OXYGEN FORENSICS

Oxygen Forensic® Detective

Release notes

Version 16.0
September 2023

The latest update to our flagship solution is here, Oxygen Forensic® Detective v.16.0. Key features include:

- APK Downgrade support for Android OS 12 – 13
- Decryption and extraction of VeraCrypt containers
- Passcode brute force for Apple Notes and Briar app
- Cloud extraction of Clubhouse, Bumble, and Google Messages
- New categories in the Image Categorization engine

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

Mobile Forensic Updates

Support for Xiaomi Redmi devices

In Oxygen Forensic® Detective v.16.0, we added the ability to extract hardware keys and decrypt physical dumps of Xiaomi devices based on the Qualcomm SDM439 chipset. Xiaomi Redmi 7A, Xiaomi Redmi 8, and Xiaomi Redmi 8A devices running Android OS 7 or higher are now supported.

Extended support for UNISOC-based devices

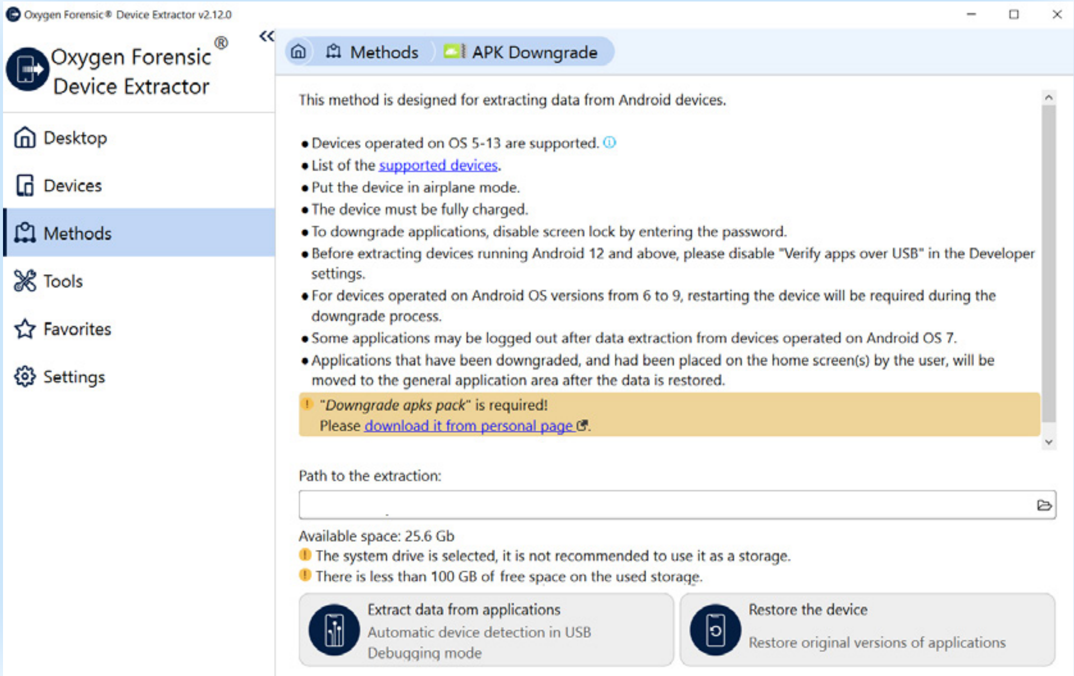
We also added support for the devices based on the UNISOC T606, T616, T612, and T310 chipsets and running Android OS 10 – 13. Now you can extract hardware keys to decrypt physical dumps of many HTC, Motorola, Nokia, Realme, ZTE, and other devices based on these chipsets.

Samsung Browser extraction via Android Agent

You can now quickly collect Samsung 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 extraction can be imported into Oxygen Forensic® Detective for review and analysis. The evidence set will include saved logins and passwords, history, bookmarks, downloads, and other available data.

Enhanced APK Downgrade method

Our APK Downgrade method allows extraction of popular apps by temporarily downgrading app versions so that they are included in the ADB backup. In Oxygen Forensic® Detective v.16.0, we added support for Android OS versions 12 and 13. Now you can extract data from many more Android devices using this method. With our support for WhatsApp, Instagram, Facebook, Twitter, and 40 other supported apps, you will have access to much more critical evidence.


Oxygen Forensic® Device Extractor v2.12.0
Oxygen Forensic® Device Extractor
Desktop
Devices
Methods
Tools
Favorites
Settings
Methods
APK Downgrade

This method is designed for extracting data from Android devices.

- Devices operated on OS 5-13 are supported.
- List of the supported devices.
- Put the device in airplane mode.
- The device must be fully charged.
- To downgrade applications, disable screen lock by entering the password.
- Before extracting devices running Android 12 and above, please disable "Verify apps over USB" in the Developer settings.
- For devices operated on Android OS versions from 6 to 9, restarting the device will be required during the downgrade process.
- Some applications may be logged out after data extraction from devices operated on Android OS 7.
- Applications that have been downgraded, and had been placed on the home screen(s) by the user, will be moved to the general application area after the data is restored.

! "*Downgrade apks pack*" is required!
Please download it from personal page.

Path to the extraction:

Available space: 25.6 Gb
! The system drive is selected, it is not recommended to use it as a storage.
! There is less than 100 GB of free space on the used storage.

Extract data from applications
Automatic device detection in USB Debugging mode

Restore the device
Restore original versions of applications

Enhanced iOS Agent method

We significantly enhanced the ability to extract full file system and keychain via the iOS Agent. Now you can extract them from devices with iOS versions 14.6 – 14.8.1, 15.6 – 15.7.1, and 16.0 – 16.5.

Decryption of Apple Notes and Briar app

We added passcode brute force for encrypted Apple Notes and Briar app.

If an Apple Note is encrypted, you can click the Enter passcode button on the toolbar of the Apple Notes section and brute force the passcode using our various available attacks.

You can now brute force the passcode for Briar app installed on Android devices. This functionality is available in the Full File System extraction method.

New App support

We added support for the following new apps:

- Threads (Android, iOS)
- TikTok Lite (Android)
- TanTan (Android, iOS)
- 1Password (Android, iOS)

The total number of supported app versions now exceeds 40,000.

Import Updates

In Oxygen Forensic® Detective v.16.0, we added the ability to import the following images:

- Physical dumps of Xiaomi Redmi 7A/8/8A based on the Qualcomm SDM439 chipset
- Physical dumps of the UNISOC T606/T616/T612, and T310 chipsets
- XRY backups of versions 10.3.1 and newer

Additionally, you can now select artifacts to import and analyze from Oxygen Forensic® KeyScout extractions. This is a great time-saving feature as you do not need to import the whole extraction anymore.

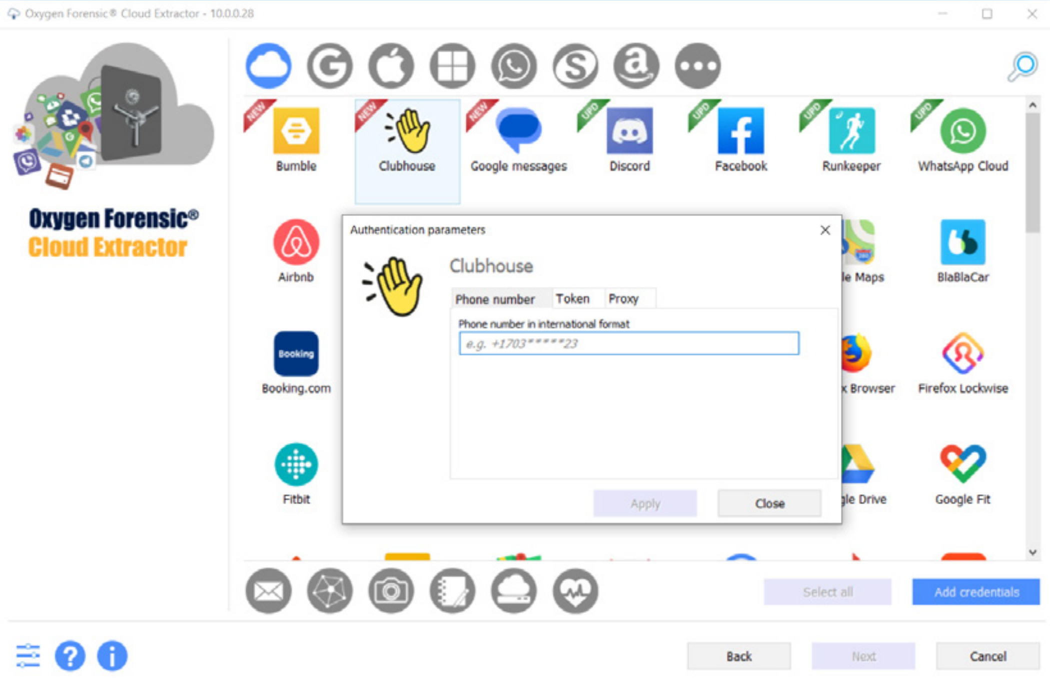
Cloud Forensic Updates

Bumble data extraction

Bumble is another new service added in Oxygen Forensic® Detective v.16.0. Data extraction from this dating app is supported via phone number or token. Extracted evidence will include profile info, contacts, messages, and album photos.

Clubhouse data extraction

Launched in 2020, Clubhouse currently has over 10 million weekly active users. The latest Oxygen Forensic® Cloud Extractor enables data extraction from Clubhouse via phone number or token. The extracted data set includes account info, contacts, audio messages and replays, chats, notifications, and information about the houses.



Google Messages extraction

Now you can also extract Google Messages from the cloud. Use a token or scan a QR code with a mobile device to gain access to this cloud service. The evidence set will include information about the account owner, SIM cards, contacts, as well as private and group chats.

With this version, the total number of supported cloud services is now 105.

Computer Artifacts

Deleted files recovery

We added the ability to recover deleted files from FAT16, FAT32, and exFAT file systems. To do so, select the "Recover deleted files" option in the KeyScout Search settings, then, select drives and partitions where you want to recover deleted files.

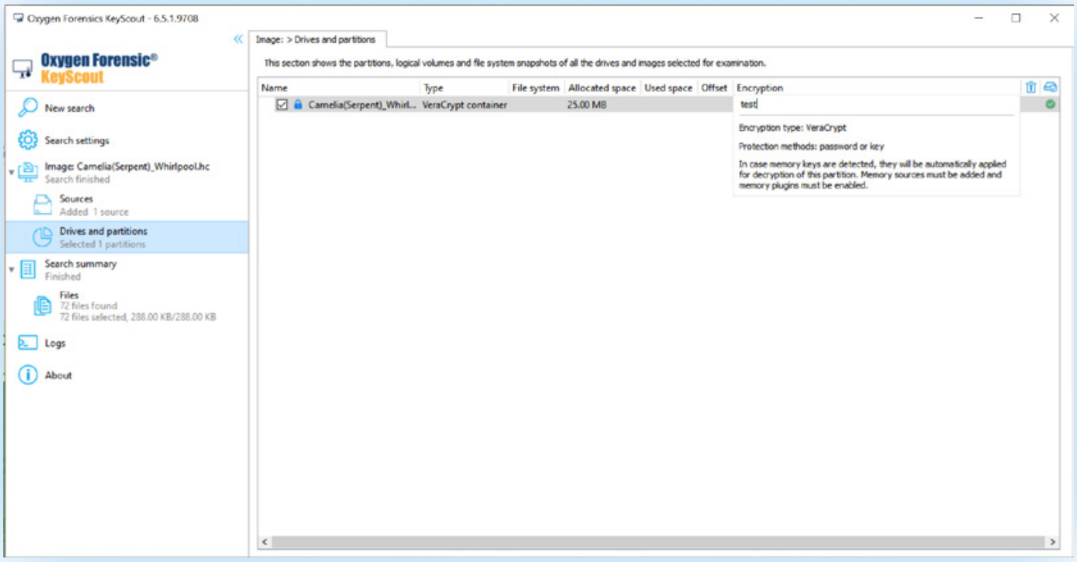
Decryption of VeraCrypt containers

The updated Oxygen Forensic® KeyScout can now extract VeraCrypt encryption keys from Windows RAM. With a found VeraCrypt encryption key drive, partitions and separate file containers can be decrypted.

The key features of this functionality include:

- Support for standard and hidden containers
- Detection of drives, partitions, or file containers protected with VeraCrypt
- Extraction of VeraCrypt encryption keys of any versions
- Support for all 15 VeraCrypt encryption algorithms

In addition to VeraCrypt encryption keys, drives and partitions can be decrypted with a known password in Oxygen Forensic® KeyScout.



This section shows the partitions, logical volumes and file system snapshots of all the drives and images selected for examination.

Name	Type	File system	Allocated space	Used space	Offset	Encryption
☑ Camelia(Serpent)_Whirl...	VeraCrypt container		25.00 MB			test

Encryption type: VeraCrypt

Protection methods: password or key

In case memory keys are detected, they will be automatically applied for decryption of this partition. Memory sources must be added and memory plugins must be enabled.

New artifacts

The updated Oxygen Forensic® KeyScout enables users to collect the following new artifacts:

- Installed Homebrew packages from macOS
- Shim Cache from Windows
- The information about permissions that were given to applications on Windows
- NordVPN from Windows, macOS, and GNU/Linux
- PureVPN from Windows, macOS, and GNU/Linux
- VLC Media Player from Windows, macOS, and GNU/Linux
- A paid version of ViPole from Windows, macOS, and GNU/Linux
- Telegram stories from macOS

Moreover, we added decryption of Viber databases from macOS and WhatsApp databases from Windows images.

Data Analysis Updates

We enhanced our analytical sections with two features:

- New categories are added to the Image Categorization section: medical, meme, offensive gesture, and schematic.
- A new smart filter now allows showing events before and after those events marked with a particular tag in the Timeline section.

Interested in trying out Oxygen Forensic® Detective v.16.0?

Request a free trial