

Oxygen Forensic[®] Detective Analysis Table

Oxygen Forensics is a leading global digital forensics solutions provider, specializing in mobile device, cloud, drones, and IoT data. Oxygen Forensic[®] Detective (OFD) is the only all-in-one software that enables law enforcement and enterprises to extract and decode data from various sources, analyze digital evidence, and draw useful insights for legal proceedings and criminal investigations in one intuitive interface. Below is a list of the features included in a license, at no additional charge.

Oxygen Forensic[®] Detective v.14.6

MOBILE FORENSICS

- **Number of supported devices** **30,565**

OFD supports a wide range of Apple iOS and Android devices as well as KaiOS devices and MTK feature phones.

- **Locked device support** **Yes**

OFD offers proprietary screen lock bypass methods for Android devices based on Exynos, Kirin, Qualcomm, MTK, and Spreadtrum chipsets.

- **Unlocked device support** **Yes**

OFD offers various methods for unlocked Android devices: full file system extraction, extraction via OxyAgent, APK Downgrade method, and others.

- **iOS support** **Yes**

OFD v14.6 has added the ability to extract the full file system and keychain data via checkm8 vulnerability from Apple iOS devices running iOS 15.6 beta. If running iOS 16.0 Beta, full file system and keychain data can be extracted from iPhone 8, iPhone 8 Plus, and iPhone X. We continue to extend our support for iOS Agent method to the devices with iOS versions 15.0-15.1.1. OFD also provides the iTunes backup method and full file extraction via SSH.

- **Device images parsing** **Yes**

OFD imports and parses a great number of backups and images including GrayKey, Chip-Off, JTAG images, Huawei, Xiaomi, Samsung SmartSwitch backups, Warrant Returns, Google Takeout data, and many others.

- **Brute force of encrypted backups and images** **Yes**

OFD has a built-in module that offers brute force for iTunes backups, Huawei backups, various Android backups, and physical images.

- **Media card extraction** **Yes**

OFD provides physical extraction of media cards via memory card reader.

- **SIM card extraction** **Yes**

OFD offers SIM card data extraction and recovery via SIM card reader.

- **Smart watch extraction** **Yes**

OFD offers MTK smart watch data extraction via standard USB cable.

- **Unique apps support** **752**

OFD divides unique apps into various categories, including Business, Fitness, Messengers, Navigation, Social Networking, and more.

Version 14.6 adds selective chat extraction from WhatsApp and WhatsApp Business apps from unlocked Android devices via Android Agent.

- **App versions support** **33,155**

App support is Oxygen Forensics priority. We update parsing of most popular apps in every software release. On-demand app support is available. We also focus our research on secure messengers and vault apps decryption, including WickrMe, Signal, Telegram, CoverMe, and many others.

CLOUD FORENSICS

- **Cloud services** **102**

The built-in Oxygen Forensic® Cloud Extractor supports the largest number of cloud services, including WhatsApp QR, WickrMe, Mi Cloud, Huawei Cloud, E-mail Server, iCloud backups, and many others. The new version of OFD has added support for OnlyFans service.

- **Connection configurable through proxy** **Yes**

Connection configurable through proxy allows users to hide their real IP address while working, which makes investigation process safer.

- **Credentials collection** **Yes**

OFD extracts credentials from Apple iOS and Android devices as well as Windows, macOS, and Linux computers. They include Google, Facebook, Twitter tokens, and lots of passwords to various apps that can be immediately used for cloud data extraction.

- **WhatsApp extraction methods** **Yes**

Oxygen Forensic® Cloud Extractor offers a method of WhatsApp backup decryption via phone number, access to the WhatsApp server, and WhatsApp data extraction via QR method.

COMPUTER FORENSICS

- **Live system extraction** **KeyScout**

Oxygen Forensic® KeyScout extracts credentials, user data from all popular desktop web browsers, messengers, and email clients as well as collects system files on live system. Moreover, it can capture RAM and save it to raw format for further analysis. Various filters and search templates are available for targeted data collection.

- **Supported images** **Yes**

Oxygen Forensic® KeyScout can parse various Windows, macOS, and Linux images, including E01, AD1, L01, and many others. Virtual machine images are also supported.

- **Compatible with** **Windows | MacOS | Linux**

Oxygen Forensic® KeyScout runs on all the three indicated OS.

IOT FORENSICS

- **IoT** **Amazon Alexa | Google Home**

OFD extracts complete IoT data, including voice recordings from mobile apps or the cloud. Our solution can find IoT cloud credentials in mobile devices and in PCs.

DRONE FORENSICS

- **Drone extraction** **Yes**

OFD offers the ability to do drone extraction via USB cable and supports commonly used methods of drone physical images and flight log parsing from popular DJI and Parrot models.

- **Drone mobile app parsing** **Yes**

OFD parses native DJI and Parrot drone apps from Apple iOS and Android devices. They can be a good alternative to direct drone extraction as they also contain drone flight history.

- **Drone cloud** **Yes**

OFD offers extraction of drone flight history and other information from DJI, SkyPixel, and Parrot clouds that can be accessed via login/password or token found in mobile apps or on PCs.

DATA ANALYSIS

- **Events and links analysis** **Yes**

OFD offers built-in Timeline and Social Graph for deep events, and links analysis both for one extraction and a case.

- **Image categorization** **Yes**

Image categorization engine classifies images into 18 different categories: pornography, extremism, graphic violence, drugs, alcohol, weapons, gambling, child abuse, documents, currency, identification documents, and other.

- **Facial categorization** **Yes**

Categorize human faces using this built-in technology. The Facial categorization feature is available in the Faces section and can identify faces wearing glasses, hats, and protective masks. Moreover, search by faces is available in the Search section.

- **Optical Character Recognition (OCR)** **Yes**

This feature converts words found in images into machine-encoded, searchable text. 12 languages are supported. Once OCR has been run, investigators can use the quick filter to search for text across the processed images.

- **Maps** **Yes**

OFD offers both online and offline maps with the rich functionality of defining frequently visited places, common locations, and building routes including interactive ones.

- **Data search** **Yes**

OFD provides a great variety of search options – predefined keyword lists, regular expressions, faces, hex search, search by hash sets including Project VIC and PhotoDNA, search in parsed data and search inside files, etc. Search can be performed in one or several extractions.

- **Tags and filters** **Yes**

OFD offers the ability to mark extracted items as important as well as set predefined and custom tags, and filter by them.

- **Call data records analysis** **Yes**

Process and analyze call data records obtained from wireless providers. Visualize geo coordinates on the map and identify links between callers.

- **Data viewers** **Yes**

OFD has built-in Plist and SQLite Viewers with the powerful functions to analyze the contents of databases and files.

- **Evidence viewer** **Yes**

A free portable Oxygen Forensic® Viewer is designed to view all types of extractions previously saved to the Oxygen Forensic® Backup (OFBX) format.

DATA EXPORT

- **Number of file export formats** **10 formats**

OFD allows users to export all or selected data to a wide range of formats that include PDF, RTF, XLS, XML, Load File, and many others.