Лабораторная работа №2 часть 1

Работа с вирусами

**Задание**

**1.1. Используя оболочку DosBox, книгу про ассемблер, набрать исходный текст ВИРУСА DHog68, транслировать, линковать, получить com-файл в папке про ПАПУ.**

**1.2. Скопировать всё содержимое папки про ПАПУ в папку HOG.**

**1.3. Сделать папку HOG активной, используя исполнимый модуль td.exe ПОШАГОВО ВЫПОЛНИТЬ программу DHog68.**

**1.4. Проверить, действительно ли происходит заражение всех файлов папки. Для этого с помощью ОТЛАДЧИКА td.exe ПОвкШАГОВО ВЫПОЛНИТЬ программу, получаемую в результате загрузки в отладчик файла Mrak.asm (файл, в котором до выполнения шага 1.3. находился исходный текст решения задачи про папу).**

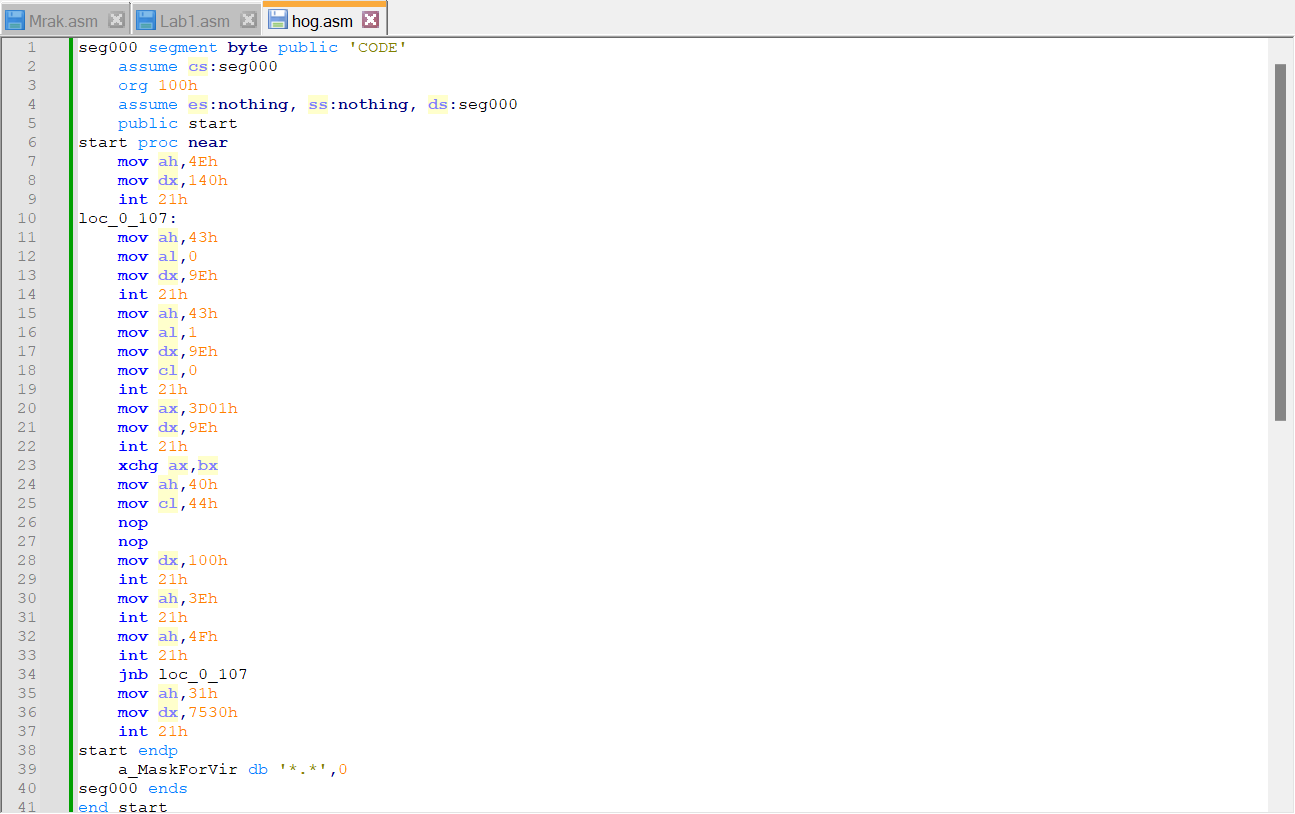
**1.5. Проверить, каким образом НА ПОЯВЛЕНИЕ ЭТОГО ФАЙЛА.com реагирует Ваша антивирусная защита (если пока её нет – установить любой бесплатный антивирусник).**

**1.6. Используя защиту, протестировать файлы, находящиеся только в папках DHOG и в папке про папу.**

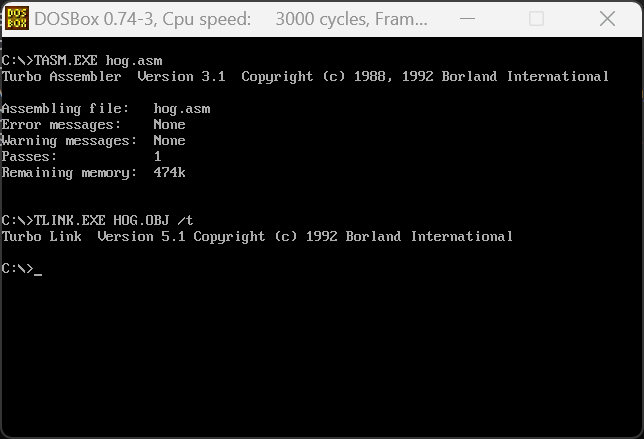
**1.7. Весь процесс ЗАДОКУМЕНТИРОВАТЬ и прислать, как всегда, отчёт о проделанной работе в виде известных Вам трёх файлов до 23-59 21.10.2024 года!**

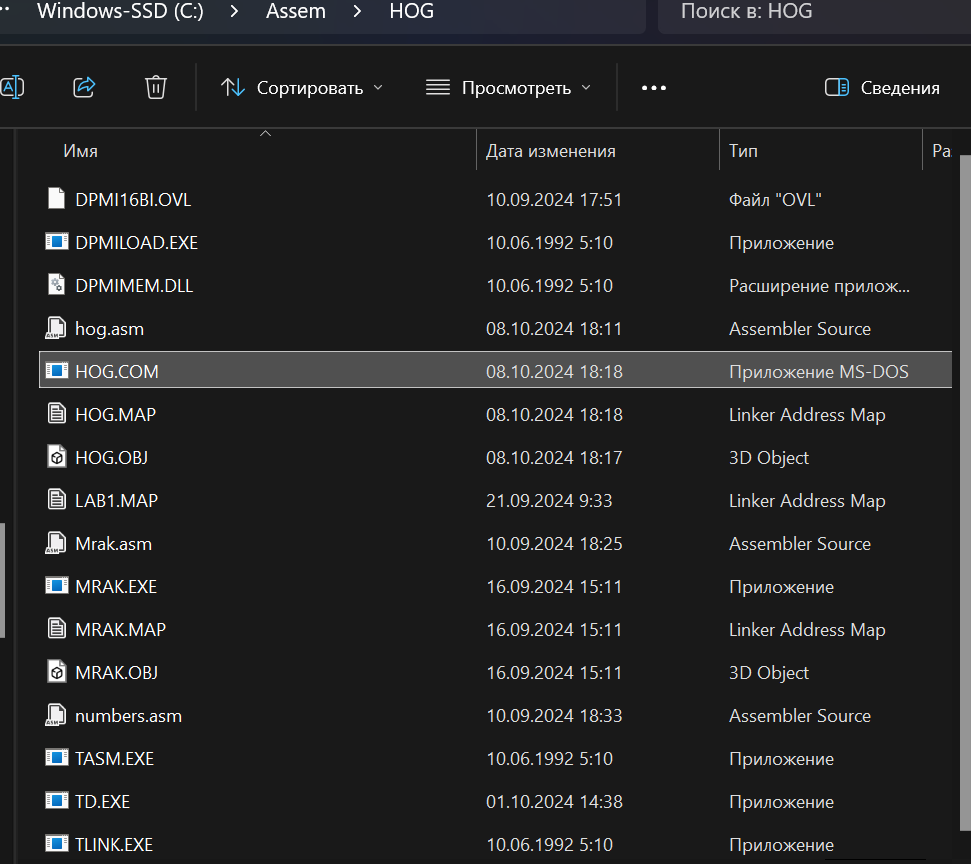
**Ход решения**

На всякий случай продублирую код из лекции с DHOG68:



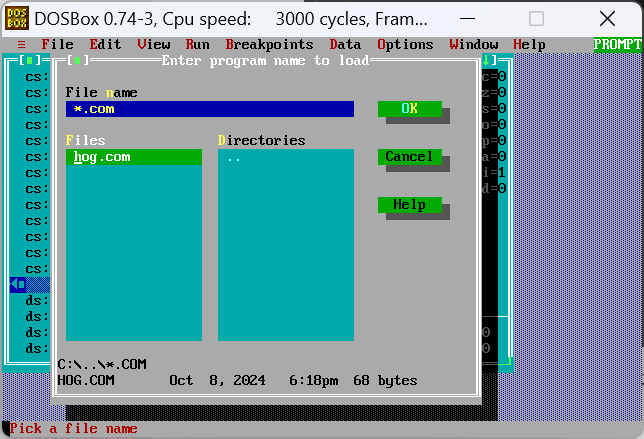
Теперь будем транслировать и линковать, используя уже известные нам TASM и TLINK. Я заранее перенесла все файлы с ПАПОЙ в новую папкуHOG.



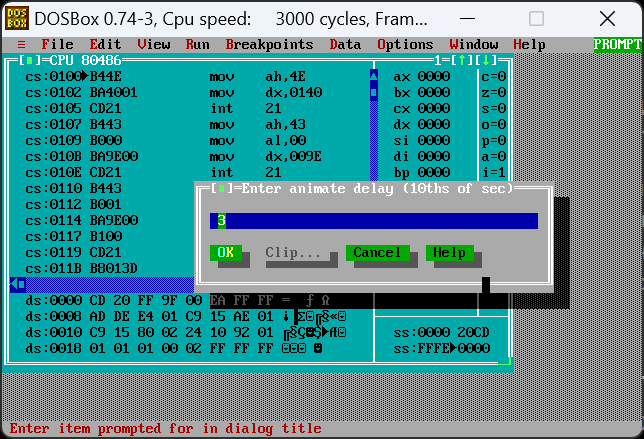


Я на картинке выделила то, что у нас создался нужный нам файл HOG.COM

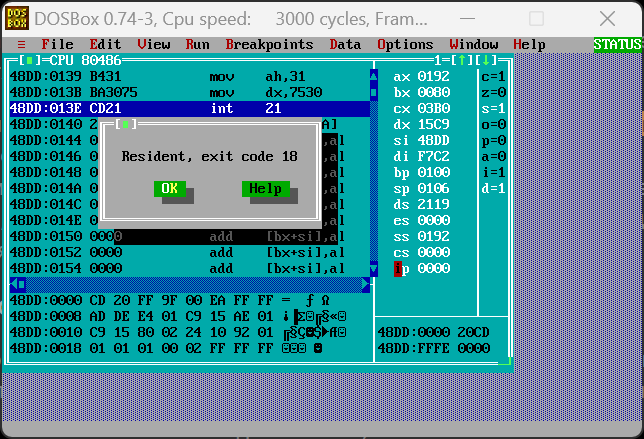
Теперь нам надо запустить турбо-отладчик td.exe. В нём мы запустим нам hog.com



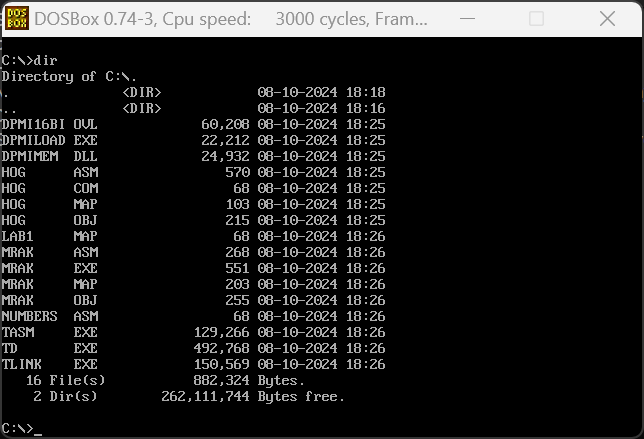
Теперь нам надо запустить пошаговую отладку. Для этого выбираем Run -> Animate



Можете поменять значения, но я всё оставила. Нажимаем ОК и ждём.



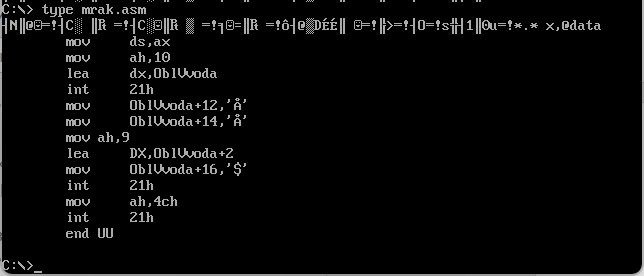
Теперь, на всякий случай, проверим, были ли файлы изменены:



Теперь попробуем запустить отладчик:

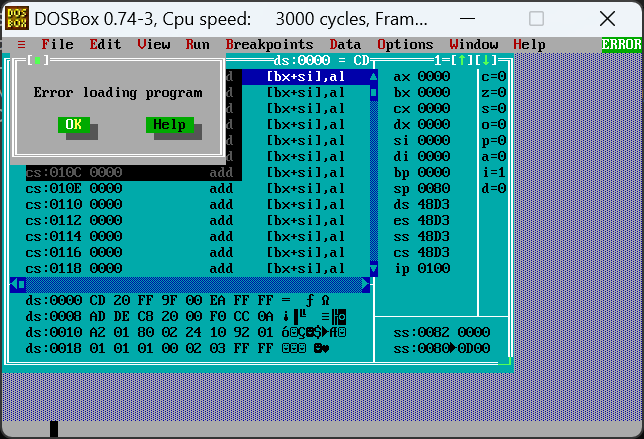
А он не запускается! Но без паники – всё идёт как надо

А вот какую красоту мы увидим, если захотим посмотреть содержимое нашего mrak.asm



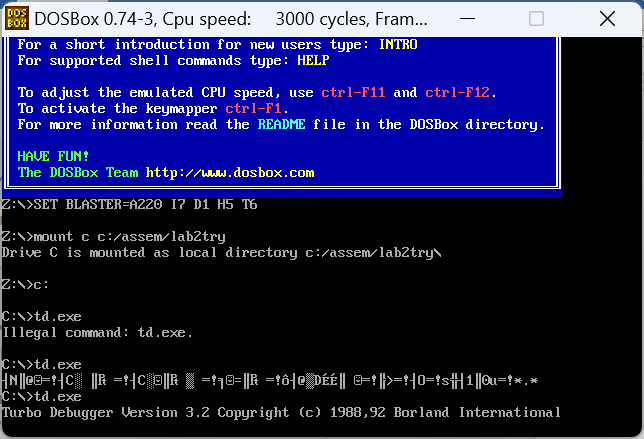
Впечатляет, правда?

Давайте попробуем заново скопировать файл отладчика и запустить наш мрак ассемблеровский.

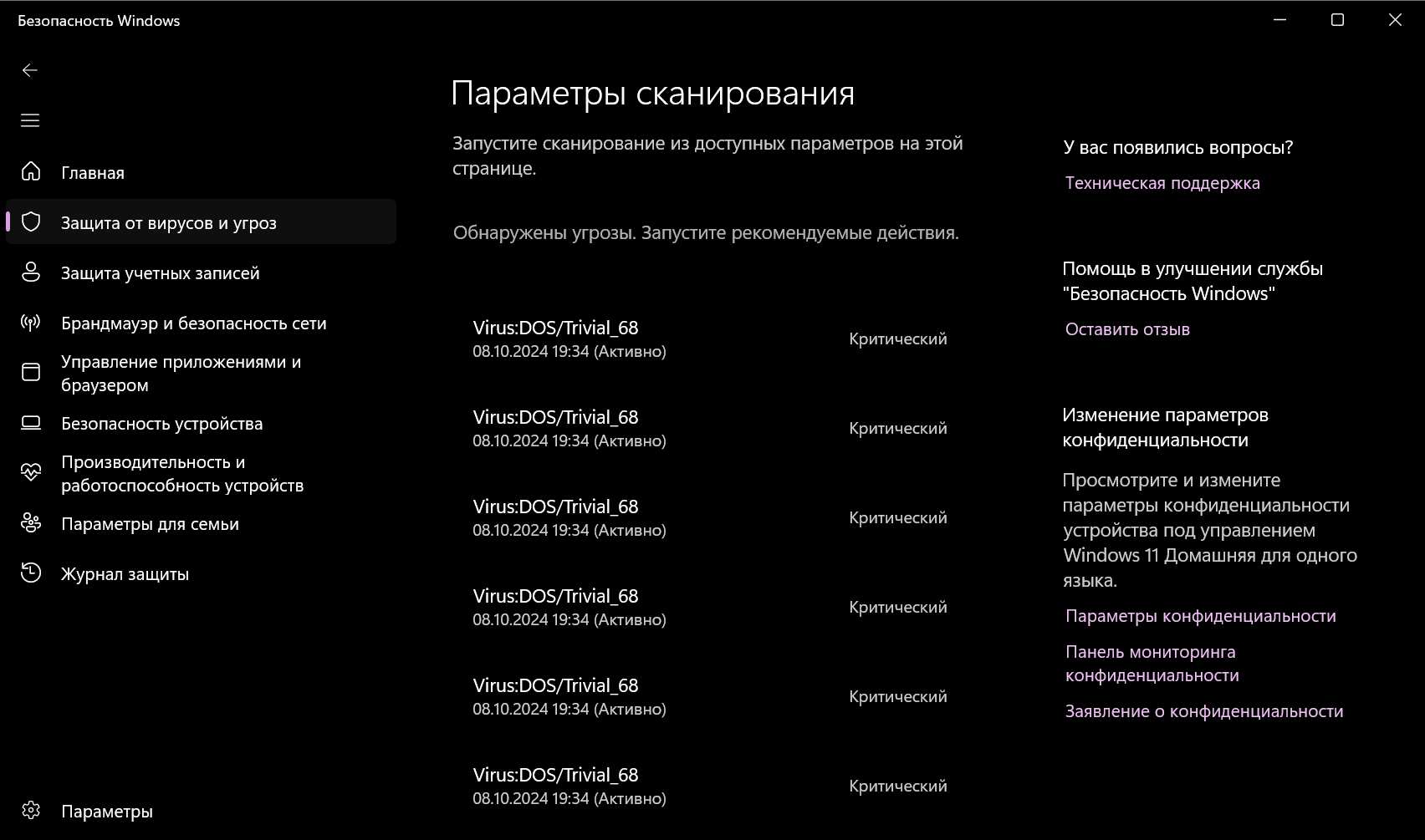


Не получится так. Надо пробовать запустить пошагово mkar.exe.

Загружаем, как и hog.com, а потом через тот же Animate запускаем. Но, увы, турбо-отладчик просто вылетает, после выполнения шага.



Спросим у антивируса Windows Defender, что он думает о папке HOG. Увидим, что всей файлы папки – вирусы.



А теперь проверим, как там наш ПАПА поживает:

