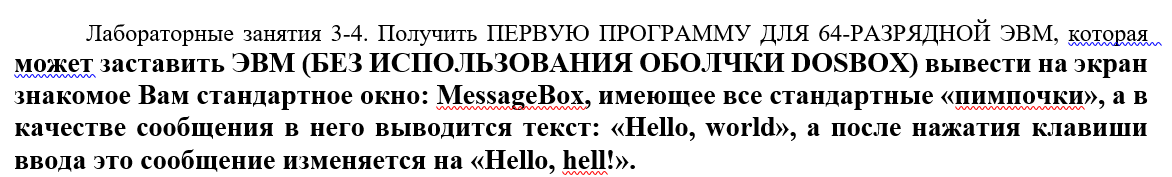
Занятие 17.09.2024

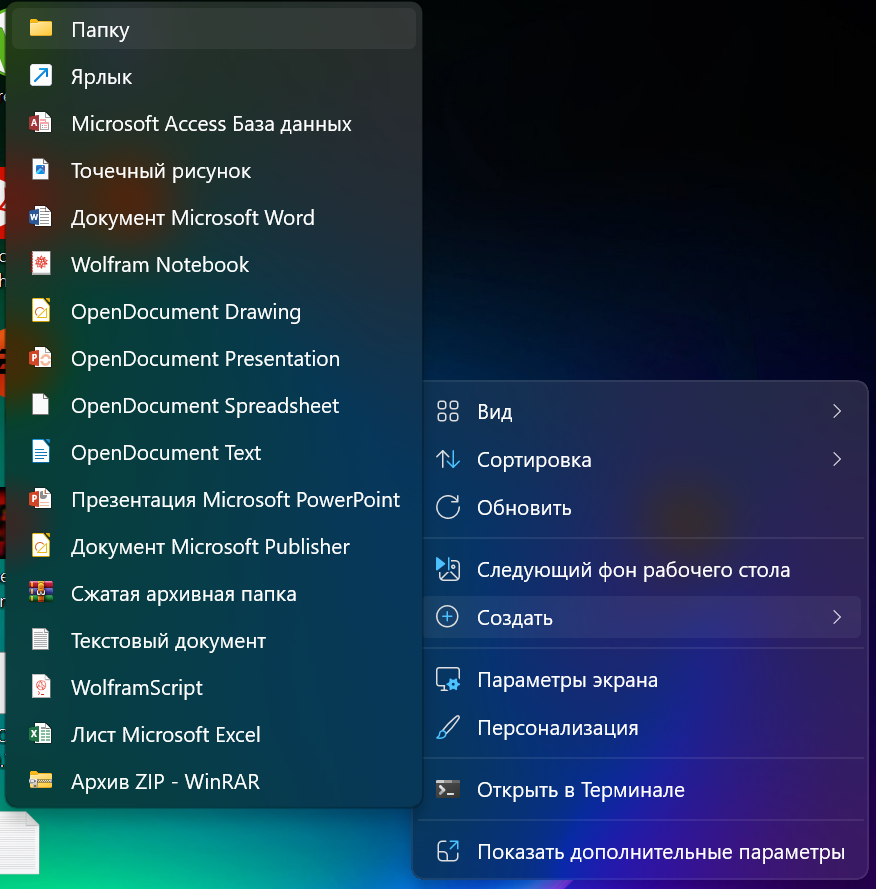
Лабораторное занятие №3



Начнём выполнение задания с создания папки на рабочем столе

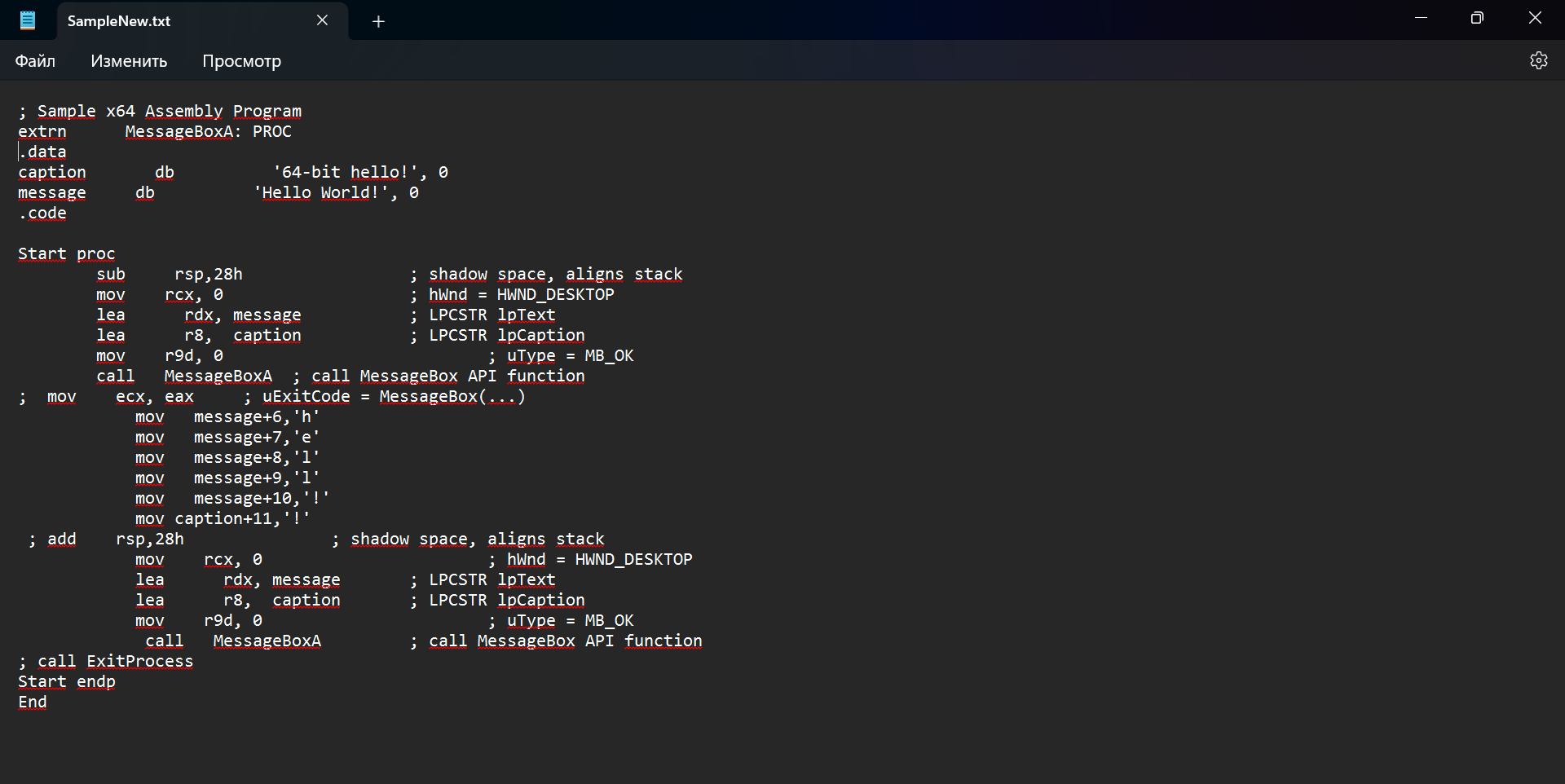


Для этого нажимаем правой кнопкой мыши по пустому месту, выбираем «Создать» и выбираем «Папку»

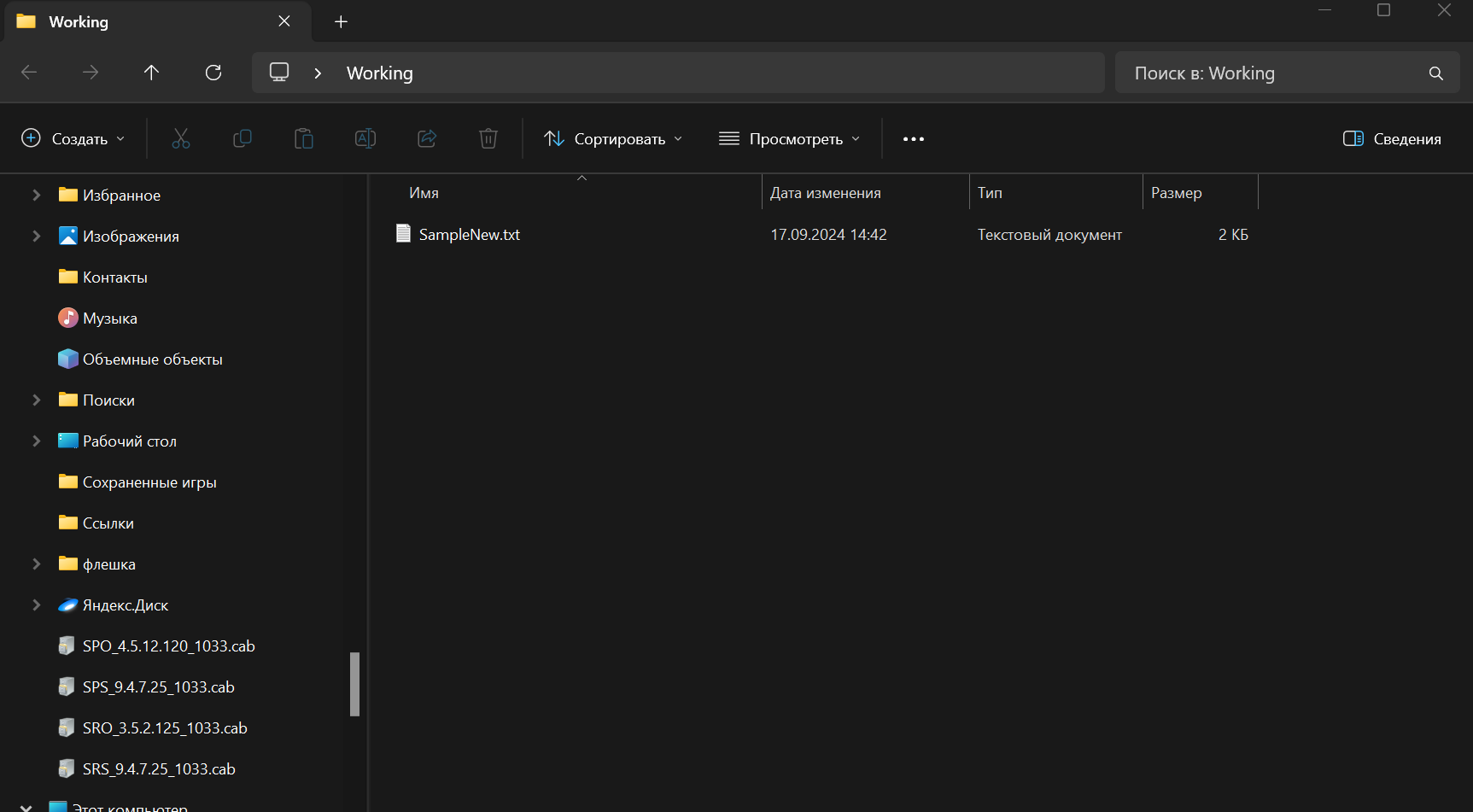


Созданную папку называем Working.

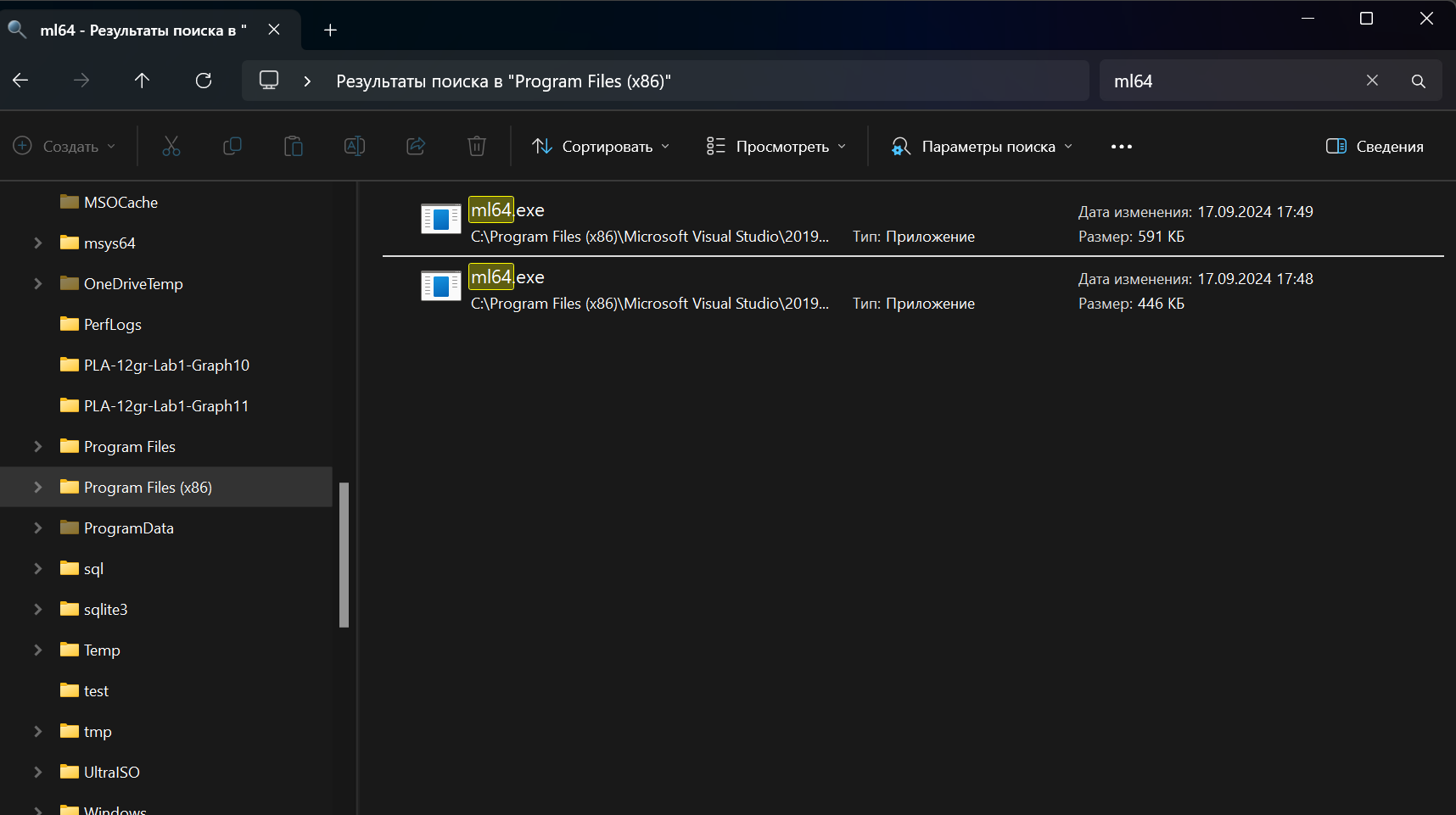


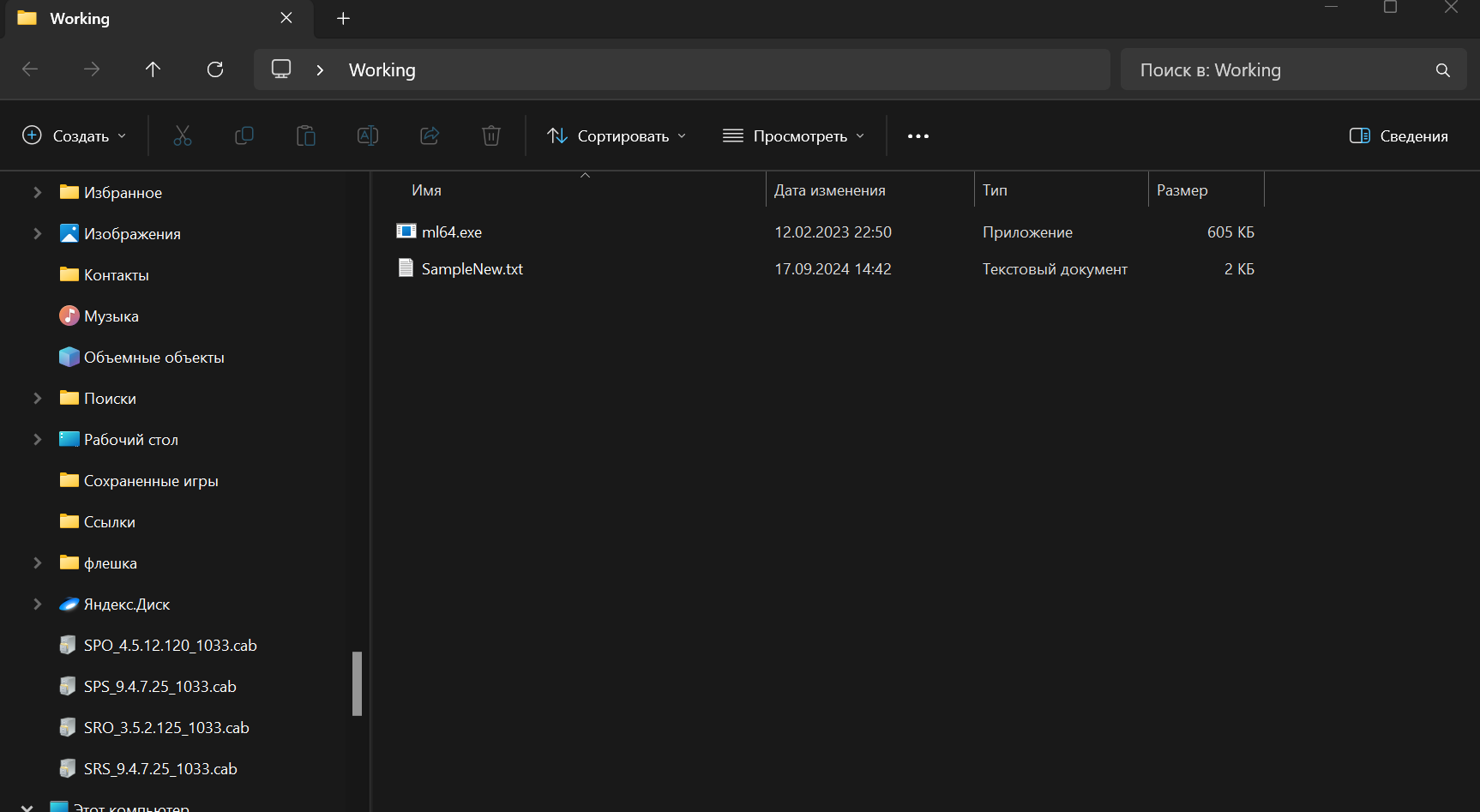
Теперь нам нужно через блокнот создать txt-файл. Можно сразу перейти в папку и там создать пустой файл, открыв его через блокнот. В файле набираем текст, предоставленный в документе с лабораторным занятием №3.

Данный файл сохраняем.

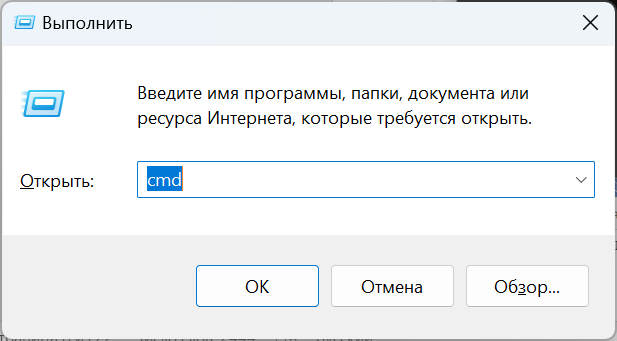


Теперь нам требуется найти файл ml64.exe. У меня они все лежат в папке Program Files (x86). Выбираем нужный и копируем в папку Working.

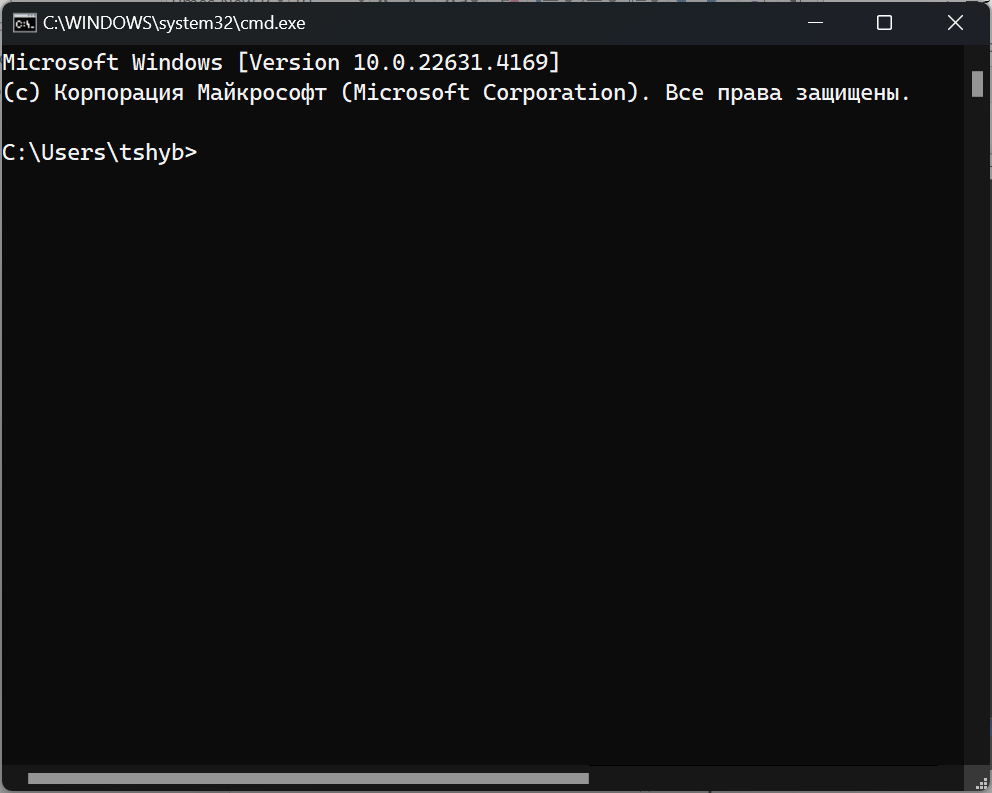




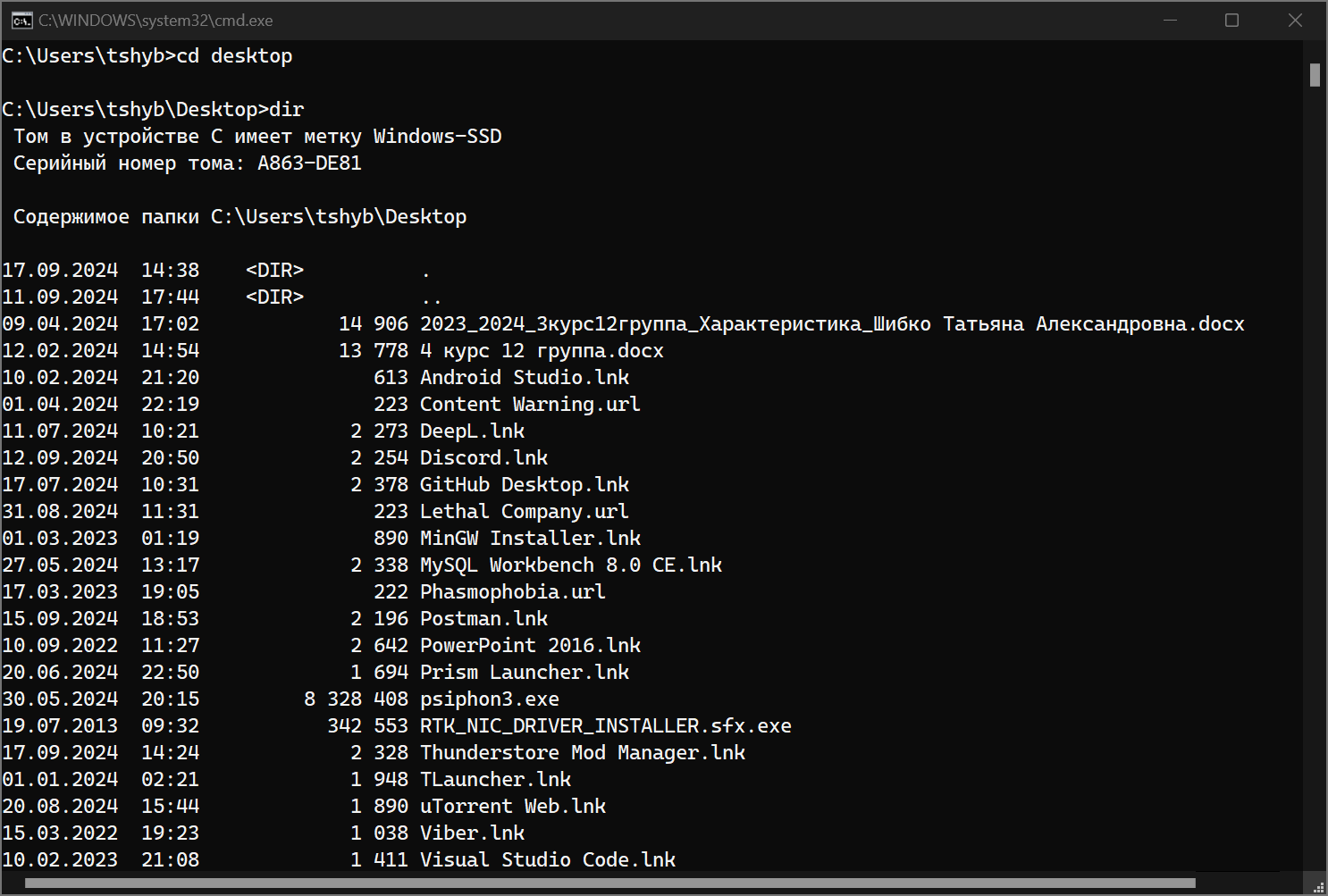
Теперь нам требуется открыть командную строку. Делаем это через сочетание клавиш Win+R и вводим в появившемся окне cmd. Далее нажимаем ОК.

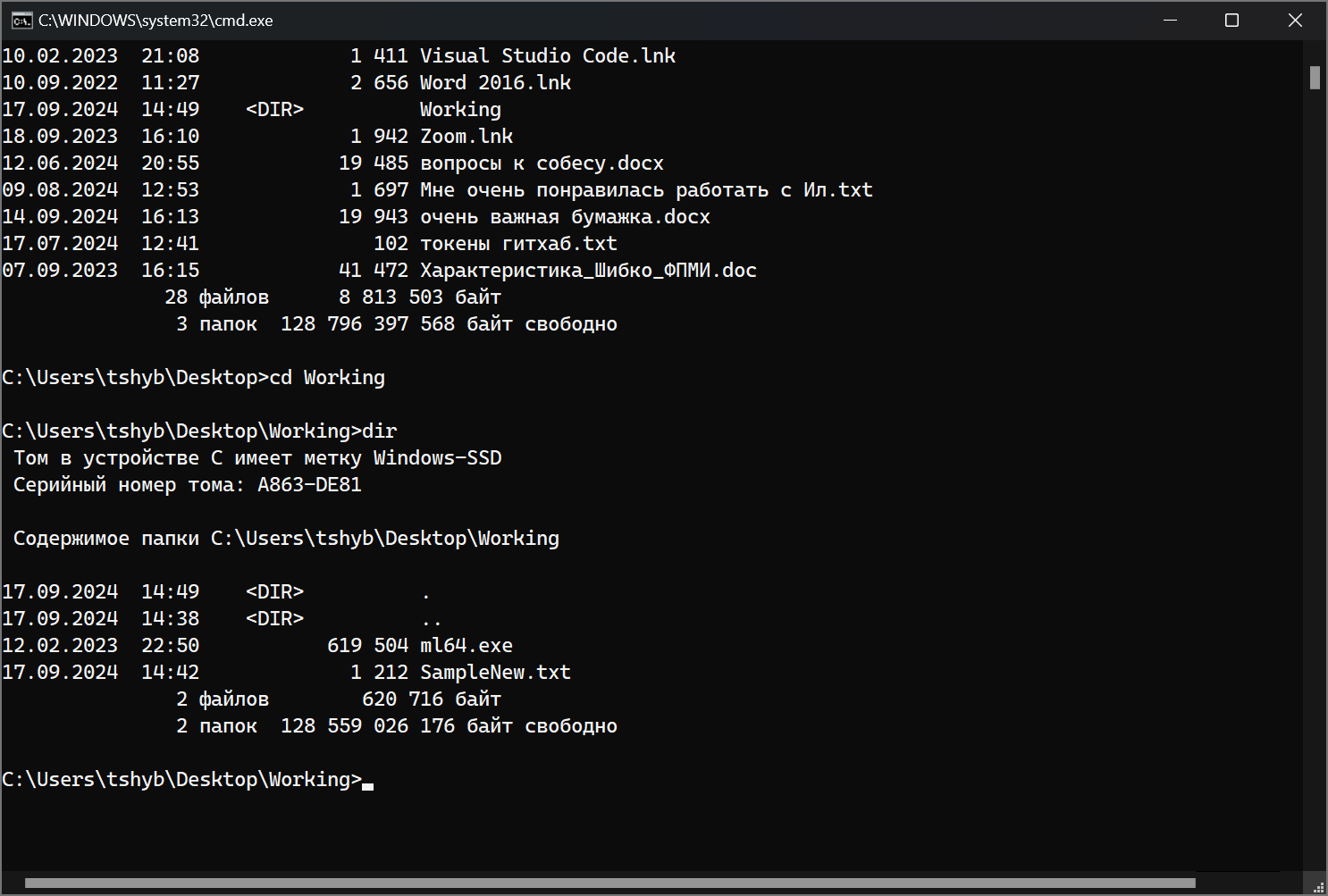


Нам открылась командная строка.

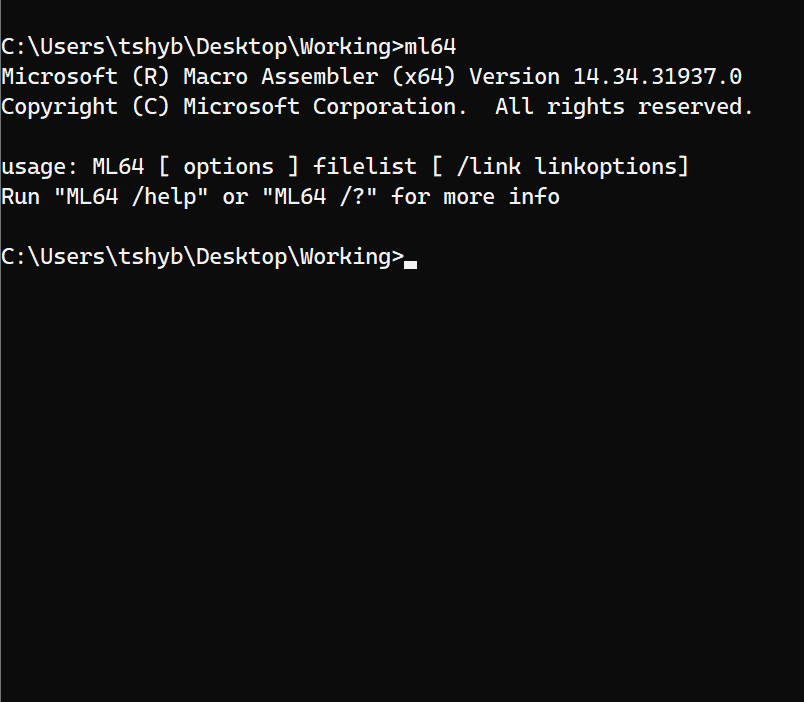


Теперь мы можем через команду cd desktop переключить на рабочий стол. А если введём команду dir, то увидим всё, что лежит на рабочем столе. Но нас интересуется наша папка Working, поэтому вводим cd Working и оказываемся в нашей папке. Введя повторно dir, мы увидим, что в папке лежат нужные нам SampleNew.txt и ml64.exe.

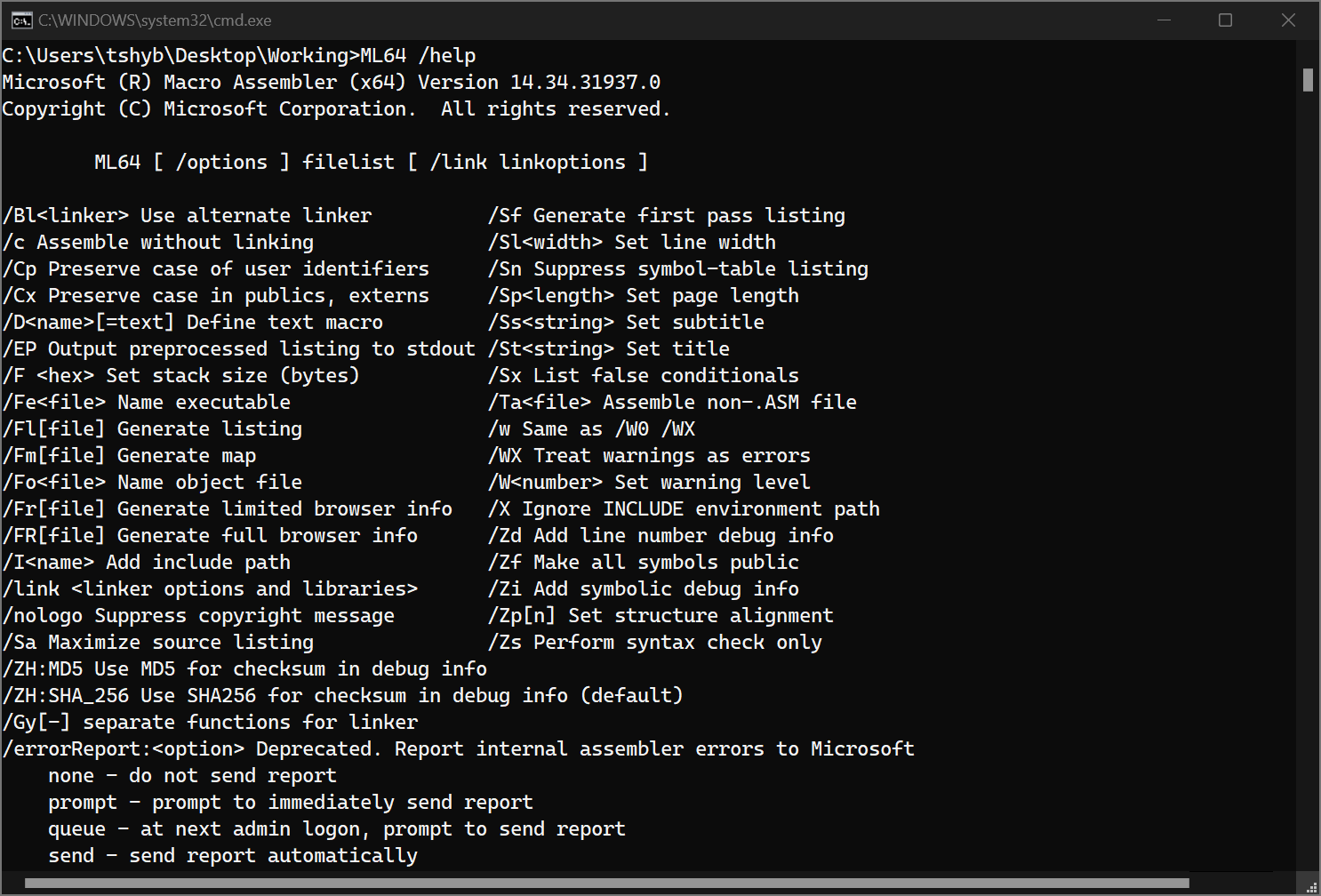




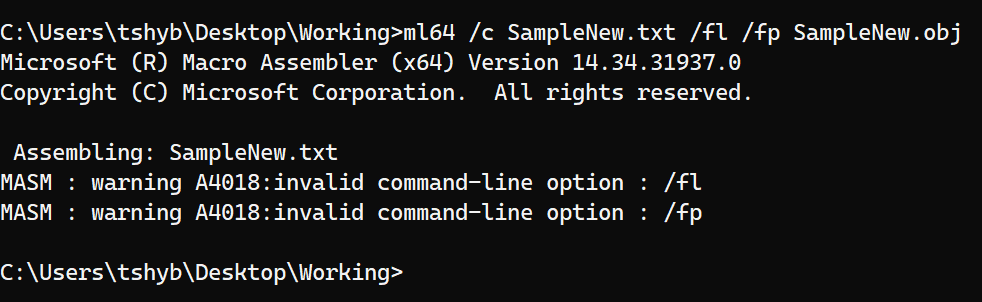
Попробуем запустить транслятор ml64.



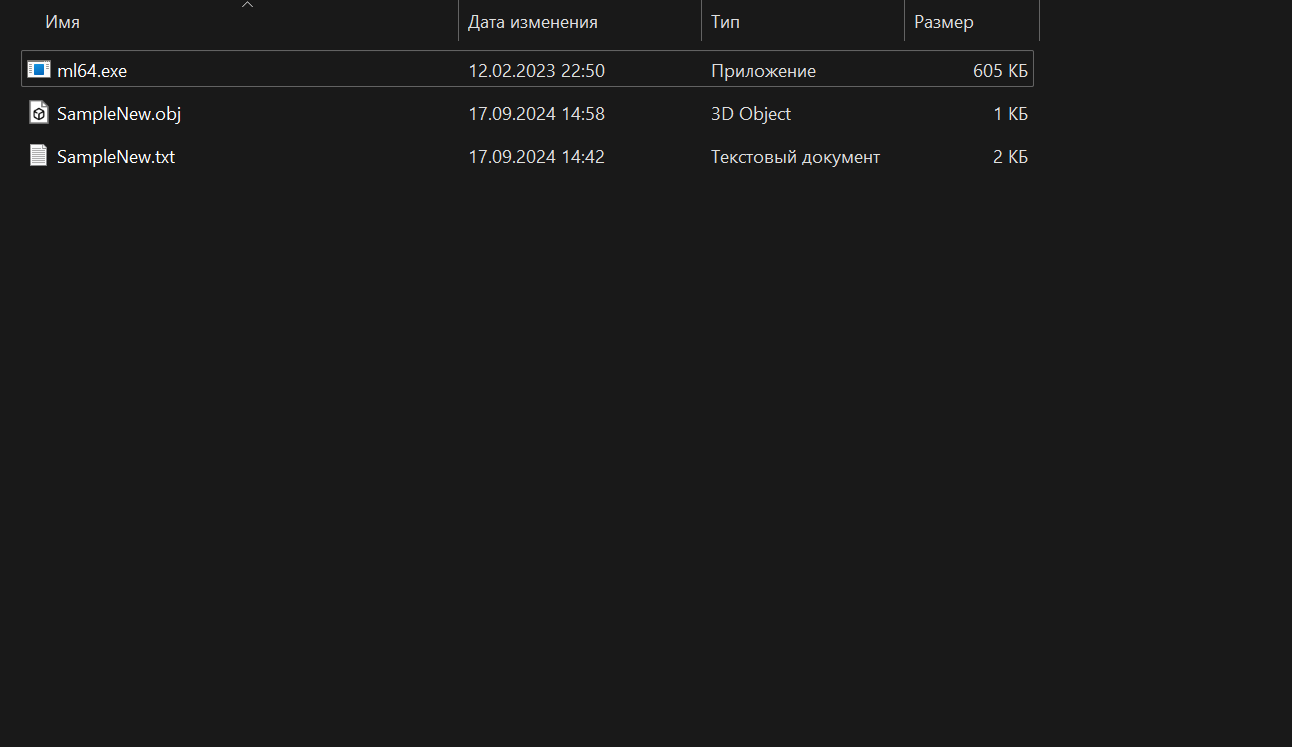
Для справки (или в качестве профилактики), пропишем ml64 /help и посмотрим, что нам вывело.



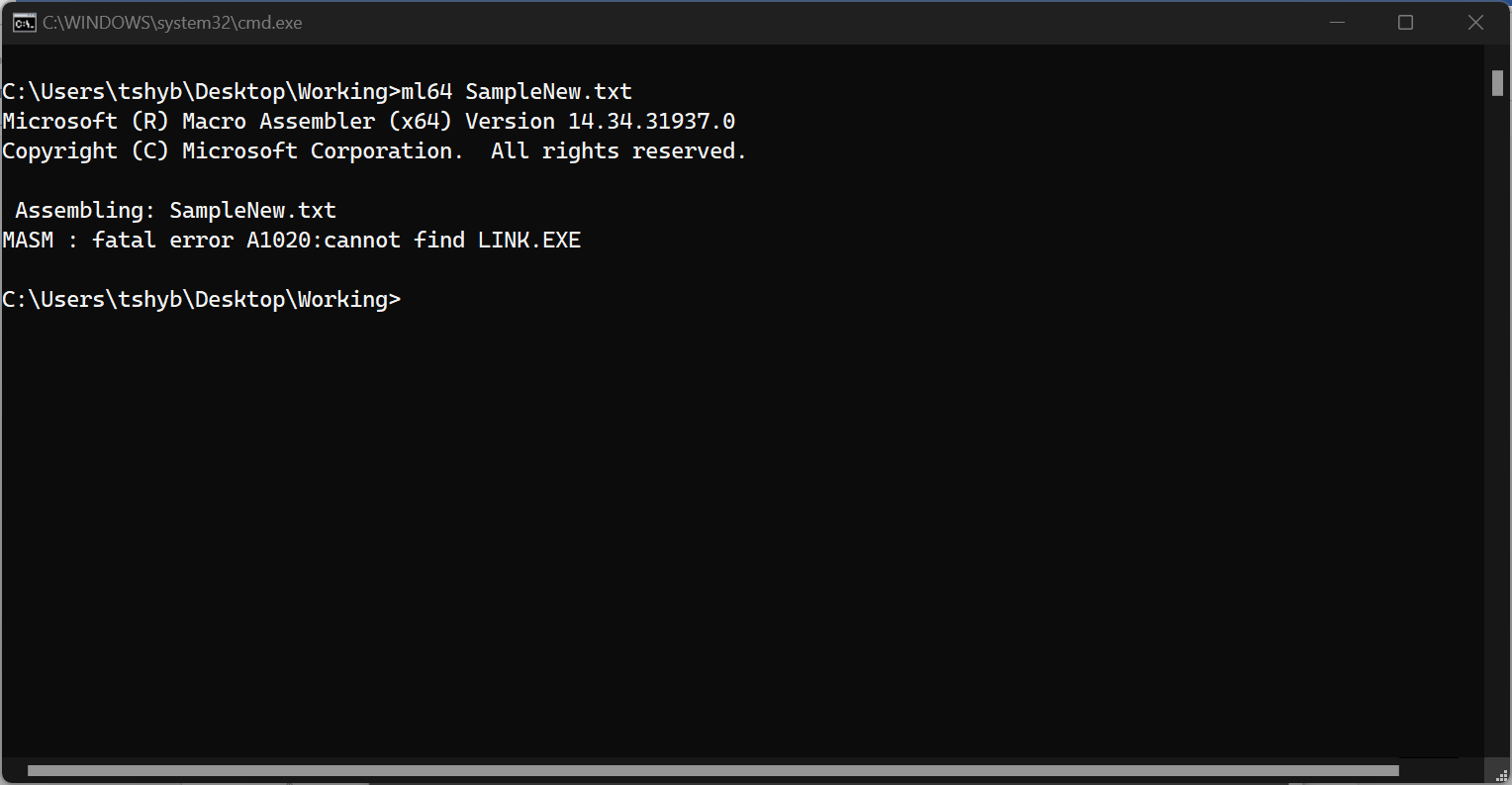
В общем, много текста, но сейчас нас интересует получение исполняемого модуля. Для этого нам требуется прописать ml 64 /c SampleNew.txt /fl /fp SampleNew.obj



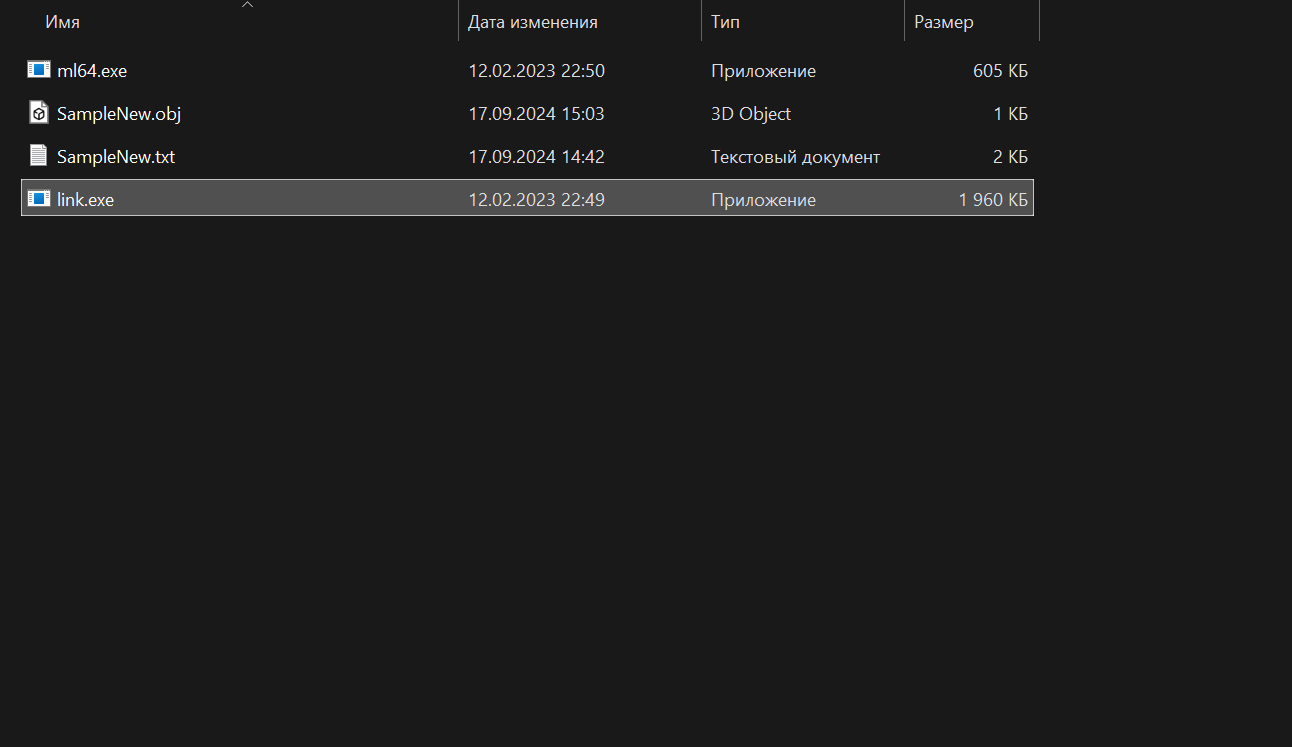
Заходим в папку Working и видим, что всё получилось.



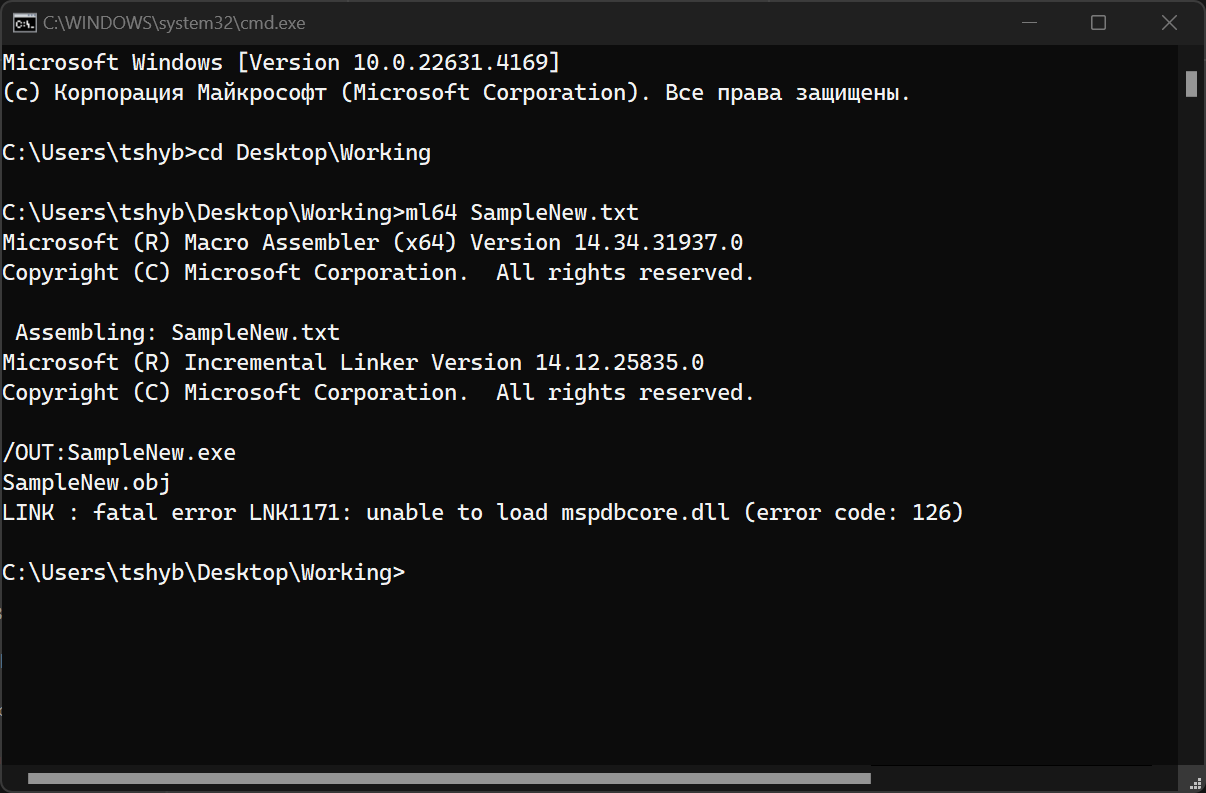
Теперь попробуем ввести просто ml64 SampleNew.txt



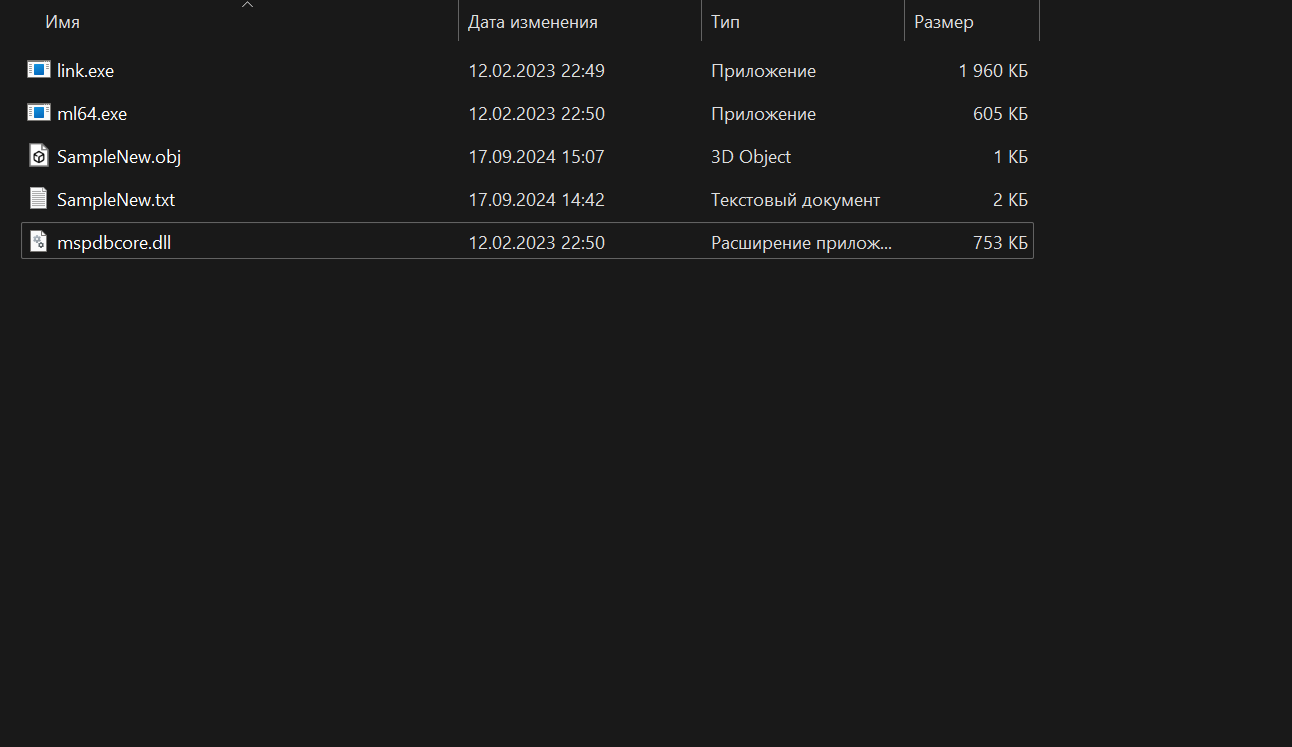
Как видим, командная строка вывела нам ошибку о том, что не может найти LINK.EXE. Добавляем его в папку так же, как и ml64.exe



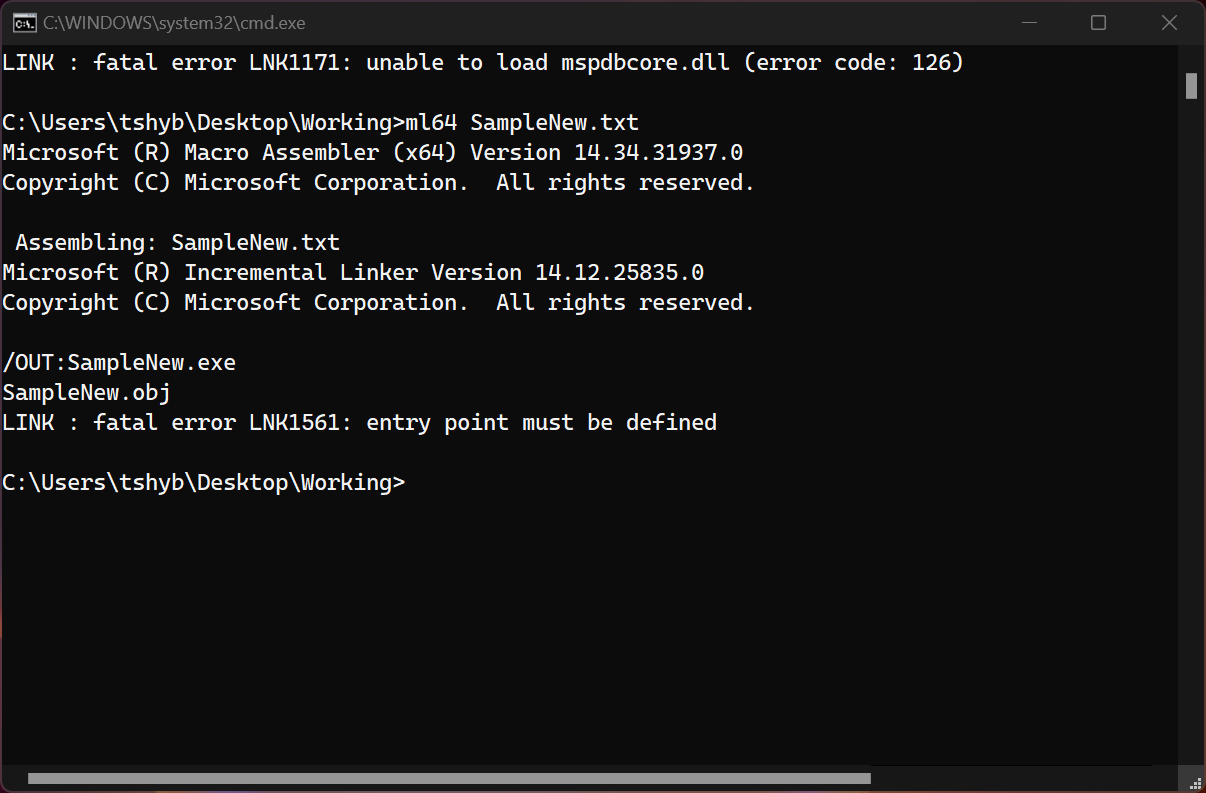
Пробуем снова ml64 SampleNew.txt и теперь у нас новая головная боль – отсутствие mspdbcore.dll.



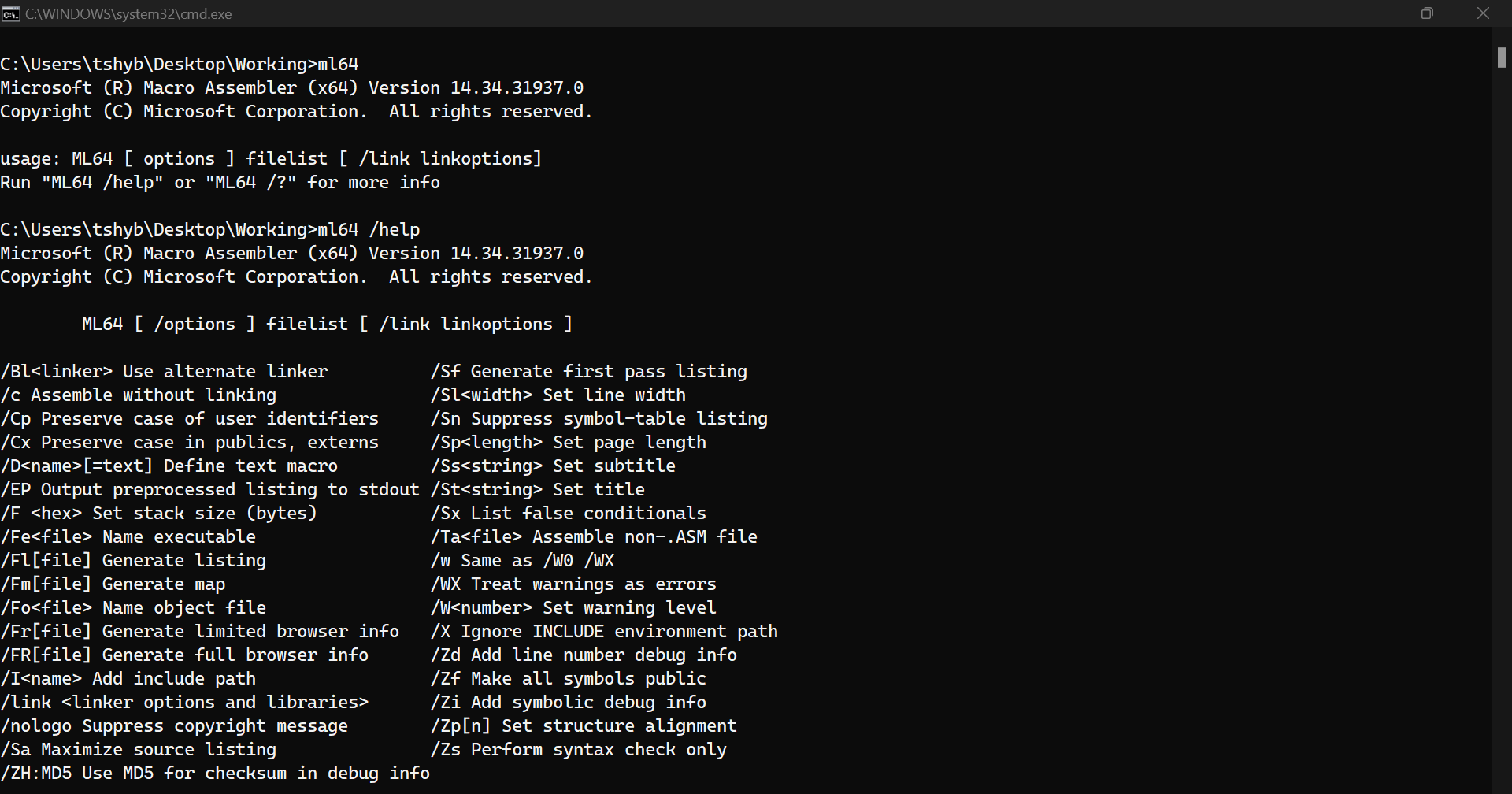
Находим недостающий файл и копируем в папку Working.

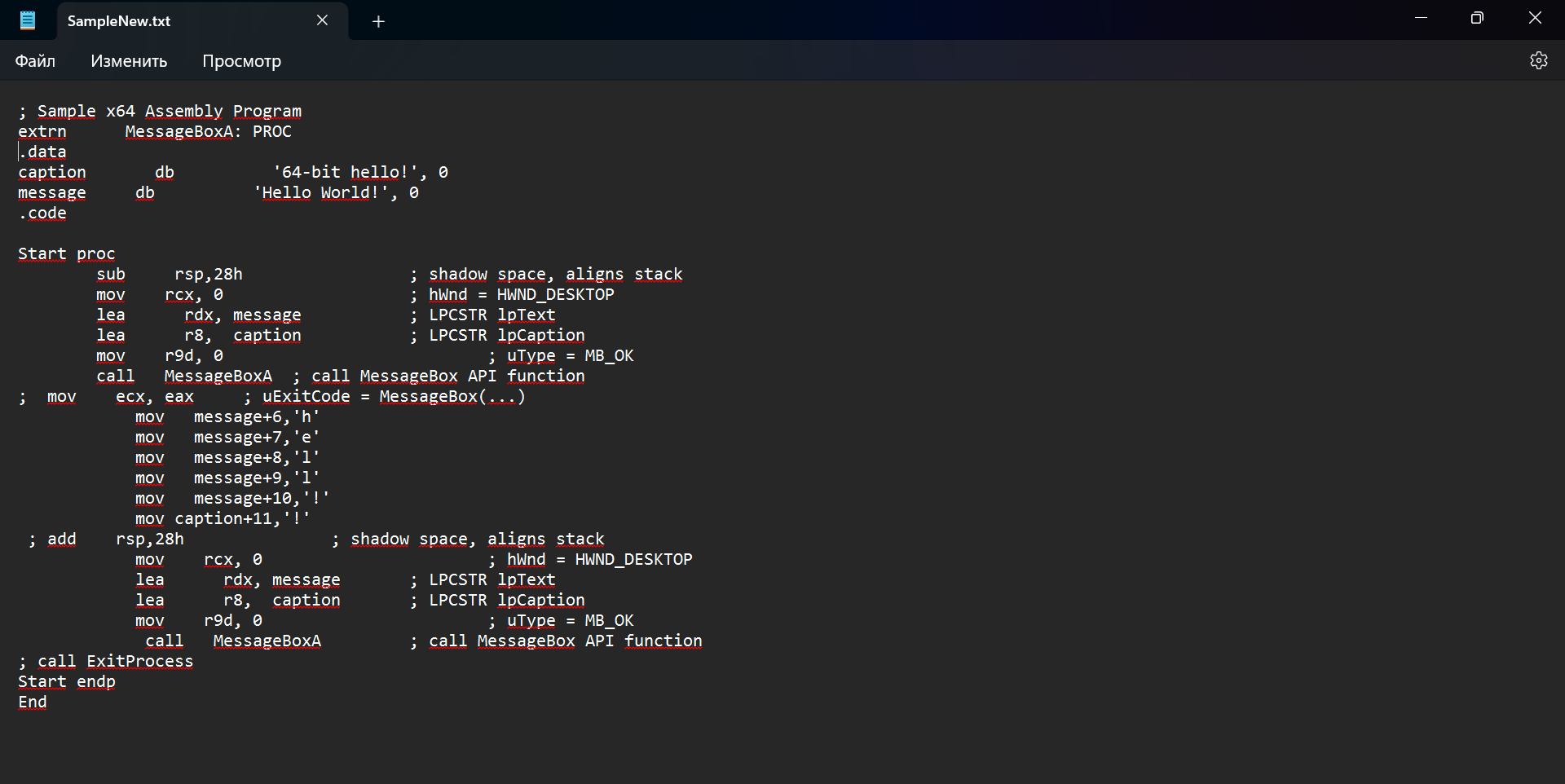


Третья попытка. Вводим ml64 SampleNew.txt и… Новая ошибка. Нам не хватает какой-то точки входа.



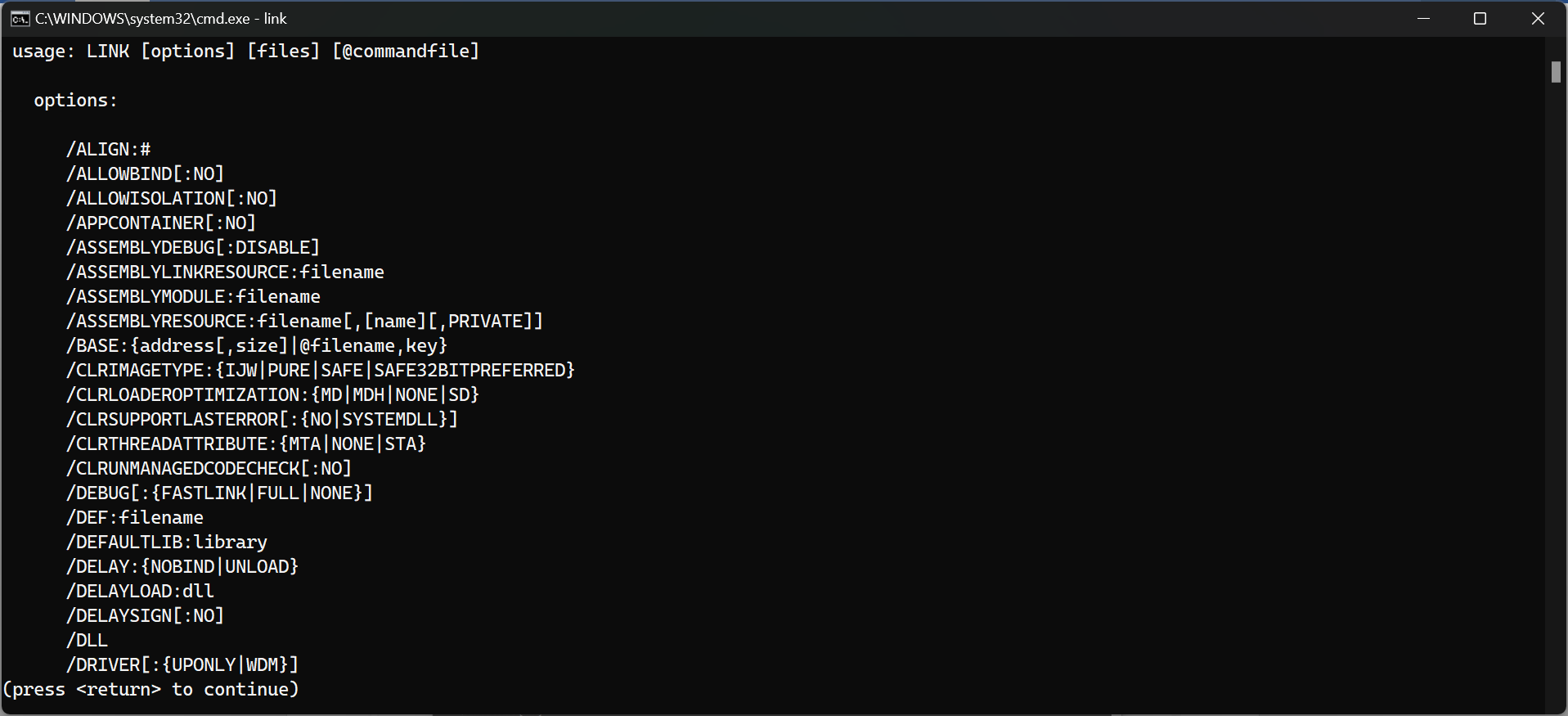
Чтоб её решить, попробуем покопаться в опциях ml64. Снова вводим ml64 /help и смотрим наш исходный код в SampleNew.txt.

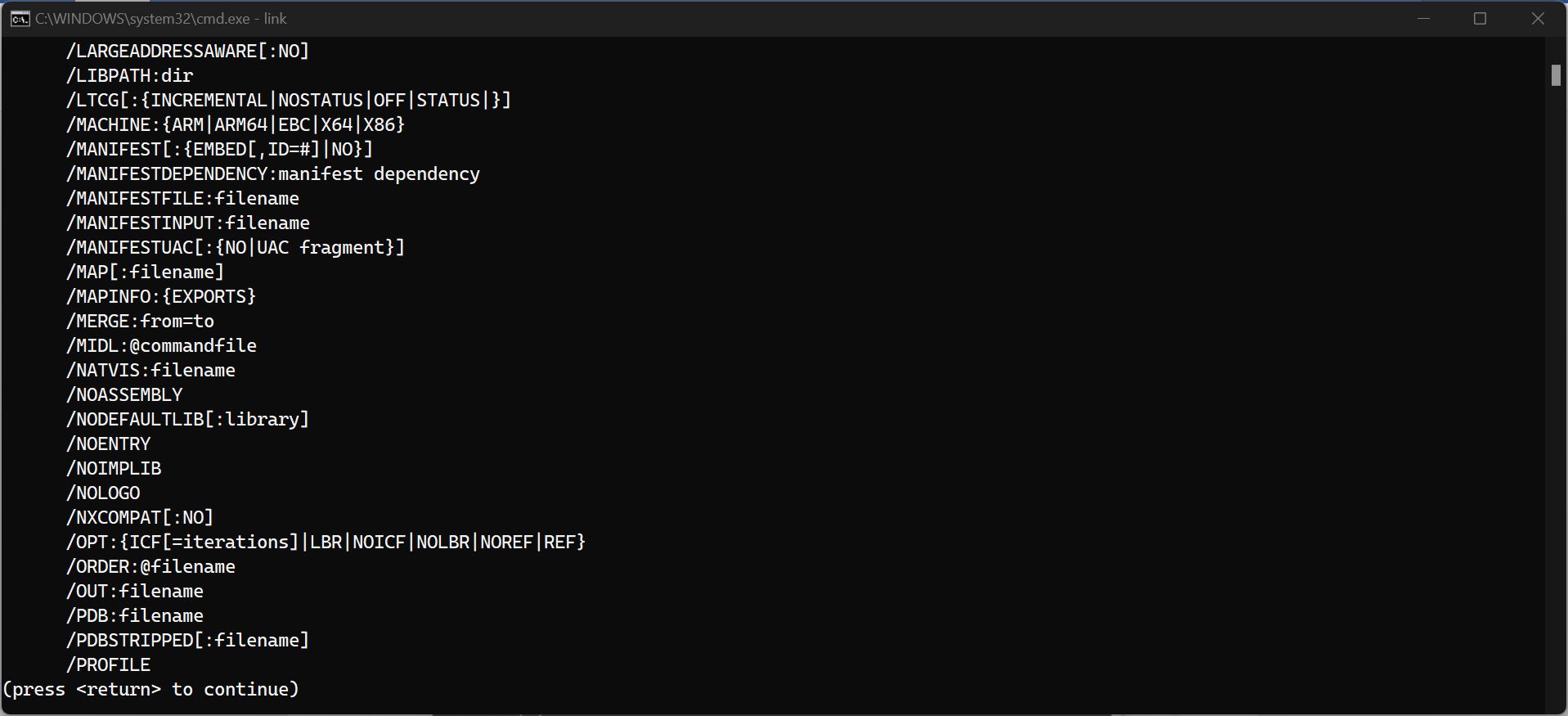


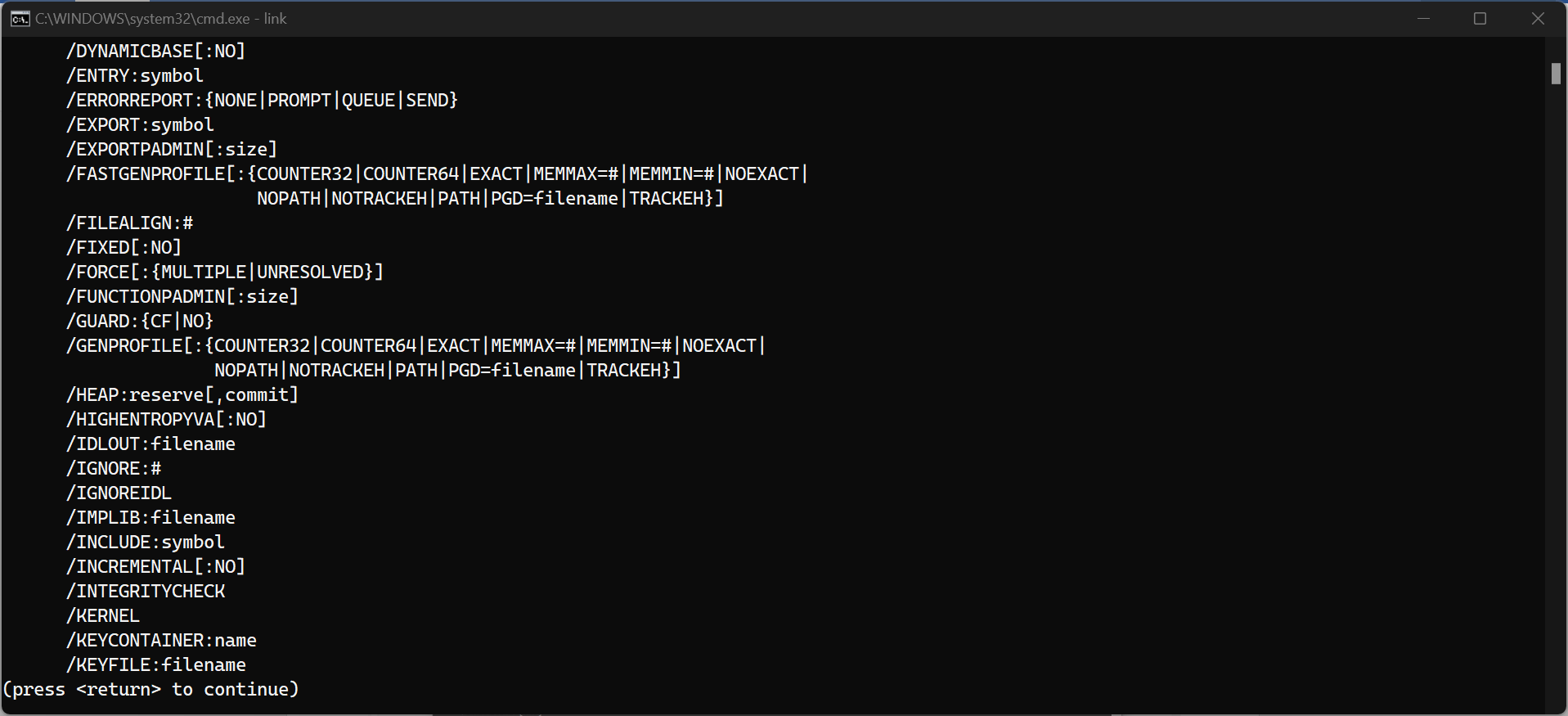


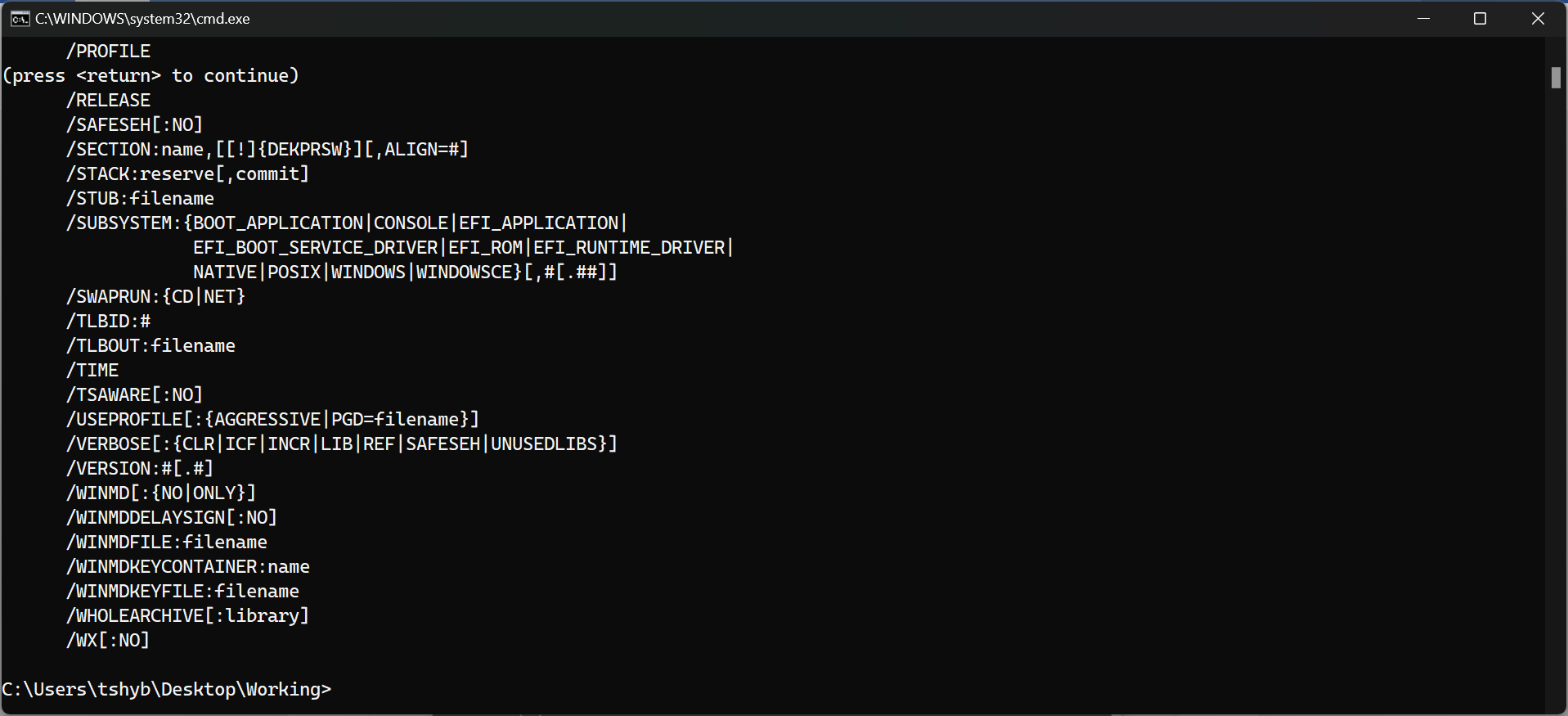
Очень похоже, что наша точка входа –это адрес первой машинной команды, получаемый в результате трансляции и линковки исходного текста.

Давайте теперь посмотрим, какие есть опции у link. Просто вводим в командную строку link и смотрим…. Опций очень много.

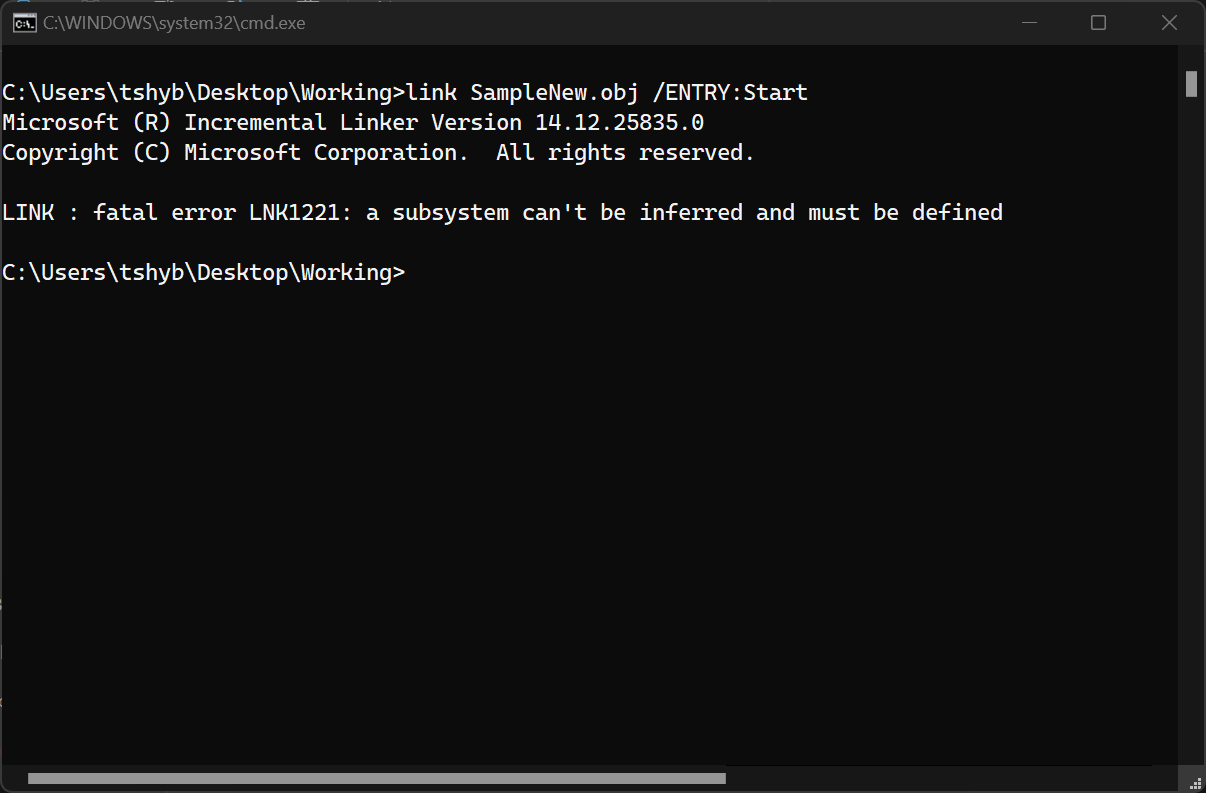






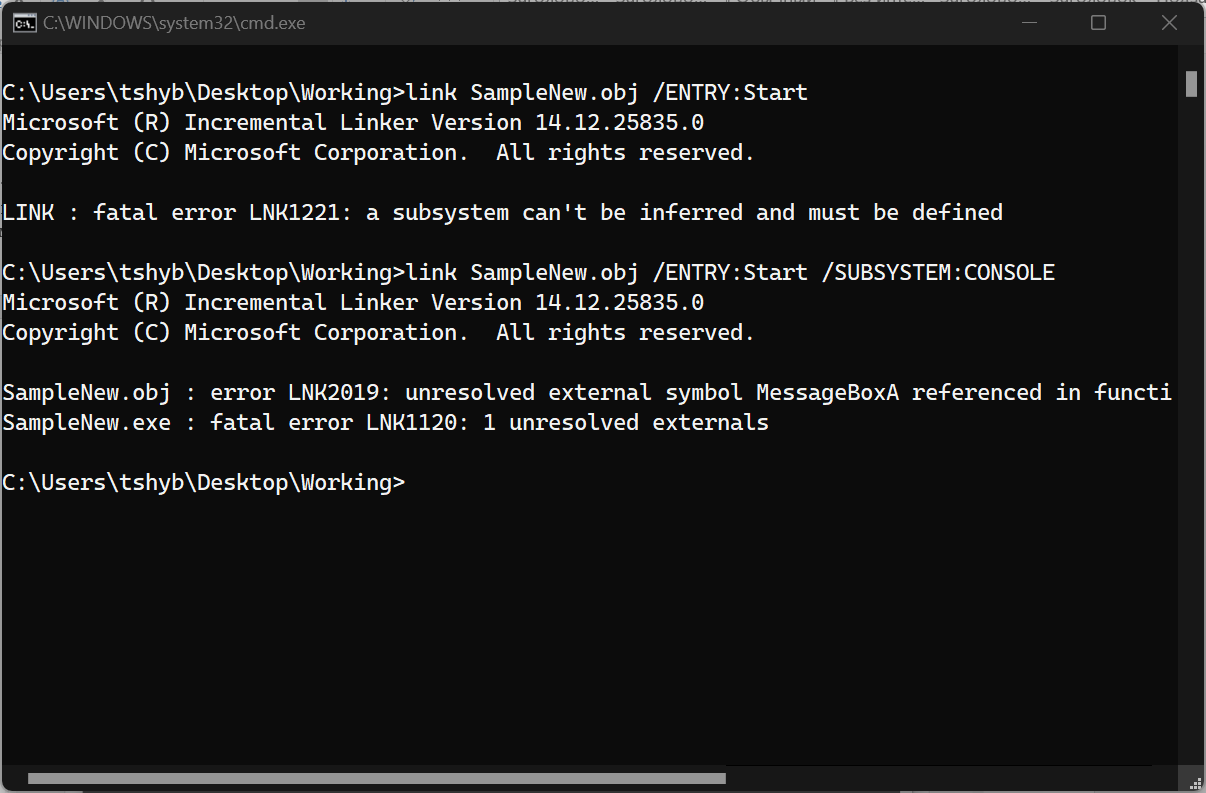


Попробуем у link прописать имя линкуемого файла (в нашем случае это SamleNew.obj) и попробовать указать некую точку входа. Получаем команду link SampleNew.obj /ENTRY:Start



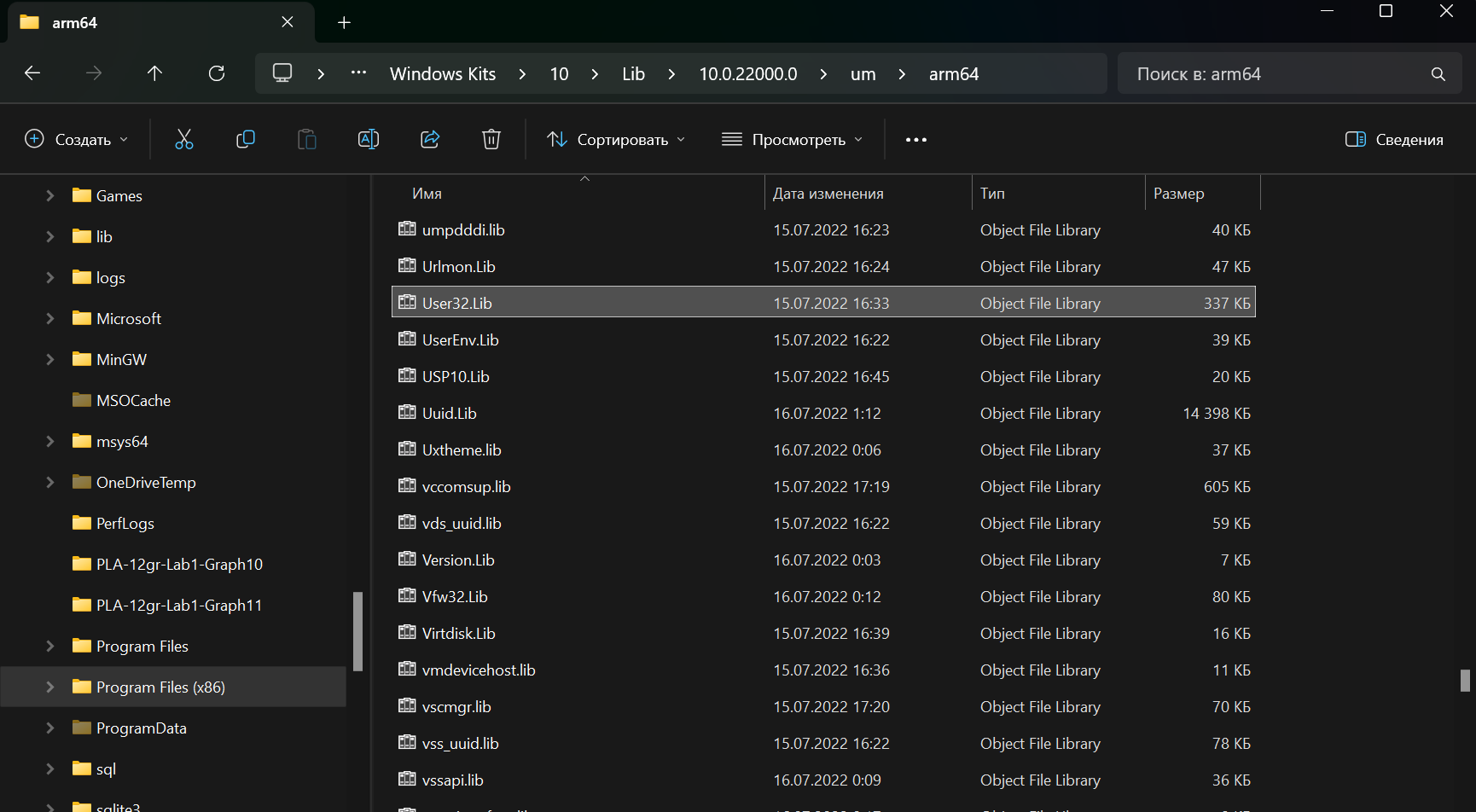
Что ж, теперь нам поругалось на subsystem. Для этого можно вернуть снова к опциям link и почитать там. Вообще, существую три параметра subsystem: BOOT\_APPLICATION, CONSOLE и WINDOWS, но я сэкономлю ваше время в рамках данной задачи и скажу, что нам нужно дополнить предыдущую строку /SUBSYSTEM:CONSOLE

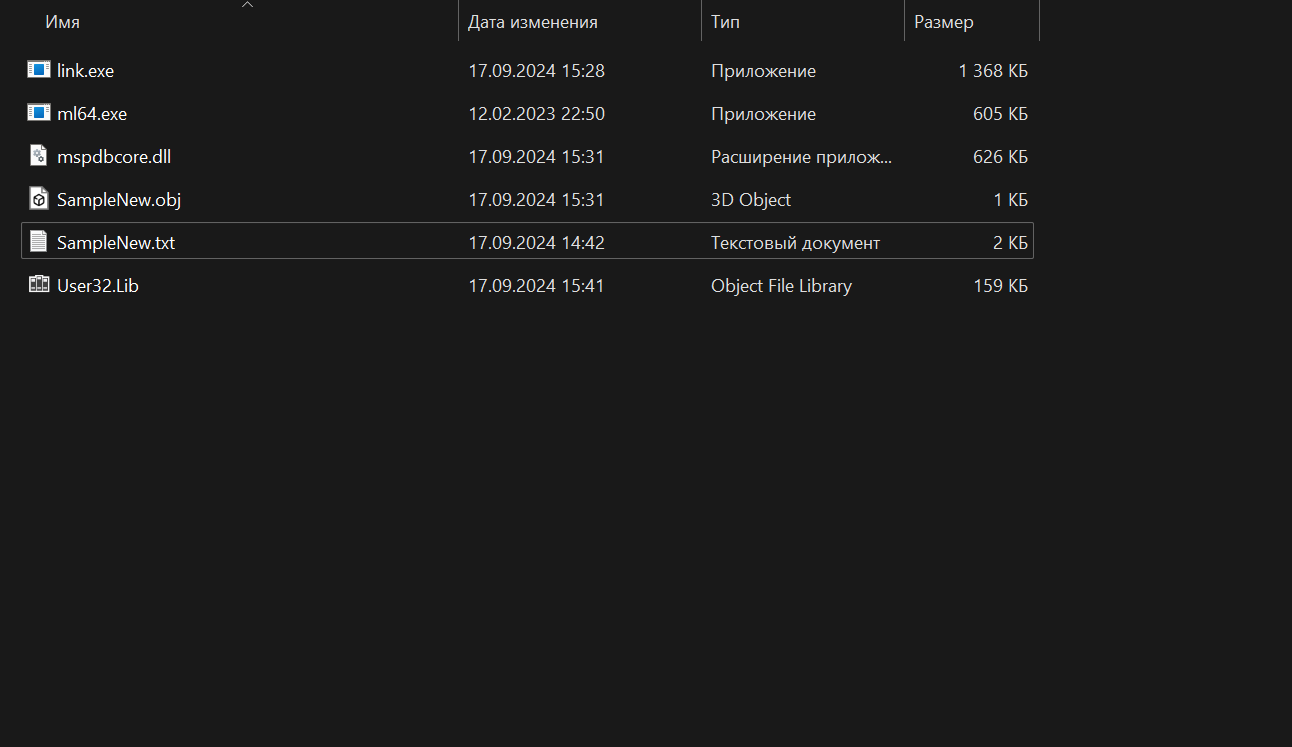
Получаем вот такую строку: link SampleNew.obj /ENTRY:Start /SUBSYSTEM:CONSOLE



Запустили и смотрим, что теперь не так. Час от часу не легче. Нам не хватает MessageBoxA, но его можно достать из имеющегося в нашей системе LIB-а User32.lib.  
Данный файл лежал у меня по такому пути: C:\Program Files (x86)\Windows Kits\10\Lib\10.0.22000.0\um\arm64

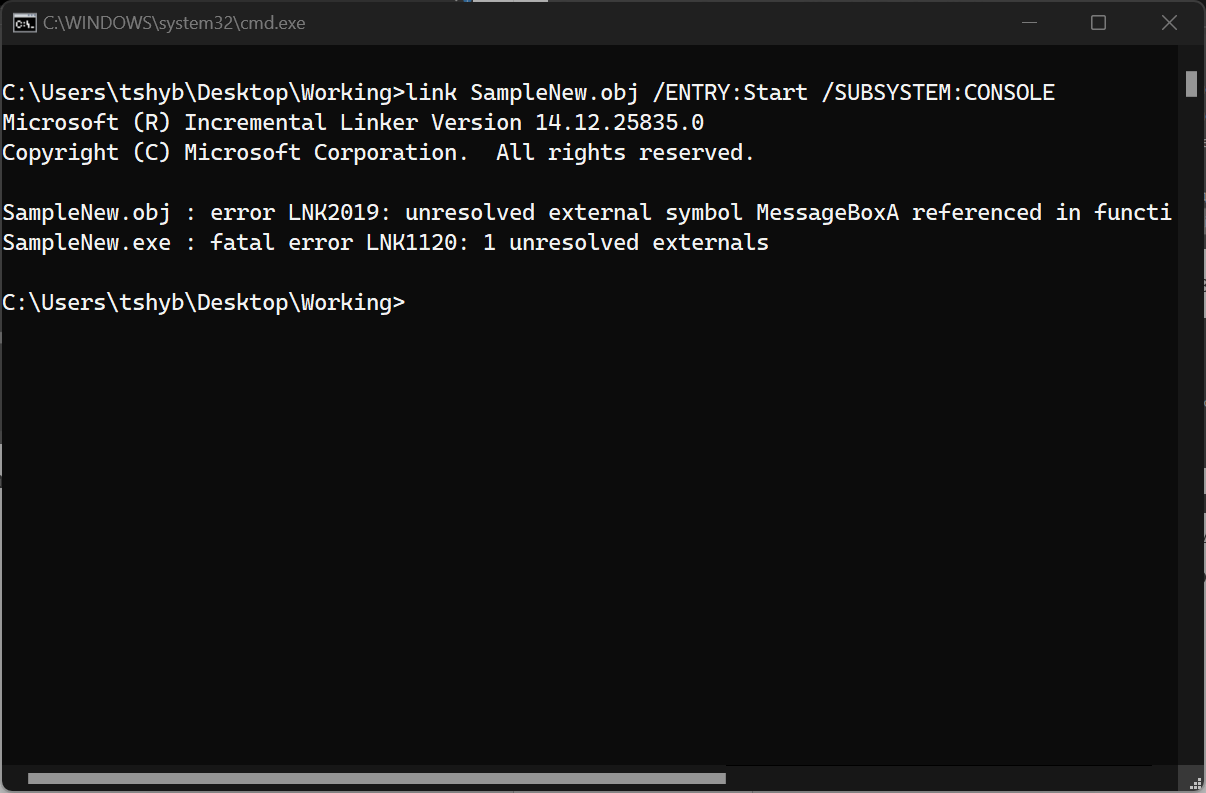
Нам нужно его скопировать в папку Working.

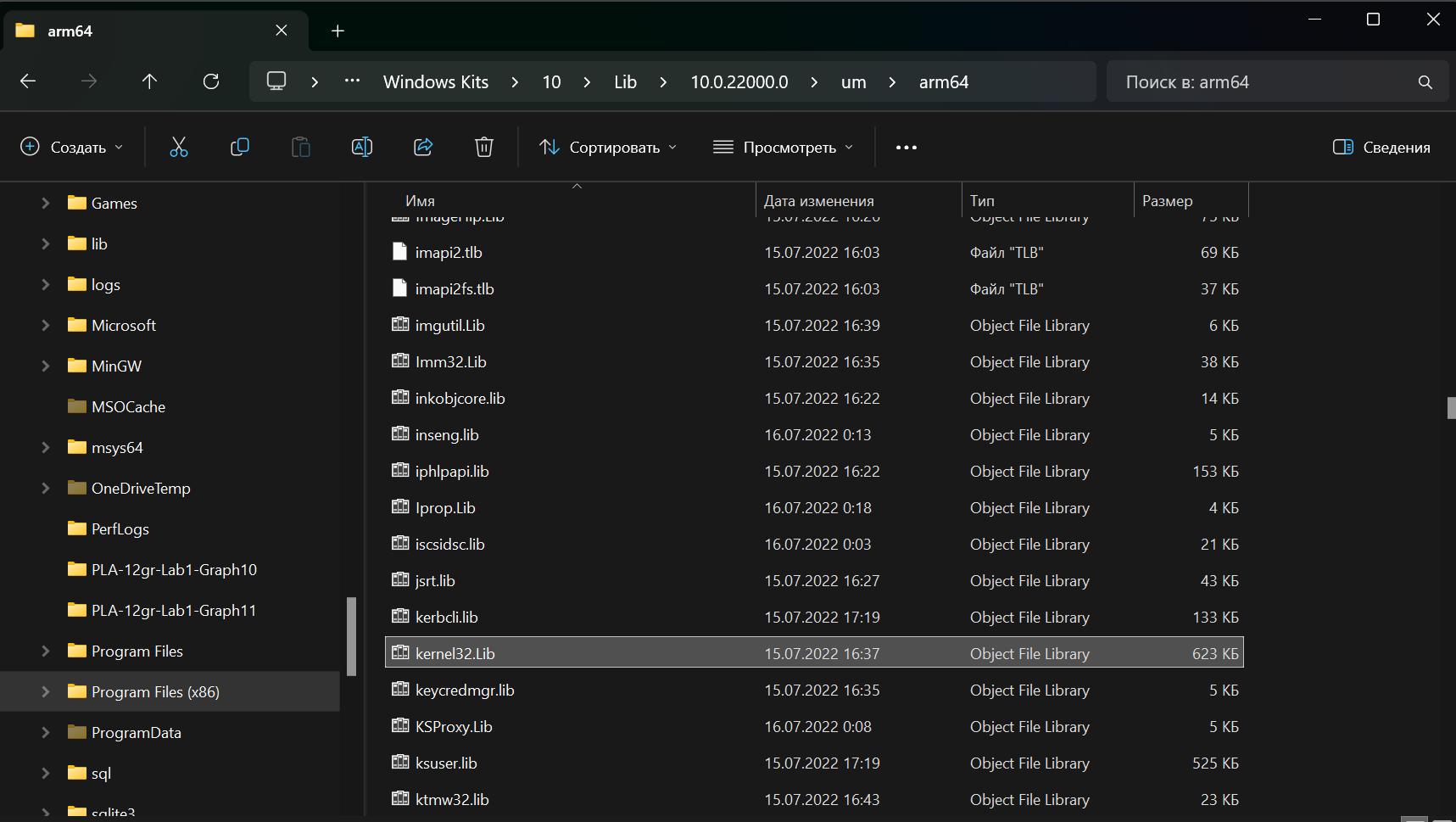


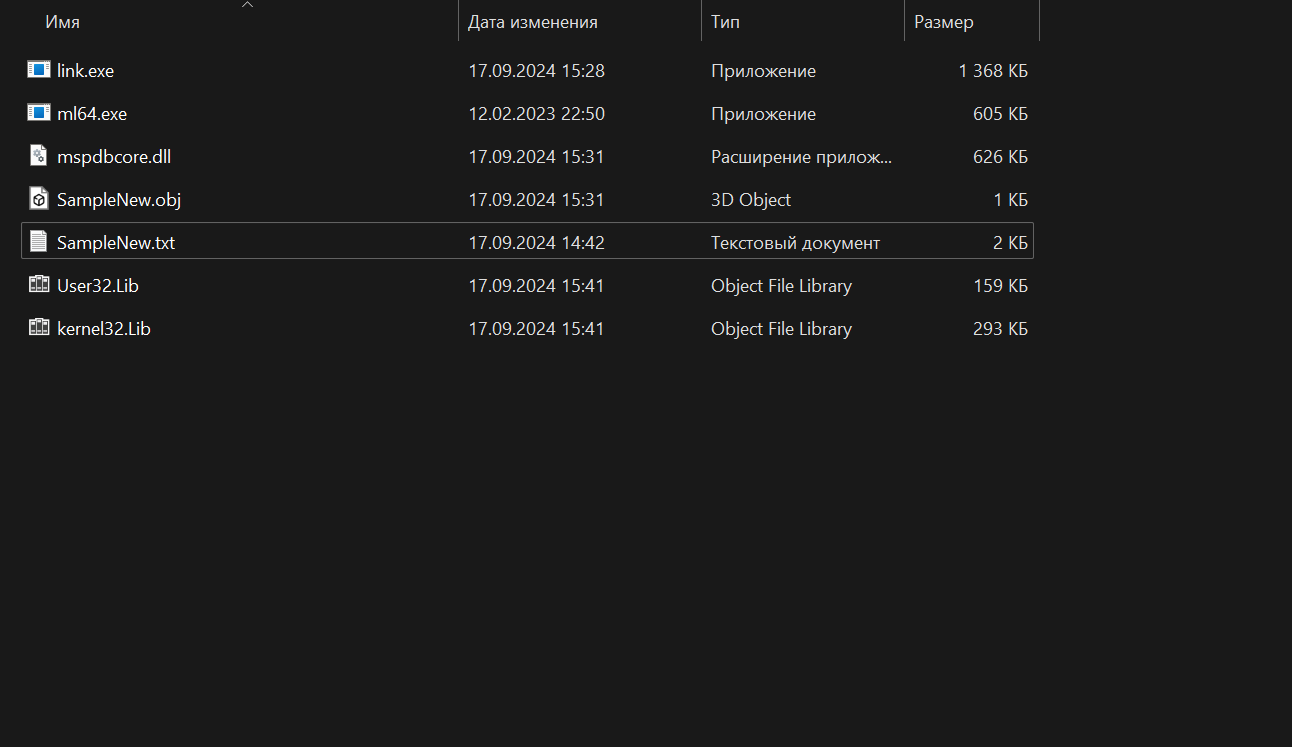


Чудесно. Снова пишем link SampleNew.obj /ENTRY:Start /SUBSYSTEM:CONSOLE и никакого прогресса. Если долго мучиться, то можно понять, что:

1. Нам нужно писать не /SUBSYSTEM:CONSOLE, а /SUBSYSTEM:BOOT\_APPLICATION
2. Нам нужна ещё одна LIB-а: kernel32.lib. Её можно найти там же, где и User32.lib. Копируем наш kernel32.lib в папку Working



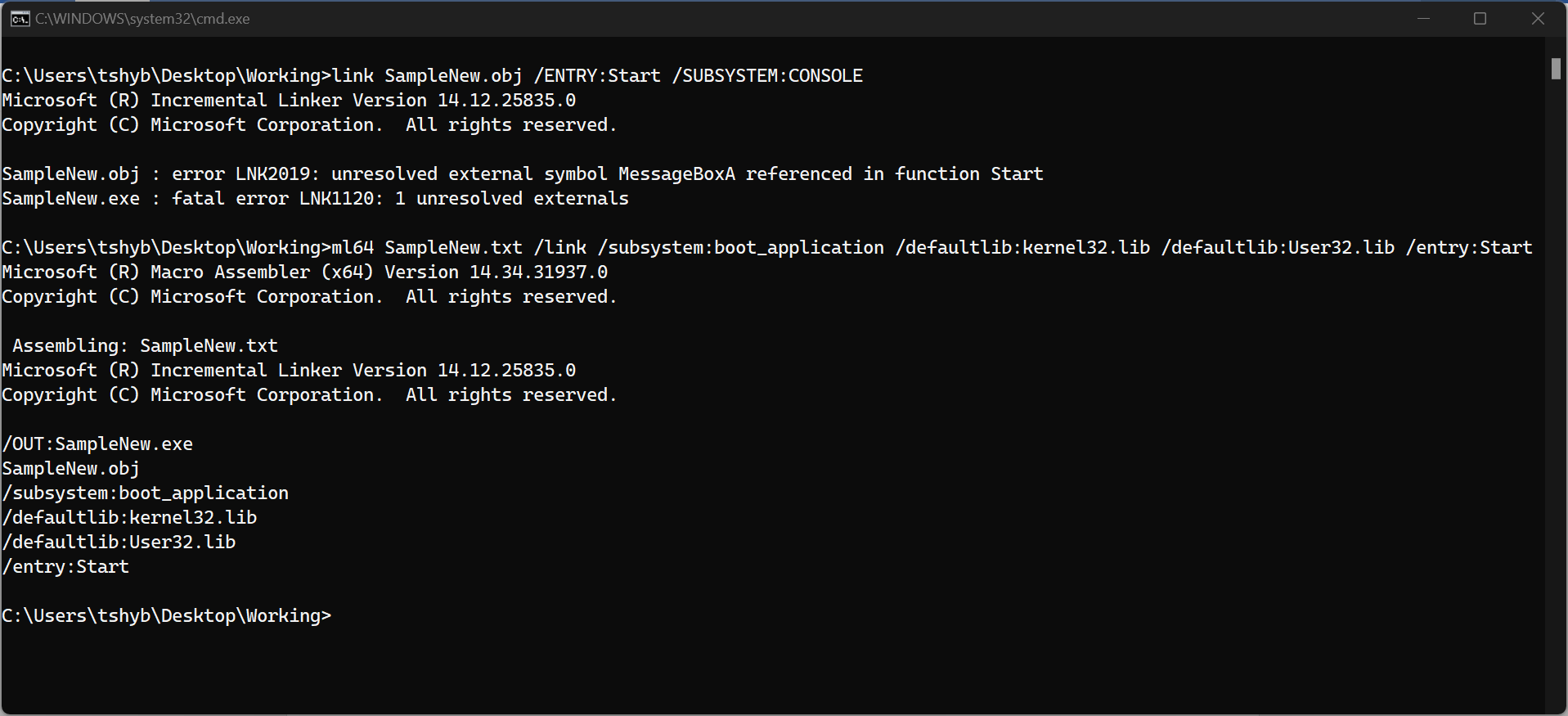


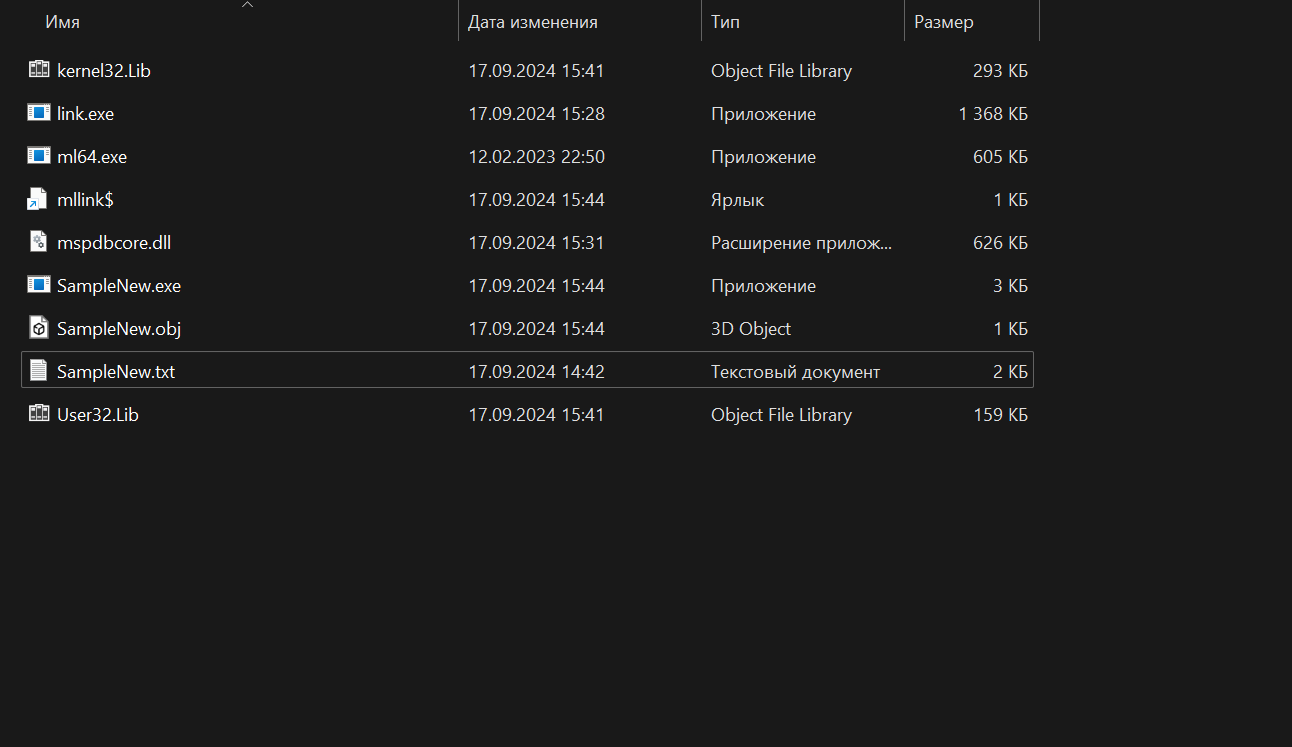


Если внимательно изучить предоставленные нам материалы к 3 лабораторному занятию, то можно увидеть строку, благодаря которой мы получим, наконец-то, что-то путное.

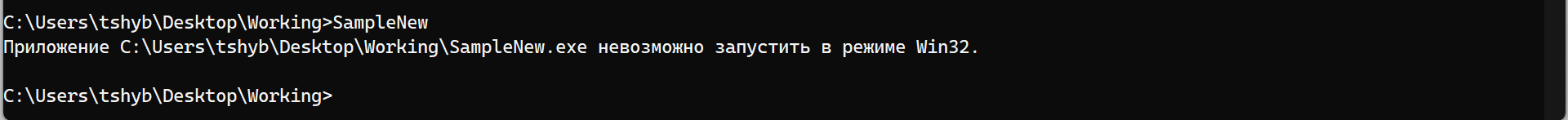
Нужная строка: ml64 SampleNew.txt /link /subsystem:boot\_application /defaultlib:kernel32.lib /defaultlib:User32.lib /entry:Start

После того, как мы запустили команду, в папке Working должно появиться SampleNew.exe.

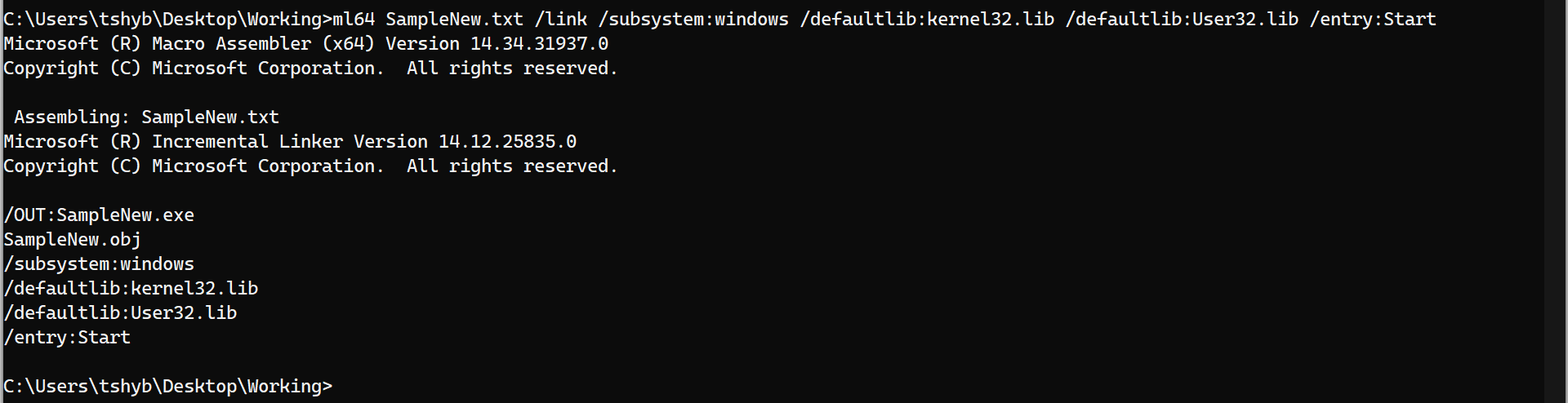




Давайте попробуем запустить наш exe, как мы делали это в DosBox. Просто вводим SampleNew.exe и видим ошибку…



В целом, эту ошибку решить достаточно легко. Надо просто вместо /subsystem:boot\_application ввести /subsystem:windows.  
Получаем вот такой вариант: ml64 SampleNew.txt /link /subsystem:windows /defaultlib:kernel32.lib /defaultlib:User32.lib /entry:Start



Теперь мы снова пишем SampleNew.exe и всё работает!

