- Steps required to crack a safe?

1. Understand the inner working
2. Use the right tools
3. Listen for the right TICK
4. Do the magic
5. Open the safe

Understand the Inner Working (1)

- Input devices: Keyboard

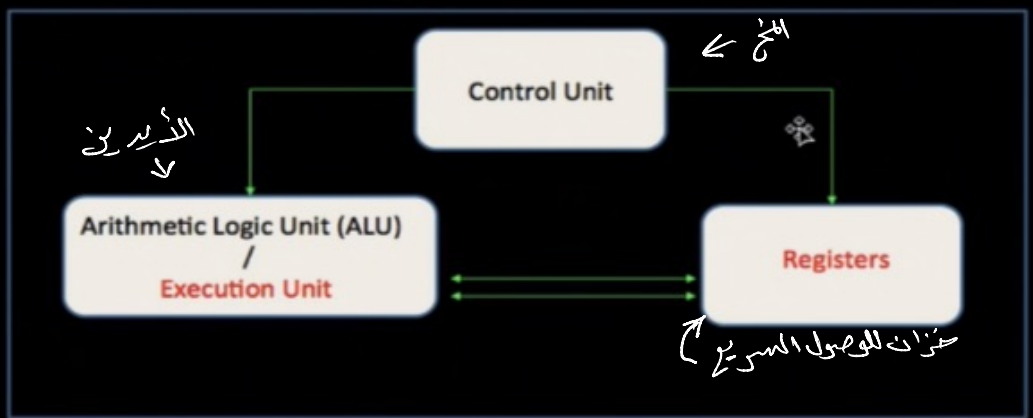
- Central Processing Unit: CPU

- Memory

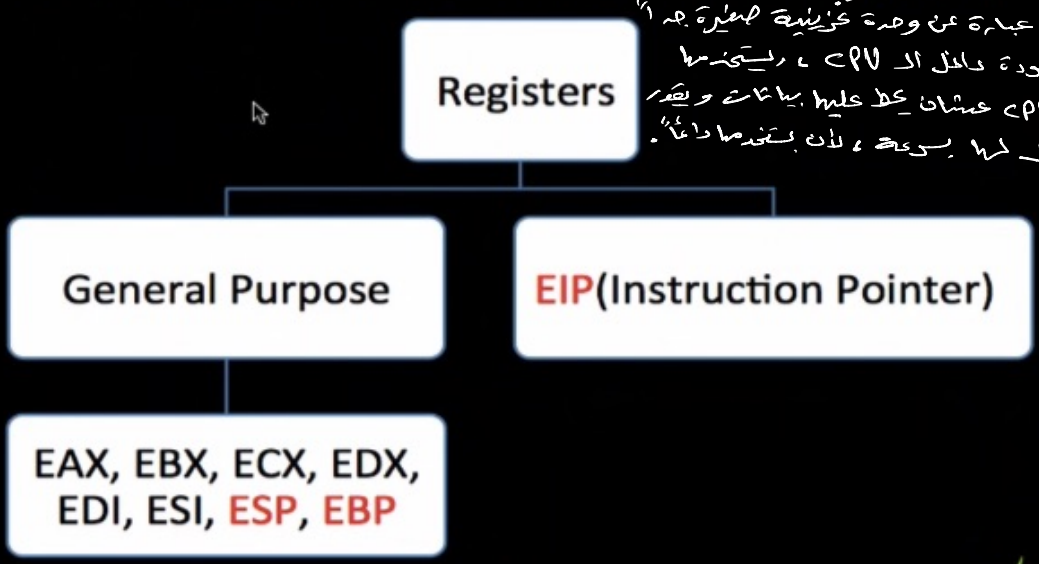
- Output Devices: Monitor

Understand the Inner Working (2)

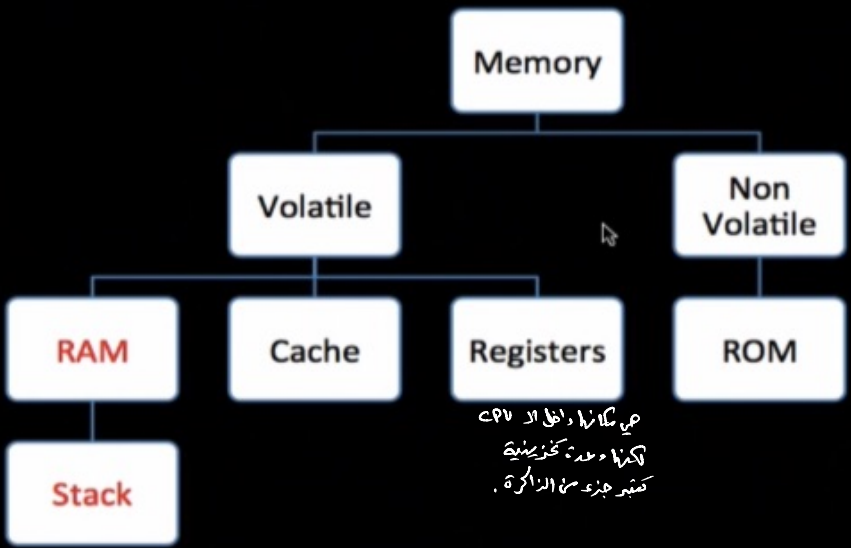
Central Processing Unit / Microprocessor



Understand the Inner Working (3)



Understand the Inner Working (4)

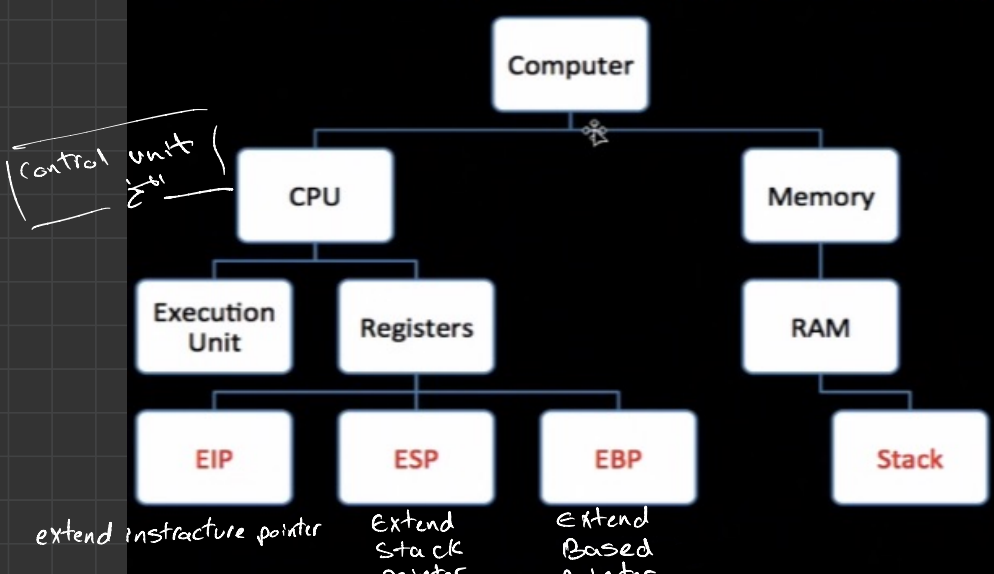


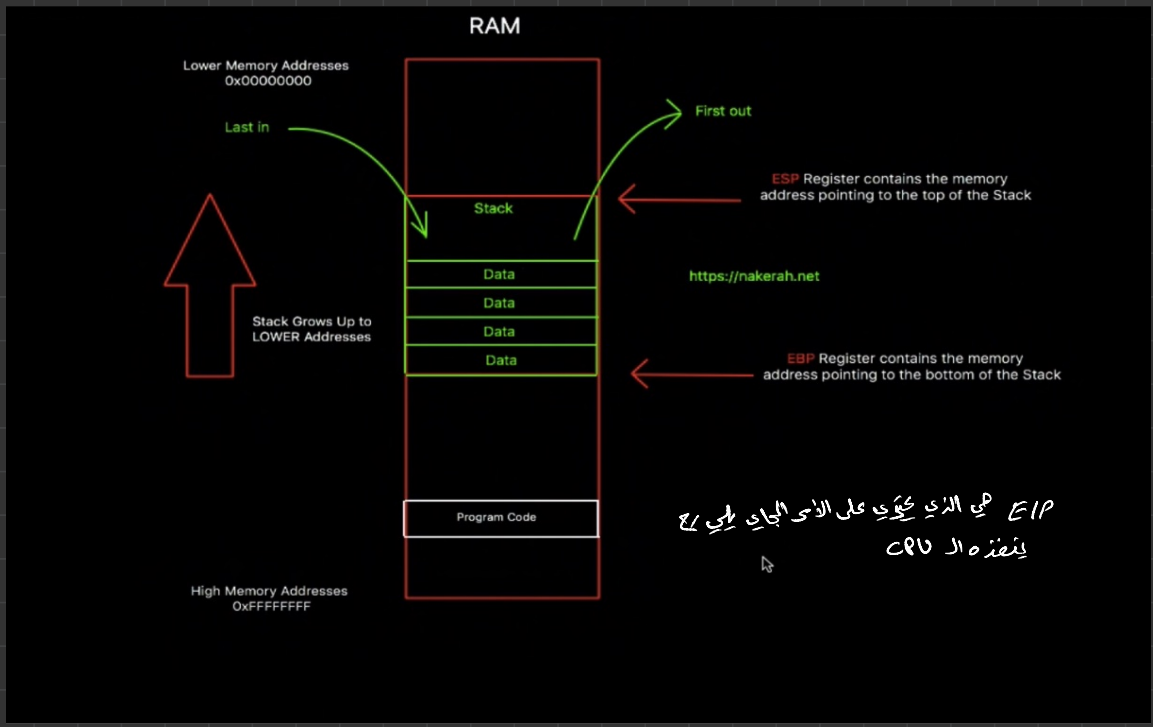
هي طريقة الحفاظ على الحاسوب يحتفظ فيها حتى لو طفيت الحاسوب . وهيك الـ BIOS

هي مكانها داخل الـ CPU لكنها وحدة تخزينية تعتبر جزء من الذاكرة .

www.Nakerah.net

Understand the Inner Working (4)



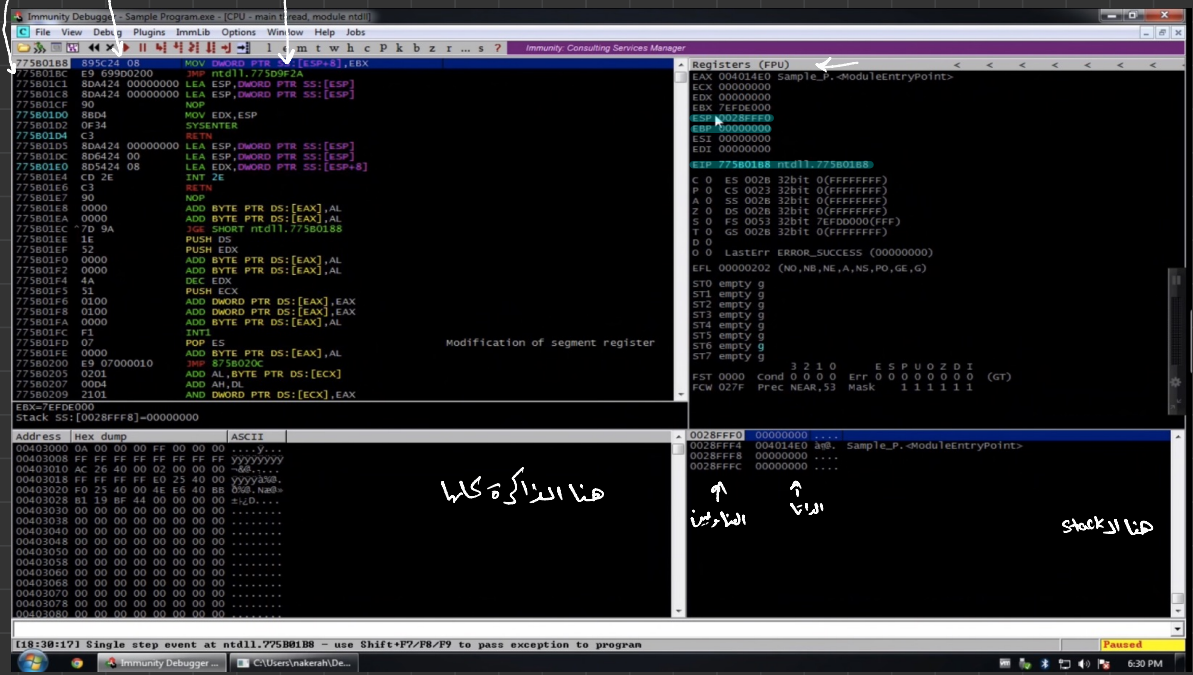


EIP هي الذي يحتوي على الأمر الجاي إلي لازم ينفذه الـ CPU

مؤشر العمليات

يترجم الـ Assembly لـ Hexadecimal

الأمر اللي إلي لازم يتطبق ويتم ترجمته لـ assembly

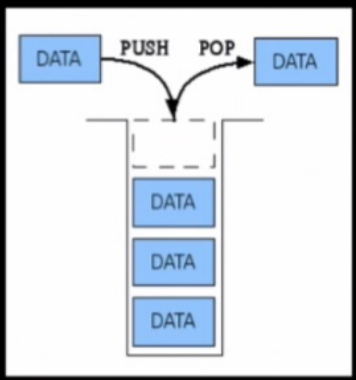


Stack

Understand the Inner Working (7)

- Stack

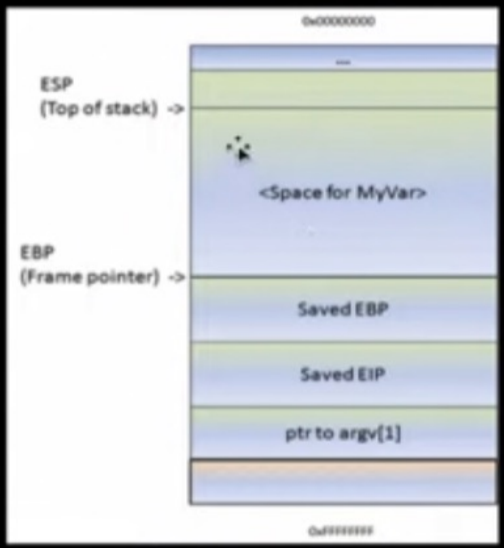
1. Used by functions
2. PUSH and POP 4bytes for x86
3. Last input first output
4. ESP and EBP : Top and Bottom
5. Grows towards lower addresses



Understand the Inner Working (6)

1. Push function arguments
   - Command line arguments
2. Call function
   - PUSH return address to restore normal execution after callee terminates & jmp to the callee.
3. push ebp
   - save caller ebp to restore it after callee terminates
4. mov ebp, esp
   - Make top and bottom of the stack equal "create new stack frame for the callee"
5. sub esp, N
   - reserve space on the stack for callee local variables
6. Callee inner working
7. Mov esp, ebp
   - restore old value of esp
8. pop ebp
   - restore old value of ebp
9. Return
   - restore original execution flow by executing instruction located at saved return address

Producing BOF Condition (1)

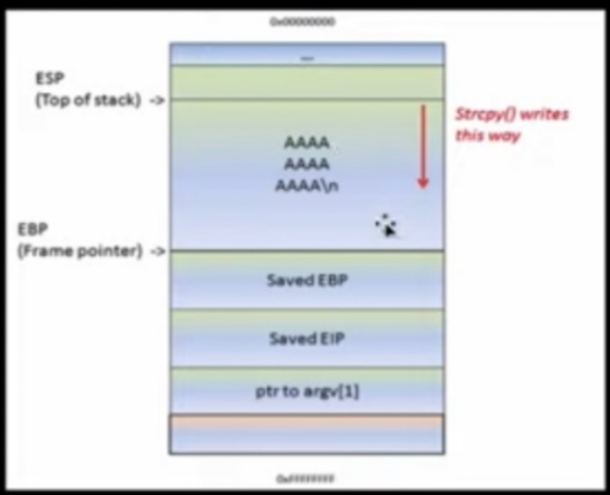



```
#include "string.h"

void do_something(char *Buffer)
{
    char MyVar[8];
    strcpy(MyVar,Buffer);
}

int main (int argc, char **argv)
{
    do_something(argv[1]);
    printf
}
```


Producing BOF Condition (2)



Producing BOF Condition (3)