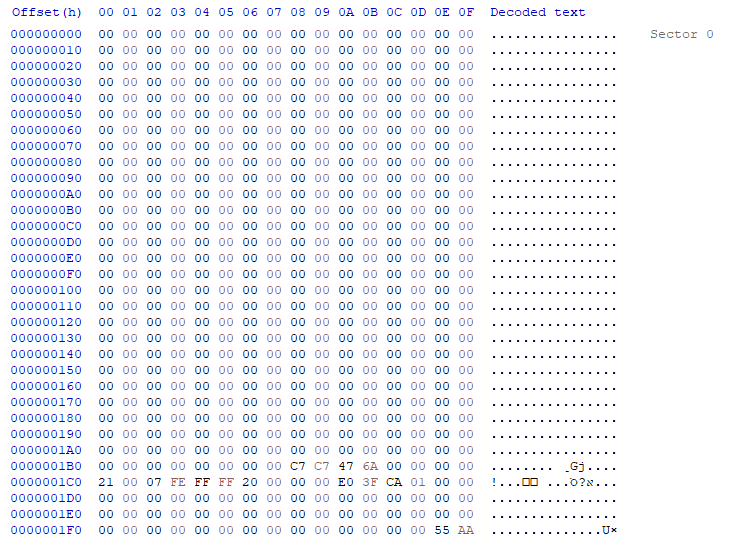
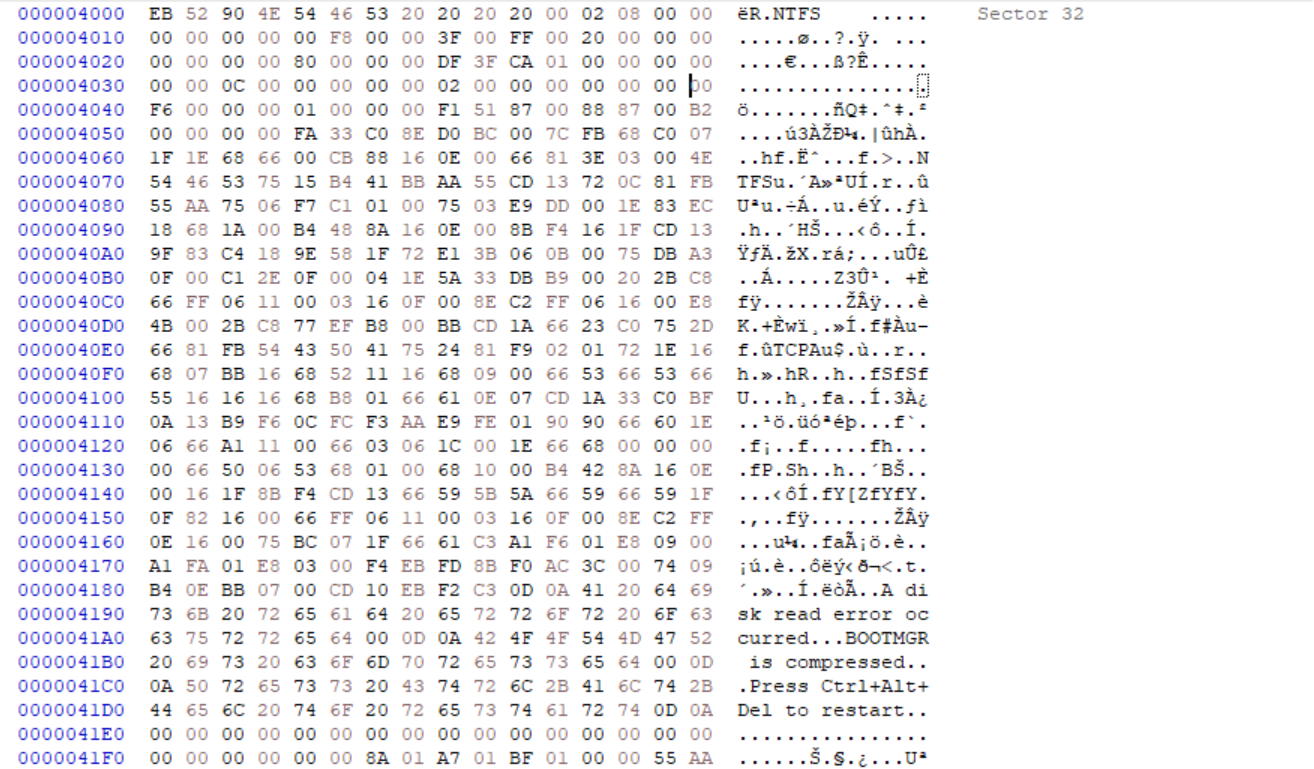
**עבודת הגשה בנושא מערכות קבצים-NFTS**

PBR

מתוך ה-MBR נגיע לסקטור הראשוני ממנו מתחיל ה-PBR



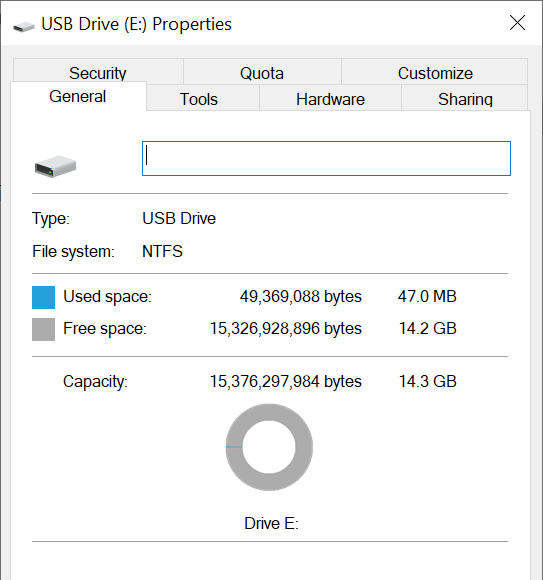
אנחנו רואים כי הסקטור הראשוני הוא 21 בהקסדצימלי. כאשר נמיר 21 לדצימלי, נגיע ל-33 ונראה כי ה-PBR הוא בסקטור 32 בשורה 4000 בהקס'



ה-PBR מסתיים בשורה 0F41 בהקס' לפי הסיומת של AA 55

ניתן למצוא את כמות הבתים לסקטור- 200 בהקסדצימלי, כלומר 512 בתים

ניתן למצוא את כמות הסקטורים בכל קלסטר- 8 בהקסדצימלי. כלומר 8 סקטורים בכל קלסטר.

כמות הסקטורים הכללית היא 1CA3FDF בהקס' נמיר לדצימלי ונקבל 30,031,839, נוסיף 32 לכמות הסקטורים שלפני ה-PBR ונקבל ערך של 30,031,871

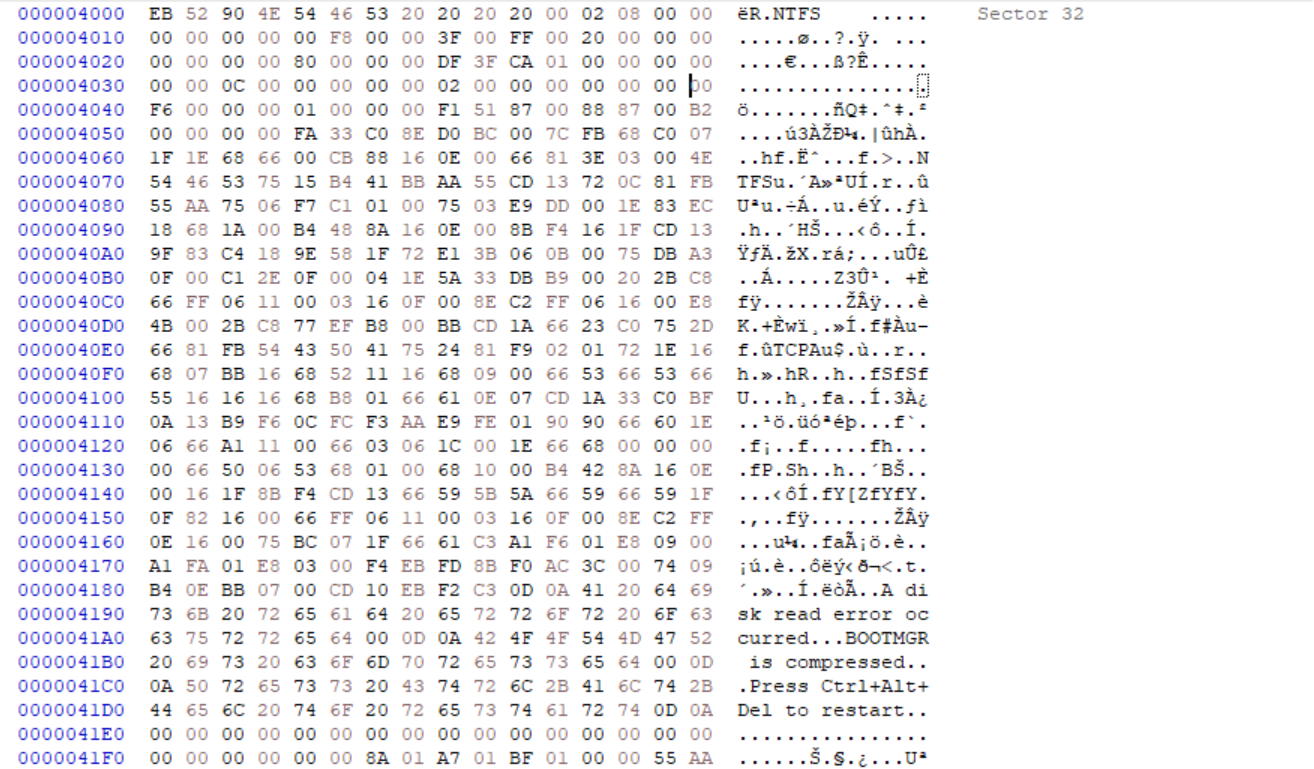
הגודל של הזיכרון הוא כמות הסקטורים כפול 512. נכפיל ונגיע ל-14.32 ג'יגה בייט שזה הגודל של הדיסק און קי.

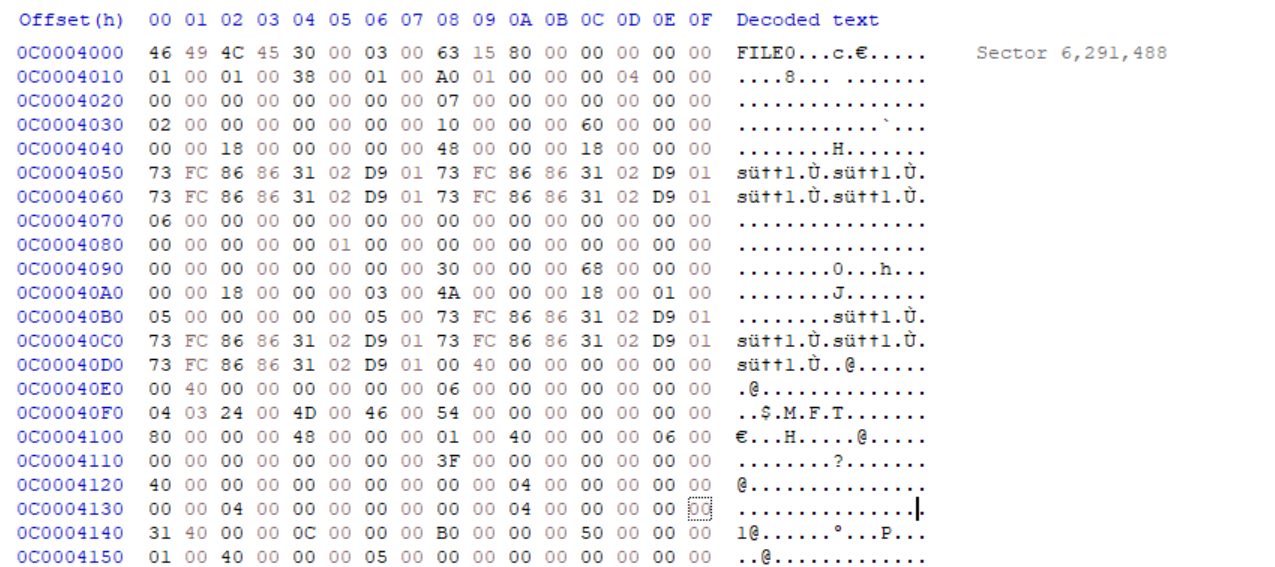
הגודל של ה-PBR עצמו הוא גודל של סקטור אחד כפול 512 בייטים. כלומר, 512 בייטים שהם חצי קילובייט.

ניתן למצוא את הקלסטר הראשון של ה-MFT- 0000C.

BITMAP

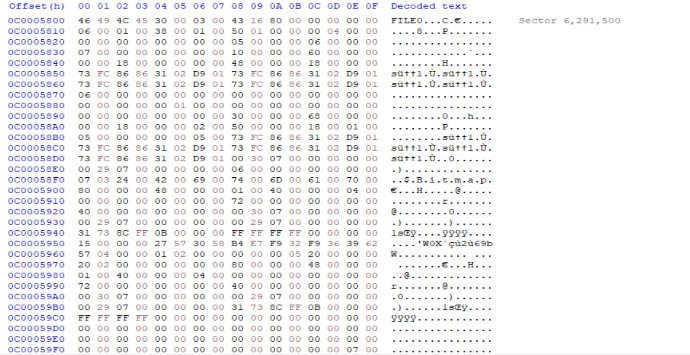
נמצא את הקלסטר של טבלת ה-MFT ונמצא את הentry השישי. כלומר, הקלסטר הוא קלסטר מספר 0000C ונצטרך להכפיל בכמות הסקטורים לכל קלסטר (כלומר, 8). נמיר את המספר לדצימלי ונוסיף 32 כי זה הסקטור ממנו אנחנו מתחילים (הסקטור של ה-PBR). נגיע לסקטור מספר 6,291,488



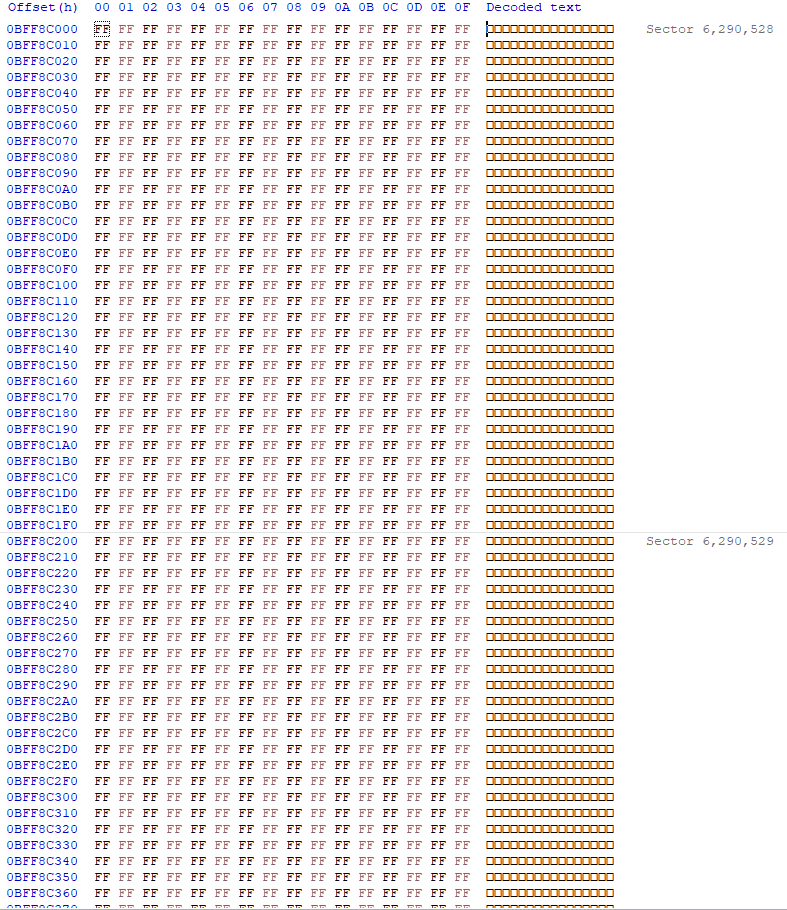
ונגיע ל-MFT

על מנת להגיע ל-BITMAP נמצא את הENTRY השישי ב-MFT:

ניתן לראות כי ה-BITMAP מאוזכר ב-ENTRY השישי של ה-MFT. על מנת להגיע ל-BITMAP נחפש את הסקטור הראשון שלו. הקלסטר הראשון שלו הוא 0BFF8C כלומר, 786316. כדי להגיע לסקטור, נכפיל ב-8 ונקבל סקטור של 6290528. כמות הקלסטרים הכוללת היא 73 בהקס' כלומר 115 קלסטרים. נכפיל ב-8 ונקבל 920 סקטורים. הsize הוא כמות הבתים בסקטור כפול מספר הסקטורים, כלומר, 920\*512 = 471040 בתים.

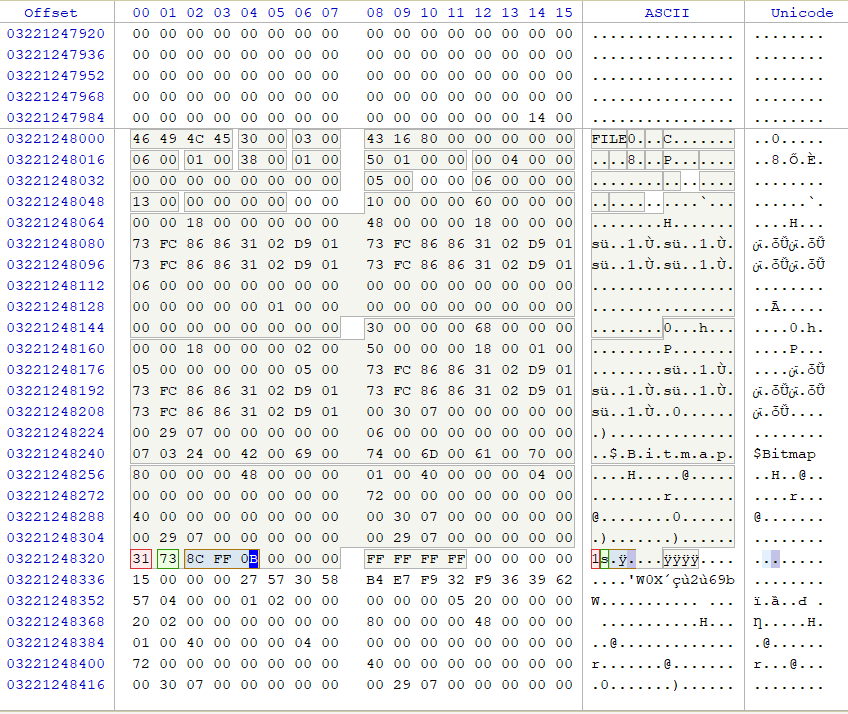


כעת נוכל למצוא את ה end address: מתחיל בקלסטר 786316 וגודלו 115 קלסטרים ולכן הend address הוא קלסטר 786431 כלומר סקטור 6291448 או 5hFFFF8

 הנה ה BITMAP:

עכשיו נראה היכן נמצא על קובץ/תיקייה:

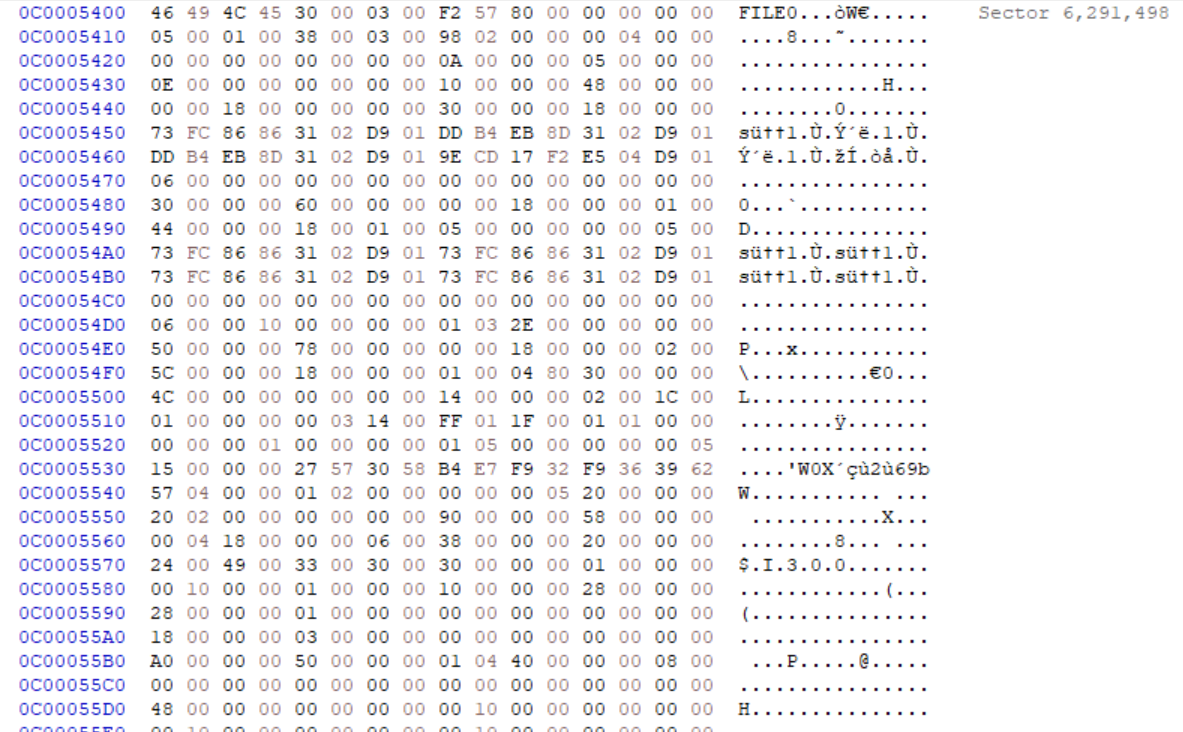
File1: sector 6291572 -> cluster 786446 -> (/bytes per cluster) = 1536 bitmap offset.



size

First cluster

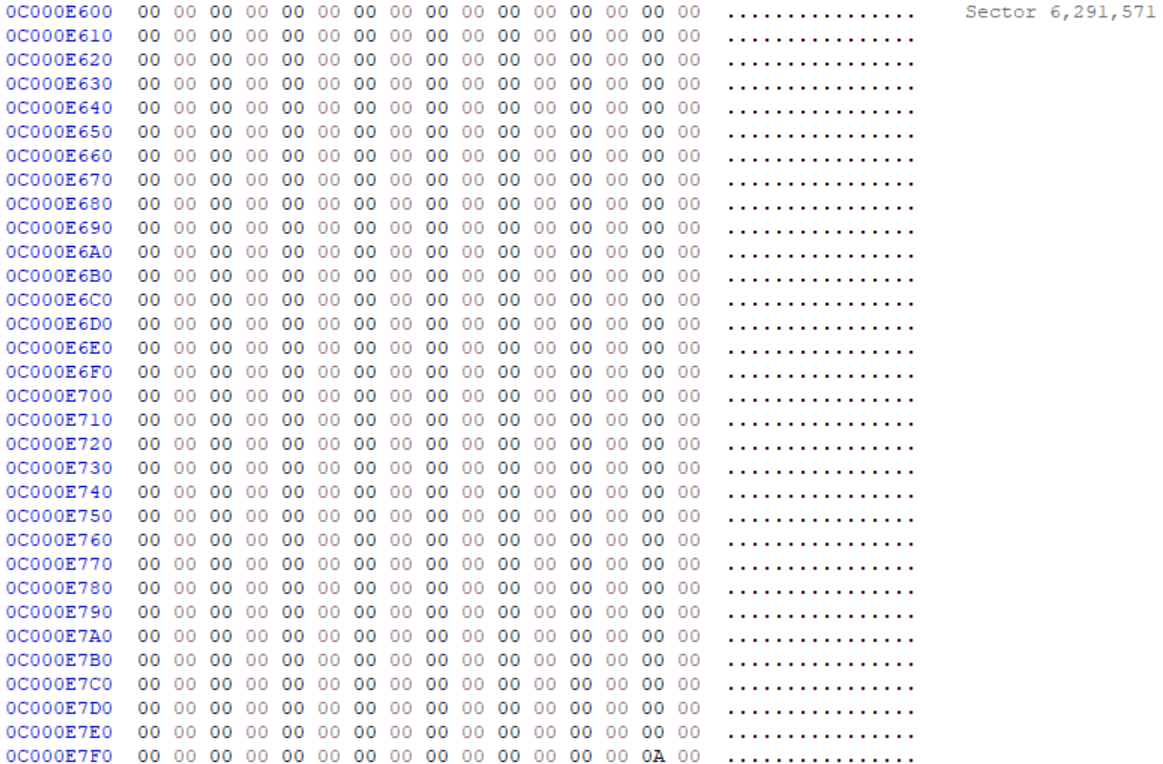
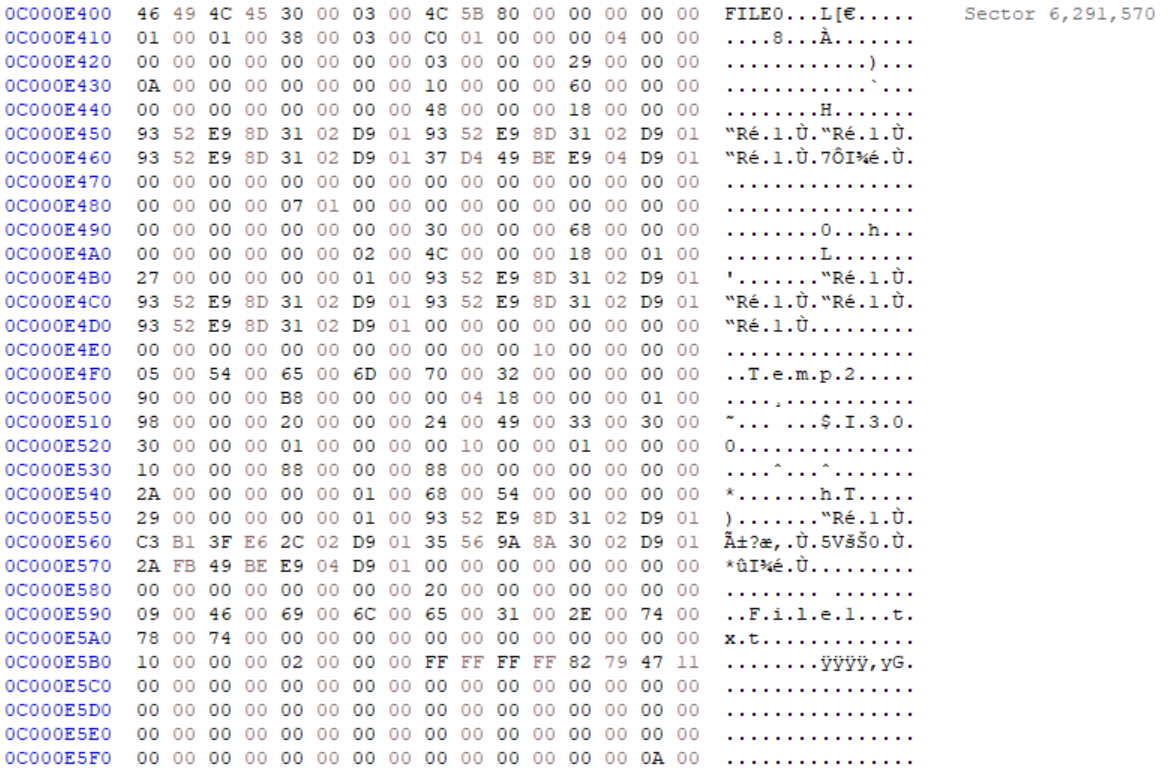
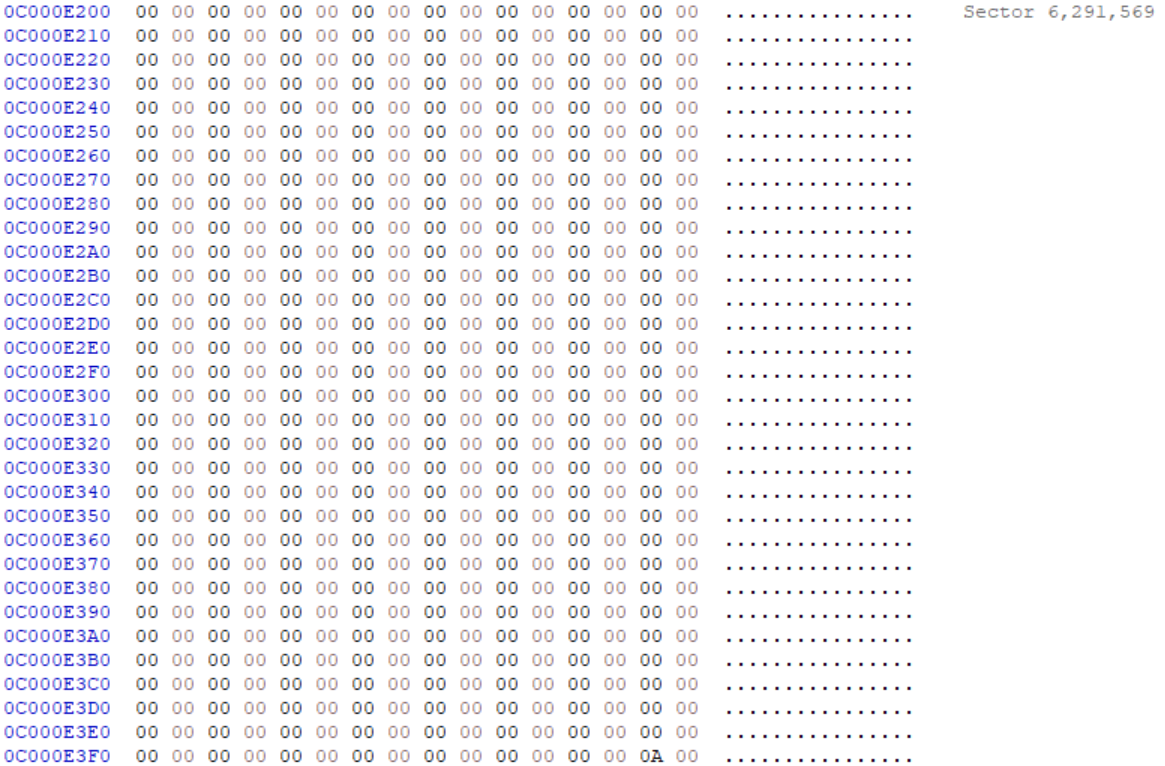
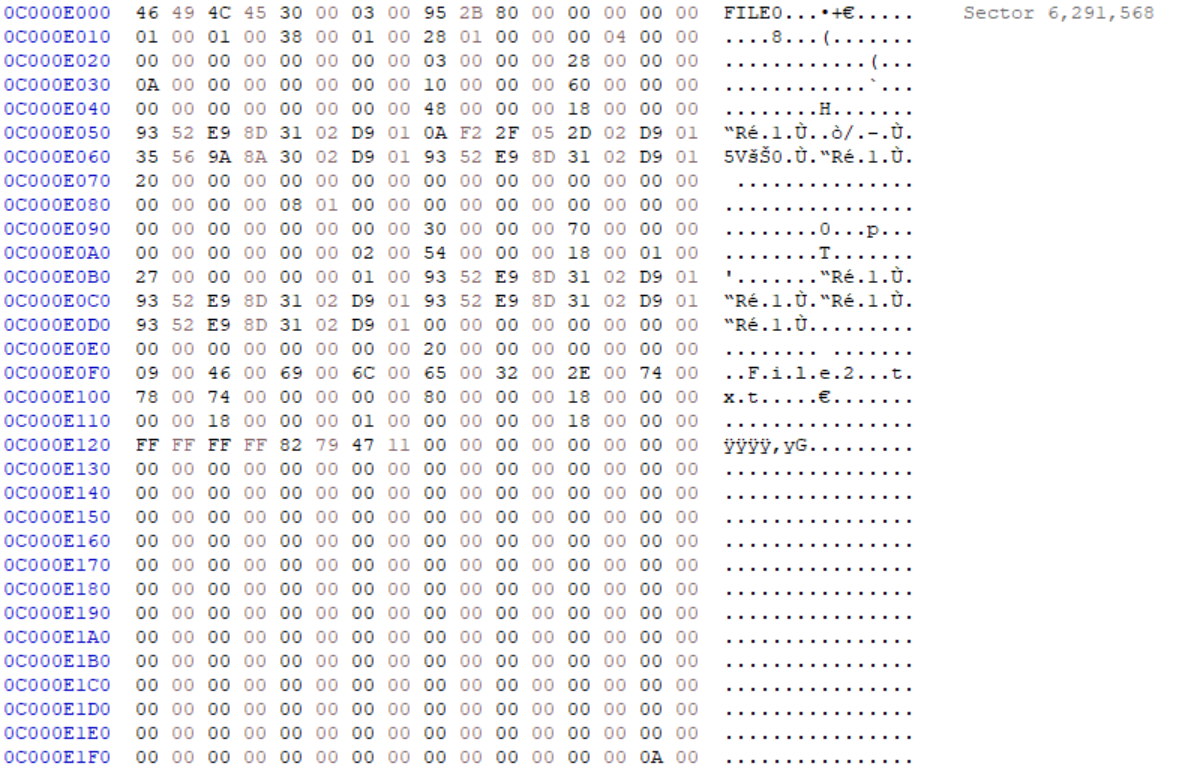
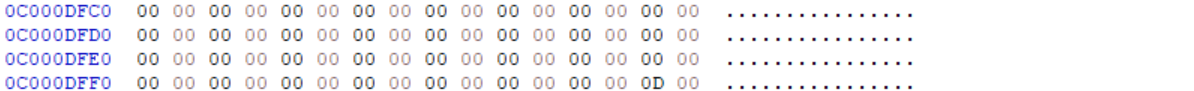
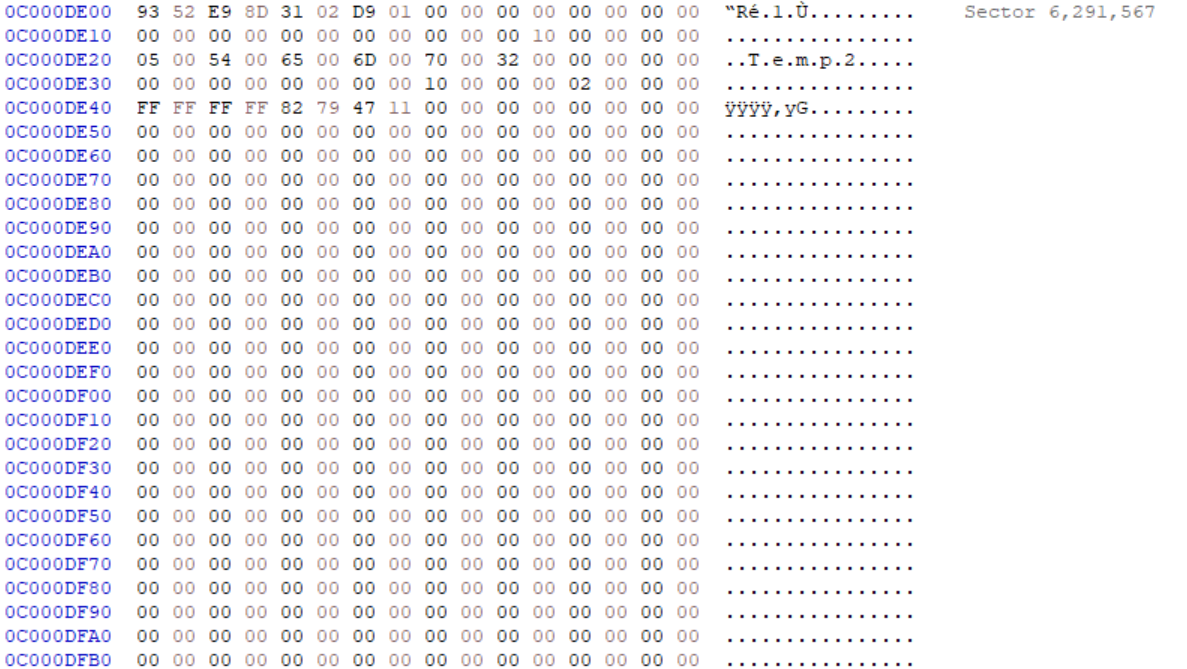
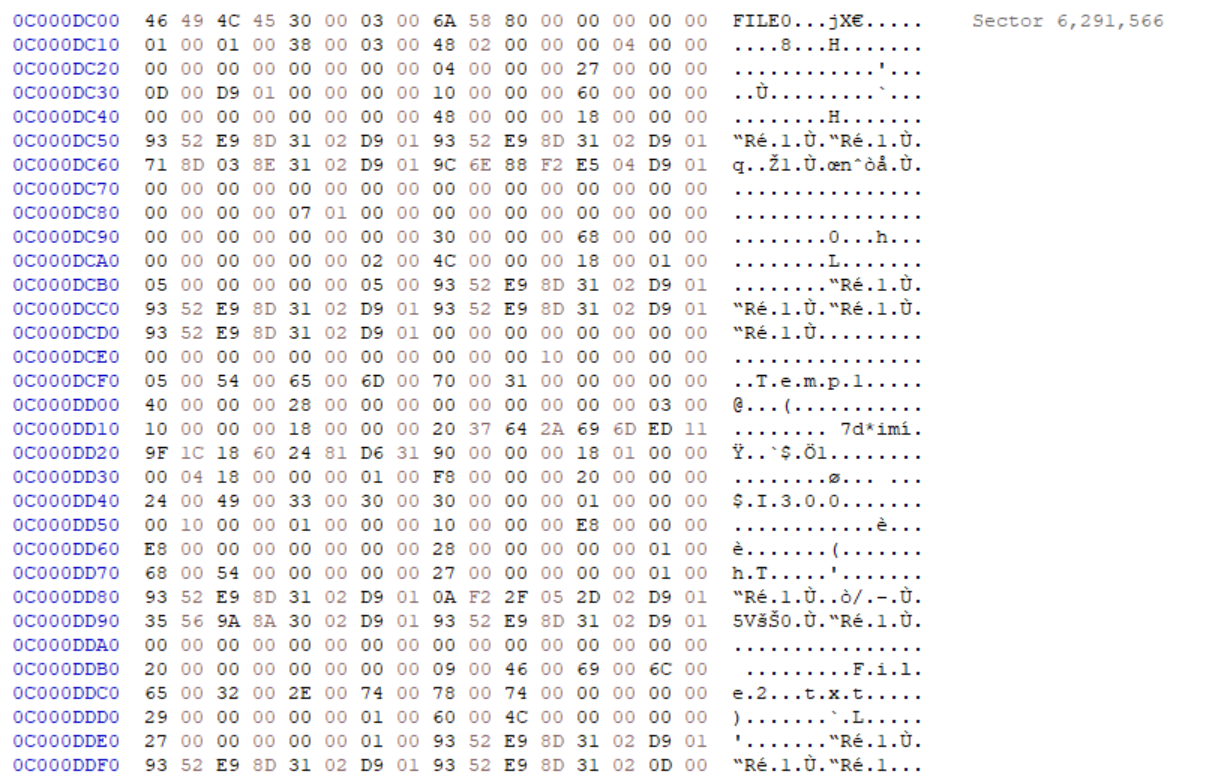
ROOT DIRECTORY

ה-ROOT DIRECTORY נמצא ב-ENTRY החמישי ב-MFT:

ניתן לראות שהוא מתחיל בכתובת C0005400 בהקסדצימלי ומסתיים לאחר 2 סקטורים בכתובת C00057F0. גודלו הוא שני סקטורים. כלומר, קילובייט אחד.

FILES AND FOLDERS

Start address of temp1



Start address of temp2

Start address of file2

נסתכל על כל קובץ או תיקייה בנפרד:

Temp1

ניתן לראות שבתיקייה temp1 יש את temp2 ואת file2.txt

* start address: 0x0C000DC00
* end address: 0x0C000DE40
* size: 0x0C000DE40 - 0x0C000DC00 = 3221282368d -3221281792d = 576 bytes
* list of indexed clusters:

- file2.txt: sectors 6291568- 6291569

- temp2: sector 6291570

attributes:

- $10: **type** -$STANDARD\_INFRMATION, **offset**-056 **resident**? – yes, **content**- File creation time, File modification time, Record changed time, Last Access time, File Permissions, Maximum number of versions, Version number, Class ID, Owner ID, Security ID, Quota Charged, Updated Sequence Number.

- $30: **type**- $FILE\_NAME, **offset**-152, **resident**? – yes, **content**- Parent directory file record number, Parent directory sequence number, File Creation time, File modification time, Record changed time, Last access time, Allocated size, Real size, File attributes, File name length, File name namespace, File name.

- $40: **type**- $OBJECT\_ID, **offset-256, resident?** – yes, **content-** object id

- $90: **type**- $INDEX\_ROOT, **offset**-296**, resident?** – yes, **content-** index root

File2.txt

Table

Description automatically generated

start address: 0x0C000E000

end address: 0x0C000E120

size: 0x0C000E120 - 0x0C000E000 = 3221283104d – 3221282816d = 288 bytes

attributes:

- $10: **type** -$STANDARD\_INFRMATION, **offset**-056, **resident**? – yes, **content**- File creation time, File modification time, Record changed time, Last Access time, File Permissions, Maximum number of versions, Version number, Class ID, Owner ID, Security ID, Quota Charged, Updated Sequence Number.

- $30: **type**- $FILE\_NAME, **offset**-152, **resident**? – yes, **content**- Parent directory file record number, Parent directory sequence number, File Creation time, File modification time, Record changed time, Last access time, Allocated size, Real size, File attributes, File name length, File name namespace, File name.

- $80: **type**- $DATA, **offset-264, resident?** – yes, **content-** Actual data of file (empty)

Table

Description automatically generated with low confidenceTemp2:

start address: 0x0C000E400

end address: 0x0C000E420

size: 0x0C000E420- 0x0C000E400= 3221283872d– 3221283840d= 32 bytes

list of indexed clusters:

* file1.txt: sector 6291572

attributes:

- $10: **type** -$STANDARD\_INFRMATION, **offset**-056, **resident**? – yes, **content**- File creation time, File modification time, Record changed time, Last Access time, File Permissions, Maximum number of versions, Version number, Class ID, Owner ID, Security ID, Quota Charged, Updated Sequence Number.

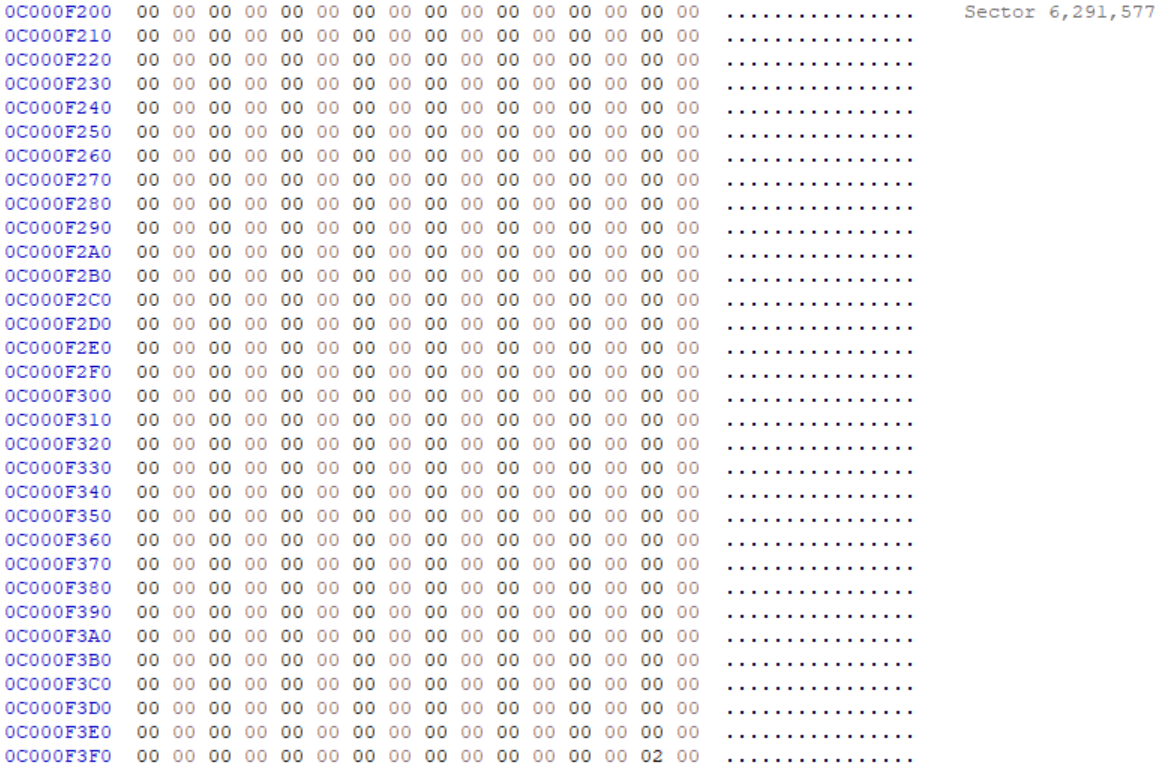
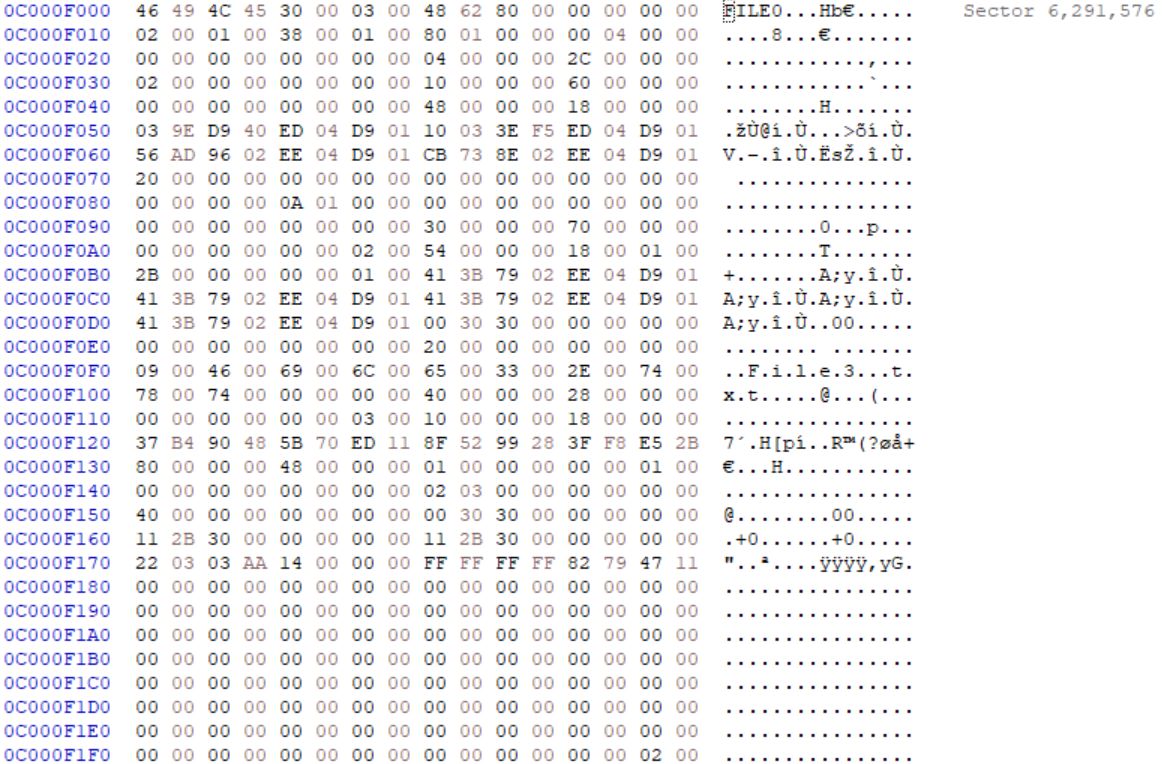
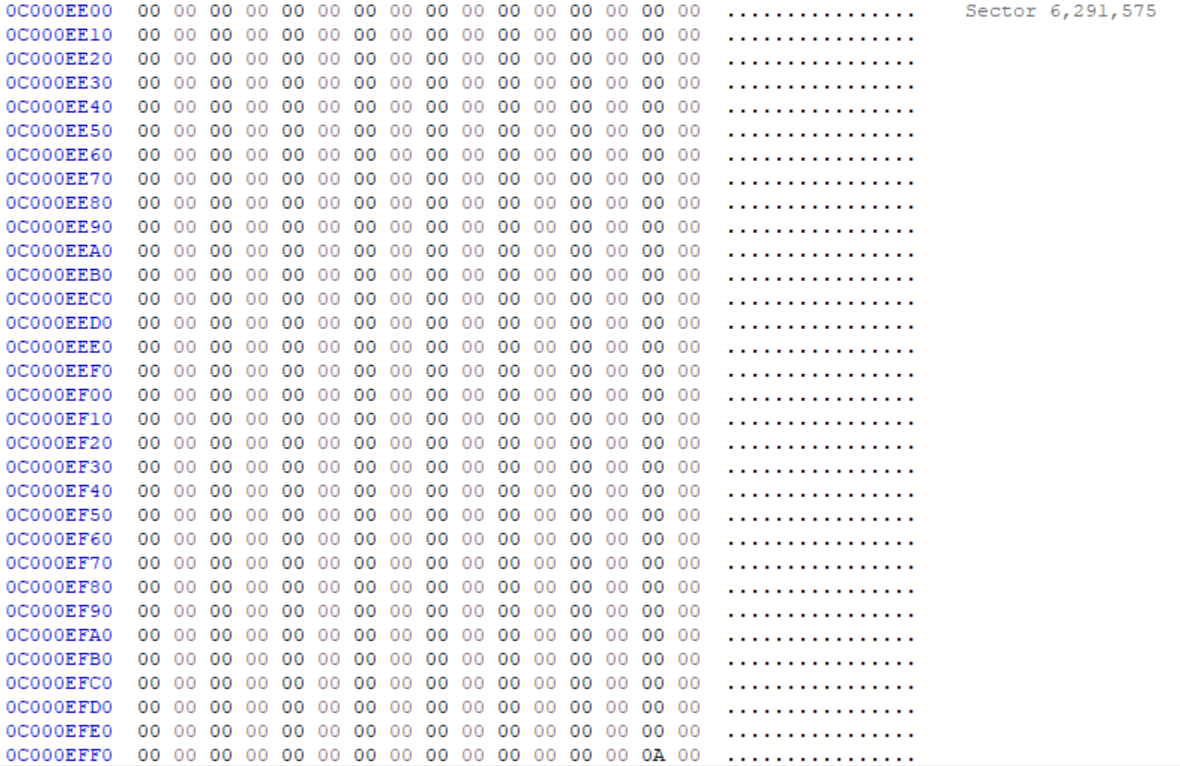
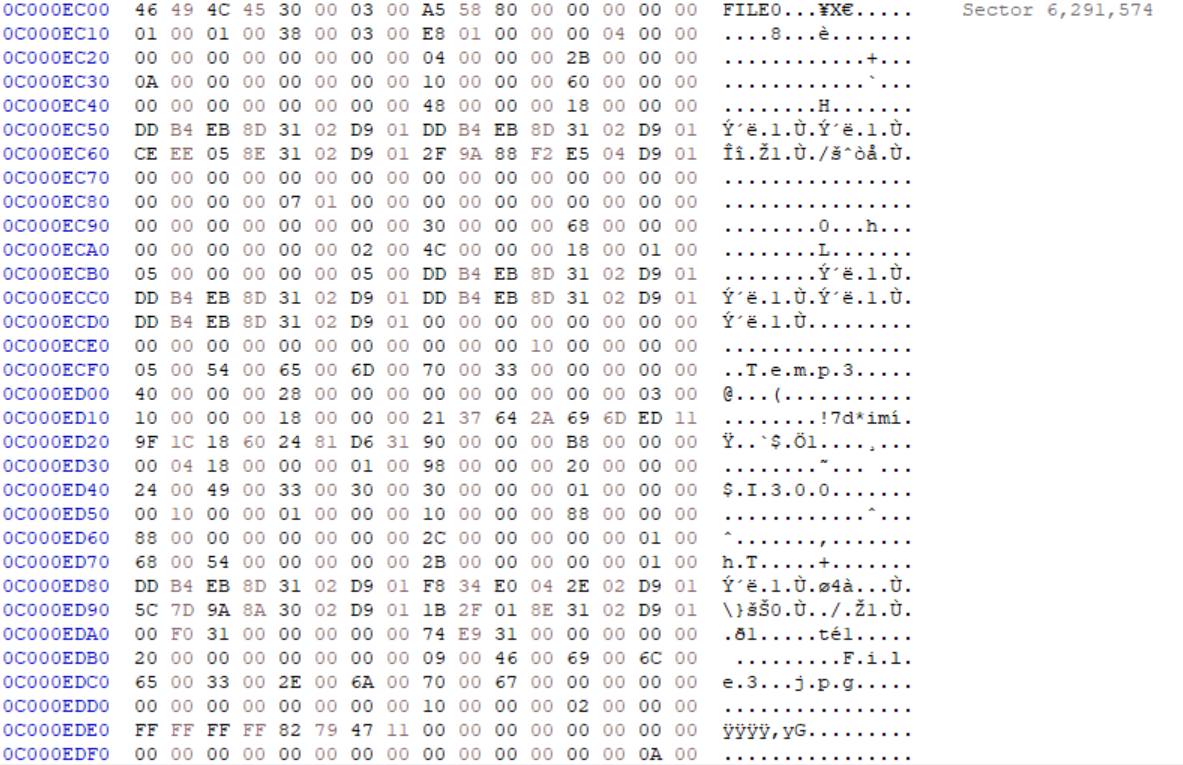
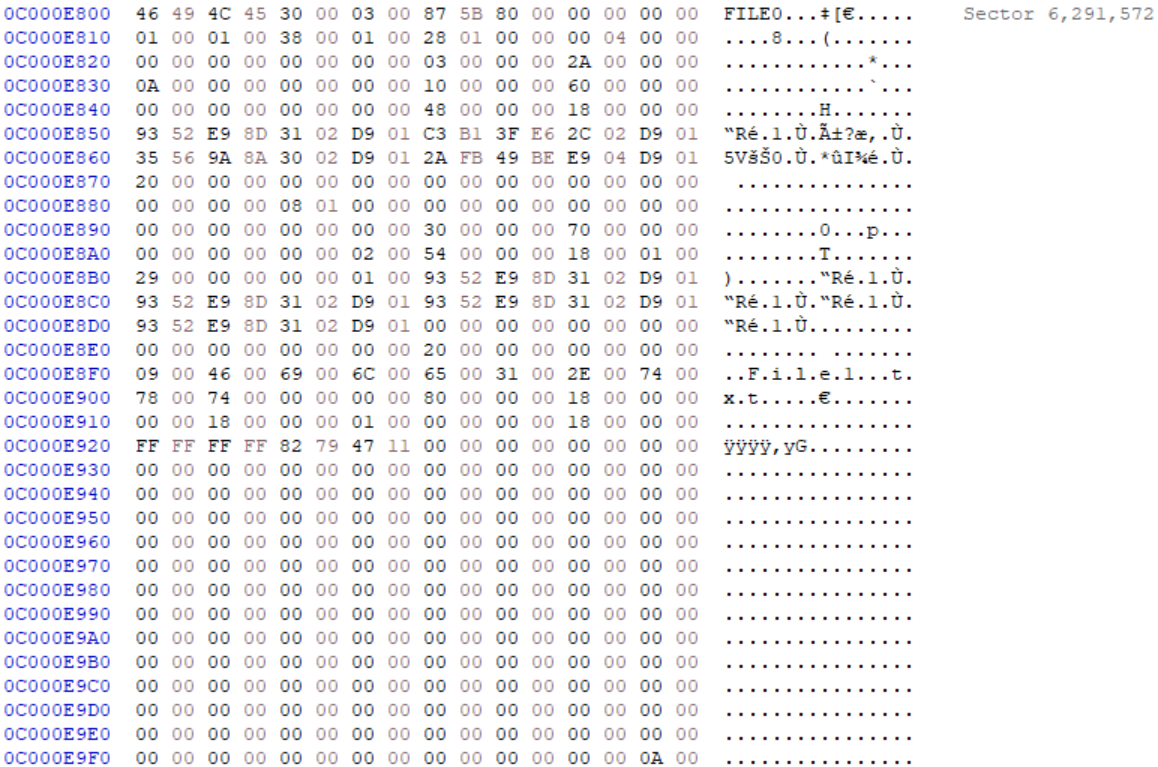
- $30: **type**- $FILE\_NAME, **offset**-152, **resident**? – yes, **content**- Parent directory file record number, Parent directory sequence number, File Creation time, File modification time, Record changed time, Last access time, Allocated size, Real size, File attributes, File name length, File name namespace, File name.

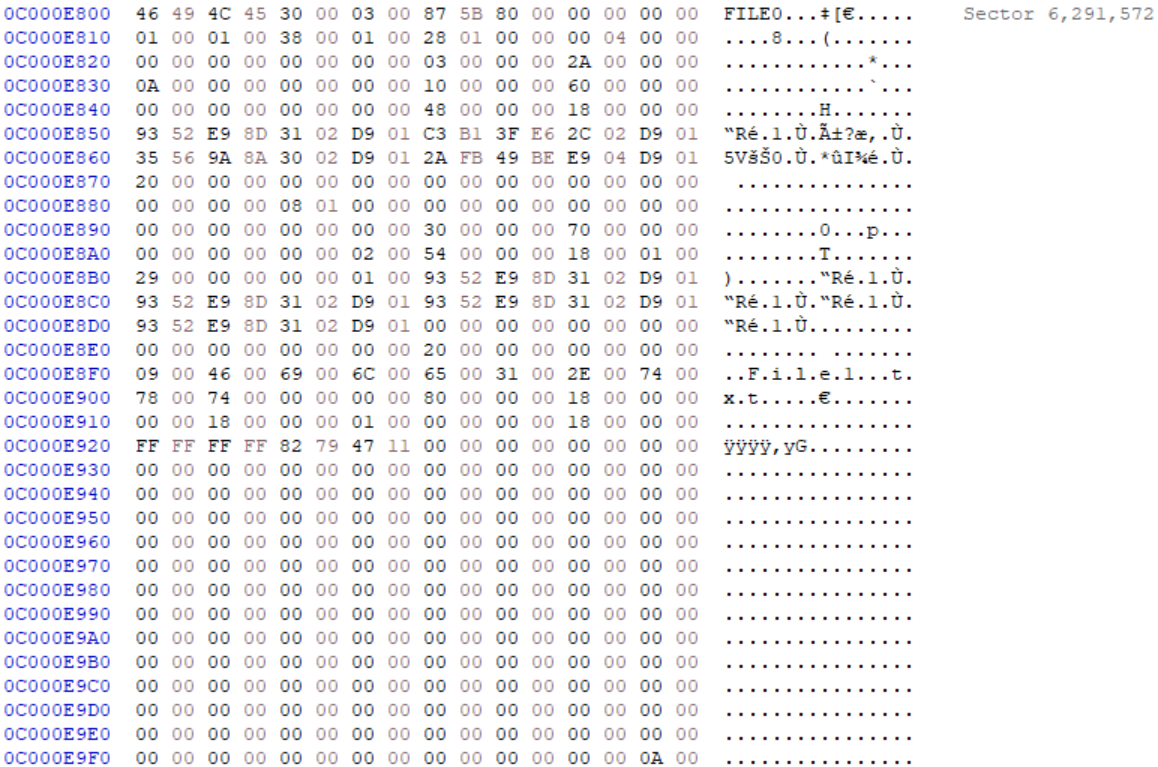
- $90: **type**- $INDEX\_ROOT, **offset**-256**, resident?** – yes, **content-** index root, index heade

Starting address of temp3

Start address of file3

Start address of file1



File1.txt:

start address: 0x0C000E800

end address: 0x0C000E920

size: 0x0C000E920- 0x0C000E800= 3221285152d – 3221284864d= 288 bytes

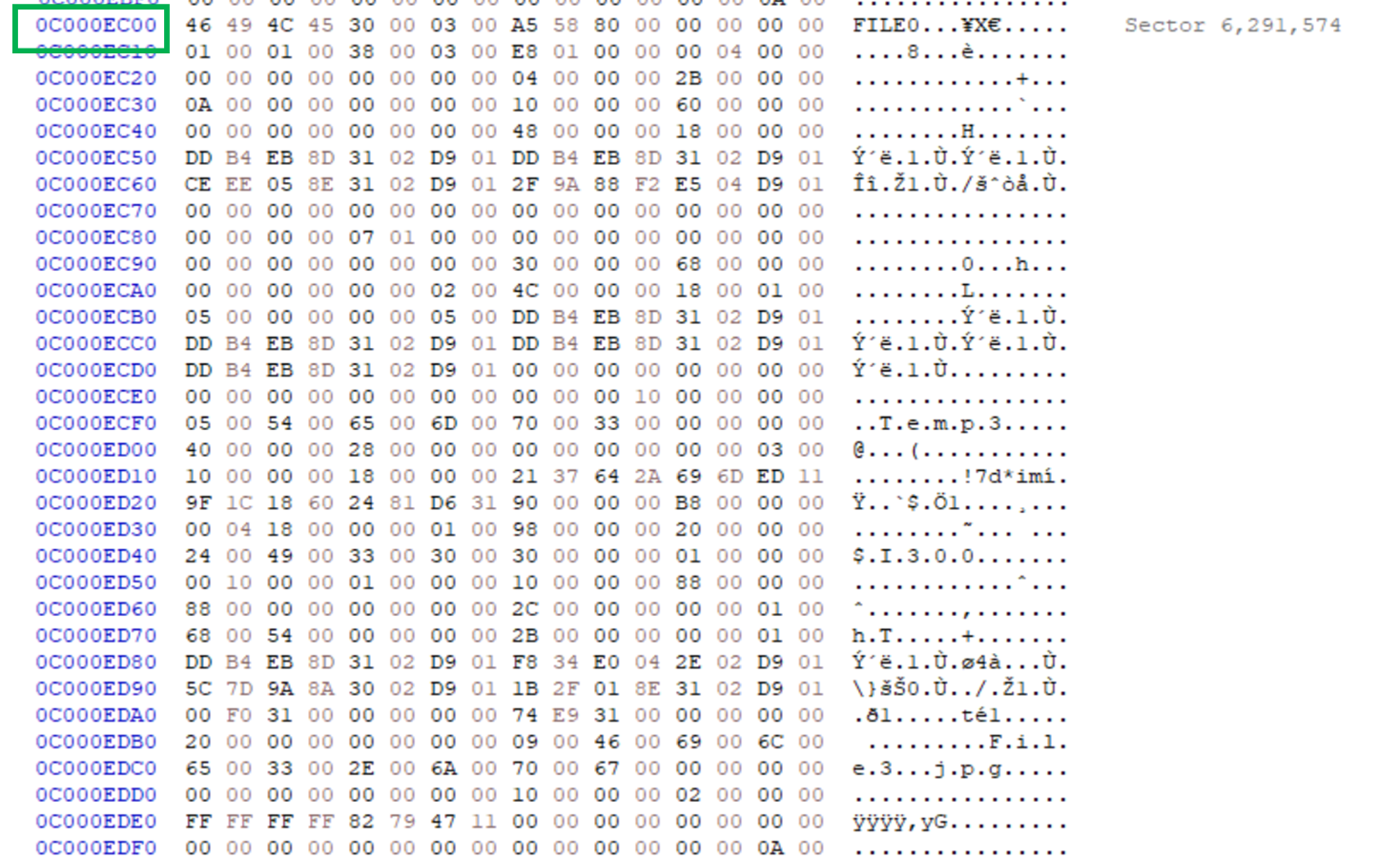
attributes:

- $10: **type** -$STANDARD\_INFRMATION, **offset**-056, **resident**? – yes, **content**- File creation time, File modification time, Record changed time, Last Access time, File Permissions, Maximum number of versions, Version number, Class ID, Owner ID, Security ID, Quota Charged, Updated Sequence Number.

- $30: **type**- $FILE\_NAME, **offset**-152, **resident**? – yes, **content**- Parent directory file record number, Parent directory sequence number, File Creation time, File modification time, Record changed time, Last access time, Allocated size, Real size, File attributes, File name length, File name namespace, File name.

- $80: **type**- $DATA, **offset-264, resident?** – yes, **content-** Actual data of file (empty)

Temp3



start address: 0x0C000EC00

end address: 0x0C000EDE0

size: 0x0C000EDE0- 0x0C000EC00= 3221286368d– 3221285888d= 480 bytes

list of indexed clusters:

* file3.jpg: sector 6291576

attributes:

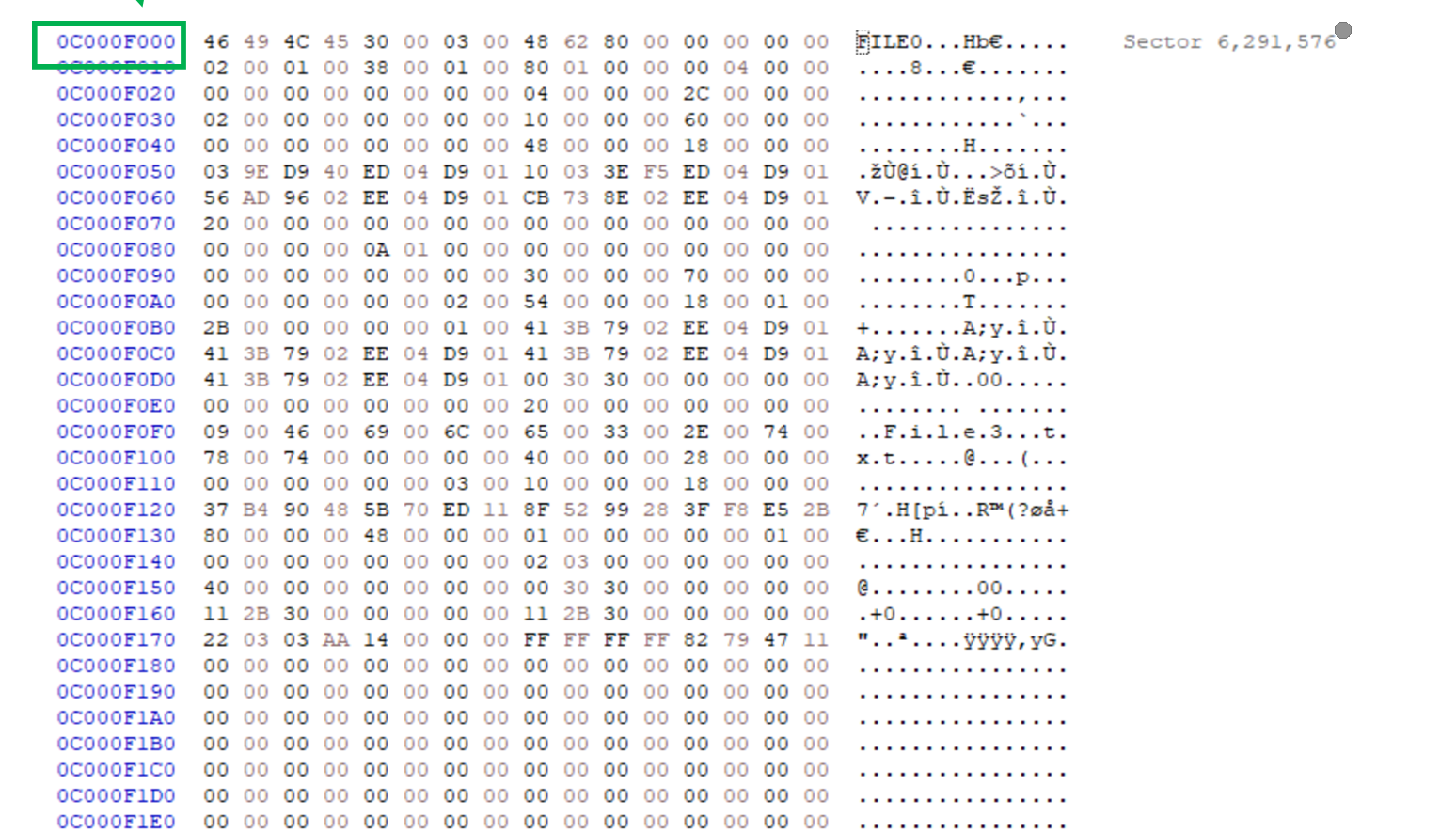
- $10: **type** -$STANDARD\_INFRMATION, **offset**-056, **resident**? – yes, **content**- File creation time, File modification time, Record changed time, Last Access time, File Permissions, Maximum number of versions, Version number, Class ID, Owner ID, Security ID, Quota Charged, Updated Sequence Number.

- $30: **type**- $FILE\_NAME, **offset**-152, **resident**? – yes, **content**- Parent directory file record number, Parent directory sequence number, File Creation time, File modification time, Record changed time, Last access time, Allocated size, Real size, File attributes, File name length, File name namespace, File name.

- $40: **type**- $OBJECT\_ID, **offset-256, resident?** – yes, **content-**object id

- $90: **type**- $INDEX\_ROOT, **offset**-296**, resident?** – yes, **content-** index root, index header

File3.txt



start address: 0x0C000F000

end address: 0x0C000F170

size: 0x0C000E920- 0x0C000E800= 3221287280– 3221286912= 368 bytes

attributes:

- $10: **type** -$STANDARD\_INFRMATION, **offset**-056, **resident**? – yes, **content**- File creation time, File modification time, Record changed time, Last Access time, File Permissions, Maximum number of versions, Version number, Class ID, Owner ID, Security ID, Quota Charged, Updated Sequence Number.

- $30: **type**- $FILE\_NAME, **offset**-152, **resident**? – yes, **content**- Parent directory file record number, Parent directory sequence number, File Creation time, File modification time, Record changed time, Last access time, Allocated size, Real size, File attributes, File name length, File name namespace, File name.

- $40: **type**- $OBJECT\_ID, **offset-264, resident?** – yes, **content-**object id

- $80: **type**- $DATA, **offset-304, resident?** – yes, **content-** Actual data of file (empty)

משום שקובץ זה הוא קובץ גדול ניתן לראות שהוא לוקח יותר מcluster אחד

