Oxygen Forensic® Detective

Release notes

Version 16.2
March 2024

The latest update to our flagship solution is here, Oxygen Forensic® Detective v.16.2. Key features include:

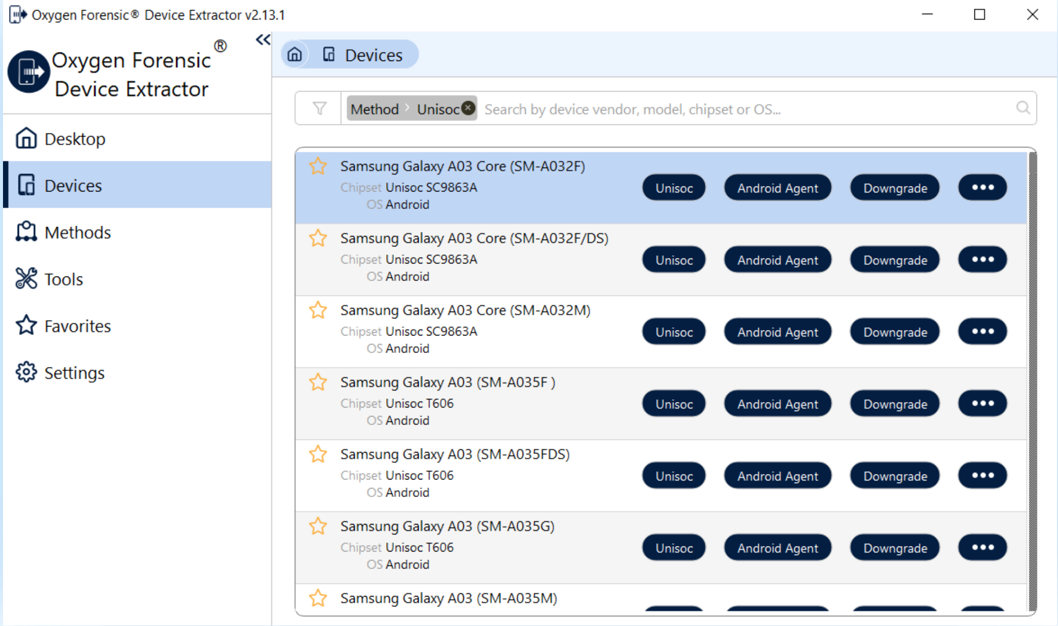
- Enhanced support for UNISOC-based devices
- Import of Apple Warrant Returns
- Steam data extraction
- Passcode brute force for 7-ZIP archives and iTunes backups
- Preliminary data export

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 UNISOC-based devices

Added support 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. Our tests show extraction speeds 7-8 times faster than before.


Oxygen Forensic® Device Extractor v2.13.1
Oxygen Forensic® Device Extractor
Desktop
Devices
Methods
Tools
Favorites
Settings
Devices
Method
Unisoc
Search by device vendor, model, chipset or OS...

Device	Chipset	OS				
Samsung Galaxy A03 Core (SM-A032F)	Unisoc SC9863A	Android	Unisoc	Android Agent	Downgrade	•••
Samsung Galaxy A03 Core (SM-A032F/DS)	Unisoc SC9863A	Android	Unisoc	Android Agent	Downgrade	•••
Samsung Galaxy A03 Core (SM-A032M)	Unisoc SC9863A	Android	Unisoc	Android Agent	Downgrade	•••
Samsung Galaxy A03 (SM-A035F)	Unisoc T606	Android	Unisoc	Android Agent	Downgrade	•••
Samsung Galaxy A03 (SM-A035FDS)	Unisoc T606	Android	Unisoc	Android Agent	Downgrade	•••
Samsung Galaxy A03 (SM-A035G)	Unisoc T606	Android	Unisoc	Android Agent	Downgrade	•••
Samsung Galaxy A03 (SM-A035M)						

Support for the MT6781 and MT6877 chipsets

Added support for two more 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, and more.

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 and Samsung Galaxy S9+.

Extraction of the second WhatsApp account via Android Agent

Extract second authorized account of WhatsApp or WhatsApp Business on an Android device using Android Agent. Evidence set will include contacts, calls, and chats.

Extended checkm8 support

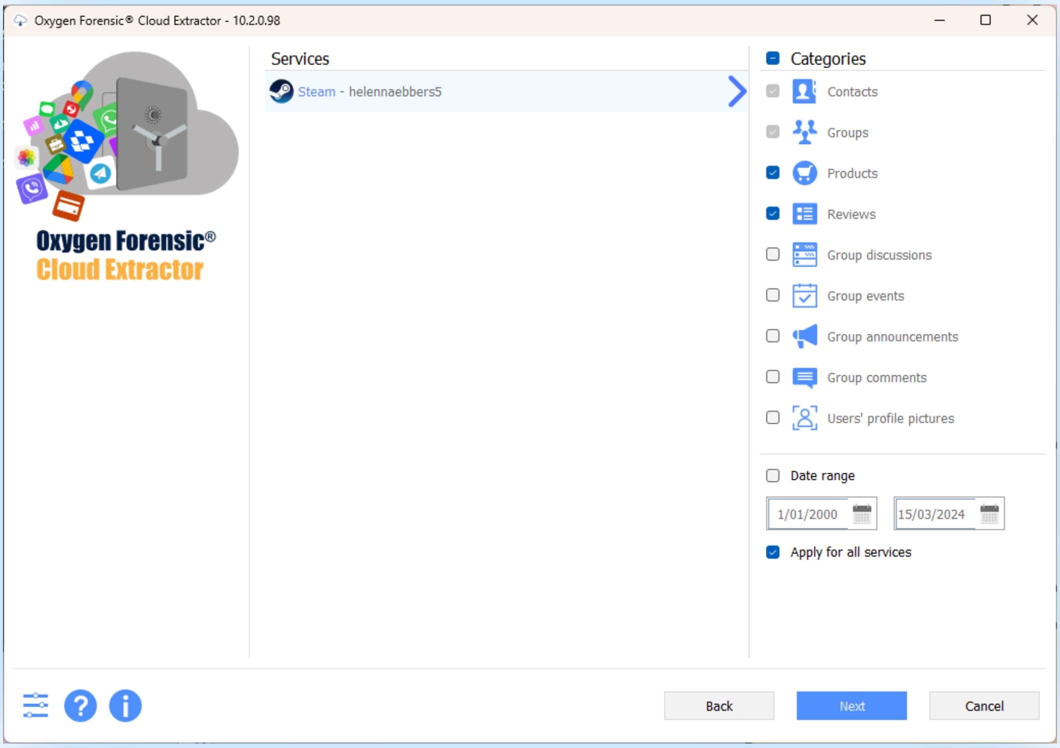
Extract full file system via checkm8 from iPads running iOS 16. The following models and iOS versions are supported:

- 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

Cloud Forensic 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 the account information, contacts, products, reviews, groups, group discussions, group events, group announcements, and group comments.



Services

Steam - helennaebbers5

■ Categories

- ☑ Contacts
- ☑ Groups
- ☑ Products
- ☑ Reviews
- □ Group discussions
- □ Group events
- □ Group announcements
- □ Group comments
- □ Users' profile pictures

□ Date range

1/01/2000 15/03/2024

☑ Apply for all services

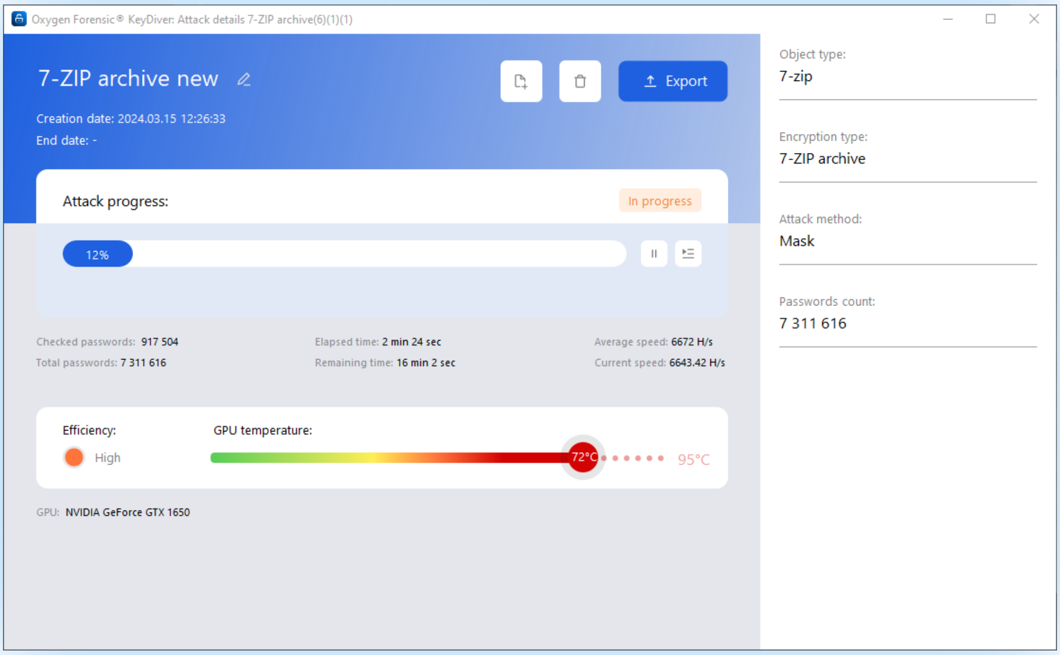
Computer Artifacts

Passcode brute force module

Enhanced Oxygen Forensic® KeyDiver capabilities to find passcodes to:

- encrypted iTunes backups
- encrypted 7-ZIP archives

Attack methods can be created using a dictionary, mask, or a user's personal data from an extraction.



Oxygen Forensic® KeyDiver: Attack details 7-ZIP archive(6)(1)(1)

7-ZIP archive new

Creation date: 2024.03.15 12:26:33
End date: -

Attack progress: In progress

12%

Checked passwords: 917 504
Total passwords: 7 311 616
Elapsed time: 2 min 24 sec
Remaining time: 16 min 2 sec
Average speed: 6672 H/s
Current speed: 6643.42 H/s

Efficiency: High

GPU temperature: 72°C 95°C

GPU: NVIDIA GeForce GTX 1650

Object type: 7-zip

Encryption type: 7-ZIP archive

Attack method: Mask

Passwords count: 7 311 616

Search by file signatures

Search Microsoft Office files by file signatures selecting this option in the Files tab of Oxygen Forensic® KeyScout. This feature might be useful when extensions of Microsoft Office files are altered or deleted by a user.

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 (mac-OS)

General

Enhanced Chats View

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

Import

Import of Apple Warrant Returns

Import and parse Apple Warrant Returns. Parsed data will include contacts, calendars, notes, messages, reminders, photos, iCloud Drive, Find My Friends, and other available data.

Other 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 Forensic® Detective.
- Import and parse VDI images of Android extractions.
- 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 might be useful if an investigator needs a basic report to kickstart an investigation or to compare the number of artifacts provided by different extraction methods.

Interested in trying out Oxygen Forensic® Detective v.16.2?

Request a free trial