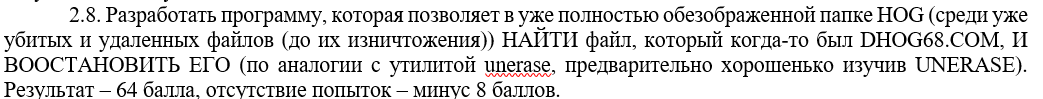
Лабораторная работа №2 часть 2

Антивирус

**Задание**



**Ход решения**

Давайте сначала почитаем про утилиту unerase, найдём её исполнимый файл.

Увы, в чудо-книге я найти ничего не смогла, поэтому полезем на помойку.

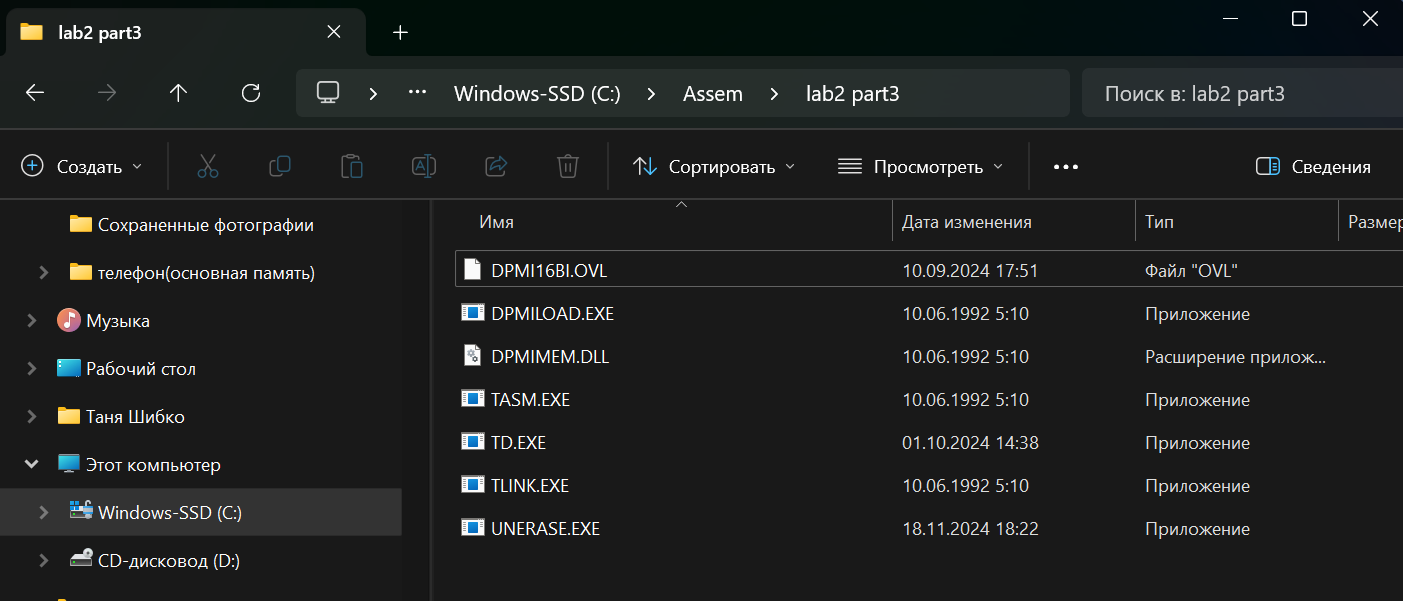
Если кратко:

unerase — это утилита для восстановления удалённых файлов с дисков, использующих файловые системы FAT и NTFS. Она сканирует диск на наличие удалённых данных и позволяет пользователю восстанавливать файлы, которые ещё не были перезаписаны.

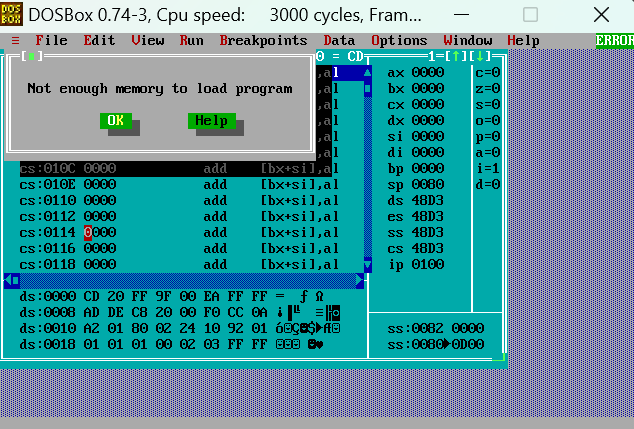
Основные функции:

* Восстановление файлов: Находит и восстанавливает удалённые файлы.
* Поддержка файловых систем: Работает с FAT и NTFS.
* Командная строка: Управление через интерфейс командной строки.
* Поиск по атрибутам: Позволяет искать файлы по имени, размеру и дате.

В папку с лабораторной я уже положила необходимые (наверное) TASM, TLINK, TD и новую утилиту UNERASE.



Давайте попробуем запустить эту утилиту через отладчик.



Ну, значит, не запустим. Будем верить помойке. Другого выбора у нас всё равно нет.

Попробуем написать свою программу:

.model tiny

.stack 100h

.data

msg db 'Searching for HOG.COM in HOG...$'

found\_msg db 'File HOG.COM found! Restoring...$'

not\_found\_msg db 'File HOG.COM not found.$'

filename db 'HOG\HOG.COM', 0

backup\_filename db 'HOG\HOG\_RESTORED.COM', 0

buffer db 512 dup(0)

file\_found db 0

.code

start:

mov ax, @data

mov ds, ax

mov ah, 09h

lea dx, msg

int 21h

call find\_file

cmp file\_found, 0

je file\_not\_found

mov ah, 09h

lea dx, found\_msg

int 21h

call restore\_file

jmp exit\_program

file\_not\_found:

mov ah, 09h

lea dx, not\_found\_msg

int 21h

exit\_program:

mov ax, 4C00h

int 21h

find\_file:

mov ah, 4Eh

lea dx, filename

int 21h

jc file\_not\_found

mov file\_found, 1

ret

restore\_file:

mov ah, 3Dh

mov al, 0

lea dx, filename

int 21h

jc file\_not\_found

mov bx, ax

mov ah, 3Ch

lea dx, backup\_filename

int 21h

jc file\_not\_found

mov di, ax

read\_loop:

mov ah, 3Fh

lea dx, buffer

mov cx, 512

int 21h

jc done

mov ah, 40h

mov cx, ax

lea dx, buffer

int 21h

jmp read\_loop

done:

mov ah, 3Eh

int 21h

mov ah, 3Eh

int 21h

ret

end start

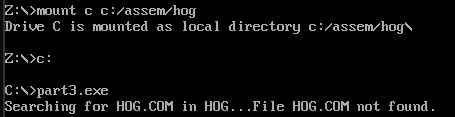
Соберём исполнимый файл:



Результат:



Попробовала переключиться на папку HOG



Видимо, я и УБИЛА, и УДАЛИЛА, и ИЗНЕЧТОЖИЛА файл, поэтому программа не смогла найти. Ну или я плохо старалась.

В любом случае, попытка – не пытка.