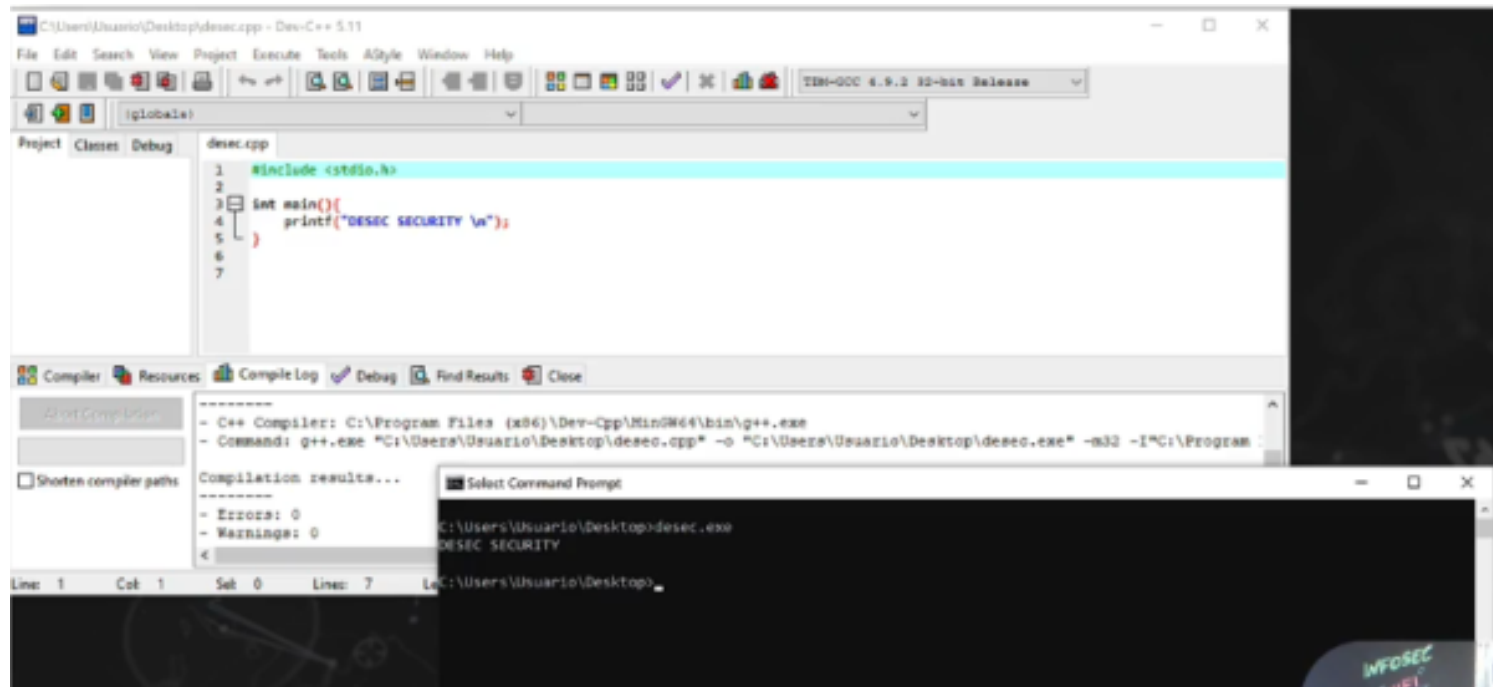


Conceitos e Programas Essenciais

Compilador

Converte código de alto nível em baixo nível trazendo um arquivo executável



Decompilador

Processo para ver o código de máquina e assembly de um executável

```
C:\Users\Usuario\Desktop>objdump -d -M intel sleep.exe

sleep.exe:      file format pei-i386

Disassembly of section .text:

00401000 <.text>:
  401000:      31 c0                xor     eax,eax
  401002:      b8 28 23 00 00      mov     eax,0x2328
  401007:      50                  push    eax
  401008:      bb 10 90 12 76      mov     ebx,0x76129010
  40100d:      ff d3              call    ebx
  ...
```

→ **objdump** é um decompilador para linux e para windows

→ -d é pra fazer desassembly
→ -M é para passar a sintaxe que vamos utilizar (no caso, a da intel),
Caso n passássemos a sintaxe (ou syntax), ele usaria por padrão a da ATNT

Assembler

Um assembler é um programa que traduz a linguagem assembly em código de máquina

Após usar um assembler, será gerado um **object file** que é uma representação binária do programa.

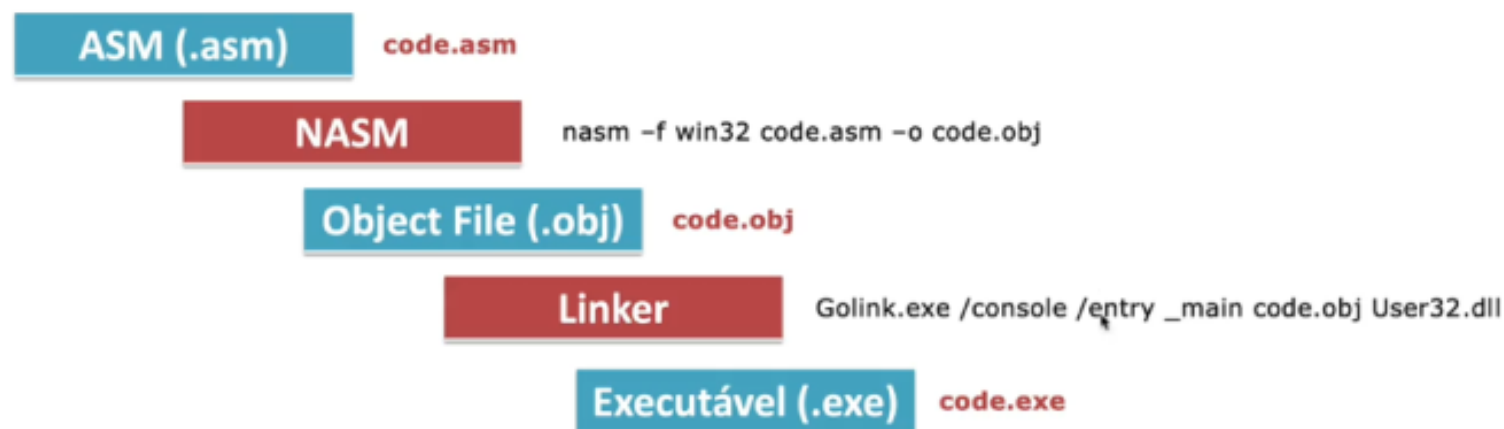
Um **linker** vai combinar os arquivos necessários para gerar o executável final.

Por Exemplo:

Vamos supor que no código escrito você utiliza uma função externa que faz parte da **User32.dll** então após gerar o **object file** é necessário usar um **linker** para que o programa consiga usar as funções em User32.dll. O linker por sua vez vai resultar em um arquivo executável final.



Processo

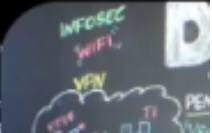


- 1- Montamos o código em assembly (code.asm)
- 2- Com o auxílio do **nasm** (um assembler) geramos o object file (code.obj) - que é a representação binária do programa que acabamos de escrever (code.asm)
- 3- Por meio do **Golink.exe** (linker), fazemos a associação com as bibliotecas externas e geramos o executável (code.exe)

```

~~~~~
                                Debbuger
~~~~~

```



→ o debugger é um programa que nos permite carregar outro programa em execução e ver ele em diversos formatos: Registradores, Stack, Memória e Opcodes

+ Aqui há o procedimento a ser tomado para a execução das atividades apresentadas em aula