OXYGEN FORENSIC®
DETECTIVE

All-in-one forensic tool

Data Extraction

MOBILE DEVICES

Oxygen Forensic® Detective offers data extraction from Apple iOS, Android devices, feature phones, media, and SIM cards. Because time is always of importance, simultaneous acquisition of several devices is available. Oxygen Forensic® Detective imports numerous backups and images, including iTunes, Android backups, GrayKey, JTAG, Chip-off, UFED, XRY images, .dar archives, Warrant Returns and more.

Oxygen Forensic® Detective uses proprietary methods to bypass screen locks on mobile devices, including Samsung, Huawei, Sony, as well as devices based on Mediatek, Spreadtrum, Kirin, Exynos or Qualcomm chipsets. Oxygen Forensic® Detective can also automatically find passwords to encrypted iTunes backups and Android images.

CLOUD SERVICES

The built-in Oxygen Forensic® Cloud Extractor allows investigators to gain access to a tremendous amount of cloud services that include iCloud, Google, Microsoft, Samsung, Huawei, E-mail server, Facebook, Twitter, Instagram, Dropbox, WhatsApp, Telegram, Viber, WickrMe, etc. Our Cloud Extractor also offers the exclusive ability to decrypt WhatsApp backups via phone number.

Investigators may utilize account credentials, phone number, tokens or QR code to access any supported cloud storage. Using our software, you can extract credentials and tokens directly from a mobile device as well as collect them on Windows, Mac and Linux OS computers. Credentials can then be used to extract evidence from the associated cloud service.

DRONES

Oxygen Forensic® Detective enables the verbose data parsing and analysis from drone collections, flight logs, mobile apps and cloud services. Oxygen Forensic® Detective can create or import drone physical dumps and parse GPS locations showing valuable route data as well as device telemetry to include: speed, direction, altitude, temperature, and more. Currently, various models of DJI and Parrot drones are supported.

Data parsing from drone applications is also available from iOS and Android devices. Investigators can decode drone images and videos, locations with time stamps and other data. Additionally, drone data extraction from cloud services can be accomplished via login/password or token from DJI, SkyPixel or My Parrot clouds.

COMPUTER

Oxygen Forensic® KeyScout utility focuses on extracting and decrypting credentials, system files, and user data from web browsers and desktop apps on computers running Windows, macOs or Linux.

Currently there are numerous desktop apps supported, including WhatsApp, Viber, WickrMe, Telegram, Skype, Signal, Microsoft Mail, Microsoft Outlook, Thunderbird, all the popular Web browsers, pre-installed Apple apps, etc. Collected tokens and passwords can be immediately used for cloud data extraction while extracted web browser, messenger and email data can be imported into Oxygen Forensic® Detective software for further analysis and analytics with mobile data artifacts in one case.

IOT DEVICES

Oxygen Forensic® Detective currently offers data extraction from two popular IoT devices – Amazon Alexa and Google Home. Since it is difficult to extract data directly from devices, we provide investigators with the ability to access alternative sources – cloud and mobile apps. Investigators can gain access to cloud information via login/password or token that can often be extracted from the user's PC or mobile devices. Oxygen Forensic® Cloud Extractor acquires a complete evidence set including voice recordings that can be played directly our software interface. Oxygen Forensic® Detective also extracts IoT app data from Apple iOS and Android devices.

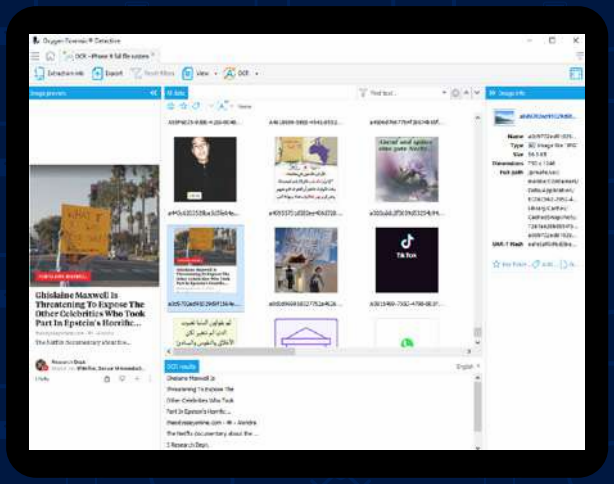
WEARABLES

Oxygen Forensic® Detective performs logical acquisition of smartwatches based on MTK chipset allowing forensic experts to extract device model, contacts, calls, messages, multimedia files, and other data. Moreover, the software acquires complete data from various fitness apps, like Apple Health (including data synched with Apple Watch), Samsung Health, Google Fit, FitBit, Endomondo, and more. This valuable data can be extracted both from mobile devices and cloud services and often contains a tremendous amount of geo locations with time stamps, health data, steps and stair count with additional user statistics.

Data Analysis

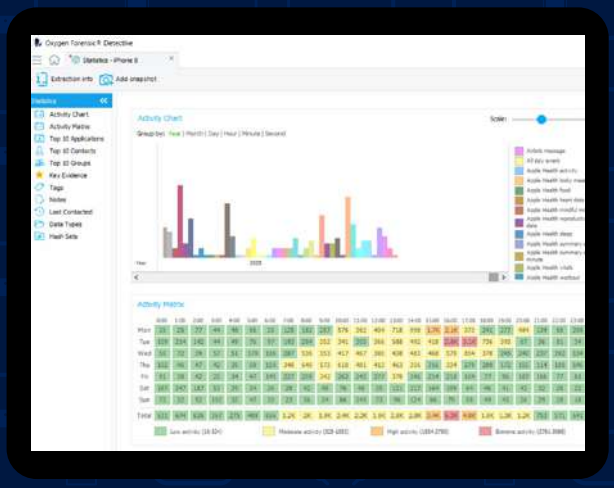
OPTICAL CHARACTER RECOGNITION

Investigators no longer have to spend time manually transcribing text within a picture. Oxygen Forensic® Detective includes the 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 across the processed images.



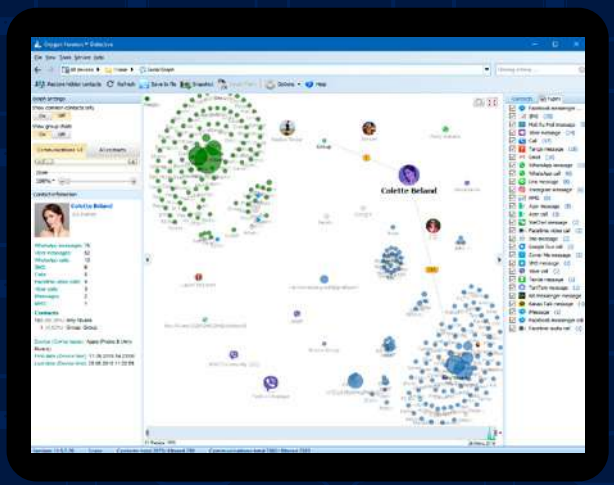
STATISTICS

The Statistics section consists of several widgets, that are divided into two categories–data on the device and investigator interaction. Data on the device is displayed in the first widgets and shows the data present within the extraction in charts or tables (Activity Chart, Activity Matrix, Last Contacted, Data Types, Top 10 Applications, Contacts, or Groups). The second group of widgets, or investigator interactions widgets, display the investigator's interactions with the evidence: assigning tags, marking data as Key Evidence, adding and editing notes, running hash set searches.

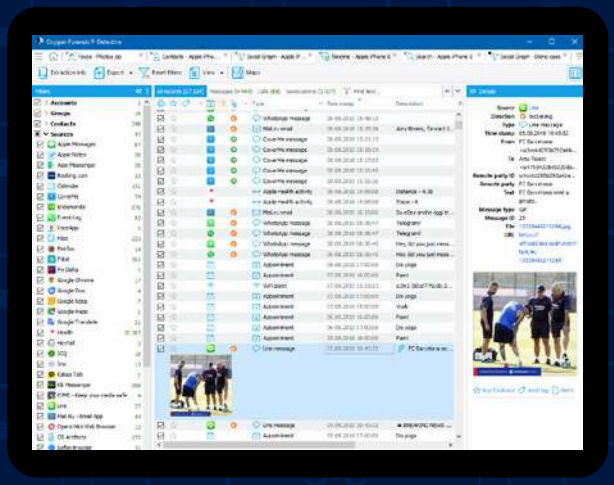


SOCIAL LINKS

The built-in Social Graph provides a convenient platform to explore social connections between a device owner and contacts or between several devices. Using the Social Graph investigators can identify the device owners closest contacts in one click. Click on any contact to open a card containing detailed information about the selected contact and all communications across device sources. The Social Graph interface is dynamic and nimble, and investigators can drag and drop to move, hide, or merge contacts while producing a crystal clear view of device and case connections.

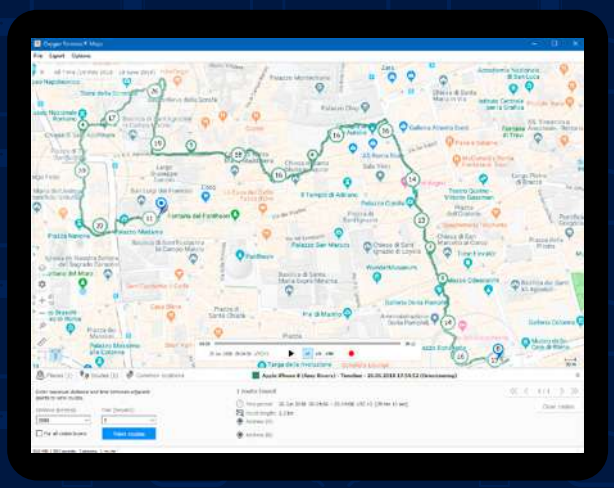


Data Analysis



TIMELINE

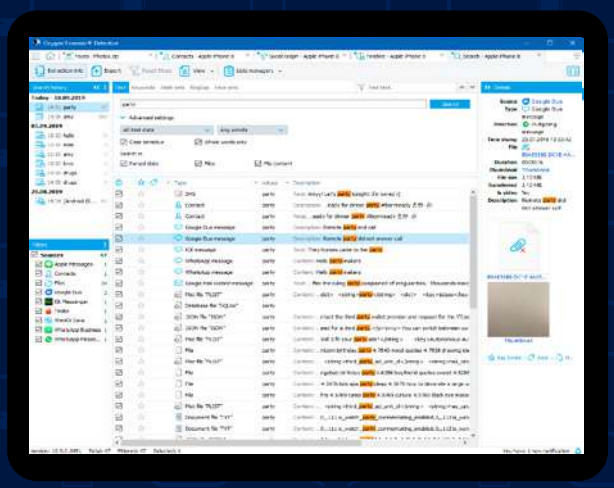
The Timeline section provides a view of all device events in one list – chats within apps, calls, web activity, web connections, photos and videos, calendar events, and more. Events can be viewed for one device or a group of devices, allowing easy identification of common group activities. Sort and filter by date, time, activity frequency, contact, remote party, or other data points to focus only on the most relevant data. The GEO Timeline tab contains the full list of geo coordinates from all the sources that include photos, videos, apps, drone flight logs, and more.



MAPS

Oxygen Forensic® Detective acquires geo coordinates from all possible sources including mobile devices, drones, cloud storages, media cards, and imported images. Once analyzed, the data can be viewed within our Oxygen Forensic® Maps either online or offline. The Maps module includes the ability to:

- Identify a device's frequently visited places
- Visualization of a device's movements within specified period of time
- Pinpointing common locations of several devices
- Playing an animated route showing the direction of travel

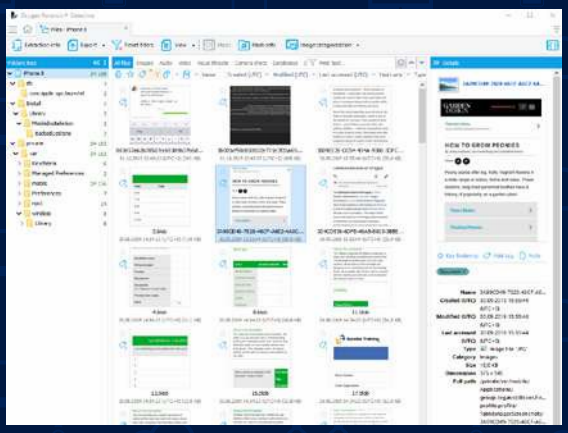


DATA SEARCH

Oxygen Forensic® Detective allows investigators to search across a single device, all devices in a case, or all devices in a database for text, phone numbers, email addresses, geo coordinates, IP addresses, MAC addresses, credit card numbers, and file hashes including Project VIC. A Regular Expression library is available for custom search functions, and the Keyword List Manager and Watchlists allow investigators to create a set of keywords and perform searches during or after an extraction.

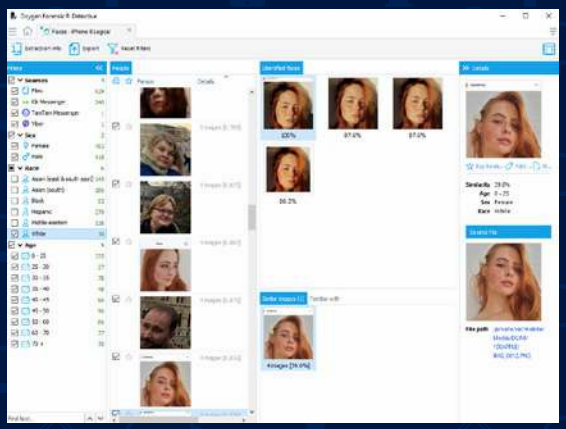
Data Analysis

IMAGE CATEGORIZATION



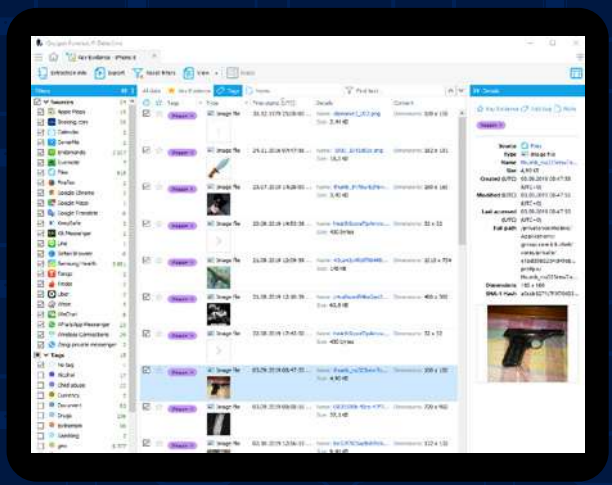
Oxygen Forensic® Detective provides the ability to categorize images from twelve different classes that includes pornography, extremism, drugs, alcohol, and weapons. Our image categorization is available when importing device data and also on already imported extractions. Investigators can select all or selected categories while also having the ability to fine-tune the positive "hit" settings. After running the image analysis, the number of matching images for each supported category is tagged and shown in Key Evidence and the Files sections. Investigators can review the tagged data and manually exclude any false positives.

FACIAL RECOGNITION



Oxygen Forensic® Detective offers the ability for investigators to categorize human faces as well as conduct searches for specific faces in one or more extractions. The facial recognition is available in the Faces section at no additional charge. The unique features include detailed face analytics (gender, race, age), and support for massive volumes of data. Using the built-in facial recognition investigators will spend less time looking through thousands of photos or videos in mobile, cloud or computer extractions.

KEY EVIDENCE AND TAGGING



The Key Evidence section displays all records that have been bookmarked in other sections by the investigator. This section is where all entries identified as evidence and relevant to a case are found, making data analysis easier and saving valuable time. Investigators can bookmark important evidence in a single device or several devices and export it later to one data report. More importantly, Oxygen Forensic® Detective also offers a number of predefined tags, to include: Nudity, Weapon, Guns, Important, and many others. Investigators can also create and set their own tags and export entries to data reports by simply selecting the relevant tags.

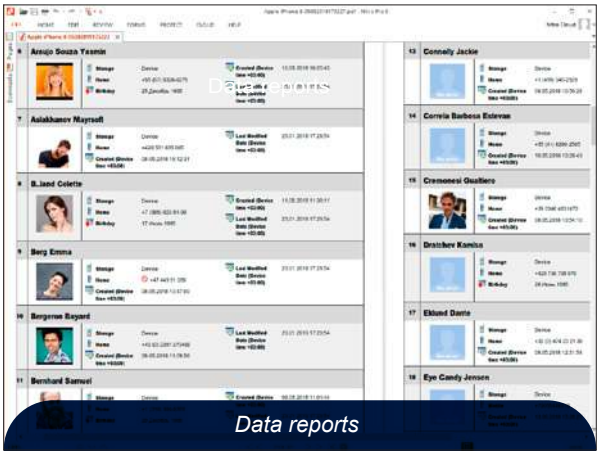
Data Export

OFB BACKUPS

All extracted data can be saved to an Oxygen Forensic Backup (OFBX) clicking on Save to archive button on the main toolbar of Oxygen Forensic® Detective. This OFB backup can be imported back to Oxygen Forensic® Detective anytime later or can be sent to colleagues to be opened in the Oxygen Forensic® Viewer. The Viewer is a free portable utility for viewing and sharing collected evidence from Oxygen Forensic® Detective. It can be downloaded from the customer area and requires no installation or activation.

DATA REPORTS

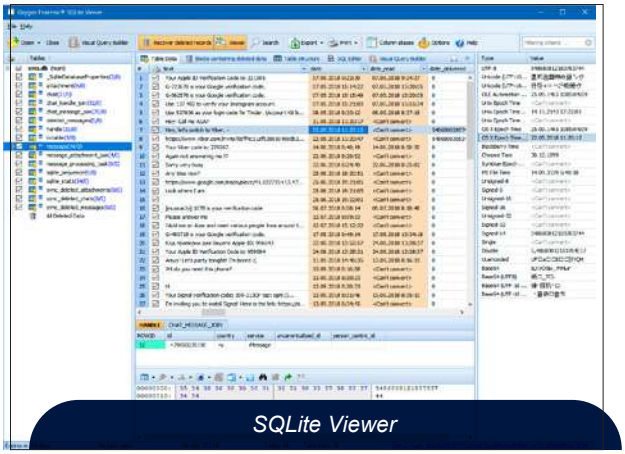
Oxygen Forensic® Detective enables data export from any section to many popular file formats including PDF, RTF, XLS, XML, HTML, etc. A report can be created to include a single device, several devices, several sections or even selected records. Reports are highly customizable to display only the data required, for any type of case. Our XML reports can be integrated into other analytic software platforms. Oxygen Forensic® Detective can also export data in to the Relativity software format.


Data reports

Data Viewers

PLIST VIEWER

The built-in Oxygen Forensic® Plist Viewer offers advanced analyzing of Plist files: investigators can open plain XML and binary XML files, view entries according to their type (string, data, numbers etc.), convert values, open external files for analysis, export .plist file data in XML format for further analysis by external tools.


SQLite Viewer

SQLITE VIEWER

The built-in Oxygen Forensic® SQLite Viewer is a powerful 64-bit tool for examining SQLite files. With this tool, investigators can open any SQLite database, recover deleted records, convert values to a readable format, build visual and non-visual SQL queries and save them for further use, run search and finally export selected entries to customization data reports.

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 St Suite #300
Alexandria, VA 22314

support@oxygen-forensic.com

+1 (703) 888-2327

DUNS 078884550 / CAGE 741G3

www.oxygen-forensic.com