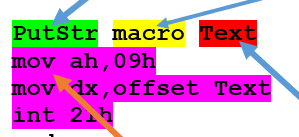
Отчёт Лаб работа 2 часть 2

2.1:

К одной из лекций мы уже набирали исходный текст антивируса, я его немного модифицировал, взяв из текста лекции 7 «AntiDHog. Начало» макроопределение и макрокоманды:



И добавил это вместо вызова библиотечной функции из текста книги, получился исходный текст на языке записи алгоритмов:

;======AntiDHog.asm ===================================

;======Переместить указатель в файле ===================================

MoveFPos macro F\_Handle, FPos

mov ax, 4200h

mov bx, F\_Handle

xor cx, cx

mov dx, FPos

int 21h

endm

PutStr macro Text

mov ah,09h

mov dx,offset Text

int 21h

endm

seg000 segment byte public 'CODE'

assume cs:seg000

org 100h

assume es:nothing,ss:nothing,ds:seg000

;====== S U B R O U T I N E ===================================

public start

start proc near

PutStr TitleStr

;====== Поставить DTA

mov ah,1ah

mov dx,offset DTA

mov cx,27h

int 21h

;========================

mov ah,4eh

mov dx,offset a\_MaskForVir

int 21h

BegScan:

;==== Переслать имя в переменную FName =====

push ds

pop es

mov si, FN\_Ofs

mov di, offset FName

mov cx, 13

rep movsb

;======================================

mov ah, 43h

mov al, 0

mov dx, offset FName

int 21h

mov ah, 43h

mov al,1

mov dx, offset FName

mov cl, 0

int 21h

mov ax, 3d10h

mov dx, offset FName

int 21h

mov FHandle, ax

mov ah, 40h

mov cl, 44h

nop

nop

call InfoAboutFile

call ReadSignature

cmp SignatureFound,0

je NextFile

call KillExecutable

call RemoveExecutable

NextFile:

call CureInfo

mov ah,4fh

int 21h

jnb BegScan

int 20h

start endp

;===========================================

a\_MaskForVir db '\*.\*',0

DTA db 43 dup (0)

FN\_Ofs equ offset DTA+1eh

FName db 128 dup(0)

IName db 128 dup(0)

SignatureFound db 0

SignatureArray db 14 dup(0)

VirSignature db 0cdh,21h,0b4h,43h,0b0h,01h,0bah

db 9eh,00h,0b1h,00h,0cdh,21h,0b8h

Int20Cmd db 0cdh,20h

FHandle dw 0

TitleStr db '+----------------------------+',13,10

db '|AntiDHog - antivirus example|',13,10

db '+----------------------------+',13,10,'$'

NormStr db ' - Ok',13,10,'$'

CureStr db ' - Deleted',13,10,'$'

;=========================================================

ReadSignature proc near

mov SignatureFound,0

MoveFPos FHandle 0eh

mov ah,3fh

mov bx,FHandle

mov cx,14

mov dx,offset SignatureArray

int 21h

cld

push ds

pop es

mov si,offset VirSignature

mov di,offset SignatureArray

mov cx,14

repe cmpsb

jnz Finish

mov SignatureFound,1

Finish: ret

ReadSignature endp

KillExecutable proc near

MoveFPos FHandle 0

mov ah,40h

mov bx,FHandle

mov cx,2

mov dx,offset Int20Cmd

int 21h

mov ah,3eh

mov bx,FHandle

int 21h

ret

KillExecutable endp

RemoveExecutable proc near

mov ah,41h

mov dx,offset FName

int 21h

ret

RemoveExecutable endp

InfoAboutFile proc near

push ds

pop es

mov si,offset FName

mov di,offset IName

NextChar: lodsb

stosb

cmp al,0

jne NextChar

dec di

mov byte ptr [di],'$'

PutStr IName

ret

InfoAboutFile endp

CureInfo proc near

mov ah,9

mov dx,offset NormStr

cmp SignatureFound,0

je ContMsg

mov dx,offset CureStr

ContMsg: int 21h

ret

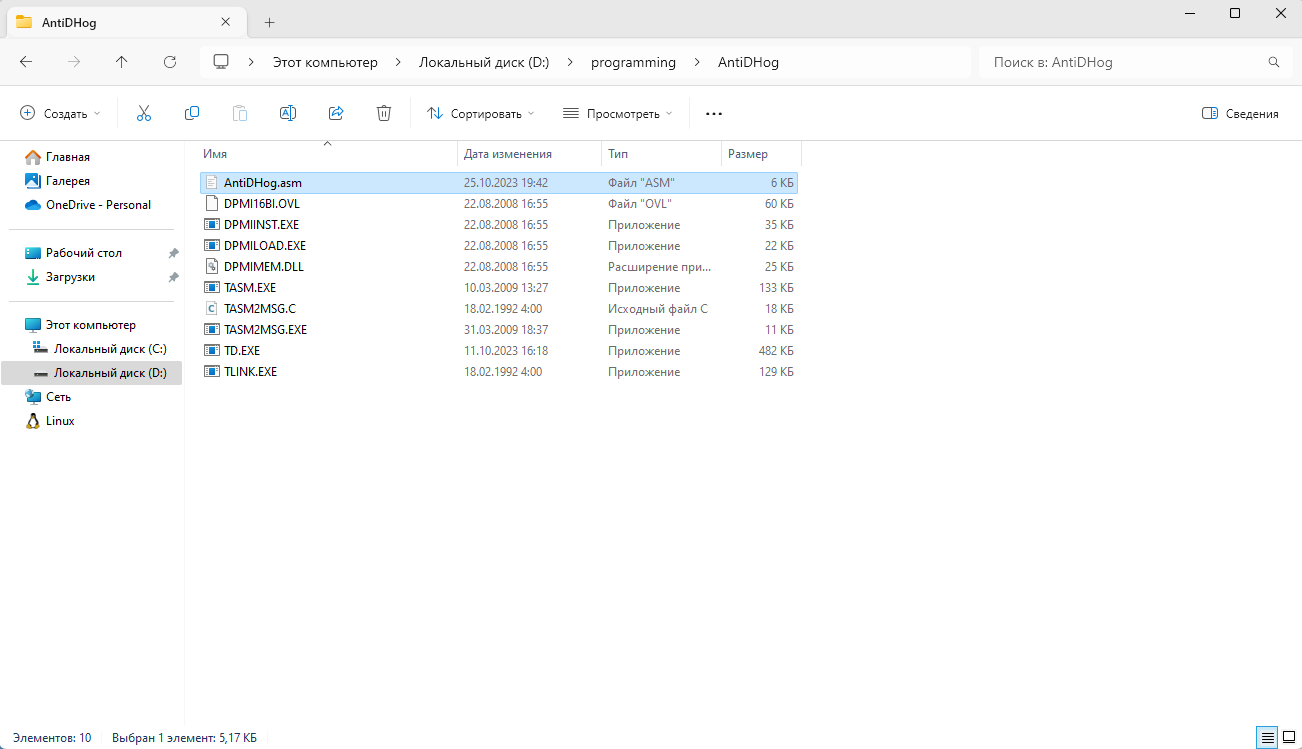
CureInfo endp

seg000 ends

end start

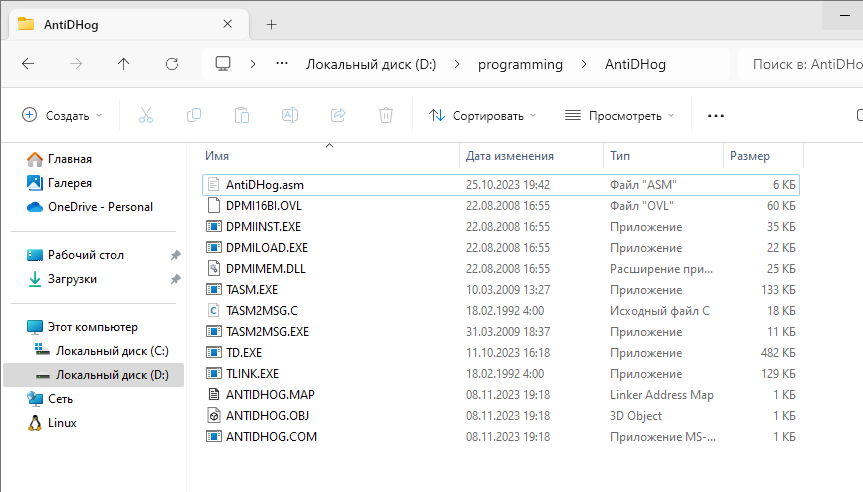
;=========================================================

Далее я создал папку и добавил в неё транслятор, линковщик, дополнительные файлы и исходный текст

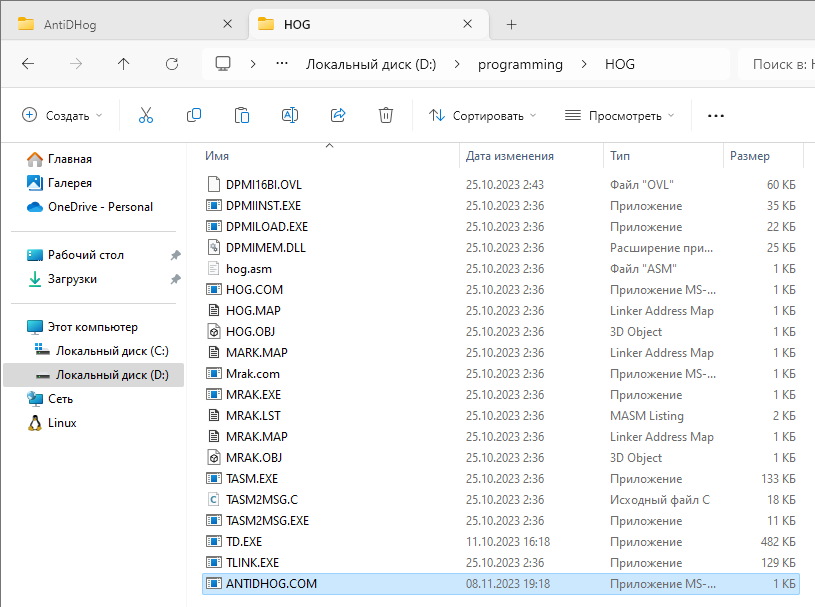


2.1



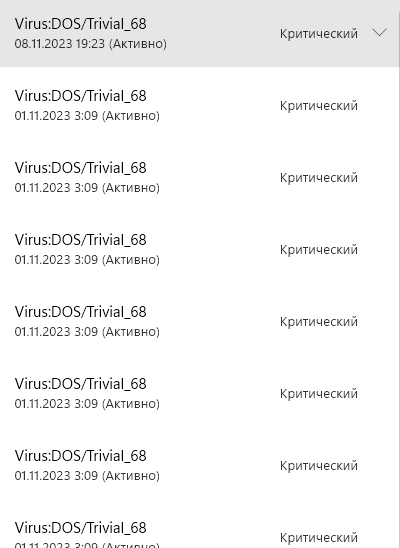


Сначала я транслировал и линковал antidhog.asm в папке и исправными транслятором и линковщиком, т.к. в задании на это нет ограничений, а после этого перенёс антисвинью в папку со свиньёй, то есть я «получил исполнимый модуль в папке HOG»



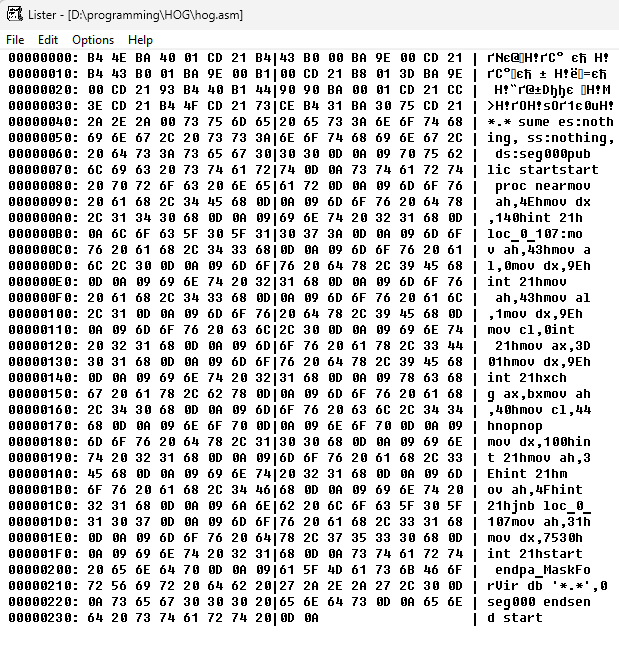
2.3

На появление исполнимого модуля антивируса моя антивирусная защита никак не реагирует в отличие от файлов, заражённых вирусом:



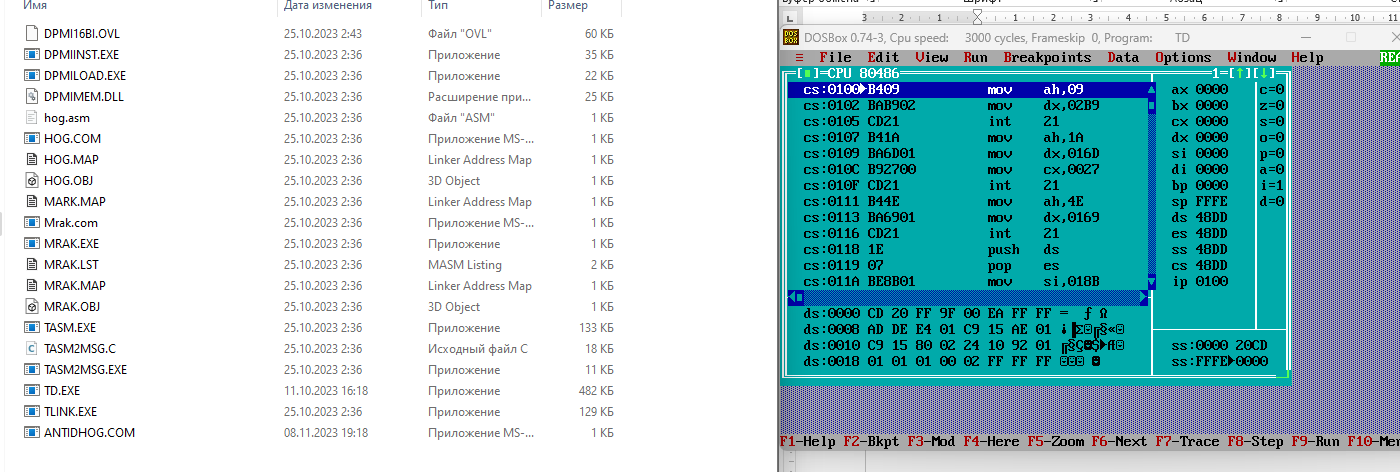
2.4

Как видим, в начале файла какаято муть☹

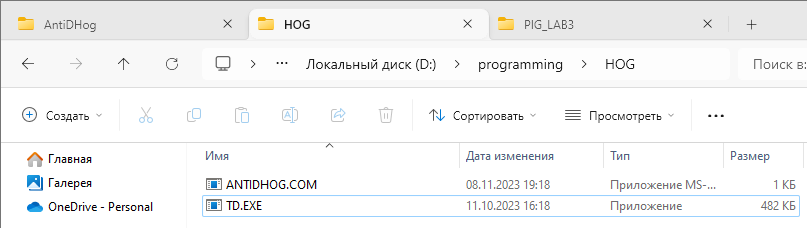


2.4(2):

До отладки и тестирования:



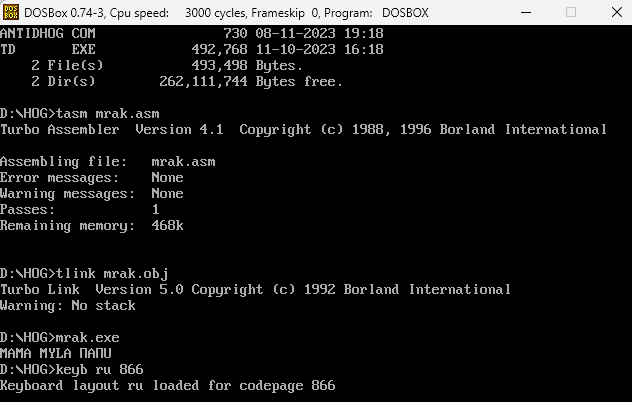
После:



В процессе отладки я уже не заскринил, но можно заметить, что не заражённые файлы уцелели, заражённые же файлы испарились(новый термин подразумевающий удаление файлов, но не изничтожение)

2.5

Ну я скопировал мрак из другой папки, как и транслятор…. И линковщик… но не знаю, что тут должно было удивительного произойти…



До копирования выполнение мрака.асм не представлялось возможным ввиду отсутствия исполнимого модуля мрака(предположительно, произошло удаление, т.к. файлы буквально пропали с диска, не убийство, т.к. при убийстве они бы остались но в начале файлов была бы команда int 20h) как такого, как и файла с исходным текстом программы, как и вообще всех файлов в этой папке кроме антисвиньи и дебаггера….

После запуска антидхога теперь:



(сначала вместо океев были крокозябры, в коде были русские буквы, но я исправил и прикрепил уже исправленный текст на языке записи алгоритмов)

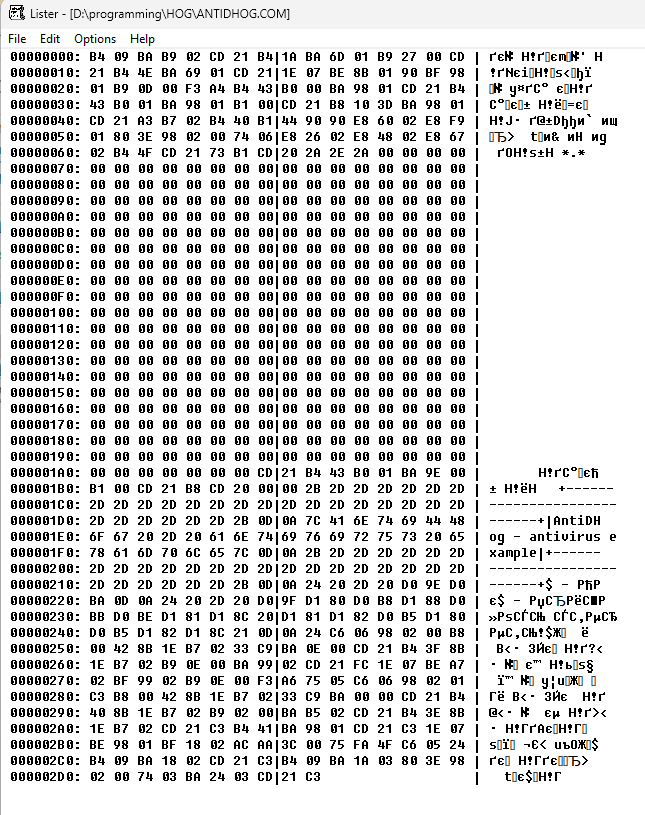
p.s. при первом запуске почти все файлы были написаны как Deleted(не удивительно), кроме td.exe и antidhog.com, потому что они и не были заражены

2.6

Честно говоря я не знаю как проверить средствами оболочки операционной системы windows, происходит ли удаление или изничтожение файлов, поэтому давайте представим что для этого пункта произошло изничтожение, а для предыдущего – удаление и сделаем вид, что задание сделано правильно(пожалуйста не снимайте 16 баллов я попытался☹)

2.7

До обработки папки HOG:



После обработки папки HOG:

Спойлер: ничего не поменялось

