OXYGEN FORENSIC®

DETECTIVE 11.0

OCTOBER 2018

USE NEW WHATSAPP EXTRACTION METHOD

WhatsApp is without doubt the most popular messenger in the world with over 1.5 billion users globally. Thus, extracting complete WhatsApp content from all possible sources is essential for any investigation.

Commonly used methods of WhatsApp data acquisition involve extracting data from mobile devices and their cloud backups. Oxygen Forensic® Detective v.11 introduces an industry-first alternative method of WhatsApp data extraction.

In the new software version, you can access complete WhatsApp data by scanning a QR code from a mobile app or using the WhatsApp token from a PC. This token can be extracted by our KeyScout utility from the WhatsApp desktop app or from desktop Web browsers.

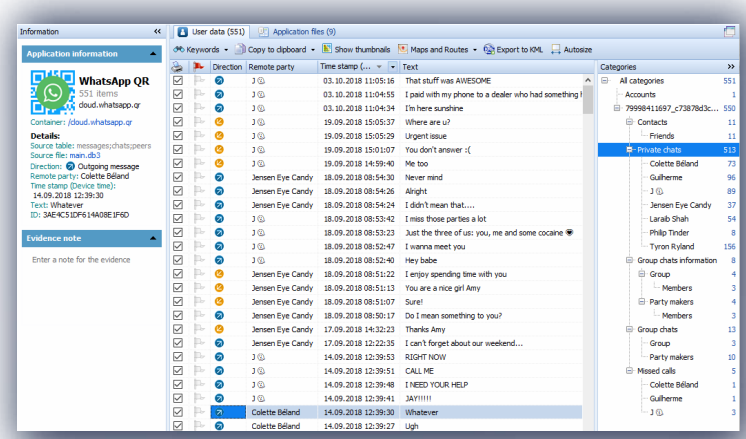
Once data is extracted, you will be able to download WhatsApp communications from the subject's account any time later when an investigation requires by using a specially generated WhatsApp QR token available in the Cloud Accounts section of Oxygen Forensic® Detective.

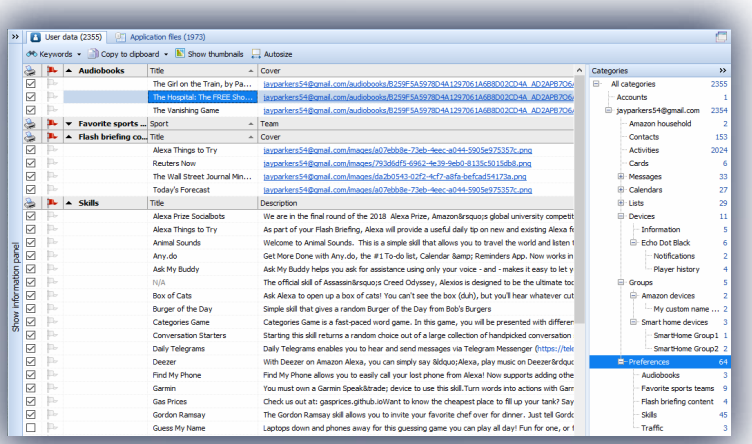
AQCUIRE IOT DEVICES

Digital assistants are already a part of everyday life and have been successfully used to solve several crimes. Oxygen Forensic® Detective v.11 brings support for the two most popular digital assistants – Amazon Alexa and Google Home.

You can access Amazon Alexa cloud using a username and password or token. A token can be found on the device's associated computer with Oxygen Forensic® KeyScout and used in Cloud Extractor. The software acquires a complete evidence set from Amazon Alexa, including account and device details, contacts, messages, calendars, notifications, lists, activities, skills, etc.

Google Home data can be extracted via Google username/password or a master token found in mobile devices. Extracted Google Home data includes account and device details, voice commands, and information about users.Google Home data can also be acquired from the Google Home mobile app on Apple iOS and Android devices.





55 cloud services

20300+ unique devices

440+ unique apps

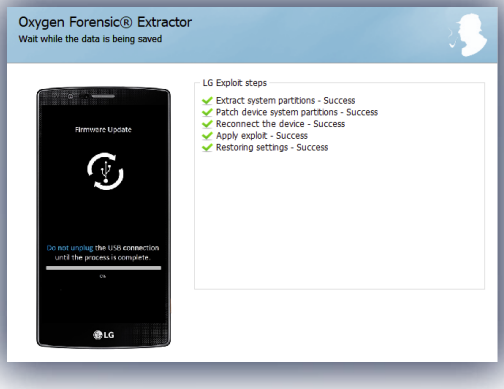
8300+ app versions

BRUTEFORCE LG DUMPS

Many modern Android devices have an encrypted user partition, which often makes a physical extraction useless. An encrypted dump at the end of acquisition requires an investigator to find another solution to decrypt it.

In our new Oxygen Forensic® Detective, we introduce the industry-exclusive opportunity to brute force and decrypt encrypted user partitions of LG devices. How does it work? You extract an LG device in DFU mode and, once a physical dump is created, you are prompted to apply a special exploit and brute force the encrypted user partition using the built-in Passware module.

Currently we support LG G5 and V10 devices, but the number of supported devices will grow in future releases.

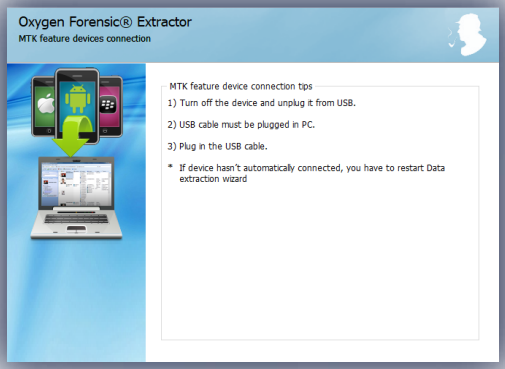


EXTRACT SMARTWATCHES

The popularity of smartwatches is growing, so we've added the ability to extract data from smartwatches based on MediaTek chipsets.

Oxygen Forensic® Detective performs logical acquisition of MTK smartwatches and allows forensic experts to extract device model, contacts, calls, messages, multimedia files, and other data.

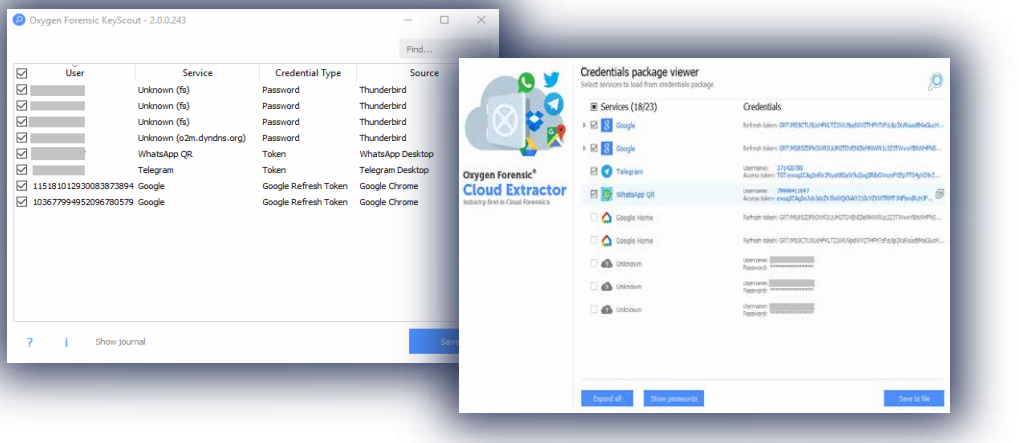
Currently over 30 smartwatch models are supported, including Kobwa K2BB-033, Leealra m26 Smart Bluetooth Watch, Leegoal T58, Meixunda T58, Ordro T58, Rosimee Q50, TAILHOO Y3, Vwar w58, Xiaomi Mi Bunny Watch Q, Zeblaze Smartwatch, and others.



FIND MORE CREDENTIALS ON PC

The updated Oxygen Forensic® KeyScout detects a wide range of new credentials and tokens on a subject's computer. The new version finds the WhatsApp QR token in WhatsApp desktop app and in Web browsers. It also detects Amazon Alexa and Telegram tokens in Web browsers as well as the Google Refresh token in Google Chrome browser. All tokens can be saved as an OCPK file to be opened and used in Oxygen Forensic® Cloud Extractor.

Oxygen Forensic® KeyScout is available at no additional charge in the Tools menu of Oxygen Forensic® Detective and allows detection of various logins and tokens on a computer as well as Wi-Fi hotspot credentials.



APPLICATIONS

iOS

DJI GO (3.1.42)
DJI GO 4 (4.3.1)
Google Duo (39.0)
Google Home (1.31.910)
GroupMe (5.24.0)
Instagram (63.0)
Kik (14.5.0)
Line (8.12.0)
Opera Mini (16.0.13)
Skype (8.30.1)
TamTam (2.4.12)
Telegram (4.9)
Twitter (7.29.2)
Viber (9.6.6)
Waze (4.43)
WhatsApp (2.18.92)

ANDROID

CoverMe (2.8.8)
DJI GO (3.1.43)
DJI GO 4 (4.3.0)
Endomondo (18.8.1)
Facebook (190.0.0.34.94)
Facebook Messenger Lite (42.0.0.9.189)
Firefox Focus (6.1.1)
Google Chrome (69.0.3497.100)
Google Hangouts (23.0.0)
Google Home (1.30.43)
Google Translate (5.23.0)
Instagram (62.0)
Kik (14.6.0.13597)
LinkedIn (4.1.209)
Line (8.12.2)
Romeo (3.1.0)
TamTam (2.0.0)
Telegram (4.9.1)
Strava (64.0.0)
Viber (9.5.0.6)
Waze (4.43.1.1)
WhatsApp (2.18.277)
And many others!

MOBILE DEVICES

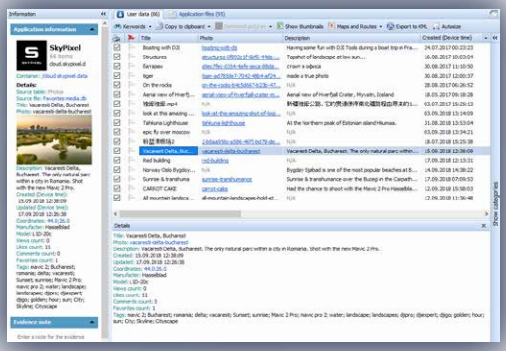
Alcatel 7 LTE AM
Allview AX502 3G
Archos Access 57
Asus ROG Phone
Asus ZenFone 5
BBK Vivo Nex
Coolpad Cool Play C7
Doogee HOMTOM S7
Gome Fenmmy Note
Gome S7
Highscreen Easy Power
HTC U12 life Global
Huawei Enjoy 8 Dual
Huawei Honor 7A Pro
Huawei Maimang 7 Dual
Huawei P Smart Dual
InnJoo Fire 4
Lava Z60
Lenovo Tab M10 LTE
LG K100 K Series K3
Meizu 16 Plus Premium Edition
Micromax Yu Ace
Motorola Moto Z3
Nokia 5.1
Nokia X5
Oppo A3s Dual SIM
Orange Rise 33
Panasonic Toughbook FZ-N1
Positivo Twist Max S540
Samsung SM-A530D Galaxy A8
Samsung SM-G960F Galaxy S9
Samsung SM-N9600 Galaxy Note 9
Samsung SM-T590 Galaxy Tab A 10.5
Sharp Aquos D10 Dual SIM LTE EU
Smartisan JianGuo Pro 2
Snail MOQI i7 Game Mobile
Sony Xperia XZ3 WiMAX
Sugar P1 TD-LTE Dual SIM
Tecno Mobile Pop 1s
Telstra Essential Plus
Xiaomi Black Shark 2
Zopo Flash X3
ZTE Axon 9 Pro
And many others!

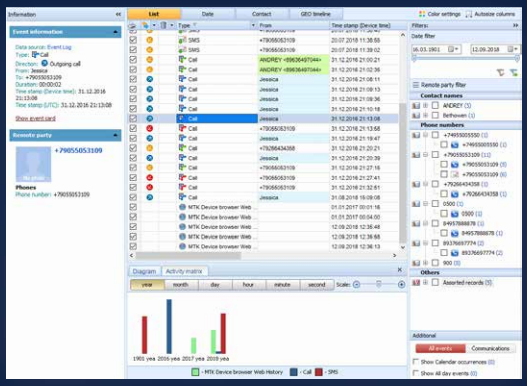
EXTRACT MORE DRONE DATA

Oxygen Forensic® Detective 11.0 brings two important enhancements to drone forensic capabilities. Now, you can root DJI drones with the latest firmware and gain access to Skypixel cloud service, the world's largest drone and aerial photo and video sharing platform.

Access to SkyPixel is available via username/password or token. The software extracts account information, messages, notifications, followers, following, media files, and comments. Photos and videos are extracted together with their time stamps, however geo-coordinates that were assigned by the file owner may not be precise.

New exploits allow you to root DJI Spark drones with the latest firmware to gain complete access to their internal memory and flight logs. The feature is exclusively available in Oxygen Forensic® Detective software.





ACQUIRE MTK FEATURE PHONES

Oxygen Forensic® Detective has supported Android devices based on MTK chipsets for many years including screen lock bypass methods. Beginning with version 11.0 we've also added the ability to do a logical extraction of MTK Feature phones. Now investigators can acquire all basic information from these phones: contacts, calls, messages, calendar, notes, multimedia files, and other available data.

To connect an MTK Feature phone, open Oxygen Forensic® Extractor and select the "MTK Feature devices" option. You will be asked to switch off the phone and connect it to the PC using a regular cable. Once data is acquired it will be available to view and analyze in the interface of Oxygen Forensic® Detective.

OTHER FEATURES

PROXY SUPPORT

We've added proxy settings for a number of cloud services. You can choose to connect via TOR, system or custom settings. Currently the ability to select proxy settings are supported for Amazon Alexa, Google, Telegram, Dropbox, WhatsApp QR, and Twitter services.

ENHANCED EXPORT

We've introduced a number of improvements to our export engine. In the latest version, launch exports significantly faster in sections with large amounts of data. Check our website for the full list of improvements