Министерство образования и науки Российской Федерации

Севастопольский государственный университет

Кафедра ИС

Отчет

По дисциплине: “Технические средства информационных систем”

Лабораторная работа №6

“ Исследование способов анализа и отладки приложений Win32

в среде отладчика OllyDbg”

Выполнил:

ст.гр. ИС/б-32

Долженко И.А.

Проверил:

Дрозин А.Ю.

Севастополь

2019

1 ЦЕЛЬ РАБОТЫ

Исследование архитектуры 32-разрядных процессоров и возможностей отладчика OllyDbg при разработке и отладке приложений Win32 для, приобретение практических навыков по анализу и отладке программ на языке ассемблера.

2 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Создать приложение типа Win32 с графическим интерфейсом, вычисляющее сумму и разность двух чисел: первое число – номер в группе, второе – число, противоположное номеру первой буквы фамилии в алфавите (отрицательное число в дополнительном коде). Противоположным к некоторому х называется число, равное х по абсолютной величине, но обратное по знаку.

2. Загрузить разработанное приложение в отладчик.

3. Исследовать работу программы в отладчике OllyDbg:

Проанализировать, какие изменения происходят в различных регистрах процессора:

- изменяйте значения регистров EAX и EBX таким образом, чтобы произошли изменения состояний флагов O, P, Z, S, C;

- поместите значение в стек с помощью инструкции PUSH;

- извлеките значение из стека с помощью инструкции POP;

- изучите принцип работы инструкции MOV c 8-ми, 16-ти и 32-х разрядными регистрами;

- изучите работу математических инструкций: INC, DEC, ADD, SUB, MUL, IMUL, DIV, NEG;

- измените значение регистра ESP;

- измените значение регистра EIP.

3 ХОД РАБОТЫ

Для исследования возможностей отладчика OllyDbg было разработано приложение app.exe. После загрузки приложения в отладчик OllyDbg регистр EIP, указывающий на инструкцию, которая должна выполнится, устанавливается на адрес команды, которая будет выполняться первой (рис. 1).

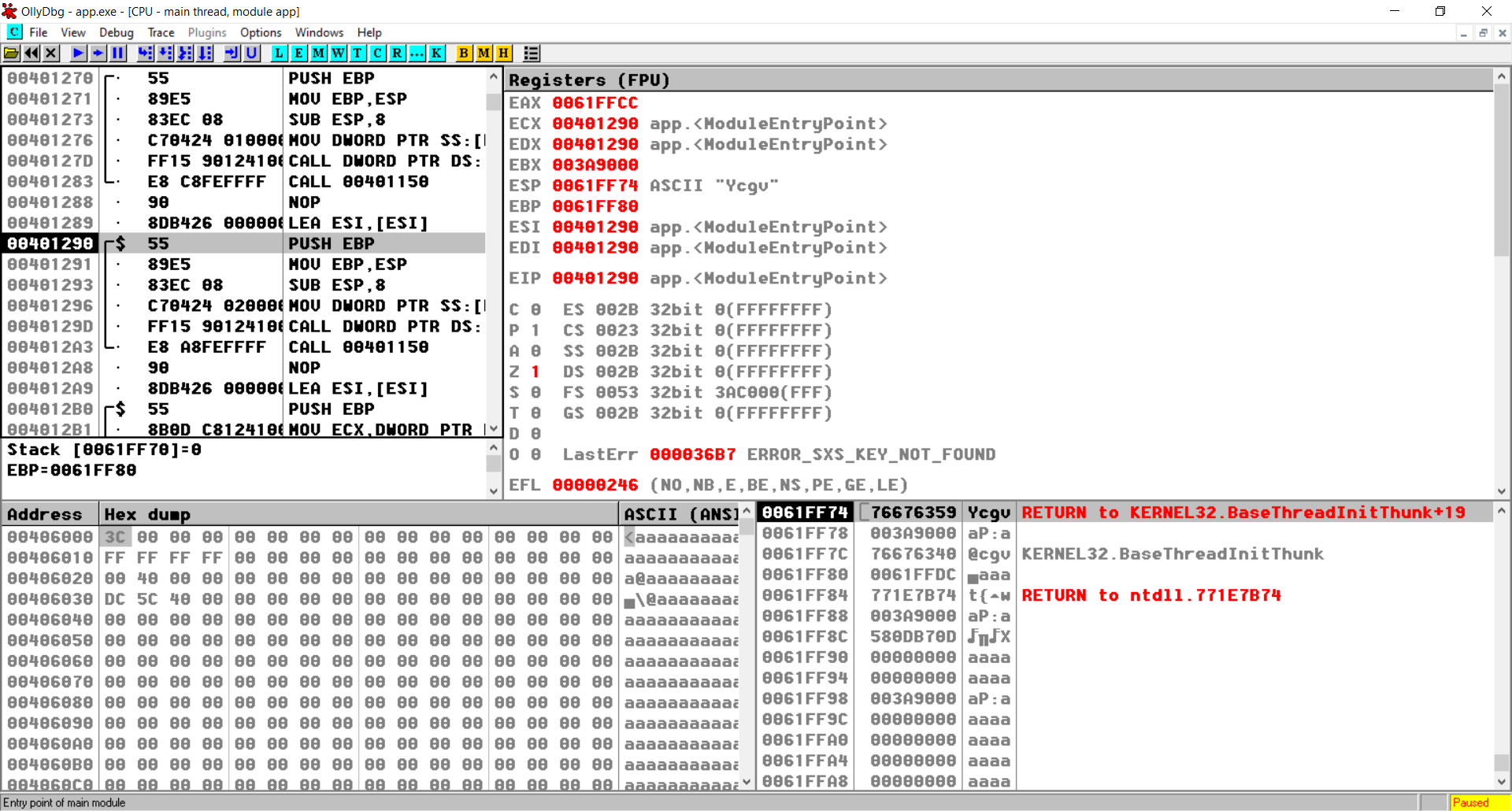


Рисунок 1 – Начальное значение регистра EIP

Изменим значение регистра ЕАХ на 7FFFFFFF (рис.2).

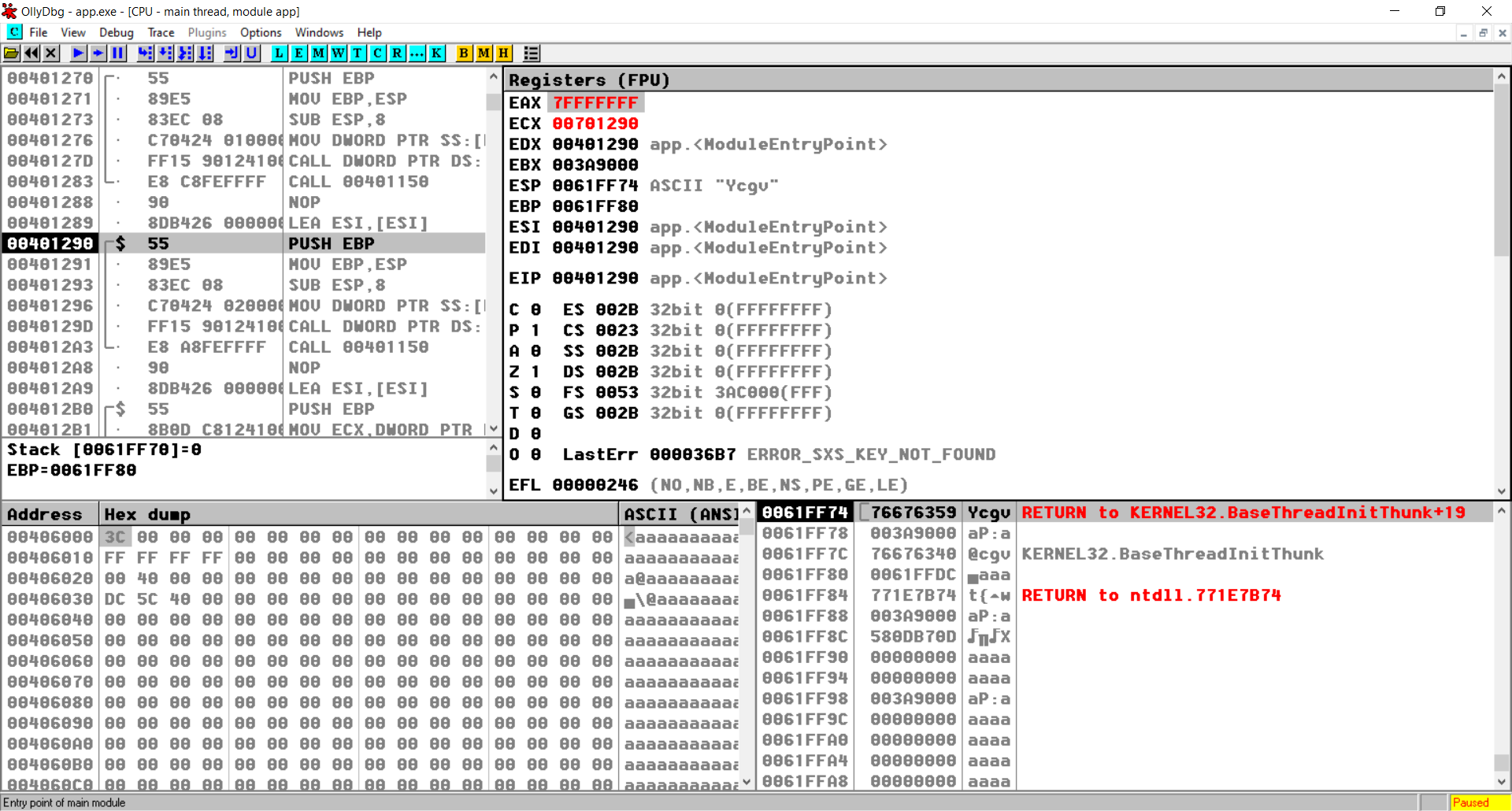


Рисунок 2 – Изменение регистра ЕАХ

Затем прибавим 1, из-за чего сумма превысит максимальное позитивное число. Для этого через окно Assemble изменим инструкцию на команду ADD EAX, 1.

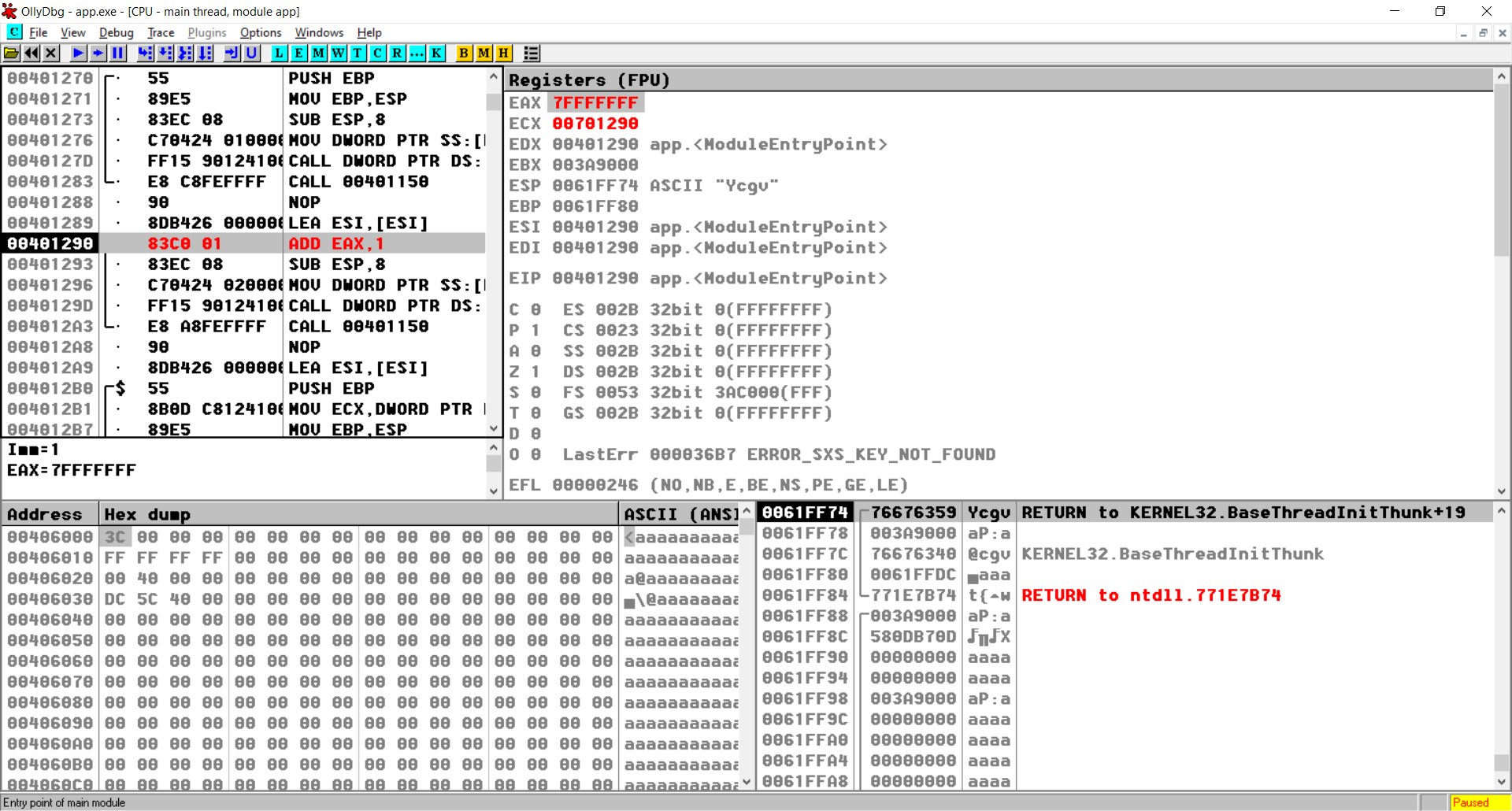


Рисунок 3 – Изменение команды

На данный момент флаг O равен нулю (рис.1). Но после выполнения команды сложения в EAX записалось значение 80000000 и знак числа изменился (рис. 4).

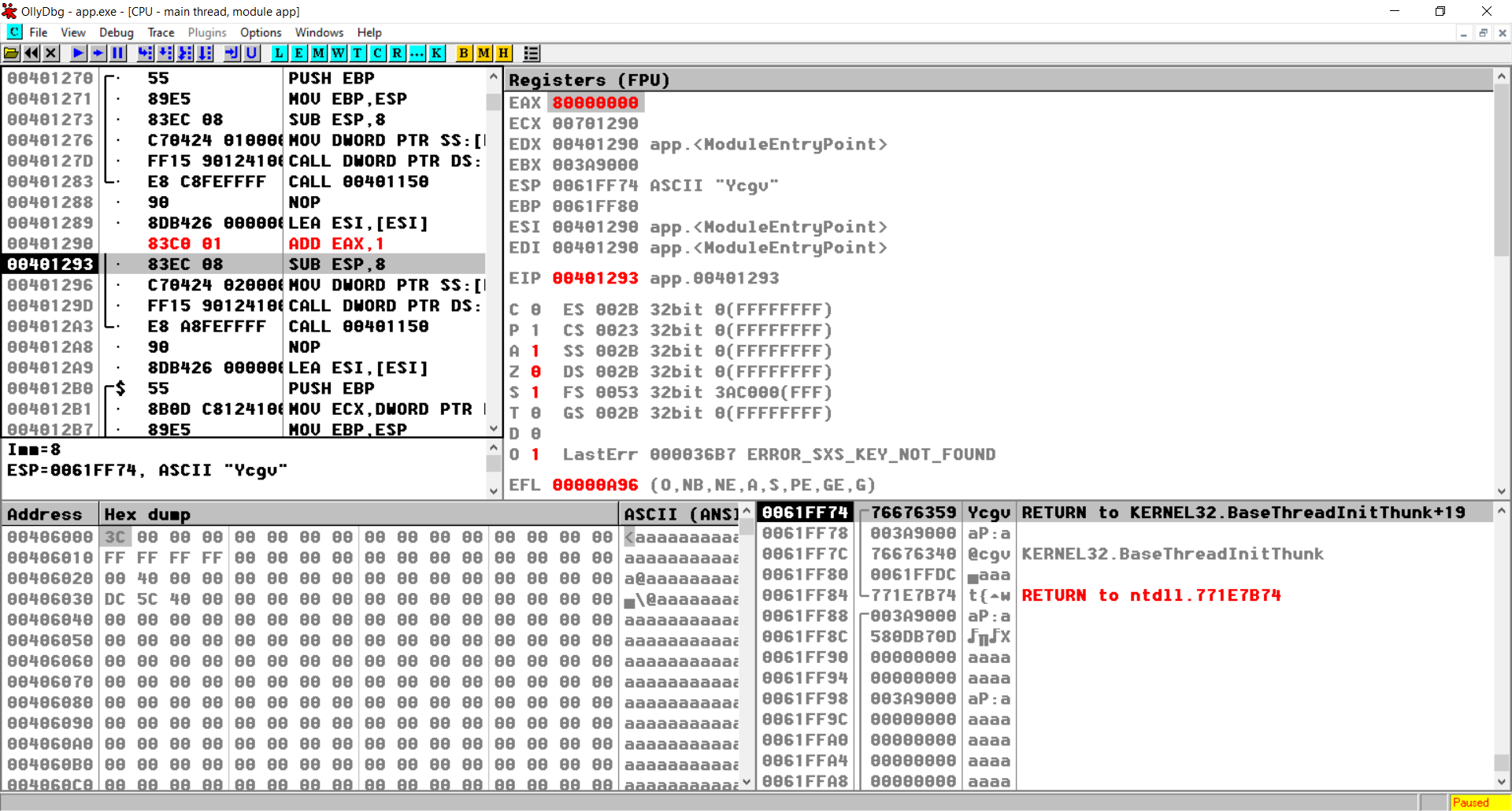


Рисунок 4 – Изменение флагов

Теперь используем команду PUSH (инструкция для помещения значения в стек). Обратим внимание что до применения этой команды указатель на начало стека ESP имеет адрес 0061FF74 и по этому адресу лежит значение 76676359 как показано на рисунке 1. После применения команды PUSH ЕАХ (00401293) ESP получил адрес = 0061FF6C и в стек было занесено значение регистра ЕАХ = 80000000 (рис. 5).

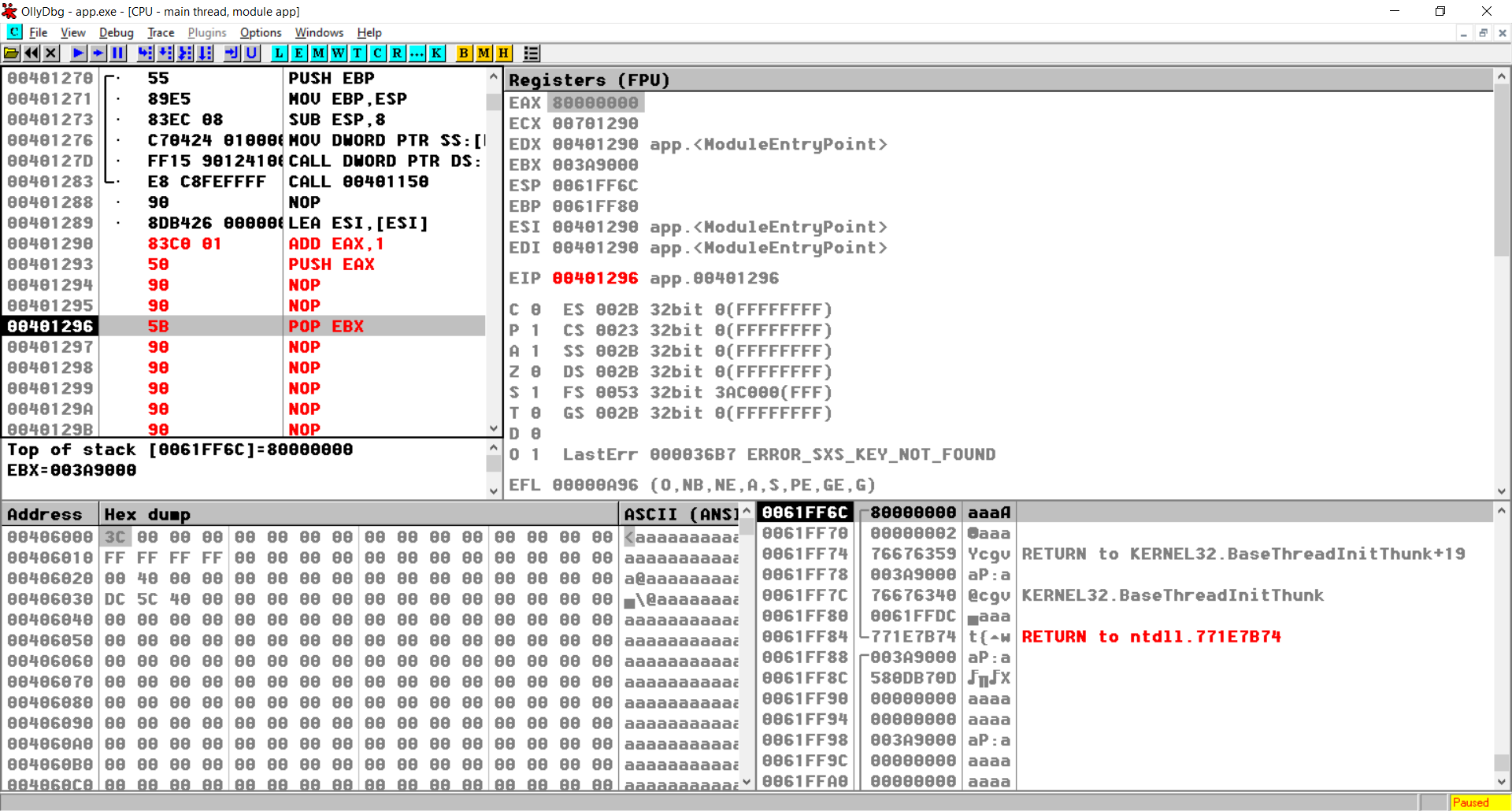


Рисунок 5 – Занесение в стек

Инструкция POP является обратной по отношению к PUSH: она достает первое значение из стека и помещает его в указанное параметром инструкции место назначения. Воспользуемся командой POP ЕВХ. Результат представлен на рисунке 6.

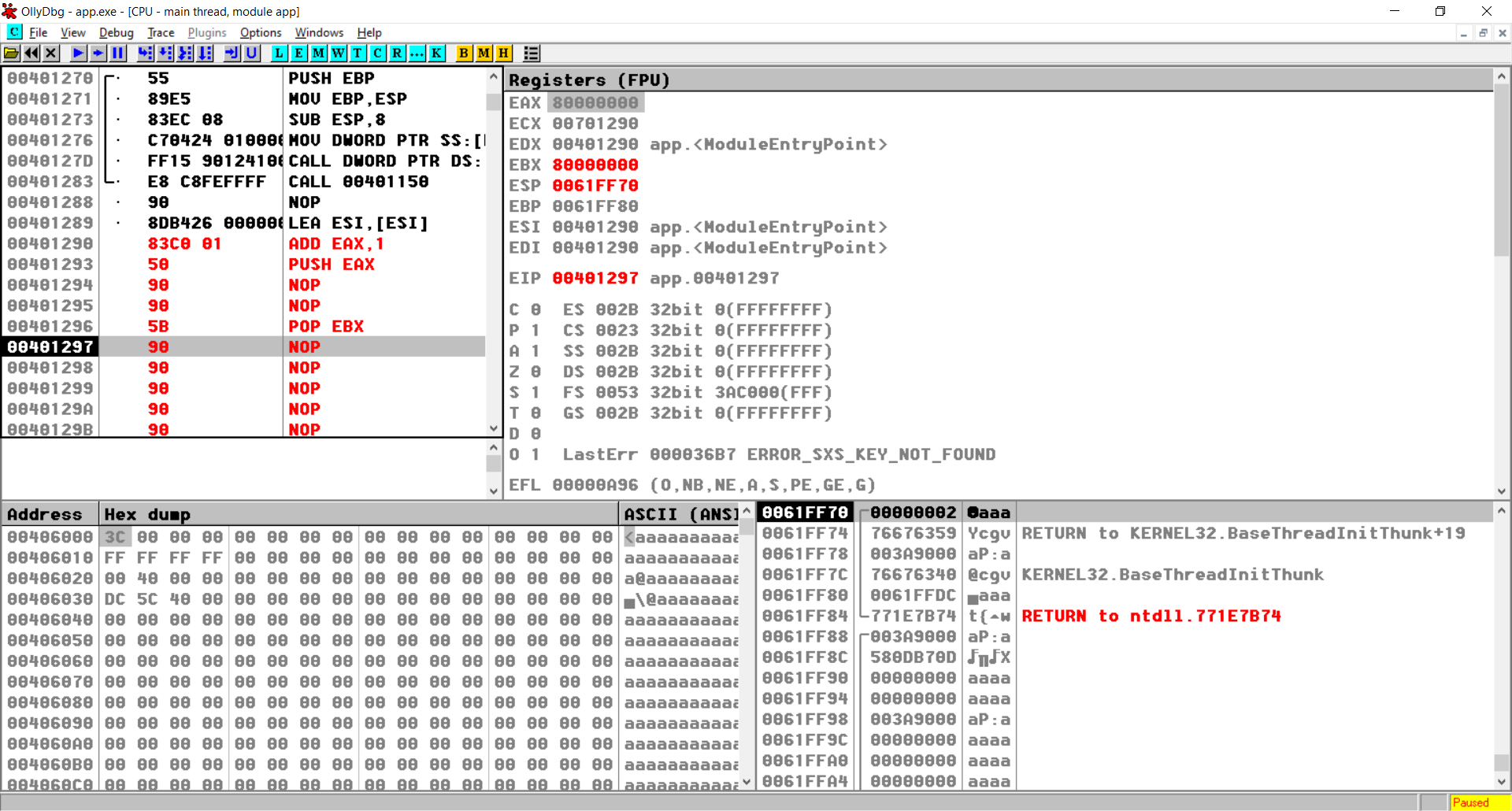


Рисунок 6 – Извлечение из стека

Теперь используем команду MOV с 8-ми разрядным регистром CL (команда 0040129D) и с 16-ти разрядным регистром DX (команда 0040129F). Результат этих команд представлен на рисунке 7.

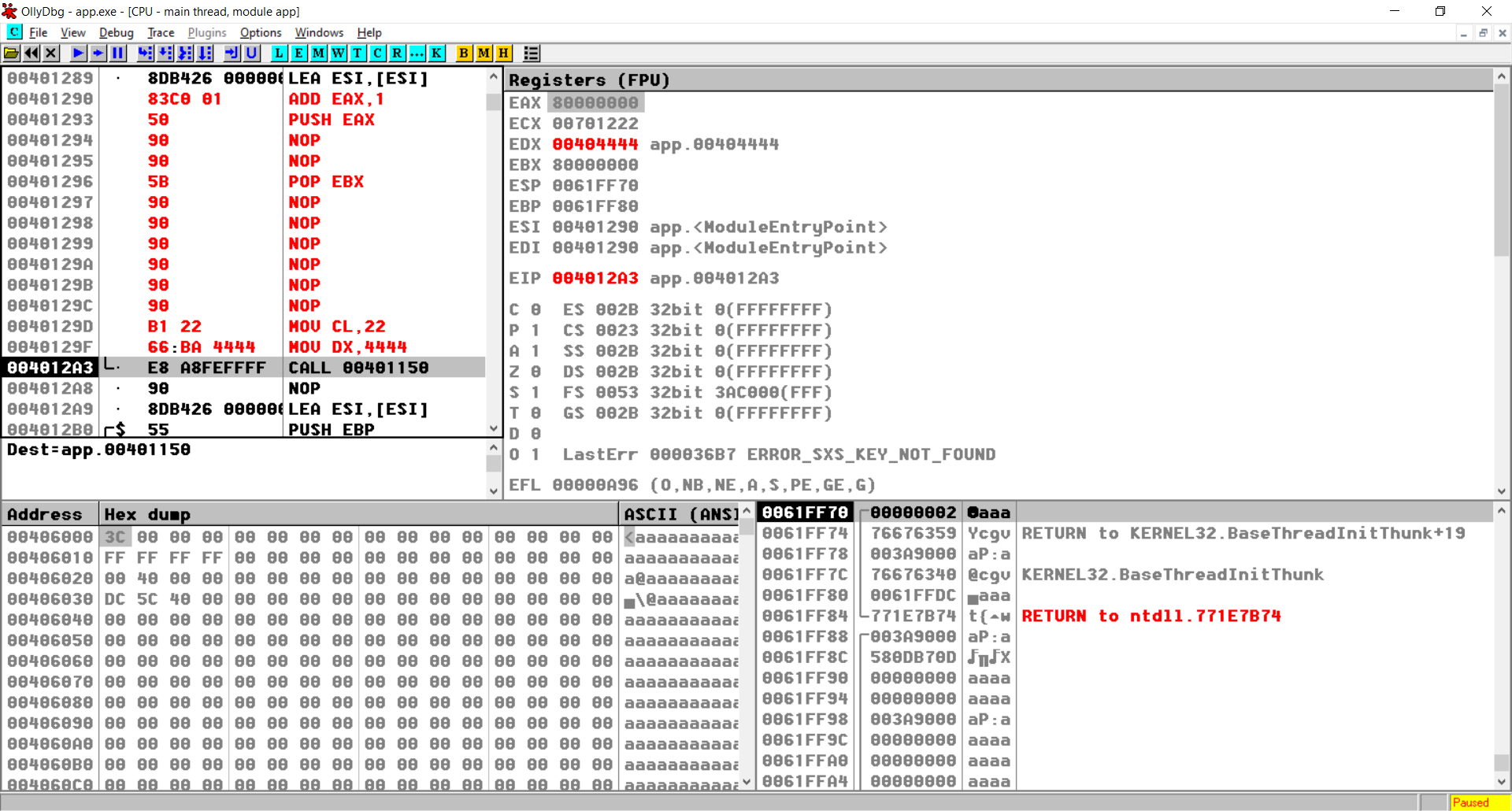


Рисунок 7 – Применение команды MOV

Теперь изменим значение регистра EIP. Для этого выберем команду по адресу 004012В0 и в меню при нажатии правой клавишей выберем «New origin here». Результат представлен на рисунке 8.

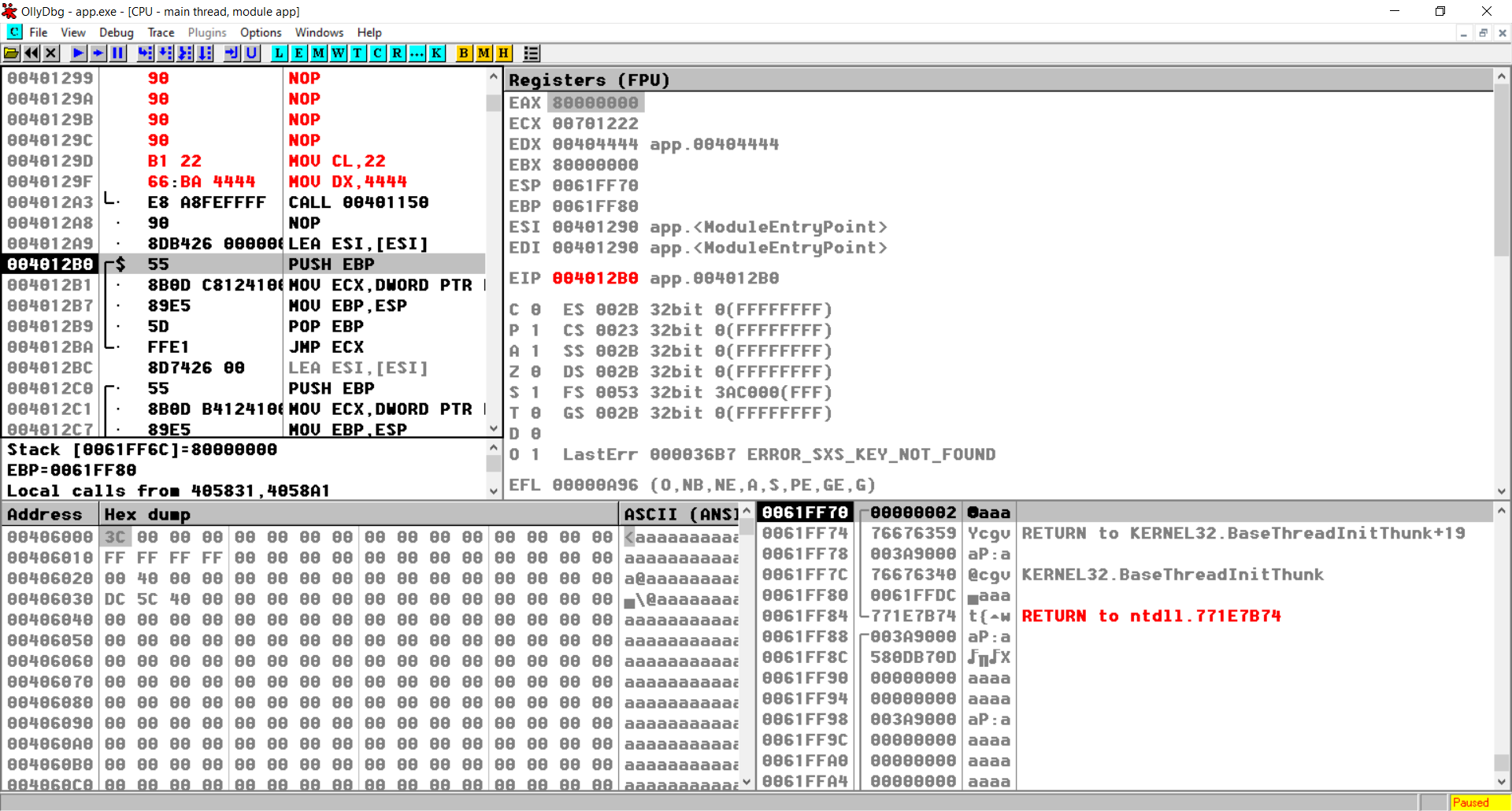


Рисунок 8 – Изменение значения регистра EIP

ВЫВОДЫ

В ходе выполнения лабораторной работы были исследованы архитектура 32-разрядного процессора и возможности отладчика OllyDbg при разработке и отладке приложения Win32. Были приобретены практические навыки по анализу и отладке программ на языке ассемблера.