

Оставь надежду,
Всяк сюда входящий
© Данте Алигьери

Методичка по решению практических заданий по файловой системе NTFS

Шаг 1 - Анализ загрузочного сектора

Теория. Взглянем на пример загрузочного сектора:

```
offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00 | 00020800 NTFS .....
00000010 00 00 00 00 00 00 F8 00 00 00 00 00 00 00 00 00 | .....ø.....
00000020 00 00 00 00 80 80 00 70 C9 02 00 00 00 00 00 00 | .....pÉ.....
00000030 04 00 00 00 00 00 00 97 2C 00 00 00 00 00 00 00 | .....[,.....
00000040 F6 00 00 00 01 00 00 00 0C 58 C8 60 06 F9 38 17 | ö.....XÈ`.ù8.
00000050 00 00 00 00 0E 1F BE 71 7C AC 22 C0 74 0B 56 B4 | .....%q|~"Àt.V´
00000060 0E BB 07 00 CD 10 5E EB F0 32 E4 CD 16 CD 19 EB | .»...í.^ëð2äí.í.ë
00000070 FE 54 68 69 73 20 69 73 20 6E 6F 74 20 61 20 62 | bThis is not a b
00000080 6F 6F 74 61 62 6C 65 20 64 69 73 6B 2E 20 50 6C | ootable disk. Pl
00000090 65 61 73 65 20 69 6E 73 65 72 74 20 61 20 62 6F | ease insert a bo
000000A0 6F 74 61 62 6C 65 20 66 6C 6F 70 70 79 20 61 6E | otable floppy an
000000B0 64 0D 0A 70 72 65 73 73 20 61 6E 79 20 6B 65 79 | d..press any key
000000C0 20 74 6F 20 74 72 79 20 61 67 61 69 6E 20 2E 2E | to try again ..
```

Рисунок 1 - пример загрузочного сектора

В зоне «1» у нас указывается система хранения. Если у вас там не NTFS, то идите читать методичку по FAT.

В зоне «2» указан размер одного сектора в байтах.

В зоне «3» указано сколько секторов в одном кластере.

В зоне «4» указано смещение до MFT таблицы в кластерах.

Практика. Посмотрим на данный загрузочный сектор:

```

offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00| ̈́RNTFS .....
00000010 00 00 00 00 00 00 F8 00 00 00 00 00 00 00 00 00| .....ø.....
00000020 00 00 00 00 80 00 80 00 FB C2 02 00 00 00 00 00| ....B.B.ŮÅ.....
00000030 04 00 00 00 00 00 00 00 2F 2C 00 00 00 00 00 00| ...../.....
00000040 F6 00 00 00 01 00 00 00 4F 78 22 5F B7 BD 8D 55| ö.....Ox"_.%U
00000050 00 00 00 00 0E 1F BE 71 7C AC 22 C0 74 0B 56 B4| .....%q|~"Ät.V´
00000060 0E BB 07 00 CD 10 5E EB F0 32 E4 CD 16 CD 19 EB| .»...f.^ëð2äf.f.ë
00000070 FE 54 68 69 73 20 69 73 20 6E 6F 74 20 61 20 62| pThis is not a b
00000080 6F 6F 74 61 62 6C 65 20 64 69 73 6B 2E 20 50 6C| ootable disk. Pl
00000090 65 61 73 65 20 69 6E 73 65 72 74 20 61 20 62 6F| ease insert a bo
000000A0 6F 74 61 62 6C 65 20 66 6C 6F 70 70 79 20 61 6E| otable floppy an
000000B0 64 0D 0A 70 72 65 73 73 20 61 6E 79 20 6B 65 79| d..press any key
000000C0 20 74 6F 20 74 72 79 20 61 67 61 69 6E 20 2E 2E| to try again ..
000000D0 2E 20 0D 0A 00 00 00 00 00 00 00 00 00 00 00 00| . .....
000000E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....
000000F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....
00000100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....
00000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....
00000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....
00000130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....

```

Рисунок 2 - загрузочный сектор

Проанализировав его, делаем вывод, что:

1. Система хранения – NTFS
2. Размер сектора – 0x0200 – 512 байт
3. Количество секторов в кластере – 0x08 – 8 сектор
4. Смещение до MFT таблицы в кластерах - 0x04 - 4 кластера

На этом анализ загрузочного сектора окончен.

Шаг 2 - Переход в MFT таблицу

Теория. Следующим шагом будет переход в MFT таблицу. Для этого нужно умножить размер сектора, на количество секторов в кластере и на смещение до MFT таблицы в кластерах (как их определить, см. Шаг 1) и мы получим смещение таблицы MFT. То есть формула смещения до MFT

таблицы следующая: Размер сектора*Количество секторов в кластере*Смещение до MFT таблицы в кластерах.

Для того, чтобы получить сектор начала таблицы MFT, нужно полученный результат умножения разделить на размер сектора. То есть формула первого сектора таблицы MFT следующая: Смещение до MFT таблицы / Размер сектора.

Практика. Посчитаем смещение до MFT-таблицы по выше написанной формуле: $0x200 * 8 * 4 = 0x4000$.

Калькулятор

DEC:	16384	HEX:	0x4000
Счеты	$0x200 * 8 * 4$		Вычислить

Рисунок 3 - Подсчёт смещения до MFT таблицы

0x4000 - offset таблицы MFT. Теперь посчитаем сектор MFT таблицы:

$0x4000 / 0x200 = 32$. Перейдём в полученный сектор:

```
offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00004000 46 49 4C 45 30 00 00 00 00 00 00 00 00 00 00 00 FILE0.....
00004010 01 00 01 00 38 00 01 00 98 01 00 00 00 04 00 00 ....S...
00004020 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 .....
00004030 A8 09 00 00 00 00 00 00 10 00 00 00 60 00 00 00 .....
00004040 00 00 18 00 00 00 00 00 48 00 00 00 18 00 00 00 .....H...
00004050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004070 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00004090 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00 .....0...h...
000040A0 00 00 18 00 00 00 02 00 4A 00 00 00 18 00 01 00 .....J...
000040B0 05 00 00 00 00 00 05 00 00 6F 9A 23 05 A2 D9 01 | .....o...fU.
000040C0 00 6F 9A 23 05 A2 D9 01 00 6F 9A 23 05 A2 D9 01 | .....o...fU.
000040D0 00 6F 9A 23 05 A2 D9 01 00 70 00 00 00 00 00 00 | .....o...fU...p...
000040E0 00 6C 00 00 00 00 00 00 06 00 00 00 00 00 00 00 | .....l...
000040F0 04 03 24 00 4D 00 46 00 54 00 00 00 00 00 00 00 | .....$.M.F.T.....
00004100 80 00 00 00 00 48 00 00 01 00 40 00 00 00 01 00 | .....H.....@...
00004110 00 00 00 00 00 00 00 00 7A 02 00 00 00 00 00 00 | .....
00004120 40 00 00 00 00 00 00 00 B0 27 00 00 00 00 00 00 | .....@.....
00004130 00 98 27 00 00 00 00 00 98 27 00 00 00 00 00 00 | .....@'.....
00004140 17 7B A7 A4 AA AA AA AA AA AA AA AA AA AA AA AA | .....f.....
```

Имя файла	ZRMcy/zFTTw/rXrmr/ZRMcy		
Инструменты			
Номер сектора	32	Выгрузить	
Ответ			
MD5			Отправить
Калькулятор			
DEC:	32	HEX:	0x20
Счеты	$0x200 * 8 * 4$		Вычислить

Рисунок 4 - MFT таблица

Мы попали в сектор таблицы MFT, congratulations, но это еще далеко не все)

Шаг 3 - Переход в корневую папку

Теория. Для того, чтобы попасть в корневую папку, нужно узнать размер записи MFT(см. рисунок 5) и умножить его на 5 и прибавить смещение до MFT таблицы. То есть формула смещения до корневой папки следующая: Смещение до MFT таблицы + Размер записи MFT*5. Тогда формула сектора корневой папки будет следующая: Смещение до корневой папки/Размер сектор.

offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00004000	46	49	4C	45	30	00	03	00	00	00	00	00	00	00	00	00	FILE0.....
00004010	01	00	01	00	38	00	01	00	98	01	00	00	00	04	00	008...[?].
00004020	00	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00
00004030	A8	09	00	00	00	00	00	00	10	00	00	00	60	00	00	00`...
00004040	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00H.....
00004050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00004060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00004070	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00004080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00004090	00	00	00	00	00	00	00	00	30	00	00	00	68	00	00	000...h...
000040A0	00	00	18	00	00	00	02	00	4A	00	00	00	18	00	01	00J.....
000040B0	05	00	00	00	00	00	05	00	80	09	C6	56	D7	A1	D9	01[?].ÆV×;Û.
000040C0	80	09	C6	56	D7	A1	D9	01	80	09	C6	56	D7	A1	D9	01	[?].ÆV×;Û.[?].ÆV×;Û.
000040D0	80	09	C6	56	D7	A1	D9	01	00	70	00	00	00	00	00	00	[?].ÆV×;Û...p.....
000040E0	00	6C	00	00	00	00	00	00	06	00	00	00	00	00	00	00	..1.....
000040F0	04	03	24	00	4D	00	46	00	54	00	00	00	00	00	00	00	..\$.M.F.T.....
00004100	80	00	00	00	48	00	00	00	01	00	40	00	00	00	01	00	[?].H.....@.....
00004110	00	00	00	00	00	00	00	00	7A	02	00	00	00	00	00	00z.....
00004120	40	00	00	00	00	00	00	00	B0	27	00	00	00	00	00	00	@.....°'.....

Рисунок 5 - Пример размера записи MFT

Практика. Посмотрим на нашу MFT-таблицу (см. рис. 4). Из неё видно, что размер записи MFT равен 0x400. Теперь посчитаем смещение до корневой папки: $0x4000 + 0x400 * 5 = 0x5400$.

Калькулятор

DEC:	21504	HEX:	0x5400
Счеты	0x200 * 8 * 4 + 0x400 * 5		Вычислить

Рисунок 6 - Подсчёт смещения до корневой папки

Теперь посчитаем сектор корневой директории: $0x5400 / 0x200 = 42$.

Перейдём в этот сектор:

данные сектора

```

offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0005400 46 49 4C 45 30 00 03 00 00 00 00 00 00 00 00 00 FILE0.....
0005410 05 00 01 00 38 00 03 00 00 02 00 00 00 04 00 00 |...8.....
0005420 00 00 00 00 00 00 00 00 06 00 00 00 05 00 00 00 |.....
0005430 0C 00 00 00 00 00 00 10 00 00 00 48 00 00 00 00 |.....H...
0005440 00 00 18 00 00 00 00 30 00 00 00 18 00 00 00 00 |.....0....
0005450 00 6F 9A 23 05 A2 D9 01 67 C0 C9 62 05 A2 D9 01 |.oB#.fU..gAÉb.fU..
0005460 67 C0 C9 62 05 A2 D9 01 67 C0 C9 62 05 A2 D9 01 |gAÉb.fU..oB#.fU..
0005470 26 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |&.....
0005480 30 00 00 00 60 00 00 00 00 00 18 00 00 00 01 00 |0...`.....
0005490 44 00 00 00 18 00 01 00 05 00 00 00 00 05 00 00 |D.....
00054A0 00 6F 9A 23 05 A2 D9 01 67 C0 C9 62 05 A2 D9 01 |.oB#.fU..oB#.fU..
00054B0 00 6F 9A 23 05 A2 D9 01 67 C0 C9 62 05 A2 D9 01 |.oB#.fU..oB#.fU..
00054C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....
00054D0 06 00 00 10 00 00 00 01 03 2E 00 00 00 00 00 00 |.....
00054E0 50 00 00 00 48 00 00 01 00 40 00 00 00 02 00 00 |P...H.....@...
00054F0 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 |.....
0005500 40 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 |@.....
0005510 2C 10 00 00 00 00 00 2C 10 00 00 00 00 00 00 00 |,.....
0005520 21 02 0F 0B 00 00 00 90 00 00 00 58 00 00 00 00 |!.....B...X...
0005530 00 04 18 00 00 00 03 38 00 00 00 20 00 00 00 00 |.....8....
0005540 24 00 40 00 33 00 30 00 30 00 00 01 00 00 00 00 |с т з а а

```

Задача

Имя файла ZRMCy/zFTTw/rXrmr/ZRMCy

Инструменты

Номер сектора [Выгрузить](#)

Ответ

MD5

Калькулятор

DEC: 42 HEX: 0x2a

Счеты (0x200 * 8 * 4 + 0x400 * 5) / 0x2a

Рисунок 7 - Корневая директория

Шаг 4 - Нахождение таблицы индексов для текущей папки

Теория. Таблица индексов - таблица, содержащая имена всех файлов и директорий в текущей папки, а также смещение до этих файлов / директорий относительно таблицы MFT.

Чтобы перейти в таблицу индексов, нужно для начала найти определённый атрибут таблицы индексов. Всего атрибутов 7:

1. 10 - STANDARD_INFORMATION
2. 30 - FILE_NAME
3. 50 - SECURITY
4. 80 - DATA
5. 90 - ROOT_INDEX
6. A0 - INDEX_ALLOCATION
7. B0 - BITMAP

Из них нам важны лишь 4-ый и 6-ый атрибуты.

Для того, чтобы попасть в таблицу индексов нужно найти атрибут A0. Он хранится в таблице атрибутов.

Для начала найдём таблицу атрибутов. Для этого нам понадобится смещение от текущей папки до таблицы атрибутов. Оно всегда находится здесь:

```
offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00005400 46 49 4C 45 30 00 03 00 00 00 00 00 00 00 00 | FILE0.....
00005410 05 00 01 00 38 00 03 00 00 02 00 00 00 04 00 00 | ....8.....
00005420 00 00 00 00 00 00 00 00 06 00 00 00 05 00 00 00 | .....
00005430 0C 00 00 00 00 00 00 00 10 00 00 00 48 00 00 00 | .....H...
00005440 00 00 18 00 00 00 00 00 30 00 00 00 18 00 00 00 | .....0.....
00005450 00 DF 8C 99 E1 A1 D9 01 3B 4D A3 D7 E1 A1 D9 01 | .ßðáÿÛ.;MExáÿÛ.
00005460 3B 4D A3 D7 E1 A1 D9 01 00 DF 8C 99 E1 A1 D9 01 | ;MExáÿÛ..ßðáÿÛ.
00005470 26 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | &.....
00005480 30 00 00 00 60 00 00 00 00 00 18 00 00 00 01 00 | 0...`.....
00005490 44 00 00 00 18 00 01 00 05 00 00 00 00 00 05 00 | D.....
000054A0 00 DF 8C 99 E1 A1 D9 01 00 DF 8C 99 E1 A1 D9 01 | .ßðáÿÛ..ßðáÿÛ.
000054B0 00 DF 8C 99 E1 A1 D9 01 00 DF 8C 99 E1 A1 D9 01 | .ßðáÿÛ..ßðáÿÛ.
000054C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
000054D0 06 00 00 10 00 00 00 00 01 03 2E 00 00 00 00 00 | .....
000054E0 50 00 00 00 48 00 00 00 01 00 40 00 00 00 02 00 | P...H.....@....
000054F0 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 | .....
00005500 40 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 | @.....
00005510 2C 10 00 00 00 00 00 00 2C 10 00 00 00 00 00 00 | ,.....,.....
00005520 21 03 84 16 00 00 00 00 90 00 00 00 58 00 00 00 | !.ð.....ð...X...
```

Рисунок 8 - Смещение от текущей папки до таблицы атрибутов

Теперь чтобы найти начало таблицы атрибутов(смещение до первого атрибута) надо к смещению текущей папки прибавить смещение до таблицы атрибутов. То есть формула начала таблицы атрибутов следующая: Смещение текущей папки + смещение до таблицы атрибутов.

Первые 4 байта занимает идентификатор типа атрибута, который показывает что это за атрибут. Следующие 4 байта занимает размер атрибута. Это является шаблоном для всех атрибутов.

offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00005400	46	49	4C	45	30	00	03	00	00	00	00	00	00	00	00	00	FILE0...
00005410	05	00	01	00	38	00	03	00	00	02	00	00	00	04	00	008.....
00005420	00	00	00	00	00	00	00	00	00	06	00	00	00	05	00	00
00005430	0C	00	00	00	00	00	00	00	10	00	00	00	48	00	00	00H...
00005440	00	00	18	00	00	00	00	00	30	00	00	00	18	00	00	000.....
00005450	00	DF	8C	99	E1	A1	D9	01	3B	4D	A3	D7	E1	A1	D9	01	.ß¸áÿÛ.;MExáÿÛ.
00005460	3B	4D	A3	D7	E1	A1	D9	01	00	DF	8C	99	E1	A1	D9	01	;MExáÿÛ.ß¸áÿÛ.
00005470	26	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	&.....
00005480	30	00	00	00	60	00	00	00	00	00	18	00	00	00	01	00	0...^.....
00005490	44	00	00	00	18	00	01	00	05	00	00	00	00	00	05	00	D.....
000054A0	00	DF	8C	99	E1	A1	D9	01	00	DF	8C	99	E1	A1	D9	01	.ß¸áÿÛ.ß¸áÿÛ.
000054B0	00	DF	8C	99	E1	A1	D9	01	00	DF	8C	99	E1	A1	D9	01	.ß¸áÿÛ.ß¸áÿÛ.
000054C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000054D0	06	00	00	10	00	00	00	00	01	03	2E	00	00	00	00	00
000054E0	50	00	00	00	48	00	00	00	01	00	40	00	00	00	02	00	P...H....@.....
000054F0	00	00	00	00	00	00	00	00	02	00	00	00	00	00	00	00
00005500	40	00	00	00	00	00	00	00	00	18	00	00	00	00	00	00	@.....
00005510	2C	10	00	00	00	00	00	00	2C	10	00	00	00	00	00	00	,.....,.....
00005520	21	03	84	16	00	00	00	00	90	00	00	00	58	00	00	00	!¸.....¸...X...
00005530	00	04	18	00	00	00	03	00	38	00	00	00	20	00	00	008... ..

Рисунок 9 - пример атрибута

После того, как мы нашли начало таблицы атрибутов надо найти нужный нам атрибут. На данном шаге это «A0».

Назовём смещение до начала таблицы атрибутов буквой «М». Поиск нужного атрибута происходит следующим образом:

1. Смотрим идентификатор атрибута. Если он равен тому, что мы ищем, то останавливаемся, иначе переходим ко второму пункту
2. Смотрим размер атрибута
3. Выполняем следующее действие: $M = M + \text{размер атрибута}$
4. Переходим по смещению M , тем самым попав в начало следующего атрибута
5. Возвращаемся в пункт 1

После того как мы нашли запись нужного нам атрибута, надо её проанализировать.

The image shows a hex dump of memory data. Several fields are highlighted with red boxes and numbered 1 through 5:

- 1:** Points to the attribute identifier 'A0' in the first row.
- 2:** Points to the non-resident flag '01' in the first row.
- 3:** Points to the offset '48' in the third row.
- 4:** Points to the series list '21 01 11 0B' in the fifth row.
- 5:** Points to the data size '10' in the fourth row.

The hex dump lines are as follows:

```

00005580 A0 00 00 00 50 00 00 00 01 04 40 00 00 00 05 00 | ...P.....@.....
00005590 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
000055A0 48 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 | H.....
000055B0 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 | .....
000055C0 24 00 49 00 33 00 30 00 21 01 11 0B 00 00 00 00 | $.I.3.0.!.....
000055D0 B0 00 00 00 28 00 00 00 00 04 18 00 00 00 04 00 | °...(.....
000055E0 08 00 00 00 20 00 00 00 24 00 49 00 33 00 30 00 | .... ..$.I.3.0.
000055F0 01 00 00 00 00 00 00 00 FF FF FF FF 00 00 0C 00 | .....ÿÿÿÿ....
  
```

Рисунок 10 - пример атрибута «A0»

В зоне 1 указан идентификатор атрибута.

В зоне 2 указан флаг нерезидентности (01 - нерезидентный, 00 - резидентный).

В зоне 3 указано смещение до списка серий от начала атрибута.

В зоне 4 указан пример списка серий (он не всегда будет там, надо считать по смещению).

В зоне 5 указан размер данных.

Атрибут «A0» не может быть резидентным.

В выделенной области указано смещение до списка серий от начала атрибута. То есть формула смещения до списка серий будет следующая: M + смещение до списка серий от начала атрибута.

В рамках данного методического пособия у нас нет необходимости углубляться в теоретические определения списка серий, следовательно просто применим его на практике.

После того как мы найдём список серий, переместившись на его смещение, возьмём его первый байт и сложим его цифры(например если байт равен 21, то делаем так: $2 + 1 = 3$), полученное значение означает сколько байт после первого нужно взять. После того как мы взяли необходимое число байт их надо правильно разбить. Делается это следующим образом:

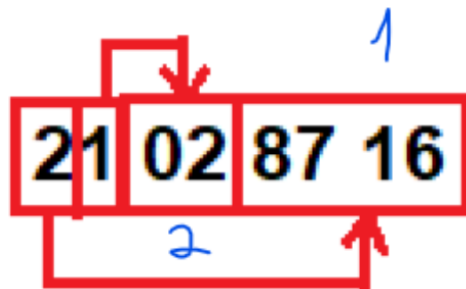


Рисунок 11 - Пример разбиение списка серий

В зоне 1 указано смещение до области данных в кластерах от 0.

В зоне 2 указано сколько кластеров занимает область данных.

Далее нам нужно переместиться в область данных на таблицу индексов. Для этого нам надо умножить размер сектора на количество секторов в кластере и на полученное смещение. То есть формула смещения области данных на таблицу индексов следующая: Размер сектора*Количество секторов в кластере*Смещение до области данных в кластерах.

Чтобы найти сектор области данных на таблицу индексов надо смещение области данных на таблицу индексов поделить на размер сектора. То есть формула следующая: Смещение области данных на таблицу индексов / Размер сектора.

На этом моменте можно было бы уйти курить траву, или что тяжелее, однако еще не время, впереди столько всего не интересного)

Практика. Ещё раз взглянем на корневую папку:

данные сектора

offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00005400	46	49	4C	45	30	00	03	00	00	00	00	00	00	00	00	00
00005410	05	00	01	00	38	00	03	00	00	02	00	00	00	04	00	00
00005420	00	00	00	00	00	00	00	00	06	00	00	00	05	00	00	00
00005430	0C	00	00	00	00	00	00	00	10	00	00	00	48	00	00	00
00005440	00	00	18	00	00	00	00	00	30	00	00	00	18	00	00	00
00005450	00	6F	9A	23	05	A2	D9	01	67	C0	C9	62	05	A2	D9	01
00005460	67	C0	C9	62	05	A2	D9	01	00	6F	9A	23	05	A2	D9	01
00005470	26	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00005480	30	00	00	00	60	00	00	00	00	18	00	00	00	01	00	00
00005490	44	00	00	00	18	00	01	00	05	00	00	00	00	05	00	00
000054A0	00	6F	9A	23	05	A2	D9	01	00	6F	9A	23	05	A2	D9	01
000054B0	00	6F	9A	23	05	A2	D9	01	00	6F	9A	23	05	A2	D9	01
000054C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000054D0	06	00	00	10	00	00	00	00	01	03	2E	00	00	00	00	00
000054E0	50	00	00	00	48	00	00	00	01	00	40	00	00	00	02	00
000054F0	00	00	00	00	00	00	00	00	01	00	00	00	00	00	00	00
00005500	40	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00
00005510	2C	10	00	00	00	00	00	00	2C	10	00	00	00	00	00	00
00005520	21	02	0F	08	00	00	00	00	90	00	00	00	58	00	00	00
00005530	00	04	18	00	00	03	00	38	00	00	00	20	00	00	00	00
00005540	74	00	00	00	33	00	30	00	00	00	00	01	00	00	00	00

Задание

Имя файла: ZRMCy/zFTTw/rXrmr/ZRMCy

Инструменты

Номер сектора: 42 [Выгрузить](#)

Ответ

MD5:

Калькулятор

DEC: 42 HEX: 0x2a

Счеты: $(0x200 * 8 * 4 + 0x400 * 5) / 0x2$

Рисунок 12 - Корневая директория

Из него видно, что смещение до таблицы атрибутов равно 0x38. Тогда начала таблицы атрибутов равно $0x200 * 8 * 4 + 0x400 * 5 + 0x38$. Получаем 0x5438.

Далее ищем атрибут «A0». После того, как нашли его, взглянем на него:

```

-----
00005580 A0 00 00 00 50 00 00 00 01 04 40 00 00 00 05 00| ...P.....@.....
00005590 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....
000055A0 48 00 00 00 00 00 00 00 00 10 00 00 00 00 00| H.....
000055B0 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00| .....
000055C0 24 00 49 00 33 00 30 00 21 01 11 0B 00 00 00 00| $.I.3.0.!.....
000055D0 B0 00 00 00 28 00 00 00 00 04 18 00 00 00 04 00| °...(.....
000055E0 08 00 00 00 20 00 00 00 24 00 49 00 33 00 30 00| .... ..$.I.3.0.
000055F0 01 00 00 00 00 00 00 00 FF FF FF FF 00 00 0C 00| .....ÿÿÿÿ....

```

Рисунок 13 - Атрибут «A0»

Из него видно, что атрибут нерезидентный, смещение до списка серий от атрибута равно 0x48. Тогда смещение до списка серий равно 0x5580 + 0x48. Получаем 0x55C8.

Далее смотрим список серий. Он следующий: 21 01 11 0B.

Проанализировав его, получаем, что смещение до таблицы индексов равно 0xb11. Тогда сектор таблицы индексов равен $0x200 * 8 * 0xb11 / 0x200$.

Получаем 22664. Перейдём в него:

```

offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00B11000 49 4E 44 58 28 00 09 00 00 00 00 00 00 00 00 00| INDX(.....
00B11010 00 00 00 00 00 00 00 00 28 00 00 00 00 00 07 00 00| .....(..D...
00B11020 E8 0F 00 00 00 00 00 00 47 0E D9 01 00 00 01 00| è.....G.Ü.....
00B11030 D9 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00| Ü.....
00B11040 04 00 00 00 00 00 04 00 68 00 52 00 00 00 00 00| .....h.R.....
00B11050 05 00 00 00 00 05 00 00 6F 9A 23 05 A2 D9 01 00| .....oö#.#.Ü.
00B11060 00 6F 9A 23 05 A2 D9 01 00 6F 9A 23 05 A2 D9 01| .oö#.#.Ü.
00B11070 00 6F 9A 23 05 A2 D9 01 00 10 00 00 00 00 00 00| .oö#.#.Ü.
00B11080 00 0A 00 00 00 00 00 00 06 00 00 00 00 00 00 00| .....
00B11090 08 03 24 00 41 00 74 00 74 00 44 00 65 00 00| ..$.A.t.t.r.D.e.
00B110A0 66 00 00 00 00 00 01 00 08 00 00 00 00 08 00 00| f.....
00B110B0 68 00 52 00 00 00 00 05 00 00 00 00 00 05 00| h.R.....
00B110C0 00 6F 9A 23 05 A2 D9 01 00 6F 9A 23 05 A2 D9 01| .oö#.#.Ü.
00B110D0 00 6F 9A 23 05 A2 D9 01 00 6F 9A 23 05 A2 D9 01| .oö#.#.Ü.
00B110E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....
00B110F0 06 00 00 00 00 00 00 08 03 24 00 42 00 61 00 00| .....$.B.a.
00B11100 64 00 43 00 6C 00 75 00 73 00 00 00 00 07 00 00| d.C.I.u.s.....
00B11110 06 00 00 00 00 00 06 00 60 00 50 00 00 00 00 00| .....".P.....
00B11120 05 00 00 00 00 05 00 00 6F 9A 23 05 A2 D9 01| .....oö#.#.Ü.
00B11130 00 6F 9A 23 05 A2 D9 01 00 6F 9A 23 05 A2 D9 01| .oö#.#.Ü.

```

Имя файла

Инструменты

Номер сектора [Выгрузить](#)

Ответ

MD5 [Отправить](#)

Калькулятор

DEC:
HEX:

Счеты [Вычислить](#)

Рисунок 14 - Таблица индексов

Шаг 5 - Переход по таблице индексов в следующую директорию

Теория. Попад в таблицу индексов надо сделать несколько вещей.

Во-первых найти смещение начала данных.

Таблица индекса состоит из заголовка (который всегда имеет фиксированный размер), после этого находится список маркеров, далее идет область данных. Каждый маркер занимает 2 байта. Смещение до списка маркеров и количество маркеров хранятся в заголовке:

```

offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00B43800 49 4E 44 58 28 00 09 00 00 00 00 00 00 00 00 00 | INDX(.....
00B43810 00 00 00 00 00 00 00 00 28 00 00 00 D0 07 00 00 | .....(...D...
00B43820 E8 0F 00 00 00 00 00 00 46 0E D9 01 00 00 01 00 | è.....F.Ù....
00B43830 D9 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | Ù.....
00B43840 04 00 00 00 00 00 04 00 68 00 52 00 00 00 00 00 | .....h.R....
00B43850 05 00 00 00 00 00 05 00 00 DF 8C 99 E1 A1 D9 01 | .....ßáÛ.
00B43860 00 DF 8C 99 E1 A1 D9 01 00 DF 8C 99 E1 A1 D9 01 | .ßáÛ.ßáÛ.
00B43870 00 DF 8C 99 E1 A1 D9 01 00 10 00 00 00 00 00 00 | .ßáÛ.....
00B43880 00 0A 00 00 00 00 00 00 06 00 00 00 00 00 00 00 | .....
00B43890 08 03 24 00 41 00 74 00 74 00 72 00 44 00 65 00 | ..$.A.t.t.r.D.e.
00B438A0 66 00 00 00 00 00 01 00 08 00 00 00 00 08 00 | f.....
00B438B0 68 00 52 00 00 00 00 00 05 00 00 00 00 00 05 00 | h.R.....

```

Рисунок 15 - Пример таблицы индексов

В зоне 1 указано смещение до списка маркеров.

В зоне 2 указано количество маркеров в списке

Теперь нам нужно найти смещение до начала данных таблицы индексов.

Чтобы это сделать мы должны сложить смещение таблицы индексов и смещением до списка маркеров, далее к этому прибавить количество маркеров, умноженное на 2 (так как размер маркера 2 байта). То есть формула смещение до начала данных таблицы индексов следующая:

Смещение таблицы индексов + Смещением до списка маркеров + количество маркеров * 2.

Получаем смещение, однако данные после атрибута, всегда начинаются со смещения, кратного 8 (оканчивается на 0 или 8), поэтому к текущему количеству маркеров прибавляем 1, до тех пор, пока не дойдем до смещения, кратного 8.

offset 00 01 02 03 04 05 06 07 08 0A 0B 0C 0D 0E 0F

00B43800 45 4E 44 58 28 00 09 00 00 00 00 00 00 00 | INDX(.....

00B43810 00 00 00 00 00 00 28 00 00 00 D0 07 00 00 |(....D...|

00B43820 E8 0F 00 00 00 00 00 46 0E D9 01 00 01 00 | e.....F.U....|

00B43830 D9 01 00 00 00 00 00 00 00 00 00 00 00 00 | U.....|

00B43840 04 00 00 00 00 04 00 68 00 52 00 00 00 00 |h.R.....|

00B43850 05 00 00 00 00 05 00 DF 8C 99 E1 A1 D9 01 |80B43U..|

00B43860 00 DF 8C 99 E1 A1 D9 01 00 DF 8C 99 E1 A1 D9 01 | .80B43U...80B43U..|

00B43870 00 DF 8C 99 E1 A1 D9 01 00 10 00 00 00 00 00 00 | .80B43U.....|

00B43880 00 0A 00 00 00 00 00 00 06 00 00 00 00 00 00 ||

00B43890 08 03 24 00 41 00 74 00 74 00 72 00 44 00 65 00 | ..\$.A.t.t.r.D.e. 3

00B438A0 66 00 00 00 00 01 00 08 00 00 00 00 08 00 00 | f.....|

00B438B0 68 00 52 00 00 00 00 05 00 00 00 00 05 00 | h.R.....|

00B438C0 00 DF 8C 99 E1 A1 D9 01 00 DF 8C 99 E1 A1 D9 01 | .80B43U...80B43U..|

00B438D0 00 DF 8C 99 E1 A1 D9 01 00 DF 8C 99 E1 A1 D9 01 | .80B43U...80B43U..|

00B438E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ||

00B438F0 06 00 00 00 00 00 00 08 03 24 00 42 00 61 00 |\$.B.a....|

00B43900 64 00 43 00 6C 00 75 00 73 00 00 00 00 07 00 | d.C.l.u.s.....|

00B43910 06 00 00 00 00 00 06 00 00 00 50 00 00 00 00 |P.....|

00B43920 05 00 00 00 00 05 00 00 DF 8C 99 E1 A1 D9 01 |80B43U..|

Имя файла UNEPq/KFIMB/UNEPq/UNEPq

Инструменты

Номер сектора 23068

Ответ

MD5

Отправить

Калькулятор

DEC:	11810880	HEX:	0xb43840
------	----------	------	----------

Счеты	$0xb43800 + 0x28 + 12 * 2$	Вычислить
-------	----------------------------	-----------

В зоне 1 указано смещение относительно MFT таблицы до данного файла/папки

В зоне 2 указано смещение до следующего индекса, относительно текущего

В зоне 3 указано имя рассматриваемого атрибута (Для того, чтобы понять имя, провести линию относительно полученного смещения и найти ближайшее к смещению имя(см. рис. 15))

Смотрим на имя, если оно не равно папке или файлу, который требуется найти, то мы переходим на следующий индекс, путем сложения текущего смещения и смещения до следующего атрибута.

Снова сравниваем имена и продолжаем переходить по индексам до тех пор, пока не попадем в нужную папку.

Стоит отметить, что папка после файла \$Volume - корневая, поэтому там нет названия.

Когда мы дошли до названия файла/директории, мы получаем первые 2 байта(см. рис. 16), это и будет являться смещением относительно таблицы MFT. Теперь надо посчитать смещение до файла/директории. Формула следующая: Смещение MFT таблицы + Смещение относительно таблицы MFT.

Чтобы получить сектор, в котором хранится файл/директория надо поделить смещение до файла/директории на размер сектора. То есть формула сектора файла/директории следующая: Смещение до файла/директории / Размер сектора.

```
offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00C5A400 00 00 02 00 00 00 00 06 00 00 00 00 00 00 00| .....
00C5A410 07 03 24 00 55 00 70 00 43 00 61 00 73 00 65 00| ..$.U.p.C.a.s.e.
00C5A420 03 00 00 00 00 00 03 00 60 00 50 00 00 00 00 00| .....P.....
00C5A430 05 00 00 00 00 00 05 00 66 D1 A5 FA A1 D9 01| .....fñwújÛ.
00C5A440 00 66 D1 A5 FA A1 D9 01 00 66 D1 A5 FA A1 D9 01| .fñwújÛ..fñwújÛ.
00C5A450 00 66 D1 A5 FA A1 D9 01 00 00 00 00 00 00 00 00| .fñwújÛ.....
00C5A460 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00| .....
00C5A470 07 03 24 00 56 00 6F 00 6C 00 75 00 6D 00 65 00| ..$.V.o.l.u.m.e.
00C5A480 05 00 00 00 00 00 05 00 58 00 44 00 00 00 00 00| .....X.D.....
00C5A490 05 00 00 00 00 00 05 00 66 D1 A5 FA A1 D9 01| .....fñwújÛ.
00C5A4A0 09 ED F5 E5 FA A1 D9 01 09 ED F5 E5 FA A1 D9 01| .iðáújÛ..iðáújÛ.
00C5A4B0 00 66 D1 A5 FA A1 D9 01 00 00 00 00 00 00 00 00| .fñwújÛ.....
00C5A4C0 00 00 00 00 00 00 00 26 00 00 10 00 00 00 00 00| .....8.....
00C5A4D0 01 03 2E 00 00 00 00 39 02 00 00 00 00 01 00 00| .....9.....
00C5A4E0 60 00 4C 00 00 00 00 05 00 00 00 00 00 05 00 00| `L.....
00C5A4F0 60 F9 30 A7 FA A1 D9 01 28 2C EC E5 FA A1 D9 01| `ùø$újÛ.(,iáújÛ.
00C5A500 28 2C EC E5 FA A1 D9 01 60 F9 30 A7 FA A1 D9 01| (,iáújÛ..ùø$újÛ.
00C5A510 00 30 00 00 00 00 00 58 22 00 00 00 00 00 00 00| .0.....X".....
00C5A520 20 00 00 00 00 00 00 05 00 42 00 6E 00 5A 00 00| .....B.n.Z.
00C5A530 56 00 78 00 00 00 00 40 00 00 00 00 00 01 00 00| V.X.....ß.....
00C5A540 60 00 4C 00 00 00 00 05 00 00 00 00 00 05 00 00| `L.....
00C5A550 2F DD 11 A7 FA A1 D9 01 55 AD 36 A7 FA A1 D9 01| /Y.$újÛ.üø$újÛ.
00C5A560 55 AD 36 A7 FA A1 D9 01 2F DD 11 A7 FA A1 D9 01| üø$újÛ./Y.$újÛ.
00C5A570 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....
00C5A580 20 00 00 10 00 00 00 05 00 64 00 43 00 68 00 00| .....d.C.h.
00C5A590 5A 00 6C 00 00 00 00 00 55 00 00 00 00 01 00 00| .....Z.L.....U.....
00C5A5A0 60 00 4C 00 00 00 00 05 00 00 00 00 00 05 00 00| `L.....
00C5A5B0 55 0A 13 A7 FA A1 D9 01 46 0E 3B A7 FA A1 D9 01| U..$újÛ.F.;$újÛ.
00C5A5C0 46 0E 3B A7 FA A1 D9 01 55 0A 13 A7 FA A1 D9 01| F.;$újÛ.U..$újÛ.
00C5A5D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....
00C5A5E0 20 00 00 10 00 00 00 05 00 4D 00 51 00 56 00 00| .....M.Q.V.
00C5A5F0 41 00 78 00 00 00 00 00 47 00 00 00 00 49 0E 00| A.X.....G.....I.
```

Имя файла

MQVAX/NxFWI/OuUmg/BnZVx

Инструменты

Номер сектора

25298

Выгрузить

Ответ

MD5

Отправить

Калькулятор

DEC:

12952984

HEX:

0xc5a598

Счеты

0x200 * 8 * 0xc5a + 0x28 + 12 * 2 + 0x68 *

Вычислить

Для заметок

Рисунок 17 - Первые два байта записи файла/директории

Перейдя в найденный сектор мы попадём в искомую папку. Далее, повторяя шаги 4 и 5, переходим по остальным папкам и находим файл.

Практика. Ещё раз взглянем на таблицу индексов:


```

offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00B11000 49 4E 44 58 28 00 09 00 00 00 00 00 00 00 00| INDX(.....
00B11010 00 00 00 00 00 00 00 00 28 00 00 00 00 07 00| .....(....D...
00B11020 E8 0F 00 00 00 00 00 00 47 0E D9 01 00 00 01| è.....G.Û.....
00B11030 D9 01 00 00 00 00 00 00 00 00 00 00 00 00 00| Û.....
00B11040 04 00 00 00 00 00 04 00 68 00 52 00 00 00 00| .....h.R.....
00B11050 05 00 00 00 00 00 05 00 00 6F 9A 23 05 A2 D9 01| .....oB#.фÛ.
00B11060 00 6F 9A 23 05 A2 D9 01 00 6F 9A 23 05 A2 D9 01| .oB#.фÛ..oB#.фÛ.
00B11070 00 6F 9A 23 05 A2 D9 01 00 10 00 00 00 00 00 00| .oB#.фÛ.....
00B11080 00 0A 00 00 00 00 00 00 06 00 00 00 00 00 00| .....
00B11090 08 03 24 00 41 00 74 00 74 00 72 00 44 00 65 00| ..$.A.t.t.r.D.e.
00B110A0 66 00 00 00 00 00 01 00 08 00 00 00 00 08 00| f.....
00B110B0 68 00 52 00 00 00 00 00 05 00 00 00 00 05 00| h.R.....
00B110C0 00 6F 9A 23 05 A2 D9 01 00 6F 9A 23 05 A2 D9 01| .oB#.фÛ..oB#.фÛ.
00B110D0 00 6F 9A 23 05 A2 D9 01 00 6F 9A 23 05 A2 D9 01| .oB#.фÛ..oB#.фÛ.
00B110E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....
00B110F0 06 00 00 00 00 00 00 00 08 03 24 00 42 00 61 00| .....$.B.a.
00B11100 64 00 43 00 6C 00 75 00 73 00 00 00 00 07 00| d.C.l.u.s.....
00B11110 06 00 00 00 00 00 06 00 60 00 50 00 00 00 00| .....`.P.....
00B11120 05 00 00 00 00 00 05 00 00 6F 9A 23 05 A2 D9 01| .....oB#.фÛ.
00B11130 00 6F 9A 23 05 A2 D9 01 00 6F 9A 23 05 A2 D9 01| .oB#.фÛ..oB#.фÛ.
00B11140 00 6F 9A 23 05 A2 D9 01 00 10 00 00 00 00 00 00| .oB#.фÛ.....

```

Рисунок 18 - Таблица индексов

Из неё видно, что смещение до списка маркеров от начала таблицы индексов равно 0x28, а количество маркеров равно 9. Соответственно смещение до начала данных равно $0xB11000 + 0x28 + 9 * 2$. В теперь прибавляем единицу к 9, пока смещение не станет кратным 8. В итоге получаем, что смещение до начала данных равно $0xB11000 + 0x28 + 12 * 2$.

Далее переходим по индексам до тех пор, пока не найдём нужный нам атрибут(папку, в которую нам надо перейти). Взглянем на него:

```

00B11710 54 00 77 00 00 00 00 00 44 00 00 00 00 01 00| T.w.....D.....
00B11720 60 00 4C 00 00 00 00 00 05 00 00 00 00 05 00| `.L.....
00B11730 99 3D 2D 25 05 A2 D9 01 F9 94 53 25 05 A2 D9 01| B=-%.фÛ.ûB$%.фÛ.
00B11740 F9 94 53 25 05 A2 D9 01 99 3D 2D 25 05 A2 D9 01| ûB$%.фÛ.B=-%.фÛ.
00B11750 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....
00B11760 20 00 00 10 00 00 00 00 05 00 5A 00 52 00 4D 00| .....Z.R.M.
00B11770 43 00 79 00 00 00 00 00 BD 01 00 00 00 01 00| C.y.....X.....
00B11780 60 00 4C 00 00 00 00 00 05 00 00 00 00 05 00| `.L.....

```

Рисунок 19 - Необходимый атрибут

Из него видно, что смещение до файла/папки от начала таблицы MFT равно 0x44. Посчитаем смещение до файла/папки: $0x200 * 8 * 4 + 0x400 * 0x44$. Делим полученное число на 512 и получаем сектор файла/папки. Перейдём в него:

```

offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00015000 46 49 4C 45 30 00 03 00 00 00 00 00 00 00 00 00| FILE0.....
00015010 01 00 01 00 38 00 03 00 28 02 00 00 00 04 00 00| ....8...(.....
00015020 00 00 00 00 00 00 00 00 06 00 00 00 44 00 00 00| .....D...
00015030 20 00 00 00 00 00 00 00 10 00 00 00 48 00 00 00| .....H...
00015040 00 00 00 00 00 00 00 00 30 00 00 00 18 00 00 00| .....0.....
00015050 99 3D 2D 25 05 A2 D9 01 F9 94 53 25 05 A2 D9 01| Ì=-%.çÛ.ÛÛS%.çÛ.
00015060 F9 94 53 25 05 A2 D9 01 99 3D 2D 25 05 A2 D9 01| ÛÛS%.çÛ.Ì=-%.çÛ.
00015070 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....
00015080 30 00 00 00 68 00 00 00 00 00 00 00 00 00 03 00| 0...h.....
00015090 4C 00 00 00 18 00 01 00 05 00 00 00 00 00 05 00| L.....
000150A0 99 3D 2D 25 05 A2 D9 01 99 3D 2D 25 05 A2 D9 01| Ì=-%.çÛ.Ì=-%.çÛ.
000150B0 99 3D 2D 25 05 A2 D9 01 99 3D 2D 25 05 A2 D9 01| Ì=-%.çÛ.Ì=-%.çÛ.
000150C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....
000150D0 20 00 00 10 00 00 00 00 05 00 5A 00 52 00 4D 00| .....Z.R.M.
000150E0 43 00 79 00 00 00 00 00 50 00 00 00 68 00 00 00| C.y....P...h...
000150F0 00 00 00 00 00 00 01 00 50 00 00 00 18 00 00 00| .....P.....
00015100 01 00 04 80 14 00 00 00 24 00 00 00 00 00 00 00| ...Û....$......
00015110 34 00 00 00 01 02 00 00 00 00 00 05 20 00 00 00| 4.....
00015120 20 02 00 00 01 02 00 00 00 00 00 05 20 00 00 00| .....
00015130 20 02 00 00 02 00 1C 00 01 00 00 00 00 03 14 00| .....
00015140 FF 01 1F 00 01 01 00 00 00 00 00 01 00 00 00 00| Ÿ.....
00015150 90 00 00 00 58 00 00 00 00 04 18 00 00 00 02 00| Ì...X.....
00015160 38 00 00 00 20 00 00 00 24 00 49 00 33 00 30 00| 8... ..$.I.3.0.
00015170 30 00 00 00 01 00 00 00 00 10 00 00 01 00 00 00| 0.....
00015180 10 00 00 00 28 00 00 00 28 00 00 00 01 00 00 00| ....(...(.....
00015190 00 00 00 00 00 00 00 00 18 00 00 00 03 00 00 00| .....
000151A0 00 00 00 00 00 00 00 00 A0 00 00 00 50 00 00 00| ..... ..P...
000151B0 01 04 40 00 00 00 05 00 00 00 00 00 00 00 00 00| ..@.....
000151C0 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00| .....H.....
000151D0 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00| .....
000151E0 00 10 00 00 00 00 00 00 24 00 49 00 33 00 30 00| .....$.I.3.0.
000151F0 21 01 32 3E 00 00 00 00 B0 00 00 00 28 00 20 00| !.2>....°...( .

```

Рисунок 20 - Следующая папка

Далее повторяем шаги с четвёртого по пятый до тех пор пока не найдём требуемый файл.

«Безумие - это повторение одного и того же действия, в надежде на изменение»

© Ваас Монтенегро

Шаг 6 - Анализ записи файла

Теория. Первое, что нужно сделать, это в таблице индексов файла найти атрибут 80, затем определить его флаг резидентности. Если резидентный, то смотрите рисунок 17, если нерезидентный, то вспоминаем рисунок 10.

```
offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00052C00 46 49 4C 45 30 00 03 00 00 00 00 00 00 00 00| FILE0.....
00052C10 01 00 01 00 38 00 01 00 F0 01 00 00 00 04 00 00| ....8...đ.....
00052C20 00 00 00 00 00 00 00 00 05 00 00 00 38 01 00 00| .....;...
00052C30 14 00 00 00 00 00 00 00 10 00 00 00 48 00 00 00| .....H...
00052C40 00 00 00 00 00 00 00 00 30 00 00 00 18 00 00 00| .....0.....
00052C50 66 AB 20 A7 FA A1 D9 01 E9 1E AA BF FA A1 D9 01| f« šú;Û.é.žú;Û.
00052C60 E9 1E AA BF FA A1 D9 01 9F 24 F6 E5 FA A1 D9 01| é.žú;Û.Û$ôâú;Û.
00052C70 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| .....
00052C80 30 00 00 00 68 00 00 00 00 00 00 00 00 00 03 00| 0...h.....
00052C90 4C 00 00 00 18 00 01 00 C1 00 00 00 00 00 01 00| L.....Á.....
00052CA0 66 AB 20 A7 FA A1 D9 01 66 AB 20 A7 FA A1 D9 01| f« šú;Û.f« šú;Û.
00052CB0 66 AB 20 A7 FA A1 D9 01 66 AB 20 A7 FA A1 D9 01| f« šú;Û.f« šú;Û.
00052CC0 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00| 0.....
00052CD0 20 00 00 00 00 00 00 00 05 00 42 00 6E 00 5A 00| .....B.n.Z.
00052CE0 56 00 78 00 00 00 00 00 50 00 00 00 68 00 00 00| V.x.....P...h...
00052CF0 00 00 00 00 00 00 01 00 50 00 00 00 18 00 00 00| .....P.....
00052D00 01 00 04 80 14 00 00 00 24 00 00 00 00 00 00 00| ...Û....$.
00052D10 34 00 00 00 01 02 00 00 00 00 00 00 05 20 00 00 00| 4.....
00052D20 20 02 00 00 01 02 00 00 00 00 00 00 05 20 00 00 00| .....
00052D30 20 02 00 00 02 00 1C 00 01 00 00 00 00 03 14 00| .....
00052D40 FF 01 1F 00 01 01 00 00 00 00 00 00 01 00 00 00 00| ŷ.....
00052D50 80 00 00 00 48 00 00 00 00 00 00 00 00 00 02 00| Û...H.....
00052D60 30 00 00 00 18 00 00 00 29 CE C9 5B 64 7E 7A 25| 0.....)ÎÉ[d~z%
00052D70 36 A2 2E ED A8 32 34 8A 09 89 24 3E F3 DF 3F| 6¢.í"24ÛÛ.Û$>óß?
00052D80 90 7A 9F AF 5A 55 90 5C FA C5 B8 B4 B3 7B 78 0A| ÛzÛ"ZUÛ\úÂ, "³{x.
00052D90 E1 73 DD 04 A1 CA D2 89 80 00 00 00 50 00 00 00| ášÝ.¡ÊòÛÛ...P...
00052DA0 01 01 40 00 00 00 04 00 00 00 00 00 00 00 00 00| ..@.....
00052DB0 04 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00| .....H.....
00052DC0 00 50 00 00 00 00 00 00 35 4D 00 00 00 00 00 00| .P.....5M.....
00052DD0 35 4D 00 00 00 00 00 00 6F 00 00 00 00 00 00 00| 5M.....o.....
00052DE0 21 05 CB 35 00 00 00 00 FF FF FF FF 00 00 00 00| !.Ě5....ýýýý...
00052DF0 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 14 00| ýýýý.....
```

Рисунок 21 - Области выделения для резидентного атрибута

В зоне 1 указан идентификатор типа атрибута.

В зоне 2 указан флаг нерезидентности.

В зоне 3 указан размер данных файла.

В зоне 4 указано смещение до данных от начала атрибута 80.

Найдя атрибут, мы должны найти смещение конца данных. Для этого нам надо прибавить к смещению атрибута смещение до данных и размер данных. То есть формула смещения конца данных следующая: Смещение атрибута + Смещение до данных + Размер данных.

Теперь мы скачиваем все сектора начиная с того, в котором был найден атрибут 80, заканчивая тем сектором, где находится смещение конца данных.

Практика. Взглянем на запись файла:

```
offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0005800 46 49 4C 45 30 00 03 00 00 00 00 00 00 00 00 00 FILE0.....
0005810 01 00 01 00 38 00 01 00 F0 01 00 00 00 04 00 00 |...8...8.....
0005820 00 00 00 00 00 00 00 00 05 00 00 00 06 02 00 00 |.....
0005830 18 00 00 00 00 00 00 10 00 00 00 48 00 00 00 |.....H...
0005840 00 00 00 00 00 00 00 30 00 00 00 18 00 00 00 |.....0.....
0005850 1F 21 48 25 05 A2 D9 01 0A 8C CA 49 05 A2 D9 01 |.IhG.40..8E1.40.
0005860 0A 8C CA 49 05 A2 D9 01 0A FA C9 62 05 A2 D9 01 |.8E1.40..0Eb.40.
0005870 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....
0005880 30 00 00 00 68 00 00 00 00 00 00 00 03 00 |0...h.....
0005890 4C 00 00 00 18 00 01 00 5D 00 00 00 00 01 00 |L.....].
00058A0 1F 21 48 25 05 A2 D9 01 1F 21 48 25 05 A2 D9 01 |.IhG.40..IhG.40.
00058B0 1F 21 48 25 05 A2 D9 01 1F 21 48 25 05 A2 D9 01 |.IhG.40..IhG.40.
00058C0 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 |@.....
00058D0 20 00 00 00 00 00 00 05 5A 00 52 00 4D 00 |.....Z.R.M.
00058E0 43 00 79 00 00 00 00 50 00 00 68 00 00 00 00 |C.y.....P...h...
00058F0 00 00 00 00 00 01 00 50 00 00 18 00 00 00 00 |.....P.....
0005900 01 00 04 80 14 00 00 24 00 00 00 00 00 00 00 |...B...$.
0005910 34 00 00 00 01 02 00 00 00 00 05 20 00 00 00 |4.....
0005920 20 02 00 00 01 02 00 00 00 00 05 20 00 00 00 |.....
0005930 20 02 00 00 02 00 1C 00 01 00 00 00 03 14 00 |.....
0005940 FF 01 1F 00 01 01 00 00 00 00 01 00 00 00 00 |y.....
0005950 80 00 00 00 48 00 00 01 00 40 00 00 02 00 00 |B...H.....@.....
0005960 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 |.....
0005970 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 |@.....@.....
0005980 08 34 00 00 00 00 00 08 34 00 00 00 00 00 00 |.4.....4.....
0005990 21 04 91 30 00 00 00 80 00 00 00 50 00 00 00 |I.B0.....B...P...
00059A0 01 01 40 00 00 00 04 00 00 00 00 00 00 00 00 |.4.....
00059B0 03 00 00 00 00 00 00 48 00 00 00 00 00 00 00 |.....H.....
00059C0 00 40 00 00 00 00 00 2D 3C 00 00 00 00 00 00 |@.....<.....
00059D0 2D 3C 00 00 00 00 00 43 00 00 00 00 00 00 00 |<.....C.....
00059E0 21 04 D1 1D 00 00 00 FF FF FF FF 00 00 00 00 |I.B.....yyyy
00059F0 FF FF FF FF 00 00 00 00 00 00 00 00 18 00 |yyyy.....
```

Имя файла

ZRMCy/zFTTw/rXrmr/ZRMCy

Инструменты

Номер сектора

1068

Выгрузить

Ответ

MD5

Отправить

Калькулятор

DEC:

547152

HEX:

0x85950

Счеты

0x85800 + 0x38 + 0x48 + 0x68 * 2

Вычислить

Для заметок

21 01 3D 2E

Рисунок 22 - Запись искомого файла

Далее ищем в нём атрибут 80. Взглянем на него:


```

00085950 80 00 00 00 48 00 00 00 01 00 40 00 00 00 02 00| H...H.....@.....
00085960 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00| .....
00085970 40 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00| @.....@.....
00085980 0B 34 00 00 00 00 00 00 0B 34 00 00 00 00 00 00| .4.....4.....
00085990 21 04 91 30 00 00 00 00 80 00 00 00 50 00 00 00| !.00....0...P...
000859A0 01 01 40 00 00 00 04 00 00 00 00 00 00 00 00 00| ..@.....
000859B0 03 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00| .....H.....
000859C0 00 40 00 00 00 00 00 00 2D 3C 00 00 00 00 00 00| .@.....-<.....
000859D0 2D 3C 00 00 00 00 00 00 43 00 00 00 00 00 00 00| -<.....C.....
000859E0 21 04 D1 1D 00 00 00 00 FF FF FF FF 00 00 00 00| !.ñ....üüüü....
000859F0 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 18 00| üüüü.....

```

Рисунок 23 - Атрибут 80

Из него видно, что он нерезидентный, смещение до списка серий равно 0x40, размер файла 0x340B. Найдём список серий, он равен: 21 04 91 30.

Из него видно, что смещение до начала данных равно 0x3091 сектор от начала образа NTFS и данные занимают пространство 4 кластеров сектор

Считаем смещение до начала данных и переходим по нему: $0x200 * 8 * 0x3091$

```

offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
03091000 42 38 99 6C 06 C4 17 AD 6C 24 BA 43 EC C4 F7 06| 8881.A.15*ciA+.
03091010 D6 1C 9C D7 DE A2 75 F4 9D 4F 01 28 E3 9B 69 58| 0.8x*fu000. (88IX
03091020 A6 A3 82 E1 DF FF 5A 4A 8E F8 A2 91 A4 80 95 12| |888yZ30ef8m"8.
03091030 24 EF EC FE 4D 69 F7 C5 4A DE EC C5 51 A8 D0 C7| $Ijmi+AmplAQ"8C
03091040 D3 C5 11 3F 13 D4 7A 07 F3 68 09 02 E9 47 1C 00| 0A.7.0z.0k..eg..
03091050 19 74 27 48 43 8B 60 7B A1 7E 69 51 44 8C 71 92| .t'Kc~" {j-iQ00q8
03091060 F7 F8 E0 3C 1D F1 13 CD 76 5D 48 58 3B 9D 33 73| +0Ac.ñ.fv)KX;83s
03091070 8B 29 09 0E 79 9E F3 3E E3 A7 C3 88 93 9E 17 78| u).,y00>0$A.88.(
03091080 5E 66 3B 94 80 4A A8 0F CC 85 8E 24 7A 56 B0 41| ^f;887".Ij8$zv^A
03091090 56 56 DB 65 FF B7 66 E0 D8 E1 C5 A0 18 B5 2C D2| vV0ey-fa0A .µ,0
030910A0 18 BD 59 DE FA 3E DA 5E BC 60 B7 D0 BA 19 3D DA| .Xv8u>0^X"·Ye.,u0
030910B0 1E 75 84 34 AC 10 02 5A 72 68 65 D3 A5 92 C5 25| .u84-..Zrke0v8A%
030910C0 43 C3 5D 07 90 88 CE 69 82 7B BF F5 0F C5 87 F5| CA].8.Ii8(z0.A80
030910D0 05 74 90 FE 68 1A E0 39 68 C8 C9 91 F0 3C 9D 55| .t8ph.89ktE80<8U
030910E0 76 D0 F5 43 E3 4C 4C 90 4F 3A 0E B6 4B 2F 22 D8| vY0CAlL80:·9K/"0
030910F0 EE 4E F6 86 15 5E AD F7 21 68 3D 07 94 AC 68 F9| iN08.^+lh=x8-kü
03091100 CA 8B 58 70 D0 66 93 36 5A C1 00 65 BE 84 BE E6| E8xp0f86ZA.eN8ka
03091110 89 94 AB BE 84 78 B2 C5 21 08 B4 87 FC 14 A7 51| ^8x88{^A].^·ü.5Q
03091120 1E B2 4C F4 80 11 38 93 04 71 3B 0E E6 41 04 DC| .^L08.88.q;·8A.U
03091130 11 37 C0 FF A8 D0 D4 6A 30 73 15 6F 87 7B D7 A1| .7Aÿ~Y0j0s.08(xj
03091140 79 E7 24 9E 6C 48 04 0F F3 13 86 63 4A F5 A9 86| yC$8LK..0.8c7000
03091150 13 FC 89 91 A7 7F CE 8D 68 77 C6 CA 4D F7 11 2E| .ü8$88I^808E8..
03091160 E2 59 E3 09 54 5A E7 59 14 81 16 30 62 25 44 8C| äVä.TZçY.8.ob80X
03091170 04 2C D1 36 A5 C9 8A D0 28 B9 FD 70 8E DE 1E AA| .,ñ8vE80(^ÿ)8p.*
03091180 02 DF 96 E5 56 FF 22 A4 64 64 AF 82 D5 29 80 C5| .888vÿ"8dd"80j8A
03091190 CF 5F 95 BC 26 E2 14 B1 18 2D F9 80 E8 B3 CC 9C| Y_88A.+.i88^I8
030911A0 2D 88 43 36 A2 35 8D 38 03 A7 8E 85 D8 9F 29 54| -8C64508.$8800)T
030911B0 FF A5 0C 50 A1 78 0B 8A 08 99 89 A1 6F 2F B5 8D| yX.P|x.8.88jo/µ8
030911C0 69 48 FC 66 8D 71 26 C0 B5 B9 AB 8A 59 32 59 A5| iñüf8q&Aÿ"u~Y2YX
030911D0 82 FC 29 7F 1F CF 8E BE 28 09 D5 6A 65 ED 26 FF| 8Ü)8.I88(.0jei8ÿ
030911E0 93 50 4B CF 98 94 7A FB B9 7A 61 63 17 05 8B 00| 8PKI888z0^zac...·.
030911F0 5A F3 87 FC FD 15 05 E9 AF 01 19 10 78 0E 83 6C| Z088ÿ..é"...x.8I

```

Имя файла

ZRMCy/zFTTw/rXrmr/ZRMCy

Инструменты

Номер сектора

99464

Выгрузить

Ответ

MD5

Отправить

Калькулятор

DEC: 5.6015625

HEX: 0x5.9a

Счеты

0x0B34 / 0x200

Вычислить

Для заметок

21 04 91 30

0B 34

Рисунок 24- Начало данных файла

Так как у нас данные находятся в пределах 4 кластеров, а в каждом кластере 8 секторов, то нужно скачать 32 сектора включая текущий.

Шаг 7 - Вычисление контрольной суммы

Теория. Если у вас несколько файлов, то объединяете их с помощью команды `cat` строго в порядке, в котором они расположены на сайте. После этого выполняете команду `dd`. Команда, в общем виде: *dd if=Название объединённого файла skip=\$((смещение до данных файла)) bs=1 count=\$((размер файла)) | md5sum*.

Практика. Применим вышеописанные команды:

```
root@DESKTOP-E8F9G50:/mnt/c/Users/Oleg/Desktop/Универ/OS# cat 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 > final
root@DESKTOP-E8F9G50:/mnt/c/Users/Oleg/Desktop/Универ/OS# dd if=final bs=1 count=$((0x340b)) | md5sum
13323+0 records in
13323+0 records out
1b36197149bc32dc3085f28188eac3a5 -
13323 bytes (13 kB, 13 KiB) copied, 5.96714 s, 2.2 kB/s
```

Рисунок 25 - Применение команд

Затем копируем полученную контрольную сумму и вставляем её в поле для ответа на сайте и нажимаем кнопку «Отправить». Теперь, если вы всё сделали правильно, то получите подобное сообщение:

Уведомление от сайта fat.bk252.ru

Поздравляю! Ответ верный!

Закреть

Рисунок 26 - Уведомление от сайта

Конец.