Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное

образовательное учреждение высшего образования

«Комсомольский-на-Амуре государственный университет»

Факультет компьютерных технологий

Кафедра «МОП ЭВМ»

ЛАБОРАТОРНАЯ РАБОТА 6

по дисциплине «Операционные системы и оболочки»

## Исследование структуры NTFS

Студент группы 6ИСб-1 О. Хусейнов

Преподаватель В.А Тихомиров

2018

Цель: Изучить теоретические вопросы организации NTFS и провести экспериментальное восстановление «поврежденного файла» с раздела NTFS винчестера.

Задания:

1. С помощью программы DiskProbe исследовать структуру MFT на винчестере.
2. С помощью программы DiskProbe провести восстановление файла.

**Выполнение:**

В пункте меню «Drive» выбираем логический диск. В открывшимся окне выбираем диск С, на котором хранится файл, и нажимаем Set Active (рисунок 1).

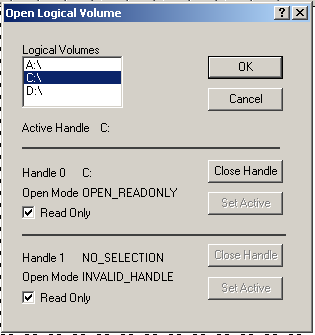


Рисунок 1 – Активность диска

Чтение происходит с диска С. После читаем первый сектор в Read и обнаруживаем нашу файловую систему NTFS. Переходим в режим просмотра NTFS (рисунок 2).

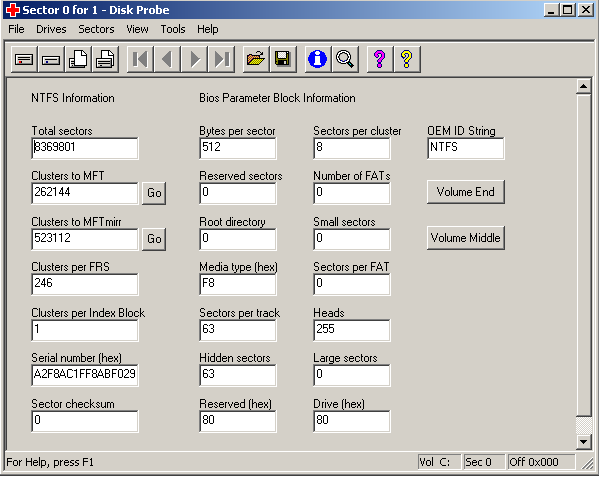


Рисунок 2 – Просмотр NTFS

Получаем данные о количестве секторов в кластере и переходим в MFT-раздел. Начинаем поиск файла. По окончанию поиска мы обнаруживаем сектор, в котором содержится запись о нашем файле (рисунок 3).

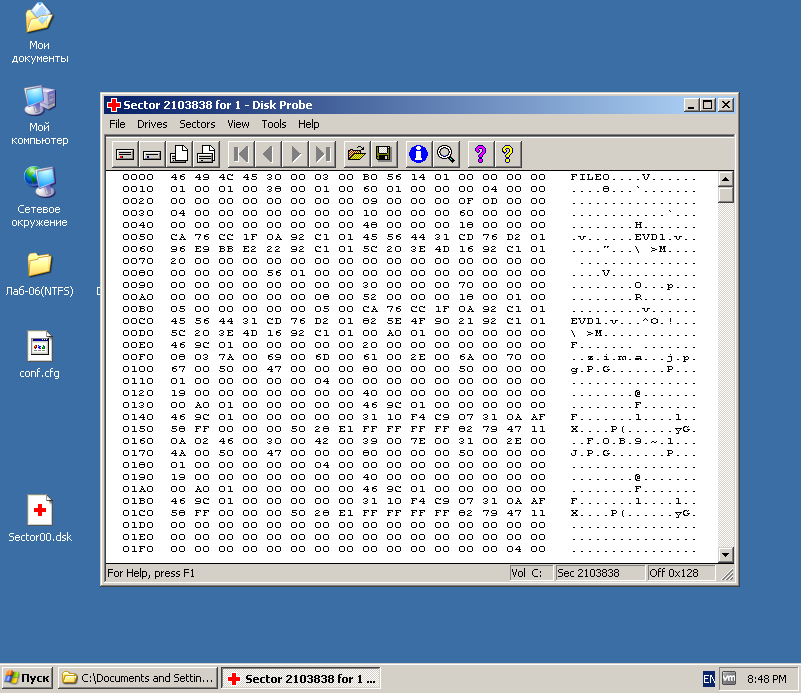


Рисунок 3 – Запись в MFT о файле

В найденном секторе содержится байтовая цепочка, которая представляет из себя последовательность экстендов(адресов), из которых мы можем определить номера секторов, содержащие данные нашего файлы по таблице 1. Определив номера секторов, можно найти части данных файла (рисунки 4-5).

Байтовая цепочка имеет вид: 31 10 F4 С9 07 31 0A AF 58 FF

Таблица 1

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| N | Длина экстенда | | Смещение экстенда | | Адрес экстенда | |
| кластера | сектора | кластера | сектора | кластера | сектора |
| 1 | 10 | 128 |  |  | 07С9F4 | 4083616 |
| 2 | A | 80 | FF58AF | 133875064 | 10722A3 | 17244835 |

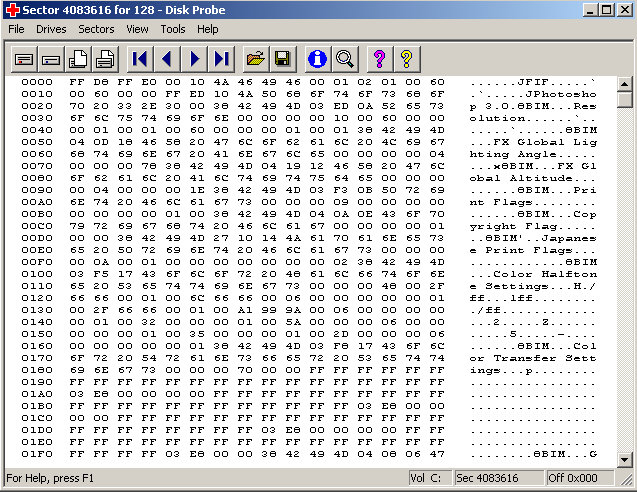


Рисунок 4 – Первая часть данных о картинке

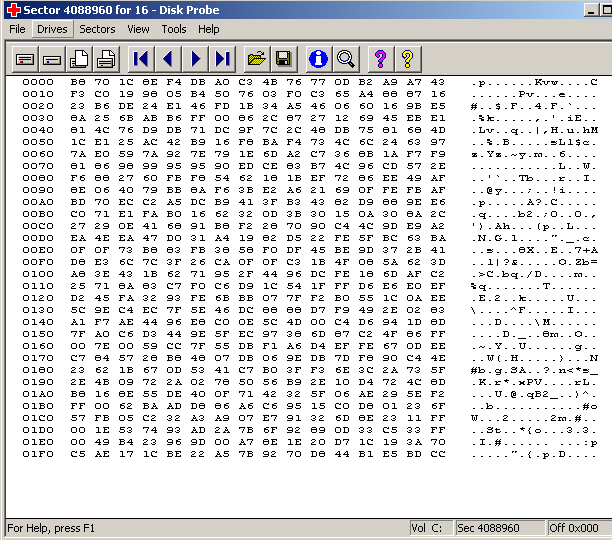


Рисунок 5 – Вторая часть данных о картинке

Найденные части следует сохранить, а после объединить воедино с помощью командной строки (рисунок 6).

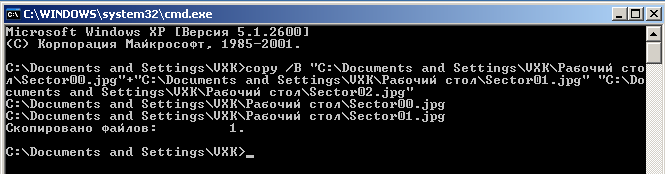


Рисунок 6 – Объединение частей

Итогом является готовая единая картинка (рисунок 7).



Рисунок 7 – Восстановленная картинка