

# Oxygen Forensic<sup>®</sup> Detective

# Release notes Version 15.5 May 2023



The latest update to our all-in-one solution is here, Oxygen Forensic<sup>®</sup> 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<sup>®</sup> 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.

	>
🖻 🛱 Methods 🛛 🔯 MTK Android	
This method is designed for extracting data from Android devices based on MediaTek chi	ipsets.
• Extraction of physical image and hardware encryption keys is supported for devices bas chipsets: MT6580, MT6737, MT6739, MT6753, MT6761, MT6765, MT6785, MT6768.	sed on the following
• List of the <u>supported devices</u> .	
A pack of images showing the location of Test Points on the device boards is available Please download it from personal page.	<u>.</u>
<ul> <li>To connect Samsung, Huawei and Motorola devices in MTK mode, please short the Test</li> <li>You will have to connect the device twice during the extraction, if its image is encrypted</li> <li>If the encryption is enabled on the device, but the hardware keys could not have been a unaccessible.</li> <li>Make sure the <u>MediaTek PreLoader USB driver</u> is installed before connecting the device</li> <li>If after data extraction the device doesn't load in normal mode, disconnect it from USB a few seconds and then it would be possible to turn it on in normal mode.</li> </ul>	d using hardware keys. read, user data will be e to PC.
• The device must be fully charged.	
<ul> <li>To connect a device and extract data from it, you might need to disable DAA.</li> </ul>	
Path to the extraction:	
	ß
Available space: 34.3 Gb	B
Available space: 34.3 Gb	

## Support for the UNISOC T610/T618/T700 chipsets

In Oxygen Forensic<sup>®</sup> 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<sup>®</sup> 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<sup>®</sup> 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.

😑 🞧 🐌 Samsung Customizatio	n Ser	.×.					
i Extraction info	·V	Reset fillers	View + Ch Mans	🔬 Geo data - 💆 Down	ihad -		
🗴 Samsung Customization S 候 🛔	Al d	ata Coritacts	Timeline		Y Find text	~ ~	>> Detals
Categories 2 171		40 4	Start time stamp (Rome)	End time stamp (Rome)	Application ID	✓ Time ▲	ALL ALL ALL
Account 1		京.	26-04-2023 13:18:12 (UTC+2)	26-04.2023 13:18:15 (UTC+2)	com.joeykrim.rootcheck	Europ	Add tag S No
Applications usage history 308			26.04.2023 13:16:14 (UTC+2)	26.04.2023 13:17:36 (UTC+2)	com.runtastic.android.results.lite	Euros	Source file inferenceengine Source file 540 K5 size Source table app_usage
Places 4			26,04,2023 13:15:55 (UTC+2)	26.04.2023 13:15:58 (UTC+2)	com.runtastic.android.results.lite	Europ	
Locations history 76			26,04.2023 13:15:53 (UTC+2)	26.04.2023 13:15:55 (UTC+2)	com.android.vending	Europ	
Motion history 1 026		÷.	26.04.2023 13:09:18 (UTC+2)	26.04.2023 13:10:21 (UTC+2)	com.android.vending	Europ	
(1) Web history 10	10 D		26.04.2023 13:08:45 (UTC+2)	26.04.2023 13:08:55 (UTC+2)	com.samsung.android.app.notes	Europ	Start time 26.04.2023 13:18:1
Search history 2		sic.	26.04.2023 13:07:55 (UTC+2)	26.04.2023 13:08:24 (UTC+2)	com.android.settings	Europ	stamp (UTC+2)
Wi-Fi connections history 13		\$	26.04.2023 13:07:34 (UTC+2)	26.04.2023 13:07:36 (UTC+2)	com.android.settings	Euros	(Rome)
O Settings 147		÷	26.04.2023 13:07:12 (UTC+2)	26.04.2023 13:07:25 (UTC+2)	com.android.vending	Europ	End time 26.04.2023 13:18:1 stamp (UTC=2)
A Notifications 310		÷.	26.04,2023 13:07:03 (UTC+2)	26,04,2023 13:07:09 (UTC+2)	com.android.settings	Europ	(Rome)
<ul> <li>Events logs 274</li> </ul>		4	26.04.2023 13:06:32 (UTC+2)	26.04.2023 13:06:33 (UTC+2)	com.android.vending	Europ	
Screen state 259			26.04.2023 13:06:13 (UTC+2)	26.04.2023 13:06:27 (UTC+2)	com.android.vending	Euros	Application com.joeykrim.roo ID
Charging 10			26.04.2023 13:03:42 (UTC+2)	26.04.2023 13:04:55 (UTC+2)	com.android.vending	Europ	
Headphones 3			26.04.2023 13:03:36 (UTC+2)	26.04.2023 13:03:39 (UTC+2)	com.android.vending	Euros	
Bluetooth connections 2		÷.	26.04.2023 13:03:21 (UTC+2)	26.04.2023 13:03:22 (UTC+2)	com.android.settings	Europ	
			26.04.2023 13:03:10 (UTC+2)	26.04.2023 13:03:11 (UTC+2)	com.sec.android.app.myfiles	Europ	
		4	26.04.2023 13:02:45 (UTC+2)	26.04.2023 13:03:05 (UTC+2)	com.android.chrome	Europ	
		\$2	26.04.2023 13:02:24 (UTC+2)	26.04.2023 13:02:26 (UTC+2)	com.samsung.android.app.contacts	Europ	
		Sc.	26.04.2023 13:02:03 (UTC+2)	26.04.2023 13:02:10 (UTC+2)	com.samsung.android.app.atracker	Europ	
			26.04.2023 13:00:45 (UTC+2)	26.04.2023 13:02:00 (UTC+2)	com.samsung.android.app.atracker	Europ	
		4	26.04.2023 13:00:01 (UTC+2)	26.04.2023 13:00:36 (UTC+2)	com.samsung.android.forest	Europ	
		☆	26.04,2023 12:59:50 (UTC+2)	26,04,2023 12:59:58 (UTC+2)	com.samsung.android.forest	Europ	
		合	26.04.2023 12:59:33 (UTC+2)	26.04.2023 12:59:44 (UTC+2)	com.samsung.android.dialer	Europ	
		÷	26.04.2023 12:59:16 (UTC+2)	26.04.2023 12:59:22 (UTC+2)	com.samsung.android.dialer	Euros ~	
	<					>	
	Gro	up by: Day   H	our   Minute				
	1						
ind text						1	

# **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
  - $\cdot$  Chats with bots
  - · Private channels and groups (only account messages)
  - Public channels and groups (only account messages)
- Active sessions
- Attachments
  - Photos
  - Videos
  - $\cdot$  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<sup>®</sup> 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<sup>®</sup> KeyScout can decrypt it with a known password or BitLocker recover key.
- If a drive partition is protected and locked, Oxygen Forensic<sup>®</sup> 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<sup>®</sup> KeyScout work, investigators can use Oxygen Forensic<sup>®</sup> KeyScout to decrypt it or use the OS API to find data in a decrypted logical drive.

	This section shows the partitions, logical	I volumes and file sy	stem snapshots of	all the drives and images s	selected for exa	minatori.		
x* KeyScaul	Name	Type	File system	Allocated space U	Jsed space	Officet	Supported	Encrypted
New search	DK MegaFlash 2023_04_19			~			ð	
	p1_ntfs/Unlabeled NTF		NTFS	1.95 GB		0x100000	0	
image:	Basic data partition/NO		FAT16	1000.00 MB		0x7d100000	0	
Search not startind	Basic data partition/NO		FAT32 exFAT	1000.00 MB		0xbb900000	0	
Sources	p4_exfAT_LIN/Unlabele	GPT partition GPT partition	EXT2	1000.00 MB 1000.00 MB		0xfa100000 0x138900000	0	
Added Tsource	p5_ext2/p5_ext2_L p6_ext1/p6_ext1_L	GPT partition	EXT2	1000.00 MB		0x132900000	0	
Drives and partitions	p_ext/p_ext/_c	GPT partition	EXT4	1000.00 MB		0x1b5900000	6	
G Internet and participants	all projekter projekterje	GPT partition	EATH	1000.00 MB		0x164100000	O Unsupporte_	
and the second second	9 p9 HFSP LNX/Unlabele		HFS+	1000.00 MB		0x232900000	C Cincipperte	
Logs	p10.XFS/Unlabeled XFS		XES	1000.00 MB		0x271100000	0	
	Basic data partition	Bitlocker contai	~ 2	1000.00 MB		0x2#900000	O Unsupporte	
About	P12 #7855	GPT partition		1000.00 MB		0x2ee100000	O Unsupporte	
	P13 HPS LNOLMabele		HES	1000.00 MB		0x32c900000	O Unsupporte_	
	- P13 JP5	GPT partition	mrs	1000.00 MB		0x35b100000	O Unsupporte	
		GPT partition		1000.00 MB		0x3a9900000		
	#15_MILPS2 #16_REPSEA	GPT partition		1000.00 MB		Dx 3e8100000	O Unsupporte	
							O Unsupporte_	
	017_REISERFS	GPT partition		1000.00 MB		0x426900000	Unsupporte_	
	D P18_00/	GPT partition		1000.00 MB		0x465100000	Unsupporte	
	#10_64IN(O)	<b>GPT</b> partition		1000.00 MB		0x4a3900000	O Unsupporte	
	EL #20_SWAP	GPT partition		1000.00 MB		0x4e2100000	O Unsupporte	
	\$11,0VM,2V	GPT partition		1.95 68		0x520900000	O Unsupporte_	
	P22_LVM_PV	<b>GPT</b> partition		1.95 GB		0x59d900000	O Unsupporte	
	233,6VAK_PV	GPT partition		2.93 GB		0x51x900000	Unsupporte	
	#24_UVM_PV	<b>GPT</b> partition		500.00 MB		0x5d6100000	O Unsupporte	
	C #15,UVM #9	GPT partition		3.91.68		Dx6F5500000	O Unsupporte_	
	🛃 🔒 Basic data partition	Bitlocker contai		790.00 MB		0x7ef500000	0	
	Basic data partition	Bitlocker contai	FAT32	790.00 MB		0x820b00000	0	and the second second second
	🗧 🔒 Basic data partition	Bitlocker contai	FAT16	790.00 ME		0x852100000	0	Encryption type: BitLocker (AES 128 CBC)
	P27_XFS/Unlabeled XFS	GPT pertition	XFS.	3.91 GB		0x8e9500000	0	Protection methods: password, recovery password
	PJU CVAR PV	<b>GPT</b> partition		5.86 GB		0x9e1500000	Unsupporte	In case memory keys are detected, they will be automatically applied
	P29_APFS/APFS contai	GPT partition	APES .	10.91 G8		0xb5a500000	0	for decryption of this partition. Memory sources must be added and
	APFS	Volume	APFS				0	memory plugins must be enabled.
	🛃 🔒 APFS 2 Enc	Volume	APFS	1 C C			0	O Enter Medictumind

# 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<sup>®</sup> 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**