

MOBILedit Forensic

User Guide - MOBILedit Forensic Express

Exported on 11/24/2021

Table of Contents

1	Introduction	19
1.1	System Requirements.....	19
1.2	Purchase	19
1.3	Download & Installation	20
1.4	License activation	20
1.5	Single phone license activation	21
1.5.1	How to	21
1.6	Offline activation.....	23
1.7	Dongle license activation	24
1.8	Deactivation	24
1.9	Getting Started.....	25
1.9.1	Before you begin	25
1.9.2	Connecting phones.....	25
1.9.3	Getting maximum including deleted data.....	26
1.9.4	Password and PIN breaking.....	26
1.10	Home Screen	26
1.11	Settings.....	27
1.11.1	Global Settings	27
1.11.2	Investigator details	27
1.11.3	Logging	28
1.12	Updates	28
1.13	MOBILedit BETA testing program.....	29
1.14	Offline updates.....	30
1.14.1	How to	30
1.15	What data can be extracted?	31
1.16	Add-ons.....	32
1.16.1	App downgrade.....	33
1.16.2	App engine.....	33
1.16.3	iOS screenshots.....	33
1.16.4	Cell towers.....	34
1.16.5	Face Matcher	34

1.16.6	File exclude list.....	34
1.16.7	Photo Recognizer.....	34
1.16.8	Malware Detection.....	34
1.16.9	Recovery.....	34
1.16.10	EDL.....	35
1.17	Localization.....	35
2	Introduction to phone forensics.....	39
2.1	Terms.....	39
2.2	Deleted data.....	40
2.2.1	Physical extraction.....	40
2.2.2	SQL databases.....	40
2.2.2.1	How SQLite data recovery works.....	41
2.2.3	Basic recovery method.....	41
2.2.4	Clutter filtering.....	41
2.2.4.1	How it works:.....	41
2.2.5	What deleted data can be recovered?.....	41
2.2.5.1	Android.....	42
2.2.5.2	iOS.....	42
2.3	Physical extraction.....	42
2.4	Recovery mode.....	44
2.4.1	How to set the phone to recovery mode.....	44
2.4.2	Connecting phone.....	45
2.5	Android recovery data acquisition.....	45
2.6	How to unlock bootloader on Android.....	46
2.6.1	How to.....	46
2.7	Security Bypassing.....	49
2.7.1	How to.....	49
2.8	Physical Extraction - EDL Hack.....	50
2.8.1	How to.....	50
2.8.2	List of supported devices.....	54
2.8.3	Additional sources.....	55
2.9	Physical extraction - LG Hack.....	55
2.9.1	How to.....	55

2.10	Physical Extraction - MTK Hack	60
2.10.1	How to	60
2.11	KaiOS Physical analysis	64
2.11.1	Physical extraction.....	64
2.11.1.1	EDL Hack.....	65
2.11.1.2	MTK Hack.....	65
2.11.2	Example of connecting a specific device in EDL mode:	66
2.12	How to root an Android phone?	68
2.12.1	What does rooting an Android actually mean?	69
2.12.2	How do I root an Android phone?	69
2.13	Dirty COW	70
2.13.1	How to	70
2.14	Use TWRP to bypass Android lockscreen.....	73
2.14.1	How to	73
2.15	Flash phone with recovery image - TWRP.....	78
2.15.1	How to	78
2.15.2	Where to find the physical image for later use	81
2.15.3	If the button will not appear.....	81
2.16	CMD method - Flashing TWRP on non-Samsung devices	84
2.16.1	Requirements:.....	84
2.16.2	How to	84
2.17	ODIN method - Flashing TWRP on Samsung devices	86
2.17.1	Requirements.....	86
2.17.2	How to	86
2.18	How to boot into recovery on Android.....	89
2.18.1	How do I boot into recovery mode?.....	89
2.18.1.1	New Samsung Galaxy devices	90
2.18.1.2	Old Samsung devices.....	90
2.18.1.3	New Samsung devices	91
2.18.1.4	Honor/Huawei.....	91
2.18.1.5	LG	92
2.18.1.6	HTC	93
2.18.1.7	Motorola	93
2.18.1.8	Google/Nexus phones.....	94

2.18.1.9	ASUS	95
2.18.1.10	OnePlus	96
2.18.1.11	Nokia.....	96
2.18.1.12	Xiaomi.....	97
2.19	Lockdown method - Unlocking a passcode-protected iPhone	98
2.20	How to jailbreak an iOS device?	100
2.20.1	What does jailbreaking mean?	100
2.20.2	How do I jailbreak an iOS device?	100
2.21	Jailbreaking iPhone with checkra1n.....	101
2.21.1	How to boot checkra1n from a flash drive.....	101
2.21.2	How to enter firmware settings (BIOS)	102
2.21.3	Jailbreaking with Checkra1n.....	105
2.22	Damaged/broken phone data extraction	108
2.23	Supported phones in Unlocking database	109
3	Connecting a device.....	112
3.1	Supported phones	112
3.1.1	MOBILedit supports:	112
3.2	Device connection screen.....	112
3.2.1	iOS.....	113
3.2.2	Android	113
3.3	Connection wizard	114
3.3.1	“How to connect” wizard.....	115
3.3.2	Android	118
3.3.2.1	Cable connection	119
3.3.2.2	Wi-Fi connection	125
3.3.3	iPhone.....	127
3.3.3.1	Cable connection	128
3.3.3.2	Wi-Fi connection	133
3.3.4	Windows Phone.....	134
3.3.5	Other phones.....	136
3.4	Android	138
3.4.1	Connecting Android phone via USB cable	138
3.4.2	Connecting Android phone via Wi-Fi.....	138
3.4.3	If your phone doesn't connect	139

3.4.4	How to enable USB debugging.....	139
3.4.4.1	Android 4.2 and higher	139
3.4.4.2	Huawei devices	139
3.4.4.3	Xiaomi devices.....	140
3.4.4.4	Android 4	141
3.4.4.5	Android 2.3	141
3.4.5	How to enable "Stay awake" option	141
3.4.5.1	How to	141
3.4.6	How to confirm RSA fingerprint	146
3.4.7	Connecting in MTP mode.....	147
3.4.7.1	How to	147
3.4.7.2	Android 6.0 and higher	148
3.4.8	How to install a universal Android driver.....	148
3.4.9	How to install HTC drivers	150
3.4.9.1	How to	150
3.4.10	Connecting via Bluetooth.....	153
3.4.11	Connector installation	156
3.4.11.1	How to install our app manually	157
3.4.12	Connector permissions.....	158
3.4.13	Extraction without the Connector app	159
3.5	iOS.....	160
3.5.1	Connecting iPhone by USB cable	161
3.5.1.1	iTunes for Windows not installed.....	161
3.5.1.2	iTunes for Windows installed	161
3.5.1.3	Jailbroken iPhone and full file system extraction.....	161
3.5.2	Connecting iPhone by Wi-Fi.....	161
3.5.3	How to install correct Apple drivers.....	162
3.5.3.1	How to	162
3.5.4	How to disable the auto-lock option	168
3.5.4.1	iOS 10 and higher	168
3.5.4.2	iOS 9.x and earlier	168
3.6	How to Connect Apple Watch.....	168
3.6.1	What can you extract	169
3.6.2	Example of Apple Watch data in PDF report.....	170
3.7	Info button on the connection screen	176

3.7.1	Capabilities:.....	178
3.7.2	Commands:	178
3.7.3	Properties:	178
3.8	Disconnecting phone	179
3.9	File Manager	179
3.10	Other	179
3.10.1	Nokia feature phones.....	179
3.10.2	Connecting Windows phone.....	180
3.10.2.1	Whats is supported	180
3.10.2.2	How to connect Windows Phone	180
3.10.2.3	Windows CE Phone connection.....	180
3.10.3	Connect BlackBerry via WiFi.....	181
3.10.3.1	MOBILedit and Phone Copier Express installation guide	181
3.10.3.2	MOBILedit Forensic Express installation guide	184
3.10.4	Blackberry OS devices	190
3.11	Android - Español.....	190
3.11.1	Si su teléfono no se conecta	191
3.11.2	Conexión Wi-Fi con Android	191
3.11.3	Android - Habilitar la opción "Permanecer activo"	191
3.11.4	Conexión en modo MTP	196
3.11.4.1	Para Android 6.0 o superior:.....	200
3.11.5	Android - Confirmar la huella digital RSA	200
3.11.6	Cómo instalar el controlador universal de Android	201
3.11.7	Cómo habilitar la depuración USB.....	203
3.11.7.1	Ver todas las instrucciones con imágenes.....	203
3.11.7.2	Dispositivos Huawei.....	210
3.11.7.3	Dispositivos Xiaomi.....	211
3.12	Android - Português	212
3.12.1	Como conectar o telefone por cabo USB.....	213
3.12.1.1	Se o seu telefone não se conecta	213
3.12.2	Como conectar o telefone por Wi-Fi	214
3.12.3	Conexão Wi-Fi Android	214
3.12.4	Conectando no modo MTP	214
3.12.4.1	Para usuários do Android 6.0 e superior:.....	218

3.12.5	Android - Confirme a impressão digital da RSA.....	219
3.12.6	Android - Ativar a opção "Fique acordado"	220
3.12.7	Como instalar o driver do Universal Android	225
3.12.8	Como viabilizar a verificação do USB	227
3.12.8.1	Veja todas as instruções com imagens	228
3.12.8.2	Dispositivos Huawei.....	234
3.12.8.3	Dispositivos Xiaomi.....	235
4	Sources of data.....	237
4.1	Import data.....	237
4.1.1	MOBILedit Backup XML.....	238
4.1.2	Android ADB backup file	238
4.1.3	iTunes backup folder	239
4.1.4	Data from folder	239
4.1.5	Data from ZIP file	239
4.1.6	Physical Image	239
4.1.7	Huawei backup folder.....	240
4.1.8	Xiaomi backup folder.....	240
4.1.9	Cellebrite UFED Report	240
4.1.10	Oxygen Backup XML.....	240
4.1.11	Samsung Smart Switch backup	240
4.1.12	Samsung feature phone	241
4.2	Samsung feature phone 's backup import.....	241
4.3	Samsung Smart Switch backup	243
4.3.1	How to	243
4.4	Reveal iTunes Backup.....	248
4.4.1	How to	249
4.5	Huawei backup.....	251
4.5.1	How to	252
4.6	Xiaomi-MIUI backup.....	255
4.6.1	Local backup in phone.....	256
4.6.2	Mi PC suite backup	257
4.7	Built-in SIM Cloning.....	258
4.7.1	Data extraction.....	259
4.7.2	SIM Cloning.....	260

4.7.3	Create a custom SIM card:	263
5	Forensic reports	266
5.1	Filtering.....	266
5.1.1	Global filters	266
5.1.2	Local filters	266
5.1.3	Highlights	266
5.1.4	File filtering.....	266
5.2	Global Filters	266
5.2.1	Filter by time	267
5.2.2	Filter by contact	268
5.2.3	Filter using a text string	268
5.2.4	Filter by location	269
5.3	Full content vs. Specific selection	269
5.3.1	Full Content.....	269
5.3.2	Specific Selection.....	270
5.4	Parental check.....	271
5.5	Case details	272
5.5.1	Show data sources	273
5.5.1.1	The PDF report:	273
5.5.1.2	The HTML report:	273
5.5.1.3	The XLSX report:.....	274
5.5.1.4	Clutter filtering.....	274
5.5.2	Title Page and Header information.....	274
5.6	Local filters	276
5.7	How to make reports smaller	277
5.7.1	Filtering.....	277
5.7.2	PDF Splitting.....	277
5.7.3	Clutter filtering.....	277
5.7.4	Source of data	277
5.8	Report customization	278
5.8.1	Creating custom translation.....	278
5.8.2	Editing text which is already in MOBILedit Forensic express.....	281
5.8.3	Editing time formats	282
5.9	Backup password breaking	284

5.9.1	Entering password directly.....	285
5.9.2	Dictionary attack.....	285
5.9.3	PIN attack.....	287
5.10	Output folders structure.....	288
5.10.1	HTML Report.....	289
5.10.2	PDF Reports.....	289
5.10.3	MS Excel Report.....	290
5.10.4	MOBILedit Backup.....	290
5.10.5	MOBILedit Export.....	290
5.10.6	Report subfolder "Phone".....	290
5.10.7	Additional backup folders – iTunes, ADB, and iCloud.....	291
5.10.8	Logs and other files.....	291
5.10.9	Files and long folder paths.....	291
5.11	Running extraction.....	291
5.12	Outputs - reports, exports, and backups.....	292
5.12.1	HTML Report.....	293
5.12.1.1	Report_long.html.....	293
5.12.1.2	Report_index.html.....	294
5.12.2	PDF Report.....	295
5.12.2.1	Single file.....	295
5.12.2.2	Multiple files.....	296
5.12.3	MS Excel report.....	296
5.12.4	Export & backups.....	297
5.12.4.1	MOBILedit Backup.....	297
5.12.4.2	MOBILedit Export.....	298
5.12.4.3	Cellebrite UFDR.....	298
5.12.4.4	ADB and iTunes backups.....	299
5.13	Load report configuration.....	299
5.14	Export name and destination.....	300
5.15	MOBILedit Export XML documentation.....	301
5.15.1	Who is this document for?.....	301
5.15.2	Basic concepts.....	301
5.15.3	Brief description of XML.....	301
5.15.4	More about files.....	302

5.15.5	Containers, items, parts and others.....	302
5.15.6	Data sources.....	303
5.15.7	A few notes on use	303
5.15.8	Explanation of table items.....	303
5.15.8.1	Occurrence indicators.....	303
5.15.8.2	Data types.....	304
5.15.8.3	Containers in detail - attributes and nested tags	304
5.15.8.4	Items in detail - attributes and nested tags.....	311
5.15.8.5	Parts in detail - attributes	319
5.15.9	XSD file structure specification	324
5.16	Malware detection	324
6	Specific selection	325
6.1	Data - Screenshots of report settings.....	325
6.2	Data - Summary	325
6.3	Data - Deleted data	325
6.4	Data - Captured phone photos.....	326
6.4.1	Take picture.....	326
6.4.2	Capture screenshot.....	327
6.4.3	Import.....	328
6.5	Data - Accounts	329
6.6	Data - Contacts.....	329
6.6.1	Contacts.....	329
6.6.1.1	Display order of contacts.....	330
6.6.1.2	Example of contacts report:	331
6.7	Data - Messages.....	332
6.7.1	The display order of messages	333
6.7.2	Example of messages report:	334
6.8	Data - Emails.....	335
6.8.1	Example of email report:	338
6.9	Data - Calls.....	340
6.9.1	Example of call logs report:	341
6.10	Data - Organizer	342
6.10.1	Example of organizer report:.....	343

6.11	Data - Applications.....	345
6.11.1	Applications.....	345
6.11.2	App downgrade feature	345
6.12	Data - Application list.....	346
6.12.1	List of applications.....	346
6.12.2	Extract APK files from the phone.....	347
6.12.3	Malware detection	347
6.13	Data - Photo recognizer	347
6.14	Data - Face Matcher	351
6.15	Data - Photos	354
6.15.1	Example from the report:	356
6.16	Data - Image files.....	356
6.16.1	Example of images report with photo recognizer:	358
6.17	Data - Large images.....	360
6.18	Data - Audio files	361
6.18.1	Example of audio files report:	362
6.19	Data - Video files.....	363
6.19.1	Example of contacts report:	365
6.20	Data - Video storyboard (FFmpeg)	366
6.20.1	Overview	366
6.20.2	Installation	366
6.20.3	Storyboard settings	369
6.20.4	Uninstallation.....	369
6.21	Data - Documents.....	369
6.22	Data - Files	372
6.22.1	All files.....	372
6.22.2	List of application files.....	372
6.22.3	Exclude Files	372
6.22.4	Example of a files report:	372
6.23	Data - Matched Files.....	373
6.23.1	Example of a report with Matched Files:.....	373
6.24	Data - Application usage.....	373
6.25	Data - Bluetooth pairings.....	373

6.25.1	Example of Bluetooth pairings report:.....	374
6.25.2	Example of seen Bluetooth devices report:.....	375
6.26	Data - Cell towers	375
6.26.1	Example of cell towers report:.....	376
6.27	Data - Contact analysis	376
6.28	Data - Cookies	379
6.28.1	Example of cookies report:.....	379
6.29	Data - GPS locations.....	380
6.29.1	Locations	380
6.30	Data - Notifications	382
6.31	Data - Screen unlocking history	384
6.32	Data - Passwords.....	384
6.33	Data - SIM card	386
6.34	Data - System logs.....	386
6.35	Data - User dictionary	387
6.36	Data - WiFi networks	387
6.36.1	Example of WiFi networks report:	388
6.37	Data - Web	388
6.38	Data - Timeline	389
6.38.1	Generate timeline	390
6.38.2	Order by time	390
6.38.3	Filter by time	390
6.38.4	Selected items.....	390
6.38.5	Timeline data may contain for example:	391
6.38.6	Example of timeline report:.....	392
6.39	Data - Data extraction log.....	392
7	Applications.....	394
7.1	Supported applications	394
7.1.1	Sort and search	394
7.1.2	The database.....	395
7.2	Advanced techniques to extract messages and files	396
7.2.1	Rooting / Jailbreaking	397
7.2.1.1	Rooting	397

7.2.1.2	Jailbreaking.....	397
7.2.2	Creating a physical image of your device	398
7.2.2.1	MTK Hack.....	398
7.2.2.2	EDL Hack.....	398
7.2.2.3	LG Hack.....	398
7.2.2.4	TWRP Method	399
7.2.2.5	Dirty Cow	399
7.2.3	Using an App downgrade function in our software MOBILedit Forensic Express.....	399
7.3	How to make an application backup	399
7.4	Request to add support for analysis of an application	407
7.5	App downgrade	408
7.5.1	Functionality	409
7.5.2	List of supported apps	412
8	Camera Ballistics.....	413
8.1	About Camera Ballistics technology	415
8.2	Minimum system requirements	416
8.3	How to activate	417
8.4	Main page	418
8.5	Camera Ballistics - Updates.....	419
8.6	Learn - Create fingerprint	420
8.7	Analyze - process photos	423
8.8	Image quality requirements	428
8.9	How to create Logs	429
9	FAQ.....	430
9.1	How to buy additional licenses?	430
9.2	How to make reports smaller?	430
9.2.1	Split the PDF report file to multiple files.....	431
9.2.2	Use filtering	433
9.3	Does MOBILedit Forensic Express offer viewer or data analysis tool?	433
9.4	What are the types of logs?.....	435
9.4.1	Extraction logs.....	435
9.4.2	Application Logs.....	435

9.4.3	Communication logs.....	435
9.5	Where to find previous Android backup?.....	435
9.6	iTunes backup password is required each time I run analysis	436
9.7	Does MOBILedit Forensic Express have the capability of extracting data from iCloud?	436
9.8	What are the types of logs and how to use them for troubleshooting.....	437
9.8.1	Extraction logs.....	437
9.8.2	MOBILedit Application Logs	437
9.8.3	Communication logs.....	437
9.8.4	How to get logs for troubleshooting?	438
9.8.5	What to do in case the program crashes unexpectedly?	438
9.9	What if there is no information in a report from iPhone?	438
9.10	How reliable is recovered data?	439
9.11	I connected the phone but can not press 'next' to next step	439
9.12	What if the connector installation has failed?	439
9.13	What if the PDF report is empty or incomplete?.....	440
9.14	What if the connection is suspended during extraction?.....	440
9.15	What is the difference between software and individual package update?	440
9.16	What if I have a blank page in my report?	441
9.17	How to get as much data as possible from WhatsApp	441
9.17.1	1) Rooting / Jailbreaking	442
9.17.1.1	Rooting	442
9.17.1.2	Jailbreaking.....	442
9.17.2	2) Creating a physical image of your device	443
9.17.2.1	MTK Hack.....	443
9.17.2.2	EDL Hack.....	444
9.17.2.3	LG Hack.....	444
9.17.2.4	TWRP Method	444
9.17.2.5	Dirty Cow	445
9.17.3	3) Using an App downgrade function in our software MOBILedit Forensic Express.....	445
9.17.4	4) Captured phone photos.....	445
10	MOBILedit Releases.....	446
10.1	7.4. Update	446
10.2	7.3. Update	446

10.2.1	What's new	447
10.2.2	Improvements and bugfixes.....	449
10.2.3	Application updates.....	449
10.3	7.2. Update	450
10.3.1	What's new	450
10.3.2	Improvements and bugfixes.....	450
10.4	7.1. Update	451
10.4.1	What's new	451
10.4.2	Improvements and bugfixes.....	454
10.5	7.0.3. Update	454
10.5.1	What's new	454
10.5.2	Improvements and bugfixes.....	454
10.6	7.0.2. Update	454
10.6.1	What's new	455
10.6.2	Improvements and bugfixes.....	455
10.7	7.0.1. Update	456
10.7.1	What's new	456
10.7.2	Other improvements.....	456
10.8	7.0. Update	457
10.8.1	What's new	457
10.8.2	Other improvements.....	459
10.8.3	Application analysis improvements.....	459
10.9	6.1.1. Update	460
10.9.1	What's new	460
10.9.2	Bugfixes and minor improvements.....	460
10.9.3	New app analysis	460
10.9.4	Improved app analysis.....	461
10.10	6.1. Update	461
10.10.1	What's new	461
10.10.2	Bugfixes and minor improvements.....	461
10.10.3	Improved app analysis.....	461
10.11	6.0.1. Update	461
10.11.1	Improvements.....	462
10.11.2	Bugfixes	462

10.12	6.0. Update	462
10.12.1	Now available in two editions - PRO and STANDARD.....	463
10.12.2	New features and improvements.....	463
10.12.3	Bugfixes	463

MOBILedit Forensic is a phone and cloud extractor, data analyzer, and report generator all in one solution.


A powerful 64-bit application using both the physical and logical data acquisition methods, MOBILedit is excellent for its advanced application analyzer, deleted data recovery, live updates, a wide range of supported phones including most feature phones, fine-tuned reports, concurrent phone processing, and easy-to-use user interface. With the password and PIN breaker, you can gain access to locked ADB or iTunes backups with GPU acceleration and multi-threaded operations for maximum speed.

Forensic offers maximum functionality at a fraction of the price of other tools. It can be used as the only tool in a lab or as an enhancement to other tools through its data compatibility. When integrated with Camera Ballistics it scientifically analyzes camera photo origins.

1 Introduction

MOBILedit Forensic Express¹ is a phone and cloud extractor, data analyzer and report generator all in one solution. A powerful 64-bit application using both the physical and logical data acquisition methods. MOBILedit is excellent for its advanced application analyzer, deleted data recovery, live updates, a wide range of supported phones including most feature phones, fine-tuned reports, concurrent phone processing, and easy-to-use user interface.


With the advanced password and PIN breaker, you can gain access to locked ADB or iTunes backups with GPU acceleration and multi-threaded operations for maximum speed. When integrated with Camera Ballistics it scientifically analyzes camera photo origins.

 In case you'll have any questions regarding MOBILedit Forensic Express, do not hesitate to contact our dedicated support team [here](#)².

1.1 System Requirements

To enjoy the best possible user experience, make sure your computer meets the minimum system requirements such as:

- CPU: Intel Core i3 is minimum, i7 is recommended for concurrent extractions, CPU with AVX is required for Face Matcher and Photo Recognizer
- RAM: 4 GB as minimal configuration, 16 GB is recommended for analyzing phones with a lot of data
- HDD: free space of 20 GB on the system drive, plus suitable storage space for the reports
- OS: 64-bit OS is required, Windows 7 SP1 and above (Windows 7 SP1, Windows 8.1, or Windows 10). 32-bit version can be used on special occasions, it is not recommended for processing more data and can be either downloaded or requested on-demand.
- Minimum screen resolution: 1250x800, recommended 1920x1080
- High-quality cables (mini USB, iPhone variations) for connecting the phones are essential

 To install MOBILedit Forensic Express successfully, please disable your antivirus program. If enabled, our hacking features (i.e. Dirty Cow hack) may trigger the antivirus warning system. If it is not possible to disable it completely, disable at least the automatic scan of the folders. By disabling your antivirus program you will also prevent any possible errors that may occur during installation and extraction.

1.2 Purchase

You can purchase MOBILedit Forensic Express from our [online store](#)³ and receive your activation key via email immediately.

Contact our sales team⁴ if you'd like to:

- Place a higher quantity order
- Include our products in a large tender
- Become one of our resellers
- Receive VIP service

¹ <https://www.mobiledit.com/forensic-express>

² <https://www.mobiledit.com/contact>

³ <https://www.mobiledit.com/store>


⁴ <http://www.mobiledit.com/contact>

- Learn more about custom development options
- Inquire about our discounts for law enforcement and educational institutions


1.3 Download & Installation

To start using MOBILedit Forensic Express you need to download and install the program to your computer first.

You can download MOBILedit Forensic Express on our main download page [here](#)⁵.

 If you already have MOBILedit Forensic Express installed on your computer, go to the [Getting Started](#) (see [page 25](#)) section to learn more.

1.4 License activation

 There are two types of activation possibilities: online activation and activation by physical dongle. Each one has its own advantages.

Online activation specifics

- the license can be purchased online, it is delivered immediately and the activation is also online
- the computer needs to be connected to the internet
- one license is exactly for one computer
- can be deactivated online too


Dongle license specifics

- a dongle is a device with a special security chip, that you connect to a USB
- needs to be physically delivered by the carrier
- the license works only if the dongle is present
- allows for better sharing of licenses within departments: you can have multiple installations of our products in your department and in one-time work only on those with the dongle inserted

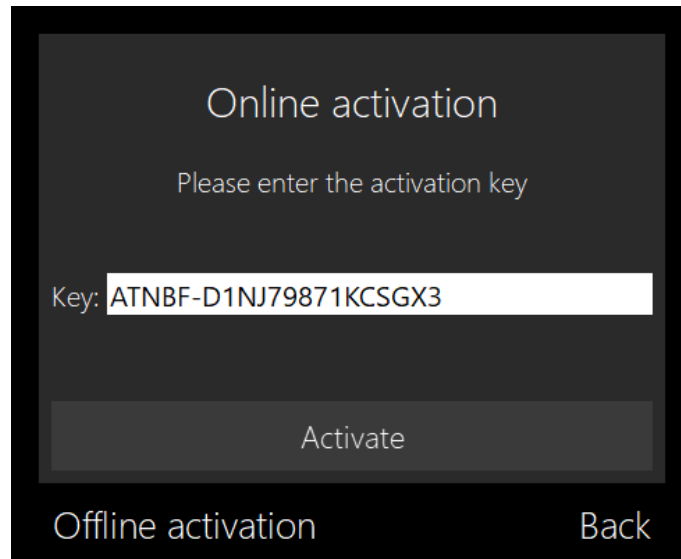
You can choose which mode is better for your purpose.


With a full license, you can use MOBILedit Forensic Express with an unlimited number of phones. To activate your license, follow the steps below:

1. Launch the software.
2. Click on the “Activate” button.
3. Enter the key you have received.

 If you have been using an activated demo license, deactivate the demo key and then activate the software with your new full license key.

⁵ <http://www.mobiledit.com/downloads#forensic>



 The digital key version of MOBILedit Forensic Express is not compatible with the **dongle**. Read how to use the dongle version [here](#)(see page 24).

1.5 Single phone license activation

With a single phone license, you can use only a single phone to work with MOBILedit Forensic Express. Once you activate the license it becomes locked to the selected phone.

1.5.1 How to

1. Download and install MOBILedit Forensic Express from <http://www.mobiledit.com/downloads#forensic>

Forensic products

Extract and deeply analyze phone content including deleted data, application's data, passwords, geolocations and anything what might reside in the phone. Professional tool for authorities as well as for enterprise and end users.



MOBILedit Forensic Express

[DOWNLOAD](#) (Windows 64-bit) | Version 7.0.3.16830 | [WHAT'S NEW](#) | [LEARN MORE](#)

Available Add-Ons:

LIVE UPDATES


Get new Live Updates of App Analyzer, get info about releases [here](#). See the list of supported apps [here](#).

TRANSLATIONS

Create report templates in any language.

APP DOWNGRADE

Downgrade apps to older versions with weaker security.

 [setup_MOBILeditF...exe](#) ^

2. Install the correct USB drivers for your phone. We recommend downloading a [complete driver package](#)⁶.

Phone Drivers

Device drivers necessary to connect a phone to Windows and start using our products.



Universal Android driver

DOWNLOAD

Size **16.7 MB**

Universal phone driver suitable for most Android phones.



Apple device drivers

DOWNLOAD

Version **1.0.9.7** | Size **7.0 MB**

Driver for Apple devices running iOS 3 and higher. This driver works only with MOBILedit! version 5.5 and higher. This driver doesn't require installation of iTunes.



Individual USB phone drivers

[Click here for more details](#)

3. Run MOBILedit Forensic Express and click on "Activation".

i If you have already bought MOBILedit Forensic Express click on "Activate" and fill in all the necessary details. If you haven't bought MOBILedit Forensic Express yet, click on "Purchase license" and proceed with the purchase itself

4. Connect your phone to PC via USB cable, Bluetooth, or Wi-Fi. On iOS, unlock the device and confirm your trust for the computer. On Android, unlock the device and enable USB debugging mode, then confirm your trust for the computer (more information on enabling USB debugging can be found [here](#)(see page 139)).

! Be aware that it is not possible to activate a phone with Android 10 OS with a single phone license through wifi. However, if you activate a phone through a cable, you will be able to use it with wifi later.

5. After you successfully connect your phone, click on "Next" and you will be prompted to activate the phone.

6. Click on "Activate selected phone". Your phone's IMEI number will be now used by the software in order to recognize it. Once you activate the single phone license, you will be able to **run unlimited extractions** on the registered phone.

i Please note that the single phone license is limited in features like non-standard import, physical image creation, or Photo Analyzer. The features will not work with a Single phone license!

⁶ <http://www.mobiledit.com/downloads#phone-drivers>

1.6 Offline activation

In order to activate your license offline, follow a few simple steps below:

1. Create an offline activation file and place it on a USB flash drive.
2. Download MOBILedit Forensic Express and place it on a USB flash drive.
3. Install the software on the offline computer.
4. Input your activation key details into the activation dialogue and click the “Export request” button (this step must be done on the offline computer).

5. An activation file will be automatically generated. The file must be uploaded to the www.mobiledit.com/activation⁷ page, once you are back online.

6. Submit the file, hit the "Generate activation" button, and a new offline activation file will be ready to download.

Upload activation file

Generate activation

⁷ <http://www.mobiledit.com/activation>

7. Place the new file on the USB flash drive and return to your offline computer to complete the offline activation.
8. Select the Import button (Import Activation) in the activation dialogue and your offline activation is complete.

i Offline activation is possible for unlimited licenses only. To activate a single phone license it is necessary to have an internet connection.

1.7 Dongle license activation

The dongle is a hardware license key which can be used only with a special binary version of MOBILedit Forensic Express.



In order to get this special binary version, you need to request it directly from our sales department. You can contact our sales through this [webform](#)⁸.

To activate your license with the dongle, follow the steps below:

1. Download and install the dongle version of MOBILedit Forensic Express you received from our sales representative.
2. Insert MOBILedit dongle to a USB port, there is no device drivers installation required.
3. Run MOBILedit Forensic Express, it will check the dongle and allow for the full functionality of the product according to a license you purchased.
4. If you remove the dongle, the product will stop working.
5. In order to check the status of the license, go to the Activation.

i Each time you want to start MOBILedit Forensic Express, you'll need to have the MOBILedit dongle inserted in the computer.

1.8 Deactivation

Since MOBILedit Forensic Express can be linked to only one PC at a time, if you plan to move to a new PC or OS, you will need to de-activate it on the previous one.

If you plan to reinstall your OS or move to another computer, you need to de-activate your license first. To de-activate your license, follow a few simple steps below:

1. Go to Help -> License manager -> Deactivate License.
2. Reactivate your license with the same key on a new computer.

⁸ <https://www.mobiledit.com/contact>

1.9 Getting Started

- [Before you begin](#)(see page 25)
- [Connecting phones](#)(see page 25)
- [Getting maximum including deleted data](#)(see page 26)
- [Password and PIN breaking](#)(see page 26)


MOBILedit Forensic Express performs mobile phone content extractions and is used by professionals in law enforcement, military as well as in the corporate and private sectors. By connecting a phone via USB cable, Wi-Fi or Bluetooth you can perform individual examinations of most of the mobile devices and generate reports in [multiple formats](#)(see page 292) (PDF, HTML, Excel, etc.) for a variety of needs.

MOBILedit Forensic Express can retrieve messages, call logs, pictures, contacts, apps, calendar events, emails, passwords, media, file systems, deleted data, and much more. You can even [select specific data](#)(see page 325) which you want to extract from the device.

1.9.1 Before you begin

For the best possible experience, we recommend taking a look at the [minimum system requirements](#)(see page 416).

[Download](#)⁹ and install MOBILedit Forensic Express if you haven't already. [Activate](#)(see page 20) the software with a [valid license](#)(see page 19).

 The digital key version of MOBILedit Forensic Express is not compatible with the dongle. For the dongle version please [contact](#)¹⁰our technical support.

The step by step installation guide is available in the video below:



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=hh932-gU9Yg#action=share>

Before connecting the phone, be sure you have installed the necessary device drivers on your PC. You can download our [Complete Driver Pack](#)¹¹.

When connecting an Android device with the 64-bit version of MOBILedit Forensic Express, the device driver provided by the manufacturer of the phone might not allow a proper connection between the device and the software. You might need to replace it with the [universal ADB \(Android\) driver](#)(see page 148).

1.9.2 Connecting phones

- [Android](#)(see page 138)
- [iOS](#)(see page 160)
- [Other](#)(see page 179)

⁹ <http://www.mobiledit.com/download-list/forensic-express>

¹⁰ <https://www.mobiledit.com/contact>

¹¹ <http://www.mobiledit.com/download-list/phone-drivers>

1.9.3 Getting maximum including deleted data

While MOBILedit Forensic Express is a very powerful extraction tool and extracts practically all information available, advanced users looking to get even more information from the phone should first 'root' or 'jailbreak' the phone.


Android [rooting](#)(see page 68) is an important step that will allow maximum data and deleted data acquisition. If you cannot or do not want to root the phone, you can alternatively use the [Application Downgrade](#)(see page 408) feature to find hidden data and deleted data in certain supported apps.


For iPhone or iOS devices supply the iTunes backup password. [Jailbreaking an iPhone](#)(see page 100) can bypass several types of Apple prohibitions for the end-user, including modifying the operating system (enforced by a "locked bootloader"), installing non-officially approved applications via side loading, and granting the user elevated administration-level privileges (rooting). You can also try to bypass the passcode on locked iOS devices with the [Lockdown Files Method](#)(see page 98).

1.9.4 Password and PIN breaking

MOBILedit Forensic Express offers all kinds of password bypassing tools such as [MTK hack](#)(see page 60), [LG hack](#)(see page 55), [EDL hack](#)(see page 50), and [flashing phones with recovery image](#)(see page 78).

Additional data can be found in either the iTunes or ADB backups. In case the backup is password-protected, you can use the [Password Breaker](#)(see page 284) to bypass the protection.

 Keep in mind that these features are only included in our [PRO version](#)¹².

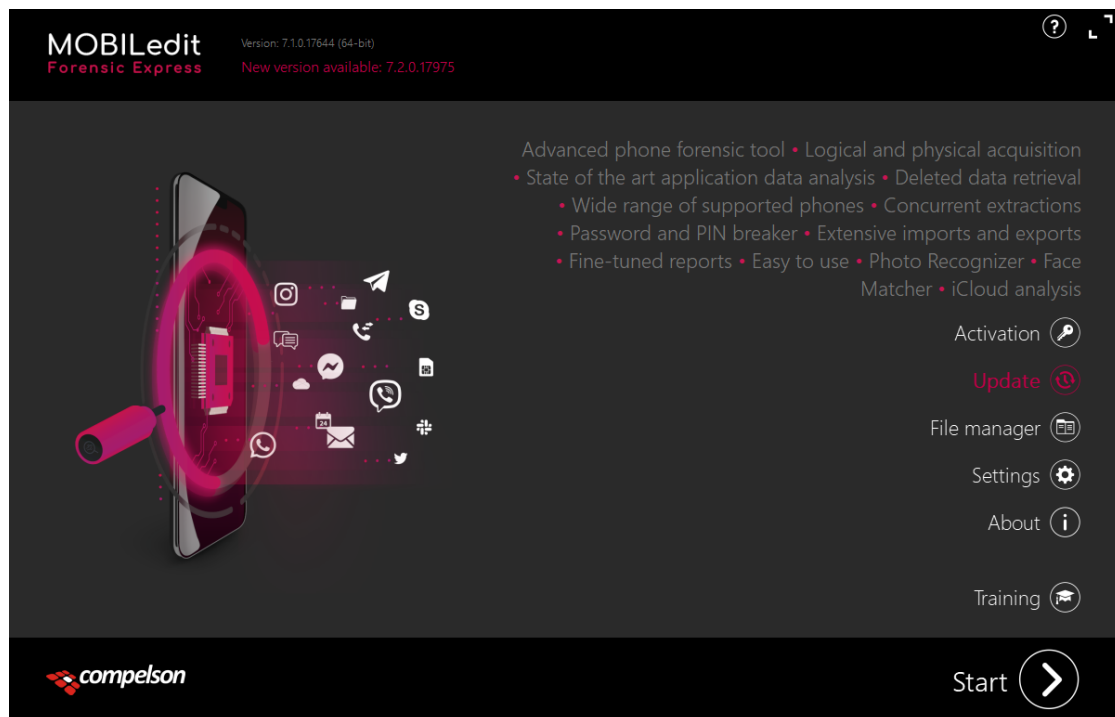
 In case you'll have any questions regarding MOBILedit Forensic Express, do not hesitate to [contact](#)¹³ our dedicated support team.

1.10 Home Screen

This is your Home screen. You will see this screen every time you start MOBILedit Forensic Express. On this page, you can change your activation info or deactivate the software, check for updates to find out if a new version is available, manage your files to view, move and copy all files that are in your computer, edit your personal settings, find information about the software, access our expert training material, and most importantly start your phone analysis.

¹² <https://www.mobiledit.com/online-store/forensic-express>

¹³ <https://www.mobiledit.com/contact>



i Learn everything you need to know to connect your phone in [Connecting a device](#)(see page 112) section.

1.11 Settings

- [Global Settings](#)(see page 27)
- [Investigator details](#)(see page 27)
- [Logging](#)(see page 28)

In the settings, you are able to customize and edit various useful details such as Generic global settings, Investigator details, and Logging.

1.11.1 Global Settings

In Global Settings, you can change the language of the UI and set if you want to show our product logo in your reports. We currently support English, Czech, Slovak, Spanish, Portuguese, and Chinese (in beta version as of this moment).

i Keep in mind that the language in these settings does not affect the language of reports

1.11.2 Investigator details

Investigator details section allows you to fill in the investigator details which will appear in every report you will create.


1.11.3 Logging

The logging section allows you to edit the log level, max log size, or access logs folder and clear them.

We currently have 4 levels of logging:

- Off
- Basic
- Detailed
- Debug

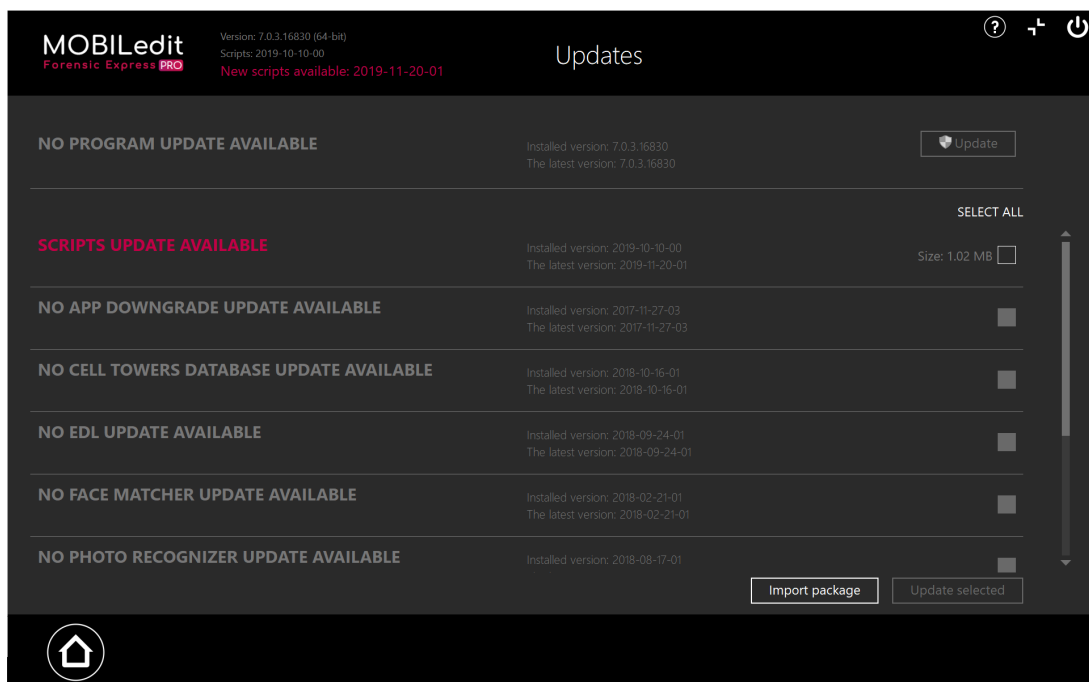
We advise you to set the Log levels to **Debug** and the max log size to at least **4096KB**. The logs are very helpful in case there is a problem that you have to report to our Support team. You can find an article on how to send us logs [here](#)(see page 437).

 Every level of logging makes the extraction a bit slower because the software has to keep track of every step you and the device make and writes it down.

1.12 Updates

Upon clicking on the Check for updates button you will see a screen informing you about available updates for the software, or for some of its [add-ons](#)(see page 32).

Simply click on the Update button next to the category you would like to update. Once done, a new package will be downloaded and installed.



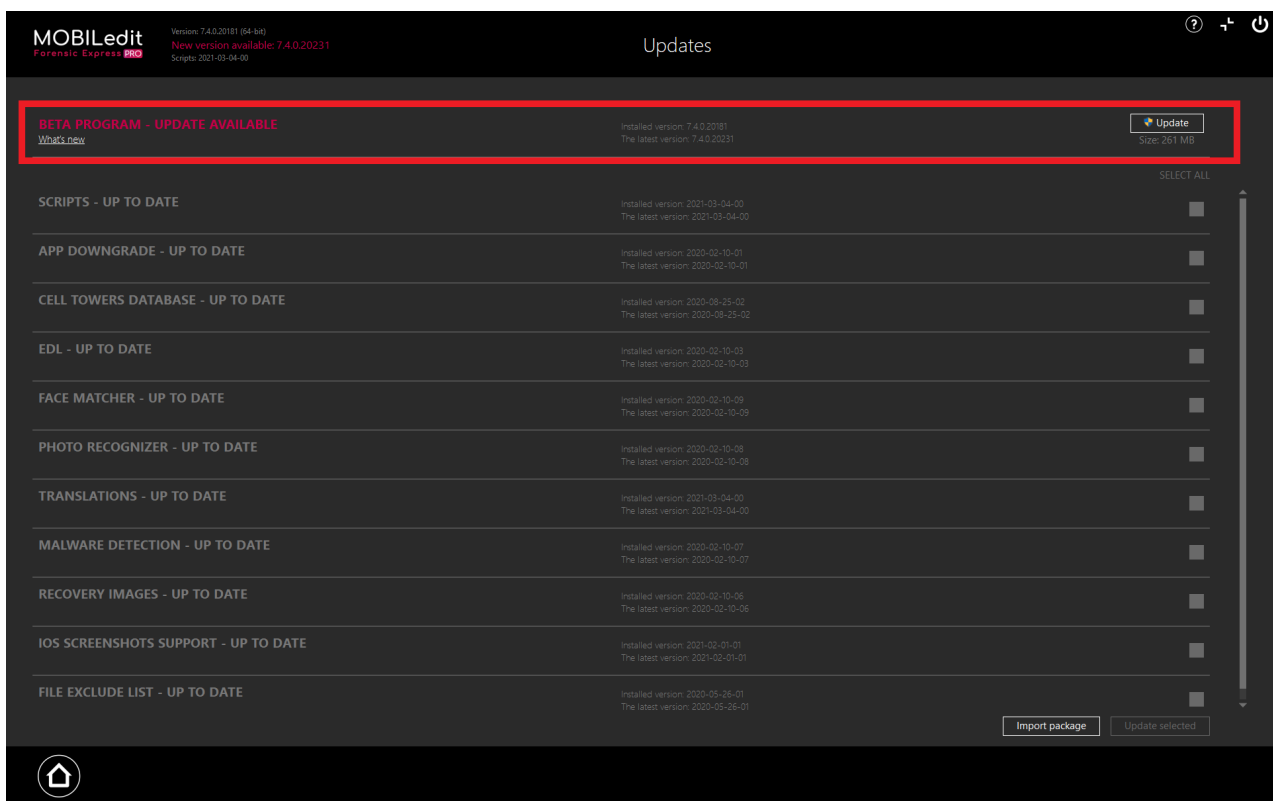
1.13 MOBILedit BETA testing program

i BETA testing program provides our users early access to updates with our soon-to-be-released features, improvements and bug fixes, and also it helps product is being tested on as many various devices as possible before it goes public.

By joining our public BETA program you get the opportunity to participate in our testing program, get your hands to our new features before it goes public, and provide us feedback.

In case you are interested, just contact us via our form [here](#).¹⁴

The BETA option will be activated for your license key immediately, and you will be notified directly in MOBILedit - the Updates section every time the version is released.



It is possible to re-download the official version any time by inserting your license key [here](#).¹⁵

For withdrawing from our BETA program, contact us in the same way as mentioned before.

⚠ Disclaimer: BETA version might be less stable than an officially released one, so please take that into the consideration. Usage in real cases and investigations is not recommended.

¹⁴ <https://www.mobiledit.com/contact>

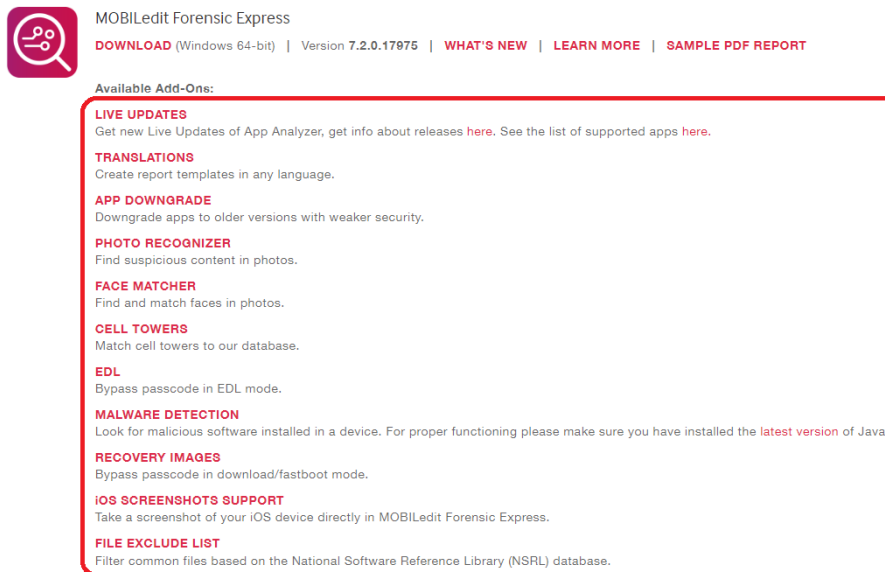
¹⁵ <https://www.mobiledit.com/previous-versions-downloads>

1.14 Offline updates

Version 5.0 and higher have the option to update offline. To update MOBILedit Forensic Express on an offline computer, you'll need to download the update packages first from our [website](#)¹⁶ and transfer them to an offline computer.

1.14.1 How to

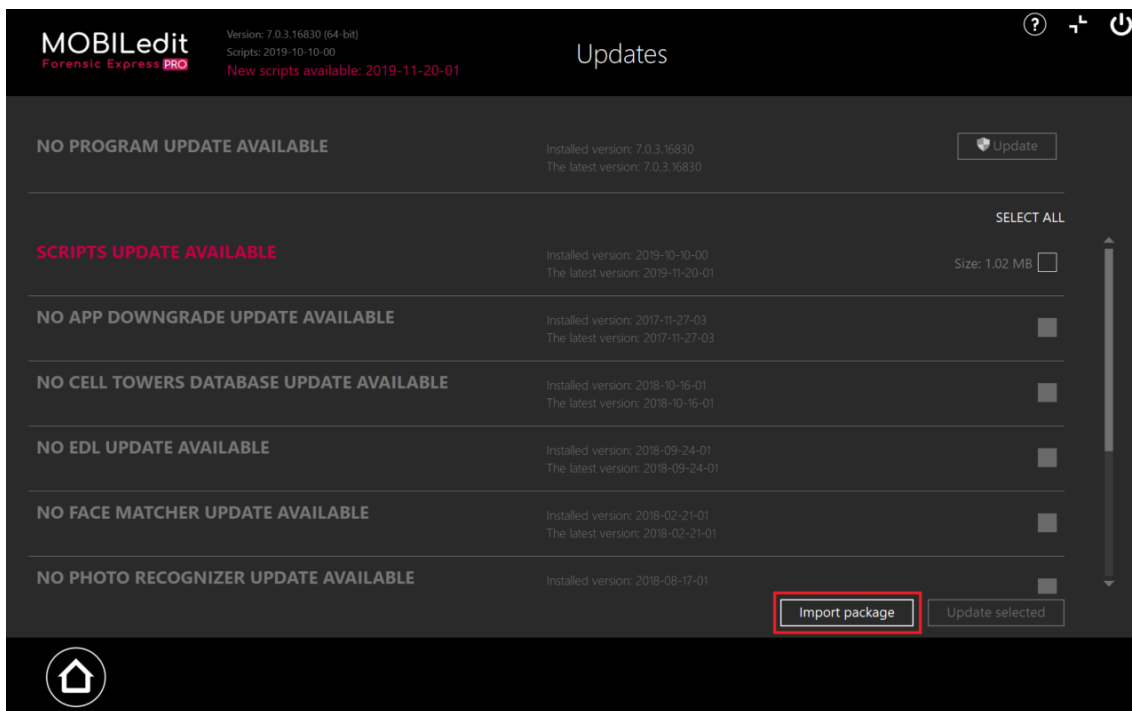
1. Download the latest packages [here](#)¹⁷.



2. Click on the desired update package. The downloading will start automatically.
3. Once the download is complete, transfer the packages to an offline computer and run MOBILedit Forensic Express.
4. On the home screen click on "Check for updates".
5. On the following screen, click on "Import package".

¹⁶ <https://www.mobiledit.com/downloads#forensic>

¹⁷ <http://www.mobiledit.com/downloads#forensic>



6. Locate and open the update packages. Once opened, the update will start automatically (MOBILedit Forensic Express might be restarted during the process).

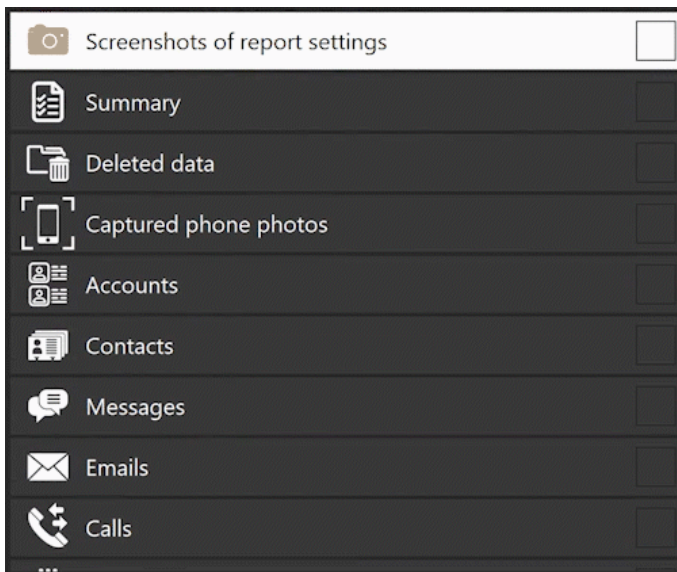
1.15 What data can be extracted?

MOBILedit Forensic Express automatically uses multiple communication protocols and advanced techniques to capture the maximum potential data from each phone and its operating system. It then combines all of the found data, removes any duplicates, and presents it all in one complete, customized and easy to read report.

We support over 1000+ applications as of this time and we are still adding more. If you need to analyze an app that is not yet supported, we can add it upon your request. To request app support visit our application database [here](https://apps.mobiledit.com/)¹⁸.

Below is a list of categories that can be selected for extraction and analysis while using the [specific selection](#) (see page 325). By selecting categories from this list you are essentially defining what will be extracted from the phone as well as what chapters you will see in the report.

¹⁸ <https://apps.mobiledit.com/>



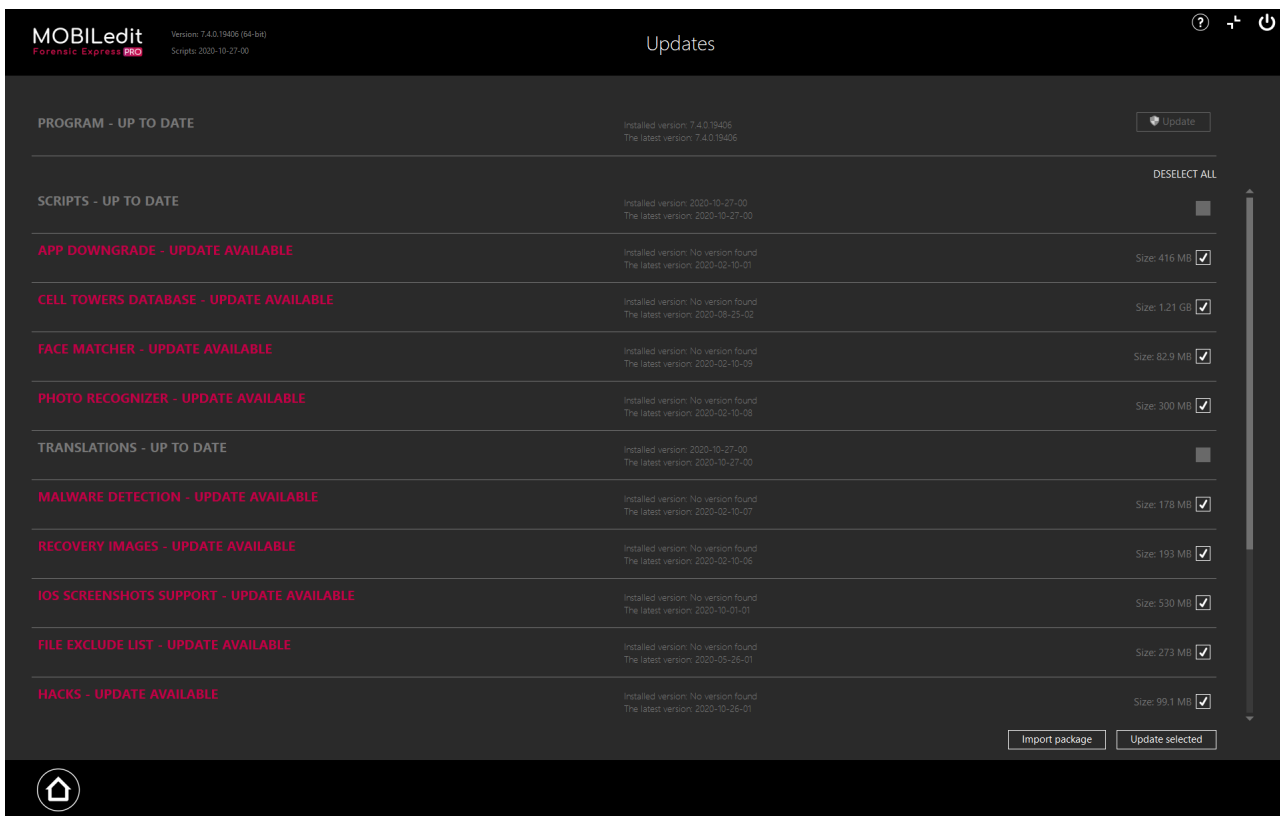
Disclaimer

Please note that for devices with Android version 7 and above the non-native application data - such as social media, email, internet activity or GPS locations - extraction is not supported (or can yield very little useful information), unless the phone is rooted or direct access to the phone files can be established.

1.16 Add-ons

- [App downgrade](#)(see page 33)
- [App engine](#)(see page 33)
- [iOS screenshots](#)(see page 33)
- [Cell towers](#)(see page 34)
- [Face Matcher](#)(see page 34)
- [File exclude list](#)(see page 34)
- [Photo Recognizer](#)(see page 34)
- [Malware Detection](#)(see page 34)
- [Recovery](#)(see page 34)
- [EDL](#)(see page 35)

Below you will find a list of add-ons which can be updated in the Updates section from the main menu. All of the following add-ons give you advanced options and are essential for extracting as much data as possible. We are continuously working on updates for MOBILedit Forensic Express, so whenever you receive an update notification, make sure to update all of the newly released packages.



1.16.1 App downgrade

Some applications manufacturers made restrictions on what data can be acquired from their apps. This is especially relevant for non-rooted phones.

To bypass this you can use the App downgrade, feature in MOBILedit Forensic Express, which will downgrade the apps to a version, in which there was no problem in obtaining the data from them directly.

You can read more about App downgrade [here](#)(see page 408).


The App downgrade feature must be activated in the specific selection.

1.16.2 App engine

The app engine turns on automatically as a source for the application script during the analysis. It is part of the program from the start and does not have to be downloaded separately.

1.16.3 iOS screenshots

Captured phone photos enable you to make a screenshot of the phone's display, import your own images or take a picture with the webcam. For Android OS devices this feature is turned on automatically.

 To enable this feature on iOS devices, you will need to download the iOS screenshots package from the Updates section.

1.16.4 Cell towers

Data about cell towers that the subject phone was connected to can be obtained. However, this is only possible with rooted Android phones. Obtained cell tower locations can be individually viewed on the map through the provided link.

When installed, it is turned on automatically both for the specific selection and full content.

1.16.5 Face Matcher

Face matcher is a neat feature which allows you to find photos with faces and compares them with provided source images. It can be turned on in the specific selection and to activate it, you need to upload at least one source image.

 To read more about can Face Matcher [here](#)(see page 351).


1.16.6 File exclude list

This feature allows the user to filter regular and unnecessary files. The filtering is based on hashes which the software gathers from NIST as a part of [NSLR packages](#)¹⁹ for Android and iOS.

1.16.7 Photo Recognizer

The Photo recognizer is powered by artificial intelligence module utilizing machine learning to automatically recognize suspicious content in photos such as drugs, nudity, weapons, currency and documents.

Photo recognizer can be turned on the specific selection if the respective package is installed.

 To read more about Photo recognizer click [here](#)(see page 347).

1.16.8 Malware Detection

Malware detection lets you check the extracted application APK files for malware. It must be installed first and turned on in the Application list section. To make Malware detection feature work properly, make sure to have Java installed on your computer.

1.16.9 Recovery

Recovery mode helps you to extract more data from an Android device. It is used by TWRP to flash the recovery.

¹⁹ <https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl>

 To read more about recovery click [here](#)(see page 44).

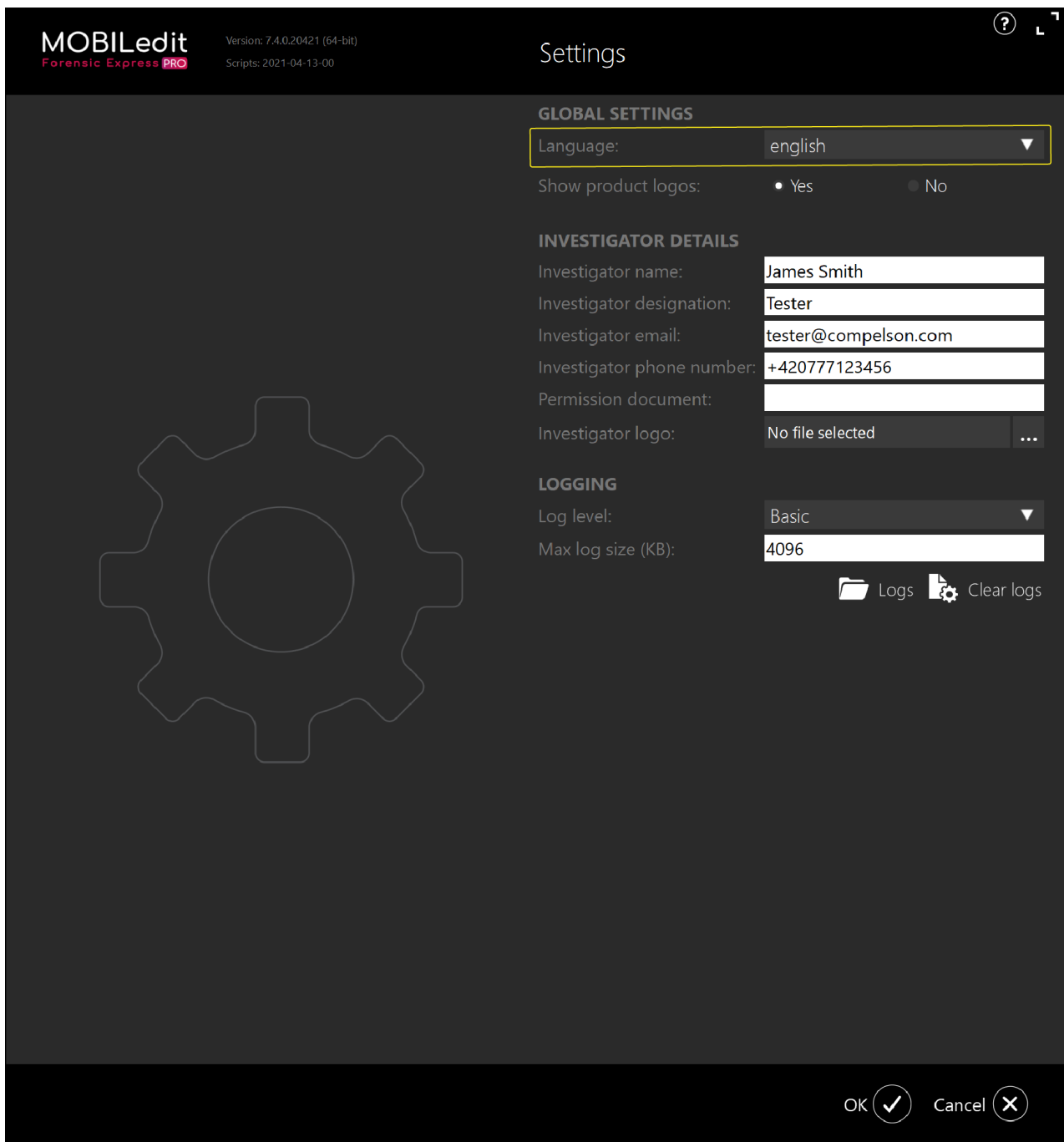
1.16.10 EDL

EDL package consists of programmers that are essential for [EDL hack](#)(see page 50). In future releases, this package will be removed and replaced by one that will be same for all of these hacks.

1.17 Localization

MOBILedit Forensic allows you to choose multiple options when it comes to both **User Interface** and **reports**:


User Interface language can be selected in the *settings* section:



Full product User Interface options:


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

The final **report** can be customized in the *specify report details* section:



Version: 7.4.0.20421 (64-bit)
Scripts: 2021-04-13-00

Specify report details



Apple iOS Device

REPORT SETTINGS:

Report time zone: Computer time zone (Europ ▼)

Report language: Nederlands ▼

Time format: local (dd.MM.yyyy H:mm:ss) ▼

Show data sources: Yes No

Clutter filtering: Yes No

CASE DETAILS:

Case label: Test_Sample

Case evidence number: 123456

Case evidence details: No

Case notes: Test_Sample

Clear Case details

PHONE DETAILS:

Device label: iPhone for testing

Device name: Apple iOS Device

Device ID: XY

Device evidence number: 123

Owner name:

Owner phone number:

Phone notes:

INVESTIGATOR DETAILS:

Investigator name: James Smith


Investigator designation: Tester



Investigator email: tester@compelson.com

Investigator phone number: +420777123456

Permission document:

Investigator logo: No file selected ...




Back  Next 

Generated reports are available in the following languages:

- English
- Spanish
- Portuguese
- German
- Estonian
- Chinese
- Korean

- Dutch
- Polish
- Slovak
- Czech

 The list of supported languages is not final and will be continuously expanded within future releases.

2 Introduction to phone forensics

In this chapter, you will find all the information you need to know to successfully operate with the mobile phone and MOBILedit Forensic Express to extract as much data as possible for your investigation.

2.1 Terms

Below you can find meanings and explanations for various abbreviations and terms used in our products and manuals:

ADB - Android Debug Bridge - allows the user to communicate and control their Android device using Windows/Linux/macOS command line.

API - Application Programming Interface - set of clearly defined methods of communication between various software com

Bootloader - enables the installed operating system to boot and startup while it verifies that all the software is genuine

Download mode - Samsung's alternative for Fastboot, requires Odin or Heimdall to communicate with PC

Fastboot - diagnostic protocol included with the SDK package used primarily to modify the flash filesystem of Android devices via USB connection from host computer

iOS - the mobile operating system used exclusively in Apple devices such as iPhones and iPads

Hotkey combination - a combination of keys used to boot into either recovery or Fastboot mode on Android devices ponents

CDMA - Code-division multiple access

CWM - ClockWorkMod recovery - another custom Android recovery

DFU - Device Firmware Upgrade mode allows all devices to be restored from any state

EDL - Emergency Download mode. This is the special mode through which users can perform various tasks like unbricking, unlock bootloader, and installation of any custom ROMs.

FRP - Factory Reset Protection - prevents the user from unlocking the phone if it was previously reset without removing the Google account

GSM - Global System for Mobile Communications

HTML - Hypertext Markup Language - is the standard markup language for creating web pages and web applications

ICCID - Integrated Circuit Card Identifier - used to identify SIM cards

IMEI - International Mobile Equipment Identity - a unique number to identify mobile devices

IMSI - International Mobile Subscriber Identity - used to identify the user of a cellular network

MAC - Media Access Control - a unique identifier assigned to network interfaces for communications at the data link layer of a network segment

MTK - MediaTek - mostly used for chipset

MTP - Media Transfer Protocol

OEM - Original Equipment Manufacturer

PTP - Photo Transfer Protocol

RSA - Rivest-Shamir-Adleman cryptosystem

SIM - Subscriber identity module

UFED - Universal Forensic Extraction Device

UFDR - UFED Physical Analyzer Report Package

TWRP - Team Win Recovery Project - one of the custom recoveries for Android devices

USB - Universal Serial Bus - an industry standard for cables, connection, communication, and power supply

XML - Extensive Markup Language - defines a set of rules for encoding documents both human and machine-readable

2.2 Deleted data

- [Physical extraction](#)(see page 40)
- [SQL databases](#)(see page 40)
 - [How SQLite data recovery works](#)(see page 41)
- [Basic recovery method](#)(see page 41)
- [Clutter filtering](#)(see page 41)
 - [How it works:](#)(see page 41)
- [What deleted data can be recovered?](#)(see page 41)
 - [Android](#)(see page 42)
 - [iOS](#)(see page 42)

With MOBILedit Forensic, you can recover deleted data in numerous ways. One option is recovering data from SQLite (or SQL) databases; another one is recovering files and folders from [Physical extraction](#)(see page 42). Below we will explain what each of these methods does and what kind of information you can recover.

2.2.1 Physical extraction

Physical extraction allows you to recover deleted files and folders which are still available through the file system and the SQL databases, which makes it the best option.

MOBILedit Forensic offers various ways to obtain a physical image, such as [EDL](#)(see page 50), [LG](#)(see page 55), [MTK](#)(see page 60) hacks. These can only be used with Android and KaiOS devices.


Time plays a big role in data recovery - the longer you wait, the lesser are the chances for a successful recovery. Restarting the device or even apps decreases the chance for data recovery.



Deleted files can be extracted from the physical dump on Android and KaiOS devices.

2.2.2 SQL databases

SQL databases allow you to recover the data which were marked as deleted or are still present in a database file. It also enables you to recover data from phones where you are unable to obtain the physical image, such as with iOS devices. SQLite is the most common way to store data for both **iPhone** and **Android**.

 A rooted device enables us to get straight to the file system and SQL databases as well, which increases the chance to obtain deleted data.

2.2.2.1 How SQLite data recovery works

There are three files associated with a database which may contain deleted records.


1. The database file - *<database name>* (https://www.sqlite.org/fileformat2.html#section_1²⁰)
2. The rollback journal - *<database name>-journal* (https://www.sqlite.org/fileformat2.html#section_3²¹)
3. The write-ahead log - *<database name>-wal* (https://www.sqlite.org/fileformat2.html#section_4²²)

2.2.3 Basic recovery method

When SQLite B-Tree is parsed, Freeblocks and Unallocated blocks are detected.

We know which table blocks belong to, so we know the data types of item columns that should be recovered. Data in each block (Freeblocks and Unallocated blocks) is read sequentially.

Each potential item found in the database has a header with data types and lengths of incoming data, so we read the whole block of data as if it could be considered a header. If it fits the table data types it is most likely a deleted item.

 Recovered records may be corrupted, incomplete or duplicate of an existing record.

2.2.4 Clutter filtering

The Clutter filtering will help you to discover and remove unusable or random files. It has to be explicitly turned on under the “Deleted data only” settings, as it is turned off by default when the program is installed for the first time. This set up will help you to filter all duplicate or incomplete records.

2.2.4.1 How it works:

- Each processed table in the database is defined as a set of columns.
- Each recovered record is compared (according to the set of columns) with all valid records and all previous recovered records.
- Depending on the result of comparison the record is processed (duplicates are thrown away).

2.2.5 What deleted data can be recovered?

Recovered deleted data will appear in the report with the proper tag. Deleted data type depends on the phone being used.

²⁰ <https://www.sqlite.org/fileformat2.html#section%5F1>

²¹ <https://www.sqlite.org/fileformat2.html#section%5F3>

²² <https://www.sqlite.org/fileformat2.html#section%5F4>

2.2.5.1 Android


MOBILedit can retrieve maximum deleted data mainly in these cases:

- Physical acquisition or physical image analysis is being used
- Older version of Android or an older application is on the phone
- Application downgrade method is being used - available in MOBILedit
- Phone is rooted

If one of the above methods isn't used, MOBILedit can still get some deleted application data, such as messages, browsing history, etc.

2.2.5.2 iOS


MOBILedit can retrieve deleted calls and messages if you have a password to an iTunes backup. In addition, some application data can be retrieved using the [iTunes backup method](#)(see page 248). We can also retrieve deleted photos from an iPhone up to 30 days after being deleted.

 While MOBILedit often successfully recovers valuable information, no data recovery can be guaranteed. Keep in mind that the particular deleted data might be no longer present in the phone. We can recommend using more forensic tools, so you try more methods. If you are an expert, the last chance is to search for data manually.

2.3 Physical extraction

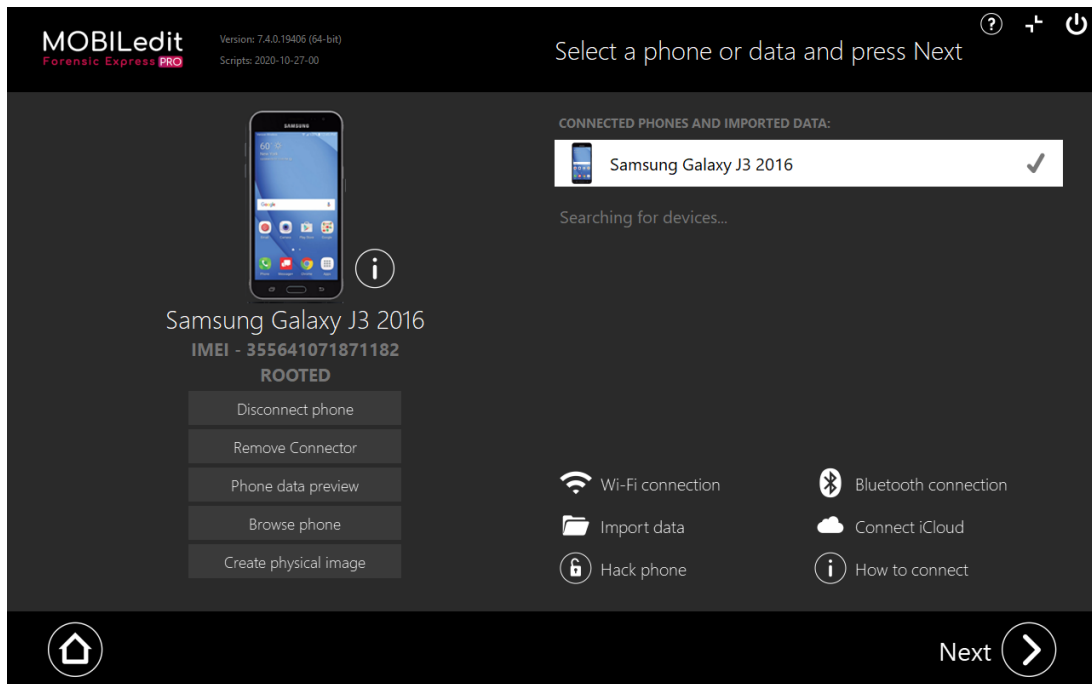
MOBILedit Forensic Express can perform physical extraction - a bit-by-bit image of data in the phone.

In order to perform a successful physical extraction, you need to have a rooted phone.

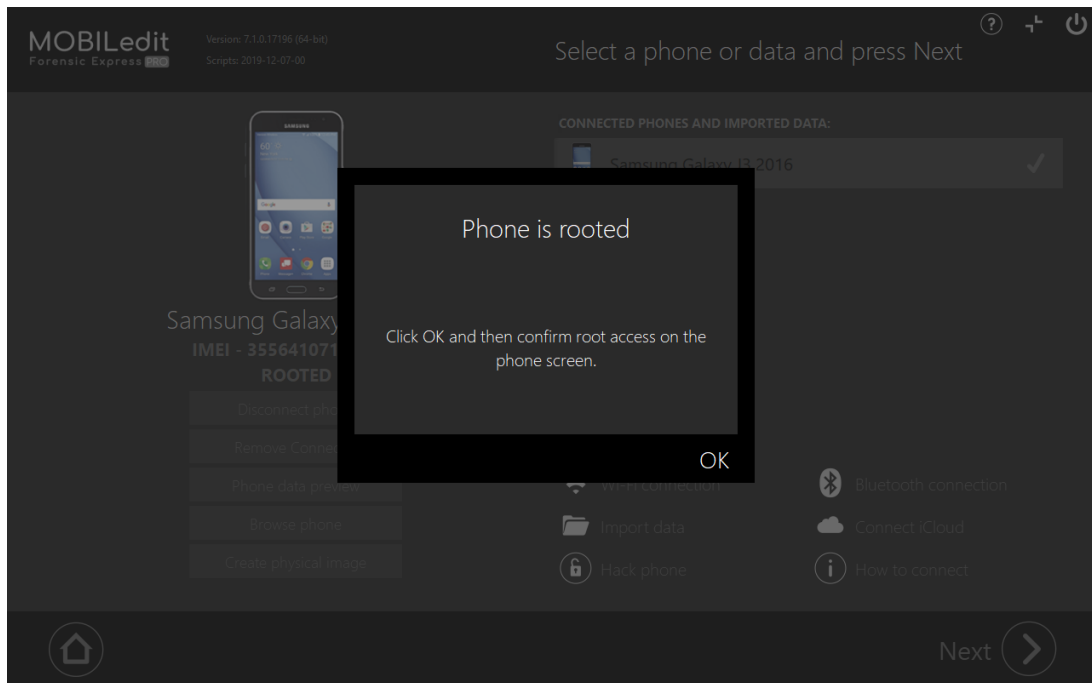
 For more information on rooting a phone please go to [How to root an Android phone?](#)(see page 68)

Physical extraction can also be performed on some Android phones utilizing exploits in their security system, for example, a set of [MTK](#)(see page 60) chipset-based phones and some [LG](#)(see page 55) models.

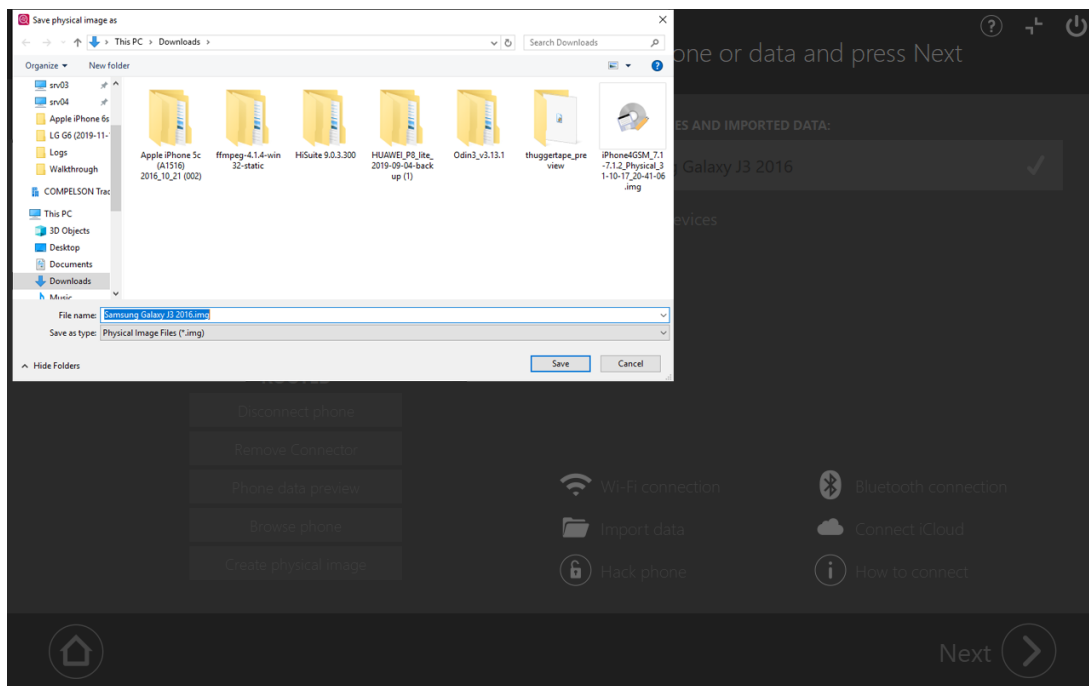
If the phone is rooted and connected successfully, the "Create physical image" button will be displayed under the picture of the phone.



Confirm root access on the phone (a popup will appear on your phone's screen, please tap on "Grant Access") and click OK.



Choose a name for the image file to be created, make sure you have enough space on the destination drive (the physical image will be as big as the full phone's storage):



After the physical image is created, it can be loaded into MOBILedit Forensic Express and then analyzed with results presented in a report.

i Please note that the Physical Image creation option is ONLY available in the Unlimited version of MOBILedit Forensic Express. The option to import a Physical Image is in addition available also in the Applications Analyser of ours.

2.4 Recovery mode

- [How to set the phone to recovery mode](#)(see page 44)
- [Connecting phone](#)(see page 45)

This page contains information about how to use a recovery mode in order to extract more data from an Android device.

Main benefits:

- Extraction from both rooted and non-rooted devices without knowing their screen lock password
- Creation of the device's physical image and reusing/reanalyzing it multiple times in the future to get better results without the need of having the device present
- Screen lock protection bypass - for more information go to [“Use TWRP to bypass Android lockscreen](#)(see page 73)”

2.4.1 How to set the phone to recovery mode

More information about recovery mode is available in an article [“How to boot into recovery on Android](#)(see page 89)”.

A guide on how to install the custom recovery on Samsung devices is available at “[ODIN method - Flashing TWRP on Samsung devices](#)(see page 86)”.

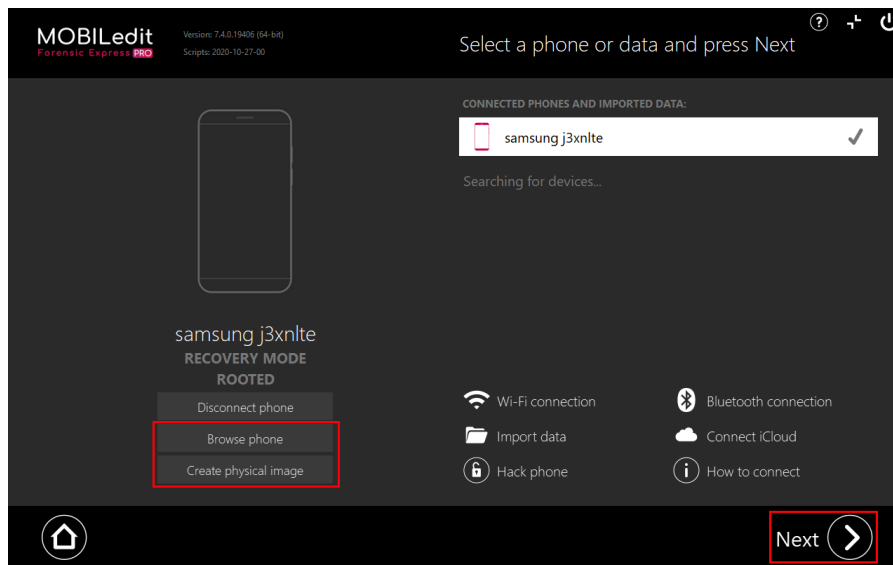
A guide on how to install the custom recovery on non-Samsung devices is available at “[CMD method - Flashing TWRP on non-Samsung devices](#)(see page 84)”.

2.4.2 Connecting phone

After you have prepared your device, simply open MOBILedit Forensic Express and connect the phone with a cable.

Choose whether you want to create a physical image, browse phone, or perform an extraction.

All other settings are the same as when you connect the phone in a device mode.



2.5 Android recovery data acquisition

Every Android phone has a "recovery" partition which is used for performing factory resets using an OEM's preloaded tools. However, this partition can be modified in order to replace the default tools by third-party recovery tools such as [TWRP](#)²³ or [CWM](#)²⁴.

These recoveries are (unlike the stock ones) capable of modifying all the internal system partitions of your phone or tablet (they need this capability in order to flash custom firmware).

TWRP even comes with a built-in file manager with unlimited root access so you can modify, add, or delete any system files manually.

The most important thing is that TWRP has a working MTP connection and ADB enabled, which **allows us to extract almost all data stored on your device and create physical images from them.**

By default, you can flash TWRP (or another recovery) image files to almost any device with an unlocked bootloader (a locked bootloader prevents users from sideloading any software to system partitions, so in order to flash anything on such device, you need to unlock the bootloader first).

²³ <https://twrp.me/about/>

²⁴ https://forum.xda-developers.com/wiki/ClockworkMod_Recovery

You can do so by using the "Fastboot" mode which allows the user to flash various system partitions including recovery. You can control your phone in the "fastboot" mode using Windows or Linux command line (similar to ADB).

The universal commands for flashing recovery images while in the "fastboot" mode are:

- **fastboot flash recovery "xxx.img"** – flash certain recovery image
- **fastboot oem unlock** – unlocks bootloader on supported devices
- **fastboot boot "xxx.img"** – boots straight from IMG file
- **fastboot reboot recovery** – reboots to recovery
- **fastboot reboot** – reboots the device

Samsung phones are different. They have "Download mode" instead of regular fastboot. Therefore, they can be controlled using Odin, a tool for flashing software developed by Samsung, or its open-source alternative called Heimdall.

Samsung phones also don't have their own recovery partition like other Android smartphones. Instead, they have a special ramdisk (a small IMG partition mounted by the kernel before and while booting the system) as a part of "boot.img" dedicated specifically for recovery.


2.6 How to unlock bootloader on Android

Unlocking bootloader is an essential step in the process of modifying system partitions such as flashing TWRP recovery. Locked bootloader prevents users from loading or flashing custom firmware into their devices.

Most of the phones with locked bootloaders can be officially unlocked by following a guide on the OEM's website.

This usually consists of submitting your phone's Device ID and IMEI and getting a device-specific unlock code which is then used in the "fastboot" command in order to authorize the unlocking process.

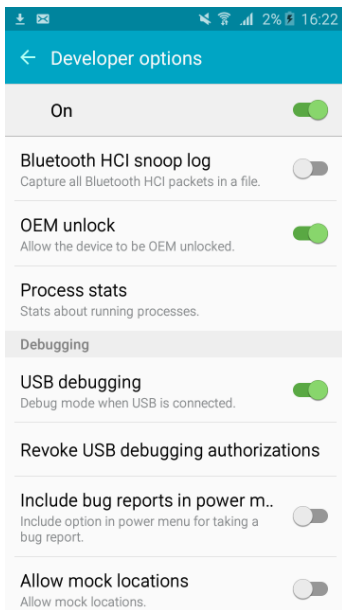
In this article, we will focus on the general process of unlocking bootloaders without specific steps on how to do so provided by the manufacturer.

 Keep in mind that unlocking the device's bootloader may void your warranty. We recommend storing all the data first since some devices wipe their data once their bootloader is unlocked.

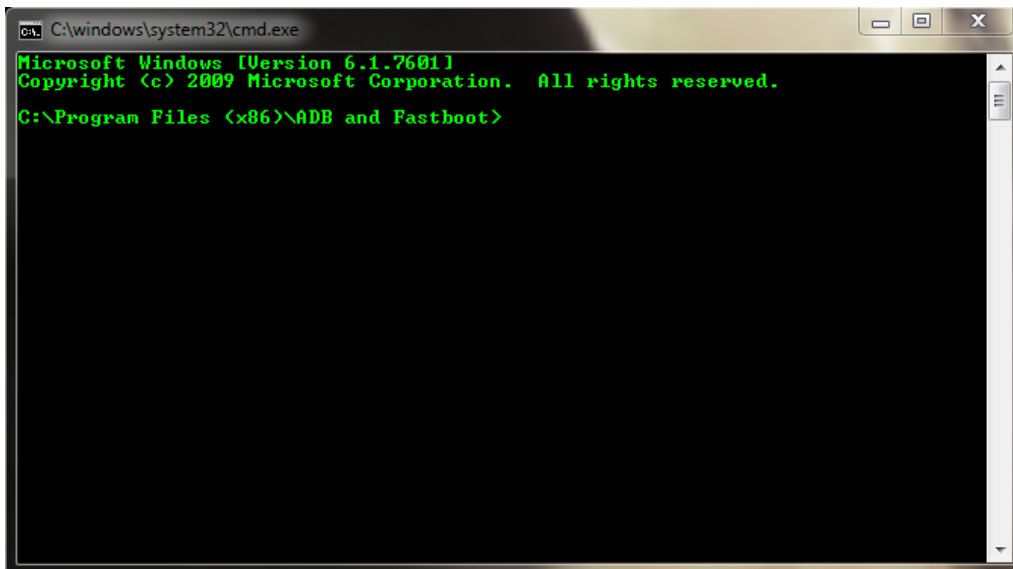
2.6.1 How to

1. Install ADB and Fastboot on your PC
(we recommend using [Minimal ADB and Fastboot](#)²⁵ as it is lightweight, comes in a simple installation package and does the job perfectly)
2. Enable developer options by navigating to Settings - About phone and clicking on "Build number" seven times.
3. Go to developer options and enable the "OEM unlock" option as well as "USB debugging"

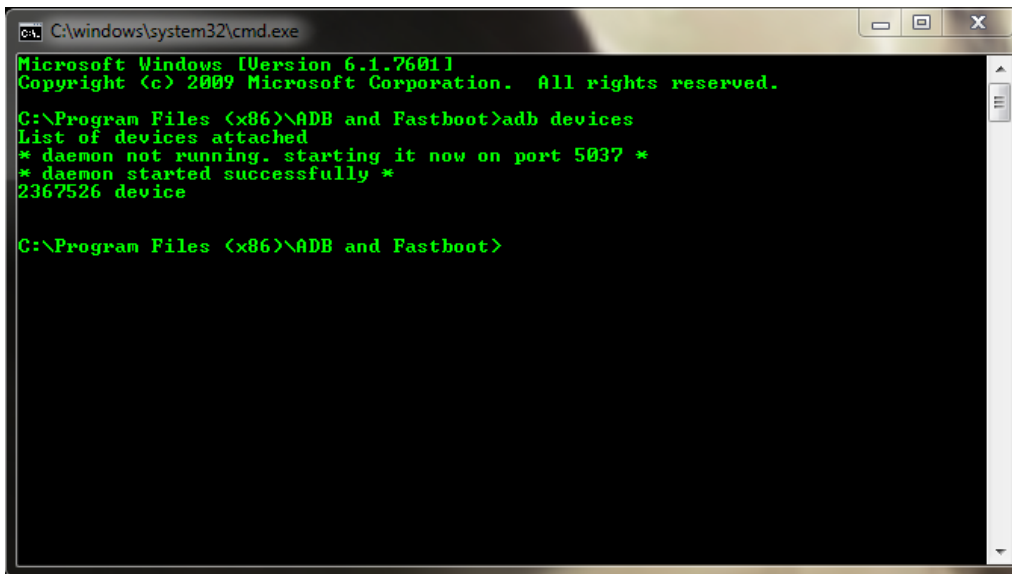
²⁵ <https://www.androidfilehost.com/?fid=746010030569952951>



4. Connect the phone to your PC and open a command-line window as an administrator from the folder where you have your ADB and Fastboot installed.



5. Type "*adb devices*" into the command line to see if your device is recognized by ADB.



```

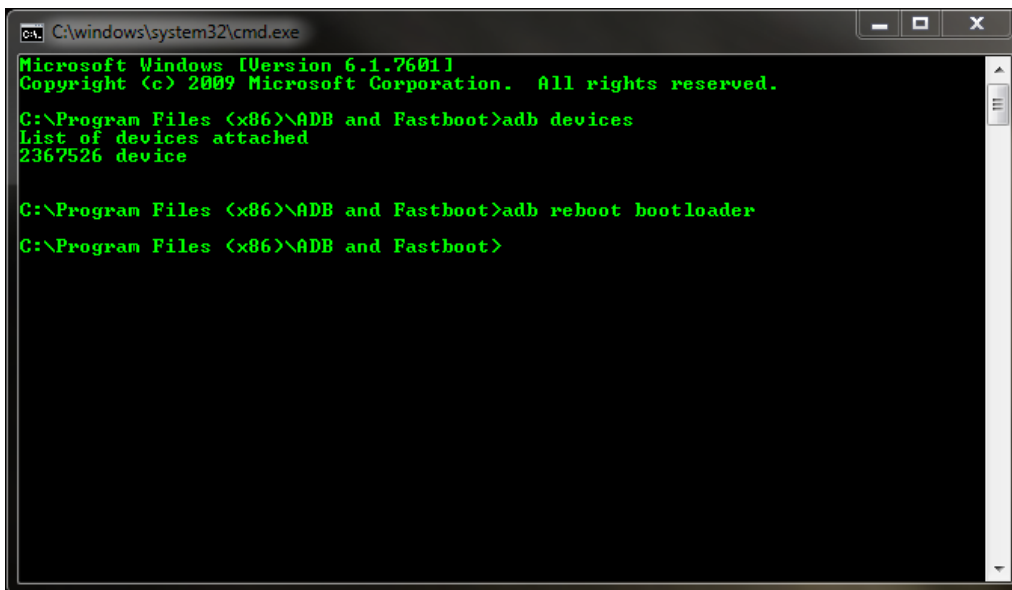
C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\ADB and Fastboot>adb devices
List of devices attached
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
2367526 device

C:\Program Files (x86)\ADB and Fastboot>

```

6. Type “adb reboot bootloader” into the command line wait until your device reboots into Fastboot mode.



```

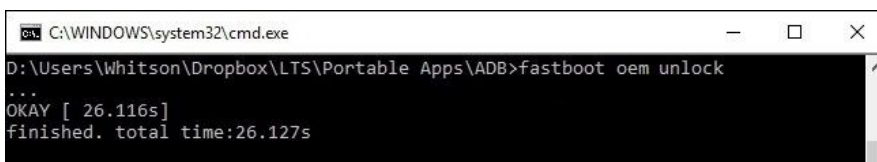
C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\ADB and Fastboot>adb devices
List of devices attached
2367526 device

C:\Program Files (x86)\ADB and Fastboot>adb reboot bootloader
C:\Program Files (x86)\ADB and Fastboot>

```

7. Once your phone reboots into fastboot mode, type the "fastboot oem unlock" command and press Enter.




```

C:\WINDOWS\system32\cmd.exe
D:\Users\Whitson\Dropbox\LTS\Portable Apps\ADB>fastboot oem unlock
...
OKAY [ 26.116s]
finished. total time:26.127s

```


8. Confirm the action on your phone's screen (if prompted).

9. After the process has finished, you can type "fastboot reboot" to boot your phone back into Android or proceed straight to flashing a custom recovery.

 Flashing custom images onto Samsung phones is done by Odin which means you only need to enable the "OEM unlock" option and proceed straight to the flashing process. Find out more in our article on [How to flash TWRP on Samsung devices \(ODIN method\)](#)(see page 86).

2.7 Security Bypassing

This new feature will help you to get a physical image of the device if you don't know the passcode, PIN or pattern lock.

 This process **does not remove** the passcode, PIN or pattern lock and device will remain locked.

Main benefits:

- Extraction from both rooted and non-rooted devices without knowing their screen lock password
- Creation of the device's physical image and reusing/reanalyzing it multiple times in the future to get better results without the need of having the device present

2.7.1 How to

1. On the main screen click on "Security bypassing".
2. Choose security bypassing approach.

By model

- Select model of the device from the list and click "Next".
- Choose an action for selected device and click "Next".
- Follow on-screen guide how to connect phone.

By chipset

- Choose chipset of the device from the list and click "Next".
- Choose an action for the selected chipset and click "Next".
- Choose unlocking variant and it will display the supported phones and click "Next".
- Follow on-screen guide how to connect phone.

Generic profile

- if you don't know the exact model or chipset of the device, you can select how do you want to connect your device such as MTK, EDL, Checkra1n, Root using Dirty COW, etc.

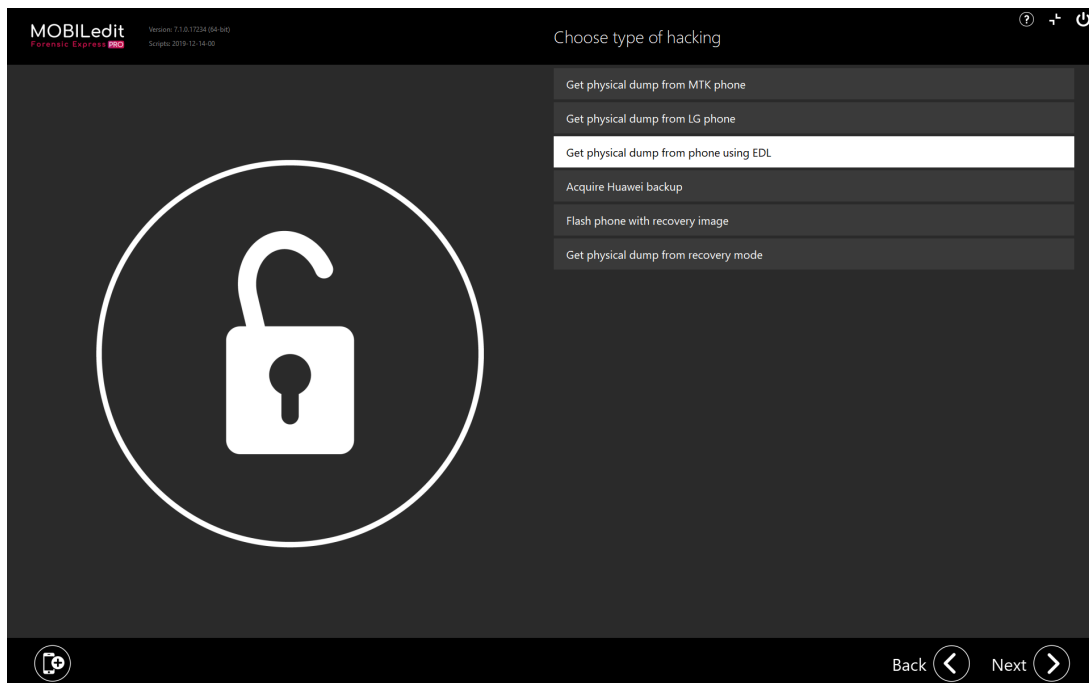
2.8 Physical Extraction - EDL Hack

- [How to](#)(see page 50)
- [List of supported devices](#)(see page 54)
- [Additional sources](#)(see page 55)

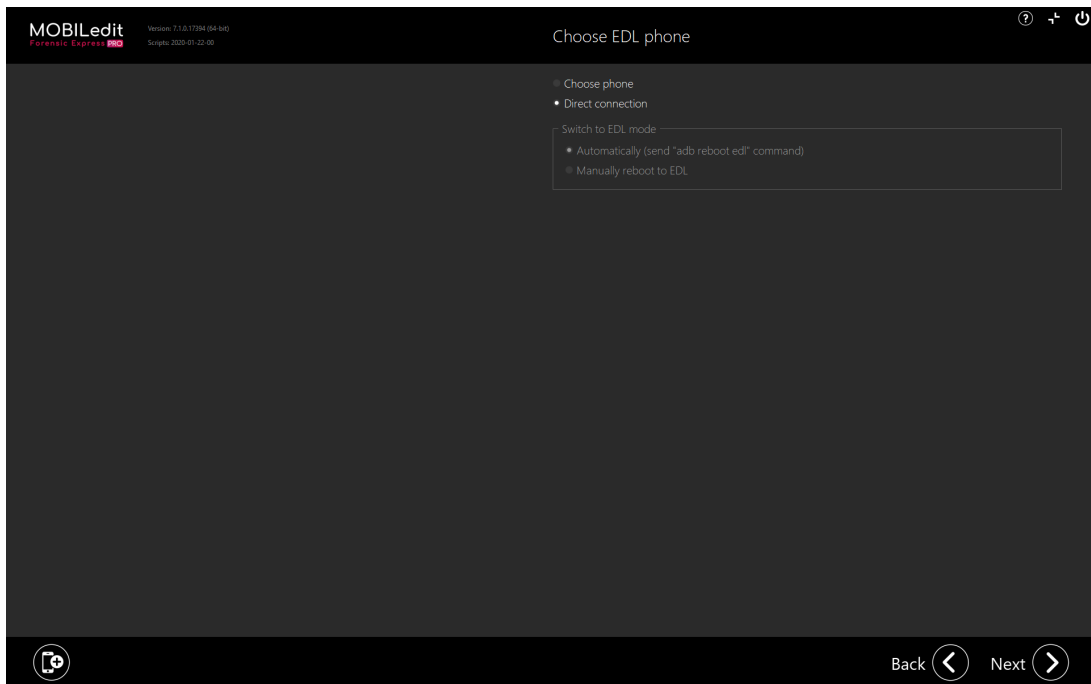
EDL Hack is a way of extracting physical images from phones with Qualcomm chipsets. This option does not require the phone to be rooted and works on most of the Qualcomm-equipped devices.

2.8.1 How to

1. On the main screen click on "Hack phone".
2. Choose "Get physical dump from the phone using EDL".



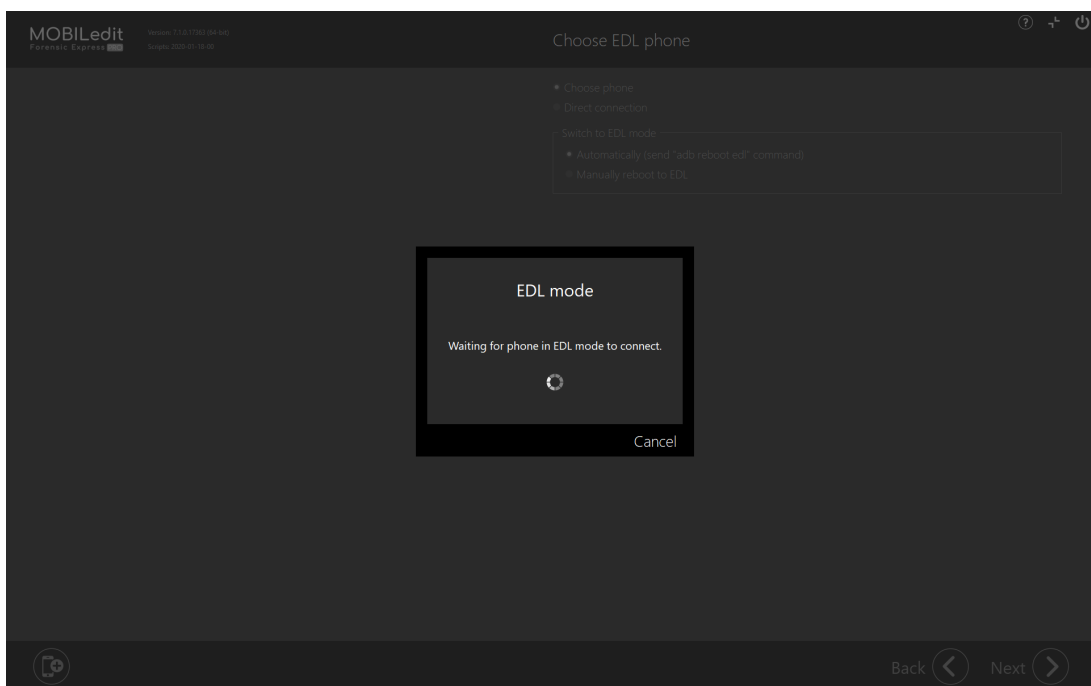
3. Select the type of connection and way how to switch the phone to EDL mode, then click "Next".



The best option is to select the connected phone with Automatically send adb command if it is supported. If you have the phone in the EDL mode already, select the direct connection.

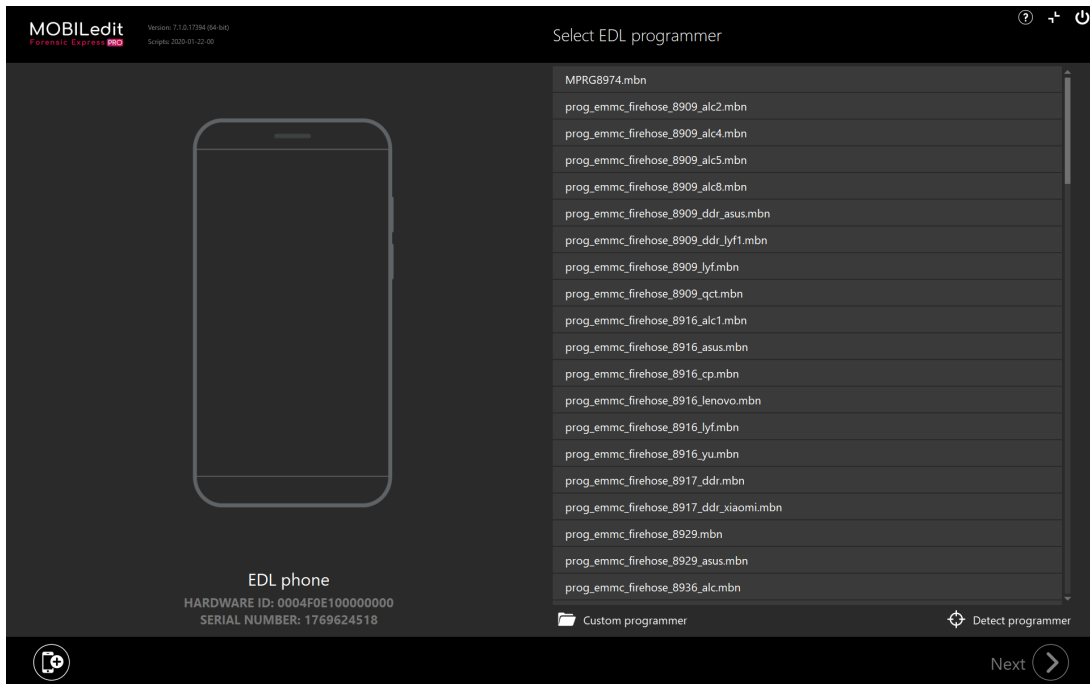
Use the "Manual reboot to EDL" option only if you have to hold the button combination to reboot the phone into EDL.

4. The screen below will display.



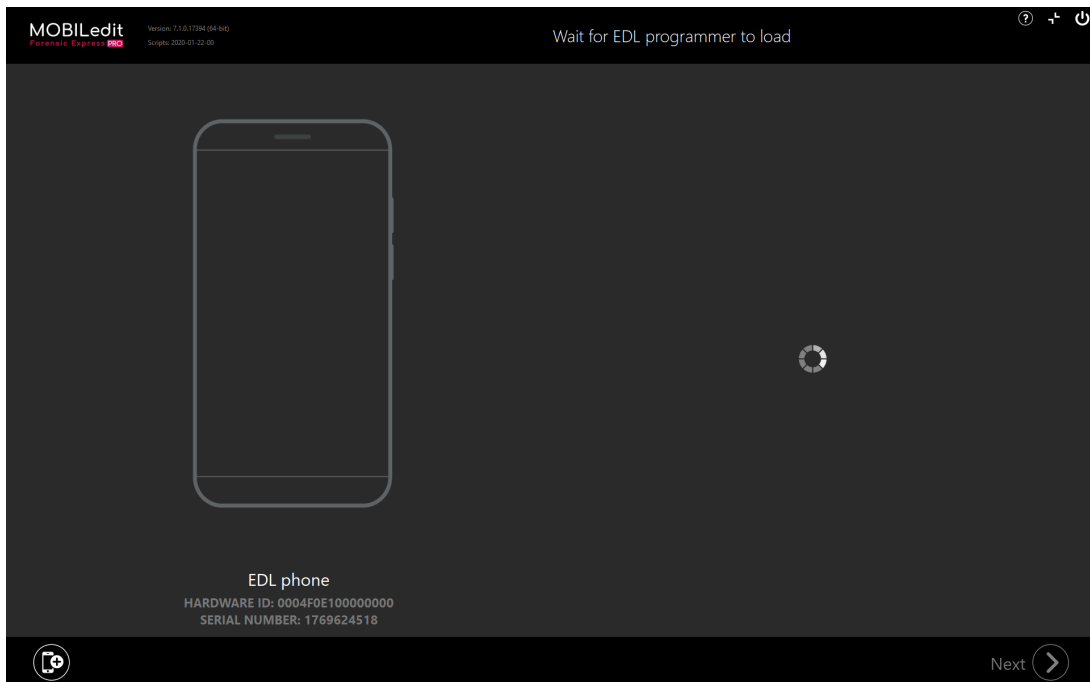
5. The screen with the list of programmers will display.

The MOBILedit Forensic Express will auto-detect the best EDL programmer for a connected phone. Now simply click "Next".



i You can use your own downloaded programmer, by clicking on "Custom programmer".

6. MOBILedit Forensic Express will continue with loading the programmer into a connected device.

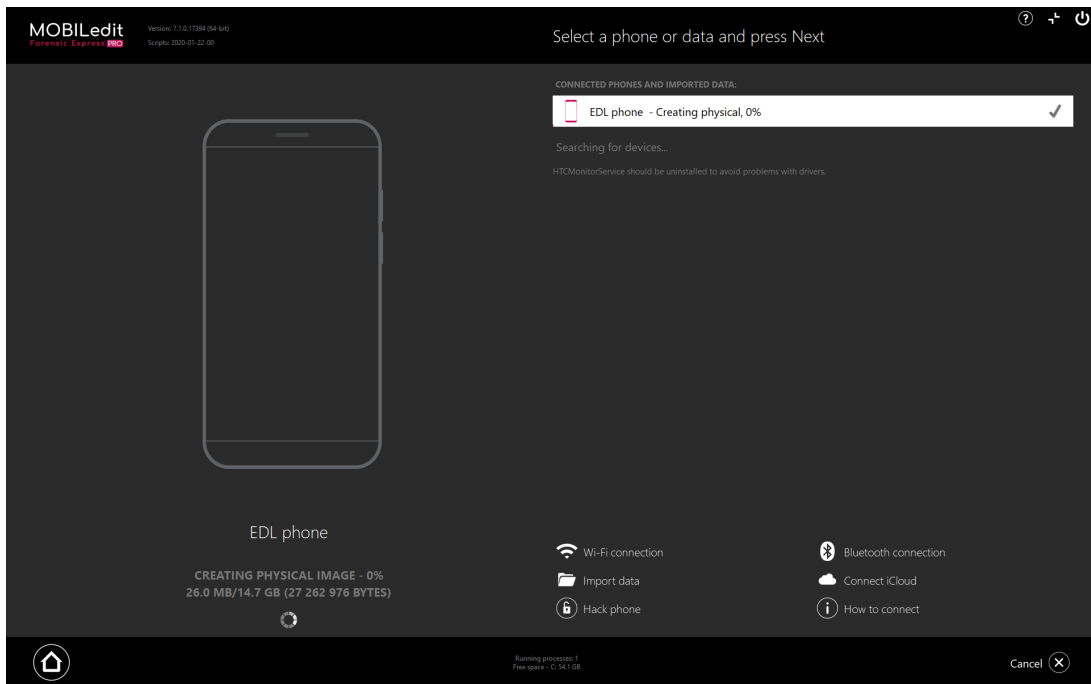


7. You will then be asked to select a location on your disk, where the physical image will be stored. Please note that the physical image is as large as the full phone’s storage.

8. The extraction will start right after.



9. You can see the physical image being extracted on this screen. This may take a while depending on the amount of data stored in your device.



After the extraction has finished, you will be able to find the IMG file at the destination location you have chosen.

2.8.2 List of supported devices

Google Nexus 5 (Button combination: Volume UP + Volume Down + Power. When display goes off, release Power. After few seconds release remaining buttons)

Google Nexus 5X (with EDL cable)

LG G3 S

LG G4

Nokia 6

Nokia 5 (with EDL cable)

Nexus 6

Nexus 6P

Moto G4 Plus

OnePlus 5

OnePlus 3T

OnePlus 3

OnePlus 2

OnePlus X

OnePlus One

ZTE Axon 7

ZUK Z1

ZUK Z2

Xiaomi Note 5A

Xiaomi Note 5 Prime

Xiaomi Note 4

Xiaomi Note 3

Xiaomi Note 2

Xiaomi Mix

Xiaomi Mix 2

Xiaomi Mi 6

Xiaomi Mi 5s

Xiaomi Mi 5s Plus

Xiaomi Mi 5x

Xiaomi Mi 5

Xiaomi Mi 3

Xiaomi Mi A1

Xiaomi Mi Max2

Xiaomi Redmi Note 3

Xiaomi Redmi Note 4G (with EDL cable)

Xiaomi Redmi 5A

Xiaomi Redmi 4A

With the release of the MIUI 8.0 was the EDL access with using the adb command "adb reboot edl" suspended.

For some cases might also work adb command "fastboot oem edl" for this you will need an unlocked bootloader.

2.8.3 Additional sources

Test points for the Xiaomi devices: <http://en.miui.com/thread-638042-1-1.html>

Additional articles about EDL and advanced methods:

<https://alephsecurity.com/2018/01/22/qualcomm-edl-1/>

<https://www.xda-developers.com/exploit-qualcomm-edl-xiaomi-oneplus-nokia/>

2.9 Physical extraction - LG Hack

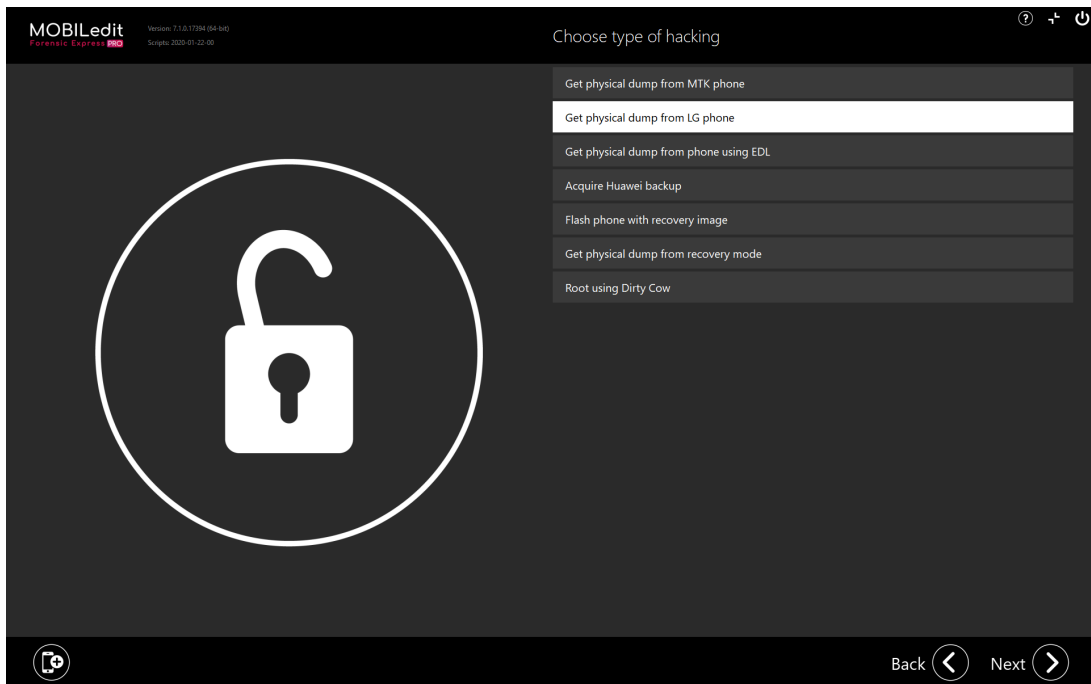
LG Hack works on all LG smartphones with the new version of LG LAF protocol (this is a service download mode similar to Samsung Odin download mode). Every LG smartphone from the year 2013 and newer should therefore support our LG hack. This exploit takes advantage of "LG Flash Mode" - used primarily for updating firmware.

With some of them - LG G4 for example - you can even browse the phone's filesystem via the "Browse Phone" option in Forensic Express.

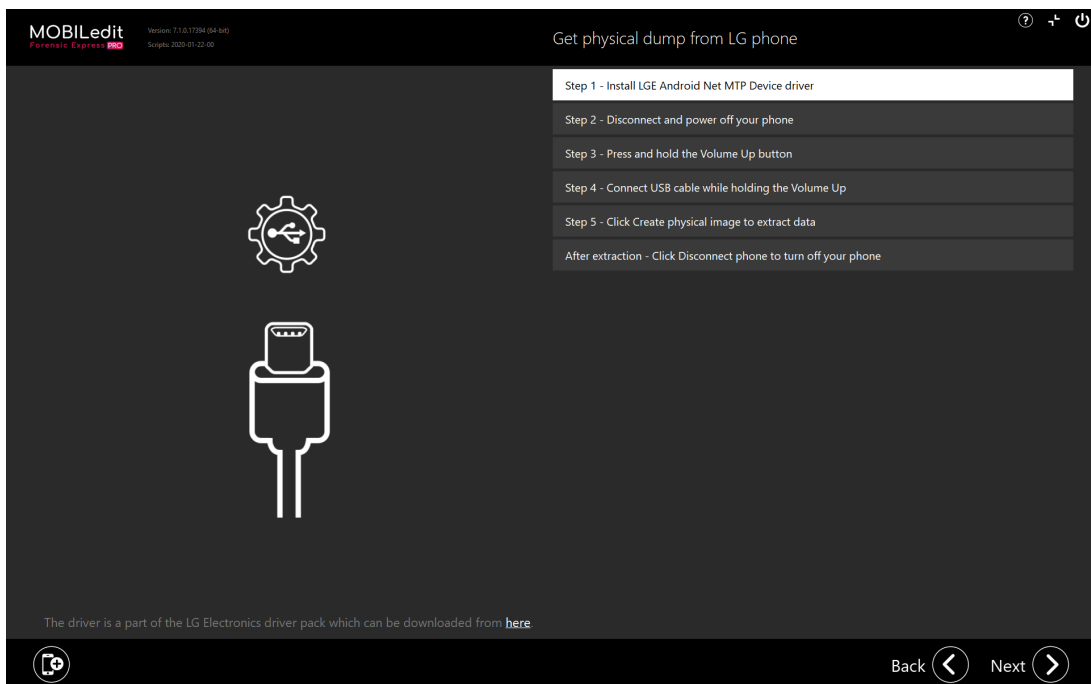
There is a way that you may be able to extract a physical image from LG phones without root access (rooting the phone).

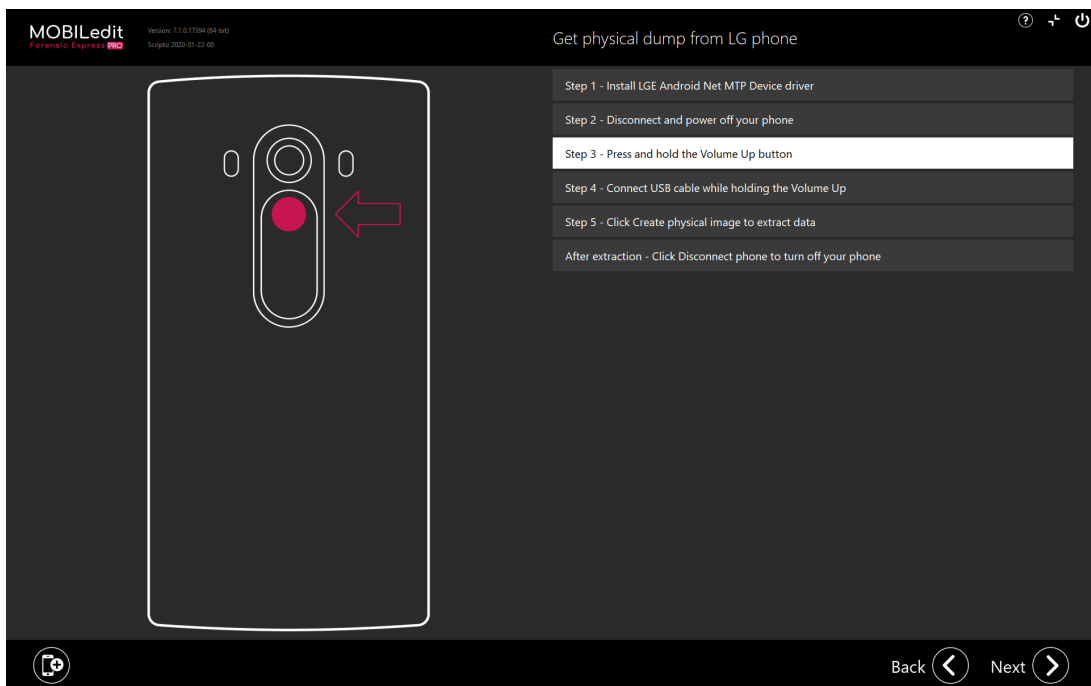
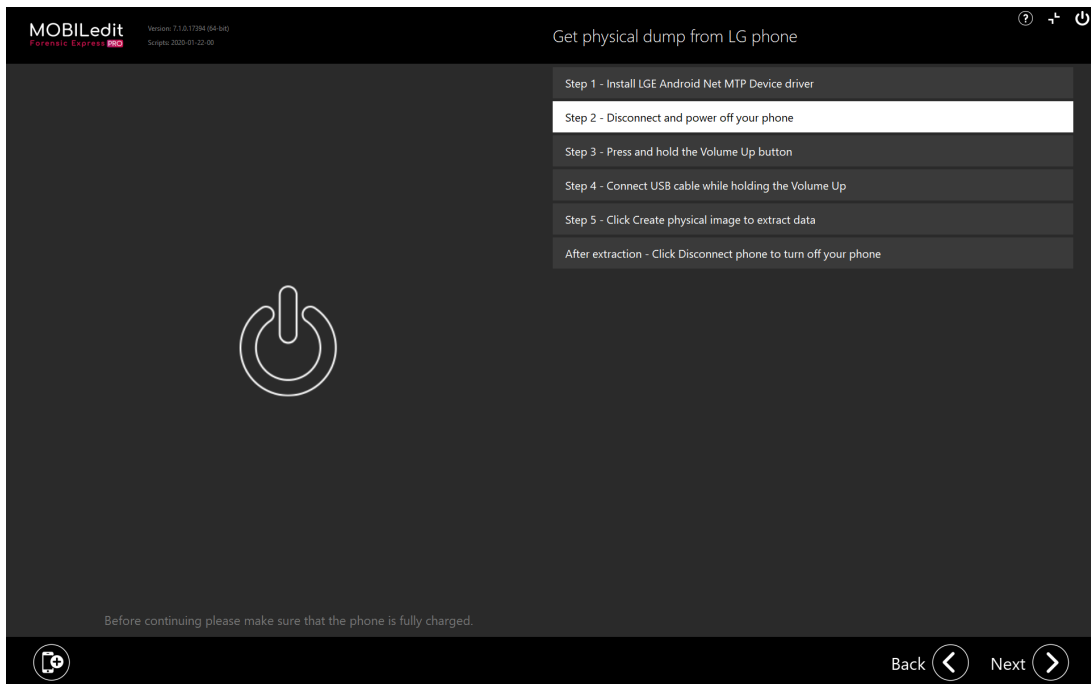
2.9.1 How to

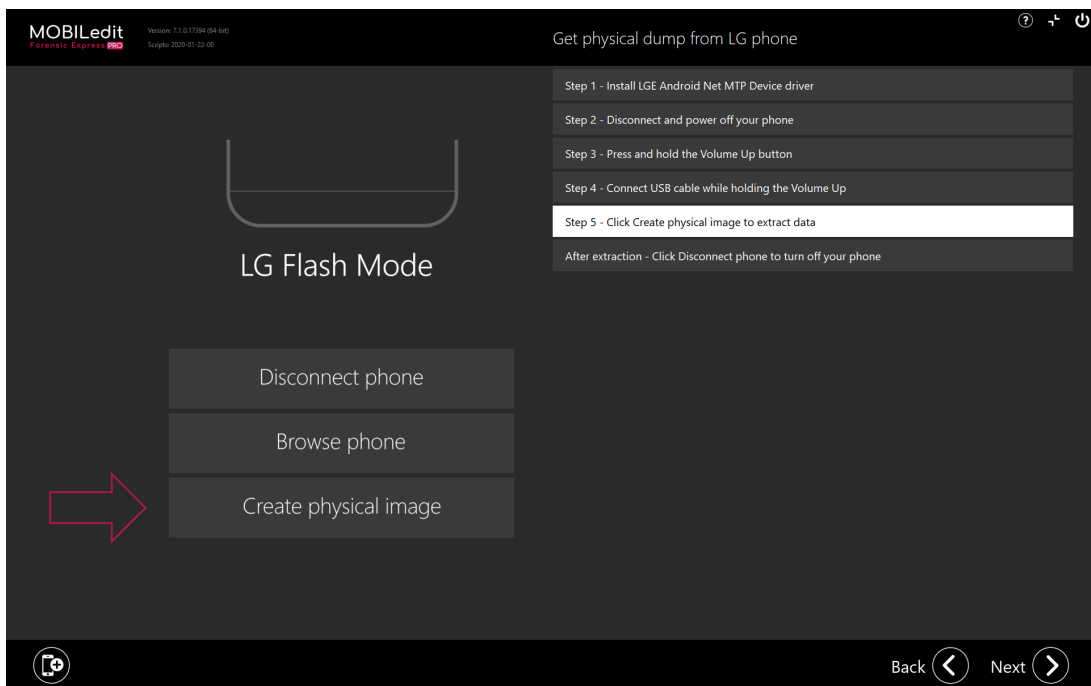
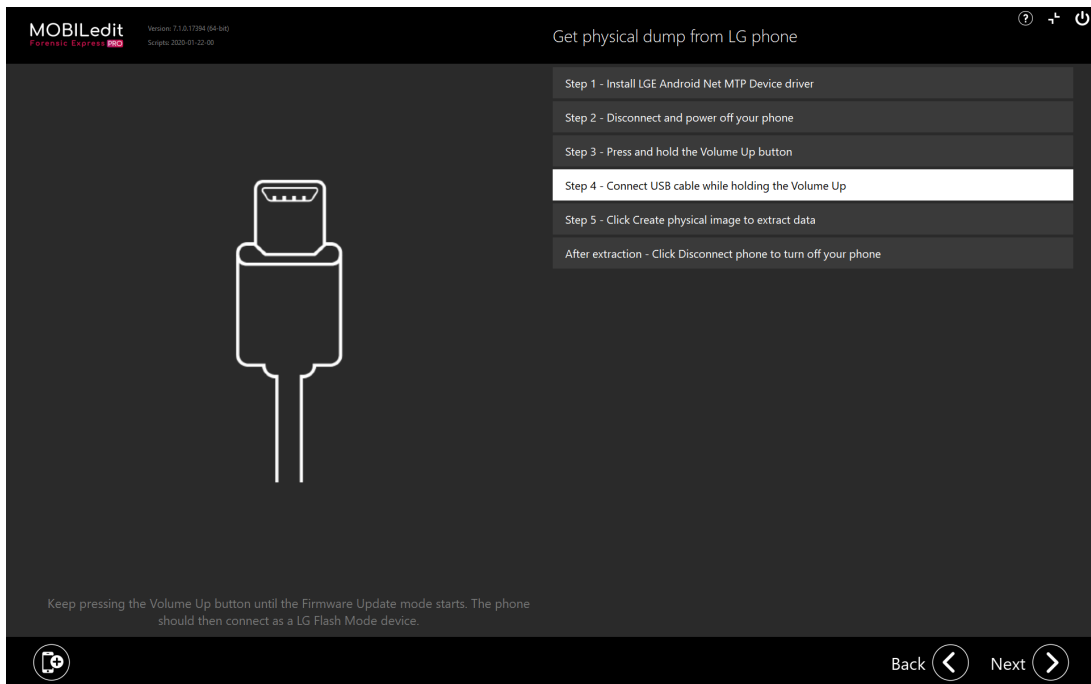
1. On the start page click on "Hack phone".
2. Select "Get physical dump from LG phone".

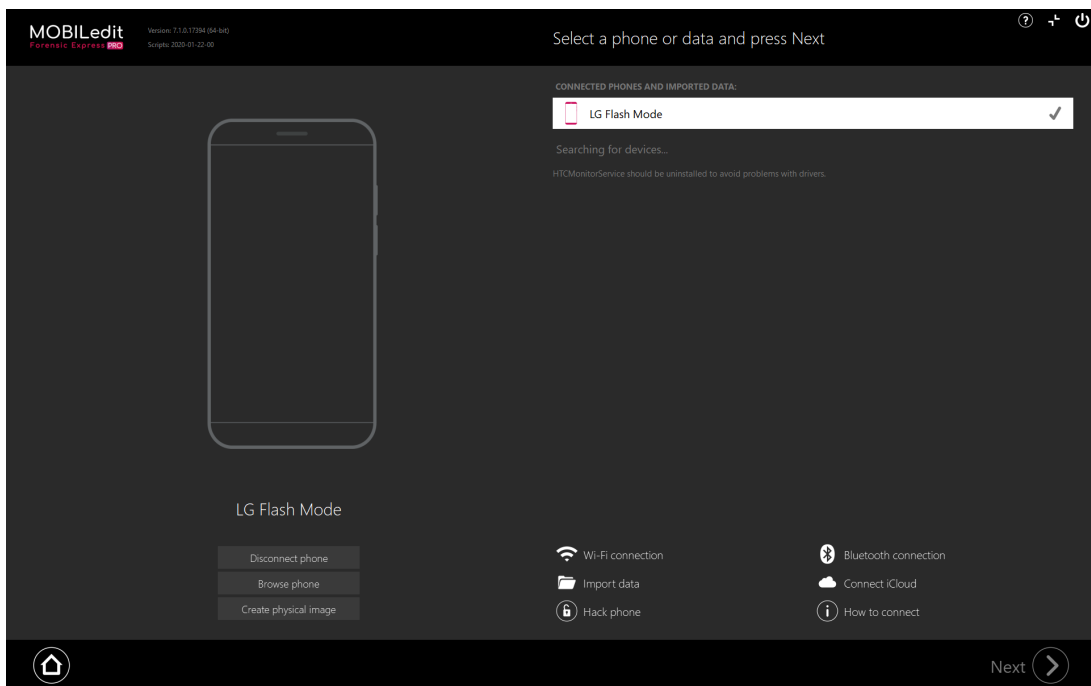
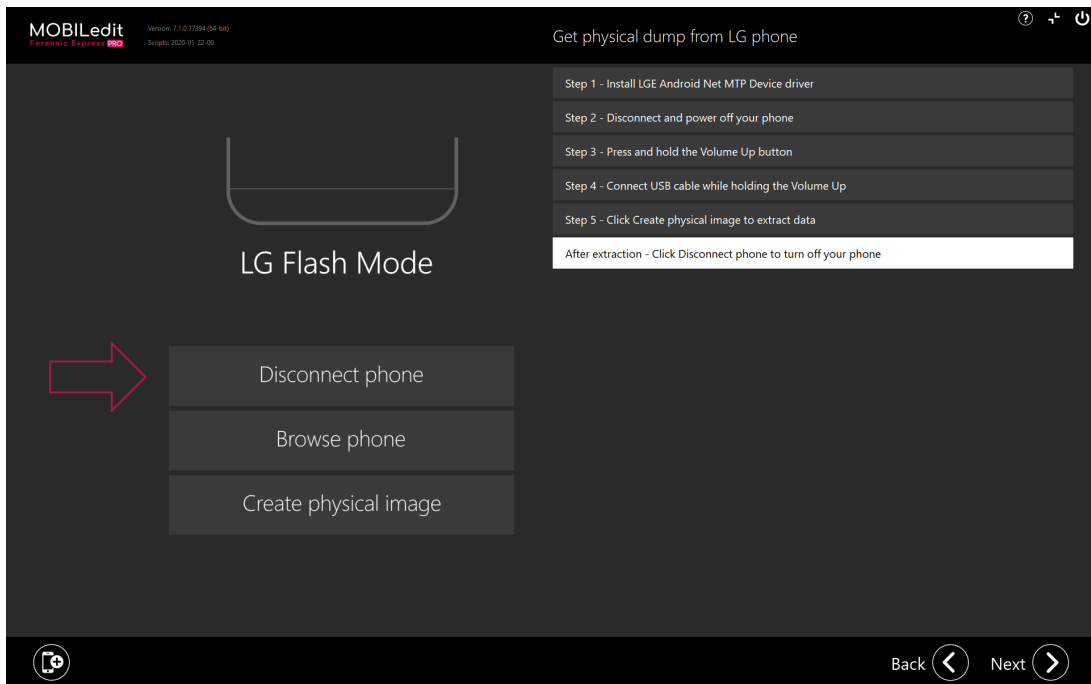


3. Follow the on-screen guide as seen in the pictures below.

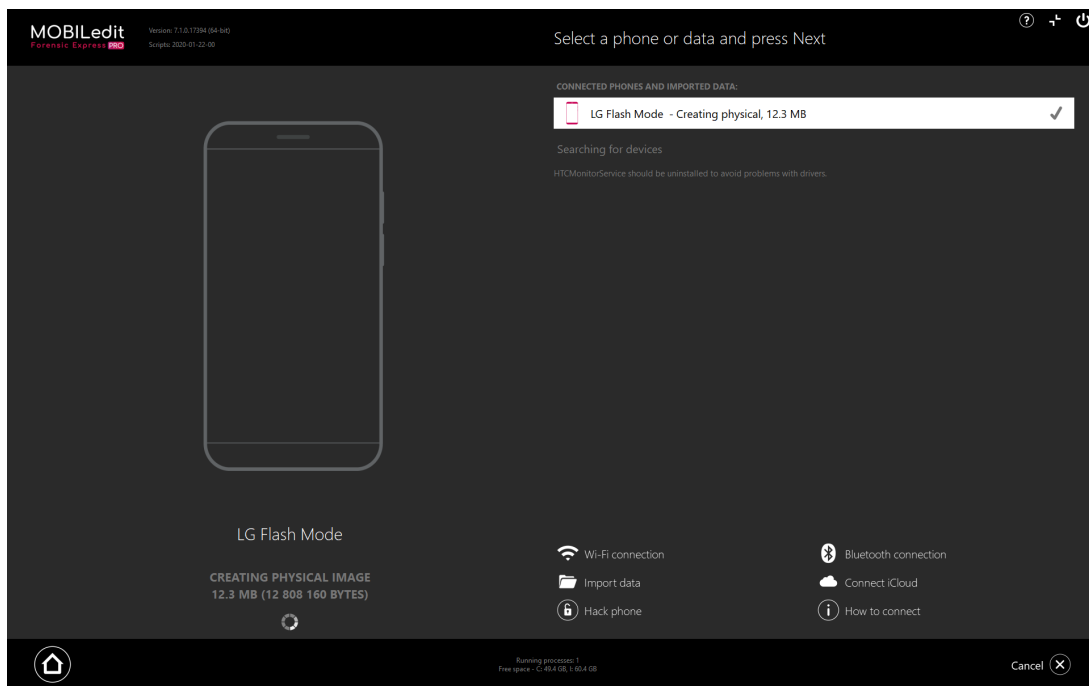








4. You can see the physical image is being extracted on the next screen. This may take a while, depending on the amount of data stored in your device.

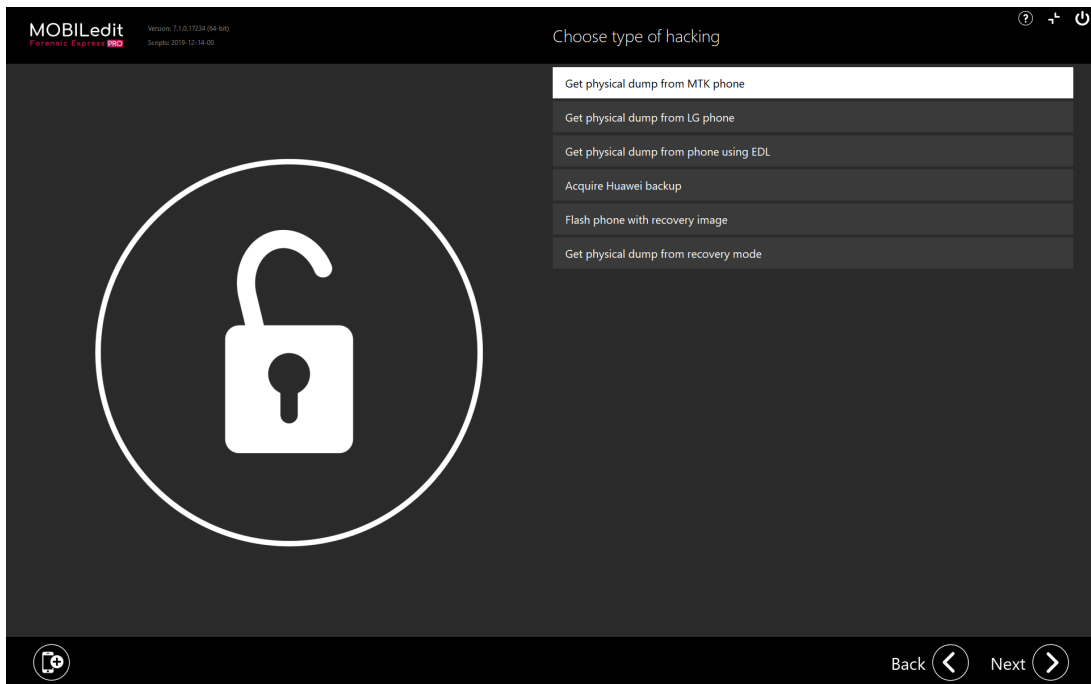


2.10 Physical Extraction - MTK Hack

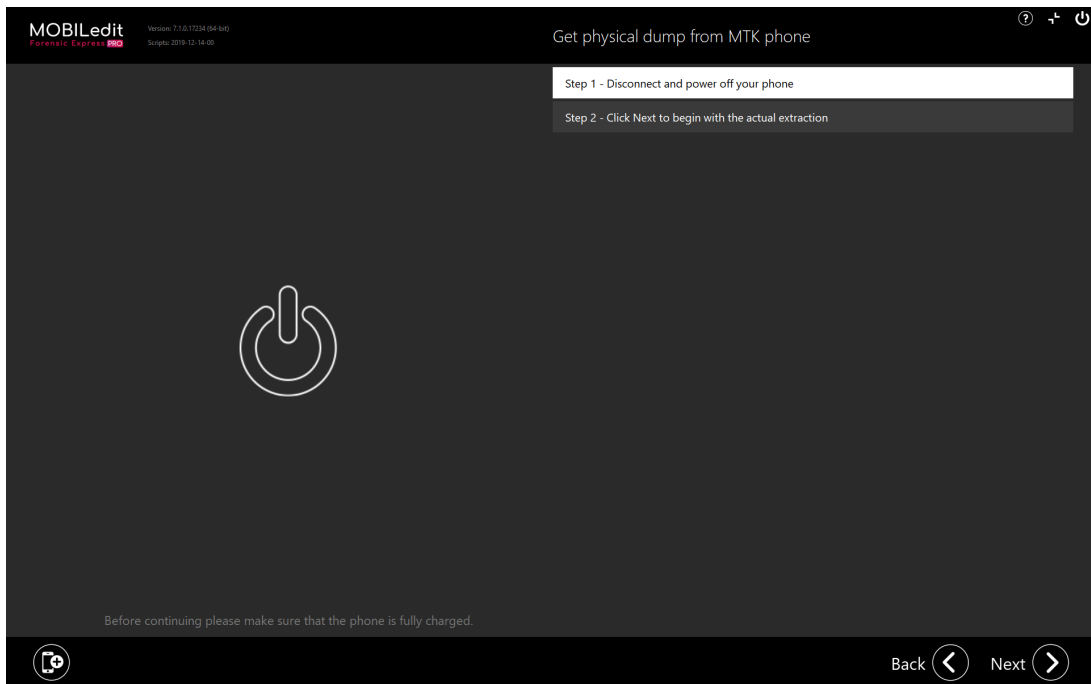
MTK Hack is a way of extracting a physical image from phones equipped with MediaTek chipsets without root access (rooting the phone). This exploit method does not work on all MTK-equipped devices, however, it is sometimes the only way of acquiring the physical image from a locked or even turned-off phone.

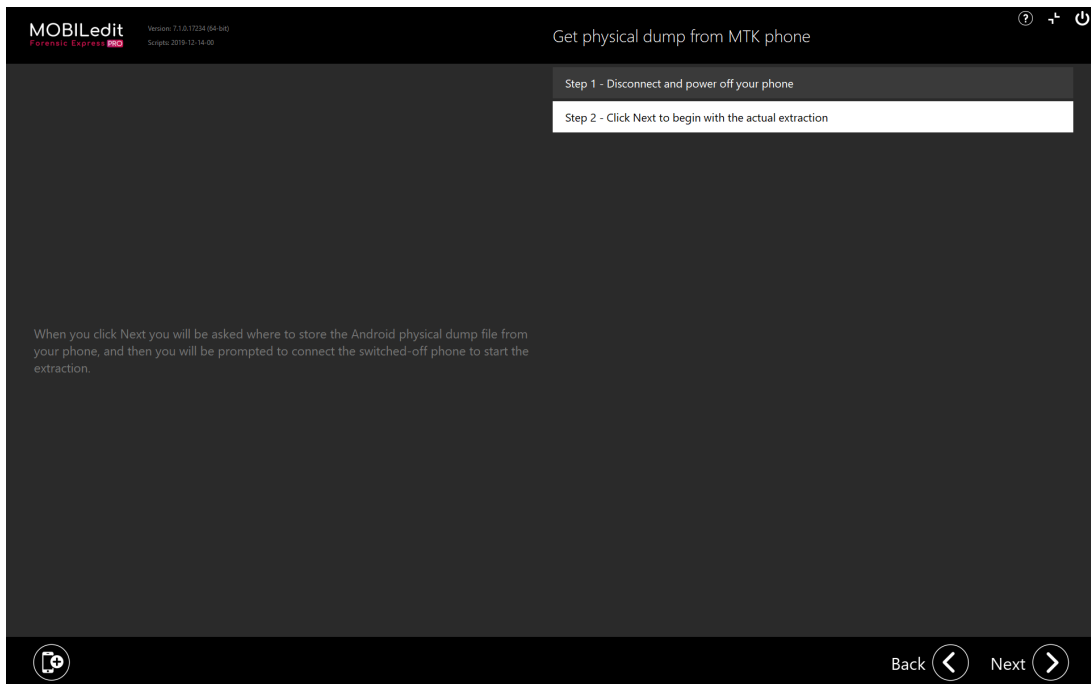
2.10.1 How to

1. On the main screen click on "Hack phone".
2. Choose "Get physical dump from MTK phone".



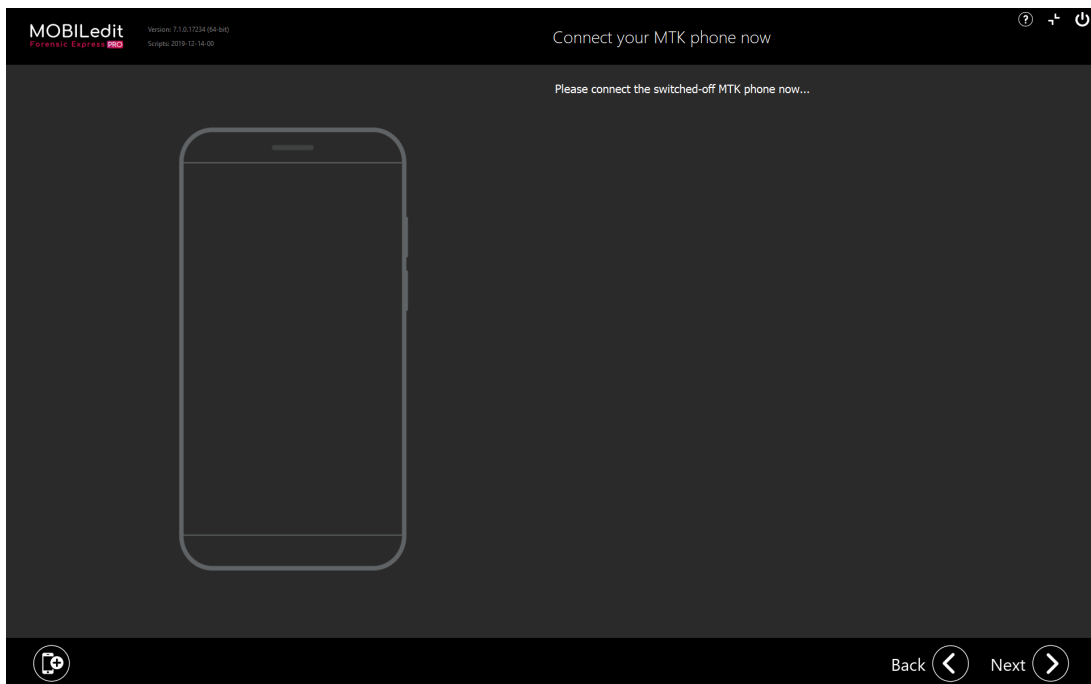
3. Click "Next" and follow the on-screen guide.



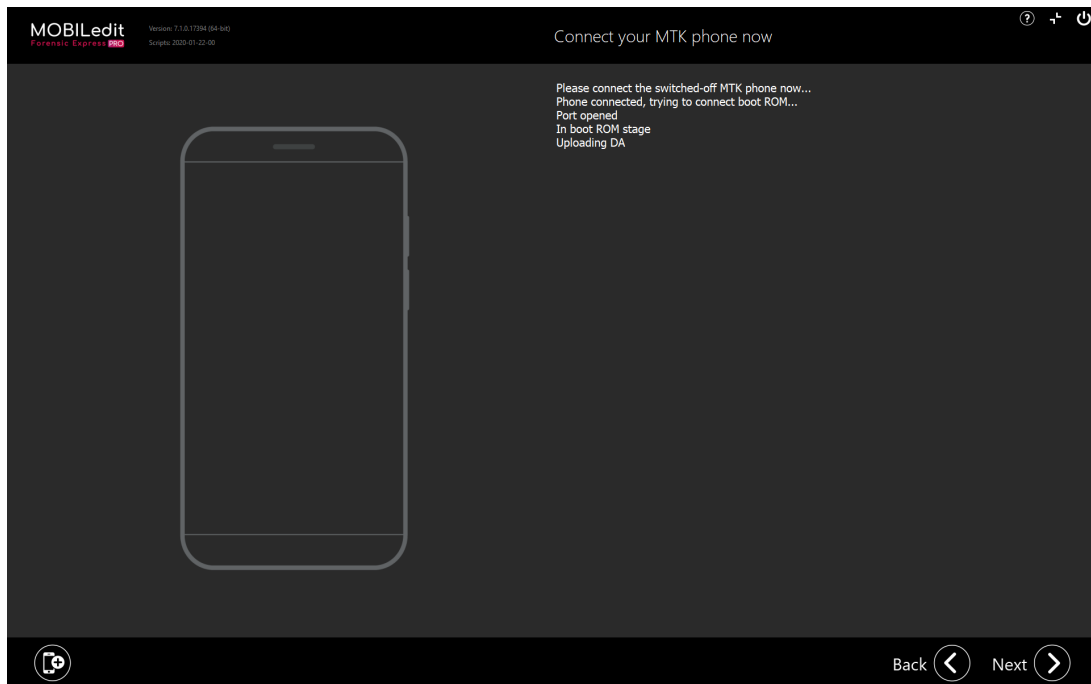


4. You will be asked to select a location on your disk, where the physical image will be stored. Please note that the physical image is as big as the full phone 's storage.

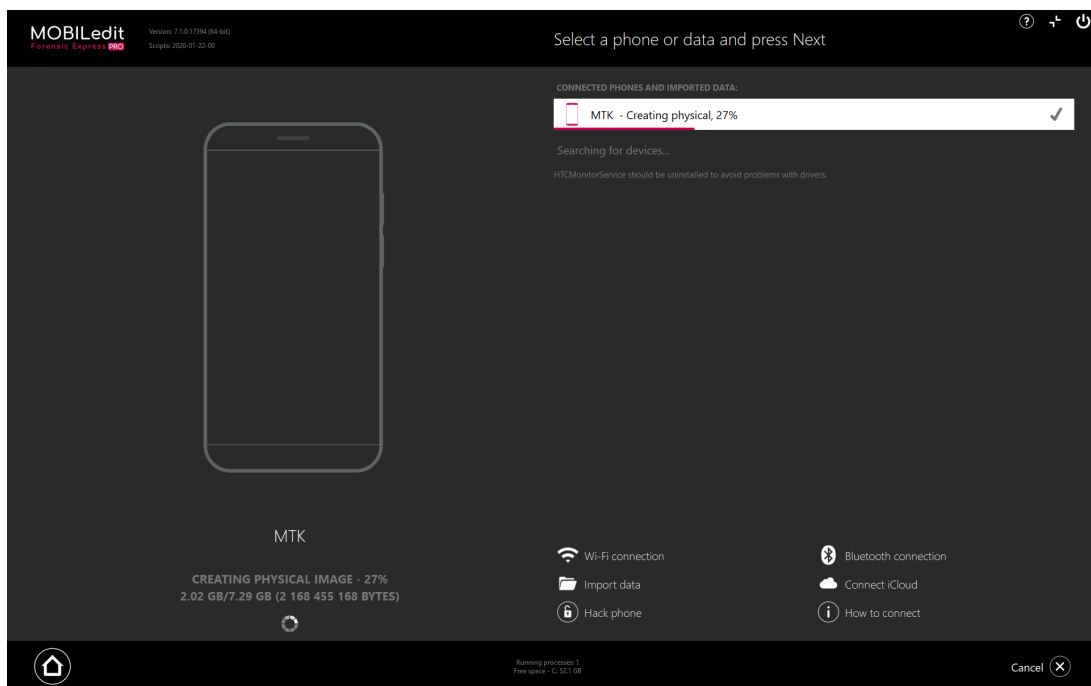
5. Then you will be asked to connect the switched-off MTK phone.



6. After the phone has been connected to a screen similar to the one below should appear; if not, the MTK hack is probably not available for your device.



7. This should only take a few seconds and in some cases 1-2 minutes; the extraction will start right after.



8. You can see the physical image being extracted on this screen. This may take a while depending on the amount of data stored in your device.

9. After the extraction has finished, you will be able to find the IMG file at the destination location you have chosen.

i This method does not work for most MTK devices with locked bootloaders. In order to use MTK hack on such devices, the bootloader has to be unlocked first.

2.11 KaiOS Physical analysis

- Physical extraction(see page 64)
 - EDL Hack(see page 65)
 - MTK Hack(see page 65)
- Example of connecting a specific device in EDL mode:(see page 66)

KaiOS is a Linux-based operating system designed for feature phones and is completely supported by MOBILedit on a physical level. The physical analysis provides you with all the important data such as contacts, messages, organizer, browser history, browser bookmarks, calls, alarms, notes, WhatsApp, and more.

KaiOS operating system is very popular among feature phones such as Alcatel, Nokia, Accent, Telma and many other local brands. Its user interface is specifically designed for non-touchscreen phones with keypads; however, it still allows its users to use modern apps such as Facebook, YouTube, WhatsApp, Twitter, etc. KaiOS is very popular in Asia, Africa, Latin America, and it is the second most used OS in India.

To import the physical image, simply click on [Import data](#)(see page 237).

i It is not always possible to load all of the partitions from the physical image, which is standard behaviour in case some of the partitions do not contain any useful user data or if it is encrypted.



2.11.1 Physical extraction

Physical image from KaiOS devices can be extracted using the following methods:

2.11.1.1 EDL Hack

The EDL hack is a way of extracting physical images from phones with Qualcomm chipsets without root access (rooting the phone). You can find a guide on how to proceed with the EDL hack [here](#)(see page 50).

2.11.1.2 MTK Hack

MTK hack enables you to extract physical image from phones with MediaTek chipsets without root access (rooting the phone). This exploit method does not work on all MTK-equipped devices, but sometimes it is the only way of acquiring the physical image because the phone does not have to be booted up or unlocked in order to perform this operation; which means you can try even if the phone is off or locked. You can find a guide on how to proceed with the MTK hack [here](#)(see page 60).

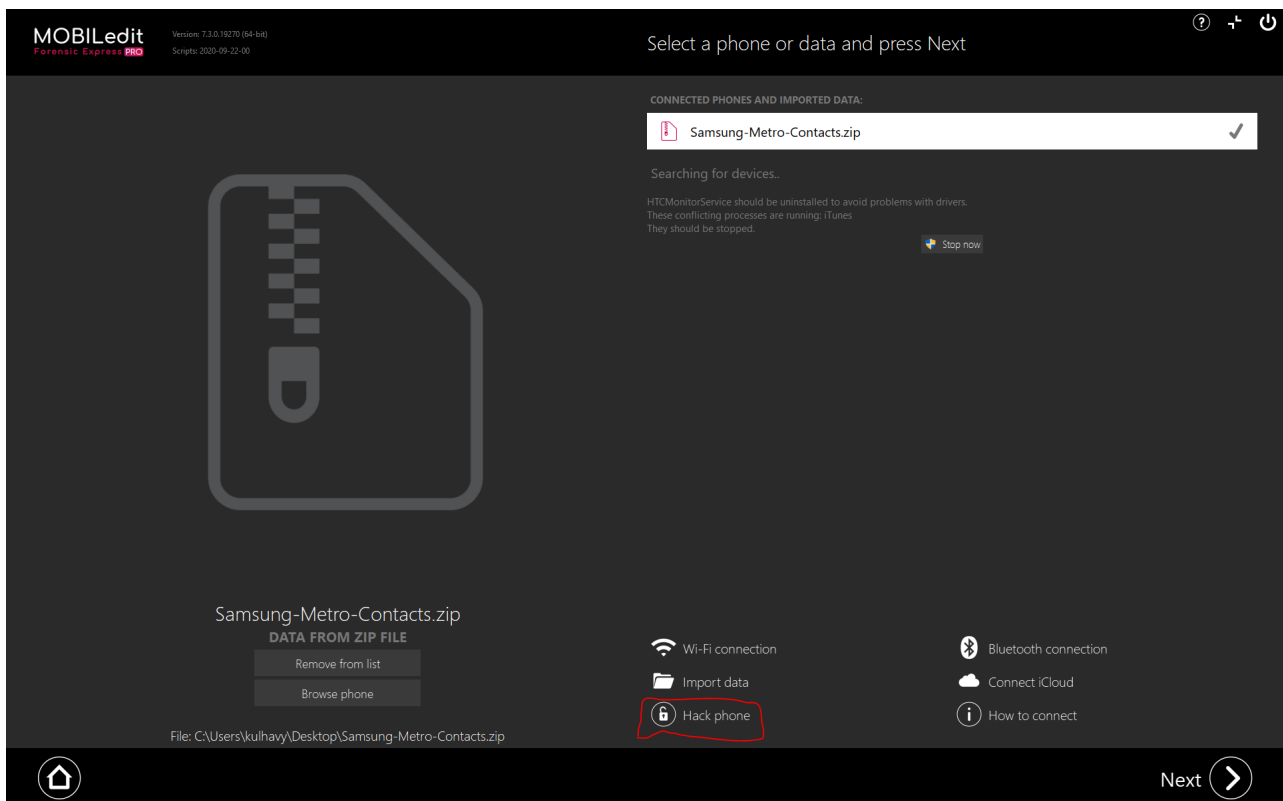
 Examples of supported **KaiOS** devices:

- Jio JioPhone 2
- JioPhone F30C
- JioPhone F101K
- JioPhone F120B
- JioPhone F220B
- JioPhone F211S
- JioPhone F250Y
- JioPhone F271I
- JioPhone F10Q
- JioPhone F41T
- JioPhone F50Y
- JioPhone F61F
- JioPhone F81E
- JioPhone F90M
- JioPhone LF-2401
- JioPhone LF-2402
- JioPhone LF-2403
- JioPhone LF-2403N
- JioPhone F300B
- Nokia 3310
- Nokia 105
- Nokia 216
- Nokia 220
- Nokia 230
- Nokia 8110
- Nokia 2720 Flip
- Nokia 800 Tough
- Cat B35
- Alcatel Go Flip 3
- Alcatel Cingular Flip 2
- Positivo P70S
- MTN Smart
- Nubia 50K
- Jazz Digjt 4G
- Orange Sanza 2
- Kitochi 4G Smart

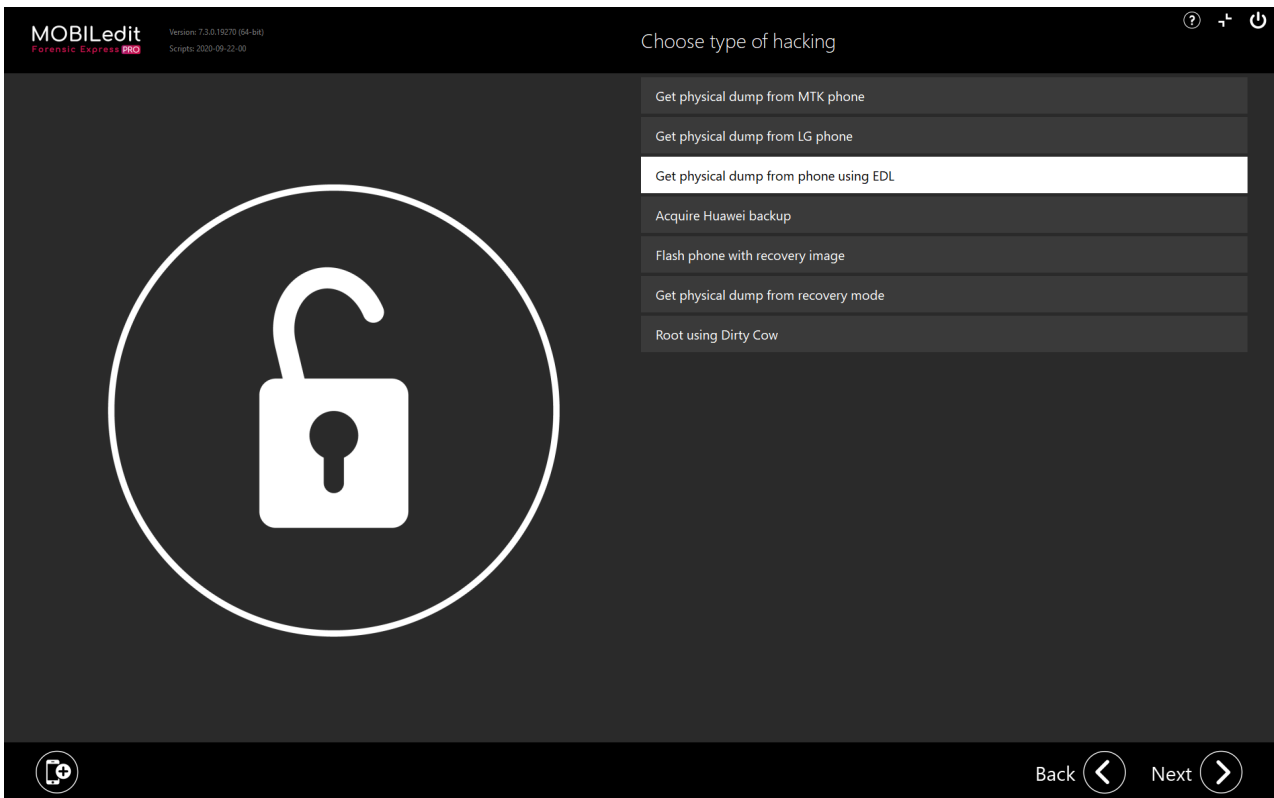
- Orange Sanza XL
- Wi-Kif 4G +
- Vodacom Smart Kitochi (Vida)
- Hape Online
- Afriphone
- QMobile 4G Plus
- Vodacom Smart Kitochi (Azumi)
- Sigma X-Style S3500 sKai
- Zoey Smart
- Energy E241
- Doro 7050
- and more!

2.11.2 Example of connecting a specific device in EDL mode:

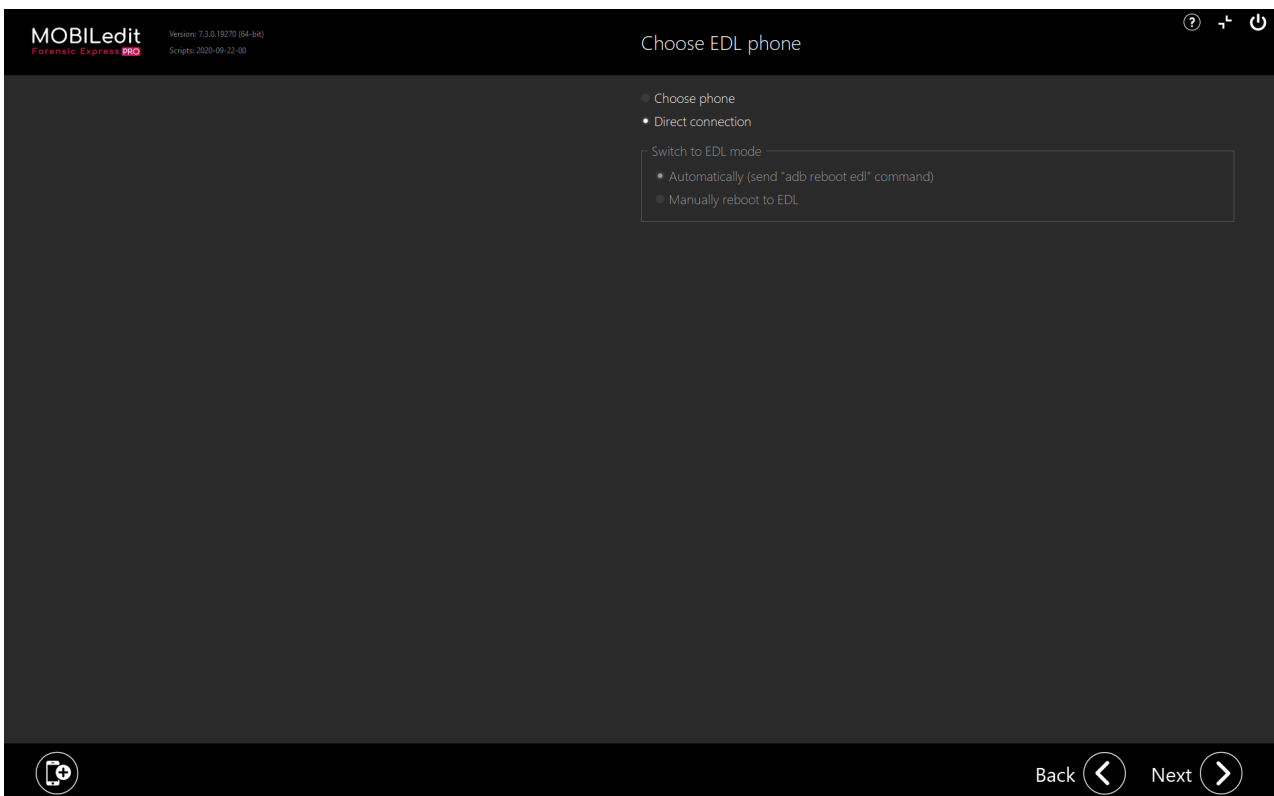
1. Click on the "Hack phone" option.



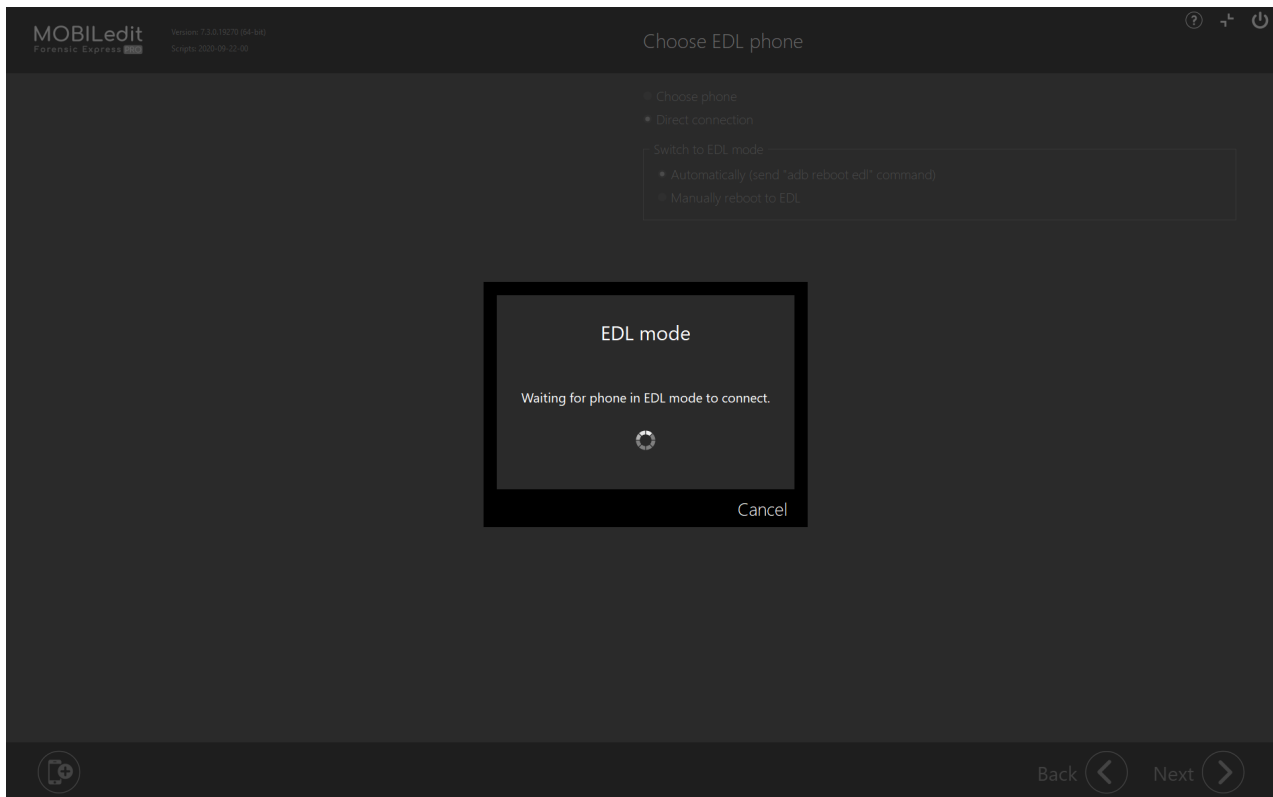
2. Choose the "get physical dump from phone using EDL".



3. Pick the "Direct connection".



4. Click "next".



5. Keep it like that and take the phone. Take out the battery and put it back again to make sure the phone is restarted. **Do not turn it on.**

6. Press and HOLD the * button, and connect the device to the PC. (while still holding the * button), wait for the vibration. After the vibration, release the * button and your device should be connected.

i Sometimes you have to repeat the procedure if you are not successful on the first try, just make sure you take out and in the battery for each try.

2.12 How to root an Android phone?

- [What does rooting an Android actually mean?\(see page 69\)](#)
- [How do I root an Android phone?\(see page 69\)](#)

There are countless ways in which you can use root access on your Android smartphone, but in this article, we will focus on those used in conjunction with MOBILedit Forensic Express.

Our software uses root access to obtain as much data as possible (including deleted data).

It's also crucial to have a rooted phone in order to perform application analysis and physical dump of any Android phone using MOBILedit Forensic Express or any other software.

2.12.1 What does rooting an Android actually mean?

It is important to realize that Android runs on Linux kernel, which means it is a Linux-based operating system with a few major changes to make it suitable for touchscreens.

When you root your Android phone, you are essentially using an exploit to unlock one of Linux's basic functionalities - access to the core of the operating system, which is normally only accessible by phone manufacturers.

Once you gain root access you can use it to manipulate, change, remove, or add anything inside your Android phone.


2.12.2 How do I root an Android phone?

Most Android devices should be able to be rooted. However, the process of rooting is specific to each phone model, version of Android, and build number. You will always need to find the right tool depending on your phone model.


You can root a majority of **old school Android phones** using an app called **KingoRoot**²⁶, if for some reason this method doesn't work for you (locked bootloader, Knox, etc.) or you have a **modern Android device** then you may be able to find help on **XDA Developers**²⁷, which is a website with a large active user community dedicated entirely to Android smartphones.

 You can also check other techniques we offer in getting more information from the device [here](#)(see page 396).

Please note that sometimes it is necessary to unlock your phone's bootloader in order to root it. You can either find a step-by-step tutorial on how to unlock the bootloader on your phone manufacturer's webpage or you can use a technique described on our user-guide [here](#)(see page 46).

 Some devices tend to wipe all the data once the bootloader is unlocked. We recommend storing the phone's data before rooting it.

Once rooting has been completed successfully the phone is then switched to so-called "rooted mode". In this mode, you will be able to extract and analyze the deleted data, create physical images, access more data from applications, and have more available data for extraction in general.

 Rooting your phone may void the manufacturer's warranty and could cause security risks. Please take this into consideration before performing this process.
Rooting a Samsung device can trip the Knox Warranty void flag which will make the data stored in Knox permanently inaccessible.

²⁶ <https://www.kingoapp.com/>

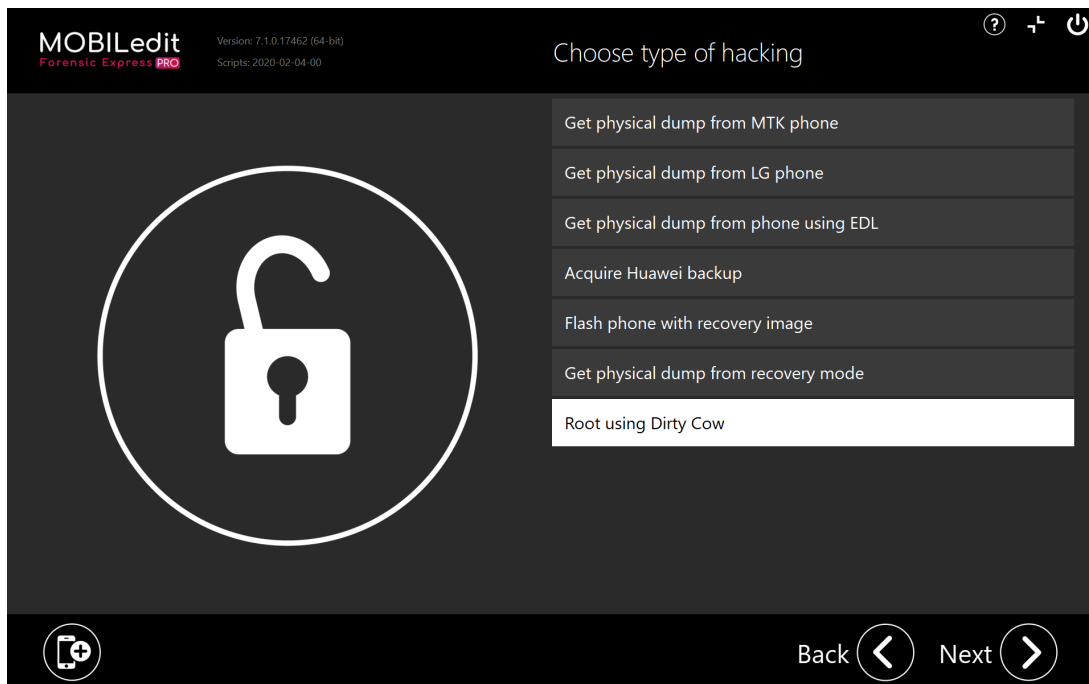
²⁷ <http://xda-developers.com/>

2.13 Dirty COW

Dirty COW is a computer security vulnerability that affected all Linux-based operating systems, including Android devices, that used older versions of the Linux kernel created before 2018. If you have an Android device with a version under 7, you can try to root your device using the Dirty cow exploit.

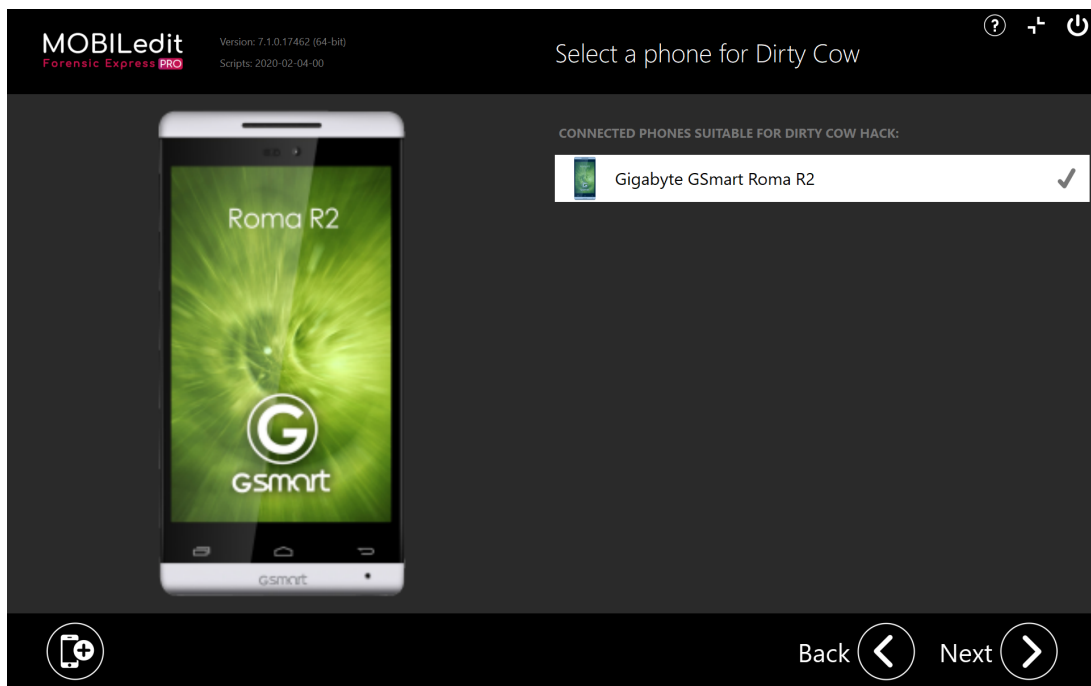
2.13.1 How to

1. Click on "Hack phone" and choose "Root using Dirty Cow".

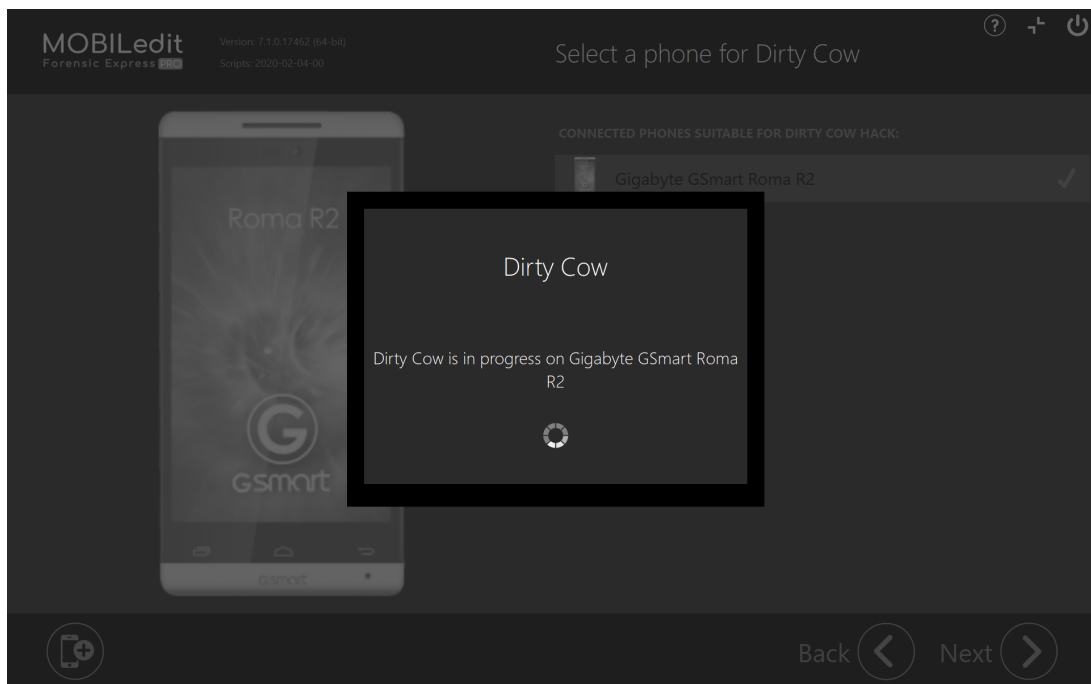


2. Select the phone that you want to be rooted.


i MOBILedit Forensic Express automatically detects what phones can be rooted so if your device does not show in this category then it cannot be exploited.

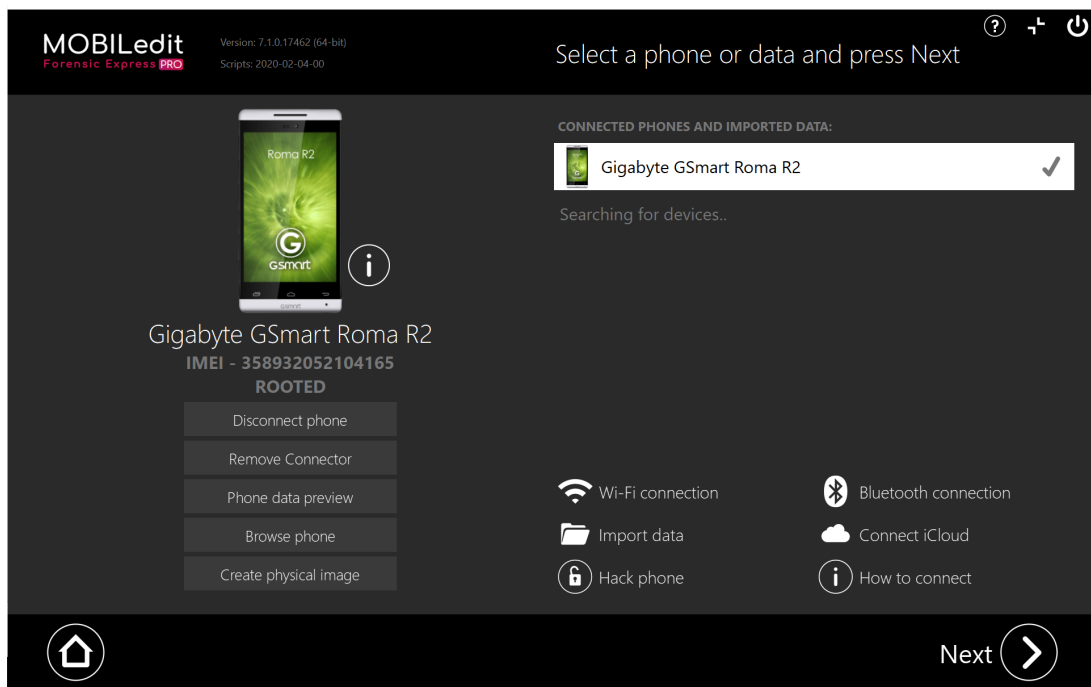


3. Click on "Next" and proceed with the exploit.

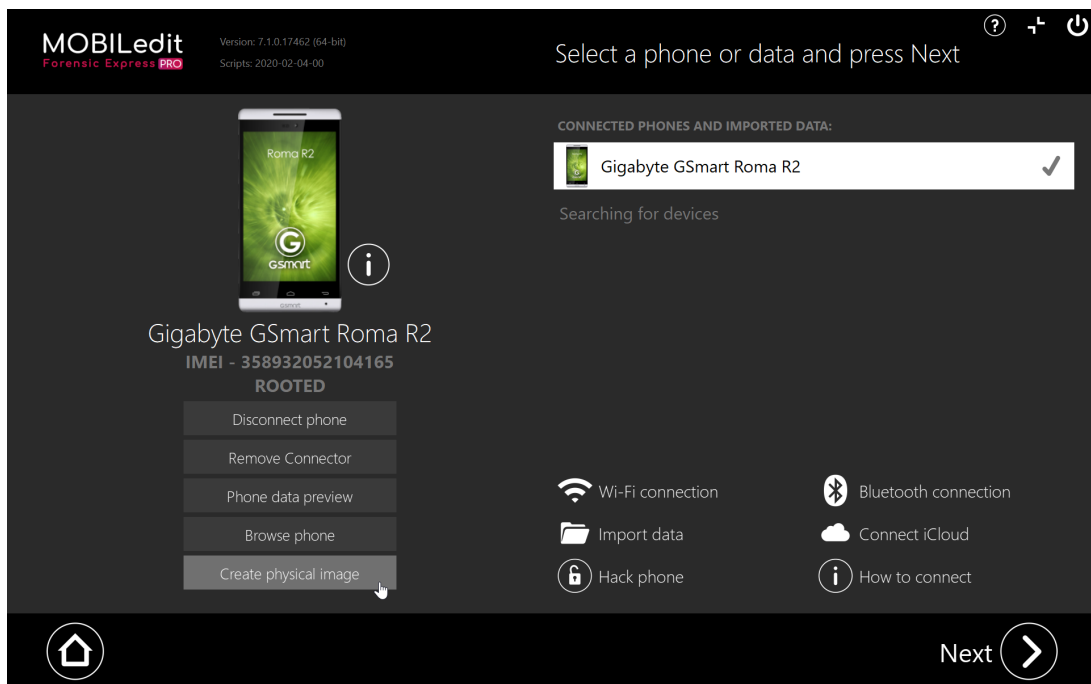


4. When everything is finished you should see a text ROOTED below the IMEI - as you can see in the screenshot below.

 If nothing shows up after the exploit, then reconnect your device



5. Click on "Create physical image".




6. When your physical image is created click on "Import data" and choose "Physical image".

7. Select the image you have just created and proceed like you would with a normal extraction.

i Dirty COW is a temporary root and will be gone once you will restart your device.

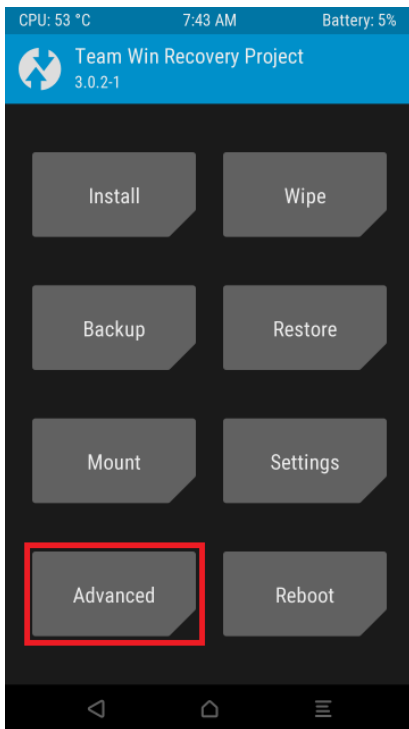
2.14 Use TWRP to bypass Android lockscreen

TWRP custom recovery makes it quite easy to remove any kind of lock (except for fingerprint) from your Android device.

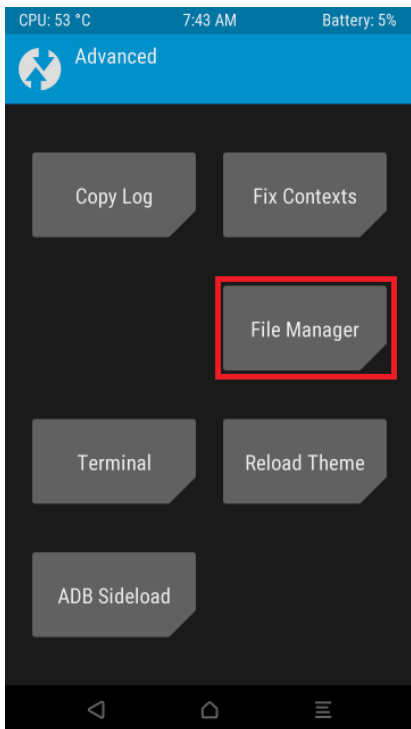
 To read more about TWRP go to “[Flash phone with recovery image - TWRP](#)(see page 78)”.

2.14.1 How to

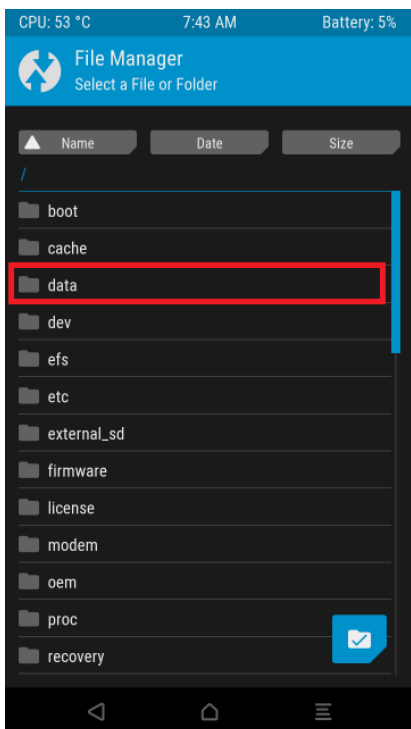
1. Reboot your phone into TWRP and click the "Advanced" button.

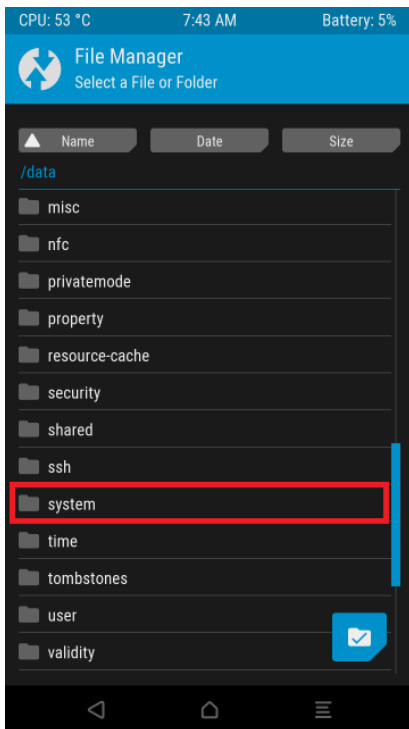


2. In the advanced options, click on "File Manager".

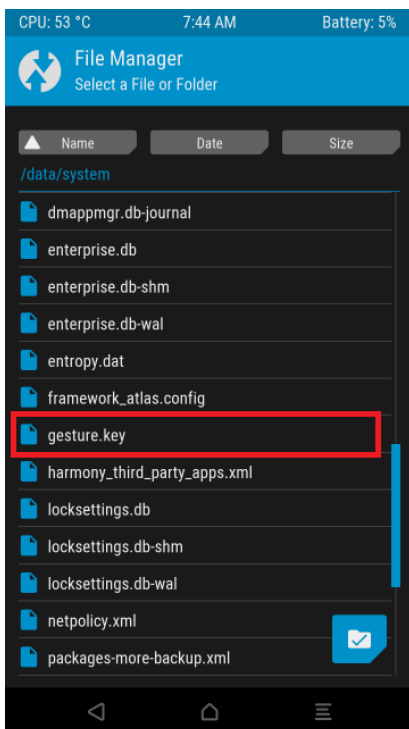


3. Navigate to \data\system.

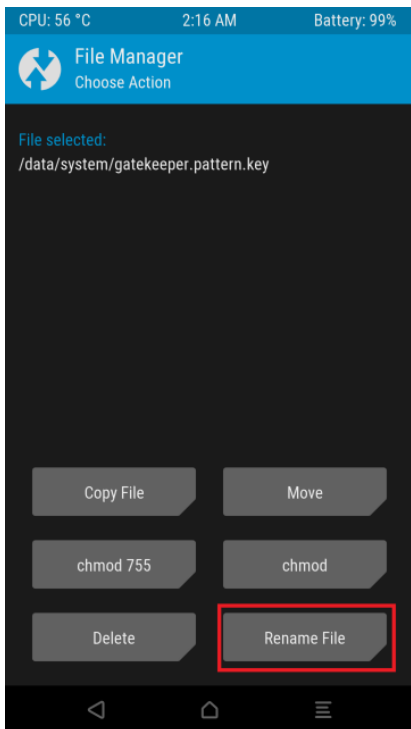




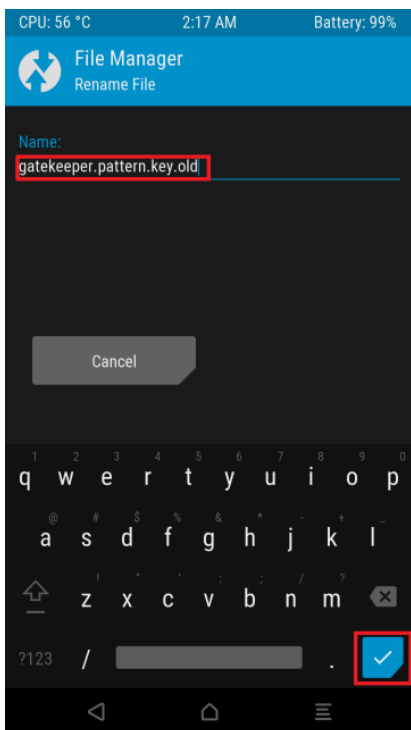
4. Locate the "gesture.key", "password.key", "gatekeeper.pin.key" or "gatekeeper.pattern.key" file.



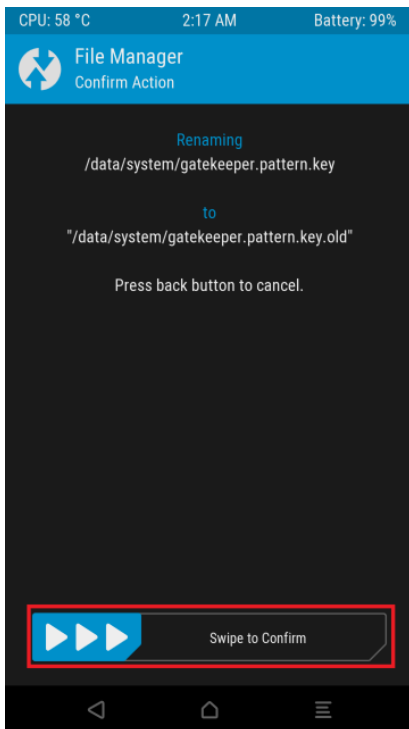
5. Long-press on the '*.key' file to reveal more options and choose "Rename File".



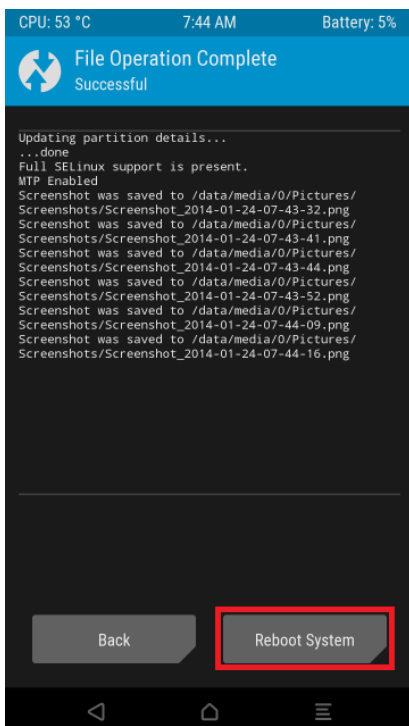
6. Add the extension ".old" to the file (the lock screen will be enabled afterwards by deleting the ".old" from the file name extension).




7. "Swipe" to confirm the renaming of the file.



8. After the file has been renamed, just click on "Reboot System".



9. After you boot into an Android, your lock screen should be removed completely or should accept any pattern/ PIN/password you will try.

 On some devices, the lock screen file can be named differently but it will always have ".key" at the end.

2.15 Flash phone with recovery image - TWRP


- [How to](#)(see page 78)
- [Where to find the physical image for later use](#)(see page 81)
- [If the button will not appear](#)(see page 81)


Every Android phone has a "recovery" partition which is by default used for performing factory resets using an OEM's preloaded tools. However, this partition can be modified in order to replace the default tools by third-party recovery tools such as [TWRP](#)²⁸.

These recoveries are (unlike the stock ones) capable of modifying all the internal system partitions of your phone or tablet (they need this capability in order to flash custom firmware).

TWRP even comes with a built-in file manager with unlimited root access so you can modify, add or delete any system files manually. This process allows you to gain physical image, therefore bypass the otherwise locked device's protection.

If the image is encrypted by the system itself, we are only able to get the encrypted physical image.

 The device has to have its bootloader unlocked in order to proceed with this method.

 Before we start this procedure, be aware that everything you do is at your own risk, every device does behave differently.

2.15.1 How to

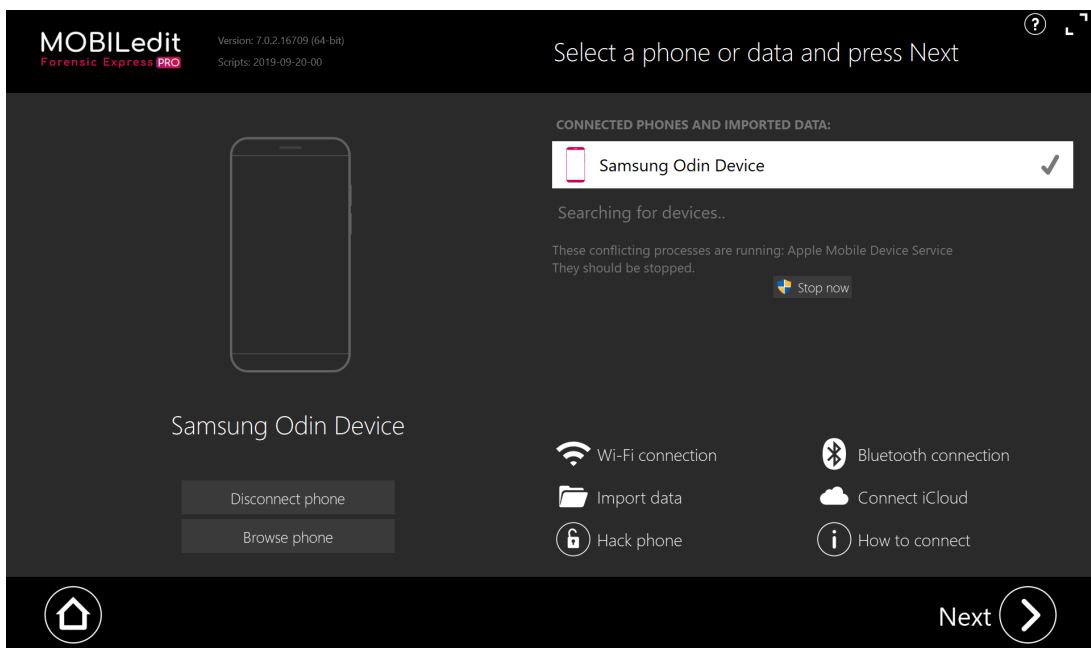
1. Download TWRP for your device (you can use for example a page: twrp.me²⁹).
2. Once you will have the .img file, load MOBILedit Forensic Express and navigate to the "Hack phone section" and select "Flash phone with recovery image".

²⁸ <https://twrp.me/about/>

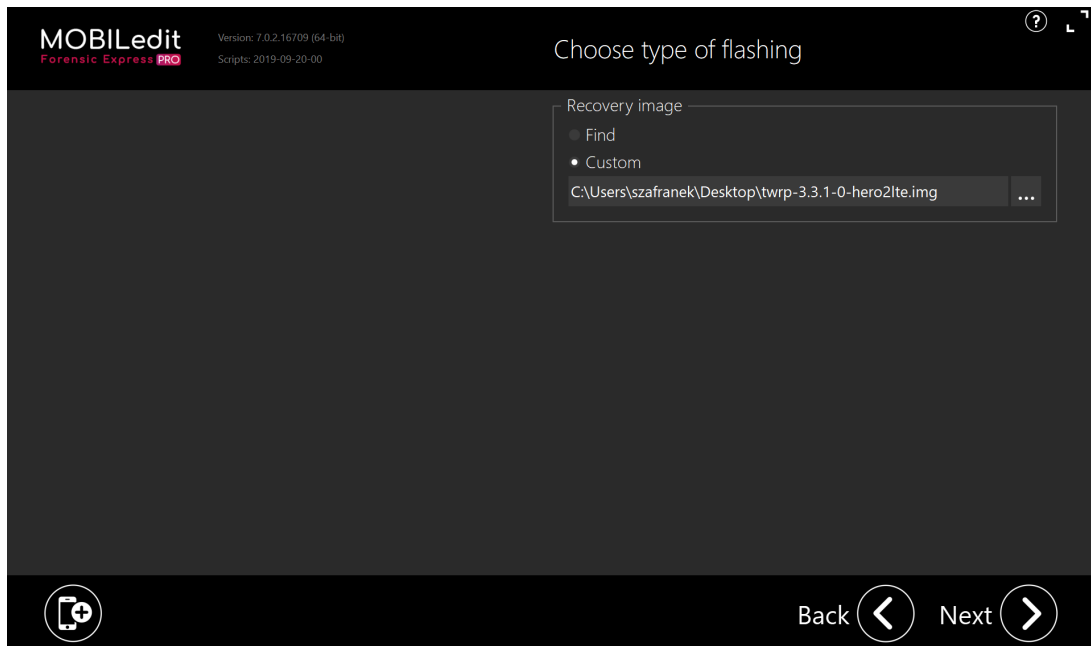
²⁹ <http://twrp.me>



3. Set the device to the download/fastboot mode and connect it to the PC.



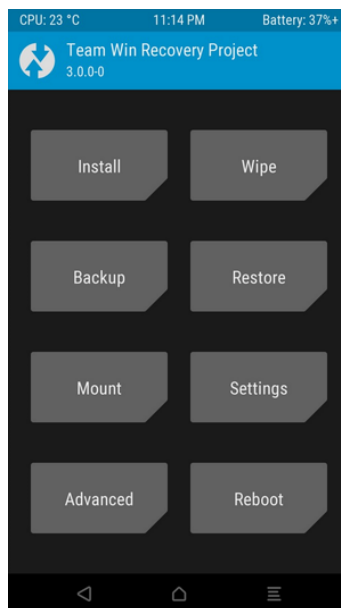
4. Click next and select "Custom" and import the .img file.

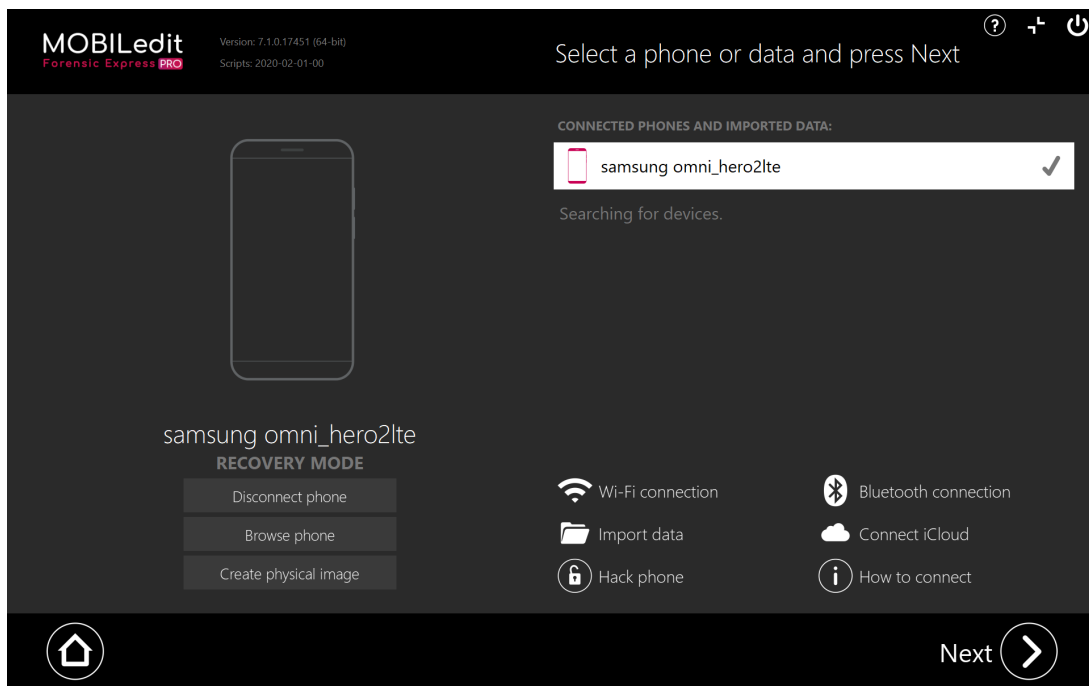


5. Proceed with the installation.

6. If the phone did not boot into TWRP right away, access it manually by holding vol. UP + Power + Home button.

If you see this on your device and computer, you have done everything correctly.





7. Proceed as you would do a normal extraction. If you want to just extract information into pdf.

2.15.2 Where to find the physical image for later use

We suggest clicking on the "Create physical image" button. Our software will determine which of the file in your device is the physical image and will begin creating.

2.15.3 If the button will not appear

1. Click the "Browse phone" button.

i If a pop-up message appears with a warning that you have an old connector just click **no**

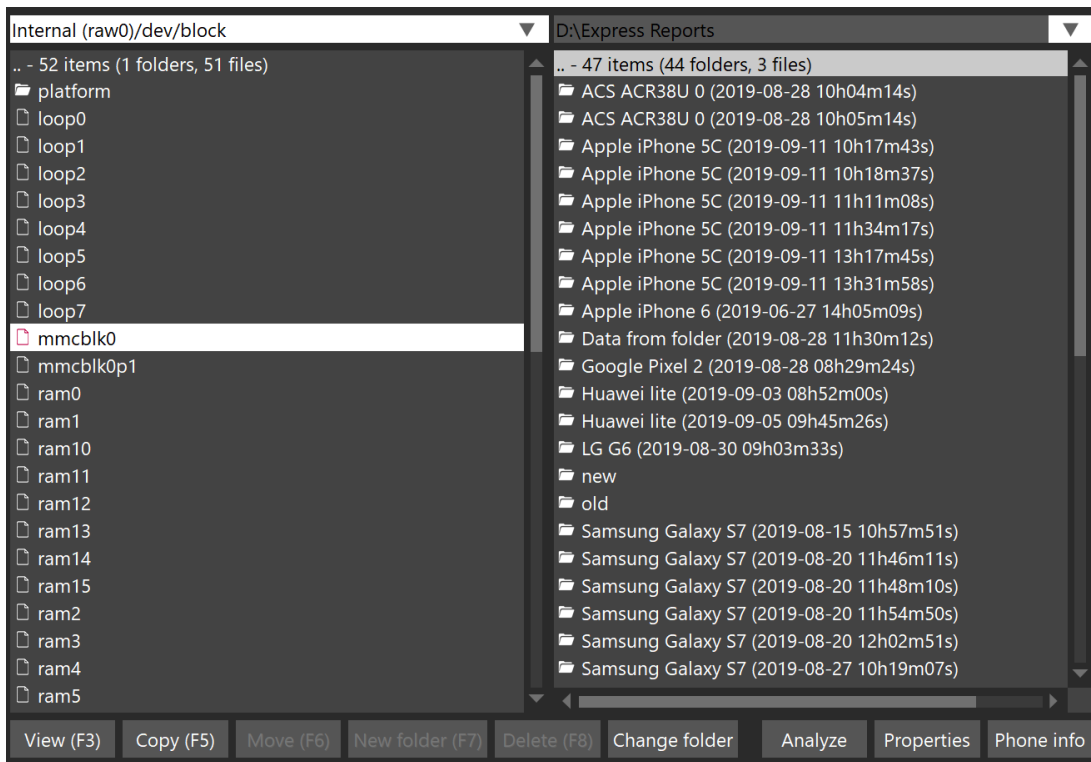
2. Navigate through internal (raw0) > dev > block.

There you should see a file called **mmcblk0**, copy that file to whatever folder you want by pressing F5 or the copy button.

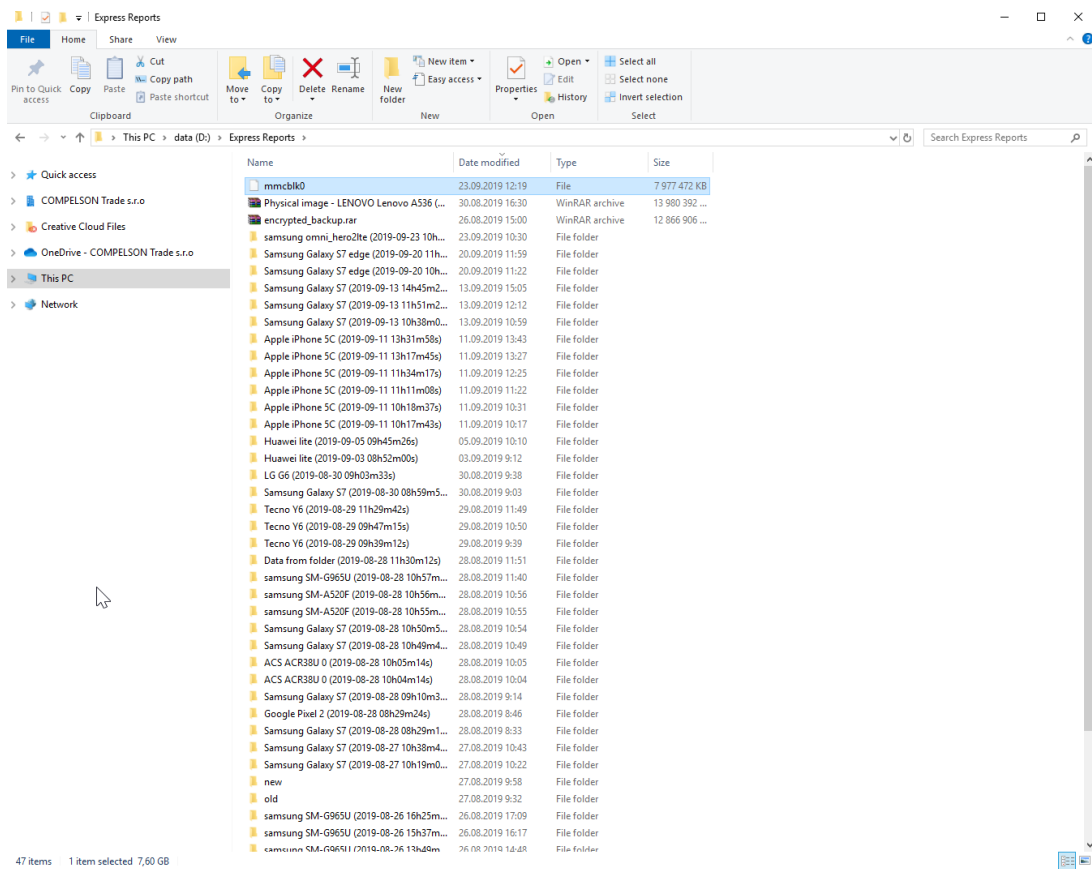
i If you do not see the file **mmcblk0** then there is a possibility that the physical image might be called differently, if that would occur please contact our [customer support](https://www.mobiledit.com/contact)³⁰.

(on the right side you can choose the destination)

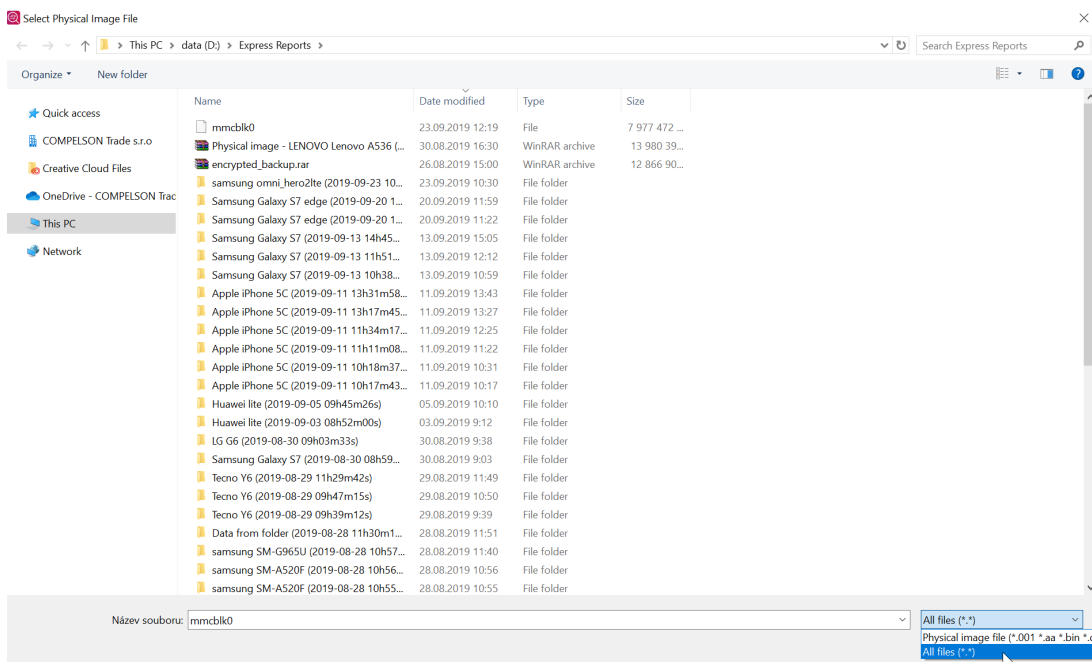
³⁰ <https://www.mobiledit.com/contact>



3. After the copying is finished, you should see the file in the desired folder.



If you would like to analyze this file later, then you need to click on the "Import data" button in MOBILedit Forensic Express and choose the "Physical image". Keep in mind that you need to select all files in the bottom right corner for mmcblk0 to show up, as seen in the screenshot below.



⚠ Procedures like this may cause irreversible harm to your device, please proceed with extra caution. Feel free to [contact us](https://www.mobiledit.com/contact)³¹ if you are not sure, we cannot take responsibility for the wrong image or any damage caused during this procedure.

2.16 CMD method - Flashing TWRP on non-Samsung devices

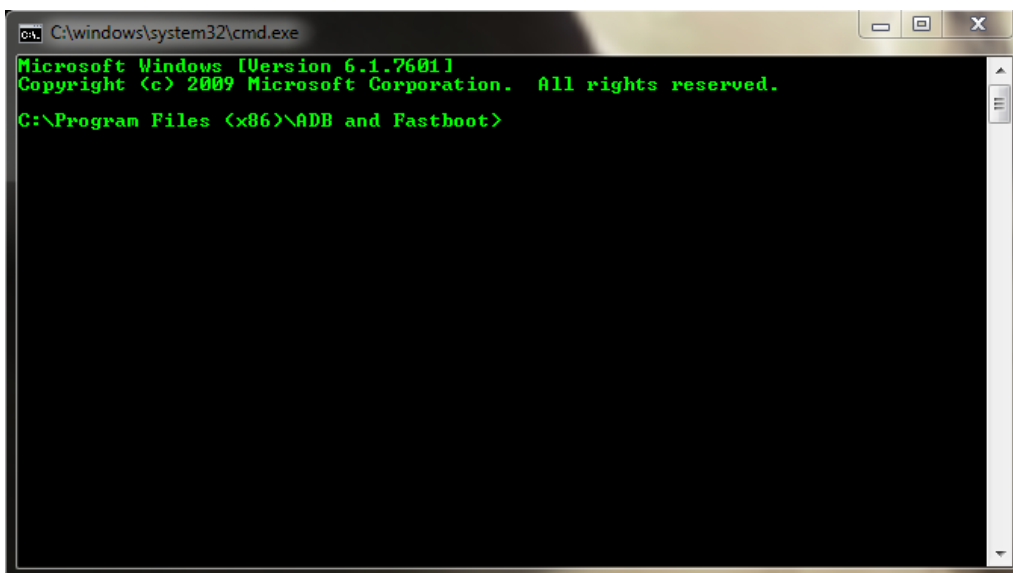
2.16.1 Requirements:

1. Your Android device
2. Unlocked bootloader
3. ADB and Fastboot installed on your PC
4. Computer with Windows 7 and above or Linux
5. All the correct drivers for your phone installed
6. TWRP image file for your device (ends with ".IMG")

2.16.2 How to

If your device is locked or you cannot boot into the system, use the hotkey combination for your phone to boot into Fastboot mode and skip straight to step 6.

1. Make sure you have USB debugging enabled on your device.
2. Connect your phone to your PC via USB.

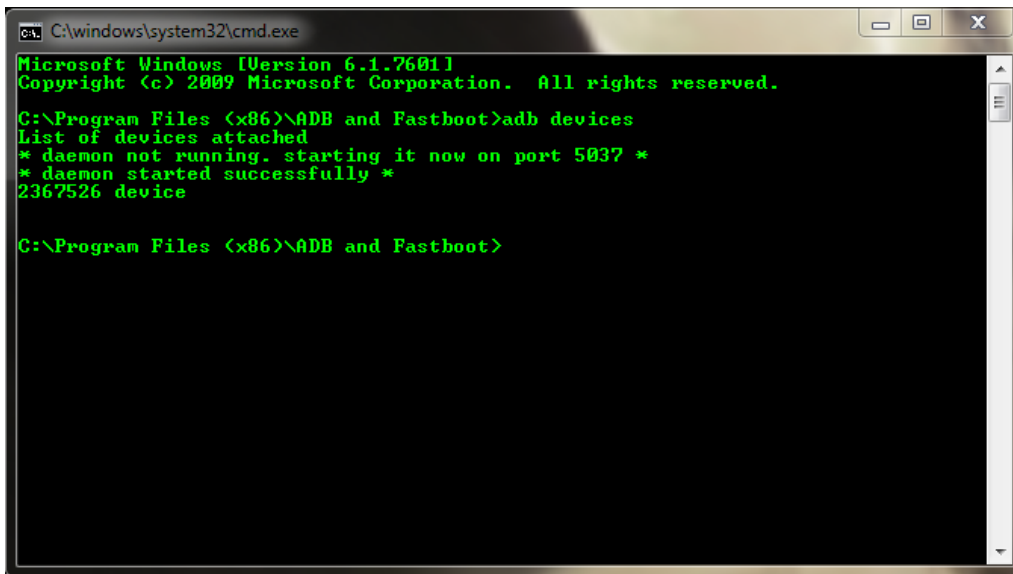


```
C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Program Files (x86)\ADB and Fastboot>
```

Open command line (CMD) in the folder you have your ADB and Fastboot installed or use Minimal ADB & Fastboot.

3. Type `"adb devices"` into the command line to see if your device is recognized by ADB.

³¹ <https://www.mobiledit.com/contact>

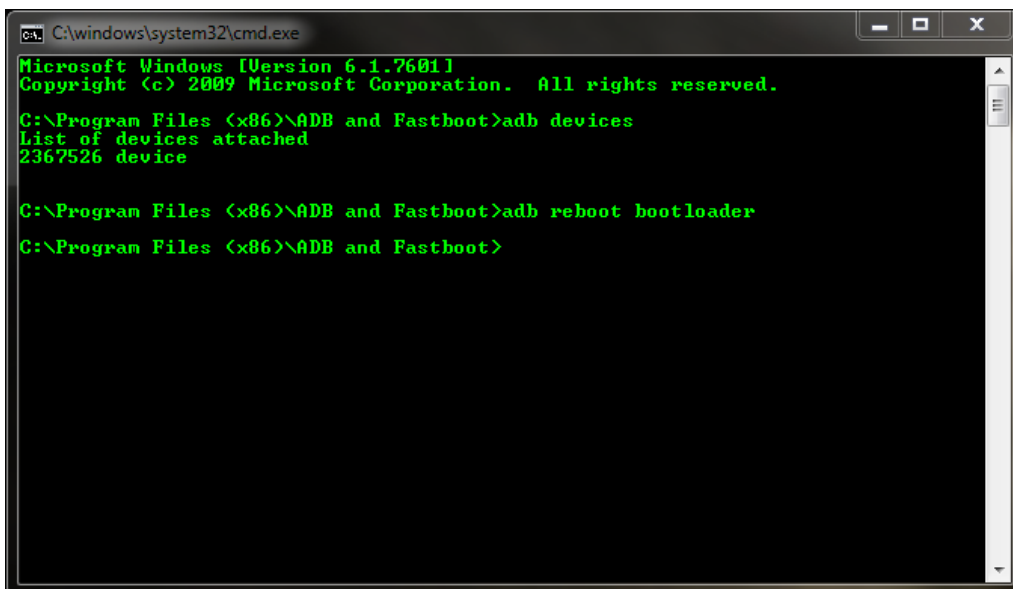


```
C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\ADB and Fastboot>adb devices
List of devices attached
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
2367526 device

C:\Program Files (x86)\ADB and Fastboot>
```

4. Type "*adb reboot bootloader*" into the command line and wait until your device reboots into Fastboot mode.



```
C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

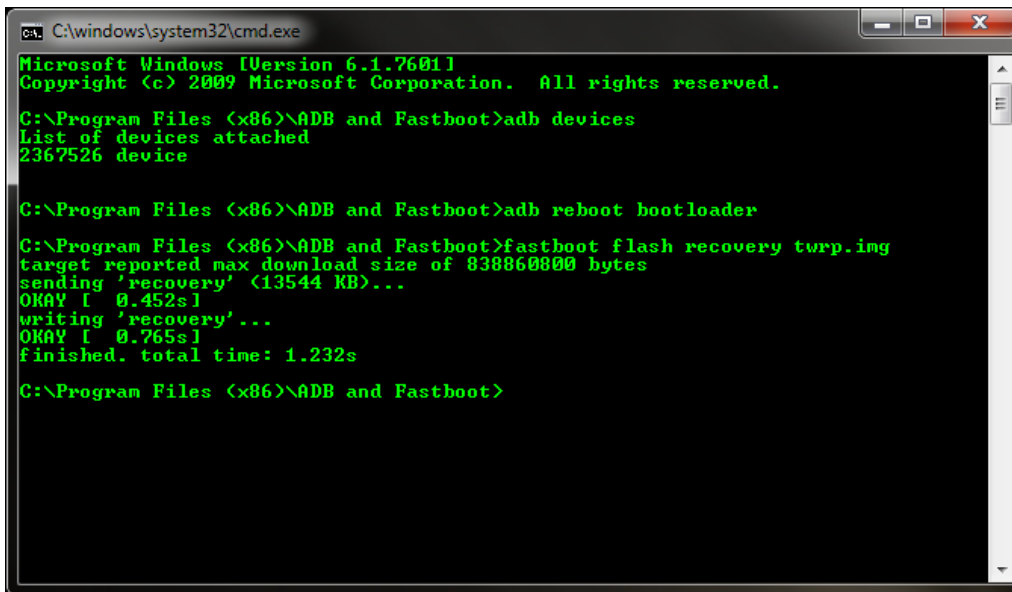
C:\Program Files (x86)\ADB and Fastboot>adb devices
List of devices attached
2367526 device

C:\Program Files (x86)\ADB and Fastboot>adb reboot bootloader
C:\Program Files (x86)\ADB and Fastboot>
```

5. Copy the TWRP image file to the folder where your ADB and fastboot is installed (for example: C:\Program Files (x86)\Minimal ADB & Fastboot).

6. Rename the file to "twrp.img"

7. Type "*fastboot flash recovery twrp.img*" into the command line and wait for the process to finish.



```

C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\ADB and Fastboot>adb devices
List of devices attached
2367526 device


C:\Program Files (x86)\ADB and Fastboot>adb reboot bootloader


C:\Program Files (x86)\ADB and Fastboot>fastboot flash recovery twrp.img
target reported max download size of 838860800 bytes
sending 'recovery' (13544 KB)...
OKAY [ 0.452s]
writing 'recovery'...
OKAY [ 0.765s]
finished. total time: 1.232s

C:\Program Files (x86)\ADB and Fastboot>

```

8. After the process has finished, you can type *"fastboot reboot"* to reboot your phone back to Android, or, switch it off and use hotkey combination to boot straight into your newly flashed TWRP.


 Flashing custom recoveries may void your warranty!

 You can also try to use our in-built flashing tool for TWRP, more information is available [here](#)(see page 78).

2.17 ODIN method - Flashing TWRP on Samsung devices

2.17.1 Requirements

1. Your Samsung device
2. All the [correct drivers](#)³² for your phone installed
3. Computer with Windows 8 or newer
4. Odin 3.09 or newer
5. ADB installed on your PC
6. The TWRP image file for your device in TAR archive (download from [here](#)³³)

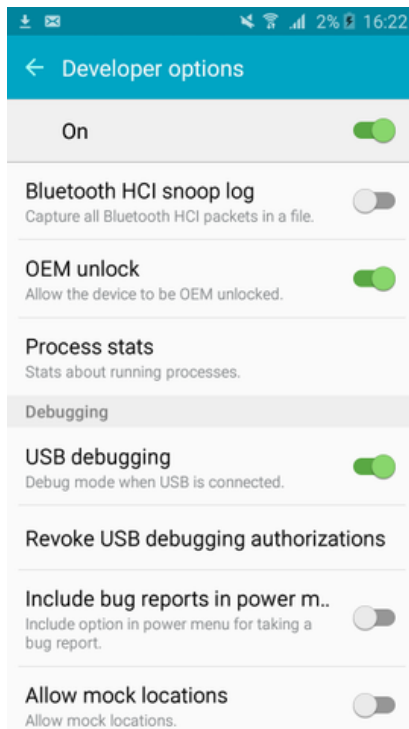
 If you're a Linux user, please use Heimdall instead of Odin.

2.17.2 How to

1. Make sure that you have enabled "OEM unlock" (if available) as seen on the screenshot below.

³² <http://www.mobiledit.com/download-list/phone-drivers>

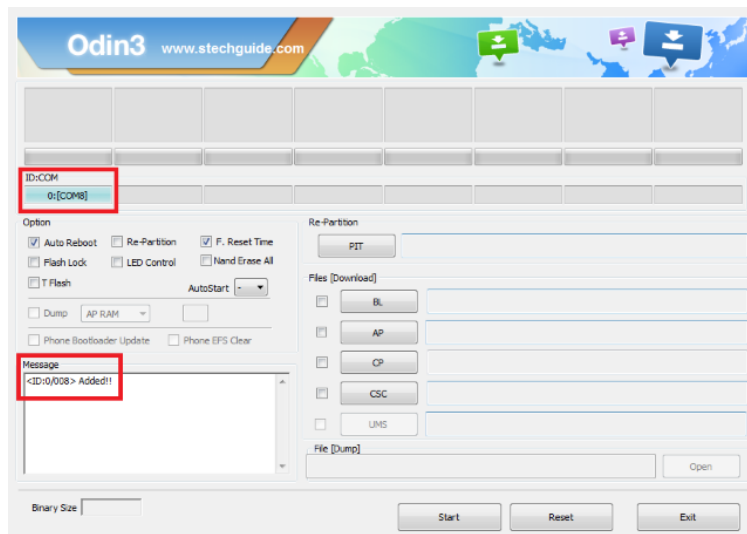
³³ <https://twrp.me/Devices/>



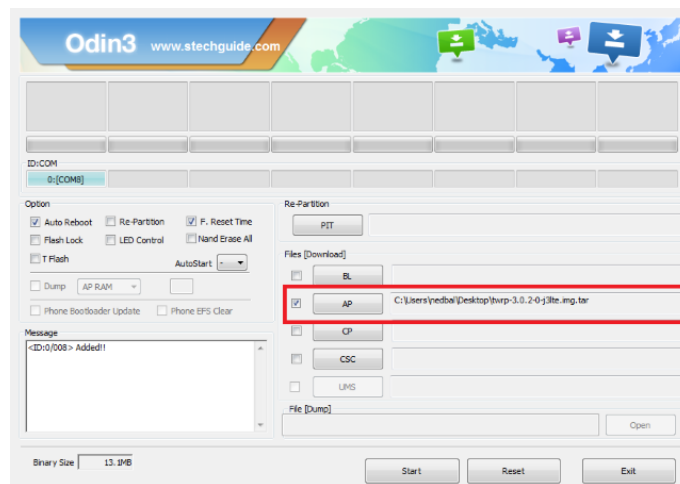
2. Start Odin and restart your phone into "Download mode" by turning it off and holding the 'volume down', 'home' and 'power' buttons for a few seconds.



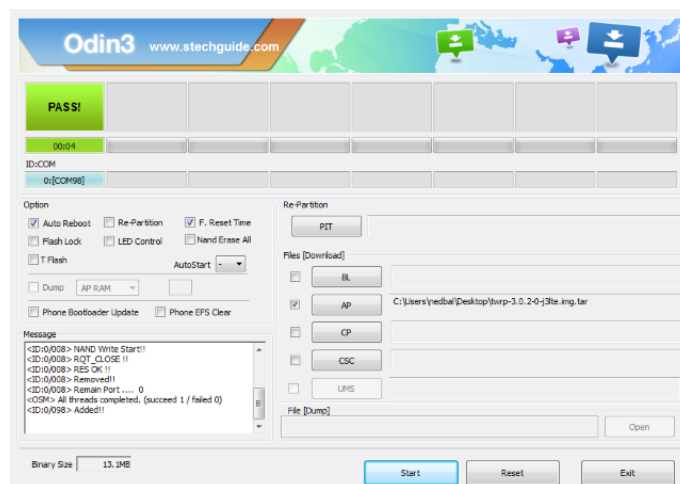
3. Connect your phone to the PC via USB, Odin should recognize a new device:




4. Make sure that the "Re-Partition" option in Odin is disabled.
5. Click on the "AP" button in Odin and choose your TWRP image (should end with ".img.tar").




6. Click on the "AP" button in Odin and choose your TWRP image (should end with ".img.tar").



7. Once the text "PASS!" appears in Odin, your device should automatically reboot. You can then boot into your new recovery straight from Android using "*adb reboot recovery*" command.

 You can also try to use our in-built flashing tool for TWRP, more information is available [here](#)(see page 78).

 Flashing custom recoveries may void your warranty and trip the Knox Warranty void flag!

2.18 How to boot into recovery on Android

- [How do I boot into recovery mode?](#)(see page 89)
 - [New Samsung Galaxy devices](#)(see page 90)
 - [Old Samsung devices](#)(see page 90)
 - [New Samsung devices](#)(see page 91)
 - [Honor/Huawei](#)(see page 91)
 - [LG](#)(see page 92)
 - [HTC](#)(see page 93)
 - [Motorola](#)(see page 93)
 - [Google/Nexus phones](#)(see page 94)
 - [ASUS](#)(see page 95)
 - [OnePlus](#)(see page 96)
 - [Nokia](#)(see page 96)
 - [Xiaomi](#)(see page 97)

A recovery is a tool used to perform a factory reset and install system updates by default. There are many custom recoveries (CWM, TWRP, etc.) made especially to flash custom ROMs (unofficial builds of Android) and to perform similar under-the-hood changes and modifications to your device.

When you enter recovery mode, you don't actually start up your Android operating system - which comes in handy when your system is corrupted or unbootable. If you intend to root your Android device, you will likely need to use recovery in order to flash SuperSU binaries.

2.18.1 How do I boot into recovery mode?

There are three ways to boot into recovery:

1. Assuming your phone is already rooted, you can use an app to boot into recovery directly from your Android home screen.
2. You can use ADB command to reboot into recovery once your Android phone is in fastboot mode and connected to your PC via USB at the same time.
3. Recovery is also accessible by pressing and holding specific keys while your phone is turned off. This is sometimes called "hotkey combination".

In this article, we will focus on the third method - hotkey combination.

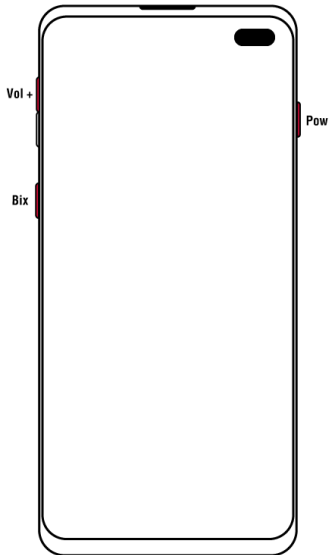
So how exactly does hotkey combination work?

Unfortunately, each phone manufacturer has their own different combination of buttons required to press in order to boot into recovery.

Below you can find most major manufacturers' hotkey combinations and instructions.

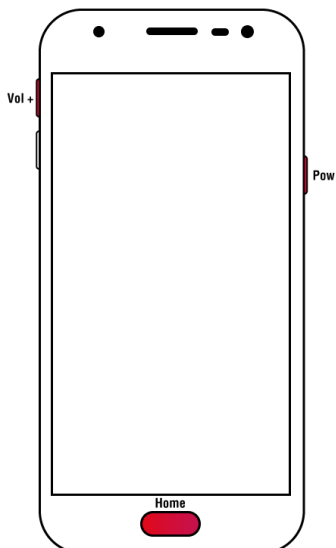
2.18.1.1 New Samsung Galaxy devices

Press and hold volume up, Bixby, and Power buttons simultaneously.



2.18.1.2 Old Samsung devices

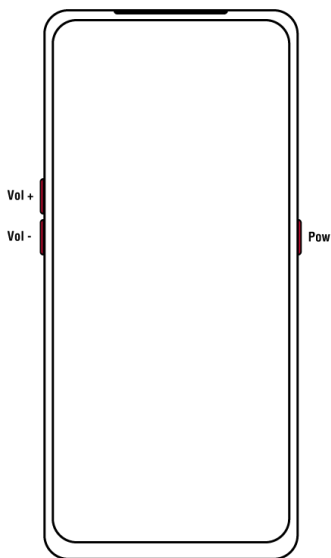
Press and hold Volume Up, Home, and Power buttons altogether.



2.18.1.3 New Samsung devices

Press and hold the Volume Up + Volume Down + Power buttons at the same time.

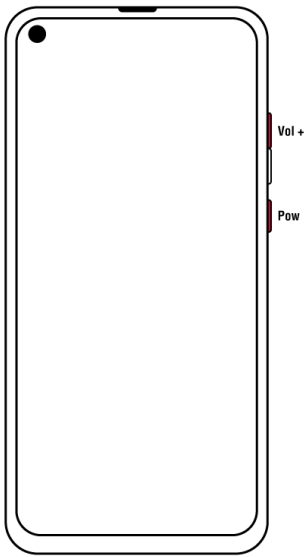
As soon as the screen turns off, release the Volume Down button and keep Volume Up + Power buttons pressed.



2.18.1.4 Honor/Huawei

Press and hold Volume Up + Power button while the device is powered off.

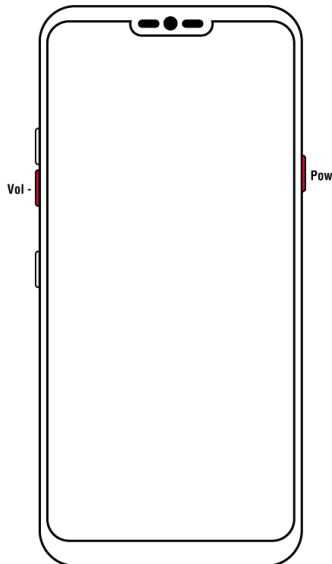
Release the buttons when you see the Huawei/Honor logo.



2.18.1.5 LG

Power off the device then press and hold the Power and Volume Down buttons simultaneously.

Release the Power Button as soon as it shows LG logo, continue to hold the Volume Down and then press the Power button again.



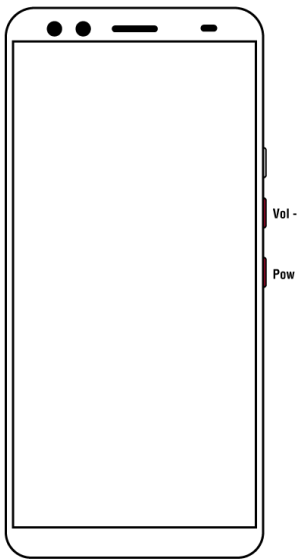
2.18.1.6 HTC

Turn off your phone, then hold down Volume Down + Power button (older devices: Home + Power button).

Release the Power Button when HTC logo appears.

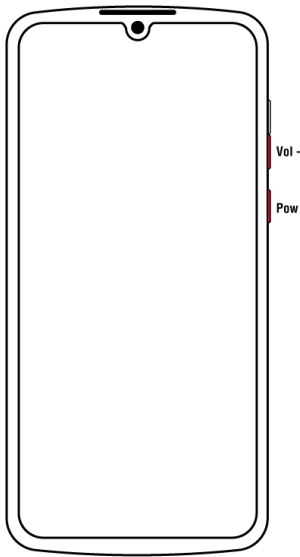
HTC legend

To enter into Recovery: (while turned off) Press Down on Trackball + Volume Down + Power Highlight Recovery with the volume keys and select with the Power key.



2.18.1.7 Motorola

With the device powered off, press and hold Volume Down + power button together.

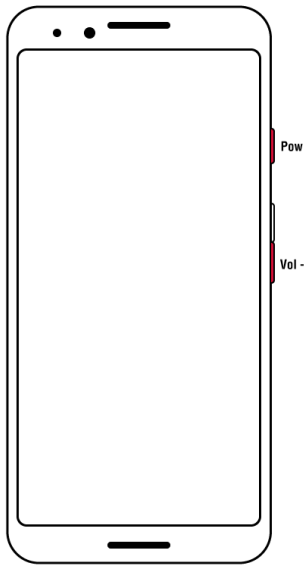


2.18.1.8 Google/Nexus phones

Access fastboot by pressing and holding the Power and Volume Down buttons at the same time until you see the fastboot screen.

In Fastboot mode, press the Volume Down button twice to select Recovery then press the Power button to confirm the selection.

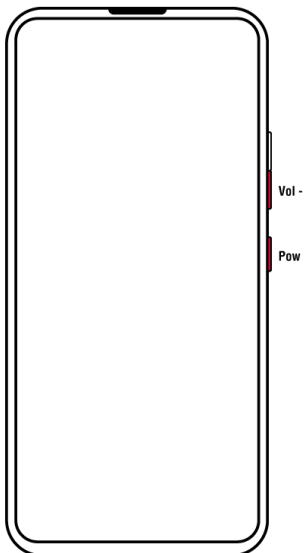
When you see the broken Android on your screen, press and hold the Power button then press the Volume Up button once. Your device should boot into recovery mode.



2.18.1.9 ASUS

With the device powered off, press and hold Volume Down + Power button together.

When the device starts to release the power button and continue to hold Volume Down.



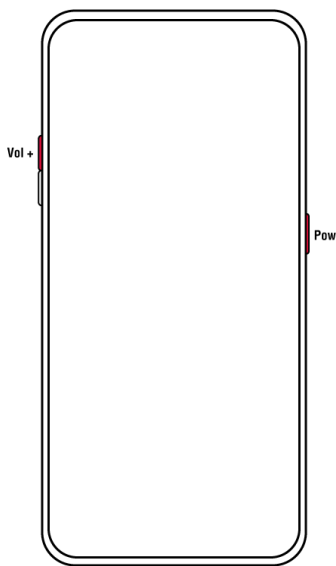
2.18.1.10 OnePlus

Press and hold Volume Up + Power button.

Release the Power button when you see the OnePlus logo and keep holding the Volume Up button until you see the fastboot mode splash screen.

Navigate using the volume key to the Recovery Mode.

Alternatively, with the device powered off, press and hold Volume Down + Power button until you see the OnePlus logo.

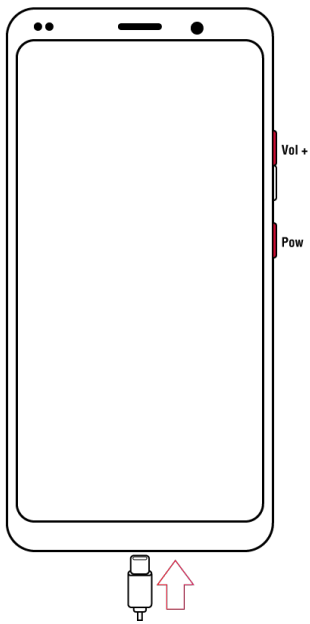


2.18.1.11 Nokia

Turn off the device and connect it to a charger. When you see the battery charging indicator, press and hold the Volume Up + Power buttons.

Release the keys when the Android logo appears. On most Nokia devices such as the Nokia 8, Nokia 7, Nokia 5, 5.1, Nokia 6, 6.1, etc. you should already be in recovery mode.

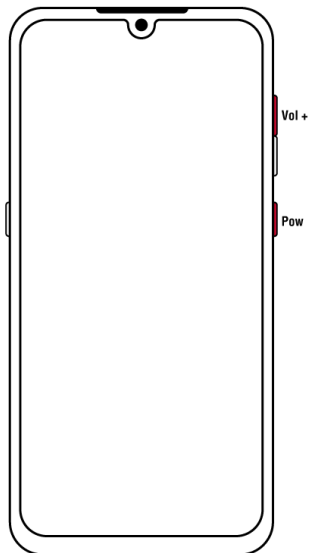
On devices such as the Nokia 1, press and hold the Power button again and press the Volume Up button once.



2.18.1.12 Xiaomi

With the device powered off, press and hold Volume Up + Power button.

When the device starts, release the power button and continue to hold the Volume Up.



2.19 Lockdown method - Unlocking a passcode-protected iPhone

MOBILedit Forensic Express is able to connect to iPhones protected by passcodes. Many iPhone users use iTunes, especially for managing music and almost everyone has connected their iPhone to iTunes at least once. To get through the passcode, you need to access the computer that the locked iPhone was connected to and obtain the 'lockdown file' that iTunes creates automatically for any iPhone that connects to that PC.

i Lockdown method does NOT unlock phone (eg. screen will stay locked, even if it's successful), but enables our software to communicate with phone and extract data from it, that can be used for further examination.

You will find the lockdown files located in the iTunes folder along with one of these file paths, depending on your operating system.

- **Windows Vista, 7, 8, 10**

C:\ProgramData\Apple\Lockdown

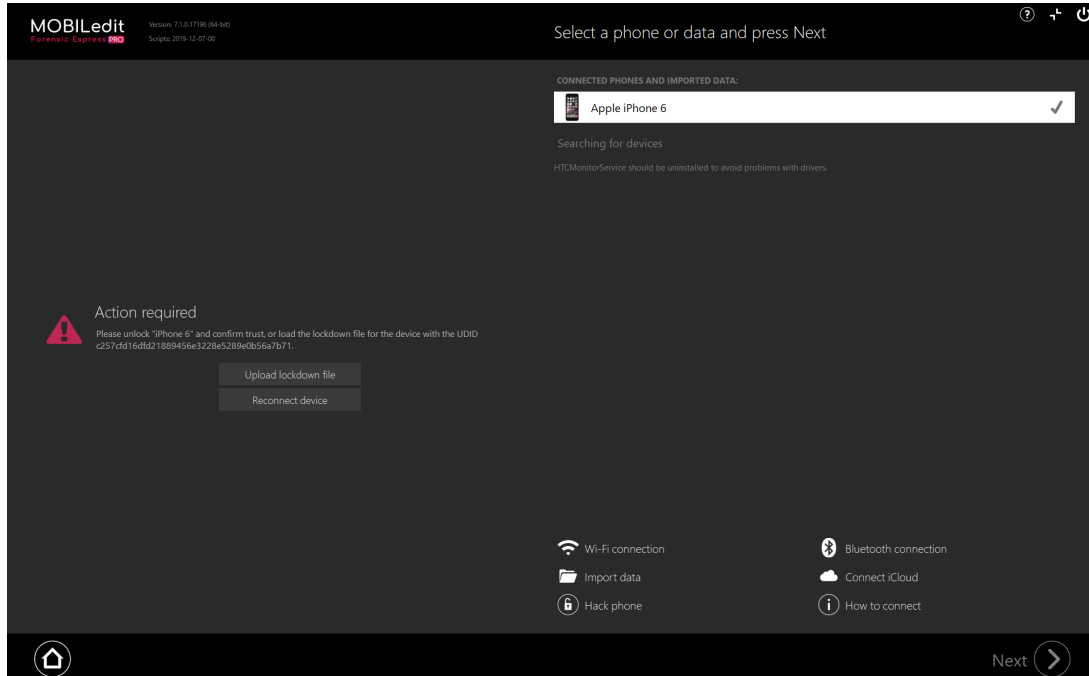
- **Windows 2000/XP**

C:\Documents and Settings\All Users\Application Data\Apple\Lockdown

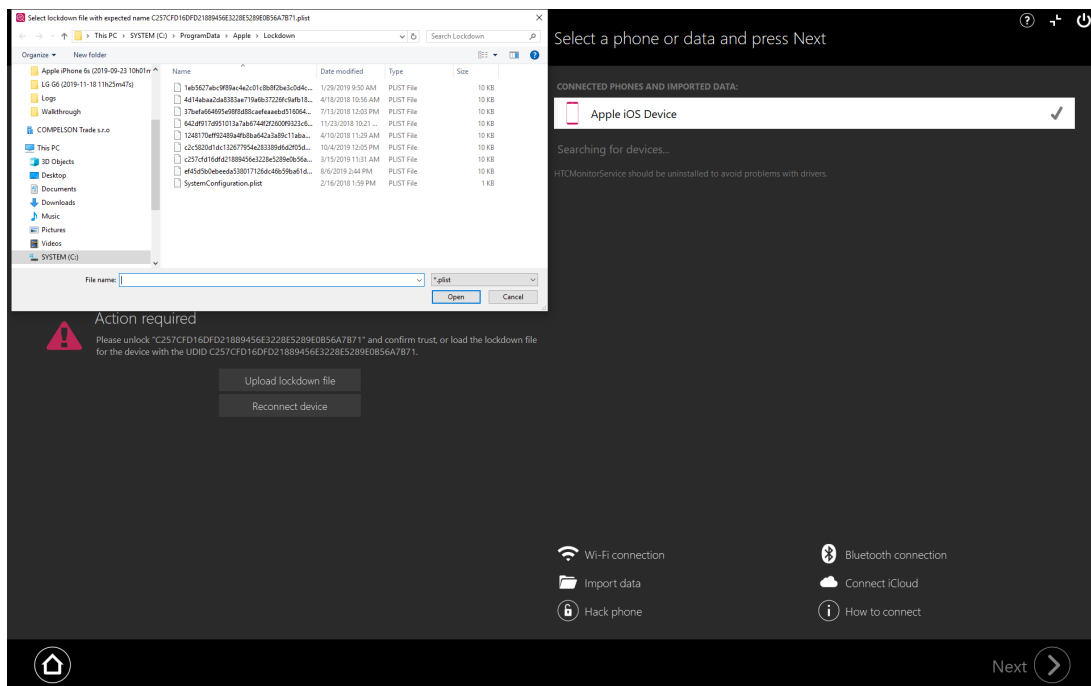
- **Mac OS X**

/var/db/lockdown

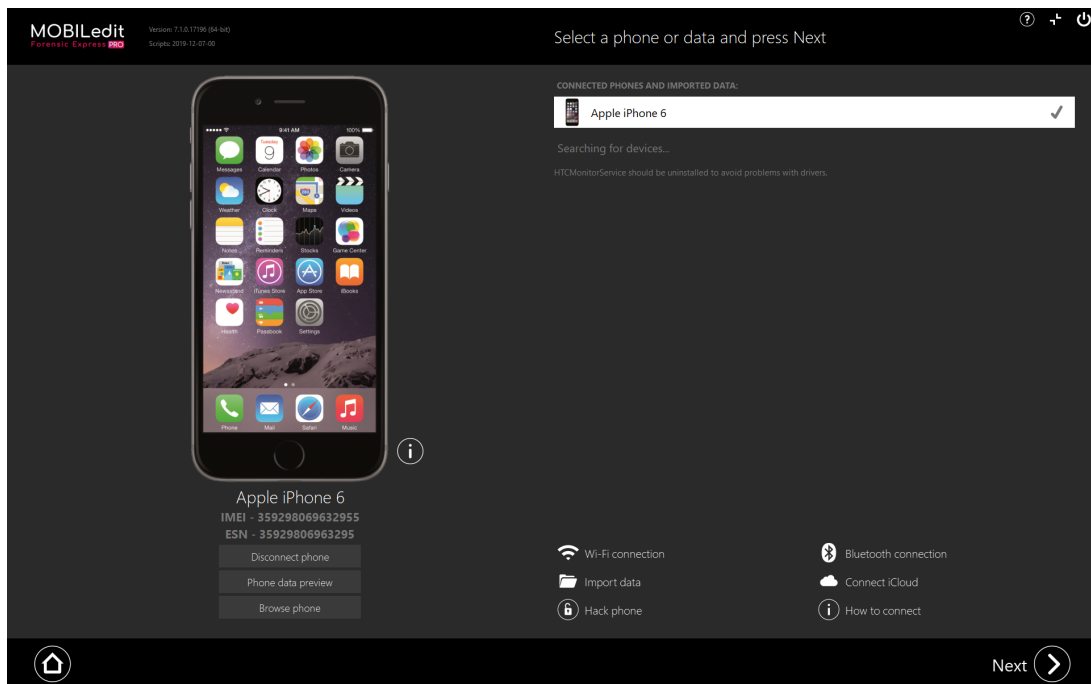
After finding these files, move them to a different location on the disk or transfer them to the computer with MOBILedit Forensic Express installed if needed. Once you have the file, click on the "Upload lockdown file".



Then select your lockdown file.




Click on Open and your iPhone will reconnect and will be unlocked.



i If your device is running iOS 9, or higher, if device was rebooted prior connecting, lockdown files are not accepted by device, until first device unlock.

The **lockdown files method** works in different ways for certain iOS versions.

- for *iOS 8* and lower, it works basically without any limitations (reboot doesn't affect accepting lockdown files, lockdown file is unique to device and can be used even after factory reset)
- for *iOS 9 - 11.2*, it does work without any significant limitations (except reboot explained above)
- for *iOS 11.3* and above the expiration date for the lockdown file added, after one week from last computer connection, they will become invalid.
- for *iOS versions 11.4* and above the "restricted mode" was introduced, which means if the device is disconnected from the PC for more than an hour or connected to the PC it was never connected before, the user is forced must unlock phone to connect, otherwise the PC will not recognize device is connected to USB.

 Restricted mode is turned on by default, however, the user can disable it in the settings.


2.20 How to jailbreak an iOS device?

- [What does jailbreaking mean?](#)(see page 100)
- [How do I jailbreak an iOS device?](#)(see page 100)

Jailbreaking device enables MOBILedit Forensic Express to extract more data from your iPhone or iPad.

Some of the primary reasons why people jailbreak their devices include:

- Sideloaded apps
- Option to set and use alternative apps
- Customization of the otherwise closed iOS user interface
- Tethering your Mac to your iPhone
- Ability to browse the entire internal memory filesystem of your device


 Learn how to jailbreak iPhone with checkra1n [here](#)(see page 101).

2.20.1 What does jailbreaking mean?

When you jailbreak an iOS device, you basically modify the software to remove the restrictions and limitations set by Apple.

With a jailbroken device, you will also be able to access and investigate the phone's internal storage and browse the entire filesystem. You also will be able to download software from alternative stores as well as straight from the internet.

2.20.2 How do I jailbreak an iOS device?

 Please do note that our support team can help you with problems that might occur after the device is jailbroken, but the whole process of jailbreaking is only **done by the user**

There are three ways of jailbreaking your iOS:

1. **Tethered** - This method requires you to connect your iPhone to your computer and use an external application to jailbreak it. Once you restart your iPhone, the jailbreak is undone, but please note: your device will not be usable until you jailbreak it again using the same method.
2. **Semi-tethered** - This method doesn't require you to connect your iPhone to a computer in order to jailbreak it, however, the jailbreak is still undone every time you reboot your device, or, after a certain amount of time passes.
3. **Untethered** - This method doesn't necessarily require a computer to perform a jailbreak on your device and also modifies the iOS on a deeper level which means that no matter how many times you reboot your device, it stays jailbroken until you manually "un-jailbreak" it.

There are specific known ways to jailbreak almost every iPhone, iPad or iPod Touch running on almost every iOS, except the latest releases - as it usually takes a few months to find a way of jailbreaking the newest version of iOS.

This means that there is no way of describing them all in a single article.

However, currently, the most often used apps for jailbreaking iOS devices are Pangu or Cydia Impactor. You can learn more about how Cydia works on the app developer's official website at [this link](#)³⁴, or you can read [this article](#)³⁵ which describes a simplified process of iOS jailbreaking.

You can find a full list of available jailbreaks for each device [here](#)³⁶.



Also, keep in mind that our software might not recognize in the main menu that your device is jailbroken or not - it is due to service AFC2 or SSH not being accessible. If that happens do not worry it won't affect the extraction in any way.



Jailbreaking a device may void the manufacturer's warranty and could cause security risks. Please take this into consideration before performing this process.

2.21 Jailbreaking iPhone with checkra1n

- [How to boot checkra1n from a flash drive](#)(see page 101)
- [How to enter firmware settings \(BIOS\)](#)(see page 102)
- [Jailbreaking with Checkra1n](#)(see page 105)

2.21.1 How to boot checkra1n from a flash drive

Bootra1n is a Linux distribution which enables users to boot checkra1n on any PC without having to install additional software or an OS.

Bootra1n flash doesn't have signed loader, which is why you will need to boot directly into your computer. This is a standard procedure on all modern computers with UEFI and Secure boot.

To disable Secure boot, you will need to enter computer firmware settings.


On some computers, you can enter firmware with a hotkey once it is turned on, but usually, this is not possible because of fast boot technology, that boots directly into the installed operating system.

You can force your computer to allow you to enter the firmware directly from Windows.

³⁴ <http://www.cydiaimpactor.com/>

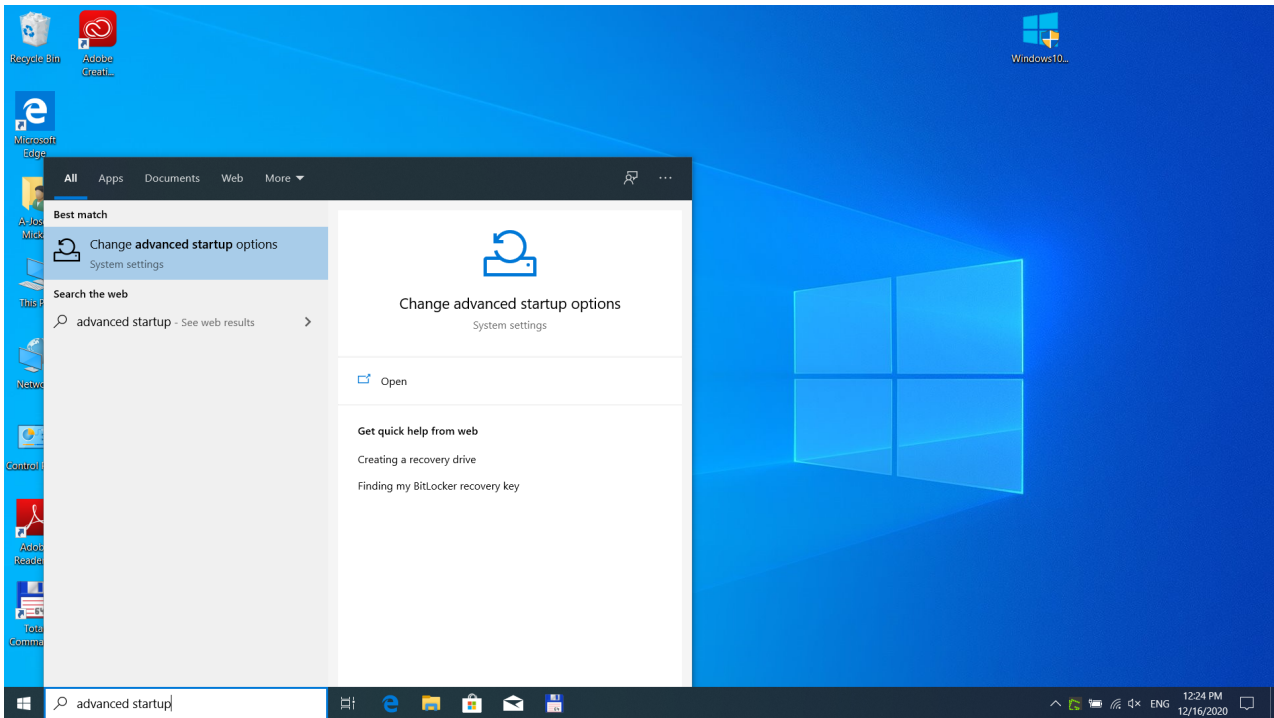
³⁵ <https://downloadcydia.org/cydia-impactor/>

³⁶ <https://www.reddit.com/r/jailbreak/wiki/escapeplan/guides/jailbreakcharts>

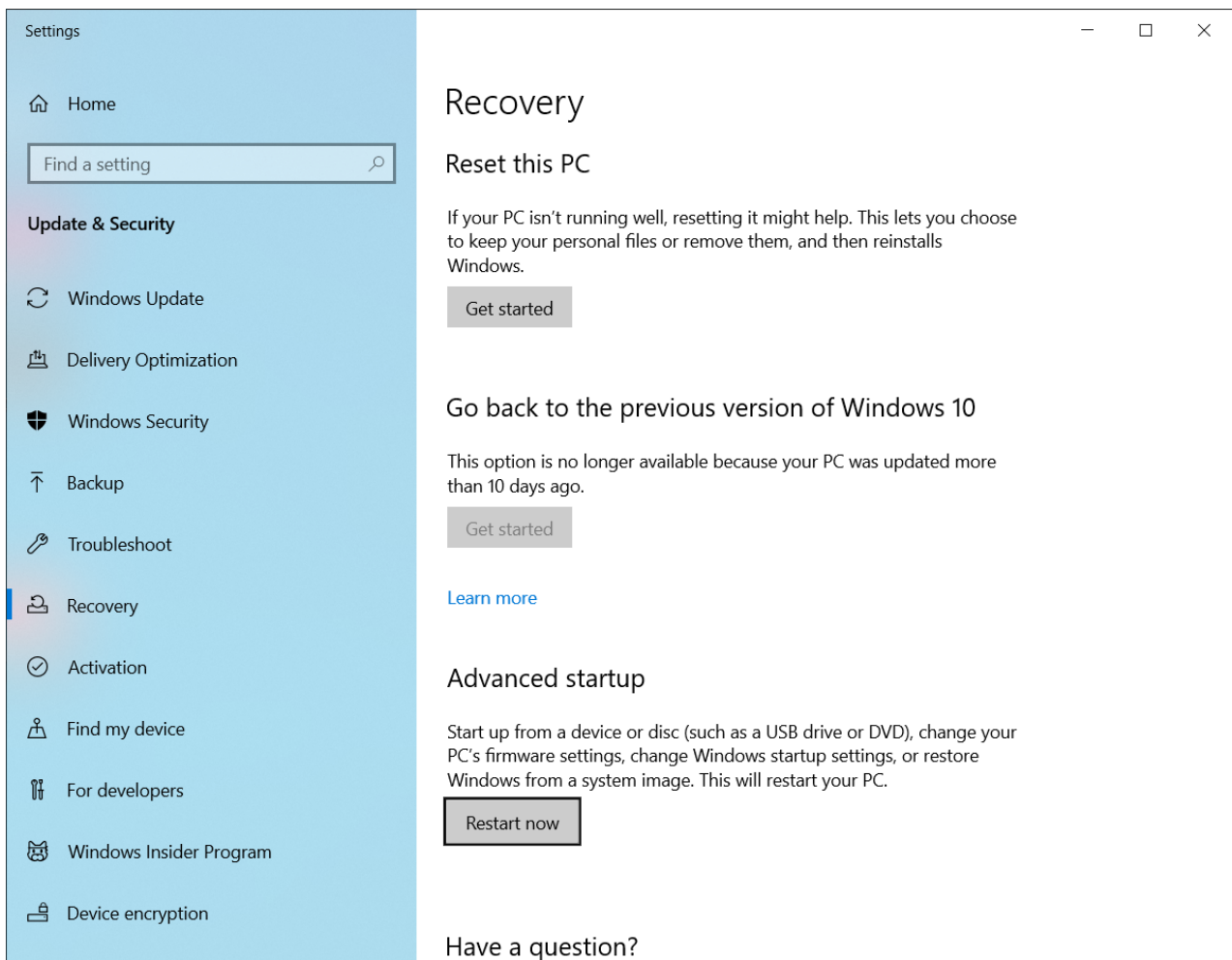
 Firmware varies by manufacturer and model. We used HP Probook 440G5 for our demonstration (many recent HP computers have similar firmware setting).

2.21.2 How to enter firmware settings (BIOS)

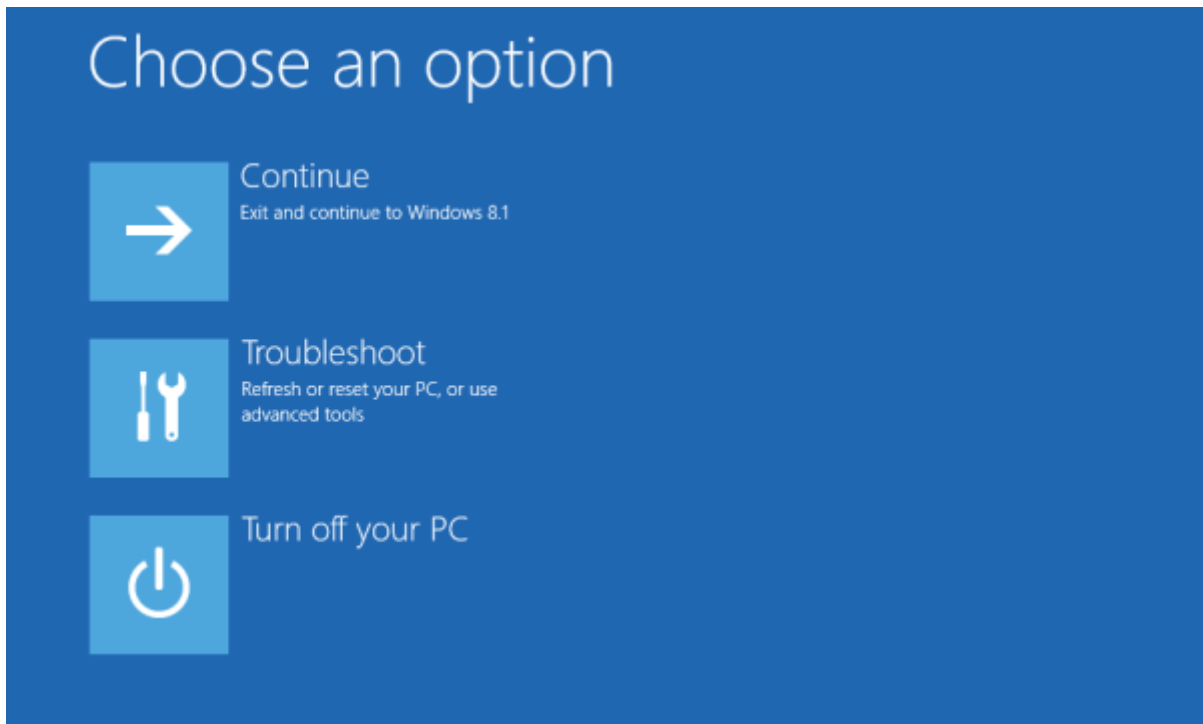
1. Search for **Advanced startup** option.



2. When you go to the Advanced startup, you should see Windows setting screen with startup option preselected. Click Restart now.

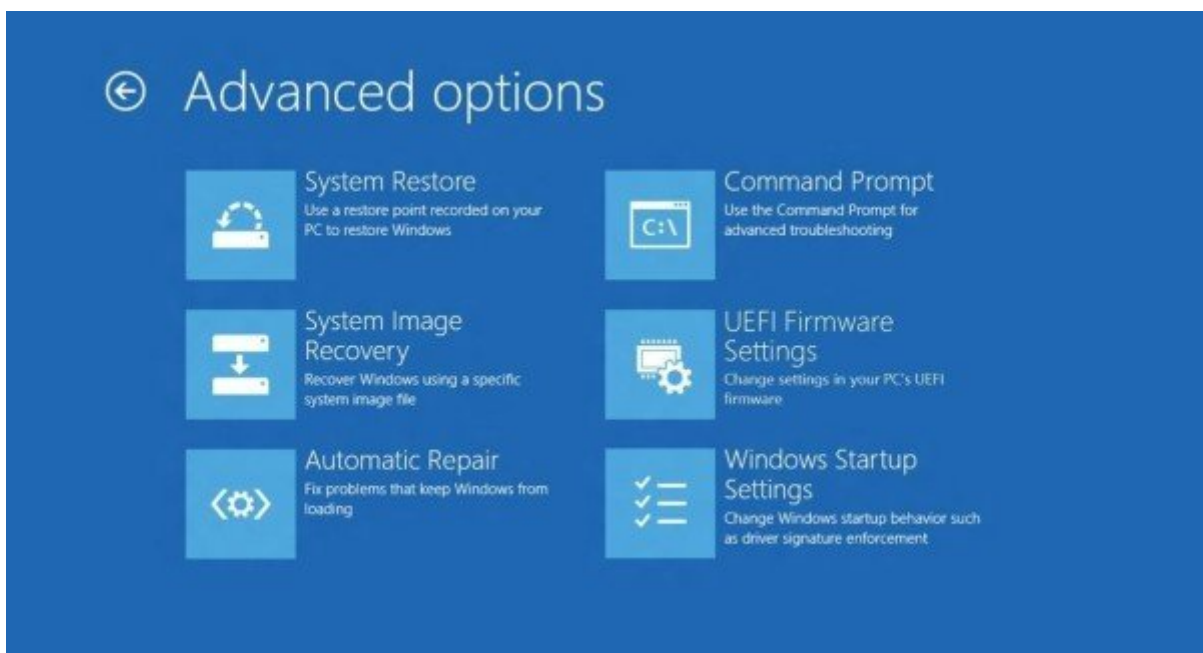


3. The computer will reboot into advanced startup mode, giving you an option to do various maintenance and recovery-related operations. Select **troubleshoot**.



4. On the next screen, select **Advanced options**.

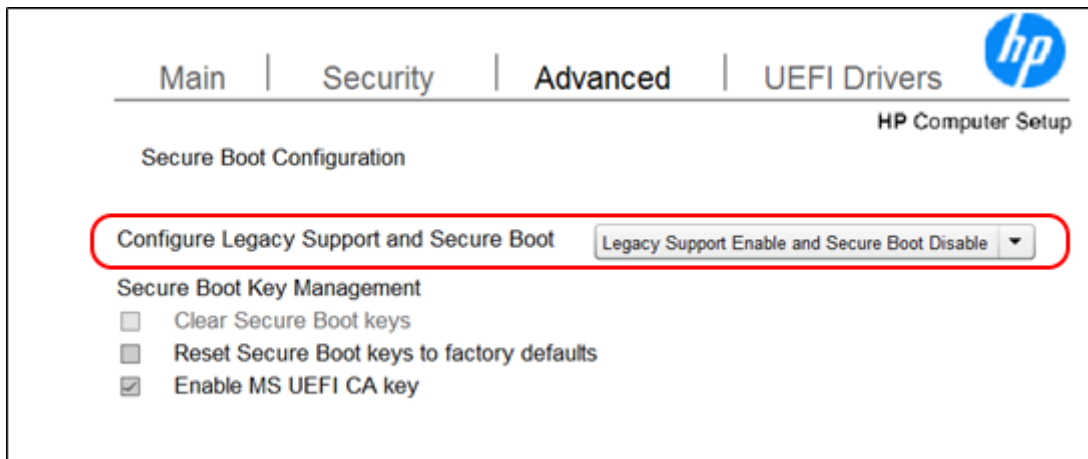
5. Select **UEFI Firmware Settings**.



6. Restart your computer.

7. After restarting the computer you will either enter firmware settings (BIOS) or you will be presented with further options. The correct option is **BIOS Setup**.

8. When you enter BIOS, you need to search for Secure boot option and disable it. In our example of BIOS, it's located under the advanced settings page.



9. Save your changes. The way how to do that depends on a computer which you are using (in our example, you can either click F10 or go to the main section and save it there).

i Before you save your settings (which will effectively restart the computer), make sure that USB flash drive with bootra1n is inserted into the computer.

10. When the secure boot is disabled it effectively disables the fastboot as well, so you should be able to call the boot menu of your device with hotkey after powerup. Usually, it's one of the following keys: ESC, F2, F9, F10 (please refer to your device manual).

11. Once your computer enters the boot menu, you should be presented with an option to boot from the flash drive. On our HP Probook, it is **General Udisk** option.

12. When you boot from the flash drive, you will be presented with a boot menu for bootra1n. Select **void linux** (USB safe).

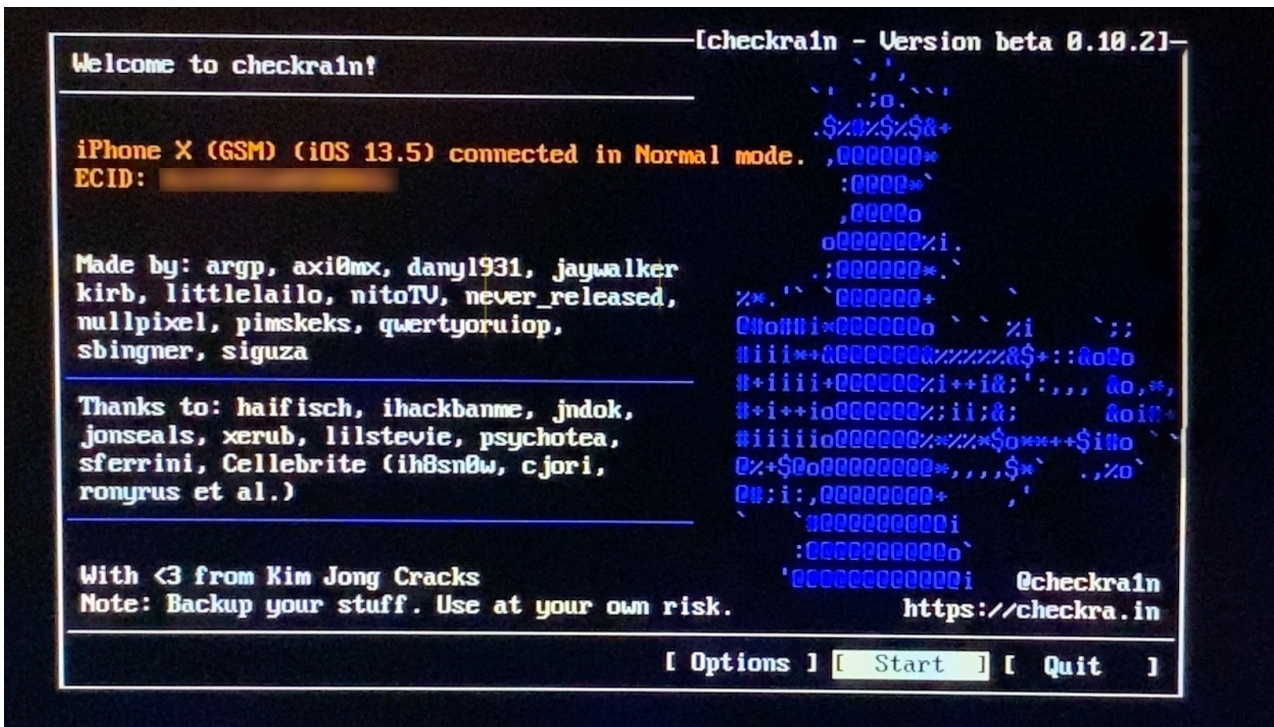
i Booting from flash drive doesn't access your computer hard disk, only the flash drive, and anything you connect to USB.

13. Once the boot sequence is finished, you will be presented with a login screen. Use login **root** and password **voidlinux**. At the shell prompt, type checkra1n and hit enter. This will run Checkra1n in interactive mode.

2.21.3 Jailbreaking with Checkra1n

The version of Checkra1n on flash disk supports all models from iPhone 5s to iPhone X (iPhone XR/XS are not supported), all iPads with A7-A11 bionic processor (see <https://checkra.in/>) and iOS 12.0 up to 14.2.0. You can enable option unsupported device support if you want to try the combination that is not supported.

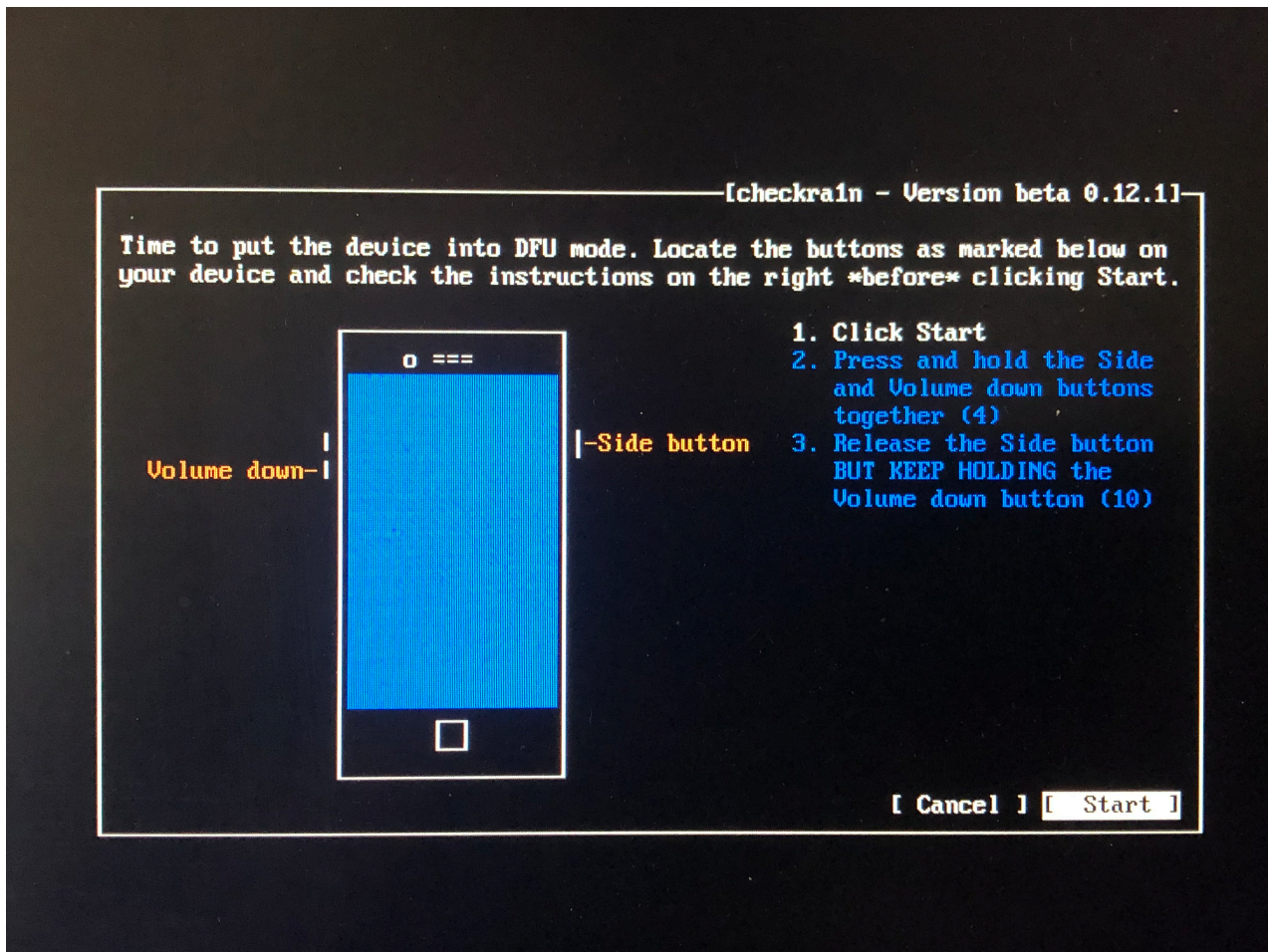
1. With Checkra1n running on your computer, connect your device via a Lightning cable and then click the Start button and select OK.



⚠ If the USB security is enabled in iOS device settings and the device was not connected to any computer for more than one hour, you will need to unlock the device or put it manually to restore mode, otherwise, it will not be detected by checkra1n.

i It is recommended to use the standard Lightning to USB Cable. Do not use any USB hubs (only USB-C to USB-A adapter if needed).

2. Select “Next” and then proceed with the instructions that the app gives you. This will result in your device going into DFU Mode.



3. Checkra1n will essentially take over the process once it detects the device in DFU Mode. The iPhone or iPad will reboot a few times during the process so don't get concerned when that happens.

4. When you are finally told that the process is finished, you can unplug the Lightning cable and tap the checkra1n app on your device to launch the app.



- Checkra1n is a **semi-tethered jailbreak** where the device is able to start up on its own, but it will no longer have a patched kernel, and therefore will not be able to run modified code. It will, however, still be usable for normal functions, just like stock iOS, unlike a **tethered jailbreak**, which would not boot at all. You can read more about jailbreaking iOS device [here](#)(see page 100).

i Don't forget to reenable your secure boot, or windows might not start.

2.22 Damaged/broken phone data extraction

In order to obtain any data from a phone using our products, it is necessary to have the phone connected to a PC - either by USB cable, Wi-Fi, or Bluetooth.

If the device has a damaged cable port and a traditional USB cable connection is not possible, you can try to connect with Bluetooth or Wi-Fi.

i USB cable connection is recommended in order to acquire maximum data; depending on the device manufacturer, Bluetooth and WI-Fi connection may only be able to yield limited or no data.

If the screen is damaged or is no longer responsive to touch, you can always use OTG to connect a PC mouse to the device. You can then use the mouse on the phone to navigate the device settings (just like a mouse is used with a PC) in order to enable [USB debugging](#)(see page 139) or [OEM unlock](#)(see page 46) in developer options. The [OTG³⁷](#) option only applies to Android devices.

³⁷ https://en.wikipedia.org/wiki/USB_On-The-Go

If you are unsure your phone will connect prior to purchasing MOBILedit Forensic Express, read more about supported phones [here](#)³⁸.

 Please, do not hesitate to [contact us](#)³⁹ if you need more support.

2.23 Supported phones in Unlocking database

Digital evidence is often a key factor in criminal investigations today. Lawful access to digital evidence can mean the difference between discovering the truth and a criminal investigation remaining unsolved.

MOBILedit in a new released 8 version brings a new improved phone unlocking feature.

MOBILedit support the most popular manufactures.

A detailed list of all supported phones you can see as a paying customer ([HERE](#))

The following is a list of brands and systems to illustrate our wide range of supported phones. Thousands of phone models are supported.

- 360
- 5Star
- Accent
- Ace
- Agetel
- AGM
- Alcatel
- ANS
- Apple
- Archos
- Ark
- ASUS
- Blackphone
- BLU
- BQ
- Brondi
- Casper
- CAT
- Cellatel
- Cherry
- China Mobile
- Colors
- Condor
- Coolpad
- Cyrus
- DEXP
- Doogee
- ELEPHONE
- Energy
- Evercoss
- General Mobile

³⁸ <http://www.mobiledit.com/phones/>

³⁹ <http://www.mobiledit.com/contact>

- Gigabyte
- Gionee
- Google
- Gphone
- Haier
- Highscreen
- Hisense
- Honor
- Hotwav
- HTC
- Huawei
- Hyundai
- iCALL
- IKU
- Impression
- Infinix
- Inoi
- Intex
- Itel
- Jio
- Jivi
- Kara
- Karbonn
- Konrow
- K-Touch
- Kudae
- Lanix
- Lava
- Lenovo
- Lephone
- LeTV
- LG
- LYF
- M4
- Maximum
- Maximus
- Maxvi
- Meizu
- Micromax
- Mifaso
- Mobicel
- Motorola
- Myfon
- Nobby
- Nokia
- OnePlus
- OPPO
- Otho
- Panasonic
- Phicomm
- POCO
- Polaroid
- Positivo

- Prestigio
- PT Mobile
- Qmi
- QMobile
- Rivo
- Samsung
- Siragon
- Smartfren
- Smartisan
- Starlight
- Stylus
- Swipe
- Symphony
- TCL
- Tecno
- Texet
- True Smart
- Versus
- Vertex
- Vestel
- Vivo
- Vodafone
- Walton
- WE
- Wiko
- Wileyfox
- Winstar
- Woo
- Xiaomi
- XOLO
- Yuho
- Yusun
- Zelta
- Ziox
- ZTE



Please note that this list is incomplete. "NOT LISTED" does not necessarily mean "NOT SUPPORTED".

3 Connecting a device

MOBILedit Forensic Express supports a wide variety of Android phones except for some special, incompatible or rare models. All iPhone models without exception. Windows Phones only with limited possibilities and most feature phones.

The following guides based on specific operation systems will explain everything you need to know in order to successfully connect your phone to MOBILedit Forensic Express.

 Download our printable instruction sheet [here](#)⁴⁰.

3.1 Supported phones

MOBILedit supports all of the major brands and models. We do not have a list of specific supported phones, since there is almost every day a new phone released on the market.

3.1.1 MOBILedit supports:

- All Android phones except some special, incompatible or rare models
- All iPhone models
- Windows Phones with limited possibilities
- KaiOS feature phones including Nokia, JioPhone, Alcatel, Positivo, etc.

 In case you'll have more questions, don't hesitate to contact us [here](#)⁴¹.

3.2 Device connection screen

- [iOS](#)(see page 113)
- [Android](#)(see page 113)

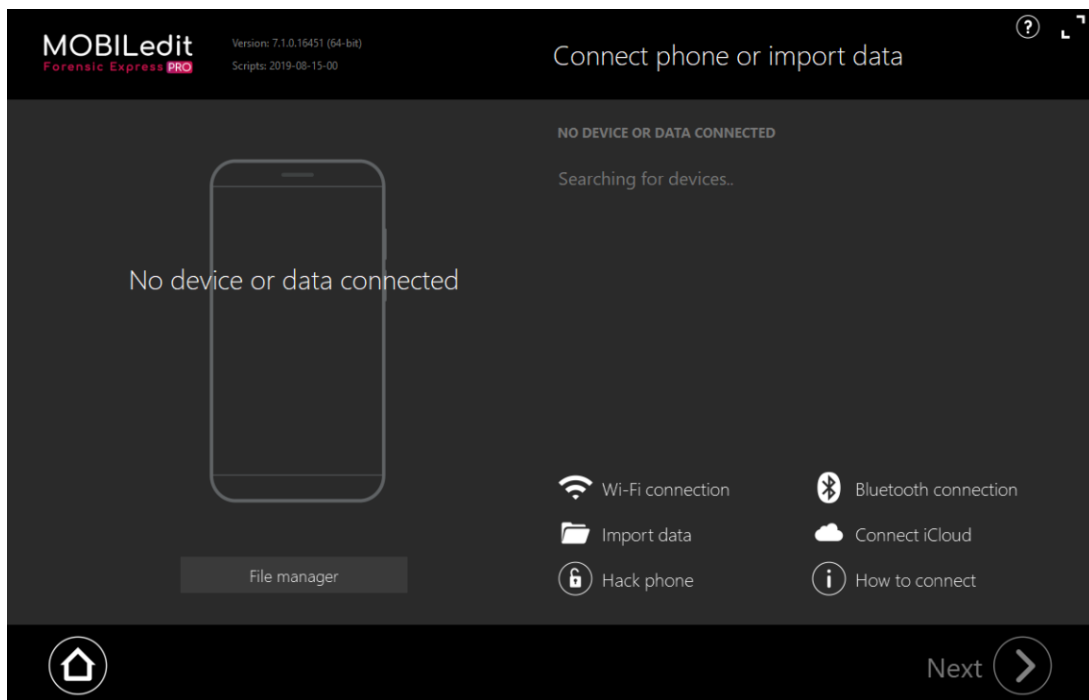
The device connection screen displays all connected devices. Once the device is connected successfully, MOBILedit comes up with the automatic phone detection feature which makes it easy to use.


If the device still does not appear to be connected, we suggest to check the USB connection and install the preferred phone drivers available for download [here](#)⁴².

⁴⁰ <http://download.mobiledit.com/documents/Connection%20sheet%20A4%20Europe.pdf>

⁴¹ <https://www.mobiledit.com/contact>

⁴² <https://www.mobiledit.com/download-list/phone-drivers>



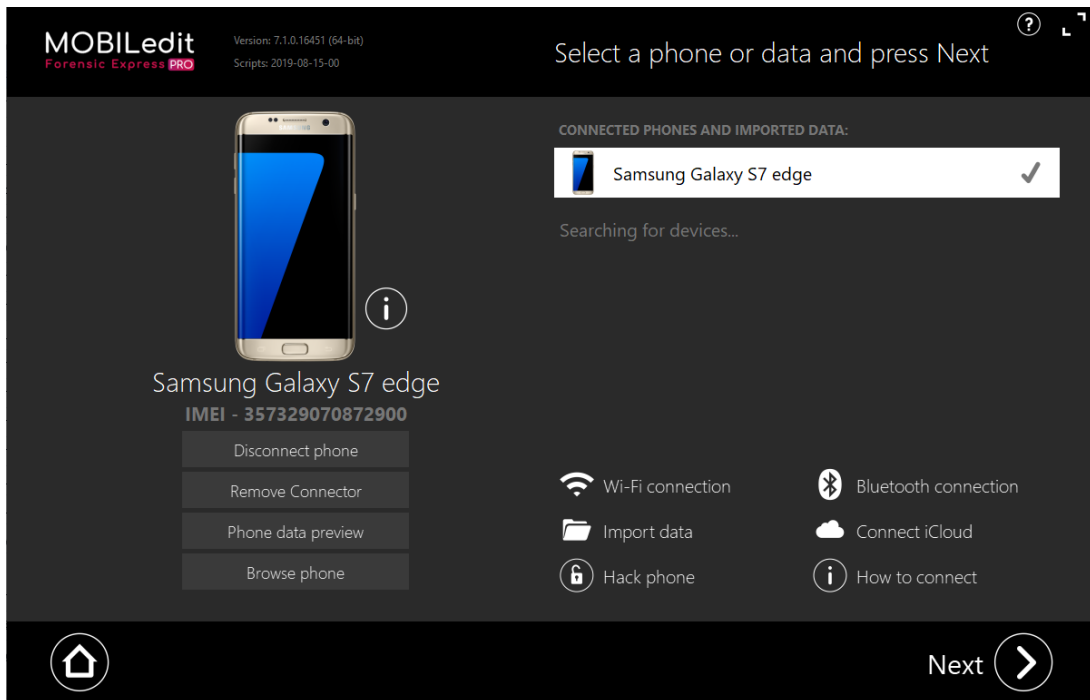
 Learn more about connecting a phone at '[How to connect phone](#)'(see page 114).

3.2.1 iOS

While connecting iOS device, there will be a pop-up message on the screen, select "Trust" and iOS device will appear connected on the MOBILedit Forensics program home page

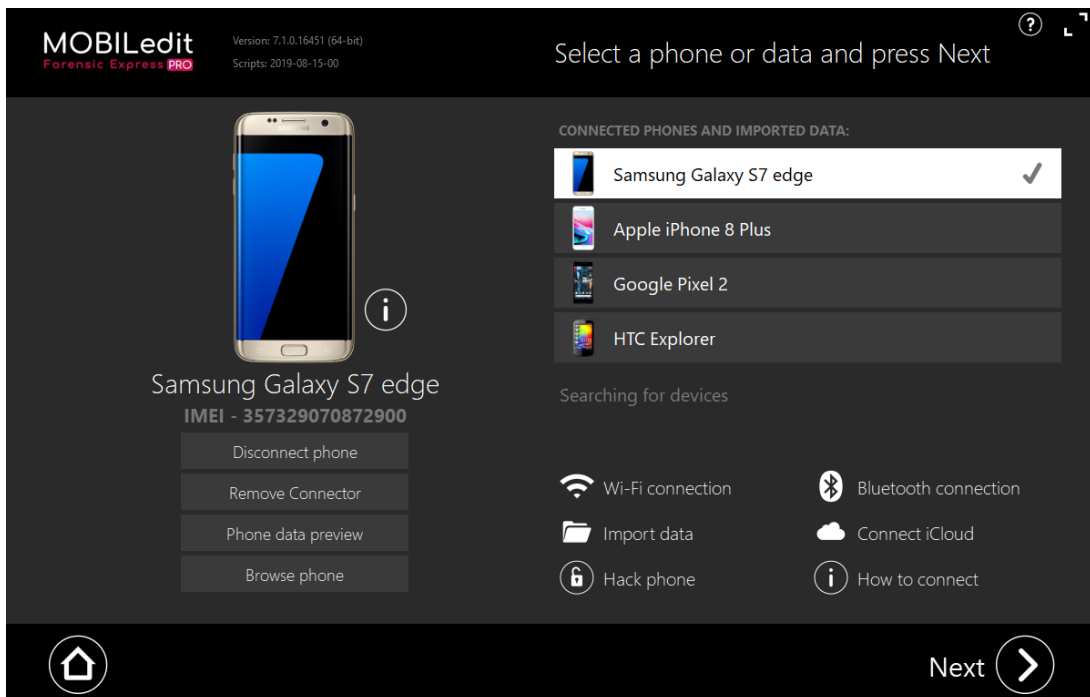
3.2.2 Android

While connecting, you will see the USB debugging pop-up message on the screen, select "Allow" and the device will appear connected on the MOBILedit Forensics program home page.



You can also connect multiple devices to MOBILedit Forensic Express.

You don't have to wait for the device extraction to get completed and you can easily start with another extraction at the same time by just clicking over the connection page.



3.3 Connection wizard

- [“How to connect” wizard](#)(see page 115)

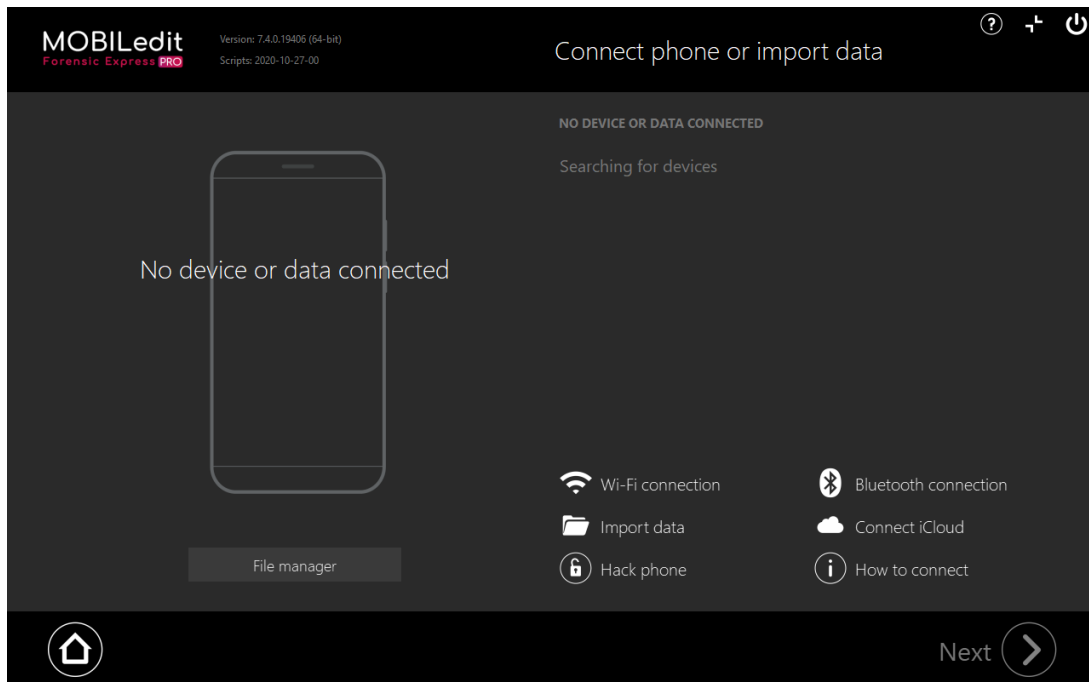
- [Android](#)(see page 118)
 - [Cable connection](#)(see page 119)
 - [Wi-Fi connection](#)(see page 125)
- [iPhone](#)(see page 127)
 - [Cable connection](#)(see page 128)
 - [Wi-Fi connection](#)(see page 133)
- [Windows Phone](#)(see page 134)
- [Other phones](#)(see page 136)

The phone connection wizard will guide you through simple to follow instructions allowing even a novice to work with the product. It also eliminates stress by showing you which setting you need and what buttons to press to make sure your phone connects every time.

If a phone connected to the computer was not auto-detected by the program, you can manually connect it with the help of the connection wizard.

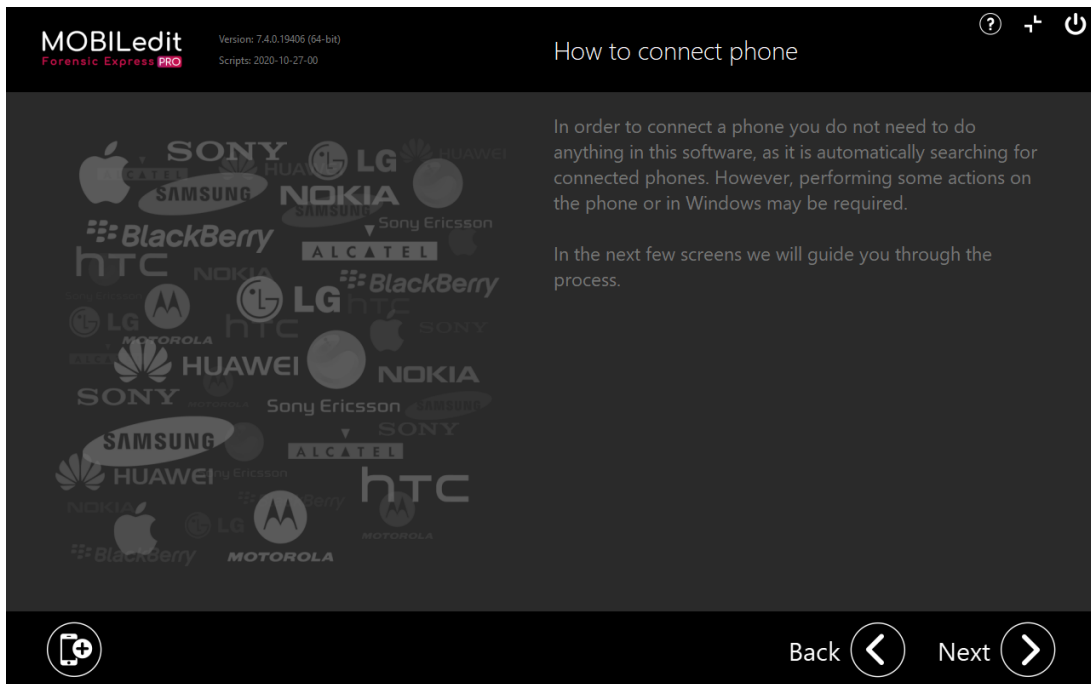
3.3.1 “How to connect” wizard

On the intro screen, select the **"i"** button - **How to connect phone**.

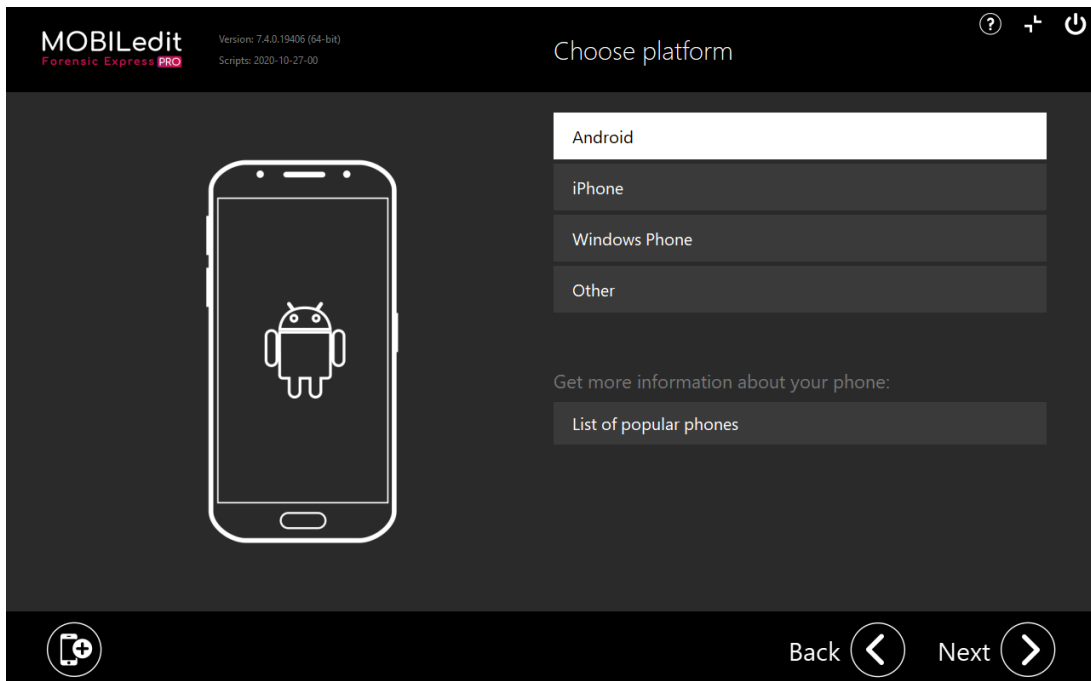


The next screen will indicate that the program should auto-detect all phones; however, there could be some problems with drivers or phone settings, preventing auto-detection.

If the connected phone still has not appeared on the intro screen, please click on the **"Next"** button and let the connection wizard help you with connecting the phone manually.



In the next step, you will choose the platform (operating system) of the phone. The options are the following: Android, iPhone, Windows Phone, Other (feature phones, etc.).

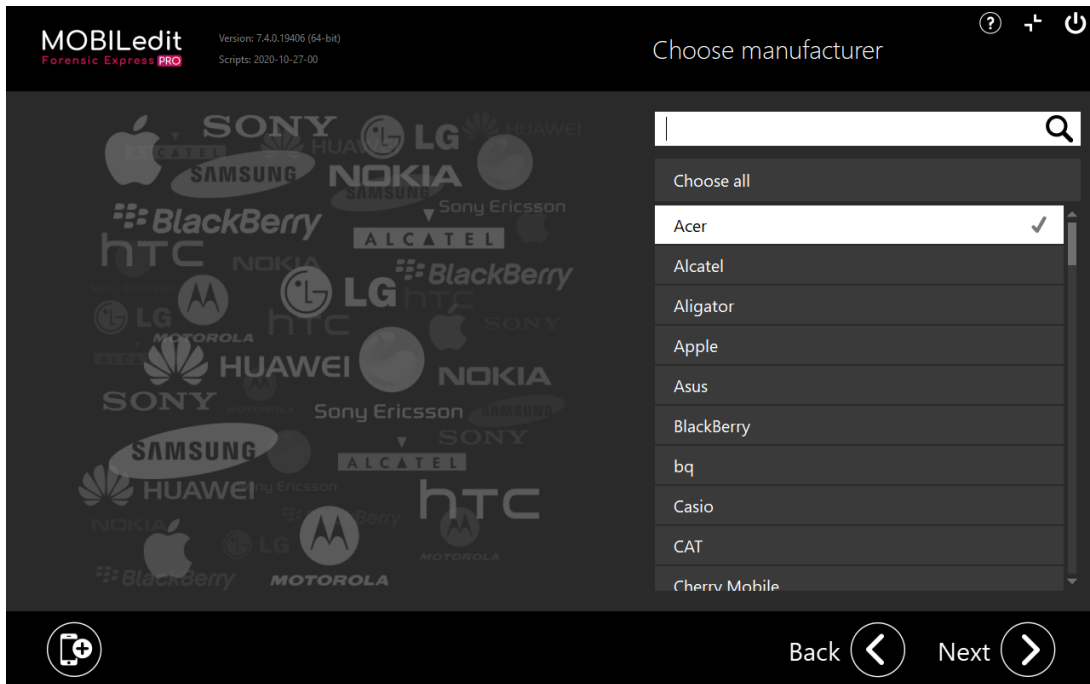


Near the bottom of the page, there is also an option ('List of popular phones') that will help you get more information about the phone to be connected.

This option should be selected if you are not sure which platform/operating system, the connected phone works on

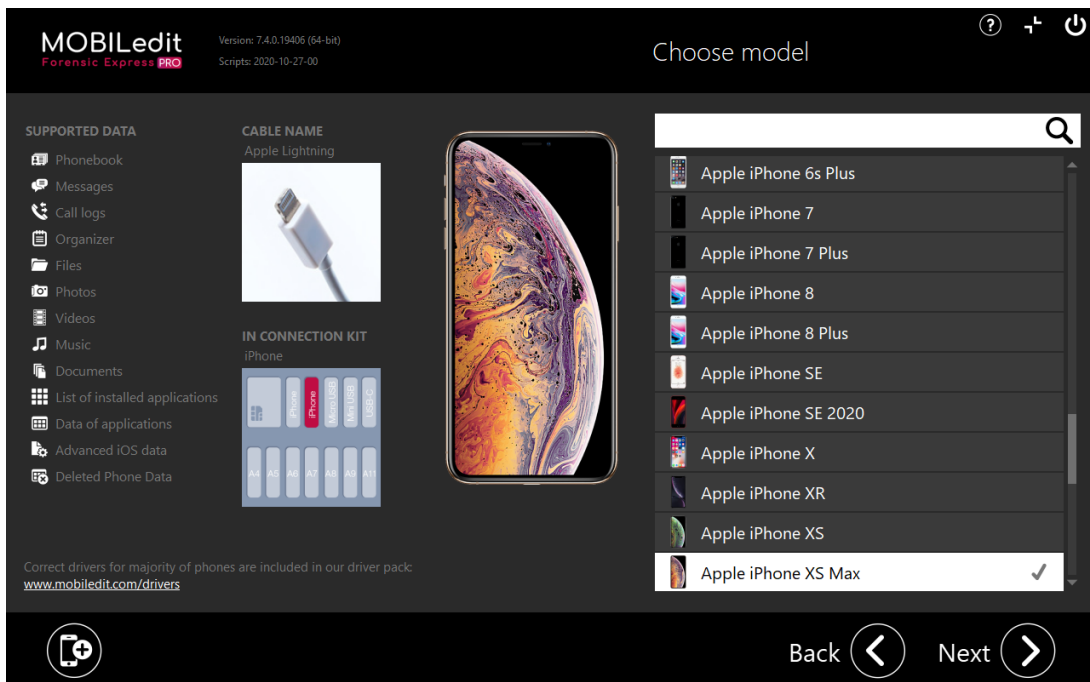
or when more detailed information is needed.

After clicking on it, there is an option to choose the specific manufacturer of the connected device on the next page.



Selecting a particular phone manufacturer will provide a list of all supported devices from that manufacturer. Also, "**Choose all**" can be selected, which will show a list of all supported devices.

Clicking on a specific device will show all detailed info about it, including a list of supported data and which cable from our Connection Kit (if you have the Kit) is the proper connection cable for the phone.

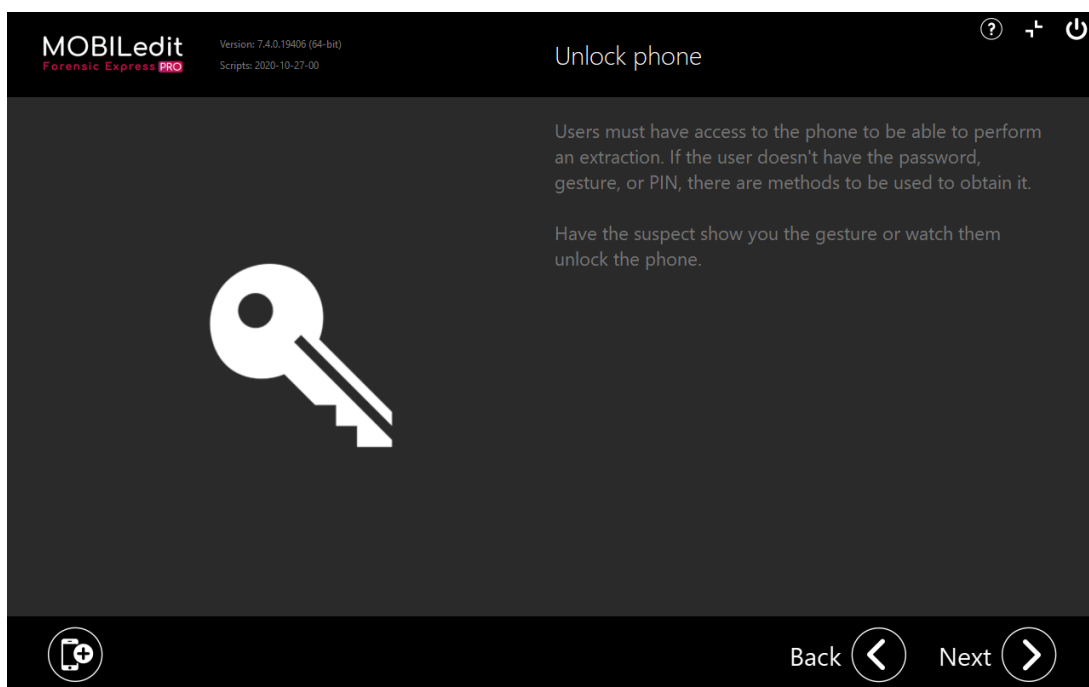


By clicking on the **"Next"** button now, you return to the "Choose platform" screen where you can select your phone's operating system platform. From here, select your platform and let the manual walk you through step by step.

Please note that the Bluetooth connection is not a part of the Connection Wizard since it's done rather differently and requires a direct connection between the PC and the phone, which cannot be established from within MOBILedit Forensic Express, nor the connector app but must be done in the Windows settings/options. More info on the BT connection could be found [here](#)(see page 153) for Android phones and [here](#)(see page 180) for Windows Phones.

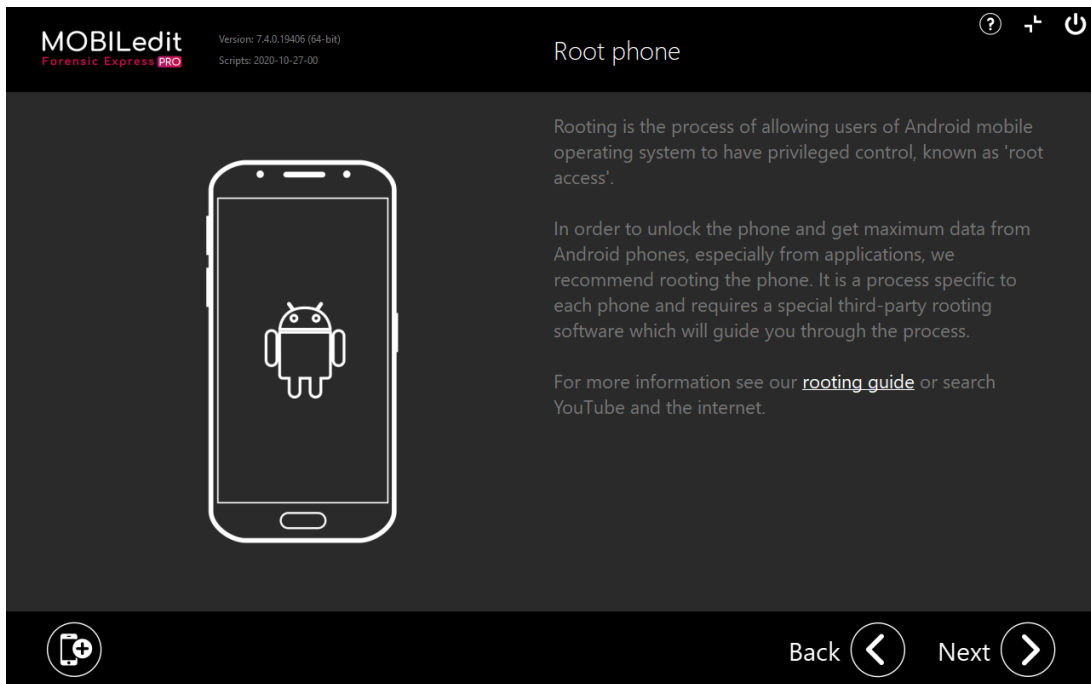
3.3.2 Android

The first screen of the Android connection wizard shows a warning that unlocking the phone is essential for data extraction. Please have the phone unlocked.

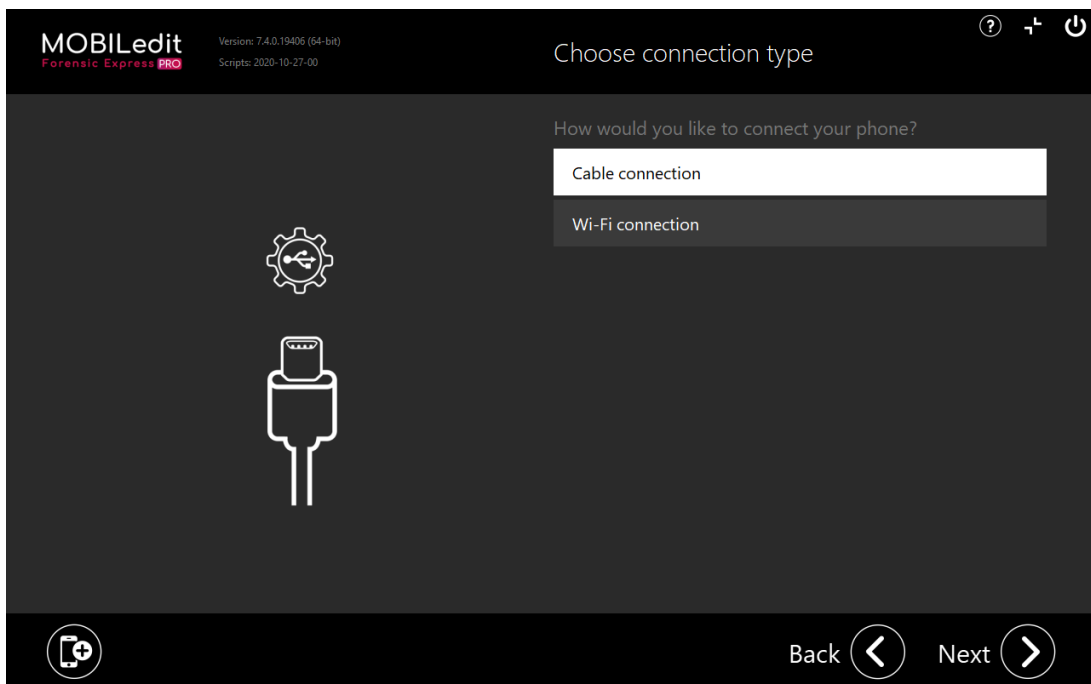


The next screen shows all info about rooting the device, which is a highly recommended step for Android devices because in most cases rooting the device will provide much more data from the phone.

More detailed info on how to root an Android phone is available [here](#)(see page 68).

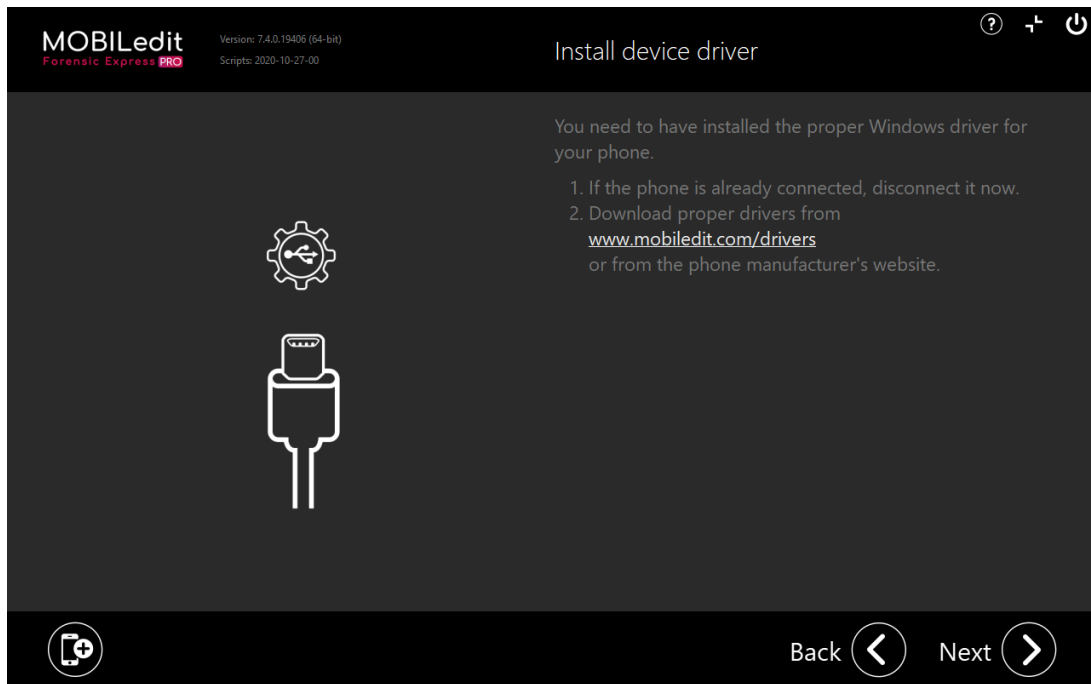


The next step allows the user to choose between the USB cable and Wi-Fi connection of the phone.

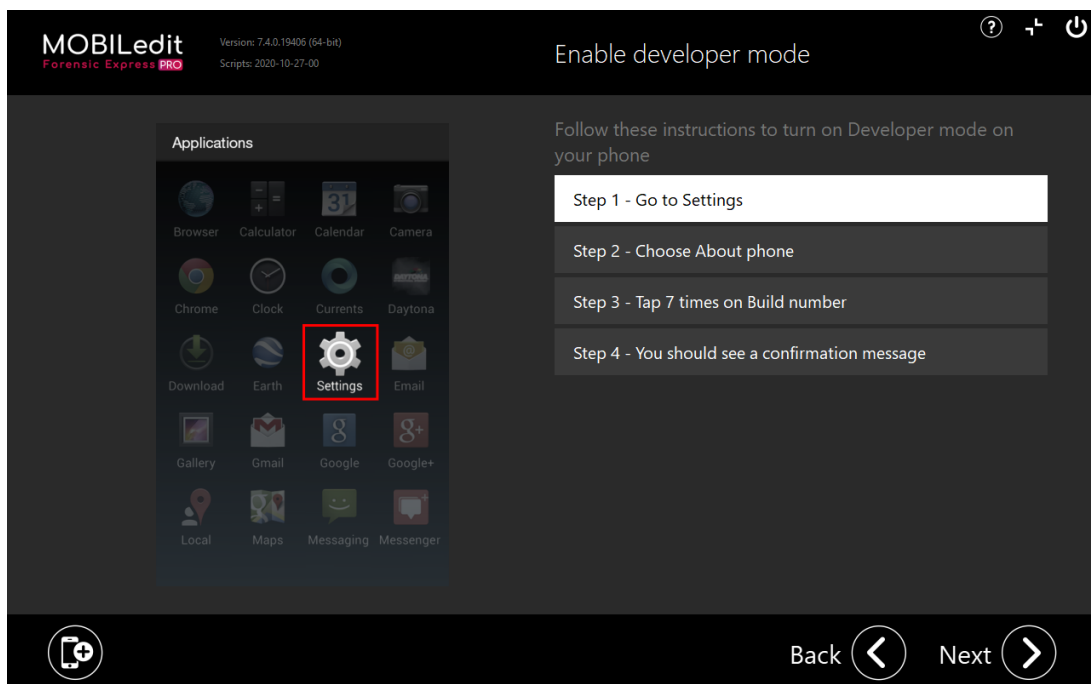


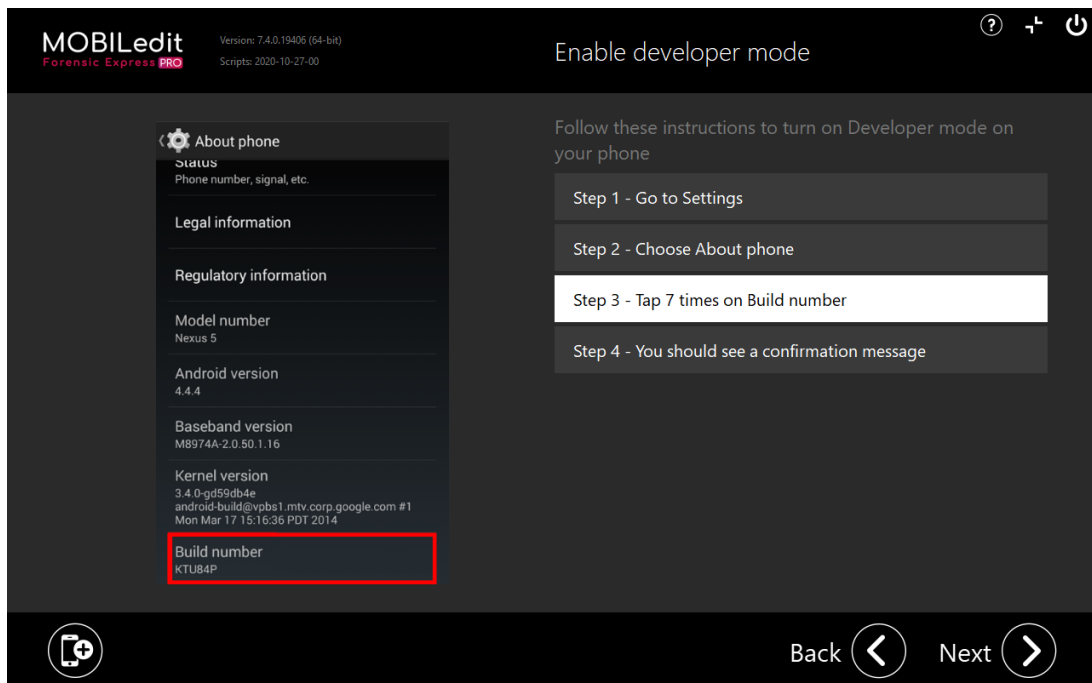
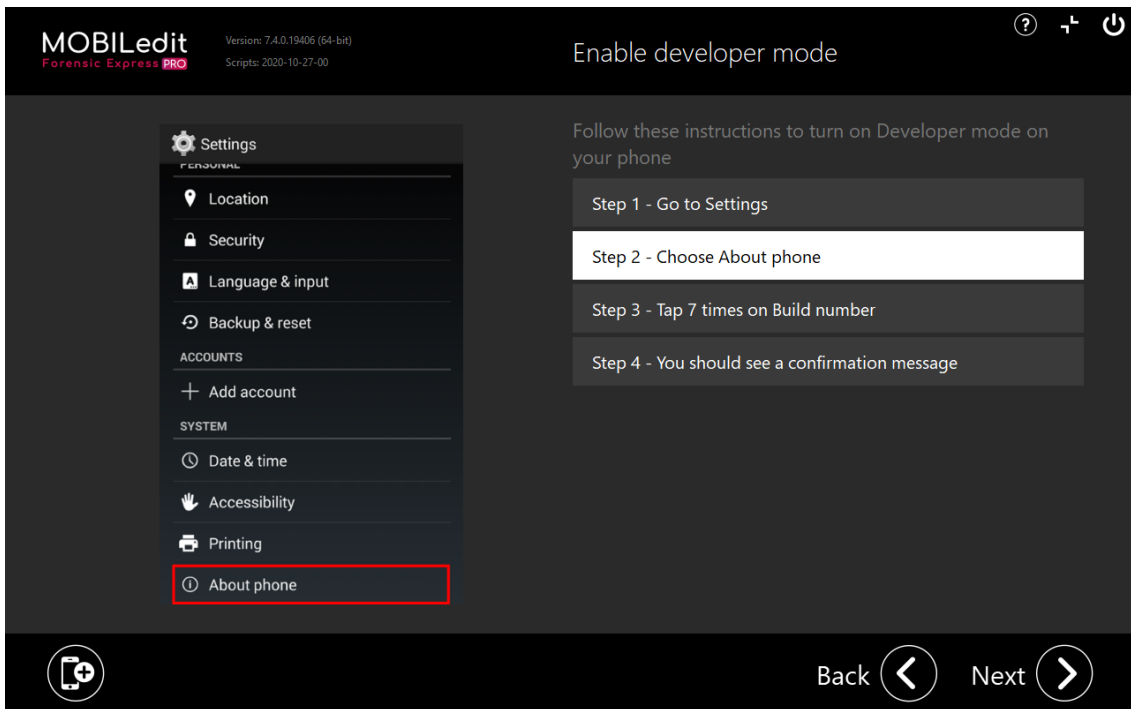
3.3.2.1 Cable connection

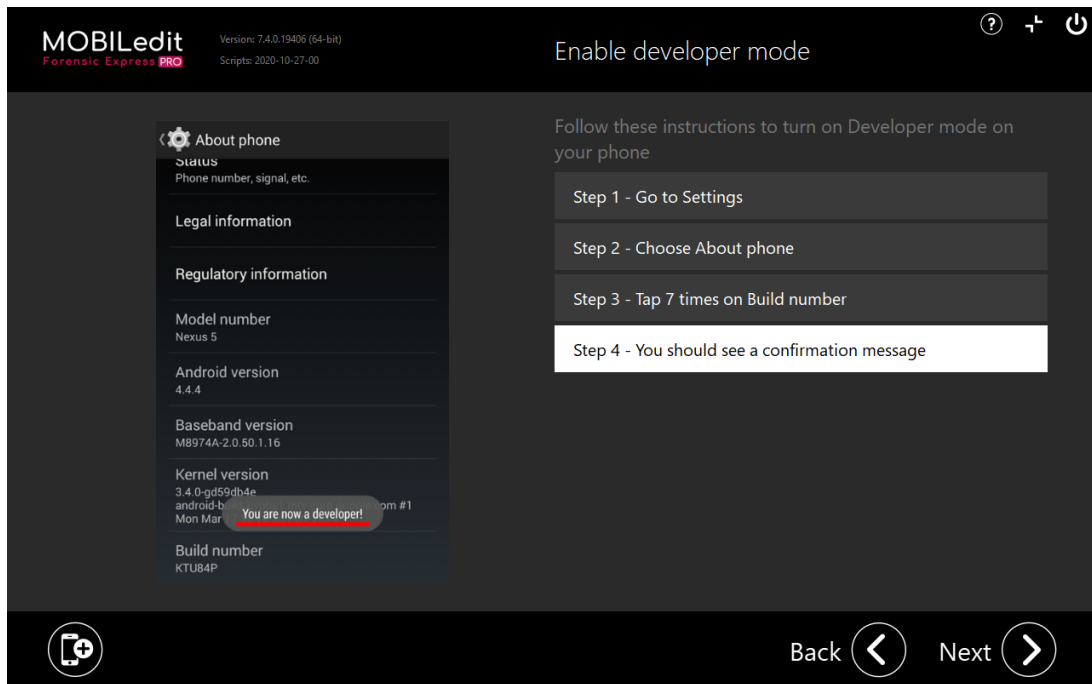
The first screen of the cable connection wizard asks the user to download and install the proper drivers for the phone. This step is absolutely necessary for the phone to work correctly with the program.



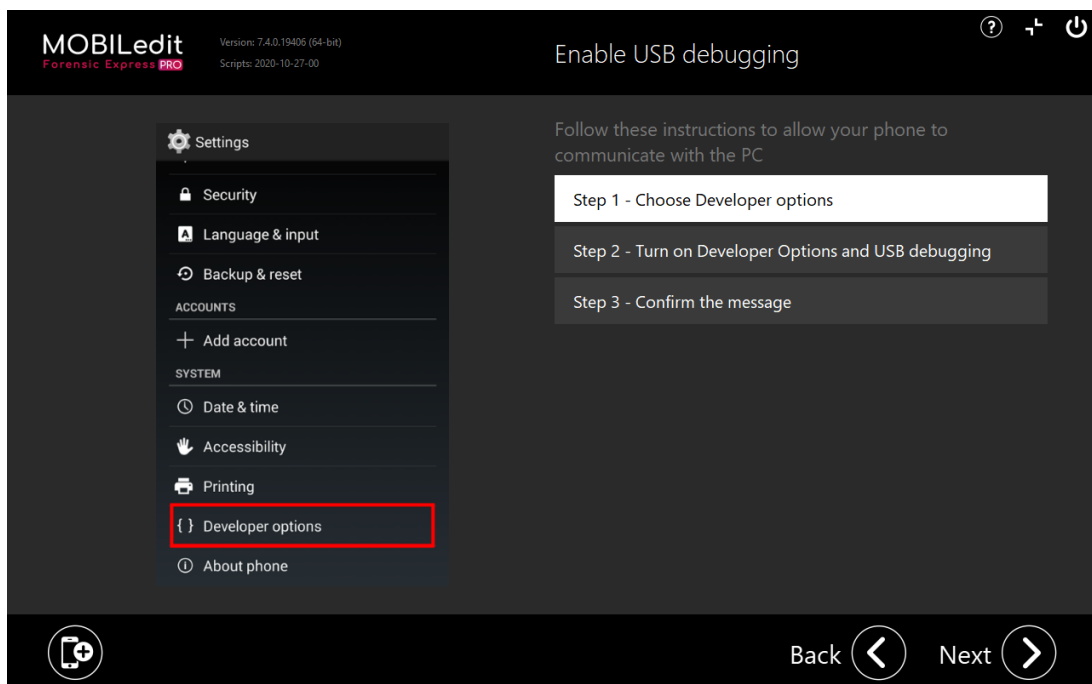
The next few screens will guide the user on how to enable the Developer options on the device, which is required for a proper working connection.

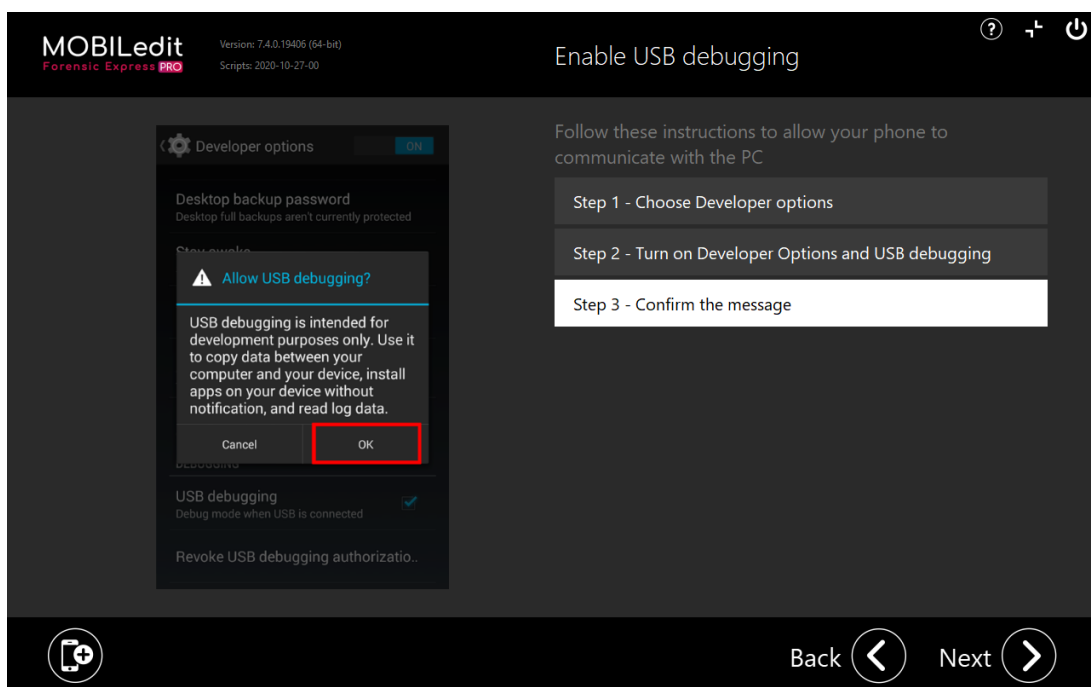
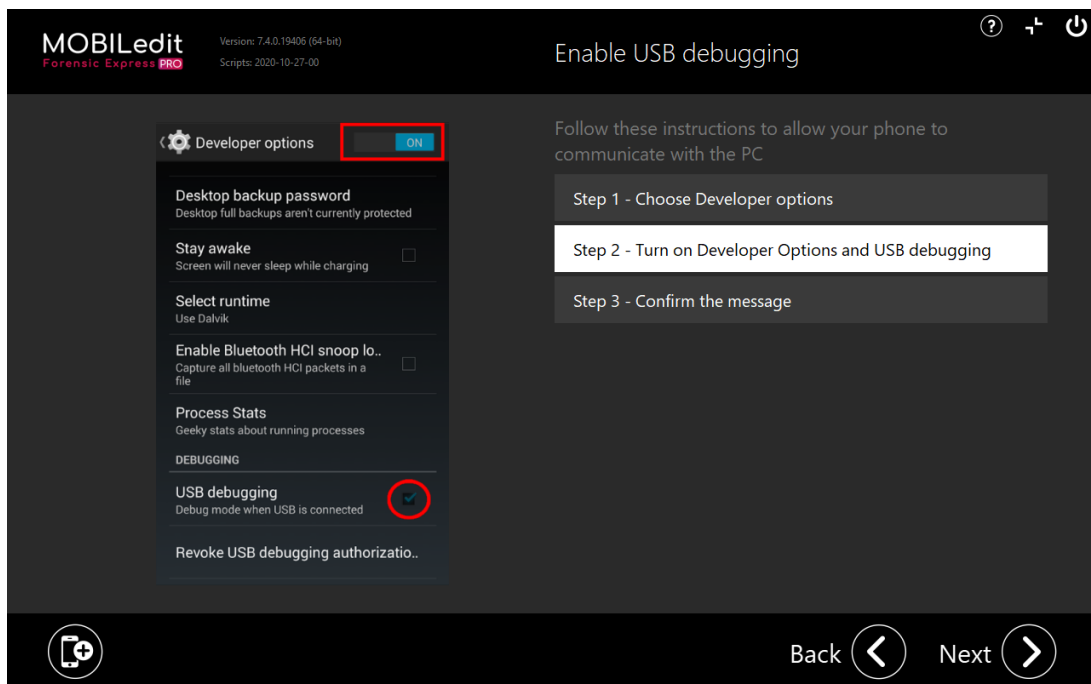




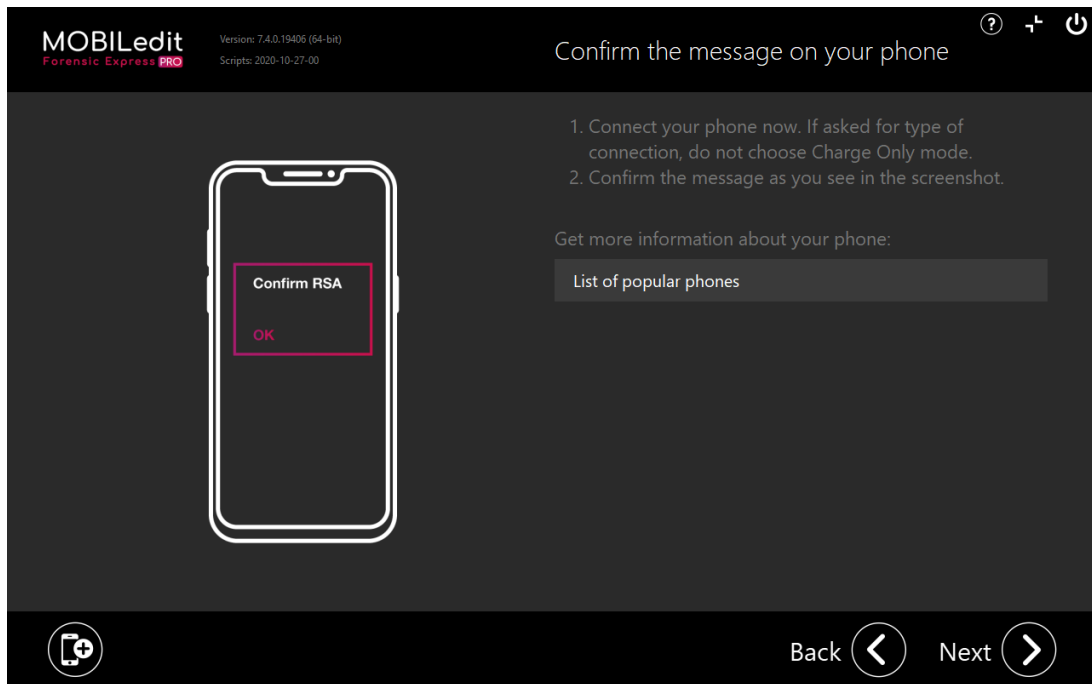


After enabling developer mode click the **"Next"** button and proceed with the next few steps about how to enable USB debugging on the phone, which will provide stable and working communication between the phone and the computer.

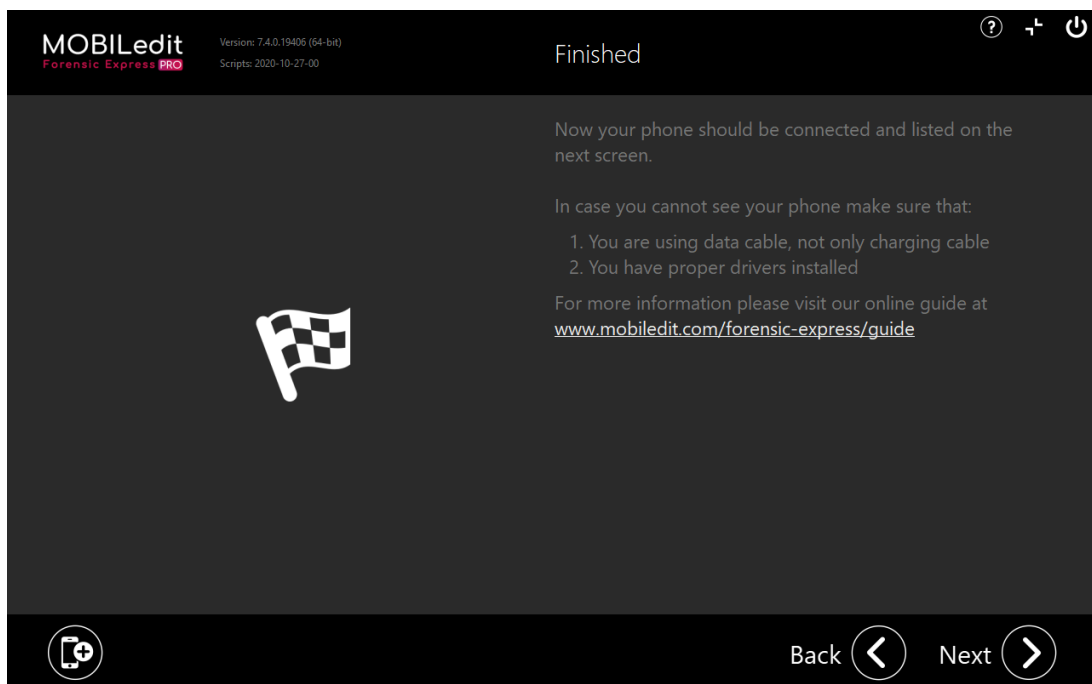




The last step of the Android connection wizard asks the user to allow the RSA confirmation and to choose either the PTP or MTP communication protocol - choosing either option is ok. Please note that "Charge only" should not be selected because no data will be obtained from the phone when connected in this way.

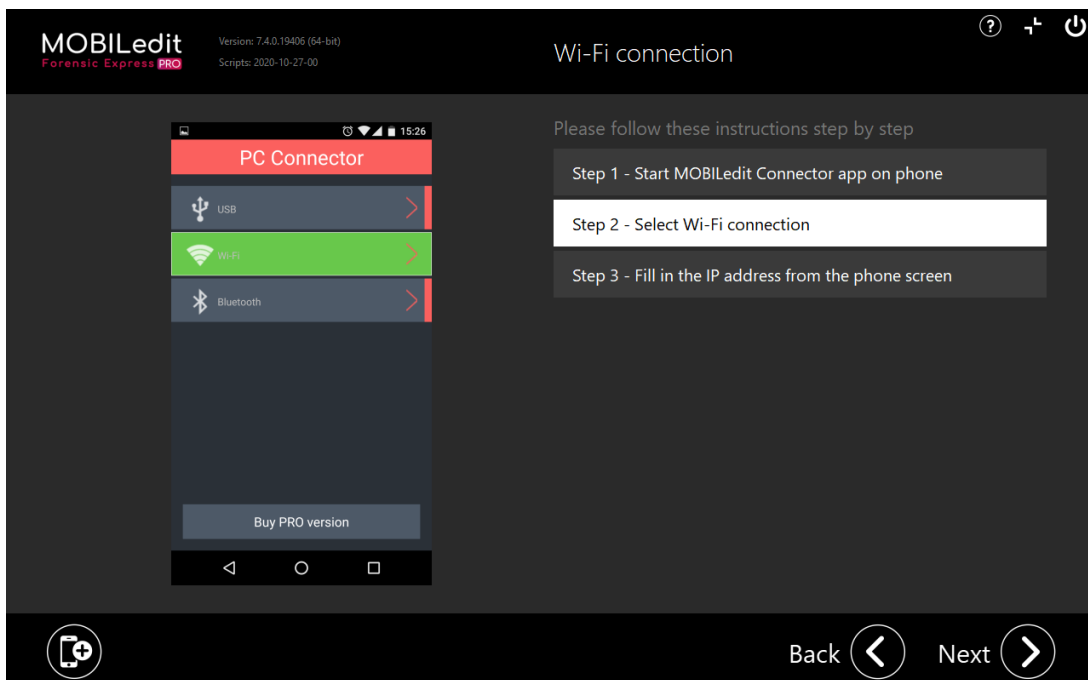
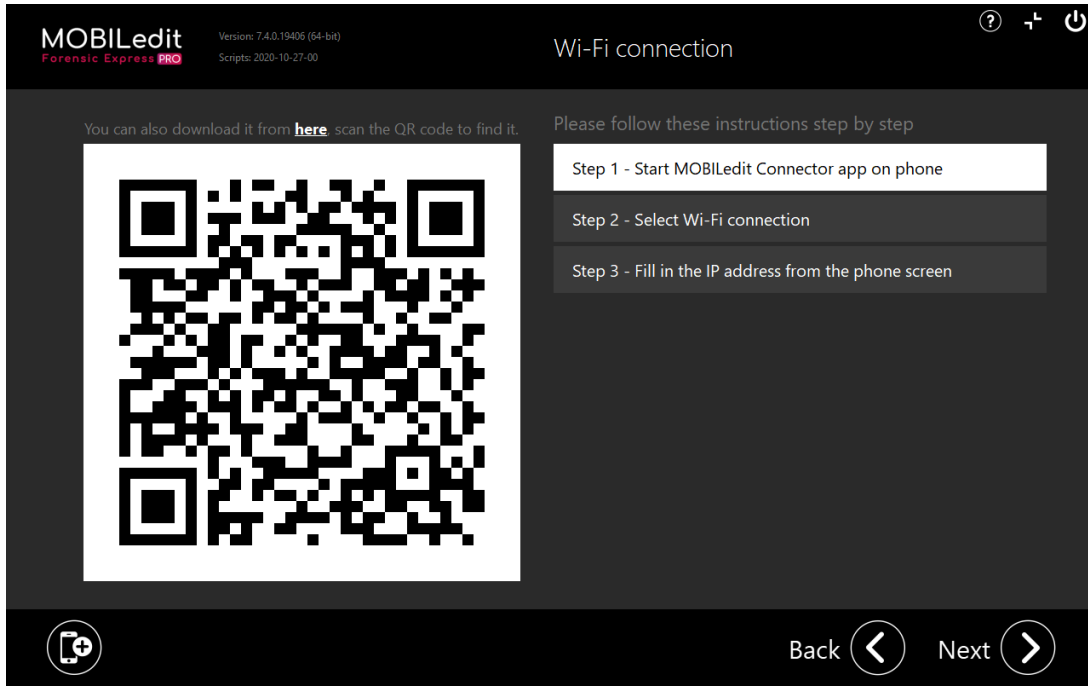


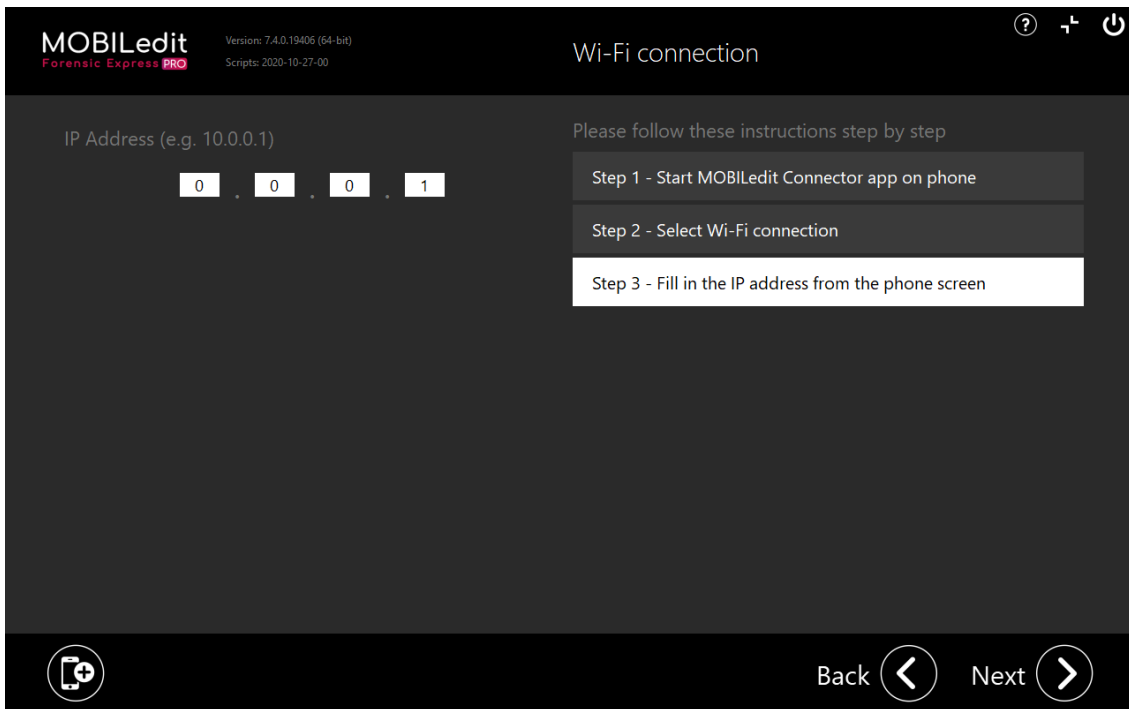
The phone should now be connected properly. If you have not successfully connected, the last screen of the wizard will offer tips that could give you a reason for the phone not connecting to MOBILedit Forensic Express. This page also provides a link to a more detailed web-manual.



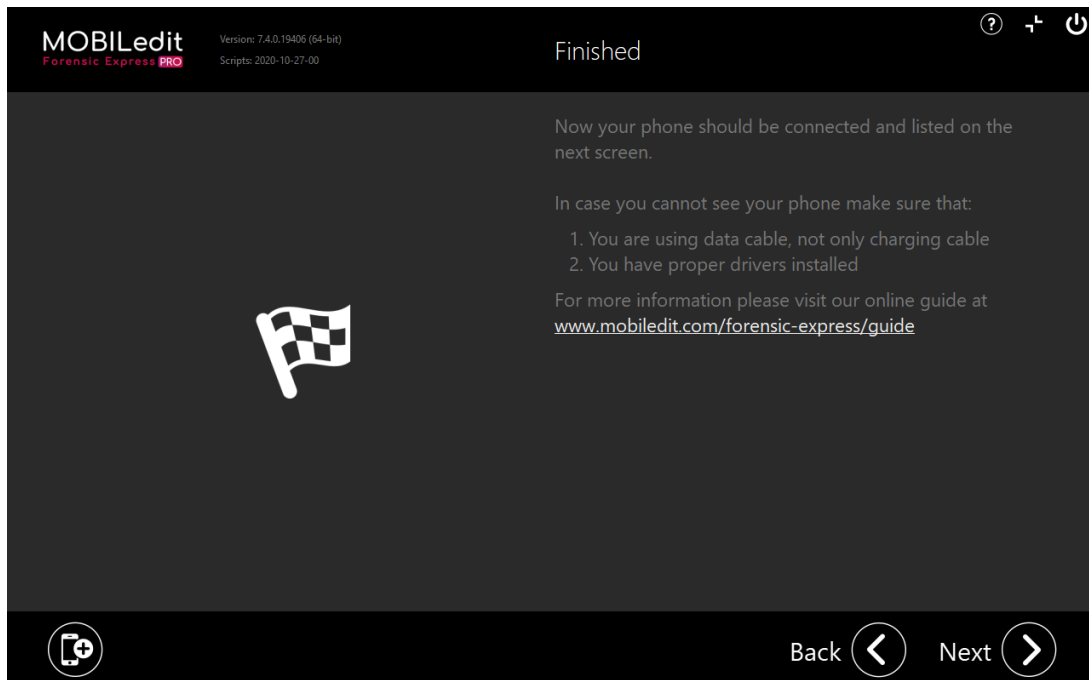
3.3.2.2 Wi-Fi connection

To connect a phone via Wi-Fi, the user will first have to install the "Connector App". The first few steps of the wizard will tell the user how to download it and how to work with it, so a proper connection can be established.



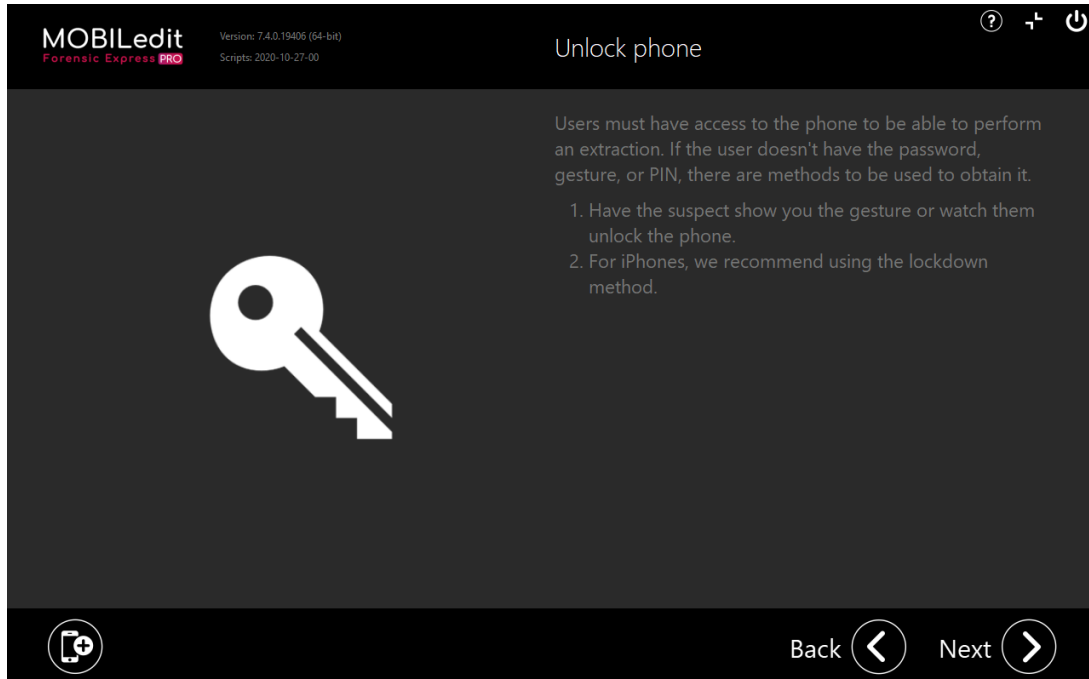


After the IP address is filled in correctly, the phone should be connected and visible on the intro screen. If it isn't, the last screen of the wizard will provide tips that could give you a reason for the phone not connecting to MOBILedit Forensic Express. This page also provides a link to a more detailed web-manual.



3.3.3 iPhone

The first screen of the iPhone connection wizard shows a warning that unlocking the phone is essential for data extraction. Please have the phone unlocked.



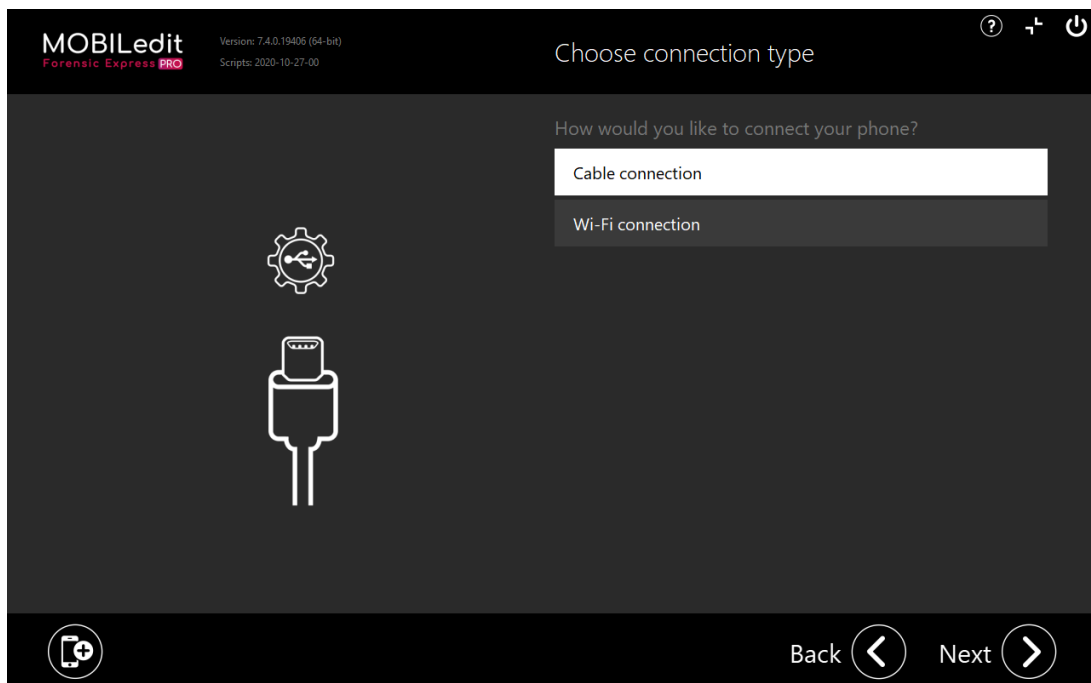
The next screen shows all info about jailbreaking the device, which is a highly recommended step for iOS devices because, in most cases, jailbreaking will provide much more data from the phone.

More info on how to jailbreak an iPhone is available [here](#)(see page 100).

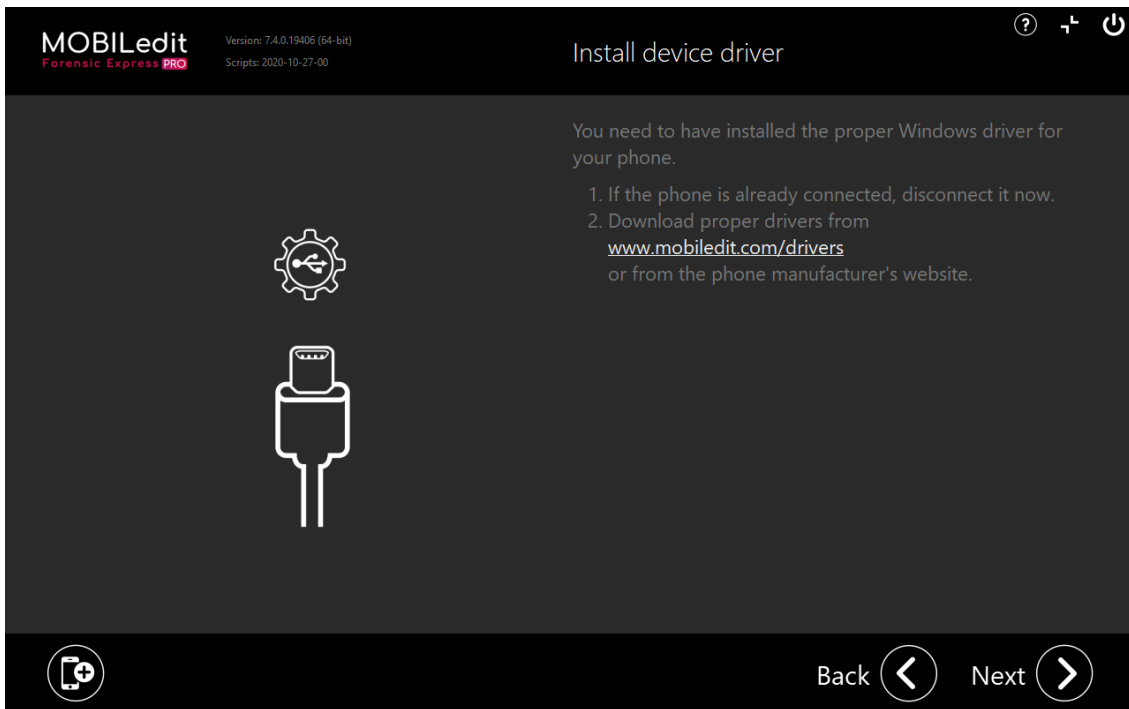


The next step allows the user to choose between USB cable and Wi-Fi connection of the phone.

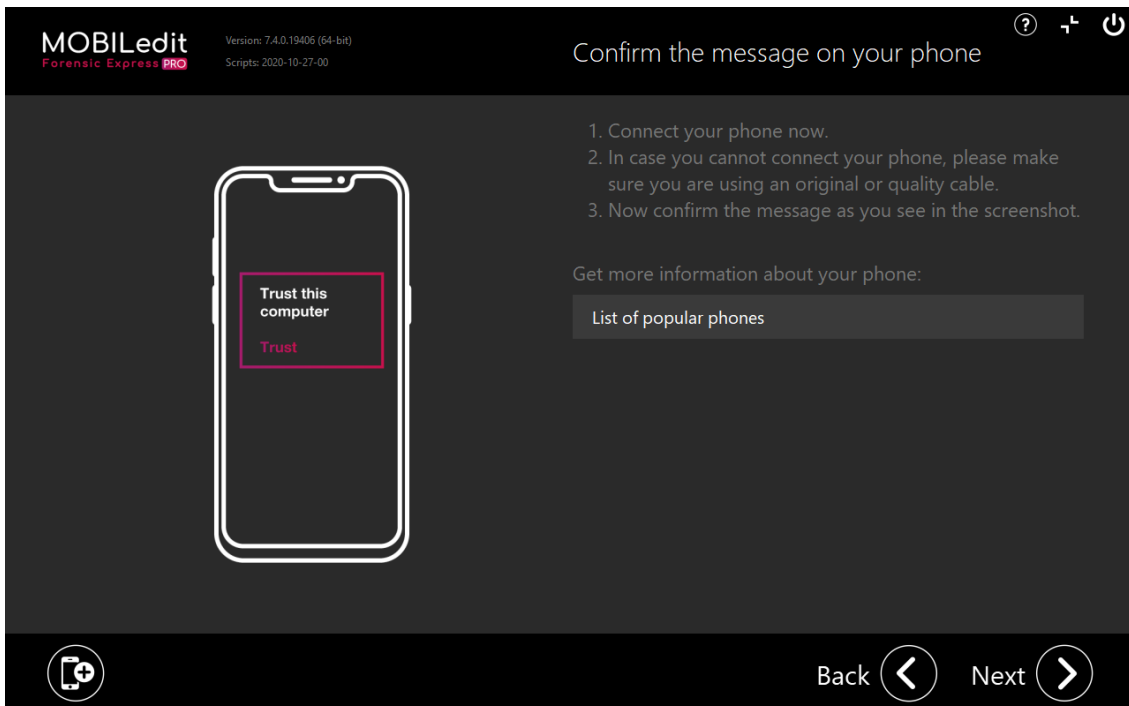
3.3.3.1 Cable connection



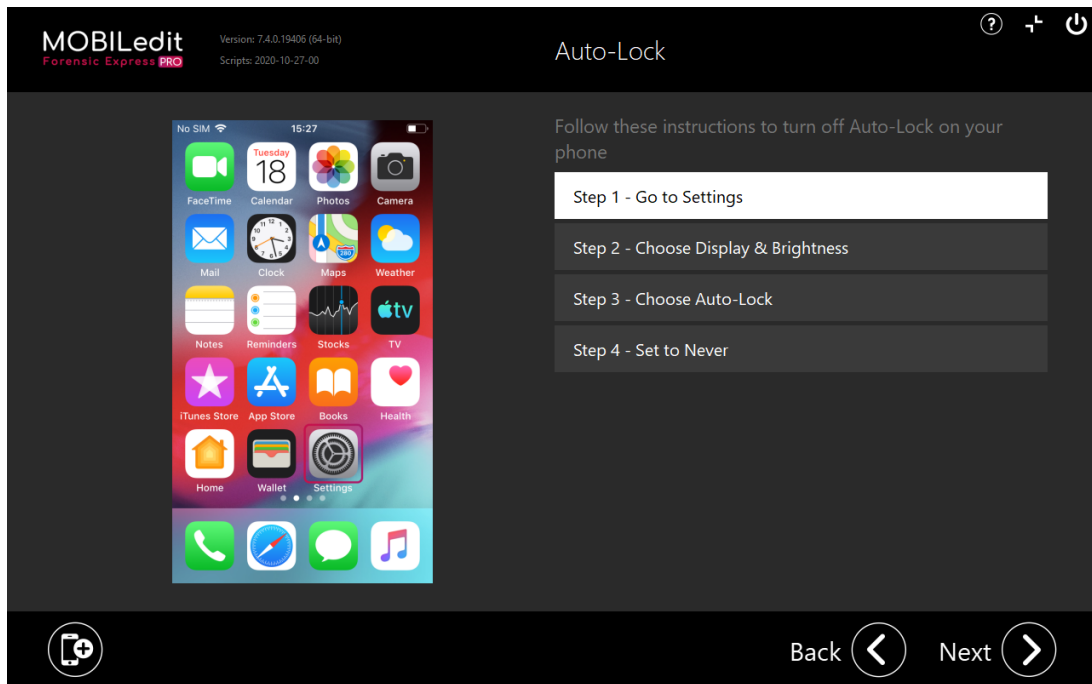
1. Install the Windows drivers:



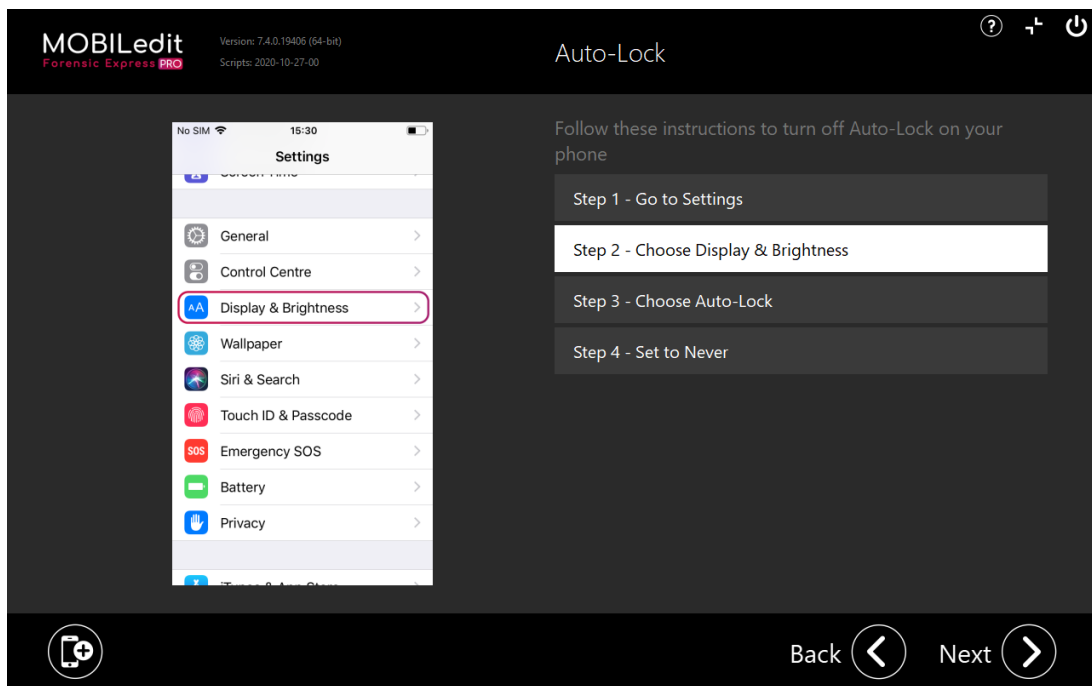
2. Confirm the trust message on the device's screen.



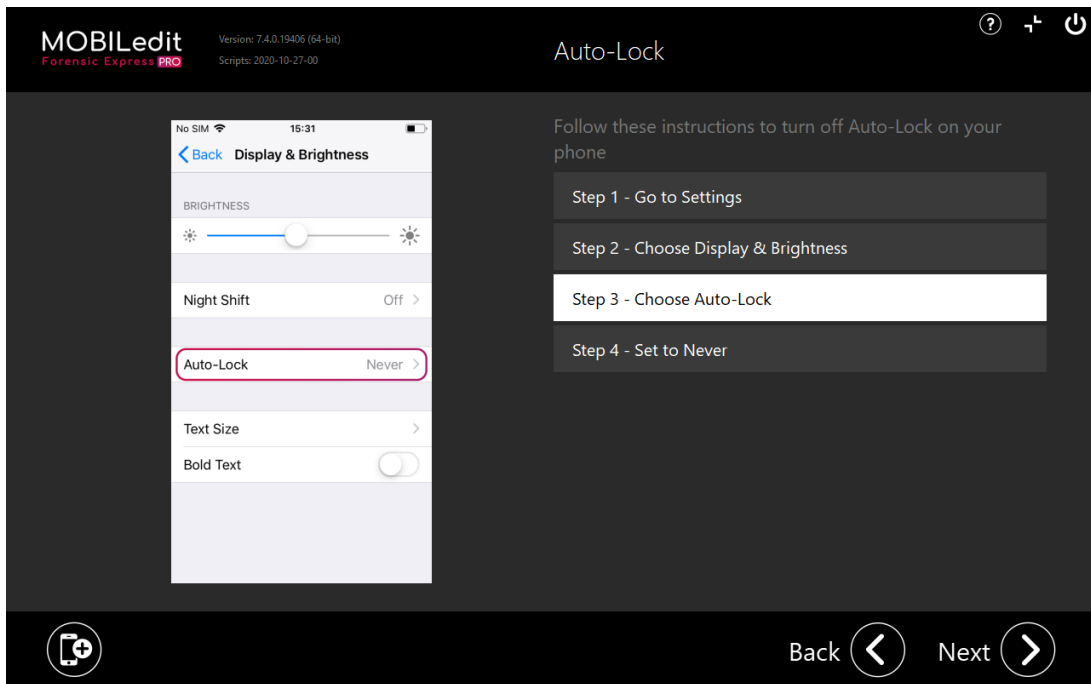
3. Go to Settings.



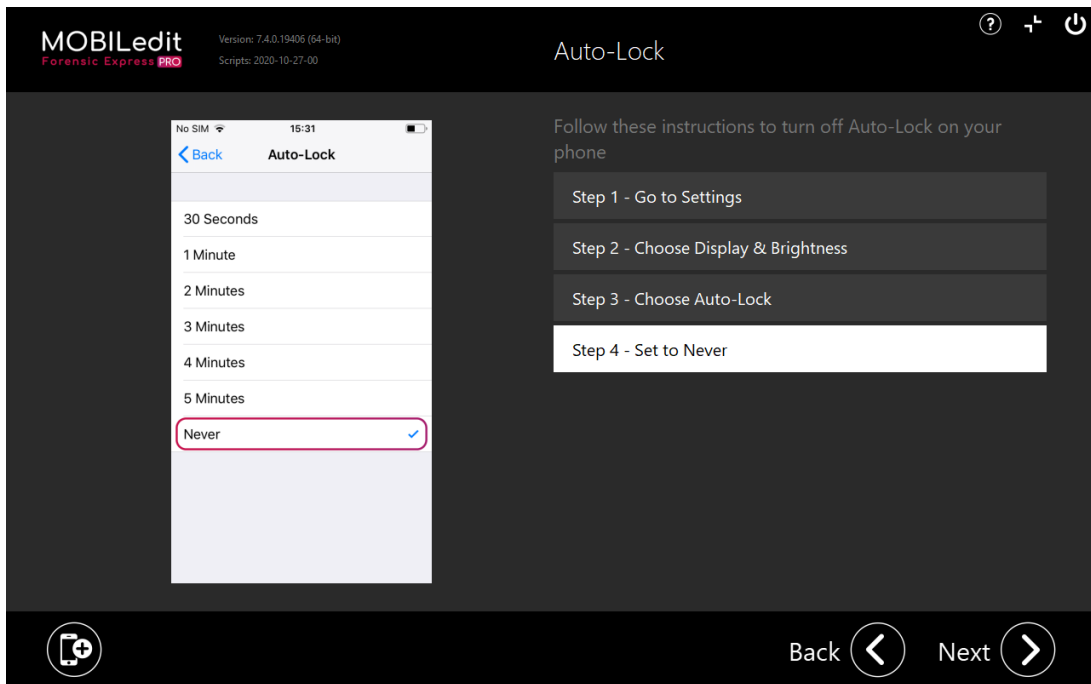
4. Choose Display & Brightness.

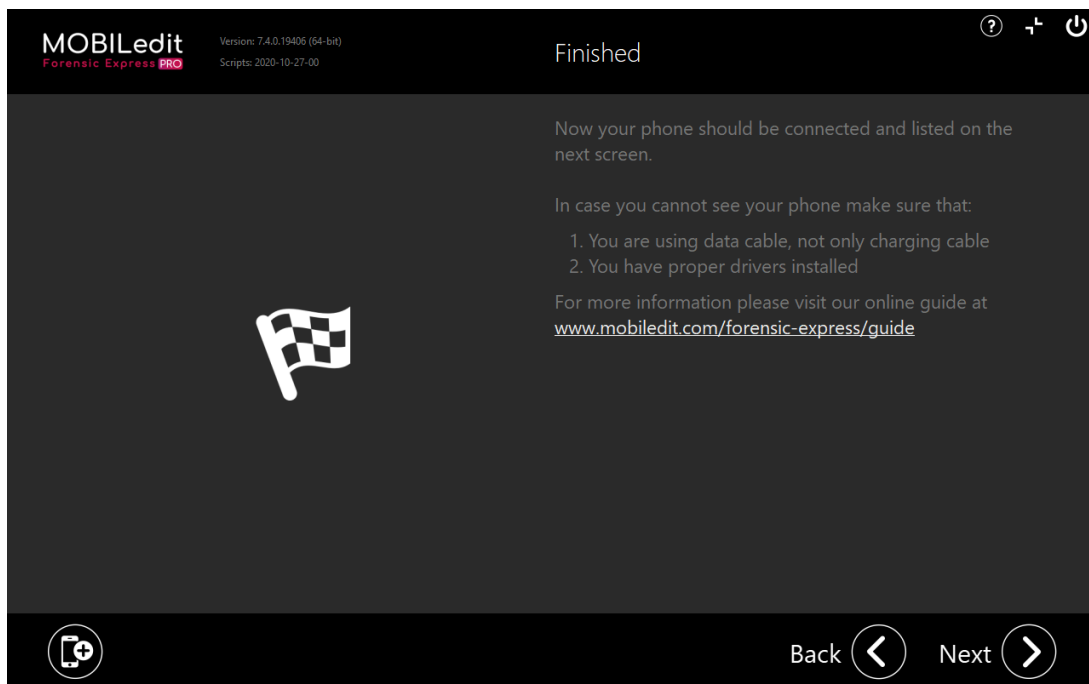


5. Choose Auto-Lock.

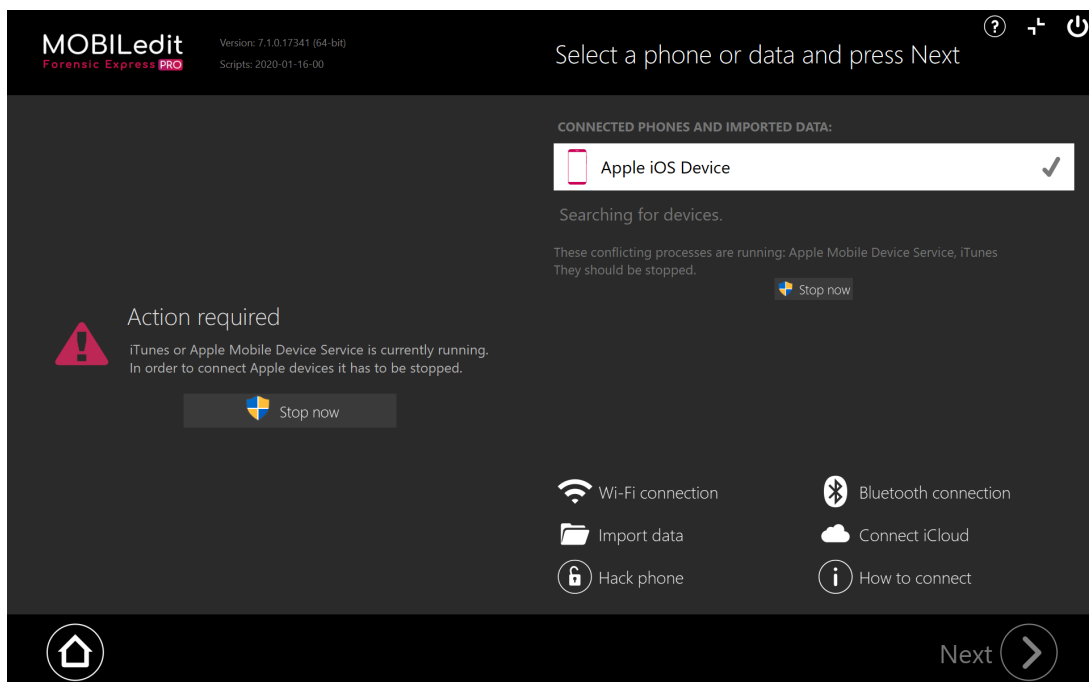


6. Set to never:





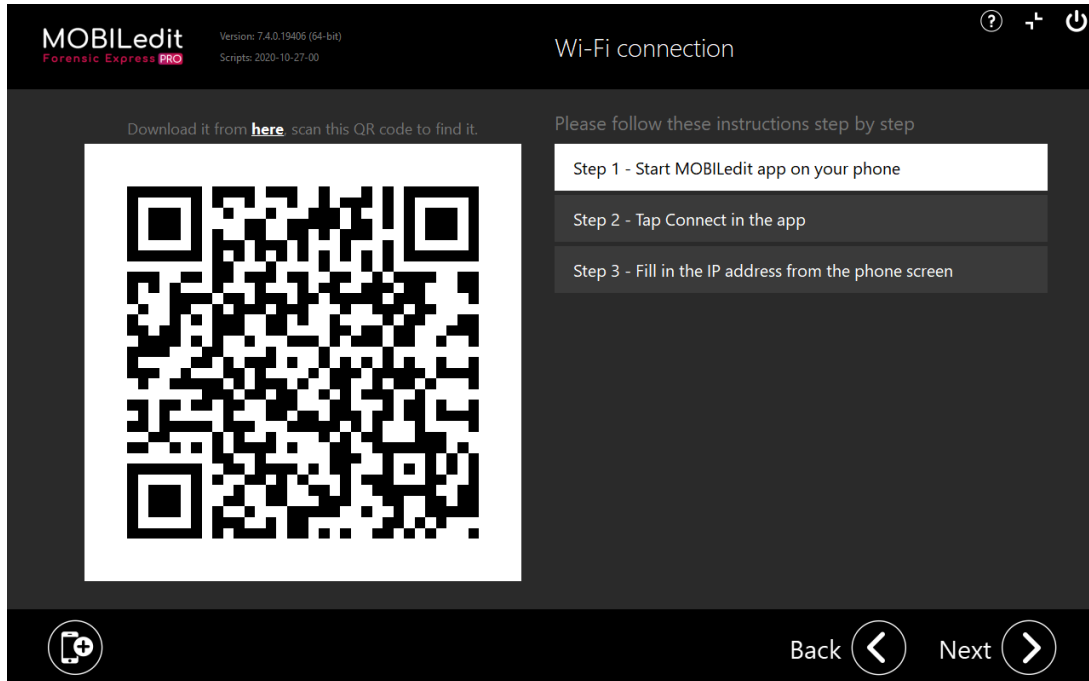
7. When using a cable connection, you need to have the latest version of iTunes and the correct drivers installed; it is also necessary to stop the ongoing Apple Mobile Device Service.



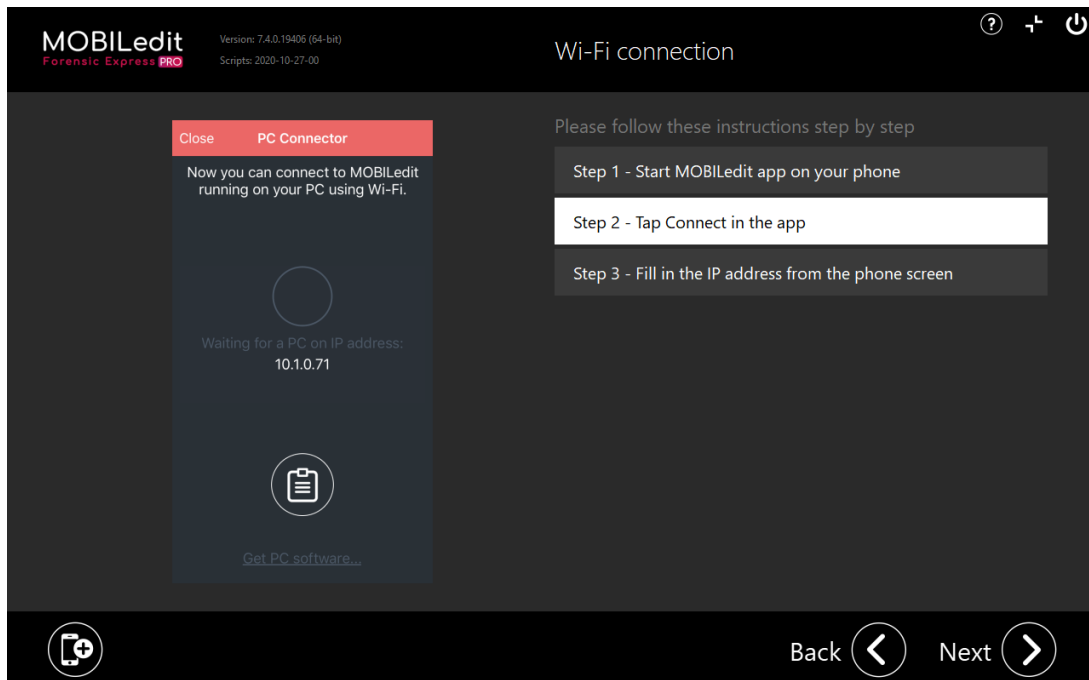
8. The last step to connect the phone is to press the confirm trust button that will pop up on the phone's screen. The phone should now be connected properly. If it isn't, the last screen of the wizard will provide tips which could give you a reason for the phone not connecting to MOBILedit Forensic Express. This page also provides a link to a more detailed web-manual.

3.3.3.2 Wi-Fi connection

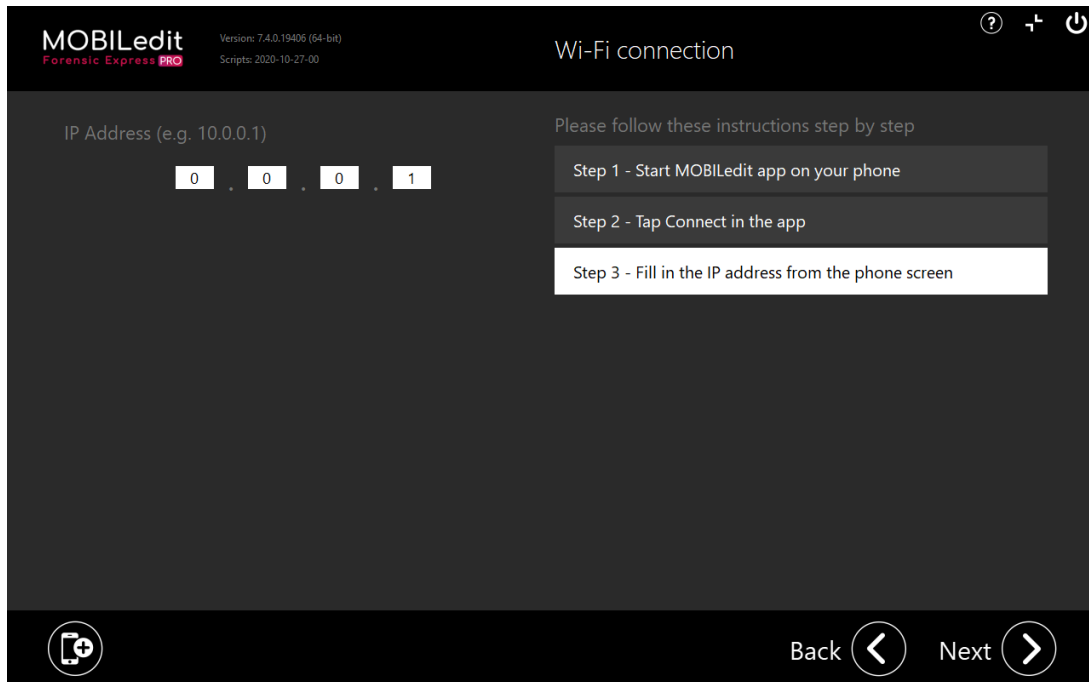
To connect an iPhone via Wi-Fi, the user will need the MOBILedit App. You can download the MOBILedit app from App Store for free. The first few steps of the wizard will tell the user how to download it and how to work with it, so a proper connection might be established.



1. Tap connect in the app.



2. Fill in the IP address form the phone screen.

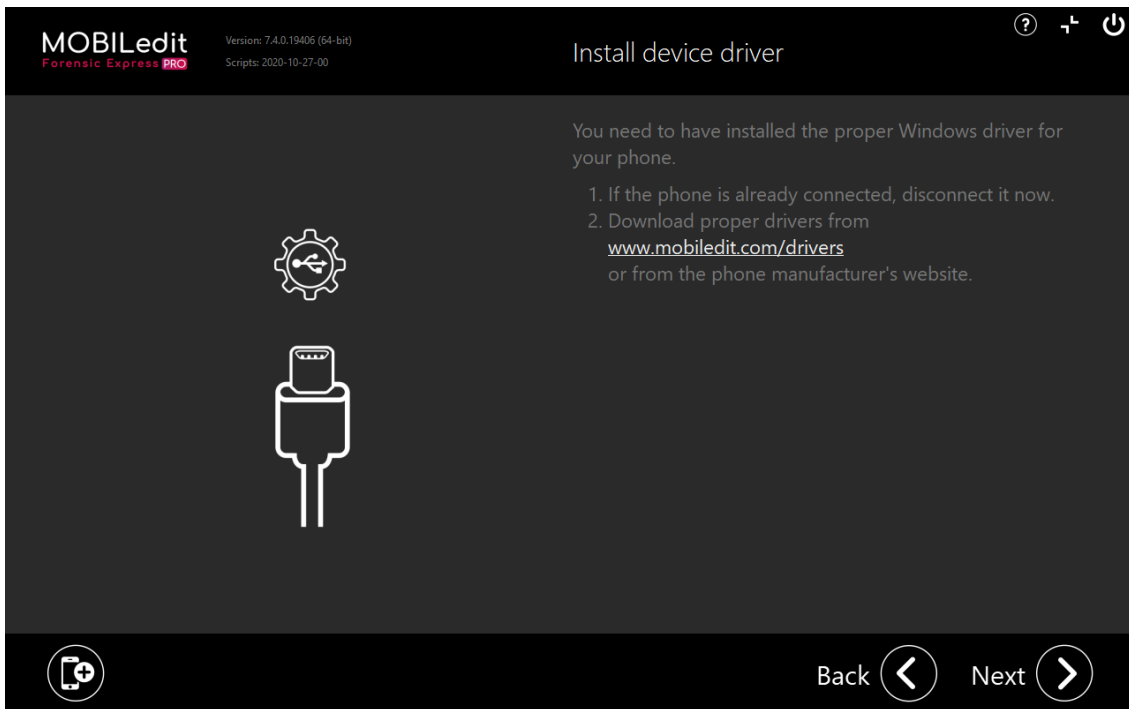


Once the IP address has been filled correctly, the phone should be connected, and this will be visible on the intro screen. The phone should now be connected properly. In the case it isn't, the last screen of the wizard will provide tips that could give you a reason for the phone not connecting to MOBILedit Forensic Express. This page also provides a link to a more detailed web-manual.

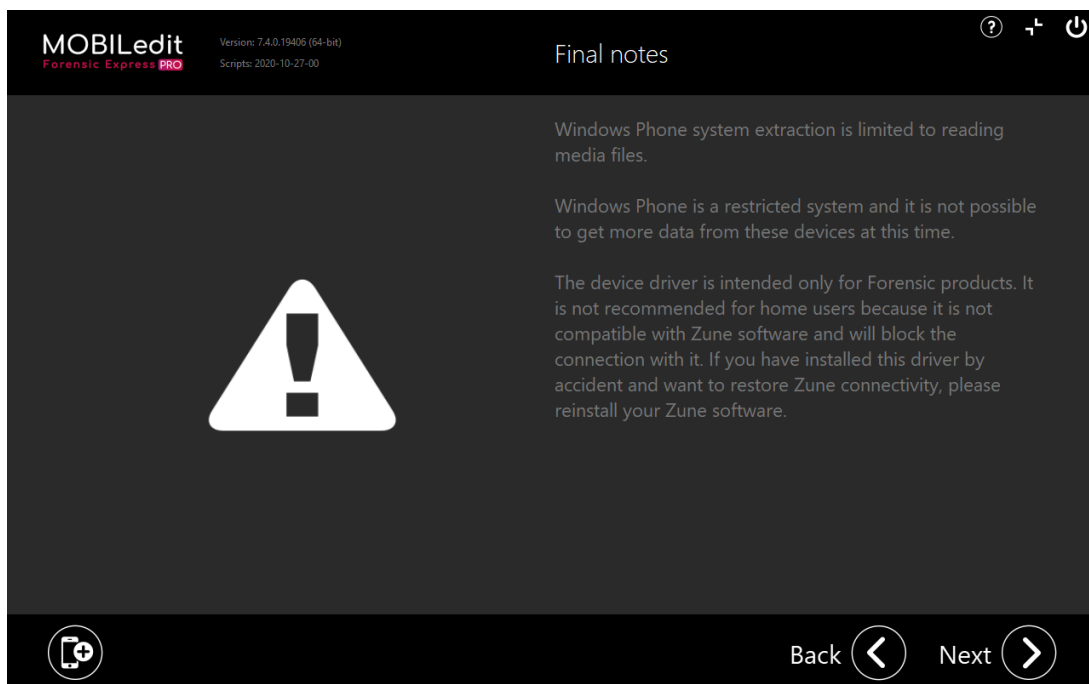
3.3.4 Windows Phone

In order to connect a Windows Phone, the correct drivers need to be installed on the computer. These drivers can be found [here](http://www.mobiledit.com/download-list/phone-drivers)⁴³. The first screen of the connection wizard will guide the user through the process of installing these drivers.

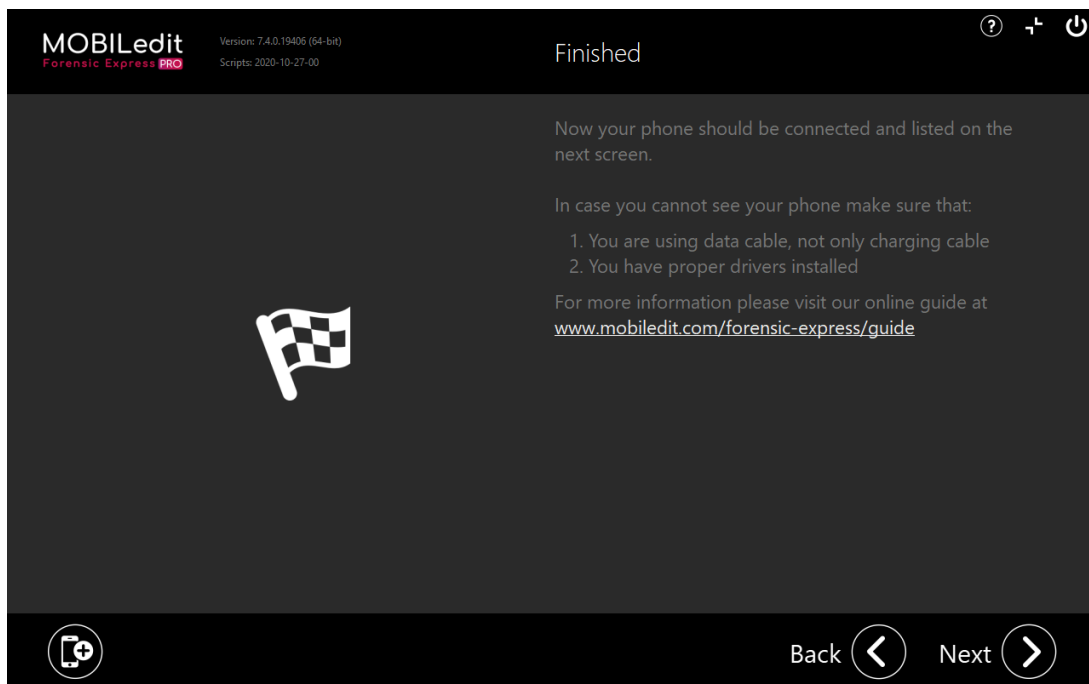
⁴³ <http://www.mobiledit.com/download-list/phone-drivers>



Please note that these drivers might disable the phone’s communication with standard programs and thus are intended to only be used for data extraction by professionals, as mentioned on the second screen.

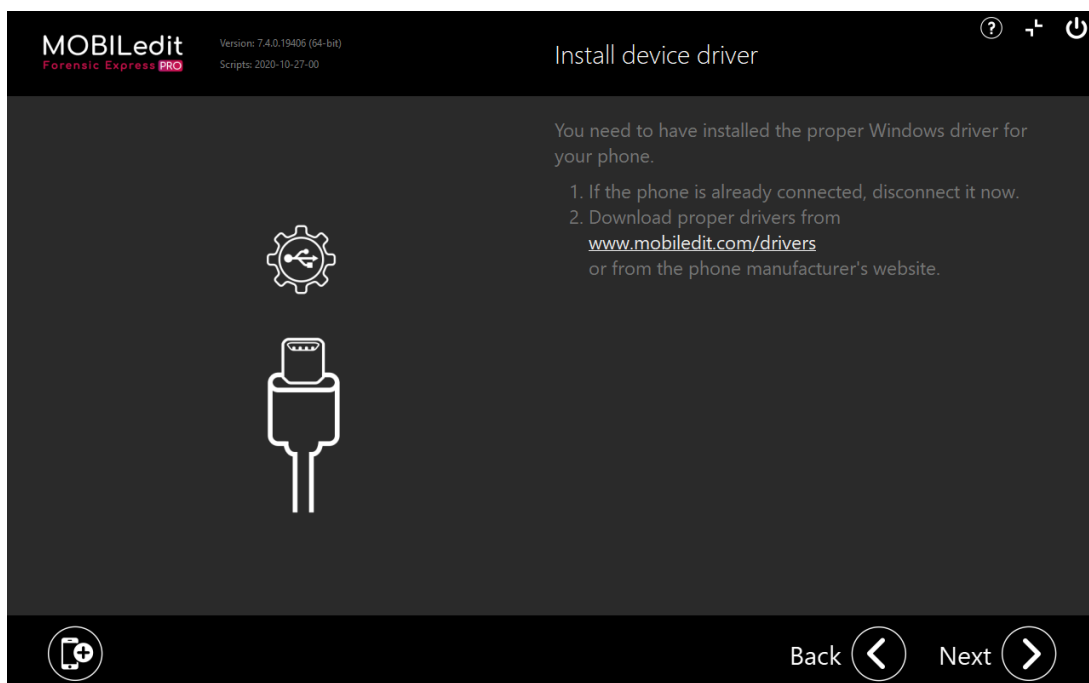


The phone should now be connected properly. In case it isn't, the last screen of the wizard will provide tips that could give you a reason for the phone not connecting to MOBILedit Forensic Express. This page also provides a link to a more detailed web-manual.

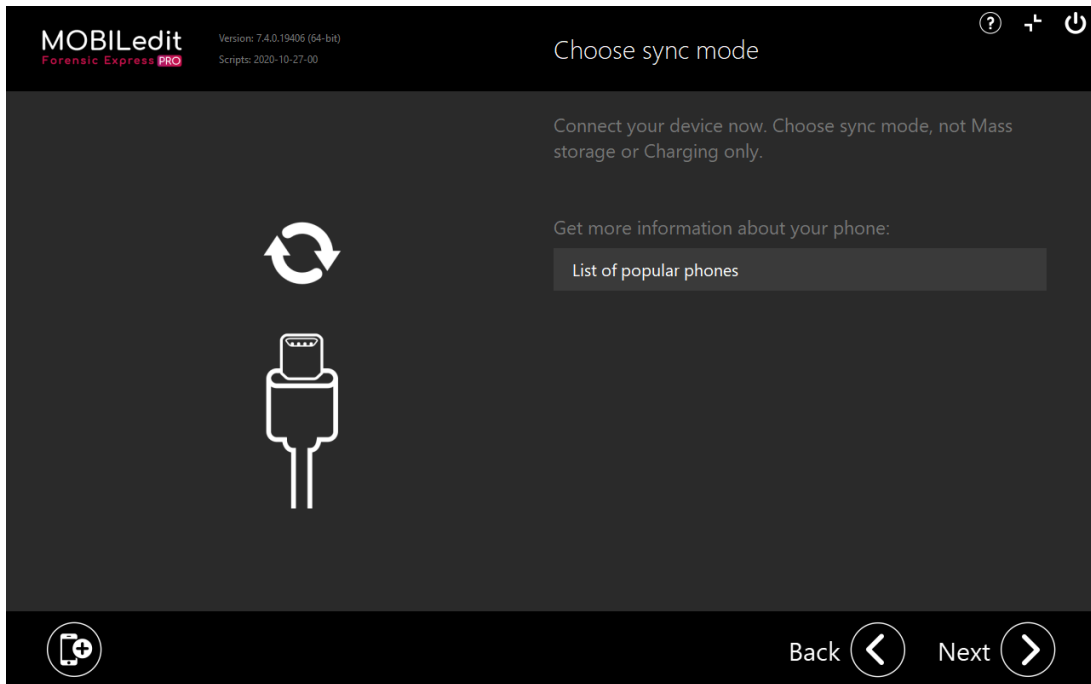


3.3.5 Other phones

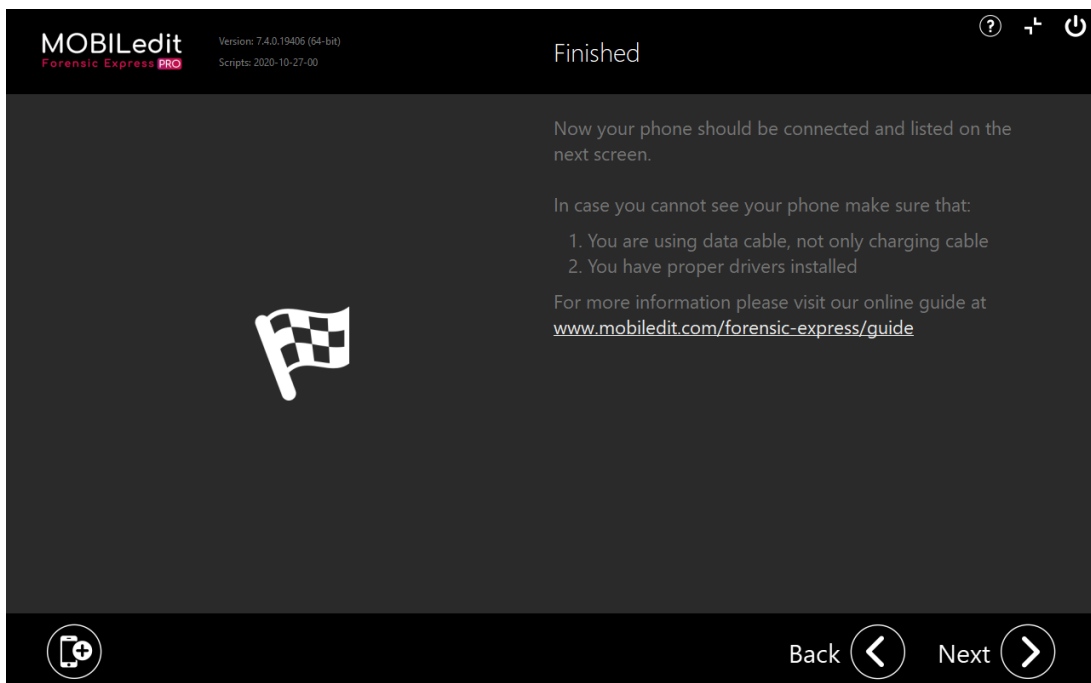
For connecting other phones (feature phones, etc.) one must have the proper drivers installed on the computer. The first screen of the manual will show the user how to do so.



For proper communication of the phone with the computer, it is essential to connect it in the **sync mode** (please note that connecting as 'charge only' or as 'mass storage' might disable extraction of any data from the phone).



The phone should now be connected properly. If it isn't the last screen of the wizard will provide tips that could give you a reason for the phone not connecting to MOBILedit Forensic Express. This page also provides a link to a more detailed web-manual.



3.4 Android

The following article will explain all the necessary steps that need to be undertaken in order to successfully connect an Android phone to MOBILedit Forensic Express. The procedure is required only for the first connection. An Android phone can be connected to a PC by USB cable, which transfers data faster or via Wi-Fi which is easier.

- [Connecting Android phone via USB cable](#)(see page 138)
- [Connecting Android phone via Wi-Fi](#)(see page 138)
- [If your phone doesn't connect](#)(see page 139)

3.4.1 Connecting Android phone via USB cable



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=y_78HkdT_hw&feature=emb_logo

To connect an Android phone, follow the steps below:

1. [Enable USB debugging](#)(see page 139), so your phone can be connected to a PC
2. [Enable "Stay awake" option](#)(see page 141), so the phone doesn't disconnect
3. Download and install the [Universal Android driver](#)(see page 148)
4. Connect your phone to a PC and start MOBILedit Forensic Express
5. [Confirm RSA fingerprint](#)(see page 146) on your phone's display
6. [Select MTP mode](#)(see page 147) on the phone's display
7. Now you've successfully connected your phone



In case you connected your phone to the PC prior to step 3 above, a wrong driver might have been installed on it by Windows. That would cause MOBILedit not to recognize the phone. Click [here](#)(see page 148) for a guide on how to remove the Windows incorrect driver by our Universal android one.


3.4.2 Connecting Android phone via Wi-Fi

Download the **Android Connector application** from [Google Play](#)⁴⁴ or from our downloads [page](#)⁴⁵.
Now start the connection app on your phone and follow the steps below:

1. Make sure your Wi-Fi is turned on and you are connected on the same network.
2. Run MOBILedit and click on the Connect button.
3. Select Phone – Wi-Fi Connection and then enter the IP address as displayed on the phone.
4. Allow the connection on your phone if the key corresponds with the key in Connection Wizard.
5. Once your phone is located, click on the "Finish" button and the device will connect automatically.

⁴⁴ <https://play.google.com/store/apps/details?id=com.compelson.migrator>

⁴⁵ <http://www.mobiledit.com/downloads.htm>

 Be aware that it is not possible to activate a phone with Android 10 OS with a single phone license through wifi. However, if you activate a phone through a cable, you will be able to use it with wifi later.

3.4.3 If your phone doesn't connect

- MOBILedit will require the installation of a small app called Connector into your phone. If it does not install automatically we recommend reconnecting the phone and restart MOBILedit or download the Connector app directly from [Google Play](#)⁴⁶. In case you have a Xiaomi phone, [allow required settings](#)(see page 139) prior to installation.
- USB debugging not turning on? Is the RSA key not showing on the screen? Try turning the USB debugging off and on again after you connected the phone.
- Make sure that the phone is not set in Mass Storage mode.
- If you use any other phone tool, such as HTC Manager, Eclipse, Android Studio, you need to stop the ADB process in Task Manager or uninstall the software, if it doesn't help.
- In case you are using Windows 7 OS and your phone is not automatically connected, nor recognized, please follow the article of [manually changing the ADB driver](#)(see page 148).
- Problems with connecting a Huawei phone? Go [here](#)(see page 139) to check how to avoid them.
- Problems with connecting a Xiaomi phone? Go [here](#)(see page 139) to check how to avoid them.

3.4.4 How to enable USB debugging

- [Android 4.2 and higher](#)(see page 139)
- [Huawei devices](#)(see page 139)
- [Xiaomi devices](#)(see page 140)
- [Android 4](#)(see page 141)
- [Android 2.3](#)(see page 141)

3.4.4.1 Android 4.2 and higher

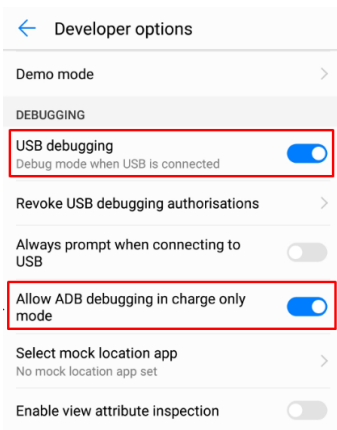
The USB Debugging is in the “Developer Options” menu item, but it is hidden, you need to reveal it first:

1. Go to Settings -> About Phone.
2. Go to “Build Number” at the end of the Scroll list.
3. Tap on “Build Number” (“Android version” for some devices) repeatedly 7 times. On your third tap, you should see a message indicating that you only have 4 more taps to go to ‘become a developer’.
4. Go back to the Setting page. You should see the Developer Options menu item in your settings list now.
5. Open Developer Options and check USB debugging -> ON.

3.4.4.2 Huawei devices

In case you are turning on the USB debugging on a Huawei device, make sure to also "allow the debugging usage in charge only mode" in the Debugging section in Developer Options. This will prevent most of the cases, where USB debugging is turning itself off, because of EMUI.

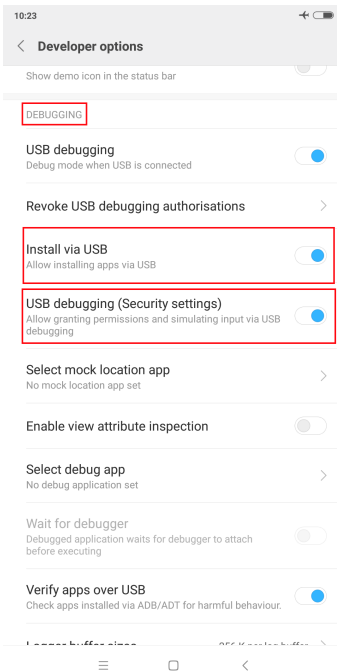
⁴⁶ <https://play.google.com/store/apps/details?id=com.compelson.meconnector>



i For EMUI 5.0 and higher, it might be necessary to connect the phone to the PC prior to enabling USB debugging, because it may otherwise keep turning itself off automatically.

3.4.4.3 Xiaomi devices

In case you are turning on the USB debugging on a Xiaomi device, make sure to enable all the categories in the Debugging section in Developer Options. This will ensure that the connector app is able to be installed on your phone.



i Enabling both these options will require you to have a SIM card inserted in the phone and also to be logged into Mi Account.

3.4.4.4 Android 4

Go to Settings -> Developer options and enable USB debugging.

3.4.4.5 Android 2.3

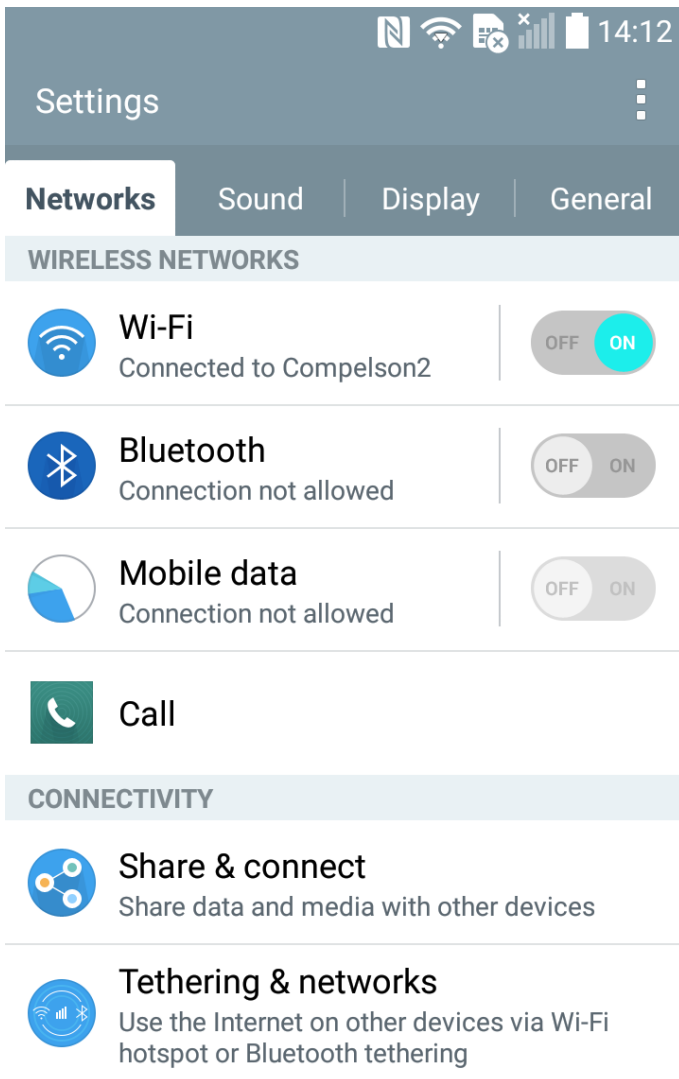
Go to Settings -> Applications -> Development and enable USB debugging.

3.4.5 How to enable "Stay awake" option

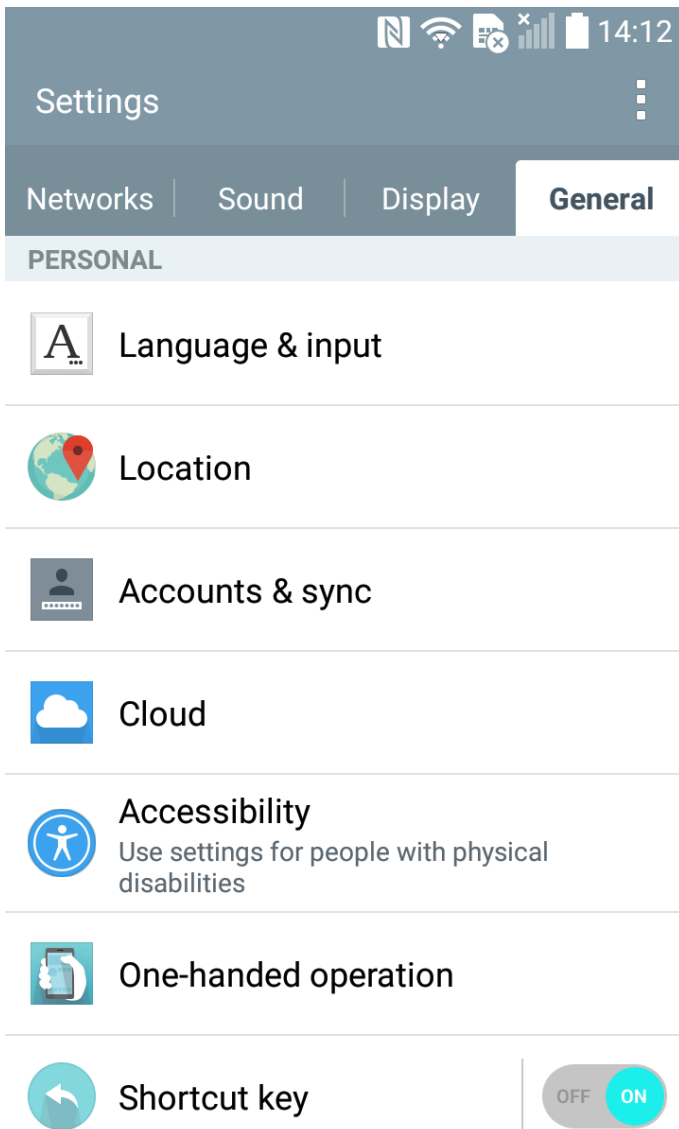
The Stay Awake option should be set on your phone to allow continual communication between the phone and the software. If the phone is not set to Stay Awake and is for example set to Power Saving mode, the phone may disconnect from other sources including our software and interrupt the process of extraction and analysis.

3.4.5.1 How to

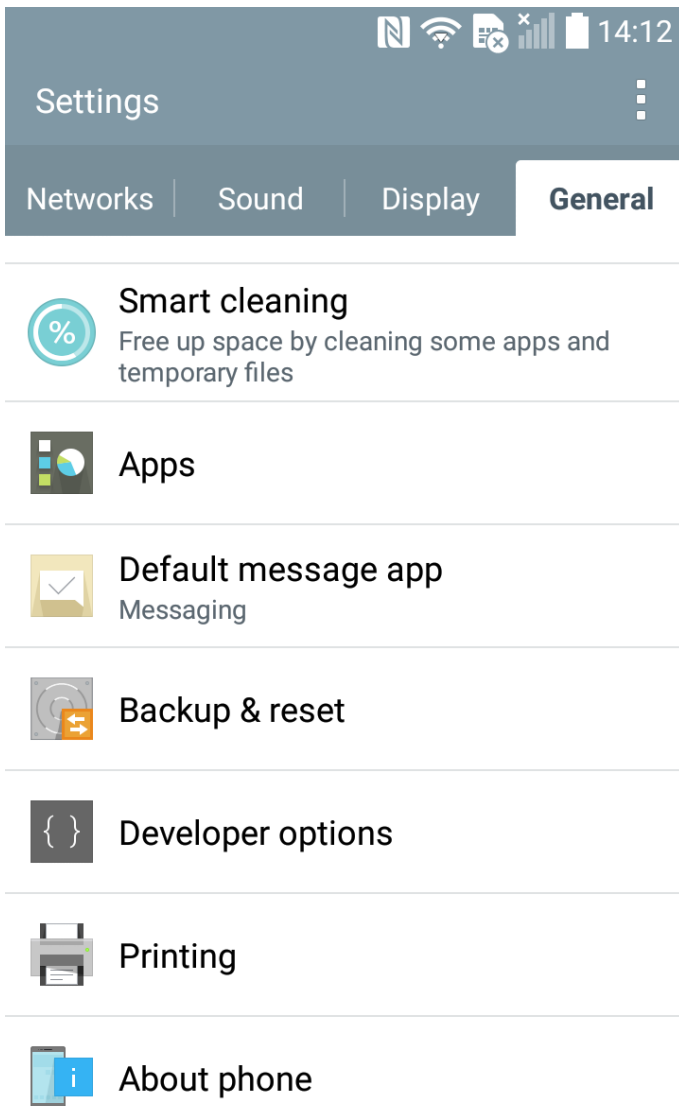
1. Go to Settings on your phone.



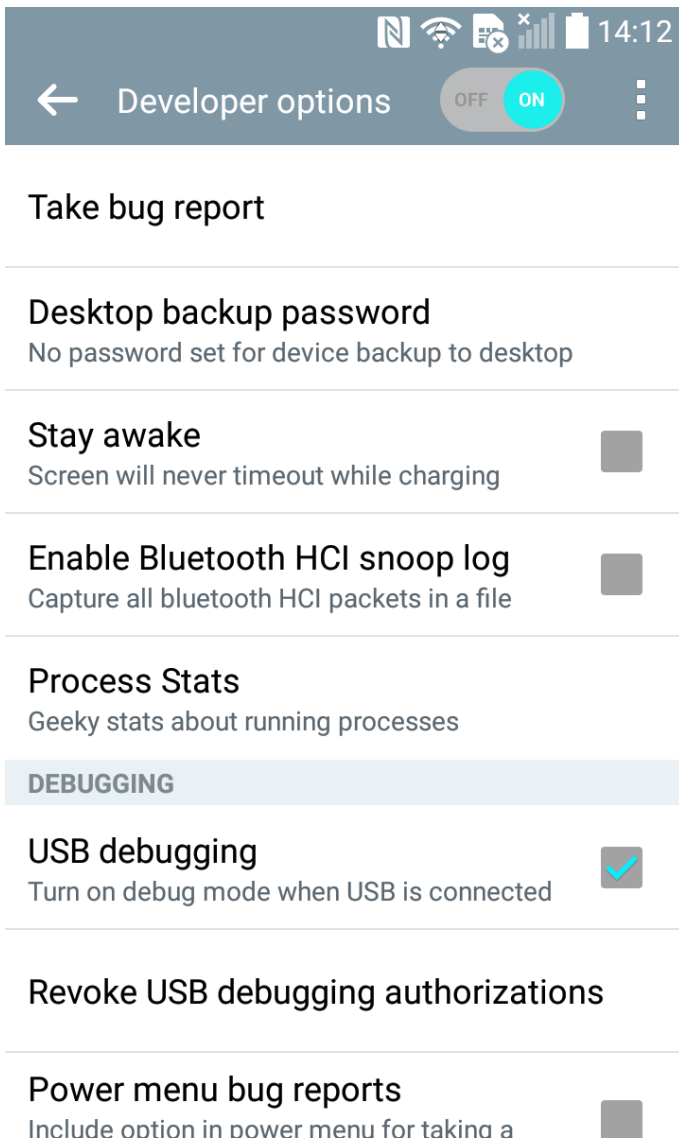
2. Choose "General" in the Settings bookmarks.



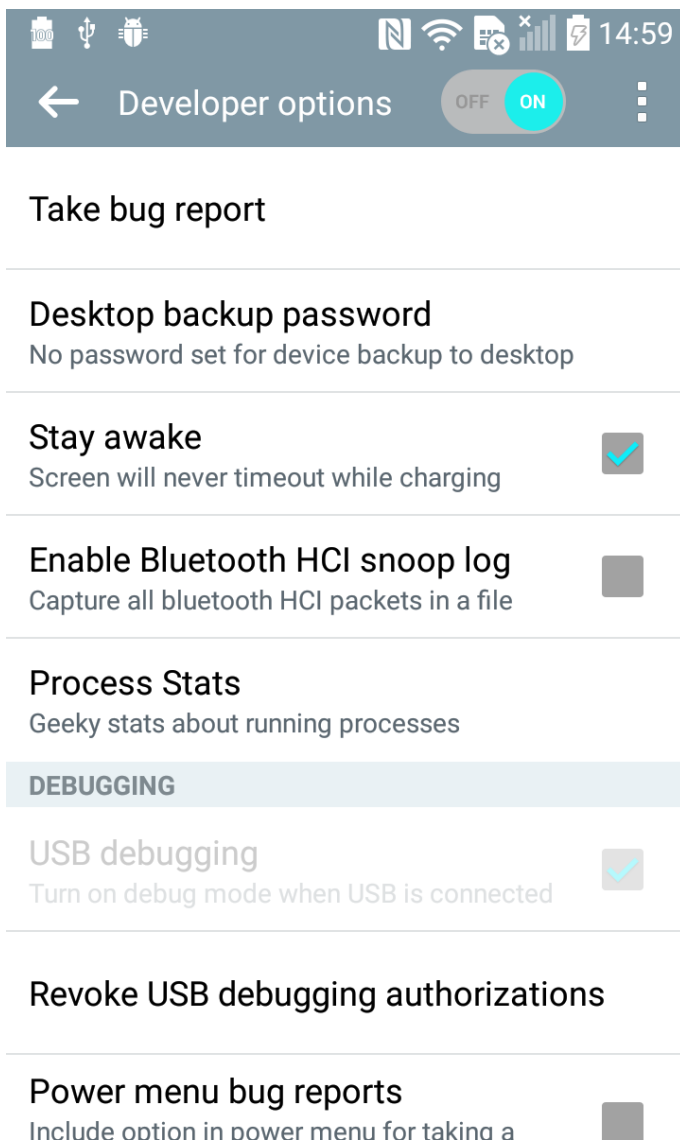
3. Scroll down to find the [developer options](#)(see page 139).



4. Open the Developer Options and find the "Stay Awake" option line.

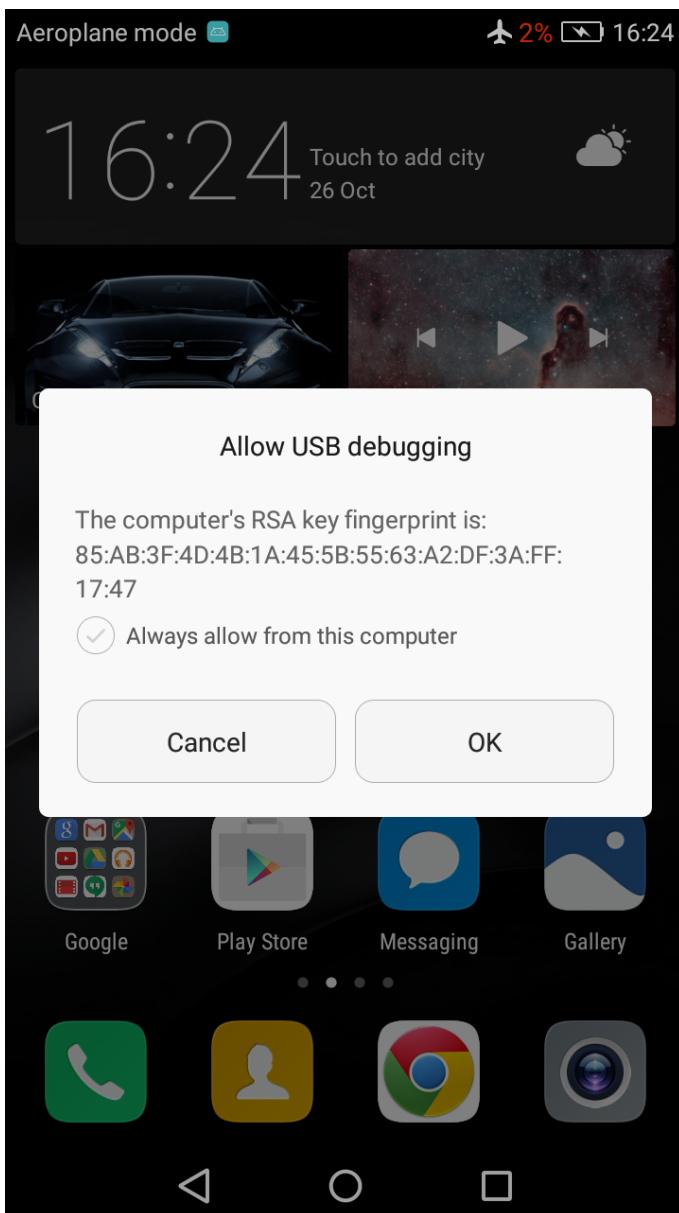


5. Click in the box next to Stay awake to enable the prevention of the screen blacking out.



3.4.6 How to confirm RSA fingerprint

There should be a pop-up window on your device's screen with a message (as shown on the picture below) which asks you to confirm the RSA fingerprint. If there is no dialog, please reconnect the phone and the dialog will reappear.



i If you are using a multi-account phone, make sure you are using the main account. Otherwise, you won't be able to use our software properly and you will face difficulties while connecting your device.

3.4.7 Connecting in MTP mode

Some phones tend to automatically connect in "**charge only**" mode. To ensure the fastest possible communication and transfer speed, please change the connection mode to **MTP (Media Device)**.

3.4.7.1 How to

1. Swipe down on your phone, find the notification about "**USB options**" and tap on it.

2. A page from settings will appear asking you to select the desired connection mode. Please select **MTP (Media Transfer Protocol)**. MTP basically lets you browse files and folders stored on your device, however, some phones may be required to be unlocked in order to enable MTP.
3. Wait for your phone to automatically reconnect. Some phone models (i.e. Huawei) have this option done a bit differently in the UI. After swiping down you'll find the following notification, simply select **"Files"** and you're done.

3.4.7.2 Android 6.0 and higher

Upon connecting, your phone will ask for permission for the PC connection to access data and files. Simply click on the **"Allow"** button and you're all set.

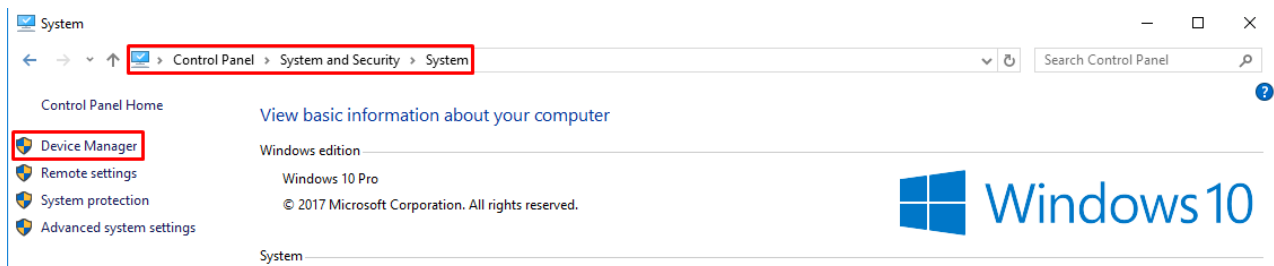
3.4.8 How to install a universal Android driver

In some cases, the drivers provided by the manufacturer of the phone do not allow a proper device connection, which is required for our products to successfully communicate with the device. Hence there is a need to replace this driver with the Universal Android driver.

If you need to install an unsigned driver, click [here](#)⁴⁷.

Below is a guide on how to proceed with the installation and replacement of this driver.

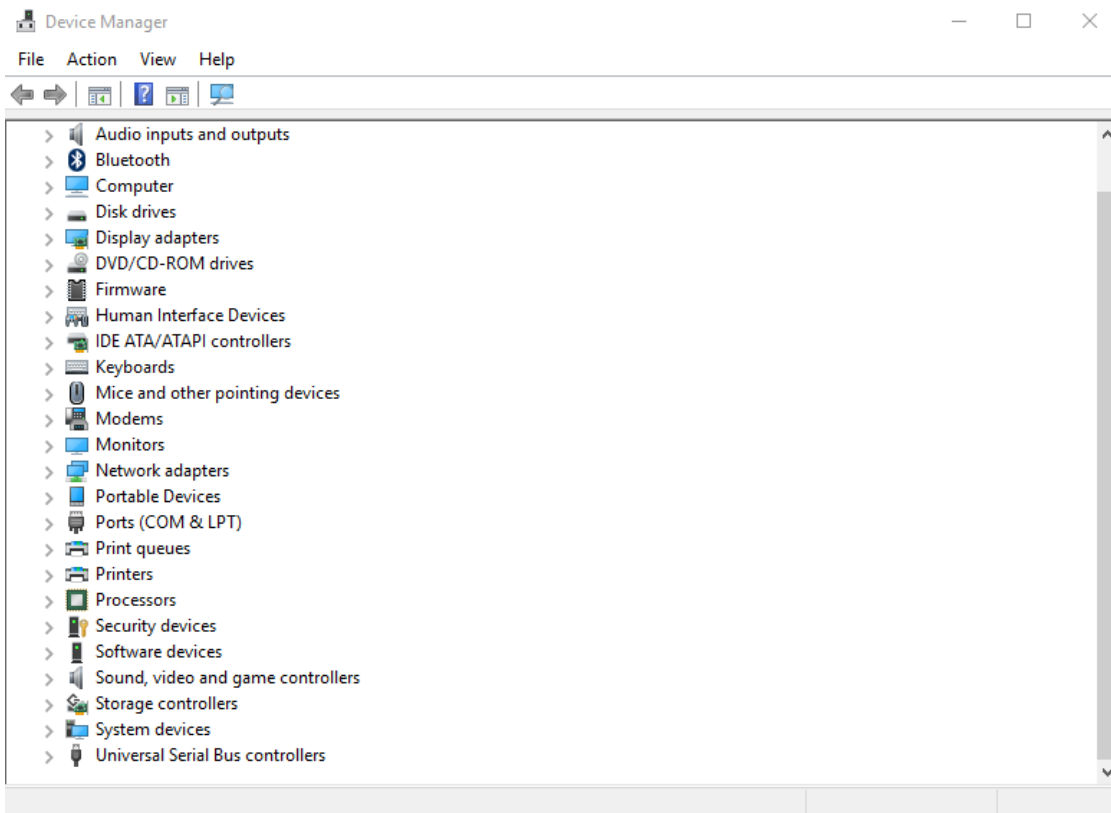
1. Download and install the Universal Android driver from our website [here](#)⁴⁸.
2. When the driver is installed, plug in your device.
3. Open the System Properties dialog - press **Win+Break** on the keyboard. (or start the Control Panel and go to "System and Security" and then to "System")



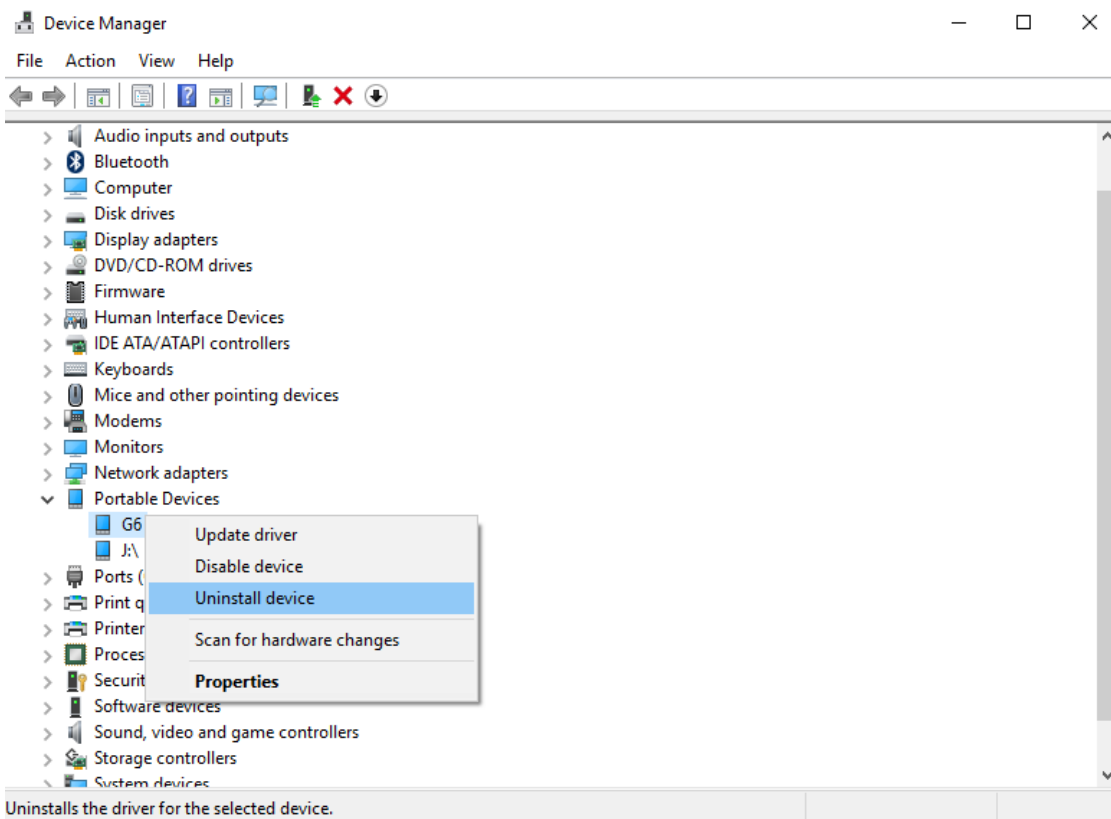
4. Click on the "Device Manager" link.

⁴⁷<https://www.howtogeek.com/167723/how-to-disable-driver-signature-verification-on-64-bit-windows-8.1-so-that-you-can-install-unsigned-drivers/>


⁴⁸<http://www.mobiledit.com/download-list/universal-android-driver>



5. In the Device Manager locate your Android device, right-click on it and select "Uninstall".



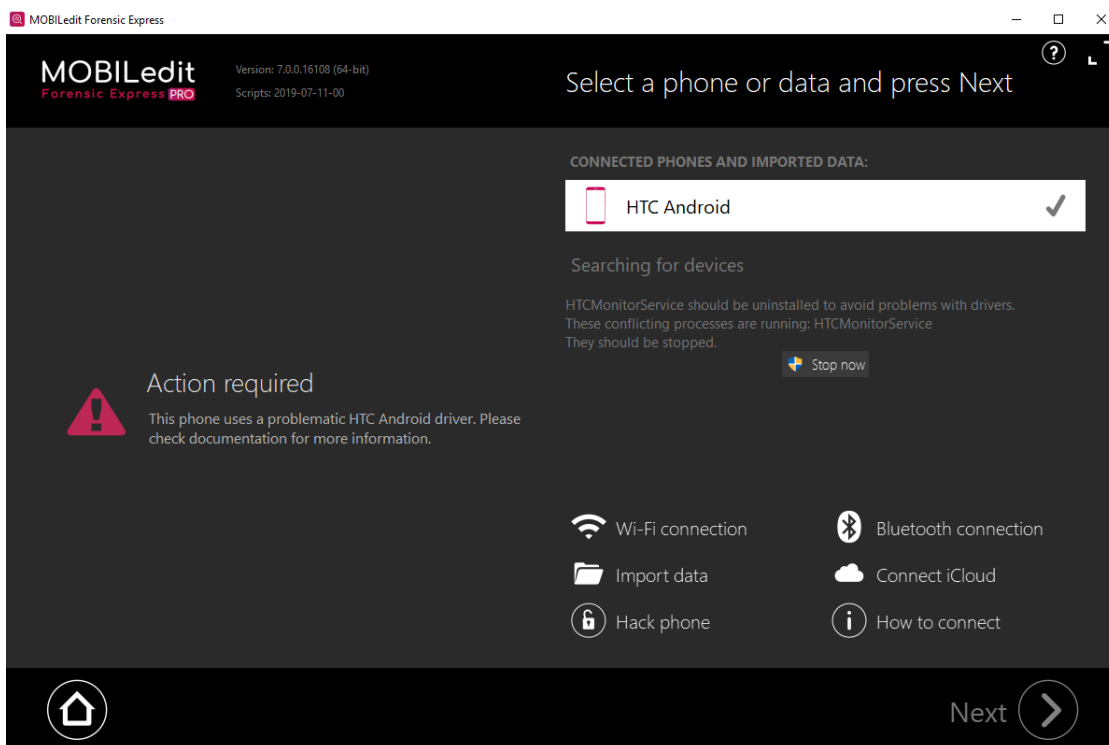
6. After that is done, close the Device Manager and reconnect the phone.
7. Upon connecting it again, our Universal driver will automatically locate and "catch" the phone, before an incorrect driver is installed by Windows.

 If this did not work for you or you are in need of further assistance, please contact us [here](#)⁴⁹.

3.4.9 How to install HTC drivers

Some users might experience an issue where our software gives out a warning that the user's device uses a problematic HTC Android driver.

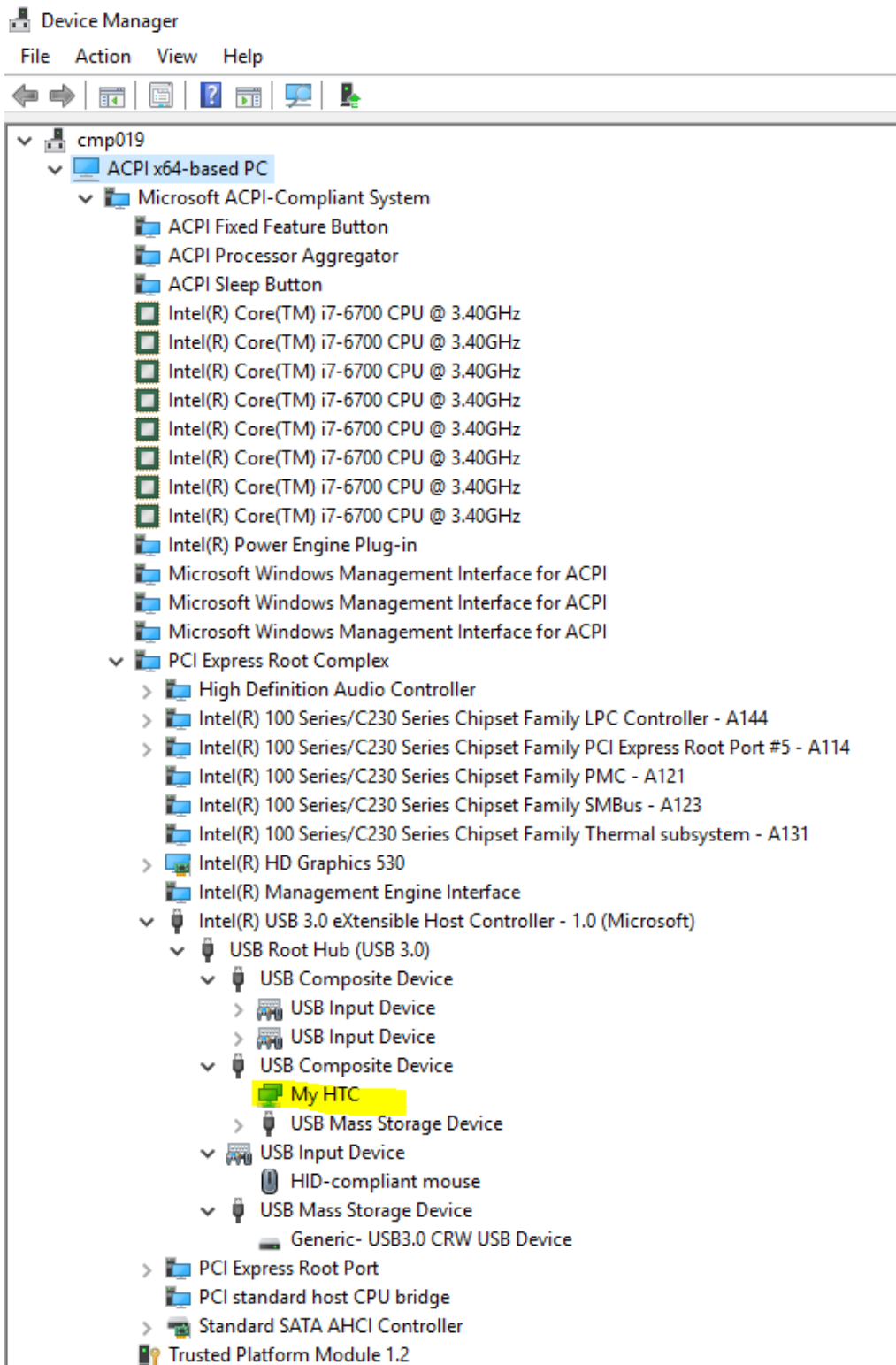
3.4.9.1 How to



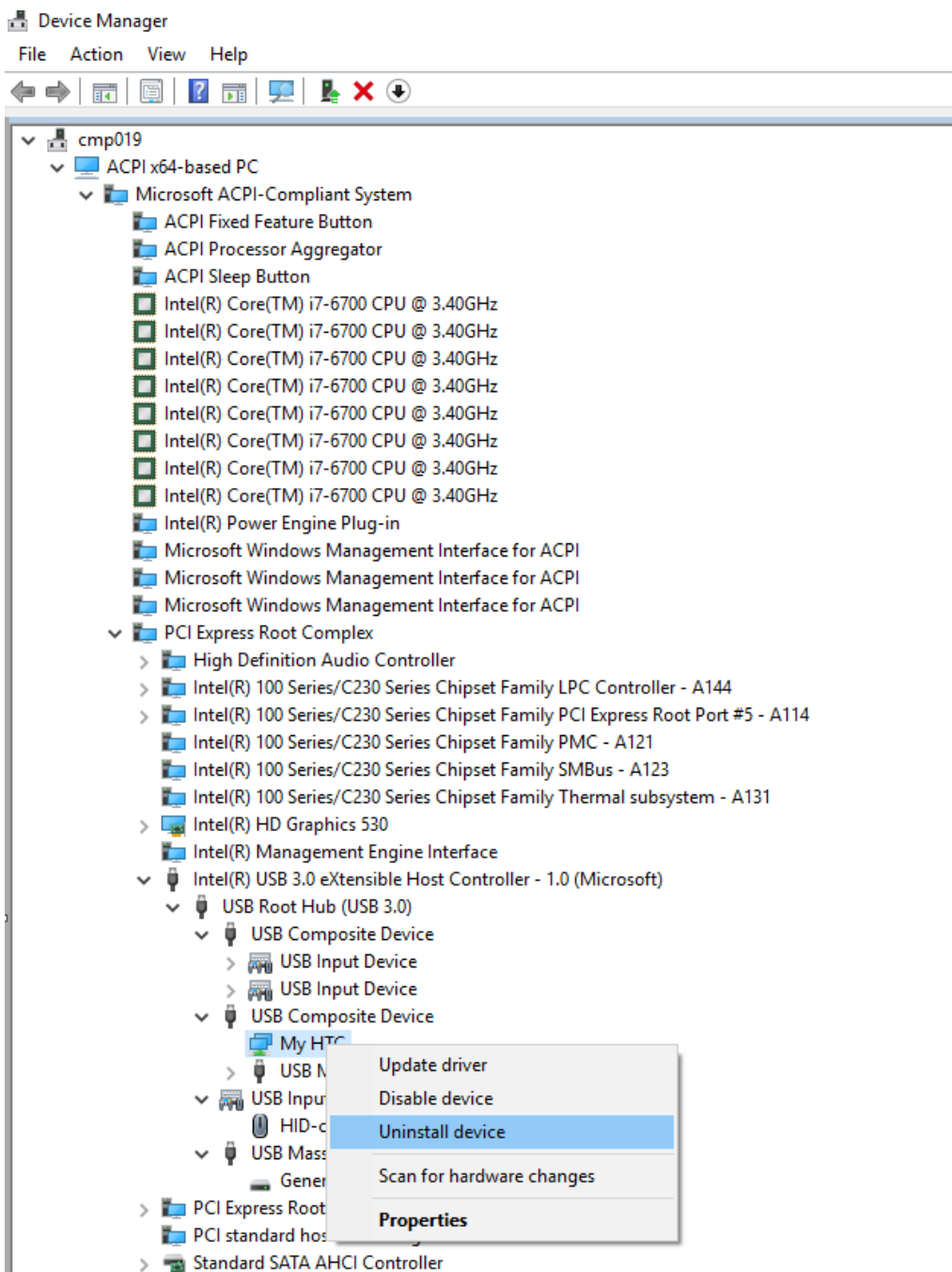
1. First of all keep your device connected to your PC or laptop then uninstall all of the existing drivers which you have previously downloaded for the HTC, and download ADB Universal driver from our website, click [here](#)⁵⁰ to download it.
2. It is necessary to remove the existing drivers completely from the system, you do so by going to the Device manager manually or by pressing the "Windows" and "R" keys and typing: devmgmt.msc and then hitting enter. A device manager window will pop up. In the upper left corner click on "View" and select "Devices by connection" afterwards navigate through the menus as seen in the screenshot below.

⁴⁹ <http://www.mobiledit.com/contact>

⁵⁰ <https://www.mobiledit.com/download-list/universal-android-driver>



3. Right-click on "My HTC" and uninstall it.



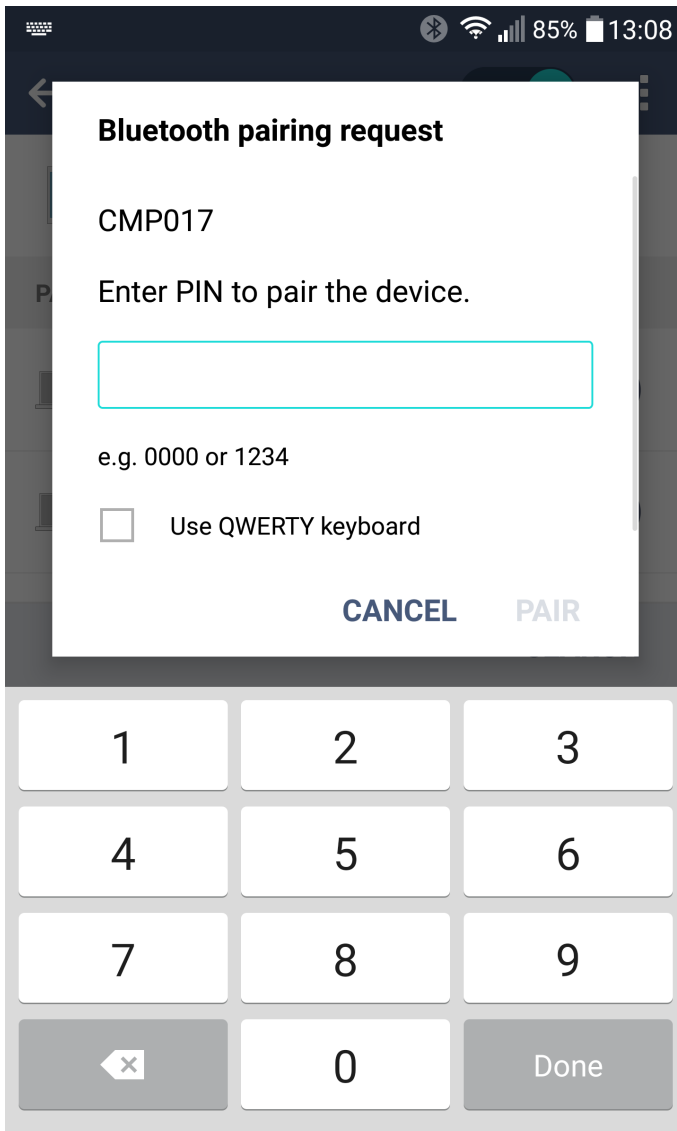
4. Install the Universal ADB driver and then reconnect your HTC device. You can check if you did everything correctly by opening the device manager > "View" > "Devices by connection". You should see an HTC Android Phone USB Device as your installed driver for your HTC device.

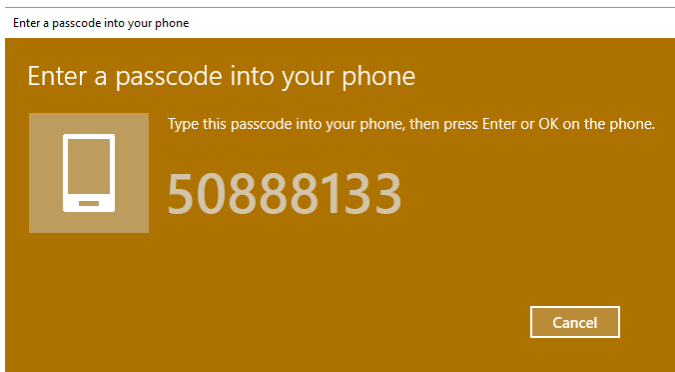
5. Re-run MOBILedit Forensic Express and your HTC device should be connected.

3.4.10 Connecting via Bluetooth

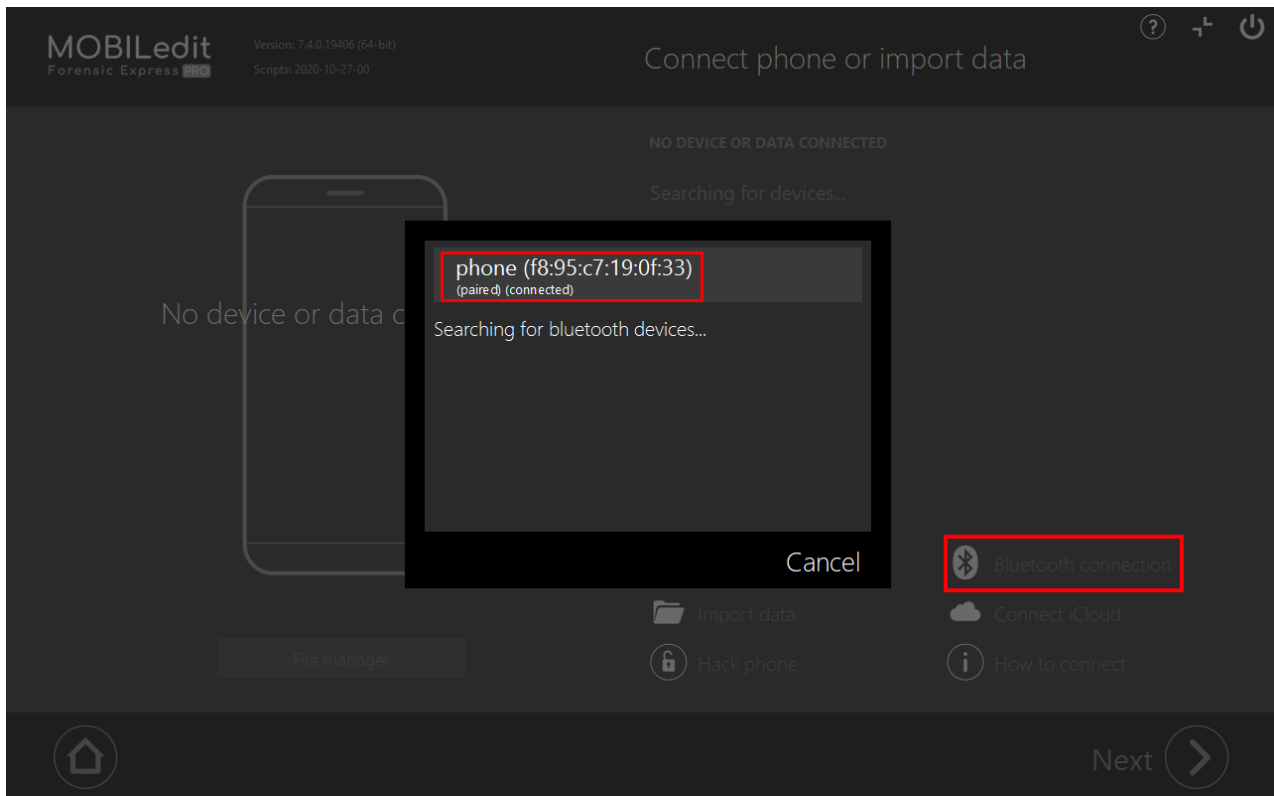
In order to successfully establish a Bluetooth connection between an Android device and a PC, you'll need to turn on Bluetooth on both of them and then. Once the Bluetooth connection is established click on "Pair" on either the phone or the PC.

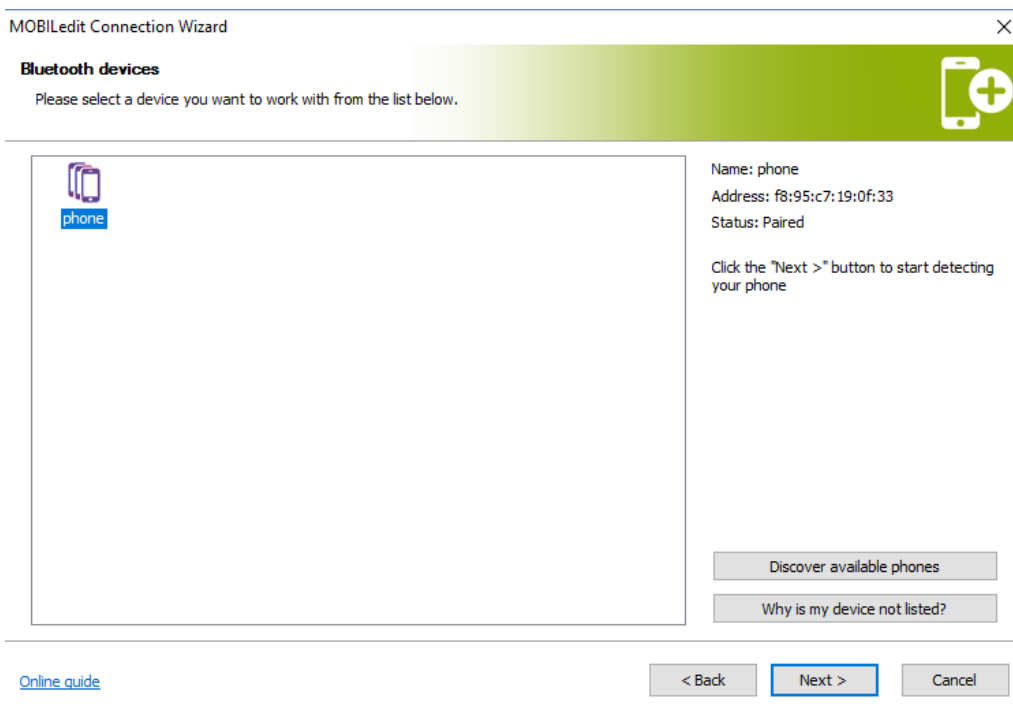
When attempting to pair you will be asked to provide a matching password on both the phone and the PC as seen below on the screenshots.





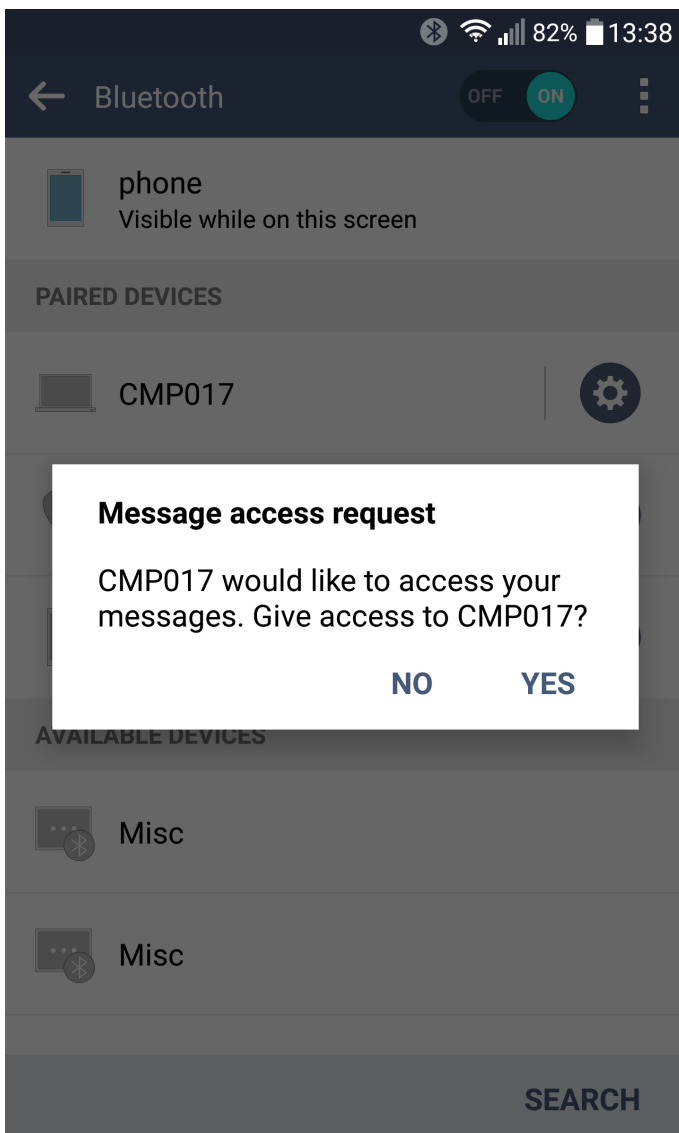
When pairing is done successfully you will see the phone in connected Bluetooth devices in your PC's BT settings. When this is done you can view the connected phone in MOBILedit (or any other software of ours). Simply go to the Connection Wizard and select Android - BT connection. Your phone will be found by our Wizard - click on it and connection should be established.





When the connection with the phone is established in MOBILedit you may proceed to work with the phone as if it was connected via cable. Please note there will be some limitations to this, due to not all the data being accessible via BT. Most phones will allow you to read contacts, messages, and media files.


On Android 5.x and newer, you will be asked by the phone's OS to allow the PC to access the phonebook, messages etc. A confirmation message will appear on your phone asking you to grant permission for the BT connection to read the phonebook, to read messages, etc. It is necessary to confirm this message by tapping on "allow" / "yes", otherwise empty data will be read.

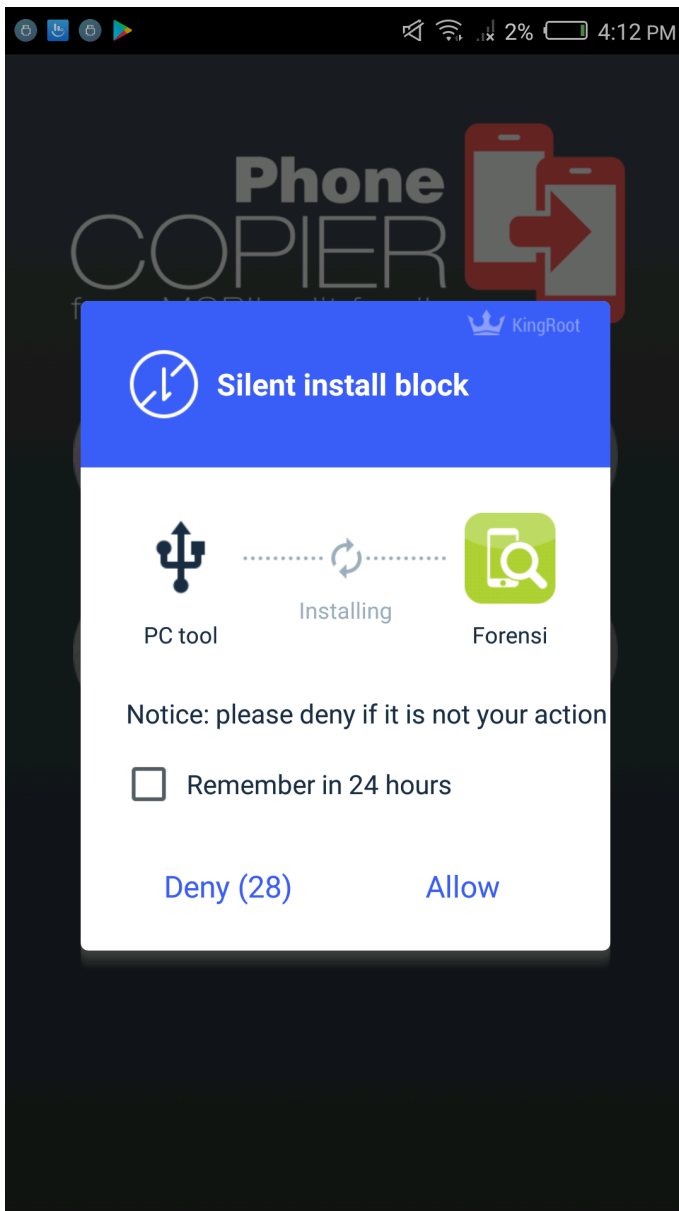


3.4.11 Connector installation

To ensure a successful and stable connection between the phone and the PC, it is required to install our Connector app, which will provide communication between the phone and the PC.

Usually, it takes only a few seconds to get it installed and everything will be done automatically if possible.

 On some phones, it is required to manually allow the installation of the connector app.



3.4.11.1 How to install our app manually

1. Download the .apk version forensic connector from our website [here](https://www.mobiledit.com/download-list/android-forensic-connector?rq=forensic)⁵¹.
2. Allow installation from unknown sources:
 - From a Home screen, swipe up or down from the centre of the display to access the apps screen.
 - Navigate: Settings. > Apps.
 - Tap Menu icon (upper-right).
 - Tap Special access.
 - Tap **Install unknown** apps.
 - Select the **unknown** app then tap the **Allow** from this **source** switch to turn on or off.

⁵¹ <https://www.mobiledit.com/download-list/android-forensic-connector?rq=forensic>

1. Transfer the .apk to your Android device.
2. Install it on your device.

i Keep in mind that you might need to allow Install application from unknown sources/install unknown apps.

! This installation allowance might be blocked by USB debugging security measures. Go [here](#)(see page 139) to learn how to turn them off.

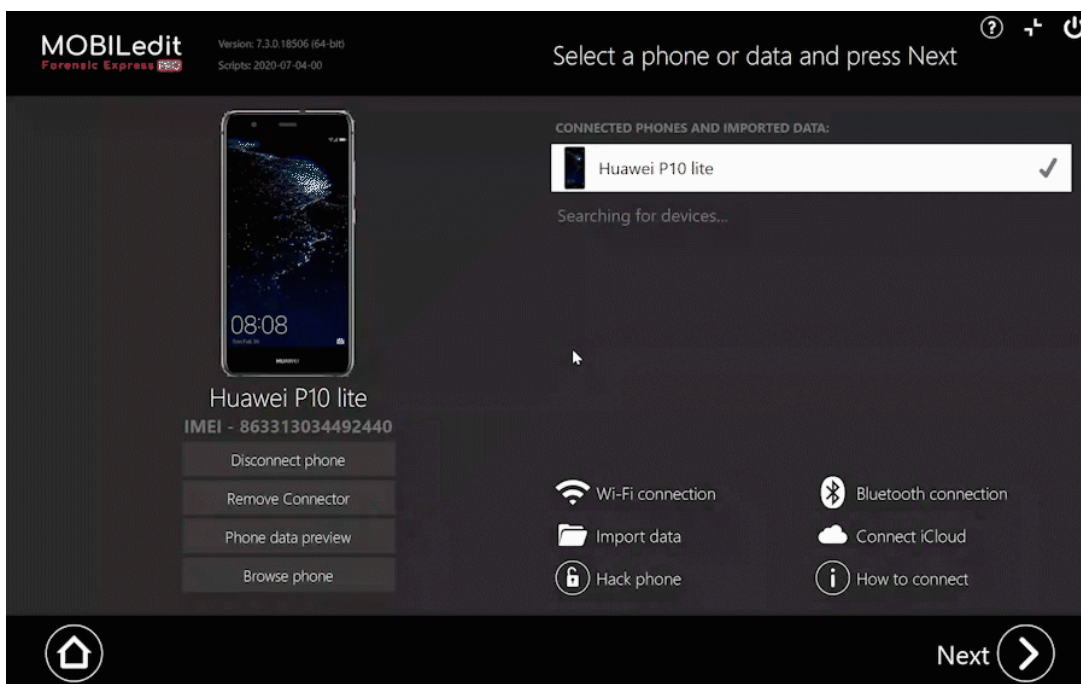
3.4.12 Connector permissions

Due to Android 's policy changes, applications now do request permissions separately. After updating to a newer version of Forensic Express, you will be asked to confirm them manually.

i Connector app is installed automatically, in case you are experiencing any kind of issues or want to install it manually, please visit the dedicated guide [here](#)(see page 156).

If you connect a device with outdated Connector app, you will receive a warning: *Old Connector in the phone*.

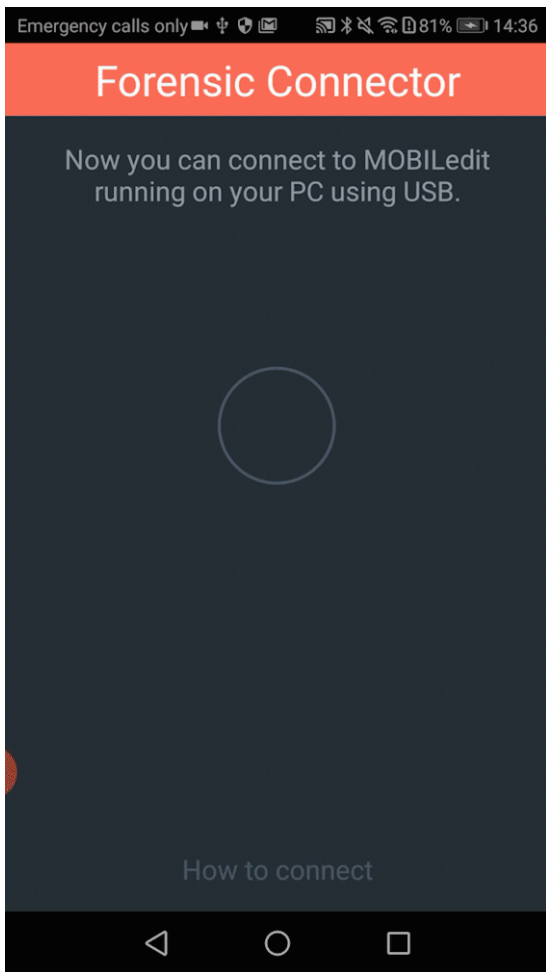
Simply click the "yes" option and wait a few seconds until our software installs the connector to your phone.



The process is fully automatic. After a successful update, you will be prompt to manually confirm all the permissions on your device.

Permissions required by our app are:

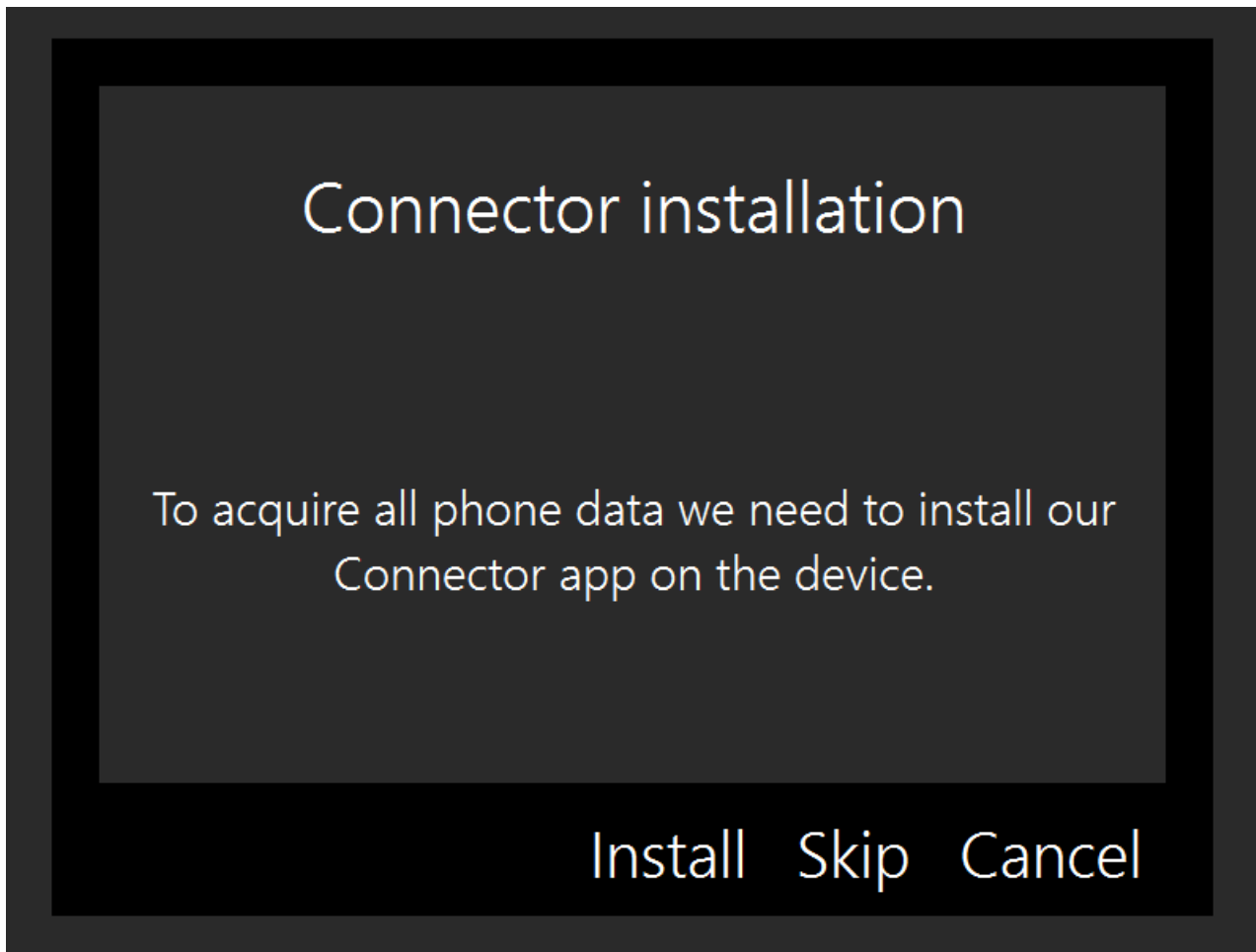
Contacts, SMS messages, calendar, call logs, locations, photos, media, and files.



i If you won't allow any of these permissions, the final results will not have all of the information in the export.


3.4.13 Extraction without the Connector app

Since version 8.0, it is possible to perform the extraction without installing the Connector application. You can simply press the skip button while the info tab pops up:



Please keep in mind, that once you skip the installation, the only option to revoke the installation tab is to disconnect the device using the ✕ button and connect it again:



 Note: extraction without the Connector app will provide significantly less data, so, please use it only if necessary.

3.5 iOS

- [Connecting iPhone by USB cable](#)(see page 161)
 - [iTunes for Windows not installed](#)(see page 161)
 - [iTunes for Windows installed](#)(see page 161)
 - [Jailbroken iPhone and full file system extraction](#)(see page 161)
- [Connecting iPhone by Wi-Fi](#)(see page 161)

The following article will explain everything you need to know in order to successfully connect an iPhone to MOBILedit Forensic Express. iPhone can be connected either by cable or via Wi-Fi. All iOS versions are supported.


3.5.1 Connecting iPhone by USB cable

The advantage of MOBILedit is that it can extract data from the iPhone from a computer with iTunes for Windows installed or without, which are very different ways of communication.

3.5.1.1 iTunes for Windows not installed

There is no need to install the iTunes Windows application to use MOBILedit (it is usually required by competitive solutions). In this case, MOBILedit is able to communicate directly with iPhone or iPad, just through the Apple device driver.

1. Install correct [Apple drivers](#)(see page 162).
2. Connect device to USB
3. Enable device communication
 - a. If you know passcode
 - I. Unlock the device screen.
 - II. Disable the "Auto-Lock" option(see page 168).
 - III. Confirm trust message on device screen.
 - b. If you don't know passcode use the [Lockdown method](#)(see page 98)

 If you want to use the [Checkra1n Jailbreak](#)⁵², the installation of iTunes is still required, since the communication requires Apple mobile device service.


3.5.1.2 iTunes for Windows installed

If you have the iTunes Windows application already installed, MOBILedit can also communicate with iPhone. In this case, MOBILedit uses protocols of Apple Mobile service, which is already part of iTunes installation.

You can follow the same procedure as above, starting from **point 2**.

3.5.1.3 Jailbroken iPhone and full file system extraction

If the iPhone is jailbroken, MOBILedit is able to extract all files, including application sandboxes or system files. To achieve this, MOBILedit needs iTunes installed so please follow the above instructions. You can jailbreak iPhones by using MOBILedit Connection Kit.

 Even with jailbreak, device encryption is still working, eg. if device was not unlocked after reboot, very limited set of data is available for extraction. Also some application protect files, when phone is locked, so for full filesystem extraction, you still need unlock phone.

3.5.2 Connecting iPhone by Wi-Fi

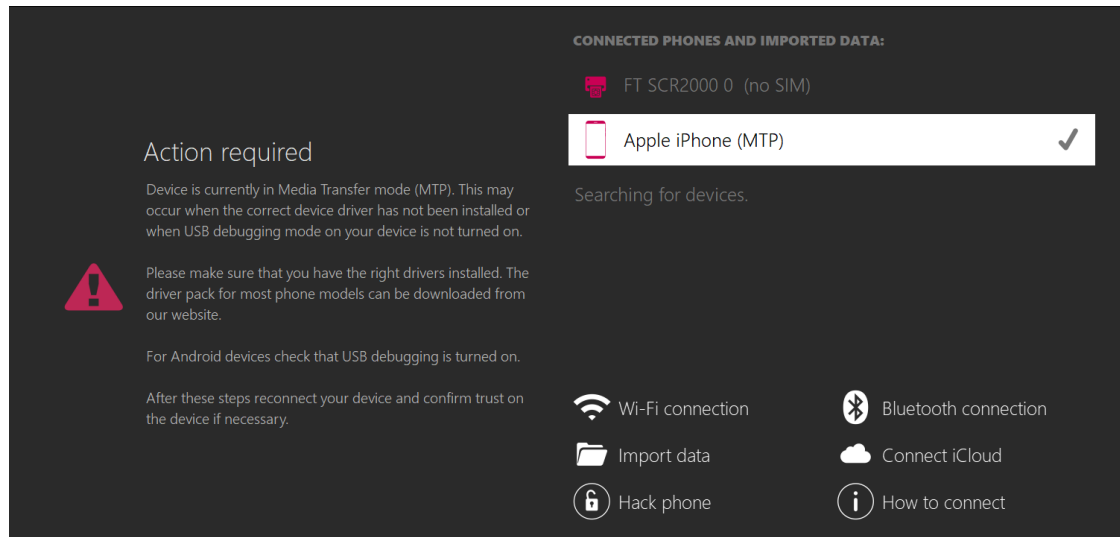
Using a Wi-Fi connection you will be able to work only with contacts, but including those stored in clouds, such as iCloud, Google contacts, Exchange server, etc. By using MOBILedit you will be able to fully write to contacts, edit, delete.

If you're having trouble with the connection, continue here: [Issues with the connection](#)(see page 162).

⁵² <https://forensic.manuals.mobiledit.com/MM/Jailbreaking-iPhone-with-checkra1n.2419785743.html>

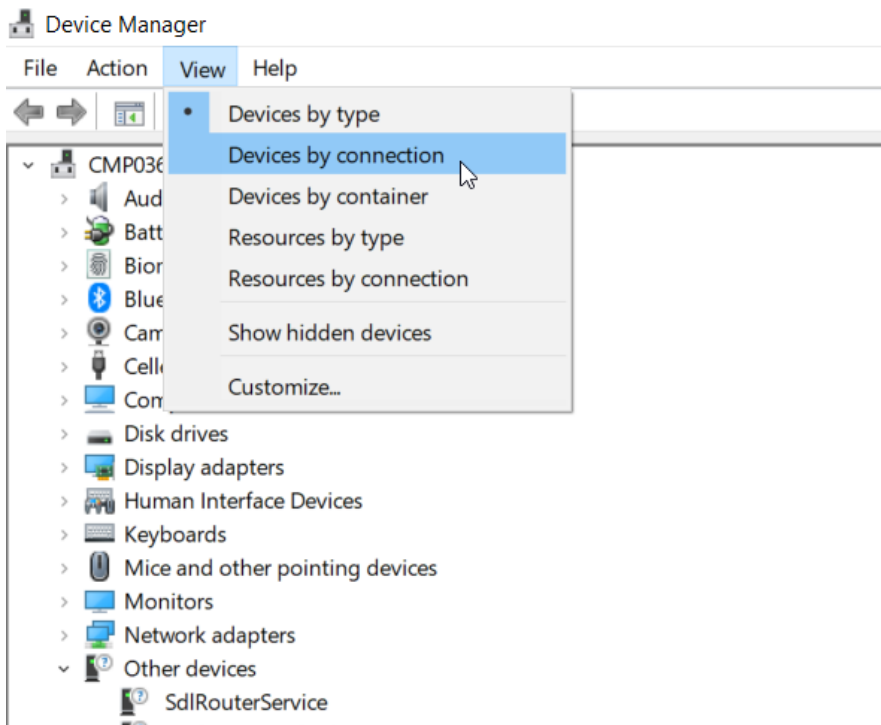
3.5.3 How to install correct Apple drivers

It is necessary to install device drivers properly. By default, Windows installs limited MTP media driver, which doesn't work.



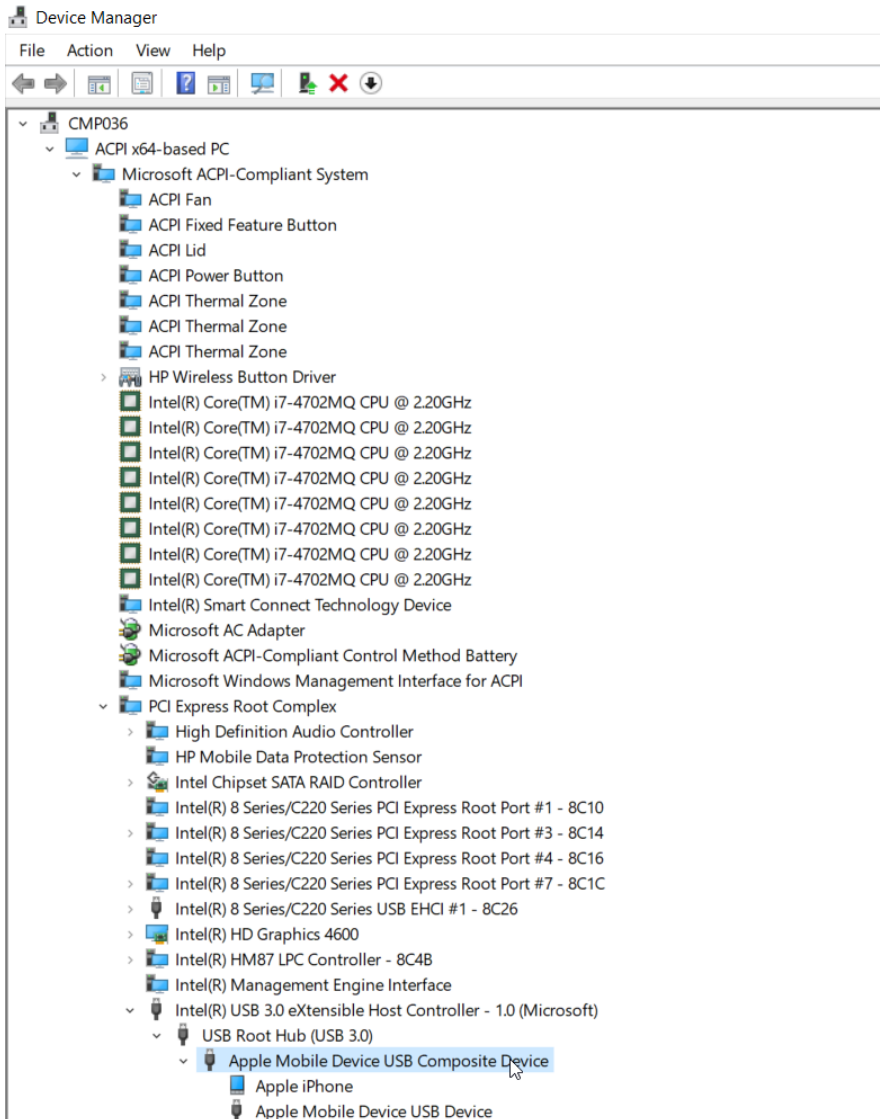
3.5.3.1 How to

1. Download and install the Apple drivers from our page [here](#)⁵³.
2. Open the Device Manager and change the view to "Devices by connection"



⁵³ https://download.mobiledit.com/drivers/setup_cdd_apple_1_0_10_0.exe

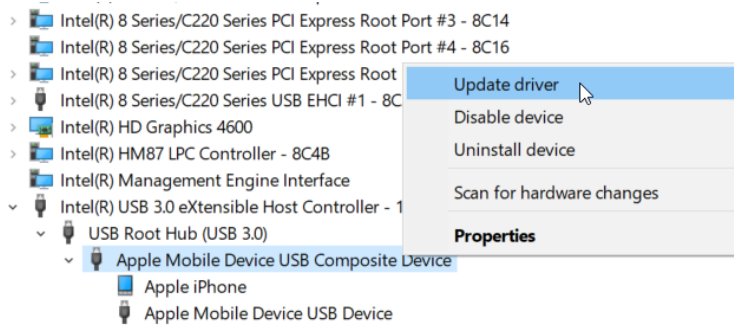
3. Expand section "ACPI x64-based PC" and sub-sections as you can see on picture below.



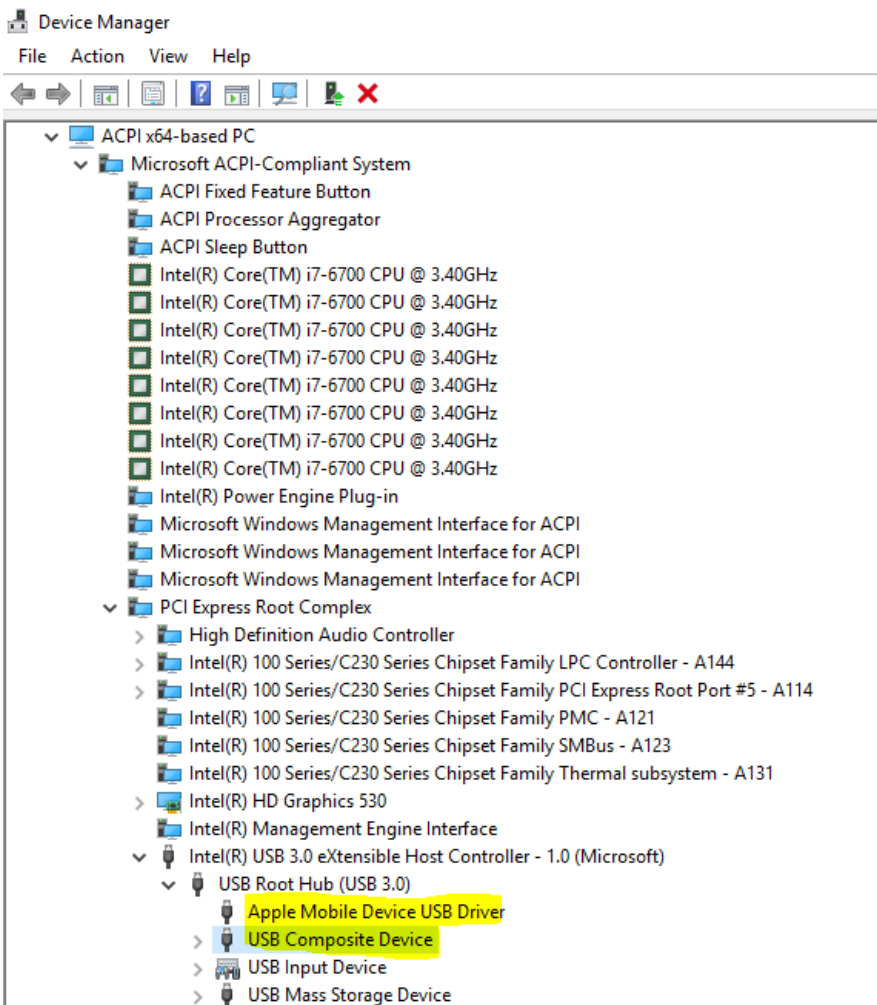
i If you see the "Apple Mobile Device USB Composite Device" continue with steps below, otherwise contact the [customer support](https://www.mobiledit.com/contact)⁵⁴ for additional help.

4. Right-click on "Apple Mobile Device USB Composite Device" and select "Update driver".

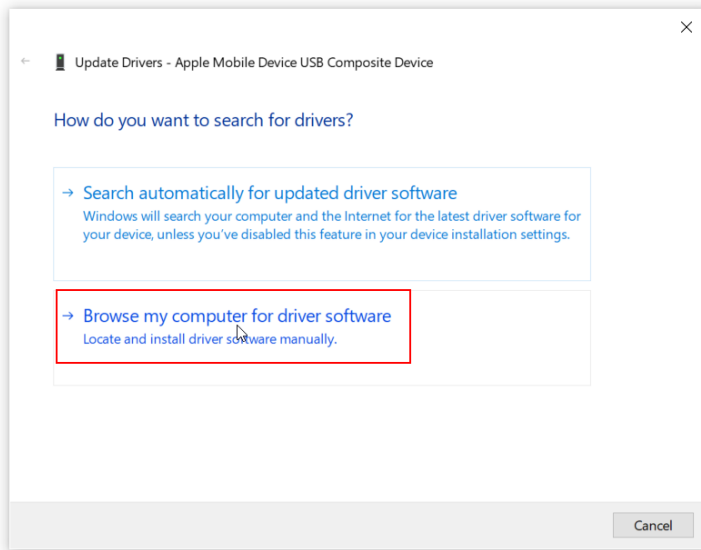
⁵⁴ <https://www.mobiledit.com/contact>



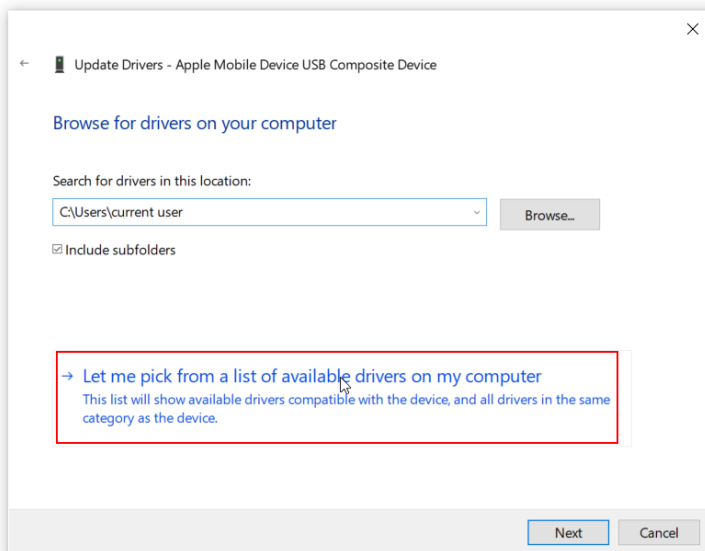
5. If Connecting iPhone model higher than 7, Select Apple USB Driver & USB Composite Device → Right-click → select Update Driver.



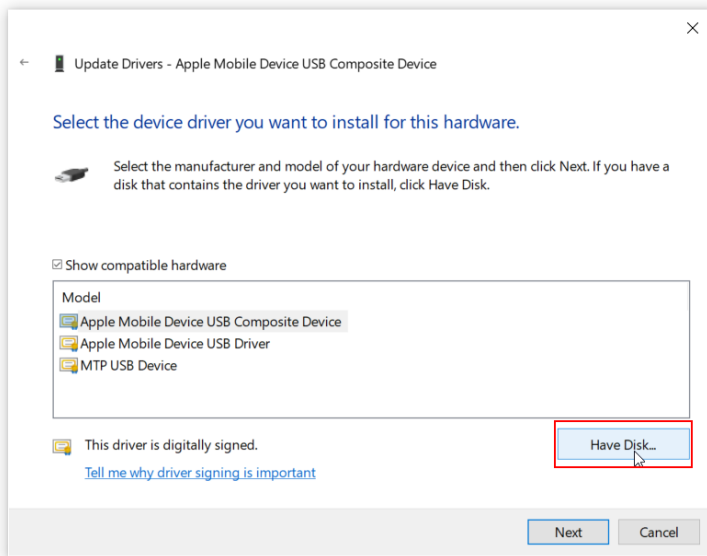
6. After selecting update driver, if a new window appears, select the option viewed below.



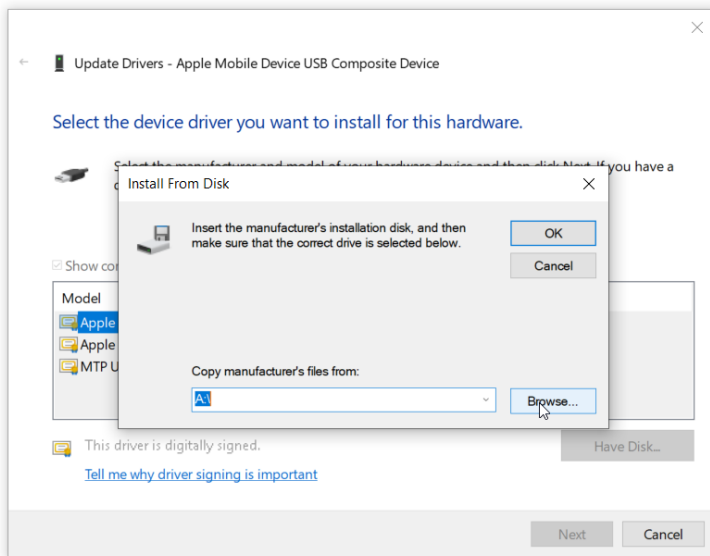
7. Next step is to click on the "Let me pick....." option.



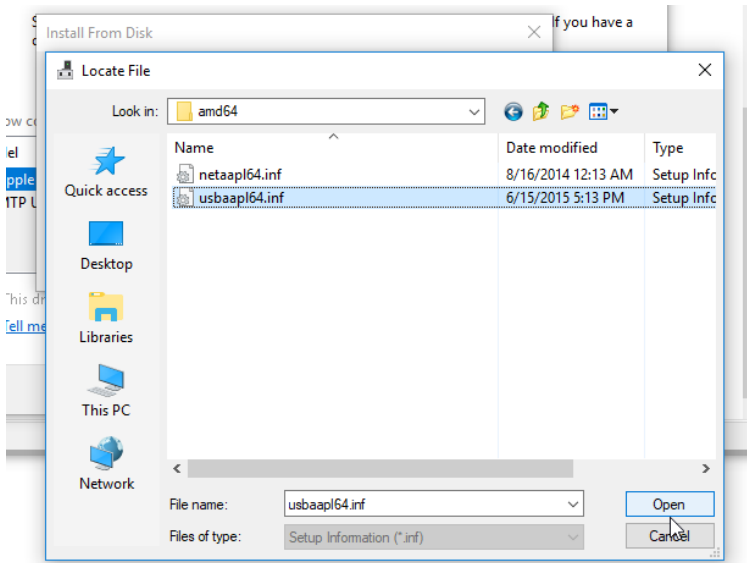
8. Choose "Have disk".



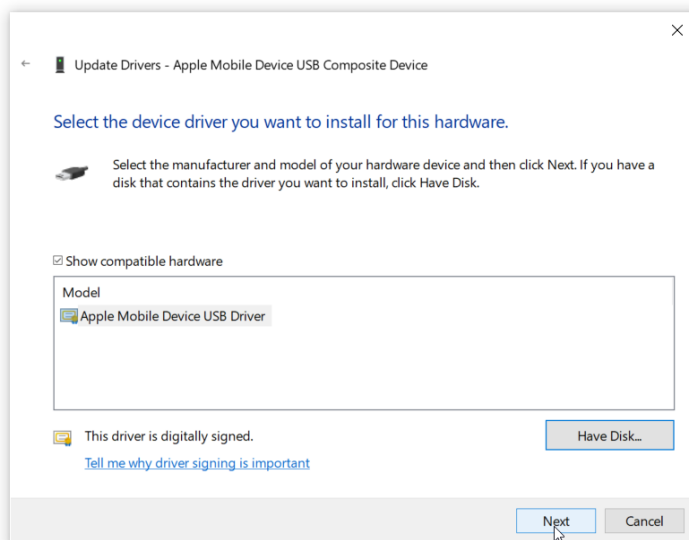
9. Click Browse and navigate to C:\Program Files\Compiled Driver Disc (Full)\Apple\amd64 (for 64-bit Windows) or \i386 (for 32-bit Windows).

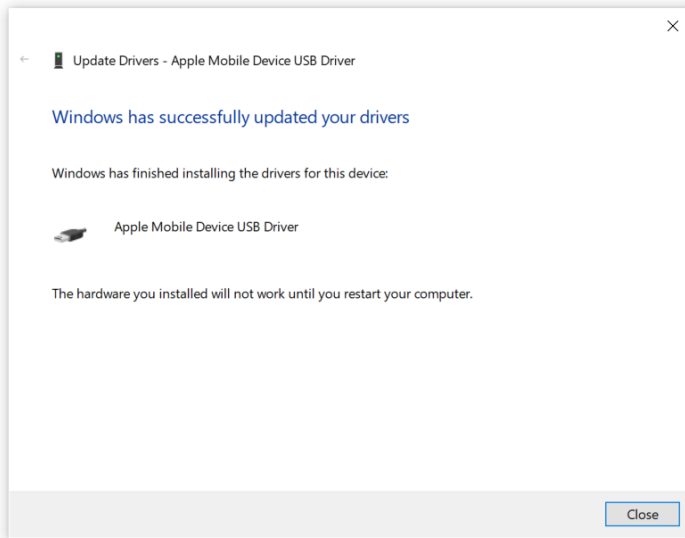


10. Choose usbaapl64 (64-bit Windows) or usbaapl (32-bit Windows) and click "Open".




11. Then click "Next" and "Close"





12. Restart the computer if requested.

 If you are still unable to connect your iOS device to the MOBILedit Forensic Express, please [contact our customer support](#)⁵⁵ for assistance.

3.5.4 How to disable the auto-lock option

To disable the auto-lock option, depending on the iOS version, follow the steps below:

3.5.4.1 iOS 10 and higher

1. Go to "Settings"
2. Choose "Display & Brightness"
3. Click on "Auto-Lock" and select "Never"

3.5.4.2 iOS 9.x and earlier

1. Go to "Settings" on your phone
2. Choose "General"
3. Scroll down to find the "Auto-Lock" option
4. Click on it and select "Never"

3.6 How to Connect Apple Watch

- [What can you extract](#)(see page 169)
- [Example of Apple Watch data in PDF report](#)(see page 170)

Our software can connect and extract information from Apple Watch up to series 5 by connecting it to your device via a specially designed Apple connector.

⁵⁵ <https://www.mobiledit.com/contact>

- i** For Apple watches series 0 and 1 is needed an **iBUS S1** connector.
For Apple watches series 2 and 3 is needed an **iBUS S2** connector.
For Apple watches series 4 and 5 is needed an **iBUS S4/S5** connector.

Once you successfully assembled the connector and connected the watch to your PC you should be prompted with a trust message on them.

At this point, you are going to proceed with the extraction as you would with any other device.



3.6.1 What can you extract

- Device info
- MAC addresses
- Memory
- UID
- SW revision
- Notes
- Voice recordings
- Files
- Application list
- Synchronized Photos (with their Locations, if they are available)
- and System logs

3.6.2 Example of Apple Watch data in PDF report

Table of Contents

Organizer

 Calendar Accounts

 Events

 Tasks

 Notes

Application List

Photos

Image Files

Audio Files

Video Files

Files

 Internal Files

 Applications Files

 Extra Files

 Misc Files

Locations

 GPS Locations

Logs

 System Logs



Timeline

Device Properties

Manufacturer	Apple
Product	Watch Series 3 38mm
HW Revision	N121sAP, Model:MQKV2
Platform	Apple
SW Revision	6.2.8_Firmware:iBoot-5540.144.2_Build:17U63
Device Name	Rudy's Apple Watch
Serial Number	FHLWV283J5X0
Device Unique ID	0ad7e3610e8bc5a64127e48b10e4bd529a5c0d6c
Device Time	2020-07-22 15:07:50 (UTC+2)
Time Zone	Europe/Prague
Wi-Fi MAC Address	50:A6:7F:D4:CF:75
Bluetooth Address	50:A6:7F:D1:CE:54
Ethernet Address	50:A6:7F:C4:FA:BE
Jailbroken	No
SIM Card	No
Total Storage	7.5 GB
Used Storage	4.8 GB

Notes (2)

All application notes, sorted by time in ascending order

1 Na žertvách 2196/34		Voice Note
	Created	2019-07-24 11:03:11 (UTC+2)
Duration	00:00:09	
Created	Modified	Last Visit
2019-07-24 11:03:11 (UTC+2)	-	-
Reminder	Removed	
No	No	
Source File	phone/raw0/Recordings/CloudRecordings.db : 0x13ace0 (Table: ZCLOUDRECORDING)	
2 Nahrávka		Voice Note
	Filename	20200709_125608.m4a
	Path	phone/raw0/Recordings/20200709_125608.m4a
	Size	103 KB
	Created	2020-07-09 12:56:08 (UTC+2)
	Modified	2020-07-09 12:56:21 (UTC+2)
Duration	00:00:13	
Created	Modified	Last Visit
2020-07-09 12:56:08 (UTC+2)	-	-
Reminder	Removed	
No	No	
Source File	phone/raw0/Recordings/CloudRecordings.db : 0x13abfd (Table: ZCLOUDRECORDING)	

Application List (59)






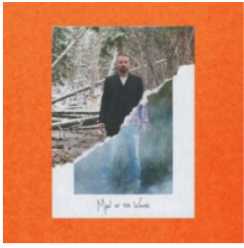

	AccuWeather com.yourcompany.TestWithCustomTabs.watchkitapp User Application Version: 1	Application Size: 20.1 MB	Data Size: 688.0 KB	Cache Size:
	Aktivita com.apple.ActivityMonitorApp System Application Version: 1.0	Application Size: 0 B	Data Size: 0 B	Cache Size:
	App Store com.apple.AppStore System Application Version: 1	Application Size: 0 B	Data Size: 0 B	Cache Size:
	AppStoreTrampoline com.apple.AppStoreTrampoline System Application Version: 1	Application Size: 0 B	Data Size: 0 B	Cache Size:
	Audioknihy com.apple.NanoBooks System Application Version: 144	Application Size: 780.0 KB	Data Size: 8.0 KB	Cache Size:



Image Files (8)

A subset of phone and application image files filtered by criteria: path not indicating a redundant image, sorted by time in ascending order

1 135a7f117cdc5b8f00203d0b79574b909c17b3																	
	<table border="1"> <tr><td>Filename</td><td>135a7f117cdc5b8f00203d0b79574b909c17b3</td></tr> <tr><td>Path</td><td>phone/raw0/iTunes_Control/iTunes/Artwork/Originals/ff/135a7f117cdc5b8f00203d0b79574b909c17b3</td></tr> <tr><td>Size</td><td>17.7 KB</td></tr> <tr><td>Created</td><td>2019-10-03 22:01:51 (UTC+2)</td></tr> <tr><td>Modified</td><td>2019-10-03 22:01:57 (UTC+2)</td></tr> <tr><td>Width</td><td>272 px</td></tr> <tr><td>Height</td><td>272 px</td></tr> <tr><td>Format</td><td>jpeg</td></tr> </table>	Filename	135a7f117cdc5b8f00203d0b79574b909c17b3	Path	phone/raw0/iTunes_Control/iTunes/Artwork/Originals/ff/135a7f117cdc5b8f00203d0b79574b909c17b3	Size	17.7 KB	Created	2019-10-03 22:01:51 (UTC+2)	Modified	2019-10-03 22:01:57 (UTC+2)	Width	272 px	Height	272 px	Format	jpeg
Filename	135a7f117cdc5b8f00203d0b79574b909c17b3																
Path	phone/raw0/iTunes_Control/iTunes/Artwork/Originals/ff/135a7f117cdc5b8f00203d0b79574b909c17b3																
Size	17.7 KB																
Created	2019-10-03 22:01:51 (UTC+2)																
Modified	2019-10-03 22:01:57 (UTC+2)																
Width	272 px																
Height	272 px																
Format	jpeg																
2 9f8a1f20d53515533d4e0c90c3d86cdf1cd04																	
	<table border="1"> <tr><td>Filename</td><td>9f8a1f20d53515533d4e0c90c3d86cdf1cd04</td></tr> <tr><td>Path</td><td>phone/raw0/iTunes_Control/iTunes/Artwork/Originals/ff/9f8a1f20d53515533d4e0c90c3d86cdf1cd04</td></tr> <tr><td>Size</td><td>20.4 KB</td></tr> <tr><td>Created</td><td>2019-10-03 22:49:16 (UTC+2)</td></tr> <tr><td>Modified</td><td>2019-10-03 22:49:16 (UTC+2)</td></tr> <tr><td>Width</td><td>272 px</td></tr> <tr><td>Height</td><td>272 px</td></tr> <tr><td>Format</td><td>jpeg</td></tr> </table>	Filename	9f8a1f20d53515533d4e0c90c3d86cdf1cd04	Path	phone/raw0/iTunes_Control/iTunes/Artwork/Originals/ff/9f8a1f20d53515533d4e0c90c3d86cdf1cd04	Size	20.4 KB	Created	2019-10-03 22:49:16 (UTC+2)	Modified	2019-10-03 22:49:16 (UTC+2)	Width	272 px	Height	272 px	Format	jpeg
Filename	9f8a1f20d53515533d4e0c90c3d86cdf1cd04																
Path	phone/raw0/iTunes_Control/iTunes/Artwork/Originals/ff/9f8a1f20d53515533d4e0c90c3d86cdf1cd04																
Size	20.4 KB																
Created	2019-10-03 22:49:16 (UTC+2)																
Modified	2019-10-03 22:49:16 (UTC+2)																
Width	272 px																
Height	272 px																
Format	jpeg																

Audio Files (23)

A subset of phone and application audio files filtered by criteria: path not indicating a redundant image, sorted by time in ascending order

1	842A2553-7EB8-4E75-880F-68A1FBB497C6	
	Path	phone/raw0/Recordings/CloudRecordings_SUPPORT/ FBF/ 842A2553-7EB8-4E75-880F-68A1FBB497C6
	Size	52.2 KB
	🕒 Created	2020-02-15 13:54:19 (UTC+1)
	🕒 Modified	2020-02-15 13:54:26 (UTC+1)
	👤 Name	Core Media Audio
	🕒 Duration	00:00:07
2	262708890252070030.m4p	
	Path	phone/raw0/Purchases/262708890252070030.m4p
	Size	6.49 MB
	🕒 Created	2020-06-02 12:27:13 (UTC+2)
	🕒 Modified	2020-06-02 12:27:22 (UTC+2)
	🕒 Duration	00:03:04

Locations


GPS Locations (1)

All GPS locations, sorted by time in ascending order

[Click here](#) to view GPS locations in interactive map

Latitude	50.09592 °
Longitude	14.42577 °
🕒 Time	1970-01-01 01:00:00 (UTC+1)
Event Origin	Media Photos
Event Type	Image

1 IMG_0945.JPG



📄 Filename	IMG_0945.JPG								
📄 Path	phone/raw0/DCIM/100APPLE/IMG_0945.JPG								
📄 Size	3.34 MB								
🕒 Created	2019-02-09 20:43:55 (UTC+1)								
🕒 Modified	2019-02-09 20:43:55 (UTC+1)								
🕒 Accessed	2020-09-01 19:39:49 (UTC+2)								
📍 Position	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>Latitude</td> <td>50.09592 °</td> </tr> <tr> <td>Longitude</td> <td>14.42577 °</td> </tr> <tr> <td>Time</td> <td>1970-01-01 01:00:00 (UTC+1)</td> </tr> <tr> <td>Altitude</td> <td>224 m</td> </tr> </table>	Latitude	50.09592 °	Longitude	14.42577 °	Time	1970-01-01 01:00:00 (UTC+1)	Altitude	224 m
Latitude	50.09592 °								
Longitude	14.42577 °								
Time	1970-01-01 01:00:00 (UTC+1)								
Altitude	224 m								
🕒 Exposure Time	1 / 6061 s								
📏 Focal Length	4.25 mm								
📏 F-Number	1.8								
📏 Lens Info	Apple iPhone XR back camera 4.25mm f/1.8, Focal length 4.25 mm, f/1.8								
↔️ Width	3024 px								
⬆️ Height	3780 px								
📷 Camera Manufacturer	Apple								
📷 Camera Model	iPhone XR								
📄 Format	jpeg								
🕒 Date of Generation	2019-02-08 13:58:16 (UTC+1)								
🕒 Date of Digitization	2019-02-08 13:58:16 (UTC+1)								



Files

Internal Files (263 files)

Filename	Size	Created	Modified	Accessed
/				
/DCIM/				
/DCIM/100APPLE/		2019-10-03 21:40:23	2020-07-23 01:40:09	
IMG_0928.JPG	84.1 KB	2020-07-10 14:36:38	2020-07-10 14:36:43	
SHA-256 hash: DF8CFFB8F11E2C41A87357986E185FC429699AAE300936B6A108E4D9350D881F MD5 hash: 216BA7899D82889B71CBEB182644B0FA				
IMG_0945.JPG	3.34 MB	2019-02-09 20:43:55	2019-02-09 20:43:55	2020-09-01 19:39:49
SHA-256 hash: C0C16B01DBB6C183601151149C2D64AD672A497E6874BB1625F12B07C47D0E24 MD5 hash: 8433D68461E16A75C8E8CDA1DF0C1481				
IMG_4053.JPG	251 KB	2020-07-12 22:22:02	2020-07-12 22:22:02	2020-09-01 19:39:26
SHA-256 hash: C27AF7E7A57E7555ACF68B0F2CA167208941821AD76E6111EBD6CFC650E7EDCC MD5 hash: 8A74D580CD860C16A54AFCCEZ7102D2B				
IMG_4097.JPG	4.13 MB	2020-07-21 18:52:15	2020-07-21 18:52:16	2020-09-01 19:39:27
SHA-256 hash: D0907611398130795A47A28FB8D60717688BDD019C4CE3762B25DC6410B9E71 MD5 hash: B02E0186E6C0C9933B2B31B8BF1B97F0				
IMG_4106.JPG	3.43 MB	2020-07-24 22:03:23	2020-07-24 22:03:23	2020-09-01 19:39:17
SHA-256 hash: 8EE91C7152629834135C3EC6A4A5931F0E82E6B1F6BC42D0C3E1C43847860B248 MD5 hash: C47F0A728684E9EC44FF6399EEFCF46A				
/PhotoData/		2019-10-03 21:31:32	2020-03-25 09:07:16	
Photos.sqlite	2.85 MB	2019-10-03 21:31:32	2020-07-21 00:09:55	
SHA-256 hash: 9B51E6B6E7F693B7DFA9121795B89F2ECB05A42F5D1B152EDFD97F6771DA9EF MD5 hash: 31B36C0991040370FA869DC62E658349				
Photos.sqlite-shm	32.0 KB	2019-10-03 21:31:33	2020-07-15 21:18:00	
SHA-256 hash: 022C8D2C69DB55F988D712F5F8D2989BE097CDD57E9736628798CB07759ED166 MD5 hash: B085468FD4E4C6C1366D659A6B0051BB				
Photos.sqlite-wal	1.46 MB	2019-10-03 21:31:33	2020-07-22 00:07:06	
SHA-256 hash: DBC4F20FAA7377DB7D994C0337235A7E75140AA5835B6466528066994E8433 MD5 hash: 97C368436BC50C579215963897B1DC0E				
protection	0 B	2019-10-03 21:31:34	2019-10-03 21:31:34	
SHA-256 hash: E3B0C44298FC1C149AFBF4C8996FB92427AE41E46498934CA495991B7852B855 MD5 hash: D41D8CD98F00B204E9800998ECF8427E				

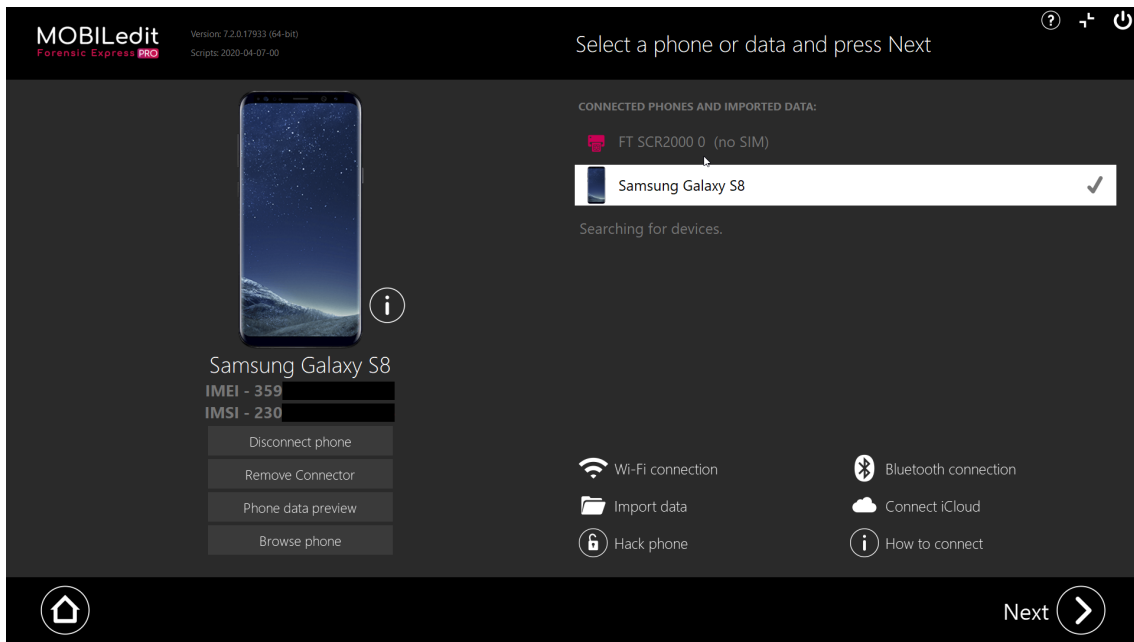
System Logs

Diagnostic logs (sysdiagnose)

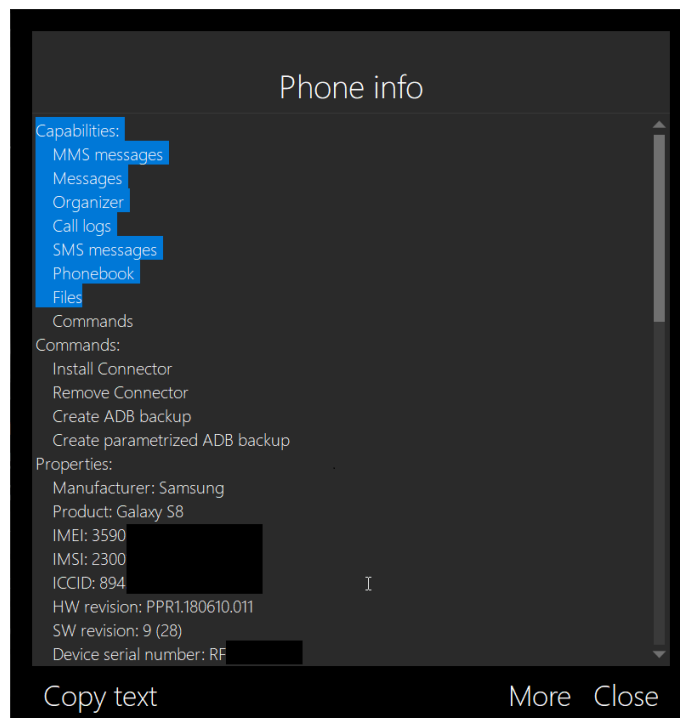
Ethernet Address	50:a6:7f:c4:fa:be
Wi-Fi MAC Address	50:a6:7f:d4:cf:75
Bluetooth Address	50:a6:7f:d1:ce:54
Hardware Model	N121sAP
Platform	t8004
Firmware	iBoot-5540.144.2
 User Name	Rudy's Apple Watch
 Device Name	Apple Watch
Product	Watch OS
Type	Watch3,3
Version	6.2.8
Device Build Version	17U63
Country Code	CN
Serial Number	FHLWV283J5X0
Device Unique ID	0ad7e3610e8bc5a64127e48b10e4bd529a5c0d6c
Total Data Available	2.9 GB
Total Data Capacity	4.8 GB
Total Disk Capacity	7.5 GB
Total System Available	0 B
Total System Capacity	2.5 GB

3.7 Info button on the connection screen

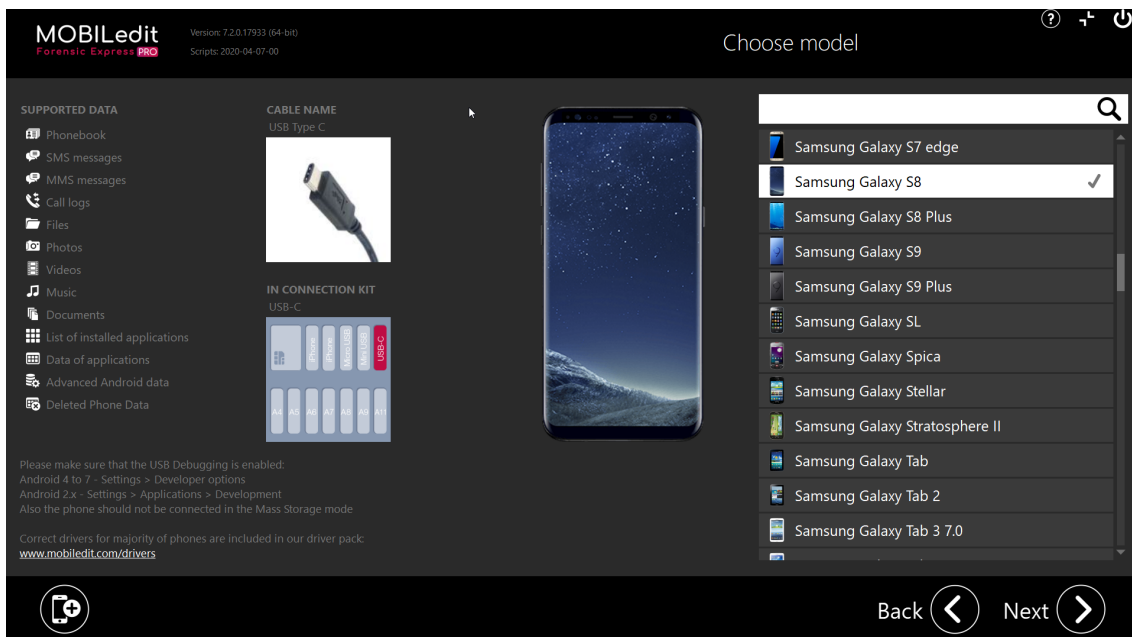
After connecting your device, an **info button** ⓘ will appear next to the picture of your phone:



The button will provide you with detailed info about the connected device and allows you to copy all the displayed info:



The **More** button will take you to the screen with additional information related to your device model.



The **Info** button will provide you with the following details:

- Capabilities
- Commands
- Properties

3.7.1 Capabilities:

Data that can be harvested by our software. Namely call logs, SMS/MMS, Organizer, Emails, Messages, Files.

i additional available data will be shown during the process. This part does not represent the final report.

3.7.2 Commands:

Commands we are able to send to your phone in order to cooperate, such as Connector installation and update, passwords, backups creating, re/authentications, and such.

3.7.3 Properties:

General info about the device such as manufacturer, IMSI, SIM card info, accounts linked to the device, HW info, storage info, etc.

i This advanced feature only shows basic data from the connected device. For complete acquisition please use the standard full/specific extraction.

3.8 Disconnecting phone

After finishing phone data extraction (you will see the text "**Data extraction finished**" in the white log panel) you can safely disconnect the phone from the PC.

```

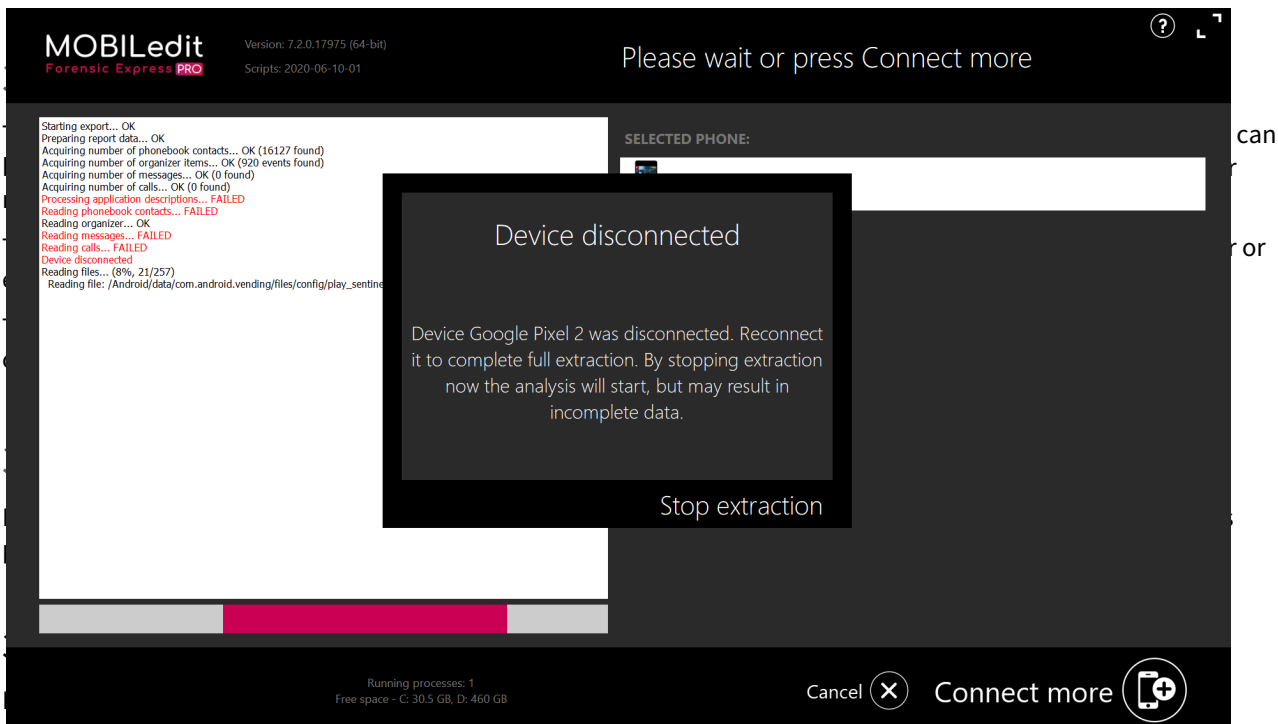
Preparing report data... OK
Acquiring the number of organizer items... OK
Reading organizer... OK
Reading files... OK (114 files succeeded, 0 files failed)
Data extraction finished
  All 57 organizer items were successfully extracted
  All 114 documents were successfully extracted
Phone can be disconnected now
Processing source data... OK
Preparation for exports..
  
```

If extracting from an Android phone please make sure that you uninstall the Forensic Connector application from the phone (this application is used for communication between the PC and the Android phone).

To uninstall Forensic Connector, please follow steps below:

1. Go to Settings / Applications
2. Select Forensic Connector from the list
3. Tap on Uninstall and confirm

If the phone is disconnected during the extraction process, you will get a 'Warning' message that the phone has been disconnected. You can either reconnect the phone to continue with the extraction or skip the extraction and continue with exports. Please note that if you do not complete the entire data extraction process the result will be incomplete phone data exports.



Upon connecting the phone to your PC you will be asked in which mode should the phone be connected.

Select either Nokia OVI and wait for drivers to be installed or Nokia Suite mode to ensure the ability of the phone to communicate with the PC

3.10.2 Connecting Windows phone

3.10.2.1 Whats is supported

Windows Phone is a very closed OS, which gives it better security and stability, but there is no tool available to fully manage the phone content. You can manage files using a few tools but you can not manage your contacts, messages, and others.

We worked hard to offer the maximum possible. Our software can read contacts from this phone using Bluetooth. MOBILedit can also write contacts into this phone. It is impossible to manage contacts online, but you can write contacts using Phone Copier Express or Data Transfer plugin in MOBILedit.

So you are able to:


- Read contacts using Bluetooth
- Write contacts using cable connection and our driver (not available for Forensic products)
- Manage your media files

3.10.2.2 How to connect Windows Phone

What you need is a device driver for Windows and your specific phone, you can download it from the manufacturer's website or [here](#)⁵⁶.

[Connecting Windows Phone via USB cable](#)⁵⁷ **only for MOBILEEDIT!**

[Connecting Windows Phone via Bluetooth](#)⁵⁸ **only for MOBILEEDIT!**

 It is not recommended to have Zune software installed. This software will block your connection with our software. If you have installed Zune by accident and want to work with our software, please uninstall your Zune software. During the driver installation, you will be prompted by your operating system to confirm the acceptance of our driver.

3.10.2.3 Windows CE Phone connection

Download the phone driver [here](#)⁵⁹. If you are using the computer with the version of the Windows 10 1703 and above it is necessary to do the settings change.

After the driver installs, it is necessary to right-click on Start, and then click on Computer Management /Services & Applications /Services.

Scroll down to right-click on "Windows Mobile-2003-based device connectivity" to select Properties / Log On.

Switch to "Local System account" with checking "Allow service to interact with desktop" then click OK.

⁵⁶ <http://www.mobiledit.com/downloads#phone-drivers>

⁵⁷ <https://phonemanager.manuals.mobiledit.com/UGME/Connecting-Windows-Phone-via-USB-cable.2151743546.html>

⁵⁸ <https://phonemanager.manuals.mobiledit.com/UGME/Connecting-Windows-Phone-via-Bluetooth.2151710732.html>

⁵⁹ <https://support.microsoft.com/en-us/help/931937/description-of-windows-mobile-device-center>

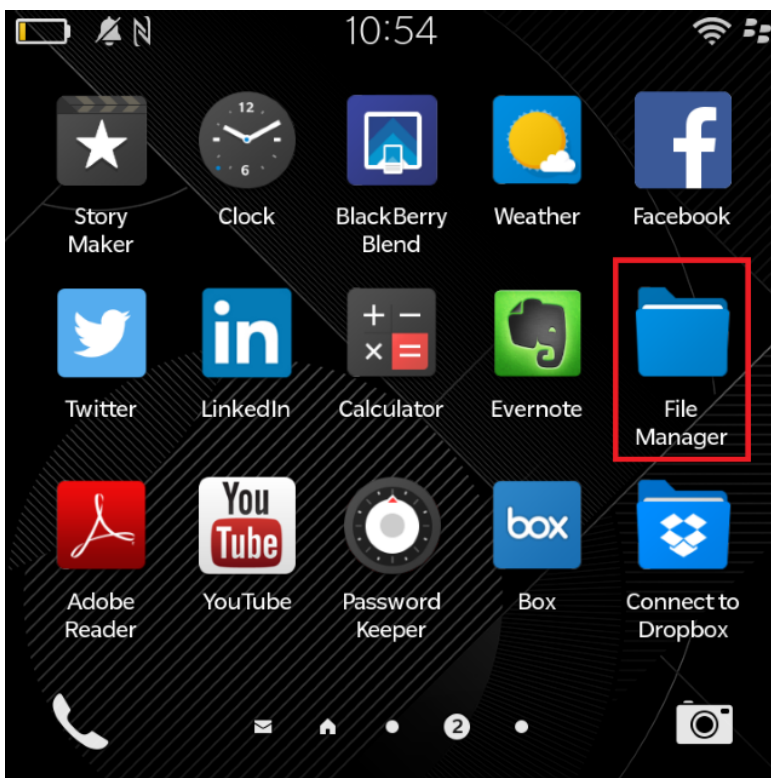
3.10.3 Connect BlackBerry via WiFi

BlackBerry OS 10 allows the user to install Android apps onto BlackBerry devices thanks to the Android Compatibility Layer. This can be used to install the Android Connector app in order to connect your device to MOBILedit products via the WiFi network.

You'll find a guide on how to install the Connector app below:

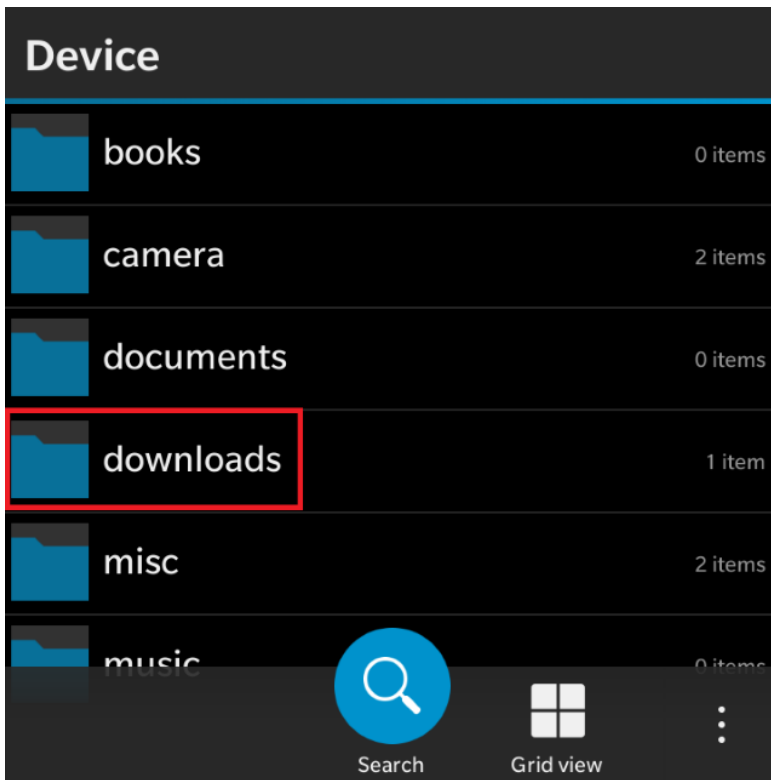
3.10.3.1 MOBILedit and Phone Copier Express installation guide

1. On your BlackBerry device, go to [this page](#)⁶⁰ and download the latest PhoneCopier.apk file
2. Open the File Manager app

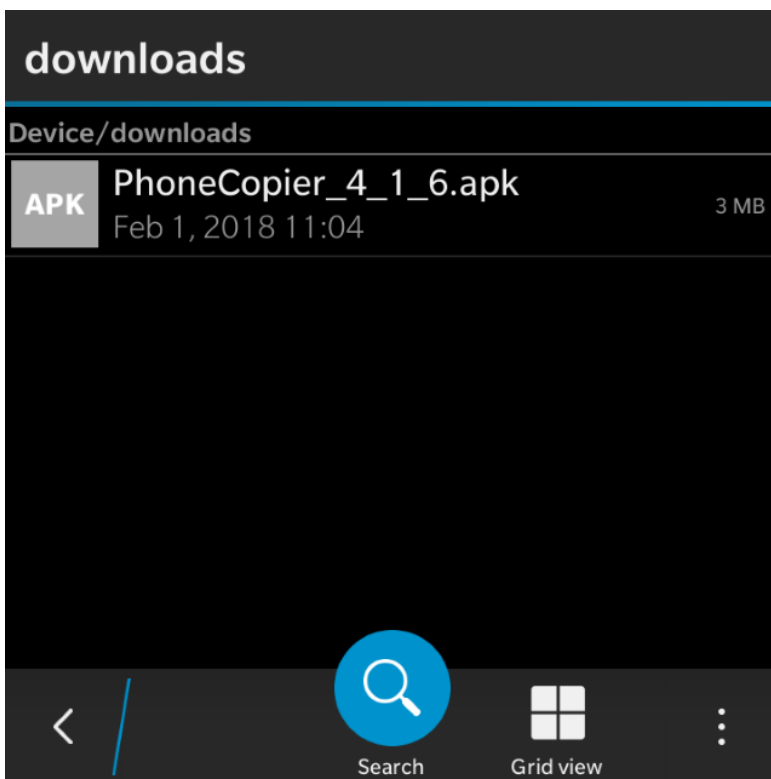


Open the "downloads" folder

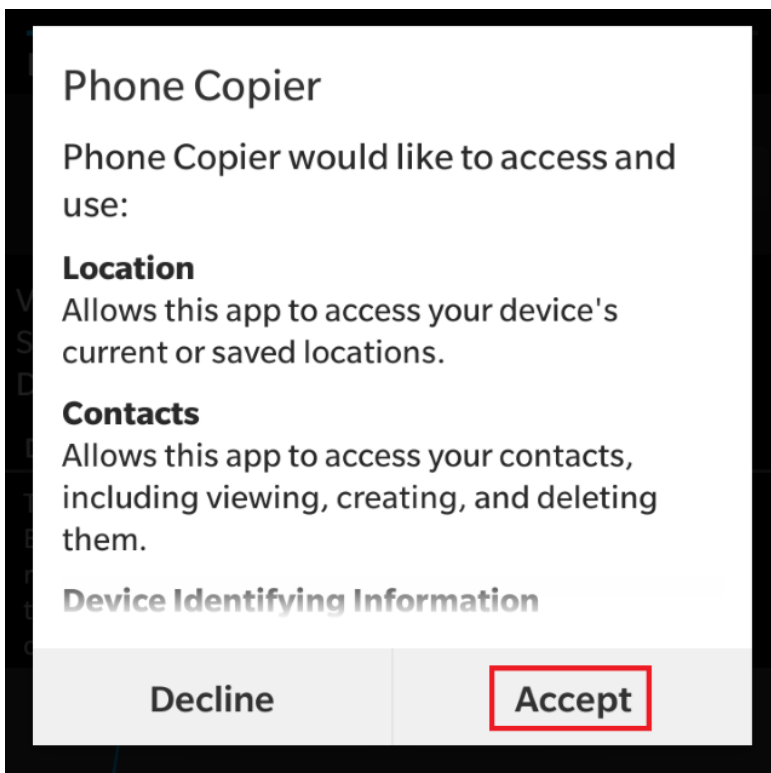
⁶⁰ <http://www.mobiledit.com/download-list/phone-copier-for-android>



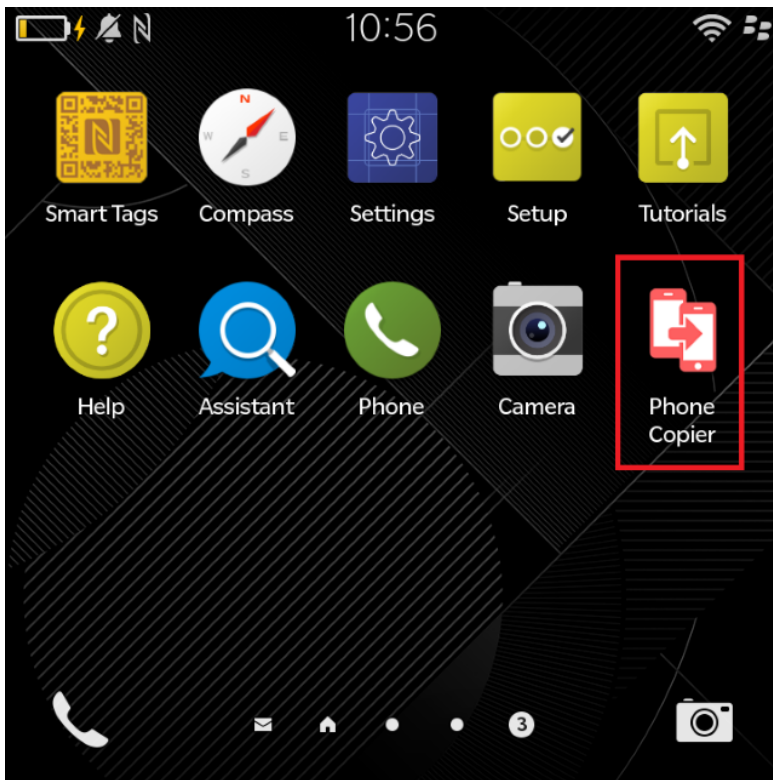
Find the PhoneCopier.apk file and open it



On the next screen, click on "Install" and accept the request for data access



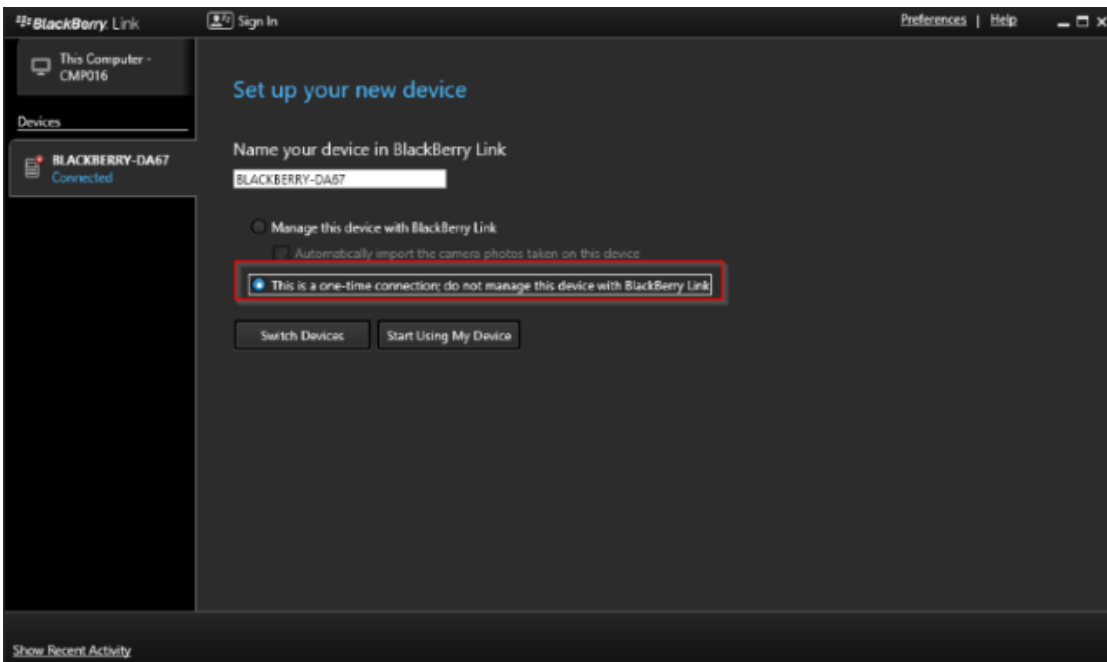
After the installation, you'll find the Phone Copier app on your home screen



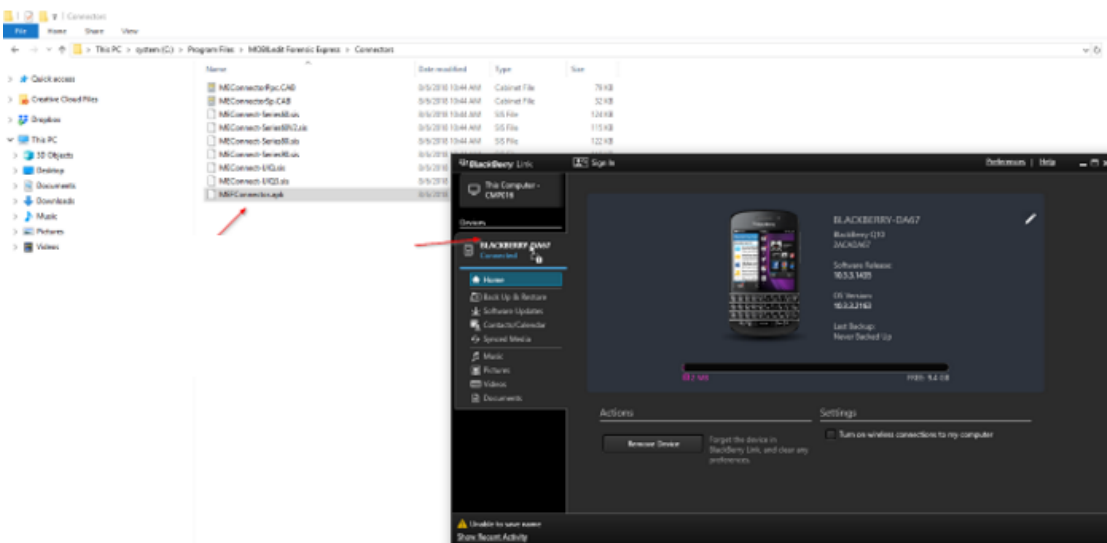
3.10.3.2 MOBILedit Forensic Express installation guide

1. Download the Blackberry Link software [here](https://us.blackberry.com/software/desktop/blackberry-link)⁶¹
2. Install it.
3. Connect your Blackberry OS 10 device using the USB cable to the computer.
4. Select the one-time connection and click "Start Using My Device"

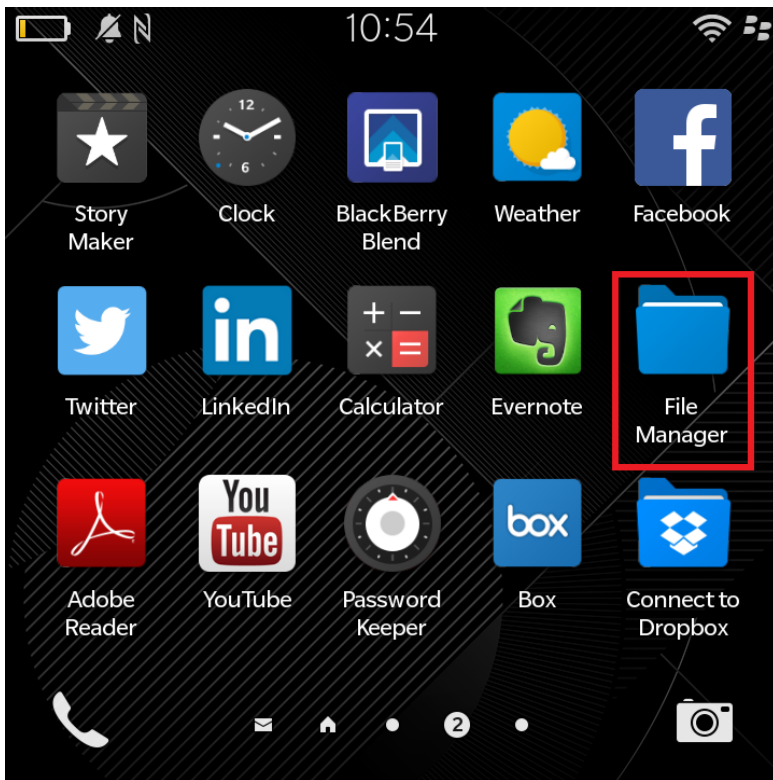
⁶¹ <https://us.blackberry.com/software/desktop/blackberry-link>



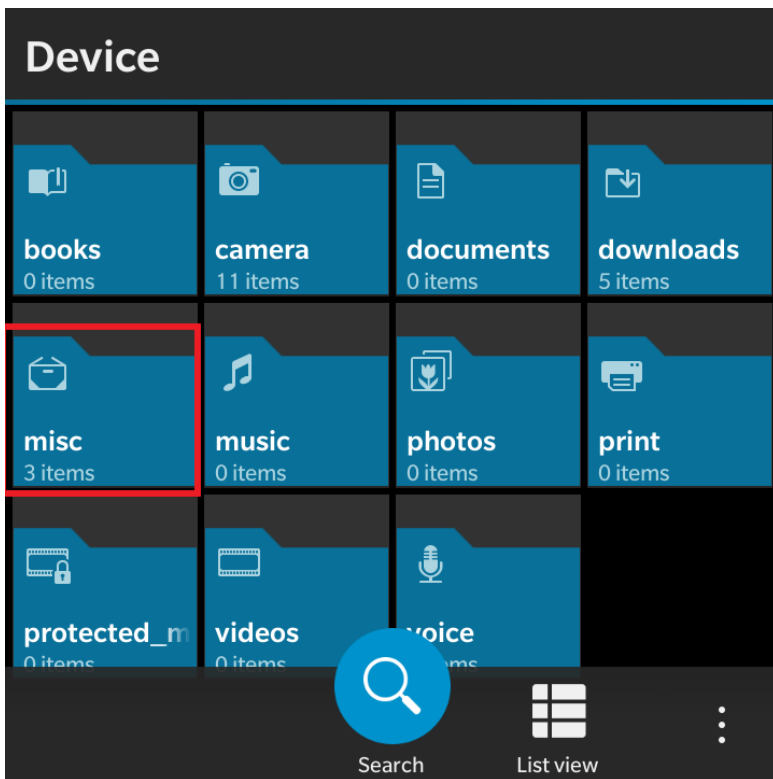
5. Go to the folder where you have installed the MOBILedit Forensic Express (default C:\Program Files\MOBILedit Forensic Express).
6. Open the "Connectors" subfolder.
7. Drag and drop the MEFCconnector.apk file into your Blackberry device in Blackberry Link.



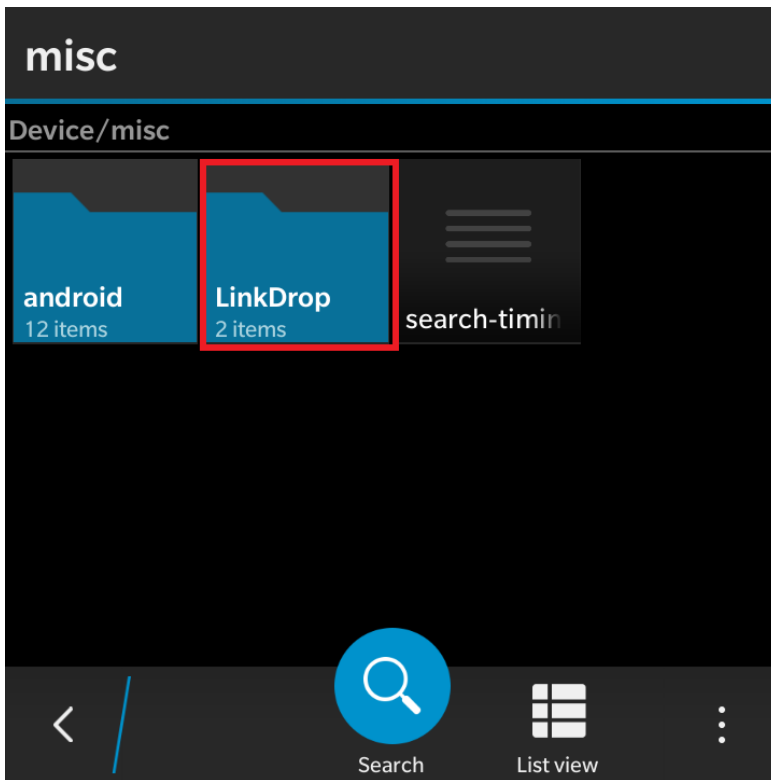
8. On your device open the File Manager app.



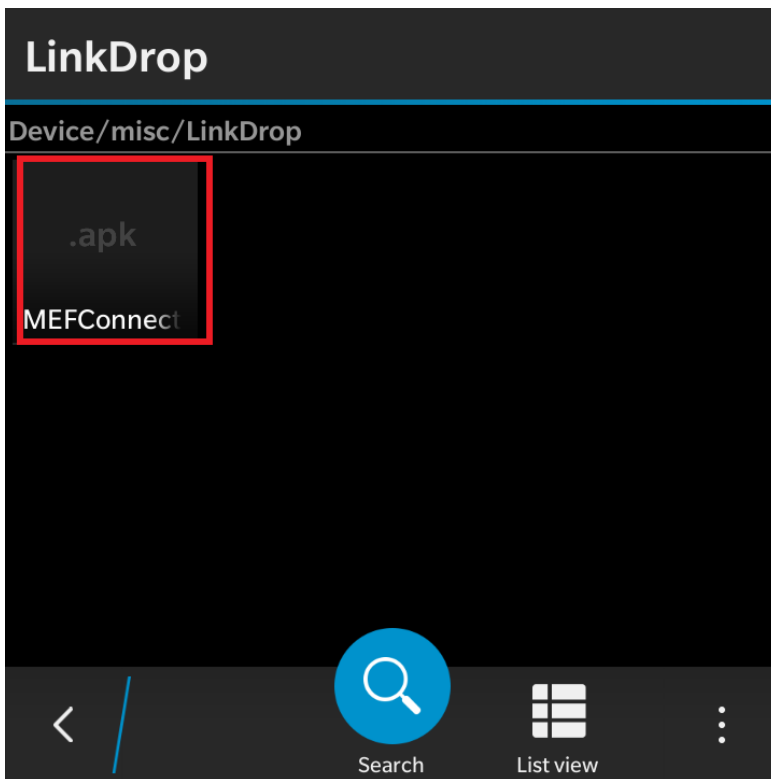
9. Open the "misc" folder



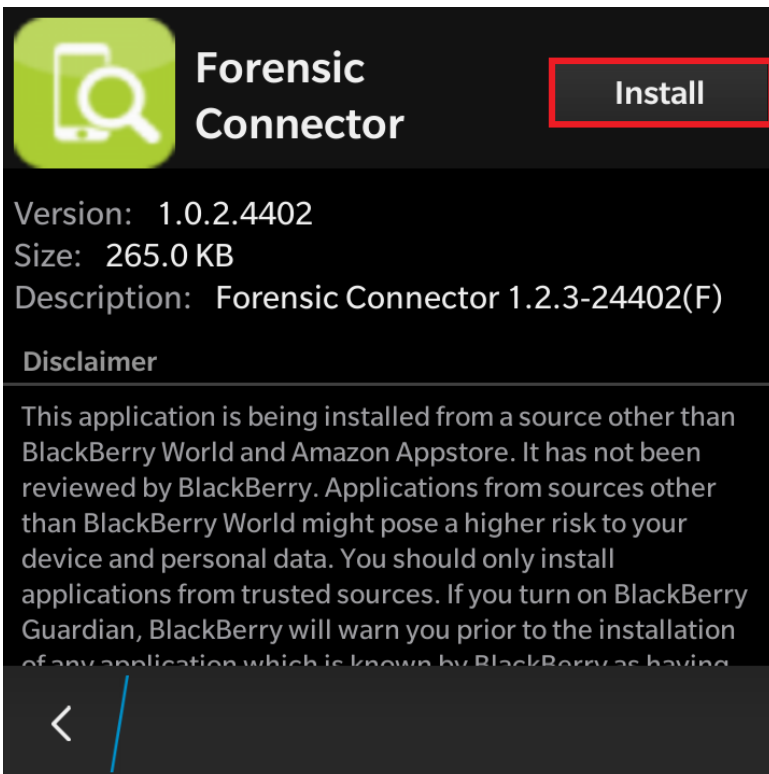
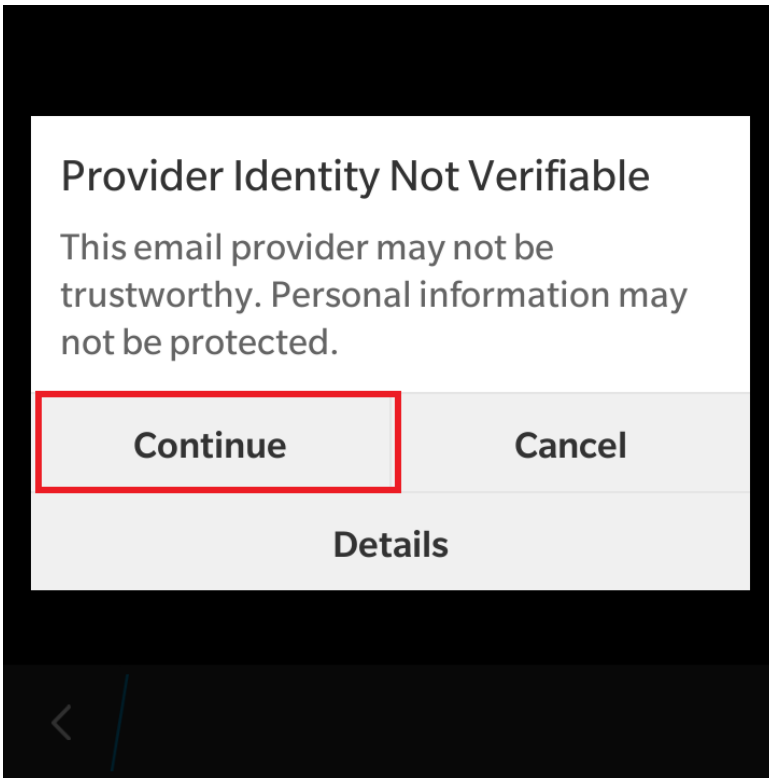
10. Open the "LinkDrop" folder

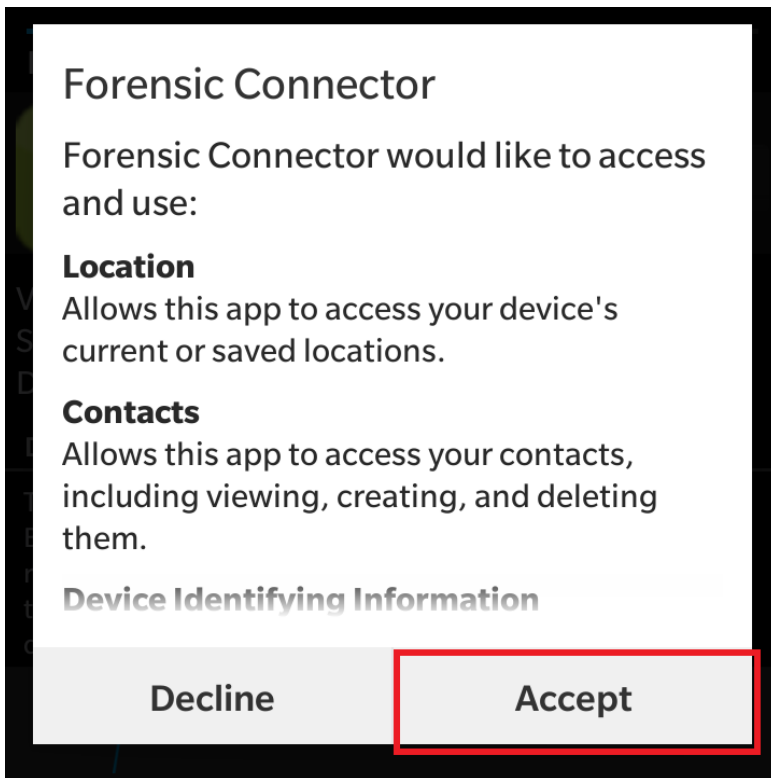


11. Find the MEFConnector.apk file and open it

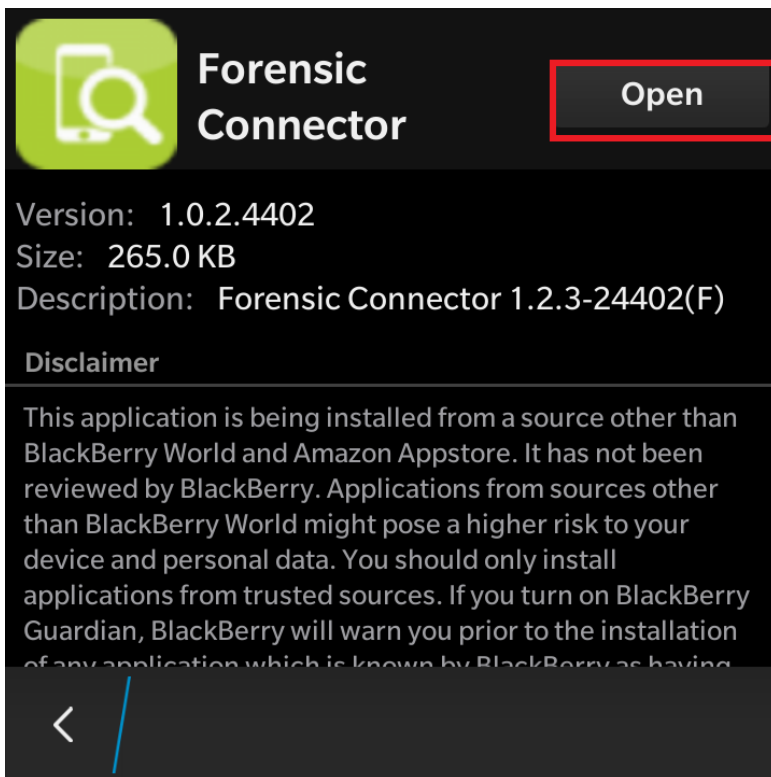



12. On the next screen, click on "Install" and accept the request for data access





13. Open the app and proceed to connect your device.



 Please note that you will not be able to access either internal or user filesystem using this connection method.

3.10.4 Blackberry OS devices

Blackberry has a very unique and secured OS which is hard to work with, however, we have done the maximum to offer as much support as possible.

Phones with **Blackberry OS 10** can be connected to the MOBILedit via Bluetooth or WiFi.

Bluetooth connection allows you to read contacts stored on the device, nevertheless, this content is Read-Only. WiFi connection will provide you with more data, however, the connection requires the installation of the **Android Compatibility Layer**⁶². The amount of data depends on what will be allowed by the emulator itself. Please follow our step-by-step instructions [here](#)(see page 181).

Devices running **Blackberry OS 9 and earlier** can be connected to MOBILedit via cable connection. This will allow you to manage and see the whole content of your Blackberry such as Messages, Phone book, Calendar, Application, and Media.

It is only necessary to install the correct drivers, MOBILedit should recognize your phone by itself.

3.11 Android - Español


Para conectar correctamente un teléfono, se deben completar algunos pasos fundamentales para esta herramienta o cualquier otra. Estos ajustes solo serán necesarios la primera vez. Después de realizarlos, podrá disfrutar de las funcionalidades de todos nuestros productos. Se puede conectar el teléfono Android a un PC por medio de un cable USB, que permite una transferencia de datos más rápida, o por wifi, que resulta más fácil.

[Descargue aquí nuestro folleto de instrucciones para imprimirlo](#)⁶³



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=y_78HkdT_hw&feature=emb_logo

 ¡No conecte el teléfono a su PC antes del paso 3!

Habilite la depuración USB para que su teléfono se pueda conectar a un PC

1. [Habilite la opción Permanecer activo](#)(see page 203) para que su teléfono no se desconecte
2. Instale el controlador para dispositivos Windows para su teléfono, descargable [aquí](#)⁶⁴
3. Ahora conecte su teléfono a un PC que ejecute MOBILedit
4. [Confirme la huella digital RSA](#)(see page 200) en la pantalla de su teléfono
5. [Seleccione el modo MTP](#)(see page 196) en la pantalla del teléfono

⁶² <https://www.blackberry.com/us/en/support/desktop-software-downloads>

⁶³ <https://download.mobiledit.com/documents/connection%20sheet%20a4%20lt.%20america.pdf>

⁶⁴ <http://www.mobiledit.com/download-list/universal-android-driver>

¡Ya puede disfrutar de nuestro producto! No necesita hacer nada más, MOBILedit encontrará su teléfono automáticamente.

Si usted conectó su teléfono al PC antes del paso 3, es posible que Windows haya instalado el controlador equivocado. En ese caso, MOBILedit no podrá reconocer el teléfono. [Aquí](#)⁶⁵ encontrará una guía para borrar el controlador incorrecto de Windows con nuestro controlador universal de Android.

3.11.1 Si su teléfono no se conecta

- MOBILedit solicitará la instalación en su teléfono de una pequeña aplicación llamada Connector. Si no se instala automáticamente, recomendamos reconectar el teléfono y reiniciar MOBILedit, o descargar la app Connector directamente [aquí](#)⁶⁶. Si su teléfono es de la marca Xiaomi, otorgue permisos para los ajustes necesarios antes de la instalación.
- ¿La depuración por USB no se activa? ¿La clave RSA no aparece en la pantalla? Intente desactivar la depuración por USB y reactivarla de nuevo después de conectar el teléfono.
- Asegúrese de que el teléfono no esté en modo de almacenamiento masivo.
- Si lo anterior no soluciona el problema y usted utiliza cualquier otra herramienta de teléfono, como HTC Manager, Eclipse o Android Studio, será necesario detener el proceso ADB en el Administrador de tareas, o desinstalar el software.
- Si utiliza el sistema operativo Windows 7 y su teléfono no se conecta automáticamente o no es detectado, siga [las instrucciones en el artículo](#)(see page 225) sobre cómo cambiar manualmente el controlador ADB.
- ¿Problemas para conectar un teléfono Huawei? Haga clic [aquí](#)(see page 203) para averiguar cómo evitarlos.
- ¿Problemas para conectar un teléfono Xiaomi? Haga clic [aquí](#)(see page 203) para averiguar cómo evitarlos.

3.11.2 Conexión Wi-Fi con Android

La aplicación de Android Connector se puede descargar en nuestra [página](#)⁶⁷ de descargas. Ahora inicie la aplicación de conexión en su teléfono.

- Asegúrese de que el wifi esté encendido y que esté conectado a la misma red.
- Ejecute MOBILedit y haga clic en el botón Conectar.
- Seleccione Teléfono - Conexión wifi y después introduzca la dirección IP que aparece en la pantalla del teléfono.
- Otorgue permiso para la conexión en su teléfono si la clave coincide con la clave del Connection Wizard

Su teléfono será localizado. Puede hacer clic en el botón Terminar para que el dispositivo se conecte automáticamente.

¡Genial! Acaba de conectar su teléfono por medio de su red wifi.

3.11.3 Android - Habilitar la opción "Permanecer activo"

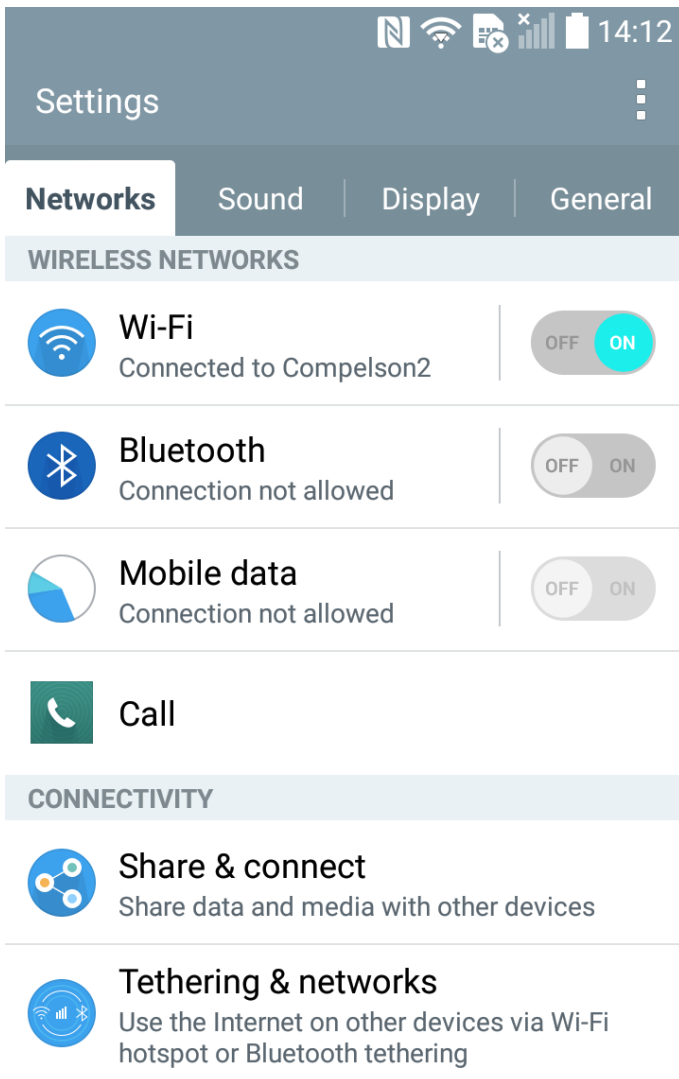
La opción Permanecer activo debería estar configurada en su teléfono para permitir una comunicación continua entre el teléfono y el software. Si el teléfono no está configurado en Permanecer activo, y está en modo Ahorro de energía, podría desconectarse de nuestro software, y de otras fuentes, e interrumpir el proceso de extracción y análisis.

1. Acceda a la Configuración de su teléfono.

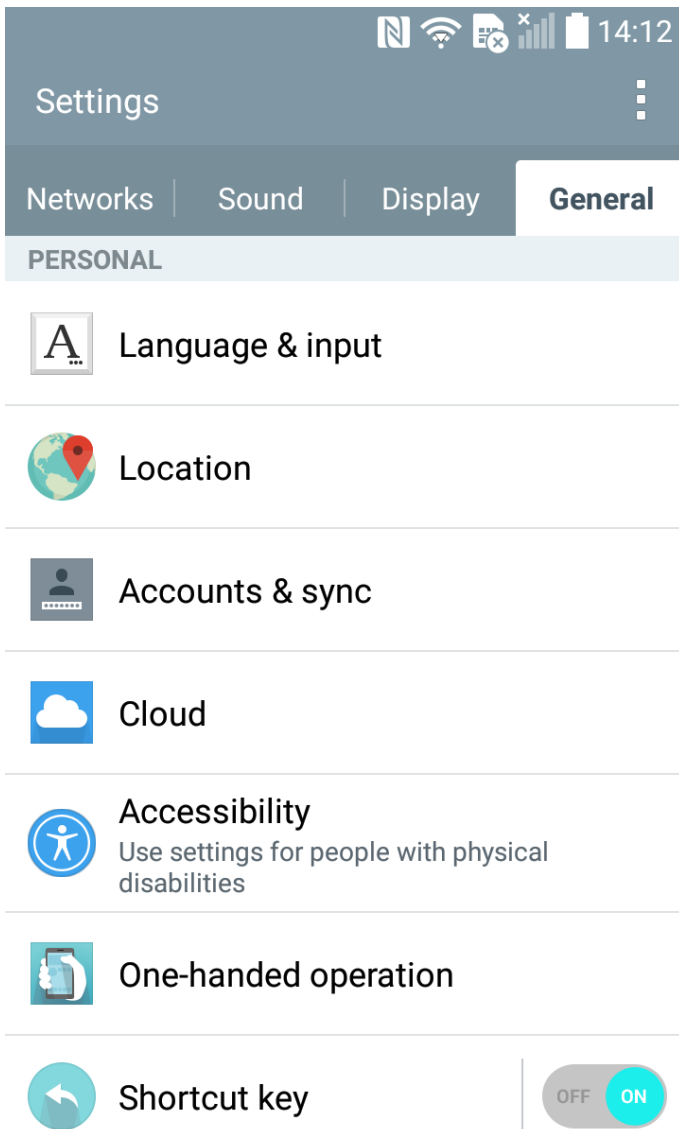
⁶⁵ <https://www.mobiledit.com/download-list/universal-android-driver>

⁶⁶ <https://www.mobiledit.com/downloads>

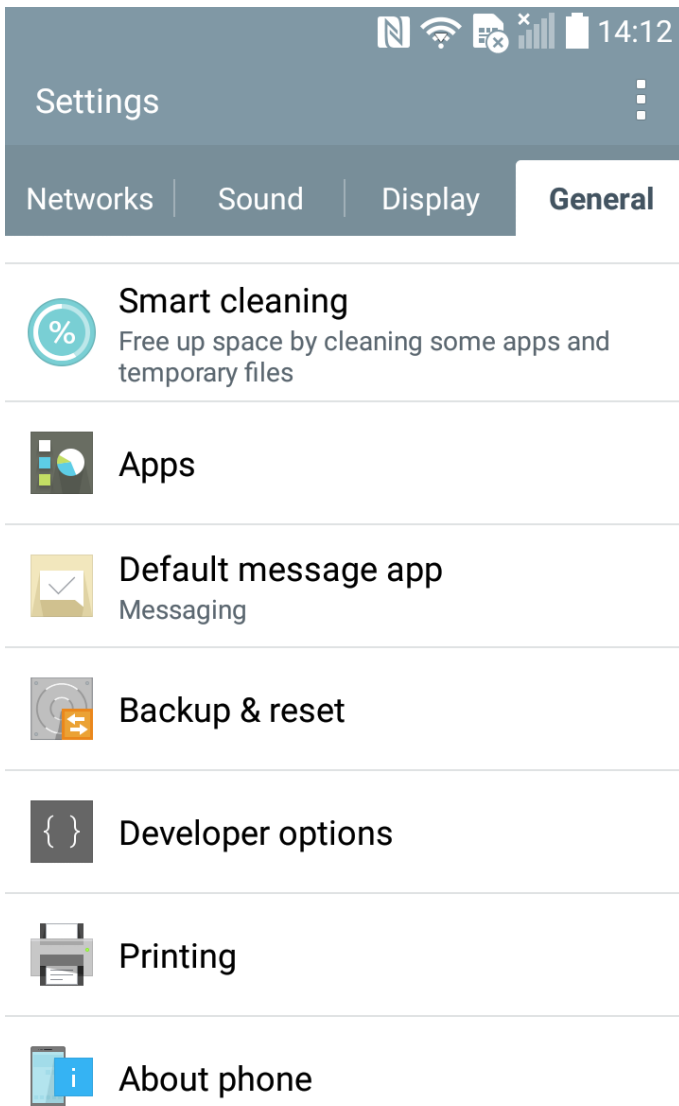
⁶⁷ <http://www.mobiledit.com/downloads.htm>




2. Elija "General" en los Marcadores de Configuración.

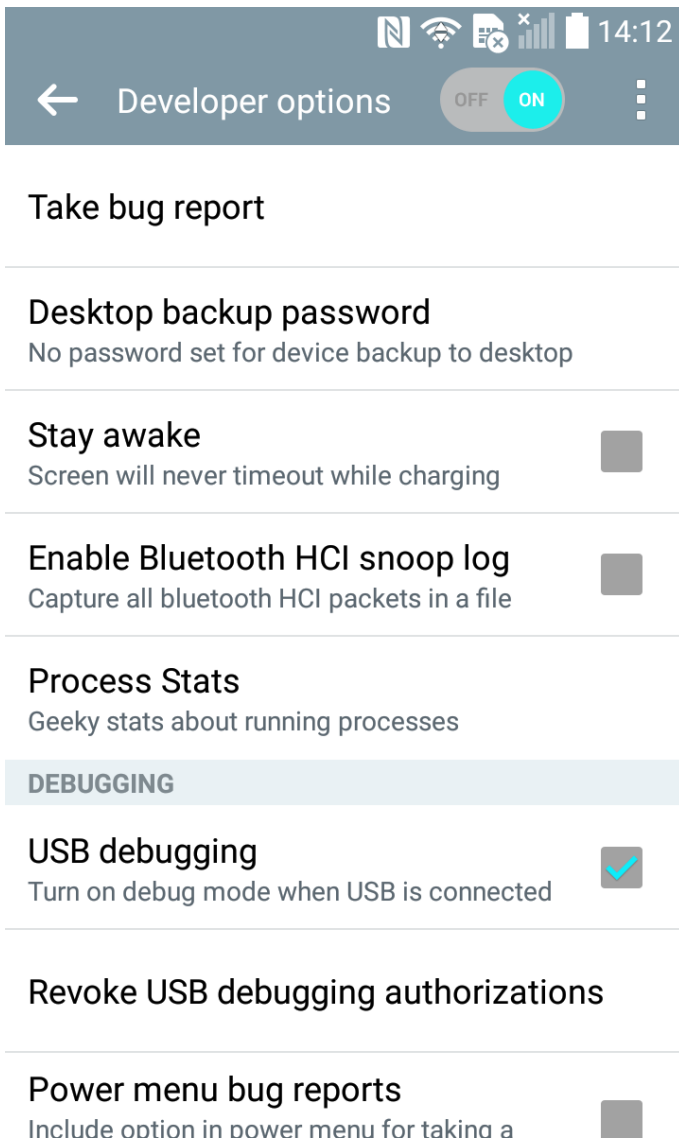


3. Desplácese hacia abajo hasta encontrar las "Opciones del desarrollador".

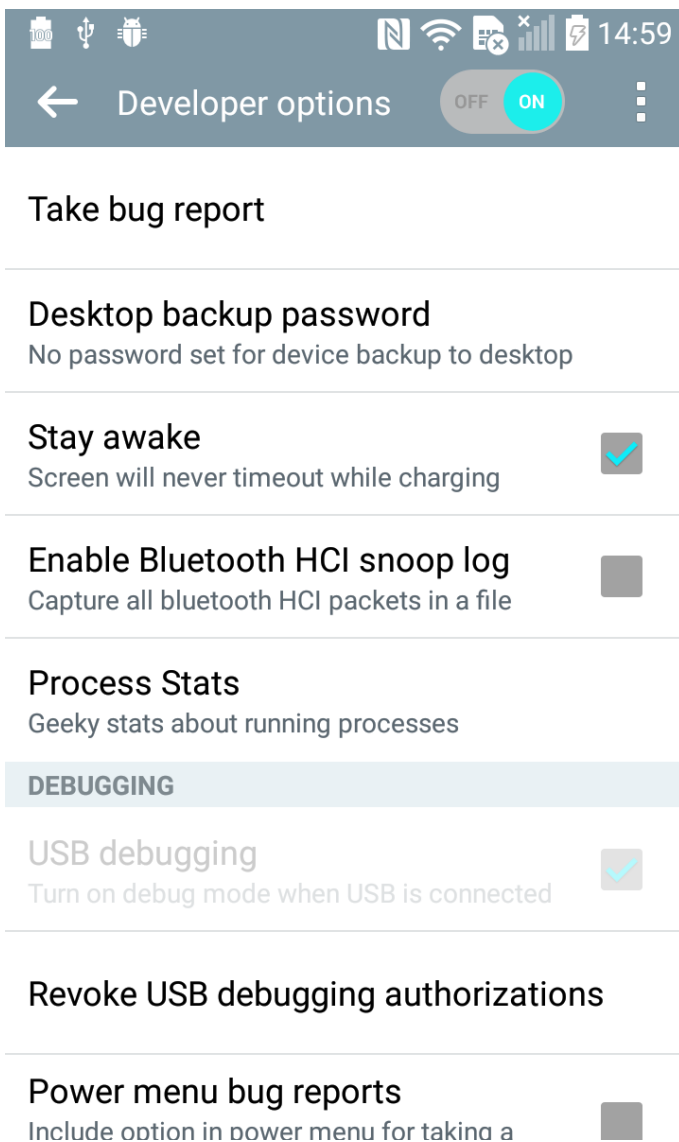


 Haga clic aquí para obtener una guía sobre cómo habilitar las Opciones del desarrollador en su teléfono.

4. Abra las Opciones del desarrollador y localice la opción "Permanecer activo".



5. Haga clic en la caja junto a Permanecer activo para evitar que la pantalla se apague.



3.11.4 Conexión en modo MTP

Algunos teléfonos tienden a conectarse automáticamente en modo "solo carga". Con el fin de asegurar la velocidad de comunicación y de transferencia más rápidas, cambie el modo de conexión a MTP (Media Device).

Puede seguir estos pasos para configurarlo.

1. Desplácese hacia abajo y localice la notificación sobre las "opciones de USB". Selecciónela.



2. Aparecerá una página de ajustes pidiéndole que seleccione el modo de conexión deseado. Seleccione MTP (Media Transfer Protocol).

MTP le permite navegar por archivos y carpetas almacenados en su dispositivo. Sin embargo, algunos teléfonos necesitan estar desbloqueados para habilitar el MTP



3. Espere a que su teléfono se vuelva a conectar automáticamente. A continuación, sus notificaciones deberían aparecer así.



Algunos modelos de teléfonos (p. ej. Huawei) presentan esta opción de manera diferente en la interfaz de usuario. Desplácese hacia abajo para encontrar la siguiente notificación. Simplemente seleccione "Archivos" y habrá terminado.

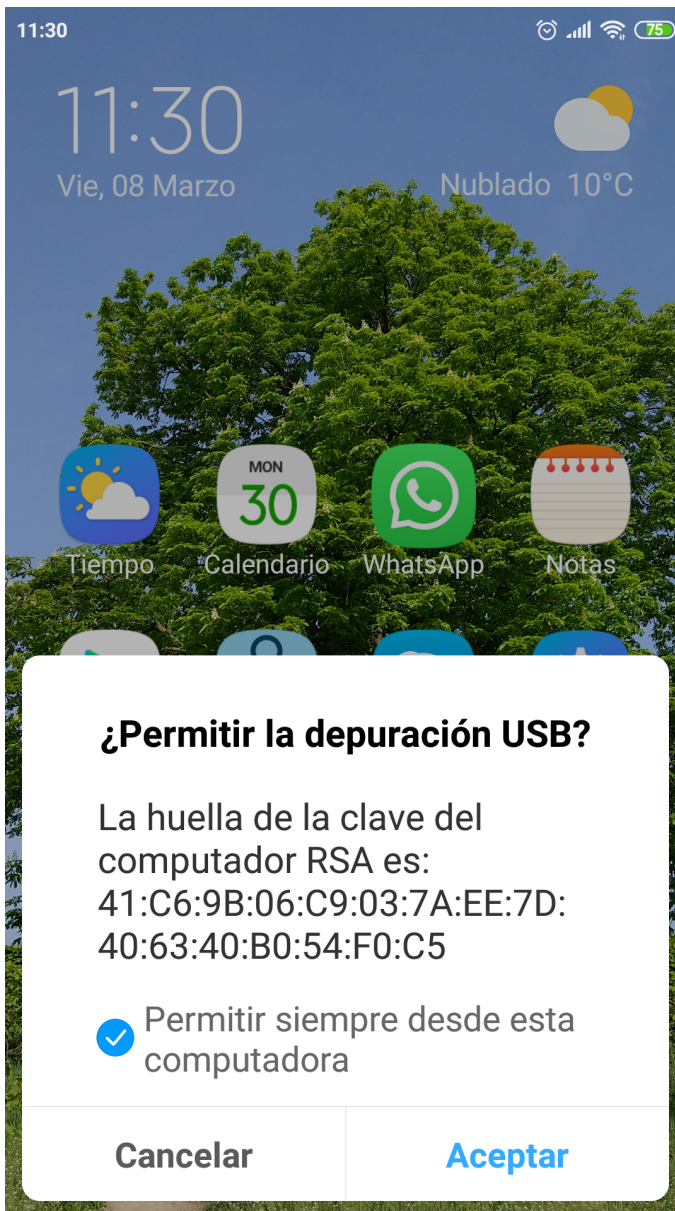


3.11.4.1 Para Android 6.0 o superior:

Al conectarse, el teléfono le pedirá permiso para que la conexión por PC acceda a sus datos y archivos. Simplemente haga clic en el botón "Permitir" y habrá terminado.

3.11.5 Android - Confirmar la huella digital RSA

Este mensaje le indica que necesita confirmar la huella digital RSA en la pantalla del teléfono. Debería aparecer una ventana emergente en la pantalla de su dispositivo. Si no aparece un cuadro de diálogo, vuelva a conectar el teléfono para que vuelva a aparecer.




Nota para usuarios multicuenta: Si utiliza un teléfono multicuenta, asegúrese de estar utilizando la cuenta principal. De lo contrario, no podrá utilizar nuestro software correctamente y tendrá dificultades al conectar su dispositivo.

3.11.6 Cómo instalar el controlador universal de Android

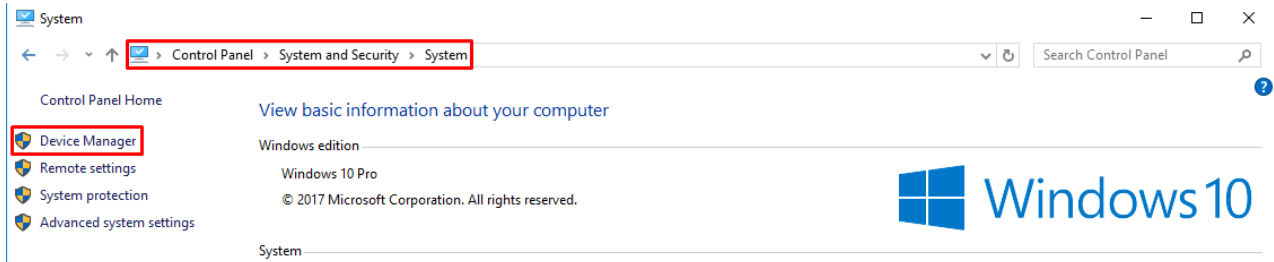
En algunos casos, los controladores proporcionados por el fabricante del teléfono no permiten una conexión de dispositivos adecuada, requisito necesario para que nuestros productos puedan comunicarse correctamente con el dispositivo.

Por tanto, es necesario reemplazar este controlador por el controlador universal de Android.

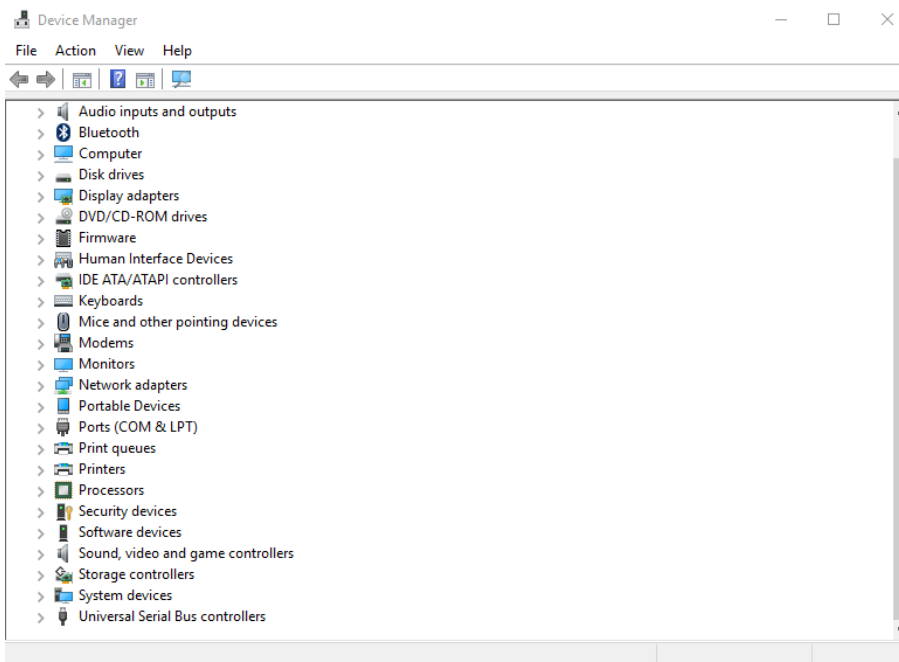
A continuación encontrará una guía sobre cómo proceder con la instalación y la sustitución de este controlador.

 Si necesita instalar un controlador no firmado, haga clic aquí para saber cómo hacerlo..

1. Descargue e instale el controlador universal de Android desde nuestra web haciendo clic [aquí](#)⁶⁸.
2. Cuando esté instalado el controlador, conecte su dispositivo.
3. Abra el diálogo Propiedades del sistema y presione Windows+Pausa/Inter en el teclado (o inicie el Panel de control y acceda a "Sistema y seguridad" y después a "Sistema").

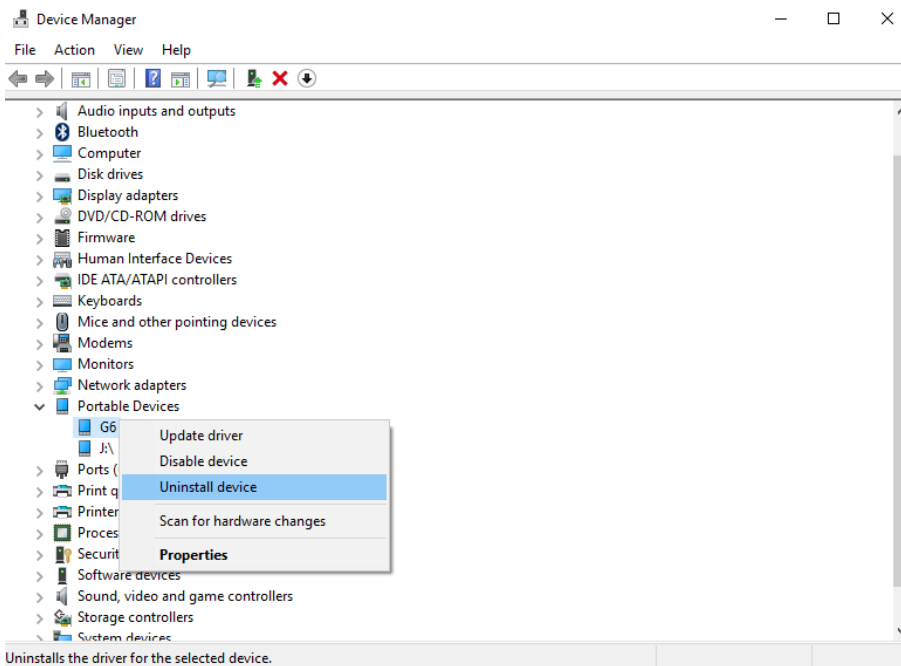


4. Haga clic en el vínculo "Administrador de dispositivos".



5. En el Administrador de dispositivos, localice su dispositivo Android, haga clic derecho y seleccione "Desinstalar".

⁶⁸ <http://www.mobiledit.com/download-list/universal-android-driver>



6. Después de completar ese paso, cierre el Administrador de dispositivos y vuelva a conectar el teléfono.

7. Al conectarlo de nuevo, nuestro controlador universal localizará y "atrapará" automáticamente el teléfono antes de que Windows instale un controlador incorrecto.

Si esto no funciona o necesita más ayuda, ¡póngase en contacto con nosotros aquí!

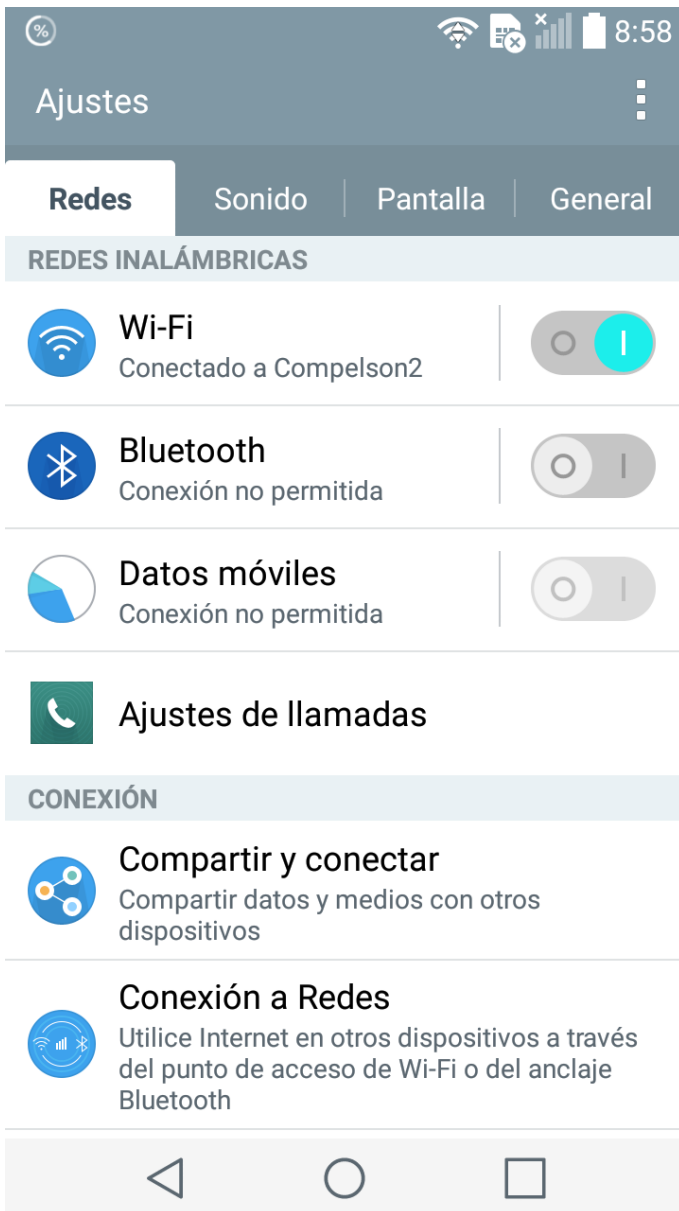
3.11.7 Cómo habilitar la depuración USB

La depuración por USB se encuentra en las "Opciones del desarrollador", pero está oculto. Primero tendrá que hacerlo visible:

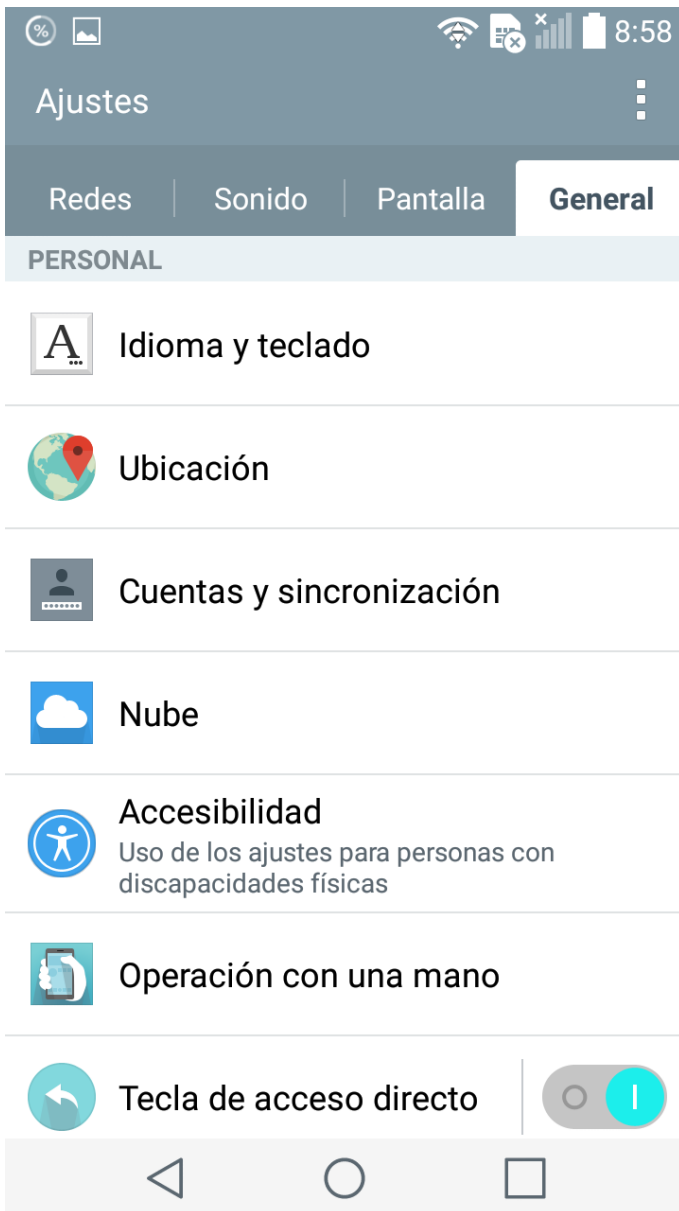
1. Acceda a Configuración -> Acerca del teléfono
2. Acceda a "Número de compilación" al final de la lista desplegable.
3. Presione 7 veces el "Número de compilación" ("Versión Android" en algunos dispositivos). Al presionar por tercera vez, aparecerá un mensaje indicando que tras presionar 4 veces más accederá al "modo desarrollador".
4. Vuelva a la página de Configuración. Ahora debería aparecer una Opción para desarrolladores en la lista de configuración.
5. Seleccione las Opciones del desarrollador y active la Depuración por USB -> ON

3.11.7.1 Ver todas las instrucciones con imágenes

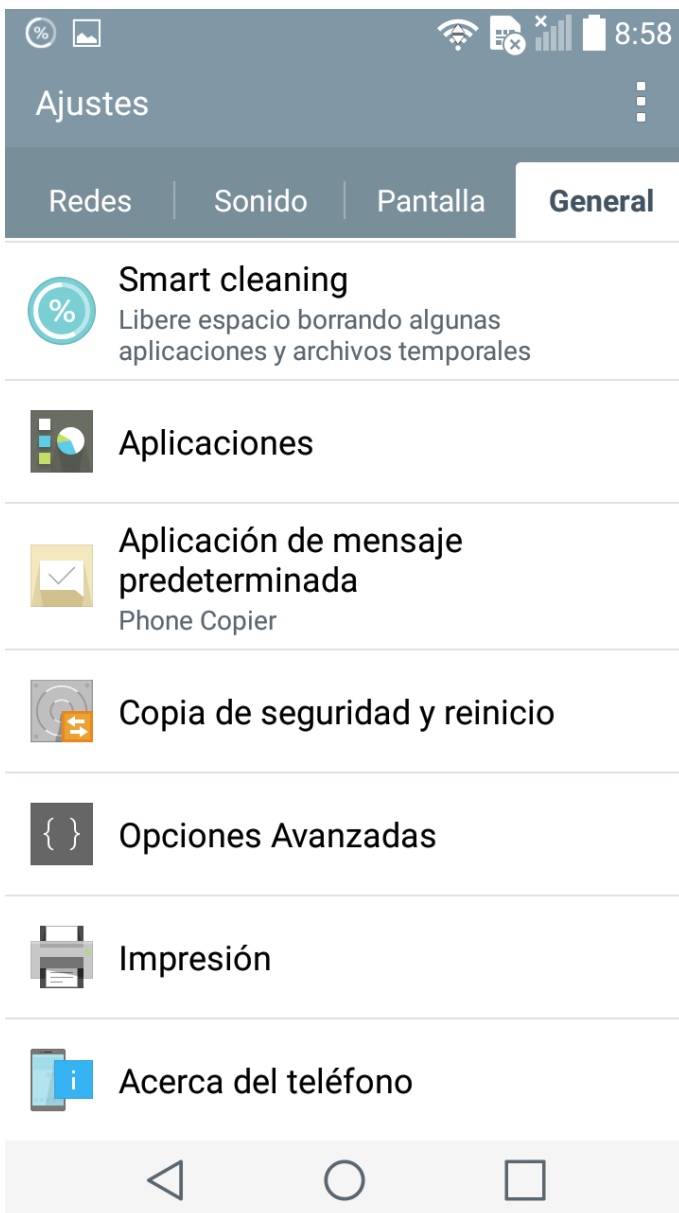
1. Acceda a la Configuración de su teléfono.



2. Elija "General" en los Marcadores de Configuración.



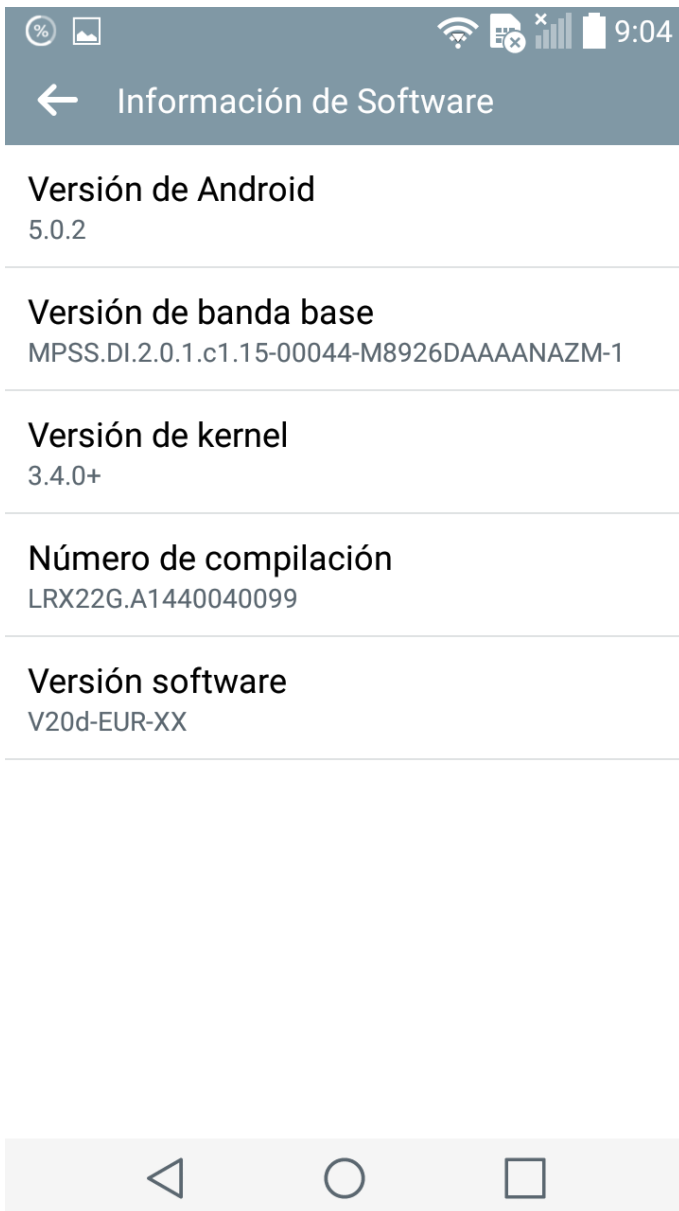
3. Acceda a la sección Acerca del teléfono.



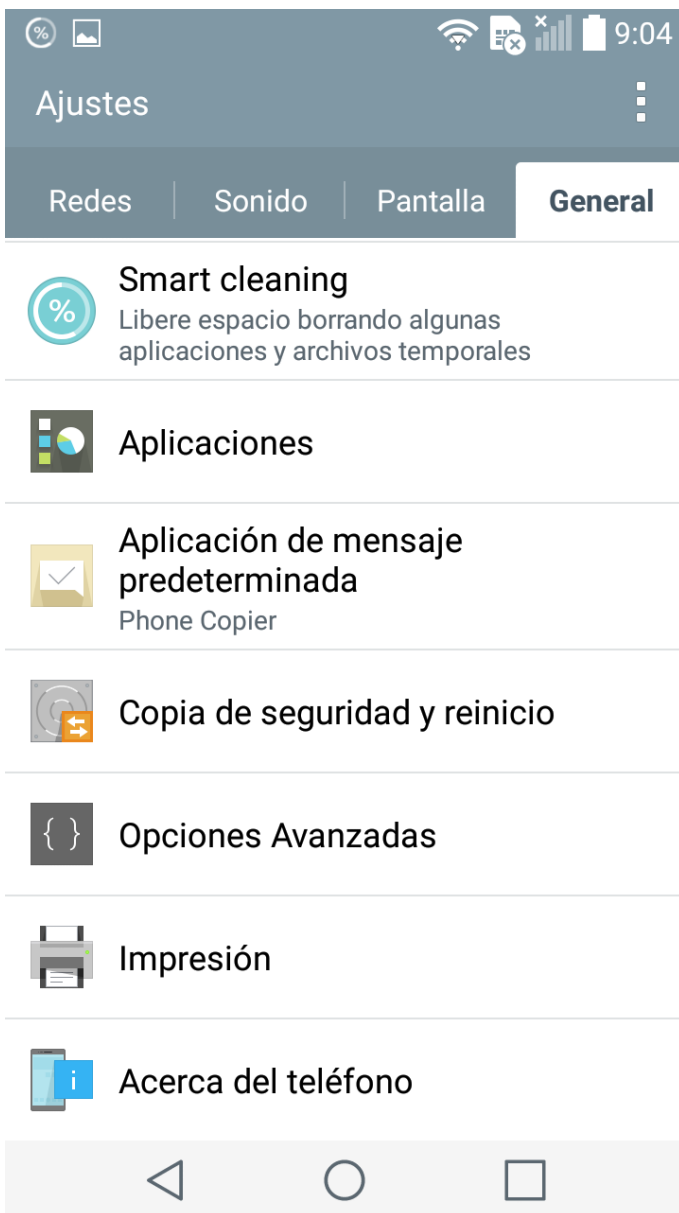
4. Acceda a la información del software



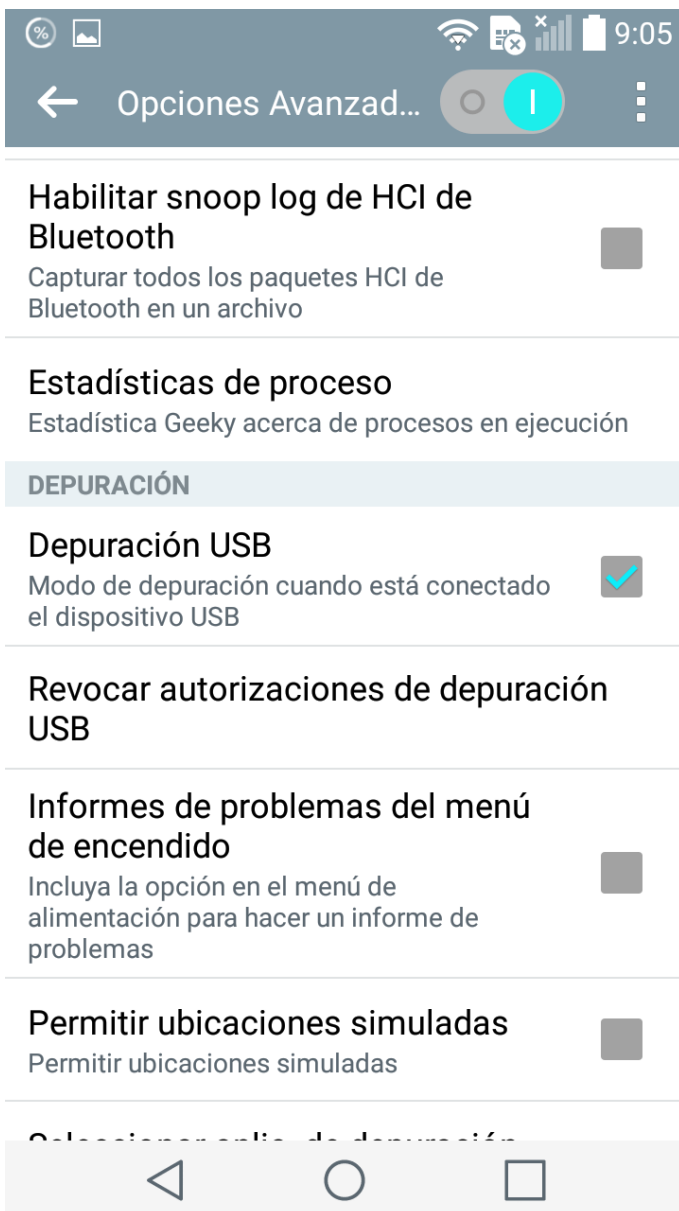
5. Presione 7 veces el "Número de compilación", para que aparezca el siguiente mensaje



6. Vuelva atrás y desplácese hacia abajo hasta encontrar las "Opciones del desarrollador".

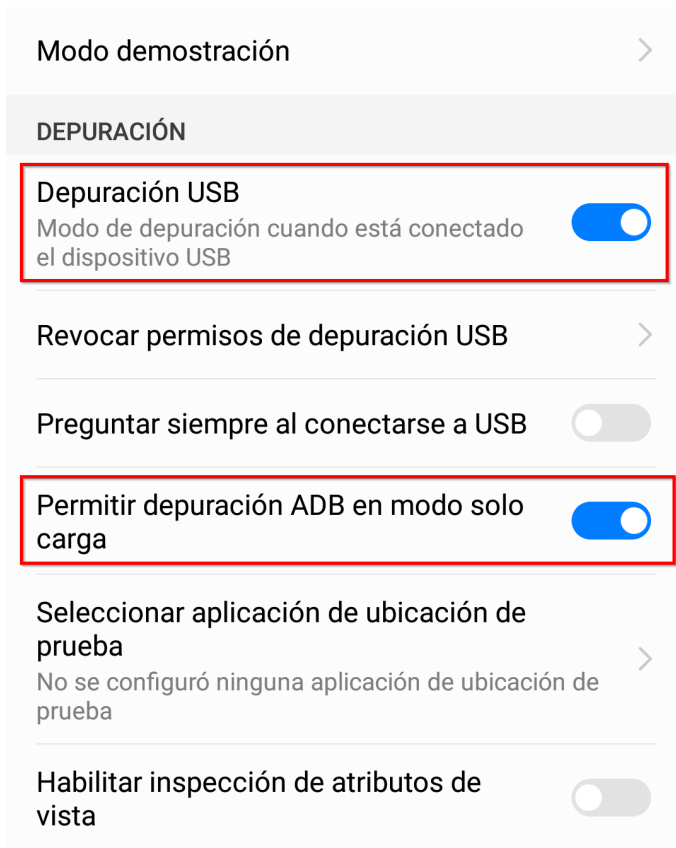



7. Haga clic en la opción "Depuración por USB" y confirme el mensaje que aparece en la pantalla



3.11.7.2 Dispositivos Huawei

Si está activando la depuración por USB en un dispositivo Huawei, asegúrese también de "permitir depuración ADB en modo solo carga" en la sección de Depuración en las Opciones del desarrollador. Esto evitará la mayoría de los casos, cuando la depuración por USB se apague automáticamente a causa del EMUI.



 Para EMUI 5.0 o superior, quizá sea necesario conectar el teléfono al PC antes de habilitar la depuración por USB, ya que de lo contrario podría seguir apagándose automáticamente.

3.11.7.3 Dispositivos Xiaomi

Si está activando la depuración por USB en un dispositivo Xiaomi, asegúrese también de habilitar todas las categorías en la sección de Depuración en las Opciones del desarrollador. Esto permitirá que la app Connector se pueda instalar en su teléfono.

< Opciones de desarrollador

DEPURACIÓN

Depuración USB

Modo depuración cuando el USB
esté conectado



Revocar permisos de depuración USB



Instalar vía USB

Permitir la instalación de
aplicaciones vía USB




Depuración USB (Ajustes de seguridad)

Permitir la concesión de permisos y la simulación de entrada a través de la depuración USB



Acceso directo al reporte de errores



 Para habilitar estas dos opciones, necesitará insertar una tarjeta SIM en el teléfono y haber iniciado sesión en Mi Cuenta.

3.12 Android - Português

Para obter uma conexão telefônica bem-sucedida, há uns passos importantes que devem ser seguidos para essa ou qualquer outra ferramenta. Isso só é necessário pela primeira vez. Depois da primeira vez, você pode aproveitar a funcionalidade de todos os nossos produtos. Um telefone Android pode ser conectado a um PC por cabo USB, que transfere dados mais rapidamente ou através de Wi-Fi, o que é mais fácil.

[Faça o download da nossa folha de instruções para impressão aqui \(em inglês\)](#)⁶⁹

⁶⁹ <http://download.mobiledit.com/documents/Connection%20sheet%20A4%20Europe.pdf>

3.12.1 Como conectar o telefone por cabo USB



Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=y_78HkdT_hw&feature=emb_logo

i Não ligue o telefone ao seu PC antes do passo 3!

1. [Ative a verificação do USB](#)(see page 227), para que seu telefone possa ser conectado a um PC
2. [Ative a opção Ficar Acordado](#)⁷⁰, para que o telefone não seja desconectado
3. Instale o driver de dispositivo do Windows para o seu telefone, [baixe aqui](#)⁷¹
4. Agora conecte seu telefone a um PC com MOBILedit ligado
5. [Confirme a impressão digital RSA](#)(see page 219) no ecrã do seu telefone
6. [Selecione o modo MTP](#)(see page 214) no display do celular

Agora aproveite nosso produto! Você não precisa fazer mais nada, o MOBILedit encontrará seu telefone automaticamente.

Caso você tenha conectado seu telefone ao PC antes da etapa 3 acima, Windows podia instalar um driver errado. Isso causaria que a MOBILedit não reconhece o telefone.

[Aqui](#)⁷² está um guia sobre como remover o driver incorreto do Windows pelo nosso Universal Android One.

3.12.1.1 Se o seu telefone não se conecta

- O MOBILedit exigirá a instalação de um pequeno aplicativo chamado Connector no seu telefone. Se ele não for instalado automaticamente, recomendamos reconectar o telefone e reiniciar o MOBILedit ou baixar o aplicativo Connector diretamente do [Google Play](#)⁷³. Caso você tenha um telefone Xiaomi, [permita as configurações necessárias](#)(see page 227) antes da instalação.
- Verificação do USB não se liga? Chave RSA não está aparecendo na tela? Tente desligar e ligar novamente a verificação do USB depois de conectar o telefone.
- Assegure-se de que o telefone não esteja definido no modo de armazenamento em massa.
- Se você usar qualquer outra ferramenta de telefone, como o HTC Manager, Eclipse, Android Studio, você precisa interromper o processo de ADB no Gerenciador de Tarefas ou desinstalar o software, se isso não ajudar.
- Caso você esteja usando o sistema operacional Windows 7 e seu telefone não esteja conectado automaticamente, nem seja reconhecido, siga o artigo [de Alteração manual do driver ADB](#)(see page 225).
- Problemas com a conexão de um telefone Huawei? Vá [aqui](#)(see page 227) para verificar como evitá-los.
- Problemas com a conexão de um telefone Xiaomi? Vá [aqui](#)(see page 227) para verificar como evitá-los.



Todos os telefones Android são suportados, exceto alguns modelos especiais e incompatíveis. A maneira mais fácil de verificar se o seu telefone é suportado é baixar MOBILedit e conectar seu telefone.

⁷⁰ <https://support.mobiledit.com/portal/kb/articles/4-android-ativar-a-op%C3%A7%C3%A3o-fique-acordado>

⁷¹ <http://download.mobiledit.com/documents/Connection%20sheet%20A4%20Europe.pdf>

⁷² <https://support.mobiledit.com/portal/kb/articles/como-instalar-o-driver-do-universal-android>

⁷³ <https://play.google.com/store/apps/details?id=com.compelson.meconnector>

3.12.2 Como conectar o telefone por Wi-Fi

Você também pode conectar seu telefone Android por **Wi-Fi**, é mais fácil, mas o telefone e o PC precisam estar na mesma rede, por favor, leia as [instruções](#) (see page 214).

3.12.3 Conexão Wi-Fi Android

O **aplicativo Android Connector** pode ser baixado do [Google Play](#)⁷⁴ ou da nossa [página](#)⁷⁵ de downloads.

Agora inicie o aplicativo de conexão em seu telefone.

- Verifique se o seu Wi-Fi está ligado e se você está conectado na mesma rede.
- Ligue o MOBILedit e clique no botão Connect.
- Selecione Telefone - Conexão Wi-Fi e insira o endereço IP conforme exibido no telefone.
- Permita a conexão em seu telefone se a chave corresponder à chave no Assistente de conexão.

Sendo encontrado seu telefone, clique no botão Concluir e o dispositivo se conectará automaticamente.

Ótimo, você acabou de conectar seu telefone usando sua rede Wi-Fi.

3.12.4 Conectando no modo MTP

Alguns telefones tendem a se conectar automaticamente no modo "**somente carga**". Para garantir a velocidade de comunicação e velocidade de transferência mais rápidas possíveis, altere o modo de conexão para **MTP (Dispositivo de Mídia)**.

Você pode seguir estes passos para fazer isso.

1. Deslize para baixo no telefone e encontre a notificação sobre "**opções de USB**". Toque nele.

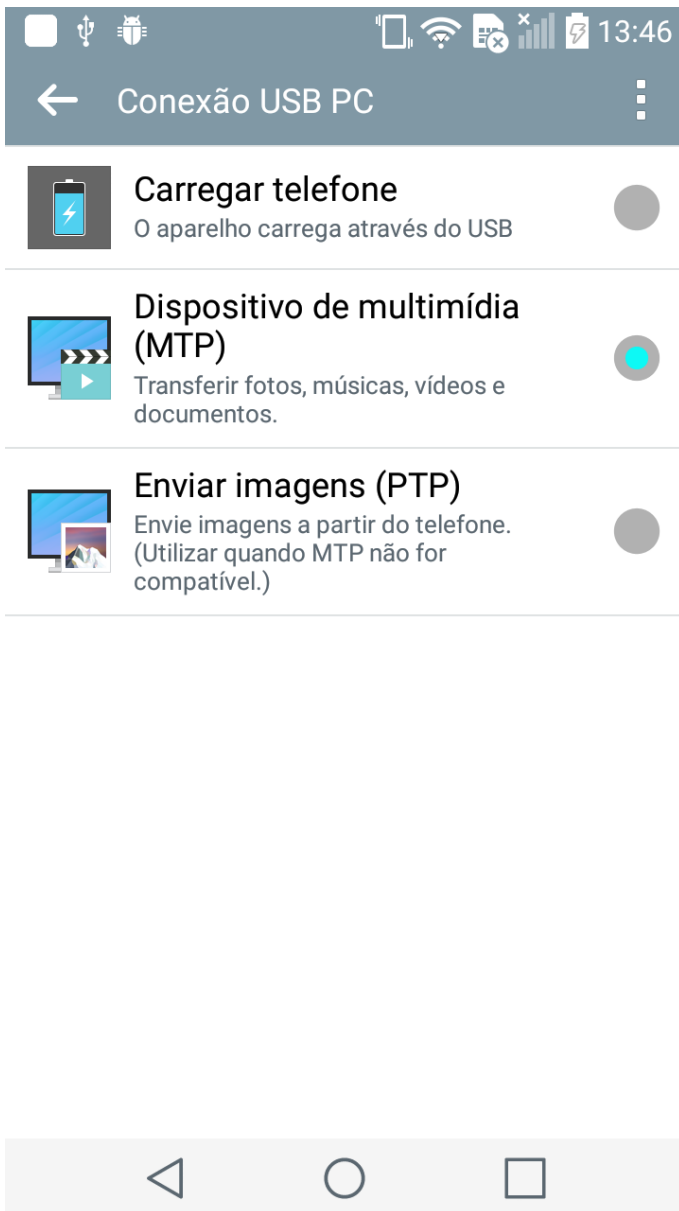
⁷⁴ <https://play.google.com/store/apps/details?id=com.compelson.migrator>

⁷⁵ <https://www.mobiledit.com/downloads>

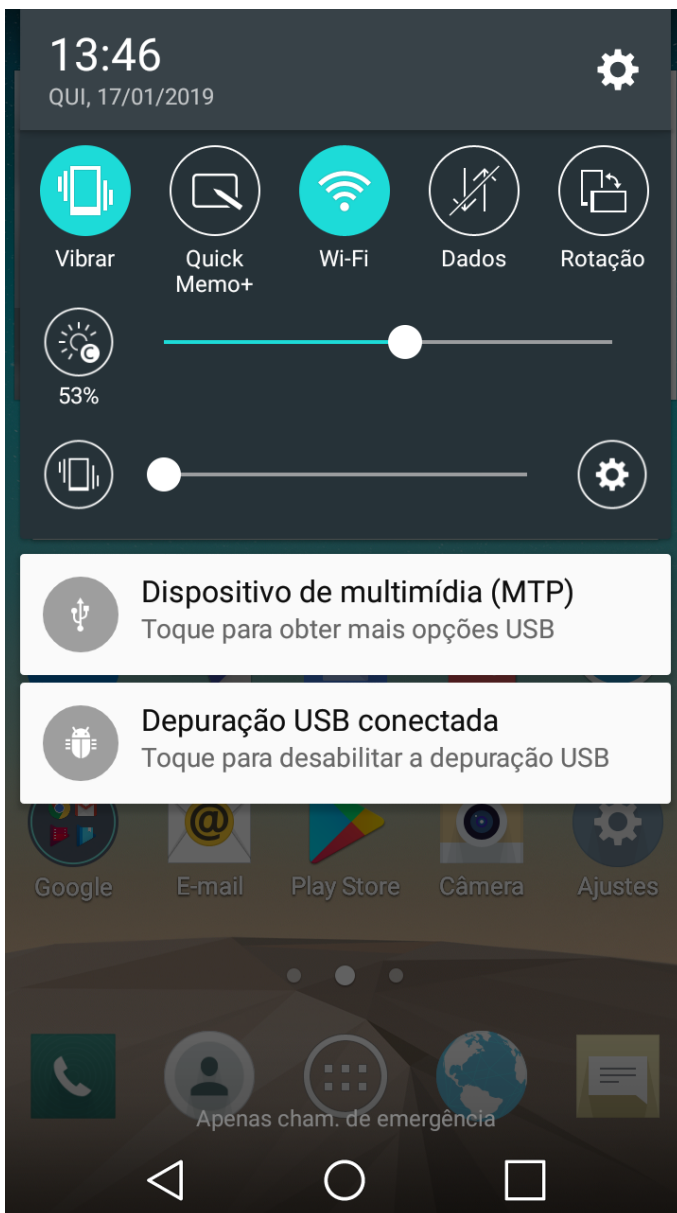


2. Uma página de configurações aparecerá pedindo selecionar o modo de conexão desejado. Por favor seleccione **MTP (Media Transfer Protocol)**.

O MTP basicamente permite que você navegue por arquivos e pastas armazenados no seu dispositivo, no entanto, alguns telefones podem precisar ser desbloqueados para ativar o MTP



3. Aguarde até que seu telefone reconecte automaticamente. Suas notificações devem ficar assim.

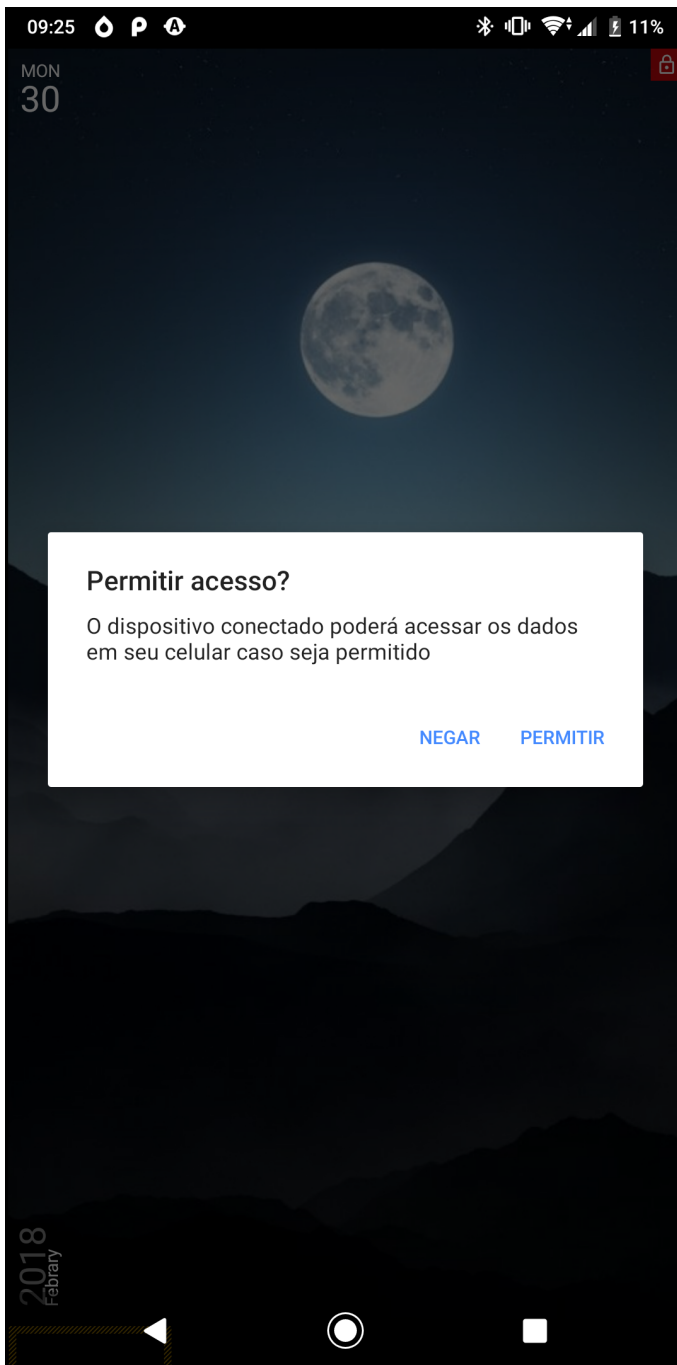


Alguns modelos de telefone (por exemplo Huawei) têm essa opção feita de maneira um pouco diferente na interface do usuário. Depois de deslizar para baixo, você encontrará a seguinte notificação, basta selecionar "**Arquivos**" e pronto.



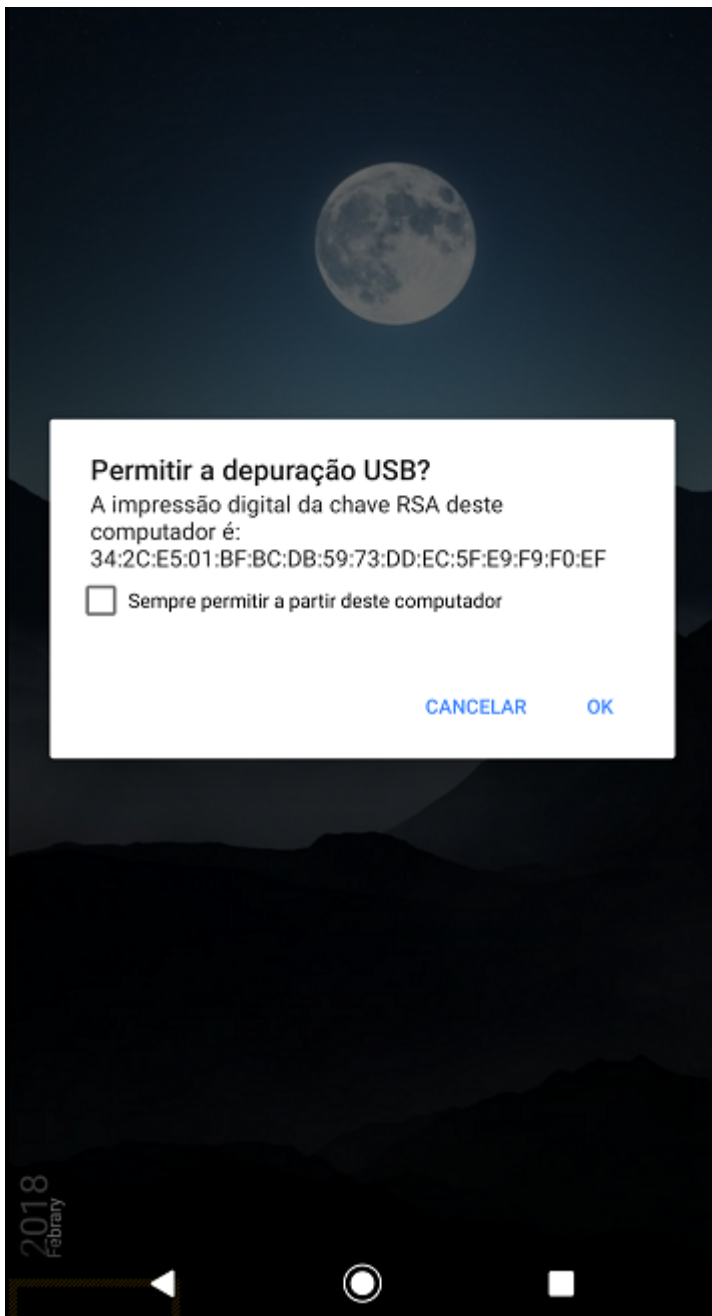
3.12.4.1 Para usuários do Android 6.0 e superior:

Ao conectar-se, seu telefone solicitará permissão para a conexão com o PC para acessar dados e arquivos. Basta clicar no botão **"Permitir"** e está tudo pronto.



3.12.5 Android - Confirme a impressão digital da RSA

Esta mensagem informa que você precisa confirmar a impressão digital RSA na tela do telefone. Deve haver uma janela pop-up na tela do seu dispositivo. Se não houver diálogo, reconecte o telefone para que a caixa de diálogo seja exibida novamente.



Observação para usuários com várias contas: se você estiver usando um telefone com várias contas, verifique se está usando a conta principal. Caso contrário, você não poderá usar nosso software adequadamente e terá dificuldades ao conectar seu dispositivo.

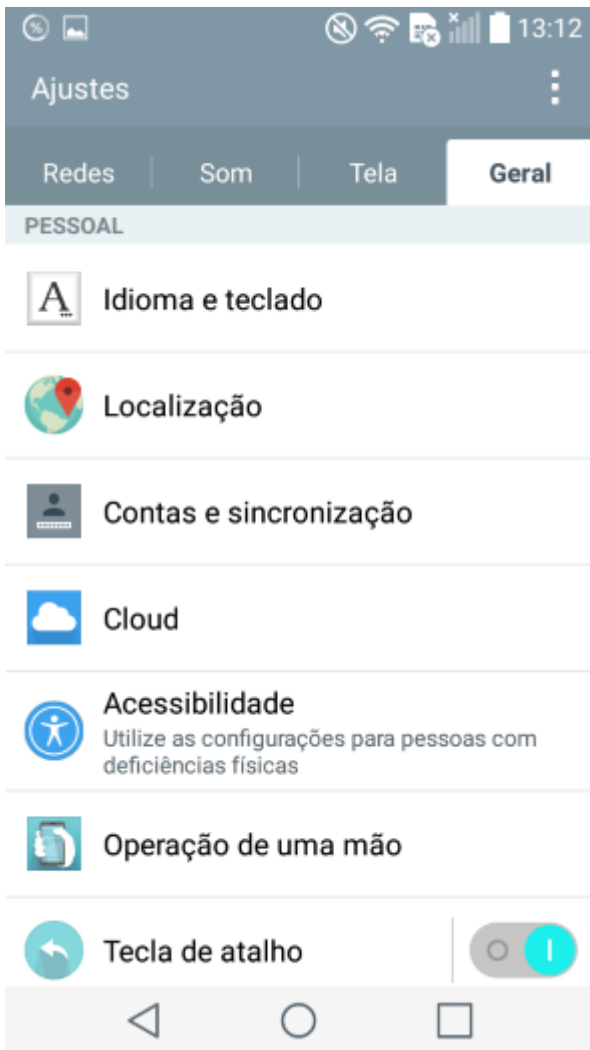
3.12.6 Android - Ativar a opção "Fique acordado"

A opção Fique Acordado deve estar definida no seu telefone para permitir a comunicação contínua entre o telefone e o software. Se o telefone não estiver definido como Permanecer Acordado e estiver, por exemplo, definido no modo de Economia de Energia, o telefone poderá se desconectar de outras fontes, incluindo nosso software, e interromper o processo de extração e análise.

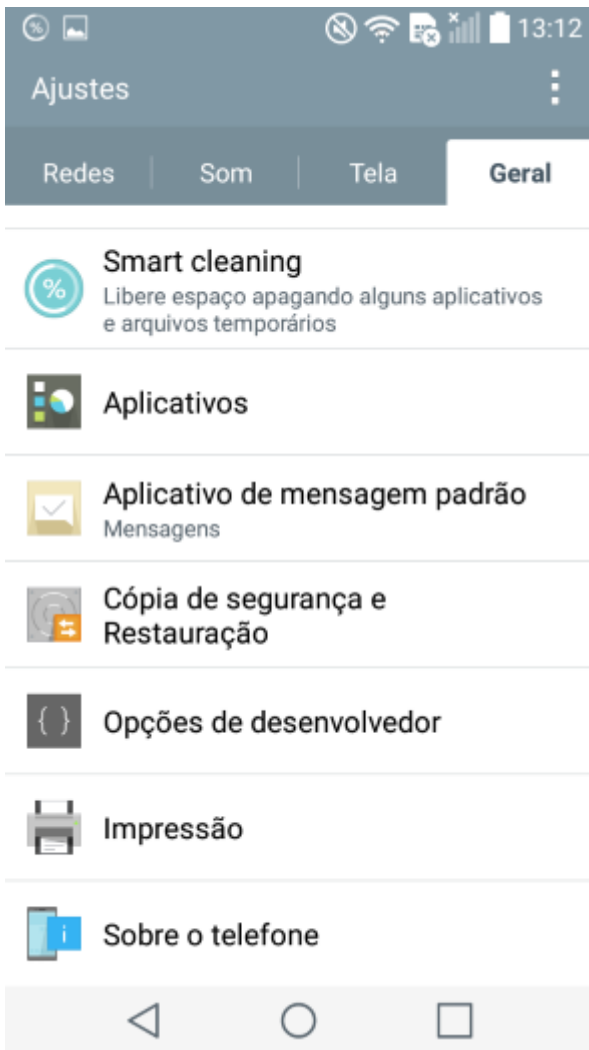
1. Vá para Configurações no seu telefone.



2. Escolha "Geral" nos favoritos das Configurações.



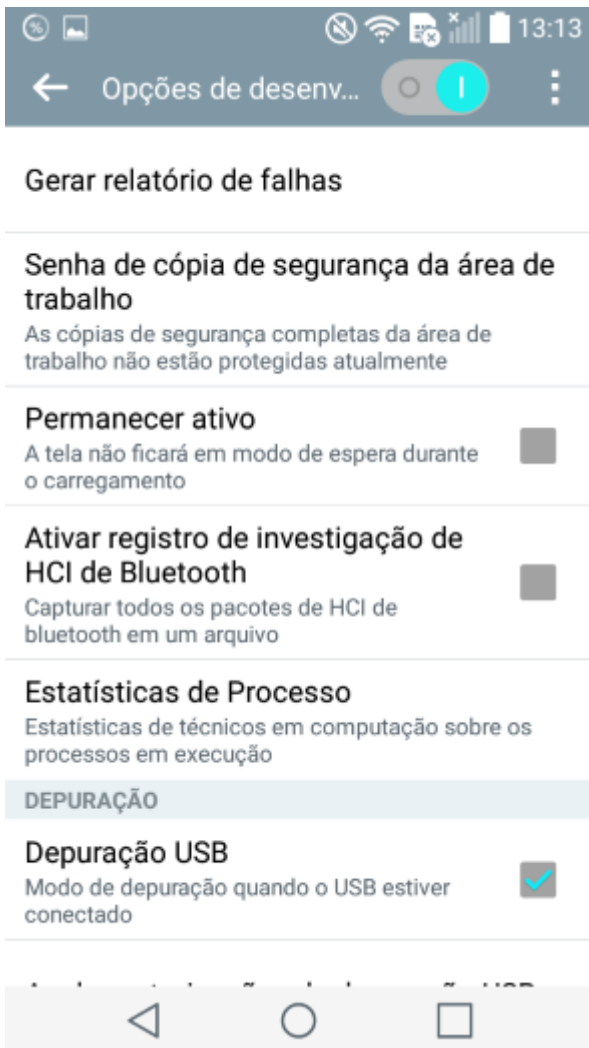
3. Role para baixo para encontrar as "Opções do Desenvolvedor".



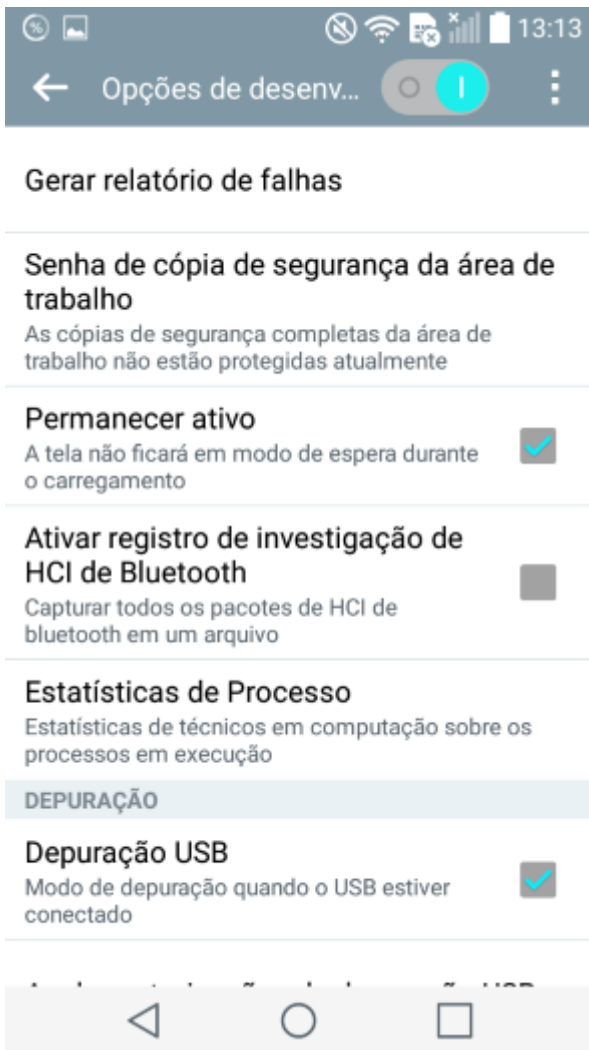
Clique [aqui](#)⁷⁶ para orientar como ativar as Opções do Desenvolvedor no seu telefone.

4. Abra as Opções do Desenvolvedor e encontre a linha de opção "Fique Acordado".

⁷⁶https://support.mobiledit.com/portal/kb/articles/como-viabilizar-a-verifica%C3%A7%C3%A3o-do-usb#Veja_todas_as_instrues_com_imagens



5. Clique no botão ao lado de Ficar Acordado para ativar a prevenção da tela escurecendo.



3.12.7 Como instalar o driver do Universal Android

Em alguns casos, os drivers fornecidos pelo fabricante do telefone não permitem uma conexão adequada do dispositivo, o que é necessário para que nossos produtos se comuniquem com o dispositivo com êxito. Portanto, é necessário substituir esse driver pelo driver Universal Android.

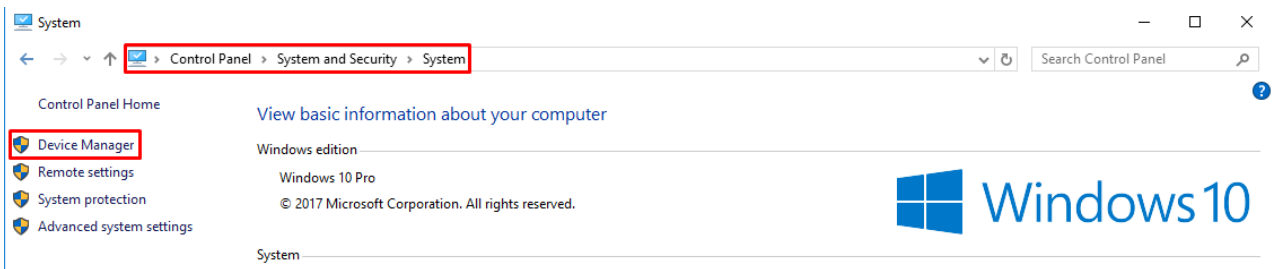
Abaixo você encontrará um guia sobre como proceder com a instalação e substituição deste driver.

i Se você precisar instalar um driver não assinado, por favor, verifique como o fazer [aqui](#)⁷⁷.

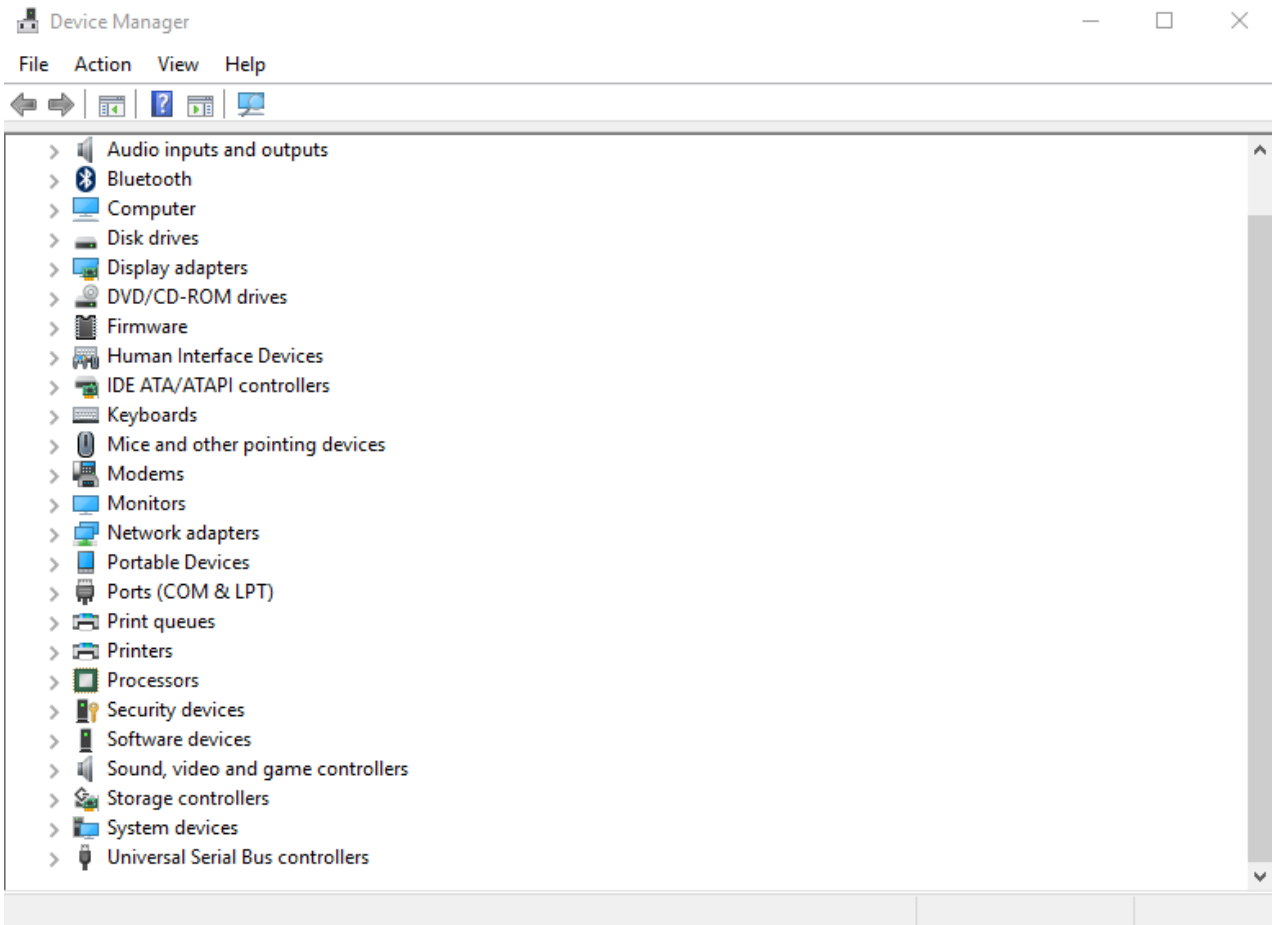
1. Baixe e instale o driver Universal Android do nosso site [aqui](#)⁷⁸.
2. Quando o driver estiver instalado, conecte seu dispositivo.
3. Abra o diálogo Propriedades do Sistema - pressione **Win + Break** no teclado. (ou inicie o Painel de Controle e vá para "Sistema e Segurança" e depois para "Sistema")

⁷⁷<https://www.howtogeek.com/167723/how-to-disable-driver-signature-verification-on-64-bit-windows-8.1-so-that-you-can-install-unsigned-drivers/>

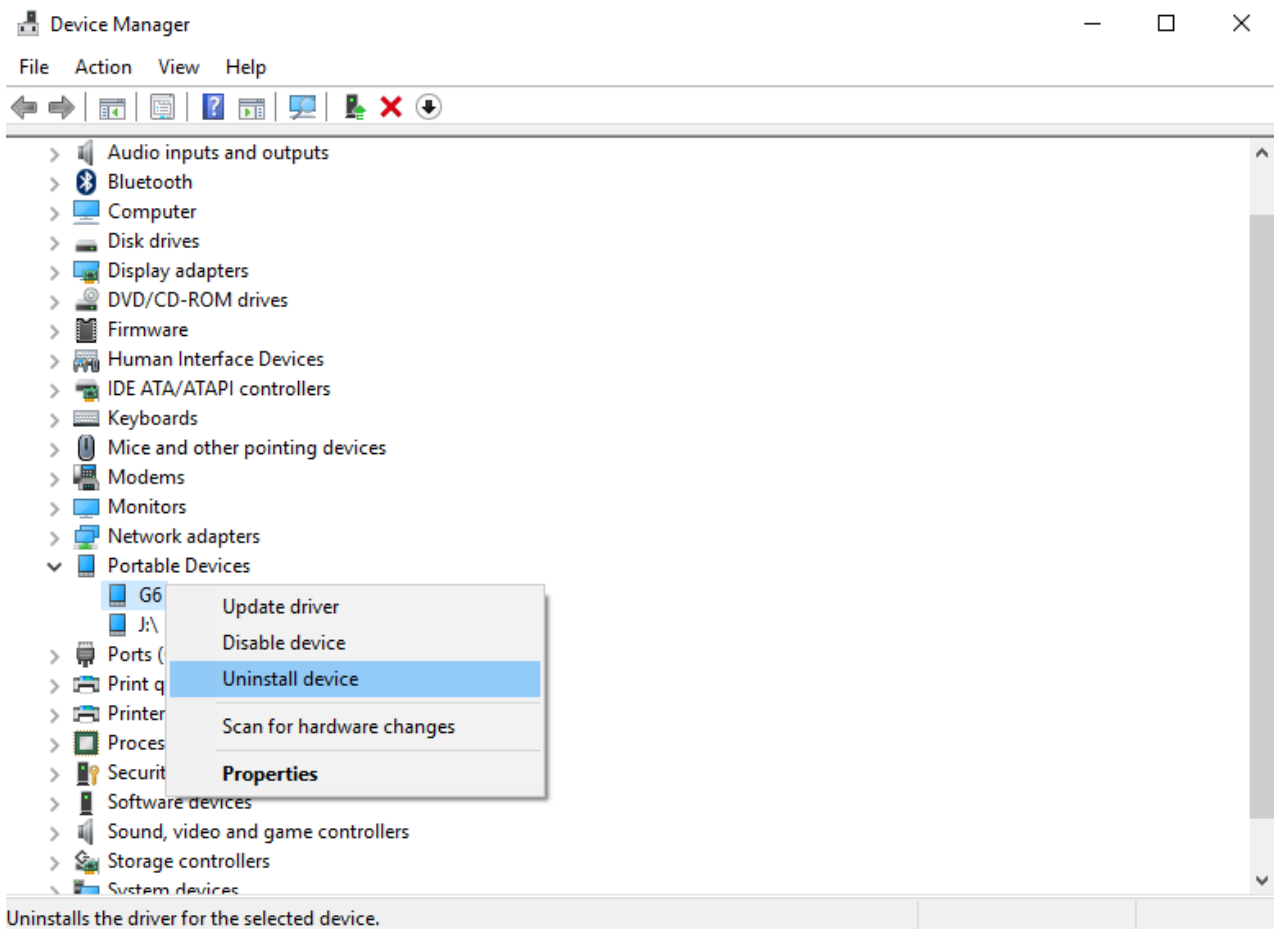
⁷⁸<http://www.mobiledit.com/download-list/universal-android-driver>



4. Clique no link "Gerenciador de Dispositivos".



5. No Gerenciador de Dispositivos, localize seu dispositivo Android, clique com o botão direito nele e selecione "Desinstalar".



6. Depois disso, feche o Gerenciador de Dispositivos e reconecte o telefone.

7. Ao conectá-lo novamente, nosso driver Universal localizará automaticamente e "capturará" o telefone, antes que um driver incorreto seja instalado pelo Windows.

Se isso não funcionou para você ou você está precisando de mais assistência, entre em contato conosco [aqui!](http://www.mobiledit.com/contact)⁷⁹

3.12.8 Como viabilizar a verificação do USB

A verificação do USB está no menu "Opções do desenvolvedor", mas está oculta, você precisa revelá-la primeiro:

Vá para Configurações -> Sobre o telefone.

1. Vá para "Build Number" no final da lista de rolagem.
2. Toque em "Número de montagem" ("Versão Android" para alguns dispositivos) repetidamente 7 vezes. No seu terceiro toque, você verá uma mensagem indicando que você só tem mais quatro toques para "tornar-se um desenvolvedor".
3. Volte para a página de configuração. Você deverá ver o item de menu Opção de Desenvolvedor na sua lista de configurações agora.
4. Abra as opções do desenvolvedor e verifique a verificação do USB -> ON

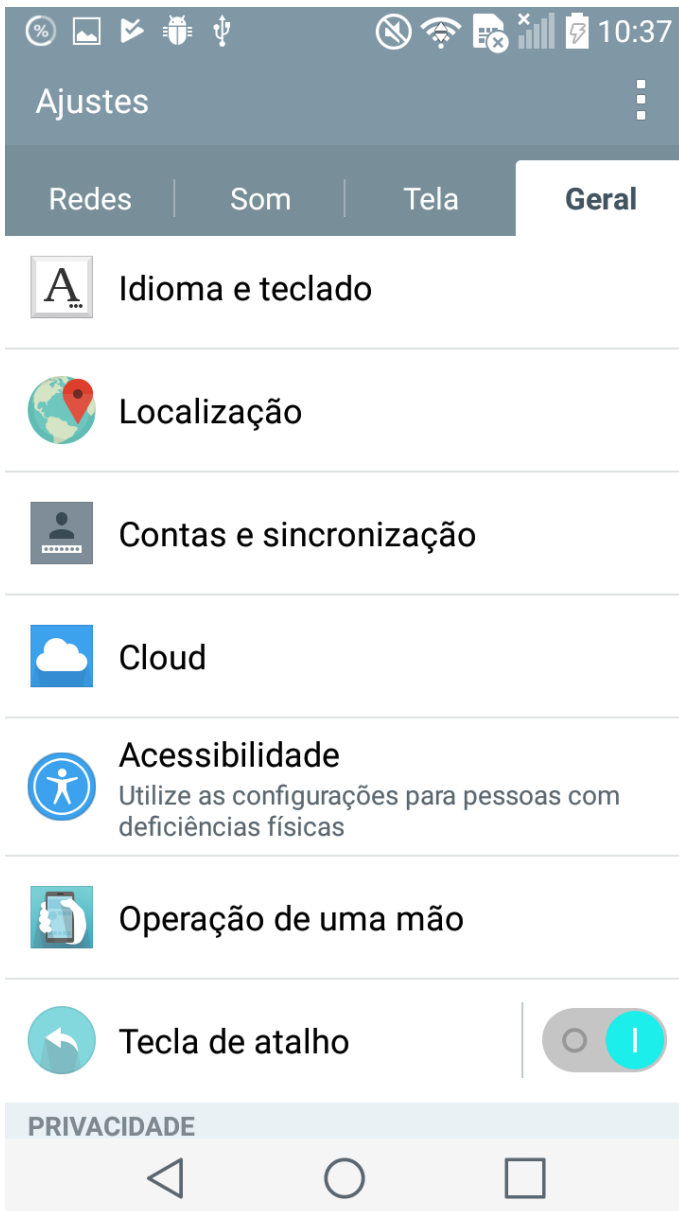
⁷⁹ <http://www.mobiledit.com/contact>

3.12.8.1 Veja todas as instruções com imagens

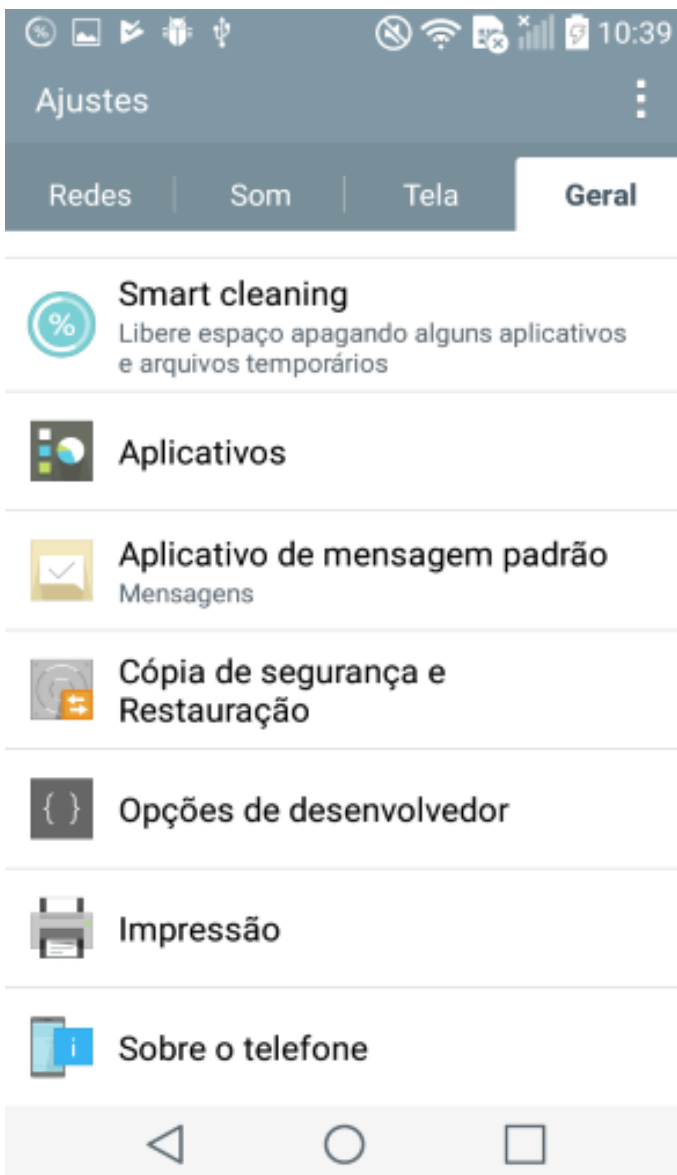
1. Vá para Ajustes no seu telefone.



2. Escolha "Geral" nos favoritos das Configurações.



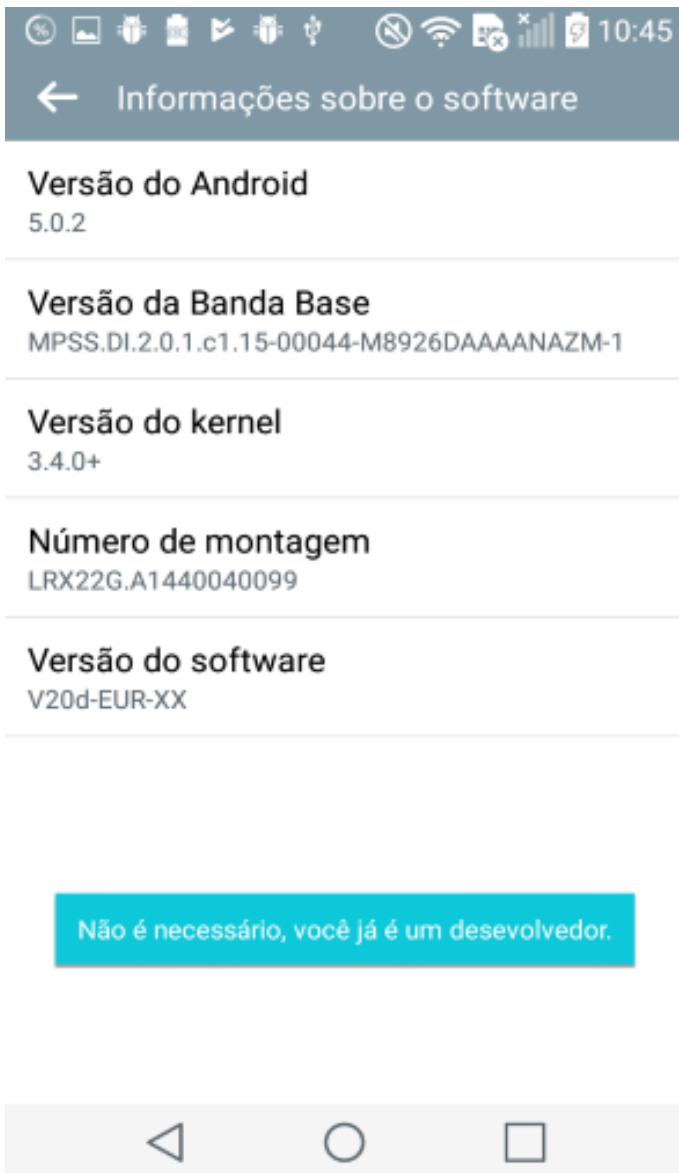
3. Vá para a seção Sobre o telefone.



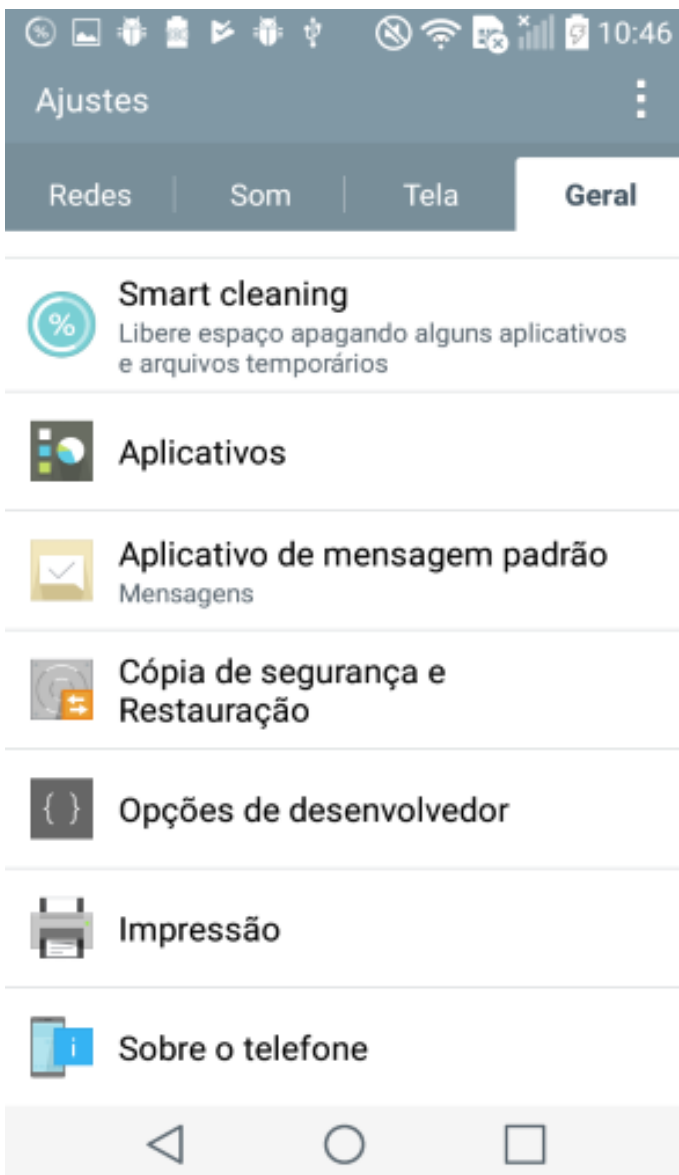
4. Vá para informações sobre o software



5. Toque 7 vezes em "Número de montagem" e você verá a seguinte mensa



6. Volte e role para baixo para encontrar as "Opções do desenvolvedor".



7. Clique na opção "Depuração do USB" e confirme a mensagem que aparece na tela



3.12.8.2 Dispositivos Huawei

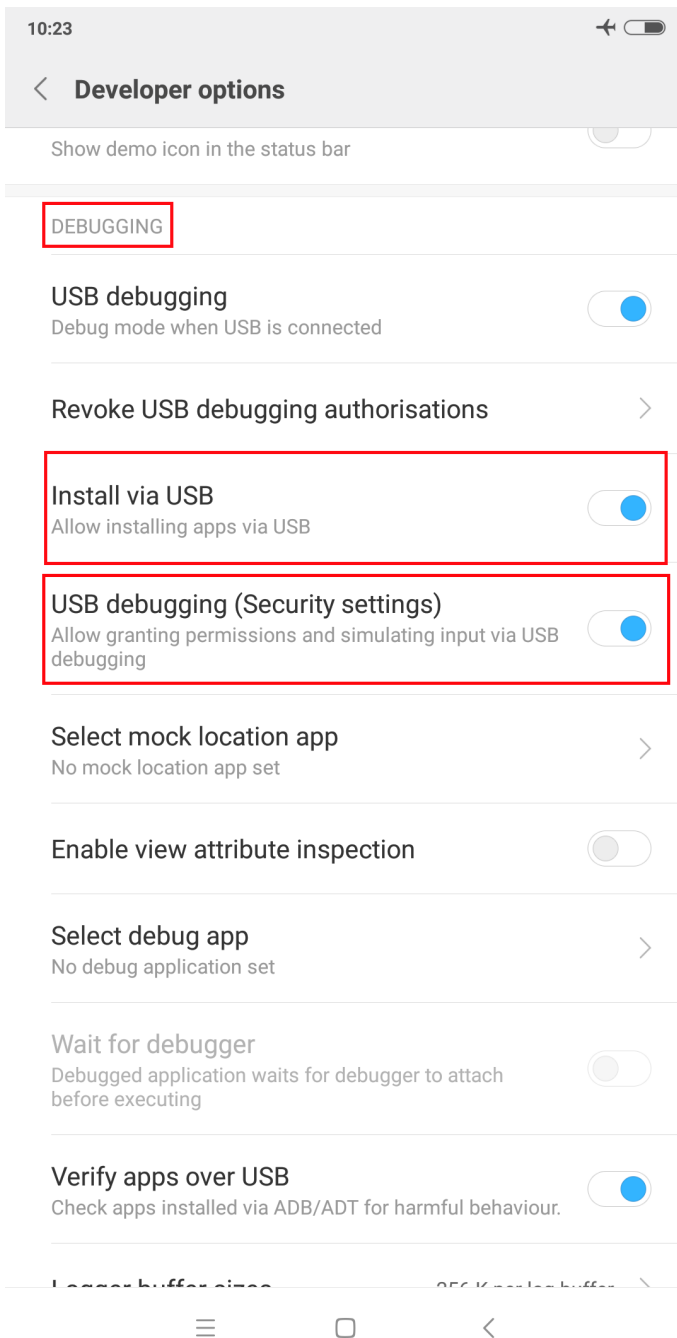
Caso você esteja ativando a verificação do USB em um dispositivo Huawei, assegure-se de também "permitir o uso de verificação apenas no modo de carregamento" na seção Verificação nas Opções do desenvolvedor. Isso evitará a maioria dos casos em que a verificação do USB está sendo desativada por causa d l.



i Para EMUI 5.0 e superior, pode ser necessário conectar o telefone ao PC antes de ativar a verificação do USB, porque se pode desligar automaticamente.

3.12.8.3 Dispositivos Xiaomi

Caso você esteja ativando a verificação do USB em um dispositivo Xiaomi, assegure-se de ativar todas as categorias na seção Depuração nas Opções do desenvolvedor. Isso garantirá que o aplicativo de conector possa ser instalado em seu telefone.



i Enabling both these options will require you to have a SIM card inserted in the phone and also to be logged into Mi Account.

4 Sources of data

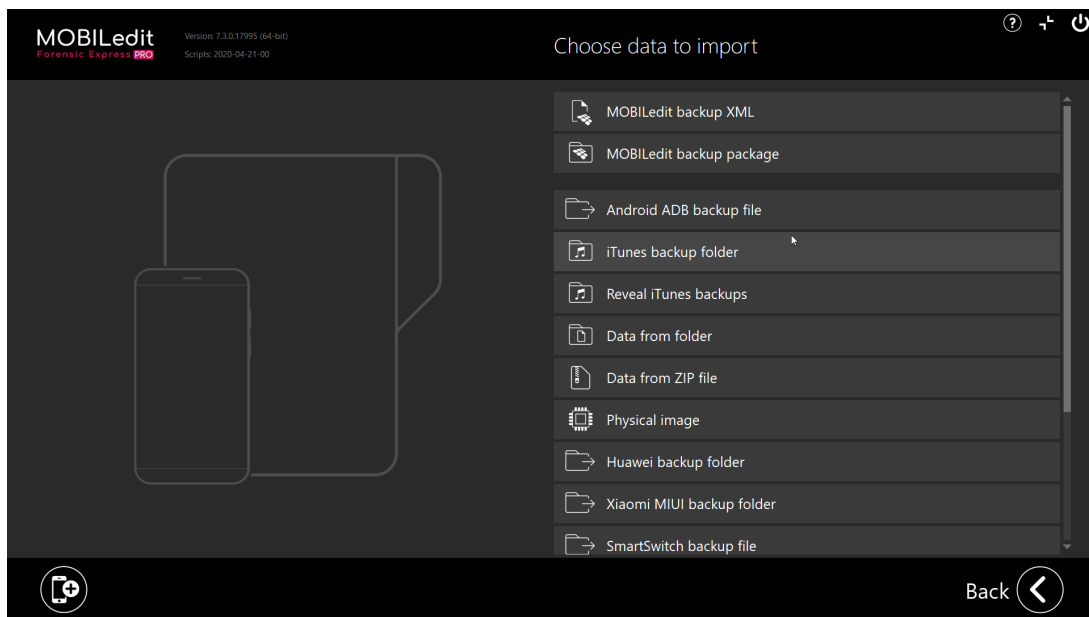
In this chapter, you can find information and step by step guides for various methods used for accessing crucial sources of data to extract.

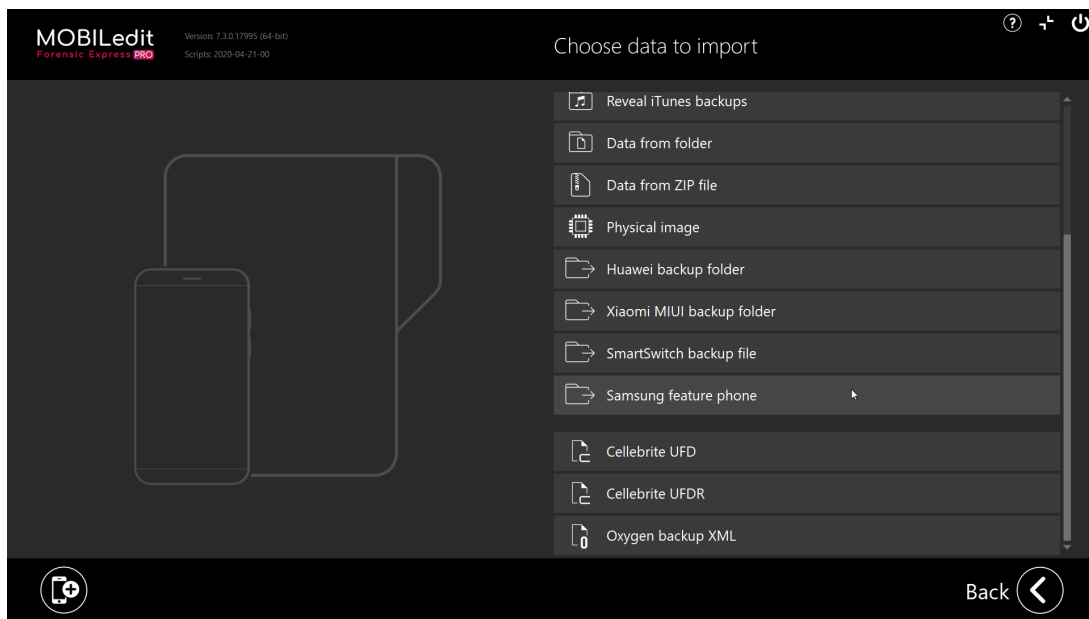
4.1 Import data

- [MOBILedit Backup XML](#)(see page 238)
- [Android ADB backup file](#)(see page 238)
- [iTunes backup folder](#)(see page 239)
- [Data from folder](#)(see page 239)
- [Data from ZIP file](#)(see page 239)
- [Physical Image](#)(see page 239)
- [Huawei backup folder](#)(see page 240)
- [Xiaomi backup folder](#)(see page 240)
- [Cellebrite UFED Report](#)(see page 240)
- [Oxygen Backup XML](#)(see page 240)
- [Samsung Smart Switch backup](#)(see page 240)
- [Samsung feature phone](#)(see page 241)

Data does not always need to be extracted directly from a live connected device. It is also possible to load one of several available backup formats or other compatible file types and process their content in the same fashion as if the physical device was present.

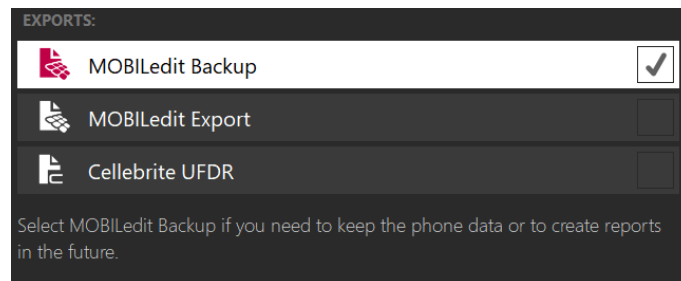
Import data screen





4.1.1 MOBILedit Backup XML

This is the native backup format of our products - MOBILedit Forensic, MOBILedit Forensic Express, and Phone Copier Express. Anytime you perform an export, you may select MOBILedit Backup as one of the output formats. This will generate a `mobiledit_backup.xml` file, which can be loaded later, and processed again with a different configuration.



i This import option is available for all the license types of MOBILedit Forensic Express.


4.1.2 Android ADB backup file

Allows loading an Android ADB backup. You may be prompted to enter a password if the backup is encrypted.

w This import option is NOT available for the Single Phone license of MOBILedit Forensic Express.


4.1.3 iTunes backup folder

It allows you to load an iTunes backup, which is in the form of a folder, typically named with a 40-character hexadecimal code and containing a set of similarly named binary files. Usually, an iTunes backup is encrypted, in which case you will be prompted to enter the password.

 This import option is available for all the license types of MOBILedit Forensic Express.


4.1.4 Data from folder

Will analyze media files, such as photos and videos for all possible metadata such as GPS locations displayed in maps, timestamps, camera model, etc. A wide range of media formats is supported besides standard JPG, PNG, GIF, AVI, MP4, MKV we analyze also RAW and new HEIF/HEIC with H.265. Also, audio files and documents can be analyzed. MOBILedit Forensic Express also analyzes videos and [storyboard](#)(see page 366), so it can be understood without playing videos or when printed. Timeline of all media files can be created. If you have [Camera Ballistics](#)(see page 413) installed, then you get information if a photo comes really from the camera analyzed or not.

 This import option is available ONLY for the Unlimited license of MOBILedit Forensic Express.

4.1.5 Data from ZIP file

Will analyze zipped media files, such as photos and videos for all possible metadata such as GPS locations displayed in map, timestamps, camera model etc. A wide range of media formats is supported besides standard JPG, PNG, GIF, AVI, MP4, MKV we analyze also RAW and new HEIF/HEIC with H.265. Also, audio files and documents can be analyzed. MOBILedit Forensic Express also analyzes videos and [creators of storyboard](#)(see page 366), so it can be understood without playing videos or when printed. Timeline of all media files can be created. If you have [Camera Ballistics](#)(see page 413) installed, then you get information if a photo comes really from the camera analyzed or not.

 This import option is available ONLY for the Unlimited license of MOBILedit Forensic Express.


4.1.6 Physical Image

In case you have made a [Physical Image](#)(see page 42) of your phone, this is the option for you to select. Locate the image on your disk and proceed to analyze it, as if it was a live connected phone with more data available.

 This import option is NOT available for the Single Phone license of MOBILedit Forensic Express.


4.1.7 Huawei backup folder

Allows loading a [Huawei backup](#)(see page 251). You may be prompted to enter a password if the backup is encrypted.

 This import option is available ONLY for the Unlimited license of MOBILedit Forensic Express.


4.1.8 Xiaomi backup folder

Allows loading a [Xiaomi backup](#)(see page 255). You may be prompted to enter your password if the backup is encrypted.

 This import option is available ONLY for the Unlimited license of MOBILedit Forensic Express.


4.1.9 Cellebrite UFED Report

With this option, you can load .ufdr archives from Cellebrite UFED, which allows you to analyze applications and extract data that Cellebrite may not have been able to.

 This import option is NOT available for the Single Phone license of MOBILedit Forensic Express.


4.1.10 Oxygen Backup XML

With this option, you can load backups from Oxygen Forensic Suite, which allows you to analyze applications and extract data that Oxygen may not have been able to.

 This import option is available ONLY for the Unlimited license of MOBILedit Forensic Express.

4.1.11 Samsung Smart Switch backup

This option allows you to load and analyze [Samsung Smart Switch backup](#)(see page 243) files in MOBILedit Forensic Express

 This import option is available ONLY for the Unlimited license of MOBILedit Forensic Express.

4.1.12 Samsung feature phone

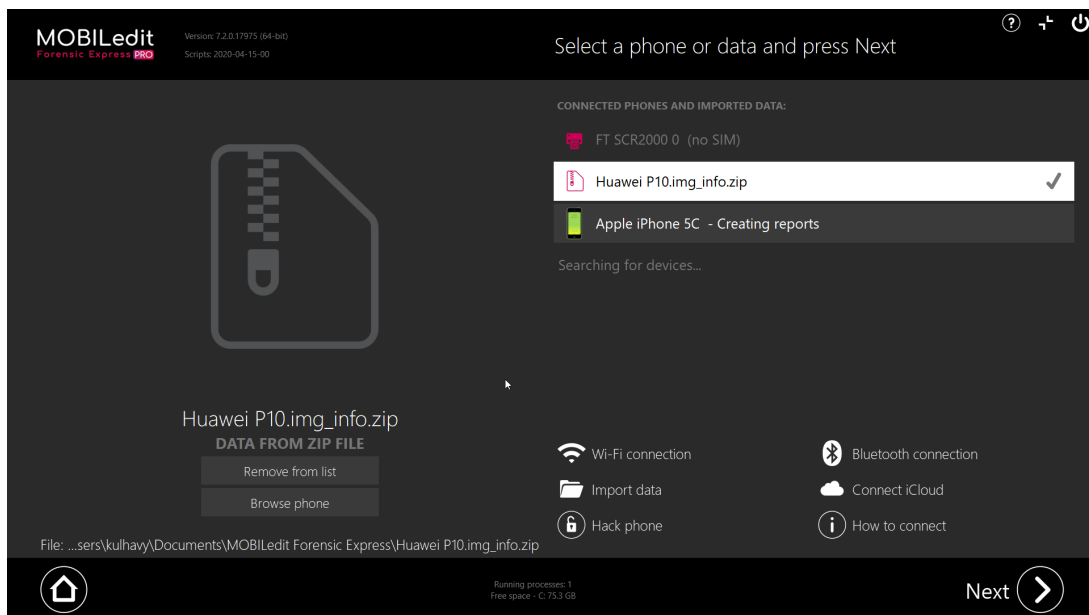
Allows importing backup files created from Samsung feature phones. (Phones without operating system).

More information [here](#).(see page 241)

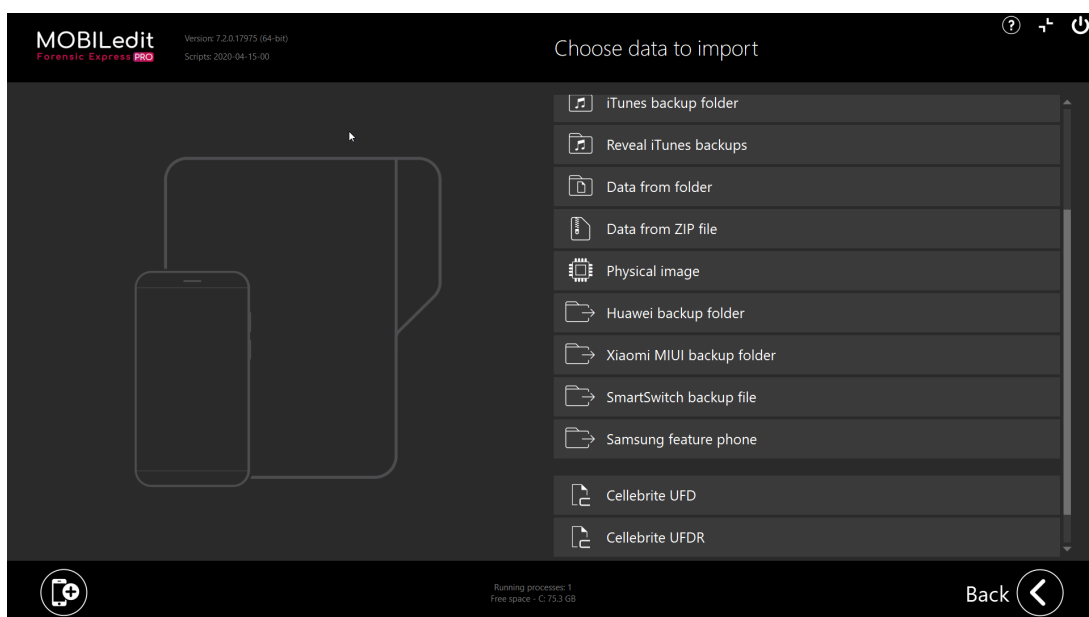
4.2 Samsung feature phone ´s backup import

Backups created in Samsung feature phones are supported by MOBILedit forensic express.

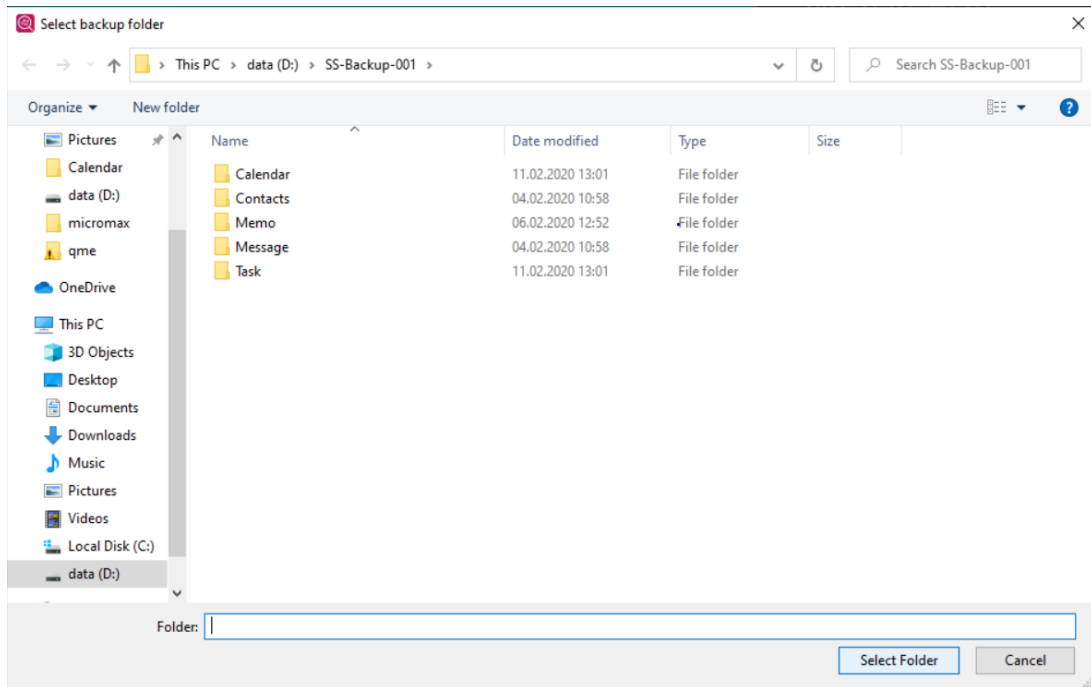
Simply click the **Import data**(see page 237) button on the lower centre section:



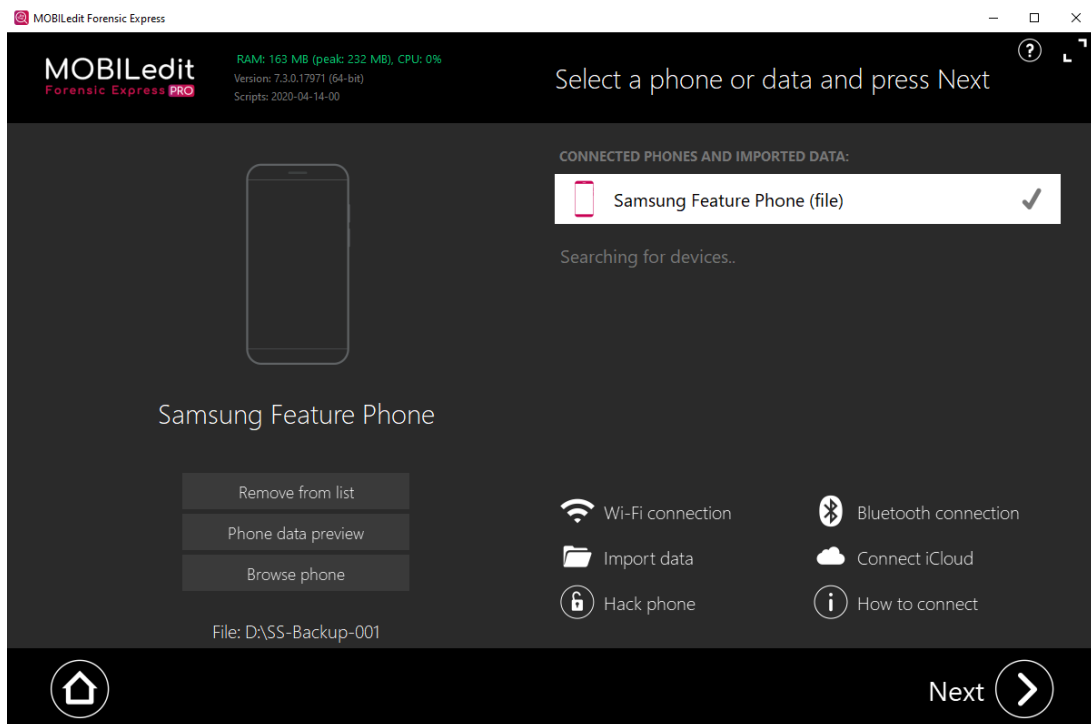
Proceed by selecting the **Samsung feature phone** option:



Select your desired backup:



Continue with the standard acquisition by clicking **next**.



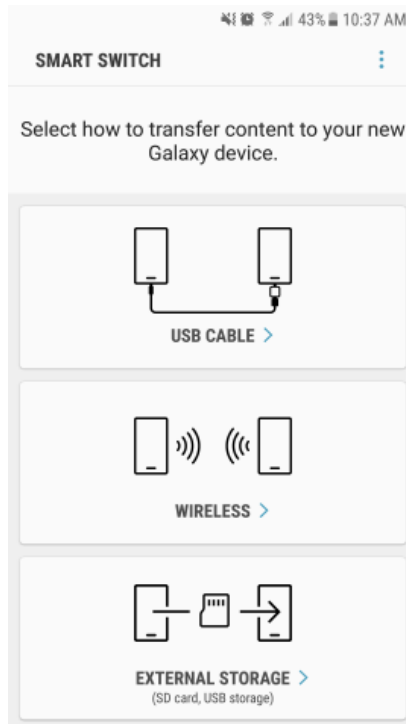
i Backup files from Samsung feature phones have to be created in the device itself by using their built-in feature. Newer models support the SmartSwitch backup option, which is also compatible with MOBILedit software.

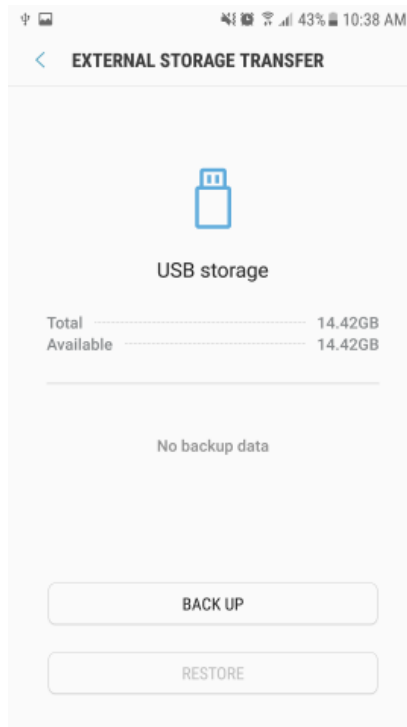
4.3 Samsung Smart Switch backup

With MOBILedit, you can upload and analyze Samsung Smart Switch backup files. Below you can find a guide on how to create this backup and upload it to the software.

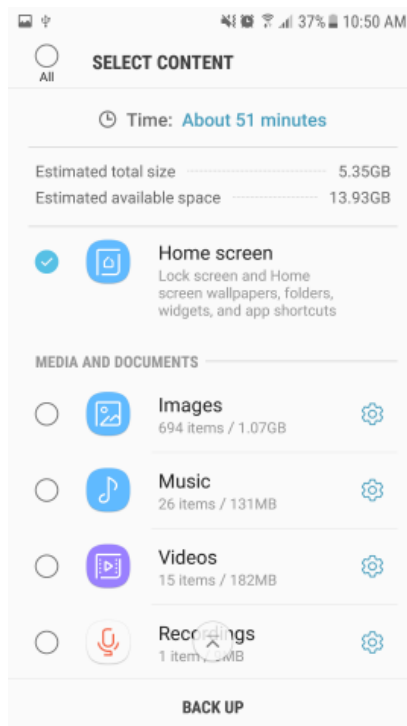
4.3.1 How to

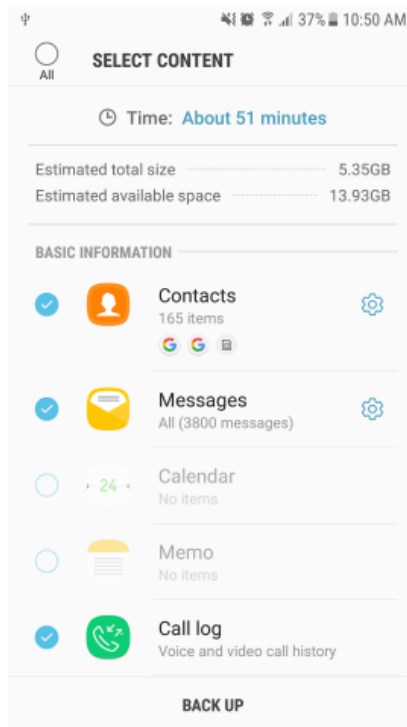
1. Open the Smart Switch app on your Samsung device and select the "EXTERNAL STORAGE" option.



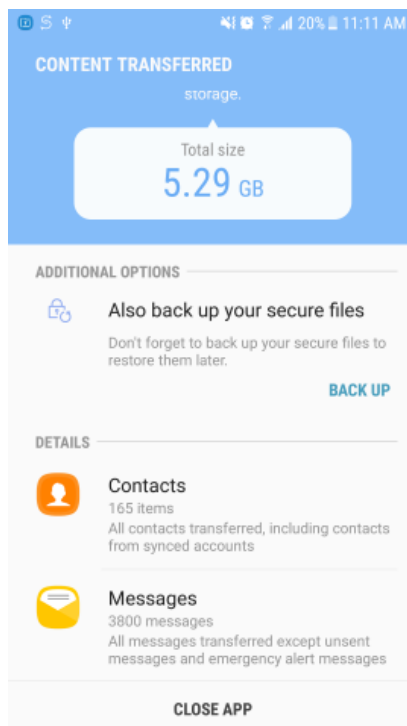


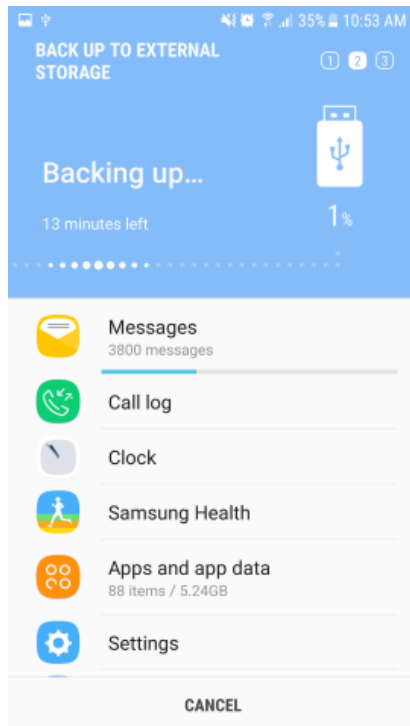
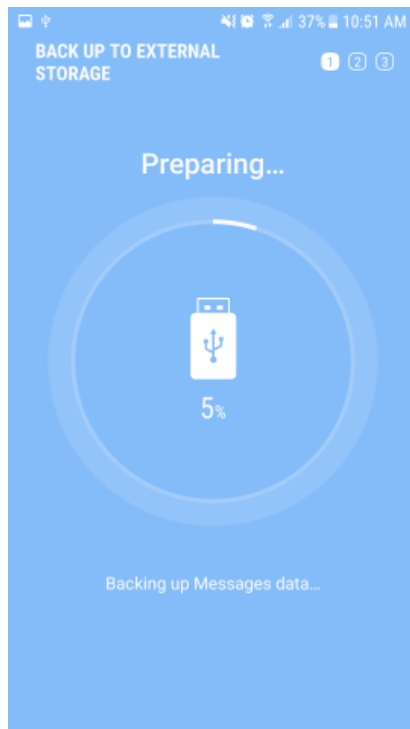
2. Connect your USB flash drive via OTG cable and select which data you want to back up.



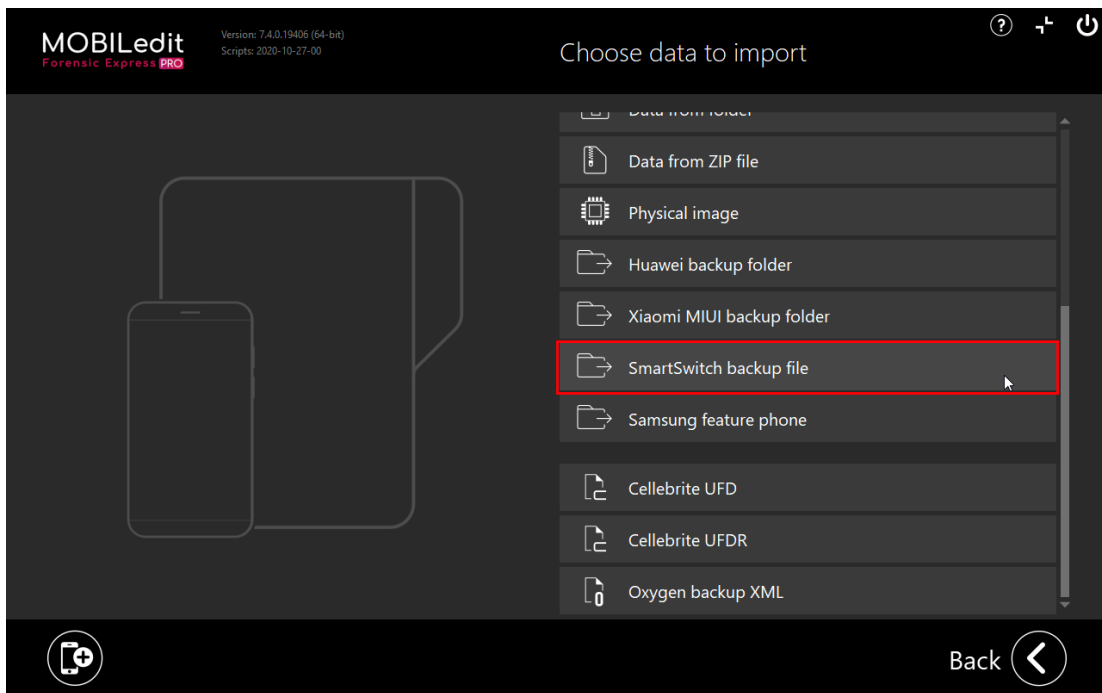
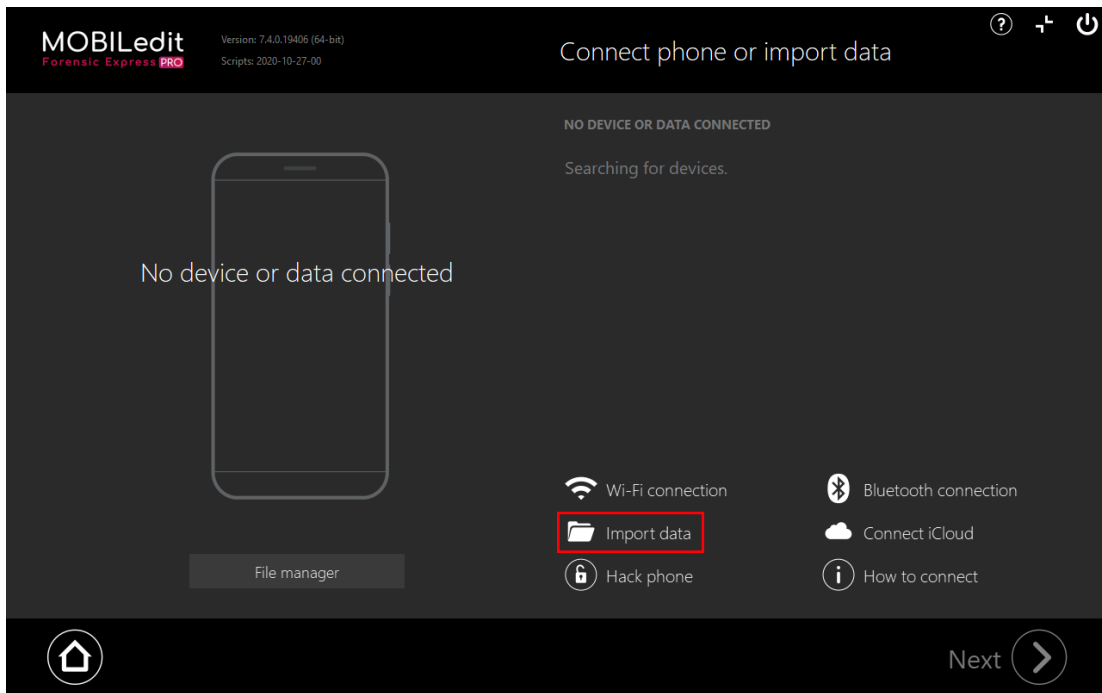


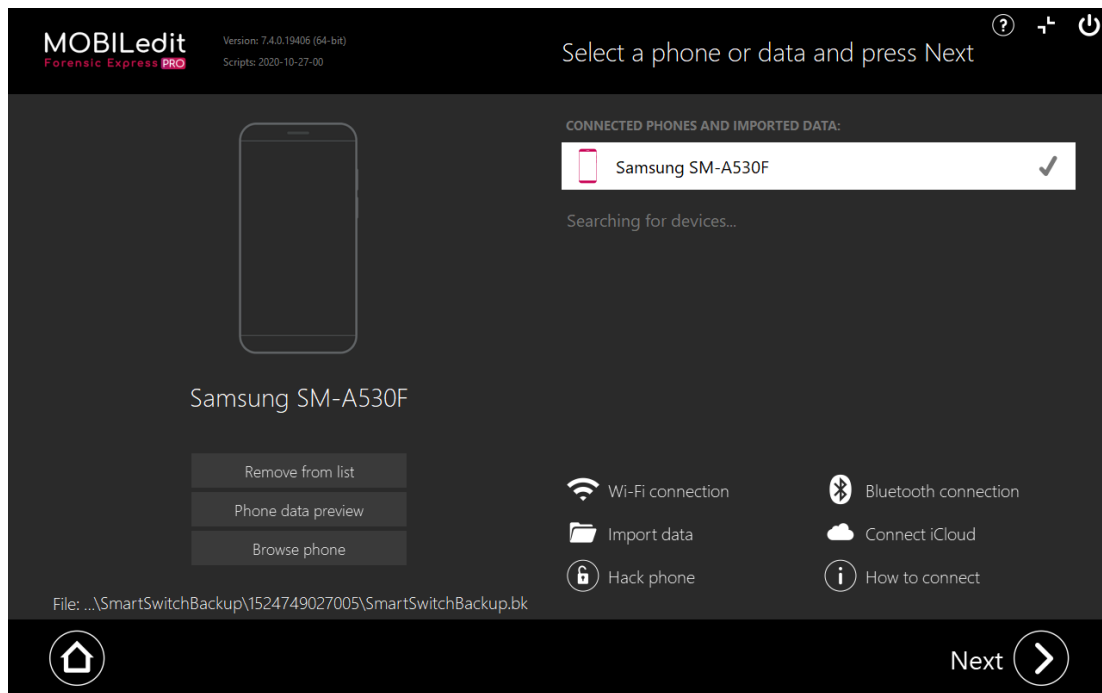
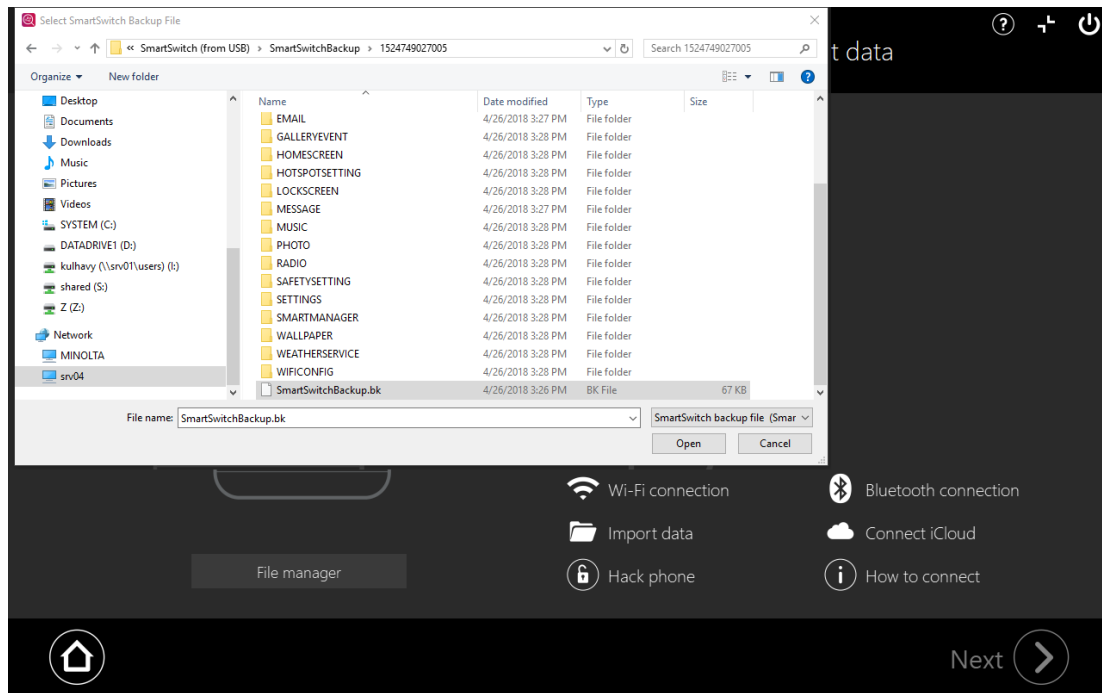
3. Click on the "BACK UP" button and wait for the process to finish.





4. Connect the USB drive to your PC, open Forensic Express and load the backup file as seen on the screenshots below:





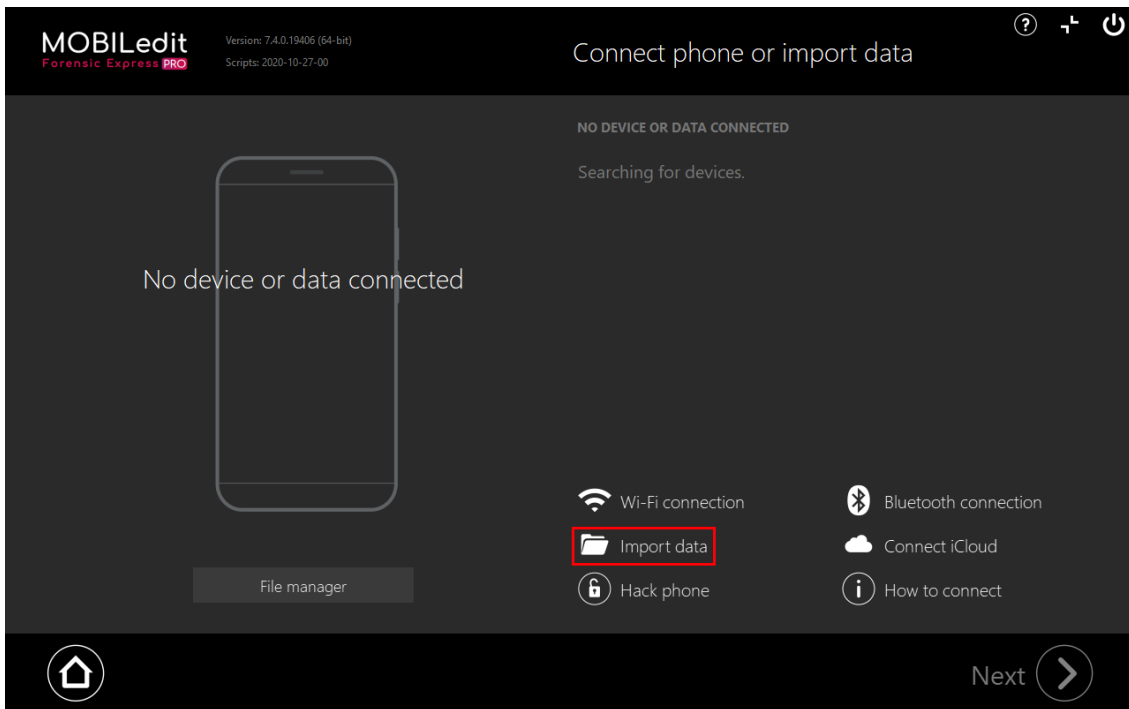
5. Now the backup file has been loaded and is ready to be analyzed.

4.4 Reveal iTunes Backup

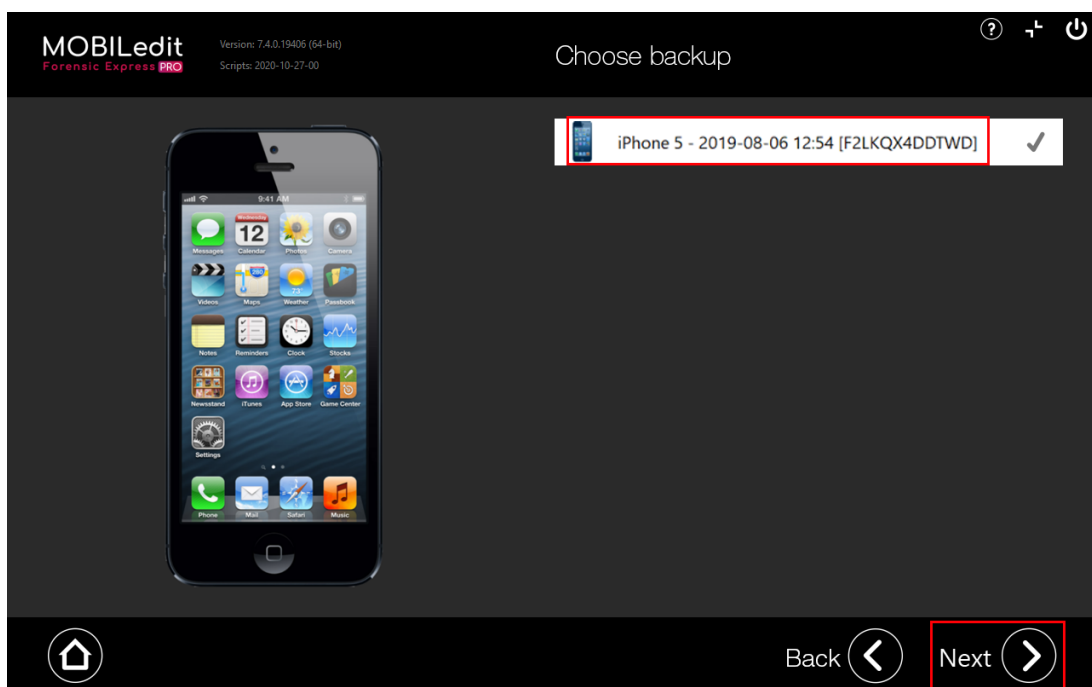
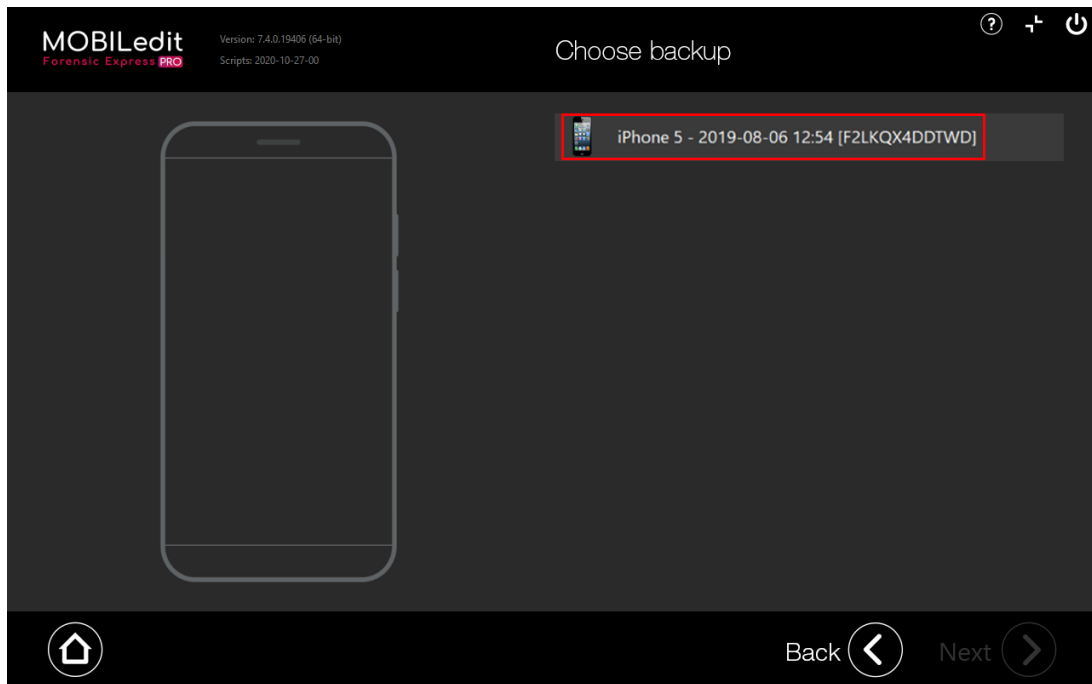
If you previously used iTunes software to back up your iOS device, you can use this feature in order to extract data from the created iTunes backup using MOBILedit Forensic Express.

4.4.1 How to

1. Open MOBILedit Forensic Express.
2. Click on "Import data".

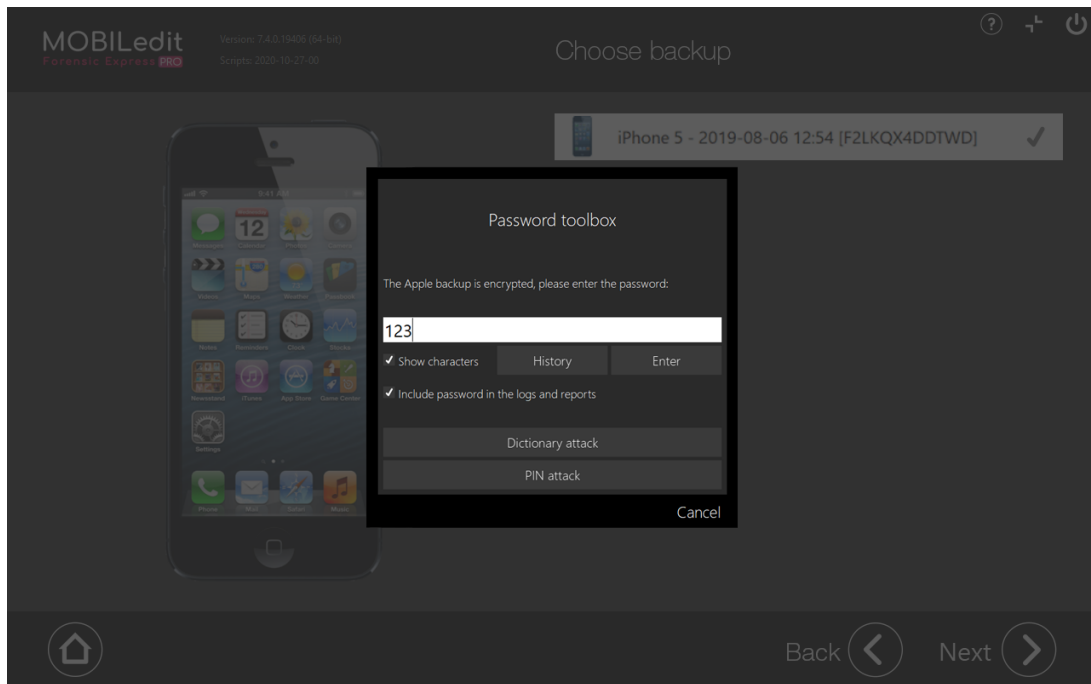


3. Choose the "Reveal iTunes backups" option.
4. A list of available backups will show up - choose which one you want to extract data from.

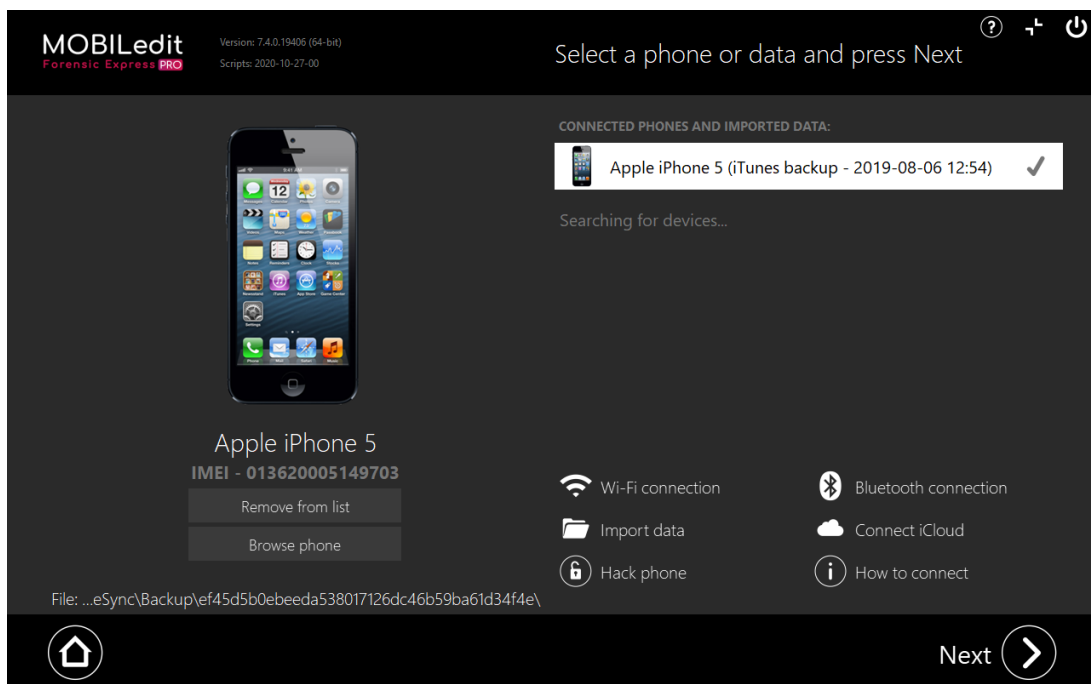


5. Once you've selected a backup, click Next and enter the password for the backup (if required). If you don't know the password, you can always try to break it with our [password breaker](#)(see page 284).

i In case the password is non-existent, it is automatically to "123" (and unset after the extraction is finished).



6. After entering the correct password, the backup will be loaded into MOBILedit Forensic Express and you'll be able to perform an extraction just as if an actual device were connected.



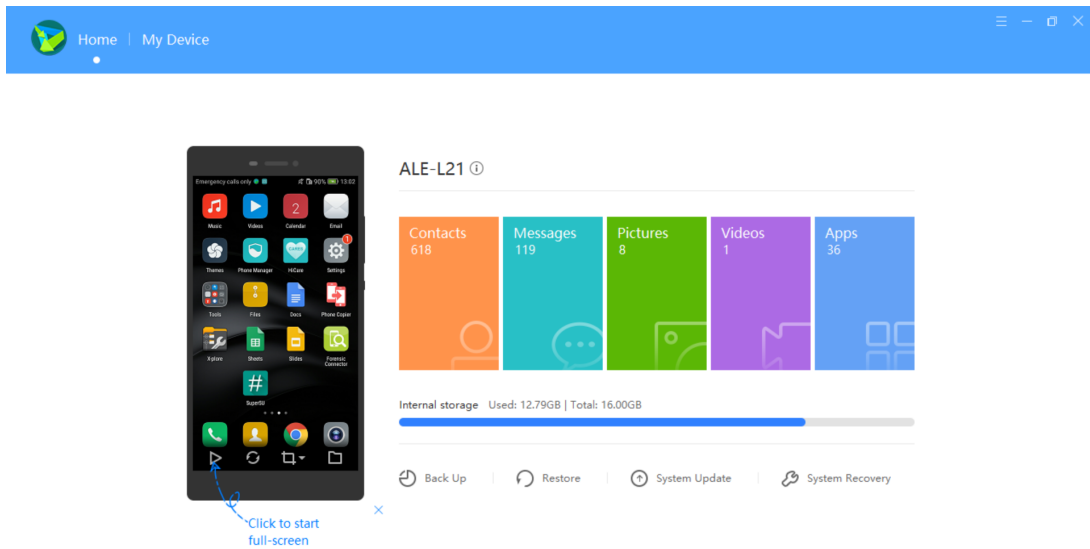
4.5 Huawei backup

This option allows users to extract even more data from Huawei devices than they would be able to get while extracting from a live connected phone.

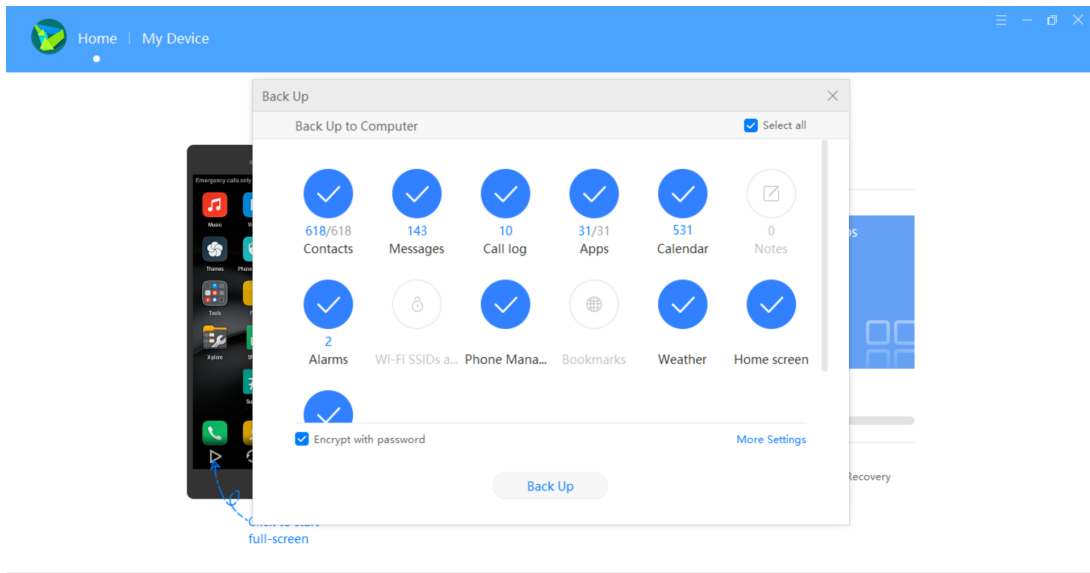
Basically, all you need to do is create and save a backup of your Huawei device using HiSuite software provided by Huawei; MOBILedit Forensic Express will then extract the data from the [imported data](#) (see page 237) backup you have created (instead of from the phone itself).

4.5.1 How to

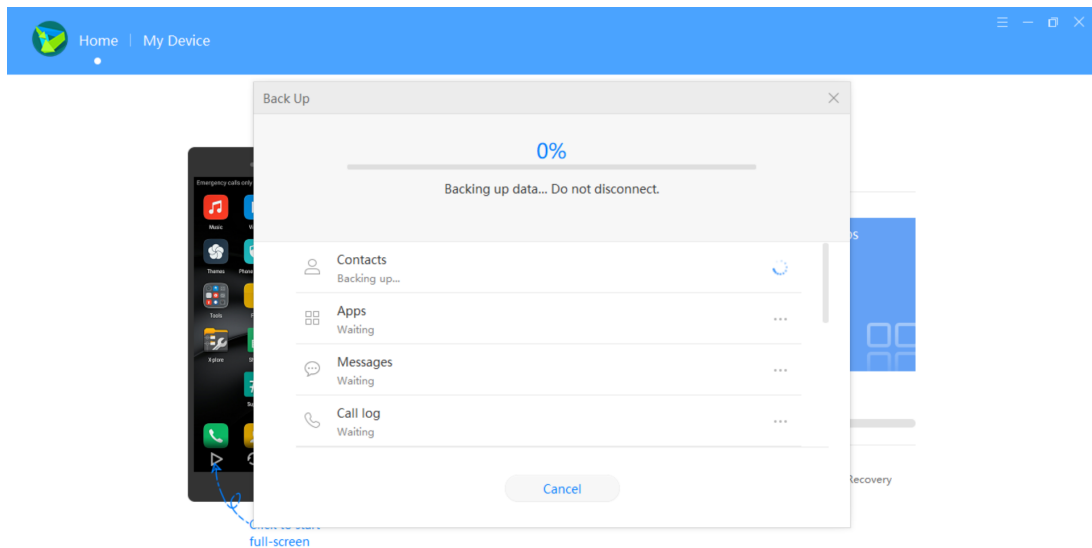
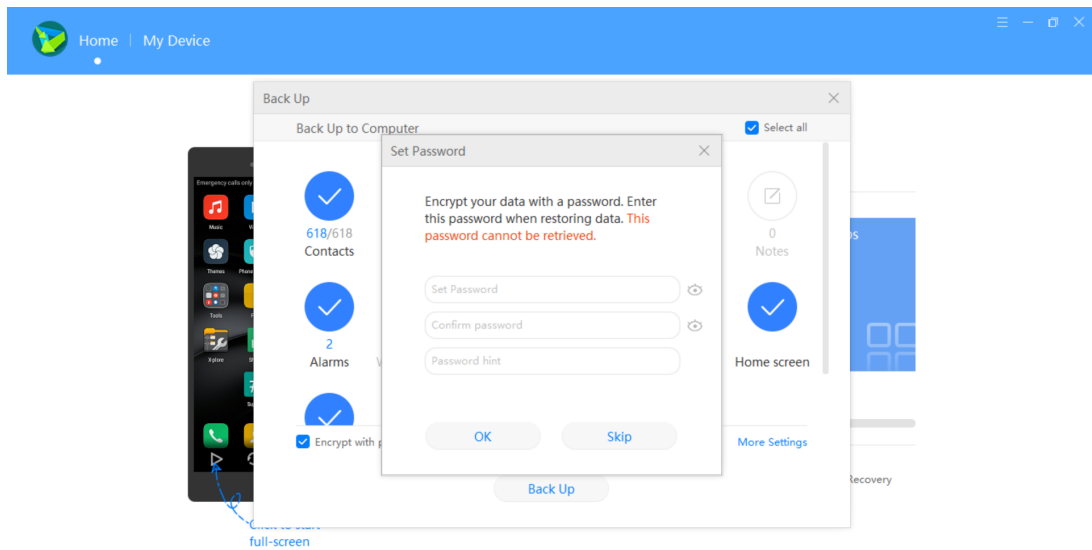
1. Download the latest HiSuite and install it on your PC.



2. Open it and connect your phone via USB cable.
3. Click on the **"Back Up"** button and wait for the HiSuite to load data which can be backed up.

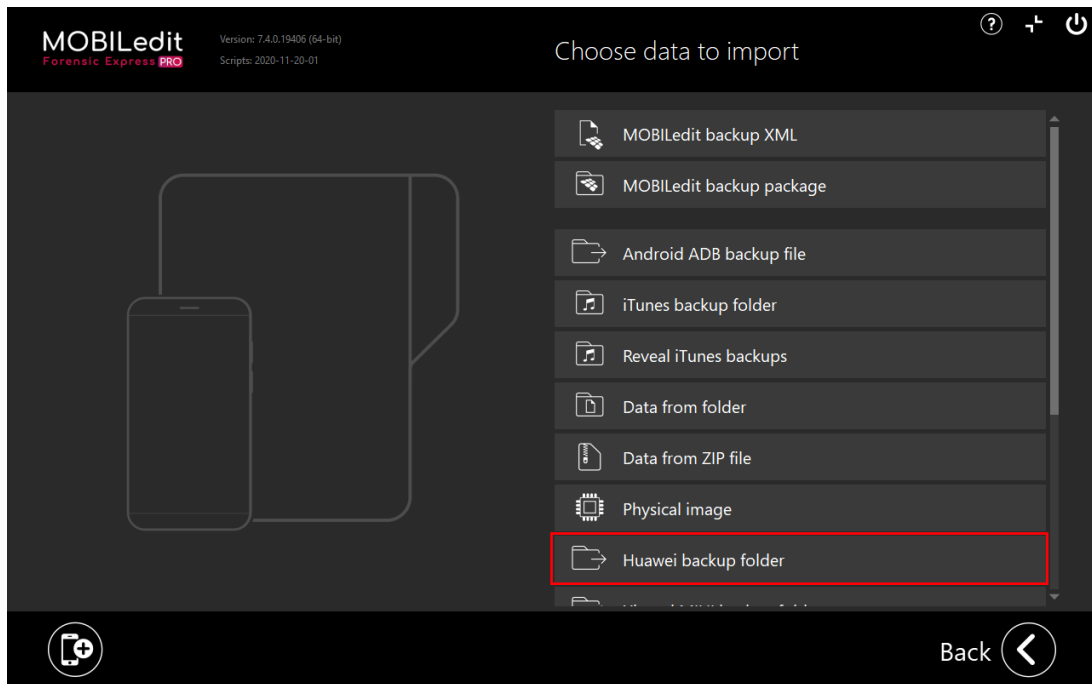


4. **IMPORTANT** - before creating the actual backup, make sure to encrypt it with a password as shown in the picture below. Otherwise, a universal password will be generated and the backup file will be useless for analysis in Forensic Express.

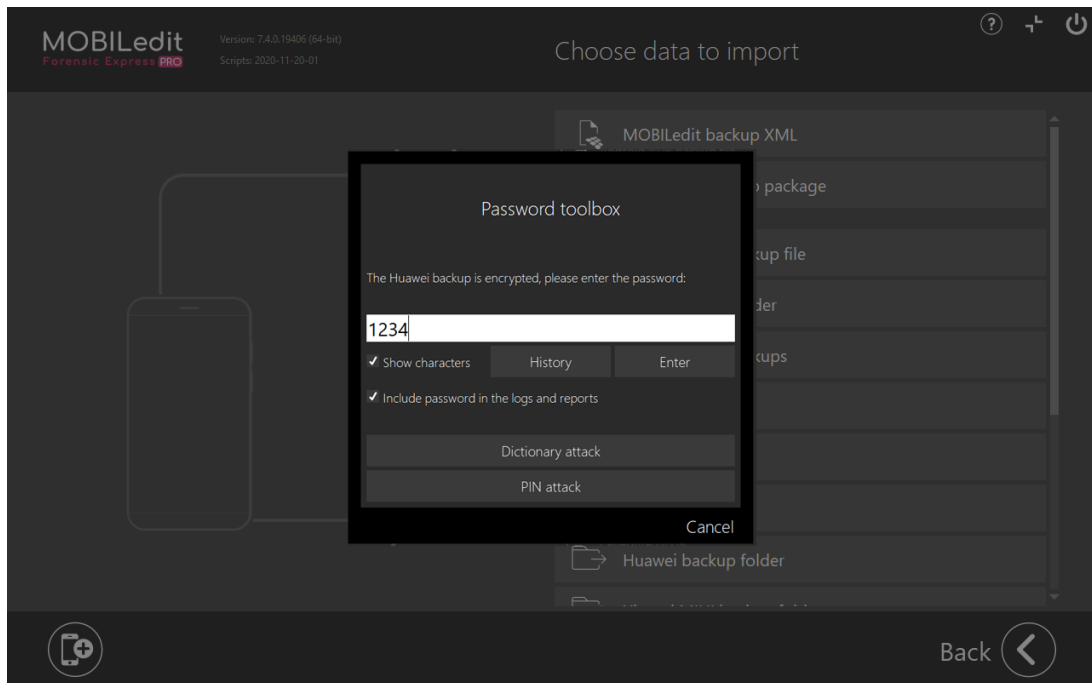


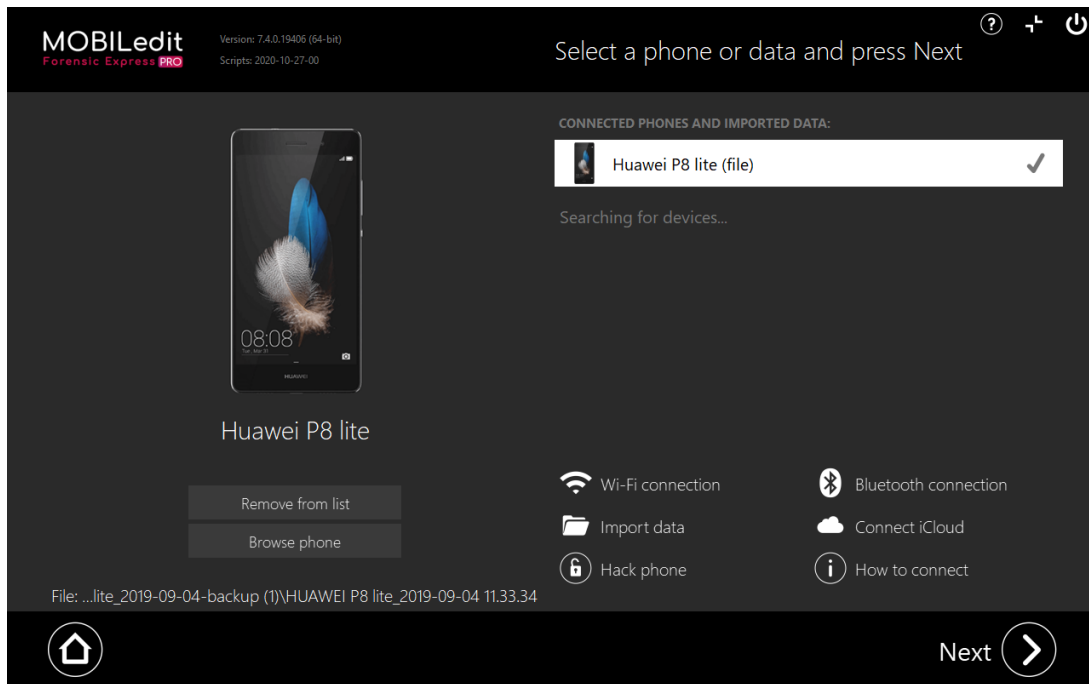
5. After you've set a password, proceed to create the actual backup of your device.

6. once the backup process is finished, open Forensic Express, click on "**Import data**(see page 237)" and choose "**Huawei backup folder**".



7. Choose the folder you've saved your backup in, enter the password you created for the Huawei backup, and start the extraction in the same way you would do with a live connected phone.



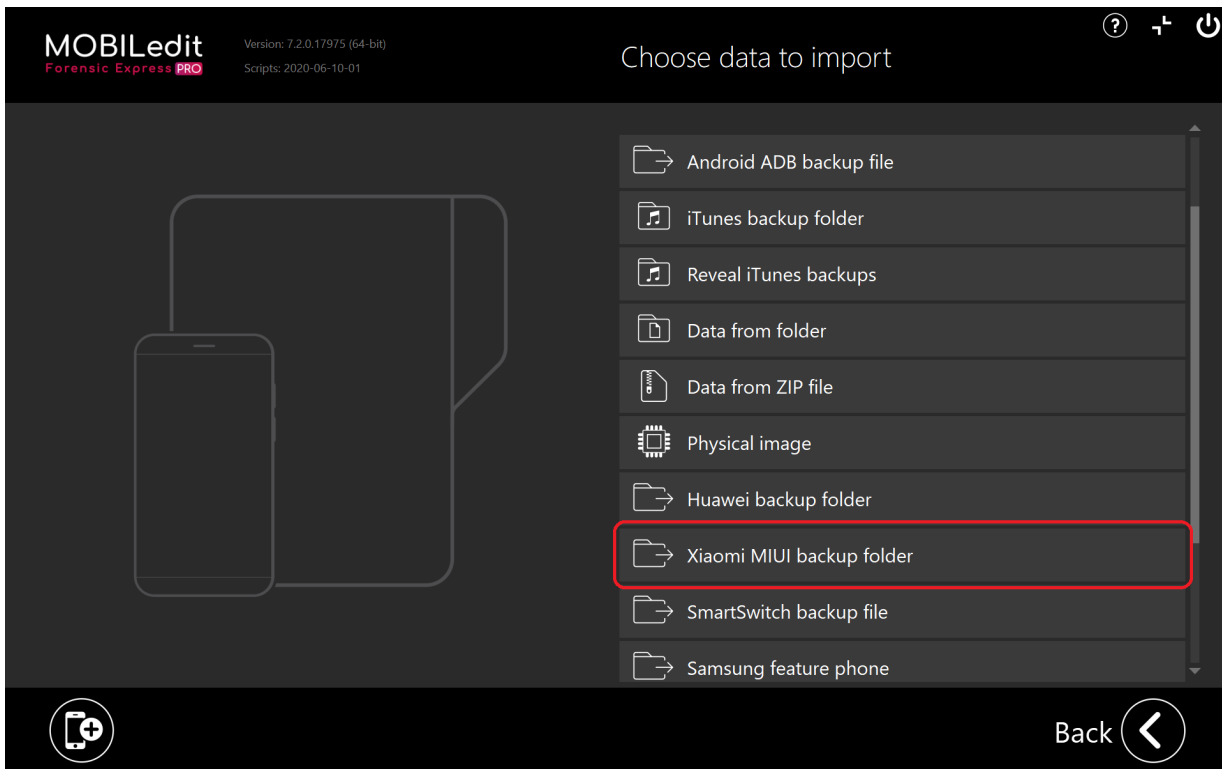


4.6 Xiaomi-MIUI backup

- [Local backup in phone](#)(see page 256)
- [Mi PC suite backup](#)(see page 257)

If you have a non-rooted Xiaomi phone you can get better results by extracting data from an MIUI backup than you would get using a classic 'full content' extraction.

Choose the "import data" option and then choose the “Xiaomi MIUI backup folder”:




4.6.1 Local backup in phone

1. Open "Settings".
2. Tap on "About phone".
3. Tap on "Back up and reset".
4. Select "Mobile backups".
5. Select what you want to back up and lastly hit the "Back up" button.
6. Once it is finished the back up is stored on SD card or in internal memory (if you do not have an SD card). The path is : **/MIUI/Backup/Allbackup**

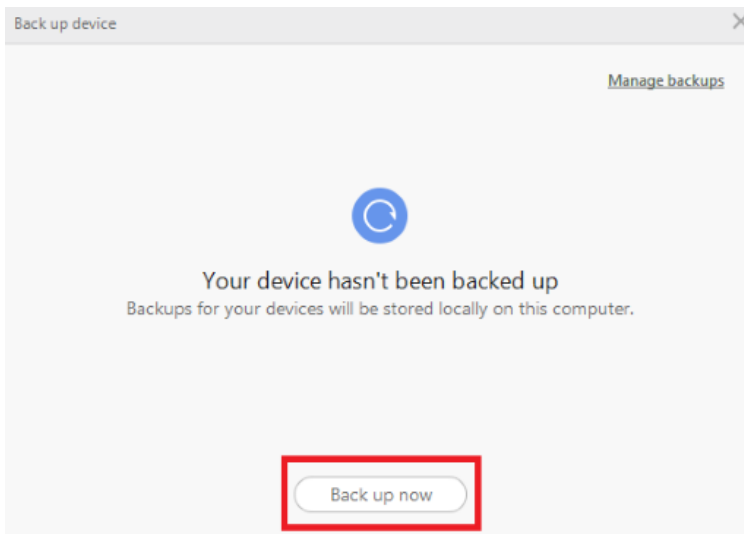
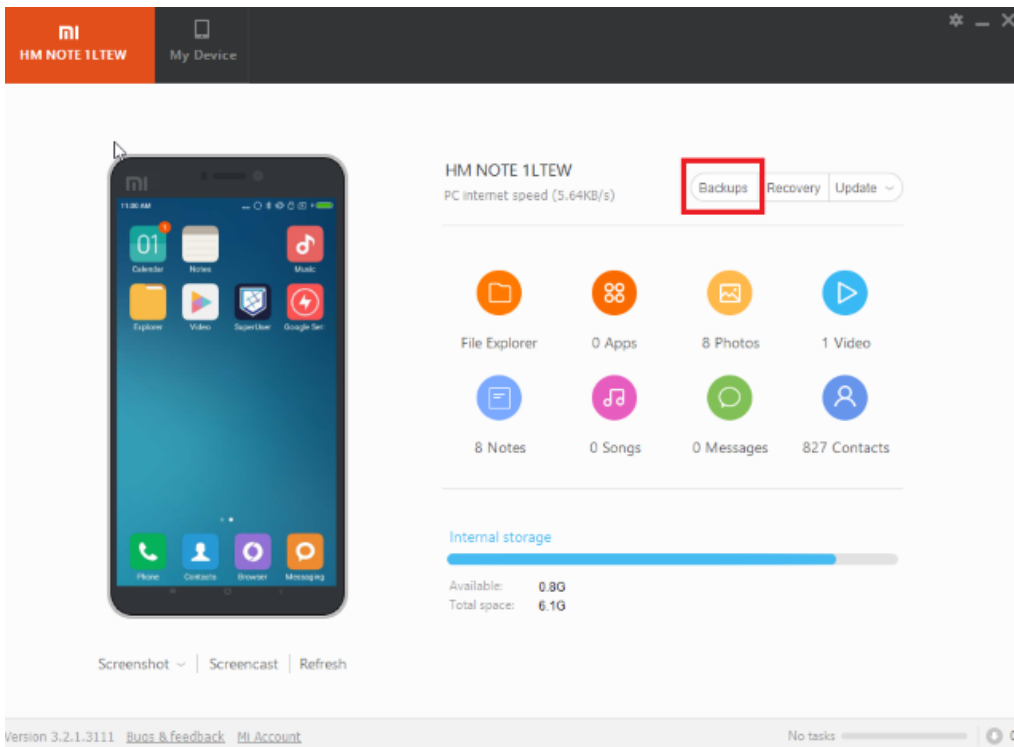
Below is an animated image that shows all the steps of creating a local backup of the phone.



 Some items might fail, it is due to Xiaomi not supporting the application.

4.6.2 Mi PC suite backup

1. Connect your Xiaomi device to your computer via USB.
2. Open Mi PC Suite and click on "Backups".
3. On the Backup device window, you can see information about available backups.
4. Click on "Back up Now".



5. The backup folder is by default located at **C:\Xiaomi\MiPhoneManager\Data\XXXXXX.git**

4.7 Built-in SIM Cloning

- Data extraction (see page 259)
- SIM Cloning (see page 260)
- Create a custom SIM card: (see page 263)

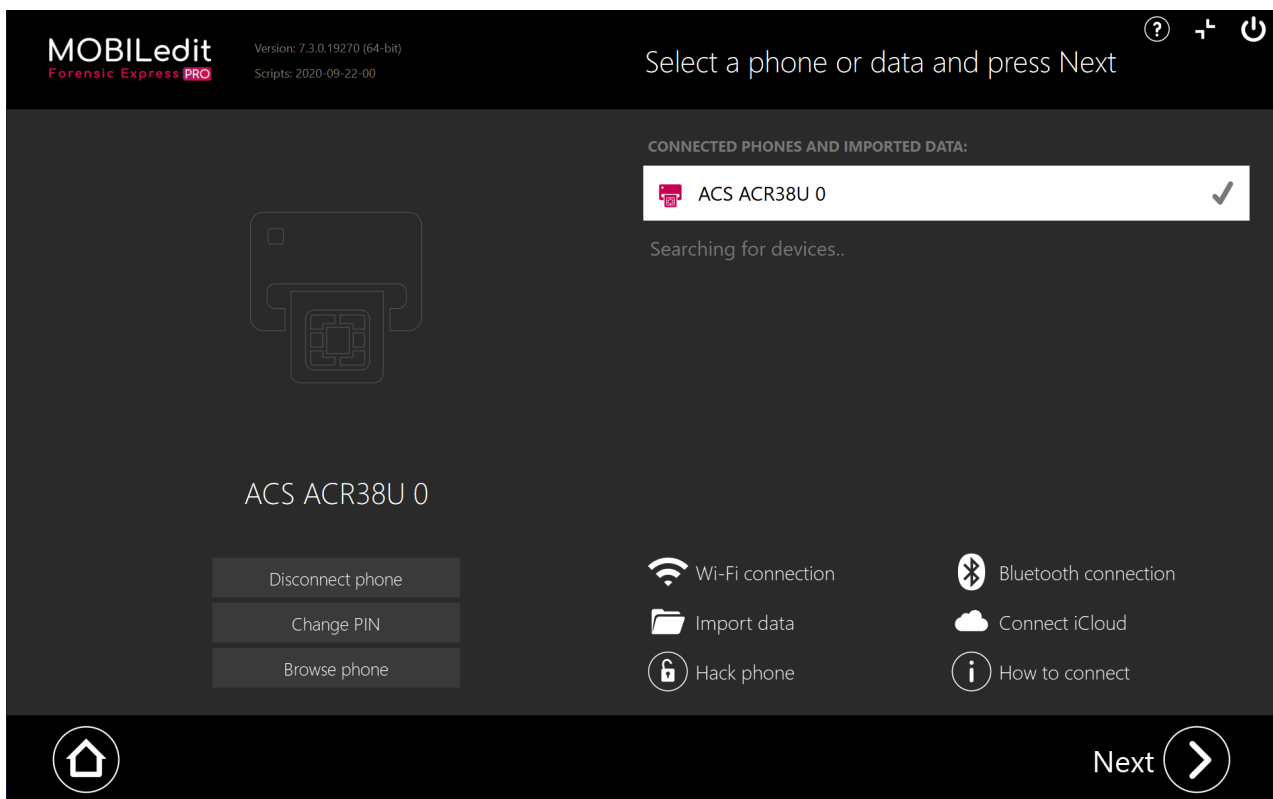
i The built-in SIM Clone functionality enables you to copy the content of investigated SIM card to a rewritable MOBILedit SIM Clone Card directly from MOBILedit. This way you can isolate the phone from the mobile network while you don't have any issues regarding a missing or changed SIM within the phone.

SIM Cloning does bring three new possible options:

- Data extraction
- SIM card cloning
- Creating a custom SIM card

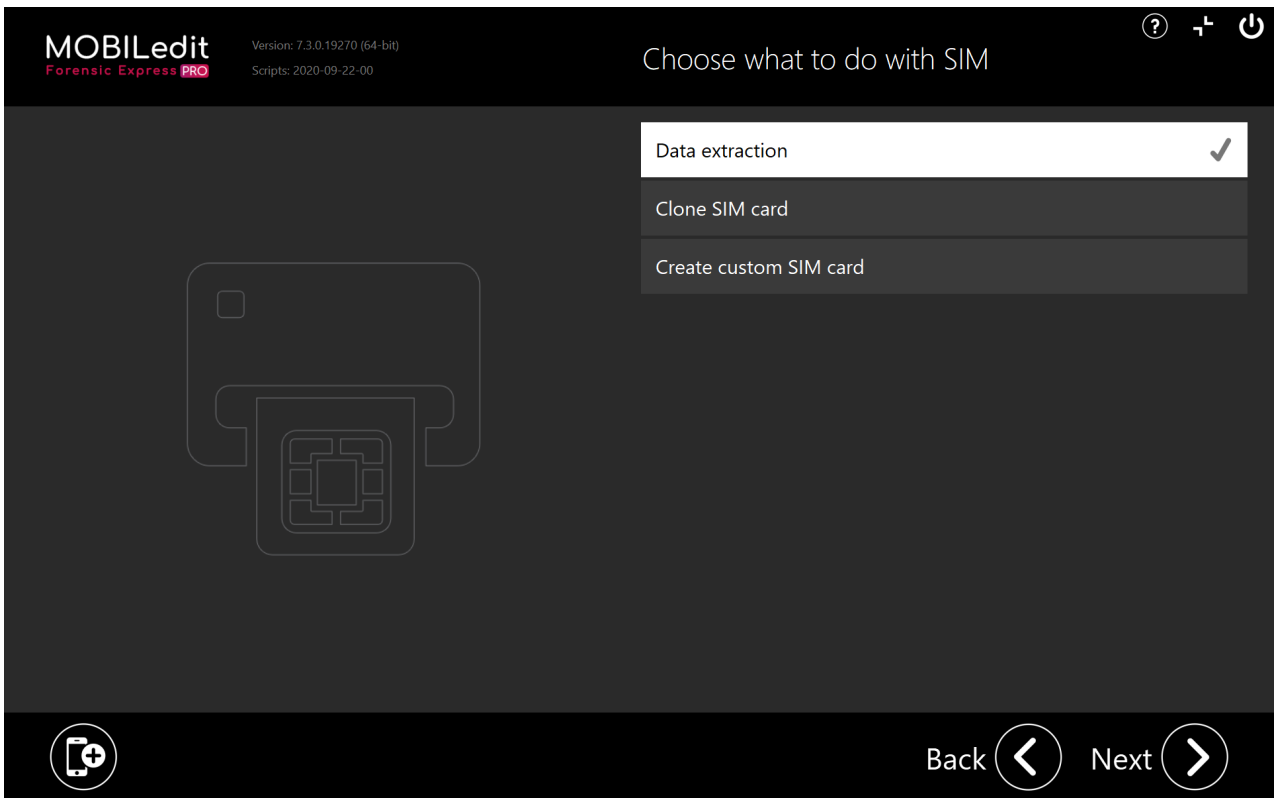
i For successful work with our SIM clone tool we recommend the use of ACS readers, which you can also find in our MOBILedit connection kit.

The first step is for every option is to insert the **SIM card reader** containing a SIM card:



4.7.1 Data extraction

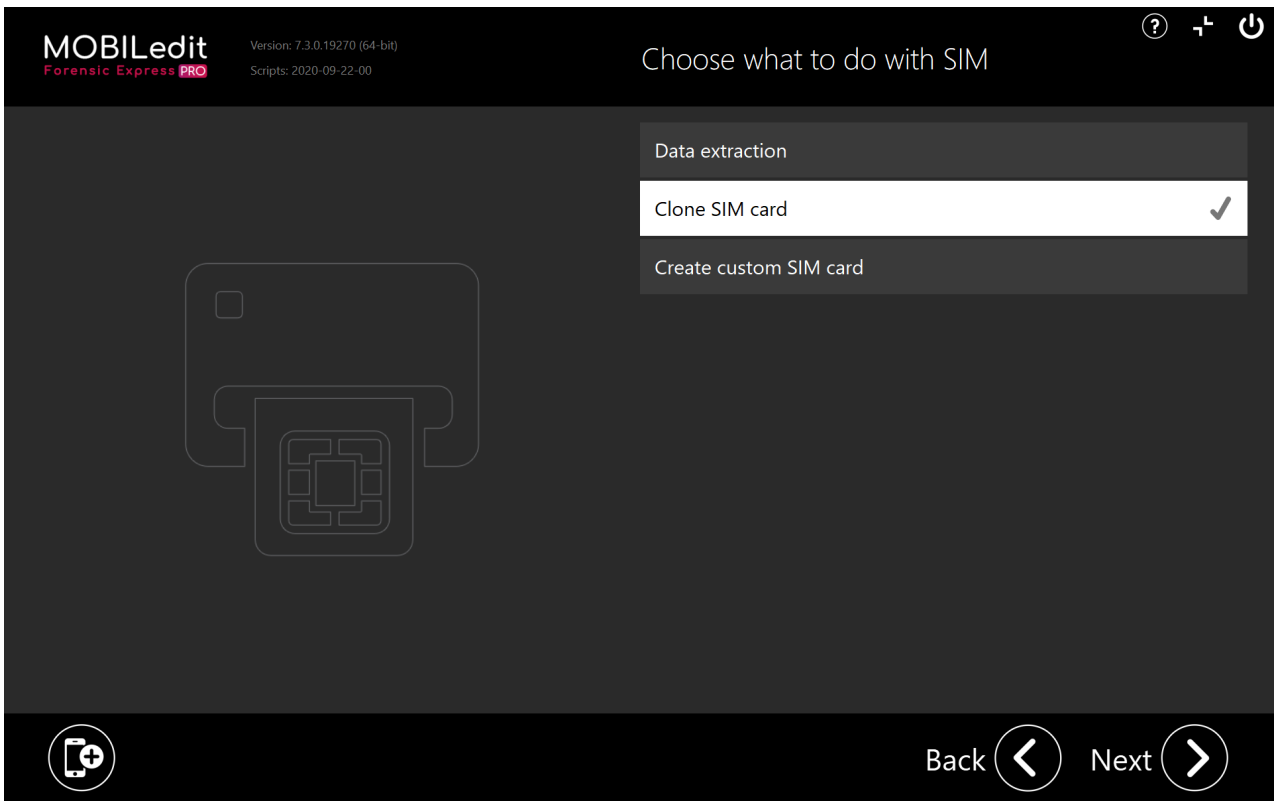
Insert a SIM card you want to extract and choose the first option:



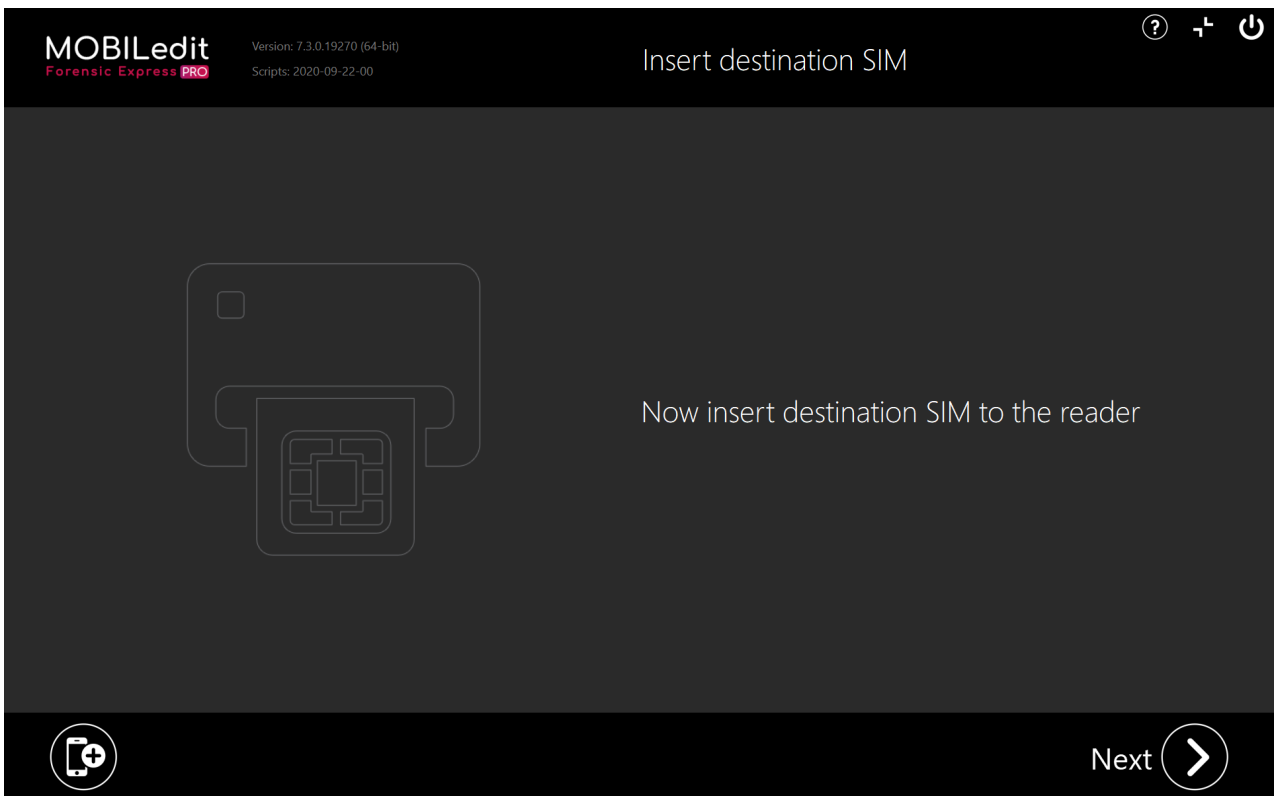
Now you can proceed with regular extraction.

4.7.2 SIM Cloning

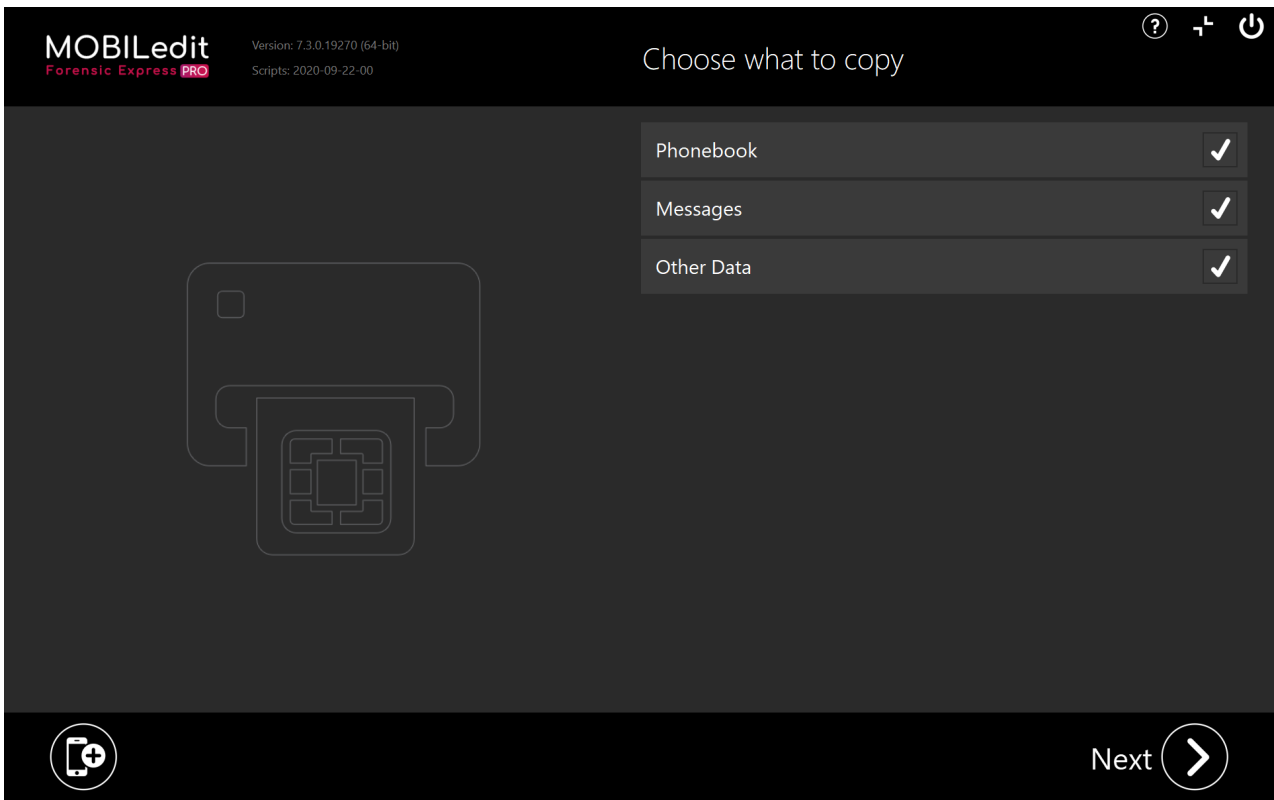
Select the **Clone SIM card** option:



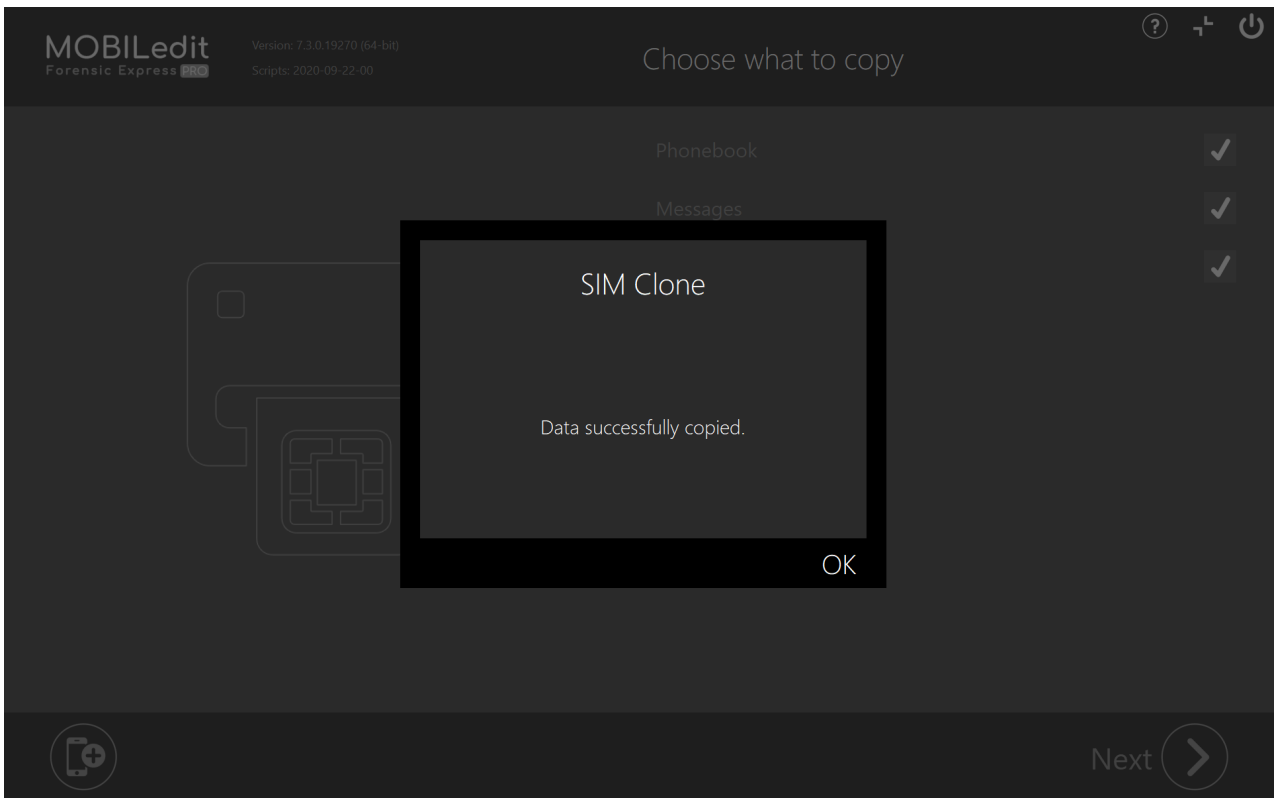
Now insert the **destination SIM card** to the reader:



Choose the desired data and click the **next** button:

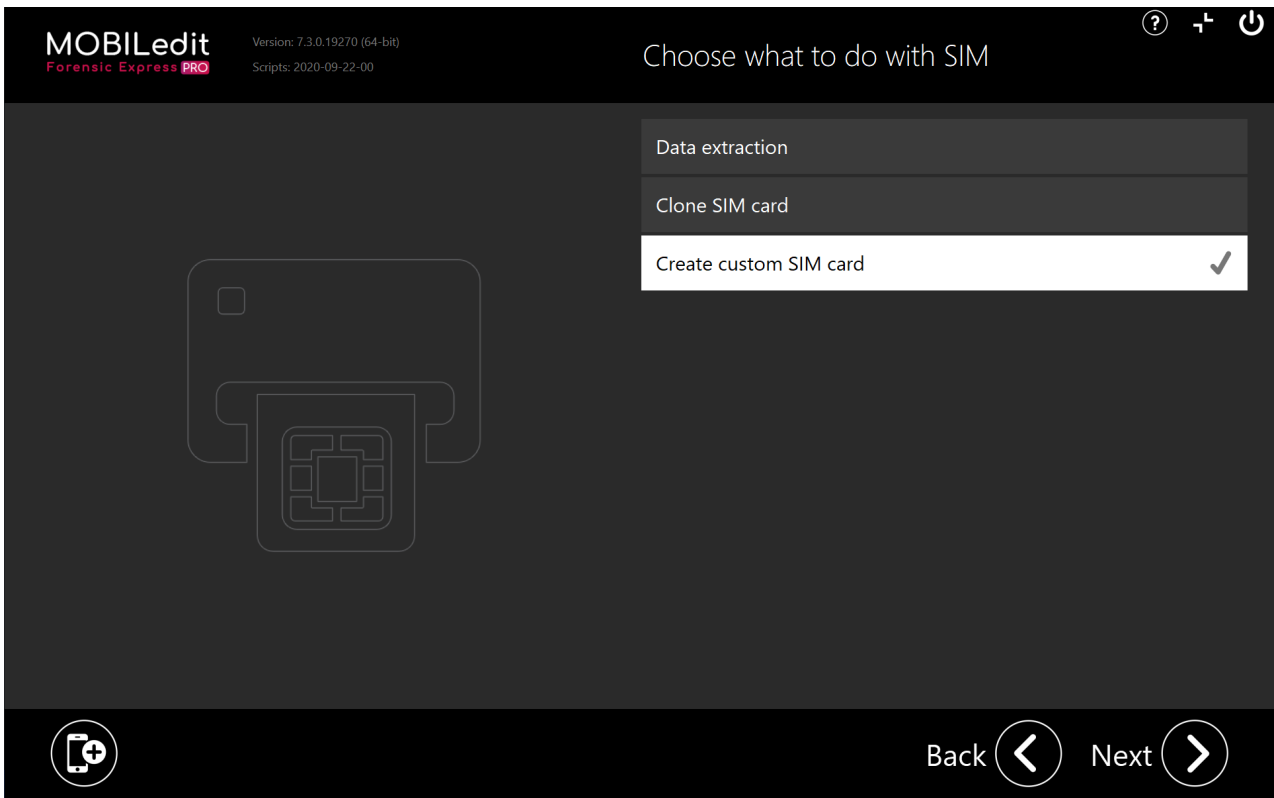


Success.

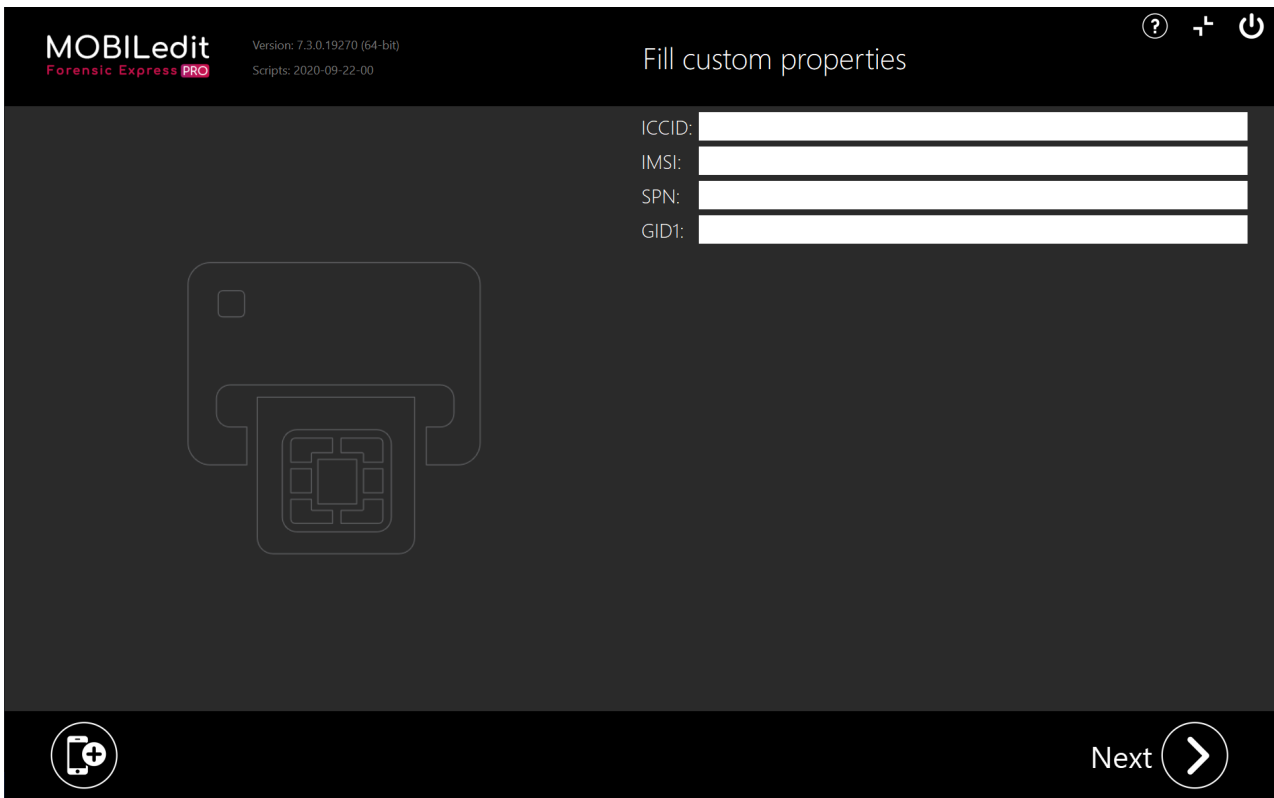


4.7.3 Create a custom SIM card:

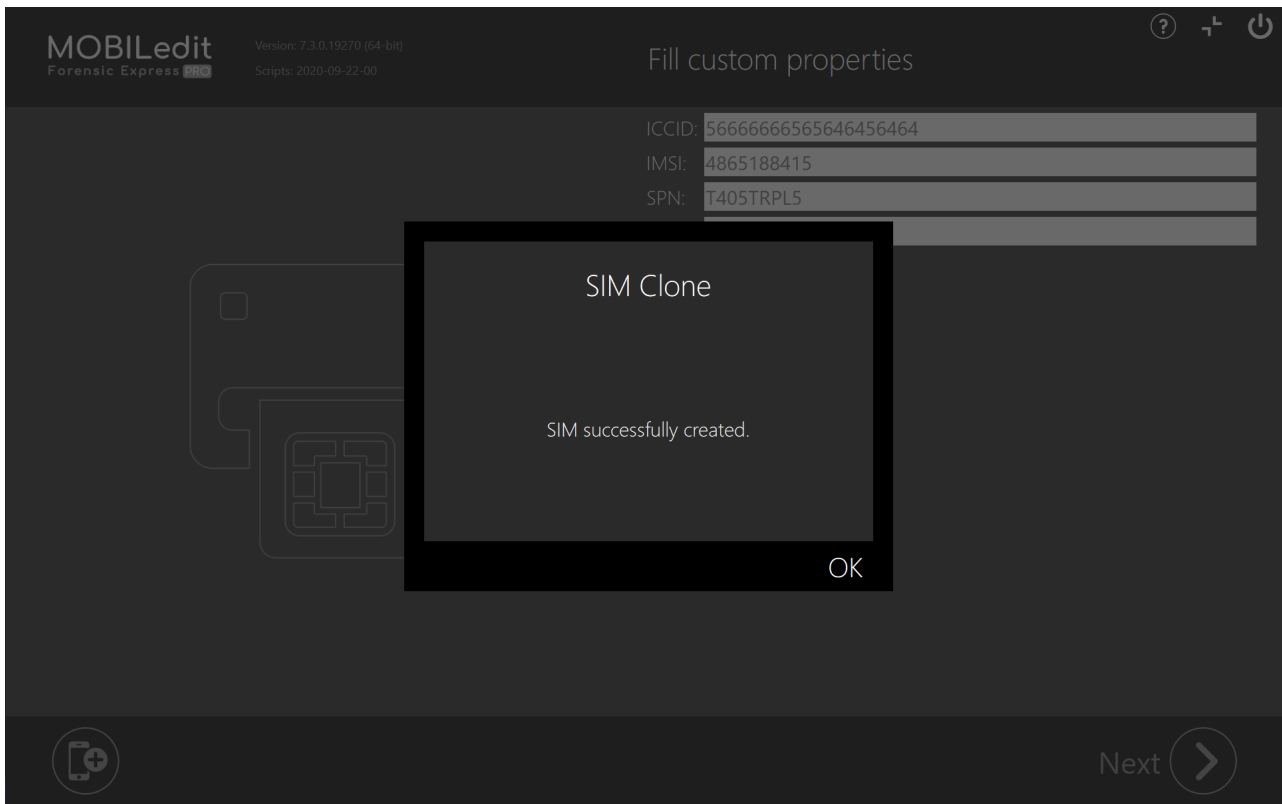
Choose the **Create custom SIM card** option:



Fill in the properties and click the **next** button:



All done:



5 Forensic reports

We've dedicated a big effort to refining reports, so they are customizable, easy to read, concise, and professional. An enhanced report configurator allows you to define exactly which data will be extracted from the phone and how the report will look. Each report is divided into sections, labeled with icons, pictures, and highlighted relevant data so you can find evidence quickly. A complete, configurable, and comprehensive list of all events with a time-stamp is shown on a timeline, and messages can be filtered by conversation or by contact names.

Reports are available in PDF, XLS, or HTML formats, and you can generate data exports compatible with the other data analysis tools you use in your lab, such as UFED.

5.1 Filtering

- [Global filters](#)(see page 266)
- [Local filters](#)(see page 266)
- [Highlights](#)(see page 266)
- [File filtering](#)(see page 266)

In order to get only the right data, you can set your filters at the start of the process, so extraction will adjust accordingly to not extract unwanted data and speed-up the process, where possible.

5.1.1 Global filters

Allows you to extract and create reports of the information that is only relevant to the case, or, only of what you want to be displayed in the final reports. Data can be filtered by time, contact, text string or location.

5.1.2 Local filters

Local filters are filters used in the "[Specific selection](#)"(see page 325) section - unlike the Global filters they only apply to specific content. Contains the following parameters: order, time, location, name, and path.

5.1.3 Highlights

This option creates a special section where all desired data will be present without affecting the rest of the report.

5.1.4 File filtering

Files can be filtered based on the [National Software Reference Library \(NSRL\)](#)⁸⁰ database of common files which effectively reduces the number of exported files. In order to use this feature, a package called File exclude list has to be downloaded in the Updates section.

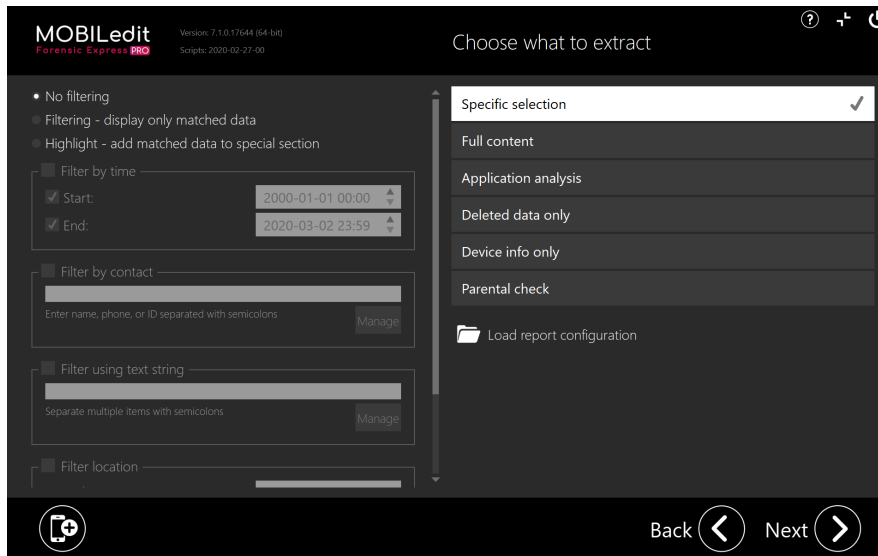
5.2 Global Filters

- [Filter by time](#)(see page 267)
- [Filter by contact](#)(see page 268)
- [Filter using a text string](#)(see page 268)

⁸⁰ <https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl>

- [Filter by location](#)(see page 269)

When choosing [Specific selection](#)(see page 325) you have an option to filter the content of the report by setting specific filter parameters. This allows you to extract and create a report based on the information that is only relevant to the case, or, only of what you want in the final report.



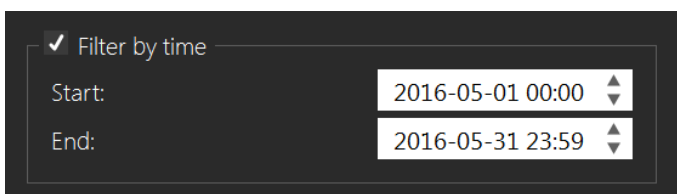
Filters can be applied globally to the entire report, or locally within specific selections with the exception of the Time filter. If you set the Time filter globally, you cannot use a different one locally.

On the 'Configure your report' page local filter settings can be set within each specific selection (Contacts, Messages, Emails, Call Logs...etc.). If both global and local filter methods are used simultaneously, only the data that satisfies both filters will be displayed in the report.

All filters using text are not case-sensitive (both upper and lower case letters are recognized). Text filters ignore diacritics (i.e. accents, glyphs, symbols and other marks added to letters in various languages), and ignore all non-alphanumeric characters (! @ # \$ % & etc.). Multiple search terms can be specified - such as names, phone numbers or specific keywords and phrases - but should be separated by semicolons. At least one of the items must have a match in order to be displayed in the report. If the search terms contain spaces, each word is searched for separately, but all words must be present in a single text value simultaneously.


5.2.1 Filter by time

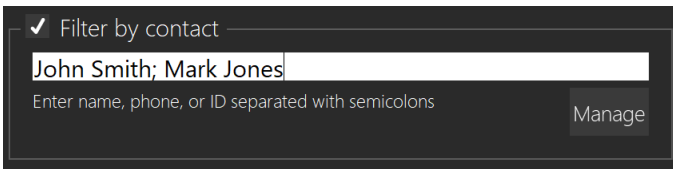
Most sections can be filtered by time. When this filter is enabled, you may enter a time range, and only items that contain a timestamp in this range will be listed in the report. This may be for example the timestamp of a message, the time of a call, a calendar event, the creation or modification time of a file, photo or contact, and others. The time entered is in the time zone of your computer. Unlike other filter types, if you set the Time filter globally, you cannot use a different one locally.



5.2.2 Filter by contact

Some sections and/or the entire report can be filtered by single or multiple contacts. In this context, a name, phone number, email, or another identifier can also be used in the filtered search. When creating the 'Contacts report' as a specific selection, the list of contacts will be exported to the final report and the phone numbers linked to messages and calls will be paired with contact entries. Therefore you can type in a name or another keyword found in the contact information, and items with a reference to this contact will be matched. If you do not create a report for Contacts, you must type in the phone number, name or another identifier directly present in the contact entries you are searching for. The global filter will not affect sections that aren't related to contacts, such as the organizer or file system.

 It is important to search the contact/contact number in the format it is has been saved on the device.



✓ Filter by contact

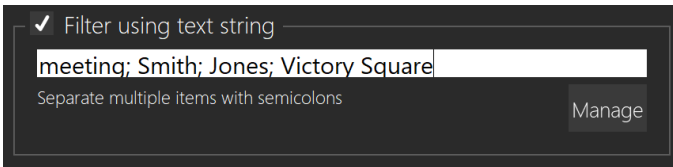
John Smith; Mark Jones

Enter name, phone, or ID separated with semicolons

Manage

5.2.3 Filter using a text string

The global text string filter will find items from any section that contain the specified substring entries.




✓ Filter using text string

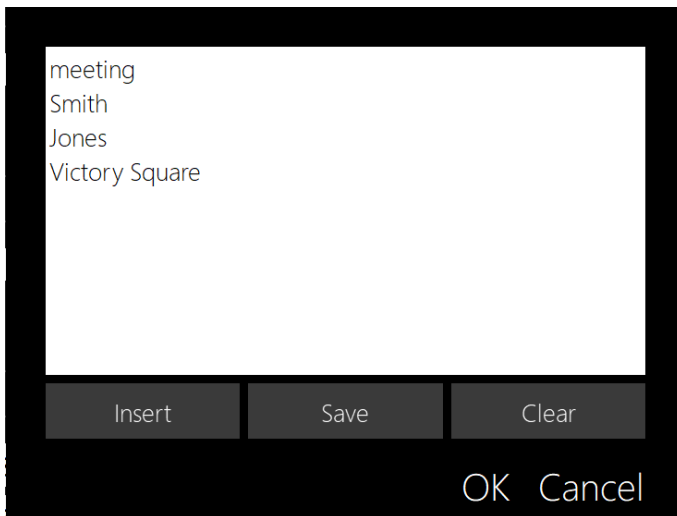
meeting; Smith; Jones; Victory Square

Separate multiple items with semicolons

Manage

For both **contact** and **text string** filters, you can click the manage button which will let you Save and Insert your custom text filters.

 When you click Insert, you are able to import UTF-8 text file where each keyword is in a separate line.



i Keep in mind that to separate multiple items you need to enter every word into another row.

5.2.4 Filter by location

For location info, you can use the location filter, where you can search through your device by typing in the Latitude, Longitude, and the distance from which the, for example, some other photos might've been taken.

! Filtering only applies for reports, exports (i.e. UFDR) will not be affected.

5.3 Full content vs. Specific selection

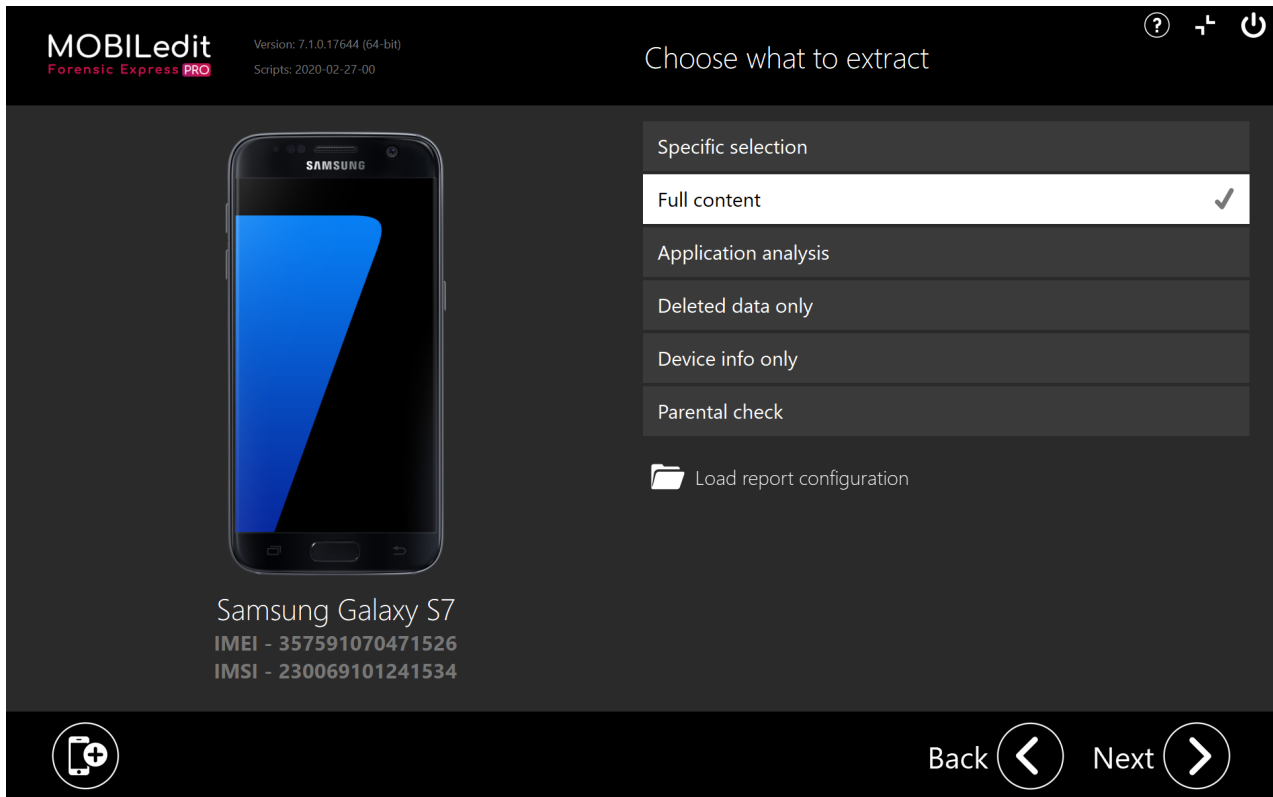
- [Full Content](#)(see page 269)
- [Specific Selection](#)(see page 270)

There are two options you can use to generate your report - **Full content** and **Specific selection**(see page 325).

5.3.1 Full Content

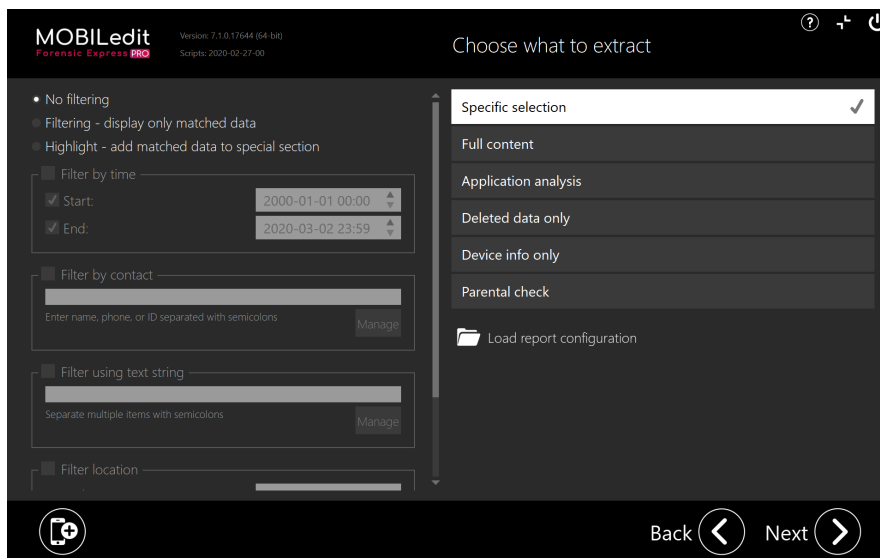
If you choose Full content, all available data will be exported and listed in the report, albeit only once. Some sections, which repeat data in a different form, such as Timeline, will be omitted. All applications will be analyzed, which may take a significant amount of time. The entire report configuration will be skipped. When you generate a

MOBILedit Backup XML with this option, it can fully substitute the physical phone as a source for future reports. For detailed aggregation and more options use the specific selection export.

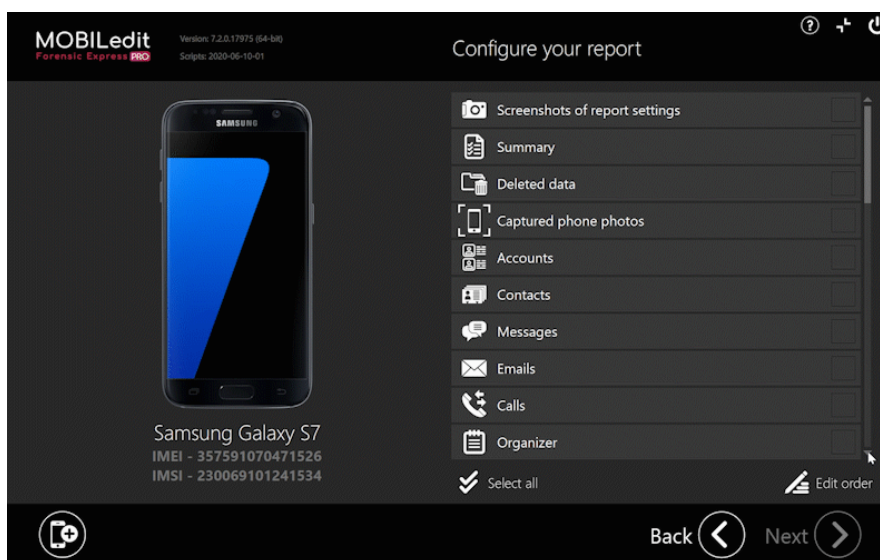


5.3.2 Specific Selection

The Specific selection option allows for a much higher level of control over the contents of the report. With Specific selection, you can configure everything from types of data to extract (contacts, messages, files, applications,...) and applications to include, to the details like what order to list the entries in, or how to display messages or photos. Additionally, it allows you to set up filters and recount all the data in chronological order in the timeline. All of these settings can be configured separately and customized for specific search criteria in each section.

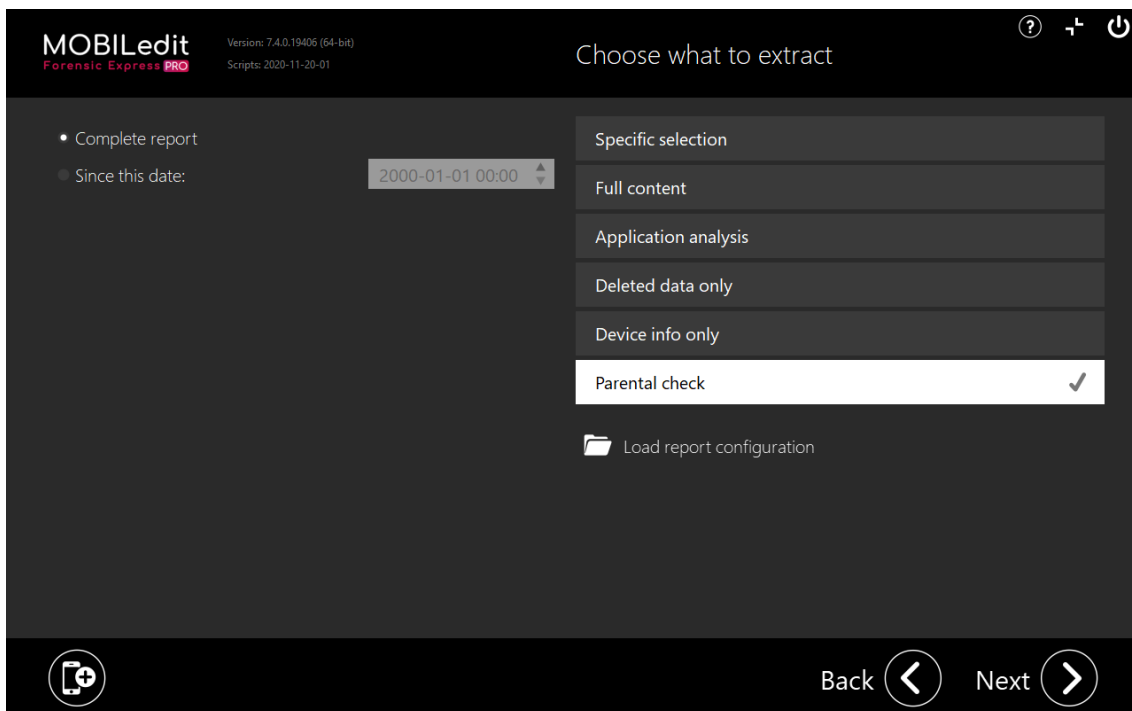


Upon clicking on the Next button you will be asked to select the categories you want to be exported from the phone as seen on the screenshots below. Moreover, additional filters can be set for each such category.



5.4 Parental check

The Parental Check option is a carefully predefined selection for getting the best results. It is optimized for situations when you as a parent want to check your children's phone.



The following data will be exported and listed in the report:

- Contacts
- Messages
- Emails
- Call logs
- Organizer
- Apps
- Images
- Video
- Bookmarks
- Locations
- Notifications
- Passwords
- Web history
- Web search
- Contacts analysis

i If you perform more than one extraction from the same device, only the new and changed or modified data will show up in the report.

5.5 Case details

- [Show data sources](#)(see page 273)
 - [The PDF report](#):(see page 273)
 - [The HTML report](#):(see page 273)
 - [The XLSX report](#):(see page 274)
 - [Clutter filtering](#)(see page 274)
- [Title Page and Header information](#)(see page 274)

To keep track of your cases and extractions you can enter case details, phone details and investigator details on the Case Details page. The case details and the investigator details you will be saved for the next time when you open the program.

Report time zone: Phone time zone (Europe/Pragut)

Report language: Default (english)

Time format: ISO (yyyy-MM-dd hh:mm:ss)

Show data sources: Yes No

Clutter filtering: Yes No

CASE DETAILS:

Case label: Grand theft auto

Case evidence number: 8974969-589

Case evidence details: Stolen 3 cars

Case notes: Audi, Mercedes, Ferrari

Clear Case details

Device label: Valentine's phone

Device name: Samsung Galaxy S7

Device ID: 56547992458

Device evidence number: 6814259-484

Owner name: Richmond Valentine

Owner phone number: +15648875459

Phone notes: Contains a video and pictures of the

INVESTIGATOR DETAILS:

Investigator name: Dexter Morgan

Investigator designation: PCI

Investigator email: morgan@investigations.com

Investigator phone number: +15439568150

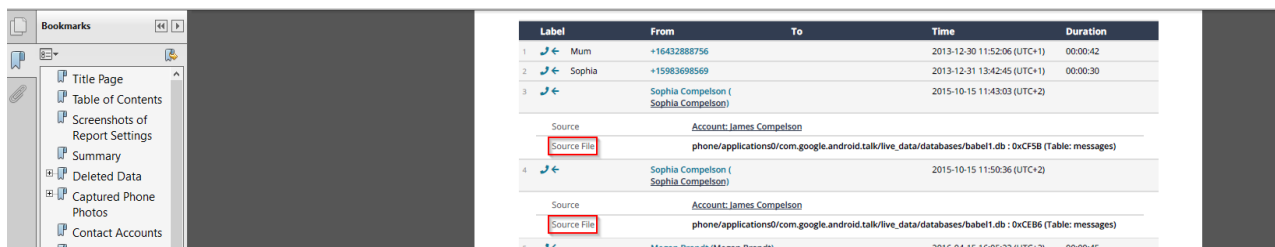
Permission document: All permissions granted

Investigator logo: ...cuments\myinvestigatorlogo.jpg

5.5.1 Show data sources

When this setting is enabled (set as "Yes"), the resulting report will contain information about the data source file. You can see the example of the added data source file in the pictures below.

5.5.1.1 The PDF report:



5.5.1.2 The HTML report:

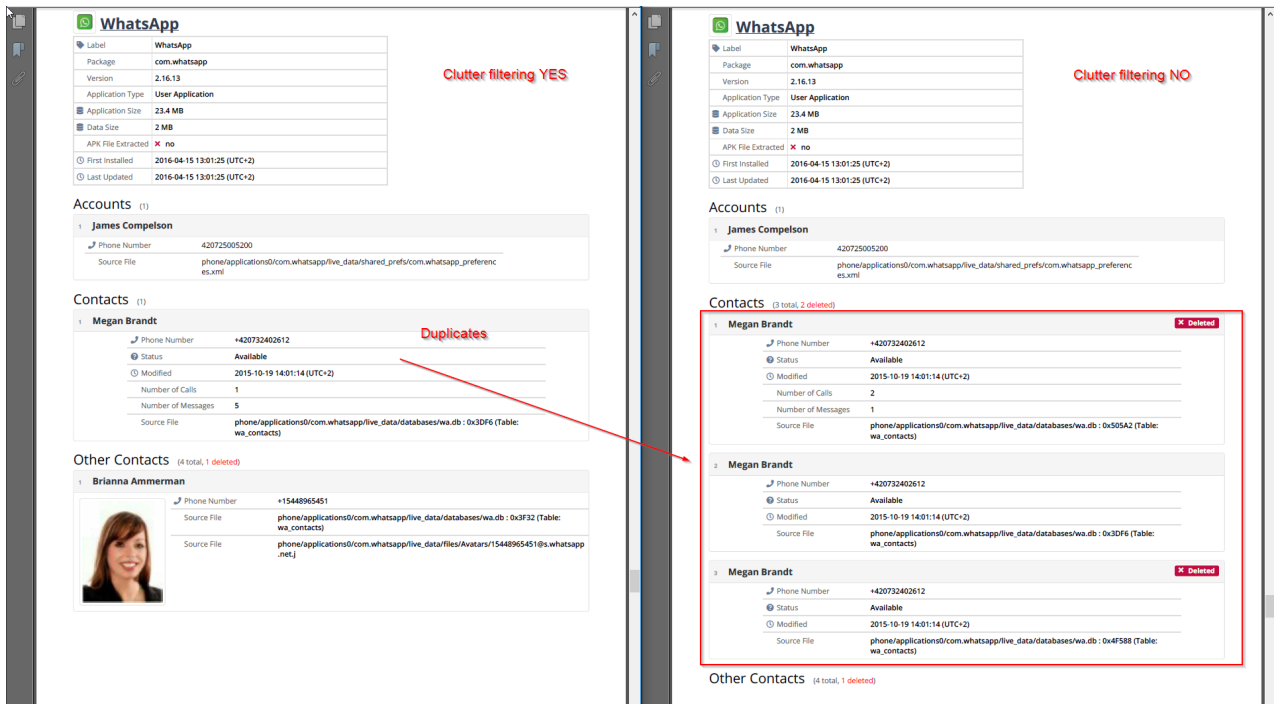


5.5.1.3 The XLSX report:

A	B	C	D	E	F	G	H	I	J	K	L	
1	exf_ID	Label	Deleted	Contact/References	Contact/exf_ID	Phone Number	Is Hangouts User	Type	Account/References	Account/exf_ID	Source File Path	Source File Table
82	_25518	Abdallah Mmenga	no						Facebook	_5732	phone/applications0/com.facebook.katana/live_data/databases/contacts_db2	contacts
83	_25560	Abdullahi Muhammad	no						Facebook	_5740	phone/applications0/com.facebook.katana/live_data/databases/contacts_db2	contacts
84	_25798	Abesid Mohamedi	no						Messenger	_5740	phone/applications0/com.facebook.orca/live_data/databases/threads_db2	thread_users
85	_25583	Abesid Mohamedi	no						Facebook	_5732	phone/applications0/com.facebook.katana/live_data/databases/contacts_db2	contacts
86	_25809	Abidemi Azeez	no						Messenger	_5740	phone/applications0/com.facebook.orca/live_data/databases/threads_db2	thread_users
87	_25594	Abidemi Azeez	no						Facebook	_5732	phone/applications0/com.facebook.katana/live_data/databases/contacts_db2	contacts
88	_25785	Abosedede Oke	no						Messenger	_5740	phone/applications0/com.facebook.orca/live_data/databases/threads_db2	thread_users
89	_25514	Abosedede Oke	no						Facebook	_5732	phone/applications0/com.facebook.katana/live_data/databases/contacts_db2	contacts

5.5.1.4 Clutter filtering

When enabled, the final report does not contain duplicated data and clutter is reduced to a minimum. If set as no, all data records are displayed in the report.



5.5.2 Title Page and Header information

The details you entered will be clearly displayed in the final HTML/PDF report. On the Title Page, you will see the Case Label name, Case Evidence number and Case Evidence Notes will be displayed in the upper-right section of the page. Below this information on the Title Page will be the Device Information. On the bottom of the Title Page, you will find the Investigator Information such as investigator name, investigator logo, email, phone number and permission document.

In the header of each page of the PDF report, you will find the Case Label, the Case evidence number and the Device label.



FORENSIC EXPRESS PHONE CONTENT REPORT

Grand theft auto

Case Evidence Number: **8974969-589**




Manufacturer Samsung
Product Galaxy S7
HW Revision NRD90M
Platform Android
SW Revision 7.0 (24)
Serial Number 9885e8343491523350
Adb Backup Password 1234
Unlocking Pattern 6304258
IMEI 357591070471526
Rooted No
SIM Card Yes
Owner Phone Number +15648875459
Operator O2-CZ, MCC: 230, MNC: 2

Case Information	
Case Label	Grand theft auto
Case Evidence Number	8974969-589
Case Evidence Details	Stolen 3 cars

Audi, Mercedes, Ferrari

Device Information	
Device Label	Valentine's phone
Device Name	Samsung Galaxy S7
Device ID	56547992458
Device Evidence Number	6814259-484
Owner Name	Richmond Valentine
Owner Phone Number	+15648875459
Phone Notes	Contains a video and pictures of theft

Investigator Information	
	
Investigator Name	Dexter Morgan
Investigator Designation	PCI
Investigator Email	morgan@investigations.com
Investigator Phone Number	+15439568150
Permission Document	All permissions granted

Extraction Information	
Data Extraction Started	2018-03-22 13:12:20 (UTC+1)
Data Extraction Finished	2018-03-22 13:13:08 (UTC+1)
Extracted by	Phone Forensics Express 2.6.0.3935
Report Generated by	MOBILedit Forensic Express PRO 7.1.0.17644
Applications Analyzed by	AppEngine 2020-02-27-00

Device Properties	
Manufacturer	Samsung
Product	Galaxy S7
HW Revision	NRD90M
Platform	Android
SW Revision	7.0 (24)
Serial Number	9885e8343491523350
Adb Backup Password	1234
Unlocking Pattern	6304258
Device Time	2018-03-22 12:24:28 (UTC+1)
Manual Time	No
Time Zone	Europe/Prague
Manual Time Zone	No
IMEI	357591070471526
LACCID	LAC: 1133, CID: 203698066
Wi-Fi MAC Address	AC:3F:3E:18:32:C4
Bluetooth Address	A4:84:31:25:91:5C
Rooted	No
SIM Card	Yes
IMSI	230069101241534
SIM Card Country	Czech Rep.
ICCID	8942020187302690297
Owner Phone Number	+15648875459
Operator	O2-CZ, MCC: 230, MNC: 2

5.6 Local filters

Local filters are filters used in [Specific selection](#)(see page 325) - unlike the [Global filters](#)(see page 266), they only apply to specific content.

Using local filters, you can filter most of the parameters related to the data you selected, such as:

- order (ascending or descending)
- time
- location
- name
- path

and sort by:

- filename
- fullpath
- time
- content




Keep in mind that if you will sort, for example, the messages by content: "**Hi**" you will get even words that have the word Hi in them... for example a word: **this**

Local filters are applied to the data which you choose in Specific selection:

- contacts
- messages
- emails
- calls
- organizer
- applications
- photo recognizer

- face matcher
- photos
- image files
- large images
- audio files
- video files
- documents
- filesystems
- contact analysis
- GPS locations
- web
- timeline

 If you select a local filter, it will be always prioritized against [global filters](#)(see page 266) (i.e. if you choose a specific date in the global filter and different date in the local filter, both will be shown in the report)

5.7 How to make reports smaller

- [Filtering](#)(see page 277)
- [PDF Splitting](#)(see page 277)
- [Clutter filtering](#)(see page 277)
- [Source of data](#)(see page 277)

This article contains some tips for you on how to reduce the size of the PDF reports with MOBILedit Forensic Express.

5.7.1 Filtering

This feature allows you to trim down the report data by selecting the exact time interval or a contact name and a text string. More information is available [here](#)(see page 266).

5.7.2 PDF Splitting

Brings you the option for easier manipulation with files. Each file is named by the data contained therein. Read more about the PDF report [here](#)(see page 292).

5.7.3 Clutter filtering

Enabling Clutter filtering will allow you to report less content and the report with therefore be only as large as is needed. Clutter filtering helps you with cleaning and removing duplicate data and other clutter. Details are available [here](#)(see page 272).

5.7.4 Source of data

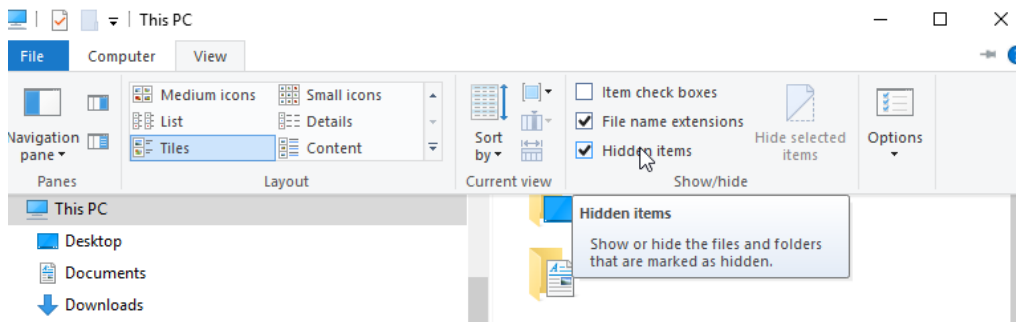
Disabling the Source of data information will allow you to report less content and the report with therefore be only as large as is needed. The Source of data gives you the exact path and filename to the source file. Details are available [here](#)(see page 272).

5.8 Report customization

You can create your own report customization and language translations. A template file for your own report language translation is located at:

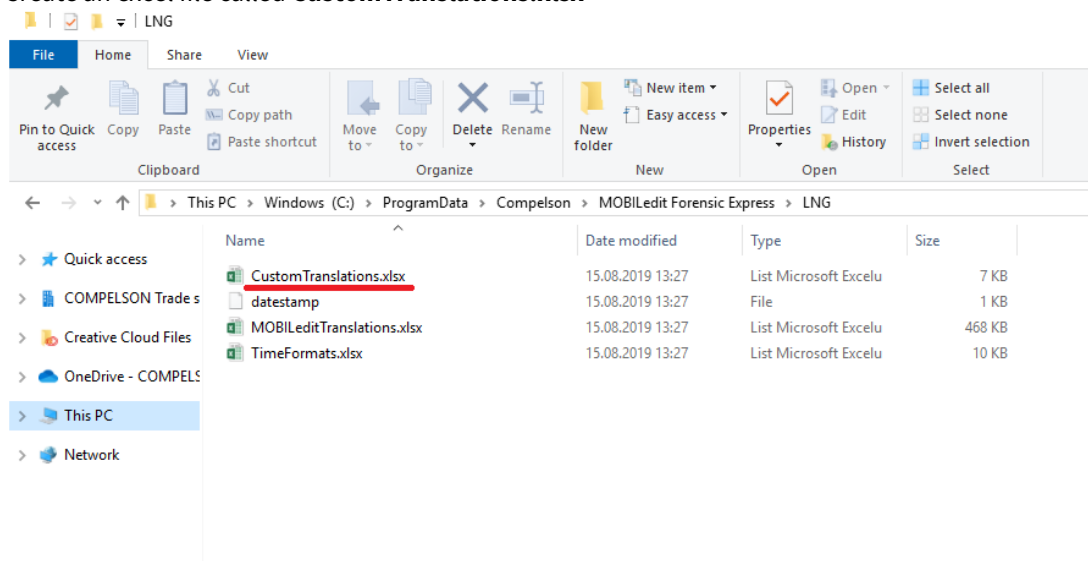
C:\ProgramData\Compelson\MOBILedit Forensic Express\LNG

Folder "**ProgramData**" is hidden, so you might need to enable viewing of the hidden files first.



5.8.1 Creating custom translation


1. Navigate to the folder with MOBILedit languages (path to the needed folder: **C:\ProgramData\Compelson\MOBILedit Forensic Express\LNG**).
2. Create an excel file called **CustomTranslations.xlsx**

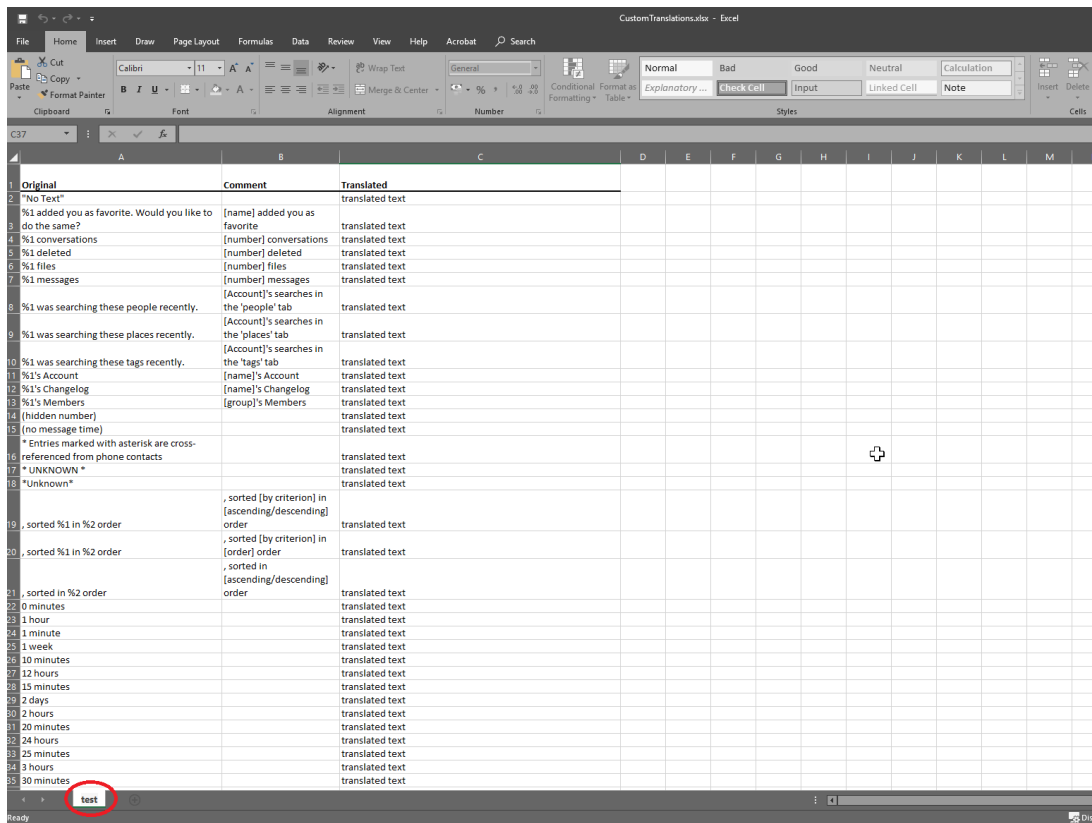


3. Access the **MOBILeditTranslations.xlsx**
4. Copy everything that is in the "Template" sheet.

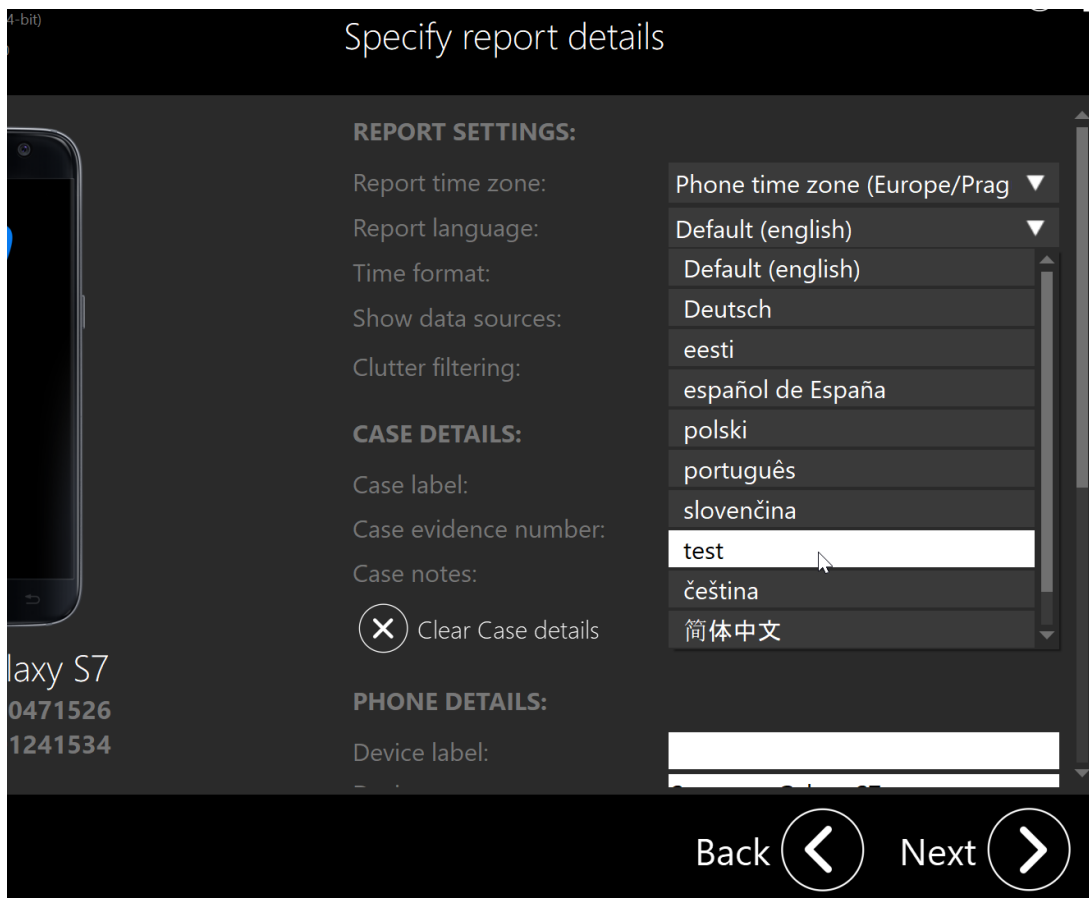
	A	B	C
	Original	Comment	Translated
1			
2	"No Text"		
3	%1 added you as favorite. Would you like to do the same?	[name] added you as favorite	
4	%1 conversations	[number] conversations	
5	%1 deleted	[number] deleted	
6	%1 files	[number] files	
7	%1 messages	[number] messages	
8	%1 was searching these people recently.	[Account]'s searches in the 'people' tab	
9	%1 was searching these places recently.	[Account]'s searches in the 'places' tab	
10	%1 was searching these tags recently.	[Account]'s searches in the 'tags' tab	
11	%1's Account	[name]'s Account	
12	%1's Changelog	[name]'s Changelog	
13	%1's Members	[group]'s Members	
14	(hidden number)		
15	(no message time)		
16	* Entries marked with asterisk are cross-referenced from phone contacts		
17	* UNKNOWN *		
18	*Unknown*		
19	, sorted %1 in %2 order	, sorted [by criterion] in [ascending/descending] order	
20	, sorted %1 in %2 order	, sorted [by criterion] in [order] order	
21	, sorted in %2 order	, sorted in [ascending/descending] order	
22	0 minutes		
23	1 hour		
24	1 minute		
25	1 week		
26	10 minutes		
27	12 hours		
28	15 minutes		
29	2 days		
30	2 hours		
31	20 minutes		
32	24 hours		
33	25 minutes		
34	3 hours		
35	30 minutes		
36	45 minutes		
37	5 minutes		

5. Open the **CustomTranslations.xlsx** and paste the copied template sheet.
6. Now you need to do is just put the translated words into the "Translated" column.
7. Rename the template sheet to whatever you would like to see it in the program (e.g. "test").

 You can also use shortcuts like fr, h, ru, etc. Our software then displays these shortcuts as Français, Magyar, Русский.



8. Save it, restart MEFE and now you should be able to see the translated text.



i You can, of course, have multiple custom translations in the CustomTranslations.xlsx

We will be grateful if when you create any new language translation that you would be so kind as to send it to us, so we can make it a part of our software and it will be available to other users. So you can become a part of our supporters group. Do not hesitate to [contact us](http://www.mobiledit.com/contact/)⁸¹ if you need more support.

i If you want your translation to be featured in Forensic Express please send it to us for validation. If approved, it will be made public with the release of the next version of our product.

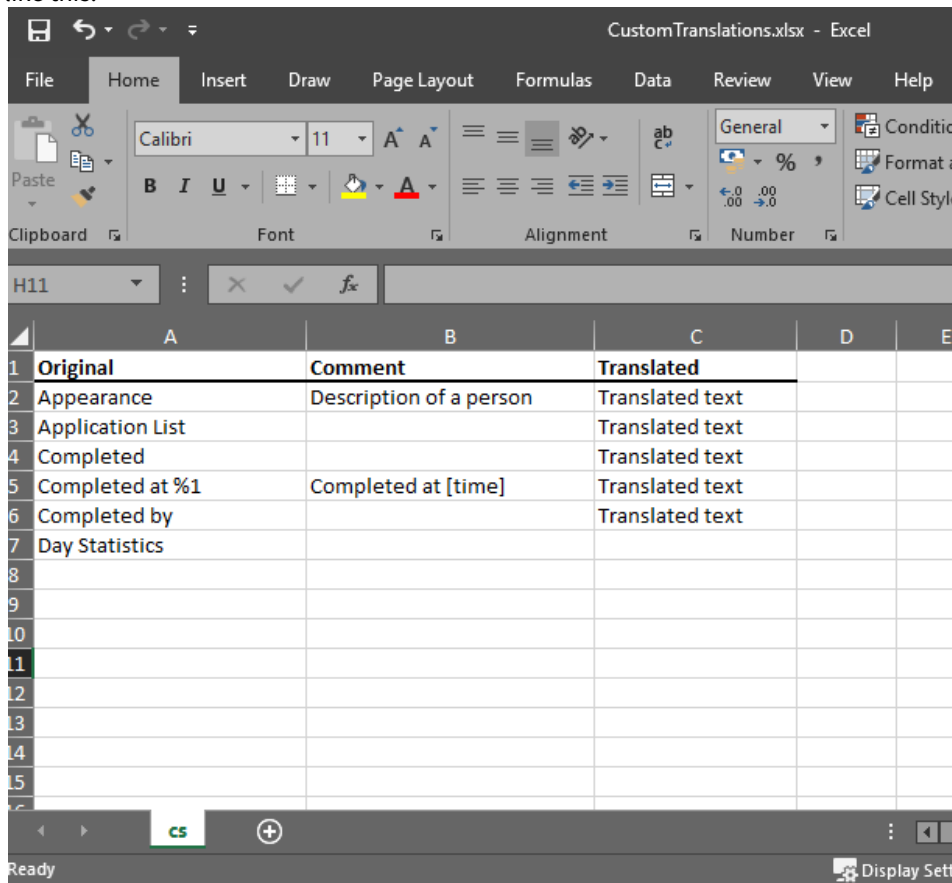
5.8.2 Editing text which is already in MOBILedit Forensic express


If you want to edit some language which we have already created, then:

1. navigate to the folder with languages (C:\ProgramData\Compelson\MOBILedit Forensic Express\LNG)
2. create an excel file called CustomTranslations.xlsx
3. access the MOBILeditTranslations.xlsx
4. Copy the words you want to edit, keep in mind that the first line should always contain **Original; Comment; Translated**, as seen in the picture below.
5. Open the CustomTranslations.xlsx and paste the copied words.

⁸¹ <http://www.mobiledit.com/contact/>

6. Put the translated text in the translated column.
7. Rename the template sheet to whatever language you would like to edit (e.g. cs). The final result should look like this:

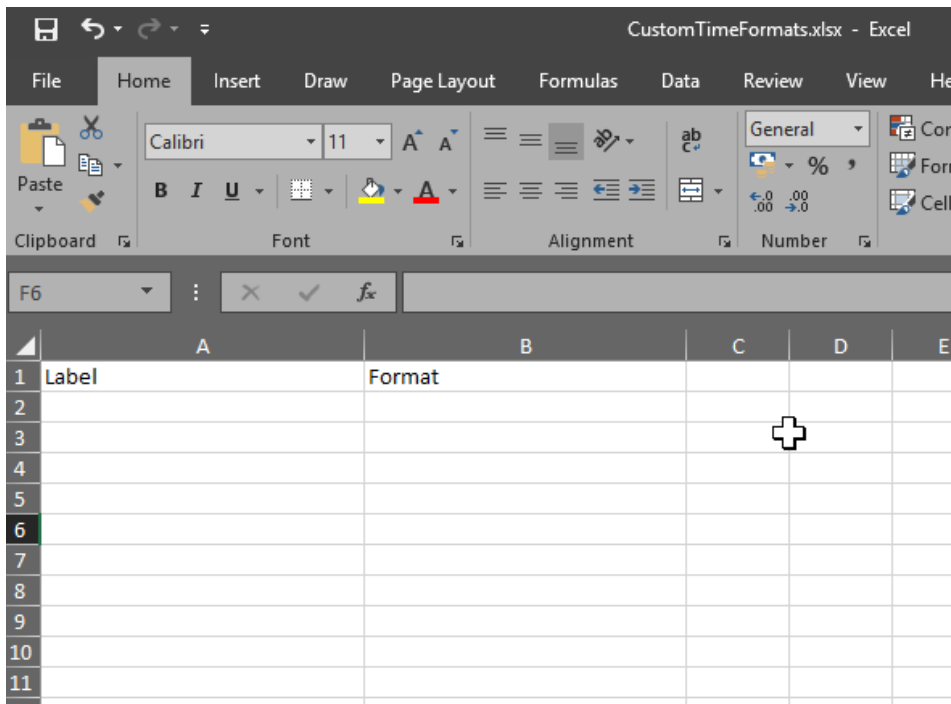


 The sheet must have the same name as in the MOBILeditTranslations.xlsx

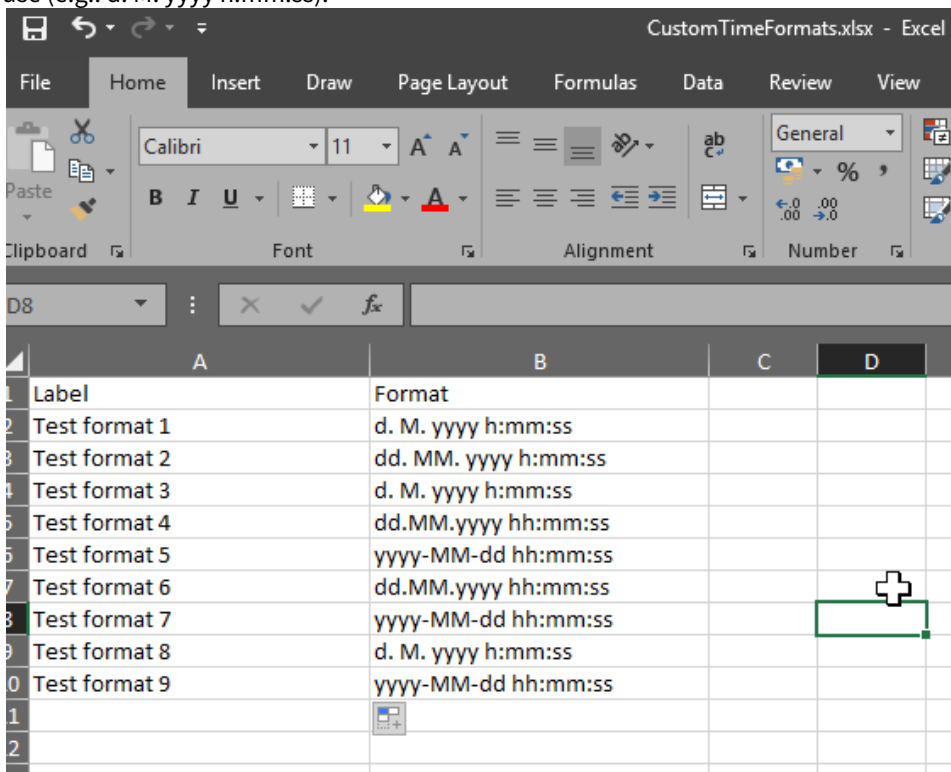
8. Save it restart MEFE and now you have successfully edited the desired word(s).

5.8.3 Editing time formats

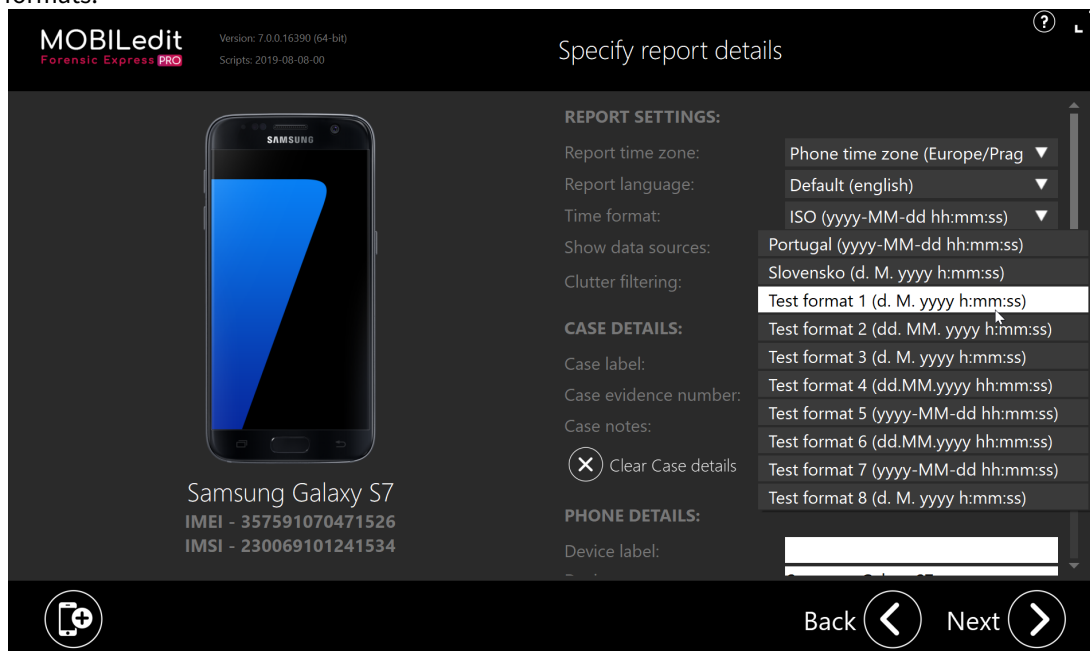
1. Navigate to: **C:\ProgramData\Compelson\MOBILedit Forensic Express\LNG**
2. Create an excel folder called **CustomTimeFormats.xlsx**
3. Open the folder and in the first-line type: **Label** and **Format**



4. Type **names** in the "Label" column (e.g.: Test format 1), and in the "Format" column the **format** you want to use (e.g.: d. M. yyyy h:mm:ss).



5. Save it, restart MOBILedit forensic express and now you should be able to see the added custom time formats.

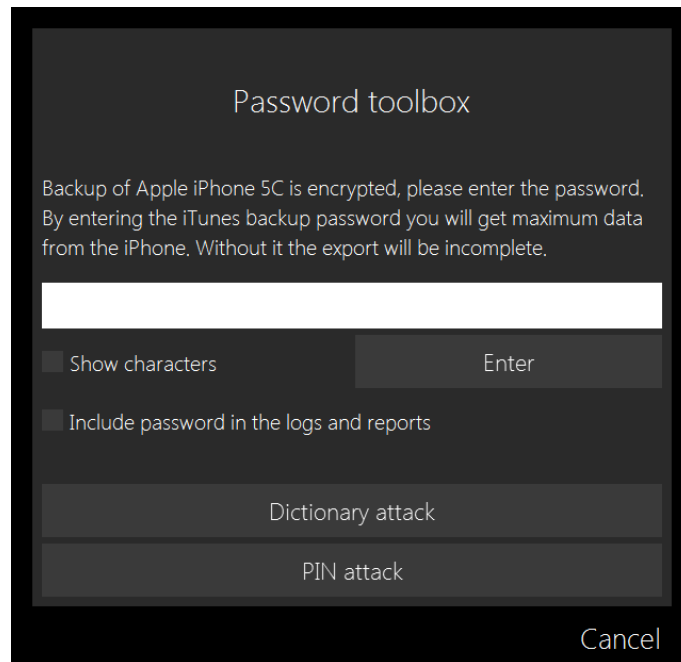


5.9 Backup password breaking

- [Entering password directly](#)(see page 285)
- [Dictionary attack](#)(see page 285)
- [PIN attack](#)(see page 287)


MOBILedit Forensic Express allows you to extract iTunes backups from iOS devices in addition to ADB backups from Android devices. You can even load historical backups that have been created previously for detailed analysis or comparison.

It is not uncommon to find backups that are protected with some form of password or a code. In order to analyze such backup, the password must be obtained to gain access. There are multiple tools and methods that are offered in the software that will save a significant amount of time for investigators.



5.9.1 Entering password directly

The password can be entered directly if it was obtained during an investigation or through other means. There is an unrestricted number of attempts allowed to enter the password, so you can't get permanently locked out. You can also see a history of the previously entered unsuccessful passwords.

 You can choose to include a password into the logs and reports.

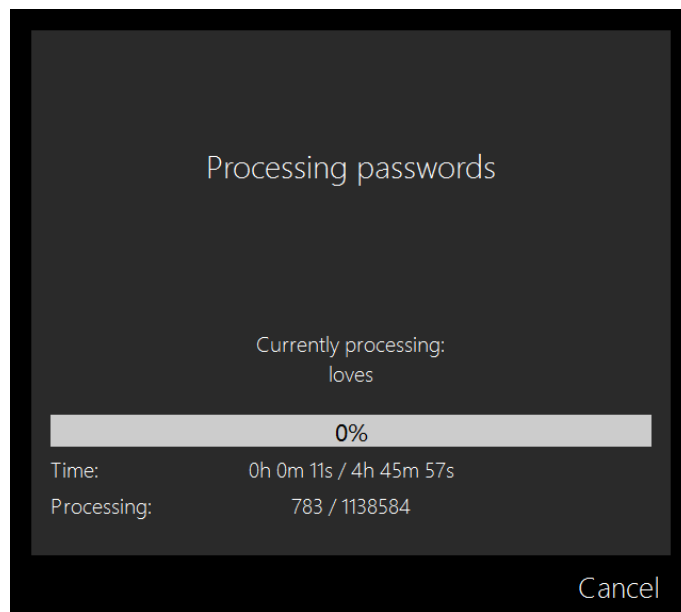
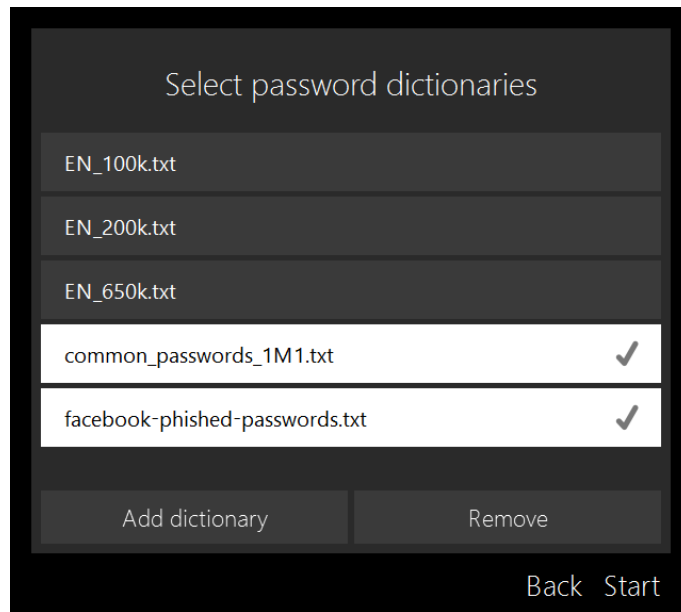
5.9.2 Dictionary attack

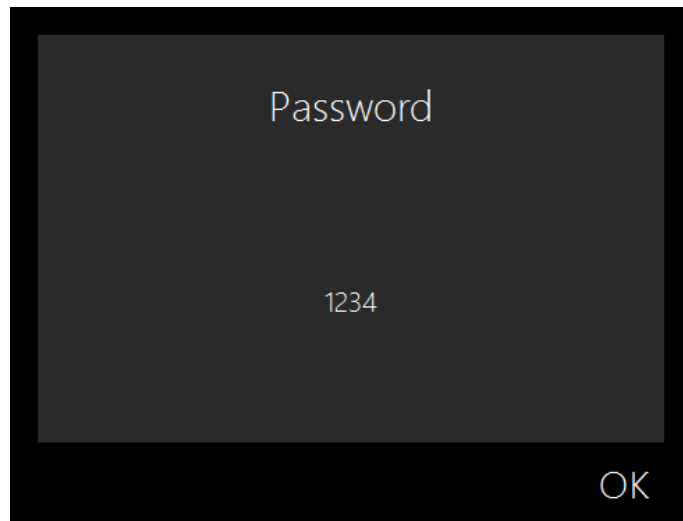
Dictionary attacks simply go through a list of supplied strings and try to enter them as the password. An investigator can either use one of our supplied dictionaries or use his or her own dictionary. Our product ships with the following dictionaries:

1. EN_100k.txt - english dictionary containing 100 thousand words.
2. EN_200k.txt - english dictionary containing 200 thousand words.
3. EN_650k.txt - english dictionary containing 650 thousand words.
4. common_passwords_1M1.txt - file containing 1.1 million of the most commonly used passwords.

In order to add your own dictionary just provide path to a text file after clicking "Add dictionary". All dictionaries must contain words separated by a newline.

Multiple dictionaries can be used in a single Dictionary attack.

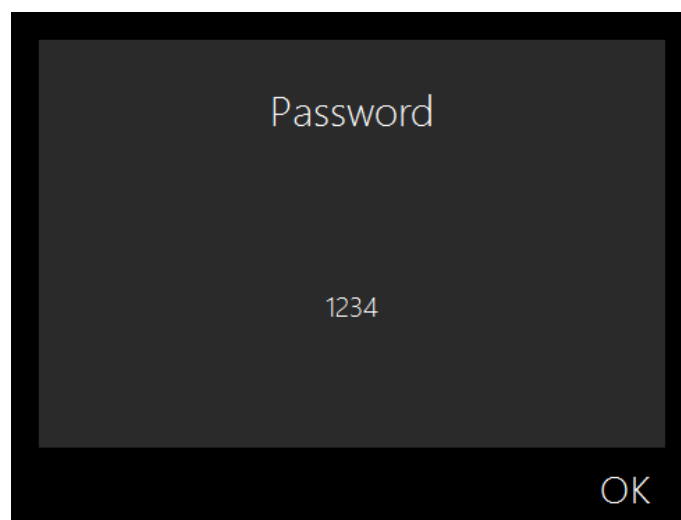
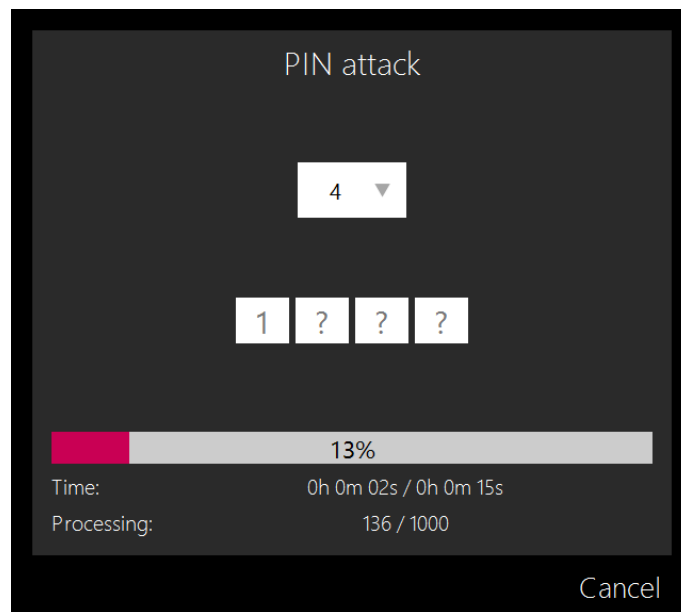




5.9.3 PIN attack

PIN attack assumes that the password contains digits exclusively. Password length is chosen and some digits can be entered manually if they are known.



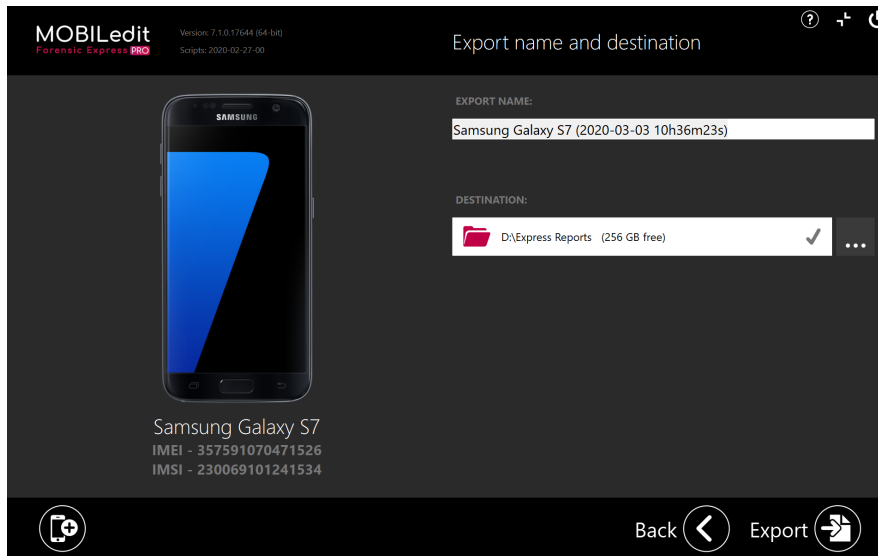


5.10 Output folders structure

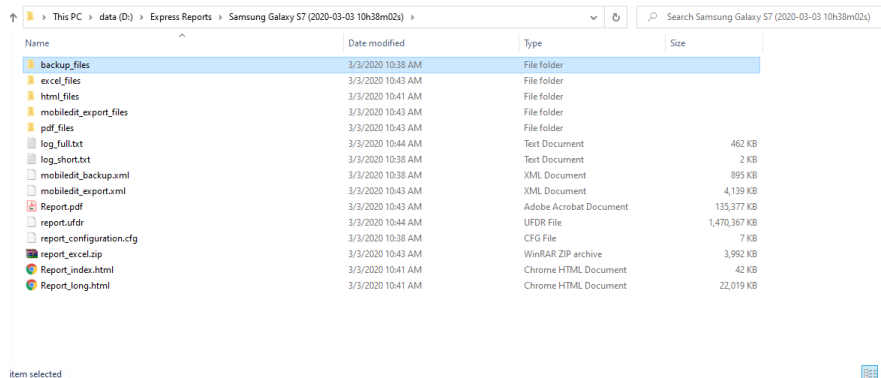
- [HTML Report](#)(see page 289)
- [PDF Reports](#)(see page 289)
- [MS Excel Report](#)(see page 290)
- [MOBILedit Backup](#)(see page 290)
- [MOBILedit Export](#)(see page 290)
- [Report subfolder "Phone"](#)(see page 290)
- [Additional backup folders – iTunes, ADB, and iCloud](#)(see page 291)
- [Logs and other files](#)(see page 291)
- [Files and long folder paths](#)(see page 291)

All results of the data extraction and analysis are contained in one folder, which is the base folder of all the reports and exports. By default, this folder has a name consisting of the phone name, the date and time when the

processing started, such as Samsung Galaxy S7 (2020-03-03 10h36m23s). You can change the export name and the destination folder if you need to.



Contents of the folder mainly depend on which output formats have been selected, plus there are a few files that are related to the extraction and analysis in general.



5.10.1 HTML Report

HTML reports are saved in two ways – one is the whole report stored in one file, **Report_long.html**, and the other one is the full report divided into multiple files (one file per main report section) and the index to the whole report is **Report_index.html**. The reason for this distinction is that the reports might be too big to open in some browsers.

All of the images and linked files (which also means all files extracted from the phone, for a given report) are stored in the folder **html_files**. This folder belongs to the HTML reports and, if copied, all of these folders and files should be kept together. It will help you in case you need to make a copy of the specific report.

5.10.2 PDF Reports

The PDF report is similar to the HTML report – in fact, it is generated from a special version of the HTML file – and the name of the report is **Report.pdf**. In this report, all images are stored inside of the PDF, in a suitable resolution so the PDF file itself can be used for distribution of the report, but there are links from the PDF to additional content

stored in the folder named **pdf_files**, such as all the extracted files (application databases and the like) and also the images in their original resolution.

When the resulting pdf report file might be too large causing the pdf generation phase could fail, it is better to use the **PDF Report – Multiple Files** options, which generates multiple PDF files, one per each report section. The files start with numbers such as 01_Screenshots_of_User_Settings.pdf, 02_Summary.pdf, etc., and all the pdf files are again linked to the **pdf_files** folder.

5.10.3 MS Excel Report

This report format generates multiple files divided by the content of the phone, saved as a .XLSX document (for this you need to have MS Excel installed on your PC). There is no folder related to this format as no additional files are saved during the report, and if you need the related files they have to be taken from the other report folders. The file names have the format such as **xlsReport.xlsx** and **xlsReport_SIM Card.xlsx**.

5.10.4 MOBILedit Backup

MOBILedit Backup is the format that stores all the information that has been extracted from the phone, and that can be opened later to create additional reports, either with different options and parameters or in a newer version of Forensic Express with improved features such as enhanced recovery of deleted data. The file name is **backup.mobiledit**, all related files are stored in the folder **backup_files**, and to open the backup use the option **Open file** in the main window (when you press Start after launching the application.)

5.10.5 MOBILedit Export

This export format contains all analyzed information from the phone, including data from applications and the recovered deleted data, its file name is **export.mobiledit** and the related folder with files is **mobiledit_export_files**.

5.10.6 Report subfolder "Phone"

This subfolder is similar for the mentioned folders above and it contains subfolders:

Name	Content
application0	applications and their data, not user shared galleries
application1	special content, logs from apps or content providers
raw0	the whole phone file system
raw3	file system which is shared with apps, for example, images, music, downloads, user galleries
misc	temporary files, icons, thumbnails, contacts pictures, message attachments

You might need this information in case you want to browse the extracted data (image, audio, and video files) without opening the report. It also might include little differences based on the phone you were extracting (Android or iOS).

5.10.7 Additional backup folders – iTunes, ADB, and iCloud

If you specify that you want an Android (ADB) backup or iTunes backup, then these additional phone backups are stored in the output folder as well, in subfolders named `adb_backup` and `apple_backup`, respectively. These separate backups can be opened too, using the Open file option. ADB backup is also typically created when any application data are needed, and iTunes backup (which contains lots of useful information) is used for most of the operations with an iPhone or an iPad.

If you are using the iCloud analyzer, then downloaded iCloud backups are stored in a subfolder named `icloud_backups`.

5.10.8 Logs and other files

There are three specific files in the report folder.

File **log_full.txt** contains all information that was presented on the screen in the white log window, together with all files copied from the phone, and if the password breaker has been used then it contains the resultant password as well.

In the **log_short.txt** there is summary info of the extraction phase, together with a list of failed items indicating what might be missing in the report, such as skipped folders. The contents of this file are also included in the HTML and pdf reports in the Data Extraction Log section.

File **report_configuration.cfg** contains all parameters of the whole report, and if you need to create the same report from a different phone you can load this configuration file using the **Load report configuration** at the start of the report.

5.10.9 Files and long folder paths

All the files in the report subfolders are stored in a tree structure that is based on the original data in the phone, so advanced users might be able to get any files for additional analysis or any other purpose.

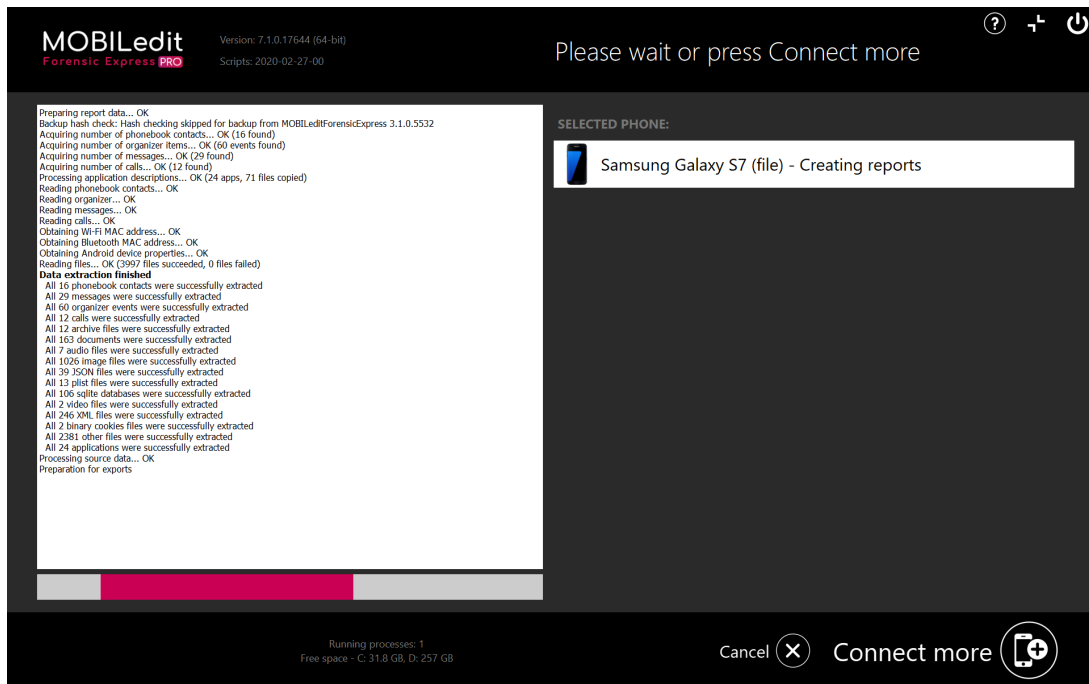
When copying the subfolders (or the whole report folder) please be aware that the full paths might be longer than the usual limit of 255 characters still present in the Windows shell. It means that while the file system supports paths as long as 32000 characters (and this is true for many older versions of MS Windows), the standard copy/paste or drag and drop file operation will not work well with these folders. In Windows 10 it seems to be finally addressed, and in other cases, you might use either a third-party file manager (such as Total Commander), or a zip/archive file manager that can handle these long paths.

5.11 Running extraction

When running an extraction, on the left side of your screen you will see a log that will be saved in the results dictionary as `log_full.txt`. On the right side, you will see the connected device. If you are extracting from more than one device at a time you can toggle between them by clicking on the specific device.

You can return to the [Device connection screen](#) (see page 112) by clicking the button at the bottom right corner. Your current extractions will remain running in the background and you will then be able to begin extractions from additional devices.

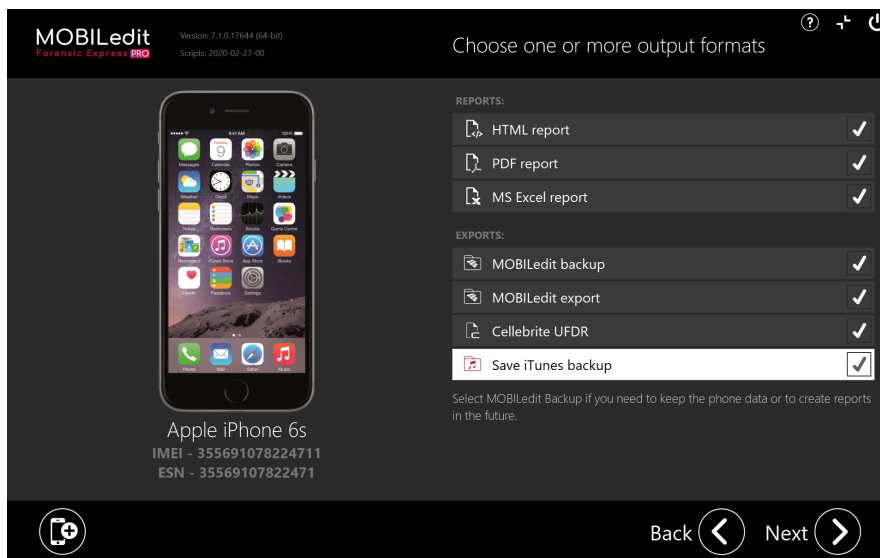
When an extraction is running you can cancel it by clicking the Cancel button. After the extraction, the Cancel button will be replaced with the View results button, which will open the directory with all your selected [backups](#), [exports](#), and [reports](#)(see page 292).



5.12 Outputs - reports, exports, and backups

- [HTML Report](#)(see page 293)
 - [Report_long.html](#)(see page 293)
 - [Report_index.html](#)(see page 294)
- [PDF Report](#)(see page 295)
 - [Single file](#)(see page 295)
 - [Multiple files](#)(see page 296)
- [MS Excel report](#)(see page 296)
- [Export & backups](#)(see page 297)
 - [MOBILedit Backup](#)(see page 297)
 - [MOBILedit Export](#)(see page 298)
 - [Cellebrite UFDR](#)(see page 298)
 - [ADB and iTunes backups](#)(see page 299)

Create multiple formats of reports and exports after extracting data from a phone, each customizable to your specific needs. To continue you must select at least one format. More information about the structure of each file format can be found in the following section - Reports in detail.



All report formats are human-readable and can be opened using supported web browsers, PDF viewers, and Microsoft Office applications.

5.12.1 HTML Report

An HTML report format can be opened using your web browser (we recommend using Google Chrome, Mozilla Firefox, Microsoft Edge, or Internet Explorer 11). This format does not include a full backup of phone data - to create a full backup please use the MOBILedit Backup export format as well.

i This option will automatically generate two HTML files into the export folder.

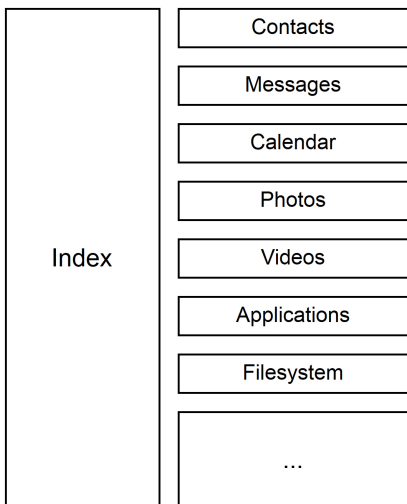
5.12.1.1 Report_long.html

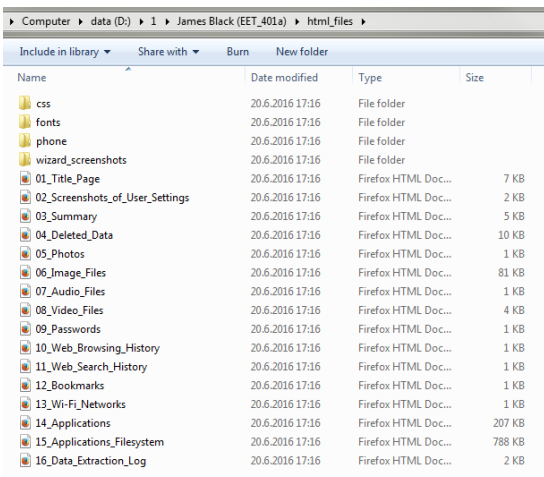
- the full HTML report file with all content
- please note that this file can be large (100MB and more), therefore web browsers may have problems opening or viewing the file if such a large amount of data was extracted from the phone - if you experience problems while opening the HTML file, use the *Report_index.html* file instead



5.12.1.2 Report_index.html

- HTML report split into multiple HTML files based on sections





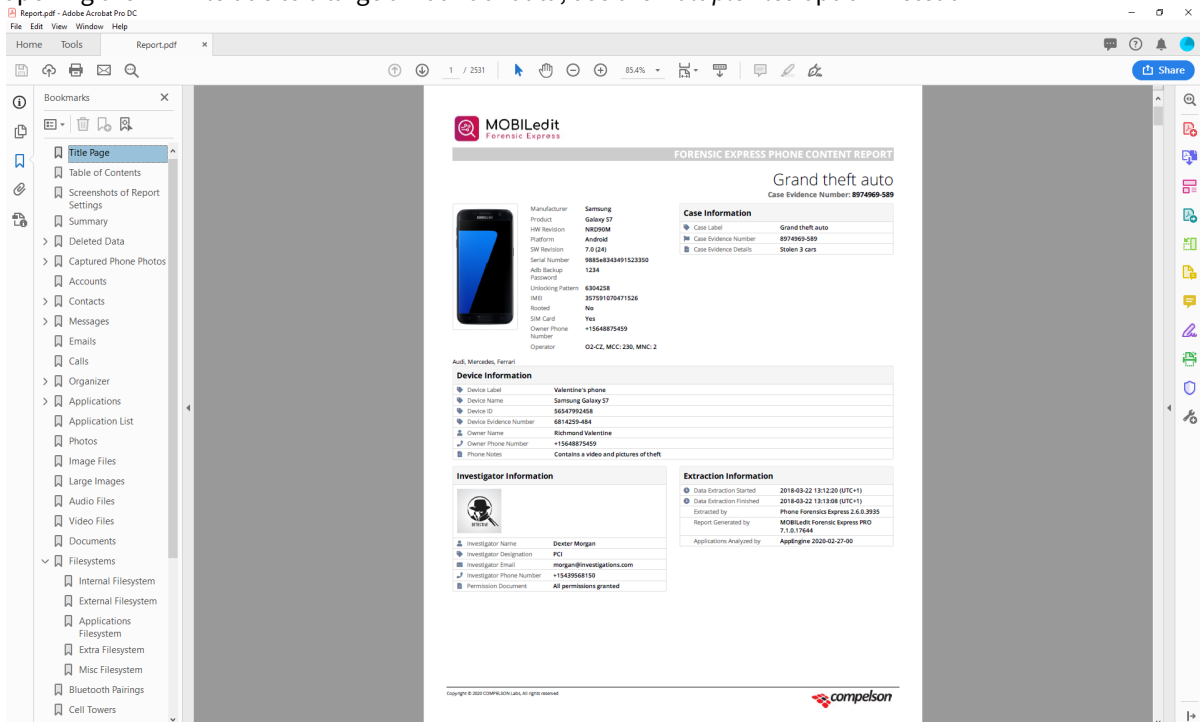
5.12.2 PDF Report

PDF report format can be opened using your PDF viewer or editor (we recommend using Adobe Acrobat or Adobe Reader).

You can choose from two types of PDF reports - Single File or Multiple Files. Your selection will be automatically generated in the export folder:

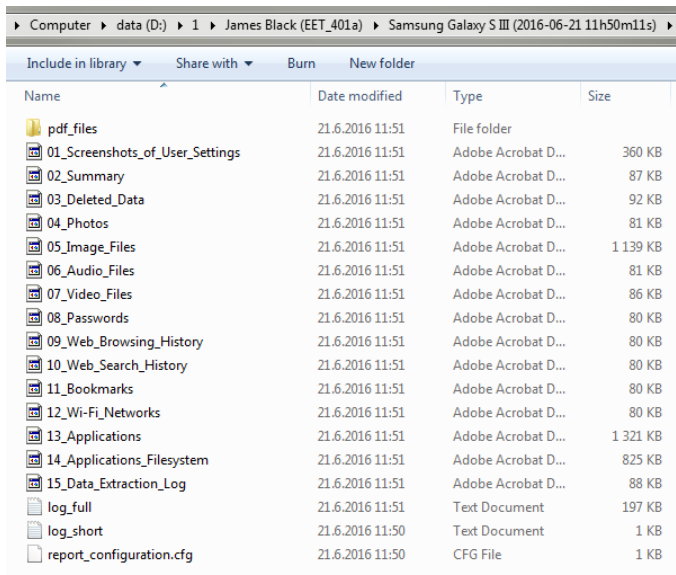
5.12.2.1 Single file

- contains the full PDF report file with all extracted content
- please note that this file can be large (1GB and more), if you experience problems while generating or opening the PDF file due to a large amount of data, use the *Multiple files* option instead



5.12.2.2 Multiple files

- The PDF report is split into multiple PDF files based on sections



Name	Date modified	Type	Size
pdf_files	21.6.2016 11:51	File folder	
01_Screenshots_of_User_Settings	21.6.2016 11:51	Adobe Acrobat D...	360 KB
02_Summary	21.6.2016 11:51	Adobe Acrobat D...	87 KB
03_Deleted_Data	21.6.2016 11:51	Adobe Acrobat D...	92 KB
04_Photos	21.6.2016 11:51	Adobe Acrobat D...	81 KB
05_Image_Files	21.6.2016 11:51	Adobe Acrobat D...	1 139 KB
06_Audio_Files	21.6.2016 11:51	Adobe Acrobat D...	81 KB
07_Video_Files	21.6.2016 11:51	Adobe Acrobat D...	86 KB
08_Passwords	21.6.2016 11:51	Adobe Acrobat D...	80 KB
09_Web_Browsing_History	21.6.2016 11:51	Adobe Acrobat D...	80 KB
10_Web_Search_History	21.6.2016 11:51	Adobe Acrobat D...	80 KB
11_Bookmarks	21.6.2016 11:51	Adobe Acrobat D...	80 KB
12_Wi-Fi_Networks	21.6.2016 11:51	Adobe Acrobat D...	80 KB
13_Applications	21.6.2016 11:51	Adobe Acrobat D...	1 321 KB
14_Applications_FileSystem	21.6.2016 11:51	Adobe Acrobat D...	825 KB
15_Data_Extraction_Log	21.6.2016 11:51	Adobe Acrobat D...	88 KB
log_full	21.6.2016 11:51	Text Document	197 KB
log_short	21.6.2016 11:50	Text Document	1 KB
report_configuration.cfg	21.6.2016 11:50	CFG File	1 KB

Please note that in case the single PDF file is about to be really big, it will be automatically split into multiple files to prevent loading issues and also to ensure the faster creation of the reports. This will typically happen when the extracted device contains a lot of photos or videos (media files in general).

5.12.3 MS Excel report

MS Excel report can be opened using the Microsoft Excel application (we recommend using Microsoft Excel 2010 or newer).

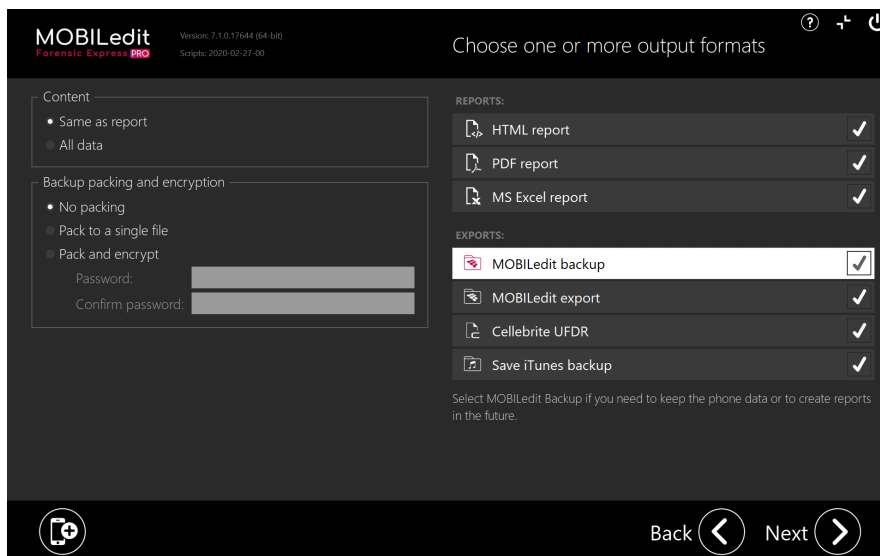
Name	Date modified	Type	Size
log_full	21.6.2016 14:27	Text Document	6 706 KB
log_short	21.6.2016 14:06	Text Document	2 KB
report_configuration.cfg	21.6.2016 13:50	CFG File	7 KB
xls_HTC_One_M9	21.6.2016 14:16	Microsoft Excel W...	3 126 KB
xls_HTC_One_M9_Applications_Google_...	21.6.2016 14:17	Microsoft Excel W...	10 KB
xls_HTC_One_M9_Applications_Google_...	21.6.2016 14:17	Microsoft Excel W...	12 KB
xls_HTC_One_M9_Applications_Google_...	21.6.2016 14:17	Microsoft Excel W...	10 KB
xls_HTC_One_M9_Applications_HTC_Sen...	21.6.2016 14:17	Microsoft Excel W...	10 KB
xls_HTC_One_M9_Applications_Instagram	21.6.2016 14:17	Microsoft Excel W...	10 KB
xls_HTC_One_M9_Applications_Internet	21.6.2016 14:17	Microsoft Excel W...	14 KB
xls_HTC_One_M9_Applications_Mapy_cz	21.6.2016 14:26	Microsoft Excel W...	10 KB
xls_HTC_One_M9_Applications_Meteor	21.6.2016 14:26	Microsoft Excel W...	10 KB
xls_HTC_One_M9_Applications_OneDrive...	21.6.2016 14:26	Microsoft Excel W...	11 KB
xls_HTC_One_M9_Applications_SplenDO	21.6.2016 14:26	Microsoft Excel W...	20 KB
xls_HTC_One_M9_Applications_Viber	21.6.2016 14:26	Microsoft Excel W...	32 KB
xls_HTC_One_M9_Applications_Viber_Sto...	21.6.2016 14:26	Microsoft Excel W...	13 KB
xls_HTC_One_M9_Applications_X-plore	21.6.2016 14:17	Microsoft Excel W...	225 KB
xls_HTC_One_M9_Applications_Yahoo_M...	21.6.2016 14:26	Microsoft Excel W...	10 KB
xls_HTC_One_M9_Deleted_Data	21.6.2016 14:16	Microsoft Excel W...	33 KB
xls_HTC_One_M9_Passwords	21.6.2016 14:17	Microsoft Excel W...	12 KB
xls_HTC_One_M9_SIM_Card	21.6.2016 14:17	Microsoft Excel W...	10 KB

Each record and contact has its own exf_ID xxx. You can view all data related to a specific ID by searching through the desired MS Excel list.

5.12.4 Export & backups

All export formats are machine-readable and can be used to process extracted data in other applications or to make a full backup of any device which can be later opened and analyzed without having the device live connected again.

5.12.4.1 MOBILedit Backup

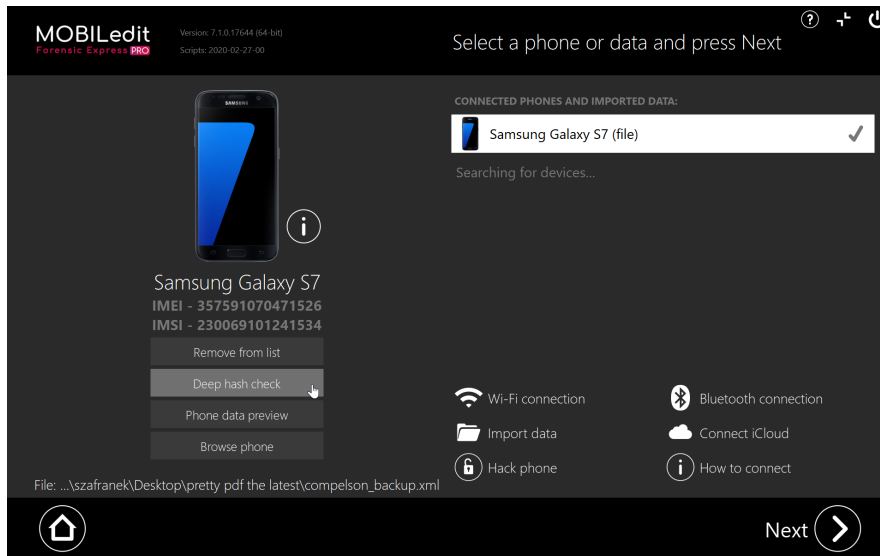


MOBILedit Backup XML contains a full phone data backup that can be opened, browsed, and analyzed again, as well

as archived for further use. The complete filesystem structure is put into the *mobiledit_backup.xml* file and all phone data is copied into *the backup_files* subfolder.

You can set packing and password protection for Backup. The Hash protection is set automatically when the backup creation was selected. The default hashing method is SHA-256, which is more secure than the MD5.

The master backup hash check is done when you import the MOBILedit backup.



The hash for each file in the backup can be checked by running the deep hash check.

5.12.4.2 MOBILedit Export

MOBILedit Export is an XML file used to export extracted and analyzed data into other applications. You can set Hash protection as well.

At the end of each report is displayed the result of the hash check, possible failures are included.

```

2018-11-02 10:07:05 Data extraction started - MOBILedit Forensic Express, version 6.0.0.14448 (x64)
2018-11-02 10:16:11 All 318 archive files were successfully extracted
2018-11-02 10:16:11 All 110 audio files were successfully extracted
2018-11-02 10:16:11 All 1 certificates were successfully extracted
2018-11-02 10:16:11 All 834 documents were successfully extracted
2018-11-02 10:16:11 All 3279 image files were successfully extracted
2018-11-02 10:16:11 All 494 json files were successfully extracted
2018-11-02 10:16:11 All 512 sqlite databases were successfully extracted
2018-11-02 10:16:11 All 12 video files were successfully extracted
2018-11-02 10:16:11 All 1519 xml files were successfully extracted
2018-11-02 10:16:11 Extracted 9017 out of 9019 other files, 2 failed
2018-11-02 10:15:55 [read failure] /data/misc/keystore/user_0/10147_USRCERT_com+^appsflyer+\KSAAppsFlyerId=1513074669849+]302652310656184864+\KSAAppsFlyerRIC
2018-11-02 10:15:55 [hash failure] /data/misc/keystore/user_0/10147_USRCERT_com+^appsflyer+\KSAAppsFlyerId=1513074669849+]302652310656184864+\KSAAppsFlyerRIC
2018-11-02 10:15:55 [read failure] /data/misc/keystore/user_0/10147_USRPKEY_com+^appsflyer+\KSAAppsFlyerId=1513074669849+]302652310656184864+\KSAAppsFlyerRIC
2018-11-02 10:15:55 [hash failure] /data/misc/keystore/user_0/10147_USRPKEY_com+^appsflyer+\KSAAppsFlyerId=1513074669849+]302652310656184864+\KSAAppsFlyerRIC
2018-11-02 10:16:06 All 218 applications were successfully extracted
2018-11-02 10:16:11 Data extraction finished

```

5.12.4.3 Cellebrite UFDR

This export file can be exported into and opened by the Cellebrite Mobile Forensics line of products.

5.12.4.4 ADB and iTunes backups

MOBILedit Forensic Express can now create and save ADB (Android) or iTunes (iOS) backups of your devices.

i If the ADB backup creation freezes, simply disconnect the phone, restart it, connect it to the PC and the MOBILedit Forensic Express will request the ADB back up again.

! Filtering only applies to final reports. Please, keep in mind that other outputs (such as UFDR), will not be affected by filtering and data selection.

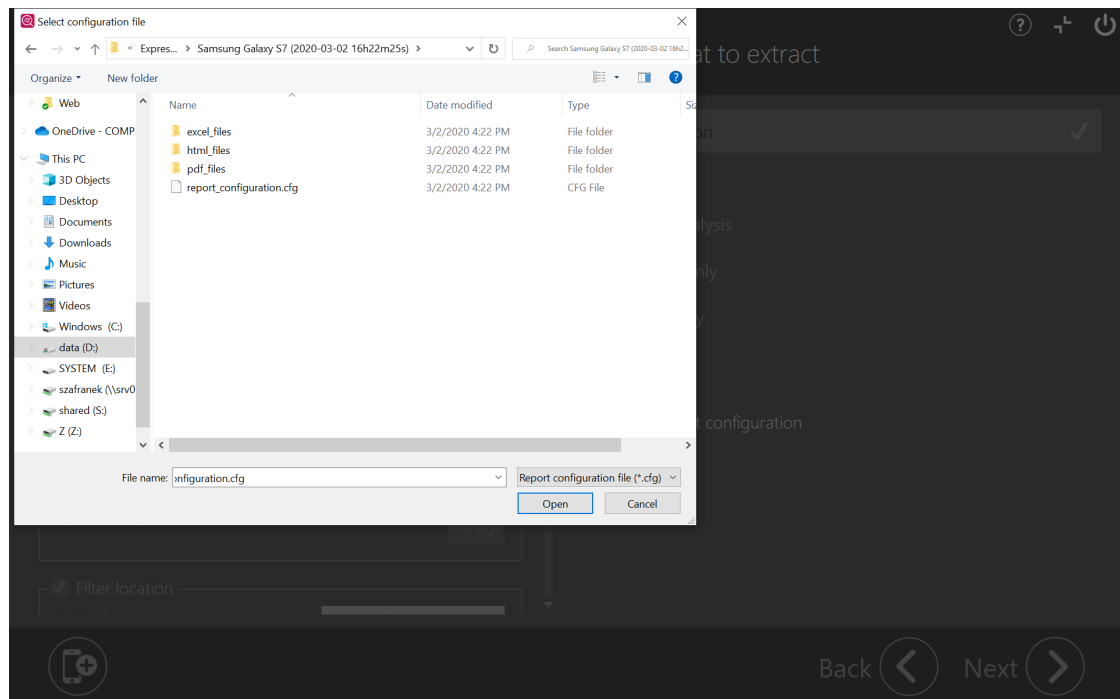
In case you select MOBILedit backup, all relevant information will be present as well. For example, GPS data might be present in various other sections, such as images.

5.13 Load report configuration

To speed up the configuration of your report, you may use the configuration of a previous report as a template. The report configuration file is always automatically saved inside the report folder. To load it, simply click "Load report configuration" on the report type selection page, navigate to the report with the desired configuration, and select report_configuration.cfg in its folder.

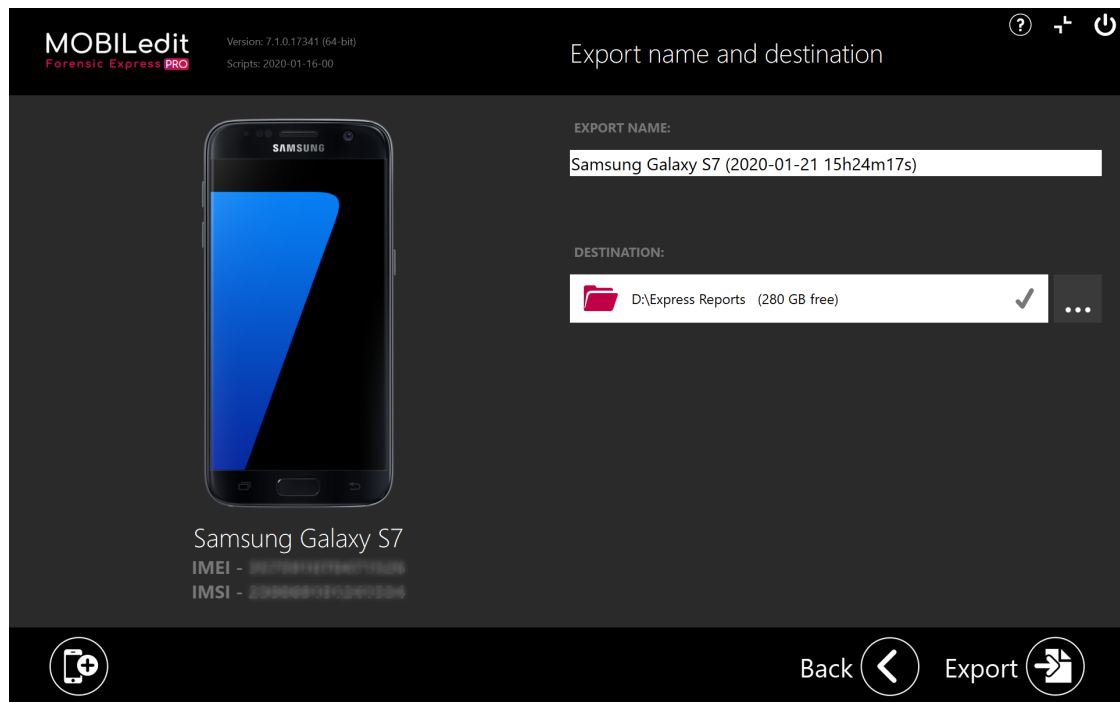
Once a configuration file is loaded, the subsequent forms will be filled with the same values as they were in the respective report. You can of course change some of them before proceeding with the export.

 Load report configuration

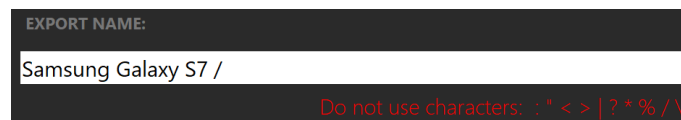


5.14 Export name and destination

Once you have selected data to be exported, you are prompted to select a name and a parent folder to save exports. The export name is automatically filled by a combination of phone name, current date, and time.



You can choose your own export name, but please **do not** use invalid path characters as shown in the image below when choosing an export name, otherwise, you will not be able to continue.



The application will create a sub-folder according to the export name and settings and put the export file system structure inside.

Name	Date modified	Type	Size
backup_files	1/21/2020 3:26 PM	File folder	
html_files	1/21/2020 3:27 PM	File folder	
pdf_files	1/21/2020 3:27 PM	File folder	
log_full.txt	1/21/2020 3:27 PM	Text Document	2 KB
log_short.txt	1/21/2020 3:26 PM	Text Document	1 KB
mobileedit_backup.xml	1/21/2020 3:26 PM	XML Document	6 KB
Report.pdf	1/21/2020 3:27 PM	Adobe Acrobat Docu...	328 KB
report_configuration.cfg	1/21/2020 3:26 PM	CFG File	5 KB
Report_index.html	1/21/2020 3:27 PM	Chrome HTML Docu...	3 KB
Report_long.html	1/21/2020 3:27 PM	Chrome HTML Docu...	15 KB

5.15 MOBILedit Export XML documentation

- [Who is this document for?\(see page 301\)](#)
- [Basic concepts\(see page 301\)](#)
- [Brief description of XML\(see page 301\)](#)
- [More about files\(see page 302\)](#)
- [Containers, items, parts and others\(see page 302\)](#)
- [Data sources\(see page 303\)](#)
- [A few notes on use\(see page 303\)](#)
- [Explanation of table items\(see page 303\)](#)
 - [Occurrence indicators\(see page 303\)](#)
 - [Data types\(see page 304\)](#)
 - [Containers in detail - attributes and nested tags\(see page 304\)](#)
 - [Items in detail - attributes and nested tags\(see page 311\)](#)
 - [Parts in detail - attributes\(see page 319\)](#)
- [XSD file structure specification\(see page 324\)](#)

5.15.1 Who is this document for?

 This document is a data specification for 3rd party developers

This document is an introduction to a specification of MOBILedit Forensic Express export XML. It describes the format and structure of the export XML, as well as additional rules that affect its appearance. It is primarily intended for third-party developers who will further process the export XML and import its data to their solutions such as databases or viewers of digital evidence.

5.15.2 Basic concepts

Data (e.g. contacts, messages, call logs) obtained from the device is referred to as items and a set of such items as a container. They usually have an almost identical tag name distinguished only by quantity, such as CONTACT and CONTACTS, MESSAGE and MESSAGES, CALL and CALLS. However, even items are such, only smaller, containers that contain information of various natures: texts, numbers, logical values, dates, addresses, etc. Gradually, the designations CONTAINER, ITEM and PART have become established for this triad of data of various levels. The first two ones are represented in the XSD file by the abstract types CONTAINERTYPE and ITEMTYPE. PART (leaf in the XML tree) is expressed by its string value supplemented by various attributes. In the past, this simple data structure would suffice, but in modern devices with a large number of applications, there was a need to group them into even higher units (SOURCE and SOURCES tags). Also various file systems are an essential part of them (FILESYSTEM, FOLDER, FILE tags and others). And to ensure that the data is not completely passive, e.g. the IDENTIFIERPART, DATASOURCEPART tags take care of their activation (interconnection). Finally, the addition of the MEFEXPORT root tag and other auxiliary tags (e.g. PROPERTIES, PHONEPHOTO) created a comprehensive set used to describe all the information extracted from a physical device or other sources. It remains to add that the relationship between CONTAINER, ITEM and PART is not always so one-way and there is a set of exceptions in their interconnection.

5.15.3 Brief description of XML

Although XSD allows great variability in the data structure, the generated XMLs show identical features, which can be described relatively easily. The introductory tag MEFEXPORT (root) contains a set of PROPERTIES with information about the case, the examiner, the device and the application itself. The most important, however, is the

SOURCE tag (currently just one), which accumulates a description of all device data (or alternative data source). SOURCE again first of all contains information about the device, including its image. This is followed by a description of all the files that are part of the export. These ones are divided according to the physical or logical storage into one or more FILESYSTEM (FILESYSTEM corresponds to the classic storage composed of FOLDER and FILES). Other tags represent various containers with global data (contacts, SMS, MMS, etc.) followed by data obtained by application analysis. Each application has its own SOURCE, which encapsulates its data and uses the same sub tags as the SOURCE on the global level to record them. All applications are grouped in one SOURCES container.

5.15.4 More about files

All files and directories in the export are included under one or more FILESYSTEM tags. FILESYSTEM must contain exactly one FOLDER, which can already contain any number of other FOLDER and FILE tags. It is worth noting here that although FOLDER is of type ITEMTYPE, it contains other tags of ITEMTYPE type (FOLDER and FILE). The FILEPART tag is used where it is needed to link a specific file. Linking is done via the path attribute. Important tags of the ITEMTYPE type, which also use a link to the FILEPART file, are the so-called media files AUDIO, IMAGE, VIDEO and, surprisingly, DOCUMENT (the parent tag is always MEDIA). All of these must contain exactly one FILEPART tag. Another IMAGEPART tag has more options, it can be linked to both a file (FILE) and an image (IMAGE) via the path attribute. Just the IMAGE tag can contain other interesting data (e.g. width and height). The last of the important ones that contain FILEPART is the MESSAGEFILE tag, which is an attachment (even multiple) inserted into a message. If it is a physical location of files, then they are on the relative path to the export XML, this path is specified in the 'files' attribute of the MEFEXPORT tag.

5.15.5 Containers, items, parts and others

Genuine containers derived from CONTAINERTYPE are: SOURCES, SOURCE, ACCOUNTS, ALARMS, AUTOFILLS, BOOKMARKS, BTPAIRINGS, CALLS, CELLTOWERS, CONTACTS, CONTAINER, CONVERSATIONS, COOKIES, CREDITCARDS, DOWNLOADS, EVENTS, FILESYSTEM, GROUPS, LOGITEMS, MEDIA, MEDIAFOLDER, MESSAGES, NETWORKS, NEWS, NOTES, NOTIFICATIONS, PAGES, PASSWORDS, PLACES, ROUTES, SEARCHES, TASKS, TRANSACTIONS, TYPEDTEXT

Genuine items derived from ITEMTYPE are: ACCOUNT, ALARM, AUTOFILL, BOOKMARK, BTPAIRING, CALL, CELLTOWER, CONTACT, ITEM, CONVERSATION, COOKIE, CREDITCARD, DOCUMENT, DOWNLOAD, EVENT, FOLDER, FILE, GROUP, LOGITEM, AUDIO, IMAGE, VIDEO, MESSAGE, MESSAGEFILE, NETWORK, NEWSITEM, NOTE, NOTIFICATION, PAGE, PASSWORD, PLACE, ROUTE, SEARCH, TASK, TRANSACTION, WORD

Genuine parts derived from character string are: ADDRESSPART, BOOLPART, CAMERABALLISTICSPART, DATASOURCEPART, DATEPART, DATETIMEPART, DURATIONPART, ENUMPART, FILEPART, GENDERPART, GEOPART, IDENTIFIERPART, IDREFERENCEPART, IMAGEPART, NUMBERPART, RECURRENCEPART, TEXTPART, TIMEPART, THUMBNAILPART, URLPART

Individual containers are specialized for certain items. For which, it is already known by their name (e.g. TASKS for TASK). However, there is also various other data that does not correspond to any specific container. In this case, the general CONTAINER is used, the data in it are marked as ITEM. Unfortunately, there is currently no easy way to programmatically recognize what type of data it is.

In order not to isolate the data in their containers, they are linked together by references. There are two tags for this: IDENTIFIERPART and IDREFERENCEPART. What type of binding it is, it can be decided according to the attribute "type", e.g. if type is "account", the linked tag is ACCOUNT. However, not all values of the type attribute may be clear, so it is important to verify the target item (or items). In addition, it may not always be valid.

5.15.6 Data sources

Each ITEMTYPE obtained by analyzing a particular file should list that file using the DATASOURCEPART. Pairing with a physical file is the same as other links to the file system, i.e. via the path attribute. There can be more links, they can also be hierarchized in a simple way.

5.15.7 A few notes on use

Over the years of use, it has crystallized additional rules that are not and cannot be recorded in the XSD file. They are:

- The application SOURCE tag no longer contains any other SOURCE.
- The binding of the data item (ITEMTYPE) with the corresponding ACCOUNT tag is done via IDREFERENCEPART (type = "account"), any other variants even valid according to XSD are inadmissible.
- The GROUP tag contains references (IDENTIFIERPART, type = "participant") to its members (CONTACT and GROUP), not the other way around.
- The CONVERSATION tag contains references (IDENTIFIERPART, type = "participant") to its members (CONTACT, GROUP, and ACCOUNT).
- The MESSAGE tag contains (if known) a reference (IDREFERENCEPART, type = "conversation") to its conversation (CONVERSATION), the opposite approach is no longer used.
- The MESSAGE tag contains (if known) references (IDENTIFIERPART) to the items involved. The type is "from", "to" or a general "participant". Other types of messages may use other variants, e.g. "cc", "bcc", etc.
- The CALL tag follows similar rules like MESSAGE.
- Do not mix different reference parts (IDENTIFIERPART vs. IDREFERENCEPART) for the same situations e.g. MESSAGE to its CONVERSATION.

5.15.8 Explanation of table items

5.15.8.1 Occurrence indicators

cnt	meaning	description
!	just one	
?	0 or 1	
+	1 or more	
*	0 or more	

5.15.8.2 Data types

dtp	meaning	description
S	string	
N	number	integer or 64-bit integer
R	real	double
E	enumeration	defined in the XSD file
B	boolean/logical	“true” or “false”
D	date	date corresponding to ISO 8601, i.e. in the format yyyy-MM-dd optionally with time zone (Z for UTC or [+ -] HH: mm)
T	time	time corresponding to ISO 8601, i.e. in the format HH: mm: ss optionally with time zone (Z for UTC or [+ -] HH: mm) and decimal part of seconds
DT	datetime	date and time corresponding to ISO 8601, i.e. in the format yyyy-MM-ddTHH: mm: ss optionally with time zone (Z for UTC or [+ -] HH: mm) and decimal part of seconds

5.15.8.3 Containers in detail - attributes and nested tags

All red values in the table are inherited from CONTAINERTYPE.

For dtp and cnt, see the table of data types and the table of occurrence indicators in the legend section.

container\attribute	xml:id	label	type	analysis¹⁾	class	structure²⁾	description³⁾
dtp	S	S	E	E	E	E	S
MEFEXPORT²⁾							
		attribute	dtp	cnt	description		
		dtdtversion	R	!	fixed value “2.0”		

container\attribute	xml:id	label	type	analysis ¹⁾	class	structure ²⁾	description ³⁾
	appversion			!			
	created			!			
	application			!			
	files		S	!	typically “mobiledit_export_files”		
PROPERTIES⁴⁾	!	?	?		?		
SOURCES	!	!	?			?	?
SOURCE⁵⁾	!	!	?			?	?
ACCOUNTS	!	!	?	?		?	?
ALARMS	!	!				?	?
AUTOFILLS	!	!				?	?
BOOKMARKS	!	!				?	?
BTPAIRINGS	!	!				?	?
CALLS	!	!		?		?	?
CELLTOWERS	!	!				?	?
CONTACTS	!	!	?	?		?	?
CONTAINER	!	!	?			?	?
CONVERSATIONS	!	!		?		?	?
COOKIES	!	!				?	?
CREDITCARDS	!	!				?	?

container\attribute	xml:id	label	type	analysis ¹⁾	class	structure ²⁾	description ³⁾
DOWNLOADS	!	!				?	?
EVENTS	!	!	?	?		?	?
FILESYSTEM	!	!	?		?	?	?
	attribute		dtp	cnt	description		
	path		S	?			
	priority			?			
	index			?			
GROUPS	!	!				?	?
LOGITEMS	!	!				?	?
MEDIA	!	!	?			?	?
	attribute		dtp	cnt	description		
	priority			?			
MEDIAFOLDER	!	!				?	?
MESSAGES	!	!	?	?		?	?
NETWORKS	!	!	?		?	?	?
NEWS	!	!				?	?
NOTES	!	!		?	?	?	?
	attribute		dtp	cnt	description		
	deleted			?			

container\attribute	xml:id	label	type	analysis ¹⁾	class	structure ²⁾	description ³⁾
NOTIFICATIONS	!	!				?	?
PAGES	!	!				?	?
PASSWORDS	!	!			?	?	?
	attribute		dtp	cnt	description		
	significance			?			
PLACES	!	!				?	?
ROUTES	!	!				?	?
SEARCHES	!	!			?	?	?
TASKS	!	!		?	?	?	?
	attribute		dtp	cnt	description		
	deleted			?			
TRANSACTIONS	!	!				?	?
TYPEDTEXT	!	!			?	?	?
PHONEPHOTOS	!	?	?				
THUMBNAILS							

1) “forensic” if data were obtained by file analysis

2) sorting flag

3) this is the real name of the attribute

4) MEFEXPORT and PROPERTIES are not genuine ITEMTYPE tags, but they have a very important function in our XML tree

5) the "reference" attribute is no longer used

container\child cnt	PROPERTIES	SOURCE	not ITEMTYPE * by default	ITEMTYPE * by default
MEFEXPORT¹⁾	*	?		
PROPERTIES¹⁾			see tables below	
SOURCES		+		
SOURCE	*	*3)	SOURCES	ITEMTYPE ²⁾
			IMAGEPART	
			PHONEPHOTOS	
			METANOTE	
ACCOUNTS	*			ACCOUNT
ALARMS				ALARM
AUTOFILLS				AUTOFILL
BOOKMARKS	*			BOOKMARK
BTPAIRINGS				BTPAIRING
CALLS	*			CALL
CELLTOWERS				CELLTOWER
CONTACTS	*			CONTACT
CONTAINER	*			ITEM
CONVERSATIONS	*			CONVERSATION
COOKIES				COOKIES

container\child cnt	PROPERTIES	SOURCE	not ITEMTYPE * by default	ITEMTYPE * by default
CREDITCARDS				CREDITCARD
DOWNLOADS				DOWNLOAD
EVENTS	*			EVENT
FILESYSTEM	*			FOLDER !
GROUPS	*			GROUP
LOGITEMS				LOGITEM
MEDIA				AUDIO
				IMAGE
				VIDEO
				DOCUMENT
MEDIAFOLDER			MEDIA	
MESSAGES	*			MESSAGE
NETWORKS	*			NETWORK
NEWS				NEWSITEM
NOTES	*			NOTE
NOTIFICATIONS				NOTIFICATION
PAGES	*			PAGE
PASSWORDS				PASSWORD

container\child cnt	PROPERTIES	SOURCE	not ITEMTYPE * by default	ITEMTYPE * by default
PLACES	*			PLACE
ROUTES	*			ROUTE
SEARCHES	*			SEARCH
TASKS	*			TASK
TRANSACTIONS				TRANSACTION
TYPEDTEXT	*			WORD
other non-CONTAINERTYPE tags				
PHONEPHOTOS			PHONEPHOTO	
FOLDER				FOLDER
				FILE
VIDEO			THUMBNAILS ?	
THUMBNAILS			THUMBNAIL	
DOCUMENT			DOCUMENTCONTENT ?	
DOCUMENTCONTENT			TEXTPART	
CONVERSATION				MESSAGE ³⁾
MESSAGE				MESSAGEFILE

¹⁾ MEFEXPORT and PROPERTIES are not genuine ITEMTYPE tags, but they have a very important function in our XML tree

2) ACCOUNT, ALARM, AUTOFILL, BOOKMARK, BTPAIRING, CALL, CELLTOWER, CONTACT, ITEM, CONVERSATION, COOKIE, CREDITCARD, DOCUMENT, DOWNLOAD, EVENT, FOLDER, FILE, GROUP, LOGITEM, AUDIO, IMAGE, VIDEO, MESSAGE, MESSAGEFILE, NETWORK, NEWSITEM, NOTE, NOTIFICATION, PAGE, PASSWORD, PLACE, ROUTE, SEARCH, TASK, TRANSACTION, WORD

3) unused combination

5.15.8.4 Items in detail - attributes and nested tags

All red values in the table are inherited from ITEMPTYPE.

item\attribute	xml:id	label	type	time	deleted
dtp	S	S	E	DT	B
ACCOUNT	!	?		?	?
ALARM	!	?		?	?
AUTOFILL	!	?		?	?
BOOKMARK	!	?		?	?
BTPAIRING	!	?		?	?
CALL	!	?	!	?	?
CELLTOWER	!	?		?	?
CONTACT	!	?		?	?
ITEM	!	?		?	?
CONVERSATION	!	?		?	?
COOKIE	!	?		?	?
CREDITCARD	!	?		?	?
DOCUMENT	!	?		?	?
DOWNLOAD	!	?		?	?

item\attribute	xml:id	label	type	time	deleted
EVENT	!	?	?	?	?
FOLDER	!	?		?	?
FILE	!	?	!	?	?
	attribute	dtp	cnt	description	
	filename	S	?		
	path	S	?		
	size	N	?		
	created	DT	?		
	modified	DT	?		
	accessed	DT	?		
	mimetype	S	?		
	hash	S?	?		
	md5hash	S?	?		
	sha1hash	S?	?		
	sha256hash	S?	?		
	sha512hash	S?	?		
	name	S?	?		
iscommon	B?	?			
hashCategories	S	?			

item\attribute	xml:id	label	type	time	deleted
GROUP	!	?		?	?
LOGITEM	!	?	!	?	?
AUDIO	!	?		?	?
IMAGE	!	?		?	?
	attribute	dtp	cnt	description	
	width	N	?		
	height	N	?		
VIDEO	!	?		?	?
MESSAGE	!	?	!	?	?
MESSAGEFILE	!	?	?	?	?
NETWORK	!	?		?	?
NEWSITEM	!	?		?	?
NOTE	!	?	?	?	?
NOTIFICATION	!	?		?	?
PAGE	!	?		?	?
PASSWORD	!	?		?	?
PLACE	!	?	?	?	?
ROUTE	!	?		?	?
SEARCH	!	?		?	?

item\attribute	xml:id	label	type	time	deleted					
TASK	!	?		?	?					
TRANSACTION	!	?	?	?	?					
WORD	!	?	?	?	?					
other non-ITEMTYPE tags										
PHONEPHOTO	!									
	attribute	dtp	cnt	description						
	path	S	?							
	note	S	?							
THUMBNAIL										
	attribute	dtp	cnt	description						
	name	S	!							
	position		!							
	timestamp		!							
	path	S	!							
METANOTE	!	!	!							
item\part¹⁾	ADDR	BOOL	CMBL	DTSR	DATE	DTIM	DUR	ENUM	FILE	GEN
	GEO	IDEN	IDRF	IMG	NUM	RECR	TEXT	TIME	THMB	URL
ACCOUNT	*	*		*	*	*	*	*		*
	*	*	*	*	*	*	*	*		*

item\part ¹⁾	ADDR	BOOL	CMBL	DTSR	DATE	DTIM	DUR	ENUM	FILE	GEN
	GEO	IDEN	IDRF	IMG	NUM	RECR	TEXT	TIME	THMB	URL
ALARM		*		*	*	*	*			
					*		*	*		
AUTOFILL				*		*				
		*			*		*			
BOOKMARK		*		*		*				
	*	*	*	*	*		*			*
BTPAIRING				*		*				
							*			
CALL		*		*		*	*		*	
		*	*				*			*
CELLTOWER				*		*				
	*				*		*			
CONTACT	*	*		*	*	*	*	*		*
	*	*	*	*	*	*	*	*		*
ITEM	*	*		*	*	*	*	*	*	*
	*	*	*	*	*	*	*	*		*
CONVERSATION	*	*		*	*	*	*	*		*
	*	*	*	*	*	*	*	*		*

item\part ¹⁾	ADDR	BOOL	CMBL	DTSR	DATE	DTIM	DUR	ENUM	FILE	GEN
	GEO	IDEN	IDRF	IMG	NUM	RECR	TEXT	TIME	THMB	URL
COOKIE				*		*				
							*			
CREDITCARD				*		*				
		*	*		*		*			*
DOWNLOAD				*		*	*		*	
		*	*		*		*			*
EVENT	*	*		*	*	*	*			
	*	*	*	*	*	*	*			*
FOLDER	*	*		*	*	*	*	*		*
	*	*	*	*	*	*	*	*		*
FILE	*	*		*	*	*	*	*		*
	*	*	*	*	*	*	*	*		*
GROUP		*		*		*				
		*	*	*	*		*			*
LOGITEM				*		*				
		*			*		*			
AUDIO				*			*		!	
	*						*			

item\part ¹⁾	ADDR	BOOL	CMBL	DTSR	DATE	DTIM	DUR	ENUM	FILE	GEN
	GEO	IDEN	IDRF	IMG	NUM	RECR	TEXT	TIME	THMB	URL
IMAGE			*	*		*			!	
	*		*		*		*			*
VIDEO				*		*	*		!	
	*		*		*		*		?	*
DOCUMENT				*					!	
MESSAGE	*	*		*	*	*	*	*		*
	*	*	*	*	*	*	*	*		*
MESSAGEFILE	*	*			*	*	*	*	*1)	*
	*	*	*	*	*	*	*	*		*1)
NETWORK		*		*		*				
	*	*			*		*			
NEWSITEM				*		*				
		*	*		*		*			*
NOTE		*		*		*	*		*	
	*	*	*		*		*			*
NOTIFICATION	*	*		*		*				
	*	*	*		*		*			*

item\part ¹⁾	ADDR	BOOL	CMBL	DTSR	DATE	DTIM	DUR	ENUM	FILE	GEN
	GEO	IDEN	IDRF	IMG	NUM	RECR	TEXT	TIME	THMB	URL
PAGE		*		*		*				
	*	*	*	*	*		*			*
PASSWORD				*		*			*	
					*		*			*
PLACE	*	*		*	*	*	*	*		*
	*	*	*	*	*	*	*	*		*
ROUTE	*	*	*	*	*	*	*	*		*
	*	*	*		*		*			*
SEARCH	*	*		*	*	*	*	*		*
	*	*	*	*	*	*	*	*		*
TASK	*	*		*	*	*	*			
	*	*	*	*	*	*	*			*
TRANSACTION		*		*		*				
	*	*	*				*			
WORD				*						
							*			
PROPERTIES ²⁾	*	*			*	*	*	*		*
	*	*	*	*	*	*	*	*		*

¹⁾ ADDR, BOOL etc. are abbreviations for the individual parts described above

- 2) MESSAGEFILE must contain at least one FILEPART or one URLPART
- 3) PROPERTIES is not genuine ITEMTYPE, but includes most of the PART tags

5.15.8.5 Parts in detail - attributes

part	attribute	cnt	dtp	description
ADDRESSPART	<i>text value</i>		N/A	
	type	!	E	used by drvman CONTACT only
	class	?	E	for “raw”, full address in the street
	street	?	S	
	addressextension	?	S	
	pobox	?	S	
	locality	?	S	
	region	?	S	
	country	?	S	
	postalcode	?	S	
BOOLPART	<i>text value</i>		B	
	type	!	E	
CAMERABALLISTICSPART	<i>text value</i>		N/A	
	probability	!	R	
	correlation	!	R	
	status	!	S	error text if fingerprint not found
	match	!	S	boolean value written as “0” or “1”

	fingerprint	!	S	path to fingerprint
DATASOURCEPART	<i>text value</i>		N/A	
	type	?	E	“main” or “other”
	priority	!	N	“0” for “main” otherwise “1” “0” is the highest priority
	path	!	S	path to the file from which ITEM was obtained
	table	?	S	database table name
	offset	?	N	64-bit integer
DATEPART	<i>text value</i>		D	
	type	!	E	
DATETIMEPART	<i>text value</i>		DT	
	type	!	E	
	flag	?		for “incomplete”, the text value does not include year (and/or other parts?)
DURATIONPART	<i>text value</i>		N	64-bit integer, number of seconds
	type	!	E	
ENUMPART	<i>text value</i>		S	value part of [type, value] pair
	type	!	E, S	type part of [type, value] pair
FILEPART	<i>text value</i>		N/A	
	type	!	E	
	filename	?	S	

	path	?	S	path to the file
	size	?	N	in bytes
	created	?	DT	
	modified	?	DT	
	accessed	?	DT	
	mimetype	?	S	
	hash	?	S	hexadecimal
	md5hash	?	S	hexadecimal
	sha256hash	?	S	hexadecimal
	name	?	S	
GENDERPART	<i>text value</i>		N/A	
	gender	?	E	“male“, ”female” or ”unknown”
GEOPART	<i>text value</i>		N/A	
	type	!	E	
	time	?	DT	
	latitude	!	R	in degrees
	longitude	!	R	in degrees
	accuracy	?	N	in meters
	altitude	?	N	in meters
	speed	?	N	in meters per second

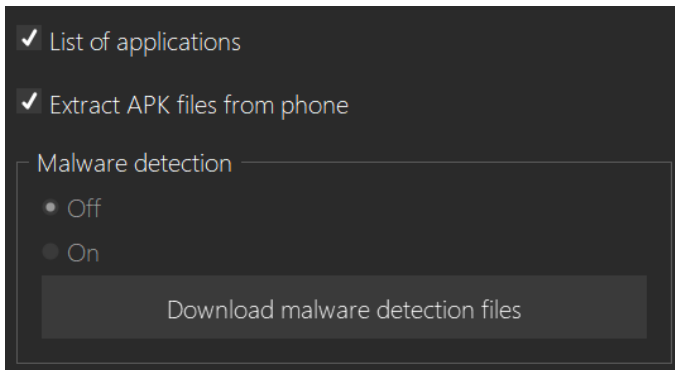
	heading	?	R	direction in degrees
IDENTIFIERPART	<i>text value</i>		S	displayed value
	type	!	E	
	linking	?	E	for “cross-referenced”, source and target can be from different SOURCE
	idrefs	!	S	references somewhere, separated by space
IDREFERENCEPART	<i>text value</i>		S	same as the idrefs
	type	?	E	
	idrefs	!	S	reference somewhere
IMAGEPART	<i>text value</i>		N/A	
	type	?	E	
	path	!	S	path to the file
	height	?	N	
	width	?	N	
	mimetype	?	S	
NUMBERPART	<i>text value</i>		N, R	
	type	!	E	
	notation	?	E	“real” nebo “int”; “real” if empty
	unit	?	E	
RECURRENCEPART	<i>text value</i>		N/A	
	type	!	E	

	frequency	?	E	“once“, “daily“, “weekly“, “fortnightly“, “monthly“, “yearly“, “weeklyex“, “daysinweek“, “daysinmonth“
	interval	?	N	e.g. once in 3 years, the interval is 3
	until	?	DT	
	dayflags	?	S	“SU“, “MO“, “TU“, “WE“, “TH“, “FR“, “SA“
	occurrence	?	N	e.g. every 2nd Sunday, the occurrence is 2
	numofrepeating	?	N	
TEXTPART	<i>text value</i>		S	
	type	!	E	
TIMEPART	<i>text value</i>		T	time
	type	!	E	
THUMBNAILPART	<i>text value</i>		N/A	
	name	!	S	file name
	path	!	S	path to the file
URLPART	<i>text value</i>		S	URL itself
	type	!	E	
	path	?	S	path to the file
	timestamp	?	DT	download time

5.15.9 XSD file structure specification

Following XSD file describes the structure of MOBILedit export XML format. Feel free to download it [here](#)⁸².


5.16 Malware detection



Malware detection is an AI-based feature thoroughly crafted to search for harmful malware. Installation files (APK files) are being scanned and compared with the already existing (and regularly updated) databases.

Infected files will be shown in the final report with additional info about the APK files, however, they will not be affected (or even removed) in any way, since the main goal is to keep the connected device in the very same state.

The potentially harmful file will not be executed, therefore cannot harm your PC, nor mobile device.

 We do recommend turning off your PC anti-virus program since it might delete potentially harmful files so they will not be discovered and shown in the final report.

 Malware detection is an add-on feature, manually downloadable from [here](#).⁸³

⁸² <https://forensic.manuals.mobiledit.com/MM/2417360967/ExportXML20.xsd>

⁸³ <http://download.mobiledit.com/pfe/AppengineScripts/latestMWD.package>

6 Specific selection

Learn all you need to know about the data that can be analyzed, extracted and filtered with MOBILedit Forensic Express.

6.1 Data - Screenshots of report settings

Screenshots of report settings allow you to display the settings you chose for your extraction. They will be displayed in the report and simplify the troubleshooting. They can be also used as a reference for different report settings for other cases or extractions.

6.2 Data - Summary

A synoptic list showing all the gathered data as well as their amount:

Summary

Contacts	
Contact List	0
Photo Recognizer	
Recognized Images of Currency	0
Recognized Images of Documents	0
Recognized Images of Drugs	0
Recognized Images of Extremist symbols	0
Recognized Images of Nudity	0
Recognized Images of Upskirt	38
Recognized Images of Weapons	0
Photos	
Image Files	36651
Large Images	84
Audio Files	2455
Video Files	47
Documents	8893
Filesystems	
Internal Filesystem	137417 files
Misc Filesystem	0 files
Locations	
GPS Locations	0
Timeline	54888

6.3 Data - Deleted data

We do offer more ways to recover deleted data. The first one is recovering the data from SQLite databases, the second one is recovering the files and folders from **Physical images**(see page 42).

SQL databases allow you to recover the data which were marked as deleted or are still present in a database folder. SQLite is the most common way to store data for both **iPhone** and **Android**.

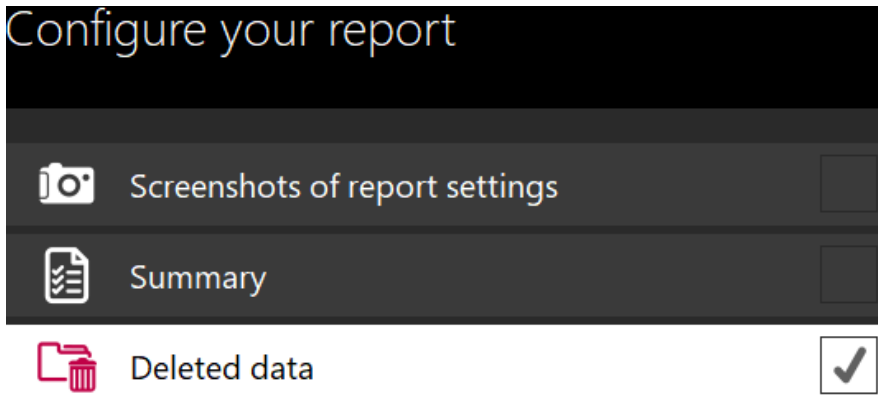
Physical images allow you to recover deleted folders and files which are still available through the file system, plus the SQL databases as well, which makes it the best option to obtain the lost data.

With Rooted/jailbroken devices we are able to get straight to the file system and SQL databases as well.

Devices without the root or jailbreak are the hardest ones to recover, yet there is still a chance to obtain some of the data although it will be significantly less than the options above (or none).

Velocity also plays a big role in data recovery - the longer you wait, the lesser are the chances for successful operation. Restarting the device (or even apps) might increase the risk of permanent loss of your deleted data as

well.



i It is never 100% guaranteed you will be able to retrieve deleted data. The amount of recovered deleted data depends on various factors such as how long is it since the data was deleted (30 days at most), was it a factory reset or not and such.

6.4 Data - Captured phone photos



Captured phone photos selection allows you to:

1. **Webcam:** take a picture of the examined phone using the web camera.
2. **Phone:** capture screenshot of the phone display (Android and iOS only)
3. **Import:** select photos of your selection from your internal or external drive

i Capturing screenshots from the phone might be very useful when you need to add data which cannot be obtained to your report. For example encrypted conversations from unrooted devices.

6.4.1 Take picture

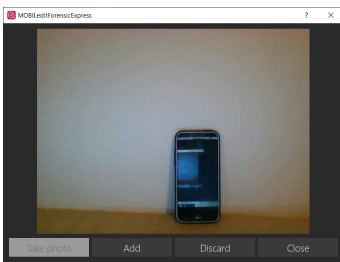
This feature allows you to take a picture of the phone or a device you are going to investigate using your webcam. You can take as many pictures as you need and these will be added into the report.

Click on the **Webcam** button:



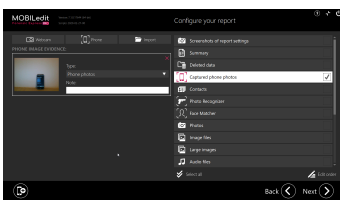
A new window will appear.

Aim at your investigated device with the Webcam and click the **Take photo** button:

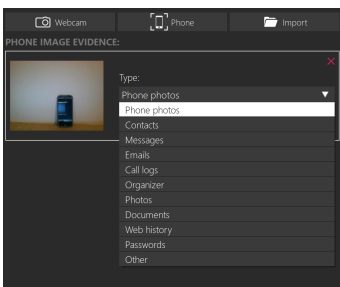


Add will save the taken photo. **Discard** will return you to the previous window. **Close** will close the window and all changes will be lost.

Taken pictures will be saved under the menu on the left side of the screen:



You can change the type of photo or add a note. You can take multiple photos:



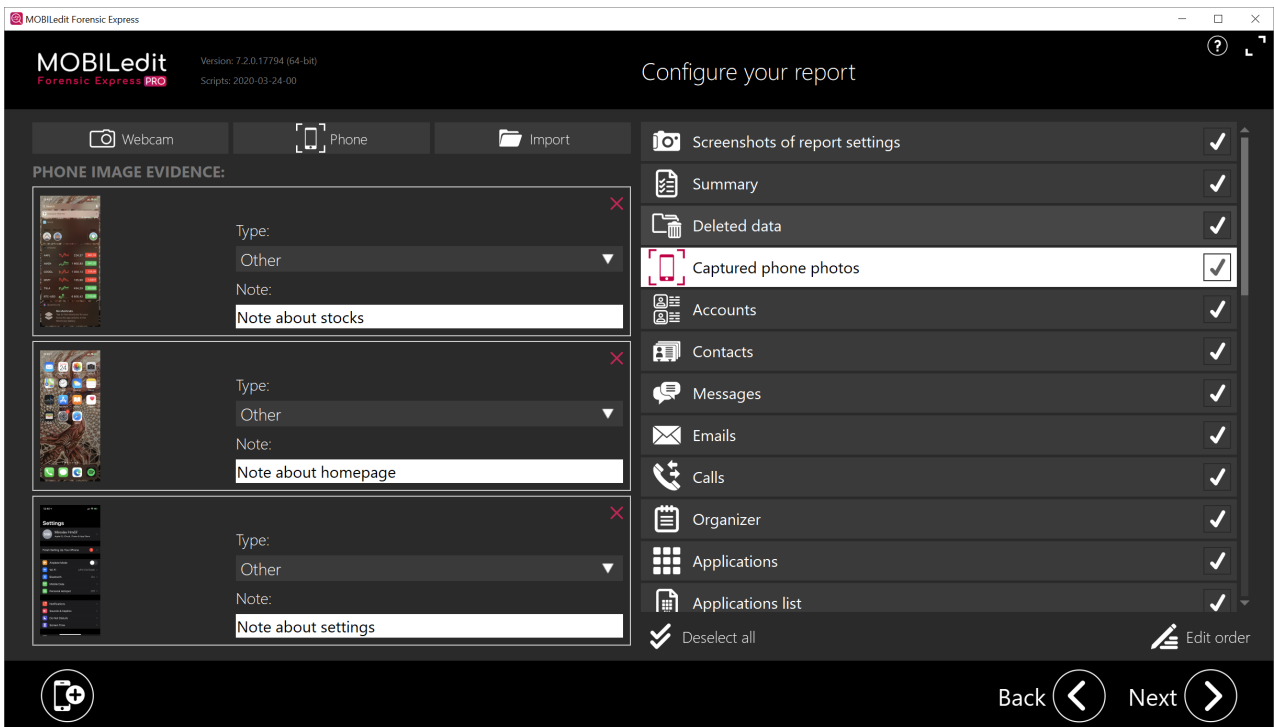
6.4.2 Capture screenshot

Simply take a screenshot of anything displayed on your device.

Click on the **Phone** button:



Captured screenshots will be saved under the menu on the left side of the screen:



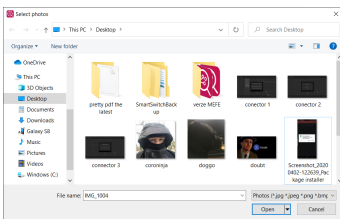
You can change the type of screenshot, add a note to it and take as many screenshots as you like.

6.4.3 Import

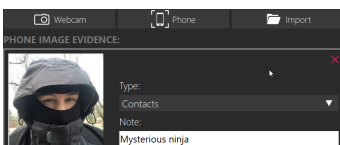
Click on the **Import** button:



The **Windows File Explorer** window will open:



Browse the folder to find your desired photo and click the **Open** button.
The selected photo will appear:



You can change the type of photo, add a note to it and take as many as you like.

Case Label:

Case Evidence Number:

Device Label:

Captured Phone Photos





Contacts (1)



Mysterious ninja

6.5 Data - Accounts

This section shows all the accounts linked to the device such as Facebook, Google, and others:

1 WhatsApp		
	Name	WhatsApp
	Type	com.whatsapp
	Associated Contacts	30
	Source File	phone/applications1/Content Providers/Accounts.xml
2 Google		
	Name	[REDACTED]@gmail.com
	Type	com.google
	Associated Contacts	54
	Source File	phone/applications1/Content Providers/Accounts.xml
3 Messenger		
	Name	Messenger
	Type	com.facebook.messenger
	Associated Contacts	17
	Source File	phone/applications1/Content Providers/Accounts.xml
4 Ůčet Samsung account		
	Name	[REDACTED]@gmail.com
	Type	com.osp.app.signin
	Source File	phone/applications1/Content Providers/Accounts.xml

6.6 Data - Contacts

6.6.1 Contacts



Phone contacts – retrieves all contacts from the phone; typically what is contained in the standard phone book.

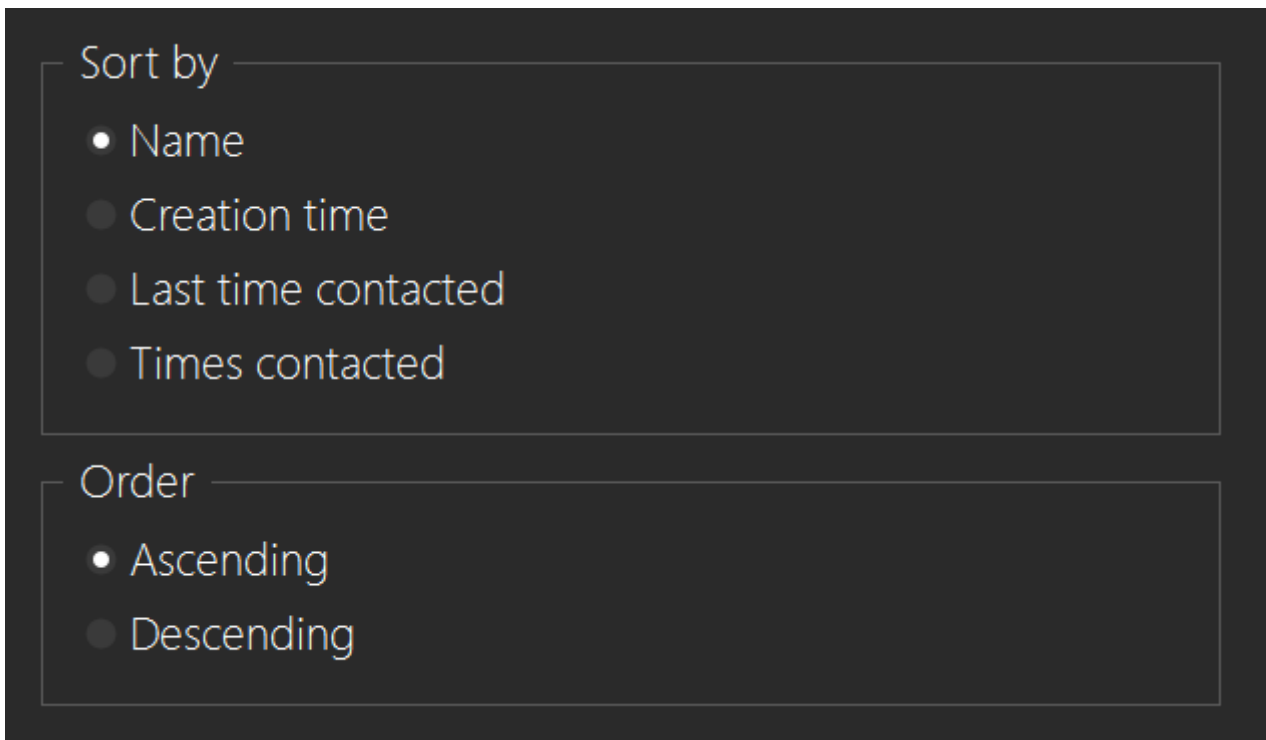
SIM contacts – contacts from the SIM card, if present in the phone and the phone allows access to the SIM card data.

Application contacts – if selected, all contacts from all applications will be merged together with the phone contacts in the main Contacts section. If not selected, application contacts will still be displayed in their respective application sections.

Data from vCard files – if selected, all vCard files retrieved from the phone will be analyzed, and the results will be merged to the Contacts section as well.

Deleted contacts - shows deleted contacts from all options above - unless you filter them out.

6.6.1.1 Display order of contacts



Contacts in the report can be ordered by:

- Name
- Time the contact was created (this is useful for locating newly added contacts)
- Time the contact was last communicated with (such as who was called most recently)
- How many times the contact has been interacted with (frequent contacts)

However, the last three options are not available on all phones. 'Creation time' can only be retrieved from iOS and recent versions of Android. 'Last time contacted' and 'Times contacted' are only available from Android phones.

To see examples of what reports will look like, based on various settings, go to the 'Report in details' section.

6.6.1.2 Example of contacts report:

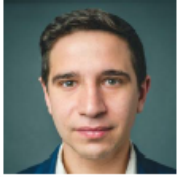
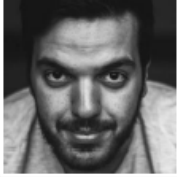

Case Label: Kentucky church

Case Evidence Number: 8974969-589-468

Device Label:

Contacts (16)

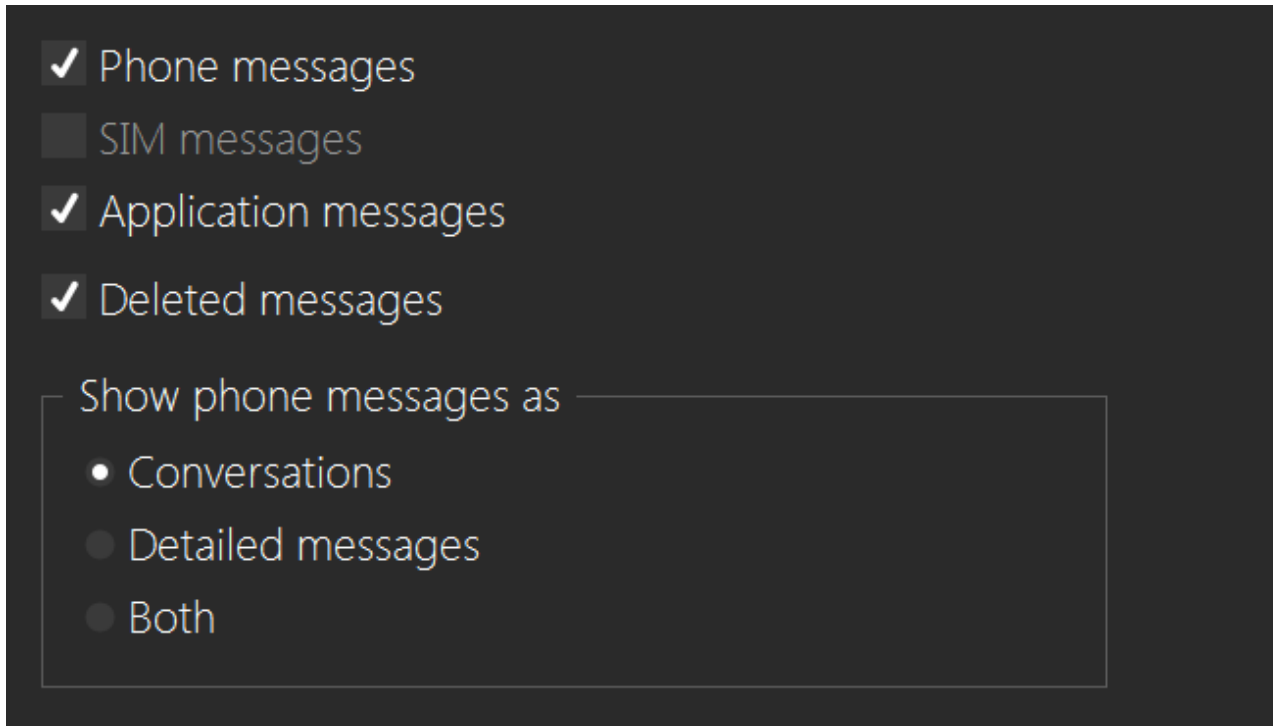
All phone and SIM contacts, sorted by name in ascending order

1 Aaron Witcher Phone Memory																					
	<table border="1"> <tr><td>Group ID</td><td>621</td></tr> <tr><td>First Name</td><td>Aaron</td></tr> <tr><td>Last Name</td><td>Witcher</td></tr> <tr><td>Mobile</td><td>+7698754122</td></tr> <tr><td>Home Email</td><td>a.witcher@mail.ru</td></tr> <tr> <td>Home Address (Google Maps)</td> <td> <table border="1"> <tr><td>Street</td><td>Karla Marksa Street, 124</td></tr> <tr><td>Country</td><td>Russia</td></tr> </table> </td> </tr> <tr><td>Birthday</td><td>1954-01-01 01:00:00 (UTC+1)</td></tr> </table>	Group ID	621	First Name	Aaron	Last Name	Witcher	Mobile	+7698754122	Home Email	a.witcher@mail.ru	Home Address (Google Maps)	<table border="1"> <tr><td>Street</td><td>Karla Marksa Street, 124</td></tr> <tr><td>Country</td><td>Russia</td></tr> </table>	Street	Karla Marksa Street, 124	Country	Russia	Birthday	1954-01-01 01:00:00 (UTC+1)		
Group ID	621																				
First Name	Aaron																				
Last Name	Witcher																				
Mobile	+7698754122																				
Home Email	a.witcher@mail.ru																				
Home Address (Google Maps)	<table border="1"> <tr><td>Street</td><td>Karla Marksa Street, 124</td></tr> <tr><td>Country</td><td>Russia</td></tr> </table>	Street	Karla Marksa Street, 124	Country	Russia																
Street	Karla Marksa Street, 124																				
Country	Russia																				
Birthday	1954-01-01 01:00:00 (UTC+1)																				
2 Alkiviadis Loukas Phone Memory																					
	<table border="1"> <tr><td>Group ID</td><td>628</td></tr> <tr><td>First Name</td><td>Alkiviadis</td></tr> <tr><td>Last Name</td><td>Loukas</td></tr> <tr><td>Mobile</td><td>+30657452894</td></tr> <tr><td>Home Email</td><td>loukas@mail.gr</td></tr> <tr> <td>Home Address (Google Maps)</td> <td> <table border="1"> <tr><td>Street</td><td>Valaoritou 33</td></tr> <tr><td>Locality</td><td>Trikala</td></tr> <tr><td>Country</td><td>Greece</td></tr> </table> </td> </tr> <tr><td>Birthday</td><td>1979-04-05 02:00:00 (UTC+2)</td></tr> </table>	Group ID	628	First Name	Alkiviadis	Last Name	Loukas	Mobile	+30657452894	Home Email	loukas@mail.gr	Home Address (Google Maps)	<table border="1"> <tr><td>Street</td><td>Valaoritou 33</td></tr> <tr><td>Locality</td><td>Trikala</td></tr> <tr><td>Country</td><td>Greece</td></tr> </table>	Street	Valaoritou 33	Locality	Trikala	Country	Greece	Birthday	1979-04-05 02:00:00 (UTC+2)
Group ID	628																				
First Name	Alkiviadis																				
Last Name	Loukas																				
Mobile	+30657452894																				
Home Email	loukas@mail.gr																				
Home Address (Google Maps)	<table border="1"> <tr><td>Street</td><td>Valaoritou 33</td></tr> <tr><td>Locality</td><td>Trikala</td></tr> <tr><td>Country</td><td>Greece</td></tr> </table>	Street	Valaoritou 33	Locality	Trikala	Country	Greece														
Street	Valaoritou 33																				
Locality	Trikala																				
Country	Greece																				
Birthday	1979-04-05 02:00:00 (UTC+2)																				
3 Alphonso Neely Phone Memory																					
	<table border="1"> <tr><td>Group ID</td><td>622</td></tr> <tr><td>First Name</td><td>Alphonso</td></tr> <tr><td>Last Name</td><td>Neely</td></tr> <tr><td>Mobile</td><td>+1889567412</td></tr> <tr><td>Home Email</td><td>alphonso.n@kmail.com</td></tr> <tr> <td>Home Address (Google Maps)</td> <td> <table border="1"> <tr><td>Street</td><td>25 S 2nd St Black River Falls, WI</td></tr> <tr><td>Country</td><td>USA</td></tr> </table> </td> </tr> <tr><td>Birthday</td><td>1989-09-06 02:00:00 (UTC+2)</td></tr> </table>	Group ID	622	First Name	Alphonso	Last Name	Neely	Mobile	+1889567412	Home Email	alphonso.n@kmail.com	Home Address (Google Maps)	<table border="1"> <tr><td>Street</td><td>25 S 2nd St Black River Falls, WI</td></tr> <tr><td>Country</td><td>USA</td></tr> </table>	Street	25 S 2nd St Black River Falls, WI	Country	USA	Birthday	1989-09-06 02:00:00 (UTC+2)		
Group ID	622																				
First Name	Alphonso																				
Last Name	Neely																				
Mobile	+1889567412																				
Home Email	alphonso.n@kmail.com																				
Home Address (Google Maps)	<table border="1"> <tr><td>Street</td><td>25 S 2nd St Black River Falls, WI</td></tr> <tr><td>Country</td><td>USA</td></tr> </table>	Street	25 S 2nd St Black River Falls, WI	Country	USA																
Street	25 S 2nd St Black River Falls, WI																				
Country	USA																				
Birthday	1989-09-06 02:00:00 (UTC+2)																				

6.7 Data - Messages

"Phone messages" groups the SMS, MMS, iMessages, application messages and any standard phone messages together. Forensic Express can find any variation of these types of message and present the gathered data in the report generated.

Emails and Email messages are gathered separately in their own section and will not be shown in the Messages section of the report.



Phone messages – standard phone messages, which covers SMS, MMS, and iMessages on iPhones.

SIM messages – messages retrieved from the SIM card, if available.

Application messages - if selected, all messages from all applications will be merged together with the standard phone messages. If not selected, application messages will be shown only in their respective application sections of the report.

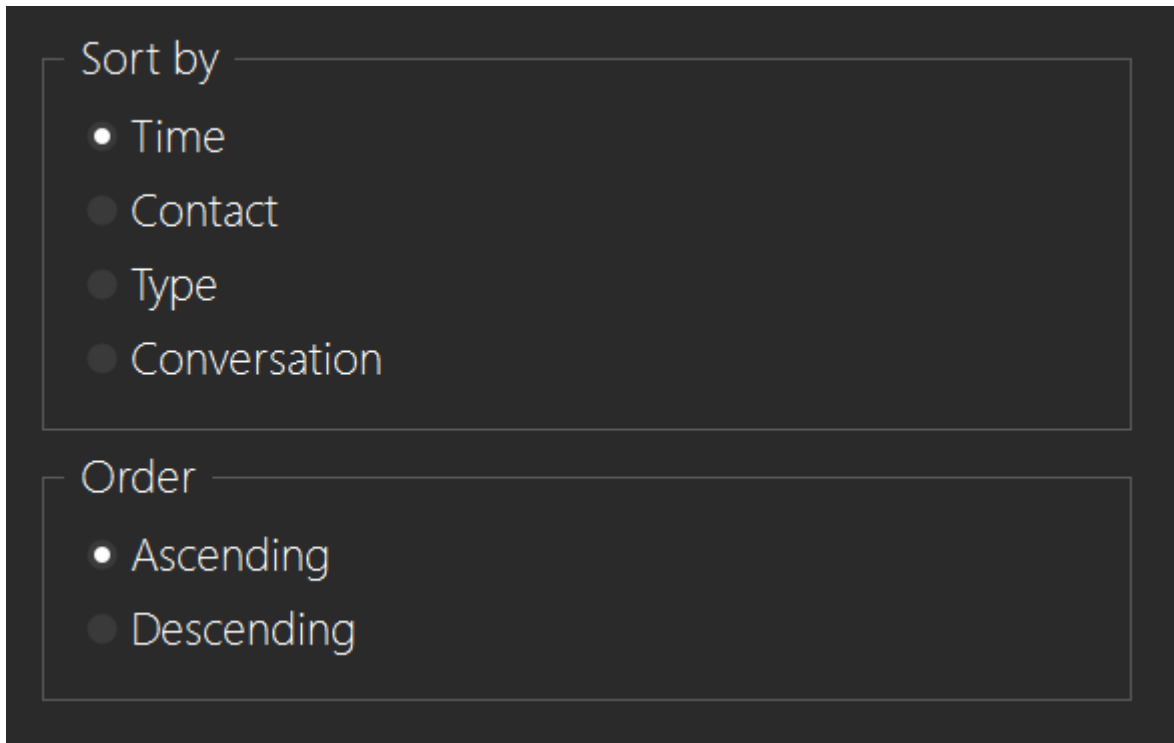
Deleted messages – this option turns on the recovery of deleted messages, wherever it is possible. Any recovered deleted messages are placed together with regular messages and are visibly marked as 'deleted'.

Conversations - displays phone messages in the conversation view only, which is a shorter format; but please note that it is possible that not all available information stored in the messages may be displayed.

Detailed messages - shows messages with all details, without the conversations.

Both – shows the conversations followed by the detailed messages.

6.7.1 The display order of messages



Messages in the report can be ordered by:

- Time, which sorts by the time and date they were sent or received
- Contact name in the message
- Type of the message, such as sent or received
- The conversation that the message is included in

To see examples of what reports will look like, based on various settings, go to the Report in the details section.

6.7.2 Example of messages report:

Case Label: Kentucky church

Case Evidence Number: 8974969-589-468

Device Label:

Conversations (74 conversations, 543 messages, 15 deleted)

All phone and application conversations, sorted by time in descending order

* Entries marked with asterisk are cross-referenced from phone contacts

Legend:

Sent message
Received message
Draft
Failed message
Unknown message
Deleted message*

1 +420722165520

Last Activity 2018-05-31 14:23:00 (UTC+2)


Participants +420722165520, me

	Hey how are you today?	2018-05-24 14:13:54 (UTC+2)
+420722165520	Not feeling too good, hbu?	2018-05-24 14:14:13 (UTC+2)
+420722165520	Same here	2018-05-24 14:15:06 (UTC+2)
+420722165520	I really hate my ringtone	2018-05-24 14:15:22 (UTC+2)
+420722165520	So what? just change it	2018-05-24 14:15:46 (UTC+2)
+420722165520	I don't want to	2018-05-31 13:30:22 (UTC+2)
+420722165520	So you hate it but you don't want to change it?	2018-05-31 13:31:10 (UTC+2)
+420722165520	Exactly. I love the way it irritates me	2018-05-31 13:31:39 (UTC+2)
+420722165520	What is wrong with you?	2018-05-31 13:32:04 (UTC+2)
+420722165520	I'm a truly broken human being	2018-05-31 13:39:37 (UTC+2)
+420722165520	You should see someone about that	2018-05-31 13:42:17 (UTC+2)
+420722165520	I won't	2018-05-31 13:48:00 (UTC+2)
+420722165520	I know that	2018-05-31 14:01:35 (UTC+2)
+420722165520	This conversation is utterly meaningless	2018-05-31 14:01:54 (UTC+2)
+420722165520	Indeed	2018-05-31 14:19:44 (UTC+2)
+420722165520	Why are we even talking to each other?	2018-05-31 14:20:20 (UTC+2)
+420722165520	Because they need some report messages	2018-05-31 14:20:50 (UTC+2)
+420722165520	Are we getting paid for this tho?	2018-05-31 14:21:10 (UTC+2)

6/20/2018 12:50 PM

Generated by Compelson MOBILedit Forensic Express 5.3.0.12966

56/2537

 Keep in mind that if you will filter, for example, the messages by content: "**Hi**" you will get even words that have the word Hi in them... for example a word: **this**

6.8 Data - Emails

Emails section, if enabled, shows all email messages from all sources, merged into one list. The sources are typically email applications from the phone, and if it's possible you can also get deleted emails.

- Phone emails
- Application emails
- Deleted emails

Sort by

- Time
- Contact
- Type
- Conversation

Order

- Ascending
- Descending

Filter by time

Start:

2000-01-01 00:00



End:

2016-09-26 23:59



Filter by contact

Enter name, email, or ID. Separate multiple contacts with semicolons

Filter by email content

Separate multiple items with semicolons

Please note, that many applications (such as Gmail or default email apps) store their data online. In such cases, it is not possible to obtain the full body of the email, because it is simply not available on the phone itself and no forensic software gets access to online storages of Google etc. In these cases, only basic information about the email (sender, receiver, date, time, header and maybe a part of the body) is obtained.

6.8.1 Example of email report:









Case Label: Kentucky church

Case Evidence Number: 8974969-589-468

Device Label:

Emails (24 total, 12 deleted)

All application emails, sorted by time in ascending order

1		1971-12-02 00:40:45 (UTC+1)	Unknown															
<table border="1"> <tr> <td>Display Name</td> <td>James Compelson</td> </tr> <tr> <td>From</td> <td>ions.yahoo.com>\Yahoo@communications.yah</td> </tr> <tr> <td>To</td> <td>oo.com\Yahoo Mailvalentine.v</td> </tr> <tr> <td>Reply To</td> <td>eryrich@yahoo.comreplies@communi</td> </tr> <tr> <td>Subject</td> <td>Yahoo Mail\T\Richmond, comple</td> </tr> <tr> <td>Source</td> <td>Email</td> </tr> <tr> <td>Source File</td> <td>phone/applications0/com.android.email/live_data/databases/EmailProvider.db : 0x7AD5 (Table: Message_Deletes)</td> </tr> </table>					Display Name	James Compelson	From	ions.yahoo.com>\Yahoo@communications.yah	To	oo.com\Yahoo Mailvalentine.v	Reply To	eryrich@yahoo.comreplies@communi	Subject	Yahoo Mail\T\Richmond, comple	Source	Email	Source File	phone/applications0/com.android.email/live_data/databases/EmailProvider.db : 0x7AD5 (Table: Message_Deletes)
Display Name	James Compelson																	
From	ions.yahoo.com>\Yahoo@communications.yah																	
To	oo.com\Yahoo Mailvalentine.v																	
Reply To	eryrich@yahoo.comreplies@communi																	
Subject	Yahoo Mail\T\Richmond, comple																	
Source	Email																	
Source File	phone/applications0/com.android.email/live_data/databases/EmailProvider.db : 0x7AD5 (Table: Message_Deletes)																	
2		1973-05-21 19:04:24 (UTC+2)	Unknown															
<table border="1"> <tr> <td>To</td> <td>Sophia Compelson</td> </tr> <tr> <td>Source</td> <td>Gmail</td> </tr> <tr> <td>Source File</td> <td>phone/applications0/com.google.android.gm/live_data/databases/mailstore.james.compelson@gmail.com.db : 0x451AB (Table: messages)</td> </tr> </table>					To	Sophia Compelson	Source	Gmail	Source File	phone/applications0/com.google.android.gm/live_data/databases/mailstore.james.compelson@gmail.com.db : 0x451AB (Table: messages)								
To	Sophia Compelson																	
Source	Gmail																	
Source File	phone/applications0/com.google.android.gm/live_data/databases/mailstore.james.compelson@gmail.com.db : 0x451AB (Table: messages)																	
3	 Dropbox <no-reply@dropbox.com>	2015-10-14 12:34:59 (UTC+2)	Received															
<p>Download Dropbox on your computer to complete your setup! Download Dropbox Sa...</p> <table border="1"> <tr> <td>Subject</td> <td>Download Dropbox on your computer!</td> </tr> <tr> <td>To</td> <td><james.compelson@gmail.com></td> </tr> <tr> <td>Source</td> <td>Gmail</td> </tr> <tr> <td>Source File</td> <td>phone/applications0/com.google.android.gm/live_data/databases/mailstore.james.compelson@gmail.com.db : 0x70FB (Table: messages)</td> </tr> </table>					Subject	Download Dropbox on your computer!	To	<james.compelson@gmail.com>	Source	Gmail	Source File	phone/applications0/com.google.android.gm/live_data/databases/mailstore.james.compelson@gmail.com.db : 0x70FB (Table: messages)						
Subject	Download Dropbox on your computer!																	
To	<james.compelson@gmail.com>																	
Source	Gmail																	
Source File	phone/applications0/com.google.android.gm/live_data/databases/mailstore.james.compelson@gmail.com.db : 0x70FB (Table: messages)																	
4	 Dropbox <no-reply@dropbox.com>	2015-10-14 12:35:52 (UTC+2)	Received															
<p>Hi James, You've connected a new app, 'Samsung Device', to your Dropbox. You ...</p> <table border="1"> <tr> <td>Subject</td> <td>You've connected a new app to Dropbox</td> </tr> <tr> <td>To</td> <td><james.compelson@gmail.com></td> </tr> <tr> <td>Source</td> <td>Gmail</td> </tr> <tr> <td>Source File</td> <td>phone/applications0/com.google.android.gm/live_data/databases/mailstore.james.compelson@gmail.com.db : 0x7773 (Table: messages)</td> </tr> </table>					Subject	You've connected a new app to Dropbox	To	<james.compelson@gmail.com>	Source	Gmail	Source File	phone/applications0/com.google.android.gm/live_data/databases/mailstore.james.compelson@gmail.com.db : 0x7773 (Table: messages)						
Subject	You've connected a new app to Dropbox																	
To	<james.compelson@gmail.com>																	
Source	Gmail																	
Source File	phone/applications0/com.google.android.gm/live_data/databases/mailstore.james.compelson@gmail.com.db : 0x7773 (Table: messages)																	

6.9 Data - Calls

- Phone call logs
- Application call logs
- Deleted calls

Phone call logs – all the standard calls from the phone.

Application call logs – if selected it will merge all calls retrieved from any application analysis into the main section.

Deleted calls – turns on the recovery of deleted entries from the call logs.

6.9.1 Example of call logs report:

Case Label: Kentucky church

Case Evidence Number: 8974969-589-468

Device Label:

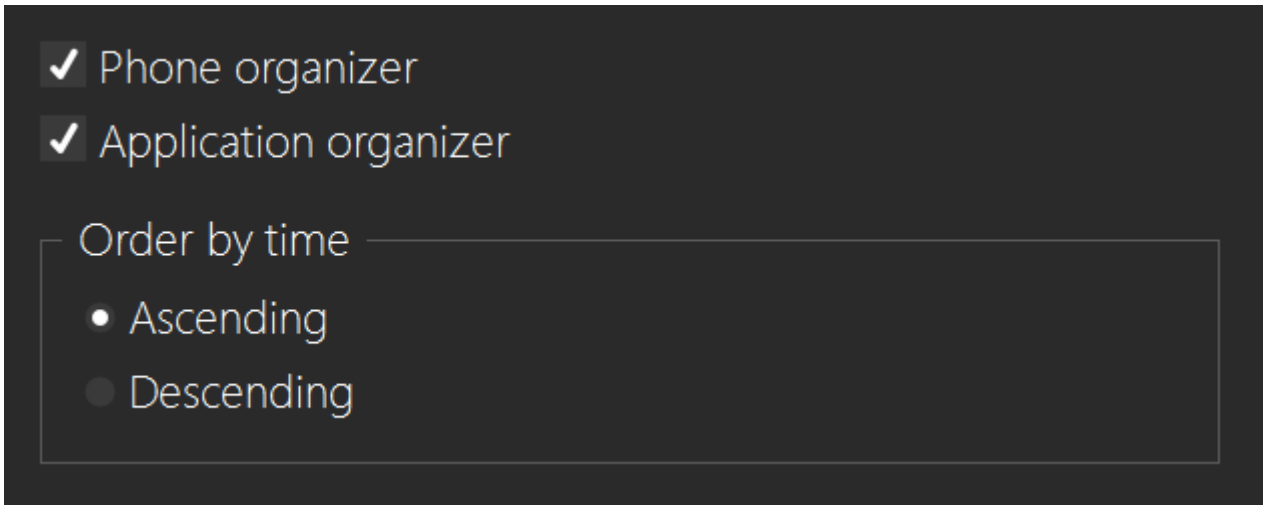
Calls (18 total, 2 deleted)

All phone and application calls, sorted by time in ascending order

* Entries marked with asterisk are cross-referenced from phone contacts

Label	From	To	Time	Duration
1	Mum	+16432888756	2013-12-30 11:52:06 (UTC+1)	00:00:42
2	Sophia	+15983698569	2013-12-31 13:42:45 (UTC+1)	00:00:30
3	Sophia Compelson (Sophia Compelson)		2015-10-15 11:43:03 (UTC+2)	
Source		Account: James Compelson		
Source File		phone/applications0/com.google.android.talk/live_data/databases/babel1.db : 0xCF5B (Table: messages)		
4	Sophia Compelson (Sophia Compelson)		2015-10-15 11:50:36 (UTC+2)	
Source		Account: James Compelson		
Source File		phone/applications0/com.google.android.talk/live_data/databases/babel1.db : 0xCEB6 (Table: messages)		
5	Megan Brandt (Megan Brandt)		2016-04-15 16:05:23 (UTC+2)	00:00:45
Source		WhatsApp		
Source File		phone/applications0/com.whatsapp/live_data/databases/msgstore.db : 0x636BC (Table: messages)		
Source File		phone/applications0/com.whatsapp/live_data/databases/wa.db (Table: wa_contacts)		
6		+420732402612 (Megan Brandt)	2016-04-15 16:35:17 (UTC+2)	00:00:00
Source		Viber		
Source File		phone/applications0/com.viber.voip/live_data/databases/viber_data : 0x21CB (Table: calls)		
7		+420732402612 (Megan Brandt)	2016-04-15 16:36:38 (UTC+2)	00:00:27
Source		Viber		
Source File		phone/applications0/com.viber.voip/live_data/databases/viber_data : 0x2F3F (Table: calls)		
8		+420732402612 (Megan Brandt)	2016-04-15 16:36:38 (UTC+2)	00:00:27
Source		Viber		
Source File		phone/applications0/com.viber.voip/live_data/databases/viber_messages : 0x8FD4 (Table: messages_calls)		
9	Sophia	+15983698569	2017-01-02 12:39:12 (UTC+1)	00:00:00
10	Lisa	+15423698569 (Lisa Cahow)*	2017-01-02 13:35:55 (UTC+1)	00:00:41
11	Lisa	+15423698569 (Lisa Cahow)*	2017-01-02 15:37:47 (UTC+1)	00:02:30
12	Sister	+13498398732	2017-01-04 15:07:15 (UTC+1)	00:01:07
13	Sister	+13498398732	2017-01-10 20:15:15 (UTC+1)	00:00:00
14	Sophia	+15983698569	2017-01-24 17:18:51 (UTC+1)	00:00:00
15		+420226889618	2017-01-30 10:52:13 (UTC+1)	00:00:00
16	Chose Martinez	+18654698559	2018-03-02 03:23:11 (UTC+1)	00:00:29
17	James Doormann	+17494698369	2018-06-01 23:05:15 (UTC+2)	00:03:31
18		+420564778118	2018-11-03 13:50:13 (UTC+1)	00:00:00

6.10 Data - Organizer



Phone organizer – retrieves available items (events, tasks, notes) from the standard phone organizer.

Application organizer – merges also organizer items retrieved from the application data. Organizer entries can be sorted by time in the ascending or the descending order.

6.10.1 Example of organizer report:

Case Label: Kentucky church

Case Evidence Number: 8974969-589-468

Device Label:

List of Calendars (7 total, 2 deleted)

1	Deleted	
Type	com.android.huawei.phone	
Account	phone	
Source File	phone/applications0/com.android.providers.calendar/live_data/databases/calendar.db : 0x7B42 (Table: Calendars)	
2 Phone		
Owner	Phone	
Time Zone	GMT	
Type	com.android.huawei.phone	
Account	Phone	
Source File	phone/applications0/com.android.providers.calendar/live_data/databases/calendar.db : 0x7F9E (Table: Calendars)	
3 Birthday calendar		
Owner	Phone	
Time Zone	GMT	
Type	com.android.huawei.birthday	
Account	Phone	
Source File	phone/applications0/com.android.providers.calendar/live_data/databases/calendar.db : 0x7DCD (Table: Calendars)	
4		Deleted
Contacts		
Owner	#contacts@group.v.calendar.google.com	
Time Zone	UTC	
Type	com.google	
Account	compelson.report@gmail.com	
Associated Events	7	
Source File	phone/applications0/com.android.providers.calendar/live_data/databases/calendar.db : 0x7B30 (Table: Calendars)	
5 compelson.report@gmail.com		
Owner	compelson.report@gmail.com	
Time Zone	UTC	
Type	com.google	
Account	compelson.report@gmail.com	
Source File	phone/applications0/com.android.providers.calendar/live_data/databases/calendar.db : 0x7E52 (Table: Calendars)	

Case Label: Kentucky church

Case Evidence Number: 8974969-589-468

Device Label:

Events (9 total, 7 deleted)

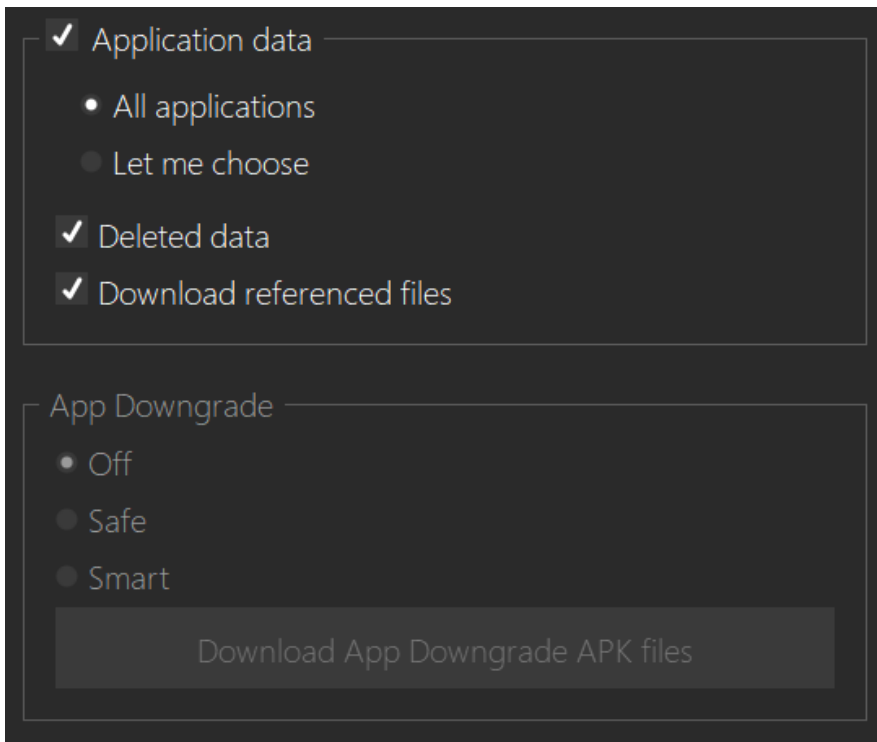
All phone and application organizer events, sorted by time in ascending order

Type	Start	End	Recurrence
1 Regular	2018-04-23 02:00:00 (UTC+2)		Yearly
Label	Testname Testmiddle Testsurname		
Calendar	Testname Testmiddle Testsurname		
Duration	1 day		
Time Zone	UTC		
Reminder	Notification -540 minutes before		
Reminder	Notification 9540 minutes before		
Source File	phone/applications0/com.android.providers.calendar/live_data/databases/calendar.db : 0x21513 (Table: Attendees, Calendars, Events, Reminders)		
2 Regular	2018-04-23 02:00:00 (UTC+2)		Yearly
Label	Testname Testmiddle Testsurname		
Calendar	Testname Testmiddle Testsurname		
Duration	1 day		
Time Zone	UTC		
Reminder	Notification -540 minutes before		
Reminder	Notification 9540 minutes before		
Source File	phone/applications0/com.android.providers.calendar/live_data/databases/calendar.db : 0x21436 (Table: Attendees, Calendars, Events, Reminders)		
3			Deleted
Label	2018_BIRTHDAY_71980f498da7f2f9		
Calendar ID	4		
Name	Rozanne Elvis		
Type	BIRTHDAY		
Email	e.rozanne@gmail.com		
Id	116195449015101104533		
Picture Url	https://calendar.google.com/googlecalendar/images/cake.gif		
Source	Calendar		
Source File	phone/applications0/com.google.android.calendar/live_data/databases/timelydata.db : 0x39DC (Table: timelydata)		
4			Deleted

6.11 Data - Applications

6.11.1 Applications

Application data – retrieves and processes data of applications. Results of the app analysis are shown in the reports, and the raw application data are also stored in the export folder, which makes additional processing and analysis possible.



All applications – will process all available application data from the phone.

Let me choose – if selected then when you press 'Next' to continue, it will show a list of all apps and you will be able to select only the ones that you want to process.

Deleted data – turns on a recovery of the deleted application data.

Download referenced files - download the referenced files from the chat message stored online.

App Downgrade – more detailed information is available [here\(see page 408\)](#).

6.11.2 App downgrade feature

Second, is to use MOBILedit Forensic Express ´s feature called "App downgrade". This will cause the apps to resort to a previous version, where vulnerabilities are present allowing access to data that otherwise would be unattainable. Find more about the App downgrade feature [here\(see page 408\)](#).

Example of applications report:

Case Label: Kentucky church

Case Evidence Number: 8974969-589-468

Device Label:

Applications (24)

Any.do

Label	Any.do
Package	com.anydo
Version	4.9.5.1
Application Type	User Application
Application Size	29.3 MB
Cache Size	0 B
First Installed	2018-04-13 11:51:59 (UTC+2)
Last Updated	2018-05-25 13:14:33 (UTC+2)

Contacts (2 total, 2 deleted)

1 Josef Compelson Deleted	
Email	compelson.test@gmail.com
Picture Url	https://graph.facebook.com/774783652638151/picture?height=200&type=normal&width=200
Source File	phone/applications0/com.anydo/live_data/databases/data : 0x23F54 (Table: shared_list_members)
2 Josefine Compelson Deleted	
Email	another.compelson.test@gmail.com
Picture Url	https://lh3.googleusercontent.com/cg313GcmClg/AAAAAAAAAAI/AAAAAAAAARTc/lbhFCInnx_g/photo.jpg
Source File	phone/applications0/com.anydo/live_data/databases/data : 0x23E68 (Table: shared_list_members)

Personal (9)

1 Go shopping Completed Normal				
Owner	compelson.report@gmail.com			
Created	Modified	Due	Reminder	Removed
2018-06-07 14:45:03 (UTC+2)	2018-06-07 16:28:13 (UTC+2)	2018-06-07 13:52:03 (UTC+2)	-	-
Source File	phone/applications0/com.anydo/live_data/databases/data : 0xCE93 (Table: anydo_tasks)			

6/20/2018 12:51 PM

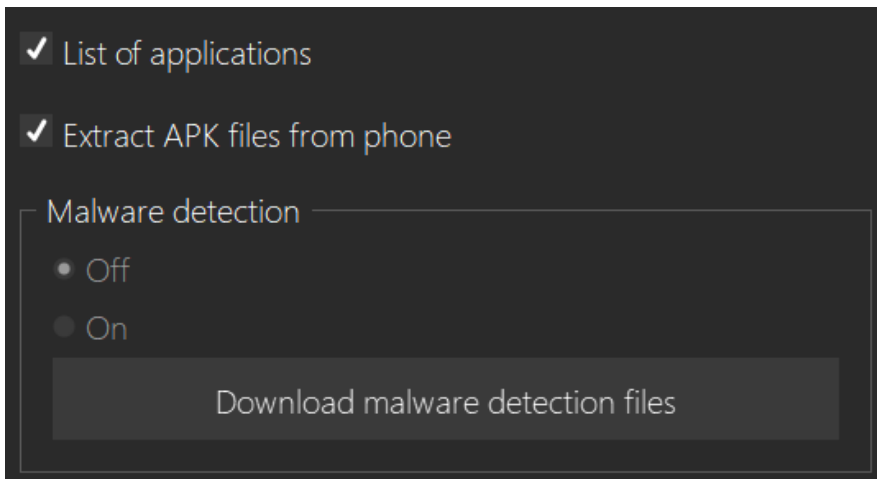
Generated by Compelson MOBILedit Forensic Express 5.3.0.12966

1113/2537

6.12 Data - Application list

6.12.1 List of applications

List of all applications located in your device.




6.12.2 Extract APK files from the phone

Does extract additional APK installation files from your device.

6.12.3 Malware detection

Check the extracted application APK files for malware. This information is displayed in the report under each application section or application.

 To download Malware detection add-on click [here](#)⁸⁴.

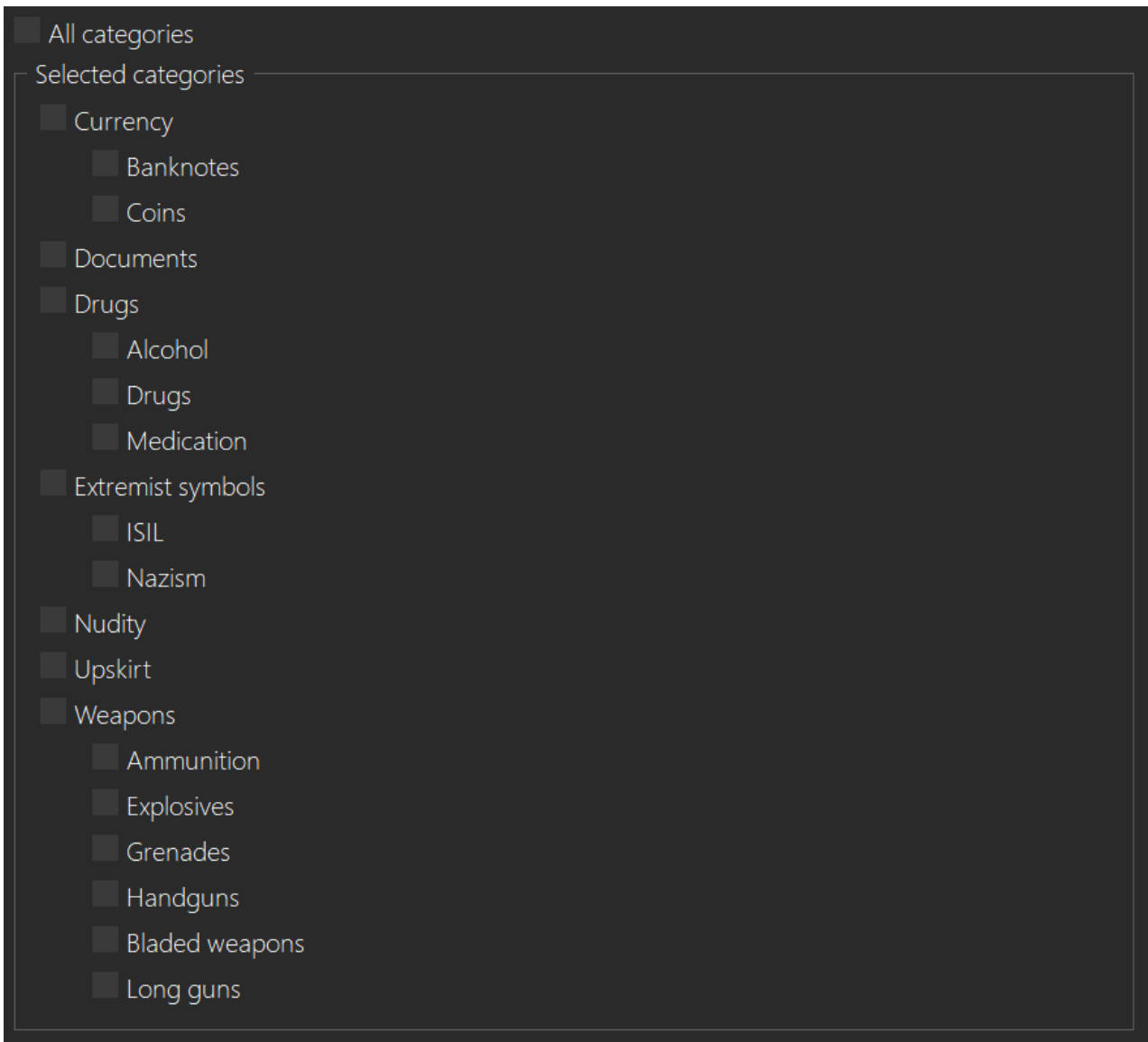
6.13 Data - Photo recognizer

This feature offers a photo analysis from device or folder on a PC disk. The report will consist of photos tagged and sorted into categories.

The analysis is powered by artificial intelligence module utilizing machine learning to automatically recognize suspicious content in photos such as drugs, nudity, weapons, currency and documents.

This feature is available for unlimited license and classifies images into these categories:

⁸⁴ <http://download.mobiledit.com/pfe/AppengineScripts/latestMWD.package>



Photos can be filtered and sorted by the following criteria:

Analyze all image files
 Analyze only photos in media folders
 Analyze only application images

Sort by

Filename
 Full path
 Time

Order

Ascending
 Descending

Filter by time

Start: 2000-01-01 00:00
End: 2019-11-29 23:59

Filter by file name or path

Separate multiple items with semicolons

Filter by location

Latitude: 0.0
Longitude: 0.0
Distance (meters): 1000

Enter coordinates as decimal numbers

When you use the Photo recognizer feature, your images in the report will be classified like the examples below:

129 Table Tennis Power.jpg



Path	phone/raw0/other/Table Tennis Power.jpg
Size	45.5 kB
Created	2017-04-28 15:02:30 (UTC+2)
Modified	2017-04-27 11:22:36 (UTC+2)
Accessed	2017-04-28 15:02:30 (UTC+2)
Width	500 px
Height	284 px
Image Classification	Other

107 bing_000020.jpg1493118181.1752536.jpg



Path	phone/raw0/weapons-knife/bing_000020.jpg1493118181.1752536.jpg
Size	36.9 kB
Created	2017-04-28 15:04:59 (UTC+2)
Modified	2017-04-25 10:30:45 (UTC+2)
Accessed	2017-04-28 15:04:59 (UTC+2)
Width	600 px
Height	303 px
Image Classification	Weapons - Knife

101 bing_000177.jpg



Path	phone/raw0/currency-coins/bing_000177.jpg
Size	258.1 kB
Created	2017-04-28 15:08:16 (UTC+2)
Modified	2017-04-24 15:57:46 (UTC+2)
Accessed	2017-04-28 15:08:16 (UTC+2)
Width	1600 px
Height	1200 px
Image Classification	Currency - Coins

1 **bing_000028.jpg**

Path	phone/raw0/weapons-ammunition/bing_000028.jpg
Size	67.5 kB
Created	2017-04-28 15:06:22 (UTC+2)
Modified	2017-04-21 14:14:42 (UTC+2)
Accessed	2017-04-28 15:06:22 (UTC+2)
Width	1398 px
Height	786 px
Camera Manufacturer	Minolta Co., Ltd.
Camera Model	DiIMAGE 5
Date of Generation	2004-06-09 03:35:25 (unknown time zone)
Date of Digitization	2004-06-09 03:35:25 (unknown time zone)
Focal Length	13.062 mm
Image Classification	Weapons - Ammunition

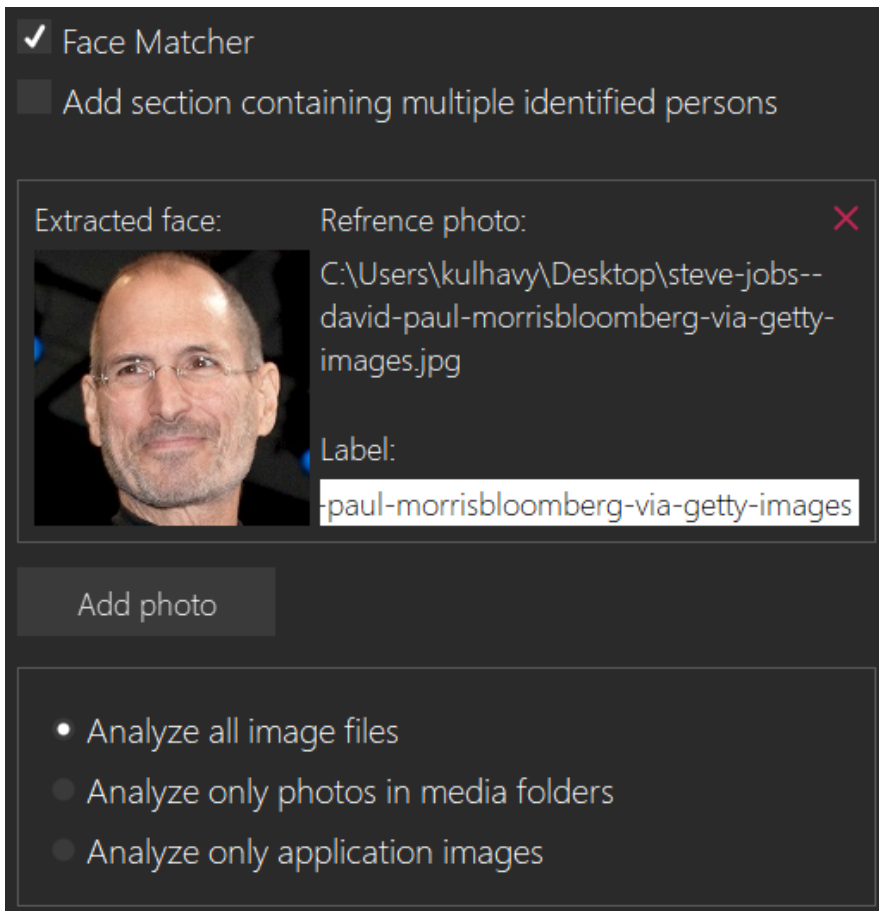
i Please note that the Photo analyzer feature is available ONLY in the Unlimited license of MOBILedit Forensic Express.

6.14 Data - Face Matcher

With this feature **MOBILedit Forensic Express** is able to find photos with faces and compare them with provided source images.

This comes in handy when you need to quickly find photos of a specific person in the investigated phones. The source image can be chosen from any folder or phone you like. The report will consist of photos matched with the reference images added before the process begins. The Face Matcher analysis is powered by an artificial intelligence module.

Below you can see the **Face Matcher** set up a screen with step by step description:



Face matcher - check the box to activate

Add section containing multiple identified persons - each photo will be stored in its own section

Add photo - allows you to pick one or multiple photos of the desired face

Analyze all image files - every image from the device will be compared to the

Analyze only photos in media folders - the search would be only applied to media folders

Analyze only application images - the search would be only applied to application data

The outcome can be sorted and filtered by the following criteria:

- Analyze all image files
- Analyze only photos in media folders
- Analyze only application images

Sort by

- Filename
- Full path
- Time

Order

- Ascending
- Descending

Filter by time

Start:

End:

Filter by file name or path

Separate multiple items with semicolons

Filter by location


Latitude:


Longitude:


Distance (meters):


Enter coordinates as decimal numbers

When you use the Face Matcher feature, your images in the report will be classified like the examples below:

16 23.jpg																					
	<table border="1"> <tr><td>Filename</td><td>23.jpg</td></tr> <tr><td>Path</td><td>phone/raw0/Nikal/23.jpg</td></tr> <tr><td>Size</td><td>25 kB</td></tr> <tr><td>Created</td><td>2018-03-27 09:24:59 (UTC+2)</td></tr> <tr><td>Modified</td><td>2018-03-02 11:06:51 (UTC+1)</td></tr> <tr><td>Accessed</td><td>2018-03-27 09:24:59 (UTC+2)</td></tr> <tr><td>SHA-256 hash</td><td>932C760007C2A77C36C19A3C18C2B12877A2AZ2B3B6654D88F42696A88A4D52A</td></tr> <tr><td>Width</td><td>537 px</td></tr> <tr><td>Height</td><td>554 px</td></tr> <tr><td>Matched Face Path</td><td>D:\FMMMAIN\Nikal.jpg</td></tr> </table>	Filename	23.jpg	Path	phone/raw0/Nikal/23.jpg	Size	25 kB	Created	2018-03-27 09:24:59 (UTC+2)	Modified	2018-03-02 11:06:51 (UTC+1)	Accessed	2018-03-27 09:24:59 (UTC+2)	SHA-256 hash	932C760007C2A77C36C19A3C18C2B12877A2AZ2B3B6654D88F42696A88A4D52A	Width	537 px	Height	554 px	Matched Face Path	D:\FMMMAIN\Nikal.jpg
Filename	23.jpg																				
Path	phone/raw0/Nikal/23.jpg																				
Size	25 kB																				
Created	2018-03-27 09:24:59 (UTC+2)																				
Modified	2018-03-02 11:06:51 (UTC+1)																				
Accessed	2018-03-27 09:24:59 (UTC+2)																				
SHA-256 hash	932C760007C2A77C36C19A3C18C2B12877A2AZ2B3B6654D88F42696A88A4D52A																				
Width	537 px																				
Height	554 px																				
Matched Face Path	D:\FMMMAIN\Nikal.jpg																				

17 26.jpg																					
	<table border="1"> <tr><td>Filename</td><td>26.jpg</td></tr> <tr><td>Path</td><td>phone/raw0/Nikal/26.jpg</td></tr> <tr><td>Size</td><td>25.4 kB</td></tr> <tr><td>Created</td><td>2018-03-27 09:24:59 (UTC+2)</td></tr> <tr><td>Modified</td><td>2018-03-02 11:08:57 (UTC+1)</td></tr> <tr><td>Accessed</td><td>2018-03-27 09:24:59 (UTC+2)</td></tr> <tr><td>SHA-256 hash</td><td>68952A3BF713E142F8096203D6B196A487DAD12BF9BC50E11F027A5213983</td></tr> <tr><td>Width</td><td>398 px</td></tr> <tr><td>Height</td><td>386 px</td></tr> <tr><td>Matched Face Path</td><td>D:\FMMMAIN\Nikal.jpg</td></tr> </table>	Filename	26.jpg	Path	phone/raw0/Nikal/26.jpg	Size	25.4 kB	Created	2018-03-27 09:24:59 (UTC+2)	Modified	2018-03-02 11:08:57 (UTC+1)	Accessed	2018-03-27 09:24:59 (UTC+2)	SHA-256 hash	68952A3BF713E142F8096203D6B196A487DAD12BF9BC50E11F027A5213983	Width	398 px	Height	386 px	Matched Face Path	D:\FMMMAIN\Nikal.jpg
Filename	26.jpg																				
Path	phone/raw0/Nikal/26.jpg																				
Size	25.4 kB																				
Created	2018-03-27 09:24:59 (UTC+2)																				
Modified	2018-03-02 11:08:57 (UTC+1)																				
Accessed	2018-03-27 09:24:59 (UTC+2)																				
SHA-256 hash	68952A3BF713E142F8096203D6B196A487DAD12BF9BC50E11F027A5213983																				
Width	398 px																				
Height	386 px																				
Matched Face Path	D:\FMMMAIN\Nikal.jpg																				

18 27.jpg																					
	<table border="1"> <tr><td>Filename</td><td>27.jpg</td></tr> <tr><td>Path</td><td>phone/raw0/Nikal/27.jpg</td></tr> <tr><td>Size</td><td>37.5 kB</td></tr> <tr><td>Created</td><td>2018-03-27 09:24:59 (UTC+2)</td></tr> <tr><td>Modified</td><td>2018-03-02 11:09:03 (UTC+1)</td></tr> <tr><td>Accessed</td><td>2018-03-27 09:24:59 (UTC+2)</td></tr> <tr><td>SHA-256 hash</td><td>5DABD54F9CFCB5C7D0DD630D50E616EDA06480DD42AB31E31959964A946E267</td></tr> <tr><td>Width</td><td>363 px</td></tr> <tr><td>Height</td><td>394 px</td></tr> <tr><td>Matched Face Path</td><td>D:\FMMMAIN\Nikal.jpg</td></tr> </table>	Filename	27.jpg	Path	phone/raw0/Nikal/27.jpg	Size	37.5 kB	Created	2018-03-27 09:24:59 (UTC+2)	Modified	2018-03-02 11:09:03 (UTC+1)	Accessed	2018-03-27 09:24:59 (UTC+2)	SHA-256 hash	5DABD54F9CFCB5C7D0DD630D50E616EDA06480DD42AB31E31959964A946E267	Width	363 px	Height	394 px	Matched Face Path	D:\FMMMAIN\Nikal.jpg
Filename	27.jpg																				
Path	phone/raw0/Nikal/27.jpg																				
Size	37.5 kB																				
Created	2018-03-27 09:24:59 (UTC+2)																				
Modified	2018-03-02 11:09:03 (UTC+1)																				
Accessed	2018-03-27 09:24:59 (UTC+2)																				
SHA-256 hash	5DABD54F9CFCB5C7D0DD630D50E616EDA06480DD42AB31E31959964A946E267																				
Width	363 px																				
Height	394 px																				
Matched Face Path	D:\FMMMAIN\Nikal.jpg																				

 Please note that the Face Matcher feature is available ONLY in the Unlimited license of MOBILedit Forensic Express.

6.15 Data - Photos

This selection provides you with photos from your device - no other images. Usually found in the DCIM folder. If available, the report will provide geo-location information. You can filter the report by time, file name or location and choose between ascending and descending order:

Photos from the phone

Show photos as

- Grid view
- Detailed photos
- Show advanced metadata

Sort by

- Filename
- Full path
- Time

Order

- Ascending
- Descending

Filter by time

Start:

End:

Filter by file name or path

Separate multiple items with semicolons

Filter by location

Latitude:

Longitude:


Distance (meters):

Enter coordinates as decimal numbers

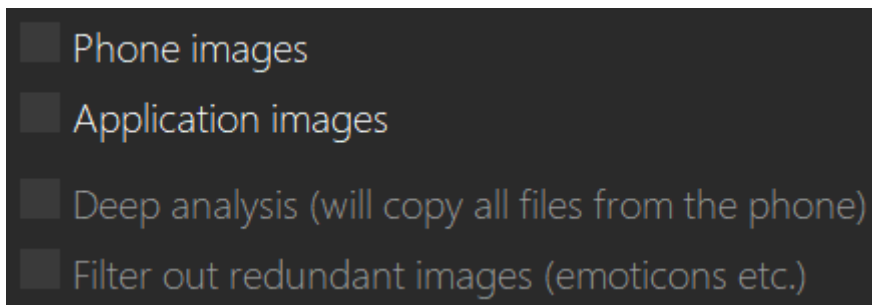
6.15.1 Example from the report:

Photos (36)

A subset of phone and application photos filtered by path not indicating a redundant image, sorted by time in ascending order

1 IMG_20190801_170605.jpg																																								
	<table border="1"> <tr> <td>Filename</td> <td>IMG_20190801_170605.jpg</td> </tr> <tr> <td>Path</td> <td>phone/raw3/DCIM/Camera/IMG_20190801_170605.jpg</td> </tr> <tr> <td>Size</td> <td>2.59 MB</td> </tr> <tr> <td>Modified</td> <td>2019-08-01 17:06:08 (UTC+2)</td> </tr> <tr> <td>Accessed</td> <td>2019-08-01 17:06:08 (UTC+2)</td> </tr> <tr> <td>SHA-256 hash</td> <td>188123E5EDB37104D65D820E467125C4A6004B89EC5308375BACD2E56AA39466</td> </tr> <tr> <td>Width</td> <td>3024 px</td> </tr> <tr> <td>Height</td> <td>4032 px</td> </tr> <tr> <td>Camera Manufacturer</td> <td>Google</td> </tr> <tr> <td>Camera Model</td> <td>Pixel 2</td> </tr> <tr> <td>Date of Generation</td> <td>2019-08-01 17:06:06 (UTC+2)</td> </tr> <tr> <td>Date of Digitization</td> <td>2019-08-01 17:06:06 (UTC+2)</td> </tr> <tr> <td rowspan="4">Position (Google Maps)</td> <td>Latitude</td> <td>50.10461 °</td> </tr> <tr> <td>Longitude</td> <td>14.47779 °</td> </tr> <tr> <td>Time</td> <td>2019-08-01 17:06:05 (UTC+2)</td> </tr> <tr> <td>Altitude</td> <td>254 m</td> </tr> <tr> <td>Exposure Time</td> <td>1 / 50 s</td> </tr> <tr> <td>Focal Length</td> <td>4.442 mm</td> </tr> <tr> <td>F-Number</td> <td>1.8</td> </tr> </table>	Filename	IMG_20190801_170605.jpg	Path	phone/raw3/DCIM/Camera/IMG_20190801_170605.jpg	Size	2.59 MB	Modified	2019-08-01 17:06:08 (UTC+2)	Accessed	2019-08-01 17:06:08 (UTC+2)	SHA-256 hash	188123E5EDB37104D65D820E467125C4A6004B89EC5308375BACD2E56AA39466	Width	3024 px	Height	4032 px	Camera Manufacturer	Google	Camera Model	Pixel 2	Date of Generation	2019-08-01 17:06:06 (UTC+2)	Date of Digitization	2019-08-01 17:06:06 (UTC+2)	Position (Google Maps)	Latitude	50.10461 °	Longitude	14.47779 °	Time	2019-08-01 17:06:05 (UTC+2)	Altitude	254 m	Exposure Time	1 / 50 s	Focal Length	4.442 mm	F-Number	1.8
Filename	IMG_20190801_170605.jpg																																							
Path	phone/raw3/DCIM/Camera/IMG_20190801_170605.jpg																																							
Size	2.59 MB																																							
Modified	2019-08-01 17:06:08 (UTC+2)																																							
Accessed	2019-08-01 17:06:08 (UTC+2)																																							
SHA-256 hash	188123E5EDB37104D65D820E467125C4A6004B89EC5308375BACD2E56AA39466																																							
Width	3024 px																																							
Height	4032 px																																							
Camera Manufacturer	Google																																							
Camera Model	Pixel 2																																							
Date of Generation	2019-08-01 17:06:06 (UTC+2)																																							
Date of Digitization	2019-08-01 17:06:06 (UTC+2)																																							
Position (Google Maps)	Latitude	50.10461 °																																						
	Longitude	14.47779 °																																						
	Time	2019-08-01 17:06:05 (UTC+2)																																						
	Altitude	254 m																																						
Exposure Time	1 / 50 s																																							
Focal Length	4.442 mm																																							
F-Number	1.8																																							

6.16 Data - Image files

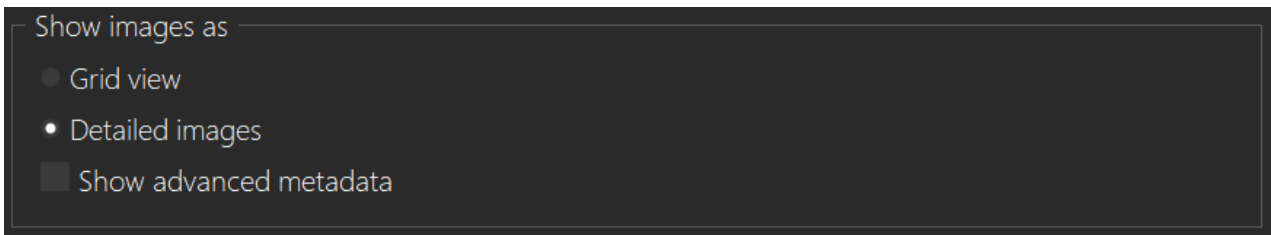


Phone images – all other images from the phone's file-system.

Application images – images retrieved from the application's data, which might also include images stored in temporary files or caches that has been detected as potential images.

Deep analysis – this option will copy all files from the phone (the same as the Full file-system option) and will perform analysis of all files to check whether they are actually image files.

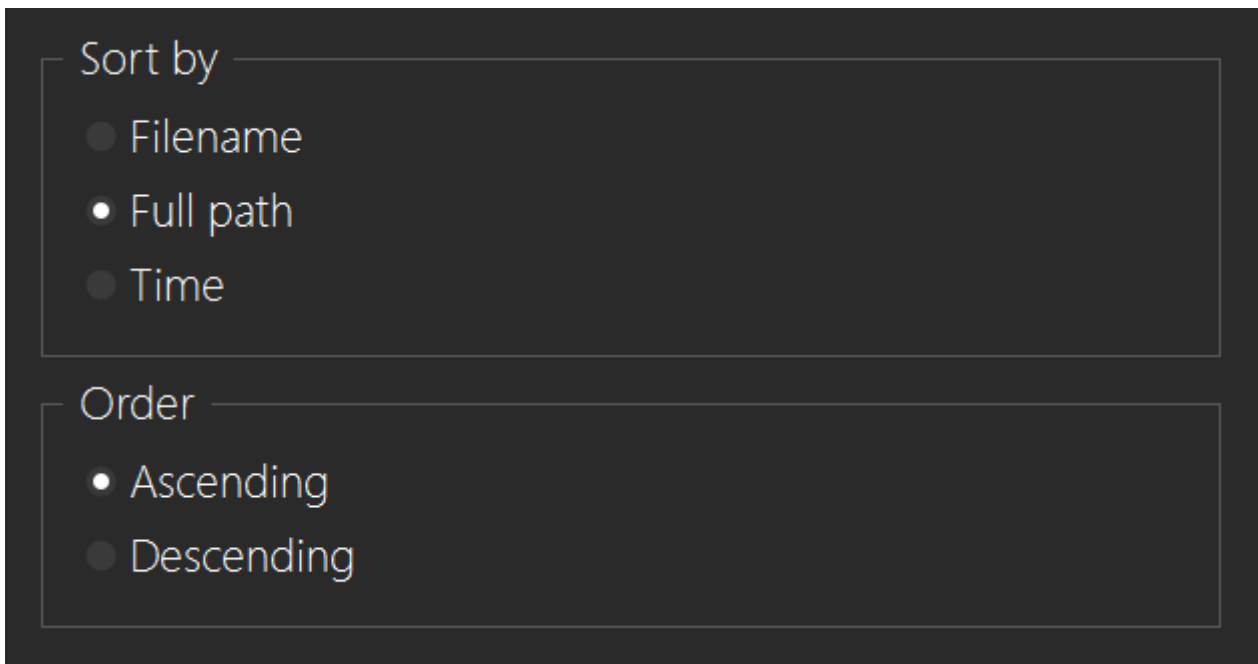
Filter out redundant images - will try to omit emojis and similar images from the reports, but these images will still be copied from the phone.



Grid view - tabular view of images

Detailed images - displays images one by one

Show advanced metadata - adds minor EXIF information such as lens info, which makes the text details longer



Files can be sorted by:

- Filename, which means only the name of the file, without its path, is used for sorting
- Full path of the file, including the location (folder) where the file was stored
- Time, of the creation or the last modification of the file


Images can be placed in ascending or descending order with any of the sort options available.

6.16.1 Example of images report with photo recognizer:

Recognized Images of Currency ⁽¹¹⁾

A subset of phone and application recognized images of currency filtered by path not indicating a redundant image, sorted by time in ascending order.

1 **bing_000180.jpg**




Filename	bing_000180.jpg
Path	phone/raw0/currency-coins/bing_000180.jpg
Size	102.6 kB
Created	2017-04-28 15:08:16 (UTC+2)
Modified	2017-04-24 15:57:47 (UTC+2)
Accessed	2017-04-28 15:08:16 (UTC+2)
SHA-256 hash	077CD757CD533C9F5F8FFCDA66B9BD1CBFA64E482407B669BBD5D592BEAE2CE
Width	570 px
Height	750 px
Camera Manufacturer	EASTMAN KODAK COMPANY
Camera Model	KODAK LS753 ZOOM DIGITAL CAMERA
Date of Generation	2011-01-19 00:35:35 (unknown time zone)
Date of Digitization	2011-01-19 00:35:35 (unknown time zone)
Exposure Time	1 / 60 s
Focal Length	6 mm
F-Number	3
Image Classification	Currency - Coins

Case Label: Kentucky church
Case Evidence Number: 8974969-589-468
Device Label:

Recognized Images of Documents ⁽⁹⁾

A subset of phone and application recognized images of documents filtered by path not indicating a redundant image, sorted by time in ascending order.

1 **oJRnCNaqM78mR4E0tkYAxh_-5B0.cnt**



Filename	oJRnCNaqM78mR4E0tkYAxh_-5B0.cnt
Path	phone/applications0/com.facebook.katana/live_data/cache/image/v2.ols100.1/4/oJRnCNaqM78mR4E0tkYAxh_-5B0.cnt
Size	49.1 kB
Modified	2018-05-31 13:38:00 (UTC+2)
Accessed	2018-05-31 13:38:00 (UTC+2)
SHA-256 hash	3D6765352781ED1957C9862E819EAC678CF623B19FA3B46E035EA1A92D3D38A2
Width	480 px
Height	800 px
Image Classification	Documents

Case Label: Kentucky church


Case Evidence Number: 8974969-589-468

Device Label:

Recognized Images of Drugs (24)

A subset of phone and application recognized images of drugs filtered by path not indicating a redundant image, sorted by time in ascending order.

1 **70126915_0a7dc99334_o_d.jpg**



Filename	70126915_0a7dc99334_o_d.jpg
Path	phone/raw0/drugs-alcohol/70126915_0a7dc99334_o_d.jpg
Size	53 kB
Created	2017-04-27 10:30:25 (UTC+2)
Modified	2017-04-27 09:42:01 (UTC+2)
Accessed	2017-04-27 10:30:25 (UTC+2)
SHA-256 hash	B7960072E82599E858BDF92A9CCCD594C5D562EB42C7F54BCD594E089056C689
Width	500 px
Height	332 px
Camera Manufacturer	NIKON CORPORATION
Camera Model	NIKON D70
Date of Generation	2005-12-03 22:39:38 (unknown time zone)
Date of Digitization	2005-12-03 22:39:38 (unknown time zone)
Exposure Time	1 / 30 s
Focal Length	35 mm
F-Number	2.8
Image Classification	Drugs - Alcohol

Case Label: Kentucky church


Case Evidence Number: 8974969-589-468

Device Label:

Recognized Images of Nudity (13)

A subset of phone and application recognized images of nudity filtered by path not indicating a redundant image, sorted by time in ascending order.

1 **bing_000018.jpg1493216851.9584255.jpg**



Filename	bing_000018.jpg1493216851.9584255.jpg
Path	phone/raw0/drugs-drugs/bing_000018.jpg1493216851.9584255.jpg
Size	25.6 kB
Created	2017-04-26 16:28:38 (UTC+2)
Modified	2017-04-26 12:51:25 (UTC+2)
Accessed	2017-04-26 16:28:38 (UTC+2)
SHA-256 hash	065F65CEBB8A6A41720DD5C74B0FCC6125AA65AFECE8786766B78E8EBCB0E1CE
Width	400 px
Height	344 px
Image Classification	Nudity - Nudity

Case Label: Kentucky church

Case Evidence Number: 8974969-589-468


Device Label:

Images with identified person "Dominika Myslivcova" ⁽⁴²⁾

A subset of phone and application Images with identified person "Dominika Myslivcova" reference photo path D:\FM\MAIN Dominika.JPG filtered by path not indicating a redundant image, sorted by time in ascending order.

Reference photo:



1 1.jpg																							
	<table border="1"> <tr> <td>Filename</td> <td>1.jpg</td> </tr> <tr> <td>Path</td> <td>phone/raw0/Dominika/1.jpg</td> </tr> <tr> <td>Size</td> <td>91.2 kB</td> </tr> <tr> <td>Created</td> <td>2018-03-27 09:24:57 (UTC+2)</td> </tr> <tr> <td>Modified</td> <td>2018-03-02 10:38:50 (UTC+1)</td> </tr> <tr> <td>Accessed</td> <td>2018-03-27 09:24:57 (UTC+2)</td> </tr> <tr> <td>SHA-256 hash</td> <td>7C00CB2D4E7087BB4731CECBD60F7BB9177D693F1B38512B6970AB1F5B7C27C5</td> </tr> <tr> <td>Width</td> <td>960 px</td> </tr> <tr> <td>Height</td> <td>720 px</td> </tr> <tr> <td>Matched Face Path</td> <td>D:\FM\MAIN Dominika.JPG</td> </tr> <tr> <td>Image Classification</td> <td>Other</td> </tr> </table>	Filename	1.jpg	Path	phone/raw0/Dominika/1.jpg	Size	91.2 kB	Created	2018-03-27 09:24:57 (UTC+2)	Modified	2018-03-02 10:38:50 (UTC+1)	Accessed	2018-03-27 09:24:57 (UTC+2)	SHA-256 hash	7C00CB2D4E7087BB4731CECBD60F7BB9177D693F1B38512B6970AB1F5B7C27C5	Width	960 px	Height	720 px	Matched Face Path	D:\FM\MAIN Dominika.JPG	Image Classification	Other
Filename	1.jpg																						
Path	phone/raw0/Dominika/1.jpg																						
Size	91.2 kB																						
Created	2018-03-27 09:24:57 (UTC+2)																						
Modified	2018-03-02 10:38:50 (UTC+1)																						
Accessed	2018-03-27 09:24:57 (UTC+2)																						
SHA-256 hash	7C00CB2D4E7087BB4731CECBD60F7BB9177D693F1B38512B6970AB1F5B7C27C5																						
Width	960 px																						
Height	720 px																						
Matched Face Path	D:\FM\MAIN Dominika.JPG																						
Image Classification	Other																						

6.17 Data - Large images

Additional section in the report showing one image per page in full size.

You can filter them by time, file name or location and choose between ascending and descending order.

Large images

Sort by

- Filename
- Full path
- Time

Order

- Ascending
- Descending

Filter by time

Start:

End:

Filter by file name or path

Separate multiple items with semicolons

Filter by location

Latitude:

Longitude:

Distance (meters):

Enter coordinates as decimal numbers

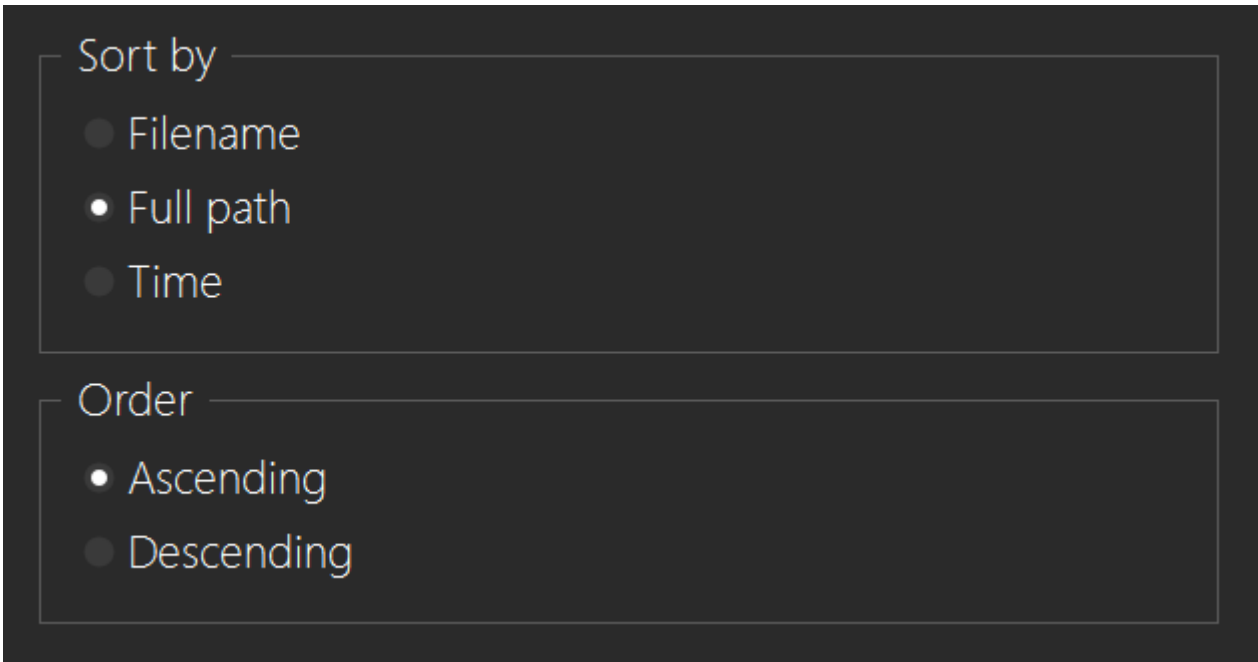
6.18 Data - Audio files

Phone audio files

Application audio files

Phone audio files – copies audio files from the phone and shows them in this report section.

Application audio files – includes also audio files retrieved from the applications.



Files can be sorted by:

- Filename, which means only the name of the file, without its path, is used for sorting
- The full path of the file, including the location (folder) where the file was stored
- Time, of the creation or the last modification of the file

Audio files can be placed in ascending or descending order with any of the sort options available.


6.18.1 Example of audio files report:

Case Label: Kentucky church Case Evidence Number: 8974969-589-468 Device Label:

Audio Files (10)

All phone and application audio files, sorted by time in ascending order

1 Over_the_horizon.mp3

	Filename	Over_the_horizon.mp3
	Path	phone/raw0/preload/INTERNAL_SDCARD/Samsung/Music/Over_the_horizon.mp3
	Size	2.6 MB
	Modified	2012-10-17 11:40:02 (UTC+2)
	SHA-256 hash	7E90D4B6DEE3AA5CC8219F4638BEB316217011610B2A38A00462D7ECEE20C262
	Name	Over the horizon
	Artist	Samsung
	Album	Samsung
	Genre	New Age
	Duration	00:02:36

6.19 Data - Video files

Phone video files
 Application video files
 Generate thumbnails
 Generate storyboard

- Fixed image count
 - Number of images: 12
 - Interval (mm:ss): 00:10
 - Maximum number of images: 2000
- Fixed time interval
 - Interval (mm:ss): 00:10
 - Maximum number of images: 2000

Phone video files – retrieves video files from the phone.

Application video files – includes video files stored in the application data.

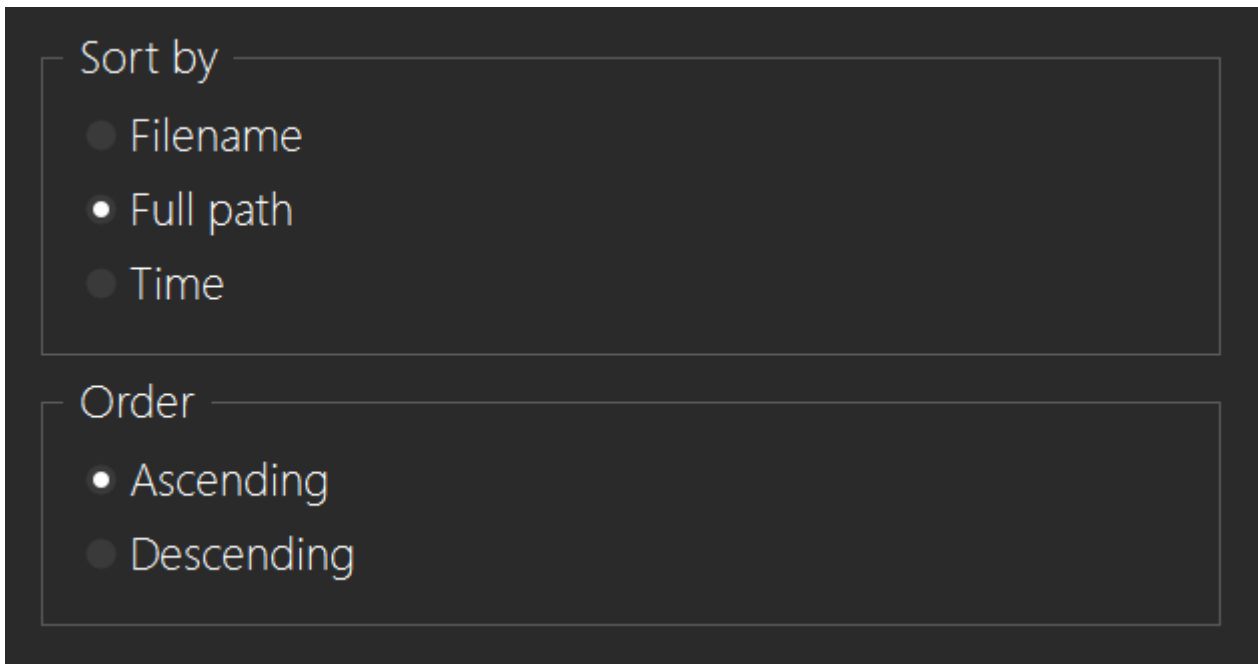
Generate thumbnails - thumbnails are shown in the report

Generate storyboard - videos are ordered in a sequence

For every video file in the report there is the key metadata, such as the length, creation time, etc, and it is also possible to create a video storyboard, which are images taken from the video at specific intervals.

Storyboards are automatically generated with video thumbnails from videos. If this feature is turned on, a storyboard is made for every video. You can set how many thumbnails you want or how often you want to generate them.

For thumbnail generation we use FFmpeg, so it needs to be installed for the Storyboard generation. Detailed information is in the Video storyboard (FFmpeg) section.



Files can be sorted by:

- Filename, which means only the name of the file, without its path, is used for sorting
- The full path of the file, including the location (folder) where the file was stored
- Time, of the creation or the last modification of the file

The sort order can be ascending or descending.

6.19.1 Example of contacts report:

Case Label: Kentucky church


Case Evidence Number: 8974969-589-468

Device Label:




Video Files (2)




All phone and application video files, sorted by time in ascending order. A fixed amount of 12 thumbnails generated from each video in equal intervals



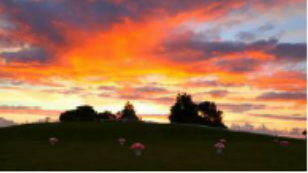
1 Wonders_of_Nature.mp4





Filename	Wonders_of_Nature.mp4
Path	phone/raw0/preload/INTERNAL_SDCARD/Samsung/Video/Wonders_of_Nature.mp4
Size	91.5 MB
Modified	2012-10-17 11:40:02 (UTC+2)
SHA-256 hash	FFB39D3FFCBCCDC3566B9BB688778BEC3E4D342AEBD66FB7C5C4C231E1B7FDE
Duration	00:01:37
Width	1280 px
Height	720 px
Framerate	29.97 fps

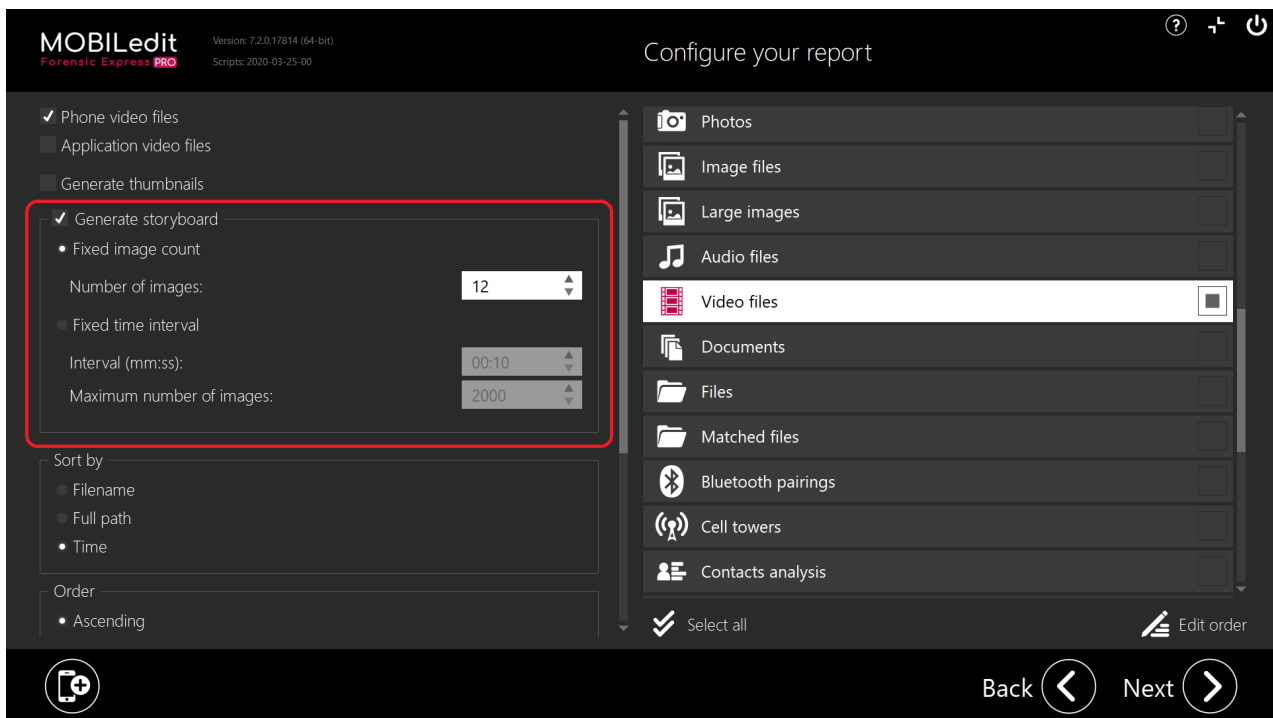




6.20 Data - Video storyboard (FFmpeg)

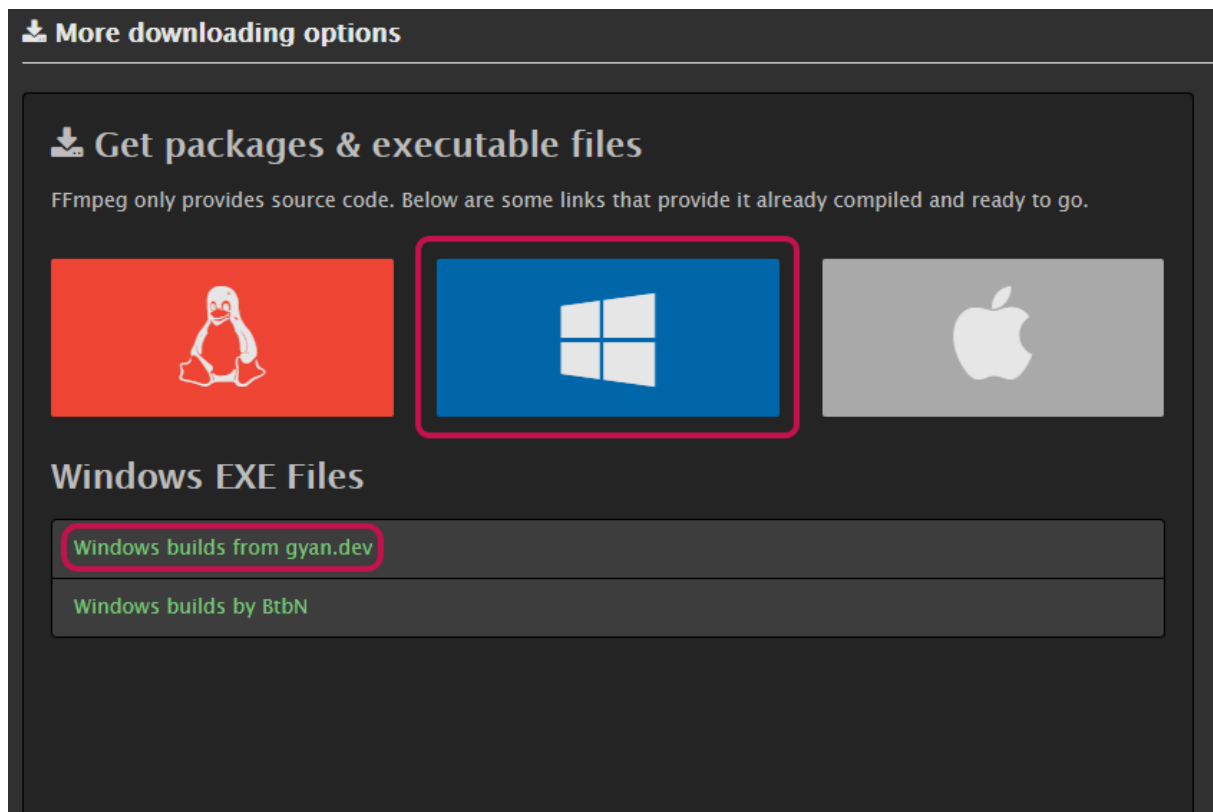
6.20.1 Overview

Because of FFmpeg's license and legal considerations, we cannot provide the FFmpeg library with our product, but you are able to download it on your own. Please read the FFmpeg's legal page at <https://ffmpeg.org/legal.html>.



6.20.2 Installation

1. Go to <https://ffmpeg.org/download.html>.
2. On this page, select one of the windows EXE files (for example: "Windows from gian.dev")

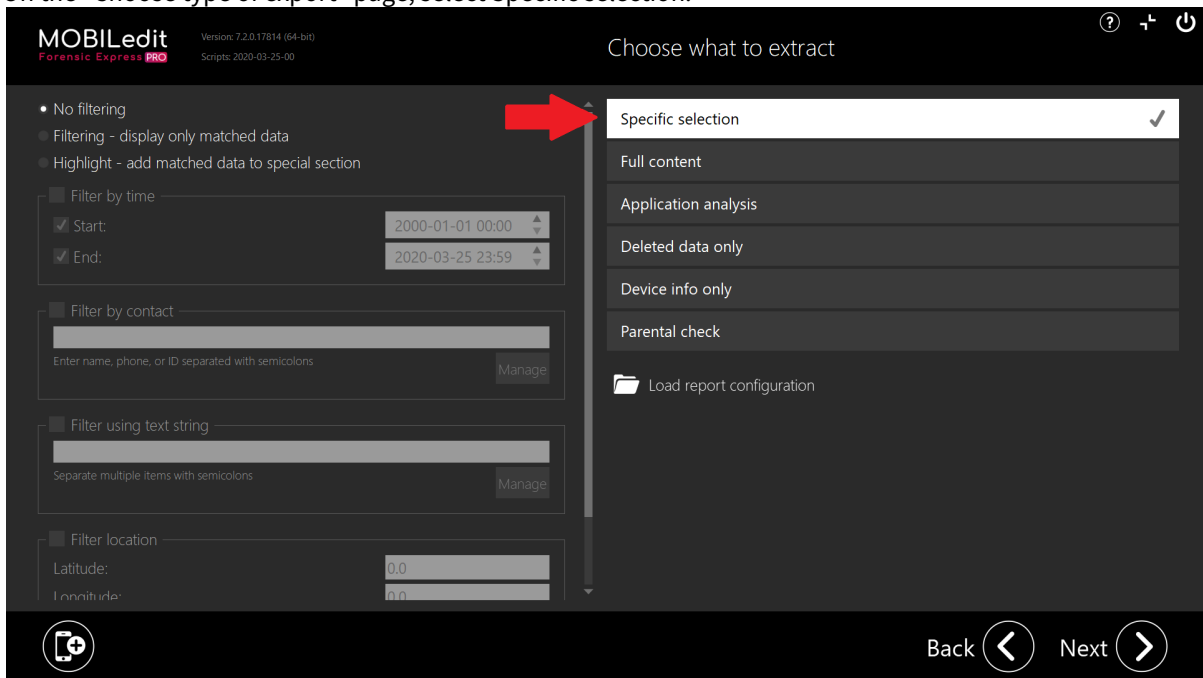


3. On the page find a release section and download the full release.

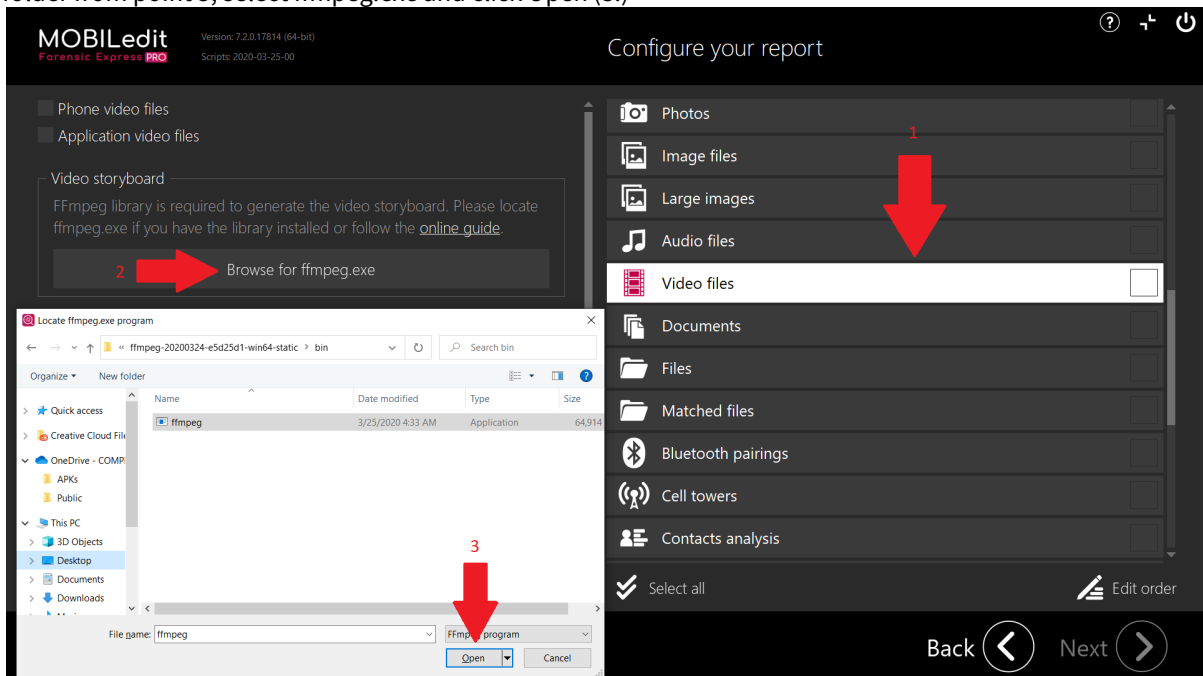


4. Extract the FFmpeg archive (ffmpeg-3.2.2-win64-static.zip in this case) on your computer. To do so right-click the FFmpeg archive, select "Extract All..." and then press the "Extract" button (you can also use another file archiver such as 7-Zip or WinRar).
5. After extraction, you should see a folder with the same name as the archive. Inside you should see the "bin" folder with ffmpeg.exe. If you don't see it, Microsoft Windows or your file archiver probably created a second folder with the same name as the archive.

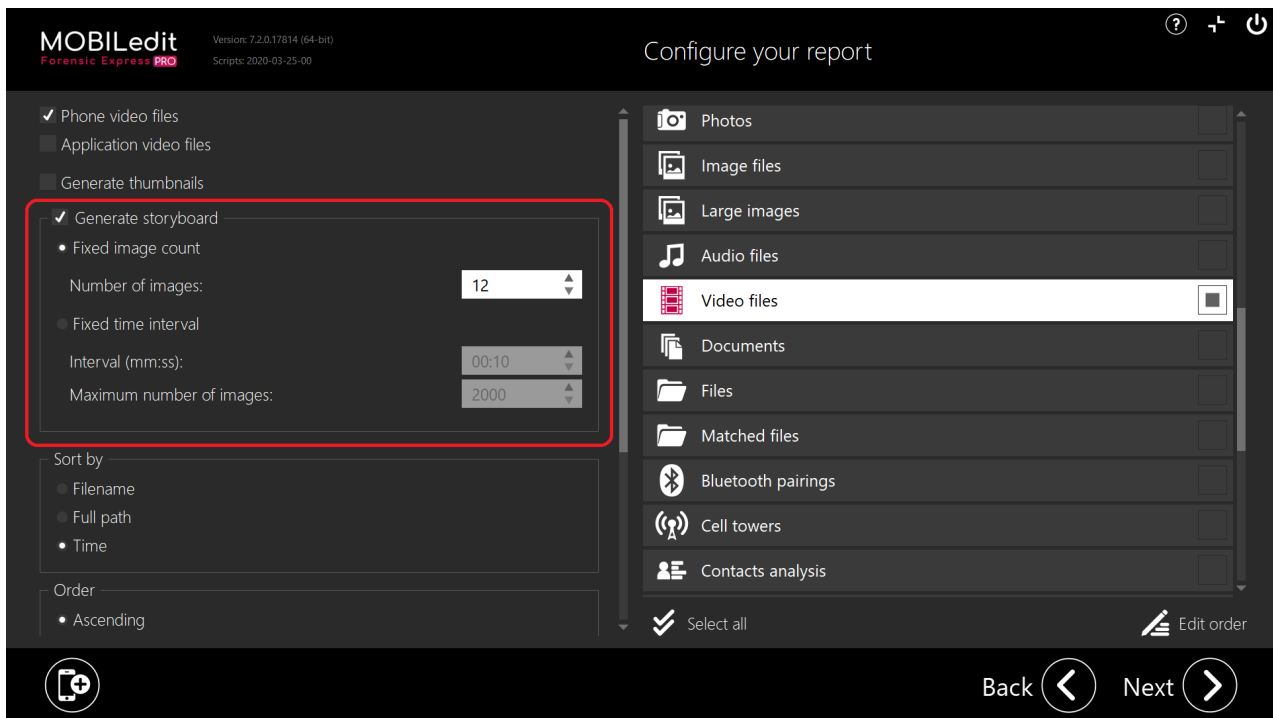
- Copy or remember the path of the "bin" folder.
- Open MOBILedit Forensic Express.
 - On the "Choose type of export" page, select Specific selection.



- On the next page select the Video option (1.) then Browse for ffmpeg.exe (2.) and finally navigate to the folder from point 5, select ffmpeg.exe and click Open (3.)



6.20.3 Storyboard settings



In the screenshot above there is a "Storyboard settings" located inside the red square, which is shown after successful installation.

A storyboard is activated by selecting the "Generate storyboard" option.

The first screenshot is generated at the start of the video.

The default setting generates 12 screenshots per video, and the following options are available:

1. **Fixed image count**

This option makes a fixed number of screenshots based on the "Number of images" setting, with one exception when the video is shorter (in seconds) than the specified number of images. If this is the case, one screenshot is created for every second of a video.

2. **Fixed time interval**

This option will create one screenshot per interval of selected duration (for example 1 screenshot at every 5 seconds of the video), which is done by using the "Interval" option. Minimal duration is one second. The "Maximum number of images" limits the maximum number of images to be created.

6.20.4 Uninstallation

Delete the folder where ffmpeg.exe is located.

6.21 Data - Documents

MOBILedit Forensic Express can extract the following formats of documents:

.doc	.docx	.ppt	.pptx	.xls	.xlsx
.odt	.odp	.ods	.pdf	.rtf	.txt
.pps	.ppsx	.msg	.pages	.tex	.wpd
.wps	.dotx	.gdoc	.xlr	.gsheet	.htm
.html	.ps				

You can specify your preferences before starting the extraction as seen on the screenshot below:

The screenshot shows a dark-themed settings window with the following sections:

- Document Selection:**
 - Documents
 - Application documents
- Preview Documents:**
 - Full Preview
 - First Lines (with a numeric input field set to 5)
 - List only
- Sort by:**
 - Filename
 - Full path
 - Time
- Order:**
 - Ascending
 - Descending
- Filter by time:**
 - Filter by time
 - Start: 2000-01-01 00:00
 - End: 2018-05-03 23:59
- Filter by file name or path:**
 - Filter by file name or path
 - [Empty text input field]
 - Separate multiple items with semicolons

Example of documents report:

Case Label: Kentucky church

Case Evidence Number: 8974969-589-468

Device Label:

Documents (21)

All phone and application documents, sorted by time in ascending order

1 log_file_camera.txt

Filename	log_file_camera.txt
Path	phone/applications0/com.evernote/live_data/files/.logs/log_file_camera.txt
Size	1 MB
Mime Type	text/plain
Modified	2017-10-14 14:56:33 (UTC+2)
SHA-256 hash	713DF4944D22F9C8D1028B1726F65382609C76A91EA17D053EA85EA56590D183

Document Preview

2015-10-14 14:56:01,975 DEBUG [Evernote] - Forked process, install exception handlers and stop application initialization

2015-10-14 14:56:01,998 DEBUG [ff] - registered crash manager

2015-10-14 14:56:02,000 DEBUG [ff] - registered nonfatal exception manager

2015-10-14 14:56:02,031 DEBUG [CameraUtil] - Heap size 512 MB, native heap size 5 MB

2015-10-14 14:56:02,032 DEBUG [CameraHolder] - getInitialCameraProxy - Build.MODEL = GT-I9505

2 log_file2.txt

Filename	log_file2.txt
Path	phone/applications0/com.evernote/live_data/files/.logs/log_file2.txt
Size	1 MB
Mime Type	text/plain
Modified	2017-10-15 12:06:35 (UTC+2)
SHA-256 hash	D2ED4C9B52C1F9F92BD76BF91AAE66F5920A058F36CBE866770746889038408A

Document Preview

2015-10-15 10:04:01,703 DEBUG [EvernoteProvider] - Provider++++onCreate()

2015-10-15 10:04:01,729 DEBUG [d] - AccountManager():userId=122114309

2015-10-15 10:04:01,733 DEBUG [b] - creating new AccountInfo():userId122114309

2015-10-15 10:04:01,758 DEBUG [d] - AccountManager():adding account::122114309::compelsonj

2015-10-15 10:04:01,758 DEBUG [d] - AccountManager():count=1

6.22 Data - Files

6.22.1 All files

If this option is selected then all files from the phone will be copied and will be included within the list in the report. Please note that it may take a long time and can consume considerable disk space, especially on rooted phones, because MOBILedit will try to copy every file from the phone.

6.22.2 List of application files

This option will show all application-related files.

6.22.3 Exclude Files

Files can be filtered based on the **National Software Reference Library (NSRL)**⁸⁵ database of common files which effectively reduces the number of exported files. In order to use this feature, a package called File exclude list has to be downloaded in the Updates section.

6.22.4 Example of a files report:

Files

Internal Files (10 files)

Filename	Size	Created	Modified	Accessed
/				
bugreports <small>SHA-256 hash: A112C7242F45D95F7E564FD62819702E794F374AA15054F98EA9E25B9EC4158F MD5 hash: 401A60BA45715FC1DF28DBEA346EAEDF</small>	56 B		1970-01-01 01:00:00	
charger <small>SHA-256 hash: D20B673E5DF443844162AD172A9C54E32C270BF0BA5144705C8826CEE1F1B51 MD5 hash: A143DA138779B8F9D00F791AB9C67CF</small>	19 B		1970-01-01 01:00:00	
d <small>SHA-256 hash: 3EA2F0DFBE463717365B699617D525321186FCB5980D7A7E878CB508DE3E25A2 MD5 hash: 9E5EAA4116E0F8BE3933D0F2CAAB545</small>	23 B		1970-01-01 01:00:00	
etc <small>SHA-256 hash: CDE5046ACA2FADCD390EB5C4B89529DD5FFD5400DF7826369976D4E4AA467CF0 MD5 hash: DBFCF3F2902621CEE723BD15C6817190</small>	17 B		1970-01-01 01:00:00	
factory <small>SHA-256 hash: B9042A8D0F10BC8851CB0A6EBC9D95584D4F11F58F208F802D6DE2A324D033A MD5 hash: 3A6584646861691A937A9532DC1AFA69</small>	15 B		2020-12-14 14:29:00	
nonplat_property_contexts <small>SHA-256 hash: 18BEAB08A195648D52A66AA3818D86AA4FFD24F9DC13CCD4C18A67A304DC85 MD5 hash: 3A857FE9217FB0A5BCA9575627090732</small>	6.83 KB		1970-01-01 01:00:00	
plat_property_contexts <small>SHA-256 hash: 5C8DD6FD093401374B8514181F764E2F04964869E70B8D61DBCSA8250FF057B6 MD5 hash: BE0EA5EE2C8EDCCFE1190311D6D2175</small>	4.23 KB		1970-01-01 01:00:00	
sdcard <small>SHA-256 hash: 0DD0FAB3AD128BFADFEDFB5F4A4BF2599DDF4D0133133755B1A3BDC0C01B2517C MD5 hash: AA9724B888FAD69CCDE702FAE2CFFD1D</small>	27 B		1970-01-01 01:00:00	
vendor <small>SHA-256 hash: E788011F52FA81BED9497718EA2B960DAD5AA8B73545001ED40C5A9A44E6F371 MD5 hash: BD47A2A5616AAC518095DC0E1305F821</small>	20 B		1970-01-01 01:00:00	
/mnt/			2020-12-14 14:29:00	
sdcard <small>SHA-256 hash: 0DD0FAB3AD128BFADFEDFB5F4A4BF2599DDF4D0133133755B1A3BDC0C01B2517C MD5 hash: AA9724B888FAD69CCDE702FAE2CFFD1D</small>	27 B		2020-12-14 14:29:12	2020-12-14 14:29:12
/oem/				
/oem/secure_storage/		1970-01-01 01:00:00	1970-01-01 01:00:00	1970-01-01 01:00:00

85 <https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl>

6.23 Data - Matched Files

Matched Files enable you to highlight files based on a user-supplied hash list. The imported hash list must be in a UTF-8 format, with each hexadecimal hash on a separate line. The suffix of the hash list must be md5, sha1, sha256 or sha512. Using Matched Files will generate a section in the report with files highlighted based on the supplied hash list.

6.23.1 Example of a report with Matched Files:





Case Label: Kentucky church

Case Evidence Number: 8974969-589-468

Device Label:

Matched Files

malware (4 files)
Files identified as "malware"

Filename	Size	Created	Modified	Accessed
 MAIN Armstrong.jpg SHA-256 hash: B151AB90130095521AD109A8522157C5719B7B5AA32991C4F29EB1FF701FD90 MD5 hash: E4D9329127EFC2B6E419AF78B0921C69	126 KB	2018-03-27 09:24:57	2018-03-02 11:24:09	2018-03-27 09:24:57
 MAIN Dominika 2.jpg SHA-256 hash: B10CS887702628BF5659ADE7E44800F44EBDCE73435E894AA87CEA48AB98EF96 MD5 hash: 21482CBOB1C6ED58876682366A0D362	117 KB	2018-03-27 09:24:57	2018-03-02 10:59:58	2018-03-27 09:24:57
 MAIN Dominika.JPG SHA-256 hash: 75963F11C6AD435BCD536EE27D229D5A18E5F59273676FDD3CC5E938A2B75DD MD5 hash: 299745D14BF13CD433CC56D40DB4FB8A	125 KB	2018-03-27 09:24:57	2018-03-02 10:57:09	2018-03-27 09:24:57
 MAIN Nicol.jpg SHA-256 hash: 8AE8B5992D4F8FACED0B1799C4C1FD5A38845EB2F8C8A317D11B93AA71067BE MD5 hash: 6028015F36321D2C3679498E2766FBCB	323 KB	2018-03-27 09:24:57	2018-03-02 11:11:09	2018-03-27 09:24:57

6.24 Data - Application usage

MOBILedit Forensic Express can extract Application data usage on Jailbroken iPhones with iOS 11.4 and below.

6.25 Data - Bluetooth pairings

Bluetooth technology has become so in demand during the last decade, as a new technology that uses a very popular method of wirelessly transferring data between two separate electronic devices such as a smartphone and a headphone, media device player, and a wireless speaker or an iPad with its keyboard.

MOBILedit Forensic can extract a list of all Bluetooth pairings between your phone and other Bluetooth devices that have connected to it or that have been within a range of devices.

MOBILedit Forensic is able to extract a list of all devices connected to your phone via Bluetooth or appeared within its reach.

6.25.1 Example of Bluetooth pairings report:

Bluetooth Pairings ⁽⁴⁾

All bluetooth connections

1 MacBook Pro	
Device Address	78:4F:43:8A:1B:DF
Source File	phone/applications1/Apple Backup/SysSharedContainerDomain-systemgroup.com.apple.bluetooth/backup/Library/Database/com.apple.MobileBluetooth.ledevices.paired.db : 0x3f56 (Table: PairedDevices)
2 Apple Pencil	
Device Address	CA:0F:88:A5:73:15
Source File	phone/applications1/Apple Backup/SysSharedContainerDomain-systemgroup.com.apple.bluetooth/backup/Library/Database/com.apple.MobileBluetooth.ledevices.paired.db : 0x3eb6 (Table: PairedDevices)
3 Apple Watch	
Device Address	A0:78:17:48:47:1C
Source File	phone/applications1/Apple Backup/SysSharedContainerDomain-systemgroup.com.apple.bluetooth/backup/Library/Database/com.apple.MobileBluetooth.ledevices.paired.db (Table: PairedDevices)
XS	
Device Address	50:7A:C5:C2:34:64
Source File	phone/applications1/Apple Backup/SysSharedContainerDomain-systemgroup.com.apple.bluetooth/backup/Library/Database/com.apple.MobileBluetooth.ledevices.paired.db : 0x3d8a (Table: PairedDevices)

6.25.2 Example of seen Bluetooth devices report:

Seen Bluetooth Devices (633)

All bluetooth connections

1	Device Address	ED:54:E3:CA:59:8D
	Source File	phone/applications1/Apple Backup/SysSharedContainerDomain-systemgroup.com.apple.bluetooth/backup/Library/Database/com.apple.MobileBluetooth.ledevices.other.db : 0x4fb6 (Table: OtherDevices)
2	Alta	
	Device Address	F5:FC:C7:F8:01:67
	Source File	phone/applications1/Apple Backup/SysSharedContainerDomain-systemgroup.com.apple.bluetooth/backup/Library/Database/com.apple.MobileBluetooth.ledevices.other.db : 0x4f68 (Table: OtherDevices)
3	[TV] Samsung 5 Series (49)	
	Device Address	40:16:3B:B8:1C:54
	Source File	phone/applications1/Apple Backup/SysSharedContainerDomain-systemgroup.com.apple.bluetooth/backup/Library/Database/com.apple.MobileBluetooth.ledevices.other.db : 0x4f03 (Table: OtherDevices)
4	Device Address	F8:04:2E:91:BA:2F
	Source File	phone/applications1/Apple Backup/SysSharedContainerDomain-systemgroup.com.apple.bluetooth/backup/Library/Database/com.apple.MobileBluetooth.ledevices.other.db : 0x4eb8 (Table: OtherDevices)
5	Charge HR	
	Device Address	EF:38:EB:2C:15:46
	Source File	phone/applications1/Apple Backup/SysSharedContainerDomain-systemgroup.com.apple.bluetooth/backup/Library/Database/com.apple.MobileBluetooth.ledevices.other.db : 0x4e64 (Table: OtherDevices)
6	Device Address	CC:B1:1A:A5:06:35
	Source File	phone/applications1/Apple Backup/SysSharedContainerDomain-systemgroup.com.apple.bluetooth/backup/Library/Database/com.apple.MobileBluetooth.ledevices.other.db : 0x4e19 (Table: OtherDevices)
7	JBL Charge	
	Device Address	FC:A8:9A:B6:6B:FF
	Source File	phone/applications1/Apple Backup/SysSharedContainerDomain-systemgroup.com.apple.bluetooth/backup/Library/Database/com.apple.MobileBluetooth.ledevices.other.db : 0x4dc4 (Table: OtherDevices)
8	MI Band 2	
	Device Address	F4:94:C7:43:E6:BA
	Source File	phone/applications1/Apple Backup/SysSharedContainerDomain-systemgroup.com.apple.bluetooth/backup/Library/Database/com.apple.MobileBluetooth.ledevices.other.db : 0x4d70 (Table: OtherDevices)

6.26 Data - Cell towers

Data about cell towers that the subject phone was connected to can be obtained. However, this is only possible with rooted Android phones. Obtained cell tower locations can be individually viewed on the map through the provided link.

6.26.1 Example of cell towers report:

Case Label: Kentucky church Case Evidence Number: 8974969-589-468 Device Label:

Cell Towers (95 total, 50 deleted)

Type	MCC	MNC	LAC	Cell ID	Last Request	Link
wcdma	230	2			1971-09-19 02:16:22 (UTC+2)	Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x46580 (Table: lru_table)						
wcdma					1972-12-09 07:22:08 (UTC+1)	Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x8123 (Table: lru_table)						
wcdma	230	2	1182	203717279	2016-07-24 11:20:36 (UTC+2)	OpenCellID Maps Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x8F26 (Table: lru_table)						
wcdma	230	2	1182	203717144	2016-07-24 12:00:13 (UTC+2)	OpenCellID Maps Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x8ED2 (Table: lru_table)						
wcdma	230	2	1182	203717695	2016-07-24 12:21:10 (UTC+2)	OpenCellID Maps Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x8E26 (Table: lru_table)						
wcdma	230	2	1182	203717267	2016-07-24 12:24:29 (UTC+2)	OpenCellID Maps Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x8DD4 (Table: lru_table)						
wcdma	230	2	1182	203716871	2016-07-24 12:34:42 (UTC+2)	OpenCellID Maps Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x8D7F (Table: lru_table)						
wcdma	230	2	1182	203717328	2016-07-25 08:39:07 (UTC+2)	OpenCellID Maps Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x8CD4 (Table: lru_table)						
wcdma	230	2	1182	203696992	2016-07-25 19:46:45 (UTC+2)	OpenCellID Maps Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x8A9F (Table: lru_table)						
lte	230	2	1182	10335489	2016-07-25 19:46:45 (UTC+2)	OpenCellID Maps Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x8AF3 (Table: lru_table)						
wcdma	230	2	1182	203717281	2016-07-26 08:45:37 (UTC+2)	OpenCellID Maps Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x8A49 (Table: lru_table)						
wcdma	230	2	1133	-1	2016-07-26 14:10:49 (UTC+2)	OpenCellID Maps Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x89A1 (Table: lru_table)						
wcdma	230	2	1133	203697167	2016-07-26 14:11:11 (UTC+2)	OpenCellID Maps Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x8949 (Table: lru_table)						
lte	230	2	1182	10342147	2016-07-26 14:11:57 (UTC+2)	OpenCellID Maps Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x88FA (Table: lru_table)						
wcdma	230	2	1133	203697170	2016-07-26 14:11:57 (UTC+2)	OpenCellID Maps Deleted
Source File phone/applications0/com.google.android.gms/live_data/databases/herrevad : 0x88A5 (Table: lru_table)						
gsm	230	2	1139	21895	2016-07-26 18:35:02 (UTC+2)	OpenCellID Maps Deleted

6/20/2018 12:51 PM Generated by Compelson MOBILedit Forensic Express 5.3.0.12966 1091/2537

6.27 Data - 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.

Contacts analysis

Sort by

- Total associated events
- Number of messages
- Total number of words in messages
- Number of calls
- Total call time

Order

- Ascending
- Descending

Filter unpopular

Minimum number of associated events:

1



Example of contact analysis report:

Case Label: Kentucky church

Case Evidence Number: 8974969-589-468

Device Label:

Contact Analysis (424 total, 1 deleted)

A subset of phone and SIM contacts filtered by a minimum of 1 associated events, sorted by the number of associated events in descending order

Contact	Origin	Total	Messages	Calls	Other
1 Gabie Case	Messenger	429	Total: 384 Received: 153 Sent: 197 Other: 34 Word Count: 2768	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	45
2 Josefine Compelson	Messenger	55	Total: 52 Received: 19 Sent: 33 Other: 0 Word Count: 244	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	3
3 Godfrey Charles	Messenger	24	Total: 23 Received: 5 Sent: 17 Other: 1 Word Count: 101	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	1
4 Timotejko Dušička	Messenger	23	Total: 22 Received: 12 Sent: 9 Other: 1 Word Count: 60	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	1
5 Agyemang McAbraham	Messenger	21	Total: 20 Received: 13 Sent: 7 Other: 0 Word Count: 93	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	1
6 Khatibu Haji	Messenger	21	Total: 20 Received: 12 Sent: 8 Other: 0 Word Count: 42	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	1
7 Kasimu Ndembo	Messenger	21	Total: 20 Received: 13 Sent: 7 Other: 0 Word Count: 148	Total: 0 Received: 0 Missed: 0 Dialed: 0 Other: 0 Total Call Time: 00:00:00	1

6.28 Data - Cookies

System cookies are only obtainable from iOS devices. Application-specific cookies are analyzed for every installed application. Cookies contain information about the web domain as well as their creation time. Specific application session cookies can be acquired which often have long expiry dates that are more likely to expire from a user signing out of the application in question.

6.28.1 Example of cookies report:

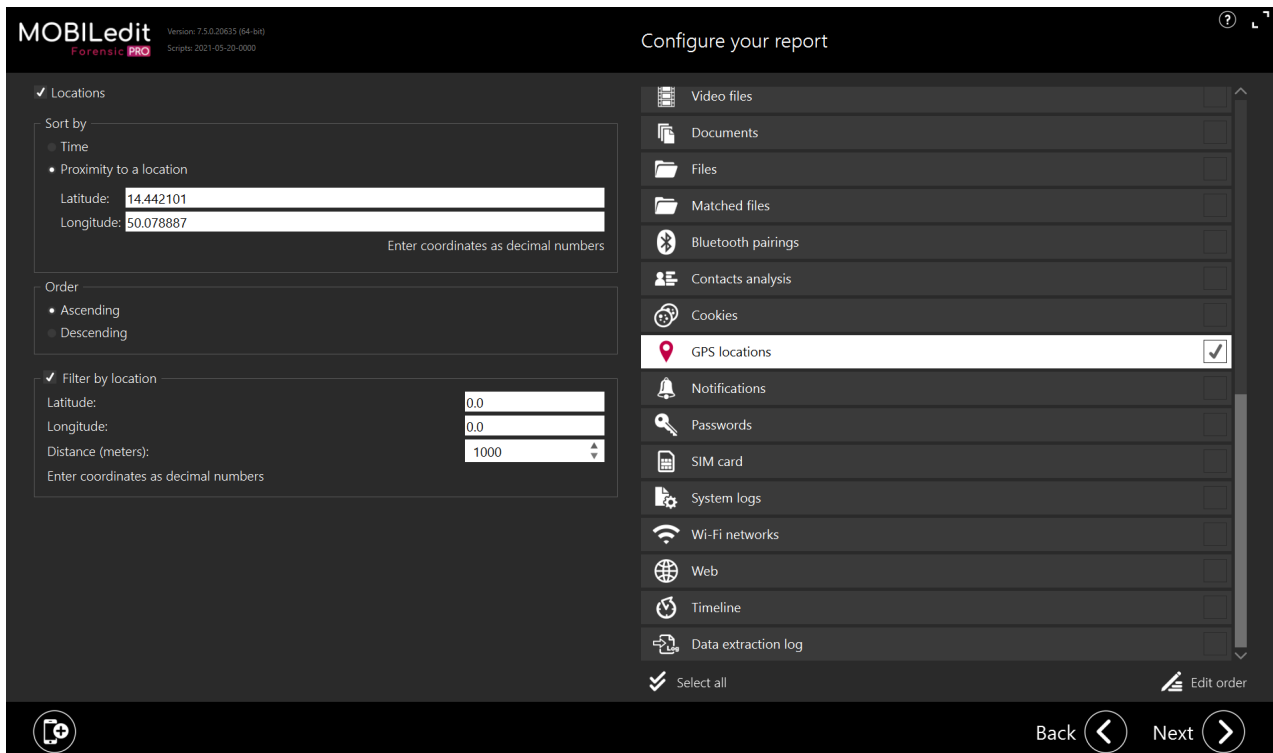
Case Label: Kentucky church Case Evidence Number: 8974969-589-468 Device Label:

Cookies (312 total, 102 deleted)

Name	Domain	Source	Created	Accessed	Expires
sess	.adnxs.com/	com.android.browser	2016-04-15 13:20:40 (UTC+2)	2016-04-15 13:20:40 (UTC+2)	2016-04-16 13:20:40 (UTC+2)
1					
Source File phone/applications0/com.android.browser/live_data/databases/webviewCookiesChromium.db : 0x8F48 (Table: cookies)					
sess	.adnxs.com/	com.android.browser	2016-04-15 13:20:40 (UTC+2)	2016-04-15 13:20:40 (UTC+2)	2016-04-16 13:20:40 (UTC+2)
1					
Source File phone/applications0/com.android.browser/backup/db/webviewCookiesChromium.db : 0x8F48 (Table: cookies)					
uuid2	.adnxs.com/	com.android.browser	2016-04-15 13:20:40 (UTC+2)	2016-04-15 13:20:40 (UTC+2)	2016-07-14 13:20:40 (UTC+2)
7782181878390178772					
Source File phone/applications0/com.android.browser/backup/db/webviewCookiesChromium.db : 0x8F02 (Table: cookies)					
uuid2	.adnxs.com/	com.android.browser	2016-04-15 13:20:40 (UTC+2)	2016-04-15 13:20:40 (UTC+2)	2016-07-14 13:20:40 (UTC+2)
7782181878390178772					
Source File phone/applications0/com.android.browser/live_data/databases/webviewCookiesChromium.db : 0x8F02 (Table: cookies)					
BizoCustomSegments	.ads.linkedin.com/	com.android.browser	2016-04-15 13:20:55 (UTC+2)	2016-04-15 13:43:35 (UTC+2)	2016-10-12 13:20:04 (UTC+2)
mtcm3FFnkG8Ie					
Source File phone/applications0/com.android.browser/live_data/databases/webviewCookiesChromium.db : 0x8AB6 (Table: cookies)					
BizoCustomSegments	.ads.linkedin.com/	com.android.browser	2016-04-15 13:20:55 (UTC+2)	2016-04-15 13:43:35 (UTC+2)	2016-10-12 13:20:04 (UTC+2)
mtcm3FFnkG8Ie					
Source File phone/applications0/com.android.browser/backup/db/webviewCookiesChromium.db : 0x8AB6 (Table: cookies)					
BizoData	.ads.linkedin.com/	com.android.browser	2016-04-15 13:20:55 (UTC+2)	2016-04-15 13:43:35 (UTC+2)	2016-10-15 01:20:04 (UTC+2)
jY3BxHjOisNKOpAhXDiSisVd0nVSCzXk3mwojwQEliZt7RkrY0a9jVBMwgbSkfc9TFzjpjV2eqwXilPow1D4v4G0ryPillukaegtP6lyXQzqT14nKlMfpjrUDXMg0TTTwoSllGz22sJE69xXoTS Pwoj3EMoH26TEDgOectDGHoMtoV0JrdLAzRpjLqTUI3E81my05ipUY79PuisRMEfrsHvpgtoSjQfwYGGeRURhK3N68TnggXisXIIHAlele					
Source File phone/applications0/com.android.browser/backup/db/webviewCookiesChromium.db : 0x8B0A (Table: cookies)					
BizoData	.ads.linkedin.com/	com.android.browser	2016-04-15 13:20:55 (UTC+2)	2016-04-15 13:43:35 (UTC+2)	2016-10-15 01:20:04 (UTC+2)
jY3BxHjOisNKOpAhXDiSisVd0nVSCzXk3mwojwQEliZt7RkrY0a9jVBMwgbSkfc9TFzjpjV2eqwXilPow1D4v4G0ryPillukaegtP6lyXQzqT14nKlMfpjrUDXMg0TTTwoSllGz22sJE69xXoTS Pwoj3EMoH26TEDgOectDGHoMtoV0JrdLAzRpjLqTUI3E81my05ipUY79PuisRMEfrsHvpgtoSjQfwYGGeRURhK3N68TnggXisXIIHAlele					
Source File phone/applications0/com.android.browser/live_data/databases/webviewCookiesChromium.db : 0x8B0A (Table: cookies)					
BizoID	.ads.linkedin.com/	com.android.browser	2016-04-15 13:20:55 (UTC+2)	2016-04-15 13:43:35 (UTC+2)	2016-10-15 01:20:04 (UTC+2)
8b5c7df3-30a1-466f-9627-3d8fc34de88e					
Source File phone/applications0/com.android.browser/live_data/databases/webviewCookiesChromium.db : 0x8C50 (Table: cookies)					
BizoID	.ads.linkedin.com/	com.android.browser	2016-04-15 13:20:55 (UTC+2)	2016-04-15 13:43:35 (UTC+2)	2016-10-15 01:20:04 (UTC+2)
8b5c7df3-30a1-466f-9627-3d8fc34de88e					

6.29 Data - GPS locations

6.29.1 Locations



MOBILedit Forensic is able to extract accurate location data from Android devices. Application analysis can also provide GPS detailed location data and sometimes entire routes - especially with mapping, fitness, and transportation applications such as Uber or MapMyRun.

This means that the sequence of GPS coordinates with timestamps is recorded and added into the report files. Photos and videos on a device may also contain GPS locations (including coordinates) in their metadata. Notes, Events, and various other items may also contain location data.

GPS locations that have been obtained can be viewed in an interactive map that allows for filtering based on the type of location points. Filtering by time can also be applied.



Example of GPS locations report:

Locations

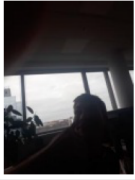
GPS Locations (7)

All GPS locations, sorted by time in ascending order

[Click here](#) to view GPS locations in interactive map

Latitude	50.10278 °
Longitude	14.45694 °
🕒 Time	2021-02-02 14:21:23 (UTC+1)
Event Origin	Media
Event Type	Image

1 JPEG_ef77773d-e316-4ef0-92b4-e2cda9f185af7930297858231999478.jpg



Filename	JPEG_ef77773d-e316-4ef0-92b4-e2cda9f185af7930297858231999478.jpg				
Path	phone/raw0/data/media/0/Android/data/com.tinder/files/Pictures/JPEG_ef77773d-e316-4ef0-92b4-e2cda9f185af7930297858231999478.jpg				
Size	1.89 MB				
🕒 Modified	2021-02-02 14:21:23 (UTC+1)				
🕒 Accessed	2021-02-02 14:19:14 (UTC+1)				
Exposure Time	1 / 213 s				
Focal Length	2.91 mm				
F-Number	1.9				
↔️ Width	3264 px				
↑ Height	2448 px				
Camera Manufacturer	samsung				
Camera Model	SM-A320FL				
Format	jpeg				
🔄 Rotation	90°				
🕒 Date of Generation	2021-02-02 14:21:23 (UTC+1)				
🕒 Date of Digitization	2021-02-02 14:21:23 (UTC+1)				
📍 Position (Google Maps)	<table style="width: 100%; border-collapse: collapse; font-size: 0.7em;"> <tr> <td style="width: 50%;">Latitude</td> <td>50.10278 °</td> </tr> <tr> <td>Longitude</td> <td>14.45694 °</td> </tr> </table>	Latitude	50.10278 °	Longitude	14.45694 °
Latitude	50.10278 °				
Longitude	14.45694 °				

GPS data might be extracted from various sources - such as image metadata. Because of this, source data might appear in the backup folder even if you have not selected them.

6.30 Data - Notifications

Notifications are retrievable from both iOS and Android devices. Application-specific notifications gathered from iOS devices include notifications that are no longer active and can contain otherwise unobtainable information such as emails and messages from applications that haven't been stored in databases.

On Android, only active Notifications can have data extracted, due to notifications being cleared after they are dismissed by the user.

Example of notifications report:

Notifications ⁽⁵⁾

1 adam.sikora73@gmail.com	
Source	com.google.android.gm
? Seen	✘ no
Source File	phone/applications1/Dumpsys/notification.log
2 String	
Source	com.google.android.gm
📄 Body	SpannableString
? Seen	✘ no
Source File	phone/applications1/Dumpsys/notification.log
3 String	
Source	com.compelson.mefconnector
📄 Body	String
? Seen	✘ no
Source File	phone/applications1/Dumpsys/notification.log
4 String	
Source	com.android.systemui
📄 Body	String
? Seen	✘ no
Source File	phone/applications1/Dumpsys/notification.log
5 Transferring media files via USB	
Source	android
📄 Body	String
? Seen	✘ no
Source File	phone/applications1/Dumpsys/notification.log

6.31 Data - Screen unlocking history

Allows you to see the history of users screen unlocks:

Screen Unlocking History ⁽²⁾

Status	Time and Date
Screen ON	0000-12-12 17:16:29 (unknown time zone)
Source File	phone/applications1/Logs/Events.log
Unlocked	0000-12-12 17:16:31 (unknown time zone)
Source File	phone/applications1/Logs/Events.log

6.32 Data - Passwords

On 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 have been saved/stored within it. Passwords contained in the keychain include Wi-Fi passwords, apple id password, passwords saved in Safari as well as various application passwords. Passwords in iOS keychain are unorganized and contain a lot of useless information, which can be filtered out of the final report.

From Android devices, we retrieve Wi-Fi passwords.

We also retrieve passwords from a lot of applications directly for both aforementioned platforms. Retrieved passwords include email passwords from various email applications, passwords saved in Web Browsers and other account passwords.

Example of passwords report:

Case Label: Kentucky church

Case Evidence Number: 8974969-589-468

Device Label:

Passwords

Passwords from Internet (Saved Passwords) (2 total, 2 deleted)

1 compelson.test@gmail.com		✖ Deleted
Host	https://www.dropbox.com	
User Name	compelson.test@gmail.com	
Password	IsME	
Source File	phone/applications0/com.android.browser/live_data/databases/webview.db : 0x202E4 (Table: password)	
2 compelson.test@gmail.com		✖ Deleted
Host	https://mobile.twitter.com	
User Name	compelson.test@gmail.com	
Password	IsME	
Source File	phone/applications0/com.android.browser/live_data/databases/webview.db : 0x202A2 (Table: password)	





Passwords from Email (Email Passwords) (2)

1 valentine.veryrich@yahoo.com	
User Name	valentine.veryrich@yahoo.com
Password Encrypted	gGP/rFhaMMxj/8hJQ9zotRN5/ro3PPH/3G6McEjX1ZI=
Password	VerySecretPass123
Protocol	imap
Address	imap.mail.yahoo.com
Port	993
Source File	phone/applications0/com.android.email/live_data/databases/EmailProvider.db : 0x13D7B (Table: HostAuth)
2 valentine.veryrich@yahoo.com	
User Name	valentine.veryrich@yahoo.com
Password Encrypted	gGP/rFhaMMxj/8hJQ9zotRN5/ro3PPH/3G6McEjX1ZI=
Password	VerySecretPass123
Protocol	smtp
Address	smtp.mail.yahoo.com
Port	465
Source File	phone/applications0/com.android.email/live_data/databases/EmailProvider.db : 0x13F2F (Table: HostAuth)

Passwords from Email (Accounts) (1)

6.33 Data - SIM card

Extracts data from the SIM card such as IMSI, Country, ICCID, and Operator as shown below:

SIM Card	
IMSI	[REDACTED]
SIM Card Country	Czech Rep.
ICCID	[REDACTED]
Operator	Mobil CZ, MCC: 230, MNC: 1
 Total Storage	54.0 GB
 Used Storage	27.5 GB
 Total SD Card Storage	7.5 GB
 Used SD Card Storage	2.2 GB

6.34 Data - System logs

System logs and "DumpSys" files can be extracted from Android phones. Android system keeps these files for debugging and monitoring purposes and the files can contain various system data like recent locations, recently connected Wi-Fi networks, recently launched and running 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 also used for the analysis of Wi-Fi networks, Locations, and Notifications.

System Logs (81 files)

Filename	Size	Created	Modified	Accessed
/				
/System Logs/				
Events.log	342.7 kB	2016-06-23 17:05:23		
Main.log	722.1 kB	2016-06-23 17:05:23		
Radio.log	364.2 kB	2016-06-23 17:05:25		
/DumpSys/				
DockObserver.log	99 B	2016-06-23 17:05:26		
SurfaceFlinger.log	16.4 kB	2016-06-23 17:05:39		
accessibility.log	218 B	2016-06-23 17:05:29		
account.log	7.5 kB	2016-06-23 17:05:30		
activity.log	145.2 kB	2016-06-23 17:05:35		
alarm.log	73.7 kB	2016-06-23 17:05:29		
android.service.gatekeeper.IGateKeeperService.log	67 B	2016-06-23 17:05:39		
appops.log	124.1 kB	2016-06-23 17:05:38		
appwidget.log	37.7 kB	2016-06-23 17:05:26		
audio.log	6.4 kB	2016-06-23 17:05:26		
backup.log	15.8 kB	2016-06-23 17:05:26		
battery.log	412 B	2016-06-23 17:05:30		
batteryproperties.log	93 B	2016-06-23 17:05:39		
batterystats.log	311.1 kB	2016-06-23 17:05:38		
bluetooth_manager.log	127 B	2016-06-23 17:05:29		
carrier_config.log	142 B	2016-06-23 17:05:25		
commontime_management.log	81 B	2016-06-23 17:05:26		
connectivity.log	6.1 kB	2016-06-23 17:05:28		
content.log	157.8 kB	2016-06-23 17:05:30		
cpuinfo.log	8.8 kB	2016-06-23 17:05:30		
dbinfo.log	48.9 kB	2016-06-23 17:05:31		
device_policy.log	1.3 kB	2016-06-23 17:05:29		

6.35 Data - User dictionary

MOBILedit Forensic Express can extract cached words written by a user on both Android and iOS devices.

On Android devices, you can also extract the whole user dictionary from the keyboard.

6.36 Data - WiFi networks

This section contains data about all Wi-Fi networks saved in a device. Such as the last connection timestamps as well as session time and passwords are especially interesting here.

Such as networks that the phone has been previously connected including when it was connected and for how long (session duration). Additionally, Wi-Fi passwords from historically connected networks can also be obtained and presented in the desired report format.

6.36.1 Example of WiFi networks report:

Case Label: Kentucky church

Case Evidence Number: 8974969-589-468

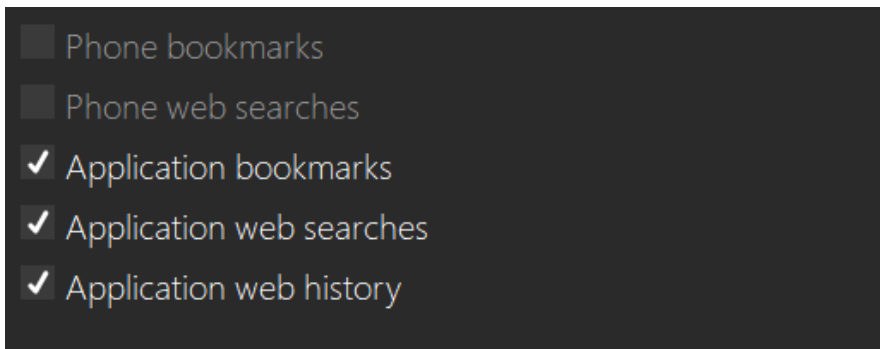
Device Label:

Wi-Fi Networks (3)

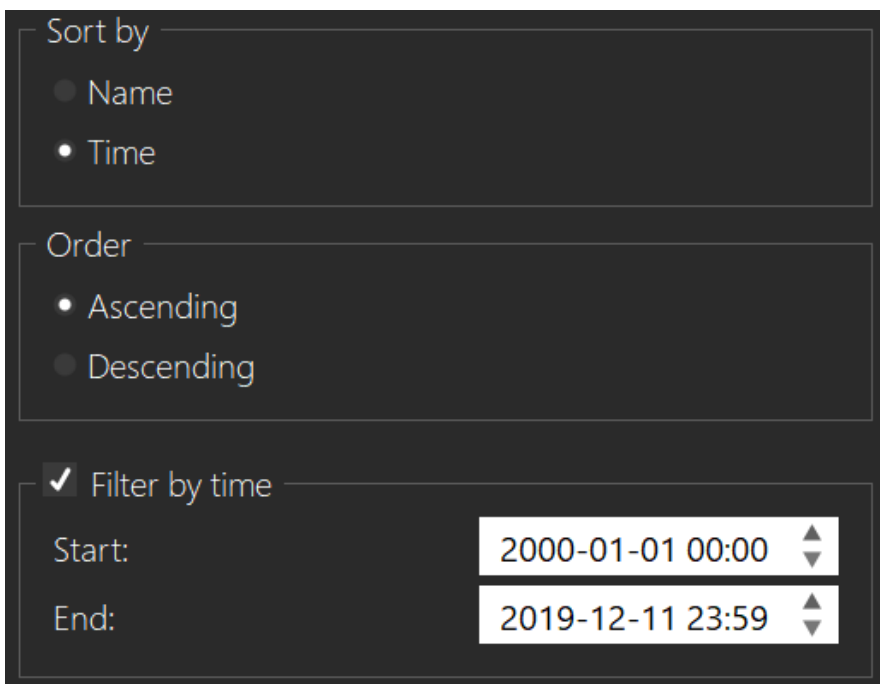
1 Internet22					
SSID		Internet22			
BSSID		4D:6D:98:0B:96:A6,			
Password		password123456			
Source		Samsung Galaxy S7			
Source File		phone/applications0/com.android.providers.settings/backup/fflattened-data			
Source File		phone/applications1/Dumpsys/netstats.log			
Source File		phone/applications1/Dumpsys/wifi.log			
Connected Time					
2017-08-04 12:00:00 (UTC+2)	2017-08-04 13:00:00 (UTC+2)	2017-08-04 14:00:00 (UTC+2)	2017-08-04 15:00:00 (UTC+2)	2017-08-04 16:00:00 (UTC+2)	
2017-08-07 15:00:00 (UTC+2)	2017-08-07 16:00:00 (UTC+2)	2017-08-07 17:00:00 (UTC+2)	2017-08-07 18:00:00 (UTC+2)	2017-08-07 19:00:00 (UTC+2)	
2017-08-26 08:00:00 (UTC+2)	2017-08-26 09:00:00 (UTC+2)	2017-08-26 10:00:00 (UTC+2)	2017-08-26 11:00:00 (UTC+2)	2017-08-27 14:00:00 (UTC+2)	
2017-09-08 17:00:00 (UTC+2)	2017-09-09 18:00:00 (UTC+2)	2017-09-09 19:00:00 (UTC+2)	2017-09-09 20:00:00 (UTC+2)	2017-09-15 19:00:00 (UTC+2)	
2 Secretnet					
SSID		Secretnet			
BSSID		34:12:46:C3:D0:6D,			
Password		Wsy94afbtd168			
Source		Samsung Galaxy S7			
Source File		phone/applications0/com.android.providers.settings/backup/fflattened-data			
Source File		phone/applications1/Dumpsys/wifi.log			
3 Wi-Fi-Home					
SSID		Wi-Fi-Home			
Password		123456789abcde			
Source		Samsung Galaxy S7			
Source File		phone/applications0/com.android.providers.settings/backup/fflattened-data			
Source File		phone/applications1/Dumpsys/netstats.log			
Connected Time					
2017-07-11 18:00:00 (UTC+2)	2017-07-11 19:00:00 (UTC+2)	2017-07-11 20:00:00 (UTC+2)			

6.37 Data - Web

MOBILedit Forensic Express can extract and analyze web searches, bookmarks, and history made by any app in the investigated device.



You can filter and customize the results as seen on the screenshot below:

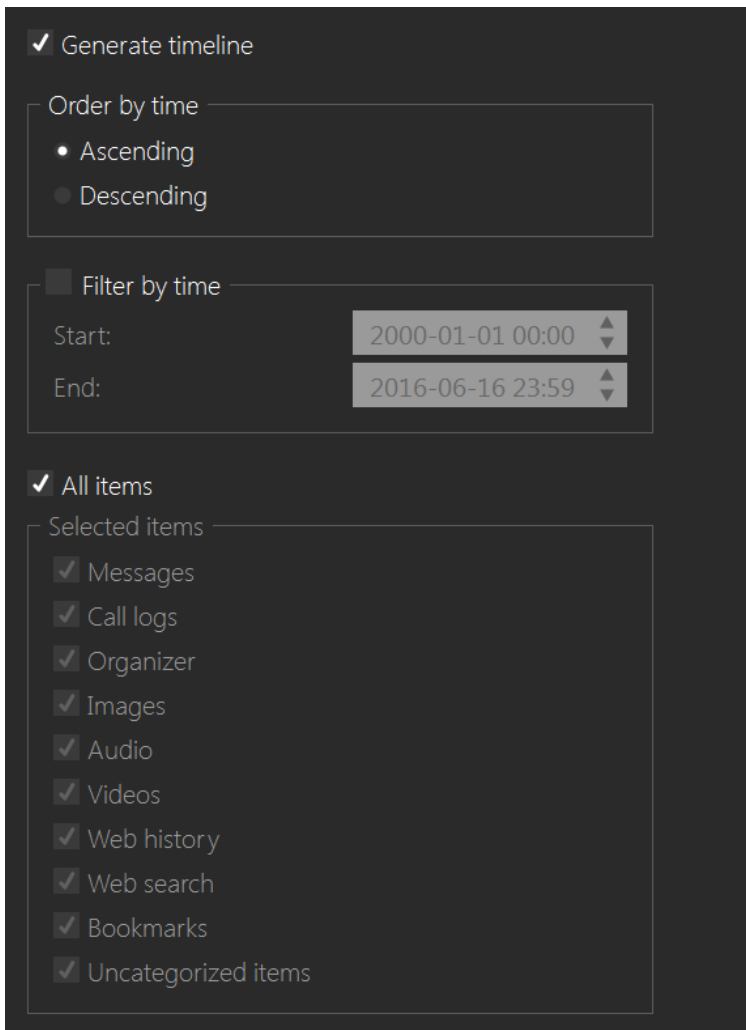


6.38 Data - Timeline

Timeline section aggregates all extracted items that contain time and date information and shows them again in chronological order.

Creation and modification time of files and folders extracted from the phone are excluded from the timeline because there is a lot of systems generated files and such information is not forensically interesting.

All data that you want to be shown in the timeline must be marked for extraction in its specific section. If you want a timeline to include messages, for example, you have to check the Messages section to be extracted.



6.38.1 Generate timeline

Turns the timeline on and off

6.38.2 Order by time

Here you can choose if events are flowing naturally - Ascending or in reverse order - Descending

6.38.3 Filter by time

Choose the start and end interval of events you want to have in the timeline.

6.38.4 Selected items

You can specify which type of items you want to appear in the timeline.

6.38.5 Timeline data may contain for example:

- Creation and modification times of contacts.
- Times when a given message was sent or received.
- Time when a given call was made.
- Time when a given event from organizer was created or modified
- Time when a given event from organizer starts or ends.
- Time when a task in an organizer was created, modified or completed.
- Time when a given image/recording/video was created or edited.
- Time when a given web page was visited.
- Time when a user searched for a given query in a web browser.
- Time when a given bookmark was created or modified.
- Time when the user logged in for last time in a given application.
- Last time when the device was connected to a given Wi-Fi network.
- Time when a given application was installed.
- Time when a given place was visited.
- Time when a given notification was created.
- Time when a given sport session from fitness application started or ended.
- Time when a given QR code was scanned.
- and plenty more.

6.38.6 Example of timeline report:

Case Label: Kentucky church Case Evidence Number: 8974969-589-468 Device Label:

Timeline (2260)

All events in ascending order

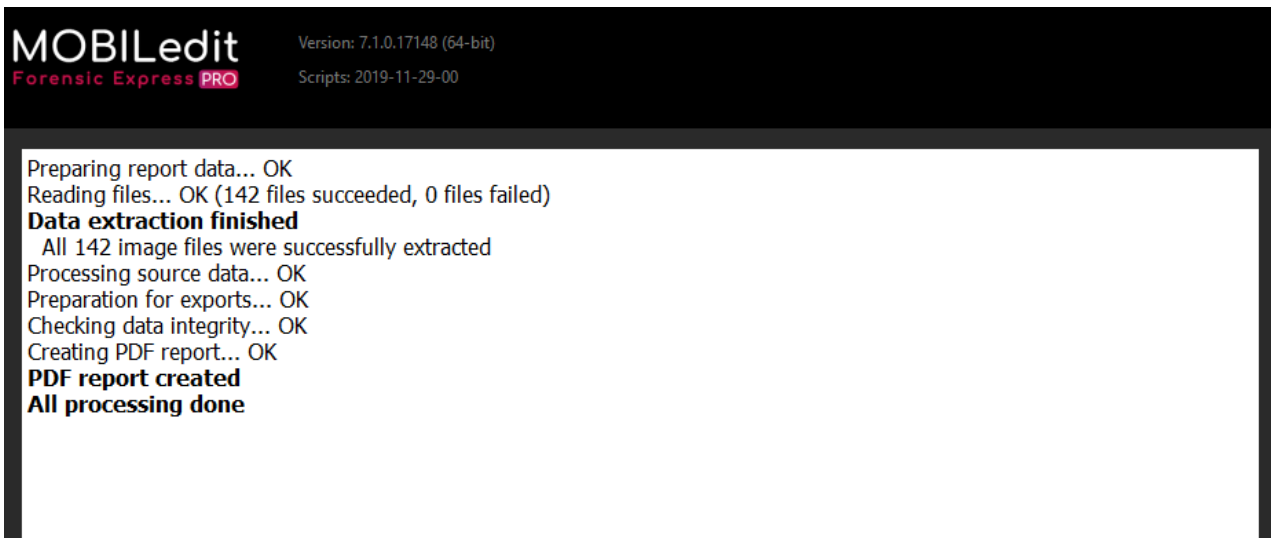
* Entries marked with asterisk are cross-referenced from phone contacts

<p>Time (connecting)</p> <p>Event Origin Phone Bluetooth Pairings</p> <p>Event Type Uncategorized Item</p>	<p>1 CMP018</p> <p>Device Address 00:11:67:83:12:F8</p> <p>Bond State Bonded</p> <p>Source File phone/applications1/Content Providers/BluetoothBonded.xml</p>
<p>Time (connected time)</p> <p>Event Origin Phone Bluetooth Pairings</p> <p>Event Type Uncategorized Item</p>	<p>2 CMP018</p> <p>Device Address 00:11:67:83:12:F8</p> <p>Bond State Bonded</p> <p>Source File phone/applications1/Content Providers/BluetoothBonded.xml</p>
<p>Time (connected time)</p> <p>Event Origin Phone Bluetooth Pairings</p> <p>Event Type Uncategorized Item</p>	<p>3 CMP018</p> <p>Device Address 00:11:67:83:12:F8</p> <p>Bond State Bonded</p> <p>Source File phone/applications1/Content Providers/BluetoothBonded.xml</p>
<p>Time (disconnected)</p> <p>Event Origin Phone Bluetooth Pairings</p> <p>Event Type Uncategorized Item</p>	<p>4 CMP018</p> <p>Device Address 00:11:67:83:12:F8</p> <p>Bond State Bonded</p> <p>Source File phone/applications1/Content Providers/BluetoothBonded.xml</p>
<p>Time (connected time)</p> <p>Event Origin Phone Bluetooth Pairings</p> <p>Event Type Uncategorized Item</p>	<p>5 CMP018</p> <p>Device Address 00:11:67:83:12:F8</p> <p>Bond State Bonded</p> <p>Source File phone/applications1/Content Providers/BluetoothBonded.xml</p>
<p>Time (disconnected)</p> <p>Event Origin Phone Bluetooth Pairings</p> <p>Event Type Uncategorized Item</p>	<p>6 CMP018</p> <p>Device Address 00:11:67:83:12:F8</p> <p>Bond State Bonded</p> <p>Source File phone/applications1/Content Providers/BluetoothBonded.xml</p>
<p>Time (connected time)</p> <p>Event Origin Phone Bluetooth Pairings</p> <p>Event Type Uncategorized Item</p>	<p>7 CMP018</p> <p>Device Address 00:11:67:83:12:F8</p> <p>Bond State Bonded</p> <p>Source File phone/applications1/Content Providers/BluetoothBonded.xml</p>

6/20/2018 12:53 PM Generated by Compelson MOBILedit Forensic Express 5.3.0.12966 1913/2537

6.39 Data - Data extraction log

Following tab displays information about ongoing extraction:



If you select the **Data Extraction Log** option in the [Specific selection](#)(see page 325), you will get a brief resume of the extraction tab in your report as well:

Data Extraction Log

```
2019-12-02 13:42:39 Data extraction started - MOBILedit Forensic Express, version 7.1.0.17148 (x64)
2019-12-02 13:42:41 All 142 image files were successfully extracted
2019-12-02 13:42:41 Data extraction finished
```

7 Applications

Perform advanced applications analysis using adaptive and in-depth methods to ensure you retrieve the most data available for each app, including deleted data and data from encrypted apps. We regularly provide updates of Forensic Express in order to support the latest apps and new versions.

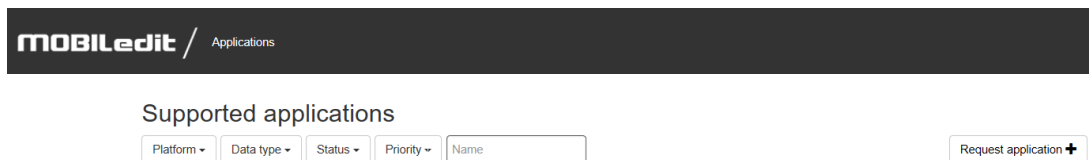
The database of the supported apps is available at <https://apps.mobiledit.com/>.

7.1 Supported applications

Due to the growing number of supported apps in Forensic Express, we have introduced a dynamic online database where you can easily find any currently supported app, what kind of data you can expect to find in each app, and even make requests for new support of any app.

The database of the supported apps is available at <https://apps.mobiledit.com/>.

7.1.1 Sort and search



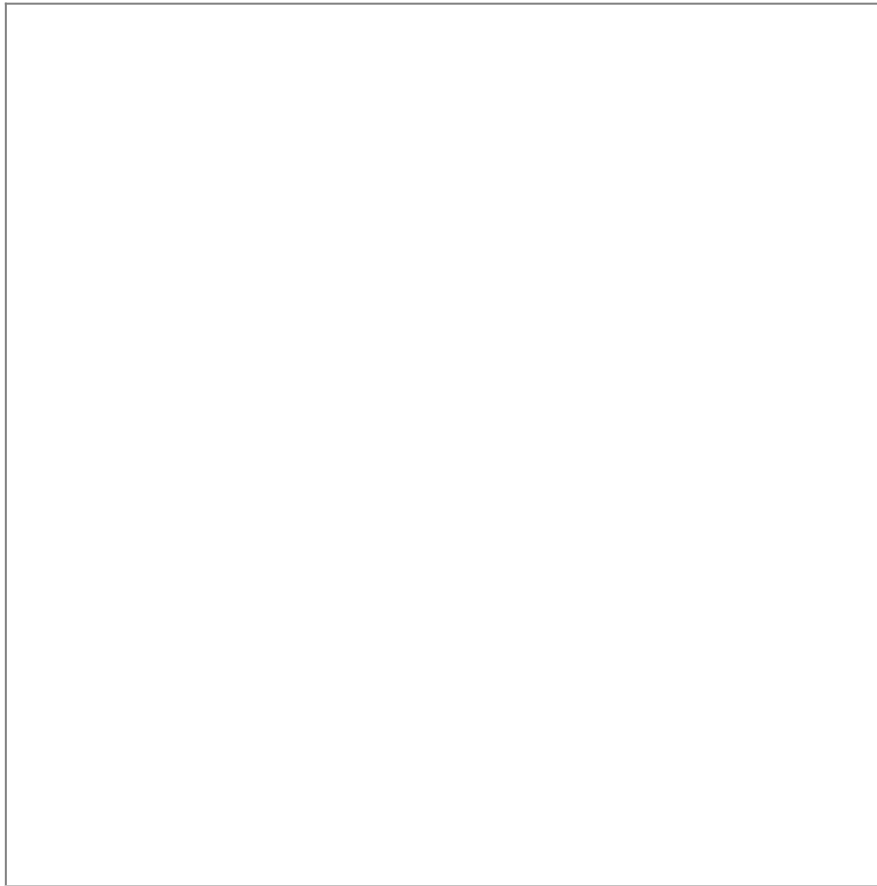
At the top of the page, you sort and search for applications based on what you want to find.

Sorting By platform	Sorting by data type	Sorting by status	Sorting by priority
Android	Accounts	Supported	Low
iOS	Passwords	Confirmed	Medium
Web	Contacts	Requested	High
	Groups		
	Messages		
	Calls		
	Organizer		
	Tasks		
	Notes		

	GPS Locations		
	Networks		
	Bookmarks		
	Search History		
	Web History		
	Media Files		
	Filesystem		
	Other		

7.1.2 The database

Below this, you can see the complete list of supported apps, together with the supported platform, supported (obtainable) data types and more info.



At the online app database page, you can also directly request support for any application to be added to the list of supported apps.

More info on how to request the support of an app is available [here](#)(see page 407).

7.2 Advanced techniques to extract messages and files

- [Rooting / Jailbreaking](#)(see page 397)
 - [Rooting](#)(see page 397)
 - [Jailbreaking](#)(see page 397)
- [Creating a physical image of your device](#)(see page 398)
 - [MTK Hack](#)(see page 398)
 - [EDL Hack](#)(see page 398)
 - [LG Hack](#)(see page 398)
 - [TWRP Method](#)(see page 399)
 - [Dirty Cow](#)(see page 399)
- [Using an App downgrade function in our software MOBILedit Forensic Express](#)(see page 399)

Some applications do not provide the information that you need (e.g. messages, call logs) by themselves since the information is encrypted by developer/manufacturer.

There are a few ways how to extract the information you need:


1. Rooting / Jailbreaking your device
2. Creating a physical image of your device
3. Using an App downgrade function in our software MOBILedit Forensic Express

7.2.1 Rooting / Jailbreaking

7.2.1.1 Rooting


Most Android devices should be able to be rooted. However, the process of rooting is specific to each phone model, version of Android and build number, so you always need to find the right tool according to your phone model.

You can root a majority of modern Android phones using an app called [KingoRoot](#)⁸⁶, if for some reason this method doesn't work for you (locked bootloader, Knox, etc.), you may be able to find help on how to root your phone at [XDA Developers](#)⁸⁷, which is a website with a large active user community dedicated entirely to Android smartphones.

 Please note that sometimes it is necessary to unlock your phone's bootloader in order to root it. You can find a step-by-step tutorial on how to unlock the bootloader on your phone manufacturer's webpage.

Once rooting has been completed successfully the phone is then switched to so-called "rooted mode", and you then will be able to extract and analyze the deleted data.

If you are in need of further assistance please let us know and we will look further to help resolve any issue you are experiencing.

 Rooting your phone may void the manufacturer's warranty and could cause security risks. Please take this into consideration before performing this process.
Rooting a Samsung device will trip the Knox Warranty void flag which will make the data stored in Knox permanently inaccessible.

7.2.1.2 Jailbreaking

There are three ways of jailbreaking your iOS:

1. **Tethered** - This method requires you to connect your iPhone to your computer and use an external application to jailbreak it. Once you restart your iPhone, the jailbreak is undone, but please note: your device will not be usable until you jailbreak it again using the same method.
2. **Semi-tethered** - This method doesn't require you to connect your iPhone to a computer in order to jailbreak it, however, the jailbreak is still undone every time you reboot your device, or, after a certain amount of time passes.
3. **Untethered** - This method doesn't necessarily require a computer to perform a jailbreak on your device and also modifies the iOS on a deeper level which means that no matter how many times you reboot your device, it stays jailbroken until you manually "un-jailbreak" it.

There are specific known ways to jailbreak almost every iPhone, iPad or iPod Touch running on almost every iOS, except the latest releases - as it usually takes a few months to find a way of jailbreaking the newest version of iOS.

This means that there is no way of describing them all in a single article.

Currently, the most often used apps for jailbreaking iOS devices are Pangu or Cydia Impactor. You can learn more about how Cydia works on the app developer's official website [here](#)⁸⁸, or you can read [this article](#)⁸⁹ which describes a simplified process of iOS jailbreaking.


⁸⁶ <https://www.kingoapp.com/>

⁸⁷ <http://xda-developers.com/>

⁸⁸ <http://www.cydaiimpactor.com/>

⁸⁹ <https://downloadcydia.org/cydia-impactor/>

You can see a full list of available jailbreaks for each device and version [here](#)⁹⁰.

 Jailbreaking a device may void the manufacturer's warranty and could cause security risks. Please take this into consideration before performing this process.


7.2.2 Creating a physical image of your device

There are many ways how to create a physical image from a device. You can, of course, use some tools of your own and use our software for extraction but our product MOBILedit Forensic Express does offer some tools as well:

7.2.2.1 MTK Hack

There is a way of extracting a physical image from phones with MediaTek chipsets without root access (rooting the phone).

This exploit method does not work on all MTK-equipped devices, but sometimes it is the only way of acquiring the physical image because the phone does not have to be booted up or unlocked in order to perform this operation; which means you can try even if the phone is off or locked.

 This will not work for most MTK devices with locked bootloaders. In order to use MTK hack on such devices, the bootloader has to be unlocked first.

More information about how to use MTK Hack in MOBILedit Forensic Express can be found [here](#)(see page 60).

7.2.2.2 EDL Hack

There is also a way of extracting physical images from phones with Qualcomm chipsets without root access (rooting the phone).

This exploit method does not work on all Qualcomm-equipped devices and it is best when used with an EDL cable. More information about how to use EDL Hack in MOBILedit Forensic Express can be found [here](#)(see page 50).

7.2.2.3 LG Hack

The "LG Hack" feature works on all LG smartphones with the new version of LG LAF protocol (this is a service download mode similar to Samsung Odin download mode). One of the first devices to feature this version was the first LG G flagship.

Every LG smartphone from the year 2013 and newer should, therefore, support our LG hack.


With some of them - LG G4 for example - you are even able to browse the phone's filesystem via the "Browse Phone" option in Forensic Express.

This exploit takes advantage of "LG Flash Mode" - used primarily for updating firmware.

More information about how to use LG Hack in MOBILedit Forensic Express can be found [here](#)(see page 55).

⁹⁰ <https://www.reddit.com/r/jailbreak/wiki/escapeplan/guides/jailbreakcharts>

7.2.2.4 TWRP Method

 The device has to have its bootloader unlocked in order to proceed with this method.

Every Android phone has a "recovery" partition which is by default used for performing factory resets using an OEM's preloaded tools. However, this partition can be modified in order to replace the default tools by third-party recovery tools such as TWRP.

These recoveries are (unlike the stock ones) capable of modifying all the internal system partitions of your phone or tablet (they need this capability in order to flash custom firmware).

TWRP even comes with a built-in file manager with unlimited root access so you can modify, add or delete any system files manually. This process allows you to gain physical image, therefore bypass the otherwise locked device's protection.

However, if the image is encrypted by the system itself, we are only able to get the encrypted physical image.

More information about how to use the TWRP method in MOBILedit Forensic Express can be found [here](#)(see page 78).

7.2.2.5 Dirty Cow

MOBILedit Forensic Express can also use a Dirty cow (Dirty Copy-On-Write) exploit which can temporarily root a device that has an Android version up to 7.


The root is removed once the device is restarted.

More information about how to use the Dirty cow exploit in MOBILedit Forensic Express can be found [here](#)(see page 70).

7.2.3 Using an App downgrade function in our software MOBILedit Forensic Express

Due to better security, some applications manufacturers made restrictions on what data can be acquired from their apps. This is especially relevant for non-rooted phones.

To bypass this we have introduced the App downgrade, feature in MOBILedit Forensic Express, which will downgrade the apps to a version, in which there was no problem in obtaining the data from them directly.

 Please note that only some apps support this feature as of yet, although we are working on expanding their list.

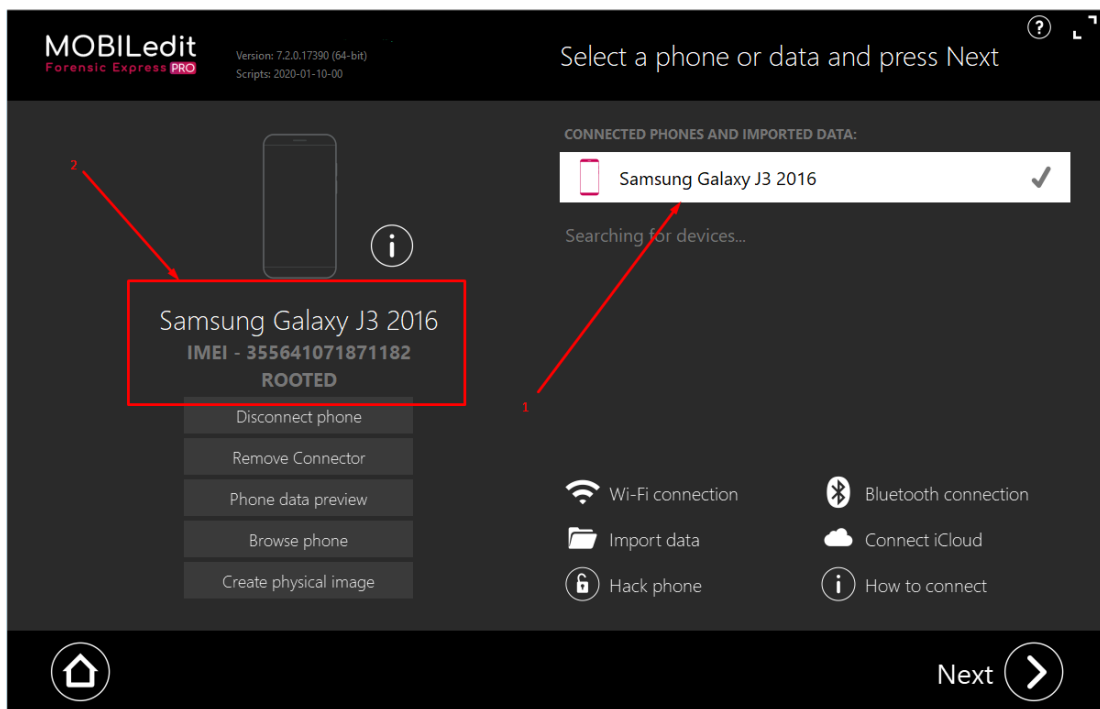
More information about how to use the App downgrade in MOBILedit Forensic Express can be found [here](#)(see page 408).

7.3 How to make an application backup

1. Open MOBILedit Forensic Express and click "Start".



2. Plug your phone to USB. You will see that on your phone Forensic Connector screen will show up. MOBILedit will then find the connected phone.

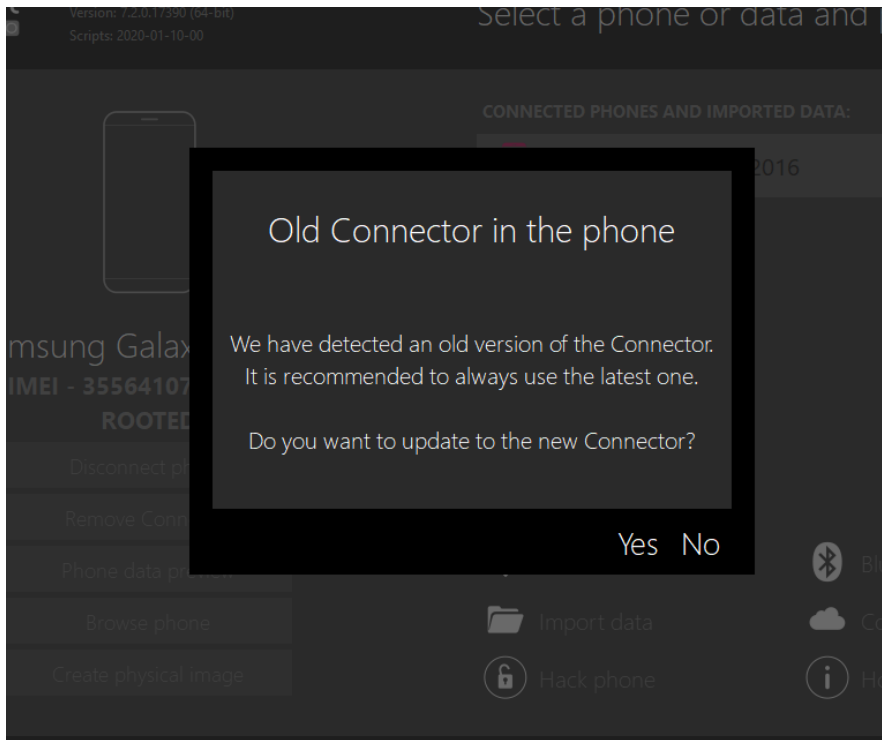


[1] Shows the phone type currently connected

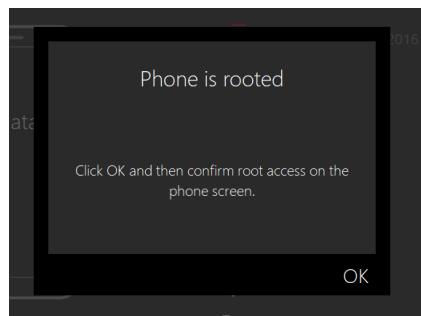
[2] Shows if the phone is rooted or not

Click on "Next".

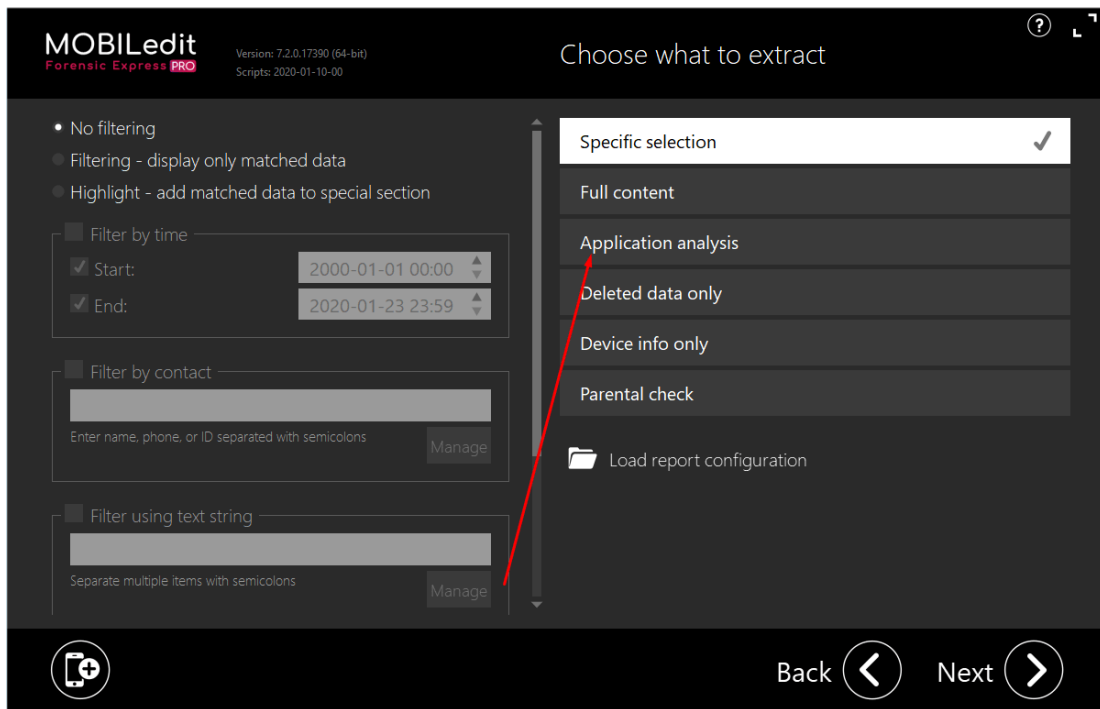
3. if you see the dialog about Old Connector as below, click Yes and wait until the Connector updates.



4. If your phone is rooted/jailbroken, you will probably see this dialog. Confirm by clicking OK.

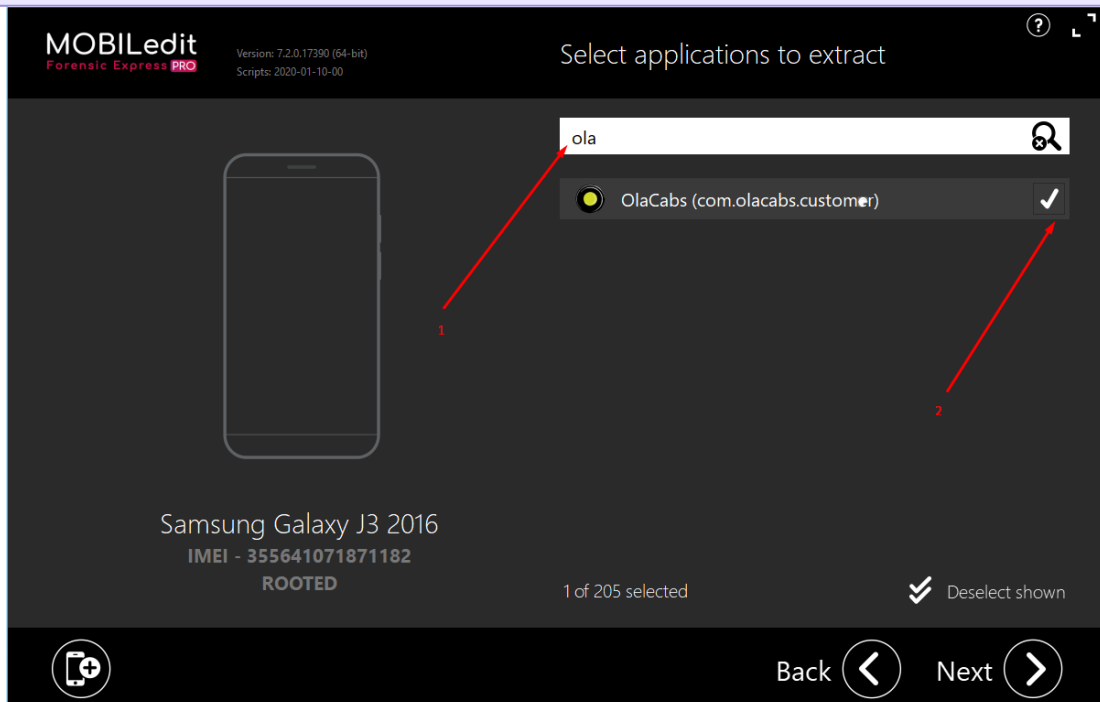


5. Now you are in the main dialog where you choose what you want to do. Choose Application analysis and confirm by clicking Next.



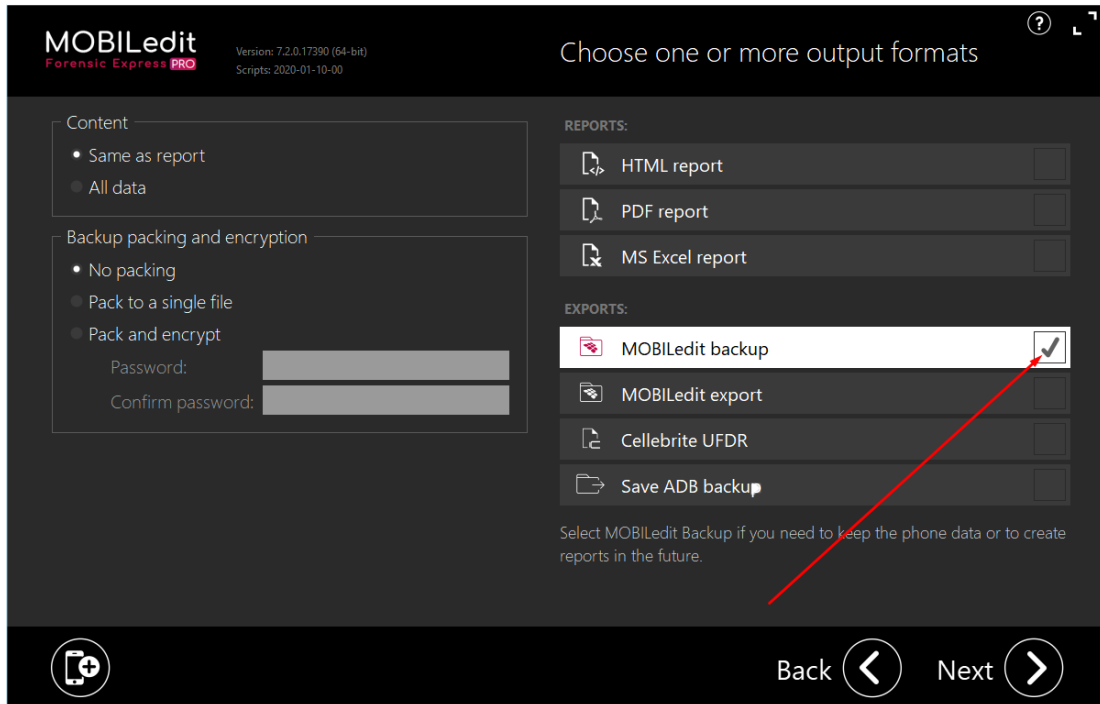
6. Now you can see a list of all the applications installed on the mobile phone. Choose the one you want to analyze. You can either scroll down with the scrollbar or use the find field where you can write down the name of the app.

Let's say you want to analyze Ola Cabs app. Write ola in the lookup field [1], OlaCabs will be listed. Make sure you check it up in the right box as shown in the picture [2]. Then click Next.



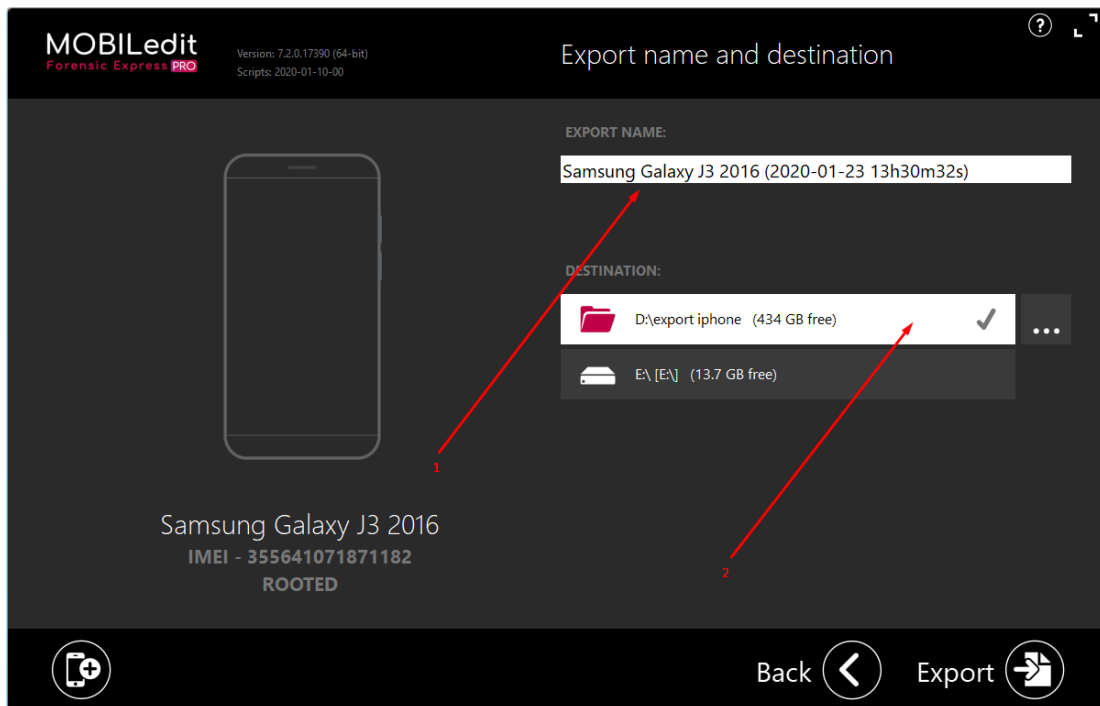
7. In the next frame, you will find details about the particular Case, Phone and Investigator. You can safely skip them all, don't fill anything just click the Next button.

8. Now you can choose which output you want to have. If you are analyzing a particular app for the first time, you need to make a backup. It will create a backup XML file together with many other files and folders that will be discussed later. Choose MOBILedit backup and click Next.

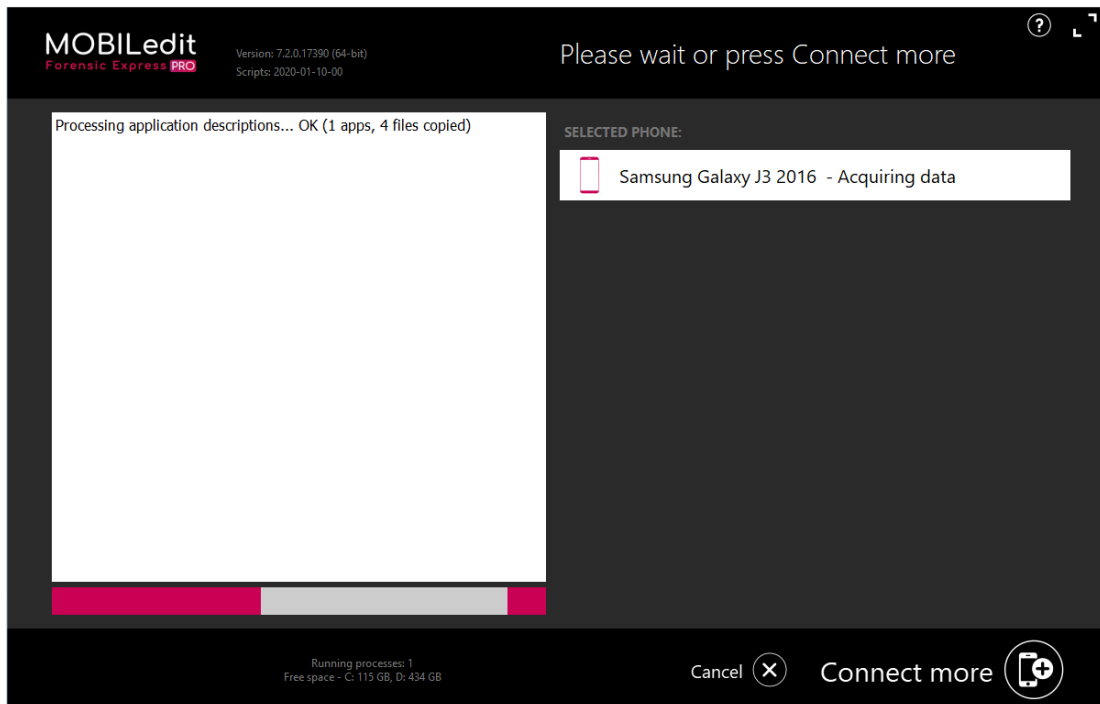


9. On the next screen you will see the Export name of the folder [1] and the Destination [2] where the export folder will be. You can change both of them. Click Export.

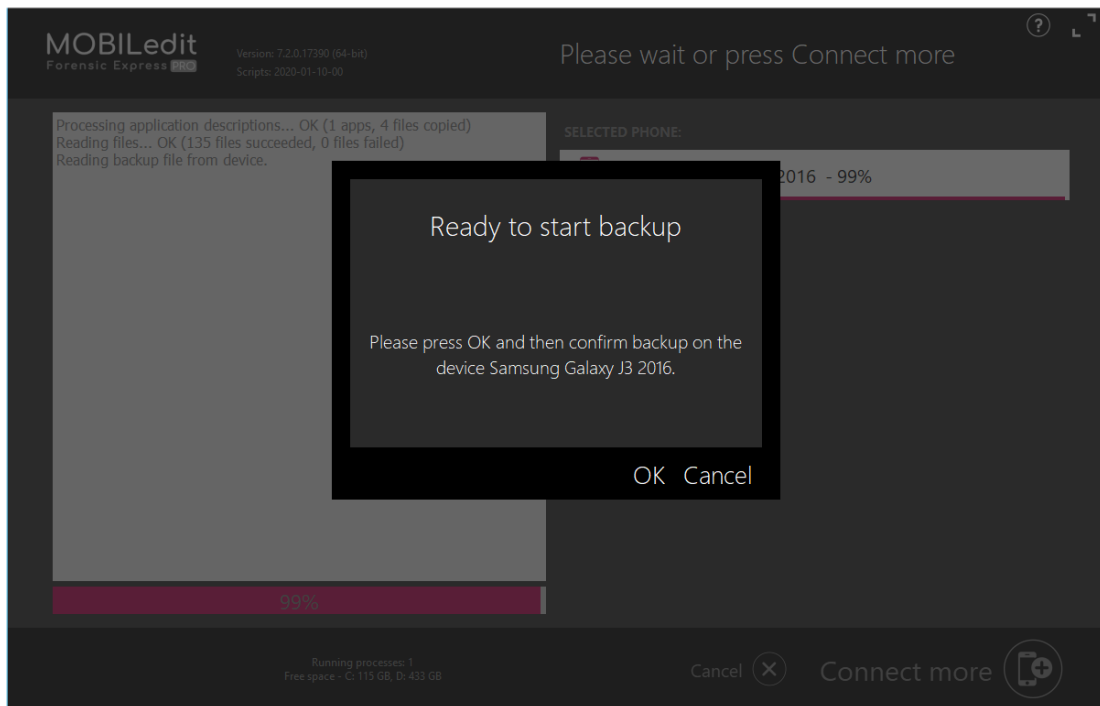
i By default, the Export name is the name of the phone together with timestamp when the backup was done and Destination is a path you can freely set.



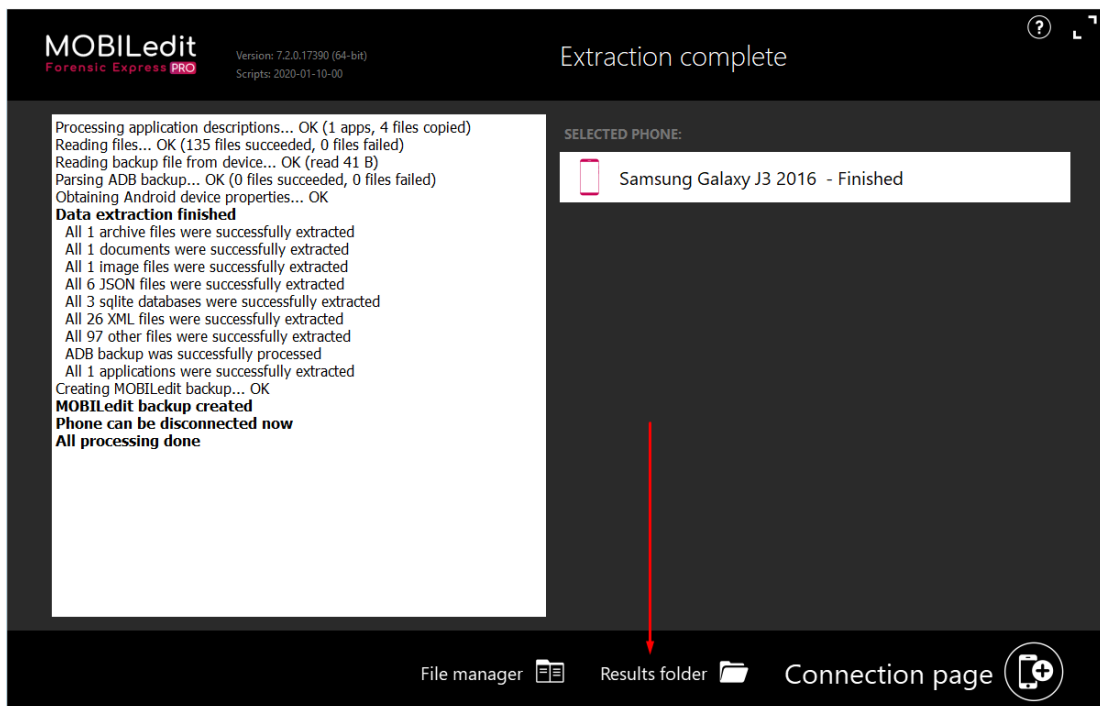
10. You will see MOBILedit started to make the backup.



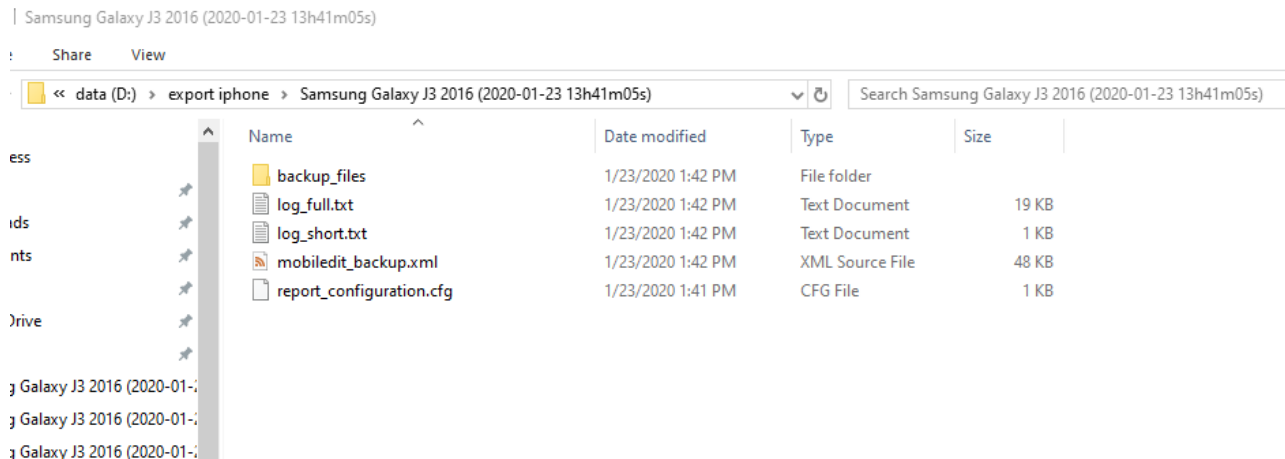
11. You will be prompted to confirm the device's backup, press OK. Then you will also be prompted to Back up data on your phone, so do not forget to confirm that as well.




12. When everything went OK, you will see a screen similar to this. Click on the Result folder to see the folder with backed up data



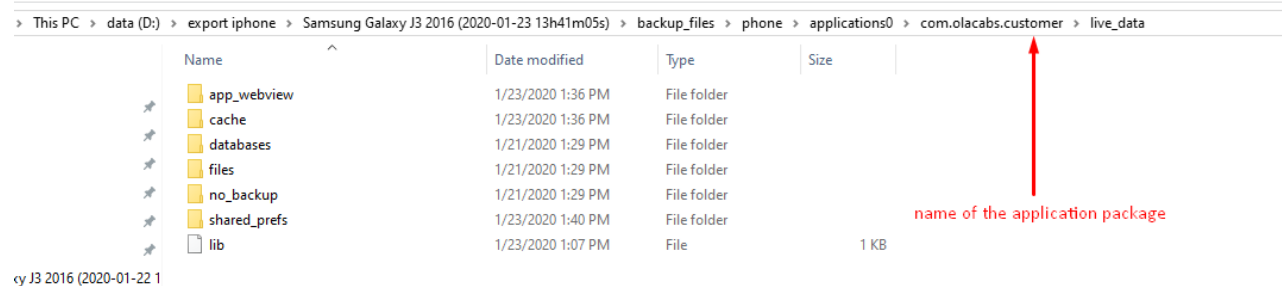
13. You should have a folder at the path you specified in step 9). The folder contains mobiledit_backup.xml and other files and folder backup_files. It should look something like this picture



14. If you dig deeper into the backup_files folder, you will see it contains other subfolders called phone and file called fileHases.csv. In the phone folder, there are 4 subfolders with possible other sub/subfolders and files.


 Which exact folders and files it contains and where they are is application-dependent.

In application0 there is a folder with the same name as is the name of the application package we just analyzed (in our case it is com.olacabs.customer), and inside there is a folder called live_data containing all the data from the backed-up application,




It is generally hard to say which data are important for further processing, and in which folders they are because it is different for each and every application. Some applications hold all of their data here and are quite simple for further processing and analyzing, other applications contain all of the data, but are quite difficult for further processing (they might be encrypted, etc..) and other applications don't hold much data in the folder, but hold their data somewhere on the cloud in online databases or somewhere else. Thus, it is always from case to case how to do further processing.

But from the first sight, for example, we might see that there is a folder database, and it should contain some valuable data in SQL (in SQLite files). So this is the way to go to try it first. But here is an important note:

 Never open the original database folder, because it can corrupt some data and you would have to make the backup once again.

Make a copy of the databases first, and if you want to look inside, open the copied file, NOT THE ORIGINAL ONE. What I would recommend is to copy the whole folder (to Desktop for example) and when you want to open a particular file, open it from that copy.

In order for us to further process and analyze an application from the backup, we need the whole original folder. In our case, the folder has a name "Samsung Galaxy J3 2016 (2020-01-23 13h41m05s)".

 Make a zip of the whole folder and send it to us via email.

7.4 Request to add support for analysis of an application

Our online database of [supported applications](#)(see page 394) allows you to directly request support for the analysis of any application. If we are successful, the app will be added to the database and you will be able to obtain data from the app.

How to make a request for support to analyze an application:

1. Visit our online application database [here](#).⁹¹
2. In the top right corner, click on "+ Request application".
3. A request form will be shown to you, please fill in as many fields as possible.

Request for application support

Application Name (optional)

Uri to appstore(optional)

Uri to google play (optional)

Platform

iOS version (optional)

Android version (optional)

Note (optional)

[Back to List](#)

© 2018 - Compelson

4. The most important thing to fill in is the URL to the App Store or Google Play Store, so we can easily locate the application to begin working on your request.

5. Click 'Create request'.

⁹¹ <https://apps.mobiledit.com/>

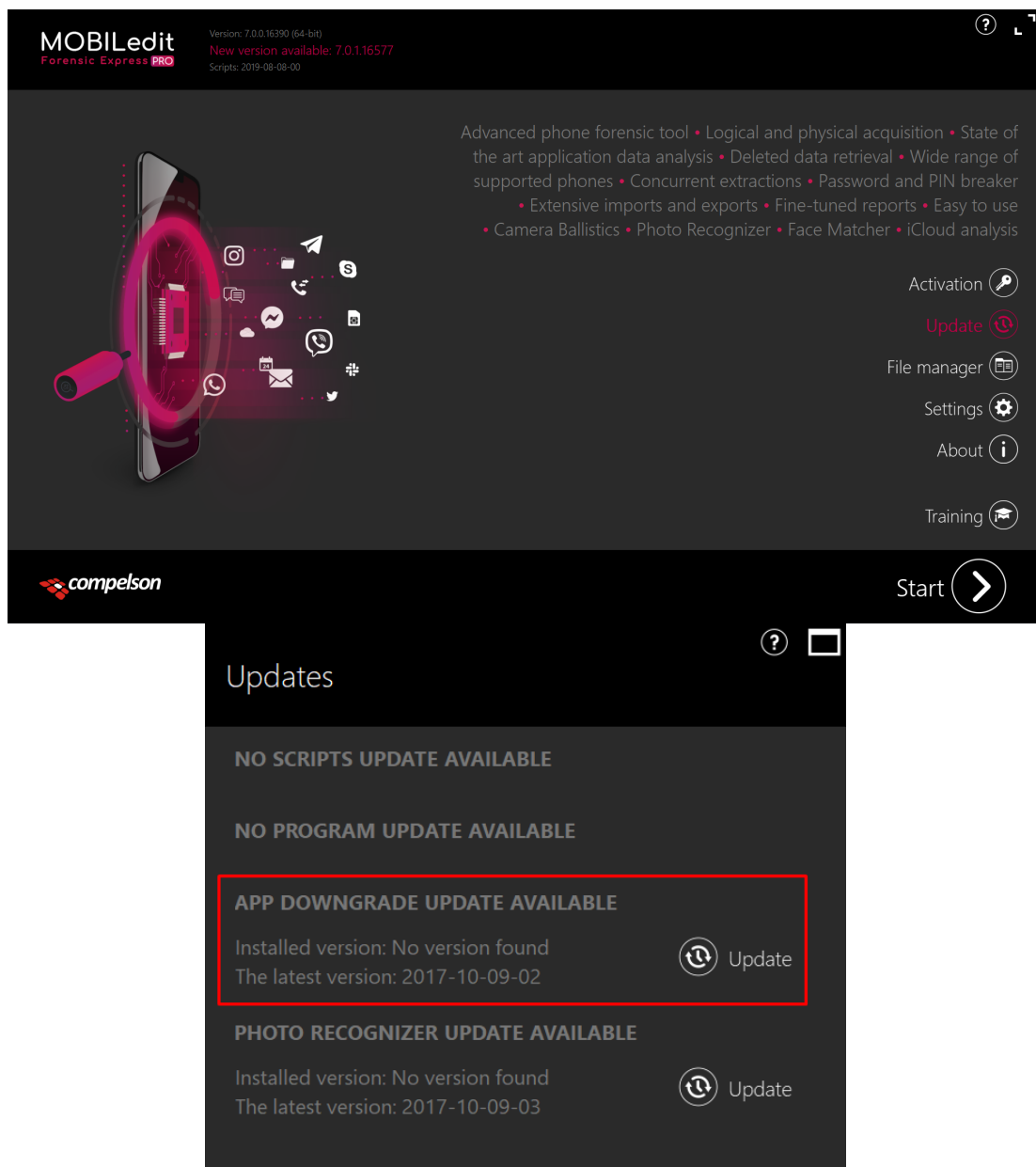
7.5 App downgrade

- [Functionality](#)(see page 409)
- [List of supported apps](#)(see page 412)

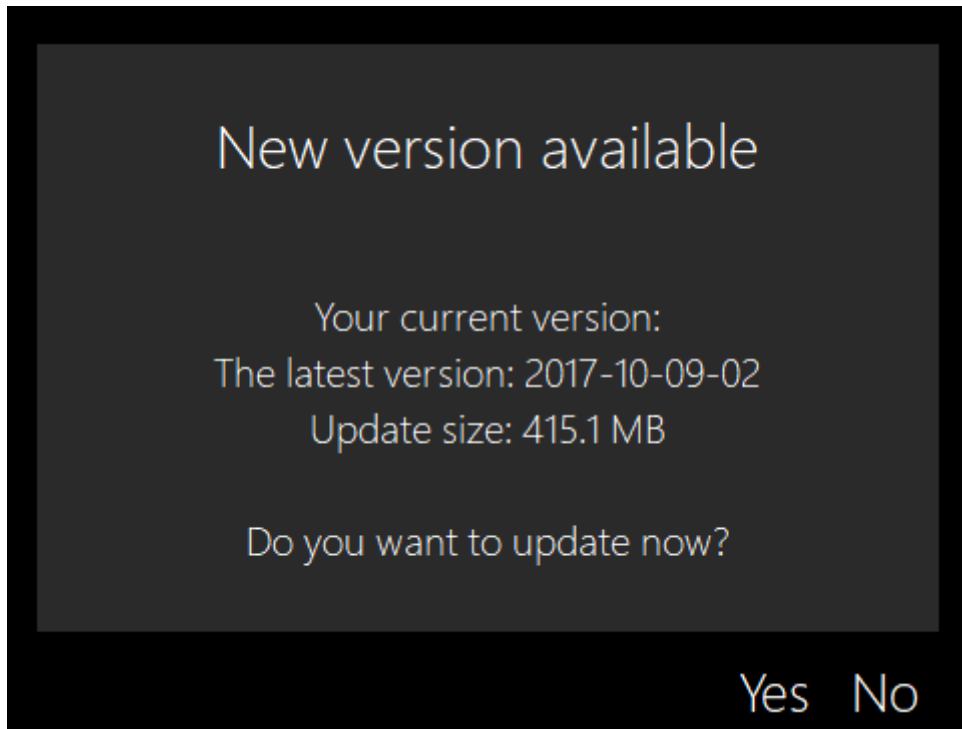
Due to better security, some applications manufacturers made restrictions on what data can be acquired from their apps. This is especially relevant for non-rooted phones.

To bypass this we have introduced the App downgrade, feature in MOBILedit Forensic Express, which will downgrade the apps to a version, in which there was no problem in obtaining the data from them directly.

On the main screen of MOBILedit Forensic Express select [Updates](#)(see page 28) and then select App downgrade update - as seen on the screenshots below.



You will then be asked to download an extension for MOBILedit Forensic Express, which consists of the apps .apk installation files. Please confirm the download and wait for it to be completely downloaded.

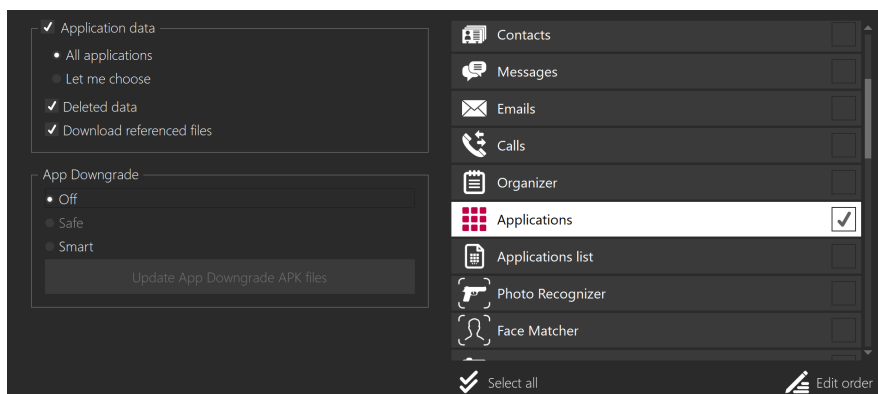


After the download, the installation will start automatically. Once finished, the App Downgrade feature will be included in the Applications section in Specific Selection while creating a report.

Settings and functionality of this feature are described below in the Functionality section of this page.

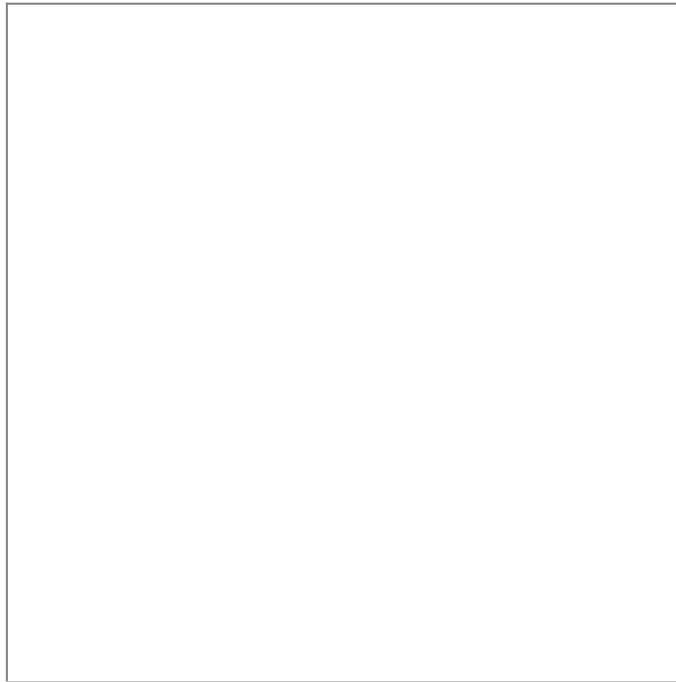
7.5.1 Functionality

To use the App downgrade function, connect a phone to MOBILedit Forensic Express, select Specific Selection, and choose Applications in the right-sided menu. You will now have the option to choose (tick) the App downgrade feature to be used in the data extraction process.

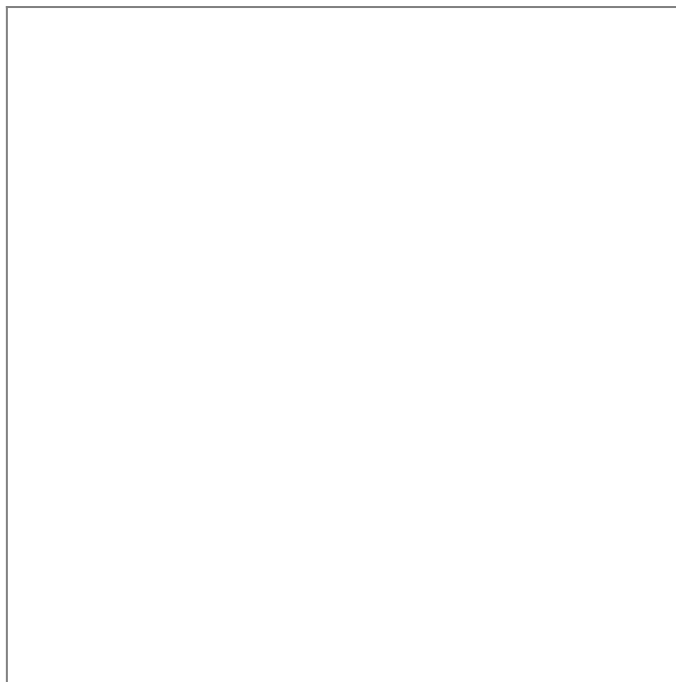


There are two options of App downgrade available - Safe and Smart. The safe option works with Android 4.4+ and 5.0+, but not higher than 6.0, while the Smart option works with the other versions. In case the version of Android

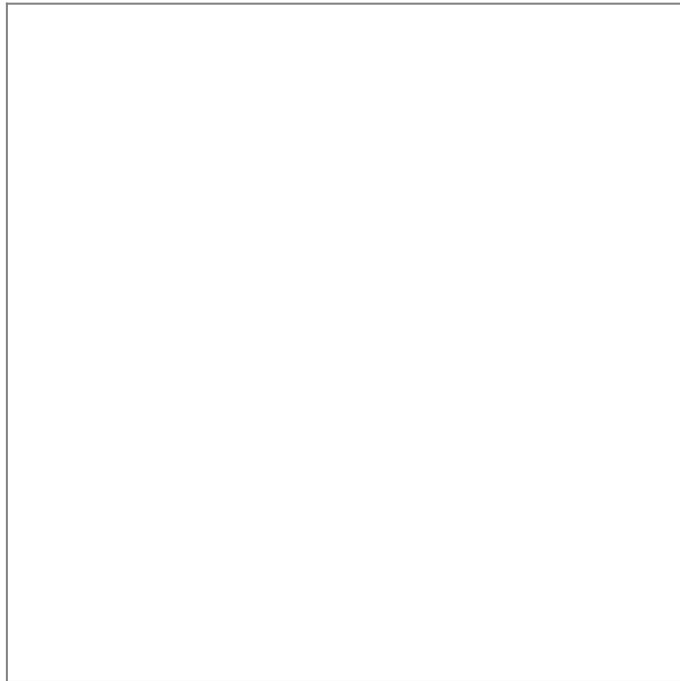
on your phone was automatically detected by MOBILedit Forensic Express, one of the App downgrade options will be accordingly greyed out, so you can be sure you are using the correct one.



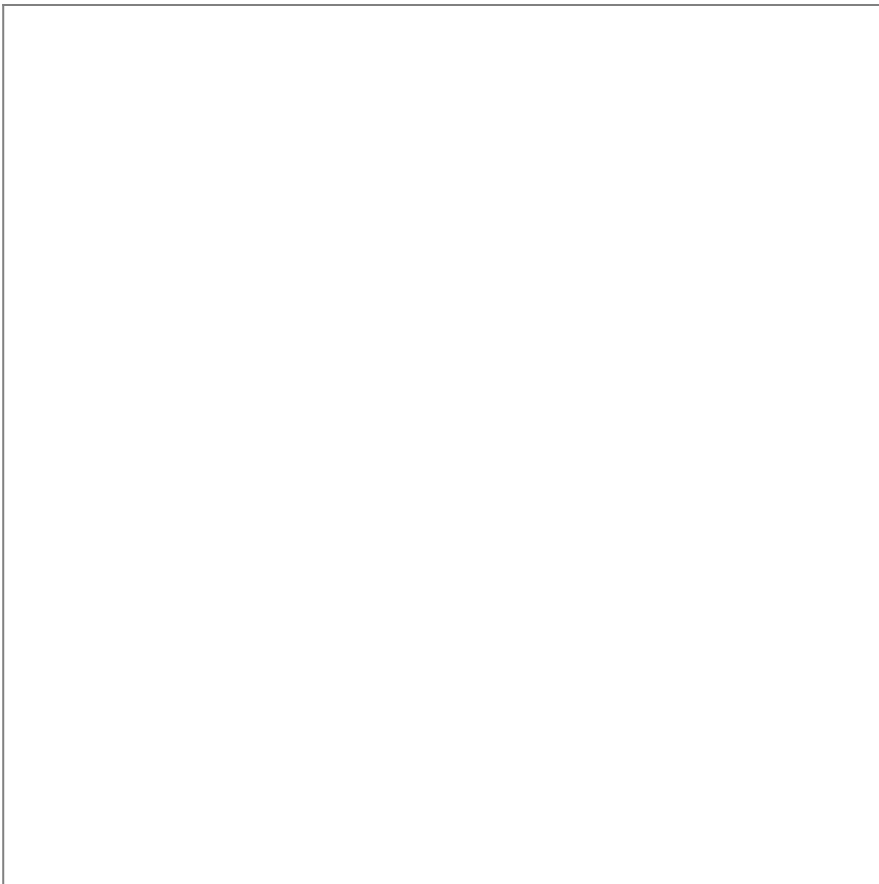
Upon continuing with the extraction you will be asked to allow a test .apk file to be installed to your phone and downgraded. This allows us to check, whether your phone supports the App downgrade feature.



Please mind the following warning message.



When the extraction is started, you will see the downgrading progress on the left side of your screen. Please note that only some apps support this feature as of yet, although we are working on expanding their list.



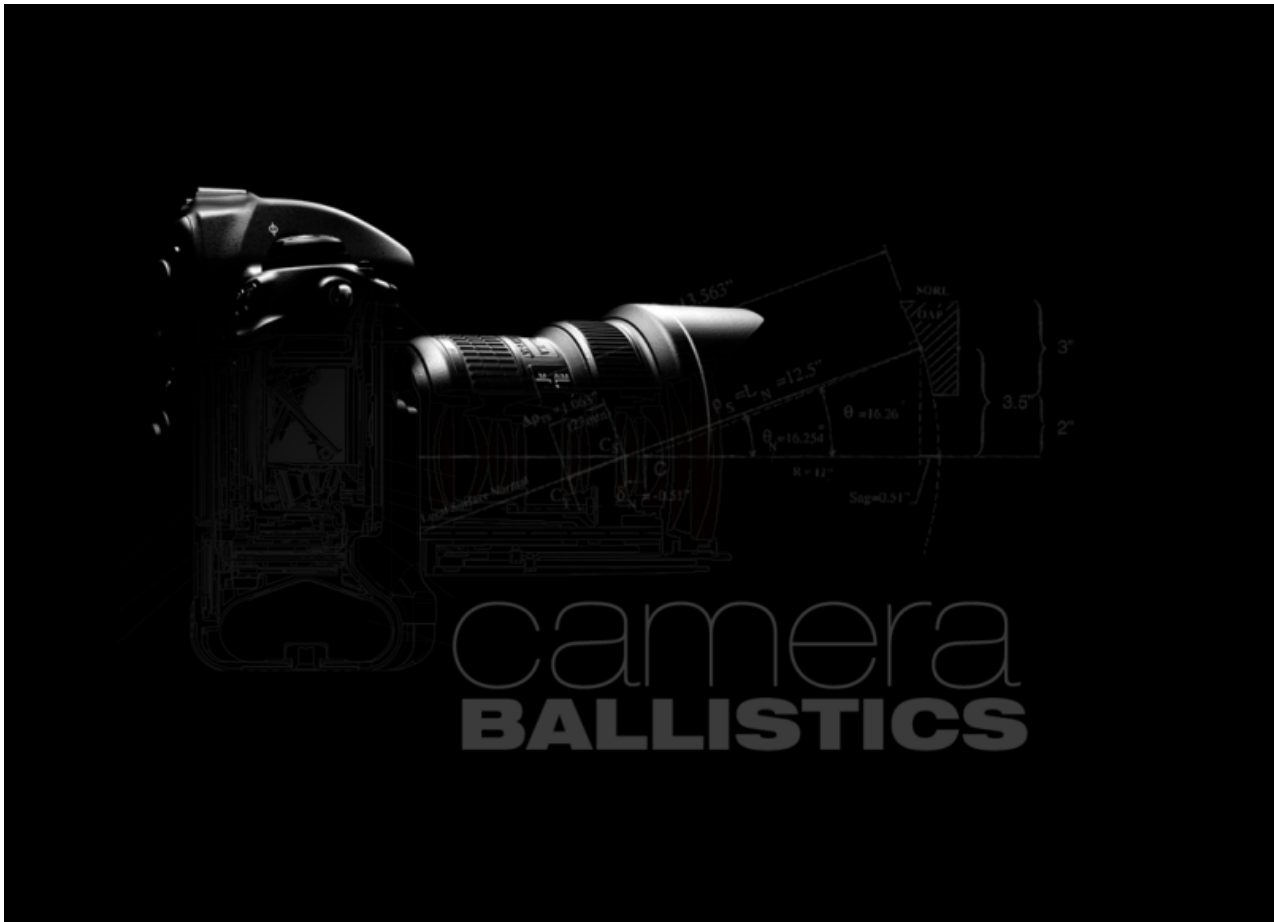
7.5.2 List of supported apps

Find below the ever-growing list of supported apps for App downgrade.

AliExpress	BlackBerry Messenger	Dolphin Browser	Dropbox	Evernote
Facebook	Google Chrome	Google Docs	Google Maps	Instagram
Kakao Talk	Keepsafe Photo Vault	LINE	Messenger	MiTalk Messenger
Mozilla Firefox	Periscope	Skype	Snapchat	Telegram
Todoist	Truecaller	Twitter	Viber	WeChat
WhatsApp	Wickr Me	WunderList		

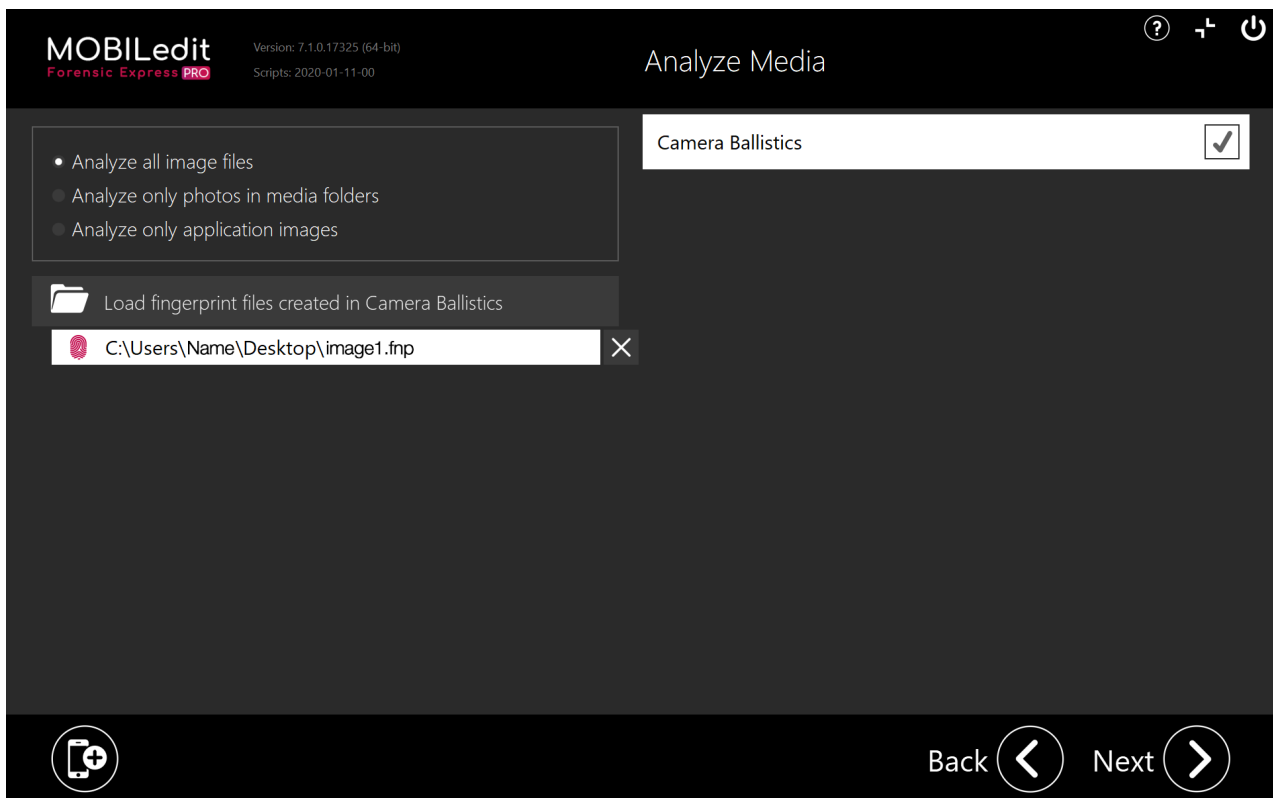
8 Camera Ballistics

Camera Ballistics uses a unique algorithmic method to determine whether a specific photo was taken by a specific camera. This feature is only available for users with a valid license of Camera Ballistics and both applications must be installed on the same machine using the same Windows user profile.



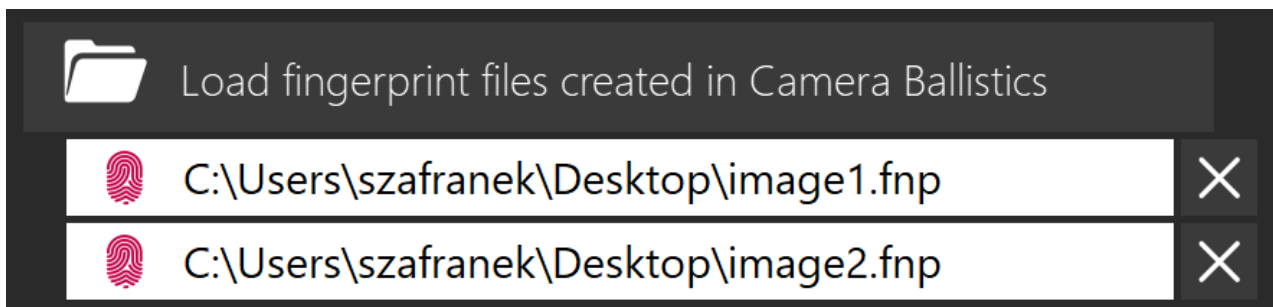
Once you enable the Camera Ballistics feature by checking the "**Use Camera Ballistics photo analyzer?**" option, you can choose from 3 modes:

1. **Analyze all image files** - all image files (contacts photos, user photos, application images, cached images, thumbnails, ...) will be analyzed
2. **Analyze only photos in media folders** - only user-generated photos (DCIM folder) will be analyzed
3. **Analyze only application images** - only image files from applications filesystem will be analyzed




You can enter up to 2 fingerprint files previously generated by Camera Ballistics. These files will not be modified during the analysis process.

Learn how to generate a fingerprint .fnp file [here](https://bit.ly/3eHdgES)⁹².



Once the export is finished you can see the result of the analysis together with image files. A green icon in the top-right of the screen indicates a positive match and the details of both selected fingerprints are available in the **Camera Ballistics** section.

⁹² <https://bit.ly/3eHdgES>

2 2018-08-13_10-53-37 (1).jpg	
	Filename 2018-08-13_10-53-37 (1).jpg
	Path phone/raw3/Media_copy/Images/2018-08-13_10-53-37 (1).jpg
	Size 499 KB
	Modified 2019-10-11 10:21:01 (UTC+2)
	Accessed 2019-10-11 10:21:01 (UTC+2)
	Exposure Time 1 / 33 s
	Focal Length 3.79 mm
	F-Number 2
	Width 1841 px
	Height 1841 px
	Camera Manufacturer HUAWEI
	Camera Model ALE-L21
	Format jpeg
	Date of Generation 2018-08-13 10:53:19 (UTC+2)
	Date of Digitization 2018-08-13 10:53:19 (UTC+2)
	Position
	Latitude 50.10465 °
	Longitude 14.47773 °
	Time 2018-08-13 10:53:16 (UTC+2)
	Altitude 252 m
	Camera Ballistics
	Fingerprint C:\Users\name\Desktop\image1.fnp
	Match ✓ Yes - Image from this camera
	Probability 0.999
	Correlation 0.161864
	Source File phone/raw3/Media_copy/Images/2018-08-13_10-53-37 (1).jpg

Learn more on how the analysis works [here](https://bit.ly/3ihXEK3)⁹³.

8.1 About Camera Ballistics technology

Image sensors suffer from several fundamental and technological imperfections that result in performance limitations and noise. If you take a picture of an absolutely evenly lit scene, the resulting digital image will still exhibit small changes in intensity between individual pixels. This can be due to pattern noise, readout noise or shot noise.

While readout noise or shot noise are random components, the pattern noise is deterministic (its behavior can be mathematically modeled and estimated) and remains approximately the same if multiple pictures of the same scene are taken. As a result, pattern noise might provide the sensor fingerprint we are searching for.

Pattern Noise (PN) has two components: Fixed Pattern Noise (FPN) and photo response nonuniformity (PRNU). FPN is independent of pixel signal; it is additive noise, and some high-end consumer cameras can suppress it. The FPN also depends on exposure and temperature.

PRNU is formed by variation in the dimensions of pixel and inhomogeneities in the silicon which results in variations in pixel output. It is multiplicative noise. Moreover, it does not depend on temperature and seems to be stable over time.

The values of PRNU noise increase with the signal level (it is more visible in pixels showing light scenes). In other words, PRNU noise is suppressed in very dark areas. Moreover, PRNU is not present in areas of an image that are completely saturated. Thus, such images should be ignored when searching for PRNU noise.

⁹³ <https://bit.ly/3ihXEK3>

Since it can be shown that PRNU has a dominant presence in the pattern noise component, PRNU noise is employed as the fingerprint of camera sensors.

Nonetheless, having a larger set of cameras of the same and different models available, and a large set of ground-truth digital images captured by these devices, one can run an experiment to measure the effectiveness and fragility of existing methods. By performing such an experiment it is fairly easy to notice that state-of-the-art source identification methods suffer from a number of basic imperfections. These have been fixed by Camera Ballistics.

There are some freely available libraries that allow the computation of PRNU. Despite this, users often fail and become disheartened. Below, we reveal three major reasons for their failure. Unfortunately, for reasons of security, we are not at liberty to divulge exactly how we managed to solve the problem of providing accurate results.

Impact of optical zoom

Perform a simple experiment. Take a camera with a rich optical zoom option and shoot some test images with varying degrees of optical zoom. Then, carry out camera source identification using the freely available PRNU software.

You'll be disappointed by your results and you'll be asking yourself how this could possibly happen. The reason is a phenomenon called vignetting, which causes a change in the PRNU values at different zoom levels. There are several types of vignetting: mechanical, optical, natural and pixel. Some types of vignetting can be completely covered by lens settings (using special filters), but most digital cameras use built-in image processing to compensate for vignetting when converting raw sensor data to standard image formats such as JPEG or TIFF.

Camera Ballistics managed to solve the problem and provide accurate results.

Impact of embedded camera software

Let's assume that we have 100 different iPhone devices. Moreover, we have a digital image captured by one of these iPhones and we want to identify the particular source device. In other words, we need to have a fingerprint of each device that distinguishes it uniquely and eliminates any features it might have in common with the other devices.

On the other hand, digital consumer cameras contain embedded software that performs operations such as color filter array (CFA) interpolation, white balancing, gamma correction, color enhancement, and interpolation (digital zoom). Because this embedded software is usually common to cameras/smartphones of the same model, it introduces similar changes in the digital images produced by these cameras. This is a serious problem that results in a higher rate of false positives when a large number of source imaging devices of same model are under investigation.

Impact of heavy JPEG compression

Let's stay with the previous iPhone example and assume that this digital camera produces heavily compressed JPEG images. As we know, highly compressed JPEG images exhibit blocking artifacts. These blocking artifacts are another change brought into the image by the camera's embedded software and they are also common to cameras of the same model. In other words, this is another source of false positive results when linking a photo to a large set of possible source cameras of the same model. Moreover, this is quite a common problem in real-life applications (for example, when inspecting Facebook photos or YouTube videos).

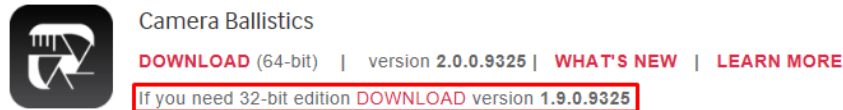
8.2 Minimum system requirements

o enjoy the best possible user experience, we recommend the minimum system requirements to be as follows:

- CPU: Core i3, recommended is Core i5 or better, AVX instruction set is required
- RAM: 2 GB as minimal configuration, 4 GB is recommended
- Disk: 0.5 GB for Camera Ballistics itself, another 32 GB recommended - due to the possibility of analyzing a lot of photos
- OS: 64-bit OS is required, Windows 7 SP1 and above (Windows 8.1 or Windows 10) - Windows 10 is recommended

- Display resolution: 1280 x 960

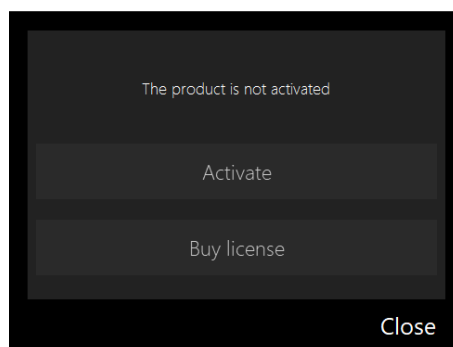
Please note there is a 32-bit version of Camera Ballistics available, in our web page [Download section](#)⁹⁴, if you need it.



8.3 How to activate

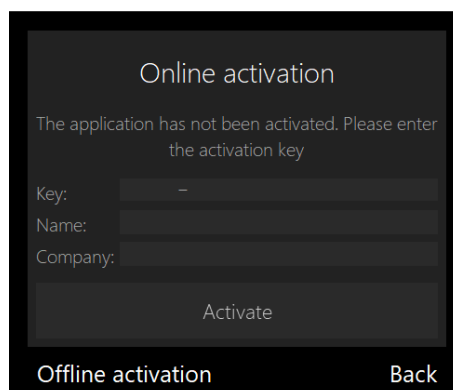
Upon starting a non-activated software you will be automatically asked to submit a license key to activate it.

If you are not asked to submit a key, simply click on the "Activation" button on the home page.



If you already have the license key, click on "Activate"

If not, the "Buy license" button will guide you directly to the [online store](#)⁹⁵.



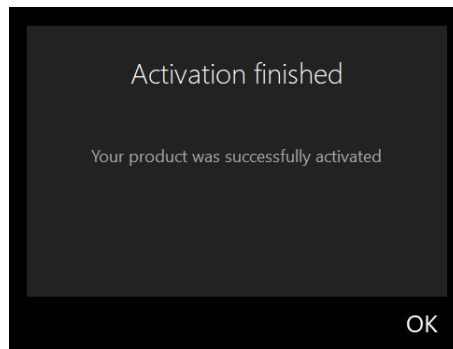
Input your activation key and, optionally, the other details and click on "Activate" to activate the software.

If you do not have an internet connection, you can always use the *Offline activation* option - more info about it is available [here](#)⁹⁶.

⁹⁴ <http://www.mobiledit.com/downloads/>

⁹⁵ <http://www.mobiledit.com/online-store/camera-ballistics>

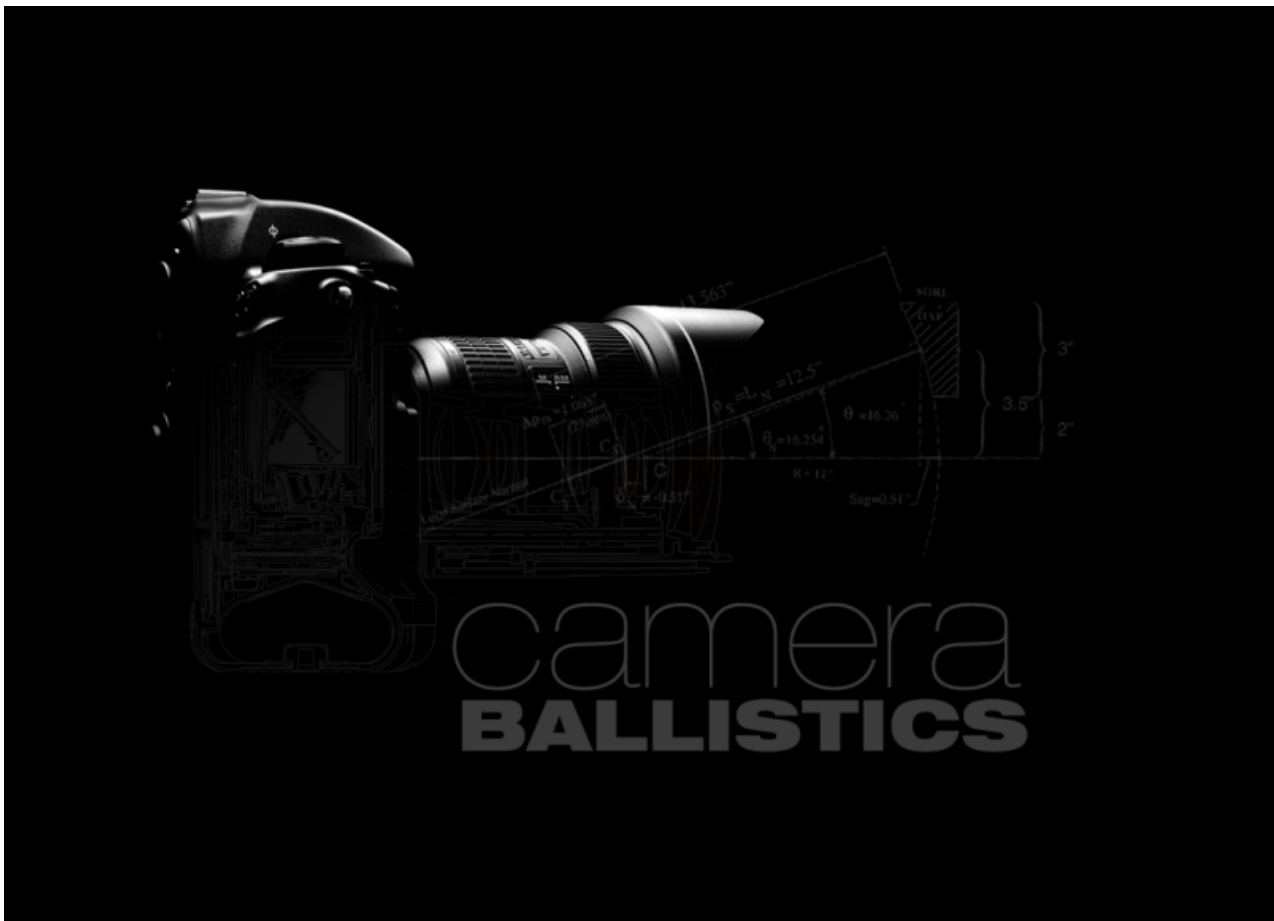
⁹⁶ <http://web.mobiledit.com/activation>



Congratulations, it is done - Camera Ballistics is now activated and offers you its full functionality. Learn more about the tool in the online manual [here](#)⁹⁷.

8.4 Main page

This is the *Home screen*. You will see this screen every time you start the Camera Ballistics. On this page, you can change your activation information, deactivate the software, or check for updates.



⁹⁷ <https://support.mobiledit.com/portal/kb/manuals/camera-ballistics>

In order to learn more about the features of this software click on *Help* or read through the rest of the online manual [here](#)(see page 413). In case of any further questions, you can always contact us [here](#)⁹⁸.

8.5 Camera Ballistics - Updates

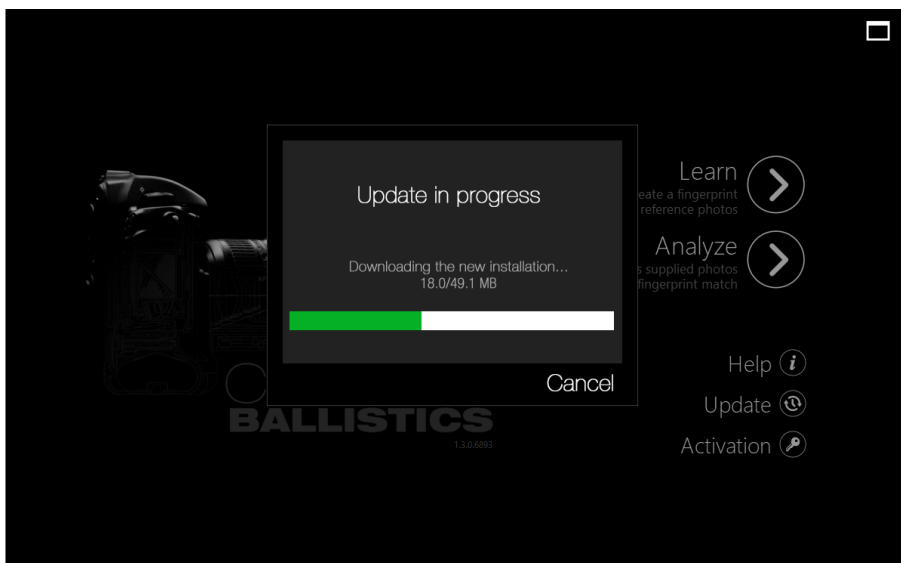
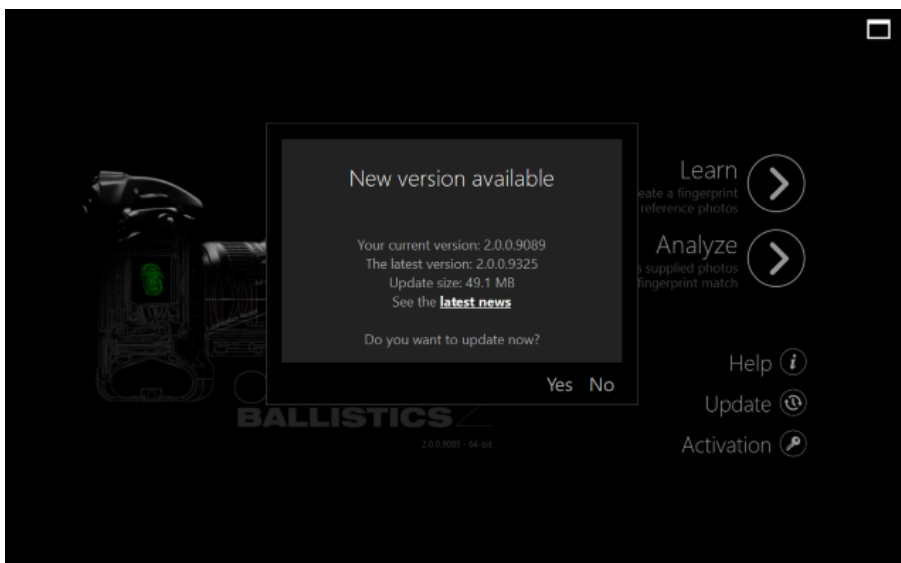
Checking for updates and getting them is very simple.

There is an "Updates" button on the home screen.

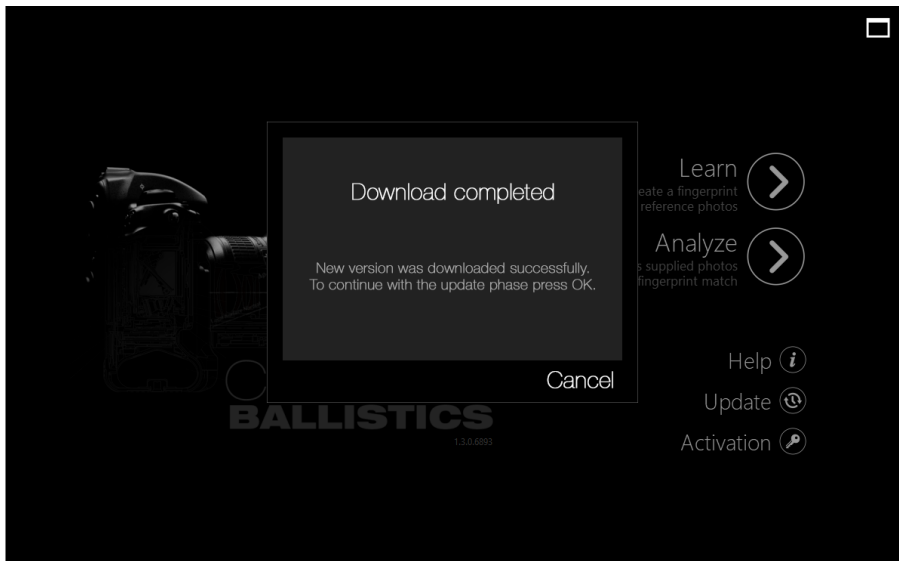
Click on the "Update" button. A window called "New version available" will appear, with information about the possibility to download an update.

This window also contains information about the new version with the latest news (under the link "latest news").

You can confirm the update by clicking on "Yes" or select "No" to download it later.



⁹⁸ <http://www.mobiledit.com/contact>



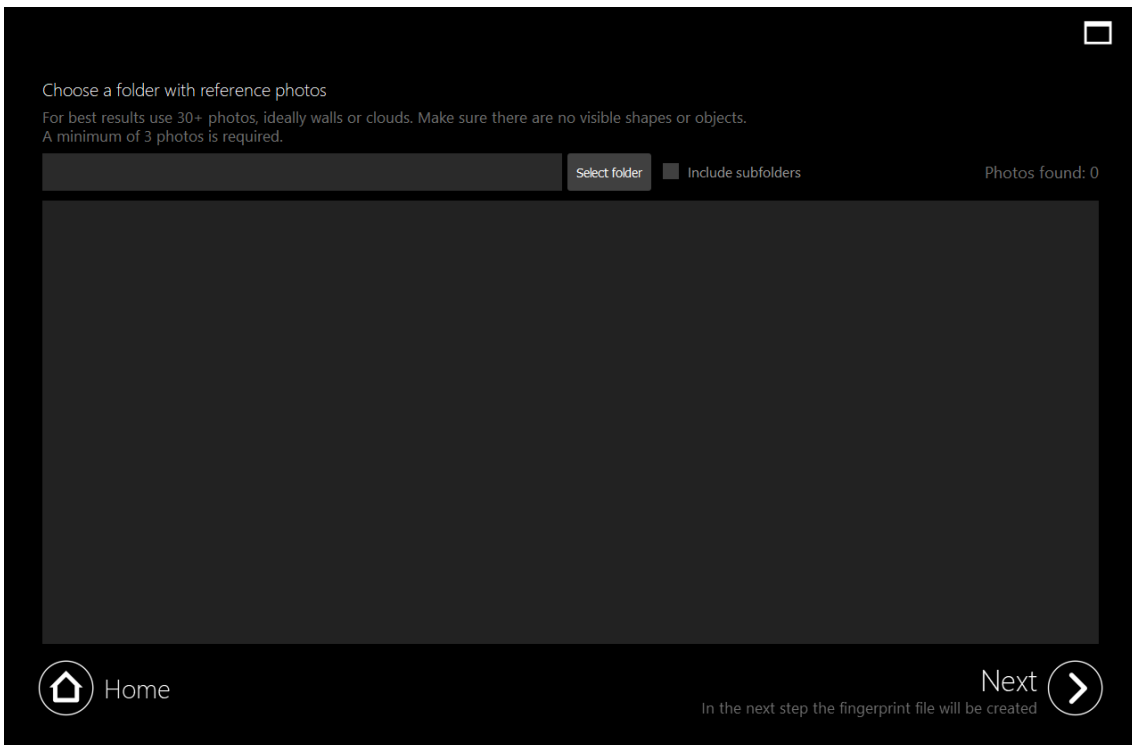
The installation will run automatically after it is downloaded.

8.6 Learn - Create fingerprint

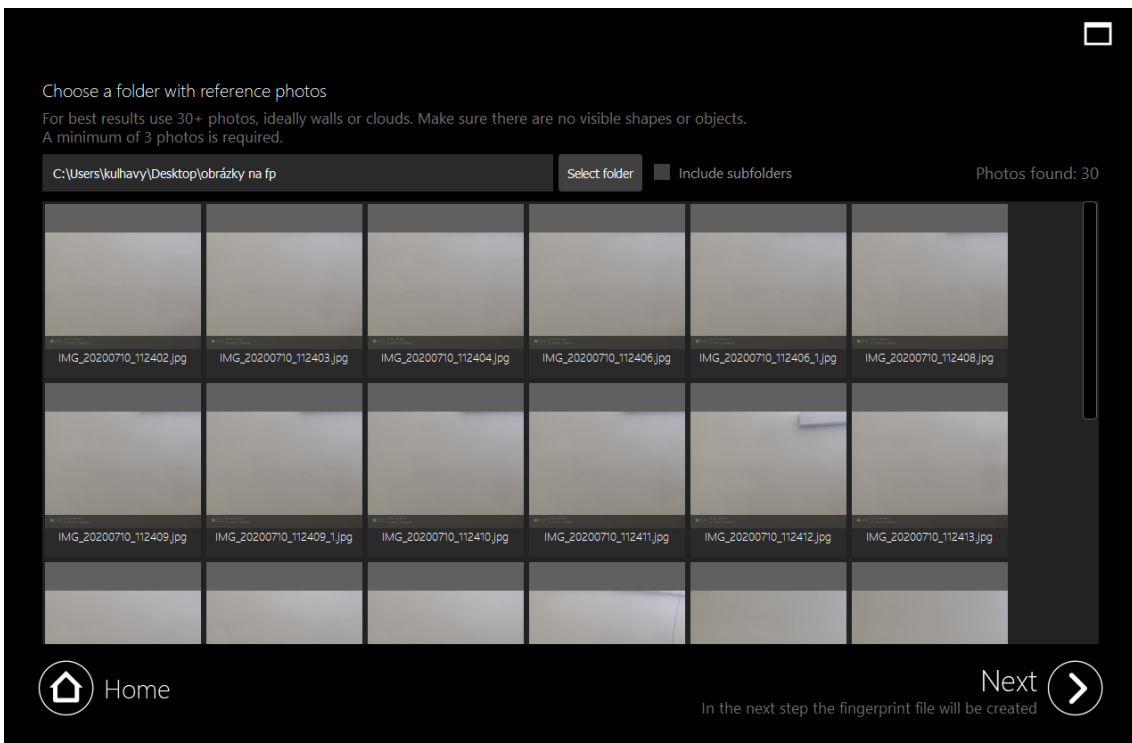
In order for Camera Ballistics to work properly a sensor fingerprint from the tested camera/phone's sensor must be created. This sensor fingerprint carries vital information about the camera specifications and unique stats and identifiers, which will later provide the software the essential information needed to determine if any photo was or was not actually taken by the camera being investigated.

It is very easy to obtain the camera sensor's fingerprint and it will take you only a few steps.

1. With the subject, device take 30+ pictures. These pictures **MUST** adhere to the following standards - they must be as simple as possible (pictures of plain white walls or sky are recommended). Do not take pictures of objects with sharp edges or angles. Best results come from white walls or sky photos. With older cameras/phones taking 30 pictures may not be enough to establish an accurate sensor fingerprint, therefore 70-80 is the recommended amount to ensure the best accuracy of the fingerprint later on.
2. Save all these pictures into a folder on your computer. This folder **MUST NOT** include anything else.
3. Open Camera Ballistic and click on "**Learn**".

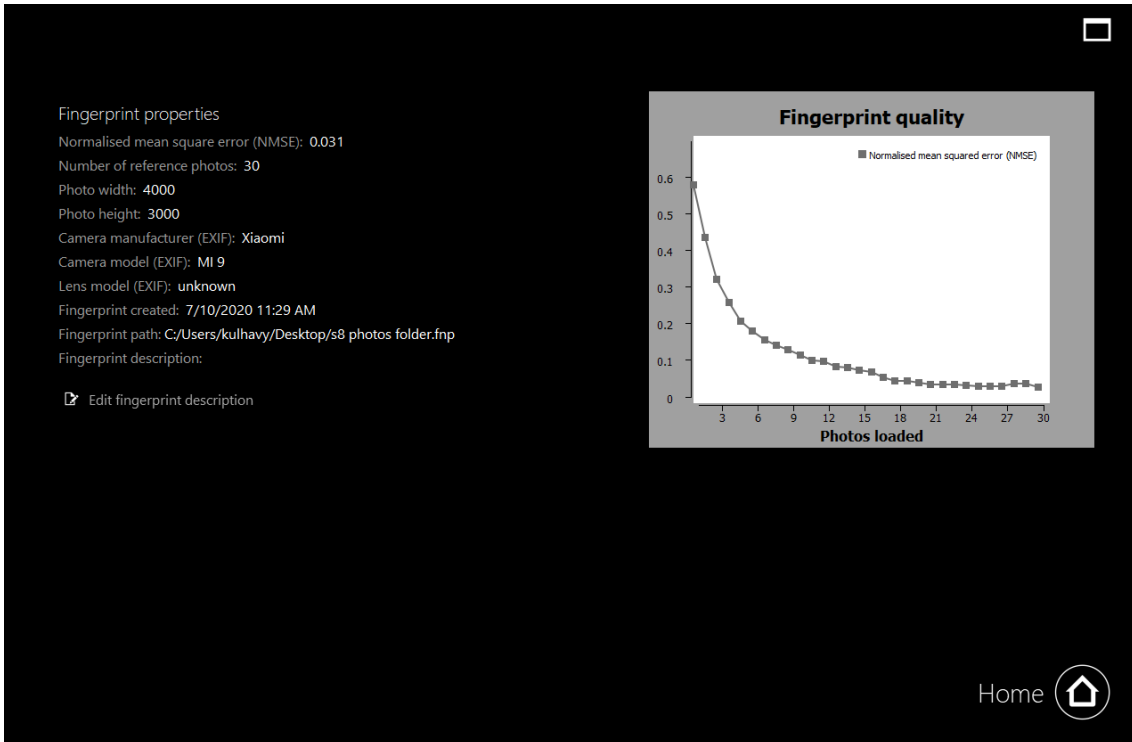


4. Locate and load the folder with the previously taken sensor fingerprint pictures. After clicking OK they will automatically load.

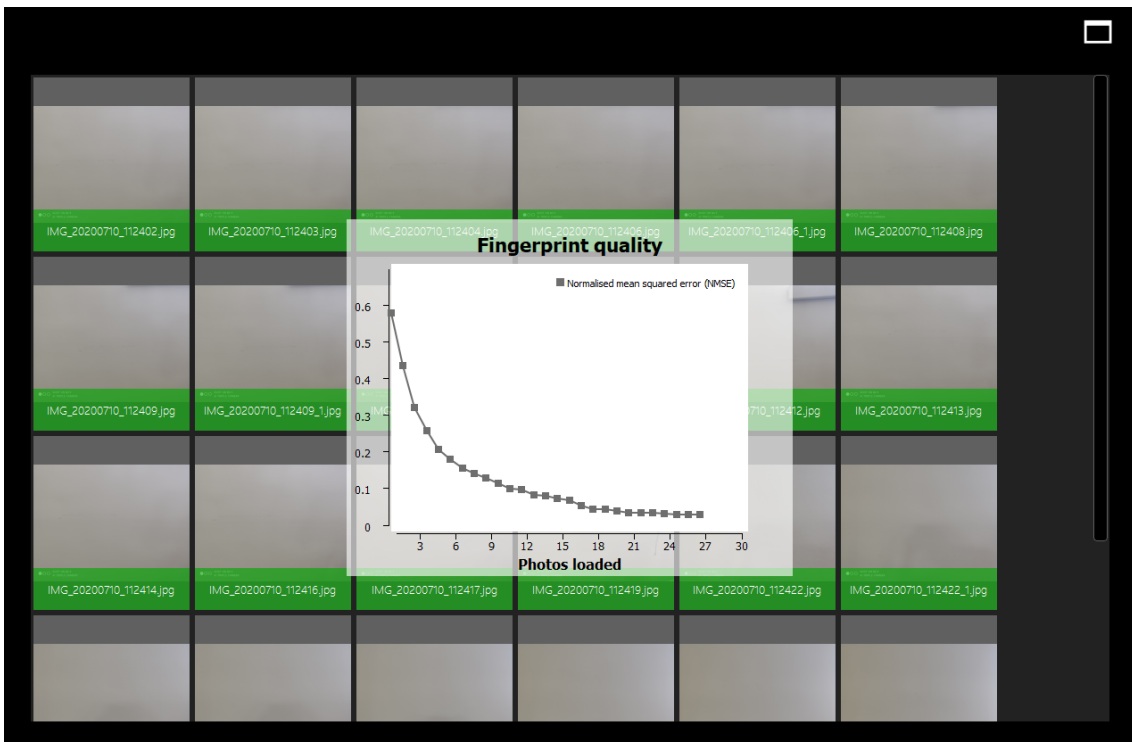


5. Now click on Next and the application will proceed to create the sensor fingerprint. You will be asked to select a

location on your computer where it will be stored. The process of fingerprint creation will then start automatically and will take up to a few minutes, depending on the number of photos that have been loaded.



6. After the fingerprint creation is finished you will see detailed info about the camera/phone as well as a graph showing the fingerprint accuracy/quality.



7. That is it - you will find the created fingerprint at the location on your computer you have selected in the previous step.

In the next phase ("Analyze"), Camera Ballistics will now be able to use the fingerprint as a reference point in determining whether a picture was or was not taken by a specific camera by comparing the "Learn" phase fingerprint photos to the actual subject photos being investigated.

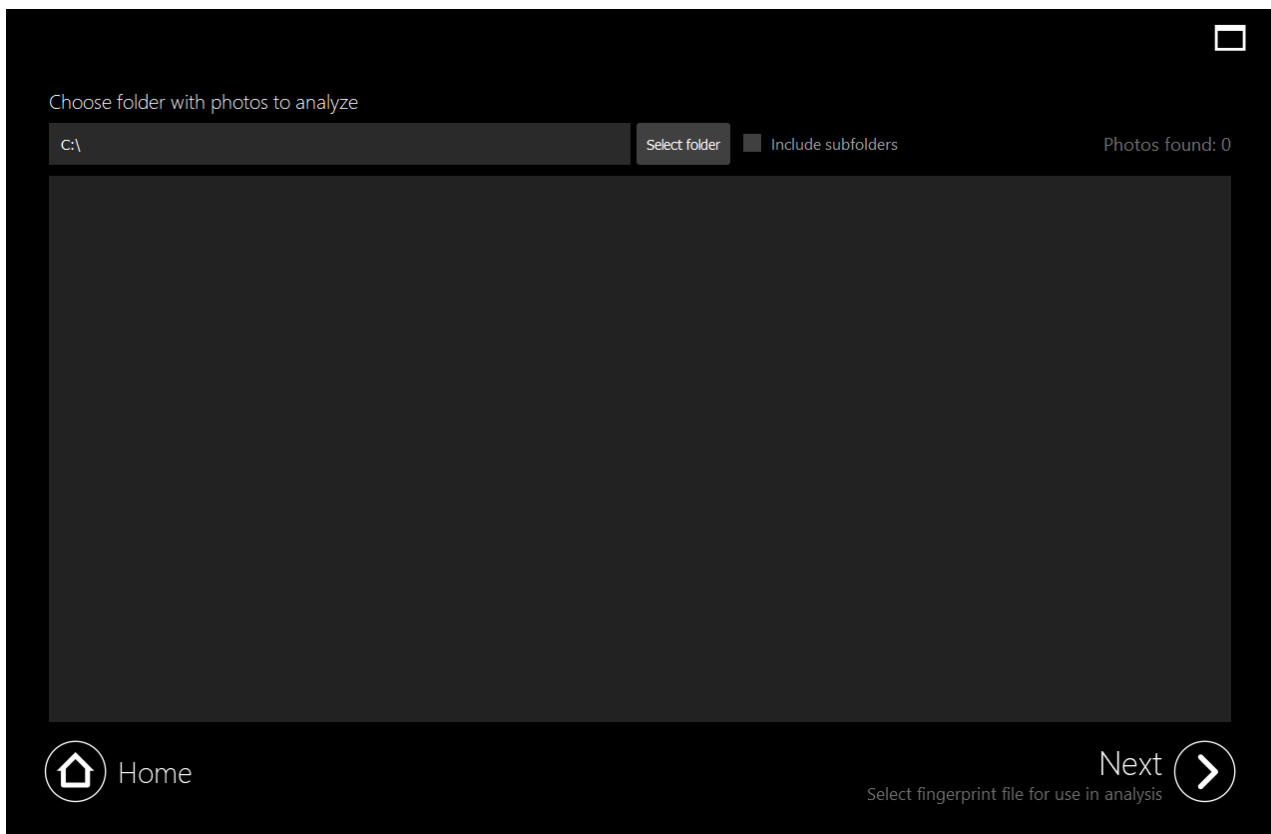
To learn about the next step, the "Analyze" phase - go [here](#)⁹⁹.

Fingerprints can also be used and integrated into our premier mobile device investigation tool [MOBILedit Forensic Express](#)¹⁰⁰ - more info about enabling Camera Ballistics within Forensic Express can be found [here](#)¹⁰¹.

8.7 Analyze - process photos

Once you have [created a reference sensor fingerprint](#)([see page 420](#)) you can use the *Analyze* function to take a folder of photos as an input, and Camera Ballistics will determine whether they were actually taken by a certain camera (of which you have the fingerprint) or not. This process is automated and should not take long.

To start, click on the "Analyze" button on the home page.



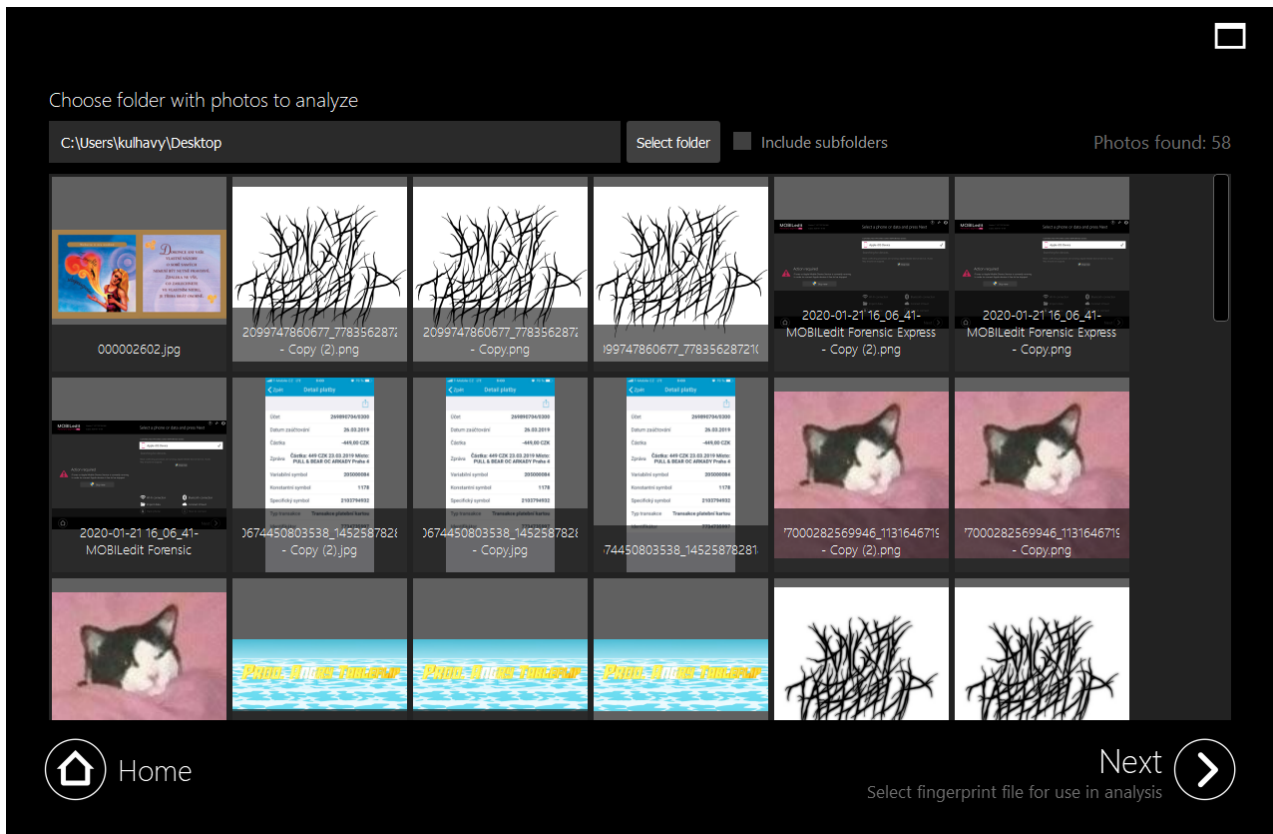
You will be asked to provide a folder of pictures - the subject photos in question you want to have analyzed.

The photos from the folder will immediately load and display in the software as a preview.

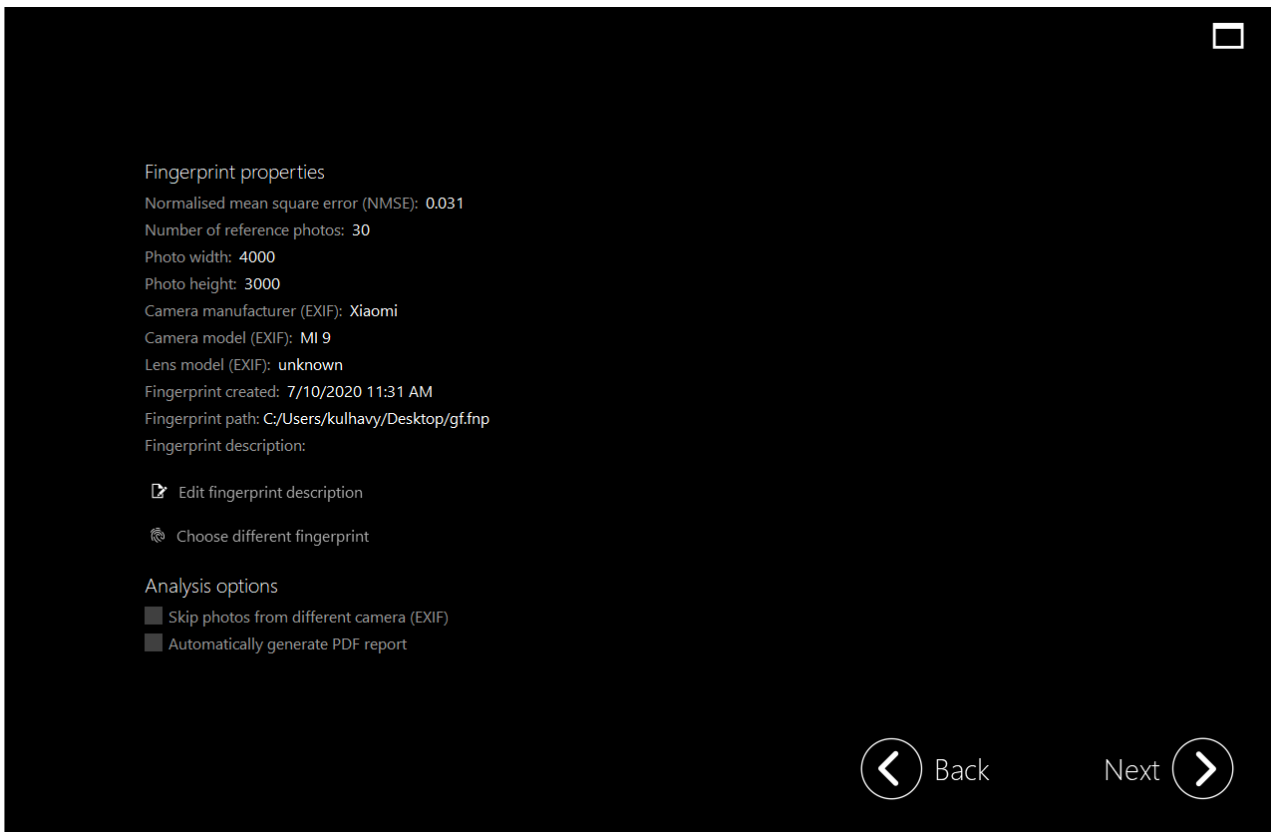
⁹⁹ <https://bit.ly/2BMLoAF>

¹⁰⁰ <http://www.mobiledit.com/forensic-express>

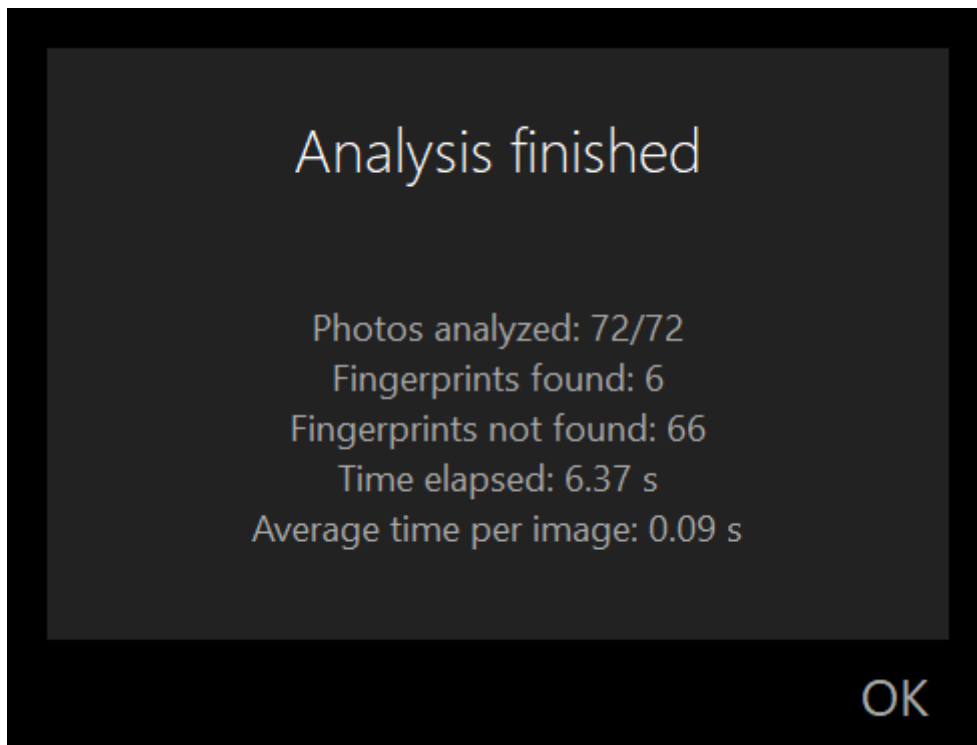
¹⁰¹ <https://bit.ly/3dK5adl>



Upon clicking the "Next" button you will be asked to provide a fingerprint. Please select the .fnp file you have previously created. Its detailed data will load and display to you. There is also some customization of the analysis available.

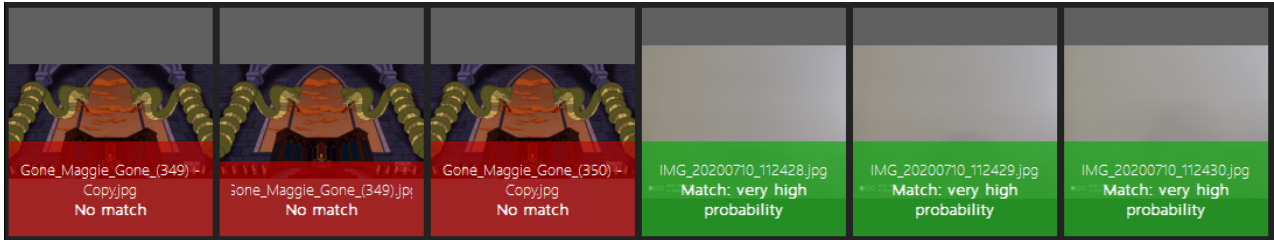


Click on "Next" to start the analysis process. This process will take up to a few minutes. The results will be then marked by green or red color.

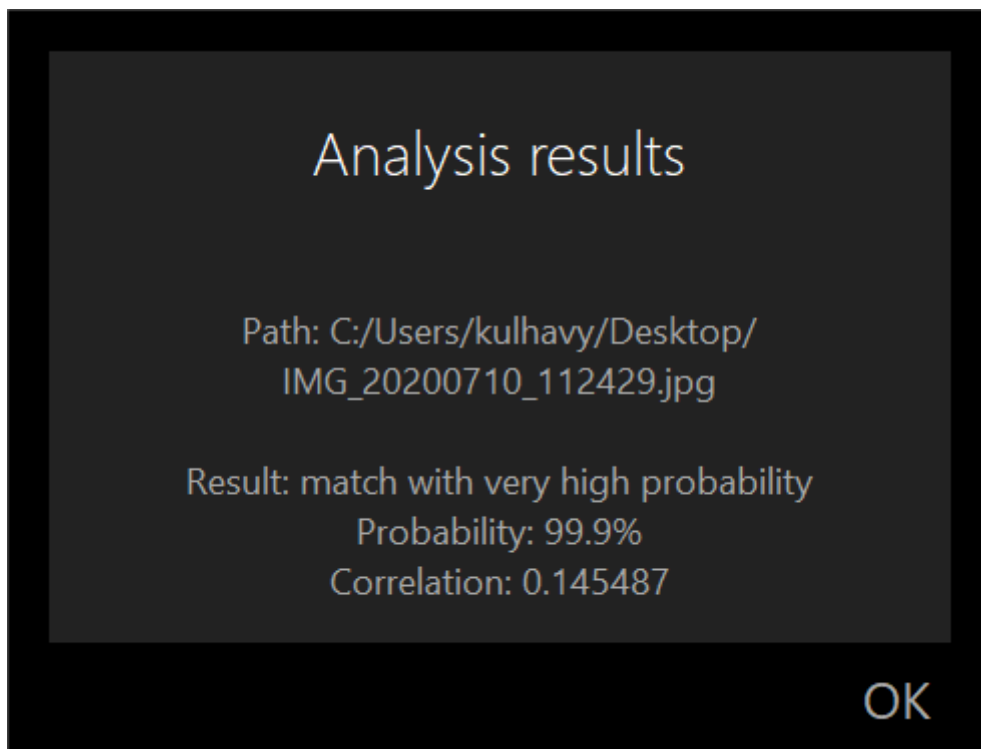


Red color means the photo was not taken by the selected camera, while green means the photo is a positive match to the camera sensor.

The matched photos are placed in four categories of the probability of how accurate the match is (very high, high, medium, low). You can view this by hovering over the photo.

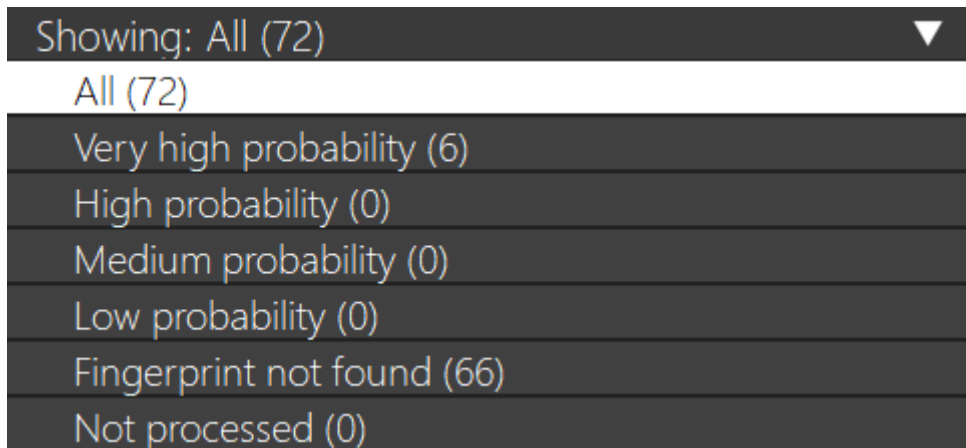


Clicking on "Show detail result" will show you all the info about the match as well as correlation.



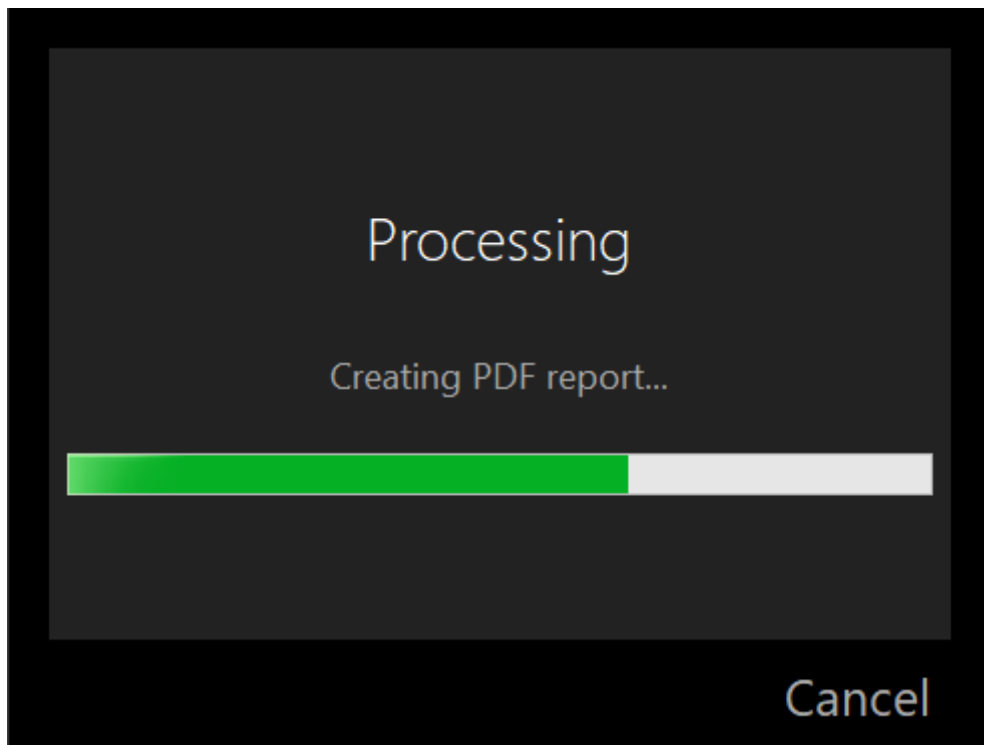
Clicking on "Show in external viewer" will open the photo in your PC's default picture viewer.

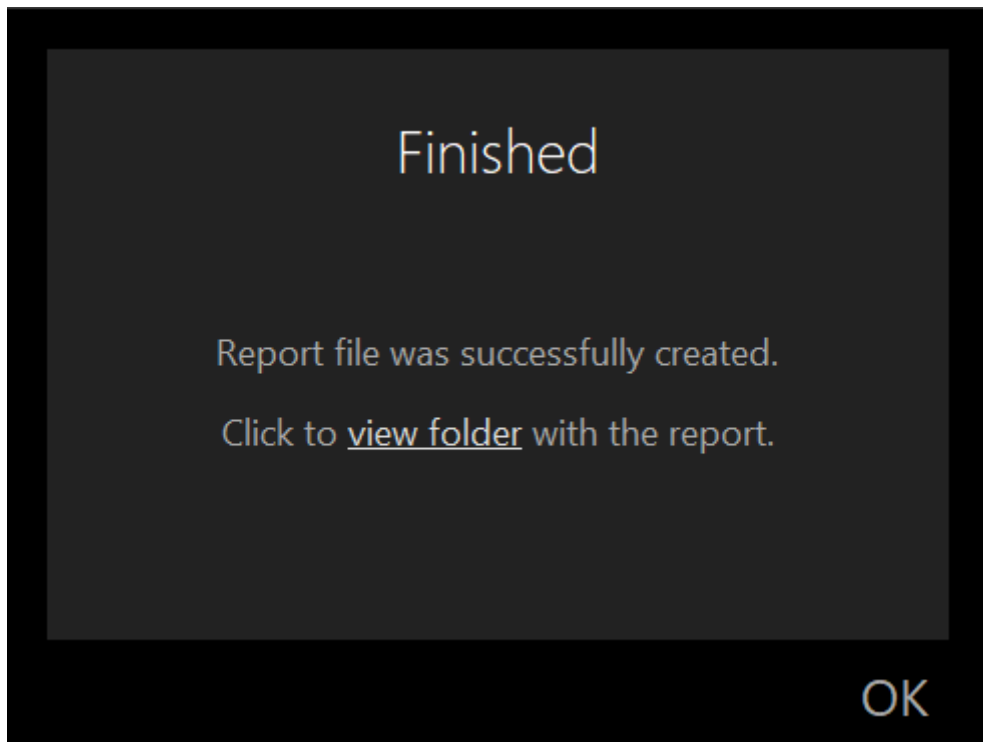
The result page also offers you the option to filter the results - see the dropdown menu in the upper right corner for more details.



If not selected earlier (in the step of loading the fingerprint) there is an option to create a PDF report available.

Simply click on the "Generate report" in the bottom right corner and select a location where you would like the .pdf file to be stored on your PC.





A PDF report, similar to the one from [MOBILedit Forensic Express](#)¹⁰², will be created.

Camera Ballistics also allows you to have the Analysis available while extracting data from a phone in Forensic Express.

8.8 Image quality requirements

Image quality requirements

To ensure the best functionality of the Camera Ballistics software we advise you to use raw and unedited photos with higher resolution. To create a fingerprint please use photos with the same resolution as the photos that are currently being investigated. If the resolution differs, we are unable to ensure that the fingerprint stays the same since the camera may behave differently on various resolutions. This may cause problems with identification resulting in photos not being correctly matched to the fingerprint.

Photos obtained from the messaging apps

If the photo was obtained from the messaging application, it is highly possible that the fingerprint of the photo has been modified. Due to modifications ongoing during the sending process, like resolution change, change of file format, or color change. If you were to create a fingerprint from photos that have gone through the same modifications as the investigated file. For example, sending them through the same messaging app as the investigated photo. This could result in creating the same or similar fingerprint as of the investigated photo. We cannot ensure the maximum similarity of the fingerprints because the apps may handle various types of photos differently. Keep in mind that in this case, you will need more photos to create the fingerprint because of the lower resolution.

Thumbnails and preview images

¹⁰² <http://www.mobiledit.com/forensic-express>

The fingerprint of the thumbnail and raw original photo will be marginally different. Same as with the messaging apps, you would have to let the photos be edited by the same process of modification as the investigated file. To achieve this, you would need a high amount of photos. We still would not be able to ensure the same quality of the fingerprint as with higher resolution photos. With resolution this low it is highly unlikely that the photo will preserve its original fingerprint and may rapidly change in different shots.

8.9 How to create Logs

Here's a quick guide of how to create logs:

1. Go to %DOCUMENTS%\Camera Ballistics on the PC you have this issue on
2. 2. Open the „Settings.ini“ file in notepad. There should be [drvman] and [Settings] sections in there, kindly rewrite these parameters as per below

```
[drvman]
```

```
MaxLogSize=20000000
```

```
EnableLogging=1
```

```
LogLevel=5
```

```
[Settings]
```

```
PortLogLevel=5
```

3. Save file and restart Camera Ballistics
4. Reproduce the issue exactly like how it happened
5. Close Camera Ballistics
6. ZIP the Logs folder, which is in %DOCUMENTS%\Camera Ballistics and send it to us
7. Delete this Logs folder after you send it to us, to clean up your PC
8. Rewrite all previous values in the Setting.ini to 0 (having them at higher numbers will cause Camera Ballistics to keep logging and take a lot of space from your disk)

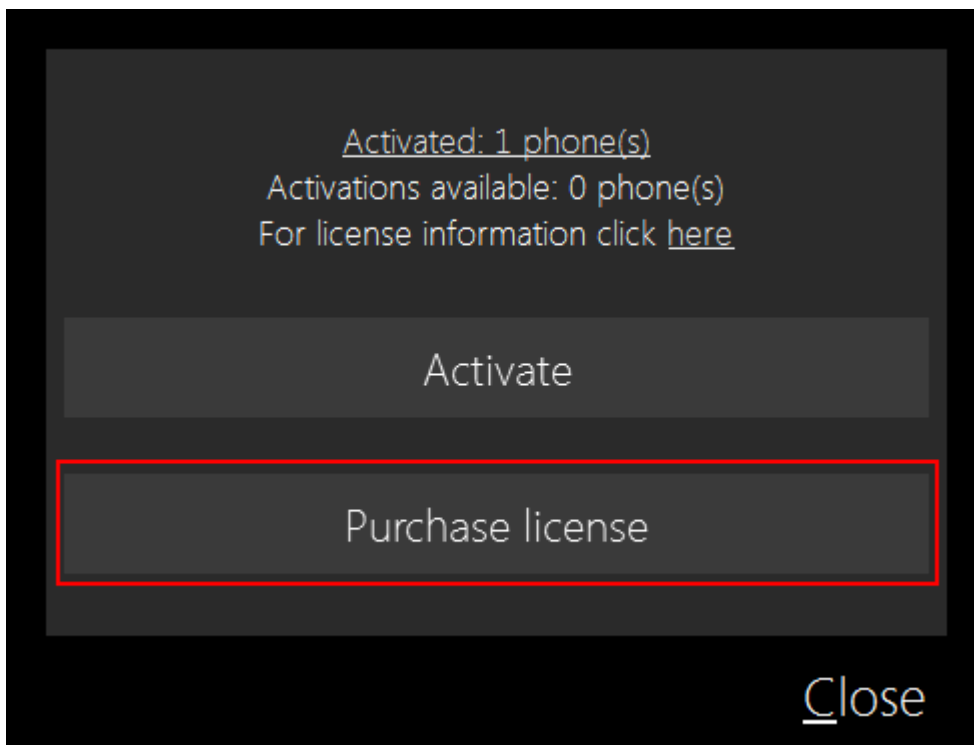
9 FAQ

In the Frequently Asked Questions (FAQs) you will find additional tips, information and guides for a complete and satisfactory experience with MOBILedit Forensic Express.

9.1 How to buy additional licenses?

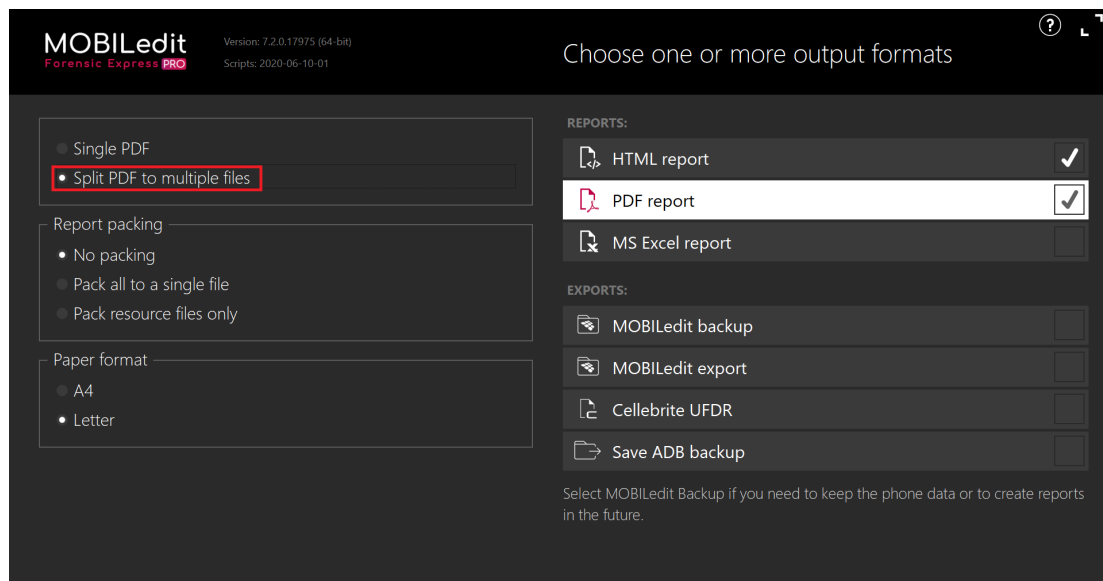
To buy additional licenses, connect the phone for which you want to activate the license for, then click next and in the activation window choose Purchase license.

If you have more slots available, Forensic Express will automatically recognize them and prompt you to allocate a license for an additional phone.



9.2 How to make reports smaller?

As a forensic expert who is working with a lot of reports on a daily basis, you might find this article very useful. It will give you some tips which can make your daily routine much more effective.

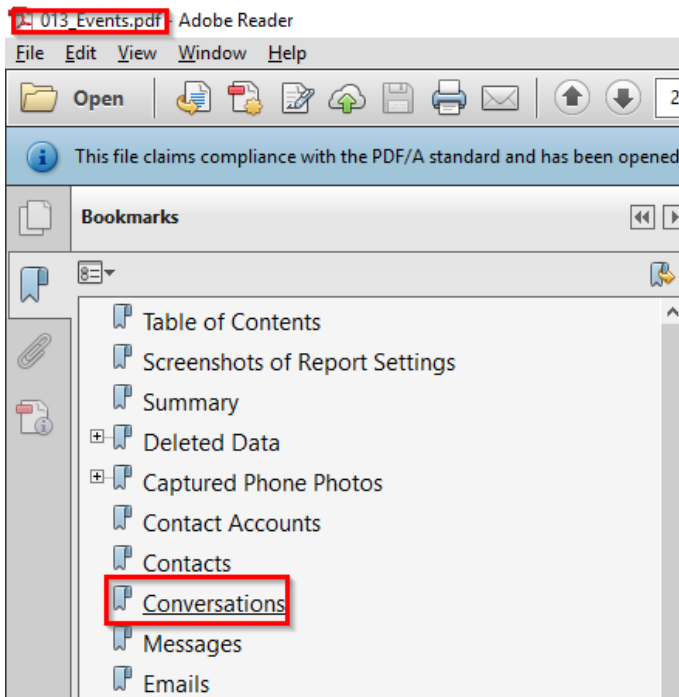


9.2.1 Split the PDF report file to multiple files

Splitting the PDF report file to multiple separate files will help you to get the report results divided by sections. It will give you a list of files named by contained data types or application's data.

016_Notes.pdf
 017_Recognized_Images_of_Currency.pdf
 018_Recognized_Images_of_Documents....
 019_Recognized_Images_of_Drugs.pdf
 020_Recognized_Images_of_Extremist_sy...
 021_Recognized_Images_of_Nudity.pdf
 022_Recognized_Images_of_Upskirt.pdf
 023_Recognized_Images_of_Weapons.pdf
 024_Images_with_identified_person_%22...
 025_Images_with_identified_person_%22...
 026_Photos.pdf
 027_Image_Files.pdf
 028_Audio_Files.pdf
 029_Video_Files.pdf
 030_Documents.pdf
 031_Passwords.pdf
 032_GPS_Locations.pdf
 033_Web_Browsing_History.pdf
 034_Web_Search_History.pdf
 035_Bookmarks.pdf
 036_User_Dictionary.pdf
 037_Wi-Fi_Networks.pdf
 038_Cell_Towers.pdf
 039_Bluetooth_Pairings.pdf
 040_Seen_Bluetooth_Devices.pdf
 041_Notifications.pdf
 042_Any.do.pdf
 043_Calendar.pdf
 044_Calendar_Storage.pdf
 045_Dialer_Storage.pdf
 046_Email.pdf
 047_Evernote.pdf
 048_Facebook.pdf
 049_Gmail.pdf
 050_Google_Play_services.pdf
 051_Hangouts.pdf
 052_Internet.pdf
 053_MapMyRun+.pdf
 054_Messenger.pdf
 055_Messenger_Lite.pdf
 056_Translate.pdf
 057_Viber.pdf
 058_WhatsApp.pdf
 059_YouTube.pdf
 060_SIM_Card.pdf

Each file includes bookmarks which are helpful in case you decide to change the PDF file you want to view. See example picture, you are in the "Events" file, but you can simply open the "Conversations" if you'd like to.



Another benefit of splitting the PDF to multiple files is that you can simply copy each file and use it separately. Each file contains not only bookmarks, but also the main report page with device info, device properties, and table of contents.



FORENSIC EXPRESS PHONE CONTENT REPORT

Kentucky church

Case Evidence Number: 8974969-589-468



Manufacturer	Samsung
Product	Galaxy S7
HW Revision	NRD90M
Platform	Android
SW Revision	7.0 (24)
Serial Number	9885e8343491523350
Adb Backup Password	1234
Unlocking Pattern	6304258
IMEI	357591070471526
Rooted	No
SIM Card	Yes
Owner Phone Number	+15648875459
Operator	O2-CZ, MCC: 230, MNC: 2

Case Information

Case Label	Kentucky church
Case Evidence Number	8974969-589-468
Case Evidence Details	

Device Information

Device Label	
Device Name	Samsung Galaxy S7
Device ID	
Device Evidence Number	6814259-484-813
Owner Name	Richmond Valentine
Owner Phone Number	+15648875459
Phone Notes	

Investigator Information

Investigator Name	Gary Unwin
Investigator Designation	
Investigator Email	gary.unwin@kingsman.com
Investigator Phone Number	+15439568150
Permission Document	

Extraction Information

Data Extraction Started	2018-03-22 13:12:20 (UTC+1)
Data Extraction Finished	2018-03-22 13:13:08 (UTC+1)
Extracted by	Phone Forensics Express 2.6.0.3935
Report Generated by	MOBILedit Forensic Express PRO 7.2.0.17975
Applications Analyzed by	AppEngine 2020-06-10-01

9.2.2 Use filtering

Filtering allows you to minimize content in the final report to the exact strings or time intervals which interests you the most. The MOBILedit Forensic Express has two-level filtering.

First is the filtering of the whole extraction. For more information go to [Global Filters](#)(see page 266).

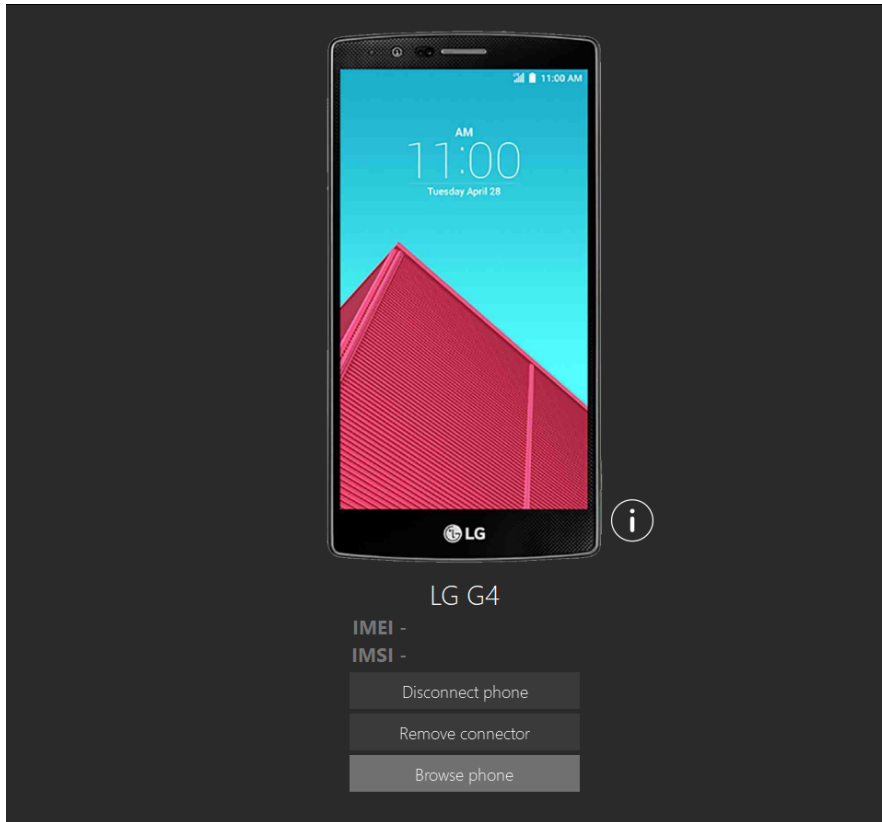
You can combine the selections, for example you know the exact time interval and the text string, then you fill these as you need. For more information go to [Local filters](#)(see page 276).

9.3 Does MOBILedit Forensic Express offer viewer or data analysis tool?

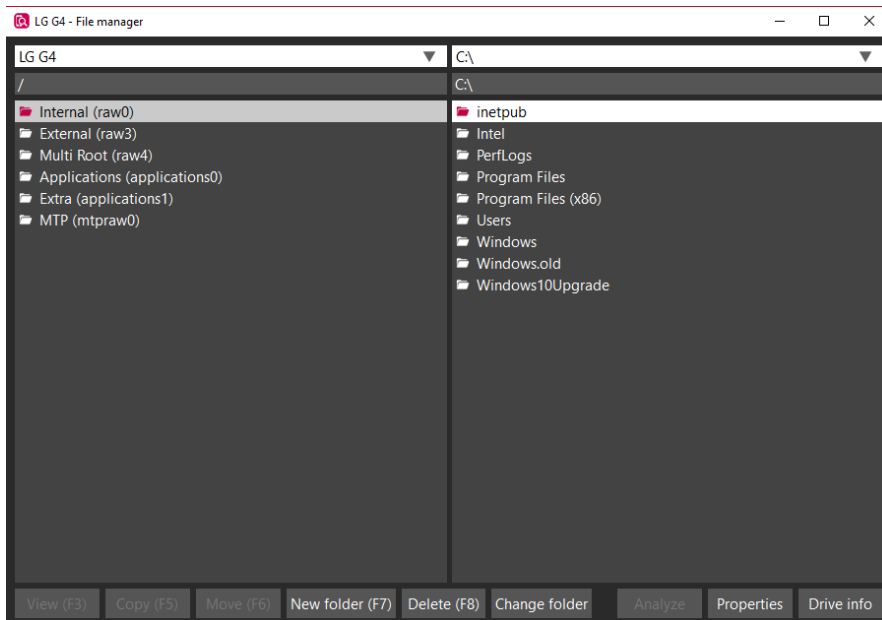
MOBILedit Forensic Express is a tool for extraction and express work, to provide you with all possible exports and reports.

We expect you to read the data in PDF, Excel, HTML, UFED and other 3rd party tools, as we provide all data in an open file structure

We also offer File Manager for connected phones. This allows you to browse the content of the phone as if it was a file system and also allows you to copy data in and out of the phone.



Moreover, there are buttons called Properties, Analyze and Phone Info, which allows you to get more detailed info about the phone or any of its data folder.



9.4 What are the types of logs?

9.4.1 Extraction logs

- The main log of the extraction process is located in the export folder, the filename is “log_full.txt”. It contains information about extracted files and everything else you can see on the screen during the extraction process and during the report generation.
- The summary of items that were extracted and what has failed during the extraction process (if there were failures) is in the "log_short.txt".
- Screenshots of user settings are located in the export folder, at “pdf_files/wizard_screenshots” or “html_files/wizard_screenshots”.

9.4.2 Application Logs

Application logs store information about how application runs and possible errors, it is stored in file main.log located in “Documents/MOBILedit Forensic Express/Logs”. If the incident is reproducible, we recommend to delete this file and run the program again in order to get fresh logs.

9.4.3 Communication logs


There are also communication logs, located in “Documents/MOBILedit Forensic Express/Logs”. If the incident is reproducible, we recommend to delete its content and run the program again in order to get fresh logs of the incident.

 You can read more details on how to collect logs for troubleshooting [here](#)(see page 437).

9.5 Where to find previous Android backup?

Here are a few places you can look for your Android backups if one or more exists. You could then restore the phone or import the backup and run the program.

1. Log-in to your Google account, in the upper right of the screen there is a small grid you can click... of the given options look in 'Google Drive' or 'Photos'
2. To find your backed-up contacts...log-in to Gmail on your PC...near upper left of the screen it will say 'Gmail' and there will be a drop-down box, select the box and click 'Contacts'
3. Your phone service provider might have a backup/cloud-based backup option- if you log-in to your cell phone account online at your PC you can check there (e.g Samsung Cloud). You can check on any PC you connected the phone to previously.
4. On your PC, click the Windows symbol (usually in the lower-left)- in the search field type backup.ab

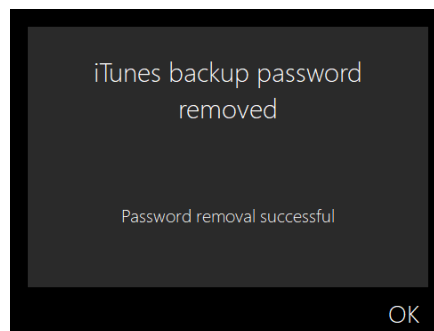
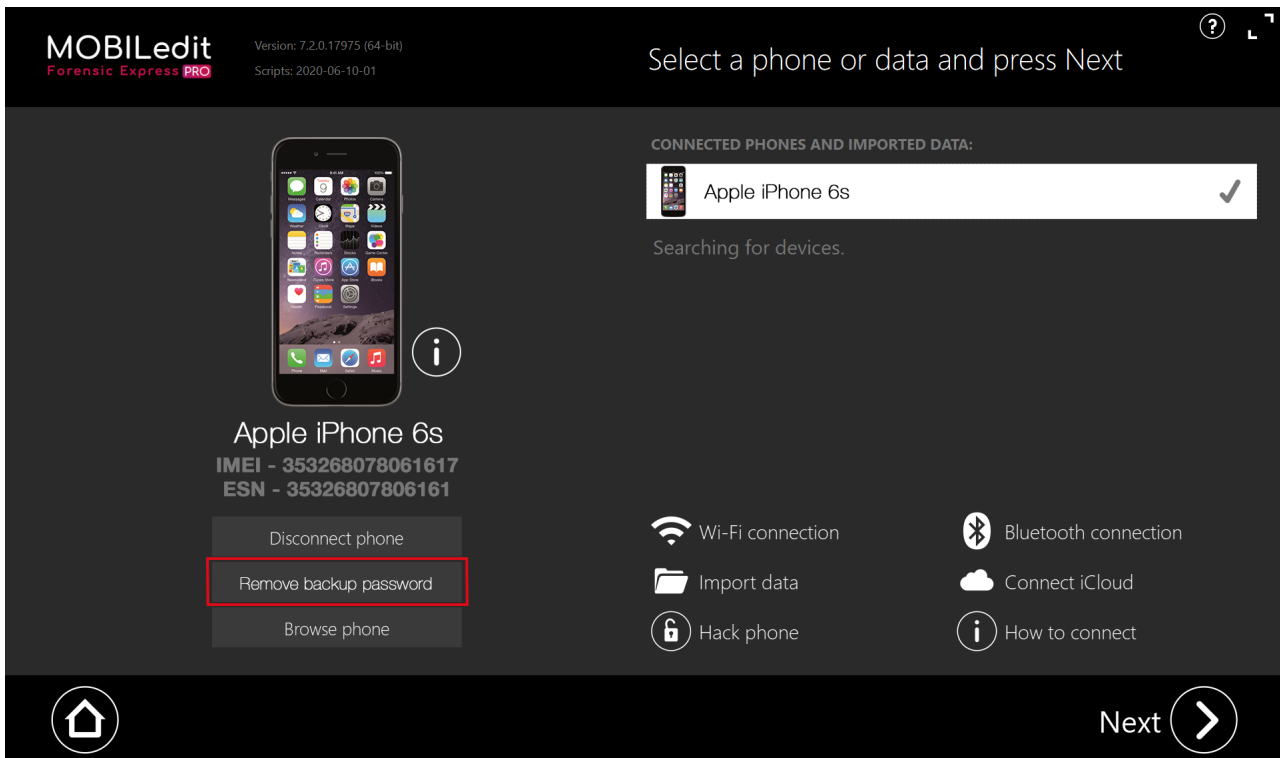
 Outside of these options you could search online or google search for other methods, or [contact us](#)¹⁰³ directly for assistance.

¹⁰³ <http://www.mobiledit.com/contact>

9.6 iTunes backup password is required each time I run analysis

Normally when you extract iTunes backup and a temporary password is set-up by MOBILedit Forensic Express is this password removed after successful extraction.


It looks like your first extraction didn't finish successfully and the iTunes Backup remained encrypted with a temporary password, for such cases, there is an option to remove the password when you connect the device.



9.7 Does MOBILedit Forensic Express have the capability of extracting data from iCloud?

Yes. Cloud Analyzer can extract and analyze iTunes backups from iCloud without the need to have the phone physically present in your lab.

Complete parsing of low level phone backup provides maximum data such as data from applications, including deleted data recovery. All versions of iOS are supported, including two-factor authentication.

 Please note that this feature is very limited in additional functions of the classic MOBILedit Forensic Express. Data import, Physical Image creation, App Downgrade or Photo Recognizer will NOT work in the Cloud analyzer!

We are working on the capability to extract data from more cloud services in upcoming versions of MOBILedit Forensic Express.

To stay informed on upcoming releases please sign up for our newsletter at www.mobiledit.com/newsletter¹⁰⁴.

9.8 What are the types of logs and how to use them for troubleshooting

Since MOBILedit is a forensic software tool, it is important for us to preserve the privacy of our customers or potentially sensitive content obtained during the acquisition of data from mobile devices. You can find different logs in MOBILedit Forensic that help you to troubleshoot the issue:

9.8.1 Extraction logs

The extraction log describes the process during extraction.


The main log of the extraction process is located in the export folder, the filename is “summary_full”. It contains information about extracted files and everything else you can see on the screen during the extraction process and during the report generation.

The summary of items that were extracted and what has failed during the extraction process (if there were failures) is in the "summary_short".

Screenshots of user settings are located in the export folder, at “pdf_files/wizard_screenshots” or “html_files/wizard_screenshots”.

9.8.2 MOBILedit Application Logs

MOBILedit Application logs store information about how the application runs and possible errors, it is stored in file main.log located in “Documents/MOBILedit Forensic Express/Logs”. If the incident is reproducible, we recommend deleting this file and run the program again in order to get fresh logs.

 The MOBILedit log and Crash dump file do not contain any personal information or sensitive data about the connected device.

9.8.3 Communication logs

Communication logs are located in “Documents/MOBILedit Forensic Express/Logs”. If the incident is reproducible, we recommend deleting its content and run the program again in order to get fresh logs of the incident.

 The communication log may contain sensitive data from the device.

¹⁰⁴ <http://www.mobiledit.com/newsletter>

When you get any of such issues, you will need to collect the MOBILedit Forensic logs to investigate further and if possible, you likely need to share the logs with the support team for further help. We want MOBILedit to serve you well, so we are keen to know if you have any trouble, so please don't hesitate to send us your log.

9.8.4 How to get logs for troubleshooting?

1. Start **MOBILedit Forensic Express**
2. On the MOBILedit home screen click on "**Settings**"
3. Find a **LOGGING** section
4. Choose from the options **Debug** (if the issue is reproducible)
5. Set maximum log size if needed, otherwise, keep the default value
6. **Try to reproduce the issue** (problem with the device connection, etc.)
7. Press the **Archive reports** button
8. We recommend packing **All log files**
9. In a report folder, you can find the final **ZIP file**
10. Send the **ZIP file** to us as an attachment [here!](#)¹⁰⁵



If you are in a situation where you are working on a case that may contain sensitive data or it is not possible to share information for legal reasons, please go to the Log folder and manually choose the main log and/or crash dump file.

9.8.5 What to do in case the program crashes unexpectedly?

1. Try to start **MOBILedit Forensic Express** again
2. On the MOBILedit home screen click on "**Settings**"
3. Find a **LOGGING** section
4. Press the **Archive reports** button
5. Choose packing **All log files**
6. In a report folder, you can find the final **ZIP file**
7. Send the **ZIP file** to us as an attachment [here!](#)¹⁰⁶



The needed files can also be found in a destination folder: C:\Users\...\Documents\MOBILedit Forensic Express\Logs


9.9 What if there is no information in a report from iPhone?

As for the empty sections in the report, the crucial thing is to enter the proper password so the iTunes backup can be created, from where we get most of the data. If this fails, it is canceled or you don't know the password, there is

¹⁰⁵ <http://www.mobiledit.com/contact>

¹⁰⁶ <http://www.mobiledit.com/contact>

not much information in the final report. This is also related to SMS, MMS and iMessages - in case you want to have the deleted ones retrieved, it is necessary to have the iTunes backup properly obtained with a correct password.

 In case you don't know the password, you can always use our Password breaking tool - you can find more info about it [here](#)(see page 284).

9.10 How reliable is recovered data?

1. Message timestamps are stored in databases as single numbers. More information about the most popular format of storing timestamps can be found here: https://en.wikipedia.org/wiki/Unix_time. Recovered data are often already partially rewritten, and if one of the rewritten items is the timestamp number, then after converting it to a readable time format you basically end up with a random date that falls into the constraints of a given timestamp system used.
2. Recovered data is never 100% reliable. However the probability of date being shifted only a little is very low. This is due to the way data are stored internally - small changes in data usually result in big changes in timestamps and it is rather hard to edit just least significant bits of the binary number that represents the timestamp. You can usually tell if the recovered item is corrupted or not. Look for indicators such as an unreadable or scrambled message body or other anomalies.

Data from one message are usually stored sequentially in the database and if some deleted entry is about to be rewritten and still remain recoverable then only the trailing part of the entry can be rewritten. Timestamps are usually stored in the front part of an entry, and therefore if they become corrupted so does everything else that follows them.

9.11 I connected the phone but can not press 'next' to next step

The phone might be connected through the MTP protocol. It is required to have a proper connection established by using our Connector app in order to continue. For this, you need to turn on 'USB debugging' and have a proper device driver installed.

Please read more details in our user guide.

For Android phones go [here](#)(see page 138).

For iOS phones go [here](#)(see page 160).

For other phone types

go [here](#)(see page 179).

9.12 What if the connector installation has failed?

Connector installation is a reliable process, so if it is not successful the phone is rejecting the installation. In this case, there is probably not enough of RAM memory, storage memory or there is something wrong with the phone. Try deleting a few apps and restarting the phone.

If it is still not possible, then the phone is not standard Android and is not compatible. [Send us](#)¹⁰⁷ more details about the specifics of the phone so that we can either add support for the device or assist in achieving a successful connection.

¹⁰⁷ <http://www.mobiledit.com/contact>

9.13 What if the PDF report is empty or incomplete?

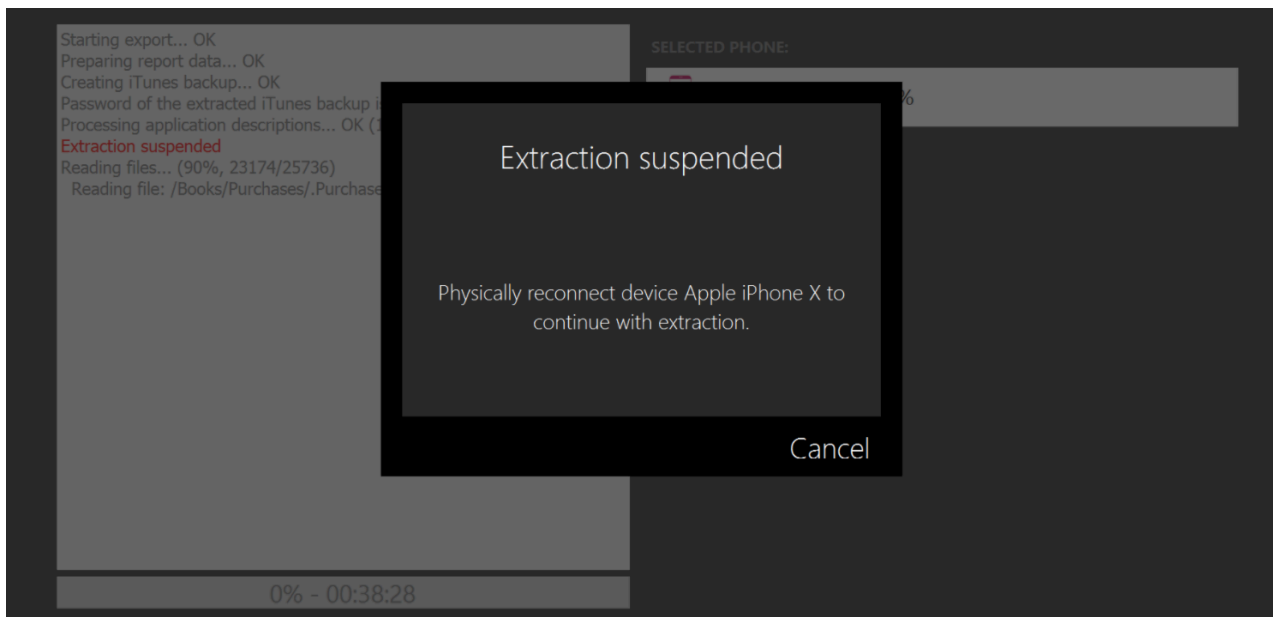
The PDF report generator will require a lot of memory especially if there is a large amount of photos or videos. It is recommended to have at least 16GB of RAM and also at least 32GB of free space on system disc for temporary data swapping. If it is still not enough, we recommend the following:

- Choose 'PDF Report - Multiple files' so the final PDF is not too large and the generation process doesn't require so much memory. It will split the report into multiple PDFs, by data categories.
- Generate HTML, Excel or UFED (available from MOBILedit Forensic Express version 3.5).
- If there is an extremely large number of images we recommend turning them off for the first round of exporting and selecting the MOBILedit Backup together with PDF Report - Multiple files. In the second round you just open the MOBILedit Backup file, without needing the phone, and running only the analysis of media. (by Generating MOBILedit Backup format, you can repeat data parsing without having the phone itself)

Please find more info on all the possible report formats [here](#)(see page 292).

9.14 What if the connection is suspended during extraction?

There is a possibility that the mobile phone disconnects during the extraction. This is a known issue of the iPhone with a large amount of data when the phone may stop answering communication requests. If that happens, there is no need to worry, MOBILedit is capable of continuing in suspended extractions. When this occurs, all you need to do is physically reconnect the phone to your computer. MOBILedit will automatically continue with the extraction, and no data will be missing.




9.15 What is the difference between software and individual package update?

Each MOBILedit software update consists of new features. Package updates consist of data, which are important or necessary for those features to work properly. For example, to use the Face matcher feature, you need to update the Face matcher package.

MOBILedit allows you to update packages related to individual features that were released or enhanced after the release of the newest update. Updating individual packages will allow you to get the latest version of a feature that you might need for your investigation.

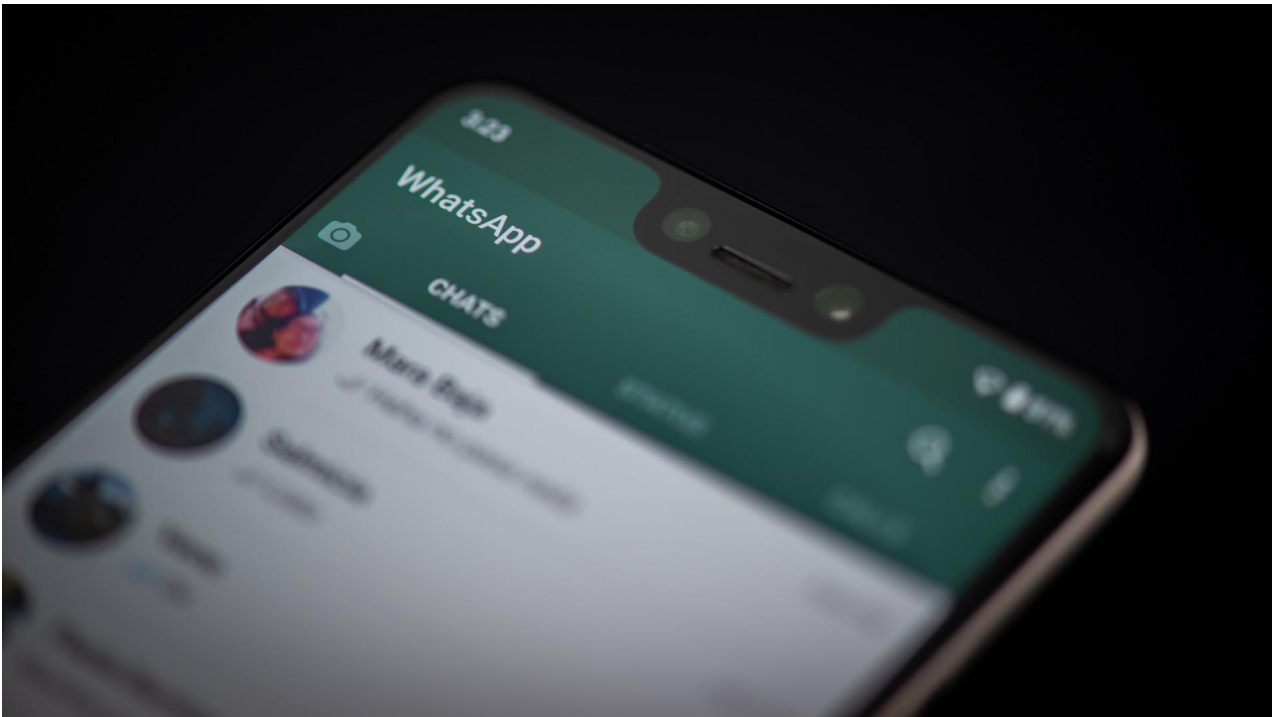
MOBILedit will work even without updating a single package, however, an important analysis might be missing without updating it.

 You can read more about Updates [here](#)(see page 28).

9.16 What if I have a blank page in my report?

When a blank page comes up in your report it indicates that MOBILedit did not find any data to recover in the selected category. The reason for this is that MOBILedit needs to differentiate between data that were not present or if there was any malfunction that prevented MOBILedit from extracting it.

9.17 How to get as much data as possible from WhatsApp



When extracting data from WhatsApp you may encounter a problem that not all expected data such as messages, call logs was included in the final report due to these data are end-to-end encrypted by developer/manufacturer. Globally, encrypted applications have become a challenge for mobile forensic science.

WhatsApp's end-to-end encryption ensures only the sender and the receiver can read or listen to what was sent, and nobody in between, not even WhatsApp. This is because, with end-to-end encryption, messages are secured with a lock, and only the recipient and sender have the special key needed to unlock and read them.

The good news is, that WhatsApp media are stored in the media folder, therefore can be located without root access. If you are using the “browse phone” function, the data will be stored on the following path: *phone/application0/com.whatsapp/live_specific/Media...*

If we speak within the limits of forensic analysis there are a few steps we need to follow to get the best result as much as possible. There are a few ways how to extract your needed information and that is by:


- Rooting / Jailbreaking your device
- Creating a physical image of your device
- Using an App downgrade function in our software MOBILedit Forensic Express

9.17.1 1) Rooting / Jailbreaking


9.17.1.1 Rooting

Most Android devices should be able to be rooted. However, the process of rooting is specific to each phone model, version of Android, and build number, so you always need to find the right tool according to your phone model.

You can root a majority of older Android phones using an app called [KingoRoot](#)¹⁰⁸, if for some reason this method doesn't work for you (locked bootloader, Knox, etc.), you may be able to find help on how to root your phone at [XDA Developers](#)¹⁰⁹, which is a website with a large active user community dedicated entirely to Android smartphones.

 Please note that sometimes it is necessary to unlock your phone's bootloader in order to root it. You can find a step-by-step tutorial on how to unlock the bootloader on your phone manufacturer's webpage.

Once rooting has been completed successfully the phone is then switched to so-called "rooted mode", and you then will be able to extract and analyze the deleted data.

 Rooting your phone may void the manufacturer's warranty and could cause security risks. Please take this into consideration before performing this process.
Rooting a Samsung device will trip the Knox Warranty void flag which will make the data stored in Knox permanently inaccessible.

9.17.1.2 Jailbreaking

There are three ways of jailbreaking your iOS:

1. **Tethered** - This method requires you to connect your iPhone to your computer and use an external application to jailbreak it. Once you restart your iPhone, the jailbreak is undone, but please note: your device will not be usable until you jailbreak it again using the same method.

¹⁰⁸ <https://www.kingoapp.com/>

¹⁰⁹ <http://xda-developers.com/>


2. **Semi-tethered** - This method doesn't require you to connect your iPhone to a computer in order to jailbreak it, however, the jailbreak is still undone every time you reboot your device, or, after a certain amount of time passes.
3. **Untethered** - This method doesn't necessarily require a computer to perform a jailbreak on your device and also modifies the iOS on a deeper level which means that no matter how many times you reboot your device, it stays jailbroken until you manually "un-jailbreak" it.

There are specific known ways to jailbreak almost every iPhone, iPad, or iPod Touch running on almost every iOS, except the latest releases - as it usually takes a few months to find a way of jailbreaking the newest version of iOS.

This means that there is no way of describing them all in a single article.

However, currently, the most often used apps for jailbreaking iOS devices are Pangu or Cydia Impactor. You can learn more about how Cydia works on the app developer's official website at [this link](#)¹¹⁰, or you can read [this article](#)¹¹¹ which describes a simplified process of iOS jailbreaking.

You can see a full list of available jailbreaks for each device and version [here](#)¹¹².

 Jailbreaking a device may void the manufacturer's warranty and could cause security risks. Please take this into consideration before performing this process.


9.17.2 2) Creating a physical image of your device

There are many ways how to create a physical image from a device. You can, of course, use some tools of your own and use our software for extraction but our product MOBILedit Forensic Express does offer some tools as well:

9.17.2.1 MTK Hack

There is a way of extracting a physical image from phones with MediaTek chipsets without root access (rooting the phone).

This exploit method does not work on all MTK-equipped devices, but sometimes it is the only way of acquiring the physical image because the phone does not have to be booted up or unlocked in order to perform this operation; which means you can try even if the phone is off or locked.

 This will not work for most MTK devices with locked bootloaders. In order to use MTK hack on such devices, the bootloader has to be unlocked first.

¹¹⁰ <http://www.cydaiimpactor.com/>

¹¹¹ <https://downloadcydia.org/cydia-impactor/>

¹¹² <https://www.reddit.com/r/jailbreak/wiki/escapeplan/guides/jailbreakcharts>

More information about how to use MTK Hack in MOBILedit Forensic Express can be found [here](#)¹¹³.

9.17.2.2 EDL Hack

There is also a way of extracting physical images from phones with Qualcomm chipsets without root access (rooting the phone).

This exploit method does not work on all Qualcomm-equipped devices and it is best when used with an EDL cable.

More information about how to use EDL Hack in MOBILedit Forensic Express can be found [here](#)¹¹⁴.

9.17.2.3 LG Hack

The "LG Hack" feature works on all LG smartphones with the new version of the LG LAF protocol (this is a service download mode similar to Samsung Odin download mode). One of the first devices to feature this version was the first LG G flagship.

Every LG smartphone from the year 2013 and newer should, therefore, support our LG hack.

With some of them - LG G4 for example - you are even able to browse the phone's filesystem via the "Browse Phone" option in Forensic Express.

This exploit takes advantage of "LG Flash Mode" - used primarily for updating firmware.

More information about how to use LG Hack in MOBILedit Forensic Express can be found [here](#)¹¹⁵.

9.17.2.4 TWRP Method



The device has to have its bootloader unlocked in order to proceed with this method.

Every Android phone has a "recovery" partition which is by default used for performing factory resets using an OEM's preloaded tools. However, this partition can be modified in order to replace the default tools with third-party recovery tools such as TWRP.

These recoveries are (unlike the stock ones) capable of modifying all the internal system partitions of your phone or tablet (they need this capability in order to flash custom firmware).

TWRP even comes with a built-in file manager with unlimited root access so you can modify, add or delete any system files manually. This process allows you to gain physical images, therefore bypass the otherwise locked device's protection.

113 <https://support.mobiledit.com/portal/kb/articles/physical-extraction-mtk-hack>

114 <https://support.mobiledit.com/portal/kb/articles/physical-extraction-mtk-hack-2-8-2018>

115 <https://support.mobiledit.com/portal/kb/articles/physical-extraction-lg-hack>

However, if the image is encrypted by the system itself, we are only able to get the encrypted physical image. More information about how to use the TWRP method in MOBILedit Forensic Express can be found [here](#)¹¹⁶.

9.17.2.5 Dirty Cow

MOBILedit Forensic Express can also use a Dirty cow (Dirty Copy-On-Write) exploit which can temporarily root a device that has an Android version up to 7.


The root is removed once the device is restarted.

More information about how to use the Dirty cow exploit in MOBILedit Forensic Express can be found [here](#)¹¹⁷.

9.17.3 3) Using an App downgrade function in our software MOBILedit Forensic Express

Due to better security, some application manufacturers made restrictions on what data can be acquired from their apps. This is especially relevant for non-rooted phones.

To bypass this we have introduced the App downgrade, feature in MOBILedit Forensic Express, which will downgrade the apps to a version, in which there was no problem in obtaining the data from them directly.

 Please note that only some apps support this feature as of yet, although we are working on expanding their list.

More information about how to use the App downgrade in MOBILedit Forensic Express can be found [here](#)¹¹⁸.

9.17.4 4) Captured phone photos

At last but not least there is always an option to simply capture screenshots of your mobile screen - for example, while having the WhatsApp chat open. This method might be lengthy, however, it is a very effective way how to get your desired conversation into the final report if every other method fails.

For more detailed info please visit our article [here](#).¹¹⁹

¹¹⁶ <https://support.mobiledit.com/portal/kb/articles/flash-phone-with-recovery-image-twrp>

¹¹⁷ <https://support.mobiledit.com/portal/kb/articles/dirty-cow-hack>

¹¹⁸ <https://support.mobiledit.com/portal/kb/articles/app-downgrade>

¹¹⁹ <https://forensic.manuals.mobiledit.com/MM/Data---Captured-phone-photos.1818165262.html>

10 MOBILedit Releases

10.1 7.4. Update

Announcing **MOBILedit Forensic Express**¹²⁰ version 7.4. This new release is mainly focused on fine-tuning the acquisition of iPhone and iPad devices.

MOBILedit users can now use three different paths when communicating with an iOS device:

1. The first one is low-level communication through the Apple device driver (downloadable from our website). This feature eliminates the need to download iTunes to your forensic workstation, as is often required by other forensic solutions. iTunes can write data to a target phone thereby affecting its forensic integrity. That's why the MOBILedit team has developed this method of communication and has now fine-tuned it making it perfectly reliable.
2. If you already have iTunes installed on your forensic workstation, (e.g., UFED, that requires it), MOBILedit can now communicate with an iOS device via the Apple Mobile Service, allowing the user a straightforward solution. (In previous versions MOBILedit required stopping this service).
3. We have added a protocol for full file system reading of jailbroken iPhones, so, if you use the checkra1n/checkm8 jailbreak available in our latest Connection Kit, you will get the full content of an iPhone including application sandboxes, keychains, system databases, iMessage, and all other hidden data.

Plus we have added support for the Dutch language. Current support of languages is as follows:

Generated reports are available in the following languages

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

Full product User Interface

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

10.2 7.3. Update

Update released September 23, 2020

We have released version 7.3 with important new features which will improve the amount of evidence you retrieve from analyzed devices. You will be able to directly extract and analyze data from Apple Watch devices, acquire and

¹²⁰ <https://www.mobiledit.com/forensic-express>

analyze physical dumps from KaiOS, connect devices with the latest Android 11 and iOS 14 operating systems and much more.

A completely revamped [User Guide for MOBILedit Forensic Express](#)¹²¹ is now also available for you, giving you better options in navigating through phone forensic knowledge.

10.2.1 What's new

Apple Watch direct reading

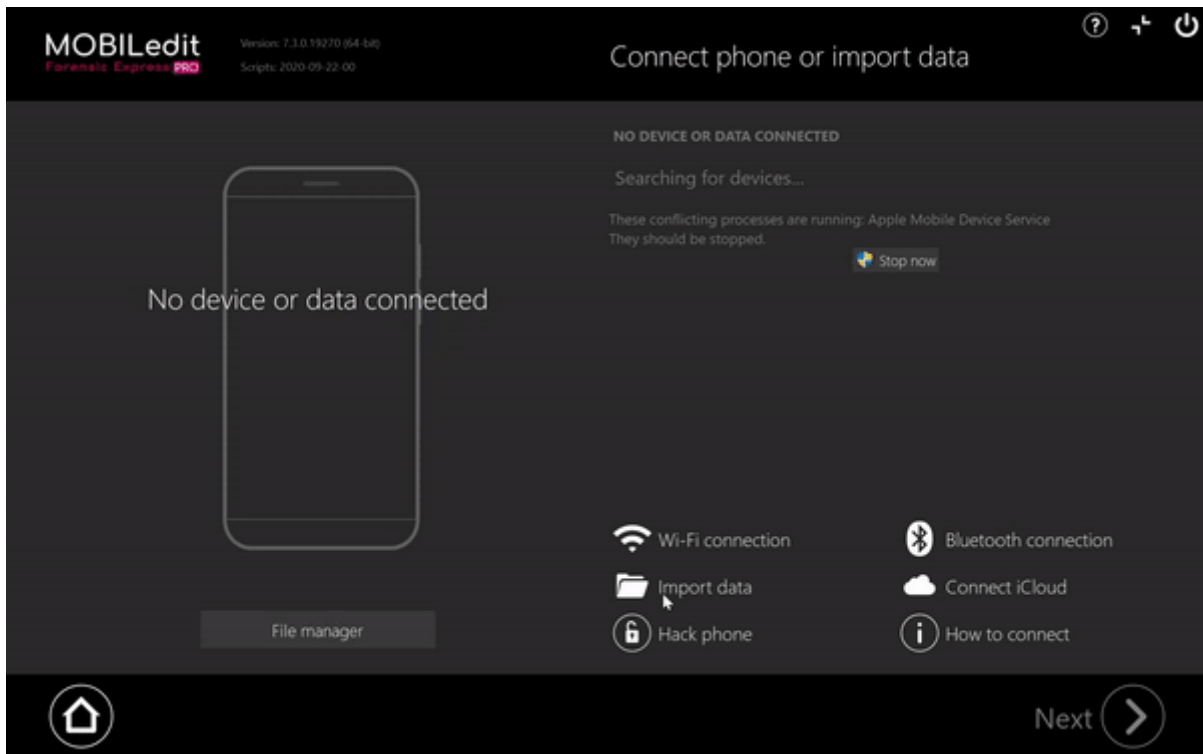
- MOBILedit is now able to read data directly from Apple Watch via a special reader and extract data such as device info (MAC addresses, memory, UID, SW revisions), Notes (recordings) and files, app list, synchronized pictures (related locations) and System logs.



KaiOS support

- KaiOS, a Linux-based operating system designed for feature phones is now completely supported on a physical level. The physical analysis provides you with all the important data such as contacts, messages, organizer, browser history, browser bookmarks, calls, alarms, notes, WhatsApp, and more. KaiOS operating system is very popular among feature phones such as Alcatel, Nokia, Accent, Telma and many other local brands.

¹²¹ <https://mobileedit.scrollhelp.site/MM/>



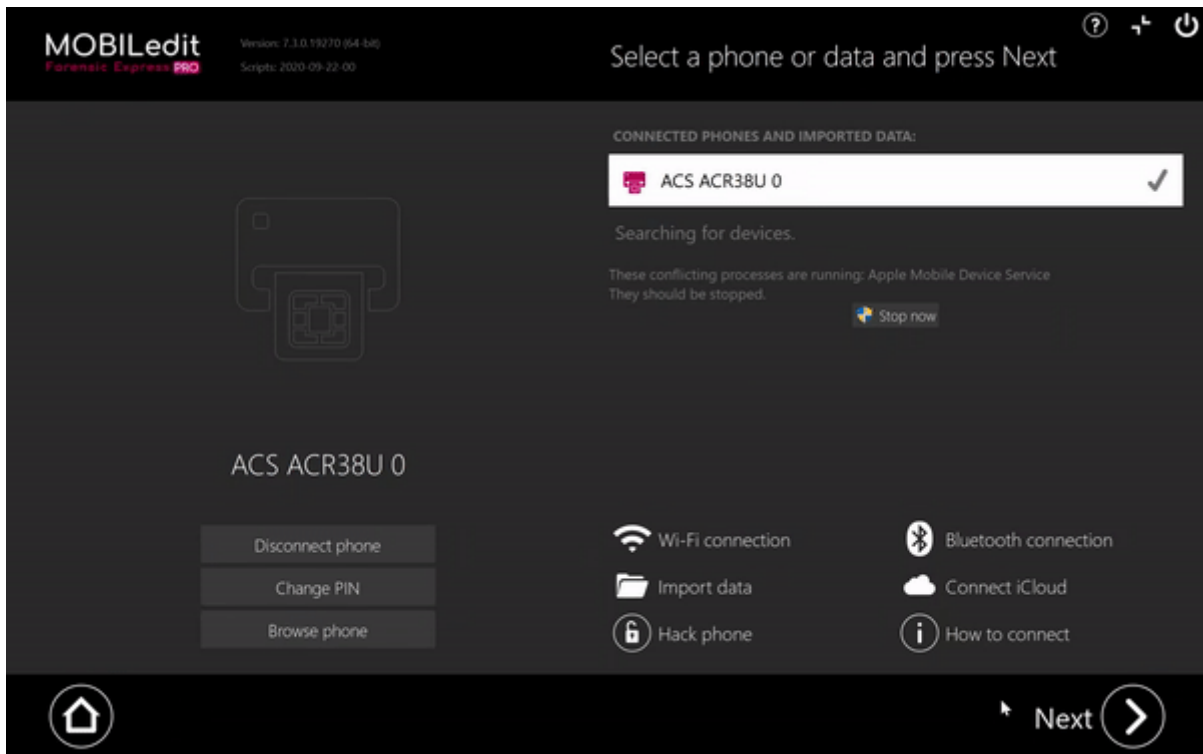
Android 11 and iOS 14 support

- The latest versions for both popular mobile operating systems are now fully supported.



Built-in SIM Cloning

- The built-in SIM Clone functionality enables you to copy the investigated SIM card to a rewritable MOBILedit SIM Clone Card directly from MOBILedit. This way you can isolate the phone from the mobile network while you don't have any issues regarding a missing or changed SIM within the phone.



10.2.2 Improvements and bugfixes

- List of all installed add-on packages are now shown in the report
- In the case of multiple reports, all files are copied and stored in one folder (phone_files), the report set is much smaller and the process is faster
- Specific selection automatically selects any available data based upon chosen settings
- GPS Locations search redesigned for better usability and increased performance
- UI has faster transitions
- Fixed disconnections of iOS devices that might occur in some cases
- Various PDF report fixes
- Loading of Huawei backups fixed
- Times and dates in Xiaomi backups fixed

10.2.3 Application updates

- Chrome
- Facebook
- Facebook Messenger
- Google Hangouts
- Google Office
- LINE
- Reddit

- Safari
- Snapchat
- Telegram
- Twitter
- WhatsApp

 Note: The single phone activation is disabled over WiFi for devices with Android 10 or newer.

10.3 7.2. Update

Update released April 20, 2020

MOBILedit Forensic Express¹²² version 7.2 is yet another evidence of continual and effective progress made by our talented development team.

As usual, our two main targets were to enhance the possibilities available for your phone forensic analysis and to improve your overall user experience. We are convinced we are gradually succeeding in both of these goals.

Below you can find all of the new features and improvements now available for you!

10.3.1 What's new

- Support for backups from Samsung feature phones
- File filtering based on the National Software Reference Library (NSRL) database of common files - reduces the number of exported files
- File highlighting based on a user-supplied hash list
- Beta version of Chinese language full product localization
- Updated Portuguese, Spanish, Czech and Slovak full product localizations
- New button on the connection screen, where you can find information about the currently connected phone
- Extended characters in PDF file names are phonetically transcribed instead of being escaped with "%xx"
- Android Connector application can be updated via Wi-Fi
- Limited Apple APFS physical image support
- Context menu in File Manager via right mouse click or with SHIFT+F10 key combination

10.3.2 Improvements and bugfixes

- UFED export/import compatibility improved
- Improved File Manager operations - Copy, Delete and Move
- Case information now extended
- iTunes Backup Reveal refreshes every time you open it
- Faster application start thanks to the optimization of how we load the update packages
- Camera Ballistics runs in background concurrently to speed up analysis
- Check for all needed Android permissions for Connector application
- Updated Czech, Portuguese, Slovak, and Spanish full product localizations
- Many minor improvements

¹²² <https://www.mobiledit.com/forensic-express>

10.4 7.1. Update

Update released February 26, 2020

Version 7.1. has plenty of new features and improvements which you will find handy along the way while working on your forensic analysis with our software.

10.4.1 What's new

iOS diagnostic logs extraction and analysis

Devices with an iOS operating system contain a special folder with low-level operating system logs. These logs (such as MobileGestalt) contain useful information about the device and networks.

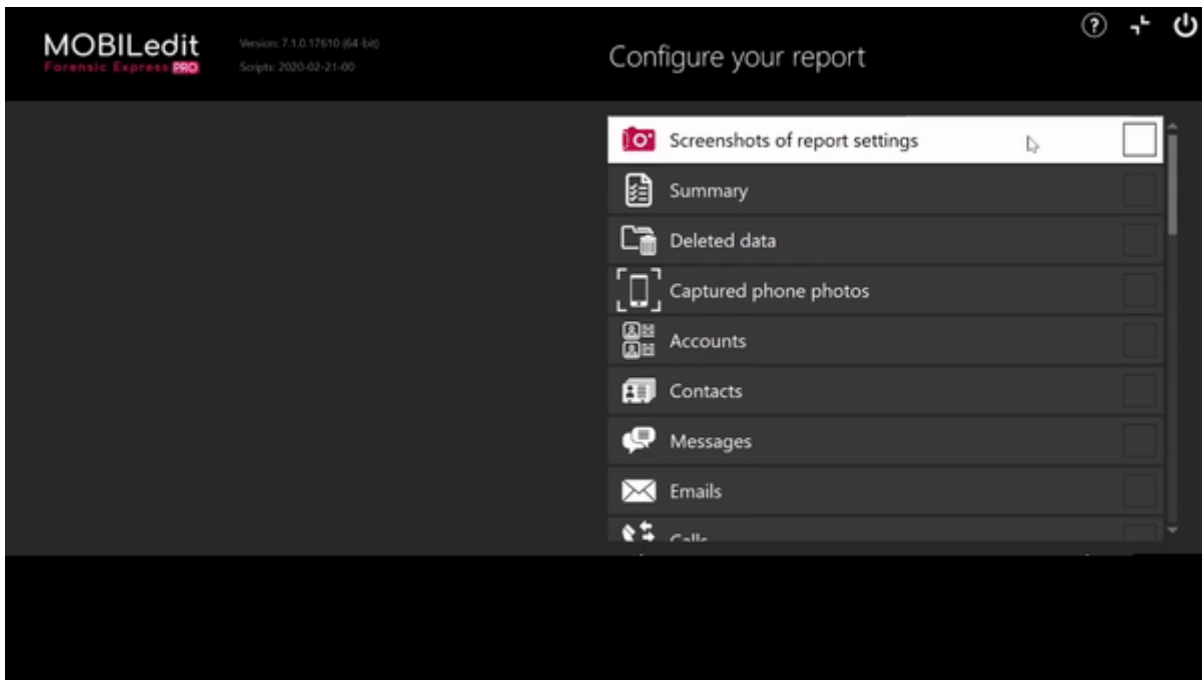
Thanks to the logs you can access the records of this information:

- Standard info about the device such as
 - device build number
 - platform
 - disk usage
 - MAC address
- When the device was activated
- How many times was the device connected/disconnected
- Where the device has been connected and for how long
 - Bluetooth
 - Wifi
- If the device was connected to a specific network, including:
 - Computer name
 - Hostname
 - Network hostname
- And many more

iOS screenshots directly from MOBILedit

A few simple clicks and you can take a screenshot of your phone directly in MOBILedit Forensic Express.

Try it yourself! Go to “Specific selection”, then “Captured phone photos”, browse manually on the device to whatever you wish to take a screenshot of and click on the “phone” button.

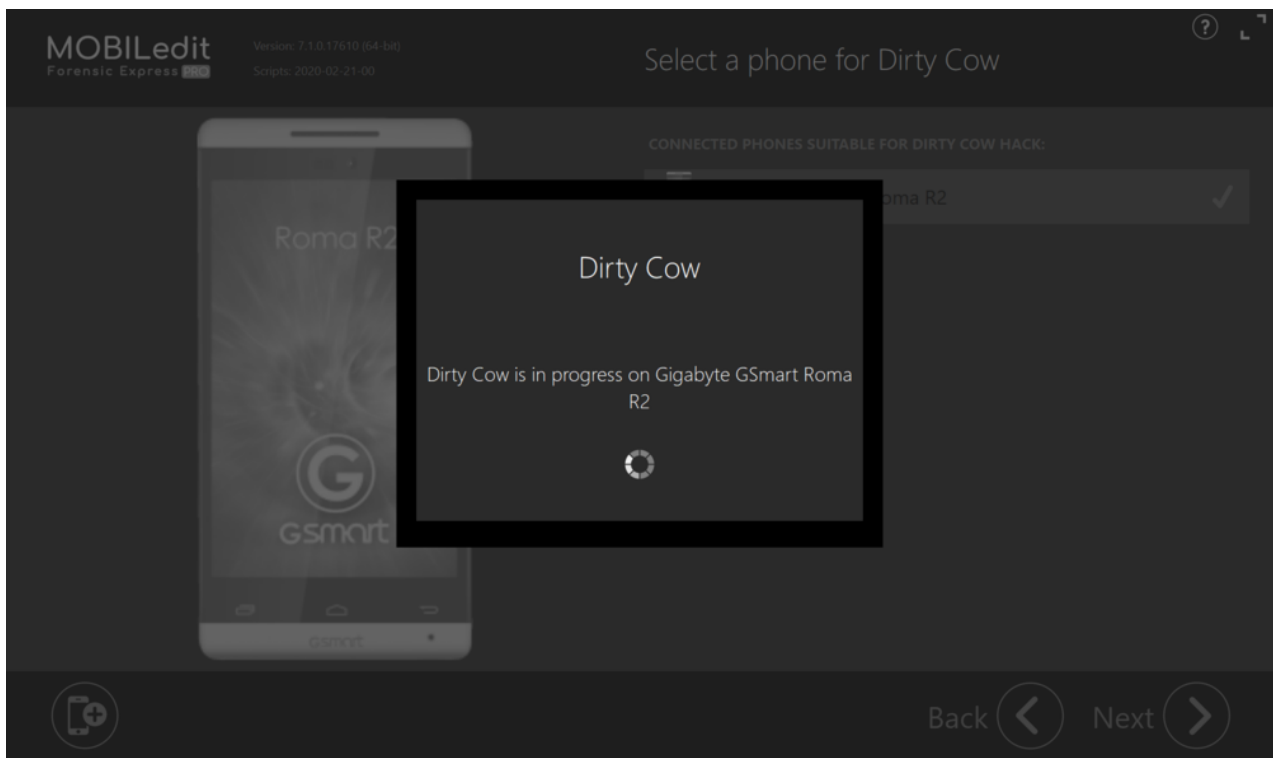


DirtyCow hack implemented

Any Android device up to version 7 can be now rooted with the Dirty Cow vulnerability directly in MOBILedit Forensic Express.

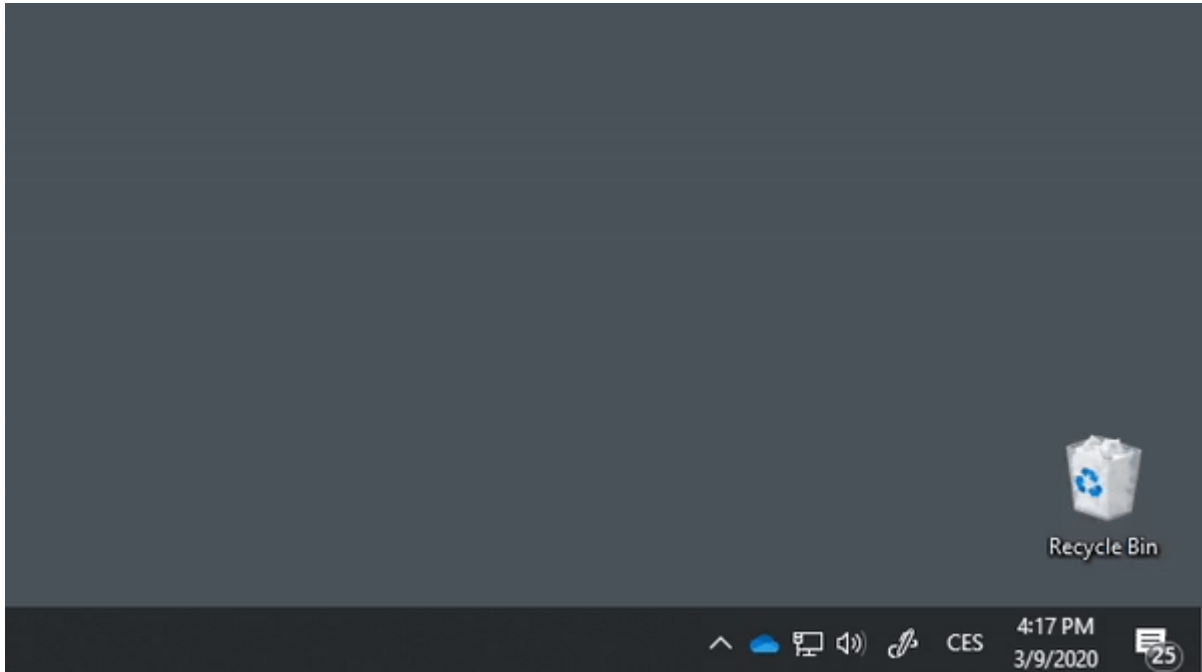
Dirty Cow is a temporary root and will be gone once you will restart the device.

[More info about the Dirty COW exploit and MOBILedit Forensic Express can be found in our User Guide\(see page 70\).](#)



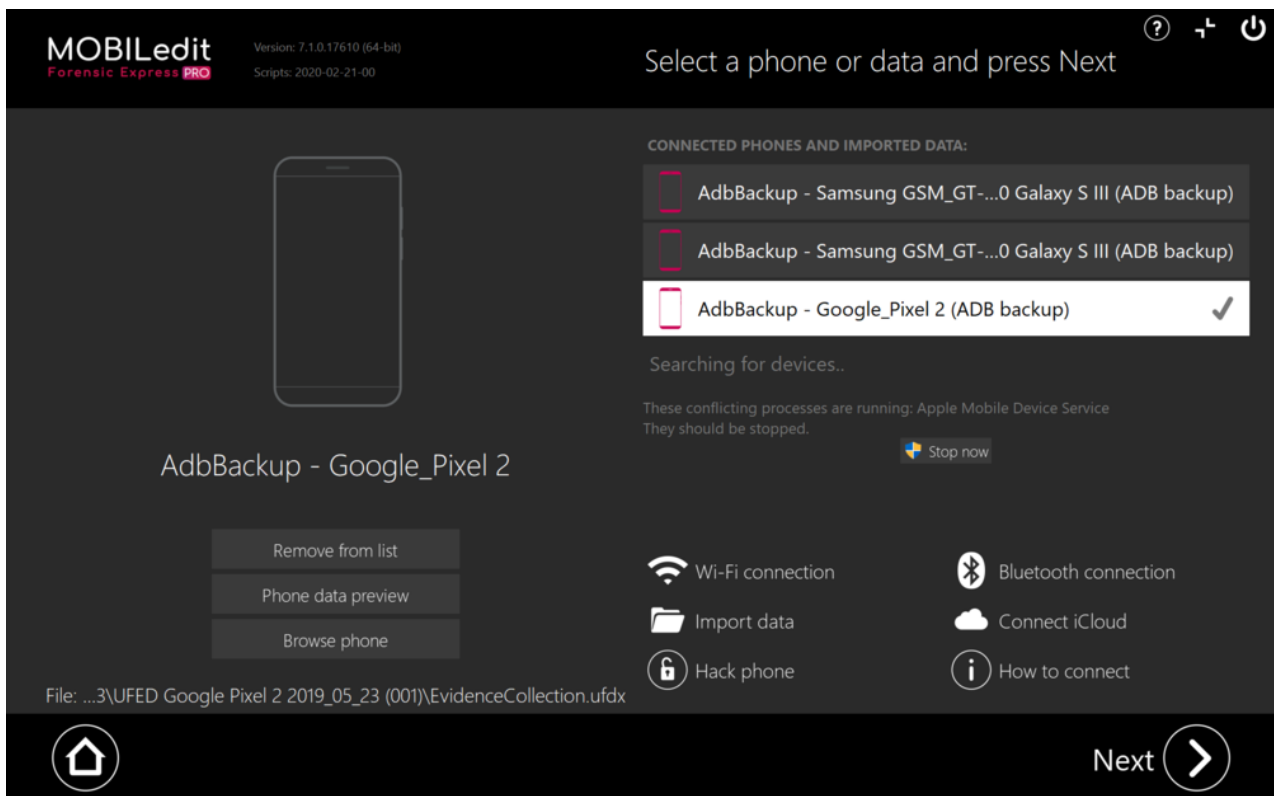
MOBILedit can notify you through Windows 10 notifications

A notification will appear whenever user interaction with MOBILedit Forensic Express is required.



UFDX file import

Extended support for Cellebrite UFED files.



New activation system

The generic alert message “Connection to the server has failed.” used for any error which might have occurred while activating a license has been abolished.

From now on, in case there is anything wrong, you’ll see only a specific message related to the error. This will help our dedicated support team to help you if it is needed.

10.4.2 Improvements and bugfixes

- UFED export/import compatibility improved
- Improved File Manager operations - Copy, Delete and Move
- Case information now extended
- iTunes Backup Reveal refreshes every time you open it
- Faster application start thanks to the optimization of how we load the update packages
- Camera Ballistics runs in background concurrently to speed up analysis
- Check for all needed Android permissions for Connector application
- Updated Czech, Portuguese, Slovak, and Spanish full product localizations
- Many minor improvements

10.5 7.0.3. Update

Update released October 10, 2019

10.5.1 What’s new

- Apple physical image import - We have implemented basic support for Apple HFS(+) physical images

10.5.2 Improvements and bugfixes

- Fixed loading of Face Matcher and Photo Recognizer packages
- Fixed issue of instances when not all metadata from media files was showing in reports
- Creates a new main.log if for some reason the old one was set as ‘read only’
- Improved description of categories in Timeline
- Improvements to the Cellebrite UFD/UFDR import/export function

MOBILedit Forensic Express¹²³ offers maximum functionality at a fraction of the price of other tools. It can be used as the only tool in a lab or as an enhancement to other tools such as UFED through its data compatibility.

10.6 7.0.2. Update

Update released September 20, 2019

iOS 13 has increased its security and many phone forensic tools don’t support it despite the fact it has been available in beta since 3rd June. It means these tools are not able to get any data or very limited data from millions of iPhones. MOBILedit fully supports iOS 13. It is clearly visible that examiners need more tools in their lab.

After the successful [release of MOBILedit Forensic Express 7.0](#)¹²⁴, our team continues with hard work and improving the product. If you are not using MOBILedit yet, [request a demo here](#)¹²⁵.

¹²³ <https://www.mobiledit.com/forensic-express>

¹²⁴ <https://www.mobiledit.com/news/release-7-0>

¹²⁵ <https://www.mobiledit.com/forensic-express/request-a-demo>

10.6.1 What's new

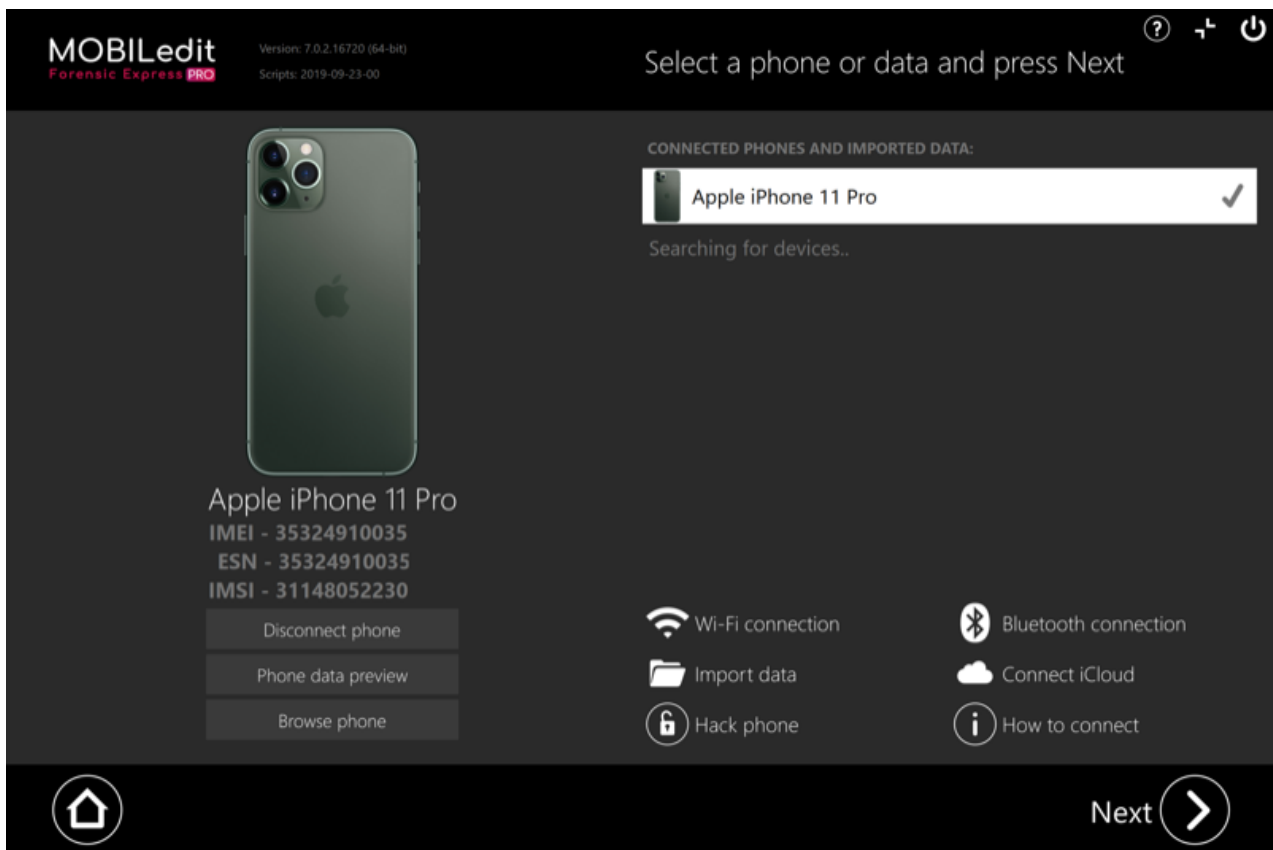
- iOS 13 is fully supported!
- **New iPhones also supported!**
We've tested them and added full support - after connecting any iPhone 11 model its name and photo displays (build 7.0.2.16723)
- Apple Watch analysis from iTunes backup
- Android 10 supported
- MTPwn hack implemented for Samsung phones - provides the content of many Samsung phones without the need of a password
- Files and folders extracted from a phone and moved to a PC will now have the same original timestamps
- Device total capacity and used space shown in reports
- Gathering information about debit or credit cards stored in Safari browser

10.6.2 Improvements and bugfixes

- Huawei backup crash fixed
- Analyses are skipped when doing only MOBILedit backup, ADB backup or iTunes backup extraction
- Improvements of Cellebrite UFD/UFDR import/export
- Snapchat Android analysis improved
- ICQ iOS analysis improved

MOBILedit Forensic Express¹²⁶ offers maximum functionality at a fraction of the price of other tools. It can be used as the only tool in a lab or as an enhancement to other tools such as UFED through its data compatibility.

¹²⁶ <https://www.mobiledit.com/forensic-express>



10.7 7.0.1. Update

Update released September 3, 2019

10.7.1 What's new

- Now with option to create your MOBILedit backups to contain only the exact matched data from Specific Selection with their corresponding reports (PDF, excel, HTML), or, you can create your MOBILedit backups to contain all phone data but only show the Specific Selection data in the reports.
- All possible device application permissions are now shown in the report if the APK file is extracted.
- Installer applications (other than Google Play) are shown for Android applications.
- Files and folders extracted from the phone will now show the original created, modified and accessed dates and times in Windows file system.

10.7.2 Other improvements

- Improved exact matches of key words using “quotations marks”, with case-sensitive searching, able to search and find specific entire words and not just a section of the word.
- Encrypted MOBILedit backup package can be read directly without unpacking.
- Improved naming of photos from webcam.
- Improved naming of unfinished PDF files. Be aware of opening these if PDF generation is still running.
- Cellebrite UFD/UFDR import/export improved
- PDF generator improved

- Physical image improved

10.8 7.0. Update

Update released August 9, 2019

MOBILedit is one of the first phone forensic tools, and since 1996 has played an important role in the industry. Now we have released a big version 7.0, moving phone forensics forward. As an expert in the field you shouldn't miss this event.

New **MOBILedit Forensic Express**¹²⁷ comes with a better user experience, better reports, better phone unlocking, is faster and brings great new features. If you are not using MOBILedit Forensic Express yet, [request a demo here](#)¹²⁸.

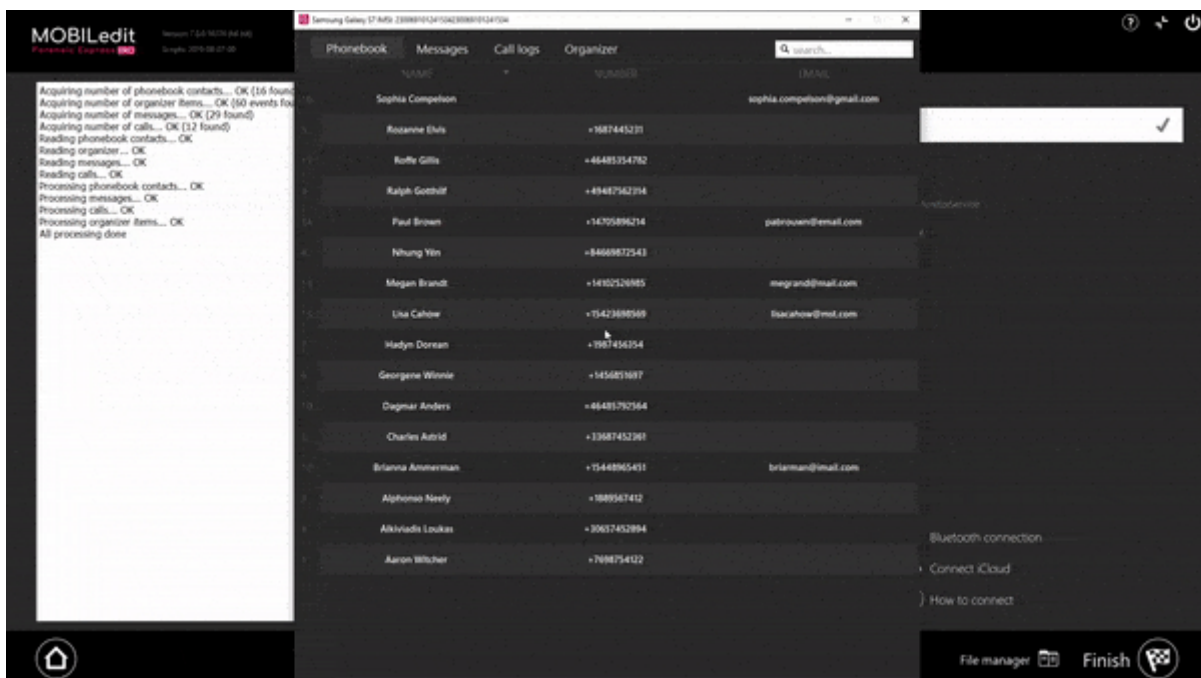
According to feedback from our customers, here's what they like the most about MOBILedit Forensic Express:

- Highest number of supported apps and best in getting data from messengers and other apps
- Fast updates with Live Updates plus on-demand application analysis
- Great in recovering deleted data
- Best reports, especially PDF, easily understandable to whoever reads them
- Ease of use, requires minimum learning
- Fast, concurrent processing of many devices
- Price effective

10.8.1 What's new

Phone data pre-viewer

- View essential data before the extraction even starts! This can rapidly speedup evidence collection to help in making the right decisions quickly.

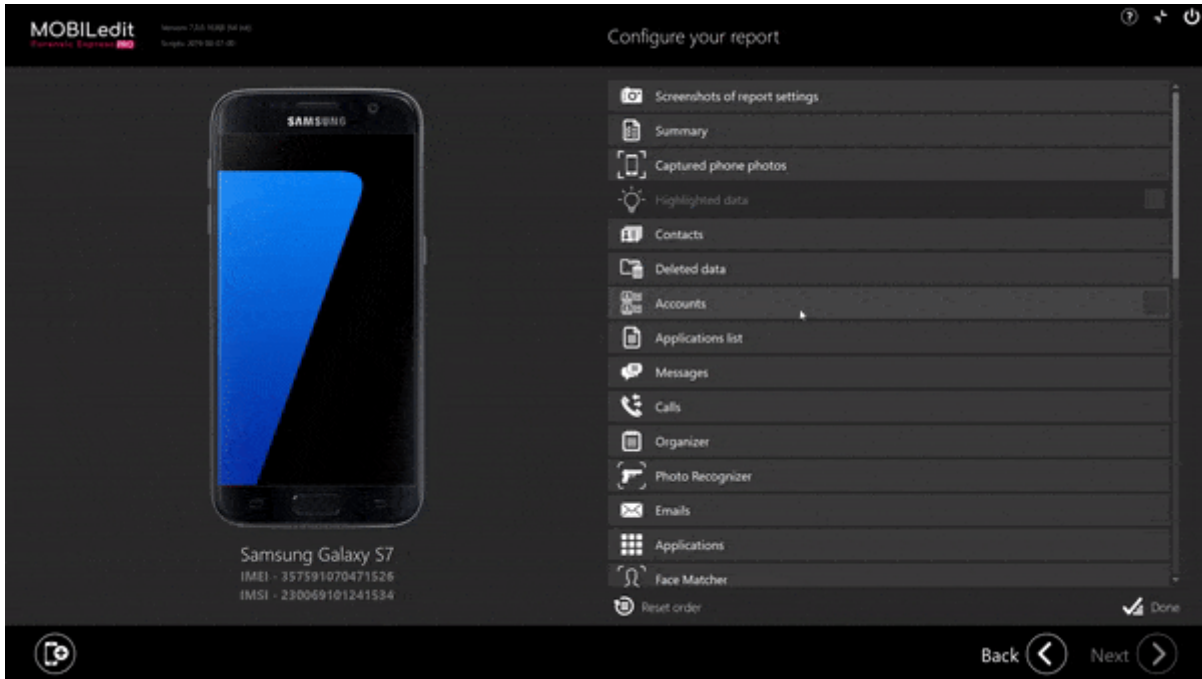


¹²⁷ <https://www.mobiledit.com/forensic-express>

¹²⁸ <https://www.mobiledit.com/forensic-express/request-a-demo>

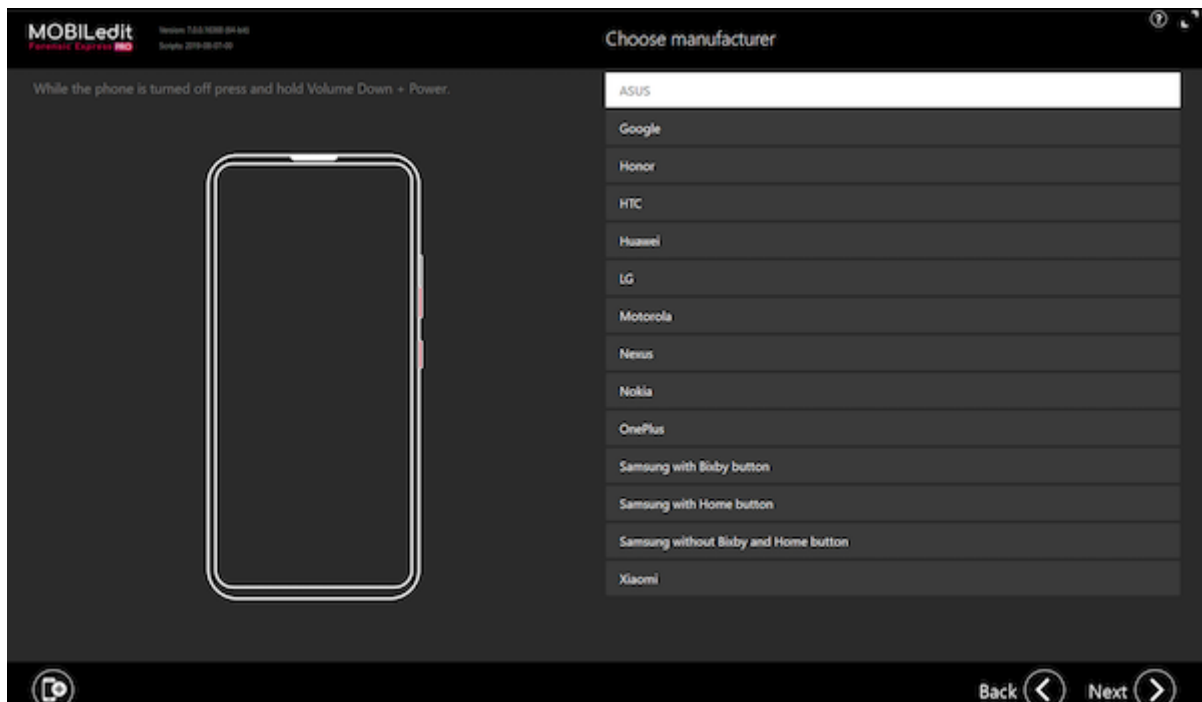
What You See Is What You Get - WYSIWYG reports

- Our reports are now fully customizable – you can choose the most important data and order them any way you want to. You can literally define the content of the report at your fingertips.



Better Android phones unlocking

- We have implemented phone unlocking by using flashing of custom recovery images for some Android phones, so you don't need to root those phones and can get the physical image with access to maximum data without knowing the user password.



Hardware license dongles now supported

- Now you can take your license with you in case you need to work in the field or do not have access to the internet. Also you can share your license with colleagues in a more flexible way.

Faster extractions of media from iPhone

- Extractions of photos and videos from new iOS devices are now much faster by using multi-threading for re-coding and resizing images.

New spyware detection

- In addition to malware we can now detect spyware by using machine-learning; we can even find new, unknown and proprietary developed spyware code.

Our best in the industry reports are now even better

- We have fine-tuned our PDF and html reports taking your case presentation to even an higher level.

MOBILedit is now fully available in these languages: Portuguese, Czech, Slovak, working on many more, let us know if you want to translate...

Easy connection of Apple devices by handling driver installation

10.8.2 Other improvements

- Huawei - HiSuite backup analysis improved
- File Manager now displays file metadata information
- iMessage photos report display improved
- Loading report configuration file improved
- Improved physical images loading
- Custom recovery image creation improved
- Drive 'free space' appearance improved

10.8.3 Application analysis improvements

Analysis of apps is very important today for successful investigations, so we have added many:

- Airbnb updated
- Agoda iOS version added
- Baidu Map Android version added
- Bitcoin Wallet added
- [Bitcoin.com](http://bitcoin.com/)¹²⁹ Wallet added
- Dolphin browser updated
- Duolingo added
- Faceapp added
- Facebook Messenger updated
- Fake GPS Free Android version added
- Fake GPS Pro Android version added
- Fake Location Android version added
- Gmail updated
- Google updated for Android and iOS version added
- Google Drive updated
- Google Maps updated
- GPS Joystick Android version added
- Hangouts updated

¹²⁹ <http://bitcoin.com/>

- Hola Fake GPS Android version added
- Hot or Not added
- ICQ updated
- Instagram updated
- iOS Notes updated
- Joyride / Jaumo added
- LinkedIn updated
- LIME added
- Location Changer Android version added
- Luno updated for Android and iOS version added
- Mycelium Wallet added
- OkCupid added
- Pinterest updated
- QQ application updated
- Skype updated
- Telegram updated
- Threema updated
- TikTok updated
- Twitter updated
- WhatsApp updated
- Yandex added
- YouTube updated
- And almost 100 weather applications added

10.9 6.1.1. Update

Update released April 18, 2019

10.9.1 **What's new**

- Now you are able to disable the display of company and product logo in the HTML and PDF report
- iCloud login via tokens is available now
- Report translations updated (Czech, Slovak, Polish, Spanish)

10.9.2 **Bugfixes and minor improvements**

- Huawei (HiSuite) backup analysis fixed
- Loading physical images bug fixed
- Faster loading of EMMC physical images
- iMessage analysis freeze fixed
- Update dialogs improved
- HTML report TOC layout in Chrome browser fixed
- iCloud logoff fixed

10.9.3 **New app analysis**

- Yubo (Android & iOS)

10.9.4 Improved app analysis

- WhatsApp (Android & iOS), timestamp "Read" added
- Inbox (Android & iOS) improved

10.10 6.1. Update

Update released March 26, 2019

10.10.1 What's new

- **We are launching free online training in English, Spanish and Portuguese, accessible from the product front page!**
- PDF splitting is back! New PDF reports now can be also split to multiple files by chapters. We also provide cross-links between items placed in different files, click an item and it will open the right file at the right place.
- iCloud backup download and analysis updated for new iOS and working at the edge of current possibilities. Two factor authentication with new iOS may still not work, as nobody in the industry is able to solve this.
- Improved speed of both iOS and Android extractions by optimizing the quantity of data, especially media.

10.10.2 Bugfixes and minor improvements

- Improved text overlay in PDF report
- Enhanced support of non-latin characters in PDF report
- Optimized Timeline results in PDF report
- Fixed Google Maps links with diacritics in reports
- Improved File Browser, filenames now can contain "%"
- Deleted photos from iOS devices have better mark
- Physical image acquisition fixed

10.10.3 Improved app analysis

- Skype for Business (Android)
- Viber (Android)
- Seznam.cz¹³⁰ (Android & iOS)
- Evernote (iOS)
- Telegram (Android)
- KakaoTalk (Android)
- K9 mail (Android)

10.11 6.0.1. Update

Update released January 24, 2019

¹³⁰ <http://Seznam.cz>

10.11.1 Improvements

- Default PDF resolution decreased from 300DPI to 150DPI - file size of report was reduced and report creation is faster, quality is same both - on the screen and when printed
- Improved de-duplication of image files from iPhone
- Improved HTML report table of content
- Facebook Messenger analysis improved
- Chinese translation updated
- Portuguese translation updated

10.11.2 Bugfixes

- PDF report localization fixed
- iTunes backup stability fixed
- Hash check error fixed

10.12 6.0. Update

Update released January 16, 2019



It is with great pleasure we present to you the new MOBILedit Forensic Express version 6.0.

We have developed an all-new PDF generator from scratch which is now much faster, requires less memory and generates the same beautiful reports.

With an ever-growing quantity of data in phones, you can now generate any size single PDF without the need of splitting. MOBILedit Forensic Express 6.0 delivers an even better experience with extraction and analysis results.

10.12.1 Now available in two editions - PRO and STANDARD

PRO edition is designed for users seeking advanced functionality - perfect for all law enforcement, industry experts and professional forensics.

Standard edition is packed with the essentials - ideal for users who need a high-quality, reliable and user-friendly forensic tool, but might not need advanced level add-ons.

All current installations of MOBILedit Forensic Express will be automatically converted to PRO edition.

The Standard edition is available for purchase in our online store, while PRO edition is available through our partners or direct sales, please contact us for pricing and availability. [Check features comparison of Standard and PRO edition here](#)¹³¹.

10.12.2 New features and improvements

- New PDF generator, fast, efficient, delivering the best reports in the industry
- Screen unlocking history added for Android phones
- Contact pictures now have links and are clickable
- Apple Watch data analysis added
- Displaying cell towers in the interactive location map
- Android account analysis is improved
- VCard contact analysis improved

10.12.3 Bugfixes

- Unexpected software termination during application analysis fixed
- Fixed differences for Camera Ballistics in the timeline
- Cookies listing in report fixed
- Temporary iTunes backup password handling improved

¹³¹ <https://www.mobiledit.com/online-store/forensic-express>