OXYGEN FORENSIC® CLOUD EXTRACTOR

Industry-first in cloud forensics

OXYGEN FORENSICS

OVERVIEW

In October 2014, Oxygen Forensics introduced the industry to Extractor for Clouds, an innovative and lightweight utility within Oxygen Forensic® software that allowed acquisition of data from Google, iCloud, and Microsoft cloud services, as well as popular SaaS offerings such as Dropbox, Box, and Bitcasa. Since then, cloud services have evolved – and so have we.

Oxygen Forensic® Cloud Extractor now supports cloud extractions through both login credentials and tokens, as well as compatibility for two-factor authentication and data decryption Oxygen Forensics keeps leadership position on cloud forensics and with each release adds support for the industry-exclusive services and methods, like WhatsApp backup decryption via token, access to WhatsApp server, drone data extraction from cloud and many others. Cloud Extractor is available at no additional charge within Oxygen Forensic® Detective.

HOW IT WORKS

1. Extract credentials or tokens from a mobile device. Oxygen Forensic® Detective parses and decodes available passwords and tokens in iOS, Android, and Windows Phone devices. A portable app Oxygen Forensic® KeyScout is also available within Detective to find and extract login credentials and tokens from Windows computers.

2. Use credentials or token to access a cloud service. Accessing cloud storage services using tokens generally leaves no digital traces, while using login/password is less advantageous to the investigator since the cloud service typically sends a notification to the account owner about the login.

3. View cloud extraction in Oxygen Forensic® Detective. Once data is extracted from a cloud storage location, the investigator can begin examination of the data in Oxygen Forensic® Detective or save for further analysis later.

4. Analyze and export cloud data. In Oxygen Forensic® Detective the investigator can conveniently analyze cloud data in Timeline, Social Graph, Key Evidence, Maps, etc. or simply create a data report.

SUPPORTED CLOUDS

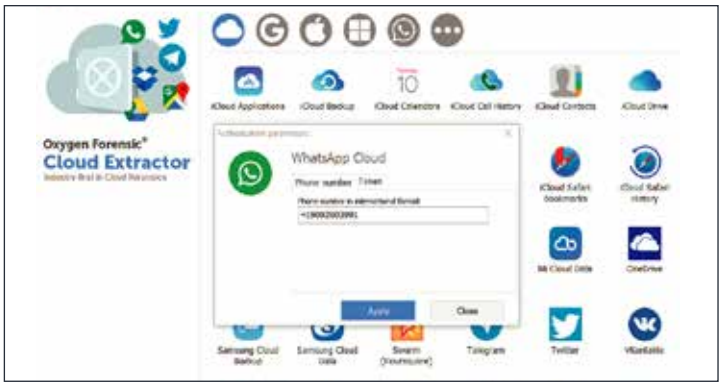
- iCloud: Contacts, Calendar, Calls, Drive, Notes, Photos, Safari, Applications, etc.
- Google: Contacts, Calendar, Chrome, Drive, Location History, My Activity, Photos, etc.
- Microsoft: Contact Device list, Contacts, Calls, Messages, Notes, Browser, Calendar, OneDrive, etc.
- Samsung: Device list, Contacts, Calls, Messages, Notes, Browser and Secure Folder
- Huawei: Device list, Contacts, Messages, Calls
- Mi Cloud: Contacts, Calendars, Calls, Messages, etc.
- IoT: Amazon Alexa, Google Home
- Health: Fitbit, Google Fit, Samsung Health
- Drones: DJI cloud, SkyPixel
- Cloud storages: Box, Dropbox
- E-mail Servers: Google, Hotmail, Yahoo, etc.
- Social Networks and Messengers: Facebook, Instagram, Twitter, Viber, WhatsApp, etc.

SO, WHY OXYGEN FORENSIC® CLOUD EXTRACTOR?

ACCESS TO WHATSAPP SERVER

Oxygen Forensic® Cloud Extractor features a unique method to access the WhatsApp Server via phone number or special token extracted from Android devices in Oxygen Forensic® Detective. This feature enables acquisition of undelivered messages, missed calls, contacts, groups and their participants, and other data.

This service is useful in investigations when the device is damaged, locked, or missing. With our built-in instructions for accessing the WhatsApp Cloud service, investigators can extract data even without the mobile device in hand.



WHATSAPP DECRYPTION METHODS

There is a standard WhatsApp backup decryption method that is based on a key file. Oxygen Forensics offers investigators a new decryption method that requires only a phone number and that is a great alternative to the commonly used key file.

Oxygen Forensic® Detective can also acquire a special WhatApp 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.

DELETED CLOUD DATA RECOVERY

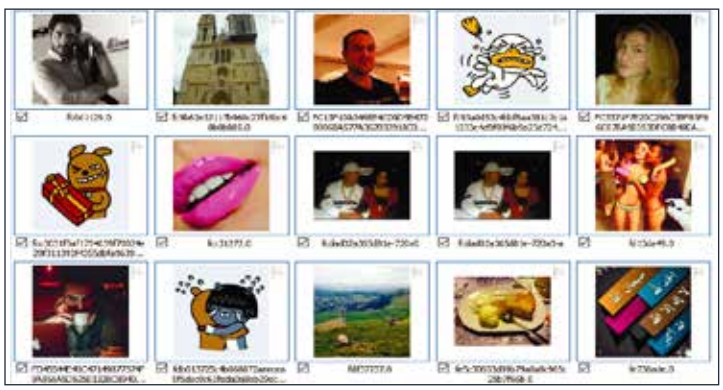
Oxygen Forensic® Cloud Extractor allows the recovery of data deleted from a mobile device:

1. Samsung Cloud. Investigators can access this service via login/password or token and extract photos and videos that were deleted from the mobile device.

2. Huawei Cloud. Investigators can easily gain access to deleted contacts.

3. Dropbox. The Oxygen Forensic® Cloud Extractor acquires information about deleted files as well as the history of their revisions.

4. Telegram Messenger. Within this cloud server investigators will often find hundreds of deleted messages.



GOLDMINE OF GEO LOCATIONS

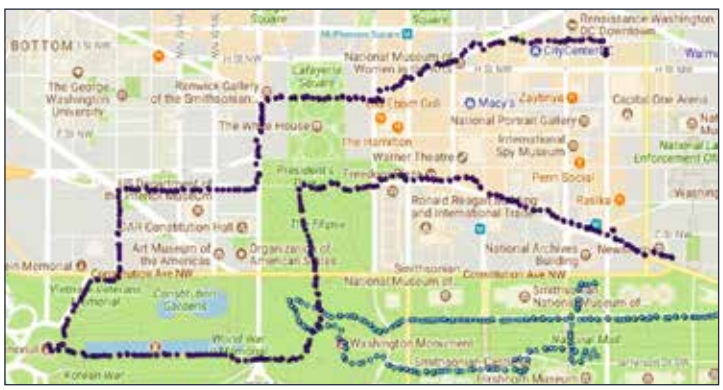
Cloud storages are a goldmine of geo locations:

1. Google Locations History. If enabled, this service records all of a user's locations, sometimes for years. This data cannot be extracted from the mobile device but is available in the user's Google Cloud account.

2. Cloud Photos. If investigators extract iCloud, Google, or Samsung photos from the various cloud services, the geo data is also retrieved.

3. Endomondo. This fitness app is a goldmine of location data, as are most fitness apps.

4. DJI Cloud. Investigators can access DJI cloud via token extracted from the drone owner's mobile device and acquire all the drone flight history with geo coordinates.



"Built-in Cloud data recovery using the Oxygen Forensic® Cloud Extractor. This is the most robust cloud extractor I have used. You can either use the credentials that have been extracted from the mobile device or even add ones that were located on a computer or supplied to you in the investigation. The amount of data from Google, Microsoft, Apple, Dropbox, WhatsApp, Facebook, IMAP accounts and many more cloud accounts is truly incredible."

Gus Dimitrelos, CyberForensic360

Oxygen Forensics, Inc
901 N. Pitt St, Suite 100
Alexandria, VA 22314
Tel: 877 969 9436

support@oxygen-forensic.com
www.oxygen-forensic.com
https://www.instagram.com/oxygenforensics/
http://twitter.com/oxygenforensic
http://facebook.com/OxygenForensics
DUNS 078884550 / CAGE 741G3