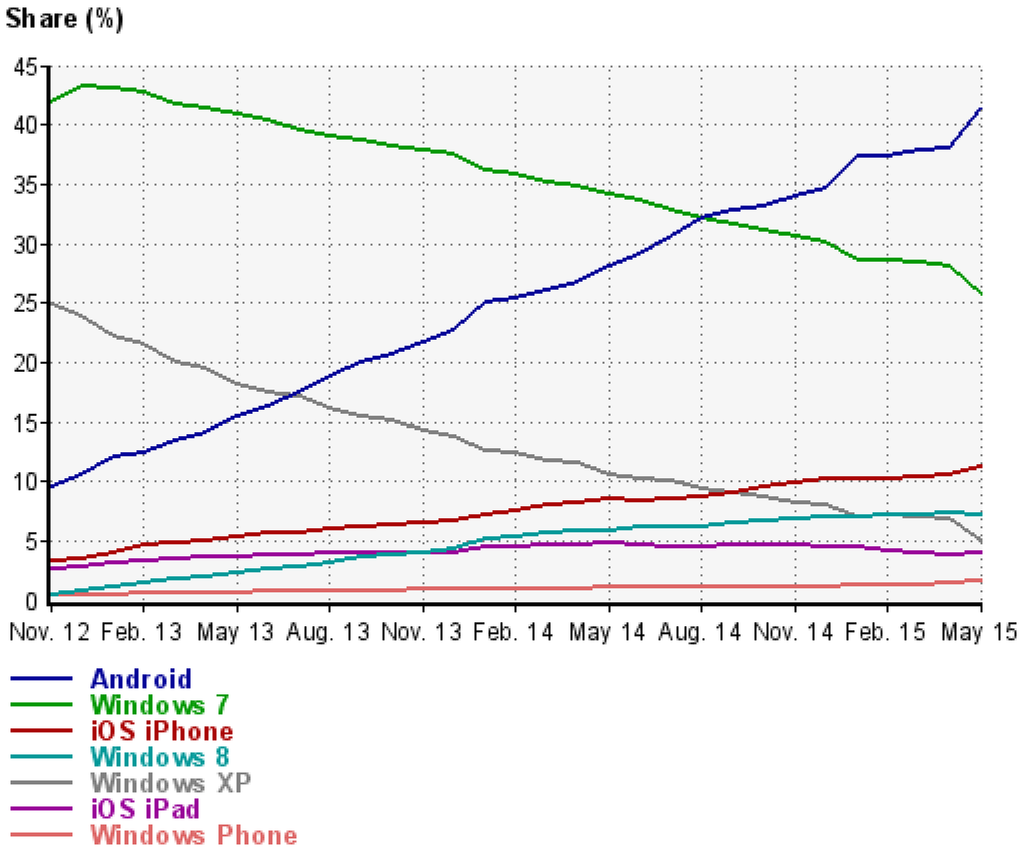
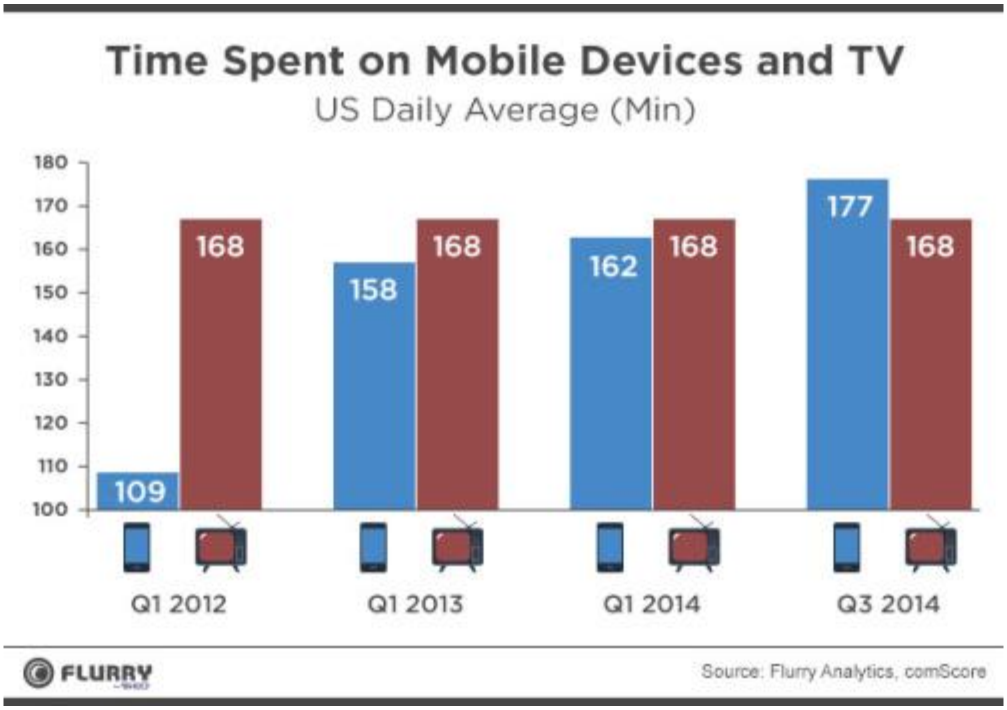
Chapter 1: Introducing Mobile Forensics



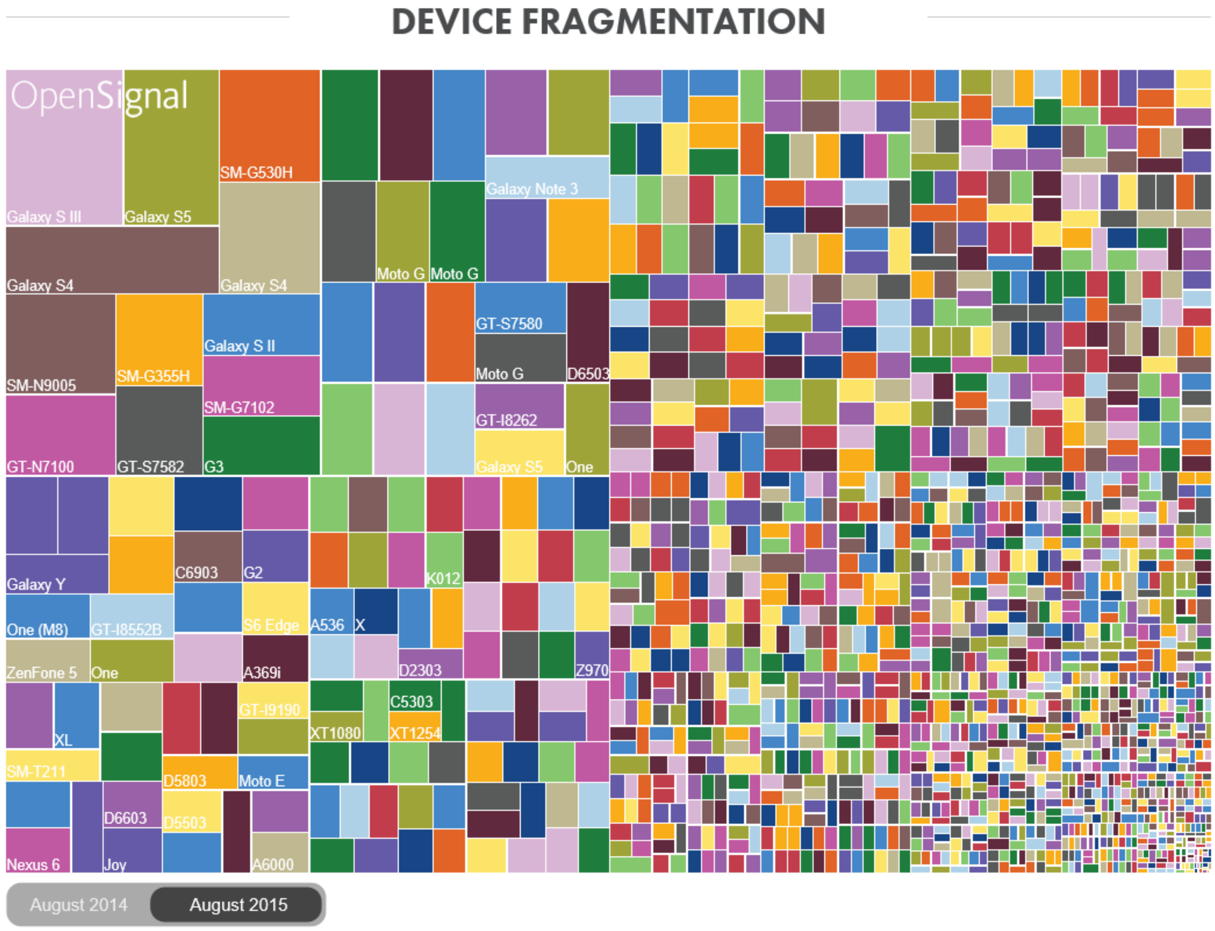


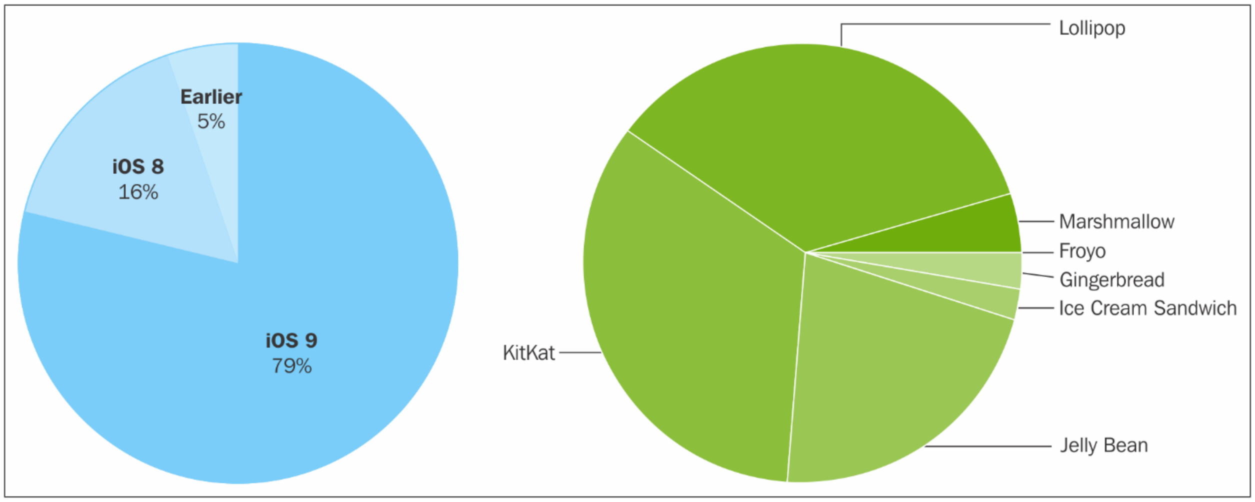
Time Spent on Mobile Devices and TV

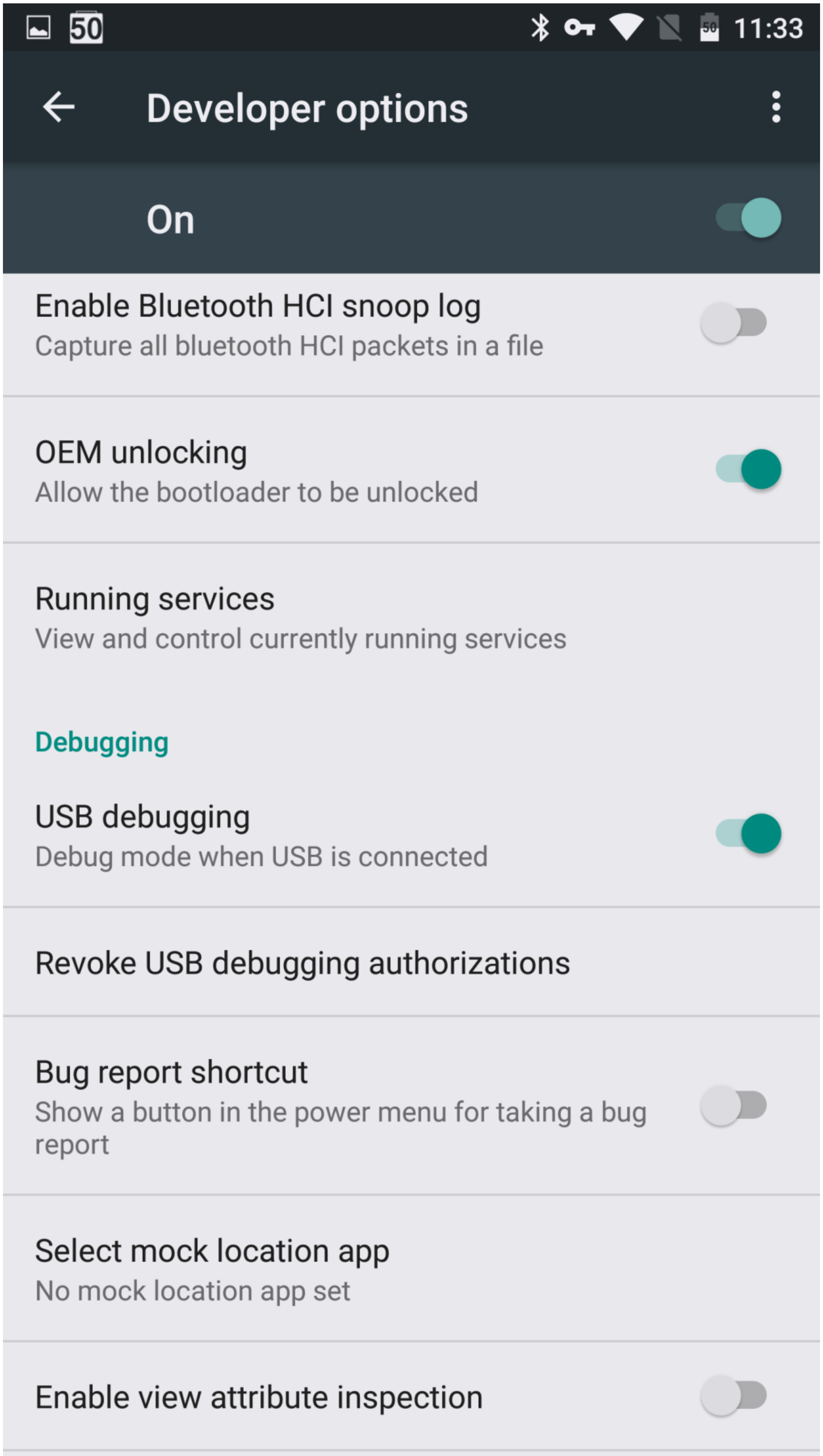
US Daily Average (Min)

Source: Flurry Analytics, comScore

Chapter 3: Acquisition – Approaching Android Devices







Developer options

On

Enable Bluetooth HCI snoop log
Capture all bluetooth HCI packets in a file

OEM unlocking
Allow the bootloader to be unlocked

Running services
View and control currently running services

Debugging

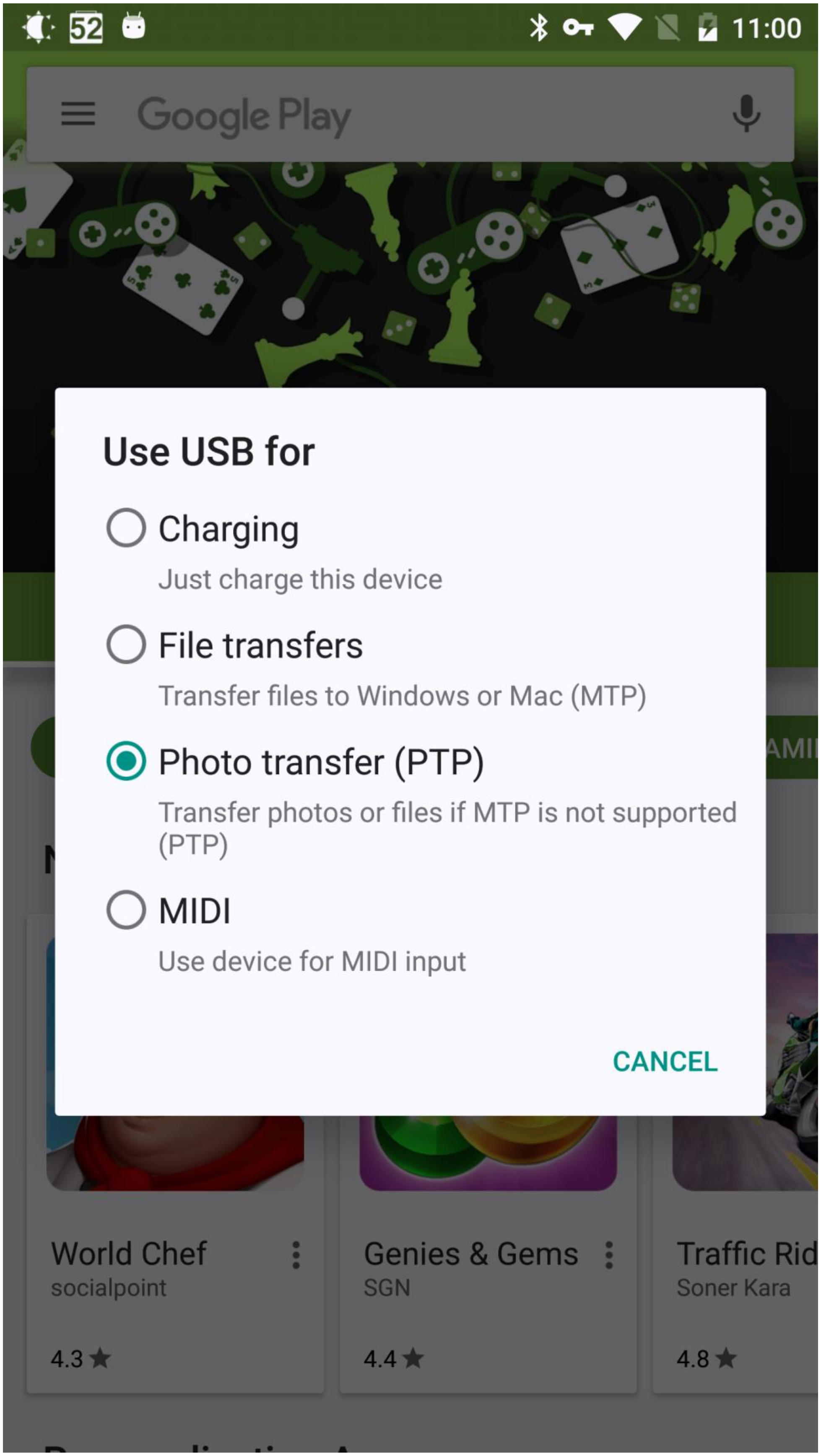
USB debugging
Debug mode when USB is connected

Revoke USB debugging authorizations

Bug report shortcut
Show a button in the power menu for taking a bug report

Select mock location app
No mock location app set

Enable view attribute inspection



Use USB for

○ Charging

Just charge this device

○ File transfers

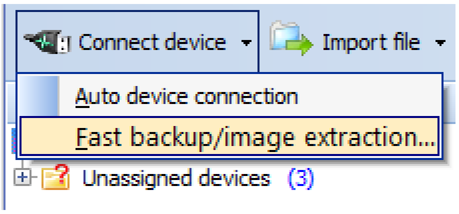
Transfer files to Windows or Mac (MTP)

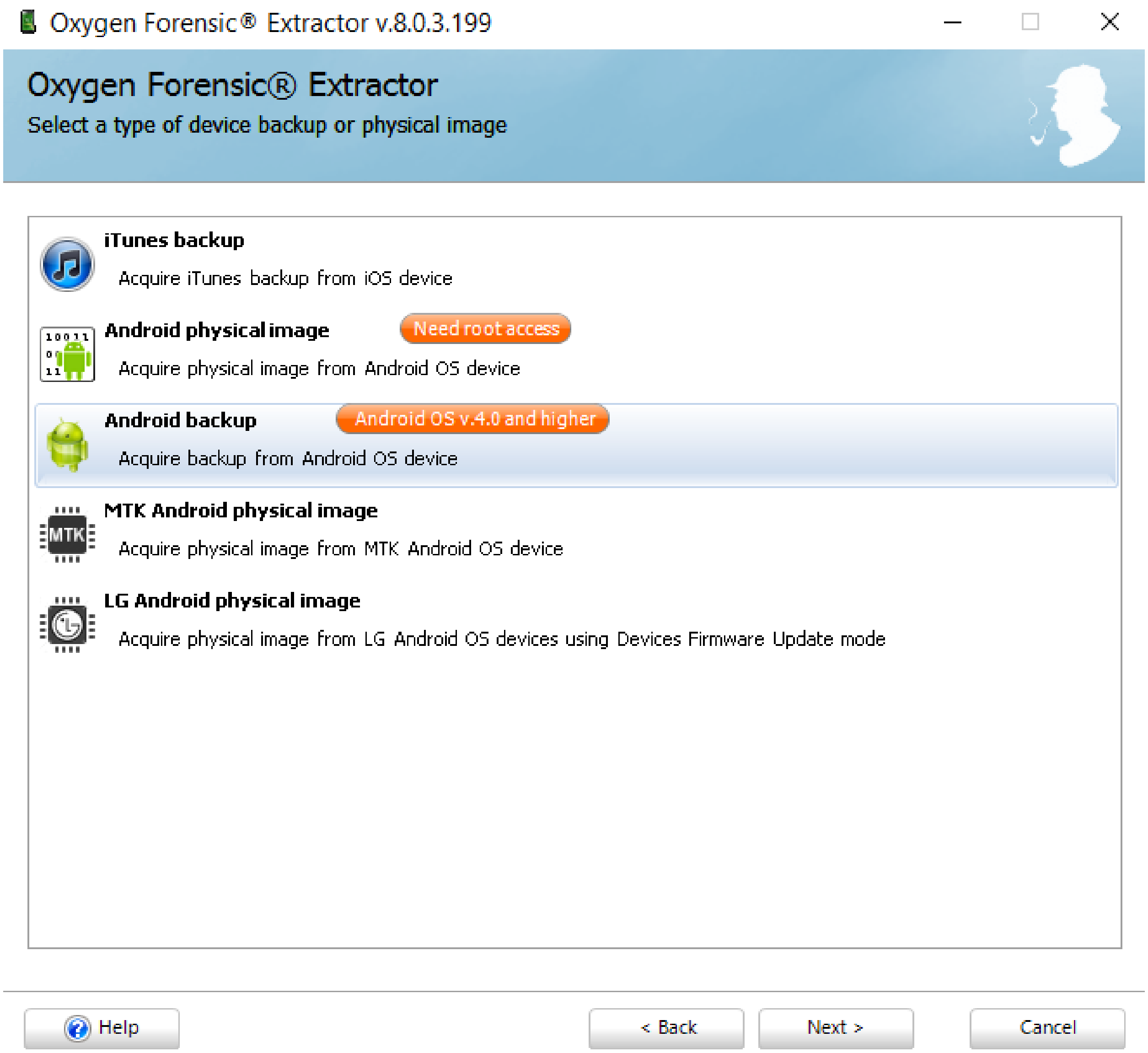
● Photo transfer (PTP)

Transfer photos or files if MTP is not supported (PTP)

○ MIDI

Use device for MIDI input





Oxygen Forensic® Extractor

Select a type of device backup or physical image

iTunes backup

Acquire iTunes backup from iOS device

Android physical image Need root access

Acquire physical image from Android OS device

Android backup Android OS v.4.0 and higher

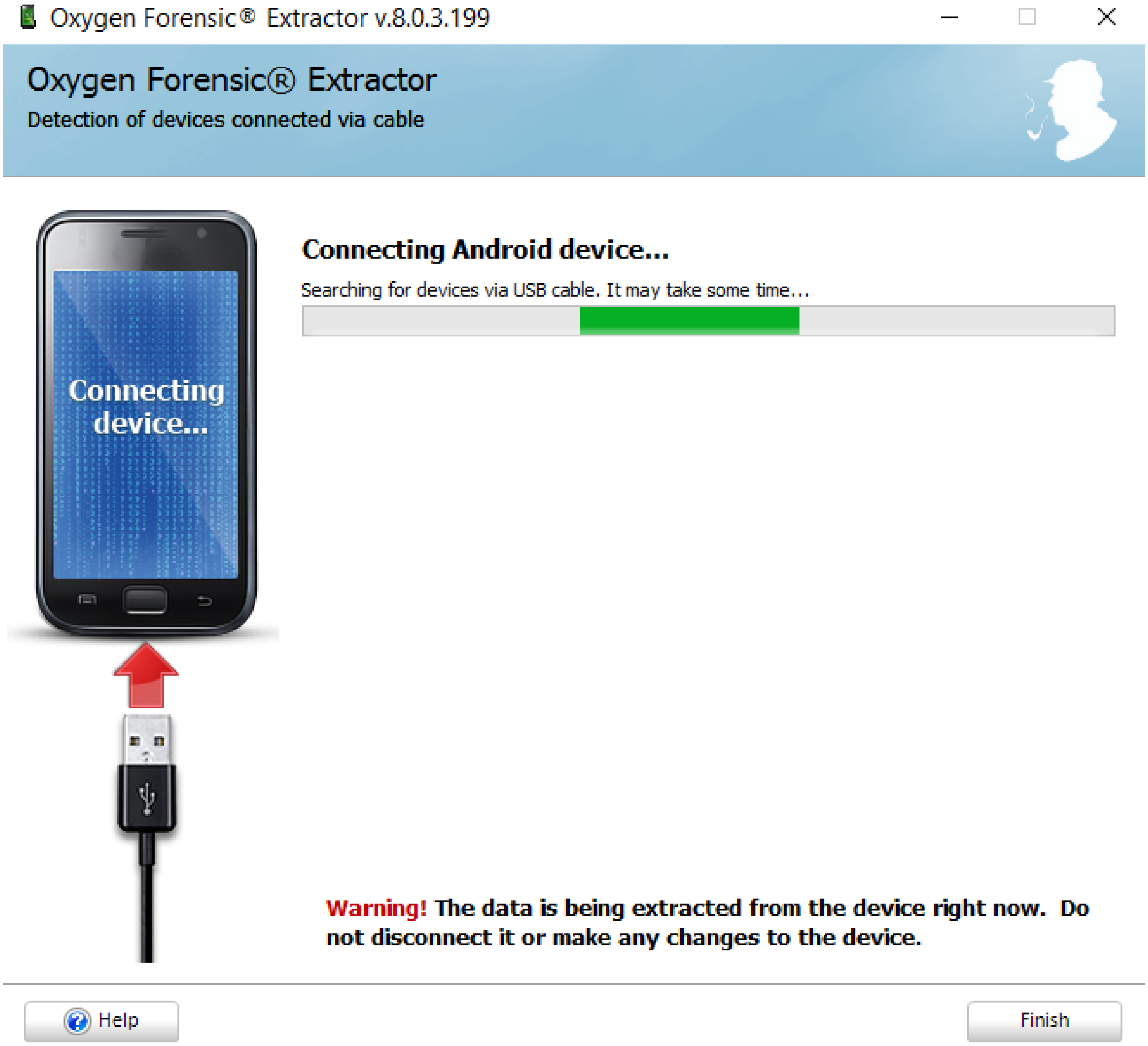
Acquire backup from Android OS device

MTK Android physical image

Acquire physical image from MTK Android OS device

LG Android physical image

Acquire physical image from LG Android OS devices using Devices Firmware Update mode



Oxygen Forensic® Extractor v.8.0.3.199

Oxygen Forensic® Extractor

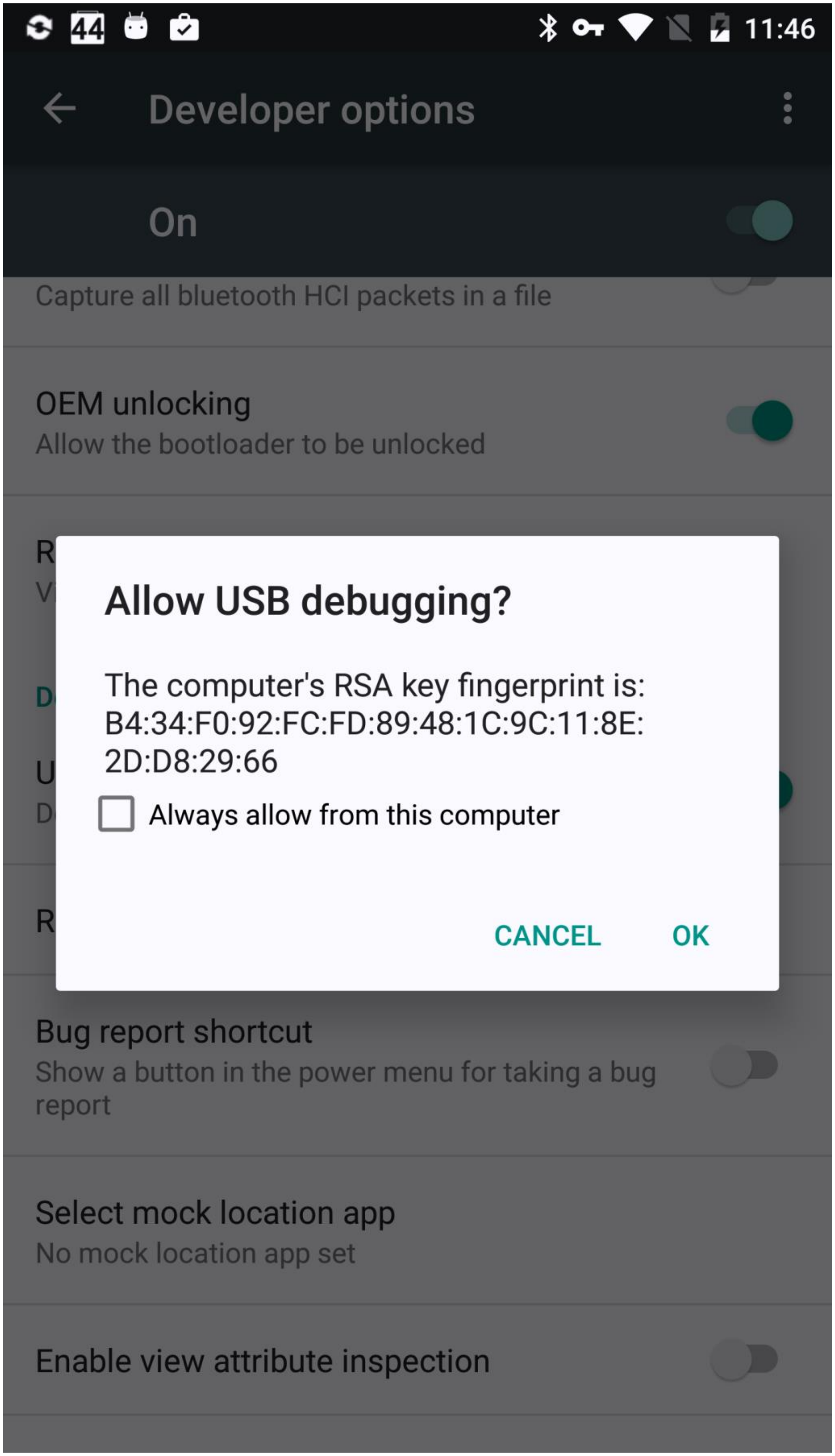
Detection of devices connected via cable

Connecting Android device...

Searching for devices via USB cable. It may take some time...

Connecting device...

Warning! The data is being extracted from the device right now. Do not disconnect it or make any changes to the device.



Developer options

On

Capture all bluetooth HCI packets in a file

OEM unlocking
Allow the bootloader to be unlocked

Allow USB debugging?

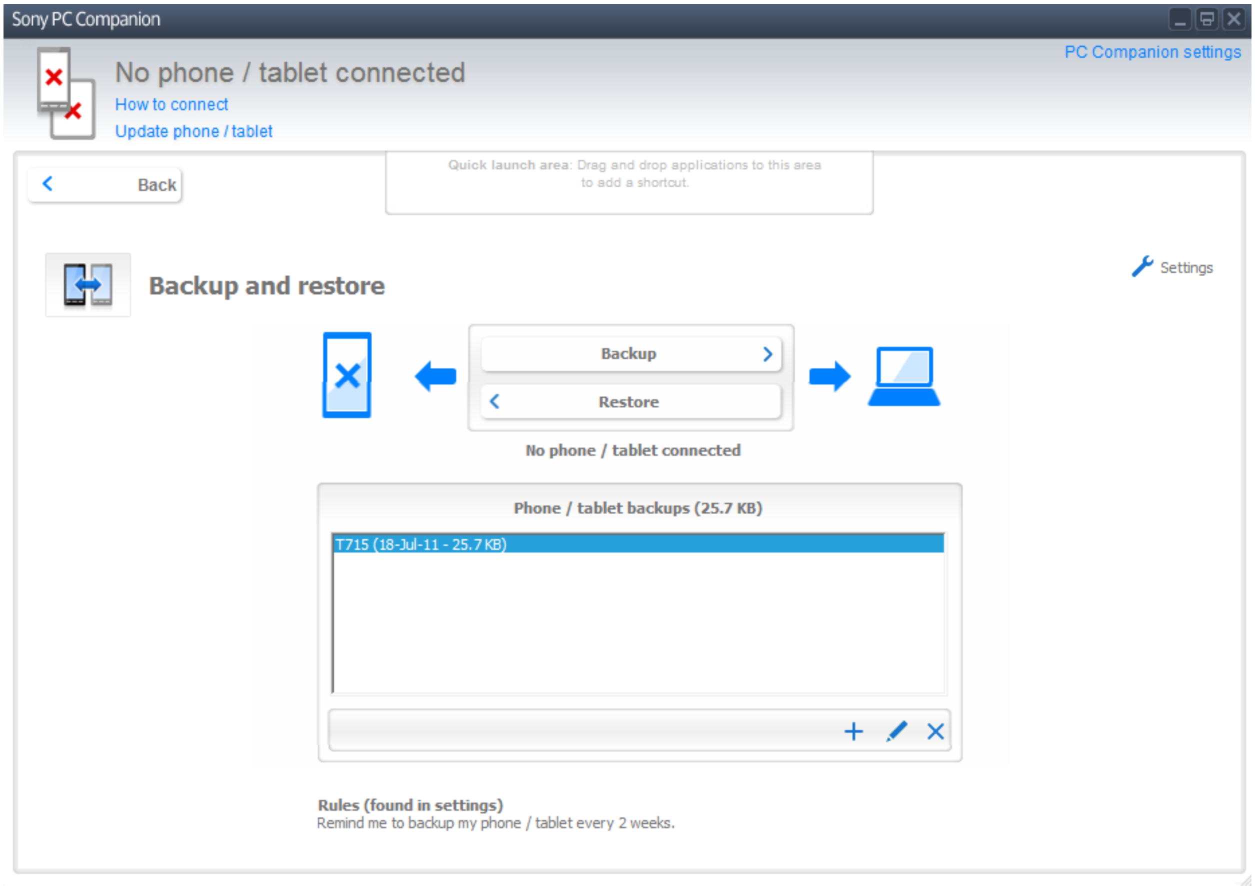
The computer's RSA key fingerprint is:
B4:34:F0:92:FC:FD:89:48:1C:9C:11:8E:
2D:D8:29:66

□ Always allow from this computer

Bug report shortcut
Show a button in the power menu for taking a bug report

Select mock location app
No mock location app set

Enable view attribute inspection



No phone / tablet connected

Quick launch area: Drag and drop applications to this area to add a shortcut.

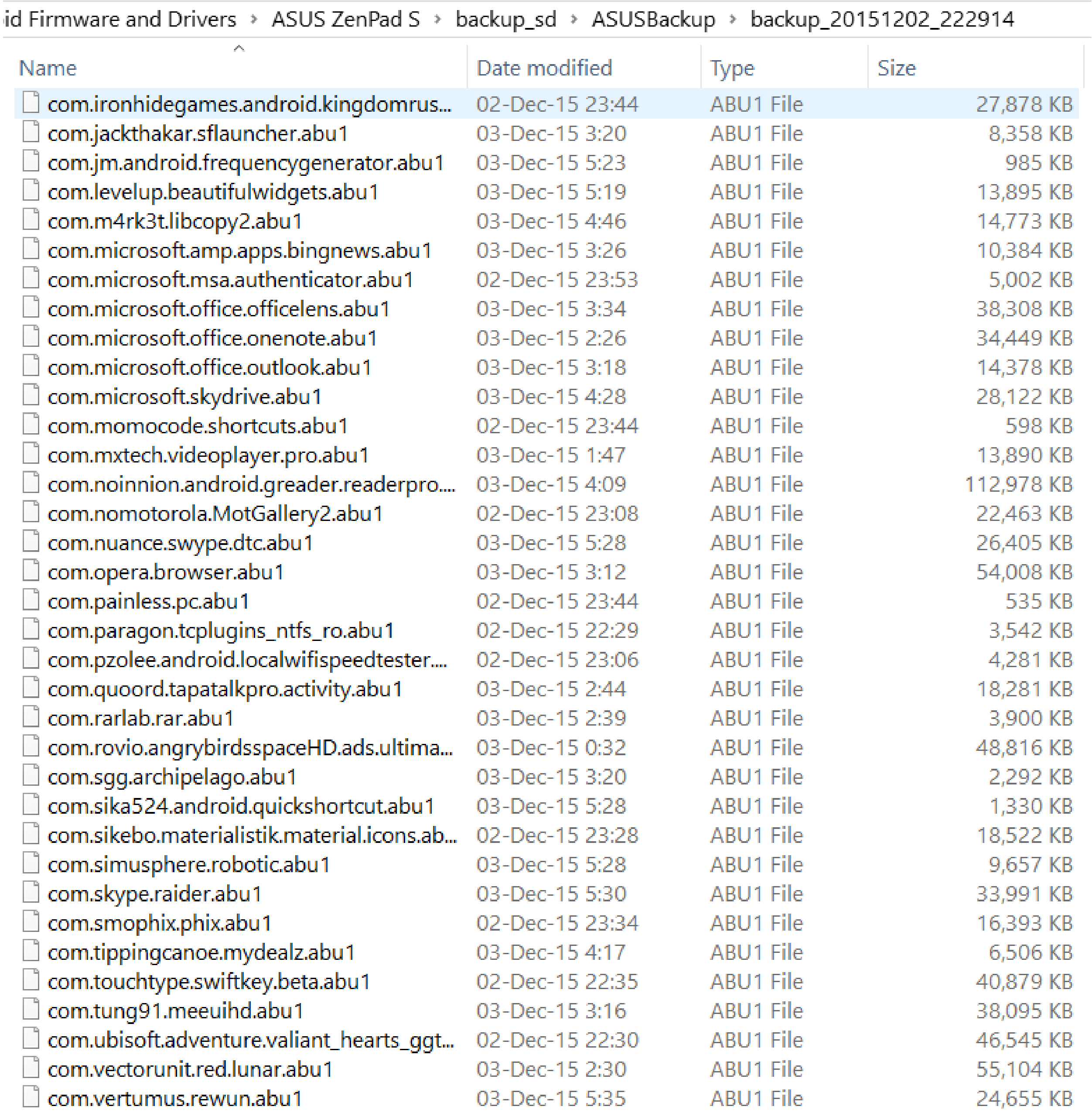
Backup and restore

No phone / tablet connected

Phone / tablet backups (25.7 KB)

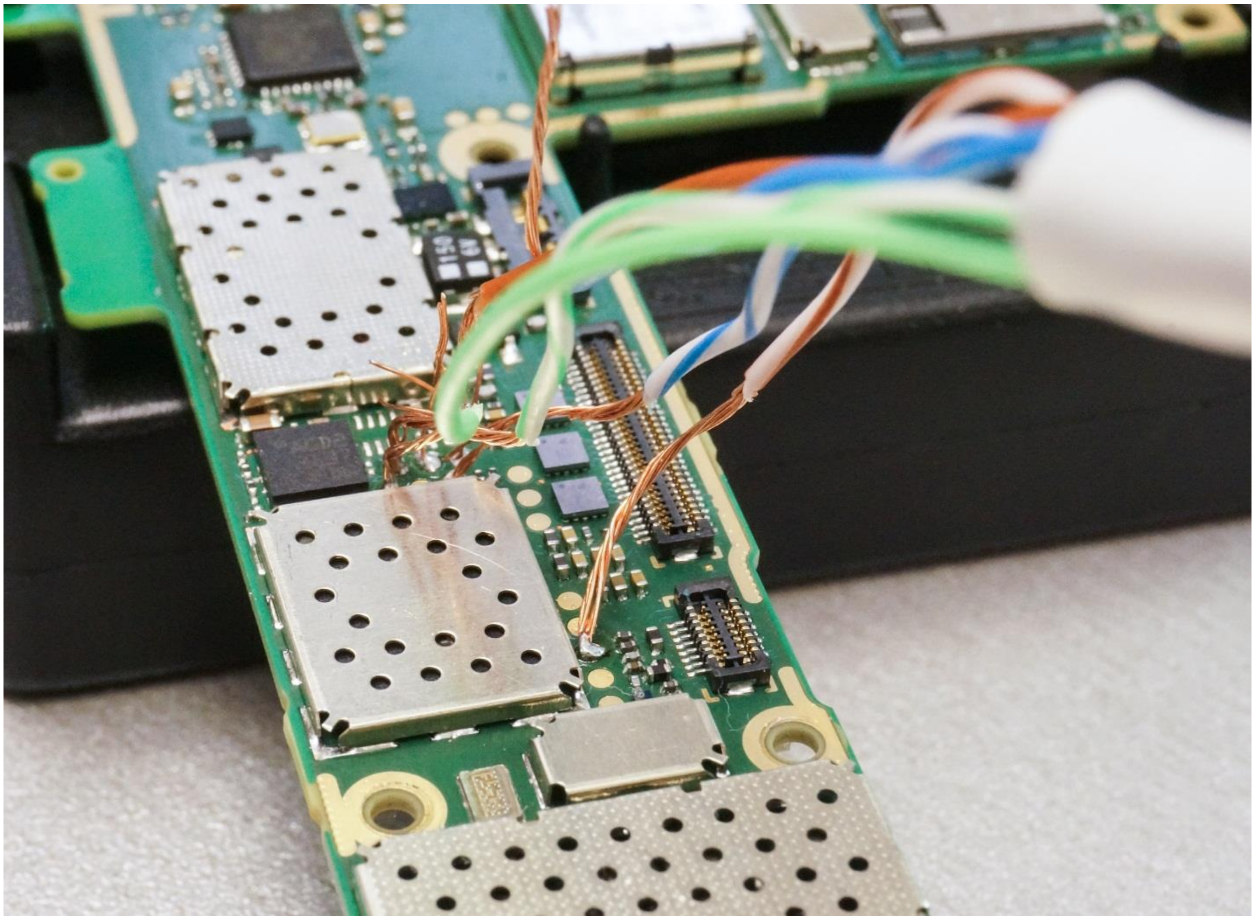
T715 (18-Jul-11 - 25.7 KB)

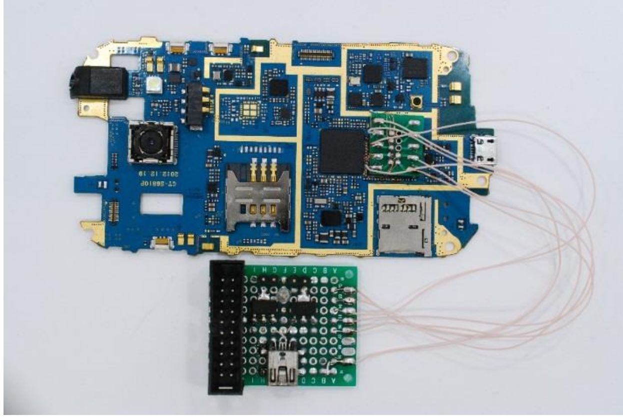
Rules (found in settings)
Remind me to backup my phone / tablet every 2 weeks.

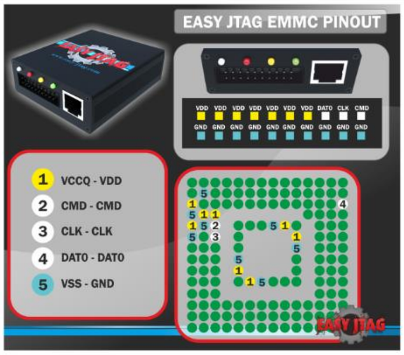


id Firmware and Drivers › ASUS ZenPad S › backup_sd › ASUSBackup › backup_20151202_222914

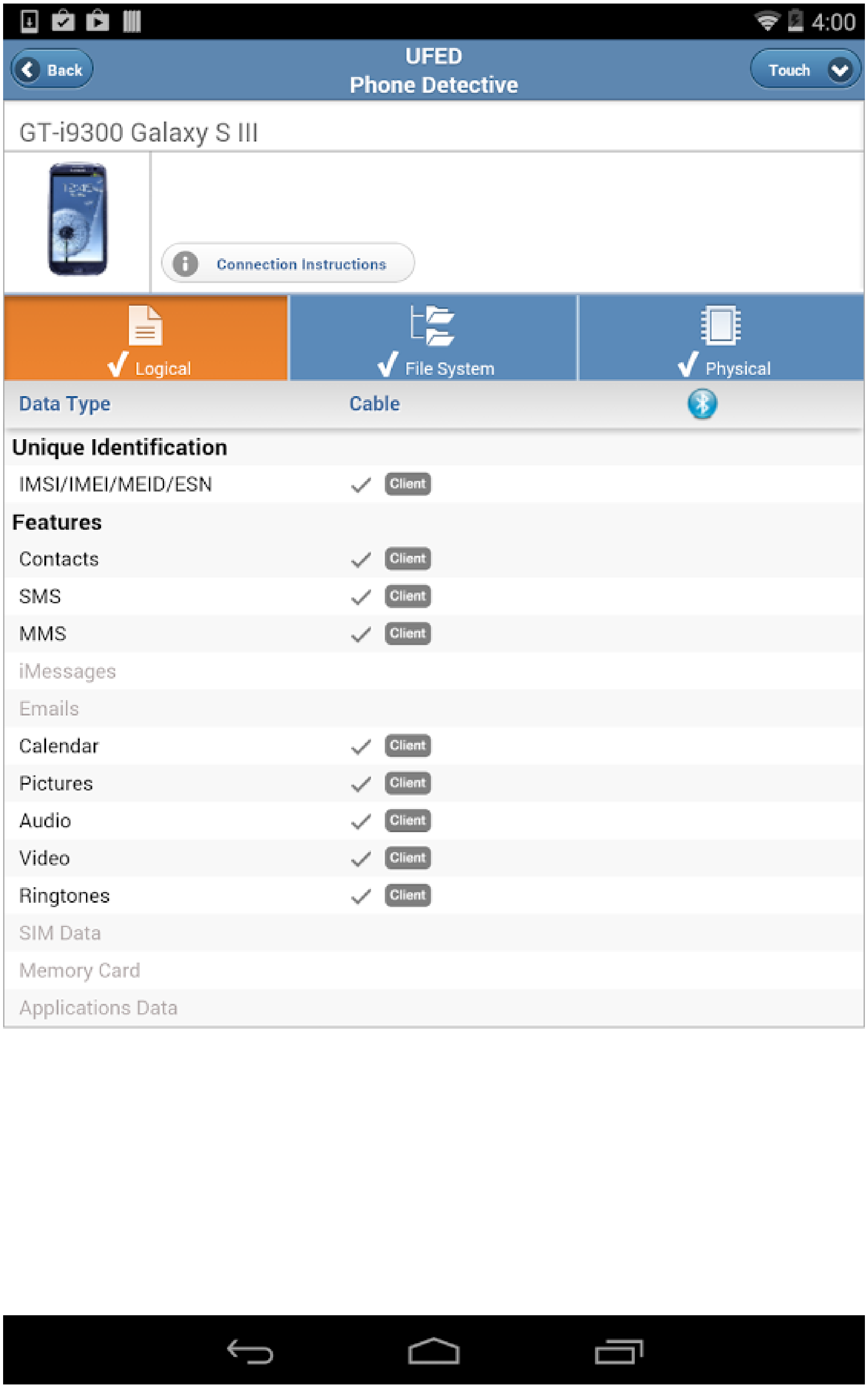
Name	Date modified	Type	Size
com.ironhidegames.android.kingdomrus...	02-Dec-15 23:44	ABU1 File	27,878 KB
com.jackthakar.sflauncher.abu1	03-Dec-15 3:20	ABU1 File	8,358 KB
com.jm.android.frequencygenerator.abu1	03-Dec-15 5:23	ABU1 File	985 KB
com.levelup.beautifulwidgets.abu1	03-Dec-15 5:19	ABU1 File	13,895 KB
com.m4rk3t.libcopy2.abu1	03-Dec-15 4:46	ABU1 File	14,773 KB
com.microsoft.amp.apps.bingnews.abu1	03-Dec-15 3:26	ABU1 File	10,384 KB
com.microsoft.msa.authenticator.abu1	02-Dec-15 23:53	ABU1 File	5,002 KB
com.microsoft.office.officelens.abu1	03-Dec-15 3:34	ABU1 File	38,308 KB
com.microsoft.office.onenote.abu1	03-Dec-15 2:26	ABU1 File	34,449 KB
com.microsoft.office.outlook.abu1	03-Dec-15 3:18	ABU1 File	14,378 KB
com.microsoft.skydrive.abu1	03-Dec-15 4:28	ABU1 File	28,122 KB
com.momocode.shortcuts.abu1	02-Dec-15 23:44	ABU1 File	598 KB
com.mxtech.videoplayer.pro.abu1	03-Dec-15 1:47	ABU1 File	13,890 KB
com.noinnion.android.greader.readerpro....	03-Dec-15 4:09	ABU1 File	112,978 KB
com.nomotorola.MotGallery2.abu1	02-Dec-15 23:08	ABU1 File	22,463 KB
com.nuance.swype.dtc.abu1	03-Dec-15 5:28	ABU1 File	26,405 KB
com.opera.browser.abu1	03-Dec-15 3:12	ABU1 File	54,008 KB
com.painless.pc.abu1	02-Dec-15 23:44	ABU1 File	535 KB
com.paragon.tcplugins_ntfs_ro.abu1	02-Dec-15 22:29	ABU1 File	3,542 KB
com.pzolee.android.localwifispeedtester....	02-Dec-15 23:06	ABU1 File	4,281 KB
com.quoord.tapatalkpro.activity.abu1	03-Dec-15 2:44	ABU1 File	18,281 KB
com.rarlab.rar.abu1	03-Dec-15 2:39	ABU1 File	3,900 KB
com.rovio.angrybirdsspaceHD.ads.ultima...	03-Dec-15 0:32	ABU1 File	48,816 KB
com.sgg.archipelago.abu1	03-Dec-15 3:20	ABU1 File	2,292 KB
com.sika524.android.quickshortcut.abu1	03-Dec-15 5:28	ABU1 File	1,330 KB
com.sikebo.materialistik.material.icons.ab...	02-Dec-15 23:28	ABU1 File	18,522 KB
com.simusphere.robotic.abu1	03-Dec-15 5:28	ABU1 File	9,657 KB
com.skype.raider.abu1	03-Dec-15 5:30	ABU1 File	33,991 KB
com.smophix.phix.abu1	02-Dec-15 23:34	ABU1 File	16,393 KB
com.tippingcanoe.mydealz.abu1	03-Dec-15 4:17	ABU1 File	6,506 KB
com.touchtype.swiftkey.beta.abu1	02-Dec-15 22:35	ABU1 File	40,879 KB
com.tung91.meeuihd.abu1	03-Dec-15 3:16	ABU1 File	38,095 KB
com.ubisoft.adventure.valiant_hearts_ggt...	02-Dec-15 22:30	ABU1 File	46,545 KB
com.vectorunit.red.lunar.abu1	03-Dec-15 2:30	ABU1 File	55,104 KB
com.vertumus.rewun.abu1	03-Dec-15 5:35	ABU1 File	24,655 KB






EASY JTAG EMMC PINOUT
VDD VDD VDD VDD VDD VDD VDD DAT0 CLK CMD
GND GND GND GND GND GND GND GND GND GND
1 VCCQ - VDD
2 CMD - CMD
3 CLK - CLK
4 DAT0 - DAT0
5 VSS - GND
EASY JTAG

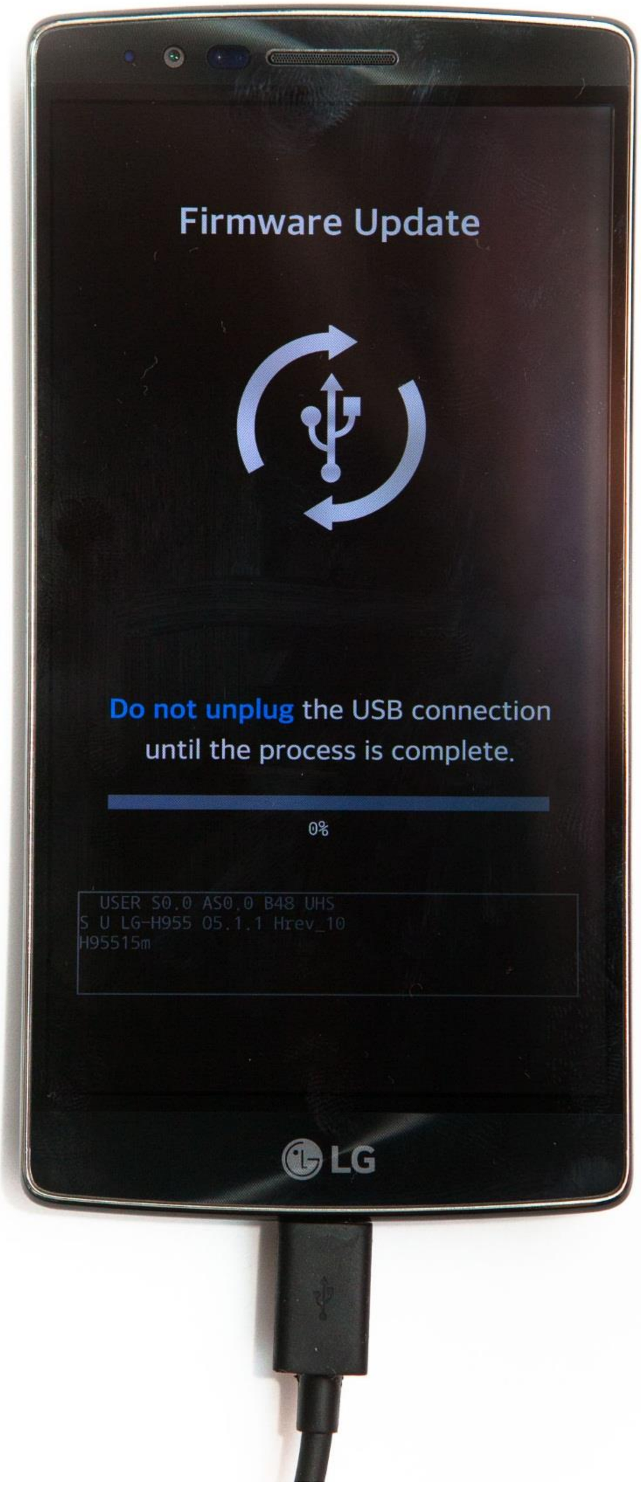
Chapter 4: Practical Steps to Android Acquisition



UFED
Phone Detective

GT-i9300 Galaxy S III

Data Type	Cable	✱
Unique Identification		
IMSI/IMEI/MEID/ESN	✓ Client	
Features		
Contacts	✓ Client	
SMS	✓ Client	
MMS	✓ Client	
iMessages		
Emails		
Calendar	✓ Client	
Pictures	✓ Client	
Audio	✓ Client	
Video	✓ Client	
Ringtones	✓ Client	
SIM Data		
Memory Card		
Applications Data		

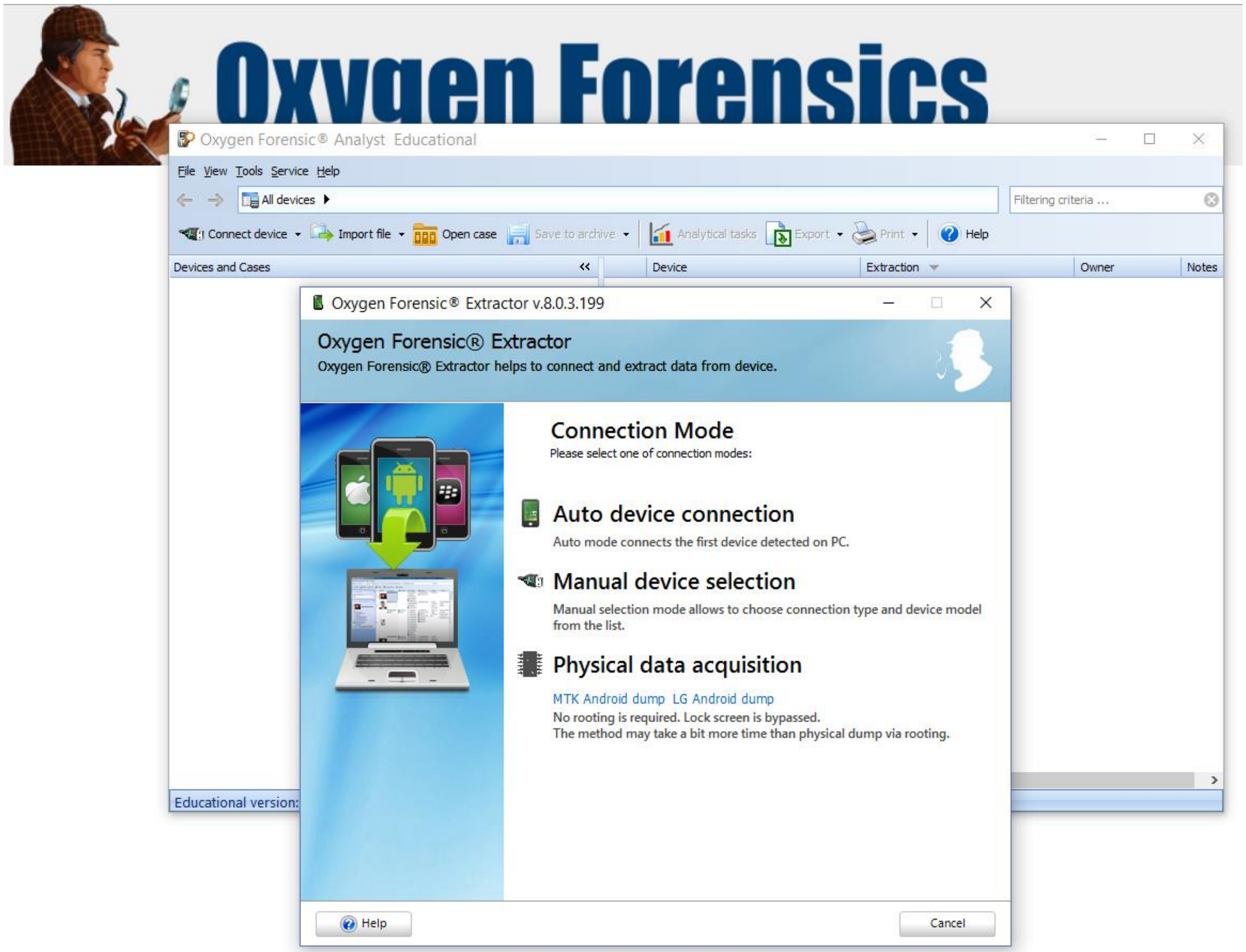


Firmware Update

Do not unplug the USB connection until the process is complete.

0%

```
  USER S0.0 AS0.0 B48 UHS
S U LG-H955 05.1.1 Hrev_10
H95515m
```



Oxygen Forensic® Extractor

Oxygen Forensic® Extractor helps to connect and extract data from device.

Connection Mode

Please select one of connection modes:

Auto device connection

Auto mode connects the first device detected on PC.

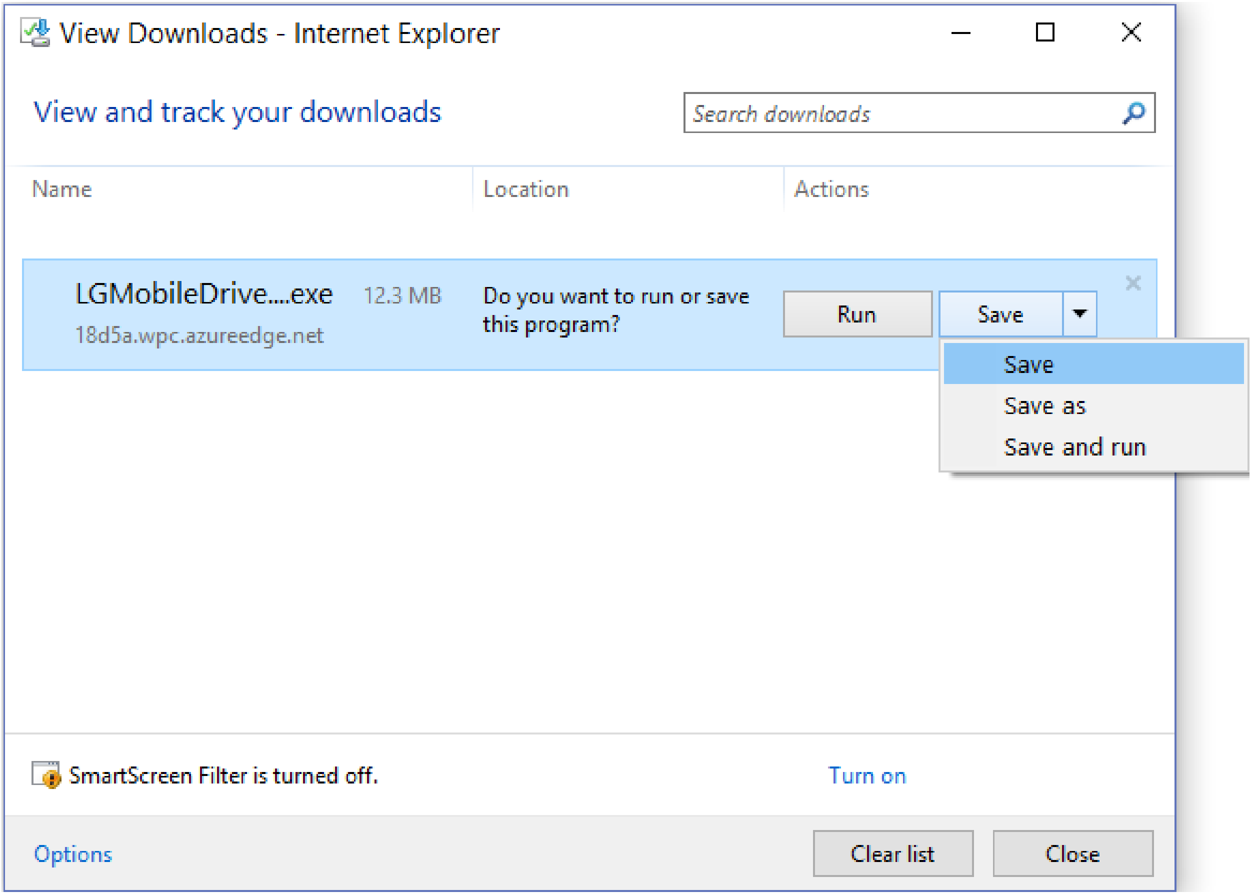
Manual device selection

Manual selection mode allows to choose connection type and device model from the list.

Physical data acquisition

MTK Android dump LG Android dump

No rooting is required. Lock screen is bypassed.
The method may take a bit more time than physical dump via rooting.



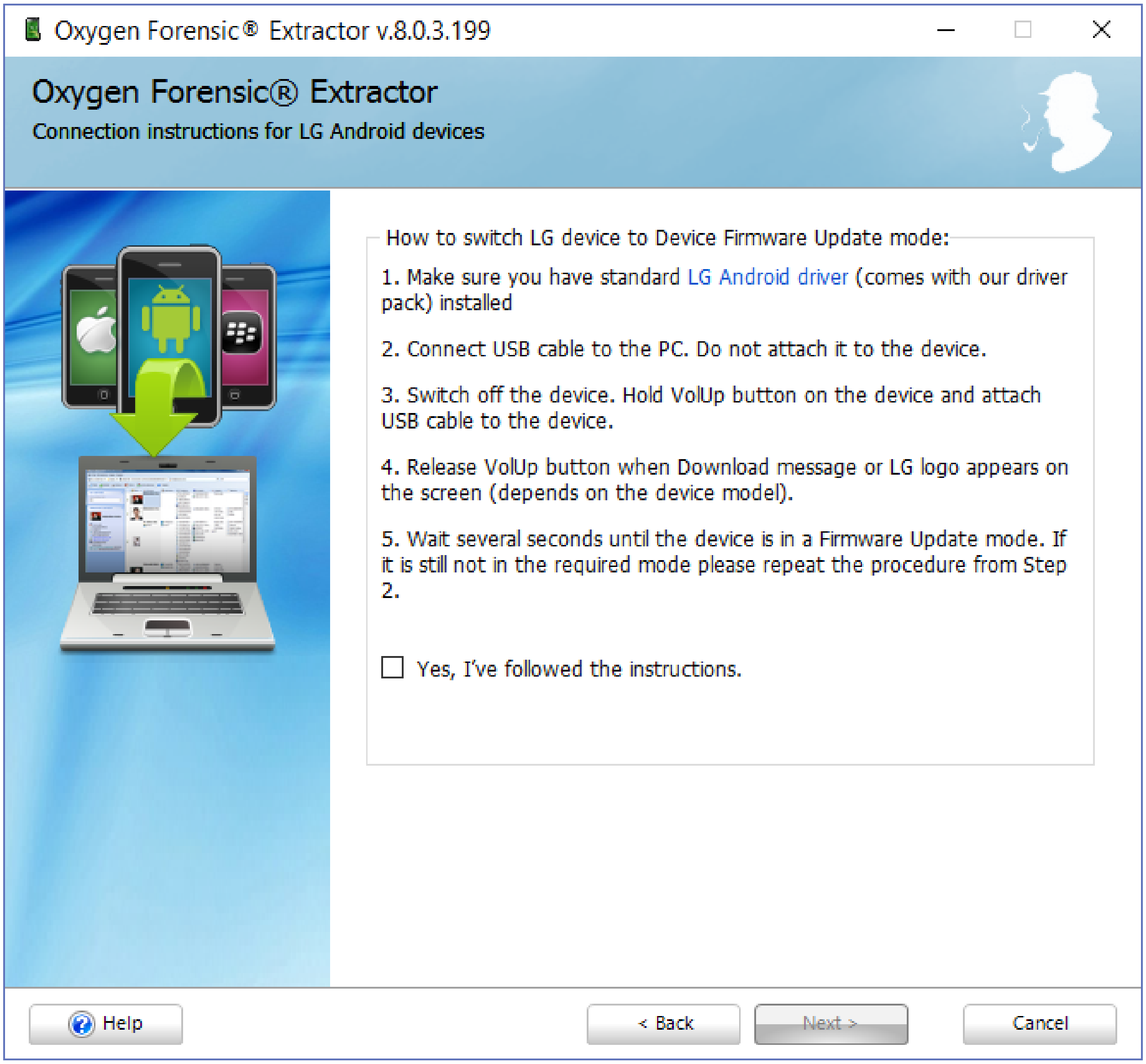
View Downloads - Internet Explorer

View and track your downloads

LGMobileDrive....exe 12.3 MB
18d5a.wpc.azureedge.net

Do you want to run or save this program?

SmartScreen Filter is turned off.



Oxygen Forensic® Extractor

Connection instructions for LG Android devices

How to switch LG device to Device Firmware Update mode:

1. Make sure you have standard LG Android driver (comes with our driver pack) installed

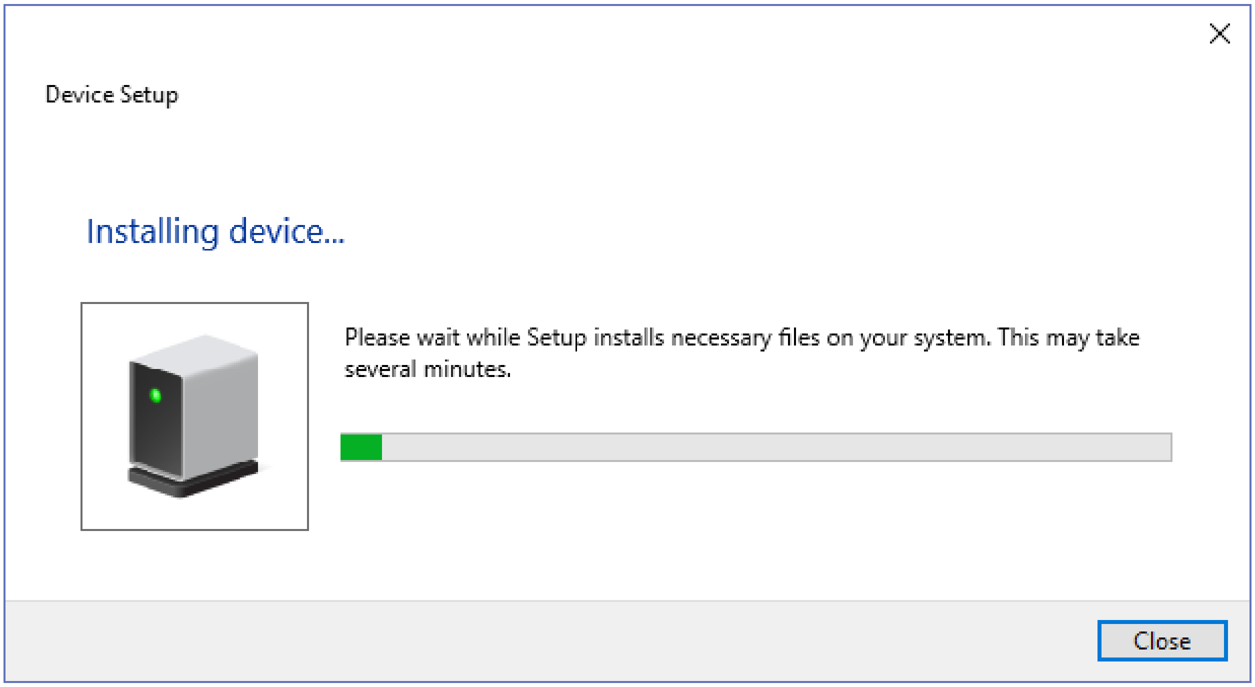
2. Connect USB cable to the PC. Do not attach it to the device.

3. Switch off the device. Hold VolUp button on the device and attach USB cable to the device.

4. Release VolUp button when Download message or LG logo appears on the screen (depends on the device model).

5. Wait several seconds until the device is in a Firmware Update mode. If it is still not in the required mode please repeat the procedure from Step 2.

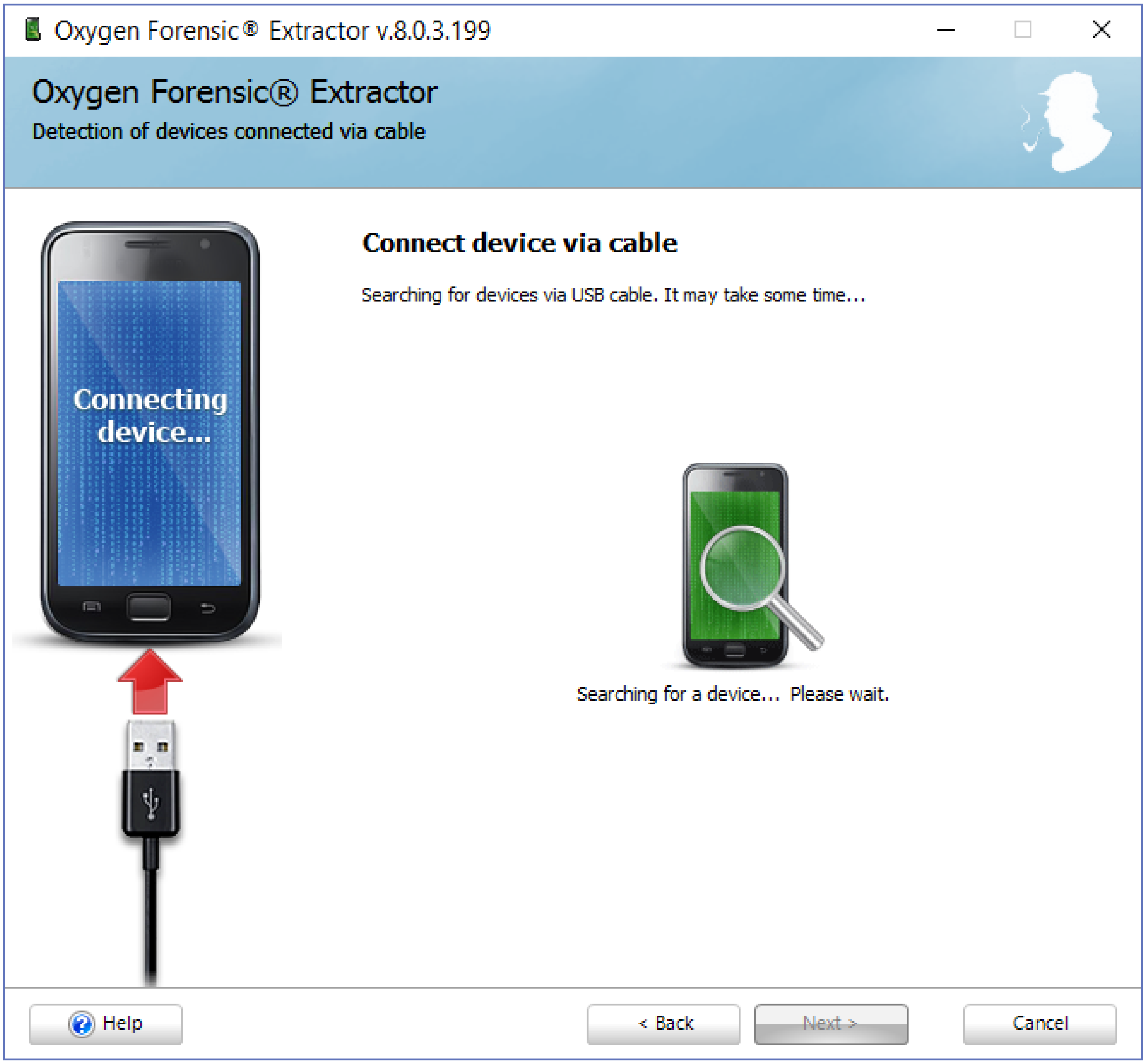
□ Yes, I've followed the instructions.



Device Setup

Installing device...

Please wait while Setup installs necessary files on your system. This may take several minutes.



Oxygen Forensic® Extractor v.8.0.3.199

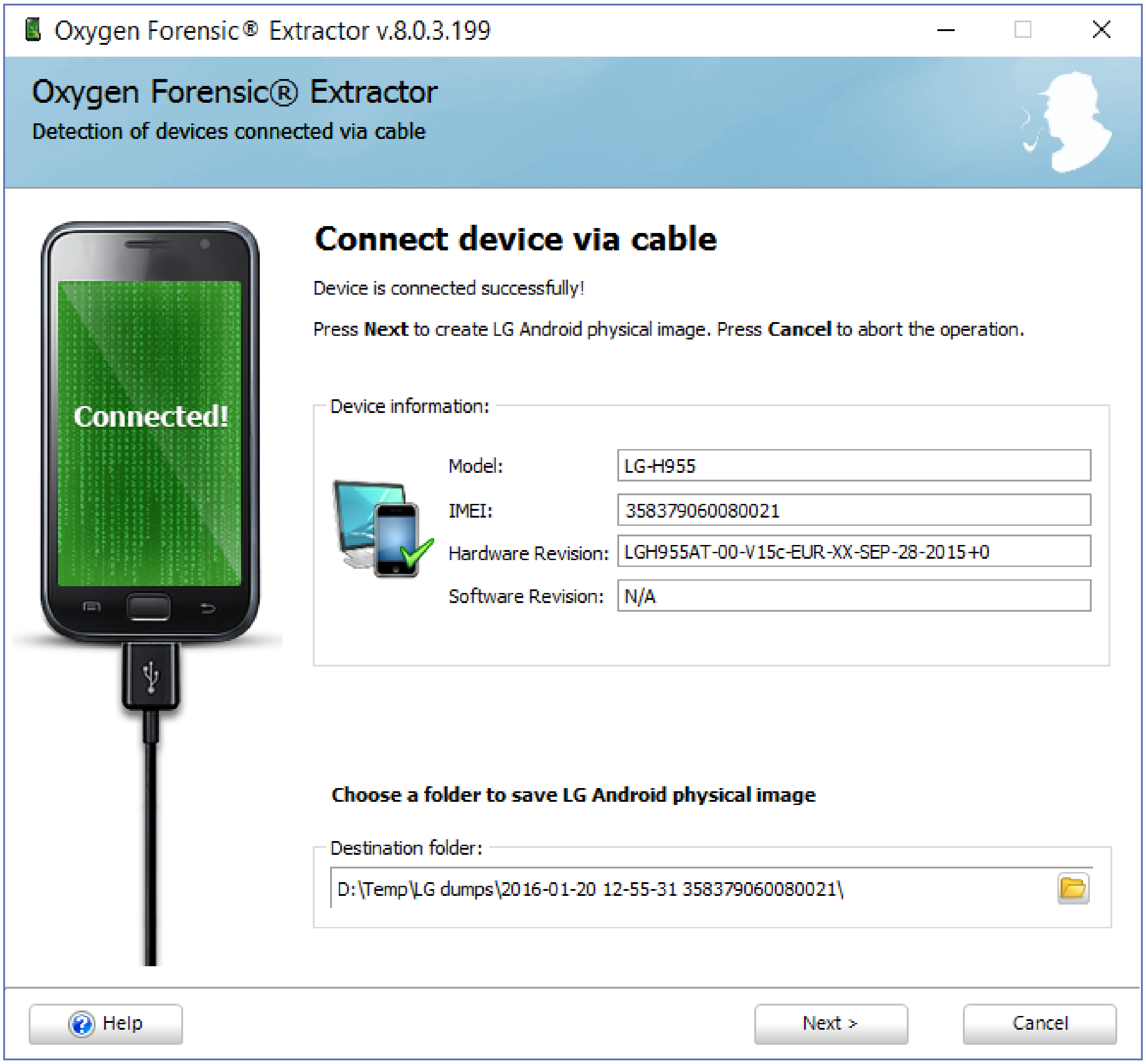
Oxygen Forensic® Extractor

Detection of devices connected via cable

Connect device via cable

Searching for devices via USB cable. It may take some time...

Searching for a device... Please wait.



Oxygen Forensic® Extractor

Detection of devices connected via cable

Connect device via cable

Device is connected successfully!

Press **Next** to create LG Android physical image. Press **Cancel** to abort the operation.

Device information:

Model: LG-H955

IMEI: 358379060080021

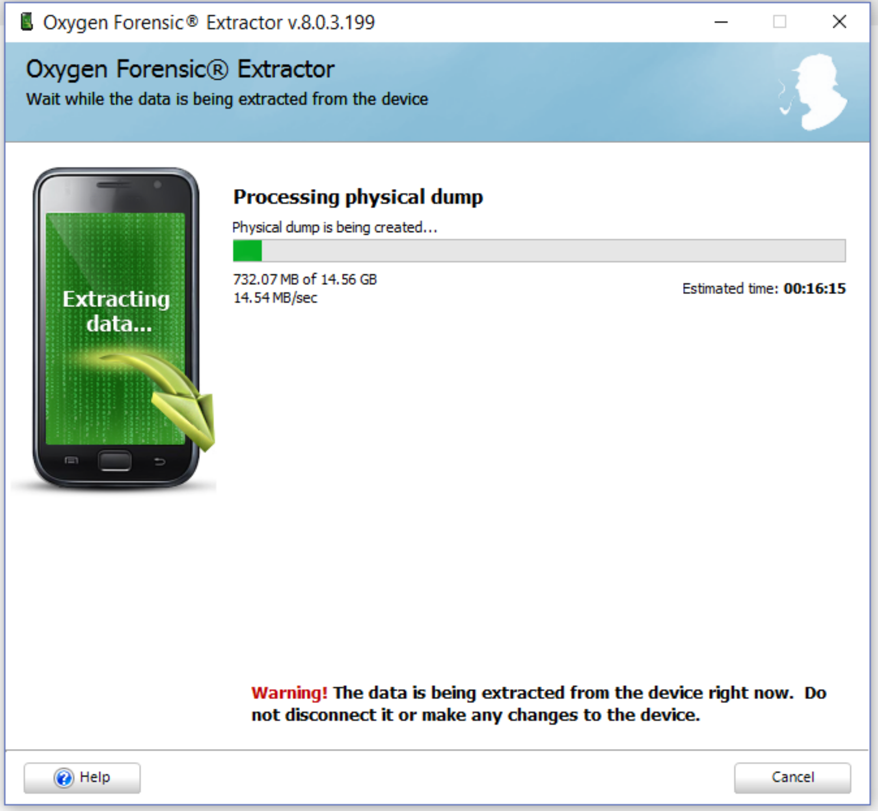
Hardware Revision: LGH955AT-00-V15c-EUR-XX-SEP-28-2015+0

Software Revision: N/A

Choose a folder to save LG Android physical image

Destination folder: D:\Temp\LG dumps\2016-01-20 12-55-31 358379060080021\

Oxygen Forensics



Oxygen Forensic® Extractor v.8.0.3.199

Oxygen Forensic® Extractor

Wait while the data is being extracted from the device

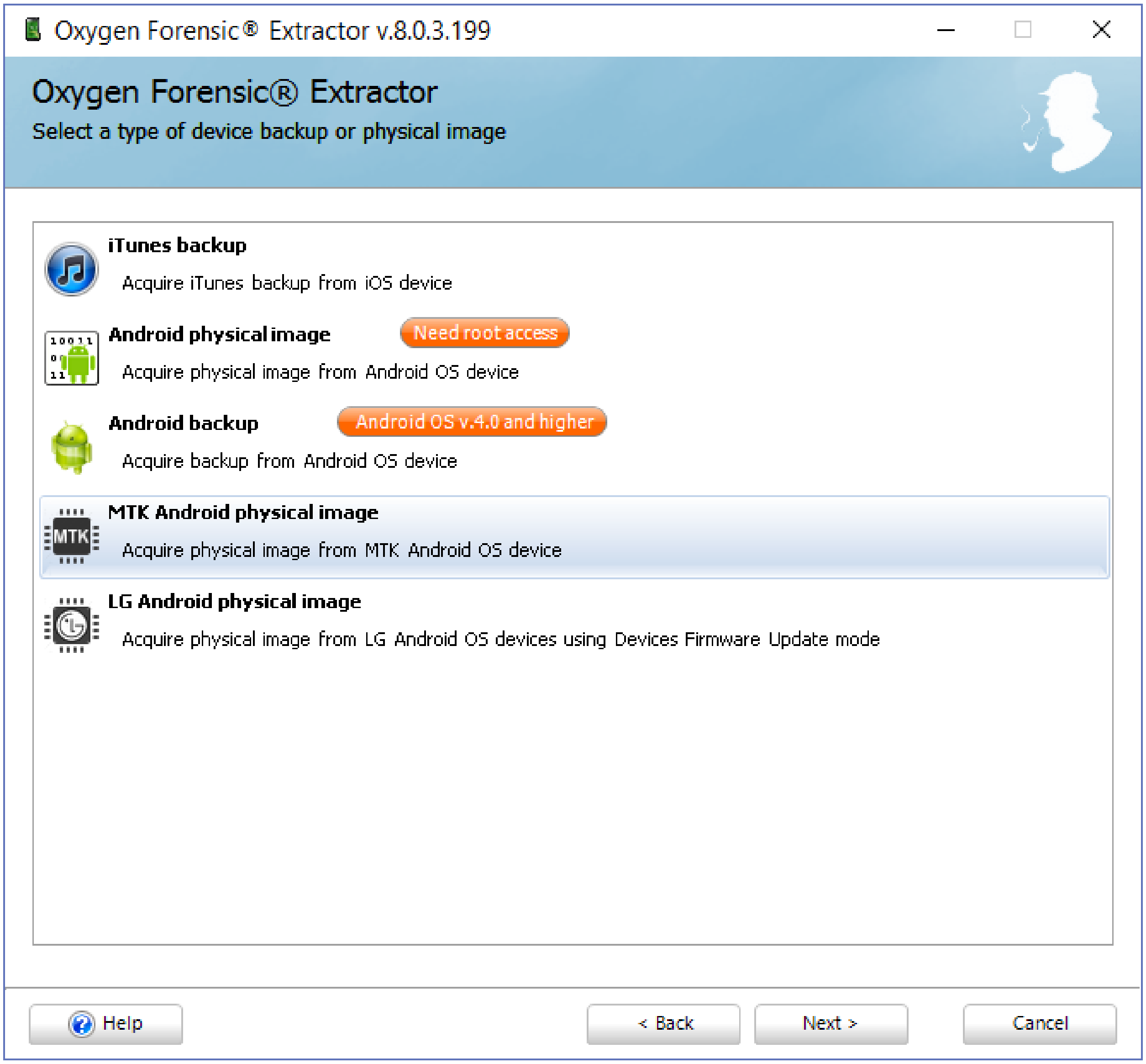
Processing physical dump

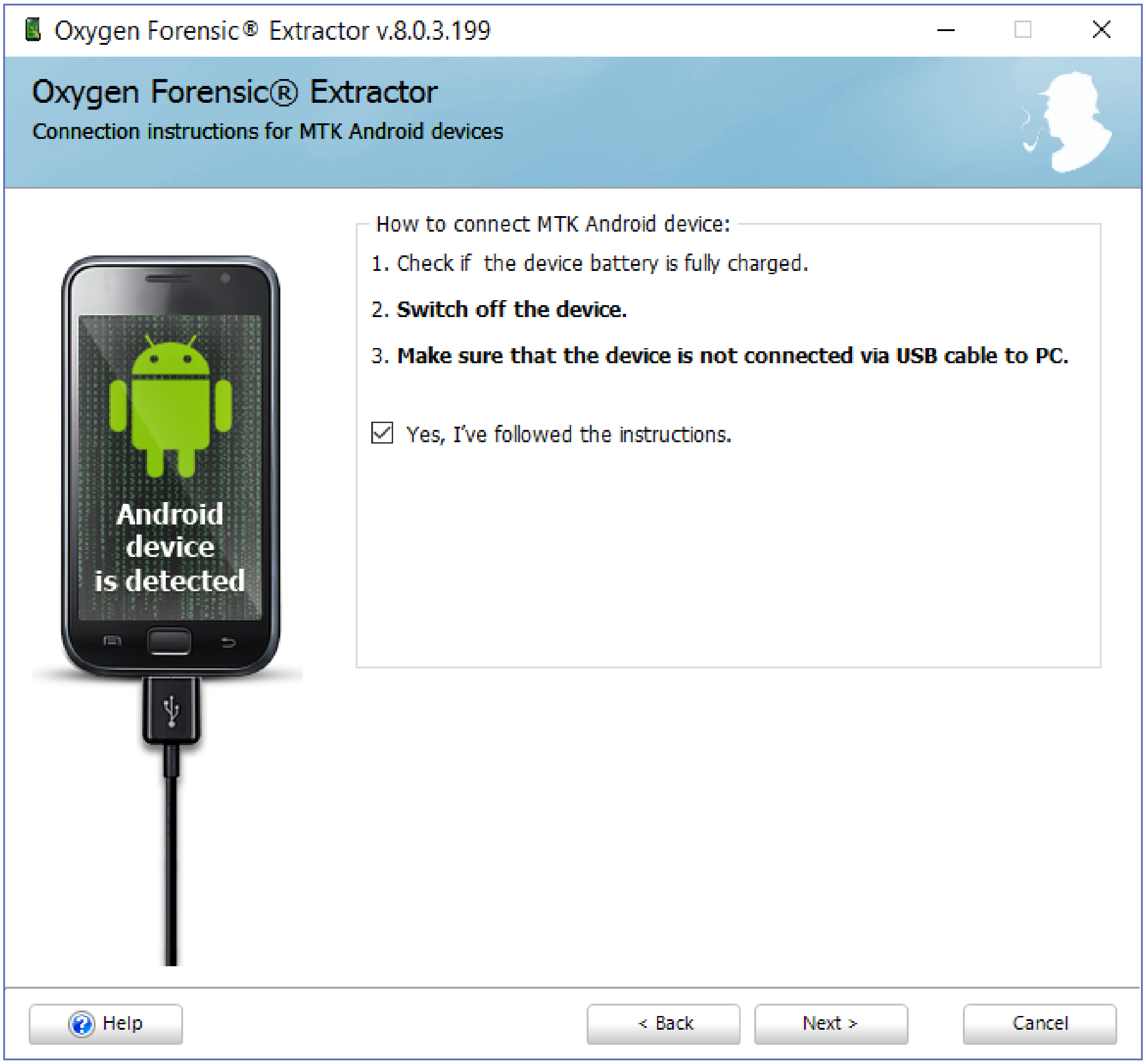
Physical dump is being created...

732.07 MB of 14.56 GB
14.54 MB/sec

Estimated time: **00:16:15**

Warning! The data is being extracted from the device right now. Do not disconnect it or make any changes to the device.





Oxygen Forensic® Extractor v.8.0.3.199

Oxygen Forensic® Extractor

Connection instructions for MTK Android devices

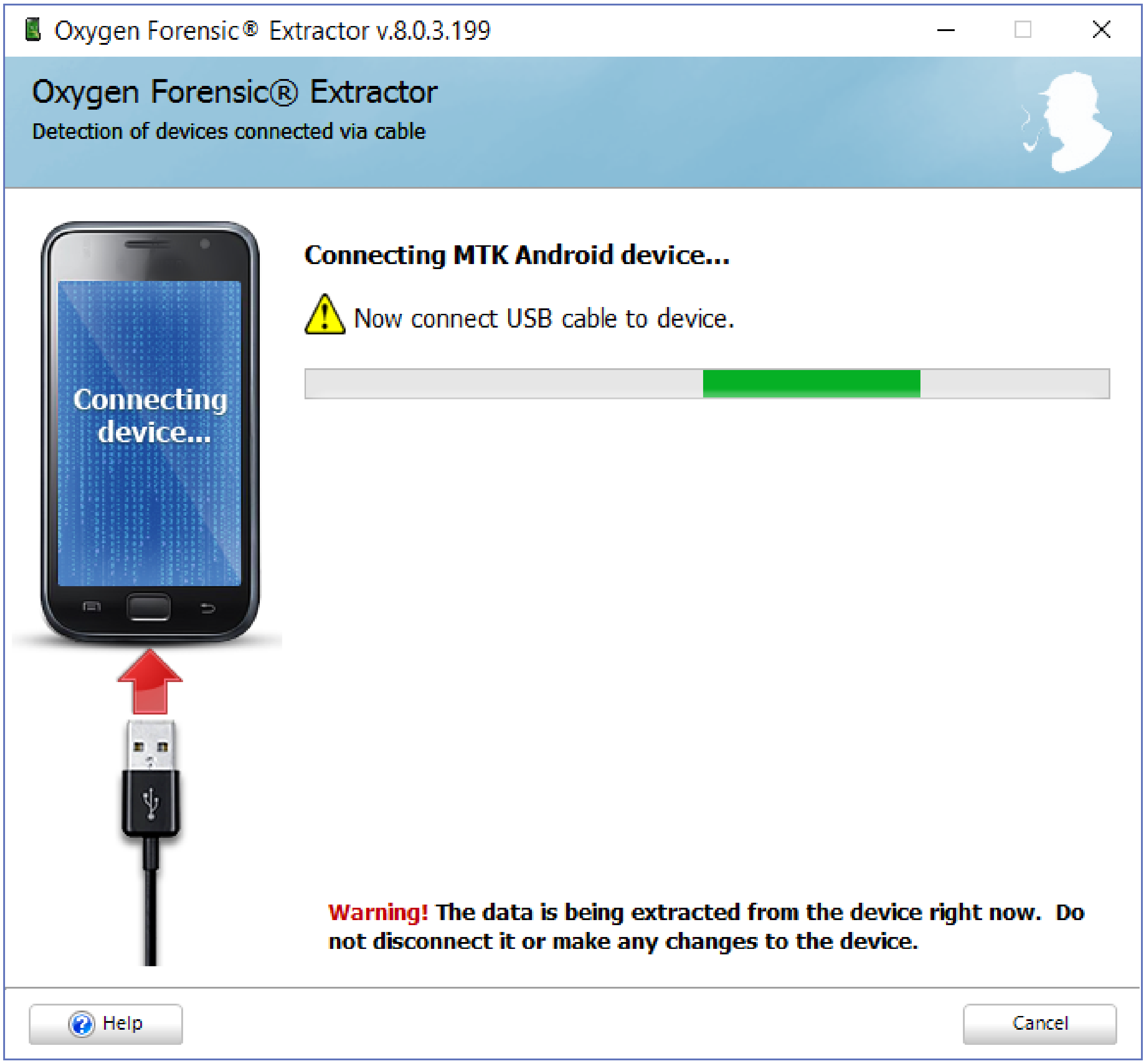
How to connect MTK Android device:

1. Check if the device battery is fully charged.

2. **Switch off the device.**

3. **Make sure that the device is not connected via USB cable to PC.**

☑ Yes, I've followed the instructions.



Oxygen Forensic® Extractor

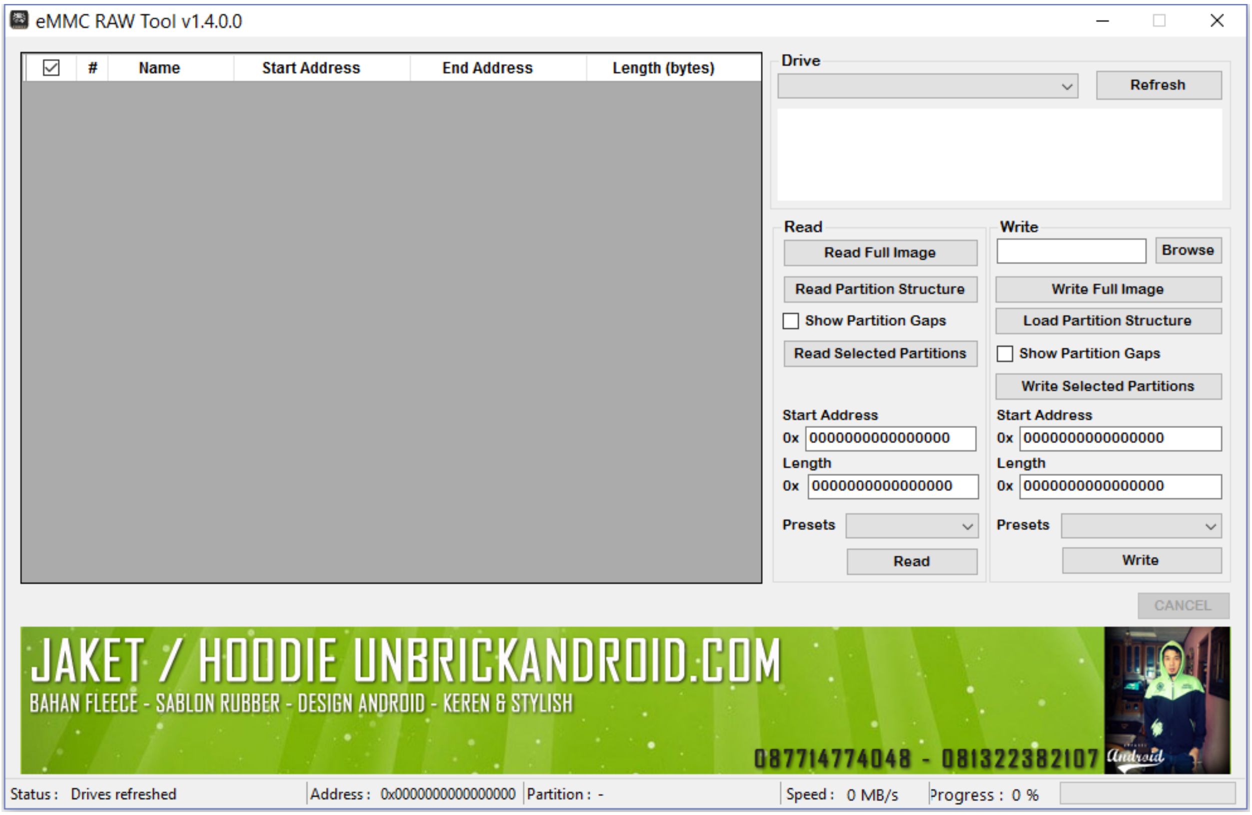
Detection of devices connected via cable

Connecting MTK Android device...

⚠ Now connect USB cable to device.

Warning! The data is being extracted from the device right now. Do not disconnect it or make any changes to the device.

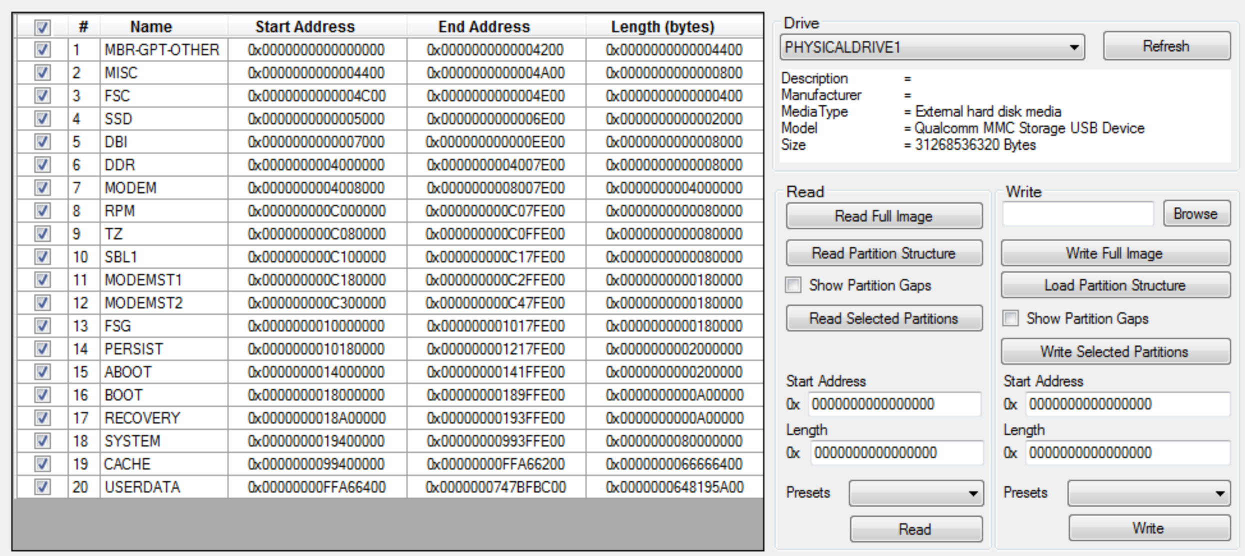
EXCLUSIVE
CELLEBRITE ENHANCES UNIQUE BOOTLOADER METHOD
LOCK BYPASS SOLUTION FOR THE MOBILE DEVICES YOU NEED THE MOST!



Start Address 0x 0000000000000000
Length 0x 0000000000000000

Start Address 0x 0000000000000000
Length 0x 0000000000000000

Status : Drives refreshed | Address : 0x0000000000000000 | Partition : - | Speed : 0 MB/s | Progress : 0 %



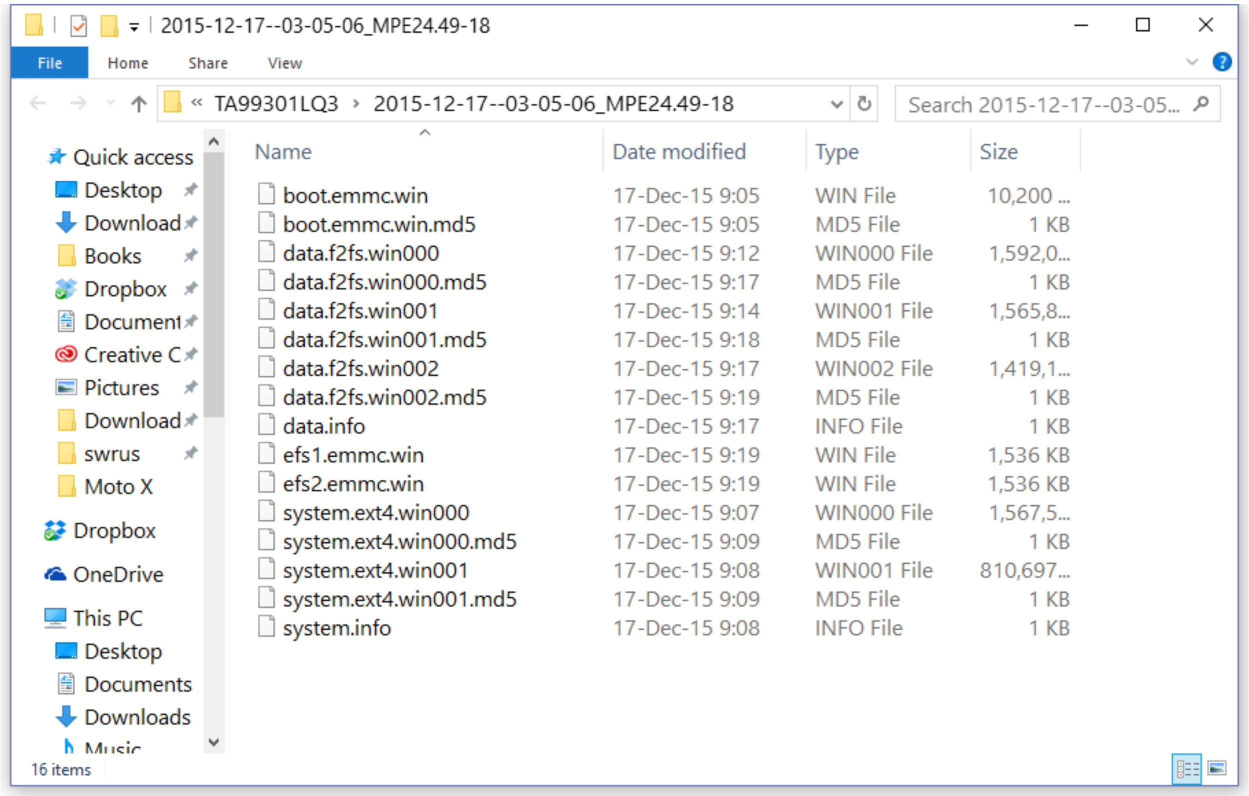
☑	#	Name	Start Address	End Address	Length (bytes)
☑	1	MBR-GPT-OTHER	0x0000000000000000	0x0000000000004200	0x0000000000004400
☑	2	MISC	0x0000000000004400	0x0000000000004A00	0x0000000000000800
☑	3	FSC	0x0000000000004C00	0x0000000000004E00	0x0000000000000400
☑	4	SSD	0x0000000000005000	0x0000000000006E00	0x0000000000002000
☑	5	DBI	0x0000000000007000	0x000000000000EE00	0x0000000000008000
☑	6	DDR	0x0000000004000000	0x0000000004007E00	0x0000000000008000
☑	7	MODEM	0x0000000004008000	0x0000000008007E00	0x0000000004000000
☑	8	RPM	0x000000000C000000	0x000000000C07FE00	0x0000000000080000
☑	9	TZ	0x000000000C080000	0x000000000C0FFE00	0x0000000000080000
☑	10	SBL1	0x000000000C100000	0x000000000C17FE00	0x0000000000080000
☑	11	MODEMST1	0x000000000C180000	0x000000000C2FFE00	0x0000000000180000
☑	12	MODEMST2	0x000000000C300000	0x000000000C47FE00	0x0000000000180000
☑	13	FSG	0x0000000010000000	0x000000001017FE00	0x0000000000180000
☑	14	PERSIST	0x0000000010180000	0x000000001217FE00	0x0000000002000000
☑	15	ABOOT	0x0000000014000000	0x00000000141FFE00	0x0000000000200000
☑	16	BOOT	0x0000000018000000	0x00000000189FFE00	0x0000000000A00000
☑	17	RECOVERY	0x0000000018A00000	0x00000000193FFE00	0x0000000000A00000
☑	18	SYSTEM	0x0000000019400000	0x00000000993FFE00	0x0000000080000000
☑	19	CACHE	0x0000000099400000	0x00000000FFA66200	0x0000000066666400
☑	20	USERDATA	0x00000000FFA66400	0x0000000747BFBC00	0x0000000648195A00

Drive: PHYSICALDRIVE1

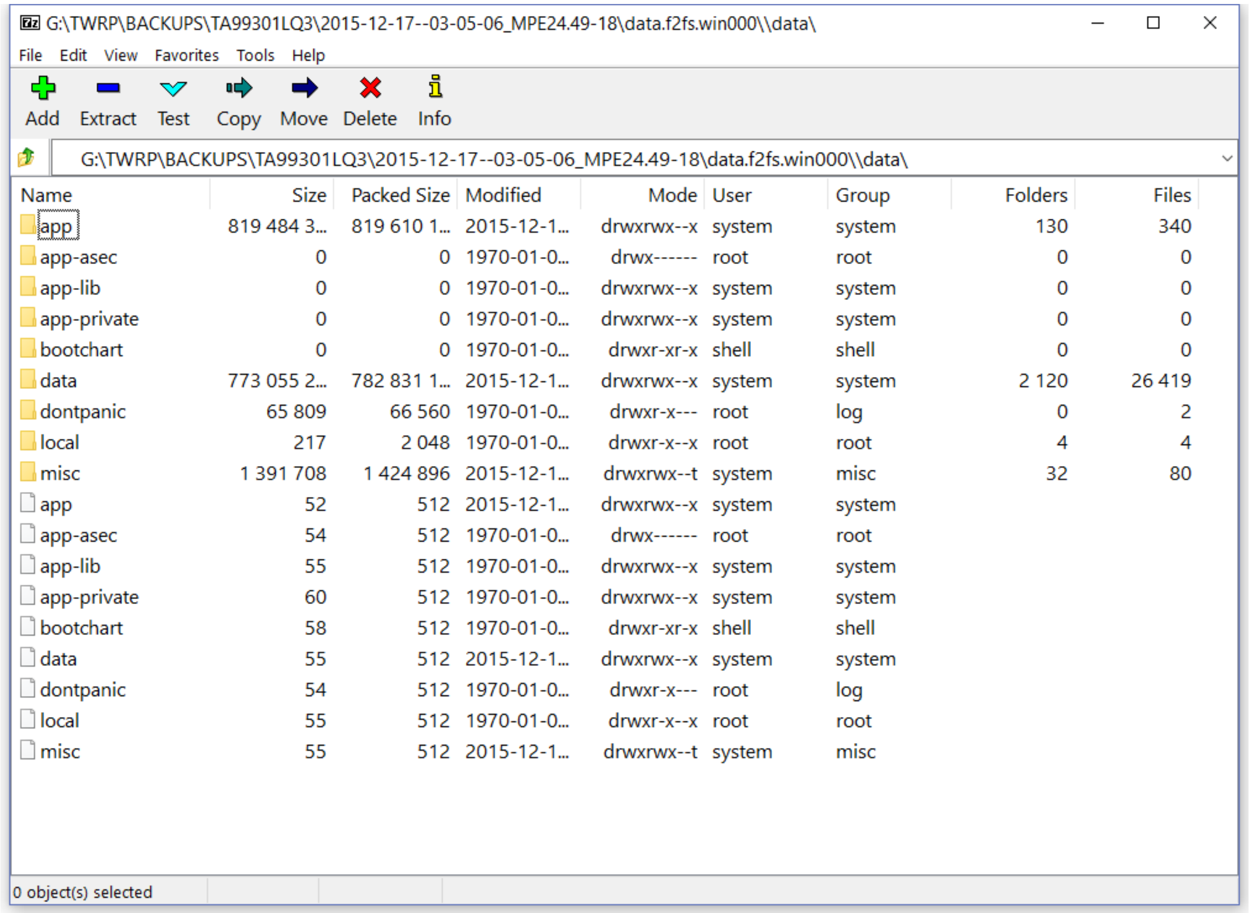
```
Description   =
Manufacturer  =
Media Type    = External hard disk media
Model         = Qualcomm MMC Storage USB Device
Size          = 31268536320 Bytes
```

Start Address 0x 0000000000000000
Length 0x 0000000000000000

Start Address 0x 0000000000000000
Length 0x 0000000000000000



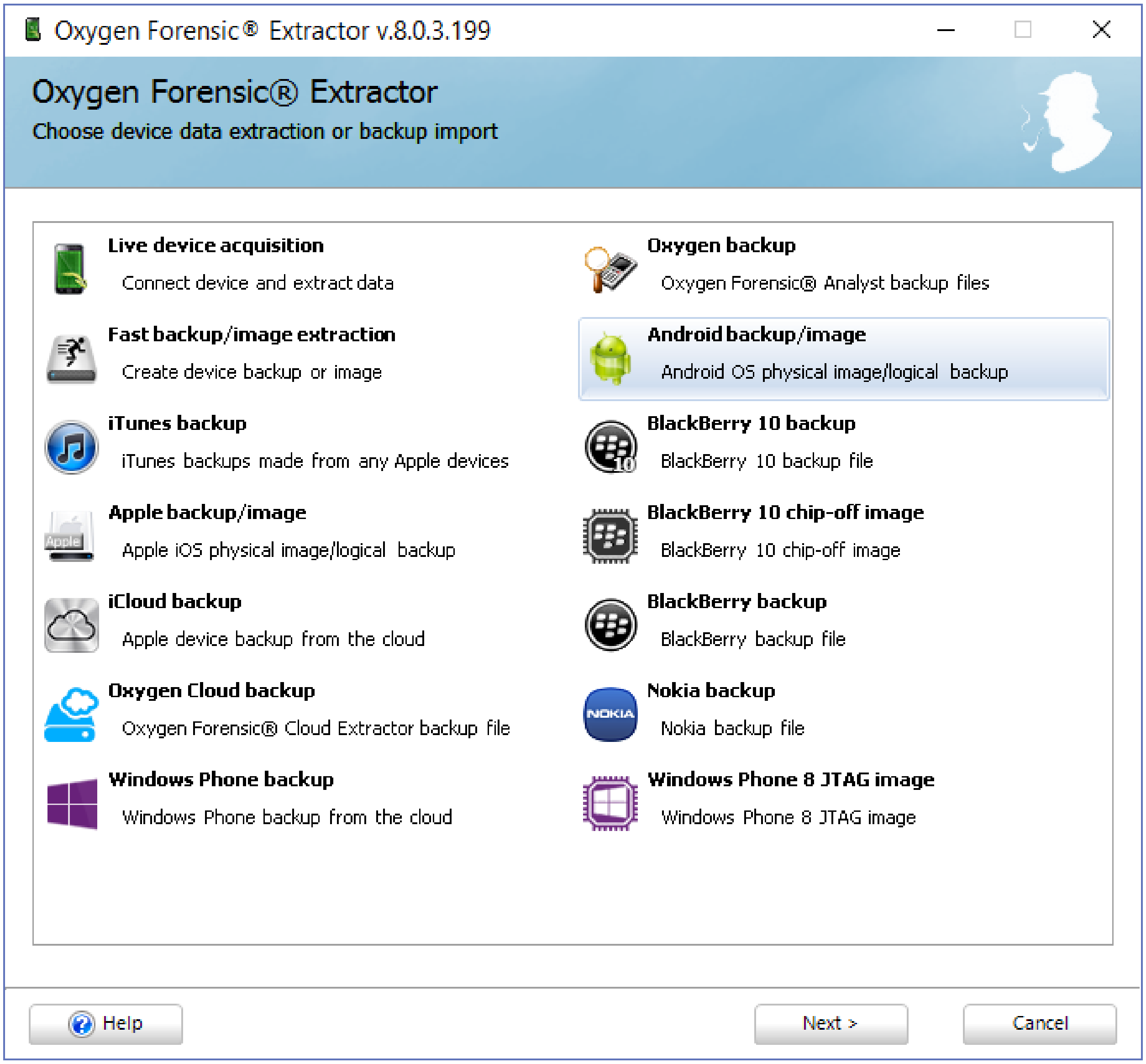
Name	Date modified	Type	Size
boot.emmc.win	17-Dec-15 9:05	WIN File	10,200 ...
boot.emmc.win.md5	17-Dec-15 9:05	MD5 File	1 KB
data.f2fs.win000	17-Dec-15 9:12	WIN000 File	1,592,0...
data.f2fs.win000.md5	17-Dec-15 9:17	MD5 File	1 KB
data.f2fs.win001	17-Dec-15 9:14	WIN001 File	1,565,8...
data.f2fs.win001.md5	17-Dec-15 9:18	MD5 File	1 KB
data.f2fs.win002	17-Dec-15 9:17	WIN002 File	1,419,1...
data.f2fs.win002.md5	17-Dec-15 9:19	MD5 File	1 KB
data.info	17-Dec-15 9:17	INFO File	1 KB
efs1.emmc.win	17-Dec-15 9:19	WIN File	1,536 KB
efs2.emmc.win	17-Dec-15 9:19	WIN File	1,536 KB
system.ext4.win000	17-Dec-15 9:07	WIN000 File	1,567,5...
system.ext4.win000.md5	17-Dec-15 9:09	MD5 File	1 KB
system.ext4.win001	17-Dec-15 9:08	WIN001 File	810,697...
system.ext4.win001.md5	17-Dec-15 9:09	MD5 File	1 KB
system.info	17-Dec-15 9:08	INFO File	1 KB



G:\TWRP\BACKUPS\TA99301LQ3\2015-12-17--03-05-06_MPE24.49-18\data.f2fs.win000\\data\

G:\TWRP\BACKUPS\TA99301LQ3\2015-12-17--03-05-06_MPE24.49-18\data.f2fs.win000\\data\

Name	Size	Packed Size	Modified	Mode	User	Group	Folders	Files
app	819 484 3...	819 610 1...	2015-12-1...	drwxrwx--x	system	system	130	340
app-asec	0	0	1970-01-0...	drwx------	root	root	0	0
app-lib	0	0	1970-01-0...	drwxrwx--x	system	system	0	0
app-private	0	0	1970-01-0...	drwxrwx--x	system	system	0	0
bootchart	0	0	1970-01-0...	drwxr-xr-x	shell	shell	0	0
data	773 055 2...	782 831 1...	2015-12-1...	drwxrwx--x	system	system	2 120	26 419
dontpanic	65 809	66 560	1970-01-0...	drwxr-x---	root	log	0	2
local	217	2 048	1970-01-0...	drwxr-x--x	root	root	4	4
misc	1 391 708	1 424 896	2015-12-1...	drwxrwx--t	system	misc	32	80
app	52	512	2015-12-1...	drwxrwx--x	system	system		
app-asec	54	512	1970-01-0...	drwx------	root	root		
app-lib	55	512	1970-01-0...	drwxrwx--x	system	system		
app-private	60	512	1970-01-0...	drwxrwx--x	system	system		
bootchart	58	512	1970-01-0...	drwxr-xr-x	shell	shell		
data	55	512	2015-12-1...	drwxrwx--x	system	system		
dontpanic	54	512	1970-01-0...	drwxr-x---	root	log		
local	55	512	1970-01-0...	drwxr-x--x	root	root		
misc	55	512	2015-12-1...	drwxrwx--t	system	misc		



Oxygen Forensic® Extractor v.8.0.3.199

Oxygen Forensic® Extractor

Choose device data extraction or backup import

Live device acquisition
Connect device and extract data

Oxygen backup
Oxygen Forensic® Analyst backup files

Fast backup/image extraction
Create device backup or image

Android backup/image
Android OS physical image/logical backup

iTunes backup
iTunes backups made from any Apple devices

BlackBerry 10 backup
BlackBerry 10 backup file

Apple backup/image
Apple iOS physical image/logical backup

BlackBerry 10 chip-off image
BlackBerry 10 chip-off image

iCloud backup
Apple device backup from the cloud

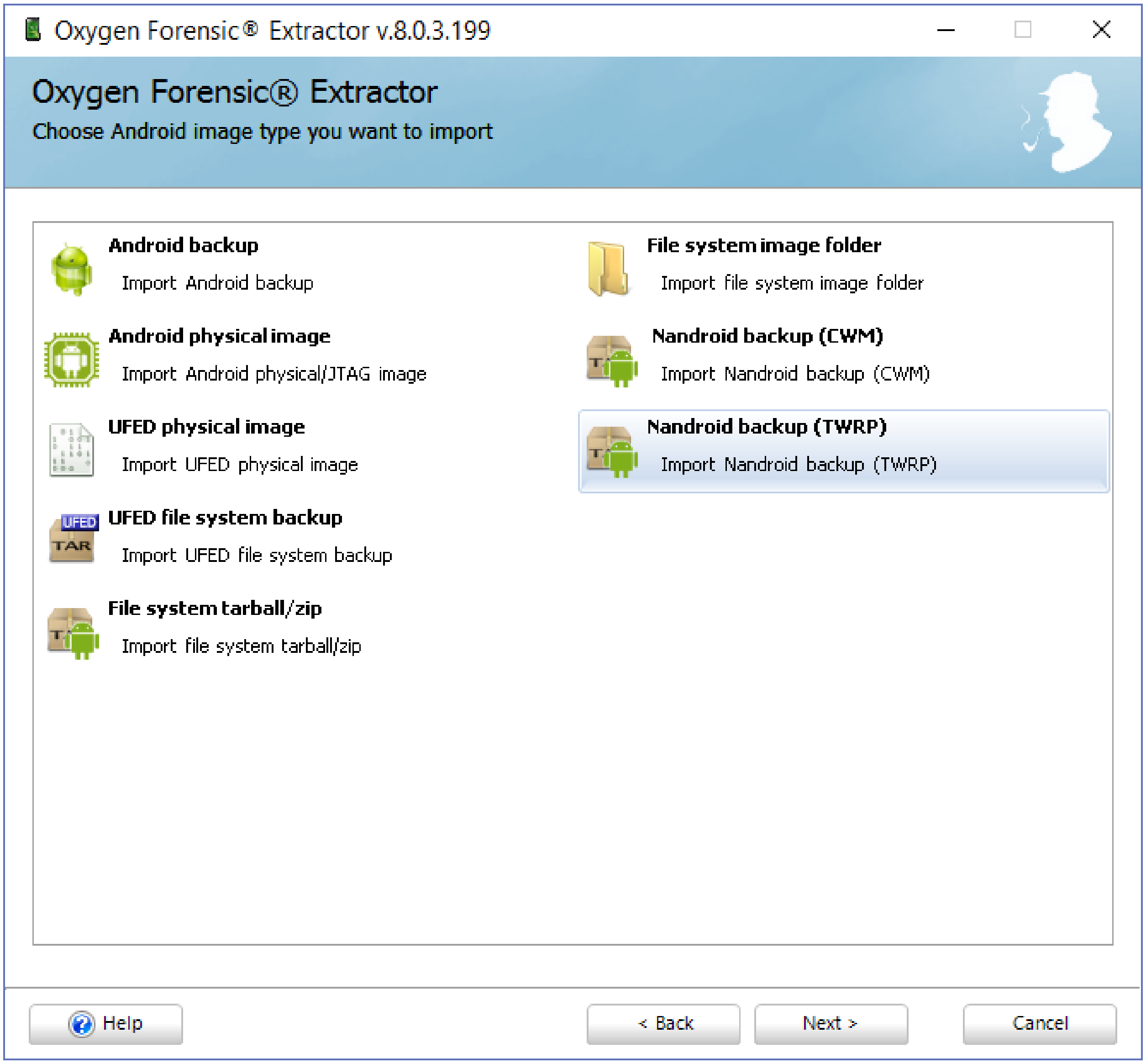
BlackBerry backup
BlackBerry backup file

Oxygen Cloud backup
Oxygen Forensic® Cloud Extractor backup file

Nokia backup
Nokia backup file

Windows Phone backup
Windows Phone backup from the cloud

Windows Phone 8 JTAG image
Windows Phone 8 JTAG image



Oxygen Forensic® Extractor v.8.0.3.199

Oxygen Forensic® Extractor

Choose Android image type you want to import

Android backup
Import Android backup

Android physical image
Import Android physical/JTAG image

UFED physical image
Import UFED physical image

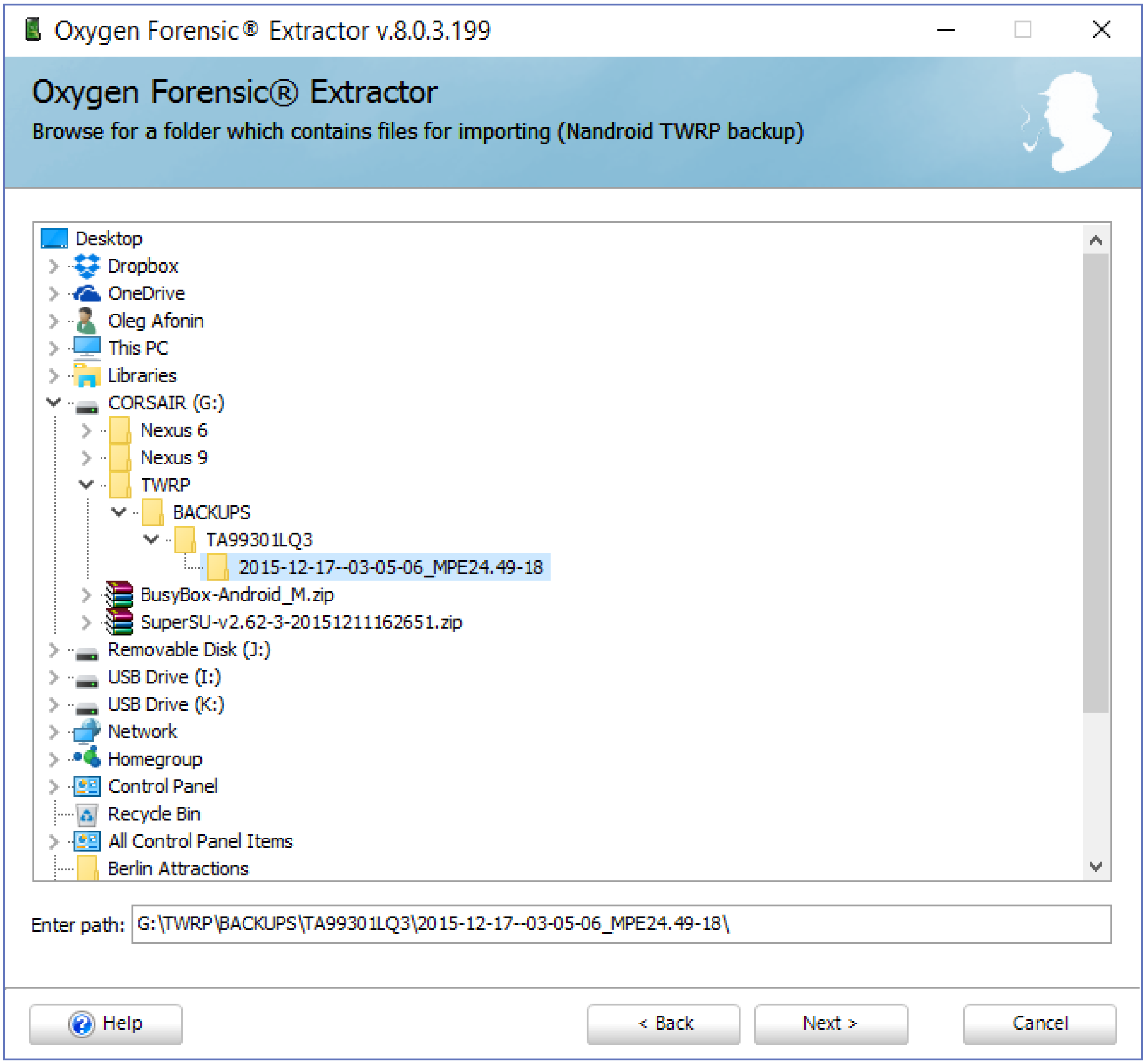
UFED file system backup
Import UFED file system backup

File system tarball/zip
Import file system tarball/zip

File system image folder
Import file system image folder

Nandroid backup (CWM)
Import Nandroid backup (CWM)

Nandroid backup (TWRP)
Import Nandroid backup (TWRP)

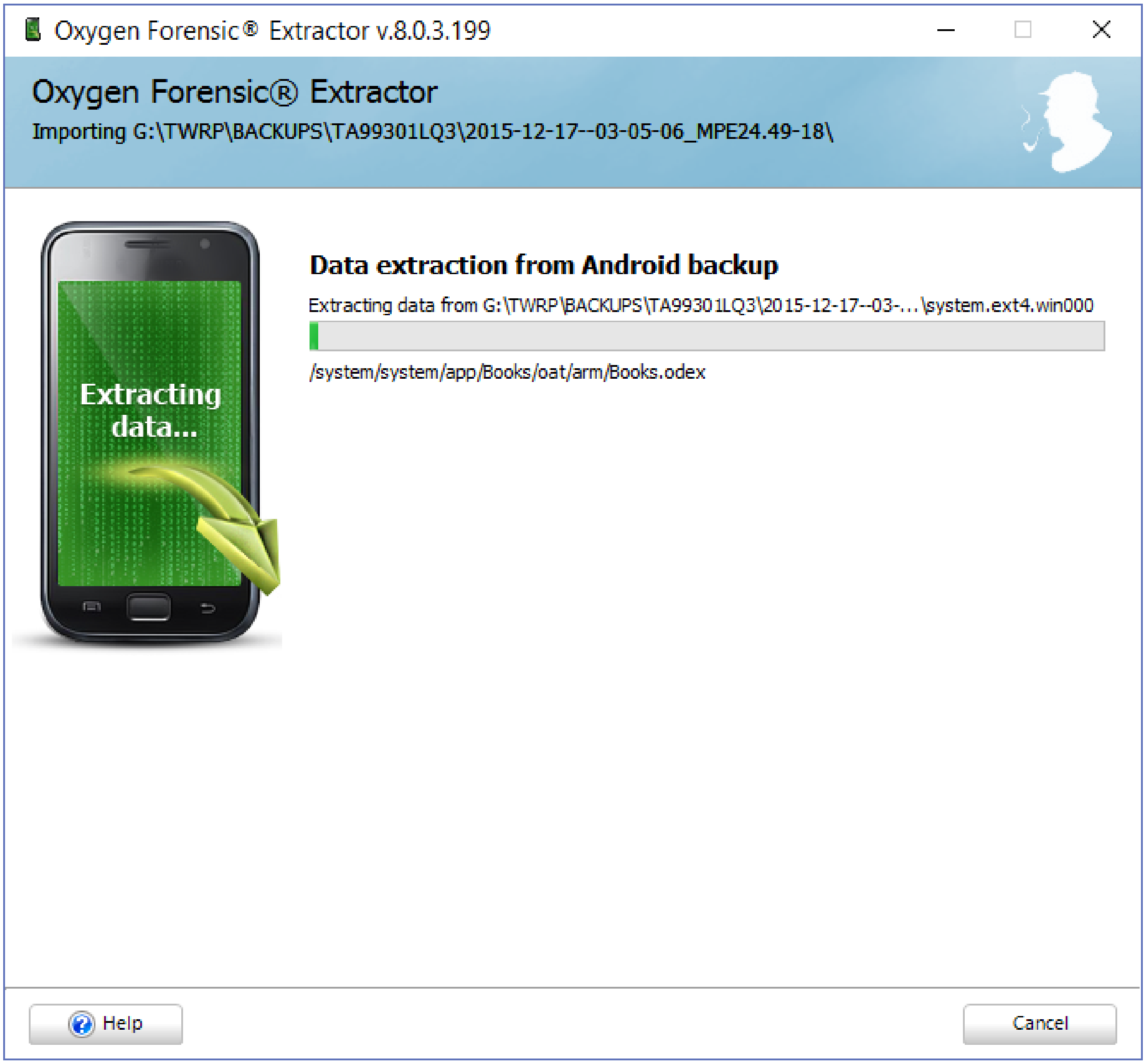


Oxygen Forensic® Extractor v.8.0.3.199

Oxygen Forensic® Extractor

Browse for a folder which contains files for importing (Nandroid TWRP backup)

Enter path: G:\TWRP\BACKUPS\TA99301LQ3\2015-12-17--03-05-06_MPE24.49-18\



Oxygen Forensic® Extractor v.8.0.3.199

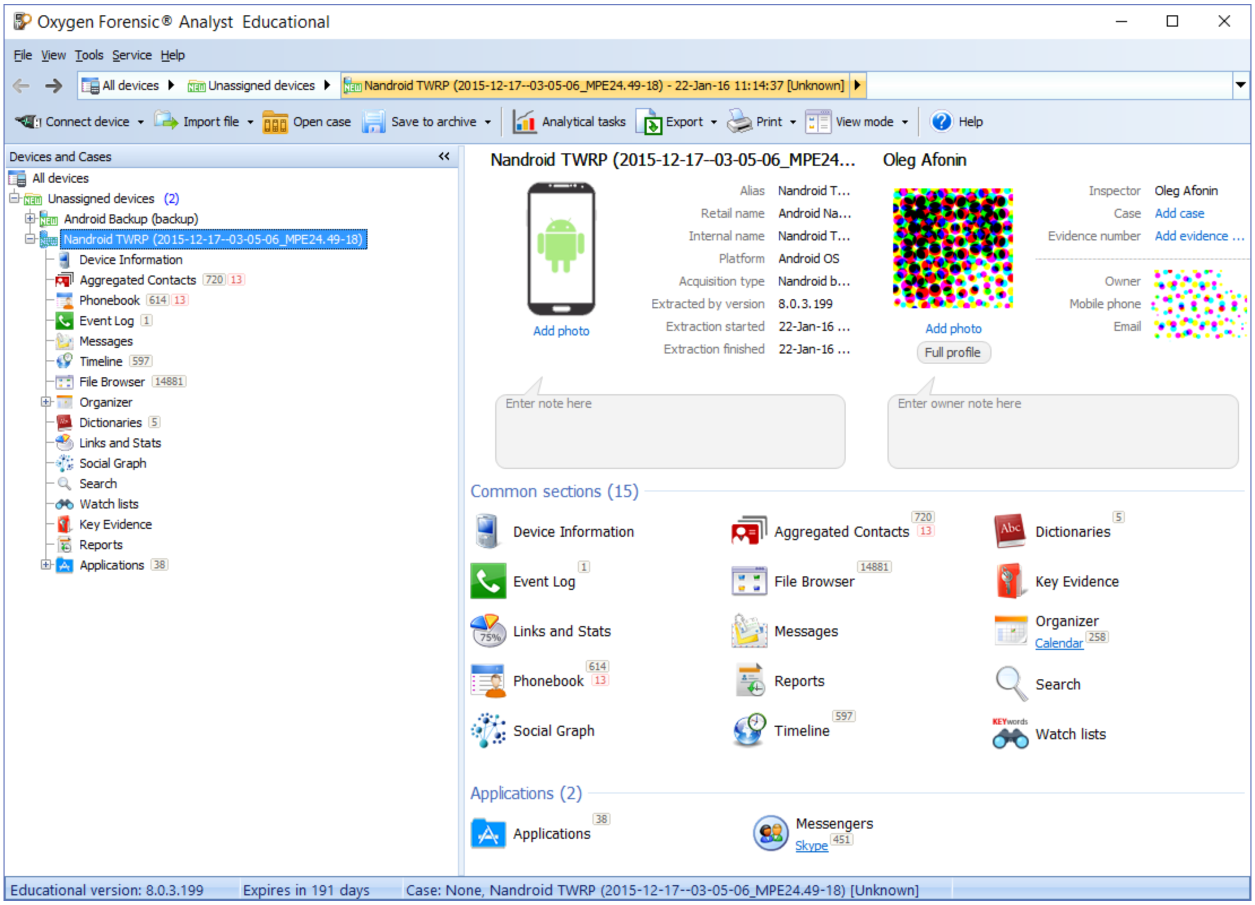
Oxygen Forensic® Extractor

Importing G:\TWRP\BACKUPS\TA99301LQ3\2015-12-17--03-05-06_MPE24.49-18\

Data extraction from Android backup

Extracting data from G:\TWRP\BACKUPS\TA99301LQ3\2015-12-17--03-...\system.ext4.win000

/system/system/app/Books/oat/arm/Books.odex


Oxygen Forensic® Analyst Educational
File View Tools Service Help
All devices
Unassigned devices
Nandroid TWRP (2015-12-17--03-05-06_MPE24.49-18) - 22-Jan-16 11:14:37 [Unknown]
Connect device
Import file
Open case
Save to archive
Analytical tasks
Export
Print
View mode
Help
Devices and Cases

All devices
Unassigned devices (2)
Android Backup (backup)
Nandroid TWRP (2015-12-17--03-05-06_MPE24.49-18)
Device Information
Aggregated Contacts 720 13
Phonebook 614 13
Event Log 1
Messages
Timeline 597
File Browser 14881
Organizer
Dictionaries 5
Links and Stats
Social Graph
Search
Watch lists
Key Evidence
Reports
Applications 38

Nandroid TWRP (2015-12-17--03-05-06_MPE24...

Alias	Nandroid T...
Retail name	Android Na...
Internal name	Nandroid T...
Platform	Android OS
Acquisition type	Nandroid b...
Extracted by version	8.0.3.199
Extraction started	22-Jan-16 ...
Extraction finished	22-Jan-16 ...

Oleg Afonin

Inspector	Oleg Afonin
Case	Add case
Evidence number	Add evidence ...
Owner	
Mobile phone	
Email	

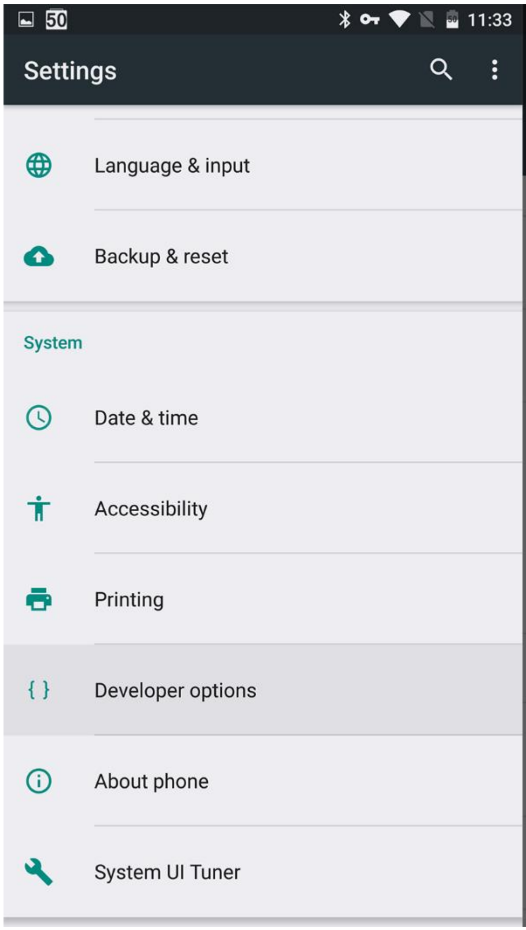
Common sections (15)

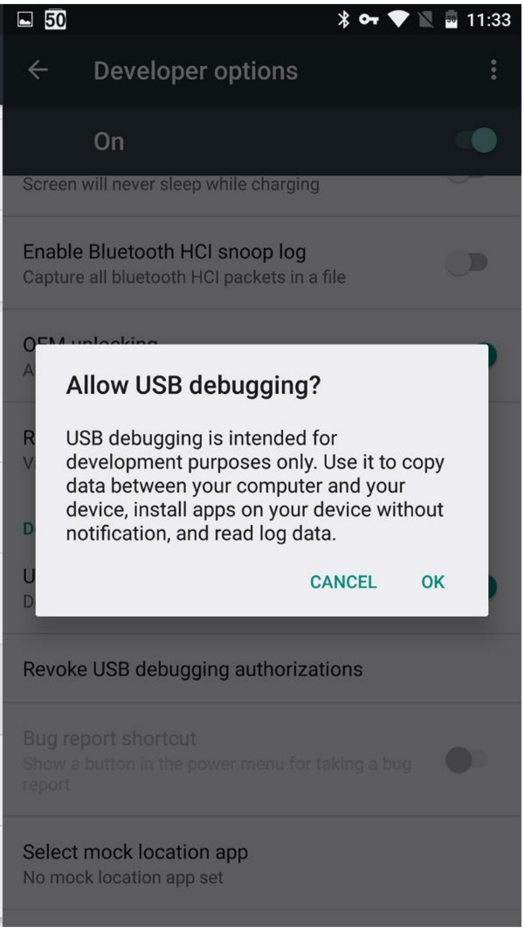
Device Information
Aggregated Contacts 720 13
Dictionaries 5
Event Log 1
File Browser 14881
Key Evidence
Links and Stats
Messages
Organizer
Calendar 258
Phonebook 614 13
Reports
Search
Social Graph
Timeline 597
Watch lists

Applications (2)

Applications 38
Messengers
Skype 451

Educational version: 8.0.3.199 Expires in 191 days Case: None, Nandroid TWRP (2015-12-17--03-05-06_MPE24.49-18) [Unknown]

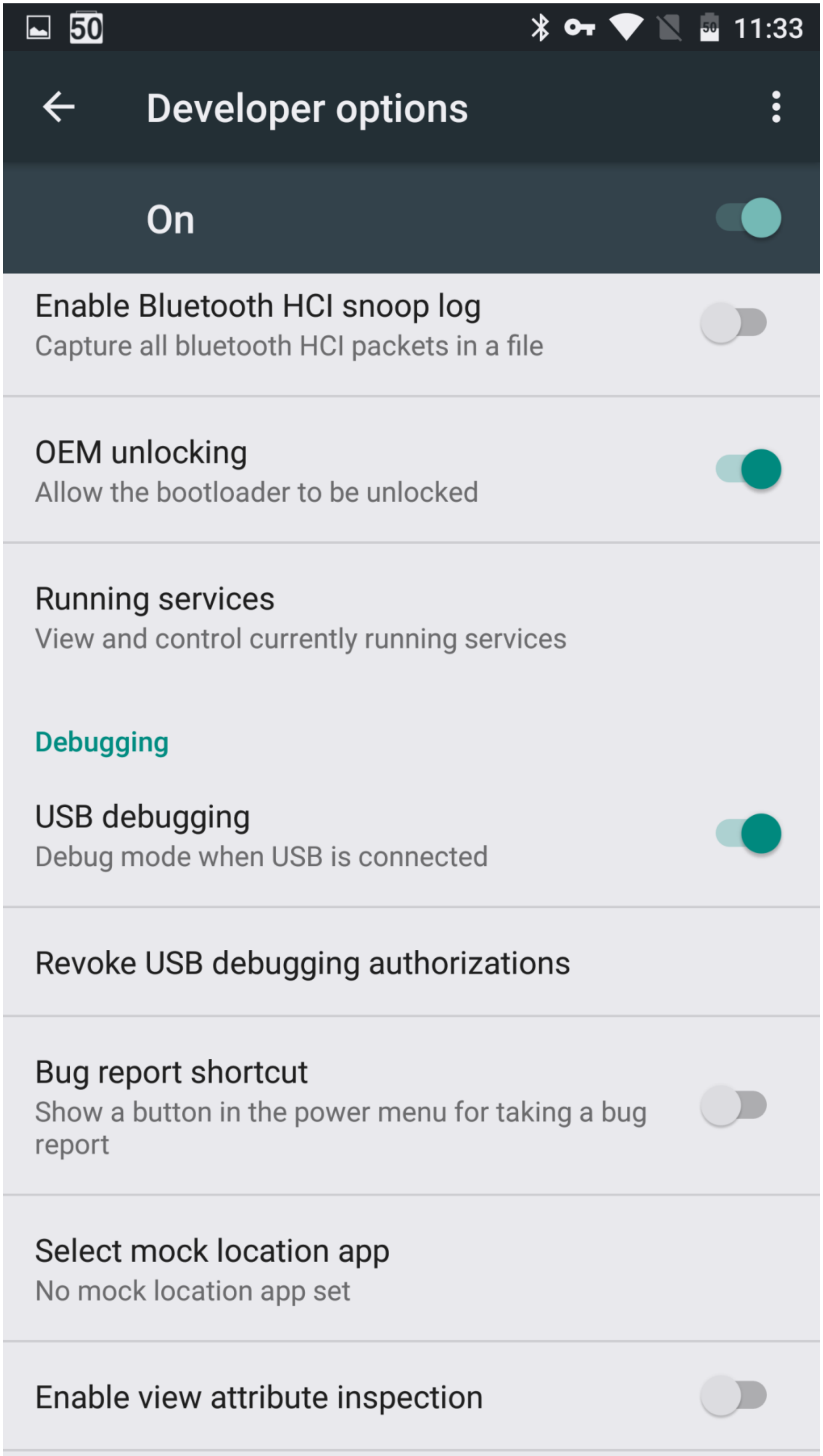



11:33
Developer options
On
Screen will never sleep while charging
Enable Bluetooth HCI snoop log
Capture all bluetooth HCI packets in a file
OEM unlocking
Revoke USB debugging authorizations
Bug report shortcut
Show a button in the power menu for taking a bug report
Select mock location app
No mock location app set

Allow USB debugging?

USB debugging is intended for development purposes only. Use it to copy data between your computer and your device, install apps on your device without notification, and read log data.

CANCEL OK



Developer options

On ●

Enable Bluetooth HCI snoop log ○
Capture all bluetooth HCI packets in a file

OEM unlocking ●
Allow the bootloader to be unlocked

Running services
View and control currently running services

Debugging

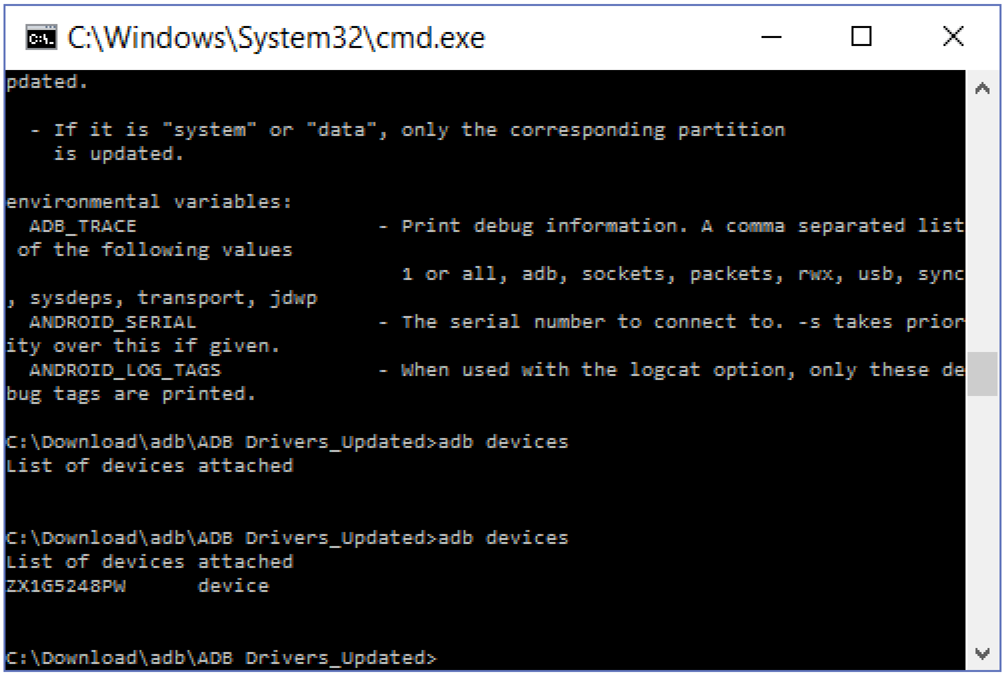
USB debugging ●
Debug mode when USB is connected

Revoke USB debugging authorizations

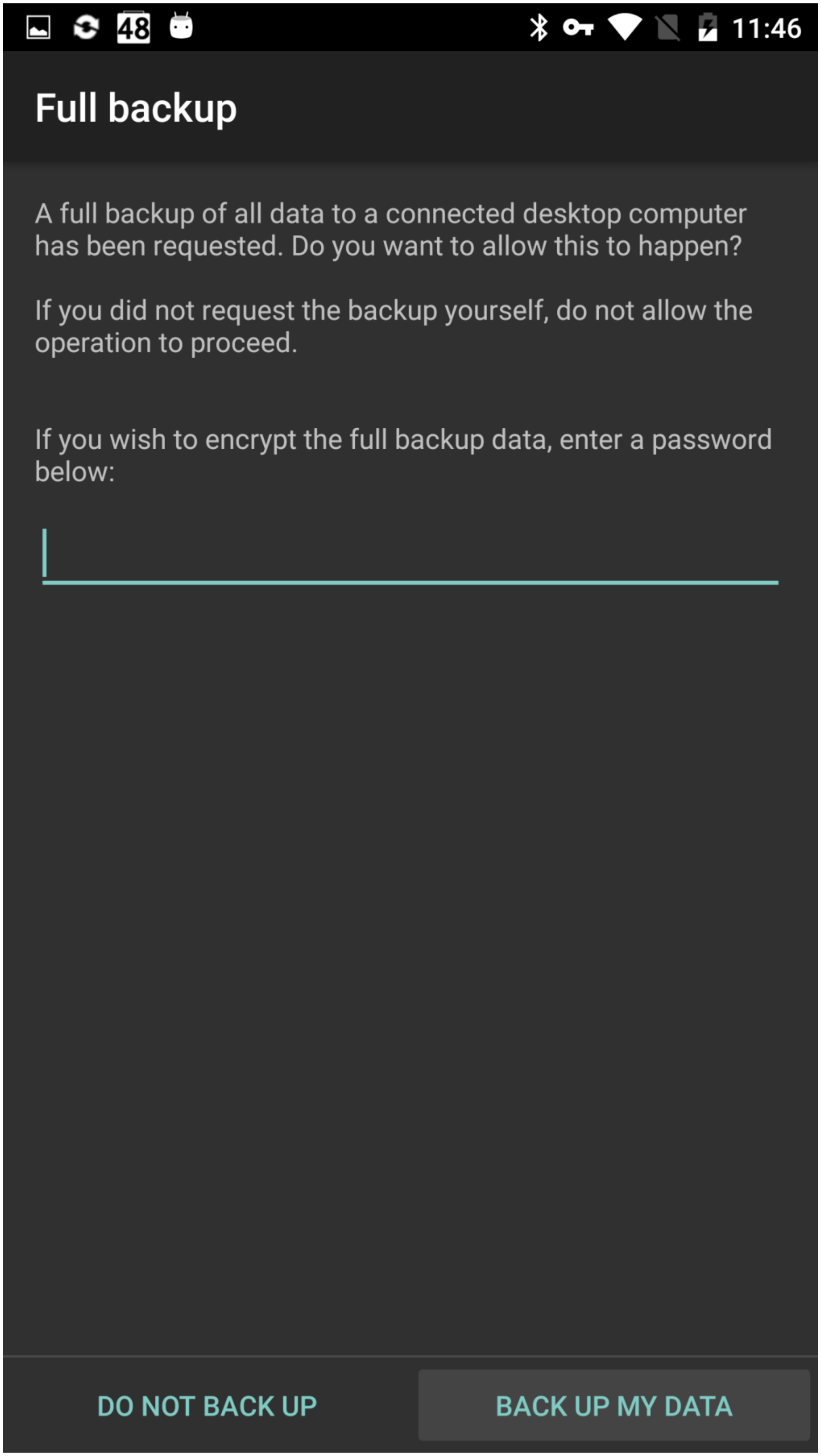
Bug report shortcut ○
Show a button in the power menu for taking a bug report

Select mock location app
No mock location app set

Enable view attribute inspection ○



```
pdated.

  - If it is "system" or "data", only the corresponding partition
    is updated.

environmental variables:
  ADB_TRACE                      - Print debug information. A comma separated list
 of the following values
                                   1 or all, adb, sockets, packets, rwx, usb, sync
, sysdeps, transport, jdwp
  ANDROID_SERIAL                 - The serial number to connect to. -s takes prior
ity over this if given.
  ANDROID_LOG_TAGS               - When used with the logcat option, only these de
bug tags are printed.

C:\Download\adb\ADB Drivers_Updated>adb devices
List of devices attached


C:\Download\adb\ADB Drivers_Updated>adb devices
List of devices attached
ZX1G5248PW      device


C:\Download\adb\ADB Drivers_Updated>
```

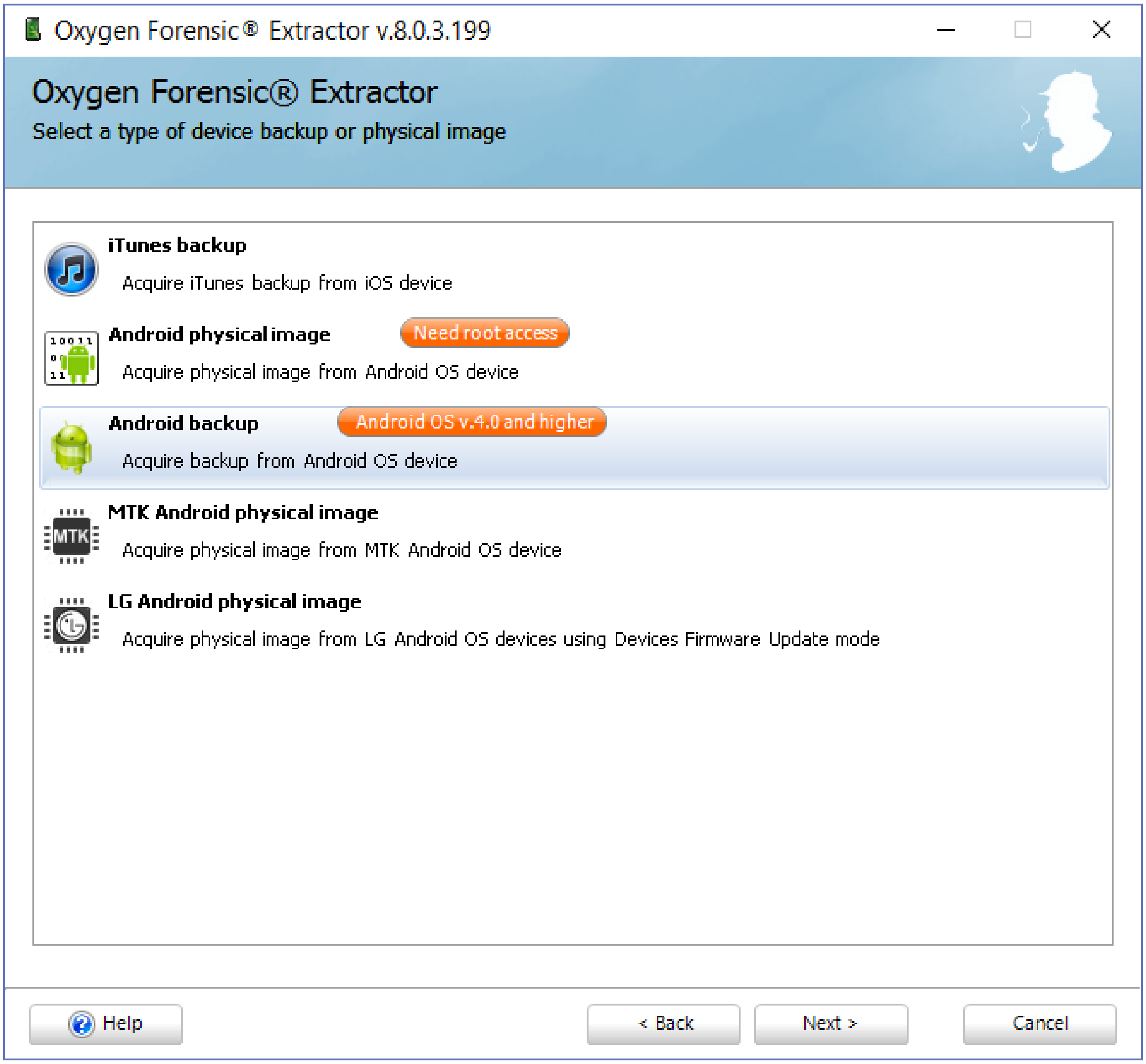


Full backup

A full backup of all data to a connected desktop computer has been requested. Do you want to allow this to happen?

If you did not request the backup yourself, do not allow the operation to proceed.

If you wish to encrypt the full backup data, enter a password below:



Oxygen Forensic® Extractor v.8.0.3.199

Oxygen Forensic® Extractor

Select a type of device backup or physical image

iTunes backup

Acquire iTunes backup from iOS device

Android physical image Need root access

Acquire physical image from Android OS device

Android backup Android OS v.4.0 and higher

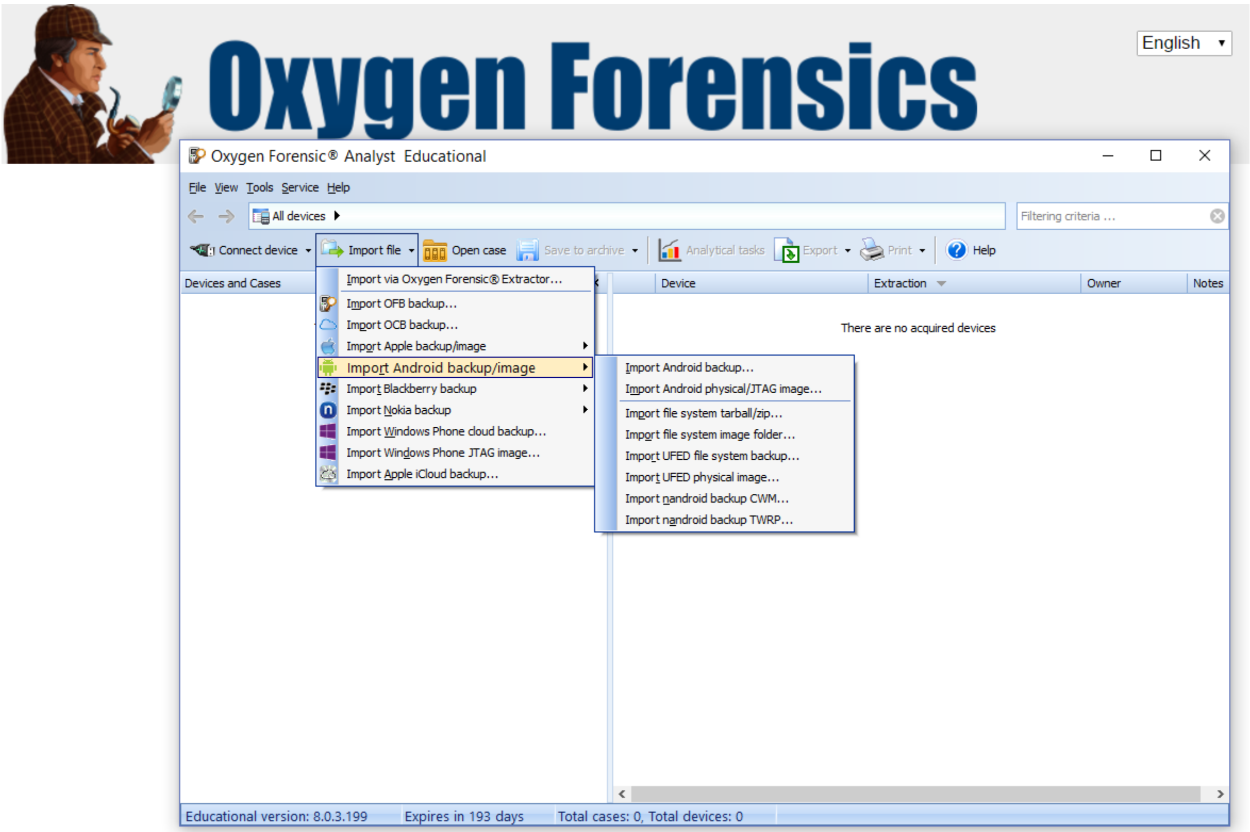
Acquire backup from Android OS device

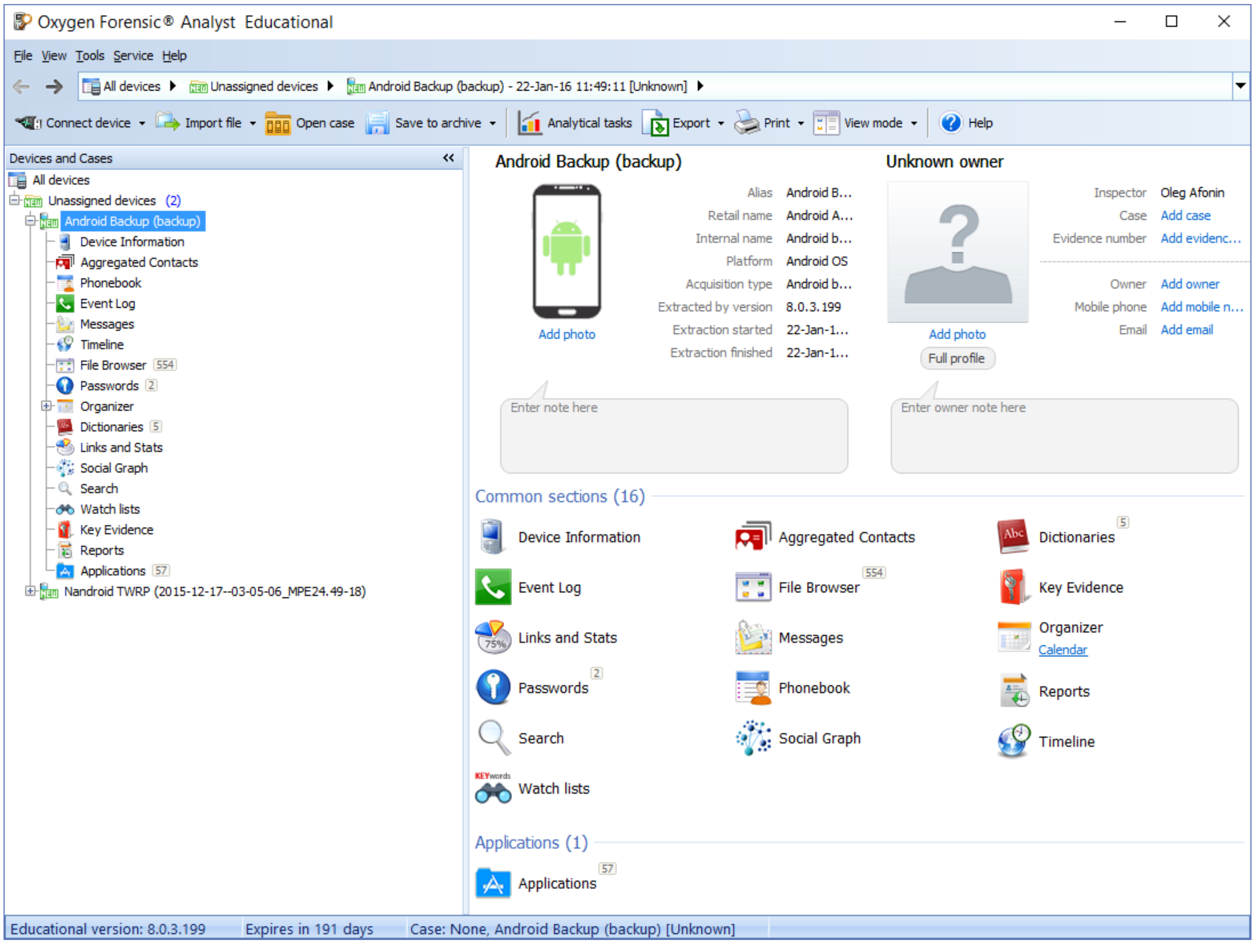
MTK Android physical image

Acquire physical image from MTK Android OS device

LG Android physical image

Acquire physical image from LG Android OS devices using Devices Firmware Update mode

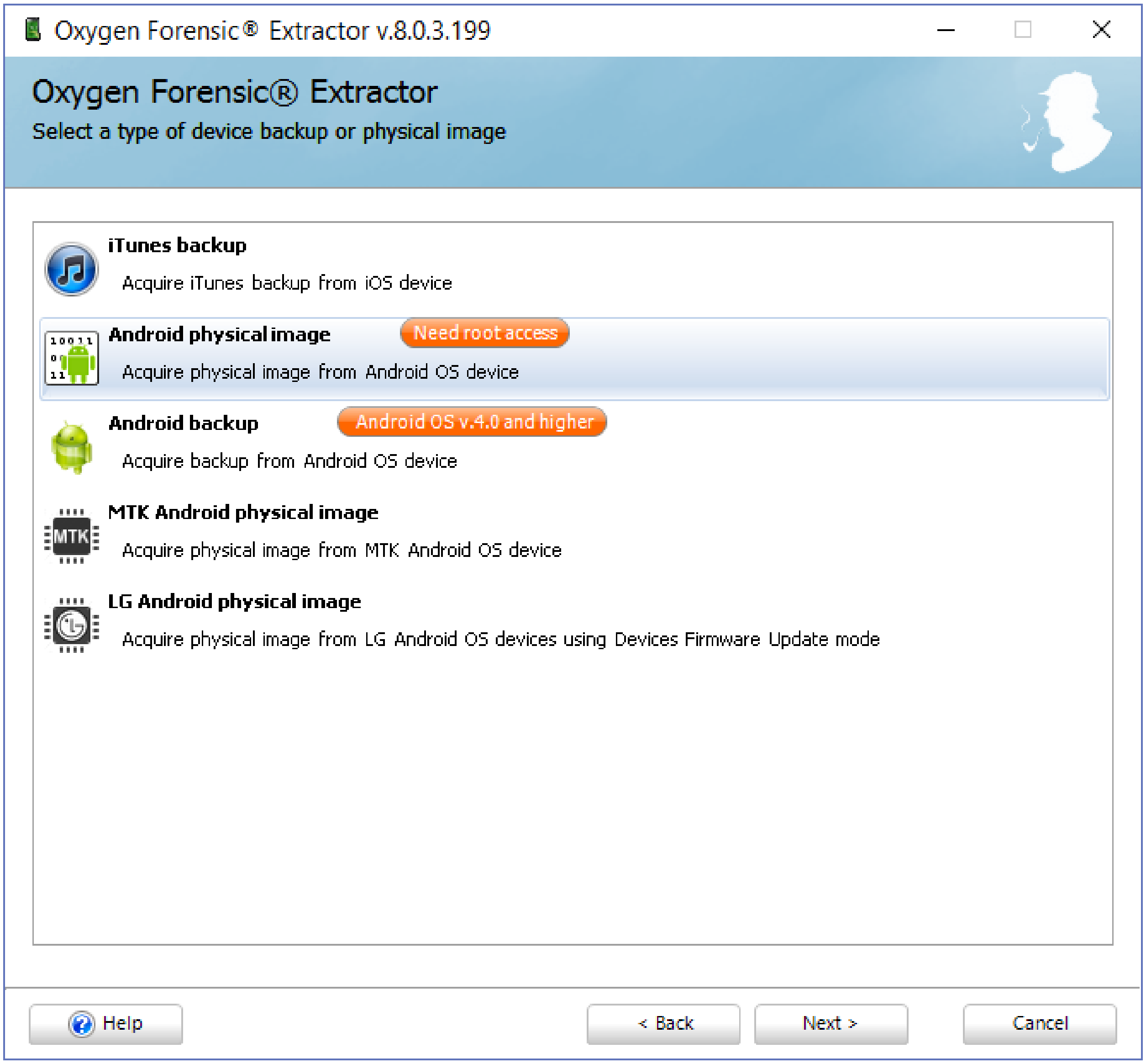

Oxygen Forensics
English
Oxygen Forensic® Analyst Educational
File View Tools Service Help
All devices
Filtering criteria ...
Connect device
Import file
Open case
Save to archive
Analytical tasks
Export
Print
Help
Devices and Cases
Device
Extraction
Owner
Notes
Import via Oxygen Forensic® Extractor...
Import OFB backup...
Import OCB backup...
Import Apple backup/image
Import Android backup/image
Import Blackberry backup
Import Nokia backup
Import Windows Phone cloud backup...
Import Windows Phone JTAG image...
Import Apple iCloud backup...
Import Android backup...
Import Android physical/JTAG image...
Import file system tarball/zip...
Import file system image folder...
Import UFED file system backup...
Import UFED physical image...
Import nandroid backup CWM...
Import nandroid backup TWRP...
There are no acquired devices
Educational version: 8.0.3.199
Expires in 193 days
Total cases: 0, Total devices: 0



Alias	Android B…
Retail name	Android A…
Internal name	Android b…
Platform	Android OS
Acquisition type	Android b…
Extracted by version	8.0.3.199
Extraction started	22-Jan-1…
Extraction finished	22-Jan-1…

Inspector	Oleg Afonin
Case	Add case
Evidence number	Add evidenc…
Owner	Add owner
Mobile phone	Add mobile n…
Email	Add email

Educational version: 8.0.3.199 Expires in 191 days Case: None, Android Backup (backup) [Unknown]



Oxygen Forensic® Extractor v.8.0.3.199

Oxygen Forensic® Extractor

Select a type of device backup or physical image

iTunes backup

Acquire iTunes backup from iOS device

Android physical image Need root access

Acquire physical image from Android OS device

Android backup Android OS v.4.0 and higher

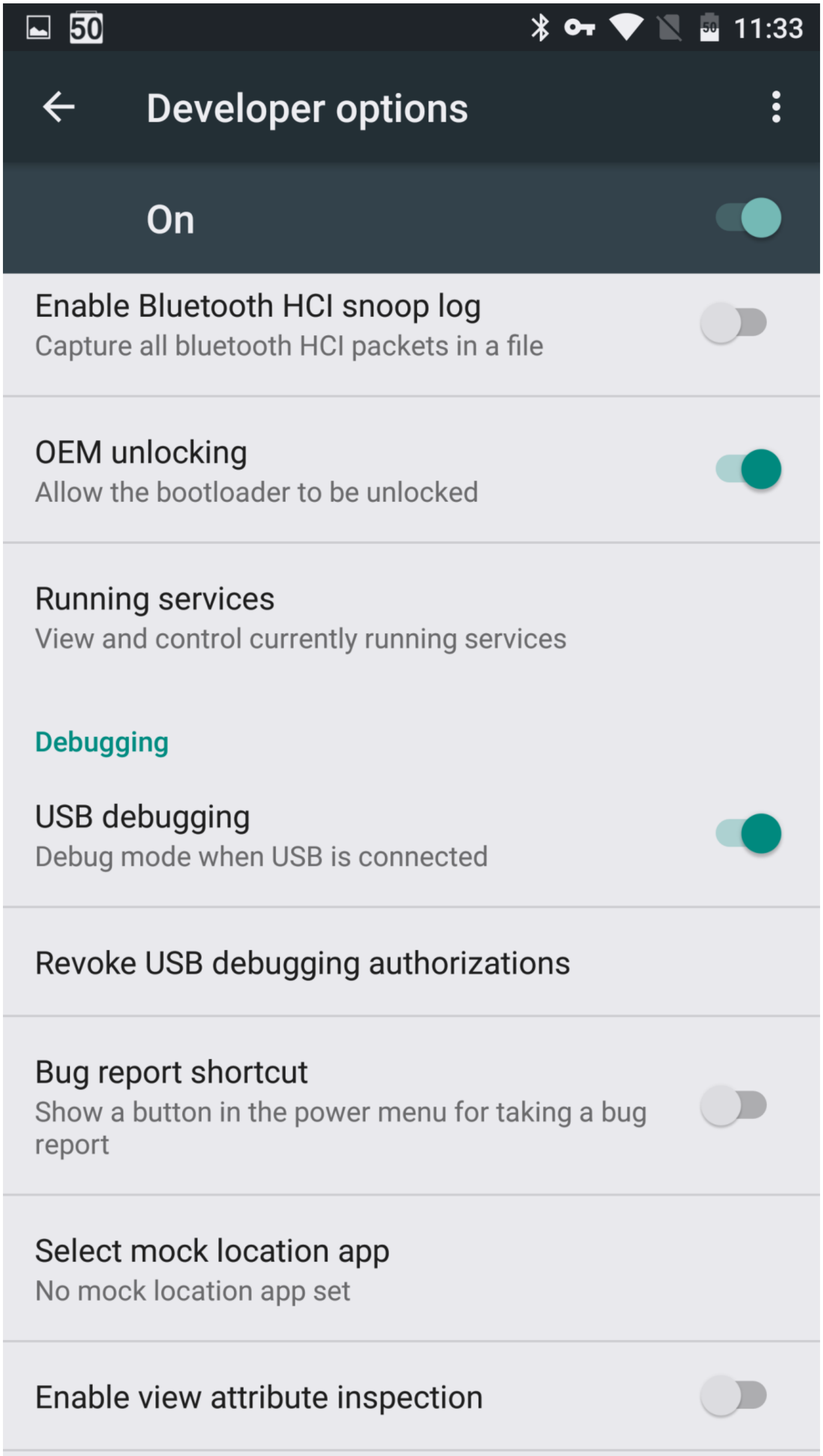
Acquire backup from Android OS device

MTK Android physical image

Acquire physical image from MTK Android OS device

LG Android physical image

Acquire physical image from LG Android OS devices using Devices Firmware Update mode



Developer options

On ☑

Enable Bluetooth HCI snoop log □
Capture all bluetooth HCI packets in a file

OEM unlocking ☑
Allow the bootloader to be unlocked

Running services
View and control currently running services

Debugging

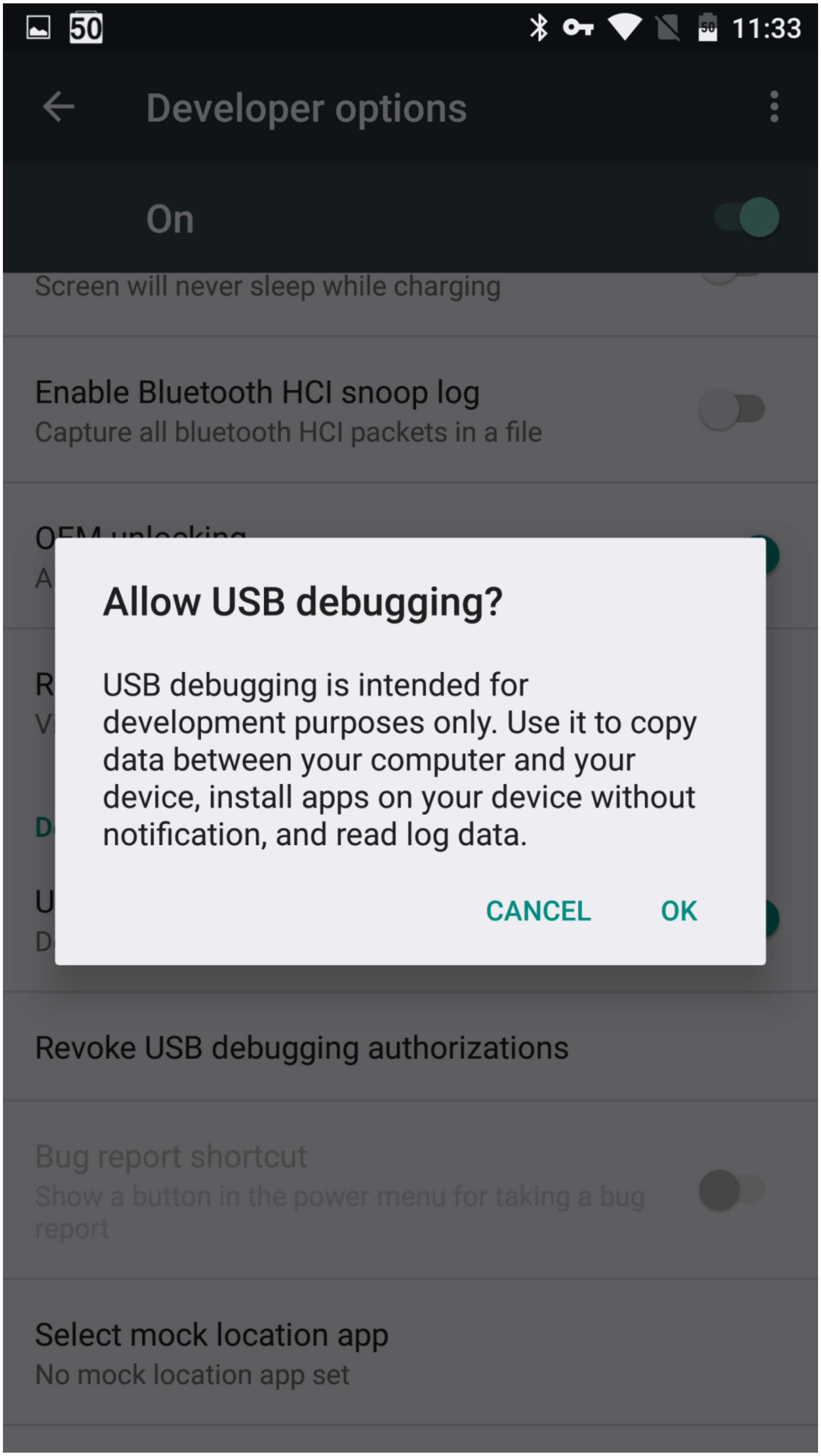
USB debugging ☑
Debug mode when USB is connected

Revoke USB debugging authorizations

Bug report shortcut □
Show a button in the power menu for taking a bug report

Select mock location app
No mock location app set

Enable view attribute inspection □



Developer options

On

Screen will never sleep while charging

Enable Bluetooth HCI snoop log
Capture all bluetooth HCI packets in a file

OEM unlocking

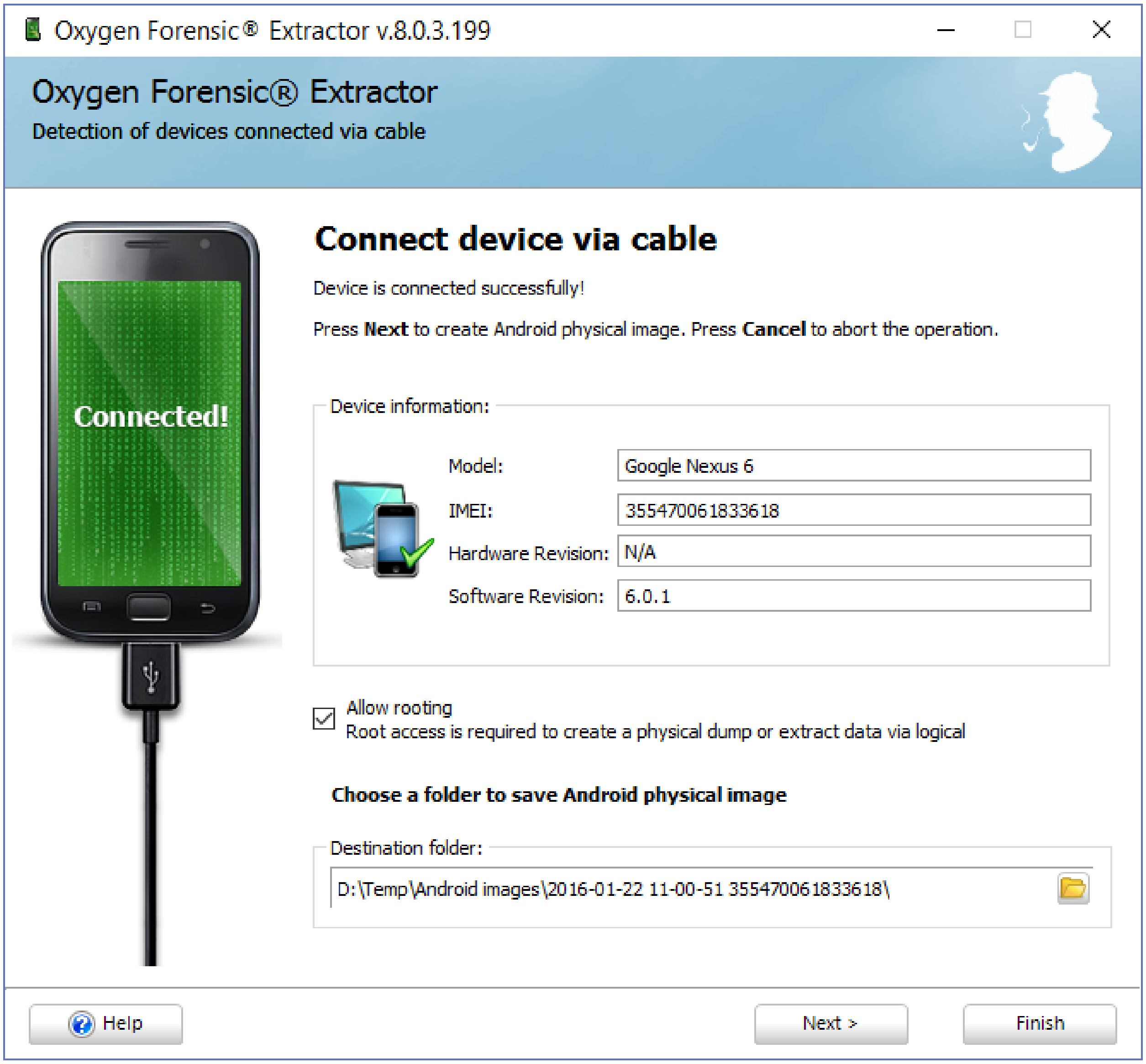
Allow USB debugging?

USB debugging is intended for development purposes only. Use it to copy data between your computer and your device, install apps on your device without notification, and read log data.

Revoke USB debugging authorizations

Bug report shortcut
Show a button in the power menu for taking a bug report

Select mock location app
No mock location app set



Oxygen Forensic® Extractor v.8.0.3.199

Oxygen Forensic® Extractor

Detection of devices connected via cable

Connect device via cable

Device is connected successfully!

Press **Next** to create Android physical image. Press **Cancel** to abort the operation.

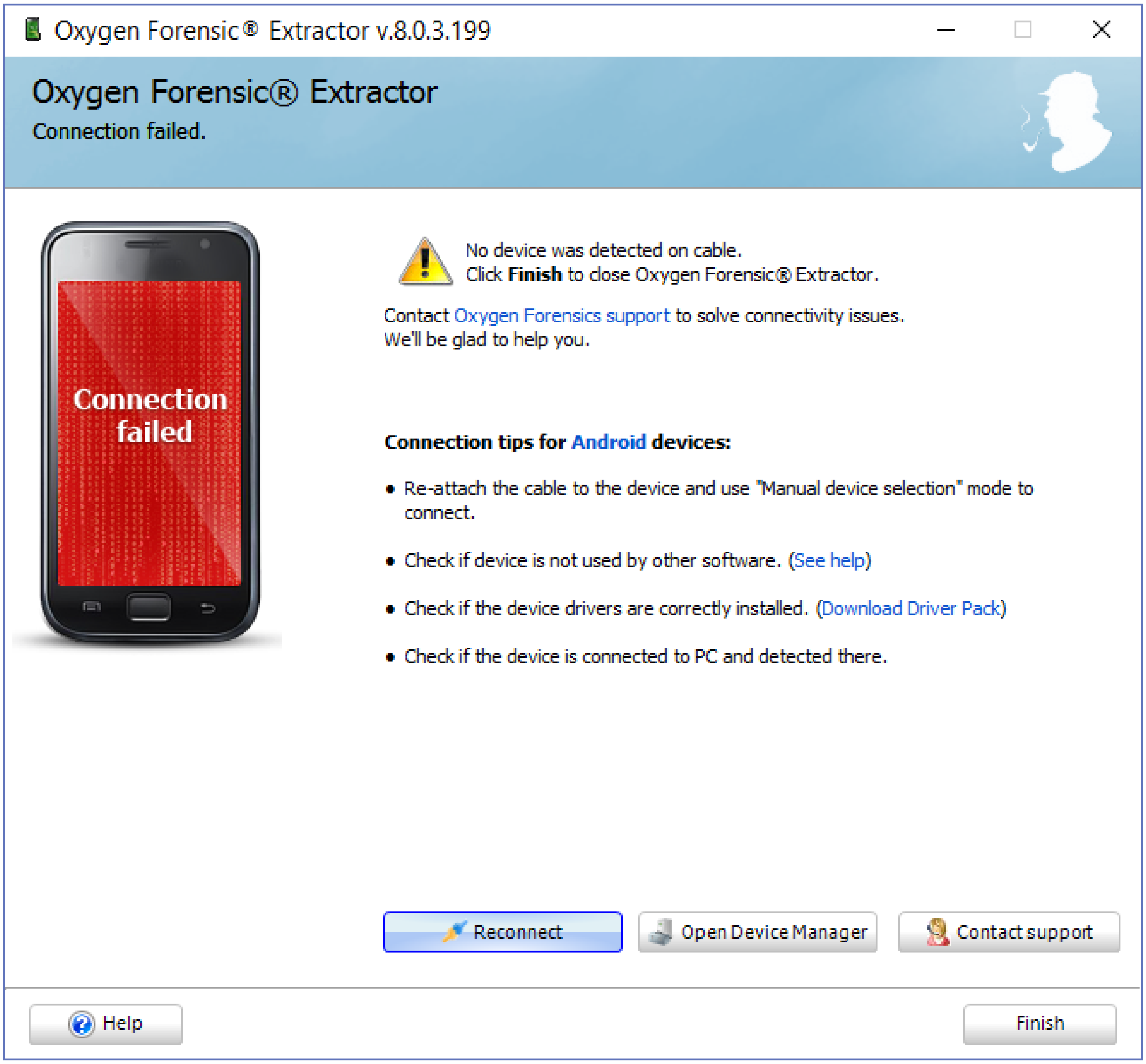
Device information:

Model:	Google Nexus 6
IMEI:	355470061833618
Hardware Revision:	N/A
Software Revision:	6.0.1

☑ Allow rooting
Root access is required to create a physical dump or extract data via logical

Choose a folder to save Android physical image

Destination folder:
D:\Temp\Android images\2016-01-22 11-00-51 355470061833618\



Oxygen Forensic® Extractor

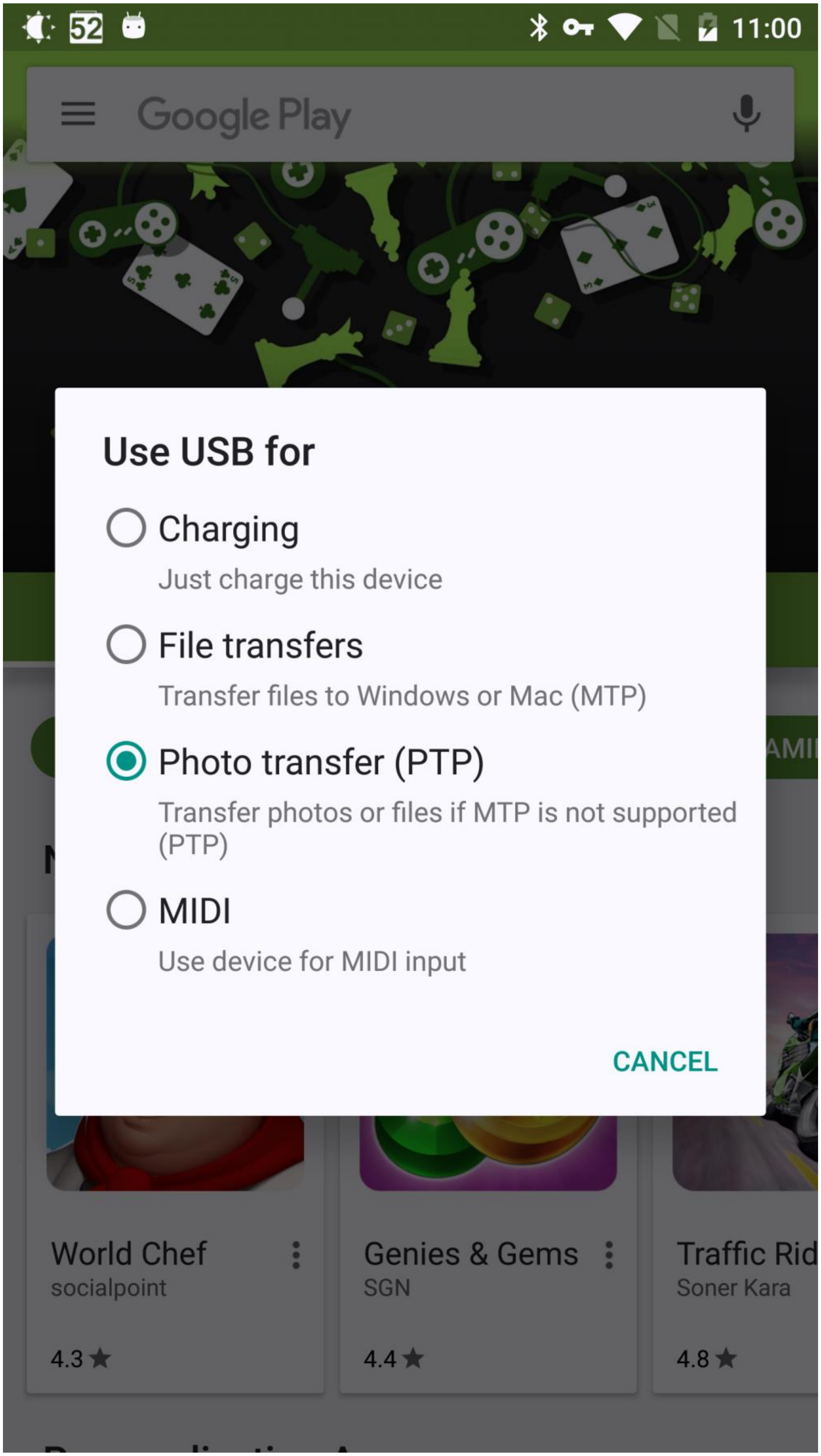
Connection failed.

No device was detected on cable.
Click **Finish** to close Oxygen Forensic® Extractor.

Contact Oxygen Forensics support to solve connectivity issues.
We'll be glad to help you.

Connection tips for Android devices:

- Re-attach the cable to the device and use "Manual device selection" mode to connect.
- Check if device is not used by other software. (See help)
- Check if the device drivers are correctly installed. (Download Driver Pack)
- Check if the device is connected to PC and detected there.



Use USB for

○ Charging

Just charge this device

○ File transfers

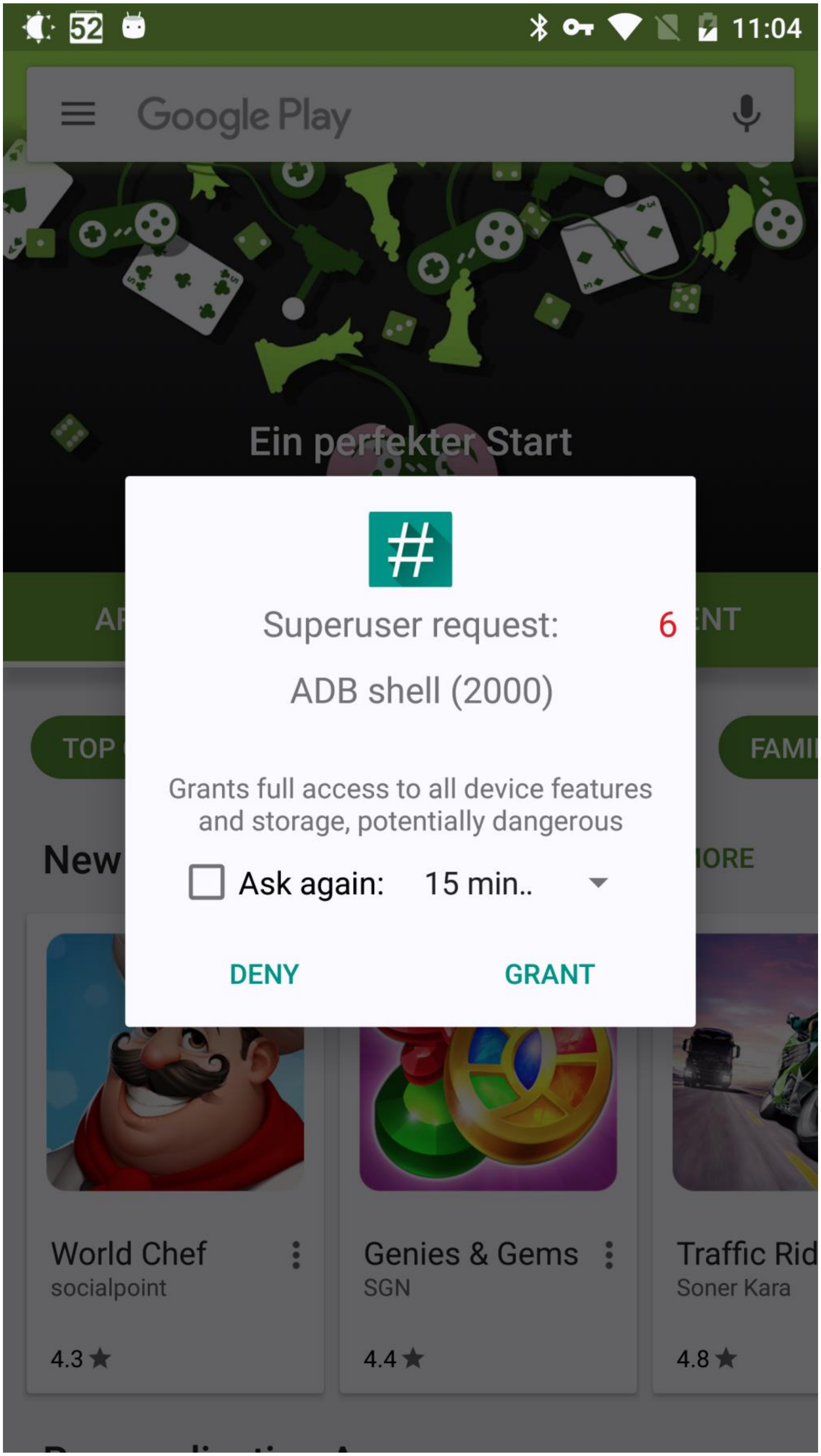
Transfer files to Windows or Mac (MTP)

● Photo transfer (PTP)

Transfer photos or files if MTP is not supported (PTP)

○ MIDI

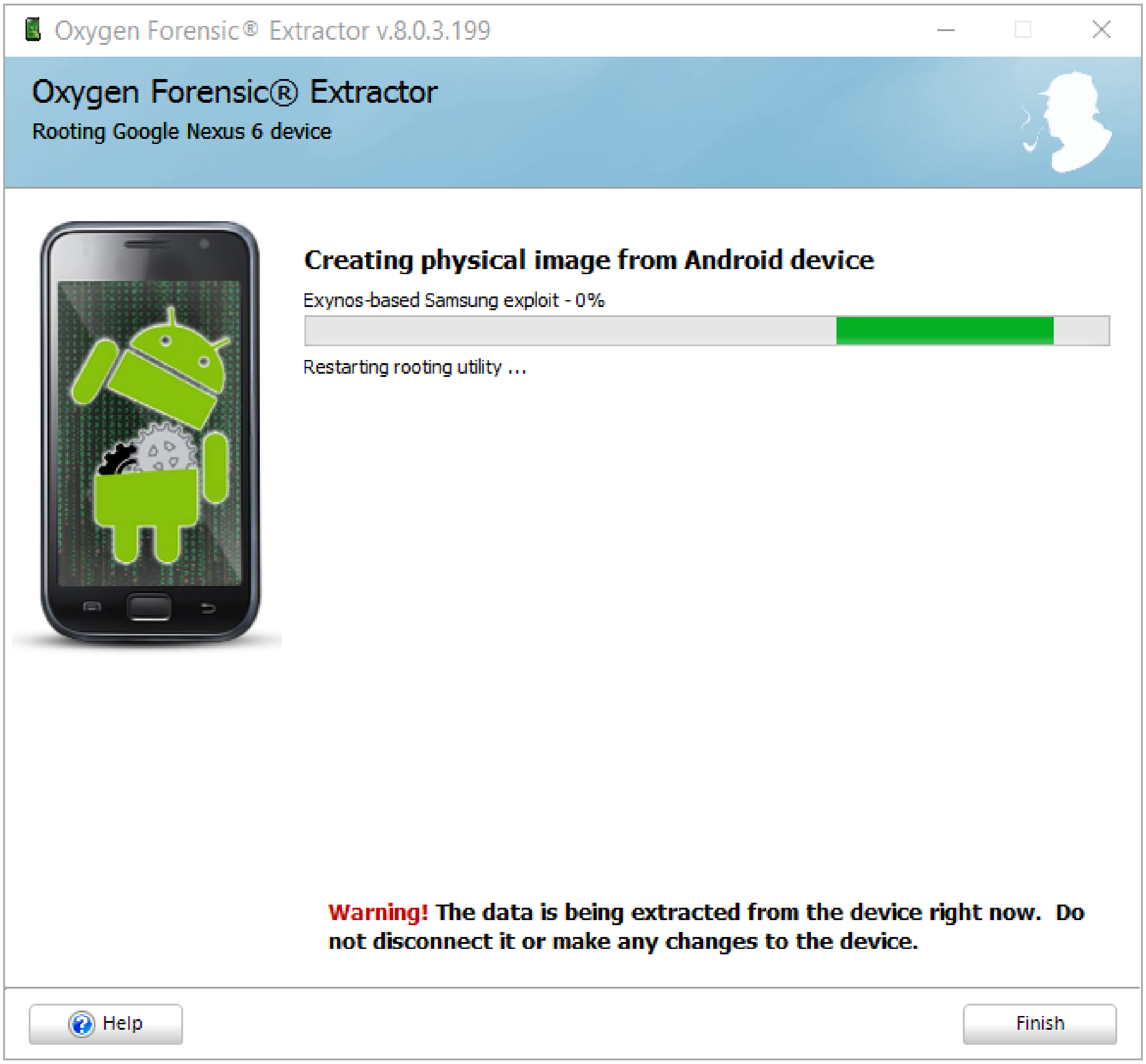
Use device for MIDI input


Superuser request: 6

ADB shell (2000)

Grants full access to all device features and storage, potentially dangerous

□ Ask again: 15 min..



Oxygen Forensic® Extractor v.8.0.3.199

Oxygen Forensic® Extractor

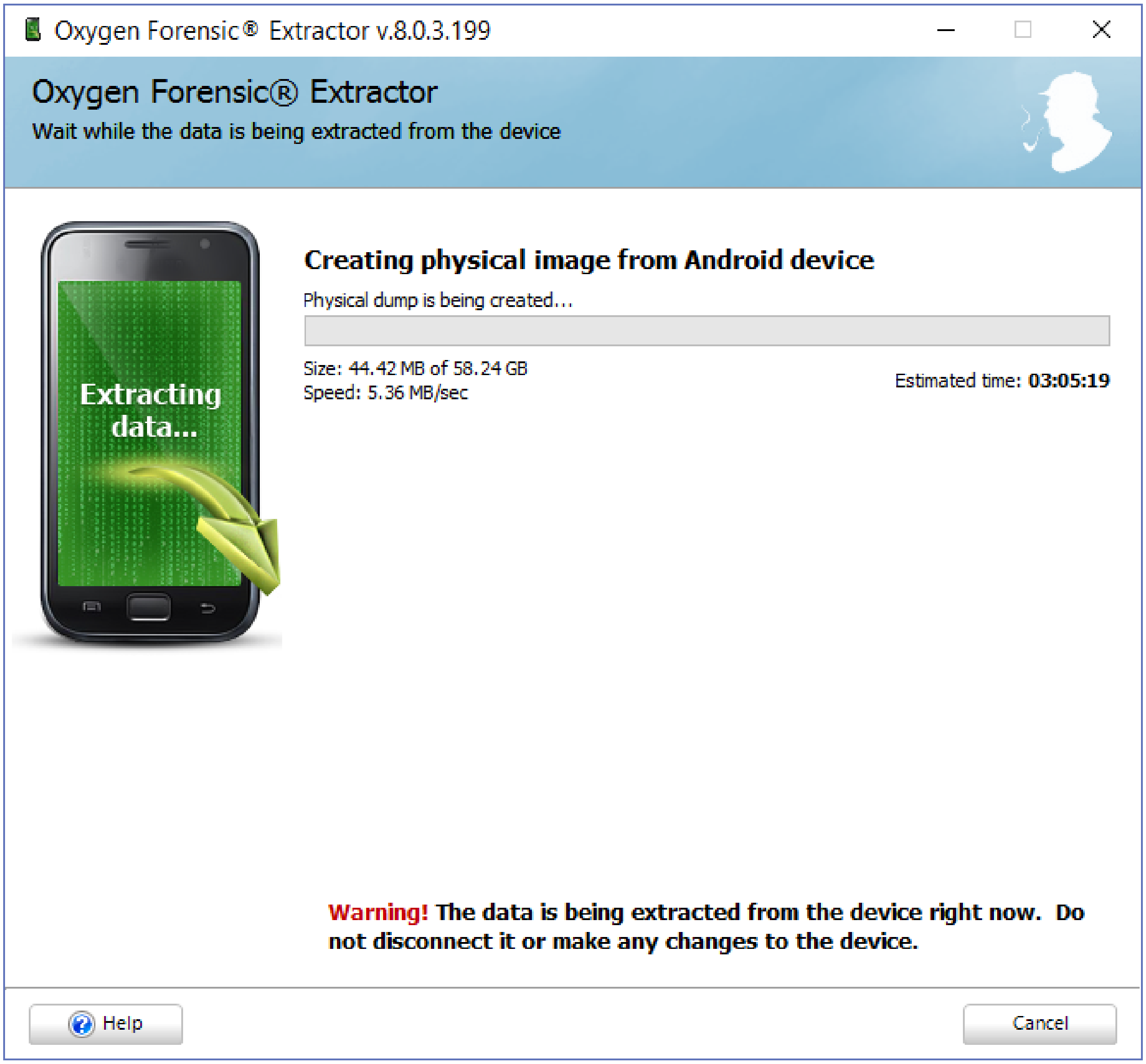
Rooting Google Nexus 6 device

Creating physical image from Android device

Exynos-based Samsung exploit - 0%

Restarting rooting utility ...

Warning! The data is being extracted from the device right now. Do not disconnect it or make any changes to the device.



Oxygen Forensic® Extractor v.8.0.3.199

Oxygen Forensic® Extractor

Wait while the data is being extracted from the device

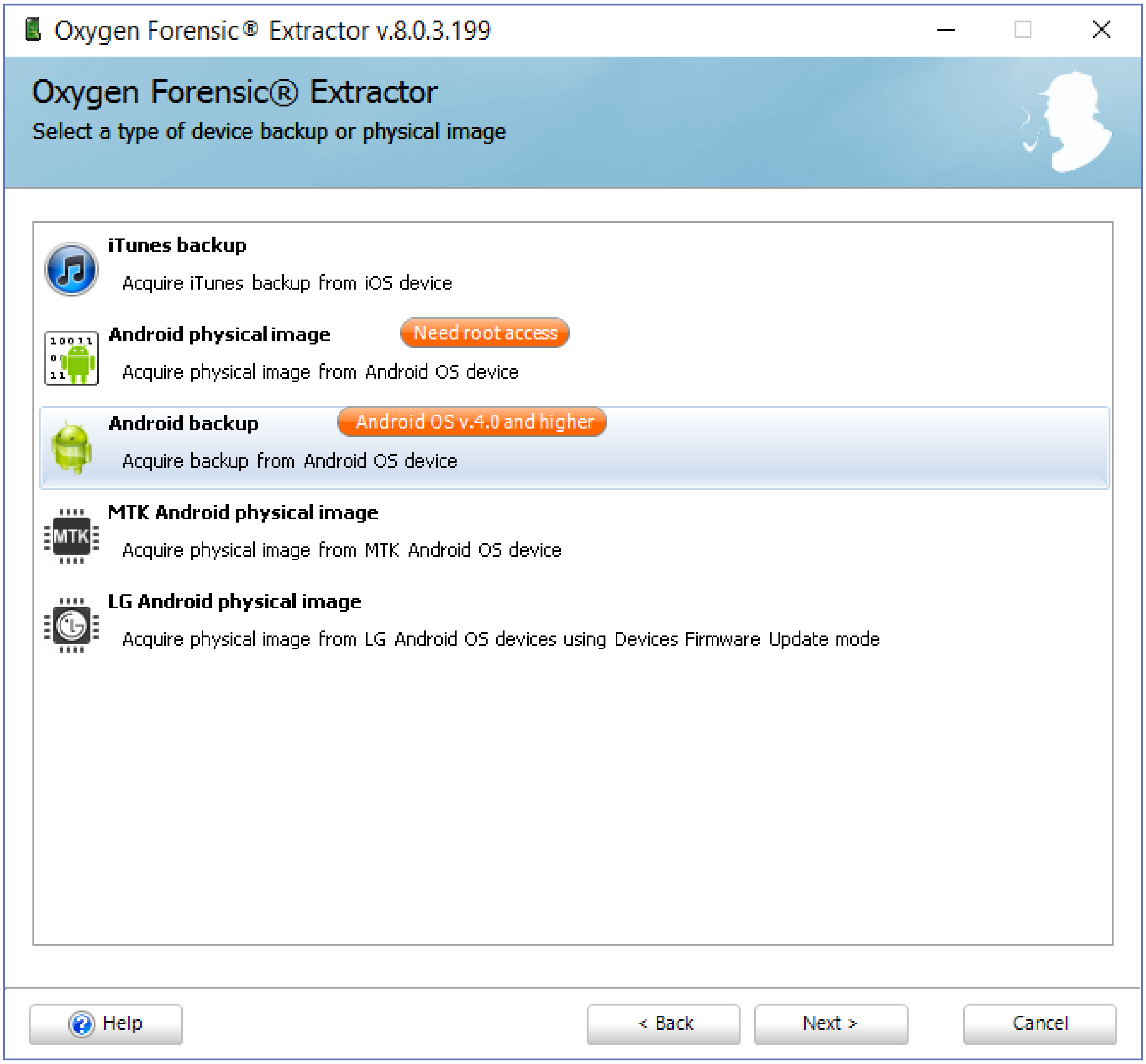
Creating physical image from Android device

Physical dump is being created...

Size: 44.42 MB of 58.24 GB
Speed: 5.36 MB/sec

Estimated time: **03:05:19**

Warning! The data is being extracted from the device right now. Do not disconnect it or make any changes to the device.



Oxygen Forensic® Extractor v.8.0.3.199

Oxygen Forensic® Extractor

Select a type of device backup or physical image

iTunes backup

Acquire iTunes backup from iOS device

Android physical image Need root access

Acquire physical image from Android OS device

Android backup Android OS v.4.0 and higher

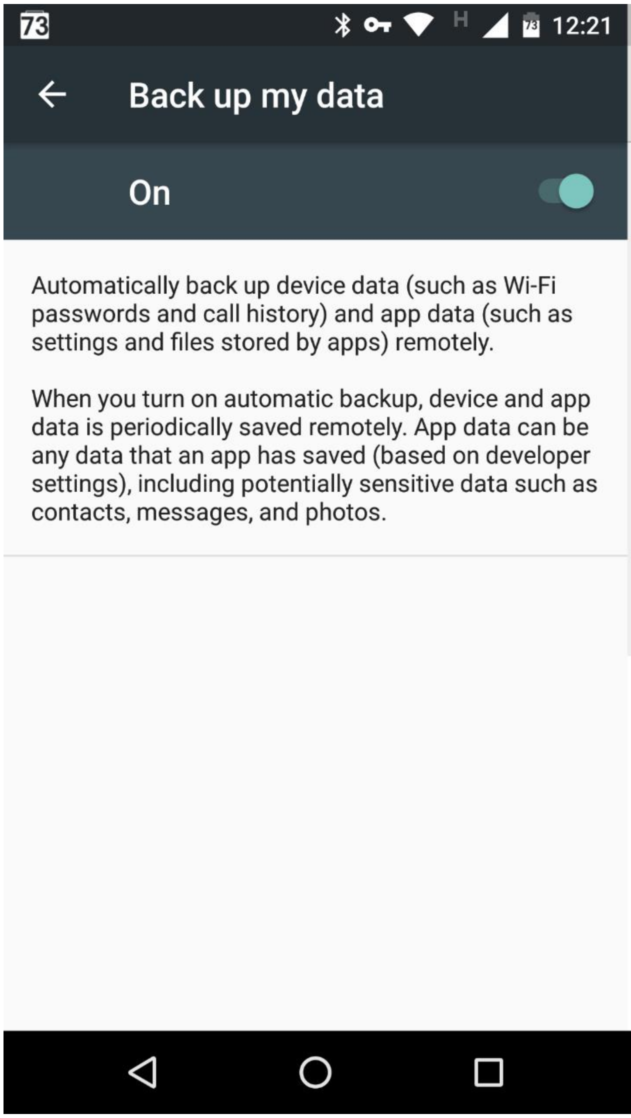
Acquire backup from Android OS device

MTK Android physical image

Acquire physical image from MTK Android OS device

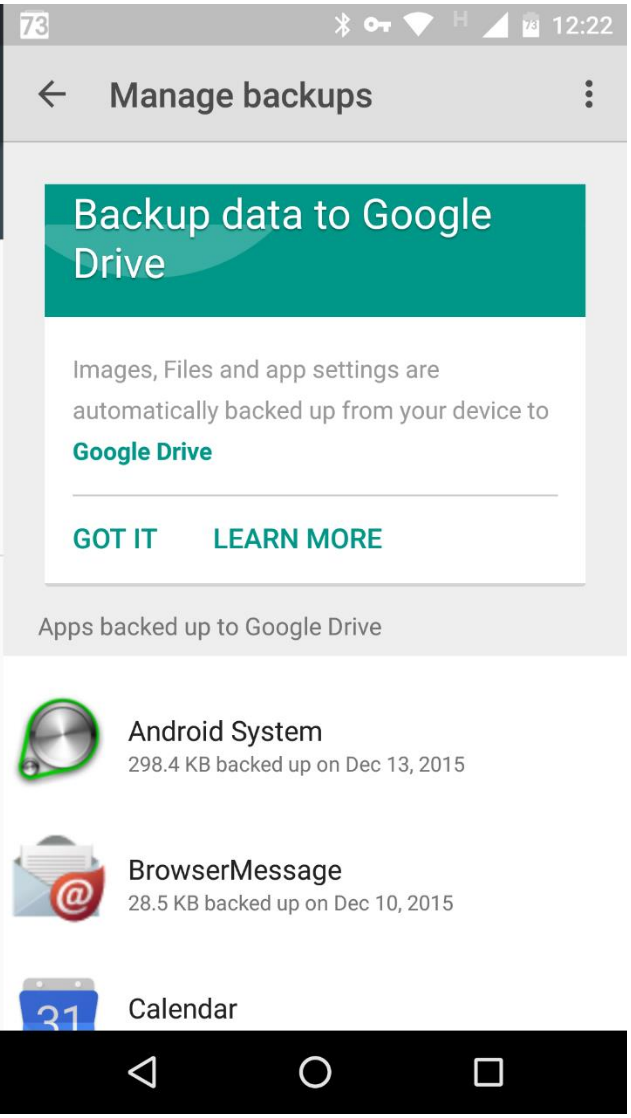
LG Android physical image

Acquire physical image from LG Android OS devices using Devices Firmware Update mode



Automatically back up device data (such as Wi-Fi passwords and call history) and app data (such as settings and files stored by apps) remotely.

When you turn on automatic backup, device and app data is periodically saved remotely. App data can be any data that an app has saved (based on developer settings), including potentially sensitive data such as contacts, messages, and photos.



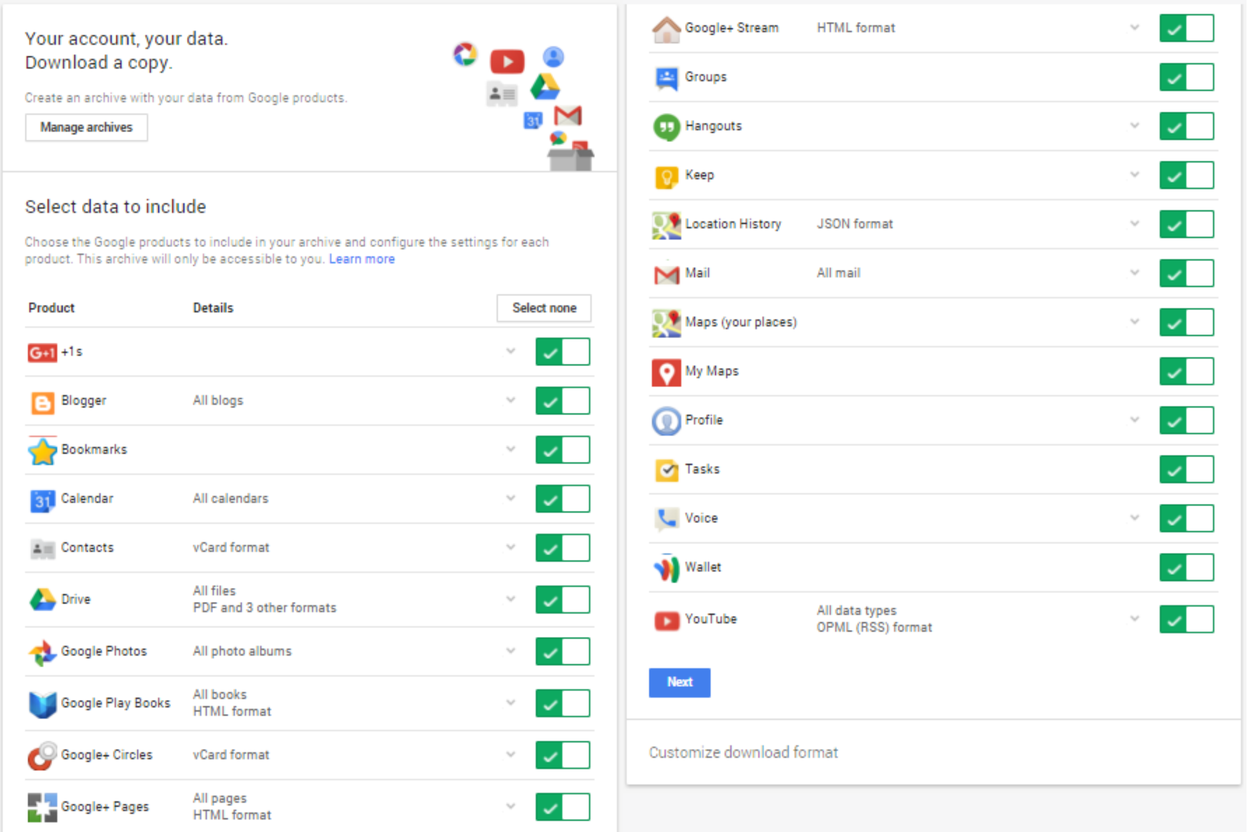
Images, Files and app settings are automatically backed up from your device to **Google Drive**

Apps backed up to Google Drive

Android System
298.4 KB backed up on Dec 13, 2015

BrowserMessage
28.5 KB backed up on Dec 10, 2015

Calendar



Your account, your data.
Download a copy.

Create an archive with your data from Google products.

Manage archives

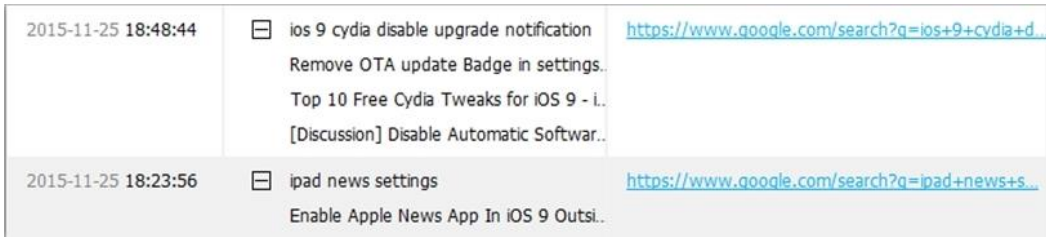
Select data to include

Choose the Google products to include in your archive and configure the settings for each product. This archive will only be accessible to you. Learn more

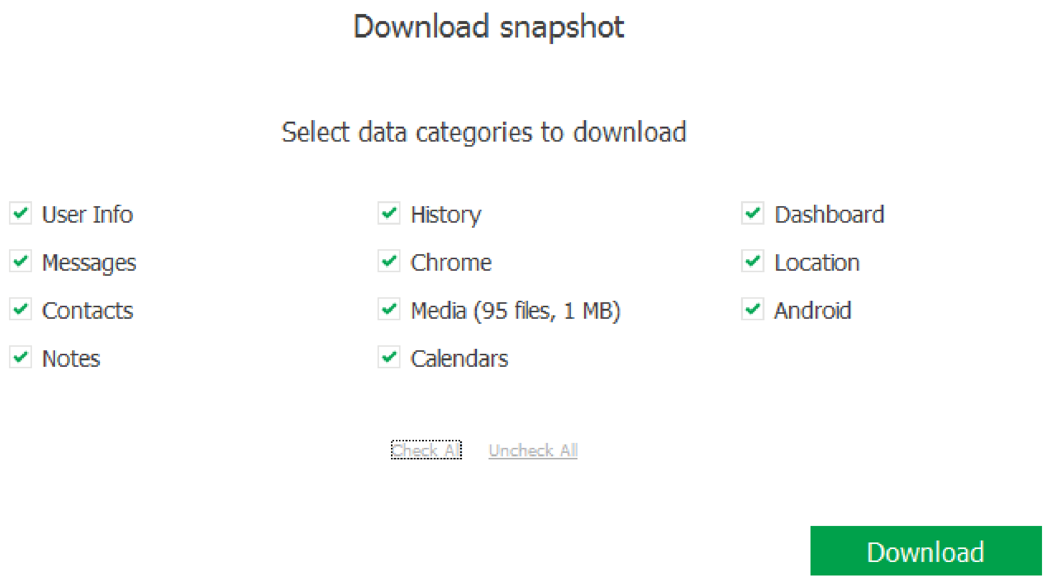
Product	Details	Select none
+1s		✓
Blogger	All blogs	✓
Bookmarks		✓
Calendar	All calendars	✓
Contacts	vCard format	✓
Drive	All files PDF and 3 other formats	✓
Google Photos	All photo albums	✓
Google Play Books	All books HTML format	✓
Google+ Circles	vCard format	✓
Google+ Pages	All pages HTML format	✓
Google+ Stream	HTML format	✓
Groups		✓
Hangouts		✓
Keep		✓
Location History	JSON format	✓
Mail	All mail	✓
Maps (your places)		✓
My Maps		✓
Profile		✓
Tasks		✓
Voice		✓
Wallet		✓
YouTube	All data types OPML (RSS) format	✓

Next

Customize download format



2015-11-25 18:48:44	ios 9 cydia disable upgrade notification Remove OTA update Badge in settings.. Top 10 Free Cydia Tweaks for iOS 9 - i.. [Discussion] Disable Automatic Softwar..	https://www.google.com/search?q=ios+9+cydia+d...
2015-11-25 18:23:56	ipad news settings Enable Apple News App In iOS 9 Outsi..	https://www.google.com/search?q=ipad+news+s...



Download snapshot

Select data categories to download

☑ User Info

☑ Messages

☑ Contacts

☑ Notes

☑ History

☑ Chrome

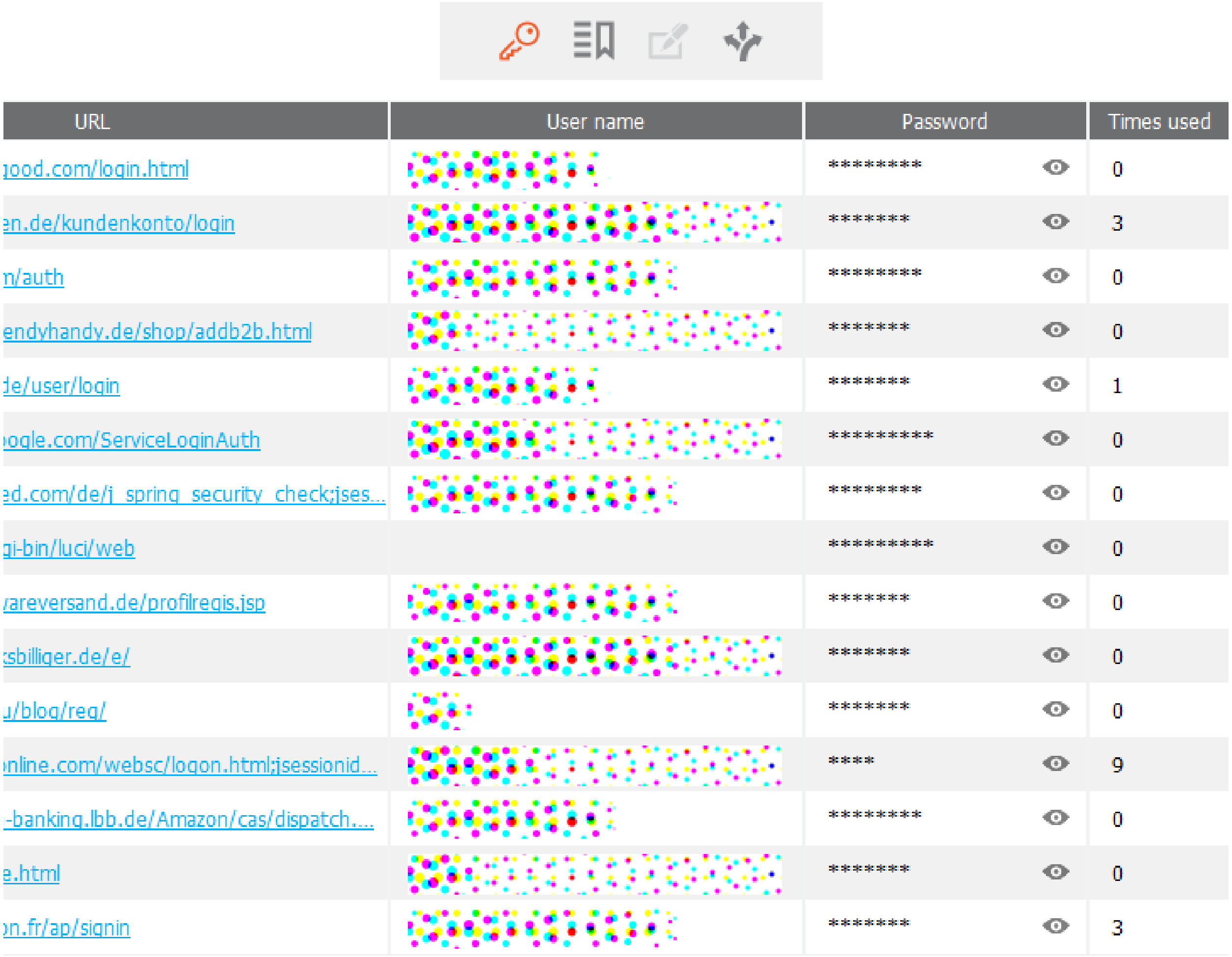
☑ Media (95 files, 1 MB)

☑ Calendars

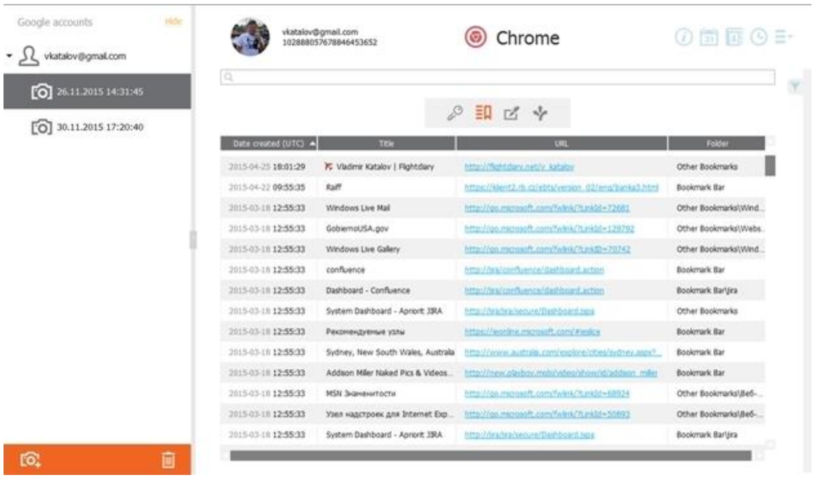
☑ Dashboard

☑ Location

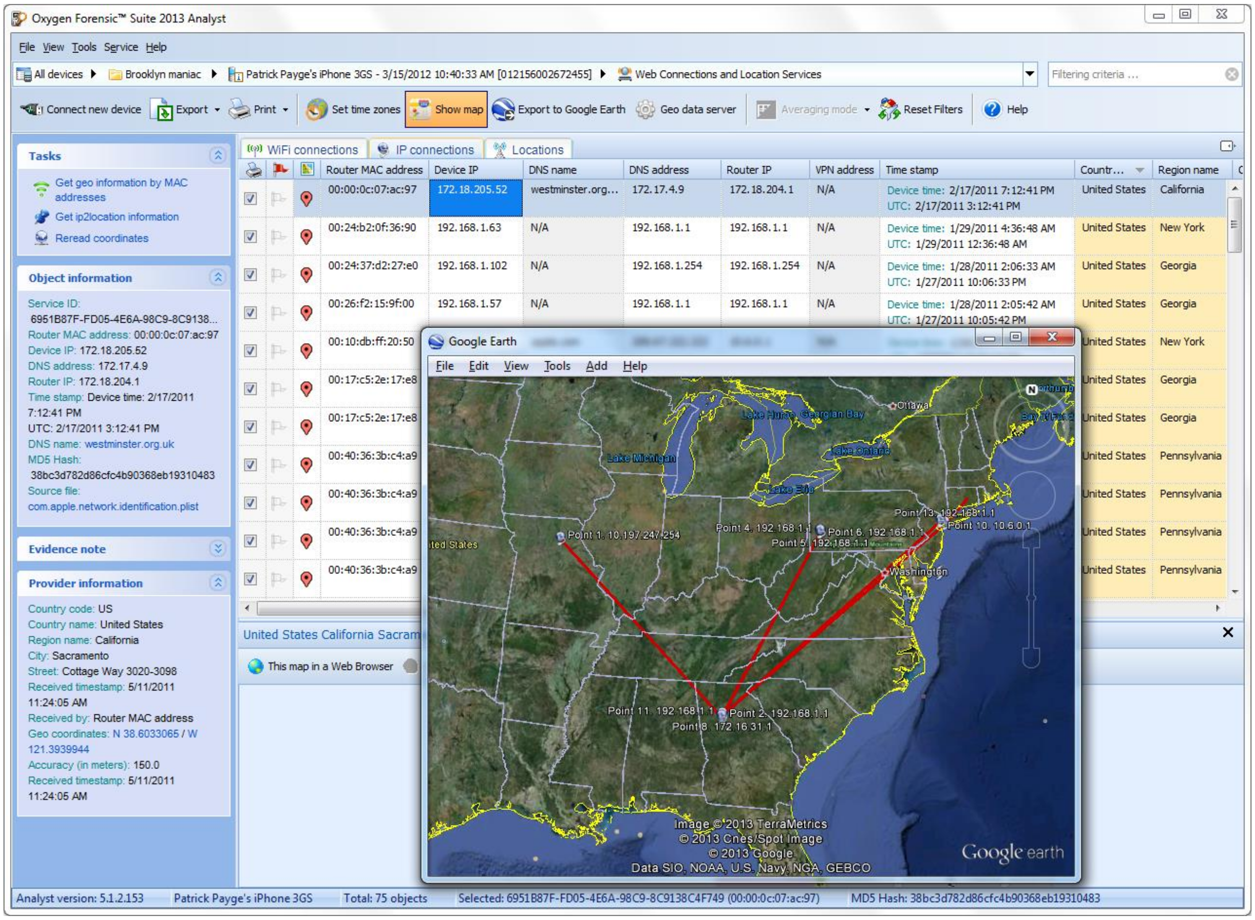
☑ Android



URL	User name	Password		Times used
jood.com/login.html	[redacted]	********	👁	0
en.de/kundenkonto/login	[redacted]	*******	👁	3
n/auth	[redacted]	********	👁	0
endyhandy.de/shop/addb2b.html	[redacted]	*******	👁	0
de/user/login	[redacted]	*******	👁	1
oogle.com/ServiceLoginAuth	[redacted]	*********	👁	0
ed.com/de/j_spring_security_check;jses…	[redacted]	********	👁	0
gi-bin/luci/web		*********	👁	0
vareversand.de/profilregis.jsp	[redacted]	*******	👁	0
ksbilliger.de/e/	[redacted]	*******	👁	0
u/blog/reg/	[redacted]	*******	👁	0
online.com/websc/logon.html;jsessionid…	[redacted]	****	👁	9
-banking.lbb.de/Amazon/cas/dispatch.…	[redacted]	********	👁	0
e.html	[redacted]	*******	👁	0
on.fr/ap/signin	[redacted]	*******	👁	3



Date created (UTC)	Title	URL	Folder
2015-04-25 18:01:29	Vladimir Katalov | Flightdiary	http://flightdiary.net/v_katalov	Other Bookmarks
2015-04-22 09:55:35	Raiff	https://klient2.rb.cz/ebts/version_02/eng/banka3.html	Bookmark Bar
2015-03-18 12:55:33	Windows Live Mail	http://go.microsoft.com/fwlink/?LinkId=72681	Other Bookmarks\Wind...
2015-03-18 12:55:33	GobiernoUSA.gov	http://go.microsoft.com/fwlink/?LinkId=129792	Other Bookmarks\Webs...
2015-03-18 12:55:33	Windows Live Gallery	http://go.microsoft.com/fwlink/?LinkID=70742	Other Bookmarks\Wind...
2015-03-18 12:55:33	confluence	http://jira/confluence/dashboard.action	Bookmark Bar
2015-03-18 12:55:33	Dashboard - Confluence	http://jira/confluence/dashboard.action	Bookmark Bar\jira
2015-03-18 12:55:33	System Dashboard - Apriorit JIRA	http://jira/jira/secure/Dashboard.jspa	Other Bookmarks
2015-03-18 12:55:33	Рекомендуемые узлы	https://ieonline.microsoft.com/#ieslice	Bookmark Bar
2015-03-18 12:55:33	Sydney, New South Wales, Australia	http://www.australia.com/explore/cities/sydney.aspx?_...	Bookmark Bar
2015-03-18 12:55:33	Addison Miller Naked Pics & Videos...	http://new.playboy.mobi/video/show/id/addison_miller	Bookmark Bar
2015-03-18 12:55:33	MSN Знаменитости	http://go.microsoft.com/fwlink/?LinkId=68924	Other Bookmarks\Веб-...
2015-03-18 12:55:33	Узел надстроек для Internet Exp...	http://go.microsoft.com/fwlink/?LinkId=50893	Other Bookmarks\Веб-...
2015-03-18 12:55:33	System Dashboard - Apriorit JIRA	http://jira/jira/secure/Dashboard.jspa	Bookmark Bar\jira



Tasks

- Get geo information by MAC addresses
- Get ip2location information
- Reread coordinates

Object information

Service ID: 6951B87F-FD05-4E6A-98C9-8C9138...
Router MAC address: 00:00:0c:07:ac:97
Device IP: 172.18.205.52
DNS address: 172.17.4.9
Router IP: 172.18.204.1
Time stamp: Device time: 2/17/2011 7:12:41 PM
UTC: 2/17/2011 3:12:41 PM
DNS name: westminster.org.uk
MD5 Hash: 38bc3d782d86cfc4b90368eb19310483
Source file: com.apple.network.identification.plist

Evidence note

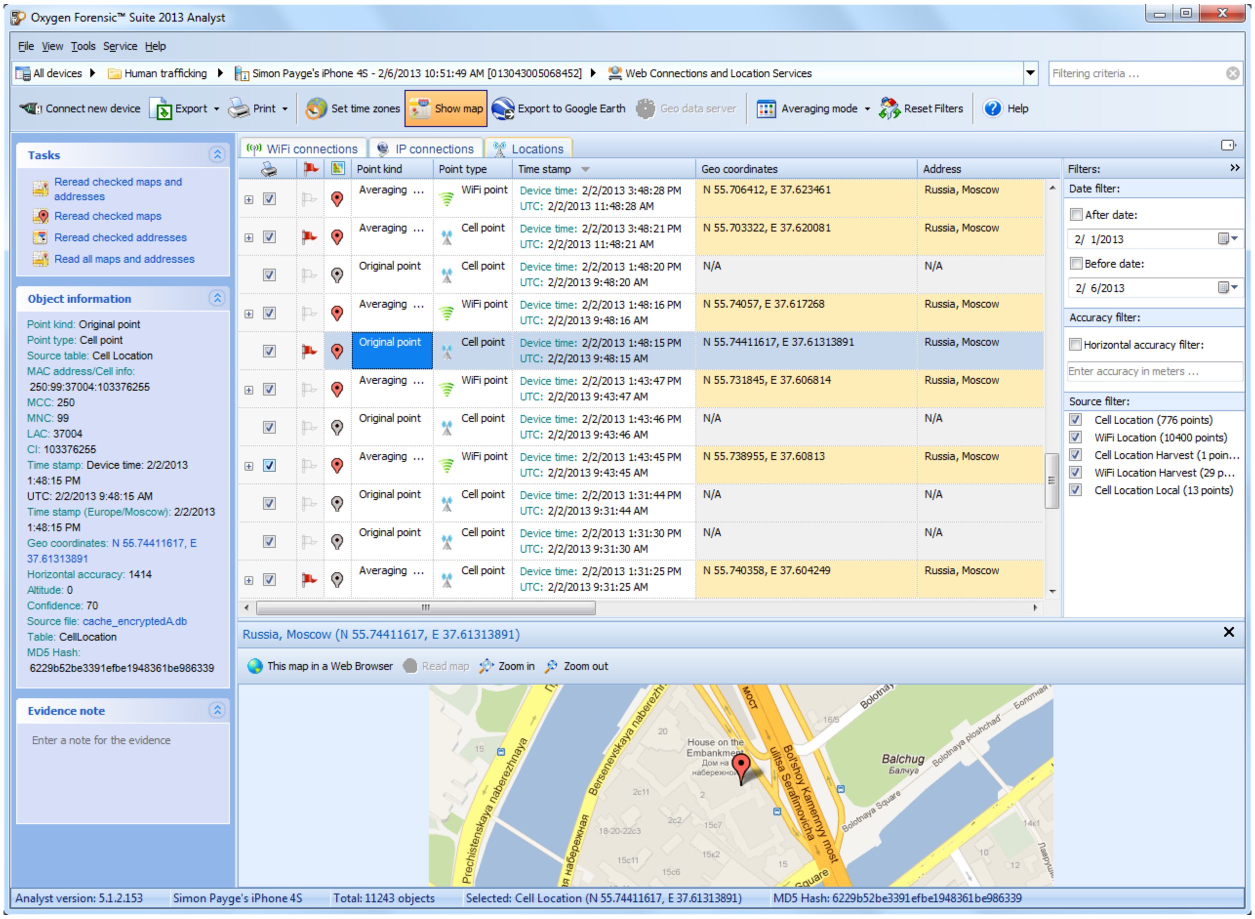
Provider information

Country code: US
Country name: United States
Region name: California
City: Sacramento
Street: Cottage Way 3020-3098
Received timestamp: 5/11/2011 11:24:05 AM
Received by: Router MAC address
Geo coordinates: N 38.6033065 / W 121.3939944
Accuracy (in meters): 150.0
Received timestamp: 5/11/2011 11:24:05 AM

			Router MAC address	Device IP	DNS name	DNS address	Router IP	VPN address	Time stamp	Countr...	Region name
☑			00:00:0c:07:ac:97	172.18.205.52	westminster.org...	172.17.4.9	172.18.204.1	N/A	Device time: 2/17/2011 7:12:41 PM UTC: 2/17/2011 3:12:41 PM	United States	California
☑			00:24:b2:0f:36:90	192.168.1.63	N/A	192.168.1.1	192.168.1.1	N/A	Device time: 1/29/2011 4:36:48 AM UTC: 1/29/2011 12:36:48 AM	United States	New York
☑			00:24:37:d2:27:e0	192.168.1.102	N/A	192.168.1.254	192.168.1.254	N/A	Device time: 1/28/2011 2:06:33 AM UTC: 1/27/2011 10:06:33 PM	United States	Georgia
☑			00:26:f2:15:9f:00	192.168.1.57	N/A	192.168.1.1	192.168.1.1	N/A	Device time: 1/28/2011 2:05:42 AM UTC: 1/27/2011 10:05:42 PM	United States	Georgia
☑			00:10:db:ff:20:50							United States	New York
☑			00:17:c5:2e:17:e8							United States	Georgia
☑			00:17:c5:2e:17:e8							United States	Georgia
☑			00:40:36:3b:c4:a9							United States	Pennsylvania
☑			00:40:36:3b:c4:a9							United States	Pennsylvania
☑			00:40:36:3b:c4:a9							United States	Pennsylvania
☑			00:40:36:3b:c4:a9							United States	Pennsylvania

United States California Sacram

Analyst version: 5.1.2.153 | Patrick Payge's iPhone 3GS | Total: 75 objects | Selected: 6951B87F-FD05-4E6A-98C9-8C9138C4F749 (00:00:0c:07:ac:97) | MD5 Hash: 38bc3d782d86cfc4b90368eb19310483



Point kind: Original point
Point type: Cell point
Source table: Cell Location
MAC address/Cell info:
250:99:37004:103376255
MCC: 250
MNC: 99
LAC: 37004
CI: 103376255
Time stamp: Device time: 2/2/2013
1:48:15 PM
UTC: 2/2/2013 9:48:15 AM
Time stamp (Europe/Moscow): 2/2/2013
1:48:15 PM
Geo coordinates: N 55.74411617, E
37.61313891
Horizontal accuracy: 1414
Altitude: 0
Confidence: 70
Source file: cache_encryptedA.db
Table: CellLocation
MD5 Hash:
6229b52be3391efbe1948361be986339

			Point kind	Point type	Time stamp	Geo coordinates	Address
⊞ ☑			Averaging ...	WiFi point	Device time: 2/2/2013 3:48:28 PM UTC: 2/2/2013 11:48:28 AM	N 55.706412, E 37.623461	Russia, Moscow
⊞ ☑			Averaging ...	Cell point	Device time: 2/2/2013 3:48:21 PM UTC: 2/2/2013 11:48:21 AM	N 55.703322, E 37.620081	Russia, Moscow
☑			Original point	Cell point	Device time: 2/2/2013 1:48:20 PM UTC: 2/2/2013 9:48:20 AM	N/A	N/A
⊞ ☑			Averaging ...	WiFi point	Device time: 2/2/2013 1:48:16 PM UTC: 2/2/2013 9:48:16 AM	N 55.74057, E 37.617268	Russia, Moscow
☑			Original point	Cell point	Device time: 2/2/2013 1:48:15 PM UTC: 2/2/2013 9:48:15 AM	N 55.74411617, E 37.61313891	Russia, Moscow
⊞ ☑			Averaging ...	WiFi point	Device time: 2/2/2013 1:43:47 PM UTC: 2/2/2013 9:43:47 AM	N 55.731845, E 37.606814	Russia, Moscow
☑			Original point	Cell point	Device time: 2/2/2013 1:43:46 PM UTC: 2/2/2013 9:43:46 AM	N/A	N/A
⊞ ☑			Averaging ...	WiFi point	Device time: 2/2/2013 1:43:45 PM UTC: 2/2/2013 9:43:45 AM	N 55.738955, E 37.60813	Russia, Moscow
☑			Original point	Cell point	Device time: 2/2/2013 1:31:44 PM UTC: 2/2/2013 9:31:44 AM	N/A	N/A
☑			Original point	Cell point	Device time: 2/2/2013 1:31:30 PM UTC: 2/2/2013 9:31:30 AM	N/A	N/A
⊞ ☑			Averaging ...	Cell point	Device time: 2/2/2013 1:31:25 PM UTC: 2/2/2013 9:31:25 AM	N 55.740358, E 37.604249	Russia, Moscow

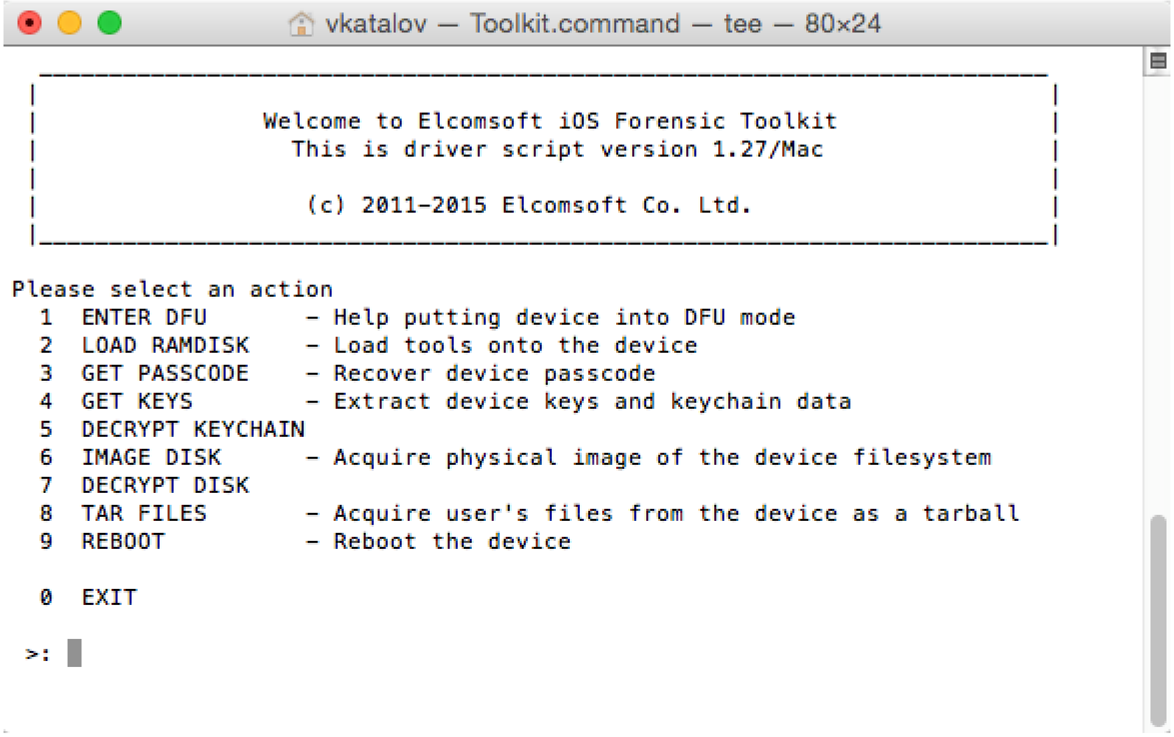
☐ After date:
2/ 1/2013
☐ Before date:
2/ 6/2013
☐ Horizontal accuracy filter:
Enter accuracy in meters ...
☑ Cell Location (776 points)
☑ WiFi Location (10400 points)
☑ Cell Location Harvest (1 poin...
☑ WiFi Location Harvest (29 p...
☑ Cell Location Local (13 points)

Russia, Moscow (N 55.74411617, E 37.61313891)

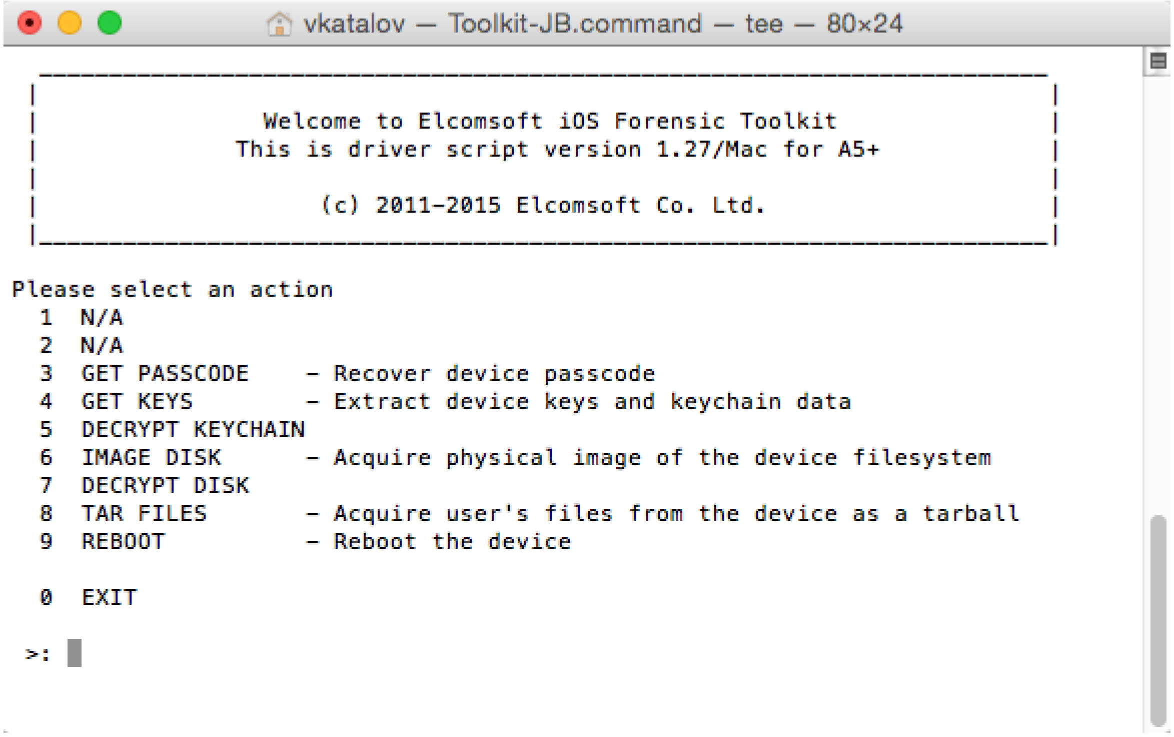
Analyst version: 5.1.2.153 | Simon Payge's iPhone 4S | Total: 11243 objects | Selected: Cell Location (N 55.74411617, E 37.61313891) | MD5 Hash: 6229b52be3391efbe1948361be986339

Elcomsoft iOS Forensic Toolkit
Elcomsoft iOS Forensic Toolkit

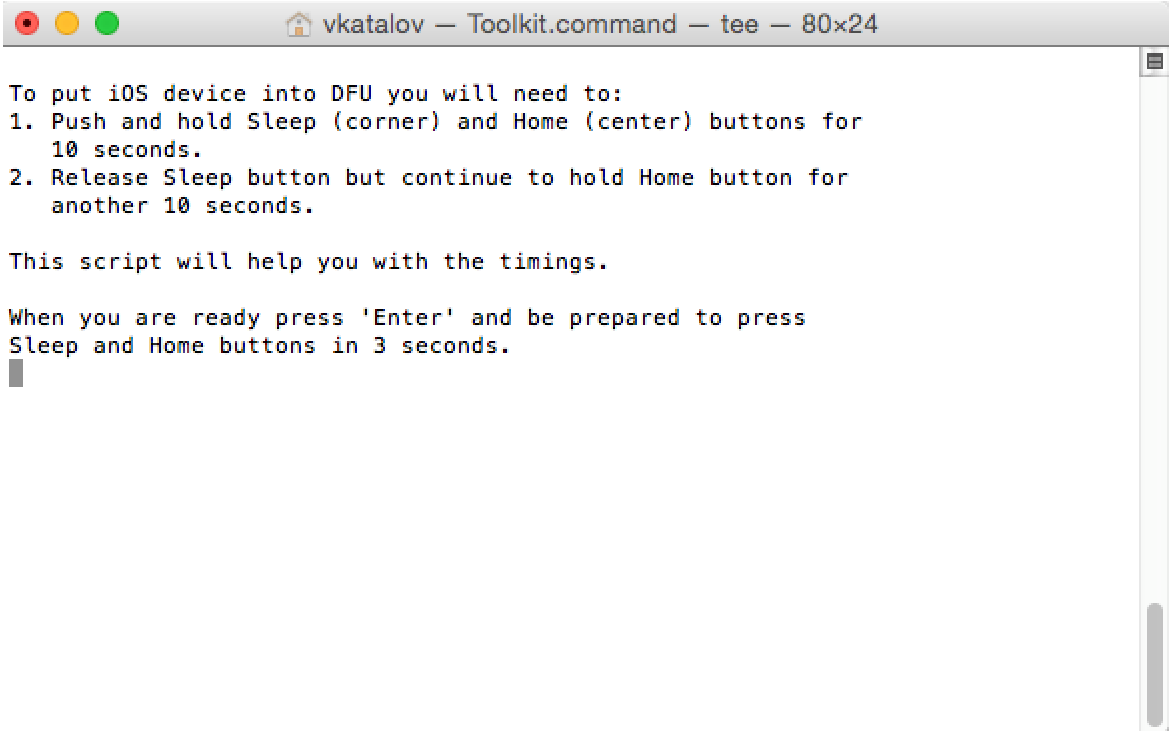
Enter Passcode



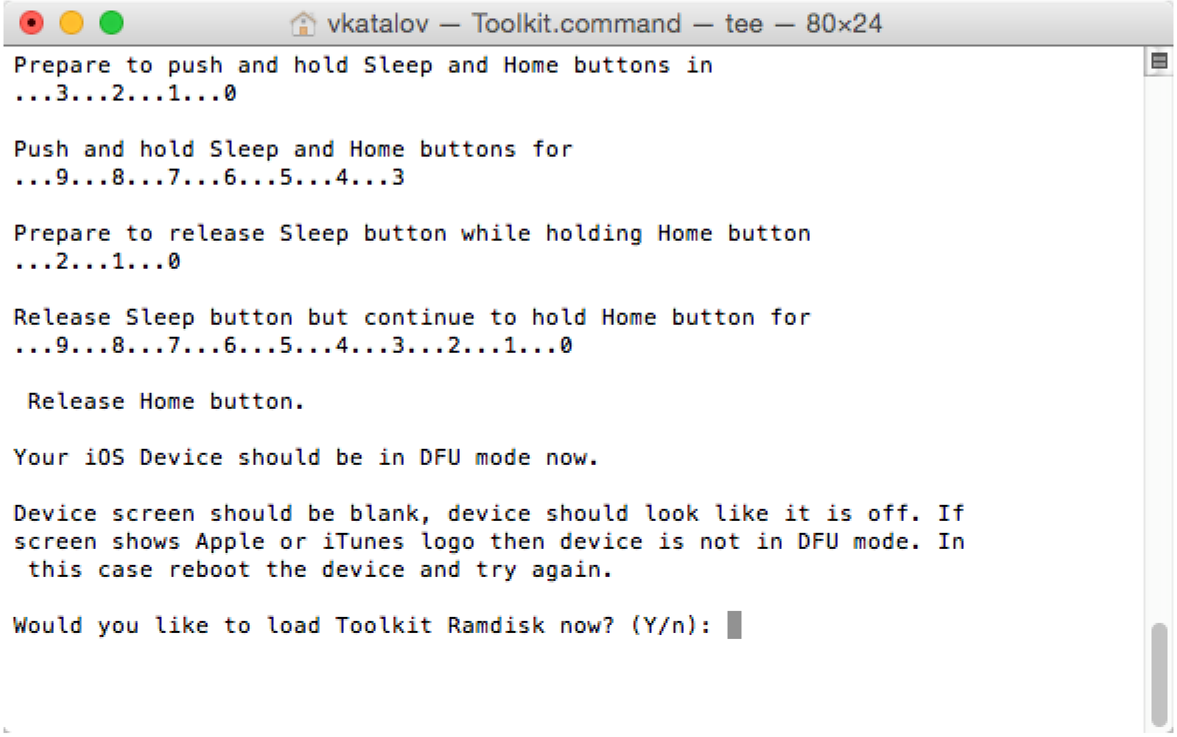
```
  _________________________________________________________________________
 |                                                                         |
 |                Welcome to Elcomsoft iOS Forensic Toolkit                |
 |                  This is driver script version 1.27/Mac                 |
 |                                                                         |
 |                   (c) 2011-2015 Elcomsoft Co. Ltd.                      |
 |_________________________________________________________________________|

Please select an action
  1  ENTER DFU       - Help putting device into DFU mode
  2  LOAD RAMDISK    - Load tools onto the device
  3  GET PASSCODE    - Recover device passcode
  4  GET KEYS        - Extract device keys and keychain data
  5  DECRYPT KEYCHAIN
  6  IMAGE DISK      - Acquire physical image of the device filesystem
  7  DECRYPT DISK
  8  TAR FILES       - Acquire user's files from the device as a tarball
  9  REBOOT          - Reboot the device

  0  EXIT

 >: 
```



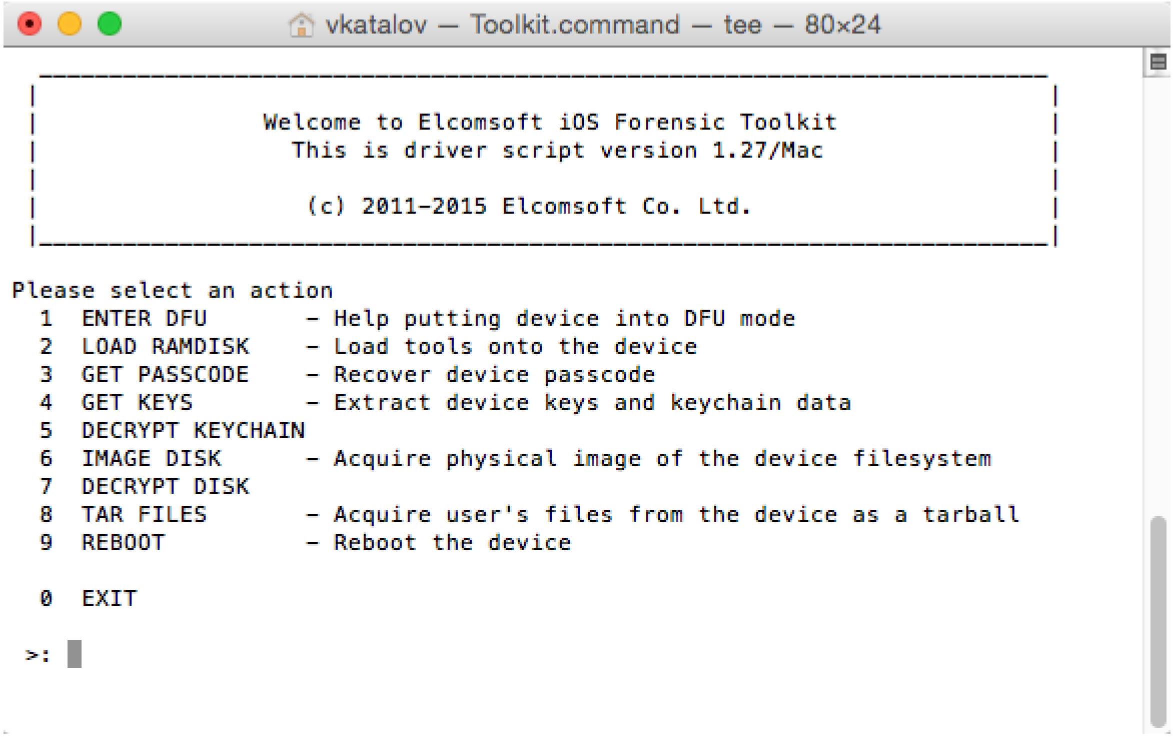
```
  _________________________________________________________________________
 |                                                                         |
 |                Welcome to Elcomsoft iOS Forensic Toolkit                |
 |              This is driver script version 1.27/Mac for A5+             |
 |                                                                         |
 |                    (c) 2011-2015 Elcomsoft Co. Ltd.                     |
 |_________________________________________________________________________|

Please select an action
  1  N/A
  2  N/A
  3  GET PASSCODE    - Recover device passcode
  4  GET KEYS        - Extract device keys and keychain data
  5  DECRYPT KEYCHAIN
  6  IMAGE DISK      - Acquire physical image of the device filesystem
  7  DECRYPT DISK
  8  TAR FILES       - Acquire user's files from the device as a tarball
  9  REBOOT          - Reboot the device

  0  EXIT

 >: 
```



```
To put iOS device into DFU you will need to:
1. Push and hold Sleep (corner) and Home (center) buttons for
   10 seconds.
2. Release Sleep button but continue to hold Home button for
   another 10 seconds.

This script will help you with the timings.

When you are ready press 'Enter' and be prepared to press
Sleep and Home buttons in 3 seconds.
```

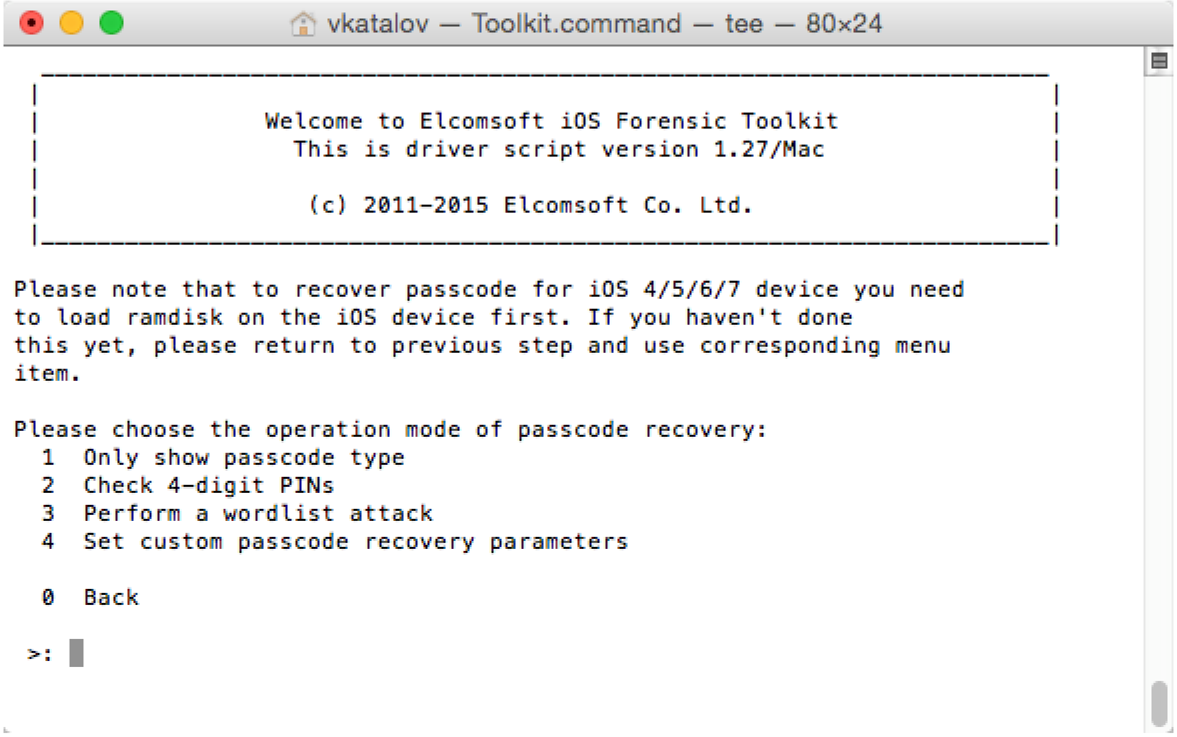


```
Prepare to push and hold Sleep and Home buttons in
...3...2...1...0

Push and hold Sleep and Home buttons for
...9...8...7...6...5...4...3

Prepare to release Sleep button while holding Home button
...2...1...0

Release Sleep button but continue to hold Home button for
...9...8...7...6...5...4...3...2...1...0

 Release Home button.

Your iOS Device should be in DFU mode now.

Device screen should be blank, device should look like it is off. If
screen shows Apple or iTunes logo then device is not in DFU mode. In
 this case reboot the device and try again.

Would you like to load Toolkit Ramdisk now? (Y/n):
```

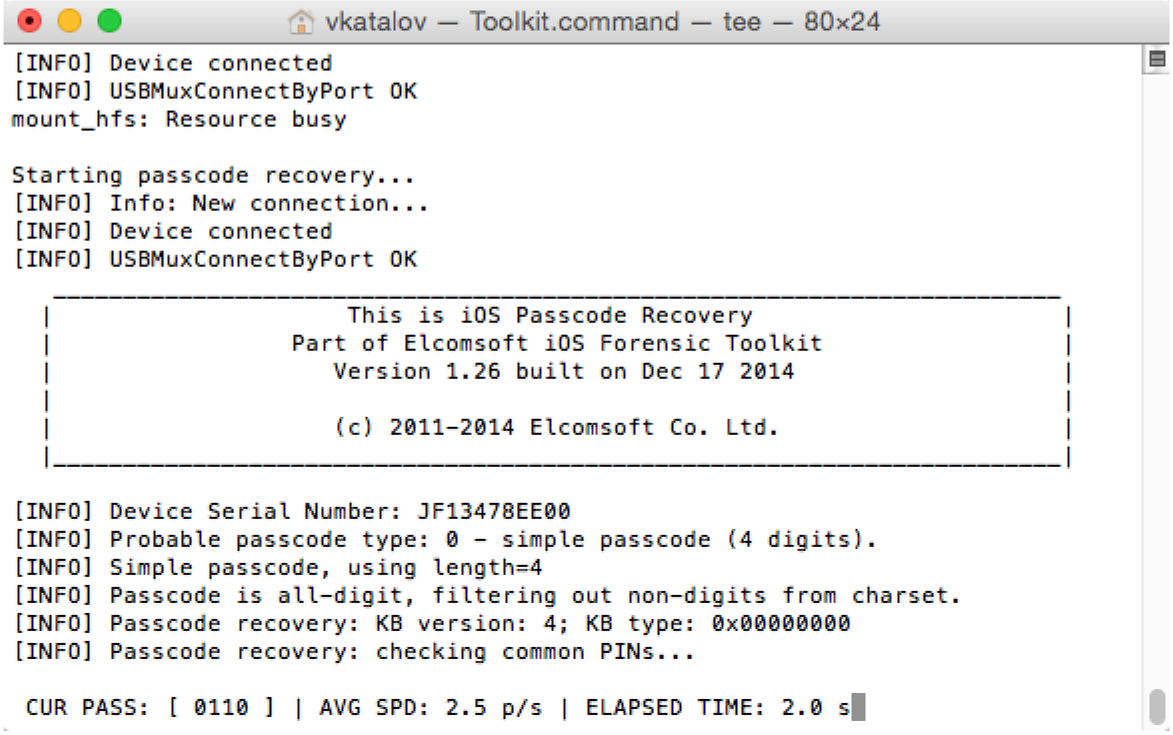


```
 ________________________________________________________________________
|                                                                        |
|                 Welcome to Elcomsoft iOS Forensic Toolkit              |
|                   This is driver script version 1.27/Mac               |
|                                                                        |
|                    (c) 2011-2015 Elcomsoft Co. Ltd.                    |
|________________________________________________________________________|

Please select an action
  1  ENTER DFU        - Help putting device into DFU mode
  2  LOAD RAMDISK     - Load tools onto the device
  3  GET PASSCODE     - Recover device passcode
  4  GET KEYS         - Extract device keys and keychain data
  5  DECRYPT KEYCHAIN
  6  IMAGE DISK       - Acquire physical image of the device filesystem
  7  DECRYPT DISK
  8  TAR FILES        - Acquire user's files from the device as a tarball
  9  REBOOT           - Reboot the device

  0  EXIT

 >:
```

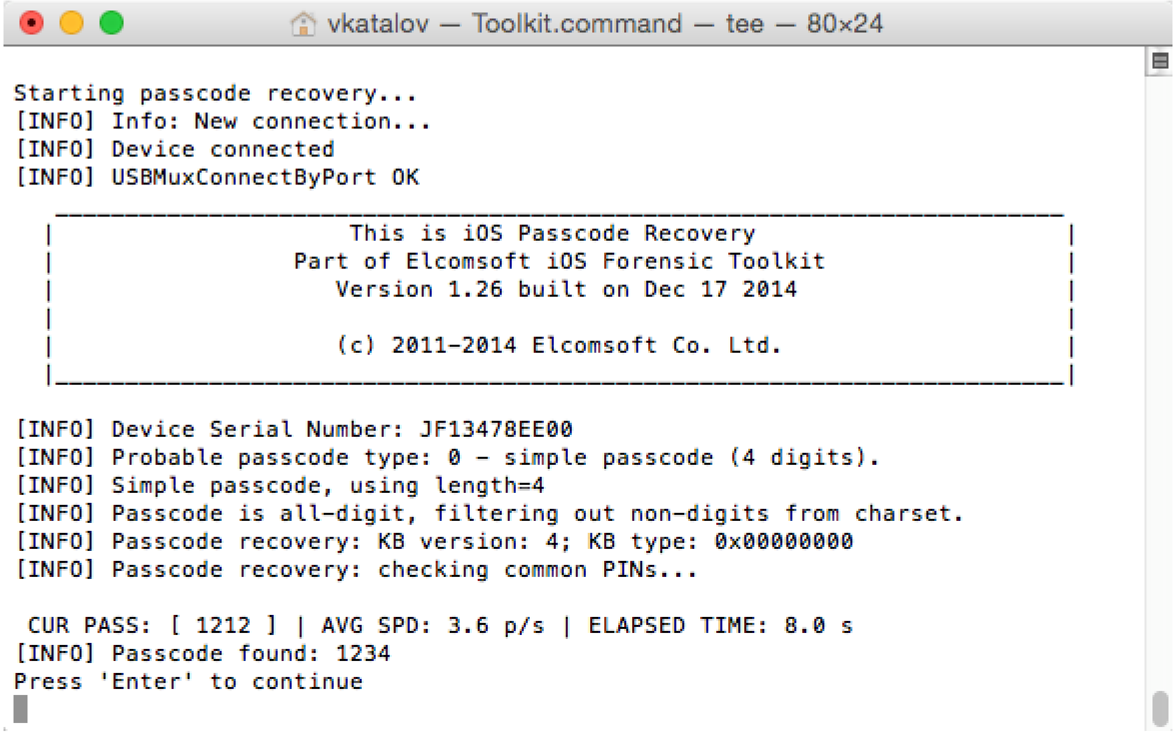
Elcomsoft iOS Forensic Toolkit
Elcomsoft iOS Forensic Toolkit
nsic Toolkit



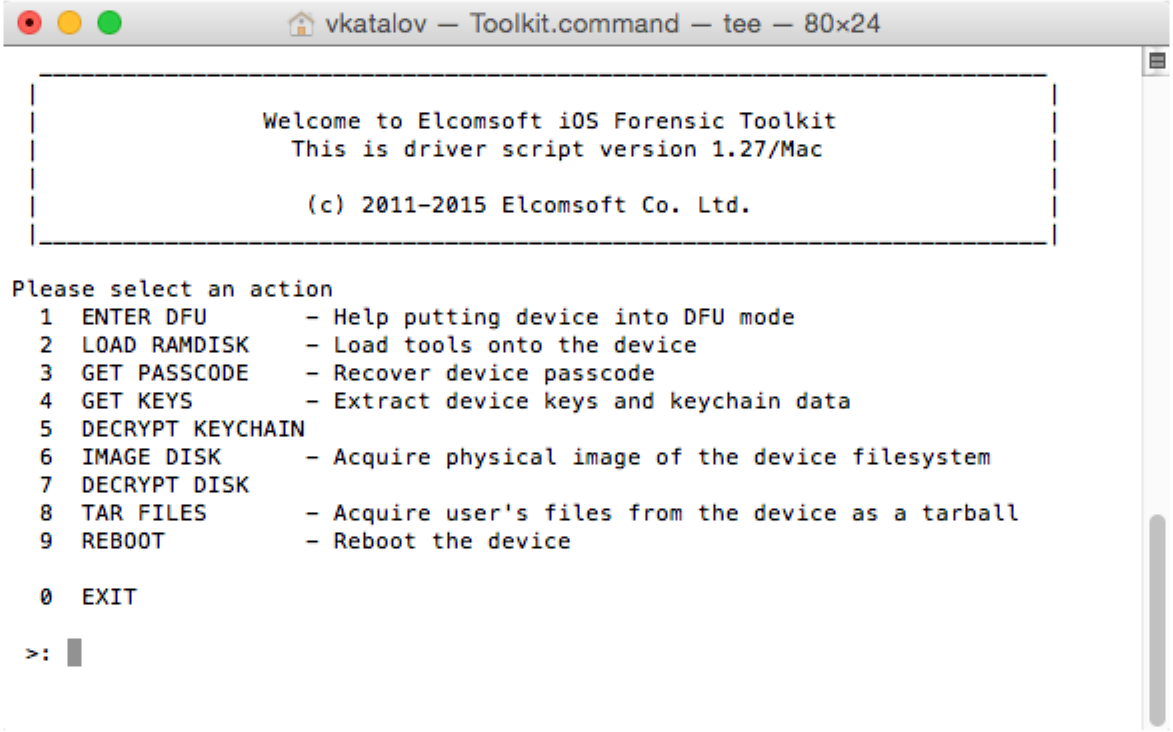
```
  ________________________________________________________________________
 |                                                                        |
 |                Welcome to Elcomsoft iOS Forensic Toolkit               |
 |                  This is driver script version 1.27/Mac               |
 |                                                                        |
 |                   (c) 2011-2015 Elcomsoft Co. Ltd.                     |
 |________________________________________________________________________|

Please note that to recover passcode for iOS 4/5/6/7 device you need
to load ramdisk on the iOS device first. If you haven't done
this yet, please return to previous step and use corresponding menu
item.

Please choose the operation mode of passcode recovery:
  1  Only show passcode type
  2  Check 4-digit PINs
  3  Perform a wordlist attack
  4  Set custom passcode recovery parameters

  0  Back

 >:
```



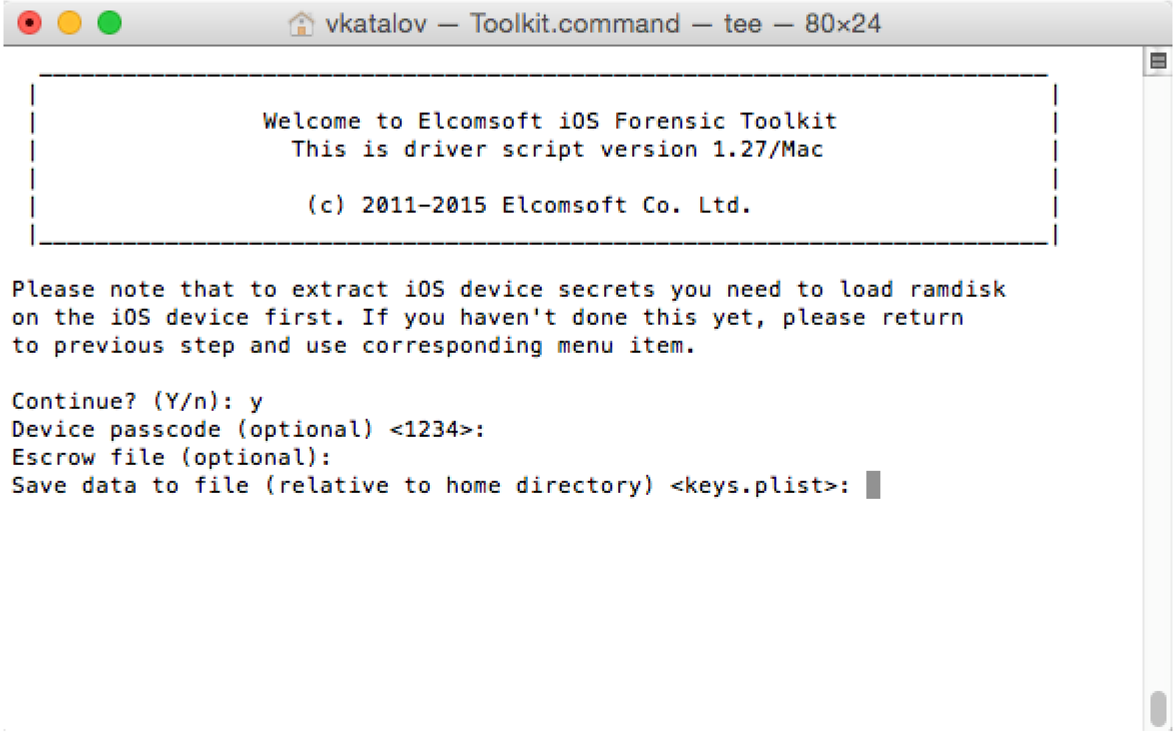
```
[INFO] Device connected
[INFO] USBMuxConnectByPort OK
mount_hfs: Resource busy

Starting passcode recovery...
[INFO] Info: New connection...
[INFO] Device connected
[INFO] USBMuxConnectByPort OK
   ________________________________________________________________________
  |                       This is iOS Passcode Recovery                    |
  |                   Part of Elcomsoft iOS Forensic Toolkit               |
  |                      Version 1.26 built on Dec 17 2014                 |
  |                                                                        |
  |                      (c) 2011-2014 Elcomsoft Co. Ltd.                  |
  |________________________________________________________________________|

[INFO] Device Serial Number: JF13478EE00
[INFO] Probable passcode type: 0 - simple passcode (4 digits).
[INFO] Simple passcode, using length=4
[INFO] Passcode is all-digit, filtering out non-digits from charset.
[INFO] Passcode recovery: KB version: 4; KB type: 0x00000000
[INFO] Passcode recovery: checking common PINs...

 CUR PASS: [ 0110 ] | AVG SPD: 2.5 p/s | ELAPSED TIME: 2.0 s
```



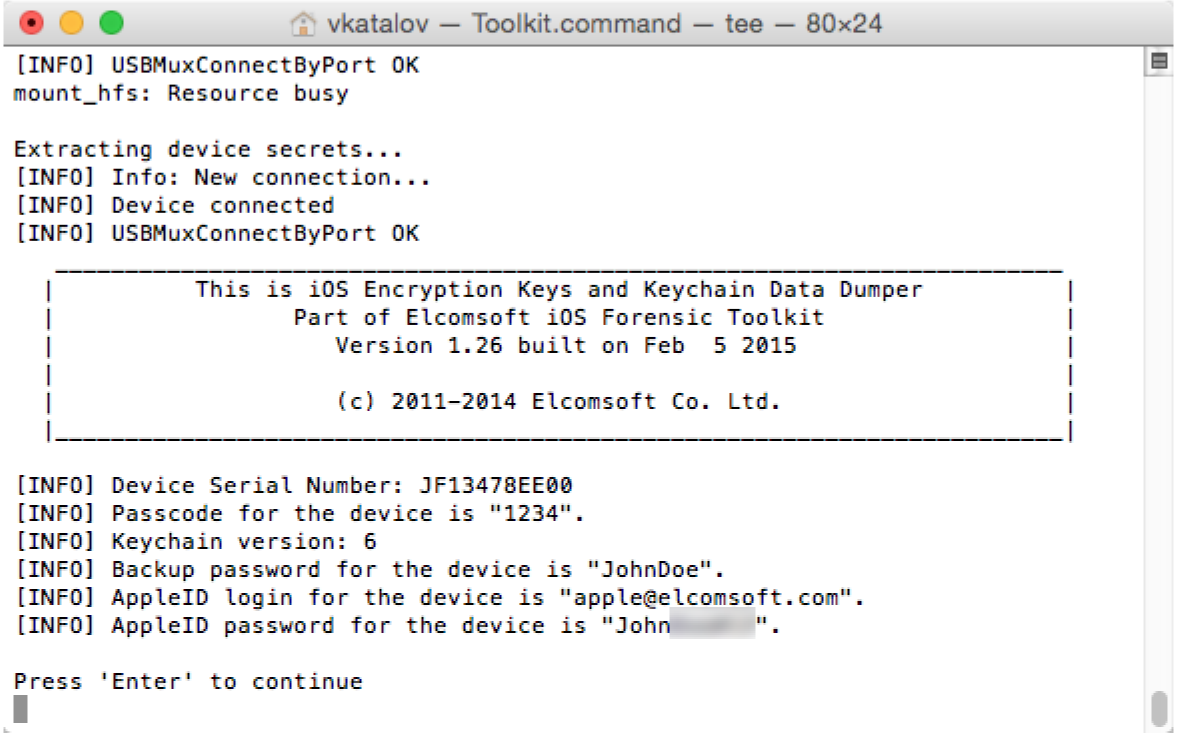
```
Starting passcode recovery...
[INFO] Info: New connection...
[INFO] Device connected
[INFO] USBMuxConnectByPort OK
    __________________________________________________________________________
   |                      This is iOS Passcode Recovery                       |
   |                  Part of Elcomsoft iOS Forensic Toolkit                  |
   |                     Version 1.26 built on Dec 17 2014                    |
   |                                                                          |
   |                     (c) 2011-2014 Elcomsoft Co. Ltd.                     |
   |__________________________________________________________________________|

[INFO] Device Serial Number: JF13478EE00
[INFO] Probable passcode type: 0 - simple passcode (4 digits).
[INFO] Simple passcode, using length=4
[INFO] Passcode is all-digit, filtering out non-digits from charset.
[INFO] Passcode recovery: KB version: 4; KB type: 0x00000000
[INFO] Passcode recovery: checking common PINs...

 CUR PASS: [ 1212 ] | AVG SPD: 3.6 p/s | ELAPSED TIME: 8.0 s
[INFO] Passcode found: 1234
Press 'Enter' to continue
```



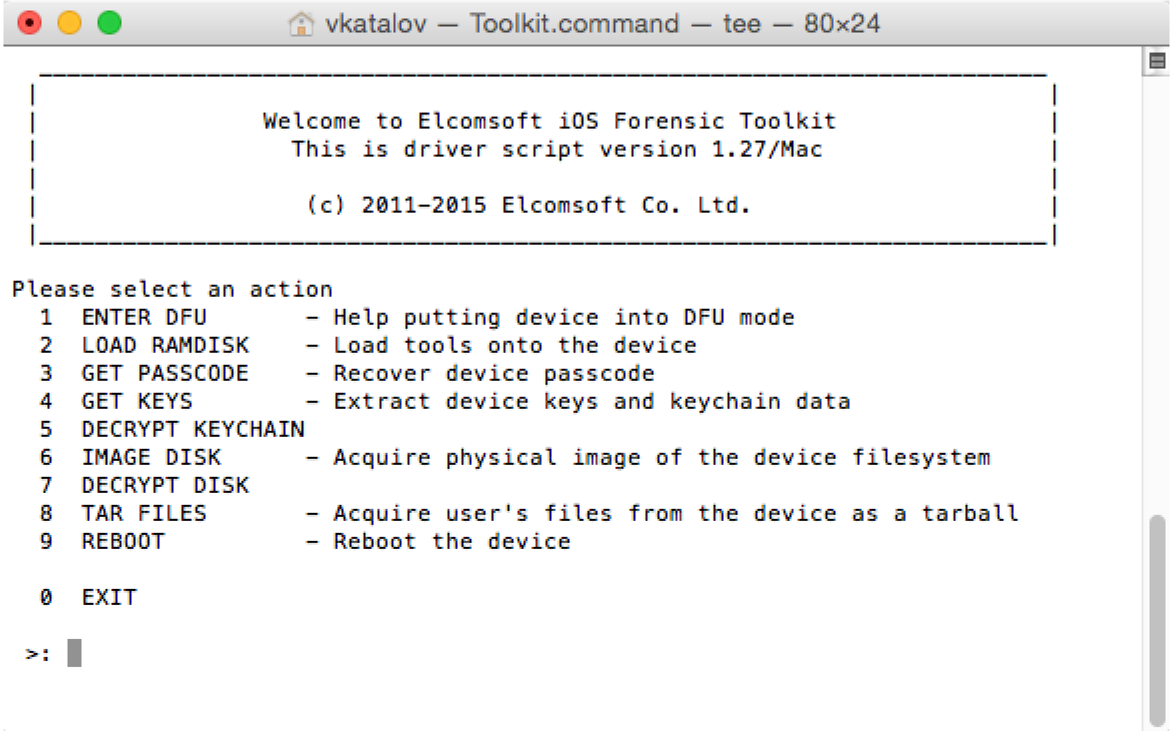
```
  __________________________________________________________________________
 |                                                                          |
 |                  Welcome to Elcomsoft iOS Forensic Toolkit               |
 |                    This is driver script version 1.27/Mac                |
 |                                                                          |
 |                     (c) 2011-2015 Elcomsoft Co. Ltd.                     |
 |__________________________________________________________________________|

Please select an action
  1  ENTER DFU        - Help putting device into DFU mode
  2  LOAD RAMDISK     - Load tools onto the device
  3  GET PASSCODE     - Recover device passcode
  4  GET KEYS         - Extract device keys and keychain data
  5  DECRYPT KEYCHAIN
  6  IMAGE DISK       - Acquire physical image of the device filesystem
  7  DECRYPT DISK
  8  TAR FILES        - Acquire user's files from the device as a tarball
  9  REBOOT           - Reboot the device

  0  EXIT

 >:
```



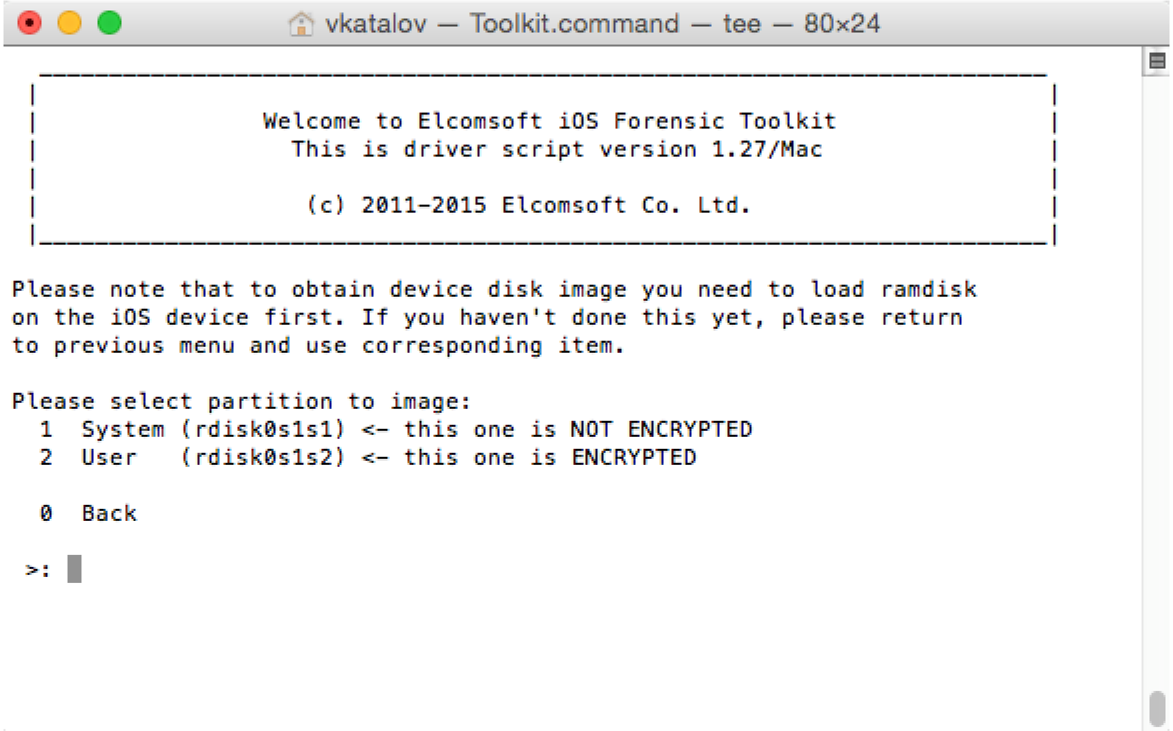
```
  ___________________________________________________________________________
 |                                                                           |
 |                Welcome to Elcomsoft iOS Forensic Toolkit                  |
 |                  This is driver script version 1.27/Mac                   |
 |                                                                           |
 |                   (c) 2011-2015 Elcomsoft Co. Ltd.                        |
 |___________________________________________________________________________|

Please note that to extract iOS device secrets you need to load ramdisk
on the iOS device first. If you haven't done this yet, please return
to previous step and use corresponding menu item.

Continue? (Y/n): y
Device passcode (optional) <1234>:
Escrow file (optional):
Save data to file (relative to home directory) <keys.plist>: 
```



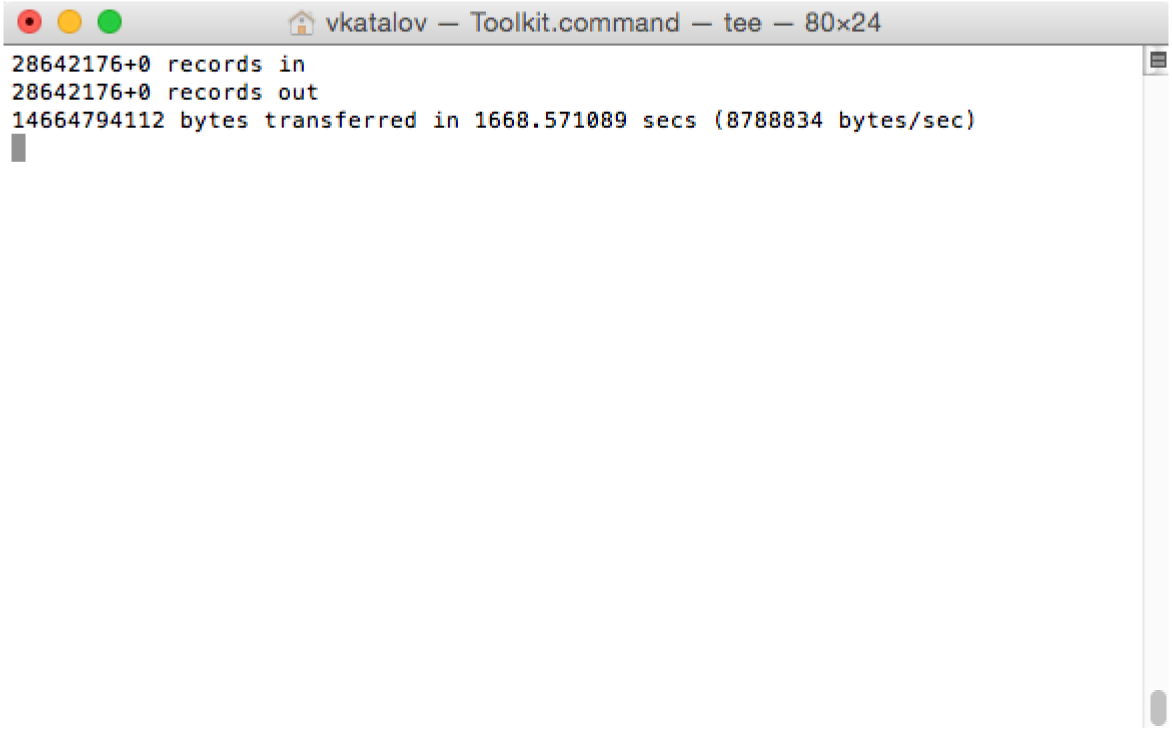
```
[INFO] USBMuxConnectByPort OK
mount_hfs: Resource busy

Extracting device secrets...
[INFO] Info: New connection...
[INFO] Device connected
[INFO] USBMuxConnectByPort OK
   ___________________________________________________________________________
  |          This is iOS Encryption Keys and Keychain Data Dumper             |
  |                 Part of Elcomsoft iOS Forensic Toolkit                    |
  |                    Version 1.26 built on Feb  5 2015                      |
  |                                                                           |
  |                    (c) 2011-2014 Elcomsoft Co. Ltd.                       |
  |___________________________________________________________________________|

[INFO] Device Serial Number: JF13478EE00
[INFO] Passcode for the device is "1234".
[INFO] Keychain version: 6
[INFO] Backup password for the device is "JohnDoe".
[INFO] AppleID login for the device is "apple@elcomsoft.com".
[INFO] AppleID password for the device is "John[redacted]".

Press 'Enter' to continue
```



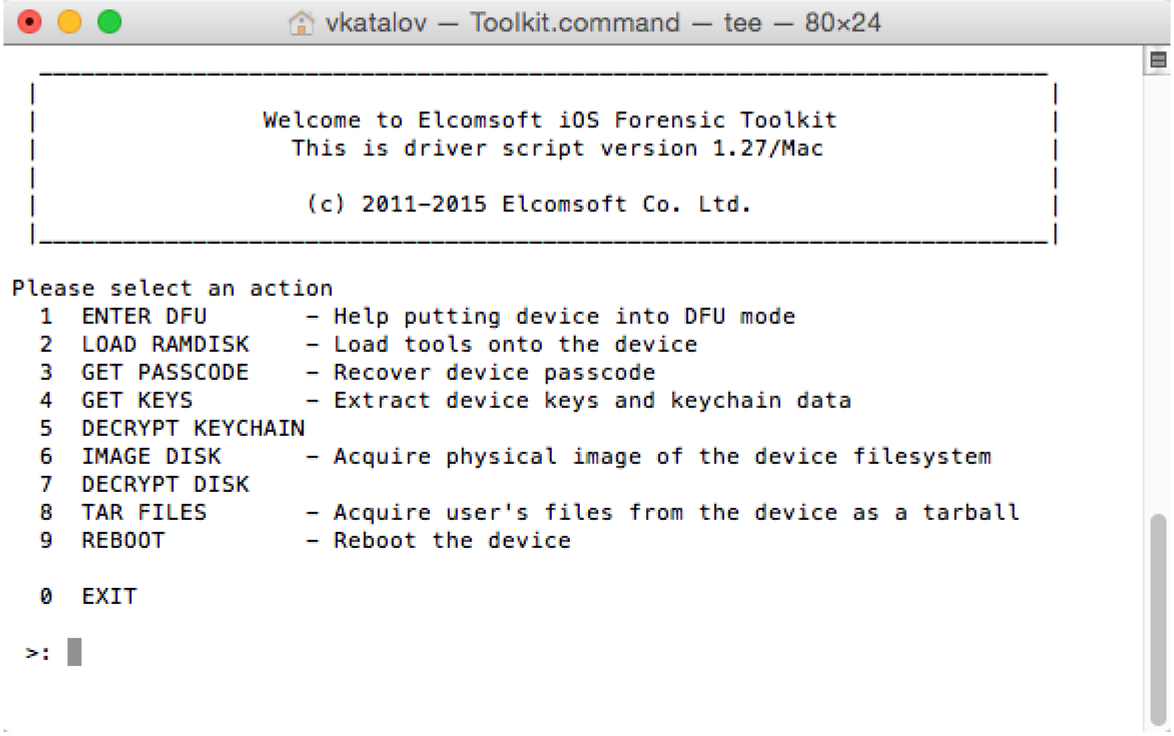
```
 ________________________________________________________________________
|                                                                        |
|                Welcome to Elcomsoft iOS Forensic Toolkit               |
|                  This is driver script version 1.27/Mac                |
|                                                                        |
|                   (c) 2011-2015 Elcomsoft Co. Ltd.                     |
|________________________________________________________________________|

Please select an action
  1  ENTER DFU        - Help putting device into DFU mode
  2  LOAD RAMDISK     - Load tools onto the device
  3  GET PASSCODE     - Recover device passcode
  4  GET KEYS         - Extract device keys and keychain data
  5  DECRYPT KEYCHAIN
  6  IMAGE DISK       - Acquire physical image of the device filesystem
  7  DECRYPT DISK
  8  TAR FILES        - Acquire user's files from the device as a tarball
  9  REBOOT           - Reboot the device

  0  EXIT

 >:
```



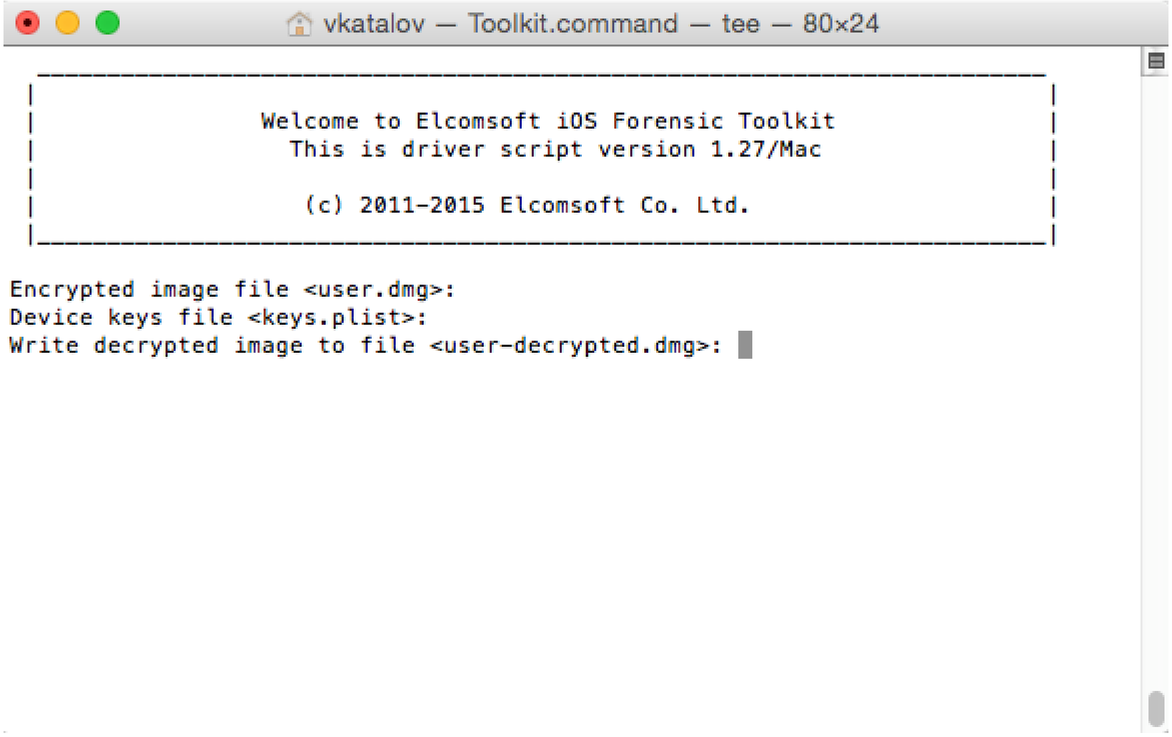
```
 ________________________________________________________________________
|                                                                        |
|                Welcome to Elcomsoft iOS Forensic Toolkit               |
|                  This is driver script version 1.27/Mac                |
|                                                                        |
|                   (c) 2011-2015 Elcomsoft Co. Ltd.                     |
|________________________________________________________________________|

Please note that to obtain device disk image you need to load ramdisk
on the iOS device first. If you haven't done this yet, please return
to previous menu and use corresponding item.

Please select partition to image:
  1  System (rdisk0s1s1) <- this one is NOT ENCRYPTED
  2  User   (rdisk0s1s2) <- this one is ENCRYPTED

  0  Back

 >:
```



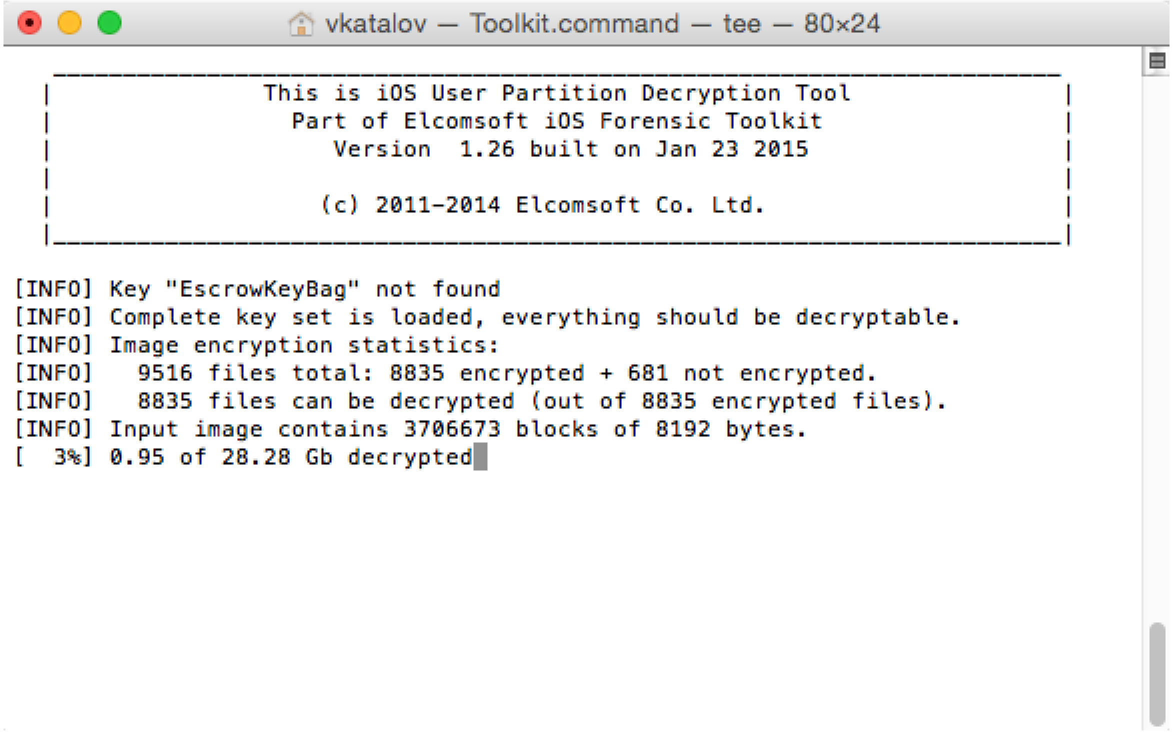
```
28642176+0 records in
28642176+0 records out
14664794112 bytes transferred in 1668.571089 secs (8788834 bytes/sec)
```



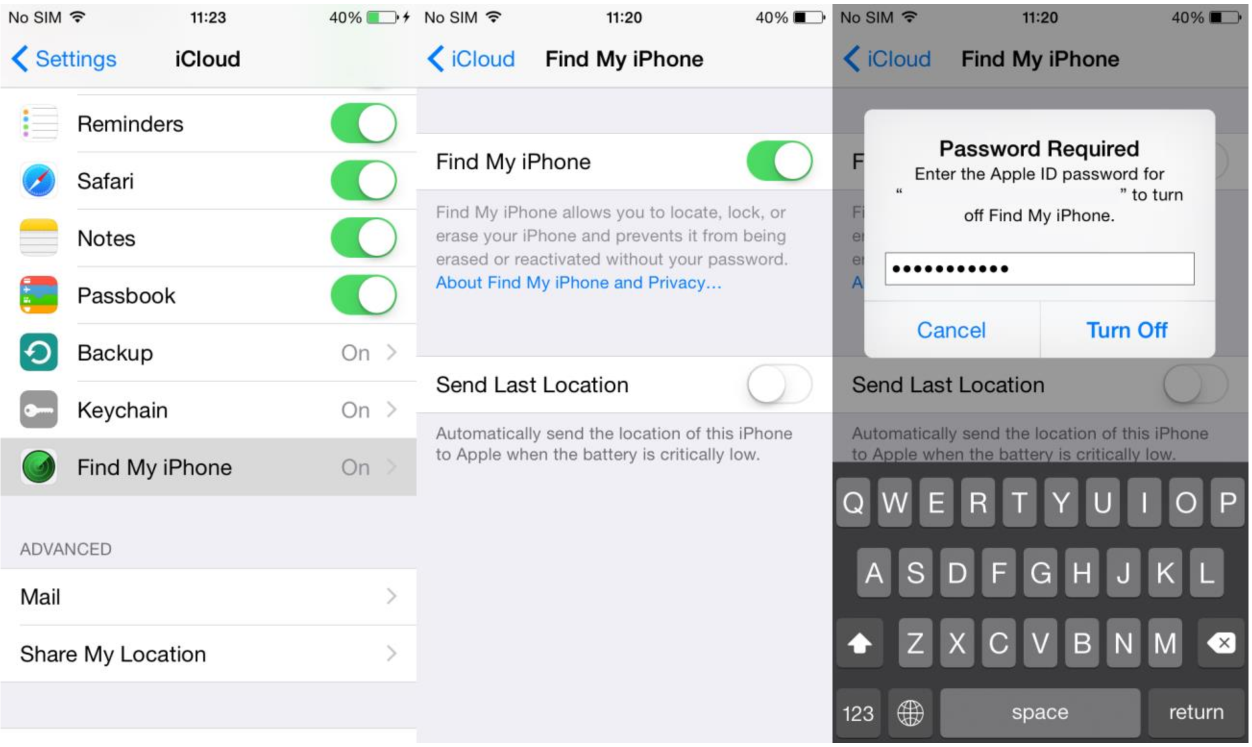
```
  _________________________________________________________________________
 |                                                                         |
 |                Welcome to Elcomsoft iOS Forensic Toolkit                |
 |                  This is driver script version 1.27/Mac                 |
 |                                                                         |
 |                   (c) 2011-2015 Elcomsoft Co. Ltd.                      |
 |_________________________________________________________________________|

Please select an action
  1  ENTER DFU       - Help putting device into DFU mode
  2  LOAD RAMDISK    - Load tools onto the device
  3  GET PASSCODE    - Recover device passcode
  4  GET KEYS        - Extract device keys and keychain data
  5  DECRYPT KEYCHAIN
  6  IMAGE DISK      - Acquire physical image of the device filesystem
  7  DECRYPT DISK
  8  TAR FILES       - Acquire user's files from the device as a tarball
  9  REBOOT          - Reboot the device

  0  EXIT

 >:
```



```
  ________________________________________________________________________
 |                                                                        |
 |                Welcome to Elcomsoft iOS Forensic Toolkit               |
 |                  This is driver script version 1.27/Mac                |
 |                                                                        |
 |                   (c) 2011-2015 Elcomsoft Co. Ltd.                     |
 |________________________________________________________________________|

Encrypted image file <user.dmg>:
Device keys file <keys.plist>:
Write decrypted image to file <user-decrypted.dmg>:
```



```
  ________________________________________________________________________
 |               This is iOS User Partition Decryption Tool               |
 |                  Part of Elcomsoft iOS Forensic Toolkit                |
 |                     Version  1.26 built on Jan 23 2015                 |
 |                                                                        |
 |                   (c) 2011-2014 Elcomsoft Co. Ltd.                     |
 |________________________________________________________________________|

[INFO] Key "EscrowKeyBag" not found
[INFO] Complete key set is loaded, everything should be decryptable.
[INFO] Image encryption statistics:
[INFO]   9516 files total: 8835 encrypted + 681 not encrypted.
[INFO]   8835 files can be decrypted (out of 8835 encrypted files).
[INFO] Input image contains 3706673 blocks of 8192 bytes.
[  3%] 0.95 of 28.28 Gb decrypted
```



No SIM 11:23 40%

Settings iCloud

Reminders ●

Safari ●

Notes ●

Passbook ●

Backup On >

Keychain On >

Find My iPhone On >

ADVANCED

Mail >

Share My Location >

No SIM 11:20 40%

iCloud Find My iPhone

Find My iPhone ●

Find My iPhone allows you to locate, lock, or erase your iPhone and prevents it from being erased or reactivated without your password. About Find My iPhone and Privacy…

Send Last Location ○

Automatically send the location of this iPhone to Apple when the battery is critically low.

No SIM 11:20 40%

iCloud Find My iPhone

Password Required

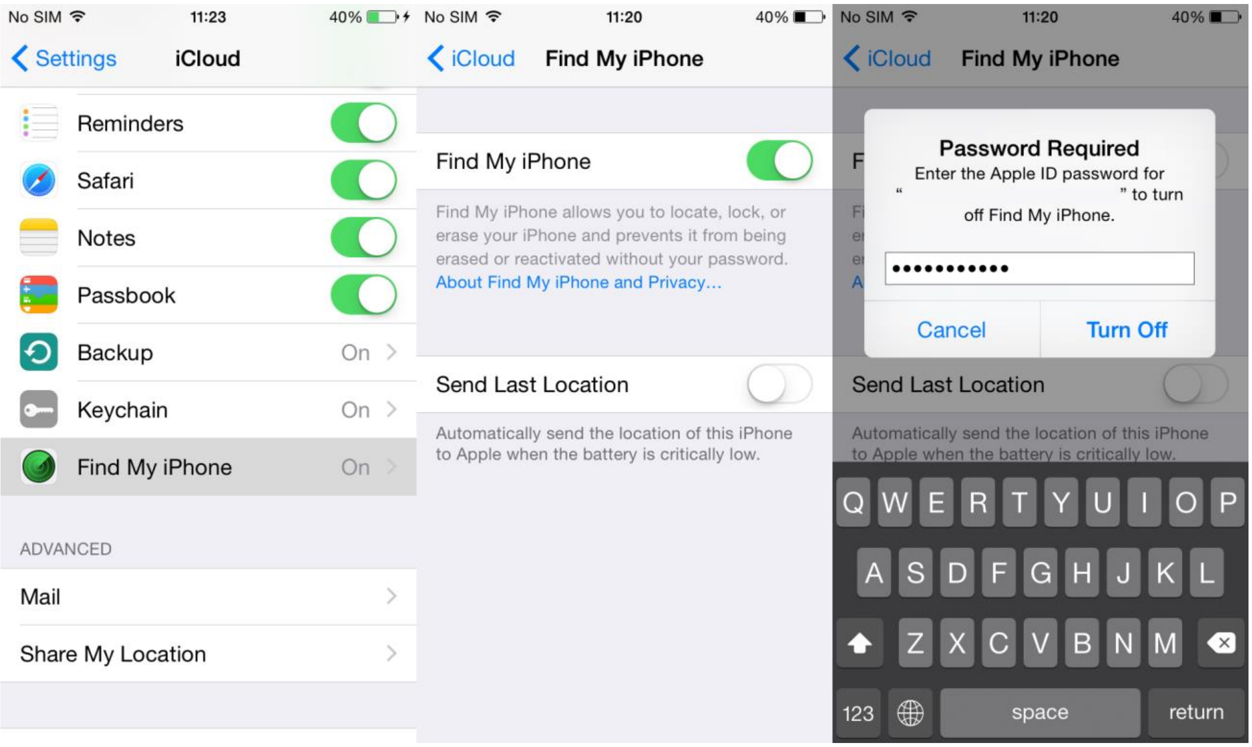
Enter the Apple ID password for “ ” to turn off Find My iPhone.

•••••••••••

Cancel Turn Off

Send Last Location ○

Automatically send the location of this iPhone to Apple when the battery is critically low.



No SIM 11:23 40%

Settings iCloud

Reminders ●

Safari ●

Notes ●

Passbook ●

Backup On >

Keychain On >

Find My iPhone On >

ADVANCED

Mail >

Share My Location >

No SIM 11:20 40%

iCloud Find My iPhone

Find My iPhone ●

Find My iPhone allows you to locate, lock, or erase your iPhone and prevents it from being erased or reactivated without your password. About Find My iPhone and Privacy…

Send Last Location ○

Automatically send the location of this iPhone to Apple when the battery is critically low.

No SIM 11:20 40%

iCloud Find My iPhone

Password Required

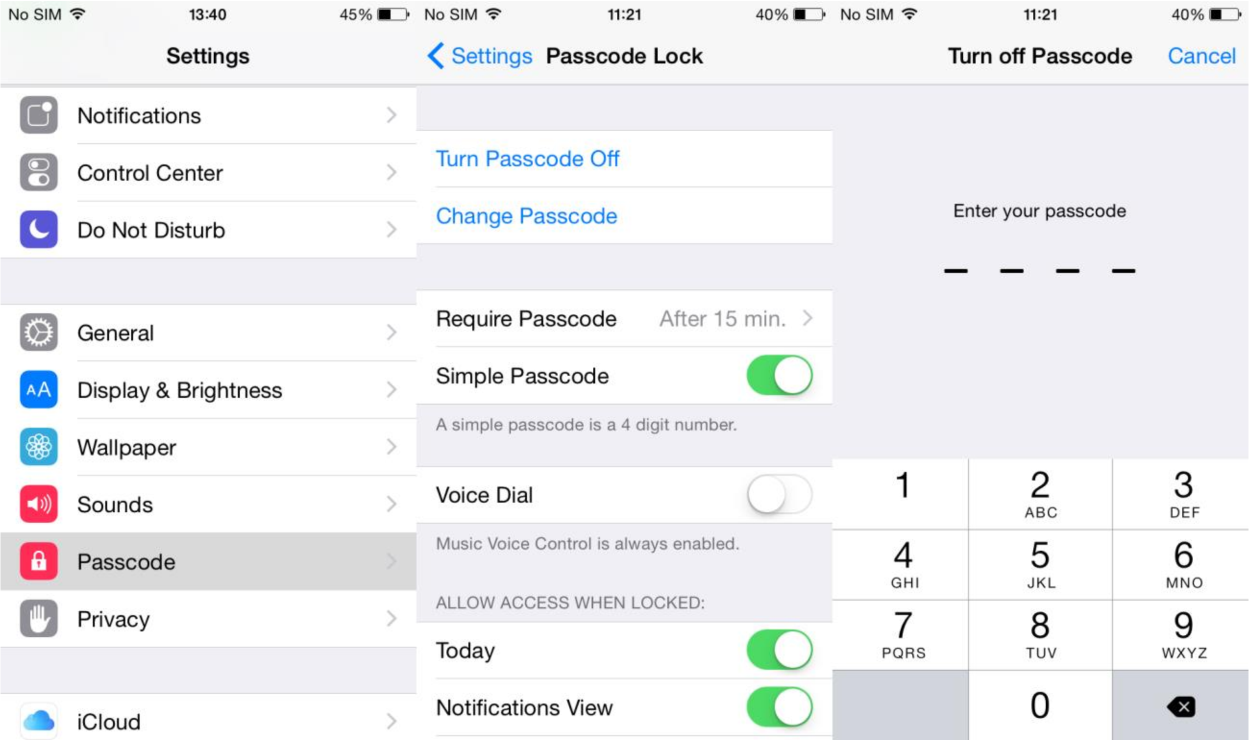
Enter the Apple ID password for “ ” to turn off Find My iPhone.

•••••••••••

Cancel Turn Off

Send Last Location ○

Automatically send the location of this iPhone to Apple when the battery is critically low.



Require Passcode After 15 min.

Simple Passcode

A simple passcode is a 4 digit number.

Voice Dial

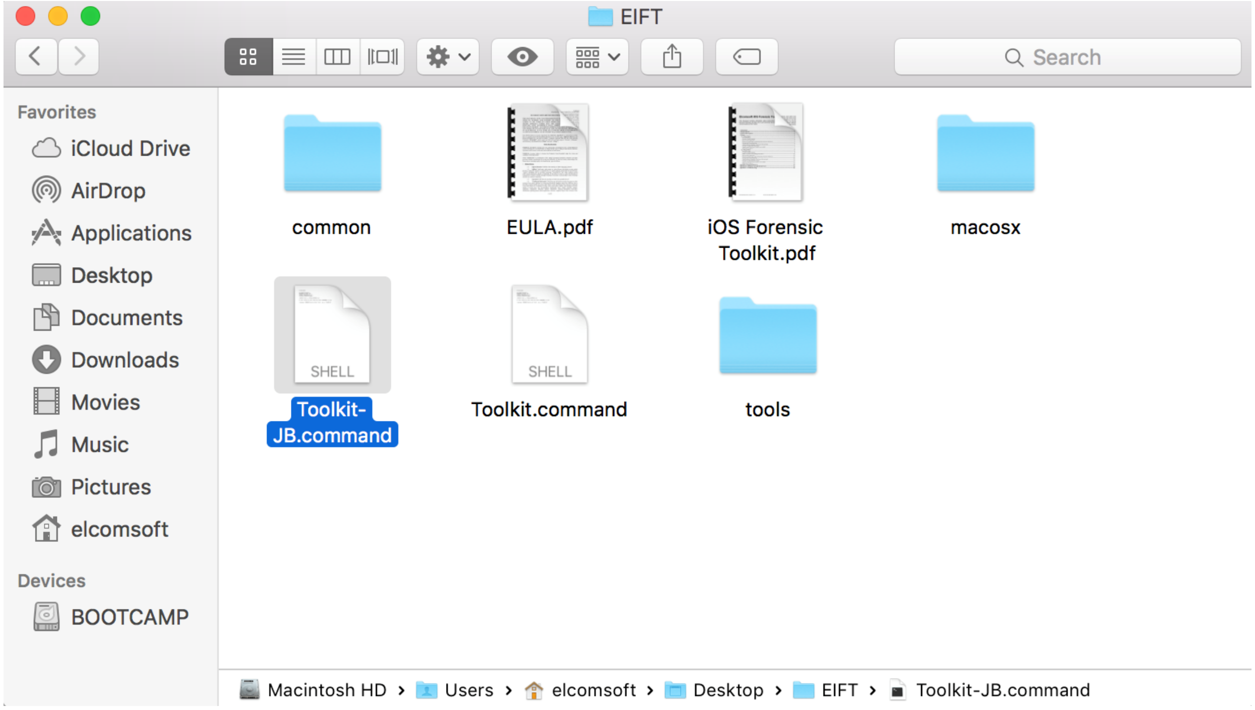
Music Voice Control is always enabled.

ALLOW ACCESS WHEN LOCKED:

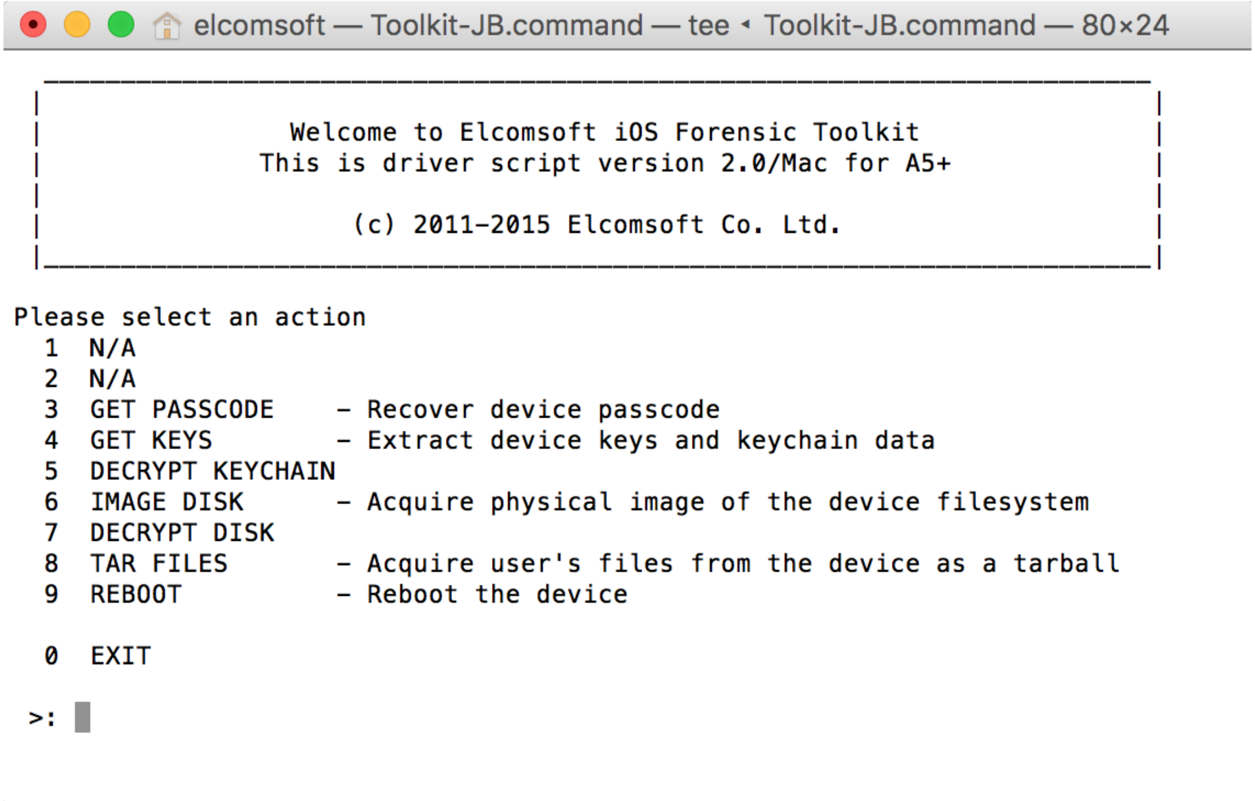
Today

Notifications View

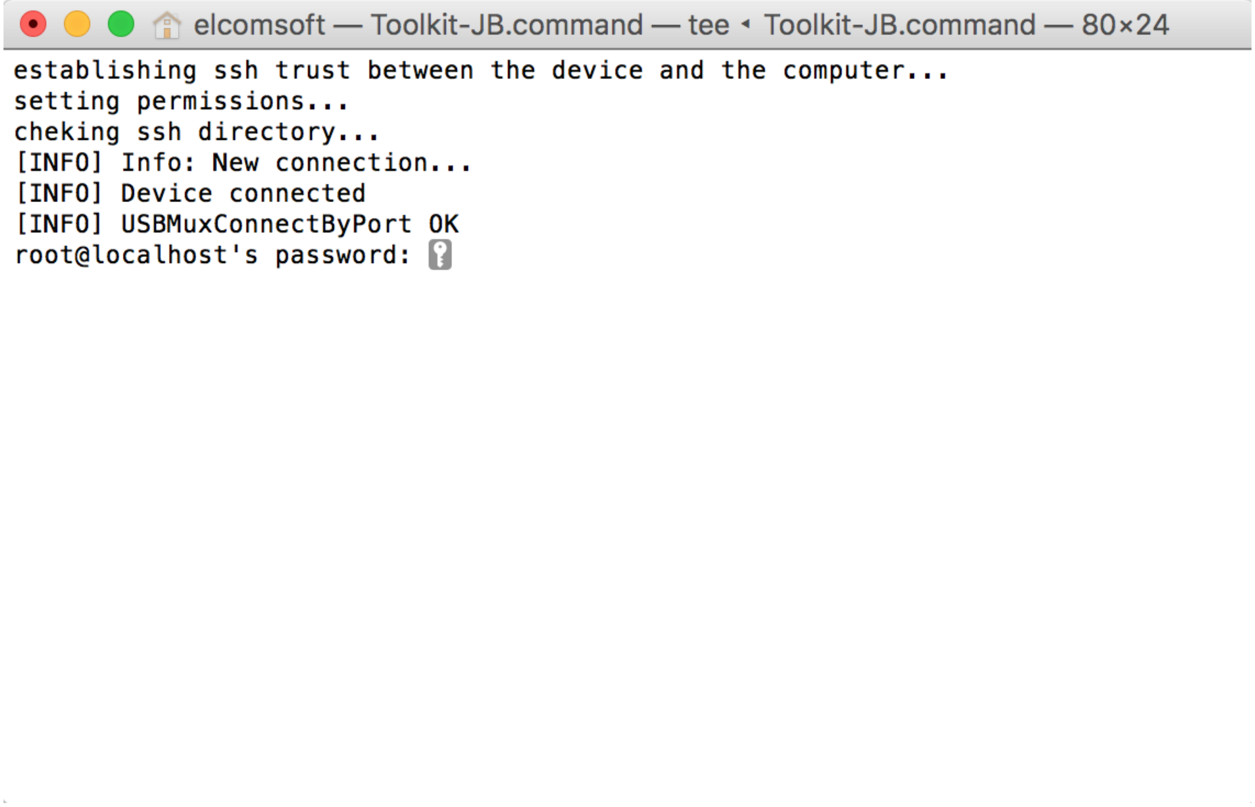
Enter your passcode



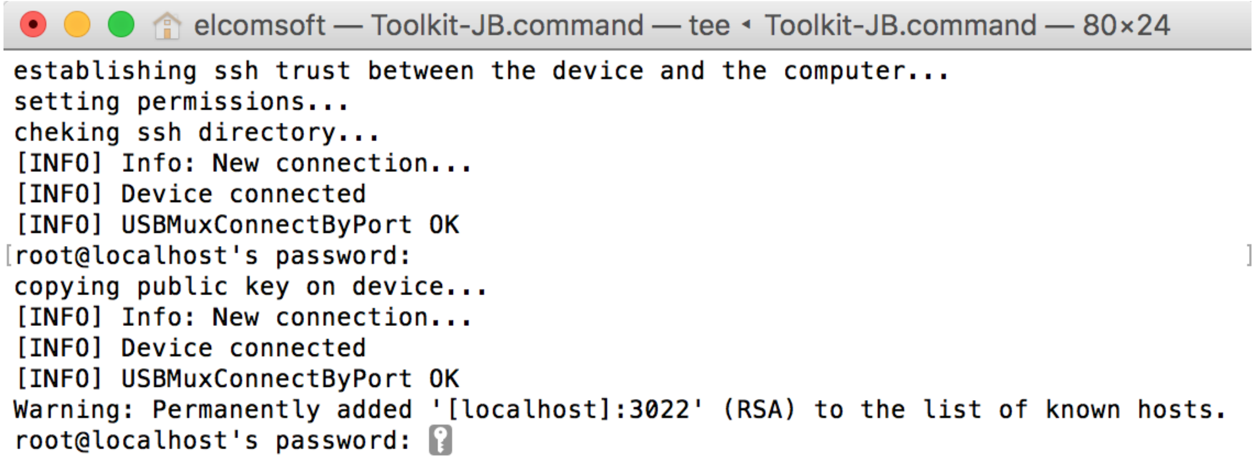
Macintosh HD › Users › elcomsoft › Desktop › EIFT › Toolkit-JB.command


elcomsoft — Toolkit-JB.command — tee ◂ Toolkit-JB.command — 80×24

```
 ________________________________________________________________________
|                                                                        |
|                 Welcome to Elcomsoft iOS Forensic Toolkit              |
|               This is driver script version 2.0/Mac for A5+            |
|                                                                        |
|                     (c) 2011-2015 Elcomsoft Co. Ltd.                   |
|________________________________________________________________________|

Please select an action
  1  N/A
  2  N/A
  3  GET PASSCODE      - Recover device passcode
  4  GET KEYS          - Extract device keys and keychain data
  5  DECRYPT KEYCHAIN
  6  IMAGE DISK        - Acquire physical image of the device filesystem
  7  DECRYPT DISK
  8  TAR FILES         - Acquire user's files from the device as a tarball
  9  REBOOT            - Reboot the device

  0  EXIT

 >:
```

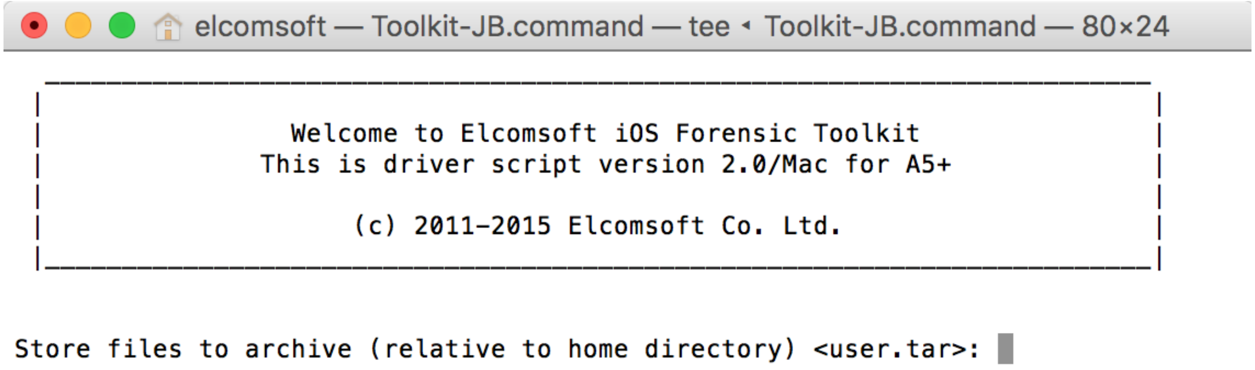

elcomsoft — Toolkit-JB.command — tee ◂ Toolkit-JB.command — 80×24

```
establishing ssh trust between the device and the computer...
setting permissions...
cheking ssh directory...
[INFO] Info: New connection...
[INFO] Device connected
[INFO] USBMuxConnectByPort OK
root@localhost's password:
```



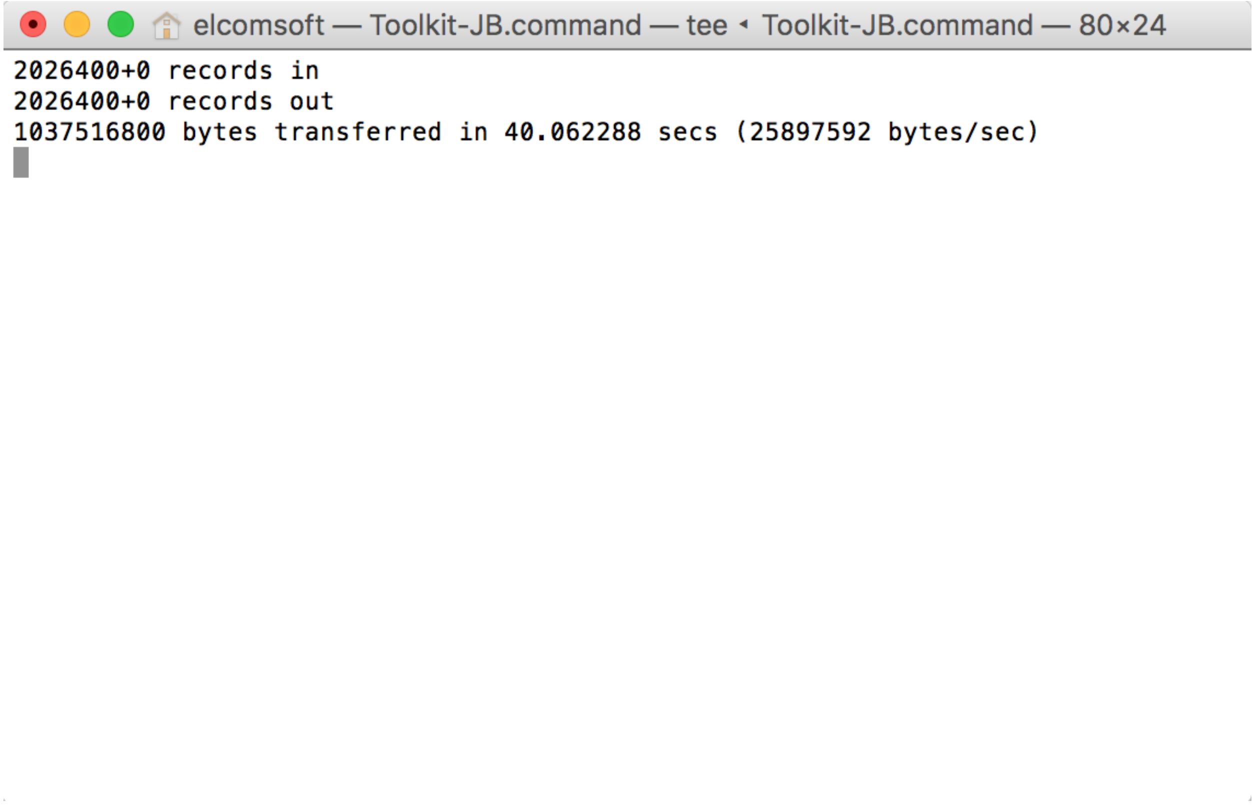
elcomsoft — Toolkit-JB.command — tee ◂ Toolkit-JB.command — 80×24

```
establishing ssh trust between the device and the computer...
setting permissions...
cheking ssh directory...
[INFO] Info: New connection...
[INFO] Device connected
[INFO] USBMuxConnectByPort OK
root@localhost's password:
copying public key on device...
[INFO] Info: New connection...
[INFO] Device connected
[INFO] USBMuxConnectByPort OK
Warning: Permanently added '[localhost]:3022' (RSA) to the list of known hosts.
root@localhost's password:
```

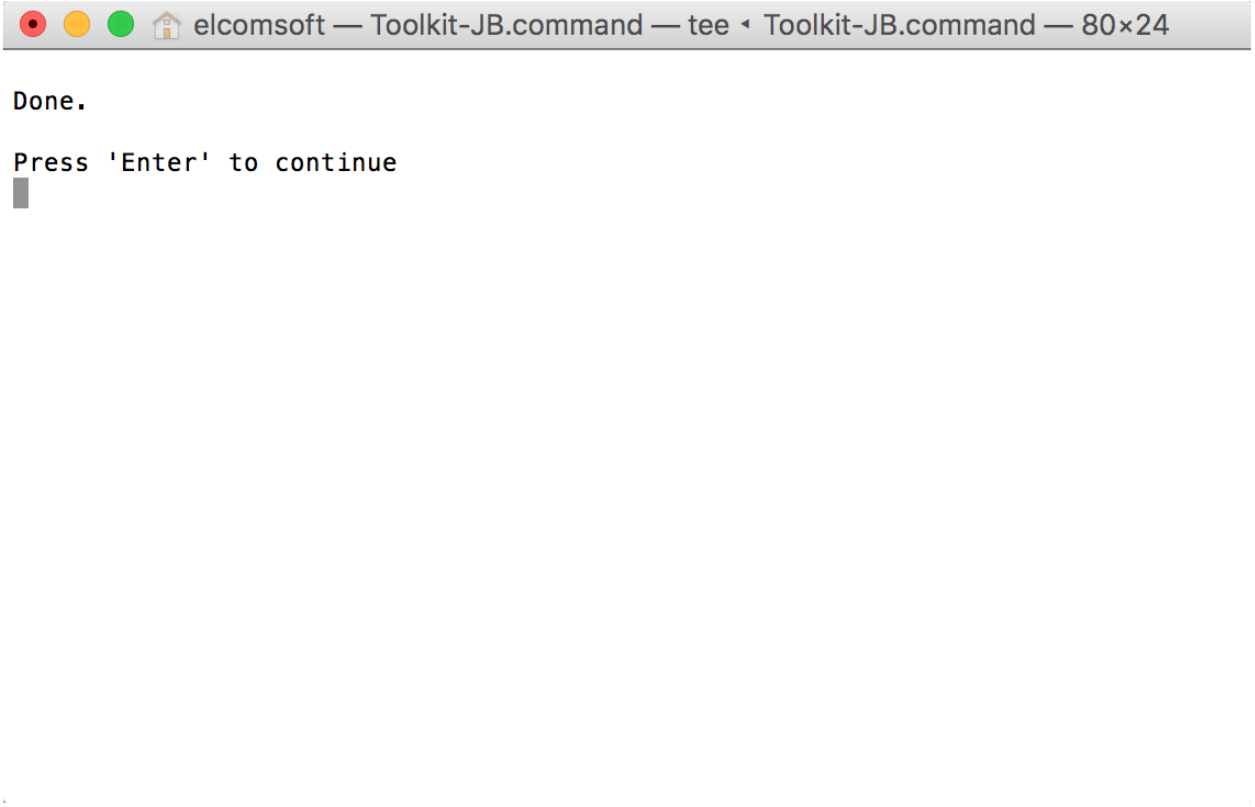


elcomsoft — Toolkit-JB.command — tee ◂ Toolkit-JB.command — 80×24

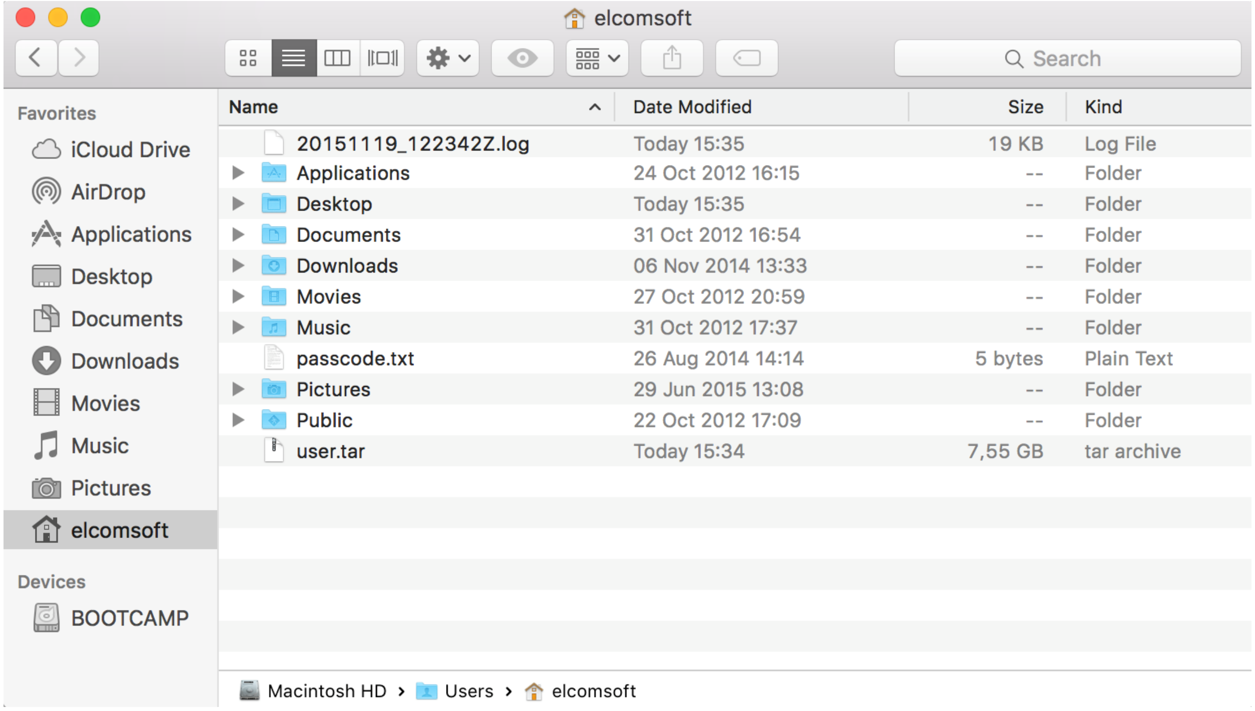
```
  ________________________________________________________________________
 |                                                                        |
 |                 Welcome to Elcomsoft iOS Forensic Toolkit              |
 |               This is driver script version 2.0/Mac for A5+            |
 |                                                                        |
 |                     (c) 2011-2015 Elcomsoft Co. Ltd.                   |
 |________________________________________________________________________|


Store files to archive (relative to home directory) <user.tar>:
```


elcomsoft — Toolkit-JB.command — tee ◂ Toolkit-JB.command — 80×24

```
2026400+0 records in
2026400+0 records out
1037516800 bytes transferred in 40.062288 secs (25897592 bytes/sec)
```

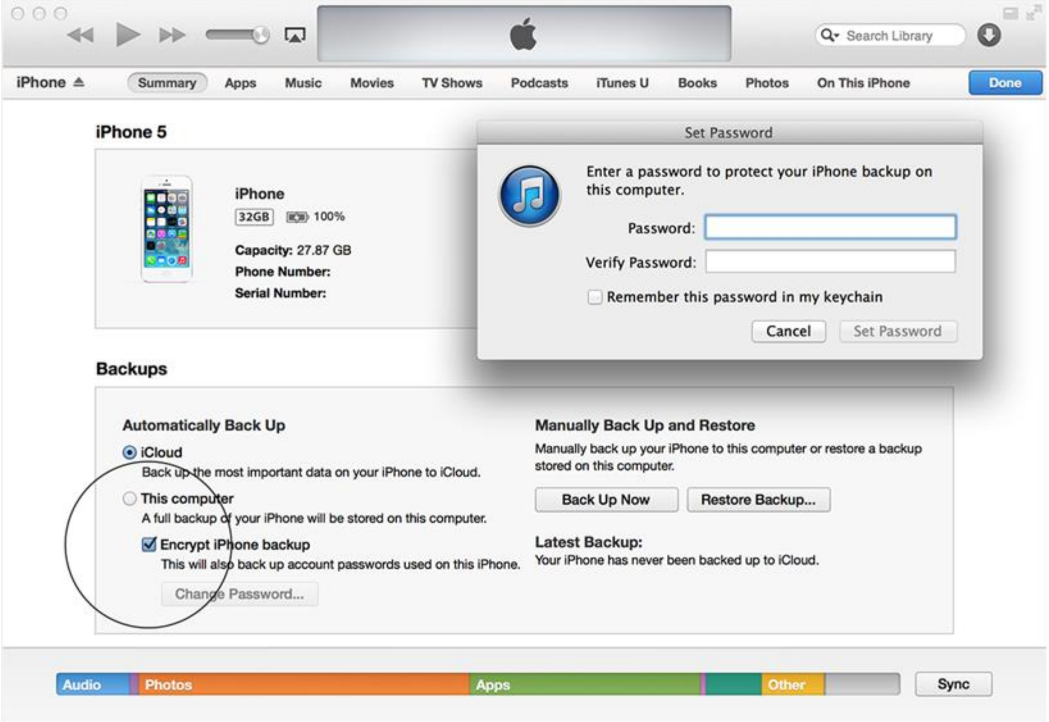

elcomsoft — Toolkit-JB.command — tee ◂ Toolkit-JB.command — 80×24

```

Done.

Press 'Enter' to continue
```



Name	Date Modified	Size	Kind
20151119_122342Z.log	Today 15:35	19 KB	Log File
Applications	24 Oct 2012 16:15	--	Folder
Desktop	Today 15:35	--	Folder
Documents	31 Oct 2012 16:54	--	Folder
Downloads	06 Nov 2014 13:33	--	Folder
Movies	27 Oct 2012 20:59	--	Folder
Music	31 Oct 2012 17:37	--	Folder
passcode.txt	26 Aug 2014 14:14	5 bytes	Plain Text
Pictures	29 Jun 2015 13:08	--	Folder
Public	22 Oct 2012 17:09	--	Folder
user.tar	Today 15:34	7,55 GB	tar archive

Chapter 6: iOS Logical and Cloud Acquisition



iPhone 5

iPhone
32GB 100%

Capacity: 27.87 GB
Phone Number:
Serial Number:

Set Password

Enter a password to protect your iPhone backup on this computer.

Password:

Verify Password:

□ Remember this password in my keychain

Cancel | Set Password

Backups

Automatically Back Up

● iCloud
Back up the most important data on your iPhone to iCloud.

○ This computer
A full backup of your iPhone will be stored on this computer.

☑ Encrypt iPhone backup
This will also back up account passwords used on this iPhone.

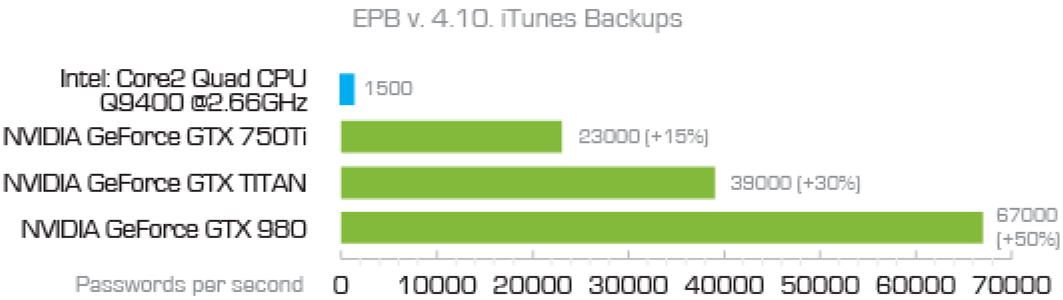
Change Password...

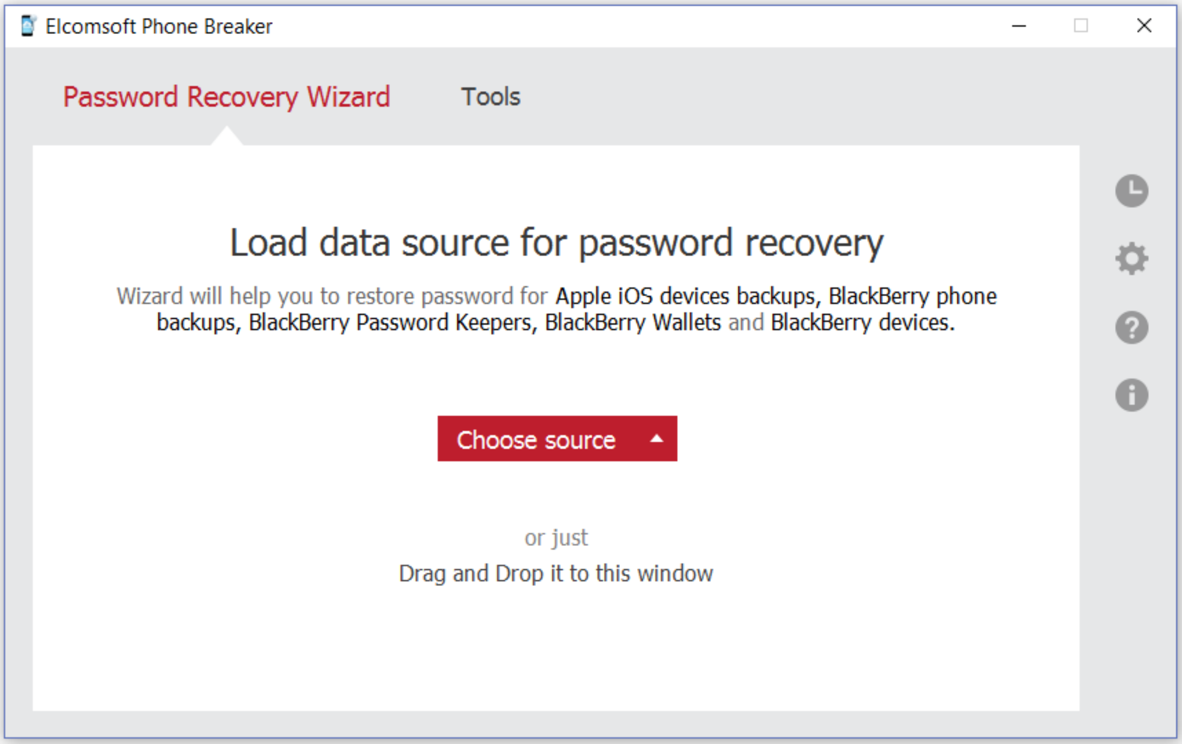
Manually Back Up and Restore

Manually back up your iPhone to this computer or restore a backup stored on this computer.

Back Up Now | Restore Backup...

Latest Backup:
Your iPhone has never been backed up to iCloud.

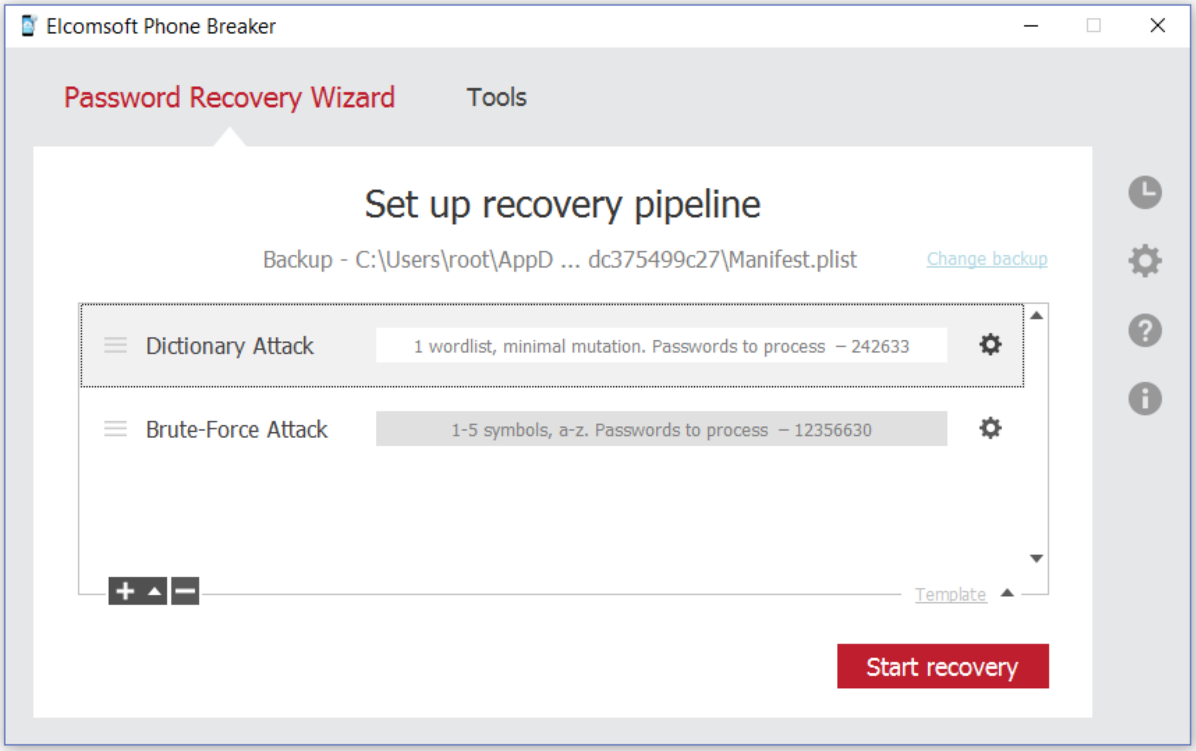




Load data source for password recovery

Wizard will help you to restore password for Apple iOS devices backups, BlackBerry phone backups, BlackBerry Password Keepers, BlackBerry Wallets and BlackBerry devices.

or just
Drag and Drop it to this window

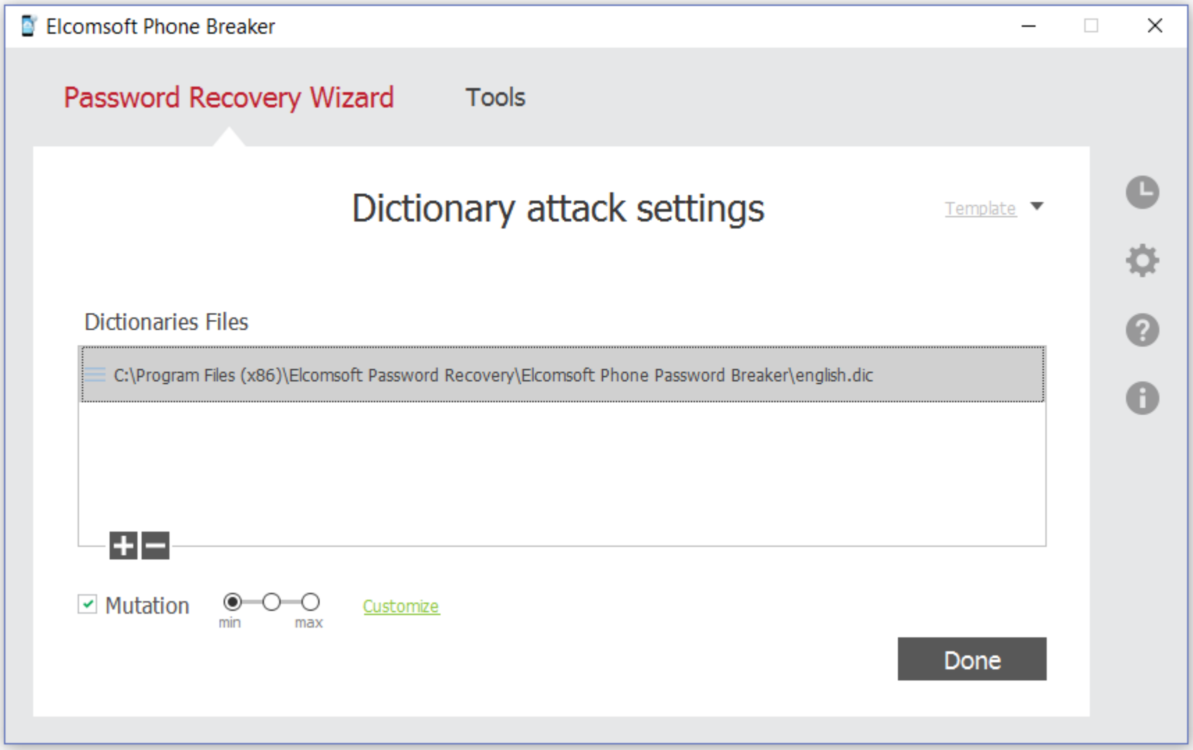


Set up recovery pipeline

Backup - C:\Users\root\AppD ... dc375499c27\Manifest.plist

Dictionary Attack — 1 wordlist, minimal mutation. Passwords to process – 242633

Brute-Force Attack — 1-5 symbols, a-z. Passwords to process – 12356630

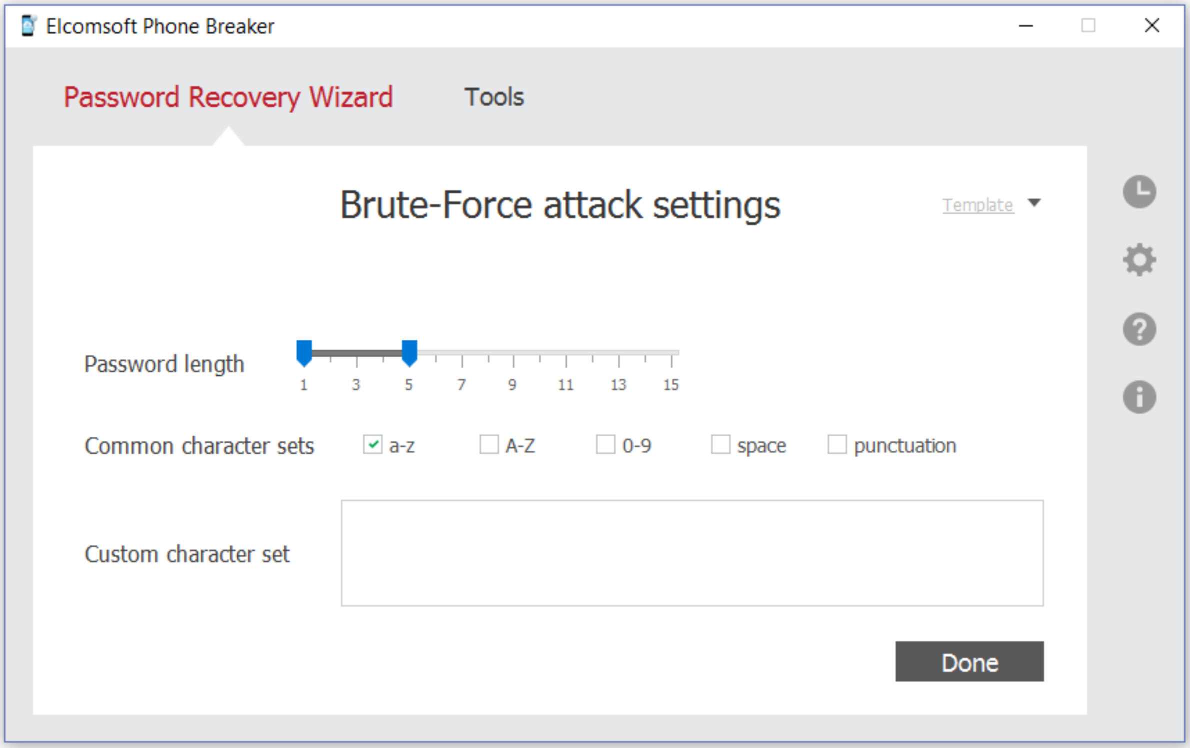


Dictionary attack settings

Dictionaries Files

C:\Program Files (x86)\Elcomsoft Password Recovery\Elcomsoft Phone Password Breaker\english.dic

☑ Mutation

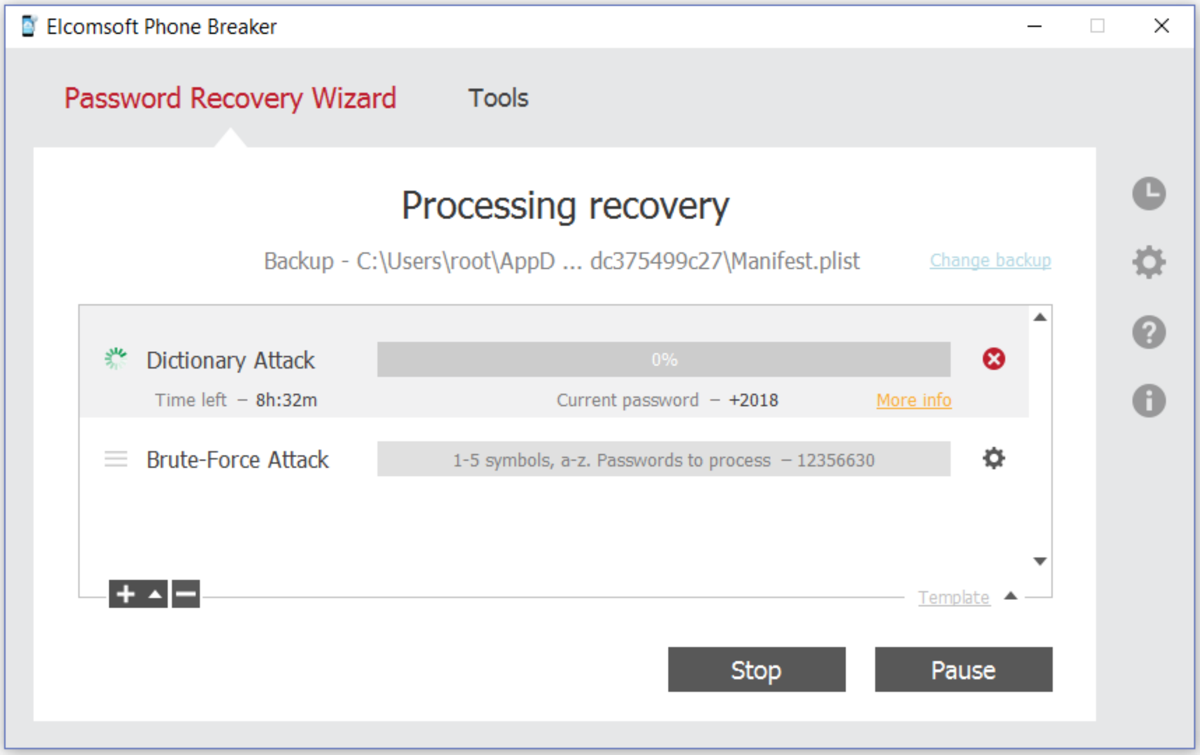


Brute-Force attack settings

Password length

Common character sets ☑ a-z □ A-Z □ 0-9 □ space □ punctuation

Custom character set



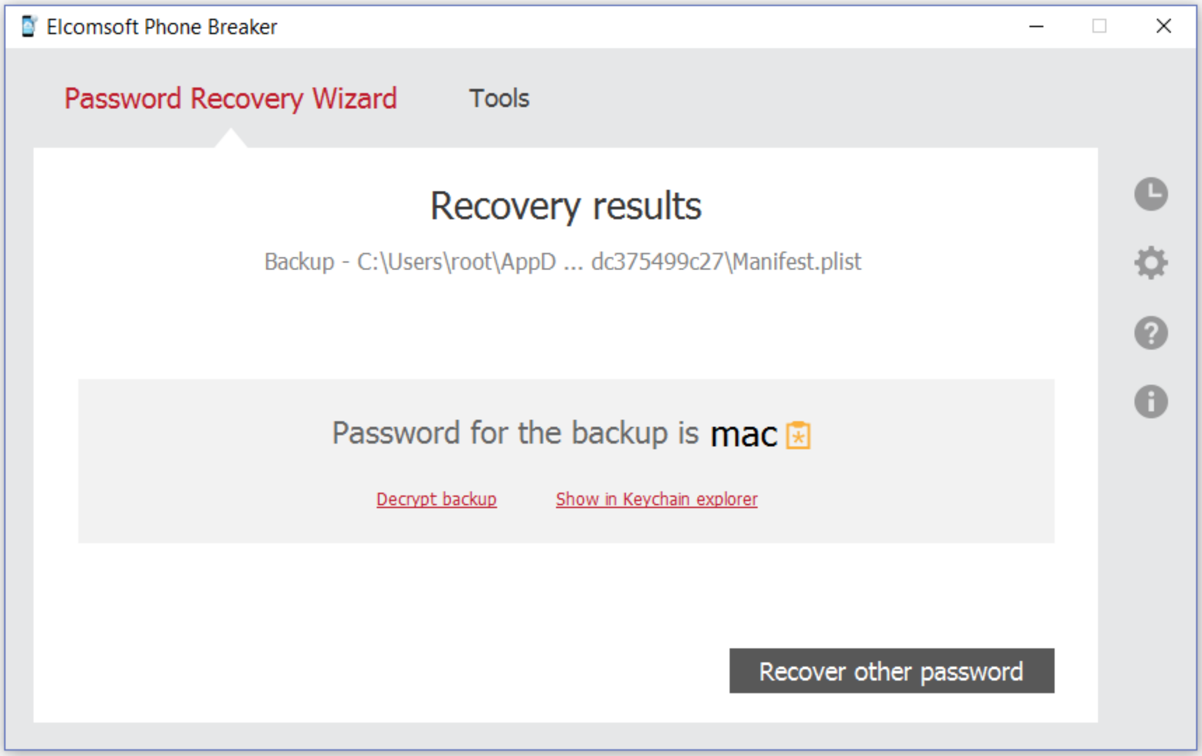
Processing recovery

Backup - C:\Users\root\AppD ... dc375499c27\Manifest.plist

Dictionary Attack 0%

Time left – 8h:32m Current password – +2018

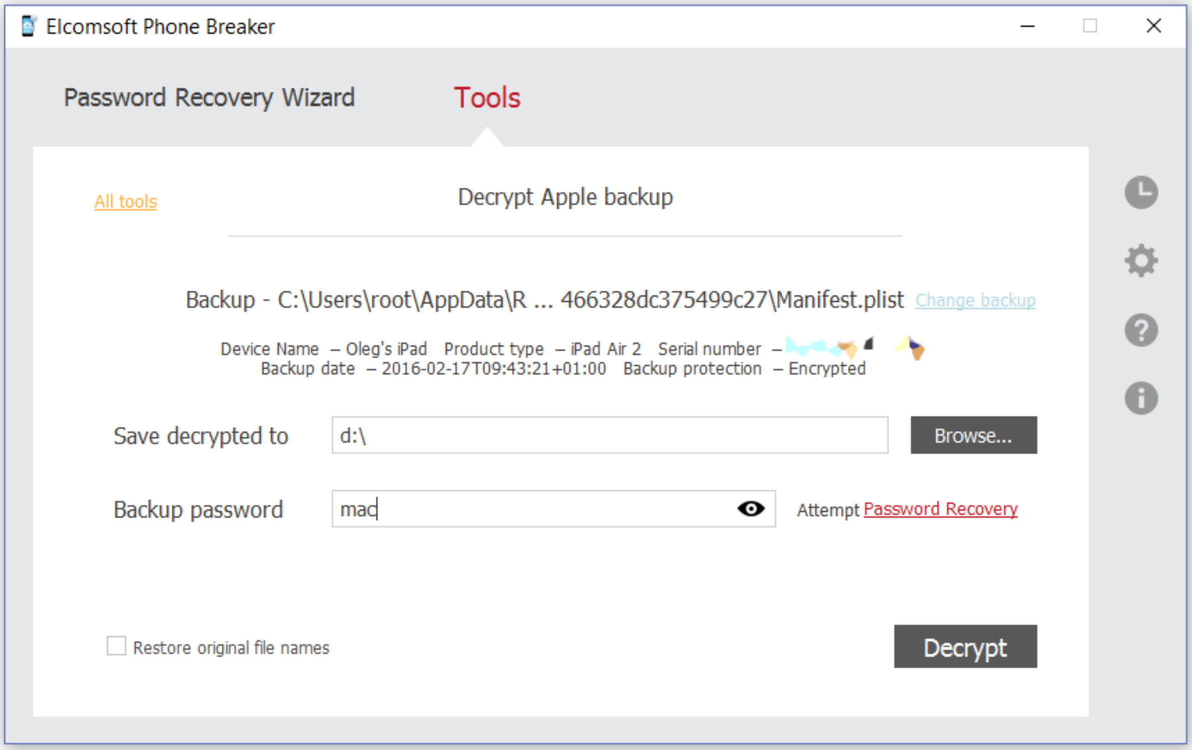
Brute-Force Attack 1-5 symbols, a-z. Passwords to process – 12356630



Recovery results

Backup - C:\Users\root\AppD ... dc375499c27\Manifest.plist

Password for the backup is mac



Elcomsoft Phone Breaker

Password Recovery Wizard   Tools

All tools

Decrypt Apple backup

Backup - C:\Users\root\AppData\R ... 466328dc375499c27\Manifest.plist Change backup

Device Name – Oleg's iPad Product type – iPad Air 2 Serial number – [redacted]
Backup date – 2016-02-17T09:43:21+01:00 Backup protection – Encrypted

Save decrypted to: d:\

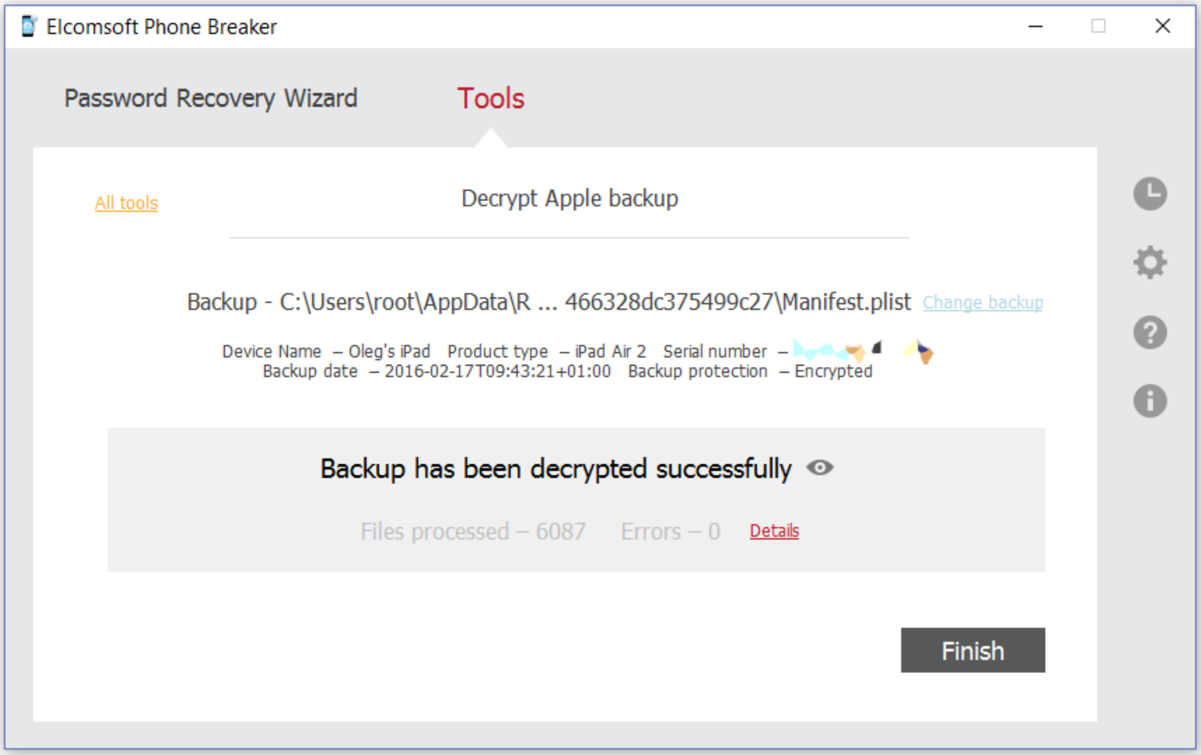
Backup password: mac

Attempt Password Recovery

□ Restore original file names

👁

👁



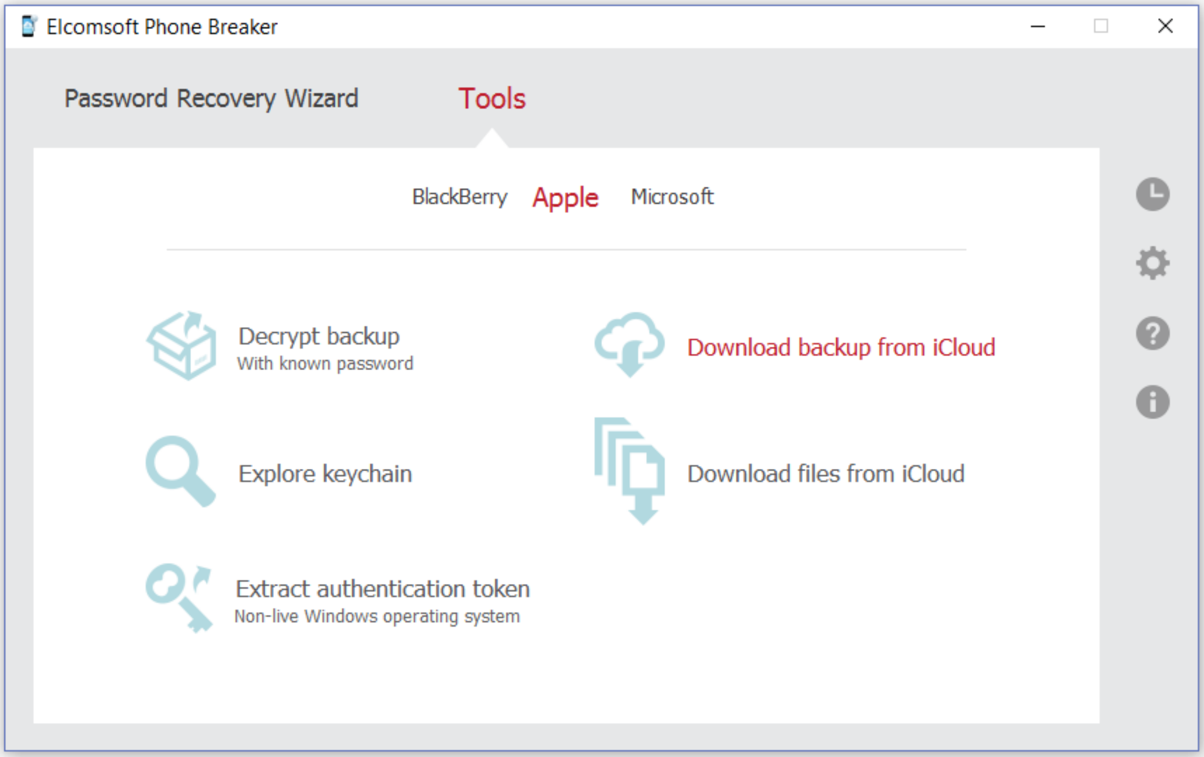
Decrypt Apple backup

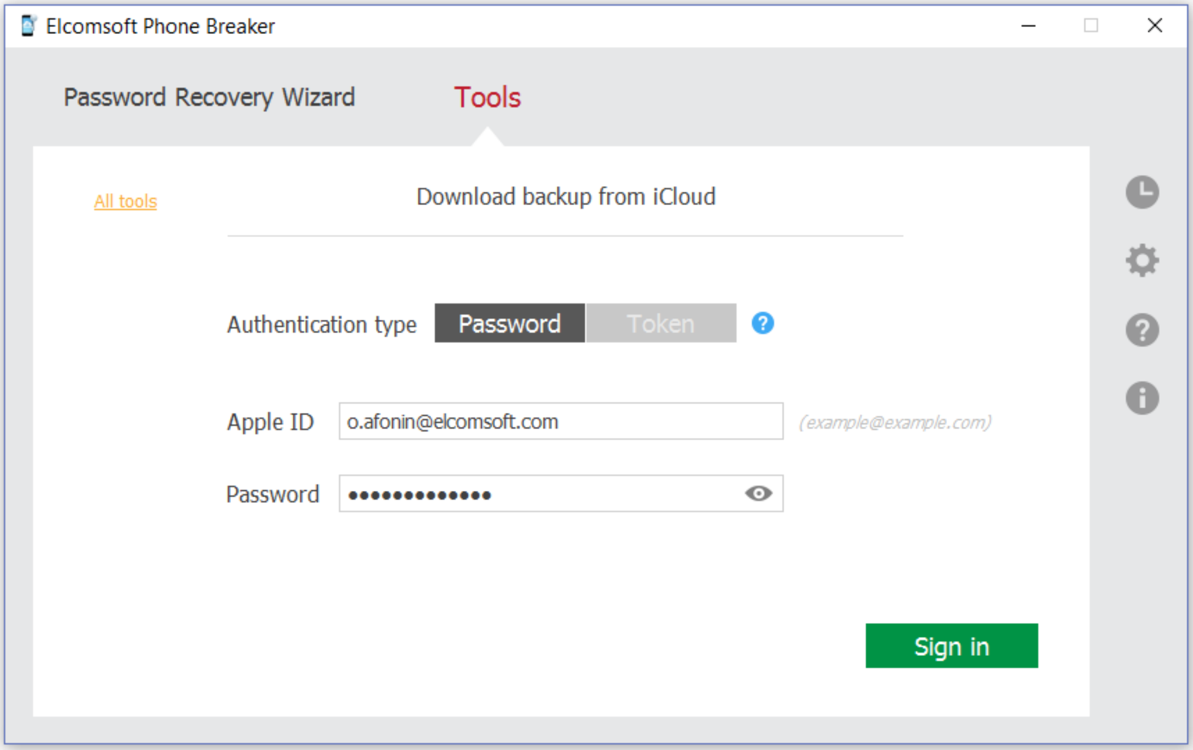
Backup - C:\Users\root\AppData\R ... 466328dc375499c27\Manifest.plist

Device Name – Oleg's iPad Product type – iPad Air 2 Serial number – [redacted]
Backup date – 2016-02-17T09:43:21+01:00 Backup protection – Encrypted

Backup has been decrypted successfully

Files processed – 6087 Errors – 0



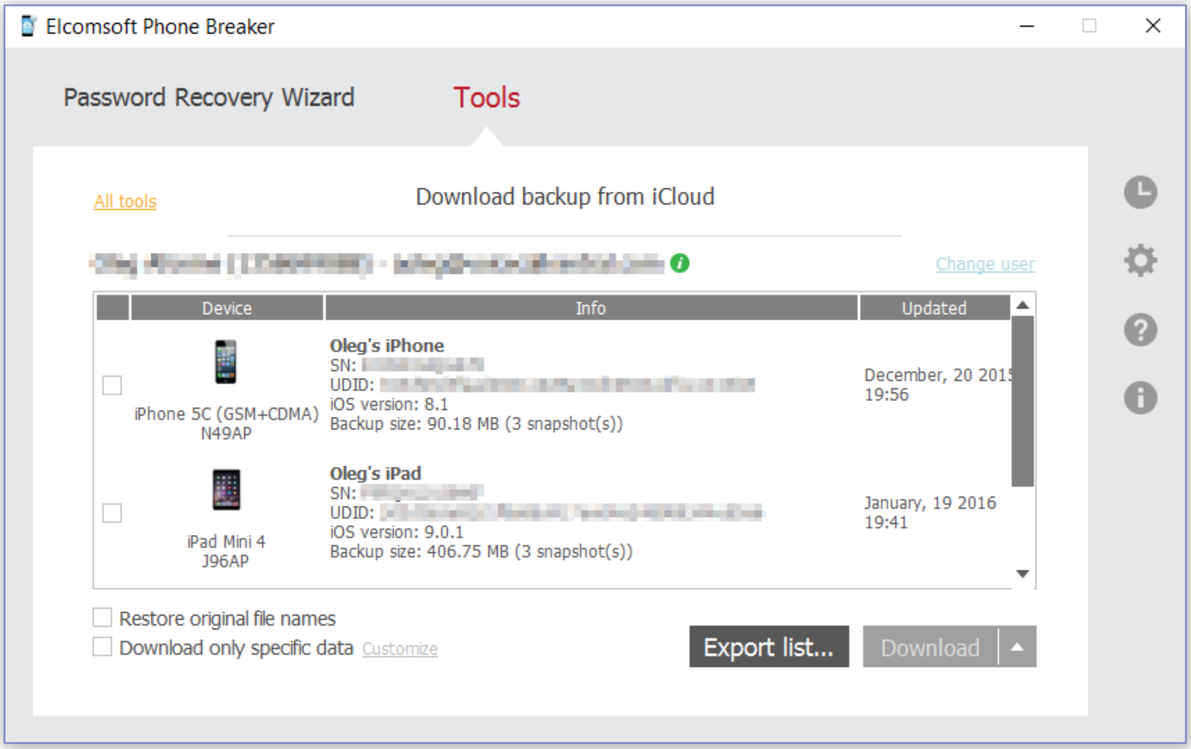


Download backup from iCloud

Authentication type: Password | Token

Apple ID: o.afonin@elcomsoft.com (example@example.com)

Password: •••••••••••••



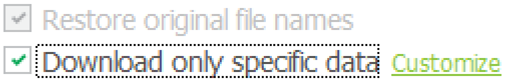
Download backup from iCloud

[redacted]

	Device	Info	Updated
□	iPhone 5C (GSM+CDMA) N49AP	**Oleg's iPhone** SN: [redacted] UDID: [redacted] iOS version: 8.1 Backup size: 90.18 MB (3 snapshot(s))	December, 20 2015 19:56
□	iPad Mini 4 J96AP	**Oleg's iPad** SN: [redacted] UDID: [redacted] iOS version: 9.0.1 Backup size: 406.75 MB (3 snapshot(s))	January, 19 2016 19:41

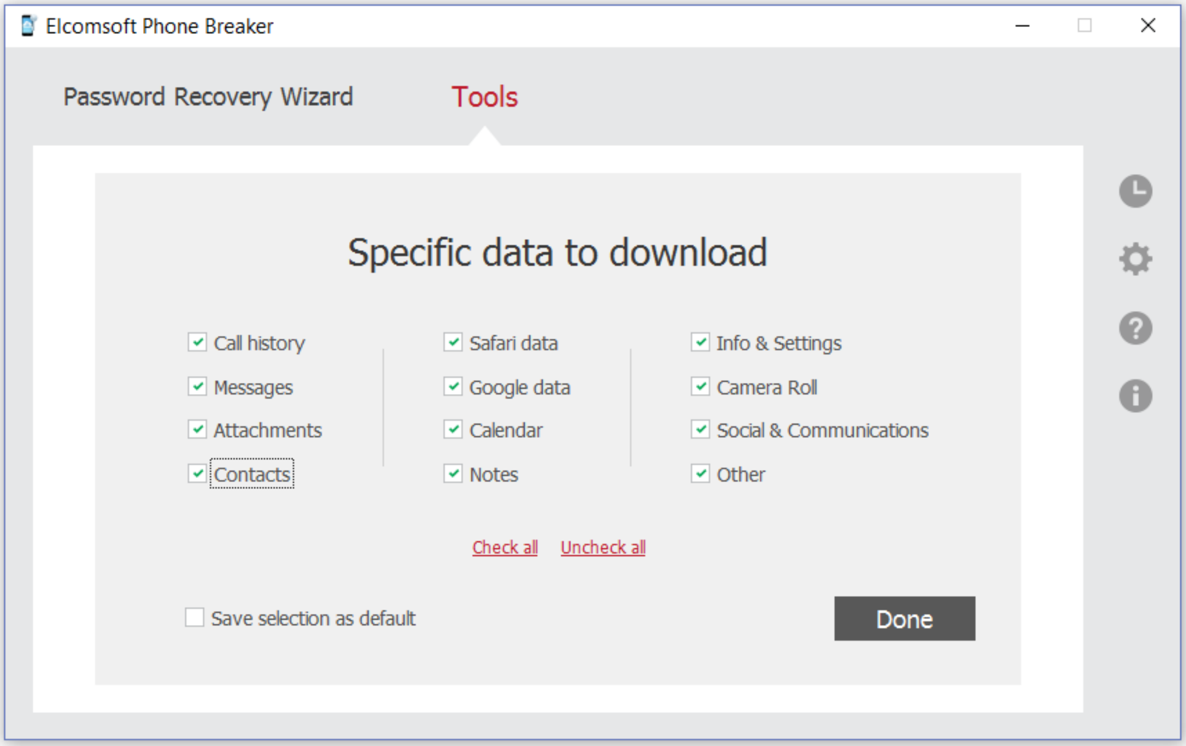
□ Restore original file names

□ Download only specific data Customize



☑ Restore original file names

☑ Download only specific data



Specific data to download

☑ Call history

☑ Messages

☑ Attachments

☑ Contacts

☑ Safari data

☑ Google data

☑ Calendar

☑ Notes

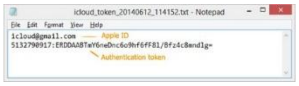
☑ Info & Settings

☑ Camera Roll

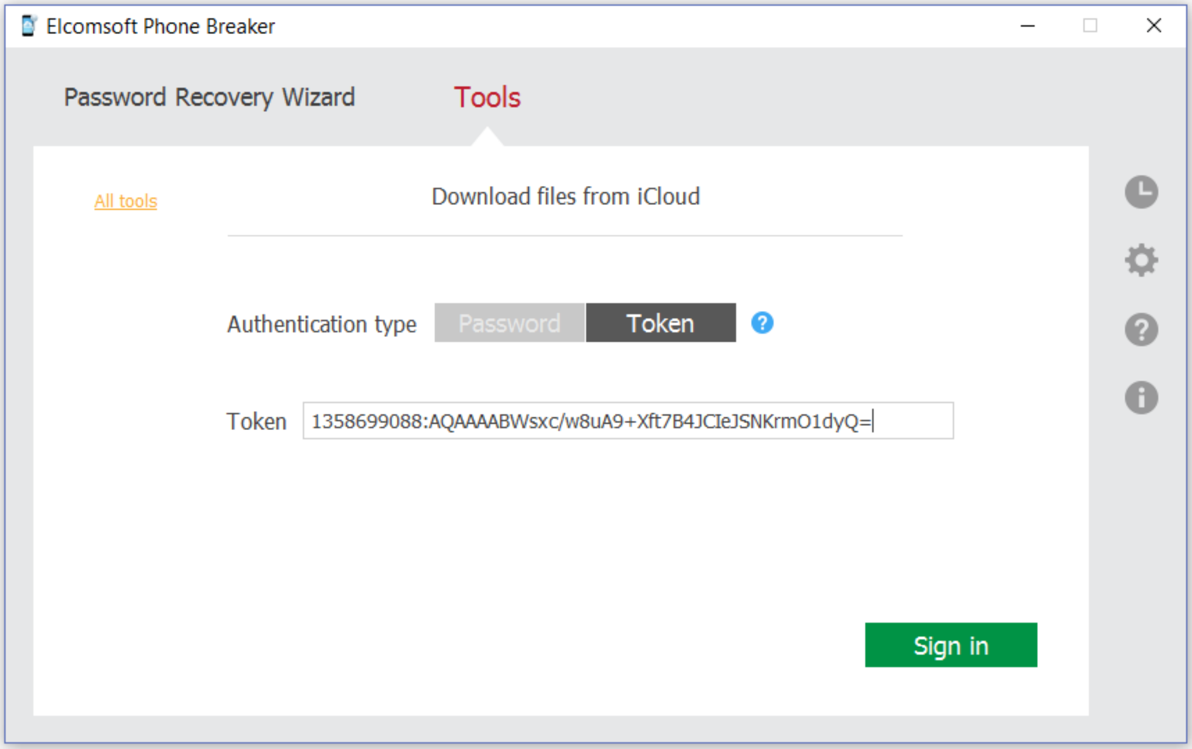
☑ Social & Communications

☑ Other

□ Save selection as default



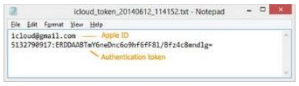
```
icloud@gmail.com
5132790917:ERDDAABTmY6neDnc6o9hf6fF81/Bfz4c8mndlg=
```



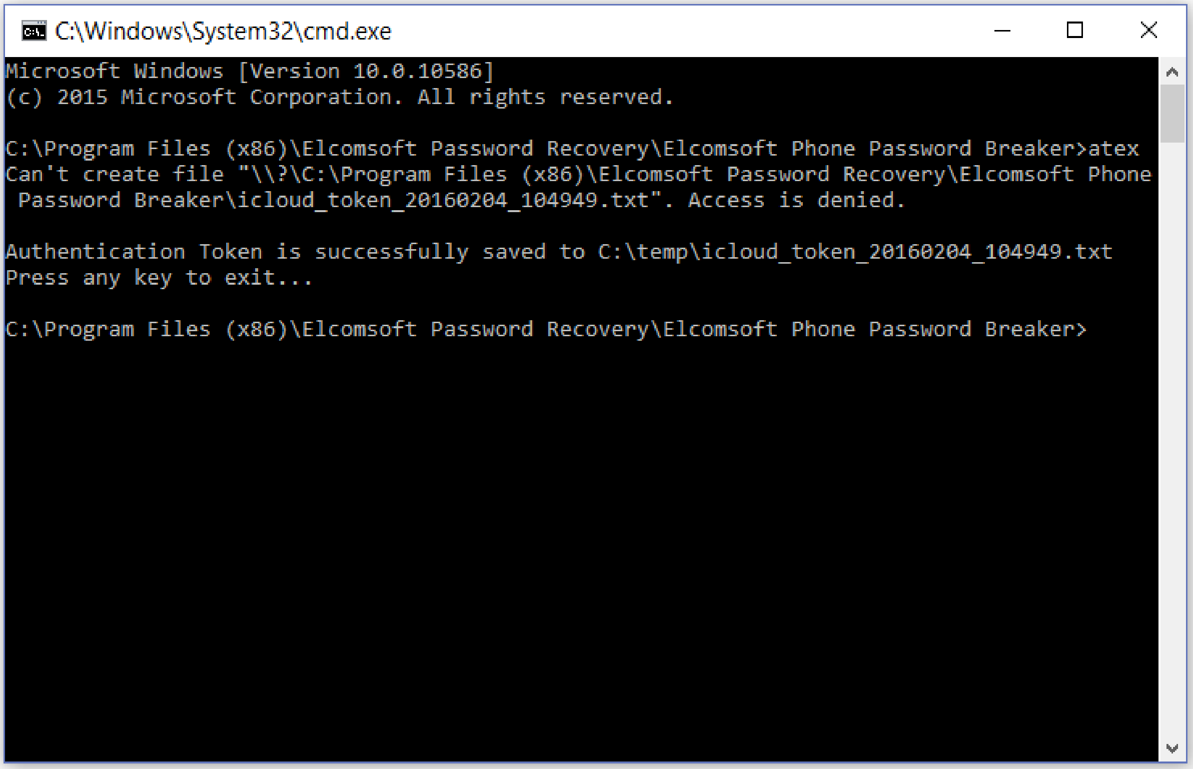
Download files from iCloud

Authentication type: Password [✓ Token]

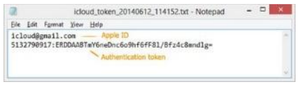
Token: 1358699088:AQAAAABWsxc/w8uA9+Xft7B4JCIeJSNKrmO1dyQ=


icloud_token_20140612_114152.txt - Notepad
File Edit Format View Help
Apple ID
Authentication token

```
icloud@gmail.com
5132790917:ERDDAABTmY6neDnc6o9hf6fF81/Bfz4c8mndlg=
```

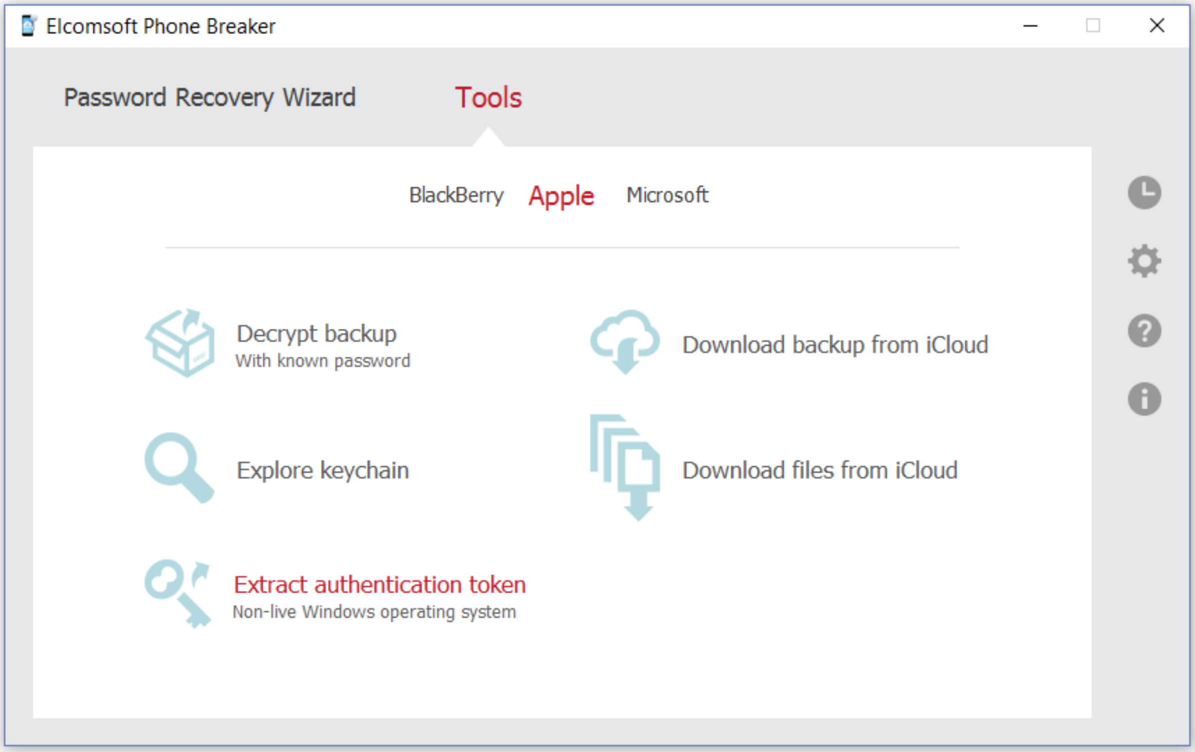


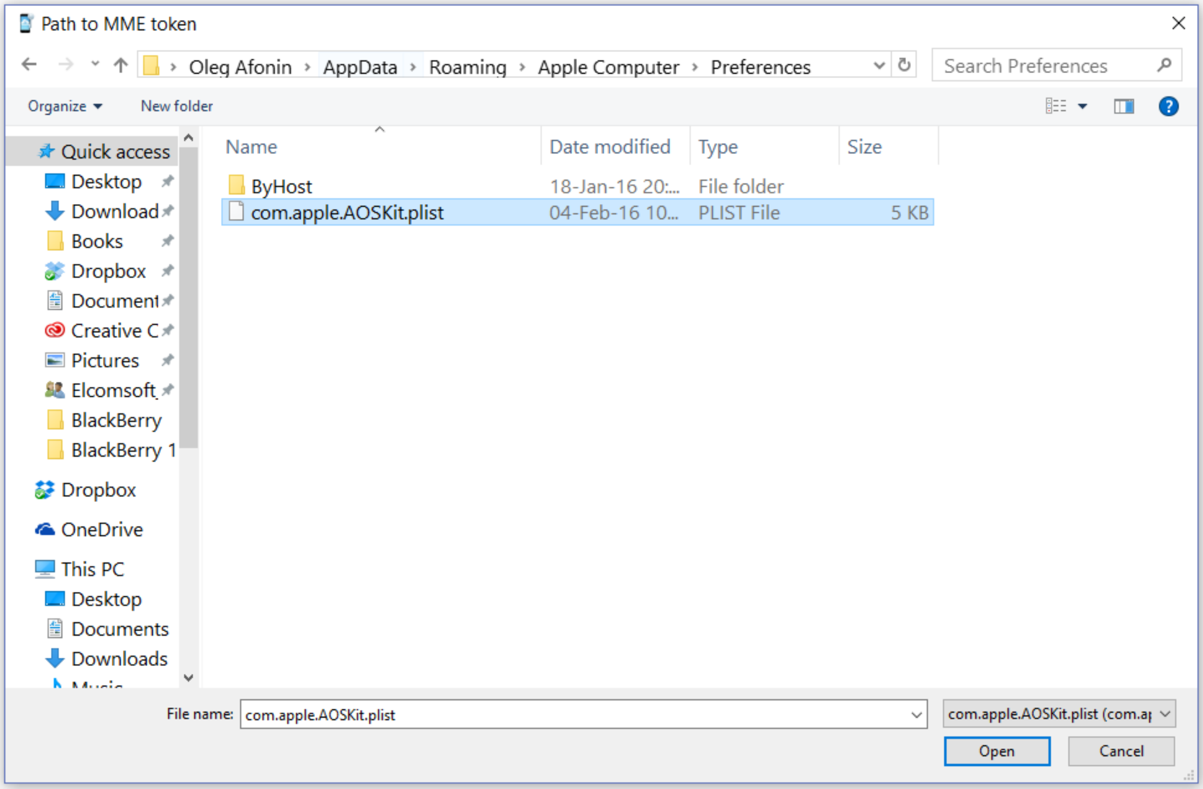
```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Elcomsoft Password Recovery\Elcomsoft Phone Password Breaker>atex
Can't create file "\\?\C:\Program Files (x86)\Elcomsoft Password Recovery\Elcomsoft Phone
 Password Breaker\icloud_token_20160204_104949.txt". Access is denied.

Authentication Token is successfully saved to C:\temp\icloud_token_20160204_104949.txt
Press any key to exit...

C:\Program Files (x86)\Elcomsoft Password Recovery\Elcomsoft Phone Password Breaker>
```



icloud_token_20140612_114152.txt - Notepad
File Edit Format View Help
Apple ID
Authentication token

```
icloud@gmail.com
5132790917:ERDDAABTmY6neDnc6o9hf6fF81/Bfz4c8mndlg=
```

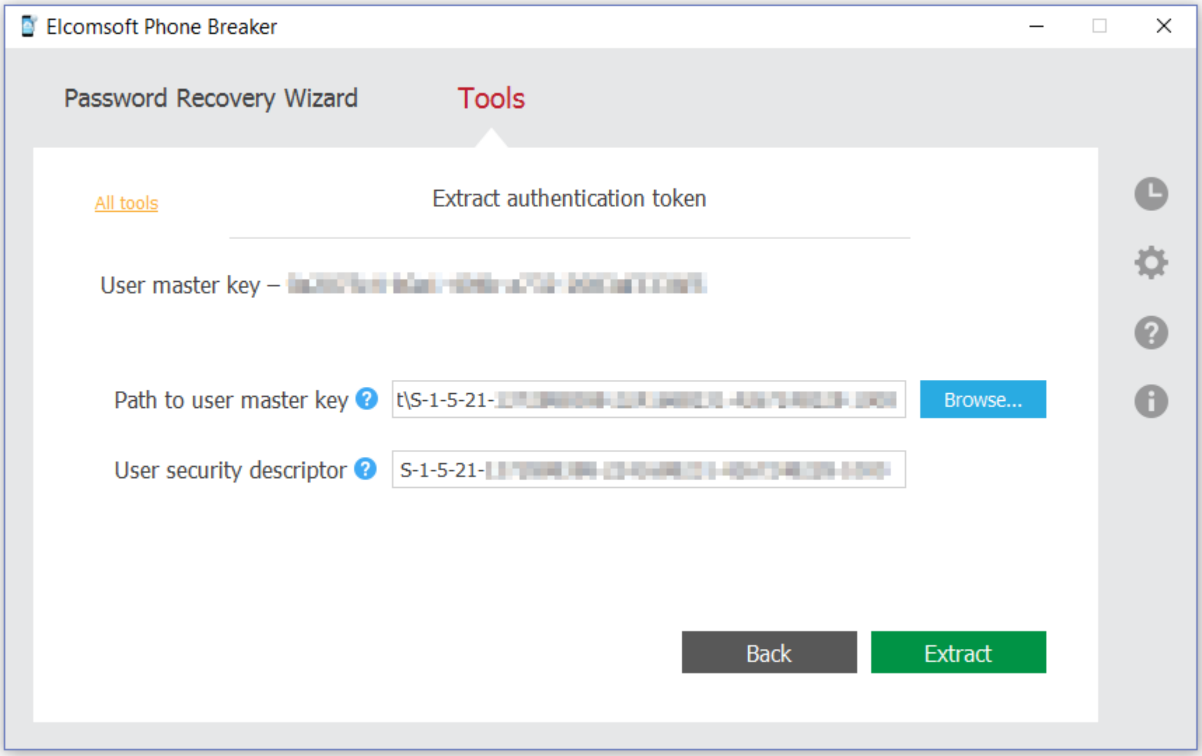




Name	Date modified	Type	Size
ByHost	18-Jan-16 20:...	File folder	
com.apple.AOSKit.plist	04-Feb-16 10...	PLIST File	5 KB

File name: com.apple.AOSKit.plist

com.apple.AOSKit.plist (com.a|

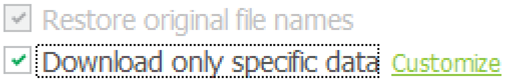


Extract authentication token

User master key – [redacted]

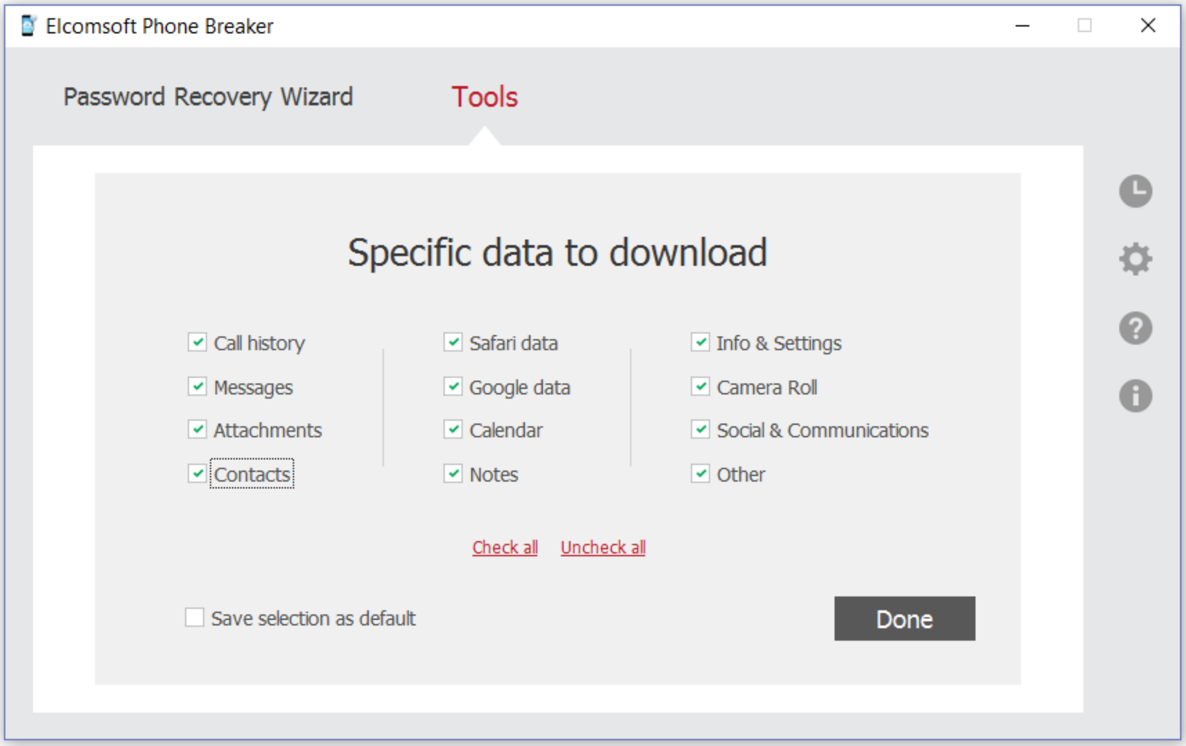
Path to user master key: t\S-1-5-21-[redacted]

User security descriptor: S-1-5-21-[redacted]



☑ Restore original file names

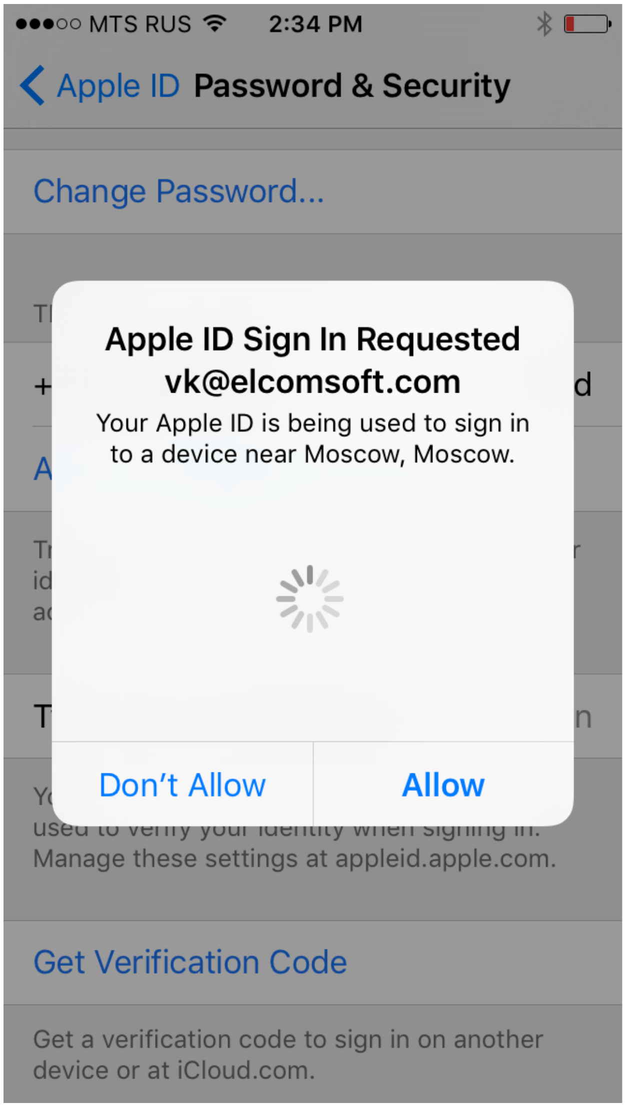
☑ Download only specific data



Specific data to download

- ☑ Call history
- ☑ Messages
- ☑ Attachments
- ☑ Contacts
- ☑ Safari data
- ☑ Google data
- ☑ Calendar
- ☑ Notes
- ☑ Info & Settings
- ☑ Camera Roll
- ☑ Social & Communications
- ☑ Other

□ Save selection as default

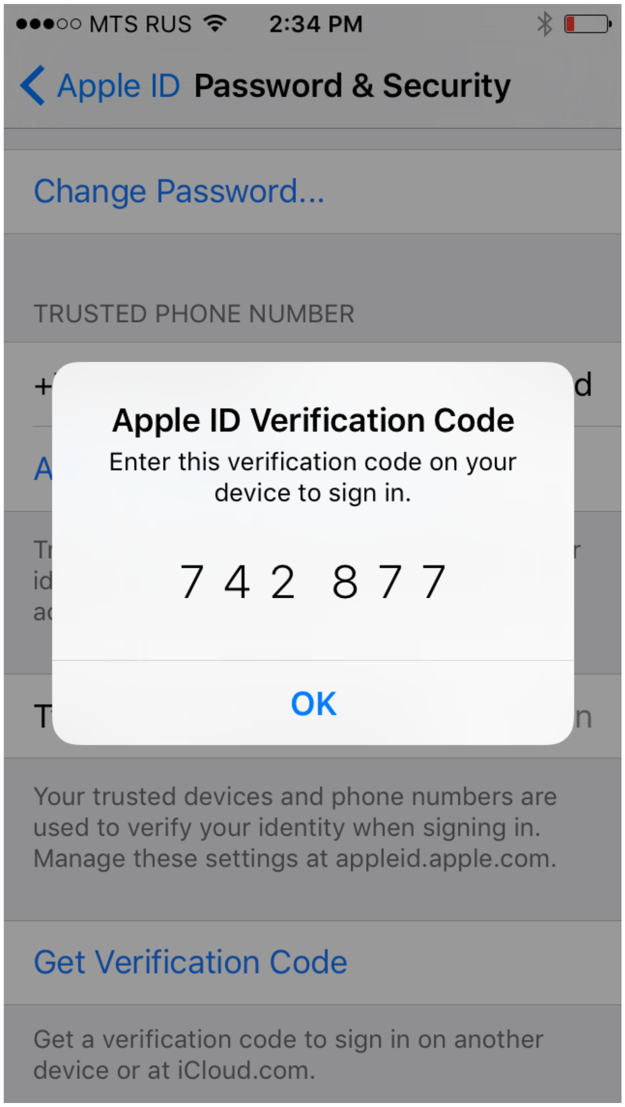


Apple ID Sign In Requested
vk@elcomsoft.com

Your Apple ID is being used to sign in to a device near Moscow, Moscow.

Manage these settings at appleid.apple.com.

Get a verification code to sign in on another device or at iCloud.com.



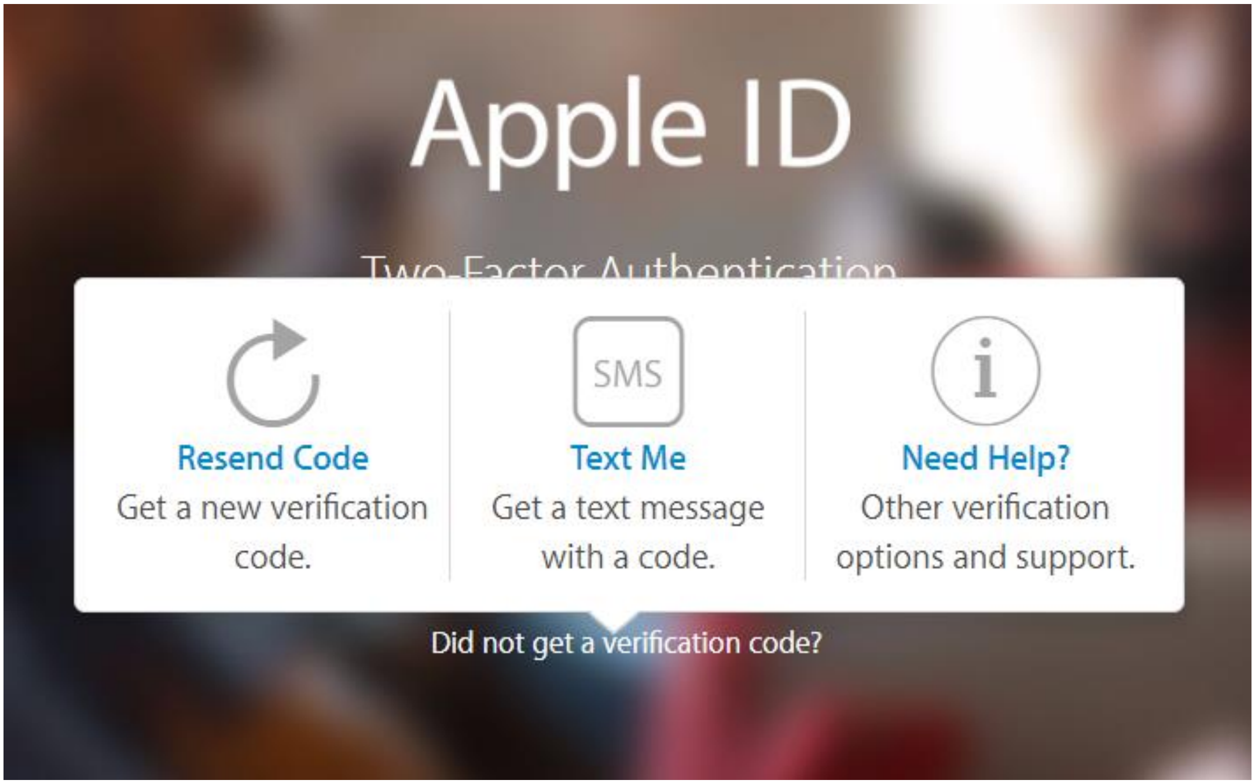
Apple ID Verification Code

Enter this verification code on your device to sign in.

742 877

Your trusted devices and phone numbers are used to verify your identity when signing in. Manage these settings at appleid.apple.com.

Get a verification code to sign in on another device or at iCloud.com.



Apple ID

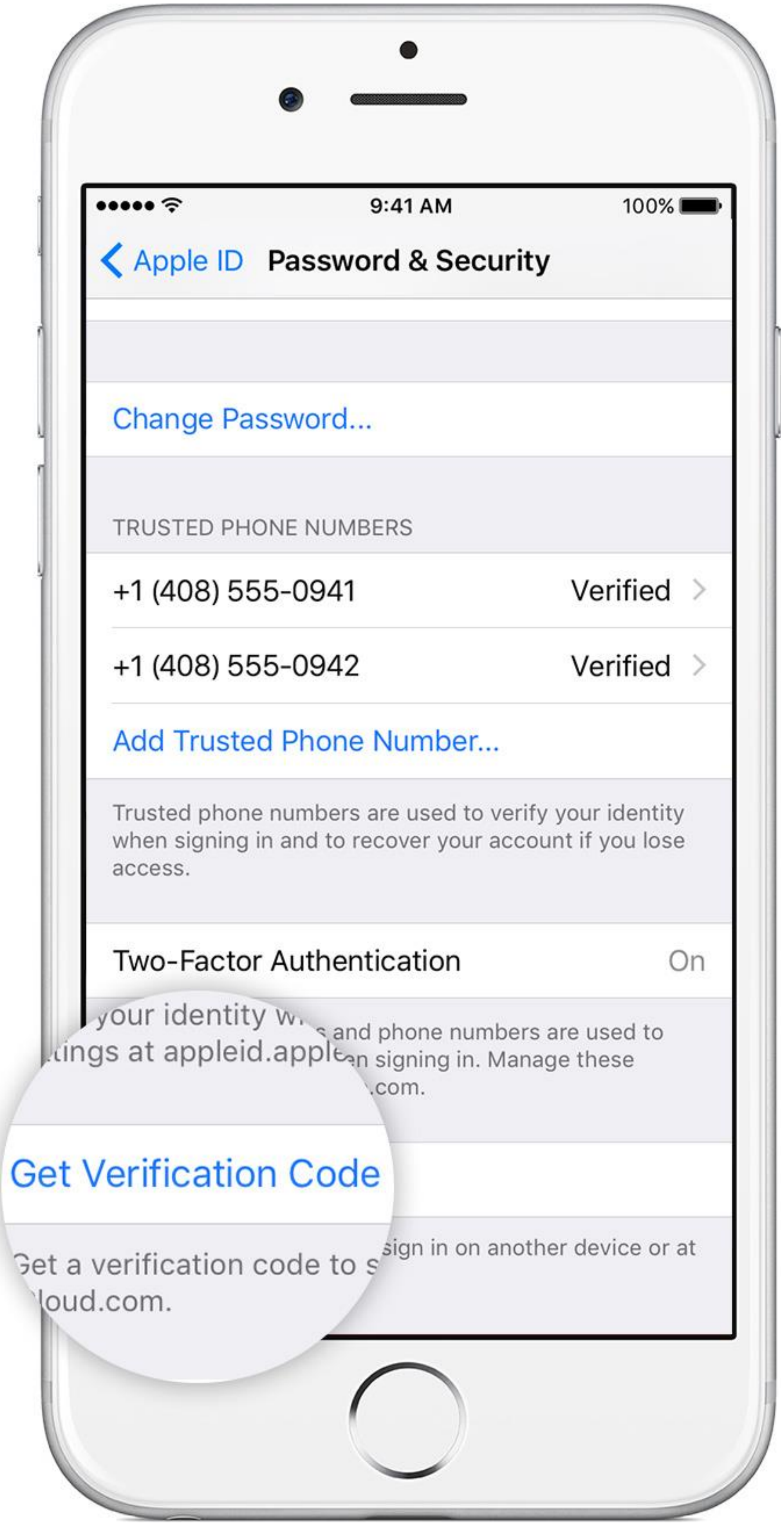
Two-Factor Authentication

Resend Code
Get a new verification code.

Text Me
Get a text message with a code.

Need Help?
Other verification options and support.

Did not get a verification code?



Apple ID Password & Security

Change Password...

TRUSTED PHONE NUMBERS

+1 (408) 555-0941 Verified

+1 (408) 555-0942 Verified

Add Trusted Phone Number...

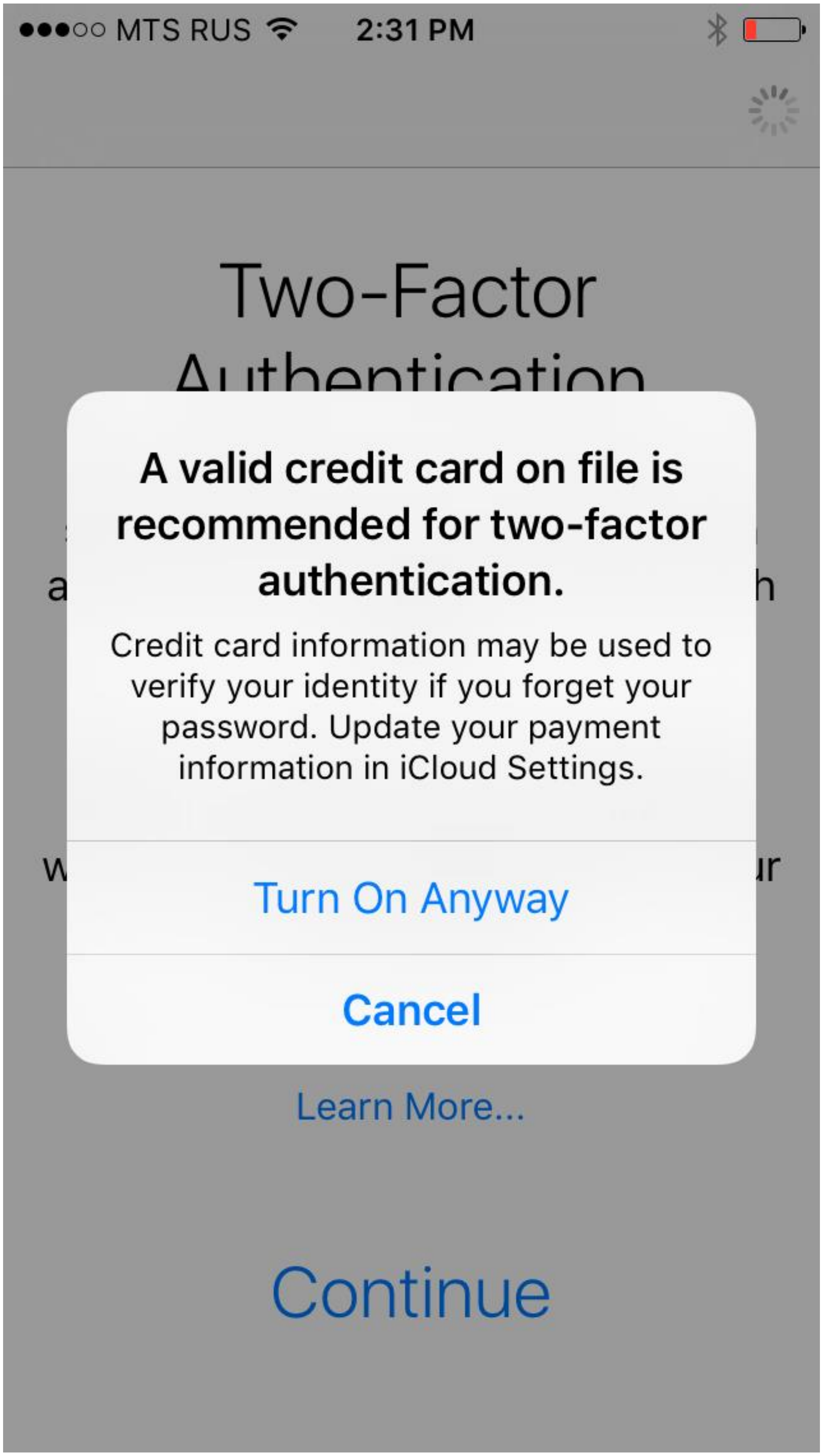
Trusted phone numbers are used to verify your identity when signing in and to recover your account if you lose access.

Two-Factor Authentication On

your identity w s and phone numbers are used to
tings at appleid.apple en signing in. Manage these
.com.

Get Verification Code

Get a verification code to s sign in on another device or at
loud.com.

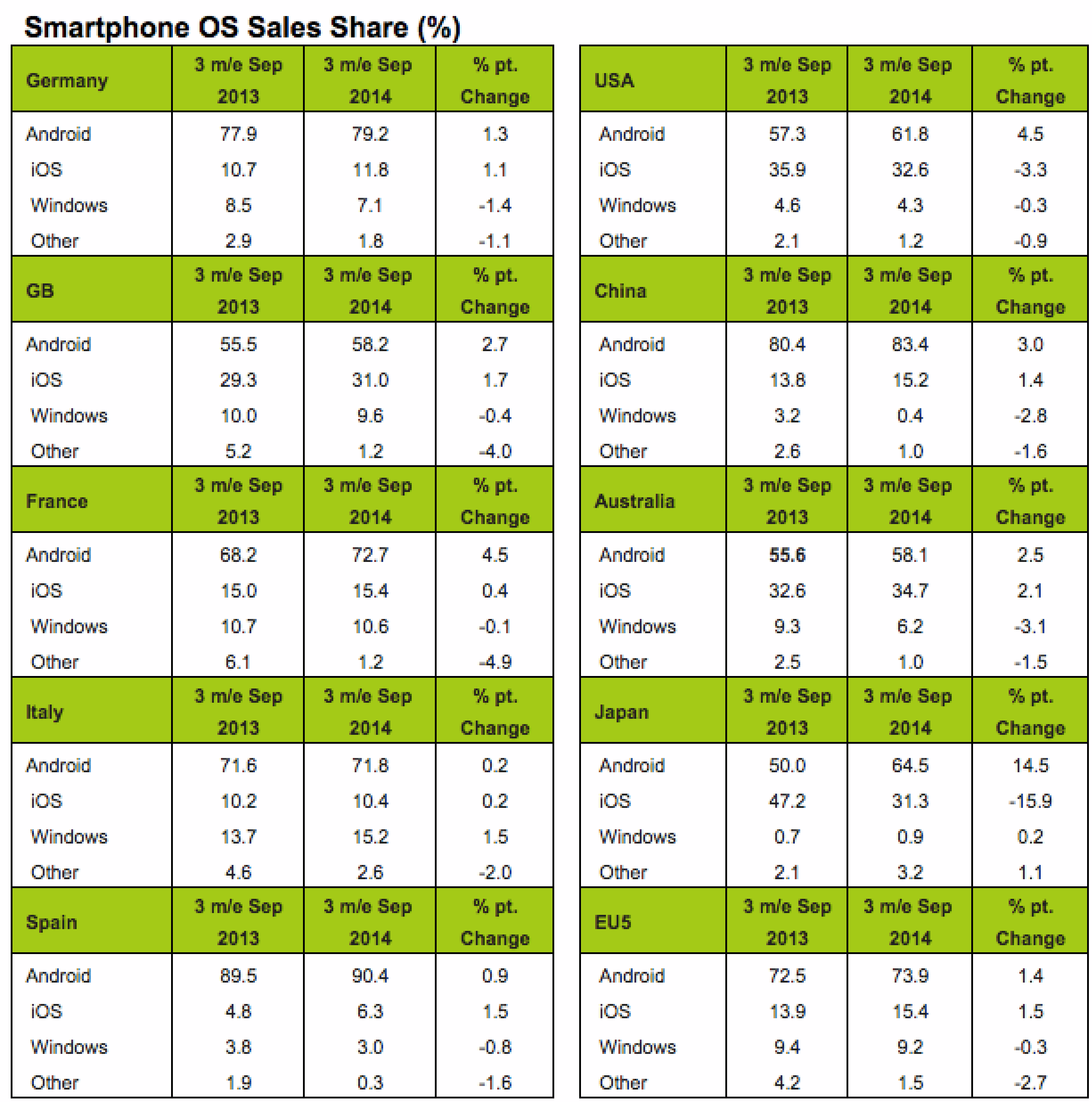


Two-Factor Authentication

A valid credit card on file is recommended for two-factor authentication.

Credit card information may be used to verify your identity if you forget your password. Update your payment information in iCloud Settings.

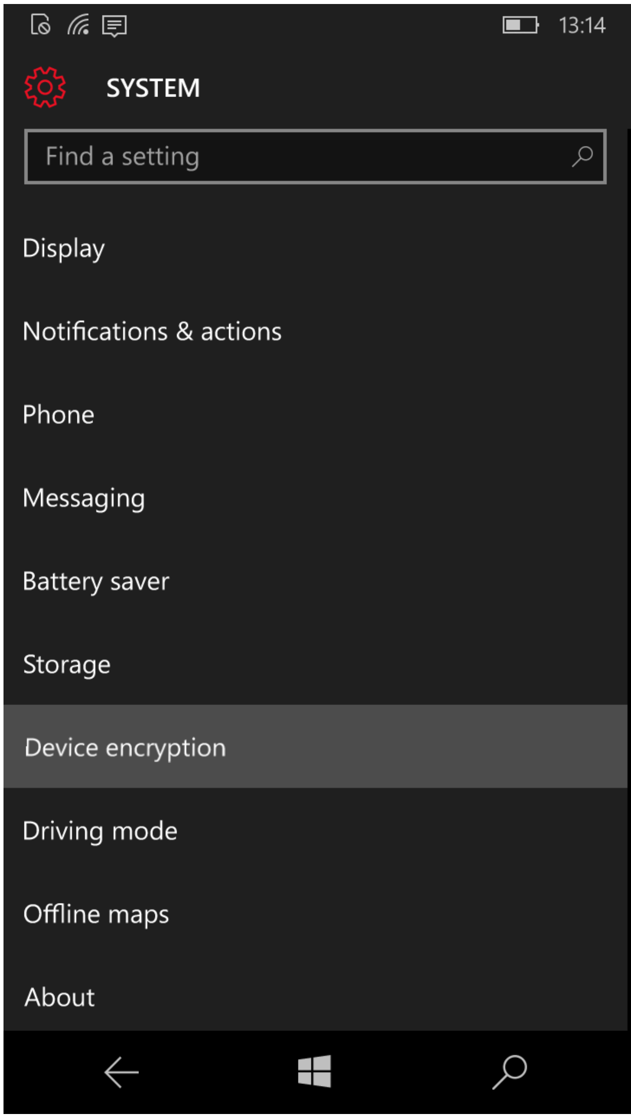
Chapter 7: Acquisition – Approaching Windows Phone and Windows 10 Mobile

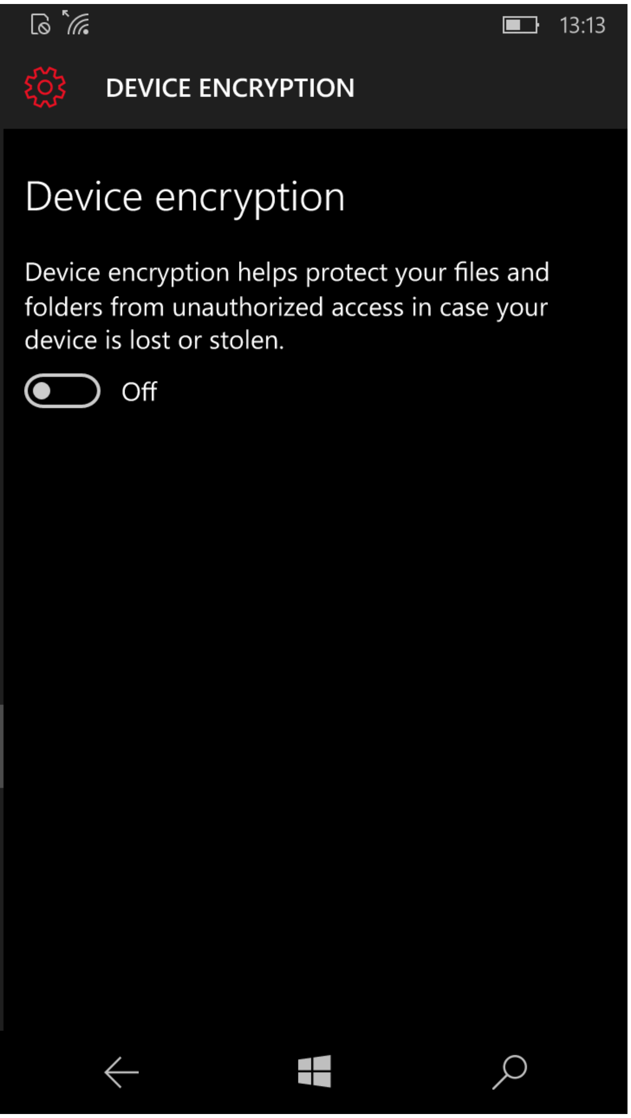


Smartphone OS Sales Share (%)

Germany	3 m/e Sep 2013	3 m/e Sep 2014	% pt. Change
Android	77.9	79.2	1.3
iOS	10.7	11.8	1.1
Windows	8.5	7.1	-1.4
Other	2.9	1.8	-1.1
GB	**3 m/e Sep 2013**	**3 m/e Sep 2014**	**% pt. Change**
Android	55.5	58.2	2.7
iOS	29.3	31.0	1.7
Windows	10.0	9.6	-0.4
Other	5.2	1.2	-4.0
France	**3 m/e Sep 2013**	**3 m/e Sep 2014**	**% pt. Change**
Android	68.2	72.7	4.5
iOS	15.0	15.4	0.4
Windows	10.7	10.6	-0.1
Other	6.1	1.2	-4.9
Italy	**3 m/e Sep 2013**	**3 m/e Sep 2014**	**% pt. Change**
Android	71.6	71.8	0.2
iOS	10.2	10.4	0.2
Windows	13.7	15.2	1.5
Other	4.6	2.6	-2.0
Spain	**3 m/e Sep 2013**	**3 m/e Sep 2014**	**% pt. Change**
Android	89.5	90.4	0.9
iOS	4.8	6.3	1.5
Windows	3.8	3.0	-0.8
Other	1.9	0.3	-1.6

USA	3 m/e Sep 2013	3 m/e Sep 2014	% pt. Change
Android	57.3	61.8	4.5
iOS	35.9	32.6	-3.3
Windows	4.6	4.3	-0.3
Other	2.1	1.2	-0.9
China	**3 m/e Sep 2013**	**3 m/e Sep 2014**	**% pt. Change**
Android	80.4	83.4	3.0
iOS	13.8	15.2	1.4
Windows	3.2	0.4	-2.8
Other	2.6	1.0	-1.6
Australia	**3 m/e Sep 2013**	**3 m/e Sep 2014**	**% pt. Change**
Android	**55.6**	58.1	2.5
iOS	32.6	34.7	2.1
Windows	9.3	6.2	-3.1
Other	2.5	1.0	-1.5
Japan	**3 m/e Sep 2013**	**3 m/e Sep 2014**	**% pt. Change**
Android	50.0	64.5	14.5
iOS	47.2	31.3	-15.9
Windows	0.7	0.9	0.2
Other	2.1	3.2	1.1
EU5	**3 m/e Sep 2013**	**3 m/e Sep 2014**	**% pt. Change**
Android	72.5	73.9	1.4
iOS	13.9	15.4	1.5
Windows	9.4	9.2	-0.3
Other	4.2	1.5	-2.7

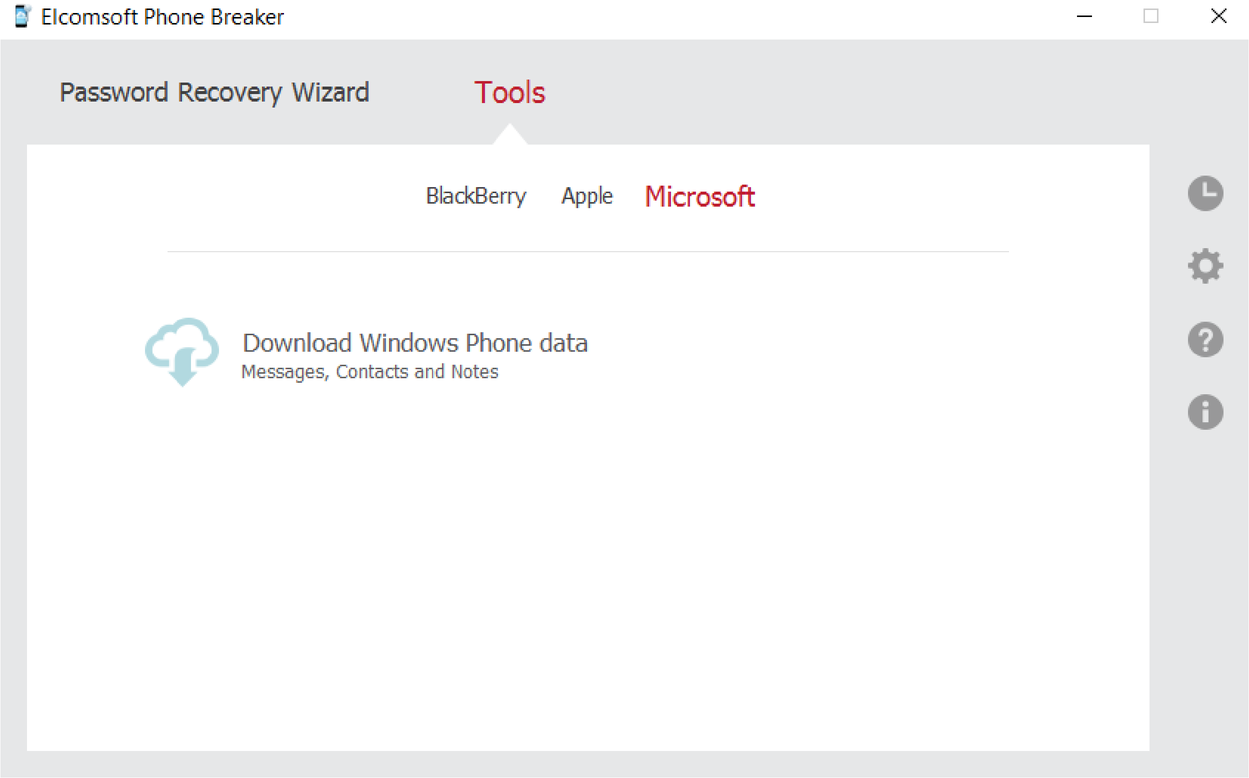




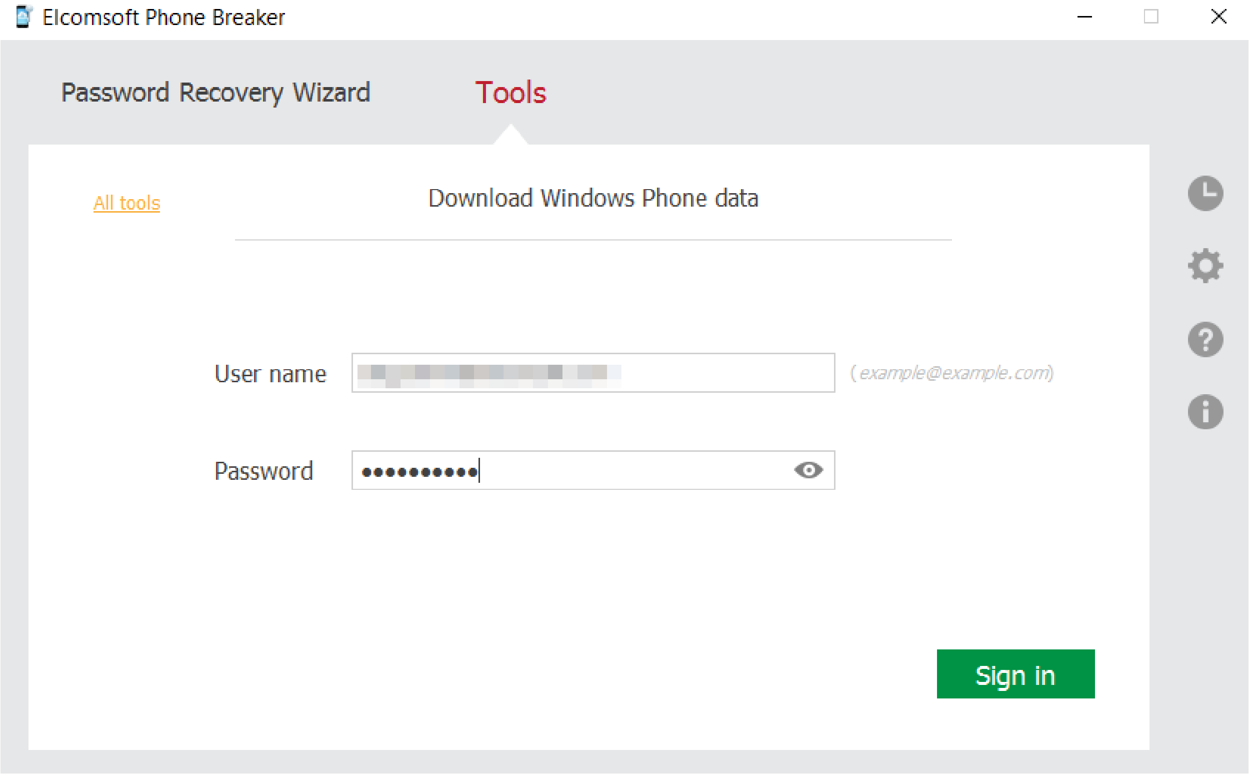
Device encryption

Device encryption helps protect your files and folders from unauthorized access in case your device is lost or stolen.

○ Off



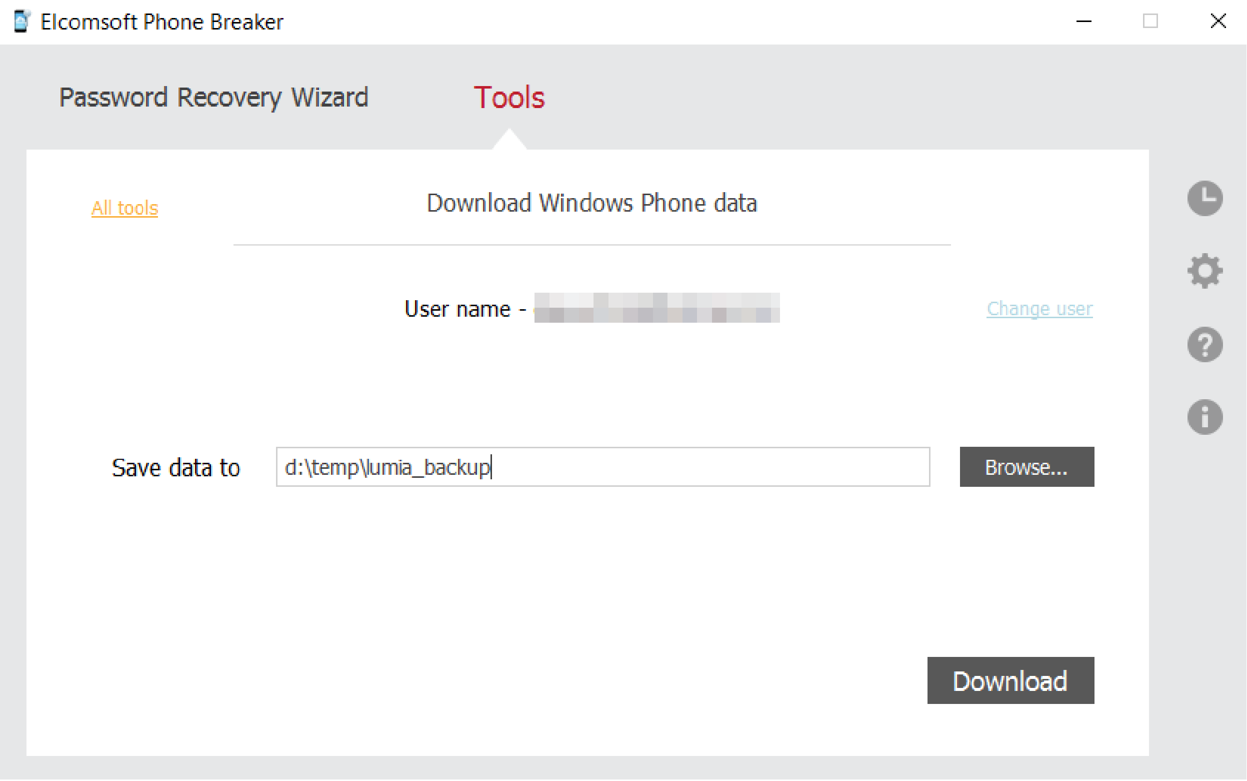
Download Windows Phone data
Messages, Contacts and Notes



Download Windows Phone data

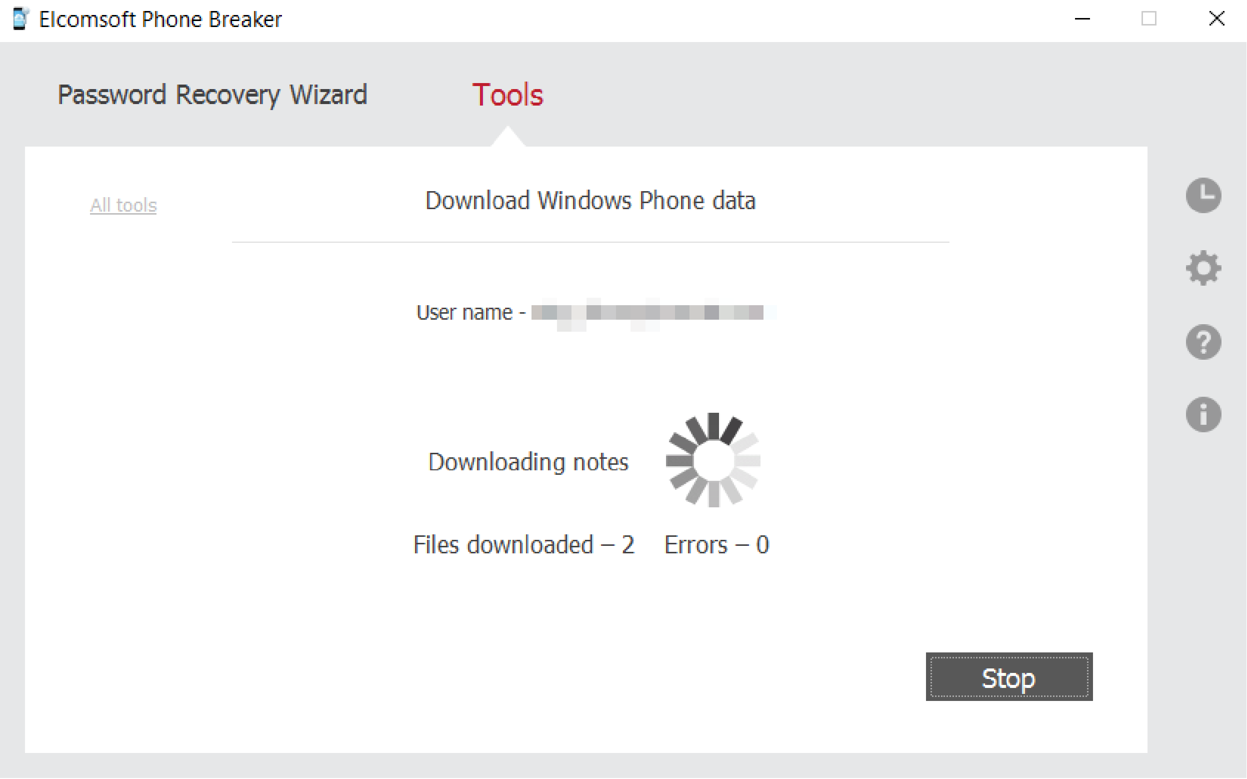
User name [redacted] (example@example.com)

Password ●●●●●●●●●●



User name - [redacted]

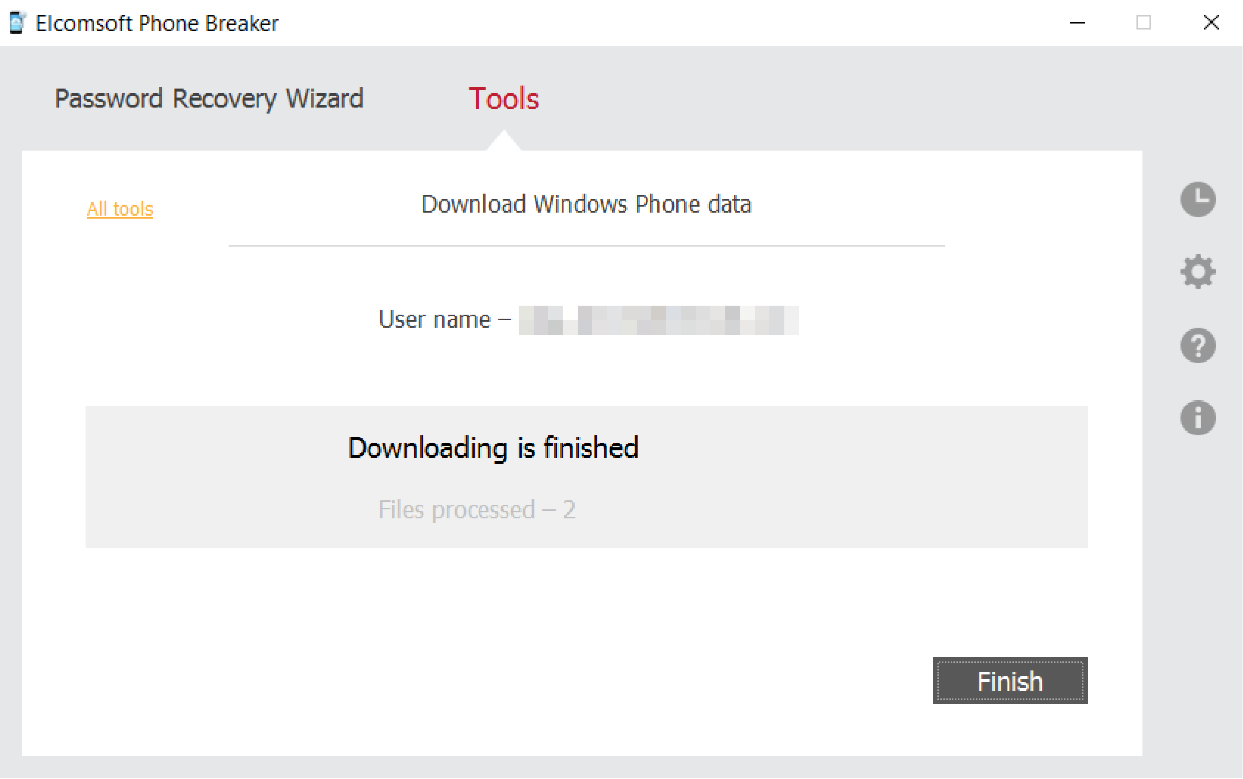
Save data to d:\temp\lumia_backup



User name - [redacted]

Downloading notes

Files downloaded – 2 Errors – 0



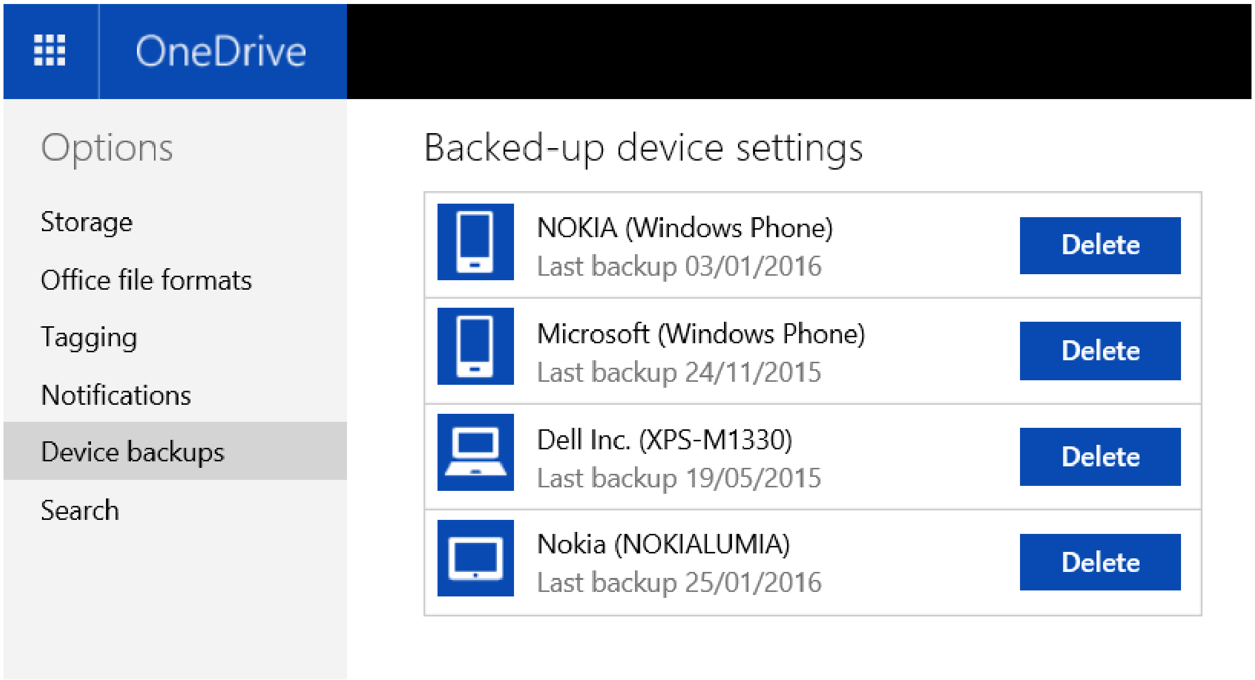
Elcomsoft Phone Breaker

Download Windows Phone data

User name – [redacted]

Downloading is finished

Files processed – 2



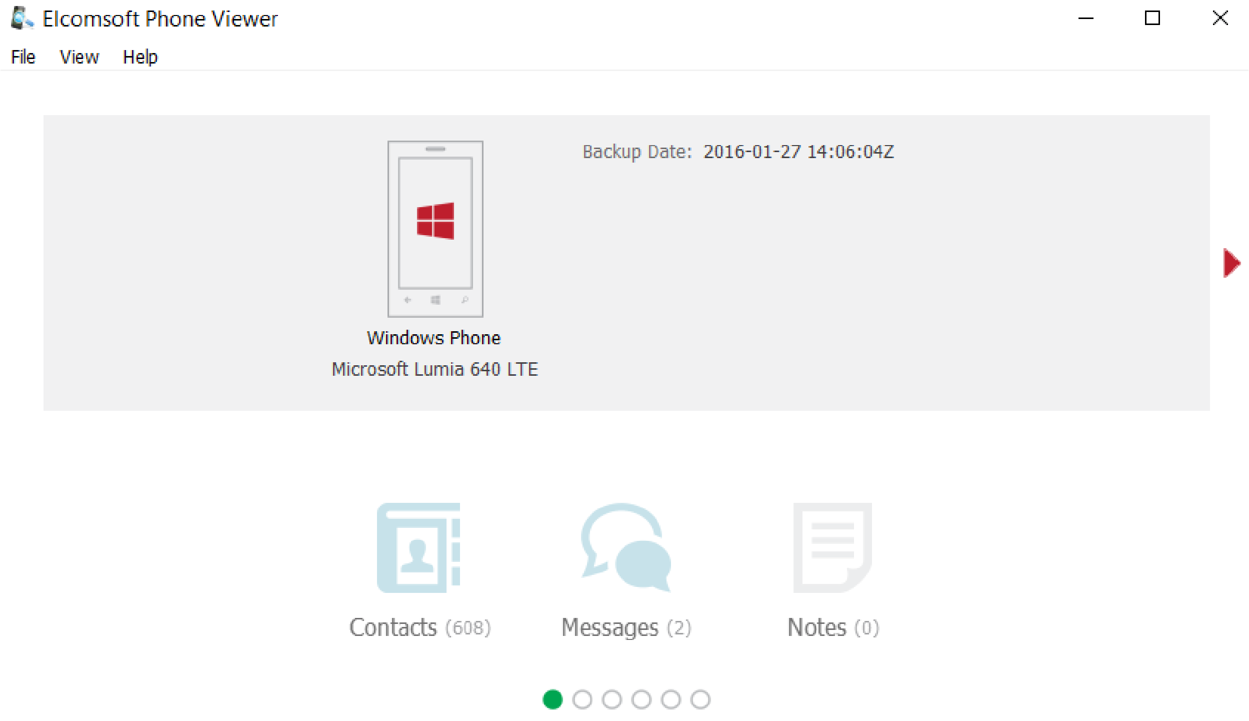
Backed-up device settings

NOKIA (Windows Phone)
Last backup 03/01/2016

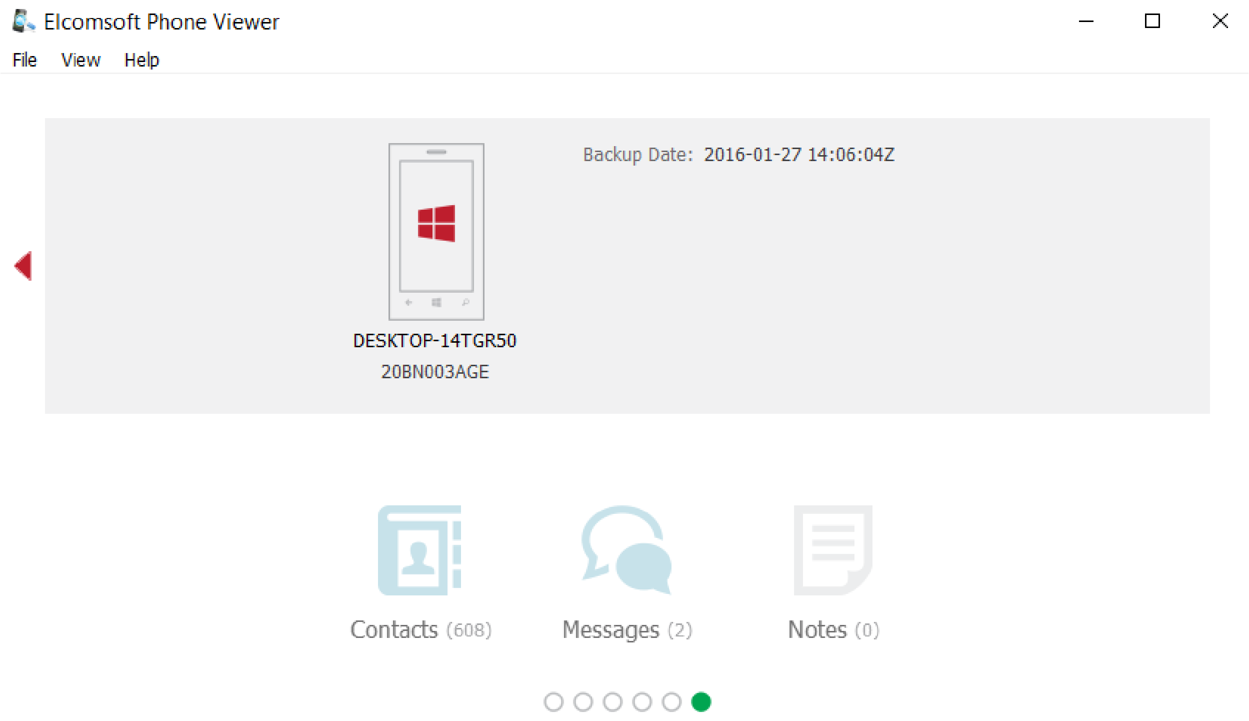
Microsoft (Windows Phone)
Last backup 24/11/2015

Dell Inc. (XPS-M1330)
Last backup 19/05/2015

Nokia (NOKIALUMIA)
Last backup 25/01/2016

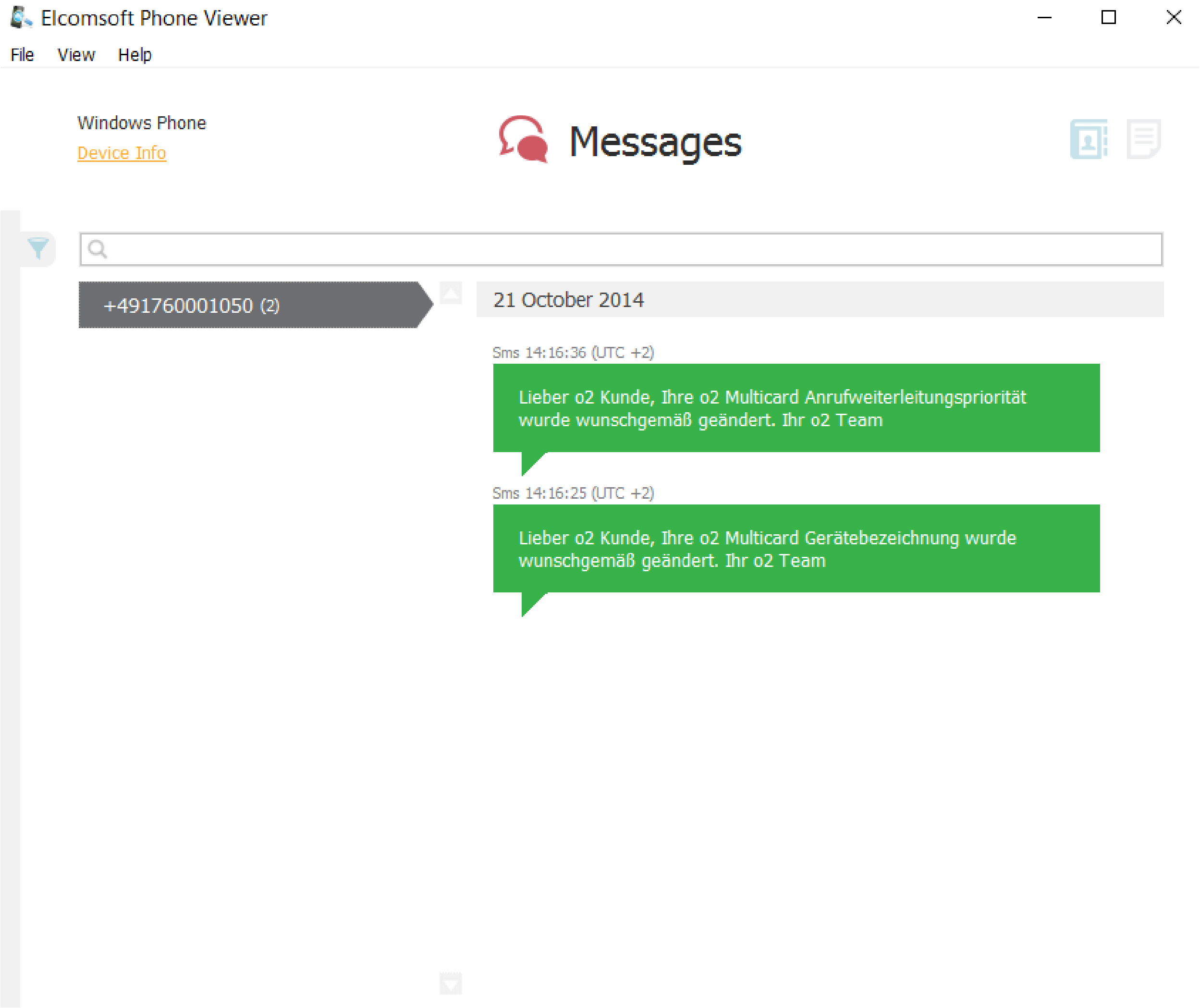


Backup Date: 2016-01-27 14:06:04Z



Backup Date: 2016-01-27 14:06:04Z

DESKTOP-14TGR50
20BN003AGE



+491760001050 (2)

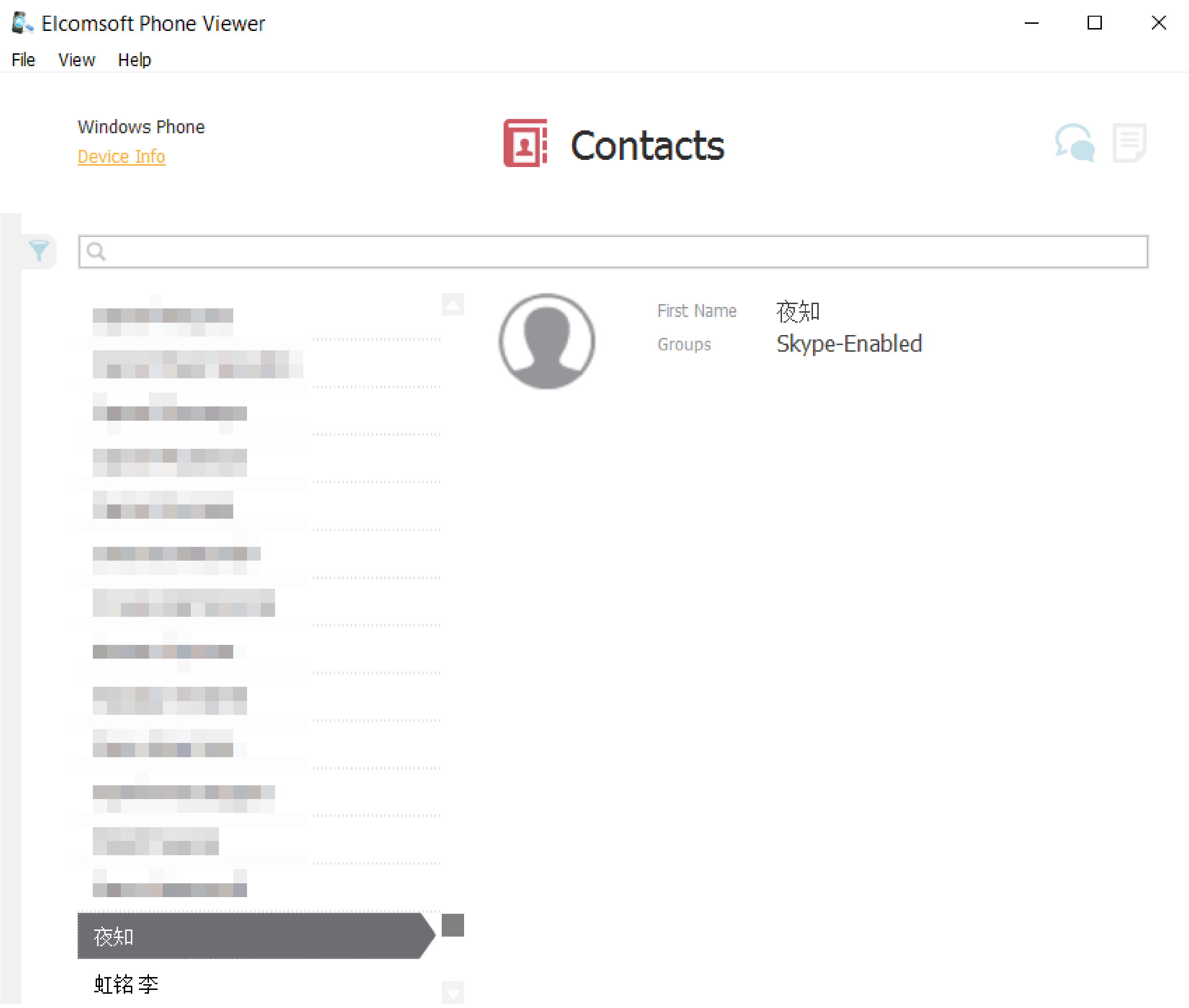
21 October 2014

Sms 14:16:36 (UTC +2)

Lieber o2 Kunde, Ihre o2 Multicard Anrufweiterleitungspriorität wurde wunschgemäß geändert. Ihr o2 Team

Sms 14:16:25 (UTC +2)

Lieber o2 Kunde, Ihre o2 Multicard Gerätebezeichnung wurde wunschgemäß geändert. Ihr o2 Team



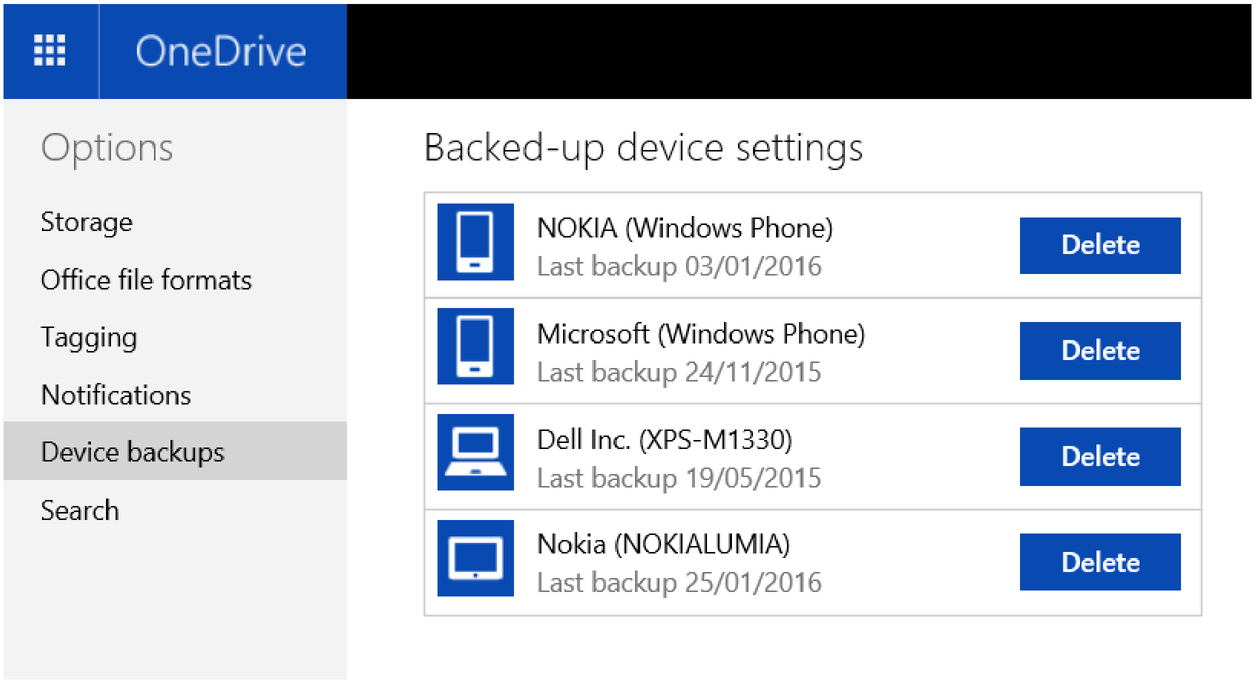
[redacted]

夜知

虹铭 李

First Name 夜知

Groups Skype-Enabled



Backed-up device settings

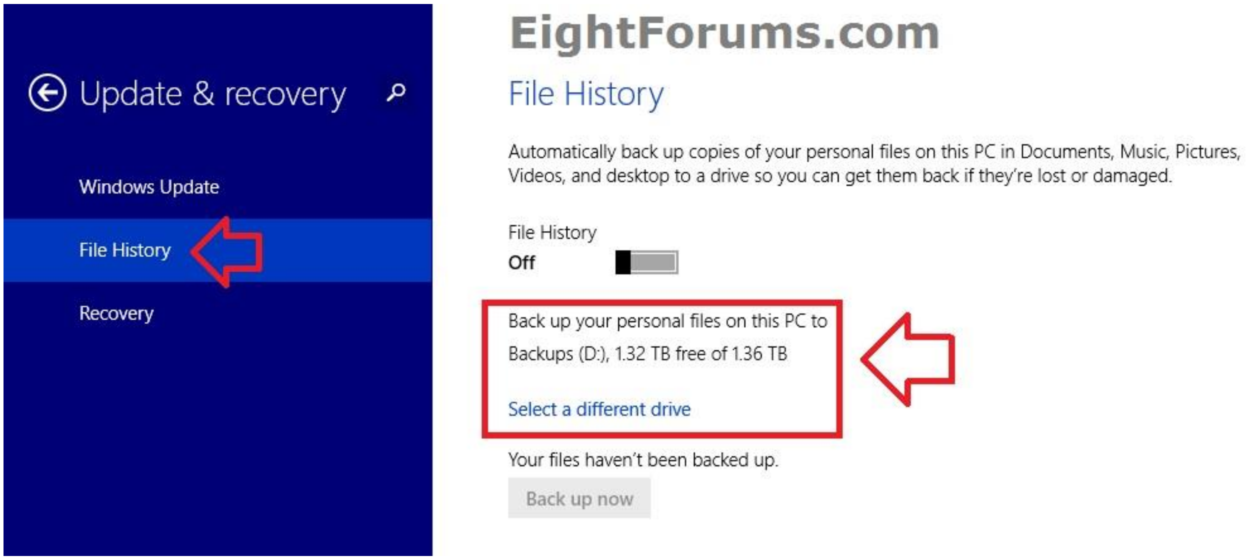
NOKIA (Windows Phone)
Last backup 03/01/2016

Microsoft (Windows Phone)
Last backup 24/11/2015

Dell Inc. (XPS-M1330)
Last backup 19/05/2015

Nokia (NOKIALUMIA)
Last backup 25/01/2016

Chapter 8: Acquisition - Approaching Windows 8, 8.1, 10, and RT Tablets



File History

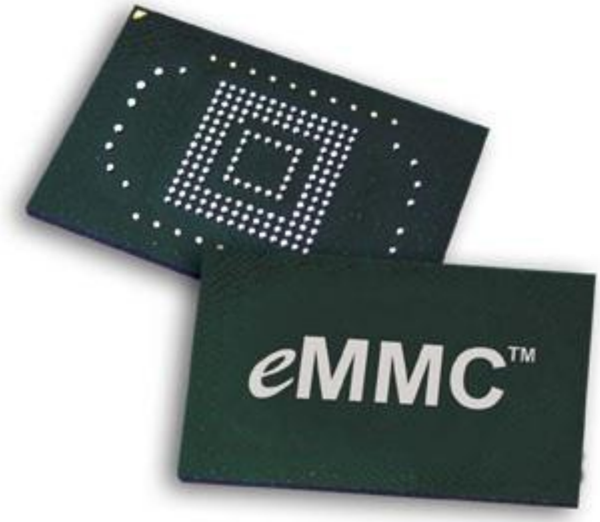
Automatically back up copies of your personal files on this PC in Documents, Music, Pictures, Videos, and desktop to a drive so you can get them back if they're lost or damaged.

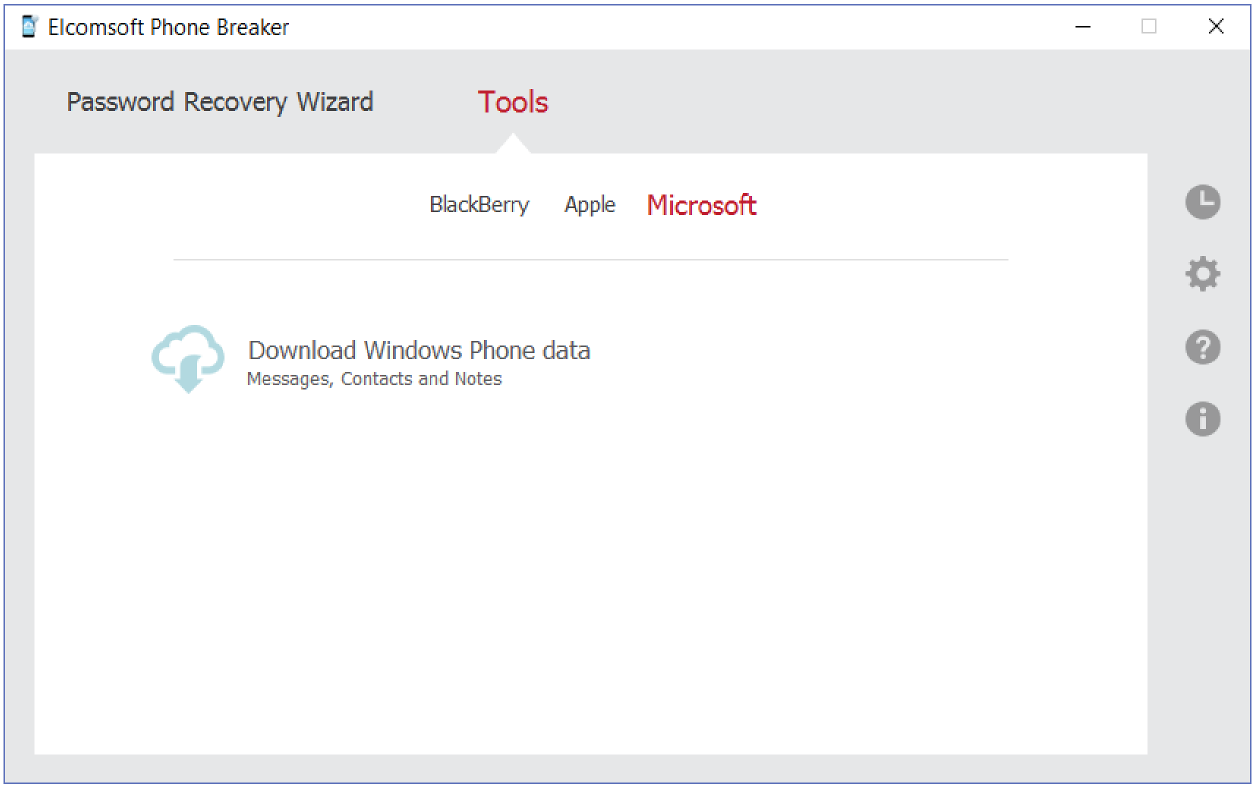
File History
Off

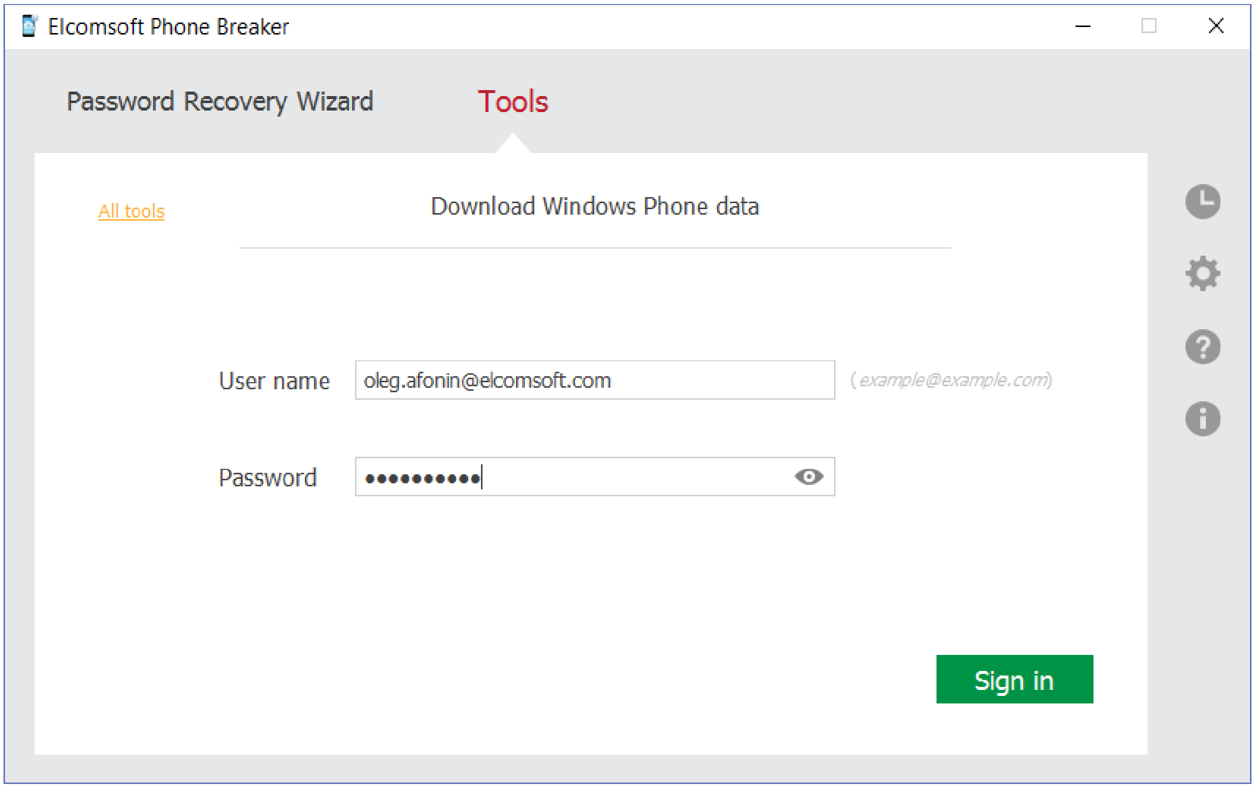
Back up your personal files on this PC to
Backups (D:), 1.32 TB free of 1.36 TB

Select a different drive

Your files haven't been backed up.

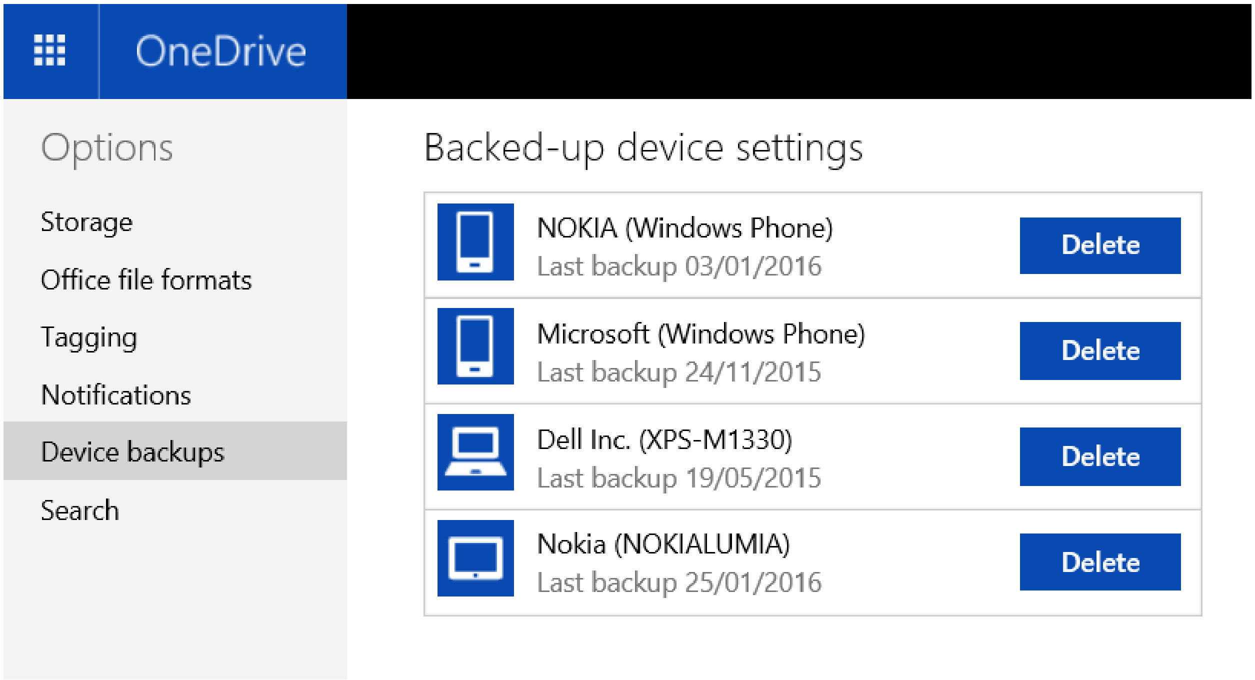






User name oleg.afonin@elcomsoft.com

Password ●●●●●●●●●●



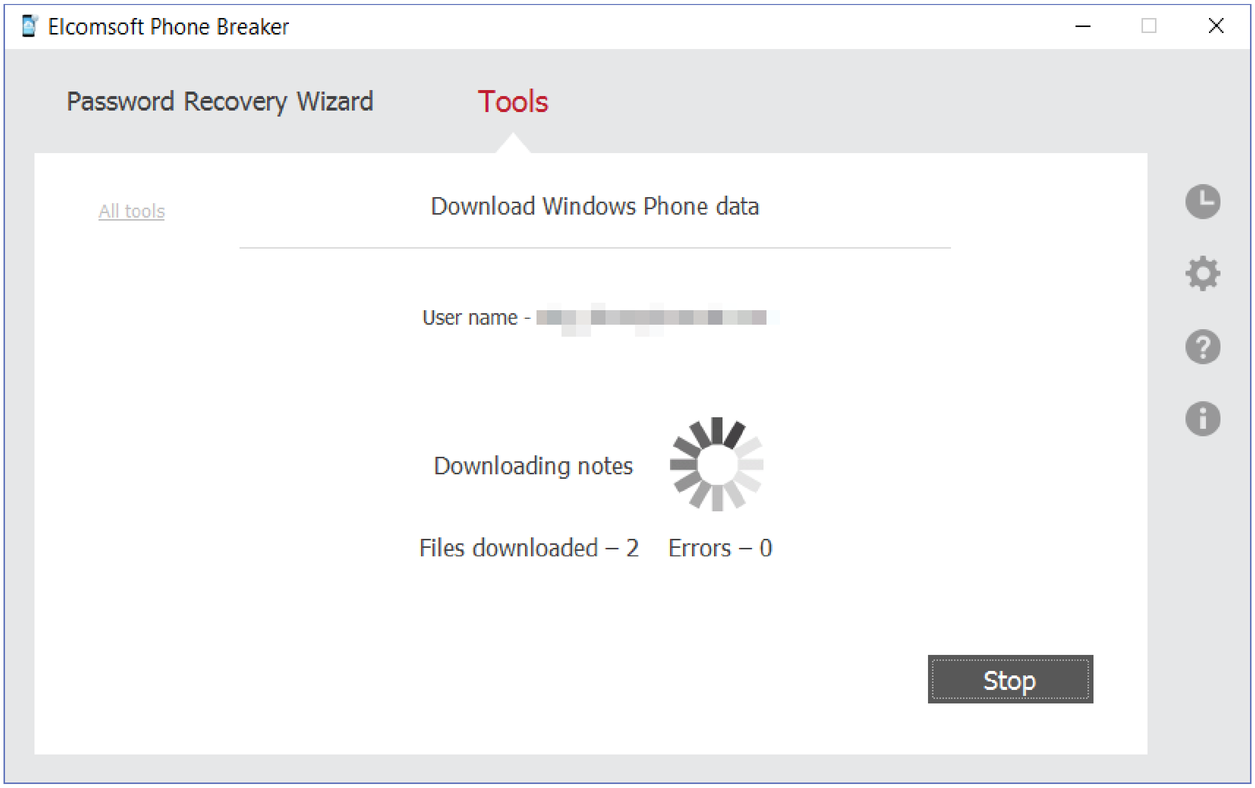
Backed-up device settings

NOKIA (Windows Phone)
Last backup 03/01/2016

Microsoft (Windows Phone)
Last backup 24/11/2015

Dell Inc. (XPS-M1330)
Last backup 19/05/2015

Nokia (NOKIALUMIA)
Last backup 25/01/2016

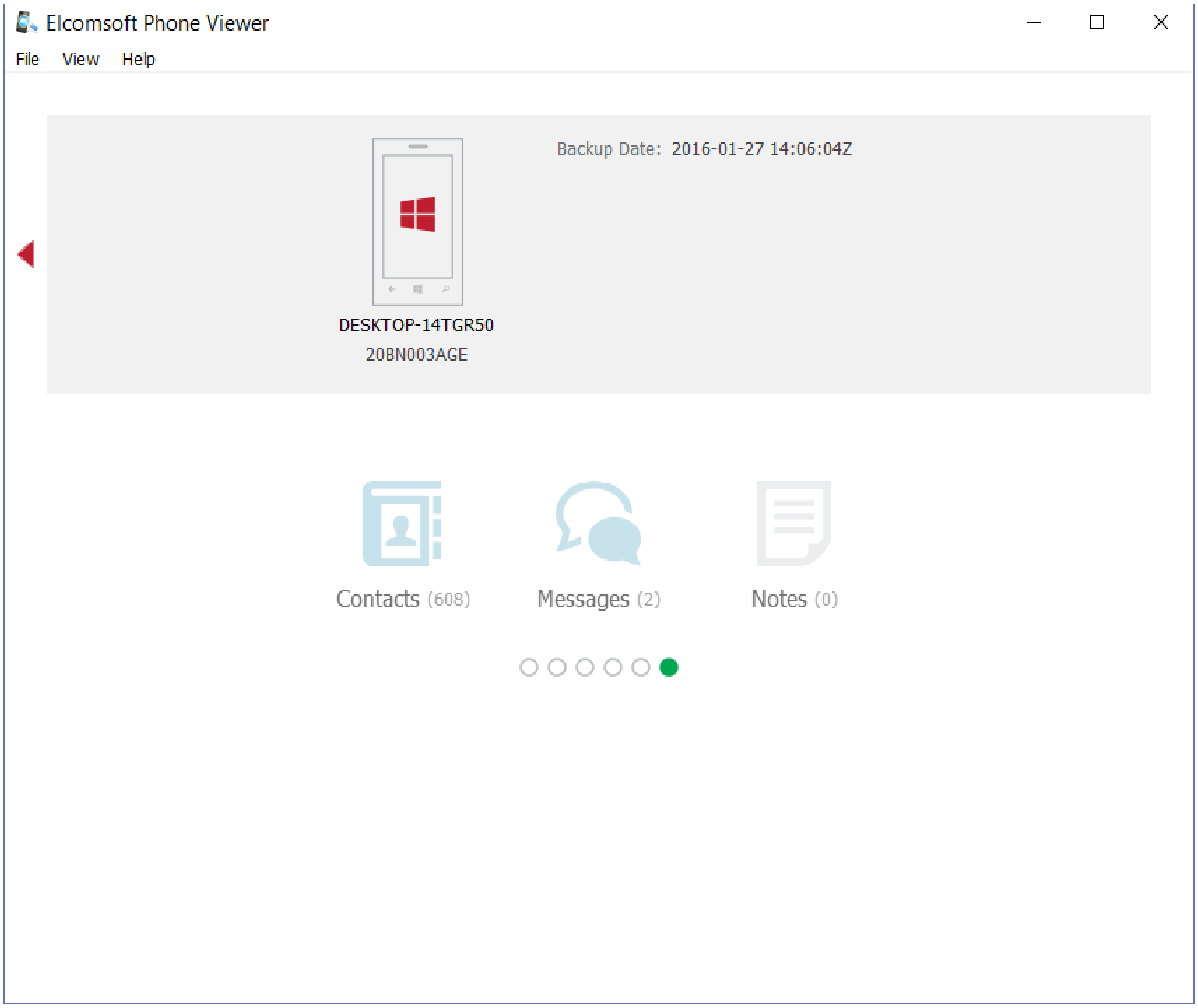


Download Windows Phone data

User name - [redacted]

Downloading notes

Files downloaded – 2 Errors – 0



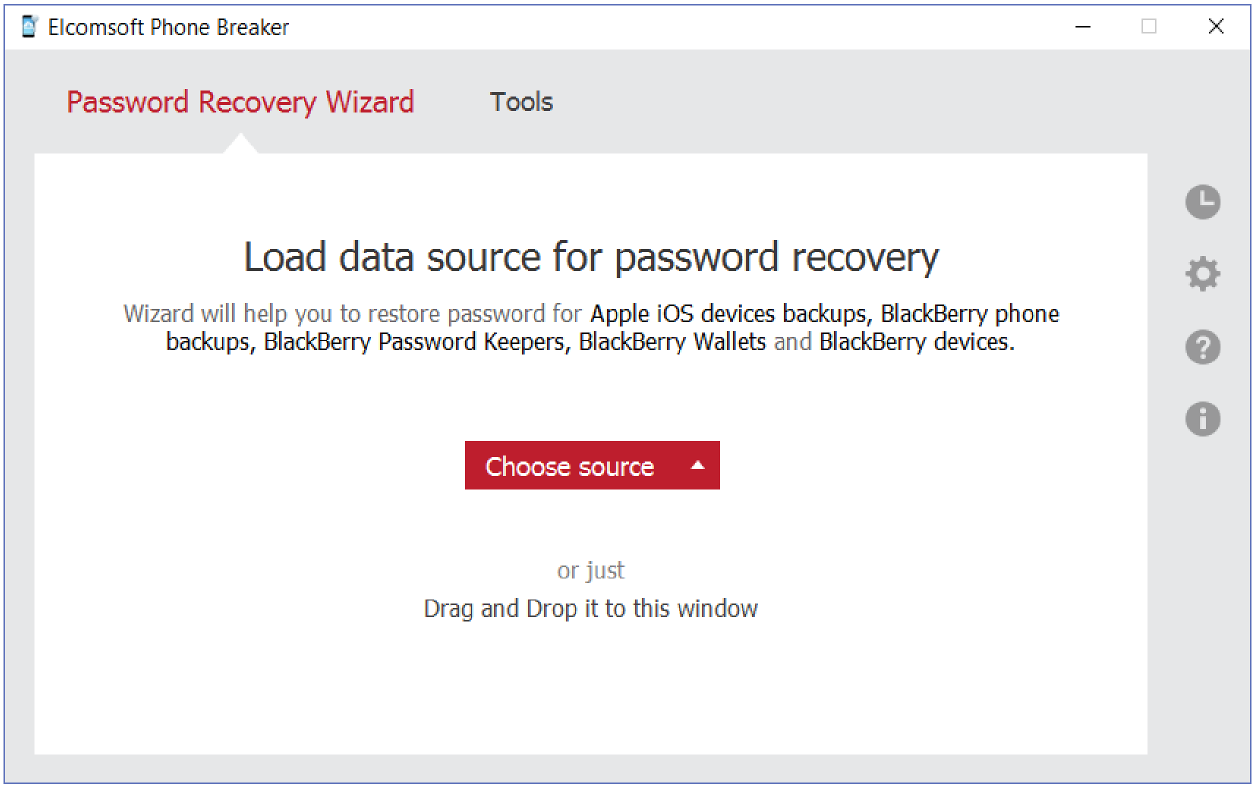
Backup Date: 2016-01-27 14:06:04Z

DESKTOP-14TGR50
20BN003AGE

Contacts (608)

Messages (2)

Notes (0)

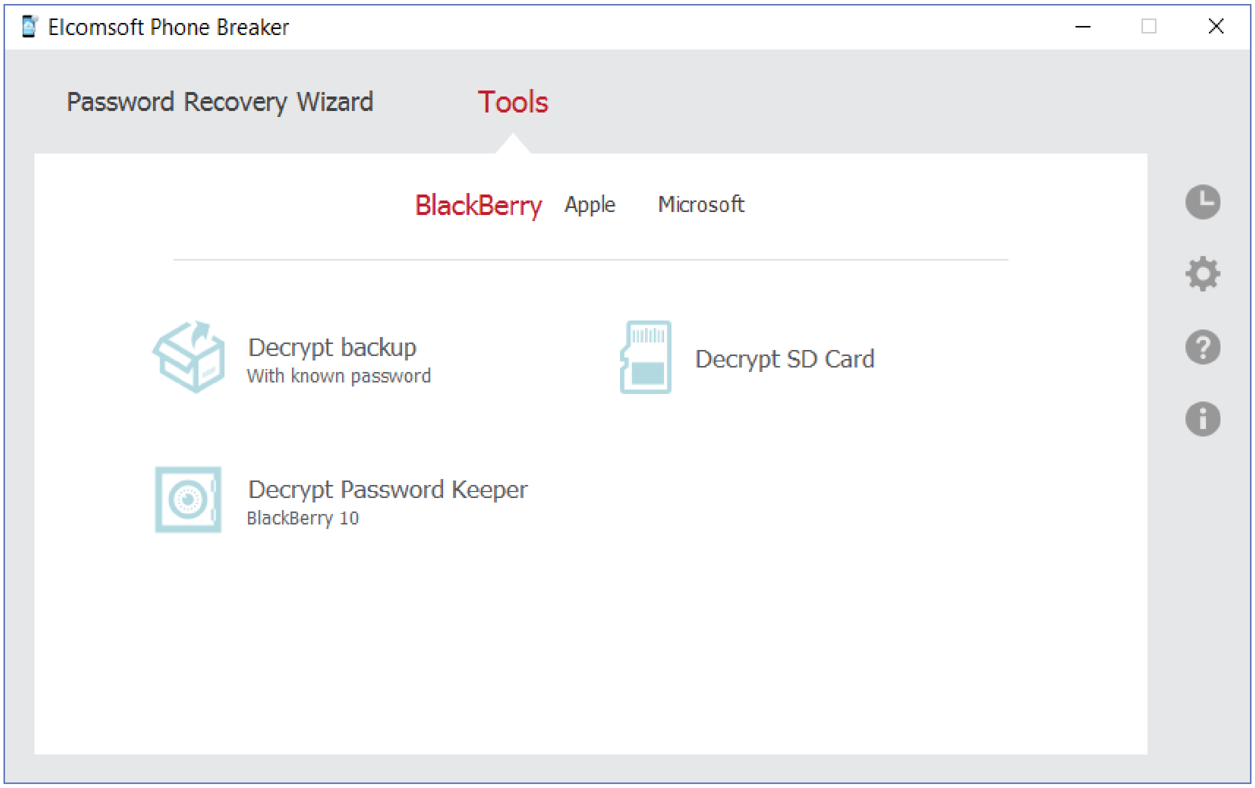


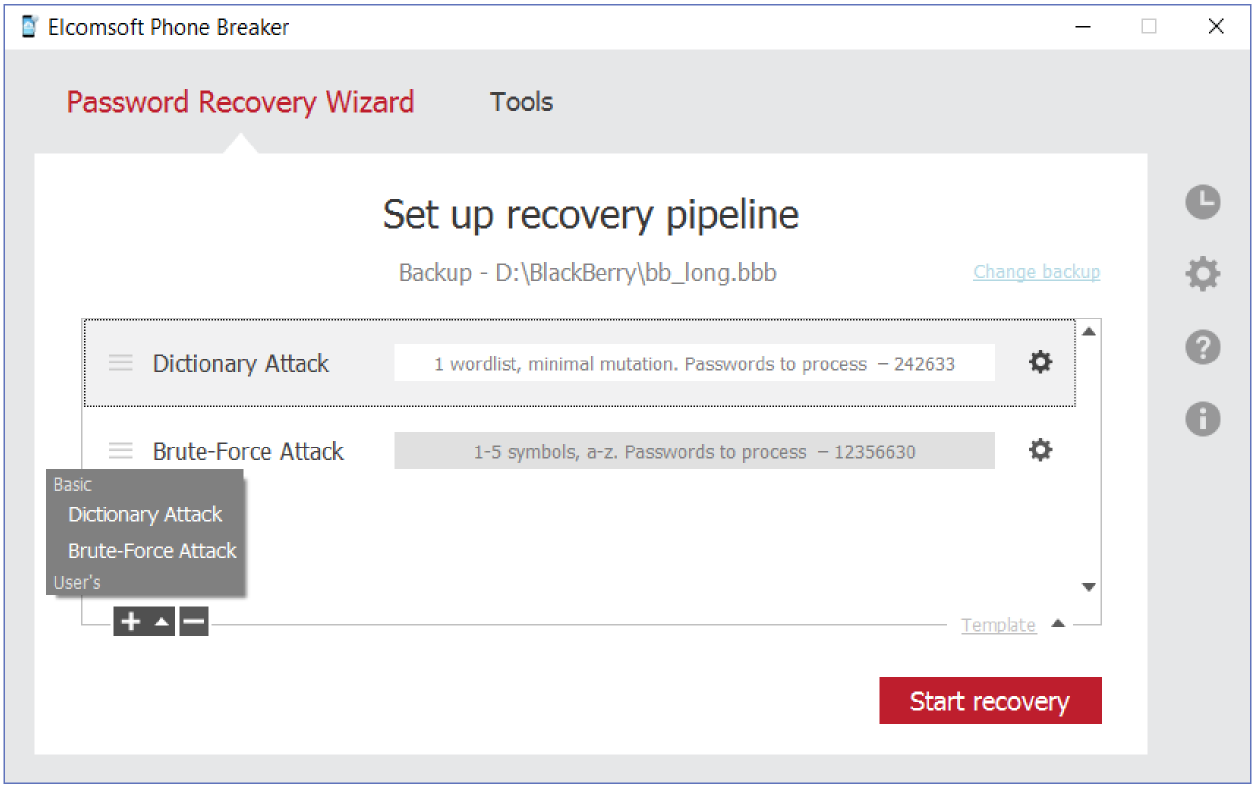
Load data source for password recovery

Wizard will help you to restore password for Apple iOS devices backups, BlackBerry phone backups, BlackBerry Password Keepers, BlackBerry Wallets and BlackBerry devices.

or just

Drag and Drop it to this window





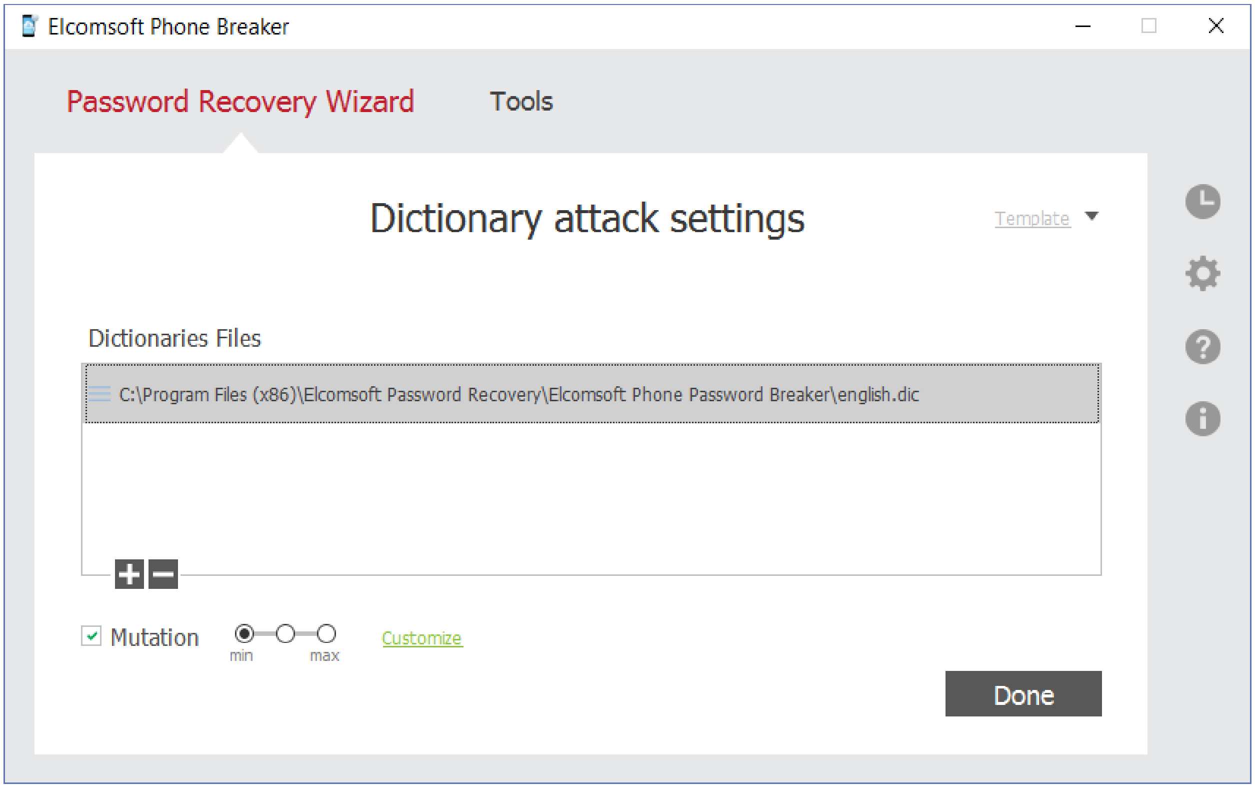
Elcomsoft Phone Breaker

Set up recovery pipeline

Backup - D:\BlackBerry\bb_long.bbb

Dictionary Attack — 1 wordlist, minimal mutation. Passwords to process – 242633

Brute-Force Attack — 1-5 symbols, a-z. Passwords to process – 12356630



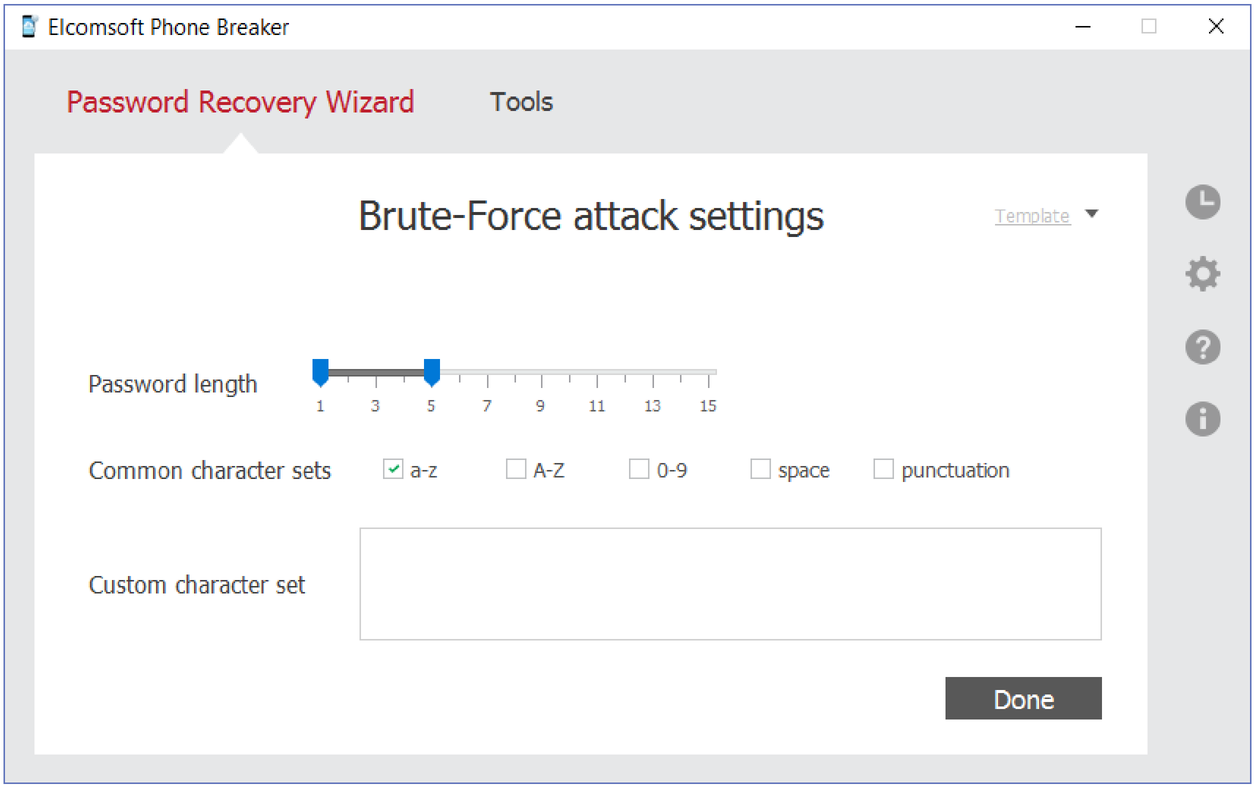
Elcomsoft Phone Breaker

Dictionary attack settings

Dictionaries Files

C:\Program Files (x86)\Elcomsoft Password Recovery\Elcomsoft Phone Password Breaker\english.dic

☑ Mutation ● min ○ ○ max

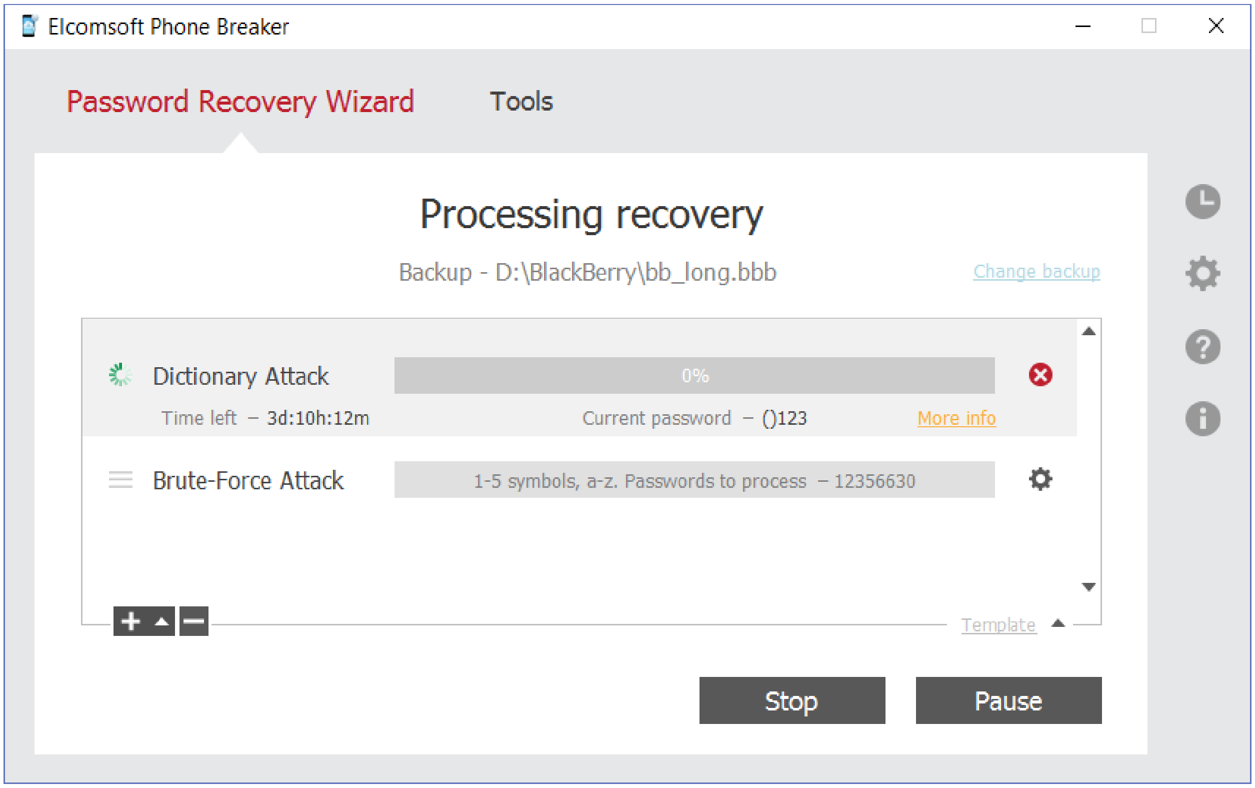


Brute-Force attack settings

Password length: 1 – 5

Common character sets ☑ a-z □ A-Z □ 0-9 □ space □ punctuation

Custom character set



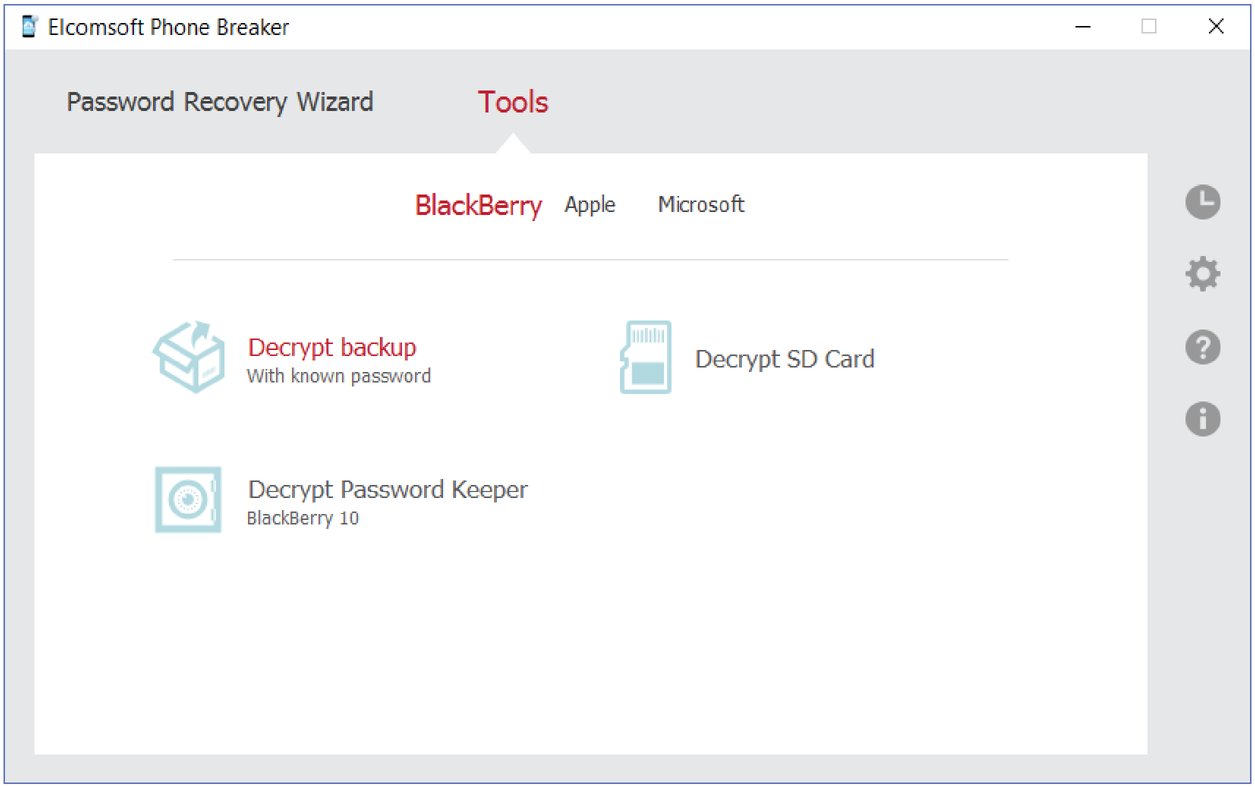
Processing recovery

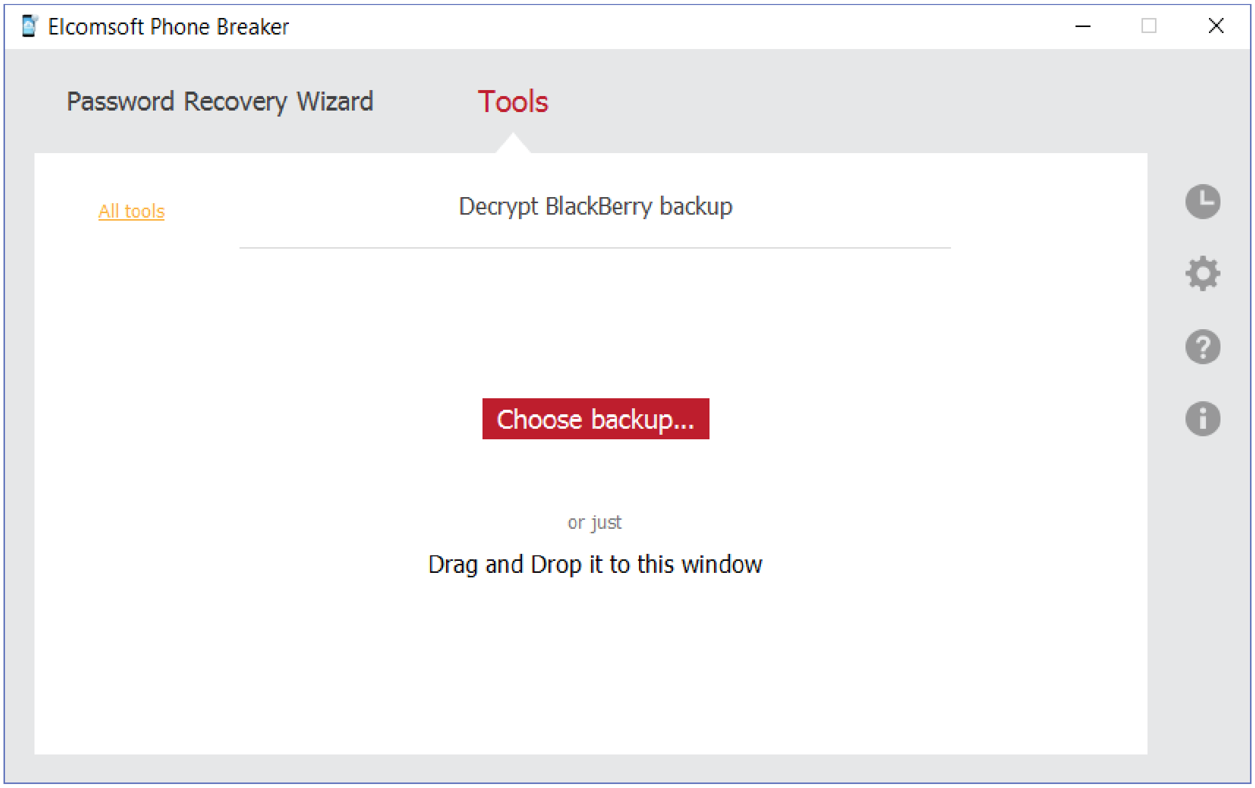
Backup - D:\BlackBerry\bb_long.bbb

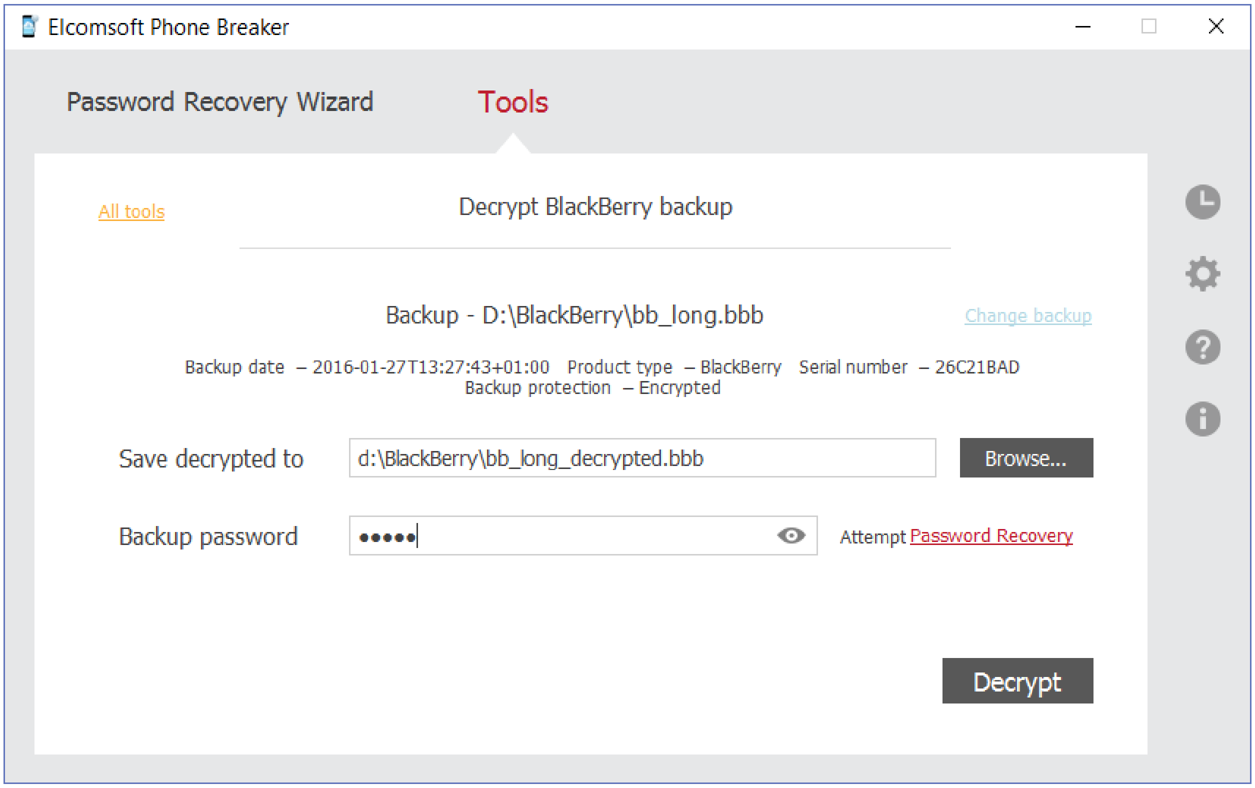
Dictionary Attack 0%

Time left – 3d:10h:12m Current password – ()123

Brute-Force Attack 1-5 symbols, a-z. Passwords to process – 12356630


Elcomsoft Phone Breaker
Password Recovery Wizard
Tools
BlackBerry
Apple
Microsoft
Decrypt backup
With known password
Decrypt SD Card
Decrypt Password Keeper
BlackBerry 10


Elcomsoft Phone Breaker
Password Recovery Wizard
Tools
All tools
Decrypt BlackBerry backup
Choose backup...
or just
Drag and Drop it to this window



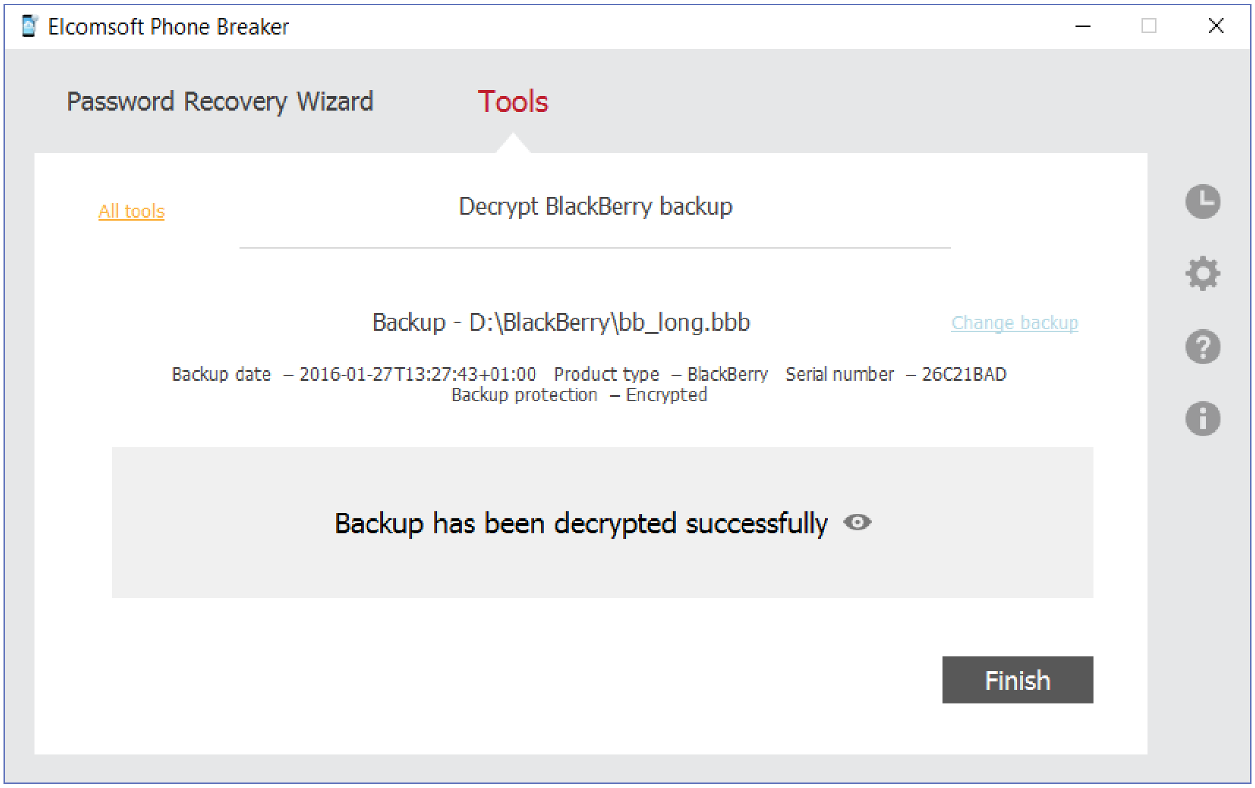
Decrypt BlackBerry backup

Backup - D:\BlackBerry\bb_long.bbb

Backup date – 2016-01-27T13:27:43+01:00 Product type – BlackBerry Serial number – 26C21BAD
Backup protection – Encrypted

Save decrypted to: d:\BlackBerry\bb_long_decrypted.bbb

Backup password: •••••

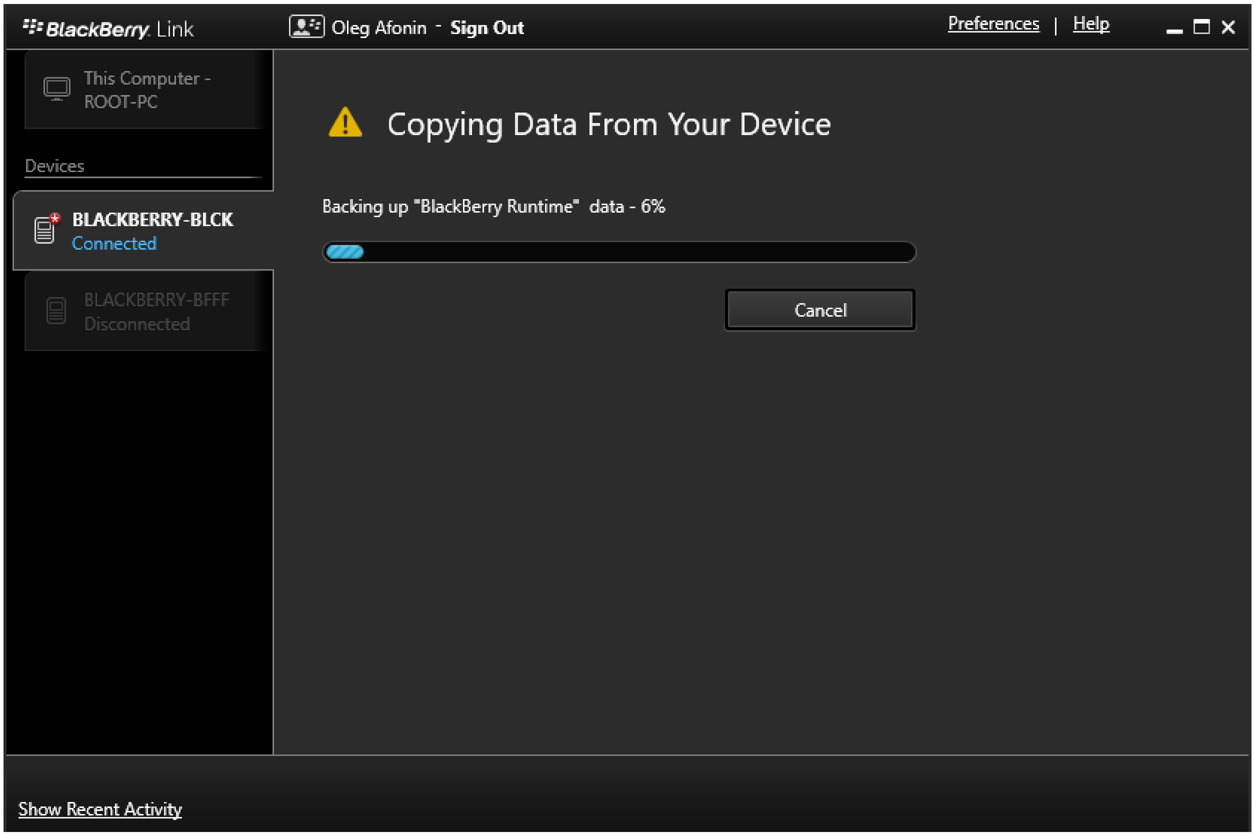


Decrypt BlackBerry backup

Backup - D:\BlackBerry\bb_long.bbb

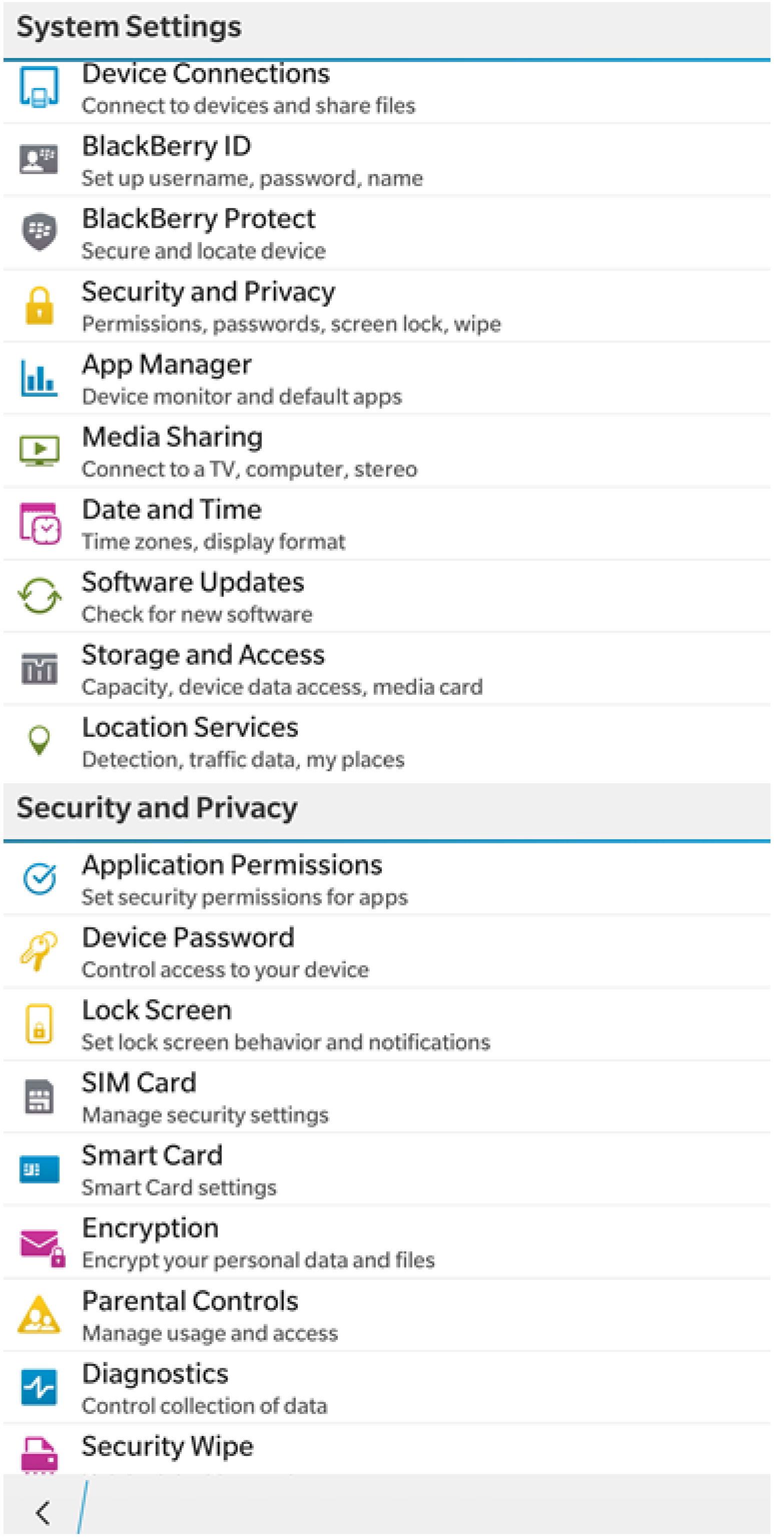
Backup date – 2016-01-27T13:27:43+01:00 Product type – BlackBerry Serial number – 26C21BAD
Backup protection – Encrypted

Backup has been decrypted successfully



Copying Data From Your Device

Backing up "BlackBerry Runtime" data - 6%



System Settings

Device Connections
Connect to devices and share files

BlackBerry ID
Set up username, password, name

BlackBerry Protect
Secure and locate device

Security and Privacy
Permissions, passwords, screen lock, wipe

App Manager
Device monitor and default apps

Media Sharing
Connect to a TV, computer, stereo

Date and Time
Time zones, display format

Software Updates
Check for new software

Storage and Access
Capacity, device data access, media card

Location Services
Detection, traffic data, my places

Security and Privacy

Application Permissions
Set security permissions for apps

Device Password
Control access to your device

Lock Screen
Set lock screen behavior and notifications

SIM Card
Manage security settings

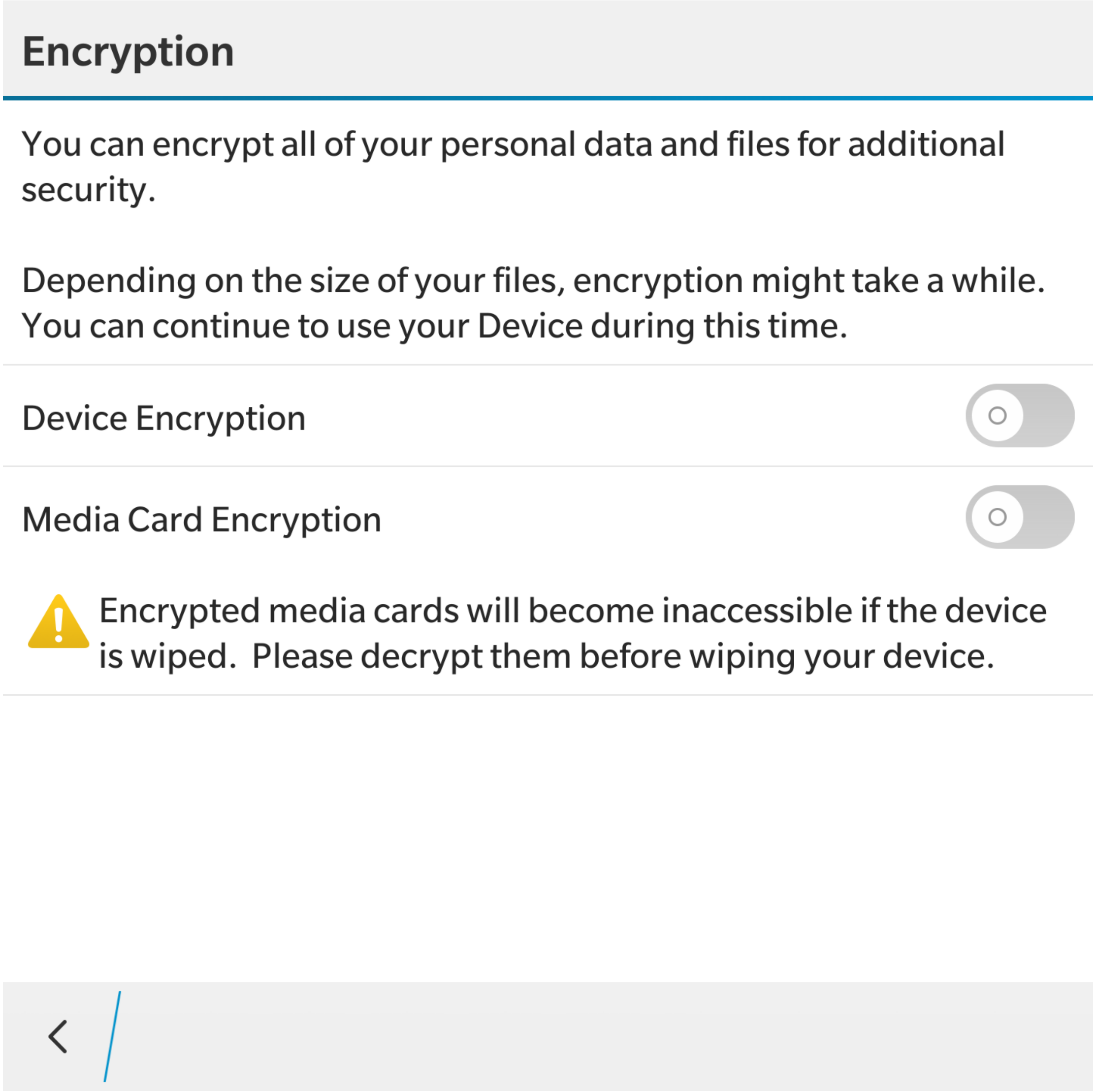
Smart Card
Smart Card settings

Encryption
Encrypt your personal data and files

Parental Controls
Manage usage and access

Diagnostics
Control collection of data

Security Wipe



Encryption

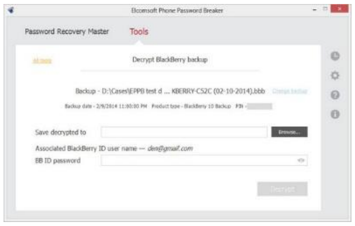
You can encrypt all of your personal data and files for additional security.

Depending on the size of your files, encryption might take a while. You can continue to use your Device during this time.

Device Encryption ○

Media Card Encryption ○

⚠ Encrypted media cards will become inaccessible if the device is wiped. Please decrypt them before wiping your device.



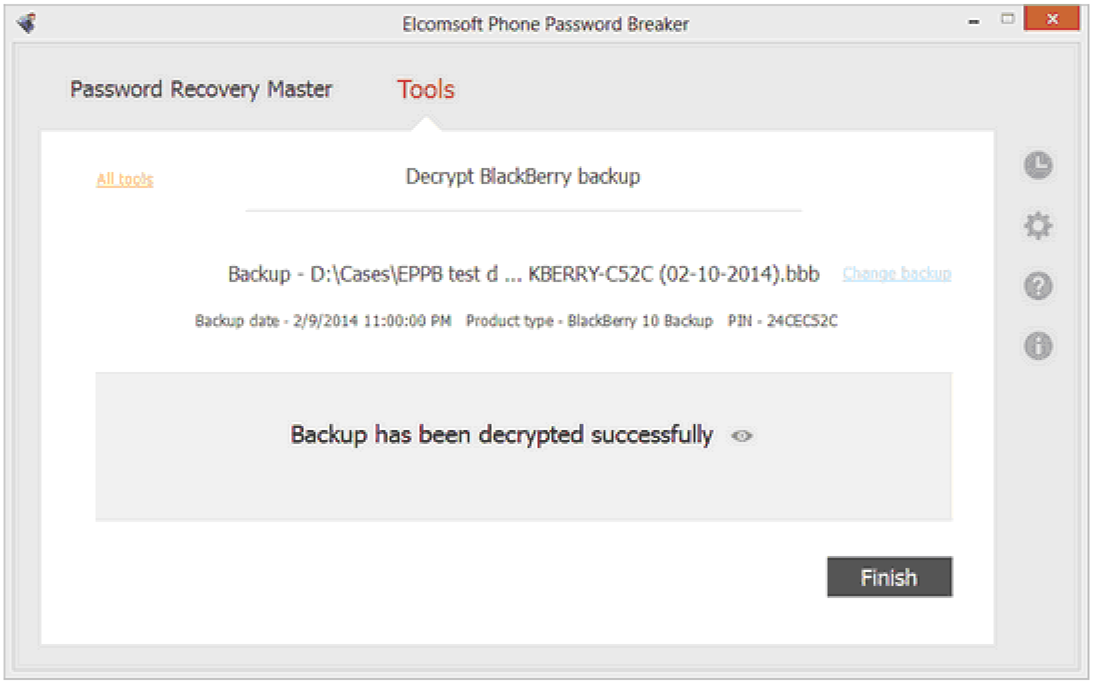
Backup - D:\Cases\EPPB test d ... KBERRY-C52C (02-10-2014).bbb

Backup date - 2/9/2014 11:00:00 PM   Product type - BlackBerry 10 Backup   PIN - [redacted]

Save decrypted to

Associated BlackBerry ID user name — *den@gmail.com*

BB ID password

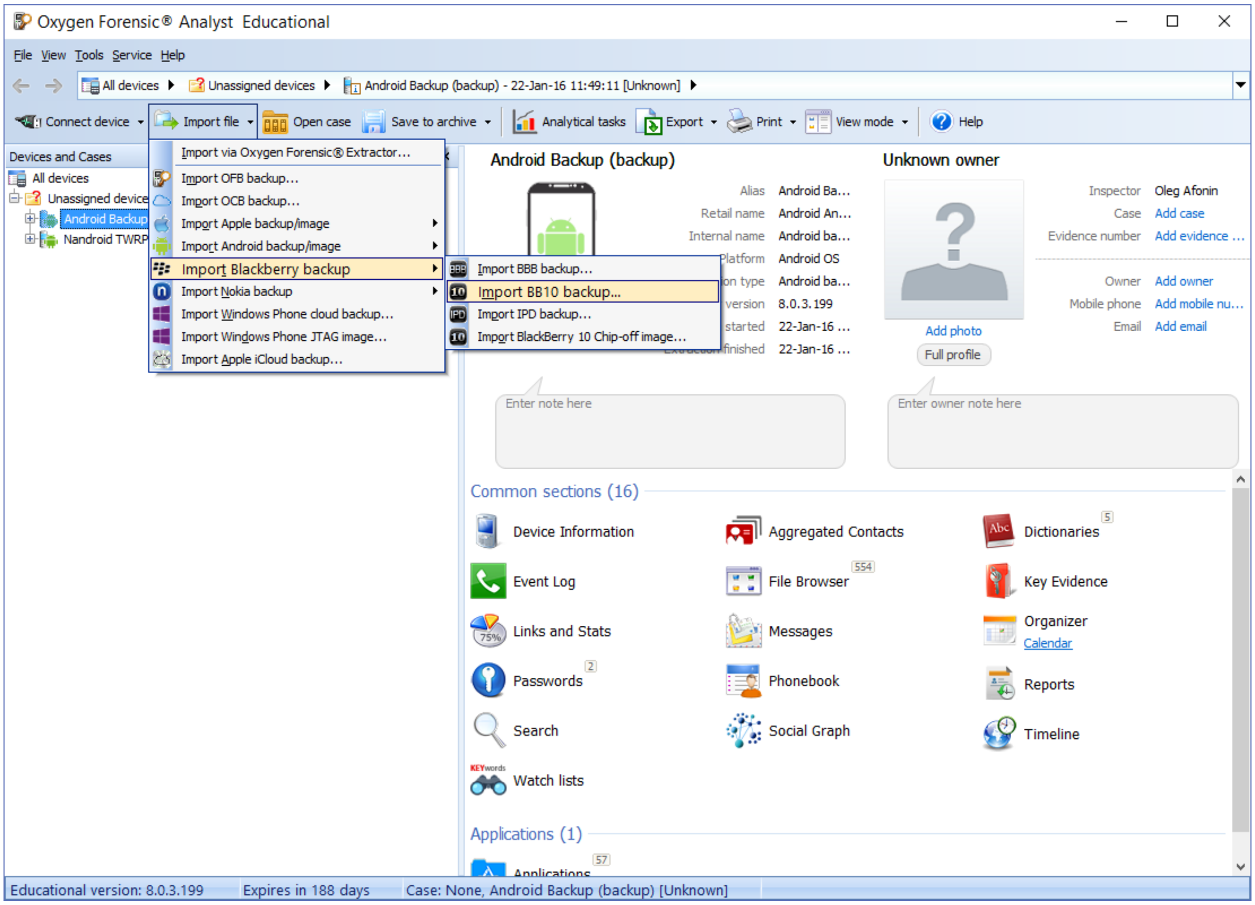


Decrypt BlackBerry backup

Backup - D:\Cases\EPPB test d ... KBERRY-C52C (02-10-2014).bbb Change backup

Backup date - 2/9/2014 11:00:00 PM Product type - BlackBerry 10 Backup PIN - 24CEC52C

Backup has been decrypted successfully



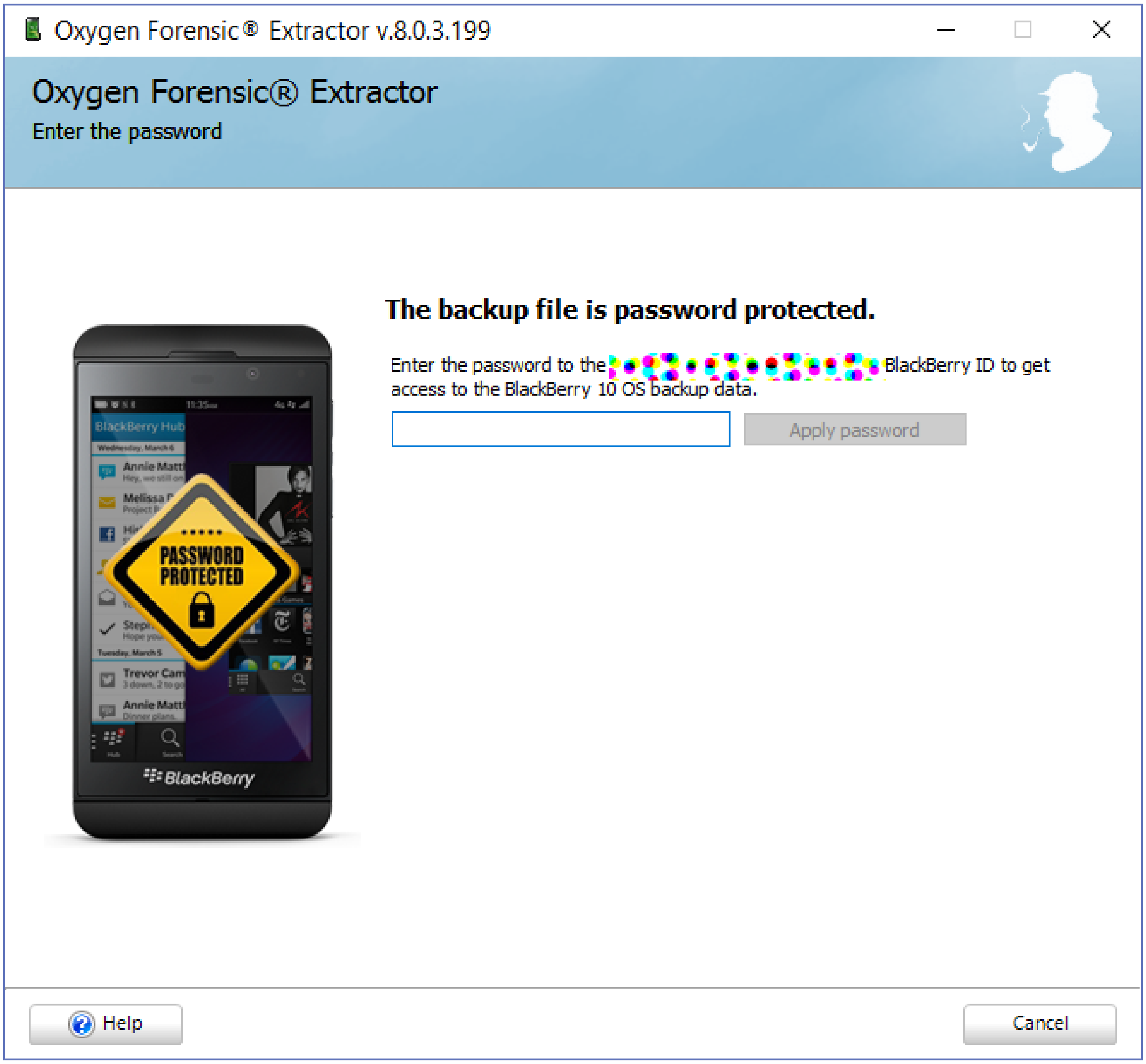
Android Backup (backup)

Alias	Android Ba...
Retail name	Android An...
Internal name	Android ba...
Platform	Android OS
on type	Android ba...
version	8.0.3.199
started	22-Jan-16 ...
Extraction finished	22-Jan-16 ...

Unknown owner

Inspector	Oleg Afonin
Case	Add case
Evidence number	Add evidence ...
Owner	Add owner
Mobile phone	Add mobile nu...
Email	Add email

Educational version: 8.0.3.199 Expires in 188 days Case: None, Android Backup (backup) [Unknown]



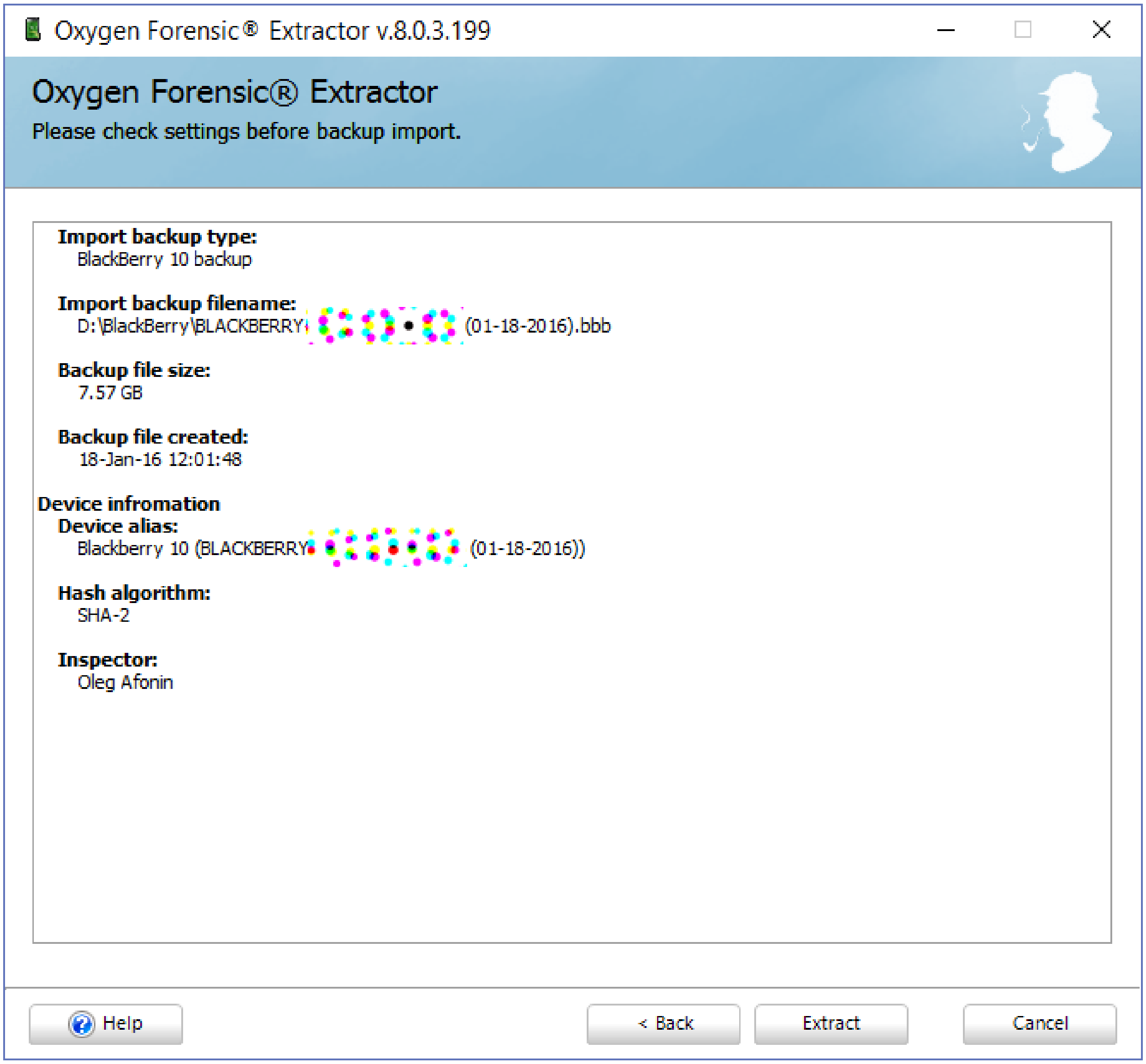
Oxygen Forensic® Extractor v.8.0.3.199

Oxygen Forensic® Extractor

Enter the password

The backup file is password protected.

Enter the password to the [redacted] BlackBerry ID to get access to the BlackBerry 10 OS backup data.



Oxygen Forensic® Extractor

Please check settings before backup import.

Import backup type:
BlackBerry 10 backup

Import backup filename:
D:\BlackBerry\BLACKBERRY[redacted] (01-18-2016).bbb

Backup file size:
7.57 GB

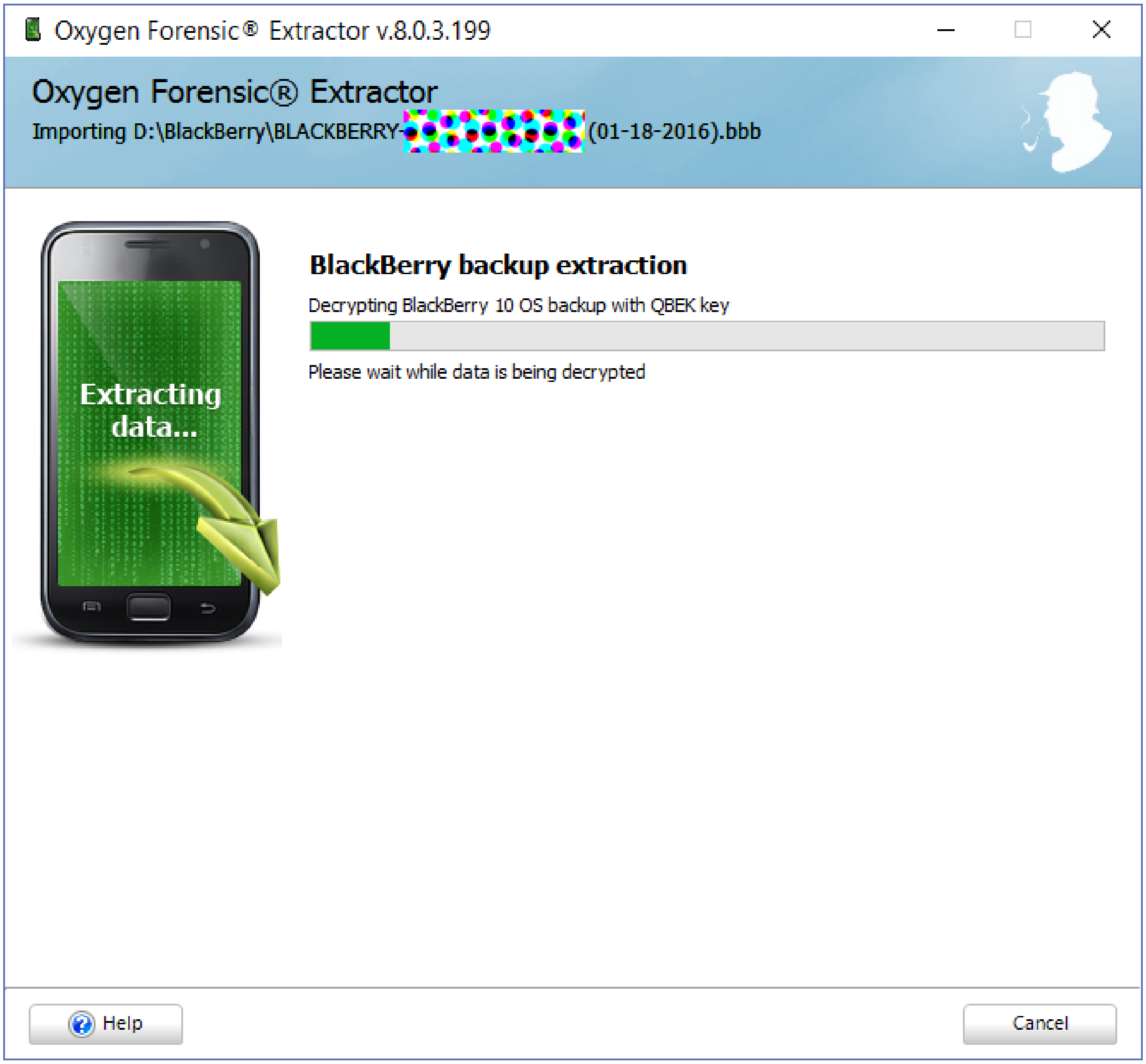
Backup file created:
18-Jan-16 12:01:48

Device infromation

Device alias:
Blackberry 10 (BLACKBERRY[redacted] (01-18-2016))

Hash algorithm:
SHA-2

Inspector:
Oleg Afonin



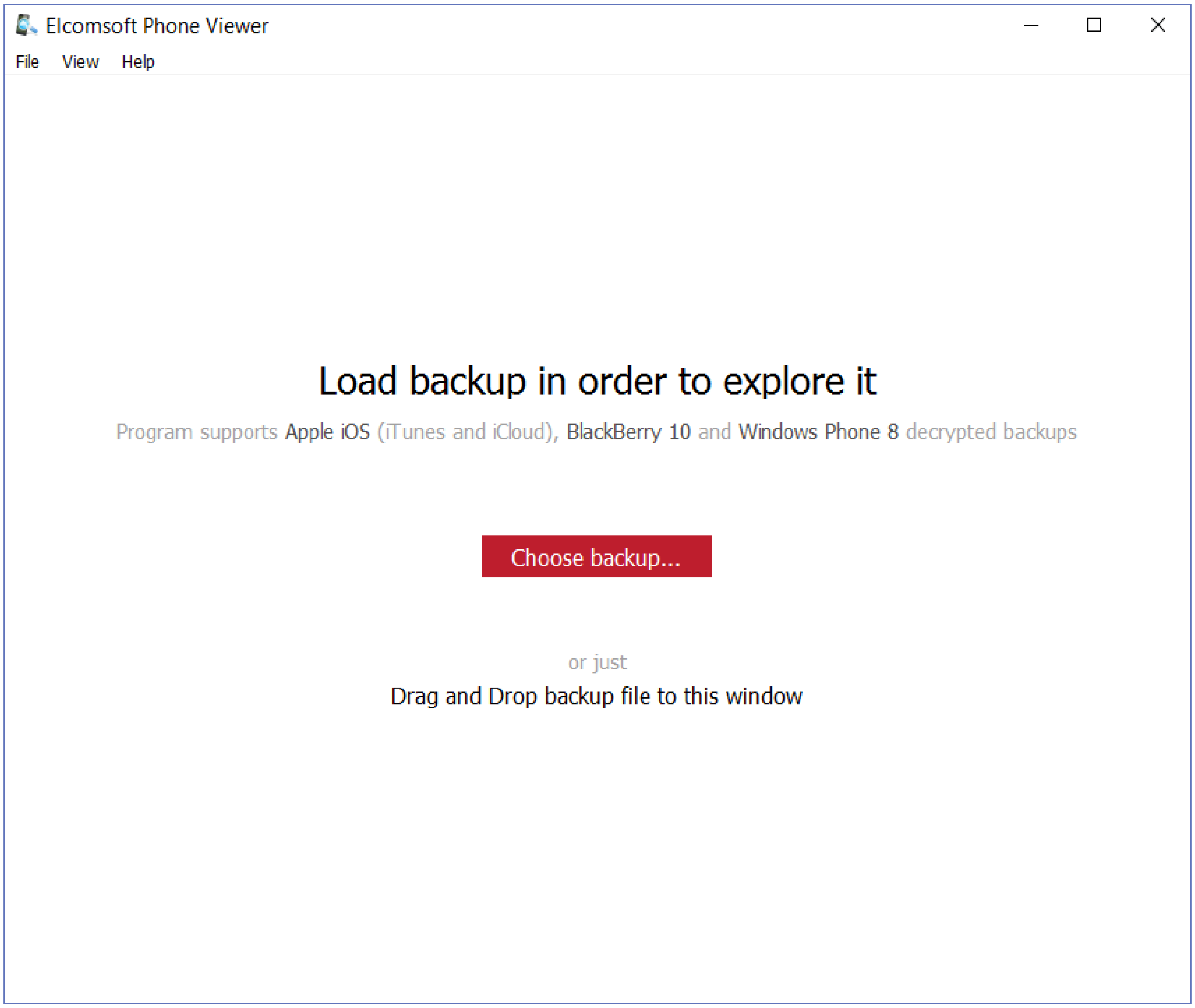
Oxygen Forensic® Extractor

Importing D:\BlackBerry\BLACKBERRY-[redacted](01-18-2016).bbb

BlackBerry backup extraction

Decrypting BlackBerry 10 OS backup with QBEK key

Please wait while data is being decrypted

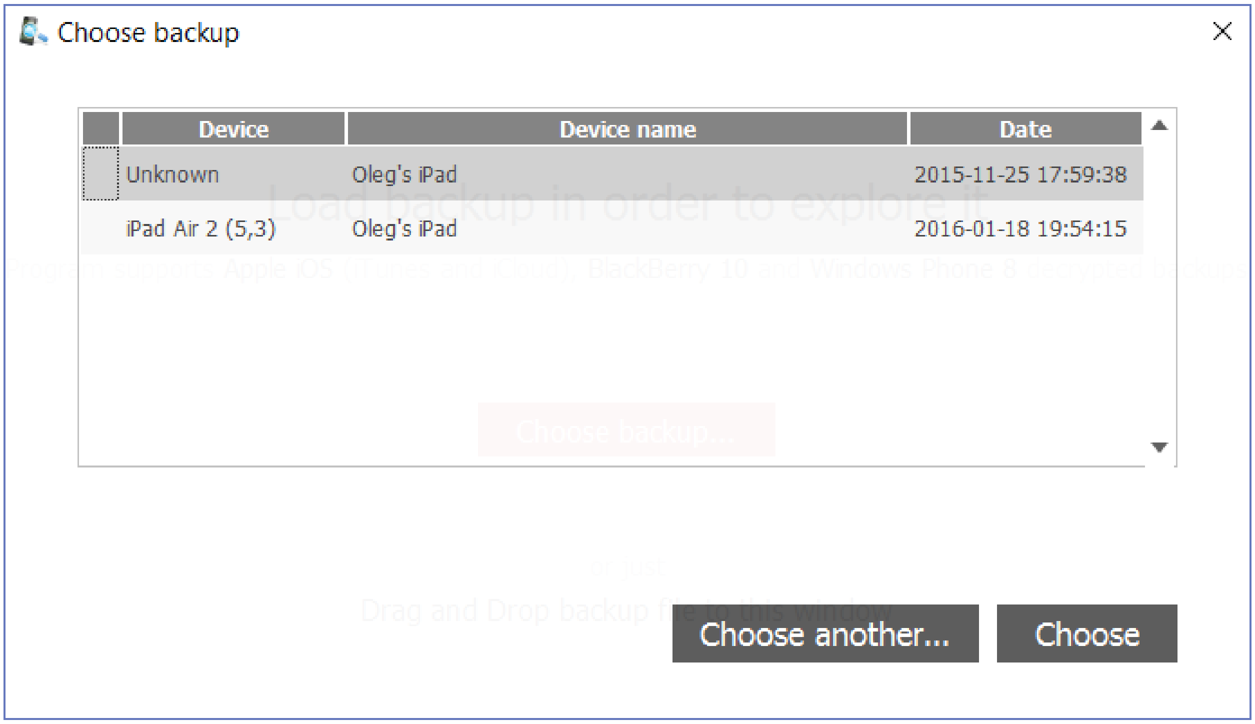


Load backup in order to explore it

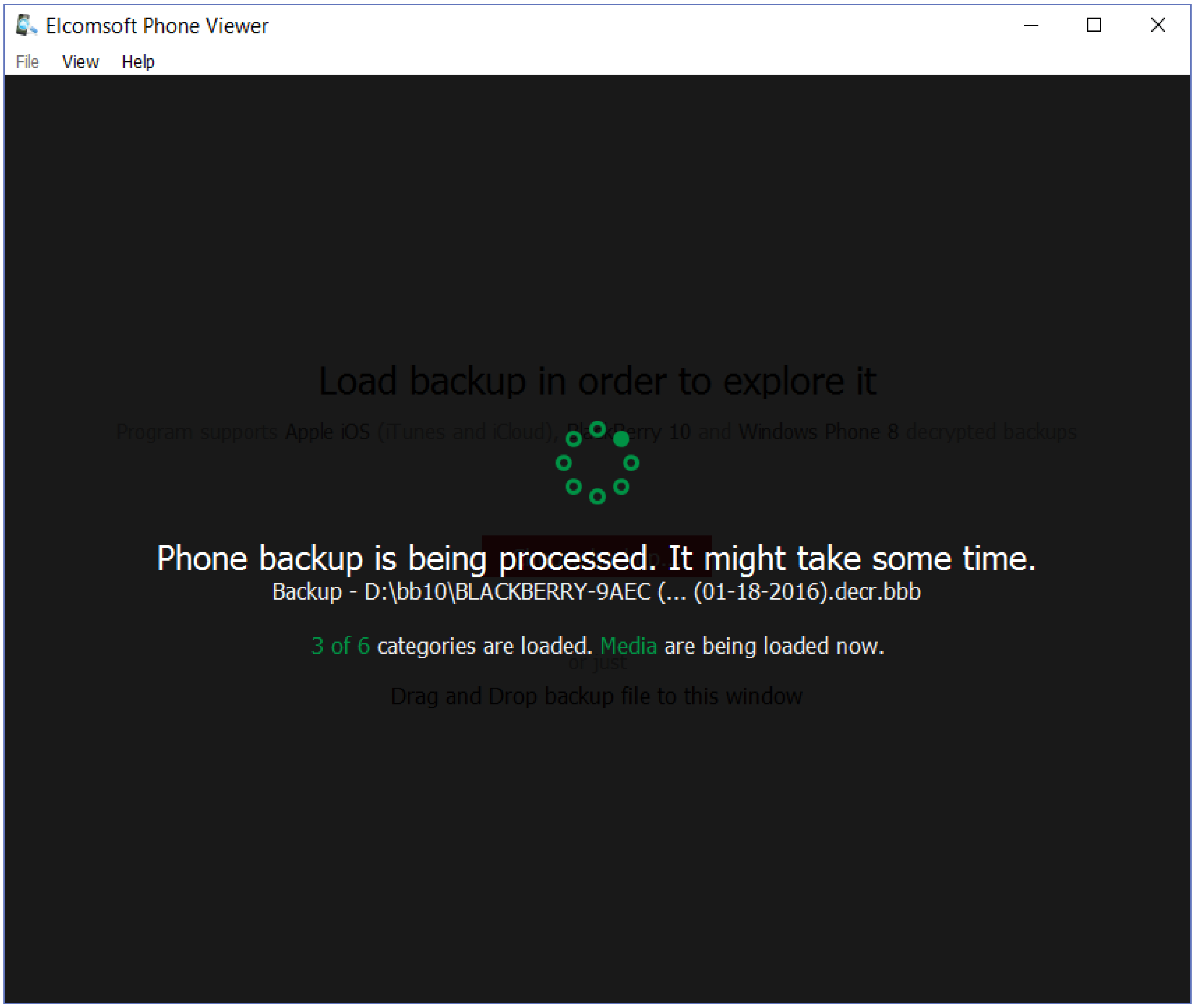
Program supports Apple iOS (iTunes and iCloud), BlackBerry 10 and Windows Phone 8 decrypted backups

or just

Drag and Drop backup file to this window



Device	Device name	Date
Unknown	Oleg's iPad	2015-11-25 17:59:38
iPad Air 2 (5,3)	Oleg's iPad	2016-01-18 19:54:15



Load backup in order to explore it

Program supports Apple iOS (iTunes and iCloud), BlackBerry 10 and Windows Phone 8 decrypted backups

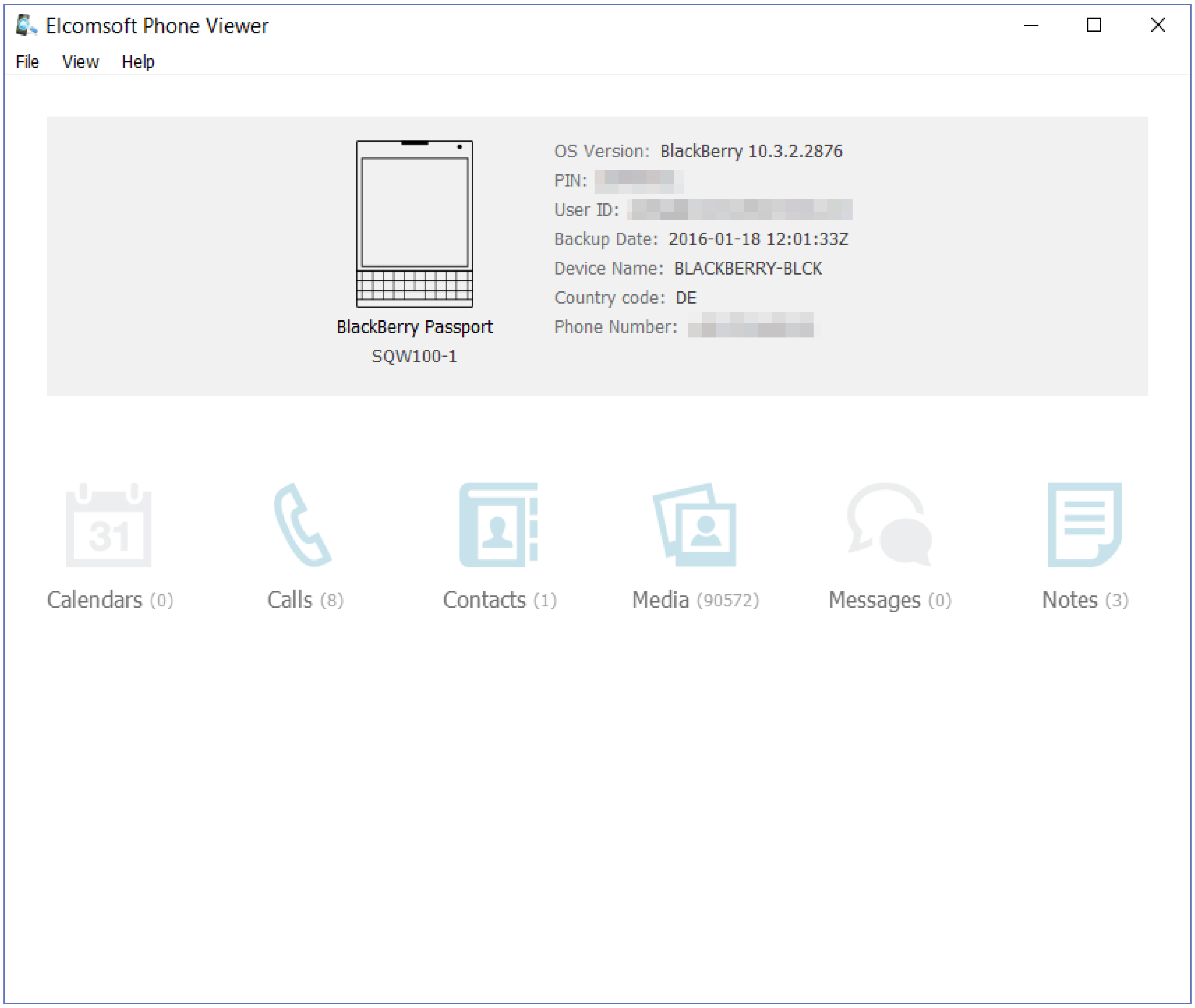
Phone backup is being processed. It might take some time.

Backup - D:\bb10\BLACKBERRY-9AEC (... (01-18-2016).decr.bbb

3 of 6 categories are loaded. Media are being loaded now.

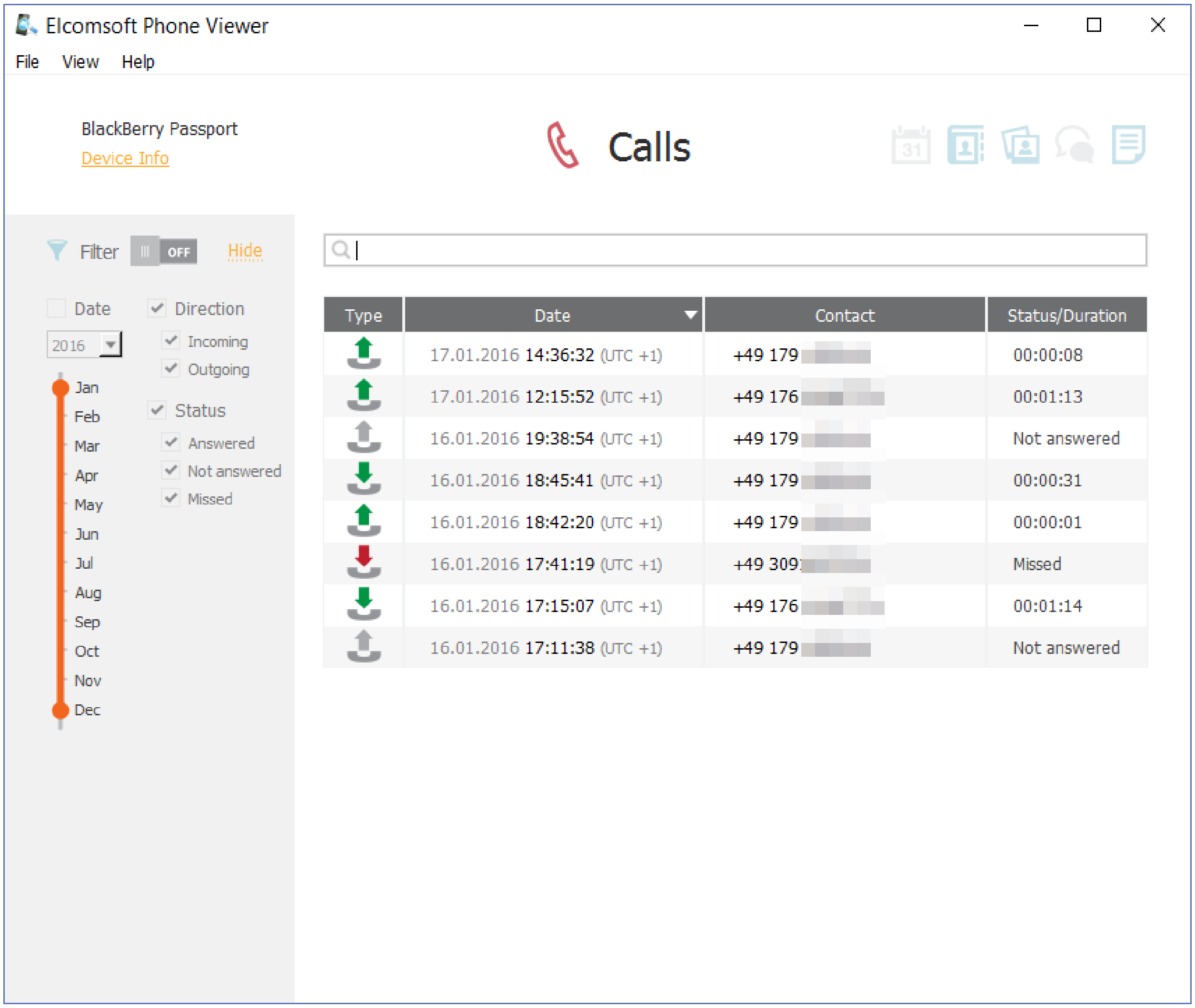
or just

Drag and Drop backup file to this window



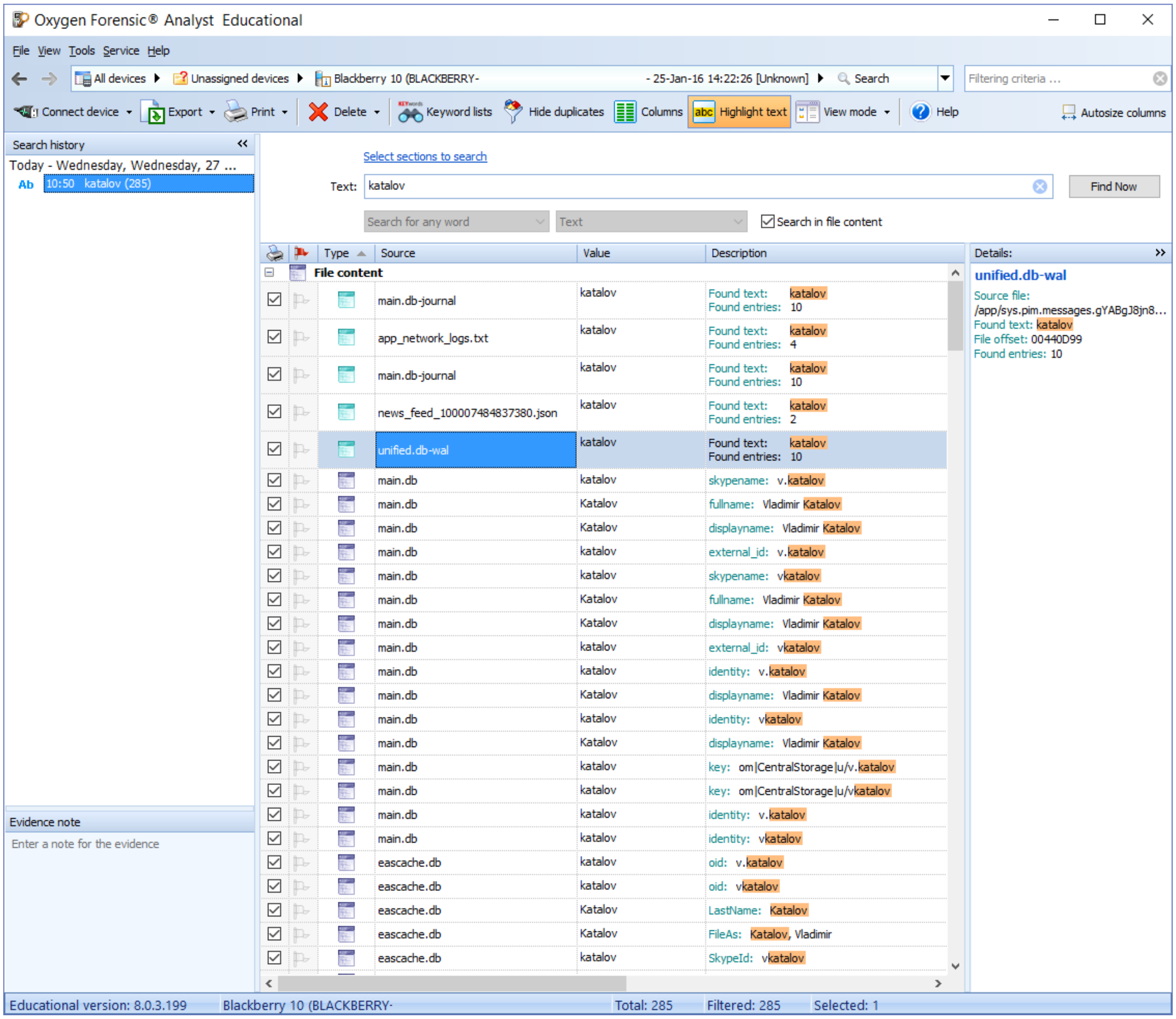
BlackBerry Passport
SQW100-1

OS Version: BlackBerry 10.3.2.2876
PIN: [redacted]
User ID: [redacted]
Backup Date: 2016-01-18 12:01:33Z
Device Name: BLACKBERRY-BLCK
Country code: DE
Phone Number: [redacted]



☑ Direction
☑ Incoming
☑ Outgoing
☑ Status
☑ Answered
☑ Not answered
☑ Missed

Type	Date	Contact	Status/Duration
↑	17.01.2016 14:36:32 (UTC +1)	+49 179 [redacted]	00:00:08
↑	17.01.2016 12:15:52 (UTC +1)	+49 176 [redacted]	00:01:13
↑	16.01.2016 19:38:54 (UTC +1)	+49 179 [redacted]	Not answered
↓	16.01.2016 18:45:41 (UTC +1)	+49 179 [redacted]	00:00:31
↑	16.01.2016 18:42:20 (UTC +1)	+49 179 [redacted]	00:00:01
↓	16.01.2016 17:41:19 (UTC +1)	+49 309 [redacted]	Missed
↓	16.01.2016 17:15:07 (UTC +1)	+49 176 [redacted]	00:01:14
↑	16.01.2016 17:11:38 (UTC +1)	+49 179 [redacted]	Not answered



Today - Wednesday, Wednesday, 27 ...

Ab 10:50 katalov (285)

Text: katalov

☑ Search in file content

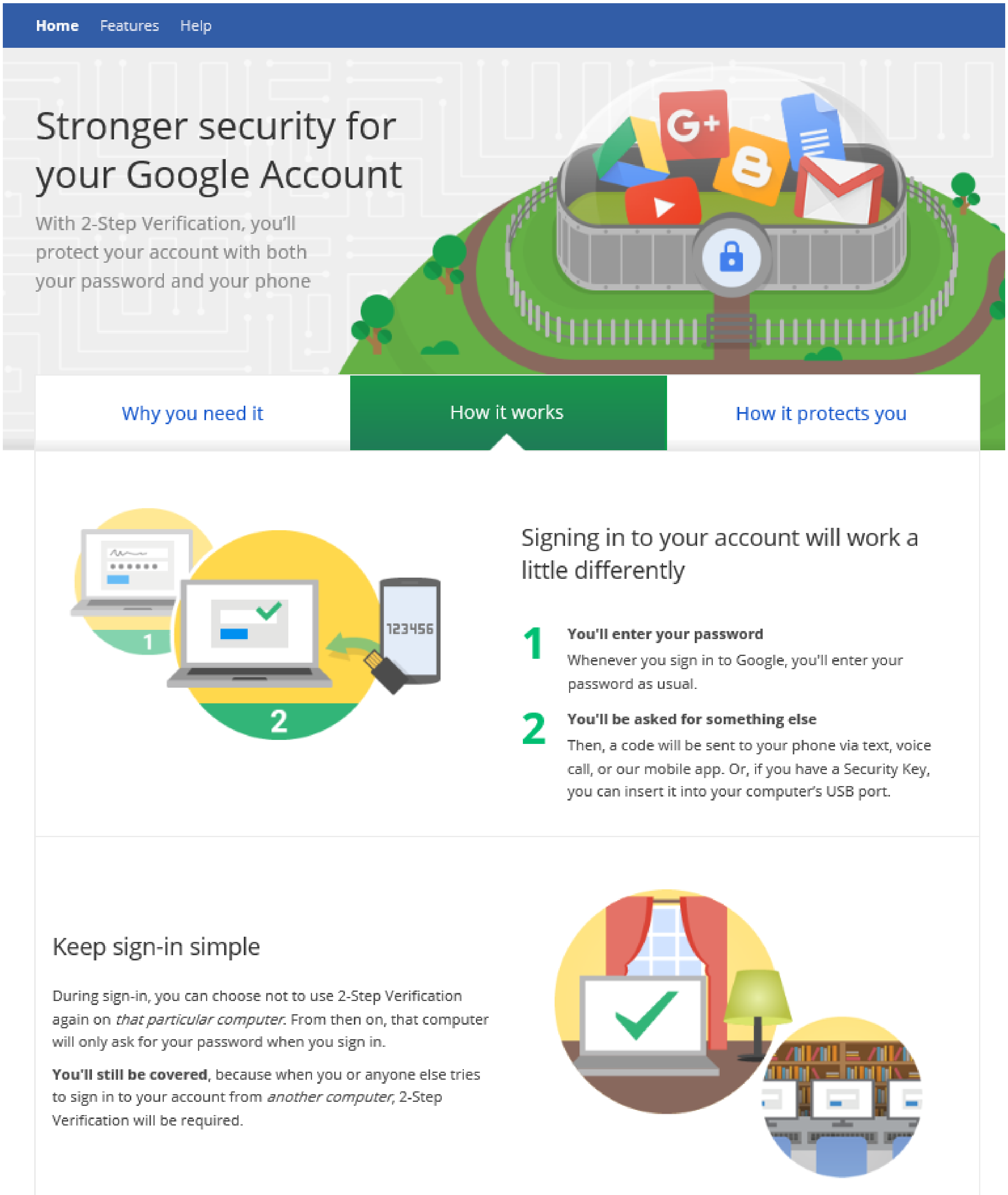
Type	Source	Value	Description
File content			
☑	main.db-journal	katalov	Found text: katalov Found entries: 10
☑	app_network_logs.txt	katalov	Found text: katalov Found entries: 4
☑	main.db-journal	katalov	Found text: katalov Found entries: 10
☑	news_feed_100007484837380.json	katalov	Found text: katalov Found entries: 2
☑	unified.db-wal	katalov	Found text: katalov Found entries: 10
☑	main.db	katalov	skypename: v.katalov
☑	main.db	Katalov	fullname: Vladimir Katalov
☑	main.db	Katalov	displayname: Vladimir Katalov
☑	main.db	katalov	external_id: v.katalov
☑	main.db	katalov	skypename: vkatalov
☑	main.db	Katalov	fullname: Vladimir Katalov
☑	main.db	Katalov	displayname: Vladimir Katalov
☑	main.db	katalov	external_id: vkatalov
☑	main.db	katalov	identity: v.katalov
☑	main.db	Katalov	displayname: Vladimir Katalov
☑	main.db	katalov	identity: vkatalov
☑	main.db	Katalov	displayname: Vladimir Katalov
☑	main.db	katalov	key: om|CentralStorage|u/v.katalov
☑	main.db	katalov	key: om|CentralStorage|u/vkatalov
☑	main.db	katalov	identity: v.katalov
☑	main.db	katalov	identity: vkatalov
☑	eascache.db	katalov	oid: v.katalov
☑	eascache.db	katalov	oid: vkatalov
☑	eascache.db	Katalov	LastName: Katalov
☑	eascache.db	Katalov	FileAs: Katalov, Vladimir
☑	eascache.db	katalov	SkypeId: vkatalov

unified.db-wal

Source file:
/app/sys.pim.messages.gYABgJ8jn8...
Found text: katalov
File offset: 00440D99
Found entries: 10

Educational version: 8.0.3.199 Blackberry 10 (BLACKBERRY- Total: 285 Filtered: 285 Selected: 1

Chapter 10: Dealing with Issues, Obstacles, and Special Cases



Stronger security for your Google Account

With 2-Step Verification, you'll protect your account with both your password and your phone

Signing in to your account will work a little differently

1 **You'll enter your password**

Whenever you sign in to Google, you'll enter your password as usual.

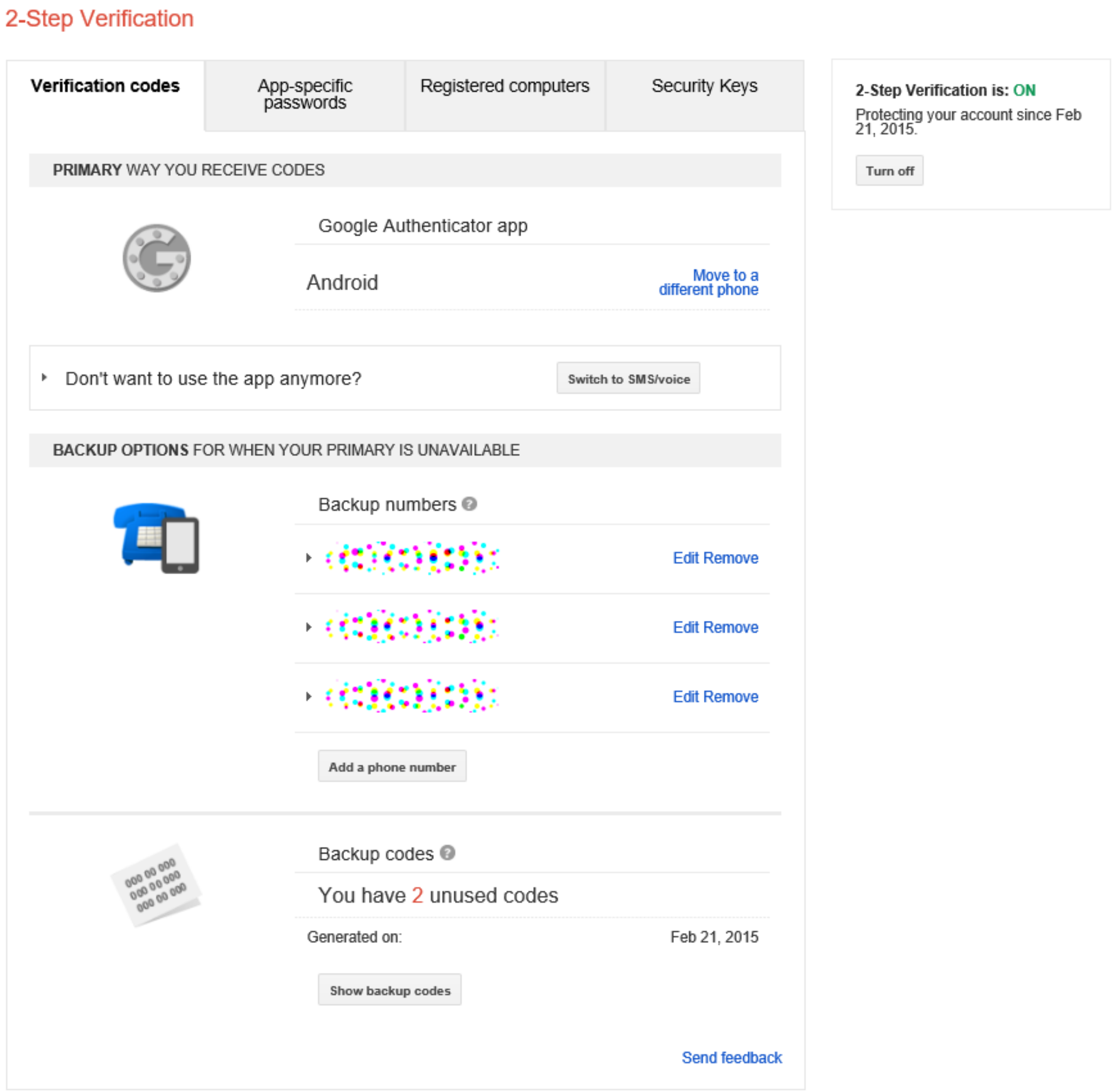
2 **You'll be asked for something else**

Then, a code will be sent to your phone via text, voice call, or our mobile app. Or, if you have a Security Key, you can insert it into your computer's USB port.

Keep sign-in simple

During sign-in, you can choose not to use 2-Step Verification again on *that particular computer*. From then on, that computer will only ask for your password when you sign in.

You'll still be covered, because when you or anyone else tries to sign in to your account from *another computer*, 2-Step Verification will be required.



2-Step Verification

Verification codes | App-specific passwords | Registered computers | Security Keys

PRIMARY WAY YOU RECEIVE CODES

Google Authenticator app

Android — Move to a different phone

Don't want to use the app anymore? [Switch to SMS/voice]

BACKUP OPTIONS FOR WHEN YOUR PRIMARY IS UNAVAILABLE

Backup numbers ?

- [redacted] — Edit Remove
- [redacted] — Edit Remove
- [redacted] — Edit Remove

[Add a phone number]

Backup codes ?

You have 2 unused codes

Generated on: Feb 21, 2015

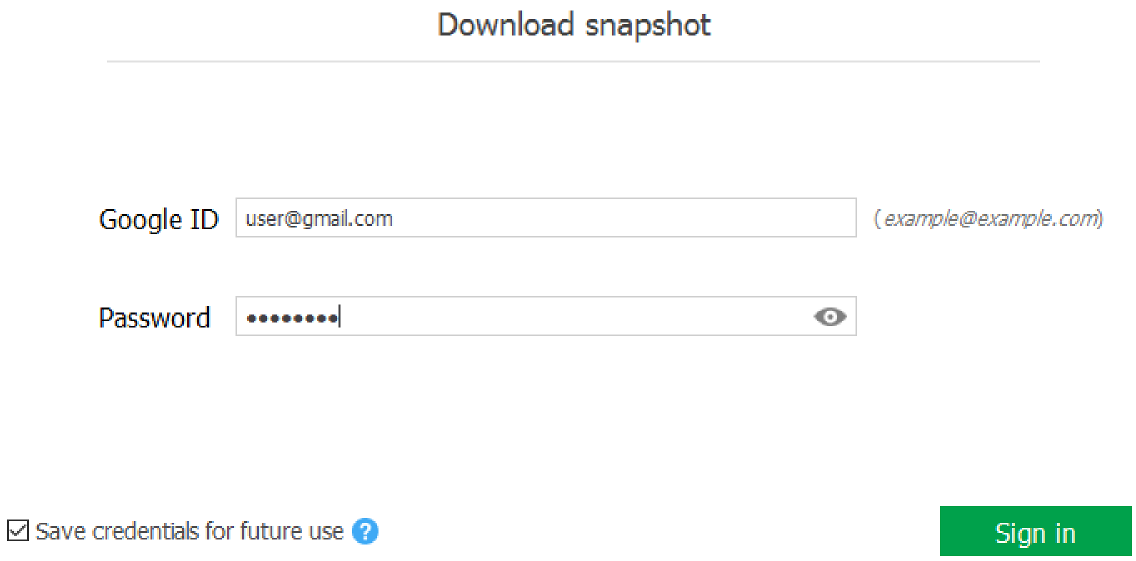
[Show backup codes]

Send feedback

2-Step Verification is: ON

Protecting your account since Feb 21, 2015.

[Turn off]

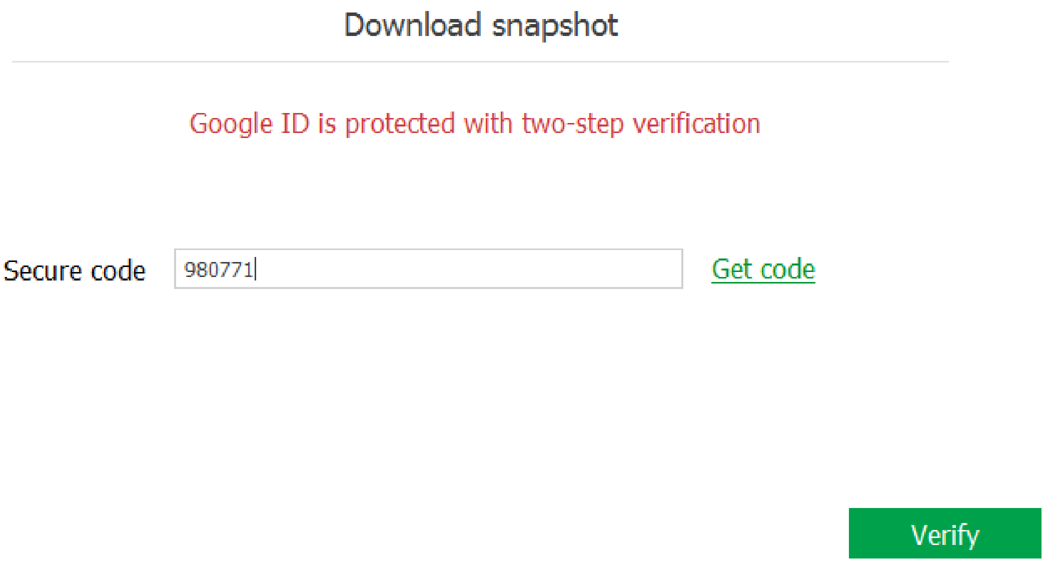


Download snapshot

Google ID: user@gmail.com (*example@example.com*)

Password: ••••••••

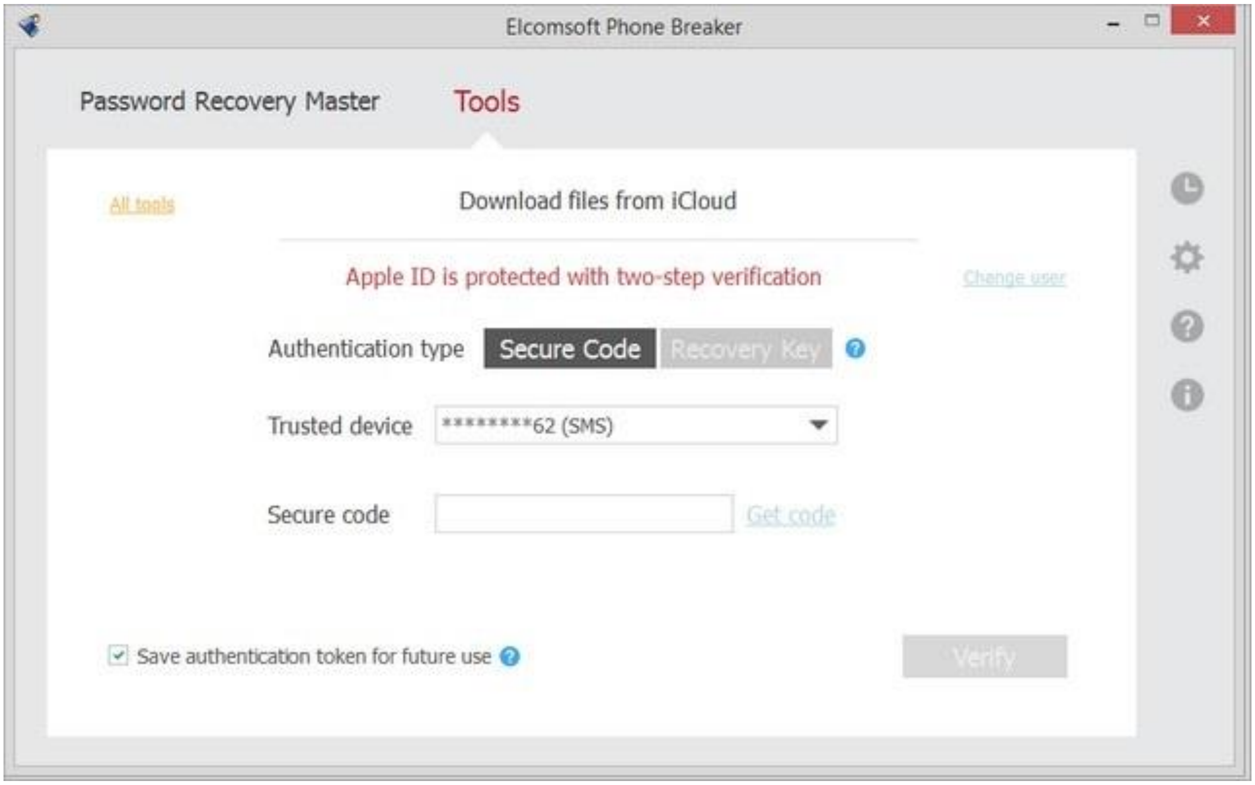
☑ Save credentials for future use



Download snapshot

Google ID is protected with two-step verification

Secure code: 980771



Apple ID is protected with two-step verification

Authentication type: Secure Code

Trusted device: ********62 (SMS)

☑ Save authentication token for future use

Two-step verification

Two-step verification is an advanced security feature that makes it harder for someone to break in to your account with just a stolen password. Learn more about whether this is right for you.

Set up two-step verification

Identity verification apps

You've set up the Microsoft account app and an authenticator app. Learn more about identity verification apps.

Set up identity verification app

Turn off existing apps

Recovery code

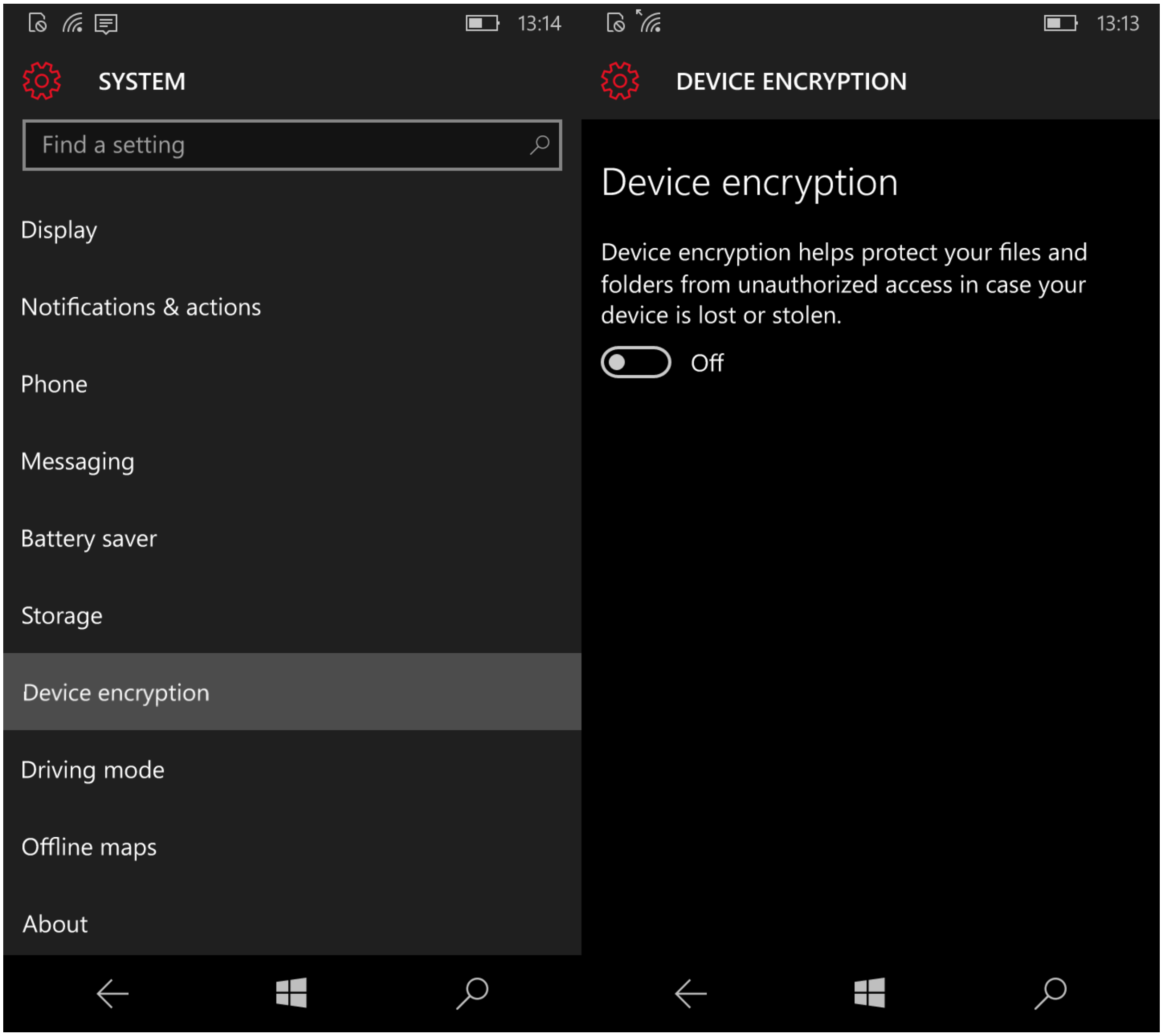
You can use your recovery code if you lose access to your security info. You need to print out your recovery code and keep it in a safe place.

Replace recovery code

Trusted devices

On your trusted devices, you don't have to enter a security code to access sensitive info (such as your credit card details). Learn more about trusted devices.

Remove all the trusted devices associated with my account



Device encryption

Device encryption helps protect your files and folders from unauthorized access in case your device is lost or stolen.

Off