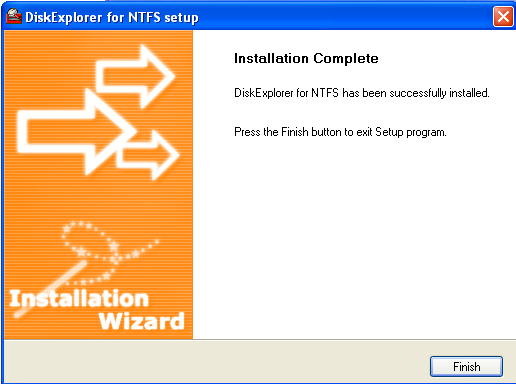
## **Исследование значимых областей следообразования ФС NTFS**

**Работу выполнил студент 431гр. Никитин А.В.**

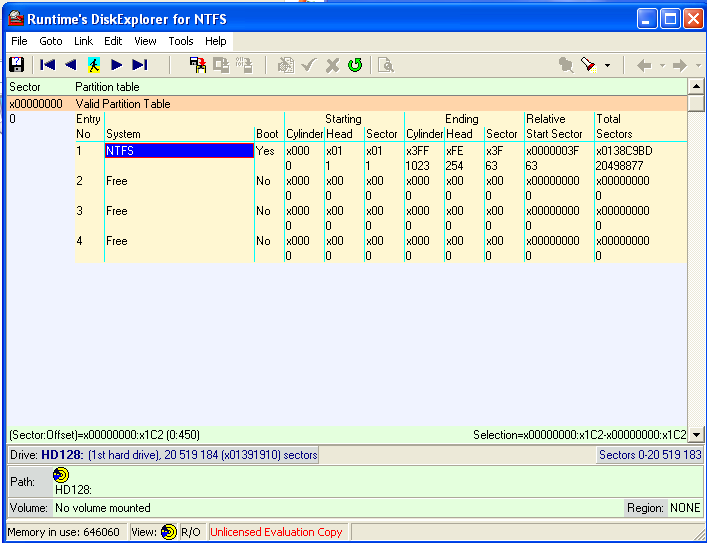
**Исследование раздела жесткого диска** ( инструмент - RT NTFS Explorer)**.**

Установил программу Disk Explorer for NTFS:



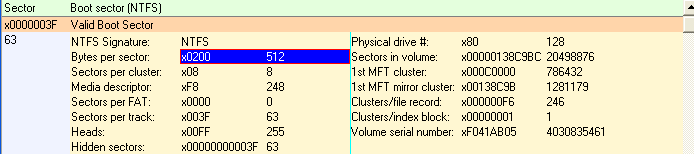
1. Определение положения и активности разделов (MBR):

- какой раздел является загрузочным?

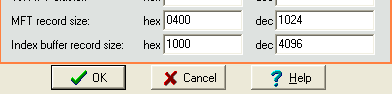
Загрузочным является раздел отмеченный флагом YES (первый):

2. Установление геометрии раздела (BR):

- каков размер кластера в байтах?

Имеем 512 байт в каждом секторе и 8 секторов в каждом кластере, поэтому размер кластера составляет 4096 байт.

- каков размер записи в MFT в байтах?



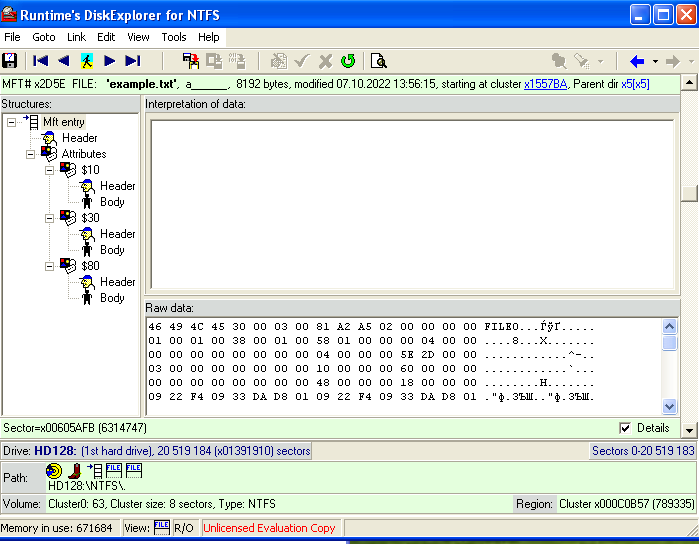
3. Создать файл длиной в 2 кластера и записать туда идентифицируемую информацию. Удалить. Не ранее, чем через 1 минуту создать файл длиной 1,5 кластера. Ответить на вопрос:

2 кластера \* 8 секторов \* 512 байт = 8912 байт.

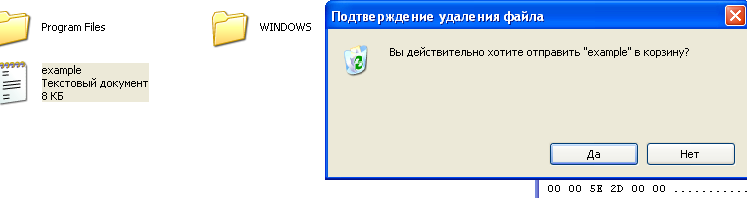
С помощью команды создал текстовый файл заданного размера:



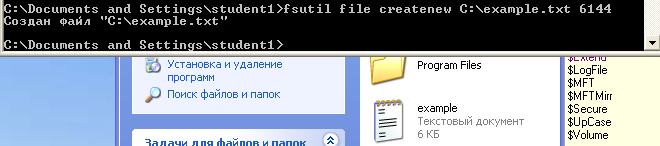
Затем нашел его с помощью Disk Explorer:

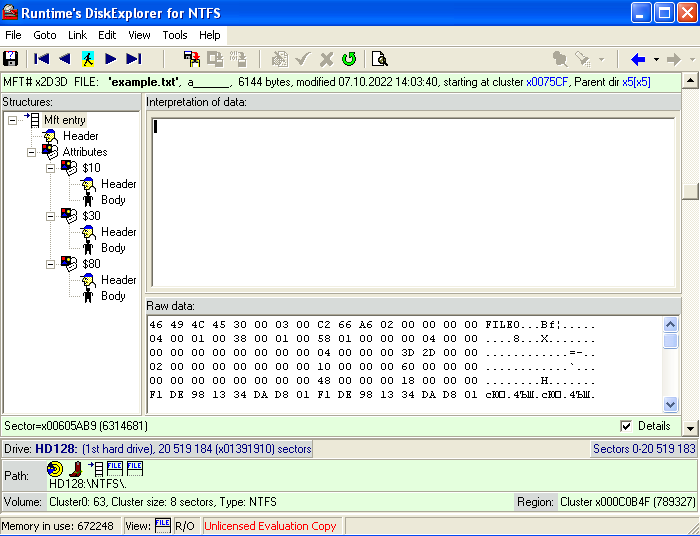


Затем удалил:



Через минуту создал новый файл уже размером 1.5 кластера (6144 байт):





- попал ли он в кластеры удаленного файла?

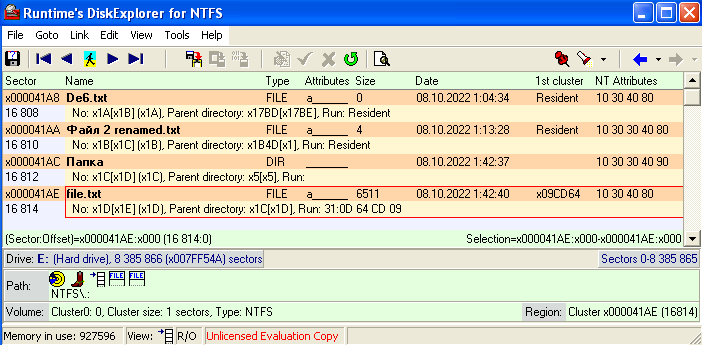
Как видно из скриншота выше, запись файла произошла не в тот же кластер, а именно: в первом случае запись начинается с кластера 1557BA, а запись нового файла начинается с кластера 75CF.

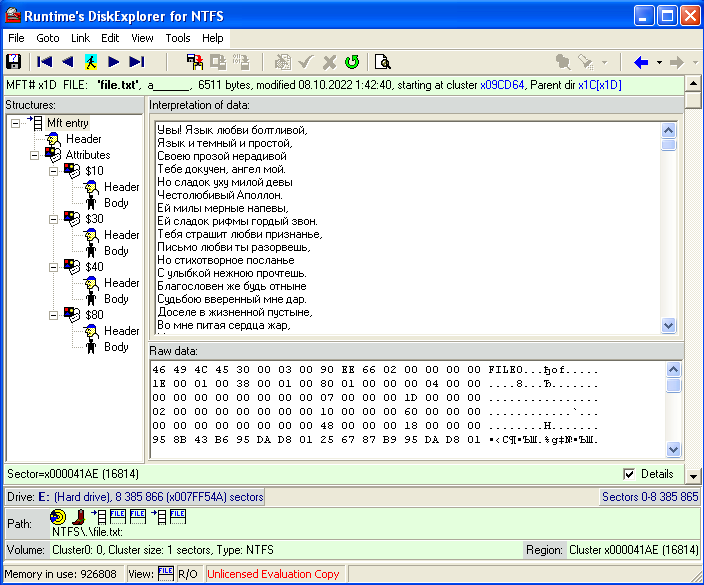
- как найти «хвост» кластера нового файла, какого его содержимое?

Хвост кластера найти не получилось, так как файл записался в совершенно другой кластер.

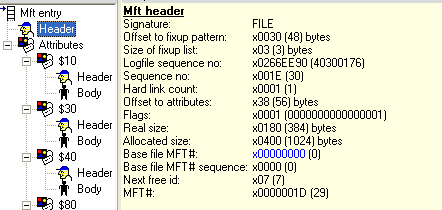
4. Запомнить (сохранить) информацию о некотором нерезидентном файле в MFT (номер MFT-записи, местоположение тела, имя в 16-ричной записи), затем удалить его без помещения в корзину.

На диске E, не являющемся системным, создал нерезидентный файл <<file1.txt>> и заполнил его некоторой информацией:



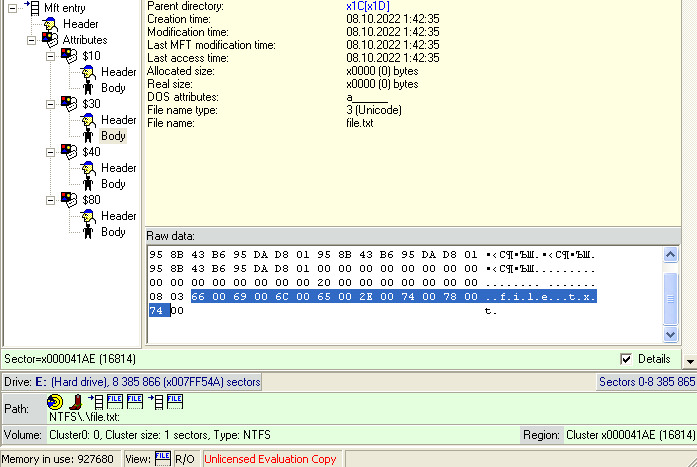
Затем открыл его в MFT Entry:

Номер в MFT составляет x0000001D (29). Заметим также, что атрибут flags до удаления равен x0001:

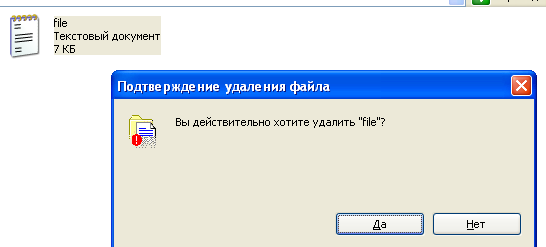


Название файла находится по атрибуту $30 в теле и в 16-ричной системе его имя будет

**66 69 6С 65 2E 74 78 74** :



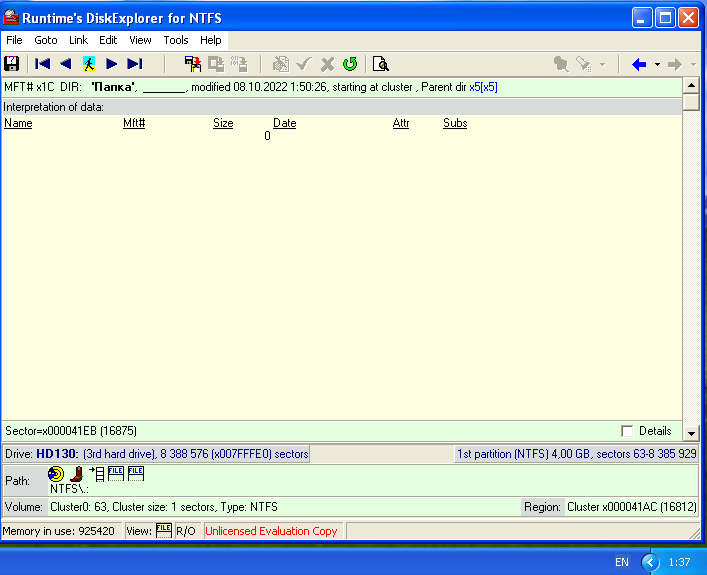
Далее удалил файл без помещения в корзину (SHIFT + DEL):



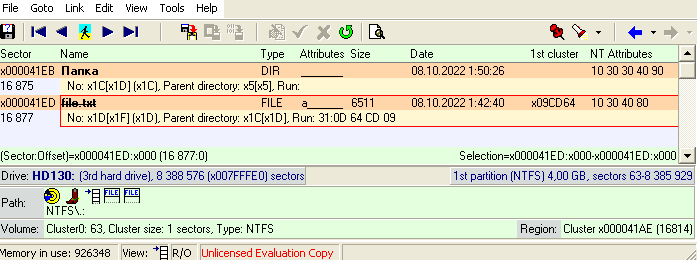
5. Поиск удаленного файла по имени с учетом того, что оно записано в UNICOD16 с использованием инструмента поиска текстовых строк Run Time NTFS Explorer. Найти информацию об удаленном файле в MFT. Ответить на вопрос:

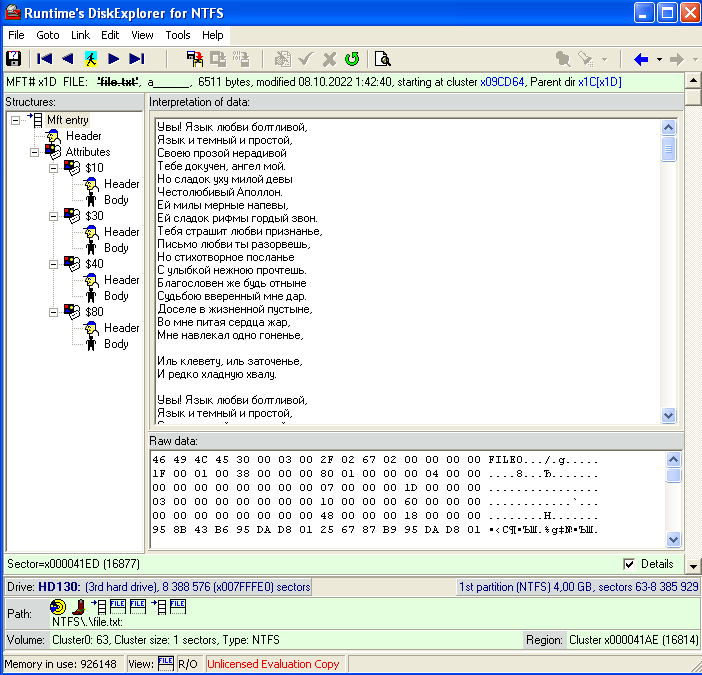
- как изменилась информация о файле в MFT?

В ходе практических действий заметил, что если попытаться удалить какой-либо файл, находящийся на одном диске с операционной системой, то спустя некоторое время информация о файле окончательно исчезает как при поиске через root directory, так и при поиске через file entry.

Попробуем найти файл через root directory, и там он будет отсутствовать в исходной папке. Также заметил, что изменилось время модификации файла и оно почему-то заранее стало больше, чем текущее время на машине. Оказалось, что информация об изменении берется не по времени на виртуальной машине, а по времени на рабочей машине:

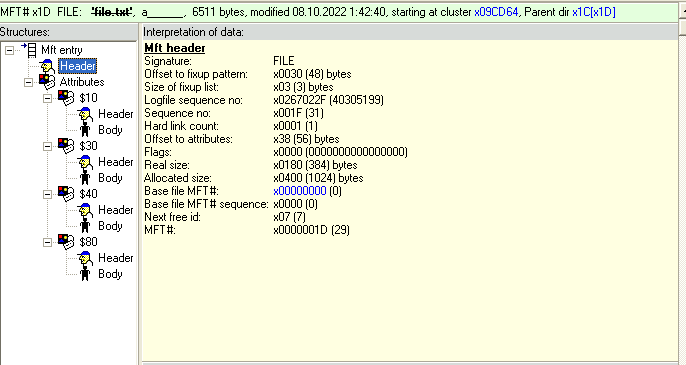
Теперь откроем просмотр данной папки с помощью File entry. Как видим, имя файла перечеркнуто, что свидетельствует о его удалении:



Теперь перейдем к просмотру файла через MFT Entry:

Заметил, что **атрибут flags, который до удаления файла был равен x0001, теперь же равен x0000.**

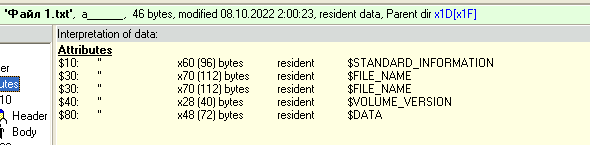
А также заметил, что **изменился атрибут Logfile sequence no**:

Количество жестких ссылок то же и состаляет 1. Номер в MFT не изменен. Размер файла также составляет 6511 байт, как и составлял до удаления, а также время модификации не поменялось.

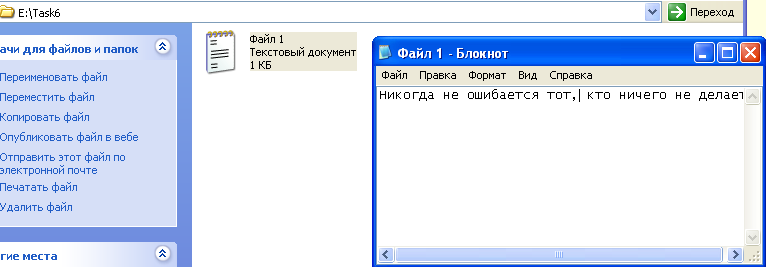
6. Проследить динамику временных характеристик файла при его копировании, перемещении и удалении в атрибутах $STANDARD\_INFORMATION и $FILE\_NAME. Заполните таблицу.

Буду заполнять таблицу построчно и для каждой строки буду прикреплять скриншоты с отображением в них временных промежутков исследуемых значений.

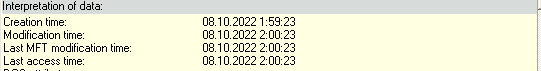
Отметим, что атрибут $10 – это атрибут $Standard\_information, а атрибут $30 – это атрибут $File\_name:



**Первая строка (Создание файла №1):**

Также как и в предыдущем задании создал текстовый файл на несистемном диске под названием Файл 1 и поместил в него некоторую информацию:

$Standard\_information:

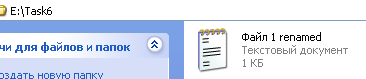
Все поля, за исключением времени создания не отличаются друг от друга. Так как файл был создан в одно время. А затем в него была помещена информация, которая перекрыла время создания файла.

$File\_name:

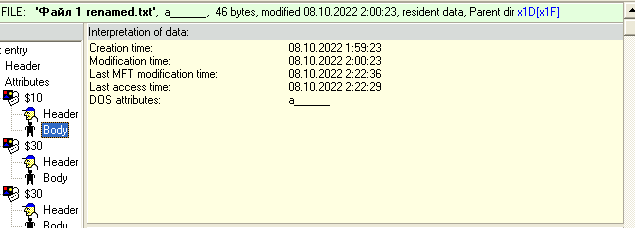
Все поля равны между собой и совпадают с полем создания файла из атрибута $10.

**Вторая строка (Переименование файла №1)**

Теперь файл будет называться Файл 1 renamed:



Теперь обновим информацию в MFT Entry и проследим за изменениями:

 $Standard\_information:

Сравнивая с предыдущими заполненными в таблице значениями текущие, видно что изменились значения полей изменения MFT и поля доступ к файлу. Последний изменился всего на 9 секунд. Поэтому, возможно, это может быть не связано с переименованием файла.

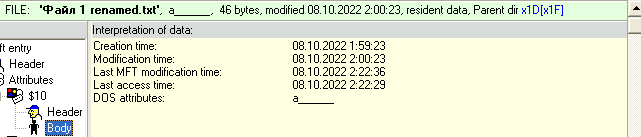
$File\_name:

В данном случае свои значения изменили все поля за исключением поля создания файла, но аналогично предполагаю, что конкретно с переименованием связано только поле изменение MFT, так как разница во времени в других полях не такая существенная.

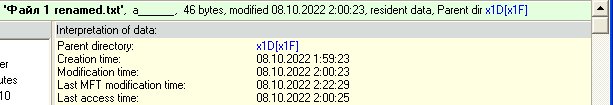
**Третья строка (Копирование файла №1 в файл №2)**

Создал новый файл и назвал его Файл 2, затем копировал информацию из первого файла во второй.

$Standard\_information:

Как видим, от предыдущих значений отличается только поле времени доступа.

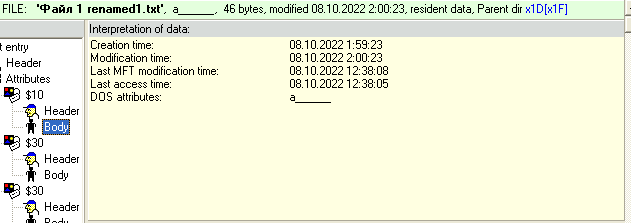
$File\_name:

Здесь никаких изменений по сравнению с предыдущими результатами не произошло.

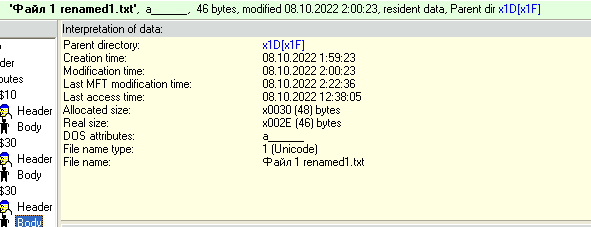
**Четвертая строка (Переименование файла №2)**

Еще раз переименовал файл, теперь его имя будет Файл 1 renamed1.

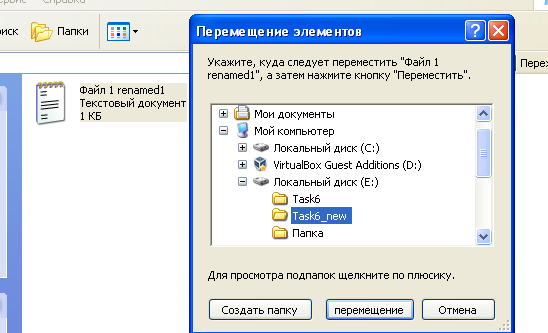
$Standard\_information:

Опять изменились только поля «Изменение MFT» и «доступ»

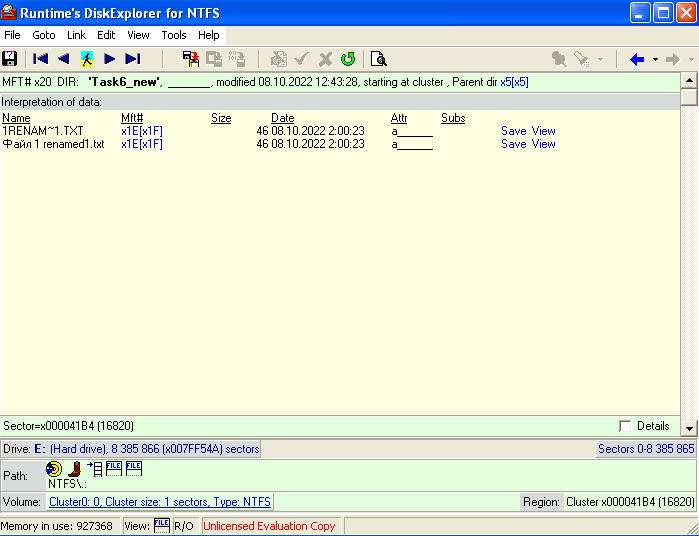
$File\_name:



**Пятая строка (Перемещение в другой каталог)**

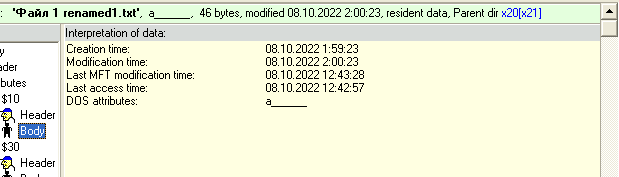
Переместил файл в другой каталог:

Спустя примерно минуту информация появилась в Disk Explorer:



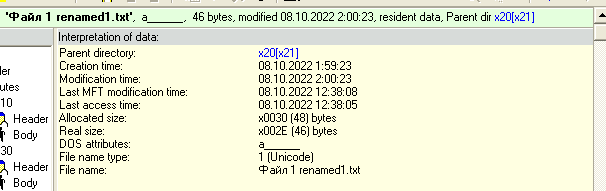
Теперь проверим состояние атрибутов.

$Standard\_information:



По сравнению с предыдущими значениями изменились поля модификации MFT и времени доступа

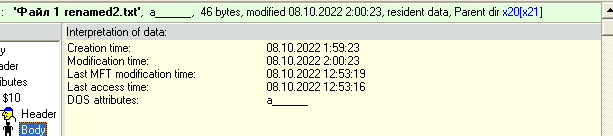
$File\_name:

По сравнению с предыдущими значениями изменилось только поле «изменение MFT»

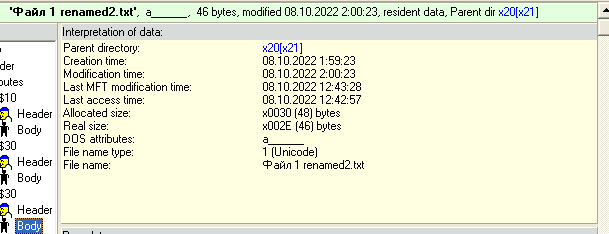
**Шестая строка(переименование №3)**

Снова переименовал файл, теперь он будет называться Файл 1 renamed2.

$Standard\_information:

Изменились поля модификации MFT и доступа.

$File\_name:

Также изменились поля модификации MFT и доступа.

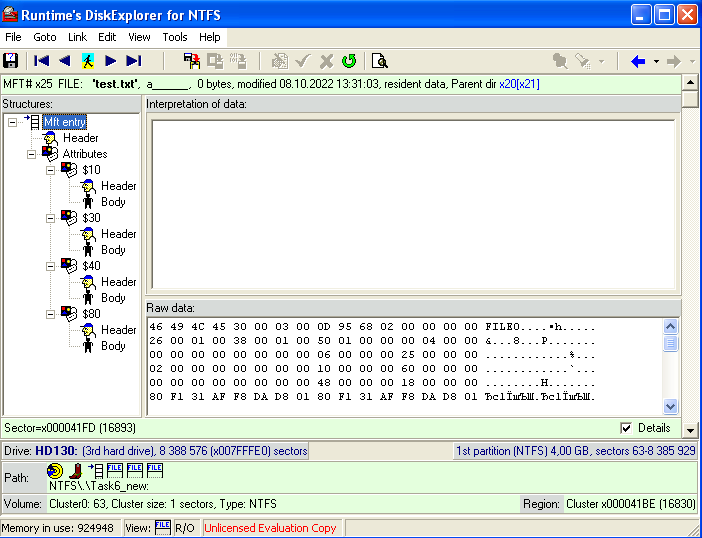
Далее представлена заполненная таблица. Если значение текущей ячейки отличается от значения ячейки, расположенной строкой выше начиная со второй строки, то данная ячейка помечена желтым цветом.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| действие с файлом | $STANDARD\_INFORMATION | | | | $FILE\_NAME | | | |
|  | создание | изменение | изменение MFT | доступ | создание | изменение | изменение MFT | доступ |
| создание файла №1 | 08.10.2022 1:59:23 | 08.10.2022 2:00:23 | 08.10.2022 2:00:23 | 08.10.2022 2:00:23 | 08.10.2022 1:59:23 | 08.10.2022 1:59:23 | 08.10.2022 1:59:23 | 08.10.2022 1:59:23 |
| Переименование файла №1 | 08.10.2022 1:59:23 | 08.10.2022 2:00:23 | 08.10.2022 2:22:36 | 08.10.2022 2:00:29 | 08.10.2022 1:59:23 | 08.10.2022 2:00:23 | 08.10.2022 2:22:29 | 08.10.2022 2:00:25 |
| копирование файла №1 в файла №2 | 08.10.2022 1:59:23 | 08.10.2022 2:00:23 | 08.10.2022 2:22:36 | 08.10.2022 2:22:29 | 08.10.2022 1:59:23 | 08.10.2022 2:00:23 | 08.10.2022 2:22:29 | 08.10.2022 2:00:25 |
| переименование файла №2 | 08.10.2022 1:59:23 | 08.10.2022 2:00:23 | 08.10.2022 12:38:08 | 08.10.2022 12:38:05 | 08.10.2022 1:59:23 | 08.10.2022 2:00:23 | 08.10.2022 12:38:03 | 08.10.2022 12:38:05 |
| Перемещение файла №1 в другой каталог | 08.10.2022 1:59:23 | 08.10.2022 2:00:23 | 08.10.2022 12:43:28 | 08.10.2022 12:42:57 | 08.10.2022 1:59:23 | 08.10.2022 2:00:23 | 08.10.2022 2:38:08 | 08.10.2022 2:38:08 |
| переименование файла №3 | 08.10.2022 1:59:23 | 08.10.2022 2:00:23 | 08.10.2022 12:53:19 | 08.10.2022 12:53:16 | 08.10.2022 1:59:23 | 08.10.2022 2:00:23 | 08.10.2022 12:43:28 | 08.10.2022 12:42:28 |

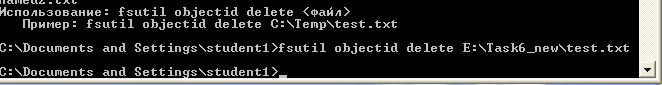
7. Проследить порядок создания и заполнения содержимым атрибута файла $OBJECT\_ID путем последовательного создания 3-х файлов, заведомо обладающих этим атрибутом.

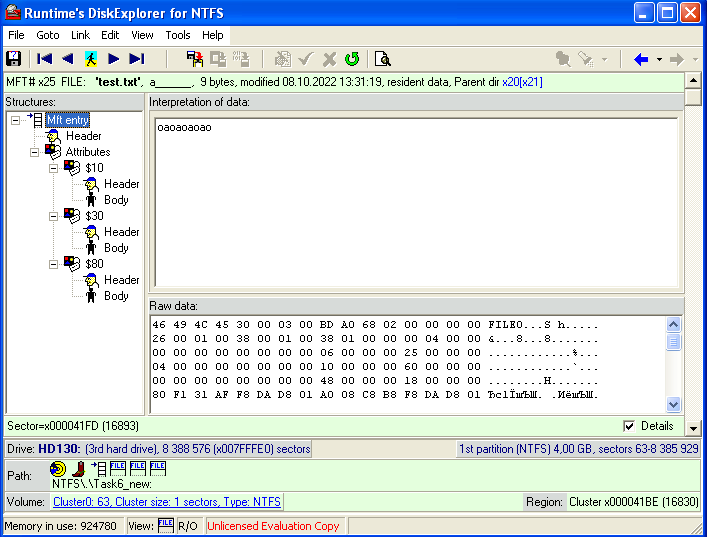
Просмотрим, какой атрибут является $Object\_id. Для этого создадим текстовый файл и с помощью команды **fsutil objectid delete E:\task6\_new\test.txt** удалим object\_id.

До удаления:

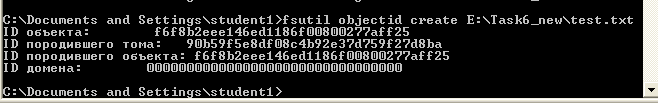


Выполняем команду:

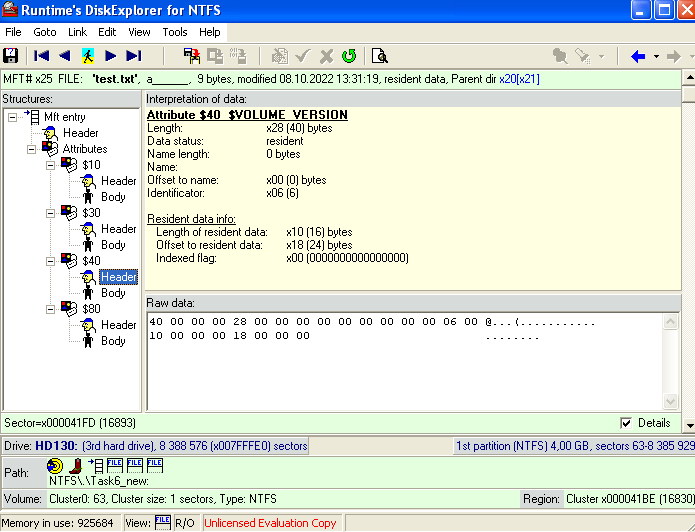


Видно, что атрибут $40 пропал:

Теперь создадим object\_id для нашего файла:

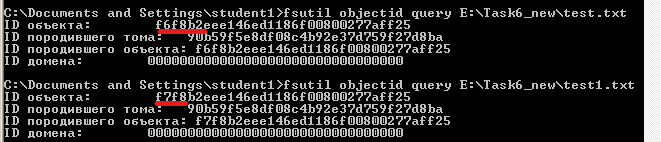


Атрибут $40 снова появился:

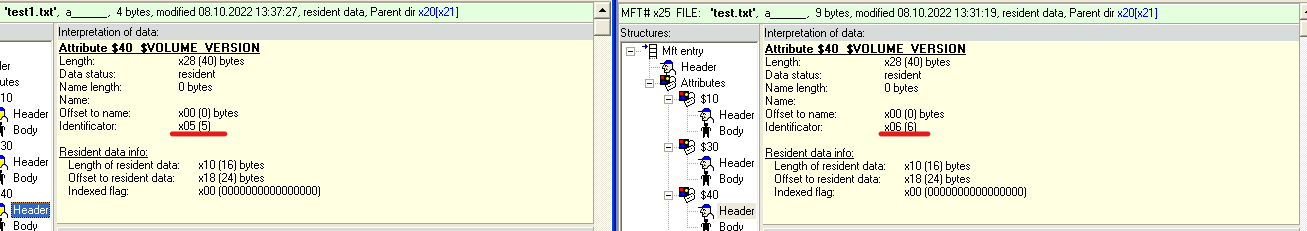


Теперь создадим еще один файл в той же папки и проверим его object\_id с помощью команды в терминале, а также просмотрим его в DiskExplorer:

Через терминал видим отличия (отметил на скриншоте):

 Через DiskExplorer:

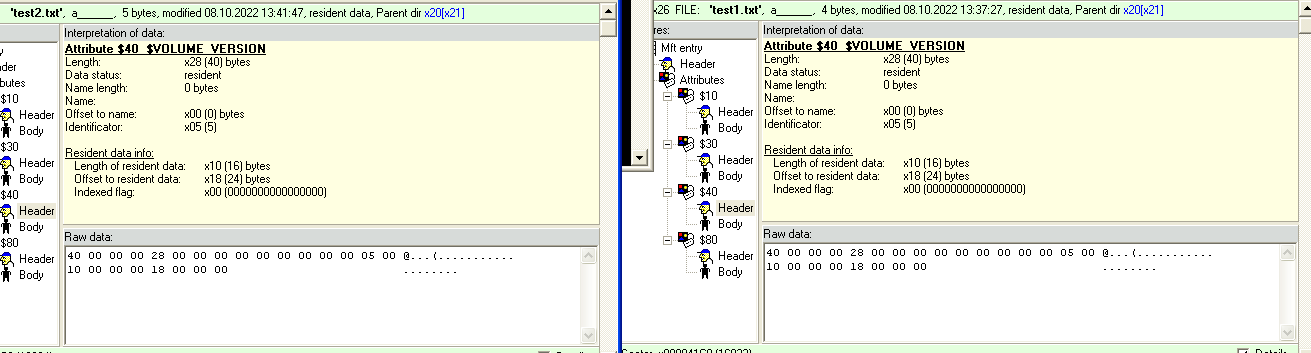
Через DiskExplorer:



Создадим третий файл и произведем те же действия:

Терминал:

Через DiskExplorer значения атрибутов второго и третьего файла совпадали, а через терминал нет:



**Упражнение по созданию именованного атрибута $DATA**

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

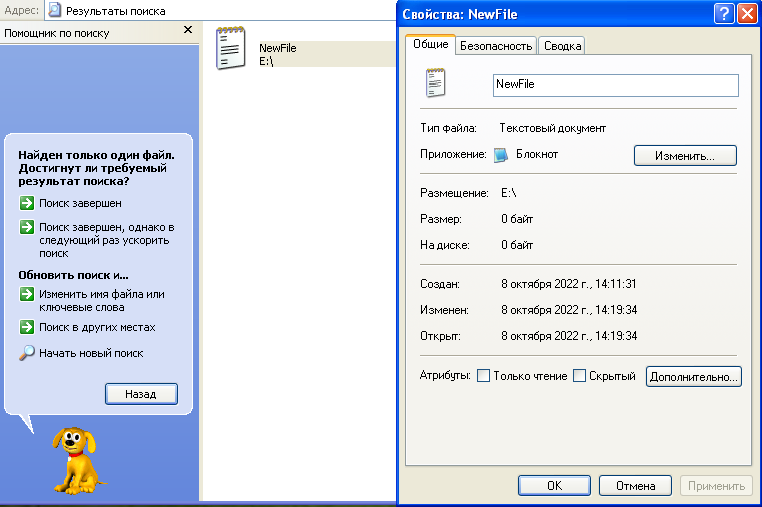
DIR > NewFile.txt: NewStream

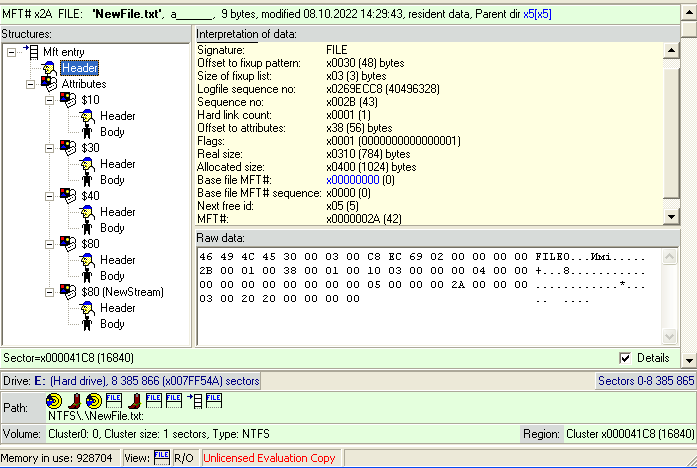
Ввел команду и сразу же создался файл:



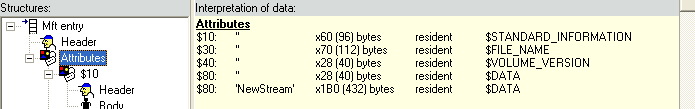
Найдите созданный файл с помощью проводника Windows и попытайтесь найти информацию о дополнительном потоке данных этого файла. Посмотрите, какой размер файла указывает проводник Windows. (Попутно можете ввести с помощью блокнота какой-нибудь текст в этот файл.) Теперь найдите созданный файл с помощью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

Итак, первым делом нашел созданный файл с помощью проводника, его размер составляет 0 байт:



Файл в MFT:

Новый поток соответствует атрибуту $80:



Поток пустым не является, его длина составляет 432 байта:

