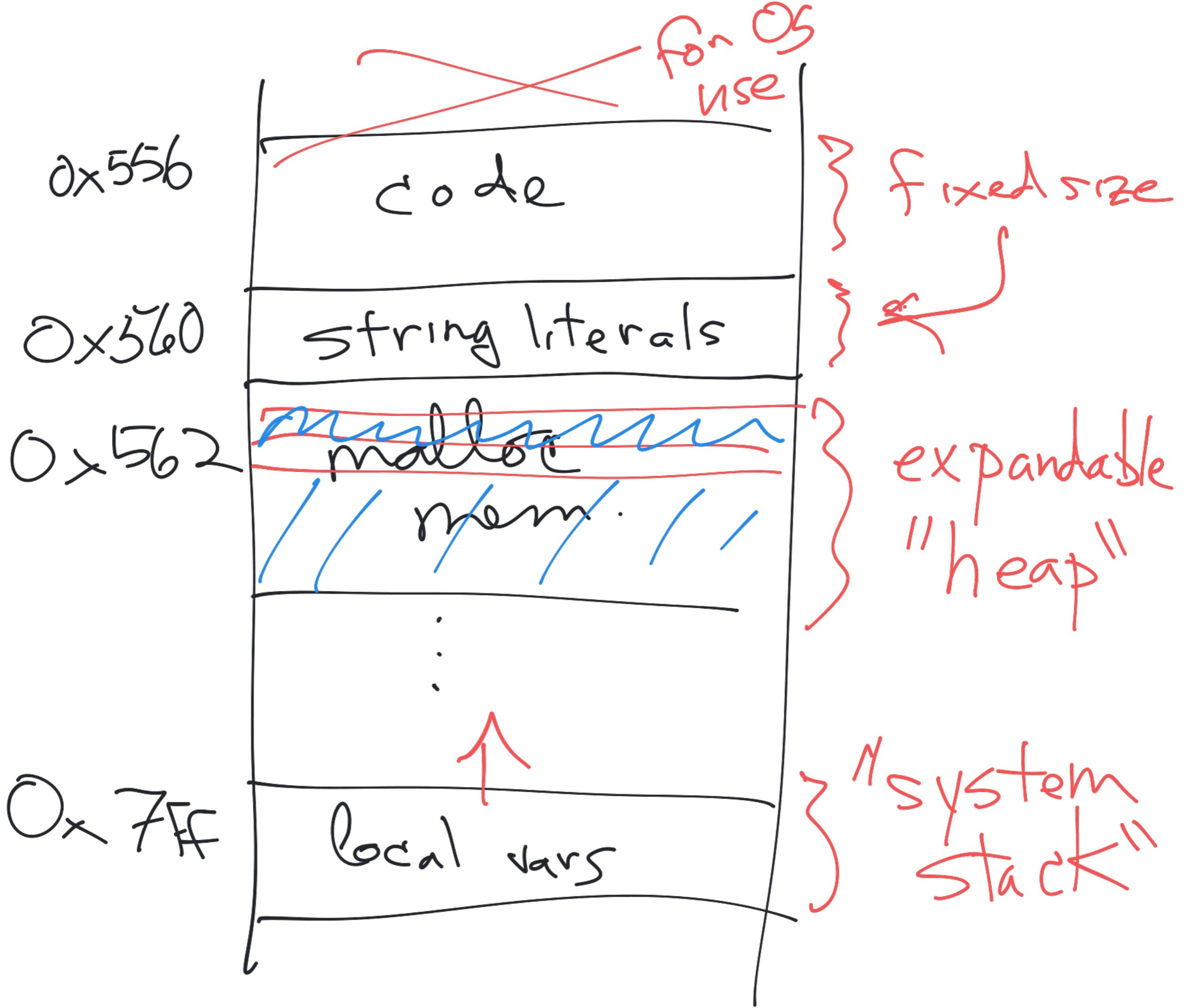
local vars: $0x7ffcd\dots$ (48 bits)

functions: $0x556\dots$
 $0x559\dots$
 $558\dots$
 564

"Hello" — $0x55f$ —
 557

$0x07fe$

malloc — $0x558$
 560
 562



int main() {

f(a,b);

}

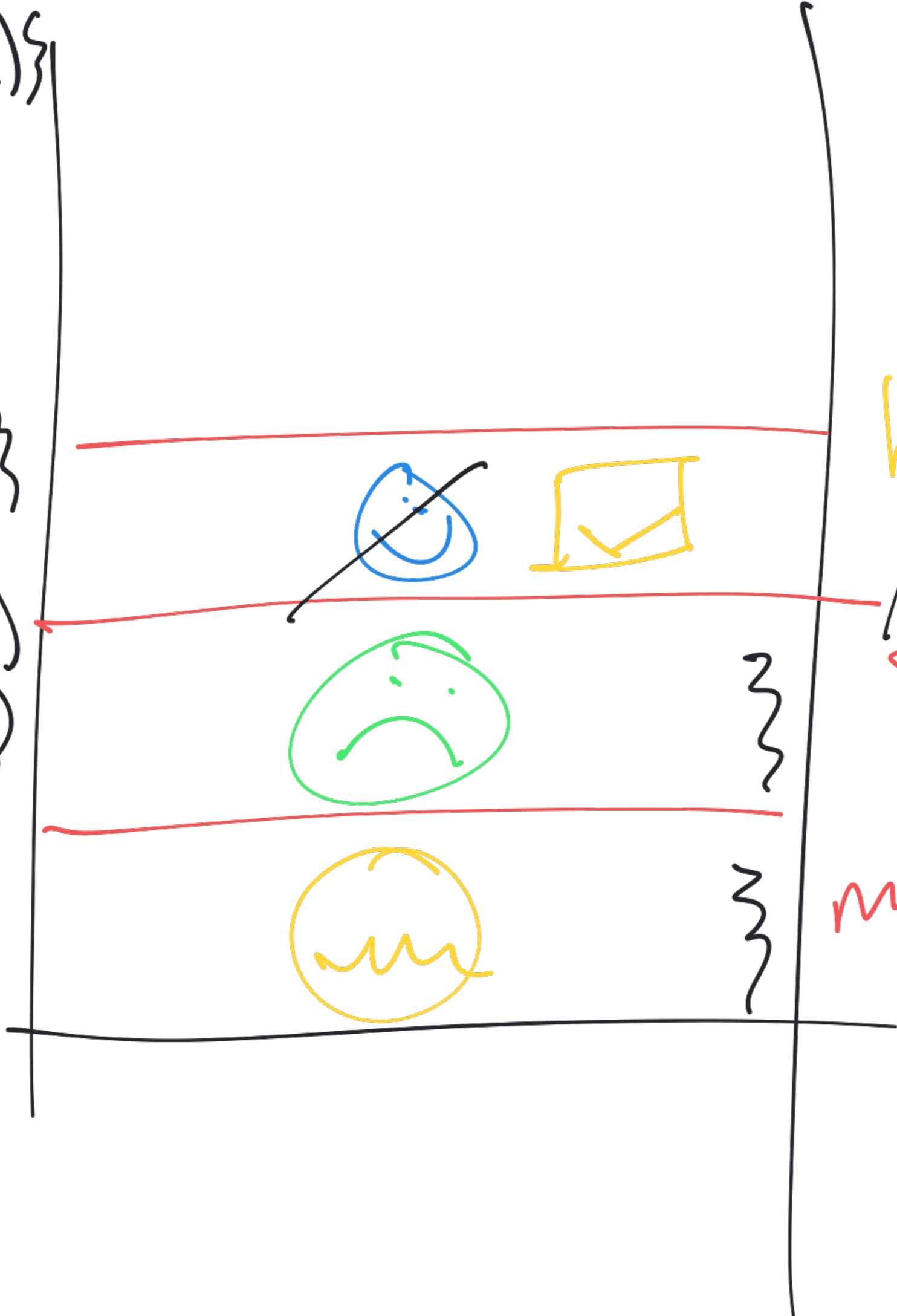
int f(x,y) {

g(x+y);
h(x-y);

}

int g() {

}

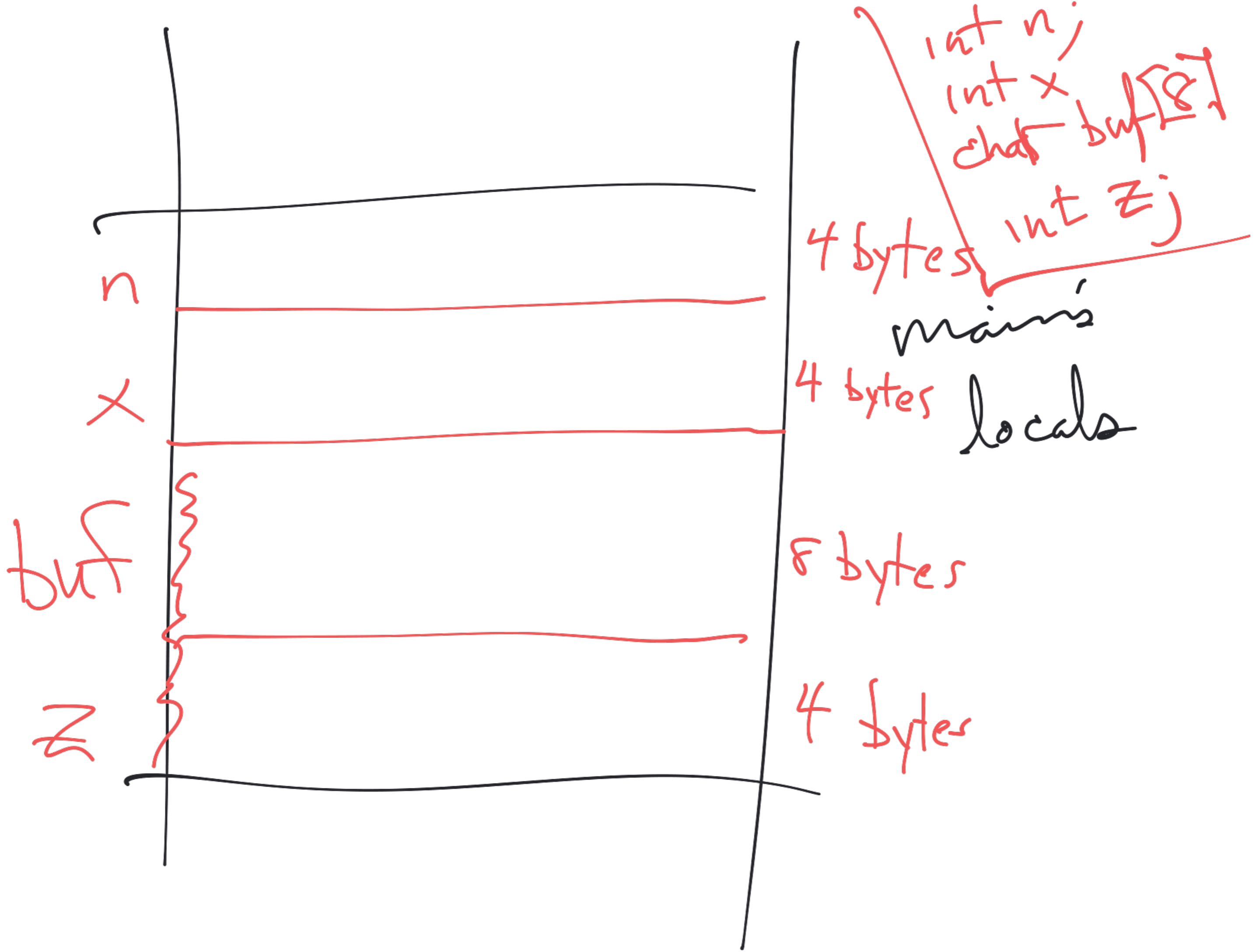


System Stack

~~g's locals~~

f's locals

main locals



{ int n; ← "automatic"
memory allocation"
(stack)

char *p = malloc(100); ← automatic

} *p ← dynamic mem.
(heap)

MOV — ~~copy~~ data from
one place to a register

Learn about

- addressing modes
- q, d, w, b

MOVQ — move a quad word (64)
MORQ — double word (32)
WORD (16)

cmp

rax, rdx

jl

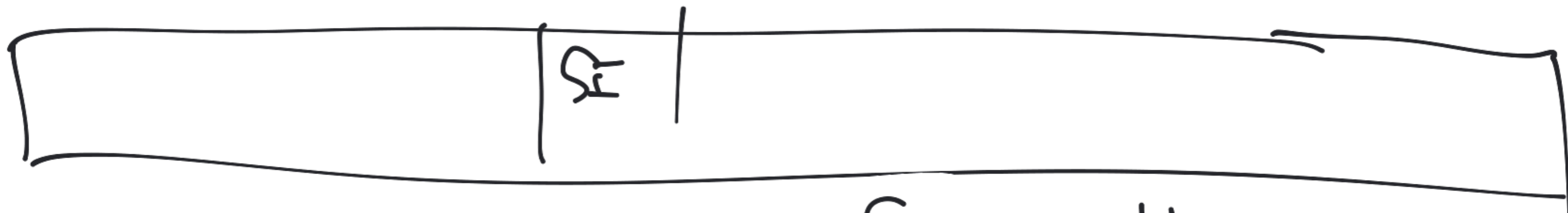
someplace



test edi, edi

AND the two operands

EFLAGS



SF = sign bit of result

ZF = 1 if result is 0

PF = 1 if # of 1 bits in result
is even

test edi, edi
jz SOME LABEL

jump if the ZF bit is 1
don't jump otherwise

START:

mov

add

test

jz

L1:

mov

add

L2:

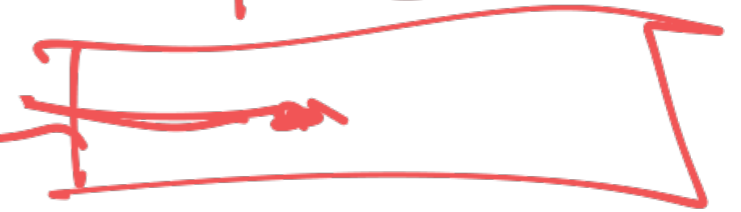
sub

ret



Program Counter

PC



CMP a, b

Compute $a - b$
(or is it $b - a$?)

Sets EFFLAGS

ZF
SF
PF

CF
OF
AF

CMP edi, 50

23 - 50 < 0

SF = 1

So JLE jumps