Oxygen Forensic® DETECTIVE

version 13.0 SEPTEMBER 2020

38,611	86	562	18,000+	83
devices	cloud services	unique apps	app versions	computer artifacts

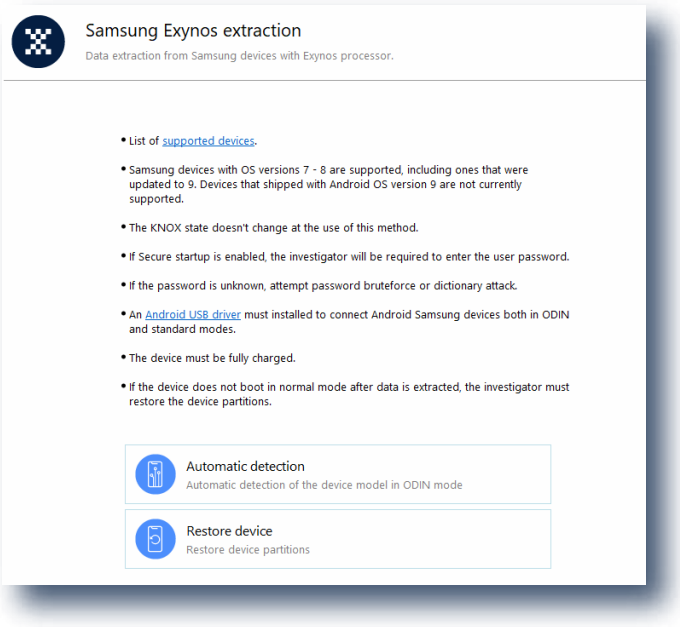
Physical acquisition of Samsung Exynos devices

MOBILE FORENSICS

Oxygen Forensic® Detective 13.0 introduces the ability to bypass screen locks, perform physical acquisitions, and decrypt data from Samsung devices based on Exynos chipsets. The functionality is available for Samsung devices running Android OS 7, 8, and 9 and covers 76 different device models. If a Samsung device is not supported investigators can request support directly from the Oxygen Forensic Detective interface.

Oxygen Forensic® Detective can perform physical acquisitions without updating the KNOX counter. If Secure startup is enabled on a device, the software offers the unique opportunity to brute force the passcode and decrypt the extracted physical dump.

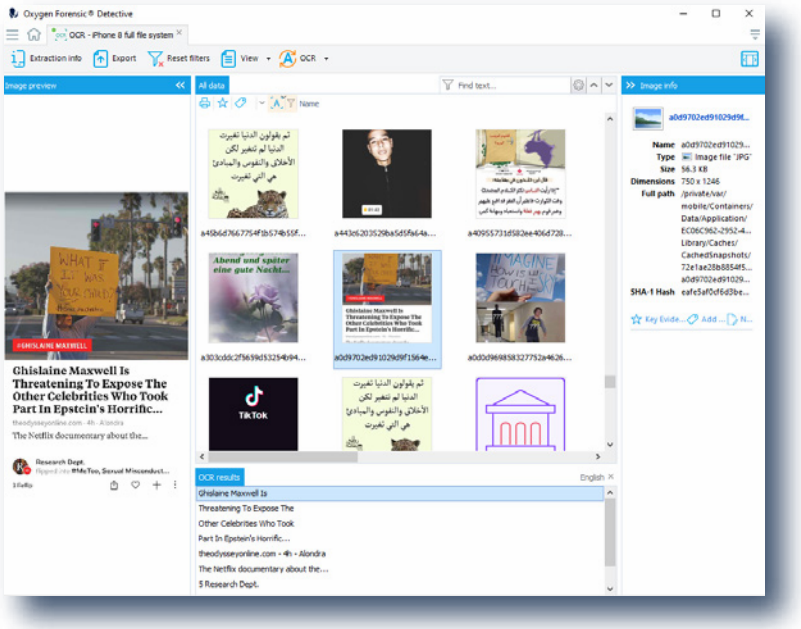
Exynos is the 5th chipset supported by Oxygen Forensics' screen lock bypass methods. The others are Kirin, MTK, Qualcomm, and Spreadtrum.



Optical Character Recognition

DATA ANALYSIS

Investigators no longer have to spend time manually transcribing text within a picture. Oxygen Forensic® Detective 13.0 includes a new OCR section, which allows investigators to easily convert any words contained in a screenshot or photo to machine-encoded text. To enable and configure this feature, go to Options/Advanced Analytics in the software. Then, in the OCR section, run image OCR by pressing the relevant button on the toolbar. Once OCR has been run investigators can use the quick filter to search for text in many different languages across the processed images.



Support for new cloud services

CLOUD EXTRACTOR

Our total number of supported cloud services now equals 86! We've enhanced support for many of our existing cloud services, as well as added 3 new clouds to our catalogue.

- **Zoom.** Access the Zoom cloud using login credentials or a token found in Apple iOS and Android devices. Extracted evidence will include the account information, contacts, chats and conferences.
- **Huawei Cloud Backups.** Besides the already supported Huawei Cloud Data services, now there is an opportunity to extract complete Huawei Cloud Backups using login credentials, a token, QR code, or SMS code.
- **Firefox Lockwise.** Access to this service is available via login credentials or a token found in Apple iOS devices. Investigators can extract the account information, as well as saved logins and passwords.

Support for new computer artifacts

COMPUTER ARTIFACTS

This update comes with an improved Oxygen Forensic® KeyScout, which is now able to collect more new artifacts from computers. First, it allows investigators to extract all available user data from Telegram Desktop, Skype, Drobox, WhatsApp Desktop, and Google Sync on Windows and macOS.
Second, investigators can extract several new system files such as $MFT files that contain information about the NTFS file system, Events from the Windows registry, and Prefetch files that contain information on what apps have been run on the PC. In addition, there is an opportunity to run KeyScout with Admin rights to gain low level access to Windows drives and, thus, to more complete information. Lastly, all the extracted system files are not shown in System Artifacts section in Oxygen Forensic® Detective.

Enhanced support for WhatsApp

MOBILE FORENSICS

We have added two improvements to our WhatsApp extraction methods.

- Using an installed OxyAgent, investigators can now collect additional data from Android devices, such as audio and video calls, full information about contacts participating in group chats, contact pictures, and more.

- The new decryption method for WhatsApp iCloud and WhatsApp Google allows backups to be decrypted using a WhatsApp Cloud token. This WhatsApp Cloud token decrypts any WhatsApp backups associated with the same phone number. After the WhatsApp Cloud service is used, this token is automatically saved in the software.

Import of Meiya Pico extractions

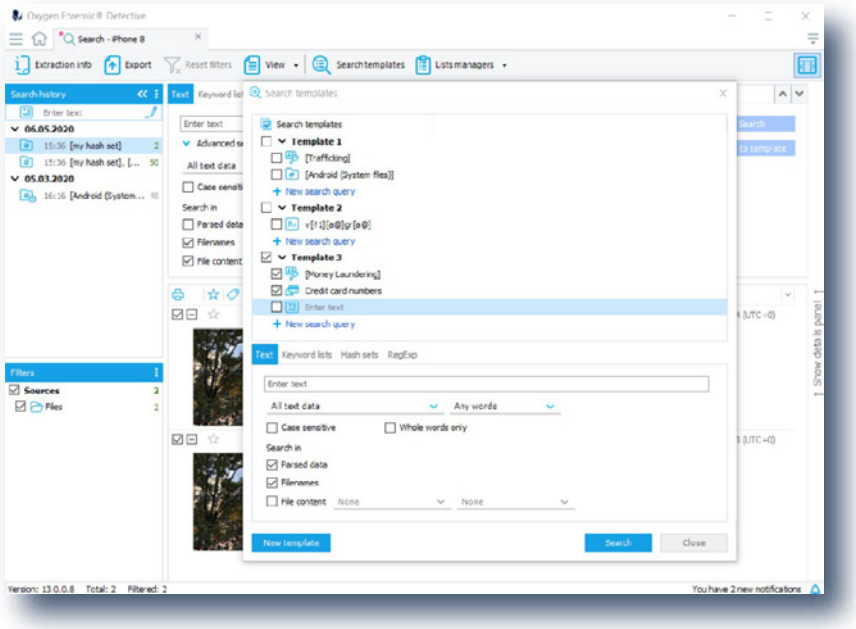
MOBILE FORENSICS

Investigators can now import and analyze extractions created by Meiya Pico's mobile forensic tool for both Apple iOS and Android devices. Oxygen Forensic® Detective will fully parse all data available in Meiya Pico backups.

Search templates

DATA ANALYSIS

Investigators can search for data more quickly using Search Templates. These templates can contain any supported search criteria, including RegEx, Keywords, Hash Sets, Text, etc. Searches can be done for parsed data, file names, or file content. Users have the ability to create their own Search Templates, which can later be saved in the Search section.



Device support

MOBILE FORENSICS

We have added support for over 500 new Android devices: Oysters AntarcticE, Xiaomi Mi 10 Lite_5G, ZTE BLADE V8 MINI, Samsung Galaxy Tab S7_ 5G, Samsung Galaxy Note20 Ultra 5G, Samsung Galaxy Z Fold2 5G, Samsung Galaxy Z Flip 5G, etc. The total number of supported devices is 38,611.

App support

MOBILE FORENSICS

Oxygen Forensic® Detective 13.0 brings support for a couple of new apps that include Zynn, Google, Firefox Lockwise and Gallery Vault as well as updates data parsing from over 800 new app versions from Apple iOS and Android devices. The total number of supported versions now exceeds 18,000.