Файловая система NTFS

МЕТАФАЙЛЫ

В предыдущих сериях…

- Любые данные в файловой системе хранятся в виде файлов (как пользовательские, так и служебные)
- Файл в терминах NTFS представлен набором атрибутов
- Основные атрибуты файла: $Standard_Information, $File_Info, $Data, $Attribute_List

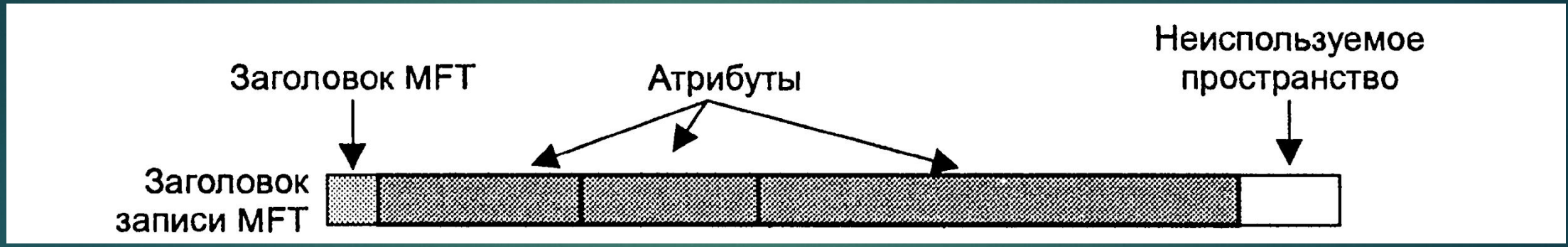
Категории данных

- Категория данных файловой системы – ***общая информация о файловой системе в целом***
- Категория данных содержимого – ***фактическое содержимое файла***
- Категория метаданных – ***различная служебная информация о состоянии файла/ов***
- Категория данных имен файлов – ***информация об именах файлов***
- Категория прикладных данных – ***описание различных специальных возможностей файловой системы***

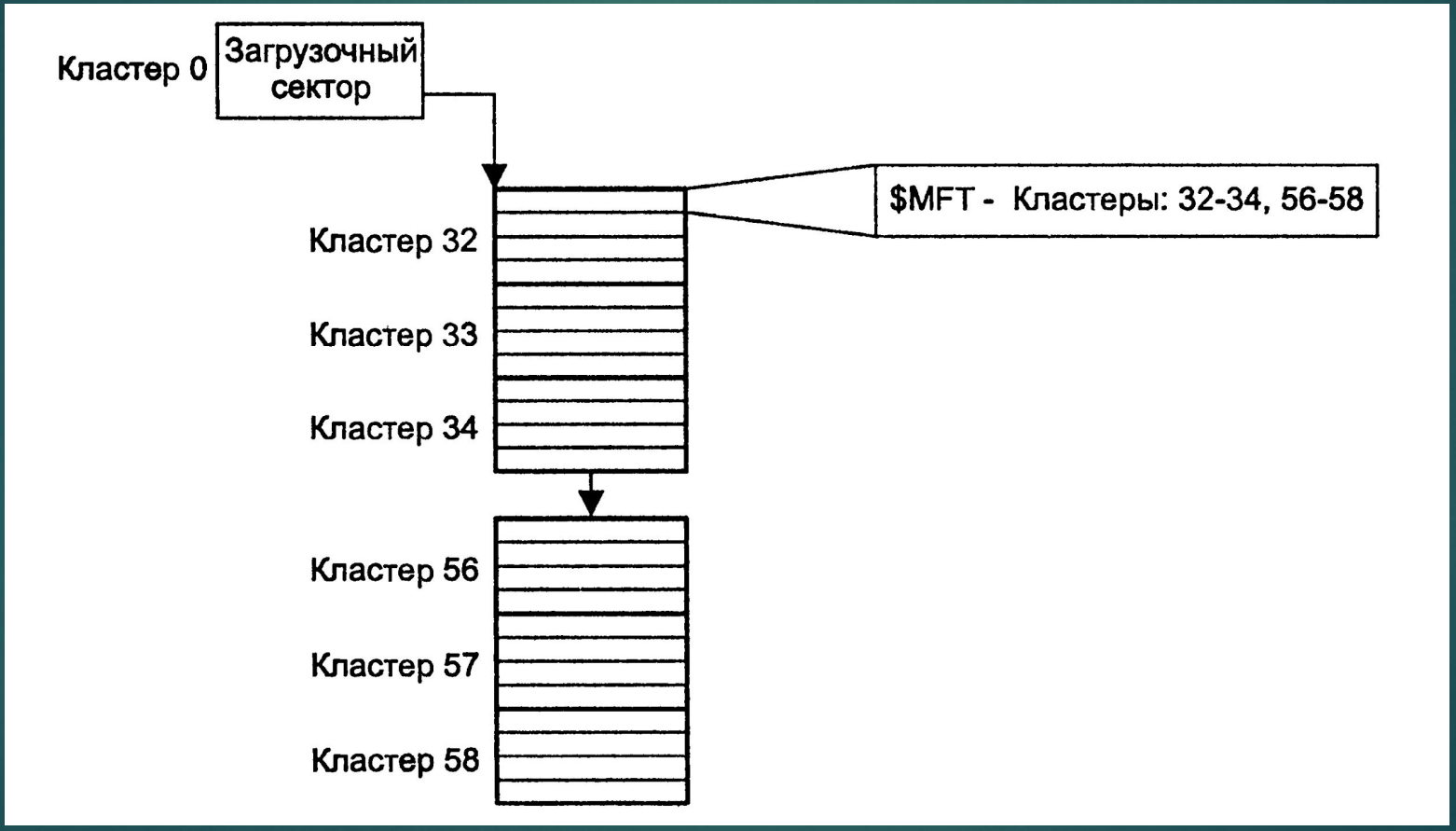
Взаимодействие пяти категорий данных

MFT

- MFT – сердце файловой системы



MFT и $MFT


Кластер 0
Загрузочный сектор
$MFT - Кластеры: 32-34, 56-58
Кластер 32
Кластер 33
Кластер 34
Кластер 56
Кластер 57
Кластер 58

Структура MFT-записи

Диапазон	Описание	Необходимость
0–3	Сигнатура («FILE»)	Нет
4–5	Смещение массива маркеров	Да
6–7	Количество элементов в массиве маркеров	Да
8–15	Номер LSN для $LogFile	Нет
16–17	Порядковый номер	Нет
18–19	Счетчик ссылок	Нет
20–21	Смещение первого атрибута	Да
22–23	Флаги (использования и каталога)	Да
24–27	Используемый размер записи MFT	Да
28–31	Выделенный размер записи MFT	Да
32–39	Адрес базовой записи	Нет
40–41	Идентификатор следующего атрибута	Нет
42–1023	Атрибуты и маркеры	Да

$Boot и $Volume

- $Boot ссылается на первый кластер файловой системы, хотя в реальности под загрузочную запись выделяется 16 секторов
- В NTFS может находится резервная копия NTFS boot sector, причем наиболее вероятные 3 места её расположения
- $Volume хранит в себе метку тома и идентификатор
  - $Volume_name – имя тома в кодировке Unicode UTF-16

```
0000000: 4e00 5400 4600 5300 2000 4400 6900 7300  N.T.F.S. .D.i.s.
0000016: 6b00 2000 3200                           k. .2.
```

  - $Volume_information

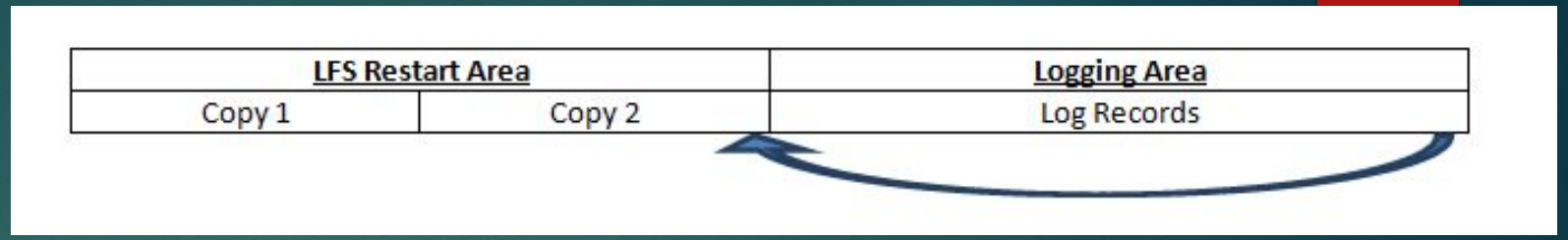
Диапазон	Описание	Необходимость
0–7	Не используется	Нет
8–8	Основная версия	Да
9–9	Дополнительная версия	Да
10–11	Флаги (см. табл. 13.22)	Нет

Значение	Описание
0x0001	Флаг обновления
0x0002	Изменение размера $LogFile (журнал файловой системы)
0x0004	Обновление тома
0x0008	Монтирование в NT
0x0010	Удаление журнала изменений
0x0020	Восстановление идентификаторов объектов
0x8000	Изменяется chkdsk

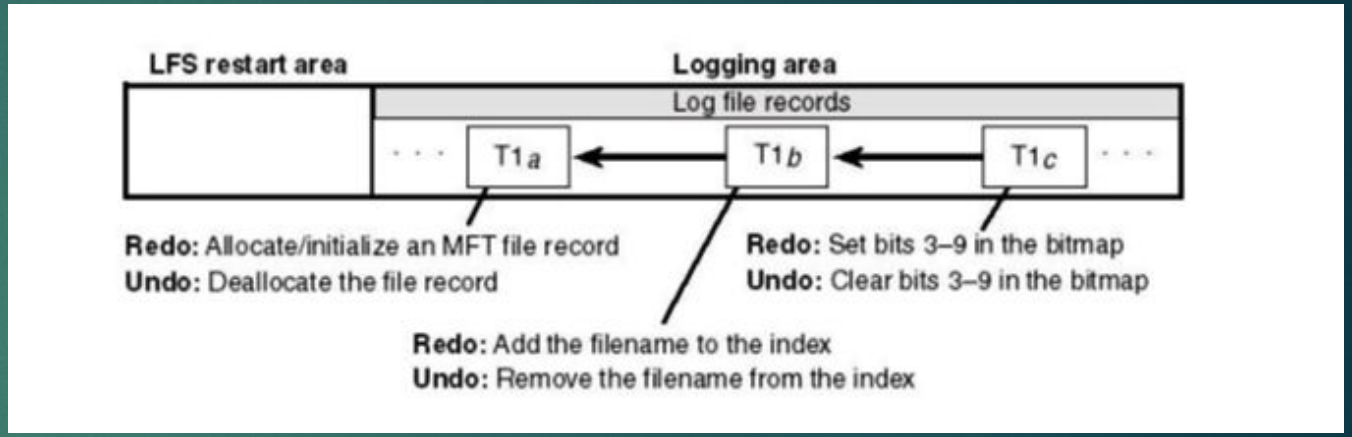
$BitMap

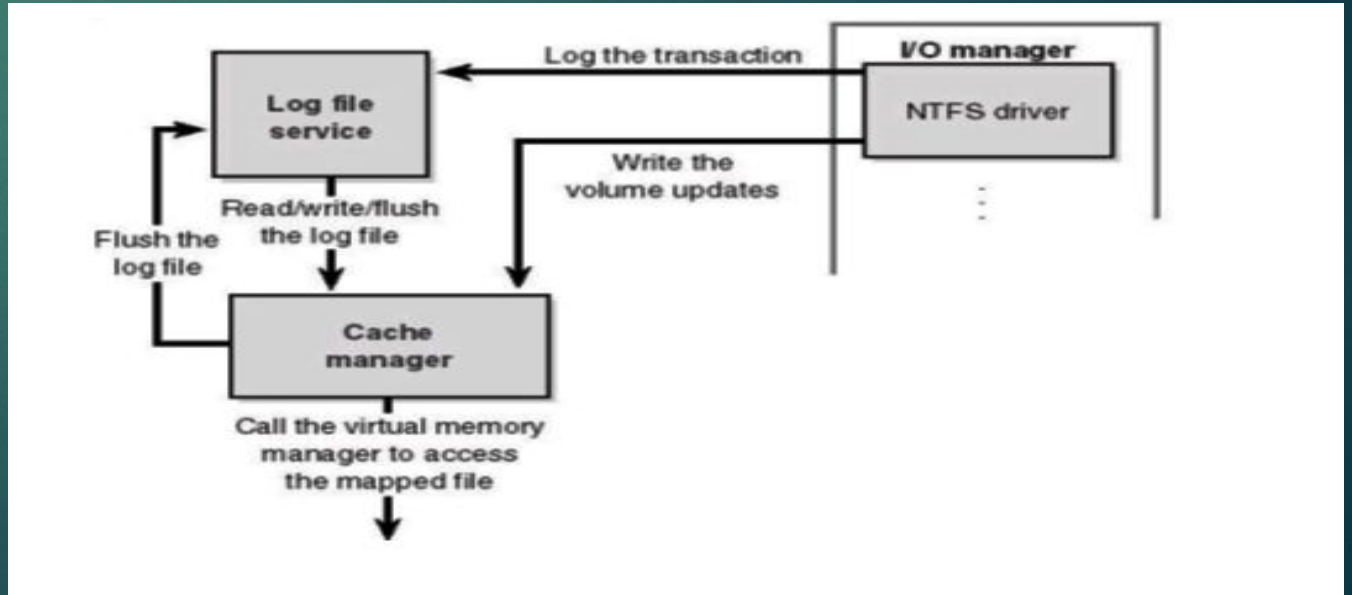
- Атрибут $DATA этого файла содержит один бит для каждого кластера файловой системы; например, бит 0 представляет кластер 0, а бит 1 представляет кластер 1. Если бит равен 1, значит, кластер выделен; если бит равен 0, кластер свободен.
- **ПРИМЕР:** Если кластер равен 2 секторам, то для NTFS Boot Sector в файле $Bitmap будет следующая картина:
  - ***1111 0000*** **……01001110001111**

$logFile



- Файл $LogFile (запись MFT 2) используется в качестве журнала NTFS. Он обладает стандартными файловыми атрибутами, а данные журнала хранятся в атрибуте $ DATA.
- Журнал делится на страницы по 4096 байт и хранит в себе информацию необходимую для восстановления тома в случае каких-либо проблем с записью
- В данный файл изменения записываются либо ядром ФС, либо ОС





$UsnJrnl

- В нем фиксируются изменения, вносимые в файлы. Имя файла журнала — \$Extend\$UsrJrnl
- Информация хранится в атрибуте $DATA. Имя этого атрибута — $J.
- Данные журнала не являются необходимыми для выполнения основных функций файловой системы — хранения и выборки данных.

Флаг	Описание
0x00000001	Перезапись атрибута $DATA по умолчанию
0x00000002	Расширение атрибута $DATA по умолчанию
0x00000004	Усечение атрибута $DATA по умолчанию
0x00000010	Перезапись именованного атрибута $DATA
0x00000020	Расширение именованного атрибута $DATA
0x00000040	Усечение именованного атрибута $DATA
0x00000100	Создание файла или каталога
0x00000200	Удаление файла или каталога

Флаг	Описание
0x00000400	Изменение расширенных атрибутов файла
0x00000800	Изменение дескриптора безопасности
0x00001000	Переименование — запись в журнале изменений содержит старое имя
0x00002000	Переименование — запись в журнале изменений содержит новое имя
0x00004000	Изменение состояния индексирования содержимого
0x00008000	Изменение основных атрибутов файла или каталога
0x00010000	Создание или удаление жесткой ссылки
0x00020000	Изменение состояния сжатия
0x00040000	Изменение состояния шифрования
0x00080000	Изменение идентификатора объекта
0x00100000	Изменение точки подключения
0x00200000	Создание, удаление или изменение именованного атрибута $DATA
0x80000000	Закрытие файла или каталога