Oxygen Forensic® DETECTIVE

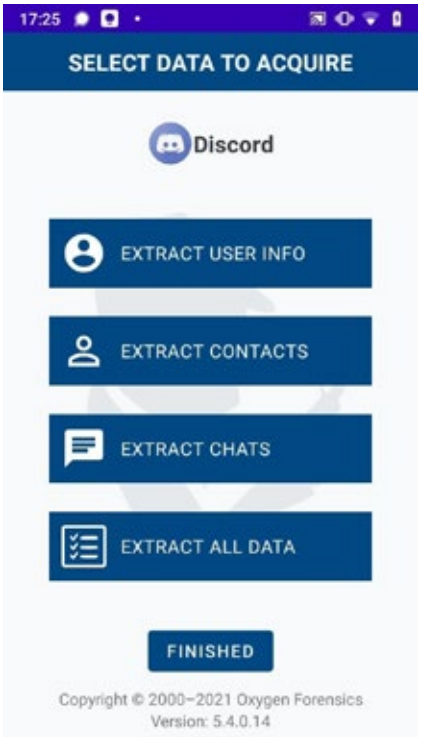
version 13.4 MARCH 2021

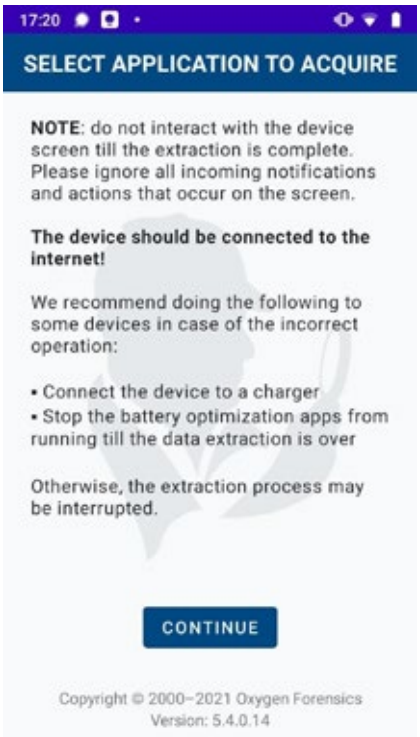
New Method for Discord Extraction

MOBILE FORENSICS

In addition to the direct extraction of Discord app data from Apple iOS and Android devices, there is now one more method available in our software. Oxygen Forensic® Detective v.13.4 will allow Discord data extraction from any unlocked Android device via OxyAgent. To do this, install OxyAgent on a device, choose Discord in the "Extract third-party applications data" menu, and follow the instructions. Once data is collected, import it into Oxygen Forensic® Detective. Investigators can expect the following artifacts: account info, contacts, private chats, group chats, and channels.

Please note, this OxyAgent method is also compatible with WhatsApp, WhatsApp Business, and Signal Messenger, using any unlocked Android device.





Hash Calculation for Imported Images

MOBILE FORENSICS

Image hashing is critical to preserving the integrity of digital evidence. Investigators now have the ability to calculate hash values for images.

Hash may be calculated for following extraction types:

- Android physical images: .ewc, .zip or .bin (1 file without extension or multi select from open-dialog)
- iTunes backup (.zip)
- Android or Apple Tarball file system (.zip)
- Android backup: .ab, .ewc
- Memory card physical image (.bin)
- Memory card file system (.zip)

Enhanced Support for MTK Devices

MOBILE FORENSICS

Oxygen Forensic® Detective v.13.4 provides enhanced support for Android devices with MTK chipsets. Previously our software offered physical extraction of MTK-based Android devices with T6 and Microtrust versions of TrustZone. In version 13.4, we've added support for the RSEE version and improved support for the T6 version. This means investigators can now bypass screen locks and extract evidence from many more Android devices based on MT6739, MT6737 and MT6580 chipsets. To do this, select the "Physical MTK image" method in Oxygen Forensic Extractor.

TikTok and Discord Cloud Data

CLOUD FORENSICS

To access TikTok data from the cloud, investigators need to use either the phone number, login credentials, or Google credentials. If 2FA is set, investigators will receive a code at the connected phone number or email address. Evidence sets will include account details, contacts, login history, wallet, notifications, chats, posts, and favorites.

Authorization in Discord is available using login credentials or a token found on Windows and macOS by Oxygen Forensic® KeyScout. If 2FA is enabled, investigators will be sent an SMS or authenticator code. Discord cloud extractions will include account info, contacts, chats, channels, and other available data.

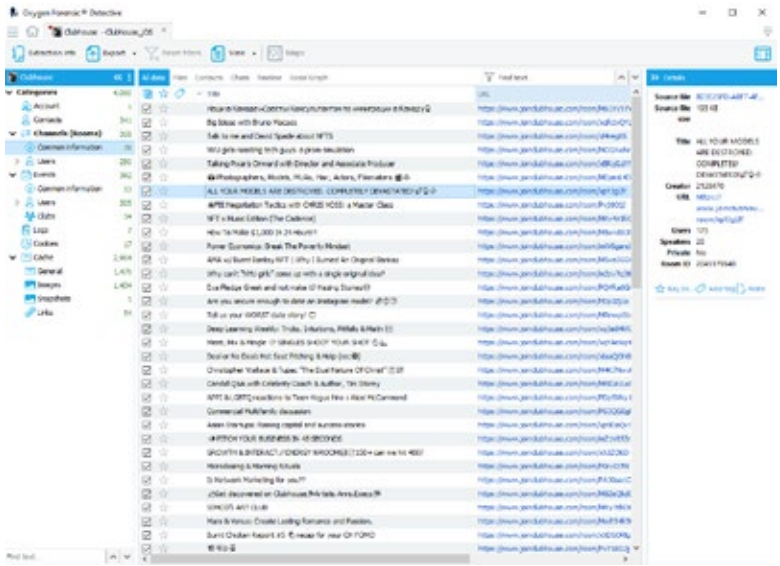
The new Oxygen Forensic® Cloud Extractor introduces updated authorization algorithms for SecMail and Amazon Alexa services.

New App Support

MOBILE FORENSICS

Oxygen Forensic® Detective v.13.4 brings support for four new apps and updates data parsing for many already supported apps. Let's see what's new:

- **Clubhouse** - A popular social network for drop-in audio conversations. For data extraction, we recommend using checkm8 vulnerability in Oxygen Forensic® Detective. Investigators will be able to extract the account info, contacts, channels, events, clubs, logs, cookies, cache, and other available data.
- **Lime and Bird** - Scooter and bike-sharing apps. The number of artifacts acquired will depend on the extraction method and the device OS. Extractions may include account info, vehicles, rides, balance history, nearby parking, cache, cookies, and more.
- **Steam Mobile** - In response to our customers, we've added support for this messenger. Evidence sets will consist of account info, contacts, chats, cookies, and cache.
- **Yahoo Mail** – We've added complete data parsing for Apple iOS devices and updated support for Android devices.



Data Export Enhancements

GENERAL

Oxygen Forensic® Detective v.13.4 now allows investigators to set multiple date and time filters when exporting data to external formats. Additionally, we've significantly sped up the overall data export process.

New Computer Artifacts

COMPUTER ARTIFACTS

The updated Oxygen Forensic® KeyScout can collect a variety of great, new artifacts. Let's take a look.

- Import and parsing of AccessData AD1 logical images made from Windows, macOS, and Linux computers.
- User data collection from GroupMe, Microsoft Mail, and Internet Explorer.
- New Windows System artifacts include information about logon sessions, system resource usage, installed updates, pending renames, and deleted files.
- New macOS system artifacts include information about installed apps, logon sessions, and terminal history sessions.

Global Search in SQLite databases

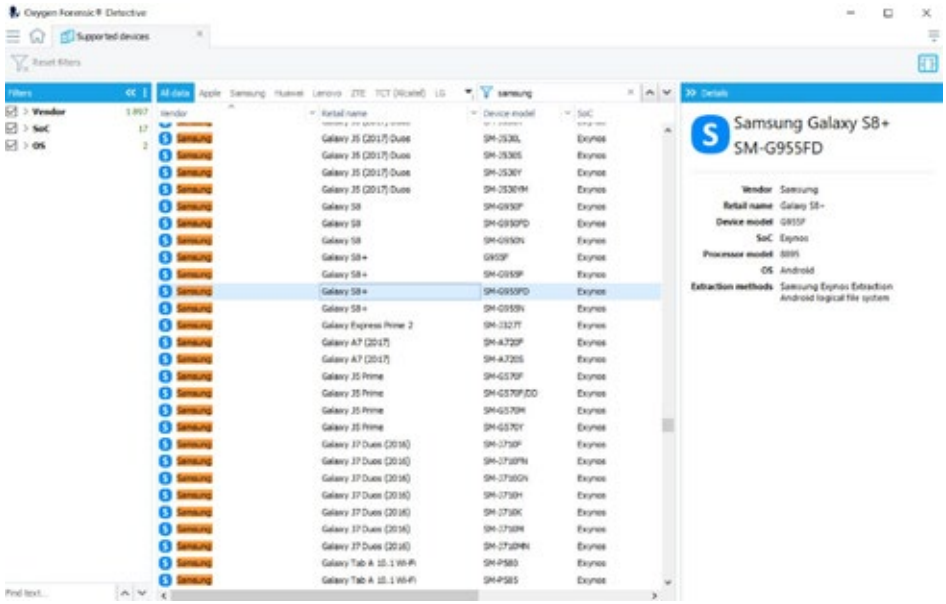
GENERAL

In the Viewer for SQLite databases, investigators can now run a search through all or selected database tables. There are various options for search criteria that can be applied. For example, investigators have the ability to search in text, number, or binary fields.

Supported Devices List

GENERAL

Investigators can now instantly check if a device is supported in Oxygen Forensic® Detective. Go to the Options menu, click "Supported Devices" for the complete list of supported devices and the extraction methods available for each.



Resolved issues

- Time zone could not be changed from UTC in the Contacts section
- Refreshing the Duplicates panel in the Files section
- After Email (IMAP) cloud extractions, unread emails were marked as read
- Occurred during Nandroid TWRP and CWM backup import
- Smart Filter did not work in Timeline
- Not all menu options were shown in OxyAgent on Android devices with low-resolution screens
- Date/time filter did not work for the drone flight logs
- Data parsing of iTunes backup made from iPhone 11
- Occurred after applying filters in the Social Graph section.
- Birthday date parsing in the Contacts section of Facebook Messenger (Android).
- "To" column was incorrectly displayed in Snapchat (Android).
- Device information was not parsed from com.apple.preferences.plist from OFBR backups.