

Undefined

magic \$1234567; (%rbp)

int *x = (int *) 1234567;

int y = *x;

imp. defined

- consistent w/ program

- char signed or not

- # of bits in an int

- 2's complement

2^{48} - 256 TB

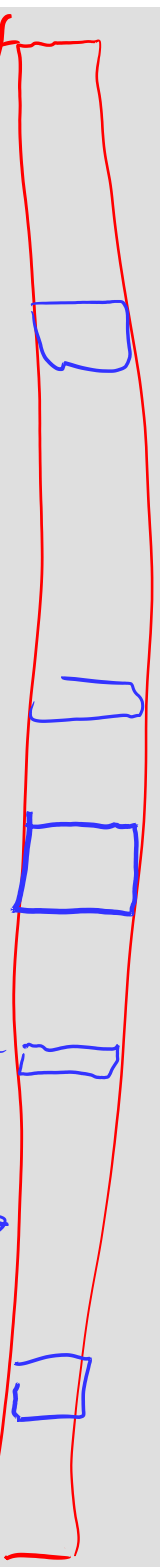
void *

0x123400000000



ffffffffff

00000000



Segment

read
write
execute

Segmentation
fault

impl - defined padding

```
struct foo {  
    int i;  
    double d;  
    struct foo *p;  
};
```

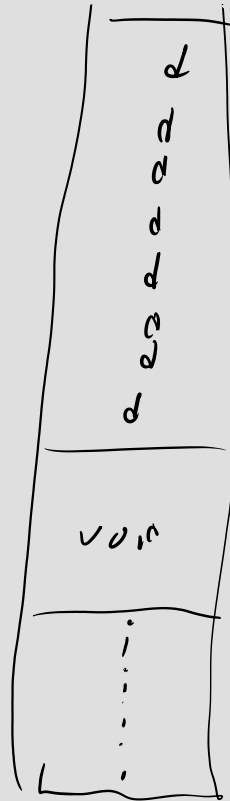
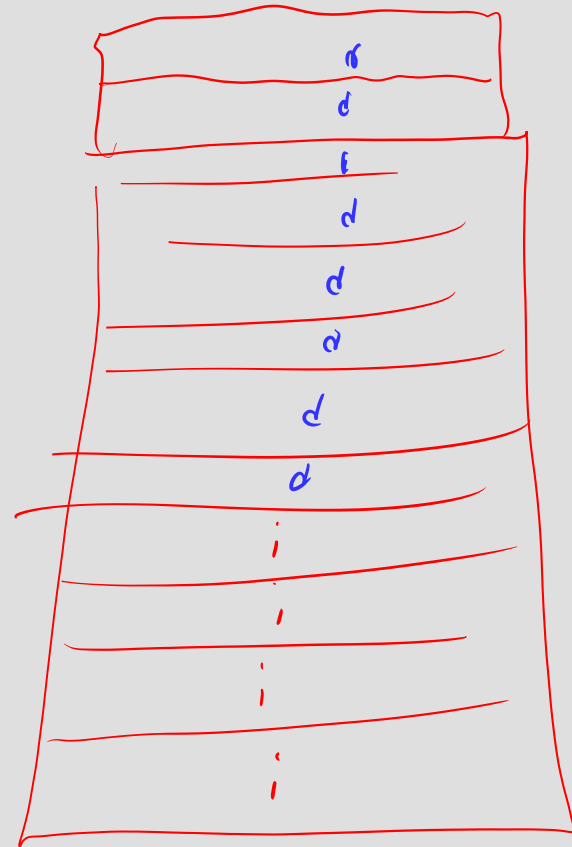
```
struct foo x;
```

```
x.d
```

```
struct foo y = x
```

$\%rax$
 Δx

$4 (\%rax)$
 8



Array

int x[10]

x is almost always treated like int *

int *y

*y → deref, 1st value

y[0] → *y

*(y+2) → deref 3rd value

y[2] → *(y+2)

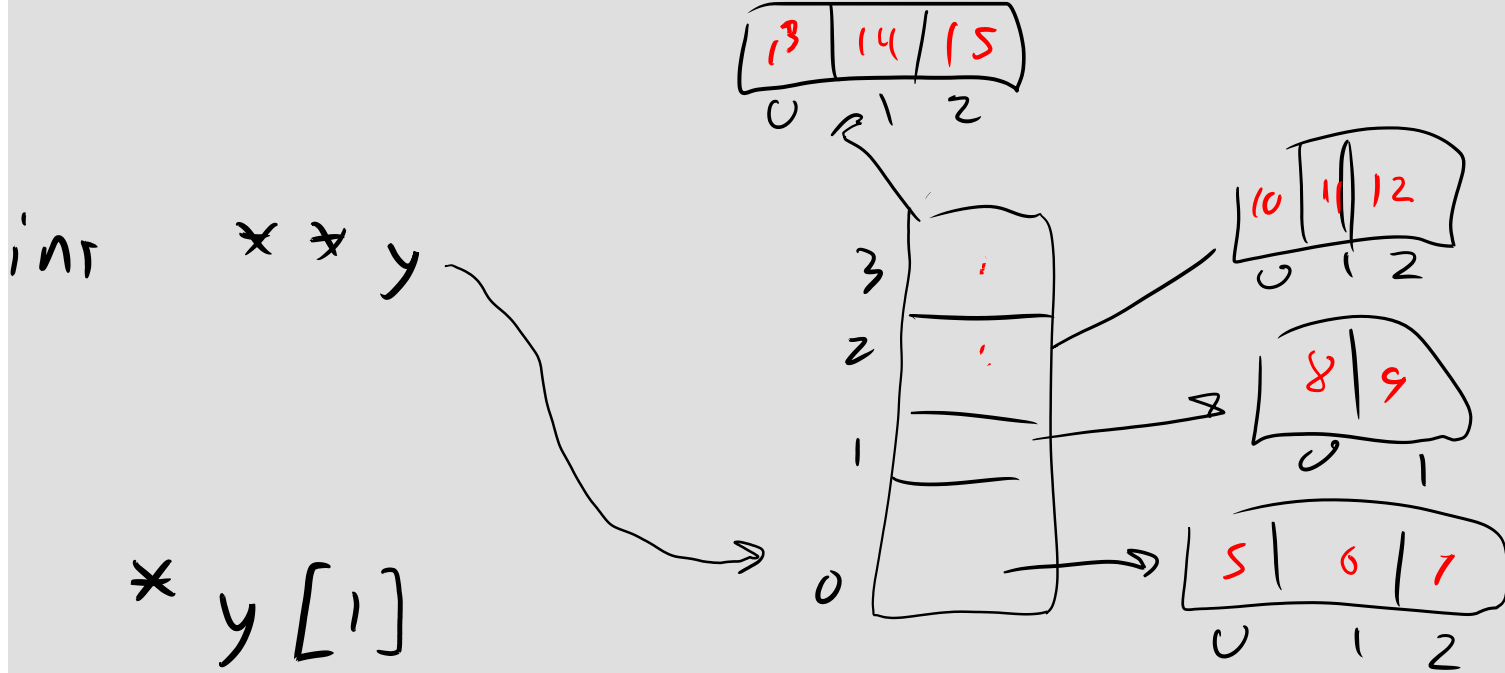
sizeof(y) → 8

&y → int **

sizeof(x) → 40

&x → &(x[0]) → int *

~~&**x~~ ~~==~~ ~~&x~~



89

8

6

(* y) [1]

*(y [1])

y [0] [1]

y [1] [0]