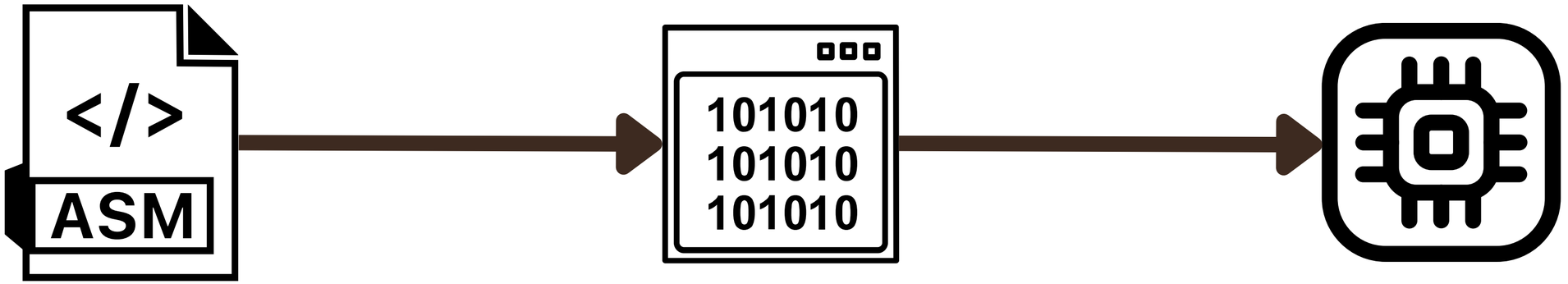
Reverse engineering

Introduction

Back to basics

Comment fonctionne un processeur ?



À retenir : l'assembleur est le langage de programmation le plus bas niveau

À titre de comparaison

Hello world Python

```
print("Hello World")
```

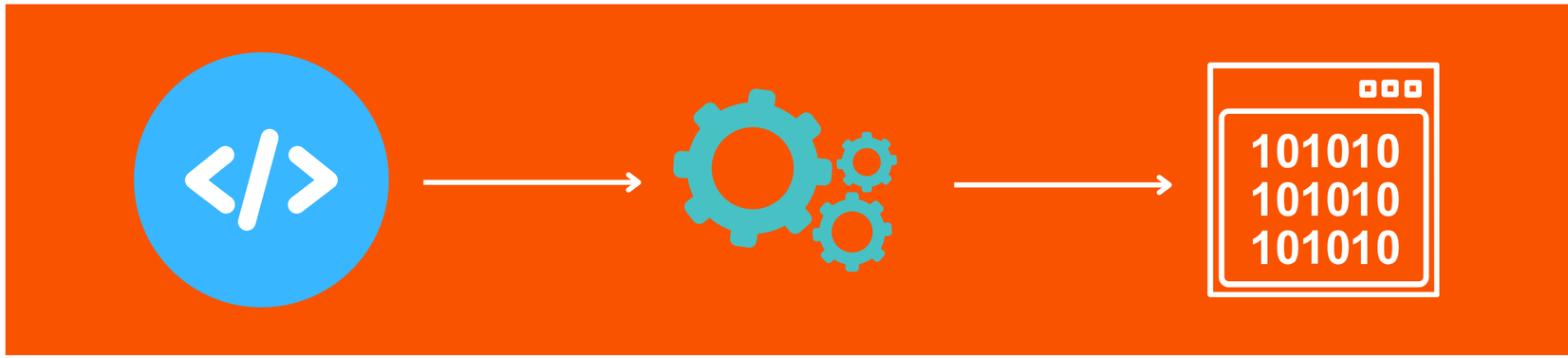
Hello world ASM

```
global _start

section .text
;Writing Code in .text section
_start:
        mov eax, 0x4
        mov ebx, 0x1
        mov ecx, message
        mov edx, mlen
        int 0x80
        ;Above code will print on screen

        mov eax, 0x1
        mov ebx, 0x1
        int 0x80
        ;Above code will exit

section .data
; Initialized data. Hello World string is initialized here.
        message: db "Hello World!", 0xA
        mlen    equ $-message
~
~
```

Compilation vs Interprétation

Deux types de langages...

Compilation



Interprétation

Décompilation et désassemblage

Un peu de vocabulaire de bricoleur

01 Retrouver le code

Désassembler, décompiler...
Varie en fonction des languages et des architectures

02 Lire le code

Déobfusquer, débugger, schématiser et patcher pour comprendre comment le programme fonctionne

03 Fun and profit

Tout ce qui en résulte : en fonction du contexte on peut exploiter le programme ou utiliser les informations récoltées directement

Reverse in a nutshell

Un résumé plus ou moins clair de la discipline

```
++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>---.
<++++++++++++++++++..>>++++++++.<+++++++++++++++.
<+++.>>++++++++++.<---------------.>--------------.
<<+.>>++++..<<-.>>++.-------.--.
```

Boîte à outils

GDB
The GNU Project
Debugger

objdump

Conseil pour l'apprentissage : chaque outil à sa couche d'abstraction, attention à ne pas trop simplifier dès le début

Cadre légal

En France

- Légal à but d'interopérabilité
- Illégal si publication ou reproduction

Dans le monde

Renseignez-vous !

Le hacking sauvage et non-encadré demeure illégal peu importe les circonstances

Ready to go

Le premier challenge est peut-être plus proche que vous ne le pensez...