

**ОТЧЕТ О ВЫПОЛНЕНИИ**

**практической работы №3**

**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:** Отладка и дизассемблирование программ

**Цель работы:** практическое знакомство с методикой отладки и дизассемблирования программ на языке ассемблера с помощью отладчика OllyDbg

**Ход работы:**

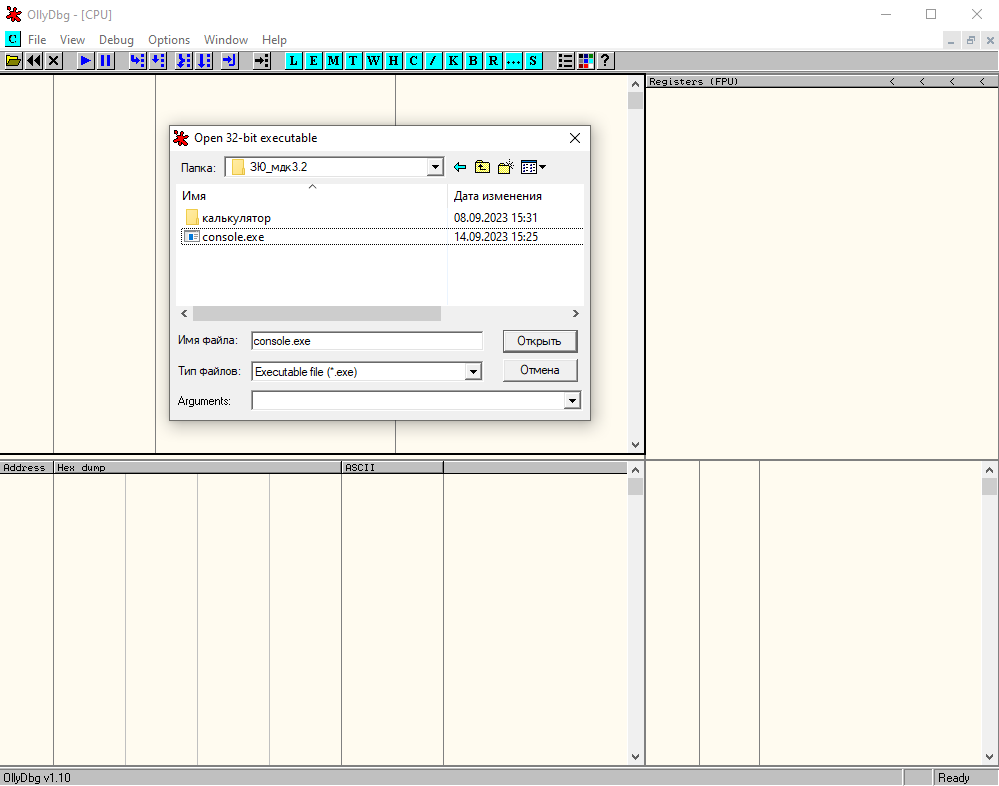


Рис. 1

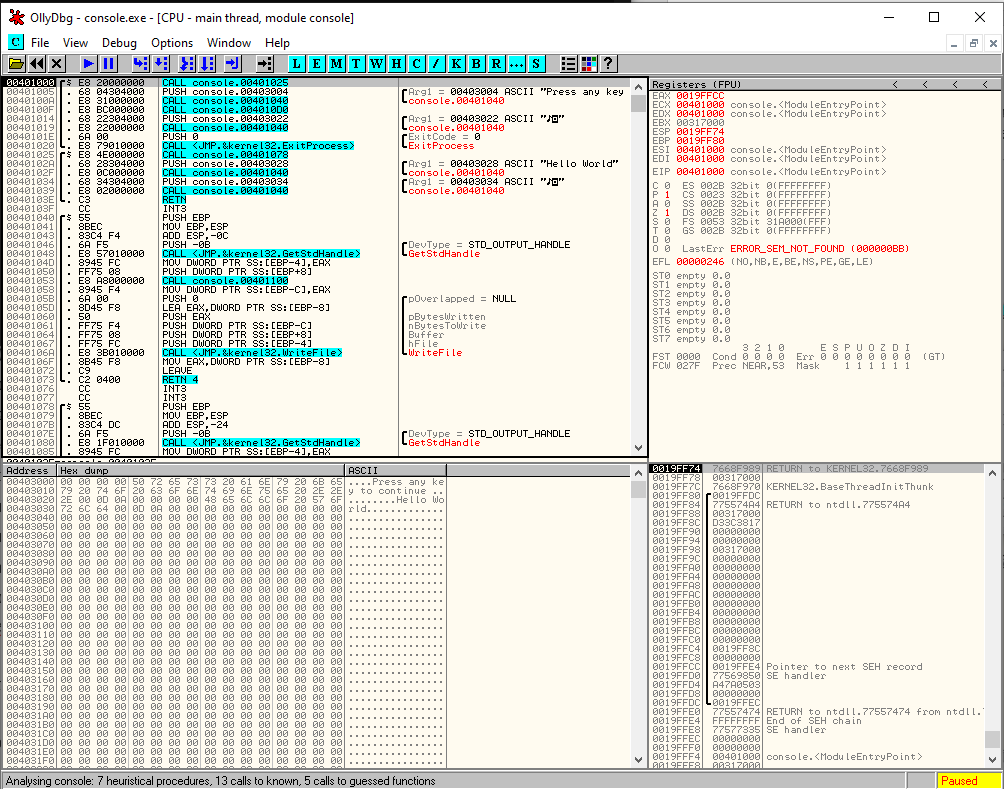


Рис. 2

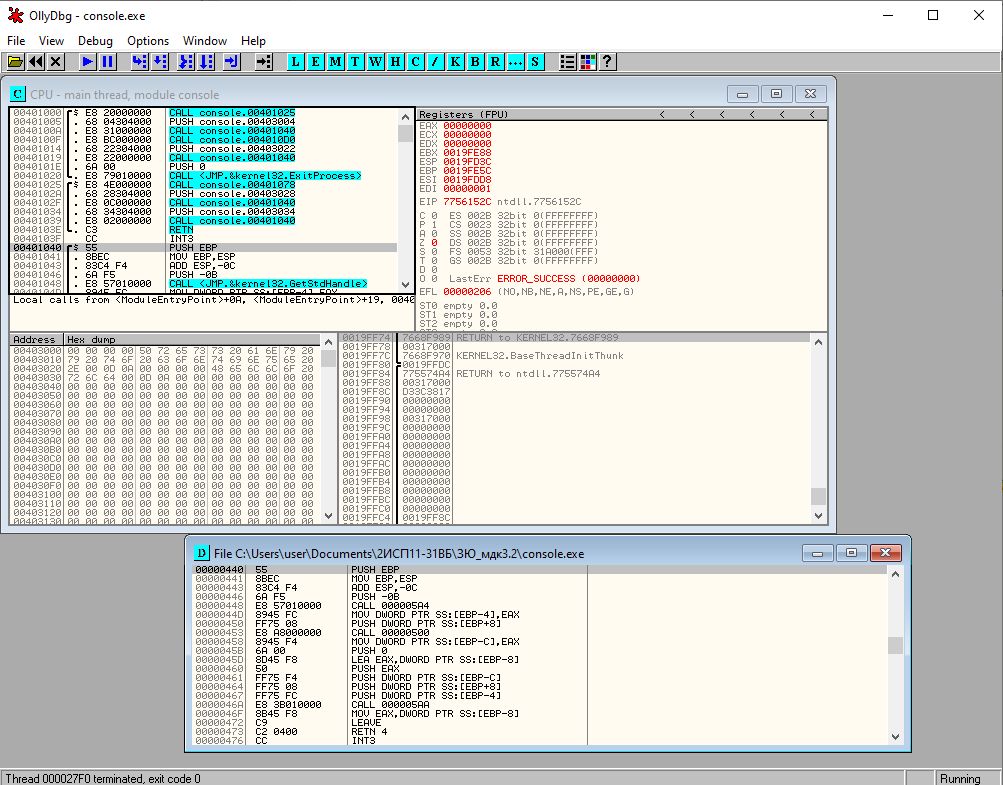


Рис. 3

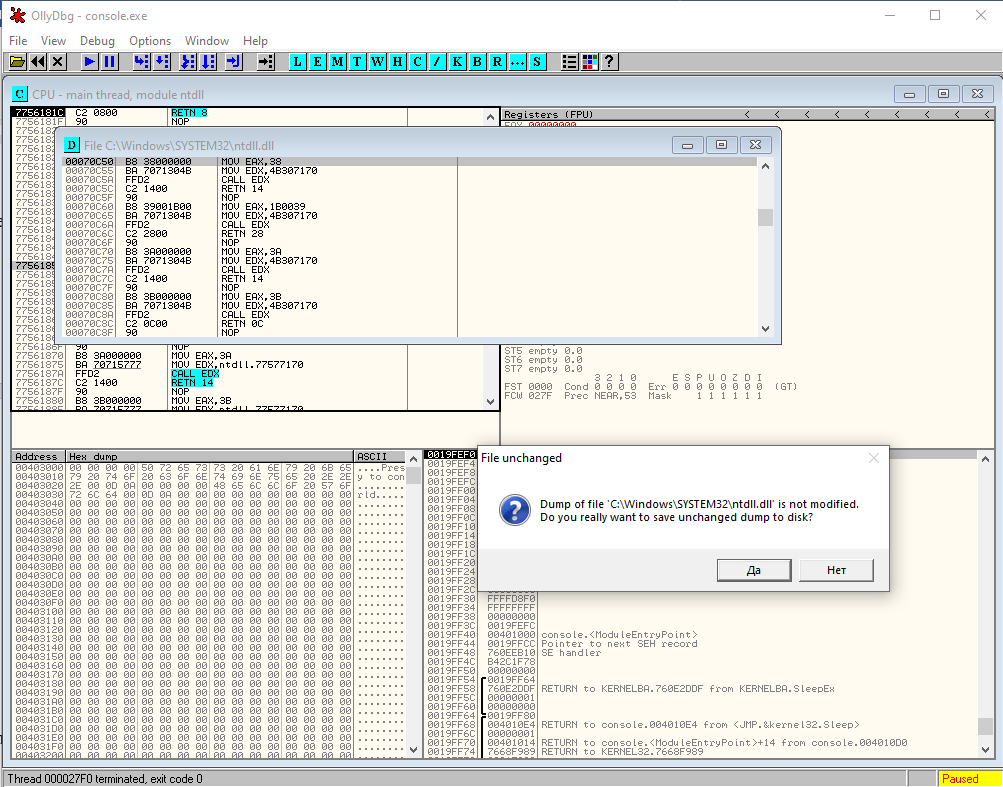


Рис. 4

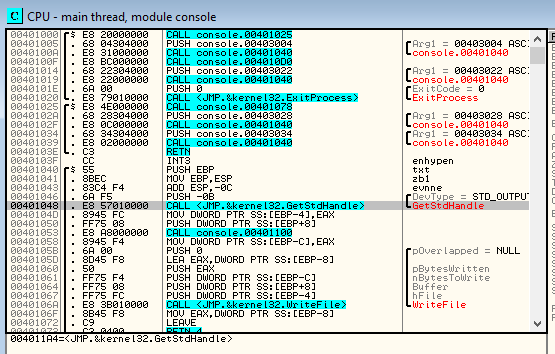


Рис. 5

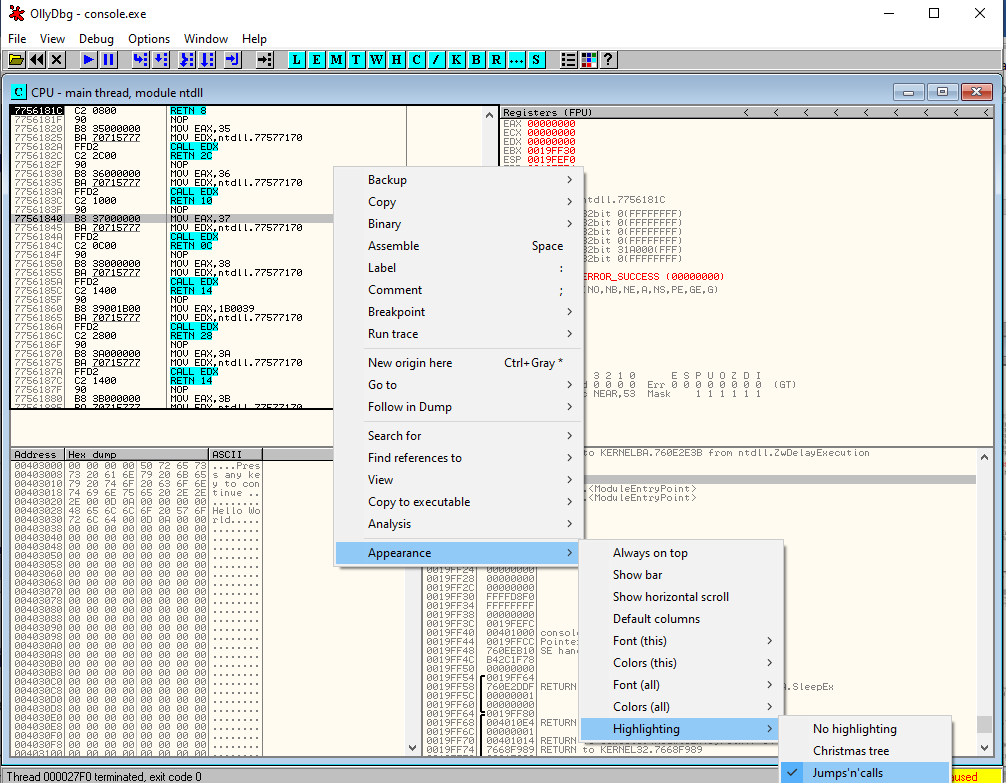


Рис. 6

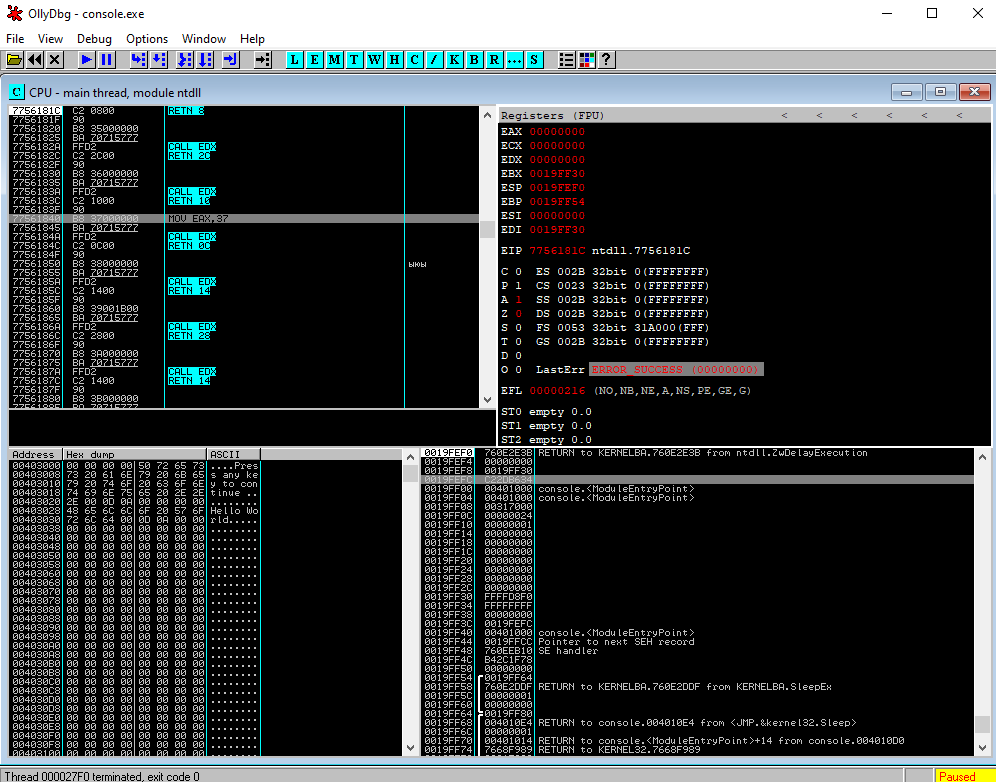


Рис. 7

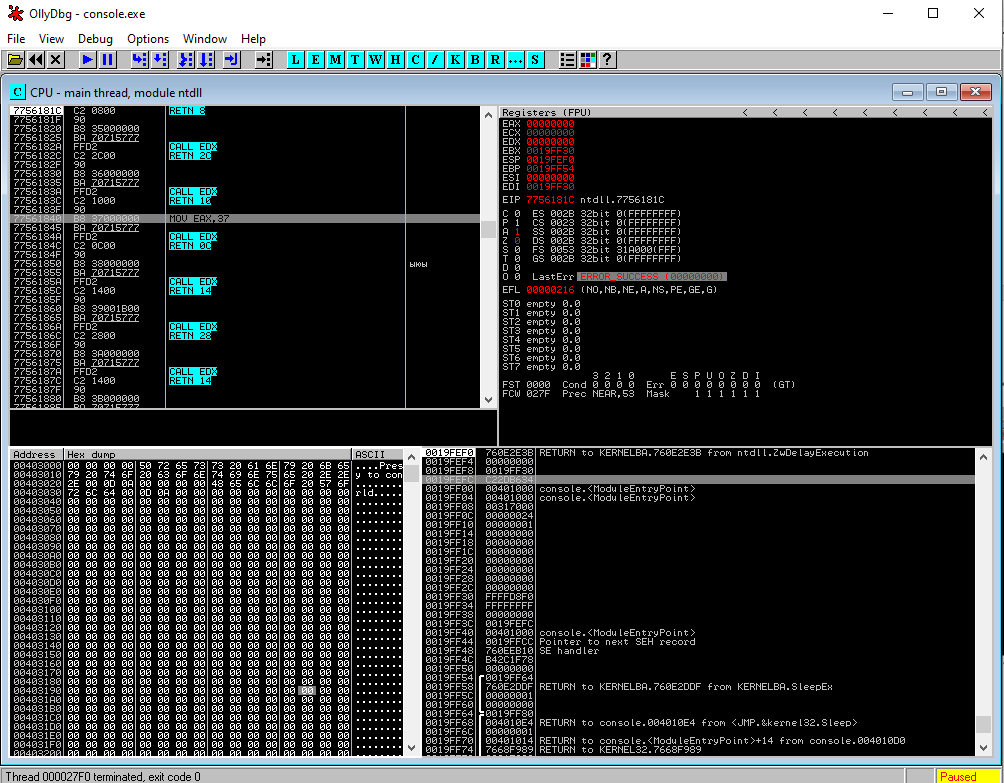


Рис. 8

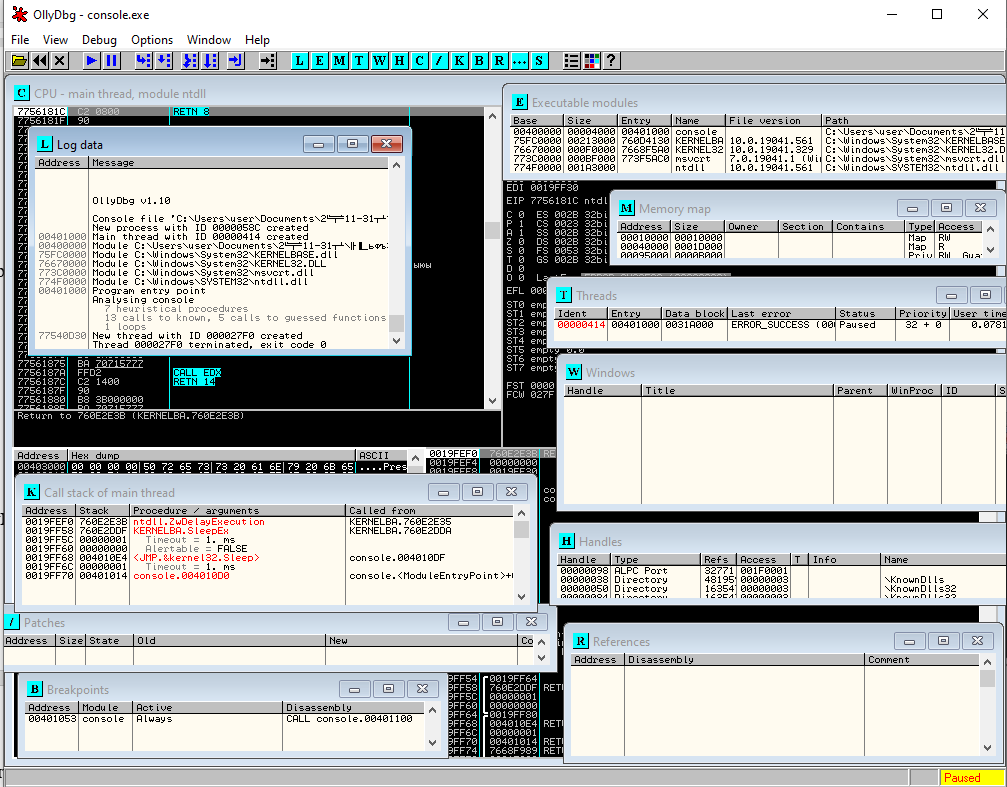


Рис. 9

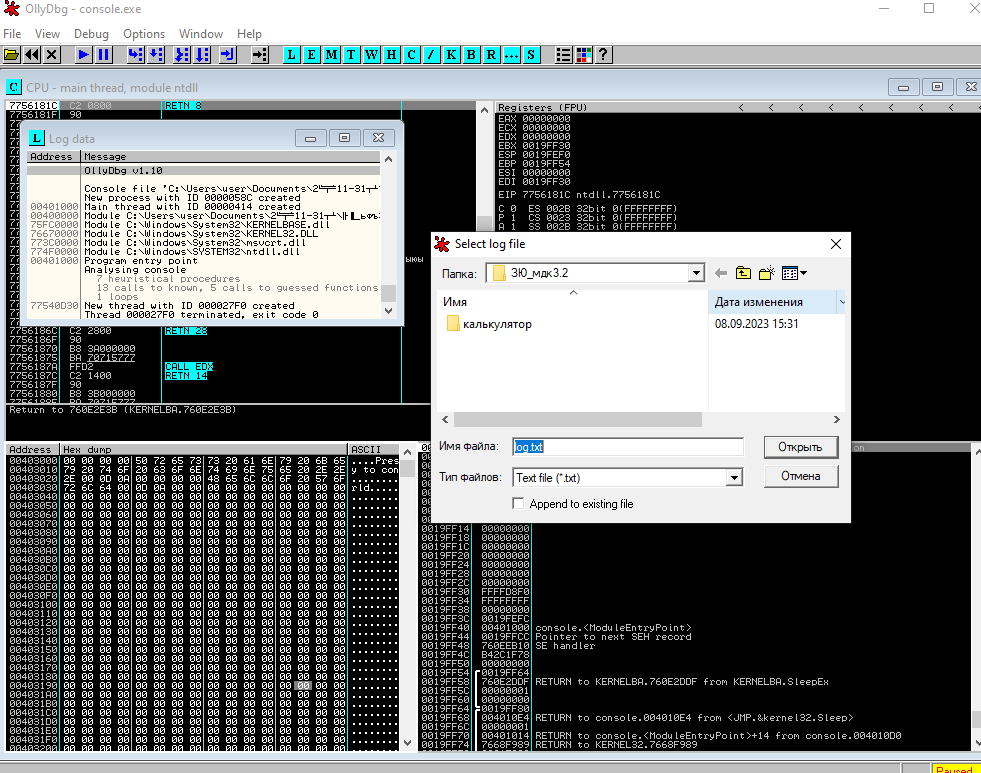


Рис. 10

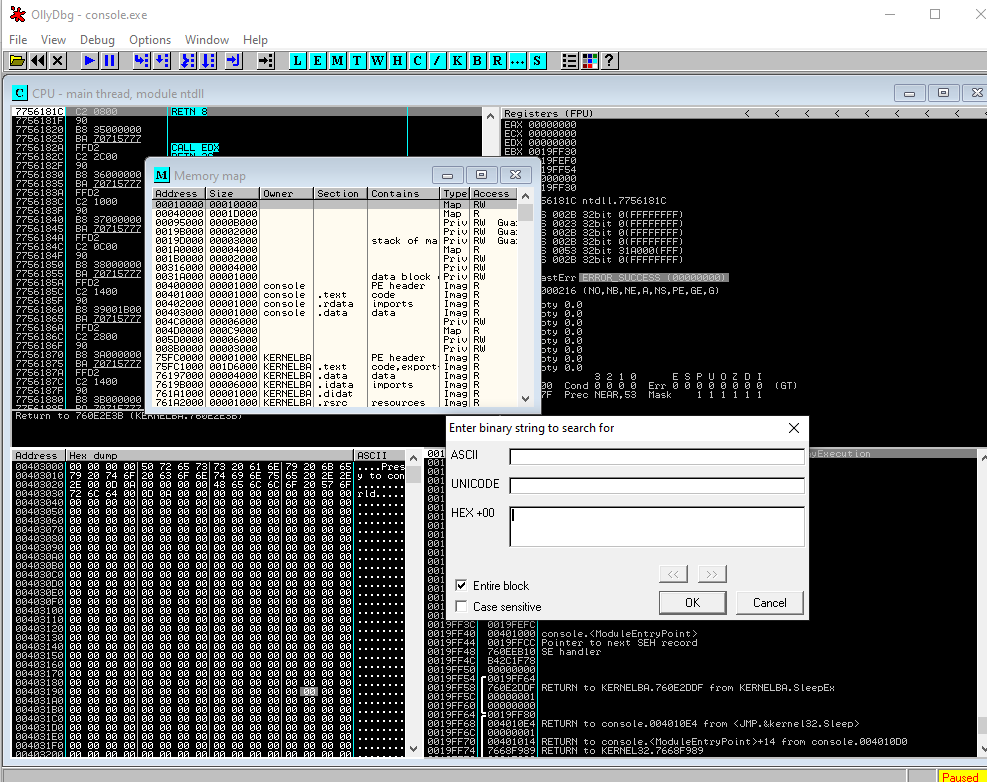


Рис. 11

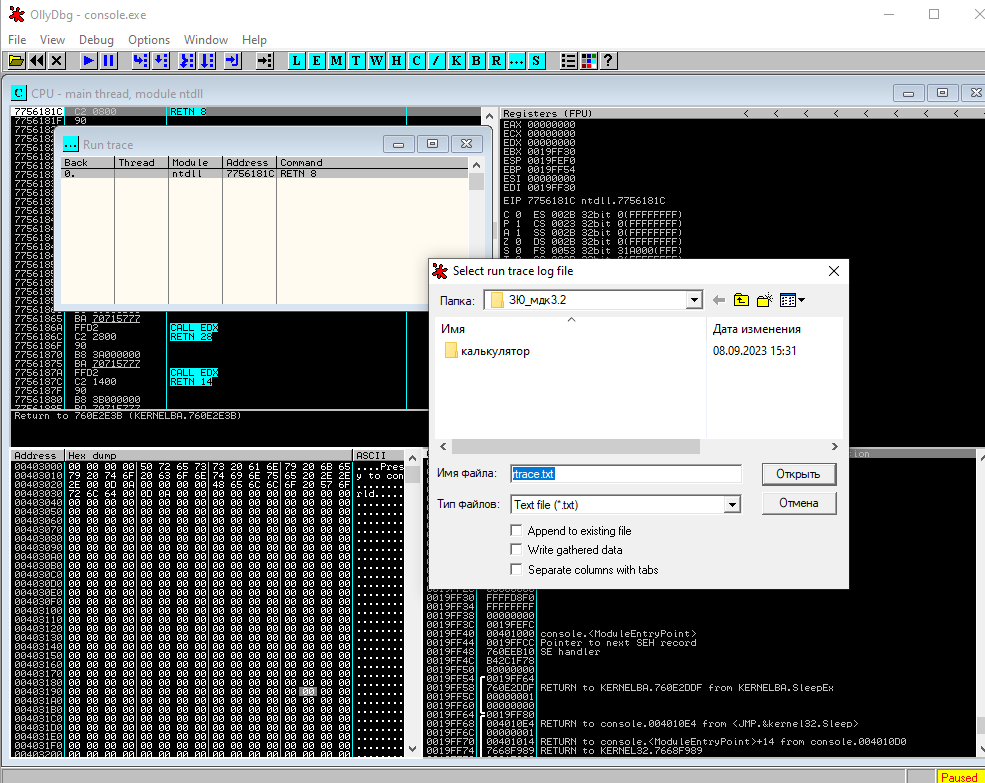


Рис. 12

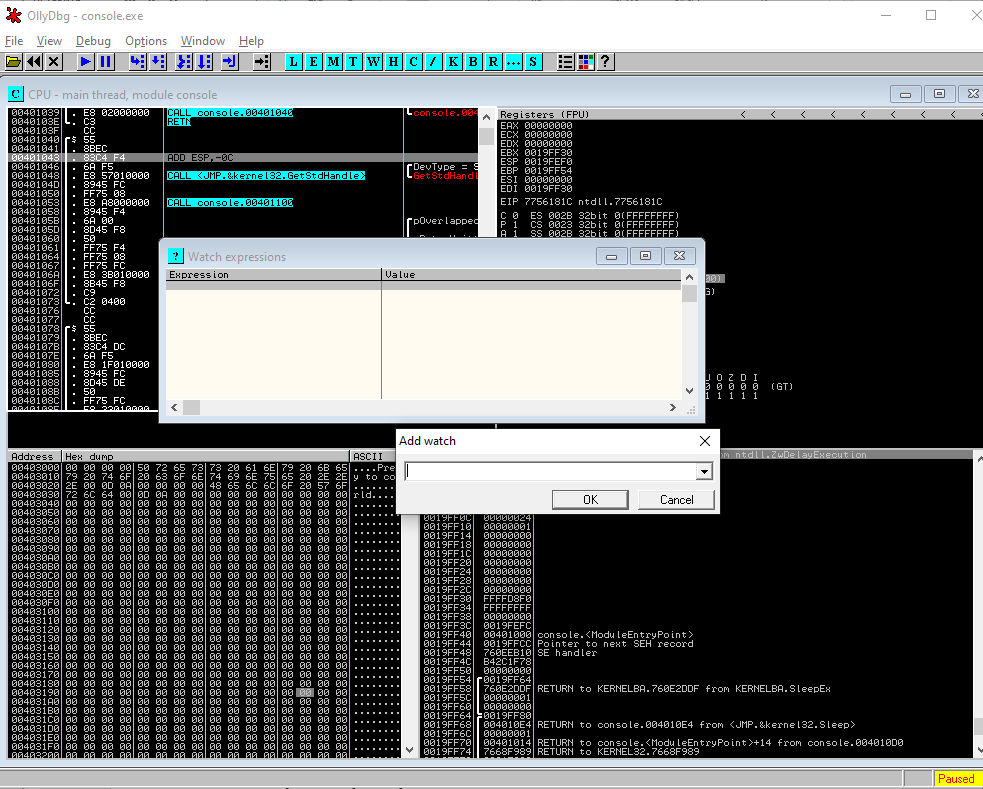


Рис. 13

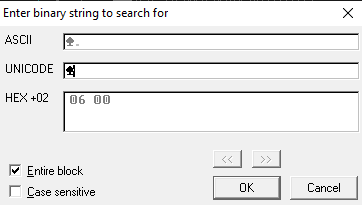


Рис. 14

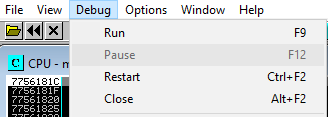


Рис. 15

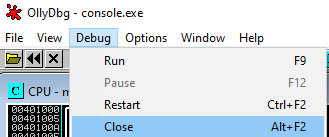


Рис. 16

**Контрольные вопросы:**

1. **Назначение программы OllyDbg. Версии программы. –** Выполнить программу пошагово, пошаговая отладка, прямая трассировка, профилирование, внесение исправлений; Версии: 1.10, 2.01
2. **Области применения программы –** Дизассемблирование, анализ выполнения программы и разветвление, встроенный ассемблер
3. **Средства отладки программ в OllyDbg -** Можете выполнять программу пошагово (команду за командой), со входом в подпрограммы или выполнять их за один шаг
4. **Пошаговая отладка. -** Устанавливает контрольную точку на каждой выбранной команде и удаляет ее, когда команда достигнута
5. **Прямая трассировка -** Выполняет программу пошагово и записывает еѐ выполнение в большой круговой буфер
6. **Горячие клавиши OllyDbg -** F7: выполняет одну строку кода (если находимся на CALL, то переходим внутрь вызванного участка кода).

F8: выполняет одну команду (строку кода) (если находимся на CALL, то просто выполняет вызов без перехода внутрь и переходит на следующую за CALL строку). Выполняя одну команду за другой, мы можем в трех остальных окнах следить за тем, как меняется содержимое регистров, секции данных и секции стека.

F2: устанавливает обычную точку останова на отмеченной строке. Чтобы убрать эту точку останова, надо ещё раз нажать F2.

F9: запускает программу, которая будет выполняться до тех пор, пока не встретит точку останова, не произойдет исключение или же не прекратит работу по каким-либо причинам. Когда программа запущена, в нижнем правом углу OllyDbg отображается слово RUNNING. Чтобы временно прекратить выполнение программы, нужно нажать F12 или DEBUG-> PAUSE

1. **Просмотр значений переменных -** При нажатии комбинации Ctrl + B появляется окно поиска. Строка для поиска может вводиться в виде последовательности символов, байтов, символов в кодировке Unicode. Для поиска команд используется комбинация Ctrl + F. Командой меню можно вызвать окно наблюдения. В появившемся окне можно добавить наблюдение, т.е. определить выражение, за которым отладчик будет наблюдать (выводить значение этого выражения). Значения которых отслеживаются при каждом выполнении команды процессора.