OXYGEN FORENSICS

Oxygen Forensic® DETECTIVE

Release notes

Version 15.0 | September 2022

A new version of our flagship software is available, Oxygen Forensic® Detective v.15.0. This version introduces the following key features:

- Screen lock bypass for Xiaomi devices
- Android Keystore extraction from Qualcomm-based Huawei devices
- Semantic Location History parsing from Google Takeout
- New tool for calls and messages analysis
- Facial Categorization enhancements

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

Mobile Forensic Updates

Screen lock bypass for Xiaomi devices

In Oxygen Forensic® Detective v.15.0, we extend our support for Xiaomi devices with File-Based Encryption (FBE) by adding two more MTK chipsets: Helio G88 (MT6768) and Helio G90T (MT6785).

Oxygen Forensic® Detective extracts hardware keys and allows you to either enter the known password or to find it with the built-in brute force module.

Supported devices include Xiaomi Redmi 10 Prime 2022, Xiaomi Redmi 10 Global, Xiaomi Redmi 10 Prime, and Xiaomi Redmi Note 8 Pro.

Android Keystore extraction from Qualcomm-based Huawei devices

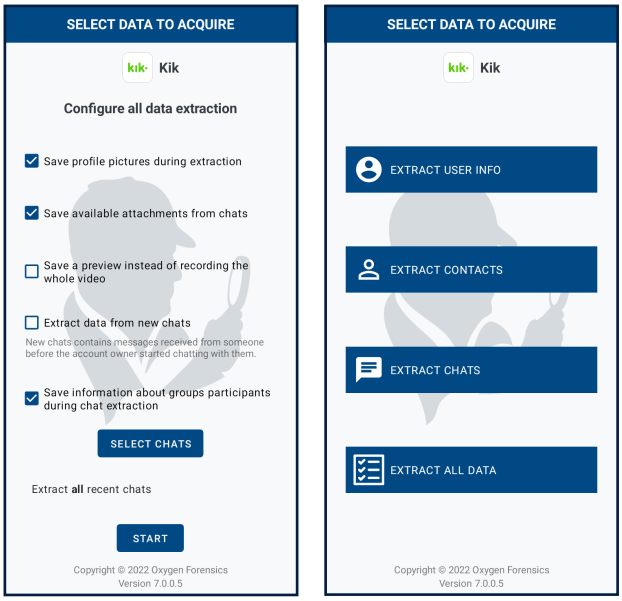
We've added the ability to extract encryption keys from the Android Keystore from Huawei devices based on the Qualcomm chipsets: MSM8917, MSM8937, and MSM8940.

To use this functionality, select the Huawei Qualcomm EDL method in the Oxygen Forensic® Device Extractor. With the extracted encryption keys, Oxygen Forensic® Detective can currently decrypt ProtonMail, Silent Phone, and Signal apps.

Kik Messenger extraction via Android Agent

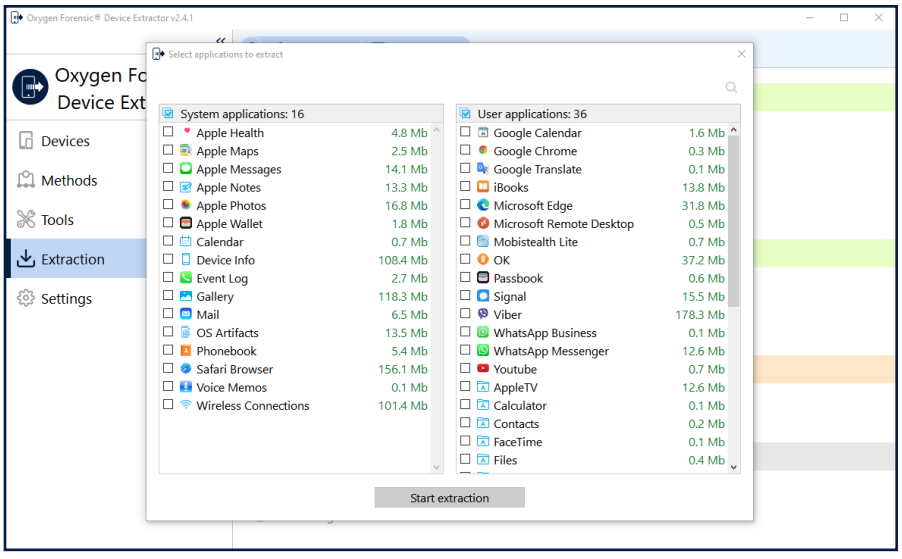
Now you can quickly collect Kik Messenger contacts as well as private and group chats from any unlocked Android device using Android Agent. It can be installed on a device via USB, WiFi, or OTG device.

Once the acquisition process is finished, the Android Agent extraction can be imported into Oxygen Forensic® Detective for review and analysis.



iOS selective extraction

We've enhanced the ability to selectively extract evidence from Apple iOS devices. Previously, only selective extraction was available for the 30 most popular apps. Now you can choose any installed app for extraction. This feature is available for the checkm8, SSH, and iOS Agent extraction methods.



Redesigned SIM card extraction

In this software version, we've redesigned the SIM Card extraction method and now it is available in the new Oxygen Forensic® Device Extractor.

App support

In Oxygen Forensic® Detective v.15.0, we've added support for the following new apps:

- Temp Mail (iOS, Android)
- Phone by Google (Android)
- Huawei Notes (Android)
- Calculator# (iOS)
- Calculator+ (iOS)
- Bigo Live (iOS)

The total number of supported app versions exceeds 33800.

Cloud Forensic Updates

Updated support

We've completely redesigned our support for Box, a popular file sharing service. Now many new artifacts can be extracted:

- Contacts
- Collections
- Tasks
- Notifications
- Notes
- Sessions
- Comments to files and notes

We've also updated the authorization algorithm for OnlyFans. Now the lists that the account owner follows can be extracted from Twitter.

Computer Artifacts

KeyScout updates

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

- list of network connections from volatile memory (Windows)
- list of loaded modules from volatile memory (Windows)
- list of open files from volatile memory (Windows)
- CryptnetURLCache (Windows)
- WMI persistence (Windows)
- Stage Manager (macOS 13)

Updated artifact support includes:

- Microsoft Edge (Windows)
- Tor Browser (Windows, macOS, and Linux)
- Calendar, Reminders, Notes, System Events, User Activity (macOS13)

Data Import

Brute force for Oppo device extractions

Passcode brute force is now available for extractions of Oppo devices based on the MT6765 chipset and having File-Based Encryption. Supported device models include: Oppo A16, Oppo A16s, and Oppo A16K.

Semantic Location History parsing

There are two sources of location data in a Google Takeout: Location History file and Semantic Location History files created for every month.

Semantic Location History data can now be fully parsed by Oxygen Forensic® Detective when the Google Takeout file is imported. Semantic Location History files contain detailed information about the account owner's visited locations and journeys.

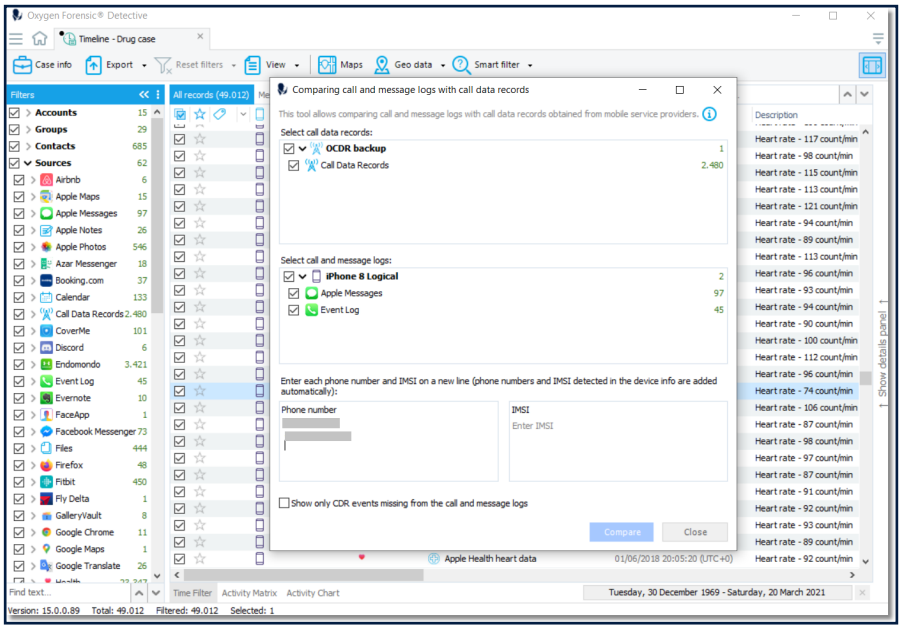
Data Analysis

Comparison of call and message logs with CDR

Oxygen Forensic® Detective v.15.0 presents a new analysis tool – the ability to compare call and message logs extracted from a device with Call Data Records provided by mobile service providers.

This feature is useful in situations when calls or messages have been manually deleted from a device. Using this comparison tool, you can fill in the gaps and see the complete picture.

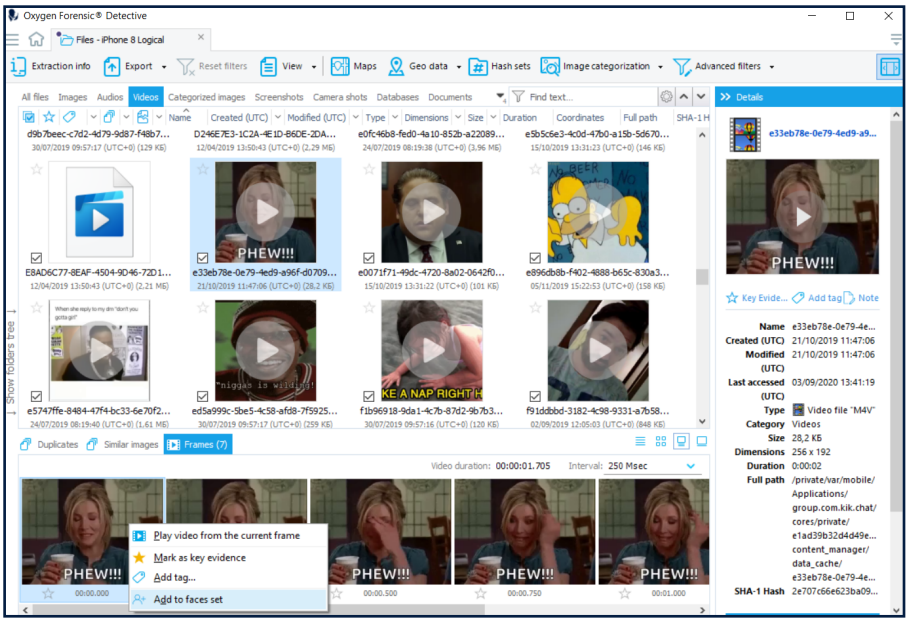
To perform the comparison, go to the Timeline section and select the “Compare call and message logs with call data records” option in the Smart Filters. Once you select the devices and CDRs for comparison, the software will show you calls and messages in one list, in chronological order.



Facial Categorization updates

We’ve added two enhancements:

- In the Files section you can add a face from a video frame to a face set that can be used to search faces in extracted evidence.
- We’ve added a multi-thread facial categorization using both CPU and GPU. You can choose a number of threads on the Advanced analytics tab in the software Options menu.



Search in file metadata

You can now run search in file metadata on the Text, Keywords, and RegExp tabs of the Search section. This option is also included in search templates.

Resolved Issues

- Error while trying to export realm db section
- Import freezes during Thunderbird parsing (Windows)
- Issues with iPhone XS and XR extraction via iOS Agent
- Xiaomi Redmi 9C MediaTek MT6765G Helio G3 was extracted but not decrypted
- .odb temporary files were not deleted from a temporary folder
- AV error on opening the Plist Viewer