OXYGEN FORENSICS

Oxygen Remote Explorer

Version 1.5 | June 2024

Release notes

Oxygen Remote Explorer v.1.5 is here

Key features include:

- Malware scan of extracted files
- Remote RAM capture
- Utility for server configuration
- Import of X (Twitter) archives
- Updated support for Google cloud services

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

General

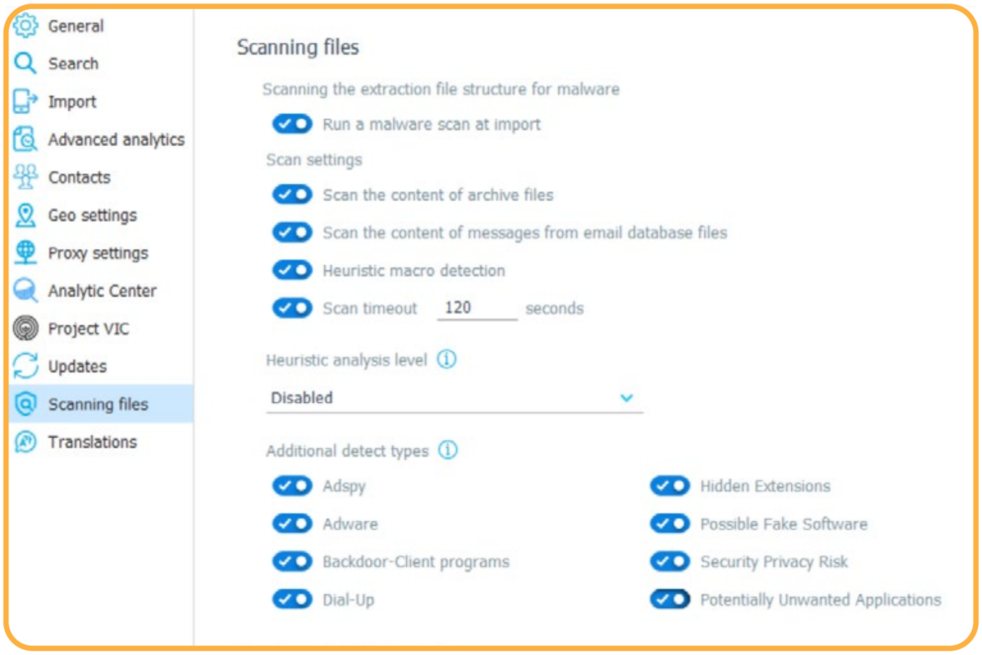
Malware scan of extracted files

The ability to scan extracted files and email databases for malware is now available to all 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.



Scanning files

Scanning the extraction file structure for malware

- ✓ Run a malware scan at import

Scan settings

- ✓ Scan the content of archive files
- ✓ Scan the content of messages from email database files
- ✓ Heuristic macro detection
- ✓ Scan timeout 120 seconds

Heuristic analysis level ⓘ

Disabled

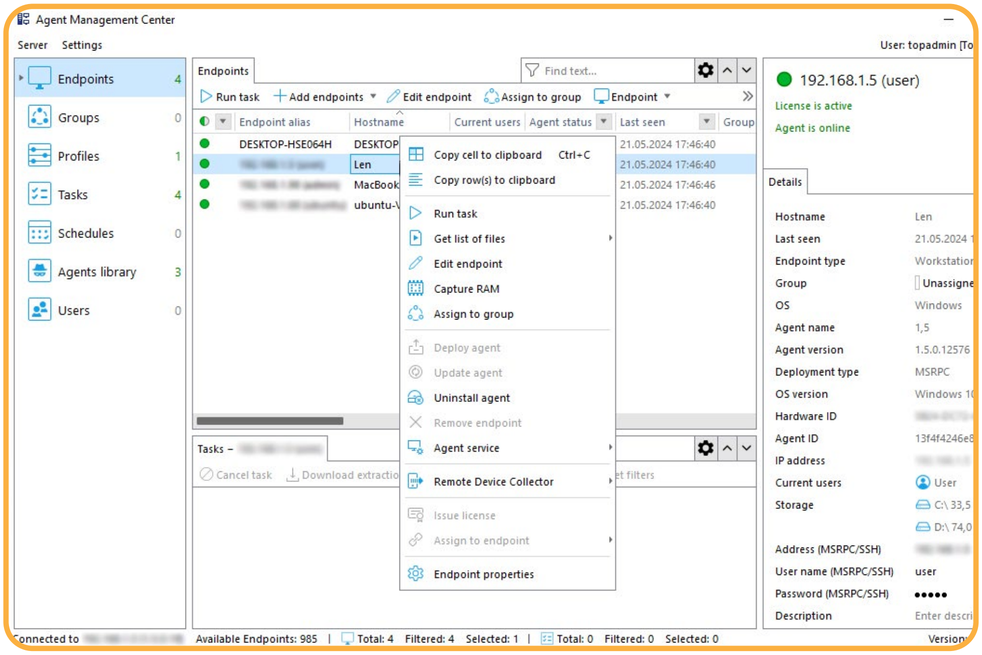
Additional detect types ⓘ

- ✓ Adspy
- ✓ Adware
- ✓ Backdoor-Client programs
- ✓ Dial-Up
- ✓ Hidden Extensions
- ✓ Possible Fake Software
- ✓ Security Privacy Risk
- ✓ Potentially Unwanted Applications

Agent Management Center Updates

Remote RAM capture

You can now create a Windows OS memory dump remotely using the Agent Management Center. To do this, right-click the endpoint of which you need a memory dump and select “Capture RAM” in the list. A dump will be created on the endpoint and then sent to the server. Then, you can download it from the server and use a third-party tool for a dump analysis.



Endpoint alias	Hostname	Current users	Agent status	Last seen	Group
DESKTOP-HSE064H	DESKTOP			21.05.2024 17:46:40	
[redacted]	Len			21.05.2024 17:46:40	
[redacted]	MacBook			21.05.2024 17:46:46	
[redacted]	ubuntu-\			21.05.2024 17:46:40	

192.168.1.5 (user)

License is active

Agent is online

Hostname	Len
Last seen	21.05.2024 1
Endpoint type	Workstatior
Group	Unassigne
OS	Windows
Agent name	1,5
Agent version	1.5.0.12576
Deployment type	MSRPC
OS version	Windows 1(
Hardware ID	[redacted]
Agent ID	13f4f4246e8
IP address	[redacted]
Current users	User
Storage	C:\ 33,5 D:\ 74,0
Address (MSRPC/SSH)	[redacted]
User name (MSRPC/SSH)	user
Password (MSRPC/SSH)	●●●●●
Description	Enter descri

Connected to [redacted] Available Endpoints: 985 | Total: 4 Filtered: 4 Selected: 1 | Total: 0 Filtered: 0 Selected: 0

Utility for server configuration

Now you can conveniently configure the server settings in the utility that is installed together with the server and is available in system tray. You can choose the parameters for the server connections, logging, extraction repository, and backup there. Previously, the server settings could be configured only by editing the Config file.

Logging Agents’ work

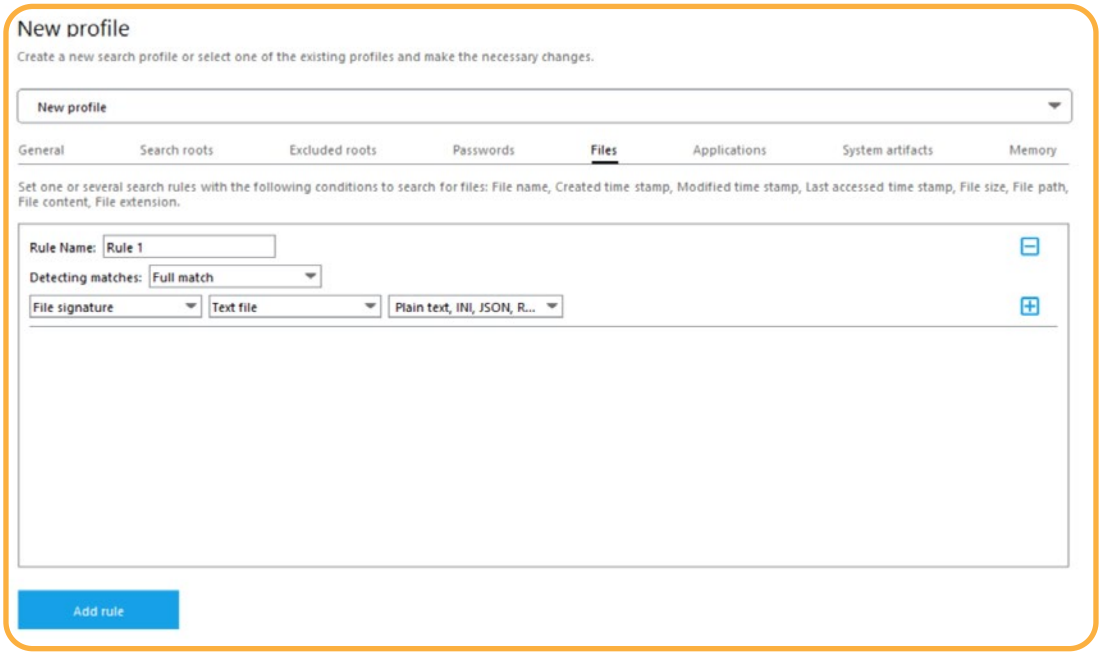
We’ve added the ability to configure logging of Agents’ work. Right click the endpoint and select the Endpoint setting in the list. In the opened window you can set the logging level, and remove and compress intervals.

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 Remote Explorer v.1.5 introduces two options for identifying files:

1. Choose the “Select file type by content” box 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.



New profile

Create a new search profile or select one of the existing profiles and make the necessary changes.

New profile

Set one or several search rules with the following conditions to search for files: File name, Created time stamp, Modified time stamp, Last accessed time stamp, File size, File path, File content, File extension.

Rule Name: Rule 1

Detecting matches: Full match

File signature | Text file | Plain text, INI, JSON, R...

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)

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

Cloud Forensic Updates

Updated support for Google services

We've added the new authorization algorithm for all the supported Google services. Now you can again access Google Drive, Google Mail, Google Admin, and other supported services.

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 include 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 Remote Explorer v.1.5 brings support for screen-locked Omix and Reeder devices based on the MTK and UNISOC chipsets.

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 Remote Explorer v.1.5 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 instructions on how to switch iPhone devices into DFU using test points.

New apps

We've added support for the following artifacts:

- SD card files from external.db (Android)
- Keyboard activity (iOS)
- Control Center activity (iOS)
- Element Messenger (iOS)

Import

Import of X (Twitter) archives

Oxygen Remote Explorer v.1.5 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

Translation module updates

The following languages have been added to our Translation module: Estonian, Hebrew, Latvian, Lithuanian, Nepali, Norwegian, Romanian, and Urdu. Overall, 27 languages are now supported.

Interested in finding out more about Oxygen Remote Explorer?

Schedule a Demo