**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»  
(БГТУ им. В.Г.Шухова)**

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

Лабораторная работа №1  
дисциплина: Архитектура вычислительных систем  
тема: «Разработка программ на ассемблере.

Работа с отладчиком OllyDbg и пакетом masm32»

Выполнил: ст. группы ВТ-31  
Ковалёв И. Д.  
Проверил: Осипов О. В.

**Белгород 2019**

**Цель работы:** получить навыки создания и отладки простейших программ на ассемблере с использованием пакета masm32 и отладчика OllyDbg.

**Задания для выполнения к работе**

1. Ознакомиться со средой OllyDbg и компилятором masm32.
2. Создать и скомпилировать программу в соответствии с вариантом задания.
3. Отладить программу.
4. С помощью OllyDbg определить местонахождение переменных в сегменте данных, а также их размер.
5. Выполнить пошаговую трассировку программы. Определить какие регистры изменяют свои значения в процессе выполнения команд.

**Выполнение работы**

1. Создан файл lab1.asm со следующим содержимым:

.386 Тип процессора

.MODEL FLAT, STDCALL Модель памяти и стиль вызова подпрограмм

OPTION CASEMAP: NONE Чувствительность к регистру

INCLUDE F:\PROGRAMMS\MASM32\INCLUDE\WINDOWS.INC

INCLUDE F:\PROGRAMMS\MASM32\INCLUDE\KERNEL32.INC

INCLUDE F:\PROGRAMMS\MASM32\INCLUDE\USER32.INC

INCLUDELIB F:\PROGRAMMS\MASM32\LIB\USER32.LIB

INCLUDELIB F:\PROGRAMMS\MASM32\LIB\KERNEL32.LIB

.DATA

Sstr DB 13, 10, "Strings", 0 массив из 9 однобайтовых чисел

p DB 5 одно однобайтовое число

k DW 500 одно двухбайтовое число

s DD 5000 одно четырехбайтовое число

ten DT 88.38 10-байтовое нецелое

.CODE

START:

XOR EAX, EAX очистка регистра ЕАХ

MOV AX, k в младшие 16 бит ЕАХ поместить переменную к, будет 01F4 = 500

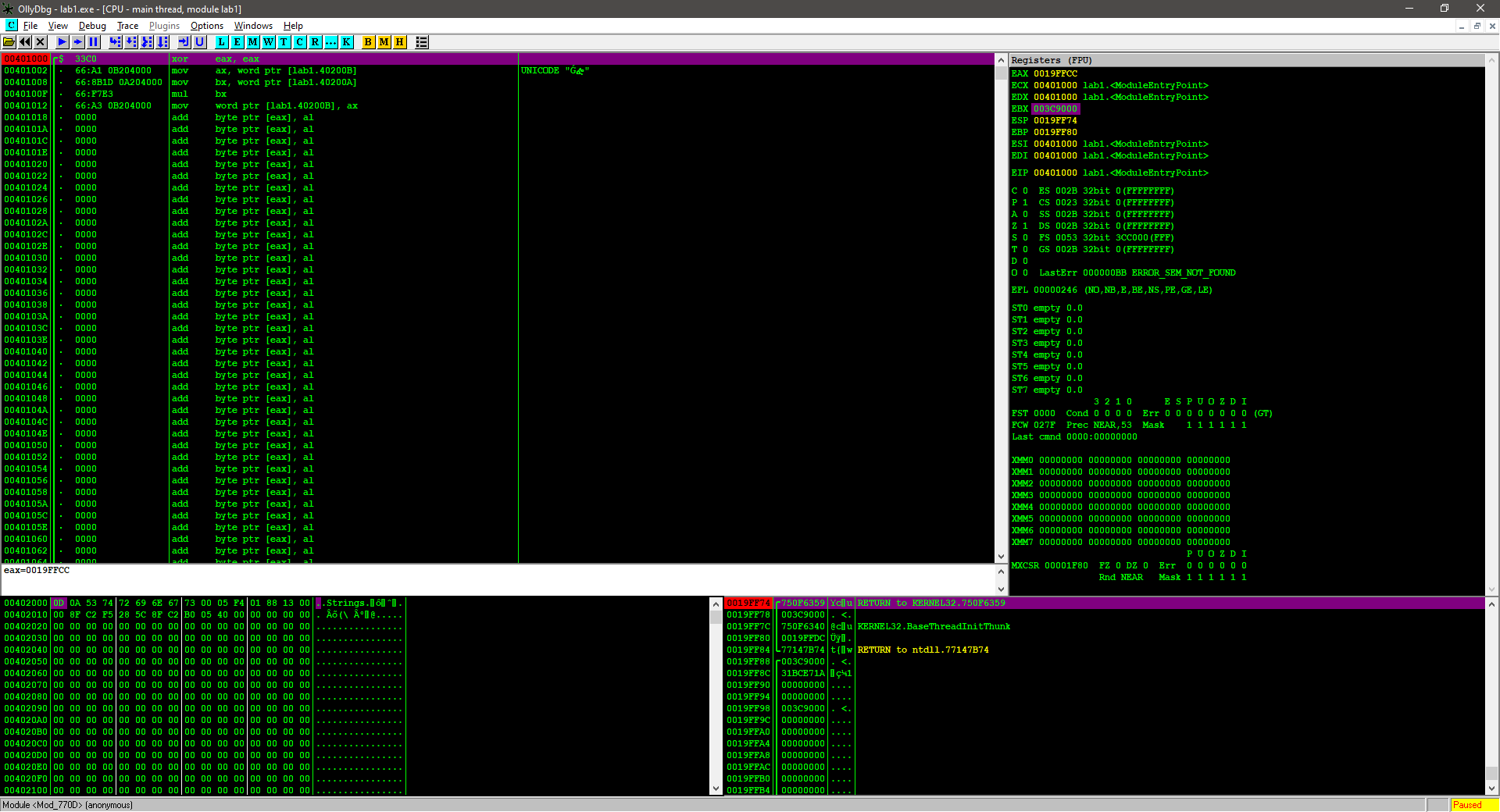
MOV BX, WORD PTR [p] в младшие 16 бит ЕВХ поместить переменную p.

MUL BX 99C4 EAX

MOV k, AX

END START

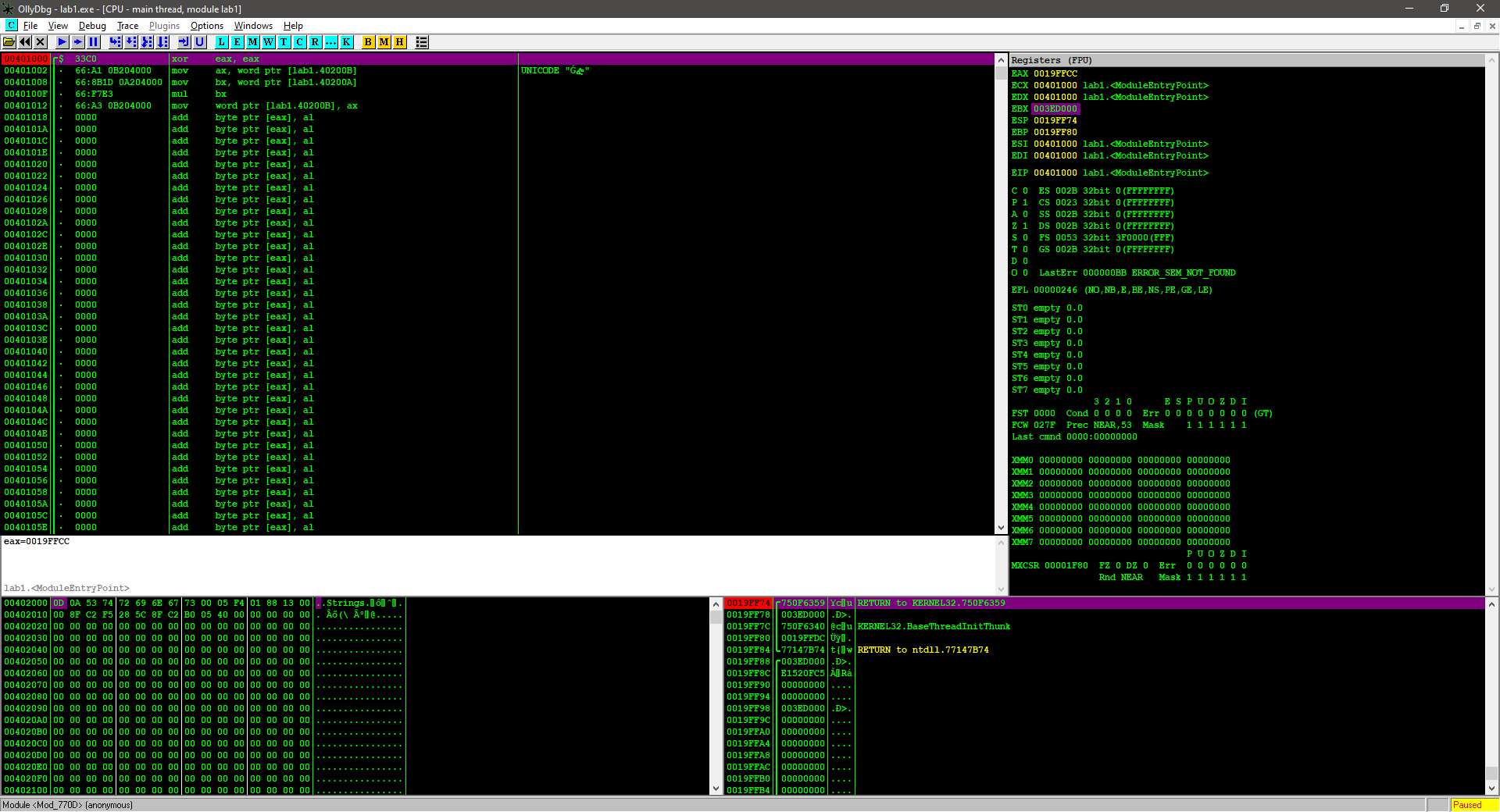
1. Программа была скомпилирована; в результате получен исполняемый файл lab1.exe
2. Исполняемый файл был открыт в OllyDbg
3. Сегмент данных содержит:



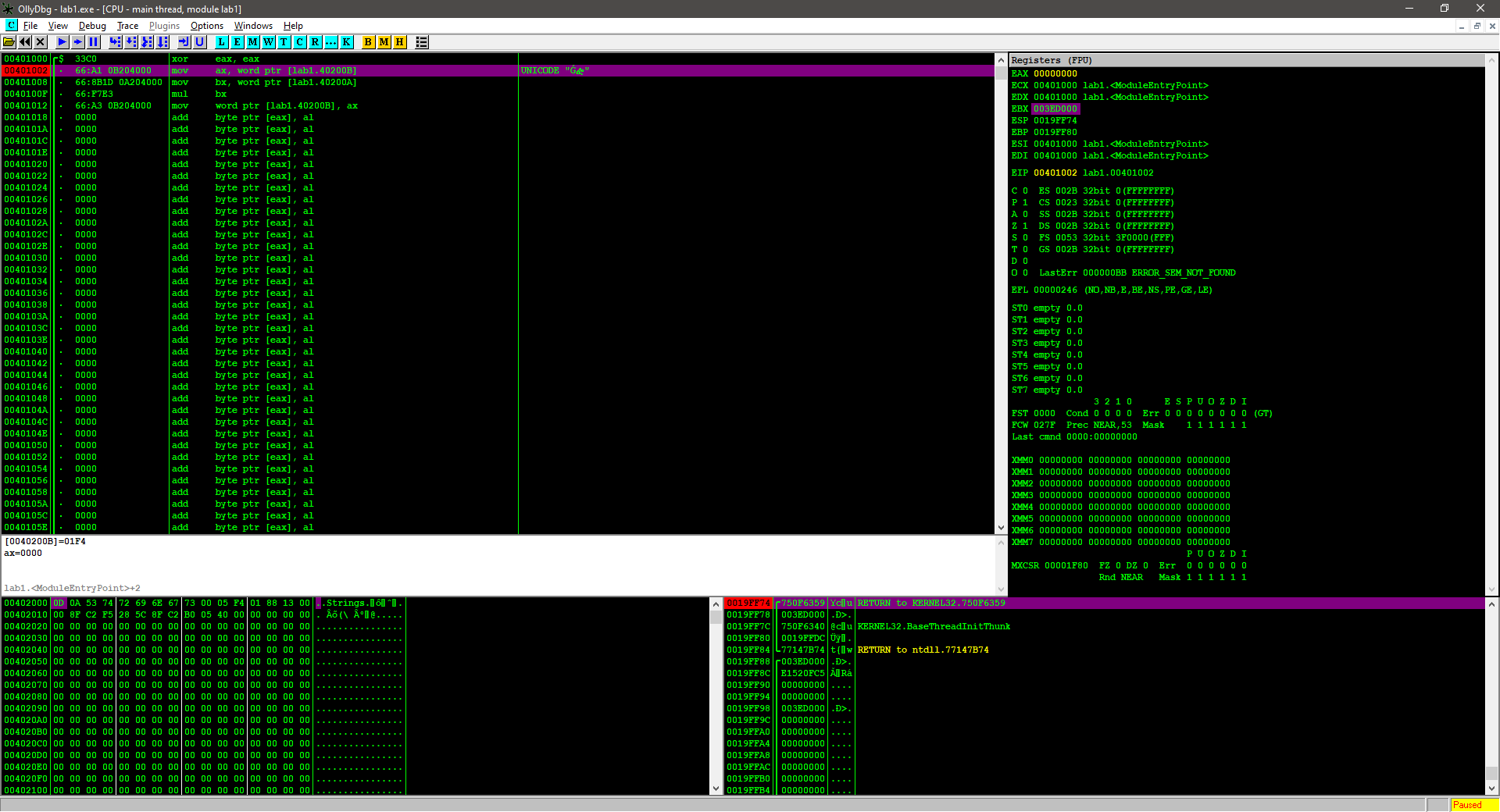
|  |  |  |  |
| --- | --- | --- | --- |
| Название переменной | Начальный адрес | Конечный адрес | Размер данных, байт |
| **Sstr** | 00402000 | 00402009 | 9 |
| **p** | 0040200A | 0040200A | 1 |
| **k** | 0040200B | 0040200C | 2 |
| **s** | 0040200D | 00402010 | 4 |
| **ten** | 00402011 | 0040201A | 10 |
| Общий размер сегмента данных: | | | **26** |

Пошаговое выполнение программы

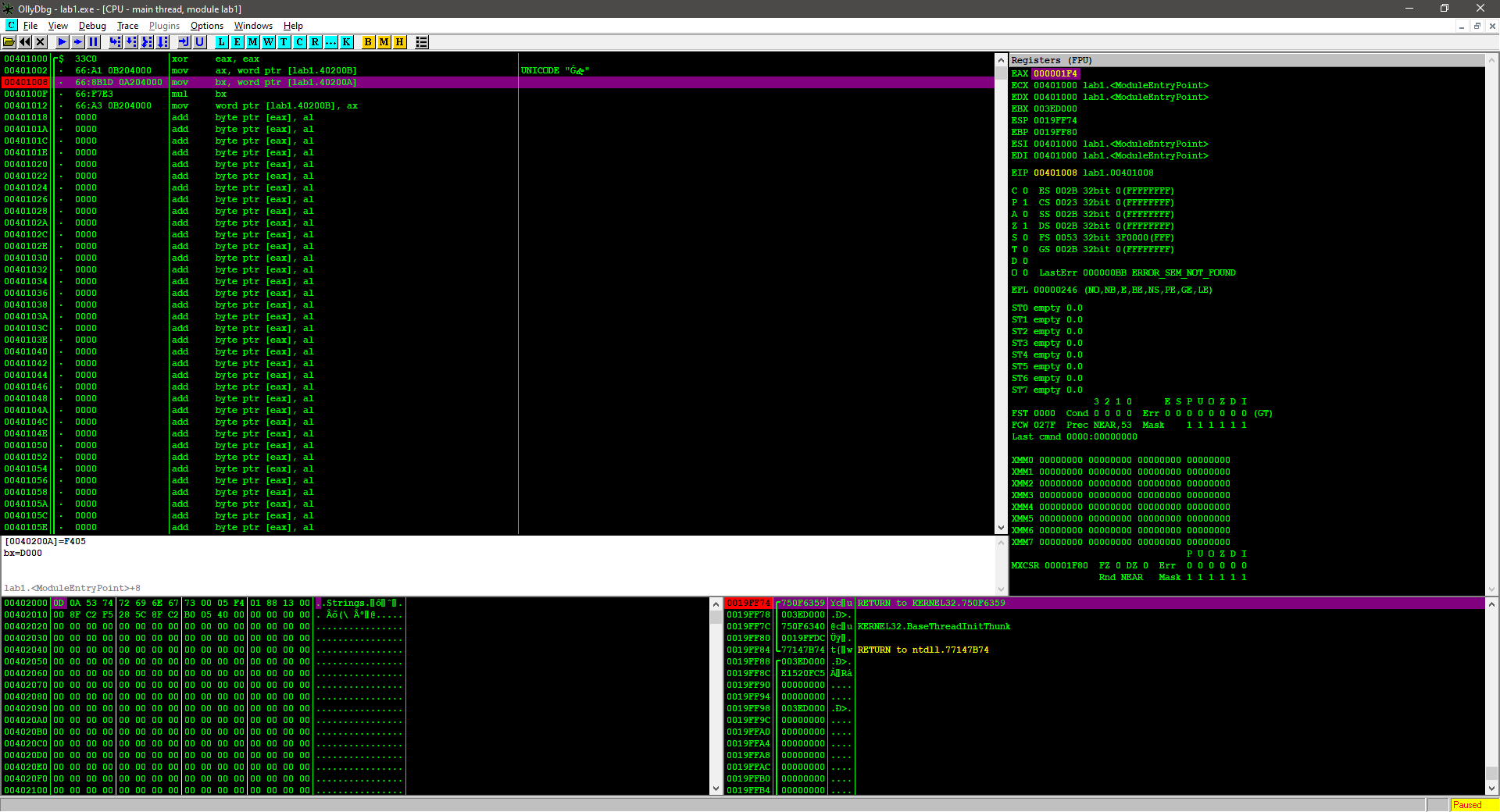
* 1. Исходное состояние регистров:



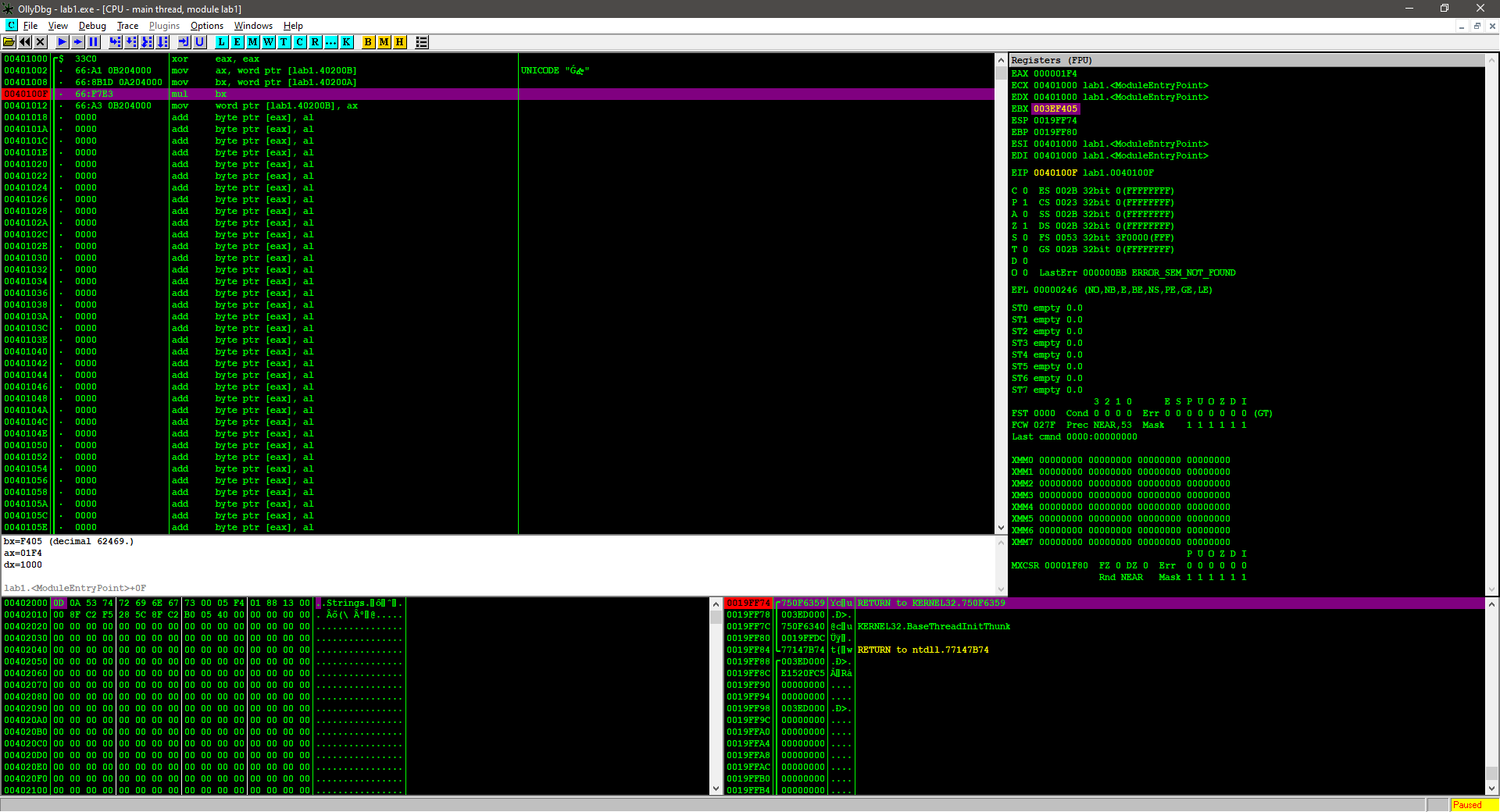
5.2 XOR EAX, EAX. Код команды – 66:А1 0В204000. Проводит операцию с содержимым регистра EAX. Результатом будет 0 в данном регистре. EIP увеличен на 2.



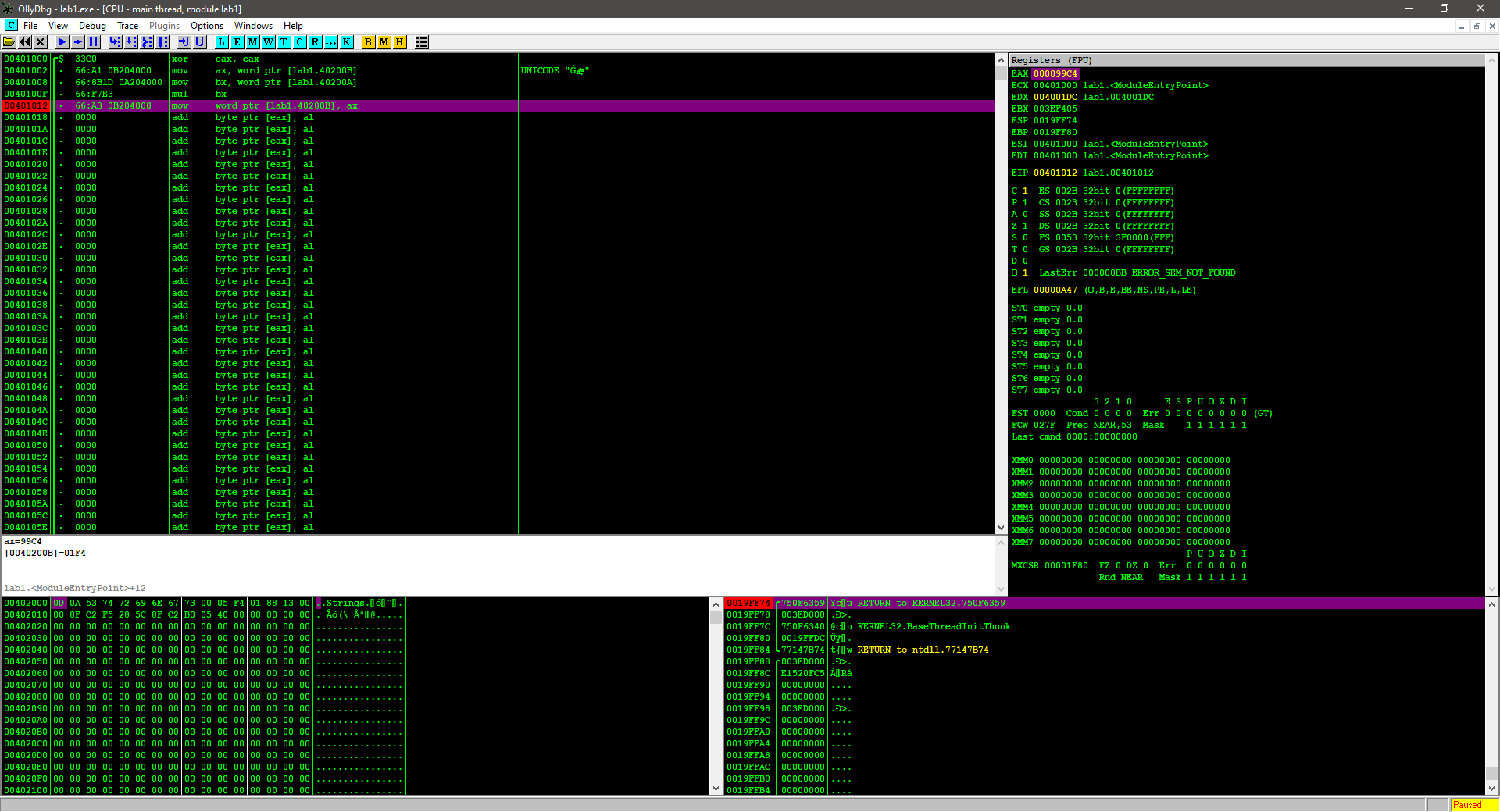
5.3 MOV AX, k. Код команды – 66:А1 0В204000. Помещает в младшие 16 бит регистра EAX значение переменной k. EIP увеличен на 6.



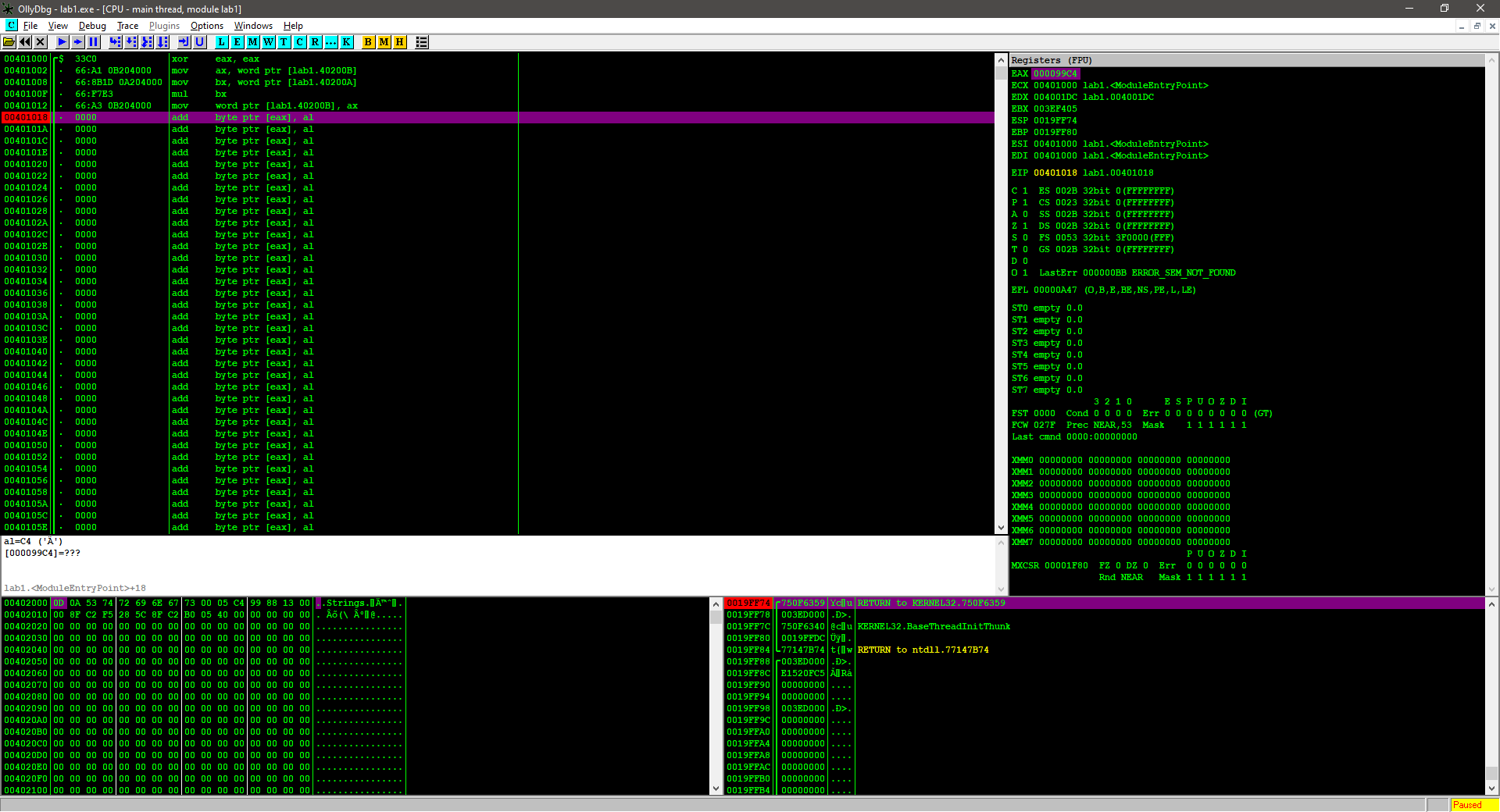
5.4 MOV BX, WORD PTR [p]. Код команды – 66:8B1D 0A204000. Помещает в младшие 16 бит регистра EBX содержимое памяти по адресу k. EIP увеличен на 7.



5.5 MUL BX. Код команды – 66:F7E3. Умножит содержимое регистра АХ на ВХ, результат умножения запишется в регистры DX и АХ. EIP увеличен на 3.



5.6 MOV k, AX. Код команды – 66:А3 0В204000. По адресу переменной k запишется содержимое регистра АХ. EIP увеличен на 6.



В результате содержимое памяти будет таким:

