Oxygen Forensic®
DETECTIVE

version 13.1 NOVEMBER 2020

39,000+ devices	**88** cloud services	**570+** unique apps	**18,800+** app versions	**92** computer artifacts

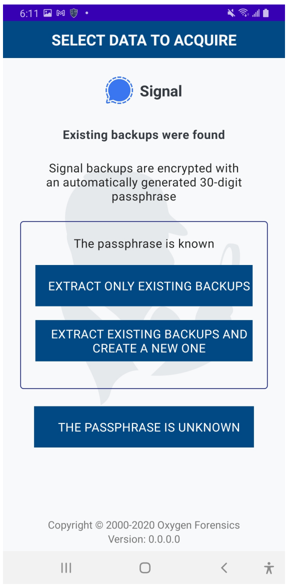
Signal Messenger extraction

MOBILE FORENSICS

Previous versions of Oxygen Forensic® Detective have allowed investigators to extract Signal Messenger from Apple iOS full file system, Android physical dumps and collect Signal data on Windows, macOS and Linux computers.

However, Oxygen Forensic® Detective 13.1 introduces yet another method of Signal data extraction from Android devices; via our OxyAgent. To run this extraction, investigators simply install our OxyAgent to an unlocked Android device .

Select "Signal", under the "Extract third-party applications data" option in OxyAgent, to extract existing backups. If there are no existing backups, you can choose to create a backup containing all the current Signal data. In either case, the evidence set will include account details, contacts, calls, and chats. Import the collected Signal data as an OxyAgent extraction to view it in
Oxygen Forensic® Detective.



6:11

SELECT DATA TO ACQUIRE

Signal

Existing backups were found

Signal backups are encrypted with an automatically generated 30-digit passphrase

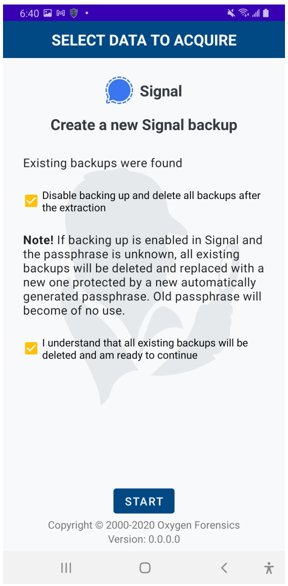
The passphrase is known

EXTRACT ONLY EXISTING BACKUPS

EXTRACT EXISTING BACKUPS AND CREATE A NEW ONE

THE PASSPHRASE IS UNKNOWN

Copyright © 2000-2020 Oxygen Forensics
Version: 0.0.0.0



6:40

SELECT DATA TO ACQUIRE

Signal

Create a new Signal backup

Existing backups were found

☑ Disable backing up and delete all backups after the extraction

Note! If backing up is enabled in Signal and the passphrase is unknown, all existing backups will be deleted and replaced with a new one protected by a new automatically generated passphrase. Old passphrase will become of no use.

☑ I understand that all existing backups will be deleted and am ready to continue

START

Copyright © 2000-2020 Oxygen Forensics
Version: 0.0.0.0

Support for MT6739 and MT6580 chipsets

MOBILE FORENSICS

We've added the ability to bypass screen locks, perform physical acquisition, and decrypt physical dumps of Android devices based on Mediatek MT6739 and MT6580 chipsets. While extracting a device, Oxygen Forensic® Detective also extracts hardware keys that are used to decrypt the collected binary image. In total, our MTK Android Physical method supports extraction and decryption for three chipsets: MT6737, MT6739 and MT6580. It should be noted, the built-in passcode brute force module is available at no additional charge.

Enhanced support for Qualcomm chipsets

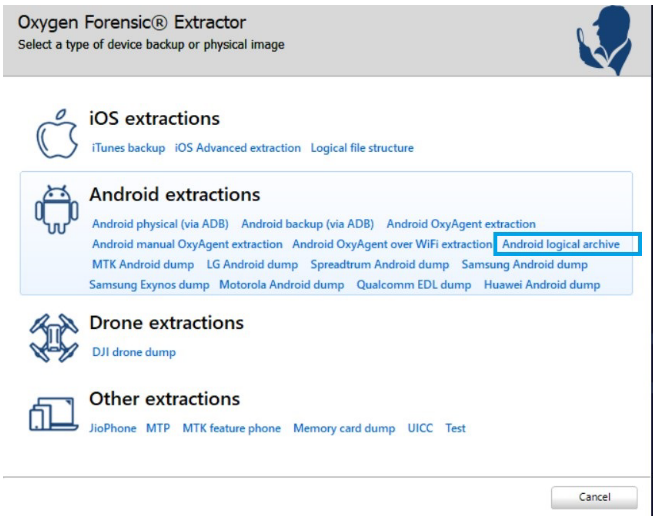
MOBILE FORENSICS

Oxygen Forensic® Detective 13.1 offers an enhanced screen lock bypass method for Android devices based on Qualcomm MSM8917, MSM8937, MSM8940 and MSM8953 chipsets. We have improved the extraction of hardware keys that are used to decrypt the extracted binary images. Supported device models now include Xiaomi A2 Lite, Xiaomi Redmi Go and Xiaomi Redmi Note 4X.

Acquisition of Android 10 devices

MOBILE FORENSICS

Oxygen Forensic® Detective 13.1 now allows investigators to perform a file system extraction of pre-rooted Android devices including those that run Android OS 10 and have File-based encryption. To extract a device, choose the "Android logical file system" option in Oxygen Forensic® Extractor and follow the instructions. When using this type of extraction users will have access to many parsed applications.



Oxygen Forensic® Extractor

Select a type of device backup or physical image

iOS extractions

iTunes backup   iOS Advanced extraction   Logical file structure

Android extractions

Android physical (via ADB)   Android backup (via ADB)   Android OxyAgent extraction
Android manual OxyAgent extraction   Android OxyAgent over WiFi extraction   Android logical archive
MTK Android dump   LG Android dump   Spreadtrum Android dump   Samsung Android dump
Samsung Exynos dump   Motorola Android dump   Qualcomm EDL dump   Huawei Android dump

Drone extractions

DJI drone dump

Other extractions

JioPhone   MTP   MTK feature phone   Memory card dump   UICC   Test

New cloud services

CLOUD EXTRACTOR

The updated Oxygen Forensic® Cloud Extractor adds support for 2 new cloud services, SecMail and Firefox Browser. At 88 unique services, the built in Cloud Extractor now supports even more services than any company in the industry.

- **SecMail** is a secure mail service. Investigators can gain access to the SecMail account via login and password. Extracted evidence will include the account information, contacts, and emails.

- **FireFox Browser.** Authorization in a browser can be done via login/ password or token found in Apple iOS devices and on Windows computers. Evidence sets will include web history, saved logins and passwords, bookmarks, opened tabs, and installed addons.

New computer artifacts

COMPUTER ARTIFACTS

With the updated Oxygen Forensic® KeyScout, investigators can now collect more new artifacts from computers. KeyScout now allows extraction of all available user data from OneDrive, Slack, and Evernote apps running on Windows and macOS computers.

In addition to applications, KeyScout can now extract several new operating system artifacts to include:

- Recent Items showing which files have been recently opened on a Windows computer.
- Files and their detailed information from the Recycle Bin on Windows OS.
- The history of WinRAR operations on Windows OS.

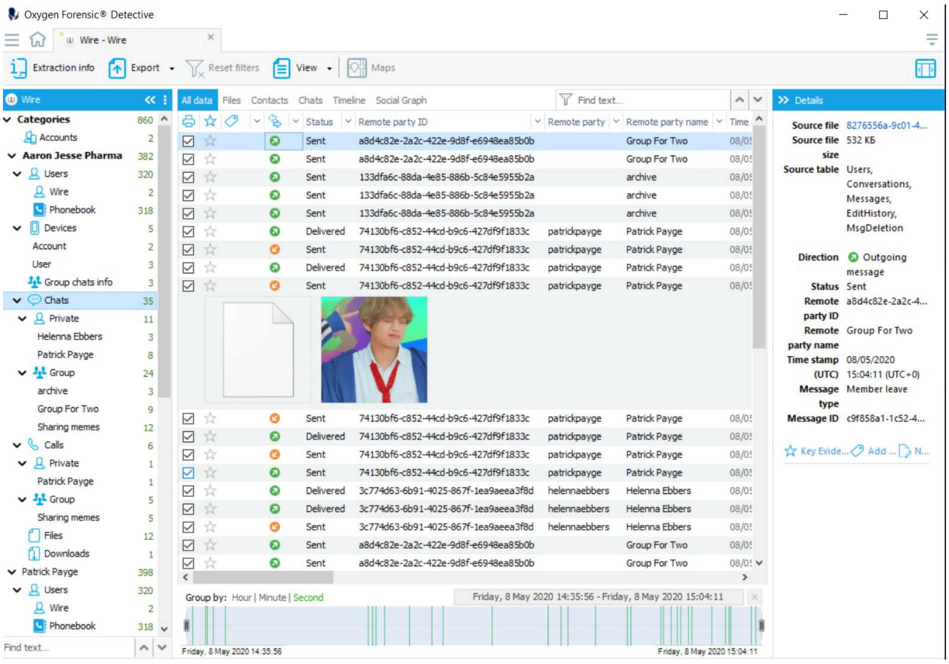
We've also significantly improved the Settings menu interface where investigators can conveniently select applications for extraction, as well as set search criteria for files.

App support

MOBILE FORENSICS

We've updated data parsing from over 800 apps. The total amount of supported app versions exceeds 18,800. Here are some important highlights for this release:

- **Wire App** - data can now be fully extracted and decrypted from Apple iOS and Android devices. Apple iOS full file system and Android physical extractions are required
- **Signal Messenger** - decryption support for data extracted from Huawei devices running Kirin chipsets
- **WhatsApp** - parsing of messages from a new ChatSearchV5f database.
- Data parsing for four more new apps - **Elyments, JioPages, Zalo** and **GroupMe**



Categories	860
Accounts	2
Aaron Jesse Pharma	382
Users	320
Wire	2
Phonebook	318
Devices	5
Account	2
User	3
Group chats info	3
Chats	35
Private	11
Helenna Ebbers	3
Patrick Payge	8
Group	24
archive	3
Group For Two	9
Sharing memes	12
Calls	6
Private	1
Patrick Payge	1
Group	5
Sharing memes	5
Files	12
Downloads	1
Patrick Payge	398
Users	320
Wire	2
Phonebook	318

			Status	Remote party ID	Remote party	Remote party name	Time
☑	☆	↗	Sent	a8d4c82e-2a2c-422e-9d8f-e6948ea85b0b		Group For Two	08/0
☑	☆	↗	Sent	a8d4c82e-2a2c-422e-9d8f-e6948ea85b0b		Group For Two	08/0
☑	☆	↗	Sent	133dfa6c-88da-4e85-886b-5c84e5955b2a		archive	08/0
☑	☆	↗	Sent	133dfa6c-88da-4e85-886b-5c84e5955b2a		archive	08/0
☑	☆	↗	Sent	133dfa6c-88da-4e85-886b-5c84e5955b2a		archive	08/0
☑	☆	↗	Delivered	74130bf6-c852-44cd-b9c6-427df9f1833c	patrickpayge	Patrick Payge	08/0
☑	☆	↙	Sent	74130bf6-c852-44cd-b9c6-427df9f1833c	patrickpayge	Patrick Payge	08/0
☑	☆	↗	Delivered	74130bf6-c852-44cd-b9c6-427df9f1833c	patrickpayge	Patrick Payge	08/0
☑	☆	↙	Sent	74130bf6-c852-44cd-b9c6-427df9f1833c	patrickpayge	Patrick Payge	08/0
☑	☆	↙	Sent	74130bf6-c852-44cd-b9c6-427df9f1833c	patrickpayge	Patrick Payge	08/0
☑	☆	↗	Delivered	74130bf6-c852-44cd-b9c6-427df9f1833c	patrickpayge	Patrick Payge	08/0
☑	☆	↙	Sent	74130bf6-c852-44cd-b9c6-427df9f1833c	patrickpayge	Patrick Payge	08/0
☑	☆	↗	Sent	74130bf6-c852-44cd-b9c6-427df9f1833c	patrickpayge	Patrick Payge	08/0
☑	☆	↗	Delivered	3c774d63-6b91-4025-867f-1ea9aeea3f8d	helennaebbers	Helenna Ebbers	08/0
☑	☆	↗	Delivered	3c774d63-6b91-4025-867f-1ea9aeea3f8d	helennaebbers	Helenna Ebbers	08/0
☑	☆	↙	Sent	3c774d63-6b91-4025-867f-1ea9aeea3f8d	helennaebbers	Helenna Ebbers	08/0
☑	☆	↗	Sent	a8d4c82e-2a2c-422e-9d8f-e6948ea85b0b		Group For Two	08/0
☑	☆	↗	Sent	a8d4c82e-2a2c-422e-9d8f-e6948ea85b0b		Group For Two	08/0

Group by: Hour | Minute | Second

Friday, 8 May 2020 14:35:56 - Friday, 8 May 2020 15:04:11

Friday, 8 May 2020 14:35:56

Friday, 8 May 2020 15:04:11

Source file	8276556a-9c01-4...
Source file size	532 КБ
Source table	Users, Conversations, Messages, EditHistory, MsgDeletion
Direction	↗ Outgoing message
Status	Sent
Remote party ID	a8d4c82e-2a2c-4...
Remote party name	Group For Two
Time stamp (UTC)	08/05/2020 15:04:11 (UTC+0)
Message type	Member leave
Message ID	c9f858a1-1c52-4...

Smart analytics

DATA ANALYSIS

We've added a Smart Filter button in the Timeline and Messages sections. This developing feature contains some of the most common scenarios that investigators may face in their day to day work. In this release, investigators have several options – to show all contacts or to filter contacts (including members of group chats) that have mentioned a certain word or phrase.

Including Oxygen Forensic Viewer to OFBX backup export

GENERAL

Now, when investigators save extracted data to the internal OFBX format, they can include the Oxygen Forensic® Viewer, which will be saved in the same folder. Choose "Include the Viewer" in the Export window and conveniently share extracted evidence and the corresponding Viewer with colleagues and other authorized personnel.

Export enhancements

GENERAL

With Oxygen Forensic® Detective 13.1 investigators can save their reports as RTF, a newly added file format. In addition, the OCR section now allows investigators to export recognized texts to a variety of external formats, including PDF, XML, XLS, Relativity, and others.