



Oxygen Forensic[®] Detective

Release notes

Version 15.5
May 2023



The latest update to our all-in-one solution is here, Oxygen Forensic® **Detective** v.15.5! This version introduces the following key features:

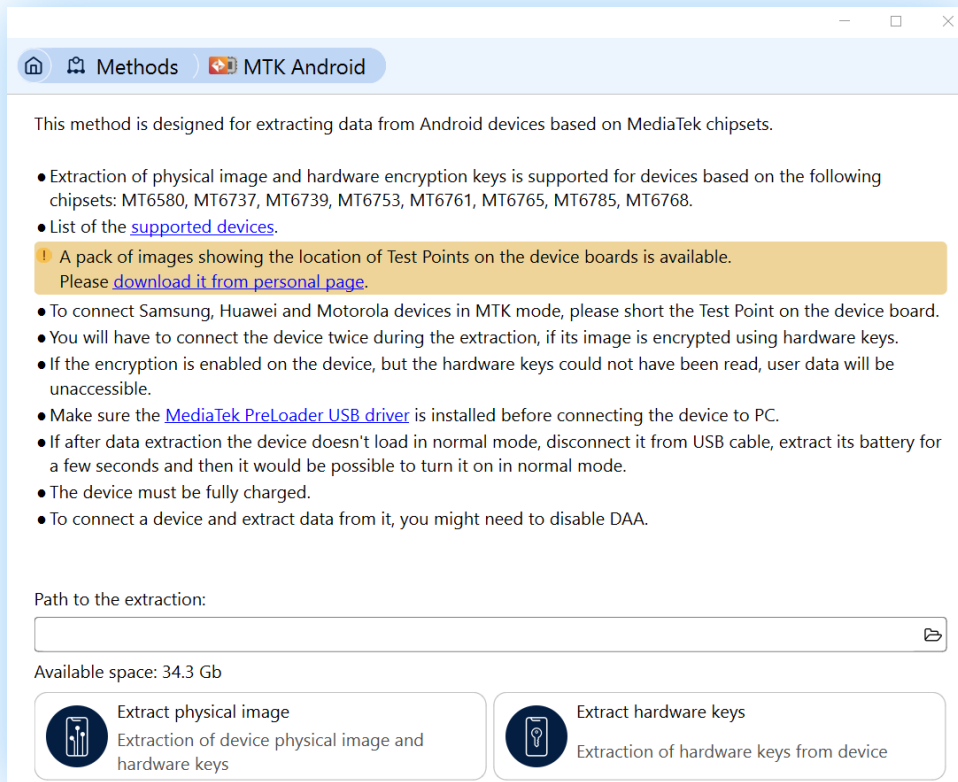
- Support for Android devices based on the MT6761 chipset
- Analysis of drive partitions protected with BitLocker
- Analysis of Windows hibernation files
- Import of Telegram Exported Data
- Parsing of Samsung Customization Service

For a full list of updates, refer to the “What’s New” file in the Oxygen Forensic® Detective “Options” menu.

Mobile Forensic Updates

Support for the MT6761 chipset

We’ve extended our MTK Android method. Oxygen Forensic® Detective v.15.5 enables extraction of hardware keys and decryption of Android devices based on the MT6761 chipset. Our support covers Xiaomi Poco C50, Xiaomi Redmi A1, Xiaomi Redmi A1+, Honor 8S 2020, Huawei Y5 2019, Huawei Y6 Prime 2019, Xiaomi Redmi 6A, and other models.



The screenshot shows a web browser window titled "Methods" with a sub-tab for "MTK Android". The page content includes:

- A heading: "This method is designed for extracting data from Android devices based on MediaTek chipsets."
- A list of supported chipsets: MT6580, MT6737, MT6739, MT6753, MT6761, MT6765, MT6785, MT6768.
- A link to "List of the supported devices."
- A yellow callout box: "A pack of images showing the location of Test Points on the device boards is available. Please download it from personal page."
- A list of instructions:
 - To connect Samsung, Huawei and Motorola devices in MTK mode, please short the Test Point on the device board.
 - You will have to connect the device twice during the extraction, if its image is encrypted using hardware keys.
 - If the encryption is enabled on the device, but the hardware keys could not have been read, user data will be inaccessible.
 - Make sure the [MediaTek PreLoader USB driver](#) is installed before connecting the device to PC.
 - If after data extraction the device doesn't load in normal mode, disconnect it from USB cable, extract its battery for a few seconds and then it would be possible to turn it on in normal mode.
 - The device must be fully charged.
 - To connect a device and extract data from it, you might need to disable DAA.
- A text input field for "Path to the extraction:" with a file explorer icon.
- A status indicator: "Available space: 34.3 Gb"
- Two buttons for extraction options:
 - Extract physical image**: Extraction of device physical image and hardware keys
 - Extract hardware keys**: Extraction of hardware keys from device

Support for the UNISOC T610/T618/T700 chipsets

In Oxygen Forensic® Detective v.15.5 we've added the ability to extract hardware keys and decrypt physical dumps of Android devices based on the UNISOC T610/T618/T700 chipsets, running Android OS 10-13 and having File-Based Encryption (FBE). Please use the Spreadtrum method for these types of extractions. Supported devices include Blackview Tab 15, Digma Pro 1480E 4G, Infinix Hot 12 Play Unisoc T610, Lenovo Tab M10 (3rd Gen), Micromax In 2b, Realme C21Y, Teclast T40 plus, and more.

Extended support for Samsung Exynos devices

Oxygen Forensic® Detective v.15.5 adds support for Samsung Exynos devices having Full-Disk Encryption (FDE) and upgraded from Android OS 9 to 10-11. This method offers passcode brute force.

Other Extractor updates

Our updated Oxygen Forensic® Device Extractor introduces several other enhancements :

- Updated extraction of Twitter, Viber, WhatsApp, and WhatsApp Business data via Android Agent.
- Added keychain extraction via iOS Agent from Apple iOS devices with versions 15.0 - 15.5.
- Added file system extraction via iOS Agent from Apple iOS devices with versions 15.0 - 15.7.1 and 16.0 - 16.1.2.
- Added full file system and keychain extraction via checkm8 from Apple iOS devices with version 15.7.5.

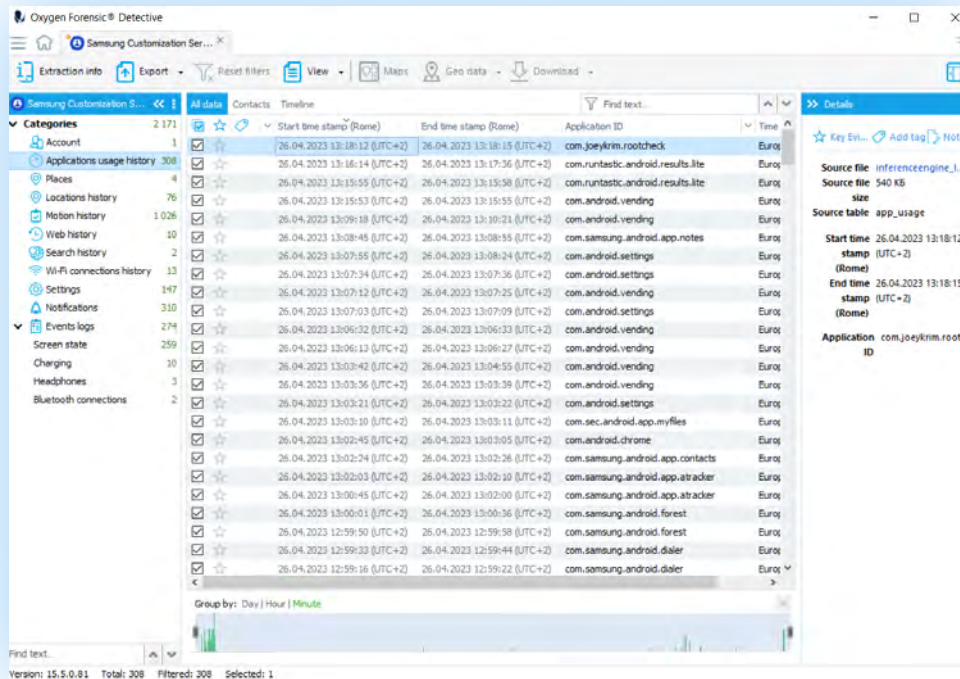
App support

We've added support for the following new apps:

- Hide It Pro (Android)
- Notepad Vault-AppHider (Android)
- Notion (Android)
- Tappsk (Apple iOS)

Moreover, we have added support for a valuable artifact – Samsung Customization Service (com.Samsung.Android.rubin.app). It collects and stores information about the user activity: application usage history, paces, location history, motion history, web history, search history, Wi-Fi connection history, settings, notifications, and events logs.

The total number of supported app versions now exceeds 38,500.



Import Updates

Import of Telegram Exported Data

We've added another source for acquiring Telegram data. Now investigators can import and parse Telegram Exported Data files that can be saved using the "Export Telegram Data" option in the Telegram app settings. To import them into our software, click the Downloaded Accounts Data option located on the software Home screen.

Telegram Exported Data files can contain the following information:

- Account information
- Contacts
- Chats
 - Private chats
 - Chats with bots
 - Private channels and groups (only account messages)
 - Public channels and groups (only account messages)
- Active sessions
- Attachments
 - Photos
 - Videos
 - Voice messages
 - Video messages
 - Stickers
 - GIF

Cloud Forensic Updates

We've added several enhancements to our Cloud Extractor tool:

- Extraction of Telegram artifacts: reactions, avatars, blocked users, group and channel requests, and Premium account information
- Updated Facebook data extraction
- Updated the ability to authorize in Tinder

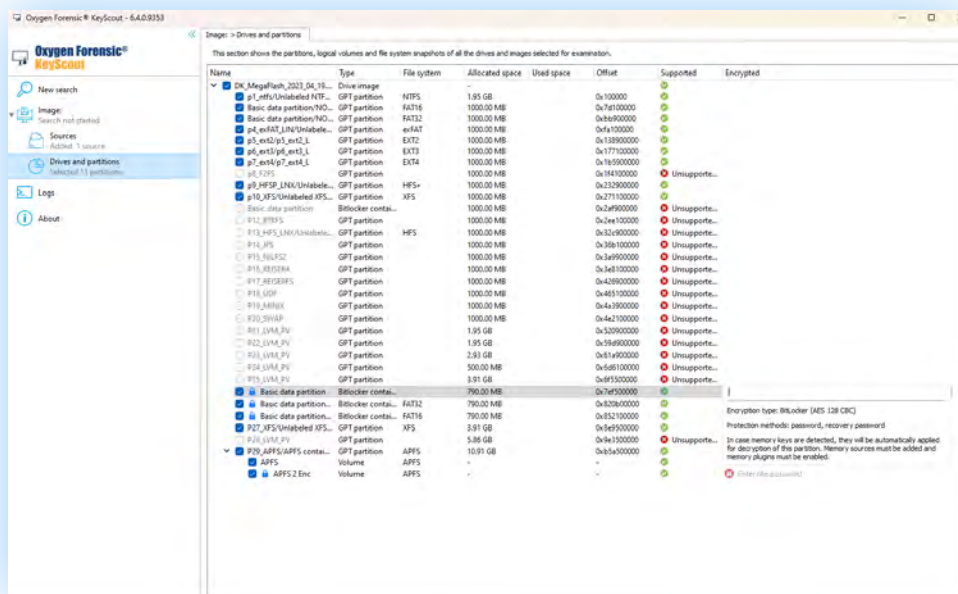
Computer Artifacts

Analysis of drive partitions protected with BitLocker

In Oxygen Forensic® Detective v.15.5 we've added the ability to analyze drive partitions protected with BitLocker.

There are four methods of analysis:

- If a drive partition is protected and locked, Oxygen Forensic® KeyScout can decrypt it with a known password or BitLocker recover key.
- If a drive partition is protected and locked, Oxygen Forensic® KeyScout can also decrypt it with a FVEK (Full Volume Encryption Key) or a VMK (Volume Master Key) extracted from RAM memory.
- If a drive partition is protected, but protectors are deleted or disabled, Oxygen Forensic® KeyScout detects this state and automatically decrypts the drive.
- If a drive partition is protected but unlocked during the Oxygen Forensic® KeyScout work, investigators can use Oxygen Forensic® KeyScout to decrypt it or use the OS API to find data in a decrypted logical drive.



Analysis of hibernation files

Investigators can now analyze hibernation files that show the state of the machine before hibernation. These files might include recent processes, malware analysis, a list of open apps, information regarding open apps, internet history, media such as videos, photos, passwords, geolocation information, and timestamps.

New and updated artifacts

With the updated Oxygen Forensic® KeyScout, users can collect the following new artifacts:

- Known network connections from Windows
- Saved pop-up notifications from macOS
- Briar data from Windows and Linux
- Notepad++ from Windows and Linux
- Information about the installed Debian Package/Advanced Packaging Tool packages from Linux

Updated artifact support includes:

- User credentials from Windows Credential Manager
- Telegram data from macOS

Interested in trying out Oxygen Forensic® **Detective v.15.5?**

[Request a free trial](#)