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:

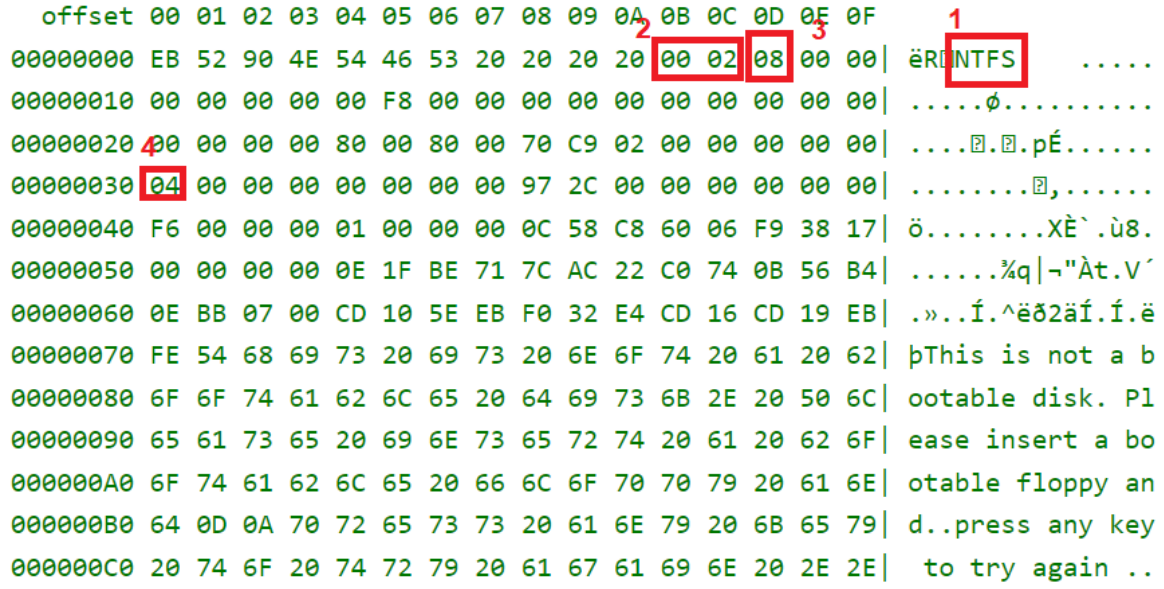


Рисунок 1 - пример загрузочного сектора

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:

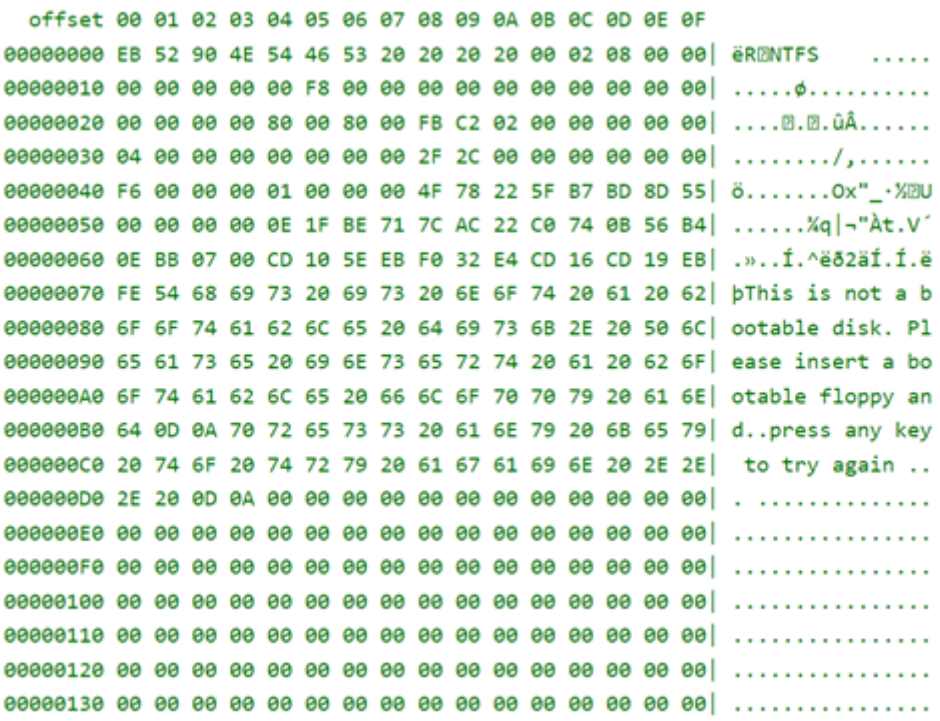


Рисунок 2 - загрузочный сектор

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.

Рисунок 3 - Подсчёт смещения до MFT таблицы

0x4000 - offset таблицы MFT. Теперь посчитаем сектор MFT таблицы: 0x4000/0x200 = 32. Перейдём в полученный сектор:

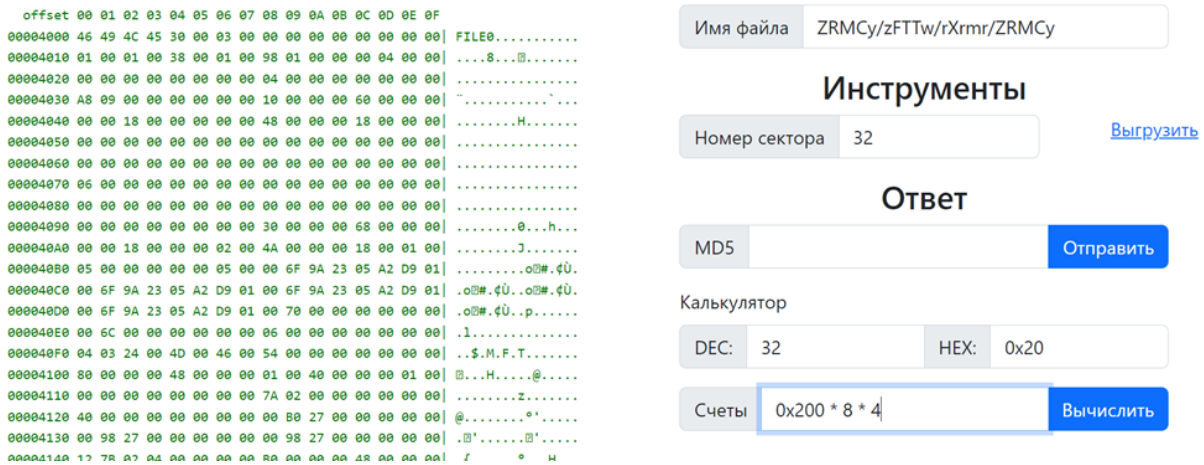


Рисунок 4 - MFT таблица

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.

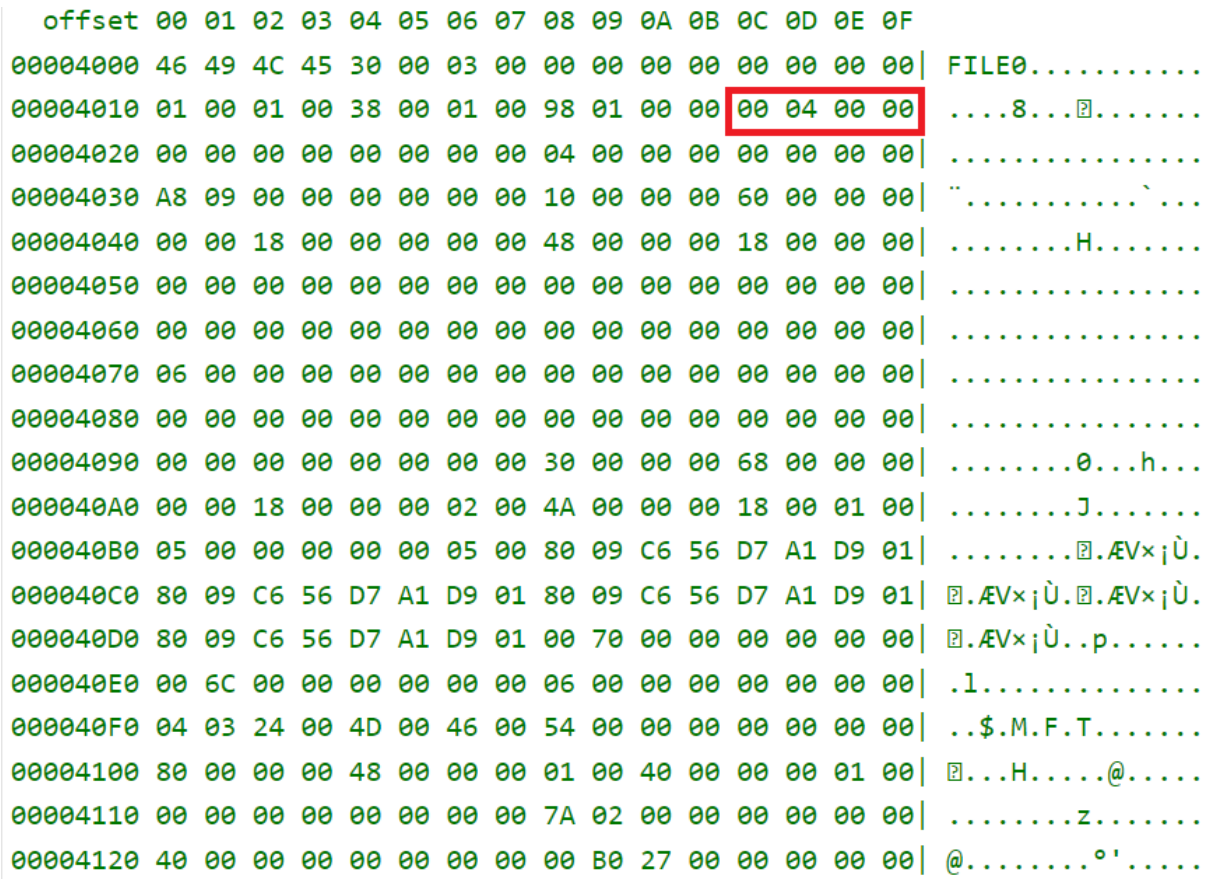


Рисунок 5 - Пример размера записи MFT

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.

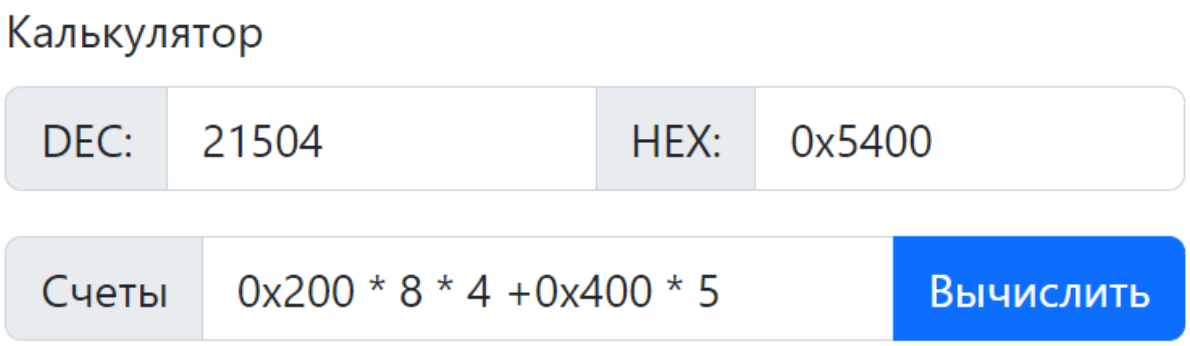


Рисунок 6 - Подсчёт смещения до корневой папки

Теперь посчитаем сектор корневой директории: 0x5400 / 0x200 = 42. Перейдём в этот сектор:

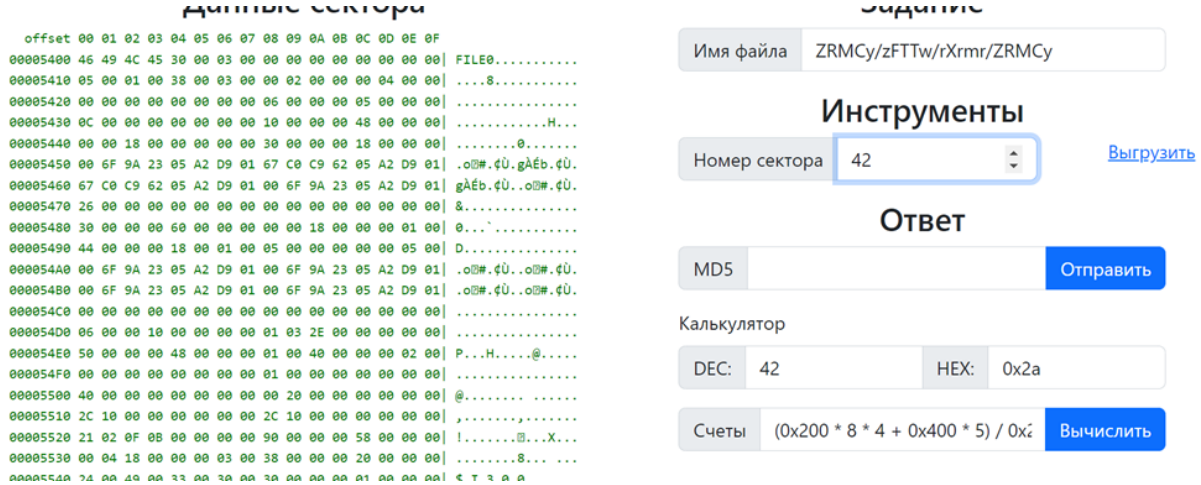


Рисунок 7 - Корневая директория

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:

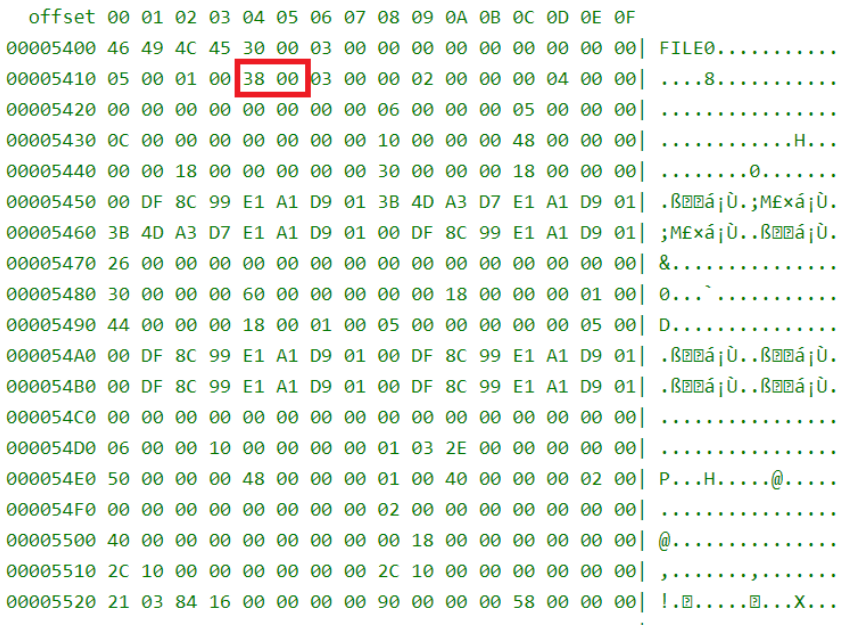
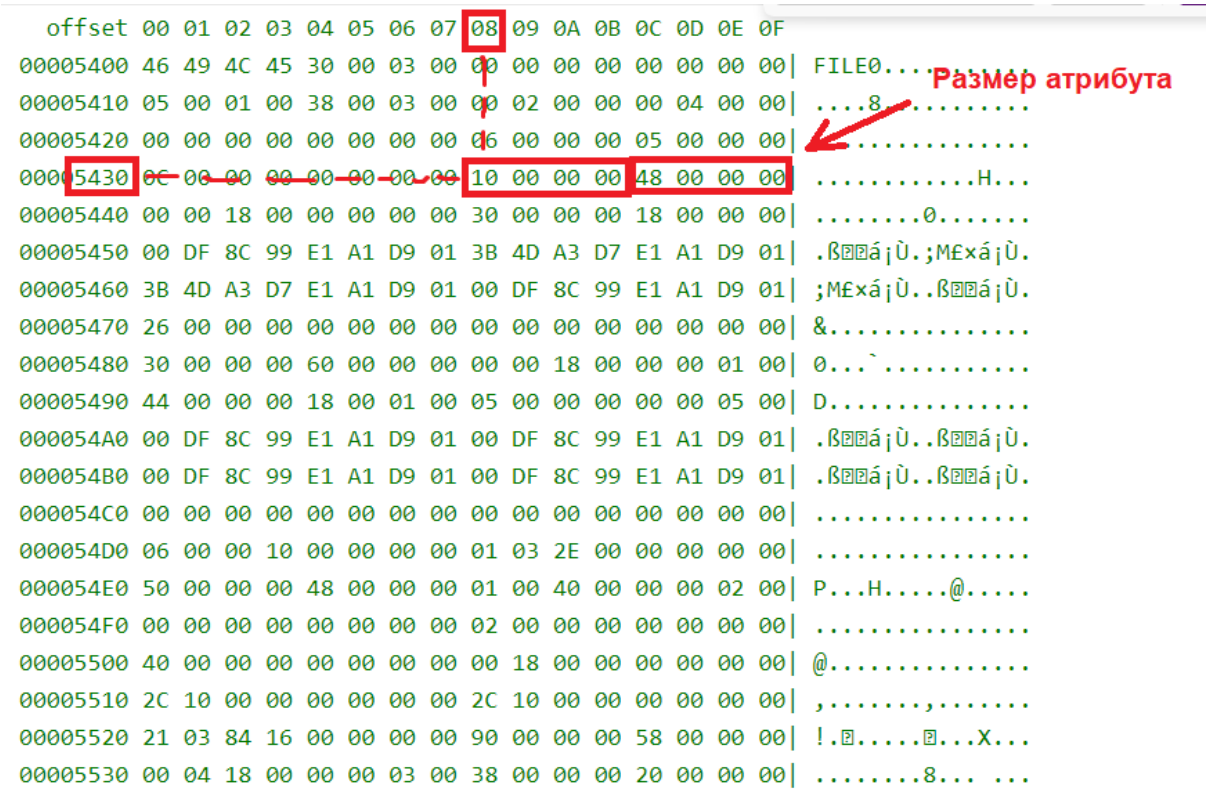


Рисунок 8 - Смещение от текущей папки до таблицы атрибутов

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 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| .ßᙌá¡Ù.;M£×á¡Ù.
00005460 3B 4D A3 D7 E1 A1 D9 01 00 DF 8C 99 E1 A1 D9 01| ;M£×á¡Ù..ßᙌá¡Ù.
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| .ßᙌá¡Ù..ßᙌá¡Ù.
000054B0 00 DF 8C 99 E1 A1 D9 01 00 DF 8C 99 E1 A1 D9 01| .ßᙌá¡Ù..ßᙌá¡Ù.
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 00 18 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| !.ᙌ.....ᙌ...X...
00005530 00 04 18 00 00 00 03 00 38 00 00 00 20 00 00 00| ........8... ...
```

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 «M». 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 + 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.

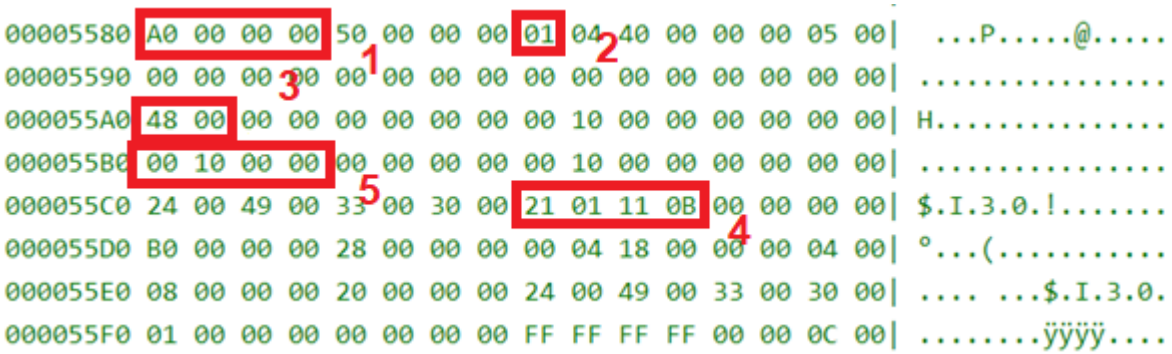


Рисунок 10 - пример атрибута «A0»

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:

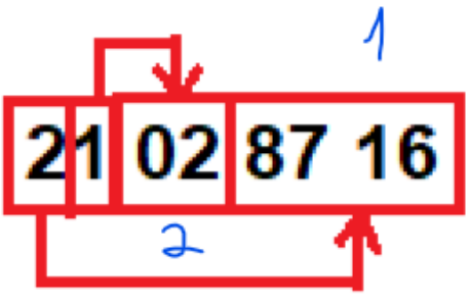


Рисунок 11 - Пример разбиение списка серий

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:

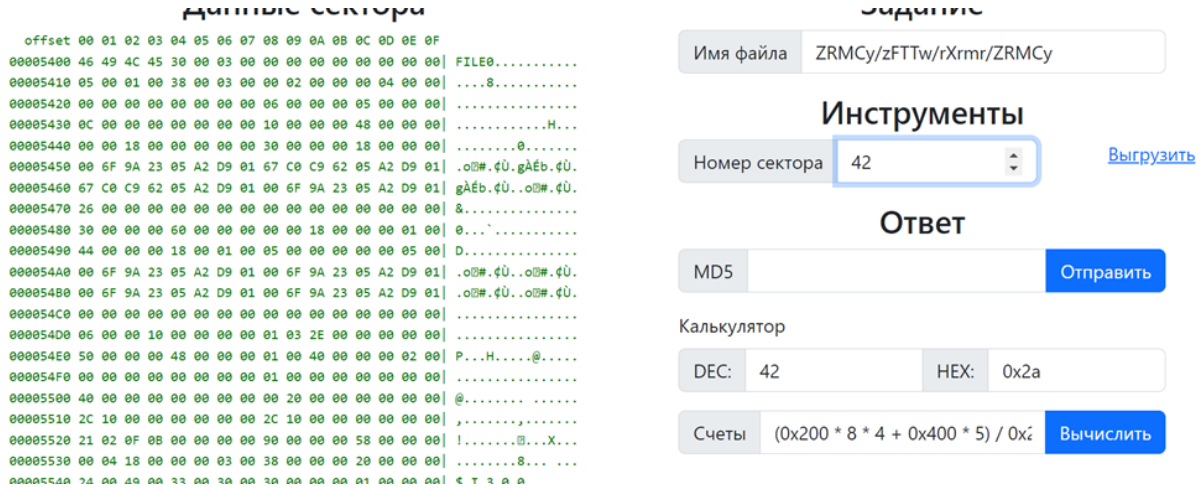


Рисунок 12 - Корневая директория

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 00| ................
000055A0 48 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00| H...............
000055B0 00 10 00 00 00 00 00 00 00 10 00 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:

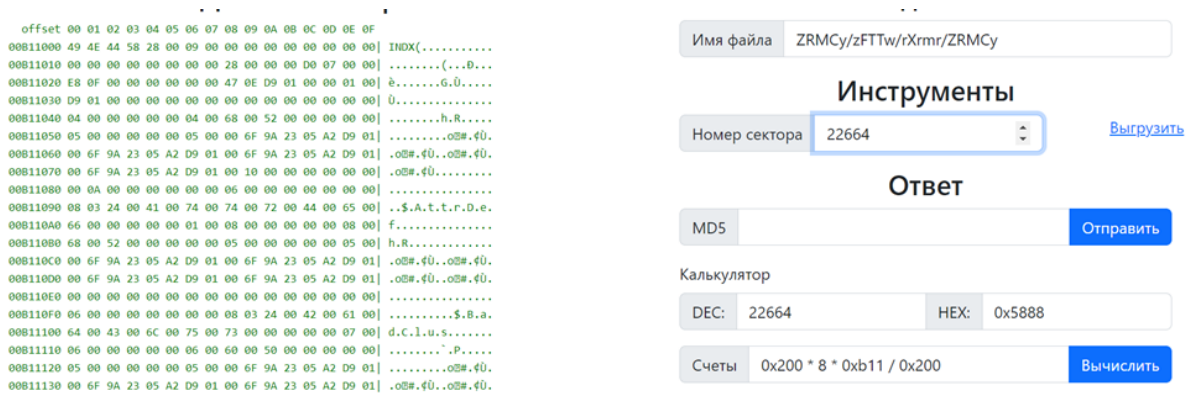


Рисунок 14 - Таблица индексов

Шаг 5 - Переход по таблице индексов в следующую директорию

Теория. Попав 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:

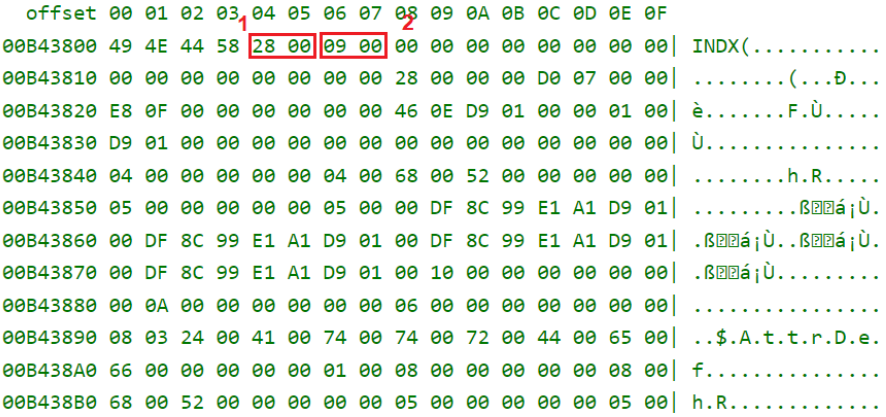


Рисунок 15 - Пример таблицы индексов

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.

Таким образом, мы получили смещение до начала данных таблицы индексов.

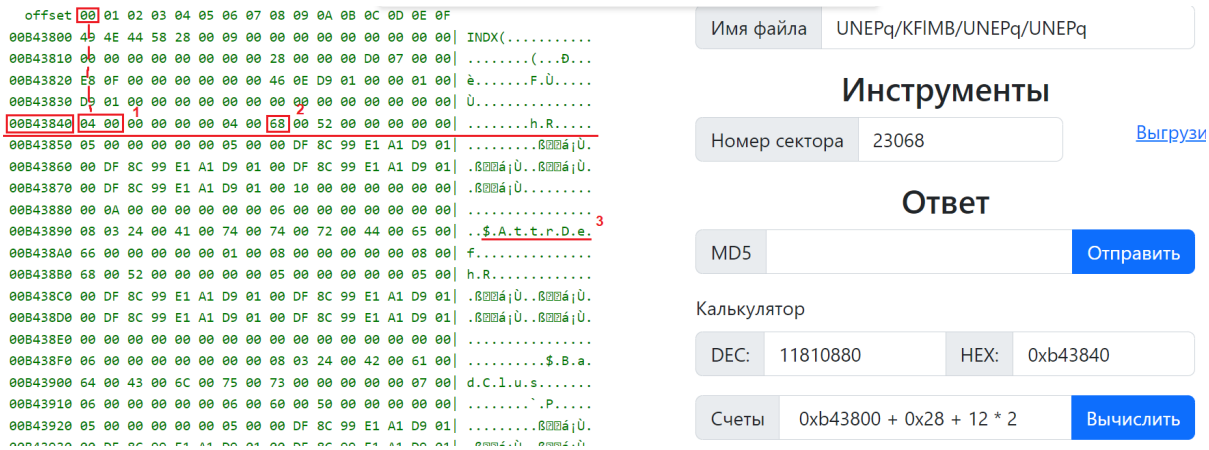


Рисунок 16 - Пример таблицы индексов

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.

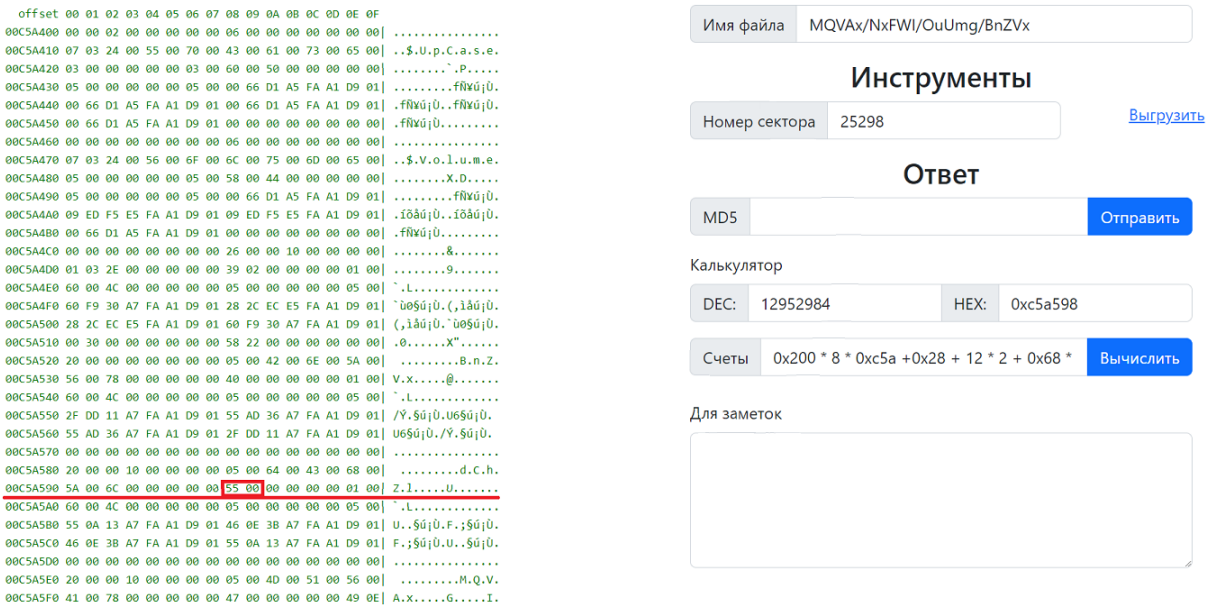


Рисунок 17 - Первые два байта записи файла/директории

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:

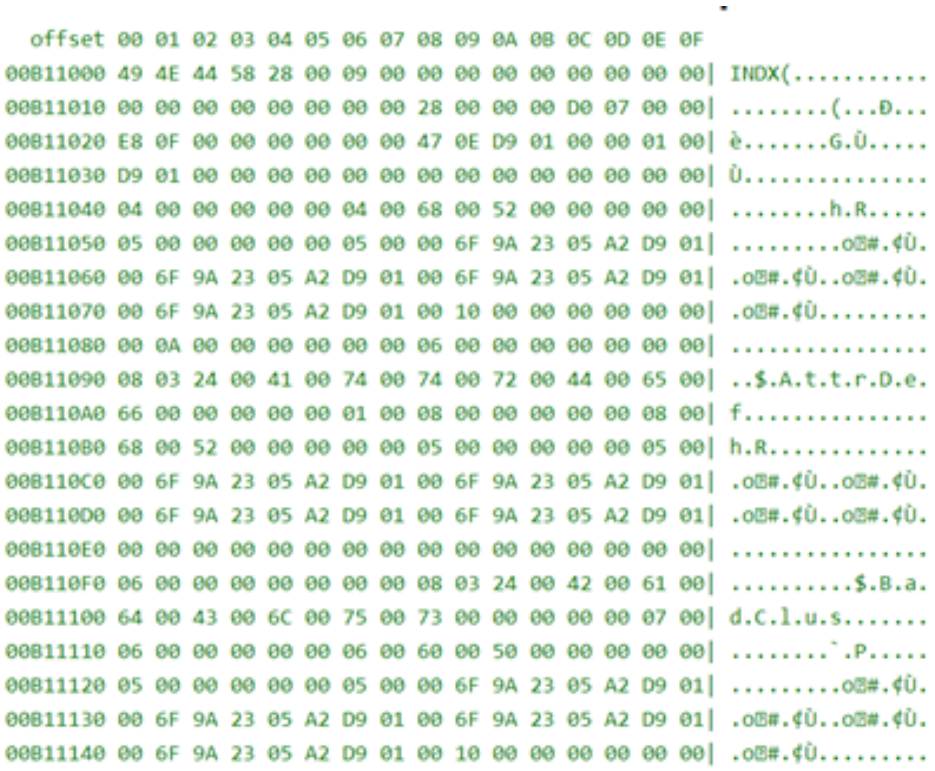


Рисунок 18 - Таблица индексов

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:

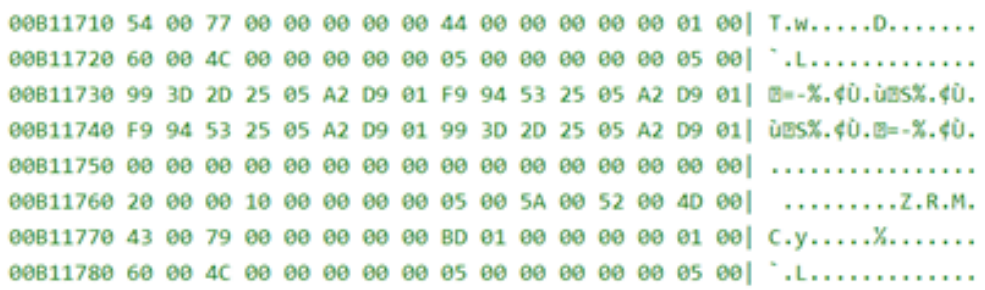


Рисунок 19 - Необходимый атрибут

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| ?=-%.¢Ù.ù?S%.¢Ù.
00015060 F9 94 53 25 05 A2 D9 01 99 3D 2D 25 05 A2 D9 01| ù?S%.¢Ù.?=-%.¢Ù.
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| ?=-%.¢Ù.?=-%.¢Ù.
000150B0 99 3D 2D 25 05 A2 D9 01 99 3D 2D 25 05 A2 D9 01| ?=-%.¢Ù.?=-%.¢Ù.
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| ...?....$.......
00015110 34 00 00 00 01 02 00 00 00 00 00 05 20 00 00 00| 4.......... ...
00015120 20 02 00 00 01 02 00 00 00 00 00 05 20 00 00 00|  .......... ...
00015130 20 02 00 00 02 00 1C 00 01 00 00 00 00 03 14 00|  ...............
00015140 FF 01 1F 00 01 01 00 00 00 00 00 01 00 00 00 00| ÿ...............
00015150 90 00 00 00 58 00 00 00 00 04 18 00 00 00 02 00| ?...X...........
00015160 38 00 00 00 20 00 00 00 24 00 49 00 33 00 30 00| 8... ...$.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.

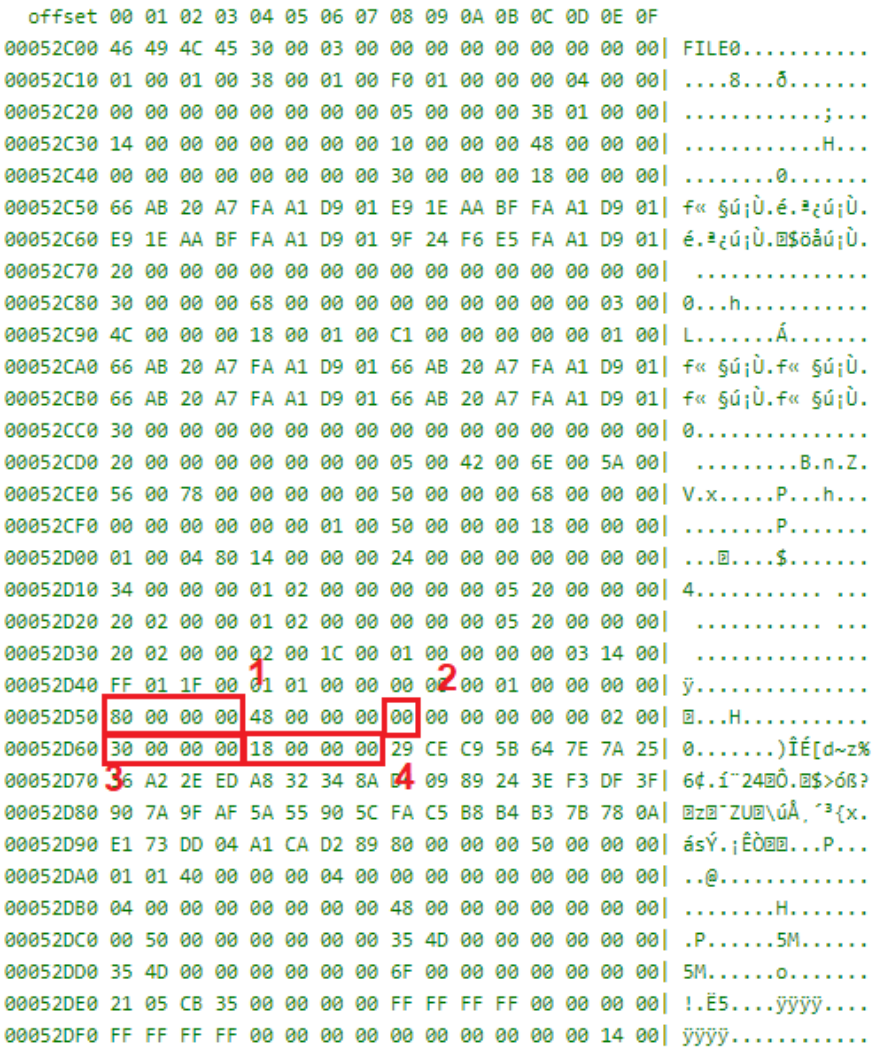


Рисунок 21 - Области выделения для резидентного атрибута

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:

Рисунок 22 - Запись искомого файла

Далее ищем в нём атрибут 80. Взглянем на него:

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

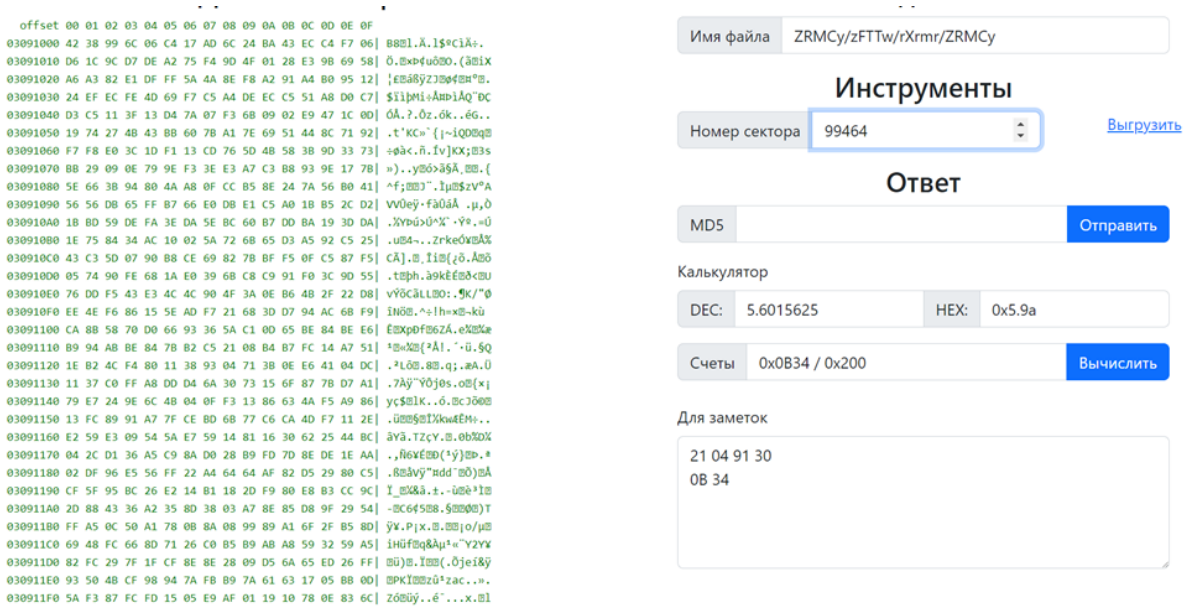


Рисунок 24- Начало данных файла

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-E8F9G5O:/mnt/c/Users/Oleg/Desktop/Универь/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-E8F9G5O:/mnt/c/Users/Oleg/Desktop/Универь/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:

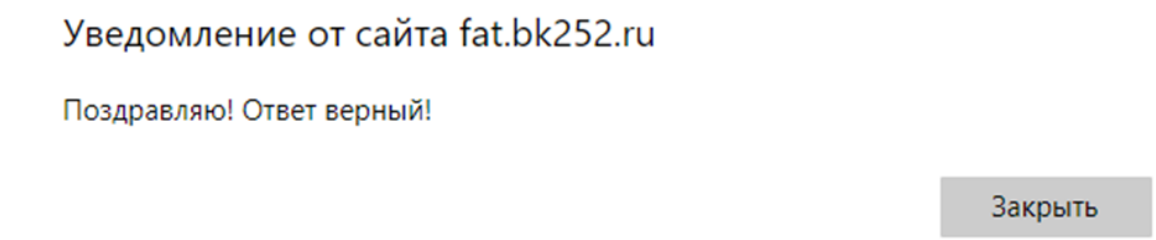


Рисунок 26 - Уведомление от сайта

Конец.