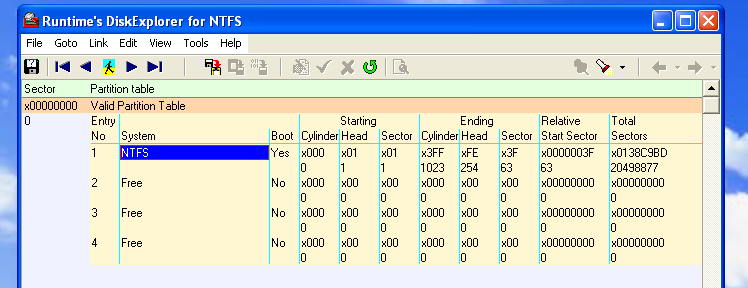
## Исследование значимых областей следообразования ФС NTFS

**Исследование раздела жесткого диска** ( инструмент -RT NTFS Explorer)**.**

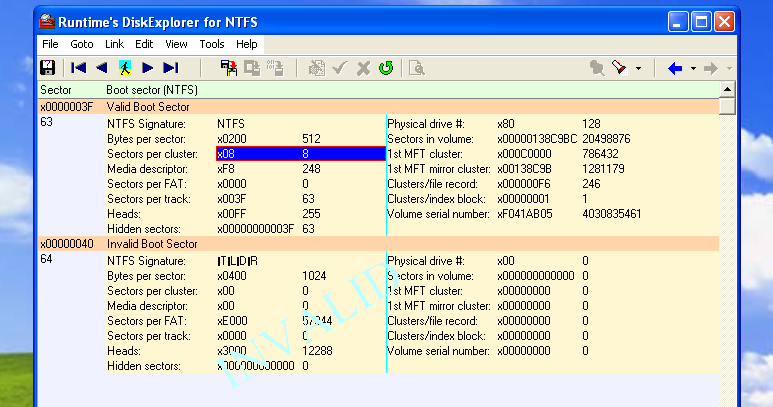
1. Определение положения и активности разделов (MBR):



- какой раздел является загрузочным?

Отмеченный флагом Yes в столбце boot

2. Установление геометрии раздела (BR):



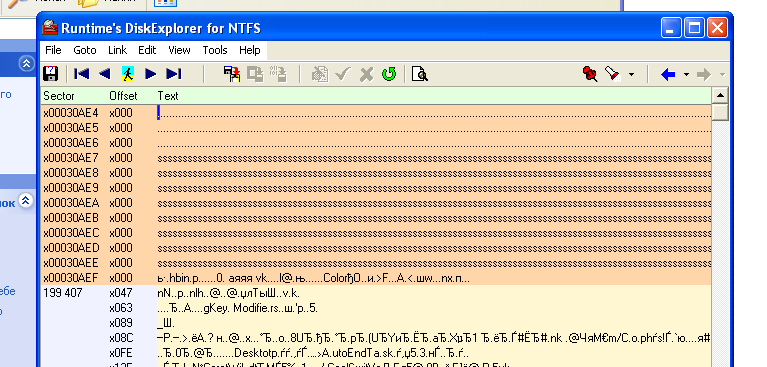
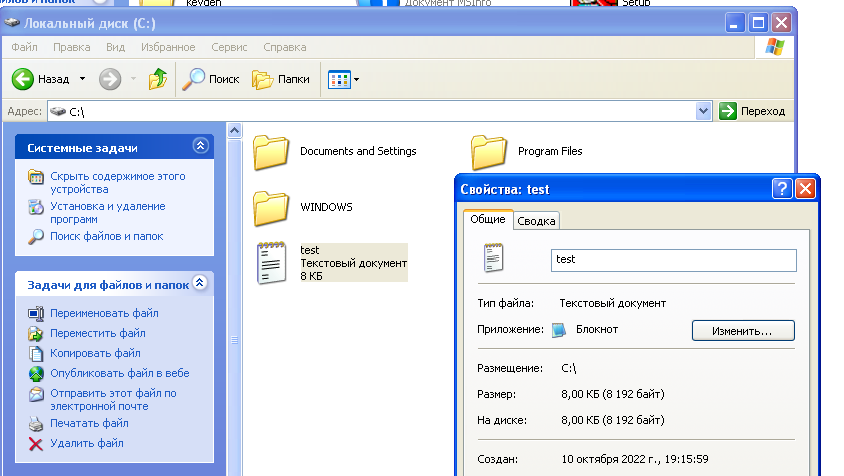
- каков размер кластера в байтах? 8 байт

- каков размер записи в MFT в байтах? 1024 байт

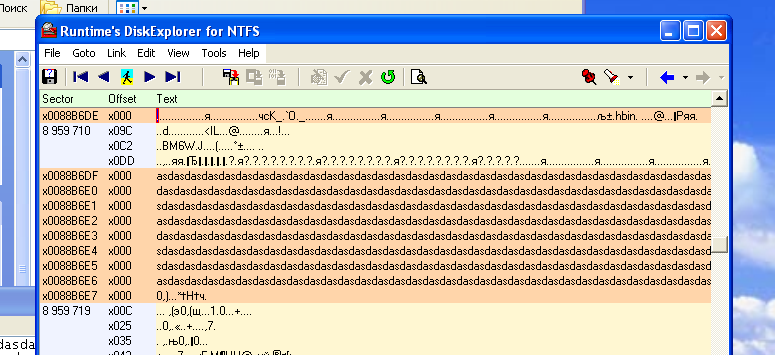
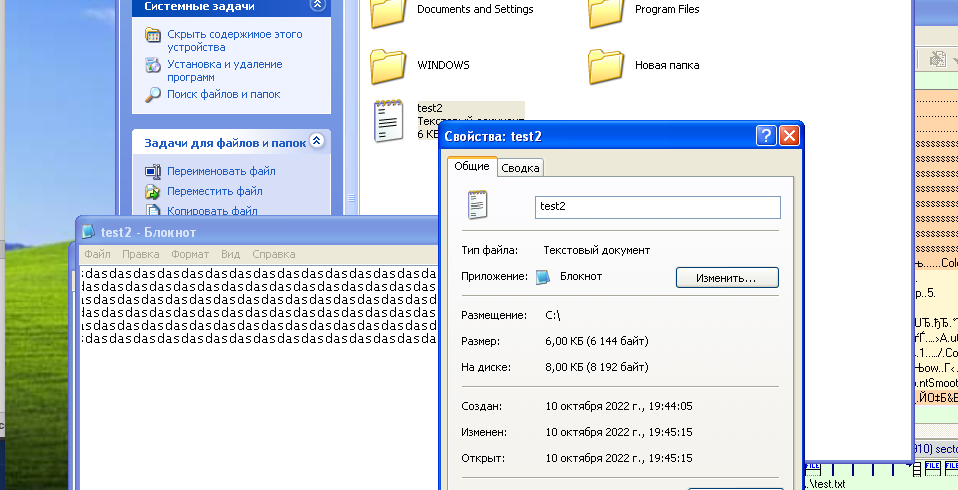
- каков размер раздела в мегабайтах? 20498876 секторов

3. Создать файл длиной в 2 кластера и записать туда идентифицируемую информацию. Удалить. Не ранее, чем через 1 минуту создать файл длиной 1,5 кластера. Ответить на вопрос:

2 кластера \* 8 секторов \* 512 байт = 8192 байт



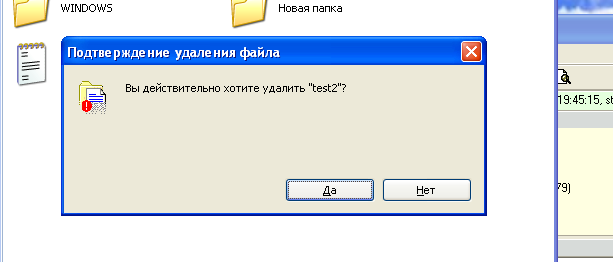
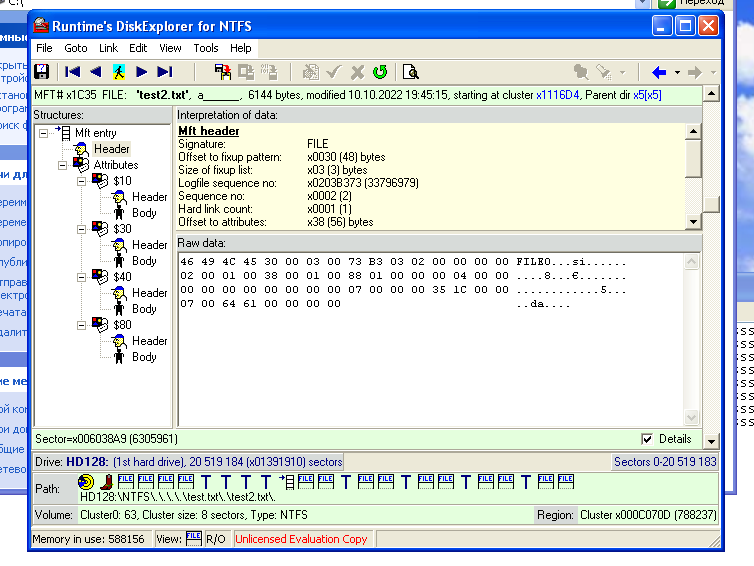
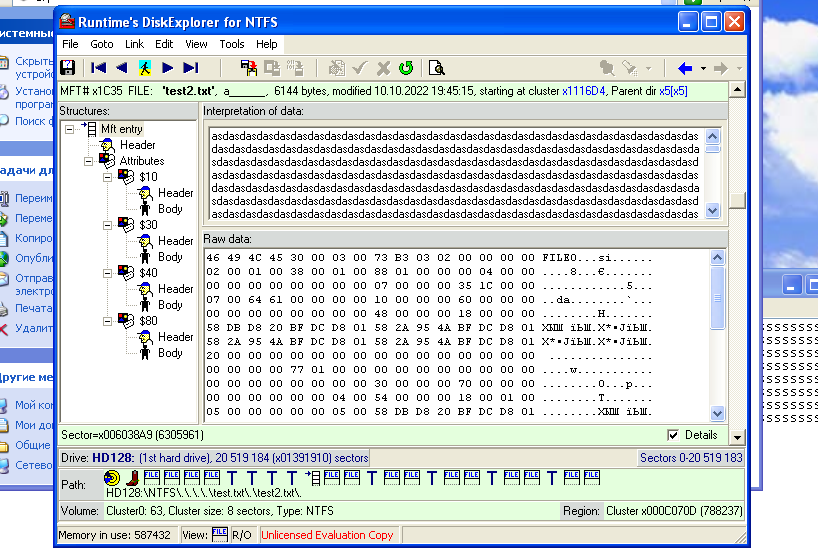
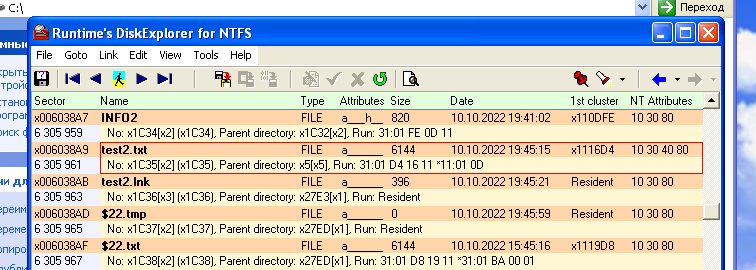
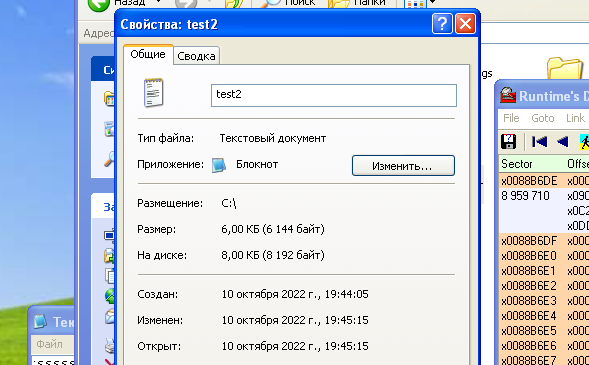
1.5 кластера \* 8 секторов \* 512 байт = 6 Кбайт



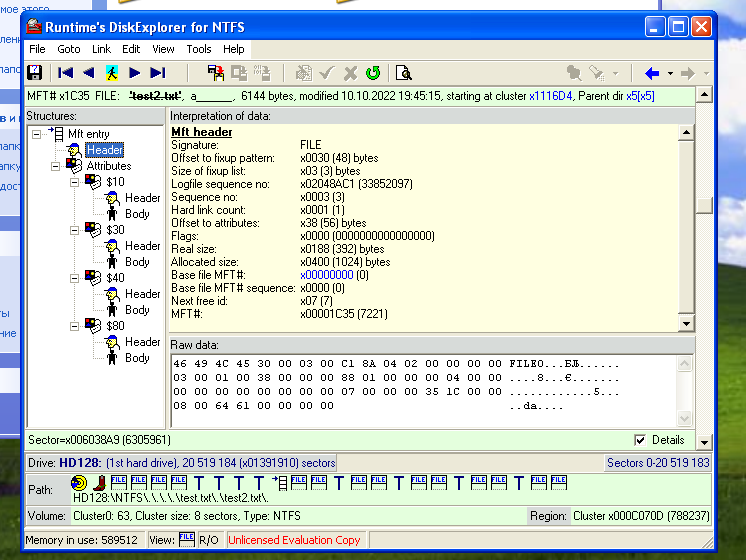
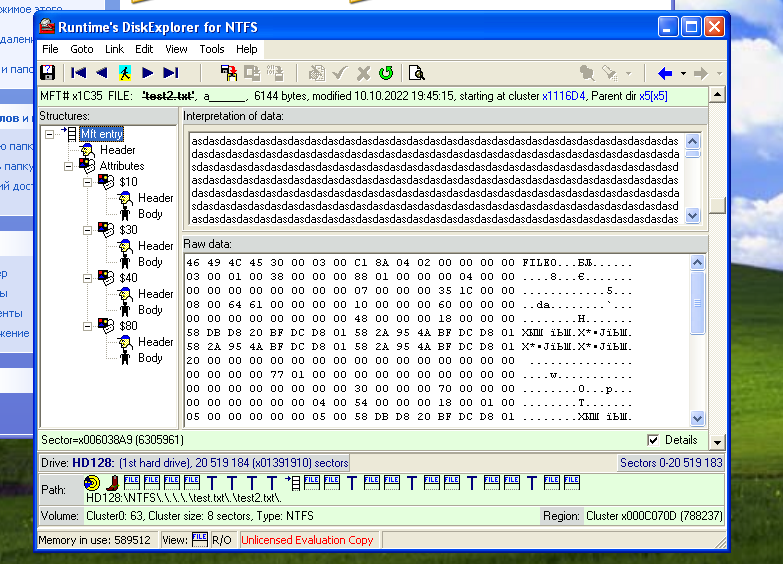
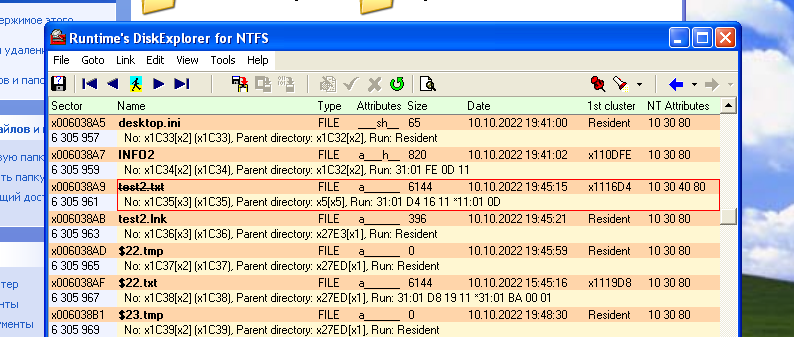
- попал ли он в кластеры удаленного файла? Нет, запись велась в разных секторах

- как найти «хвост» кластера нового файла, какого его содержимое? Никак, в хвосте кластера нового файла нет информации об удаленном файле

4. Запомнить (сохранить) информацию о некотором нерезидентном файле в MFT (номер MFT-записи, местоположение тела, имя в 16-ричной записи), за тем удалить его без помещения в корзину.



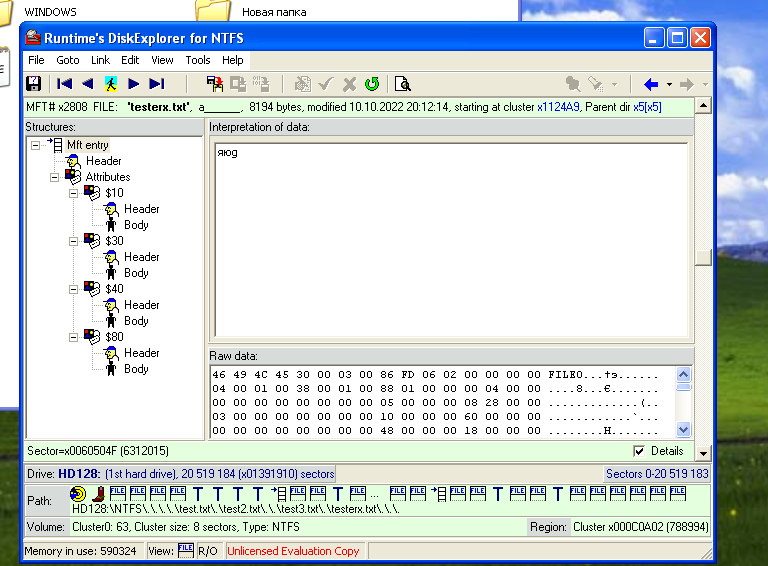
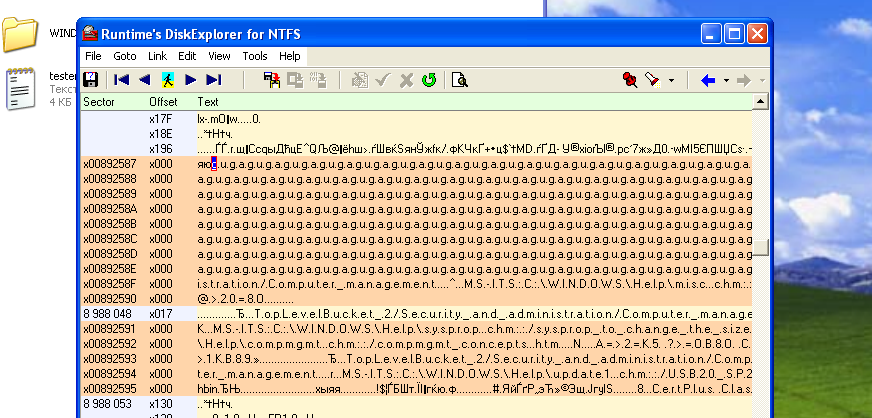
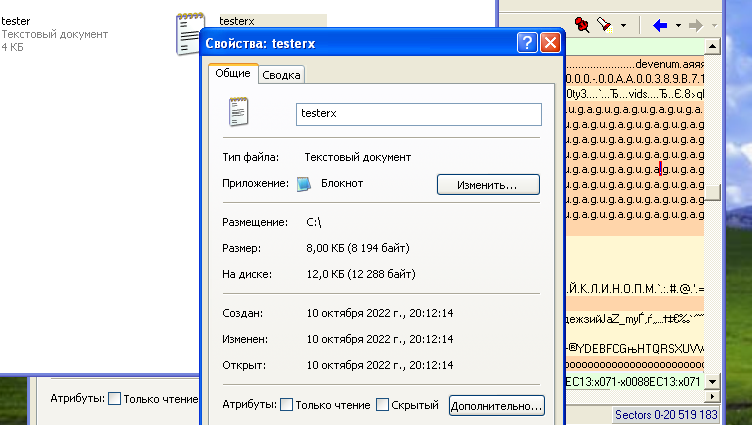
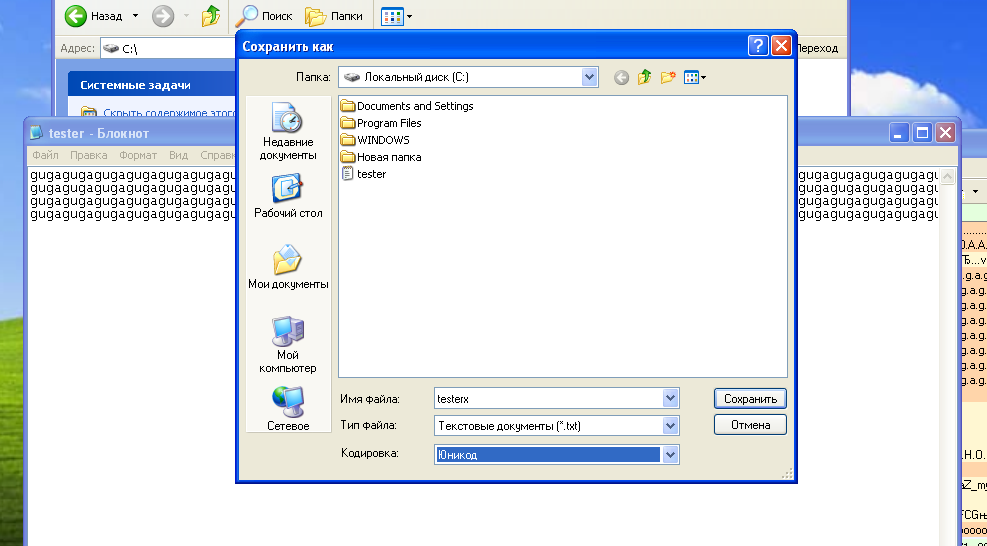
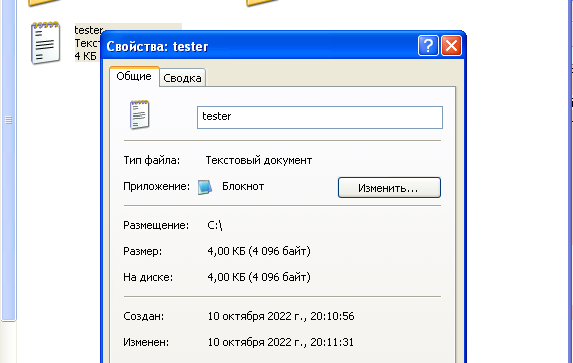
Удалив без помещения в корзину, заново найдем файл в NTFS. Имя файла стало зачеркнутым.



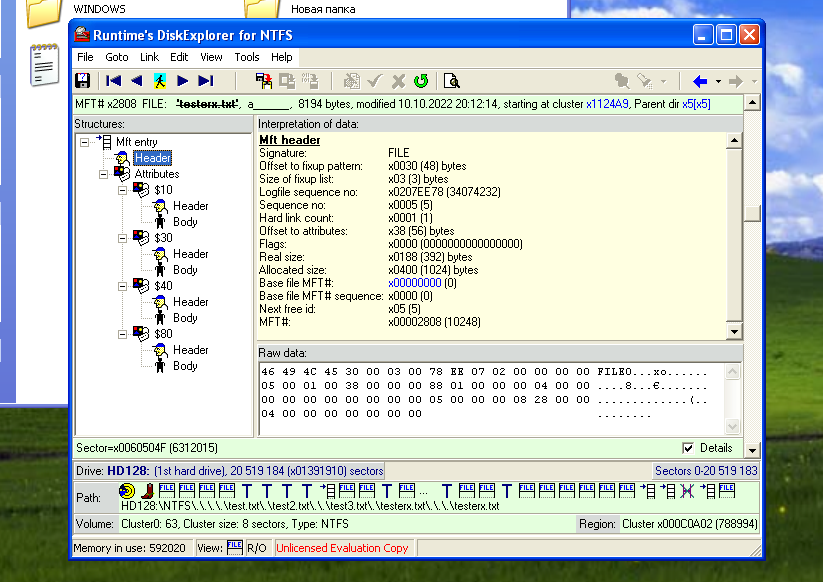
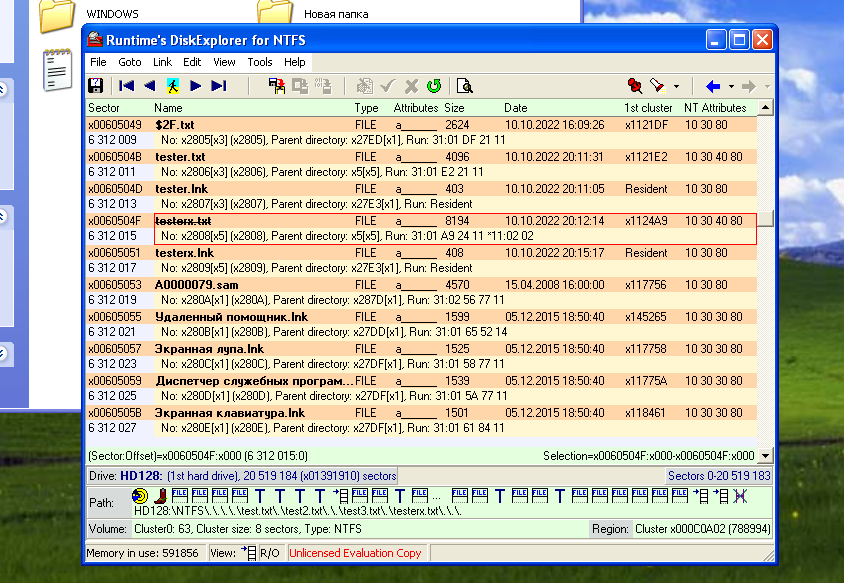
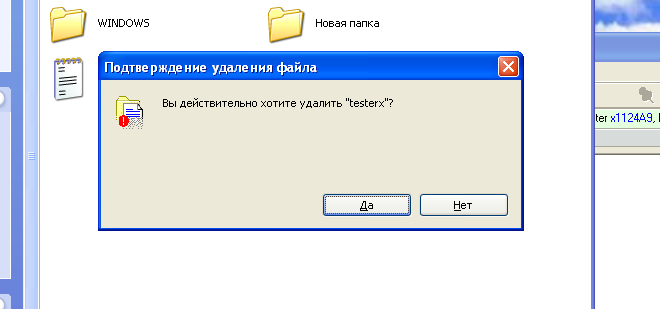
Важно – изменился заголовок в информации о файле

5. Поиск удаленного файла по имени с учетом того, что оно записано в UNICOD16 с использованием инструмента поиска текстовых строк Run Time NTFS Explorer. Найти информацию об удаленном файле в MFT. Ответить на вопрос:

Создадим txt файл и сохраним в юникоде



Удалим без перемещения в корзину

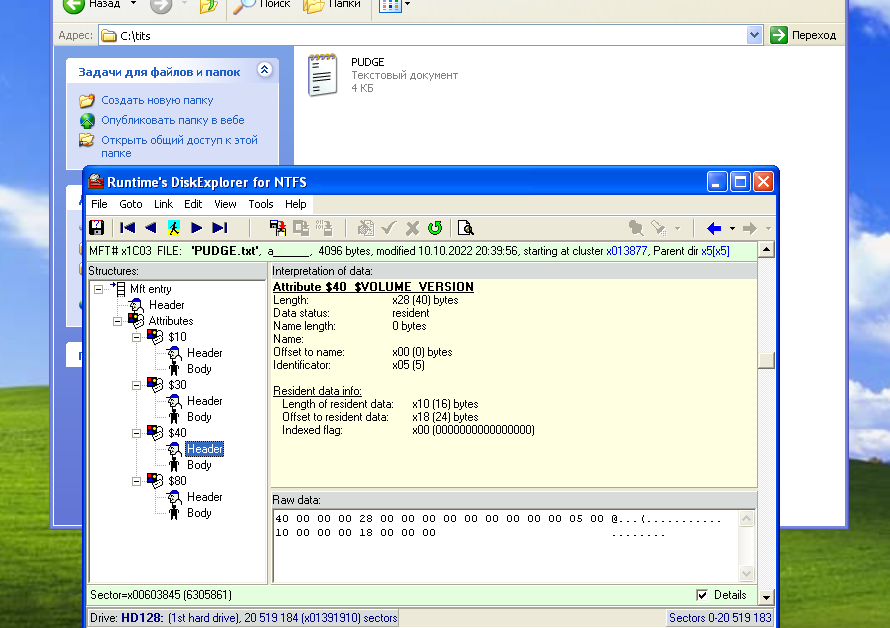
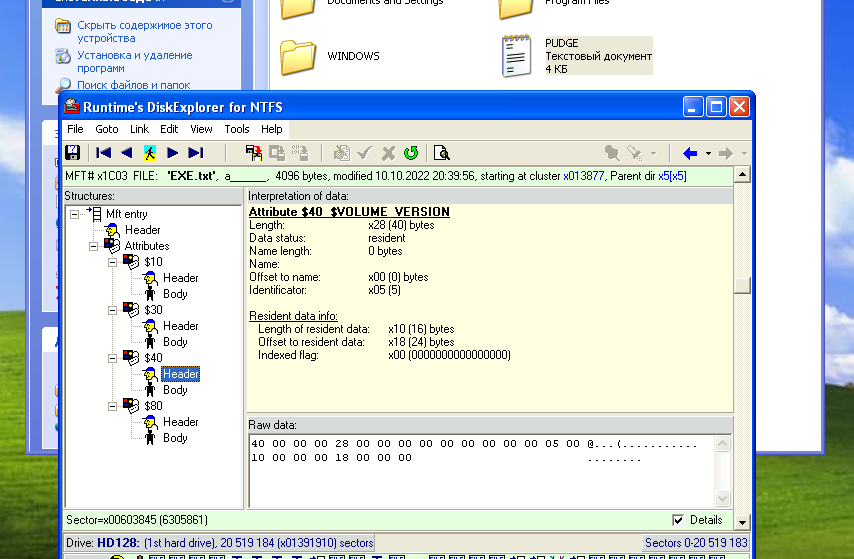
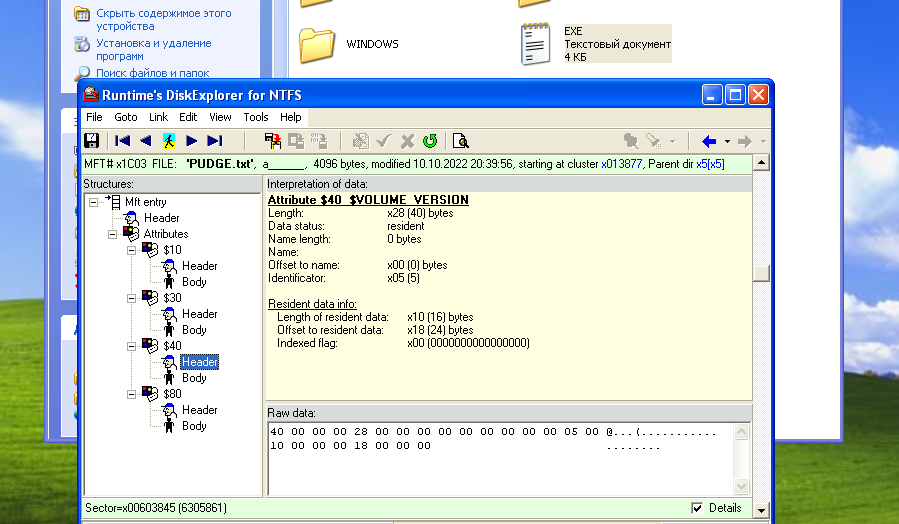
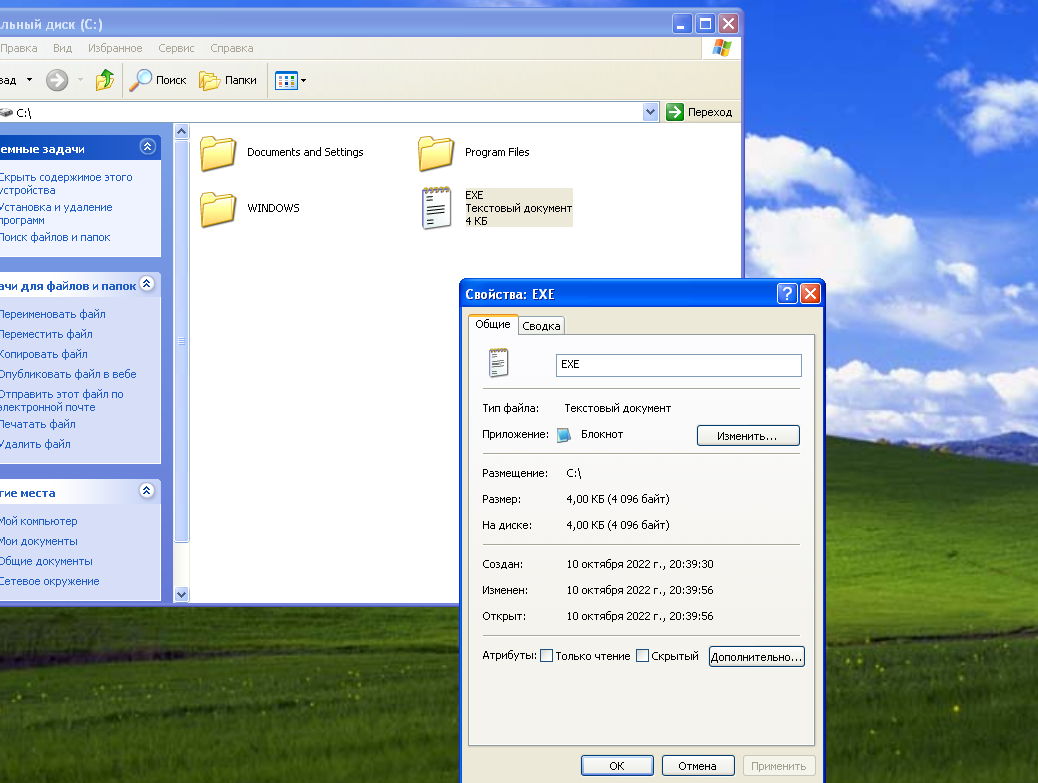


- как изменилась информация о файле в MFT? Информация не сохранилась

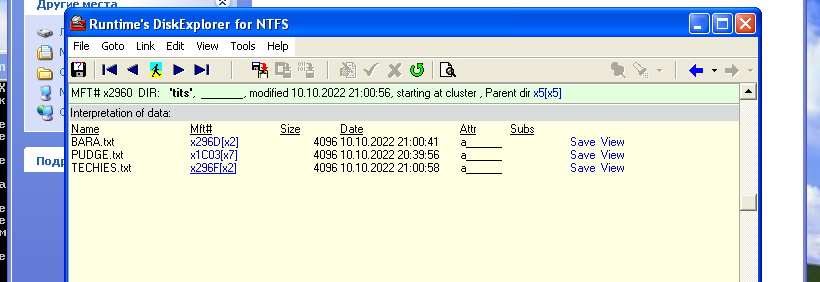
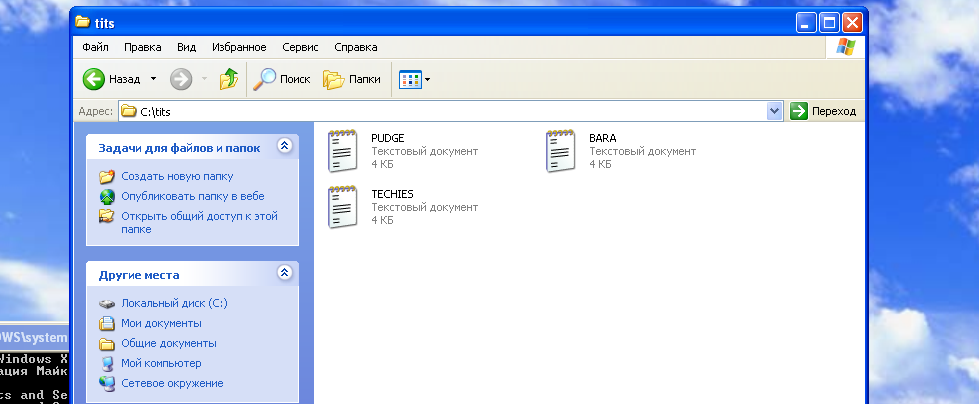
6. Проследить динамику временных характеристик файла при его копировании, перемещении и удалении в атрибутах $STANDARD\_INFORMATION и $FILE\_NAME. Заполните таблицу

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| действие с файлом | $STANDARD\_INFORMATION | | | | $FILE\_NAME | | | |
|  | создание | изменение | изменение MFT | доступ | создание | изменение | изменение MFT | доступ |
| создание файла №1 | 10.10.2022 20:23:59 | 10.10.2022 20:23:59 | 10.10.2022 20:23:59 | 10.10.2022 20:23:59 | 10.10.2022 20:23:59 | 10.10.2022 20:23:59 | 10.10.2022 20:23:59 | 10.10.2022 20:23:59 |
| Переименование файла №1 | 10.10.2022 20:23:59 | 10.10.2022 20:23:59 | 10.10.2022 20:27:24 | 10.10.2022 20:24:14 | 10.10.2022 20:23:59 | 10.10.2022 20:23:59 | 10.10.2022 20:23:59 | 10.10.2022 20:23:59 |
| копирование файла №1 в файла №2 | 10.10.2022 20:29:56 | 10.10.2022 20:23:59 | 10.10.2022 20:32:05 | 10.10.2022 20:32:00 | 10.10.2022 20:29:56 | 10.10.2022 20:23:59 | 10.10.2022 20:24:31 | 10.10.2022 18:17:12? |
| переименование файла №2 | 10.10.2022 20:29:56 | 10.10.2022 20:23:59 | 10.10.2022 20:32:05 | 10.10.2022 20:32:00 | 10.10.2022 20:29:56 | 10.10.2022 20:23:59 | 10.10.2022 20:27:24 | 10.10.2022 20:29:56 |
| Перемещение файла №1 в другой каталог в файл №3 | 10.10.2022 20:29:56 | 10.10.2022 20:23:59 | 10.10.2022 20:38:30 | 0.10.2022 20:32:00 | 10.10.2022 20:29:56 | 10.10.2022 20:23:59 | 10.10.2022 20:37:26 | 10.10.2022 20:29:56 |
| переименование файла №3 | 10.10.2022 20:29:56 | 10.10.2022 20:23:59 | 10.10.2022 20:39:40 | 0.10.2022 20:32:00 | 10.10.2022 20:29:56 | 10.10.2022 20:23:59 | 10.10.2022 20:39:01 | 10.10.2022 20:29:56 |

7. Проследить порядок создания и заполнения содержимым атрибута файла $OBJECT\_ID путем последовательного создания 3-х файлов, заведомо обладающих этим атрибутом.



Атрибут $ObjectID оставался неизменным после перемещений и переименований

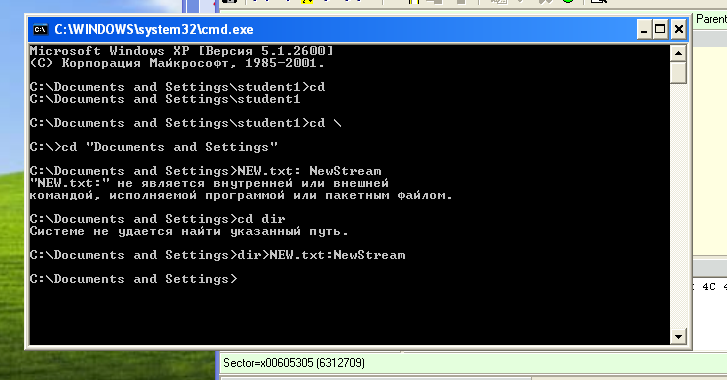
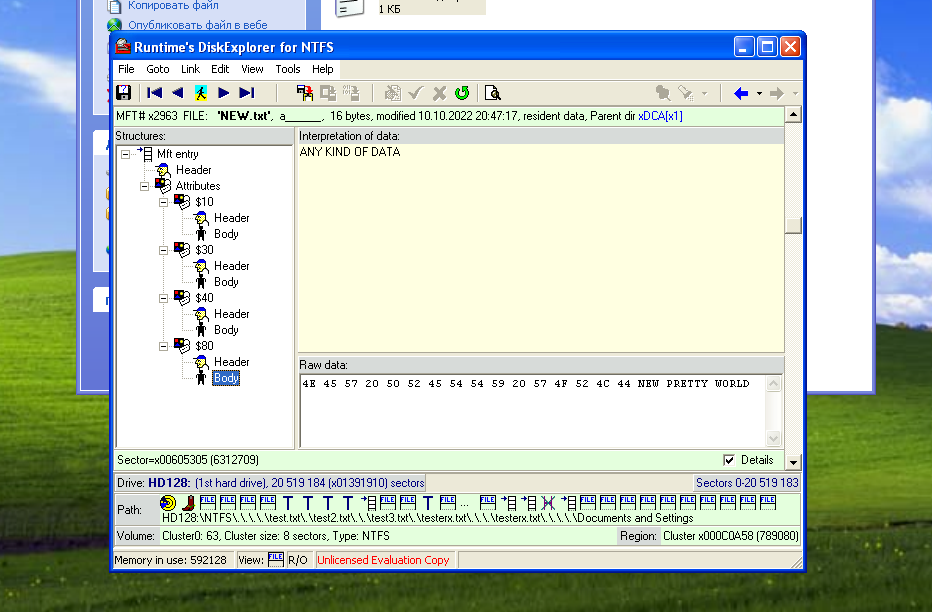
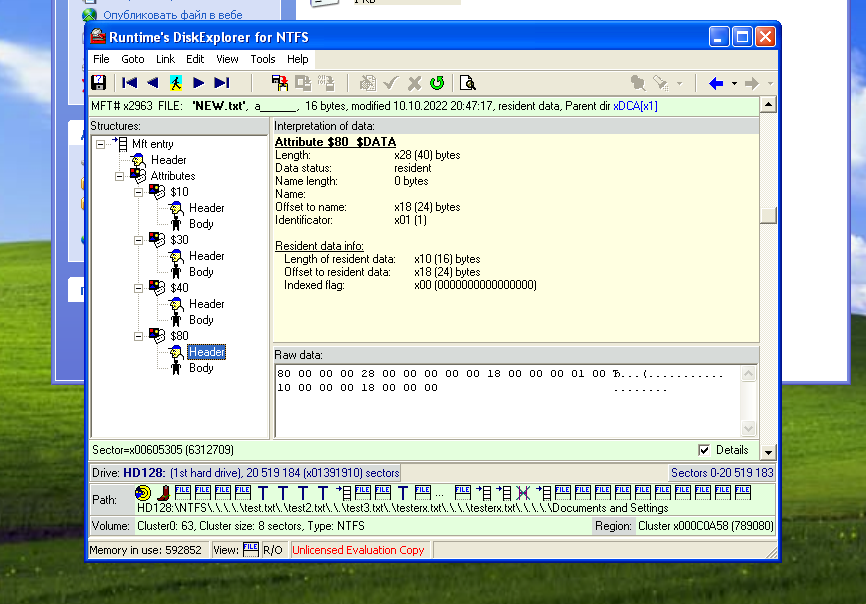
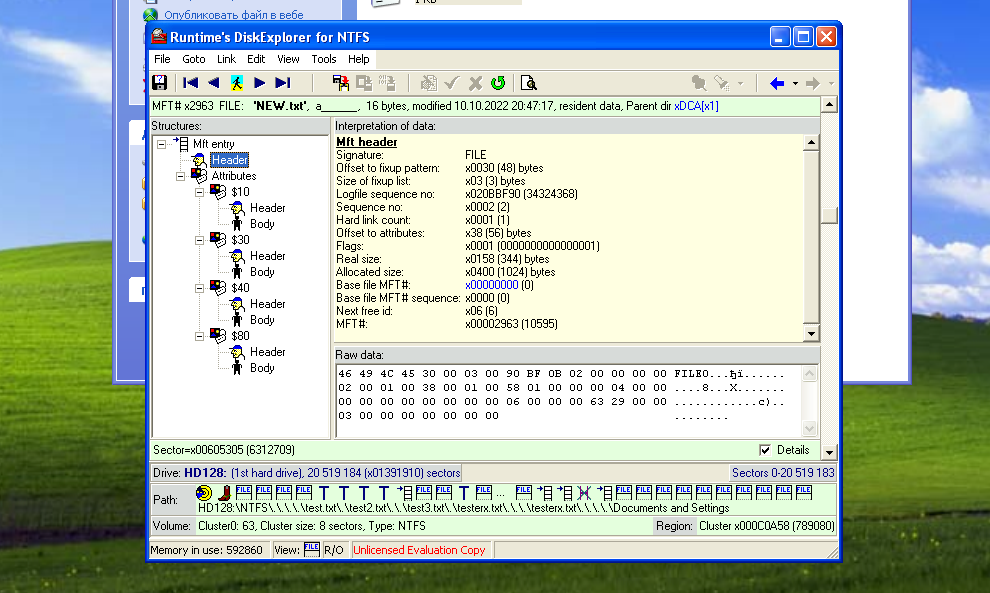
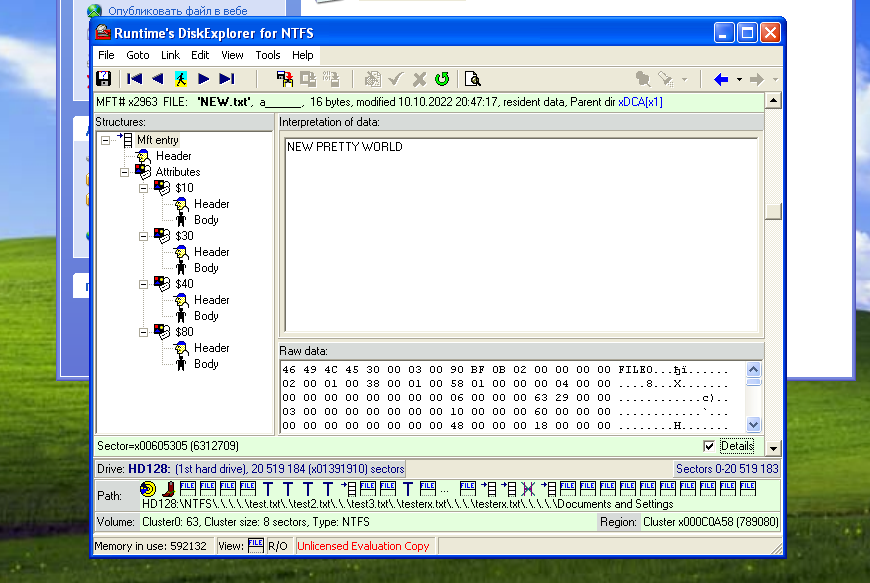
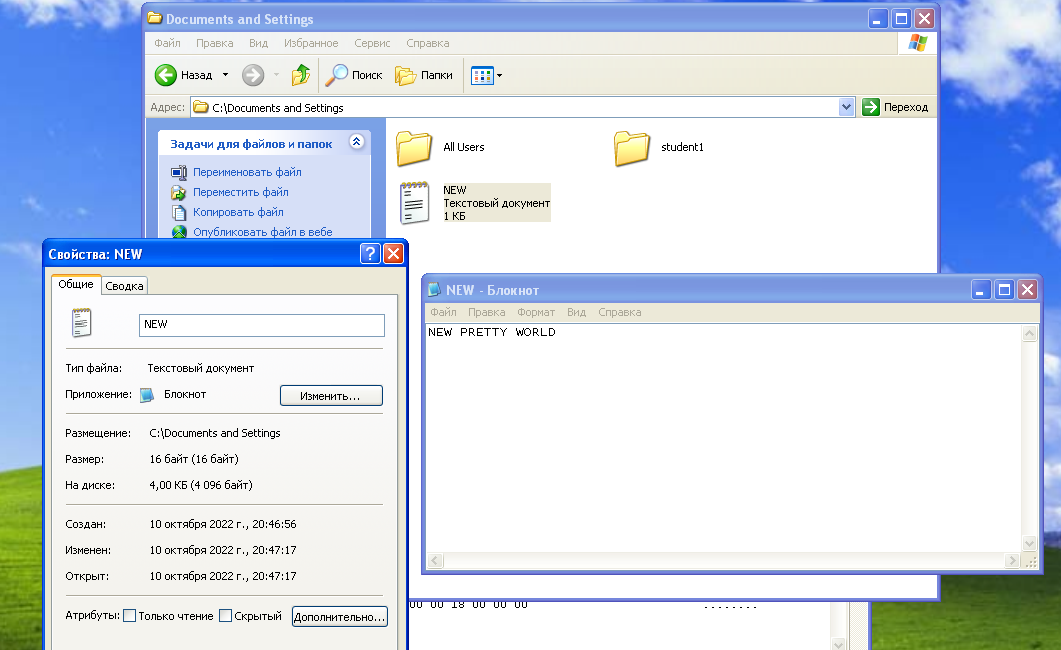


**Упражнение по созданию именованного атрибута $DATA**

8. Откройте окно командной строки. Перейдите на исследуемый раздел NTFS и введите следующую команду:

DIR > NewFile.txt: NewStream

Найдите созданный файл с помощью проводника Windows и попытайтесь найти информацию о дополнительном потоке данных этого файла. Посмотрите, какой размер файла указывает проводник Windows. (Попутно можете ввести с помощью блокнота какой-нибудь текст в этот файл.) Теперь найдите созданный файл с помощью программы RT NTFS Explorer и просмотрите его MFT-запись. Найдите описание дополнительного потока данных и просмотрите его содержимое. Является ли поток пустым?



Появился новый атрибут (дополнительный поток данных):

