



Oxygen Forensic[®] **Detective**

Release notes

Version 16.3
June 2024



The latest update to our flagship solution is here, Oxygen Forensic® **Detective** v.16.3. Key features include:

- Malware scan of extracted files
- Analysis of custom built drones
- Import of X (Twitter) archives
- Selective facial categorization
- Support for MT6750 and MT6855 chipsets

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

General

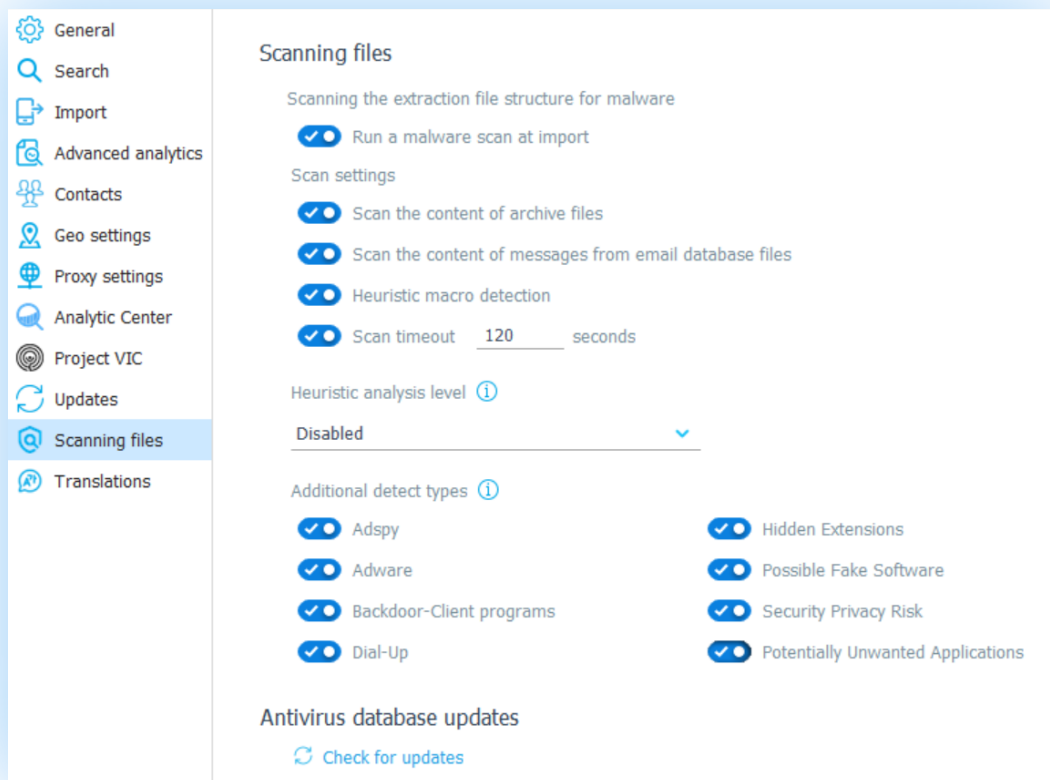
Malware scan of extracted files

The malware scan of extracted files and email databases is now available to all our users at no additional charge.

Identifiable threats include:

- Adspy
- Backdoor
- Constructor
- Dialer
- Dropper
- Exploit
- Heuristic
- Phishing
- Riskware
- Trash
- Trojware
- Virware
- Worm

After configuring the malware scan options in the Options section, you can initiate a malware scan in the Malware section of the selected extraction. The results will appear on the toolbar, displaying the scanned file status, identified threats, scan start time, and other relevant details.



Mobile Forensic Updates

Support for Snapdragon chipsets

We've added support for screen-locked Android devices based on the SDM665, SDM675, SDM730, and SDM855 chipsets. The list of supported devices includes many models released before 2020: Lenovo Z6 Pro, LG Q70, Sony Xperia 1, Xiaomi Mi A3, Xiaomi Redmi Note 7 Pro, Xiaomi Mi 9T, Xiaomi Mi 9, and many others.

Support for Omix and Reeder devices

Oxygen Forensic® Detective v.16.3 brings support for screen-locked Omix and Reeder devices based on the MTK and UNISOC chipsets.

New supported devices include:

- Omix X7
- Omix X5
- Omix X700
- Omix X600
- Reeder P13 Blue Max
- Reeder P13 Blue and other models.

Support for the MT6750 and MT6855 chipsets

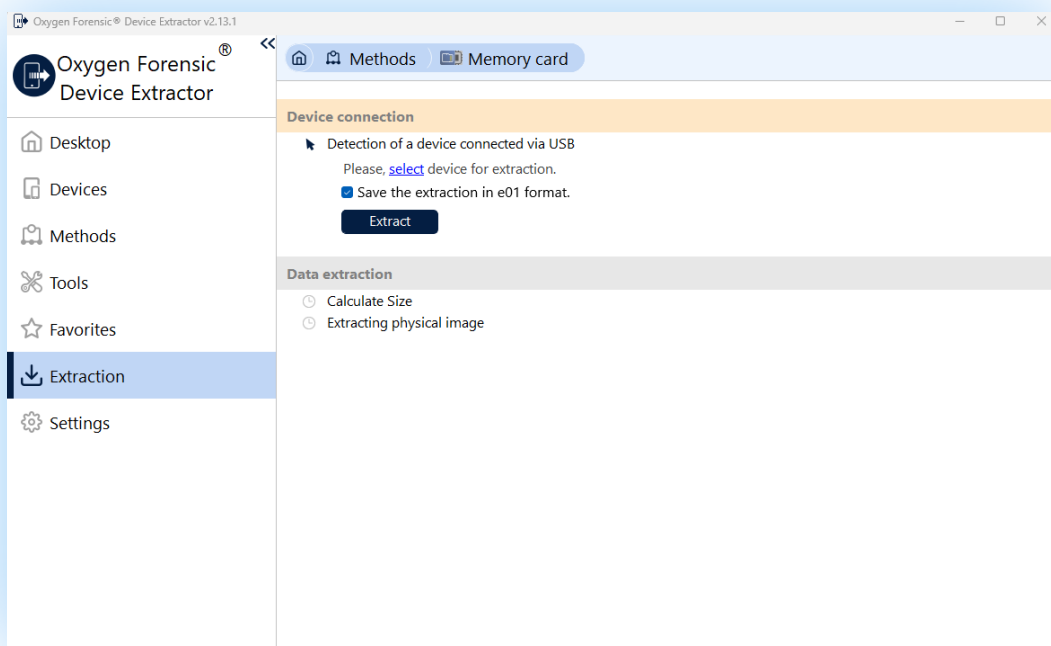
We've added support for screen-locked Android devices based on the MT6750 and MT6855 chipsets and running Android OS 10 and higher. This update covers 190 Android devices of various manufacturers.

Extraction of WhatsApp communities via Android Agent

Oxygen Forensic® Detective v.16.3 allows extraction of the communities from WhatsApp and WhatsApp Business via Android Agent. You can choose to extract all the communities or selected communities only.

Saving card memory dumps to E01

Now extracted physical dumps of memory cards can be saved to E01 format at the end of the extraction in Device Extractor.



Checkm8 method enhancements

Several enhancements have been made to this method:

- Now you can skip the necessity of switching a device to the Recovery Mode and switch it directly into DFU if the iOS version is known.
- We've also added the instructions on how to switch a device into DFU using test points.

Cloud Forensic Updates

Steam extraction enhancements

We've made two significant enhancements:

- Steam private and group chats can now be extracted.
- Authorization by scanning a QR code is added.

Computer Artifacts

Search plain text files by file signatures

In certain cases extensions of plain text files might be deleted or altered by a user. Oxygen Forensic® Detective v.16.3 introduces two options how these files can be identified:

1. Select the checkbox "Select file type by content" on the General tab of KeyScout.
2. Alternatively you can select the File signature option for plain text files on the Files tab of KeyScout.

The screenshot shows the 'New profile' dialog box with the 'Files' tab selected. The 'Rule Name' is 'Rule 1'. The 'Detecting matches' dropdown is set to 'Full match'. The 'File signature' dropdown is set to 'Text file', and the 'Plain text, INI, JSON, R...' dropdown is set to 'Plain text, INI, JSON, R...'. There is an 'Add rule' button at the bottom.

New artifacts

The following new computer artifacts are supported:

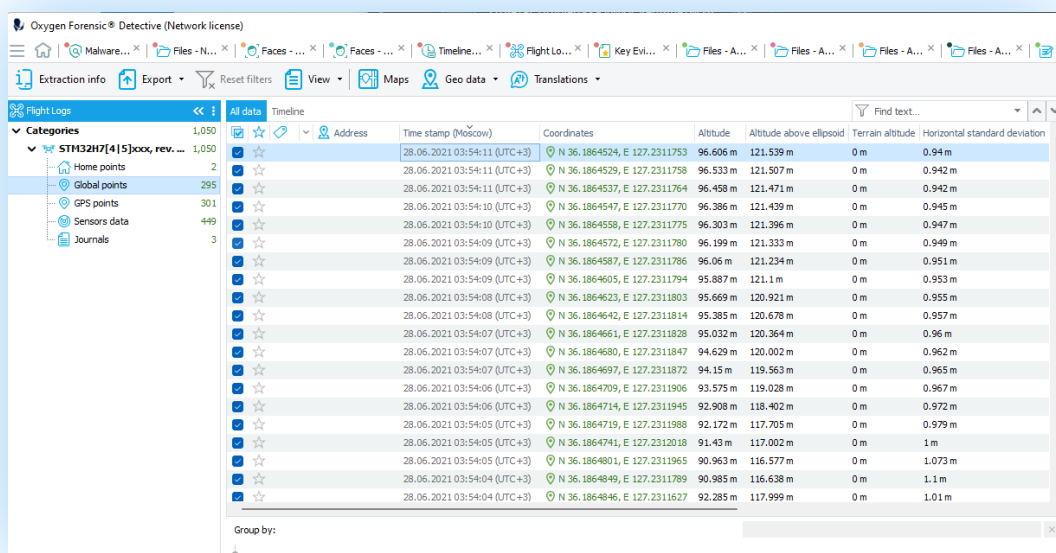
- List of installed applications from NTUSER.dat file (Windows)
- Information about packages installed by Pacman (GNU/Linux)
- Supported applications from the Arch Linux distribution
- Passwords from 1Password (Windows, macOS, GNU/Linux)

- Passwords from DuckDuckGo (macOS)
- Microsoft Defender (Windows)
- Transmission Torrent client (Windows, macOS, GNU/Linux)
- Microsoft Photos (Windows)
- Microsoft Sticky Notes (Windows)
- Apple Weather (macOS)
- Spark installed from the App Store (macOS)
- NordVPN installed from the App Store (macOS)
- Facebook Messenger installed from the App Store (macOS)
- Additional data from AnyDesk (Windows, macOS, GNU/Linux)
- Additional data from Opera (Windows, macOS, GNU/Linux)

Drone Forensic Updates

Analysis of custom built drones

PX4 Autopilot is an open-source flight control system oriented for drones and other uncrewed vehicles. Now you can analyze the flight history of custom built drones based on the PX4 controller by importing their ULog logs in Oxygen Forensic® Detective. Parsed data will include the drone information, home points, global and GPS points, sensors data and journals.



Categories	Count	Address	Time stamp (Moscow)	Coordinates	Altitude	Altitude above ellipsoid	Terrain altitude	Horizontal standard deviation
ST132H7[4]5xxx, rev. ...	1,050		28.06.2021 03:54:11 (UTC+3)	N 36.1864524, E 127.2311753	96.606 m	121.539 m	0 m	0.94 m
Home points	2		28.06.2021 03:54:11 (UTC+3)	N 36.1864529, E 127.2311758	96.533 m	121.507 m	0 m	0.942 m
Global points	295		28.06.2021 03:54:11 (UTC+3)	N 36.1864537, E 127.2311764	96.458 m	121.471 m	0 m	0.942 m
GPS points	301		28.06.2021 03:54:10 (UTC+3)	N 36.1864547, E 127.2311770	96.386 m	121.439 m	0 m	0.945 m
Sensors data	449		28.06.2021 03:54:10 (UTC+3)	N 36.1864558, E 127.2311775	96.303 m	121.396 m	0 m	0.947 m
Journals	3		28.06.2021 03:54:09 (UTC+3)	N 36.1864572, E 127.2311780	96.199 m	121.333 m	0 m	0.949 m
			28.06.2021 03:54:09 (UTC+3)	N 36.1864587, E 127.2311786	96.06 m	121.234 m	0 m	0.951 m
			28.06.2021 03:54:09 (UTC+3)	N 36.1864605, E 127.2311794	95.887 m	121.1 m	0 m	0.953 m
			28.06.2021 03:54:08 (UTC+3)	N 36.1864623, E 127.2311803	95.669 m	120.921 m	0 m	0.955 m
			28.06.2021 03:54:08 (UTC+3)	N 36.1864642, E 127.2311814	95.385 m	120.678 m	0 m	0.957 m
			28.06.2021 03:54:07 (UTC+3)	N 36.1864661, E 127.2311828	95.032 m	120.364 m	0 m	0.96 m
			28.06.2021 03:54:07 (UTC+3)	N 36.1864680, E 127.2311847	94.629 m	120.002 m	0 m	0.962 m
			28.06.2021 03:54:07 (UTC+3)	N 36.1864697, E 127.2311872	94.15 m	119.563 m	0 m	0.965 m
			28.06.2021 03:54:06 (UTC+3)	N 36.1864709, E 127.2311906	93.575 m	119.028 m	0 m	0.967 m
			28.06.2021 03:54:06 (UTC+3)	N 36.1864714, E 127.2311945	92.908 m	118.402 m	0 m	0.972 m
			28.06.2021 03:54:05 (UTC+3)	N 36.1864719, E 127.2311988	92.172 m	117.705 m	0 m	0.979 m
			28.06.2021 03:54:05 (UTC+3)	N 36.1864741, E 127.2312018	91.43 m	117.002 m	0 m	1 m
			28.06.2021 03:54:05 (UTC+3)	N 36.1864801, E 127.2311965	90.963 m	116.577 m	0 m	1.073 m
			28.06.2021 03:54:04 (UTC+3)	N 36.1864849, E 127.2311789	90.985 m	116.638 m	0 m	1.1 m
			28.06.2021 03:54:04 (UTC+3)	N 36.1864846, E 127.2311627	92.285 m	117.999 m	0 m	1.01 m

Import Updates

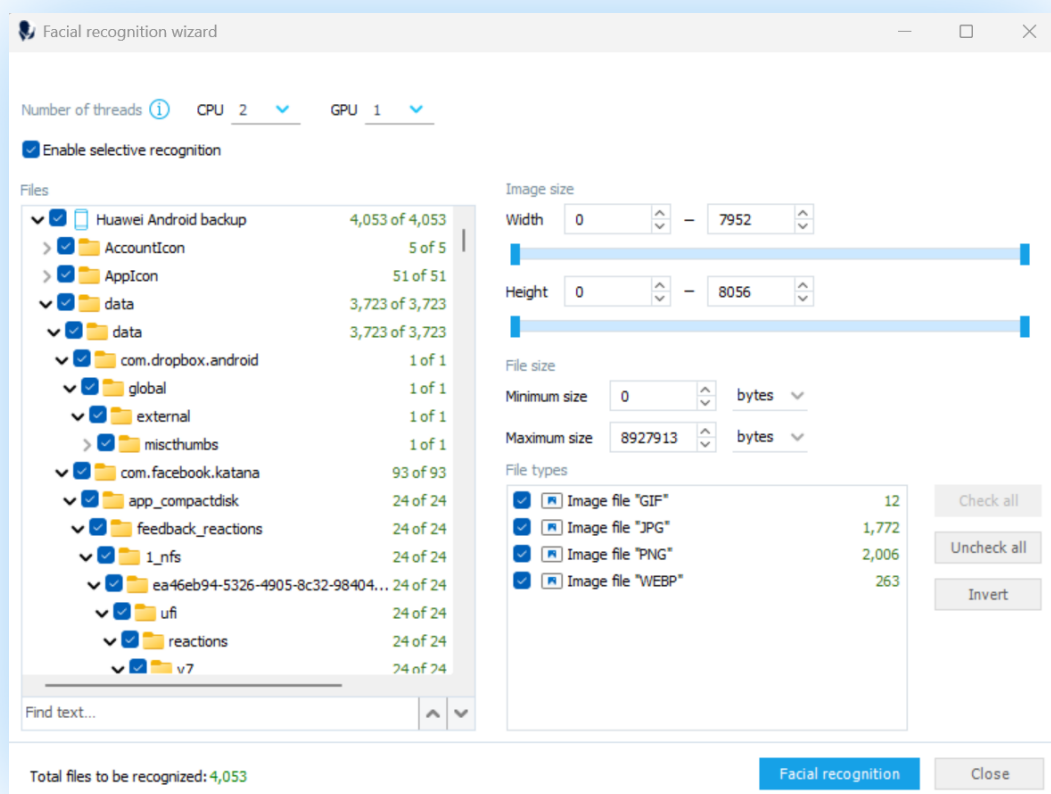
Import of X (Twitter) archives

Oxygen Forensic® Detective v.16.3 allows the import and parsing of X (Twitter) archives that can be downloaded following the official X [instruction](#). Parsed data will include contacts, group messages, direct messages, deleted tweets, followers, following, blocked users, search history, and other categories.

Data Analysis Updates

Selective facial categorization

We've added the Facial Categorization Wizard that allows the selection of specific file folders for facial categorization. With customizable file filter criteria encompassing file types, specific folders, and file sizes, this feature significantly speeds up the processing of files through our facial categorization engine.



Translation module updates

The following languages have been added to our Translation module:

- Romanian
- Estonian
- Lithuanian
- Latvian
- Norwegian
- Urdu
- Nepali
- Hebrew

Overall, 27 languages are now supported.

**Interested in trying out
Oxygen Forensic® Detective v.16.3?**

[Request a free trial](#)