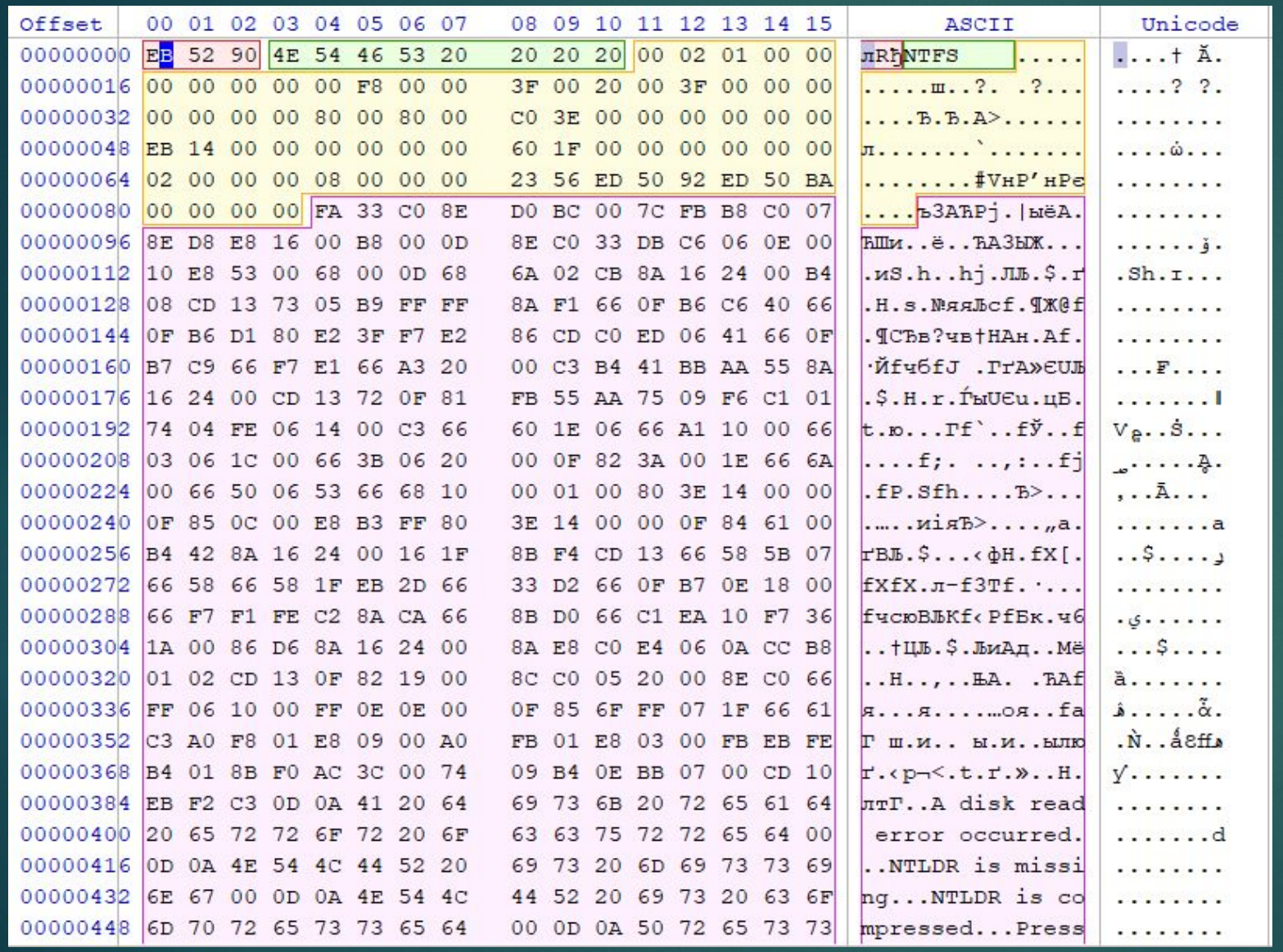
Файловая система NTFS: Атрибуты

В предыдущих сериях…

- ВСЕ ДАННЫЕ – ФАЙЛЫ ⟶ все данные в NTFS представлены в виде файлов (даже служебная информация)
- MFT – ядро файловой системы. Состоит из файловых записей (File Records) по 1024 байта (точно определяется в NTFS boot record)

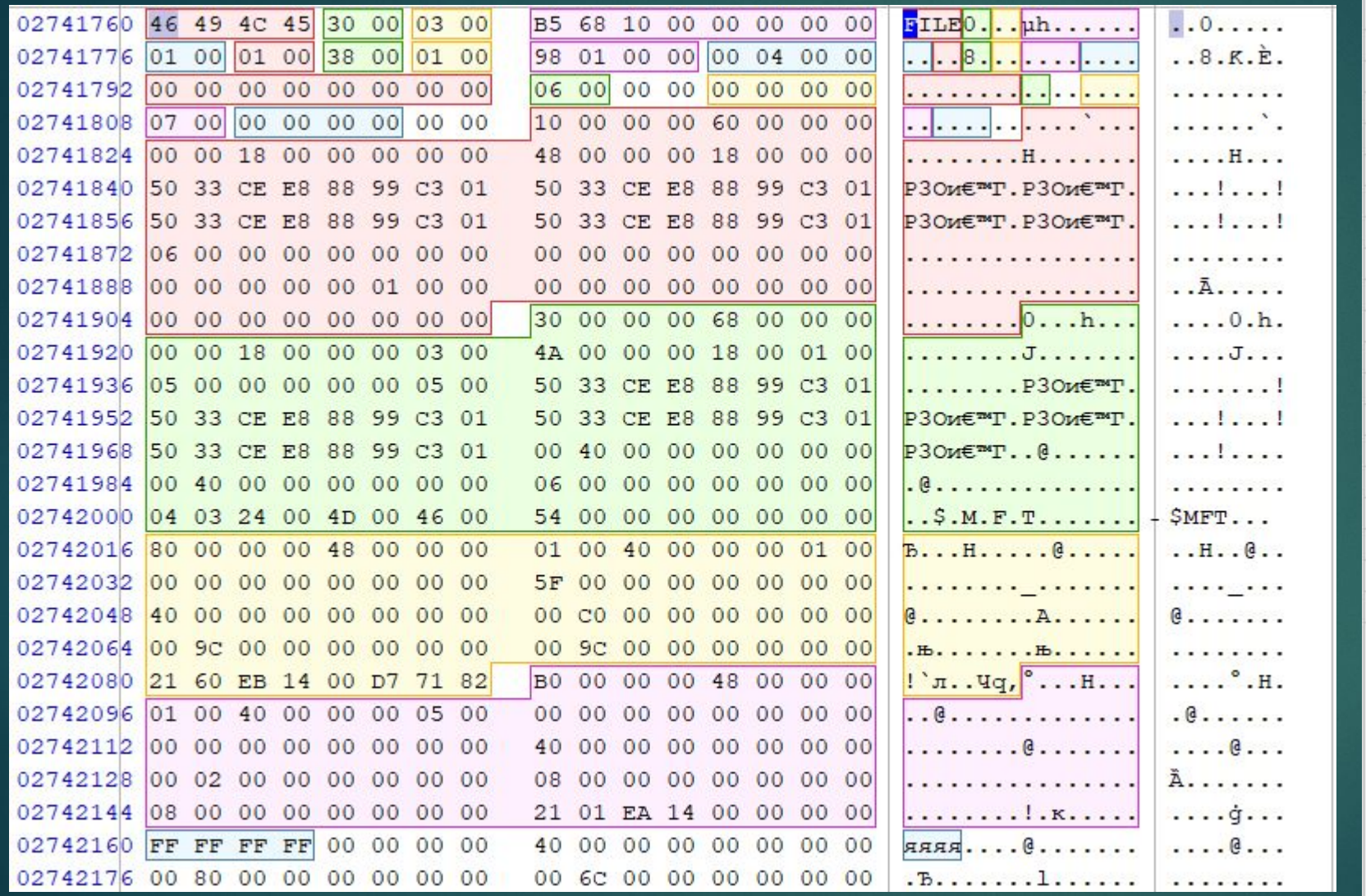


Offset	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	ASCII	Unicode
00000000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	01	00	00	лRђNTFS	....
00000016	00	00	00	00	00	F8	00	00	3F	00	20	00	3F	00	00	00	.....ш..?. .?...	.... ? ?.
00000032	00	00	00	00	80	00	80	00	C0	3E	00	00	00	00	00	00	....Ђ.Ђ.А>.....	.....
00000048	EB	14	00	00	00	00	00	00	60	1F	00	00	00	00	00	00	л.....`.....	....ώ...
00000064	02	00	00	00	08	00	00	00	23	56	ED	50	92	ED	50	BA	.....#VнP'нPє	.....
00000080	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	B8	C0	07	....ъ3АЋPj.|ыёА.	.....
00000096	8E	D8	E8	16	00	B8	00	0D	8E	C0	33	DB	C6	06	0E	00	ЋШи..ё..ЋА3ЫЖ...	.....ğ.
00000112	10	E8	53	00	68	00	0D	68	6A	02	CB	8A	16	24	00	B4	.иS.h..hj.ЛЉ.$.ґ	.Sh.ґ...
00000128	08	CD	13	73	05	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	.Н.s.№яяЉcf.¶Ж@f	.....
00000144	0F	B6	D1	80	E2	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	.¶СЂв?чв†НАн.Af.	.....
00000160	B7	C9	66	F7	E1	66	A3	20	00	C3	B4	41	BB	AA	55	8A	·Йfчбfj .ГґА»єUЉ	...F....
00000176	16	24	00	CD	13	72	0F	81	FB	55	AA	75	09	F6	C1	01	.$.Н.r.ЃыUєu.цБ.	I
00000192	74	04	FE	06	14	00	C3	66	60	1E	06	66	A1	10	00	66	t.ю...Гf`..fЎ..f	V..Ś...
00000208	03	06	1C	00	66	3B	06	20	00	0F	82	3A	00	1E	66	6A	....f;. ..,:..fj	....Ą.
00000224	00	66	50	06	53	66	68	10	00	01	00	80	3E	14	00	00	.fP.Sfh....Ђ>...	,..Ā...
00000240	0F	85	0C	00	E8	B3	FF	80	3E	14	00	00	0F	84	61	00	.…..иіяЂ>....„a.	.....a
00000256	B4	42	8A	16	24	00	16	1F	8B	F4	CD	13	66	58	5B	07	ґВЉ.$...‹фН.fX[.	..$....ر
00000272	66	58	66	58	1F	EB	2D	66	33	D2	66	0F	B7	0E	18	00	fXfX.л-f3Тf.·...	.....
00000288	66	F7	F1	FE	C2	8A	CA	66	8B	D0	66	C1	EA	10	F7	36	fчсюВЉКf‹ РfБк.ч6	.ς.....
00000304	1A	00	86	D6	8A	16	24	00	8A	E8	C0	E4	06	0A	CC	B8	..†ЦЉ.$.ЉиАд..Мё	...$....
00000320	01	02	CD	13	0F	82	19	00	8C	C0	05	20	00	8E	C0	66	..Н..,..ЊА. .ЋАf	à.....
00000336	FF	06	10	00	FF	0E	0E	00	0F	85	6F	FF	07	1F	66	61	я...я.....…оя..fa	à.....ã.
00000352	C3	A0	F8	01	E8	09	00	A0	FB	01	E8	03	00	FB	EB	FE	Г ш.и.. ы.и..ылю	.À..åёff
00000368	B4	01	8B	F0	AC	3C	00	74	09	B4	0E	BB	07	00	CD	10	ґ.‹р¬<.t.ґ.»..Н.	ÿ.....
00000384	EB	F2	C3	0D	0A	41	20	64	69	73	6B	20	72	65	61	64	лтГ..A disk read	.....
00000400	20	65	72	72	6F	72	20	6F	63	63	75	72	72	65	64	00	error occurred.	.....d
00000416	0D	0A	4E	54	4C	44	52	20	69	73	20	6D	69	73	73	69	..NTLDR is missi	.....
00000432	6E	67	00	0D	0A	4E	54	4C	44	52	20	69	73	20	63	6F	ng...NTLDR is co	.....
00000448	6D	70	72	65	73	73	65	64	00	0D	0A	50	72	65	73	73	mpressed...Press	.....

Templates

Загрузочный сектор | 355:000 | 0:000

Имя	Смещение	Значение	Копировать
Команда JMP	000	46 49 4C	EB 52 90
OEM ID	003	E0	NTFS
Блок параметров BIOS	**011**		
Байт на сектор	011	0	512
Секторов в кластере	013	0	1
Зарезервированные сект...	014	0	0
(всегда ноль)	016	01 00 01	00 00 00
(не используется)	019	00 38	00 00
Дискриптор средств	021	0	248
(не используется)	022	01 00	00 00
Секторов на дорожке	024	408	63
Количество головок	026	0	32
Скрытых секторов	028	1 024	63
(не используется)	032	00 00 00 00	00 00 00 00
Сигнатура	036	00 00 00 00	80 00 80 00
Всего секторов	040	6	16 064
Номер кластера $MFT	048	7	5 355
Номер кластера $MFTMirr	056	412 316 860...	8 032
Кластеров на сегмент зап...	064	1 572 864	2
Кластеров на индекс блока	068	0	8
Серийный номер тома	072	48 00 00 00 ...	23 56 ED 50
Контрольная сумма	080	3 905 827 664	0
Загрузочный код	084	88 99 C3 01 ...	FA 33 C0 8E
Сигнатура (55 AA)	510	07 00	55 AA



```
02741760  46 49 4C 45 30 00 03 00  B5 68 10 00 00 00 00 00  FILE0...µh......  ..0.....
02741776  01 00 01 00 38 00 01 00  98 01 00 00 00 04 00 00  ....8.....˜.....  ..8.K.È.
02741792  00 00 00 00 00 00 00 00  06 00 00 00 00 00 00 00  ................  ........
02741808  07 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00  ............`...  ......`.
02741824  00 00 18 00 00 00 00 00  48 00 00 00 18 00 00 00  ........H.......  ....H...
02741840  50 33 CE E8 88 99 C3 01  50 33 CE E8 88 99 C3 01  P3Ои€™Г.P3Ои€™Г.  ...!...!
02741856  50 33 CE E8 88 99 C3 01  50 33 CE E8 88 99 C3 01  P3Ои€™Г.P3Ои€™Г.  ...!...!
02741872  06 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................  ........
02741888  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00  ................  ..Ā.....
02741904  00 00 00 00 00 00 00 00  30 00 00 00 68 00 00 00  ........0...h...  ....0.h.
02741920  00 00 18 00 00 00 03 00  4A 00 00 00 18 00 01 00  ........J.......  ....J...
02741936  05 00 00 00 00 00 05 00  50 33 CE E8 88 99 C3 01  ........P3Ои€™Г.  .......!
02741952  50 33 CE E8 88 99 C3 01  50 33 CE E8 88 99 C3 01  P3Ои€™Г.P3Ои€™Г.  ...!...!
02741968  50 33 CE E8 88 99 C3 01  00 40 00 00 00 00 00 00  P3Ои€™Г..@......  ...!....
02741984  00 40 00 00 00 00 00 00  06 00 00 00 00 00 00 00  .@..............  ........
02742000  04 03 24 00 4D 00 46 00  54 00 00 00 00 00 00 00  ..$.M.F.T.......  - $MFT...
02742016  80 00 00 00 48 00 00 00  01 00 40 00 00 00 01 00  Ђ...H.....@.....  ..H..@..
02742032  00 00 00 00 00 00 00 00  5F 00 00 00 00 00 00 00  ........_.......  ....._...
02742048  40 00 00 00 00 00 00 00  00 C0 00 00 00 00 00 00  @........A......  @.......
02742064  00 9C 00 00 00 00 00 00  00 9C 00 00 00 00 00 00  .њ.......њ......  ........
02742080  21 60 EB 14 00 D7 71 82  B0 00 00 00 48 00 00 00  !`л..Чq‚°...H...  ....°.H.
02742096  01 00 40 00 00 00 05 00  00 00 00 00 00 00 00 00  ..@.............  .@......
02742112  00 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......  ....@...
02742128  00 02 00 00 00 00 00 00  08 00 00 00 00 00 00 00  ................  Ā.......
02742144  08 00 00 00 00 00 00 00  21 01 EA 14 00 00 00 00  ........!.к.....  ....ģ...
02742160  FF FF FF FF 00 00 00 00  40 00 00 00 00 00 00 00  яяяя....@.......  ....@...
02742176  00 80 00 00 00 00 00 00  00 6C 00 00 00 00 00 00  .Ђ.......l......  ........
```

Templates

Файловая запись NT

355:000

)710:000

Имя	Смещ	Значение
Сигнатура (должна быть 'FILE')	000	FILE
Смещение к последовательн...	004	0x30
Размер последовательности ...	006	3
Логический номер сектора в...	008	1 075 381
Порядковый номер	016	1
Количество связей каталога	018	1
Смещение до первого атриб...	020	0x38
Флаги	022	01 00
Реальный размер записи FILE	024	408
Выделенный размер записи ...	028	1 024
Базовая запись FILE	032	0
Следующий атрибут ID	040	6
ID этой записи	044	0
Номер последовательности ...	048	07 00
Массив последовательности ...	050	00 00 00 00
Атрибут $10	**056**	
Атрибут $30	**152**	
Атрибут $80	**256**	
Атрибут $B0	**328**	
Конец маркера	400	0xFFFFFFFF

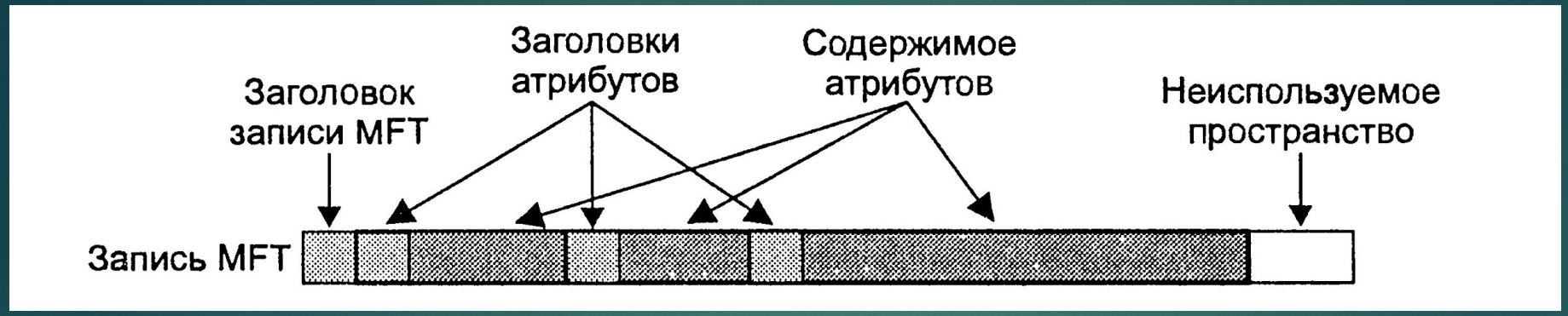
В предыдущих сериях…

Метафайлы:

Запись	Имя файла	Описание
0	$MFT	Запись для самой таблицы MFT
1	$MFTMirr	Содержит резервную копию первых записей MFT. См. раздел «Категория данных файловой системы» главы 12
2	$LogFile	Содержит журнал транзакций метаданных. См. раздел «Категория прикладных данных» главы 12
3	$Volume	Содержит информацию о томе — метка, идентификатор и версия. См. раздел «Категория данных файловой системы» главы 12
4	$AttrDef	Содержит информацию об атрибутах — значения идентификатора, имена, размеры. См. раздел «Категория данных файловой системы» главы 12
5	.	Содержит корневой каталог файловой системы. См. раздел «Категория данных файловой системы» главы 12
6	$Bitmap	Содержит признак выделения для каждого кластера файловой системы. См. раздел «Категория данных содержимого» главы 12
7	$Boot	Содержит загрузочный сектор и загрузочный код файловой системы. См. раздел «Категория данных файловой системы» главы 12
8	$BadClus	Содержит кластеры, содержащие поврежденные секторы. См. раздел «Категория данных содержимого» главы 12

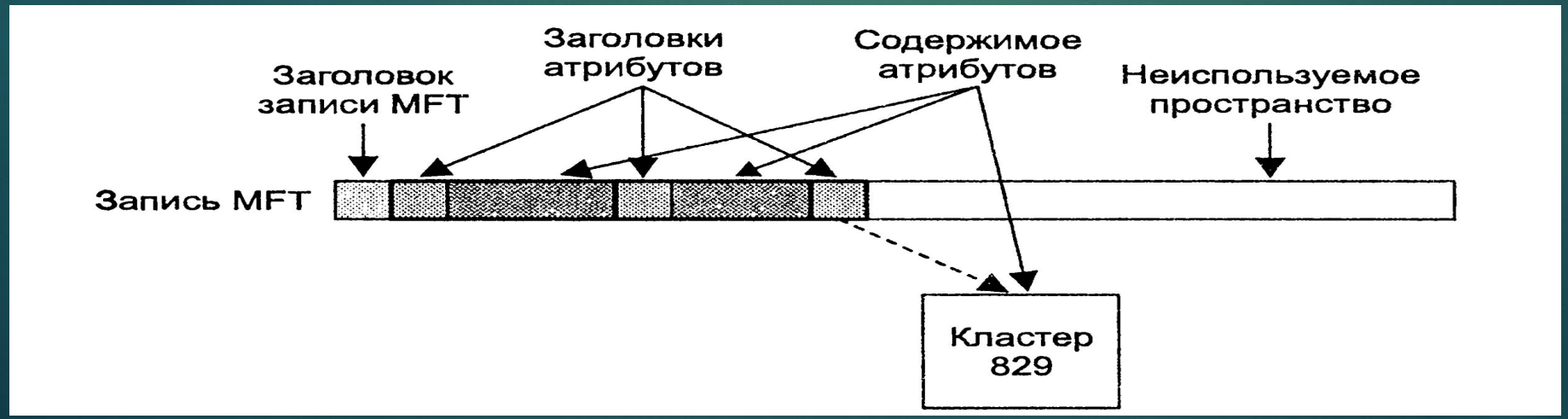
В предыдущих сериях…

- АТРИБУТЫ ЗАПИСЕЙ MFT



Атрибуты хранят основную информацию о файле.

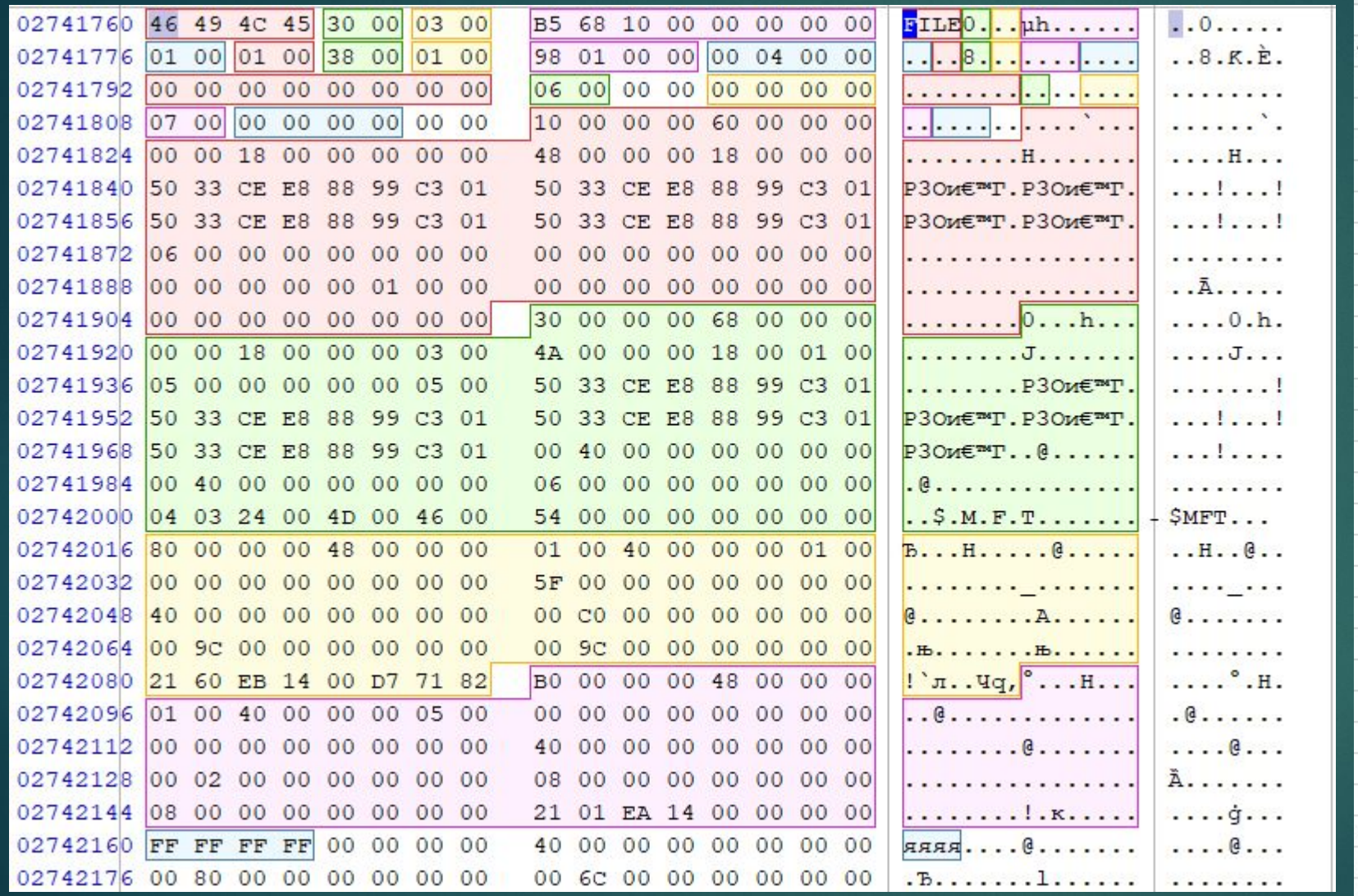
Могут быть ***резидентными*** и ***нерезидентными***



Стандартные типы атрибутов

Идентификатор типа	Имя	Описание
16	$STANDARD_INFORMATION	Общая информация (флаги; время создания, последнего обращения и модификации; владелец и идентификатор системы безопасности)
32	$ATTRIBUTE_LIST	Список других атрибутов файла
48	$FILE_NAME	Имя файла в Unicode; время создания, последнего обращения и модификации

Идентификатор типа	Имя	Описание
64	$VOLUME_VERSION	Информация о томе. Существует только в версии 1.2 (Windows NT)
80	$SECURITY_DESCRIPTOR	Время обращения и свойства безопасности файла
96	$VOLUME_NAME	Имя тома
112	$VOLUME_INFORMATION	Версия файловой системы и другие флаги
128	$DATA	Содержимое файла
144	$INDEX_ROOT	Корневой узел индексного дерева
160	$INDEX_ALLOCATION	Узлы индексного дерева, корень которого определяется атрибутом $INDEX_ROOT
176	$BITMAP	Битовая карта файла $MFT и его индексов
192	$SYMBOLIC_LINK	Информация о мягких ссылках. Существует только в версии 1.2 (Windows NT)



```
02741760  46 49 4C 45 30 00 03 00  B5 68 10 00 00 00 00 00  FILE0...µh......  .0.....
02741776  01 00 01 00 38 00 01 00  98 01 00 00 00 04 00 00  ....8.....˜.....  ..8.K.È.
02741792  00 00 00 00 00 00 00 00  06 00 00 00 00 00 00 00  ................  ........
02741808  07 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00  ............`...  ......`.
02741824  00 00 18 00 00 00 00 00  48 00 00 00 18 00 00 00  ........H.......  ....H...
02741840  50 33 CE E8 88 99 C3 01  50 33 CE E8 88 99 C3 01  P3Ои€™Г.P3Ои€™Г.  ...!...!
02741856  50 33 CE E8 88 99 C3 01  50 33 CE E8 88 99 C3 01  P3Ои€™Г.P3Ои€™Г.  ...!...!
02741872  06 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................  ........
02741888  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00  ................  ..Ā.....
02741904  00 00 00 00 00 00 00 00  30 00 00 00 68 00 00 00  ........0...h...  ....0.h.
02741920  00 00 18 00 00 00 03 00  4A 00 00 00 18 00 01 00  ........J.......  ....J...
02741936  05 00 00 00 00 00 05 00  50 33 CE E8 88 99 C3 01  ........P3Ои€™Г.  .......!
02741952  50 33 CE E8 88 99 C3 01  50 33 CE E8 88 99 C3 01  P3Ои€™Г.P3Ои€™Г.  ...!...!
02741968  50 33 CE E8 88 99 C3 01  00 40 00 00 00 00 00 00  P3Ои€™Г..@......  ...!....
02741984  00 40 00 00 00 00 00 00  06 00 00 00 00 00 00 00  .@..............  ........
02742000  04 03 24 00 4D 00 46 00  54 00 00 00 00 00 00 00  ..$.M.F.T.......  - $MFT...
02742016  80 00 00 00 48 00 00 00  01 00 40 00 00 00 01 00  Ъ...H.....@.....  ..H..@..
02742032  00 00 00 00 00 00 00 00  5F 00 00 00 00 00 00 00  ........_.......  ....._...
02742048  40 00 00 00 00 00 00 00  00 C0 00 00 00 00 00 00  @........A......  @.......
02742064  00 9C 00 00 00 00 00 00  00 9C 00 00 00 00 00 00  .њ.......њ......  ........
02742080  21 60 EB 14 00 D7 71 82  B0 00 00 00 48 00 00 00  !`л..Чq‚°...H...  ....°.H.
02742096  01 00 40 00 00 00 05 00  00 00 00 00 00 00 00 00  ..@.............  .@......
02742112  00 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......  ....@...
02742128  00 02 00 00 00 00 00 00  08 00 00 00 00 00 00 00  ................  Ā.......
02742144  08 00 00 00 00 00 00 00  21 01 EA 14 00 00 00 00  ........!.к.....  ....ģ...
02742160  FF FF FF FF 00 00 00 00  40 00 00 00 00 00 00 00  яяяя....@.......  ....@...
02742176  00 80 00 00 00 00 00 00  00 6C 00 00 00 00 00 00  .Ъ.......l......  ........
```

Templates

Файловая запись NT | 355:000 | 710:000

Имя	Смещен	Значение
Массив последовательности ...	050	00 00 00 00
Атрибут $10	**056**	
Тип атрибута	056	0x10
Длина (включая заголов...	060	96
Флаг-нерезидент	064	0
Длина имени	065	0
Смещение имени	066	0x18
Флаги	068	00 00
ID атрибута	070	0
Длина атрибута	072	72
Смещение в данных атри...	076	0x18
Индексируемый флаг	078	0
Заполнение	079	0
$STANDARD_INFORMAT...	**080**	
Файл создан (UTC)	080	23.10.2003 17:12:59
Файл изменен (UTC)	088	23.10.2003 17:12:59
Замена записи (UTC)	096	23.10.2003 17:12:59
Время доступа (UTC)	104	23.10.2003 17:12:59
Разрешения файла	112	06 00 00 00
Максимальный номе...	116	0
Номер версии	120	0
Class Id	124	0
Owner Id	128	0
Security Id	132	256
Quota Charged	136	0
Update Sequence Num...	144	0
Атрибут $30	**152**	
Атрибут $80	**256**	
Атрибут $B0	**328**	
Конец маркера	400	0xFFFFFFFF

$Standart_Information

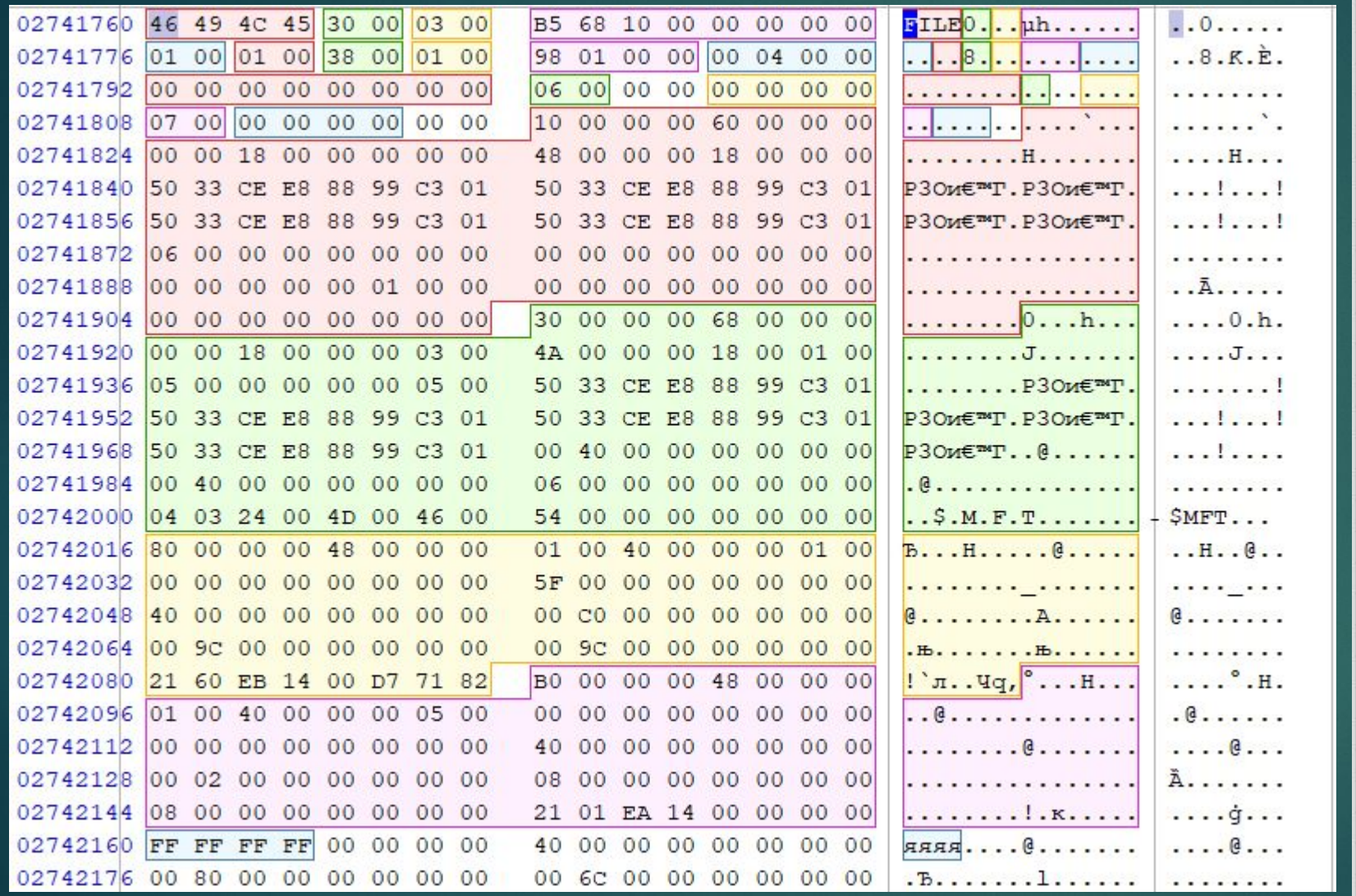
- Атрибут содержит 4 временные метки:
  - ВРЕМЯ СОЗДАНИЯ – время, в которое был создан файл
  - ВРЕМЯ ПОСЛЕДНЕЙ МОДИФИКАЦИИ – время последнего изменения атрибутов $DATA или $INDEX
  - ВРЕМЯ МОДИФИКАЦИИ – время изменения любого файла метаданных, связанных с исследуемым файлом
  - ВРЕМЯ ПОСЛЕДНЕГО ОБРАЩЕНИЯ – время последнего обращения к содержимому (чтение) файла (атрибута $DATA)

Структура атрибута $SI

Диапазон	Описание	Необходимость
0–7	Время создания	Нет
8–15	Время модификации файла	Нет
16–23	Время модификации MFT	Нет
24–31	Время обращения к файлу	Нет
32–35	Флаги (см. табл. 13.6)	Нет
36–39	Максимальное количество версий	Нет
40–43	Номер версии	Нет
44–47	Идентификатор класса	Нет
48–51	Идентификатор владельца (версия 3.0+)	Нет
52–55	Идентификатор безопасности (версия 3.0+)	Нет
56–63	Изменение квоты (версия 3.0+)	Нет
64–71	Номер USN (Update Sequence Number)	Нет

Атрибут $FILE_NAME

Диапазон	Описание	Необходимость
0–7	Базовый адрес родительского каталога	Нет
8–15	Время создания файла	Нет
16–23	Время модификации файла	Нет
24–31	Время модификации MFT	Нет
32–39	Время обращения к файлу	Нет
40–47	Выделенный размер файла	Нет
48–55	Реальный размер файла	Нет
56–59	Флаги (см. табл. 13.6)	Нет
60–63	Точка подключения	Нет
64–64	Длина имени	Да/Нет
65–65	Пространство имен (см. табл. 13.8)	Да/Нет
66+	Имя	Да/Нет



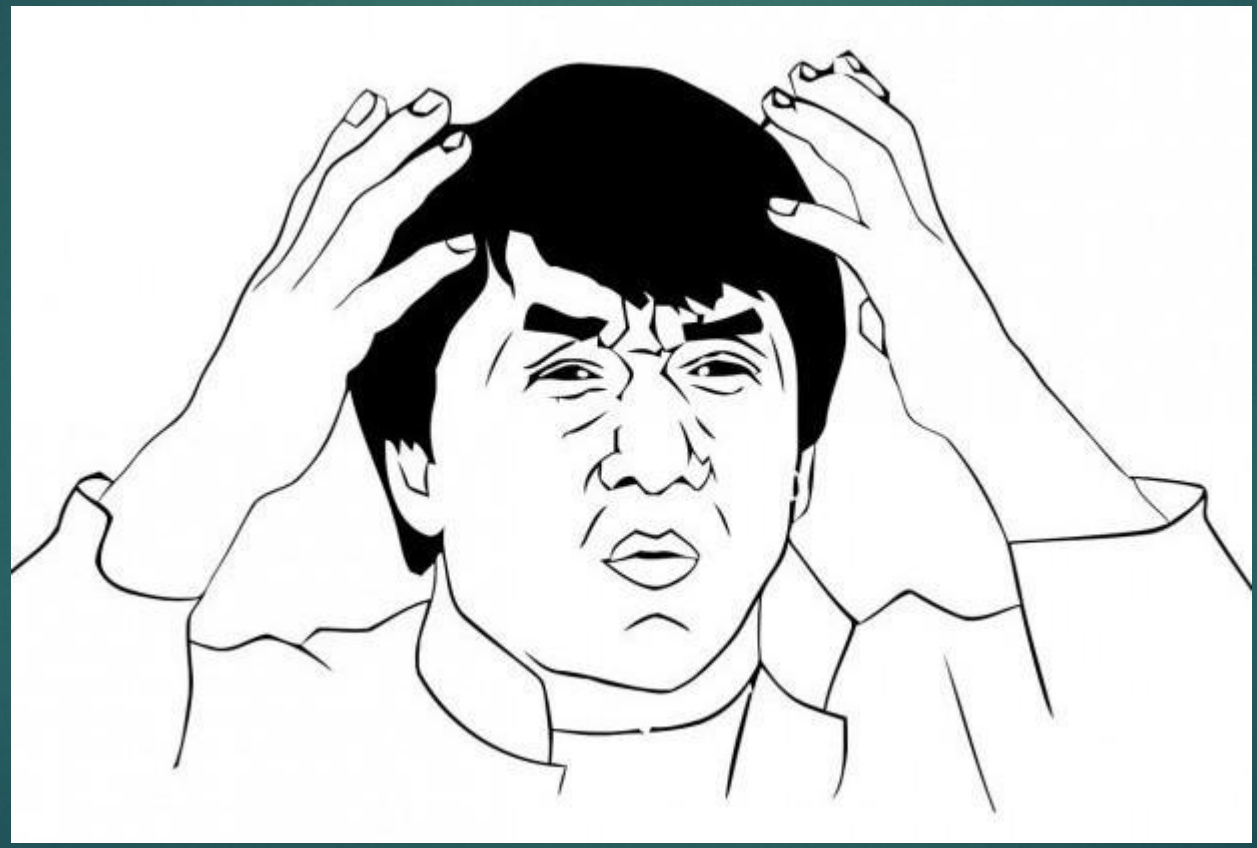
```
02741760  46 49 4C 45 30 00 03 00  B5 68 10 00 00 00 00 00  FILE0...µh......  .0.....
02741776  01 00 01 00 38 00 01 00  98 01 00 00 00 04 00 00  ....8.........  ..8.K.È.
02741792  00 00 00 00 00 00 00 00  06 00 00 00 00 00 00 00  ................  ........
02741808  07 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00  ............`...  ......`.
02741824  00 00 18 00 00 00 00 00  48 00 00 00 18 00 00 00  ........H.......  ....H...
02741840  50 33 CE E8 88 99 C3 01  50 33 CE E8 88 99 C3 01  P3Oи€™Г.P3Oи€™Г.  ...!...!
02741856  50 33 CE E8 88 99 C3 01  50 33 CE E8 88 99 C3 01  P3Oи€™Г.P3Oи€™Г.  ...!...!
02741872  06 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................  ........
02741888  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00  ................  ..Ā.....
02741904  00 00 00 00 00 00 00 00  30 00 00 00 68 00 00 00  ........0...h...  ....0.h.
02741920  00 00 18 00 00 00 03 00  4A 00 00 00 18 00 01 00  ........J.......  ....J...
02741936  05 00 00 00 00 00 05 00  50 33 CE E8 88 99 C3 01  ........P3Oи€™Г.  .......!
02741952  50 33 CE E8 88 99 C3 01  50 33 CE E8 88 99 C3 01  P3Oи€™Г.P3Oи€™Г.  ...!...!
02741968  50 33 CE E8 88 99 C3 01  00 40 00 00 00 00 00 00  P3Oи€™Г..@......  ...!....
02741984  00 40 00 00 00 00 00 00  06 00 00 00 00 00 00 00  .@..............  ........
02742000  04 03 24 00 4D 00 46 00  54 00 00 00 00 00 00 00  ..$.M.F.T.......  - $MFT...
02742016  80 00 00 00 48 00 00 00  01 00 40 00 00 00 01 00  Ъ...H.....@.....  ..H..@..
02742032  00 00 00 00 00 00 00 00  5F 00 00 00 00 00 00 00  ........_.......  ....._...
02742048  40 00 00 00 00 00 00 00  00 C0 00 00 00 00 00 00  @........A......  @.......
02742064  00 9C 00 00 00 00 00 00  00 9C 00 00 00 00 00 00  .њ.......њ......  ........
02742080  21 60 EB 14 00 D7 71 82  B0 00 00 00 48 00 00 00  !`л..Чq‚°...H...  ....°.H.
02742096  01 00 40 00 00 00 05 00  00 00 00 00 00 00 00 00  ..@.............  .@......
02742112  00 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......  ....@...
02742128  00 02 00 00 00 00 00 00  08 00 00 00 00 00 00 00  ................  Ā.......
02742144  08 00 00 00 00 00 00 00  21 01 EA 14 00 00 00 00  ........!.к.....  ....ģ...
02742160  FF FF FF FF 00 00 00 00  40 00 00 00 00 00 00 00  яяяя....@.......  ....@...
02742176  00 80 00 00 00 00 00 00  00 6C 00 00 00 00 00 00  .Ъ.......l......  ........
```

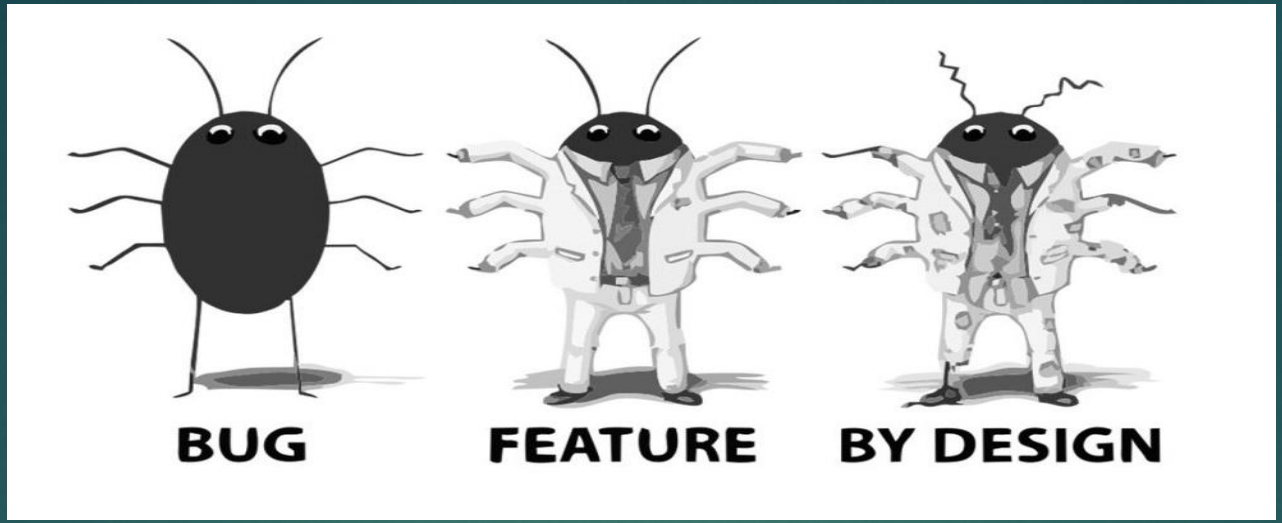
Templates

Файловая запись NT | 355:000 | 710:000

Имя	Смещен	Значение
Атрибут $10	**056**	
Атрибут $30	**152**	
Тип атрибута	152	0x30
Длина (включая заголов...	156	104
Флаг-нерезидент	160	0
Длина имени	161	0
Смещение имени	162	0x18
Флаги	164	00 00
ID атрибута	166	3
Длина атрибута	168	74
Смещение в данных атри...	172	0x18
Индексируемый флаг	174	1
Заполнение	175	0
$FILE_NAME	**176**	
Номер записи родите...	176	5
Parent directory seque...	182	5
Файл создан (UTC)	184	23.10.2003 17:12:59
Файл изменен (UTC)	192	23.10.2003 17:12:59
Замена записи (UTC)	200	23.10.2003 17:12:59
Время доступа (UTC)	208	23.10.2003 17:12:59
Allocated size	216	16 384
Real size	224	16 384
Атрибуты файла	232	06 00 00 00
(used by EAs and repar...	236	0
File name length	240	4
File name namespace	241	3
Имя файла	242	$MFT
Атрибут $80	**256**	
Атрибут $B0	**328**	
Конец маркера	400	0xFFFFFFFF

Идентичные поля времени в двух атрибутах? Зачем?





При создании файла все сведения в структуре FILE_NAME копируются из предыдущей структуры STANDARD_INFORMATION ⟶ все атрибуты времени в структуре FILE_NAME совпадают с аналогичными из структуры STANDARD_INFORMATION.

НО!

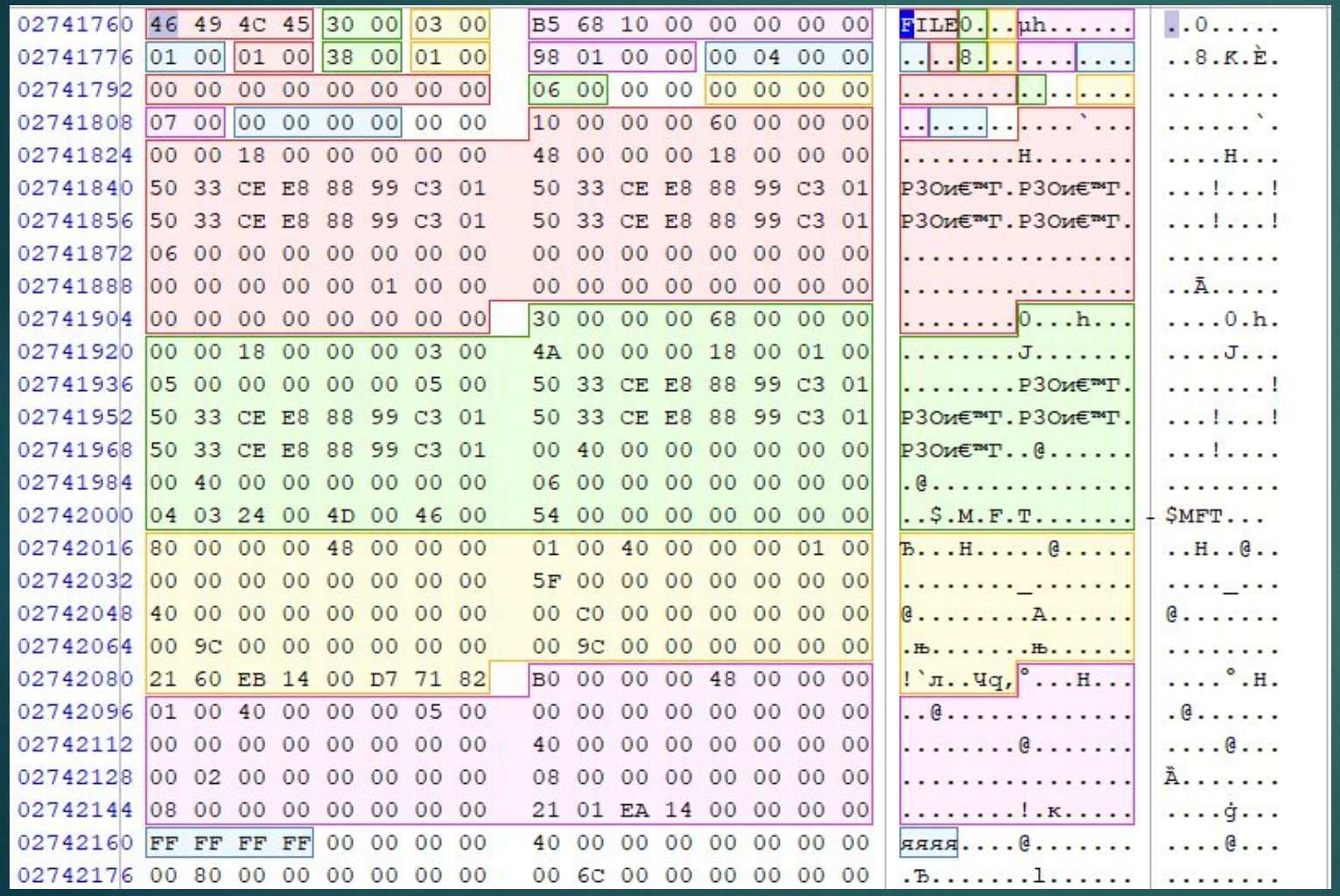
Данные в структуре $FILE_NAME создаются в момент создания файла и представляют собой копию даты создания и изменяются при переименовании, локальном перемещении, перемещении между файловыми системами, копировании и удалении файла. Следовательно, сведения в этой структуре не могут превосходить временные атрибуты из структуры $STANDARD_INFORMATION. Но это актуально именно для времени создания и изменения файла. Время последнего доступа к файлу и атрибут MFT modified могут измениться только в структуре $STANDARD_INFORMATION. Поэтому время последнего доступа к файлу следует определять по структуре $STANDARD_INFORMATION

Что не нужно делать, если вы за вами уже выехали?

- Не забывать, что менять временные метки в атрибуте $FILE_NAME по сути не имеет смысла
- Даже если их и заменить одновременно в атрибутах $SI и $FN, то это тоже ни чем не поможет
- Время последнего доступа к файлу и атрибут MFT modified могут измениться только в структуре $STANDARD_INFORMATION, что значит, что в $FN аналогичные поля лучше не менять.
- Для времени создания и изменения файла метки в $FN не могут быть «больше» чем метки в $SI, а если еще и знать, что даже эти 2 метки не меняются после создания файла в $SI, то между ними должна быть разбежка.
- Записывать во временные метки значения «меньшие» чем метки создания файловой системы для записи $MFT

В общем, играйтесь со временем правильно

Атрибут $DATA

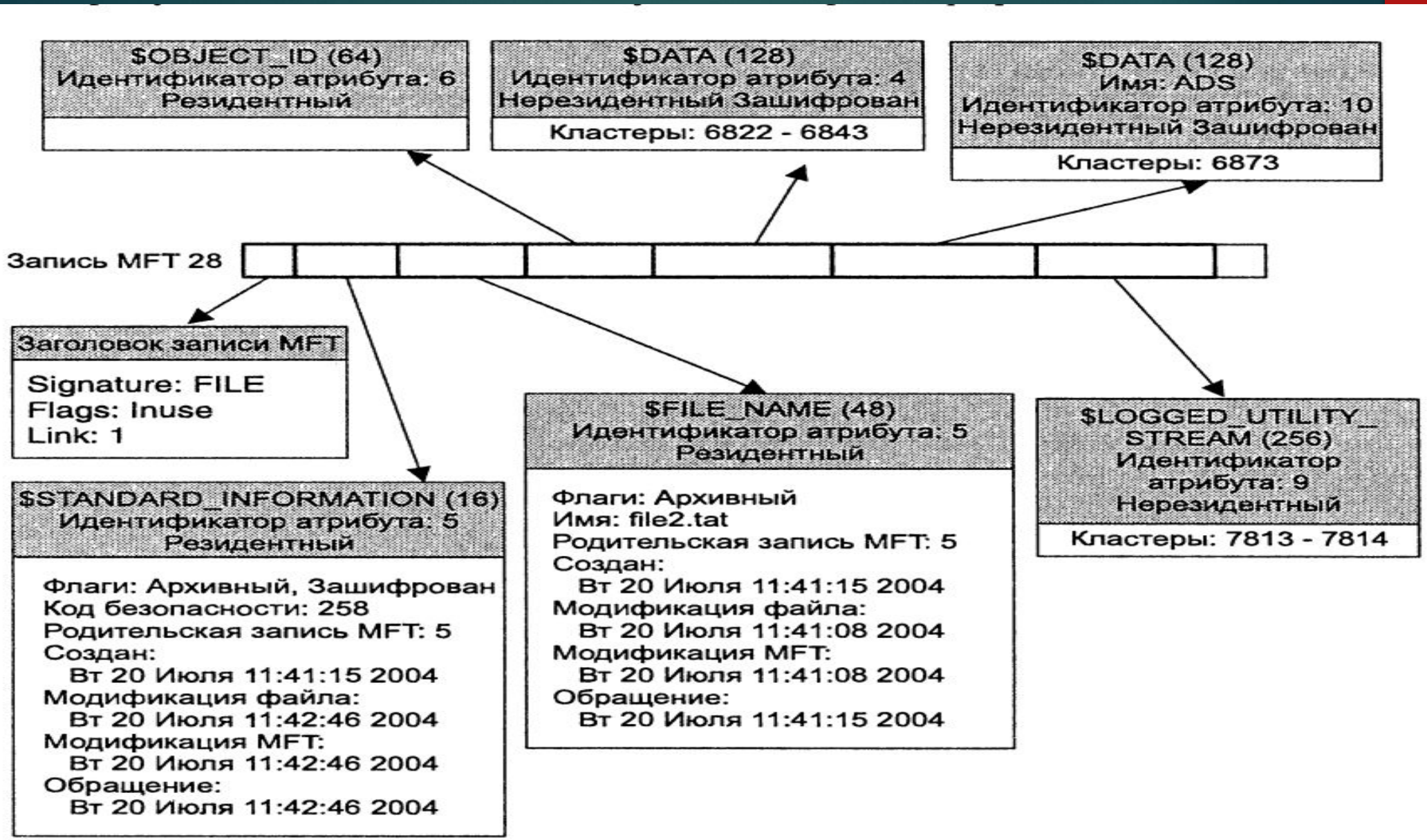


02741760	46 49 4C 45	30 00	03 00	B5 68 10 00 00 00 00 00	FILE0..µh.....	.0.....
02741776	01 00	01 00	38 00	01 00	98 01 00 00	00 04 00 00	..8.....˜.......	..8.К.È.
02741792	00 00 00 00 00 00 00 00	06 00	00 00	00 00 00 00	.....	.....
02741808	07 00	00 00 00 00	00 00	10 00 00 00 60 00 00 00	.....	.....`.
02741824	00 00 18 00 00 00 00 00	48 00 00 00 18 00 00 00	....H...	....H...
02741840	50 33 CE E8 88 99 C3 01	50 33 CE E8 88 99 C3 01	Р3Ои€™Г.Р3Ои€™Г.	...!...!
02741856	50 33 CE E8 88 99 C3 01	50 33 CE E8 88 99 C3 01	Р3Ои€™Г.Р3Ои€™Г.	...!...!
02741872	06 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....	.....
02741888	00 00 00 00 00 01 00 00	00 00 00 00 00 00 00 00	.....	..Ā.....
02741904	00 00 00 00 00 00 00 00	30 00 00 00 68 00 00 00	....0...h...	....0.h.
02741920	00 00 18 00 00 00 03 00	4A 00 00 00 18 00 01 00	....J...	....J...
02741936	05 00 00 00 00 00 05 00	50 33 CE E8 88 99 C3 01	....P3Ои€™Г.	.....!
02741952	50 33 CE E8 88 99 C3 01	50 33 CE E8 88 99 C3 01	Р3Ои€™Г.Р3Ои€™Г.	...!...!
02741968	50 33 CE E8 88 99 C3 01	00 40 00 00 00 00 00 00	Р3Ои€™Г..@.....	...!....
02741984	00 40 00 00 00 00 00 00	06 00 00 00 00 00 00 00	.@.....	.....
02742000	04 03 24 00 4D 00 46 00	54 00 00 00 00 00 00 00	..$.M.F.T.....	- $MFT...
02742016	80 00 00 00 48 00 00 00	01 00 40 00 00 00 01 00	Ъ...H.....@.....	..H..@..
02742032	00 00 00 00 00 00 00 00	5F 00 00 00 00 00 00 00	....._.....	...._...
02742048	40 00 00 00 00 00 00 00	00 C0 00 00 00 00 00 00	@.....А.....	@.....
02742064	00 9C 00 00 00 00 00 00	00 9C 00 00 00 00 00 00	.њ.....њ.....	.....
02742080	21 60 EB 14 00 D7 71 82	B0 00 00 00 48 00 00 00	!`л..Чq,°...H...	....°.H.
02742096	01 00 40 00 00 00 05 00	00 00 00 00 00 00 00 00	..@.....	.@.....
02742112	00 00 00 00 00 00 00 00	40 00 00 00 00 00 00 00	.....@.....	....@...
02742128	00 02 00 00 00 00 00 00	08 00 00 00 00 00 00 00	.....	Ā.....
02742144	08 00 00 00 00 00 00 00	21 01 EA 14 00 00 00 00	.....!.к.....	....ġ...
02742160	FF FF FF FF	00 00 00 00	40 00 00 00 00 00 00 00	яяяя....@.....	....@...
02742176	00 80 00 00 00 00 00 00	00 6C 00 00 00 00 00 00	.Ъ.....l.....	.....

Templates

Файловая запись NT | 355:000 |)710:000

Имя	Смещен	Значение
Номер последовательности ...	048	07 00
Массив последовательности ...	050	00 00 00 00
Атрибут $10	**056**	
Атрибут $30	**152**	
Атрибут $80	**256**	
Тип атрибута	256	0x80
Длина (включая заголов...	260	72
Флаг-нерезидент	264	1
Длина имени	265	0
Смещение имени	266	0x40
Флаги	268	00 00
Сжатый	:0	0
Зашифрованный	:14	0
Разреженный	:15	0
ID атрибута	270	1
Первый VCN	272	0
Последний VCN	280	95
Смещение выполнений д...	288	0x40
Размер блока сжатия	290	0
Заполнение	292	00 00 00 00
Выделенный размер	296	49 152
Реальный размер	304	39 936
Инициализированный ра...	312	39 936
$DATA	**320**	
Выполнения данных	**320**	
Размер	320	0x21
Количество класт...	321	96
Первый кластер	322	5 355
Атрибут $B0	**328**	
Конец маркера	400	0xFFFFFFFF


$OBJECT_ID (64)
Идентификатор атрибута: 6
Резидентный
$DATA (128)
Идентификатор атрибута: 4
Нерезидентный Зашифрован
Кластеры: 6822 - 6843
$DATA (128)
Имя: ADS
Идентификатор атрибута: 10
Нерезидентный Зашифрован
Кластеры: 6873
Запись MFT 28
Заголовок записи MFT
Signature: FILE
Flags: Inuse
Link: 1
$STANDARD_INFORMATION (16)
Идентификатор атрибута: 5
Резидентный
Флаги: Архивный, Зашифрован
Код безопасности: 258
Родительская запись MFT: 5
Создан:
Вт 20 Июля 11:41:15 2004
Модификация файла:
Вт 20 Июля 11:42:46 2004
Модификация MFT:
Вт 20 Июля 11:42:46 2004
Обращение:
Вт 20 Июля 11:42:46 2004
$FILE_NAME (48)
Идентификатор атрибута: 5
Резидентный
Флаги: Архивный
Имя: file2.tat
Родительская запись MFT: 5
Создан:
Вт 20 Июля 11:41:15 2004
Модификация файла:
Вт 20 Июля 11:41:08 2004
Модификация MFT:
Вт 20 Июля 11:41:08 2004
Обращение:
Вт 20 Июля 11:41:15 2004
$LOGGED_UTILITY_
STREAM (256)
Идентификатор
атрибута: 9
Нерезидентный
Кластеры: 7813 - 7814

Заключение

- Рассмотрели 3 основных атрибута
  - $STANDART_INFORMATION
  - $FILE_NAME
  - $DATA
- Первая лаба лежит на образовательном портале:
  - Срок сдачи – следующая неделя