Oxygen Forensic® DETECTIVE

version 12.5 JUNE 2020

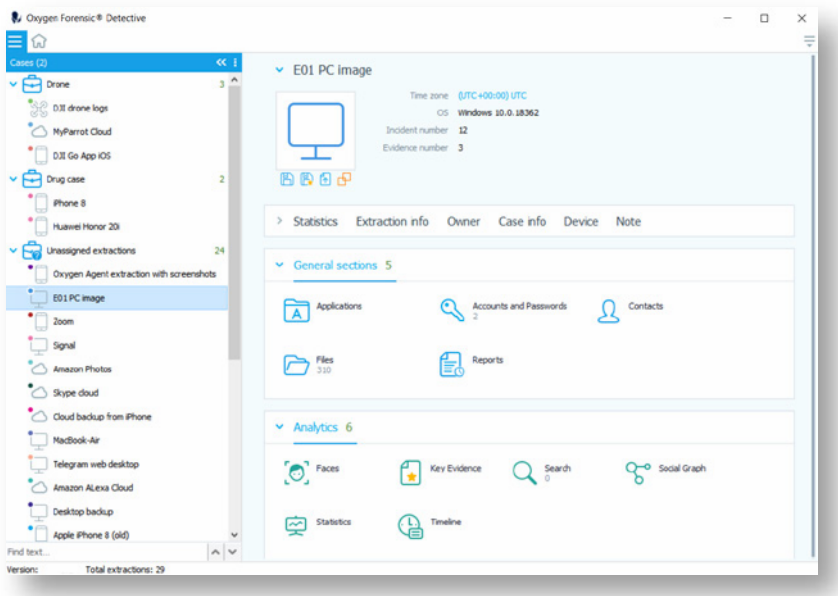
37,002	83	508	16,100+	63
devices	cloud services	unique apps	app versions	computer artifacts

E01 image support

COMPUTER ARTIFACTS, MOBILE FORENSICS

Oxygen Forensic® Detective 12.5 comes equipped with E01 PC and Android image support. To import a PC image, click the Desktop Extractions link on the software Home Screen and follow the instructions. Once the image is parsed, the extraction will be added to the device list in the Oxygen Forensic® Detective interface. Investigators will be able to merge it with other extractions (e.g., mobile or cloud) for comprehensive analysis in Files, Social Graph, Timeline, and other sections. The evidence set will include user data and credentials from the most popular Messengers, Email clients, and Web browsers. Currently E01 images of NTFS file systems are supported.

Oxygen Forensic® Detective 12.5 also imports and parses complete evidence from Android E01 images to include app data, deleted information, files, contacts, messages, calls, and other artifacts.



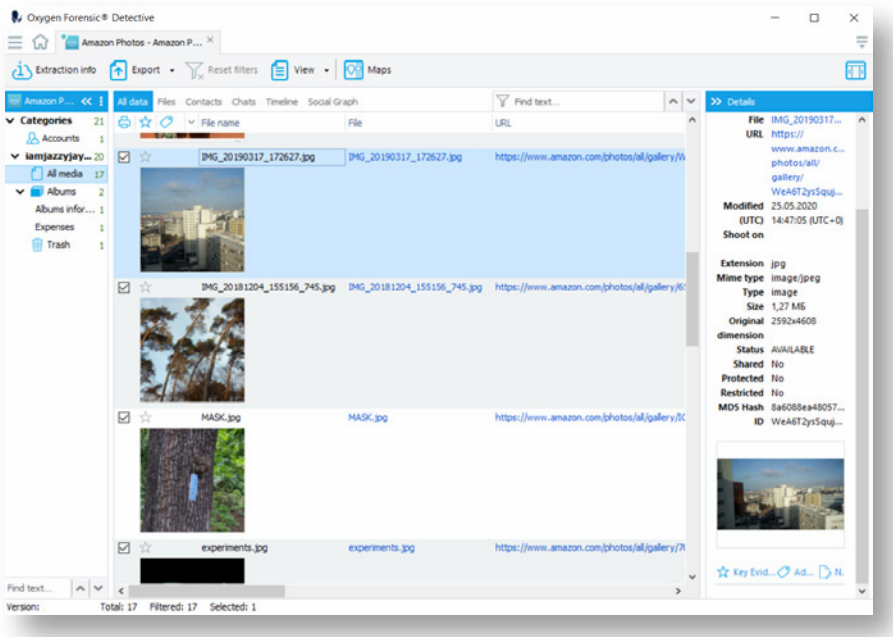
Picture 1. E01 Image Support

Amazon Photos extraction

CLOUD FORENSICS, MOBILE FORENSICS

Amazon Photos is a popular service for storing photos in the Amazon cloud. Photos can be uploaded with iOS, Android apps, Kindle devices, or through the Cloud Drive website. Oxygen Forensics introduces a comprehensive solution to extract Amazon Photos both from mobile devices and the cloud.

Oxygen Forensic® Cloud Extractor now provides access to complete Amazon Photos data from the cloud. Investigators can access the Amazon cloud via Amazon login/password or Amazon token extracted from mobile device. The cloud evidence will include account details, uploaded media files with EXIF information, deleted files, detailed information about groups, albums, etc. Moreover, Oxygen Forensic® Detective 12.5 fully extracts and parses data from Amazon Photos, as well as various apps from Apple iOS and Android devices.



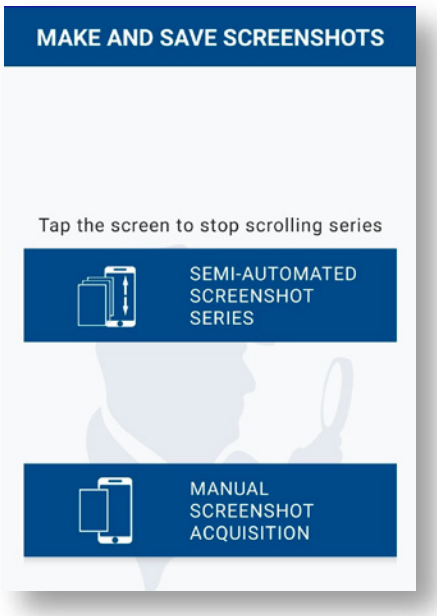
Picture 2. Amazon Photos Extraction

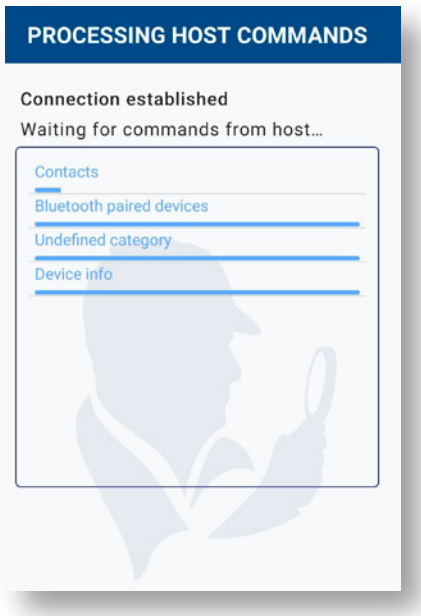
Enhanced OxyAgent utility

MOBILE FORENSICS

We offer a wide range of methods for Android device extraction that include screen lock bypass methods, rooting, ADB backup creation, and our OxyAgent method for logical acquisition. Our OxyAgent allows investigators to recover basic evidence sets from every supported Android device. In the new version, we've significantly enhanced the OxyAgent utility:

- Data extraction via Wi-Fi network: This feature is of great value, in case there are connection problems or the data extraction via USB cable is not possible due to the USB port being broken.
- The ability to select data categories for extraction.
- The ability to create screenshots of Android device data using the installed OxyAgent utility. We offer two modes, manual and semi-automatic. The semi-automatic mode allows screenshots to be made automatically from any open device screen. Screenshots can be imported into Oxygen Forensic Detective together with device data collected by OxyAgent and later viewed as one case.



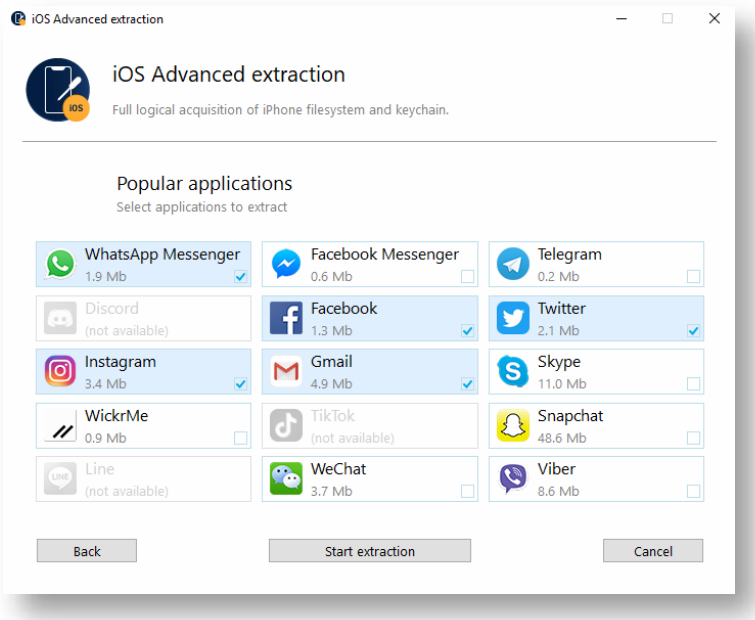


Pictures 3 and 4. OxyAgent utility

Selective extraction from Apple iOS devices

MOBILE FORENSICS

Oxygen Forensic® Detective now provides selective data extraction for jailbroken Apple iOS devices. If investigators need to acquire only particular app's data, this option will significantly save time. Our Oxygen Forensic® Extractor offers the ability to parse evidence from the most popular apps, including WhatsApp, Facebook, Twitter and others.



Picture 5. Selective Extraction from Apple iOS devices

Import of Twitter Warrant Returns

DATA IMPORT

In Oxygen Forensic® Detective 12.5 investigators can now import and parse Twitter Warrant Returns. The evidence set will include the account information, chats, tweets, devices and other data. This is the 4th type of Warrant Return we've added along with Snapchat, Facebook, and Instagram Returns.

New computer artifacts

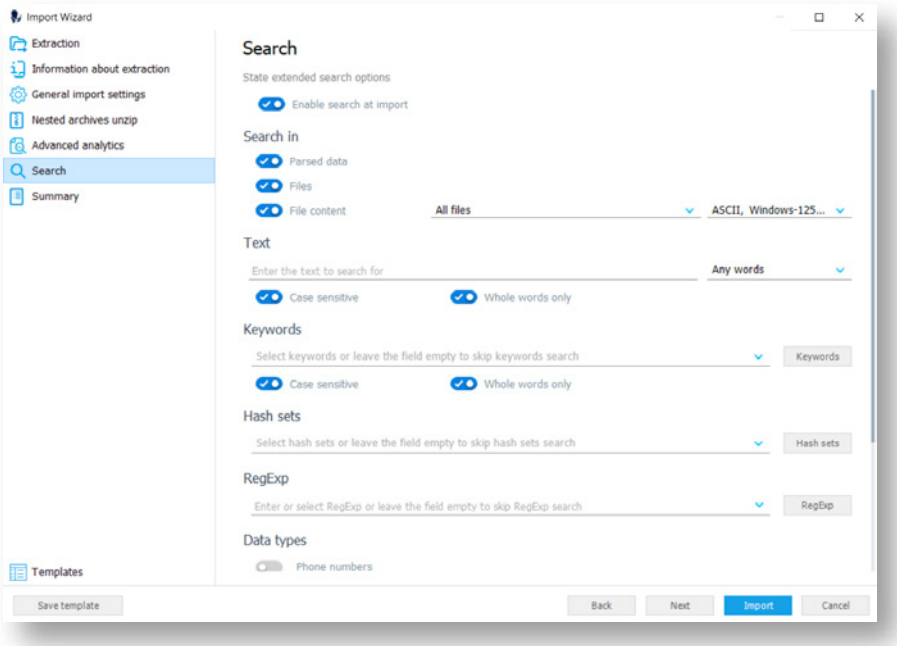
COMPUTER ARTIFACTS

The updated Oxygen Forensic® KeyScout can now collect the Task Scheduler data on Windows-based computers, as well as 4 new pre-installed Apple apps on macOS - Apple Contacts, Apple Calendars, Apple Maps, and Apple Mail.

Search during backup Import

DATA IMPORT

Oxygen Forensic® Detective supports over 30 various device and backup images. Now while importing a backup, investigators have the ability to configure the data search criteria in the Import Wizard to include: search data by text, keywords, hash sets, regular expressions, file names, or file content. Once the import is finished, investigators can view search results in the Search section.



Picture 6. Search during backup Import

Updated password brute-force module

MOBILE FORENSICS

Oxygen Forensic® Detective 12.5 offers the updated password brute force module that is used to find passcodes to encrypted iTunes backups and Android images. Now investigators can use the new attack with the popular 4-9 digit PINs and Patterns provided by Passware Inc.

Device Support

MOBILE FORENSICS

We have added support for over 950 new Android devices: Xiaomi Mi 10 lite 5G, Xiaomi Mi Note 10 Lite, Sony Xperia 10 II, Sony Xperia L4, Samsung Galaxy M01, Samsung Galaxy S20 5G, etc The total number of supported devices is 37,002.

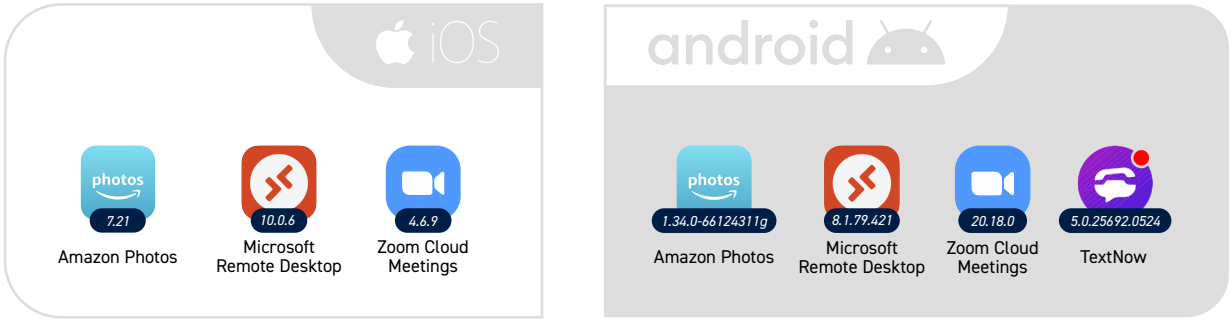
App support

MOBILE FORENSICS

The new version brings support for more applications to include Zoom Cloud Meetings, Microsoft Remote Desktop, Amazon Photos, and TextNow. Moreover, we've added location parsing from iMessages and thumbnails from Apple Photos app. Thumbnails might be of great value when the original photo no longer exists.

Overall, Oxygen Forensic® Detective 12.5 offers data parsing for over 600 new app versions from Apple iOS and Android devices. The total number of supported versions now exceeds 16,100.

New apps



Updated apps

APPLE IOS
Azar (1.42.0)
Discord (22.0)
Facebook Messenger (263.1)
Firefox (25.1)
Google Duo (89.0)
Google Chrome (81.0.4044.124)
Google Tasks (1.11.200513)
Instagram (140.0)
KakaoTalk (8.8.7)
LinkedIn (9.1.179)
Likee (3.33.0)
Skype (8.59)
SoundHound (9.4)
Speedtest (4.2.3)
Telegram (6.1.2)
VK (6.4)
WhatsApp (2.20.52)
Yandex.Maps (12.3.2)

ANDROID OS
Brosix Instant Messenger (4.5.1)
Discord (21.6)
Facebook (272.0.0.50.125)
Files By Google (1.0.312595236)
Fitbit (3.21)
Gmail (2020.03.29.306383213)
Google Chrome (83.0.4103.60)
LinkedIn (4.1.453)
OK (20.5.21)
Samsung Internet Browser (11.2.2.3)
SCRUFF (6.1802)
SoundHound (9.3.5.3)
Speedtest (4.5.7)
TikTok (16.0.4)
Twitter (8.45.0-release.00)
WhatsApp (2.20.163)
Yahoo! Mail (6.8.1)
Yandex.Maps (9.3.3)
Yandex.Mail (4.55.0)