# Table of contents

General information.................................................................................................................. 3
Installation ................................................................................................................................. 4
Connecting a mobile device....................................................................................................... 6
Extraction methods .................................................................................................................. 9
  Android data extraction ....................................................................................................... 9
  iOS device acquisition ........................................................................................................ 17
  Windows Phone device acquisition .................................................................................... 18
  Blackberry 10 device acquisition ....................................................................................... 19
  Memory card extraction ....................................................................................................... 20
  SIM card data extraction .................................................................................................... 21
Importing backups and images ............................................................................................... 22
Viewing Extracted Data.......................................................................................................... 24
  Desktop View ...................................................................................................................... 24
  Basic Sections ...................................................................................................................... 28
  Applications ......................................................................................................................... 31
Analyzing Data ....................................................................................................................... 35
  Timeline ............................................................................................................................... 35
  Aggregated Contacts .......................................................................................................... 36
  Links And Stats ............................................................................................................... 36
  Social Graph ...................................................................................................................... 37
  Search ................................................................................................................................. 38
  Key Evidence ...................................................................................................................... 39
Integration with Project VIC ................................................................................................. 39
Generating Forensic Reports ............................................................................................... 39
SQLite Database Viewer ........................................................................................................ 41
Plist Viewer ............................................................................................................................ 41
Oxygen Forensic® Cloud Extractor ......................................................................................... 42
Oxygen Forensic® Call Data Expert ....................................................................................... 45
Oxygen Forensic® Maps ....................................................................................................... 46
Drone data .............................................................................................................................. 47
General Connection Instructions ......................................................................................... 50
Copyrights and contacts ........................................................................................................ 53
General information

Oxygen Forensic® Detective is a forensic software solution designed to acquire data from mobile devices, their backups and images, memory cards, SIM cards, drones, and cloud storages. The program has played a significant role in criminal and other investigations all over the world and is used by Law Enforcement units, Police Departments, army, customs and tax services and other government authorities.

With Oxygen Forensic® Detective you can acquire and analyze:

- Device information
- Contacts
- Dialed, received, and missed calls
- Organizer data (notes, tasks, and calendar entries)
- Messages (SMS, MMS, iMessages, emails with attachments)
- Images, videos, audio files, voice records, documents, and database files
- Geo location data stored in various sources
- Device connections history (Wi-Fi, Cell Tower, etc)
- Device event logs
- Logins, passwords, and tokens extracted from applications databases (including passwords to applications, cloud storages, encrypted backups, and Wi-Fi networks)
- Deleted records and files
- Applications data from devices running iOS, Android OS, BlackBerry 10, and Windows Phone 8
- WebKit data from iOS and Android devices
- Data from cloud sources: iCloud, Google, Microsoft, Huawei, Samsung, Mi Cloud, E-Mail (IMAP) Server, DJI drone, etc.
- GPS locations, images and videos from drones
- Call Data Records received from mobile service providers
- SIM card data via SIM card reader

The current version supports 19,500+ mobile devices running different OS: Android, Bada, Blackberry, iOS, MTK, Spreadtrum and Qualcomm chipsets, Symbian, Windows Mobile 5/6, Windows Phone 8, feature phones, etc.

Oxygen Forensic® Detective allows to import and parse data from various device backups and images (Apple iOS, Android OS, Windows Phone OS, BlackBerry OS, and Nokia) as well as iOS and Android images made by other forensic tools.

Oxygen Forensic® Detective supports USB cable and Bluetooth (Microsoft, Widcomm) connections. The software works under 32-bit or 64-bit versions of Windows 10, Windows 8, and Windows 7.
Installation

Oxygen Forensic® Detective USB dongle license must be used with a USB dongle that is bundled with your Oxygen Forensic® Detective package. For this license, no Internet connection is required. After Oxygen Forensic® Detective installation please insert a USB dongle into the USB port, wait till the driver initialization, and start the main program.

Please note that USB dongle should be inserted the whole time during your work with Oxygen Forensic® Detective.

You are given the following options during the software installation which allow you to select the destination folder for Oxygen Forensic® Detective, create desktop and quick launch icons, the desired program language. Lastly, read carefully and accept the license agreement, if you agree.

After all options have been selected, click the Install button to start the installation:

When the installation is complete, you can choose to download driver pack required for device connection or immediately launch Oxygen Forensic® Detective:
Connecting a mobile device

To work with a phone, make sure it is supported by the current version of the software and all corresponding drivers were installed.

To start the extraction, connect the device to a PC with the installed program. If you use a cable connection, attach the cable to the device. For Bluetooth connection, activate it on the device and make sure it is visible and accessible.

Clicking the Connect new device button in the Oxygen Forensic® Detective interface will launch Oxygen Forensic® Extractor. Select “Device Acquisition” to automatically detect a single device connected via a cable or “Manual device selection” to connect several devices one by one. Bluetooth connection is also available. The list of available connection types depends on the mobile device capabilities and hardware installed on your computer.

To bypass the screen lock and perform physical data extraction on supported Android OS devices, choose “Physical data acquisition”. This method will allow to bypass passcodes on the supported devices: LG, Motorola, Samsung Galaxy as well as devices with Chinese chipsets. To use this option, click the required device hyperlink. Then you’ll be redirected to the appropriate screen with the instructions on how to prepare the selected Android device.
Once the extraction option is chosen, Oxygen Forensic® Extractor will begin searching for the device:

Once the connection is established, the program will display the device information:
Next screen prompts to enter the information about the device, its owner and the case it was assigned to. If the device is locked with the known password, you can enter it in the corresponding field.

You also have the option to parse applications databases and collect data for analytical sections such as Aggregated contacts, Links and Stats, Social Graph, Timeline, etc. This can be done later in Oxygen Forensic® Detective if you need to save time during the data extraction stage.

Select the information to be read by Oxygen Forensic® Extractor. Please be informed that the list of available sections depends on the mobile device and the selected extraction method.
When all data is extracted, you can open the device for viewing and analyzing data or run the Export and Print Wizard if you need to get a fast report about the device. Note that you can run Export or Print Wizard anytime while working with the device information.

**Extraction methods**

**Android data extraction**

**Android backup**

This method is used on Android devices at 4.0 and higher. Using this method, make sure that the device is not locked by a gesture/pin/password.

Connect an Android device and choose the Android backup extraction method in the program window. Oxygen Forensic® software will collect the data available via this method. Every application developer decides which user data to put in the backup. It means there is no guarantee that all apps data will be extracted.

**OxyAgent method**

This is the method that works on any supported Android device. In case other methods fail, this method will acquire at least the minimum set of data. OxyAgent has no access to the internal memory folders thus it won’t return the internal memory files and won’t recover deleted data. It will help to extract only contacts, messages, calls, calendar, and files from flash drive.

Software communicates with the Android device via ADB to acquire data via logical method. Make sure that proper drivers are installed for the ADB communication to occur. OxyAgent will be installed on the Android device. You must configure the Android device by enabling USB Debugging mode before starting Oxygen Forensic® Detective:
Follow these steps:

- Check whether the device is not locked with a passcode or pattern lock
- Enable USB DEBUGGING in SETTINGS > APPLICATIONS > DEVELOPER OPTIONS
- Enable UNKNOWN SOURCES in SETTINGS > APPLICATIONS

Physical methods involving root access

Temporary root access to a device running Android OS reveals the complete set of user data and gives the investigator full access to all device folders and subfolders. Their content is displayed in the File Browser section. Generally, this procedure requires certain knowledge, but Oxygen Forensic® products can perform it automatically. The software uses a proprietary exploit to shell root Android devices. Even though there is no 100% success guarantee, the rooting module is highly reliable for the following Android OS versions: 1.6-2.3.4 and 3.0-6.0). The rooting is removed upon restart.

There are preliminary steps to be taken for a successful rooting:

✓ Connect the Android device to a PC via cable with an Oxygen software running.
✓ Choose «Device Acquisition» in Oxygen Forensic® Extractor to automatically detect the Android device.
✓ Choose physical method via rooting in the Extractor and then choose the appropriate exploit from the list. The latest Android devices are usually rooted with the DirtyCow exploit.
✓ The procedure is over. After rooting, the File Browser section will display a detailed view of the file system. All subsequent data will be analyzed and displayed in the main Dashboard window.

**Physical support without root access**

Oxygen Forensic® Detective offers noninvasive support for selected Android devices even if rooting cannot be established. If the device is supported, you can navigate to the Oxygen Forensic® Extractor and select PHYSICAL DATA ACQUISITION.

Currently, you can select Samsung devices Android dump (via custom forensic recovery), Motorola, LG, Qualcomm, MTK or Spreadtrum Android dump on the menu. All these physical methods allow to create a full physical image and bypass any screen lock of the supported Android device.

**MTK Android dump**

The method utilized by the software requires MTK devices to be connected in a switched off mode and this allows to bypass any type of screen lock (PIN, passcode, pattern, etc). The software supports various chipsets including MT6750, MT6755, MT6737, MT6738, etc.

After the device is connected the custom bootloader is being installed. It contains the commands to read the phone memory, works with the operating memory and does not affect the phone data. Please note that you cannot use it for the phones with the locked bootloader. If the bootloader is locked, the "Connect Err = 1013" message will appear in the log files.

**LG Android dump**
This method supports popular LG models, like G5, V10 and V20. Make sure you follow the connection instructions and the device is switched into Device Firmware Update Mode.

Spreadtrum Android dump

Make sure you follow the connection instructions. The list of the supported devices (currently 100+) will be displayed prior the extraction, and you need to choose the model.
Custom forensic recovery for Samsung devices

Oxygen Forensic® Detective offers an effective and advanced method for Samsung devices acquisition. This method currently supports popular Samsung Android devices and the supported devices list is constantly growing.

Please select the Samsung Android dump from Physical data acquisition menu of the Extractor and read the instructions carefully.

The list of the supported devices is displayed prior to the extraction, and you need to choose the model. If the physical image is encrypted, the program will attempt to decrypt it in case the password is known. If the password is not known the built-in Passware utility will try find it (not in all cases).
Motorola physical dump

Oxygen Forensic® Detective offers the breakthrough technology to extract data from password-locked Motorola devices running Android OS. This innovative approach covers the latest Motorola devices released after the year 2015, like Moto X Pure, Moto G 3rd gen and Moto G 5th gen.

The method allows you to bypass any screen lock password, locked bootloader or installed FRP and gain access to the crucial evidence including applications data and deleted records. The data extraction from Motorola devices is performed automatically with a few manual manipulations on the examined device. Oxygen Forensic® Detective uploads a Fastboot image into the device that must be switched into Fastboot Flash mode. The method does not affect any user data. Physical extraction is done by using Jet Imager, the latest technology in extracting data from Android devices that allows to acquire the data in several minutes.

Qualcomm physical dump

Oxygen Forensic® Detective allows investigators to utilize the non-invasive physical acquisition technique via EDL mode and bypass screen lock on 400+ unique Android devices based on Qualcomm chipset. Utilizing EDL along with data extraction is often much faster than Chip-Off, JTAG, or ISP and typically does not require phone disassembly. Additionally, using this method does not modify the user or system data.

Oxygen Forensic® Detective provides support for devices with the following chipsets: MSM8909, MSM8916, MSM8917, MSM8926, MSM8929, MSM8936, etc. The list of supported devices includes models from: Acer, Alcatel, Asus, BLU, Coolpad, Gionee,
Huawei, Infinix, Lenovo, LG, LYF, Micromax, Motorola, Nokia, OnePlus, Oppo, Swipe, Vivo, Xiaomi and many others.

Jet Imager (fast Android data extraction)

Oxygen Forensics has made partnership with MITRE Corporation to deliver the fastest extraction method for Android devices. Thanks to the new Jet-Imager module Android devices are acquired many times faster than the previous methods allowed.

The Jet-Imager module allows to create full physical dumps from Android devices on average up to 25% faster. The extraction speed depends on how much data the device has. For example, 16GB can be extracted in 5-7 minutes, 32Gb – in 8-10 minutes.

Currently there are two extraction methods in the Jet-Imager module:

- physical extraction via custom forensic recovery
- physical extraction of pre-rooted devices

The list of compatible methods is growing.
The module is available in Oxygen Forensic® Detective license on the main Extractor screen:
iOS device acquisition

Classic logical

This is a universal method and is recommended for all iOS devices and uses iTunes backup procedure to acquire data. If iTunes backup is encrypted the software will attempt to find password using various supported attacks (brute force, dictionary attack, etc.). The method will return enough user data including deleted records and applications.

To perform an acquisition and obtain a file system collection of an Apple iOS device there are several options:

- Live Device
- Import Backup
- Import of other forensic software image

Live device collection

- Check if the iOS device is not passcode-locked.
- Check if the device is connected in a normal mode.
- Check if the latest Apple iTunes version or iOS drivers are installed.
- Select the Connect device option on the toolbar and then choose either Auto Device Connection or Manual Device Selection.
- If Auto device connection is selected, the device will be automatically connected.
- If Manual device selection is selected, the window with device model list will appear.
- Select Connect via Cable and device in a model list and press Next.

Importing an iTunes backup

Backup files of iOS devices created in iTunes can be imported in Oxygen Forensic Detective with the help of Oxygen Forensic® Extractor. Any forensic examiner can conveniently analyze the data of Apple devices in the interface of Oxygen Forensic Detective or generate reports of the acquired data.

Import file button > Import Apple backup/image>import iTunes backup…

Other Backup Images

Oxygen Forensic Detective supports the import of many other mobile software images for Apple. These can be obtained using the Oxygen Forensic® Extractor.

Import file button > Import Apple backup/image>
Windows Phone device acquisition

Currently, to access valuable user information, the examiner must obtain a physical image, either by noninvasive or invasive methods. Most examiners use JTAG methods for the Windows Phone because it offers a non-invasive method of access to the device without requiring complete disassembly, and many Windows Phone models are supported.

Windows Phone 8 are only supported at this time and the device must be unlocked. The system conducting the collection must be Windows 7 and higher.

Logical

Oxygen Forensic® Detective can acquire data over a cable or by accessing Windows Phone Cloud storage.

The first approach allows to get media files over a cable and phonebook contacts and incoming and outgoing calls over Microsoft Bluetooth connection. In this case the data are acquired from a device connected locally both via cable and Bluetooth connection. It is recommended to combine the result of both approaches for a full forensic image.

The supported collection items include:

- Phonebook
- Event Log
- File Browser – This information is obtained via MTP and are on the accessible Media area which can included Images, Videos and Documents.

To access the information on the Windows Phone Cloud, go to the Oxygen Forensic® Cloud Extractor.

Non-invasive

JTAG

Currently JTAG images from Windows Phone 8 can be imported into Oxygen Forensic® Detective using the Oxygen Forensic Extractor or the toolbar Import file button > Import Windows Phone JTAG image. The currently supported automatically parsed artifacts include:

- Phonebook
- Messages
- Calendar
- Event Log
- Tasks
- File Browser
- Applications
**Blackberry 10 device acquisition**

**Logical**

Currently, we support USB Cable connection and Backup Import for BlackBerry 10 devices. To import a backup, use the **Import file** button > Import BB10 backup. The supported collection items include:

- Phonebook
- Messages
- Calendar
- Event Log
- Notes
- Tasks
- File Browser
- Applications
- Dictionaries

**Physical**

Oxygen Forensic® Detective does not support the physical collection of BlackBerry 10 devices. However, BlackBerry 10 Chip-off images can be imported and parsed for user data as described above. Simply go to Oxygen Forensic Extractor or press **Import file** button > Import BlackBerry 10 Chip-off image.
Memory card extraction

Oxygen Forensic® Detective offers physical data extraction from memory cards of FAT32 and Ext format. Forensic experts can acquire full evidence from supported memory cards that are connected via card reader to Oxygen Forensic® Extractor. To connect a memory card, use the option below and follow the instructions:

The extracted data set may include photos with geo coordinates, videos, documents and other files. Deleted information is automatically recovered and shown with a trash bin icon. Extracted memory card files can be used in analytical sections, like Timeline and Search.
**SIM card data extraction**

Oxygen Forensic® Detective offers the ability to extract data from SIM cards via SIM card reader. Forensic experts can connect one or several SIM card readers that are compatible with Windows OS system. No special settings are required for connection. In case a SIM card is locked with a PIN code, it can be entered in the corresponding window in Oxygen Forensic® Extractor.

The program acquires both actual and deleted SIM card messages, contacts, and calls. Once acquisition is complete, you can view SIM card data together with other extractions in analytical sections, like Timeline or Social Graph.
Importing backups and images

Besides device connection and data extraction, Oxygen Forensic® Detective gives you an opportunity to import various backups and device images where all the extracted data is already saved. You can either create this backup file in our software and import it on another PC for analysis or open a backup file made by a phone management software, like iTunes for iPhone.

You can also import other image types ranging from JTAG and ChipOff images to images created by other mobile forensic solutions.

Go to toolbar sub menu or click Import via Oxygen Forensic® Extractor. This will open the Extractor with several options, some with sub menus.

Press Import backup file button on the main toolbar to import and parse a backup:

Currently Oxygen Forensic® Detective supports:
- Oxygen Cloud backup (Cloud Extractor—OCB file)
- Oxygen Backup (OFB file)
- iTunes Backup
- Apple Backup/Image
  - Non-Encrypted Apple DMG Image
  - Apple File System Tarball/Zip
  - Decrypted Elcomsoft DMG
  - Encrypted Elcomsoft DMG
  - Decrypted Lantern DMG
  - Encrypted Lantern DMG

- XRY DMG
- Apple Production DMG
- Apple Production v.2
- Windows Phone Backup
- Windows Phone 8 JTAG Image
- UFED backup/image
- Android Backup/Image
  - Android Backup
  - File System Image Folder
  - File System Tarball/ZIP
  - Android Physical Image /JTAG
  - Nandroid Backup (CWM)
  - Nandroid Backup (TWRP)
  - Android YAFFS2
  - Android TOT container
  - Xiaomi backup
  - Oppo backup
  - Huawei backup
- BlackBerry Backup
- Nokia Backup
- Memory Card Image
- UICC image
- Drone image
Viewing Extracted Data

The Devices section lists all the devices connected and seized previously as well as actions available for them.

Desktop View

On the desktop view you will be able to see at the left grid the Devices that you have acquired. Once you have assigned a device to a specific case, the case name will appear in the grid as well.

Desktop View: Command Line

The command line is located above the desktop view of the main window and contains the main buttons.
Connect Device
This button allows you to start an Extractor with Auto Device Connection or contains options for Fast backup/image extraction.

Import File
This button gives you options of importing various backups.

Open Case Button
This button lets you manage the devices by assigning them to cases as well as change database storage for the acquired phones.
Save case – allows to save a created case with with an .ofb extention.
Add case – allows for creating a new case by adding a case name and case notes
Remove case – removes the selected case and devices from Oxygen Forensic software
Save device – saves information about devices into an.ofb backup file. The file can be used to restore information later on with Extractor
Remove device – removes selected devices form the list
Devices storage – allows storing software database on a different disk. Use it when you have a specific drive to hold the database (such as a removable flash drive), or when you are short on free disk space.

Save To Archive
This buttons allows you to save acquired devices with an .ofb extensions in order to share them with a colleague that has Oxygen product as well.

Analytics
You will have an option of quick access to any analytical features of the software.
Export/Print

Prints device data allowing you to choose specific sections and applications or only export the Key Evidence section data.

You can view **Device information** in a separate window. This section will also include summarized information about all the device owner accounts in various social networks, messengers and other services.
Basic Sections

The **Phonebook** section contains contact list with personal pictures, custom field labels and speed dials. Deleted contacts from Apple iOS and Android OS devices are highlighted with a blue color and marked by a “basket” icon.

The **Calendar** section displays all meetings, birthdays, reminders and other events:

The **Tasks** section displays all the tasks with priority marks and their date/time:

The **Notes** section allows viewing notes with their date/time:

SMS, MMS, E-mail, iMessages and messages of other types are shown in **Messages** section:

Deleted messages from Apple iOS and Android OS devices are highlighted with a blue color and marked by a “basket” icon. They are automatically recovered from SQLite databases.

**File Browser** section gives you an access to the entire mobile device file system, including photos, videos, voice records and other files. Deleted files recovery is also available but highly depends on the device platform (supported for Android physical dumps, WP JTAG images, BlackBerry Chip-off, etc):
Incoming, outgoing, missed, Facetime calls history, GPRS and Wi-Fi sessions – all this information is available in Event Log section:

Deleted calls from Apple iOS and Android OS devices are highlighted with a blue color and marked by the “recycle bin” icon.

Web Connections

Web Connections section shows all web connections in one list and allows examining hot spots on the map. In this list forensic experts can find out when and where the suspect used Internet access and detect his location.

The first bookmark permits users to inspect all Wi-Fi connections. Oxygen Forensic® software extracts an approximate geo location of the place where Wi-Fi connection was used. Mini Google Maps are generated and shown according to SSID, BSSID and RSSI information extracted from the mobile device.
The other bookmark allows examining information about **Locations**. It presents the information about all the network activity of the device (Cell, Wi-Fi and GPS). It is supported for Apple iOS (jailbroken) and Android OS (rooted) devices.

**Passwords**

Oxygen Forensic® software extracts information about passwords from all possible sources: iOS keychain, apps databases, etc. Passwords can be retrieved from Apple iOS, Android OS and Windows Phone 8 devices.

**Applications**

The **Applications** section shows detailed information about system and user applications installed in Apple iOS, Android, BlackBerry 10 and Windows Phone 8 devices. Currently we support 400+ unique applications and 7000+ app versions.

Every app has a special User Data tab where all parsed user data is located. This tab contains aggregated data of the application prepared for convenient analysis (passwords, logins, all the messages and contacts, geo locations, visited places with coordinates and maps, deleted data, etc.).

Besides User Data tab Application viewer has:
- Application information tab shows the whole application registry from which data is parsed
- Application files tab presents all the files (.plist, .db, .png, etc.) associated with the app

For your convenience applications are divided into several groups on program Desktop.

Social Networks

The Social Networks section includes sub-sections with data extracted from popular social networking and dating applications: Facebook, Instagram, Twitter, LinkedIn, Tinder, Tumblr, etc.

The Facebook section allows examining the device owner’s friends list together with messages, photos, search history, geo location and other important information.
Messengers

The Messengers section includes sub-sections with data extracted from the most popular messengers: Facebook Messenger, Hangouts, Kik, Line, Skype, WeChat, Whatsapp, Viber, etc. **WhatsApp Messenger** allows viewing the contact list, messages, shared data, deleted info and other evidence.

Productivity

Oxygen Forensic® software supports mobile productivity applications – Evernote, Dropbox, Google Translate, Google Mail, iBooks, Remember The Milk, Yahoo Mail, etc. Productivity group offers at-a-glance access to emails, tasks, notes, account settings, shared photos and documents, and so on.

**Evernote** section allows viewing all the notes created, shared and synced by the device owner. Each note is created with the geo coordinate of the place where the device owner is located and this information is available in Oxygen Forensic® software. There is an opportunity to analyze deleted notes as well.

Web Browsers

Web Browsers section allows the user to extract and examine cache files such as a list of Internet sites and downloaded files of the most popular mobile web browsers (preinstalled as well as 3rd party ones) including, but not limited to Safari, Default Android Web Browser, Dolphin, Google Chrome, Opera, SkyFire, etc.

**Safari** section shows the whole history of browsing as well as bookmarks and web cache.

Navigation
Navigation section includes sub-sections with data extracted from the most popular navigation apps: Apple Maps, Google Maps, Yandex Maps, Here Maps, etc. **Google Maps** section stores all the search and route history created by the device owner.

Travel

Travel section includes sub-sections with data extracted from the most popular travel apps: Delta Airlines, Booking.com, Expedia, TripIt, etc. **Booking.com** section shows all the device owner’s hotel bookings worldwide as well as searches and hotels added to favorites.

Fitness

Fitness section includes sub-sections with data extracted from the most popular health & fitness apps: Endomondo, Nike+ Running, RunKeeper, Runtastic. These applications store the user’s sport activities and a lot of geo coordinates left by them. Analysis of the user’s locations can be of great forensic value to the mobile device examiners. **RunKeeper** section shows all the device owner’s sport activities, their locations and friends with whom he shares his sport achievements.

Multimedia

Multimedia section includes sub-sections with data extracted from the most popular multimedia apps: Hide It Pro, YouTube, etc.
Hide It Pro section shows the media files (images and video) that were hidden by the device owner. To see them on the device the password is required. Oxygen Forensic® software grants access to this hidden data bypassing the password.

Finance

Finance section includes sub-sections with data extracted from the most popular finance and Bitcoin apps, like PayPal, Breadwallet, Jaxx Blockchain, etc.

Paypal section shows all the device owner’s payment transactions made in PayPal account.

Drone

Drone section includes sub-sections with data extracted from the most popular drone apps, like DJI GO, DJI GO 4, Free Flight Pro, etc. Forensic examiners can extract the drone flight history, pictures and videos uploaded to the app, drone owner account details and even deleted data. Oxygen Forensic® software can also extract and decrypt DJI token from drone mobile apps. This token will give access to DJI cloud data.

Analyzing Data

Oxygen Forensic® Detective and Oxygen Forensic® Analyst versions contain a set of unique analytical sections: Aggregated Contacts, Links and Stats, Social Graph, Timeline, Search, Key Evidence, etc.

Timeline

Timeline section organizes all calls, messages, calendar events, application activities, web connections history, etc. in a chronological way so it is easy to analyze the device usage history without any need to switch between different sections. Timeline section is supported for one or
several mobile devices so you can easily analyze the group activity in a single graphical view. The data can be sorted, filtered and grouped by dates, usage activity, contacts or geo data.

The GEO Timeline tab allows experts to view all geo location information from the device, locating places where the suspect used the mobile device. With the help of Maps and Routes button investigators can build routes to track the device owner’s movements within specified time frame or find frequently visited places.

The section also offers several analytical charts that allow to determine the user’s activity within specified time period, with which contacts he was most active and in what applications.

**Aggregated Contacts**

The program with its *Aggregated Contacts* section allows forensic specialists to analyze contacts from multiple sources such as the Phonebook, Messages, Event Log, various Messengers and Social Networks and other apps. It also shows cross device contacts from several devices and contacts in groups created in various applications. By enabling aggregated contacts analysis, the software greatly simplifies investigators’ work and allows discovering relations and dependencies that could otherwise escape the eye.

**Links And Stats**

The *Links and Stats* section provides a convenient tool to explore social connections between device owners and their contacts by analyzing calls, text messages and messengers activities.

Table view offers in-depth analysis of the device user’s communication including all contacts, phone numbers and remote parties along with communication duration and produces a concise summary of the forensically important data.
Diagram view with a graphical chart presents a quick overlook of communication circles, allowing forensic experts to determine and analyze suspects’ communications at a glance.

Moreover experts can determine common contacts and communication activity between detected groups of suspects.

**Social Graph**

Social Graph allows investigators to review social connections between the owner of a mobile device and his contacts, as well as to investigate connections between multiple device owners. The section is highly flexible, and can be configured to either view communication statistics and build communication circles of the most frequently contacted contacts for a single device owner, or analyze links and connections between multiple device owners.

By using Social Graph, investigators have an opportunity to quickly determine common contacts discovered in multiple devices, analyze their interactions and review how they link and connect to each other in a single glance. The graph is highly customizable, allowing to include or exclude individual contacts or groups, view communications in a particular app thus to concentrate on what is essential.
Search

It’s a common situation for you to need to find some text, person or phone number in the extracted mobile device information. Oxygen Forensic® Detective has an advanced search engine.

Global Search allows discovering user data in every section of the device. Tool offers searching for text, phone numbers, emails, geo coordinates, IP addresses, MAC addresses, Credit Card numbers and hash sets (MD5, SHA1, SHA256, PhotoDNA, Project VIC). Regular expressions library is available for more custom search.

Experts can search data in a single device, all devices of the case or all acquired devices. They can choose the sections where to search the query, apply boolean terms or chose any of predefined patterns.

Keyword list manager allows creating custom set of terms and perform search for all these terms at once. For example, these can be the lists of names or the set of offensive words and phrases.

Global Search tool saves all results and offers printing and preparing reports for any number of searches.
Key Evidence

The Key Evidence section offers clean, uncluttered view of evidence marked as essential by investigators. Forensic specialists can mark certain items belonging to various sections as being essential evidence, then reviewing them all at once regardless of their original location. Key Evidence is an aggregated view that can display selected items from all sections available in Oxygen Forensic® software. The section offers the ability to review relevant information at a single glance, concentrating one’s efforts on what really matters and filtering out distracting, unimportant data.

Integration with Project VIC

Oxygen Forensic® software offers seamless integration with Project VIC and allows to use the hash sets for identification of child exploitation content. Now forensic experts can upload the library much faster than in any other competing tool and search child abuse media files in mobile and cloud extractions by Project VIC hash sets. The found results are visualized both in Project VIC section and on a separate tab in File Browser and are categorized according to the Project VIC classification.

Generating Forensic Reports

Oxygen Forensic® software allows an examiner to print reports containing all the extracted device, cloud or drone information. You can also select only specific section(s) as well.
Extracted data can be exported to a number of file formats – PDF, XLS, RTF, etc.
Oxygen Forensic® software contains viewers that can open specific databases and files.

**SQLite Database Viewer**

The SQLite Database Viewer allows analyzing database files from Apple, Android, BlackBerry 10, WP 8 devices in SQLite format. These files contain information about messages, notes, calls, applications, etc. The main Viewer window presents tables and the information they contain:

![](image)

Displaying deleted data for SQLite databases:

![](image)

The Viewer allows to search data through all the database, perform visual and non-visual SQL queries and convert values into readable format with built-in converter. SQLite database data reports are also available.

**Plist Viewer**

The Plist Viewer allows analyzing .plist files from Apple devices. These files contain information about Wi-Fi access points, speed dials, the last cellular operator, Apple Store settings, Bluetooth settings, global applications settings, etc:
**Oxygen Forensic® Cloud Extractor**

The Cloud Extractor is available in Oxygen Forensic® Detective. Oxygen Forensic® Cloud Extractor is a tool that allows the examiner to acquire data from more than 50 cloud storages:

- iCloud data
- Google data
- Microsoft data
- Samsung data
- Huawei data
- Mi Cloud data
- DJI Drone cloud data
- Data from E-mail and WhatsApp Server
- Social media data
- Other cloud storages data

Forensic experts may utilize either account credentials or token to enter the cloud account to acquire the cloud data. Extracted credentials and tokens from a mobile device are organized and displayed in the Cloud Accounts section of Oxygen Forensic® Detective.

Oxygen Forensic® Detective can also find passwords and tokens on the user’s computer with the help of Oxygen Forensic® KeyScout utility. The utility is available from the Tools menu in Oxygen Forensic® Detective or in the main menu of the Cloud Extractor.
KeyScout installs to a flash card and collects credentials from Windows PCs. The collected credentials can then be imported into Oxygen Forensic® Cloud Extractor for immediate use.

You can start the Cloud Extractor from the main interface.

Or from the dropdown Tools menu.

You can also start cloud extraction from the Cloud Accounts section. In this section you can also save account data as an OCB file and import it later into the Cloud Extractor for the analysis.
Before accessing the Cloud data the Cloud Extractor will validate the acquired credentials. You will be given a choice to choose what services, what files from those service and what date range you wish to acquire:

After the cloud data is acquired it can be viewed in Oxygen Forensic® Detective and merged with other extractions for deep data analysis in Timeline, Social Graph and other analytical tools.

**Services exclusively supported by Oxygen Forensics:**

1. Ability to extract critical evidence directly from **WhatsApp Server**. Forensic experts can acquire undelivered messages, unanswered calls, information about messages deleted from private and group chats, profile pictures and status messages of the account owner and contacts, original messages embedded into the reply, broadcast messages, etc. To use this feature, select WhatsApp Cloud service in the list of services in Oxygen Forensic® Cloud Extractor and follow the instructions.
2. Oxygen Forensic® Detective can acquire a **WhatsApp Cloud token** from Android devices that can be used to decrypt WhatsApp backups from Android devices, WhatsApp Google Drive as well as WhatsApp iCloud backups associated with the same phone number. The new decryption method leaves no digital traces and is a good alternative to the commonly used method with the key file. With this token you can also acquire undelivered messages and unanswered calls directly from the WhatsApp Server.

3. Ability to extract user data from **Samsung, Mi Cloud** and **Huawei** cloud accounts. The acquired evidence set will include not only actual but also deleted information and media files. For example, there is an opportunity to acquire photos and videos with geo coordinates from Samsung cloud that were deleted from a Samsung mobile device.

**Oxygen Forensic® Call Data Expert**

This module is available in Oxygen Forensic® Detective only. Oxygen Forensic® Call Data Expert is a program that allows importing and analysing CDR files (Call Data Records) received from mobile service providers regardless of the difference in their column formats and file layouts.
Oxygen Forensic® Call Data Expert conveniently guides the examiner through the process of converting the file into unified format in order for the file to be viewed and analyzed.

Afterwards the processed results can be viewed and analyzed by the expert allowing to build direct and indirect links between callers on the graph. Processed and analyzed results can be saved to external files on PC.

**Oxygen Forensic® Maps**

This module is available in Oxygen Forensic® Detective only. The Oxygen Forensic® Maps section offers advanced analytical capabilities for geo data analysis including:

- Open device, cloud or drone extractions directly from Oxygen Forensic® Detective or import drone flight logs, KML or GPX files from computer.
- Identify device owner’s frequently visited places
- Visualize user’s movements within specified period of time
- Pinpoint common locations of several device users

Oxygen Forensic® Maps can be used either online or downloaded for offline work.
Drone data
Oxygen Forensic® Detective currently offers the most verbose drone data parsing and analysis from drones themselves, their mobile applications and cloud storages.

Physical acquisition
Oxygen Forensic® Detective allows the expert to connect a DJI Spark drone to the examination computer via USB cable and conduct a physical collection of the embedded storage chip. Once the drone is connected a physical acquisition is available via drone rooting. It will reveal the drone complete flight history with GPS locations and metadata which includes valuable facts like speed, altitude, direction, and other evidentiary parameters.

Oxygen Forensic® Detective can also import already made drone physical dumps and parse GPS locations showing valuable route data to the examiner all within Timeline section.
Mobile apps

Oxygen Forensic® Detective extracts and parses various drone apps installed in Apple iOS and Android devices. These apps may contain the drone flight history, uploaded media files, files of other app users, deleted data and the list of drones connected to the app account. Moreover, a cloud token can be decrypted from a drone mobile app that will allow to access the drone cloud and extract additional evidence.

Cloud storage

Oxygen Forensic® Detective allows experts to access the drone cloud via password or token and extract lots of valuable data without having the drone itself:

- Account details: user name, photo, bio, website, country, date of account creation and social networks linked to this account.

- Drone information: model, total flight time, distance, and number of flights, countries where it flew, maximum speed, altitude, distance, and duration of flights, etc.

- Flight details: history with geo data, time stamps, speed, altitude, etc.
Drone logs import

The software also allows to import drone log .dat files directly into Oxygen Forensic® Maps to visualize locations and track a drone route. Logs can be taken from the drone dump or from DJI Assistant app installed on the drone owner’s computer.
General Connection Instructions

1. Make sure you have installed the drivers for the device. You can download the driver pack from your customer area (Service/Visit customer area menu in the software).

2. If you connect a device press Connect device button on the toolbar to start Oxygen Forensic® Extractor:

   ![Oxygen Forensic® Extractor](image)

   If you import an image or backup press Import file button on the toolbar and browse for it on your PC:

   ![Import backup file](image)

3. If you connect Apple iOS device plug it in, unlock and trust computer on the device:
4. If you connect **Android OS device**, enable Developer mode on it. Go to Settings > About Phone > Build number menu and tap it 7 times.

Then go to Settings>Developer Options>USB Debugging menu on the device. Tap the USB Debugging checkbox and plug the device in to the computer:

Once you connect a device running Android 4.2.2 or higher, the PC shows a dialog asking to accept an RSA key that allows debugging on this computer. Press OK to allow it.
5. If Android OS device is password-protected check if it is supported by our bypass methods located under Physical data acquisition in Oxygen Forensic® Extractor.

6. After the device is connected via cable press Device Acquisition and wait till the device is correctly detected by the software:
7. Fill out the case details and select Watch Lists with keywords if necessary:

8. Select which selections you need to acquire and enjoy extracted data!

Copyrights and contacts

Oxygen Forensic® Detective and OxyAgent are the trademarks and properties of Oxygen Forensics company.

Windows 10, Windows 8, Windows 7, Windows Phone are registered trademarks of Microsoft Corporation.

All other trademarks are owned by their respective companies.

Contacts:
The website:  http://www.oxygen-forensic.com
E-mail: support@oxygen-forensic.com
Phone: +1 (877) 969-9436