



# Oxygen Forensic<sup>®</sup> **Detective**

**Release notes**

Version 15.3  
February 2023



The latest update to our flagship solution is here, Oxygen Forensic® **Detective** v.15.3! This version introduces the following key features:

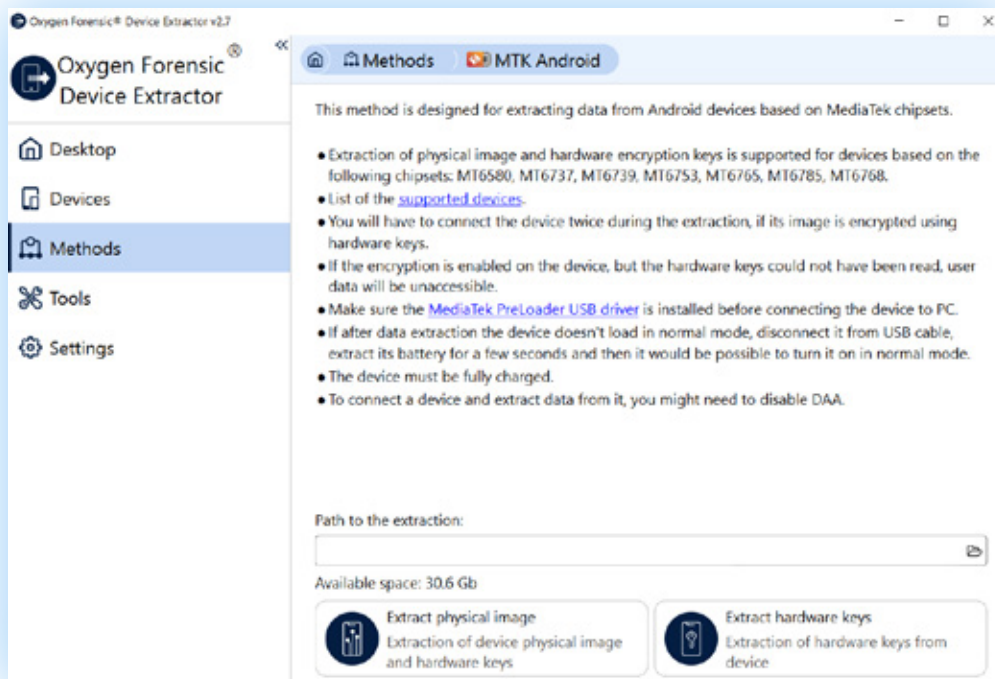
- Brute force for Samsung, Motorola and Huawei devices based on MTK chipsets
- Enhanced support for Huawei devices based on Qualcomm chipsets
- LastPass cloud extraction
- Import of Tinder archives
- Support for modified WhatsApp versions

For a full list of updates, refer to the “What’s New” file in the Oxygen Forensic® Detective “Options” menu.

## Mobile Forensic Updates

### Bruteforce for Samsung MTK devices

Users can now extract hardware keys and decrypt data from Samsung devices based on the Mediatek Helio G80 chipset and having TEE TEEGRIS. Our support covers devices running Android OS 10 and higher. Supported models include Samsung Galaxy A22 4G, Samsung Galaxy A32 4G, Samsung Galaxy F22, Samsung Galaxy M22, Samsung Galaxy M32, and others.



## Bruteforce for Huawei MTK devices

We've also added support for Huawei devices based on the MT6765 chipset, running Android OS 10, and having File-Based Encryption. Our support covers Honor 9A, Honor 9S, Huawei Y5p, and Huawei Y6p.

## Bruteforce for Motorola MTK devices

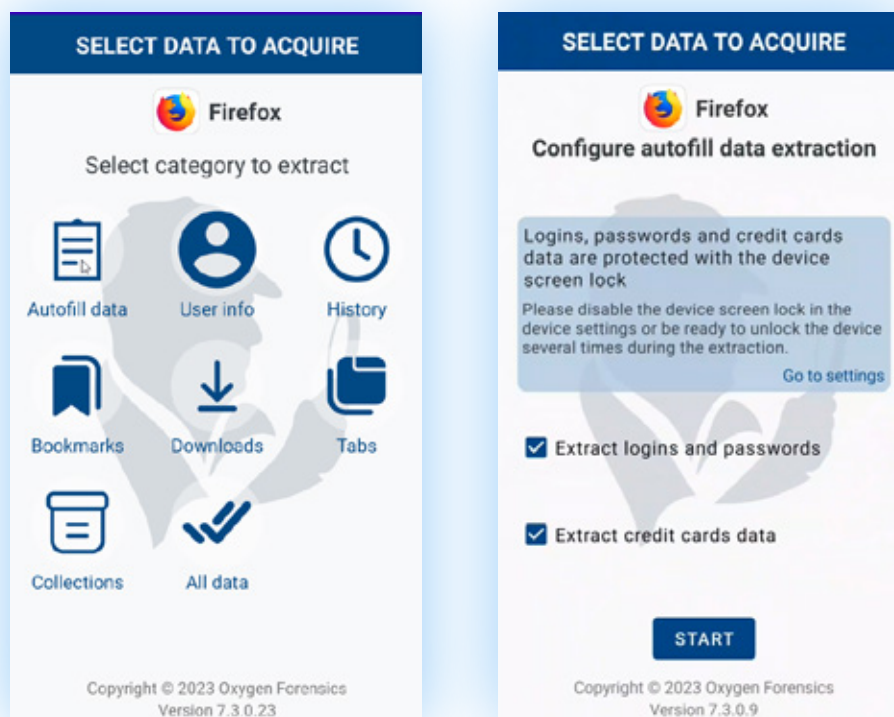
Now you can extract hardware keys and decrypt physical dumps of Motorola devices based on the MT6765 chipset, having File-Based Encryption and running Android OS 10-12. Our support covers Motorola Moto E7, Motorola Moto E7 Power, Motorola Moto G Pure, Motorola Moto E6s and Motorola Moto E6 Plus.

## Enhanced support for Huawei Qualcomm devices

Extraction and decryption of Huawei devices based on the Qualcomm SDM450 chipset has been added. Our support covers Huawei devices running Android OS 10 or higher. Supported models include Huawei Enjoy 9, Huawei Y7 2019, Huawei Y7 Pro 2019, and Huawei Y7 Prime 2019.

## Extraction of Firefox artifacts via Android Agent

Now users can extract even more Firefox artifacts via Android Agent: collections, logins and passwords, saved cards, and addresses. While collecting saved credentials and cards, the Android Agent will require that a user password be manually entered to allow the process to start.



## Extraction of Telegram groups via Android Agent

Recently, Telegram has introduced the ability to create group chats with enabled topics. With this release this type of chats can be collected via Android Agent from any supported Android devices. Selective topic extraction is available.

## iOS support updates

In Oxygen Forensic® Detective v.15.3 we've added two enhancements for iOS device support:

- We've added the ability to extract the full file system and keychain via iOS Agent from iOS devices running iOS versions 15.0 – 15.4.1. For these supported iOS versions, there is no need to authenticate an Apple ID account and obtain a certificate for signing iOS Agent.
- Users can now extract the full file system and keychain via checkm8 from Apple iOS devices based on the A10 chipset and running iOS 14 and 15 without disabling the screen lock.

## App support

In Oxygen Forensic® Detective v.15.3 we've added support for the following new apps:

- BOTIM (Apple, Android)
- GB WhatsApp (Android)
- OB WhatsApp (Android)
- FM WhatsApp (Android)
- Microsoft Bing (Android)
- BeReal (Apple)
- Moj (Apple)
- Tiki (Apple)

The total number of supported app versions now exceeds 34,800.

# Import Updates

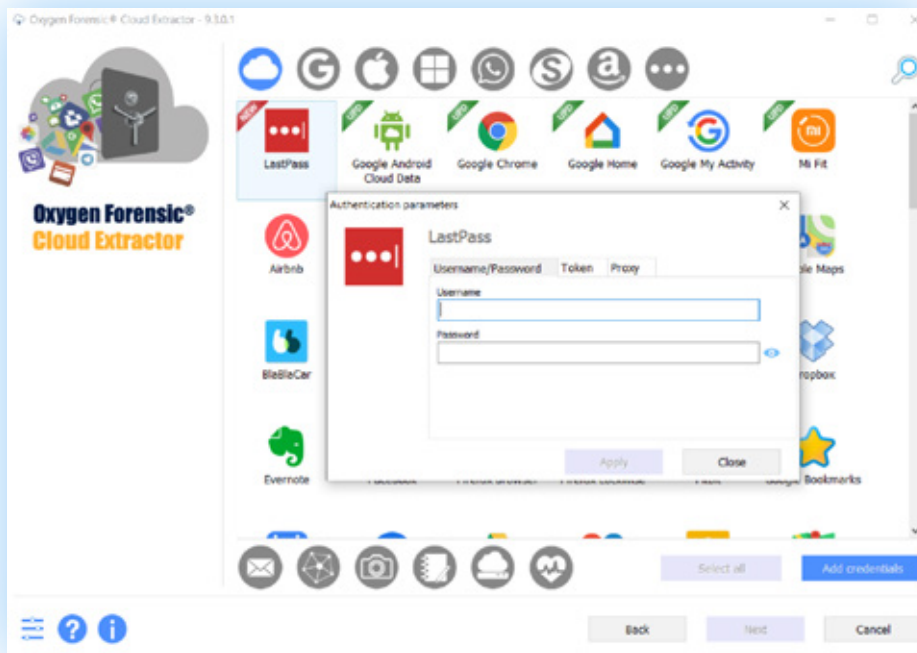
## Import of Tinder archives

In this release, users can import and parse evidence from Tinder archives. Click the Tinder archive option under the Downloaded accounts data on the Home software screen to import Tinder data. Evidence set will contain media files, messages, used apps, campaigns, purchases, Spotify artifacts, and other supported artifacts.

# Cloud Forensic Updates

## LastPass data extraction

Oxygen Forensic® Detective v.15.3 allows cloud extraction from LastPass, one of the most popular password managers. Extraction is possible via login and password or token. Evidence set will include passwords, documents, notes, and bank card details.



## Other updates

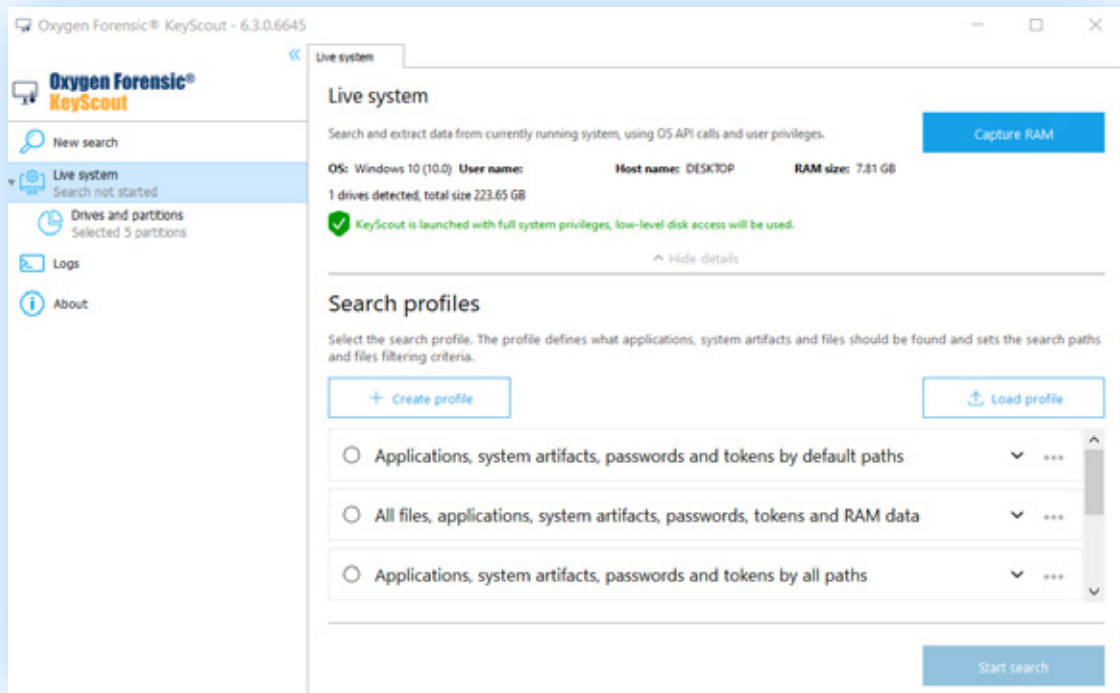
Authorization and extraction algorithms for already supported cloud services was updated – Google Home, Google Chrome, Google My Activity, MiFit, Android Cloud Data, and Huawei.

# Computer Artifacts

## Functionality updates

A number of functional and interface updates to KeyScout were introduced:

- Added extended analysis of live RAM that now includes memory pages from pagefiles
- More detailed information about data search progress
- Redesigned and simplified the work with search profiles



## New and updated artifacts

With the updated Oxygen Forensic® KeyScout, users can collect the following new artifacts:

- Background Intelligent Transfer Service (BITS) on Windows
- Diagnostic data from Windows
- Information about running processes on macOS and Linux during live system extraction
- ARP cache on macOS and Linux during live system extraction
- Dock elements from macOS
- History of commands entered in the terminal on Linux
- History of app usage on Linux
- History of Vim usage on Linux
- Brave data from Windows, macOS, and Linux

Updated artifact support includes:

- Microsoft Teams data on Windows
- Microsoft Exchange Server data on Windows
- Viber data on Windows, macOS, and Linux
- Apple Messages data on macOS

## Questions?

Contact [support@oxygen-forensic.com](mailto:support@oxygen-forensic.com)