Oxygen Forensic® Detective

Release notes

Version 15.4
April 2023

The latest update to our all-in-one solution is here, Oxygen Forensic® Detective v.15.4! This version introduces the following key features:

- Analysis of iFlight drone logs
- Huawei Health cloud extraction
- Import and parsing of MD-Next extractions
- Analysis of Windows RAM images
- Extraction of Google Chrome browser via Android Agent

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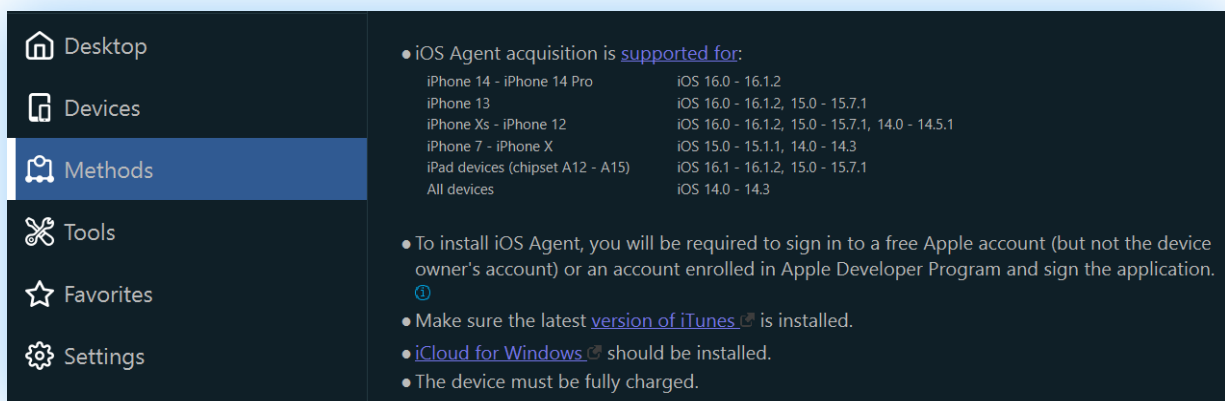
Mobile Forensic Updates

Extraction of Google Chrome artifacts via Android Agent

Oxygen Forensic® Detective v.15.4 enables extraction of Google Chrome artifacts via Android Agent from any supported unlocked Android device. Android Agent 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. Evidence sets will include account details, saved logins and passwords, credit cards, history, opened tabs, bookmarks, and downloads.

iOS Agent updates

In the recent versions of Oxygen Forensic® Detective, we've added two enhancements to the iOS Agent method:

- In the minor update of Oxygen Forensic® Detective v.15.3.1 we've added the ability to extract the full file system via iOS Agent from iOS devices running versions 15.0 – 15.7.1 and 16.0 – 16.1.2.
- Oxygen Forensic® Detective v.15.4 now allows selecting an exploit if several are available for the particular iOS device model.

🏠 Desktop	● iOS Agent acquisition is supported for:
📱 Devices	iPhone 14 - iPhone 14 Pro iOS 16.0 - 16.1.2
	iPhone 13 iOS 16.0 - 16.1.2, 15.0 - 15.7.1
🗺 Methods	iPhone Xs - iPhone 12 iOS 16.0 - 16.1.2, 15.0 - 15.7.1, 14.0 - 14.5.1
	iPhone 7 - iPhone X iOS 15.0 - 15.1.1, 14.0 - 14.3
✂ Tools	iPad devices (chipset A12 - A15) iOS 16.1 - 16.1.2, 15.0 - 15.7.1
	All devices iOS 14.0 - 14.3
☆ Favorites	● To install iOS Agent, you will be required to sign in to a free Apple account (but not the device owner's account) or an account enrolled in Apple Developer Program and sign the application. ⓘ
⚙ Settings	● Make sure the latest version of iTunes ⧉ is installed.
	● iCloud for Windows ⧉ should be installed.
	● The device must be fully charged.

App support

In Oxygen Forensic® Detective v.15.4, we've added support for the following new apps:

- iScanner (Apple iOS, Android)
- Notion (Apple)
- Session (Android)
- Telegram Web (Android)

The total number of supported app versions now exceeds 36,300.

Import Updates

Import of iFlight drone logs

We've enhanced our drone support by adding the ability to import and analyze iFlight drone logs that can be found on memory cards of remote controls. Evidence sets will include the following parameters: flight date and time, geo coordinates, battery level, altitude, and ground speed. The flight can be visualized on the built-in map in our software.

Import of iVe backups of vehicles

Now you can import and parse vehicle evidence from Berla iVe backups. To do this, click the "Third-party extractions" option in the Home screen and follow the instructions. The evidence set may include detailed vehicle information, connected mobile devices, calls, vehicle speed info, search and location history, files from the vehicle multimedia system, and other available artifacts.
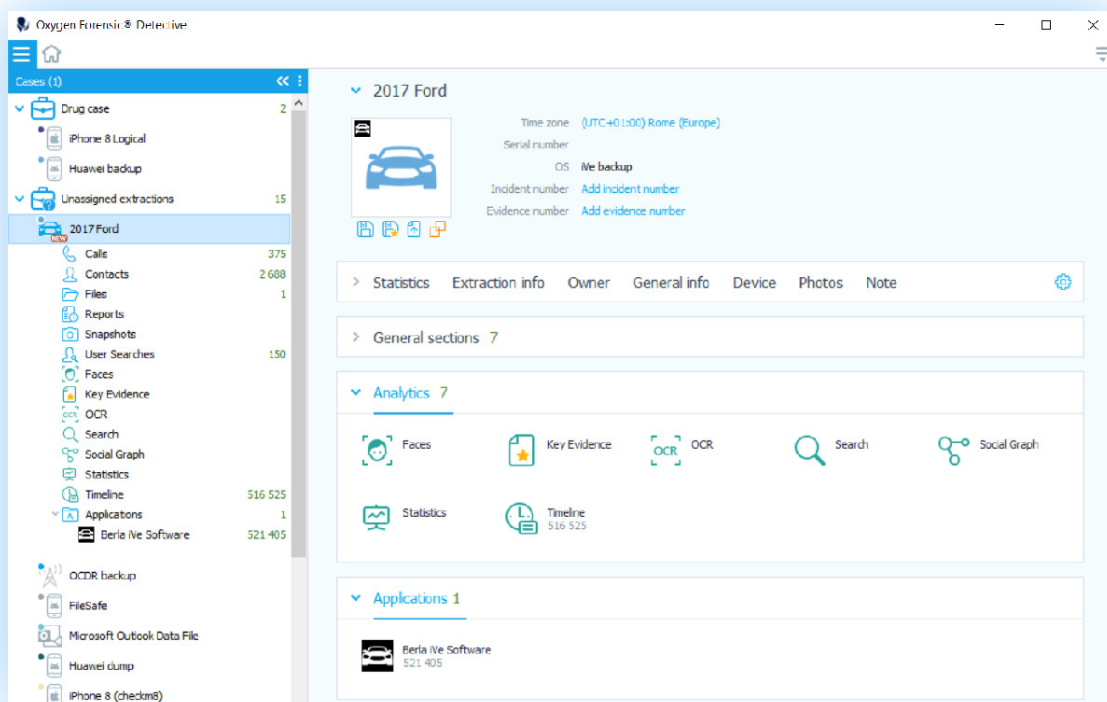
Import of MD-Next extractions

Oxygen Forensic® Detective v.15.4 can now ingest and parse MD-Next physical extractions of Android devices. Evidence sets will include all data, including apps.

Cloud Forensic Updates

Huawei Health extraction

We are enhancing our support for cloud fitness apps, and with this release, we are incorporating extraction of Huawei Health data via login and password, token, phone number, or QR code. Extracted evidence will include all health data: workouts, medical data, routes, and more.

Telegram updates

We've significantly improved support for the latest Telegram features. Now you can extract more data from Telegram cloud:

- Recent actions of group chats that are available to the group admins
- Group chats with enabled topics
- Collectible usernames

We've also updated the ability to extract Telegram tokens from Apple iOS devices.

Computer Artifacts

Functionality updates

With the updated Oxygen Forensic® KeyScout, investigators can perform the following:

- Extract data from drives and images with Logical Volume Manager partitions
- Analyze Windows RAM images in padded RAW and Crash Dump (DMP) formats while analyzing drives or drive images
- Collect and filter files by size
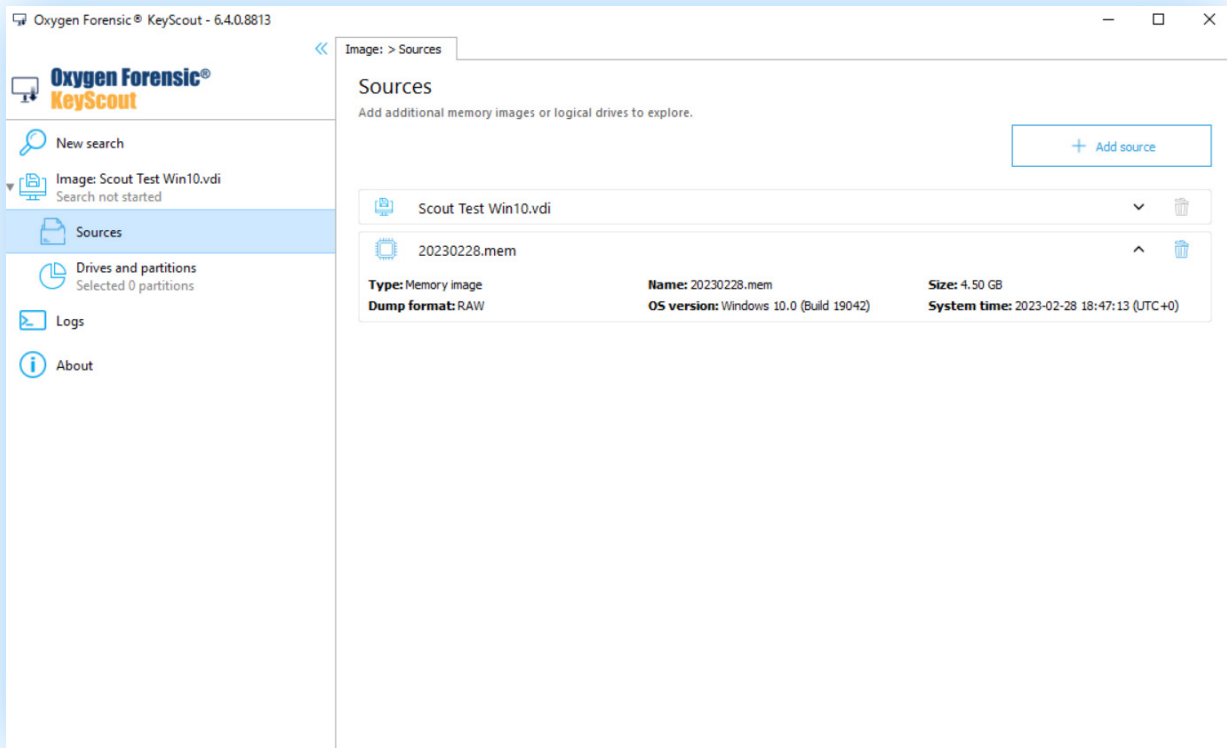
New and updated artifacts

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

- A web version of WhatsApp from Chromium, Microsoft Edge, and Brave browsers from Windows, macOS, and Linux
- A web version of Slack from Chromium, and Brave browsers from Windows, macOS, and Linux
- A web version of Instagram from Chromium, Microsoft Edge, and Brave browsers from Windows, macOS, and Linux
- AnyDesk data from Windows, macOS, and Linux
- Find My data from macOS
- The list of system user accounts and groups from macOS
- VPN connection settings from Windows

Updated artifact support includes:

- Amazon Photos from Windows and macOS
- The information about Bluetooth devices from macOS

Interested in trying out Oxygen Forensic® Detective v.15.4?

Request a free trial