Memory and Addresses

Memory is just a sequence of byte-sized storage devices.
The bytes are assigned numeric addresses, starting with zero, just like the indexing of the cells of an array.

It is the job of the operating system (OS) to:
- manage the allocation of memory to processes
- keep track of what particular addresses each process is allowed to access, and how
- reserve portions of memory exclusively for use by the OS
- enforce protection of the memory space of each process, and of the OS itself
- do all this as efficiently as possible
**Pointer Concepts**

*pointer* a variable whose value is a memory address

*pointee* a value in memory whose address is stored in a pointer; we say the pointee is the *target* of the pointer

<table>
<thead>
<tr>
<th>address</th>
<th>contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x000010F0</td>
<td>A: 42</td>
</tr>
<tr>
<td>0x0000100C</td>
<td></td>
</tr>
<tr>
<td>0x00001008</td>
<td>B: 0x000010F0</td>
</tr>
<tr>
<td>0x00001004</td>
<td>C: 0x00001008</td>
</tr>
<tr>
<td>0x00001000</td>
<td></td>
</tr>
<tr>
<td>0x00000FFC</td>
<td>D: 0x00000FF8</td>
</tr>
<tr>
<td>0x00000FF8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>??</td>
</tr>
</tbody>
</table>
Since memory addresses are essentially just integer values, pointers are the same width as integers.

A pointer has a type, which is related to the type of its target.

Pointer types are simple; there is no automatic initialization.

A pointer may or may not have a target.

Given a pointer that has a target, the target may be accessed by *dereferencing* the pointer.

A pointee may be the target of more than one pointer at the same time.

Pointers may be assigned and compared for equality, using the usual operators.

Pointers may also be manipulated by incrementing and decrementing, although doing so is only safe under precisely-defined circumstances.

By convention, pointers without targets should be set to 0 (or `NULL`).
C Syntax: Declaring Pointers

Declarations:

```c
int* p1 = NULL; // declaration of pointer-to-int

char* p2 = 0; // pointer-to-char

int** p3 = NULL; // pointer-to-a-pointer-to-int
```

One syntax gotcha:

```c
int* q1 = NULL,
q2 = NULL; // q2 is an int, not a pointer!

int* q1 = NULL,
*q2 = NULL; // q1 and q2 are both pointers
```
C Syntax: \textit{address-of} Operator

\&X returns the address of the object \(X\); the \textit{address-of operator}

\begin{verbatim}
int x = 42,
y = 99;

int* p1 = \&x; // p1 stores address of variable \(x\)
int* p2 = \&y; // p2 stores address of variable \(y\)
int** p3 = \&p2; // p3 stores address of variable \(p2\)
\end{verbatim}
### C Syntax: dereference Operator

*P names the target of the pointer P; the *dereference operator*

```c
int  x = 42, y = 99;

int*  p1 = &x;  // p1 stores address of variable x
int*  p2 = &y;  // p2 stores address of variable y

int** p3 = &p2; // p3 stores address of variable p2

int aa = *p1;   // aa stores value of the target of p1, 42
*p1 = 10;       // the target of p1, which is x, stores 10
int bb = *p3;   // illegal: *p3 is a pointer-to-int but bb
                // is just an int
int bb = **p3;  // bb stores value of the target of the
                // target of p3; p3 points to p2 and
                // p2 points to y, so bb gets value 99
```
int *X;
...
X refers to X, type is int *

&X refers to address of X, type is int **

*X refers to target of X, type is int

*&X refers to target of address of X, which is just... X

&*X refers to address of target of X, which is just... the value of X

(only makes sense syntactically if X is a pointer)
int main() {

    int  x = 42, y = 99;

    int*  p1 = &x;     // p1 stores address of variable x
    int*  p2 = &y;     // p2 stores address of variable y
    int** p3 = &p2;   // p3 stores address of variable p2

    int aa = *p1;     // aa stores value of the target of p1, 42
    *p1 = 10;         // the target of p1, which is x, stores 10

    int bb = **p3;    // bb stores value of the target of the
                     // target of p3; p3 points to p1 and
                     // p1 points to x, so bb gets value 99

    return 0;
}
main:

movl $42, -20(%ebp)
movl $99, -24(%ebp)
leal -20(%ebp), %eax
movl %eax, -4(%ebp)
leal -24(%ebp), %eax
movl %eax, -28(%ebp)
leal -28(%ebp), %eax
movl %eax, -8(%ebp)
movl -4(%ebp), %eax
movl (%eax), %eax
movl %eax, -12(%ebp)
movl -4(%ebp), %eax
movl $10, (%eax)
movl -8(%ebp), %eax
movl (%eax), %eax
movl (%eax), %eax
movl %eax, -16(%ebp)

the Stack

<table>
<thead>
<tr>
<th>ebp</th>
<th>old ebp</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebp – 4</td>
<td></td>
</tr>
<tr>
<td>ebp – 8</td>
<td></td>
</tr>
<tr>
<td>ebp – 12</td>
<td></td>
</tr>
<tr>
<td>ebp – 16</td>
<td></td>
</tr>
<tr>
<td>ebp – 20</td>
<td></td>
</tr>
<tr>
<td>ebp – 24</td>
<td></td>
</tr>
<tr>
<td>ebp – 28</td>
<td></td>
</tr>
<tr>
<td>esp</td>
<td></td>
</tr>
</tbody>
</table>

p1
p3
aa
bb
x
y
p2
### x86-32 Assembly View

**main:**

```assembly
... # x = 42; y = 99;
movl $42, -20(%ebp)  
movl $99, -24(%ebp)  
... 
```

<table>
<thead>
<tr>
<th>ebp</th>
<th>old ebp</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebp - 4</td>
<td></td>
</tr>
<tr>
<td>ebp - 8</td>
<td></td>
</tr>
<tr>
<td>ebp - 12</td>
<td></td>
</tr>
<tr>
<td>ebp - 16</td>
<td></td>
</tr>
<tr>
<td>ebp - 20</td>
<td></td>
</tr>
<tr>
<td>ebp - 24</td>
<td></td>
</tr>
<tr>
<td>ebp - 28</td>
<td></td>
</tr>
<tr>
<td>esp</td>
<td></td>
</tr>
</tbody>
</table>

The Stack

- x: 42
- y: 99
int main() {
    . . .
    int* p1 = &x;    // p1 is assigned the address of variable x
    int* p2 = &y;    // p2 is assigned the address of variable y
    . . .
}

&x    the address of x
x      is an int
&x    is an int*
&y    the address of y
x86-32 Assembly View

main:

# p1 = &x
lea -20(%ebp), %eax  # eax = ebp - 20
movl %eax, -4(%ebp)  # *(ebp - 4) = eax

# p2 = &y
lea -24(%ebp), %eax
movl %eax, -28(%ebp)

&x  the address of x:  ebp - 20
&y  the address of y:  ebp - 24

the Stack

<table>
<thead>
<tr>
<th>ebp</th>
<th>old ebp</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebp - 4</td>
<td>p1: ebp - 20</td>
</tr>
<tr>
<td>ebp - 8</td>
<td></td>
</tr>
<tr>
<td>ebp - 12</td>
<td></td>
</tr>
<tr>
<td>ebp - 16</td>
<td></td>
</tr>
<tr>
<td>ebp - 20</td>
<td>x: 42</td>
</tr>
<tr>
<td>ebp - 24</td>
<td>y: 99</td>
</tr>
<tr>
<td>ebp - 28</td>
<td>p2: ebp - 24</td>
</tr>
<tr>
<td>esp</td>
<td></td>
</tr>
</tbody>
</table>
int main() {
    . . .
    int** p3 = &p2;  // p3 is assigned the address of variable p2
    . . .
}
main:

# p3 = &p2
leal  -28(%ebp), %eax  # eax = ebp - 28
movl  %eax, -8(%ebp)    # *(ebp – 8) = eax

the Stack

<table>
<thead>
<tr>
<th>ebp</th>
<th>old ebp</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebp - 4</td>
<td>p1: ebp - 20</td>
</tr>
<tr>
<td>ebp - 8</td>
<td>p3: ebp - 28</td>
</tr>
<tr>
<td>ebp - 12</td>
<td></td>
</tr>
<tr>
<td>ebp - 16</td>
<td></td>
</tr>
<tr>
<td>ebp - 20</td>
<td>x: 42</td>
</tr>
<tr>
<td>ebp - 24</td>
<td>y: 99</td>
</tr>
<tr>
<td>ebp - 28</td>
<td>p2: ebp - 24</td>
</tr>
<tr>
<td>esp</td>
<td></td>
</tr>
</tbody>
</table>

&p2 the address of p2: ebp - 28
```c
int main() {
    . . .
    int aa = *p1;    // aa is assigned value of the target of p1;
    // p1 points to x;
    // x has the value 42
    . . .
}
```

*p1  the target of p1
p1  points to x
x  has the value 42
aa  is assigned 42

Value of *p1
  = value of target of p1
  = value of x
  = 42
```assembly
main:
    # aa = *p1
    movl  -4(%ebp), %eax  # eax = *(ebp - 4)
    movl  (%eax), %eax    # eax = *eax = *( *(ebp - 4) )
    movl  %eax, -12(%ebp) # *(ebp - 12) = eax
```

<table>
<thead>
<tr>
<th>ebp</th>
<th>old ebp</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebp - 4</td>
<td>p1: ebp - 20</td>
</tr>
<tr>
<td>ebp - 8</td>
<td>p3: ebp - 28</td>
</tr>
<tr>
<td>ebp - 12</td>
<td>aa: 42</td>
</tr>
<tr>
<td>ebp - 16</td>
<td></td>
</tr>
<tr>
<td>ebp - 20</td>
<td>x: 42</td>
</tr>
<tr>
<td>ebp - 24</td>
<td>y: 99</td>
</tr>
<tr>
<td>ebp - 28</td>
<td>p2: ebp - 24</td>
</tr>
<tr>
<td>esp</td>
<td></td>
</tr>
</tbody>
</table>

the Stack
int main() {
    . . .
    
    *p1 = 10;   // the target of p1, which is x,
    // is assigned the value 10
    
    . . .
}
main:

# *p1 = 10
movl -4(%ebp), %eax  # eax = *(ebp - 4)
movl $10, (%eax)   # *eax = 10

the Stack

<table>
<thead>
<tr>
<th>ebp</th>
<th>old ebp</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebp - 4</td>
<td>p1: ebp - 20</td>
</tr>
<tr>
<td>ebp - 8</td>
<td>p3: ebp - 28</td>
</tr>
<tr>
<td>ebp - 12</td>
<td>aa: 42</td>
</tr>
<tr>
<td>ebp - 16</td>
<td></td>
</tr>
<tr>
<td>ebp - 20</td>
<td>x: 10</td>
</tr>
<tr>
<td>ebp - 24</td>
<td>y: 99</td>
</tr>
<tr>
<td>ebp - 28</td>
<td>p2: ebp - 24</td>
</tr>
<tr>
<td>esp</td>
<td></td>
</tr>
</tbody>
</table>
```
int main() {

    int bb = **p3;  // bb stores value of the target of the
                    // target of p3; p3 points to p1 and
                    // p1 points to x, so bb gets value 99
    
}
```

**p3  the target of p3
p3  points to p1
p1  points to x
x  has the value 42

Value of **p3

\[
= \text{value of target of target of } p3 \\
= \text{value of target of } p1 \\
= \text{value of } x \\
= 42
\]
main:

# bb = **p3
movl -8(%ebp), %eax  # eax = *(ebp – 8)
movl (%eax), %eax    # eax = *eax = *( *(ebp – 8) )
movl (%eax), %eax    # eax = *eax = *( *( *(ebp – 8) ) )
movl %eax, -16(%ebp) #

```

the Stack

<table>
<thead>
<tr>
<th>ebp</th>
<th>old ebp</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebp</td>
<td>p1: ebp – 20</td>
</tr>
<tr>
<td>ebp – 4</td>
<td>p3: ebp – 28</td>
</tr>
<tr>
<td>ebp – 8</td>
<td>p3: ebp – 28</td>
</tr>
<tr>
<td>ebp – 12</td>
<td>aa: 42</td>
</tr>
<tr>
<td>ebp – 16</td>
<td>bb: 99</td>
</tr>
<tr>
<td>ebp – 20</td>
<td>x: 10</td>
</tr>
<tr>
<td>ebp – 24</td>
<td>y: 99</td>
</tr>
<tr>
<td>ebp – 28</td>
<td>p2: ebp – 24</td>
</tr>
<tr>
<td>esp</td>
<td></td>
</tr>
</tbody>
</table>
```
#include <stdint.h>

int main() {
    uint32_t X = 100;
    uint32_t Y = 200;
    Swap(&X, &Y);
    return 0;
}

void Swap(uint32_t* A, uint32_t* B) {
    uint32_t Temp = *A; // Temp = 100
    *A = *B; // X = 200
    *B = Temp; // Y = 100
}

The *pass-by-pointer* protocol provides a called function with the ability to modify the value of the caller's variable.
x86-32 Assembly View

Swap:

```
pushl %ebp
movl %esp, %ebp
subl $16, %esp
movl 8(%ebp), %eax
movl (%eax), %eax
movl %eax, -4(%ebp)
movl 12(%ebp), %eax
movl (%eax), %edx
movl 8(%ebp), %eax
movl %edx, (%eax)
movl 12(%ebp), %eax
movl -4(%ebp), %edx
movl %edx, (%eax)
leave
ret
```

(frame for main)

<table>
<thead>
<tr>
<th>ebp + 12</th>
<th>B: &amp;Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebp + 8</td>
<td>A: &amp;X</td>
</tr>
<tr>
<td>ebp</td>
<td>old ebp</td>
</tr>
<tr>
<td>ebp - 4</td>
<td>Temp: ??</td>
</tr>
<tr>
<td>ebp - 8</td>
<td></td>
</tr>
<tr>
<td>ebp - 12</td>
<td></td>
</tr>
<tr>
<td>esp</td>
<td></td>
</tr>
</tbody>
</table>

the Stack
x86-32 Assembly View

Swap:

```assembly
... ## Temp = *A
# get A
movl 8(%ebp), %eax

# get target of A
movl (%eax), %eax

# Temp = target of A
movl %eax, -4(%ebp)
...```

[frame for main]

| ebp + 12 | B: &Y |
| ebp + 8  | A: &X |
| ebp      | return address |
| ebp - 4  | old ebp |
| ebp - 8  | Temp: 100 |
| ebp - 12 |            |
| esp      |            |

the Stack
Swap:

```assembly
## *A = *B
# get B
movl 12(%ebp), %eax

# get target of B
movl (%eax), %edx

# get A
movl 8(%ebp), %eax

# target of A =
#     target of B
movl %edx, (%eax)
```

(frame for main)

<table>
<thead>
<tr>
<th>ebp + 12</th>
<th>B: &amp;Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebp + 8</td>
<td>A: &amp;X</td>
</tr>
<tr>
<td>ebp</td>
<td>return address</td>
</tr>
<tr>
<td>ebp - 4</td>
<td>Temp: 100</td>
</tr>
<tr>
<td>ebp - 8</td>
<td></td>
</tr>
<tr>
<td>ebp - 12</td>
<td></td>
</tr>
</tbody>
</table>

(X: 200 Y: 200)

the Stack
Swap:

```assembly
## *B = Temp
# get B
movl 12(%ebp), %eax

# get Temp
movl -4(%ebp), %edx

# target of B = Temp
movl %edx, (%eax)
```

(frame for main)

<table>
<thead>
<tr>
<th>ebp + 12</th>
<th>B: &amp;Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebp + 8</td>
<td>A: &amp;X</td>
</tr>
<tr>
<td></td>
<td>return address</td>
</tr>
<tr>
<td>ebp</td>
<td>old ebp</td>
</tr>
<tr>
<td>ebp - 4</td>
<td>Temp: 100</td>
</tr>
<tr>
<td>ebp - 8</td>
<td></td>
</tr>
<tr>
<td>ebp - 12</td>
<td></td>
</tr>
<tr>
<td>esp</td>
<td></td>
</tr>
</tbody>
</table>

the Stack
The most common source of errors with direct pointer use is to dereference a pointer that does not have a valid target:

```c
int *A;
*A = 42; // A never had a target
```

```c
int *A = NULL;
if ( A != NULL )  // used correctly, NULL
    *A = 42;       // lets us check
```

```c
int *A = malloc( sizeof(int) );  // A has a target
int *B = A;                       // B shares it; alias
free(A);  // neither has a target
*B = 42;  // ERROR
```
In closing...

I shot a pointer to the heap,

and where it hit I did not care.

Now my code does make me weep,

and segfaults make me tear my hair.

- anonymous