13 группа Пархоменко Владимир

*Привет всем. На сегодняшнем занятии ИЗУЧАЕМ то, что называется ОТЛАДЧИК.*

1. *«Работаем» в рамках DosBox.*
2. *Ищем программное средство отладки под названием td.exe.*

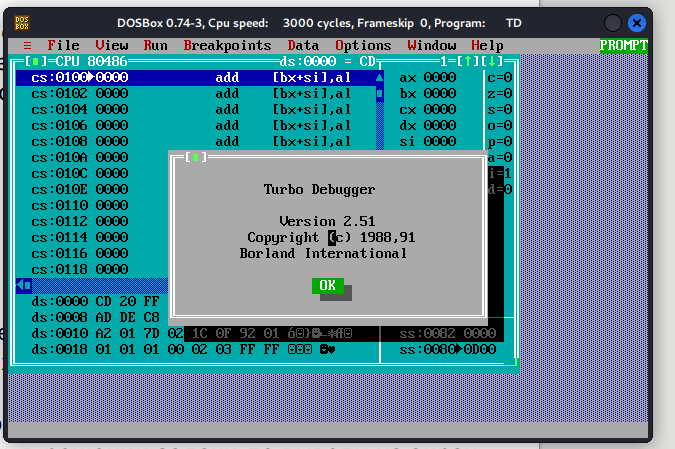
Нашли

1. *Получаем исполнимые модули типа com и exe  —  для какой угодно задачи — какая Вам нравится (можно из Лабы 1 или Лабы 2).*

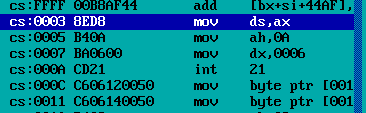
Найдем свой .exe с лабороторной «мама мыла раму»

1. *Проверяем с помощью отладчика, действительно ли сегментные регистры получают указанные в Лекции  и в книге про ассемблер значения. Находим в программе самую длинную и самую короткую КОМАНДЫ. Находим в регистрах самое большое значение и переводим в 10-ую систему счисления без калькулятора.*

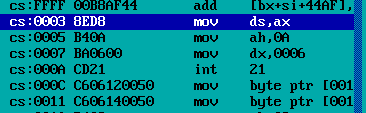
Запустим td.exe:



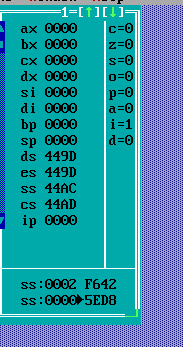
Самая короткая: mov ds, ax (8ED8)



Самая длинная: mov ( C606120050)



Самое большое значение:



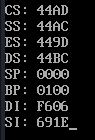
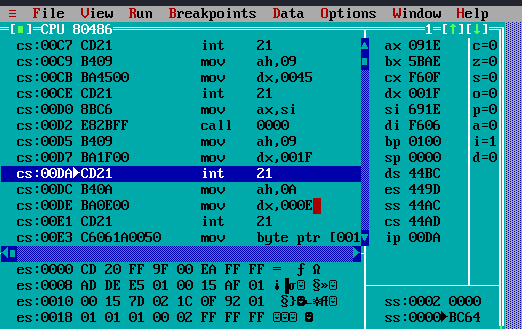
(44AD)₁₆ = (4 × 16³) + (4 × 16²) + (10 × 16¹) + (13 × 16⁰) = 17581

*5. К понравившейся Вам задаче добавляем подзадачу ВЫВОДА НА ЭКРАН в 16-ичной системе счисления ЗНАЧЕНИЙ, находящихся в сегментных регистрах НА МОМЕНТ ПРЕВРАЩЕНИЯ ИСПОЛНИМОГО МОДУЛЯ в программу. И сравниваем полученное значение с тем, что есть в отладчике. Перевод в 16-ую систему счисления значения, сидящего в AX, есть в решении задачи по выводу на экран изображений символов кодировочной таблицы.*

В исходный текст задания с лабороторной «мама мыла раму» добавим процедуру print\_word для вывода значений регистров. Каждое значение печатается с новой строки, подготовленные строки хранятся в .data.

*6. Осуществляем отладку и ПОШАГОВОЕ ВЫПОЛНЕНИЕ полученной программы по выводу на экран значений содержимого сегментных регистров.*

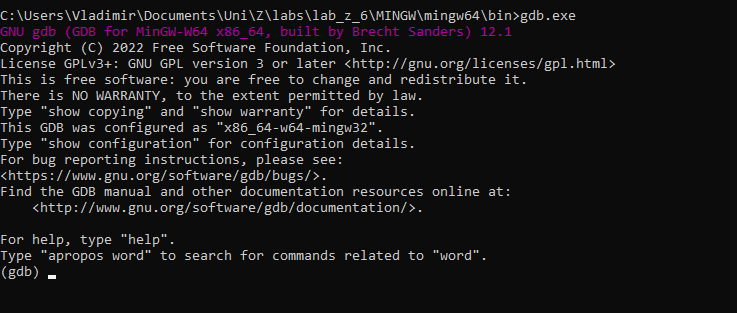
Сравним значения регистров, пошагово выполняя программу:



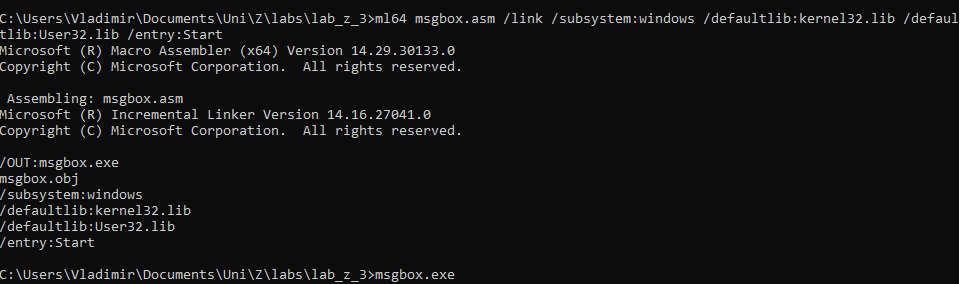
7. Пробуем с помощью отладчика td.exe пошагово выполнить программу, которая получается из исполнимого модуля Sample.exe. Пытаемся определить, какие значения получают сегментные регистры. Понятно, что ничего не получится. Обманул? Качаем из помойки какой угодно другой отладчик-дизассемблер, который «фурычит» на 64-разрядных ЭВМ.  И добавляем к боксику фрагмент, выводящий на экран значения в 16-ичной системе счисления ВСЕХ РЕГИСТРОВ, использованных в тексте Боксика!!!!

8. С помощью скачанного из помойки отладчика ПОШАГОВО выполняем Боксик (НЕ СКАЧУЩИЙ)!

Установим хороший отладчик GDB:



Вспомним как запускать messagebox:

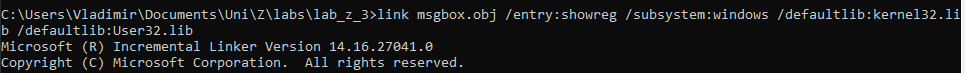


Переделаем исходный текст на вывод на экран значений регистров. Чтобы не было проблем с созданием .exe, установим nasm.



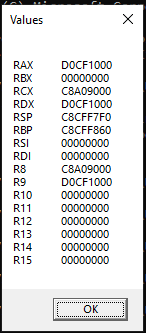
nasm -f win64 msgbox.asm -o msgbox.obj

Link.exe:

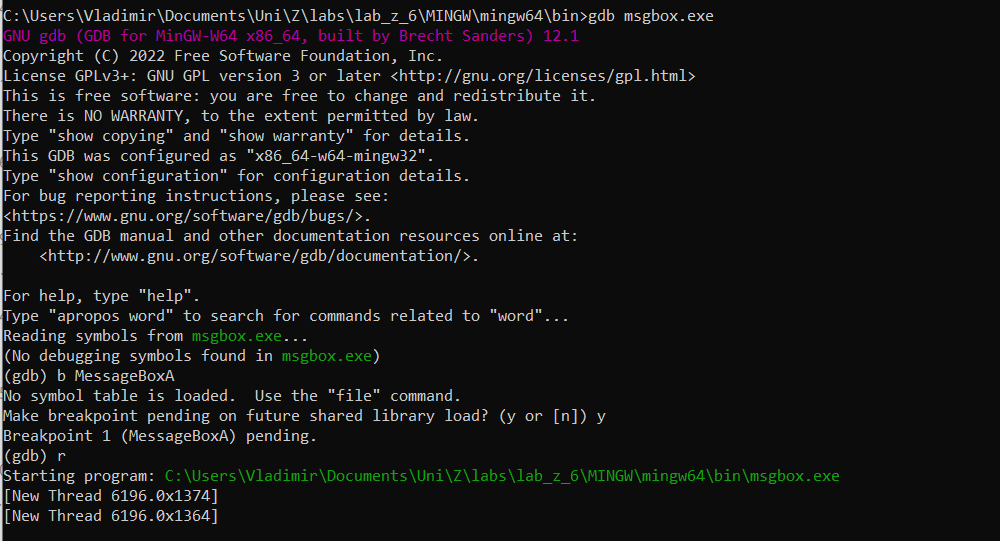


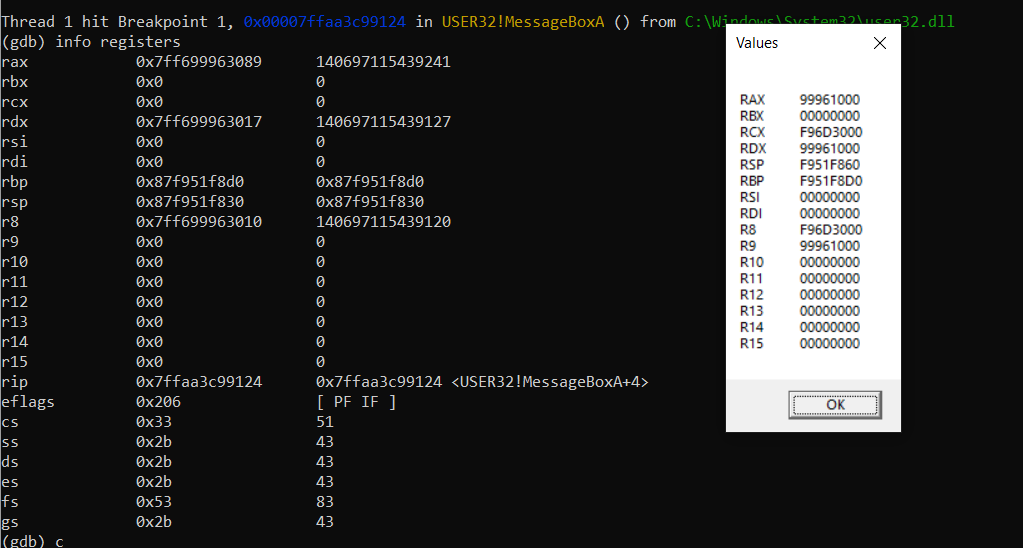
link msgbox.obj /entry:showreg /subsystem:windows /defaultlib:kernel32.lib /defaultlib:User32.lib

msgbox.exe:



Поработаем с gdb:





9. Результат — три файла — исходные тексты, исполнимые модули и ОТЧЁТ о проделанной работе ПРИСЛАТЬ мне на почту К СЛЕДУЮЩЕМУ ВТОРНИКУ!!!!

10. Продолжаем «работать» над заданиями из занятия №5 и над Лабораторной работой №2. Если возникают какие-то вопросы — задавайте их письменно ПО ПОЧТЕ!!!!