OXYGEN FORENSICS

Oxygen Forensic® DETECTIVE

Release notes

Version 14.5 | June 2022

We present the latest update of our flagship software, Oxygen Forensic® Detective, v.14.5! This version introduces support for:

- Oppo and Realme devices
- Facebook account copy
- Data extraction via iOS Agent
- Silent Phone extraction via OxyAgent
- Getting addresses from extracted geo coordinates

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

Mobile Forensics

Extraction of Oppo and Realme devices

All the recent Android devices that are based on MTK chipsets have File-Based Encryption (FBE). FBE is implemented on all the MTK devices that have pre-installed Android OS 10 or higher.

Oxygen Forensic® Detective v.14.5 introduces the ability to extract and decrypt data with the known password from Oppo and Realme devices based on the Helio G35 (MT6765) chipset and having FBE (File-Based Encryption).

Our support covers Realme C11 2020 (Helio G35), Realme C12, Realme C15 (MediaTek), Realme C20, Realme C20A, Realme C21, OPPO A16, OPPO A16K, OPPO A16s, OPPO A54s, and OPPO A55 4G.

Data extraction via iOS Agent

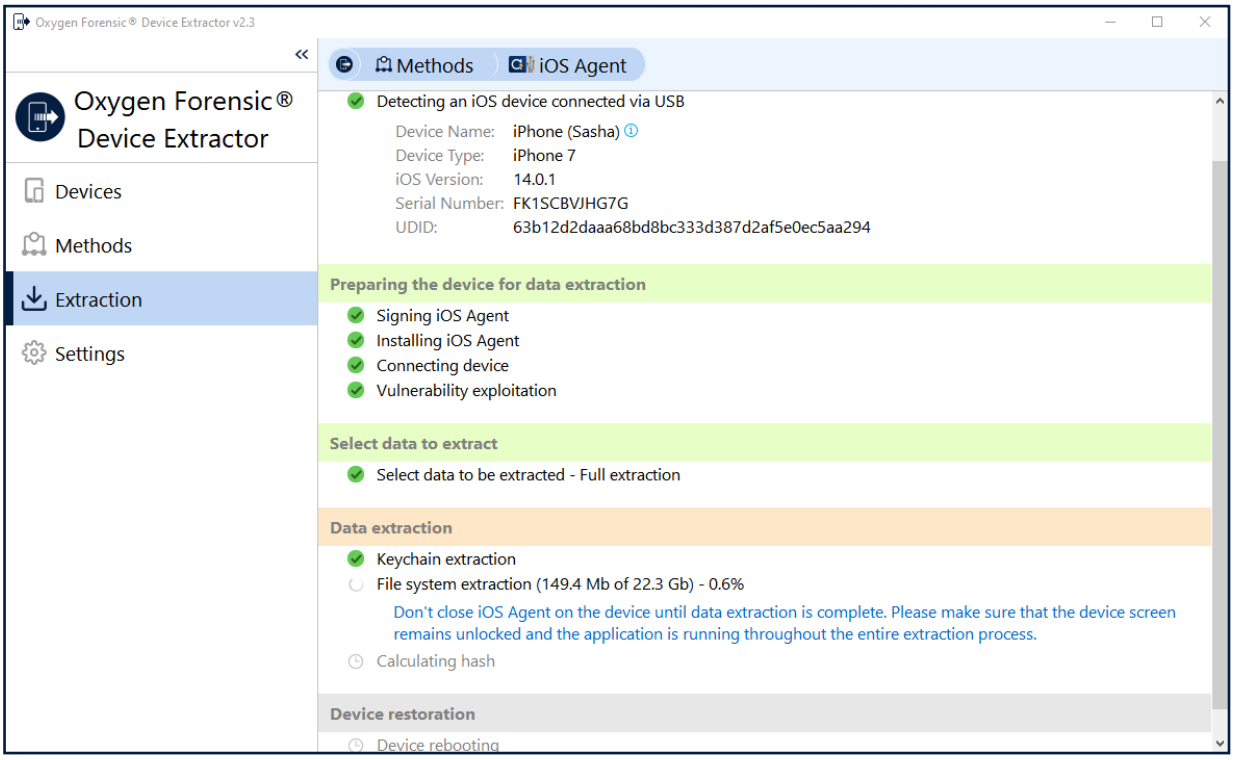
Oxygen Forensic® Detective v.14.5 introduces a new method of iOS device extraction. Now, data can be extracted using the iOS Agent utility. This method is compatible with iOS devices running versions 14.0-14.3.

The list of supported models includes iPhone 12, iPhone 11, iPhone SE (2020), iPhone XS, iPhone 8, iPhone 7, iPhone 6, iPad Pro (4th generation), iPad Air, and many others.

Oxygen Forensic® Extractor will guide you through the process of iOS Agent installation. Once the Agent is installed, you can choose to extract all or selected data.

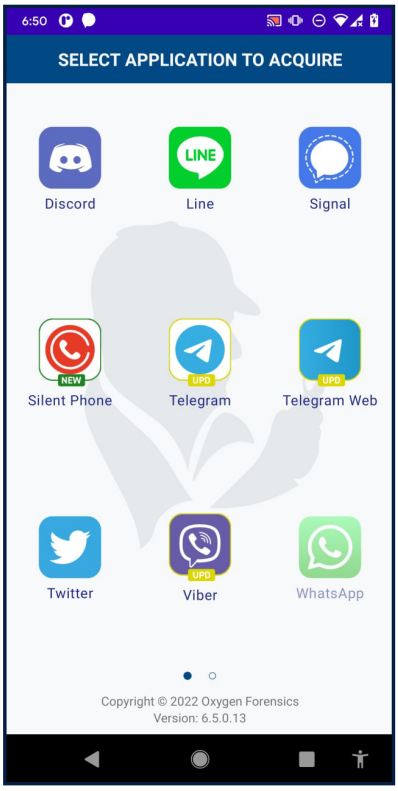
This is the 4th extraction method for iOS devices that is available in our software.

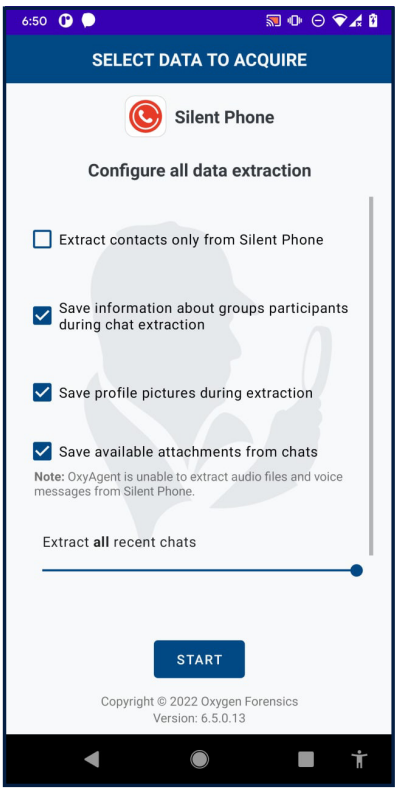
- Unlike the iTunes procedure, this method will extract more evidence, including keychain, system data, and apps.
- The checkm8 method is limited to the device models. The iOS Agent approach, on the contrary, covers more device models but is currently limited to the iOS version. We will add more versions in future releases.
- Unlike the jailbreak methods, the iOS Agent method does not modify the file system.



Silent Phone extraction via OxyAgent

Silent Phone app offers secure calls and messages. Previously, this app data could be extracted from Apple iOS and Android devices using the standard extraction methods. Now, you can also quickly collect contacts as well as private and group chats from any unlocked Android device using OxyAgent. OxyAgent can be installed on a device via USB, WiFi, or OTG device. Once the acquisition process is finished, the OxyAgent extraction can be imported into Oxygen Forensic® Detective for review and analysis.





Selective chat extraction via OxyAgent

We've added selective chat extraction from Telegram and Viber apps via OxyAgent. Please note that Telegram may have multiple accounts, and you can choose to extract all of them or selected ones.

App support

Investigators can now extract evidence from the following new apps:

- Google Chat
- Google Voice
- Twitch
- Zenly
- DingTalk
- Email.cz

The total number of supported app versions now exceeds 30,800.

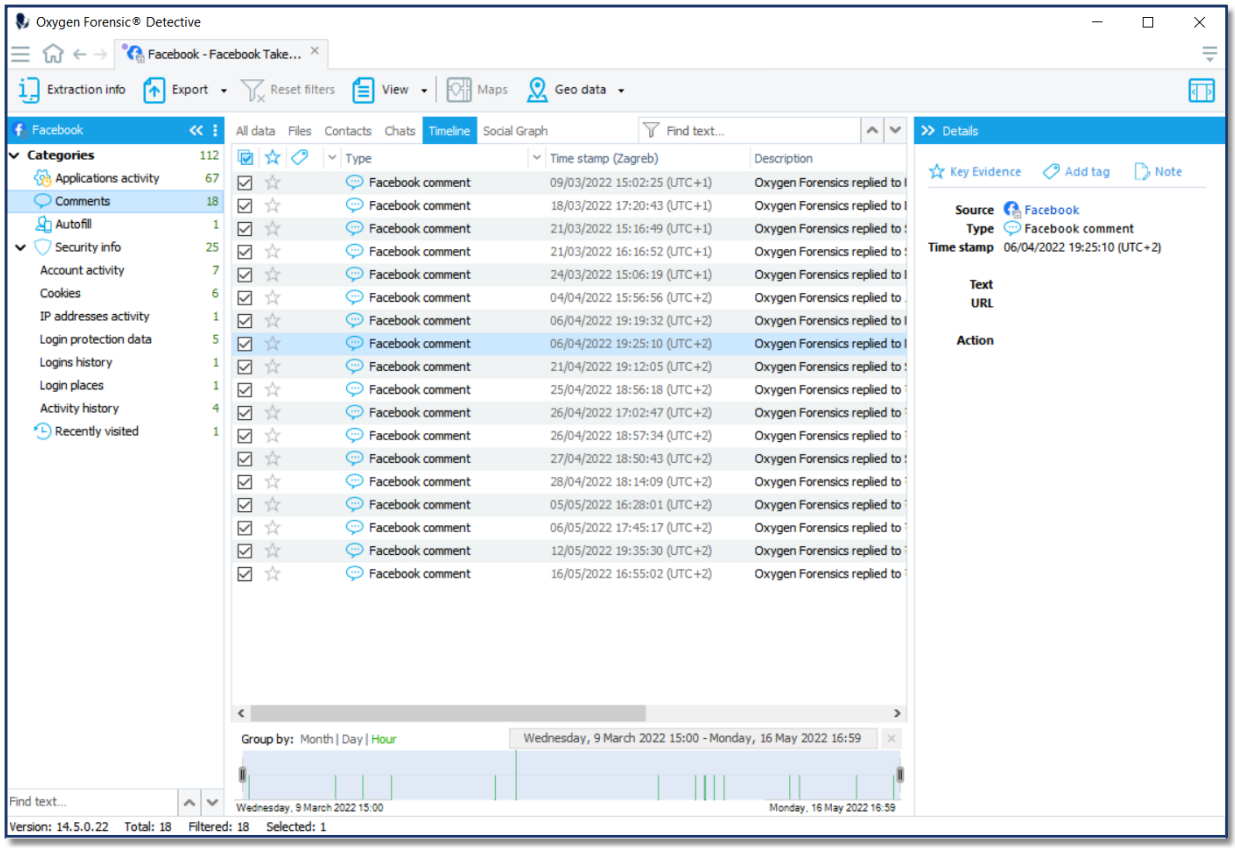
Import

Facebook account copy import

Facebook allows users to download and save their personal data. These files can be also used for investigation purposes. Information will be downloaded in the same language in which the Facebook interface is.

Oxygen Forensic® Detective v.14.5 enables import and analysis of Facebook account copy saved in HTML format. Files of the following languages are supported: English, German, French, Spanish, and Italian.

The parsed data will include many categories: contacts, chats, comments, groups, reactions, etc.



General

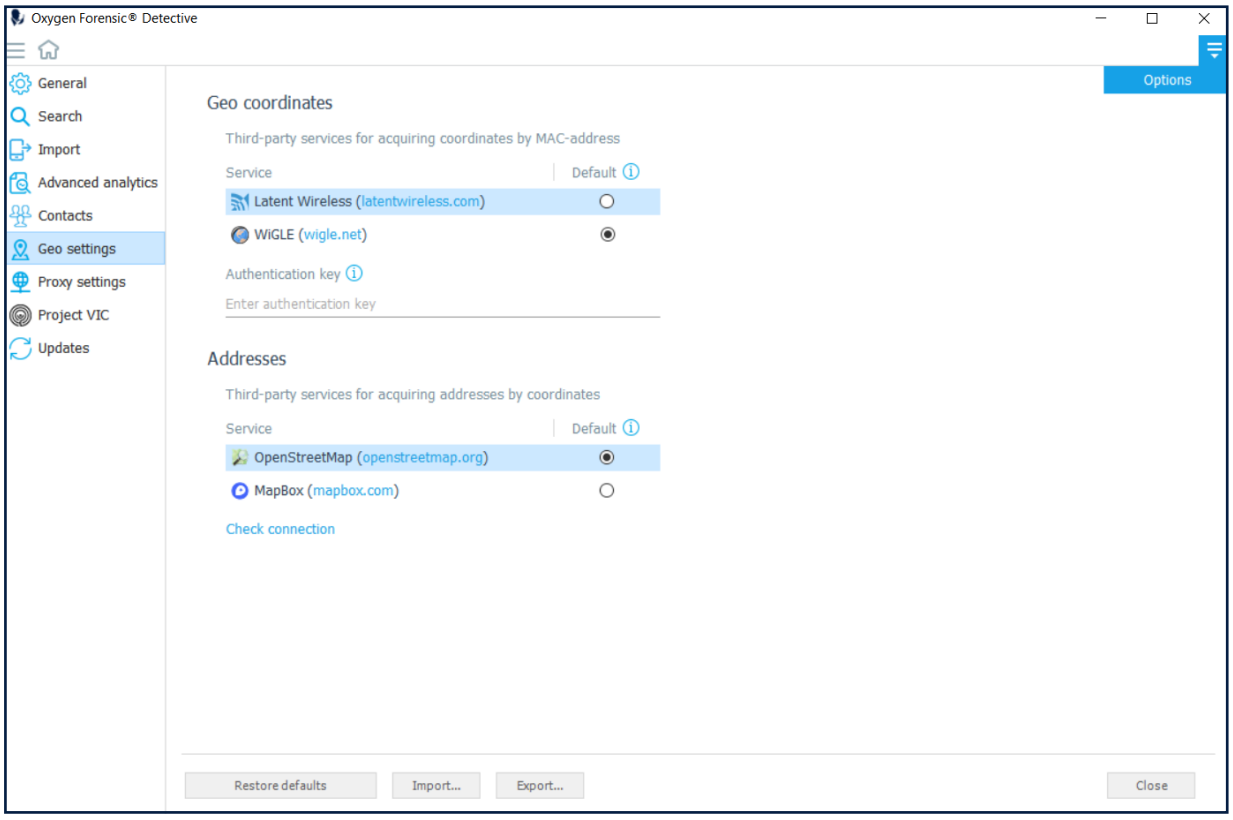
Getting addresses from extracted geo coordinates

Now a useful feature of getting addresses from geo coordinates is available in Oxygen Forensic® Detective. You can receive addresses using either OpenStreetMap or Mapbox service. Mapbox requires an authentication token to be entered in the Options menu of Oxygen Forensic® Detective.

The feature of getting addresses is available in all the sections that may contain geo coordinates - Files, Wireless Connections, and Applications. An internet connection is required.

You can get an address from a particular geo coordinate or from all of them.

Received addresses will be shown both in the grid and on the sidebar of the



Cloud Forensics

Cloud Extractor updates

In this release, we've focused on updating the authorization and extraction algorithms of already existing cloud services: Google My Activity, Google Home, Tinder, TamTam, and Discord. Due to the significant API changes, we've also had to completely re-write the extraction algorithms for Google Contacts. Now, much more data can be extracted from this service: SIP addresses, bio, contacts, last modified date, group lists, and other data.

Computer Artifacts

KeyScout updates

The updated KeyScout can now import and parse evidence from several new types of computer images:

- New Encase software formats - Ex01and Lx01
- Images of virtual machines of VMX and VBOX formats

We've also added the ability to collect OneDrive data on Windows and macOS. Additionally, we've updated support for the following apps:

- Safari
- Mozilla Firefox
- Google Chrome
- iCloud Drive
- Slack
- Telegram

Finally, we've added the ability to parse a setupapi.dev.log artifact from Windows.

Resolved issues

- Unable to extract encryption keys and decrypt Nokia 3 device dump
- Unable to decrypt Neffos C9A device dump
- Errors while parsing of Samsung Galaxy A8 dump
- Import of a device dump from a USB flash drive freezes
- Not all records are parsed from a SIM card extraction
- Unable to parse Windows Search Index
- com.apple.storebookkeeperd.plist source file is excluded from the Device information
- Errors in the Polish localization