

Санкт-Петербургский Национальный Исследовательский Университет
Информационных Технологий, Механики и Оптики
ФКТиУ

Лабораторная работа №1
по дисциплине
«Информационная безопасность»

Выполнил: Студент группы Р34113
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
 - 1.1. Сравнить свободное место на лог. диске до и после.
 - 1.2. 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:

```
C:\Users\Behruz Mansurov\Desktop>echo "Hello I'm a new file in main stream" > file.txt

C:\Users\Behruz Mansurov\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 1645-2F4A

Directory of C:\Users\Behruz Mansurov\Desktop

09/27/2021  08:52 AM    <DIR>          .
09/27/2021  08:52 AM    <DIR>          ..
02/18/2021  09:36 PM    <DIR>          2021-02-18 20.00.24 Зал персональной конференции Trainer CBS 9518587853
09/27/2021  08:52 AM                40 file.txt
07/01/2021  02:20 AM             1,111 FPS Monitor.lnk
07/01/2021  02:02 AM             420 This PC - Shortcut.lnk
               3 File(s)              1,571 bytes
               3 Dir(s) 106,167,648,256 bytes free
```

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

```
C:\Users\Behruz Mansurov\Desktop>dir > file.txt:hidden.txt

C:\Users\Behruz Mansurov\Desktop>dir file.txt
Volume in drive C has no label.
Volume Serial Number is 1645-2F4A

Directory of C:\Users\Behruz Mansurov\Desktop

09/27/2021  08:56 AM                40 file.txt
               1 File(s)              40 bytes
               0 Dir(s) 106,174,513,152 bytes free
```

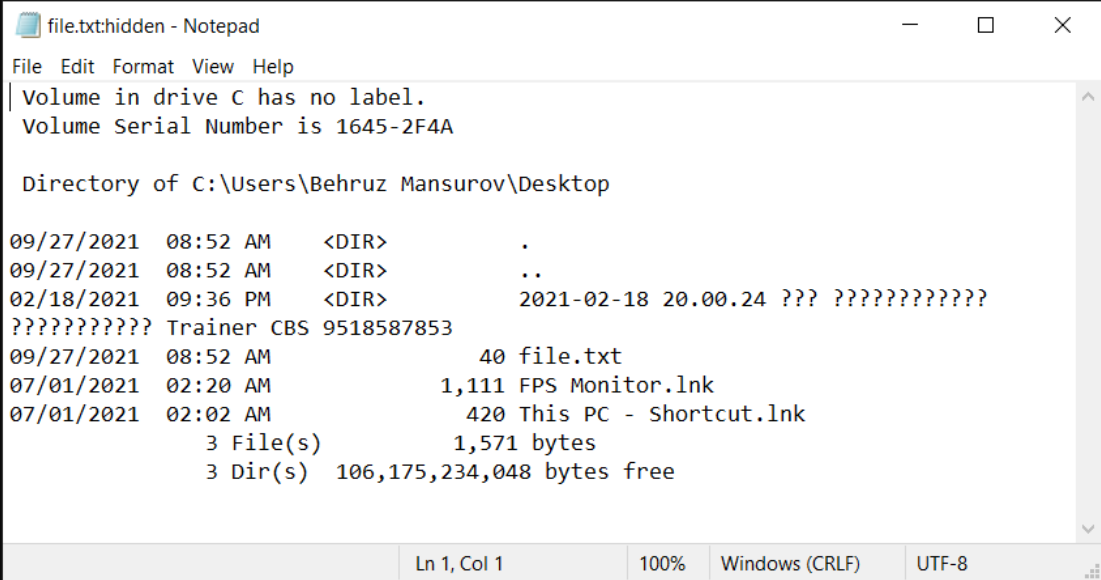
После создание альтернативного потока и перенаправления вывода команды dir видим что размер файла не изменилось и можно сделать вывод что команда dir не показывает размер альтернативного потока.

```
C:\Users\Behruz Mansurov\Desktop>more < file.txt:hidden.txt
Volume in drive C has no label.
Volume Serial Number is 1645-2F4A

Directory of C:\Users\Behruz Mansurov\Desktop

09/27/2021  08:52 AM    <DIR>          .
09/27/2021  08:52 AM    <DIR>          ..
02/18/2021  09:36 PM    <DIR>          2021-02-18 20.00.24 ??? ???????????? ???????????? Trainer CBS 9518587853
09/27/2021  08:52 AM                40 file.txt
07/01/2021  02:20 AM            1,111 FPS Monitor.lnk
07/01/2021  02:02 AM            420 This PC - Shortcut.lnk
               3 File(s)              1,571 bytes
               3 Dir(s) 106,175,234,048 bytes free

C:\Users\Behruz Mansurov\Desktop>notepad file.txt:hidden.txt
C:\Users\Behruz Mansurov\Desktop>
```



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

```
C:\Users\Behruz Mansurov\Desktop>dir gistfile.txt
Volume in drive C has no label.
Volume Serial Number is 1645-2F4A

Directory of C:\Users\Behruz Mansurov\Desktop

09/27/2021  12:42 PM    5,242,875 gistfile.txt
               1 File(s)      5,242,875 bytes
               0 Dir(s) 106,016,911,360 bytes free
```

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

```

E:\dir>type "C:\Users\Behruz Mansurov\Desktop\gistfile.txt" > test.txt:hidden.txt
E:\dir>type "C:\Users\Behruz Mansurov\Desktop\gistfile.txt" > test.txt:hidden1.txt
E:\dir>type "C:\Users\Behruz Mansurov\Desktop\gistfile.txt" > test.txt:hidden2.txt
E:\dir>type "C:\Users\Behruz Mansurov\Desktop\gistfile.txt" > test.txt:hidden3.txt
E:\dir>type "C:\Users\Behruz Mansurov\Desktop\gistfile.txt" > test.txt:hidden4.txt

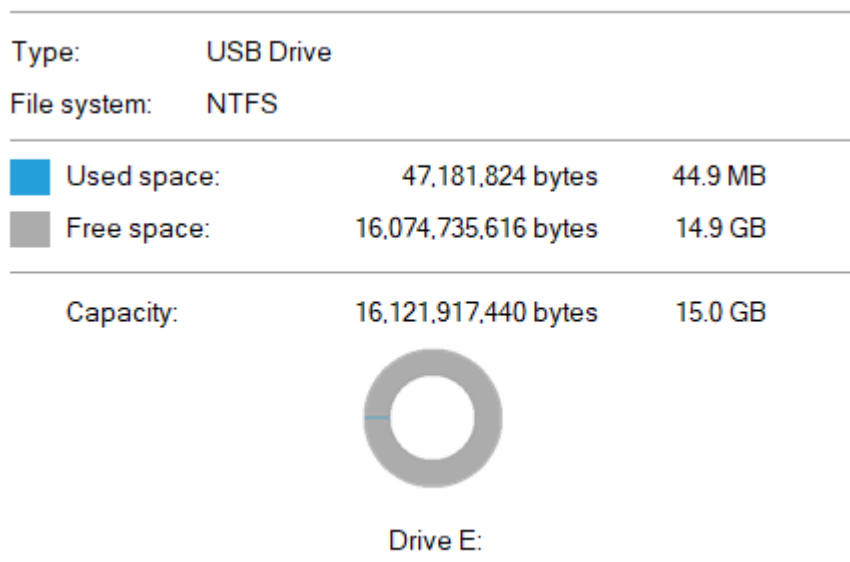
E:\dir>dir
Volume in drive E is NEW
Volume Serial Number is E215-EB61

Directory of E:\dir

09/27/2021  12:54 PM    <DIR>          .
09/27/2021  12:54 PM    <DIR>          ..
09/27/2021  12:56 PM                0 test.txt
                1 File(s)                0 bytes
                2 Dir(s)  16,048,521,216 bytes free

```

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



До записи в альтернативный поток.

Type:USB Drive

File system:NTFS

Used space:

52,424,704 bytes

49.9 MB

Free space:

16,069,492,736 bytes

14.9 GB

Capacity:

16,121,917,440 bytes

15.0 GB

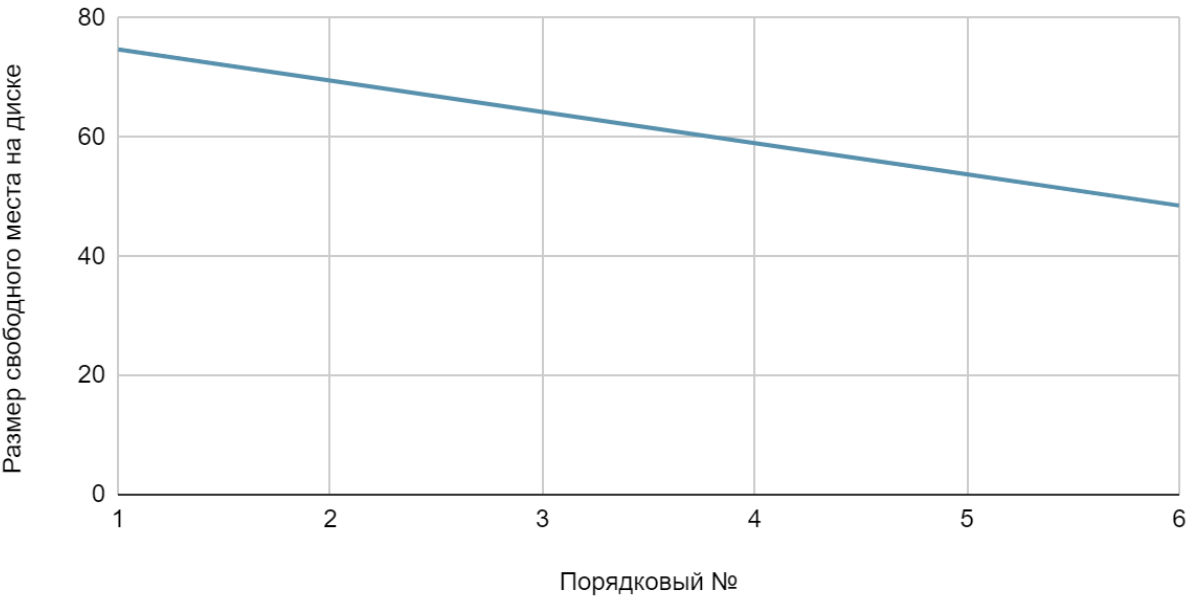
Drive E:

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

Размер свободного места на диске относительно параметра "Порядковый №"



```
E:\dir>more < test.txt:hidden1.txt > test.txt

E:\dir>dir
Volume in drive E is NEW
Volume Serial Number is E215-EB61

Directory of E:\dir

09/27/2021  01:21 PM    <DIR>          .
09/27/2021  01:21 PM    <DIR>          ..
09/27/2021  01:21 PM                0 file.txt
09/27/2021  01:31 PM          5,283,832 test.txt
               2 File(s)          5,283,832 bytes
               2 Dir(s)  16,069,451,776 bytes free
```

Чтобы скопировать содержимое альтернативного потока можно использовать команду "more < test.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.