

(<https://www.mobiledit.com/webinars>)
MOBILedit Forensic webinars. Register now!

×

MOBILedit Products Education Downloads (/downloads) News (/news) Online Store (/store)
Support Company

An investigator relies on many types of data in forensic work. Read below to find out what types of data can be extracted, analyzed, and presented. The particular data extracted will depend on the specific phone model, operating system, and its status.

Main functions

- **Phone extractor with an extremely wide range of supported phones**
- **Password breaker with GPU acceleration and multi-threaded operation for maximum speed**
- **iTunes backup analyzer**
- **Android ADB backup analyzer**
- **Applications data analyzer**
- **Photo Recognizer**
- **Deleted data recovery**
- **Cellebrite UFED data analyzer**
- **Cellebrite UFED data generator**
- **Oxygen data analyzer**
- **Report generator**
- **Security Bypassing**
- **Smartwatch analyzer**
- **Dive computer analyzer**
- **Cloud data analyzer**

Supported platforms

Logical and advanced logical extraction

- Android
- iOS

- Windows 10 Mobile
- Windows Phone 7 - 8.1
- Windows CE
- BlackBerry OS
- Symbian
- Samsung Bada
- Many feature phones from various vendors
- Apple Watch with WatchOS - direct reading through the diagnostic connector
- SIM cloning by using a smart-card reader (sold separately)

Physical extraction

- Android
- KaiOS
- Various feature phones

Open/Import files

- iTunes backup
- Android ADB backup file
- Oxygen Export XML
- Cellebrite UFDR
- Cellebrite UFD with both, logical data and physical images
- Reveal iTunes backups
- Data from folder
- Data from the ZIP file
- Physical image
- Garmin backup
- Huawei backup folder
- Xiaomi MIUI backup folder
- Samsung SmartSwitch backup file
- Samsung feature phone
- MOBILedit Backup XML
- MOBILedit backup package

Exports and reports

- HTML - creates site structure for easy data browsing using any browser
- PDF - Acrobat reader single file or multiple files
- XML - Excel
- XLS - Excel workbook
- CLBX
- UFDR - Cellebrite report file
- MOBILedit export structure of files with parsed data from phone
- MOBILedit backup structure of raw files from phone
- MOBILedit export and backup can be compressed and encrypted using AES and protected by MD5 or SHA256 hashes.

Live updates

We believe that phone forensics strongly relies on updates, so we have introduced a unique Live Update system, which allows for fast and frequent updates of important functionalities without reinstalling the software.

Live updates are available for following modules

- Application analysis script files
- Report translations
- Application downgrade files
- Photo Recognizer machine learning module
- Face Matcher machine learning module
- Cell tower locations database
- Security Bypassing binary files, such as EDL
- Recovery images
- Samsung Engineering Root
- Malware detection
- iOS developer images for screenshot support
- File Exclude List
- etc...

Supported filesystems for physical

- ext4/ext3/ext2
- F2FS
- APFS

analysis

- HFS+/HFS
- NTFS
- FAT32/FAT16/FAT12
- ExFAT
- YAFFS2
- UFS2/UFS1
- ISO 9660

Application downgrade

- AliExpress
- BBM
- Dolphin browser
- Dropbox
- Evernote
- Facebook
- Facebook Messenger
- Firefox
- Google Chrome
- Google Drive
- Google Maps
- Instagram
- KakaoTalk
- Keepsafe
- LINE
- MiTalk
- Periscope
- Skype
- Snapchat
- Telegram
- Todoist
- Truecaller
- Twitter
- Viber
- WeChat
- WhatsApp
- Wickr
- Wunderlist

Languages

Generated reports are available in following languages

- English
- Spanish
- Portuguese
- German
- Estonian
- Japanese
- Chinese
- Korean
- Dutch
- Polish
- Slovak
- Czech

Full product User Interface

- English
- Spanish
- Portuguese
- Japanese
- Chinese
- Slovak
- Czech

Integration

We understand an investigator may use many tools in an investigation. We've designed our software with the ability to integrate with other forensic tools in your lab. Import and analyze data files exported from Cellebrite UFED and Oxygen reports to uncover potentially overlooked data. Export all MOBILedit Forensic data to UFED, so you can use the UFED Viewer or Analytics for further processing to move your investigation forward.

Contacts

Three unique reports help uncover the suspect's connections.

The **Contacts Report** presents all contact details fully retrieved and analyzed, including deleted contact details when available. Contact recovery scope is from multiple sources such as phonebook and memory, vCard files, SIM card, cloud accounts and applications. Search a report directly for names, numbers, deleted contacts or other information. The report informs the investigator when the contact was created, when it was last modified and which account type it is (WhatsApp, Cloud, Gmail, Facebook etc.). Find important information such as phone numbers, email address, home address, birthday, employer, and contact profile pictures to help you put a face to a name.

With a **Contact Analysis Report** find out who the suspect has been in contact with the most, and discover crucial connections. Contact Analysis will detail the number of sent and received messages and calls including total minutes of talk-time for each contact, sorted in descending order by the number of communication events with the suspect.

The **Contact Accounts Report** will help the investigator find all phone, email, cloud, and applications accounts associated with the suspect's device..

Contact Accounts (4)

1 Google	
Name	james.compelson@gmail.com
Type	com.google
Associated Contacts	1
2 Google	
Name	james.compelson@gmail.com
Type	com.google
Dataset	plus
3 Phone Memory	
Name	vnd.sec.contact.phone
Type	vnd.sec.contact.phone
Associated Contacts	4
4 SIM	
Name	primary.sim.account_name
Type	vnd.sec.contact.sim

Contacts (13 total, 1 deleted)
All phone, application, and SIM contacts, sorted by name in ascending order

1 Brianna Ammerman Phone Memory

Group ID	380
First Name	Brianna
Last Name	Ammerman
Mobile	+15448965451
Work	+15225365111
Email	briarman@imail.com
Work Address (Google Maps)	Street 210 Washington Avenue
Locality	Albany
Region	NY
Country	United States of America
Note	Met on holidays
Number of Messages	2

2 Brianna Ammerman WhatsApp

Phone Number	+15448965451
--------------	--------------

Messages

Messages are fully retrieved for analysis and presented in the **Messages Report**, including deleted messages when available. Messages include standard phone messages (SMS, MMS, iMessages), email messages, SIM messages and application messages. Customize the report and sort by contact, timeline, conversation view, or both.

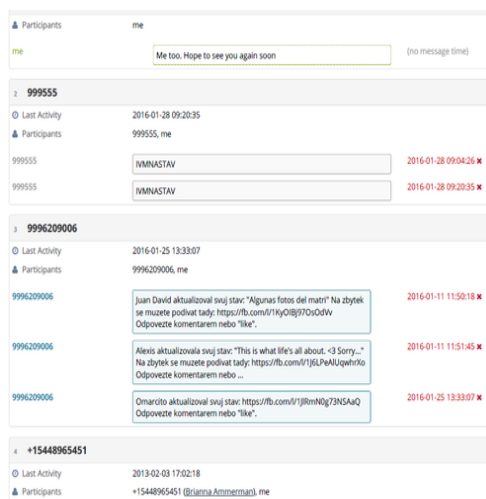
Messages (30 total, 5 deleted)
All application messages, sorted by time in ascending order

1	Evernote <no-reply@evernote.com>	2015-10-14 14:49:50	Received
Thank you for creating an Evernote account! A password will allow you to acces...			
To	<james.compelson@gmail.com>		
Subject	Create a password now to access Evernote everywhere		
Source	iMail Account: james.compelson@gmail.com		
2	Evernote <no-reply@evernote.com>	2015-10-14 14:50:24	Received
On one device, Evernote is good. On all your devices, it's sublime. Evernote ...			



Conversations

Efficiently read through entire uninterrupted conversation streams. The **Conversations Reports** separates entire conversations by contact and are ordered by time sequence. Captured conversations include all SMS, MMS, iMessages and applications messages including encrypted-messaging apps.



Call logs

The **Calls Report** provides details of all mobile service and applications-based phone calls, including deleted calls. Pin-point the time and date of when the suspect made or received calls, the duration of the call, the source (mobile, Facebook, WhatsApp etc.) and the contact and phone number associated with each call.

Calls (13 total, 2 deleted)
All phone and application calls, sorted by time in ascending order

Label	From	To	Time	Duration
1	Mum	+1643288756	2013-12-30 11:52:06	00:00:42
2	Sophia	+15983698569	2013-12-31 13:42:45	00:00:30

3	→	Sophia	+15983698569	2014-01-02 12:39:12	00:00:00
4	→	Lisa	+15423698569 (Lisa Cahow)	2014-01-02 13:35:55	00:00:41
5	←	Lisa	+15423698569 (Lisa Cahow)	2014-01-02 15:37:47	00:02:30
6	←	Sister	+13498398732	2014-01-04 15:07:15	00:01:07
7	←	Sister	+13498398732	2014-01-10 20:15:15	00:00:00
8	←	Sophia	+15983698569	2014-01-24 17:18:51	00:00:00
9	←		+42022889618	2014-01-30 10:52:13	00:00:00
10	←	Megan Brandt (Megan Brandt)		2016-04-15 16:05:23	00:00:45
Source: WhatsApp					
11	→		+420732402612 (Megan Brandt)	2016-04-15 16:35:42	00:00:00 x Deleted
Source: Viber					
12	→		+420732402612 (Megan Brandt)	2016-04-15 16:36:38	00:00:27 x Deleted
Source: Viber					
13	→		+420732402612 (Megan Brandt)	2016-04-15 16:36:38	00:00:27

Emails

Emails are fully retrieved for analysis and presented in the **Emails Report**, including deleted messages when available. Customize the report and sort by contact, timeline, conversation view, or both.

Applications

Perform an advanced applications analysis. All applications are listed and fully analyzed for their detailed data, including deleted applications data where available, and presented in the Applications Report. Narrow your search by selecting the specific applications you wish to analyze, or complete an analysis on all applications in the device. Criminals, terrorists and everyday people are using encrypted-messaging applications more than ever, now an investigator can read these messages. Raw application data are also stored in the export folder, which makes additional processing and analysis possible. MOBILedit supports over 1000 unique applications and many thousands application profiles. We offer an online detailed database of supported applications and data:

List of supported apps (<https://apps.mobiledit.com/>)

Deleted data

Deleted data is often the key information in an investigation. Deleted data details are presented in a special comprehensive **Deleted Data Report**, and also displayed within each individual analysis report. Whether it is calls, SMS, MMS, calendar events, notes, applications data, or other evidence your are looking for, MOBILedit Forensic searches deeply in databases for caches and hidden files to reveal the maximum deleted data possible.

Passwords

The **Passwords Report** will reveal passwords from many types of accounts and applications.

In iOS devices, all system passwords and most application passwords are managed through dedicated and encrypted Keychain. We are able to decrypt the keychain and retrieve all passwords that were saved in it. Passwords contained in the Keychain include: Wi-Fi passwords, appleID password, passwords saved in Safari as well as various email and application passwords, and passwords saved in web browsers and other accounts. From Android devices Wi-Fi passwords are retrieved.

Wi-Fi networks

This section contains detailed data about all Wi-Fi networks saved in a device. The **Wi-Fi Networks Report** displays the history of Wi-Fi connections in time sequential order, including the Wi-Fi network name, the last joined time and date, the last auto-joined time and date (indicates that a suspect has been a repeat visitor to the network location), SSID, BSSID, and security mode. Supported are also continued logs - connected time. Even Wi-Fi network passwords are recovered and are shown in **Password Report**.

Images

The **Images Report** will contain images from the phone file system. This includes application images – images retrieved from applications data, which might also include images stored in temporary files or caches that have been detected as potential images. An option to display large images in full size will create an additional section in the report and display one image per page. Filter out duplicate images to omit emoticons and similar images from the reports.

Photos

The **Photos Report** retrieves all device and applications photos taken by the phone, usually in the DCIM folder. iPhone deleted photos can be recovered if they were sent via MMS or from a supported application. The ability to recover deleted photos depends on many internal factors in the storage and cannot be predicted nor guaranteed. Supported is also an Apple photo format HEIF.

Cell towers

Data about cell towers that the subject phone was connected to can be obtained. Obtained cell tower locations can be individually viewed on the map through the provided link.

Audio files

Audio files are copied from the device and its applications. The **Audio Files Report** allows you to play an audio file simply by clicking on it in the report. The report also details the file path, the created and modified time, the duration of the audio file and the size of the audio file.

Video files

Video files are also copied from the device and its applications. The **Video Files Report** allows you to play a video file by clicking on it in the report. The report also details the file path, the created, modified, encoded and tagged time, the duration of the video, the size of the video file as well as the frame rate, height and width.

Organizer

The device and applications organizers are searched and analyzed, and data is presented in four distinct reports. Customize the search within a specific timeframe for calendar events, notes and tasks, or complete a full phone search.

The **Calendar Accounts Report** displays the various device and applications accounts where events are created and stored. Details include the account source, name, account owner, account email address and the number of associated events with the calendar.

An **Events Report** lists all events in detail from the device and its applications, including deleted events from calendars and other sources where events are created. Details include which calendar the event was created in, a summary, a description, start time, created time, modified time, end time, recurrence, if the event was removed or deleted and are sequenced in ascending or descending order.

Tasks are carefully compiled and presented in detail in the **Tasks Report**. Tasks found in the device and applications include the full task text content, the creation time, modified time, start time, completion time and indicates if the task was deleted.

Notes including deleted or removed notes are compiled in detail in the **Notes Report**. Gathered from the device and applications, the report includes a header title, a summary, the full text content of the note, the created, modified and last visit time, as well as if the note was removed or deleted.

Documents

Extract and preview most common document formats.

GPS locations

Knowing when and where a suspect has been is key in every investigation. The **GPS Locations Report** contains all possible GPS location data from the device and applications. We are able to extract 'last known' locations from Android devices. The analysis and report yield valuable information from map, fitness and transportation applications such as Google Maps, Pokémon Go, Nike+ Running, Uber and many more. Some applications may even contain GPS data about the entire route, and show the sequence of GPS coordinates with their timestamps recorded and stored. Photos and videos on a device may also contain GPS locations in their metadata. Customize the locations search and report by time, or search and order locations by proximity to specific GPS coordinates.

Malware detection

With MOBILedit Forensic, malware detection is based on the Yara project (<https://virustotal.github.io/yara/>), meaning that the processing is much faster and allows users to utilize any 3rd party set of malware rules available, in addition to those we supply. All extracted files are scanned and we have recently updated the malware database and added the latest spyware, such as Pegasus.

Cookies

The **Cookies Report** compiles the history of cookies in a device. System cookies are only obtainable from iOS devices. Application specific cookies are analyzed for every installed application. Cookies contain information about web domain as well as their creation, accessed and expiration time, and if the displayed cookie has been deleted.

Web browsing history

The **Web Browsing History Report** contains a consolidated web browsing history from all analyzed browser applications. Each web browsing history entry consists of the visited URL as well as time of the visit. In some cases the total number of visits of the URL is also available with the timestamps of individual visits. The report is customizable by alphabetical order or by time sequence.

Web search history

The **Web Search History Report** contains queries searched in the web browser as well as a timestamp of when the search occurred. System-wide web searches are only obtainable from Android 5.1 devices and older. Web search data is also gathered from browser application analysis.

Bluetooth pairings

Bluetooth pairing history can be discovered on both Android and iOS devices and is presented in the **Bluetooth Pairings Report**. In the report you will find the name of the Bluetooth connection, the Bluetooth address of the pairing device, the status, and on iOS- the date and time of the last connection.

Contact analysis

Contact analysis is a section with analyzed relationships between contacts and the way they were used in various modes of communication. It is also possible to skip contacts that have rarely been communicated with on that mobile phone.

Notification S

Notifications from the device and applications are presented in detail and are retrievable from iOS and Android devices. The **Notifications Report** displays notifications information including the source, the text of the notification, and the timestamp. On iOS also included are notifications that are no longer active and may contain otherwise unobtainable information, such as emails and messages from applications that do not store them in databases. On Android only active notifications are retrievable.

Bookmarks

The **Bookmarks Report** gathers device and application global browser bookmarks on iOS devices (Safari bookmarks), and on Android devices up to Android 5.1; later versions of Android only application specific bookmarks can be obtained. The report can be sorted by time or name in alphabetical order.

Keyboard cache

The **Keyboard Cache Report** contains all words that have been typed on the device and is only available on devices running iOS version 7 and older. On Android devices, we can extract User Dictionary that contains custom user-defined words.

System logs

The **System Logs Report** contains system logs and dumpsys files that can be extracted from Android phones. The Android system keeps these files for debugging and monitoring purposes and they contain system data such as recent locations, recent connected Wi-Fi networks, running applications, recently launched applications, recent cell locations and signal info, current Bluetooth MAC address and name etc. These files are listed in the System Logs section within the HTML and PDF reports and can be directly opened by clicking on their filenames. Their content is analyzed and presented in various reports such as Wi-Fi Networks, GPS Locations, Notifications etc.

File system

The **File System Report** is divided in three section according their source. **Internal** - which includes raw file system. Then **Application File System** which contains application data files. The third is the **Extra File System**, which contains information about files that are not physically present on device but are available to be extracted. This includes all files from iTunes backup on iOS devices. On Android devices, Content Providers, System Logs and DumpSys fall into this category.

Timeline

The **Timeline Report** provides insight into all device activity exactly as it occurred. The report aggregates all extracted items that contain time and date information and displays it in chronological order. Exact parameters of a generated timeline can be customized to a specific function; for example, you can select to configure a timeline of calls and messages only.

Photo recognizer

This module automatically locates and recognizes suspicious content in both photos and videos, such as weapons, drugs, nudity, currency, and documents. Photo Recognizer utilizes artificial intelligence and deep machine learning to quickly analyze an unlimited number of photos and videos, and is designed to eliminate countless hours that would be spent manually searching for key evidence in huge databases of visual media. Each piece of media is placed in its own specific category so that investigators can keep their cases well-organized and easily present the suspicious content in a fine-tuned report.

Face Matcher

This important feature easily finds photos and videos of people you are looking for. Based on the newest deep learning techniques, Face Matcher rapidly analyzes even large quantities of visual media that users often have in their phones or PCs. Eliminate countless hours spent manually looking through photo and video albums. Simply supply photos of faces you want to find, and let Face Matcher find the right photos and videos.

Security Bypassing

For a wide range of Android devices, the Security Bypassing feature allows for physical image acquisition even when the device is protected by a password or gesture, also able to bypass the lock screen with many phone models.

- MTK method
Way of extracting a physical image from phones with MediaTek chipsets without root access.
- EDL method
Way of extracting physical images from phones with Qualcomm chipsets without root access.
- LAF method
The "LAF method" feature works on all LG smartphones with the new version of the LG LAF protocol.
With some devices, we are able to browse the phone's filesystem via the "Browse Phone" option in MOBILedit Forensic.
- TWRP method
Can be used for bypassing a screen lock or extracting a physical image from phones with an unlocked bootloader.
- Rooting methods
There are several methods allowing you to temporarily root the Android device.

- Spreadtrum
This method provides a possibility to create a physical dump of internal memory from devices with Spreadtrum chipset without knowing a passcode or pattern lock.
- Kirin decrypt
This method allows you to bypass security on Huawei devices with HiSilicon Kirin chipsets and obtain unencrypted data with root access.
- Exynos decrypt
Provides root access and prevents the boot process via the chipset and is then able to access the full memory without the operating system security restrictions.
- and more...

Cloud Forensics

All information can be found at MOBILedit Cloud Forensic (<https://www.mobiledit.com/cloud-forensic>) product page

Smart screenshot

Feature for Android, allowing you to extract conversations and other information from popular messaging apps like Instagram, Signal, Skype, Telegram, Viber, Slack and WhatsApp without any user interaction on the device. This is yet another option for overcoming the challenge of obtaining evidence from applications with increasingly complex security.

Solutions

Resellers (/resellers)
Enterprises (/companies)
Universities (/education)


How To

Connect Android
(<https://forensic.manuals.mobiledit.com/MM/Android.1799815190.html>)
Connect iPhone
(<https://forensic.manuals.mobiledit.com/>)

Keep Me Informed

Join mailing list

(/newsletter)

Video channel

(<http://www.youtube.com/user>)

Stores (/operators)
Phone Manufacturers
(/manufacturers)

MM/iOS.1799389200.html)
Connect Windows Phone
(<https://forensic.manuals.mobiledit.com/MM/Connecting-Windows-phone.1803223057.html>)
Transfer messages to Android
(<https://support.mobiledit.com/portal/kb/articles/transferring-messages-into-your-android-device-version-4-4-or-higher>)
Turn on USB debugging
(<https://forensic.manuals.mobiledit.com/MM/How-to-enable-USB-debugging.1802698825.html>)
Backup phone
(<https://phonemanager.manuals.mobiledit.com/UGME/Backups.2151776296.html>)

Forensic
channel



(<https://www.linkedin.com/company/compelson>)



(<http://twitter.com/MEforensic>)

Copyright © 2023 Compelson, All rights reserved | [Privacy \(/privacy\)](#) | [Terms of Use \(/eula\)](#)
Compelson, MOBILedit is registered trademark.