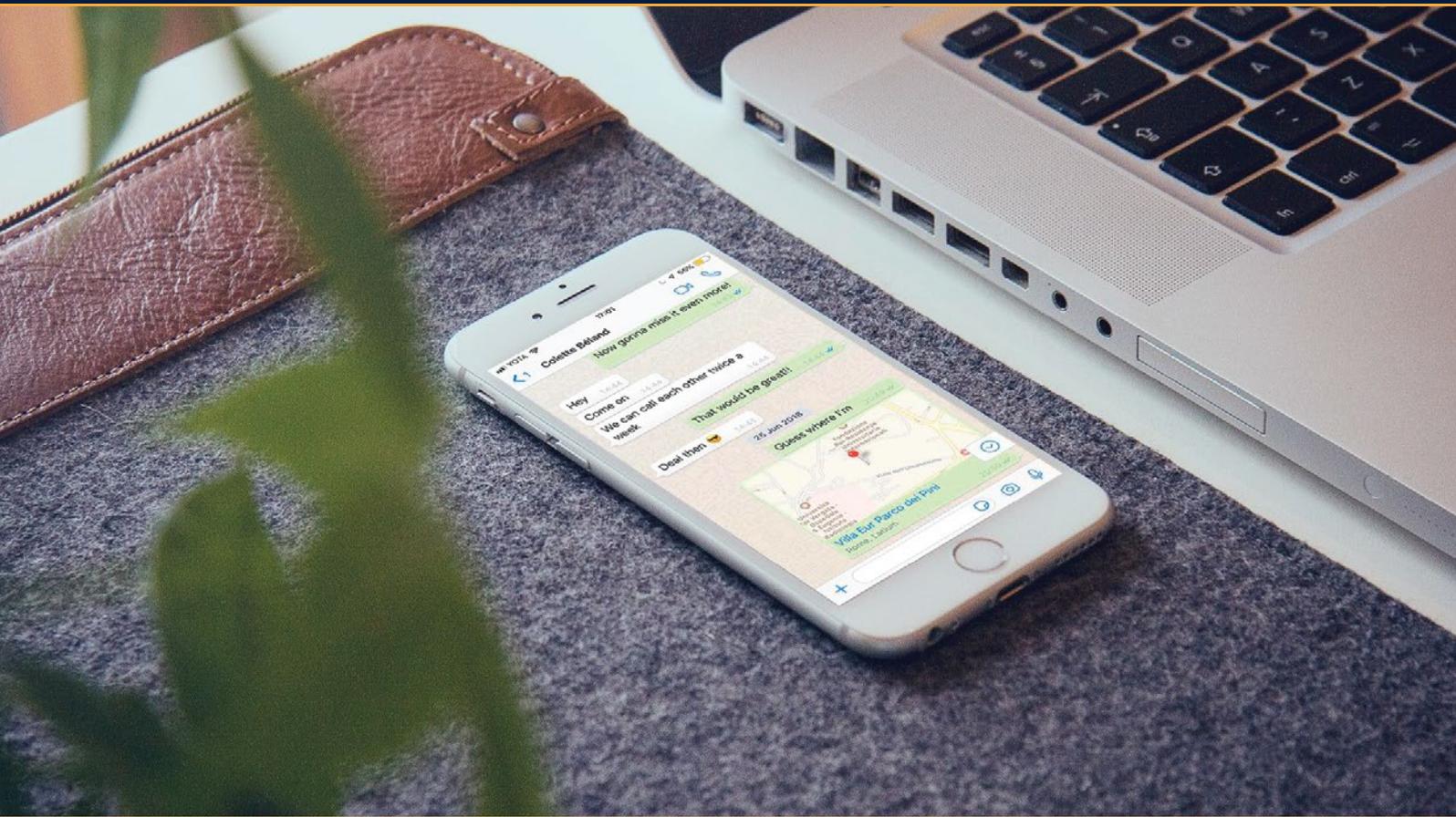# OXYGEN FORENSIC® DETECTIVE

## WhatsApp challenges. Advanced forensic acquisition and decryption techniques.

OXYGEN FORENSICS

WhatsApp is without a doubt the most popular messenger in the world. All WhatsApp messages have end-to-end encryption, meaning they are unreadable if intercepted by anyone. More importantly, WhatsApp communications are never stored on the WhatsApp server. It is no surprise with this type of security it is often the choice communication platform of criminals. Oxygen Forensics offers the most comprehensive WhatsApp data extraction and decryption tools in the market.

WHATSAPP FROM MOBILE DEVICES

End-to-end encryption, as described, only offers security for a "man-in-the-middle attack". However, the data on an Apple iOS or Android device is available in a decrypted format.

When it comes to iOS devices, all WhatsApp data can be extracted in a basic iTunes backup procedure. However, for Android devices, we recommend a physical extraction method to recover WhatsApp's evidentiary files. We offer a wide range of physical collection methods that are successful on a large variety of Android devices. Remember, when examining an Android device always check the SD card for a WhatsApp backup. This file is always encrypted, but we have you covered! You will find information about Oxygen Forensics' innovative decryption methods below. Starting from Oxygen Forensic Detective 12.6 investigators can also collect WhatsApp and WhatsApp Business chats, contacts, calls, and account information using OxyAgent, installed on an Android device.
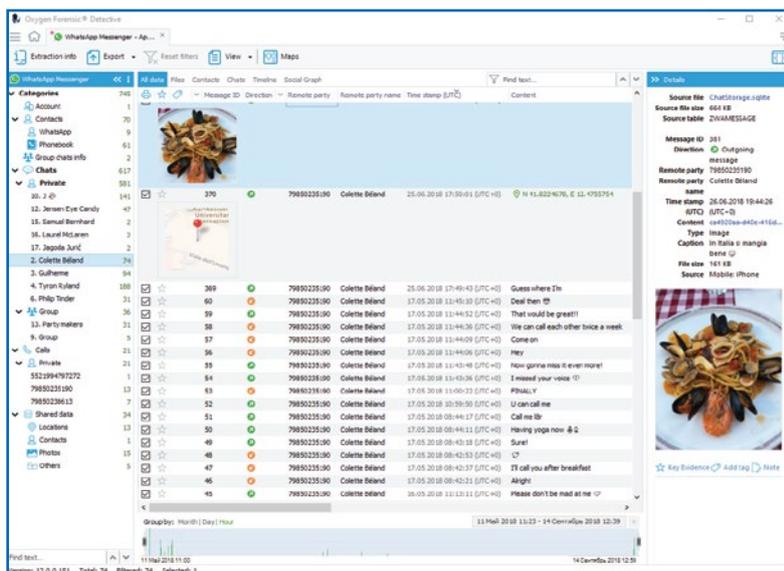

WHATSAPP FROM CLOUD

A WhatsApp user, using an iPhone or Android device, may choose to back up their chats to iCloud or Google Drive. WhatsApp backups are encrypted by default and to decrypt them a forensic investigator should have access to the SIM card to which this WhatsApp account is assigned. However, there are other methods to decrypt this data using the WhatsApp Cloud token. This is outlined more in the following paragraphs.

While extracting WhatsApp data from various cloud services there could be additional hurdles like two factor authentication (2FA) or two-step verification. Our Cloud Extractor documentation contains detailed instructions on how to overcome or disable them.

Extraction of cloud data is extremely important. Cloud may contain data that had been deleted from the device which can easily occur if synchronization is set to each week or each month.
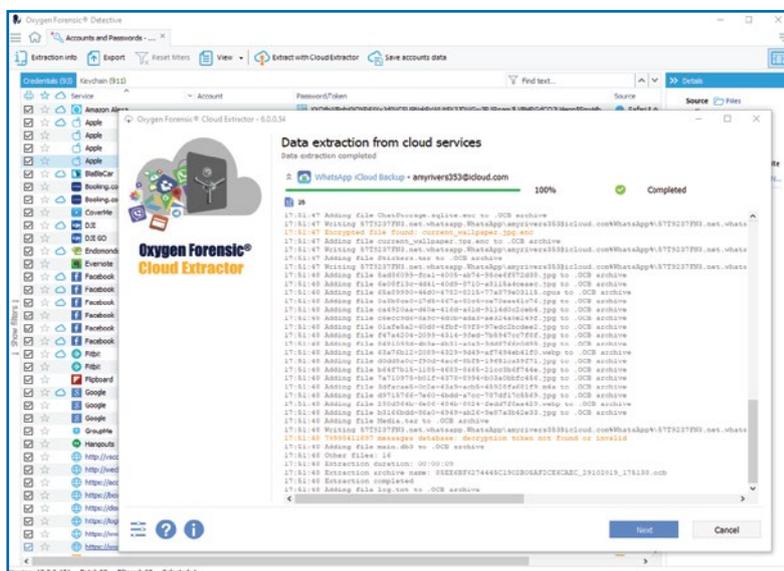
WHATSAPP BACKUP DECRYPTION

The standard WhatsApp backup decryption method used throughout the industry is based on a key file. Oxygen Forensics offers a new decryption method that requires only a phone number! Case in point: if you have found an encrypted backup on an Android's SD card with no access to the Android internal memory where the decryption key is stored, use our innovative decryption method. Our Cloud Extractor offers you an exclusive opportunity to decrypt this backup by receiving a code to the phone number assigned to the SIM card.

Not only data from the device is recoverable, but Oxygen Forensic Detective can also recover a special WhatsApp Cloud token from physical extractions of Android devices. This token can be utilized to decrypt WhatsApp backups from Android devices, WhatsApp Google Drive, and WhatsApp iCloud backups associated with the same phone number.
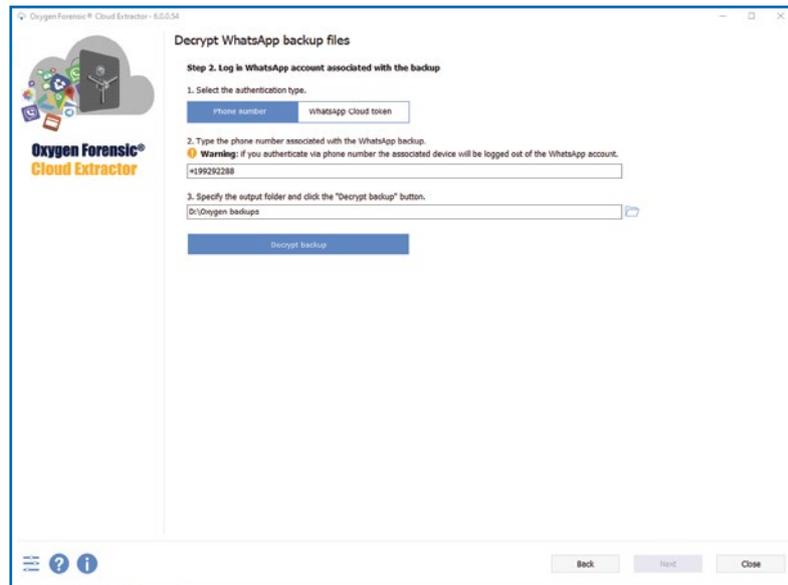
WHATSAPP CLOUD (SERVER)

It is known that WhatsApp does not store any communications on its server that have been delivered. Messages and unanswered calls that cannot be delivered (e.g., a phone has no Internet connection, or it is switched off) will be temporally stored on the server. Oxygen Forensic Detective has the unique ability to access this data from the cloud via only the phone number or special WhatsApp Cloud token extracted from Android devices.

Recommendation: if you have a locked mobile device that you cannot acquire try this: switch it off, wait for a few moments, remove the SIM card and place it into another phone that is unlocked to a carrier. Select WhatsApp Cloud service in our Cloud Extractor, select to receive a code to the SIM card. Now you will have access to the undelivered messages, unanswered calls and their contacts.
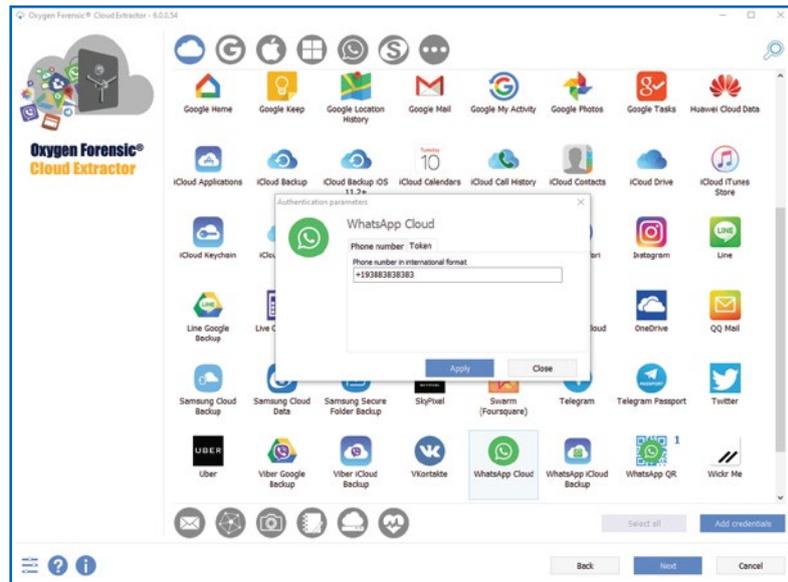
WHATSAPP VIA QR TOKEN FROM PC

WhatsApp users can communicate using WhatsApp Desktop and WhatsApp Web apps from a computer. Our exhaustive research revealed that these apps do not store any databases on the computer. However, with our free Oxygen Forensic KeyScout utility you can detect a WhatsApp QR token on a computer where WhatsApp was used. This token will allow you to extract complete WhatsApp data in our Cloud Extractor. The only condition is that the WhatsApp owner's mobile device must have an active Internet connection but may be locked. WhatsApp QR code method is ideal for data extraction from locked mobile devices.

However, if you have an unlocked mobile device but for some reason the extraction continually fails, simply scan the WhatsApp QR code from the device in our Cloud Extractor to acquire all the current WhatsApp data.
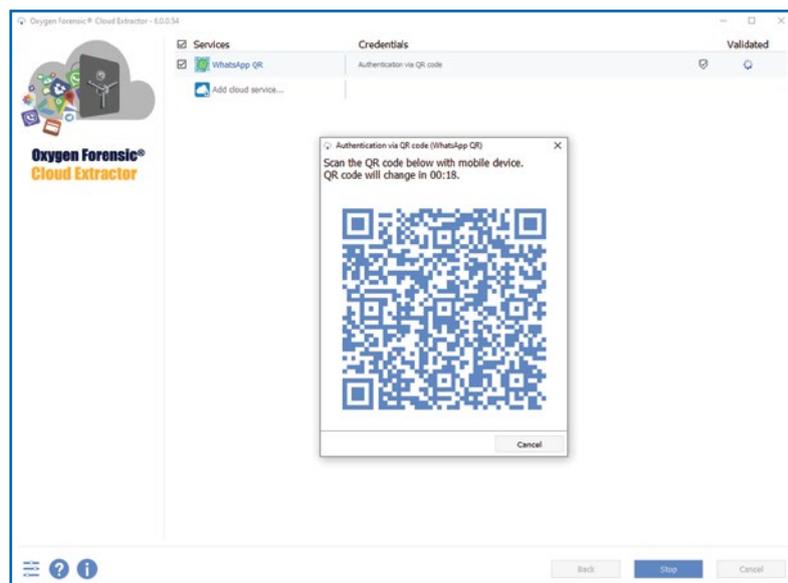
Founded in 2000, Oxygen Forensics has provided solutions in the mobile forensics market since the beginning of our mobile-connected world. Nowadays Oxygen Forensics is the leading global digital forensics software provider, giving law enforcement, federal agencies, and enterprises access to critical data and insights faster than ever before. Specializing in mobile device, cloud, drones and IoT data, Oxygen Forensics provides the most advanced digital forensic data extraction and analytical tools for criminal and corporate investigations.

909 N Washington Street
Suite #300
Alexandria, VA 22314
U.S.A.

support@oxygen-forensic.com

+1 (703) 888-2327

DUNS 078884550 / CAGE 741G3

www.oxygen-forensic.com