Oxygen Forensic® Detective

Release notes

Version 15.2
December 2022

Our latest update to our flagship solution Oxygen Forensic® Detective v.15.2 is here! This version introduces the following key features:

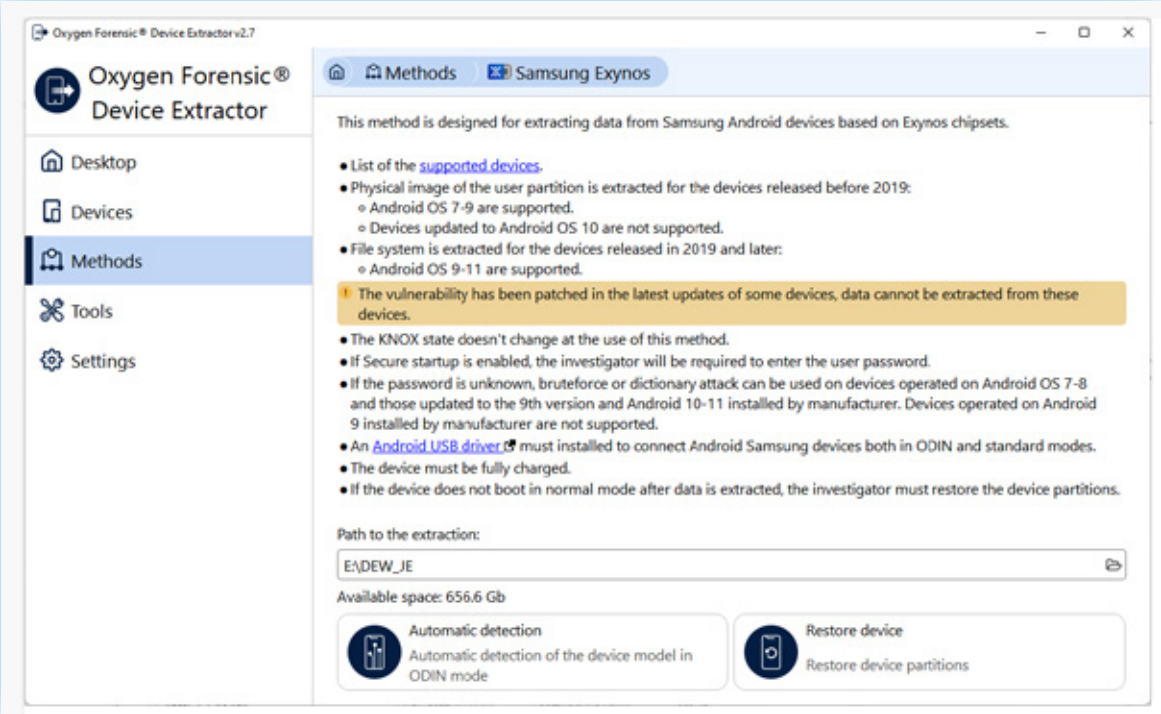
- Brute force for Samsung Exynos devices with FBE
- Runtastic cloud data extraction
- Decryption of WhatsApp backups of .crypt15 type
- Support for XFS file system

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 Exynos devices (FBE)

You can now brute force passcodes to decrypt data from Samsung Exynos devices running Android OS 10-11 and having File-Based Encryption (FBE). Our support includes the following models: Galaxy A51 5G, Galaxy A71 5G, Galaxy F41, Galaxy M21, Galaxy M31, Galaxy Xcover Pro, Galaxy Note10 Lite, and many others.



Enhanced support for MTK Android devices

In Oxygen Forensic® Detective v.15.2, we have included several enhancements for MTK-based devices. You can now extract and decrypt physical dumps of Xiaomi 6 and Xiaomi 6A devices based on the MTK6765 chipset with Full-Disk Encryption (FDE). Moreover, now you can decrypt physical images of devices based on the MT6737 chipset having TEE Trusty and FDE.

Extraction of Firefox and RCS messages via Android Agent

You can now quickly collect Firefox browser data from any unlocked Android device using our 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. The evidence set will include user info, history, bookmarks, downloads, and tabs.

We've also added extraction of RCS messages from unlocked Android devices via Android Agent. You can collect RCS messages manually using Android Agent or via USB cable, if you directly connect a device to Oxygen Forensic® Detective.

Other Device Extractor updates

We've also added the following extraction updates:

- Ability to extract full file system and keychain from iOS devices with versions 14.4-14.5.1 via iOS Agent.
- Ability to extract full file system and keychain via checkm8 from iPhone 6s and iPhone SE devices without disabling the screen lock.
- Desktop initial screen.

App support

In Oxygen Forensic® Detective v.15.2, we've added support for the following new apps:

- Xiaomi Notes (Android)
- Xabber Beta (Android)
- IRL (Android)
- JustTalk (Android)
- SafeCalc (iOS)
- Life360 (iOS)

The total number of supported app versions now exceeds 34,600.

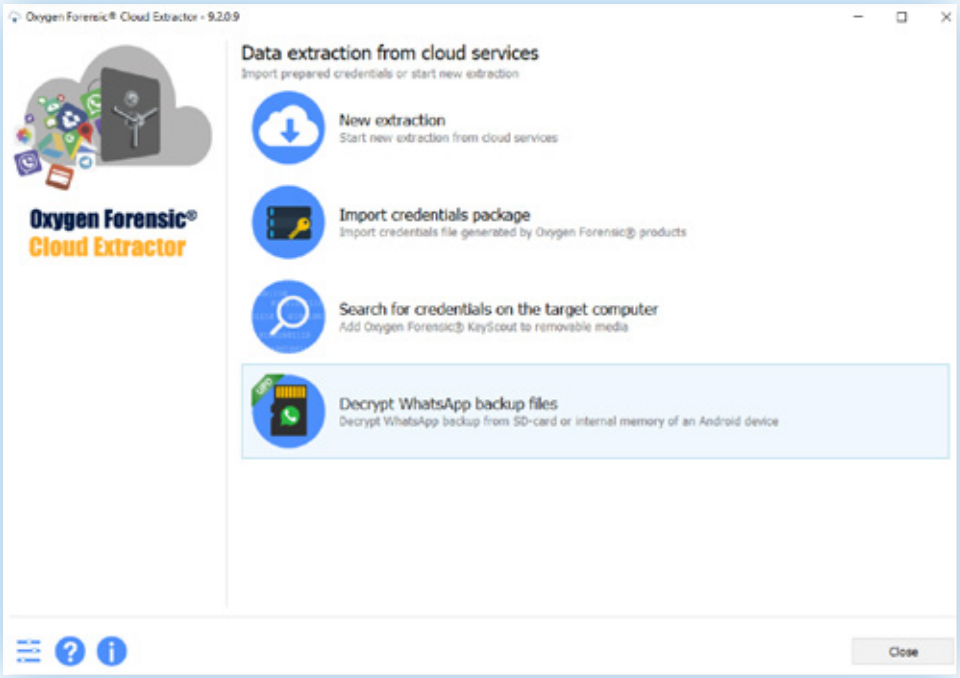
Cloud Forensic Updates

Runtastic data extraction

Oxygen Forensic® Detective v.15.2 allows extraction of workout data from Runtastic cloud account using login credentials and token. Extracted evidence sets will include account details as well as a list of activities with locations and comments.

WhatsApp backup decryption

In the latest Oxygen Forensic® Cloud Extractor, you can import and decrypt WhatsApp backups of .crypt15 format. Decryption is available via phone number or 64-digit key.

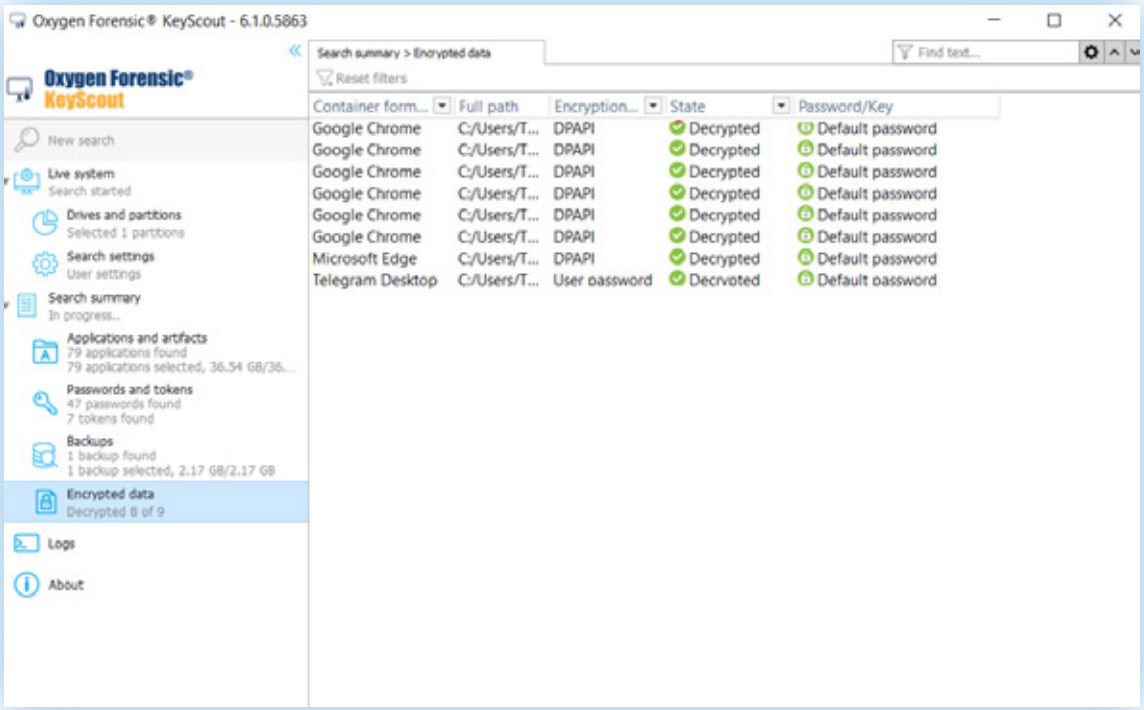


Computer Artifacts

Functionality updates

We've made a number of functional and interface updates to KeyScout:

- Added support for XFS file system
- Added the Encrypted data tab
- Added display of privilege levels on macOS
- Added extended information about data saving



New and updated artifacts

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

- DPAPI keys of the authorized user from Windows RAM
- DNS cache from Windows during live data extraction
- ARP cache from Windows during live data extraction
- Firewall rules from Windows
- Cron tasks from Linux
- System accounts and groups from Linux
- SSH keys from macOS and Linux
- Extended system information about Linux

Updated artifact support includes:

- Google Chrome browser from Windows, macOS, and Linux
- Cache from apps based on the Blink engine
- Signal app on Windows, macOS, and Linux

Resolved Issues

- Passcode bruteforce for Xiaomi Redmi 9 device starts and immediately stops
- Passcode bruteforce for Xiaomi Redmi Note 8 Pro is completed but password is not found
- Telegram token is invalid from downgrade APK extraction
- No WhatsApp contacts are extracted if selective extraction is chosen via Android Agent
- Backup import stops at the User Activity section parsing