УДК 681.3.07

ВОСТАНОВЛЕНИЕ ДАННЫХ НА ТОМЕ FAT

Разоренов Н.А.

В работе приводится анализ изменение элементов таблиц FAT, родительского каталога при выполнении над файлом команд COPY, MOVE, DEL на томе FAT32. Номер начального кластера файла определяем из Directory по FDT файла со смещением 1Ah относительно ее начала (Рис.1):

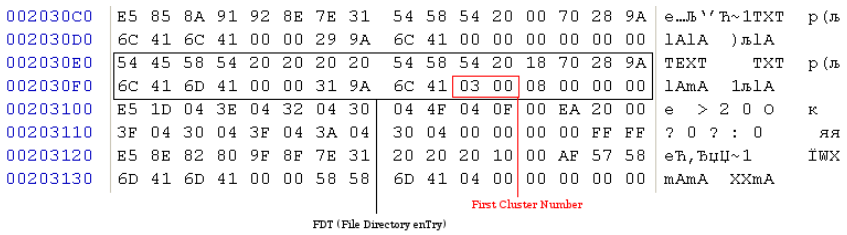
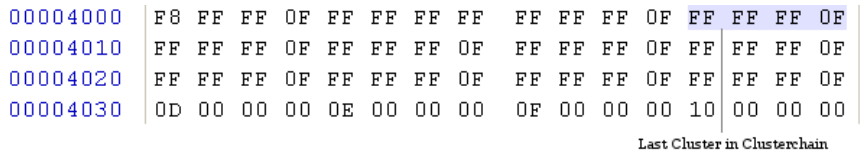


Рисунок 1 – Номер начального кластера

Номер следующего кластера файла находится в таблице FAT со смещением: начало_таблицы FAT + номер_первого_кластера_файла * 4. Если файл занимает несколько кластеров, то по этому смещению находится номер следующего кластера файла. Если же кластер является последним для файла, то значение элемента - 0FFFFFFFh.



Анализ записей каталога и элементов таблице FAT для команд move и delete показывает, что цепочка кластеров в FAT обнуляется, первый символ имени файла заменяется на E5(признак удаленной записи). Однако эти освобожденные кластера система использует не сразу, а выделяет другие кластера для уменьшения фрагментации. Таким образом имеется возможности восстановить удаленные данные.