

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):

002030C0	E5 85 8A 91 92 8E 7E 31	54 58 54 20 00 70 28 9A	e...л'л'л~1ТХТ	р (л)
002030D0	6C 41 6C 41 00 00 29 9A	6C 41 00 00 00 00 00 00	lAlA)лlA	
002030E0	54 45 58 54 20 20 20 20	54 58 54 20 18 70 28 9A	ТЕХТ ТХТ	р (л)
002030F0	6C 41 6D 41 00 00 31 9A	6C 41 03 00 08 00 00 00	lAmA lлlA	
00203100	E5 1D 04 3E 04 32 04 30	04 4F 04 0F 00 EA 20 00	e > 2 0 0	к
00203110	3F 04 30 04 3F 04 3A 04	30 04 00 00 00 00 FF FF	? 0 ? : 0	яя
00203120	E5 8E 82 80 9F 8F 7E 31	20 20 20 10 00 AF 57 58	eл, ллЦ~1	lWX
00203130	6D 41 6D 41 00 00 58 58	6D 41 04 00 00 00 00 00	mAmA XXmA	

FDT (File Directory enTry)

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 - 0FFFFFFh.

00004000	F8 FF FF 0F FF FF FF FF	FF FF FF 0F FF FF FF 0F	FF FF FF 0F
00004010	FF FF FF 0F FF FF FF 0F	FF FF FF 0F FF	FF FF 0F
00004020	FF FF FF 0F FF FF FF 0F	FF FF FF 0F FF	FF FF 0F
00004030	0D 00 00 00 0E 00 00 00	0F 00 00 00 10	00 00 00

Last Cluster in Clusterchain

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.