1) ¿Qué es el 'stack' en el contexto del lenguaje ensamblador y cómo se utiliza?

Es una estructura de los datos en memoria que tiene el principio LIFO, se utiliza para guardar datos de forma temporal, como valores de registro, direcciones de retorno en llamada a funciones y parámetros

2) Describe un escenario práctico donde el uso de ensamblador sería más ventajoso que el uso de un lenguaje de alto nivel.

En el desarrollo de un sistema de frenado antibloqueo (ABS) para automóviles, donde es crucial ejecutar las instrucciones rápidamente y tener control directo sobre el hardware.

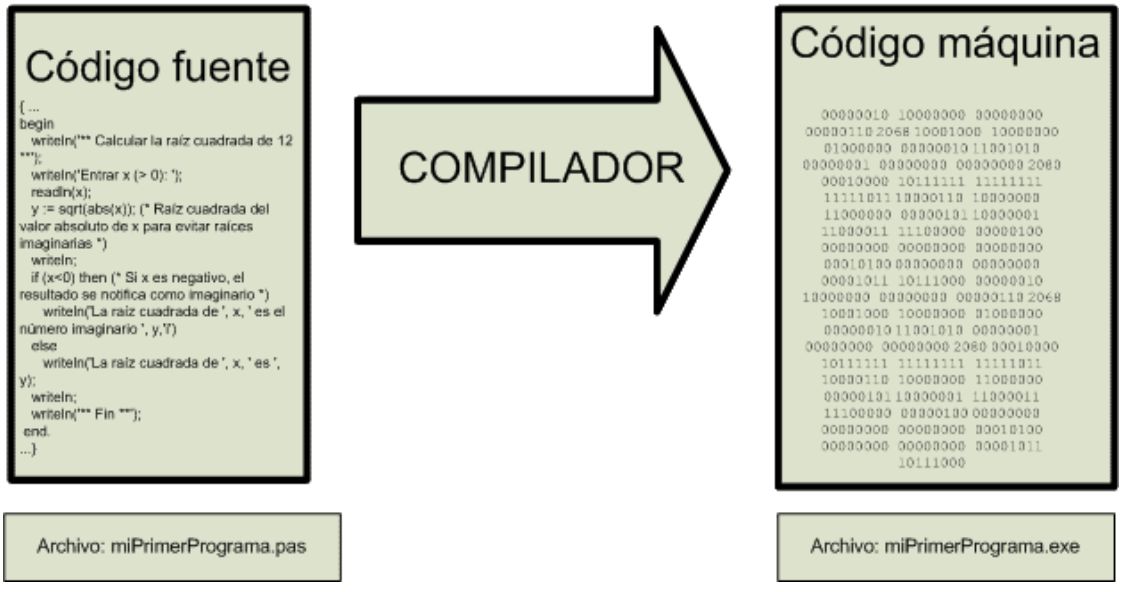
3) Explique cada línea del siguiente código del lenguaje ensamblador y diga que es lo que se está haciendo

```
MOV AX, 5      ; Línea 1
MOV BX, 10     ; Línea 2
ADD AX, BX     ; Línea 3
MOV CX, AX     ; Línea 4
```

- Línea 1: AX = 5, se almacena el valor 5 en AX
- Línea 2: BX=10, se almacena el valor 10 en BX
- Línea 3: AX= 15, suma los dos valores y se almacena en AX
- Línea 4: CX=15, el valor de AX se copia al CX

4) **Explique detalladamente cómo funcionan los compiladores**

Toma las instrucciones en lenguaje de alto nivel y lo traduce a lenguaje máquina (ceros y unos)



5) **Realizar sus propias capturas de pantalla del siguiente procedimiento:**

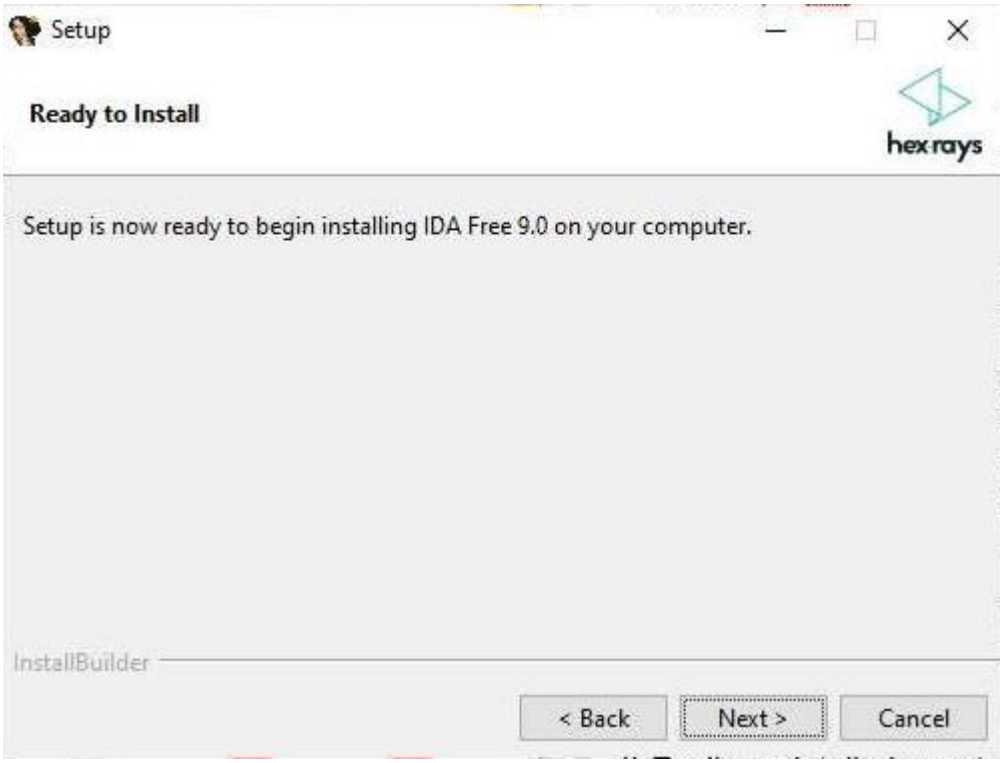
IDA: Es una de las herramientas más conocidas y potentes para el análisis de código

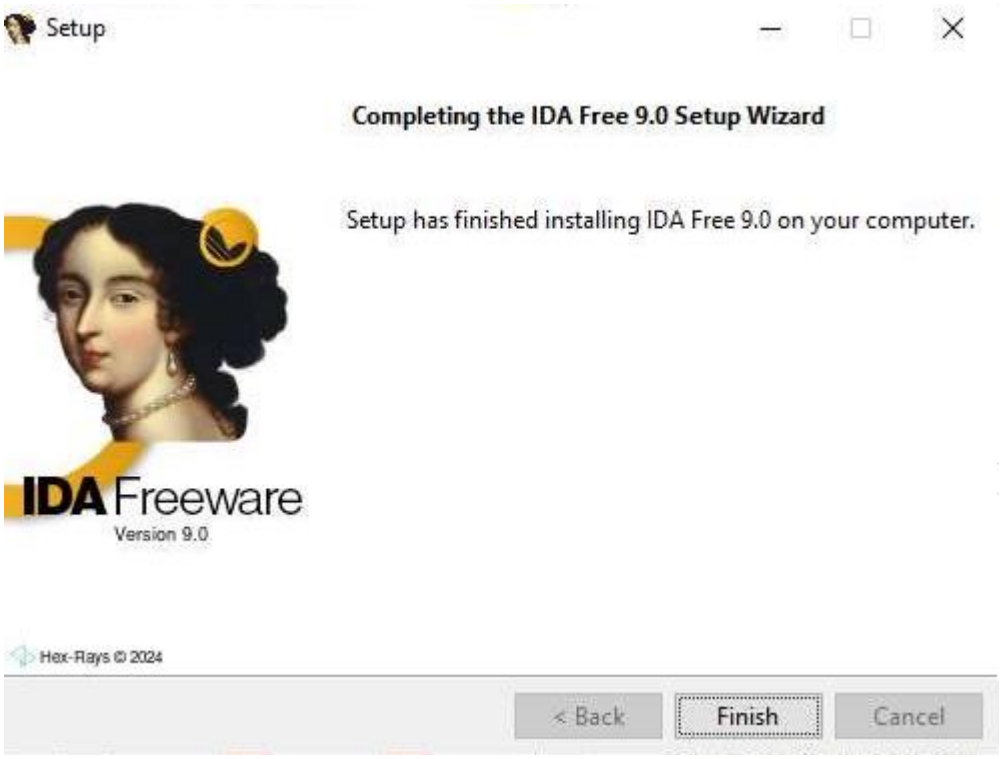
binario y desensamblado. En este laboratorio se instalará IDA FREE pero también se tiene la versión de paga IDA PRO

Paso 1:

Paso 2:

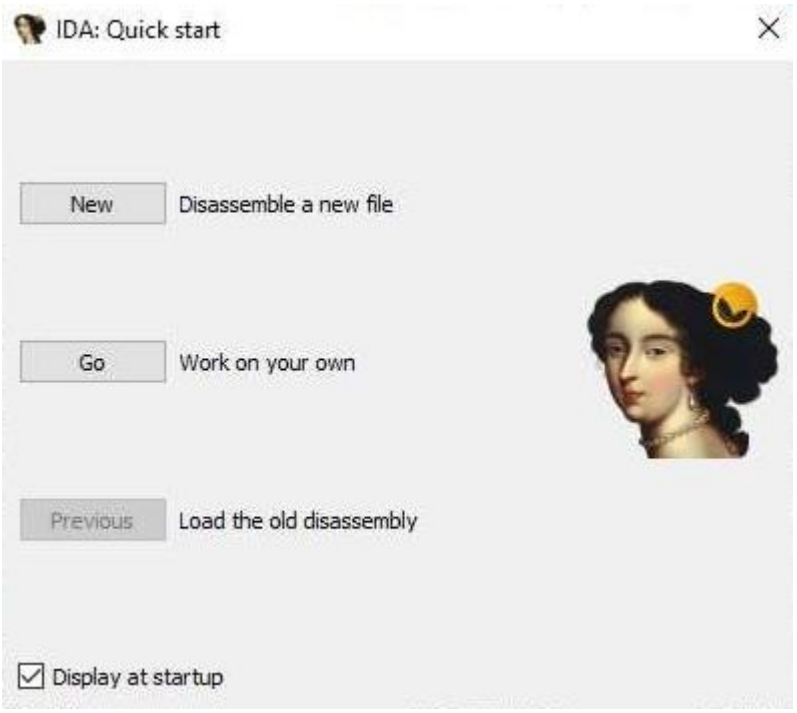

Setup
License Agreement
hex rays
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
Hex-Rays End User License Agreement
This End User License Agreement ("EULA") is a binding agreement between Hex Rays SA, with registered seat located at Rue Rennequin-Sualem 34, 4000 Liège, Belgium and registered under number 0873.473.914 ("HEX-RAYS", "we", "our", "us") and you (the "Customer", "You" or "End User") and govern, together with your Purchase Agreement, your use of the HEX-RAYS's software ("Software") and Documentation. This EULA also applies to any
Do you accept this license?
I accept the agreement
I do not accept the agreement
InstallBuilder
< Back
Next >
Cancel

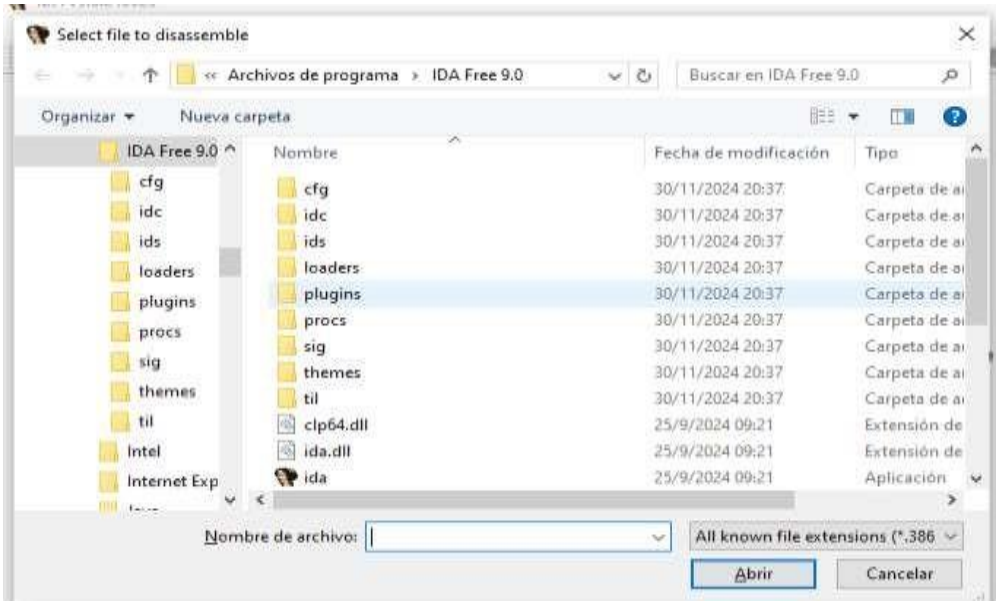

Setup
Ready to Install
hex rays
Setup is now ready to begin installing IDA Free 9.0 on your computer.
InstallBuilder
< Back
Next >
Cancel

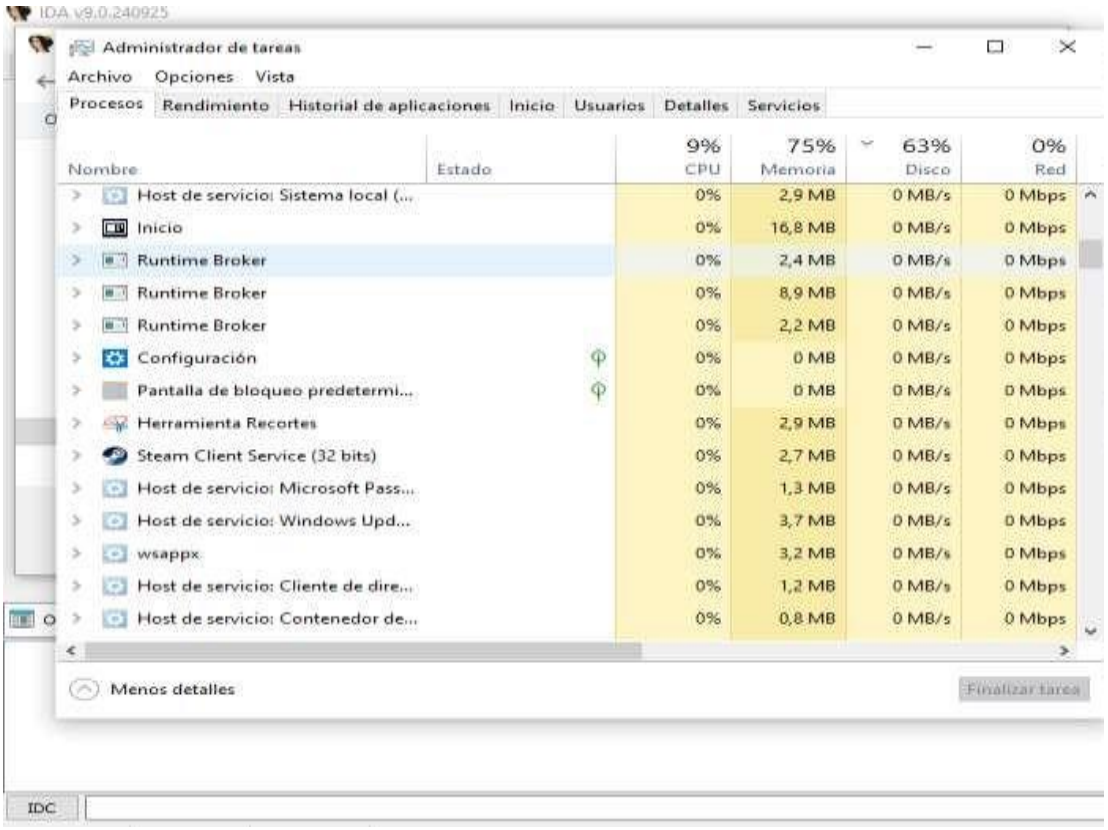

Setup
Completing the IDA Free 9.0 Setup Wizard
Setup has finished installing IDA Free 9.0 on your computer.
IDA Freeware
Version 9.0
Hex-Rays © 2024
< Back
Finish
Cancel

Paso 3:

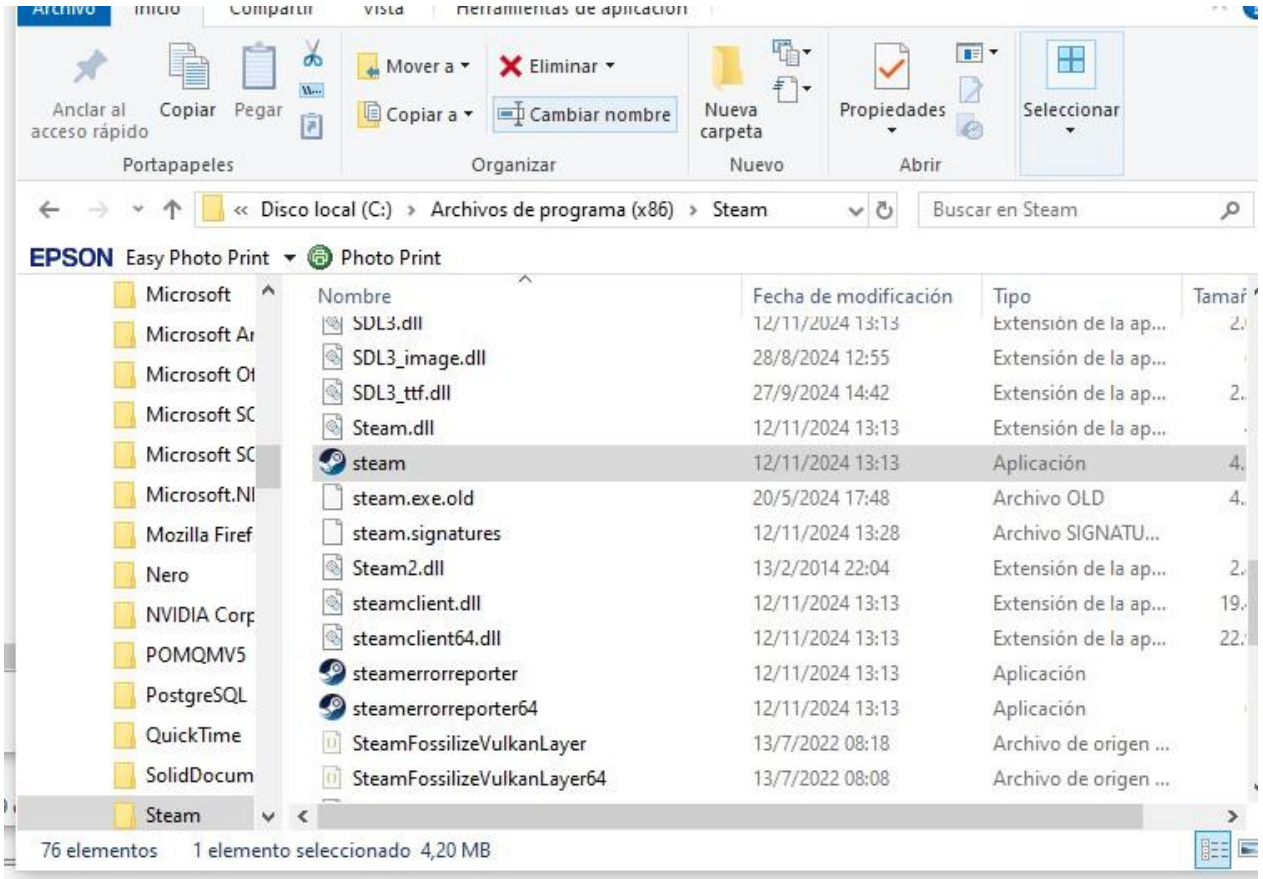

About
IDA - The Interactive Disassembler
Version 9.0.240925 Windows x64 (64-bit address size)
(c) 2024 Hex-Rays SA
Freeware version with the following limitations:
1. Only for non-commercial use
2. Without technical support
3. Only supports x86/x64 code
4. Only PE/ELF/Mach-O files are supported
5. IDAPython is not available
For commercial use please acquire the full version
www.hex-rays.com
OK

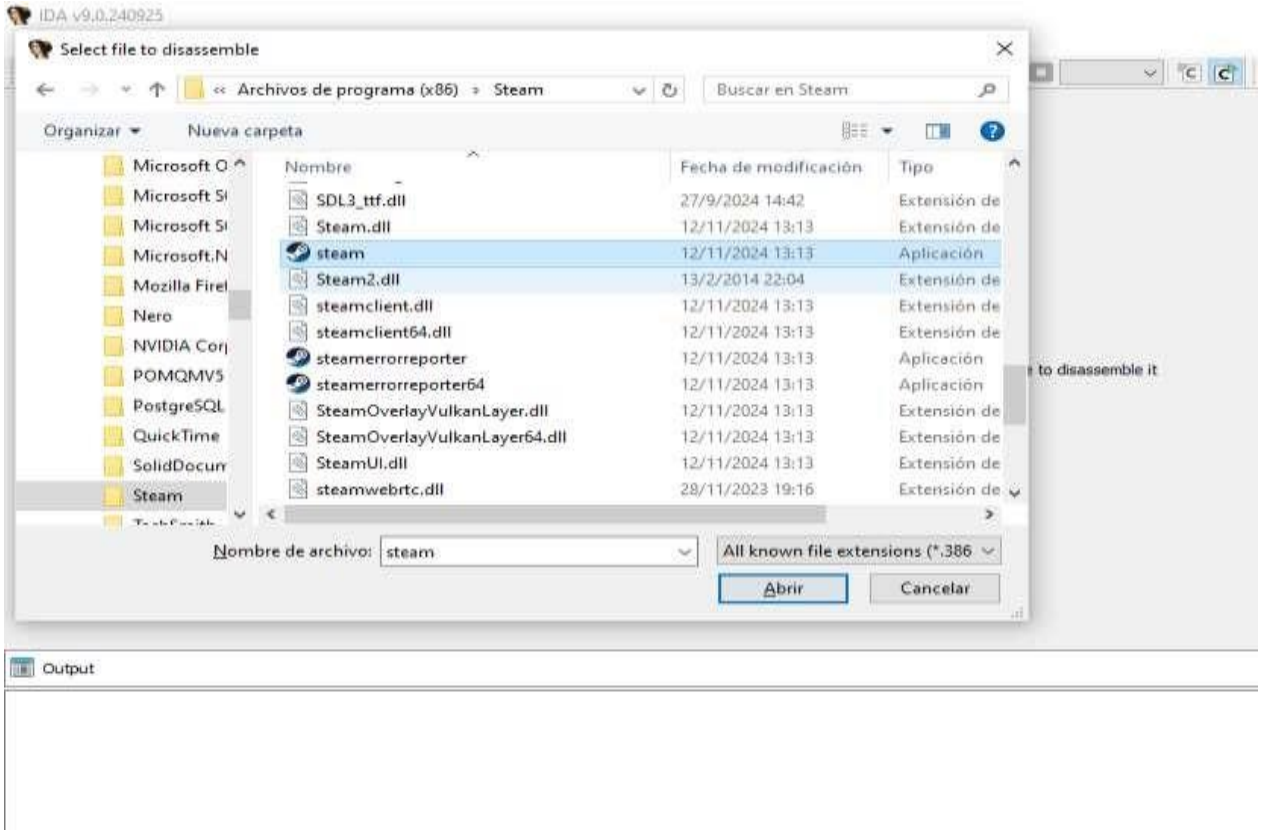

IDA: Quick start
New
Disassemble a new file
Go
Work on your own
Previous
Load the old disassembly
Display at startup

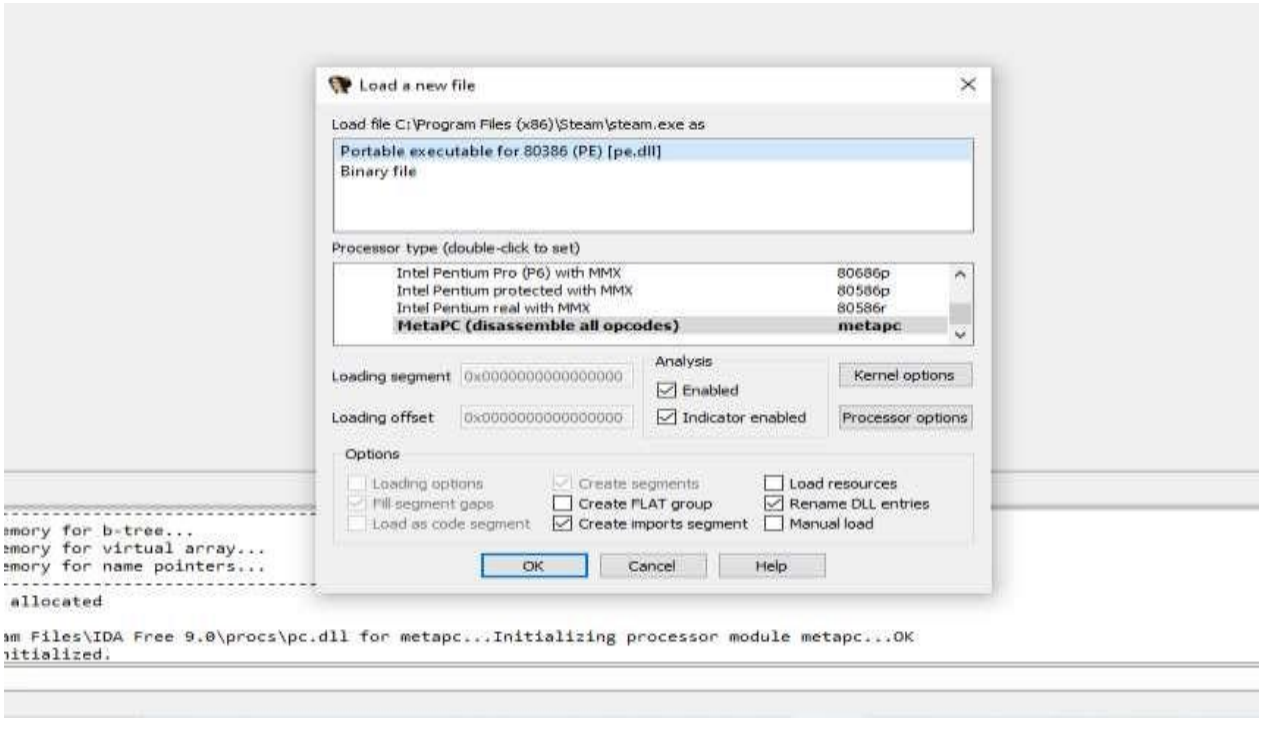

Select file to disassemble
Archivos de programa › IDA Free 9.0
Buscar en IDA Free 9.0
Organizar
Nueva carpeta
IDA Free 9.0
cfg
idc
ids
loaders
plugins
procs
sig
themes
til
Intel
Internet Exp
Nombre
Fecha de modificación
Tipo
30/11/2024 20:37
25/9/2024 09:21
clp64.dll
ida.dll
ida
Nombre de archivo:
All known file extensions (*.386
Abrir
Cancelar

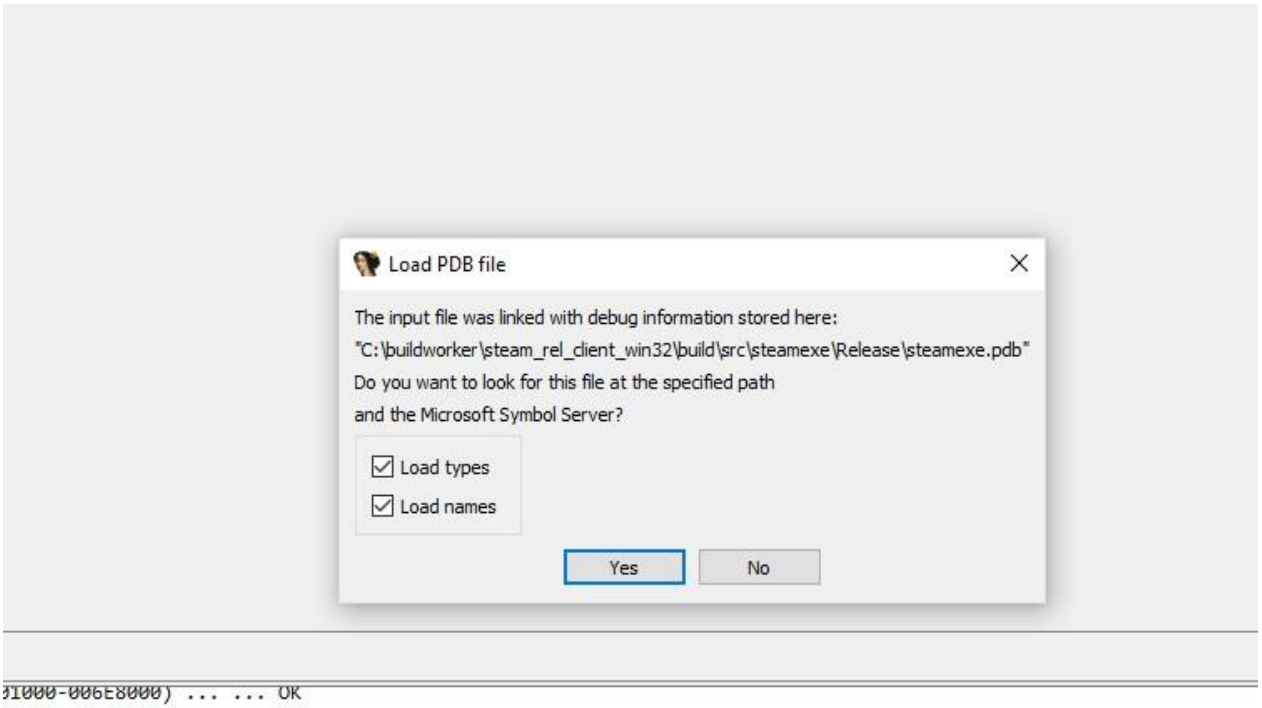


Abrimos el administrador de tareas y hacemos un clic derecho seleccionar “Abrir ubicación del archivo”




IDA v9.0.240925
Select file to disassemble
« Archivos de programa (x86) » Steam
Buscar en Steam
Organizar
Nueva carpeta
Nombre
Fecha de modificación
Tipo
SDL3_ttf.dll 27/9/2024 14:42 Extensión de
Steam.dll 12/11/2024 13:13 Extensión de
steam 12/11/2024 13:13 Aplicación
Steam2.dll 13/2/2014 22:04 Extensión de
steamclient.dll 12/11/2024 13:13 Extensión de
steamclient64.dll 12/11/2024 13:13 Extensión de
steamerrorreporter 12/11/2024 13:13 Aplicación
steamerrorreporter64 12/11/2024 13:13 Aplicación
SteamOverlayVulkanLayer.dll 12/11/2024 13:13 Extensión de
SteamOverlayVulkanLayer64.dll 12/11/2024 13:13 Extensión de
SteamUI.dll 12/11/2024 13:13 Extensión de
steamwebrtc.dll 28/11/2023 19:16 Extensión de
Microsoft O
Microsoft Si
Microsoft Si
Microsoft.N
Mozilla Firel
Nero
NVIDIA Cor
POMQMV5
PostgreSQL
QuickTime
SolidDocum
Steam
Nombre de archivo: steam
All known file extensions (*.386
Abrir
Cancelar
to disassemble it
Output

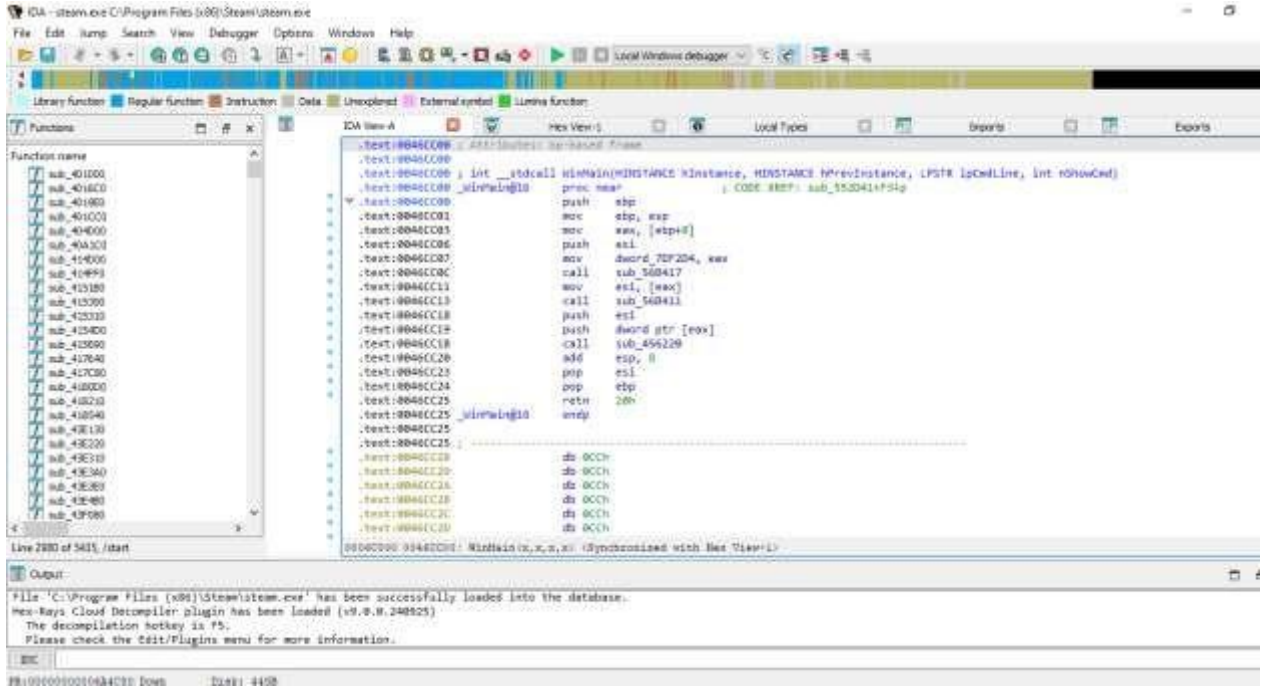

Load a new file
Load file C:\Program Files (x86)\Steam\steam.exe as
Portable executable for 80386 (PE) [pe.dll]
Binary file
Processor type (double-click to set)
Intel Pentium Pro (P6) with MMX 80686p
Intel Pentium protected with MMX 80586p
Intel Pentium real with MMX 80586r
MetaPC (disassemble all opcodes) metapc
Loading segment 0x0000000000000000
Loading offset 0x0000000000000000
Analysis
Enabled
Indicator enabled
Kernel options
Processor options
Options
Loading options
Fill segment gaps
Load as code segment
Create segments
Create FLAT group
Create imports segment
Load resources
Rename DLL entries
Manual load
OK
Cancel
Help
emory for b-tree...
emory for virtual array...
emory for name pointers...
allocated
am Files\IDA Free 9.0\procs\pc.dll for metapc...Initializing processor module metapc...OK
nitialized.

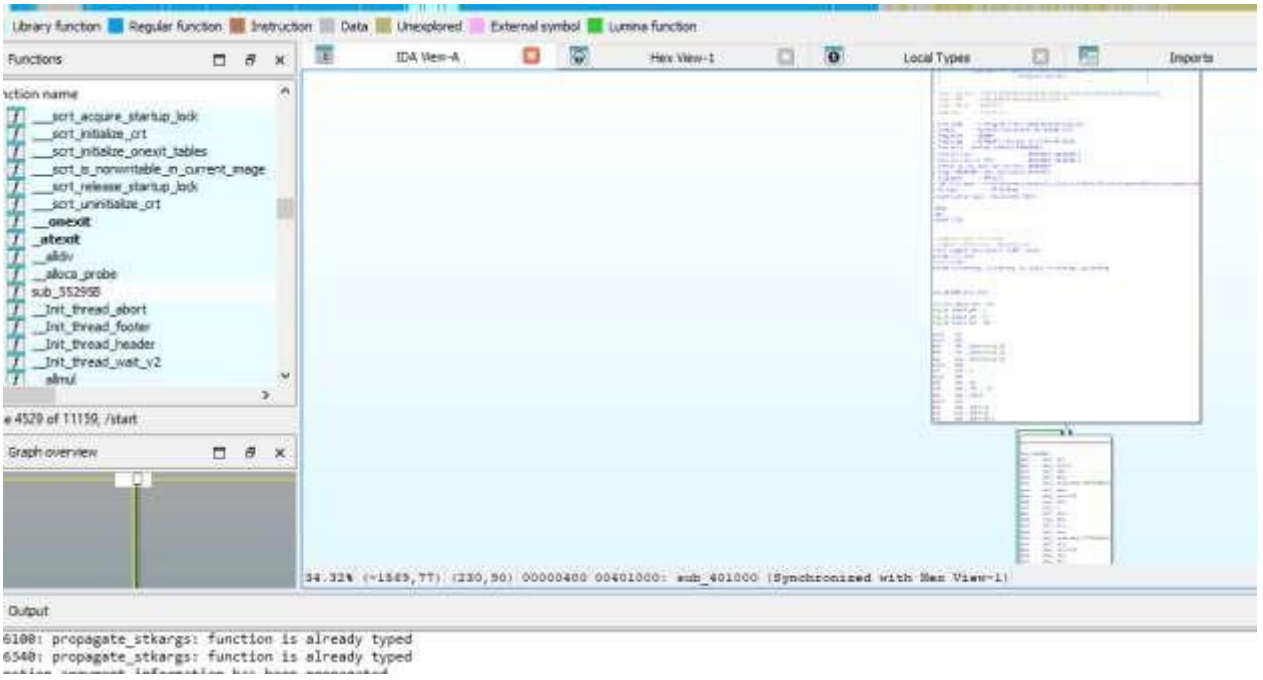


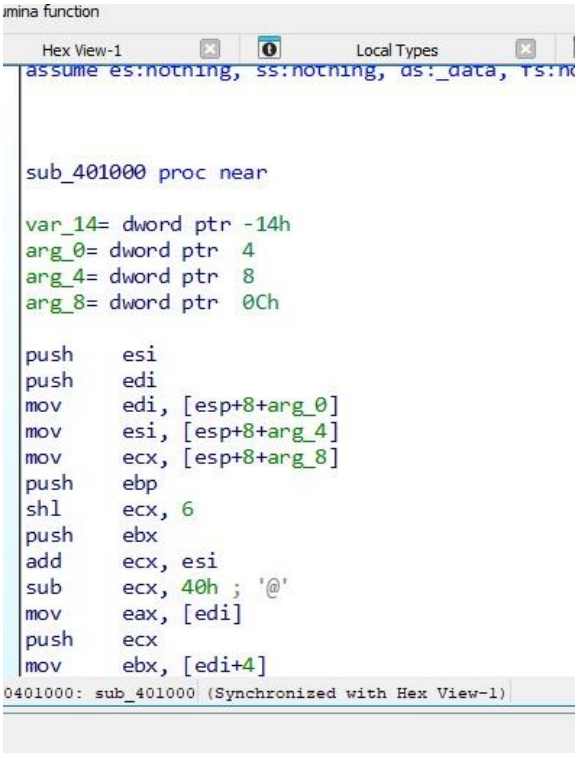

```
01000-006E8000) ... ... OK
E8000-007CE000) ... ... OK
CE000-00863000) ... ... OK


E8558-007CE000) ... ... OK
ll is used for module WS2_32...
dll is used for module WSOCK32...
```

PASO 4:




Library function
Regular function
Instruction
Data
Unexplored
External symbol
Lumina function
Functions
IDA View-A
Hex View-1
Local Types
Imports
Graph overview
Output
6100: propagate_stkargs: function is already typed
6540: propagate_stkargs: function is already typed


umina function
Hex View-1
Local Types
sub_401000 proc near
var_14= dword ptr -14h
arg_0= dword ptr 4
arg_4= dword ptr 8
arg_8= dword ptr 0Ch
push esi
push edi
mov edi, [esp+8+arg_0]
mov esi, [esp+8+arg_4]
mov ecx, [esp+8+arg_8]
push ebp
shl ecx, 6
push ebx
add ecx, esi
sub ecx, 40h ; '@'
mov eax, [edi]
push ecx
mov ebx, [edi+4]
0401000: sub_401000 (Synchronized with Hex View-1)