

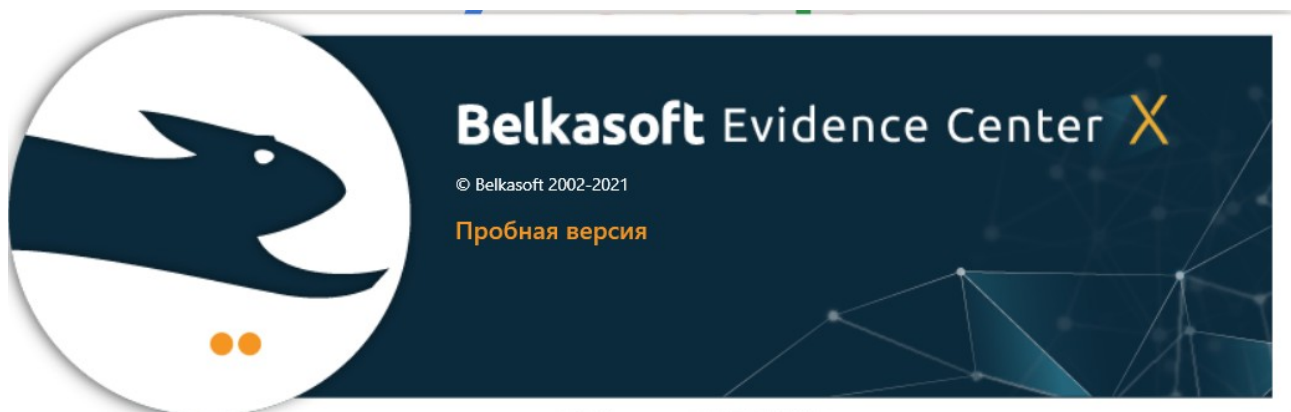
Why do you need MFT info in a forensic investigation

Okay. Let the task of our today be about low-level analysis.

And more specifically let's talk of MFT and how it can be useful to us in a forensic investigations.

First of all, you may ask, I suppose, what is MFT?

MFT – Master File Table – is a database file which maintains info on NTFS volume contents (i.e. all the files) and thus, in some point of view, represents a complete image of the volume itself. It keeps all the filenames with key file attributes (ID, size, timestamp, permissions, data content description, etc.). The keyword for us is ...[smiling]... “key”. Moreover, the general feature of MFT is to keep and securely store *all* the records regarding *all* the files presented in a volume during its lifetime. So it's obvious at this point that MFT can be a very useful thing for our purposes. And thus the task is how to acquire information from it with much efficiency.



In a matter of case we will use Belkasoft Evidence Center X, Belkasoft's flagship digital forensic suite. This product makes it easy for investigator to perform all steps of modern digital investigation (such as data acquisition, artifact extraction and recovery, analysis, reporting and sharing). The product supports mobile, computer, memory (RAM) and cloud forensics.

Both high-level and low-level analysis can be done with it. Btw it is an irreplaceable analytical tool for digital forensic laboratories of federal law enforcement agencies and state-level police departments. So we've chosen Belkasoft Evidence Center X as a powerful and comfortable – suitable – tool at all.

Belkasoft Evidence Center X | v.1.11.9199 TRIAL VERSION | 111

Dashboard File System

Case Properties

Name: 111
Investigator:
Timezone: RTZ 2 (зима)
Notes:
Path: C:\Users\user\AppData\Roaming\...
Created: 15.02.2022 15:23:30

Actions

- Add data source
- Search artifacts
- Create report
- Export to Evidence Reader
- Create key dictionary
- Prepare log files
- Delete case

Automatic searches

- URL: 886
- Phone number: 472
- Windows full paths: 288
- Email addresses: 82
- Postal codes: 72
- IP address: 20

Data sources

Show nested data sources

E:\ (2341 artifacts)

Type: Logical drive
Timezone: RTZ 2 (зима)
Path: E:\ Analyzed with errors

Pictures	2178	Documents	118	Other files	14
Encrypted files	12	Chats	7	Contacts	6
Mails	4	URLs	2		

E:\ (507 artifacts)

Type: Logical drive
Timezone: RTZ 2 (зима)
Path: E:\ Successfully analyzed

Pictures	388	Documents	118	Contacts	1
----------	-----	-----------	-----	----------	---

Application types

- Mail.ru Agent: 7
- EML files: 4
- Safari: 2

Artifacts

- Pictures: 2566
- Documents: 236
- Encrypted files: 12
- Contacts: 7
- Chats: 7

Let's see accordingly what Belkasoft Evidence Center X acquires from MFT.
Here's an example of Belkasoft's typical MFT info window.

Hex MFT info

Sequence Number: 0xA9E - 0xA9D, Flags In Use: Resident|NonResident, Offset: 0x2DE009000, Hex Value: 0x00000A9E - 0x00000A9D

*** Standard Info ***

Type: Standard Info, Attribute Number: 0x0, Size: 0x48, Is Resident: True

Created On: 10.01.2022 9:22:11,
Content Modified On: 27.10.2011 4:25:14,
Record Modified On: 27.10.2011 4:25:14,
Last Accessed On: 10.01.2022 14:25:15

*** File Name ***

Type: File Name, Attribute Number: 0x2, Size: 0x5C, Is Resident: True

File Name: AccessMUI.msi

Created On: 10.01.2022 14:25:15,
Content Modified On: 10.01.2022 14:25:15,
Record Modified On: 10.01.2022 14:25:15,
Last Accessed On: 10.01.2022 14:25:15

*** Data ***

Type: Data, Attribute Number: 0x1, Size: 0x193E00, Is Resident: False
Skip Length: 0x0, Compressed Size: 0x0, Allocated Size: 0x194000, Initialized Size: 0x193E00

Data-run entries
Flag: None, Length: 0x194, Address: 0x2DE009

There, as we may see, the Belkasoft's product gives us an amount of complete information on file's (or directory's) deployment, size, type, creation-modification-accession data, etc. Having in mind the fact that MFT keeps forever info on any object of the current file system, once NTFS got it, we're just clearly able to acquire all the vital data on the individual's content. And so, by this way, we can get access to the content itself. Does not matter if data is still kept in files or deleted, hidden in unallocated or slack space, Belkasoft Evidence Center X can easily reveal it by searching inside existing files, carving using file or record signatures, analyzing Volume Shadow Copy and many other forensically important areas (such as, for example, SQLite freelists). Btw it has a convenient Hex Viewer just in hand.

Hex

MFT info

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
000000000000	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	*****
000000000010	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	*****
000000000020	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	*****
000000000030	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	*****
000000000040	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	0D	0A	2A	2A	2A	2A	*****.****
000000000050	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	*****
000000000060	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	*****
000000000070	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	*****
000000000080	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	2A	*****
000000000090	2A	2A	2A	2A	2A	2A	0D	0A	2A	20	20	20	20	20	20	20	*****.*
0000000000A0	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
0000000000B0	20	20	20	20	49	6E	73	74	61	6C	6C	61	74	69	6F	6E	Installation
0000000000C0	20	52	65	61	64	6D	65	20	66	6F	72	20	0D	0A	2A	20	Readme for ..*
0000000000D0	20	20	20	49	6E	74	65	6C	28	52	29	20	52	61	70	69	Intel(R) Rapi
0000000000E0	64	20	53	74	6F	72	61	67	65	20	54	65	63	68	6E	6F	d Storage Techno
0000000000F0	6C	6F	67	79	20	28	49	6E	74	65	6C	28	52	29	20	52	logy (Intel(R) R
000000000100	53	54	29	20	77	69	74	68	20	53	75	70	70	6F	72	74	ST) with Support
000000000110	20	66	6F	72	3A	0D	0A	2A	20	20	20	20	20	2D	20	49	for:..* - I
000000000120	6E	74	65	6C	28	52	29	20	4F	70	74	61	6E	65	28	54	ntel(R) Optane(T
000000000130	4D	29	20	4D	65	6D	6F	72	79	20	53	79	73	74	65	6D	M) Memory System
000000000140	20	41	63	63	65	6C	65	72	61	74	69	6F	6E	5E	5E	0D	Acceleration^^.
000000000150	0A	2A	20	20	20	20	20	2D	20	52	41	49	44	20	30	2F	.* - RAID 0/
000000000160	31	2F	35	2F	31	30	5E	5E	0D	0A	2A	20	20	20	20	20	1/5/10^^.*
000000000170	2D	20	43	50	55	20	41	74	74	61	63	68	65	64	20	53	- CPU Attached S
000000000180	74	6F	72	61	67	65	5E	5E	0D	0A	2A	20	20	20	20	20	torage^^.*
000000000190	20	5E	5E	20	4E	4F	54	45	3A	20	53	75	70	70	6F	72	^^ NOTE: Suppor
0000000001A0	74	20	66	6F	72	20	74	68	69	73	20	66	65	61	74	75	t for this featu
0000000001B0	72	65	20	69	73	20	64	65	74	65	72	6D	69	6E	65	64	re is determined
0000000001C0	20	62	79	20	79	6F	75	72	20	68	61	72	64	77	61	72	by your hardwar
0000000001D0	65	20	63	6F	6E	66	69	67	75	72	61	74	69	6F	6E	0D	e configuration.
0000000001E0	0A	2A	0D	0A	2A	20	54	68	69	73	20	64	6F	63	75	6D	.*..* This docum
0000000001F0	65	6E	74	20	6D	61	6B	65	73	20	72	65	66	65	72	65	ent makes refere
000000000200	6E	63	65	73	20	74	6F	20	70	72	6F	64	75	63	74	73	nces to products
000000000210	20	64	65	76	65	6C	6F	70	65	64	20	62	79	20	49	6E	developed by In
000000000220	74	65	6C	2E	20	54	68	65	72	65	20	61	72	65	20	73	tel. There are s
000000000230	6F	6D	65	20	0D	0A	2A	20	72	65	73	74	72	69	63	74	ome ..* restrict
000000000240	69	6F	6E	73	20	6F	6E	20	68	6F	77	20	74	68	65	73	ions on how thes
000000000250	65	20	70	72	6F	64	75	63	74	73	20	6D	61	79	20	62	e products may b

Size: 29.8 Kb

This window assisting you to investigate particular bytes, make automatic type conversions, create bookmarks, run custom carving and apply various encodings.

Concerning MFT info Belkasoft Evidence Center X provides the powerful File System Explorer, which shows all volumes and partitions inside the device, existing and deleted folders, VCS snapshots, existing and deleted files.

The screenshot shows the Belkasoft Evidence Center X File System Explorer interface. The left pane displays a tree view of the file system, with the current view set to 'E:\ [11]'. The main pane shows a table of files with columns for File type, Name, Created (UTC), Modified (UTC), Access time, and Entry changed. The table lists five items: \$Objid, \$Quota, \$Reparse, \$Deleted, and \$RmMetadata. The \$Objid file is selected, and its MFT info is displayed in the bottom pane. The MFT info panel shows the following details:

Property	Value
Name	\$Objid
Created (UTC)	04.01.2020 4:02:36
Modified (UTC)	04.01.2020 4:02:36
Access time (UTC)	04.01.2020 4:02:36
Entry changed (UTC)	04.01.2020 4:02:36
MFT created (UTC)	04.01.2020 4:02:36
MFT modified (UTC)	04.01.2020 4:02:36
MFT access time (UTC)	04.01.2020 4:02:36
MFT entry changed (UTC)	04.01.2020 4:02:36
File size (bytes)	0
MD5	Not calculated
SHA1	Not calculated
SHA256	Not calculated
Full path	image\1\vol_0\ \$Extend\ \$Objid
Offset (bytes)	0
Alternate data streams count	3

Note, all this came to us through NTFS Master File Table. Just one file, but many opportunities. And that's why MFT info is essential in the forensic investigations at all.

So enjoy. :-)

Final ad

Belkasoft Evidence Center X is much more cost-effective and overall a much better value. The product offers more features for a lower price than most other products on the market. Not only does it save you money at the moment of purchase, it also helps you save every year after that with its cost-effective priced renewals. Moreover, our free Evidence Reader allows you to share your work with your colleagues at absolutely no cost, thus saving you even more! Finally, Belkasoft X customers have a wide variety of discounts towards the purchase from our partners' digital forensic products.