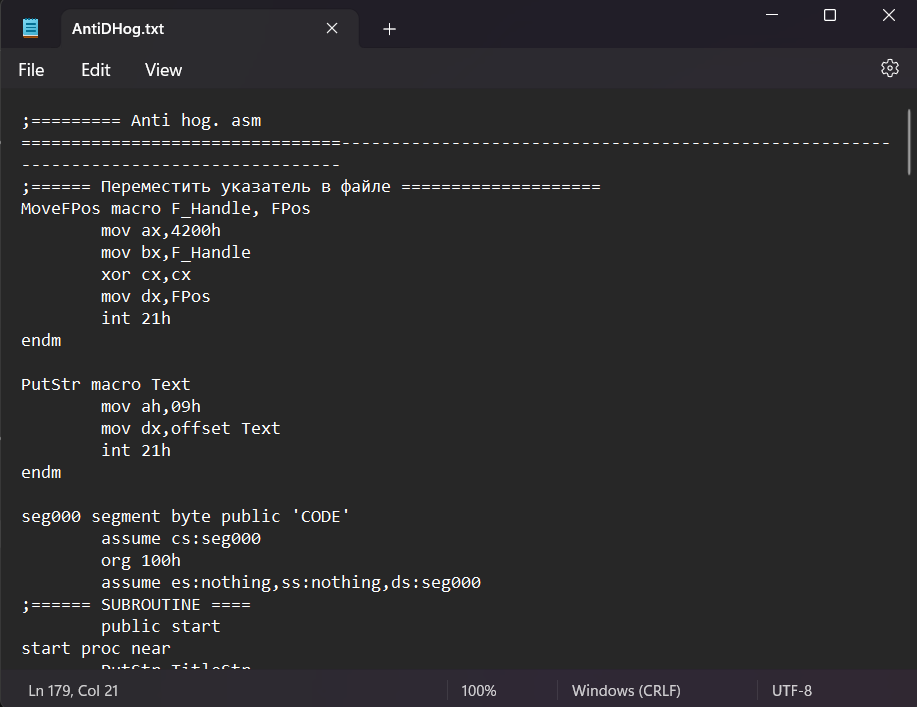
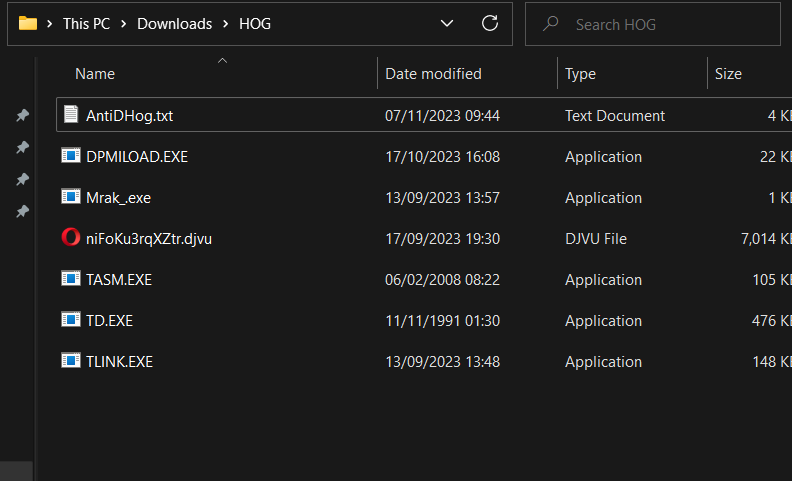
Набрал исходный текст антивируса:



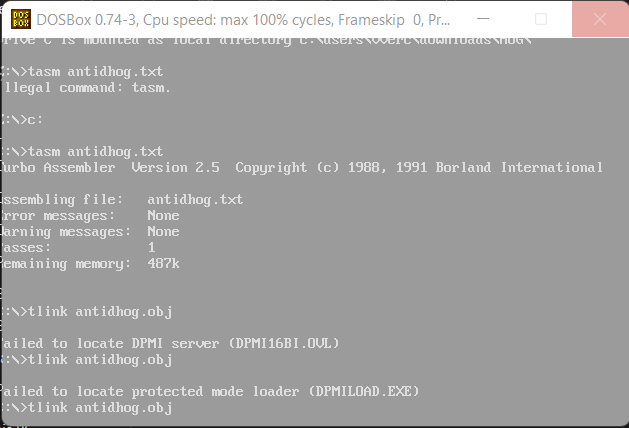
Переместил исходный текст антивируса в зараженную папку:



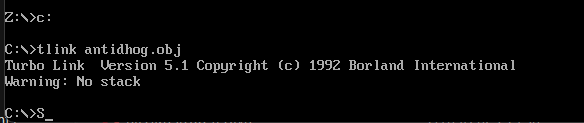
Транслировал:

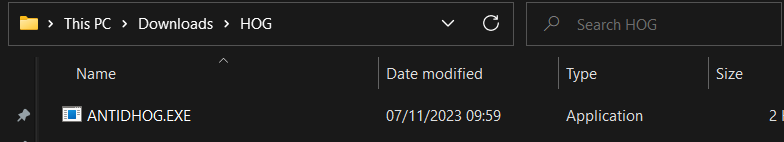


Однако слинковать не получилось(сначала добавил недостающие исполняемые модули, а потом dos box завис)

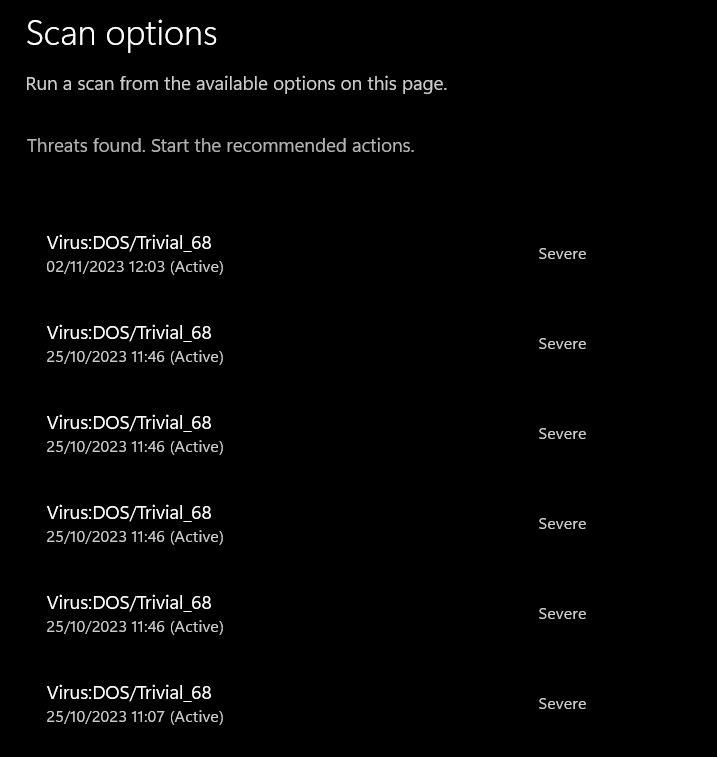


Однако я перезапустил dos-box и попробовал слинковать еще раз, после чего я получил исполняемый модуль:

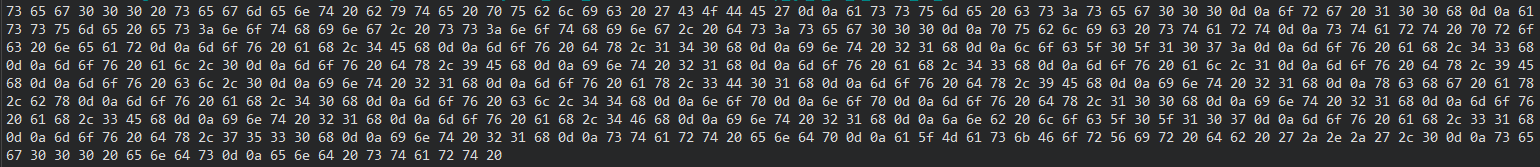




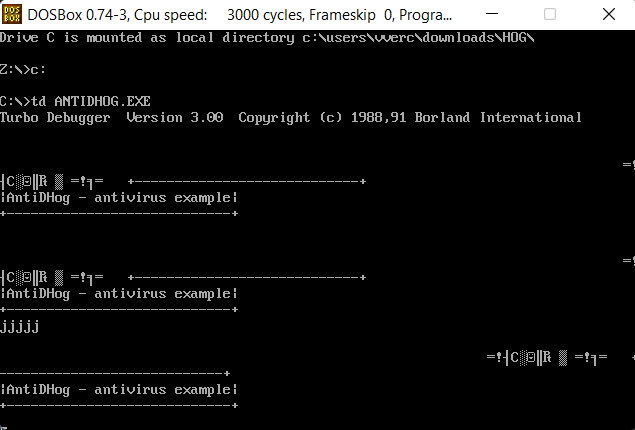
В процессе линковки антивирус отправлял уведомления. Я проверил папку с помощью антивируса после того как получил исполняемый модуль антивируса и новых угроз не обнаружил(то есть остались лишь зараженные в части первой лабораторной работы 2 файлы):



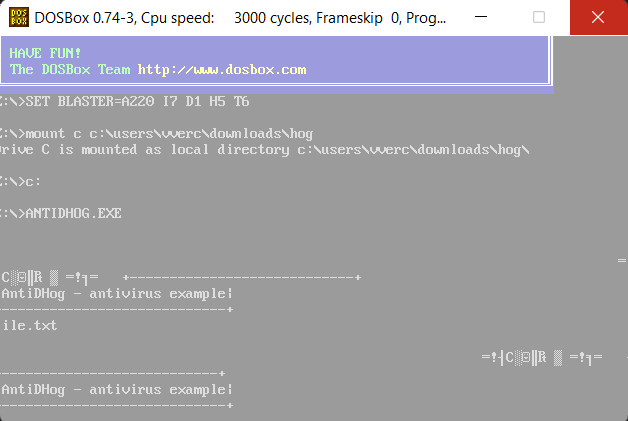
Ниже представлено в шестнадцатеричном виде содержимое файла с бывшим исходным текстом вируса:



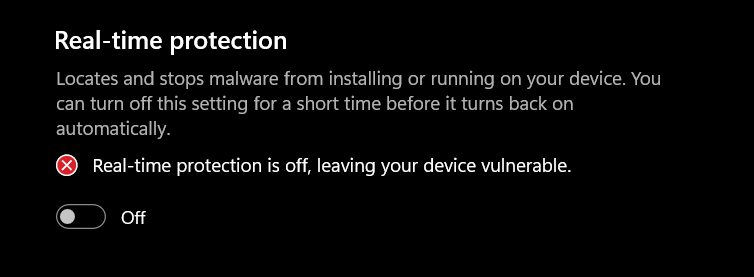
Во время отладки исполняемого модуля антивируса dos-box завис:

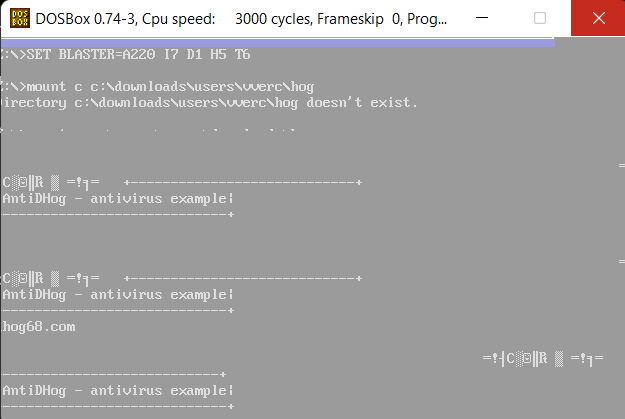


Аналогичное зависание произошло во время исполнения модуля:

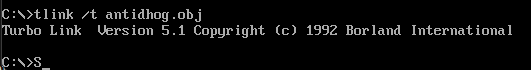


После чего я решил отключить антивирус, однако dos-box по прежнему зависал во время исполнения модуля антивируса





После я решил перелинковать полученный после транслирования объектный модуль c флагом /t :



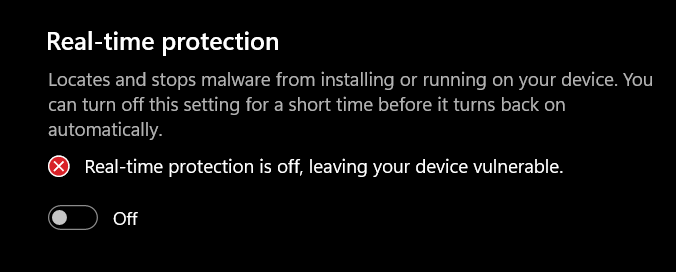
И получил исполняемый модуль с расширением .COM



После выполнения получил следующее:



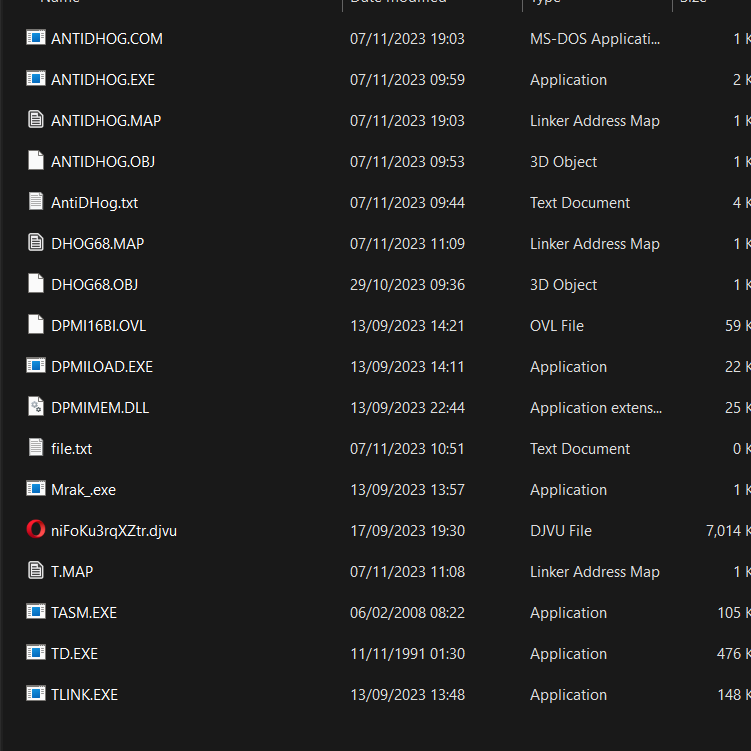
Отключил антивирус Windows



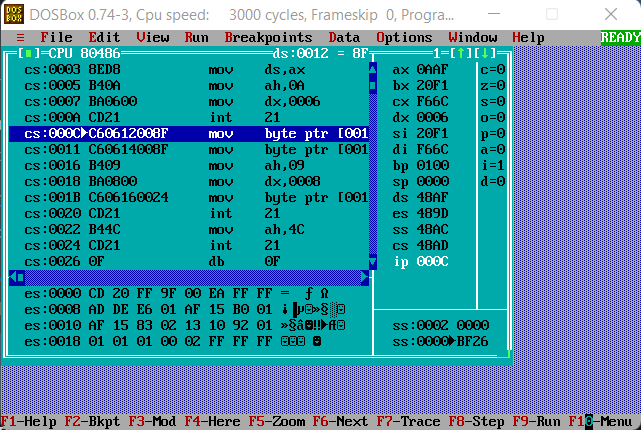
И получил следующее:



Файл dhog68.com действительно исчез:



При этом файл mrak.exe выполняется пошагово с помощью отладчика без каких-либо проблем.



То есть произошло убийство файла dhog68.com, так как до этого во время пошаговой отладки mrak.exe отладчик и DOS-BOX зависали.

Шестнадцатеричное представление исполнимого модуля-антивирусника

