



Belkasoft X
Evidence Center

"I recommend Belkasoft X to those who need an effective, efficient, intuitive and proven forensic suite at a price point that beats just about every competitor. Value? You bet."



BRETT SHAVERS
DFIR Expert, Independent Consultant,
Author, Person behind DFIR.Training website
USA 

THE SHORT STORY

[Belkasoft X](#) gives great value in both cost and features. Acquire, process, and delve into the data with an intuitive interface that cleanly shows automated categorization of forensic artifacts. Although easy to use, this is a true forensic suite that does more than what you might expect for the price of the license.

BELKASOFT X: WHAT IS IT?

[Belkasoft X](#) is Belkasoft's top forensic suite, comparable to any other forensic suite that you may be using. In several ways, Belkasoft X is not only on par with most any other forensic tool but exceeds in many areas.

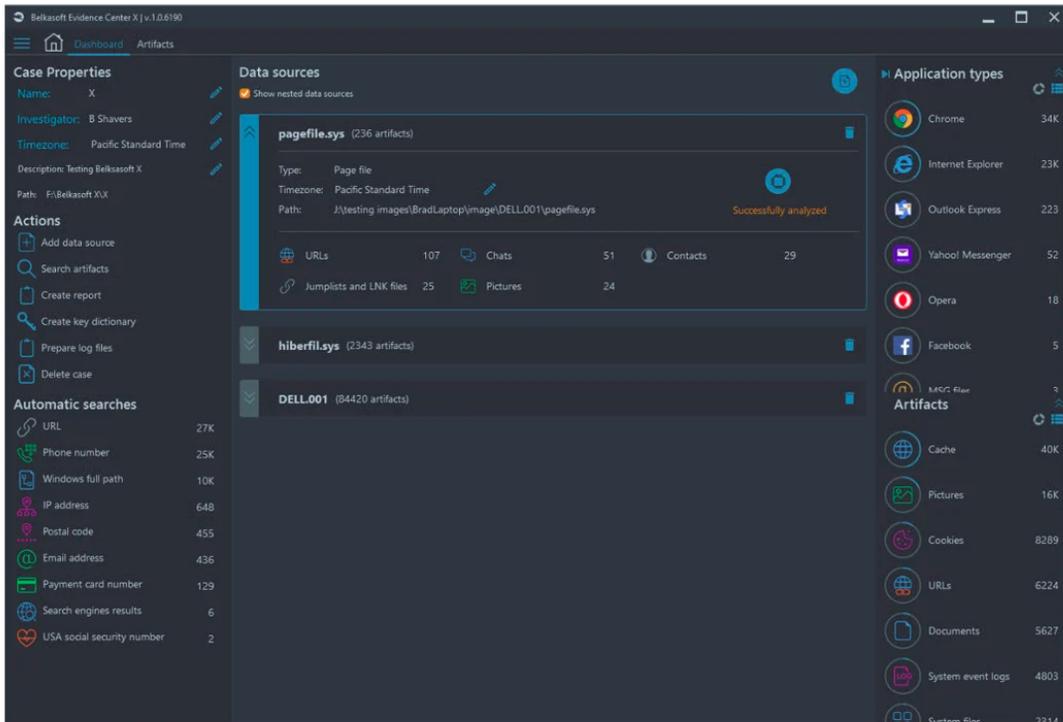


Figure 1: The Belkasoft X dashboard (dark theme)

BELKASOFT X: WHAT DOES IT DO?

As far as what [Belkasoft X](#) does, since it is a forensic suite, it does practically everything that you would expect a forensic suite to do from initial acquisition of evidence to reporting of the entirety of an analysis. This includes not only the basic computer forensics type of cases, but also mobile devices, cloud, and memory forensics. As I said, it is a full forensic suite.

If you've not heard of Belkasoft before, [download the trial of Belkasoft X](#) and run it against known data or test images to check it out. The time will be well spent to quickly and easily see how intuitive the interface has been designed.

I have experience with Belkasoft BEC with Checkm8 (iOS acquisitions) and general casework. Belkasoft X is an improved forensic platform from the Belkasoft BEC that I have used, and this is a nice improvement.

If you want to have near-personal training and exposure to Belkasoft X, check out their next webinar at <https://belkasoft.com/webinar>.

I recommend downloading the trial, checking out the webinar, and you'll have a good handle of Belkasoft X operations. It is that easy to use.

BRETT'S OPINION

Here's the thing about reviews of anything, whether it is a review of a new car or tennis racket. When I want to know the specs, I go straight to the source to get the nitty-gritty details. When I want to know if the product is worth the money, I go where I can read that someone said it is worth it or not. Just tell me if the product is worth it!

With that, if you want to know the specs of Belkasoft X, Belkasoft has been putting out webinars (next webinar previously mentioned above) and videos on what Belkasoft X does, how it does it, and how you can use it.

If you want to know if Belkasoft X is a good value for a forensic suite, the answer is unquestionably yes.

Let me qualify my opinion because the cost-to-value is only good if the product fills a need that you have at a price that is reasonable.

- 1. PRICE.** Belkasoft's pricing model is the kind of model that you hope never changes because it is less expensive than most other forensic suites, yet is not less featured.
- 2. FEATURES.** As above in #1, the features are there. Practically anything you need in forensic analysis.
- 3. SUITE:** This isn't just a common forensic tool. This is a major suite that is intuitive and drives through data, puts everything in neat categories, and lets you navigate from neatly organized artifact to the next neatly organized artifact.

There are other good points, such as I found Belkasoft to run on mid-range machines well, practically flawless when running, and fast enough processing to get near-immediate results.

Belkasoft X is the type of forensic suite that will ingest everything, nearly categorize the artifacts for you, plot geolocation data points on a map, make connections with contacts, and for anything you don't see jump right out at you, allows you to search and filter to find the artifacts to make your case. And yes, you can do hex (Figure 2) viewing, copying, and searching too.

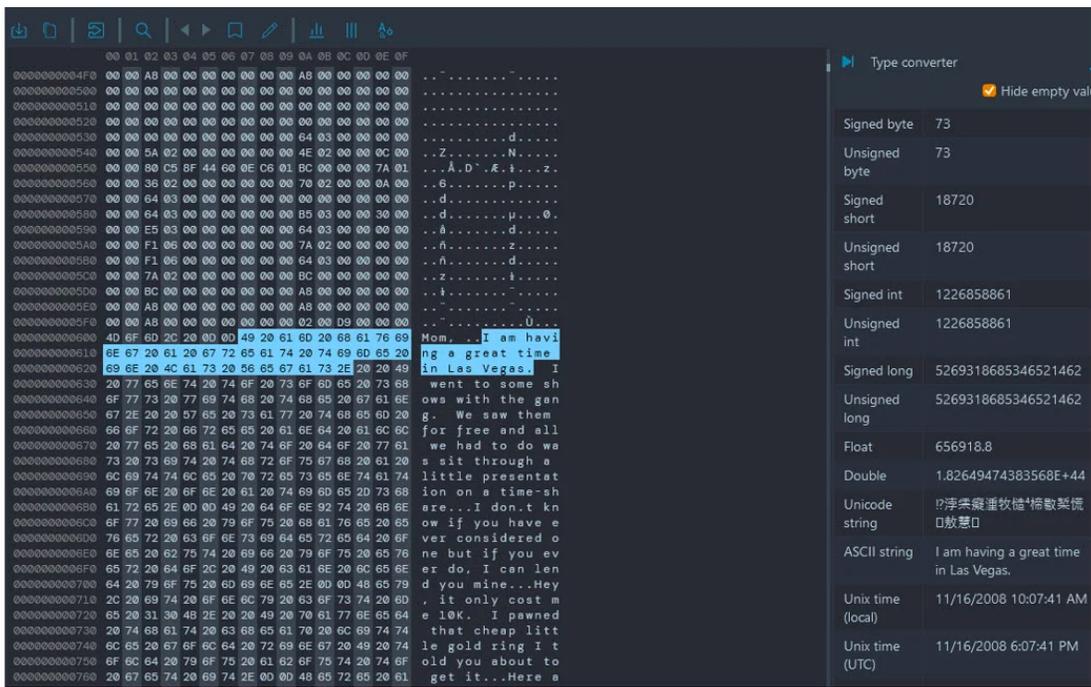


Figure 2: Yes. Hex too

IS IT FOR YOU?

Just like everything else in DFIR, it depends. It depends on your specific role and the needs of your case. Some in DFIR use small tools to do the vast majority (if not all!) of their work because that is the focus of what they are hired to do. Others use massive, enterprise-level forensic suites because that is what they are hired to do. The bell curve of everyone else uses a mixture of everything, from the small tool to the enterprise suite.

Belkasoft X fits in the big bell curve of covering a huge swath of casework. Your processes may be different from mine, then again, every case is different in how you approach the case based upon your case objectives.

Over the past years, forensic suites have improved drastically in features, and ease of use. This is where Belkasoft shines. Starting Belkasoft X gives you two options: Create case or Open case. There are forensic suites that provide such a myriad of options that you have to stop and think about which option you need to just get working in the application. For what Belkasoft X is designed to do, I prefer simplicity for several reasons, a few I will talk about. As a side note, there are other options, like Settings , that are available to choose from, but to get started right away, two big and unmistakable icons guide the way.

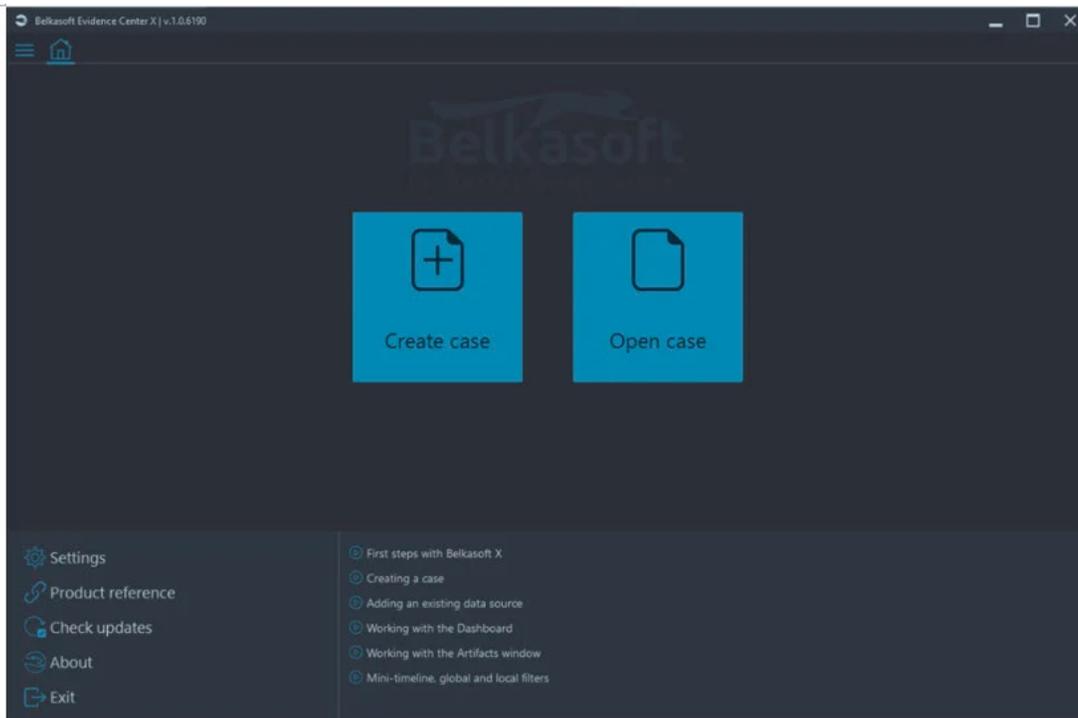


Figure 3: Starting Belkasoft X

Once in a case, the layout is clean and somehow fits amazingly well. You can see in Figure 4 where (1) in the Artifacts tab/sidebar, you can choose the automatically categorized artifacts, (2) view the artifact, (3) see the text or hex, and the details of the artifact in (4) and (5). Panels can be resized or hidden when focusing on a particular pane of interest.

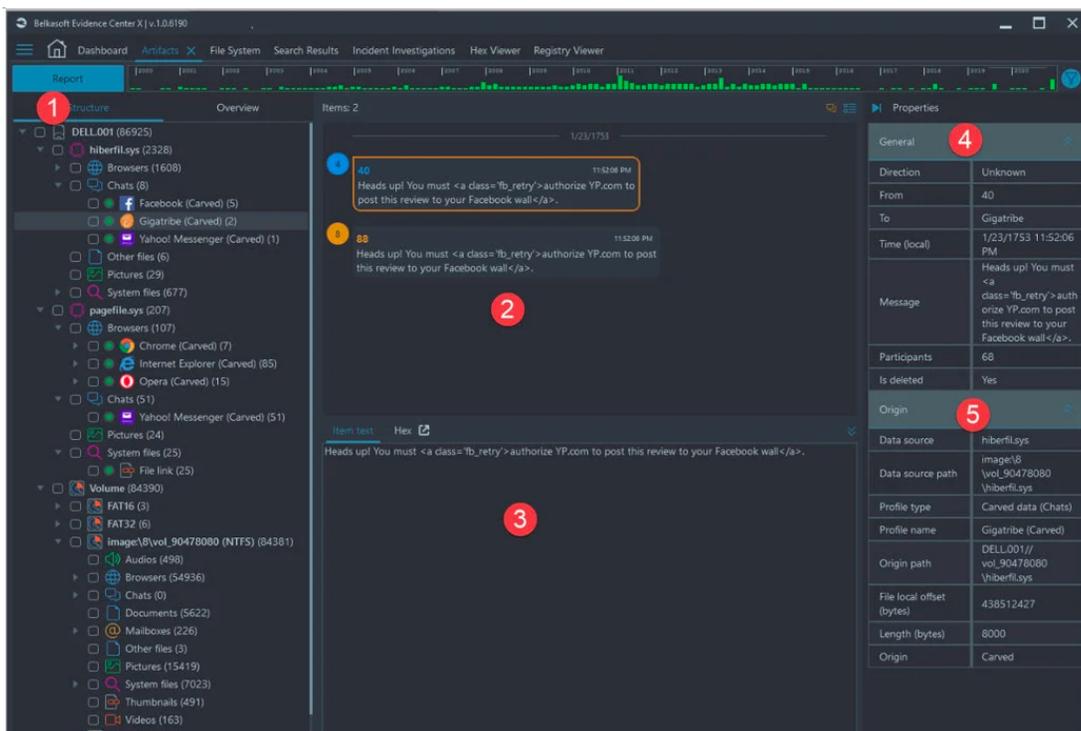


Figure 4: Layout

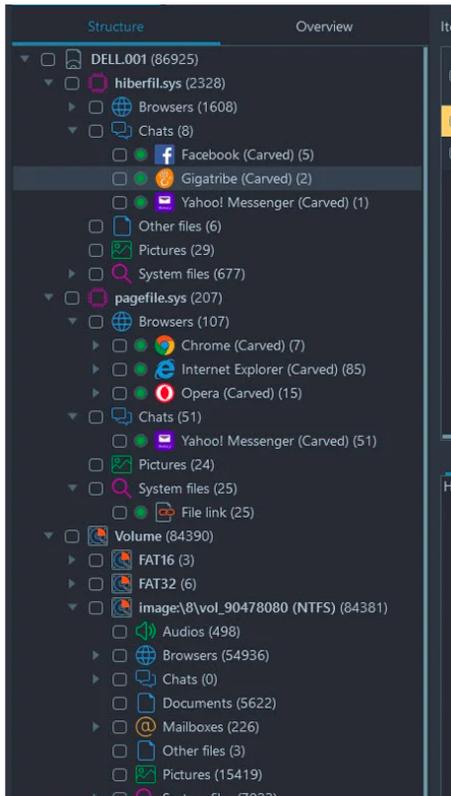


Figure 5: Artifacts sidebar

HERE'S THE THING

Data has overwhelmed us in just about every case. So much data. So many devices. So many artifacts. We need both automation and deep dives into data. Automation gives us speed in the identification of relevant artifacts, particularly when datasets are huge.

Belkasoft X does a really nice job of categorizing artifacts to quickly identify what artifacts exist, and from that, quickly determine which artifacts may be relevant to your analysis. Categorizing artifacts (Figure 5) is the new trend in forensics and is an effective method of analysis. Belkasoft X does this well.

Other time saving, automated, and amazing intuitive features are the mapping of geolocation data points (Figure 6) and the Connection Graph (Figure 7). With manual tools, the time required to dig out the artifacts needed (eg, geolocation data points), and putting the data into a visual display will take longer regardless of how smooth your process is. Belkasoft X does it with one click.

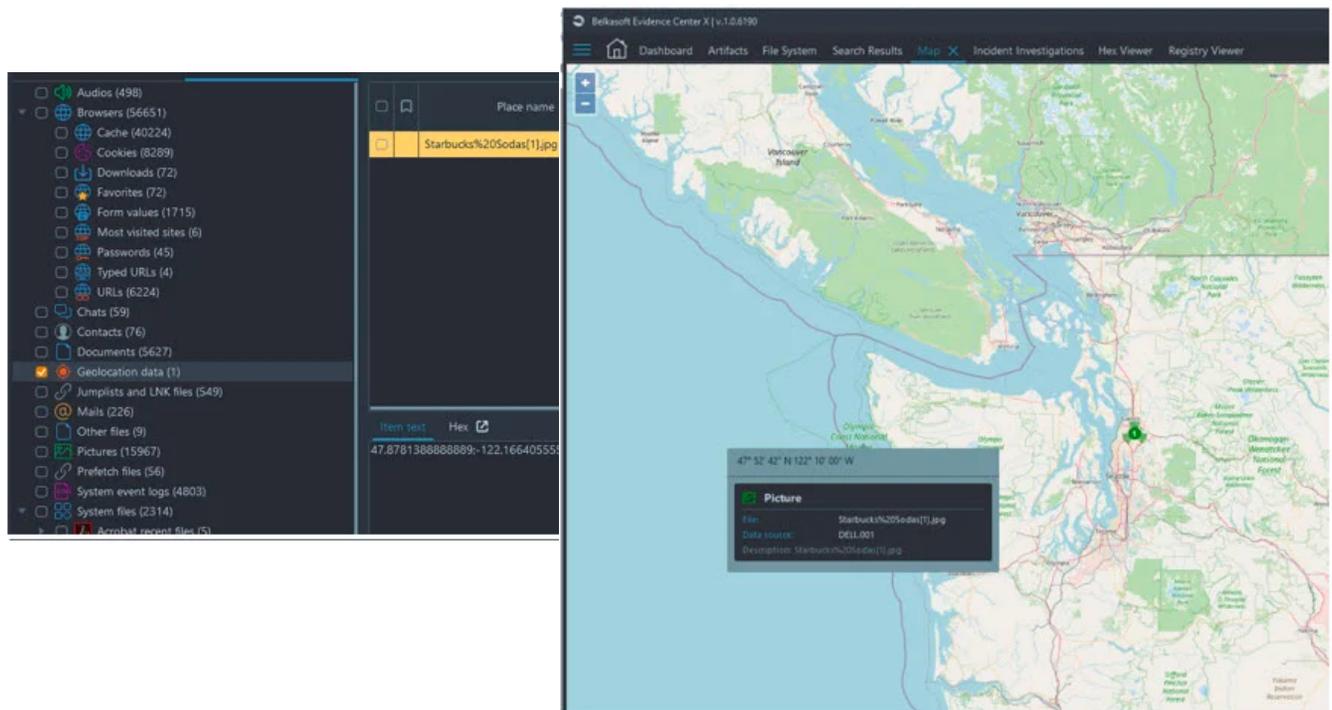


Figure 6: Map



Figure 7: Connection graph

Belkasoft is a trusted sponsor of DFIR Training. By trusted, I mean that Belkasoft's support is responsive, improvements are constant, and bugs are not ignored. I am confident to vouch for sponsors of DFIR Training when the products do as their marketing shows.

You can read the original Brett's post at

<https://www.dfir.training/dfir-training-blog/belkasoft-x>



702 San Conrado Terrace, Unit 1
Sunnyvale CA 94085 (USA)
+1 (650) 272-03-84

Try free at <https://belkasoft.com/trial>
30 days trial