Федеральное государственное бюджетное образовательное учреждение высшего образования

«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» (МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ _____ИНФОРМАТИКА И СИСТЕМЫ УПРАВЛЕНИЯ_____

КАФЕДРА _____КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ_____

О Т Ч Е Т

по лабораторной работе № ___1__

Дисциплина: __Машинно-зависимые языки и основы компиляции_____

Название лабораторной работы: _Изучение среды и отладчика_ассемблера

_____

Студент гр. ___**ИУ6-42Б** _____ _**Медведев АЕ**_

(Подпись, дата) (И.О. Фамилия)

Преподаватель _____ _____

(Подпись, дата) (И.О. Фамилия)

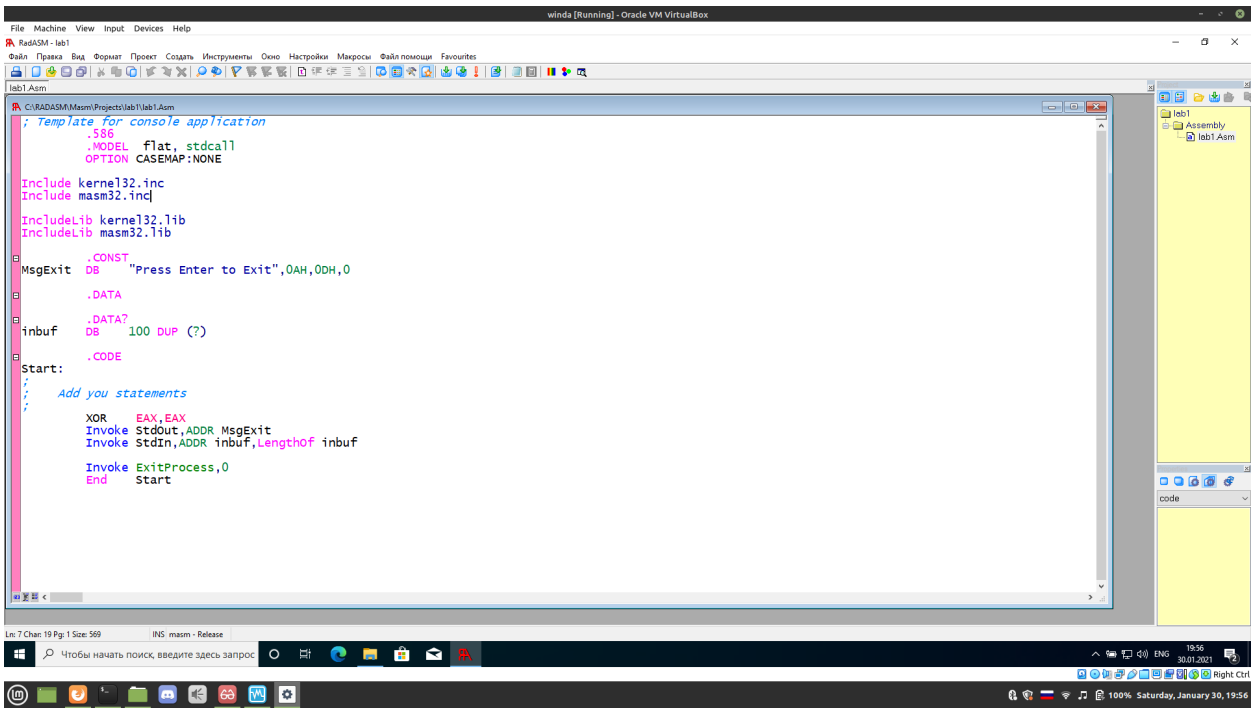
Москва, 2021_

Цель работы:

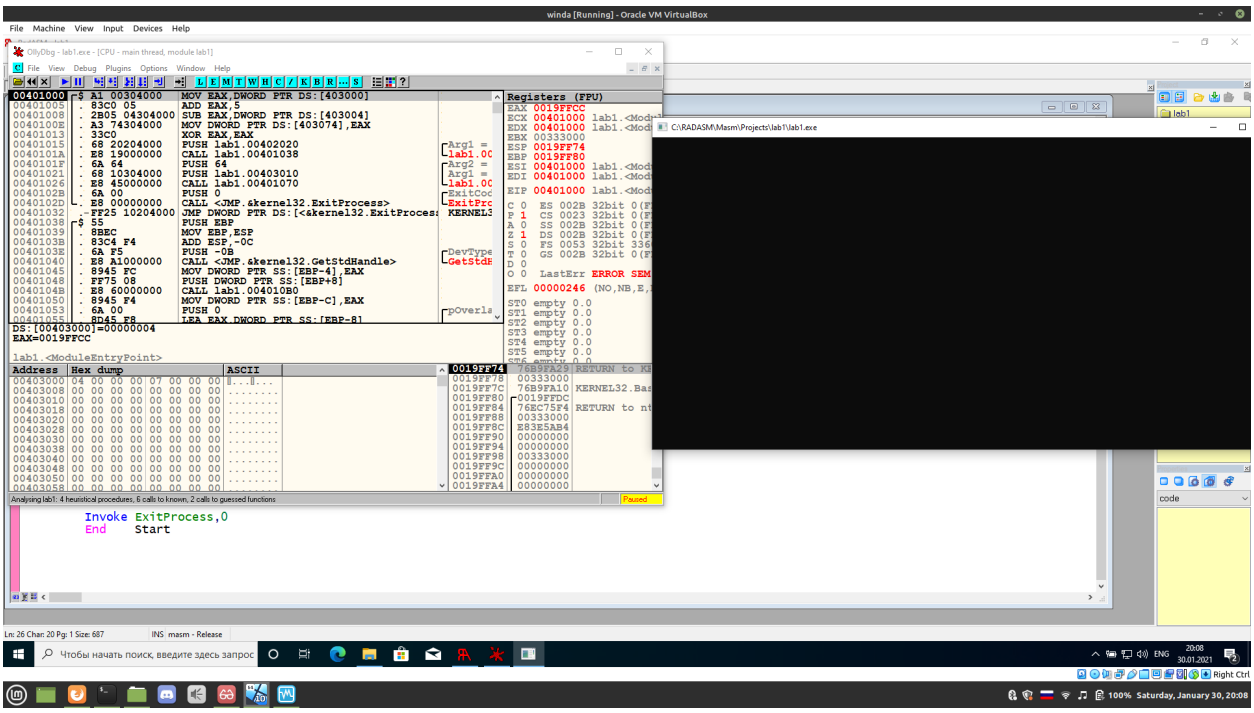
Изучение процессов создания, запуска и отладки программ на ассемблере в среде программирования RADAsm с использованием 32-разрядного отладчика OlleDBG.

Задание:

1. Запустите RADAsm, создайте файл проекта по шаблону консольного приложения. Внимательно изучите структуру программы и зафиксируйте текст с комментариями в отчете.19

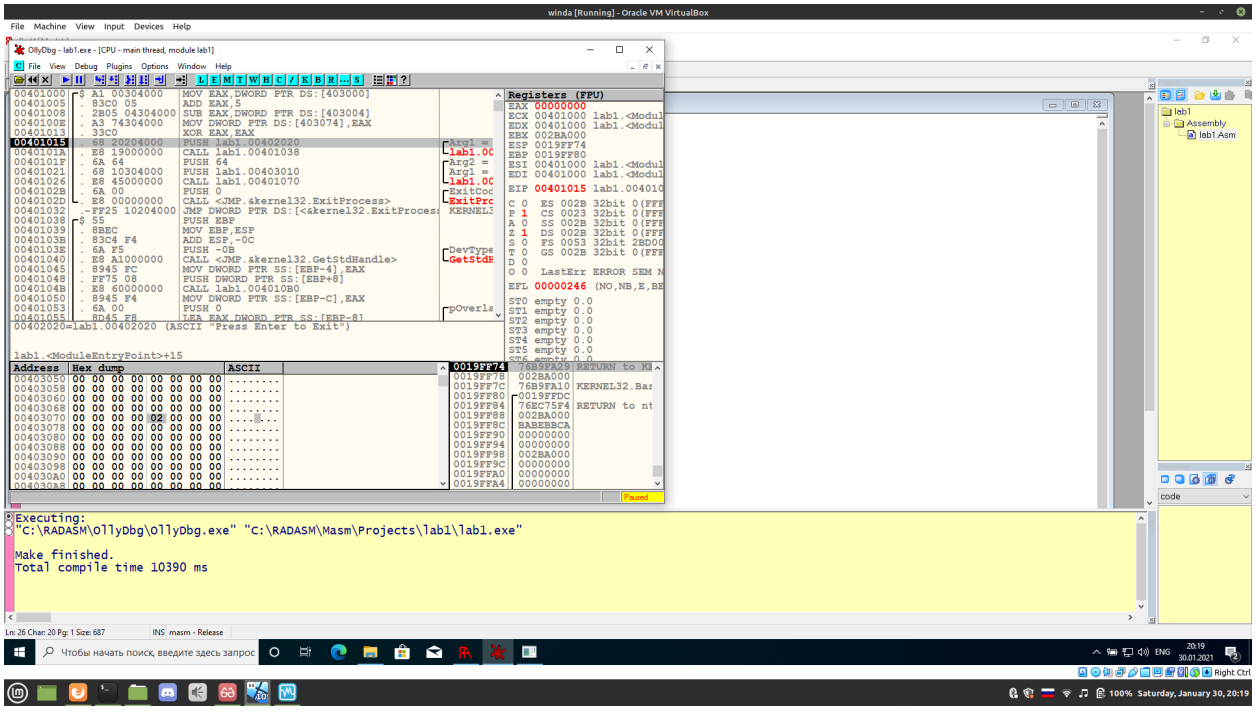


(рис. 1 Дефолтный проект)



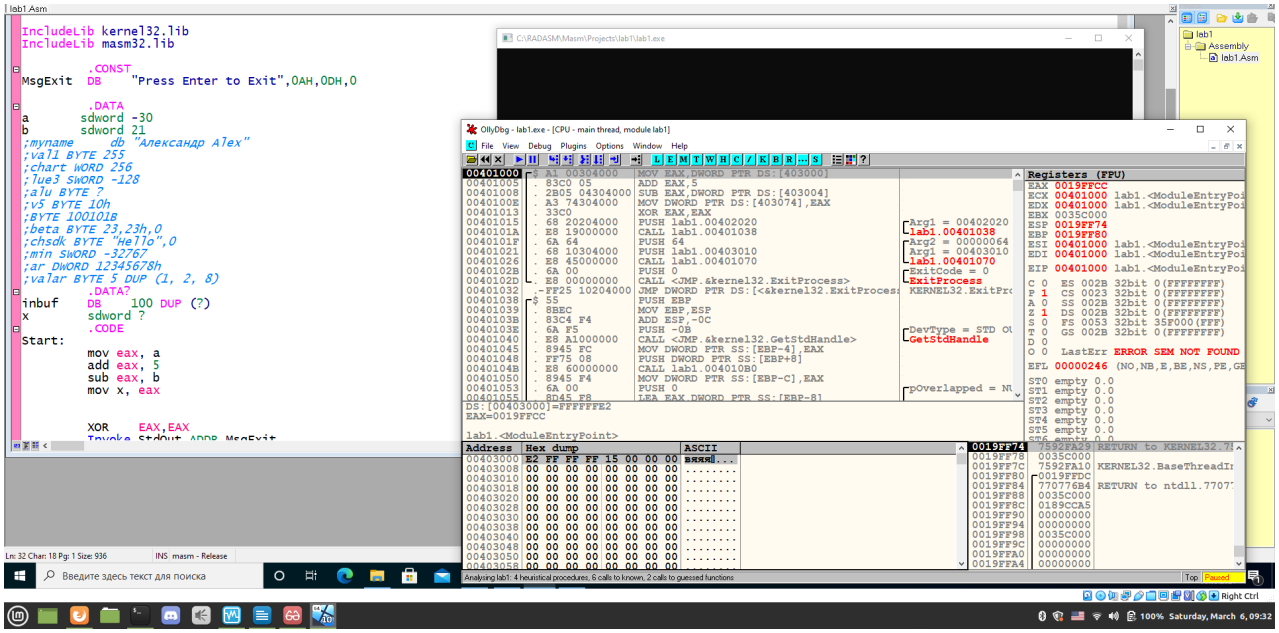
(рис. 2 Запуск стандартного проекта)

2. Запустите шаблон на выполнение и просмотрите все полученные сообщения. Убедитесь, что текст программы и настройки среды не содержат ошибок.

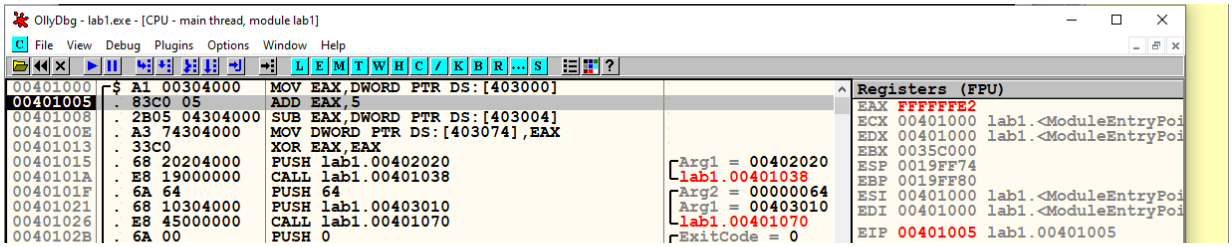


(рис. 3 ошибок при сборке нет)

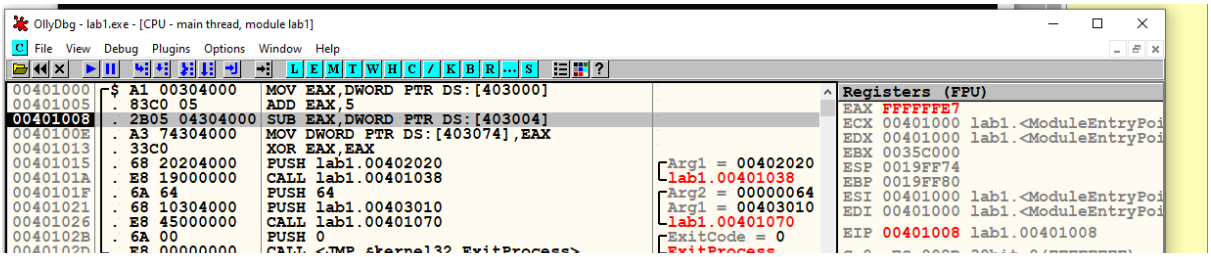
3. Добавьте директивы определения данных и команды сложения и вычитания, описанные в разделе 3 настоящих методических указаний. Найдите в отладчике внутреннее представление исходных данных, зафиксируйте его в отчете и поясните.



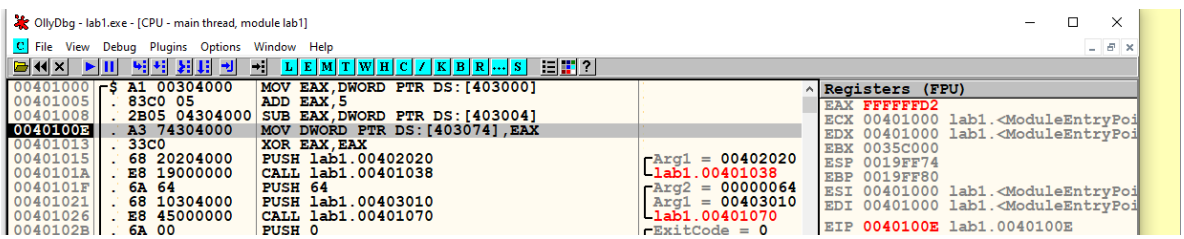
(рис. 4 Код пункта 3 и данные -30, 21)



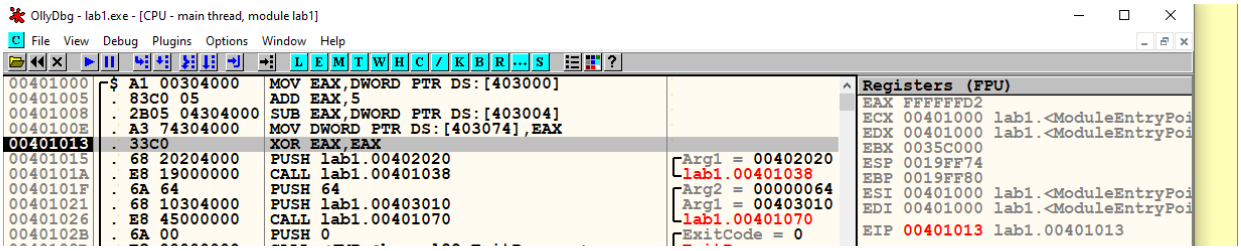
(рис. 5 запись в eax первого числа)



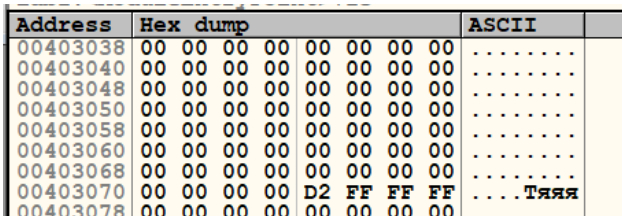
(рис. 6 добавление к eax 5)



(рис. 7 вычитание из eax второй переменной)



(рис. 8 запись ответа в переменную X)



(рис. 9 Представление переменной X в дампе памяти)

Проследите в отладчике выполнение набранной вами программы и зафиксируйте в отчете результаты выполнения каждой добавленной команды (изменение регистров, флагов и полей данных).

4. Введите следующие строки в раздел описания инициированных данных и определите с помощью отладчика внутренние представление этих данных в памяти. Результаты проанализируйте и занесите в отчет.

val1 BYTE 255

chart WORD 256

lue3 SWORD -128

alu BYTE ?

v5 BYTE 10h

BYTE 100101B

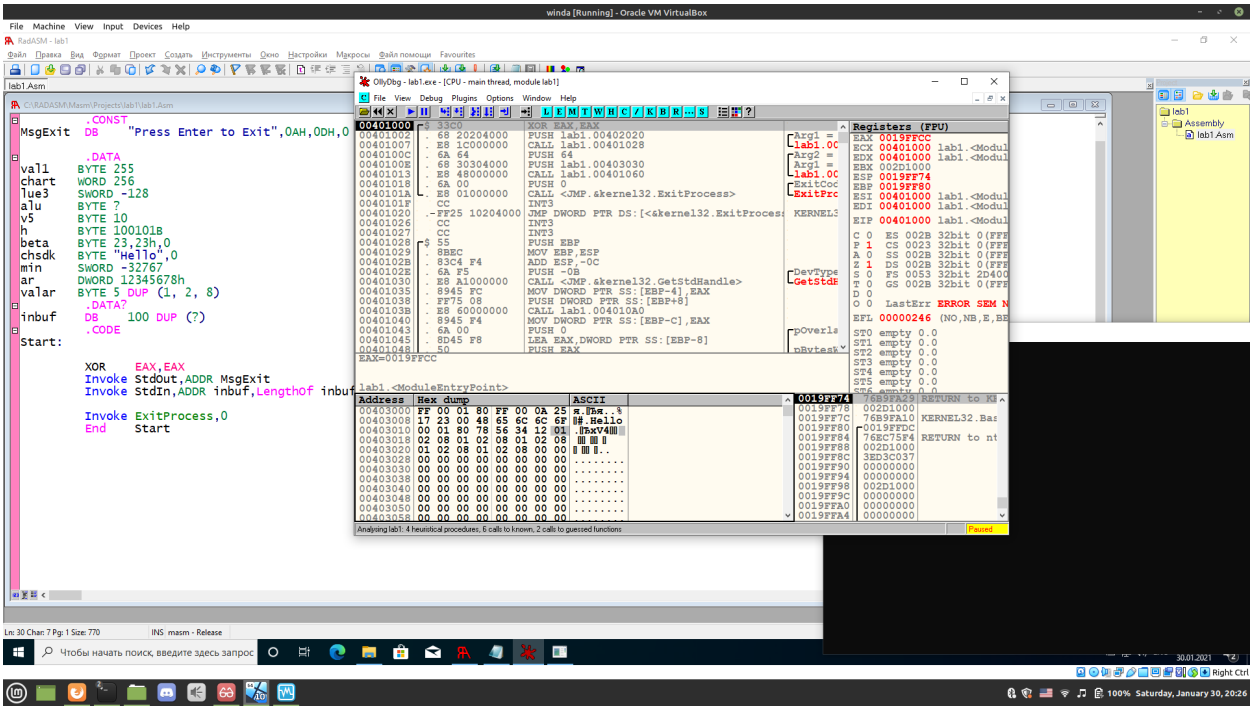
beta BYTE 23,23h,0ch

sdk BYTE Hello ,0

min SWORD -32767

ar DWORD 12345678h

valar BYTE 5 DUP (1, 2, 8)



(рис. 10 Дамп памяти пункта 4)

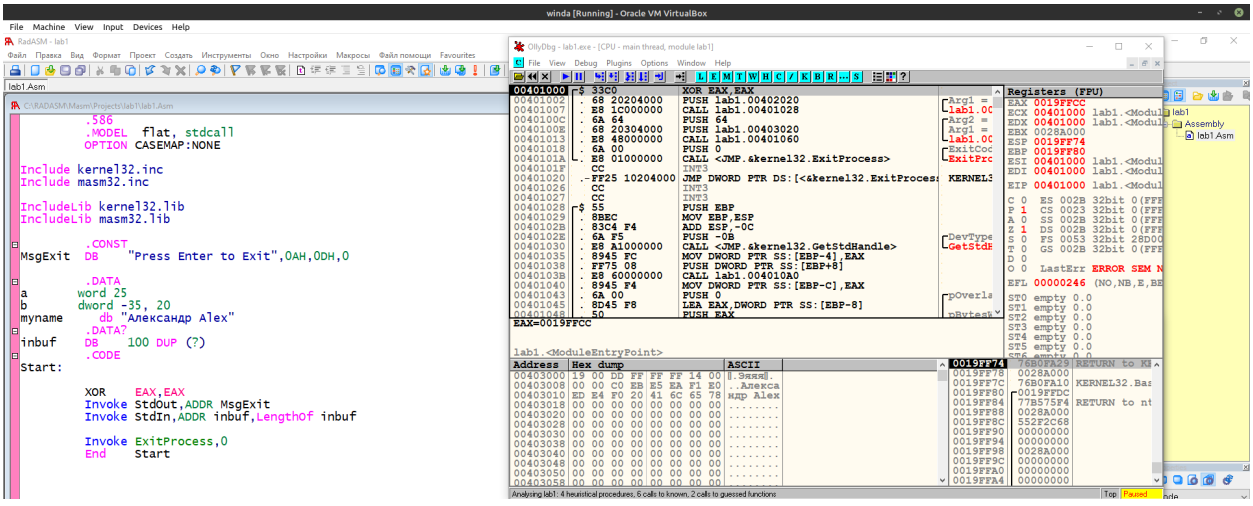
5. Определите в памяти следующие данные:

а) целое число 25 размером 2 байта со знаком;

б) двойное слово, содержащее число -35;20

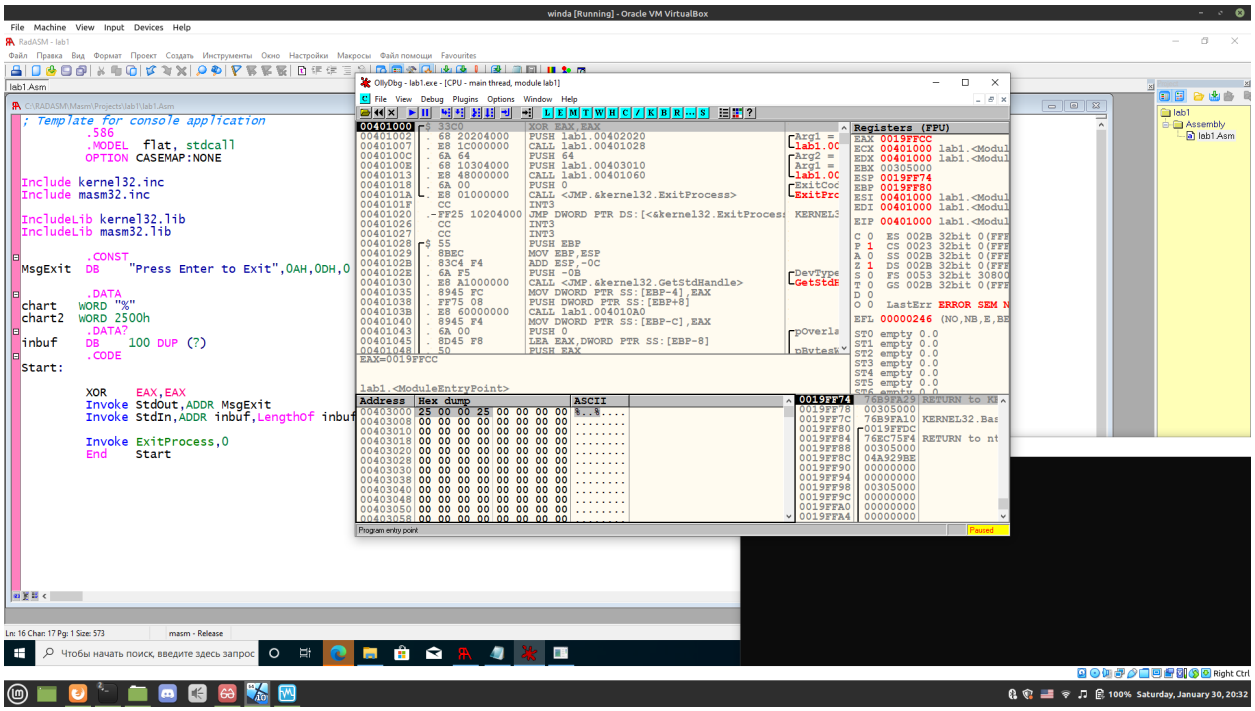
в) символьную строку, содержащую ваше имя (русскими буквами и латинскими буквами).

Зафиксируйте в отчете внутреннее представление этих данных и дайте пояснение.



(рис. 11 Дамп памяти пункта 5)

6. Определите несколькими способами в программе числа, которые во внутреннем представлении (в отладчике) будут выглядеть как 25 00 и 00 25. Проверьте правильность ваших предположений, введя соответствующие строки в программу. Зафиксируйте результаты в отчете.



(рис. 12 Дамп памяти пункта 6)

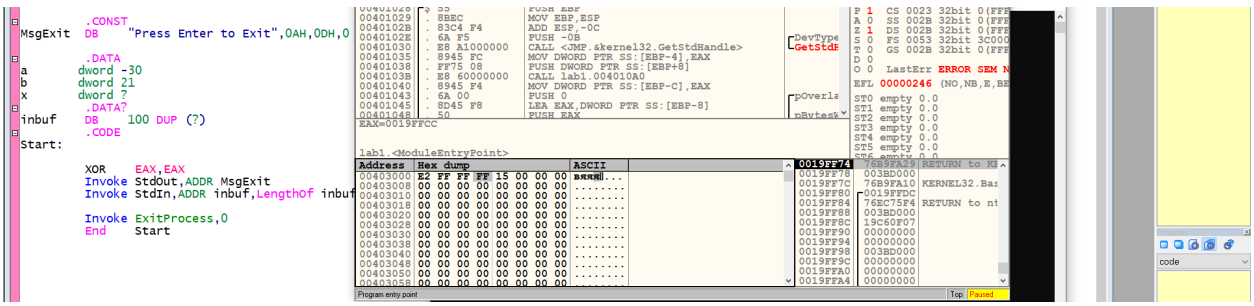
7. Замените директивы описания знаковых данных на беззнаковые:

A DWORD -30

B DWORD 21

X DWORD ?

Запустите программу и прокомментируйте результат.



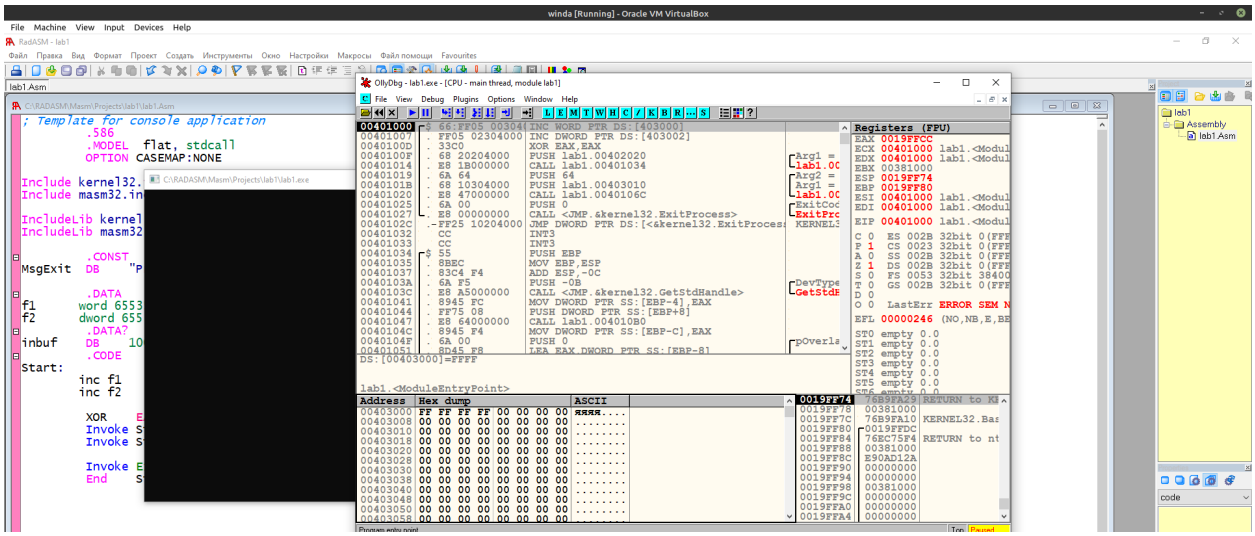
(рис. 13 Дам памяти пункта 7)

8. Добавьте в программу переменную F1=65535 размером слово и переменную F2= 65535 размером двойное слово. Вставьте в программу команды сложения этих чисел с 1:

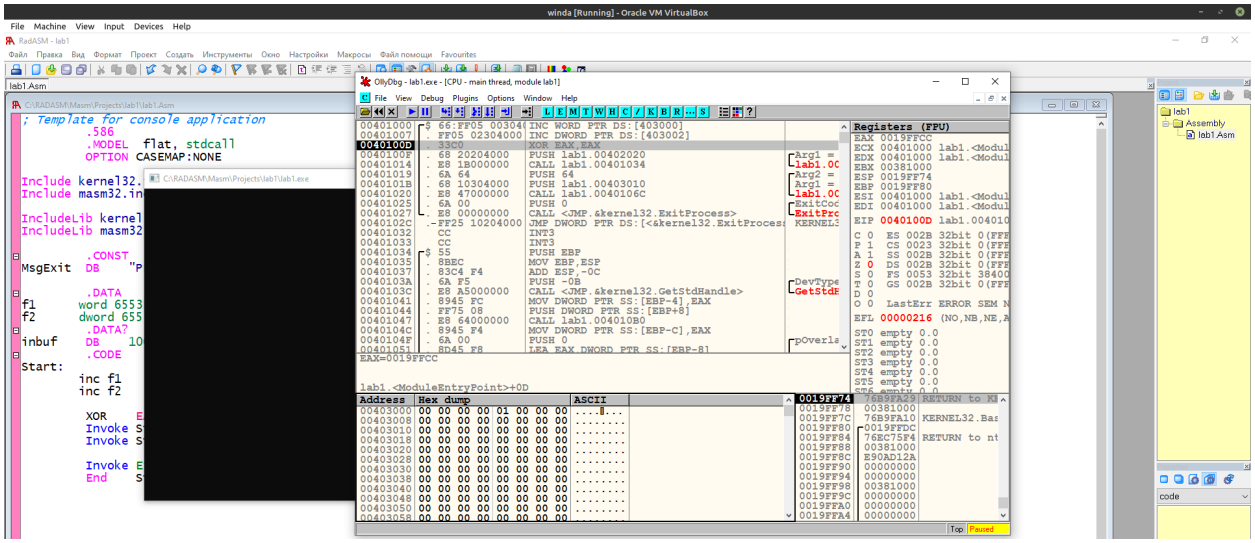
add F1,1

add F2,1

Проанализируйте и прокомментируйте в отчете полученный результат (обратите внимание на флаги).



(рис. 14 Дамп памяти пункта 8 до прибавление единиц)



(рис. 15 Дамп памяти пункта 8 после прибавление единиц)

Контрольные вопросы

1. Дайте определение ассемблеру. К какой группе языков он относится?
Язык ассемблера — низкоуровневый язык программирования, созданный для облегчения записи программ. Вместо машинных команд программист печатает мненмоники.

2. Как создать заготовку программы на ассемблере? Из каких частей она состоит?
Надо определить сегменты кода, данных и стека(автоматически). Файл должен содержать расширение .asm

3. Как запустить программу на ассемблере на выполнение? Что происходит с программой на каждом этапе обработки?
В среде radasm для запуска проекта надо сначала ассемблировать проект, потом скомпоновать. Даль запуск с отладкой или без(в зависимости от того, что нужно от этой программ программисту в данный момент).

4. Назовите основные режимы работы отладчика. Как осуществить пошаговое выполнение программы и просмотреть результаты выполнения машинных команд.

Для выполнения команды отладчика используют следующие комбинации клавиш:
– F7 - выполнить шаг с заходом в тело процедуры;
– F8 - выполнить шаг, не заходя в тело процедуры.

5. В каком виде отладчик показывает положительные и отрицательные целые числа? Как будут представлены в памяти числа:
A Word 5,-5 ?
Как те же числа будут выглядеть после загрузки в регистр AX?

В дампе памяти числа будут представлены следующем образом:
05 00 FB FF 00 00
В AX числа будут выглядеть точно также. AX- регистр размером в слово.

6. Что такое «разрядная сетка»? Как ограничения разрядной сетки влияют на представление чисел в памяти компьютера?
Разрядная сетка — количество символов для представления числа в ЭВМ.

7. Каким образом в ассемблере программируются выражения? Составьте фрагмент программы для вычисления C=A+B, где A, B и C – целые числа формата BYTE
xor ax, ax

```
mov al, a
add al, b
mov c, al
```

Вывод: В ходе лабораторной работы была изучена среда Radasm и написано тестовое консольное приложение.