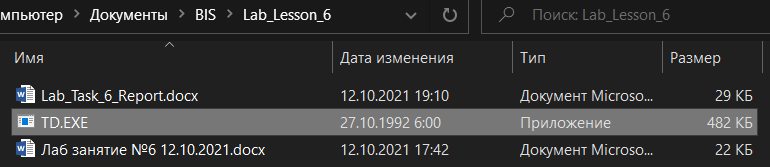
Жуковский Павел Сергеевич, 4 курс, 12 группа

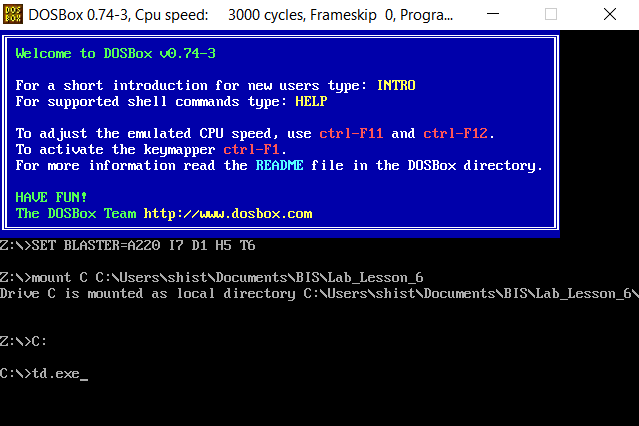
Лабораторное занятие №6 (12.10.2021)

Пароль от архива: **041**

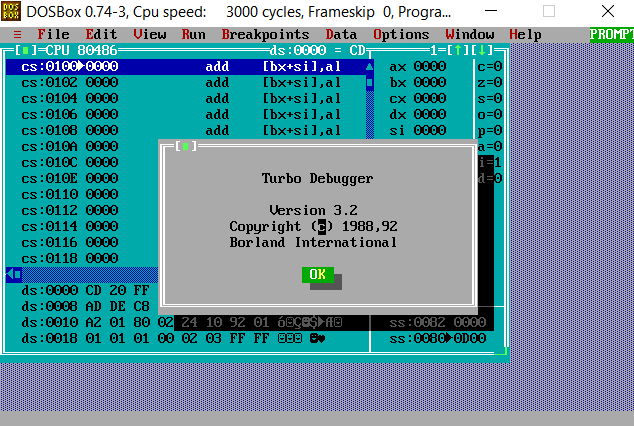
Раздобыл td.exe:



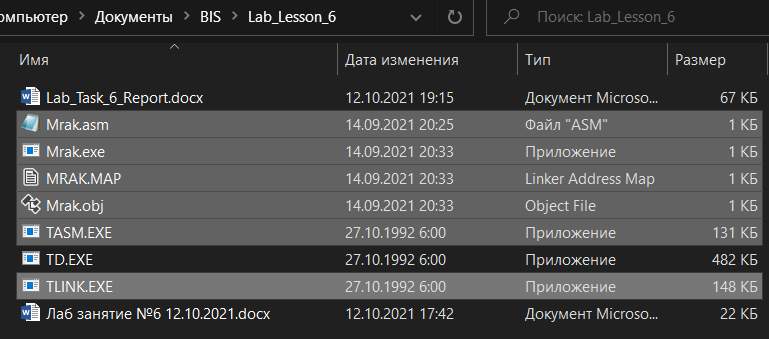
Запустил td.exe внутри DOSBox:



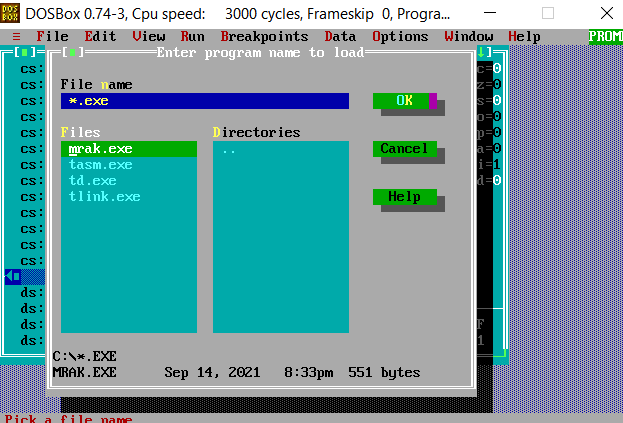
Появилось вот такое окно:



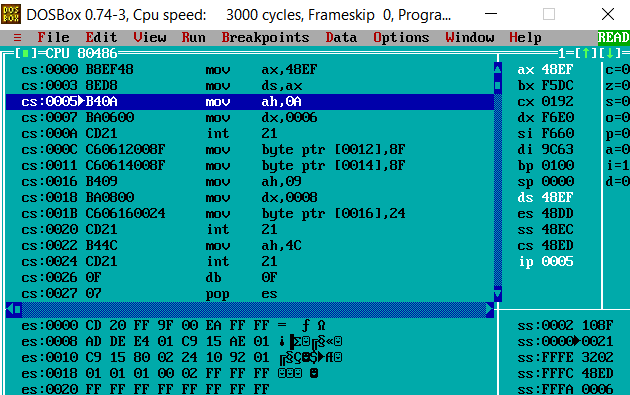
Далее я поместил в папку все файлы, принадлежащие программе «ПАПА» из 2-ого лабораторного занятия:



Позже я загрузил её в отладчик:



Далее я перешёл к команде MOV AH, 10:



Это ничто иное, как её адрес:



Адрес команды MOV OblVvoda+12,’П’:

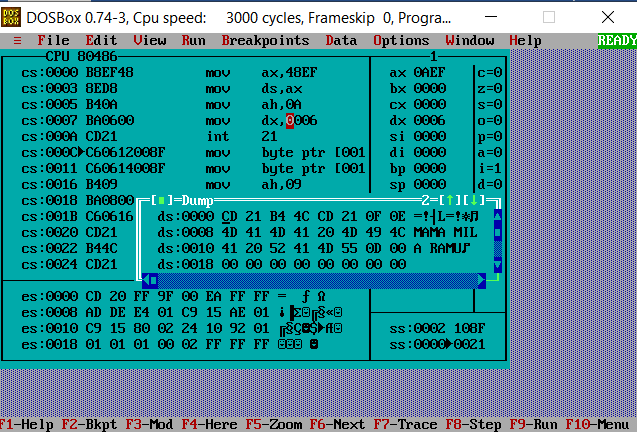


Шестнадцатеричное представление команды MOV OblVvoda+12,’П’:

cs: 00 1B C6 06 16 00 24

Далее я сделал несколько шагов, ввёл в консоли MAMA MILA RAMU, как просила от меня программа.

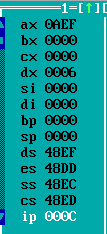
После этого я открыл View 🡪 Dump:



Содержимое области памяти ввода - OBLVVODA - в шенстнадцатеричном виде после ввода в неё "MAMA MILA RAMU":



Cодержимое всех регистров на момент выполнения команды mov OblVvoda+12,’П’ :



Соответственно в десятичной системе счисления:

ax – 2799

bx – 0

cx – 0

dx – 6

si – 0

di – 0

bp – 0

sp – 0

ds – 18671

es – 18563

ss – 18668

cs – 18669

ip – 12

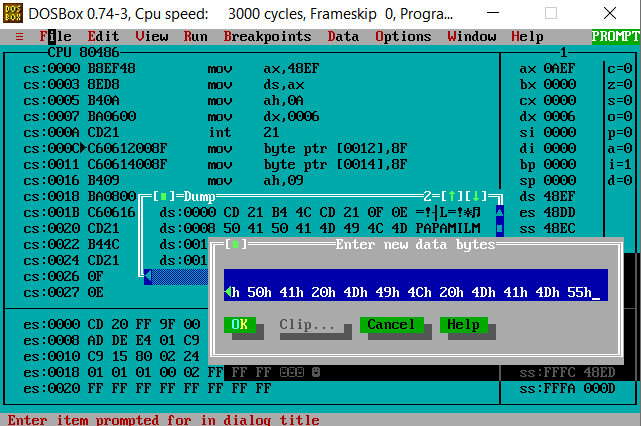
Далее нужно было заменить надпись на:

«PAPA MIL MAMU»

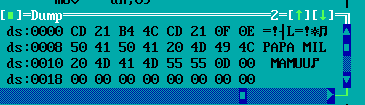
Этим символам соответствуют следующие коды (включая пробелы):

50h 41h 50h 41h 20h 4Dh 49h 4Ch 20h 4Dh 41h 4Dh 55h

Я снова открыл View 🡪 Dumb и поставил курсор на фразу MAMA MILA RAMU, чтобы ввести туда новые коды:



Итог:



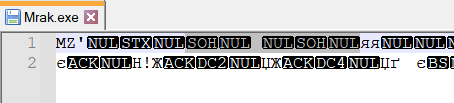
Далее, нужно было испортить исполнимый модуль. Для этого, как вариант, можно поменять его расширение .EXE на какую-нибудь ерунду:

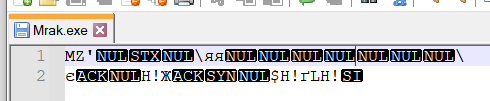


Далее, нужно было как-нибудь изменить длину исполнимого модуля, а затем попробовать запустить.

Я попробовал в лоб открыть .exe файл через какой-нибудь текстовый редактор и стереть несколько символов (то, что из себя представляют эти символы, в общем-то не очень важно):







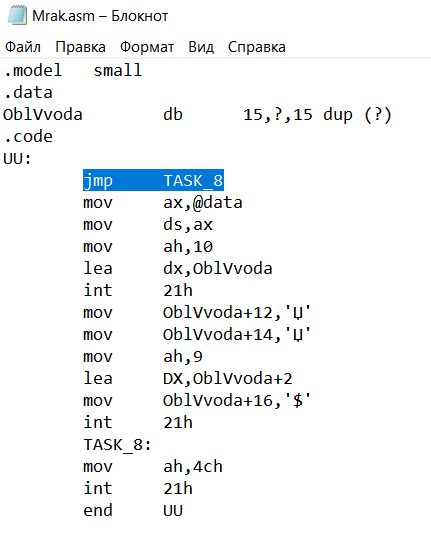
При попытке запуска ничегошеньки не происходит, видимо сломали:



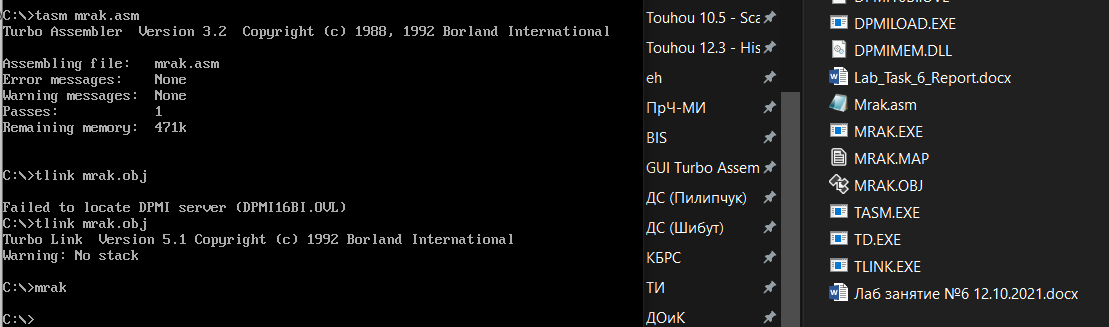
После этого я удалил испорченный исполнимый модуль, а также объектный модуль. (нам все равно придётся слегка изменить исходный текст в дальнейшем).

Далее нас просят, чтобы исполнимый модуль успешно загружался в оперативную память, но чтобы потом программа ничего не делала. Для этого достаточно, как вариант, просто перескочить через исходный текст программы.

Для этого я прописал jmp TASK\_8, эта команда поможет нам перескочить через все инструкции для программы к созданной метке TASK\_8, которая поставлена в конце программы:

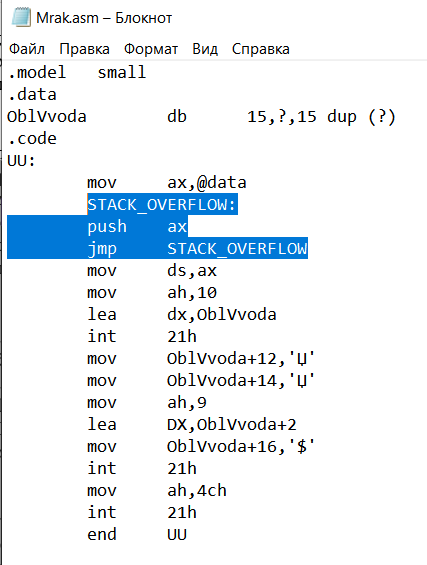


Теперь заново собираем объектный и исполнимый модуль и загружаем программу в оперативную память…

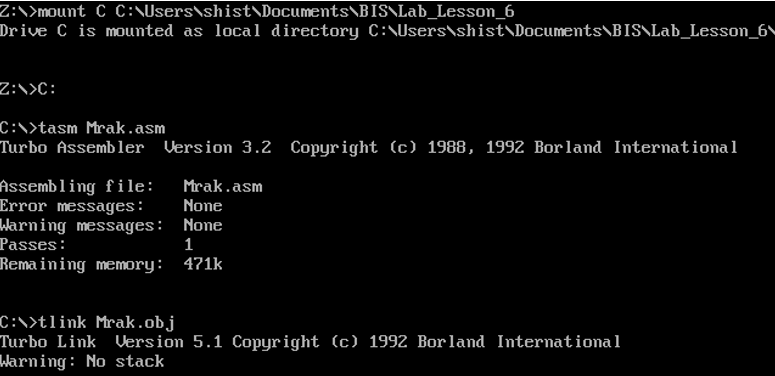


Собственно, программа была загружена в оперативную память, но ничего конечно же не произошло.

Далее, нужно чтобы программа начала выполняться, но чтобы с ней что-то пошло не так… Можно попробовать что-то поделить на ноль, но это слишком скучно, поэтому я решил попробовать сделать рекурсию со входом в метку внутри этой же метки, чтобы добиться переполнения стека… Сам стек мы будем пополнять внутри этой метки командой PUSH AX (по барабану, чем заполнять стек, так что заполняем тем, что под руку попадётся, например регистр AX):



Все благополучно собралось сначала в объектный, затем в исполнимый модуль:



При загрузке программы в оперативную память, ничего не происходит. Ввести символы невозможно, программа попросту застыла… Окно DOSBox пришлось закрыть, ибо выйти из программы невозможно. В каком-то смысле, мы создали небольшой вирус, который вынуждает пользователя закрыть окно DOSBox-а из-за невозможной дальнейшей работы в нём…



На этом сегодняшние эксперименты закончены.

Пароль от архива: **041** (на всякий случай, укажу пароль на самом верху этого отчёта тоже)