

**ОТЧЕТ О ВЫПОЛНЕНИИ**

**практической работы №2**

**по дисциплине / МДК 3.2. «Управление проектами».**

Выполнил: ст.гр. 2 ИСП11-31ВБ

Алирзаева З.Н. , Рязанова Ю.Р.

Специальность: 09.02.07 Информационные системы и программирование

Проверил: преп. Голиков Д. А.

Москва

2023

**Тема:** Дизассемблирование и отладка программ

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

**Ход работы:**

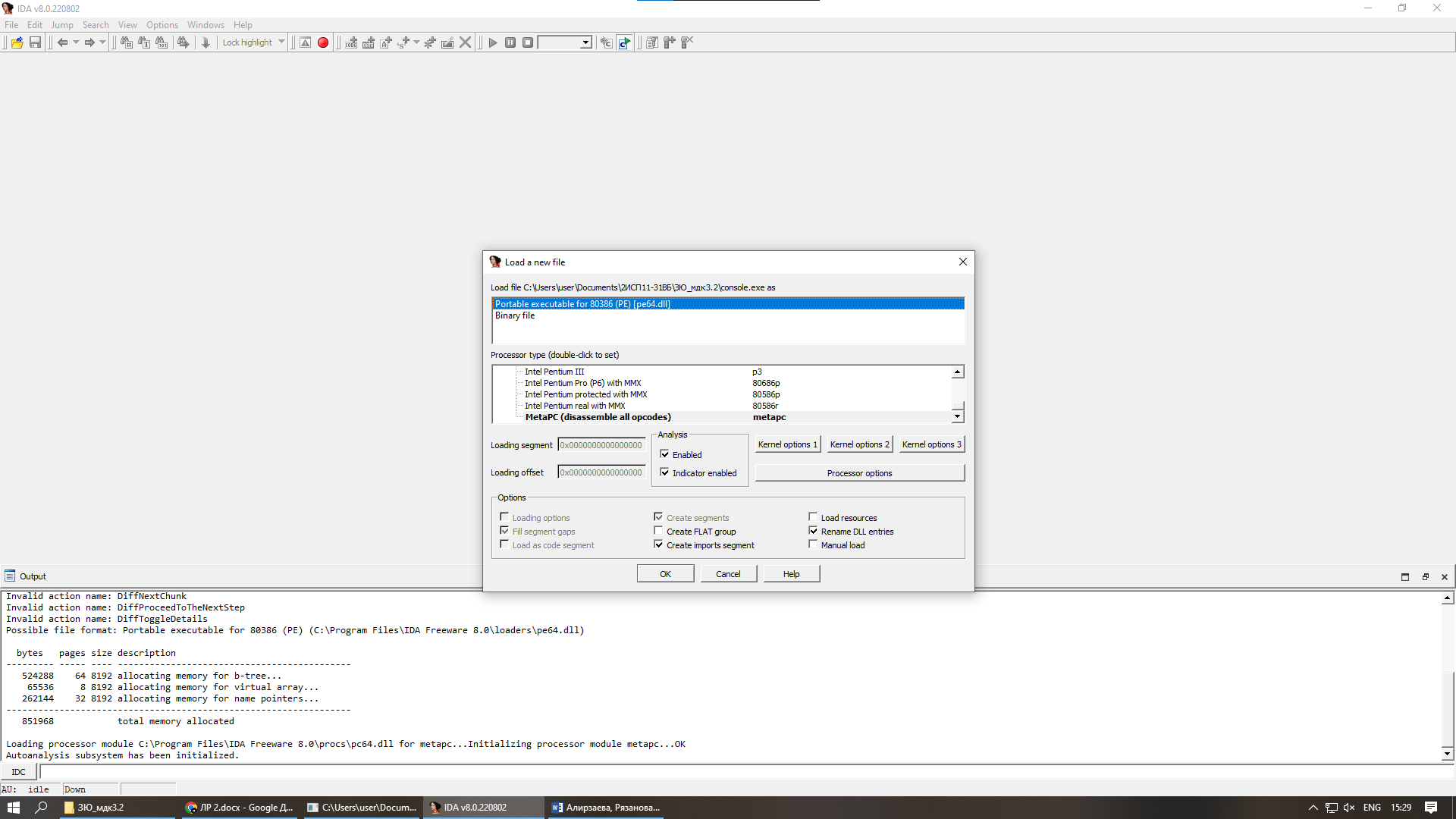


Рис. 1

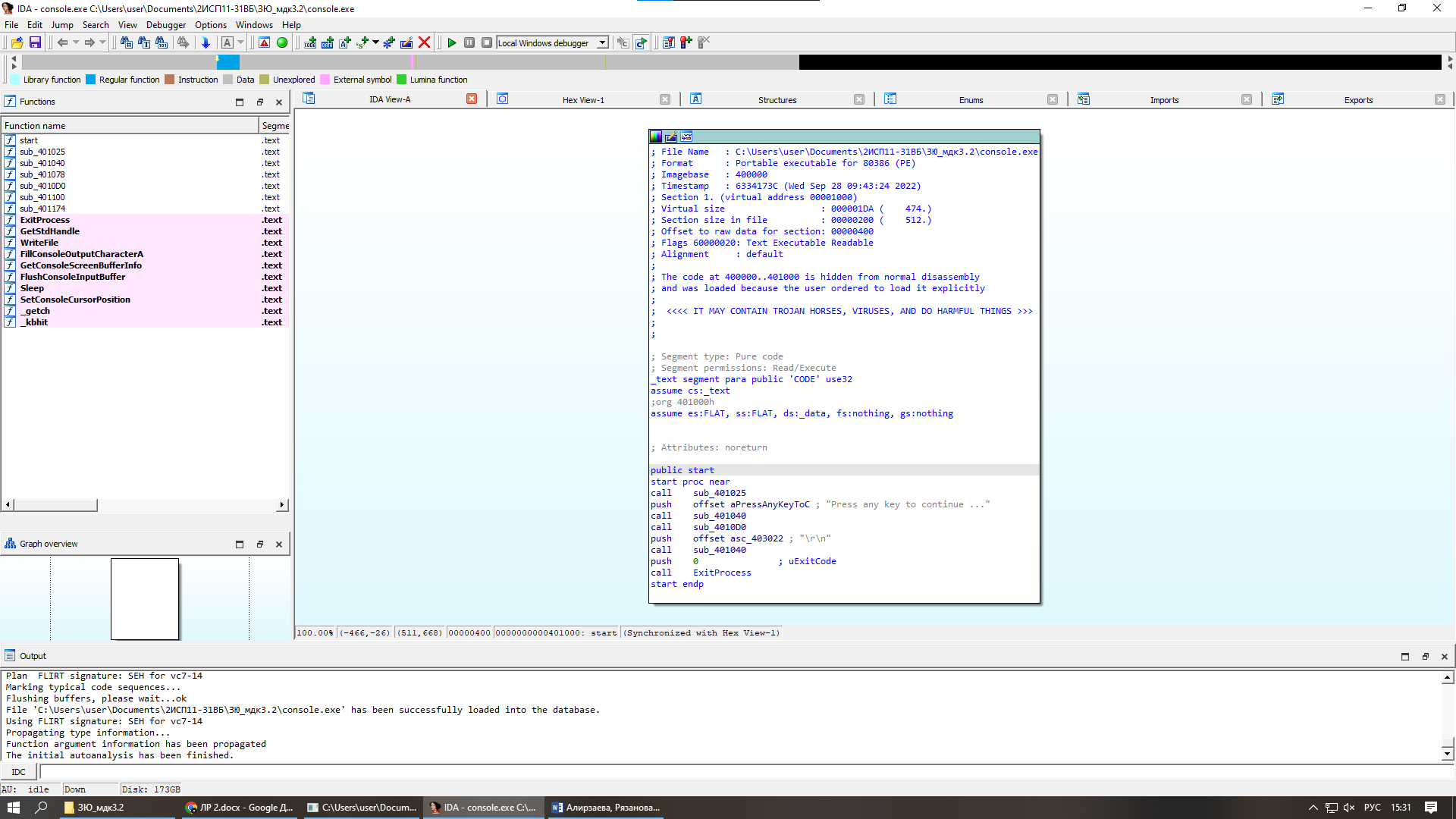


Рис. 2

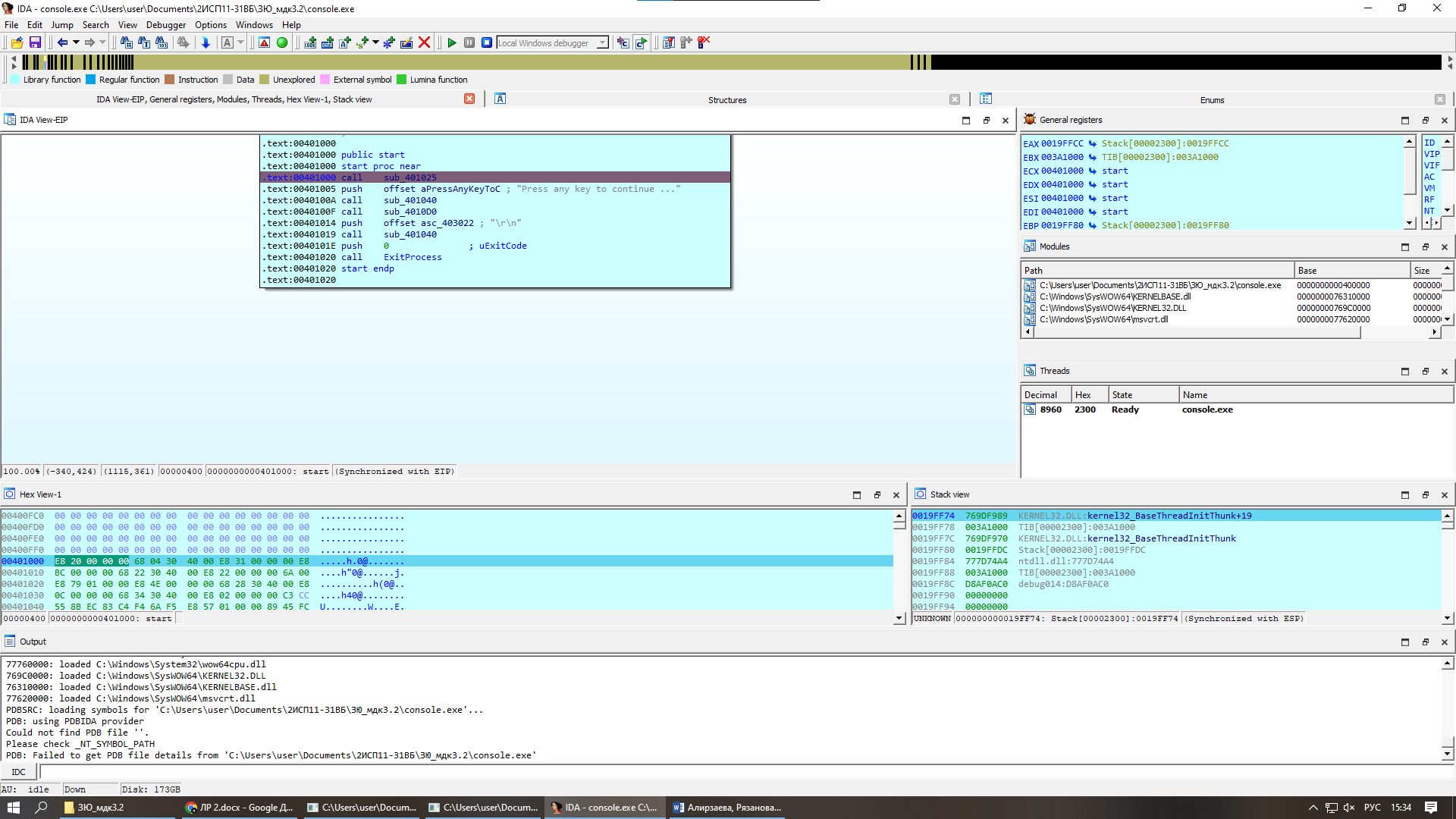


Рис. 3

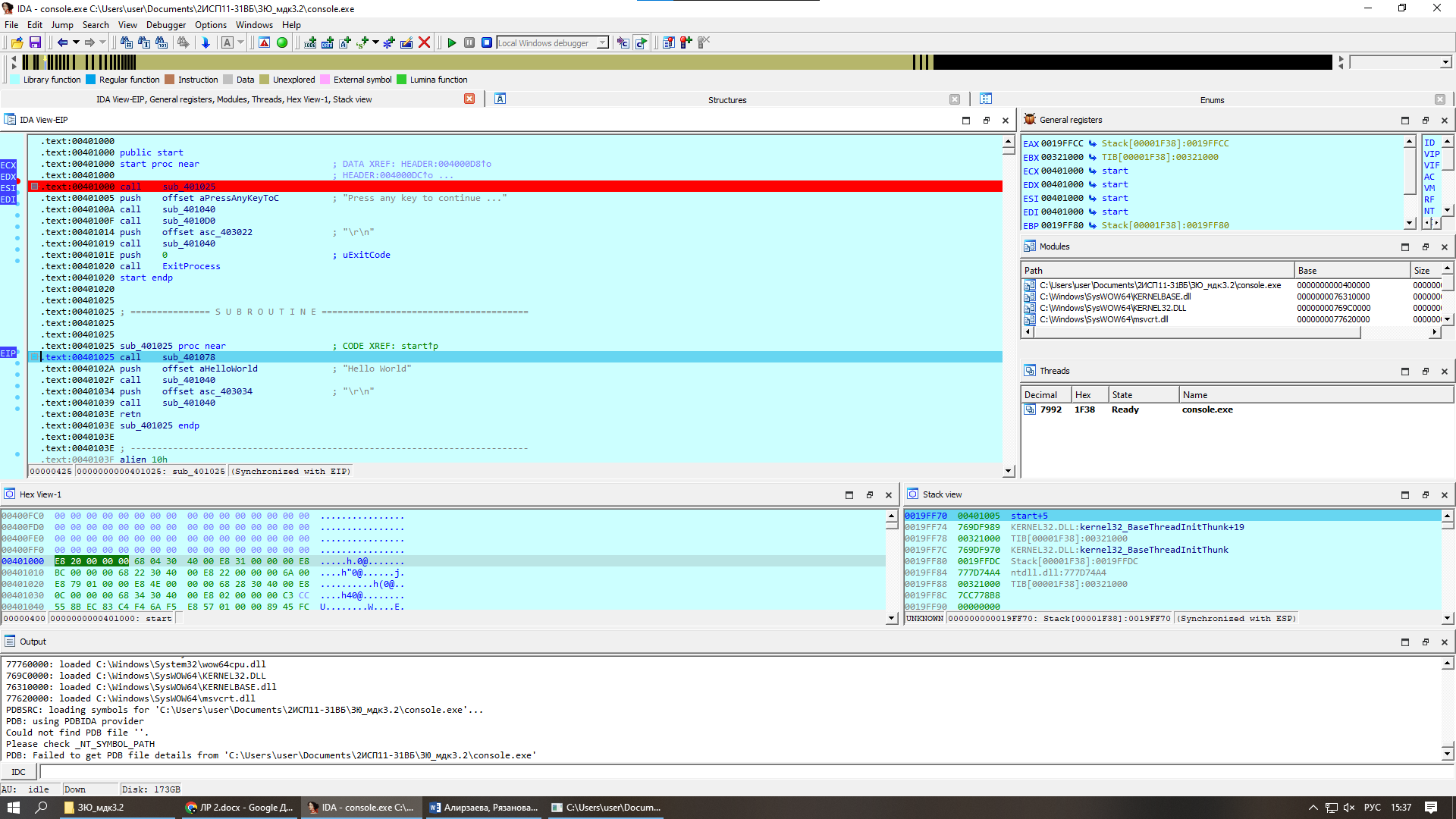


Рис. 4

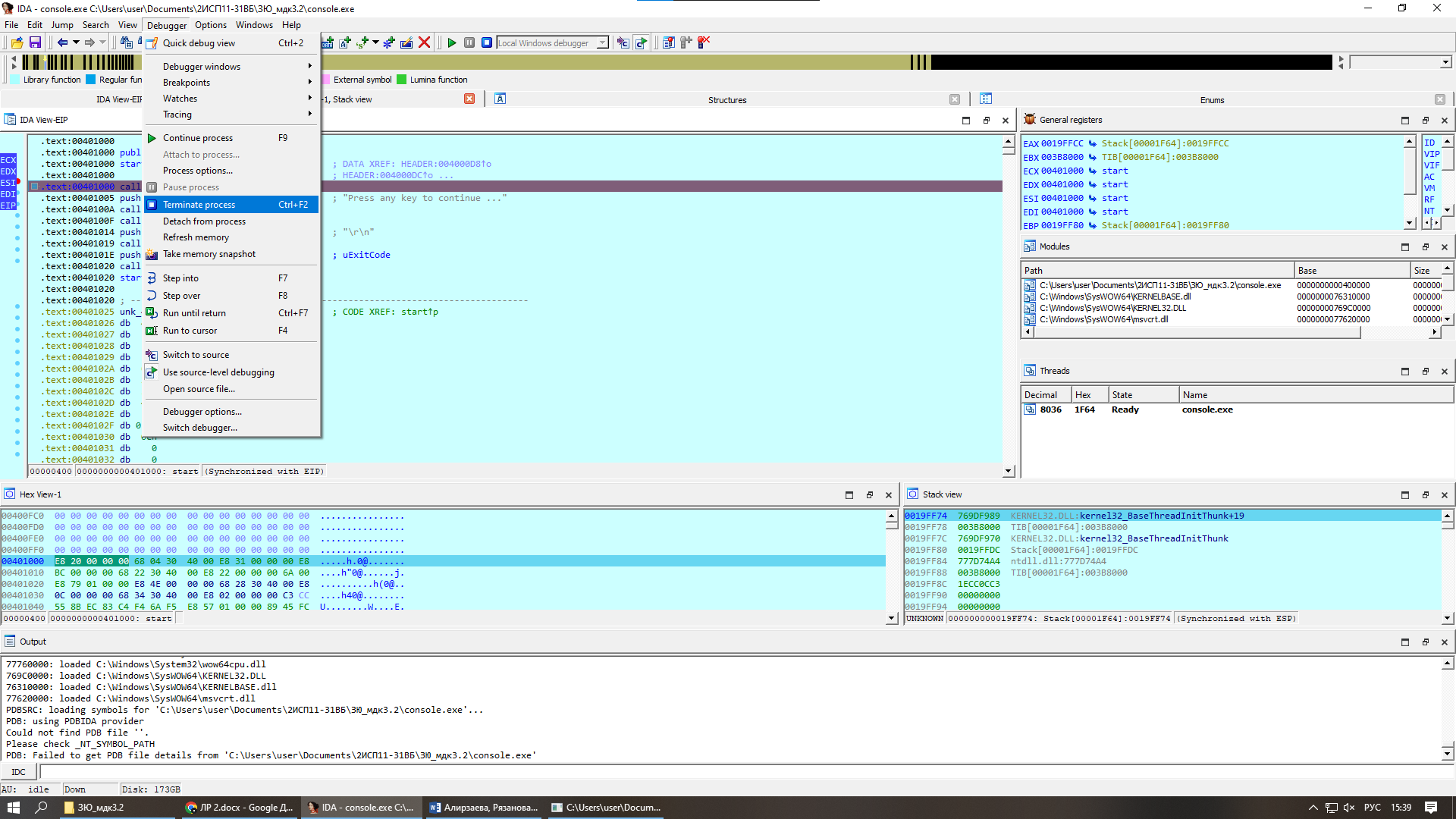


Рис. 5

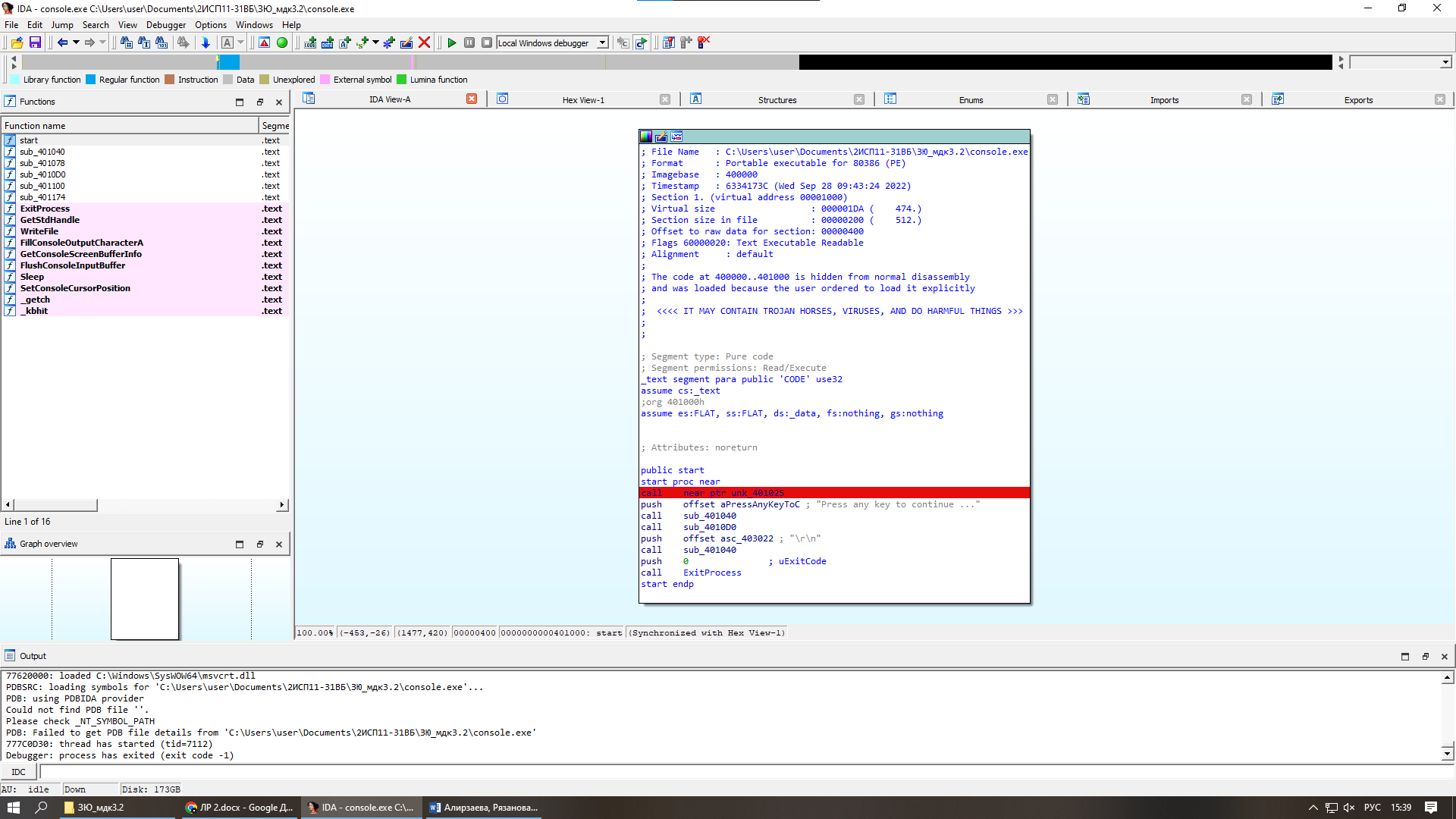


Рис. 6

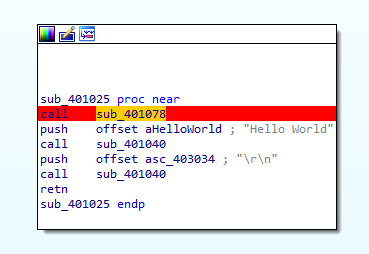


Рис. 7

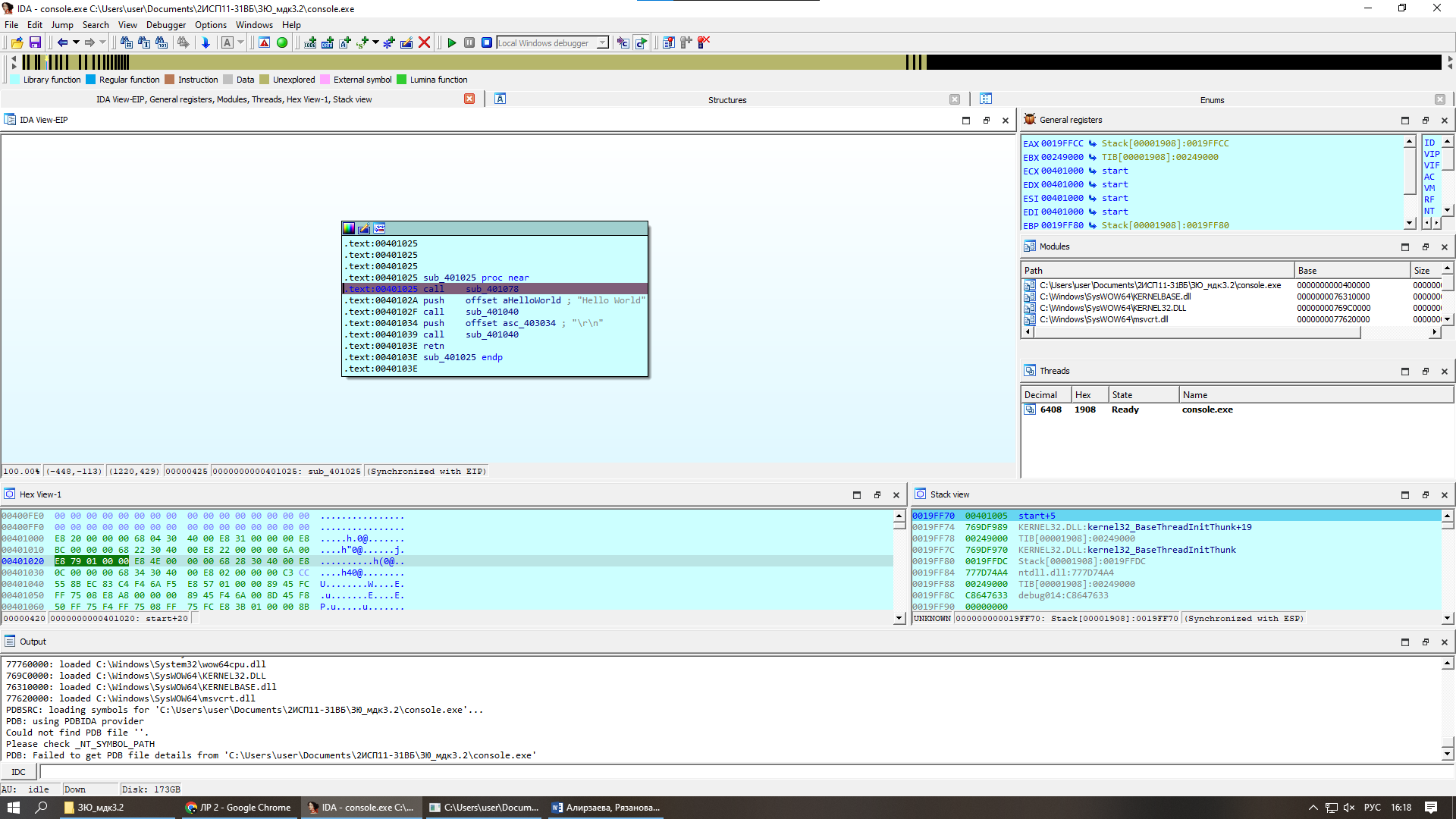


Рис. 8

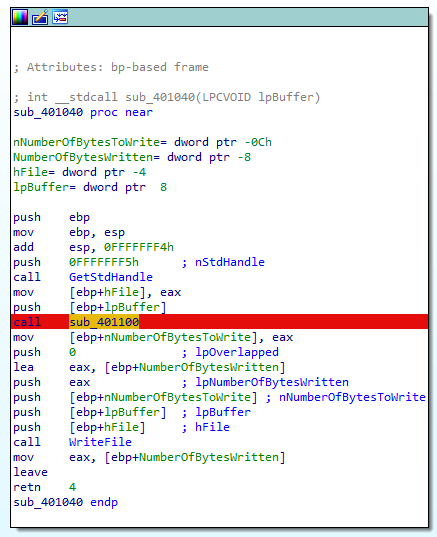


Рис. 9

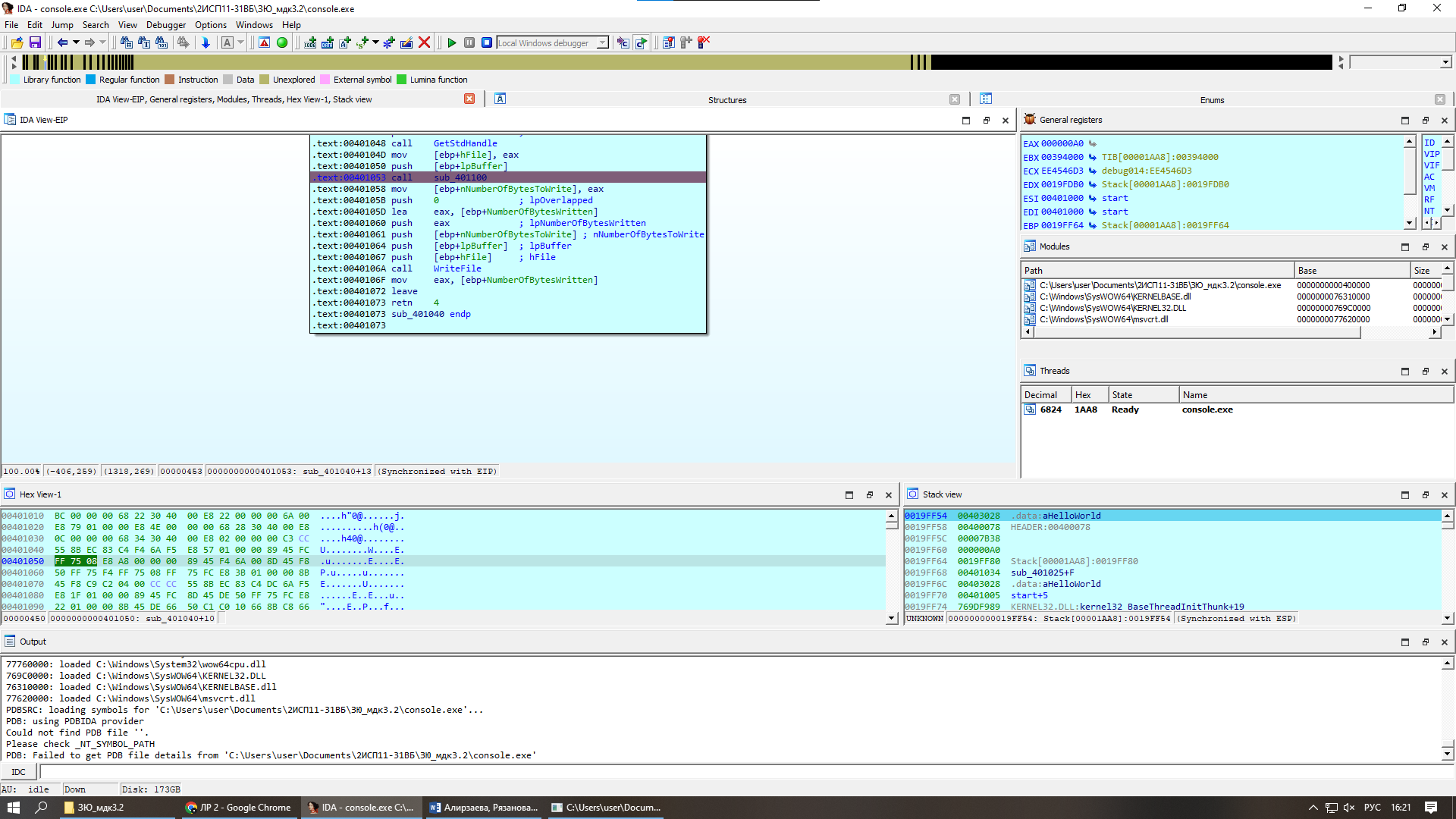


Рис. 10

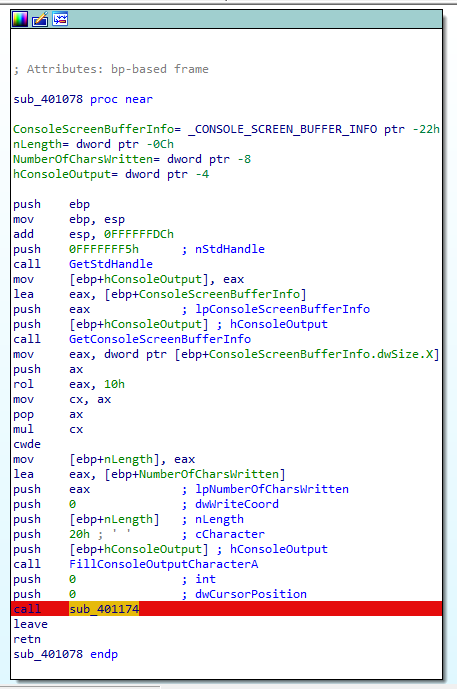


Рис. 11

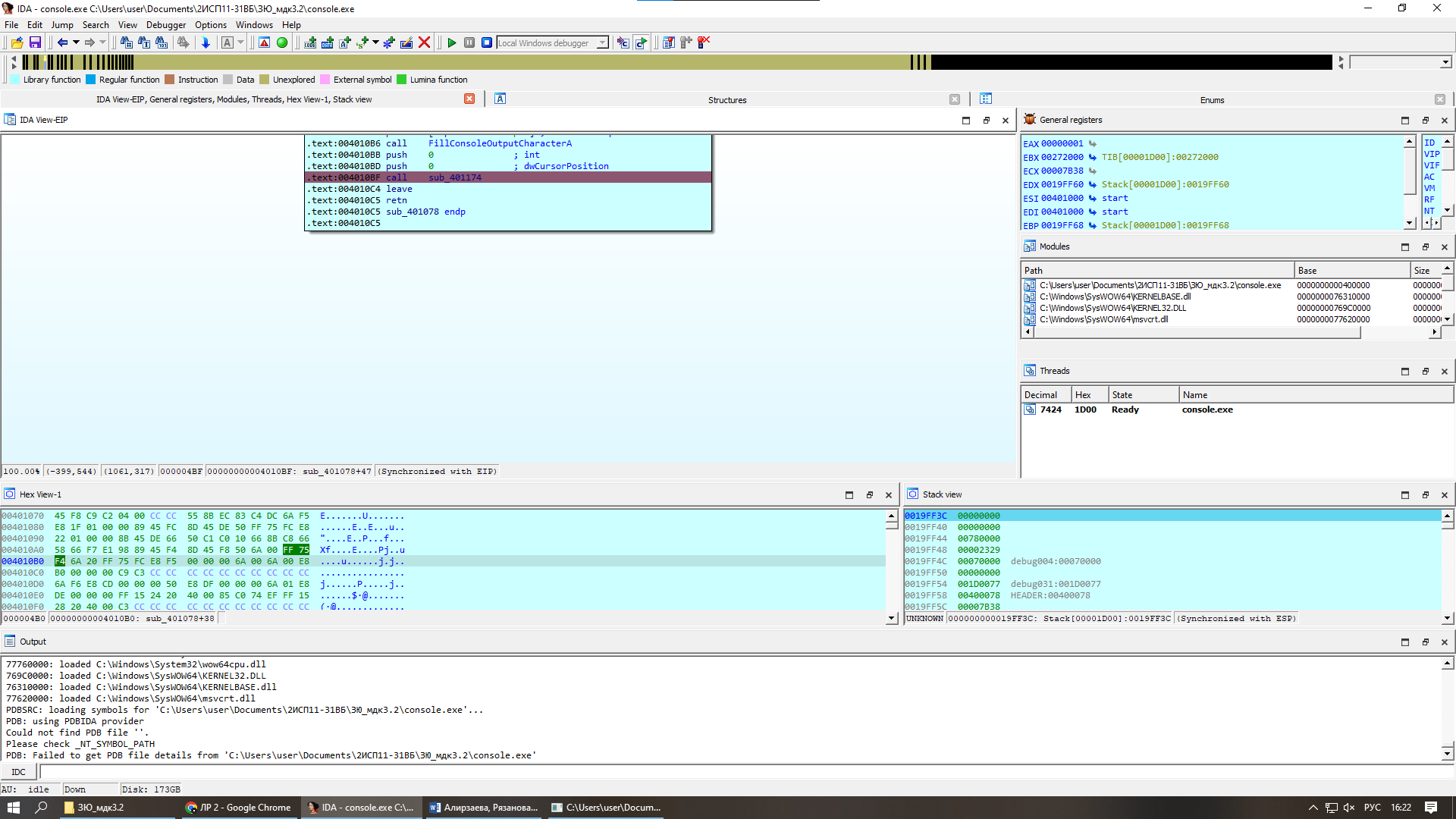


Рис. 12

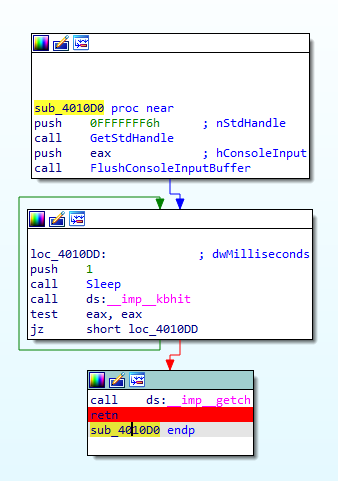


Рис. 13

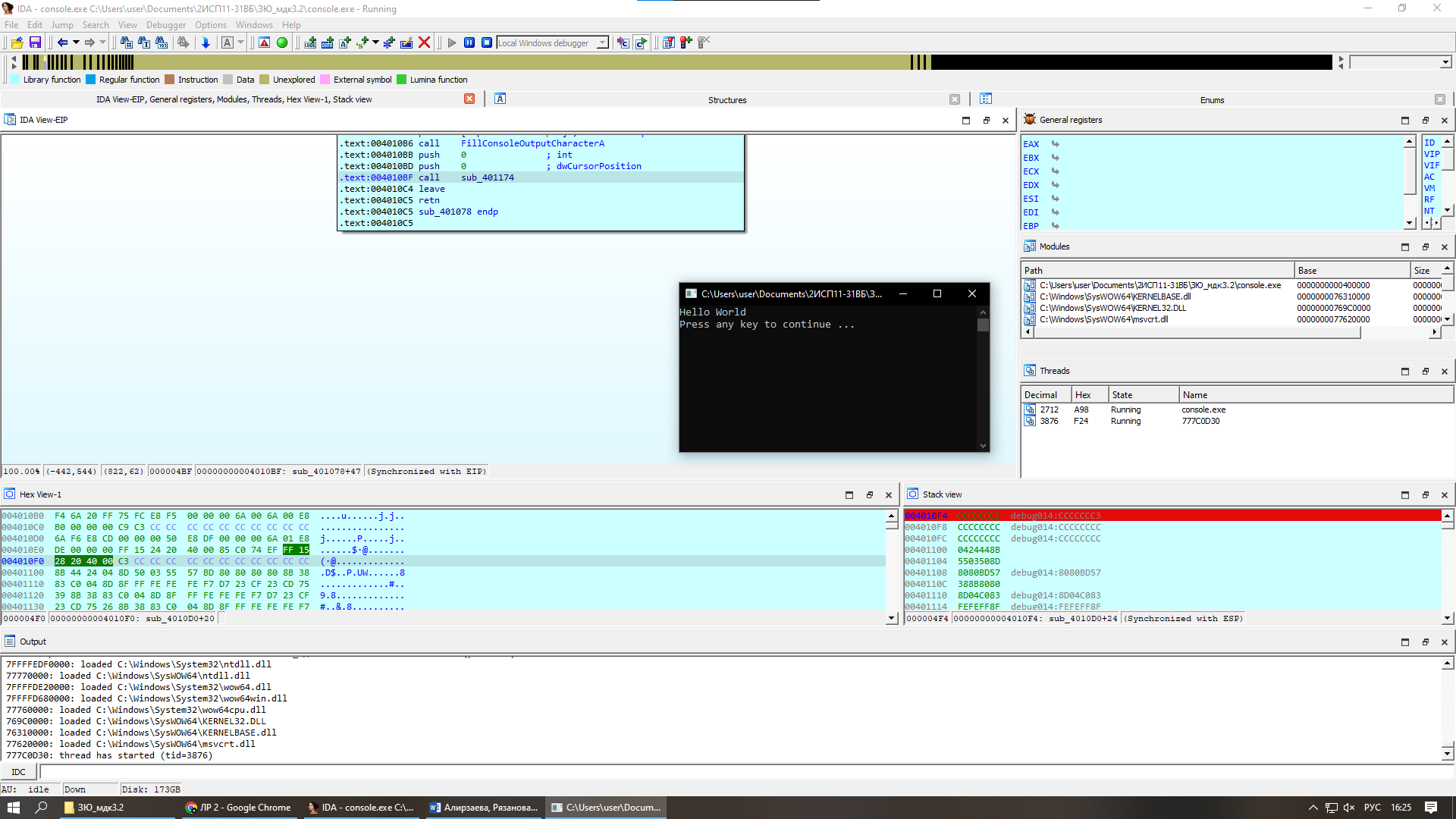


Рис. 14

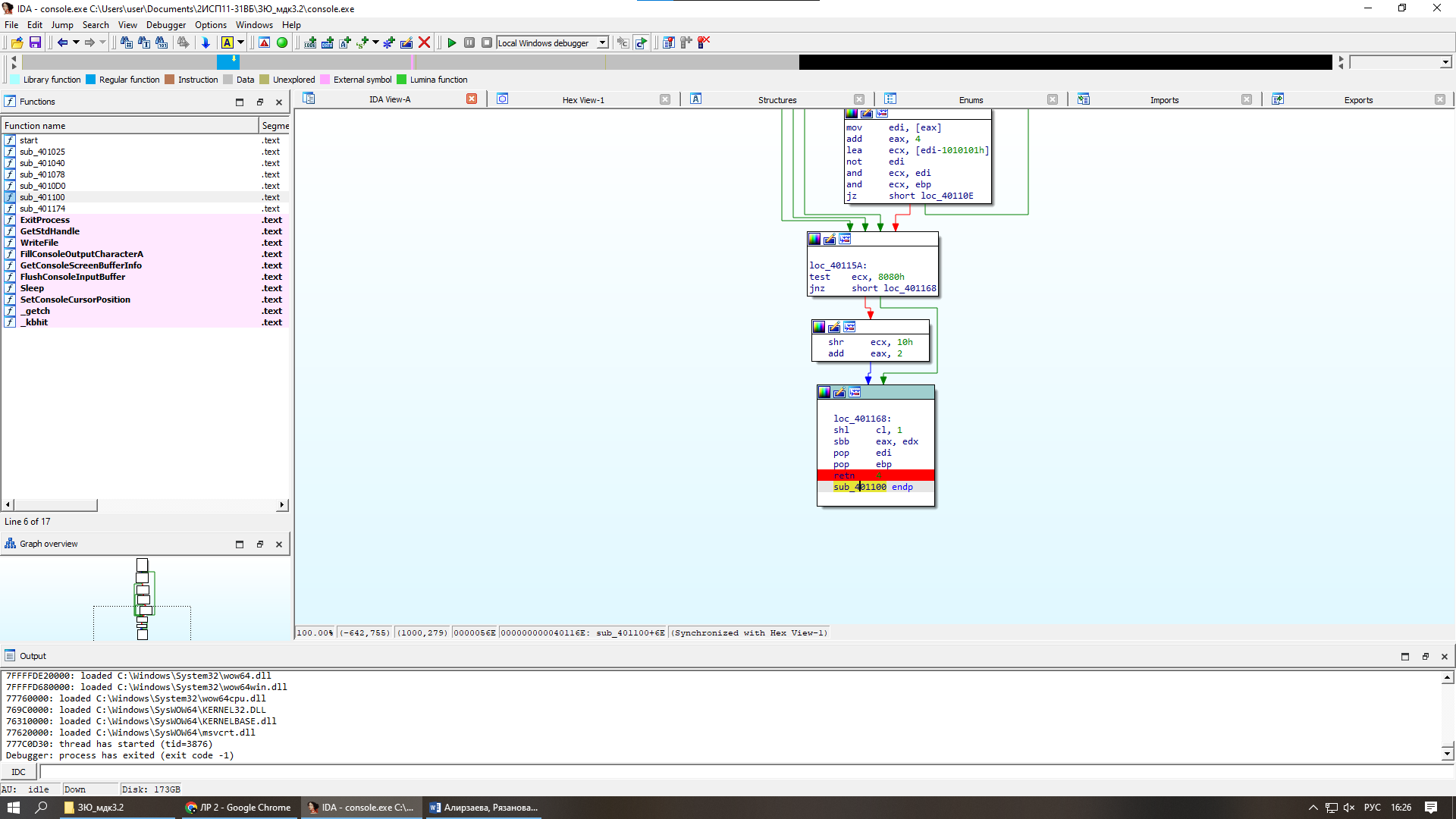


Рис. 15

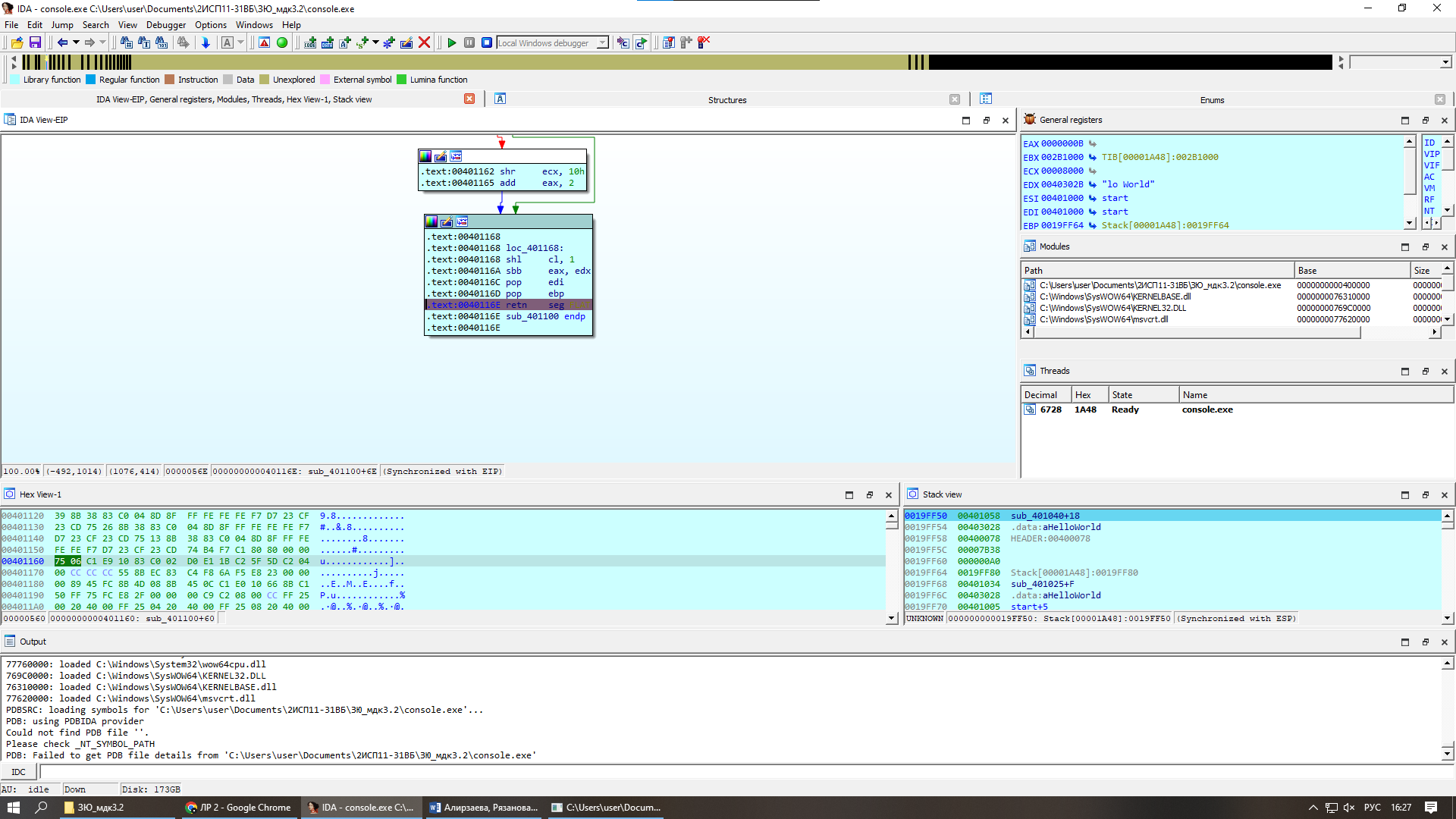


Рис. 16

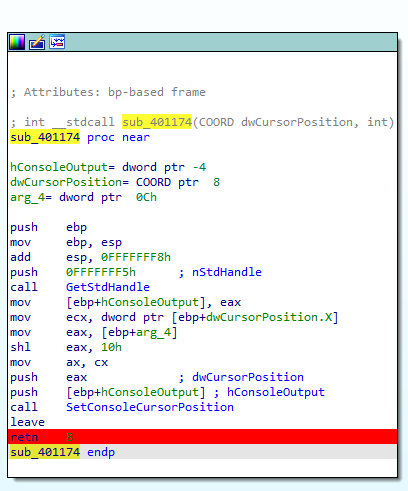


Рис. 17

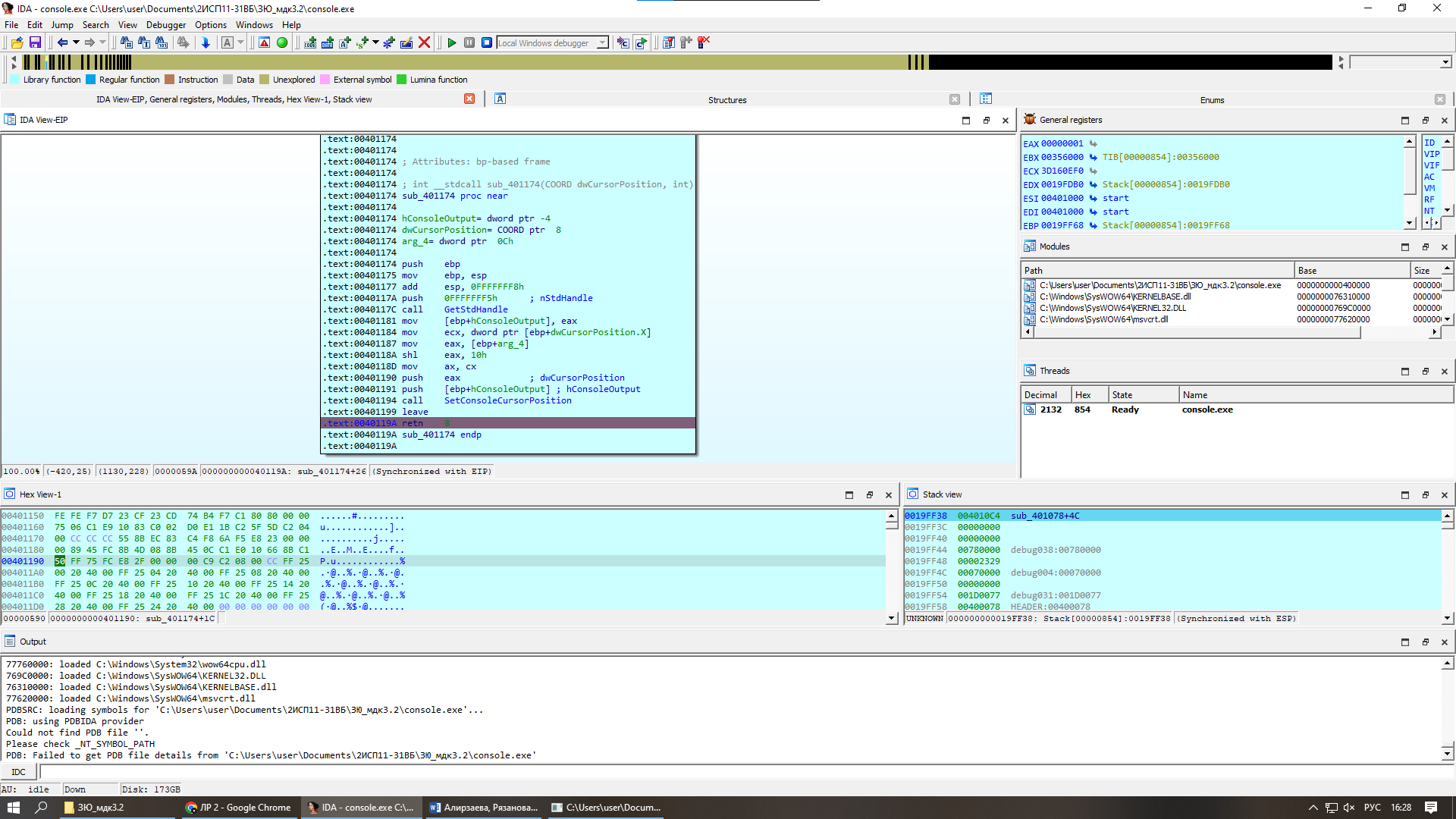


Рис. 18

**Контрольные вопросы:**

1. **В чем отличие между дизассемблером и отладчиком? –** Отладчик предназначен для поиска ошибок в программе, а дизассемблер преобразует 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.