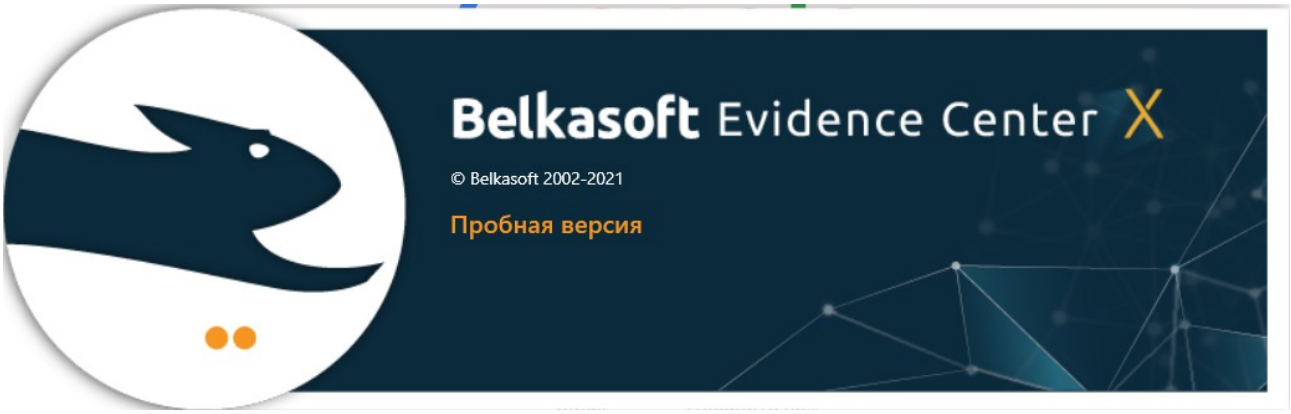
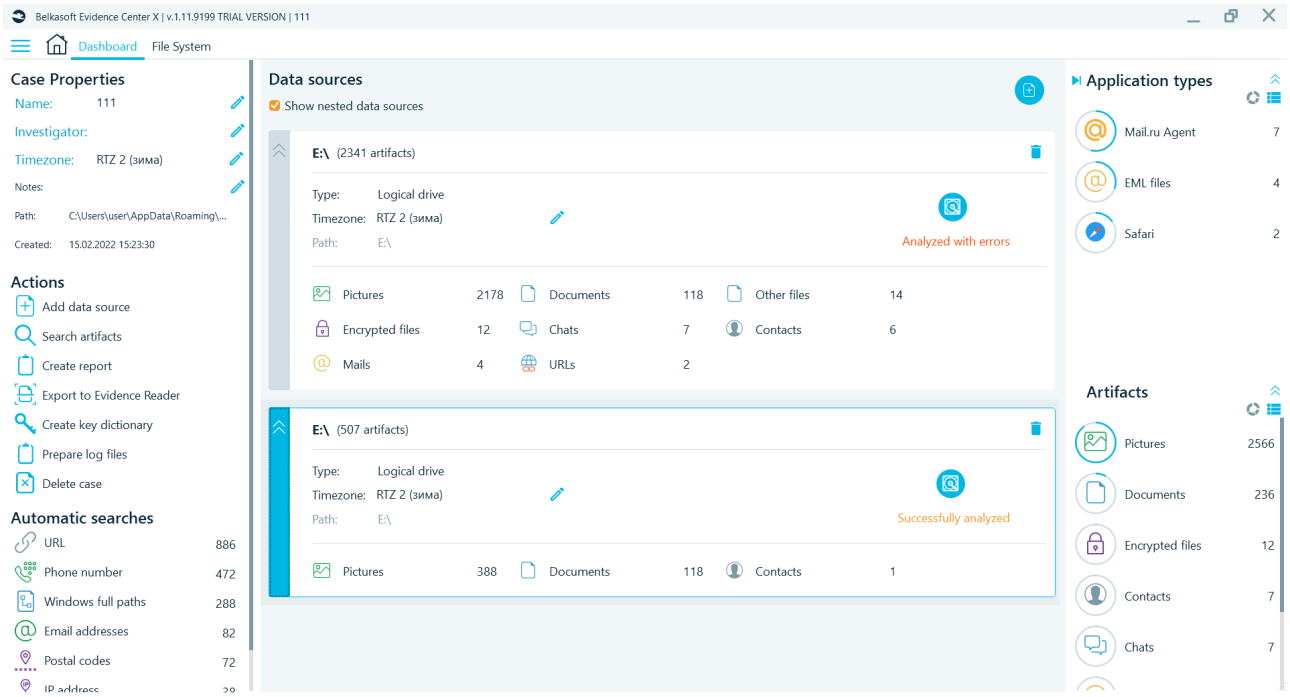
Why do you need MFT info in a forensic investigation

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.

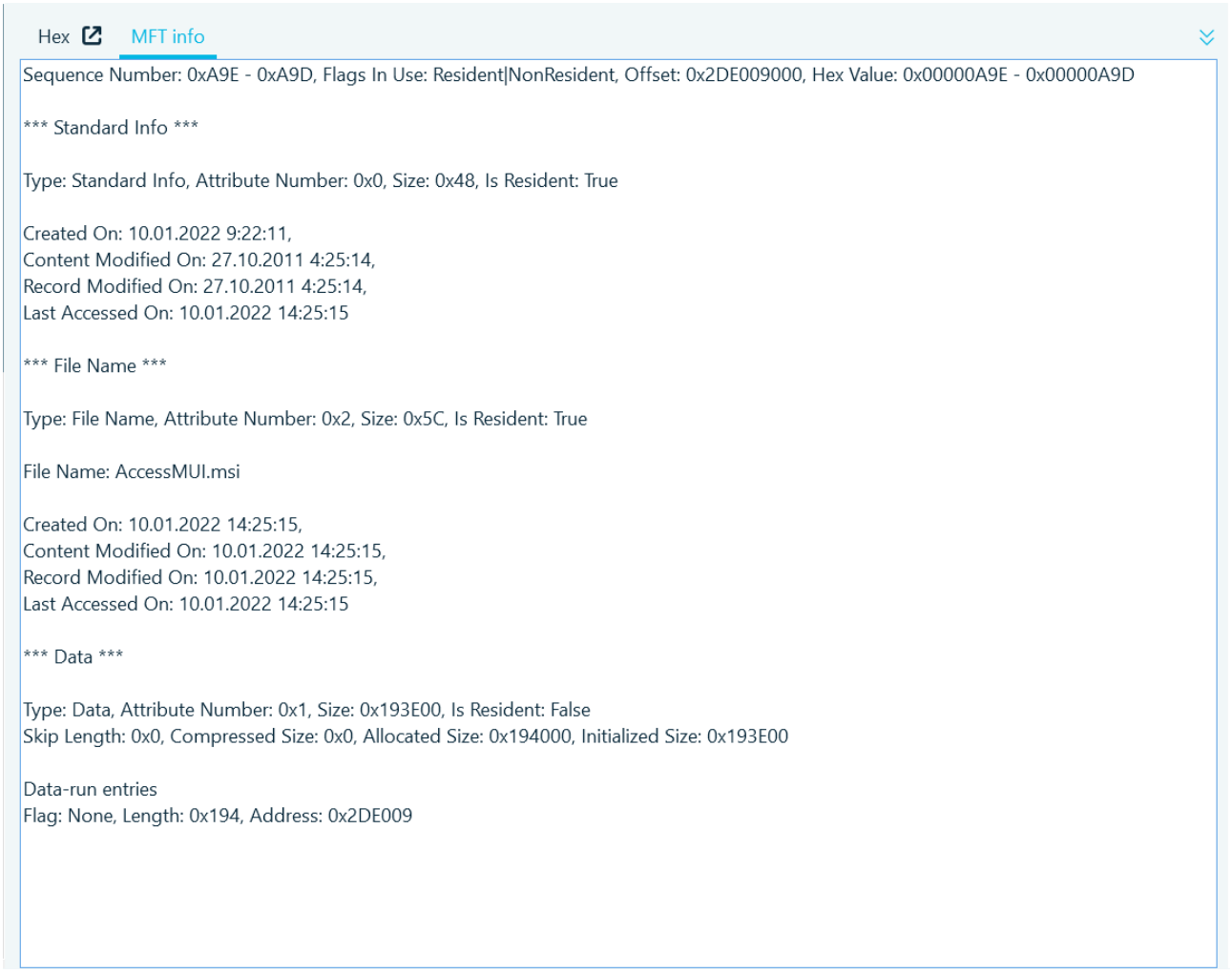
First of all, you may ask, I suppose, what is MFT?
MFT – Master File Table – is a database file which maintains info on NTFS volume contents (i.e. all the files) and thus, in some point of view, represents a complete image of the volume itself. It keeps all the filenames with key file attributes (ID, 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 effeciency.



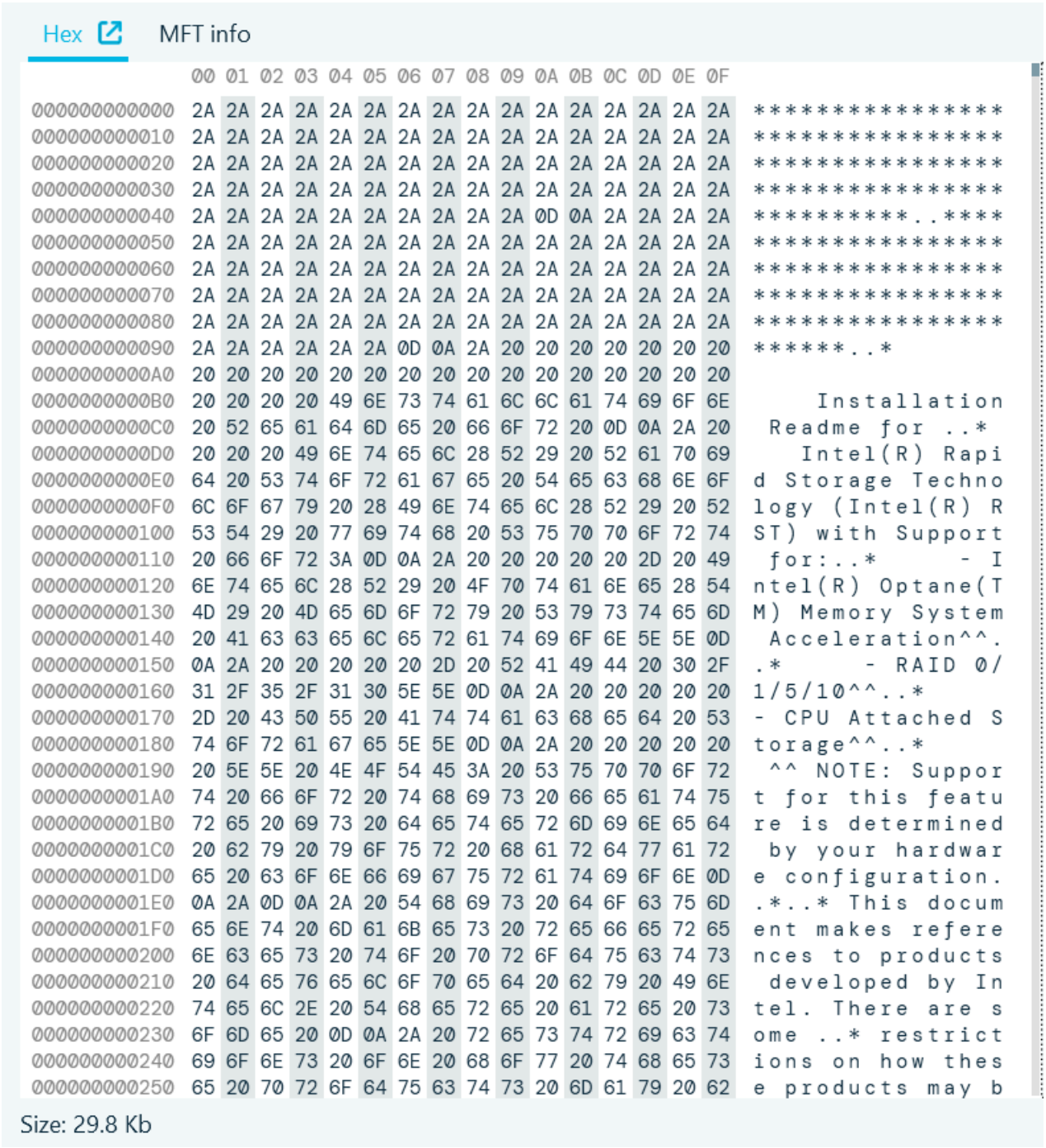
In a matter of case we will use Belkasoft Evidence Center X, Belkasoft's flagship digital forensic suite. This product makes it easy for investigator to perform all steps of modern digital investigation (such as data acquisition, artifact extraction and recovery, analysis, reporting and sharing). The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



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

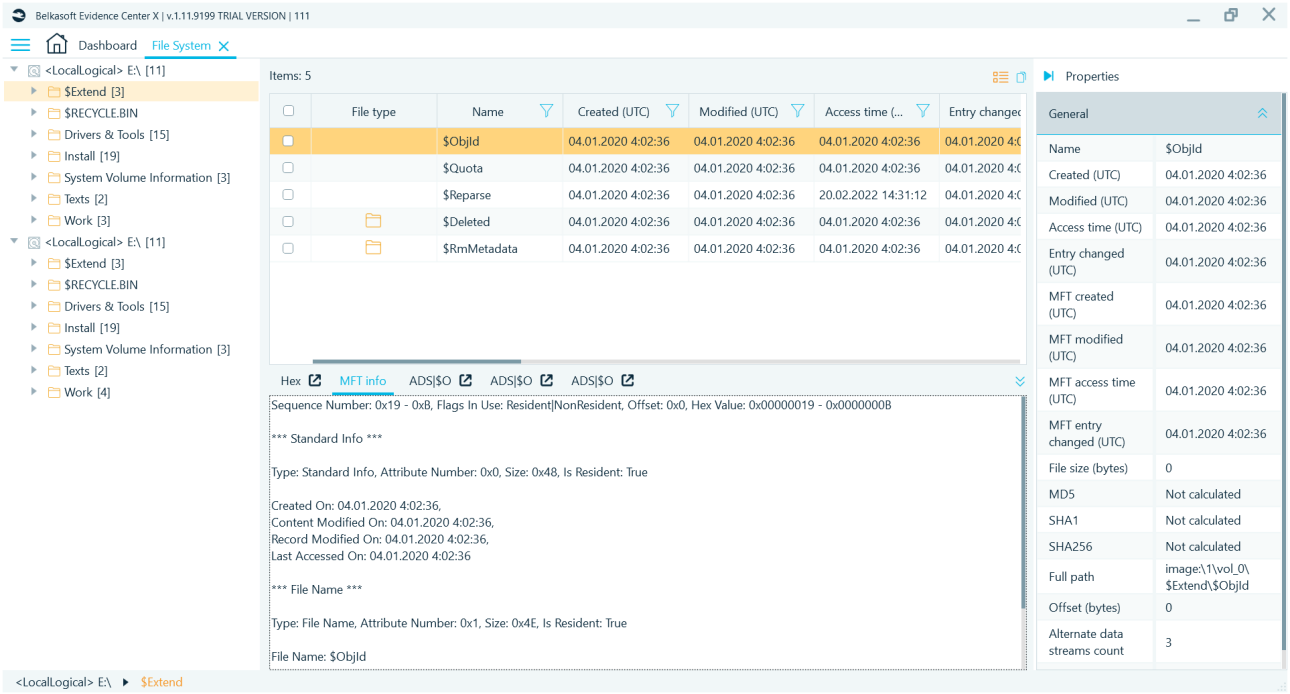


There, as we may see, the Belkasoft's product gives us an amount of complete information on file's (or directory's) deployment, size, type, creation-modification-accession data, etc. Having in mind the fact that MFT keeps forever info on any object of the current file system, once NTFS got it, we're 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.



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.



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. :-)