Санкт-Петербургский Национальный Исследовательский Университет

Информационных Технологий, Механики и Оптики

ФКТиУ

Лабораторная работа №1

по дисциплине

«Информационная безопасность»

Выполнил: Студент группы P34113

Мансуров Бехруз

Преподаватель:Оголюк А.А.

2021г.

Описание:

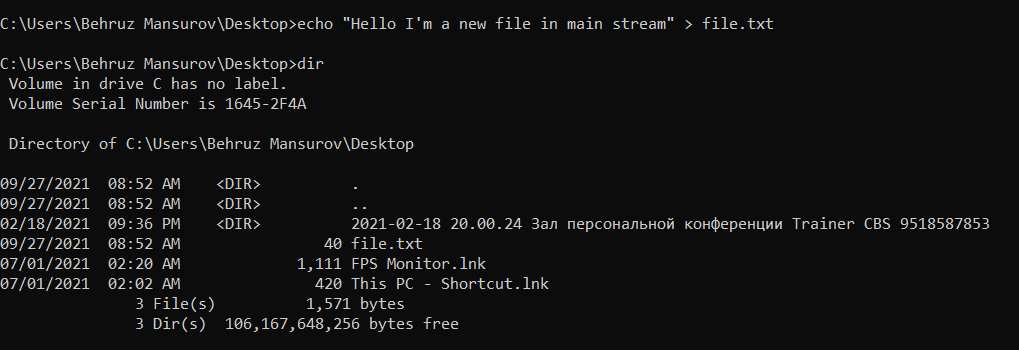
Дополнительные потоки данных в файлах NTFS.

* На томе NTFS создать файл (file.txt)
* Выполнить команду “dir > file.txt:hidden.txt”
* Вывести содержимое созданного потока на экран “more < file.txt:hidden.txt”, открыть в notepad “file.txt:hidden.txt”

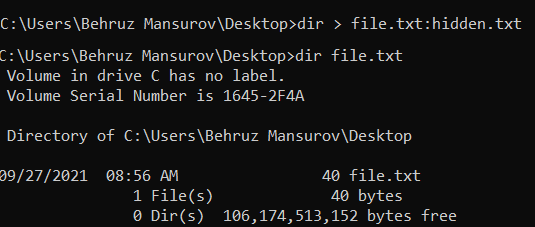
Задание:

1. Сравнить размер файла до и после создания новых потоков
   1. Сравнить свободное место на лог. диске до и после.
   2. Выводя в поток данных (известного размера) и сравнивая остаток свободного места на лог. диске построить зависимость свободного места от размера записанных данных.
2. Вывести содержание потока file.txt:hidden.txt в другой файл (test.txt)
3. Посмотреть как работают другие команды cmd.exe/command.com с потоками
4. Посмотреть как работают другие программы с потоками

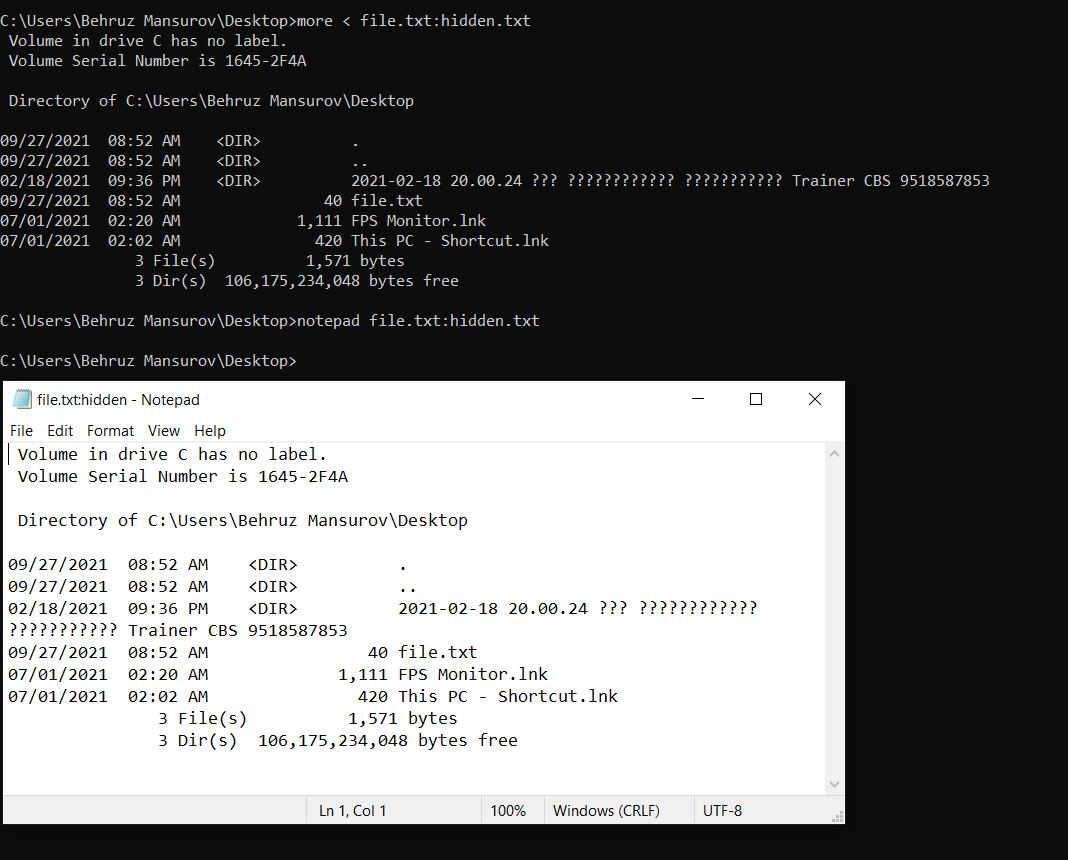
Выполнение:



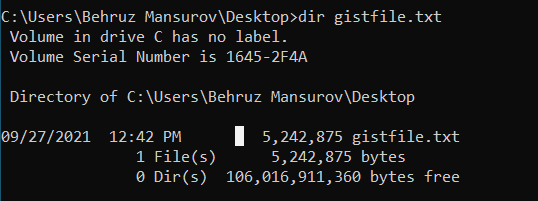
Создаем файл и пишем в нем строку и смотрим на размер файла. Размер изменился.



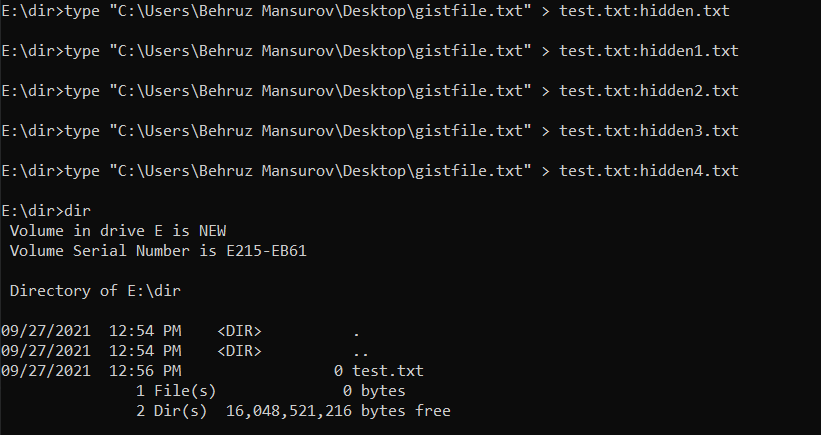
После создание альтернативного потока и перенаправления вывода команды dir видим что размер файла не изменилось и можно сделать вывод что команда dir не показывает размер альтернативного потока.



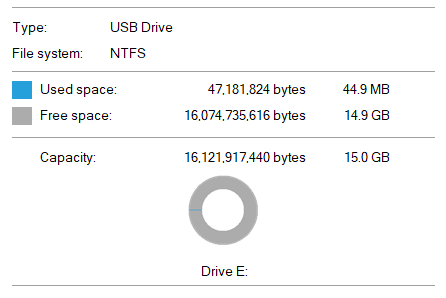
Вывод содержимого альтернативного потока на консоль и в notepad-е.



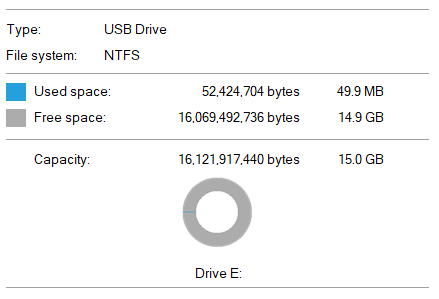
А теперь в новый логический диск E будем создавать файл и скопировать файл размером 5 мб.



Как видно из рисунка размер файла после 5 раз записи в альтернативные потоки не изменилось но размер директории изменилось.



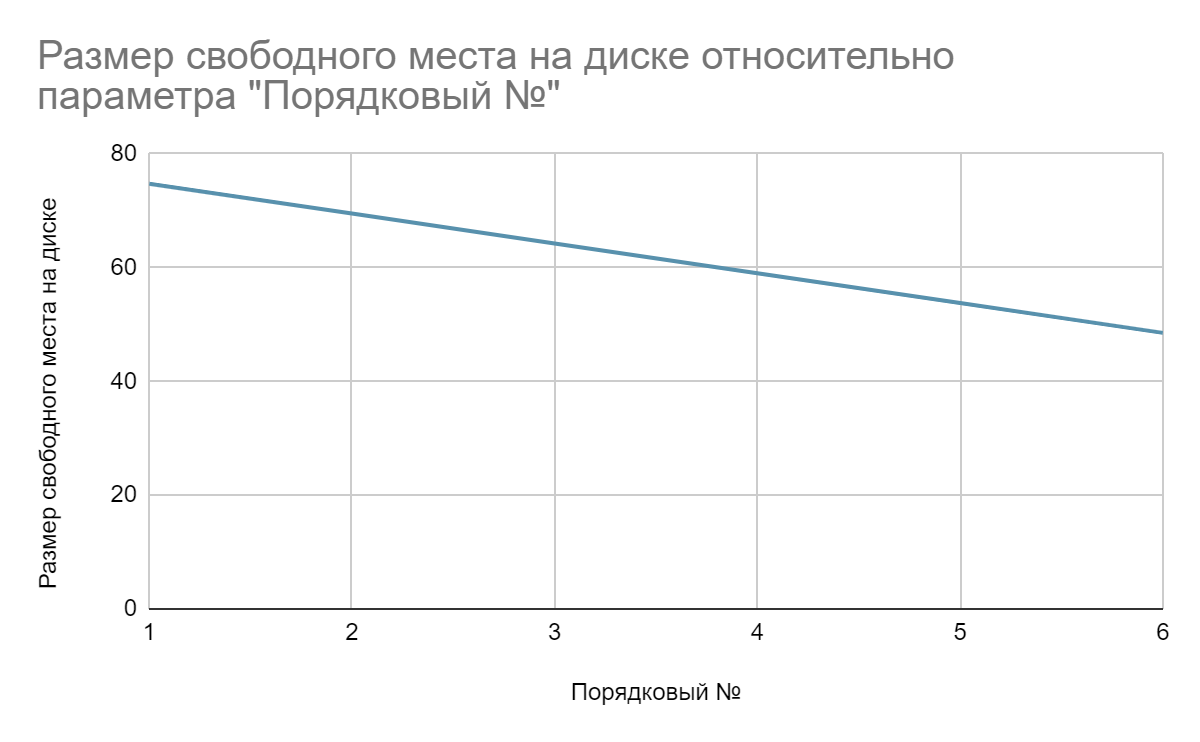
До записи в альтернативный поток.

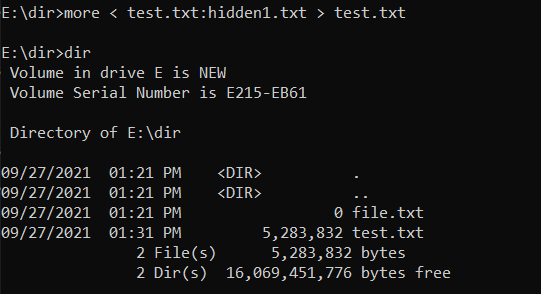


После записи в альтернативный поток.

Как видно из рисунка размер лог. диска изменилось после записи в альтернативный поток.

| Порядковый № | 1 | 2 | 3 | 4 | 5 | 6 |
| --- | --- | --- | --- | --- | --- | --- |
| Размер свободного места на диске | 74,735616 | 69,492736 | 64,249856 | 59,006976 | 53,764096 | 48,521216 |





Чтобы скопировать содержимое альтернативного потока можно использовать команду “more < text.txt:hidden1.txt > test.txt” не знаю насколько это правильно но это работает.

Вывод:

Можно сделать вывод что ADS это очень полезная вещь в плане компактности и минимализма. И еще хорошая вещь чтобы скрыть данные от посторонних глаз (работает только на людей которые не понимают ничего в компьютерной науке). И минус в том что во время скачивания из интернета можно подхватить и вредоносное ПО в качестве ADS к файлу.

В ходе выполнения лабораторной работы вспомнил как работать с командной строкой Windows и освежил свои знания о файловой системе NTFS.