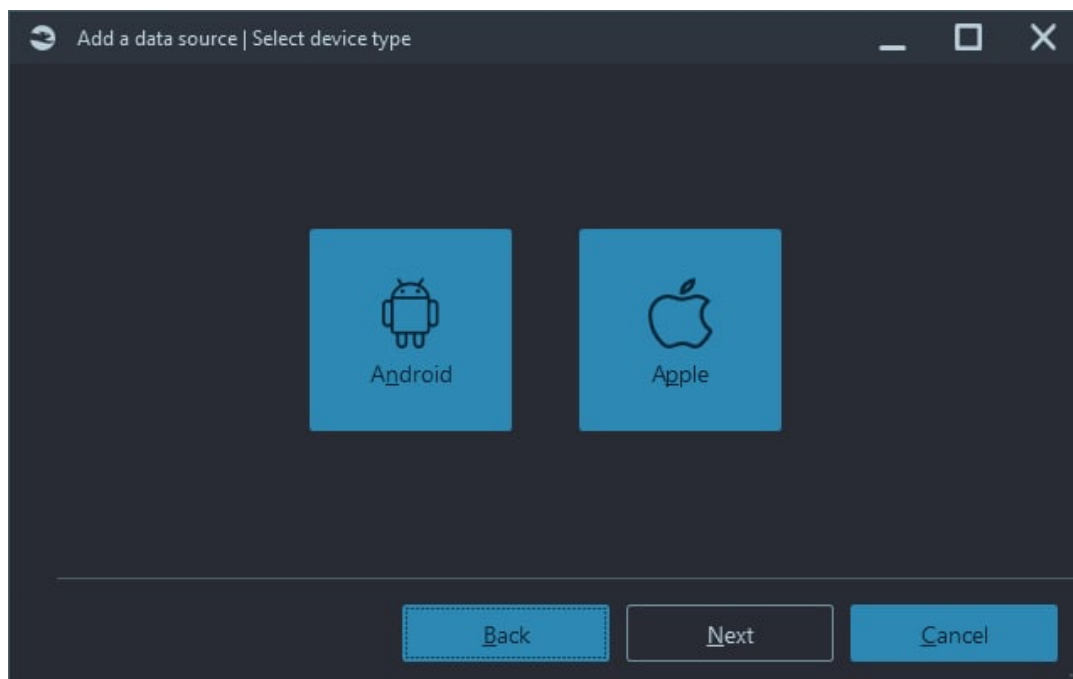


Why Belkasoft should be your tool of choice for Mobile Forensics

INTRODUCTION

Established more than 10 years ago, Belkasoft was mostly famous for its computer forensics tools. However, within the last few years, many [DFIR professionals began to choose](#) Belkasoft products specifically for our mobile acquisition and analysis functionality. Belkasoft, along with Cellebrite, was [one of the two first companies](#) in the world, which supported the Checkm8-based full file system iOS acquisition on a Windows platform—while most competitors were 6 to 12 months behind with this feature. This was just one of the reasons for the raising popularity of Belkasoft as a mobile forensic tool.

In this article we will describe the mobile forensics support that Belkasoft offers, and why Belkasoft products should be your tools of choice for working with mobile devices, whether in a digital forensic investigation or an incident response case.





Belkasoft X

[Belkasoft X](#) (Belkasoft Evidence Center X) is a flagship tool by Belkasoft for computer, mobile and cloud forensics. It can help you to acquire and analyze a wide range of mobile devices, run various analytical tasks, perform case-wide searches, bookmark artifacts, and create reports. A free trial of this tool is available at <https://belkasoft.com/trial>



Belkasoft R

[Belkasoft R](#) (Belkasoft Remote Acquisition) is a tool for forensically sound remote acquisitions of various types of devices, as well as partial images, including selected artifacts only (e.g. for compliance or eDiscovery needs). This product has a unique capability that allows for the acquisition of mobile devices remotely. A free trial of this tool is available at <https://belkasoft.com/trial>

Overview of Belkasoft's support for mobile forensics

One of the first steps—and the most important one—of working with a mobile device is data acquisition. If there is no data acquired, there is nothing to analyze. Belkasoft has sound support for acquisition of modern smart devices, including phones, tablets and even IoT devices.

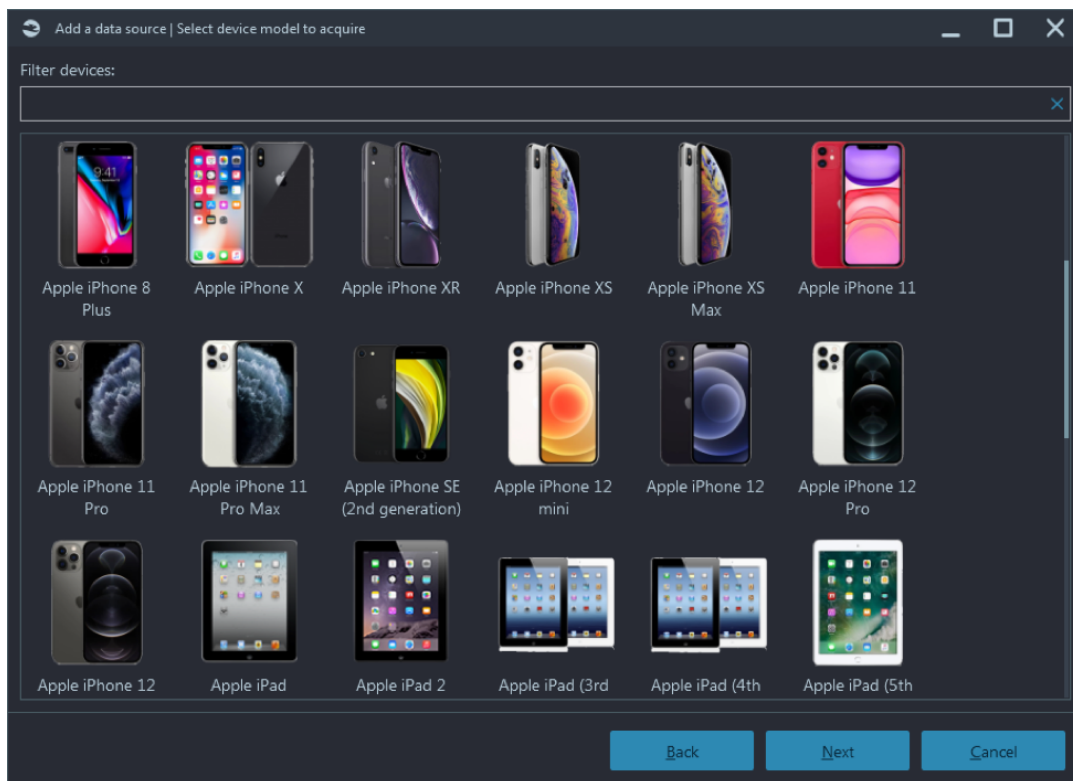
Belkasoft X supports multiple types of acquisitions for both of the most wide-spread platforms: iOS-based and Android-based devices. There is also support for Microsoft (Windows) phones, but since they are no longer produced, we will not review this support.

Both iOS and Android devices have their own peculiarities when it comes to data acquisition. There is a standard backup mechanism for both: iTunes for iOS and ADB for Android; Also, AFC and MTP/PTP protocols allow for media files extraction. Both iTunes and ADB are very limited in the volume of information available. And of course, most data can now be acquired with methods, which are not approved by device manufacturers, such as rooting, jailbreaks, exploits and so on. Many of these methods are device, or chipset-specific. This is why it is important to have multiple types of acquisition available to you. With that being said, it is important to [start with less intrusive methods](#), just to be on the safe side.

One of the great features within Belkasoft X, is that it allows you to start with the least intrusive and safest methods and continue with more comprehensive (but riskier) ones.

iOS acquisition support

For iOS, Belkasoft X supports the iTunes backup acquisition, including an interesting feature of using lockdown files to avoid unlocking the device in case a passcode is unknown. You can acquire media files with the Apple File Conduit (AFC) protocol.



More interestingly, a full file system and even the keychain (password built-in storage) can be acquired with the help of more sophisticated methods such as a jailbroken iPhone/iPad acquisition, [Checkm8-based acquisition](#) and even our [agent-based acquisition](#). To clarify, neither our Checkm8, or agent-based acquisition is a jailbreak, so they are much more forensically sound ways to acquire data—since in many countries it is legally impossible to perform a jailbreak on evidence.

Our Agent-based acquisition is just another [one of Belkasoft X's benefits](#), recognized by many customers. There are not many tools on the market which offer the same feature. It is a great complementary feature to Checkm8, since Checkm8 is limited in iOS device models (iOS devices with A5-A11 Chipsets), while agent-based acquisition works even on the latest iPhones, and the supported iOS range is huge, starting with an iOS as old as version 10.

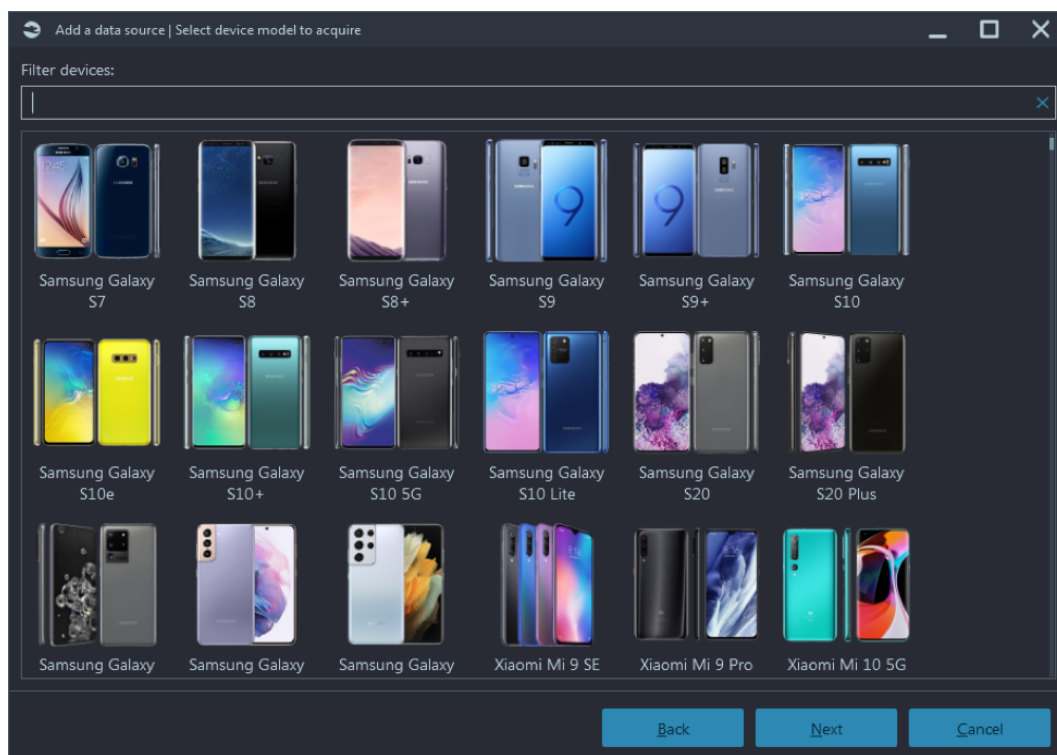
Speaking of Checkm8, Belkasoft X is adding something extra on top of competition. For example, it can [lift the so-called USB Restricted Mode](#)—a mode, which disables data transfer via a Lightning cable in one hour after the latest unlock.

There are more types of iOS acquisition such as crash log extraction, which, though limited, may give you some useful info such as latest IP addresses involved in your investigation.

To learn more on iOS acquisition with Belkasoft X, please watch our webinars available at <https://belkasoft.com/webinar>. Recorded webinars can be found on the Previous webinars tab, including [Locked iPhone investigations](#), [Bypassing iPhone USB Restricted Mode](#) and others.

Android acquisition support

For Androids, Belkasoft supports standard ADB backup creation and multiple types of acquisitions, based on ADB. One interesting method is our [APK downgrade acquisition](#), which replaces an original application file (e.g. WhatsApp) with an older version. Such older version can then be used with ADB backup creation and include much more data into our backup. Of course, at the end, the original app version is restored.



Another ADB-based method of Android acquisition by Belkasoft X, is [automated screen capturing](#). This is possibly the safest way to extract data from a device, so you may consider starting every case or acquisition with this method—before you try a riskier method.

Belkasoft X supports various Android acquisition methods, specific for particular vendors or chipsets. Among the supported methods, you will find Spreadtrum devices, MTK (MediaTek) and Qualcomm. For MTK, the product gives you as many as three different methods of acquisition, including two types of agent-based extraction and Qualcomm devices are supported via the EDL (Emergency Download) mode.

The product can also acquire rooted devices and analyze TWRP extractions. It supports analysis of JTAG images and chip-off dumps and can perfectly ingest third-party images, including forensic product images and proprietary vendor image files. For example, you can [analyze HiSuite backups](#)—as well as Xiaomi images—with the help of Belkasoft X.

To learn more on Android acquisitions within Belkasoft X, please watch our webinars available at <https://belkasoft.com/webinar>. Recorded webinars can be found on the Previous webinars tab, including [Android phones investigation: data extraction and analysis with Belkasoft X](#) and others.

Cloud forensics

Though cloud forensics is very much different from mobile forensics, performing these acquisitions can complement or corroborate data obtained from a mobile device. Since this is not the topic of this particular article, we will give two examples of useful functions in Belkasoft X, which can play a role in your mobile investigations:

- WhatsApp downloading (with or without a QR code). WhatsApp extraction is a challenging task, so every additional method you have available is priceless
- iCloud downloading. If you cannot obtain an iPhone acquisition, iCloud can be your source of data, backed up from that device to the Apple-hosted storage

Both options (as well as many others) are available within Belkasoft X, when you add a cloud-based data source to your case.

Mobile application analysis

You have now successfully imaged a device. **Congratulations!** Now you have to analyze the image contents.

There are millions of applications available for modern smartphone users and any automation of their analysis is indispensable to avoid growing case logs. Belkasoft supports more than 1500 types and version of the most popular applications, including WhatsApp, Signal, Telegram, Instagram, TikTok, [Viber](#), Tinder, Pinterest and many others.

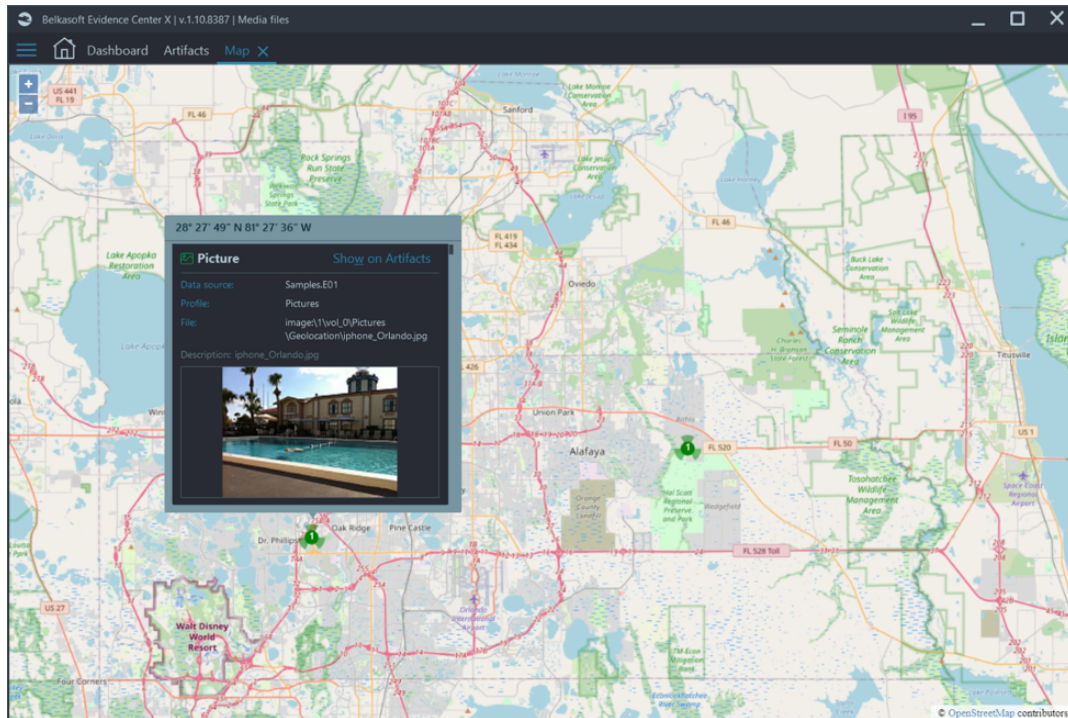
While most of these apps store data in a SQLite database ([this analysis is another story](#)), it is not as easy as open your favorite database browser to extract all the data. First, a standard freeware tool such as DB Browser for SQLite (and **even most forensic tools!**) will not recover deleted data located in freelists, or data from WAL (Write Ahead Logs) and journal files, as well as SQLite unallocated. Second, many apps use robust encryption to prevent an examiner from opening their databases without a decryption key.

Belkasoft X can [decrypt and decode multiple versions of WhatsApp](#)—and it is not necessary to have the phone rooted! You can use our APK downgrade method to extract the decryption key. iOS Signal messenger is another tough nut which [Belkasoft X can crack](#) once you have made a full file system extraction and captured the keychain (or if you have it from a third-party extraction). [Wickr Me is supported for both iOS and Android](#) platforms (as well as for computer operating systems).

In the user interface, Belkasoft X conveniently lays out various mobile (and other) artifacts, including audios, chats, documents, pictures and videos, geolocation data, cryptocurrency wallets and transactions, data from fitness trackers, sleep data, heart rate, etc.

Unlike the competition, which often allows you to have just one device in a case, you can add as many devices—whether mobile or computer—to your case. This helps you to obtain a 'birds eye view' via our Connection Graph—which will show [how different people from your case or from different devices, were communicating](#). Whether it was via chats, SMS, voicemail, or calls and email. Finally, you can make connections between your added datasets and no matter the type of device, a feature not supported by

competition. This can be tough and time-consuming manual work otherwise, to correlate data from a mobile device of one user with a laptop of another user, since you will have to work in two different software products, not necessarily talking to each other or supporting each other's formats.

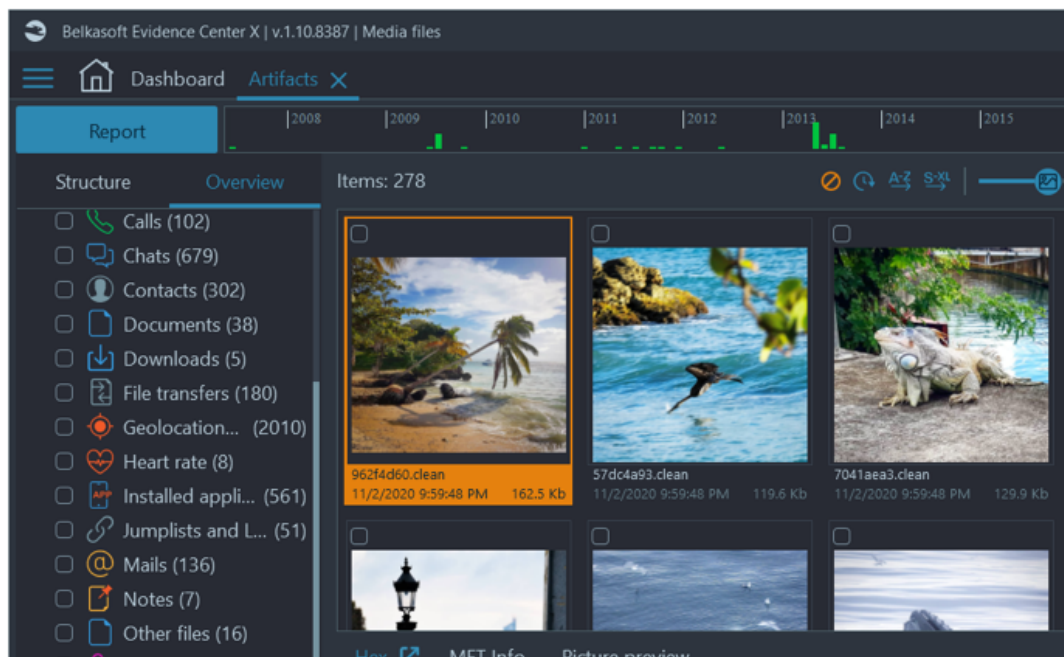


Reviewing geolocation data, such as photos made on a mobile device, with Belkasoft X's built-in Maps

Benefits of Belkasoft's solutions for mobile forensics

There are multiple reasons why Belkasoft is considered to be a tool of choice by a growing number of prominent digital forensic experts and incident responders. Among them are:

- Solid support of mobile device acquisition, including sophisticated methods such as Checkm8 and Agent-based acquisition
- Wide range of supported device models
- Forensically sound remote acquisition of mobile devices
- Huge number of mobile applications and artifacts supported out of the box by Belkasoft X
- Very affordable price: much less than any mobile forensic software by competitors



Ready to test Belkasoft?

If this article convinced you to try Belkasoft tools, you can download them from <https://belkasoft.com/trial>. The Belkasoft X installation contains sample image with both computer and mobile data.

Do you need a more sophisticated image to try? Solve our [BelkaCTF number 2](#) ('Drugdealer case'), devoted to an Android investigation. You will see the power of Belkasoft X for yourself: even the most difficult tasks can be solved with this tool in a matter of minutes.

If you do not have the time to dedicate to a full CTF, try to catch some of our [short BelkaTalk videos](#) where we answer difficult questions from across the community, some focused mainly in mobile forensics.

[Download Belkasoft X for your mobile investigations!](#)

See also:

- [Shafik Punja's review of Belkasoft X](#)
- [Types of mobile acquisition, supported by Belkasoft X](#)
- [Six steps for mobile validation](#)
- [Android APK downgrade acquisition method](#)
- [Android screen capturing method](#)
- [SQLite forensics](#) and why a free viewer is not enough
- [Analyzing HiSuite backups with Belkasoft](#)
- [iOS Signal messenger decryption](#)
- [Android Viber forensics](#)
- [How you can connect mobile data with computer data in your DFIR case?](#)
- [CTF: Investigate an Android device in a close-to-real-world case with Belkasoft X](#)
- [Webinar: iOS Locked iPhone investigations](#)
- [Webinar: Bypassing iPhone USB Restricted Mode](#)
- [Webinar: WhatsApp forensics](#)
- [Webinar: Android investigation](#)
- [Webinar: WickrMe forensics](#)
- [BelkaTalk on DFIR](#)
- [Belkasoft CTFs](#)

For more information contact us at
sales@belkasoft.com

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

702 San Conrado Terrace, Unit 1
Sunnyvale CA 94085
+1 310 625 9252 (USA)
<https://belkasoft.com>