BoyEts: Help with the study of the structure of NTFS

BoyEts
unregistered (by topic)

written 10-10-2009 22:39 Edit • Reply • Report Post • IP

Took up the study NTFS, since the topic useful, because the data that is stored on my drives, I'm serious ... and if something goes wrong, would be able to fix it. But digging in the internet constantly bumping into some older articles (in fact several versions of NTFS, I'm interested in version 3 for XP). Practical examples on the net and even less (and even more understandable in Russian). Now Currently began to study the structure of MFT First neponyatka - all point to the beginning of the table with a FILE *, and I have the same disk FILE0 ... what matter? And such a silly question - "offset 0x28" .... which means "0", "x" and "28"? have my picture for clarity.
http://s48.radikal.ru/i120/0910/be/ 663e0c9c8d29.jpg (1280x833, 340.5 Kb)

nazyura
Data Recovery Expert
Web-page

written 11.10.2009 8:13 Info • Private • Edit • Reply • Report Post • IP

There was something ... look ... Help with data recovery from HDD

BoyEts
unregistered (by topic)

written 11-10-2009 13:11 Edit • Reply • Report Post • IP

there is not, sought

Antech
Advanced Member
Location: Russia, Solar System Web-page

written 11-10-2009 20:45 Info • Private • Edit • Reply • Report Post • IP

BoyEts
several versions of NTFS
Hammer, no significant differences. The only thing that can be noted: the presence / absence of the file record numbers at offset 2Ch bytes from the beginning of the recording. It is important for recovery. *everywhere indicate the start of the table with FILE *, and I have the same disk FILE0 ... what is it?* Of course, I'm sorry, but you look at the structure FILE Record, and not only on the picture . This is the difference between versions (FILE * - old, FILE0 - new). After signature FILE located two byte field - offset USA = Update Sequence Array (array corrections). In the new version, this field 30 00 (0030h), that in the interpretation of the character is shown as "0", an old version of this field 2A 00 (002Ah), that in the interpretation of the character is shown as "*". And, if you look NTFS Version attribute 70 = VOLUME_INFORMATION metafile $ Volume, then for both versions can detect there 3.1 , ie it is one and the same version of NTFS, although in the case 2A 00 (FILE *) numbers of records are not available, and in the case of 30 00 (FILE0) have record numbers. obrazIm Thus, the signature file record - namely FILE, not FILE0 or FILE * . *"offset 0x28" .... which means "0", "x" and "28"?* prefix "0x" means hex, as well as the suffix "h": 0x28 == 28h. To translate Hex <=> Dec vinduzyatny use calculator (View - Engineers). Could you attach pictures to messages? To do this, click on "Reply" on any message there, select "New, from file" and select the picture.

BoyEts
unregistered (by topic)

written 11-10-2009 21:23 Edit • Reply • Report Post • IP

Antech
You could not attach pictures to messages? To do this, click on "Reply" on any message there, select "New, from file" and select the picture.
'll know
Thanks!
's only half an hour ago figured out FILE0 - so it is formatted in XP (but only found on the English site).
In about 0x28 .... Could you tell me to understand where that figure (which row, which column) is the value and meaning of 0x2A?
And yet - to verify the integrity MFT record something there must be the same - those tell the same example what?

Antech
Advanced Member
Location: Russia, Solar System Web-page

written 12.10.2009 11:07 Info • Private • Edit • Reply • Report Post • IP

BoyEts
figured out FILE0 - so it is formatted in XP
Yes. But is not that the formats, but the fact that I wrote above. *where that figure (which row, which column) is the value and meaning of 0x2A* Use WinHex. There have signs at the top of columns. Offset 28h - this is the third row and column of "8". Or Alt + G, Bytes, Hex, Current

position, 28. Moreover 2A - did not understand. It was about the USA offset (offset from the beginning of recording 4), there you have 30 00 (FILE0), and sometimes 2A 00 (FILE *). Hint: turn off the backlight options WinHex attributes file record. I understand that it is convenient, but it's relaxing. Automation is useful if you have already learned the basic chips FS and need to quickly make some sort of case. A study on the stage better (but not necessarily) only the basic functions used. (Incidentally, I have also turned off lights.) IMHO.

BoyEts
unregistered (by topic)

written 12.10.2009 16:33 Edit • Reply • Report Post • IP

Antech
There have signs above the columns. Offset 28h - this is the third row and column "8"
Ie 0x28 - the coordinates. In my case, these coordinates to present value 00h.
Did 0x2A can not be coordinate?

Antech
Advanced Member
Location: Russia, Solar System Web-page

written 12.10.2009 17:59 Info • Private • Edit • Reply • Report Post • IP

BoyEts
Linux NTFS (PDF, ZIP)

0x28 - the coordinates of
the coordinates. One. Field offset (starting byte field) with respect to a particular position ("zero position"). Computer memory (RAM DZU, etc.) - a one-dimensional sequence of bytes (in DZU type flash drive / floppy / screw there is a division into sectors, but you can logically work as a one-dimensional sequence, ignoring the boundaries of sectors, although very often the structure attached to the borders of sectors). What you see in the editor two coordinates - this is only for ease of reading done, the number of columns can be different from the standard 16 (have to do this in the toolbar buttons WinHex). *0x2A can not coordinate?* Maybe. The range of values of displacements in general - from 0 to N-1, where N - number of bytes available on the device.

BoyEts
unregistered (by topic)

written 12.10.2009 18:50 Edit • Reply • Report Post • IP

Antech
Thanks for knizhetsu, here vividly!
For assimilation - I have this on the screenshot unfortunate coordinate 0x2A?
Read it and you say "Array corrections MFT record size 2 * (N-1) bytes, where N - the value of the array size adjusting entries from the field at offset 0x06 ".... as I know from the area of mathematics (array) values are defined by two coordinates - the beginning and end. Then something is not fit. Where to start, where is the end?

Antech
Advanced Member
Location: Russia, Solar System Web-page

written 12.10.2009 22:56 Info • Private • Edit • Reply • Report Post • IP

BoyEts
on the screenshot I have this unfortunate coordinate 0x2A?
And what do you think ? The second line, the tenth column (counting from zero). If you have a standard of 16 products in the line, the first nibble (nibble) single-byte offset - is the row number (counting from zero), and the second nibble - column number (Ah == 10, also numbering from zero). Of course, provided that the given offset "from the start line," so to speak. If bias - not from the beginning of the string, the first nibble is the number of rows that need to shift down (when the cursor is in the initial position from which are offset), and the second nibble indicates the number of columns that you should move to the right. This is useful to quickly climb on structures (for example, to pass a chain of attributes in a file record), even if you have only a picture, and no dump. *it like you said and corrections Array* No, you have an array of adjustments at offset 30h bytes (look in column 4 row 0, numbering from zero). *region (array) values are defined by two coordinates - the beginning and the end* you have in polar coordinates array corrections set ... Array - a more general concept than a continuous range. Array elements can never be placed sequentially in memory (even virtual), and instead of an array of structures / values can be given an array of pointers. So let's not complicate things. In the on-disk-structure is a classic representation as offset + size (usually in hex, but sometimes give in dec). Thus, the final coordinate is defined as the initial size + 1. *Where is the beginning, where the end?* Regarding array corrections. This easy way to check the file record intact (easy - to consume fewer resources proca). Generated a certain two-byte value - template (it can be anything that is random). This value is written to the first element of the array adjustments (note: one element - two bytes). Further, each file sector recording (usually only 2 sectors) recorded last 2 bytes in the subsequent array elements corrections, and their location pattern is placed. To use a file record, it needs to first fix (correct) that is done in the reverse order in each sector recording the last two bytes are replaced by the corresponding element of the array, and the integrity is verified by comparing it to the template in the header record (ie, the array) with the last two bytes of each sector record. Specifically on your example. After signature FILE see box 30 00 - USA power offset 30h bytes (and not 2A, do not understand how you took 2A). Behind him - Field 03 00: Size USA - three elements (each 2 bytes). The cursor to the beginning of the recording, shimmy 3 rows down. That under the cursor? Template: E8 00. Two remaining array element - the zeros: 00 00 and 00 00. Enjoying a "last line of the sector" (indicated at the beginning offset 1F0h) - see there at the end E8 00 - it is a pattern. Is replaced by zeros. Do the same with the second recording sector, which is not in the picture (see there E8 00). I hope you understand that we can not "stupid" be replaced by zeros. Just you have to adjust the array initial values - zero.

For this post Thanks: BoyEts

BoyEts
unregistered (by topic)

written 13.10.2009 00:04 Edit • Reply • Report Post • IP

Antech
's just that's exactly what I did not give rest and you'll all spread out in the shelves where in any manual does not find! Now I'm in this part of almost everything is clear. Thank you very much! Over the last paragraph I have obmozguyu, but overall logic is glued! I will move on .....

BoyEts
unregistered (by topic)

written 29-11-2009 23:38 Edit • Reply • Report Post • IP

I finally got back to the topic.
Unfortunately neponyatki with MFT I still have, and all because a variety of sources, ntfs-old system. I have the same version of ntfs 3.1 and very hard to compare xy xy. Figure fragment my ntfs http://i071.radikal.ru/0911/33/568f13b1a479.jpg documentation Linux Project is all too technical and confusing and without examples. Search Engines give no entries .... I understand that there is no magic pill, but still, on that note, not to be confused? Remind me the knowledge needed to restore the faulty section, determine the offset, study ranlistov etc.

Doomer
Data Recovery Expert.
HDDScan author
Location: United States, Chicago Web-page

written 30.11.2009 7:37 Info • Private • Edit • Reply • Report Post • IP

BoyEts
afraid that if your drive fails and you fix them climb, you will make the final
order to pursue the study of something new and poorly documented needs analytical mind (you do not have)
a person with an analytical mind before asking what 0x, would ask Google about this, and the first link was the answer - http://ru.wikipedia.org/wiki/0x
you used to work for the same crib so badly documented information is not acceptable, because do not want to analyze
Unfortunately / fortunately in the subject in which you want to sort out work on the crib is difficult, fragmentary information and disordered and anyway requires an analysis of PS: if you suddenly want to angrily denounce me shame, I recommend not to bother, because it is useless, I'm just trying to save time and your members of the forum at the same time

Antech
Advanced Member
Location: Russia, Solar System Web-page

written 30.11.2009 9:11 Info • Private • Edit • Reply • Report Post • IP

BoyEts
documentation Linux Project is all too technical and confusing
Yes, it's clean as a reference. Very comfortable poke TOC (I PDF-version) and see the desired structure.
's article Chris Kasperski like it enough ponimabelna. I learned the basics on paper Frolovs brothers , but it just ends up on ranliste so for ranlistom refer to Article Virus or Linux NTFS (and there are examples). There are book "Forensic analysis of file systems" B. Kerrie, but this book-warez and I can not give the link here. *described ntfs-old system* there is almost no difference. Well izmenilos standard deviation of an array of adjustments, but it is "variable offset" field and change the bias does not change the version of the file system. Unless there were some so old NTFS, and that there were other structures? I have not seen such ... **Doomer** I would not say that all bad documentation NTFS. For practical purposes the main materials have described is available ...

BoyEts
unregistered (by topic)

written 30.11.2009 9:11 Edit • Reply • Report Post • IP

doomer
really helped, no longer bother to answer, especially not on a subject.

Addendum dated 30.11.2009 9:24:

Antech
Happy Birthday!
'll try it to understand itself, but even there is a difference in the displacement of which indicates the file size.
Here is an example http://rlab.ru/doc/recovery_from_damaged_ntfs.html saying that the file length is set at offset 30 that I already do not match. Plus it is impossible to make an analysis of the field units VCN, since these blocks are where I - is unclear. And in that example - "Fixup area starts at offset 002A and extends up to 002A + (2 * 0003) = 002F" - so they got 002F??

Your answer: Ask a Question

Code List
Forum List of emoticons

"Floating" response window

Name, password, icon or No icon Send without emoticons .

printable version · Search · subscribe · blacklisted · Send to friend · Statistics

Search · **New Topic** · **Leave a reply**

Jump to: Magnetic and SSD Drives "

Contact the Conference

Conference Rules · FAQ by conference · Site Map · **Search**
Want to become moderator? · Advertise · Statistics

Our projects: iXBT.com · komok.com · fotkidepo.ru · iTRate.ru