

ДИСЦИПЛИНА

Операционные системы

(полное наименование дисциплины без сокращений)

ИНСТИТУТ

Институт информационных технологий

КАФЕДРА

информационных технологий в атомной энергетике

(полное наименование кафедры)

ВИД УЧЕБНОГО

Лекция

МАТЕРИАЛА

(в соответствии с пп 1-11)

ПРЕПОДАВАТЕЛЬ

Пугачев Андрей Васильевич

(фамилия, имя, отчество)

СЕМЕСТР

IV семестр 2024 – 2025 учебный год

(указать семестр обучения, учебный год)

# Лекция № 8: «Файловая система NTFS»

«Операционные системы»

МИРЭА – Российский технологический университет

Москва. 2024-2025 у.г.

# NTFS

Файловая система NTFS (англ. New Technology File System) была впервые представлена компанией Microsoft в 1993 году.

Разработка системы началась в 1991 году Брайном Андрю, Дэвидой Гейблом, Гари Кимурой и Томом Миллером.

Версии NTFS:

- ▶ 1.2 - Windows NT;
- ▶ 3.0 - Windows 2000;
- ▶ 3.1 - Windows XP и выше.

# Целями создания

## 1. Надежность:

- ▶ журналирования;
- ▶ контрольных точек / транзакций.

## 2. Безопасность:

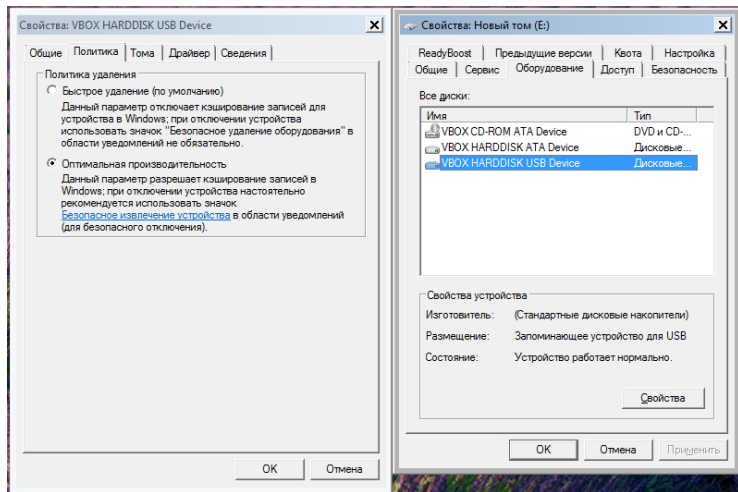
- ▶ журналирования;
- ▶ списки управления доступом (ACL);
- ▶ шифрование.

## 3. Поддержка томов большого объема.

# Как создать?

1. Использовать штатные средства ОС Windows для форматирования какого-нибудь носителя малого размера.
2. Создать образ носителя альтернативными средствами.

# Штатные средства



# Альтернативные средства

```
dd if=/dev/zero of=image.img bs=1M count=32  
mkfs.ntfs -F image.img
```

## Что читать...

1. Брайан Кэрриэ. "Криминалистический анализ файловых систем".
2. Исходные коды.



# Категория данных содержимого

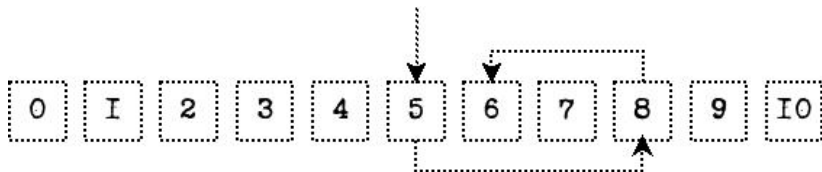
1. Битовые поля.
2. В-дерево.
3. Целочисленный тип.
4. Маркеры целостности.

# Битовые поля

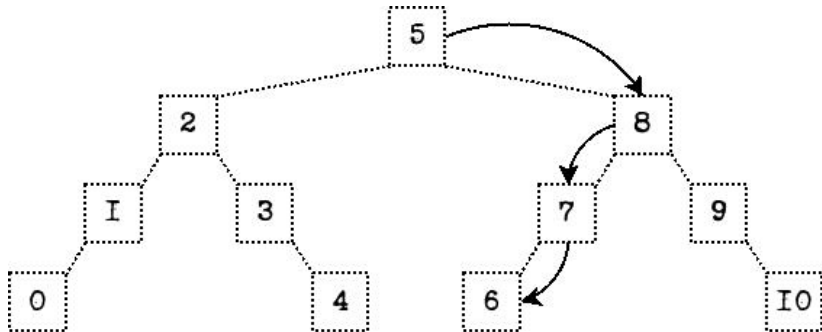
...

# В-деревья

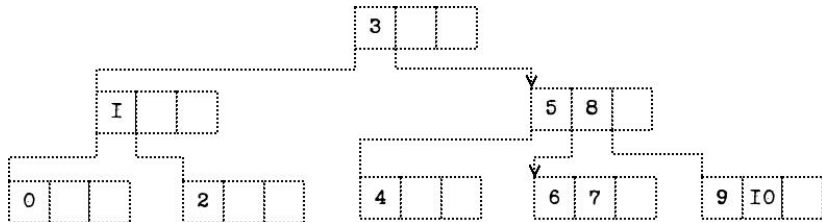
## Процесс бинарного поиска числа «6» в упорядоченном массиве



## Процесс поиска числа «6» в бинарном дереве



# В-деревья



## Целочисленный тип





# Целые числа Microsoft

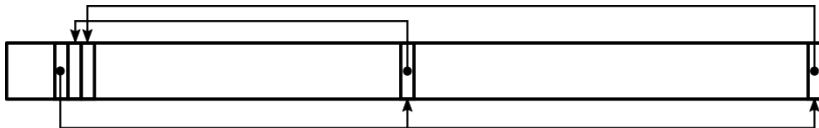
$$F(i) = \begin{cases} i, & \text{если } i \geq 0 \\ 2^i, & \text{если } i < 0 \end{cases}$$

## Маркеры целостности секторов

# Основной элемент

- ▶ массивом последовательности обновлений (англ. – Update Sequence Array).
- ▶ массивом маркеров.

# Процесс формирования массива маркеров



Записей главной файловой таблицы

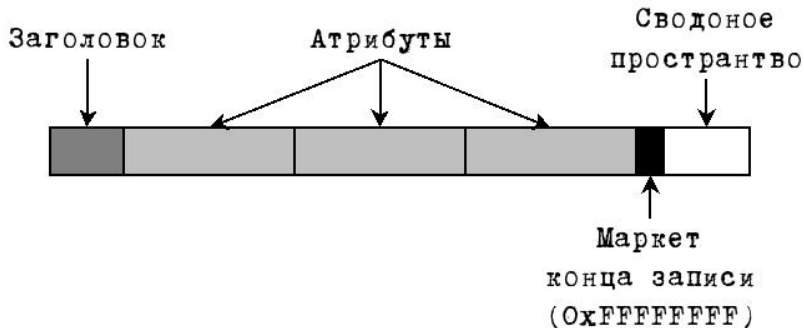
Все информация о файлах в рамках файловой системы NTFS сохраняется в специальной таблице, получившей названия Master File Table (далее – MFT).

# Структура записи

1. Заголовок.
2. Набор атрибутов. Заканчивается маркером конца записи - 0xFFFFFFFF.
3. Свободное пространство.



# Структура записи



# Структура записи

Смещение	Размер	Описание
0x00	4	Сигнатура
0x04	2	Смещение массива маркеров
0x06	2	Количество элементов массива маркеров
0x08	8	Номер записи в журнале транзакций (LSN)
0x10	2	Порядковый номер
0x12	2	Счетчик ссылок
0x14	2	Смещение первого атрибута
0x16	2	Флаги: 0x1 - запись используется
		0x2 - запись описывает каталог

Смещение	Размер	Описание
0x18	4	Используемый размер записи MFT
0x1C	4	Выделенный размер записи MFT
0x20	8	Адрес базовой записи MFT
0x28	2	Идентификатор для нового атрибута
0x2A	2	Зарезервировано
0x2C	4	Номер файловой записи

# Типы записи

Значения		Описание
HEX	ASCII	
0x454c4946	FILE	Обычная запись MFT
0x58444e49	INDX	Индексный массив
0x454c4f48	HOLE	Смысл поля чуть позже допишу....))))
0x444b4843	CHKD	Запись модифицирована утилитой chkdsk
0x44414142	BAAD	Запись битая

# Пример

0000:	4649	4c45	3000	0300	e022	I000	0000	0000	FILE0...."	Сигнатура ("FILE")
0010:	0100	0100	3800	0100	a001	0000	0004	0000	....8.....	Смещение массива маркеров (0x30)
0020:	0000	0000	0000	0000	0600	0000	0000	0000	.....\`....	Количество элементов массива маркеров (3)
0030:	0300	ffff	0000	0000	I000	0000	6000	0000	.....Н.....	Номер для журнала транзакций (0x1022e0)
0040:	0000	I800	0000	0000	4800	0000	I800	0000	T....s..T....s..	Порядковый номер (I)
0050:	540e	feb5	II73	d601	540e	feb5	II73	d601	T....s..T....s..	Счетчик ссылок (I)
0060:	540e	feb5	II73	d601	540e	feb5	II73	d601	.....0...h...	Смещение первого атрибута (0x38)
0070:	0600	0000	0000	0000	0000	0000	0000	0000	.....J.....	Флаги (0xI - запись используется)
0080:	0000	0000	0001	0000	0000	0000	0000	0000	.....T....s..	Используемый размер записи MFT (0xIa0 = 416)
0090:	0000	0000	0000	0000	3000	0000	6800	0000	T....s..T....s..	Выделенный размер записи MFT (0x400 = I024)
00a0:	0000	I800	0000	0300	4a00	0000	I800	0100	.....?.....	Адрес базовой записи MFT (0)
00b0:	0500	0000	0000	0500	540e	feb5	II73	d601	.....@.....	Идентификатор для нового атрибута (0x6)
00c0:	540e	feb5	II73	d601	540e	feb5	II73	d601	..\$.M.F.T.....	Номер файловой записи (0)
00d0:	540e	feb5	II73	d601	0040	0000	0000	0000	.....!@U.....P..	Массив маркеров
00e0:	0040	0000	0000	0000	0600	0000	0000	0000	.....@.....	АТРИБУТЫ
00f0:	0403	2400	4d00	4600	5400	0000	0000	0000	.....@.....	Маркером конца записи
0100:	8000	0000	4800	0000	0100	4000	0000	0100	.....!@U.....	Контрольные маркеры
0110:	0000	0000	0000	0000	3100	0000	0000	0000	.....T....!	СВОБОДНОЕ ПРОСТРАНСТВО
0120:	4000	0000	0000	0000	0000	0400	0000	0000	.....`.....	
0130:	0000	0400	0000	0000	0000	0400	0000	0000	.....!@U.....	
0140:	2140	5514	0018	ffff	b000	0000	5000	0000	.....P.....@.....	
0150:	0100	4000	0000	0500	0000	0000	0000	0000	.....@.....	
0160:	0100	0000	0000	0000	4000	0000	0000	0000	.....@.....	
0170:	0020	0000	0000	0000	0810	0000	0000	0000	.....T....!	
0180:	0810	0000	0000	0000	2101	5414	2101	fe1d	.....`.....	
0190:	009e	6002	801a	ffff	ffff	ffff	0000	0000	.....!@U.....	
01a0:	0000	0400	0000	0000	2140	5514	0018	ffff	.....P.....@.....	
01b0:	b000	0000	5000	0000	0100	4000	0000	0500	.....@.....	
01c0:	0000	0000	0000	0000	0100	0000	0000	0000	.....@.....	
01d0:	4000	0000	0000	0000	0020	0000	0000	0000	.....@.....	
01e0:	0810	0000	0000	0000	0810	0000	0000	0000	.....T....!	
01f0:	2101	5414	2101	fe1d	009e	6002	801a	0300	.....T....!	
0200:	ffff	ffff	0000	0000	0000	0000	0000	0000	.....`.....	
0210:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
0220:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
0230:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
0240:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
0250:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
0260:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
0270:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
0280:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
0290:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
02a0:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
02b0:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
02c0:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
02d0:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
02e0:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
02f0:	0000	0000	0000	0000	0000	0000	0000	0000	.....@.....	
0300:	0000	0000	0000	0000	0000	0000	0000	0300	.....@.....	

# Атрибуты

# Виды атрибутов

- ▶ резидентным;
- ▶ нерезидентным.

# Структура резидентного атрибута

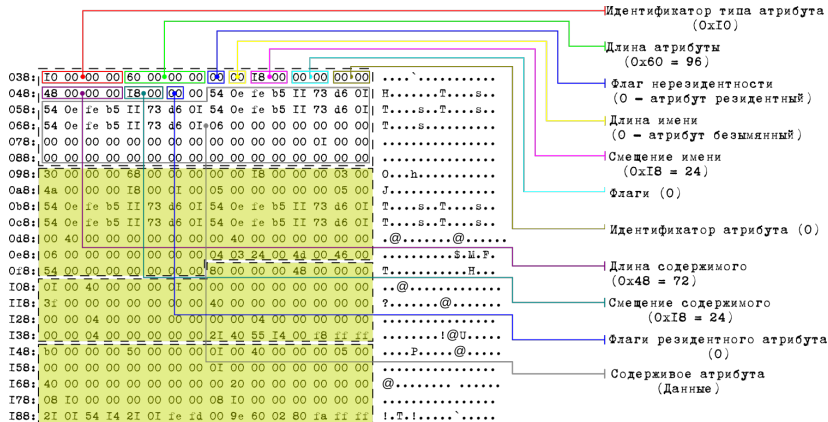
Смещение	Размер	Описание
0x00	4	Идентификатор типа атрибута
0x04	4	Длина атрибуты
0x08	1	Флаг нерезидентности (0 - резидентный)
0x09	1	Длина имени (0 - атрибут безымянный)
0x0A	2	Смещение имени
0x0C	2	Флаги
0x0E	2	Идентификатор атрибута
0x10	4	Длина содержимого
0x14	2	Смещение содержимого
0x16	1	Флаги резидентного атрибута
0x17	1	Зарезервированно



# Флаги

- ▶ 0x4000 – данные атрибута хранятся в зашифрованном виде;
- ▶ 0x8000 – атрибут является разреженным;
- ▶ 0x1 – данные атрибута сжаты.

# Пример



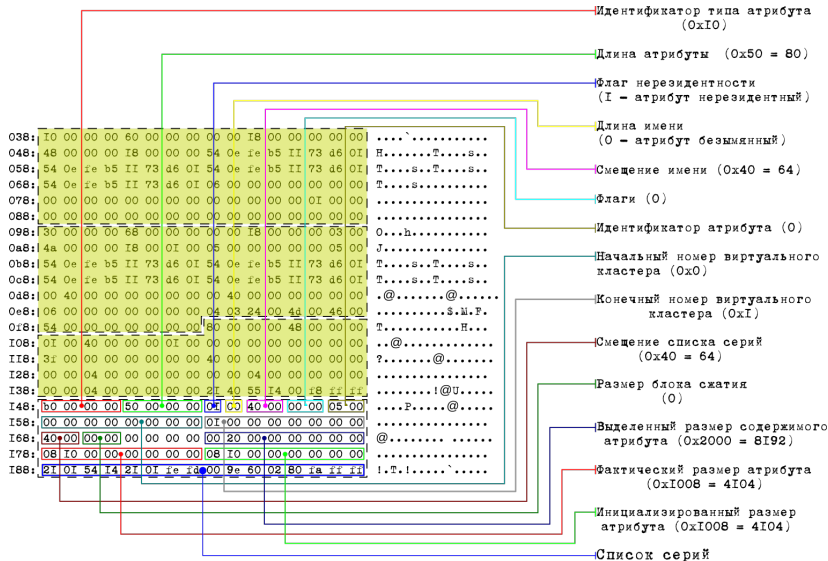
# Структура нерезидентного атрибута

Смещение	Размер	Описание
0x00	4	Идентификатор типа атрибута
0x04	4	Длина атрибуты
0x08	1	Флаг нерезидентности (1 - нерезидентный)
0x09	1	Длина имени (0 - атрибут безымянный)
0x0A	2	Смещение имени
0x0C	2	Флаги
0x0E	2	Идентификатор атрибута
0x10	8	Номер начального виртуального кластера
0x18	8	Конечные номер виртуального кластера

# Структура нерезидентного атрибута

Смещение	Размер	Описание
0x20	2	Смещение списка серий
0x22	2	Размер блока сжатия
0x24	4	Не используется
0x28	8	Выделенный размер содержимого атрибута
0x30	8	Фактический размер атрибута
0x38	8	Инициализированный размер атрибута
0x40	8	Размер атрибута после сжатия (только у сжатых атрибутов)

# Пример

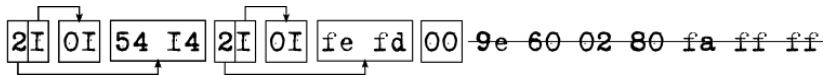


## Список серий

Список серий – это набор из элементов переменной длины, но общей структуры, последовательно размещенные друг за другом. Элементы предназначены для описания последовательностей (серий) кластеров, в которых располагаются данные атрибута.

+	-----+	-----+	-----+	+
	Старший		Младший	
+	-----+	-----+	-----+	+
	Не ноль		Не ноль	
+	-----+	-----+	-----+	+
	Ноль		Не ноль	
+	-----+	-----+	-----+	+
	Ноль		Ноль	
+	-----+	-----+	-----+	+
	Не ноль		Ноль	
+	-----+	-----+	-----+	+

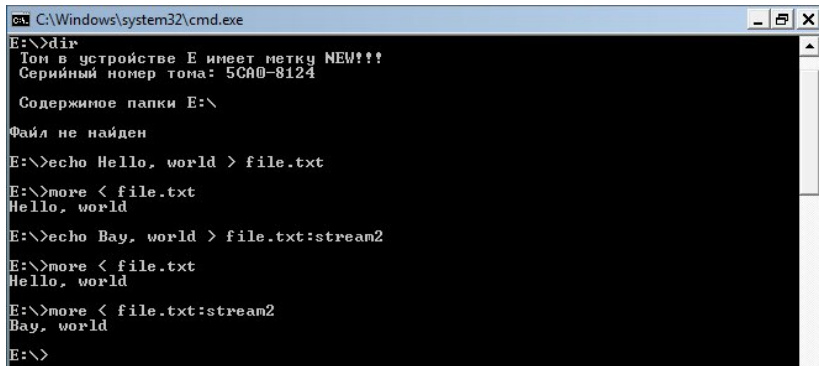
# Пример





# Альтернативные стримы

# Создание альтернативного стрима

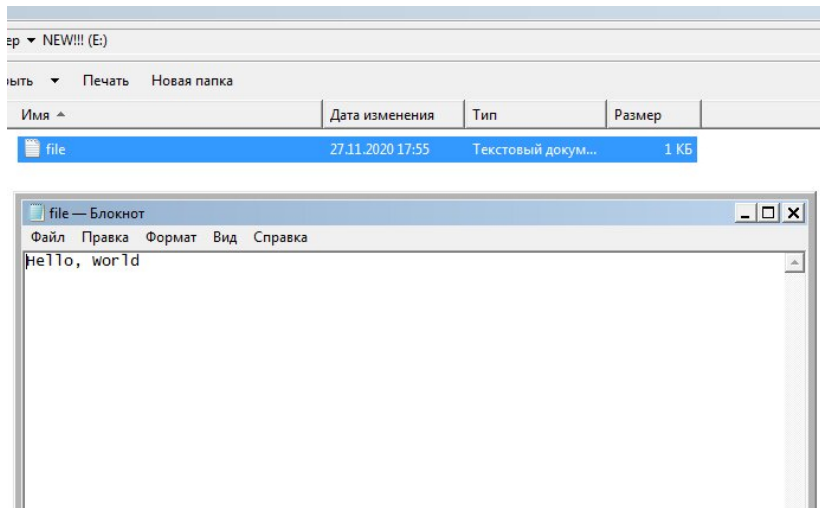


```
C:\Windows\system32\cmd.exe
E:\>dir
Том в устройстве E имеет метку NEW!!!
Серийный номер тома: 5CA0-8124

Содержимое папки E:\

Файл не найден
E:\>echo Hello, world > file.txt
E:\>more < file.txt
Hello, world
E:\>echo Bay, world > file.txt:stream2
E:\>more < file.txt
Hello, world
E:\>more < file.txt:stream2
Bay, world
E:\>
```

# Внутри фаловой записи



# Внутри фаловой записи

000	46 49 4c 45 30 00 03 00	ad ba 10 00 00 00 00 00	FILE0.....
010	04 00 01 00 38 00 01 00	98 01 00 00 00 04 00 00	.....8.....
020	00 00 00 00 00 00 00 00	07 00 00 00 28 00 00 00	.....(.....
030	04 00 00 00 00 00 00 00	10 00 00 00 60 00 00 00	.....
040	00 00 00 00 00 00 00 00	48 00 00 00 18 00 00 00	.....H.....
050	i4 1c 78 54 ad c4 d6 01	0c 0d 34 b3 ad c4 d6 01	..xT.....4....
060	0c 0d 34 b3 ad c4 d6 01	i4 1c 78 54 ad c4 d6 01	..4.....xT....
070	20 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
080	00 00 00 00 0d 01 00 00	00 00 00 00 00 00 00 00	.....
090	00 00 00 00 00 00 00 00	30 00 00 00 70 00 00 00	.....0.....p..
0a0	00 00 00 00 00 00 04 00	52 00 00 00 18 00 01 00	.....R.....
0b0	05 00 00 00 00 00 05 00	i4 1c 78 54 ad c4 d6 01	.....xT.....
0c0	i4 1c 78 54 ad c4 d6 01	i4 1c 78 54 ad c4 d6 01	..xT.....xT....
0d0	i4 1c 78 54 ad c4 d6 01	00 00 00 00 00 00 00 00	..xT.....
0e0	00 00 00 00 00 00 00 00	20 00 00 00 00 00 00 00	.....
0f0	08 03 66 00 69 00 6c 00	65 00 2e 00 74 00 78 00	..f..i..e...t..x..
100	74 00 58 00 54 00 42 04	40 00 00 00 28 00 00 00	t..X..T..B..@...(..
110	00 00 00 00 00 00 05 00	10 00 00 00 18 00 00 00	.....
120	c6 ff 57 1a 87 30 eb 11	8a 61 08 2a 27 7d b3 da	...w..o.....'}.
130	80 00 00 00 28 00 00 00	00 00 18 00 00 00 01 00	.....(.....
140	0f 00 00 00 18 00 00 00	48 65 6c 6c 61 2c 20 77	.....Hello, w...
150	61 22 6c 64 21 21 21 00	80 60 00 00 38 00 00 00	...orld!!!.....8...
160	00 07 18 00 00 00 06 00	0f 00 00 00 28 00 00 00	.....(.....
170	73 00 74 00 72 00 65 00	61 00 6d 00 32 00 39 04	s..t..r..e..a..m..2..9..
180	22 42 61 79 2c 20 77 61	72 6c 64 22 20 0d 0a 04	"Bay, world".....
190	ff ff ff ff 82 79 47 11	74 00 00 00 00 00 00 00	.....yG..t.....
1a0	80 00 00 00 18 00 00 00	00 00 18 00 00 00 01 00	.....
1b0	00 00 00 00 18 00 00 00	ff ff ff ff 82 79 47 11	.....yG.....
1c0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
*			
1f0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 04 00	.....
200	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
*			
3f0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 04 00	.....

Длина имени

Смещение имени

Длина данных

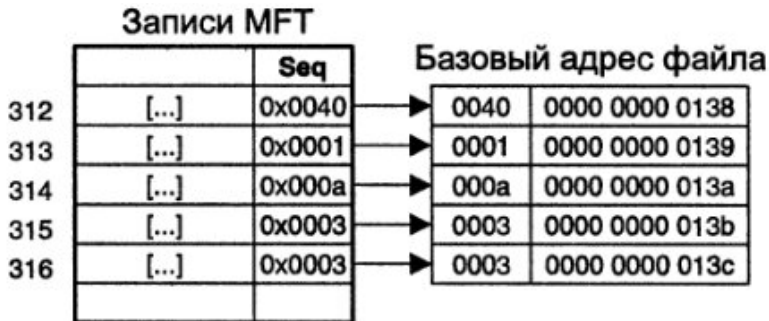
Смещение данных

Имя

Данные

# Таблица MFT

## Базовый номер записи



## После форматирования...

Где форматировали	Число использованных записей
Windows	31
Linux	18

## Основные записи



## Запись № 0

### \$MFT

Файл, который хранит данные таблицы MFT.

Свойство	Windows	Linux
Общие атрибуты	STANDARD_INFORMATION, FILE_NAME, DATA, BITMAP	
Размещение блоков данных	5205	4
Размеры блоков данных	64	7
Идентификатор нового атрибута	6	4

# Запись № 1

## \$MFTMirr

Файл, в котором хранятся первые несколько записей таблицы MFT. Предполагалось, что будет использоваться для восстановления повреждений в оригинальной таблице.

Свойство	Windows	Linux
Общие атрибуты	STANDARD_INFORMATION, FILE_NAME, DATA	
Размещение блоков данных	2	7807
Размеры блоков данных	1	1
Идентификатор нового атрибута	4	3

## Запись № 2

### \$LogFile

Журнал файловой системы.

Свойство	Windows	Linux
Общие атрибуты	STANDARD_INFORMATION, FILE_NAME, DATA	
Размещение блоков данных	4178	7808
Размеры        блоков данных	512	512
Идентификатор нового атрибута	4	3

## Запись № 3

### \$Volume

Файл используется для хранения данных о том... версия файловой системы, информация о неверном отключении, метка тома.

Свойство	Windows	Linux
Общие атрибуты	STANDARD_INFORMATION, DATA, FILE_NAME, SECURITY_DESCRIPTOR, VOLUME_NAME, VOLUME_INFORMATION	
Частные атрибуты	OBJECT_ID	
Размещение блоков данных	—	—
Размеры блоков данных	—	—
Идентификатор нового атрибута	7	6

## Запись № 4

### \$AttrDef

Файл содержит название и идентификаторы всех атрибутов, которые могут применяться в файловой системе.

Свойство	Windows	Linux
Общие атрибуты	STANDARD_INFORMATION, DATA, FILE_NAME, SECURITY_DESCRIPTOR	
Размещения блоков данных	4756	1958
Размеры блоков данных	1	1
Идентификатор нового атрибута	5	4

## Запись № 5

### Корневая директория

Свойство	Windows	Linux
Общие атрибуты	STANDARD_INFORMATION, BITMAP, FILE_NAME, SECURITY_DESCRIPTOR, INDEX_ROOT, INDEX_ALLOCATION	
Частные атрибуты	LOGGED_UTILITY_STREAM	
Размещения блоков данных	44	1957
Размеры блоков данных	1	1
Идентификатор нового атрибута	10	6

## Запись № 6

### \$Bitmap

Файл содержит битовое поле, используемое для идентификации свободных и занятых кластеров в системе.

Свойство	Windows	Linux
Общие атрибуты	STANDARD_INFORMATION, DATA, FILE_NAME	
Размещение блоков данных	5202	1959
Размеры блоков данных	1	1
Идентификатор нового атрибута	5	3

## Запись № 7

### \$Boot

Файл, хранящий данные загрузочной области и совпадающей с ней. Единственный файл в файловой системе, размещение которого четко определено для томов любой конфигурации.

Свойство	Windows	Linux
Общие атрибуты	STANDARD_INFORMATION, DATA, FILE_NAME, SECURITY_DESCRIPTOR	
Размещение блоков данных	0	0
Размеры блоков данных	2	2
Идентификатор нового атрибута	4	4



# Загрузочный сектор

Адрес \$MFT	Размер сектора	Размер кластера		Адрес \$MFTMirr	Размер записи MFT
0000	eb 52 90 4e 54 46 53 20	20 20 20 00 02 08 00 00	.R.NTFS.....		
0010	00 00 00 00 00 00 f8 00 00	3f 00 ff 00 80 00 00 00	.....?.....		
0020	00 00 00 00 00 80 00 80 00	ff e7 01 00 00 00 00 00	.....		
0030	55 14 00 00 00 00 00 00	02 00 00 00 00 00 00 00	U.....		
0040	f6 00 00 00 01 00 00 00	e4 e7 b6 a4 10 b7 a4 e0	.....		
0050	00 00 00 00 00 fa 33 c0 8e	d0 bc 00 7c fb 68 c0 07	.....3..... h..		
0060	If Ie 68 66 00 cb 88 I6	0e 00 66 81 3e 03 00 4e	..hf.....f.>..N		
0070	54 46 53 75 I5 b4 41 bb	aa 55 cd I3 72 0c 81 fb	TFSu..A..U..r...		
0080	55 aa 75 06 f7 c1 01 00	75 03 e9 dd 00 Ie 83 ec	U.u.....u.....		
0090	I8 68 Ia 00 b4 48 8a I6	0e 00 8b f4 I6 If cd I3	.h...H.....		
00a0	9f 83 c4 I8 9e 58 If 72	eI 3b 06 0b 00 75 db a3	.....X.r;...u..		
00b0	0f 00 c1 2e 0f 00 04 Ie	5a 33 db b9 00 20 2b c8	.....Z3... +..		
00c0	66 ff 06 II 00 03 I6 0f	00 8e c2 ff 06 I6 00 e8	f.....		
00d0	4b 00 2b c8 77 ef b8 00	bb cd Ia 66 23 c0 75 2d	K.+w.....f#..u-		
00e0	66 81 fb 54 43 50 41 75	24 81 f9 02 01 72 Ie I6	f..TCPau\$.....r..		
00f0	68 07 bb I6 68 70 0e I6	68 09 00 66 53 66 53 66	h...hp..h..fSfSf		
0100	55 I6 I6 I6 68 b8 01 66	61 0e 07 cd Ia 33 c0 bf	U...h..fa....3..		
0110	28 I0 b9 d8 0f fc f3 aa	e9 5f 01 90 90 66 60 Ie	(......_...f`.		
0120	06 66 a1 II 00 66 03 06	Ic 00 Ie 66 68 00 00 00	.f...f.....fh...		
0130	00 66 50 06 53 68 01 00	68 I0 00 b4 42 8a I6 0e	.fP.Sh..h...B...		
0140	00 I6 If 8b f4 cd I3 66	59 5b 5a 66 59 66 59 If	.....fY[ZfYfY.		
0150	0f 82 I6 00 66 ff 06 II	00 03 I6 0f 00 8e c2 ff	....f.....		
0160	0e I6 00 75 bc 07 If 66	61 c3 a0 f8 01 e8 09 00	...u...fa.....		
0170	a0 fb 01 e8 03 00 f4 eb	fd b4 01 8b f0 ac 3c 00	.....<..		
0180	74 09 b4 0e bb 07 00 cd	I0 eb f2 c3 0d 0a 41 20	t.....A..		
0190	64 69 73 6b 20 72 65 61	64 20 65 72 72 6f 72 20	disk read error		
01a0	6f 63 63 75 72 72 65 64	00 0d 0a 42 4f 4f 54 4d	occurred...BOOTM		
01b0	47 52 20 69 73 20 6d 69	73 73 69 6e 67 00 0d 0a	GR is missing...		
01c0	42 4f 4f 54 4d 47 52 20	69 73 20 63 6f 6d 70 72	BOOTMGR is compr		
01d0	65 73 73 65 64 00 0d 0a	50 72 65 73 73 20 43 74	essed...Press Ct		
01e0	72 6c 2b 41 6c 74 2b 44	65 6c 20 74 6f 20 72 65	rl+Alt+Del to re		
01f0	73 74 61 72 74 0d 0a 00	8c a9 be d6 00 00 55 aa	start.....U..		

## Запись № 8

### \$BadClus

Файл содержит «плохие» кластера файловой системы. Содержит два потока данных.

Свойство	Windows	Linux
Общие атрибуты	STANDARD_INFORMATION, DATA, FILE_NAME	
Размещение блоков данных	-, 0	-, 0
Размеры блоков данных	15615	15615
Идентификатор нового атрибута	5	4

## Подробная информация по файловой записи №8

```
$ istat -f ntfs ntfs.img 8
MFT Entry Header Values:
Entry: 8          Sequence: 8
$LogFile Sequence Number: 1057784
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256 (S-1-5-18)
Created:          2020-08-15 14:38:15.897250000 (-00)
File Modified:    2020-08-15 14:38:15.897250000 (-00)
MFT Modified:     2020-08-15 14:38:15.897250000 (-00)
Accessed:         2020-08-15 14:38:15.897250000 (-00)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $BadClus
Parent MFT Entry: 5      Sequence: 5
Allocated Size: 0        Actual Size: 0
Created:          2020-08-15 14:38:15.897250000 (-00)
File Modified:    2020-08-15 14:38:15.897250000 (-00)
MFT Modified:     2020-08-15 14:38:15.897250000 (-00)
Accessed:         2020-08-15 14:38:15.897250000 (-00)

Attributes:
Type: $STANDARD_INFORMATION (16-0)  Name: N/A  Resident  size: 72
Type: $FILE_NAME (48-3)             Name: N/A  Resident  size: 82
Type: $DATA (128-2)                  Name: N/A  Resident  size: 0
Type: $DATA (128-1)                  Name: $Bad  Non-Resident  size: 63959040  init_size: 0
```

sleuthkit

## Запись № 9

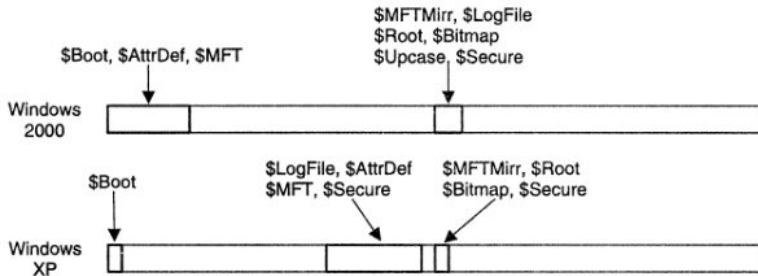
### \$Secure

Файл хранит информацию об дескрипторах безопасности

Свойство	Windows	Linux
Общие атрибуты	STANDARD_INFORMATION, DATA, FILE_NAME	
Размещение блоков данных	4691	1960
Размеры        блоков данных	65	65
Идентификатор нового атрибута	15	4

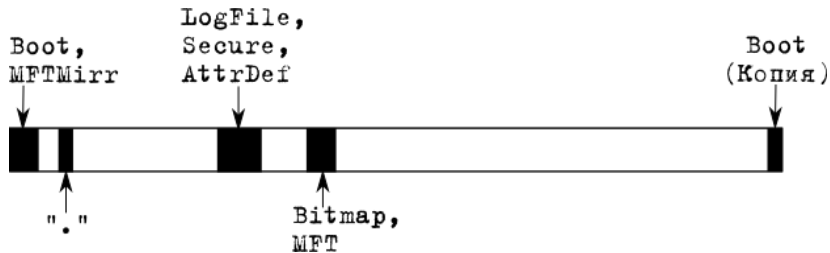
# Структура тома

# Структура тома по книжке

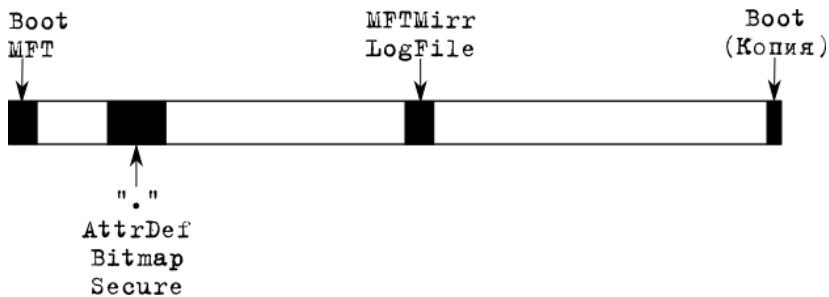


**Рис. 12.2.** Структура метаданных файловой системы, отформатированной в Windows 2000 и Windows XP

# Структура тома по Windows



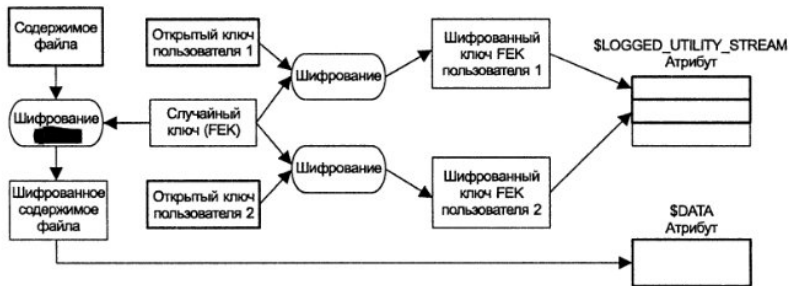
# Структура тома по Linux



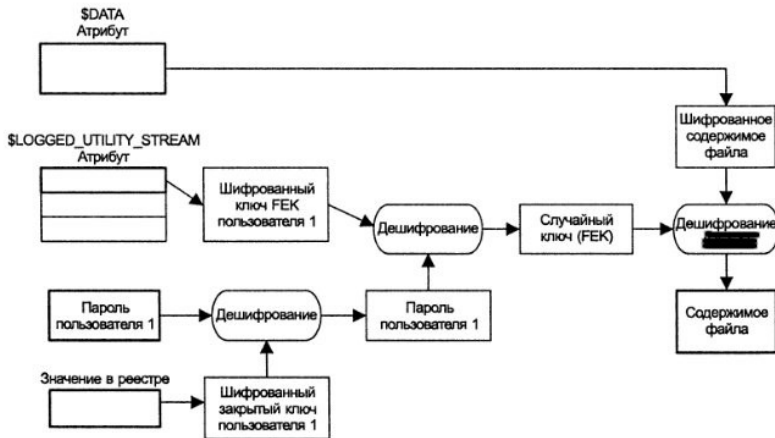


# Шифрование

## Процесс зашифрования атрибута



# Процесс расшифрования атрибута



# Транзакция

## Определение

Транзакция (англ. transaction, от лат. transactio — соглашение, договор) — минимальная логически осмысленная операция, которая имеет смысл и может быть совершена только полностью.

## Проблема

Doppelganger

# Вопросы?