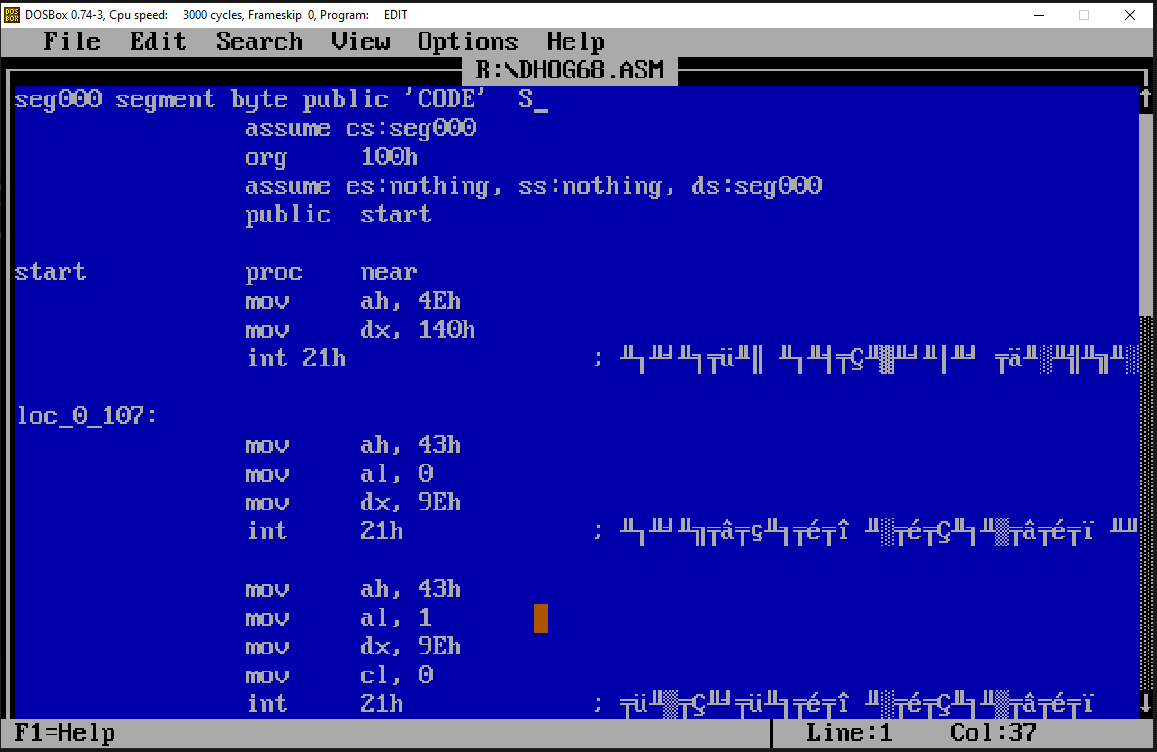
**Лабораторная работа №2.**

**Часть 1.**

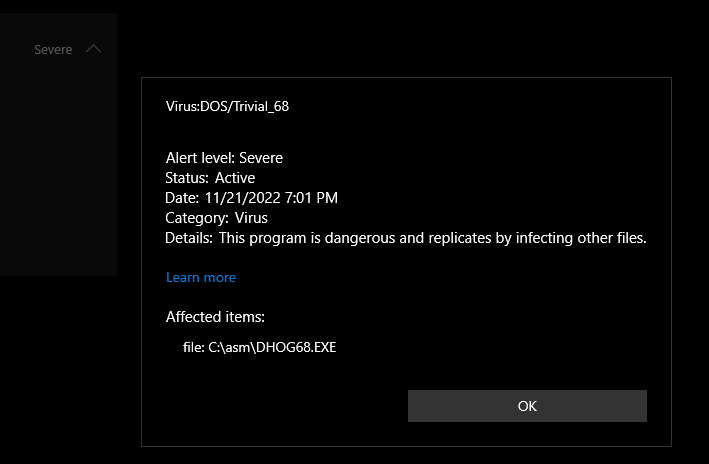
**1.1. Используя оболочку DosBox, книгу про ассемблер, набрать исходный текст ВИРУСА DHog68, транслировать, линковать, получить com-файл, и исполнить его для какой-либо папки!!! Проверить, действительно ли происходит заражение всех файлов папки. Скопировать зараженный файл в другую папку и «запустить» его.**

Переписал исходный текст ВИРУСА GHog68

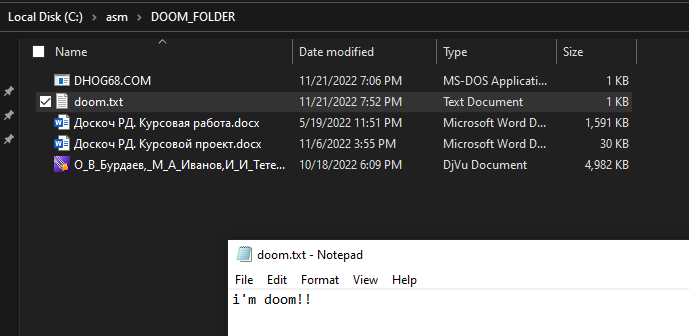


**1.2. Проверить, каким образом НА ПОЯВЛЕНИЕ ЭТОГО ФАЙЛА.com реагирует Ваша антивирусная защита (если пока её нет – установить любой бесплатный антивирусник).**

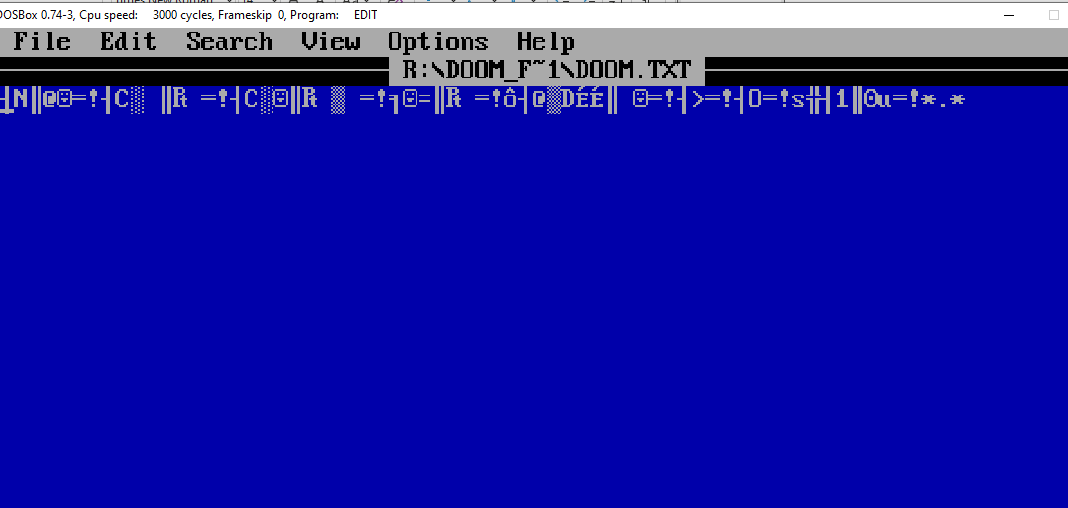
Реакция системы на попытку скомпилировать файл DHOG68.OBJ

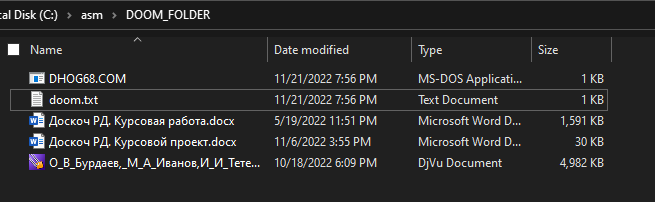


Содержимое папки DOOM\_FOLDER

****

После запуска

****



В данной папке все файлы кроме типа .docx и .djvu записались как 68 битами

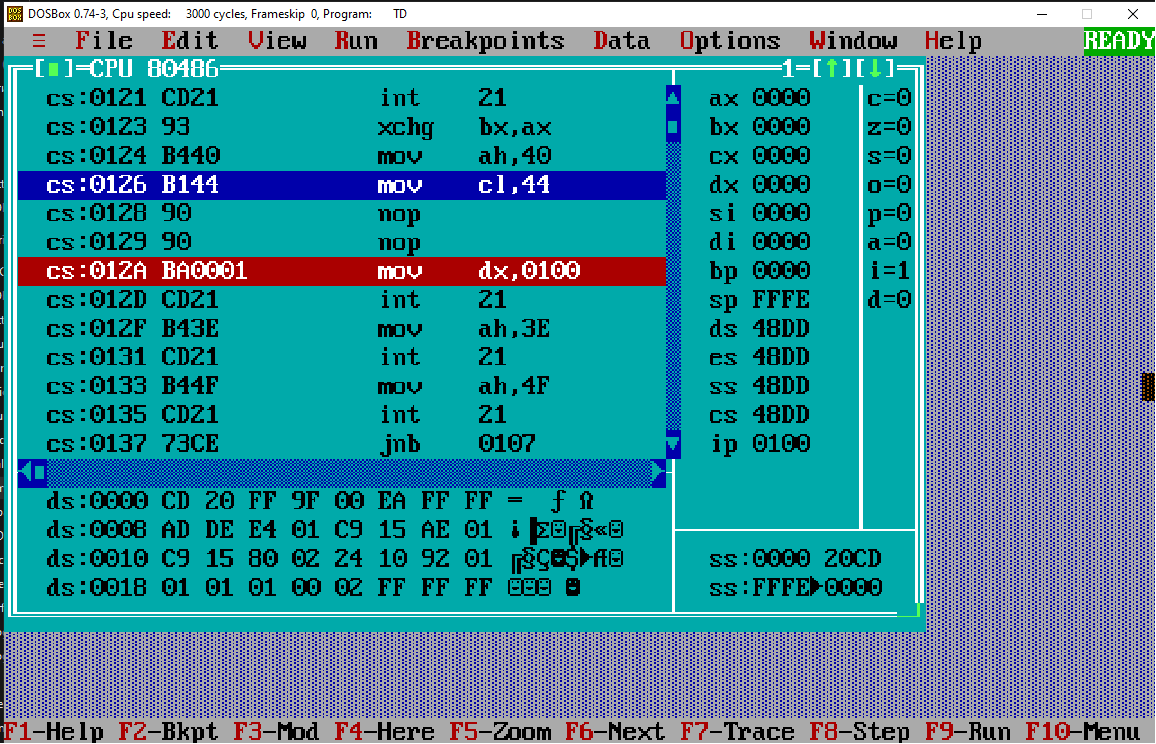
Можно сделать вывод что вирус записывает 68 байтов только в файлы формата txt

**Лабораторная работа №2.**

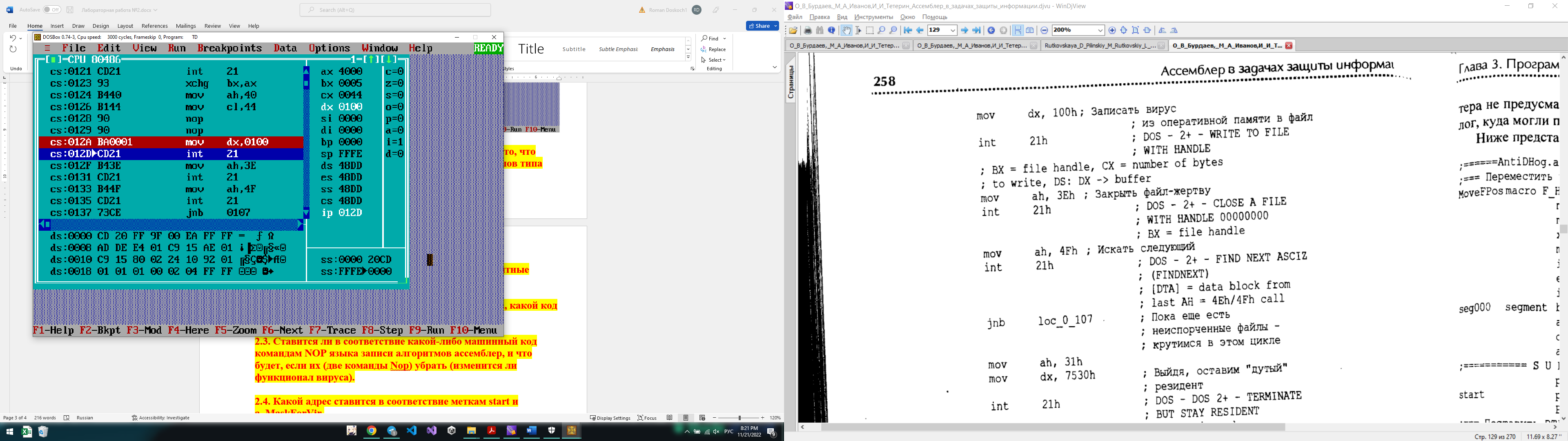
**Часть 2.**

**Используя оболочку DosBox и программное средство TurboDebugger (td.exe) исследовать полученный вирус:**

Поставил точку останова

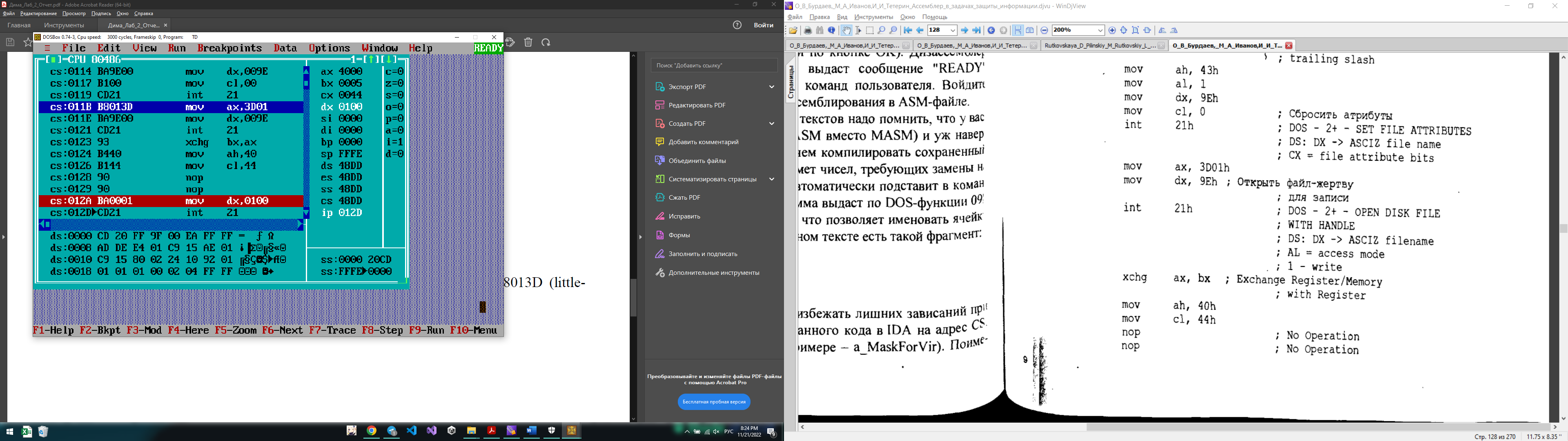


**2.1. Определить соответствует ли действительности то, что было сказано о загрузке в оперативную память файлов типа .com, а именно: какие значения получают все сегментные регистры.**



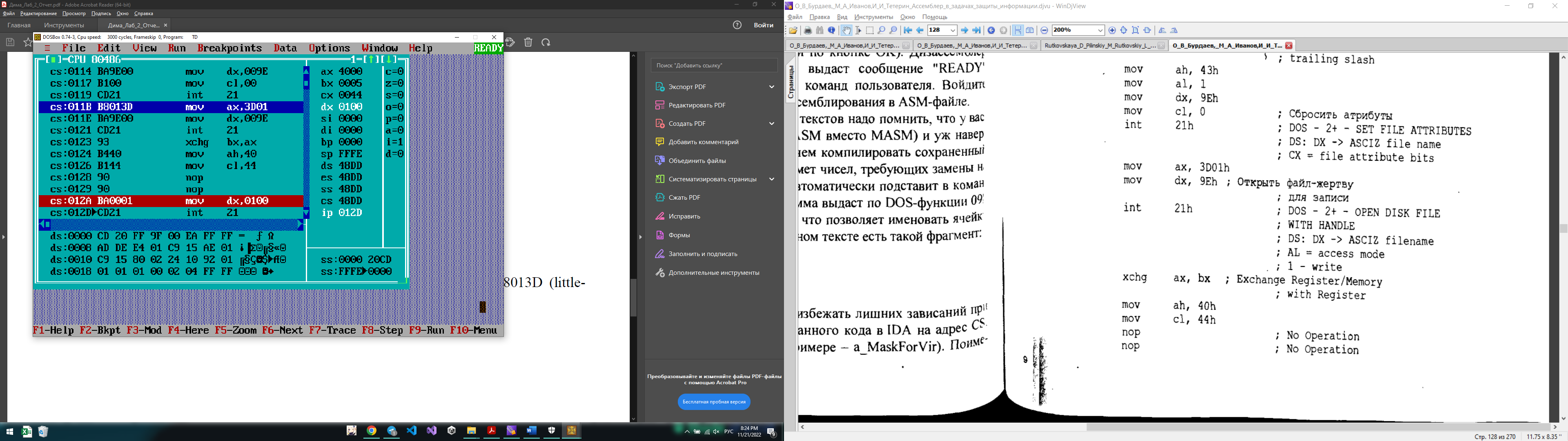
Все они имеют одинаковые значения, так как при запуске COM-файлов все они указывают на PSP.

**2.2. Показать, какая длина у команды mov ax,3D01h, какой код операции у этой команды.**



Команда mov ax, 3D01 имеет код B8013D, и, соответственно занимает 3 байта.

**2.3. Ставится ли в соответствие какой-либо машинный код командам NOP языка записи алгоритмов ассемблер, и что будет, если их (две команды Nop) убрать (изменится ли функционал вируса).**



Команде nop ставится в соответствие код 90. При их удалении функционал вируса изменится.

**2.4. Какой адрес ставится в соответствие меткам start и a\_MaskForVir,**

Метке start ставится в соответствие адрес cs:0100, так как она указывает на первую команду программы.

Метке a\_MaskForVir (указывающая на значение «\*.\*») ставится в соответствие адрес ds:0140

**2.5. ОСУЩЕСТВИТЬ ПОШАГОВОЕ ИСПОЛНЕНИЕ программы-вируса, отразив в отчете как меняется содержимое регистра AX.**

Отследим с помощью отладчика изменение значения регистра АX в ходе выполнения программы:

Шаг 0:  ax = 0000 mov ah, 4Eh

Шаг 1: ax = 4E00 mov dx, 140h

Шаг 3: ax = 0000 int 21h

Шаг 4: ax = 4300 mov ah, 43h

Шаг 7: ax = 0020 int 21h

Шаг 8: ax = 4320 mov ah, 43h

Шаг 9: ax = 4301 mov al, 1

Шаг 12 : ax = 0202 int 21h

Шаг 13: ax = 3D01 mov ax, 3D01h

Шаг 15: ax = 0005 mov dx, 9Eh

Шаг 16: ax = 0000 xchg ax, bx

Шаг 17: ax = 4000 mov ah, 40h

Шаг 22: ax = 0044 int 21h

Шаг 23: ax = 3E44 mov ah, 3Eh

Шаг 25: ax = 4F44 mov ah, 4Fh

Шаг 26: ax = 0012 int 21h

Шаг 28: ax = 3112 mov ah, 31h

Шаг 30: ax = 0192 int 21h