Belkasoft Evidence Center X

“I cannot fault the Belka X suite. It is indeed easy to use and easy to become proficient. As the swiss army knife of DFIR products, Belkasoft Evidence Center does everything well and it will not break the bank!”

FRANCOIS H. PUTTER
DFIR expert and independent consultant, Deep Truth
South Africa 🇿🇦

ABOUT THE AUTHOR

My name is Francois H. Putter I have over 14 years of Cyber Security and Digital forensics experience where I applied my craft for our intelligence services as an IT Security adviser and cyber investigator. I have also served on one of the very first INTERPOL African working parties on Cyber Crime. For a few years now I am an independent consultant with a small DFIR lab called Deep Truth and is involved in both private, corporate, criminal and civil investigations.

You can contact me directly at deeptruthforensics@gmail.com or look me up on LinkedIn.

BACKGROUND TO THE REVIEW

I was requested to review Belkasoft’s new flagship DFIR product Belkasoft X and share my personal findings on its suitability for the South African market. I decided to install the freely available demo and put it through its paces. My findings are by no means an exhaustive summary but the basic highlights of the product and then of course a few issues that lies close to my heart which I found to be really helpful.

BELKASOFT X

I trust by now, like myself you have heard of Belkasoft Evidence Center since it recently also won a top three DFIR products of the 2020 Forensic 4:cast awards, beating the popular commercial tools currently widely in use by governments and auditing firms.

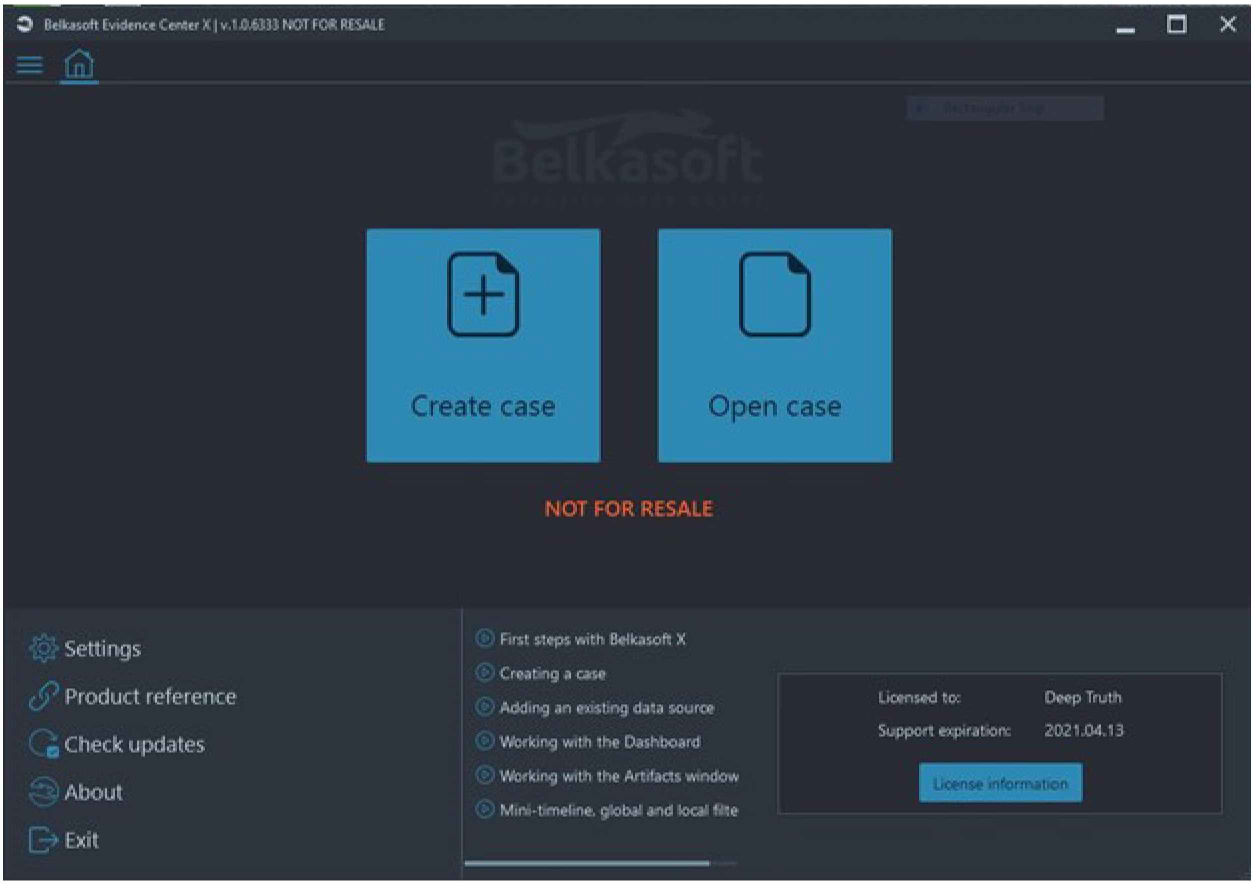
Belkasoft describes themselves as a global leader in developing advanced digital forensics software suitable for both the seasoned expert and novice alike. Belka X has an intuitive forensically workflow that will do:

- Data acquisition from various devices and clouds
- Artifact extraction and recovery
- Analysis of extracted data
- Reporting

Sharing evidence, the product supports the following types of digital forensics in a single user interface:

- Mobile forensics
- Computer forensics
- Memory (RAM) forensics
- Cloud forensics

Both high-level and low-level analysis can be done with Belkasoft X.



Belkasoft Evidence Center X | v.1.0.6333 NOT FOR RESALE

NOT FOR RESALE

Licensed to: Deep Truth

Support expiration: 2021.04.13

Create case
Open case
Settings
Product reference
Check updates
About
Exit
First steps with Belkasoft X
Creating a case
Adding an existing data source
Working with the Dashboard
Working with the Artifacts window
Mini-timeline, global and local filte
License information

My initial concern was that this product will require a huge learning curve to effectively use the Belka X suite and that training will be an non-negotiable extra expense in time and money. I have experienced this hidden cost with other commercial suites.

VALID CONCERN THEN?

The short answer is… No. It was easy! The short videos guided me to quickly get started and the clean design from the home screen onwards was really intuitive and straight forward.

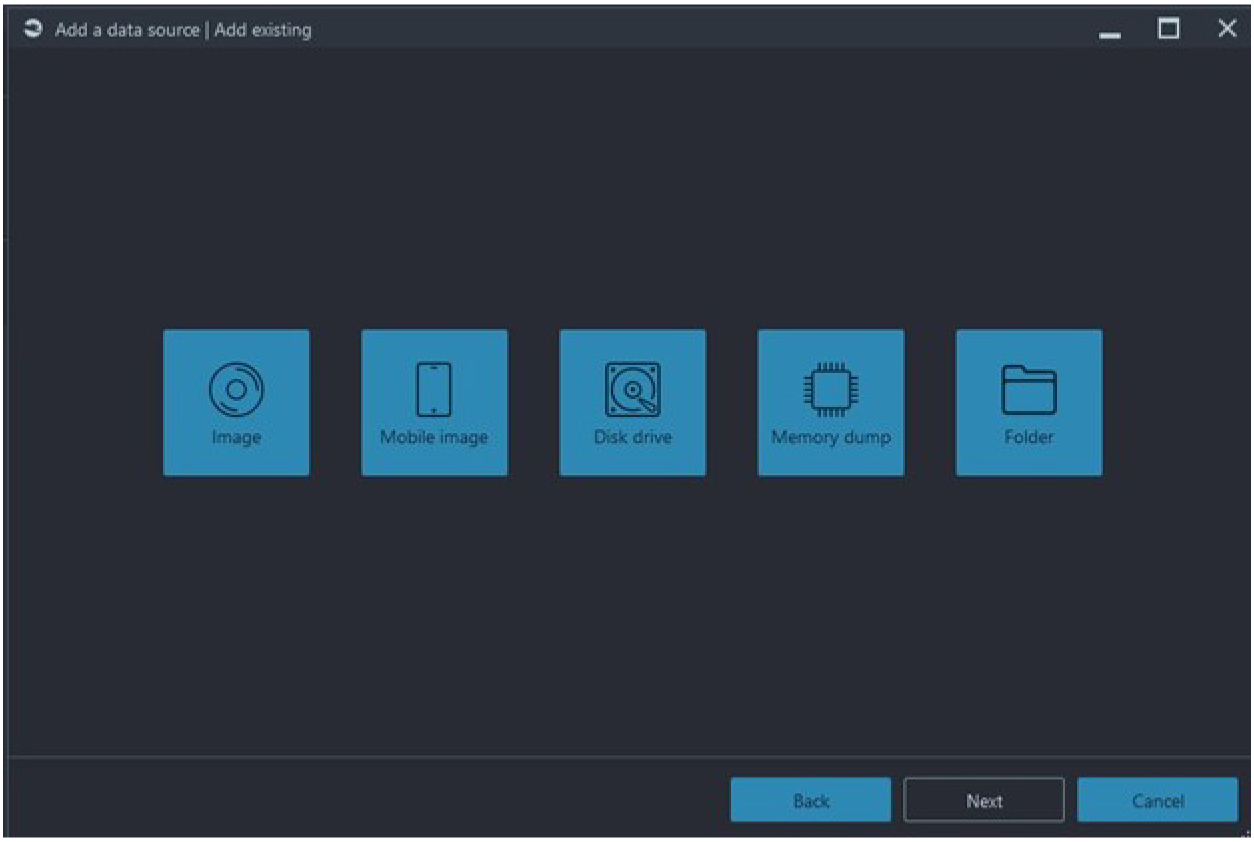
WAS IT TOO EASY?

Naturally my new concern was if it was so fast and easy to use will it truly satisfy my realistic and general technical requirements? Will I get the maximum data? Lastly, will it eventually fall short as a true all-round solution for myself and the ever cash strapped government within Southern Africa?

I will try to answer that question at the end of this review.

Here is a few of my highlights which I personally liked about Belka X.

DATA SOURCES AND ACQUISITION



By scanning the screenshot above you see that as claimed they do integrated mobile data acquisition. Belkasoft also makes sure its customers know they were the first to commercially enable the iOS acquisition of locked iPhones through the checkm8 vulnerability.

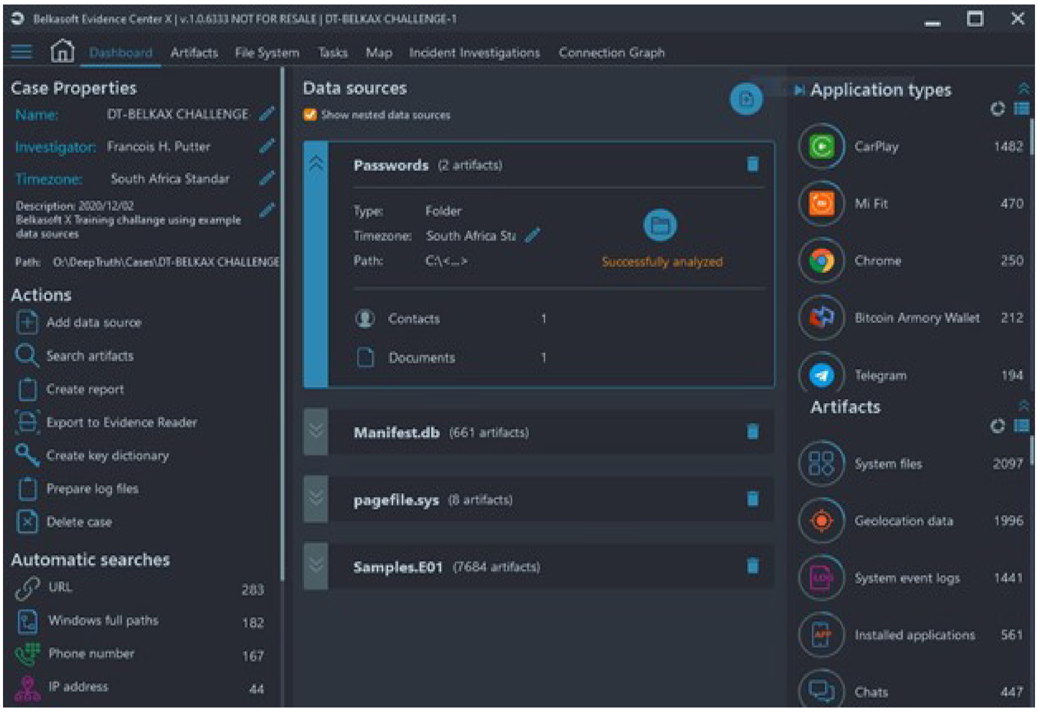
My tests on this aspect found that it works extremely well and not as I initially expected to be a marketing gimmick or afterthought. This in my eyes holds major advantages for the cash strapped consumer. No more investing in an additional mobile solution, it all gets represented for investigation and reporting in the same suite.

Once you have acquired your data source you can now choose your setting from a quick triage to an in-depth exhaustive carving looking at everything from slack space deleted data to passwords and artifacts. Triage for quick eDiscovery is a useful function saving time.

Once all triaging, carving and indexing is done, all the findings is presented in your dashboard screen from where you can go directly to your artifacts beautifully categorized for you. Detailed artifact findings can be listed under the Artifacts and File System menu items. For the old school purists and Hex lovers each data source can be traced to its basic binary source.

I cannot mention artifacts if I don't mention that I have discovered that encrypted files are not merely identified but the suite has a built-in capabilities to crack passwords, no more buying expensive third party suites! It's all included. I for one is going to save money on this capability.

Simple presentation of results on the **Dashboard**:


Belkasoft Evidence Center X | v.1.0.6333 NOT FOR RESALE | DT-BELKAX CHALLENGE-1
Dashboard
Artifacts
File System
Tasks
Map
Incident Investigations
Connection Graph

Case Properties

Name: DT-BELKAX CHALLENGE
Investigator: Francois H. Putter
Timezone: South Africa Standar
Description: 2020/12/02
Belkasoft X Training challange using example data sources
Path: O:\DeepTruth\Cases\DT-BELKAX CHALLENGE

Actions

Automatic searches

URL	283
Windows full paths	182
Phone number	167
IP address	44

Data sources

☑ Show nested data sources

Passwords (2 artifacts)

Type: Folder
Timezone: South Africa Sta
Path: C:\<...>

Successfully analyzed

Contacts	1
Documents	1

Manifest.db (661 artifacts)

pagefile.sys (8 artifacts)

Samples.E01 (7684 artifacts)

Application types

CarPlay	1482
Mi Fit	470
Chrome	250
Bitcoin Armory Wallet	212
Telegram	194

Artifacts

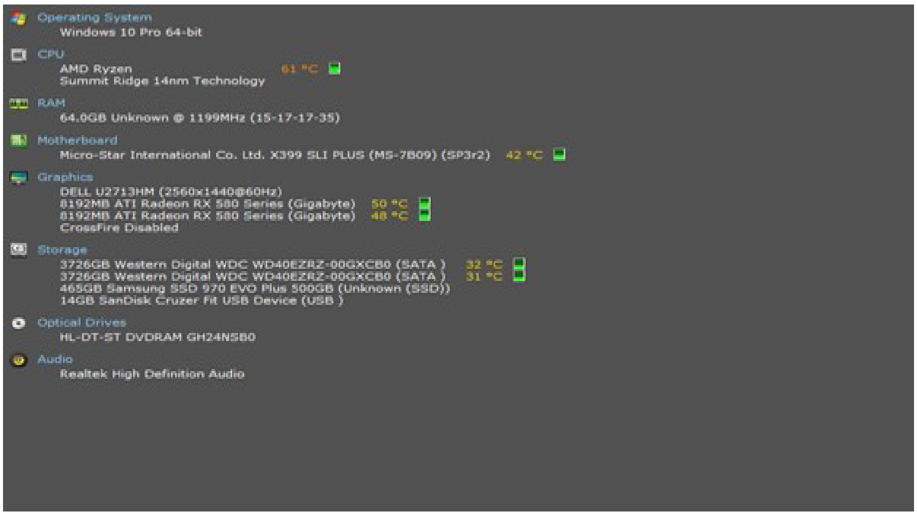
System files	2097
Geolocation data	1996
System event logs	1441
Installed applications	561
Chats	447

The results are all captured under the Dashboard menu function.

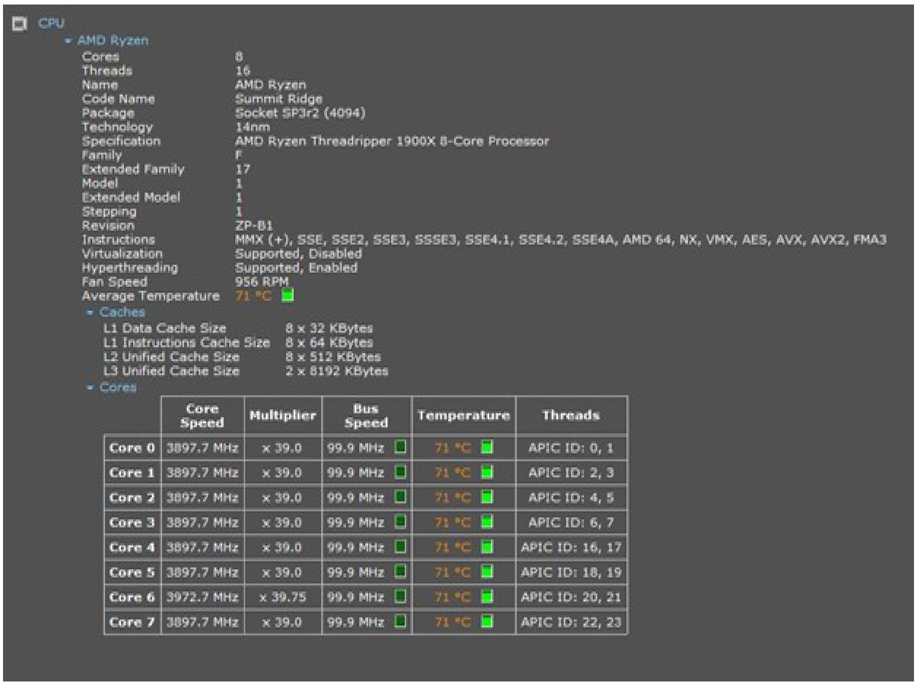
SPEED & HARDWARE CHALLENGES

I ran various tests and settings on various data sources and not once did my lab computer froze or bombed out and I was able to do some additional unrelated work while the lab PC was carving and indexing. This is a personal issue for me since I did not have the same smooth experience with 2 of the other major suites on the same setup.

For those interested with my setup:



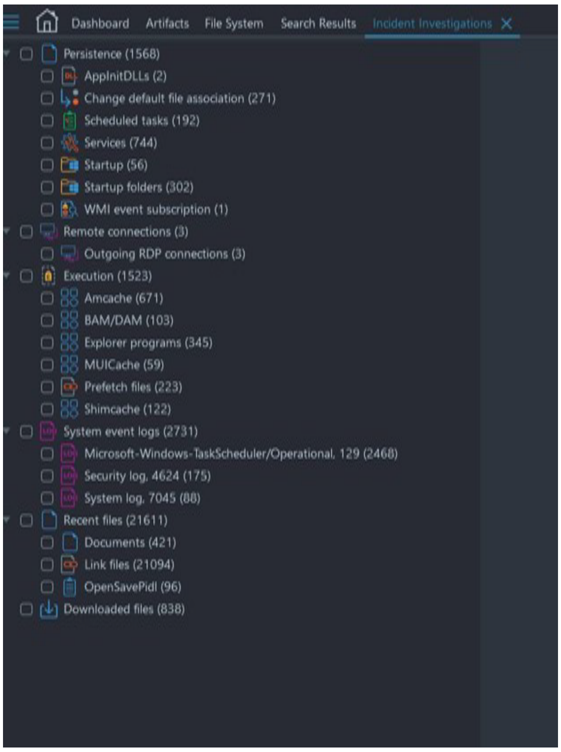
```
Operating System
    Windows 10 Pro 64-bit
CPU
    AMD Ryzen                                61 °C 🟩
    Summit Ridge 14nm Technology
RAM
    64.0GB Unknown @ 1199MHz (15-17-17-35)
Motherboard
    Micro-Star International Co. Ltd. X399 SLI PLUS (MS-7B09) (SP3r2)   42 °C 🟩
Graphics
    DELL U2713HM (2560x1440@60Hz)
    8192MB ATI Radeon RX 580 Series (Gigabyte)   50 °C 🟩
    8192MB ATI Radeon RX 580 Series (Gigabyte)   48 °C 🟩
    CrossFire Disabled
Storage
    3726GB Western Digital WDC WD40EZRZ-00GXCB0 (SATA )   32 °C 🟩
    3726GB Western Digital WDC WD40EZRZ-00GXCB0 (SATA )   31 °C 🟩
    465GB Samsung SSD 970 EVO Plus 500GB (Unknown (SSD))
    14GB SanDisk Cruzer Fit USB Device (USB )
Optical Drives
    HL-DT-ST DVDRAM GH24NSB0
Audio
    Realtek High Definition Audio
```



```
CPU
  ▾ AMD Ryzen
      Cores                   8
      Threads                 16
      Name                    AMD Ryzen
      Code Name               Summit Ridge
      Package                 Socket SP3r2 (4094)
      Technology              14nm
      Specification           AMD Ryzen Threadripper 1900X 8-Core Processor
      Family                  F
      Extended Family         17
      Model                   1
      Extended Model          1
      Stepping                1
      Revision                ZP-B1
      Instructions            MMX (+), SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2, SSE4A, AMD 64, NX, VMX, AES, AVX, AVX2, FMA3
      Virtualization          Supported, Disabled
      Hyperthreading          Supported, Enabled
      Fan Speed               956 RPM
      Average Temperature     71 °C 🟩
    ▾ Caches
        L1 Data Cache Size           8 x 32 KBytes
        L1 Instructions Cache Size   8 x 64 KBytes
        L2 Unified Cache Size        8 x 512 KBytes
        L3 Unified Cache Size        2 x 8192 KBytes
    ▾ Cores
```

	Core Speed	Multiplier	Bus Speed	Temperature	Threads
Core 0	3897.7 MHz	x 39.0	99.9 MHz 🟩	71 °C 🟩	APIC ID: 0, 1
Core 1	3897.7 MHz	x 39.0	99.9 MHz 🟩	71 °C 🟩	APIC ID: 2, 3
Core 2	3897.7 MHz	x 39.0	99.9 MHz 🟩	71 °C 🟩	APIC ID: 4, 5
Core 3	3897.7 MHz	x 39.0	99.9 MHz 🟩	71 °C 🟩	APIC ID: 6, 7
Core 4	3897.7 MHz	x 39.0	99.9 MHz 🟩	71 °C 🟩	APIC ID: 16, 17
Core 5	3897.7 MHz	x 39.0	99.9 MHz 🟩	71 °C 🟩	APIC ID: 18, 19
Core 6	3972.7 MHz	x 39.75	99.9 MHz 🟩	71 °C 🟩	APIC ID: 20, 21
Core 7	3897.7 MHz	x 39.0	99.9 MHz 🟩	71 °C 🟩	APIC ID: 22, 23

As you can see its no slouch but by far not the expensive high-end computer required by other DFIR software vendors. Good news for the budget conscious DFIR lab.



- □ Persistence (1568)
  - □ AppInitDLLs (2)
  - □ Change default file association (271)
  - □ Scheduled tasks (192)
  - □ Services (744)
  - □ Startup (56)
  - □ Startup folders (302)
  - □ WMI event subscription (1)
- □ Remote connections (3)
  - □ Outgoing RDP connections (3)
- □ Execution (1523)
  - □ Amcache (671)
  - □ BAM/DAM (103)
  - □ Explorer programs (345)
  - □ MUICache (59)
  - □ Prefetch files (223)
  - □ Shimcache (122)
- □ System event logs (2731)
  - □ Microsoft-Windows-TaskScheduler/Operational, 129 (2468)
  - □ Security log, 4624 (175)
  - □ System log, 7045 (88)
- □ Recent files (21611)
  - □ Documents (421)
  - □ Link files (21094)
  - □ OpenSavePidl (96)
- □ Downloaded files (838)

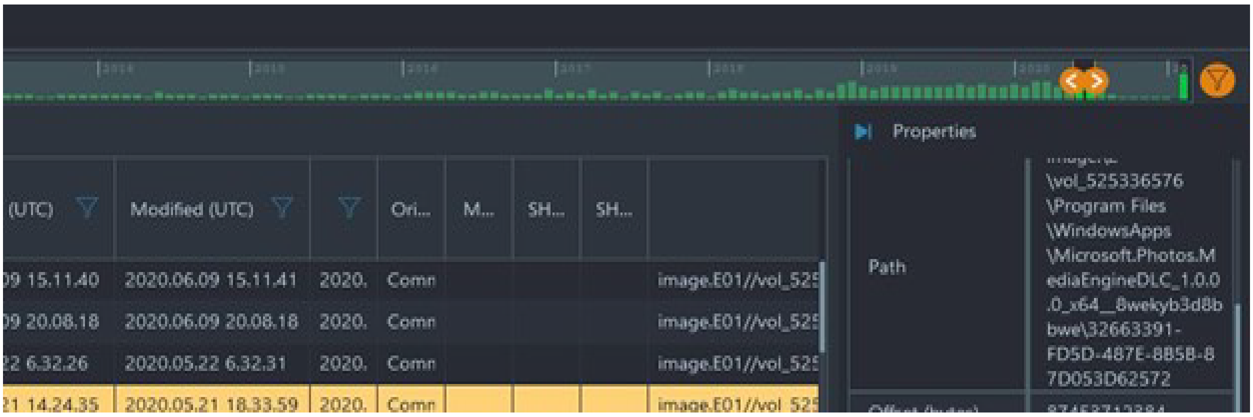
INCIDENT INVESTIGATION MODULE

A major improved factor is the Incident Investigations menu item. I can see its use for corporate and large organizations. I find it suited for hacking, ransomware and malware persistence root cause analysis.

This module is also useful for insider threat analysis and user behavior analysis especially with investigations where a user left the company to join a competitor.

SEARCHING

This bread-and-butter function of any investigation is assisted by intuitive built in custom search functions, manual search function which is also GREP enabled and the very useful timeline & mini timeline, this timeline search enables you to sift through massively less data if your searches are time specific.



(UTC)	Modified (UTC)		Ori...	M...	SH...	SH...	
09 15.11.40	2020.06.09 15.11.41	2020.	Comn				image.E01//vol_525
09 20.08.18	2020.06.09 20.08.18	2020.	Comn				image.E01//vol_525
22 6.32.26	2020.05.22 6.32.31	2020.	Comn				image.E01//vol_525
21 14.24.35	2020.05.21 18.33.59	2020.	Comn				image.E01//vol_525

Path	\vol_525336576 \Program Files \WindowsApps \Microsoft.Photos.MediaEngineDLC_1.0.0.0_x64__8wekyb3d8bbwe\32663391-FD5D-487E-8B5B-87D053D62572

MY FINDINGS IN A NUTSHELL

PROs	CONs
VALUE FOR MONEY: Up to 3 times more affordable than similar packages or the popular packages.	**CLOUD ACQUISITION:** My version of Belka X can acquire the major personal cloud providers such as Google, iCloud etc. But I feel this needs more work and is not a major selling point since my attempts in acquiring my personal clouds were not always successful.
ONE PACKAGE TO DO IT ALL: Seamless computer and mobile data source integration, HDD Decryption and Password detection and decryption.	**NO REMOTE OR AGENT BASED ACQUISITION:** With the worldwide pandemic we have seen an unprecedented need for remote workforce. Belka X would do well with such a module, I suspect it is in the making since this module used to be in previous versions.
FAST: Never freezes up my PC or hogging all resources.	**NOT MUCH**
INTUITIVE WORKFLOW: Easy to acquire, find and represent data.	
ARTIFACTS: Exhaustive list of artifacts from deleted files to SQLite apps such as WhatsApp and Telegram, Option to limit type of artifacts to find thus making the need like a e-discovery faster. IOS & Android acquisition and data presentation.	
SUITE CUSTOMIZATION & UPDATES: The standard Belka X suite has most of the functionality discussed or mentioned but suite customization makes it even more affordable if you omit certain features like decryption or mobile device functionality.	

As you can see its no slouch but by far not the expensive high-end computer required by other DFIR software vendors. Good news for the budget conscious DFIR lab.

AT THE END OF THE DAY

I tested this product for a month and I cannot fault the BelkaX suite. It is indeed easy to use and easy to become proficient. As the swiss army knife of DFIR products it does everything well and it will not break the bank!

My experience in government has taught me two things: a) Budget is always an issue & b) Obtaining and Retaining skills especially DFIR software skills is expensive and difficult. With a suite like BelkaX I feel Government and cash strapped DFIR labs will no longer need to buy multiple suites and the learning curve and training cost is significantly lower than with other products. I personally believe the type of candidate required to successfully use this suite can be now sourced from a wider pool in house or elsewhere and a IT Degree for instance is not necessary to use this product.