Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики

Лабораторная работа №1
Дисциплина «Информационная безопасность»

Выполнили:
Баев Дмитрий Владимирович
Съестов Дмитрий Вячеславович
Группа P3417

Преподаватель:
Оголюк Александр Александрович

Санкт-Петербург
2019

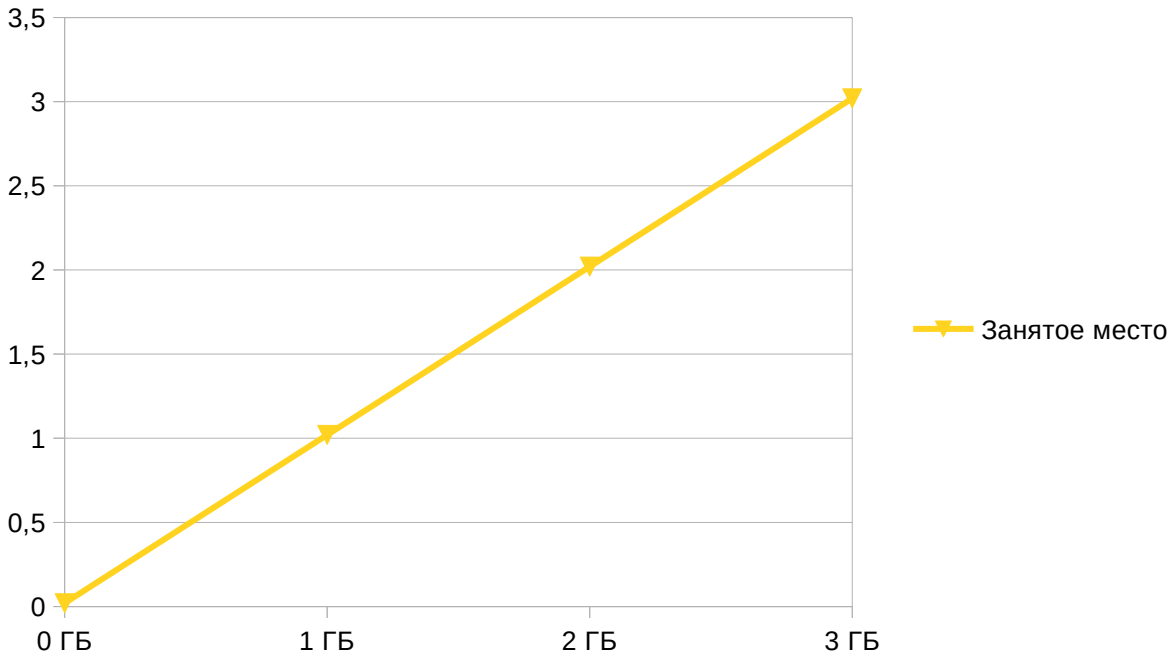
1.0. Сравнить размер файла до и после создания новых потоков.
Для просмотра размера файла с учётом АПД используется команда dir /r, недоступная в Windows XP. При просмотре свойств файла размер отображается без учёта АПД.

1.1. Сравнить свободное место на логич. диске до и после (лучше использовать достаточно большие файлы)
Мы выполнили следующую команду для создания файла размером в гигабайт:
```
fsutil file createnew bigfile.txt 1073741824
```

После этого на диске оставалось 5.62 ГБ свободного места. Затем мы записали содержимое этого файла в АПД другого файла:
```
type bigfile.txt > smallfile.txt:aaa.txt
```

Теперь на диске остаётся 4.62 ГБ, из чего можно сделать вывод, что АПД не увеличивают размер хранимых данных.

1.2. Выводя в поток данные (известного размера) и сравнивая остаток свободного места на лог. диске (использовать отличный от системного диск) построить зависимость свободного места от размера записанных данных. (в байтах)
На графике представлена зависимость занятого места на диске от объёма данных, записанных в АПД файла.



2.0. Вывести содержание потока test.txt:aaa.txt в другой файл (testdir.txt)

```
 Том в устройстве C не имеет метки.
 Серийный номер тома: 0845-1749

 Содержимое папки C:\Documents and Settings\dmitry\Рабочий стол

16.03.2020  00:46    <DIR>          .
16.03.2020  00:46    <DIR>          ..
01.03.2020  03:11             2 764 LAB1.txt
16.03.2020  00:45            93 795 lipsum.txt
01.03.2020  14:26               738 Notepad++.lnk
16.03.2020  00:45            93 795 test.txt
16.03.2020  00:43               509 testdir.txt
               5 файлов        191 601 байт
               2 папок   7 120 846 848 байт свободно
```

3.0. Посмотреть как работают другие комнды cmd.exe/command.com с потоками (например: type, echo, etc.)

- echo может выводить текст в потоки.
- cat также поддерживает ввод и вывод из потоков
- type не может вывести текст потока. Вместо него можно использовать more.
- dir, del и copy не работают на потоках.

4.0. Посмотреть как работают другие программы с потоками (notepad/hiew/word/etc.)

- notepad открывает поток как файл
- hiew открывает поток для просмотра
- Word считывает данные из альтернативных потоков (например Zone.Identifier, который создается при скачивании файла из сети) для определения потенциальной опасности файла.

Дополнительно (необязательное):

1. Предложить способ хранения и извлечения бинарных (исполняемых) файлов в дополнительных потоках файлов.
При этом подразумевается использования стандартных средств (входящих в дистриб. ОС Windows 2000/XP)

В Windows 2000 существует несколько способов запустить исполняемый код (бинарный или скрипт на Visual Basic), хранящийся в дополнительных потоках исполняемого файла:
1. Открыть файл из меню запуска (Win+R): `file:\\file.exe:stream_name`
2. Если в потоке хранится скрипт на Visual Basic, его можно запустить с помощью wscript
3. Можно создать ярлык, указывающий на поток. Также этот ярлык можно поместить в папку автозапуска, чтобы выполнять код при входе в систему
4. Можно добавить запись со значением `file.exe stream_name` в директорию реестра `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` для выполнения потоков при загрузке системы

3. Выяснить совпадают ли разграничения доступа к файлу с разграничениями доступа к потоку.

Разрешения доступа относятся ко всему файлу, а не к отдельным потокам. Таким образом, если файл доступен только для чтения, то в потоки писать нельзя.