OXYGEN FORENSIC® DETECTIVE 11.3

APRIL 2019

PARROT DRONE DATA FROM CLOUD

In Oxygen Forensic® Detective 11.2 we added the ability to import and parse Parrot's flight logs extracted from either an installed mobile app and also a drone physical dump. In our newest release we deliver groundbreaking technology to extract complete flight history data from the My Parrot Cloud.

Access to My Parrot cloud can be obtained either via login/password or token. Our built-in and included KeyScout utility can detect and extract a login and password if previously entered in a web browser on a PC. More importantly, Oxygen Forensic® Detective can extract the token to the My Parrot Cloud in the installed FreeFlight apps on both Apple iOS and Android devices. Currently My Parrot Cloud does not utilize 2-factor authentication so the extraction of the cloud data is effortless.

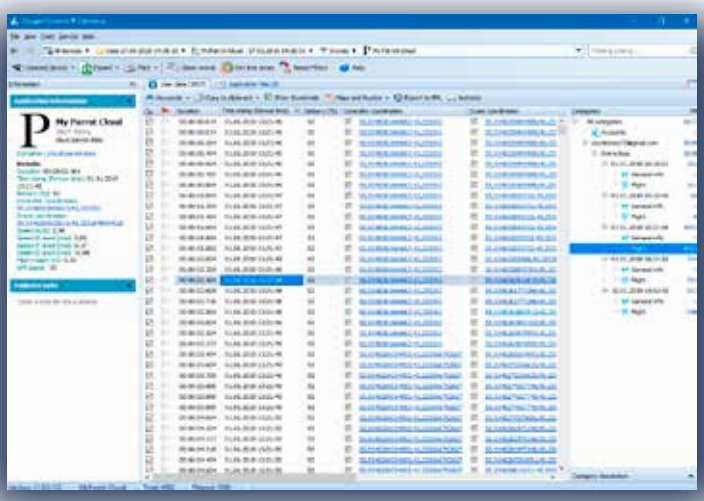
The My Parrot Cloud evidence set includes information about the account, general information about the flight and detailed flight history including metadata like speed, altitude, battery level, Wi-Fi signal, and more. Currently this exclusive method provides investigators with the most comprehensive flight history from Parrot drones on the market. But this is not all - Oxygen Forensic® Detective now parses and decodes all available drone data from FreeFlight 6 app from Apple iOS and Android devices.

MTK PHYSICAL DUMP DECRYPTION

Modern Android devices based on Mediatek chipsets can be encrypted using hardware bound keys. Without obtaining these keys device physical images cannot be decrypted, even if the default password or a custom one is known. In our previous versions of Oxygen Forensic® Detective we allowed investigators to decrypt physical dumps of older MTK devices that required no hardware bound keys. However, in Oxygen Forensic® Detective 11.3 investigators can now extract hardware bound keys from a mobile device and use them for physical dump decryption.

Now investigators can connect a locked or unlocked MTK device, do a physical dump and automatically extract hardware bound keys. With these keys the extracted data can now be decrypted with a default password. If Secure Startup was enabled, and user password set, an investigator will have to enter the known password in a special field. Password brute force will be added in a subsequent release.

Oxygen Forensic® Detective supports this industry's only decryption method for the majority of Android devices based on Mediatek MT6737 chipset but the list of supported chipsets will continue to grow.



65 cloud services

27146 unique devices

461 unique apps

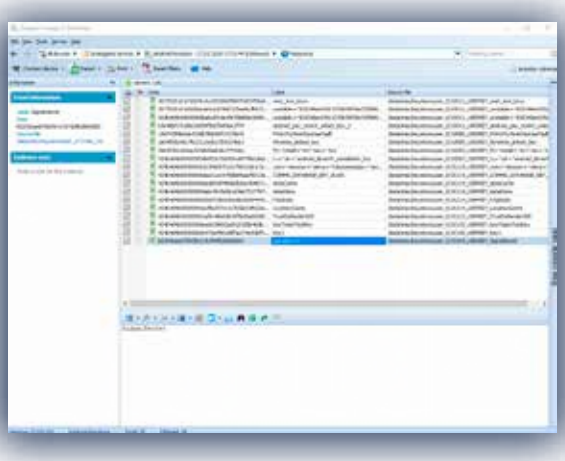
9671 app versions

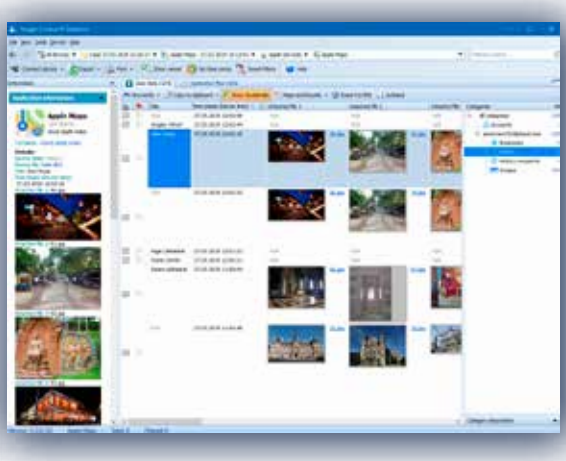
ANDROID KEYSTORE DECRYPTION

The Android Keystore system let users securely keep cryptographic keys. Much like the iOS Key Chain, some applications, like Signal, Threema, Amazon Alexa, and many others store their encryption keys in the Android Keystore. Oxygen Forensic® Detective 11.3 now extracts and decrypts all the available encryption keys and displays them in Passwords section. With access to these keys, our software now automatically decrypts Signal Messenger data including all the chats. The list of apps decrypted with the Android KeyStore keys will continue to grow.

APPLE MAPS FROM CLOUD

Apple Maps is the default map system installed with all Apple iOS devices. Classic logical extraction via iTunes backup procedure does not return Apple Map data since it is not included in the standard backup. The only current extraction method for this data would be using GrayShift's GrayKey or extraction of a jailbroken Apple iOS until now. Oxygen Forensic® Detective 11.3 now offers an alternative method of Apple Maps data extraction from iCloud using login/password or token acquired directly from an Apple iOS device logical extraction.



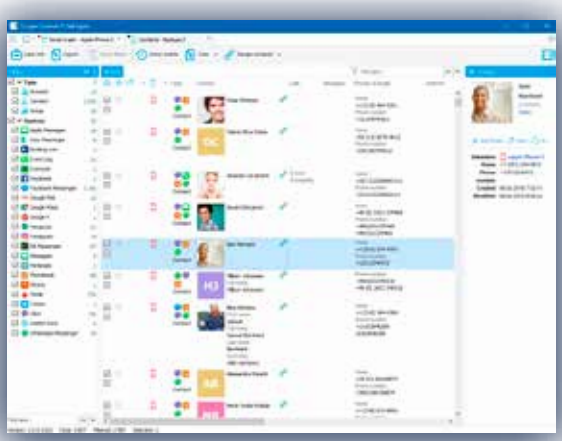


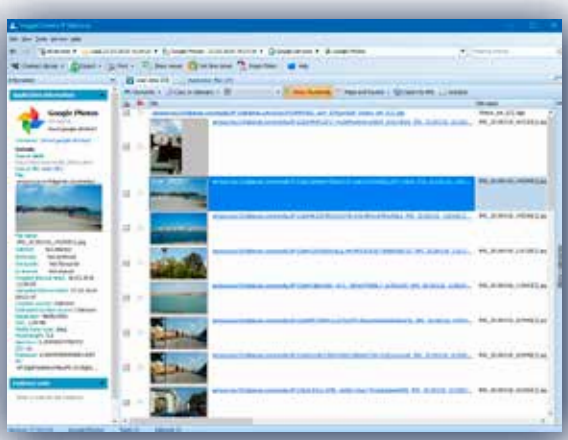
JETENGINE IMPROVEMENTS

Continually improving our included JetEngine module which allows data parsing and analysis at record speed is a priority. The included updated version offers analysis of complete DJI RAW Logs extracted from DJI physical dumps and the DJI Assistant app. With massive improvements in every release the new JetEngine now provides the ability to build a Social Graph for multiple extractions, merge similar contacts using custom settings, conveniently view JSON and XML files in a separate tab and export data to XML. For a full list of new features please refer to the WhatsNew document.

GOOGLE MAPS UPDATE

For 11.3 we've significantly updated Google Maps extraction from the associated cloud account. This valuable data can now be accessed via login/password or master token extracted from an Android device. The updated Oxygen Forensic® Detective now extracts much more data that includes: the account details, contact list, information about albums and comments to them, private and public photos with complete metadata. Also, geo coordinates extracted from Google Photos can be immediately opened in the built-in Maps module.





APPLICATIONS

iOS

Facebook (210.0)

Freeflight Pro (5.2.4)

Freeflight 6 (6.4.2)

Google Photos (4.10)

OK (7.50.1)

Telegram (5.4.1)

Telegram X (5.0.17)

WhatsApp (2.19.30)

Viber (10.3)

VK (5.9.1)

Yandex.Disk (2.68)

Yandex.Taxi (4.66)

ANDROID

Freeflight Pro (5.2.4)

Freeflight 6 (6.4.1)

Google Photos (4.10)

OK (19.3.26)

Signal (4.35.3)

Telegram (5.3.1)

WhatsApp (2.19.86)

Viber (10.3)

VK (5.24)

Yandex.Disk (4.08)

Yandex.Taxi (3.89)

Yahoo! Mail (5.36.0)

And many others!