**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

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 ПВ-31

Донцов А.А.

Проверил: Осипов О.В.

Белгород 2019

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

**Вариант 1**

.386

.model flat, stdcall

option casemap: none

include d:\masm32\include\windows.inc

include d:\masm32\include\kernel32.inc

include d:\masm32\include\user32.inc

includelib d:\masm32\lib\user32.lib

includelib d:\masm32\lib\kernel32.lib

.DATA

DB "MASM32", 0

DB 250, 251, 252, 254

a DW 500

b DW 2

cc DW 250

float1 DD 13.5

float2 DD 26.5

dmas DQ 5 DUP (5)

.CODE

START:

MOV AX, a

MOV BX, b

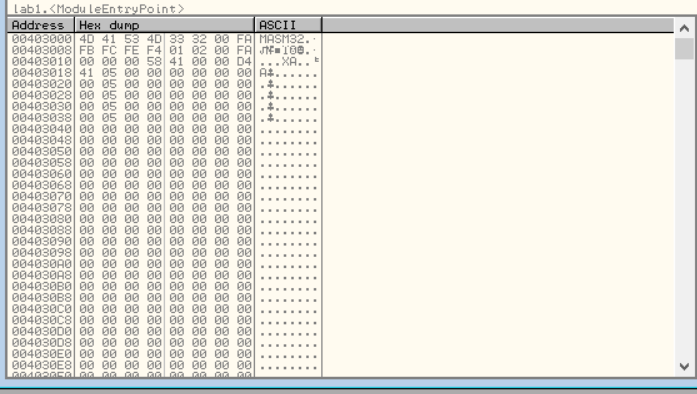
MOV CX, cc

push NULL

call ExitProcess

END START

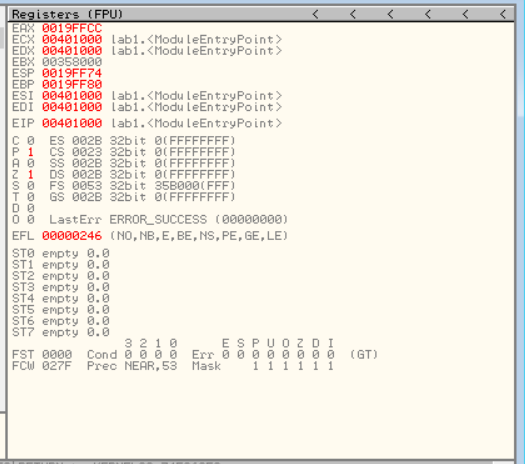
Сегмент данных содержит строку, массив цифр, 5 переменнх и один массив.



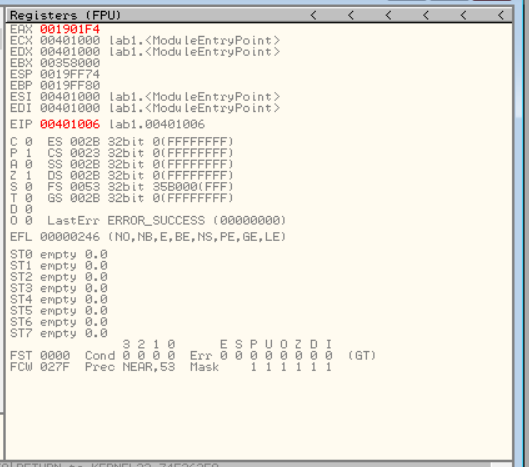
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Название переменной** | **Начальный адрес** | **Конечный адрес** | **Размер данных, байт** | **Тип** |
| **-** | 00403000 | 00403005 | 6 | Строка |
| **-** | 00403006 | 00403006 | 1 | символ окончания строки (0) |
| **-** | 00403007 | 0040300A | 4 | Массив |
| **a** | 0040300B | 0040300C | 2 | 2-байтовое целое |
| **b** | 0040300D | 0040300E | 2 | 2-байтовое целое |
| **cc** | 0040300F | 00403010 | 2 | 2-байтовое целое |
| **float1** | 00403011 | 00403014 | 4 | 4-байтовое вещественное |
| **float2** | 00403015 | 00403018 | 4 | 4-байтовое вещественное |
| **dmas** | 0040301A | 00303040 | 40 | Массив из 8-байтовых чисел |
| Общий размер сегмента данных: | | | **65** |  |

Пошаговое выполнение программы:

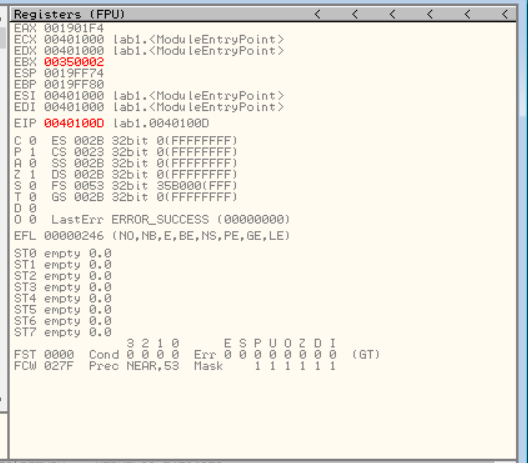
Исходное состояние регистров:



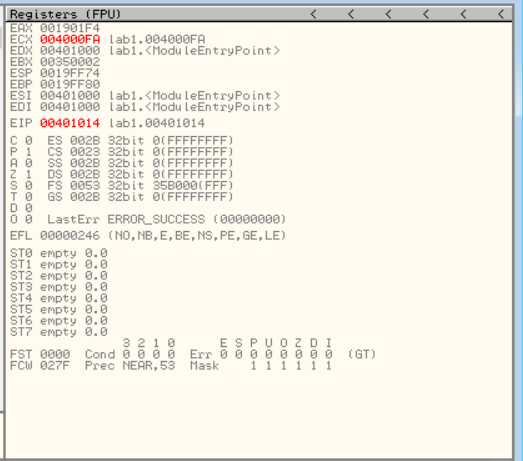
1. MOV AX, a

 Код команды – **A1 0B30400**. Команда пересылает в регистр **AX** (младшую часть EA**X**) 2 байта из ячейки памяти с адресом 0040300B (переменная **a**). Размер пересылаемых данных – 2 байт. Увеличивает **EIP** на 5 (размер кода команды).

1. MOV BX, b

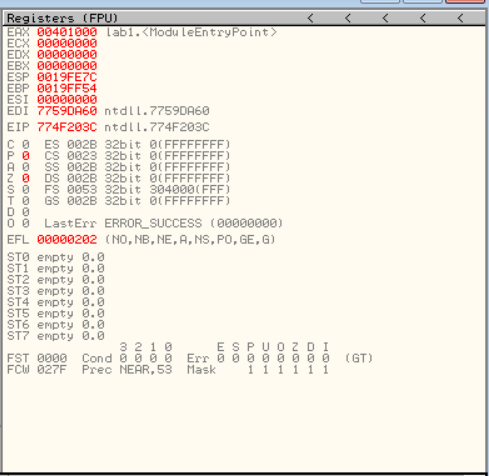
 Код команды – **8B1D 0D304**. Команда пересылает в регистр **BX** (младшую часть EB**X**) байт из ячейки памяти с адресом 40300D (переменная **b**). Размер пересылаемых данных – 2 байта. Увеличивает **EIP** на 5 (размер кода команды).

1. MOV CX, cc



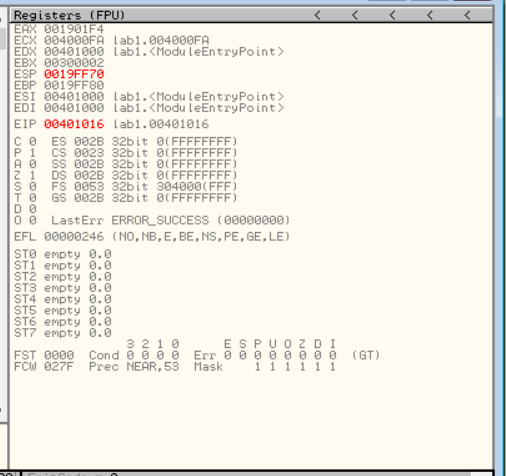
Код команды – **8B0D 0F304**. Команда пересылает в регистр **CX** (младшую часть **ECX**) 2 байта из ячейки памяти с адресом 40300F (переменная **cc**). Размер пересылаемых данных – 2 байта. Увеличивает **EIP** на 5 (размер кода команды).

5.push NULL



Код команды – **00**. Команда пересылает в регистр **ESP** значение 0(1 байт). Размер пересылаемых данных – 1 байт. Увеличивает **EIP** на 2 (размер кода команды).

6.call ExitProcess

Код команды –**E8 01000000**. Вызывает команду выхода из процесса. Увеличивает EIP на 6