**Лабораторная работа №2. Часть 2.**

**Судник Павел Олегович**

2.1. Набрать исходный текст антивируса AntiDHog (4 балла, отсутствие – минус 4 балла).

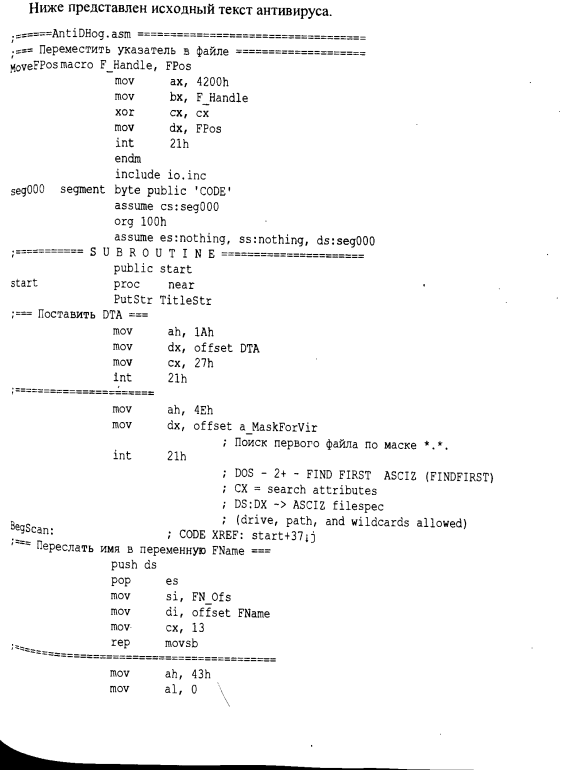


Рисунок 1 - текст антивируса в книге

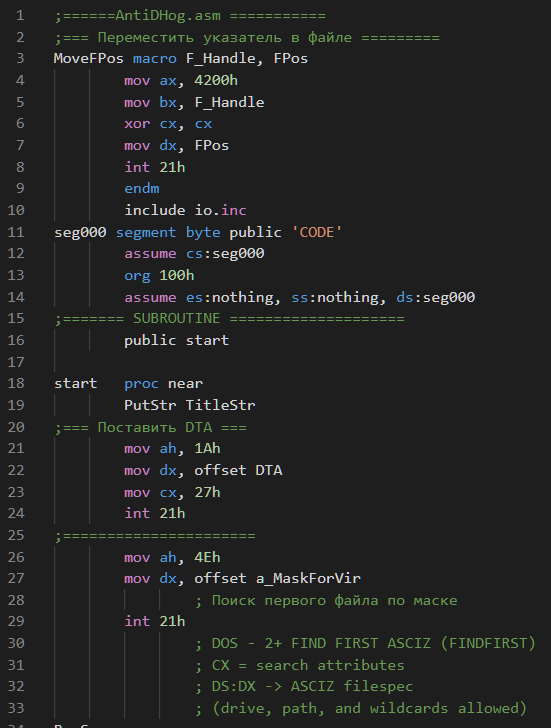
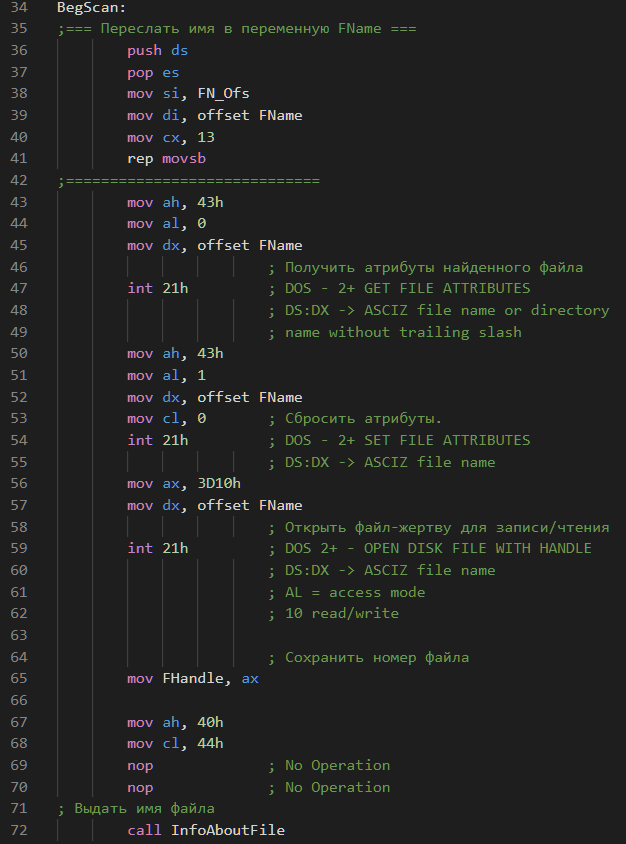
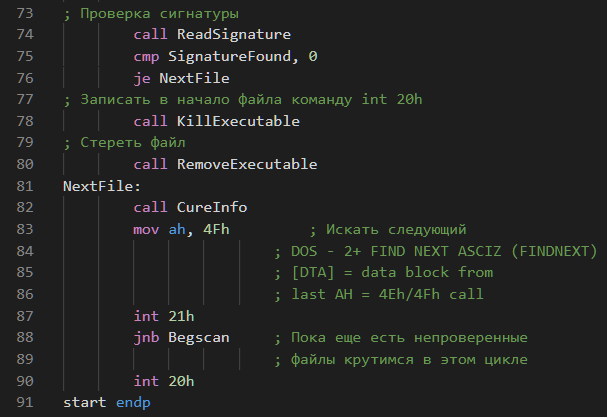
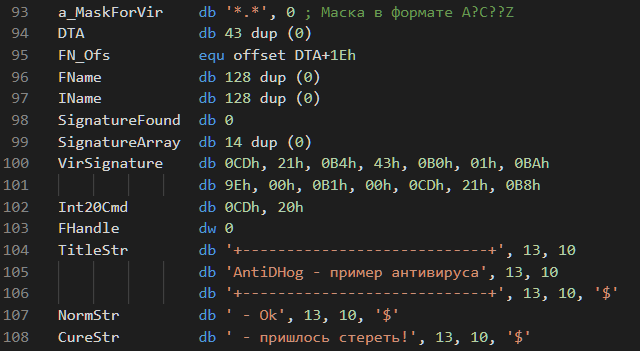
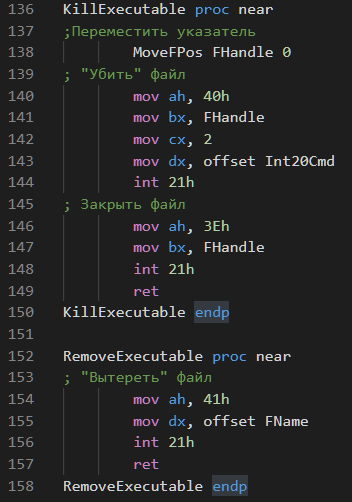
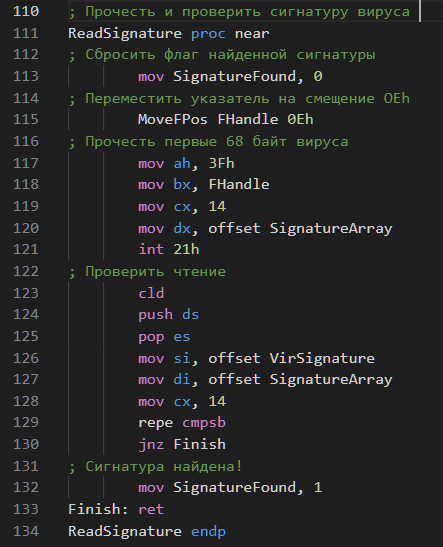


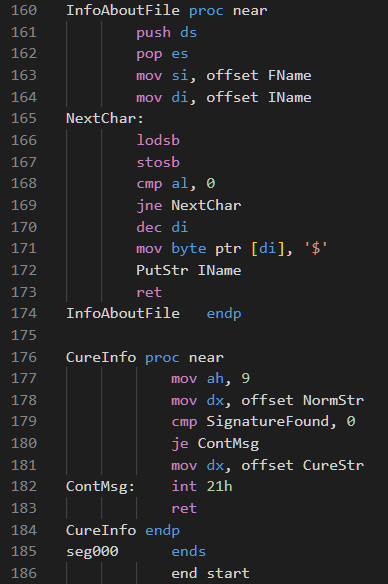
Рисунок - набранный текст на ЯЗА Assembler











2.2. Транслировать, линковать, получить исполнимый модуль в папке HOG (т.е. в папке, где файлы уже превратились в вирусы) (4 балла, отсутствие – минус 4 балла).

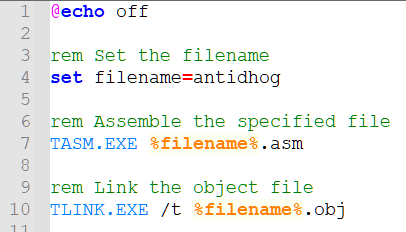


Рисунок - bat скрпит для трансляции и линковки антивируса

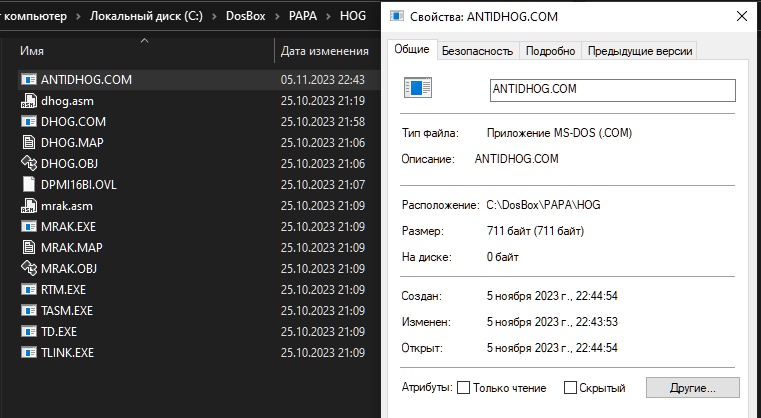


Рисунок - исполняемый модуль антивируса в зараженной папке

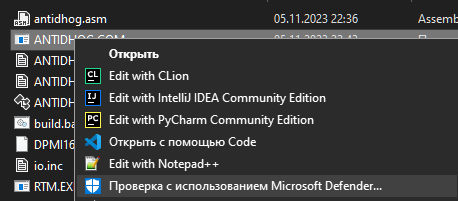
2.3. **Проверить, каким образом НА ПОЯВЛЕНИЕ ЭТОГО ФАЙЛА реагирует Ваша антивирусная защита. Отчёт в виде совокупности скрин-шотов. 16 баллов, отсутствие – минус 8 баллов.**

Рисунок - запуск проверки файла ANTIDHOG.COM антивирусом

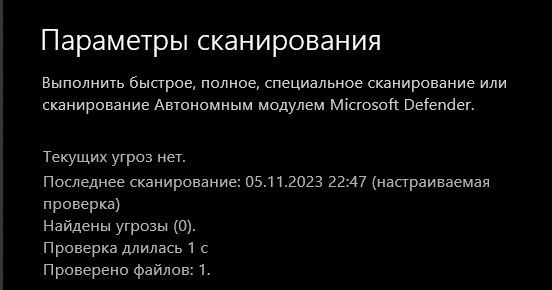


Рисунок - результат проверки файла антивирусом

Антивирус Windows Defender не нашел угроз в файле Antidhog.com

2.4. Показать в шестнадцатеричном виде содержимое файла с бывшим исходным текстом вируса, используя какой-либо текстовый редактор и отладчик – 8 баллов, отсутствие – минус 8 баллов..

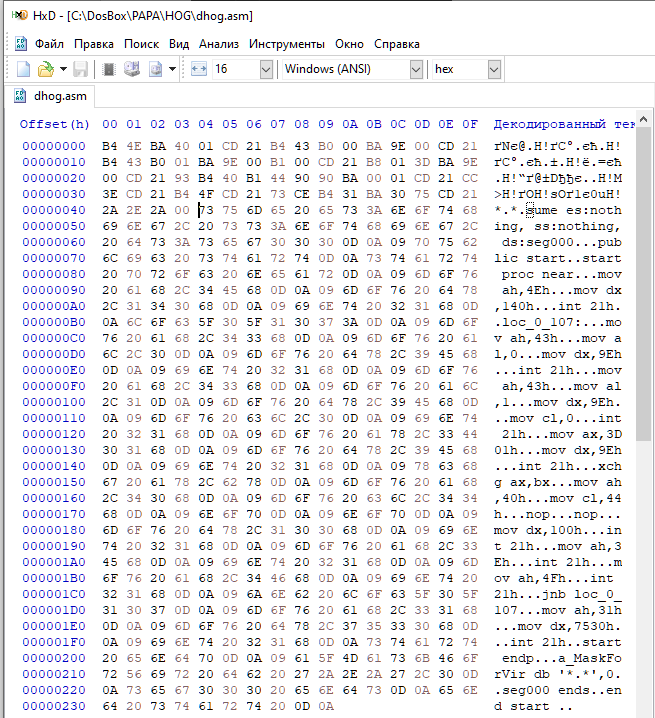


Рисунок - содержиое файла dhog.asm

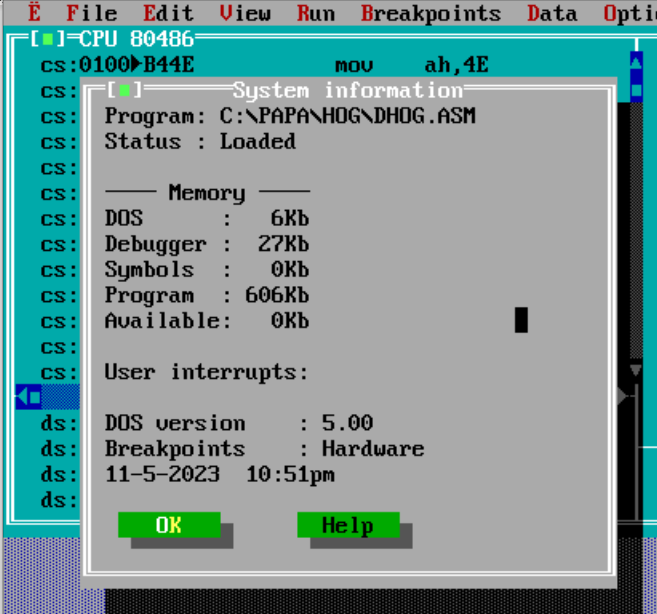


Рисунок - загрузка файла dhog.asm в отладчик

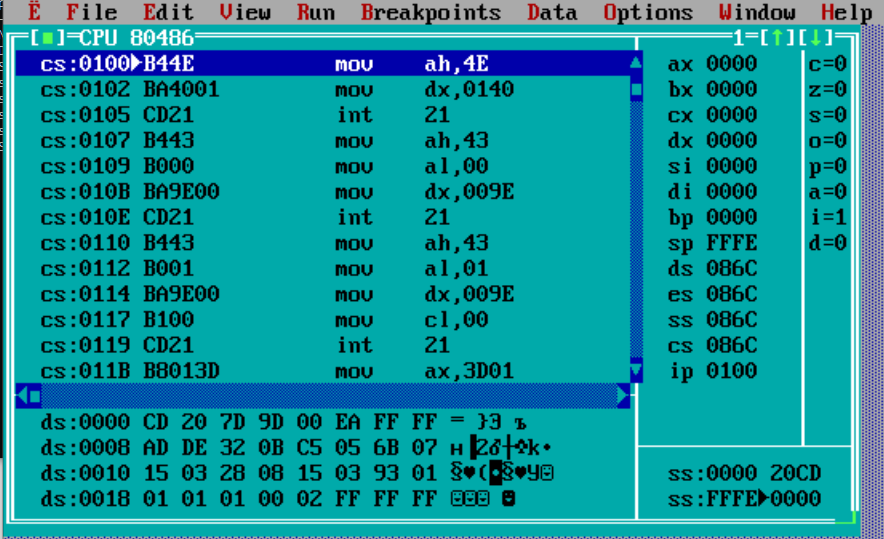


Рисунок - представление файла dhog.asm в отладчике

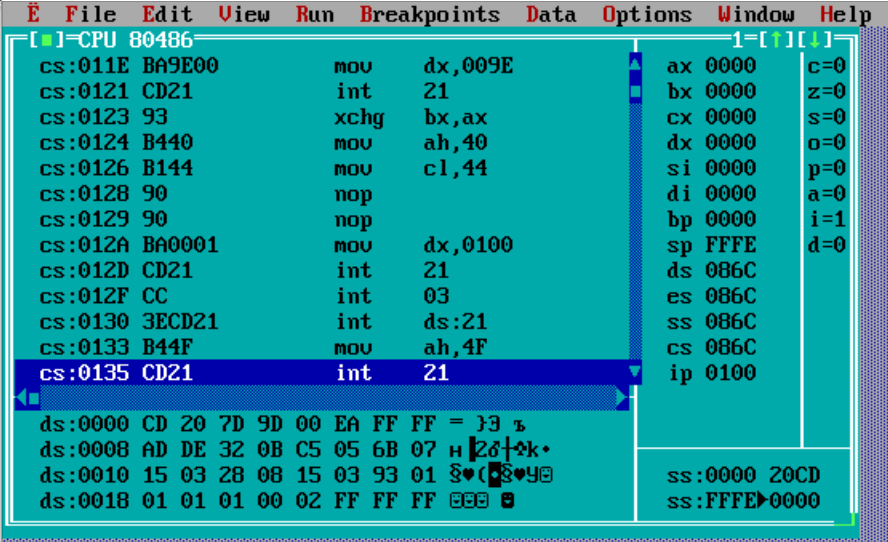


Рисунок - представление файла dhog.asm в отладчике (2)

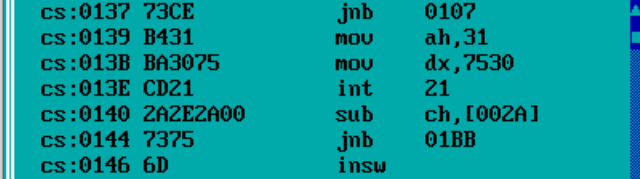


Рисунок - представление файла dhog.asm в отладчике (3)

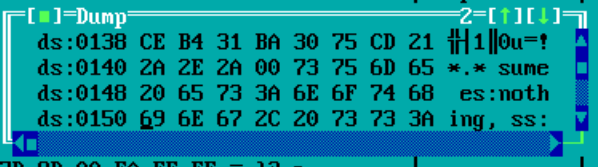


Рисунок - представление файла dhog.asm в отладчике (4)

Как видно из рисунков выше, файл dhog.asm оказался заражен после выполнения вируса dhog.com

2.5. Отладить и протестировать АНТИВИРУСНУЮ ПРОГРАММУ.

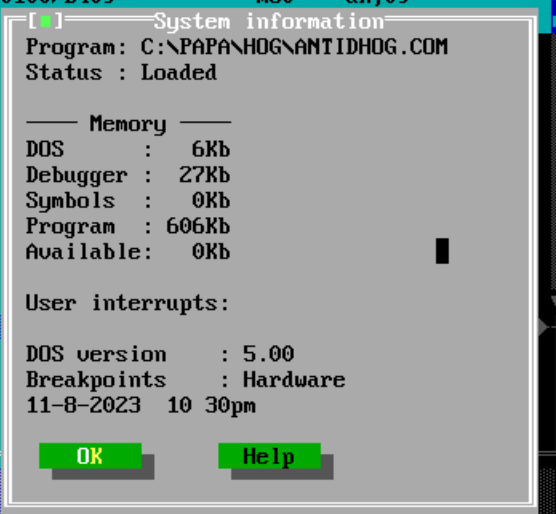


Рисунок - загрузка в отладчик файла антивируса

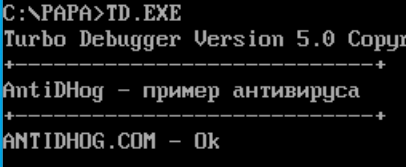


Рисунок - результат проверки антивируса самого себя (первый файл)

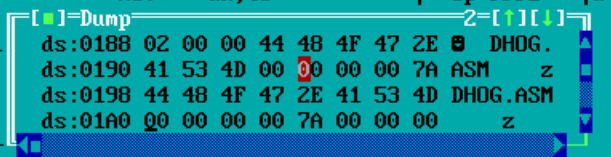


Рисунок - имя следующего файла для проверки

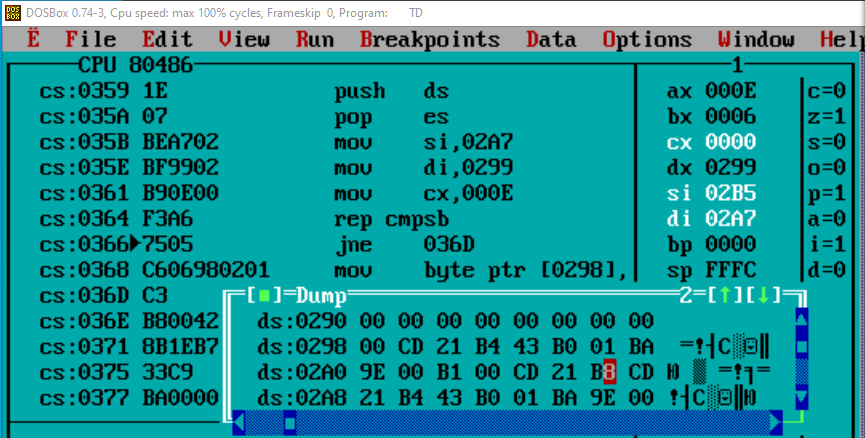


Рисунок - прочитанные 14 байт из проверяемого файла (с адреса ds:0299 по ds:02A6)

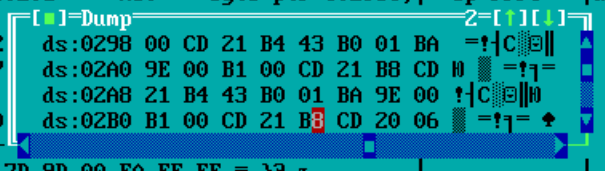


Рисунок - сигнатура вируса, с которой происходит сравнение (с адреса ds:02A7 по ds:02B4)

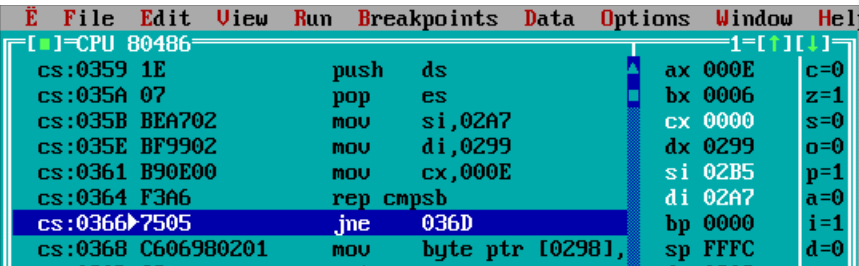


Рисунок - сигнатура найдена

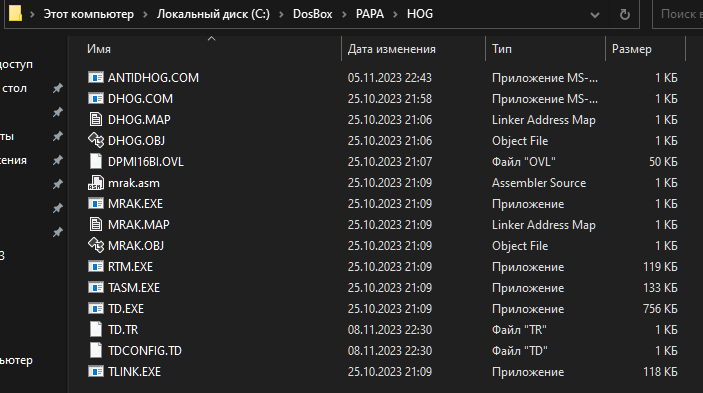


Рисунок - удаление зараженного файла

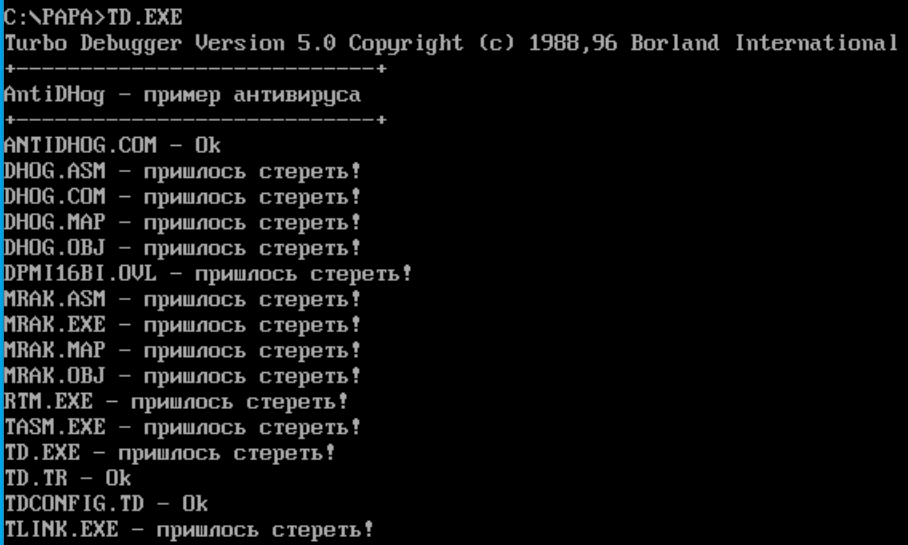


Рисунок - отчет антивируса (файлы TD.TR и TDCONFIG.TD созданы отладчиком после работы вируса и не были заражены)

2.6. **Проверить, действительно ли происходит УДАЛЕНИЕ или УБИЙСТВО всех файлов папки. То есть нужно дать ответ: убивает или удаляет. Для этого с помощью ОТЛАДЧИКА td.exe ПОШАГОВО ВЫПОЛНИТЬ программу, получаемую в результате загрузки в отладчик файла Mrak.asm. Отчёт в виде совокупности скрин-шотов. 16 баллов, отсутствие – минус 8 баллов.**

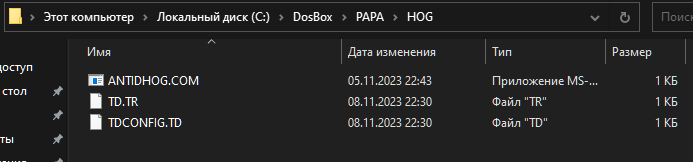
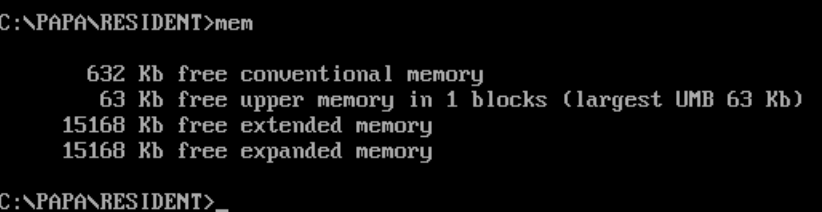


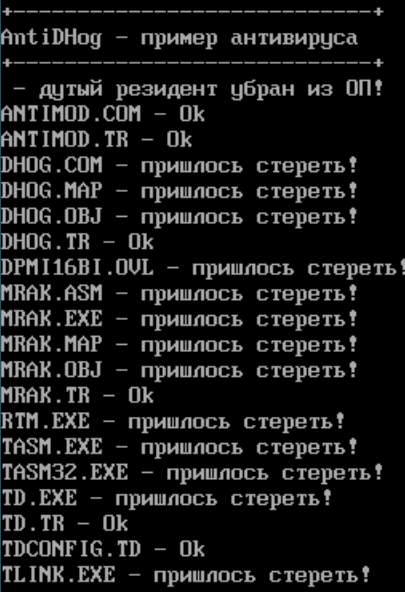
Рисунок 21 - итог работы антивируса

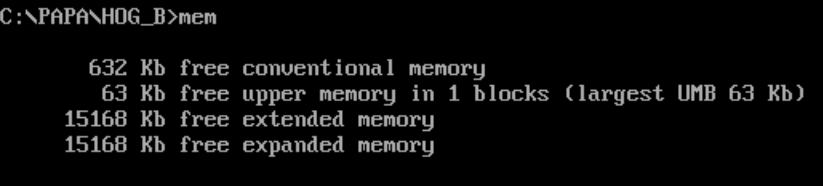
Как видно из рисунка выше, все зараженные файлы в папке HOG были удалены антивирусной программой. Таким образом можно дать ответ, что антивирус производит удаление. Тем самым пошагово выполнить mrak.asm не получится. Однако, если восстановить удаленные файлы из физического представления на жестком диске, то можно будет увидеть, что файлы также были убиты записью команды int 20h в начало файла.

2.7 Получить ПРОГРАММУ-АНТИВИРУС, КОТОРАЯ ИЗНИЧТОЖАЕТ все зараженные файлы в папке HOG И ОСВОБОЖДАЕТ ВСЮ ОПЕРАТИВНУЮ ПАМЯТЬ, ЗАГРАБАСТАННУЮ БОРОВОМ! Помнить при этом, что согласно антивируснику, УДАЛИТЬ значит удалить имя файла из реестра файлов (реально же ТЕЛО исполнимого файла, который при загрузке в оперативную память и передаче ему управления превращается в вирус, ФИЗИЧЕСКИ ПРОДОЛЖАЕТ ЛЕЖАТЬ НА ВИНЧЕСТЕРЕ). УБИТЬ – означает сделать так, чтобы ТЕЛО ПЕРЕСТАЛО ИСПОЛНЯТЬ СВОЙ ФУНКЦИОНАЛ, что в антиыируснике соответствует тому, что ПЕРВОЙ ИСПОЛНЯЕМОЙ КОМАНДОЙ ДЕЛАЕТСЯ КОМАНДА int 20h!! ИЗНИЧТОЖИТЬ ОЗНАЧАЕТ (В ДОПОЛНЕНИЕ К УБИТЬ и УДАЛИТЬ) НА МЕСТО ЗАРАЖЁННОГО ФАЙЛА НА ФИЗИЧЕСКОМ НОСИТЕЛЕ ЗАПИСЫВАЮТСЯ СЛУЧАЙНЫЕ ДАННЫЕ (например, ВСЁ чистится нулями или случайными значениями).

******

******

******

******В результате выполнения модифицированного антивируса удалось освободить оперативную память, занятую дутым резидентом.

2.8. Определить, что произошло с самим исполнимым модулем-антивирусником после обработки им папки HOG, выведя на экран шестнадцатеричное представление этого файла после антивирусника. 8 баллов, отсутствие – минус 8 баллов..

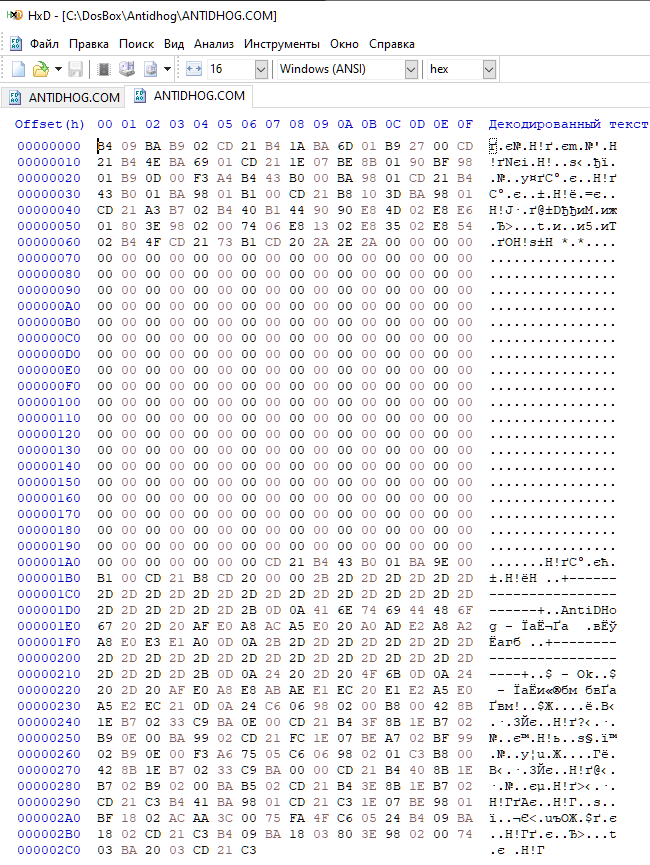


Рисунок - содержимое файла ANTIDHOG.COM до его запуска

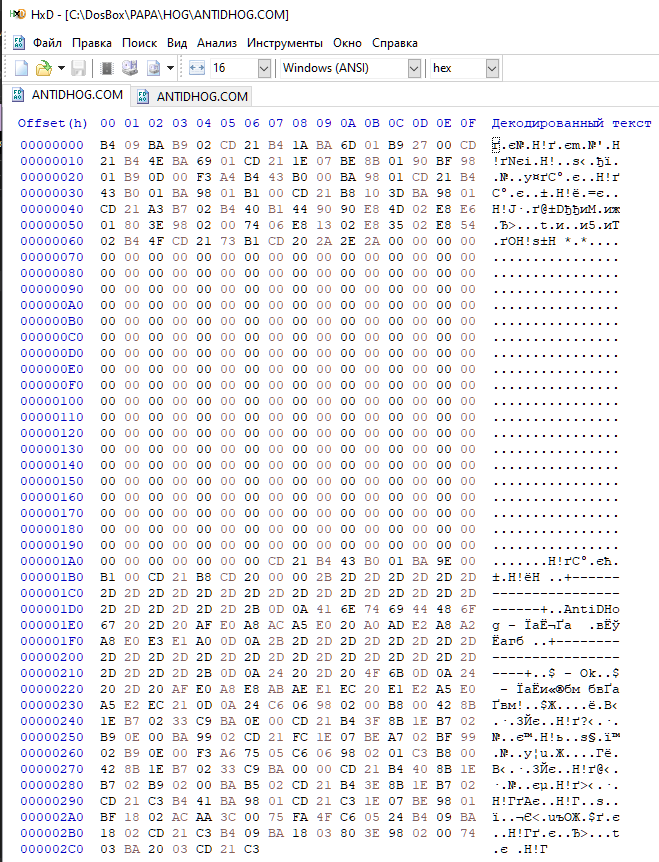


Рисунок - содержимое файла ANTIDHOG.COM после его запуска в папке с зараженными файлами

В результате можно сказать, что файл антивируса никак не изменился. На картинке видно, что файлы до запуска и после идентичны.