

<div><div><div><div><div><div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div></div></div><div><div><div><div><div><div></div></div></div><div><div><div><div><div><div></div></div></div></div></div></div><div><div><div><div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div></div>			
--	--	--	--

Responda las siguientes preguntas de **MANERA CONCISA**

1) ¿Qué es el 'stack' en el contexto del lenguaje ensamblador y cómo se utiliza? **(10 pts)**

R. En lenguaje ensamblador, el stack es una estructura de datos tipo pila (LIFO: último en entrar, primero en salir) usada para almacenar temporalmente datos, direcciones de retorno y registros. Se utiliza con las instrucciones PUSH (para guardar datos en el stack) y POP (para recuperar datos). Es clave en llamadas a funciones y gestión de variables locales.

2) Describe un escenario práctico donde el uso de ensamblador sería más ventajoso que el uso de un lenguaje de alto nivel. **(10 pts)**

R. El ensamblador es más ventajoso en escenarios donde se requiere control total del hardware y máxima eficiencia, como en:

Sistemas embebidos o de tiempo real: Por ejemplo, programar microcontroladores en dispositivos médicos o automotrices, donde es crucial optimizar el rendimiento y minimizar el consumo de recursos.

Esto permite aprovechar al máximo las capacidades del hardware y reducir el tamaño del código.

3) Explique cada línea del siguiente código del lenguaje ensamblador y diga que es lo que se está haciendo **(20 pts)**

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

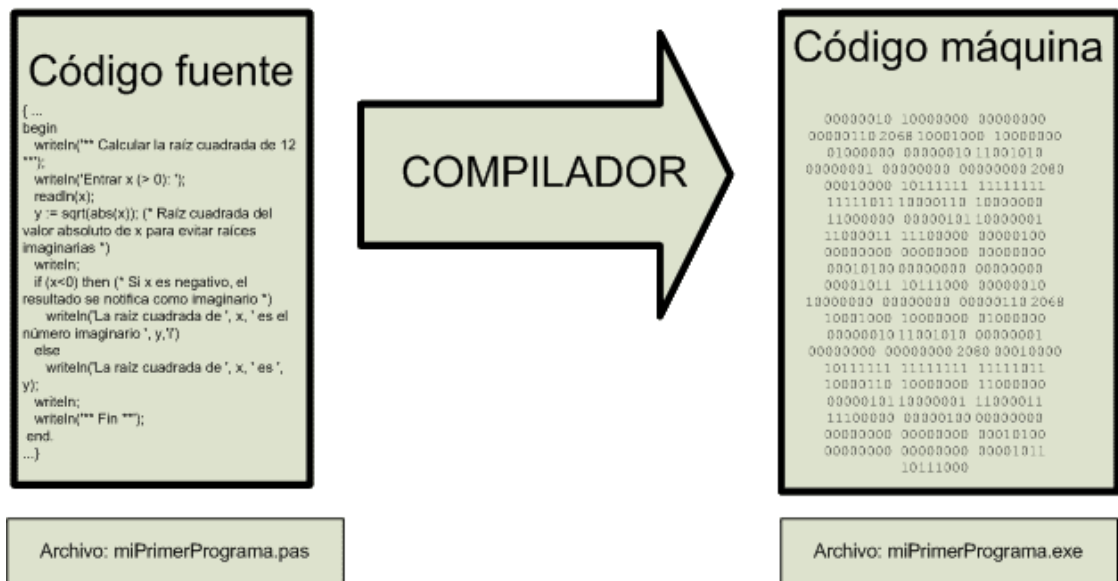
R. **MOV AX, 5:** Mueve el valor 5 al registro AX y se inicializa el registro AX con el valor 5.

MOV BX, 10: Mueve el valor 10 al registro BX y se inicializa el registro BX con el valor 10.

ADD AX, BX: Suma el contenido del registro BX al registro AX y el valor de BX 10 se suma al valor de AX 5, y el resultado 15 se almacena en AX.

MOV CX, AX: Mueve el contenido del registro AX al registro CX y el resultado de la suma 15 se copia al registro CX y el resultado final es el valor 15 que está almacenado en el registro CX.

4) Explique detalladamente cómo funcionan los compiladores **(10 pts)**



R. Los compiladores funcionan de la siguiente manera:

Análisis del código: Revisa que el código no tenga errores de escritura o lógica.

Traducción: Convierte el código a un formato intermedio y luego a código máquina.

Optimización: Mejora el código para que sea más eficiente al ejecutarse.

Generación de ejecutable: Crea un archivo que la computadora puede ejecutar directamente, como un .exe.

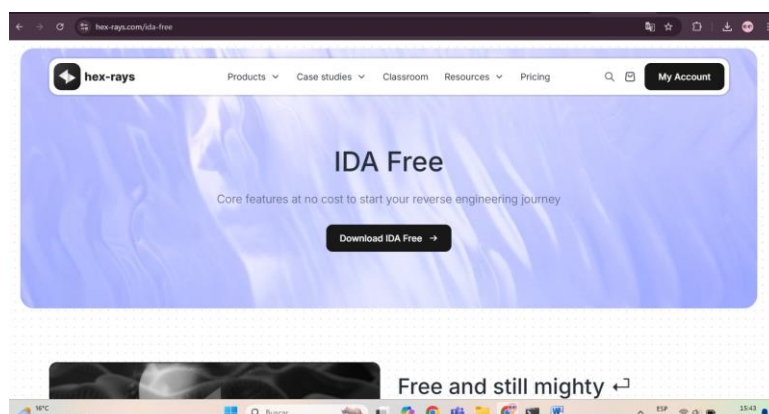
5) Realizar sus propias capturas de pantalla del siguiente procedimiento:

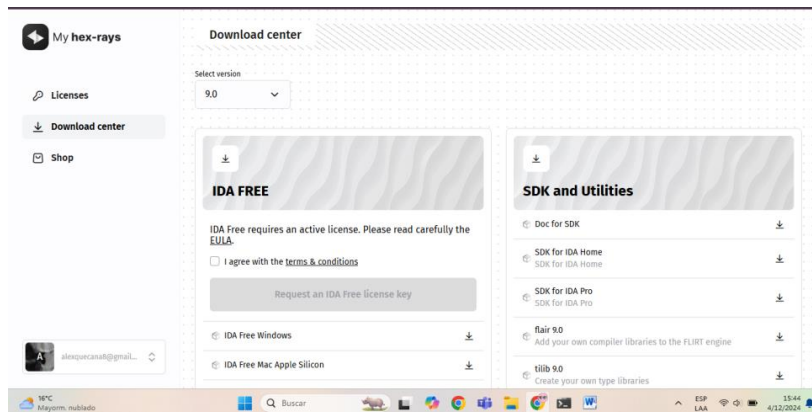
(50 pts)

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:

Descargar el software IDA FREE

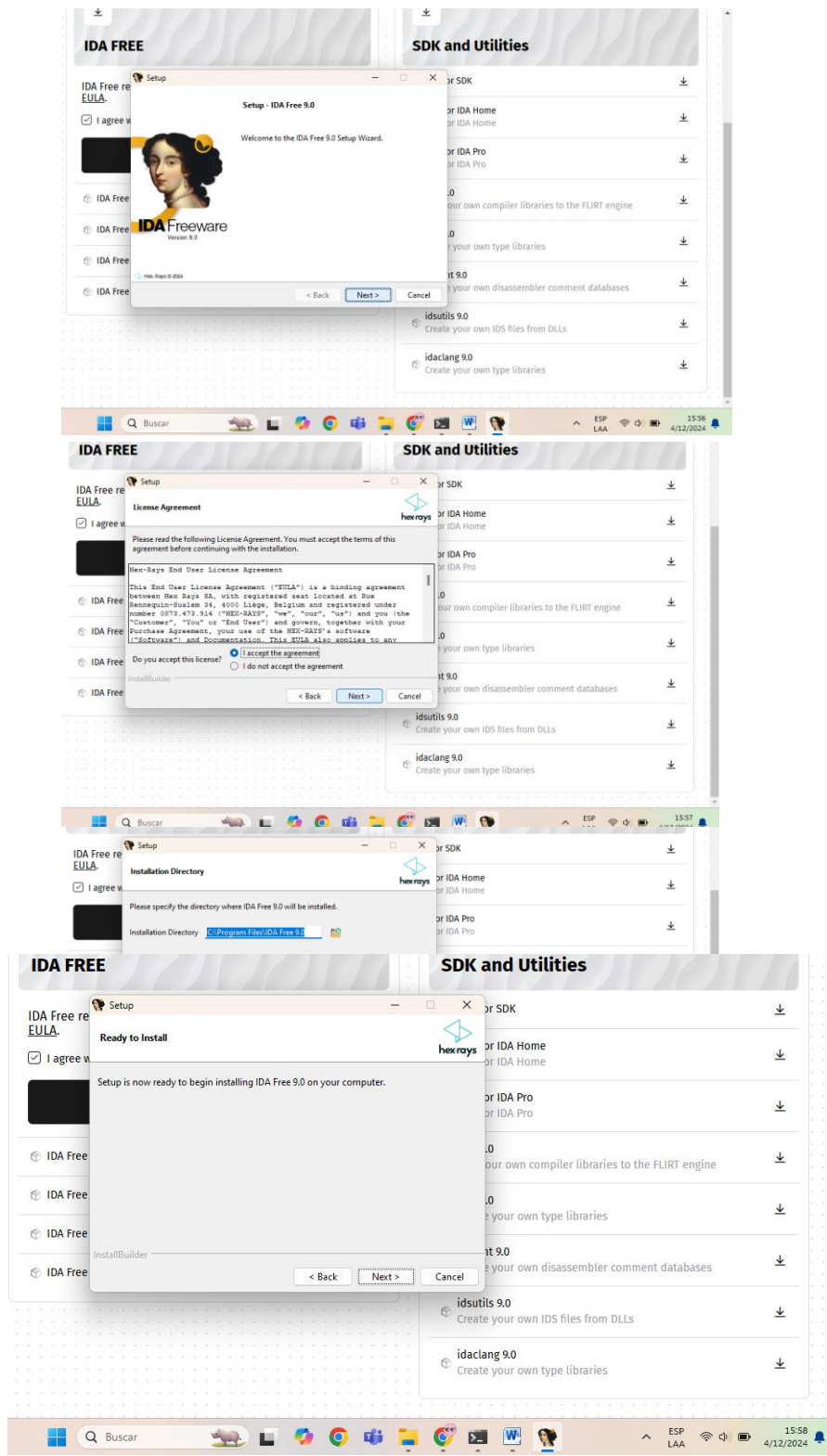




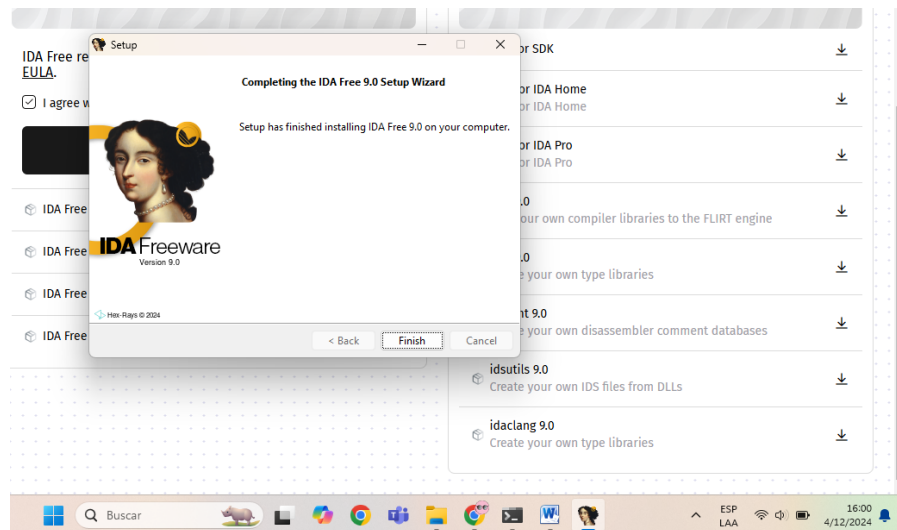
Paso 2:

Instalación

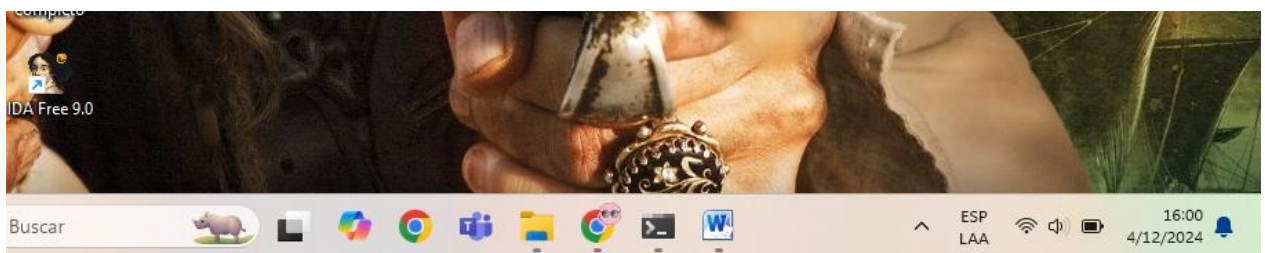
Seleccionar Next



finalizar

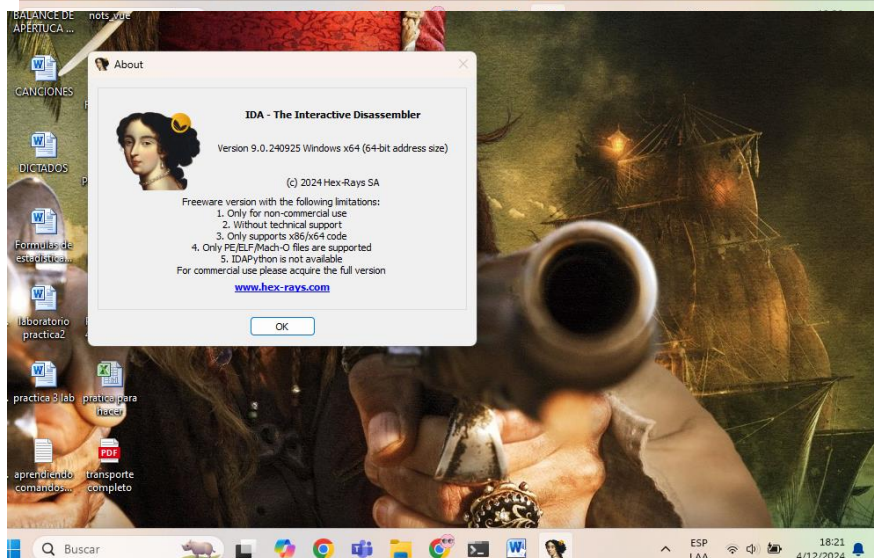
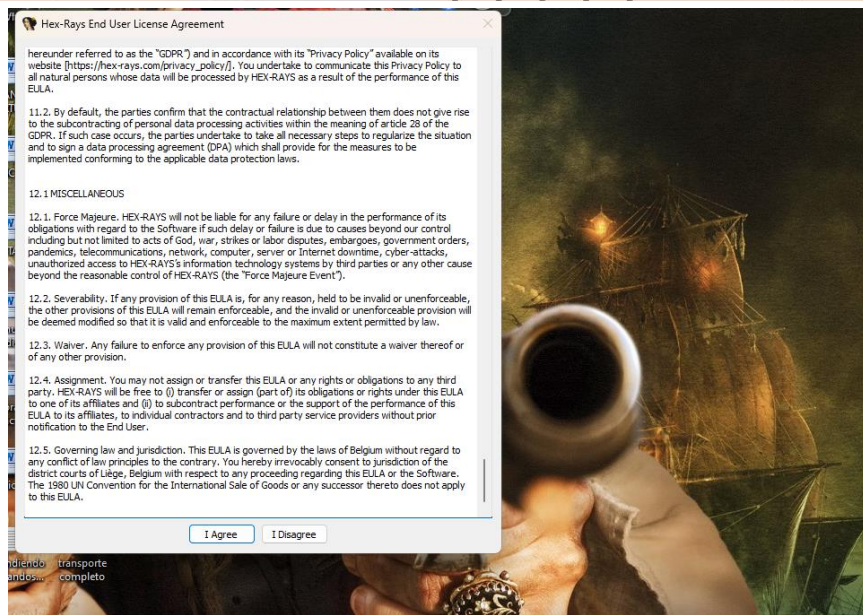
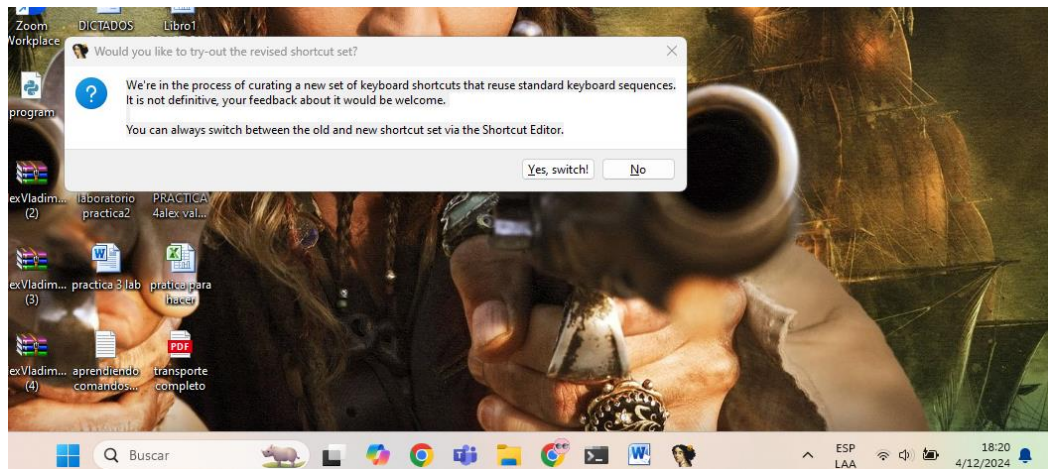


IDA INSTALADO

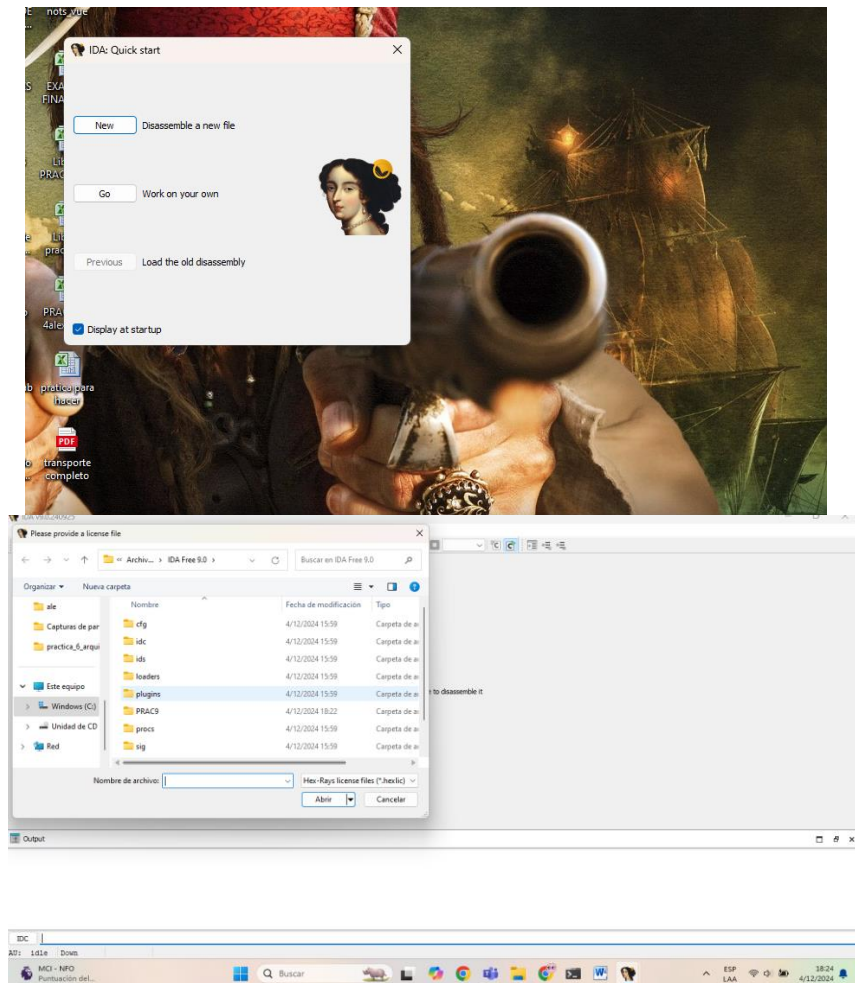


Paso 3:

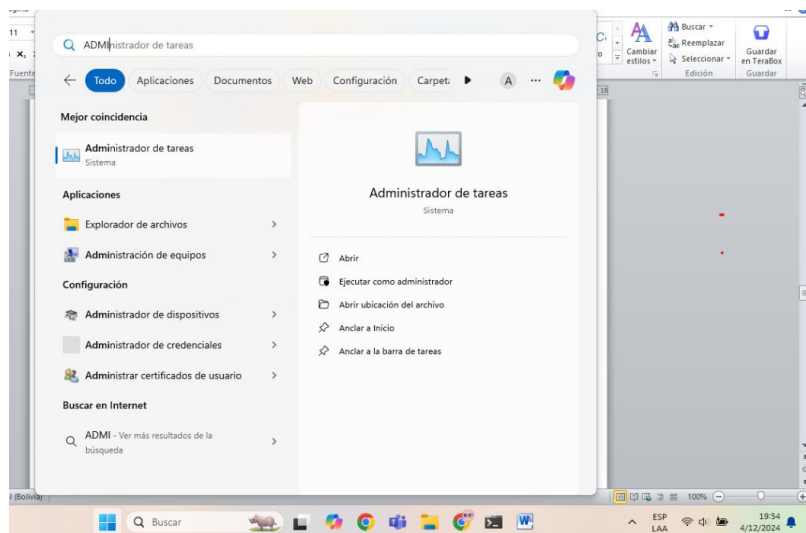
Procederemos a abrir un servicio en Windows



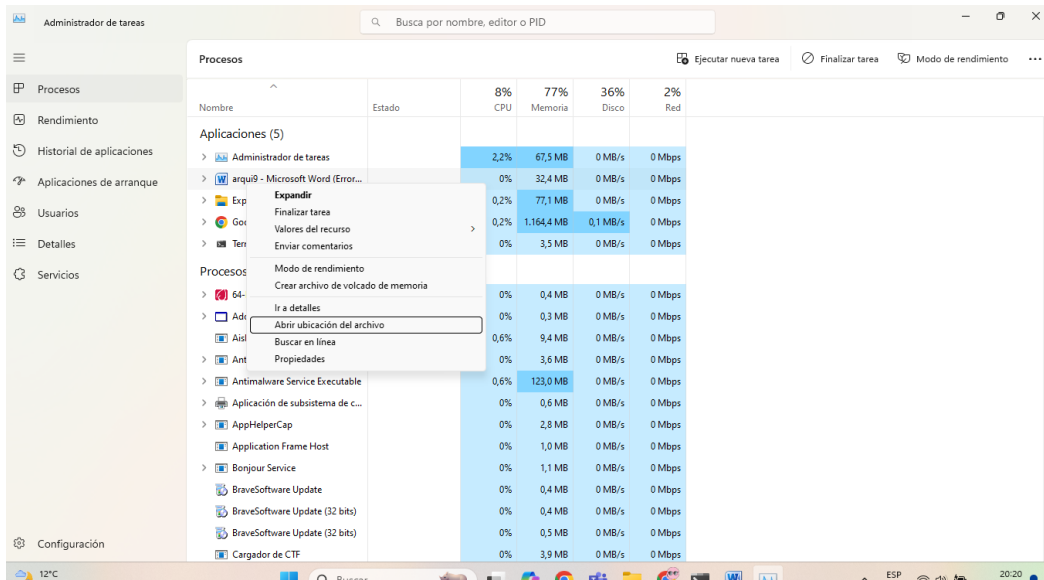
Lo que deberá hacer ahora es seleccionar "New"



Ahora deberá seleccionar algún servicio de su administrador de tareas,

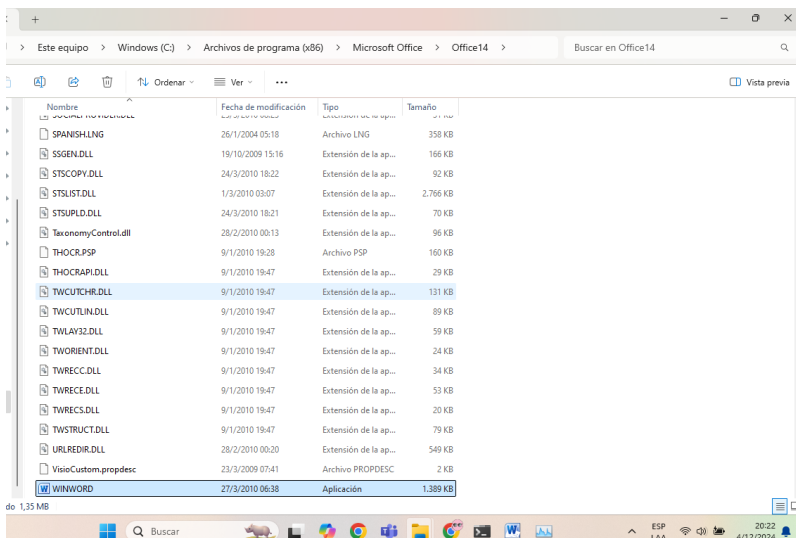


primeramente, vamos a abrir el administrador de tareas

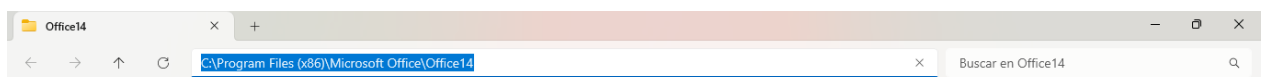


Ahora en la pestaña procesos deberá buscar cualquier servicio que se este ejecutando en tiempo real, y hacer un clic izquierdo sobre el servicio que le interesará ver el código ensamblador de este y después con un clic derecho seleccionar “Abrir ubicación del archivo”

Una vez hecho esto se abrirá la ubicación del servicio



Ahora se deberá copiar la ruta en donde esta este servicio el cual es en este caso



Una vez copiada esta ruta se deberá colocar en la ventana donde IDA nos pidió que se debe añadir un servicio a analizar

