

**ОТЧЕТ О ВЫПОЛНЕНИИ**

**практической работы № 2**

**по предмету МДК 3.2**

**Управление проектами**

Выполнил: ст. гр. 2ИСП11-31ВБ Синицын О. Е.

Специальность: 09.02.07

Информационные системы и программирование

Проверил: преподаватель Голиков Д. А.

Москва 2023

**Тема:** Дизассемблирование и отладка программ**.**

**Цель работы:** дизассемблирование и отладка с помощью IDA Pro простейшей программы.

**Ход работы:**

Открываем программу IDA Pro

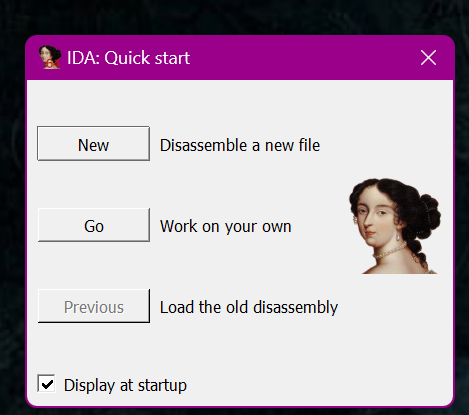


Рис.1

Нажав на кнопку «New» выбираем файл для работы с ним

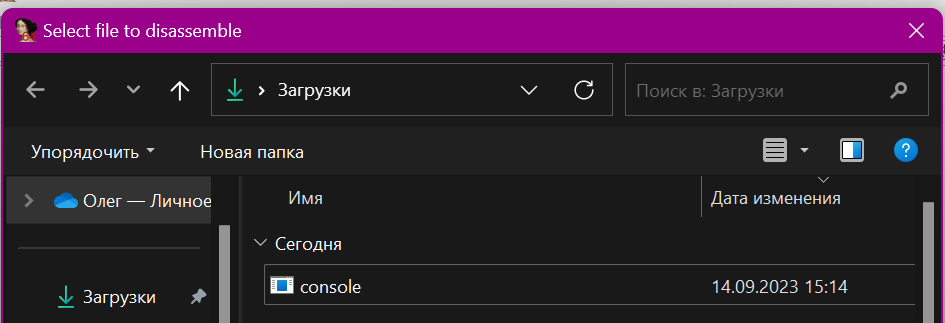


Рис.2

Открываем окно подтверждения

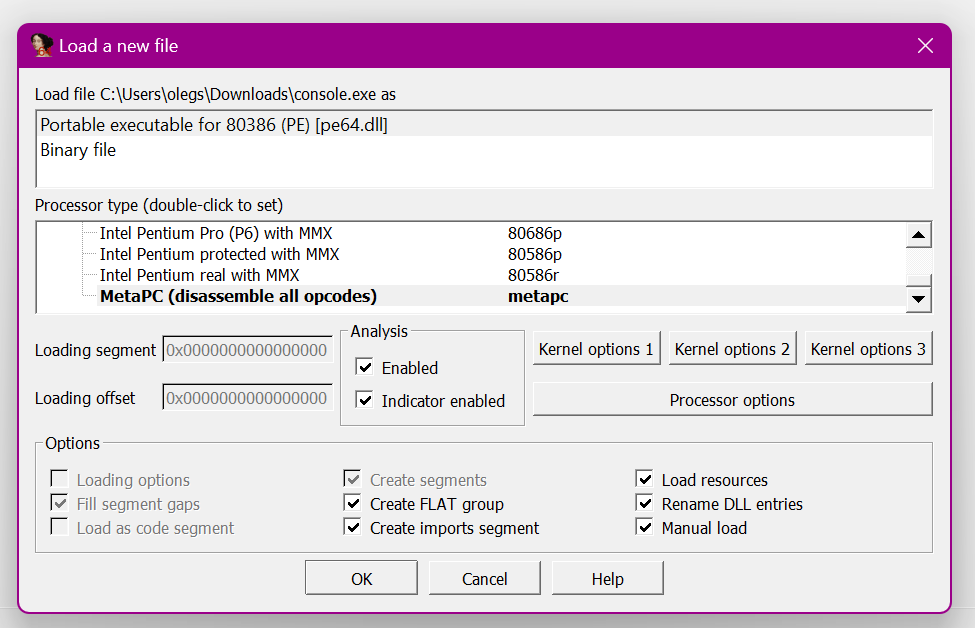


Рис.3

Получаем результаты анализа и дизассемблирования простейшей программы

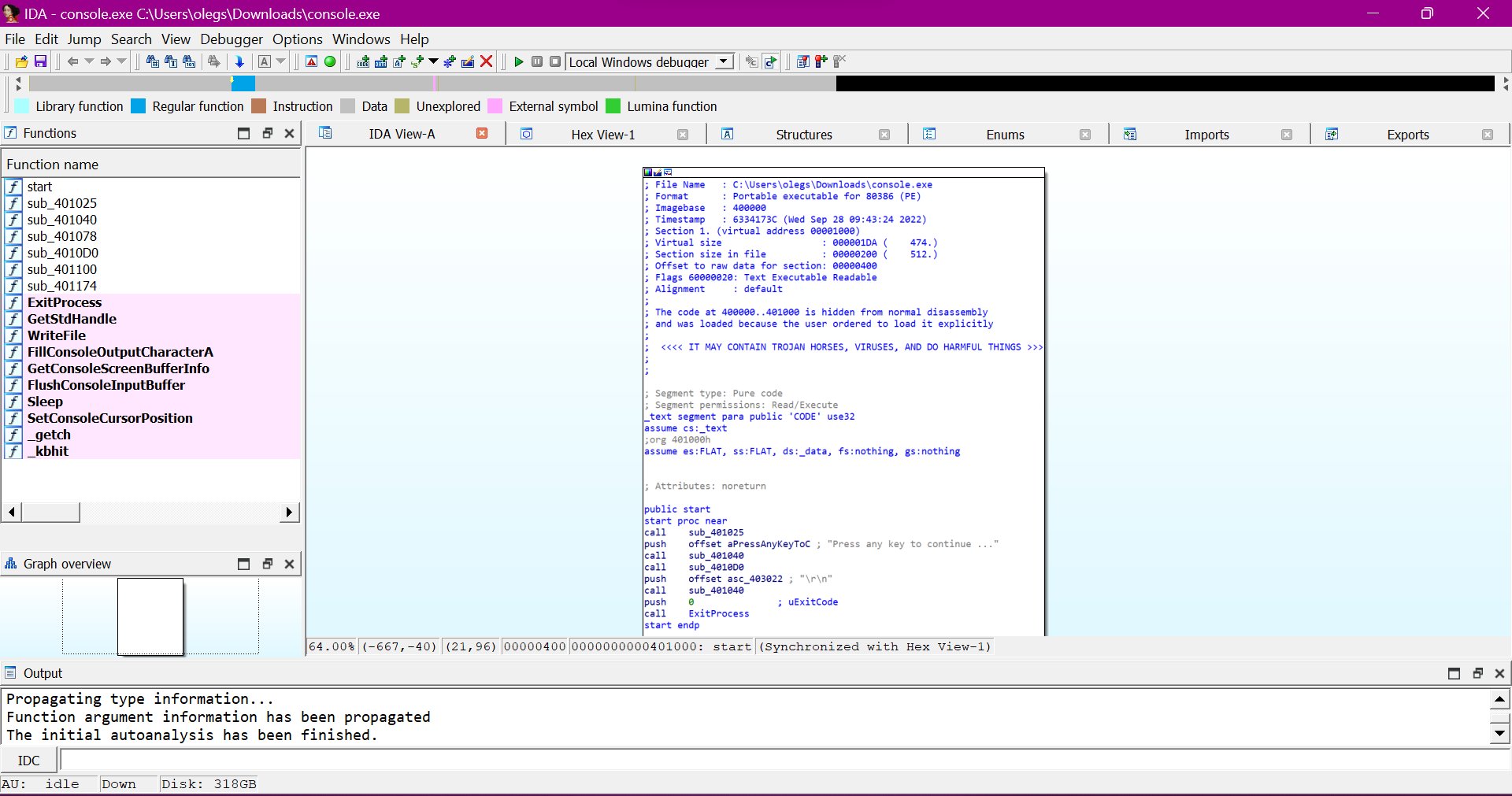


Рис.4

Предоставляю список имен простейшей программы

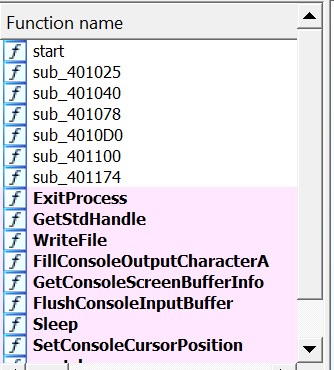


Рис.5

Заходим в меню «Debbuger»

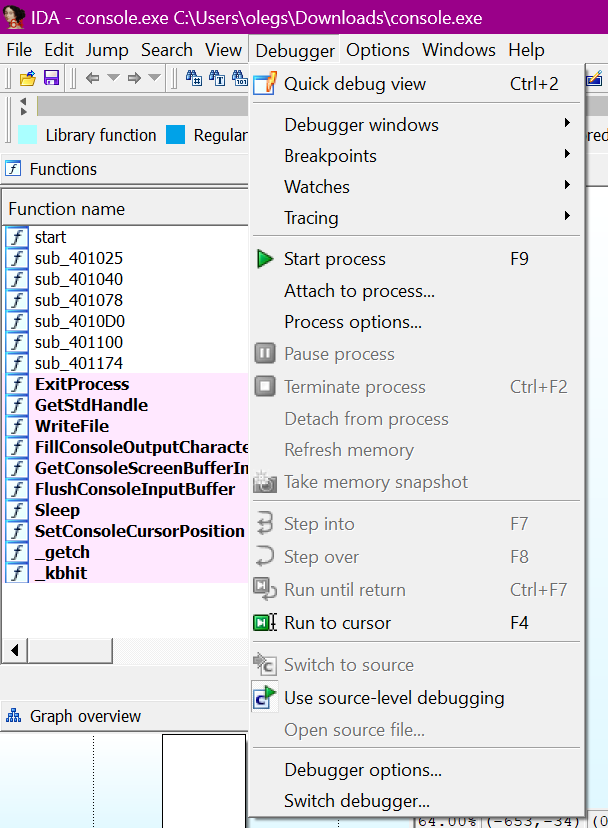


Рис. 6

В данном меню выбираем «Yes»

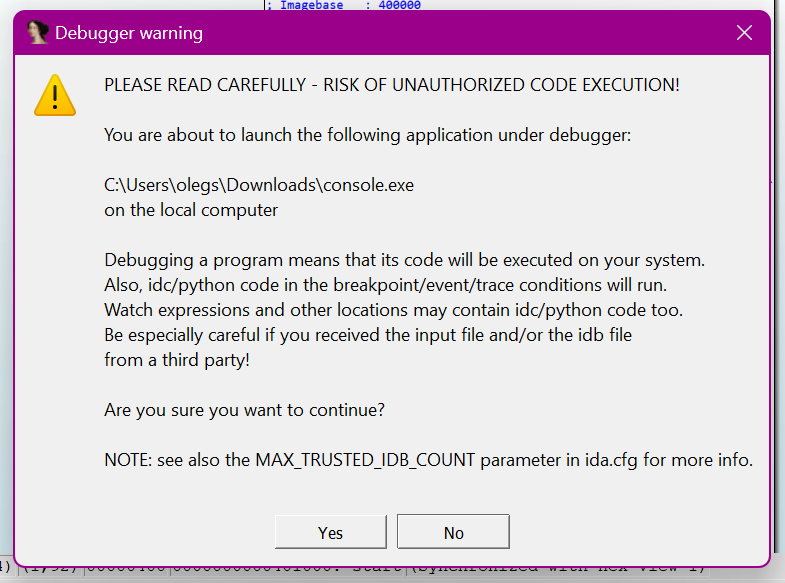


Рис.7

Окно с исполняемыми командами программы и окно отображающее содержимое регистров общего назначения

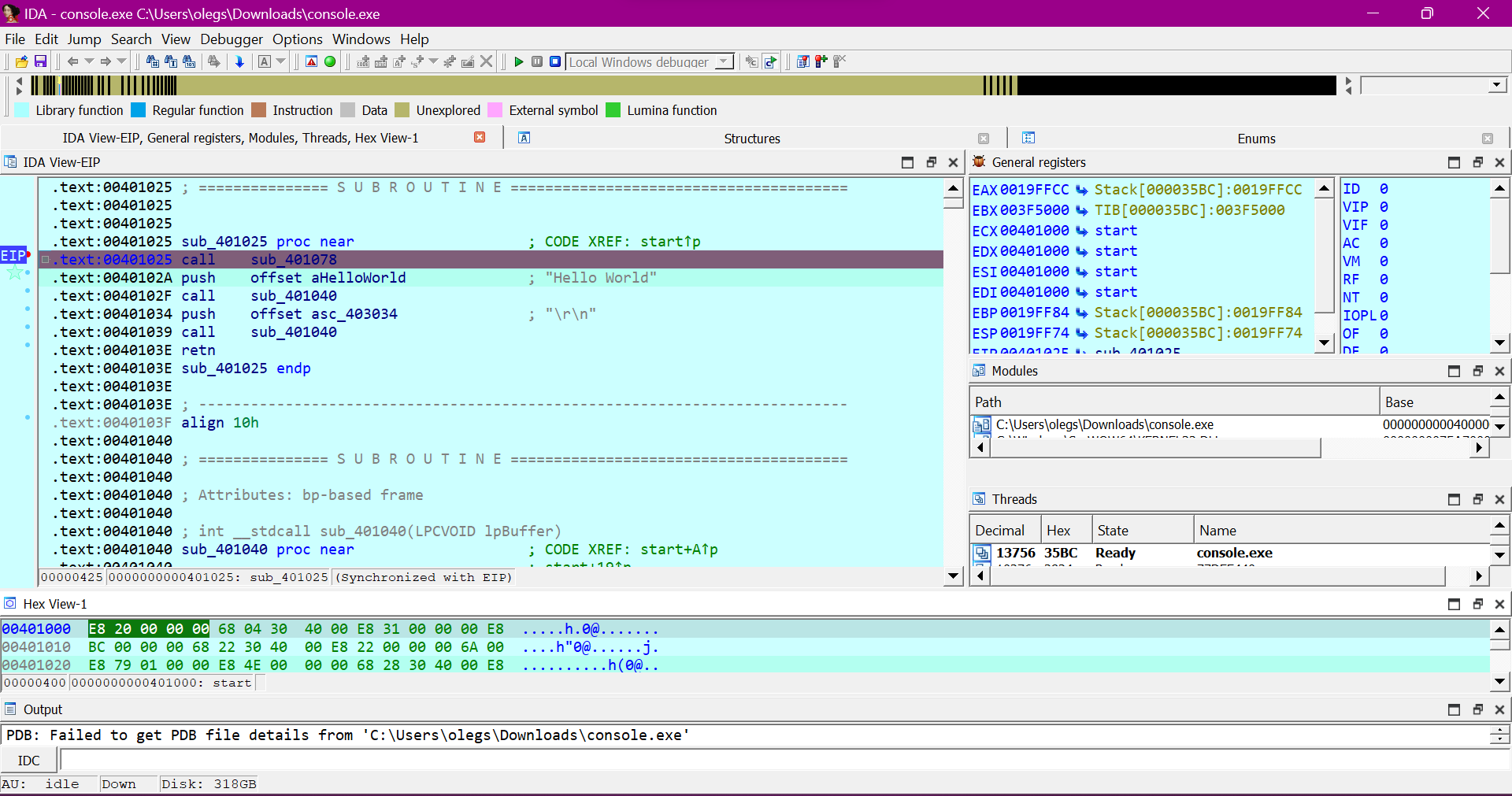


Рис.8

Переходим в «Debbuger - Terminate Process»

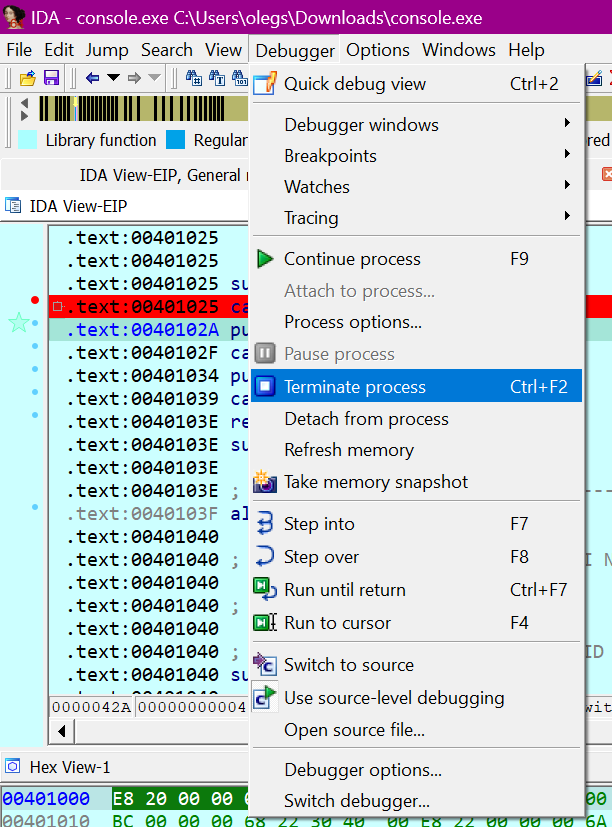


Рис. 9

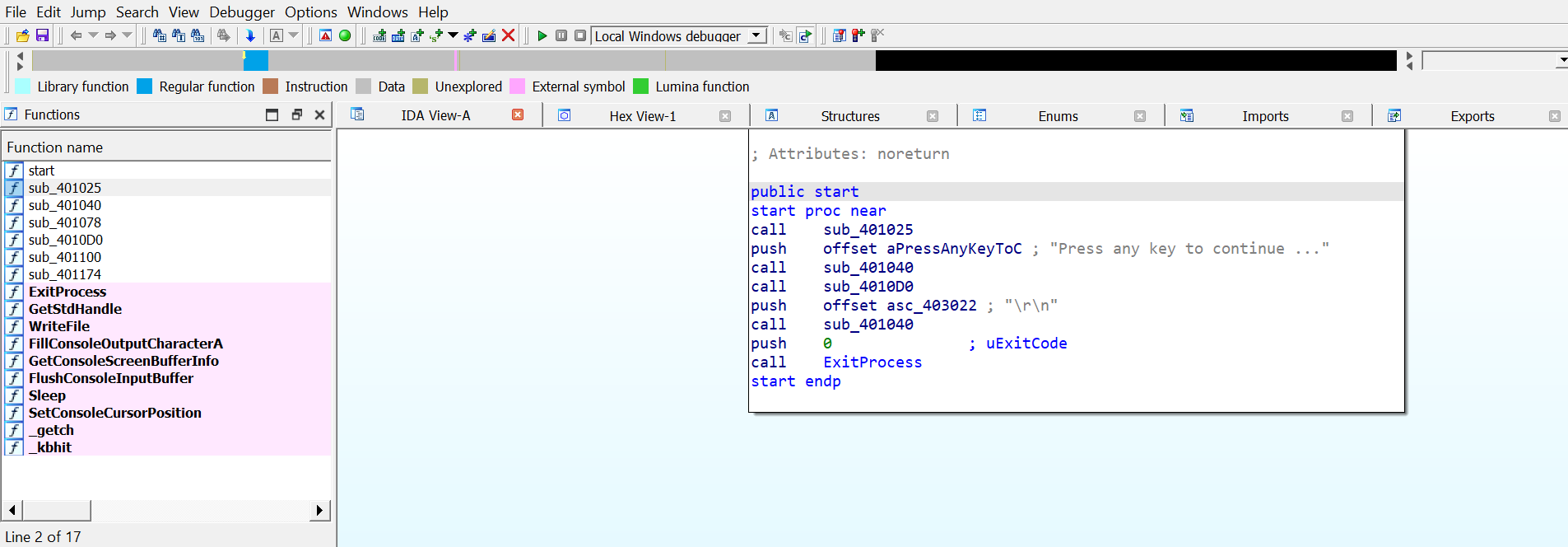


Рис.10

Дизассемблирование подпрограмм:

start

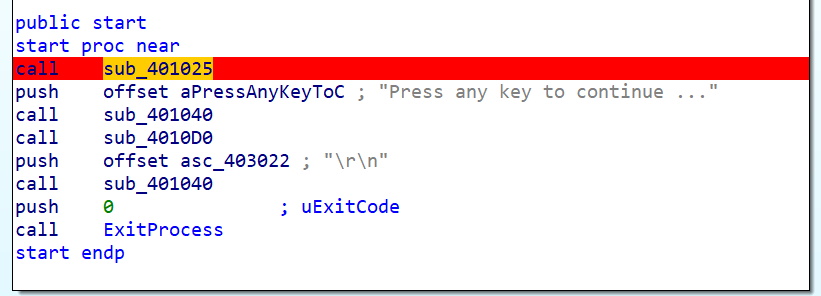


Рис. 11

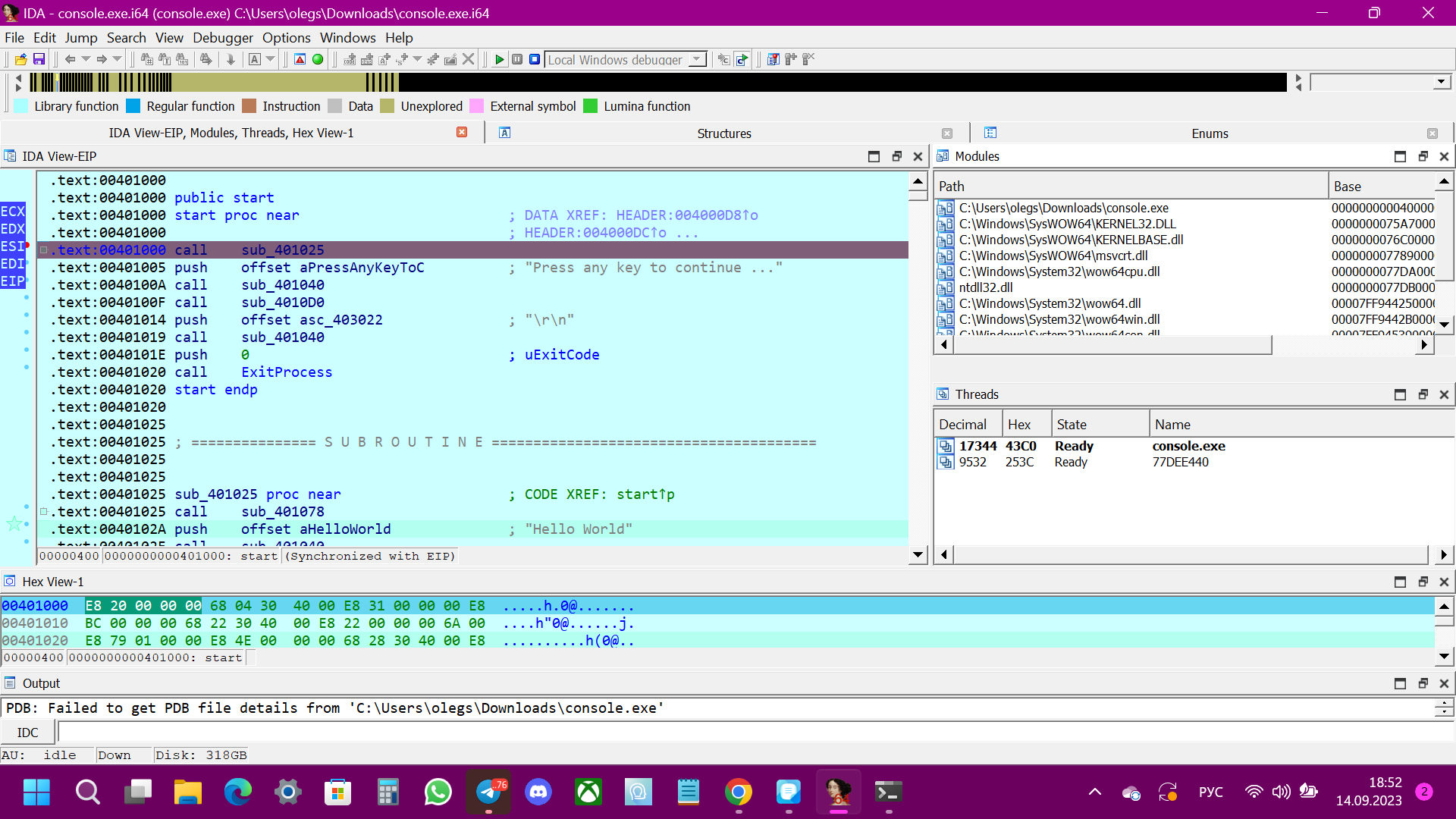


Рис. 12

sub\_401025

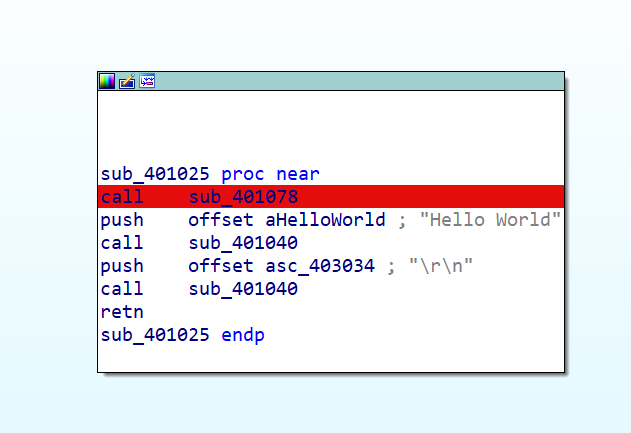


Рис.13

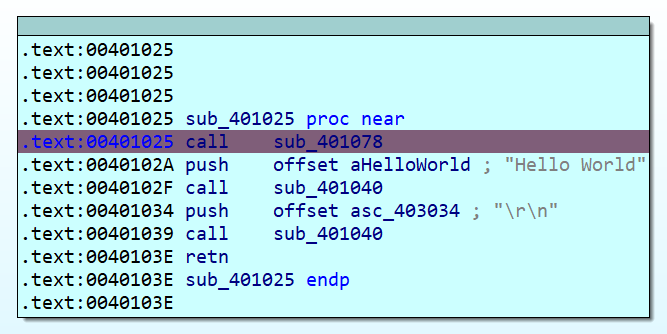


Рис.14

sub\_401040

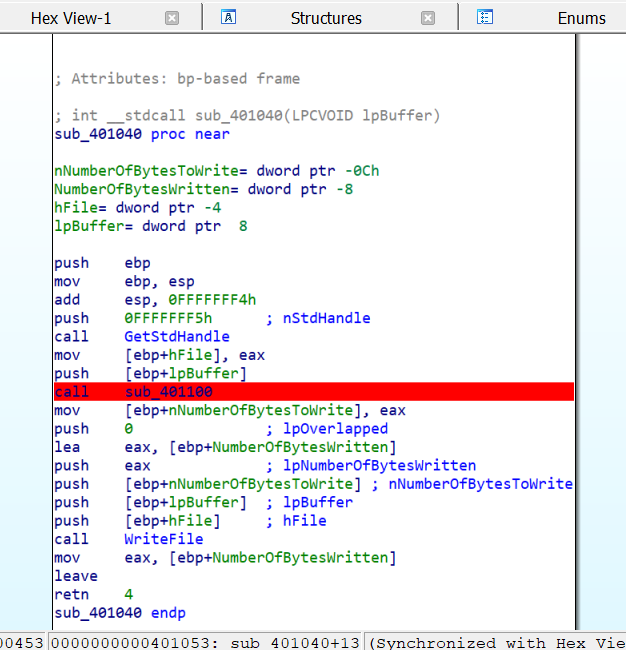


Рис.15

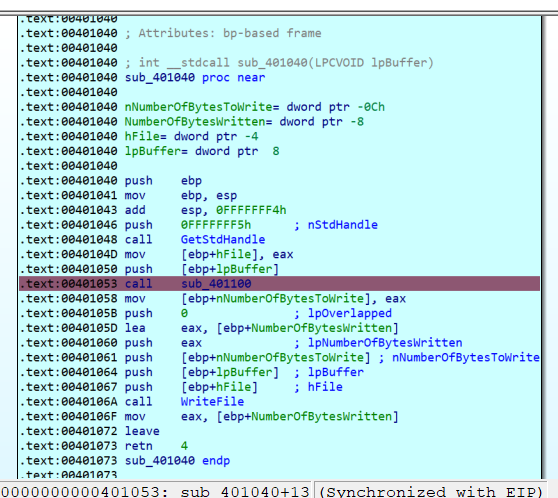


Рис.16

sub\_401078



Рис.17



Рис.18

sub\_4010D0

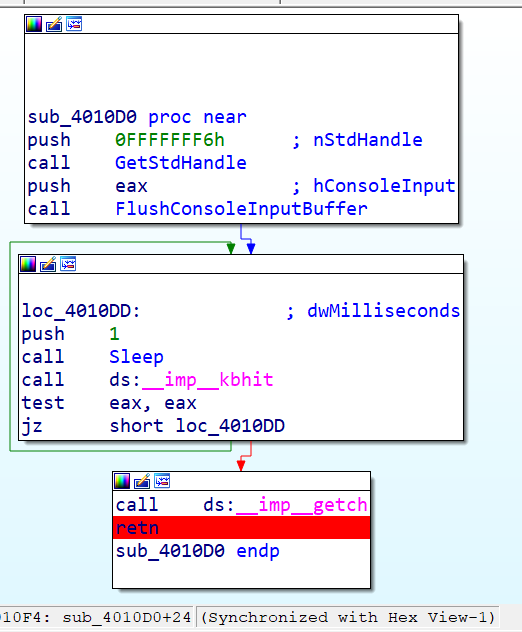


Рис.19

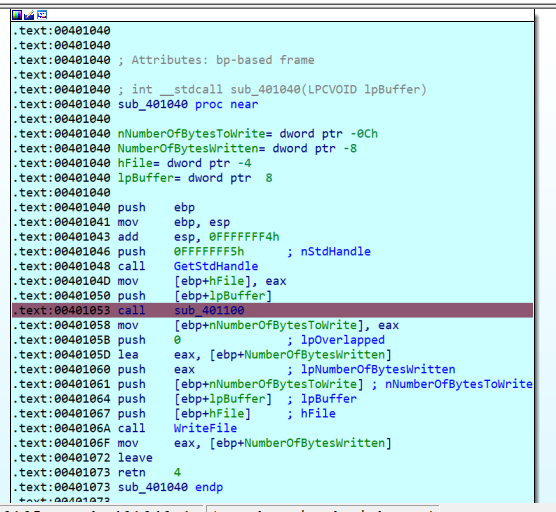


Рис.20

sub\_401100

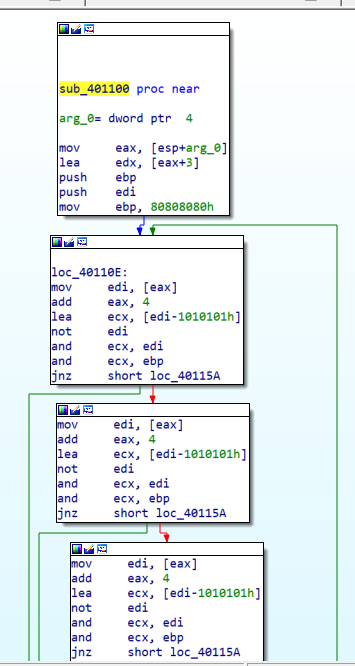


Рис.21

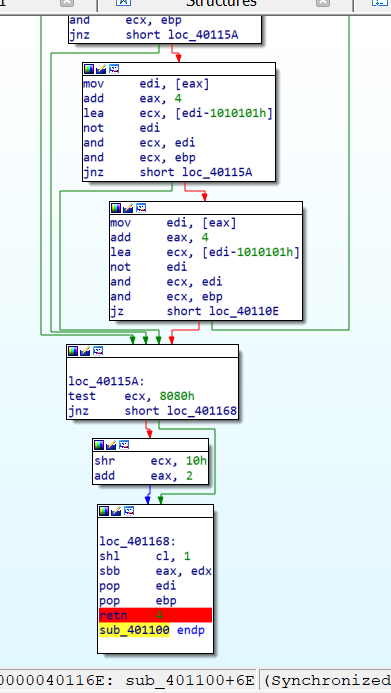


Рис.22

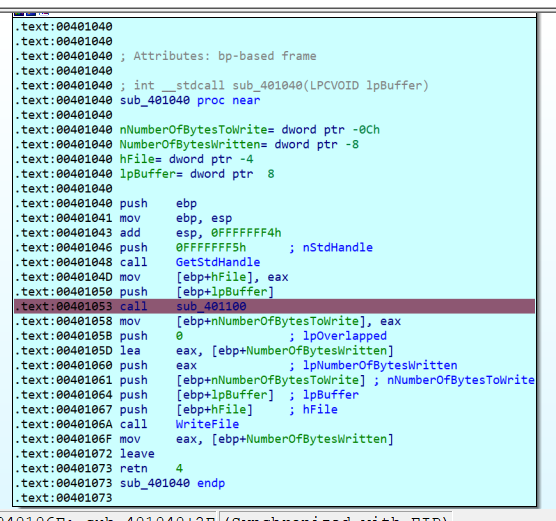


Рис.23

sub\_401174

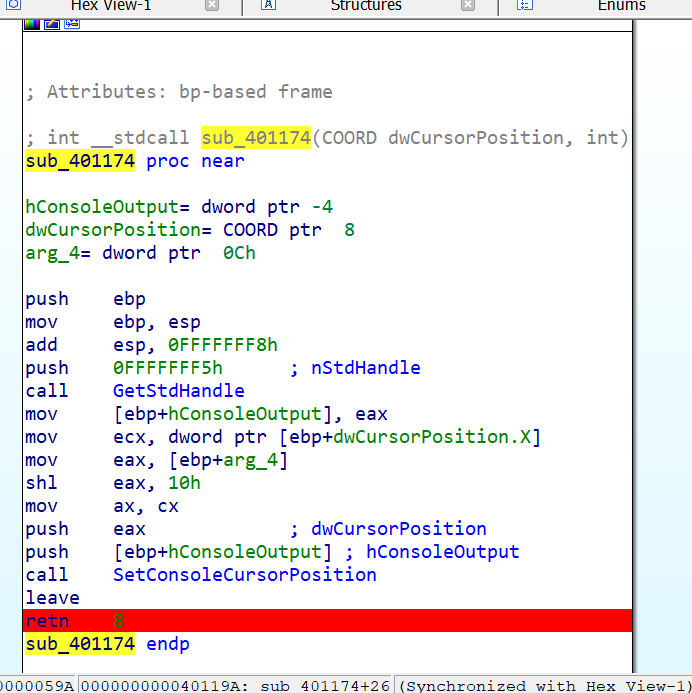


Рис.24

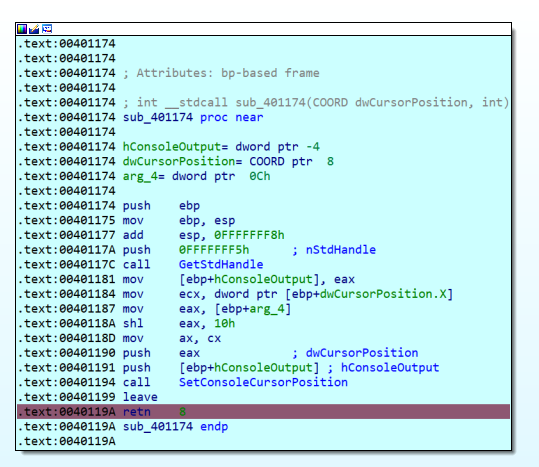


Рис.25

**Ответы на контрольные вопросы:**

**1. В чем отличие между дизассемблером и отладчиком?**

Отладчик предназначен для поиска ошибок в программе, а дизассемблерпреобразует машинный код в текст программы на языке ассемблера.

**2. Каковы основные и дополнительные возможности интерактивного дизассемблера IDA Pro?**

Он отличается исключительной гибкостью, наличием встроенного командного языка, поддерживает множество форматов исполняемых файлов для большого числа процессоров и операционных систем. Позволяет строить блок-схемы, изменять названия меток, просматривать локальные процедуры в стеке и много другое. Умеет автоматически выполнять анализ кода. Вся сила его проявляется в интерактивном взаимодействии с пользователем.

**3. Каким образом выполняется дизассемблирование исполняемых модулей формата PE в IDA Pro?**

Анализ выполняется процессорным модулем IDA. Фактически это плагин для IDA. В нашем случае IDA использует так называемый Meta PC — вариант x86/x64, учитывающий большинство твиков, которые были добавлены в архитектуру от Intel и AMD.

**4. Для чего используется граф вызова процедур и как он может быть построен в IDA Pro?**

Граф потока выполнения — основной вид дизассемблера (можно сказать, представление в виде блок-схемы алгоритма функции).

**5. Как найти точку входа программы в IDA Pro?**

Из анализа графа, можно сделать вывод о том, что точка входа в программу носит имя start.

**6. Как осуществляется отладка программы в IDA Pro?**

Отладчик начинает выполнение программы с точки входа и прерывает работу программы перед командой, отмеченной точкой останова.