OXYGEN FORENSICS

Oxygen Remote Explorer

Version 1.4.1 | May 2024

Release notes

Oxygen Remote Explorer v.1.4.1 is here. Key features include:

- iOS remote extraction dramatically improved
- Passcode brute force for 7-ZIP archives
- Search by file signatures
- Enhanced Chats View
- Preliminary data export

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

Endpoint Data Collection

iOS remote extraction enhancements

The algorithm of remote iOS extraction has been dramatically improved. Users can now selectively extract artifacts from an iOS endpoint to comply with search requirements and also alleviate server load for faster collection and transfer of extracted data for analysis.

This change will alleviate server load and will allow for faster uploading of selectively extracted data.

Agent Management Center

Several improvements have been made to the Agent Management Center:

- We've added a Notifications Center where you will be able to see all system notifications: low disk space on the server or endpoint, user rights change, and more.
- Now you can export all or selected user logs to CSV, TSV, XLSX, and HTML formats. They can be used for internal reports or troubleshooting.
- Now you can view the settings used for previous extractions. Click the link on the program's main desktop and you will be able to see the settings that were used for a particular extraction.

Computer Artifacts

Passcode brute force module

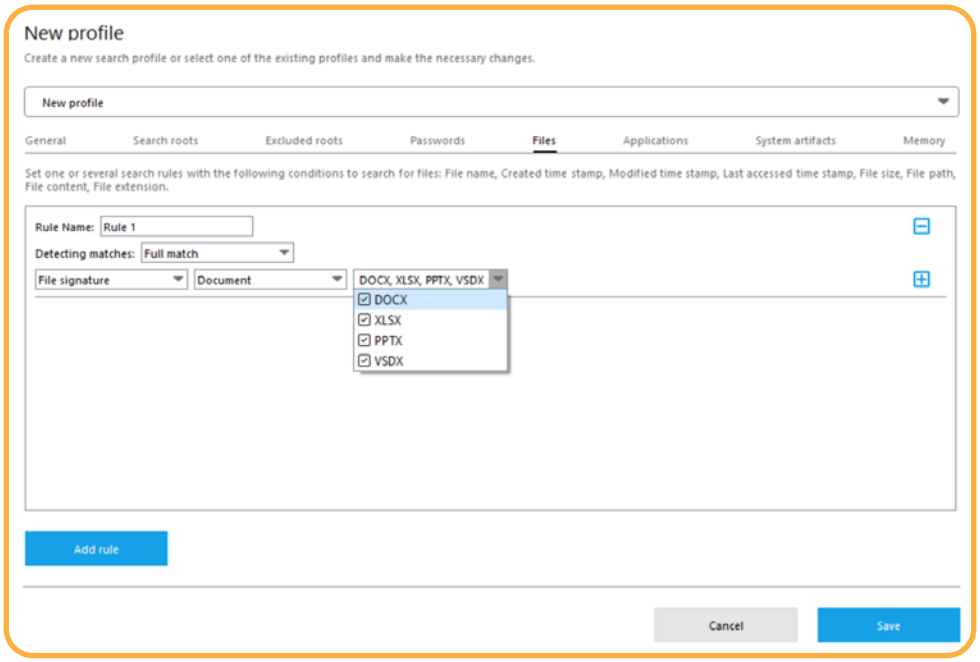
Enhanced KeyDiver Passcode recovery:

- encrypted 7-ZIP archives
- encrypted iTunes backups

Attack methods can be created using a dictionary, mask, or data extracted from collected endpoints.

Search by file signatures

File signature searching for Microsoft Office files has been added to the Documents Profile under the Files tab. This addition will benefit the investigation for standard searching but also when file extensions have been altered or files have been deleted.



New artifacts

The following new computer artifacts are supported:

- Steam (Windows, macOS, GNU/Linux)
- BitTorrent (Windows)
- 1Password (Windows, macOS, GNU/Linux)
- Box Drive (Windows, macOS)
- Box Tools (Windows, macOS)
- Web version of Box (Windows, macOS, GNU/Linux)

Updated artifacts include:

- Event log (Windows)
- WhatsApp (macOS)

Cloud Extractor Updates

Steam cloud data extraction

Extract evidence from Steam, a video game digital distribution service, from the cloud via login/password or token. Supported artifacts include:

- account information
- contacts
- products
- reviews
- groups
- group discussions
- group events
- group announcements
- group comments

Mobile Extraction Updates

Extraction of the second WhatsApp account via Android Agent

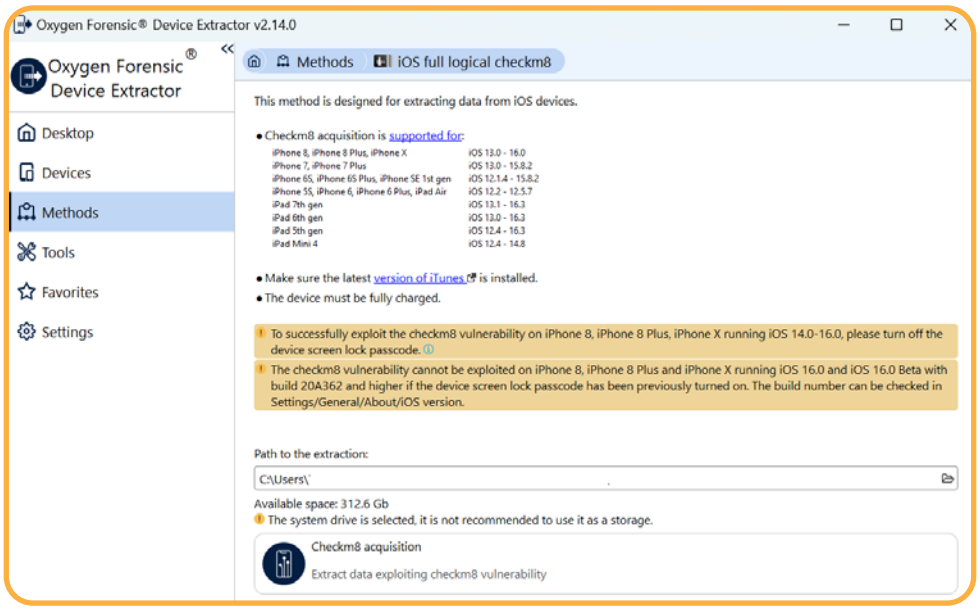
Extract a second authorized account of WhatsApp or WhatsApp Business on an Android device using Android Agent. Evidence set will include:

- contacts
- calls
- chats

Extended checkm8 support

Extract full file system via checkm8 from iPads running iOS 16. The following models and iOS versions are supported:

- iPad 7th gen: iOS 13.1 - 16.7.5
- iPad 6th gen: iOS 13.0 - 16.7.5
- iPad 5th gen: iOS 12.4 - 16.7.5



Enhanced support for UNISOC-based devices

Support has been added for screen-locked Samsung devices based on the UNISOC SC9863A chipset and running Android OS 10-13. We've also significantly accelerated data extraction from UNISOC-based Android devices, with extraction speeds now being 7-8 times faster than before.

Support for the MT6781 and MT6877 chipsets

Support has been added for two additional Mediatek chipsets - MT6781 and MT6877. You can extract hardware keys and decrypt physical dumps of screen-locked devices running Android OS 10 or higher. Supported models include:

- Xiaomi Redmi Note 12S
- Xiaomi Redmi Note 11S 4G
- Xiaomi Redmi Note 12 Pro+
- Realme 8i
- Samsung Galaxy M53 5G
- Samsung Galaxy Quantum 3
- Samsung Galaxy A34 5G

Extended support for Qualcomm-based Samsung devices

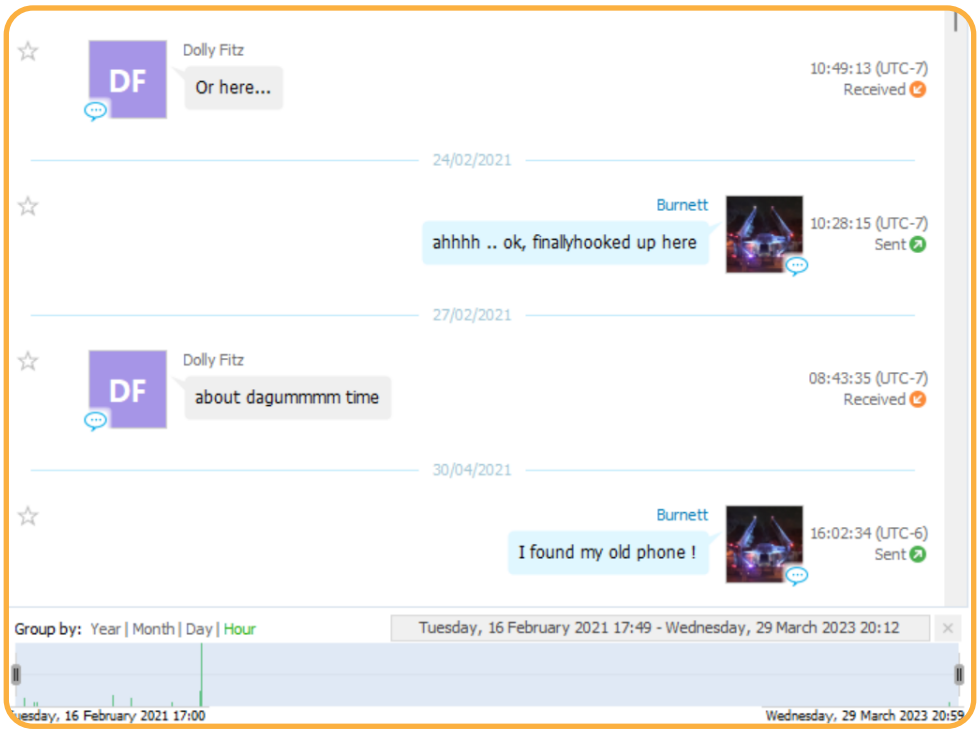
Extract evidence from screen-locked Samsung devices based on the Qualcomm Snapdragon SDM845 chipset. Supported models include:

- Samsung Galaxy Note 9
- Samsung Galaxy S9
- Samsung Galaxy S9+

General

Enhanced Chats View

Enhancements were introduced to the Chats View, focusing on improved visualization of forwarded and replied chats, as well as chat status and chat filtering. These enhancements are also included in the export of chats.



Import

Import updates

Import improvements include:

- A separate import of Apple Keychain is now available. Parsed keychain data can be found in the Accounts and Passwords section as well as in the Applications section of Oxygen Remote Explorer.
- Import and parse VDI images of Android extractions. This allows importing and analyzing the images created by Bluestacks, a popular Android emulator that is often used on computers for running apps from Google Play Store.
- Decryption of Android Keystore keys from physical images of MTK- and UNISOC-based Android extractions. With these keys the following apps can be decrypted: Briar, Jio chat, Proton Mail, Signal, Silent phone, Session, and Samsung customization service.
- Parsing of logical MD-Next extractions.

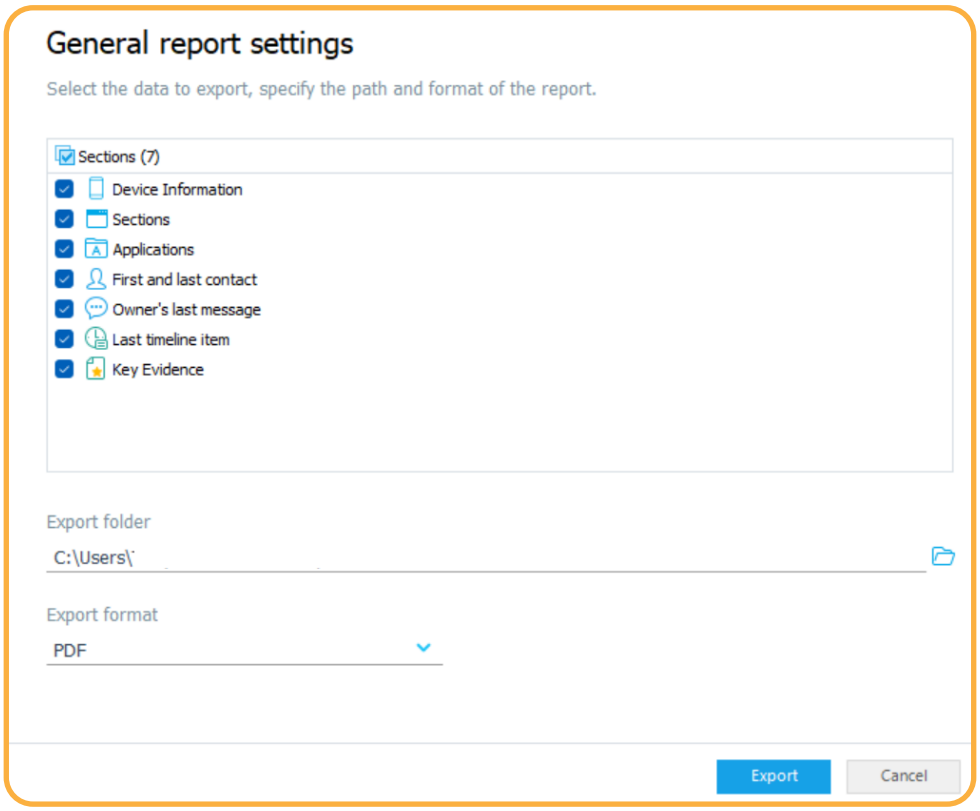
Export

Preliminary data export

Preliminary reports can be generated including the following data:

- Device/case info
- Categories and number of artifacts
- Applications and number of artifacts for each application
- First and last contacted contacts
- Last communication by the owner
- Last elements on the Timeline
- Key Evidence data

To run this type of data export, right click on Extraction in the device tree and choose the "Pre-export data" option. This feature may be useful if you need a basic report to kickstart an investigation or to compare the number of artifacts provided by different extraction methods.



Interested in finding out more about Oxygen Remote Explorer?

Schedule a Demo