CS208

W, 29 April 2026

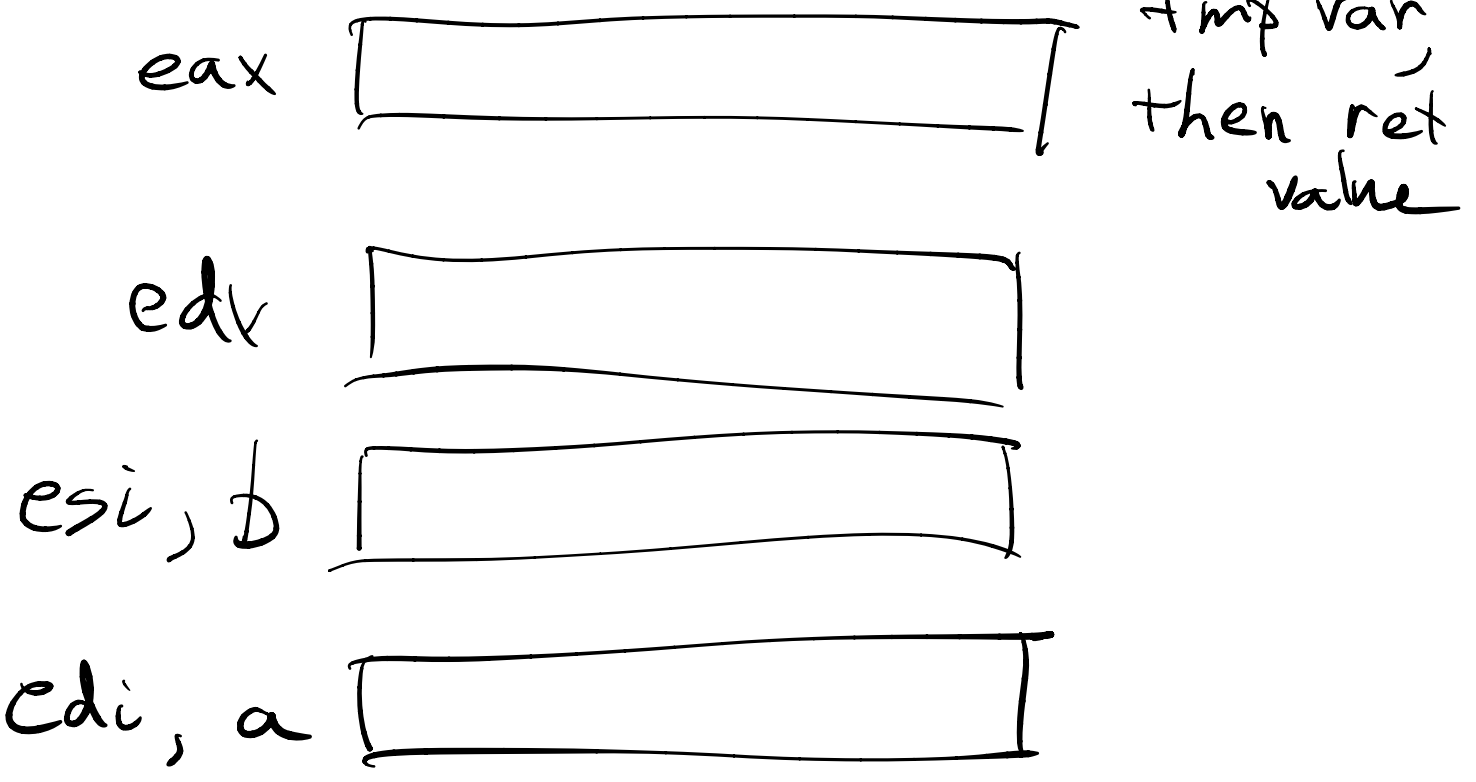
Stepping through some asm code

① parameters? edi — a
esi — b
return type? not rdx

```
int g(int a, int b)
```

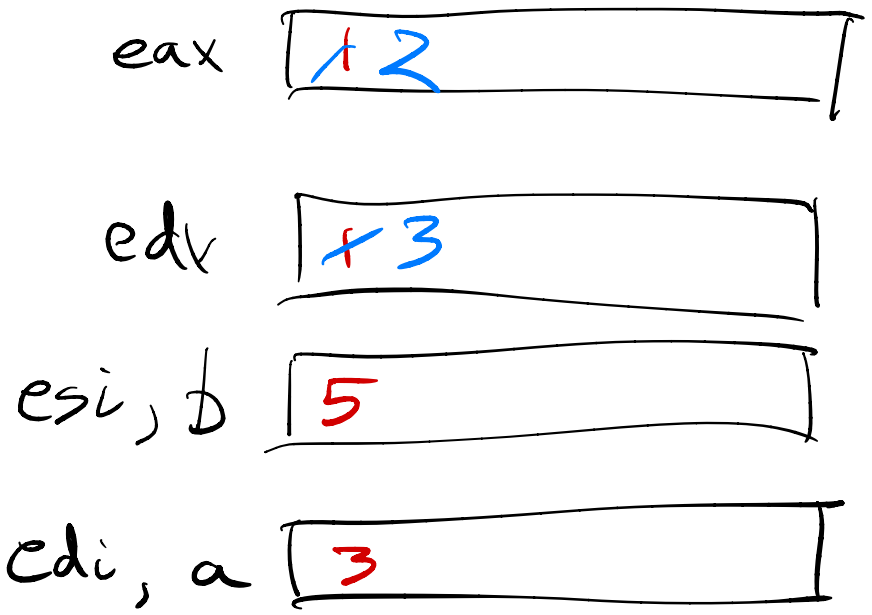
② Draw diagram of other Data

(2)



(3)

int g(int a, int b)



③ try an example

$g(3, 5)$

cmpl %esi, %eax | eax − esi = 1 − 5 = -4

SF = 1 ZF = 0

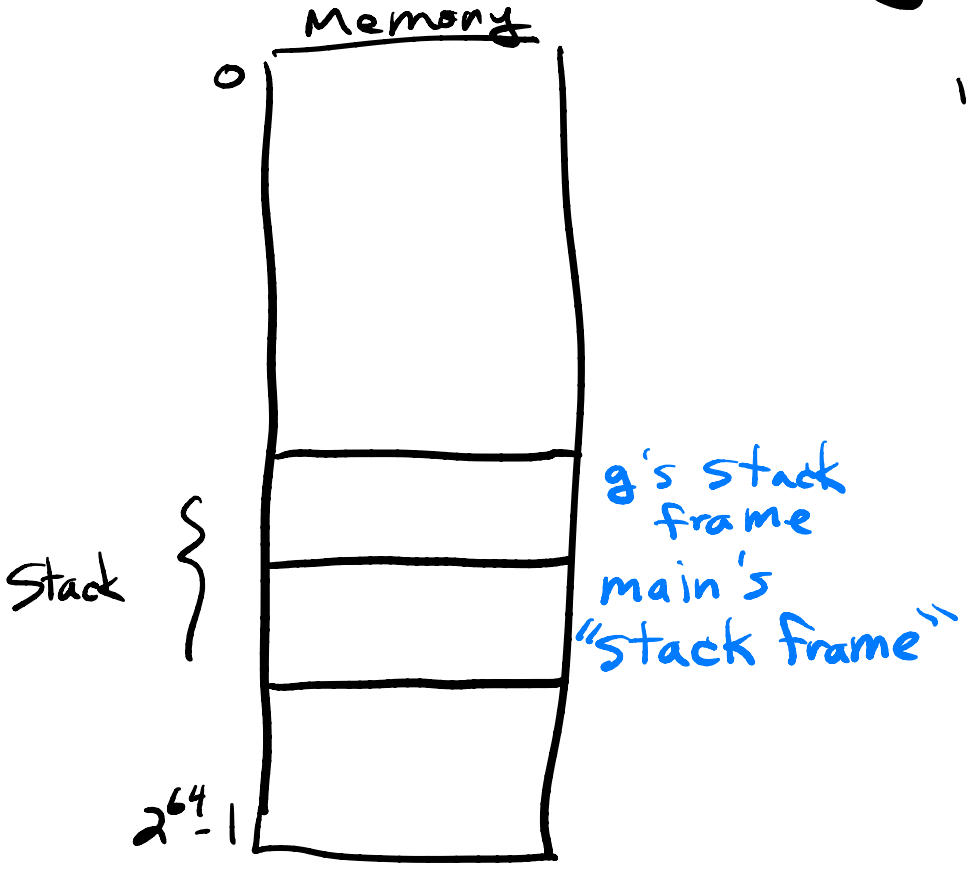
jl <0? Take the jump

④ Try to guess

```
for(eax = 1; eax < esi; eax++)
```

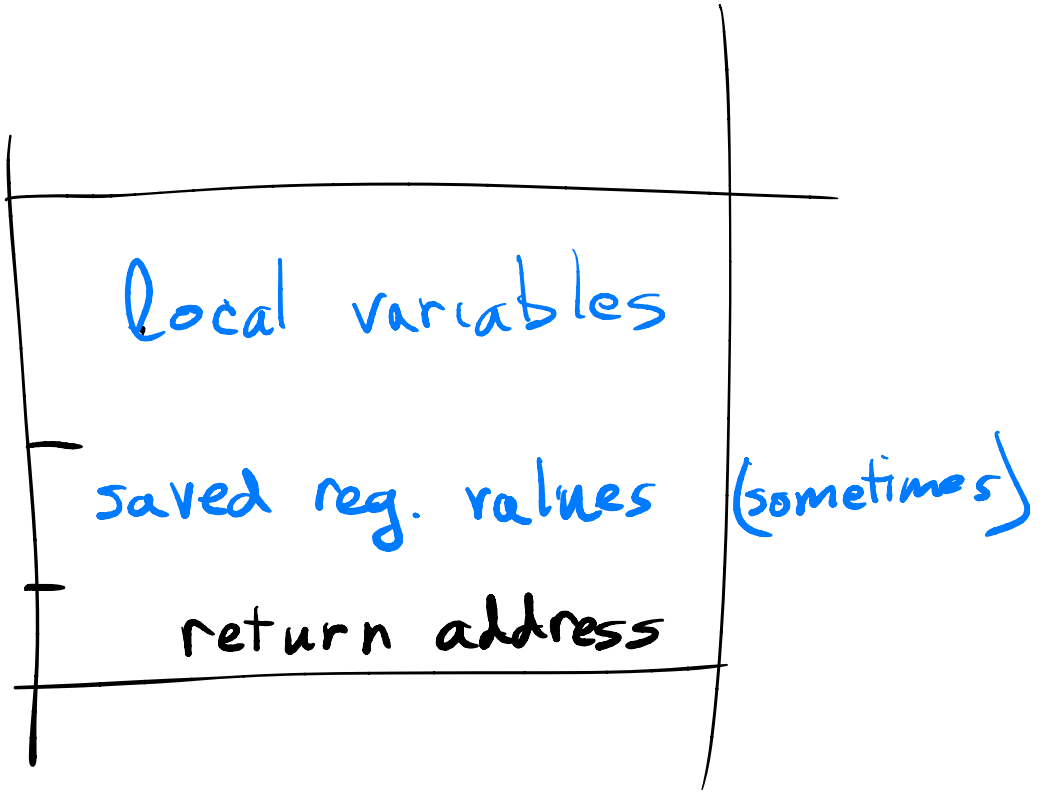
b

Stack + Calling functions




```
int main() {
    int x = g(3,5);
    :
}

int g(int b, int n) {
}
```

Stack frame


local variables
saved reg. values
(sometimes)
return address

return address

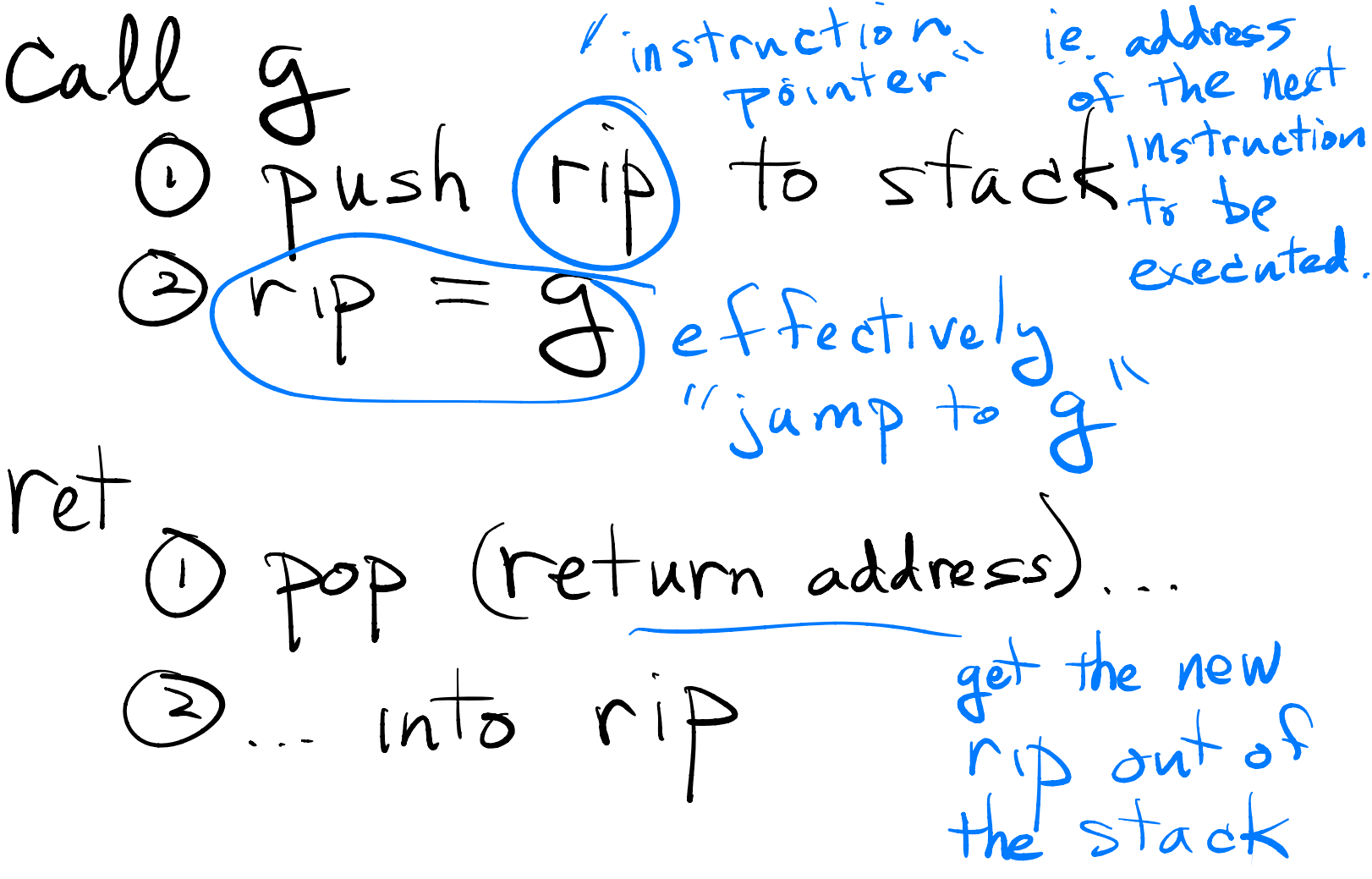
```
int main() {
    int x = g(3,5);
    int y = x+1;
    .
    .
}

int g(int b, int n) {
    .
    .
    return result;
}
```

```
movl $0x3, %edi
mov $0x5, %esi
call g
[x = eax]
[y = x + 1]
```

where does this jump target address come from?

```
movl _, %eax
ret
```

needs to jump


call g
① push rip to stack
② rip = g
"instruction pointer"
ie. address of the next instruction to be executed.
effectively "jump to g"
ret
① pop (return address)...
② ... into rip
get the new rip out of the stack