Oxygen Forensic® Detective

Release notes

Version 15.1
November 2022

Our latest update to our flagship solution Oxygen Forensic® Detective v.15.1 is here! This version introduces the following key features:

- Enhanced support for MTK-based Android devices
- Brute force for additional MainSpace in Kirin-based Huawei devices
- Import of Microsoft Outlook Data Files
- Import of Snapchat My Data
- Facial Categorization on video frames

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

Mobile Forensic Updates

Enhanced support for MTK devices

Oxygen Forensic® Detective v.15.1 brings enhanced support for MTK-based Android devices. Now Android devices that have TEE Trusty and File-Based Encryption (FBE) and are based on the MT6765 and MT6580 chipsets are supported for passcode brute force.

Moreover, our support now covers Android devices that are based on the MT6739 chipset and have TEE Kinibi and Full-Disk Encryption (FDE).

We've also added the ability to decrypt images of Xiaomi and Poco devices based on the Mediatek MT6769T chipset and having File-Based Encryption (FBE). Supported models include Xiaomi Poco M2, Xiaomi Redmi 9 Global, Xiaomi Redmi 9 Prime.

Android Keystore extraction from Qualcomm-based devices

We've added the ability to extract encryption keys from the Android Keystore from devices based on the Qualcomm chipsets: MSM8917, MSM8937, MSM8940, and MSM8953.

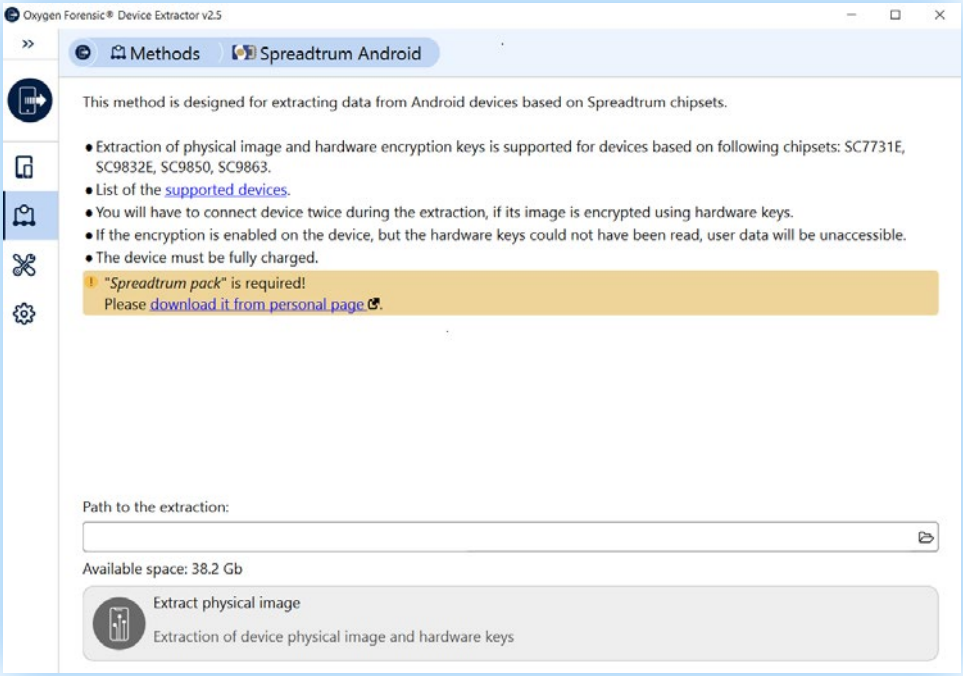
To use this functionality, select the Qualcomm EDL method in the Oxygen Forensic® Device Extractor. With the extracted encryption keys, Oxygen Forensic® Detective can decrypt Briar, ProtonMail, Silent Phone, and Signal apps.

Other Device Extractor updates

We've also included the following extraction updates:

- Redesigned extraction method for Spreadtrum-based devices. Now this method is available in the new Oxygen Forensic® Device Extractor.
- Updated the ability to extract data from Discord and added selective Discord chat extraction via Android Agent.

- Improved the interface of selective iOS data extraction via checkm8, SSH, and iOS Agent.
- Full extraction support for iPhone 14, iPhone 14 Plus, iPhone 14 Pro, and iPhone 14 Pro Max via iTunes backup procedure.



App support

In Oxygen Forensic® Detective v.15.1, we've added support for the following new apps:

- Briar (Android)
- AppLock (Android)
- Default Sound Recorder (Android)
- FileSafe (Android)
- Zoho Mail (iOS, Android)
- JustTalk (iOS)
- Microsoft Bing (iOS)
- Shazam (iOS)
- IRL (iOS)

The total number of supported app versions now exceeds 34,300.

Import Updates

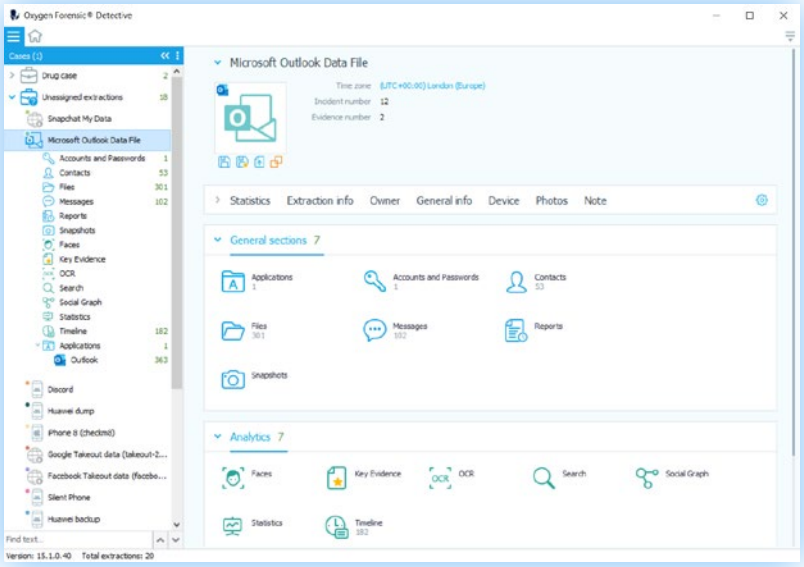
Brute force for additional MainSpace (Huawei)

A Huawei device may have more than one MainSpace (user profiles). In Oxygen Forensic® Detective v.15.1, you can brute force passcodes to the second, third, or more profiles in MainSpace.

Please note that a passcode brute force is also available for PrivateSpace.

Import of Microsoft Outlook Data Files

Now you can import and parse Microsoft Outlook Data Files of .pst/.ost file formats. Select this file format under “Desktop Data” options and follow the instructions. The parsed evidence set will include emails, contacts, calendars, and tasks.



Import of Snapchat My Data

Oxygen Forensic® Detective v.15.1 allows you to import downloaded Snapchat My Data that can be collected with the “Download My Data” function from Snapchat. The parsed evidence set will include account information, chats, calls, memories, search history, highlights, story views, and more.

We’ve also added support for the latest version of Snapchat Warrant Returns.

Cloud Forensic Updates

We’ve introduced several improvements to Oxygen Forensic® Cloud Extractor:

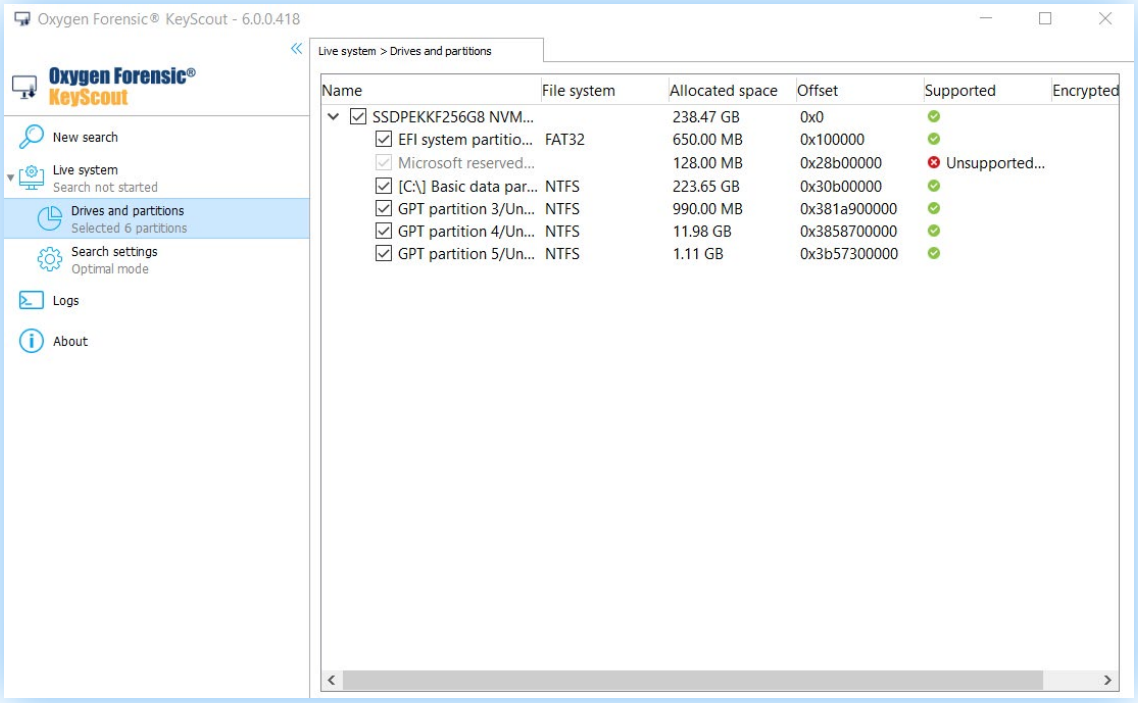
- The last view date is now extracted for Google Drive files
- You can set a path to OCB files in the Account Owner information window
- We’ve redesigned the Help menu and included new documents

Computer Artifacts

Functionality updates

We've improved the software interface and made a number of functional updates to KeyScout.

- You can now decrypt passwords, tokens, and cookies collected from other user profiles and computer images. Enter the known password in the Passwords tab within the Search settings for data decryption.
- You can select particular drives and partitions for live extraction.
- We've improved the Search Settings interface by adding detailed descriptions of the system artifacts and memory available for extraction.
- More detailed information has been added regarding every step of the data collection and saving process.



New and updated artifacts

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

- Windows Diagnostic Infrastructure (WDI) artifact on Windows
- System logs on Linux
- Microsoft To Do app on Windows
- Mail and Calendar app on Windows

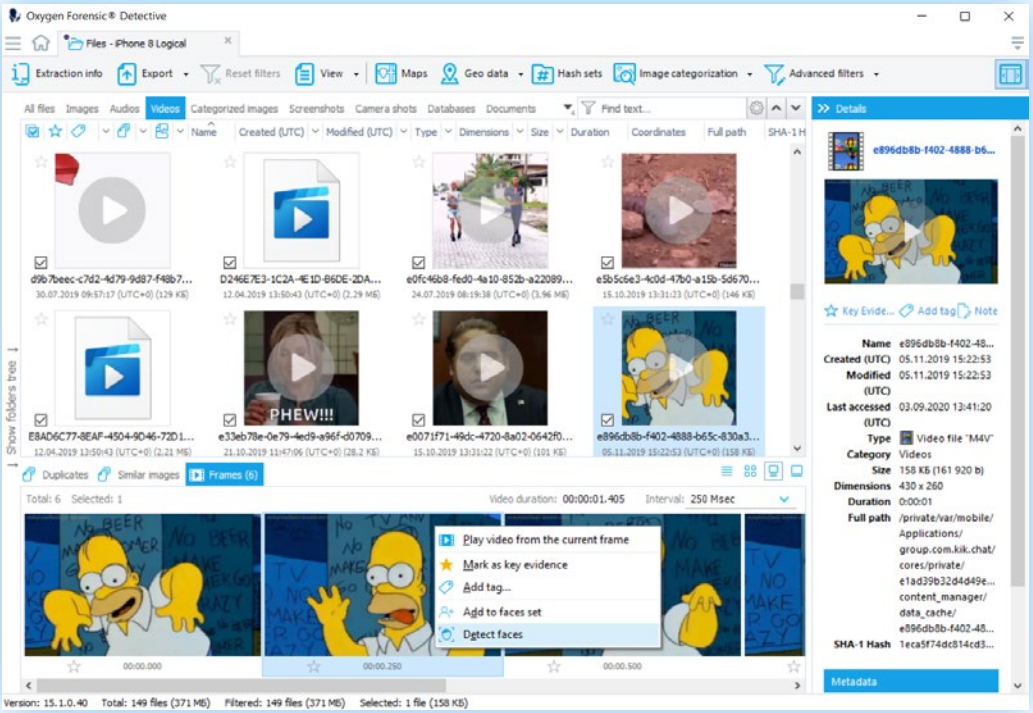
Updated artifact support includes:

- Most Recently Used (MRU) artifact on Windows
- WMI persistence artifact on Windows
- System events artifact on macOS
- Microsoft Outlook app on Windows
- Signal app on Windows, macOS, and Linux

General Updates

Facial Categorization on video frames

In the Files section, we've added the ability to categorize faces from video frames. If an extracted video has a face, you can now right click on a video frame and add it to the Faces section by selecting the "Detect face" option.



Updates in Oxygen Forensic® Viewer

We've added support for Project VIC files in Oxygen Forensic® Viewer. You can now:

- Assign Project VIC categories to images in the Files section
- Add Project VIC hash sets in the Hash Sets Manager
- Customize Project VIC categories in the Options menu

Resolved Issues

- Telegram token from Google Chrome not saving with Oxygen Forensic® KeyScout
- A section of the Oxygen Forensic® KeyScout interface displayed blank on macOS
- No data collected from Opera browser by Oxygen Forensic® KeyScout
- Android Agent extraction fails with unknown error 0xC0000002