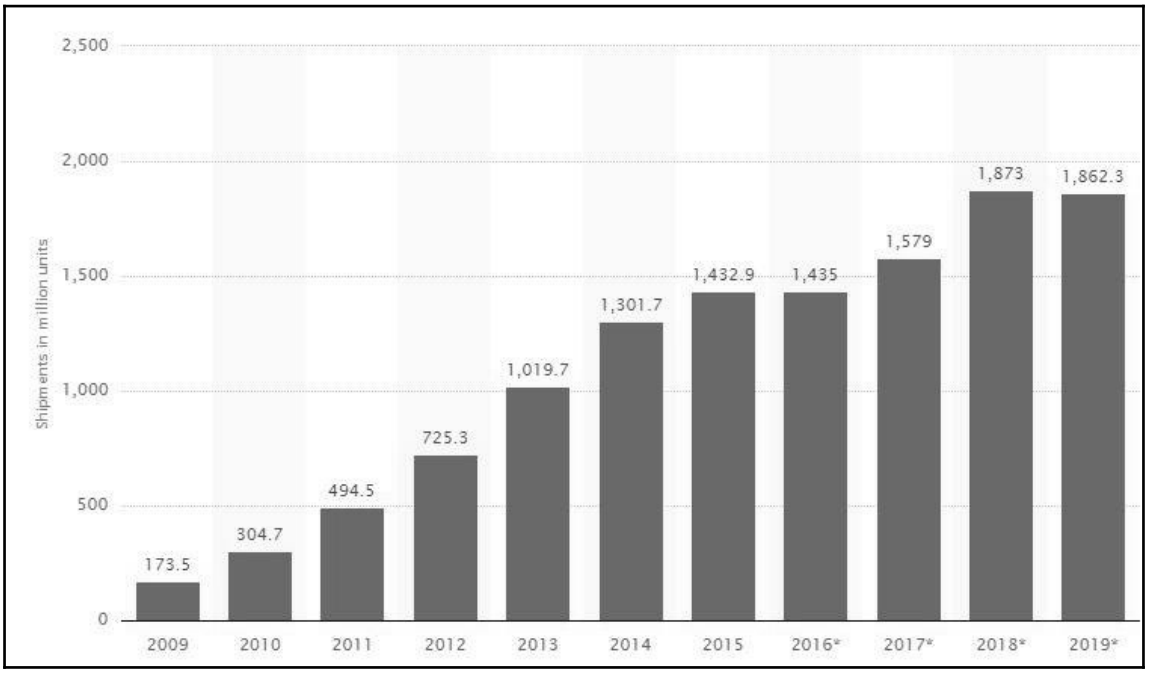
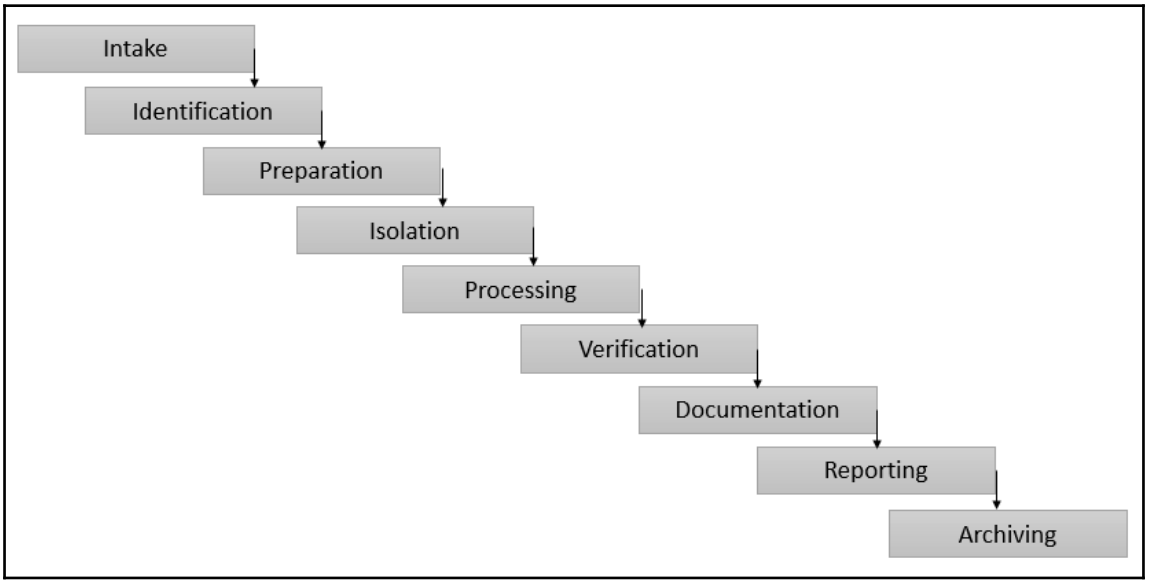
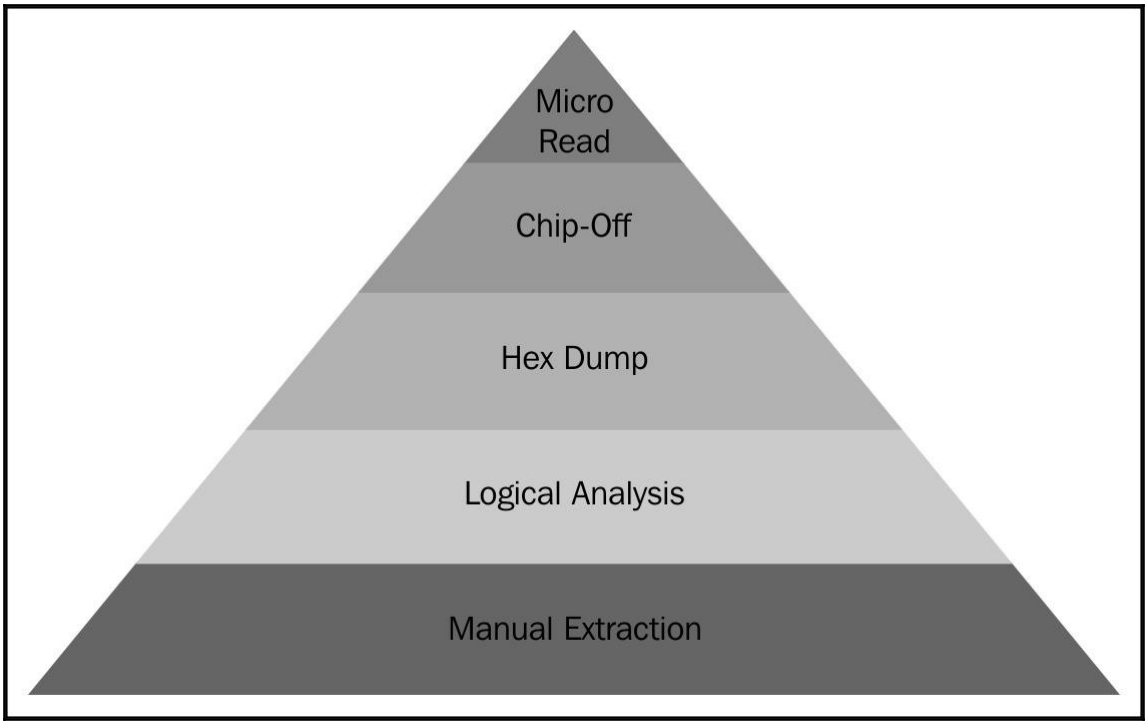
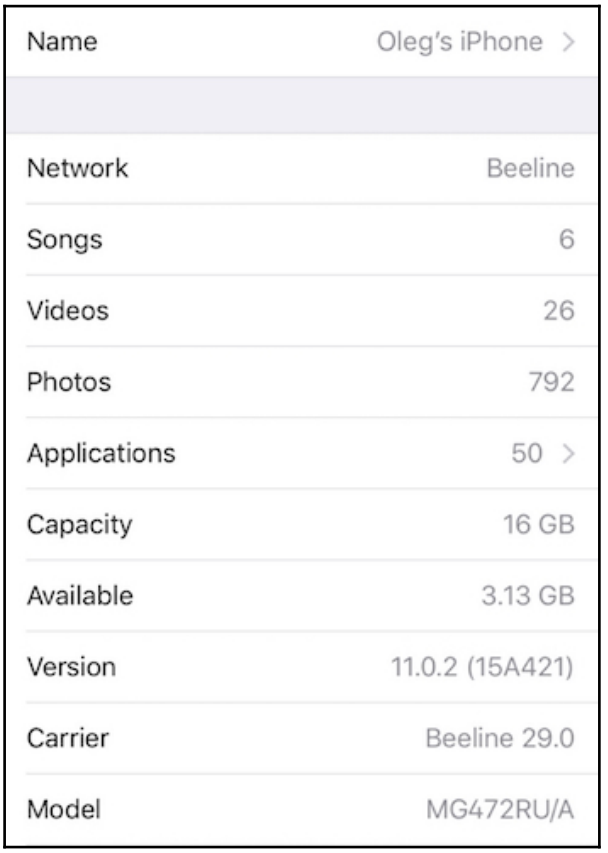
Chapter 1: Introduction to Mobile Forensics






Micro
Read
Chip-Off
Hex Dump
Logical Analysis
Manual Extraction

Chapter 2: Understanding the Internals of iOS Devices



```
olegskulkin — -bash — 80×28
Olegs-MacBook-Air:~ olegskulkin$ ideviceinfo -s
BasebandCertId: 3840149528
BasebandKeyHashInformation:
 AKeyStatus: 2
 SKeyHash: u+/tcCwvaQ+1Y9t40I4yegCEmB28mALlaROhaIVGBWo=
 SKeyStatus: 0
BasebandSerialNumber: COM6Tw==
BasebandVersion: 6.17.00
BoardId: 6
BuildVersion: 15A421
ChipID: 28672
DeviceClass: iPhone
DeviceColor: #3b3b3c
DeviceName: Oleg's iPhone
DieID: 62230050064422
HardwareModel: N61AP
HasSiDP: true
PartitionType: GUID_partition_scheme
ProductName: iPhone OS
ProductType: iPhone7,2
ProductVersion: 11.0.2
ProductionSOC: true
ProtocolVersion: 2
TelephonyCapability: true
UniqueChipID: 62230050064422
UniqueDeviceID: 4fecf6418e3fc6dc6fb787de53f51a557267b3af
WiFiAddress: 64:9a:be:81:73:54
Olegs-MacBook-Air:~ olegskulkin$ ›
```

Oleg's iPhone

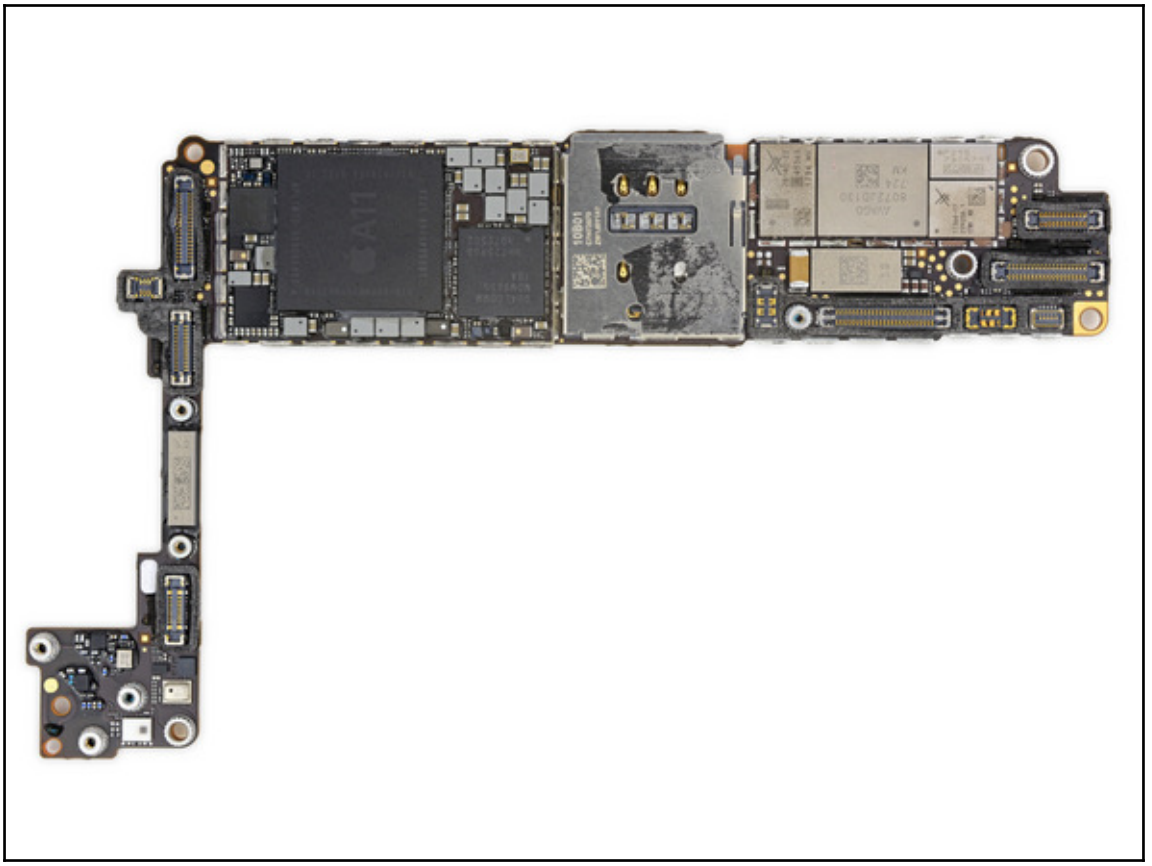
Capacity: 16.0 GB
Software Version: 11.0.3
Firmware Version: iBoot-4076.1.44
Serial Number: C7JNT4PUG5MN
Phone Number:

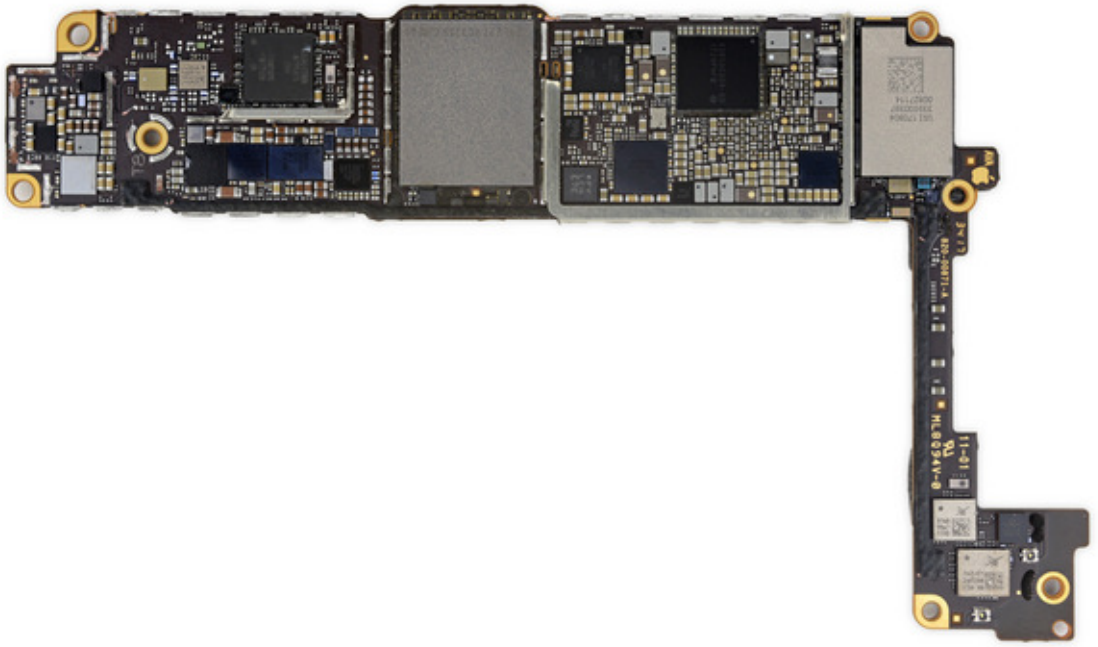
Specification	iPhone	iPhone 3G	iPhone 3GS
System on chip	Samsung Chip	Samsung Chip	Samsung Chip
Onboard RAM	128 MB	128 MB	256 MB
Connectivity	Wi-Fi, Bluetooth 2.0, GSM	Wi-Fi, Bluetooth 2.0, GSM/UMTS/HSDPA, GPS	Wi-Fi, Bluetooth 2.1, GSM, UMTS/HSDPA, GPS
Camera (megapixel)	2	2	3
Front camera	N/A	N/A	N/A
Storage (GB)	4, 8, 16	8, 16	8, 16, 32
Colors	Black	Black, white (white not in 8 GB)	Black, white (white not in 8 GB)
Connector	USB 2.0 dock connector	USB 2.0 dock connector	USB 2.0 dock connector
SIM card form-factor	Mini SIM	Mini SIM	Mini SIM
Siri support	No	No	No

Specification	iPhone 4	iPhone 4S	iPhone 5	iPhone 5C	iPhone 5S
System on chip	Apple A4	Apple A5	Apple A6	Apple A6	Apple A7
Onboard RAM	512 MB	512 MB	1 GB	1 GB	1 GB
Connectivity	Wi-Fi, Bluetooth 2.1, GSM, UMTS/HSDPA/HSUPA, GPS	Wi-Fi, Bluetooth 4, GSM, UMTS/HSDPA/HSUPA, GPS	Wi-Fi, Bluetooth 4, UMTS/HSDPA+/DC-HSDPA, GSM, GPS	Wi-Fi, Bluetooth 4, UMTS/HSDPA+/DC-HSDPA/LTE, GSM, GPS	Wi-Fi, Bluetooth 4, UMTS/HSDPA+/DC-HSDPA/LTE/TD-LTE, GSM, GPS
Camera (megapixel)	5	8	8	8	8
Storage (GB)	8, 16, 32	8, 16, 32, 64	16, 32, 64	8, 16, 32, 64	8, 16, 32, 64
Colors	Black	Black, white	Black, white	White, pink, yellow, blue, or green	Silver, space gray, or gold
Connector	USB 2.0 dock connector	USB 2.0 dock connector	Lightning connector	Lightning connector	Lightning connector
SIM card form factor	Micro SIM	Micro SIM	Nano-SIM	Nano-SIM	Nano-SIM
Siri support	No	Yes	Yes	Yes	Yes

Specification	iPhone 6	iPhone 6 Plus	iPhone 6S	iPhone 6S Plus
System on chip	Apple A8	Apple A8	Apple A9	Apple A9
CPU	1.4 GHz	1.4 GHz	1.8 GHz	1.8 GHz
Onboard RAM	1 GB	1 GB	2 GB	
Screen size (in inches)	4.7	5.5	4.7	5.5
Connectivity	Wi-Fi, Bluetooth 4.2, UMTS/HSDPA+/DC-HSDPA/LTE, CDMA, GSM, GPS	Wi-Fi, Bluetooth 4.2, UMTS/HSDPA+/DC-HSDPA/LTE, CDMA, GSM, GPS	Wi-Fi, Bluetooth 4.2, UMTS/HSDPA+/DC-HSDPA/LTE, CDMA, GSM, GPS	Wi-Fi, Bluetooth 4.2, UMTS/HSDPA+/DC-HSDPA/LTE, CDMA, GSM, GPS
Camera (megapixel)	8	8	12	12
Storage (GB)	16, 64, 128	16, 64, 128	16, 64, 128	16, 64, 128
Colors	Silver, Gold, Space Gray	Silver, Gold, Space Gray	Silver, Rose Gold, Gold, Space Gray	Silver, Rose Gold, Gold, Space Gray
Connector	Lightning connector	Lightning connector	Lightning connector	Lightning connector
SIM card form-factor	Nano-SIM	Nano-SIM	Nano-SIM	Nano-SIM
Siri support	Yes	Yes	Yes	Yes

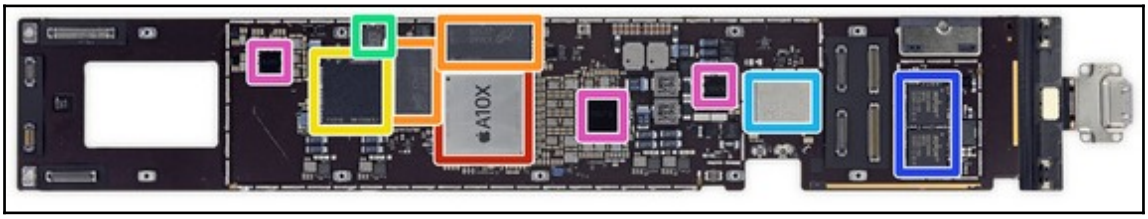
Specification	iPhone SE	iPhone 7	iPhone 7 Plus	iPhone 8	iPhone 8 Plus	iPhone X
System on chip	Apple A9	Apple A10	Apple A10	Apple A11	Apple A11	Apple A11
CPU	1.85 GHz	2.33 GHz	2.33 GHz	2.39 GHz	2.39 GHz	2.39 GHz
Onboard RAM	2 GB	2 GB	3 GB	2 GB	3 GB	3 GB
Connectivity	Wi-Fi: 802.11a/b/g/n/ac	Wi-Fi: 802.11a/b/g/n/ac with MIMO	Wi-Fi: 802.11a/b/g/n/ac with MIMO	Wi-Fi: 802.11a/b/g/n/ac with MIMO	Wi-Fi: 802.11a/b/g/n/ac with MIMO	Wi-Fi: 802.11ac with MIMO
Camera (megapixel)	12	12	12	12	12	12
Storage (GB)	16, 32, 64 & 128	32, 128 & 256	32, 128 & 256	64 & 256	64 & 256	64 & 256
Colors	Silver, Space Gray, Gold, Rose Gold	Black, Silver, Gold, Rose Gold, Jet Black, Red	Black, Silver, Gold, Rose Gold, Jet Black, Red	Silver, Space Gray, Gold	Silver, Space Gray, Gold	Silver, Space Gray
Connector	Lightning connector	Lightning connector	Lightning connector	Lightning connector	Lightning connector	Lightning connector
SIM card form-factor	Nano-SIM	Nano-SIM	Nano-SIM	Nano-SIM	Nano-SIM	Nano-SIM
Siri support	Yes	Yes	Yes	Yes	Yes	Yes

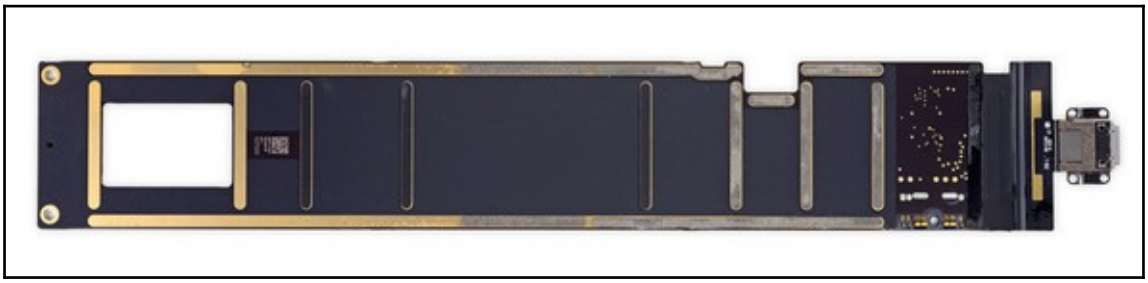




Device	Model	Initial OS	Identifier	Release date
iPad Pro 9.7-inch	A1673 A1674 A1675	9.3	iPad6,3 iPad6,4	March 31, 2016
iPad Pro 12.9-inch (2nd generation)	A1670 A1671	10.3.2	iPad7,1 iPad7,2	June 13, 2017
iPad Pro 10.5-inch	A1701 A1709	10.3.2	iPad7,3 iPad7,4	June 13, 2017

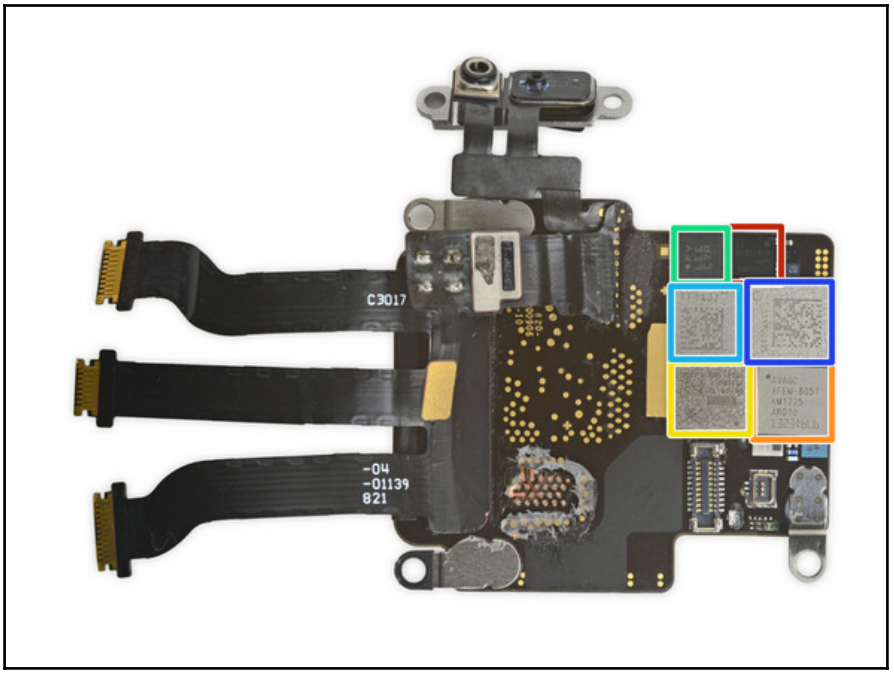
Specification	iPad Pro 9.7-inch	iPad Pro 12.9-inch (2nd generation)	iPhone 7 Plus
System on chip	Apple A9X	Apple A10X	Apple A10X
CPU	2.16 GHz	2.39 GHz	2.39 GHz
Onboard RAM	2 GB	4 GB	4 GB
Camera (megapixel)	12	12	12
Storage (GB)	32, 128 & 256	64, 256 & 512	64, 256 & 512
Colors	Silver, Space Gray, Gold, Rose Gold	Silver, Space Gray, Gold	Silver, Space Gray, Gold, Rose Gold
Connector	Lightning connector	Lightning connector	Lightning connector
Siri support	Yes	Yes	Yes

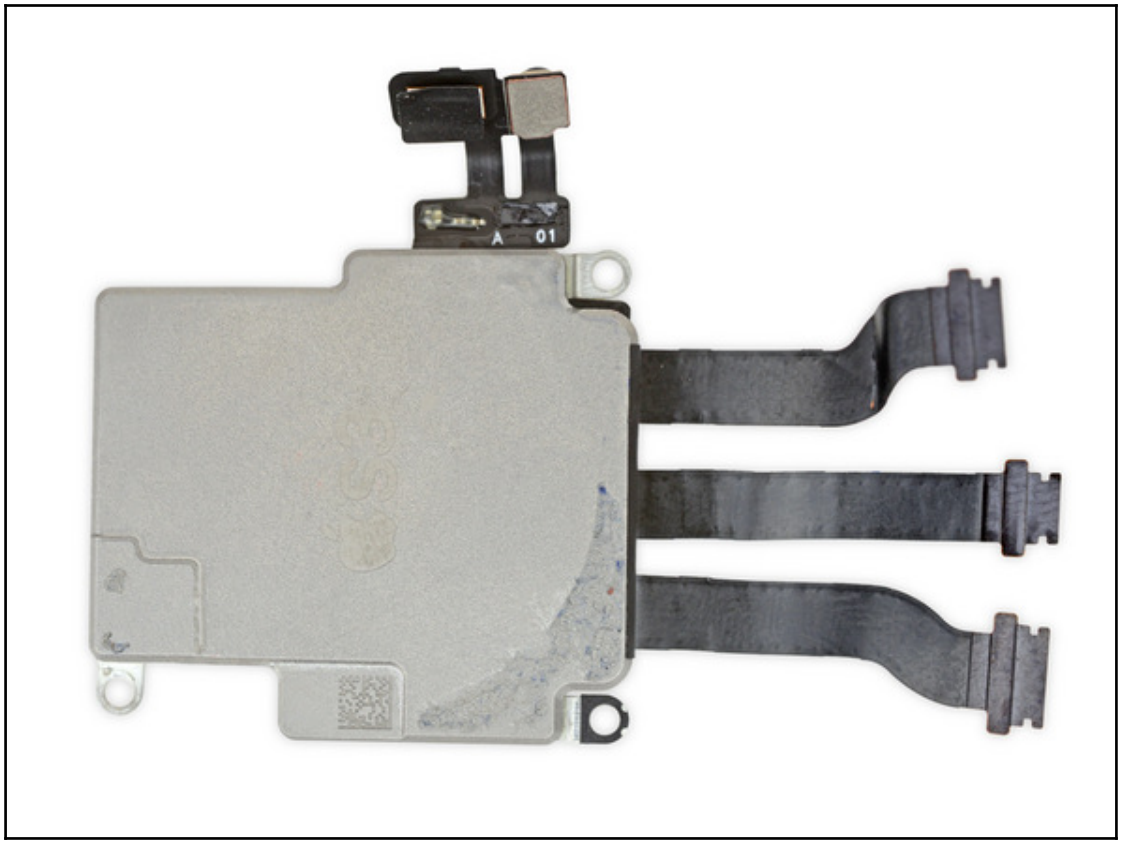


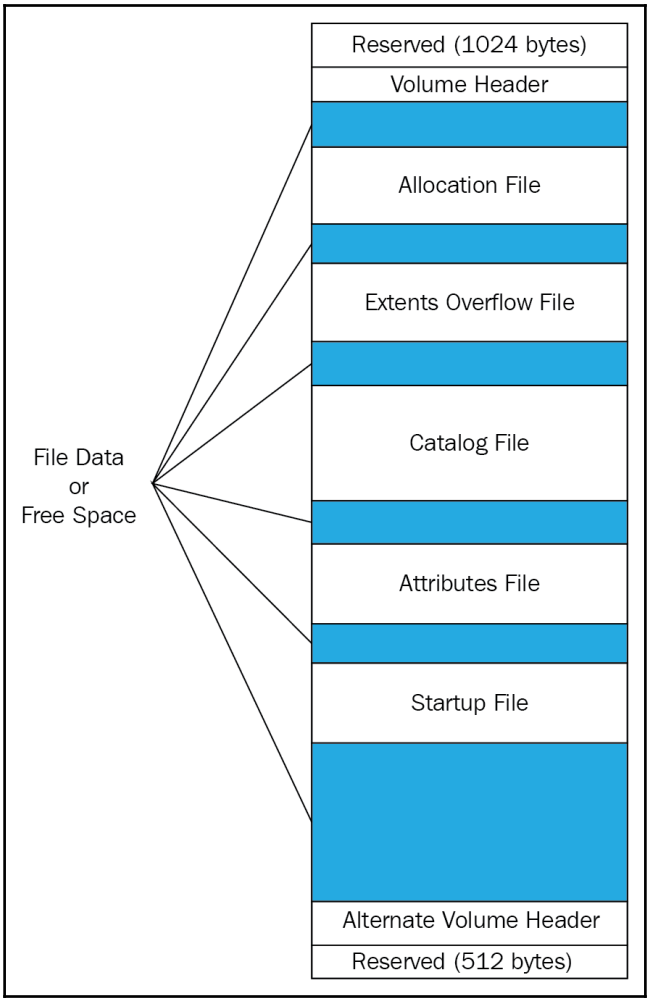


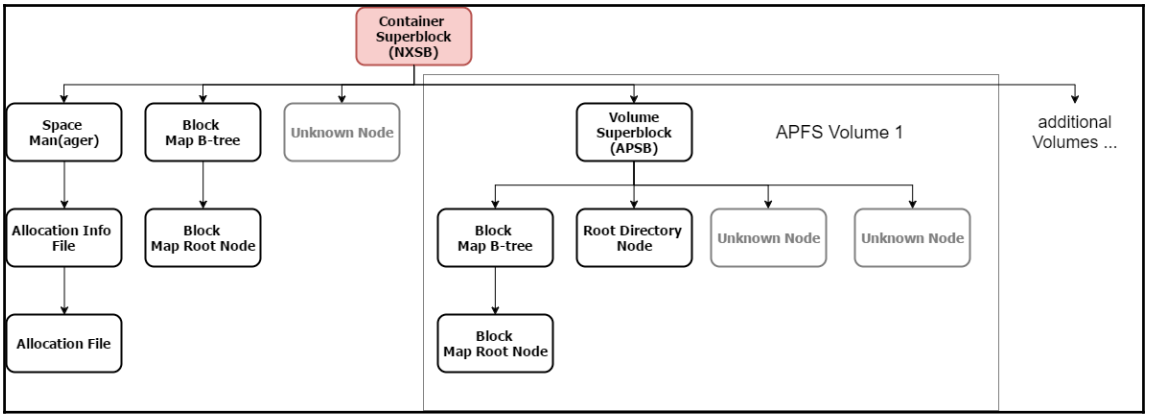
Device	Initial OS	Identifier	Release date
Apple Watch (1st generation)	watchOS 1.0	Watch1,1 Watch1,2	April 24, 2015
Apple Watch (Series 1)	watchOS 3.0	Watch2,6, Watch2,7	September 16, 2016
Apple Watch (Series 2)	watchOS 3.0	Watch2,3, Watch2,4	September 16, 2016
Apple Watch (Series 3)	watchOS 4.0	Watch3,1, Watch3,2, Watch3,3, Watch3,4	September 22, 2017 October 5, 2017 September 22, 2017

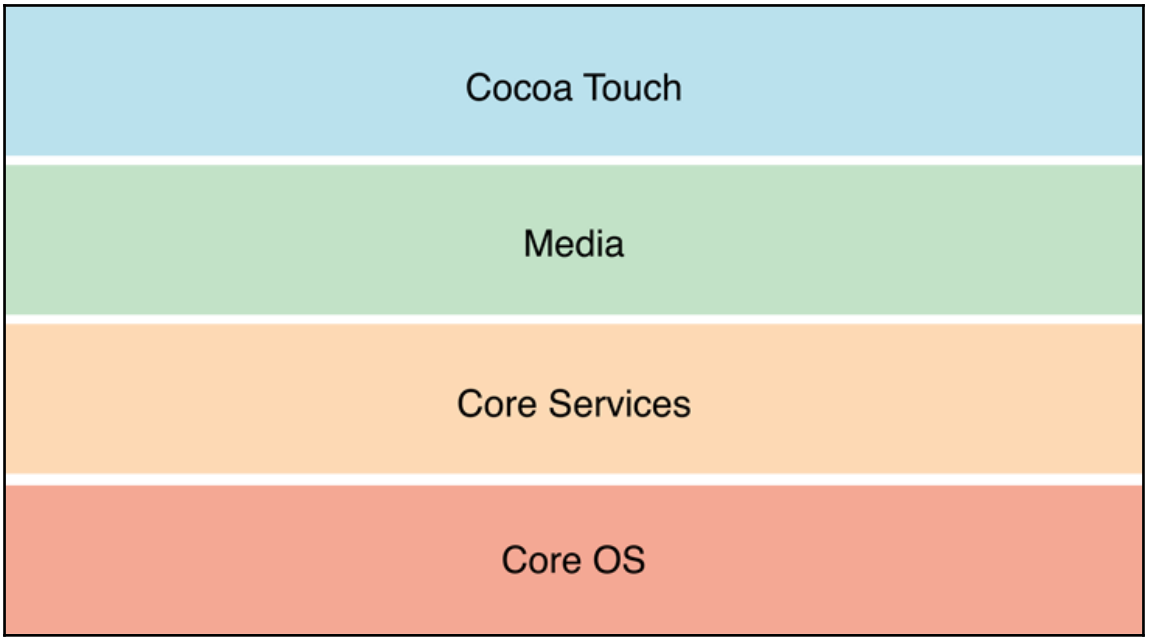
Specification	Apple Watch (1st generation)	Apple Watch (Series 1)	Apple Watch (Series 2)	Apple Watch (Series 3)
System on chip	Apple S1	Apple S1P	Apple S2	Apple S3
Onboard RAM	512 MB	Unknown	Unknown	Unknown
Storage (GB)	8	8	Unknown	16

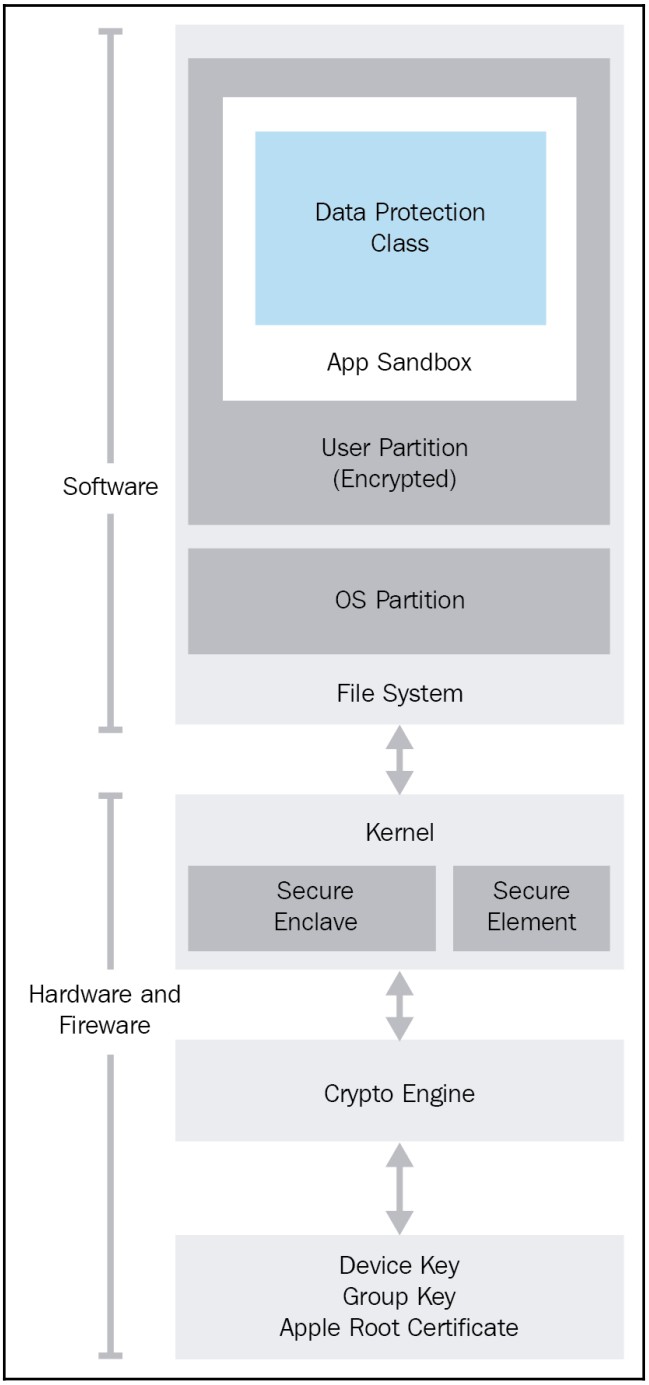

C3017
-04
-01139
821


A 01


Reserved (1024 bytes)
Volume Header
Allocation File
Extents Overflow File
Catalog File
Attributes File
Startup File
Alternate Volume Header
Reserved (512 bytes)
File Data
or
Free Space

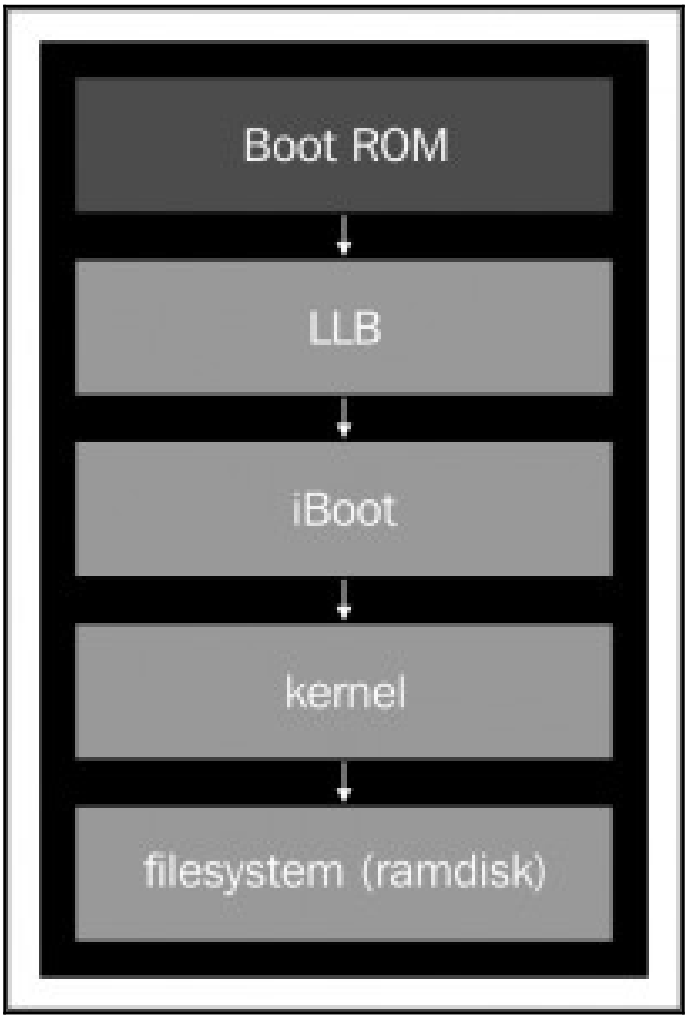

Container Superblock (NXSB)
Space Man(ager)
Block Map B-tree
Unknown Node
Volume Superblock (APSB)
APFS Volume 1
additional Volumes ...
Allocation Info File
Block Map Root Node
Block Map B-tree
Root Directory Node
Unknown Node
Unknown Node
Allocation File
Block Map Root Node

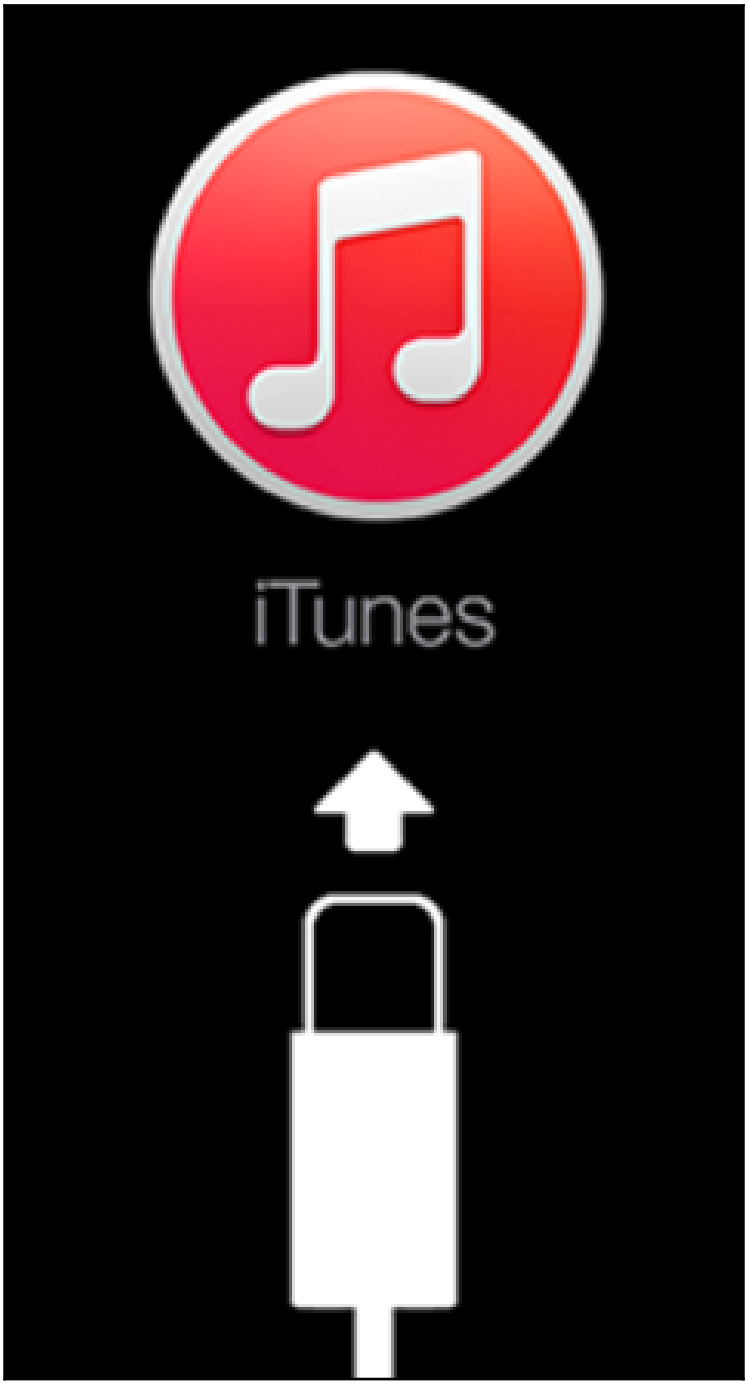

Cocoa Touch
Media
Core Services
Core OS

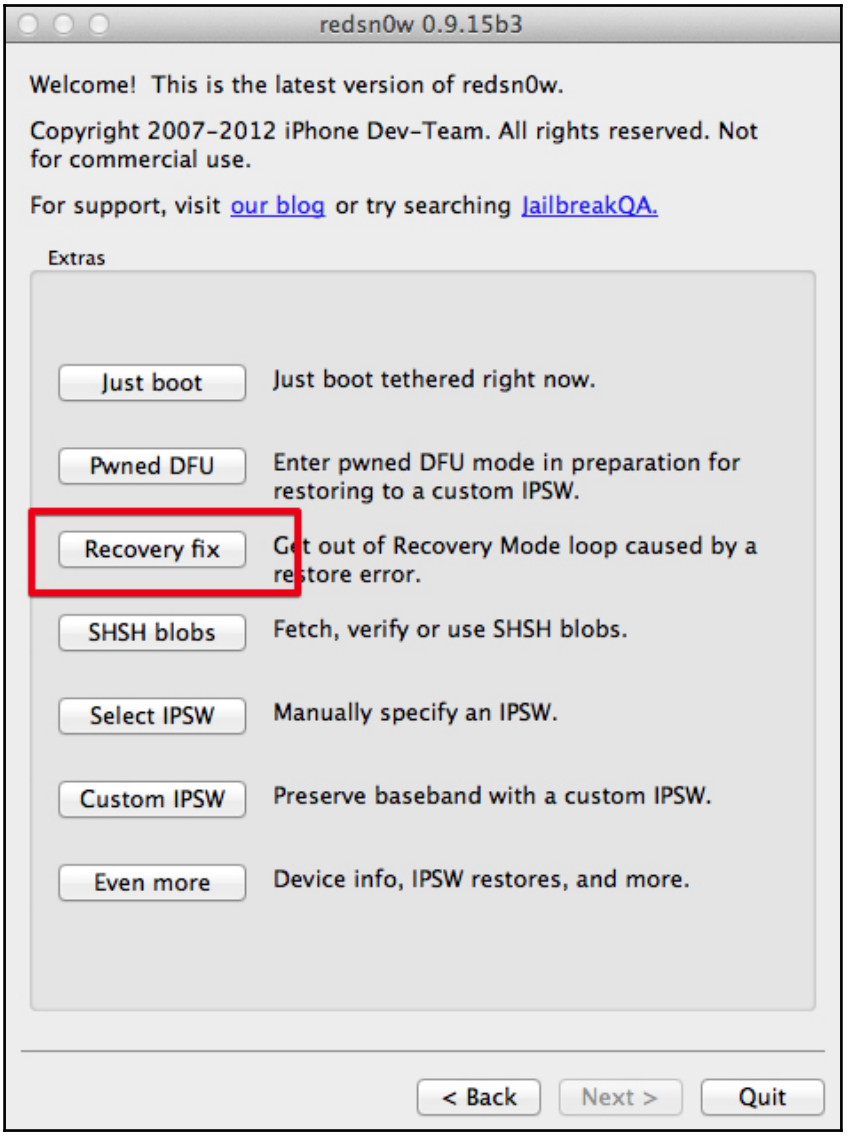

Data Protection Class
App Sandbox
User Partition (Encrypted)
OS Partition
File System
Software
Kernel
Secure Enclave
Secure Element
Hardware and Fireware
Crypto Engine
Device Key
Group Key
Apple Root Certificate

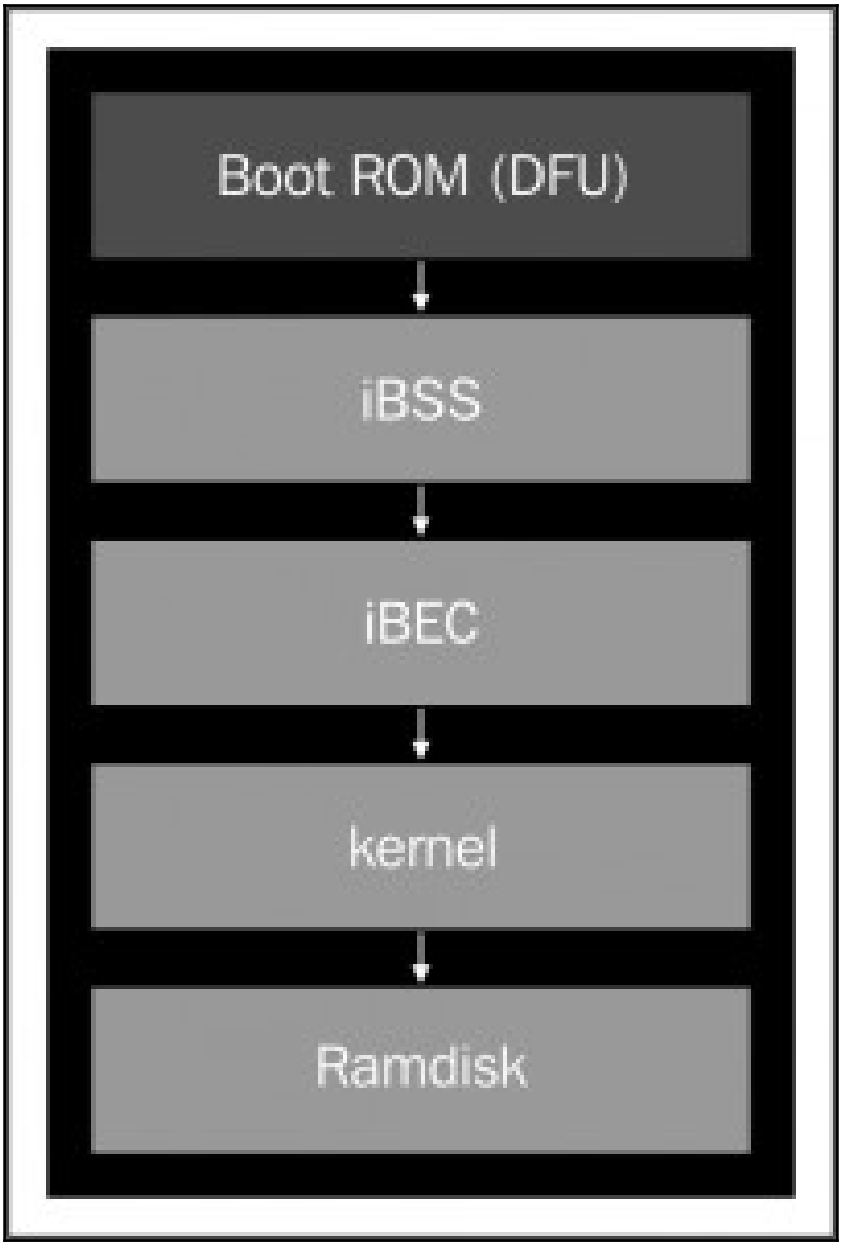
Name	Release date	Hardware			Firmware
		iPad	iPhone	iPod Touch	
JailbreakMe 3.0	July 5, 2011	1, 2	3GS, 4	1	4.2.6 – 4.2.8, 4.3 – 4.3.3
redsn0w 0.9.15 beta 3	November 1, 2012	1	3GS, 4	1	4.1 – 6.1.6
Absinthe 2.0.4	May 30, 2012	1, 2, 3	3GS, 4, 4S	1	5.1.1
evasi0n	February 4, 2013	2, 3, 4, Mini 1	3GS, 4, 4S, 5	4, 5	6.0 – 6.1.2
evasi0n7	December 22, 2013	2, 3, 4, Air, Mini 1, Mini 2	4, 4S, 5, 5S, 5C	5	7.0 – 7.0.6
p0sixspwn	December 30, 2013	2, 3, 4, Mini 1	3GS, 4, 4S, 5	4, 5	6.1.3 – 6.1.6
Pangu	June 23, 2014	2, 3, 4, Air, Mini 1, Mini 2	4, 4S, 5, 5C, 5S	5	7.1 – 7.1.2
Pangu8	October 22, 2014	2, 3, 4, Air, Air 2, Mini 1, Mini 2, Mini 3	4S, 5, 5C, 5S, 6, 6 Plus	5	8.0 – 8.1
TaiG	November 29, 2014	2, 3, 4, Air, Air 2, Mini 1, Mini 2, Mini 3	4S, 5, 5C, 5S, 6, 6 Plus	5, 6	8.0 – 8.4
PPJailbreak	January 18, 2015	2, 3, 4, Air, Air 2, Mini 1, Mini 2, Mini 3	4S, 5, 5C, 5S, 6, 6 Plus	5, 6	8.0 – 8.4
Pangu9	October 14, 2015	2, 3, 4, Air, Air 2, Mini 1, Mini 2, Mini 3, Mini 4, Pro	4S, 5, 5C, 5S, 6, 6 Plus, 6S, 6S Plus	5, 6	9.0 – 9.1
PPJailbreak	July 24, 2016	Air, Air 2, Mini 2, Mini 3, Mini 4, Pro	5S, 6, 6 Plus, 6S, 6S Plus, SE	6	9.2 – 9.3.3
mach_portal + Yalu	December 22, 2016	Pro	6S, 6S Plus, 7, 7 Plus		10.0.1-10.1.1 (depends on device)
yalu102	January 26, 2017	Air 2, Mini 2, Mini 3, Pro	5S, 6, 6 Plus, 6S, 6S Plus, SE	6	10.0.1 - 10.2
Phoenix	August 6, 2017	2, 3, 4, Mini	4S, 5, 5C	5	9.3.5
Saigon	October 15, 2017	IPad Air 2, Mini 4	SE, 6S Plus, 6 Plus, 6S	6	10.2.1

Chapter 3: Data Acquisition from iOS Devices




iTunes


redsn0w 0.9.15b3
Welcome! This is the latest version of redsn0w.
Copyright 2007-2012 iPhone Dev-Team. All rights reserved. Not for commercial use.
For support, visit our blog or try searching JailbreakQA.
Extras
Just boot
Just boot tethered right now.
Pwned DFU
Enter pwned DFU mode in preparation for restoring to a custom IPSW.
Recovery fix
Get out of Recovery Mode loop caused by a restore error.
SHSH blobs
Fetch, verify or use SHSH blobs.
Select IPSW
Manually specify an IPSW.
Custom IPSW
Preserve baseband with a custom IPSW.
Even more
Device info, IPSW restores, and more.
< Back
Next >
Quit


Boot ROM (DFU)
iBSS
iBEC
kernel
Ramdisk

Prepare the device for physical extraction

Connect > Prepare > Extract data

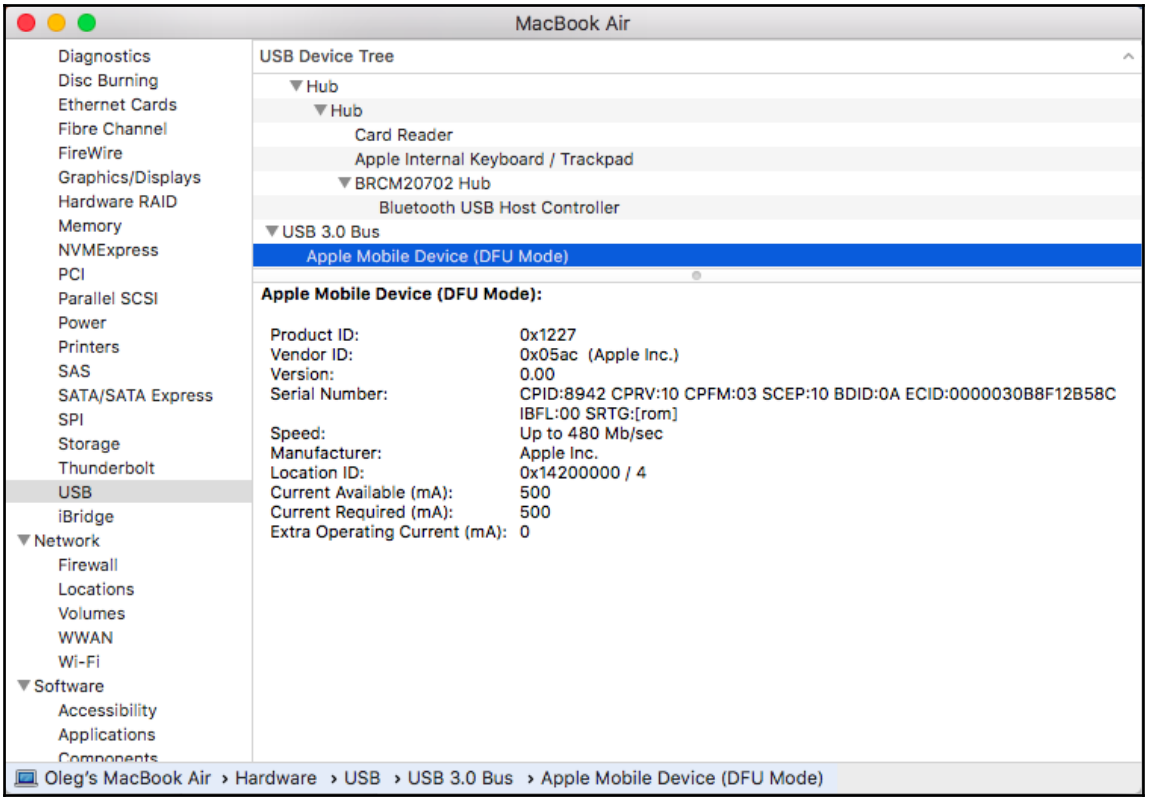
The device needs to be in DFU mode (Device Firmware Update) to enable data extraction.

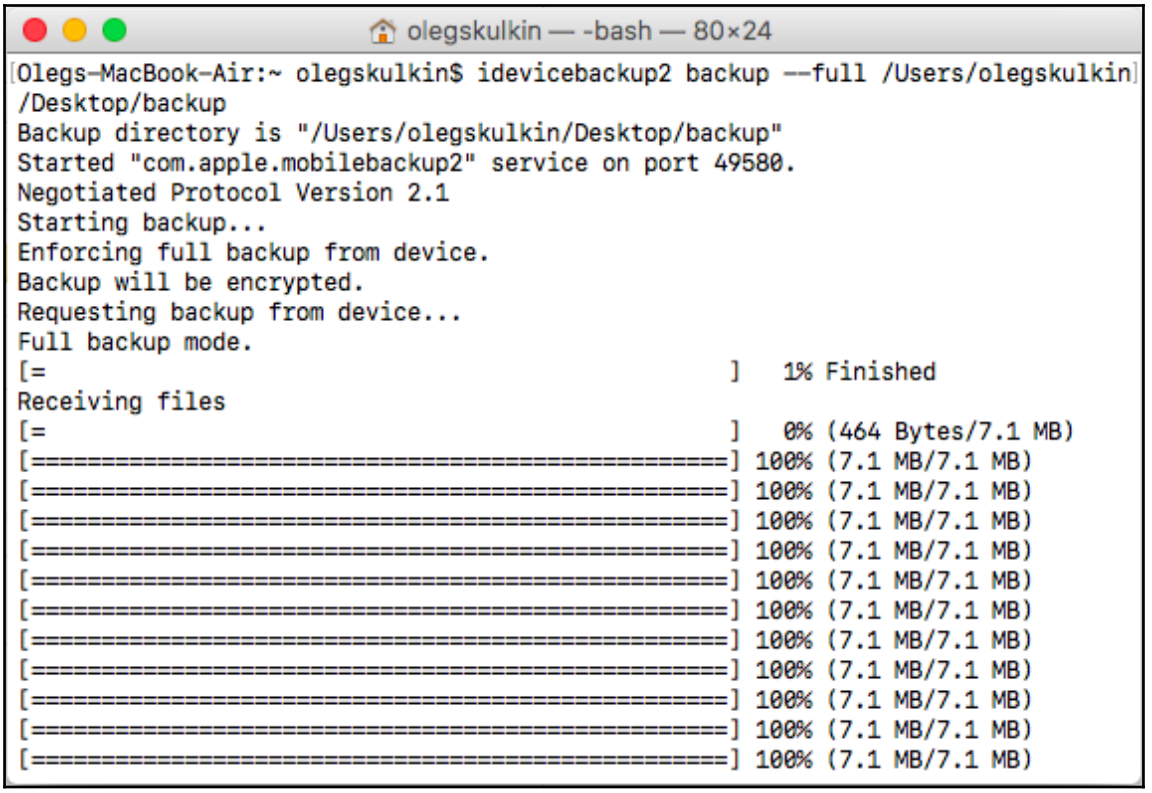
Press and hold both the Power and Home buttons.

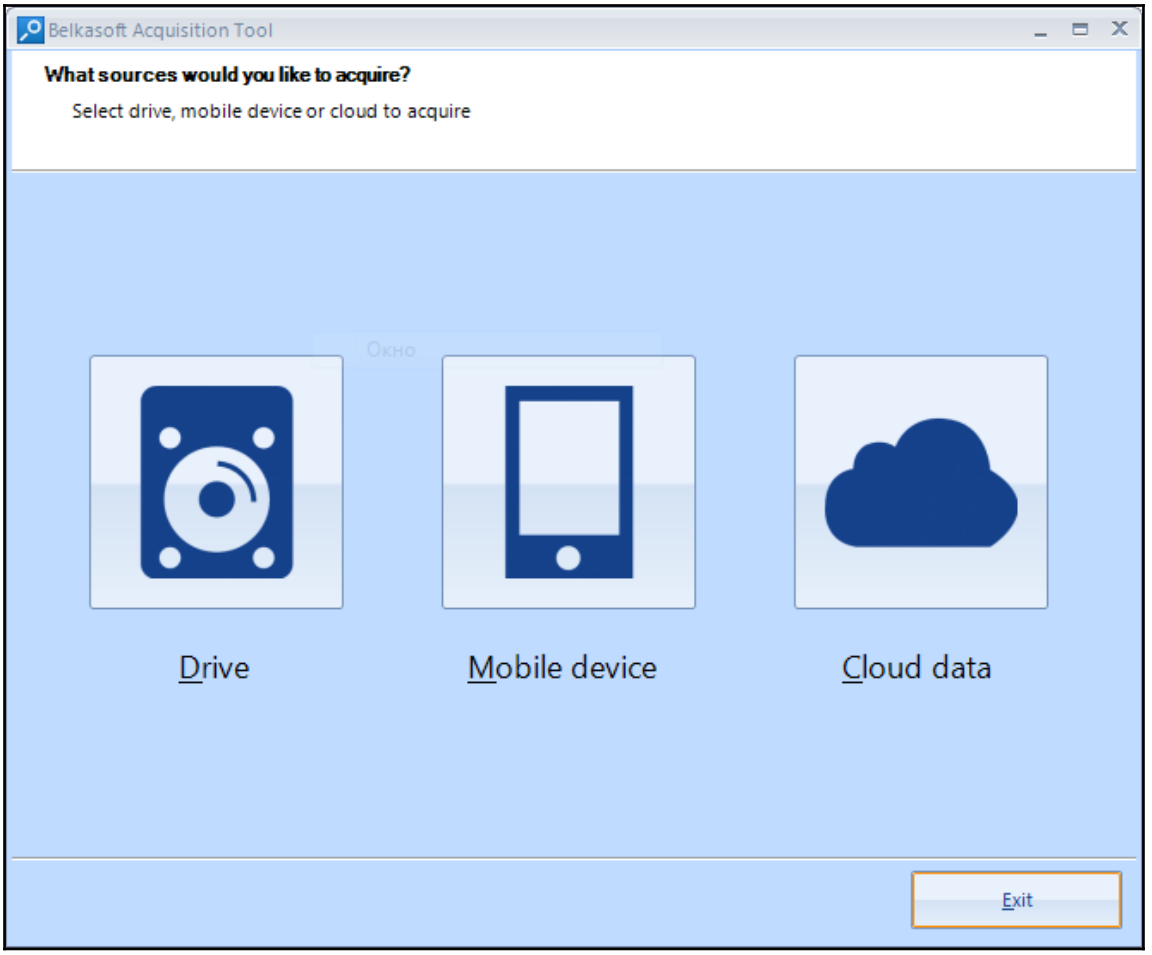
When the device screen turns black, wait 3 seconds.

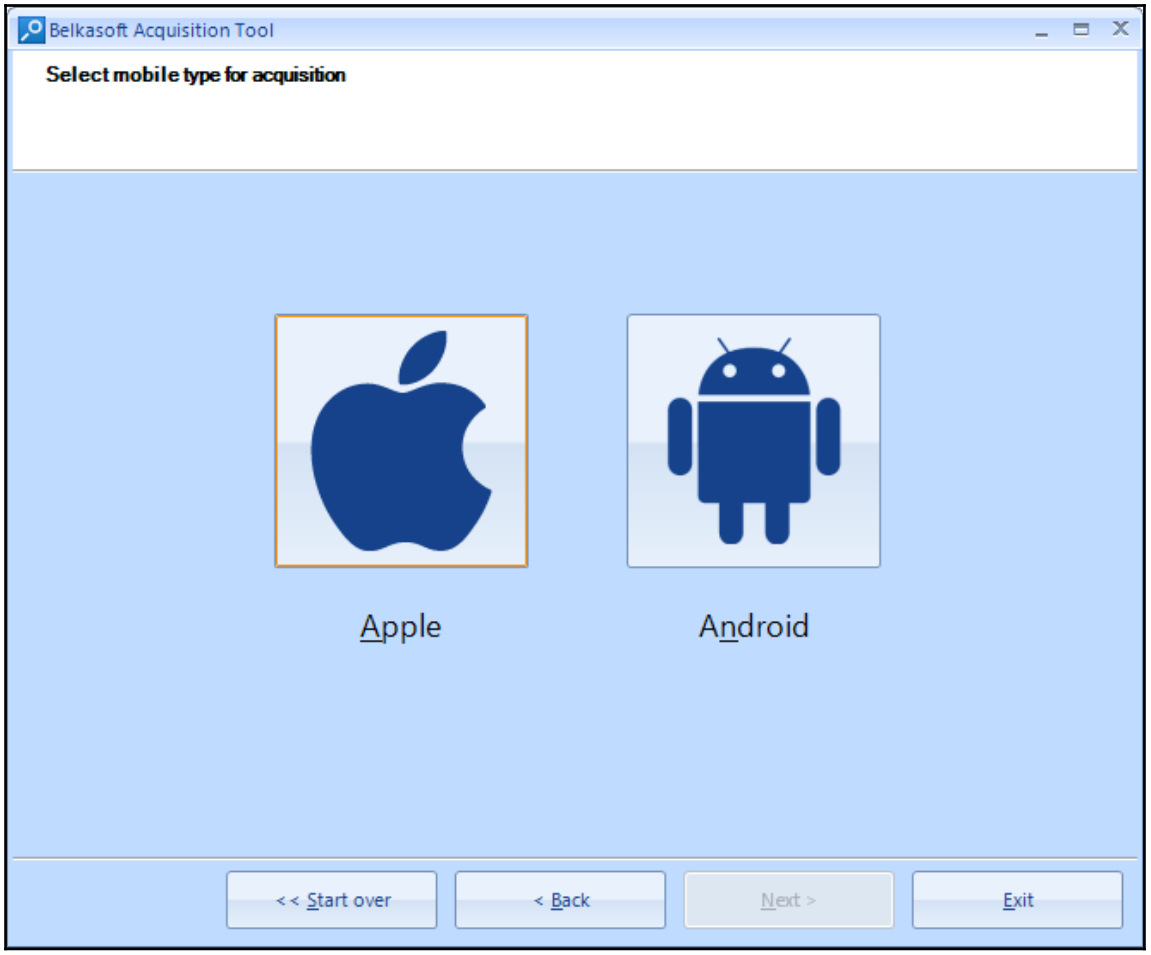
Release only the power button. Keep holding the home button.

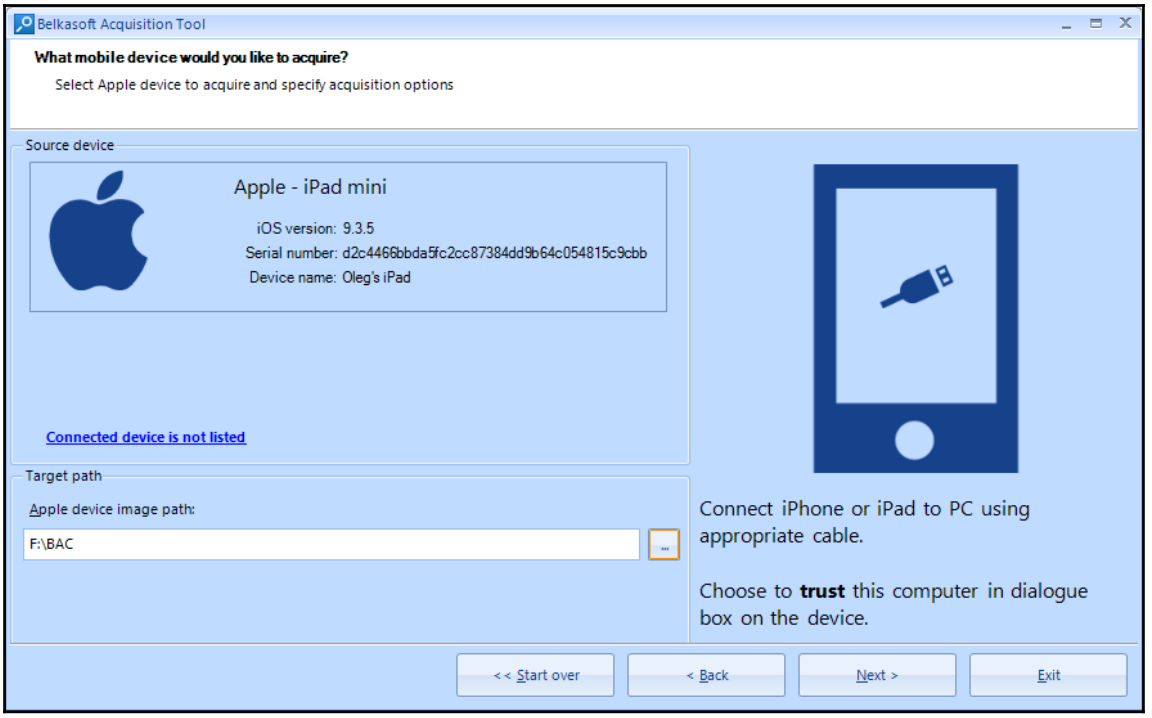
< Back

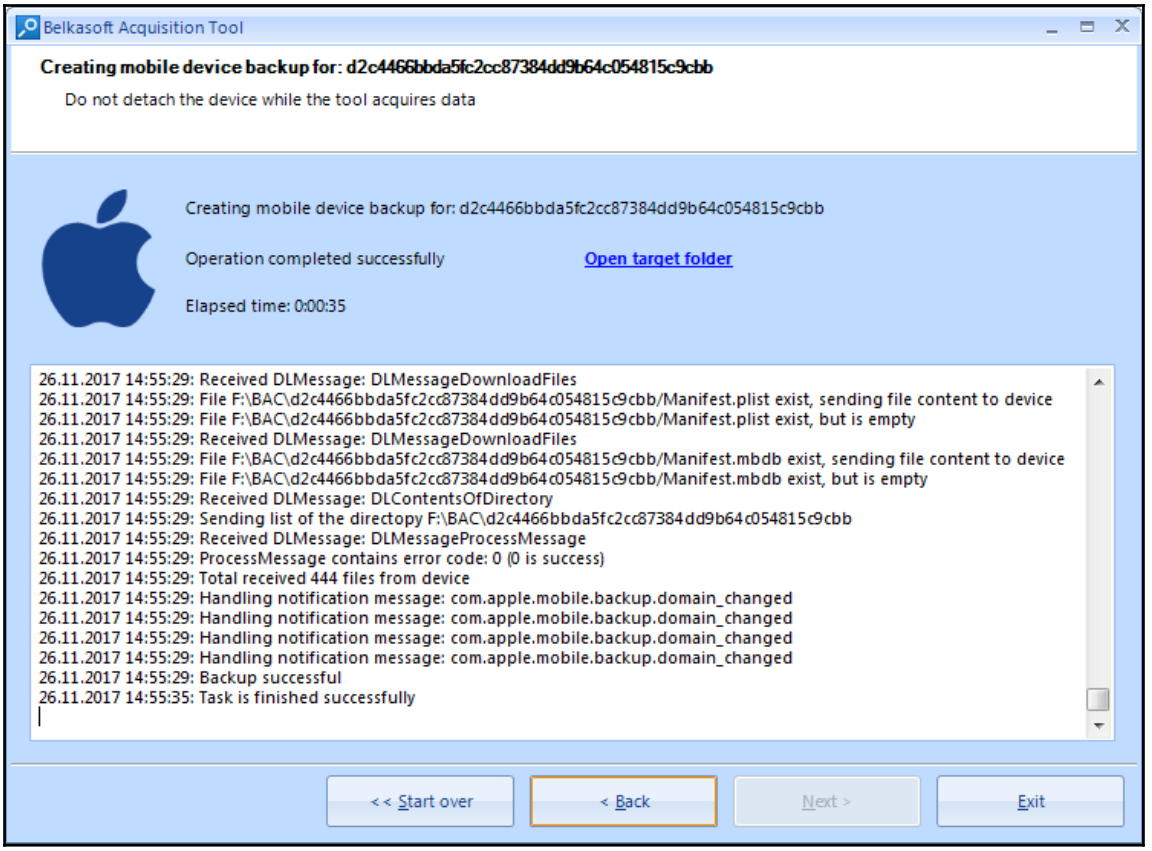

MacBook Air
Diagnostics
Disc Burning
Ethernet Cards
Fibre Channel
FireWire
Graphics/Displays
Hardware RAID
Memory
NVMExpress
PCI
Parallel SCSI
Power
Printers
SAS
SATA/SATA Express
SPI
Storage
Thunderbolt
USB
iBridge
Network
Firewall
Locations
Volumes
WWAN
Wi-Fi
Software
Accessibility
Applications
USB Device Tree
Hub
Hub
Card Reader
Apple Internal Keyboard / Trackpad
BRCM20702 Hub
Bluetooth USB Host Controller
USB 3.0 Bus
Apple Mobile Device (DFU Mode)
Apple Mobile Device (DFU Mode):
Product ID: 0x1227
Vendor ID: 0x05ac (Apple Inc.)
Version: 0.00
Serial Number: CPID:8942 CPRV:10 CPFM:03 SCEP:10 BDID:0A ECID:0000030B8F12B58C IBFL:00 SRTG:[rom]
Speed: Up to 480 Mb/sec
Manufacturer: Apple Inc.
Location ID: 0x14200000 / 4
Current Available (mA): 500
Current Required (mA): 500
Extra Operating Current (mA): 0
Oleg's MacBook Air › Hardware › USB › USB 3.0 Bus › Apple Mobile Device (DFU Mode)

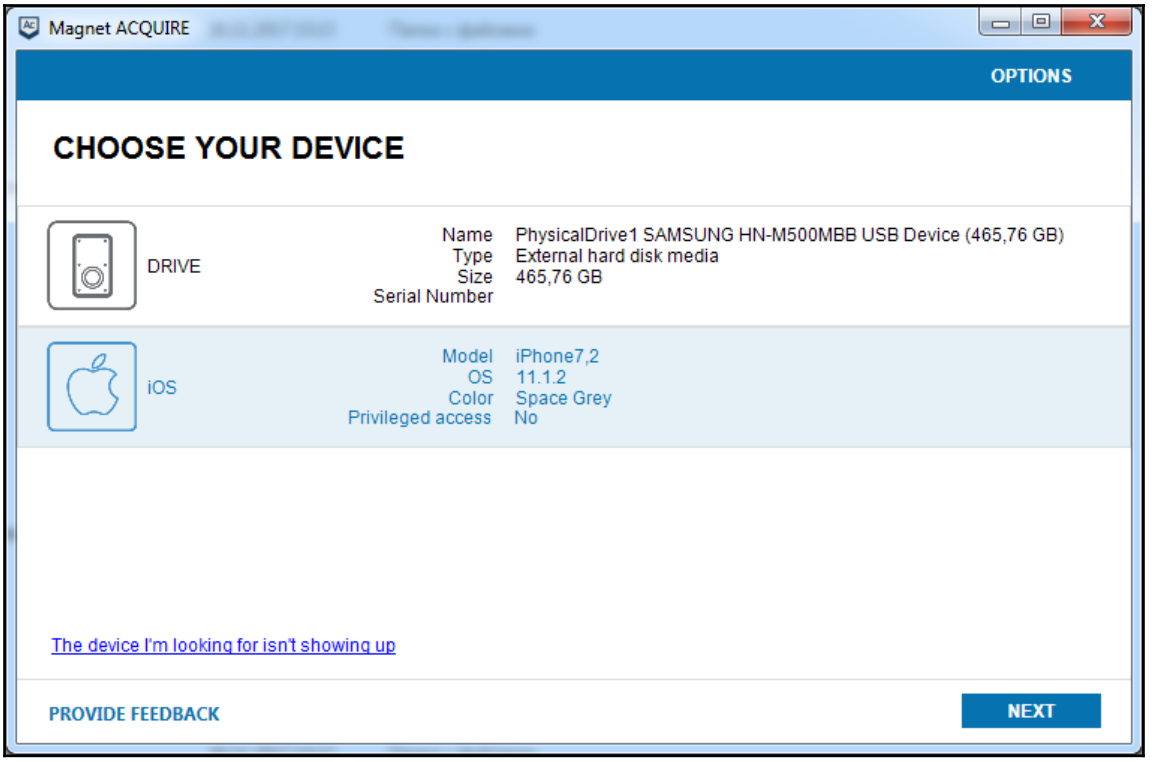

olegskulkin — -bash — 80×24
Olegs-MacBook-Air:~ olegskulkin$ idevicebackup2 backup --full /Users/olegskulkin/Desktop/backup
Backup directory is "/Users/olegskulkin/Desktop/backup"
Started "com.apple.mobilebackup2" service on port 49580.
Negotiated Protocol Version 2.1
Starting backup...
Enforcing full backup from device.
Backup will be encrypted.
Requesting backup from device...
Full backup mode.
[=] 1% Finished
Receiving files
[=] 0% (464 Bytes/7.1 MB)
[==========] 100% (7.1 MB/7.1 MB)
[==========] 100% (7.1 MB/7.1 MB)
[==========] 100% (7.1 MB/7.1 MB)
[==========] 100% (7.1 MB/7.1 MB)
[==========] 100% (7.1 MB/7.1 MB)
[==========] 100% (7.1 MB/7.1 MB)
[==========] 100% (7.1 MB/7.1 MB)
[==========] 100% (7.1 MB/7.1 MB)
[==========] 100% (7.1 MB/7.1 MB)
[==========] 100% (7.1 MB/7.1 MB)

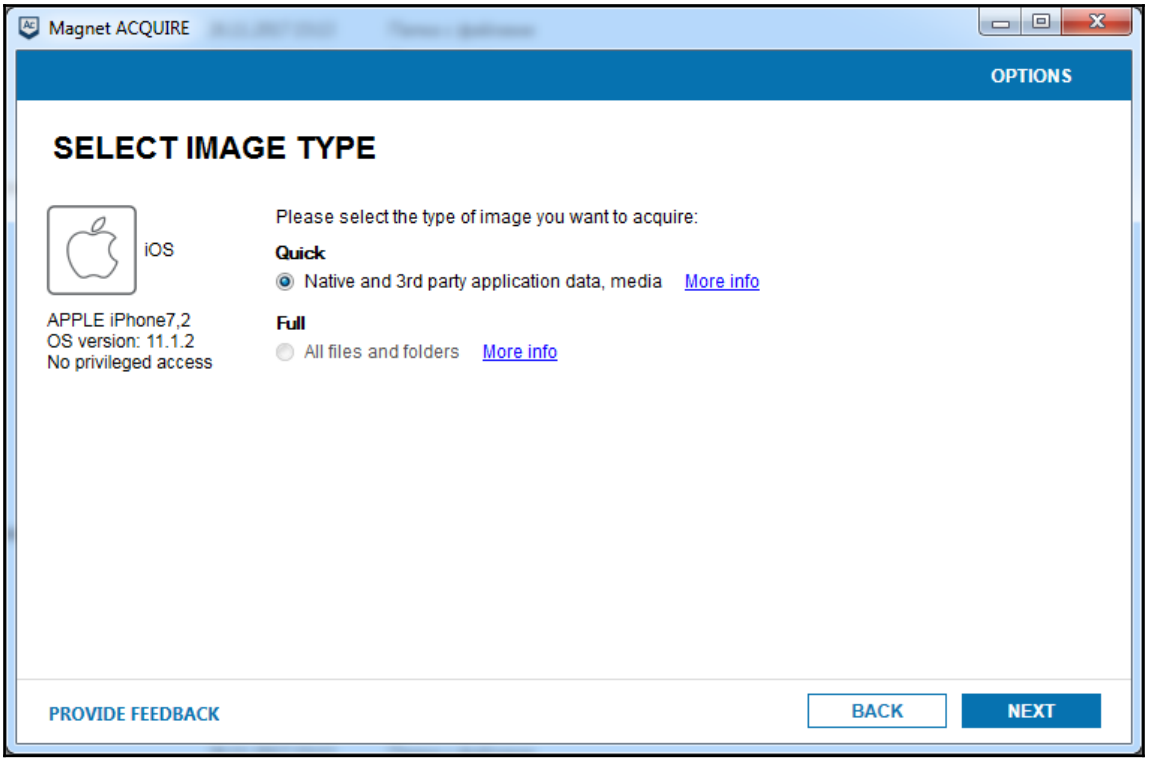

Belkasoft Acquisition Tool
What sources would you like to acquire?
Select drive, mobile device or cloud to acquire
Drive
Mobile device
Cloud data
Exit

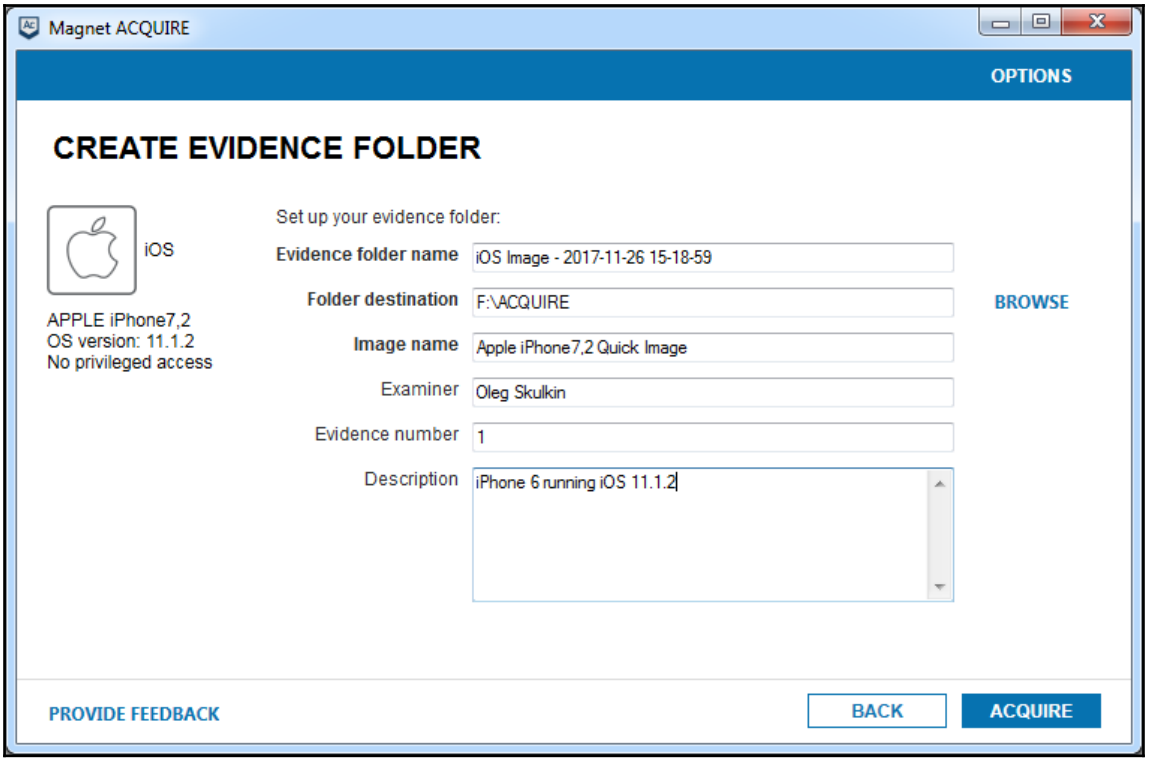

Belkasoft Acquisition Tool
Select mobile type for acquisition
Apple
Android
<< Start over
< Back
Next >
Exit

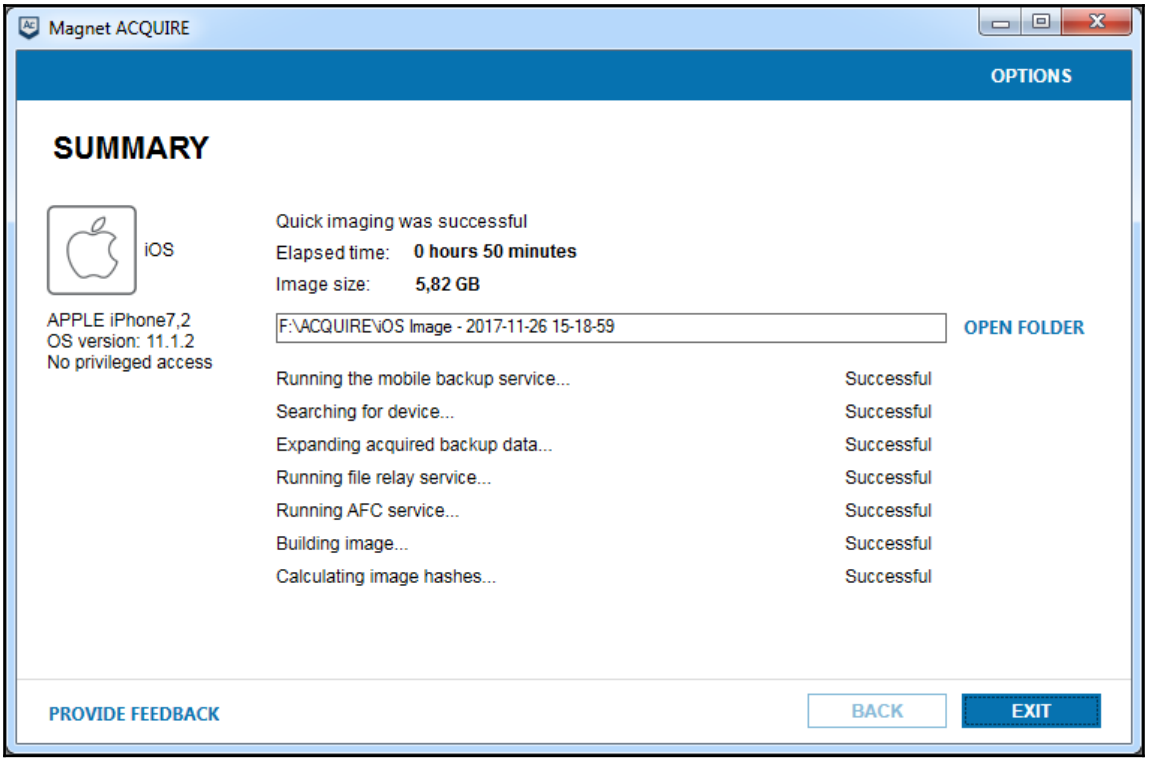

Belkasoft Acquisition Tool
What mobile device would you like to acquire?
Select Apple device to acquire and specify acquisition options
Source device
Apple - iPad mini
iOS version: 9.3.5
Serial number: d2c4466bbda5fc2cc87384dd9b64c054815c9cbb
Device name: Oleg's iPad
Connected device is not listed
Target path
Apple device image path:
F:\BAC
...
Connect iPhone or iPad to PC using appropriate cable.
Choose to trust this computer in dialogue box on the device.
<< Start over
< Back
Next >
Exit

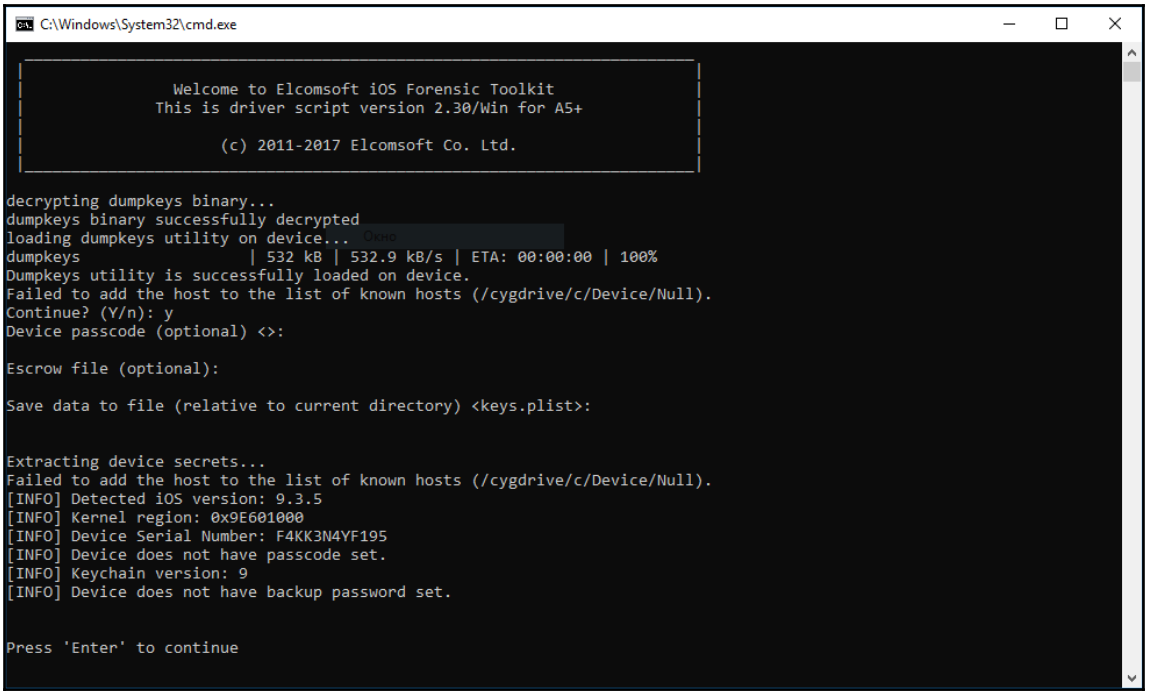

Belkasoft Acquisition Tool
Creating mobile device backup for: d2c4466bbda5fc2cc87384dd9b64c054815c9cbb
Do not detach the device while the tool acquires data
Creating mobile device backup for: d2c4466bbda5fc2cc87384dd9b64c054815c9cbb
Operation completed successfully
Open target folder
Elapsed time: 0:00:35
26.11.2017 14:55:29: Received DLMessage: DLMessageDownloadFiles
26.11.2017 14:55:29: File F:\BAC\d2c4466bbda5fc2cc87384dd9b64c054815c9cbb/Manifest.plist exist, sending file content to device
26.11.2017 14:55:29: File F:\BAC\d2c4466bbda5fc2cc87384dd9b64c054815c9cbb/Manifest.plist exist, but is empty
26.11.2017 14:55:29: Received DLMessage: DLMessageDownloadFiles
26.11.2017 14:55:29: File F:\BAC\d2c4466bbda5fc2cc87384dd9b64c054815c9cbb/Manifest.mbdb exist, sending file content to device
26.11.2017 14:55:29: File F:\BAC\d2c4466bbda5fc2cc87384dd9b64c054815c9cbb/Manifest.mbdb exist, but is empty
26.11.2017 14:55:29: Received DLMessage: DLContentsOfDirectory
26.11.2017 14:55:29: Sending list of the directopy F:\BAC\d2c4466bbda5fc2cc87384dd9b64c054815c9cbb
26.11.2017 14:55:29: Received DLMessage: DLMessageProcessMessage
26.11.2017 14:55:29: ProcessMessage contains error code: 0 (0 is success)
26.11.2017 14:55:29: Total received 444 files from device
26.11.2017 14:55:29: Handling notification message: com.apple.mobile.backup.domain_changed
26.11.2017 14:55:29: Handling notification message: com.apple.mobile.backup.domain_changed
26.11.2017 14:55:29: Handling notification message: com.apple.mobile.backup.domain_changed
26.11.2017 14:55:29: Handling notification message: com.apple.mobile.backup.domain_changed
26.11.2017 14:55:29: Backup successful
26.11.2017 14:55:35: Task is finished successfully
<< Start over
< Back
Next >
Exit

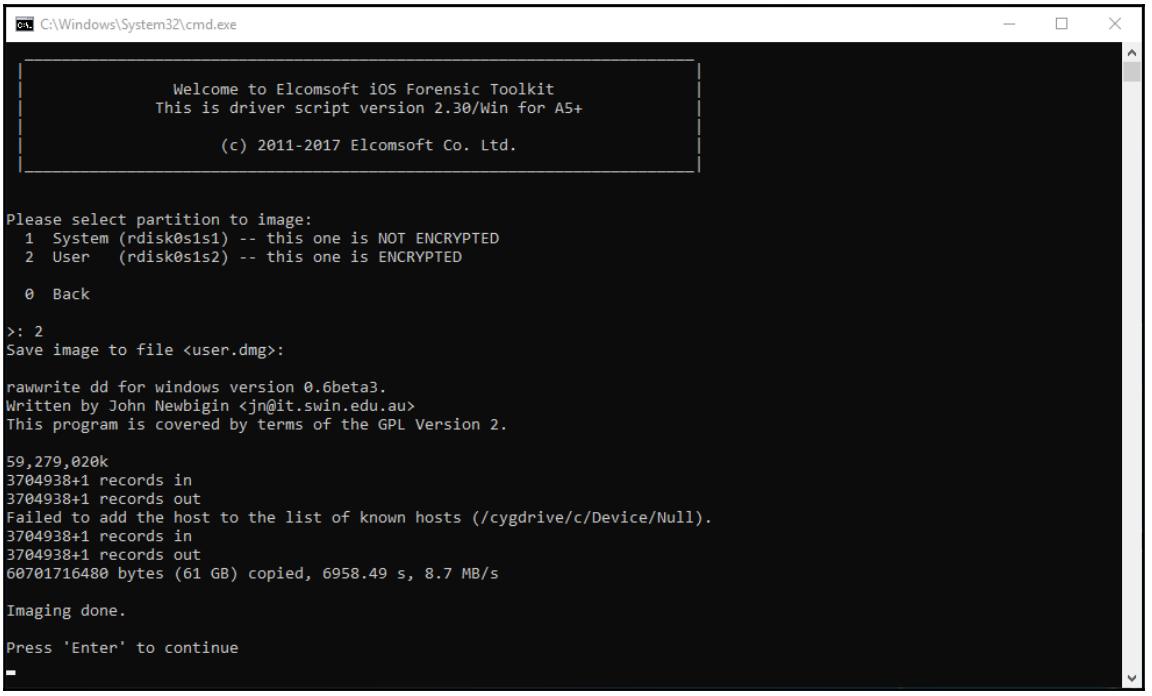

Magnet ACQUIRE
OPTIONS
CHOOSE YOUR DEVICE
DRIVE
Name PhysicalDrive1 SAMSUNG HN-M500MBB USB Device (465,76 GB)
Type External hard disk media
Size 465,76 GB
Serial Number
iOS
Model iPhone7,2
OS 11.1.2
Color Space Grey
Privileged access No
The device I'm looking for isn't showing up
PROVIDE FEEDBACK
NEXT

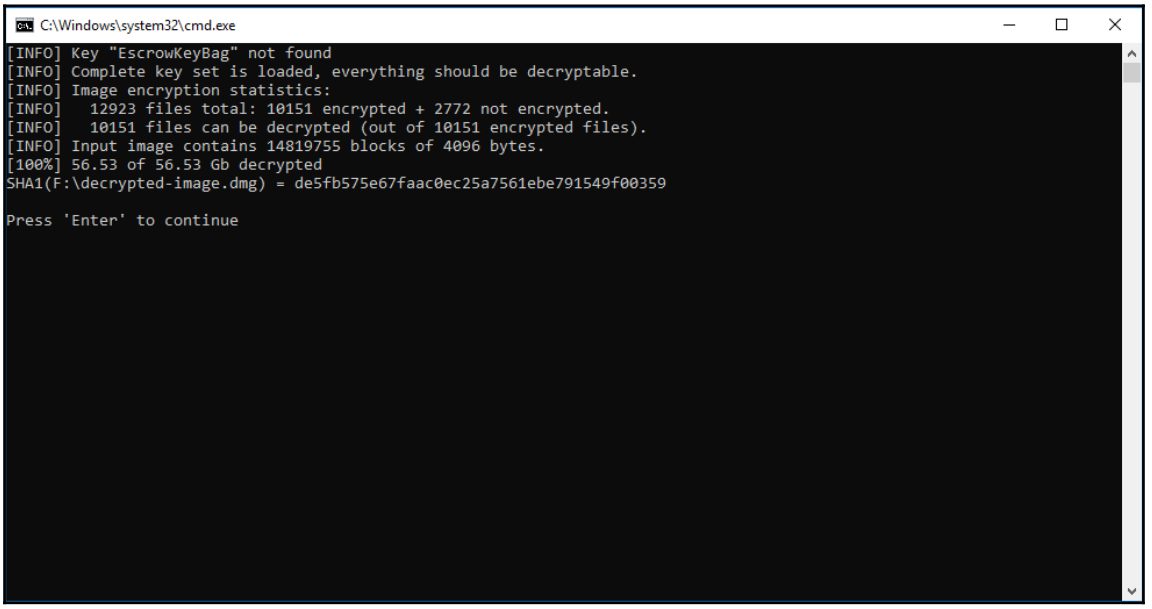

Magnet ACQUIRE
OPTIONS
SELECT IMAGE TYPE
iOS
APPLE iPhone7,2
OS version: 11.1.2
No privileged access
Please select the type of image you want to acquire:
Quick
Native and 3rd party application data, media
More info
Full
All files and folders
More info
PROVIDE FEEDBACK
BACK
NEXT


Magnet ACQUIRE
OPTIONS
CREATE EVIDENCE FOLDER
iOS
APPLE iPhone7,2
OS version: 11.1.2
No privileged access
Set up your evidence folder:
Evidence folder name
iOS Image - 2017-11-26 15-18-59
Folder destination
F:\ACQUIRE
BROWSE
Image name
Apple iPhone7,2 Quick Image
Examiner
Oleg Skulkin
Evidence number
1
Description
iPhone 6 running iOS 11.1.2
PROVIDE FEEDBACK
BACK
ACQUIRE

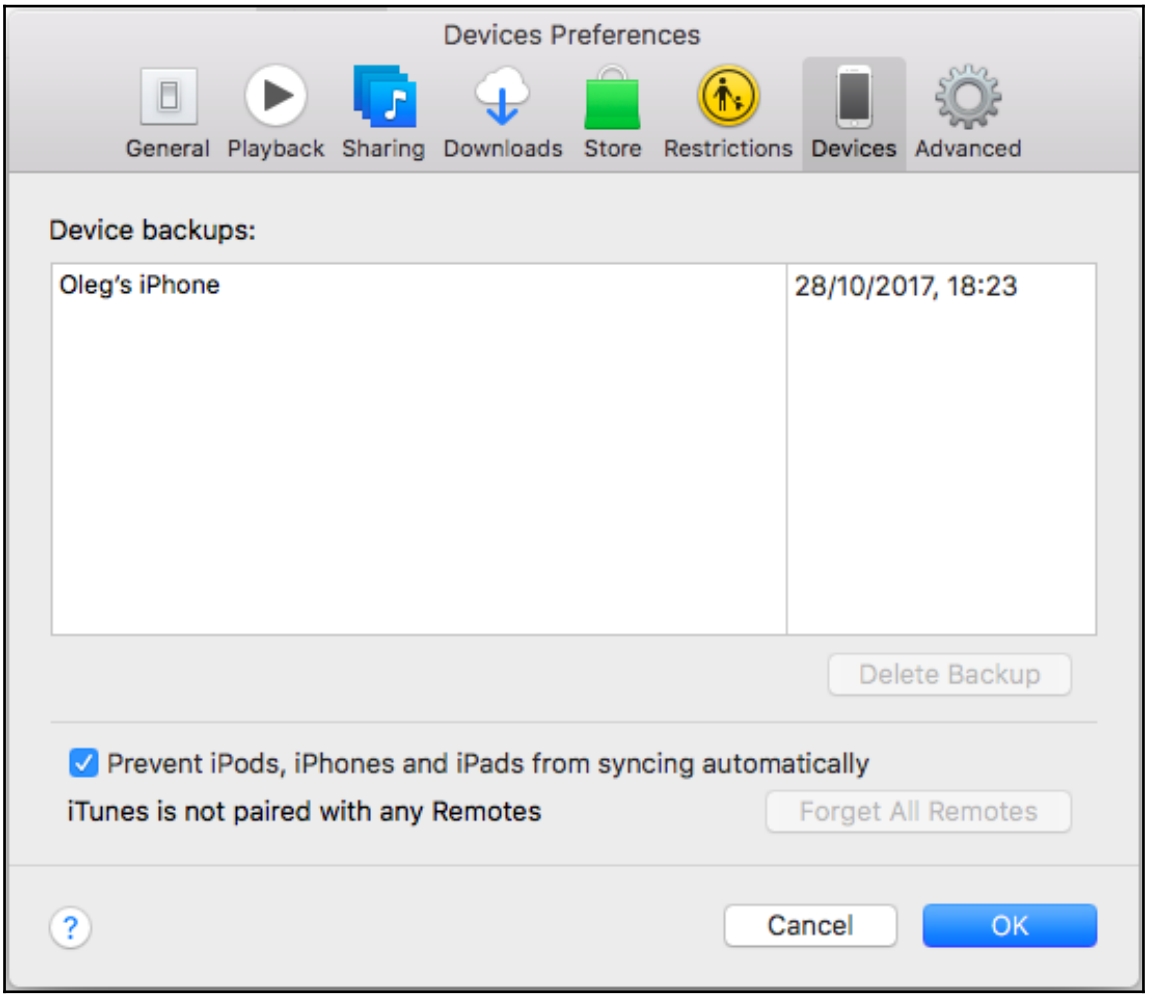

Magnet ACQUIRE
OPTIONS
SUMMARY
iOS
APPLE iPhone7,2
OS version: 11.1.2
No privileged access
Quick imaging was successful
Elapsed time: 0 hours 50 minutes
Image size: 5,82 GB
F:\ACQUIRE\iOS Image - 2017-11-26 15-18-59
OPEN FOLDER
Running the mobile backup service... Successful
Searching for device... Successful
Expanding acquired backup data... Successful
Running file relay service... Successful
Running AFC service... Successful
Building image... Successful
Calculating image hashes... Successful
PROVIDE FEEDBACK
BACK
EXIT

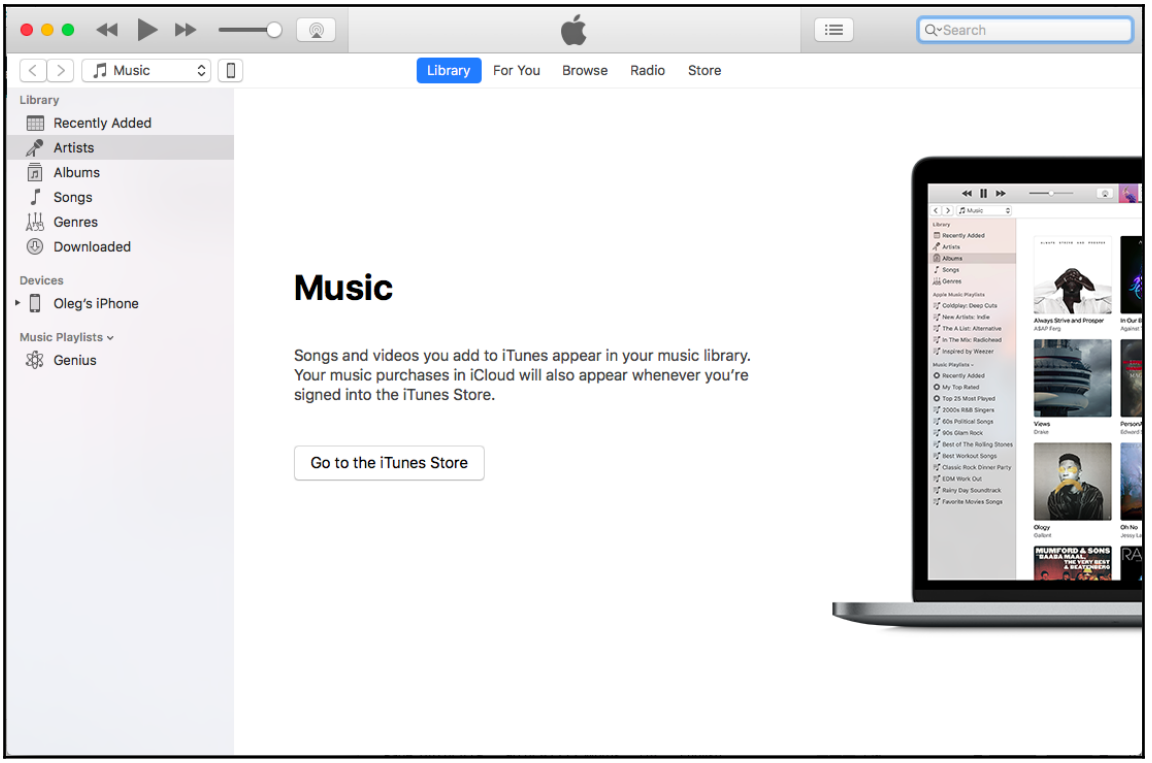

C:\Windows\System32\cmd.exe
Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 2.30/Win for A5+
(c) 2011-2017 Elcomsoft Co. Ltd.
decrypting dumpkeys binary...
dumpkeys binary successfully decrypted
loading dumpkeys utility on device...
dumpkeys | 532 kB | 532.9 kB/s | ETA: 00:00:00 | 100%
Dumpkeys utility is successfully loaded on device.
Failed to add the host to the list of known hosts (/cygdrive/c/Device/Null).
Continue? (Y/n): y
Device passcode (optional) <>:
Escrow file (optional):
Save data to file (relative to current directory) <keys.plist>:
Extracting device secrets...
Failed to add the host to the list of known hosts (/cygdrive/c/Device/Null).
[INFO] Detected iOS version: 9.3.5
[INFO] Kernel region: 0x9E601000
[INFO] Device Serial Number: F4KK3N4YF195
[INFO] Device does not have passcode set.
[INFO] Keychain version: 9
[INFO] Device does not have backup password set.
Press 'Enter' to continue


C:\Windows\System32\cmd.exe
Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 2.30/Win for A5+
(c) 2011-2017 Elcomsoft Co. Ltd.
Please select partition to image:
1 System (rdisk0s1s1) -- this one is NOT ENCRYPTED
2 User (rdisk0s1s2) -- this one is ENCRYPTED
0 Back
>: 2
Save image to file <user.dmg>:
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.
59,279,020k
3704938+1 records in
3704938+1 records out
Failed to add the host to the list of known hosts (/cygdrive/c/Device/Null).
3704938+1 records in
3704938+1 records out
60701716480 bytes (61 GB) copied, 6958.49 s, 8.7 MB/s
Imaging done.
Press 'Enter' to continue

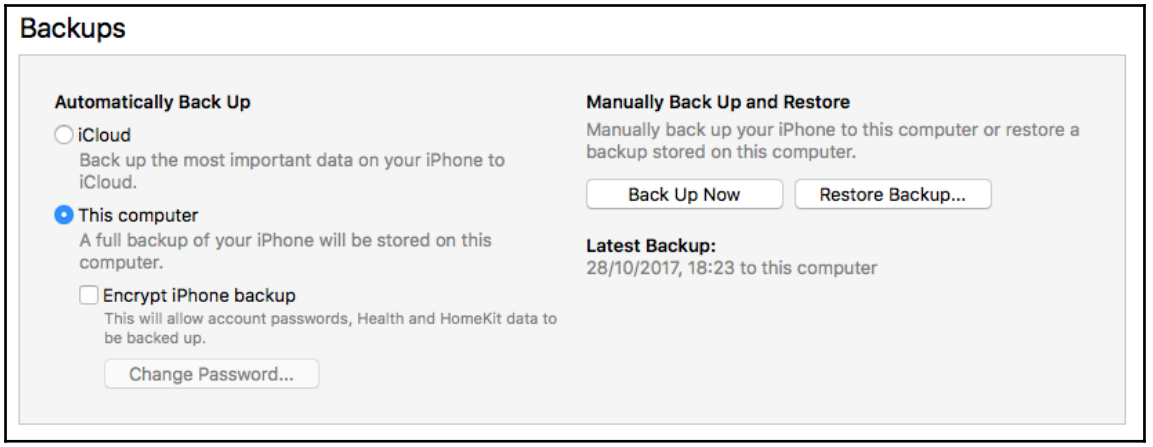

C:\Windows\system32\cmd.exe
[INFO] Key "EscrowKeyBag" not found
[INFO] Complete key set is loaded, everything should be decryptable.
[INFO] Image encryption statistics:
[INFO] 12923 files total: 10151 encrypted + 2772 not encrypted.
[INFO] 10151 files can be decrypted (out of 10151 encrypted files).
[INFO] Input image contains 14819755 blocks of 4096 bytes.
[100%] 56.53 of 56.53 Gb decrypted
SHA1(F:\decrypted-image.dmg) = de5fb575e67faac0ec25a7561ebe791549f00359
Press 'Enter' to continue

Chapter 4: Data Acquisition from iOS Backups

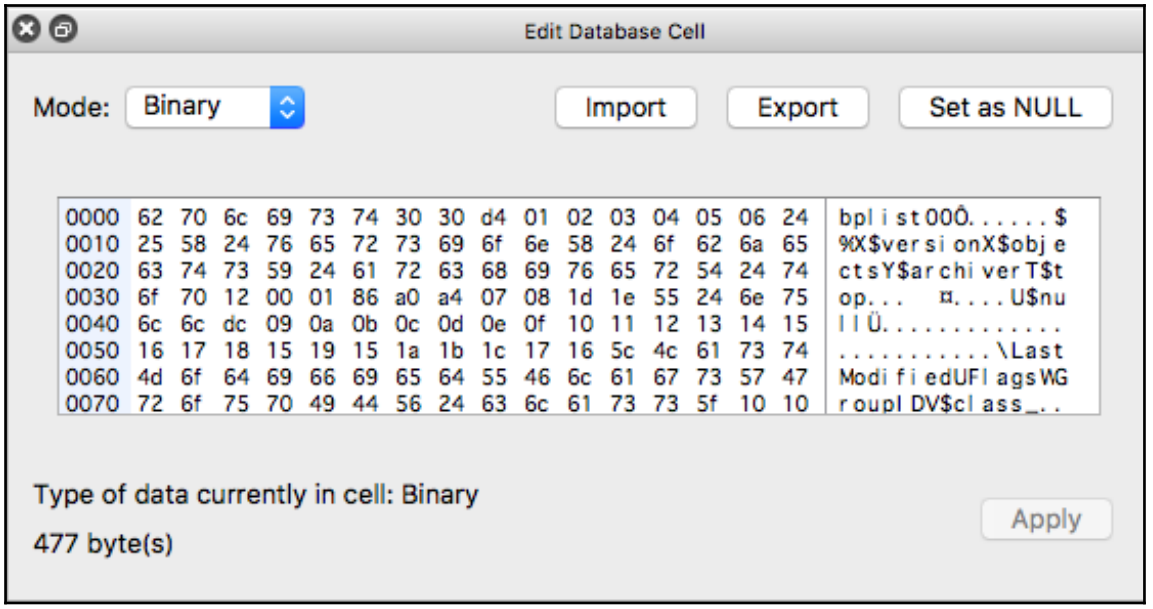


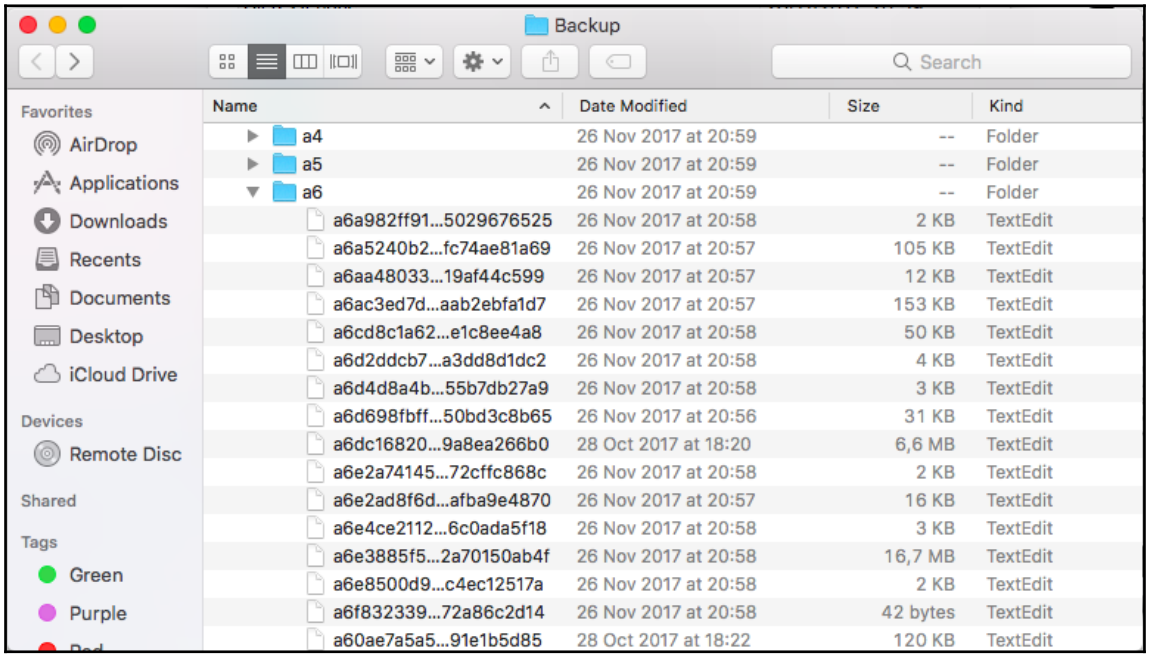

Search
Music
Library
For You
Browse
Radio
Store
Library
Recently Added
Artists
Albums
Songs
Genres
Downloaded
Devices
Oleg's iPhone
Music Playlists
Genius
Music
Songs and videos you add to iTunes appear in your music library. Your music purchases in iCloud will also appear whenever you're signed into the iTunes Store.
Go to the iTunes Store

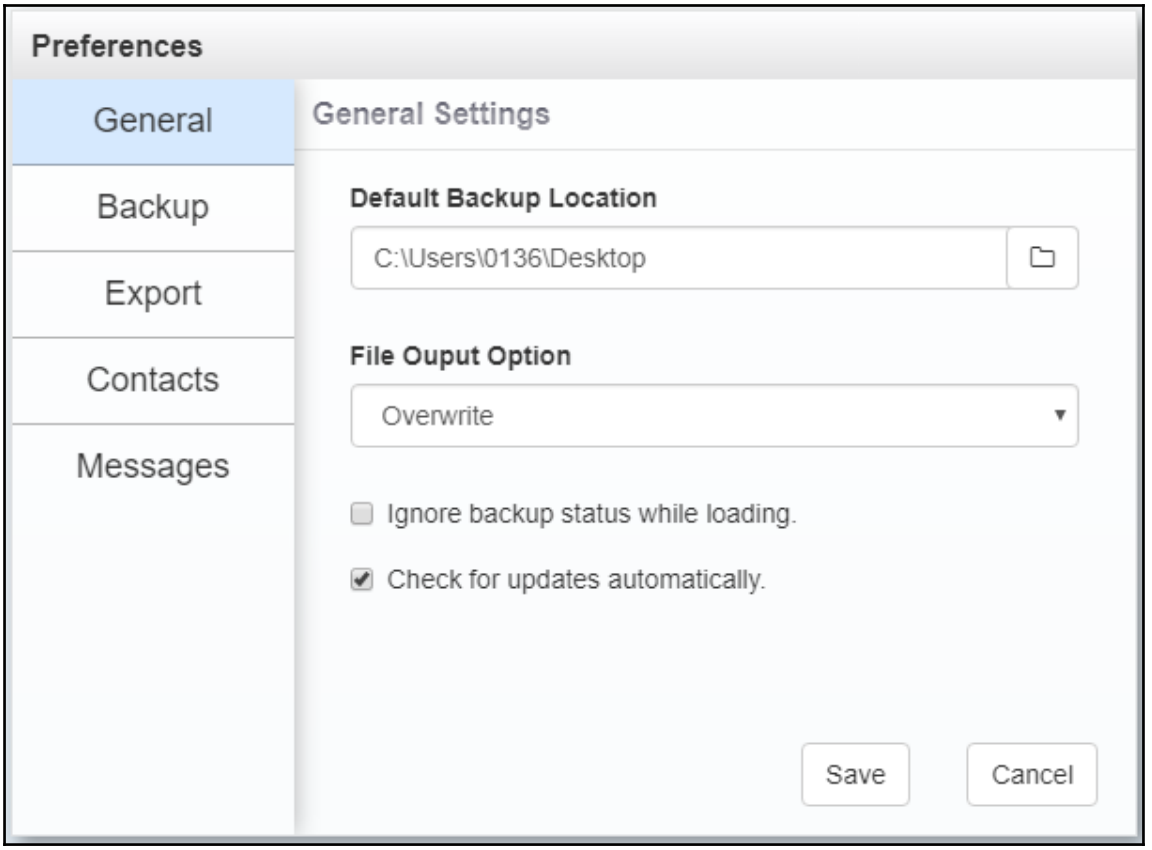

Do you want to allow this computer to access information on "Oleg's iPhone"?
If you don't allow access, you will not be able to manage or sync your iPhone with this computer.
Cancel
Continue

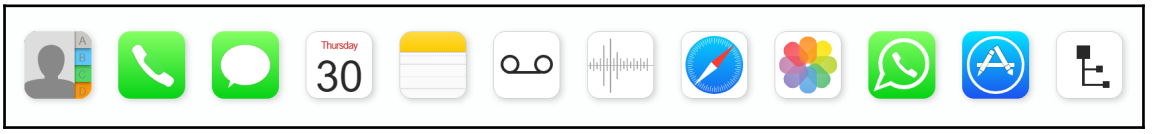


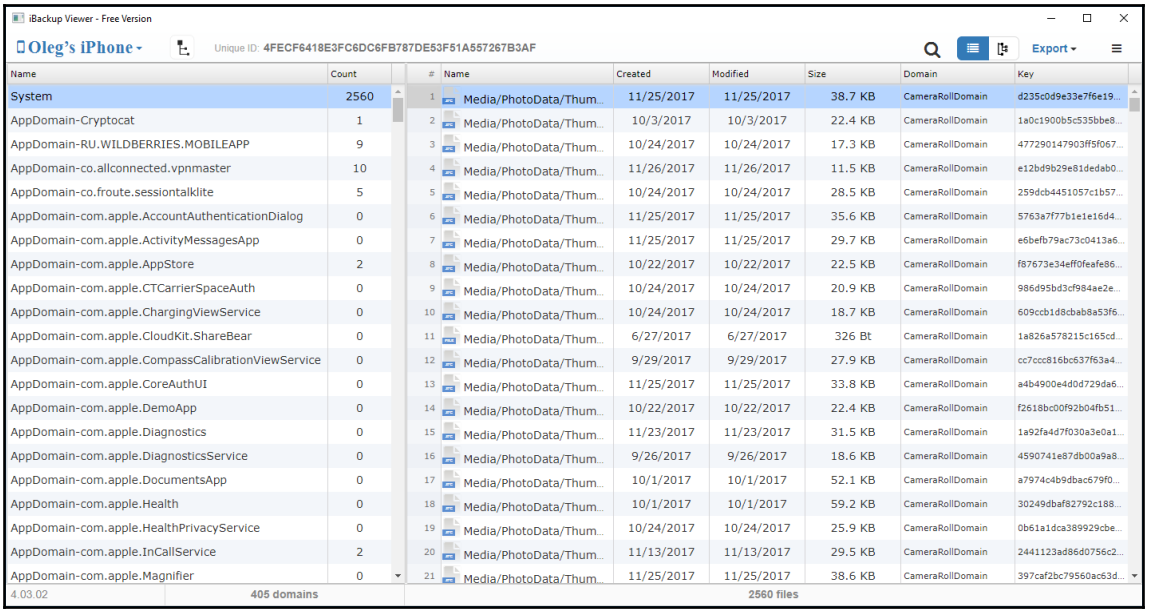
	fileID	domain	relativePath	flags	file
	Filter	Filter	Filter	Filter	Filter
3	e8281626dc6c...	AppDomainPlugin-com.a...	Library/Preferences	2	BLOB
4	d1b0eb5845a0...	AppDomainPlugin-com.a...	Documents	2	BLOB
5	be1f28f40e6e4...	CameraRollDomain		2	BLOB
6	735f4f65879e...	CameraRollDomain	Media	2	BLOB
7	f0a585e77da5...	CameraRollDomain	Media/PhotoData	2	BLOB
8	362cae198187...	CameraRollDomain	Media/PhotoData/iPhotoSandboxLibrary	2	BLOB
9	cacc5a1aca7bb...	CameraRollDomain	Media/PhotoData/Videos	2	BLOB
10	1e3b377ade50...	CameraRollDomain	Media/PhotoData/Thumbnails	2	BLOB
11	38cae1ba16df4...	CameraRollDomain	Media/PhotoData/Thumbnails/V2	2	BLOB
12	e4b86f7b2a58...	CameraRollDomain	Media/PhotoData/Thumbnails/V2/DCIM	2	BLOB
13	ae94e0607ca3...	CameraRollDomain	Media/PhotoData/Thumbnails/V2/DCIM/102APPLE	2	BLOB
14	73813e0c9e75...	CameraRollDomain	Media/PhotoData/Thumbnails/V2/DCIM/102APPLE...	2	BLOB
15	568f4d9a20e7f...	CameraRollDomain	Media/PhotoData/Thumbnails/V2/DCIM/102APPLE...	2	BLOB
16	9d0f5e50c9b4f...	CameraRollDomain	Media/PhotoData/Thumbnails/V2/DCIM/102APPLE...	2	BLOB

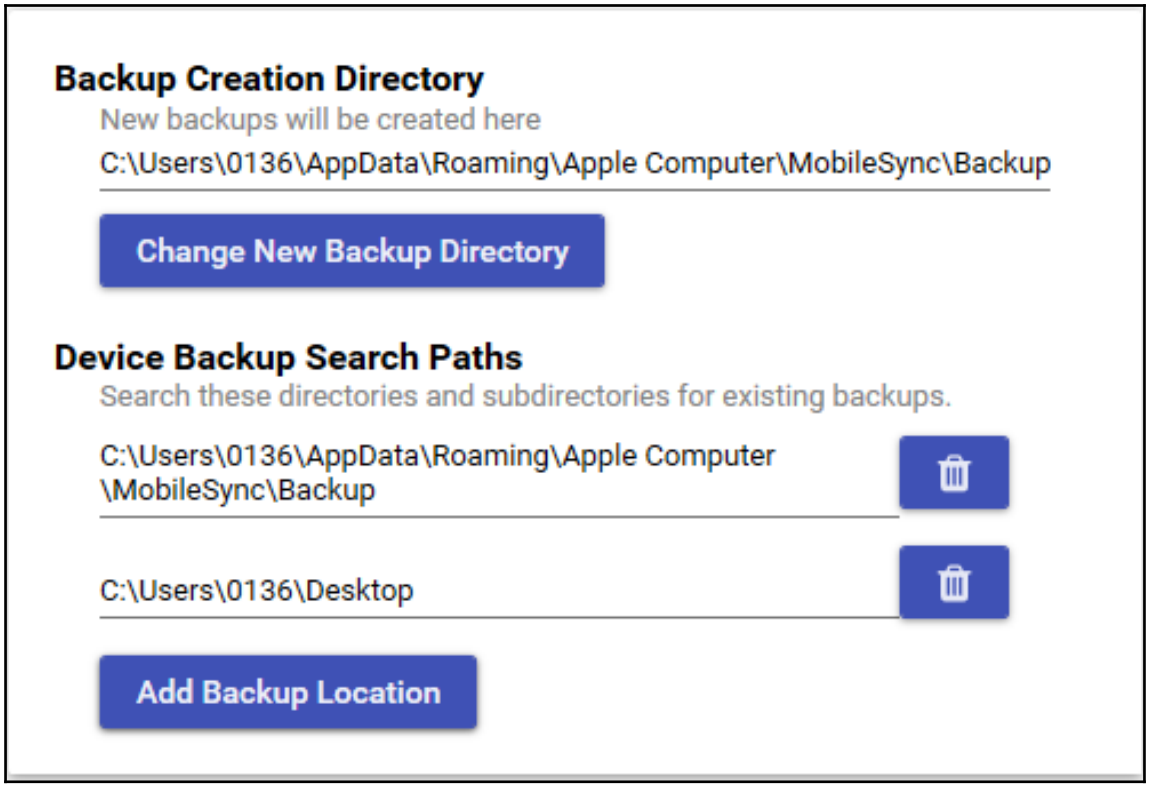

Edit Database Cell
Mode: Binary
Import
Export
Set as NULL
0000 62 70 6c 69 73 74 30 30 d4 01 02 03 04 05 06 24 bplist00Ô.....$
0010 25 58 24 76 65 72 73 69 6f 6e 58 24 6f 62 6a 65 %X$versionX$obje
0020 63 74 73 59 24 61 72 63 68 69 76 65 72 54 24 74 ctsY$archiverT$t
0030 6f 70 12 00 01 86 a0 a4 07 08 1d 1e 55 24 6e 75 op... ¤....U$nu
0040 6c 6c dc 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 llÜ.............
0050 16 17 18 15 19 15 1a 1b 1c 17 16 5c 4c 61 73 74 ....\Last
0060 4d 6f 64 69 66 69 65 64 55 46 6c 61 67 73 57 47 ModifiedUFlagsWG
0070 72 6f 75 70 49 44 56 24 63 6c 61 73 73 5f 10 10 roupIDV$class_..
Type of data currently in cell: Binary
477 byte(s)
Apply

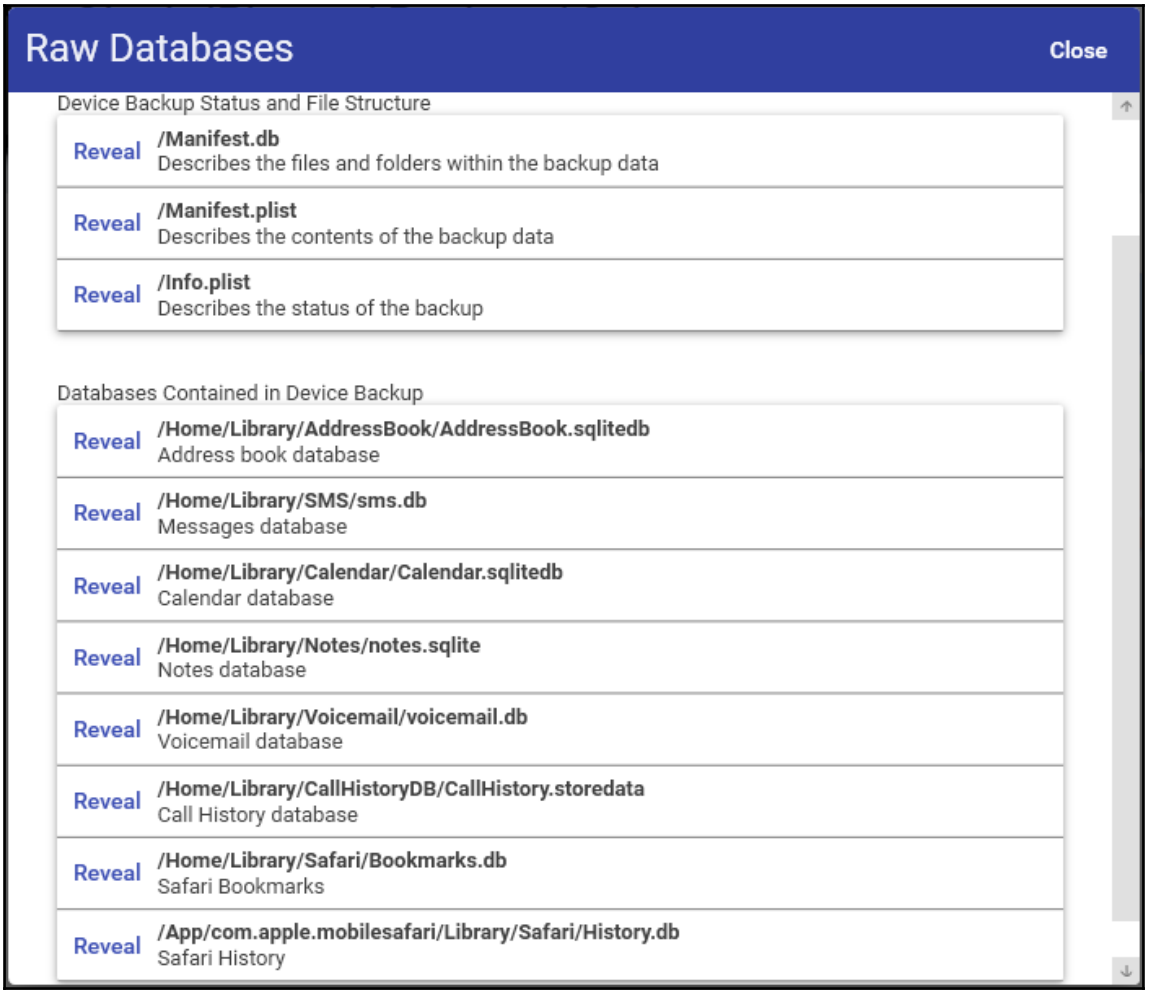

Backup
Search
Favorites
AirDrop
Applications
Downloads
Recents
Documents
Desktop
iCloud Drive
Devices
Remote Disc
Shared
Tags
Green
Purple
Name
Date Modified
Size
Kind
a4 26 Nov 2017 at 20:59 -- Folder
a5 26 Nov 2017 at 20:59 -- Folder
a6 26 Nov 2017 at 20:59 -- Folder
a6a982ff91...5029676525 26 Nov 2017 at 20:58 2 KB TextEdit
a6a5240b2...fc74ae81a69 26 Nov 2017 at 20:57 105 KB TextEdit
a6aa48033...19af44c599 26 Nov 2017 at 20:57 12 KB TextEdit
a6ac3ed7d...aab2ebfa1d7 26 Nov 2017 at 20:57 153 KB TextEdit
a6cd8c1a62...e1c8ee4a8 26 Nov 2017 at 20:58 50 KB TextEdit
a6d2ddcb7...a3dd8d1dc2 26 Nov 2017 at 20:58 4 KB TextEdit
a6d4d8a4b...55b7db27a9 26 Nov 2017 at 20:58 3 KB TextEdit
a6d698fbff...50bd3c8b65 26 Nov 2017 at 20:56 31 KB TextEdit
a6dc16820...9a8ea266b0 28 Oct 2017 at 18:20 6,6 MB TextEdit
a6e2a74145...72cffc868c 26 Nov 2017 at 20:58 2 KB TextEdit
a6e2ad8f6d...afba9e4870 26 Nov 2017 at 20:57 16 KB TextEdit
a6e4ce2112...6c0ada5f18 26 Nov 2017 at 20:58 3 KB TextEdit
a6e3885f5...2a70150ab4f 26 Nov 2017 at 20:58 16,7 MB TextEdit
a6e8500d9...c4ec12517a 26 Nov 2017 at 20:58 2 KB TextEdit
a6f832339...72a86c2d14 26 Nov 2017 at 20:58 42 bytes TextEdit
a60ae7a5a5...91e1b5d85 28 Oct 2017 at 18:22 120 KB TextEdit

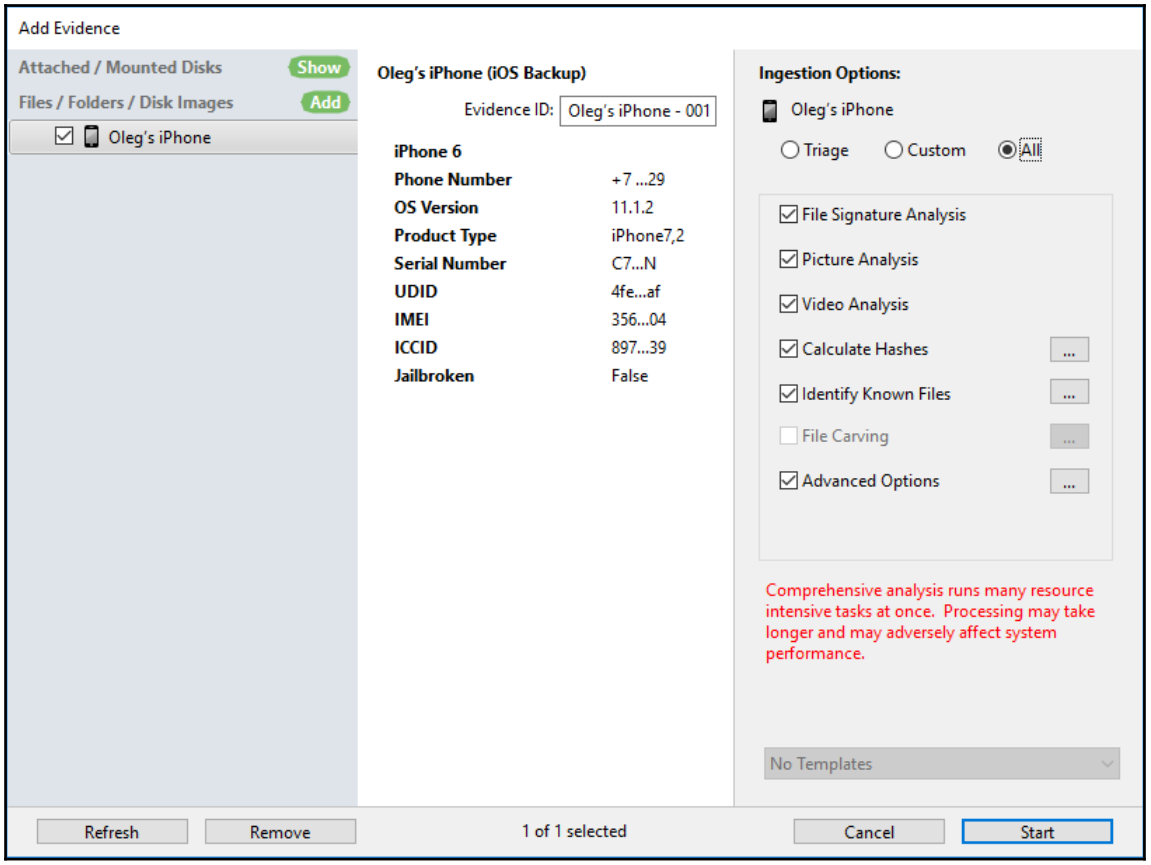

Preferences
General
Backup
Export
Contacts
Messages
General Settings
Default Backup Location
C:\Users\0136\Desktop
File Ouput Option
Overwrite
Ignore backup status while loading.
Check for updates automatically.
Save
Cancel

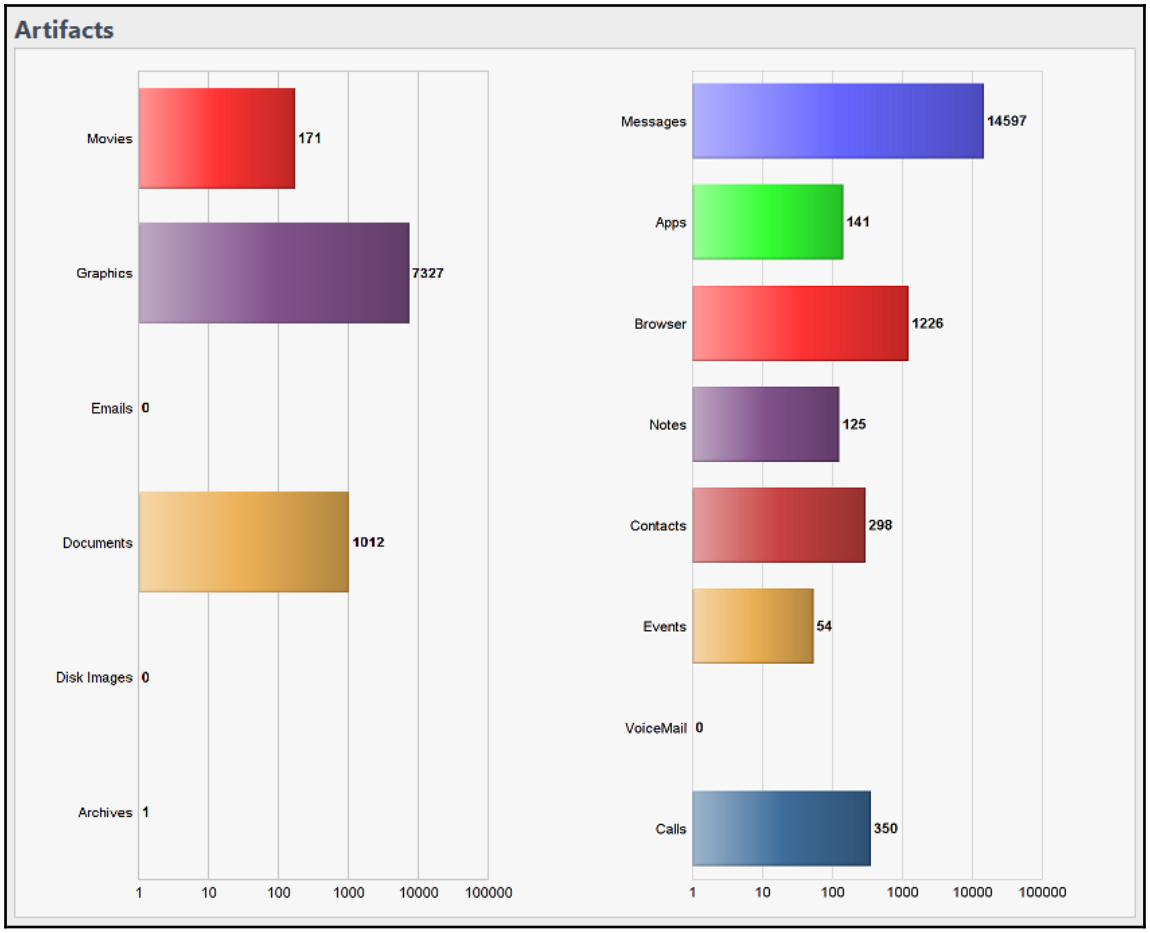

Thursday
30

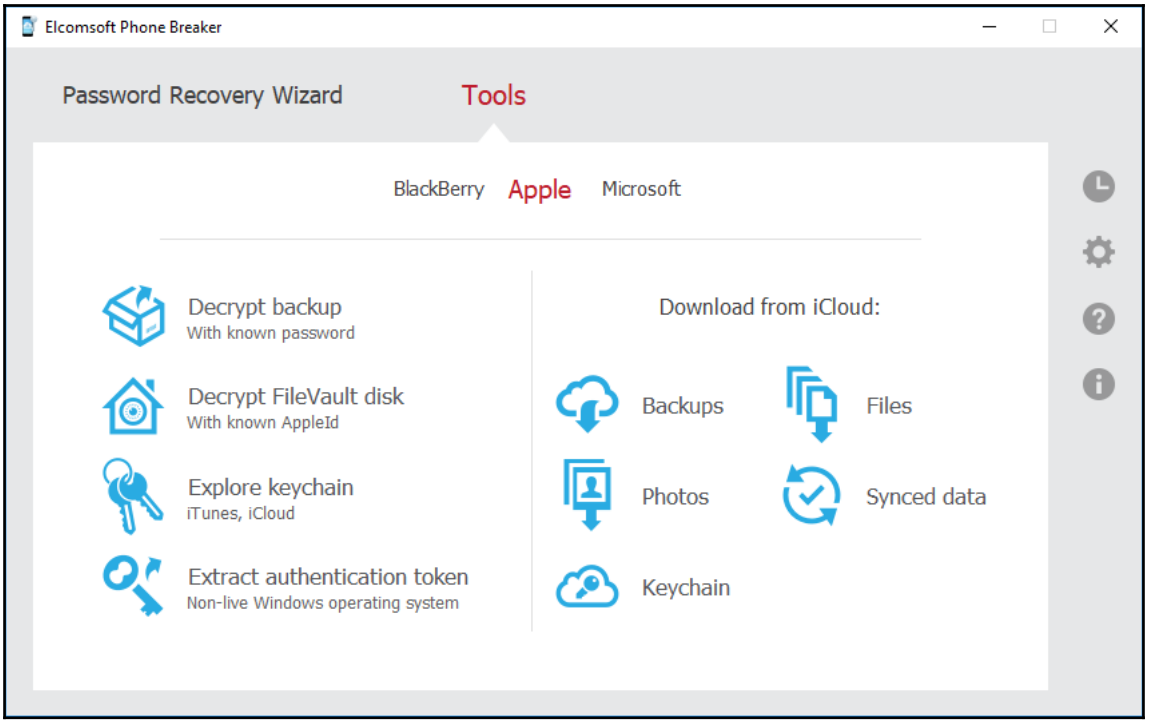

iBackup Viewer - Free Version
Oleg's iPhone
Unique ID: 4FECF6418E3FC6DC6FB787DE53F51A557267B3AF
Export
Name
Count
System
2560
AppDomain-Cryptocat
1
AppDomain-RU.WILDBERRIES.MOBILEAPP
9
AppDomain-co.allconnected.vpnmaster
10
AppDomain-co.froute.sessiontalklite
5
AppDomain-com.apple.AccountAuthenticationDialog
0
AppDomain-com.apple.ActivityMessagesApp
0
AppDomain-com.apple.AppStore
2
AppDomain-com.apple.CTCarrierSpaceAuth
0
AppDomain-com.apple.ChargingViewService
0
AppDomain-com.apple.CloudKit.ShareBear
0
AppDomain-com.apple.CompassCalibrationViewService
0
AppDomain-com.apple.CoreAuthUI
0
AppDomain-com.apple.DemoApp
0
AppDomain-com.apple.Diagnostics
0
AppDomain-com.apple.DiagnosticsService
0
AppDomain-com.apple.DocumentsApp
0
AppDomain-com.apple.Health
0
AppDomain-com.apple.HealthPrivacyService
0
AppDomain-com.apple.InCallService
2
AppDomain-com.apple.Magnifier
0
4.03.02
405 domains
Name Created Modified Size Domain Key
1 Media/PhotoData/Thum... 11/25/2017 11/25/2017 38.7 KB CameraRollDomain d235c0d9e33e7f6e19...
2 Media/PhotoData/Thum... 10/3/2017 10/3/2017 22.4 KB CameraRollDomain 1a0c1900b5c535bbe8...
3 Media/PhotoData/Thum... 10/24/2017 10/24/2017 17.3 KB CameraRollDomain 477290147903ff5f067...
4 Media/PhotoData/Thum... 11/26/2017 11/26/2017 11.5 KB CameraRollDomain e12bd9b29e81dedab0...
5 Media/PhotoData/Thum... 10/24/2017 10/24/2017 28.5 KB CameraRollDomain 259dcb4451057c1b57...
6 Media/PhotoData/Thum... 11/25/2017 11/25/2017 35.6 KB CameraRollDomain 5763a7f77b1e1e16d4...
7 Media/PhotoData/Thum... 11/25/2017 11/25/2017 29.7 KB CameraRollDomain e6befb79ac73c0413a6...
8 Media/PhotoData/Thum... 10/22/2017 10/22/2017 22.5 KB CameraRollDomain f87673e34eff0feafe86...
9 Media/PhotoData/Thum... 10/24/2017 10/24/2017 20.9 KB CameraRollDomain 986d95bd3cf984ae2e...
10 Media/PhotoData/Thum... 10/24/2017 10/24/2017 18.7 KB CameraRollDomain 609ccb1d8cbab8a53f6...
11 Media/PhotoData/Thum... 6/27/2017 6/27/2017 326 Bt CameraRollDomain 1a826a578215c165cd...
12 Media/PhotoData/Thum... 9/29/2017 9/29/2017 27.9 KB CameraRollDomain cc7ccc816bc637f63a4...
13 Media/PhotoData/Thum... 11/25/2017 11/25/2017 33.8 KB CameraRollDomain a4b4900e4d0d729da6...
14 Media/PhotoData/Thum... 10/22/2017 10/22/2017 22.4 KB CameraRollDomain f2618bc00f92b04fb51...
15 Media/PhotoData/Thum... 11/23/2017 11/23/2017 31.5 KB CameraRollDomain 1a92fa4d7f030a3e0a1...
16 Media/PhotoData/Thum... 9/26/2017 9/26/2017 18.6 KB CameraRollDomain 4590741e87db00a9a8...
17 Media/PhotoData/Thum... 10/1/2017 10/1/2017 52.1 KB CameraRollDomain a7974c4b9dbac679f0...
18 Media/PhotoData/Thum... 10/1/2017 10/1/2017 59.2 KB CameraRollDomain 30249dbaf82792c188...
19 Media/PhotoData/Thum... 10/24/2017 10/24/2017 25.9 KB CameraRollDomain 0b61a1dca389929cbe...
20 Media/PhotoData/Thum... 11/13/2017 11/13/2017 29.5 KB CameraRollDomain 2441123ad86d0756c2...
21 Media/PhotoData/Thum... 11/25/2017 11/25/2017 38.6 KB CameraRollDomain 397caf2bc79560ac63d...
2560 files

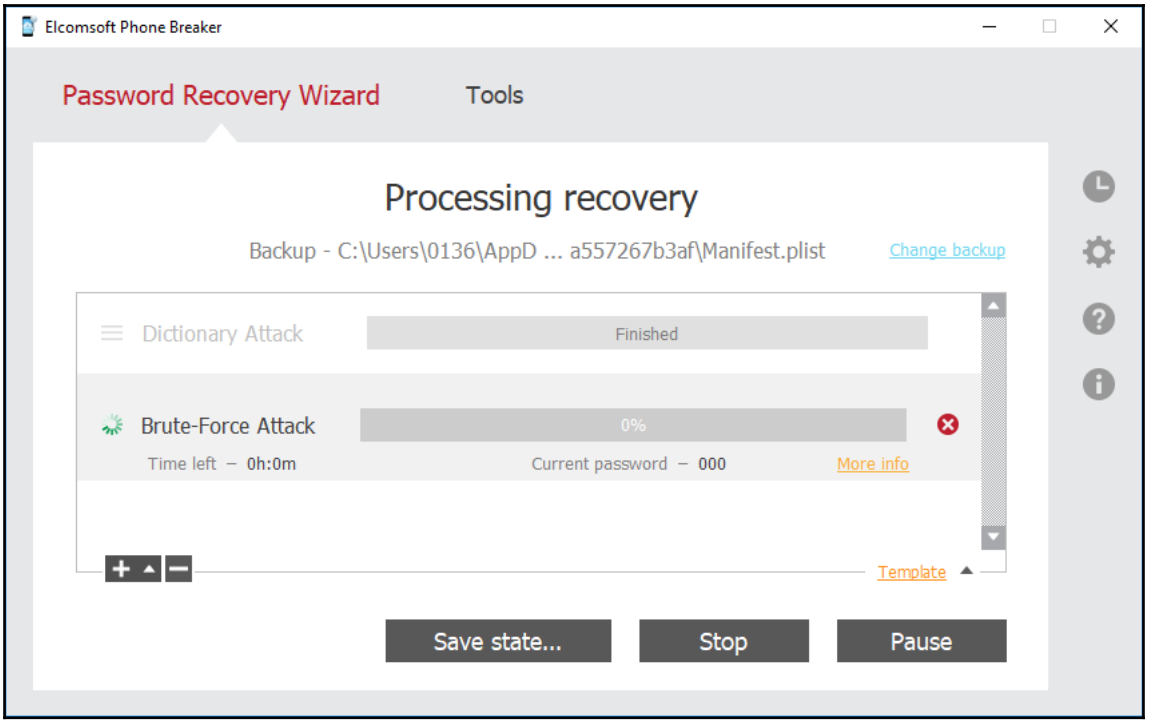

Backup Creation Directory
New backups will be created here
C:\Users\0136\AppData\Roaming\Apple Computer\MobileSync\Backup
Change New Backup Directory
Device Backup Search Paths
Search these directories and subdirectories for existing backups.
C:\Users\0136\AppData\Roaming\Apple Computer
\MobileSync\Backup
C:\Users\0136\Desktop
Add Backup Location

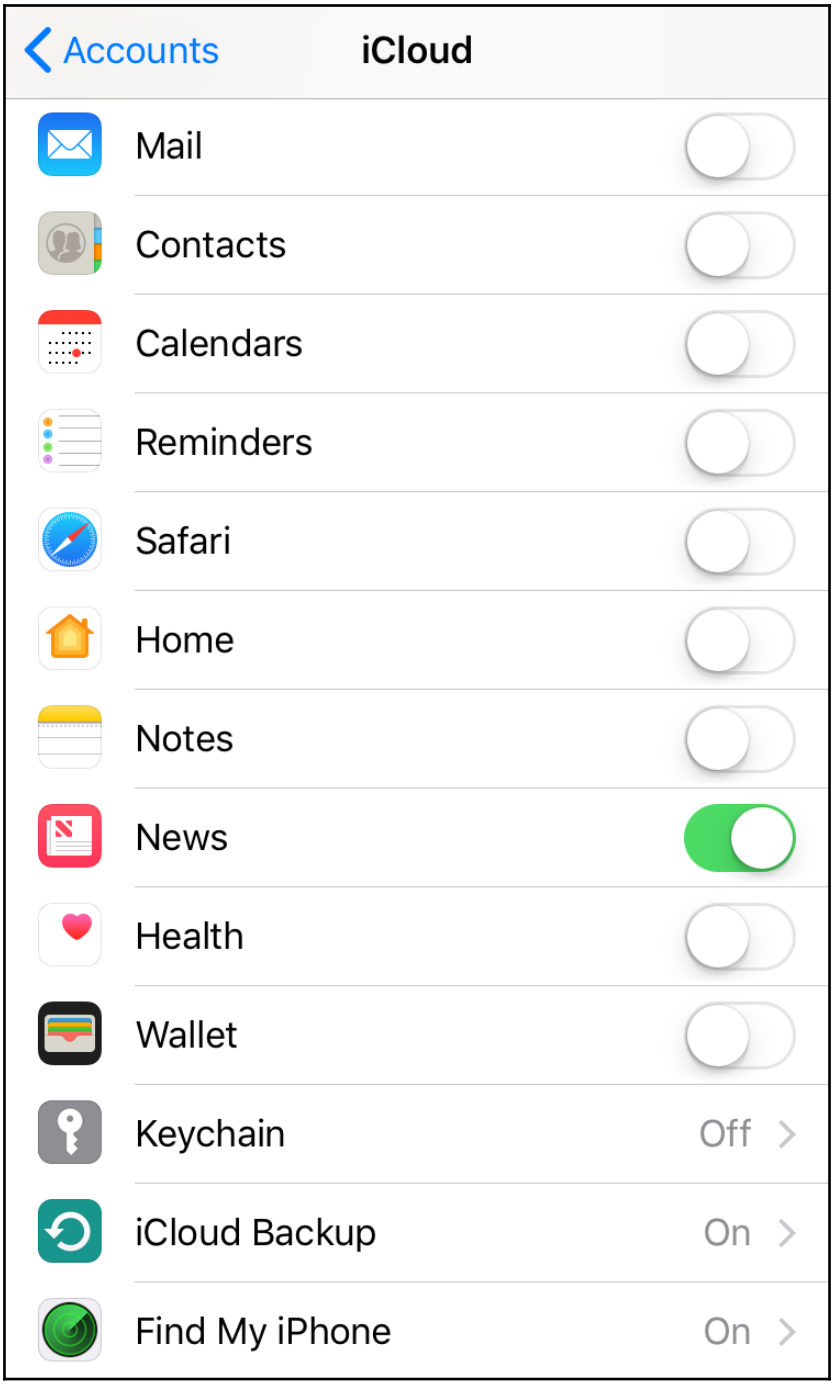

Raw Databases
Close
Device Backup Status and File Structure
Reveal
/Manifest.db
Describes the files and folders within the backup data
Reveal
/Manifest.plist
Describes the contents of the backup data
Reveal
/Info.plist
Describes the status of the backup
Databases Contained in Device Backup
Reveal
/Home/Library/AddressBook/AddressBook.sqlitedb
Address book database
Reveal
/Home/Library/SMS/sms.db
Messages database
Reveal
/Home/Library/Calendar/Calendar.sqlitedb
Calendar database
Reveal
/Home/Library/Notes/notes.sqlite
Notes database
Reveal
/Home/Library/Voicemail/voicemail.db
Voicemail database
Reveal
/Home/Library/CallHistoryDB/CallHistory.storedata
Call History database
Reveal
/Home/Library/Safari/Bookmarks.db
Safari Bookmarks
Reveal
/App/com.apple.mobilesafari/Library/Safari/History.db
Safari History

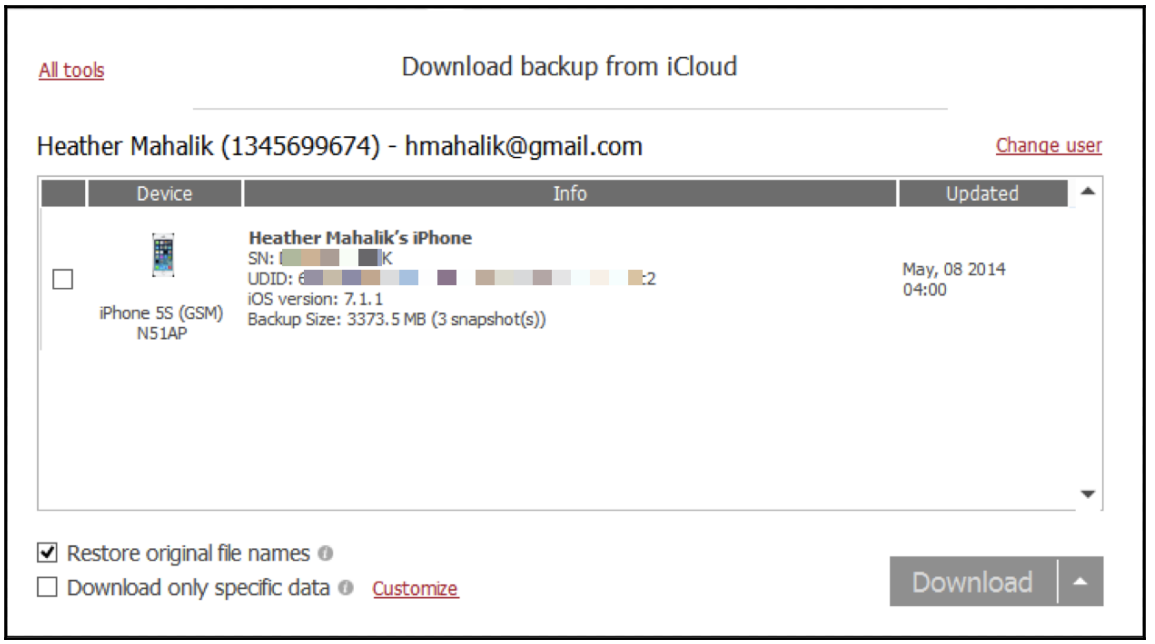

Add Evidence
Attached / Mounted Disks
Show
Files / Folders / Disk Images
Add
Oleg's iPhone
Oleg's iPhone (iOS Backup)
Evidence ID:
Oleg's iPhone - 001
iPhone 6
Phone Number
+7 ...29
OS Version
11.1.2
Product Type
iPhone7,2
Serial Number
C7...N
UDID
4fe...af
IMEI
356...04
ICCID
897...39
Jailbroken
False
Ingestion Options:
Oleg's iPhone
Triage
Custom
All
File Signature Analysis
Picture Analysis
Video Analysis
Calculate Hashes
Identify Known Files
File Carving
Advanced Options
Comprehensive analysis runs many resource intensive tasks at once. Processing may take longer and may adversely affect system performance.
No Templates
Refresh
Remove
1 of 1 selected
Cancel
Start

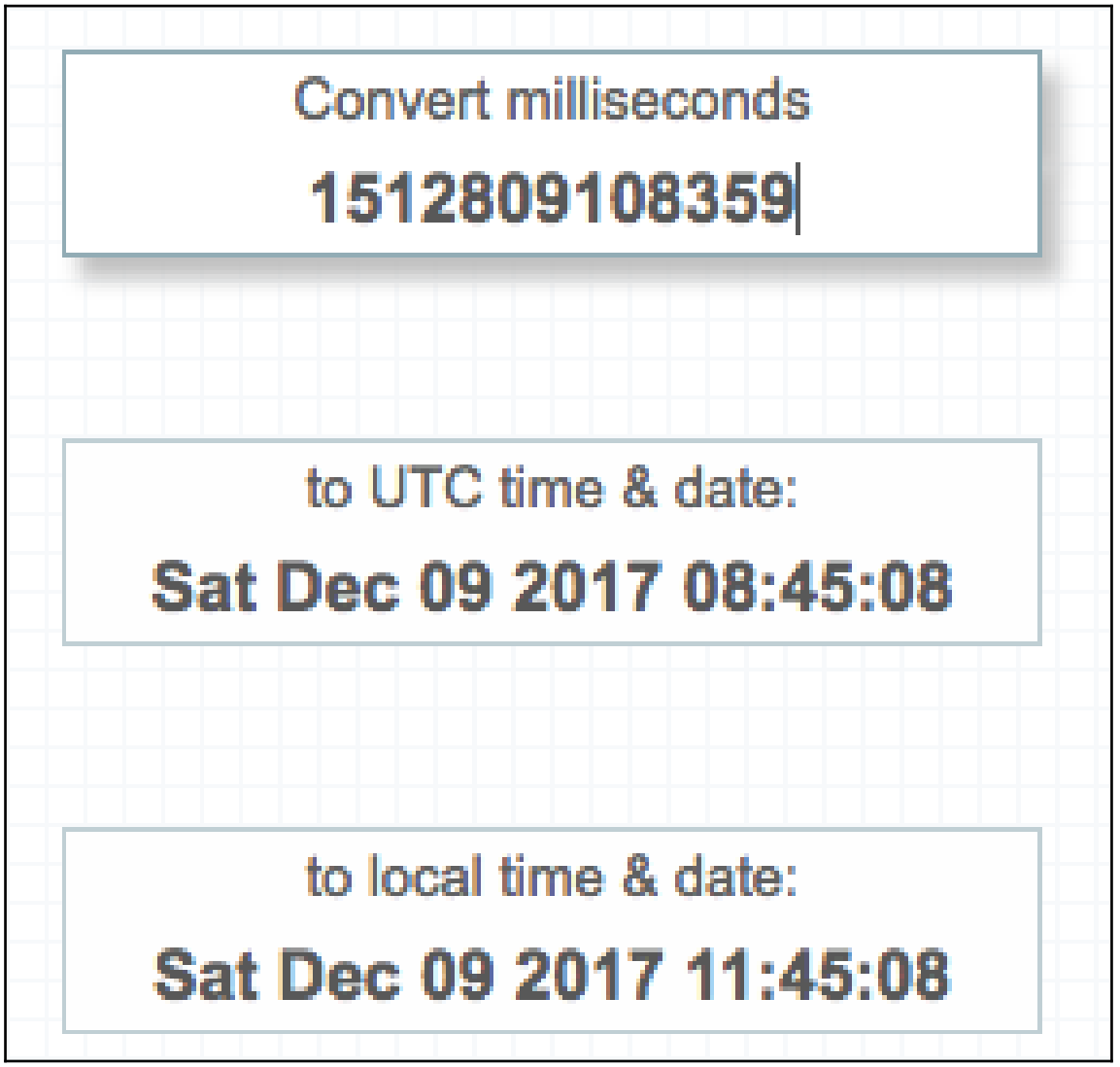

Artifacts
Movies
171
Graphics
7327
Emails
0
Documents
1012
Disk Images
0
Archives
1
1
10
100
1000
10000
100000
Messages
14597
Apps
141
Browser
1226
Notes
125
Contacts
298
Events
54
VoiceMail
0
Calls
350
1
10
100
1000
10000
100000

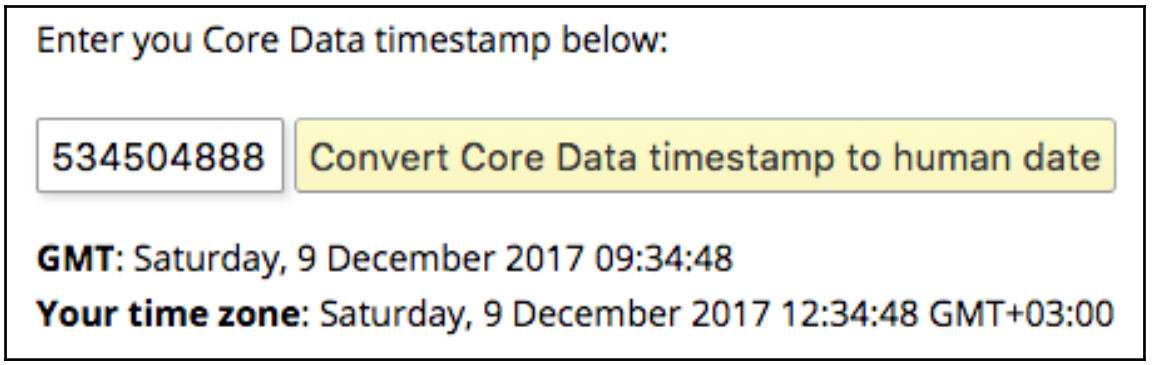

Elcomsoft Phone Breaker
Password Recovery Wizard
Tools
BlackBerry
Apple
Microsoft
Decrypt backup
With known password
Decrypt FileVault disk
With known AppleId
Explore keychain
iTunes, iCloud
Extract authentication token
Non-live Windows operating system
Download from iCloud:
Backups
Files
Photos
Synced data
Keychain

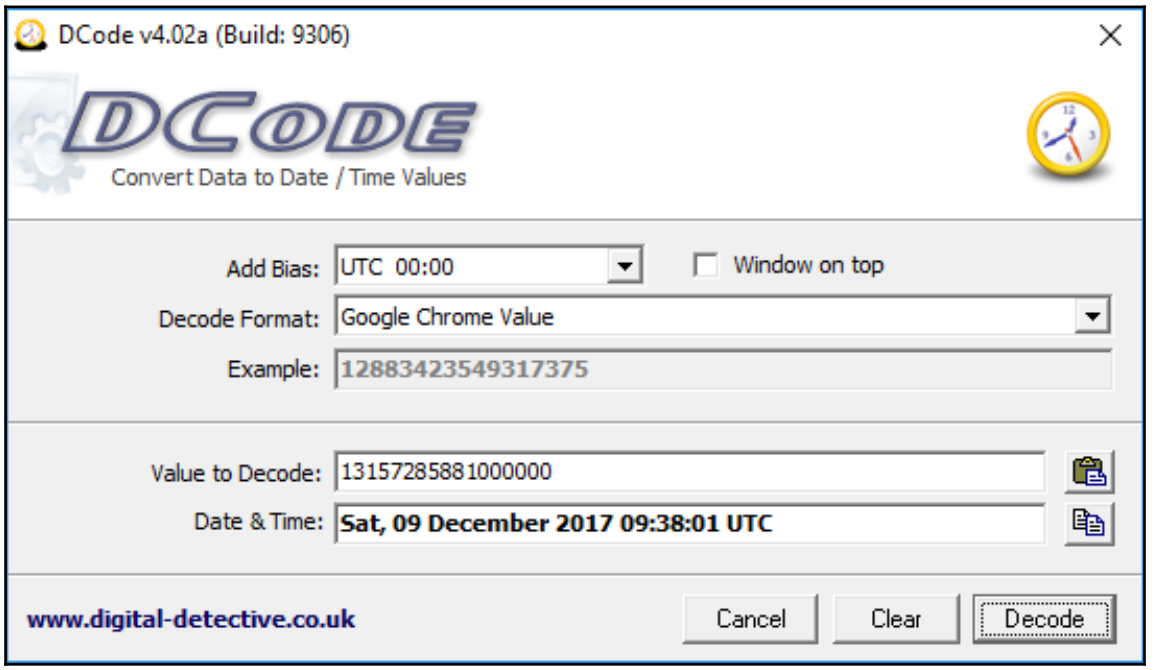

Elcomsoft Phone Breaker
Password Recovery Wizard
Tools
Processing recovery
Backup - C:\Users\0136\AppD ... a557267b3af\Manifest.plist
Change backup
Dictionary Attack
Finished
Brute-Force Attack
0%
Time left – 0h:0m
Current password – 000
More info
Template
Save state...
Stop
Pause


Accounts
iCloud
Mail
Contacts
Calendars
Reminders
Safari
Home
Notes
News
Health
Wallet
Keychain
Off
iCloud Backup
On
Find My iPhone
On


All tools
Download backup from iCloud
Heather Mahalik (1345699674) - hmahalik@gmail.com
Change user
Device
Info
Updated
Heather Mahalik's iPhone
SN:
UDID:
iOS version: 7.1.1
Backup Size: 3373.5 MB (3 snapshot(s))
iPhone 5S (GSM)
N51AP
May, 08 2014
04:00
Restore original file names
Download only specific data
Customize
Download

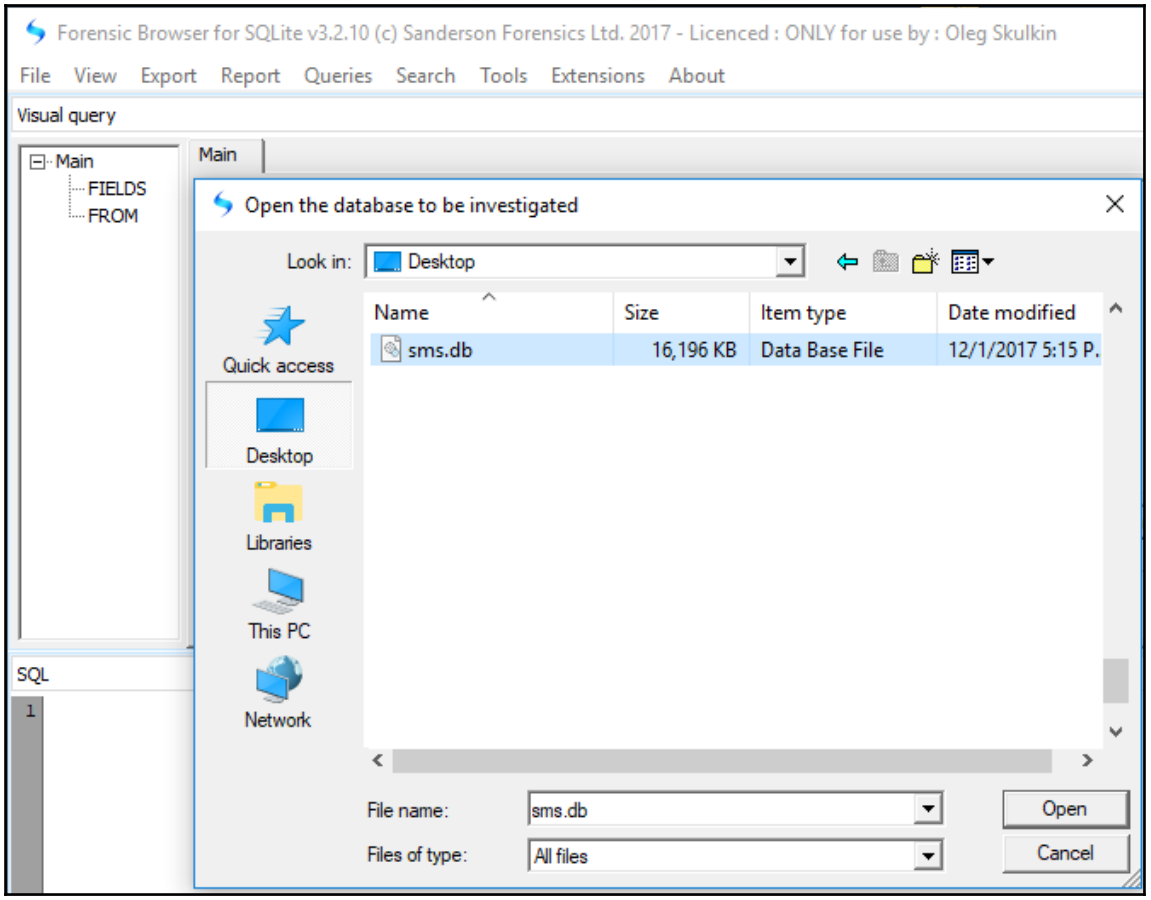

Convert milliseconds
1512809108359
to UTC time & date:
Sat Dec 09 2017 08:45:08
to local time & date:
Sat Dec 09 2017 11:45:08

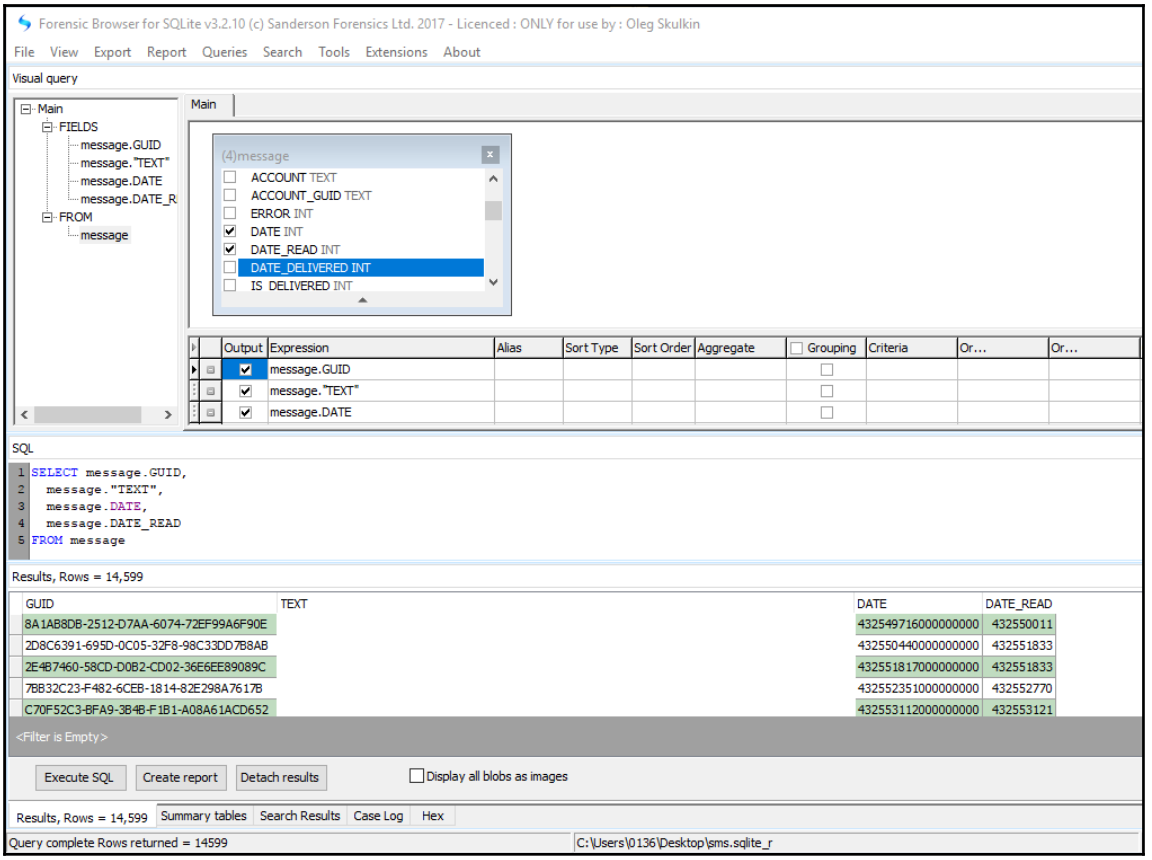

Enter you Core Data timestamp below:
534504888
Convert Core Data timestamp to human date
GMT: Saturday, 9 December 2017 09:34:48
Your time zone: Saturday, 9 December 2017 12:34:48 GMT+03:00

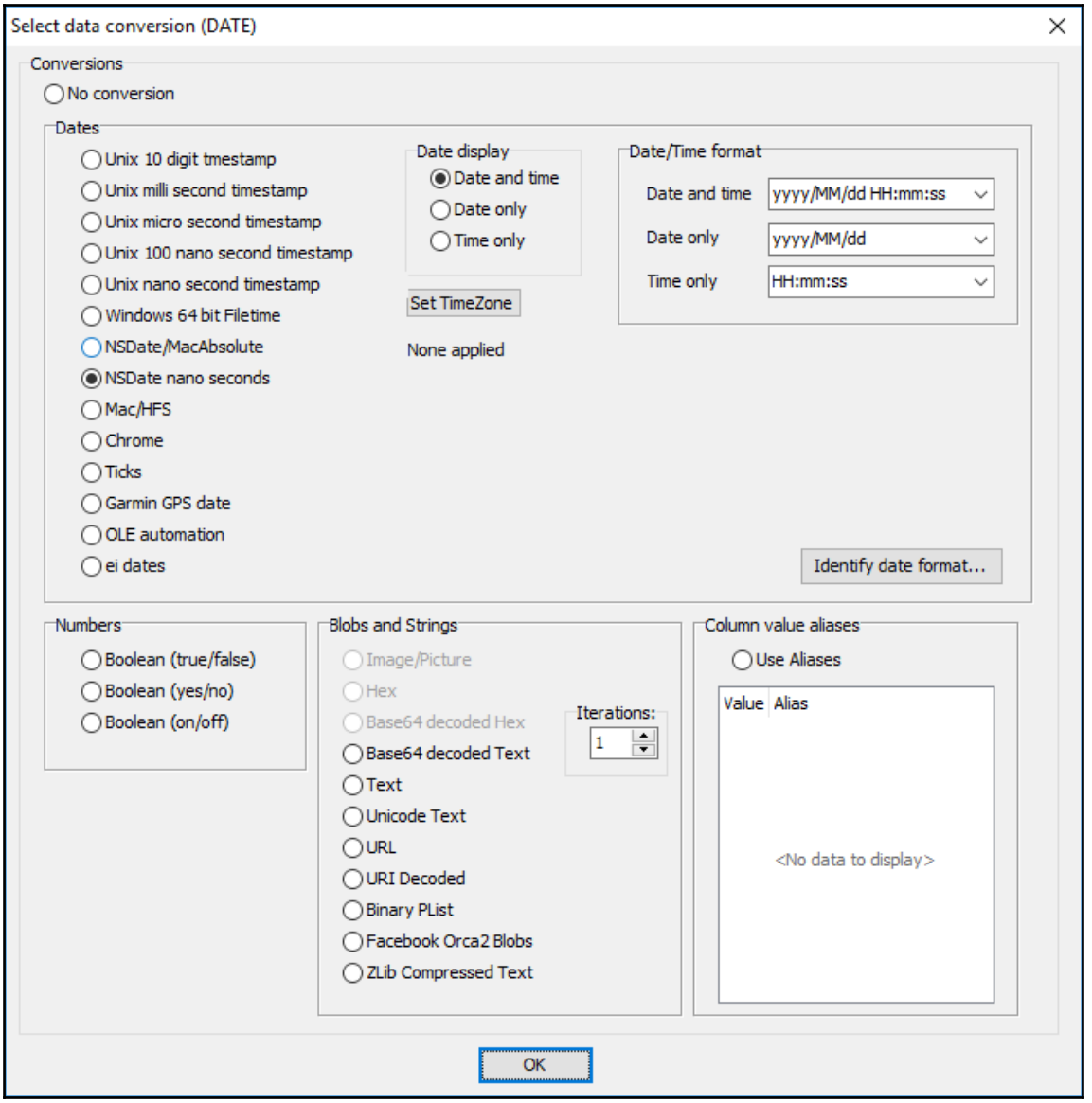

DCode v4.02a (Build: 9306)
DCODE
Convert Data to Date / Time Values
Add Bias:
UTC 00:00
Window on top
Decode Format:
Google Chrome Value
Example:
12883423549317375
Value to Decode:
13157285881000000
Date & Time:
Sat, 09 December 2017 09:38:01 UTC
www.digital-detective.co.uk
Cancel
Clear
Decode

```
sqlite> .tables
_SqliteDatabaseProperties  kvtable
attachment                 message
chat                       message_attachment_join
chat_handle_join           message_processing_task
chat_message_join          sync_deleted_attachments
deleted_messages           sync_deleted_chats
handle                     sync_deleted_messages
```

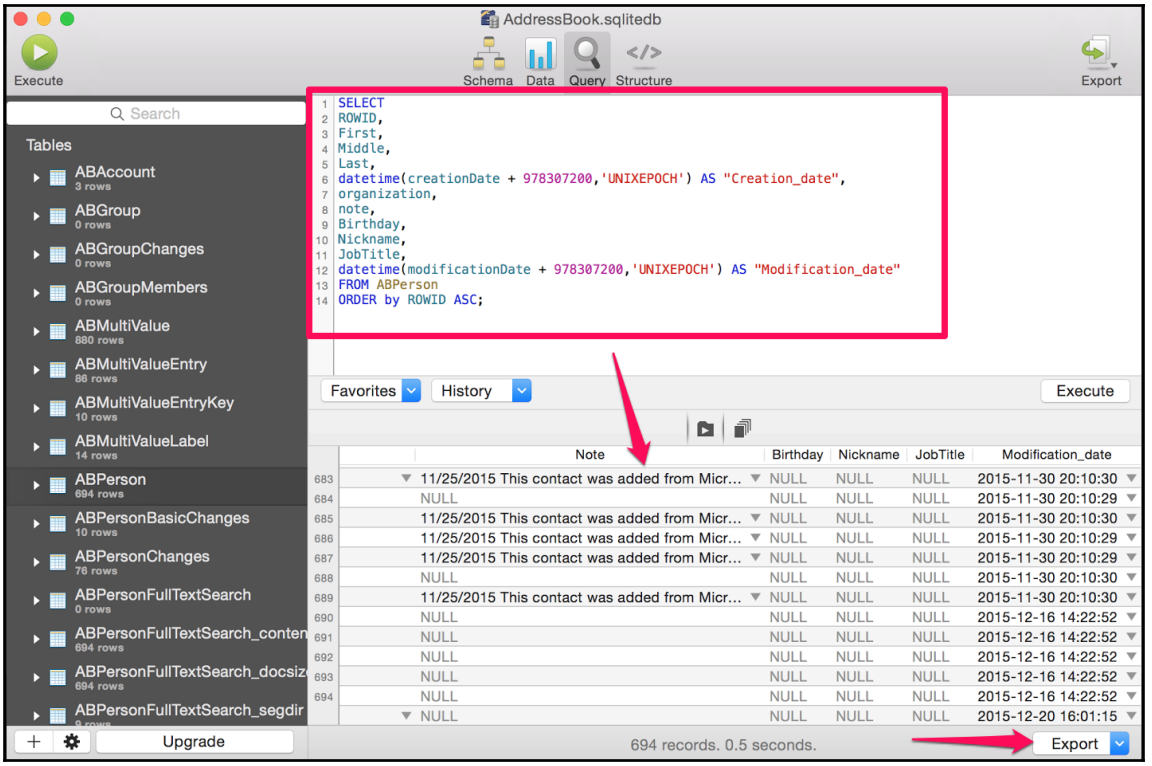
```
sqlite> .dump deleted_messages
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
CREATE TABLE deleted_messages (ROWID INTEGER PRIMARY KEY AUTOINCREMENT UNIQUE,
 guid TEXT NOT NULL);
COMMIT;
```


Forensic Browser for SQLite v3.2.10 (c) Sanderson Forensics Ltd. 2017 - Licenced : ONLY for use by : Oleg Skulkin
File View Export Report Queries Search Tools Extensions About
Visual query
Main
FIELDS
FROM
Main
Open the database to be investigated
Look in: Desktop
Quick access
Desktop
Libraries
This PC
Network
Name
Size
Item type
Date modified
sms.db
16,196 KB
Data Base File
12/1/2017 5:15 P.
File name: sms.db
Files of type: All files
Open
Cancel
SQL
1

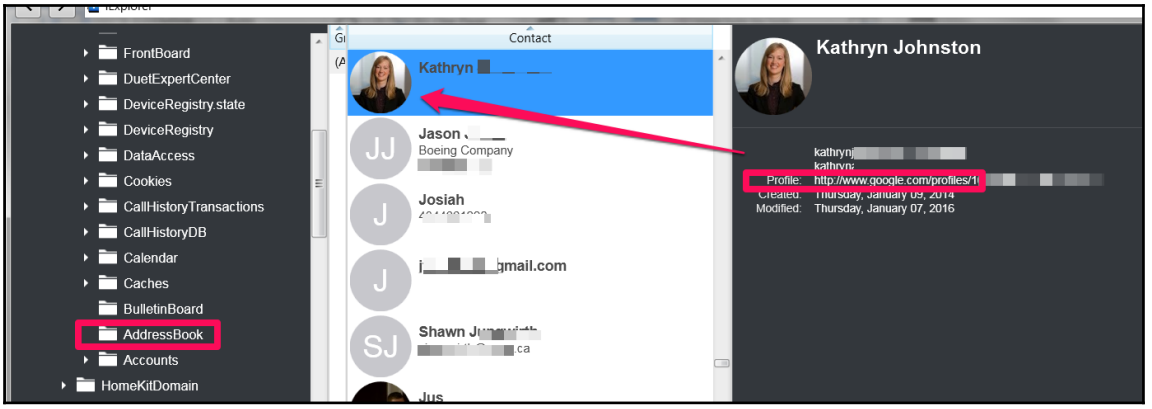

Forensic Browser for SQLite v3.2.10 (c) Sanderson Forensics Ltd. 2017 - Licenced : ONLY for use by : Oleg Skulkin
File View Export Report Queries Search Tools Extensions About
Visual query
Main
FIELDS
message.GUID
message."TEXT"
message.DATE
message.DATE_R
FROM
message
Main
(4)message
ACCOUNT TEXT
ACCOUNT_GUID TEXT
ERROR INT
DATE INT
DATE_READ INT
DATE_DELIVERED INT
IS_DELIVERED INT
Output Expression Alias Sort Type Sort Order Aggregate Grouping Criteria Or... Or...
message.GUID
message."TEXT"
message.DATE
SQL
SELECT message.GUID,
message."TEXT",
message.DATE,
message.DATE_READ
FROM message
Results, Rows = 14,599
GUID TEXT DATE DATE_READ
8A1AB8DB-2512-D7AA-6074-72EF99A6F90E 432549716000000000 432550011
2D8C6391-695D-0C05-32F8-98C33DD7B8AB 432550440000000000 432551833
2E4B7460-58CD-D0B2-CD02-36E6EE89089C 432551817000000000 432551833
7BB32C23-F482-6CEB-1814-82E298A7617B 432552351000000000 432552770
C70F52C3-BFA9-3B4B-F1B1-A08A61ACD652 432553112000000000 432553121
<Filter is Empty>
Execute SQL
Create report
Detach results
Display all blobs as images
Results, Rows = 14,599
Summary tables
Search Results
Case Log
Hex
Query complete Rows returned = 14599
C:\Users\0136\Desktop\sms.sqlite_r

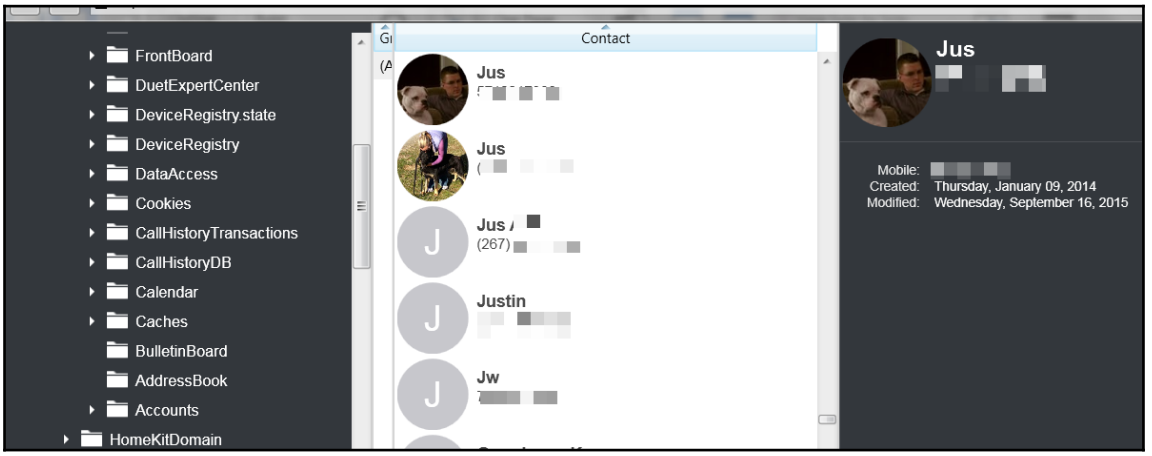

Select data conversion (DATE)
Conversions
No conversion
Dates
Unix 10 digit tmestamp
Unix milli second timestamp
Unix micro second timestamp
Unix 100 nano second timestamp
Unix nano second timestamp
Windows 64 bit Filetime
NSDate/MacAbsolute
NSDate nano seconds
Mac/HFS
Chrome
Ticks
Garmin GPS date
OLE automation
ei dates
Date display
Date and time
Date only
Time only
Set TimeZone
None applied
Date/Time format
Date and time
yyyy/MM/dd HH:mm:ss
Date only
yyyy/MM/dd
Time only
HH:mm:ss
Identify date format...
Numbers
Boolean (true/false)
Boolean (yes/no)
Boolean (on/off)
Blobs and Strings
Image/Picture
Hex
Base64 decoded Hex
Base64 decoded Text
Text
Unicode Text
URL
URI Decoded
Binary PList
Facebook Orca2 Blobs
ZLib Compressed Text
Iterations:
1
Column value aliases
Use Aliases
Value
Alias
<No data to display>
OK

DATE	DATE_READ	DATE_DELIVERED
2012/09/04 05:22:26	2012/09/04 05:22:26	2012/09/04 05:22:26
2012/09/04 05:22:47	2012/09/04 05:22:47	2012/09/04 05:22:47
2012/09/04 05:23:42	2012/09/04 05:23:42	2012/09/04 05:23:42
2012/09/04 14:04:34	2012/09/04 14:04:34	2012/09/04 14:04:34
2012/09/04 16:04:19	2012/09/04 16:04:19	2012/09/04 16:04:19
2012/09/04 16:05:37	2012/09/04 16:05:37	2012/09/04 16:05:37
2012/09/04 16:09:31	2012/09/04 16:09:31	2012/09/04 16:09:31
2012/09/04 16:15:11	2012/09/04 16:15:11	2012/09/04 16:15:11
2012/09/05 04:30:26	2012/09/05 04:30:26	2012/09/05 04:30:26
2012/09/05 08:45:37	2012/09/05 08:45:37	2012/09/05 08:45:37



ROWID	First	Middle	Last	Creation_date	Organization	Note	Nickname	Modification_date
2	Dad	<null>	<null>	2012-06-24 22:58:14	<null>	<HTCData><Favorite>actionid:	<null>	2015-09-16 23:32:56
3	Andy	<null>	<null>	2012-06-24 22:58:14	SANS Singapore	<null>	<null>	2015-09-16 23:32:56
4	Heather	<null>	Mahalik	2012-06-24 22:58:14	<null>	<null>	Hank	2015-09-16 23:32:56
5	Lee	<null>	<null>	2012-06-24 22:58:14	<null>	<null>	<null>	2015-09-16 23:32:56
6	Hayes	<null>	<null>	2012-06-24 22:58:14	<null>	<null>	<null>	2015-09-16 23:32:56
7	Tabs	<null>	<null>	2012-06-24 22:58:14	<null>	<null>	<null>	2015-09-16 23:32:56
8	Jus	<null>	<null>	2012-06-24 22:58:12	<null>	<HTCData><Favorite>actionid:	<null>	2015-09-16 23:32:56
9	Suresh	<null>	<null>	2012-06-24 22:58:14	<null>	<null>	<null>	2015-09-16 23:32:56
10	New	<null>	<null>	2012-06-24 22:58:14	<null>	<null>	<null>	2015-09-16 23:32:56
11	Crogs	<null>	<null>	2012-06-24 22:58:14	<null>	<HTCData><Favorite>actionid:	<null>	2015-09-16 23:32:56
13	Rach	<null>	<null>	2012-06-25 15:55:31	<null>	<null>	<null>	2015-09-16 23:32:56
14	Hardcopy	<null>	<null>	2012-06-25 15:55:31	<null>	<null>	<null>	2015-09-16 23:32:56






```
1  select
2  datetime(ZDATE+978307200, 'UNIXEPOCH','localtime') as "Date",
3  ZDURATION AS "Duration",
4  ZLOCATION AS "Location of device phone number",
5  ZADDRESS AS "Phone number",
6  ZSERVICE_PROVIDER AS "Service provider"
7  FROM ZCALLRECORD
```

	Date	Duration	Location of device phone number	Phone number	Service provider
218	2017-11-24 21:55:03	2794.40141099691	Russia	233	G3U8SN86TG.co.froute.sessiontalklite
219	2017-11-25 14:40:36	18.7899500131607	Russia	+7915	com.apple.Telephony
220	2017-11-25 20:28:05	908.81374502182	Russia	+7918	com.apple.Telephony
221	2017-11-26 20:12:43	420.571035027504	Russia	+7918	com.apple.Telephony

221 rows returned in 2ms from: select
datetime(ZDATE+978307200, 'UNIXEPOCH','localtime') as "Date",
ZDURATION AS "Duration",
ZLOCATION AS "Location of device phone number",
ZADDRESS AS "Phone number",

```
1  select
2  datetime(message .date/1000000000 + 978307200, 'UNIXEPOCH', 'localtime') AS "Date",
3  message .text AS "Message",
4  message .service AS "Service",
5  message .is_from_me AS "1-Sent, 0-Incoming",
6  datetime(message .date_read+978307200, 'UNIXEPOCH', 'localtime') AS "Date read",
7  handle .id AS "Phone number"
8  FROM message, handle
9  WHERE handle .ROWID = message .handle_id
```

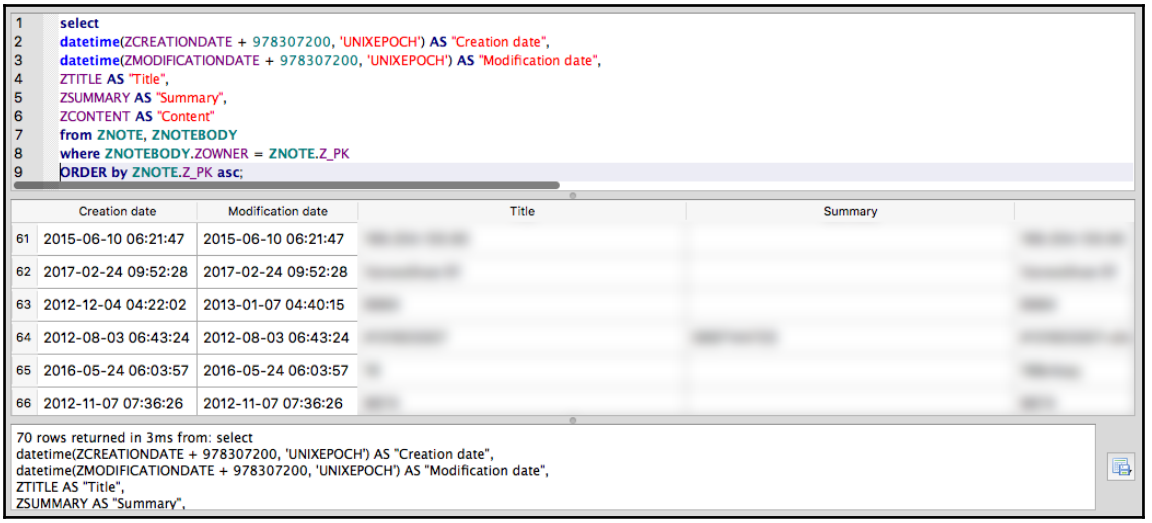
	Date	Message	Service	1-Sent, 0-Incoming	Date read	Phone number
14571	2017-11-26 14:08:14	[redacted]	SMS	0	2017-11-26 14:27:50	mtc
14572	2017-11-26 16:40:56	[redacted]	SMS	0	2017-11-26 16:41:19	smexpress
14573	2017-11-26 17:21:16	[redacted]	SMS	0	2017-11-26 17:21:26	mailru

```
14573 rows returned in 127ms from: select
datetime(message .date/1000000000 + 978307200, 'UNIXEPOCH', 'localtime') AS "Date",
message .text AS "Message",
message .service AS "Service",
message .is_from_me AS "1-Sent, 0-Incoming",
datetime(message .date_read+978307200, 'UNIXEPOCH', 'localtime') AS "Date read",
handle .id AS "Phone number"
FROM message, handle
WHERE handle .ROWID = message .handle_id
```

```
1  select
2  ROWID,
3  summary AS "Summary",
4  datetime(start_date + 978307200, 'UNIXEPOCH') AS "Start time",
5  datetime(end_date + 978307200, 'UNIXEPOCH') AS "End time"
6  FROM CalendarItem
7
```

	ROWID	Summary	Start time	End time
2	10	Veterans Day (observed)	2017-11-10 00:00:00	2017-11-10 23:59:59
3	21	Tax Day	2019-04-15 00:00:00	2019-04-15 23:59:59
4	30	Independence Day (observed)	2015-07-03 00:00:00	2015-07-03 23:59:59
5	48	Tax Day	2020-04-15 00:00:00	2020-04-15 23:59:59
6	50	Easter	2018-04-01 00:00:00	2018-04-01 23:59:59
7	58	Tax Day	2018-04-17 00:00:00	2018-04-17 23:59:59

```
52 rows returned in 4ms from: select
ROWID,
summary AS "Summary",
datetime(start_date + 978307200, 'UNIXEPOCH') AS "Start time",
datetime(end_date + 978307200, 'UNIXEPOCH') AS "End time"
FROM CalendarItem
```



```
select
datetime(ZCREATIONDATE + 978307200, 'UNIXEPOCH') AS "Creation date",
datetime(ZMODIFICATIONDATE + 978307200, 'UNIXEPOCH') AS "Modification date",
ZTITLE AS "Title",
ZSUMMARY AS "Summary",
ZCONTENT AS "Content"
from ZNOTE, ZNOTEBODY
where ZNOTEBODY.ZOWNER = ZNOTE.Z_PK
ORDER by ZNOTE.Z_PK asc;
```

	Creation date	Modification date	Title	Summary	
61	2015-06-10 06:21:47	2015-06-10 06:21:47	[redacted]		[redacted]
62	2017-02-24 09:52:28	2017-02-24 09:52:28	[redacted]		[redacted]
63	2012-12-04 04:22:02	2013-01-07 04:40:15	[redacted]		[redacted]
64	2012-08-03 06:43:24	2012-08-03 06:43:24	[redacted]	[redacted]	[redacted]
65	2016-05-24 06:03:57	2016-05-24 06:03:57	[redacted]		[redacted]
66	2012-11-07 07:36:26	2012-11-07 07:36:26	[redacted]		[redacted]

70 rows returned in 3ms from: select
datetime(ZCREATIONDATE + 978307200, 'UNIXEPOCH') AS "Creation date",
datetime(ZMODIFICATIONDATE + 978307200, 'UNIXEPOCH') AS "Modification date",
ZTITLE AS "Title",
ZSUMMARY AS "Summary",

```
mbp-hmahalik:Webkit hmahalik$ cd /Users/
hmahalik/Desktop/Webkit/LocalStorage
mbp-hmahalik:LocalStorage hmahalik$ ls
StorageTracker.db
http_www.google.com_0.localstorage
http_m.youtube.com_0.localstorage
http_www.youtube.com_0.localstorage
http_www.bing.com_0.localstorage
https_m.facebook.com_0.localstorage
mbp-hmahalik:LocalStorage hmahalik$
```

```
1  select
2  Z_PK,
3  datetime(ZDATECREATED + 978307200, 'UNIXEPOCH') AS "Created date",
4  datetime(ZMODIFICATIONDATE + 978307200, 'UNIXEPOCH') AS "Modified date",
5  datetime(ZTRASHEDDATE + 978307200, 'UNIXEPOCH') AS "Deleted date",
6  ZFILENAME AS "File name",
7  ZDIRECTORY AS "Directory",
8  ZWIDTH AS "Width",
9  ZHEIGHT AS "Height"
10 from ZGENERICASSET
11 order by Z_PK asc;
```

	Z_PK	Created date	Modified date	Deleted date	File name	Directory	Width	Height
874	2588	2017-11-12 07:04:04	2017-11-12 07:04:38	2017-11-12 07:04:38	IMG_2469.PNG	DCIM/102APPLE	750	1334
875	2589	2017-11-12 09:17:33	2017-11-12 18:26:16	NULL	IMG_2470.PNG	DCIM/102APPLE	750	1334
876	2590	2017-11-12 09:19:48	2017-11-12 09:19:48	NULL	IMG_2471.PNG	DCIM/102APPLE	750	1334
877	2591	2017-11-12 09:21:20	2017-11-12 18:26:16	NULL	IMG_2472.PNG	DCIM/102APPLE	750	1334
878	2592	2017-11-12 09:29:39	2017-11-12 18:26:16	NULL	IMG_2473.PNG	DCIM/102APPLE	750	1334

909 rows returned in 14ms from: select
Z_PK,
datetime(ZDATECREATED + 978307200, 'UNIXEPOCH') AS "Created date",
datetime(ZMODIFICATIONDATE + 978307200, 'UNIXEPOCH') AS "Modified date",
datetime(ZTRASHEDDATE + 978307200, 'UNIXEPOCH') AS "Deleted date",

Table: CompassCalibration

New Record | Delete Record

	Timestamp	MagneticX	MagneticY	MagneticZ	BiasX	BiasY	BiasZ	Level	Magnitude	Inclination
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	530275657.23...	18.090557098...	-13.98195648...	-33.90044403...	2.2520384788...	223.79827880...	-509.6311340...	3	40.890136718...	61.850692749...
2	529663736.29...	-9.014245033...	-18.66546630...	-34.38824844...	8.0672769546...	230.03048706...	-514.8070068...	3	40.152305603...	59.025756835...
3	530279208.63...	-45.12598037...	-17.03365516...	5.1629896163...	3.2767469882...	229.46755981...	-507.9128417...	4	48.509346008...	67.295646667...
4	529664175.42...	-13.64353084...	26.826248168...	-33.26204681...	-2.808065891...	225.98017883...	-505.7385559...	3	44.857067108...	61.501331329...
5	530296916.29...	8.2853183746...	8.4065904617...	-38.08319854...	-2.978725433...	227.92864990...	-506.4470214...	4	39.870372772...	51.139644622...
6	529672686.24...	-10.57118701...	-18.89097213...	-29.98459815...	1.5486146211...	225.21925354...	-507.0631408...	5	38.908626556...	63.084144592...
7	529866180.19...	-23.69696617...	-44.01729583...	-17.87157630...	-0.996582269...	231.09046936...	-506.0693664...	3	53.089195251...	68.721229553...
8	530962810.20...	-37.53378677...	-0.108085155...	-35.82220077...	0.0833697319...	230.46879577...	-510.2182617...	3	51.884754180...	57.254608154...
9	533314443.26...	-16.86403083...	-10.68627357...	-39.08018493...	-4.368422508...	225.35885620...	-510.1470031...	3	43.884532928...	67.942825317...
10	529663909.41...	12.833063125...	6.4886217117...	-37.27674865...	4.3199834823...	222.62437438...	-511.2269592...	3	39.954288482...	52.033946990...
11	533315268.93...	5.9609537124...	7.4855556488...	-41.08742904...	0.3423299789...	220.23406982...	-517.9874267...	3	42.187007904...	50.402549743...
12	529485577.67...	-17.69032287...	-25.68327522...	-35.55134582...	2.7818639278...	225.48196411...	-511.0164489...	3	47.291385650...	63.812435150...
13	532094835.48...	49.148548126...	-2.630333900...	-11.58797264...	0.7436568737...	226.71675109...	-510.7829895...	4	50.564594268...	48.636138916...
14	529927299.39...	30.233861923...	-12.52783775...	-20.19597625...	5.9965066909...	225.64849853...	-510.9455566...	3	38.456604003...	57.42578125
15	529828958.74...	-7.441396713...	-31.84716415...	-13.48861980...	-18.06754684...	233.06649780...	-521.9632568...	3	35.377380371...	49.445316314...
16	530966484.23...	-11.68542194...	2.0740261077...	-41.26337051...	-25.41053199...	237.34243774...	-515.6748046...	3	42.936176300...	59.088871002...
17	530370084.98...	-22.37540817...	-23.32030487...	-34.66993713...	-20.82223510...	234.82601928...	-514.7019653...	4	47.397266387...	57.258068084...
18	530561471.26...	17.658479690...	-34.21964263...	-21.32521438...	-20.95727539...	233.18692016...	-513.2947998...	3	44.017837524...	65.768829345...

1 - 19 of 182 | Go to: 1

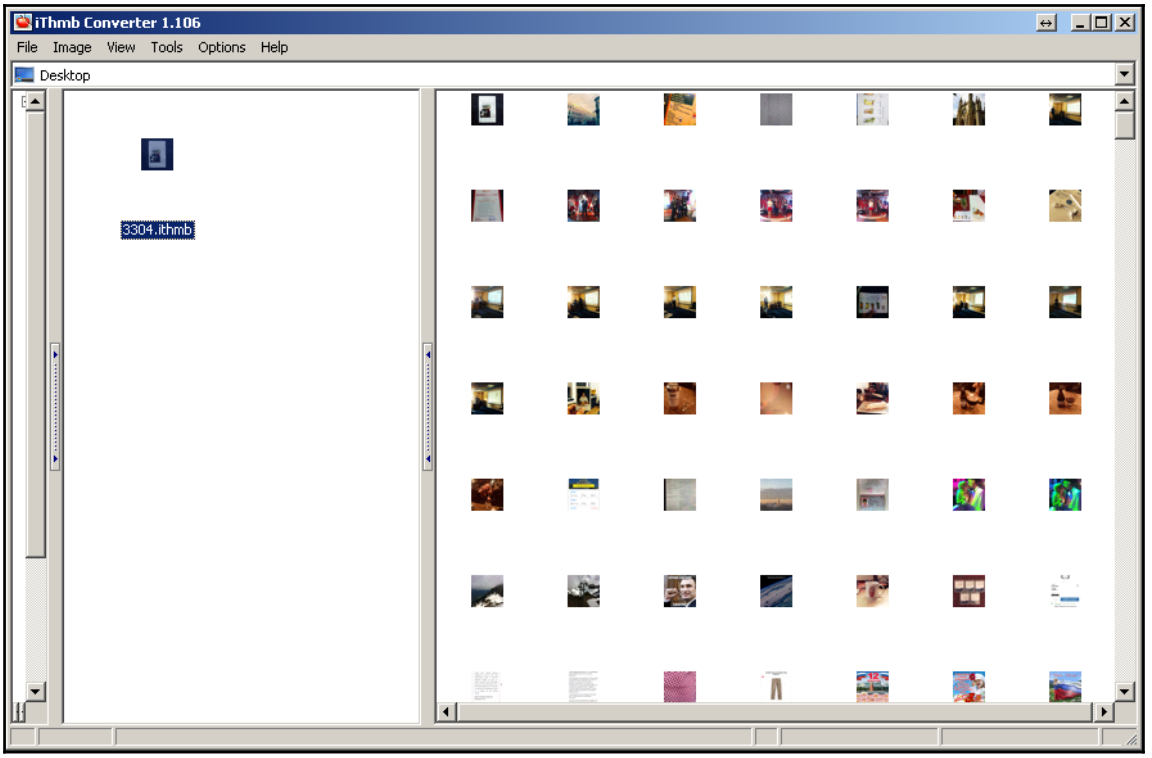
com.apple.Maps.plist

com.apple.Maps.plist 〉 No Selection

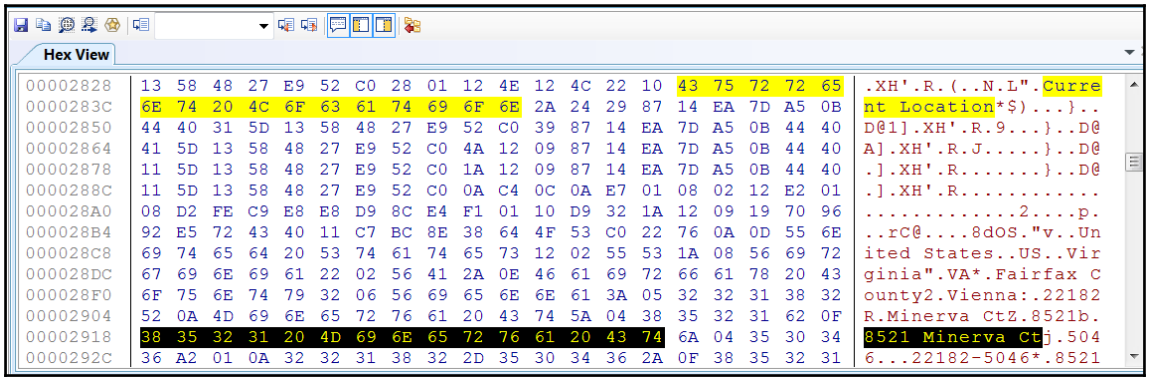
Key	Type	Value
▼ Root	Dictionary	(46 items)
LastSearchExistsKey	Boolean	YES
SearchInfoRegionChangeTimestamp	Number	519 662 334,233445
HasShownWalkingNavModeAdvisory	Boolean	YES
HasShownNavModeAdvisory	Boolean	YES
SearchRequestWithoutPromptCountKey	Number	28
LastSearchLongitudeKey	Number	30,324402195546
MapsTransportTypePreferenceWasEve...	Boolean	YES
LastAnnouncementsURL	String	https://gspe35-ssl.ls.apple.com/config/announcements?environment=prod&hardware=i
SyncManager.bookmarks.synced	Boolean	YES
__internal__searchBarPlaceholderV2-e...	String	Search for a place or address
SyncManager.recents.synced	Boolean	YES
AnnouncementsLastUpdated	Number	533 409 951,555441
SearchBarCompletionMode	Number	3
▶ DirectionsController	Dictionary	(3 items)
__internal__LastActivityCamera	Data	<09620f83 0991e14b 40114b7e 635f0bd0 42401900 00000000 00008021 00000(
SyncClientRegistrationIdentifier	String	428DB2FC-754A-4C17-82FE-F051E50982AD
LiveTrackingAutoSelectZoomLevelKey	Boolean	YES
RouteEndStringIsAtom	Boolean	YES
▶ LastViewport	Dictionary	(6 items)
RouteEndString	String	1-y Syromyatnicheskiy pereulok 37, Moscow, Russia, 105120
LastViewMode	Number	0
FavoritesBoostDate	Date	5 Oct 2017 at 20:27:44
SearchMode	Number	1
AnnouncementsETag	String	"e3bba42ec87d215eea400c6c41923d5d1ed7b5de"
MapsActivityTimestamp	Date	6 Oct 2017 at 09:48:11
GEOUsageSessionID	Data	<0894abcc 84acaaf2 a0900110 9ca3b2dc d6ecfdd6 4e>

olegskulkin — -bash — 118×24

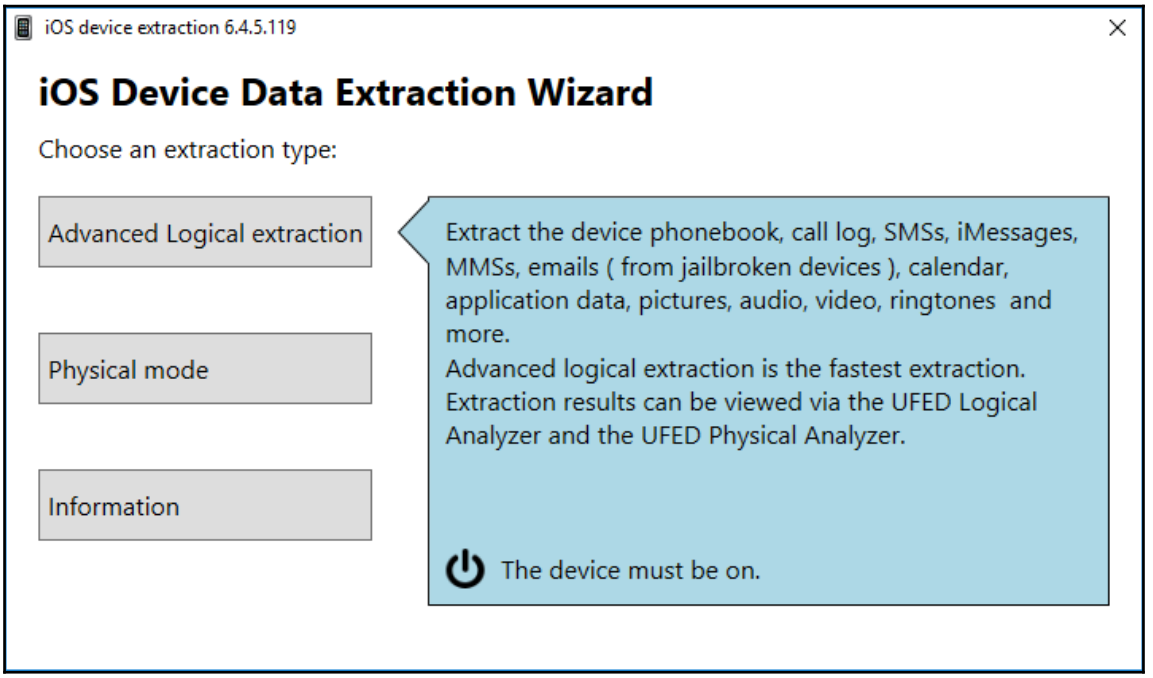
```
Olegs-MacBook-Air:~ olegskulkin$ python BinaryCookieReader.py Cookies.binarycookies
##################################################################################
# BinaryCookieReader: developed by Satishb3: http://www.securitylearn.net #
##################################################################################
Cookie : __atuvc=1%7C21%2C0%7C22%2C0%7C23%2C1%7C24; domain=www.itkkit.ru; path=/; expires=Tue, 11 Jun 2019;
Cookie : rrrbt=; domain=www.itkkit.ru; path=/; expires=Thu, 28 Dec 2017;
Cookie : LocRegionAncestors_5=1%7C324%7C417; domain=.mobile.beeline.ru; path=/; expires=Thu, 27 Jan 2022;
Cookie : LocUserRegion_5=417%7Csochi; domain=.mobile.beeline.ru; path=/; expires=Thu, 27 Jan 2022;
Cookie : BX_USER_ID=e29ddd6d5320089beeee228723d43b54; domain=www.itkkit.com; path=/; expires=Wed, 21 Jul 2027;
Cookie : __atuvc=2%7C30; domain=www.itkkit.com; path=/; expires=Tue, 23 Jul 2019;
Cookie : rrrbt=; domain=www.itkkit.com; path=/; expires=Thu, 08 Feb 2018;
Cookie : __ar_v4=%7CTQSV74R4GVCSJITSZC2MCP%3A20160111%3A1%7CACPJ7LN56VBITNNAUDPDMG%3A20160111%3A1%7CDARDKNAFP5HS5ABHGM
36J3%3A20160111%3A1; domain=.www.darkreading.com; path=/; expires=Sun, 26 Sep 2021;
Cookie : WT_NVR=0=/:1=ru-ru:2=ru-ru/windows7|en-us/windows:3=ru-ru/windows7/products|ru-ru/windows/shop|en-us/windows/
help; domain=.windows.microsoft.com; path=/; expires=Sat, 02 Jul 2022;
Cookie : UniqueID=88d3d2890bf3c839d3ed62c7f4ca3b; domain=www.titus.de; path=/; expires=Sat, 17 Aug 2019; HttpOnly
Cookie : lsn_statp=Kc9DGhQAAABdPkbhrRC5Tw%3D%3D; domain=.linksynergy.com; path=/; expires=Mon, 26 Jan 2032;
Cookie : lsn_track=UmFuZG9tSVZtmaV36aREjwyVO8S1PYpdox6Hh14ZwzUfVqWkY2RO5ccWF4f8KzvDSlWwRh%2FSJVLU7ajjfnT6xQ%3D%3D; dom
ain=.linksynergy.com; path=/; expires=Fri, 28 Jan 2022;
Cookie : _sdsat_Internal/External=internal; domain=club.pokemon.com; path=/; expires=Mon, 01 Jul 2019;
Cookie : _sdsat_Language=en; domain=club.pokemon.com; path=/; expires=Mon, 01 Jul 2019;
Cookie : _sdsat_businessUnit=pcom; domain=club.pokemon.com; path=/; expires=Mon, 01 Jul 2019;
Cookie : django_language=en; domain=club.pokemon.com; path=/; expires=Sun, 01 Jul 2018;
Cookie : visid_incap_1155802=UZmozvjASyC0eVR5Ez90HjgXhlkAAAAAQUIPAAAAAAD4ul57XrhYrR+NSN1a+DpE; domain=.sans.org; path=
```


iThmb Converter 1.106
File Image View Tools Options Help
Desktop
3304.ithmb

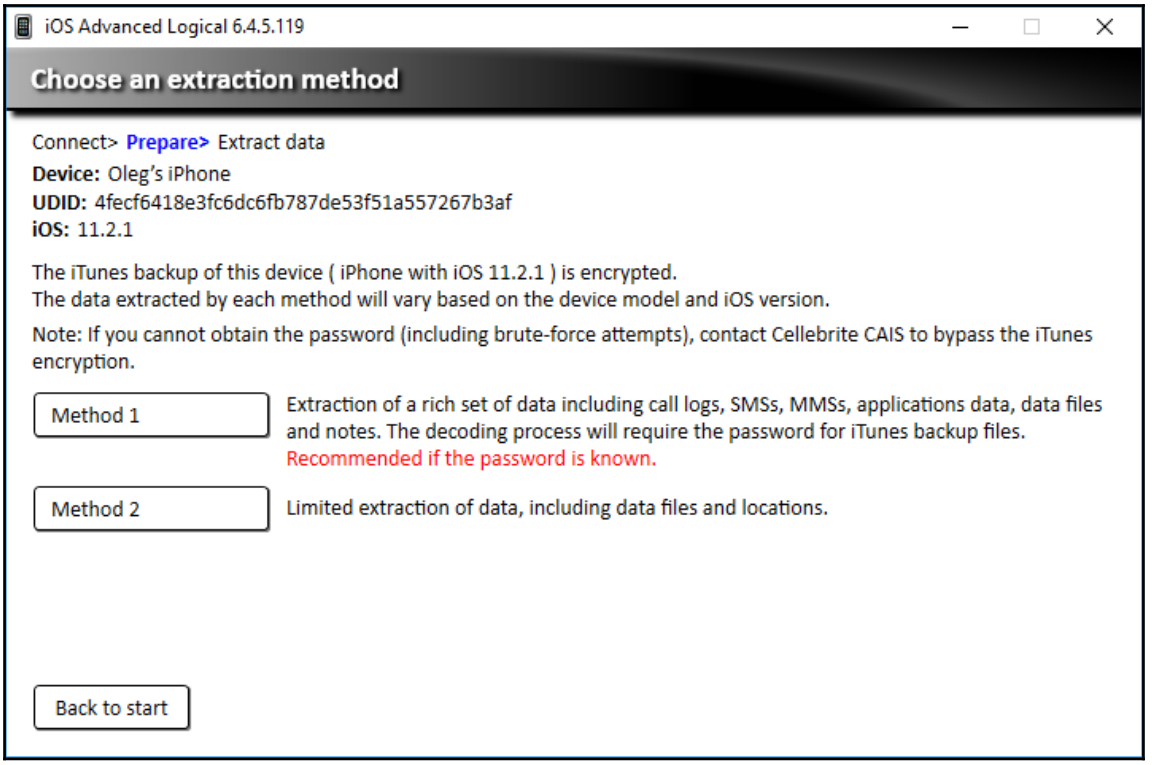

DeviceRegistry (158 files, 2,887 KB)
3FD6F245-558E-4702-87C9-83D51B039FFF (158 files, 2,887 KB)
AddressBook (2 files, 80 KB)
BulletinDistributor (2 files, 20 KB)
com.apple.NanoPhotos (2 files, 1 KB)
com.apple.private.nanoresourcegrabber (13 files, 36 KB)
CompanionSync (24 files, 1,428 KB)
CoreLocation (1 file, 1 KB)
EventKitSync (3 files, 40 KB)
Health (1 file, 44 KB)
NanoAppRegistry (42 files, 98 KB)
NanoMail (1 file, 148 KB)
NanoMaps (2 files, 41 KB)

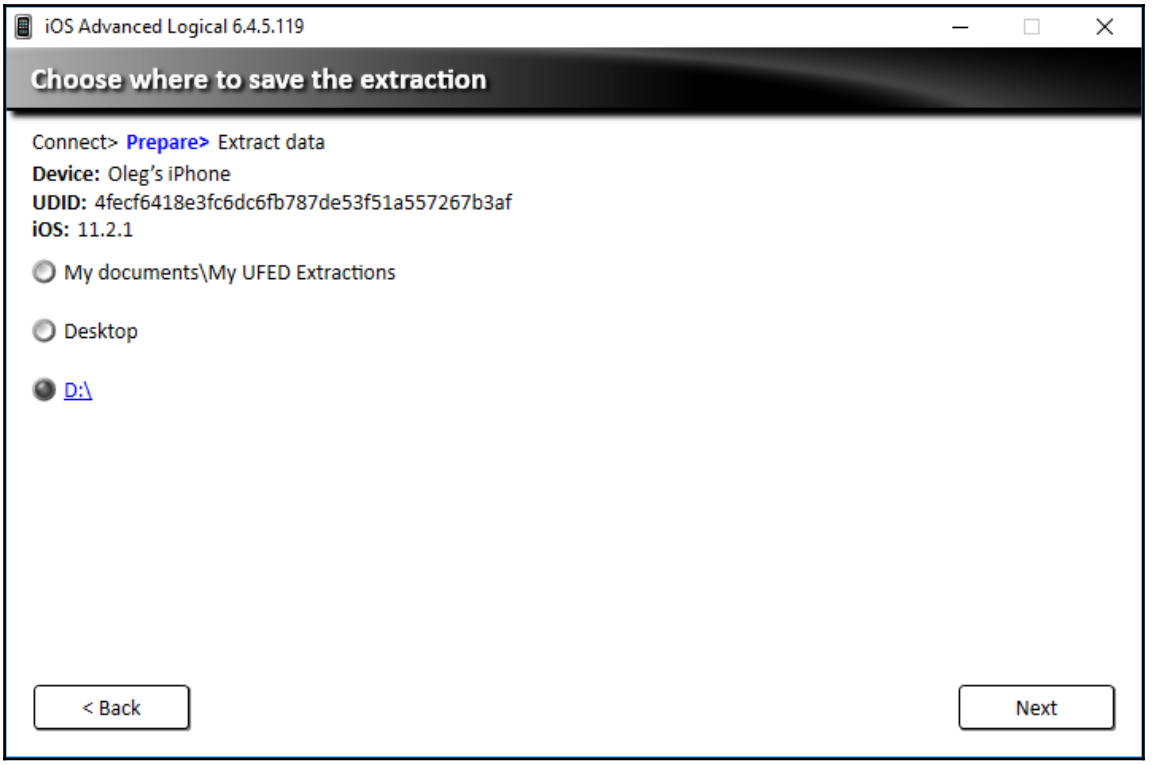

Hex View
00002828 13 58 48 27 E9 52 C0 28 01 12 4E 12 4C 22 10 43 75 72 72 65 .XH'.R.(..N.L".Curre
0000283C 6E 74 20 4C 6F 63 61 74 69 6F 6E 2A 24 29 87 14 EA 7D A5 0B nt Location*$)...}..
00002850 44 40 31 5D 13 58 48 27 E9 52 C0 39 87 14 EA 7D A5 0B 44 40 D@1].XH'.R.9...}..D@
00002864 41 5D 13 58 48 27 E9 52 C0 4A 12 09 87 14 EA 7D A5 0B 44 40 A].XH'.R.J.....}..D@
00002878 11 5D 13 58 48 27 E9 52 C0 1A 12 09 87 14 EA 7D A5 0B 44 40 .].XH'.R.......}..D@
0000288C 11 5D 13 58 48 27 E9 52 C0 0A C4 0C 0A E7 01 08 02 12 E2 01 .].XH'.R.............
000028A0 08 D2 FE C9 E8 E8 D9 8C E4 F1 01 10 D9 32 1A 12 09 19 70 96 ....2....p.
000028B4 92 E5 72 43 40 11 C7 BC 8E 38 64 4F 53 C0 22 76 0A 0D 55 6E ..rC@....8dOS."v..Un
000028C8 69 74 65 64 20 53 74 61 74 65 73 12 02 55 53 1A 08 56 69 72 ited States..US..Vir
000028DC 67 69 6E 69 61 22 02 56 41 2A 0E 46 61 69 72 66 61 78 20 43 ginia".VA*.Fairfax C
000028F0 6F 75 6E 74 79 32 06 56 69 65 6E 6E 61 3A 05 32 32 31 38 32 ounty2.Vienna:.22182
00002904 52 0A 4D 69 6E 65 72 76 61 20 43 74 5A 04 38 35 32 31 62 0F R.Minerva CtZ.8521b.
00002918 38 35 32 31 20 4D 69 6E 65 72 76 61 20 43 74 6A 04 35 30 34 8521 Minerva Ctj.504
0000292C 36 A2 01 0A 32 32 31 38 32 2D 35 30 34 36 2A 0F 38 35 32 31 6...22182-5046*.8521

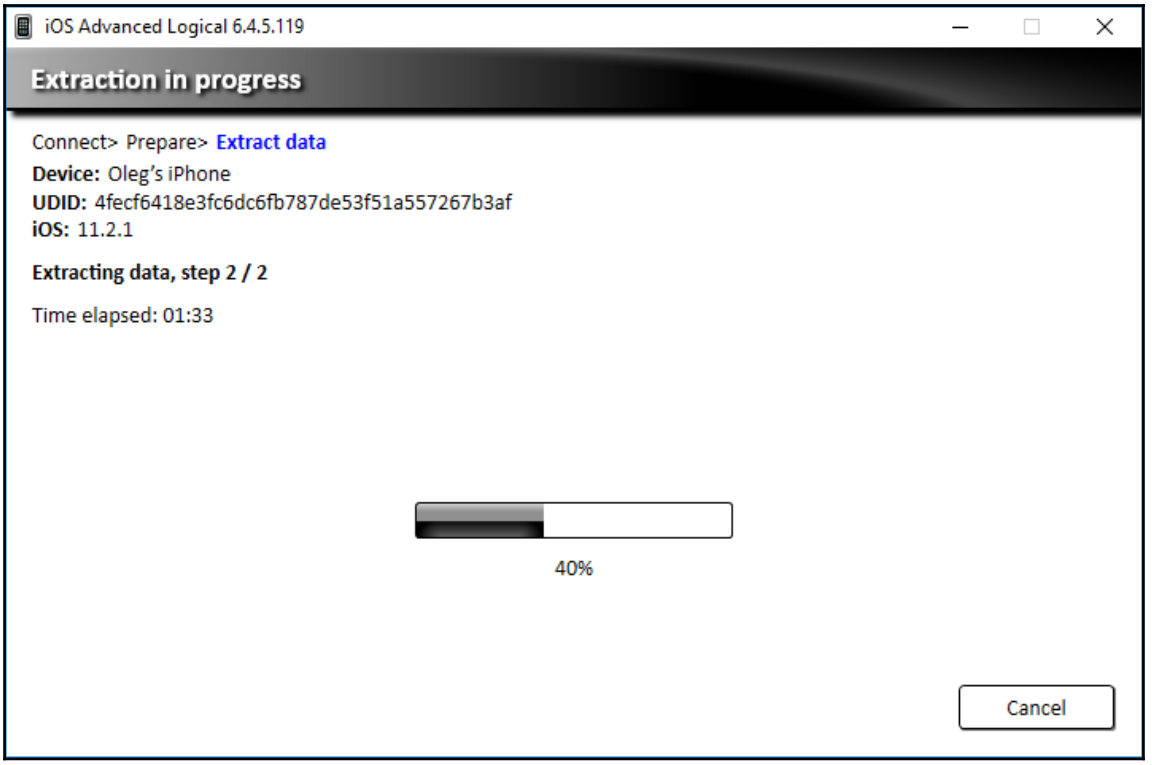
Chapter 6: iOS Forensic Tools

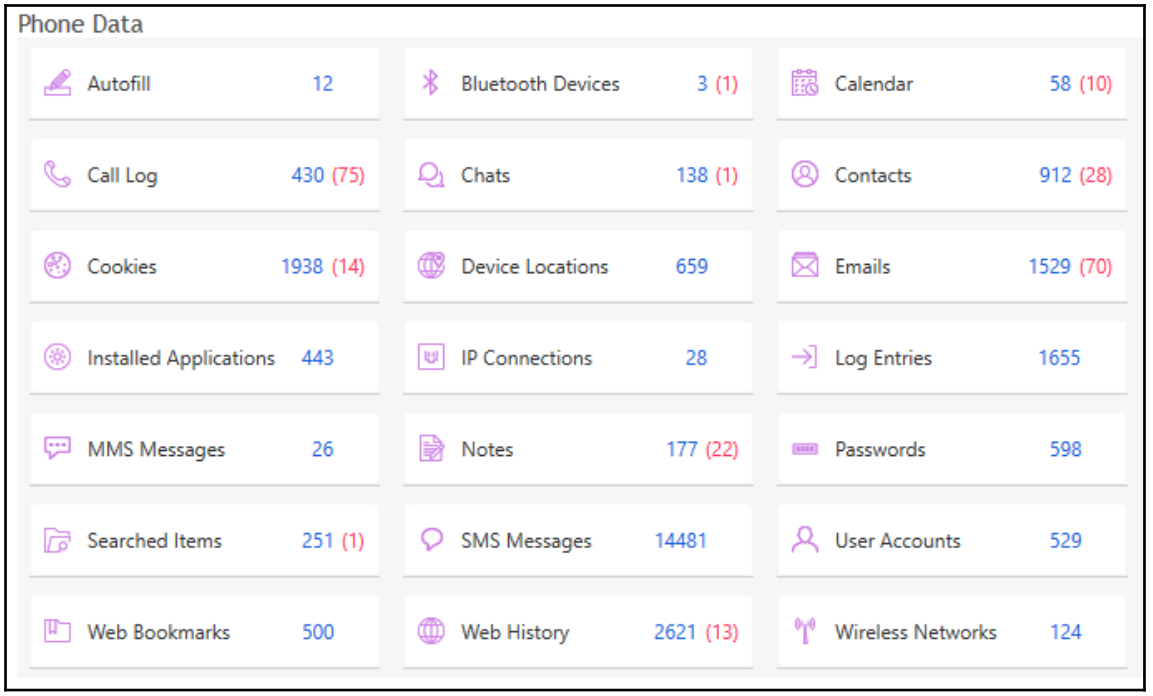


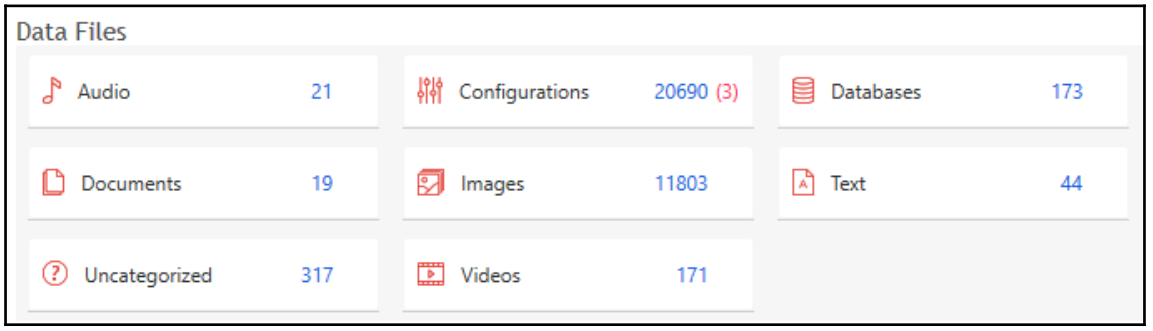

iOS Advanced Logical 6.4.5.119
Connect the device
Connect> Prepare> Extract data
Device: Oleg's iPhone
UDID: 4fecf6418e3fc6dc6fb787de53f51a557267b3af
iOS: 11.2.1
1
Make sure the device is on.
2
Cable 110
or
Adapter A
+
Tip T-110
Cable 210
Connect the device to your computer.
Back to start
Next

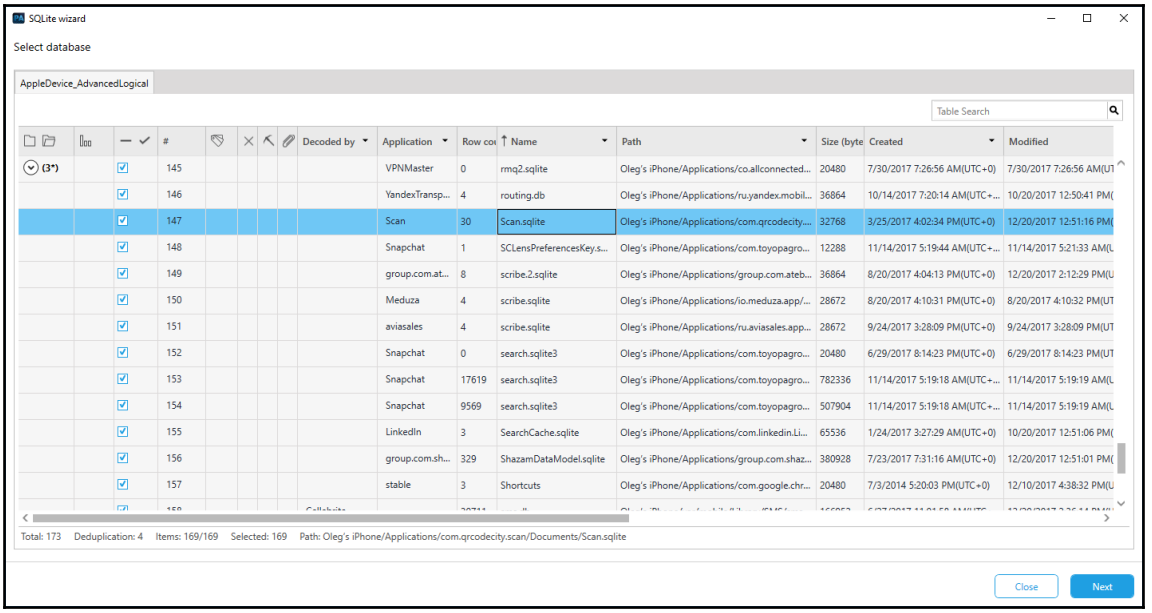

iOS Advanced Logical 6.4.5.119
Choose an extraction method
Connect> Prepare> Extract data
Device: Oleg's iPhone
UDID: 4fecf6418e3fc6dc6fb787de53f51a557267b3af
iOS: 11.2.1
The iTunes backup of this device (iPhone with iOS 11.2.1) is encrypted.
The data extracted by each method will vary based on the device model and iOS version.
Note: If you cannot obtain the password (including brute-force attempts), contact Cellebrite CAIS to bypass the iTunes encryption.
Method 1
Extraction of a rich set of data including call logs, SMSs, MMSs, applications data, data files and notes. The decoding process will require the password for iTunes backup files.
Recommended if the password is known.
Method 2
Limited extraction of data, including data files and locations.
Back to start

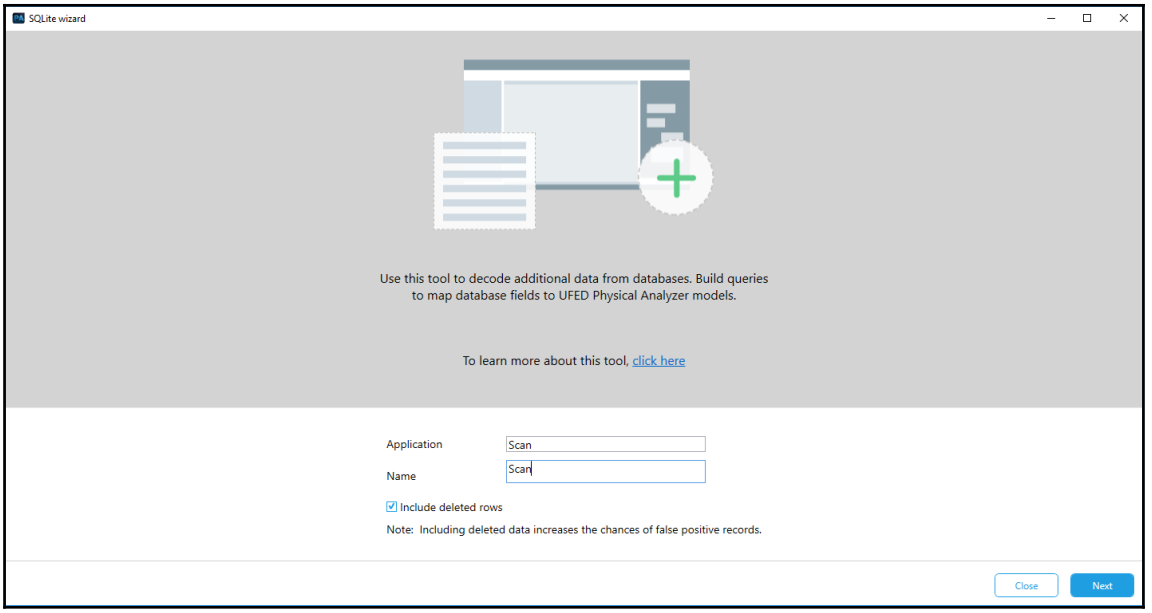

iOS Advanced Logical 6.4.5.119
Choose where to save the extraction
Connect> Prepare> Extract data
Device: Oleg's iPhone
UDID: 4fecf6418e3fc6dc6fb787de53f51a557267b3af
iOS: 11.2.1
My documents\My UFED Extractions
Desktop
D:\
< Back
Next

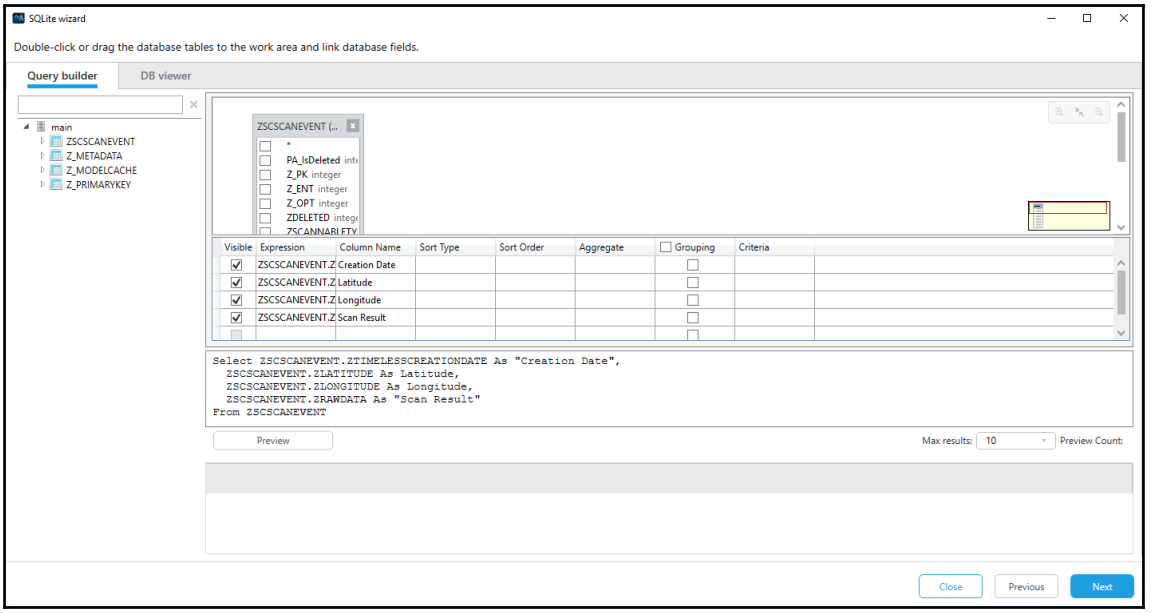

iOS Advanced Logical 6.4.5.119
Extraction in progress
Connect> Prepare> Extract data
Device: Oleg's iPhone
UDID: 4fecf6418e3fc6dc6fb787de53f51a557267b3af
iOS: 11.2.1
Extracting data, step 2 / 2
Time elapsed: 01:33
40%
Cancel

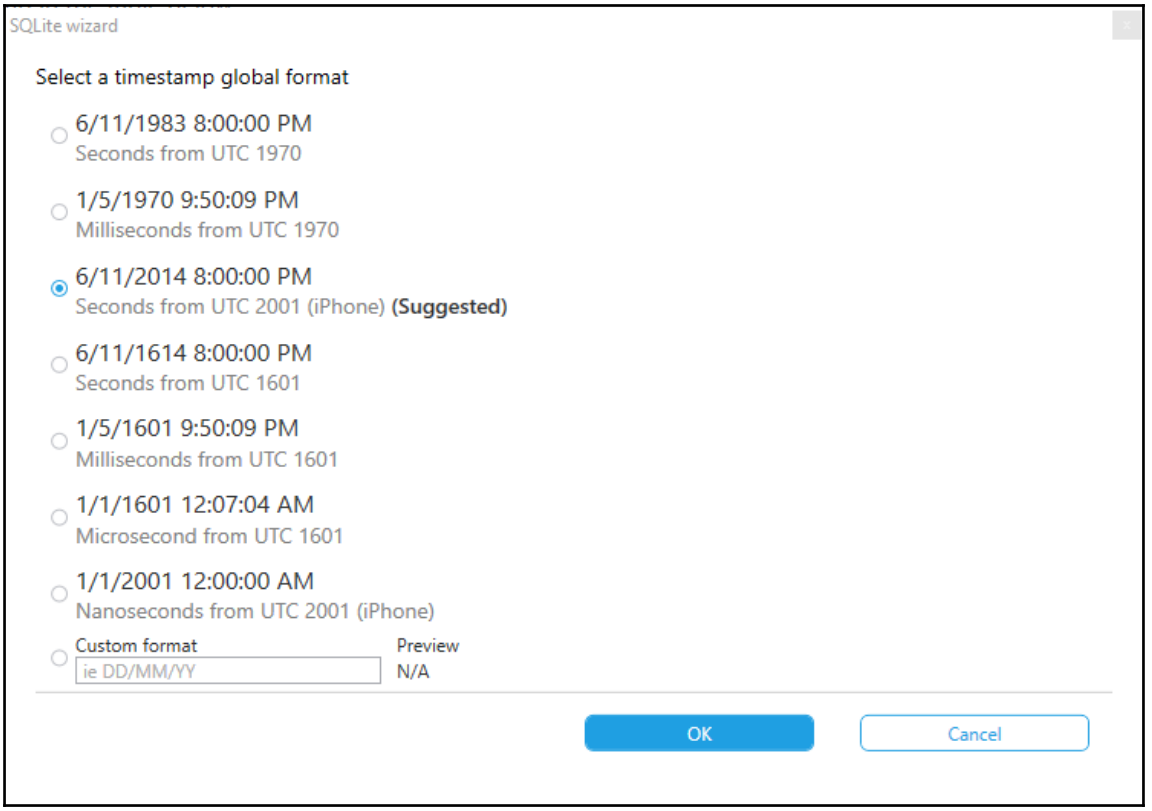

Phone Data
Autofill 12
Bluetooth Devices 3 (1)
Calendar 58 (10)
Call Log 430 (75)
Chats 138 (1)
Contacts 912 (28)
Cookies 1938 (14)
Device Locations 659
Emails 1529 (70)
Installed Applications 443
IP Connections 28
Log Entries 1655
MMS Messages 26
Notes 177 (22)
Passwords 598
Searched Items 251 (1)
SMS Messages 14481
User Accounts 529
Web Bookmarks 500
Web History 2621 (13)
Wireless Networks 124

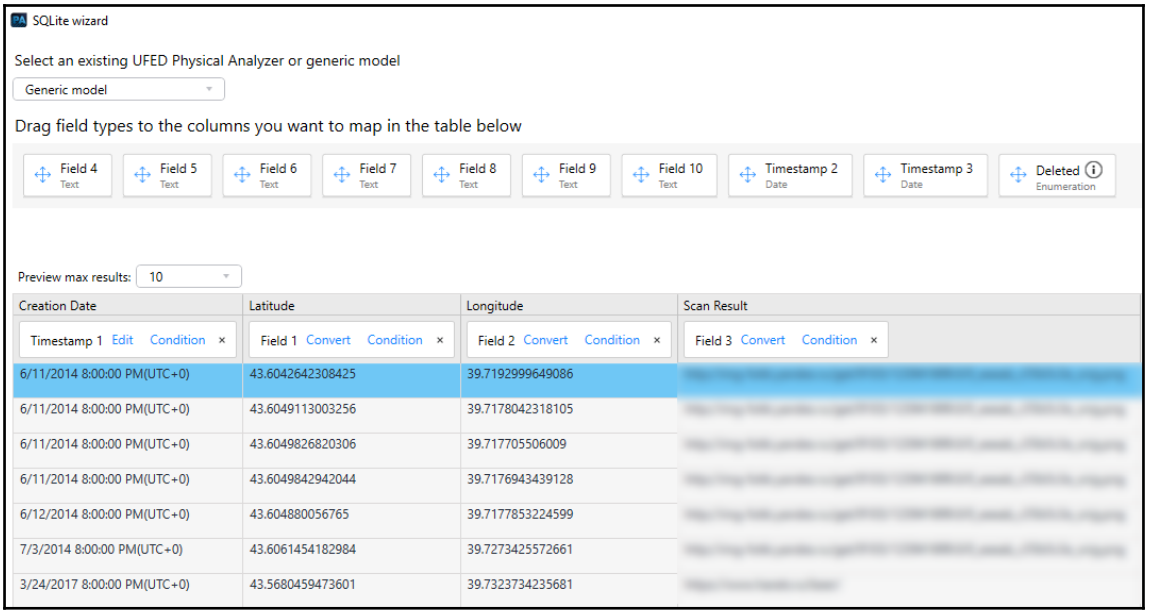

Data Files
Audio 21
Configurations 20690 (3)
Databases 173
Documents 19
Images 11803
Text 44
Uncategorized 317
Videos 171

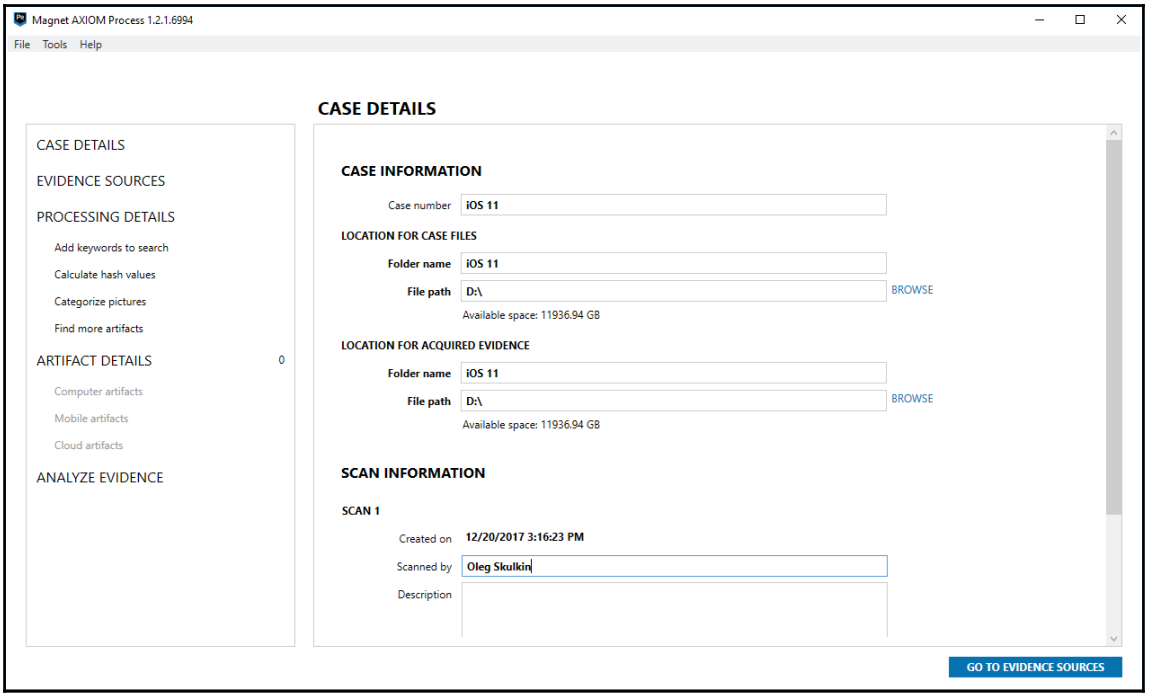

SQLite wizard
Select database
AppleDevice_AdvancedLogical
Table Search
Decoded by
Application
Row co
Name
Path
Size (byte
Created
Modified
(3*)
145 VPNMaster 0 rmq2.sqlite Oleg's iPhone/Applications/co.allconnected... 20480 7/30/2017 7:26:56 AM(UTC+0) 7/30/2017 7:26:56 AM(UT
146 YandexTransp... 4 routing.db Oleg's iPhone/Applications/ru.yandex.mobil... 36864 10/14/2017 7:20:14 AM(UTC+... 10/20/2017 12:50:41 PM(
147 Scan 30 Scan.sqlite Oleg's iPhone/Applications/com.qrcodecity.... 32768 3/25/2017 4:02:34 PM(UTC+0) 12/20/2017 12:51:16 PM(
148 Snapchat 1 SCLensPreferencesKey.s... Oleg's iPhone/Applications/com.toyopagro... 12288 11/14/2017 5:19:44 AM(UTC+... 11/14/2017 5:21:33 AM(U
149 group.com.at... 8 scribe.2.sqlite Oleg's iPhone/Applications/group.com.ateb... 36864 8/20/2017 4:04:13 PM(UTC+0) 12/20/2017 2:12:29 PM(U
150 Meduza 4 scribe.sqlite Oleg's iPhone/Applications/io.meduza.app/... 28672 8/20/2017 4:10:31 PM(UTC+0) 8/20/2017 4:10:32 PM(UT
151 aviasales 4 scribe.sqlite Oleg's iPhone/Applications/ru.aviasales.app... 28672 9/24/2017 3:28:09 PM(UTC+0) 9/24/2017 3:28:09 PM(UT
152 Snapchat 0 search.sqlite3 Oleg's iPhone/Applications/com.toyopagro... 20480 6/29/2017 8:14:23 PM(UTC+0) 6/29/2017 8:14:23 PM(UT
153 Snapchat 17619 search.sqlite3 Oleg's iPhone/Applications/com.toyopagro... 782336 11/14/2017 5:19:18 AM(UTC+... 11/14/2017 5:19:19 AM(U
154 Snapchat 9569 search.sqlite3 Oleg's iPhone/Applications/com.toyopagro... 507904 11/14/2017 5:19:18 AM(UTC+... 11/14/2017 5:19:19 AM(U
155 LinkedIn 3 SearchCache.sqlite Oleg's iPhone/Applications/com.linkedin.Li... 65536 1/24/2017 3:27:29 AM(UTC+0) 10/20/2017 12:51:06 PM(
156 group.com.sh... 329 ShazamDataModel.sqlite Oleg's iPhone/Applications/group.com.shaz... 380928 7/23/2017 7:31:16 AM(UTC+0) 12/20/2017 12:51:01 PM(
157 stable 3 Shortcuts Oleg's iPhone/Applications/com.google.chr... 20480 7/3/2014 5:20:03 PM(UTC+0) 12/10/2017 4:38:32 PM(U
Total: 173 Deduplication: 4 Items: 169/169 Selected: 169 Path: Oleg's iPhone/Applications/com.qrcodecity.scan/Documents/Scan.sqlite
Close
Next

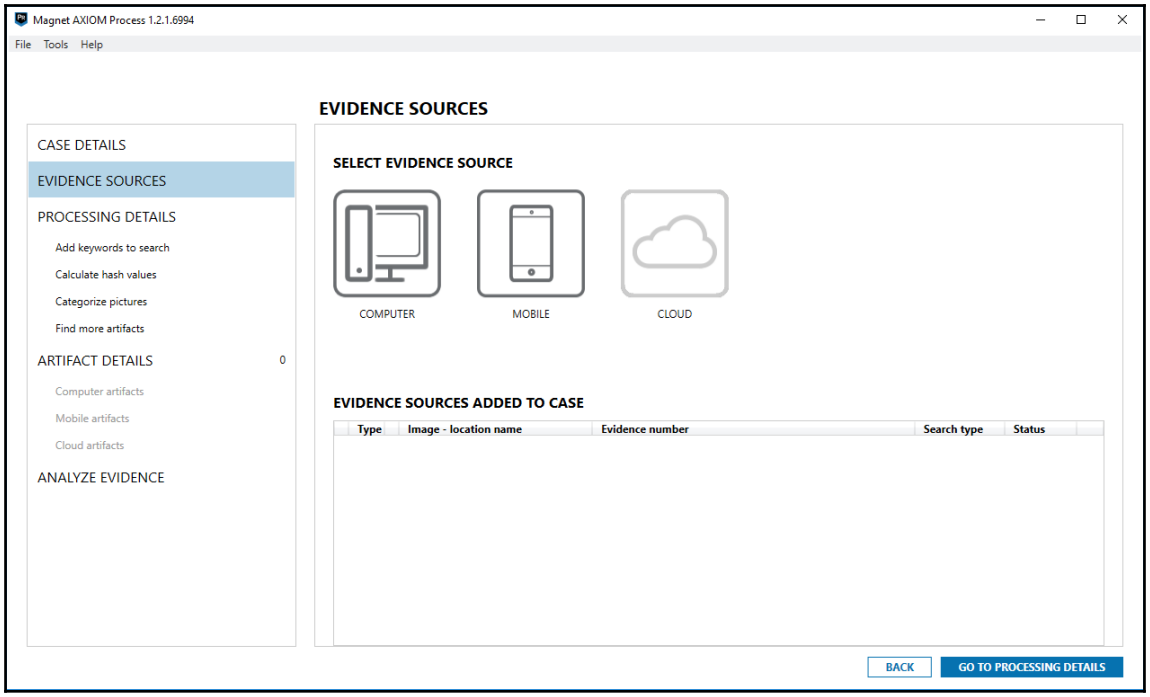

SQLite wizard
Use this tool to decode additional data from databases. Build queries
to map database fields to UFED Physical Analyzer models.
To learn more about this tool, click here
Application
Scan
Name
Scan
Include deleted rows
Note: Including deleted data increases the chances of false positive records.
Close
Next

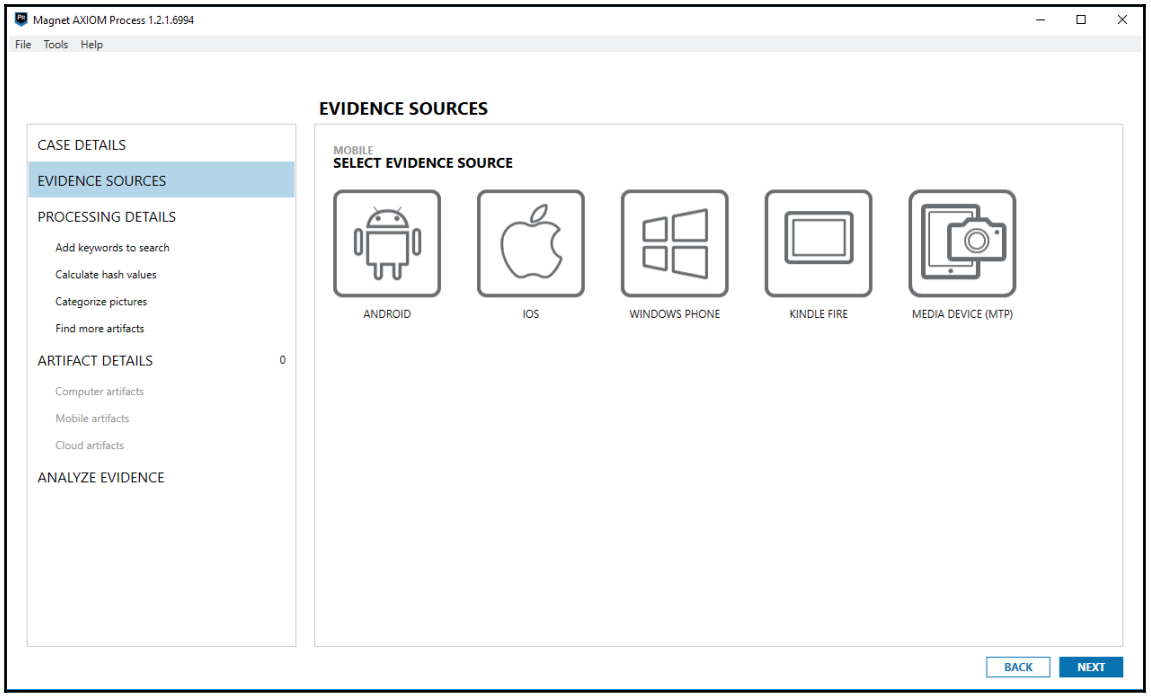

SQLite wizard
Double-click or drag the database tables to the work area and link database fields.
Query builder
DB viewer
main
ZSCSCANEVENT
Z_METADATA
Z_MODELCACHE
Z_PRIMARYKEY
ZSCSCANEVENT (...
*
PA_IsDeleted
Z_PK integer
Z_ENT integer
Z_OPT integer
ZDELETED
Visible
Expression
Column Name
Sort Type
Sort Order
Aggregate
Grouping
Criteria
ZSCSCANEVENT.Z
Creation Date
Latitude
Longitude
Scan Result
Select ZSCSCANEVENT.ZTIMELESSCREATIONDATE As "Creation Date",
ZSCSCANEVENT.ZLATITUDE As Latitude,
ZSCSCANEVENT.ZLONGITUDE As Longitude,
ZSCSCANEVENT.ZRAWDATA As "Scan Result"
From ZSCSCANEVENT
Preview
Max results:
10
Preview Count:
Close
Previous
Next

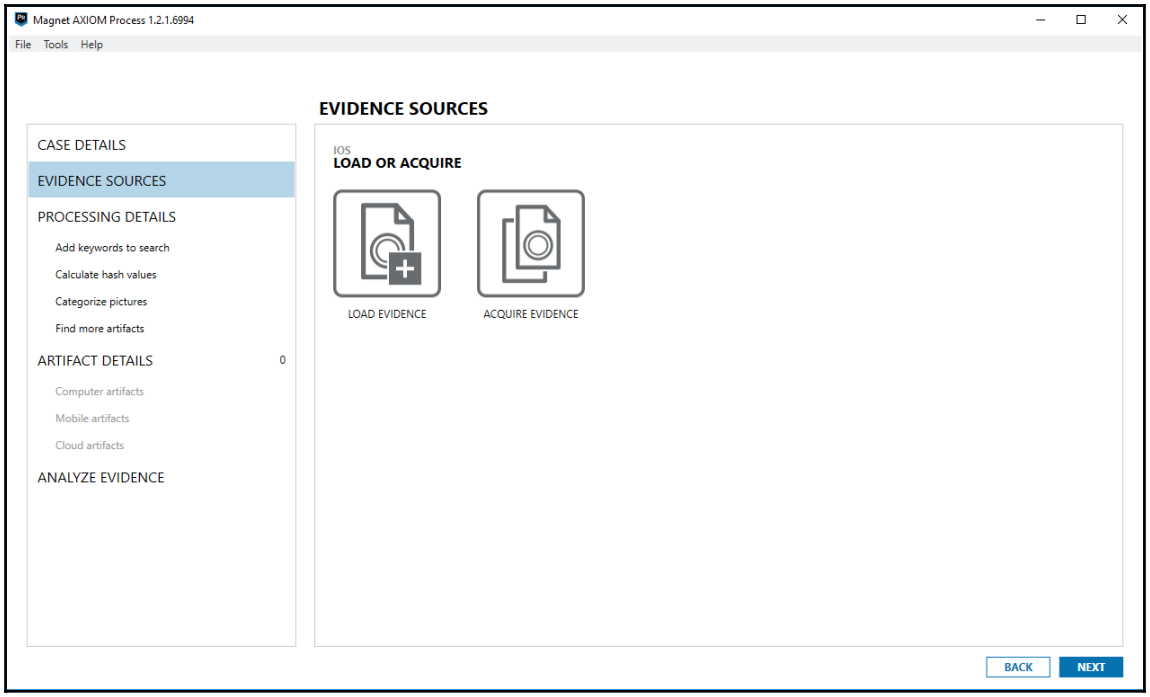

SQLite wizard
Select a timestamp global format
6/11/1983 8:00:00 PM
Seconds from UTC 1970
1/5/1970 9:50:09 PM
Milliseconds from UTC 1970
6/11/2014 8:00:00 PM
Seconds from UTC 2001 (iPhone) (Suggested)
6/11/1614 8:00:00 PM
Seconds from UTC 1601
1/5/1601 9:50:09 PM
Milliseconds from UTC 1601
1/1/1601 12:07:04 AM
Microsecond from UTC 1601
1/1/2001 12:00:00 AM
Nanoseconds from UTC 2001 (iPhone)
Custom format
ie DD/MM/YY
Preview
N/A
OK
Cancel

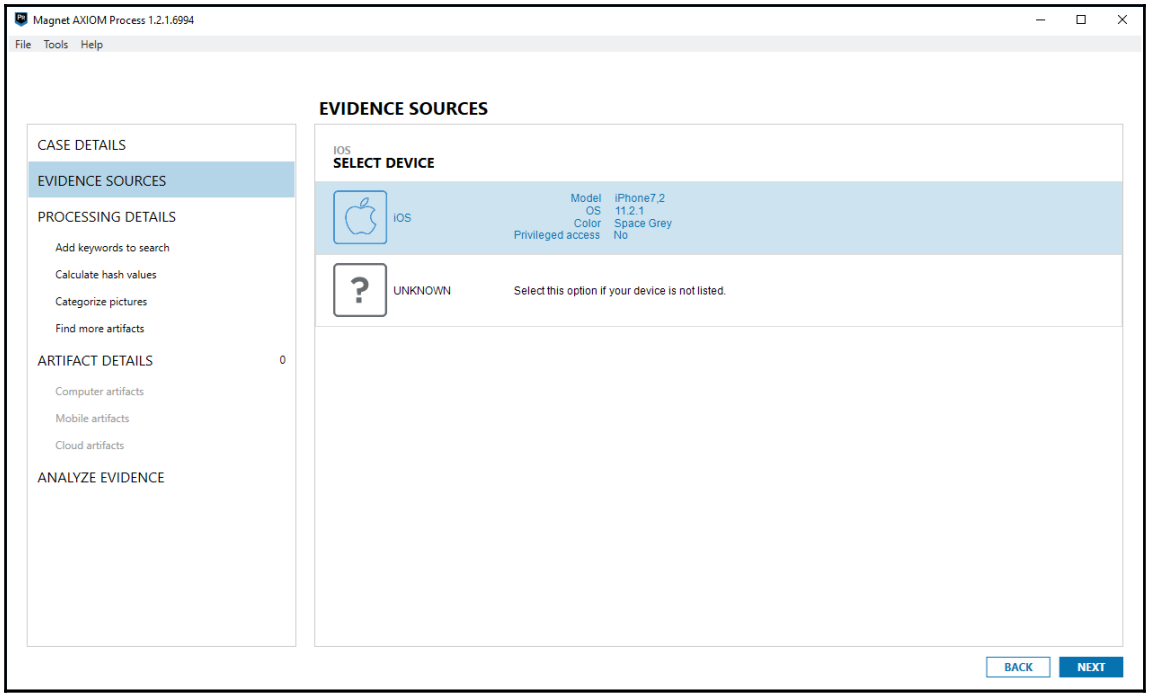

SQLite wizard
Select an existing UFED Physical Analyzer or generic model
Generic model
Drag field types to the columns you want to map in the table below
Field 4 Text
Field 5 Text
Field 6 Text
Field 7 Text
Field 8 Text
Field 9 Text
Field 10 Text
Timestamp 2 Date
Timestamp 3 Date
Deleted Enumeration
Preview max results: 10
Creation Date
Latitude
Longitude
Scan Result
Timestamp 1 Edit Condition
Field 1 Convert Condition
Field 2 Convert Condition
Field 3 Convert Condition
6/11/2014 8:00:00 PM(UTC+0) 43.6042642308425 39.7192999649086
6/11/2014 8:00:00 PM(UTC+0) 43.6049113003256 39.7178042318105
6/11/2014 8:00:00 PM(UTC+0) 43.6049826820306 39.717705506009
6/11/2014 8:00:00 PM(UTC+0) 43.6049842942044 39.7176943439128
6/12/2014 8:00:00 PM(UTC+0) 43.604880056765 39.7177853224599
7/3/2014 8:00:00 PM(UTC+0) 43.6061454182984 39.7273425572661
3/24/2017 8:00:00 PM(UTC+0) 43.5680459473601 39.7323734235681

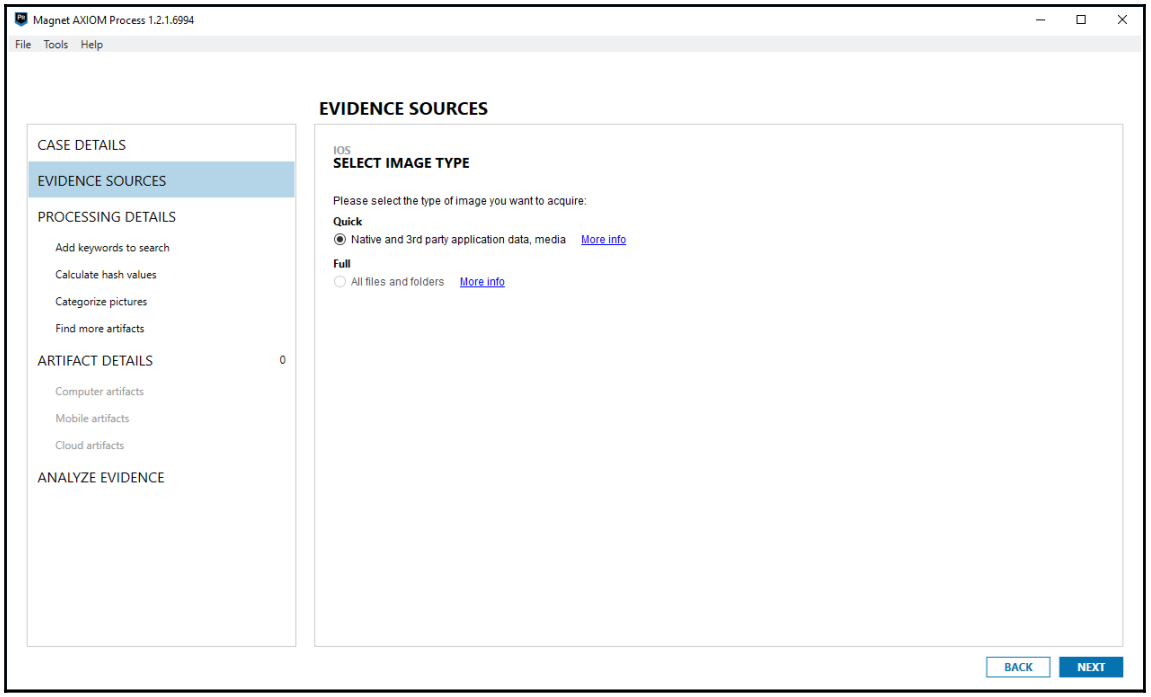

Magnet AXIOM Process 1.2.1.6994
File Tools Help
CASE DETAILS
CASE DETAILS
EVIDENCE SOURCES
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS 0
Computer artifacts
Mobile artifacts
Cloud artifacts
ANALYZE EVIDENCE
CASE INFORMATION
Case number iOS 11
LOCATION FOR CASE FILES
Folder name iOS 11
File path D:\ BROWSE
Available space: 11936.94 GB
LOCATION FOR ACQUIRED EVIDENCE
Folder name iOS 11
File path D:\ BROWSE
Available space: 11936.94 GB
SCAN INFORMATION
SCAN 1
Created on 12/20/2017 3:16:23 PM
Scanned by Oleg Skulkin
Description
GO TO EVIDENCE SOURCES


Magnet AXIOM Process 1.2.1.6994
File Tools Help
EVIDENCE SOURCES
CASE DETAILS
EVIDENCE SOURCES
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS 0
Computer artifacts
Mobile artifacts
Cloud artifacts
ANALYZE EVIDENCE
SELECT EVIDENCE SOURCE
COMPUTER
MOBILE
CLOUD
EVIDENCE SOURCES ADDED TO CASE
Type
Image - location name
Evidence number
Search type
Status
BACK
GO TO PROCESSING DETAILS

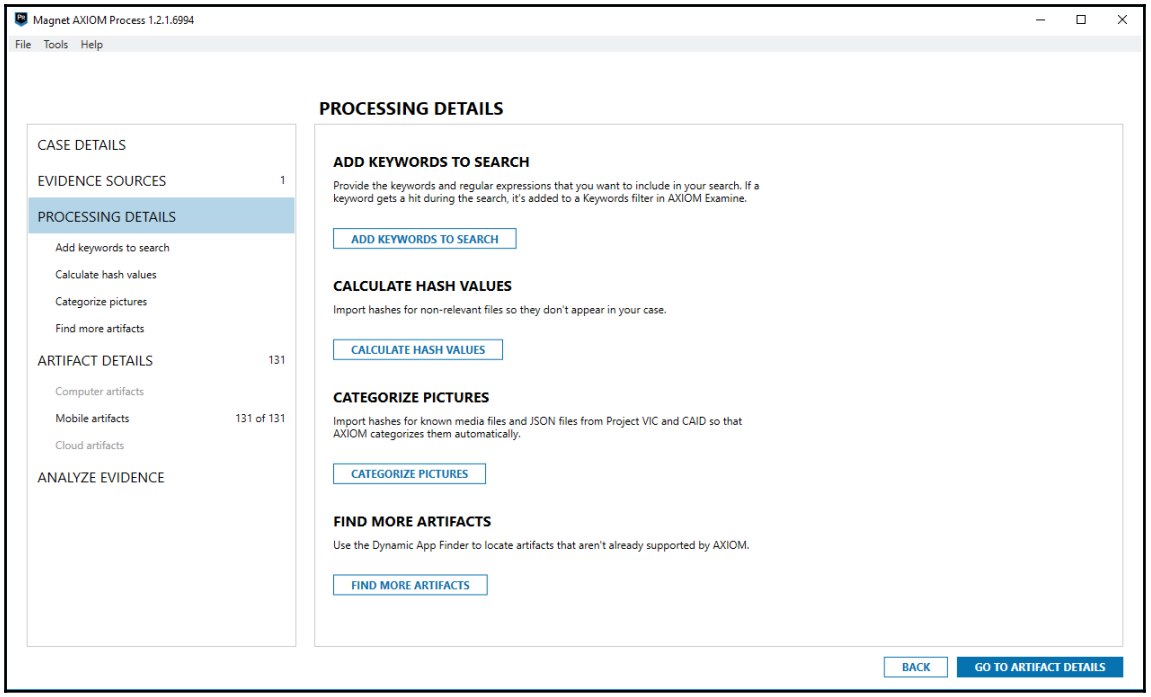

Magnet AXIOM Process 1.2.1.6994
File Tools Help
EVIDENCE SOURCES
CASE DETAILS
EVIDENCE SOURCES
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS 0
Computer artifacts
Mobile artifacts
Cloud artifacts
ANALYZE EVIDENCE
MOBILE
SELECT EVIDENCE SOURCE
ANDROID
IOS
WINDOWS PHONE
KINDLE FIRE
MEDIA DEVICE (MTP)
BACK
NEXT

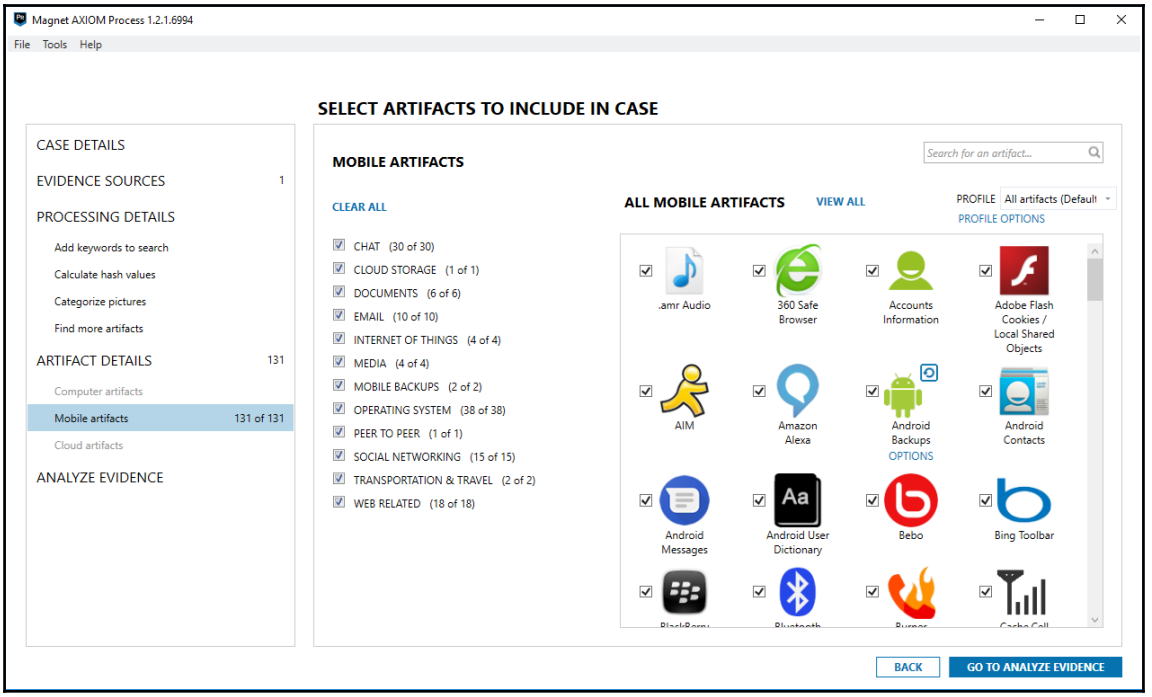

Magnet AXIOM Process 1.2.1.6994
File Tools Help
EVIDENCE SOURCES
CASE DETAILS
EVIDENCE SOURCES
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS 0
Computer artifacts
Mobile artifacts
Cloud artifacts
ANALYZE EVIDENCE
IOS
LOAD OR ACQUIRE
LOAD EVIDENCE
ACQUIRE EVIDENCE
BACK
NEXT

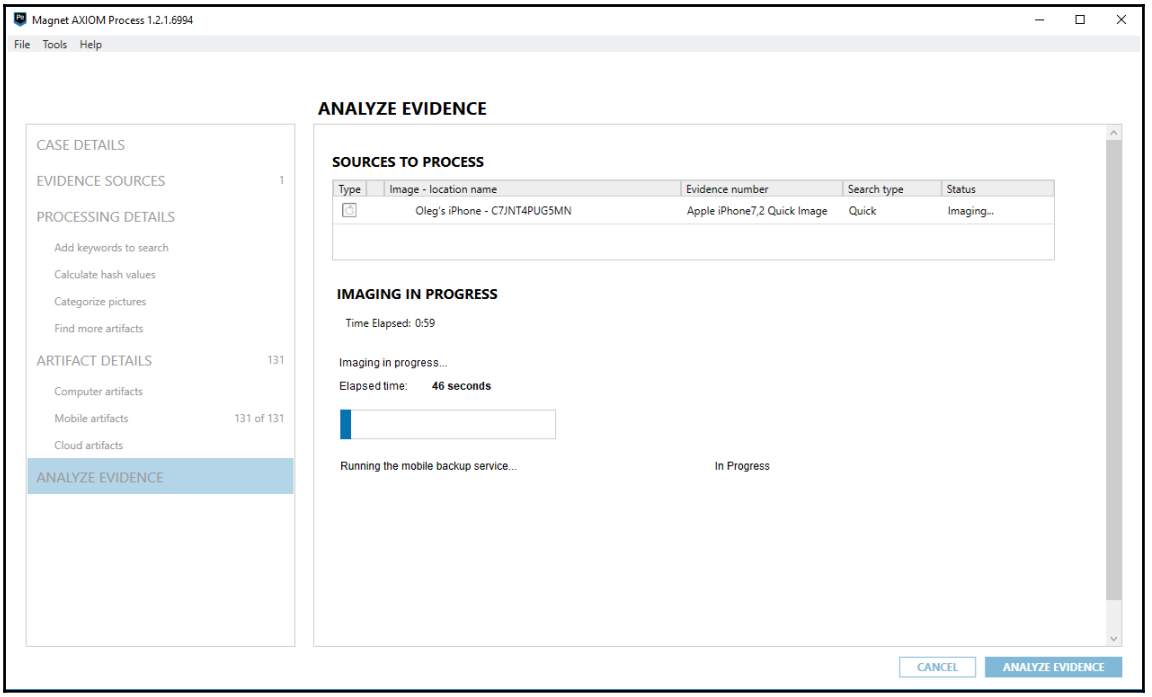

Magnet AXIOM Process 1.2.1.6994
File Tools Help
EVIDENCE SOURCES
CASE DETAILS
EVIDENCE SOURCES
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS 0
Computer artifacts
Mobile artifacts
Cloud artifacts
ANALYZE EVIDENCE
IOS
SELECT DEVICE
iOS
Model iPhone7,2
OS 11.2.1
Color Space Grey
Privileged access No
UNKNOWN
Select this option if your device is not listed.
BACK
NEXT

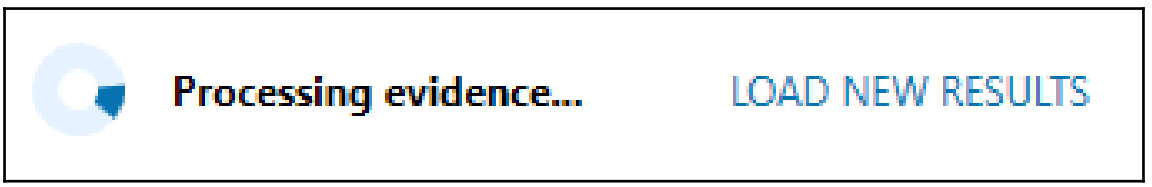

Magnet AXIOM Process 1.2.1.6994
File Tools Help
EVIDENCE SOURCES
CASE DETAILS
EVIDENCE SOURCES
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS 0
Computer artifacts
Mobile artifacts
Cloud artifacts
ANALYZE EVIDENCE
IOS
SELECT IMAGE TYPE
Please select the type of image you want to acquire:
Quick
Native and 3rd party application data, media More info
Full
All files and folders More info
BACK
NEXT

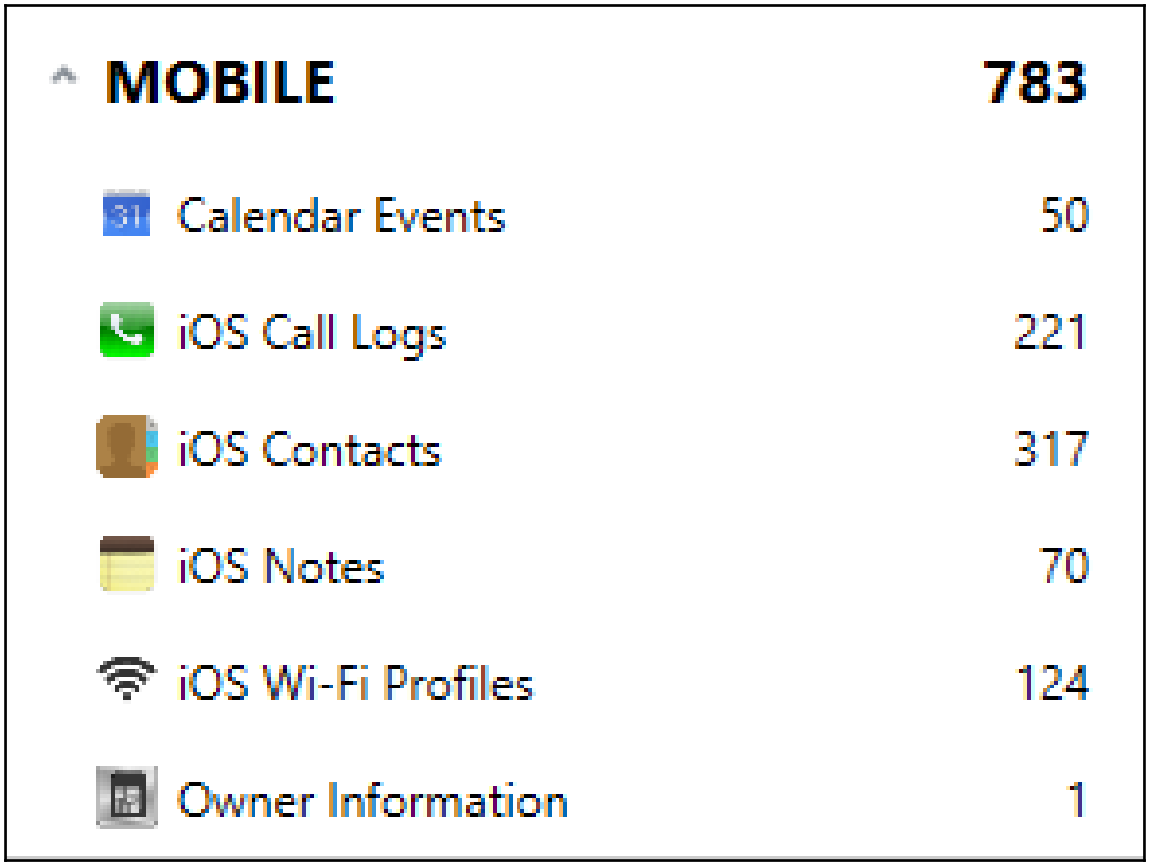

Encrypted iTunes backups
If the encrypted backup feature in iTunes is turned on, Magnet AXIOM might acquire more evidence from the device if it acquires the encrypted backup.
To acquire an encrypted iTunes backup, type the encryption password. To continue with an unencrypted backup, leave the field blank.
Password
123
OKAY

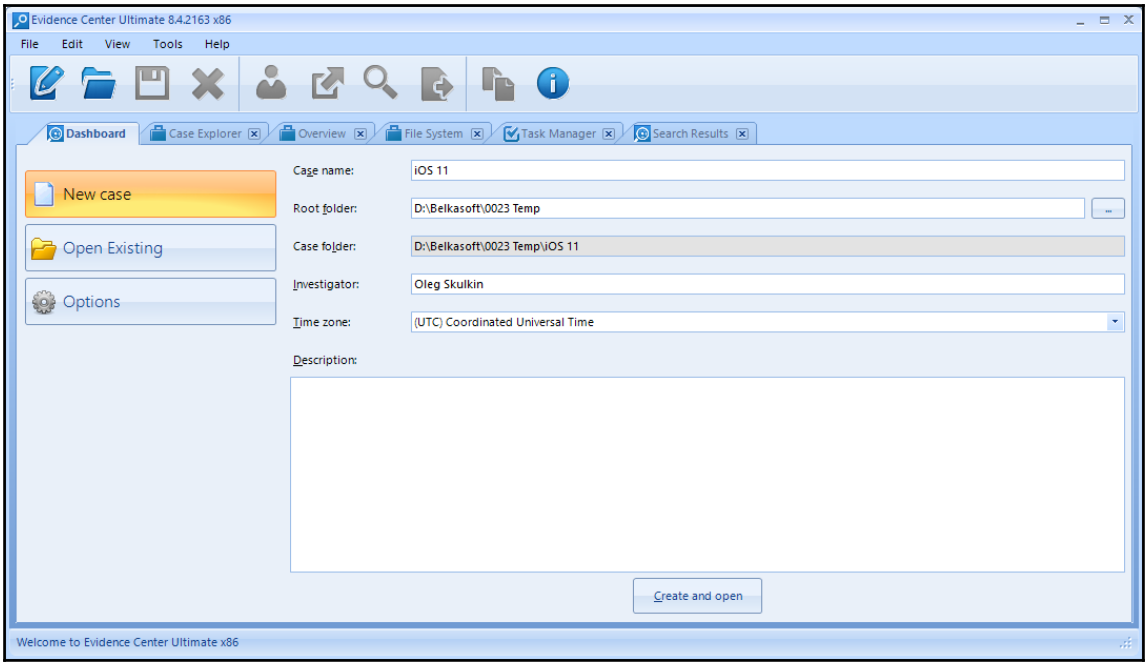

Magnet AXIOM Process 1.2.1.6994
File Tools Help
PROCESSING DETAILS
CASE DETAILS
EVIDENCE SOURCES 1
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS 131
Computer artifacts
Mobile artifacts 131 of 131
Cloud artifacts
ANALYZE EVIDENCE
ADD KEYWORDS TO SEARCH
Provide the keywords and regular expressions that you want to include in your search. If a keyword gets a hit during the search, it's added to a Keywords filter in AXIOM Examine.
ADD KEYWORDS TO SEARCH
CALCULATE HASH VALUES
Import hashes for non-relevant files so they don't appear in your case.
CALCULATE HASH VALUES
CATEGORIZE PICTURES
Import hashes for known media files and JSON files from Project VIC and CAID so that AXIOM categorizes them automatically.
CATEGORIZE PICTURES
FIND MORE ARTIFACTS
Use the Dynamic App Finder to locate artifacts that aren't already supported by AXIOM.
FIND MORE ARTIFACTS
BACK
GO TO ARTIFACT DETAILS

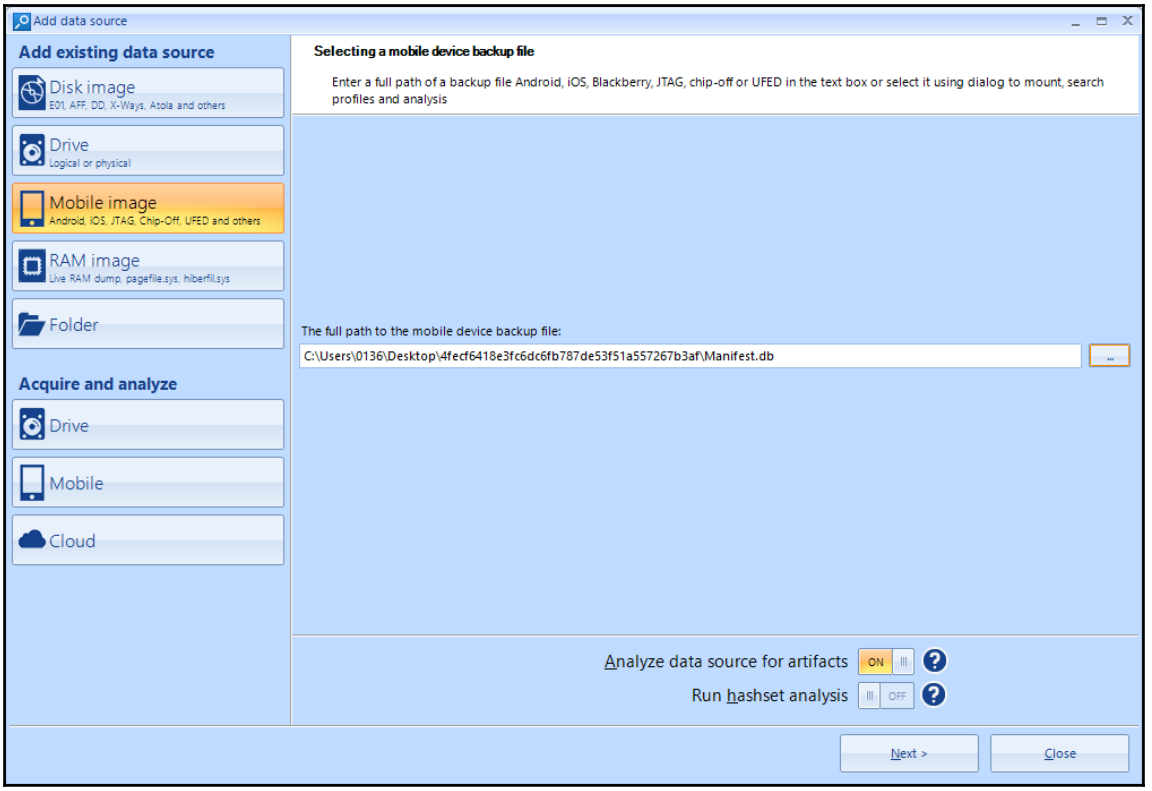

Magnet AXIOM Process 1.2.1.6994
File Tools Help
SELECT ARTIFACTS TO INCLUDE IN CASE
CASE DETAILS
EVIDENCE SOURCES 1
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS 131
Computer artifacts
Mobile artifacts 131 of 131
Cloud artifacts
ANALYZE EVIDENCE
MOBILE ARTIFACTS
CLEAR ALL
CHAT (30 of 30)
CLOUD STORAGE (1 of 1)
DOCUMENTS (6 of 6)
EMAIL (10 of 10)
INTERNET OF THINGS (4 of 4)
MEDIA (4 of 4)
MOBILE BACKUPS (2 of 2)
OPERATING SYSTEM (38 of 38)
PEER TO PEER (1 of 1)
SOCIAL NETWORKING (15 of 15)
TRANSPORTATION & TRAVEL (2 of 2)
WEB RELATED (18 of 18)
Search for an artifact...
ALL MOBILE ARTIFACTS
VIEW ALL
PROFILE All artifacts (Default
PROFILE OPTIONS
.amr Audio
360 Safe Browser
Accounts Information
Adobe Flash Cookies / Local Shared Objects
AIM
Amazon Alexa
Android Backups
OPTIONS
Android Contacts
Android Messages
Android User Dictionary
Bebo
Bing Toolbar
BACK
GO TO ANALYZE EVIDENCE

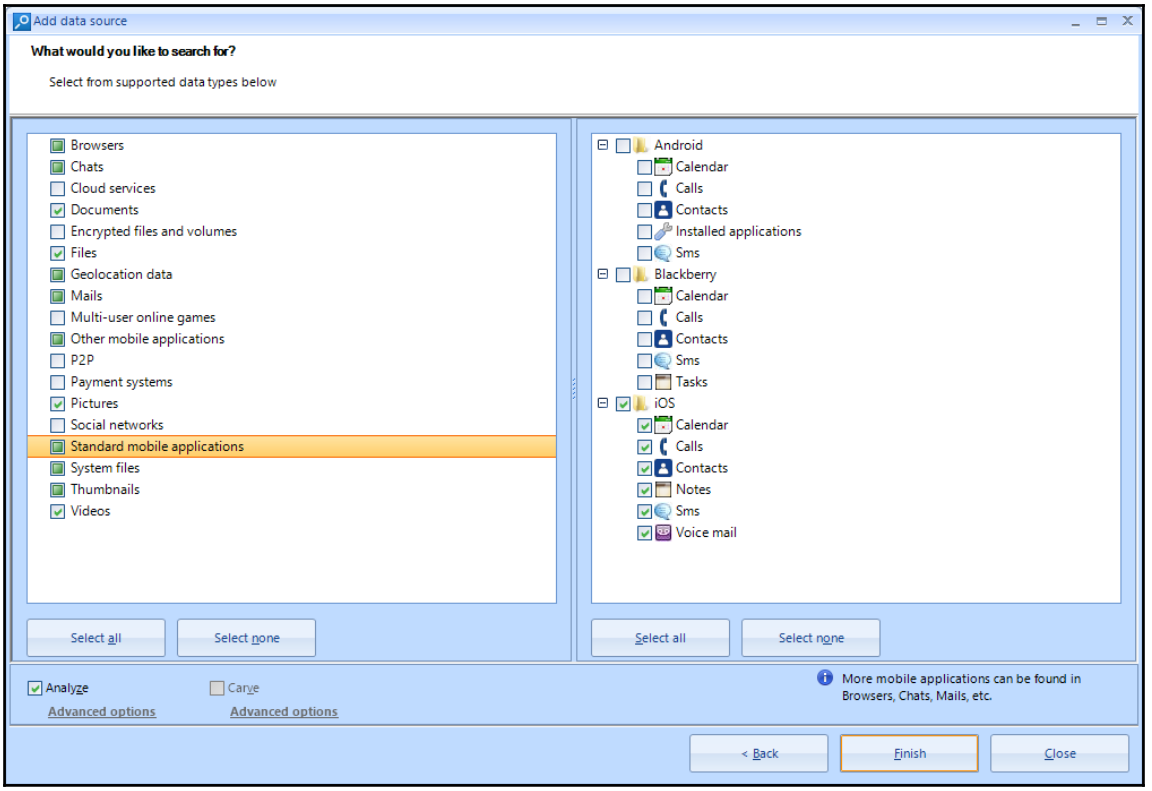

Magnet AXIOM Process 1.2.1.6994
File Tools Help
ANALYZE EVIDENCE
CASE DETAILS
EVIDENCE SOURCES 1
PROCESSING DETAILS
Add keywords to search
Calculate hash values
Categorize pictures
Find more artifacts
ARTIFACT DETAILS 131
Computer artifacts
Mobile artifacts 131 of 131
Cloud artifacts
ANALYZE EVIDENCE
SOURCES TO PROCESS
Type
Image - location name
Evidence number
Search type
Status
Oleg's iPhone - C7JNT4PUG5MN
Apple iPhone7,2 Quick Image
Quick
Imaging...
IMAGING IN PROGRESS
Time Elapsed: 0:59
Imaging in progress...
Elapsed time: 46 seconds
Running the mobile backup service...
In Progress
CANCEL
ANALYZE EVIDENCE

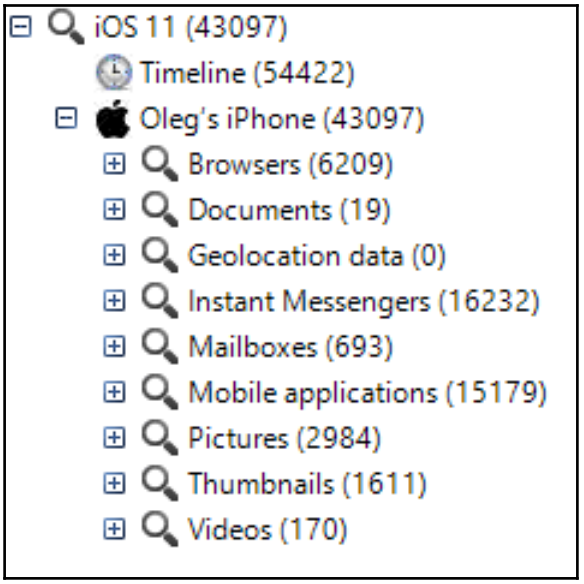

Processing evidence...
LOAD NEW RESULTS

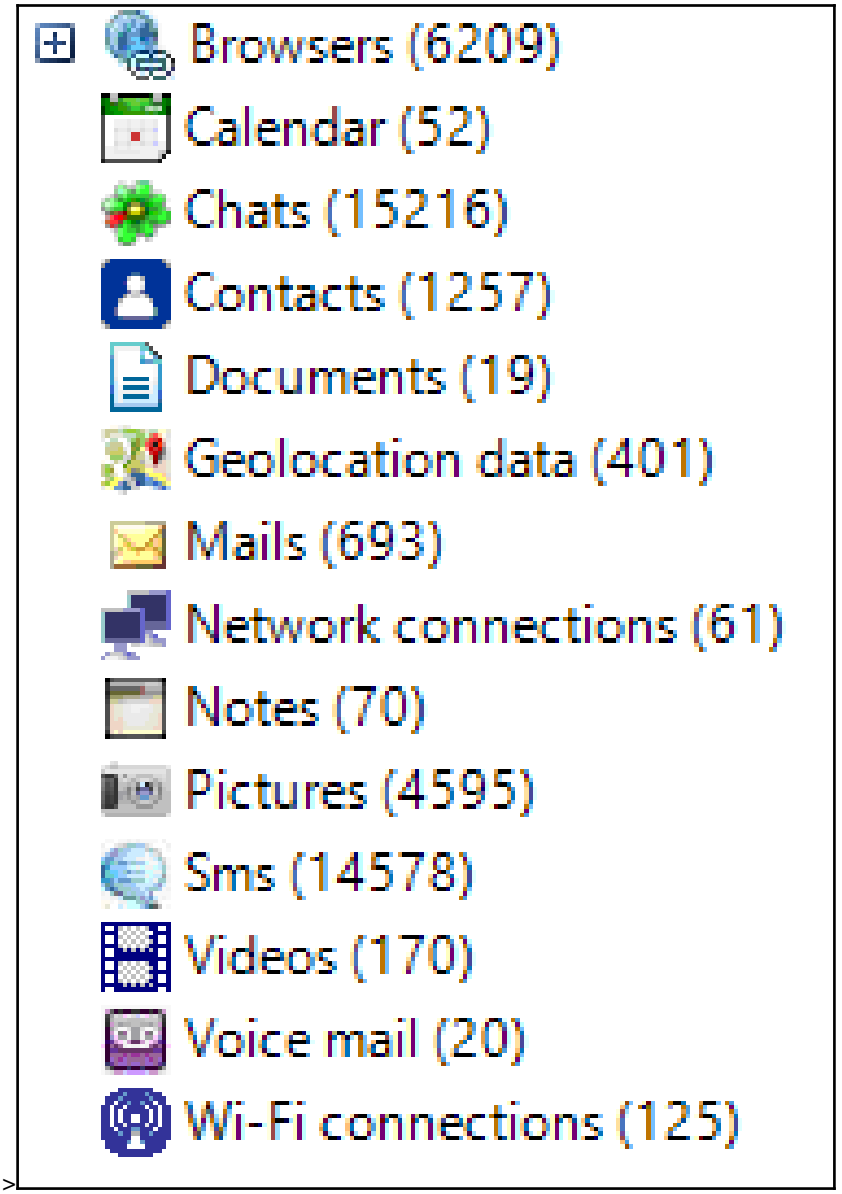

MOBILE 783
Calendar Events 50
iOS Call Logs 221
iOS Contacts 317
iOS Notes 70
iOS Wi-Fi Profiles 124
Owner Information 1

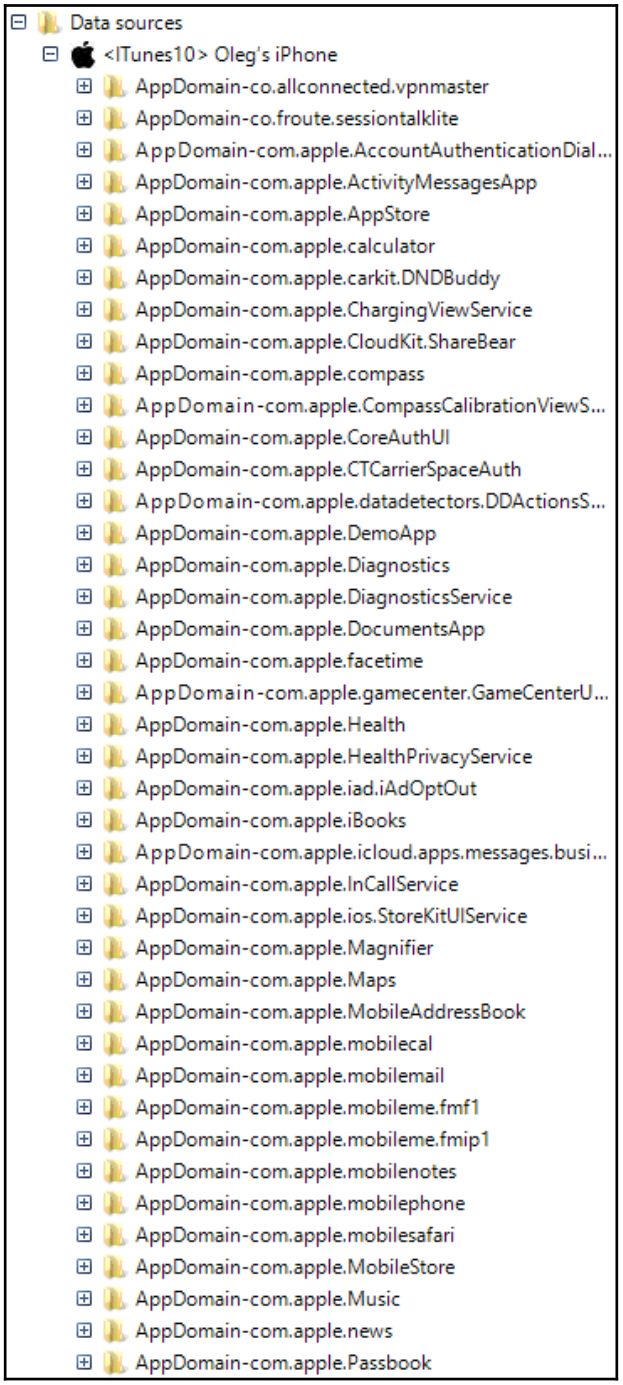

Evidence Center Ultimate 8.4.2163 x86
File
Edit
View
Tools
Help
Dashboard
Case Explorer
Overview
File System
Task Manager
Search Results
New case
Open Existing
Options
Case name:
iOS 11
Root folder:
D:\Belkasoft\0023 Temp
Case folder:
D:\Belkasoft\0023 Temp\iOS 11
Investigator:
Oleg Skulkin
Time zone:
(UTC) Coordinated Universal Time
Description:
Create and open
Welcome to Evidence Center Ultimate x86


Add data source
Add existing data source
Disk image
E01, AFF, DD, X-Ways, Atola and others
Drive
Logical or physical
Mobile image
Android, iOS, JTAG, Chip-Off, UFED and others
RAM image
Live RAM dump, pagefile.sys, hiberfil.sys
Folder
Acquire and analyze
Drive
Mobile
Cloud
Selecting a mobile device backup file
Enter a full path of a backup file Android, iOS, Blackberry, JTAG, chip-off or UFED in the text box or select it using dialog to mount, search profiles and analysis
The full path to the mobile device backup file:
C:\Users\0136\Desktop\4fecf6418e3fc6dc6fb787de53f51a557267b3af\Manifest.db
...
Analyze data source for artifacts
ON
Run hashset analysis
OFF
Next >
Close


Add data source
What would you like to search for?
Select from supported data types below
Browsers
Chats
Cloud services
Documents
Encrypted files and volumes
Files
Geolocation data
Mails
Multi-user online games
Other mobile applications
P2P
Payment systems
Pictures
Social networks
Standard mobile applications
System files
Thumbnails
Videos
Select all
Select none
Android
Calendar
Calls
Contacts
Installed applications
Sms
Blackberry
Calendar
Calls
Contacts
Sms
Tasks
iOS
Calendar
Calls
Contacts
Notes
Sms
Voice mail
Select all
Select none
Analyze
Advanced options
Carve
Advanced options
More mobile applications can be found in Browsers, Chats, Mails, etc.
< Back
Finish
Close

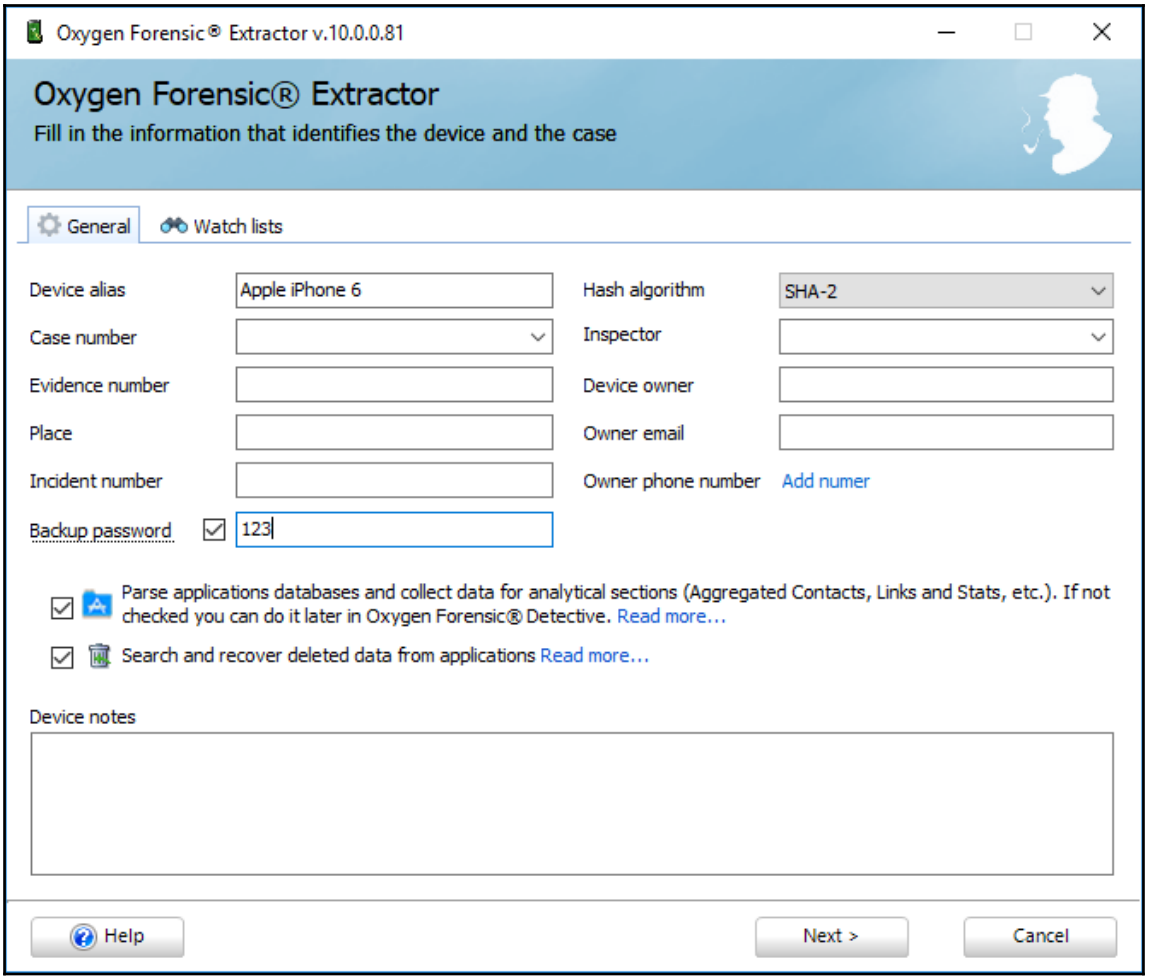

iOS 11 (43097)
Timeline (54422)
Oleg's iPhone (43097)
Browsers (6209)
Documents (19)
Geolocation data (0)
Instant Messengers (16232)
Mailboxes (693)
Mobile applications (15179)
Pictures (2984)
Thumbnails (1611)
Videos (170)

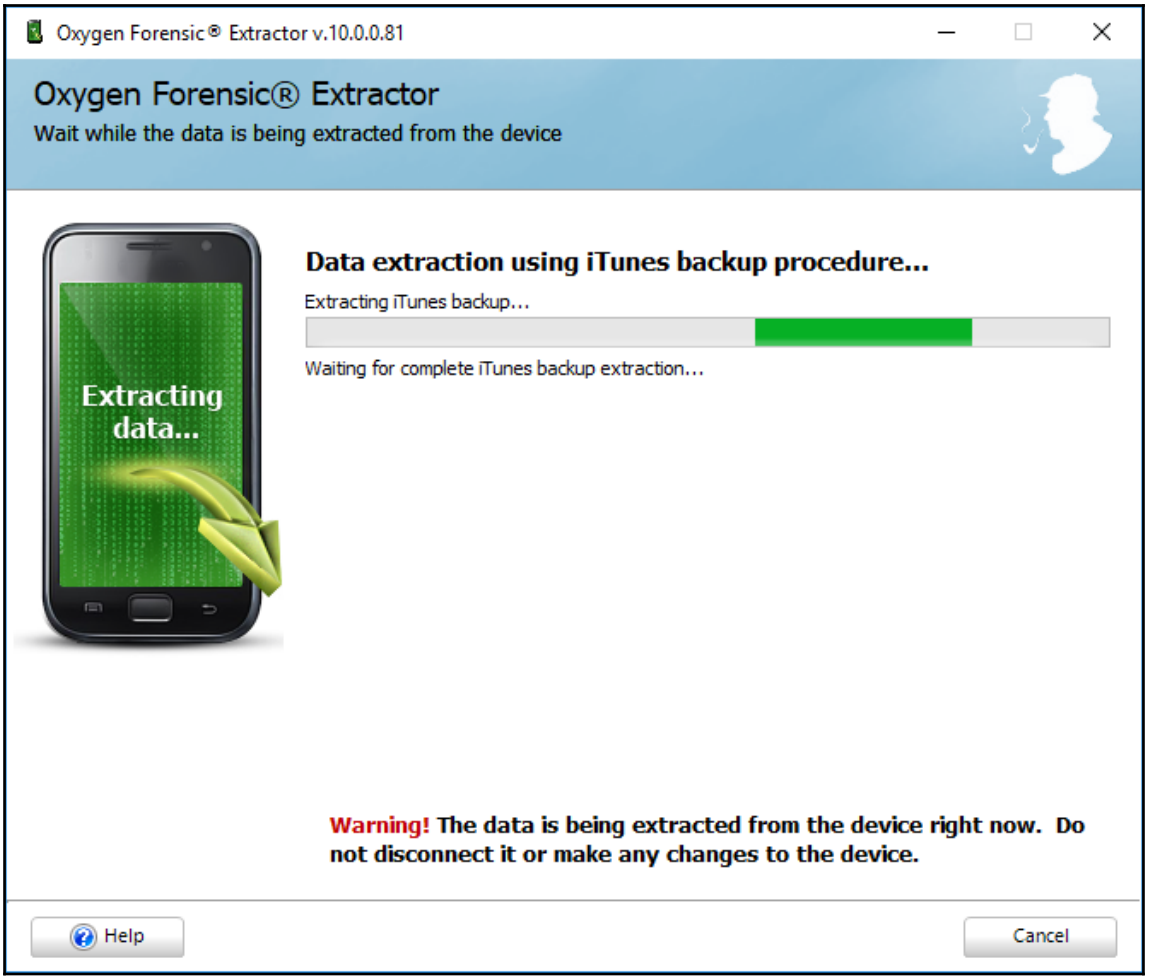

Browsers (6209)
Calendar (52)
Chats (15216)
Contacts (1257)
Documents (19)
Geolocation data (401)
Mails (693)
Network connections (61)
Notes (70)
Pictures (4595)
Sms (14578)
Videos (170)
Voice mail (20)
Wi-Fi connections (125)

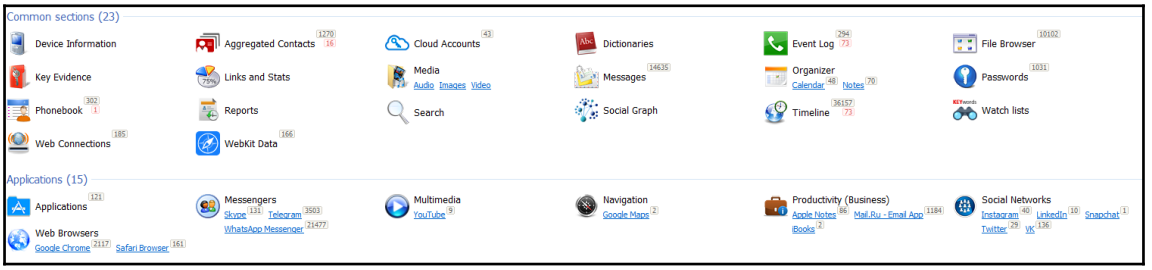

Data sources
<ITunes10> Oleg's iPhone
AppDomain-co.allconnected.vpnmaster
AppDomain-co.froute.sessiontalklite
AppDomain-com.apple.AccountAuthenticationDial...
AppDomain-com.apple.ActivityMessagesApp
AppDomain-com.apple.AppStore
AppDomain-com.apple.calculator
AppDomain-com.apple.carkit.DNDBuddy
AppDomain-com.apple.ChargingViewService
AppDomain-com.apple.CloudKit.ShareBear
AppDomain-com.apple.compass
AppDomain-com.apple.CompassCalibrationViewS...
AppDomain-com.apple.CoreAuthUI
AppDomain-com.apple.CTCarrierSpaceAuth
AppDomain-com.apple.datadetectors.DDActionsS...
AppDomain-com.apple.DemoApp
AppDomain-com.apple.Diagnostics
AppDomain-com.apple.DiagnosticsService
AppDomain-com.apple.DocumentsApp
AppDomain-com.apple.facetime
AppDomain-com.apple.gamecenter.GameCenterU...
AppDomain-com.apple.Health
AppDomain-com.apple.HealthPrivacyService
AppDomain-com.apple.iad.iAdOptOut
AppDomain-com.apple.iBooks
AppDomain-com.apple.icloud.apps.messages.busi...
AppDomain-com.apple.InCallService
AppDomain-com.apple.ios.StoreKitUIService
AppDomain-com.apple.Magnifier
AppDomain-com.apple.Maps
AppDomain-com.apple.MobileAddressBook
AppDomain-com.apple.mobilecal
AppDomain-com.apple.mobilemail
AppDomain-com.apple.mobileme.fmf1
AppDomain-com.apple.mobileme.fmip1
AppDomain-com.apple.mobilenotes
AppDomain-com.apple.mobilephone
AppDomain-com.apple.mobilesafari
AppDomain-com.apple.MobileStore
AppDomain-com.apple.Music
AppDomain-com.apple.news
AppDomain-com.apple.Passbook


Oxygen Forensic® Extractor v.10.0.0.81
Oxygen Forensic® Extractor
Select a method of device data extraction
Device acquisition
Manual device connection | Automatic connection settings
Physical data acquisition
MTK Android dump | LG Android dump | Spreadtrum Android dump
Samsung Android dump | Memory card dump | Motorola Android dump
UICC acquisition
SIM card data extraction via card reader.
Disable screen lock
Screen lock disabling for LG devices based on Android OS.
Help
Cancel

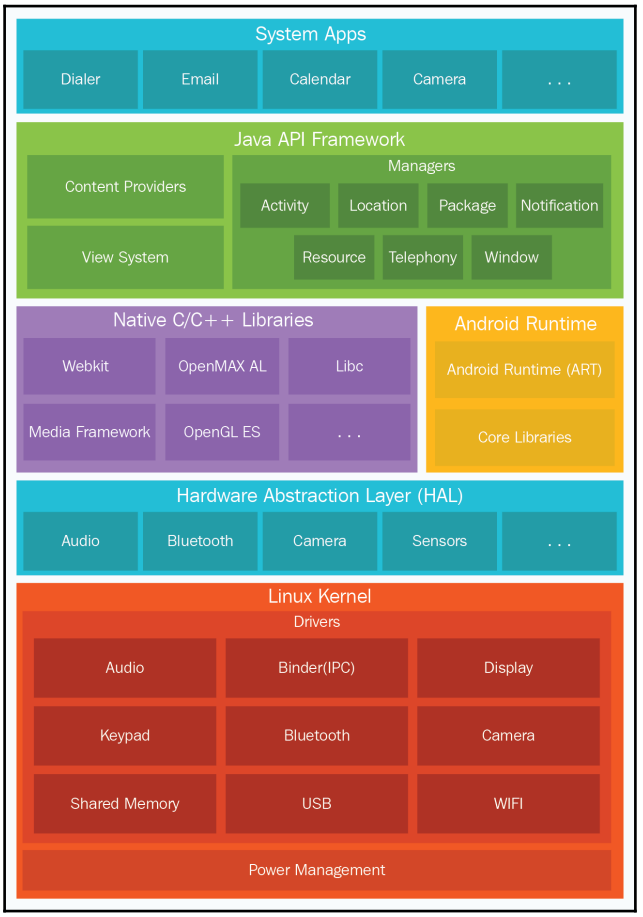

Oxygen Forensic® Extractor v.10.0.0.81
Oxygen Forensic® Extractor
Detection of devices connected via cable
Connected!
Connect device via cable
Device is detected successfully!
Press Next button to start extracting data from the device. Press Cancel if you do not need to investigate this device now.
Device information:
Model:
Apple iPhone 6
IMEI:
356957064318604
Software revision:
11.2.1
Boot loader:
Apple OS iBoot-4076.30.43
Help
Next >
Cancel

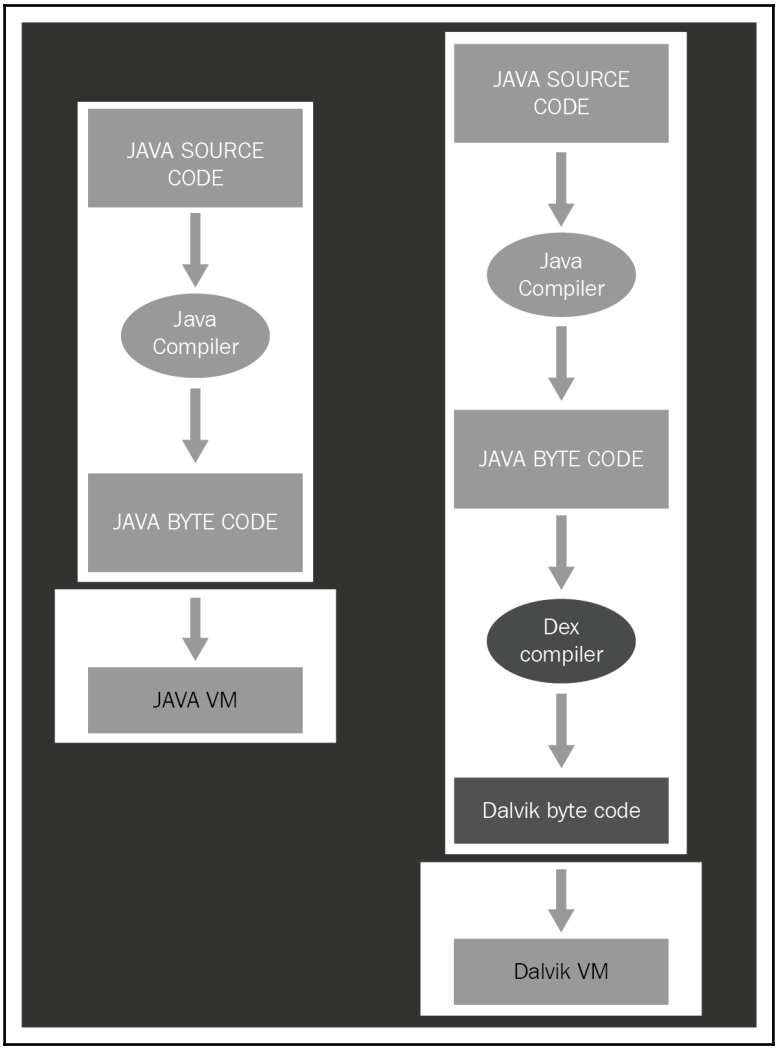

Oxygen Forensic® Extractor v.10.0.0.81
Oxygen Forensic® Extractor
Fill in the information that identifies the device and the case
General
Watch lists
Device alias
Apple iPhone 6
Case number
Evidence number
Place
Incident number
Backup password
123
Hash algorithm
SHA-2
Inspector
Device owner
Owner email
Owner phone number
Add numer
Parse applications databases and collect data for analytical sections (Aggregated Contacts, Links and Stats, etc.). If not checked you can do it later in Oxygen Forensic® Detective. Read more...
Search and recover deleted data from applications Read more...
Device notes
Help
Next >
Cancel

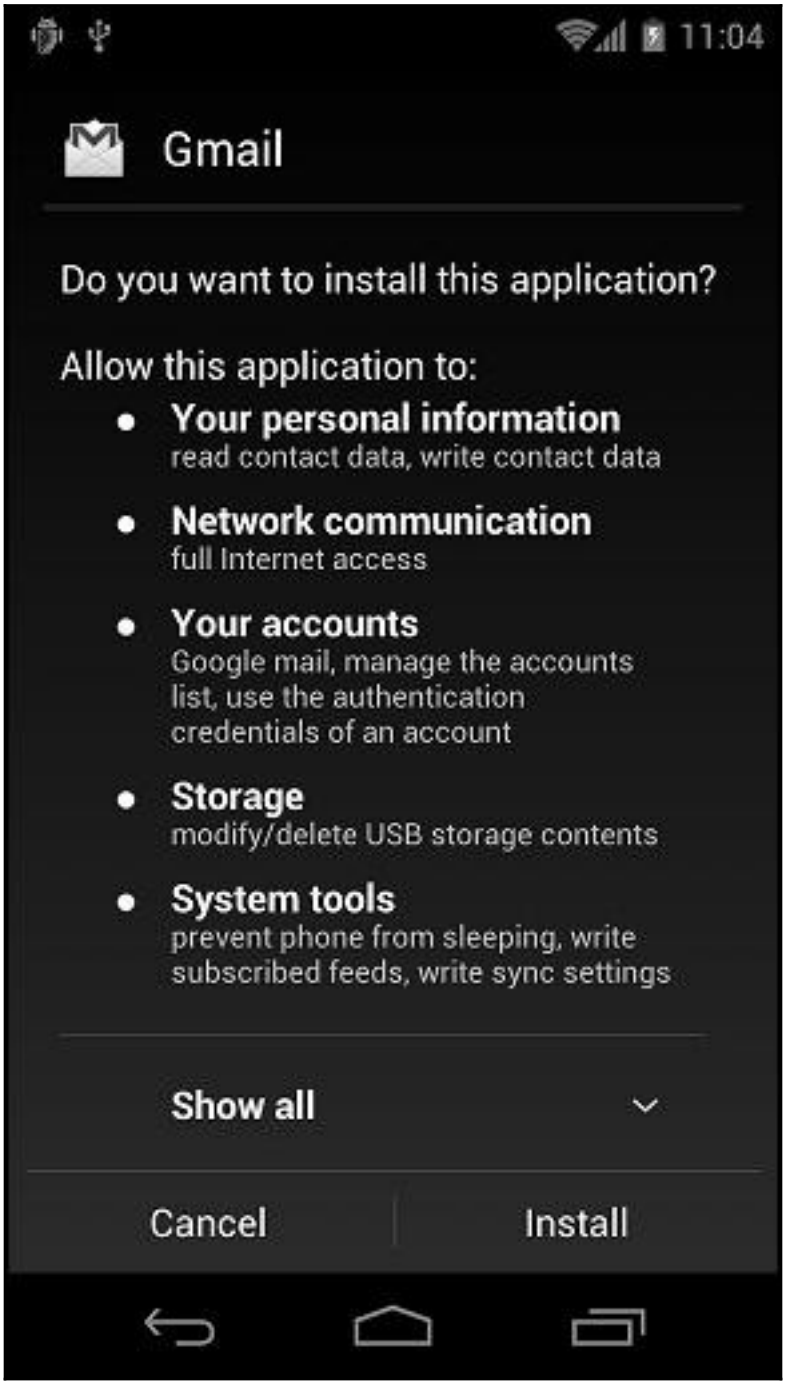

Oxygen Forensic® Extractor v.10.0.0.81
Oxygen Forensic® Extractor
Wait while the data is being extracted from the device
Extracting data...
Data extraction using iTunes backup procedure...
Extracting iTunes backup...
Waiting for complete iTunes backup extraction...
Warning! The data is being extracted from the device right now. Do not disconnect it or make any changes to the device.
Help
Cancel


Common sections (23)
Device Information
Aggregated Contacts
Cloud Accounts
Dictionaries
Event Log
File Browser
Key Evidence
Links and Stats
Media
Audio Images Video
Messages
Organizer
Calendar Notes
Passwords
Phonebook
Reports
Search
Social Graph
Timeline
Watch lists
Web Connections
WebKit Data
Applications (15)
Applications
Messengers
Skype Telegram WhatsApp Messenger
Multimedia
YouTube
Navigation
Google Maps
Productivity (Business)
Apple Notes iBooks Mail.Ru - Email App
Social Networks
Instagram LinkedIn Snapchat Twitter VK
Web Browsers
Google Chrome Safari Browser

Chapter 7: Understanding Android




JAVA SOURCE CODE
Java Compiler
JAVA BYTE CODE
JAVA VM
JAVA SOURCE CODE
Java Compiler
JAVA BYTE CODE
Dex compiler
Dalvik byte code
Dalvik VM


11:04
Gmail
Do you want to install this application?
Allow this application to:
Your personal information
read contact data, write contact data
Network communication
full Internet access
Your accounts
Google mail, manage the accounts list, use the authentication credentials of an account
Storage
modify/delete USB storage contents
System tools
prevent phone from sleeping, write subscribed feeds, write sync settings
Show all
Cancel
Install

```
root@android:/data # cd /system
root@android:/system # ls
CSCVersion.txt
SW_Configuration.xml
app
bin
build.prop
cameradata
csc
csc_contents
etc
fonts
framework
hdic
lib
media
sipdb
tts
usr
vendor
voicebargeindata
vsc
wakeupdata
wallpaper
xbin
```

```
root@android:/ # cd /data
root@android:/data # ls
ISP_CV
TMAudioSocketClient
TMAudioSocketServer
anr
app
app-asec
app-private
backup
baro.dat
cfw
clipboard
dalvik-cache
data
dontpanic
drm
fota_test
gldata.sto
gps
hidden_volume.txt
lbsdata-000.sto
local
log
lost+found
media
misc
```

```
root@android:/ # cat /proc/filesystems
nodev   sysfs
nodev   rootfs
nodev   bdev
nodev   proc
nodev   cgroup
nodev   tmpfs
nodev   binfmt_misc
nodev   debugfs
nodev   sockfs
nodev   usbfs
nodev   pipefs
nodev   anon_inodefs
nodev   devpts
        ext2
        ext3
        ext4
nodev   ramfs
        vfat
        msdos
nodev   ecryptfs
nodev   fuse
        fuseblk
nodev   fusectl
        exfat
```

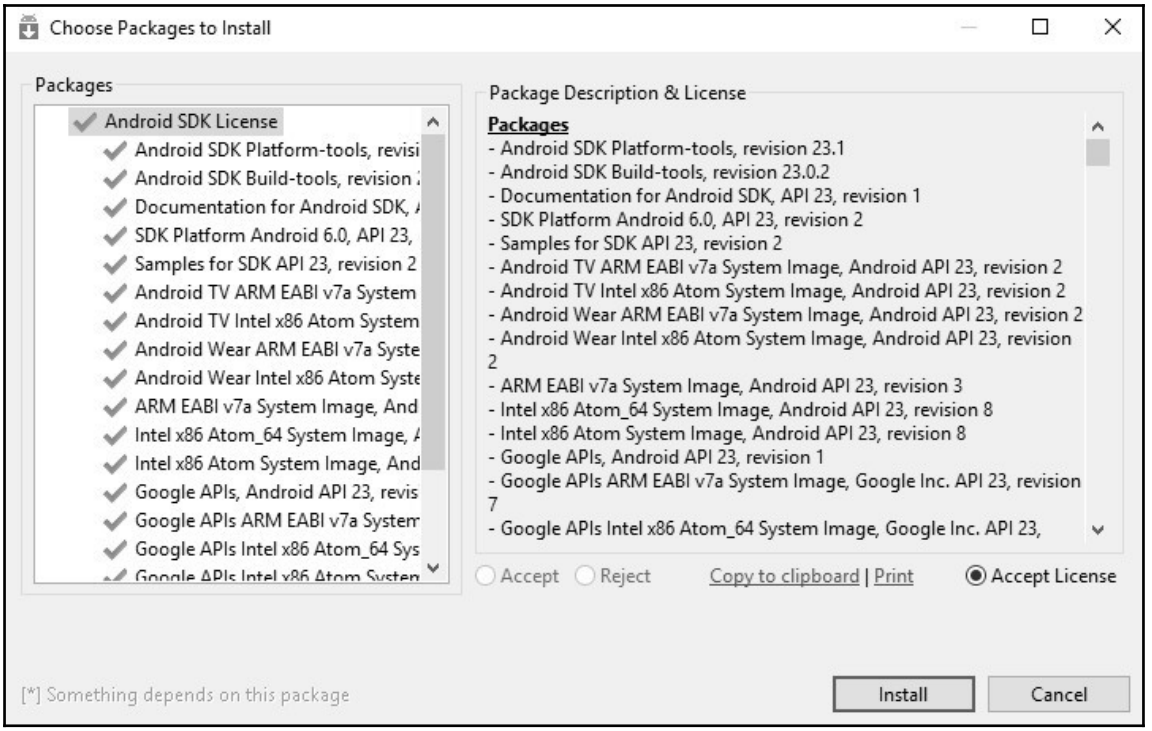
```
root@android:/ # mount
rootfs / rootfs ro,relatime 0 0
tmpfs /dev tmpfs rw,nosuid,relatime,mode=755 0 0
devpts /dev/pts devpts rw,relatime,mode=600 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,relatime 0 0
none /acct cgroup rw,relatime,cpuacct 0 0
tmpfs /mnt/asec tmpfs rw,relatime,mode=755,gid=1000 0 0
tmpfs /mnt/obb tmpfs rw,relatime,mode=755,gid=1000 0 0
none /dev/cpuctl cgroup rw,relatime,cpu 0 0
/dev/block/mmcblk0p9 /system ext4 ro,noatime,barrier=1,data=ordered 0 0
/dev/block/mmcblk0p3 /efs ext4 rw,nosuid,nodev,noatime,barrier=1,journal_async_commit,data=ordered 0 0
/dev/block/mmcblk0p8 /cache ext4 rw,nosuid,nodev,noatime,errors=panic,barrier=1,journal_async_commit,data=ordered 0 0
/dev/block/mmcblk0p12 /data ext4 rw,nosuid,nodev,noatime,barrier=1,journal_async_commit,data=ordered,noauto_da_alloc,discard 0 0
/sys/kernel/debug /sys/kernel/debug debugfs rw,relatime 0 0
/dev/fuse /storage/sdcard0 fuse rw,nosuid,nodev,noexec,relatime,user_id=1023,group_id=1023,default_permissions,allow_other 0 0
```

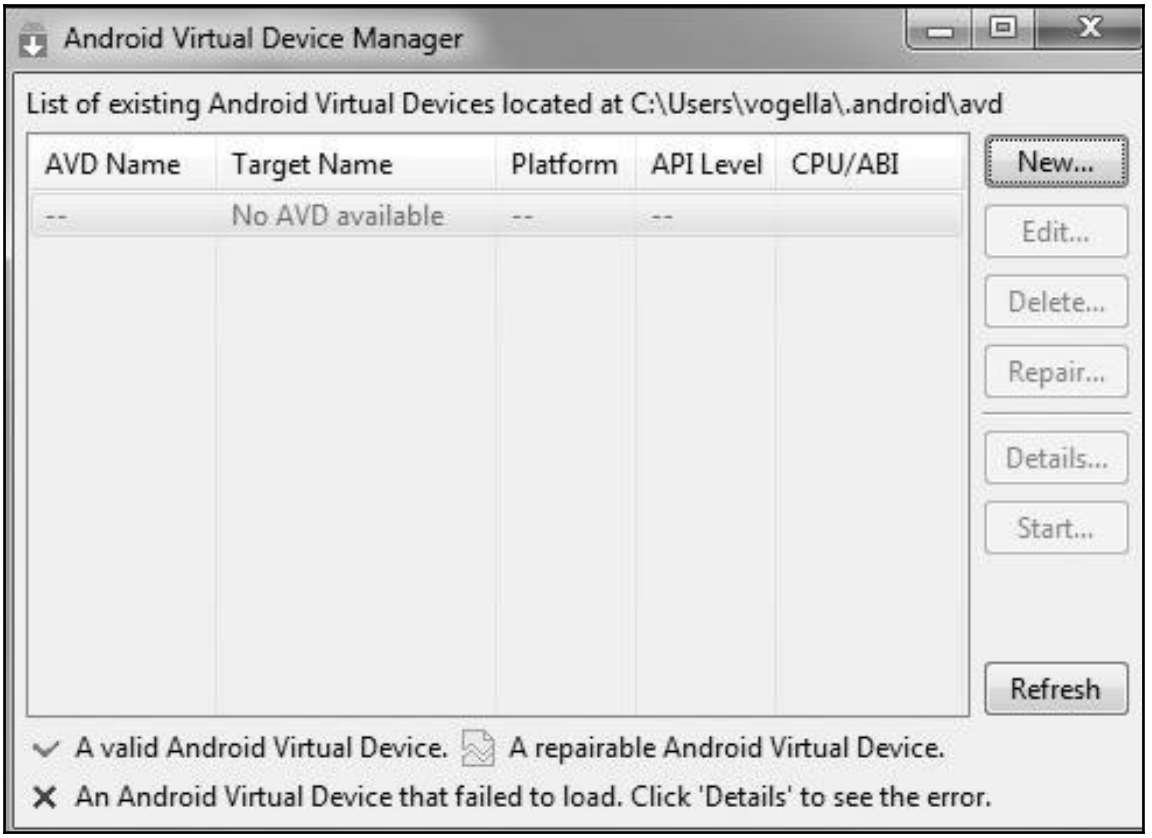
```
root@android:/ # cd /sys
root@android:/sys # ls
block
bus
class
dev
devices
firmware
fs
kernel
module
power
```

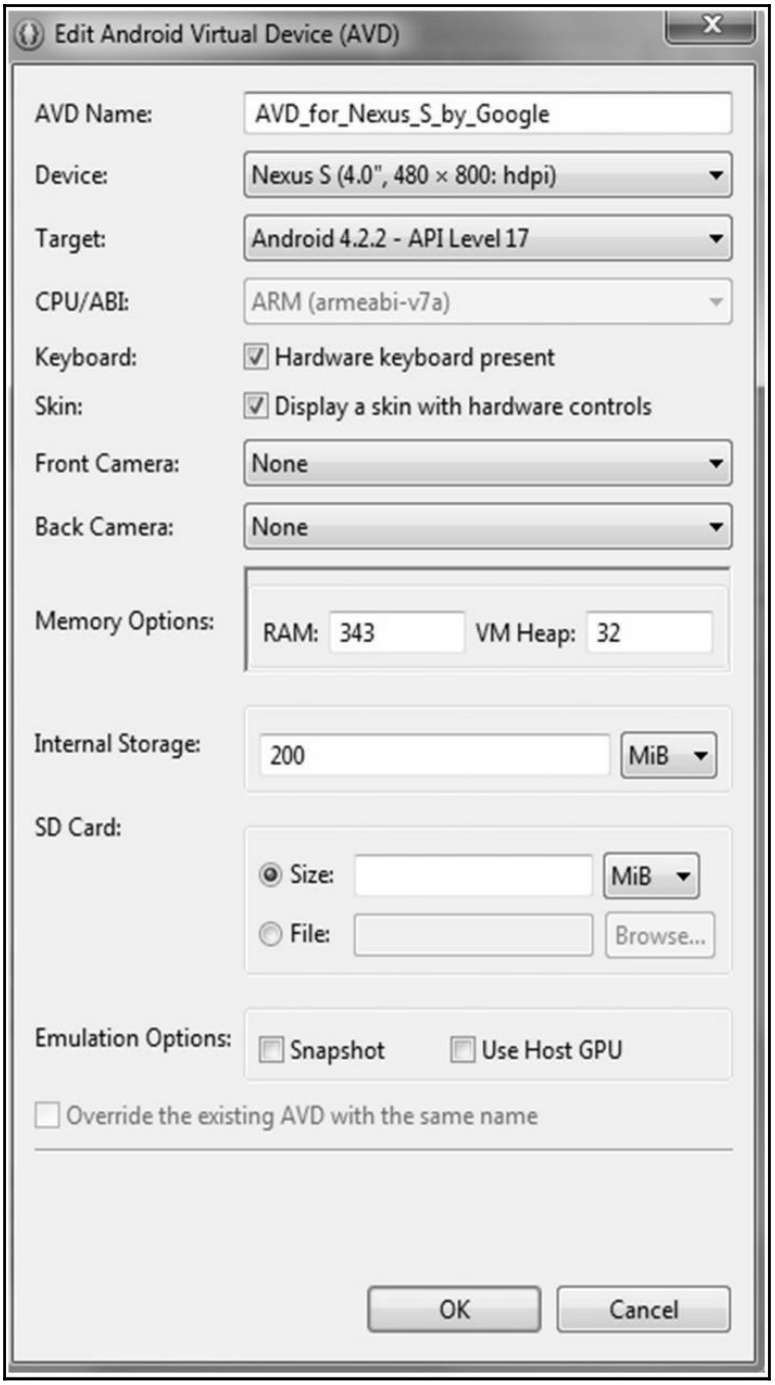
```
root@android:/ # cat /proc/cpuinfo
Processor       : ARMv7 Processor rev 0 (v7l)
processor       : 0
BogoMIPS        : 1592.52

processor       : 2
BogoMIPS        : 1990.65

processor       : 3
BogoMIPS        : 1990.65

Features        : swp half thumb fastmult vfp edsp neon vfpv3 tls
CPU implementer : 0x41
CPU architecture: 7
CPU variant     : 0x3
CPU part        : 0xc09
CPU revision    : 0

Chip revision   : 0011
Hardware        : SMDK4x12
Revision        : 000c
Serial          : [redacted]
```

```
root@android:/ # cd sdcard
root@android:/sdcard # mount
rootfs / rootfs ro,relatime 0 0
tmpfs /dev tmpfs rw,nosuid,relatime,mode=755 0 0
devpts /dev/pts devpts rw,relatime,mode=600 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,relatime 0 0
none /acct cgroup rw,relatime,cpuacct 0 0
tmpfs /mnt/asec tmpfs rw,relatime,mode=755,gid=1000 0 0
tmpfs /mnt/obb tmpfs rw,relatime,mode=755,gid=1000 0 0
none /dev/cpuctl cgroup rw,relatime,cpu 0 0
/dev/block/mmcblk0p9 /system ext4 ro,noatime,barrier=1,data=ordered 0 0
/dev/block/mmcblk0p3 /efs ext4 rw,nosuid,nodev,noatime,barrier=1,journal_async_commit,data=ordered 0 0
/dev/block/mmcblk0p8 /cache ext4 rw,nosuid,nodev,noatime,errors=panic,barrier=1,journal_async_commit,data=ordered 0 0
/dev/block/mmcblk0p12 /data ext4 rw,nosuid,nodev,noatime,barrier=1,journal_async_commit,data=ordered,noauto_da_alloc,discard 0 0
/sys/kernel/debug /sys/kernel/debug debugfs rw,relatime 0 0
/dev/fuse /storage/sdcard0 fuse rw,nosuid,nodev,noexec,relatime,user_id=1023,group_id=1023,default_permissions,allow_other 0 0
```

Chapter 8: Android Forensic Setup and Pre-Data Extraction Techniques

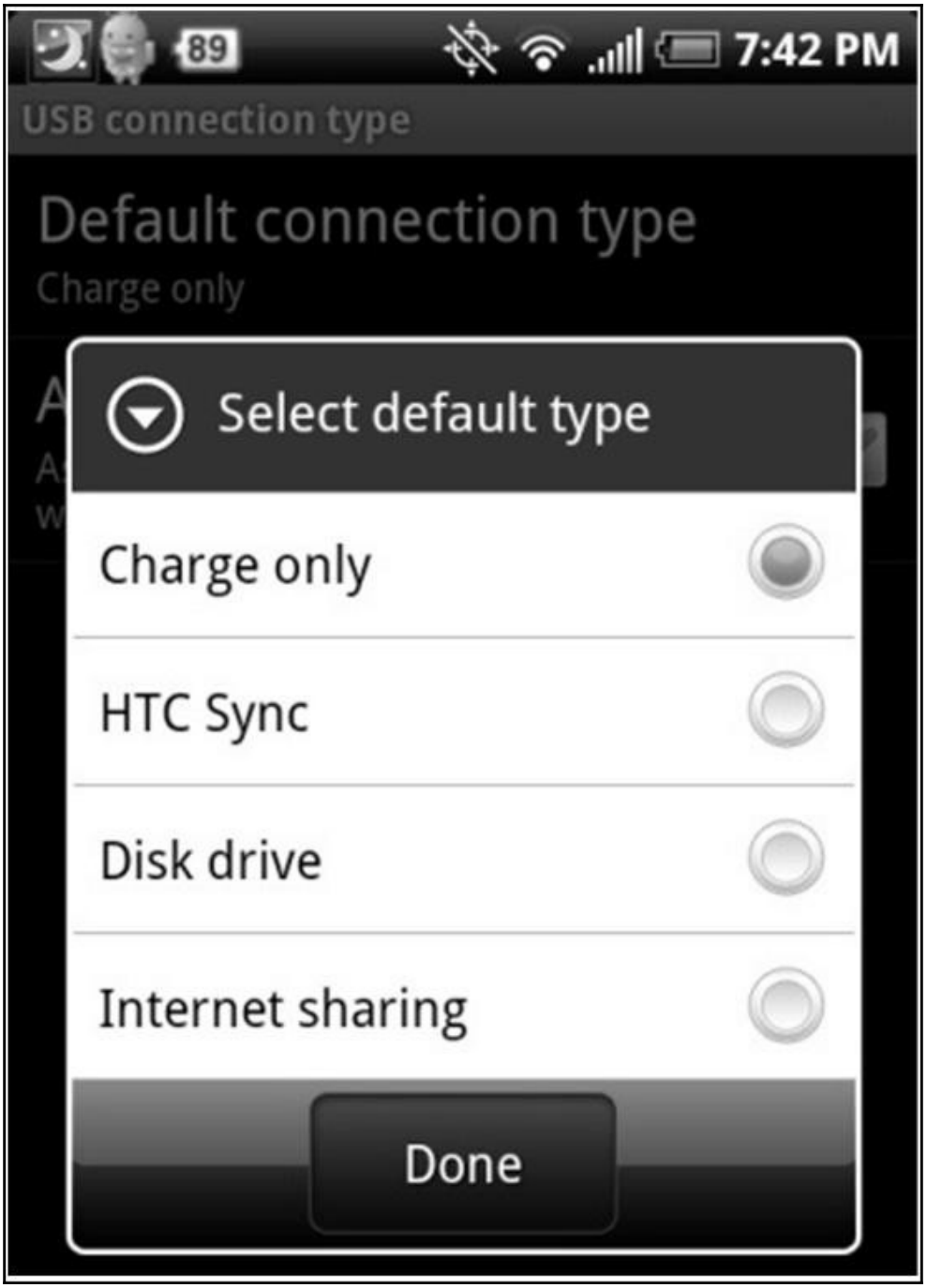

Choose Packages to Install
Packages
Android SDK License
Android SDK Platform-tools, revisi
Android SDK Build-tools, revision
Documentation for Android SDK,
SDK Platform Android 6.0, API 23,
Samples for SDK API 23, revision 2
Android TV ARM EABI v7a System
Android TV Intel x86 Atom System
Android Wear ARM EABI v7a Syste
Android Wear Intel x86 Atom Syste
ARM EABI v7a System Image, And
Intel x86 Atom_64 System Image,
Intel x86 Atom System Image, And
Google APIs, Android API 23, revis
Google APIs ARM EABI v7a System
Google APIs Intel x86 Atom_64 Sys
Package Description & License
Packages
- Android SDK Platform-tools, revision 23.1
- Android SDK Build-tools, revision 23.0.2
- Documentation for Android SDK, API 23, revision 1
- SDK Platform Android 6.0, API 23, revision 2
- Samples for SDK API 23, revision 2
- Android TV ARM EABI v7a System Image, Android API 23, revision 2
- Android TV Intel x86 Atom System Image, Android API 23, revision 2
- Android Wear ARM EABI v7a System Image, Android API 23, revision 2
- Android Wear Intel x86 Atom System Image, Android API 23, revision 2
- ARM EABI v7a System Image, Android API 23, revision 3
- Intel x86 Atom_64 System Image, Android API 23, revision 8
- Intel x86 Atom System Image, Android API 23, revision 8
- Google APIs, Android API 23, revision 1
- Google APIs ARM EABI v7a System Image, Google Inc. API 23, revision 7
- Google APIs Intel x86 Atom_64 System Image, Google Inc. API 23,
Accept
Reject
Copy to clipboard | Print
Accept License
[*] Something depends on this package
Install
Cancel

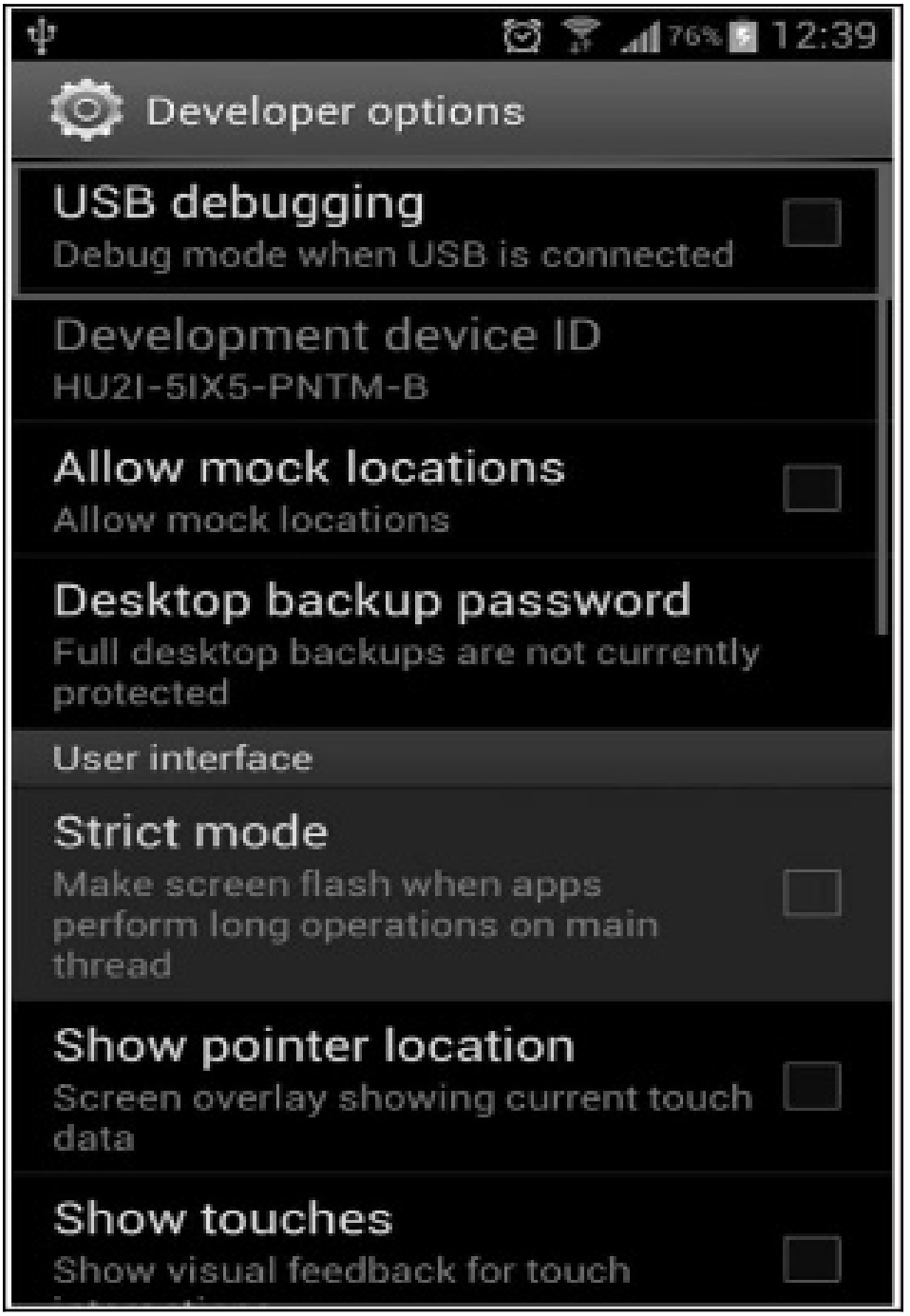

Android Virtual Device Manager
List of existing Android Virtual Devices located at C:\Users\vogella\.android\avd
AVD Name
Target Name
Platform
API Level
CPU/ABI
--
No AVD available
--
--
New...
Edit...
Delete...
Repair...
Details...
Start...
Refresh
A valid Android Virtual Device.
A repairable Android Virtual Device.
An Android Virtual Device that failed to load. Click 'Details' to see the error.

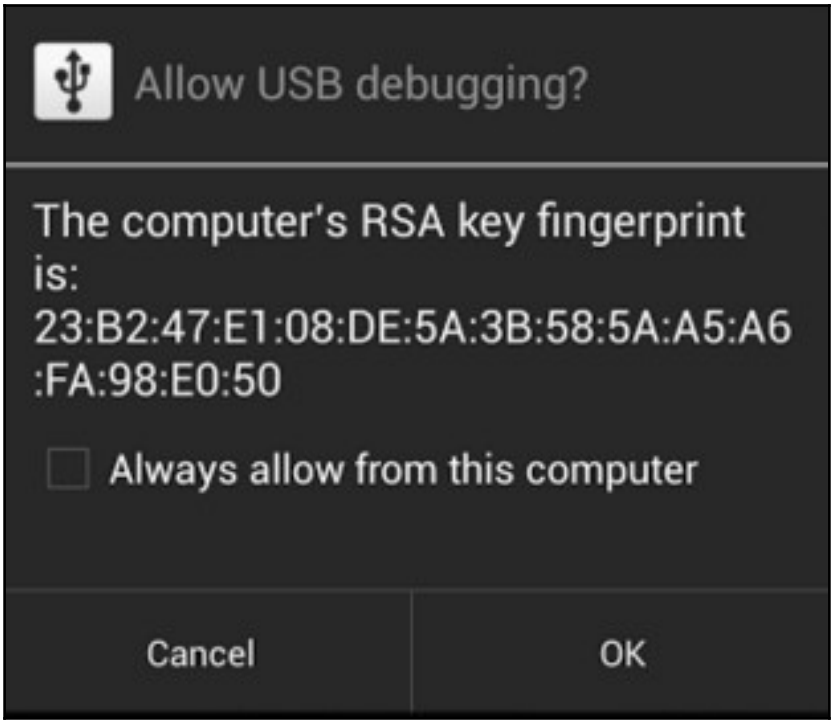

Edit Android Virtual Device (AVD)
AVD Name:
AVD_for_Nexus_S_by_Google
Device:
Nexus S (4.0", 480 × 800: hdpi)
Target:
Android 4.2.2 - API Level 17
CPU/ABI:
ARM (armeabi-v7a)
Keyboard:
Hardware keyboard present
Skin:
Display a skin with hardware controls
Front Camera:
None
Back Camera:
None
Memory Options:
RAM: 343
VM Heap: 32
Internal Storage:
200
MiB
SD Card:
Size:
MiB
File:
Browse...
Emulation Options:
Snapshot
Use Host GPU
Override the existing AVD with the same name
OK
Cancel


5554:ForensicsAVD
12:40
Google
Basic Controls
Hardware Buttons
MENU
DPAD not enabled in AVD
Hardware Keyboard
Use your physical keyboard to provide input


USB Mass Storage
USB connected
You have connected to your computer via USB. Touch the button below if you want to copy files between your computer and your Android's USB storage.
Turn on USB storage


89
7:42 PM
USB connection type
Default connection type
Charge only
Select default type
Charge only
HTC Sync
Disk drive
Internet sharing
Done

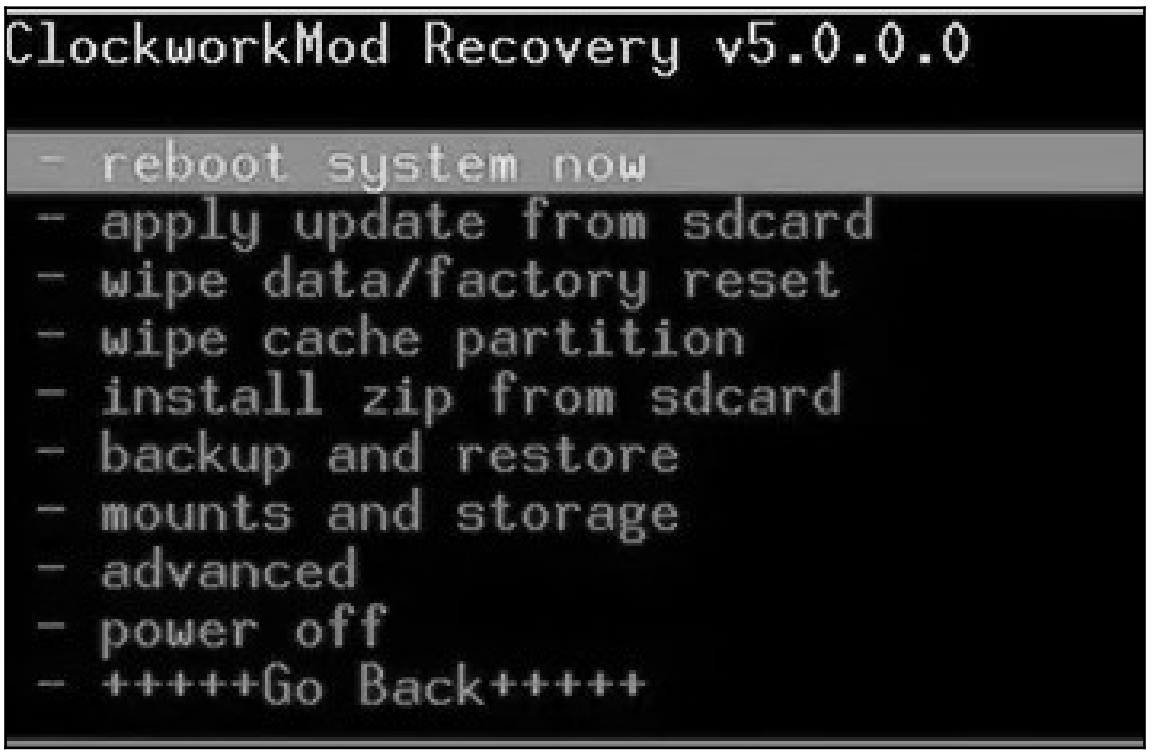

76% 12:39
Developer options
USB debugging
Debug mode when USB is connected
Development device ID
HU2I-5IX5-PNTM-B
Allow mock locations
Allow mock locations
Desktop backup password
Full desktop backups are not currently protected
User interface
Strict mode
Make screen flash when apps perform long operations on main thread
Show pointer location
Screen overlay showing current touch data
Show touches
Show visual feedback for touch



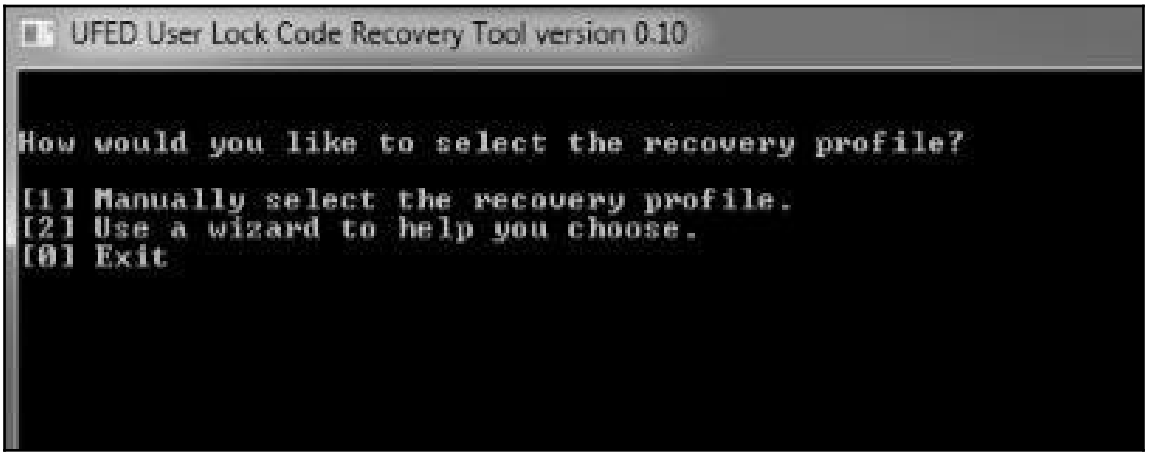

```
C:\android-sdk\platform-tools>adb.exe devices
List of devices attached
4df16ac3115e5f05        device
```

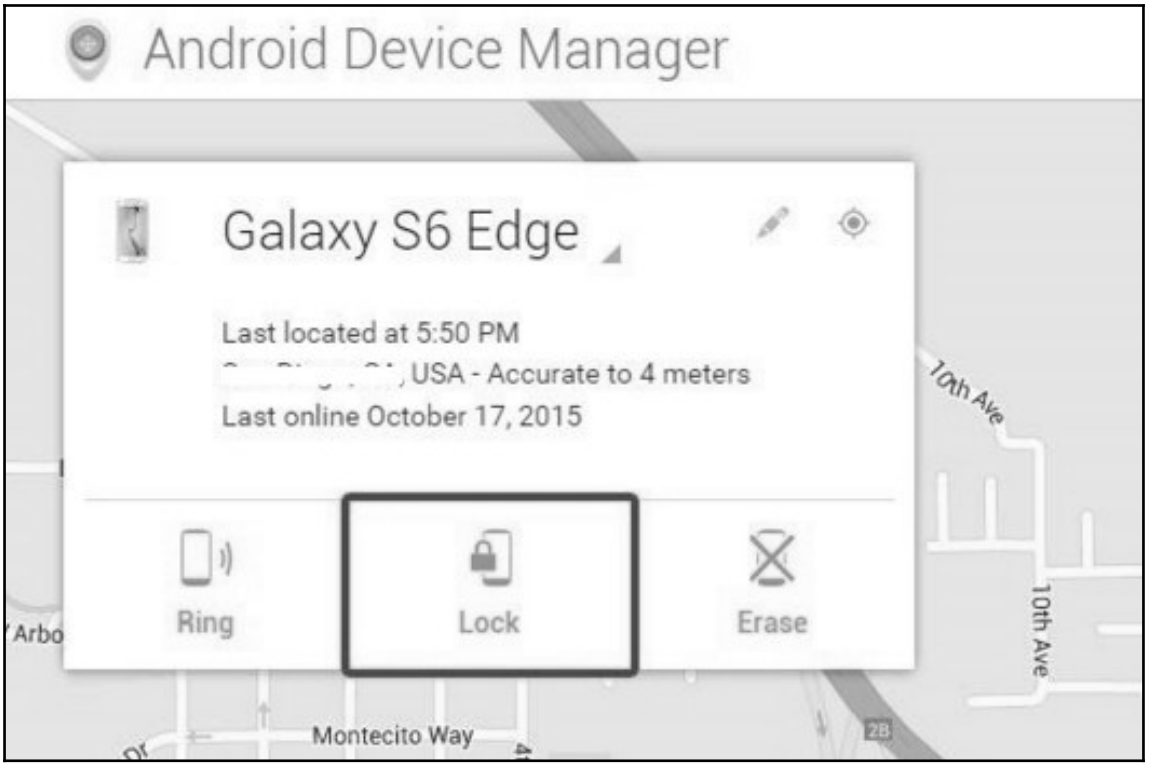
```
C:\android-sdk\platform-tools>adb.exe devices
List of devices attached
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
4df16ac3115e5f05        device
```

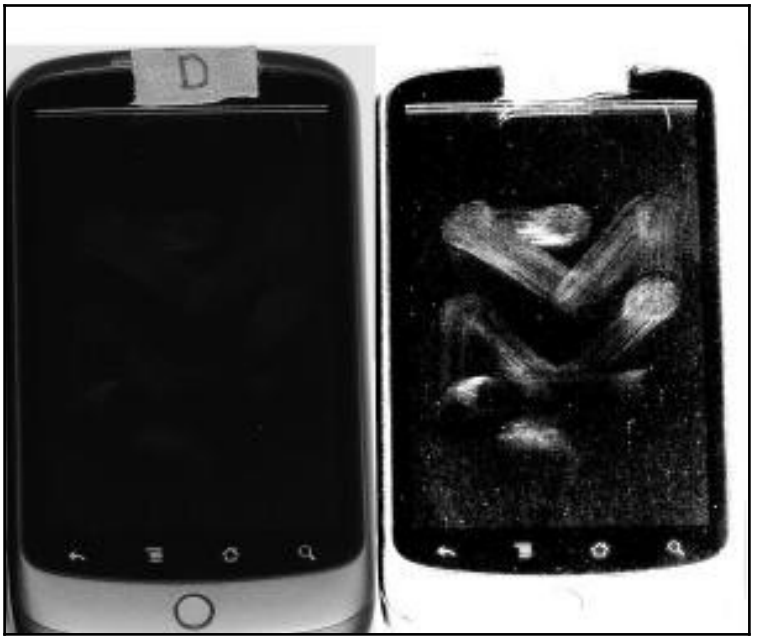
```
[redacted]:/ $ cd /data/data/com.android.providers.settings/databases
    sqlite3 settings.db
    update system set value=0 where name='lock_pattern_autolock';
c    update secure set value=0 where name='lock_pattern_autolock';
d /data/data/com.android.providers.settings/databases
    update system set value=0 where name='lockscreen.lockedoutpermanently';
     update secure set value=0 where name='lockscreen.lockedoutpermanently';
   sqlite3 settings.db
    .quit
     exit
```

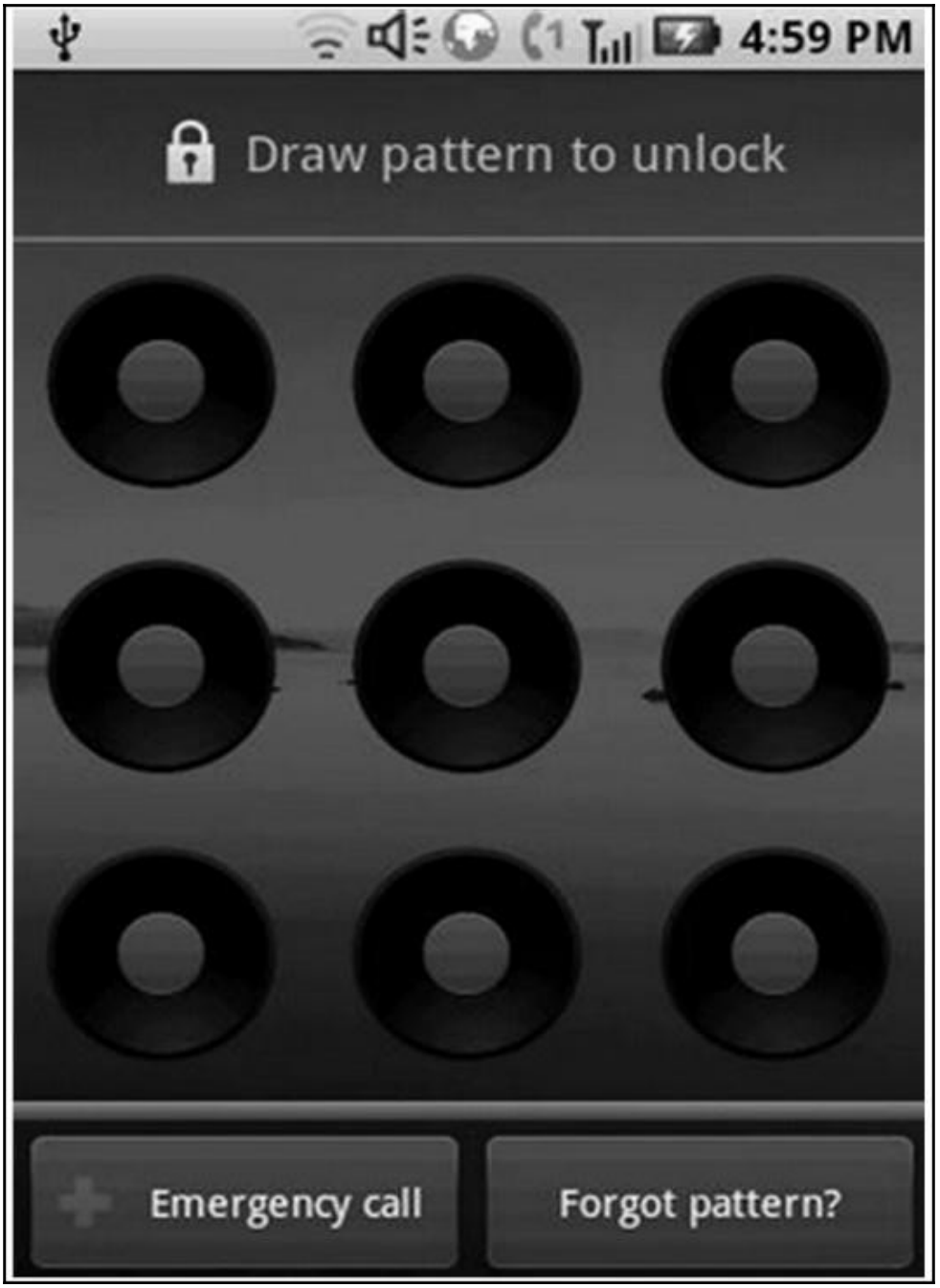


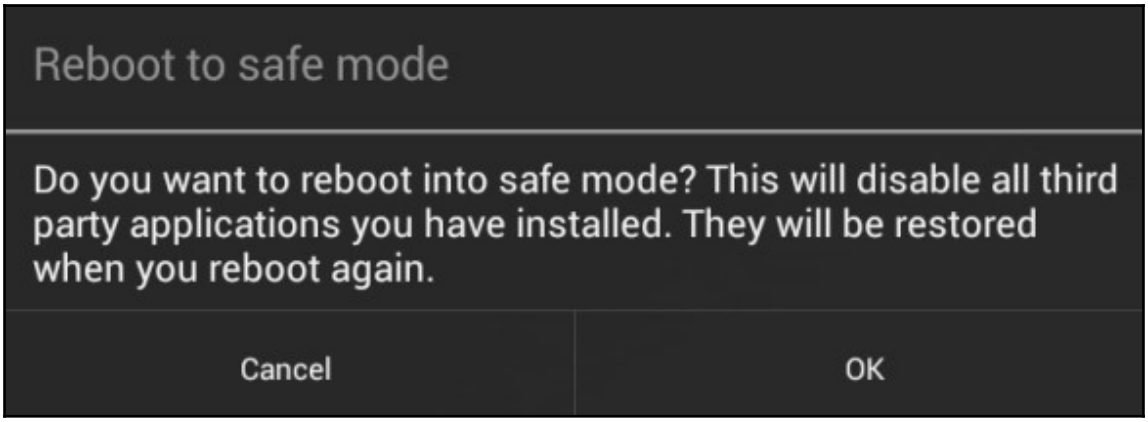
```
UFED User Lock Code Recovery Tool

Disclaimer: All actions are subject to the full responsibility of the user, and
Cellebrite is not liable for any damage to the device.

Follow the instructions to recover the lock code.

Before you begin, check your computer's power options to make sure it won't go
into sleep mode. The process could take from a few minutes up to 21 hours. You
can still use the computer during this time.


What type of device is it?

[1] Android
[2] iOS (Apple)
[0] Exit
```

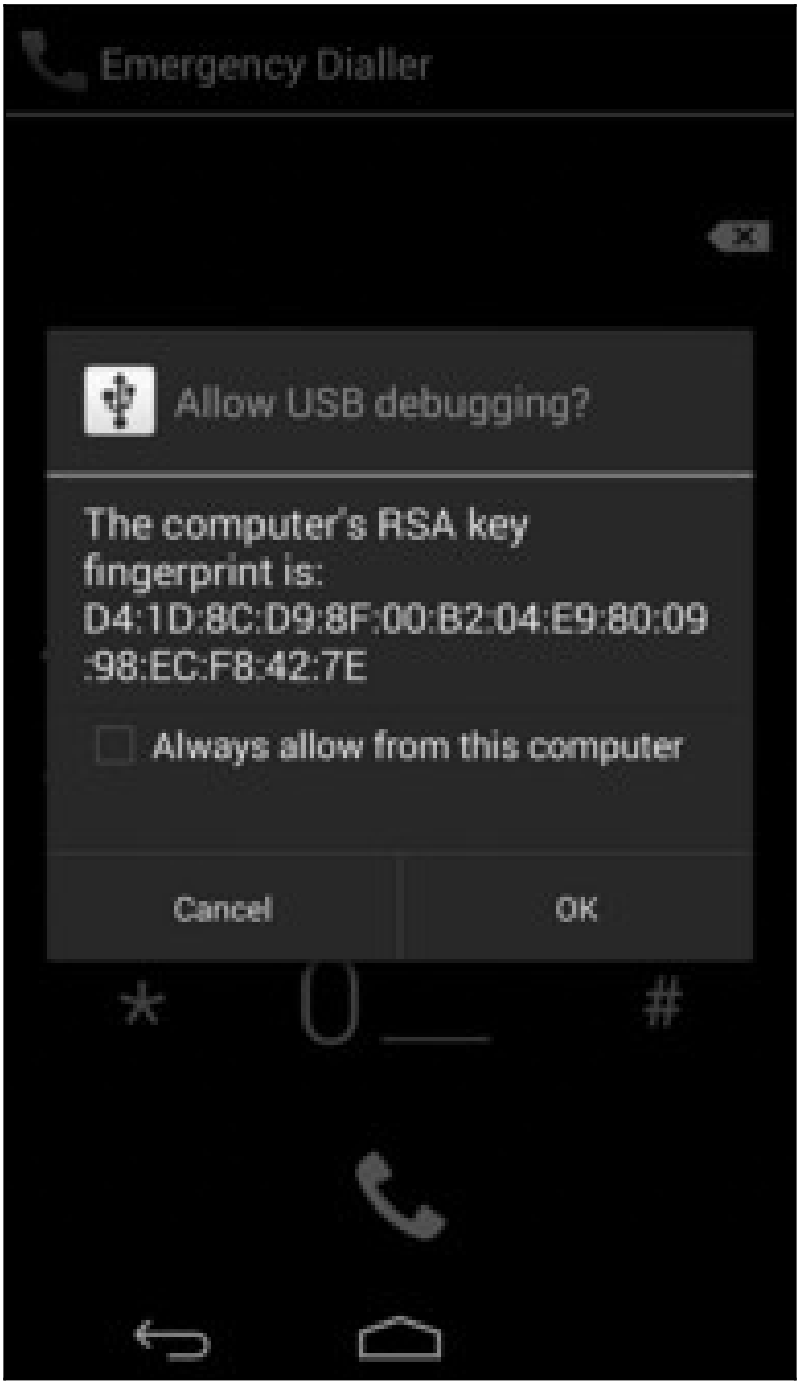


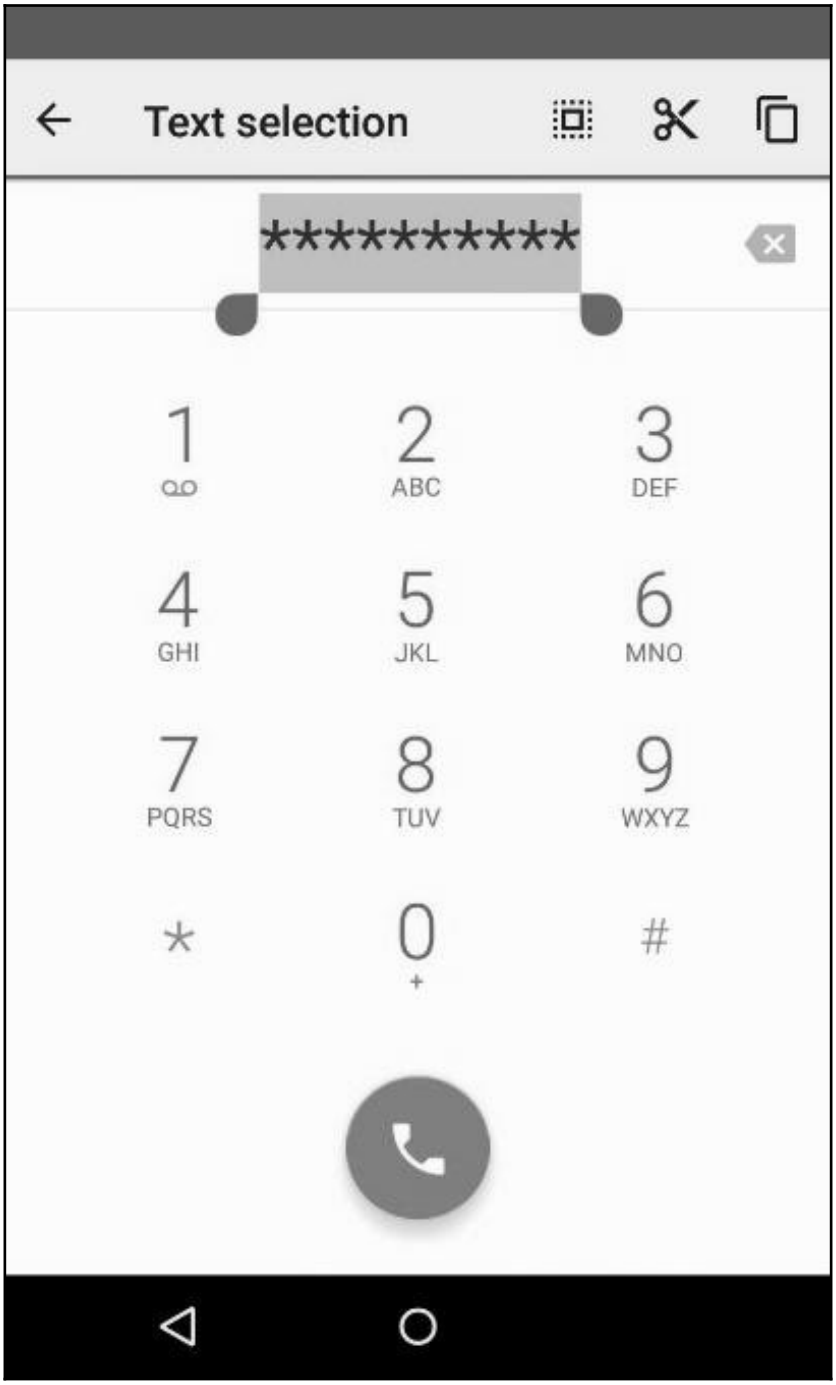

Android Device Manager
Galaxy S6 Edge
Last located at 5:50 PM
USA - Accurate to 4 meters
Last online October 17, 2015
Ring
Lock
Erase
10th Ave
10th Ave
Montecito Way
28

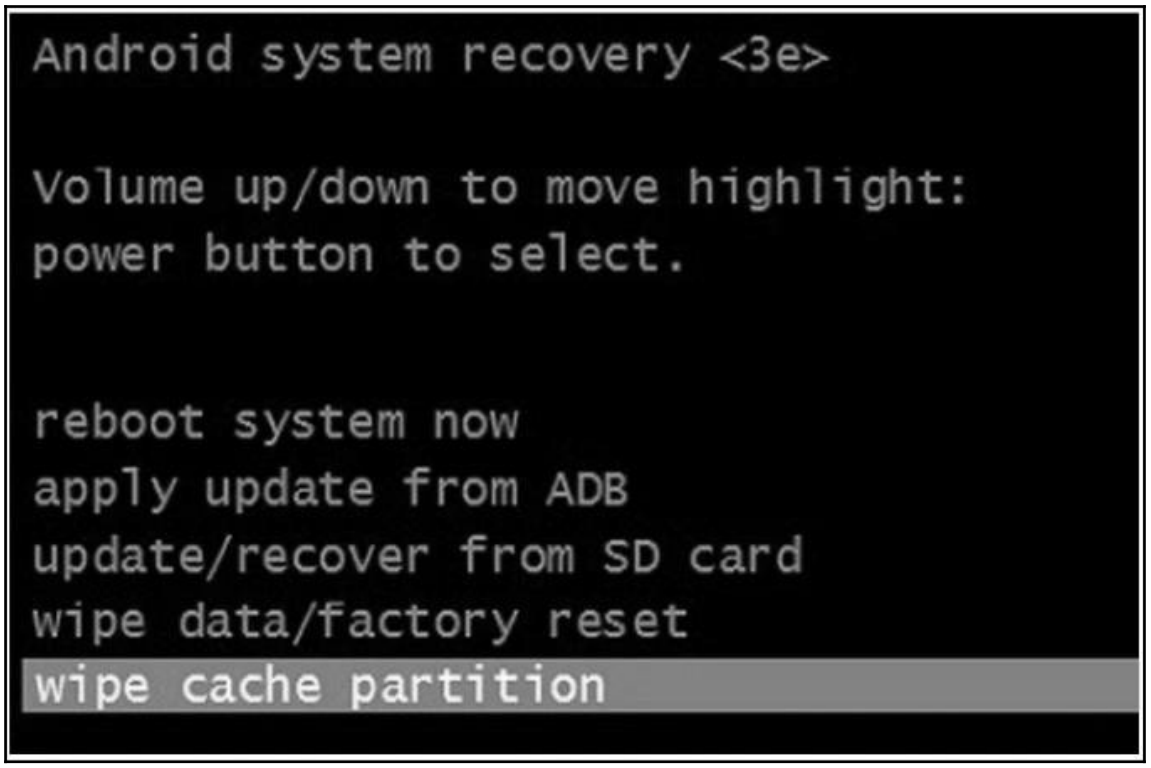

D

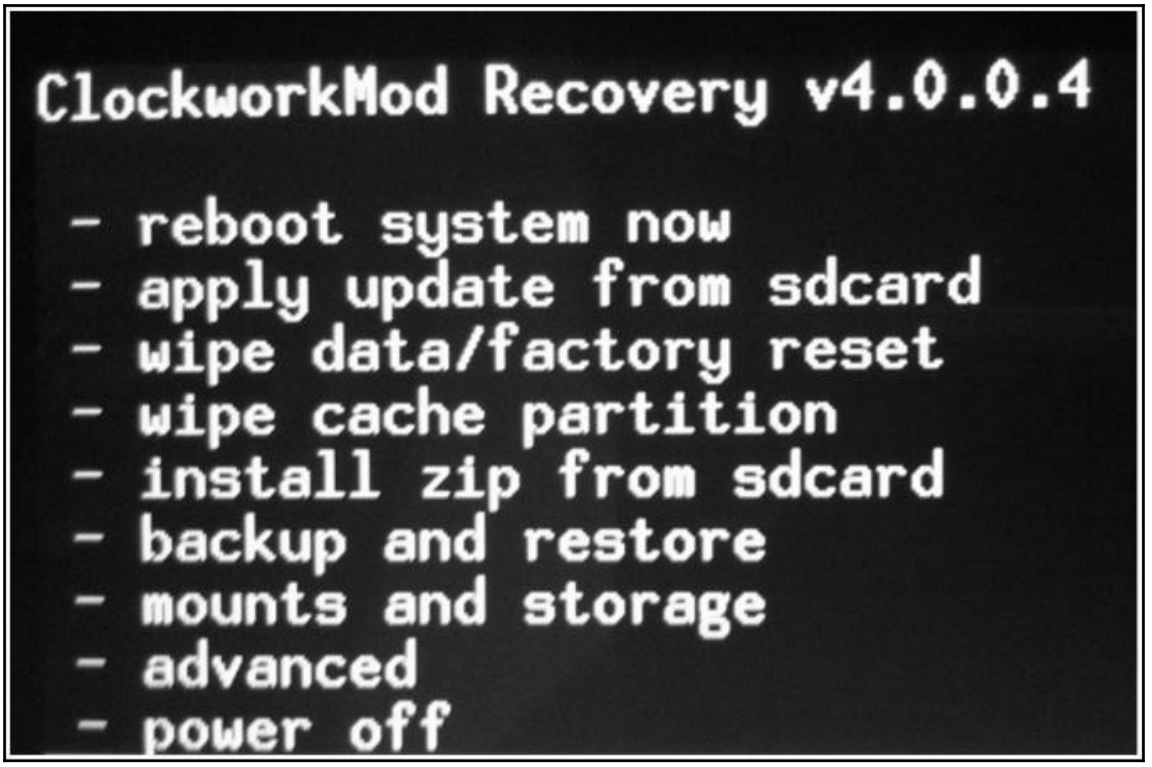

4:59 PM
Draw pattern to unlock
Emergency call
Forgot pattern?

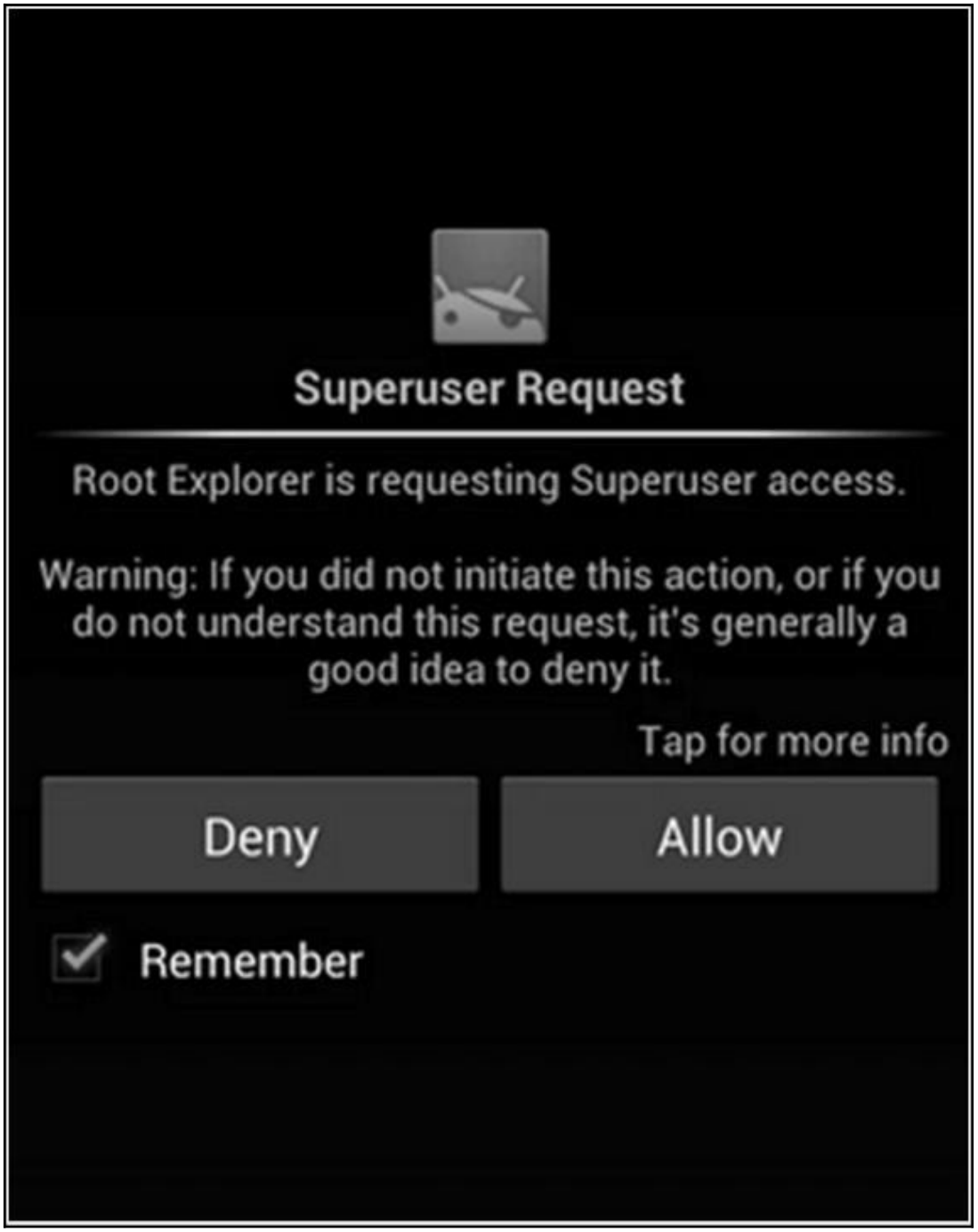

Reboot to safe mode
Do you want to reboot into safe mode? This will disable all third party applications you have installed. They will be restored when you reboot again.
Cancel
OK


Emergency Dialler
Allow USB debugging?
The computer's RSA key fingerprint is:
D4:1D:8C:D9:8F:00:B2:04:E9:80:09:98:EC:F8:42:7E
Always allow from this computer
Cancel
OK


Text selection
****
1
2
ABC
3
DEF
4
GHI
5
JKL
6
MNO
7
PQRS
8
TUV
9
WXYZ
*
0
+
#


Android system recovery <3e>
Volume up/down to move highlight:
power button to select.
reboot system now
apply update from ADB
update/recover from SD card
wipe data/factory reset
wipe cache partition


ClockworkMod Recovery v4.0.0.4
- reboot system now
- apply update from sdcard
- wipe data/factory reset
- wipe cache partition
- install zip from sdcard
- backup and restore
- mounts and storage
- advanced
- power off

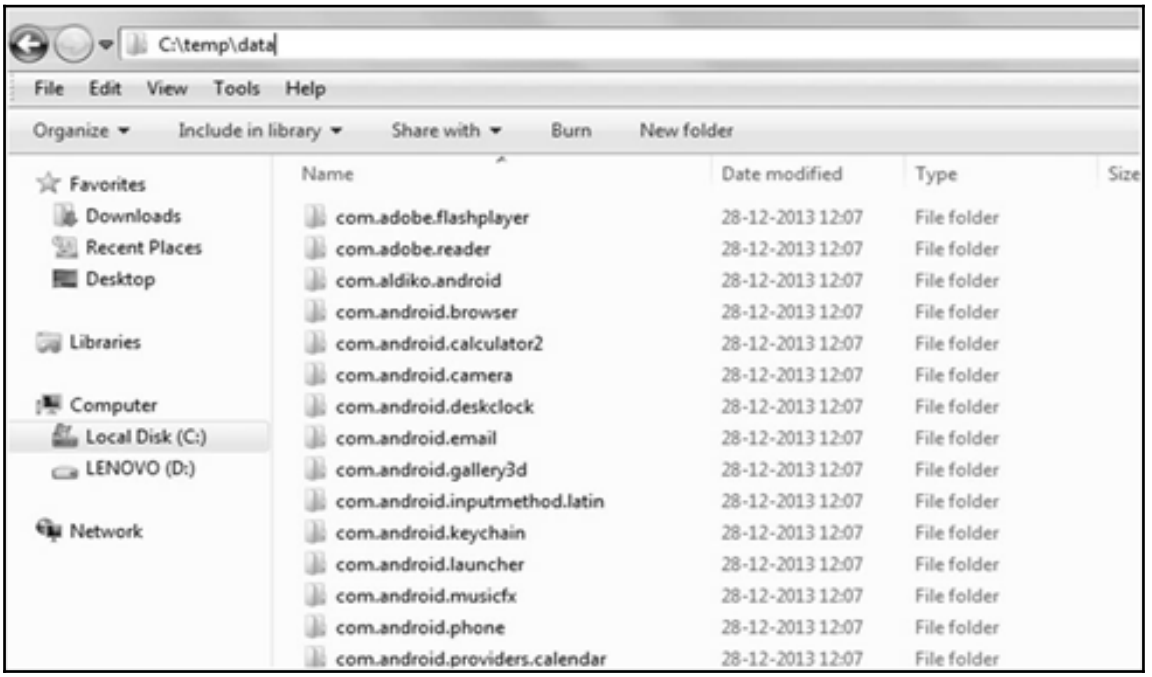

Superuser Request
Root Explorer is requesting Superuser access.
Warning: If you did not initiate this action, or if you do not understand this request, it's generally a good idea to deny it.
Tap for more info
Deny
Allow
Remember

```
C:\android-sdk\platform-tools>adb.exe shell
shell@android:/ $ cd /data/data
shell@android:/data/data $ ls
opendir failed, Permission denied
255|shell@android:/data/data $
```

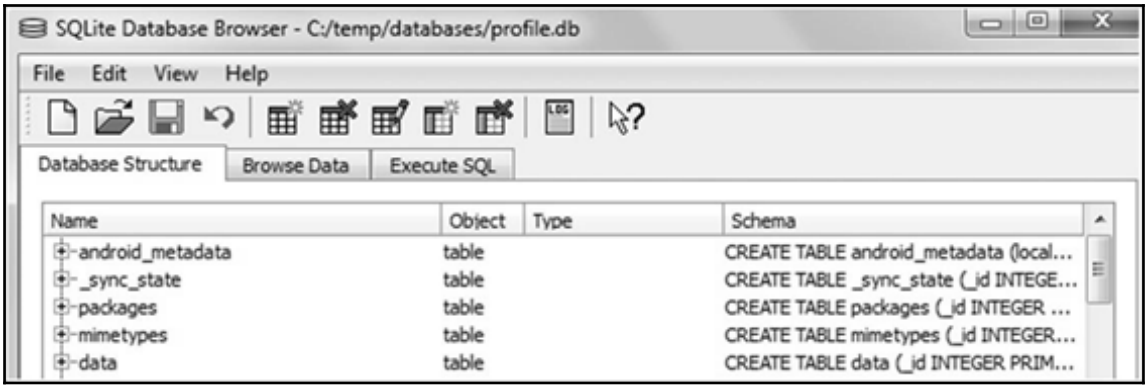
```
C:\android-sdk\platform-tools>adb.exe shell
root@android:/ # cd /data/data
root@android:/data/data # ls
android.googleSearch.googleSearchWidget
com.android.MtpApplication
com.android.Preconfig
com.android.apps.tag
com.android.backupconfirm
com.android.bluetooth
com.android.browser
```

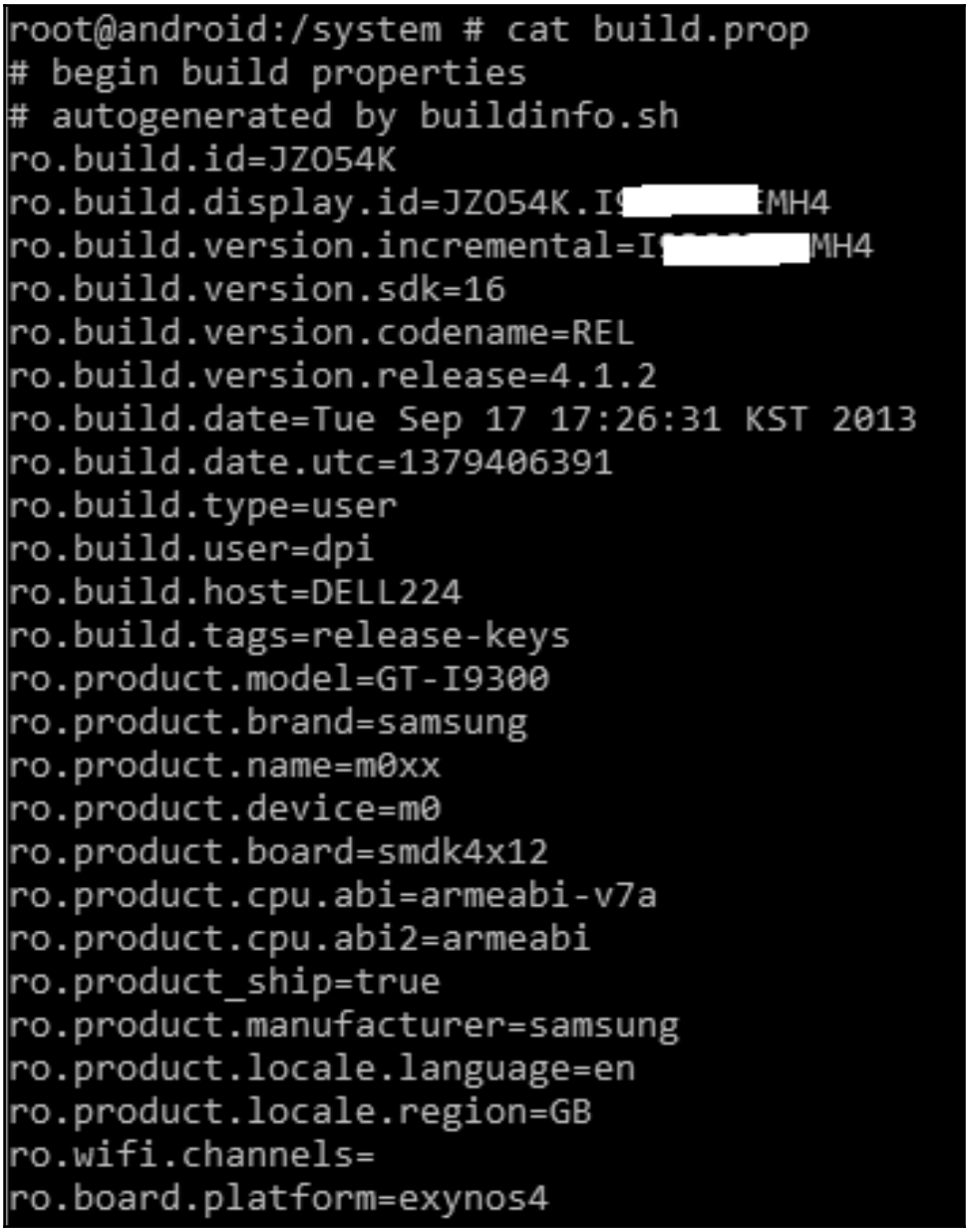
Chapter 9: Android Data Extraction Techniques

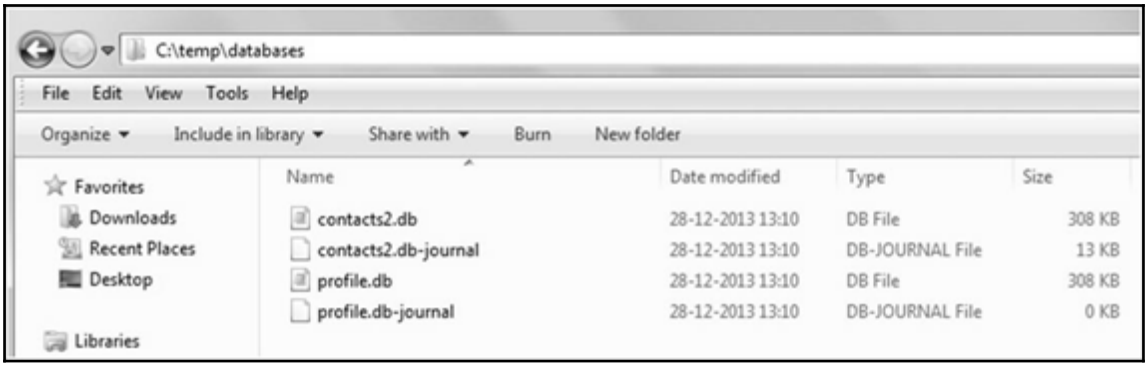
```
C:\android-sdk\platform-tools>adb.exe pull /data/data/com.dropbox.android/databases C:\temp
pull: building file list...
pull: /data/data/com.dropbox.android/databases/prefs.db-journal -> C:\temp/prefs.db-journal
pull: /data/data/com.dropbox.android/databases/prefs.db -> C:\temp/prefs.db
pull: /data/data/com.dropbox.android/databases/db.db-journal -> C:\temp/db.db-journal
pull: /data/data/com.dropbox.android/databases/db.db -> C:\temp/db.db
4 files pulled. 0 files skipped.
1753 KB/s (140352 bytes in 0.078s)
```



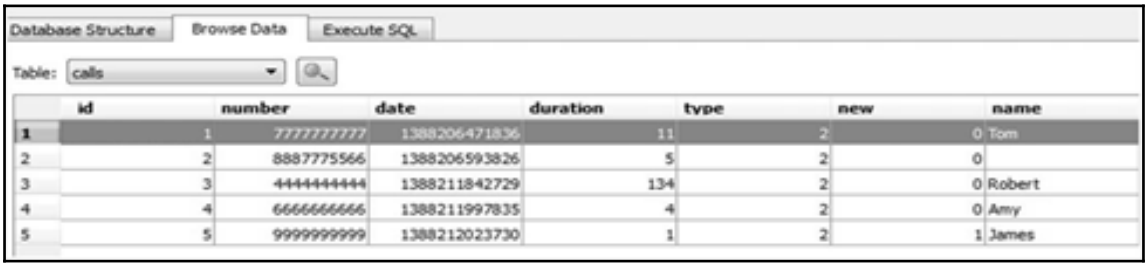

```
C:\android-sdk\platform-tools>adb.exe pull /data C:\temp
pull: building file list...
0 files pulled. 0 files skipped.
```


SQLite Database Browser - C:/temp/databases/profile.db
File Edit View Help
Database Structure
Browse Data
Execute SQL
Name
Object
Type
Schema
android_metadata
table
CREATE TABLE android_metadata (local...
_sync_state
table
CREATE TABLE _sync_state (_id INTEGE...
packages
table
CREATE TABLE packages (_id INTEGER ...
mimetypes
table
CREATE TABLE mimetypes (_id INTEGER...
data
table
CREATE TABLE data (_id INTEGER PRIM...


root@android:/system # cat build.prop
# begin build properties
# autogenerated by buildinfo.sh
ro.build.id=JZO54K
ro.build.display.id=JZO54K.I[redacted]MH4
ro.build.version.incremental=I[redacted]MH4
ro.build.version.sdk=16
ro.build.version.codename=REL
ro.build.version.release=4.1.2
ro.build.date=Tue Sep 17 17:26:31 KST 2013
ro.build.date.utc=1379406391
ro.build.type=user
ro.build.user=dpi
ro.build.host=DELL224
ro.build.tags=release-keys
ro.product.model=GT-I9300
ro.product.brand=samsung
ro.product.name=m0xx
ro.product.device=m0
ro.product.board=smdk4x12
ro.product.cpu.abi=armeabi-v7a
ro.product.cpu.abi2=armeabi
ro.product_ship=true
ro.product.manufacturer=samsung
ro.product.locale.language=en
ro.product.locale.region=GB
ro.wifi.channels=
ro.board.platform=exynos4




```
pull: /data/data/com.android.providers.contacts/databases/contacts2.db-mjF87EA798B -> C:\temp/databases/contacts2.db-mjF87EA798B
pull: /data/data/com.android.providers.contacts/databases/contacts2.db-mj7DE1FC9E3 -> C:\temp/databases/contacts2.db-mj7DE1FC9E3
pull: /data/data/com.android.providers.contacts/databases/contacts2.db-mj2151EE924 -> C:\temp/databases/contacts2.db-mj2151EE924
pull: /data/data/com.android.providers.contacts/databases/contacts2.db-mjABC96A935 -> C:\temp/databases/contacts2.db-mjABC96A935
pull: /data/data/com.android.providers.contacts/databases/profile.db-shm -> C:\temp/databases/profile.db-shm
pull: /data/data/com.android.providers.contacts/databases/profile.db-wal -> C:\temp/databases/profile.db-wal
pull: /data/data/com.android.providers.contacts/databases/profile.db -> C:\temp/databases/profile.db
pull: /data/data/com.android.providers.contacts/databases/contacts2.db-shm -> C:\temp/databases/contacts2.db-shm
pull: /data/data/com.android.providers.contacts/databases/contacts2.db-wal -> C:\temp/databases/contacts2.db-wal
pull: /data/data/com.android.providers.contacts/databases/contacts2.db -> C:\temp/databases/contacts2.db
pull: /data/data/com.android.providers.contacts/shared_prefs/com.android.providers.contacts_preferences.xml -> C:\temp/shared_prefs/com.android
rences.xml
pull: /data/data/com.android.providers.contacts/shared_prefs/ContactsUpgradeReceiver.xml -> C:\temp/shared_prefs/ContactsUpgradeReceiver.xml
pull: /data/data/com.android.providers.contacts/files/photos/2446 -> C:\temp/files/photos/2446
376 files pulled. 0 files skipped.
1820 KB/s (13795864 bytes in 7.398s)
```



	id	number	date	duration	type	new	name
1	1	7777777777	1388206471836	11	2	0	Tom
2	2	8887775566	1388206593826	5	2	0	
3	3	4444444444	1388211842729	134	2	0	Robert
4	4	6666666666	1388211997835	4	2	0	Amy
5	5	9999999999	1388212023730	1	2	1	James

```
C:\android-sdk\platform-tools>adb.exe pull /data/data/com.android.providers.telephony C:\temp
pull: building file list...
pull: /data/data/com.android.providers.telephony/databases/telephony.db-journal -> C:\temp/databases/telephony.db-journal
pull: /data/data/com.android.providers.telephony/databases/telephony.db -> C:\temp/databases/telephony.db
pull: /data/data/com.android.providers.telephony/databases/nwk_info.db-journal -> C:\temp/databases/nwk_info.db-journal
pull: /data/data/com.android.providers.telephony/databases/nwk_info.db -> C:\temp/databases/nwk_info.db
pull: /data/data/com.android.providers.telephony/databases/mmssms.db-shm -> C:\temp/databases/mmssms.db-shm
pull: /data/data/com.android.providers.telephony/databases/mmssms.db-wal -> C:\temp/databases/mmssms.db-wal
pull: /data/data/com.android.providers.telephony/databases/mmssms.db -> C:\temp/databases/mmssms.db
pull: /data/data/com.android.providers.telephony/shared_prefs/preferred-apn.xml -> C:\temp/shared_prefs/preferred-apn.xml
pull: /data/data/com.android.providers.telephony/optable.db -> C:\temp/optable.db
9 files pulled. 0 files skipped.
3096 KB/s (6193778 bytes in 1.953s)
```

address	person	date	date_sent	pro	re	stat	typ	re	sul	body
(999) 999-9999		1388223954060	0		1	-1	2			Hi.. Let's meet at 10 PM today
123	5	1388224802844	1388224803000	0	1	-1	1	0		Payment received
345	6	1388224888176	1388224888000	0	1	-1	1	0		Hello

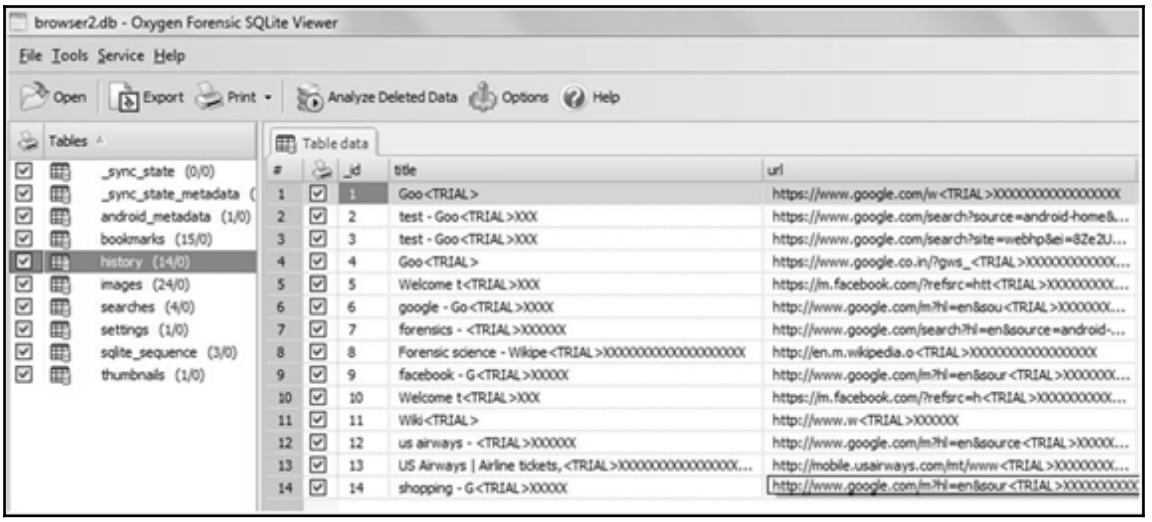
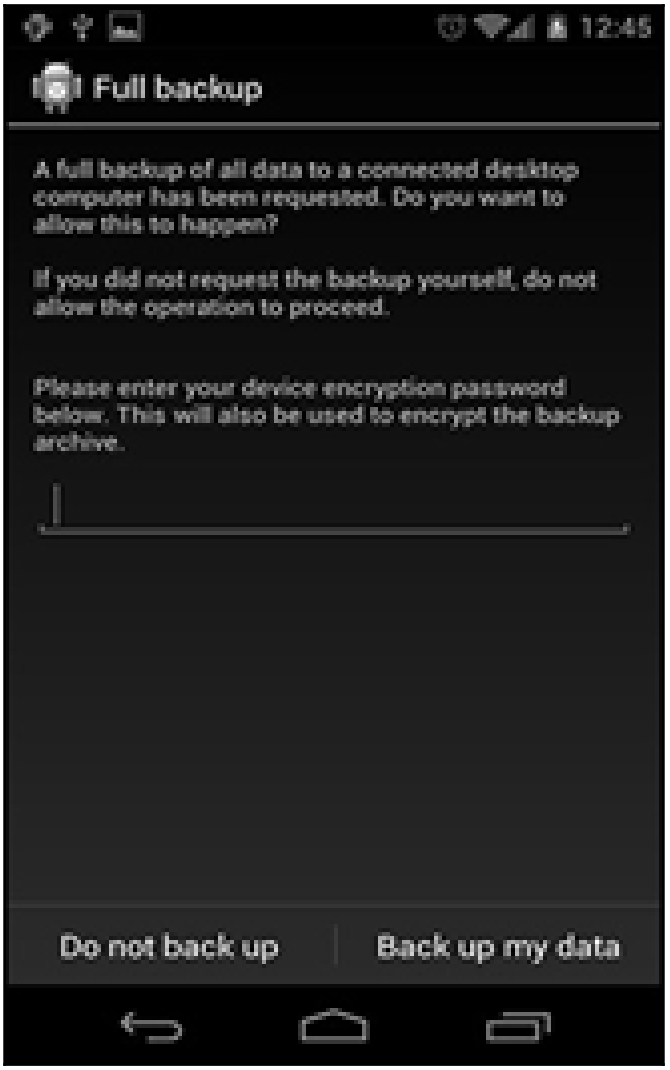


Table: friends_data

	id	user id	first name	last name	cell	other	email	birthday month
1	1	100004087623668	Lavanya				lavanyal_____@gn	2
2	2	100000005601801	Pranav	M				-1
3	3	100004630714031	Sujata	P	+91. _ _5			4
4	4	100000818058433	Sudha	C			sudaha_ @yah	1
5	5	100003499121241	Vasu	N	+91 _ 8		vasundl @y	7
6	6	100003191641871	Makka	A	+9 _ 9		i amiredd	12
7	7	1033892411	Sai	Bl	+9 0		saikumar _ vi@	9
8	8	100002190061552	Vara	K			var _@yahoo.co	3
9	9	100002328888334	Kaluri	A	+91 _ 3		lo vind@gmail.c	6
10	10	100000103323292	E	R	+919. _ 3		pithamb _ ddy@y	-1
11	11	562618335	Mukesh	K	+91 _ 9		mukesl _ 3@yahc	2

```
C:\android-sdk\platform-tools>adb.exe backup -shared -all
Now unlock your device and confirm the backup operation.
```


12:45
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.
Please enter your device encryption password below. This will also be used to encrypt the backup archive.
Do not back up
Back up my data

```
C:\android-sdk\platform-tools>adb.exe shell service list
Found 111 services:
0       SYSSCOPE: [com.sec.android.app.sysscope.service.ISysScopeService]
1       sip: [android.net.sip.ISipService]
2       phoneext: [com.android.internal.telephony.ITelephonyExt]
3       phone: [com.android.internal.telephony.ITelephony]
4       com.orange.authentication.simcard: [com.orange.authentication.simcard.ISimCardAuthenticationService]
5       iphonesubinfo: [com.android.internal.telephony.IPhoneSubInfo]
6       simphonebook: [com.android.internal.telephony.IIccPhoneBook]
7       isms: [com.android.internal.telephony.ISms]
8       nfc: [android.nfc.INfcAdapter]
9       FMPlayer: [com.samsung.media.fmradio.internal.IFMPlayer]
10      motion_recognition: [android.hardware.motion.IMotionRecognitionService]
11      samsung.facedetection_service: [com.sec.android.facedetection.IFaceDetectionService]
12      voip: [android.os.IVoIPInterface]
13      commontime_management: []
14      mini_mode_app_manager: [com.sec.android.app.minimode.manager.IMiniModeAppManager]
15      tvoutservice: [android.os.ITvoutService]
```

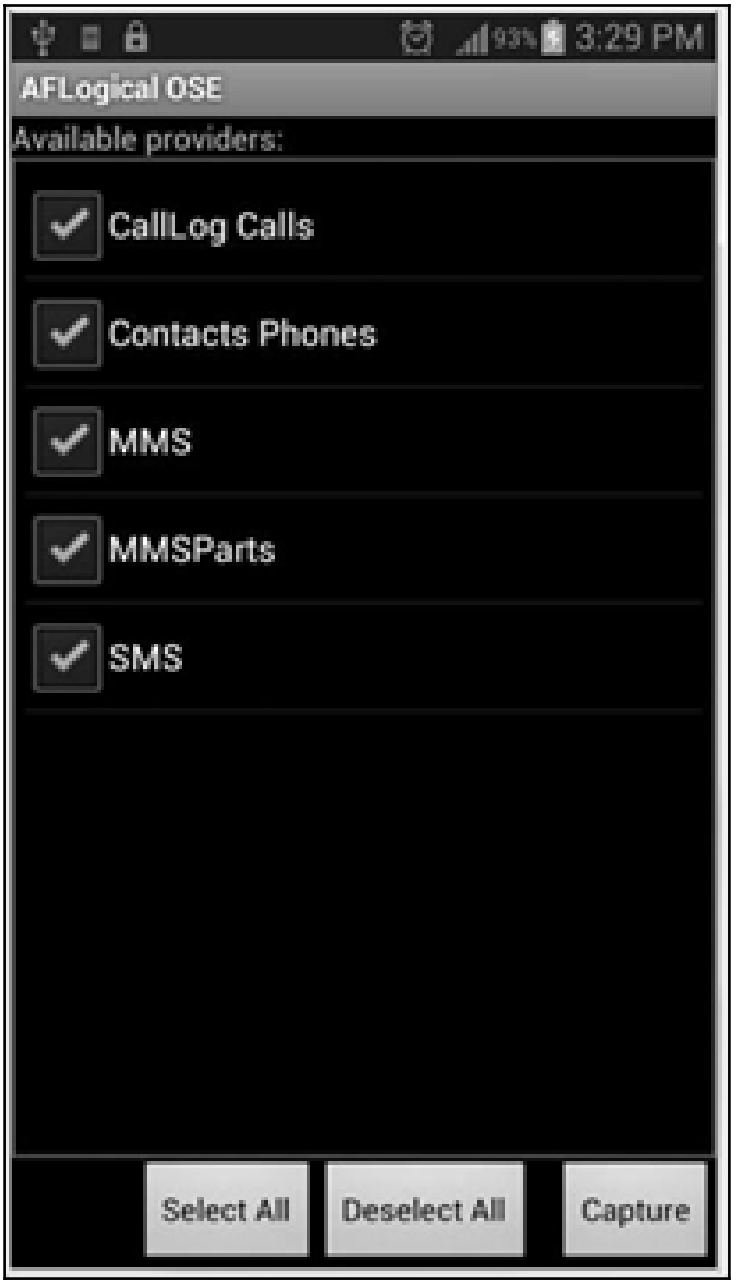
```
C:\android-sdk\platform-tools>adb.exe shell dumpsys iphonesubinfo
Phone Subscriber Info:
  Phone Type = GSM
  Device ID = 353743[illegible]6486
```

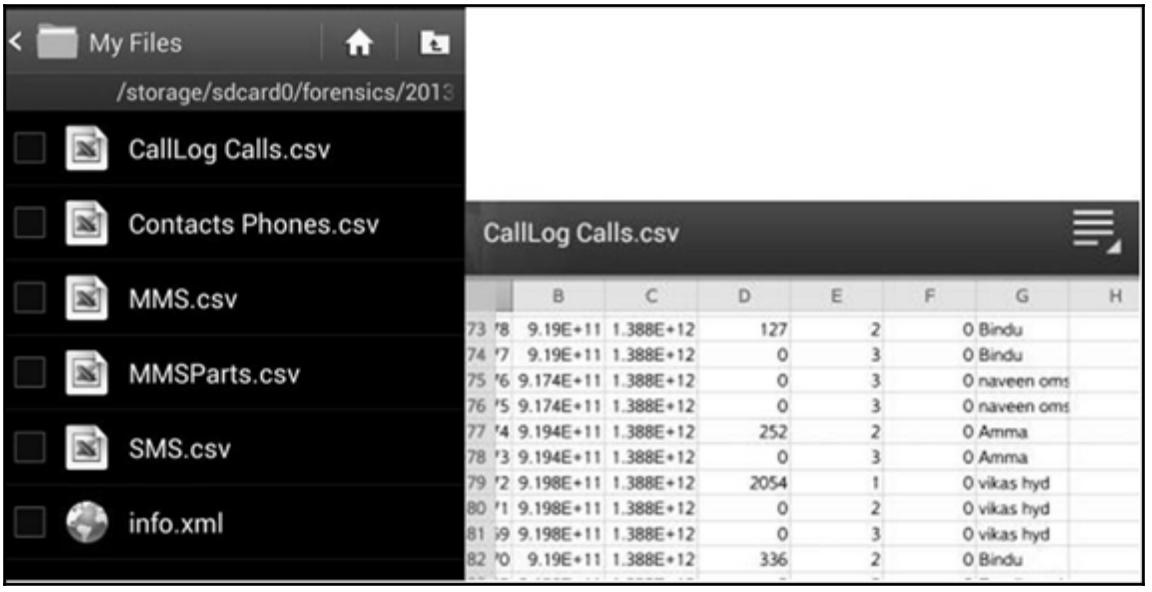
```
C:\android-sdk\platform-tools>adb.exe shell dumpsys wifi
Wi-Fi is enabled
Stay-awake conditions: 0

Internal state:
current HSM state: ConnectedState
mLinkProperties InterfaceName: wlan0 LinkAddresses: [192.168.0.106/24,]
mWifiInfo , MAC: 88:30:8a:f3:f1:d5, Supplicant state: COMPLETED, RSSI: -
mDhcpInfoInternal addr: 192.168.0.106/24 mRoutes: 0.0.0.0/0 -> 192.168.0
mNetworkInfo NetworkInfo: type: WIFI[], state: CONNECTED/CONNECTED, reas
mLastSignalLevel 2
mLastBssid 60:e3:27:be:d5:30
mLastNetworkId 1
mReconnectCount 0
mIsScanMode false
Supplicant status
bssid=60:e3:27:be:d5:30
ssid=Roro
id=1
```

```
C:\android-sdk\platform-tools>adb.exe shell dumpsys usagestats
Date: 20160129 (old data version)
Date: 20160131
  android: 1 times, 7 ms
    com.android.server.ShutdownActivity: 1 starts
  com.android.chrome: 1 times, 172801 ms
    com.google.android.apps.chrome.Main: 1 starts
    org.chromium.chrome.browser.ChromeTabbedActivity: 1 starts, 500-750ms=1
  com.sec.android.app.launcher: 4 times, 509170 ms
    com.android.launcher2.Launcher: 4 starts, 2000-3000ms=1
  com.android.backupconfirm: 2 times, 77425 ms
    com.android.backupconfirm.BackupRestoreConfirmation: 2 starts, 500-750ms=1
Date: 20160201
  android: 0 times, 3052 ms
```

```
C:\android-sdk\platform-tools>adb.exe devices
List of devices attached
4df16ac31[redacted]        device
```

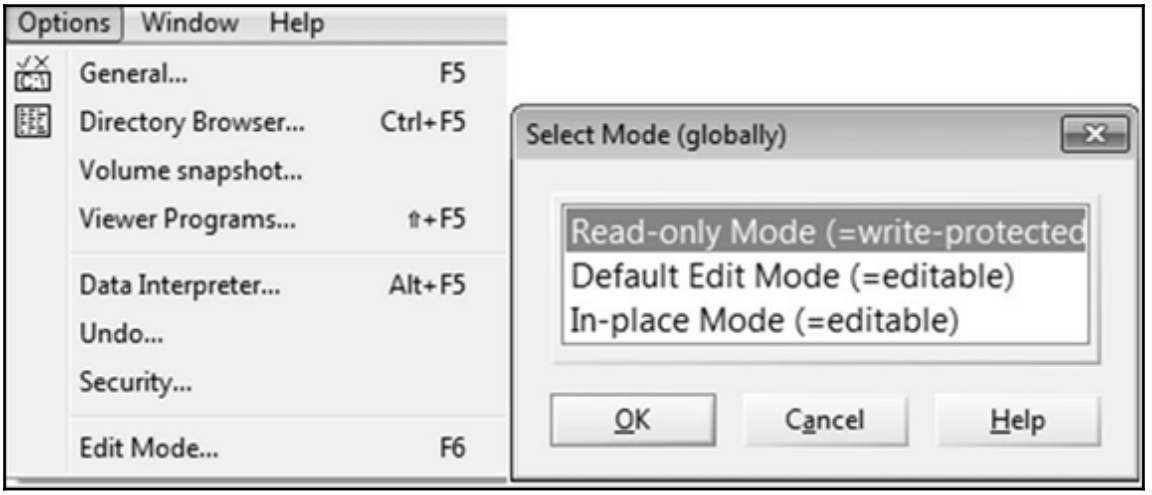
```
C:\android-sdk\platform-tools>adb.exe install AFLogical-OSE_1.5.2.apk
1798 KB/s (28794 bytes in 0.015s)
        pkg: /data/local/tmp/AFLogical-OSE_1.5.2.apk
Success
```

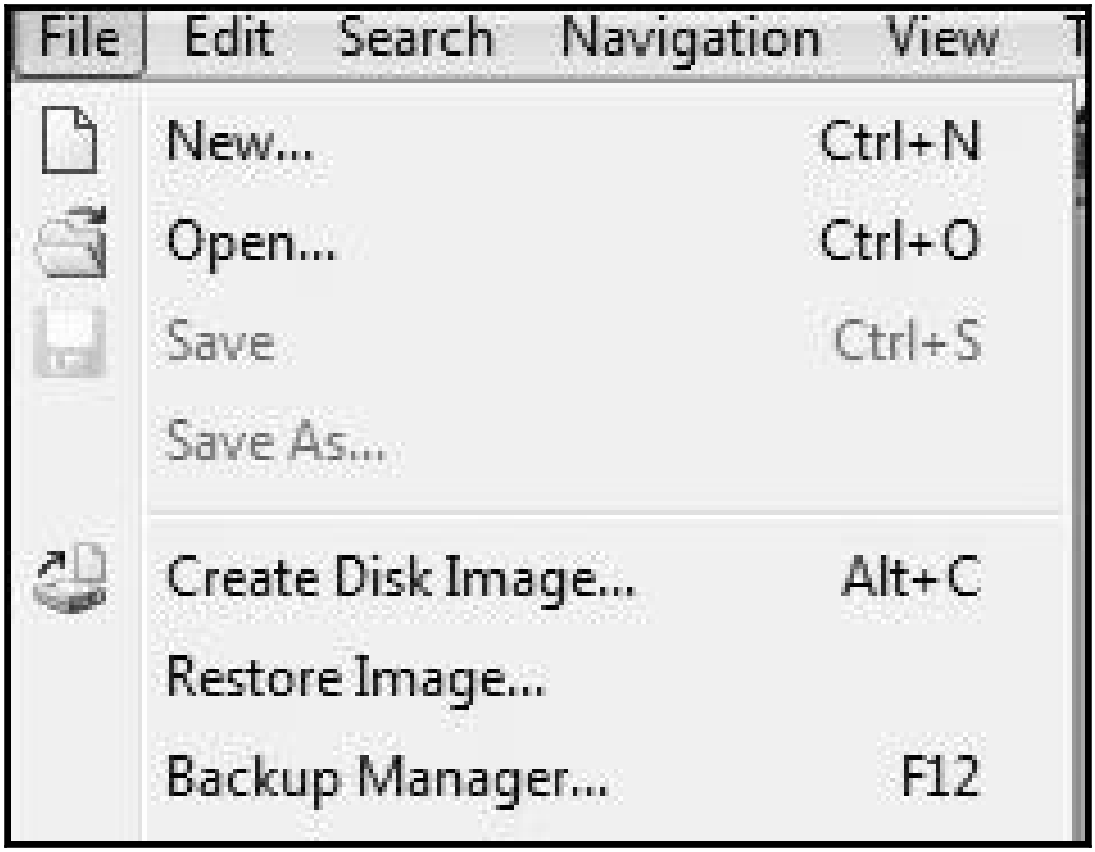

3:29 PM
AFLogical OSE
Available providers:
CallLog Calls
Contacts Phones
MMS
MMSParts
SMS
Select All
Deselect All
Capture

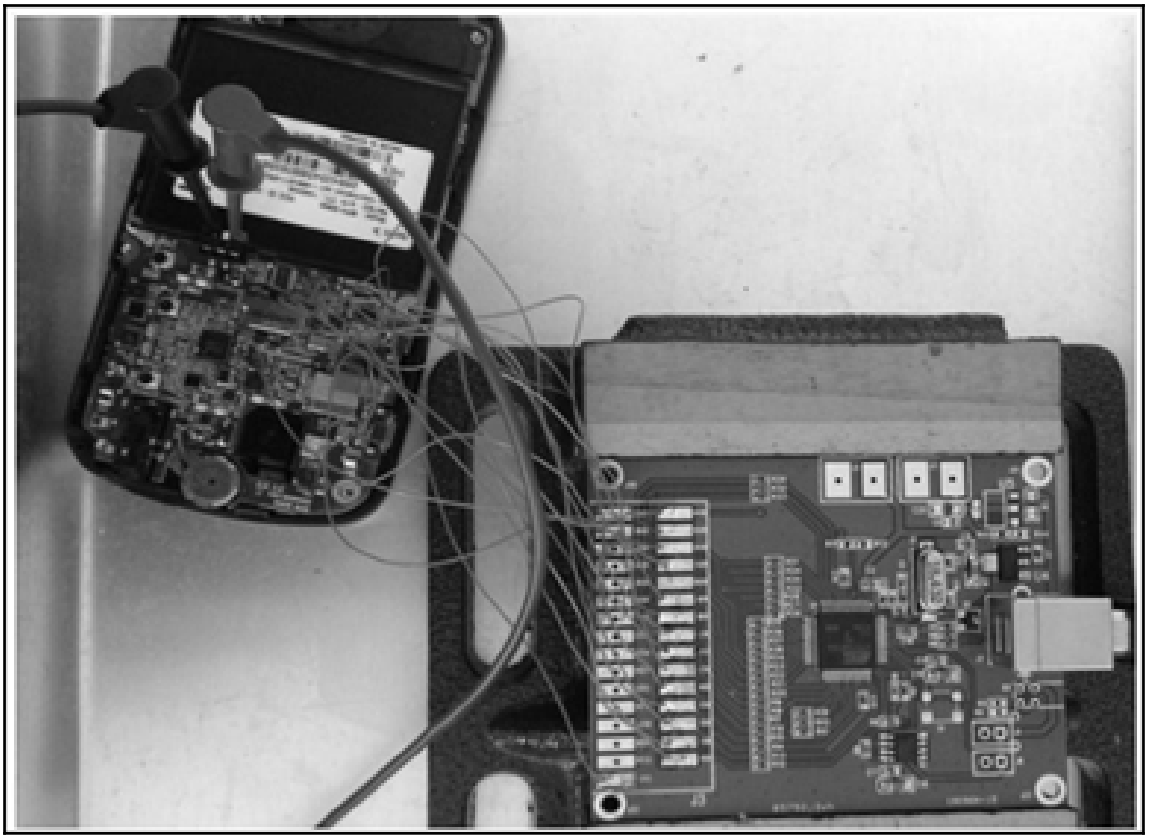



```
C:\android-sdk\platform-tools>adb.exe devices
List of devices attached
4df16ac31[redacted]        device
```

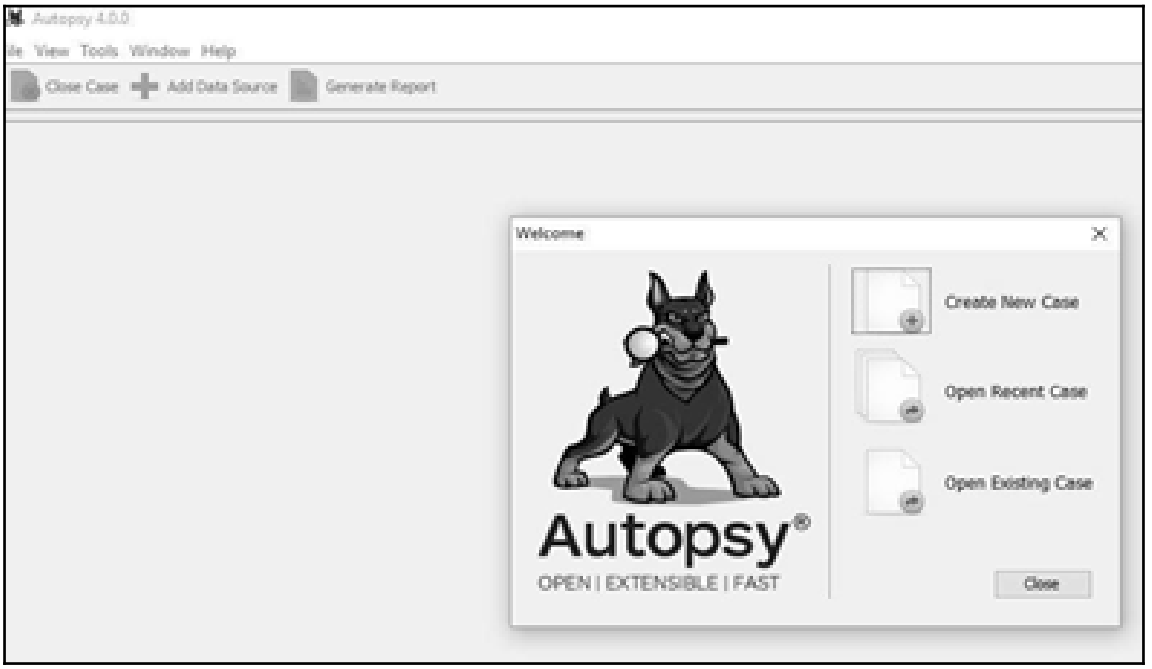
```
root@android:/ # mount
rootfs / rootfs ro,relatime 0 0
tmpfs /dev tmpfs rw,nosuid,relatime,mode=755 0 0
devpts /dev/pts devpts rw,relatime,mode=600 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,relatime 0 0
none /acct cgroup rw,relatime,cpuacct 0 0
tmpfs /mnt/asec tmpfs rw,relatime,mode=755,gid=1000 0 0
tmpfs /mnt/obb tmpfs rw,relatime,mode=755,gid=1000 0 0
none /dev/cpuctl cgroup rw,relatime,cpu 0 0
/dev/block/mmcblk0p9 /system ext4 ro,noatime,barrier=1,data=ordered 0 0
/dev/block/mmcblk0p3 /efs ext4 rw,nosuid,nodev,noatime,barrier=1,journal_asy
/dev/block/mmcblk0p8 /cache ext4 rw,nosuid,nodev,noatime,errors=panic,barrie
/dev/block/mmcblk0p12 /data ext4 rw,nosuid,nodev,noatime,barrier=1,journal_a
/sys/kernel/debug /sys/kernel/debug debugfs rw,relatime 0 0
/dev/fuse /storage/sdcard0 fuse rw,nosuid,nodev,noexec,relatime,user_id=1023
```

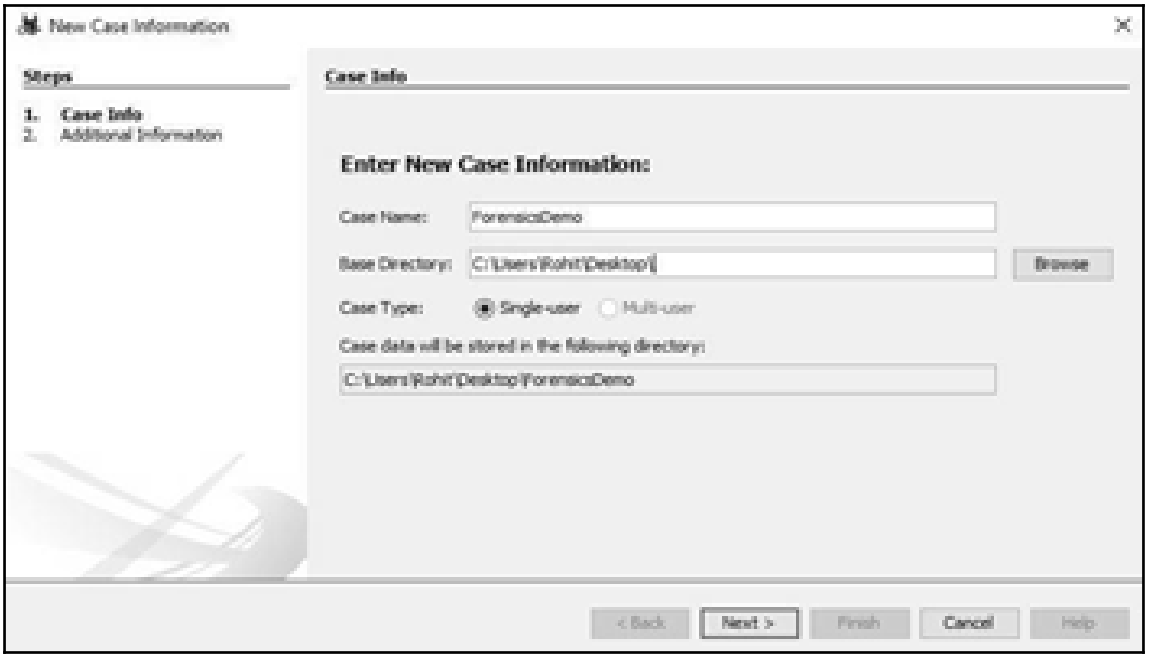


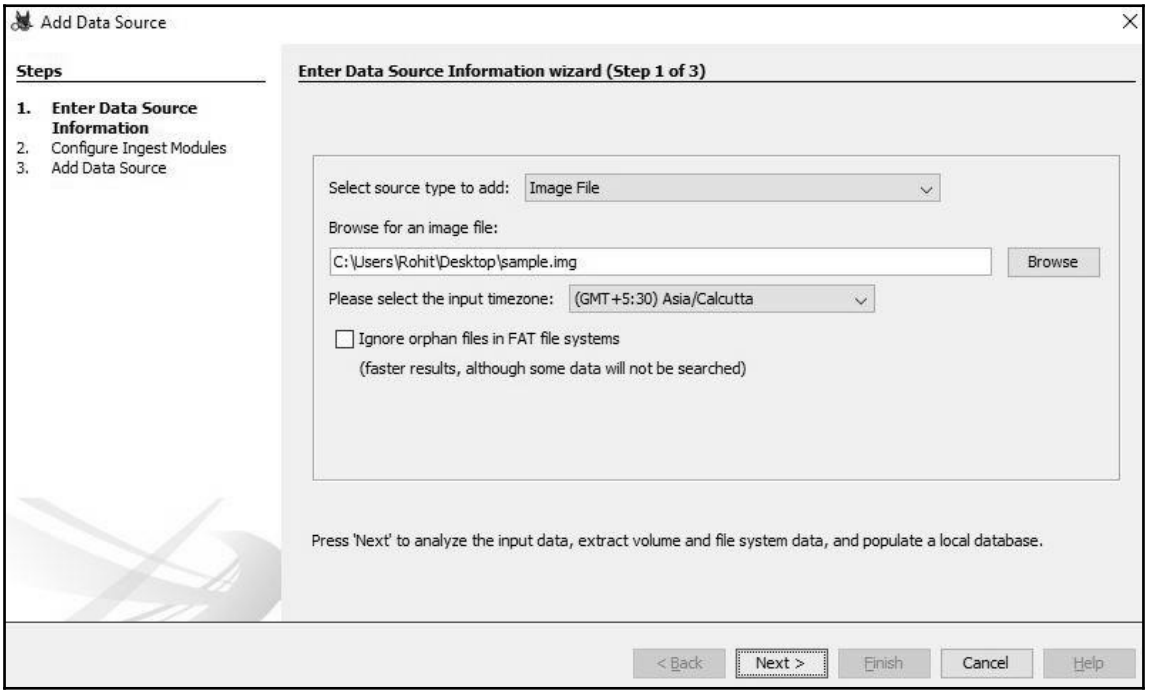

File
Edit
Search
Navigation
View
New... Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Create Disk Image... Alt+C
Restore Image...
Backup Manager... F12

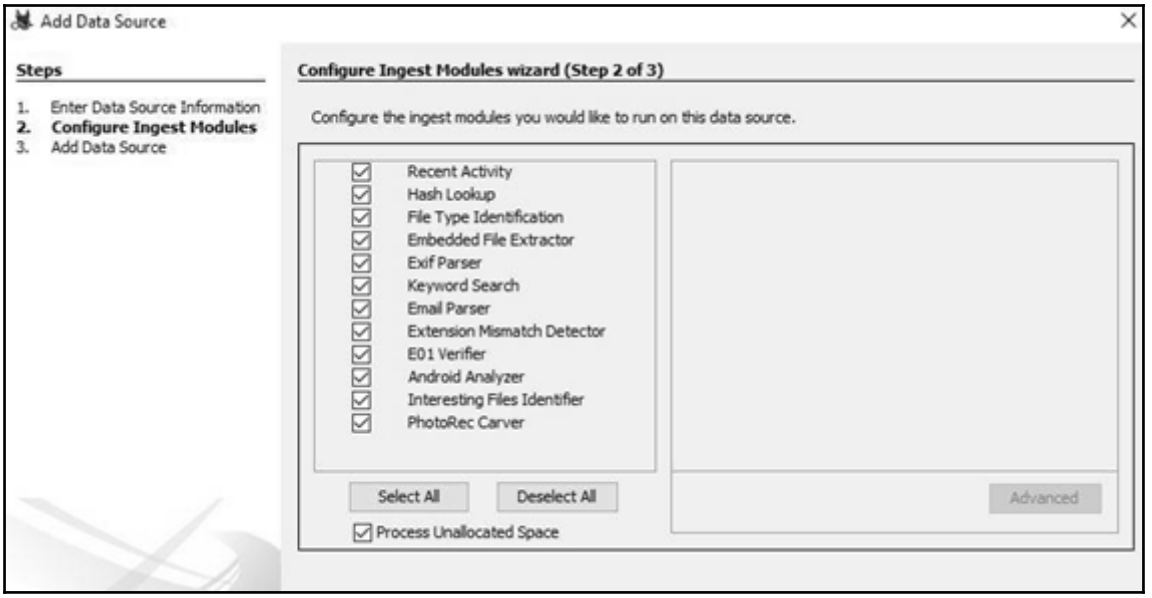


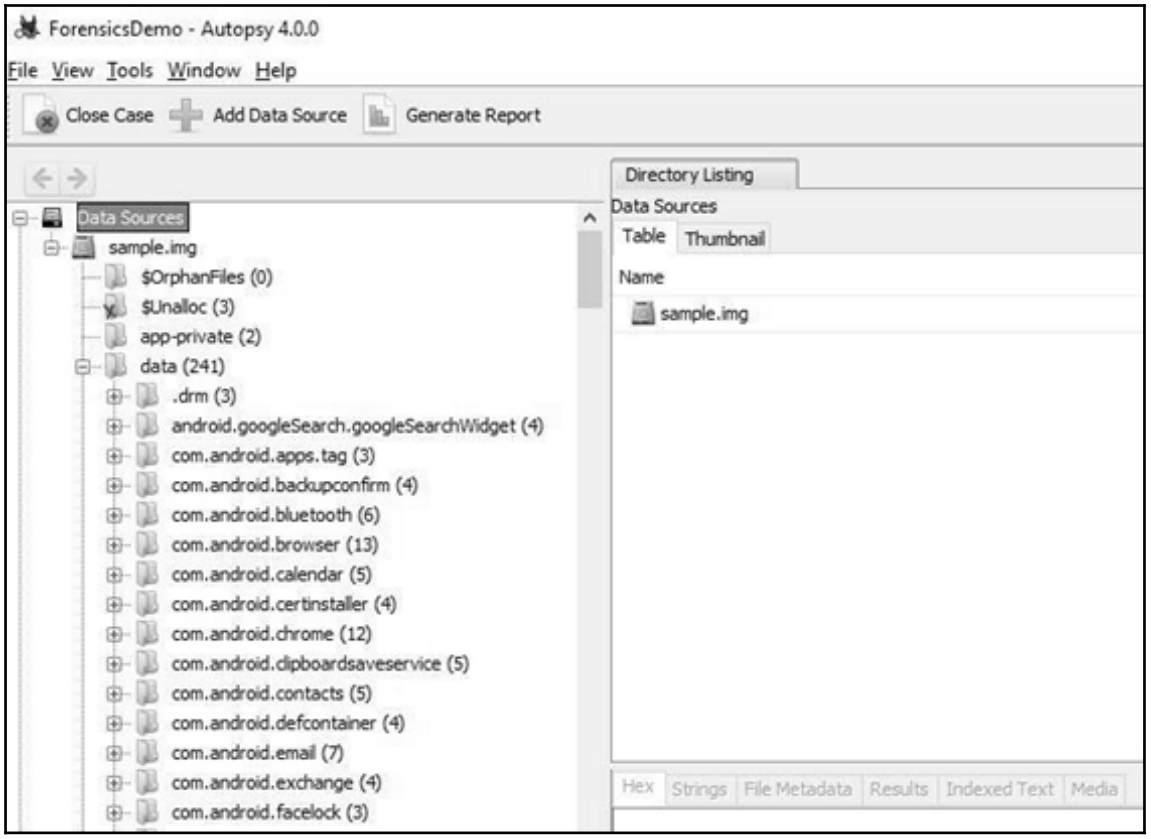
Chapter 10: Android Data Analysis and Recovery

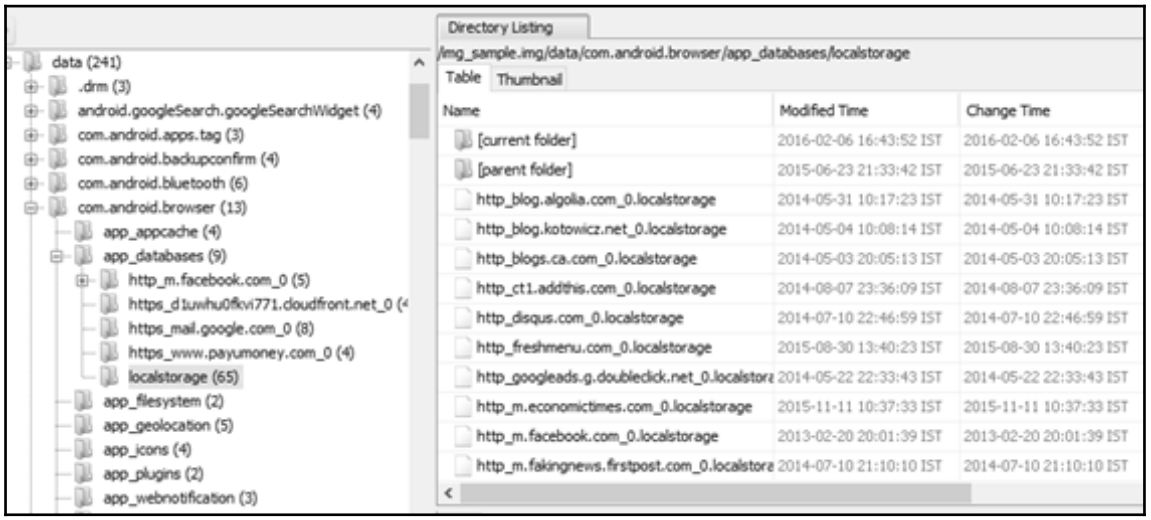


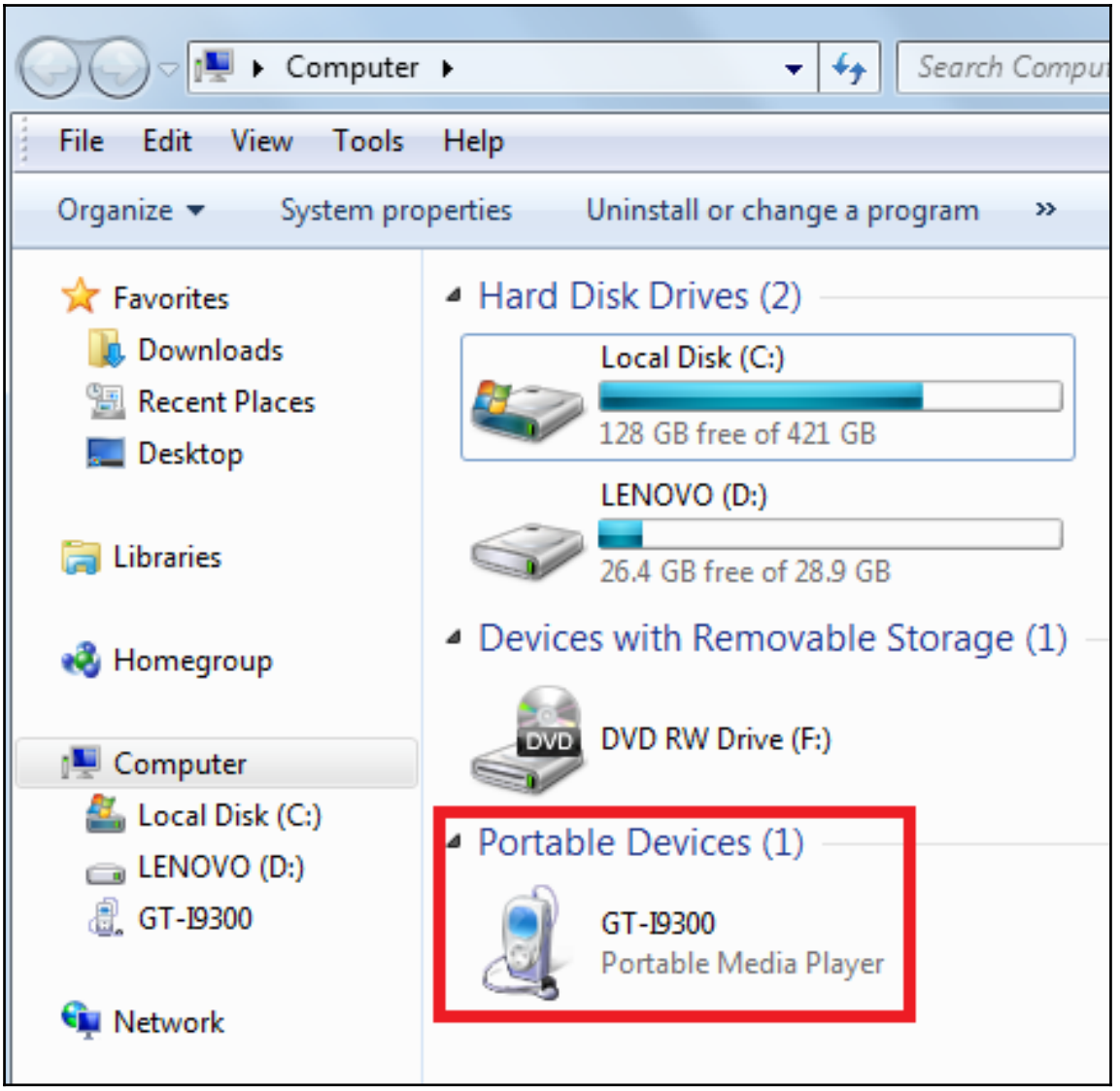

New Case Information
Steps
1. Case Info
2. Additional Information
Case Info
Enter New Case Information:
Case Name:
ForensicsDemo
Base Directory:
C:\Users\Rohit\Desktop\
Browse
Case Type:
Single-user
Multi-user
Case data will be stored in the following directory:
C:\Users\Rohit\Desktop\ForensicsDemo
< Back
Next >
Finish
Cancel
Help

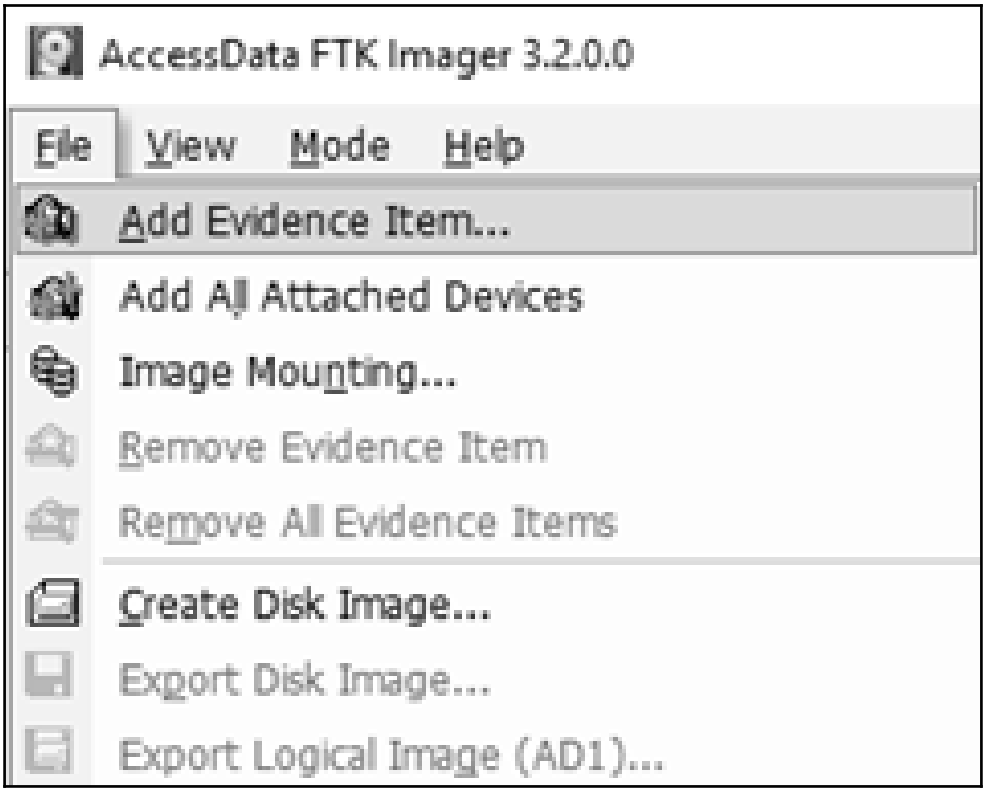

Add Data Source
Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source
Enter Data Source Information wizard (Step 1 of 3)
Select source type to add:
Image File
Browse for an image file:
C:\Users\Rohit\Desktop\sample.img
Browse
Please select the input timezone:
(GMT+5:30) Asia/Calcutta
Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)
Press 'Next' to analyze the input data, extract volume and file system data, and populate a local database.
< Back
Next >
Finish
Cancel
Help

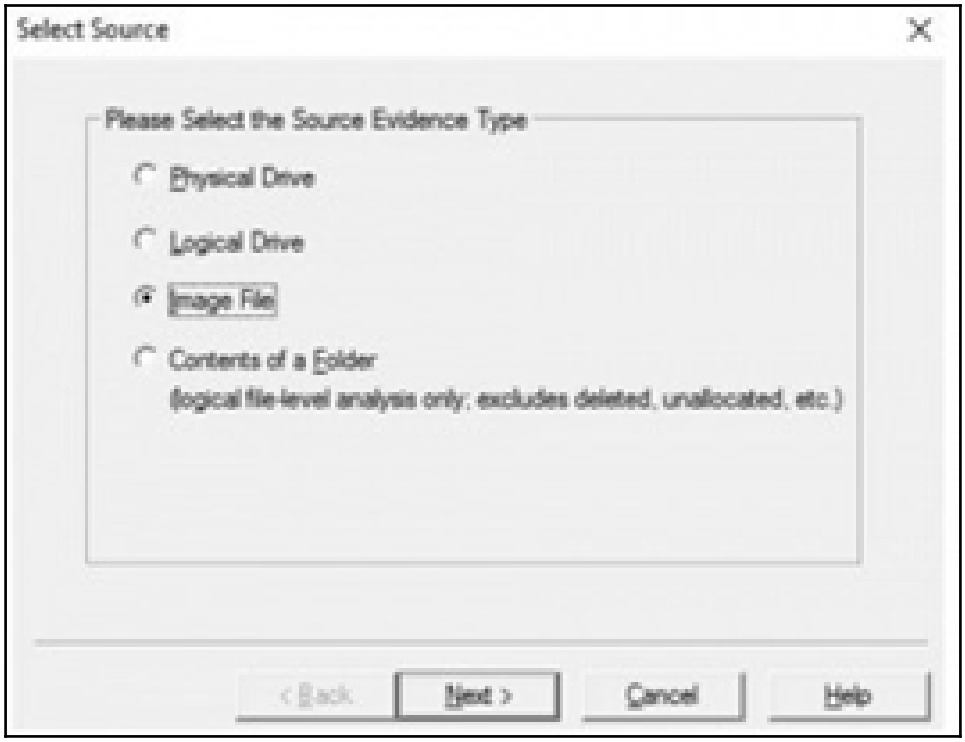

Add Data Source
Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source
Configure Ingest Modules wizard (Step 2 of 3)
Configure the ingest modules you would like to run on this data source.
Recent Activity
Hash Lookup
File Type Identification
Embedded File Extractor
Exif Parser
Keyword Search
Email Parser
Extension Mismatch Detector
E01 Verifier
Android Analyzer
Interesting Files Identifier
PhotoRec Carver
Select All
Deselect All
Advanced
Process Unallocated Space

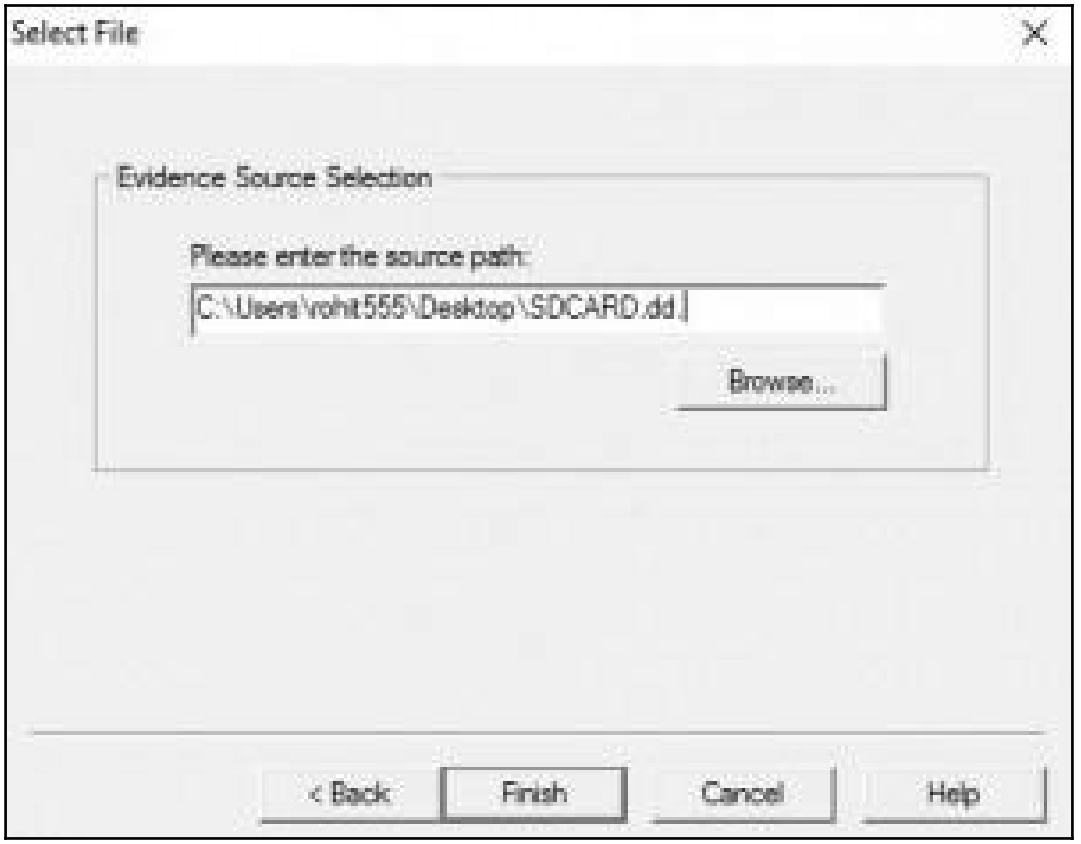

ForensicsDemo - Autopsy 4.0.0
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Directory Listing
Data Sources
Table
Thumbnail
Name
sample.img
Data Sources
sample.img
$OrphanFiles (0)
$Unalloc (3)
app-private (2)
data (241)
.drm (3)
android.googleSearch.googleSearchWidget (4)
com.android.apps.tag (3)
com.android.backupconfirm (4)
com.android.bluetooth (6)
com.android.browser (13)
com.android.calendar (5)
com.android.certinstaller (4)
com.android.chrome (12)
com.android.clipboardsaveservice (5)
com.android.contacts (5)
com.android.defcontainer (4)
com.android.email (7)
com.android.exchange (4)
com.android.facelock (3)
Hex
Strings
File Metadata
Results
Indexed Text
Media

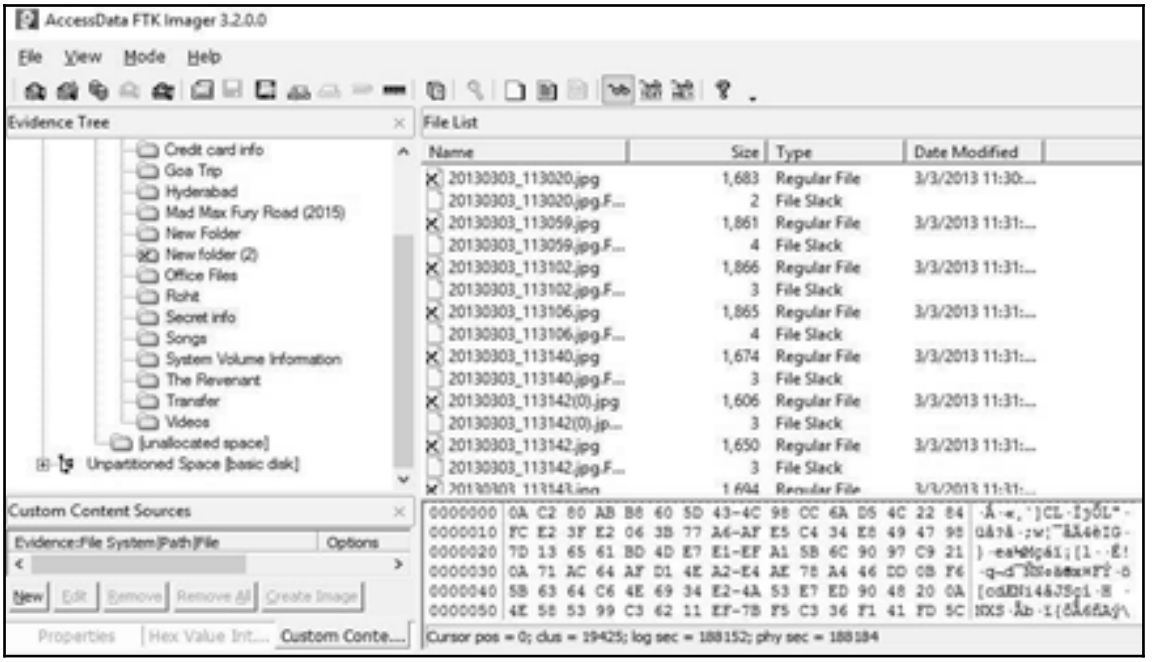

Directory Listing
/img_sample.img/data/com.android.browser/app_databases/localstorage
Table
Thumbnail
Name
Modified Time
Change Time
[current folder] 2016-02-06 16:43:52 IST 2016-02-06 16:43:52 IST
[parent folder] 2015-06-23 21:33:42 IST 2015-06-23 21:33:42 IST
http_blog.algolia.com_0.localstorage 2014-05-31 10:17:23 IST 2014-05-31 10:17:23 IST
http_blog.kotowicz.net_0.localstorage 2014-05-04 10:08:14 IST 2014-05-04 10:08:14 IST
http_blogs.ca.com_0.localstorage 2014-05-03 20:05:13 IST 2014-05-03 20:05:13 IST
http_ct1.addthis.com_0.localstorage 2014-08-07 23:36:09 IST 2014-08-07 23:36:09 IST
http_disqus.com_0.localstorage 2014-07-10 22:46:59 IST 2014-07-10 22:46:59 IST
http_freshmenu.com_0.localstorage 2015-08-30 13:40:23 IST 2015-08-30 13:40:23 IST
http_googleads.g.doubleclick.net_0.localstora 2014-05-22 22:33:43 IST 2014-05-22 22:33:43 IST
http_m.economictimes.com_0.localstorage 2015-11-11 10:37:33 IST 2015-11-11 10:37:33 IST
http_m.facebook.com_0.localstorage 2013-02-20 20:01:39 IST 2013-02-20 20:01:39 IST
http_m.fakingnews.firstpost.com_0.localstora 2014-07-10 21:10:10 IST 2014-07-10 21:10:10 IST
data (241)
.drm (3)
android.googleSearch.googleSearchWidget (4)
com.android.apps.tag (3)
com.android.backupconfirm (4)
com.android.bluetooth (6)
com.android.browser (13)
app_appcache (4)
app_databases (9)
http_m.facebook.com_0 (5)
https_d1uwhu0fkvi771.cloudfront.net_0 (4
https_mail.google.com_0 (8)
https_www.payumoney.com_0 (4)
localstorage (65)
app_filesystem (2)
app_geolocation (5)
app_icons (4)
app_plugins (2)
app_webnotification (3)

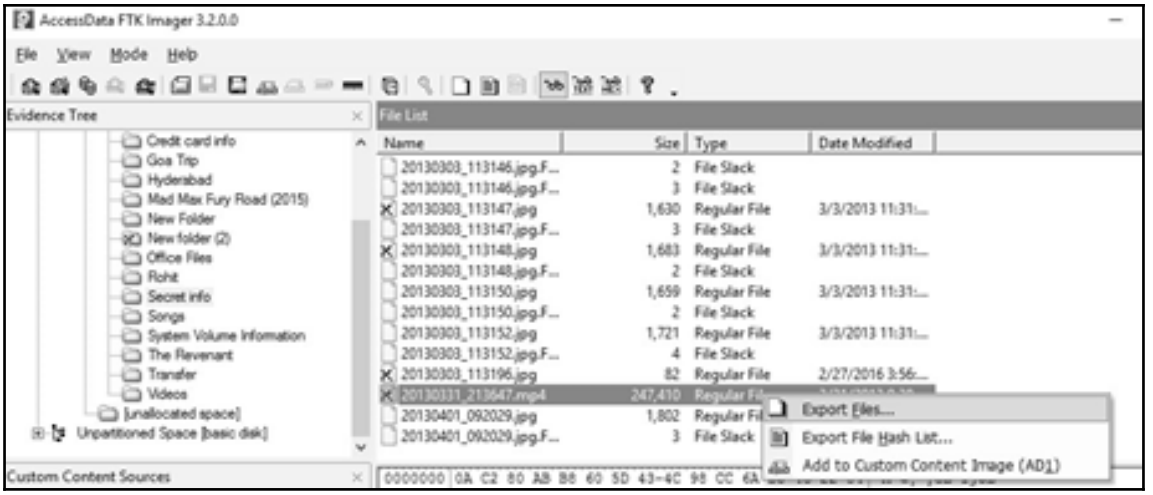

Computer
Search Compu
File Edit View Tools Help
Organize
System properties
Uninstall or change a program
Favorites
Downloads
Recent Places
Desktop
Libraries
Homegroup
Computer
Local Disk (C:)
LENOVO (D:)
GT-I9300
Network
Hard Disk Drives (2)
Local Disk (C:)
128 GB free of 421 GB
LENOVO (D:)
26.4 GB free of 28.9 GB
Devices with Removable Storage (1)
DVD
DVD RW Drive (F:)
Portable Devices (1)
GT-I9300
Portable Media Player

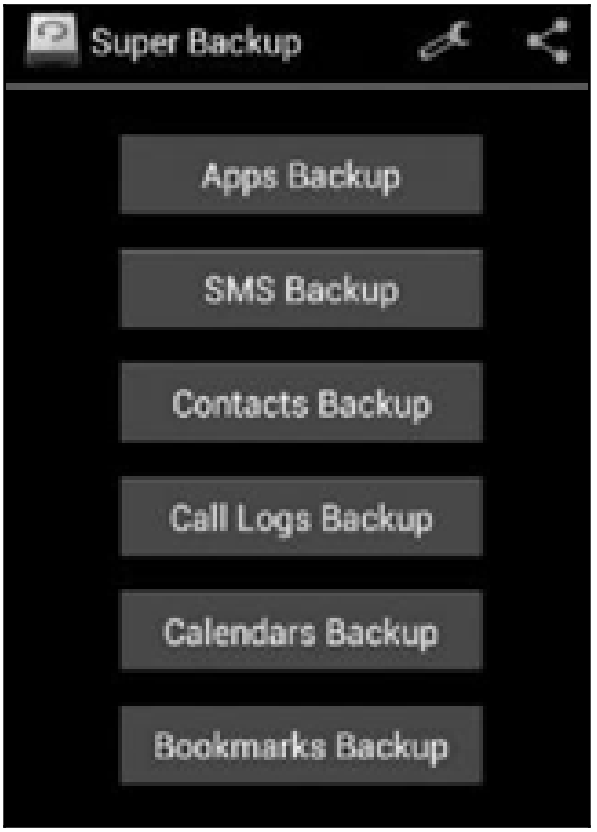

AccessData FTK Imager 3.2.0.0
File
View
Mode
Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...


Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
< Back
Next >
Cancel
Help

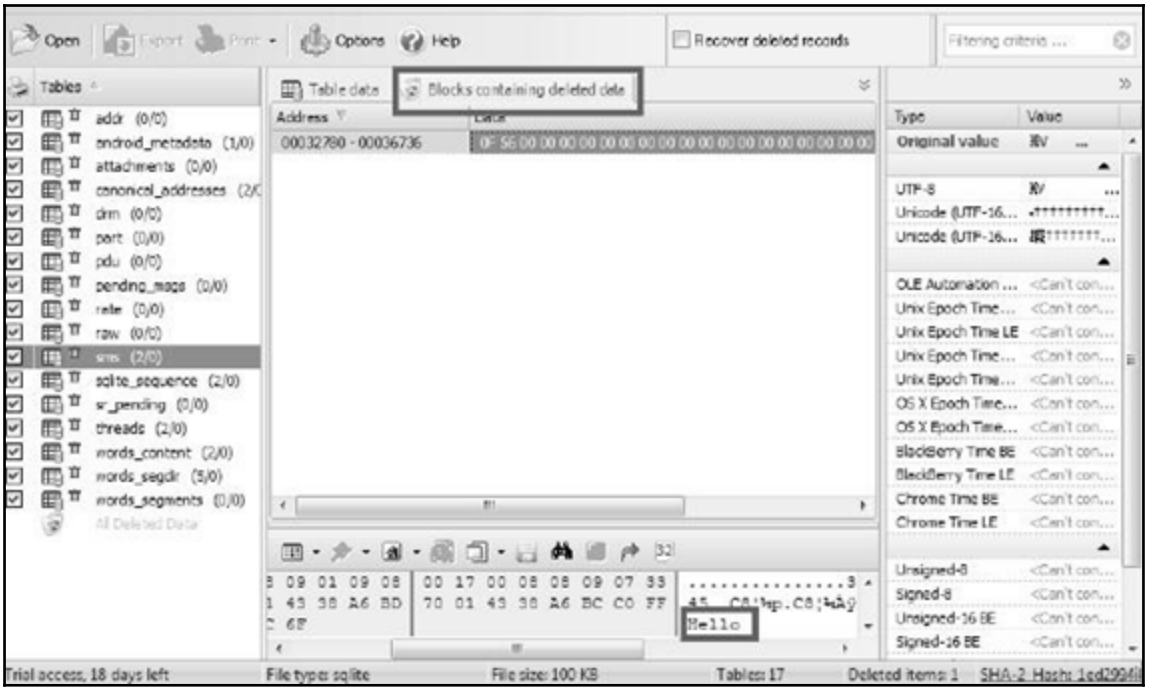

Select File
Evidence Source Selection
Please enter the source path:
C:\Users\rohit555\Desktop\SDCARD.dd
Browse...
< Back
Finish
Cancel
Help

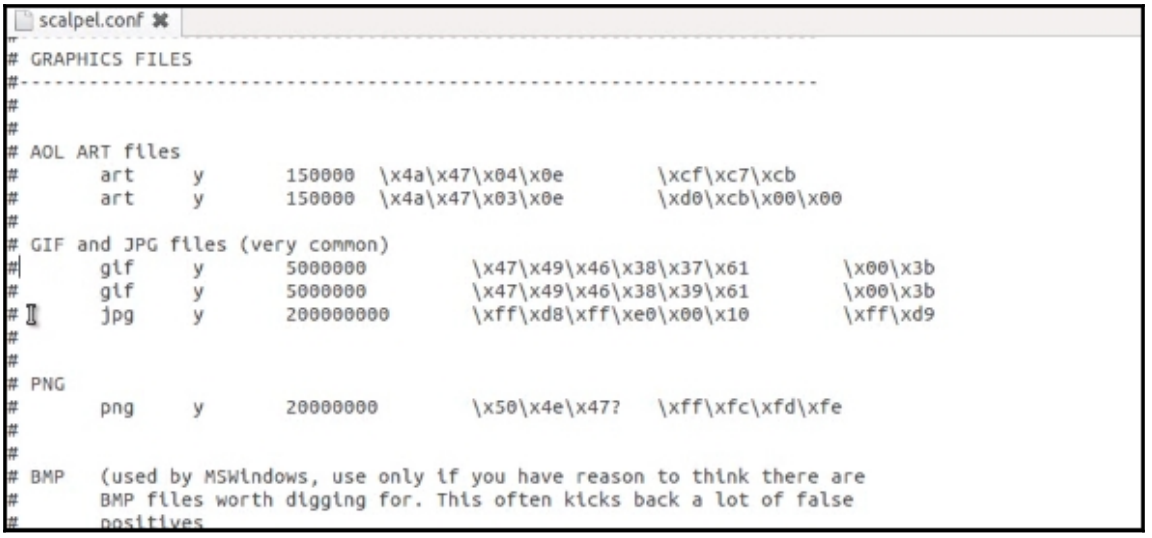

AccessData FTK Imager 3.2.0.0
File View Mode Help
Evidence Tree
File List
Credit card info
Goa Trip
Hyderabad
Mad Max Fury Road (2015)
New Folder
New folder (2)
Office Files
Rohit
Secret info
Songs
System Volume Information
The Revenant
Transfer
Videos
[unallocated space]
Unpartitioned Space [basic disk]
Name
Size
Type
Date Modified
20130303_113020.jpg 1,683 Regular File 3/3/2013 11:30:...
20130303_113020.jpg.F... 2 File Slack
20130303_113059.jpg 1,861 Regular File 3/3/2013 11:31:...
20130303_113059.jpg.F... 4 File Slack
20130303_113102.jpg 1,866 Regular File 3/3/2013 11:31:...
20130303_113102.jpg.F... 3 File Slack
20130303_113106.jpg 1,865 Regular File 3/3/2013 11:31:...
20130303_113106.jpg.F... 4 File Slack
20130303_113140.jpg 1,674 Regular File 3/3/2013 11:31:...
20130303_113140.jpg.F... 3 File Slack
20130303_113142(0).jpg 1,606 Regular File 3/3/2013 11:31:...
20130303_113142(0).jp... 3 File Slack
20130303_113142.jpg 1,650 Regular File 3/3/2013 11:31:...
20130303_113142.jpg.F... 3 File Slack
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Int....
Custom Conte....
Cursor pos = 0; clus = 19425; log sec = 188152; phy sec = 188184


AccessData FTK Imager 3.2.0.0
File View Mode Help
Evidence Tree
File List
Credit card info
Goa Trip
Hyderabad
Mad Max Fury Road (2015)
New Folder
New folder (2)
Office Files
Rohit
Secret info
Songs
System Volume Information
The Revenant
Transfer
Videos
[unallocated space]
Unpartitioned Space [basic disk]
Name
Size
Type
Date Modified
20130303_113146.jpg.F... 2 File Slack
20130303_113146.jpg.F... 3 File Slack
20130303_113147.jpg 1,630 Regular File 3/3/2013 11:31:...
20130303_113147.jpg.F... 3 File Slack
20130303_113148.jpg 1,683 Regular File 3/3/2013 11:31:...
20130303_113148.jpg.F... 2 File Slack
20130303_113150.jpg 1,659 Regular File 3/3/2013 11:31:...
20130303_113150.jpg.F... 2 File Slack
20130303_113152.jpg 1,721 Regular File 3/3/2013 11:31:...
20130303_113152.jpg.F... 4 File Slack
20130303_113196.jpg 82 Regular File 2/27/2016 3:56:...
20130331_213647.mp4 247,410
20130401_092029.jpg 1,802
20130401_092029.jpg.F... 3 File Slack
Export Files...
Export File Hash List...
Add to Custom Content Image (AD1)
Custom Content Sources

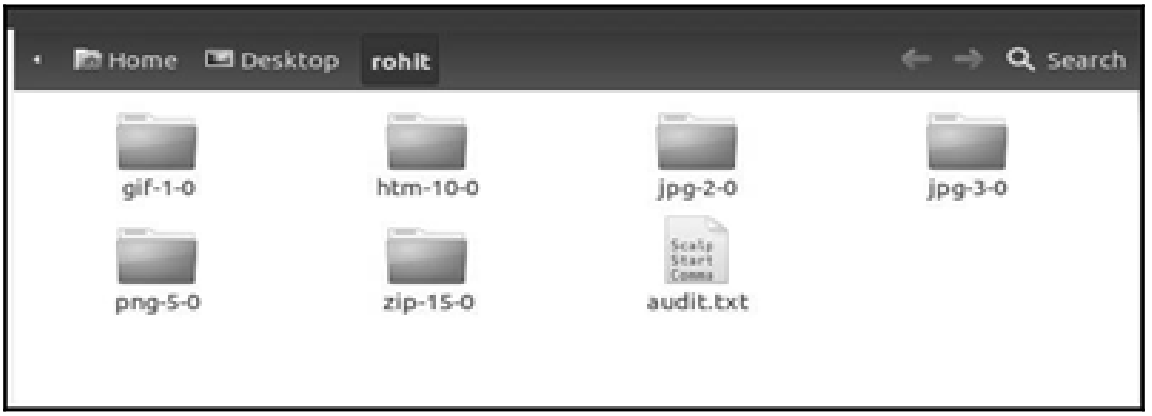


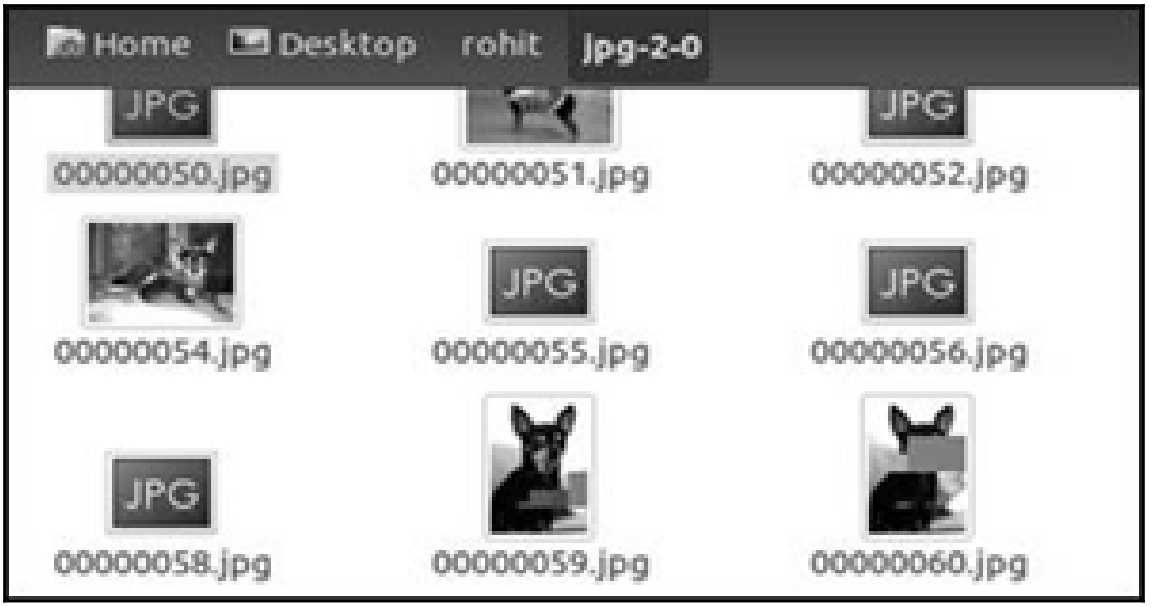

```
C:\android-sdk\platform-tools>adb.exe pull /data/data/com.android.providers.telephony/databases C:\temp
pull: building file list...
pull: /data/data/com.android.providers.telephony/databases/telephony.db-journal -> C:\temp/telephony.db-journal
pull: /data/data/com.android.providers.telephony/databases/telephony.db -> C:\temp/telephony.db
pull: /data/data/com.android.providers.telephony/databases/nwk_info.db-journal -> C:\temp/nwk_info.db-journal
pull: /data/data/com.android.providers.telephony/databases/nwk_info.db -> C:\temp/nwk_info.db
pull: /data/data/com.android.providers.telephony/databases/mmssms.db-shm -> C:\temp/mmssms.db-shm
pull: /data/data/com.android.providers.telephony/databases/mmssms.db-wal -> C:\temp/mmssms.db-wal
pull: /data/data/com.android.providers.telephony/databases/mmssms.db -> C:\temp/mmssms.db
7 files pulled. 0 files skipped.
3242 KB/s (6177288 bytes in 1.860s)
```

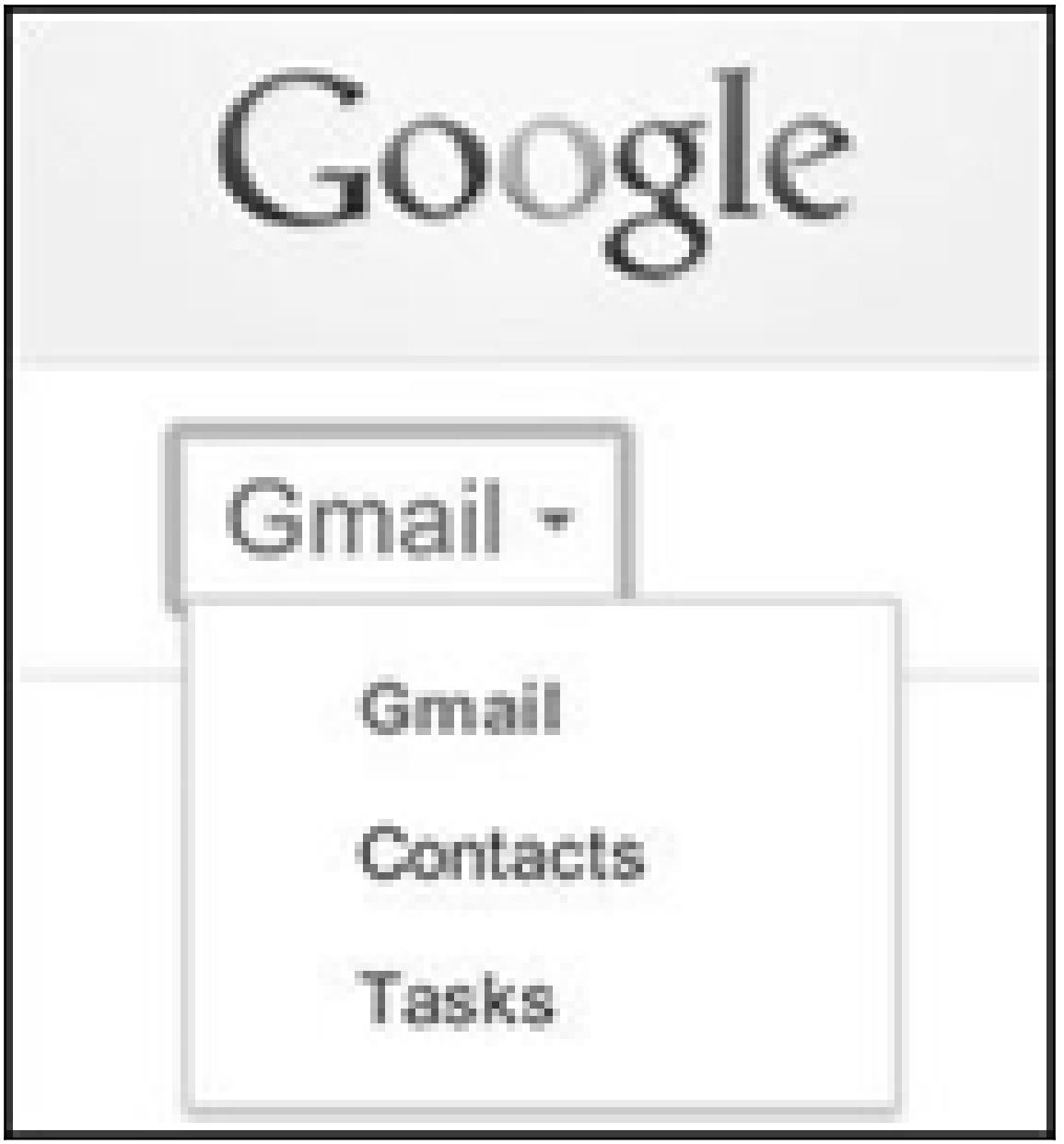

Open
Export
Print
Options
Help
Recover deleted records
Filtering criteria ...
Tables
Table data
Blocks containing deleted data
Address
Data
Type
Value
Original value
UTF-8
Unicode (UTF-16...
Unicode (UTF-16...
OLE Automation ...
Unix Epoch Time...
Unix Epoch Time LE
OS X Epoch Time...
BlackBerry Time BE
BlackBerry Time LE
Chrome Time BE
Chrome Time LE
Unsigned-8
Signed-8
Unsigned-16 BE
Signed-16 BE
Hello
Trial access, 18 days left
File type: sqlite
File size: 100 KB
Tables: 17
Deleted items: 1
SHA-2 Hashs: 1ed2994f


scalpel.conf
GRAPHICS FILES
AOL ART files
art y 150000 \x4a\x47\x04\x0e \xcf\xc7\xcb
art y 150000 \x4a\x47\x03\x0e \xd0\xcb\x00\x00
GIF and JPG files (very common)
gif y 5000000 \x47\x49\x46\x38\x37\x61 \x00\x3b
gif y 5000000 \x47\x49\x46\x38\x39\x61 \x00\x3b
jpg y 200000000 \xff\xd8\xff\xe0\x00\x10 \xff\xd9
PNG
png y 20000000 \x50\x4e\x47? \xff\xfc\xfd\xfe
BMP (used by MSWindows, use only if you have reason to think there are
BMP files worth digging for. This often kicks back a lot of false
positives

```
File  Edit  View  Search  Terminal  Help
unigeek@ubuntu:~$ scalpel -c /home/unigeek/Desktop/scalpel-android.conf /home/un
igeek/Desktop/userdata.dd -o /home/unigeek/Desktop/rohit
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/home/unigeek/Desktop/userdata.dd"

Image file pass 1/2.
/home/unigeek/Desktop/userdata.dd: 100.0% |**************|    3.9 MB    00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built.  Workload:
gif with header "\x47\x49\x46\x38\x37\x61" and footer "\x00\x3b" --> 0 files
gif with header "\x47\x49\x46\x38\x39\x61" and footer "\x00\x3b" --> 2 files
jpg with header "\xff\xd8\xff\xe0\x00\x10" and footer "\xff\xd9" --> 71 files
jpg with header "\xff\xd8\xff\xe1" and footer "\x7f\xff\xd9" --> 1 files
png with header "\x50\x4e\x47\x3f" and footer "\xff\xfc\xfd\xfe" --> 0 files
png with header "\x89\x50\x4e\x47" and footer "" --> 71 files
sqlitedb with header "\x53\x51\x4c\x69\x74\x65\x20\x66\x6f\x72\x6d\x61\x74" and
footer "" --> 0 files
email with header "\x46\x72\x6f\x6d\x3a" and footer "" --> 0 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00" and footer "\xd0\xcf\
x11\xe0\xa1\xb1\x1a\xe1\x00\x00" --> 0 files
doc with header "\xd0\xcf\x11\xe0\xa1\xb1" and footer "" --> 0 files
htm with header "\x3c\x68\x74\x6d\x6c" and footer "\x3c\x2f\x68\x74\x6d\x6c\x3e"
 --> 1 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" --> 0 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" --> 0 files
wav with header "\x52\x49\x46\x46\x3f\x3f\x3f\x3f\x57\x41\x56\x45" and footer ""
 --> 0 files
amr with header "\x23\x21\x41\x4d\x52" and footer "" --> 0 files
```



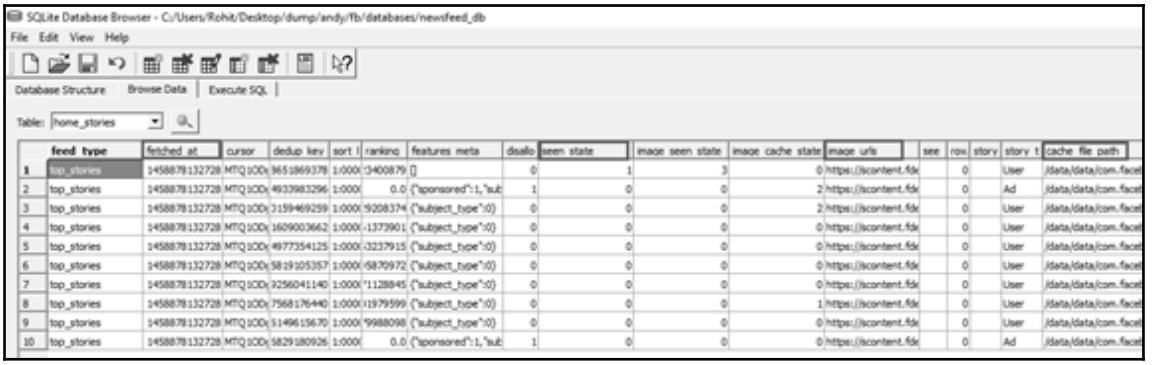

Home
Desktop
rohit
jpg-2-0
JPG
00000050.jpg
00000051.jpg
JPG
00000052.jpg
00000054.jpg
JPG
00000055.jpg
JPG
00000056.jpg
JPG
00000058.jpg
00000059.jpg
00000060.jpg


Google
Gmail
Gmail
Contacts
Tasks

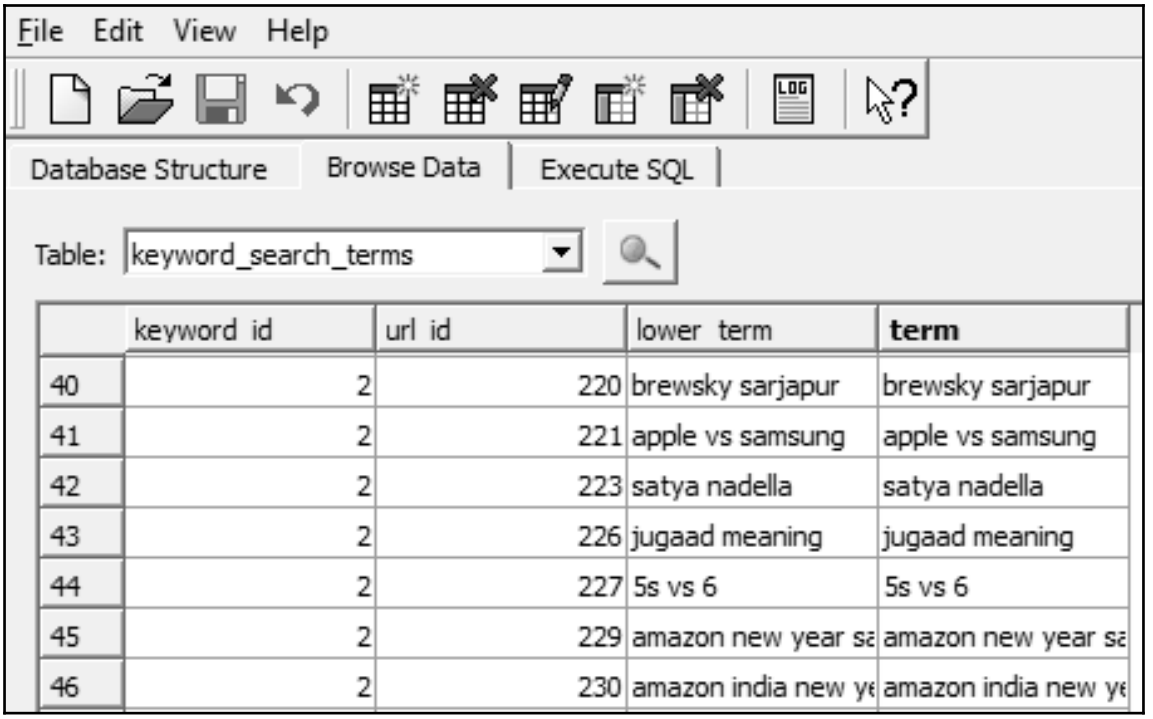

Restore Contacts
You can restore your contact list to the state that it was in at any point within the past 30 days. This is a great way to recover deleted contacts, undo an import or undo a merge. Learn more
Please select a time to restore to:
10 minutes ago
1 hour ago
Yesterday
1 week ago
Custom
0 days, 1 hours, 0 minutes.
Restore
Cancel

Chapter 11: Android App Analysis, Malware, and Reverse Engineering

```
C:\android-sdk\platform-tools>adb.exe shell
root@android:/ # cd /data/system
root@android:/data/system # cat packages.list
com.google.android.location 10021 0 /data/data/com.google.android.location
com.android.defcontainer 10026 0 /data/data/com.android.defcontainer
com.sec.android.gallery3d 10092 0 /data/data/com.sec.android.gallery3d
com.sec.android.fotaclient 10041 0 /data/data/com.sec.android.fotaclient
com.monotype.android.font.helvneuelt 10052 0 /data/data/com.monotype.android.font.
com.sec.android.motions.settings.panningtutorial 10067 0 /data/data/com.sec.andro
com.fmm.dm 10128 0 /data/data/com.fmm.dm
android.googleSearch.googleSearchWidget 10049 0 /data/data/android.googleSearch.g
com.android.providers.calendar 10087 0 /data/data/com.android.providers.calendar
com.android.bluetooth 10083 0 /data/data/com.android.bluetooth
```

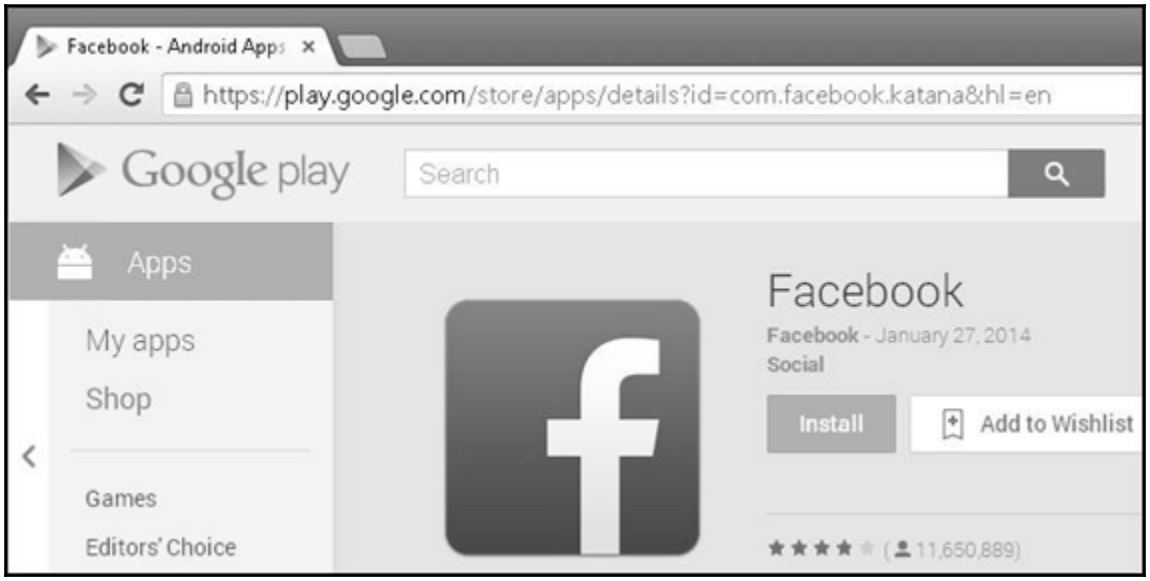



```
127|root@android:/data/data/com.google.android.gm/cache/t[redacted]@gmail.com # ls
04 Vulnerabilities-1.pptx
04 Vulnerabilities-2.pptx
05 XSS-1.pptx
05 XSS.pptx
06 SQLi.pptx
07 CSRF & Others.pptx
8311OS_08_Final_AJ-1.docx
8311OS_08_Final_AJ.docx
B05387_04_16-1.png
B05387_04_16-2.png
B05387_04_16-3.png
B05387_04_16-4.png
```



	keyword_id	url_id	lower_term	term
40	2	220	brewsky sarjapur	brewsky sarjapur
41	2	221	apple vs samsung	apple vs samsung
42	2	223	satya nadella	satya nadella
43	2	226	jugaad meaning	jugaad meaning
44	2	227	5s vs 6	5s vs 6
45	2	229	amazon new year sa	amazon new year sa
46	2	230	amazon india new ye	amazon india new ye

```
C:\android-sdk\platform-tools>adb.exe shell pm list packages
package:android
package:android.googleSearch.googleSearchWidget
package:com.android.MtpApplication
package:com.android.Preconfig
package:com.android.apps.tag
package:com.android.backupconfirm
package:com.android.bluetooth
package:com.android.browser
package:com.android.calendar
package:com.android.certinstaller
package:com.android.chrome
package:com.android.clipboardsaveservice
package:com.android.contacts
package:com.android.defcontainer
package:com.android.email
package:com.android.exchange
package:com.android.facelock
```

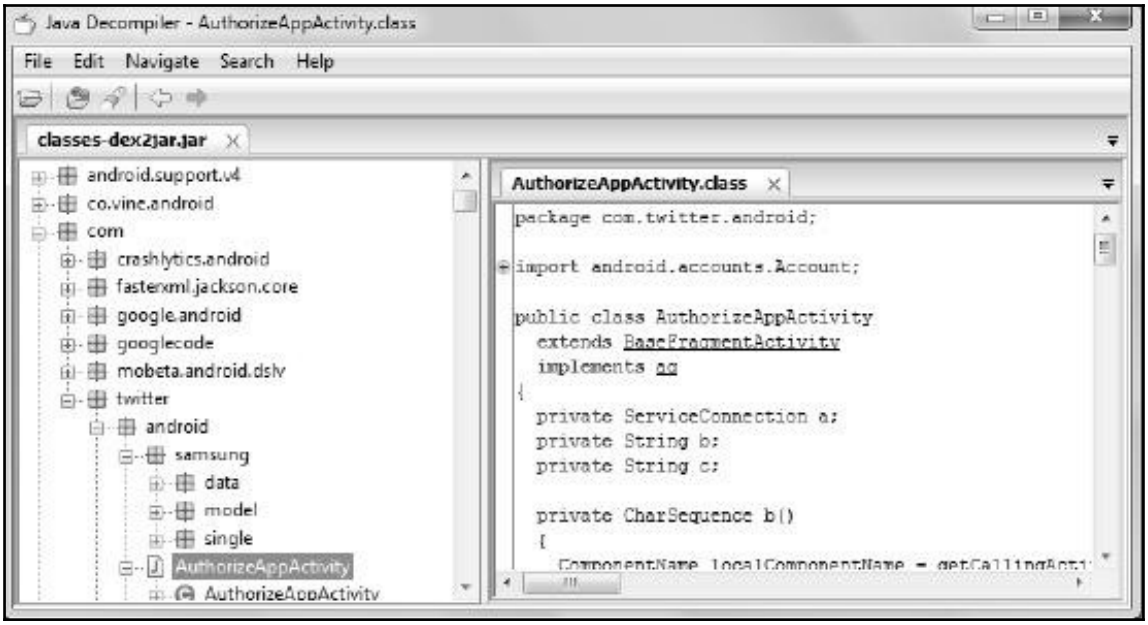


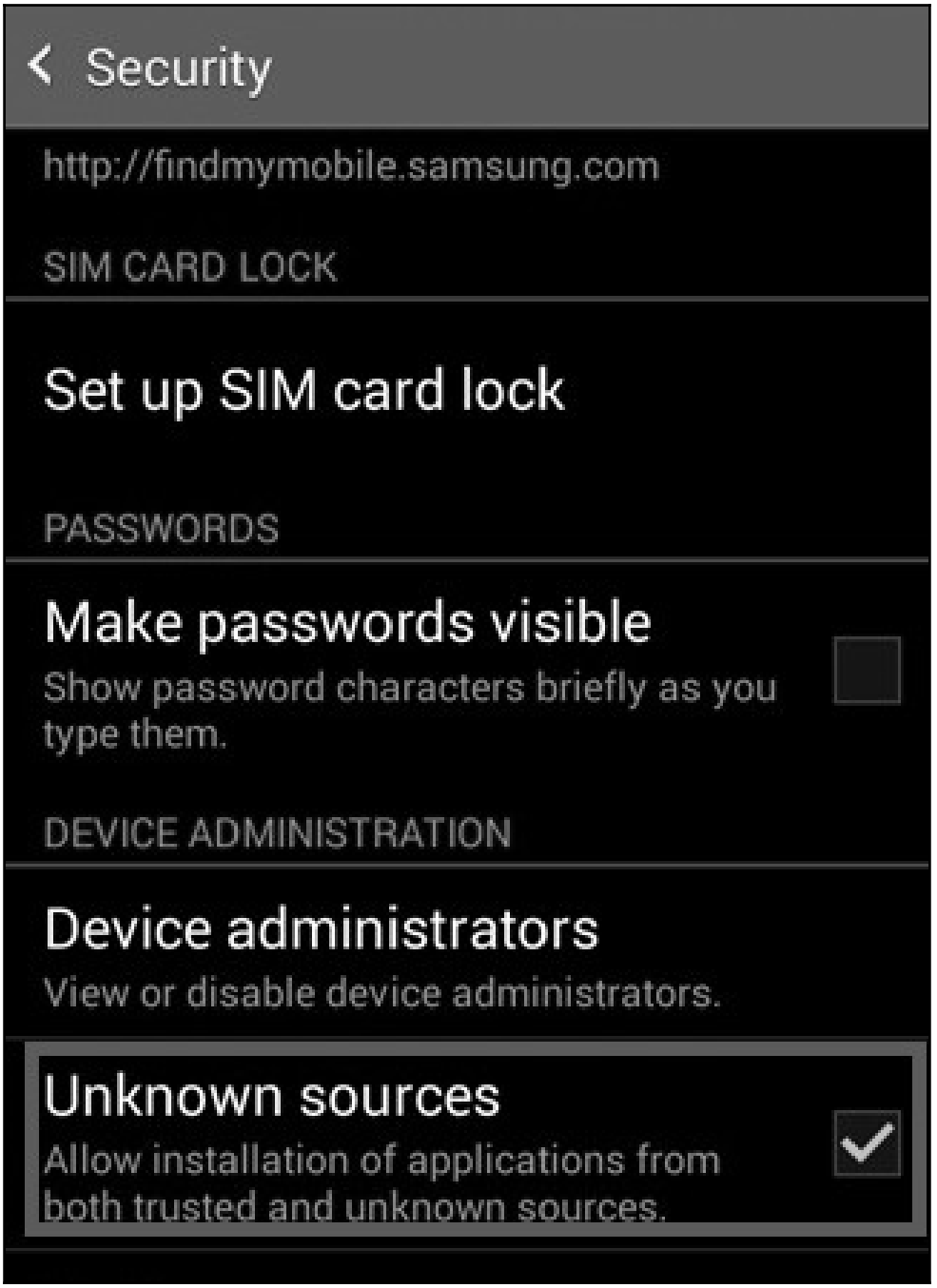
```
C:\android-sdk\platform-tools>adb.exe shell pm path com.android.chrome
package:/data/app/com.android.chrome-1.apk
```

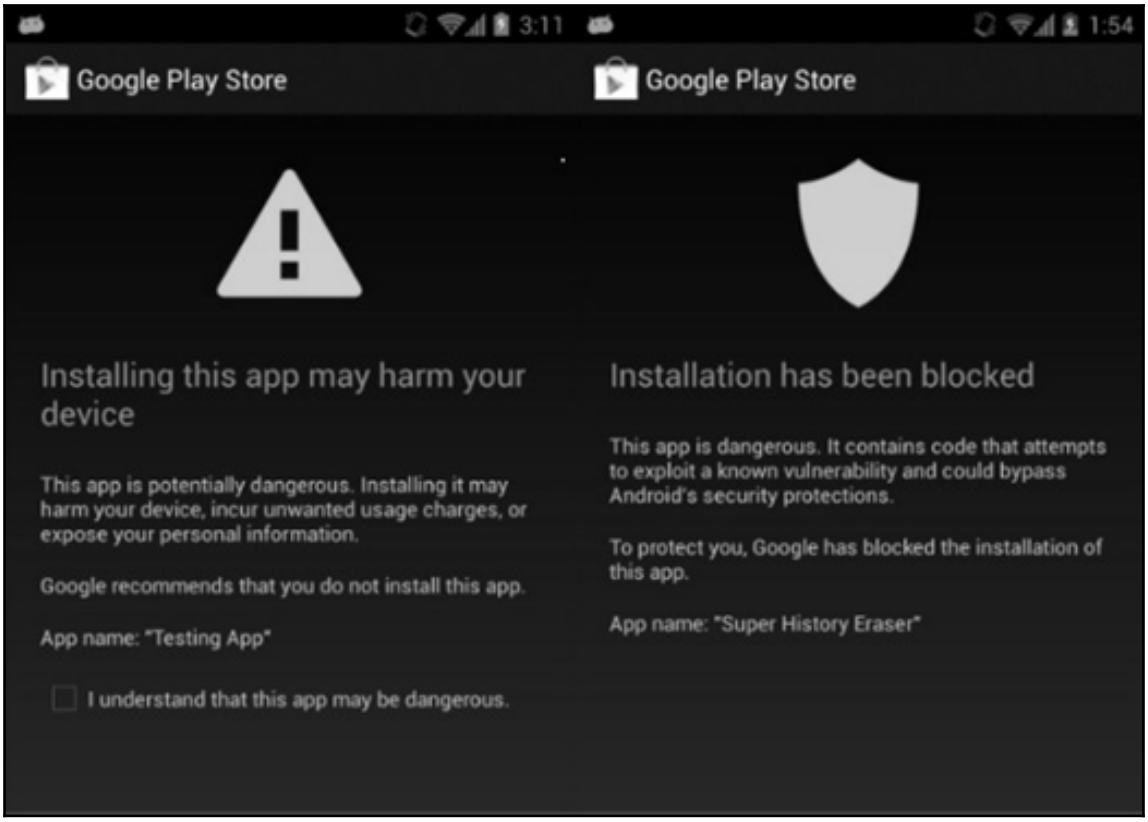
```
C:\android-sdk\platform-tools>adb.exe pull /data/app/com.android.chrome-1.apk C:\temp
3706 KB/s (42168820 bytes in 11.110s)
```

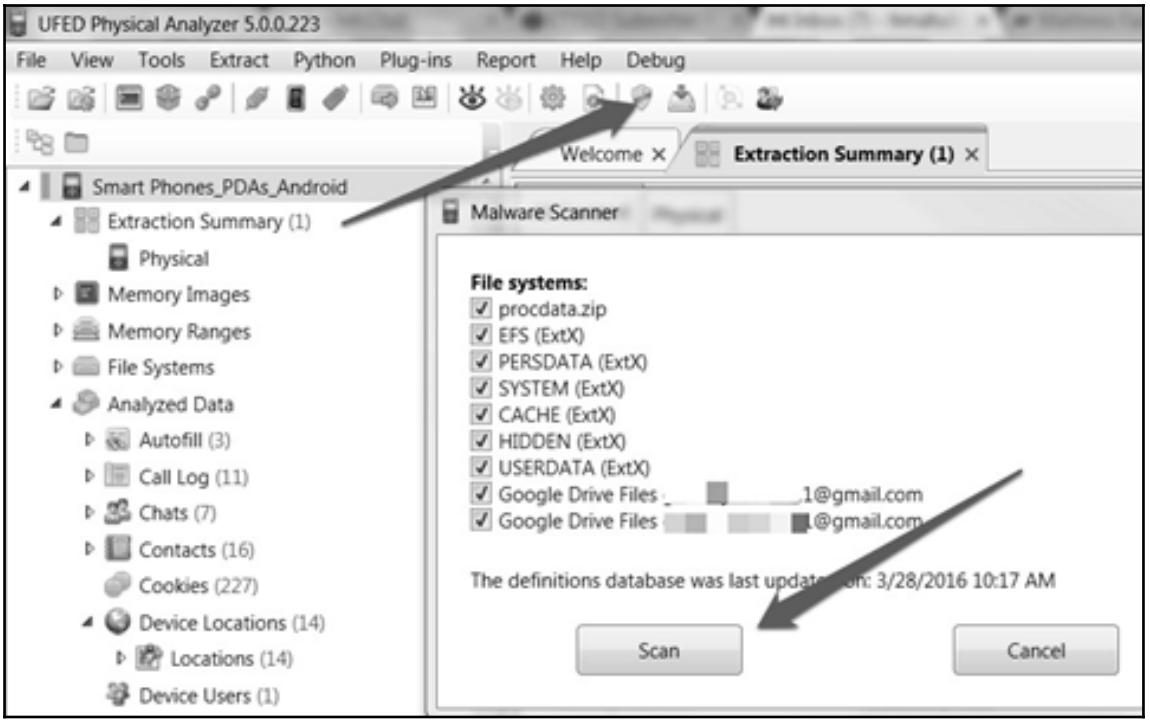
Name	Date modified	Type	Size
assets	01-02-2014 15:32	File folder	
com	01-02-2014 15:32	File folder	
lib	01-02-2014 15:32	File folder	
META-INF	01-02-2014 15:32	File folder	
res	01-02-2014 15:32	File folder	
AndroidManifest.xml	07-01-2014 11:10	XML Document	43 KB
classes.dex	07-01-2014 11:10	DEX File	3,843 KB
com.twitter.android-1.zip	01-02-2014 15:31	WinRAR ZIP archive	11,877 KB
resources.arsc	07-01-2014 11:10	ARSC File	2,282 KB

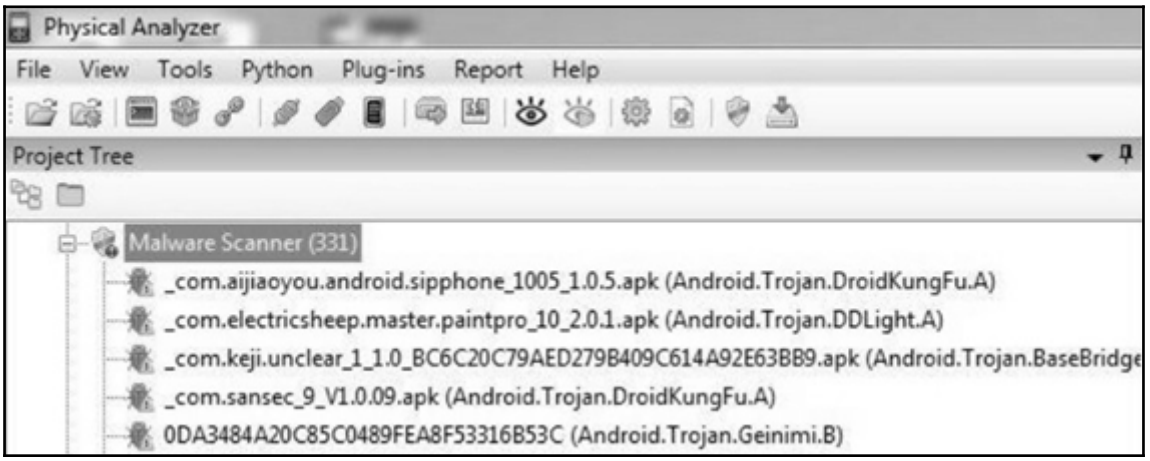
Name	Date modified	Type	Size
lib	05-06-2013 10:24	File folder	
classes.dex	07-01-2014 11:10	DEX File	3,843 KB
classes-dex2jar.jar	01-02-2014 15:43	Executable Jar File	3,699 KB
d2j-apk-sign.bat	05-06-2013 10:21	Windows Batch File	1 KB
d2j-apk-sign.sh	05-06-2013 10:21	SH File	2 KB
d2j-asm-verify.bat	05-06-2013 10:21	Windows Batch File	1 KB
d2j-asm-verify.sh	05-06-2013 10:21	SH File	2 KB
d2j-decrpyt-string.bat	05-06-2013 10:21	Windows Batch File	1 KB
d2j-decrpyt-string.sh	05-06-2013 10:21	SH File	2 KB
d2j-dex2jar.bat	05-06-2013 10:21	Windows Batch File	1 KB


Java Decompiler - AuthorizeAppActivity.class
File Edit Navigate Search Help
classes-dex2jar.jar
android.support.v4
co.vine.android
com
crashlytics.android
fasterxml.jackson.core
google.android
googlecode
mobeta.android.dslv
twitter
android
samsung
data
model
single
AuthorizeAppActivity
AuthorizeAppActivity
AuthorizeAppActivity.class
package com.twitter.android;
import android.accounts.Account;
public class AuthorizeAppActivity
extends BaseFragmentActivity
implements ag
{
private ServiceConnection a;
private String b;
private String c;
private CharSequence b()
{


Security
http://findmymobile.samsung.com
SIM CARD LOCK
Set up SIM card lock
PASSWORDS
Make passwords visible
Show password characters briefly as you type them.
DEVICE ADMINISTRATION
Device administrators
View or disable device administrators.
Unknown sources
Allow installation of applications from both trusted and unknown sources.

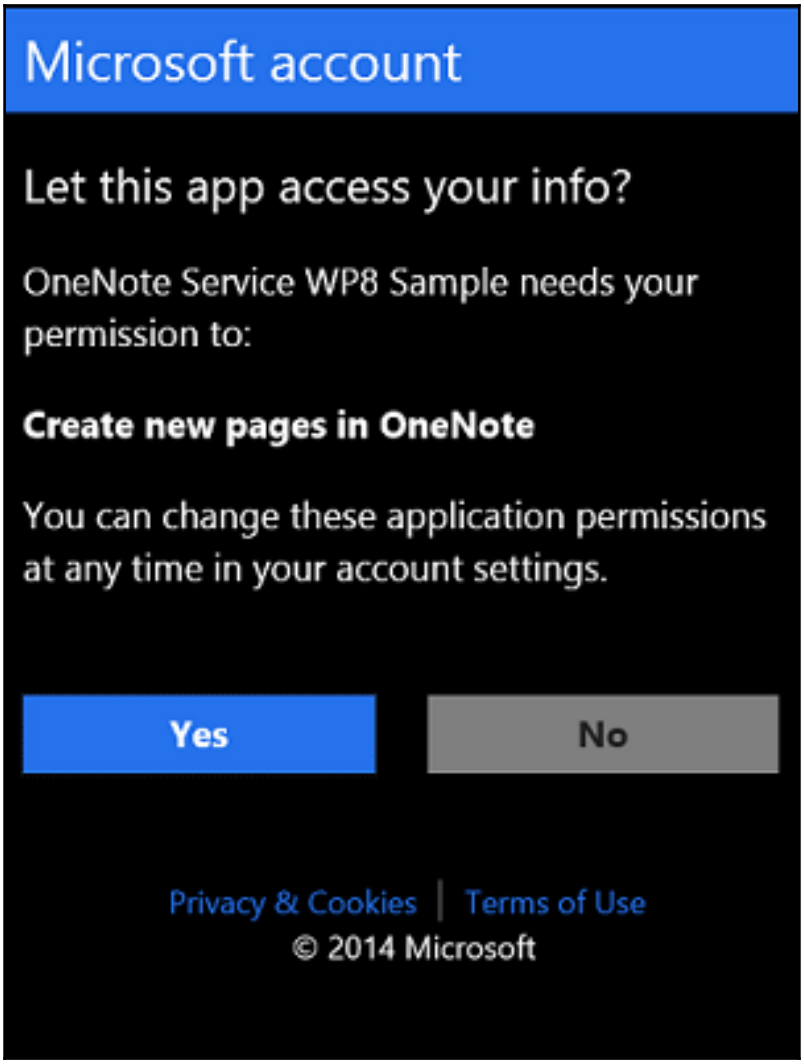

3:11
Google Play Store
Installing this app may harm your device
This app is potentially dangerous. Installing it may harm your device, incur unwanted usage charges, or expose your personal information.
Google recommends that you do not install this app.
App name: "Testing App"
I understand that this app may be dangerous.
1:54
Google Play Store
Installation has been blocked
This app is dangerous. It contains code that attempts to exploit a known vulnerability and could bypass Android's security protections.
To protect you, Google has blocked the installation of this app.
App name: "Super History Eraser"

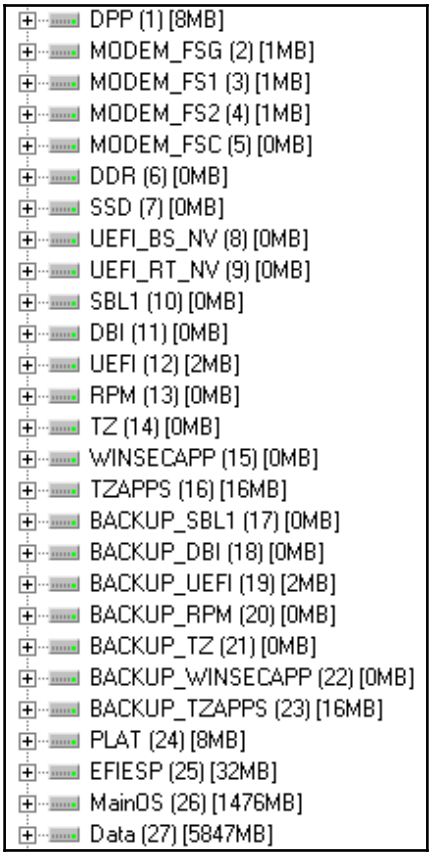

UFED Physical Analyzer 5.0.0.223
File View Tools Extract Python Plug-ins Report Help Debug
Welcome
Extraction Summary (1)
Smart Phones_PDAs_Android
Extraction Summary (1)
Physical
Memory Images
Memory Ranges
File Systems
Analyzed Data
Autofill (3)
Call Log (11)
Chats (7)
Contacts (16)
Cookies (227)
Device Locations (14)
Locations (14)
Device Users (1)
Malware Scanner
File systems:
procdata.zip
EFS (ExtX)
PERSDATA (ExtX)
SYSTEM (ExtX)
CACHE (ExtX)
HIDDEN (ExtX)
USERDATA (ExtX)
Google Drive Files
Google Drive Files
The definitions database was last updat
n: 3/28/2016 10:17 AM
Scan
Cancel

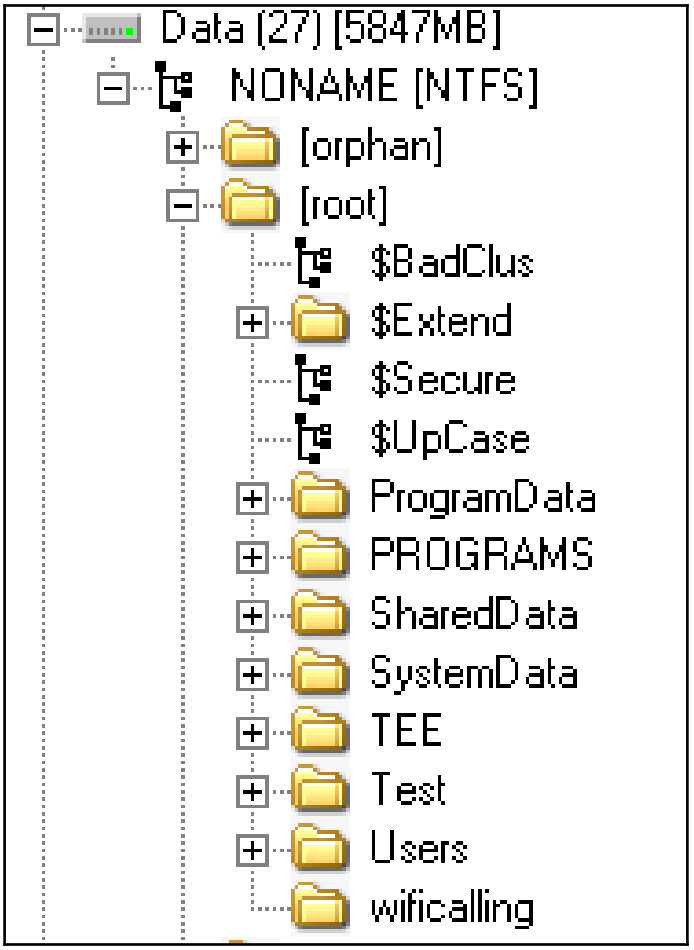

Physical Analyzer
File View Tools Python Plug-ins Report Help
Project Tree
Malware Scanner (331)
_com.aijiaoyou.android.sipphone_1005_1.0.5.apk (Android.Trojan.DroidKungFu.A)
_com.electricsheep.master.paintpro_10_2.0.1.apk (Android.Trojan.DDLight.A)
_com.keji.unclear_1_1.0_BC6C20C79AED279B409C614A92E63BB9.apk (Android.Trojan.BaseBridge
_com.sansec_9_V1.0.09.apk (Android.Trojan.DroidKungFu.A)
0DA3484A20C85C0489FEA8F53316B53C (Android.Trojan.Geinimi.B)

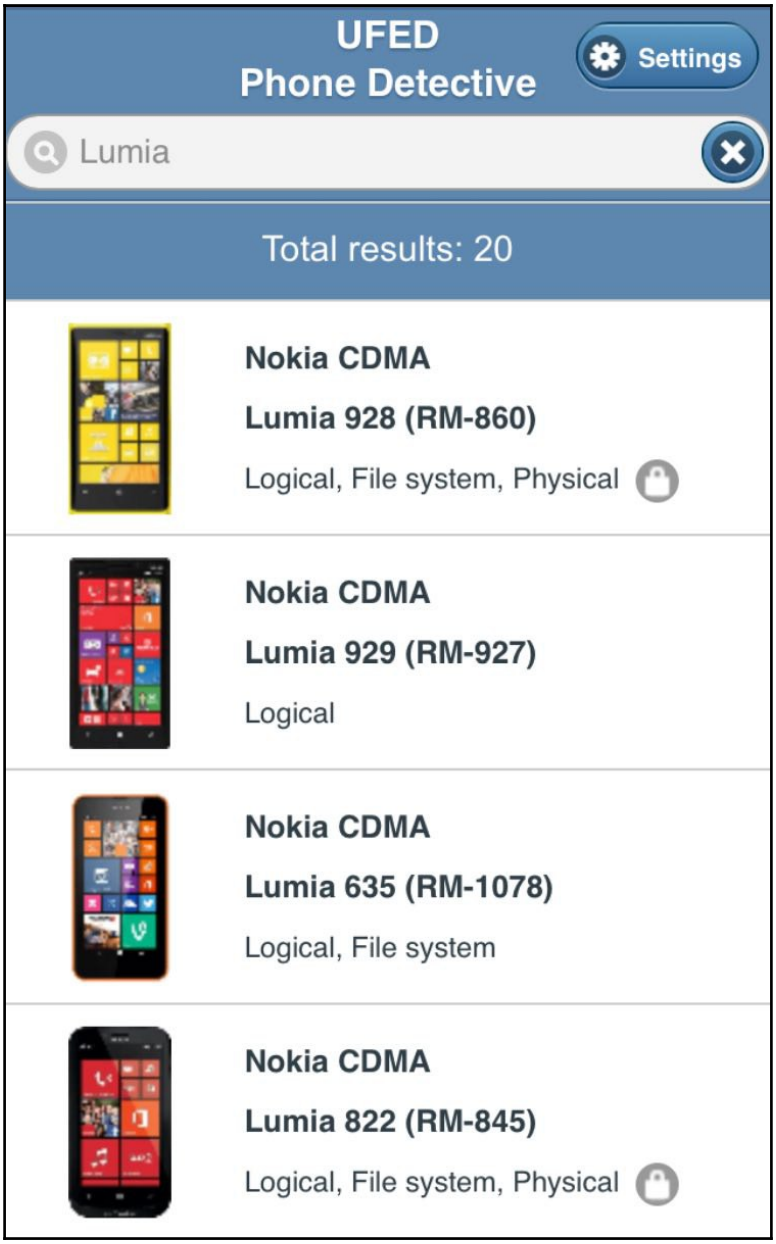
```
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION">
</uses-permission>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION">
</uses-permission>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE">
</uses-permission>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE">
</uses-permission>
<uses-permission android:name="android.permission.CALL_PHONE">
</uses-permission>
<uses-permission android:name="android.permission.CAMERA">
</uses-permission>
<uses-permission android:name="android.permission.GET_ACCOUNTS">
</uses-permission>
<uses-permission android:name="android.permission.INTERNET">
</uses-permission>
<uses-permission android:name="android.permission.MANAGE_ACCOUNTS">
</uses-permission>
<uses-permission android:name="android.permission.READ_CONTACTS">
</uses-permission>
<uses-permission android:name="android.permission.READ_PHONE_STATE">
</uses-permission>
<uses-permission android:name="android.permission.USE_CREDENTIALS">
</uses-permission>
<uses-permission android:name="android.permission.VIBRATE">
</uses-permission>
<uses-permission android:name="android.permission.WRITE_SETTINGS">
</uses-permission>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE">
</uses-permission>
```

Chapter 12: Windows Phone Forensics


Microsoft account
Let this app access your info?
OneNote Service WP8 Sample needs your permission to:
Create new pages in OneNote
You can change these application permissions at any time in your account settings.
Yes
No
Privacy & Cookies | Terms of Use
© 2014 Microsoft

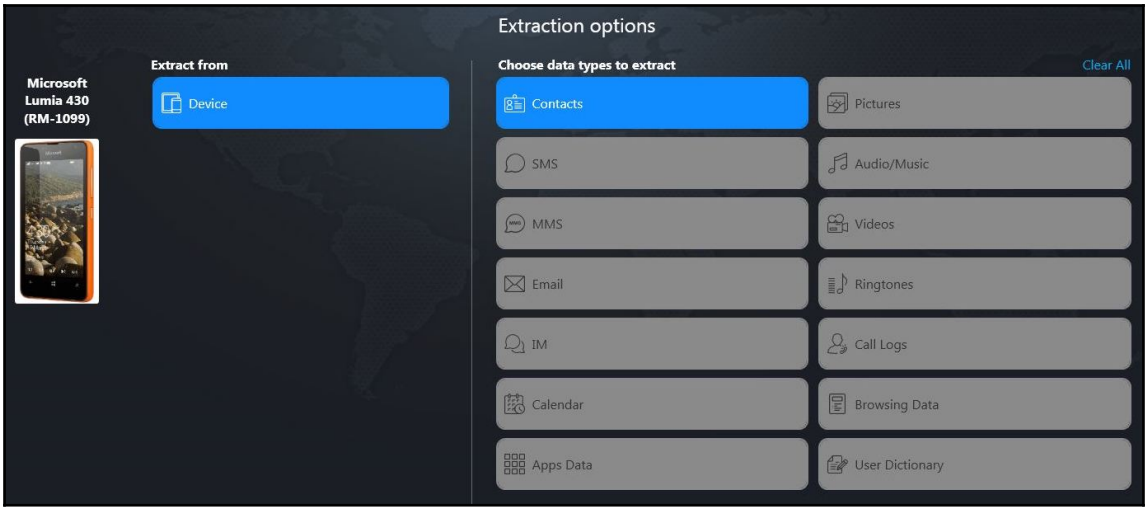

DPP (1) [8MB]
MODEM_FSG (2) [1MB]
MODEM_FS1 (3) [1MB]
MODEM_FS2 (4) [1MB]
MODEM_FSC (5) [0MB]
DDR (6) [0MB]
SSD (7) [0MB]
UEFI_BS_NV (8) [0MB]
UEFI_RT_NV (9) [0MB]
SBL1 (10) [0MB]
DBI (11) [0MB]
UEFI (12) [2MB]
RPM (13) [0MB]
TZ (14) [0MB]
WINSECAPP (15) [0MB]
TZAPPS (16) [16MB]
BACKUP_SBL1 (17) [0MB]
BACKUP_DBI (18) [0MB]
BACKUP_UEFI (19) [2MB]
BACKUP_RPM (20) [0MB]
BACKUP_TZ (21) [0MB]
BACKUP_WINSECAPP (22) [0MB]
BACKUP_TZAPPS (23) [16MB]
PLAT (24) [8MB]
EFIESP (25) [32MB]
MainOS (26) [1476MB]
Data (27) [5847MB]


Data (27) [5847MB]
NONAME [NTFS]
[orphan]
[root]
$BadClus
$Extend
$Secure
$UpCase
ProgramData
PROGRAMS
SharedData
SystemData
TEE
Test
Users
wificalling


UFED
Phone Detective
Settings
Lumia
Total results: 20
Nokia CDMA
Lumia 928 (RM-860)
Logical, File system, Physical
Nokia CDMA
Lumia 929 (RM-927)
Logical
Nokia CDMA
Lumia 635 (RM-1078)
Logical, File system
Nokia CDMA
Lumia 822 (RM-845)
Logical, File system, Physical

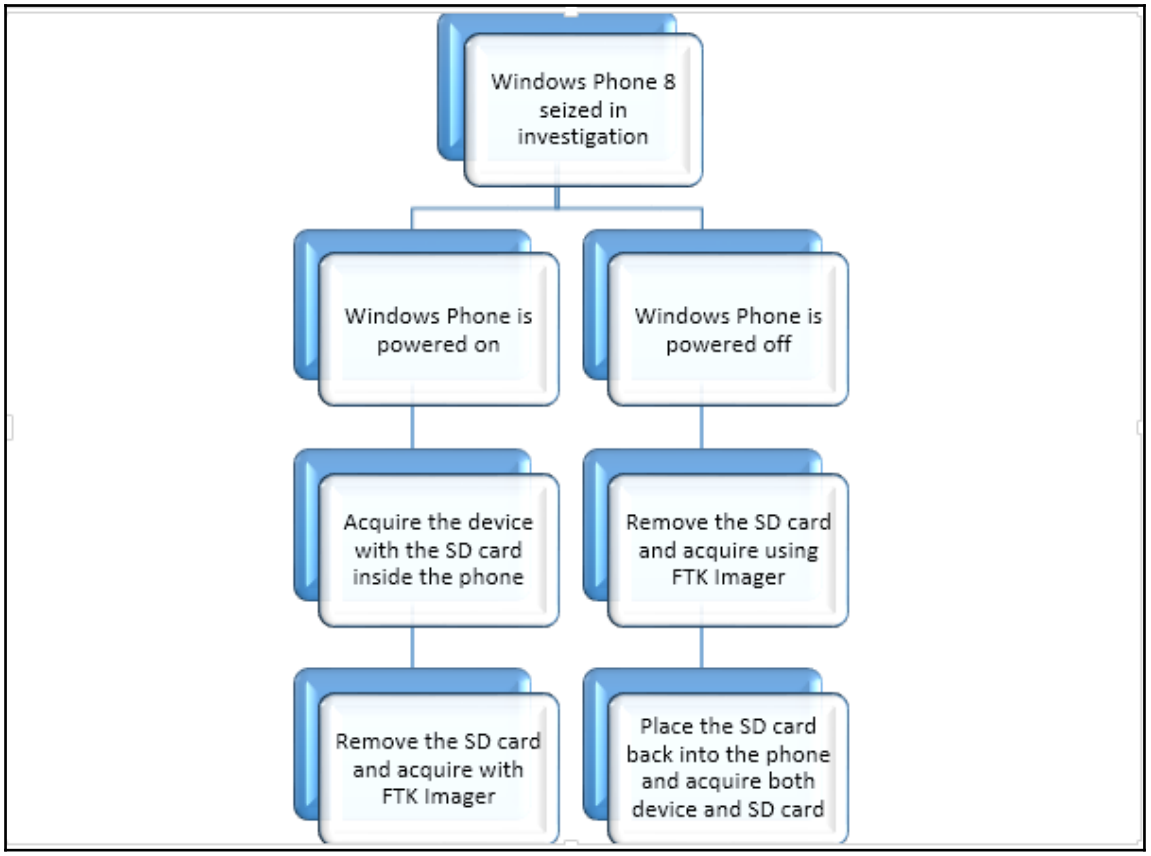

Logical Extraction
File System Extraction
Capture Images

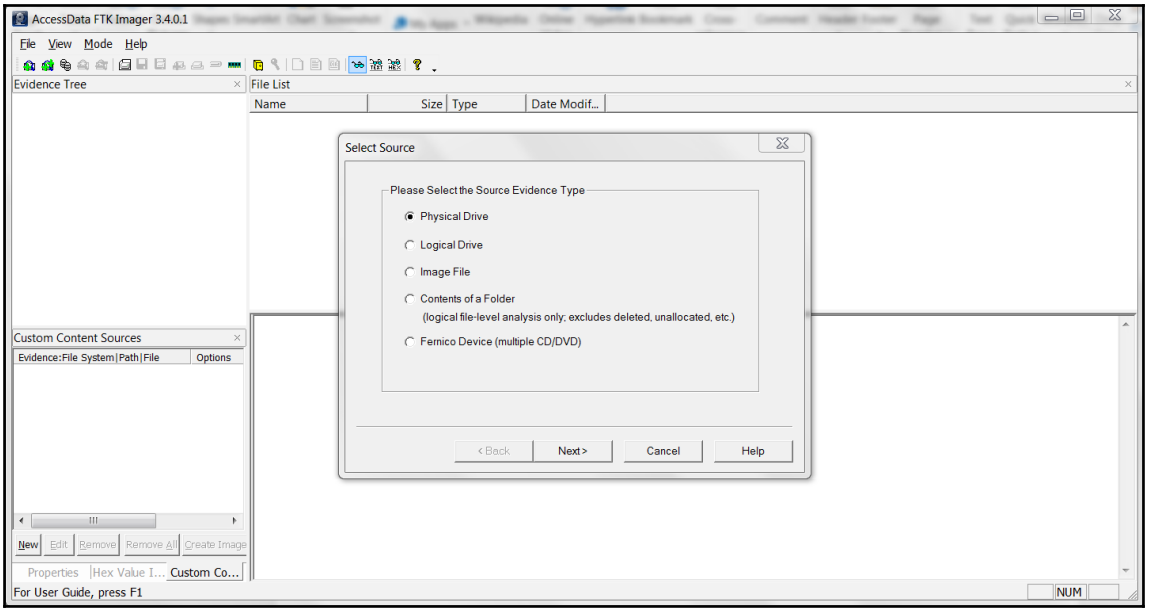

USB cable 100
Bluetooth

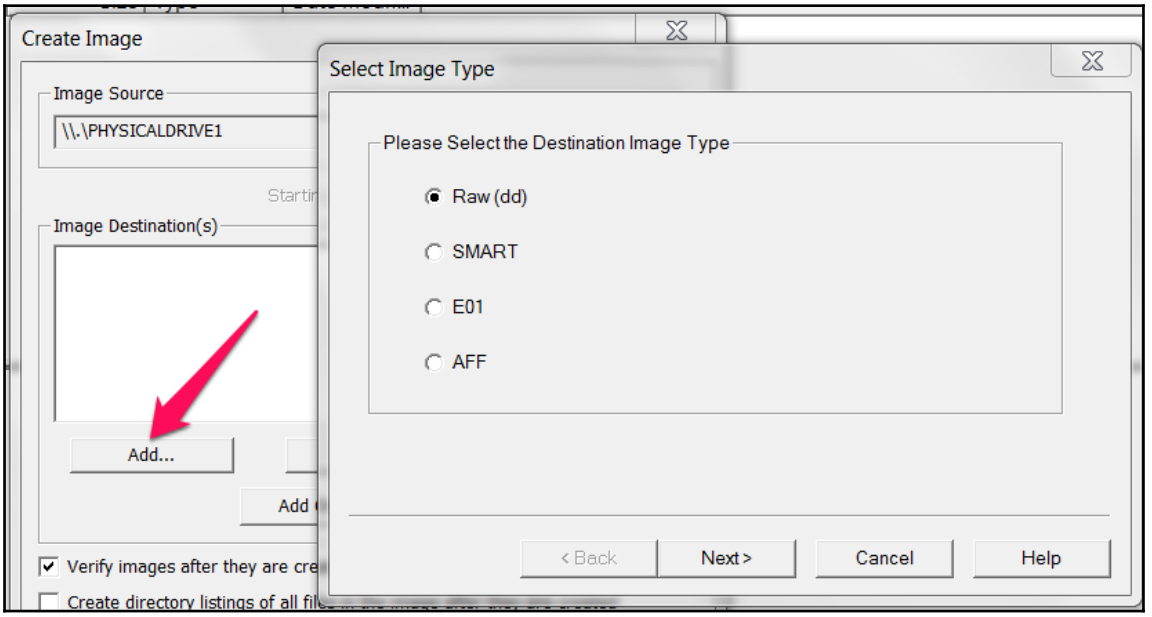

Extraction options
Microsoft Lumia 430 (RM-1099)
Extract from
Device
Choose data types to extract
Clear All
Contacts
Pictures
SMS
Audio/Music
MMS
Videos
Email
Ringtones
IM
Call Logs
Calendar
Browsing Data
Apps Data
User Dictionary

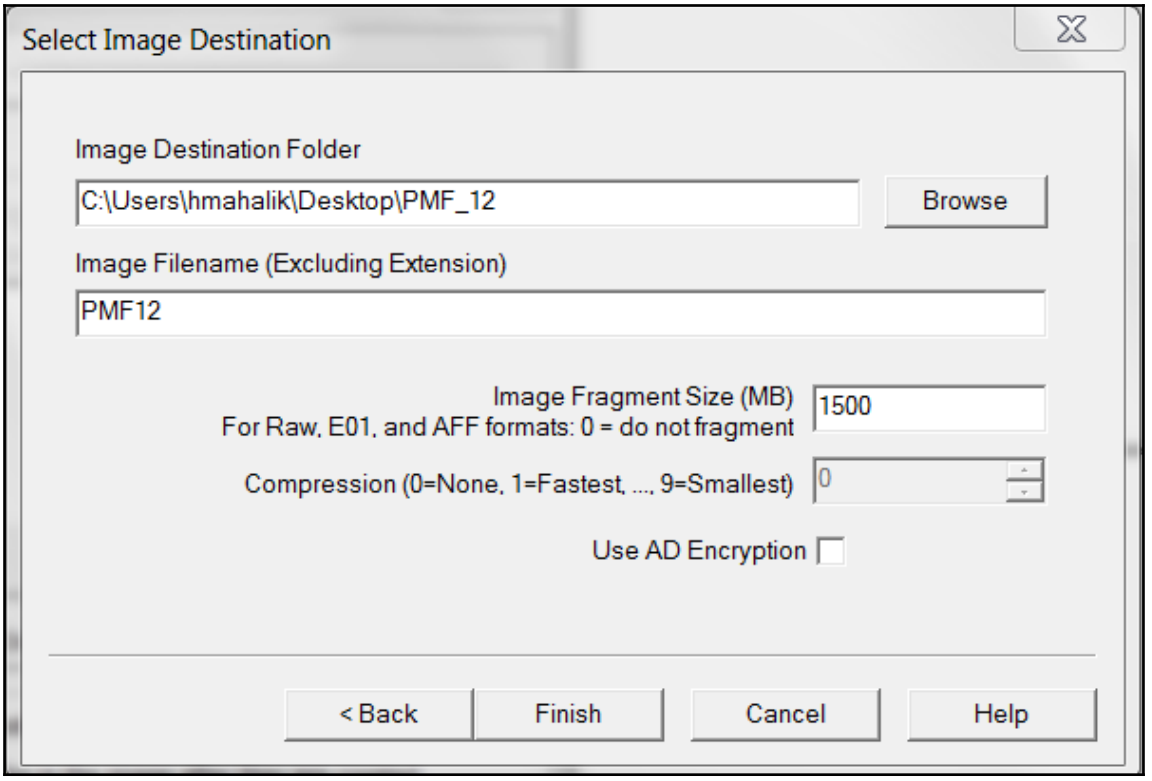

Home
Windows Phone Device Manager
Windows Phone
Manage applications
View, install and uninstall Windows Phone applications
Explore files and folders
View and copy files from or to your Windows Phone
Set up sync
Sync files and folders with your Windows Phone
Set ringtones
Add, select, or create ringtones for your Windows Phone
Organize your music, pictures and videos
Use Zune software to organize and sync music, pictures and videos with your Windows Phone
View device information
View detailed information about your Windows Phone
Change settings
Configure Windows Phone Device Manager
Connected
Name:
Model:
Software: Windows ® Phone 7
OS Version: 7.0.7004
Total Storage: 7,20 GB
Available Storage: 685,43 MB
Battery: 97 %
Mobile Operator: F SFR
More information

Name	Publisher	Installed On	Size	Version
Installed Applications				
TouchXplorer	Julien Schapman	28/02/2011	664,91 KB	1.0.0.0
TouchXperience	Julien Schapman	28/02/2011	2,42 MB	1.0.2.0
Bluetooth	Julien Schapman	28/02/2011	587,02 KB	1.0.0.0
Config. avancée	Julien Schapman	28/02/2011	1,31 MB	1.1.0.1
Éditeur de registre	Julien Schapman	28/02/2011	1,29 MB	1.1.0.0
Purchased Applications				
Config Connexion	HTC Corporation		913,10 KB	1.0.0.0
Convertisseur	HTC Corporation		1,82 MB	1.0.0.0
HTC Hub	HTC Corporation		18,04 MB	1.0.0.0


Windows Phone 8 seized in investigation
Windows Phone is powered on
Windows Phone is powered off
Acquire the device with the SD card inside the phone
Remove the SD card and acquire using FTK Imager
Remove the SD card and acquire with FTK Imager
Place the SD card back into the phone and acquire both device and SD card


AccessData FTK Imager 3.4.0.1
File View Mode Help
Evidence Tree
File List
Name
Size
Type
Date Modif...
Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value I...
Custom Co...
For User Guide, press F1
NUM


Create Image
Image Source
\\.\PHYSICALDRIVE1
Image Destination(s)
Add...
Verify images after they are cre
Create directory listings of all fil
Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help



[current folder]	2015-04-06 20:07:11 EDT	2015-04-06 20:07:11 EDT	2015-04-06 20:07:11 EDT	2017-05-20 12:13:54 EDT
[parent folder]	2017-05-23 10:16:20 EDT	2017-05-23 10:16:20 EDT	2017-05-23 10:16:20 EDT	2017-05-20 12:13:37 EDT
store.vol	2015-04-06 20:07:30 EDT	2015-04-06 20:07:30 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT
USS.chk	2015-04-06 20:07:30 EDT	2015-04-06 20:07:30 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT
USS.log	2015-04-06 20:07:30 EDT	2015-04-06 20:07:30 EDT	2017-06-05 13:37:25 EDT	2017-06-05 13:37:25 EDT
USS00005.log	2017-07-26 18:53:09 EDT	2017-07-26 18:53:09 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT
USSres00001.jrs	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT
USSres00002.jrs	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT
USStmp.log	2017-07-07 16:25:07 EDT	2017-07-26 18:53:09 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT

[current folder]	2015-04-06 20:07:11 EDT	2015-04-06 20:07:11 EDT	2015-04-06 20:07:11 EDT	2017-05-20 12:13:54 EDT
[parent folder]	2017-05-23 10:16:20 EDT	2017-05-23 10:16:20 EDT	2017-05-23 10:16:20 EDT	2017-05-20 12:13:37 EDT
FavoriteData.xml	2017-07-21 20:18:19 EDT	2017-07-21 20:18:19 EDT	2017-06-12 17:31:43 EDT	2017-06-12 17:31:43 EDT
FavoriteData.xml.tmp	2017-07-21 20:18:19 EDT	2017-07-21 20:18:19 EDT	2017-06-12 17:31:43 EDT	2017-06-12 17:31:43 EDT
Phone	2015-04-06 20:07:30 EDT	2015-04-06 20:07:30 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT
UDM.chk	2015-04-06 20:07:30 EDT	2015-04-06 20:07:30 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT
UDM.log	2015-04-06 20:07:30 EDT	2015-04-06 20:07:30 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT
UDM00001.log	2017-07-19 08:17:25 EDT	2017-07-19 11:03:33 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT
UDMres00001.jrs	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT
UDMres00002.jrs	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT	2017-05-20 12:13:54 EDT
UDMtmp.log	2017-07-19 11:03:33 EDT	2017-07-19 11:03:33 EDT	2017-07-19 11:03:33 EDT	2017-07-19 11:03:33 EDT

[current folder]	2017-07-25 20:40:46 EDT	2017-07-25 20:40:46 EDT	2017-07-25 20:40:46 EDT	2017-05-20 12:13:55 EDT
[parent folder]	2017-05-20 12:36:23 EDT	2017-05-20 12:36:23 EDT	2017-05-20 12:36:23 EDT	2017-05-20 12:13:30 EDT
V01.chk	2015-04-06 21:41:57 EDT	2015-04-06 21:41:57 EDT	2017-05-20 12:13:55 EDT	2017-05-20 12:13:55 EDT
V01.log	2015-04-06 21:41:57 EDT	2015-04-06 21:41:57 EDT	2017-07-19 12:24:21 EDT	2017-07-19 12:24:21 EDT
V0100016.log	2017-07-25 20:40:46 EDT	2017-07-25 20:40:46 EDT	2017-07-20 20:10:03 EDT	2017-07-20 20:10:03 EDT
V01res00001.jrs	2017-05-20 12:13:55 EDT	2017-05-20 12:13:55 EDT	2017-05-20 12:13:55 EDT	2017-05-20 12:13:55 EDT
V01res00002.jrs	2017-05-20 12:13:55 EDT	2017-05-20 12:13:55 EDT	2017-05-20 12:13:55 EDT	2017-05-20 12:13:55 EDT
V01tmp.log	2017-07-24 17:23:26 EDT	2017-07-25 20:40:46 EDT	2017-06-21 12:17:53 EDT	2017-06-21 12:17:53 EDT
WebCacheV01.dat	2015-04-06 21:41:57 EDT	2015-04-06 21:41:57 EDT	2017-05-20 12:13:55 EDT	2017-05-20 12:13:55 EDT

https://www.bing.com/search?q=pandora&form=M...	Internet Explorer 10-11 Content	Web Related	6/21/2017 4:16:26 PM
res://WebBrowserControlRes.dll/ErrorPageTemplate....	Internet Explorer 10-11 Content	Web Related	7/24/2017 10:36:20 PM
https://www.bing.com/search/?q=free+texting+onli...	Internet Explorer 10-11 Content	Web Related	7/19/2017 4:23:57 PM
https://trc.taboola.com/sg/thetradedesk-network/1/...	Internet Explorer 10-11 Content	Web Related	7/19/2017 4:23:28 PM
https://www.bing.com/search?q=msn&form=MB10...	Internet Explorer 10-11 Content	Web Related	7/5/2017 8:10:41 PM
http://bing.com/az/hprichbg/rb/GlastonburyMoon_...	Internet Explorer 10-11 Content	Web Related	7/20/2017 2:53:41 PM
https://trc.taboola.com/sg/appnexus-network/1/rtb-...	Internet Explorer 10-11 Content	Web Related	7/20/2017 4:03:45 PM
https://www.bing.com/rms/Framework/cj.nj/f0fe13d...	Internet Explorer 10-11 Content	Web Related	7/20/2017 3:44:38 PM
http://bing.com/az/hprichbg/rb/GlastonburyMoon_...	Internet Explorer 10-11 Content	Web Related	7/20/2017 2:53:42 PM
https://www.bing.com/search?q=how%20to%20det...	Internet Explorer 10-11 Content	Web Related	7/20/2017 3:44:38 PM
https://www.bing.com/rms/BingCore.Bundle/cj.nj/21...	Internet Explorer 10-11 Content	Web Related	7/20/2017 3:44:38 PM
https://www.bing.com/rms/BingCore.Bundle/cj.nj/77...	Internet Explorer 10-11 Content	Web Related	7/5/2017 8:10:41 PM
http://bing.com/az/hprichbg/rb/Aldabra_EN-US100...	Internet Explorer 10-11 Content	Web Related	7/19/2017 4:29:05 PM
https://www.bing.com/search?ajax=scroll&infscroll=...	Internet Explorer 10-11 Content	Web Related	7/20/2017 3:44:48 PM
https://www.bing.com/search?q=how%20to%20det...	Internet Explorer 10-11 Content	Web Related	7/20/2017 3:38:41 PM

DETAILS

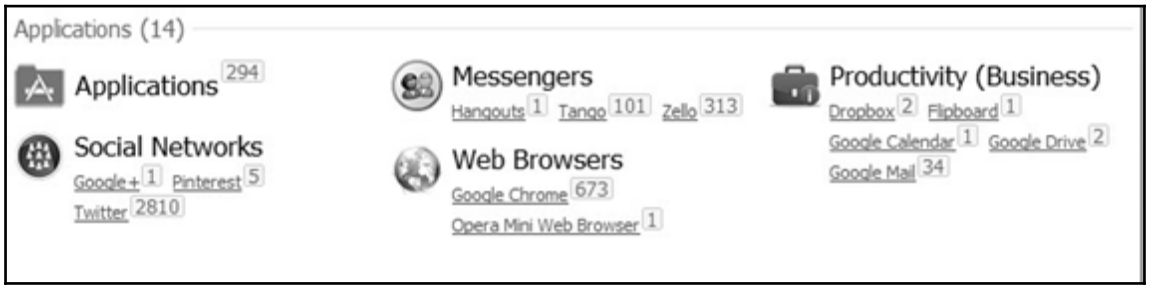
ARTIFACT INFORMATION

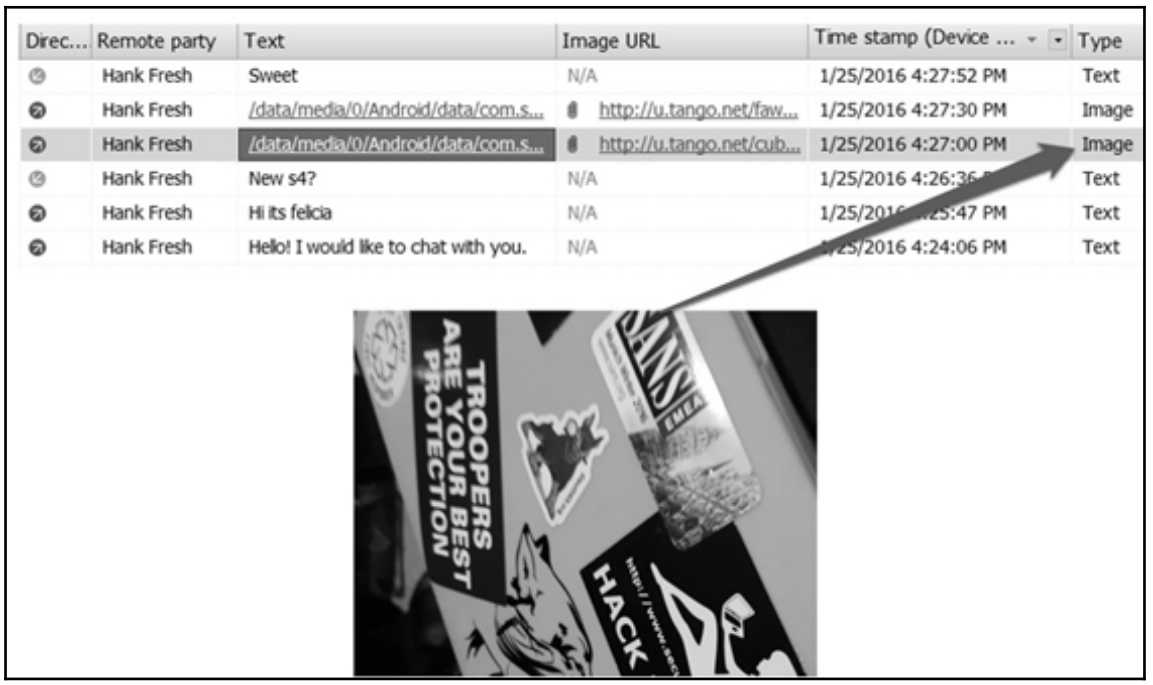
User	**DefApps**
URL	**res://webbrowsercontrolres.dll/dnserror.htm**
Accessed Date/Time	**7/24/2017 10:36:20 PM**
Page Title	**Can't find server**
Access Count	**1**

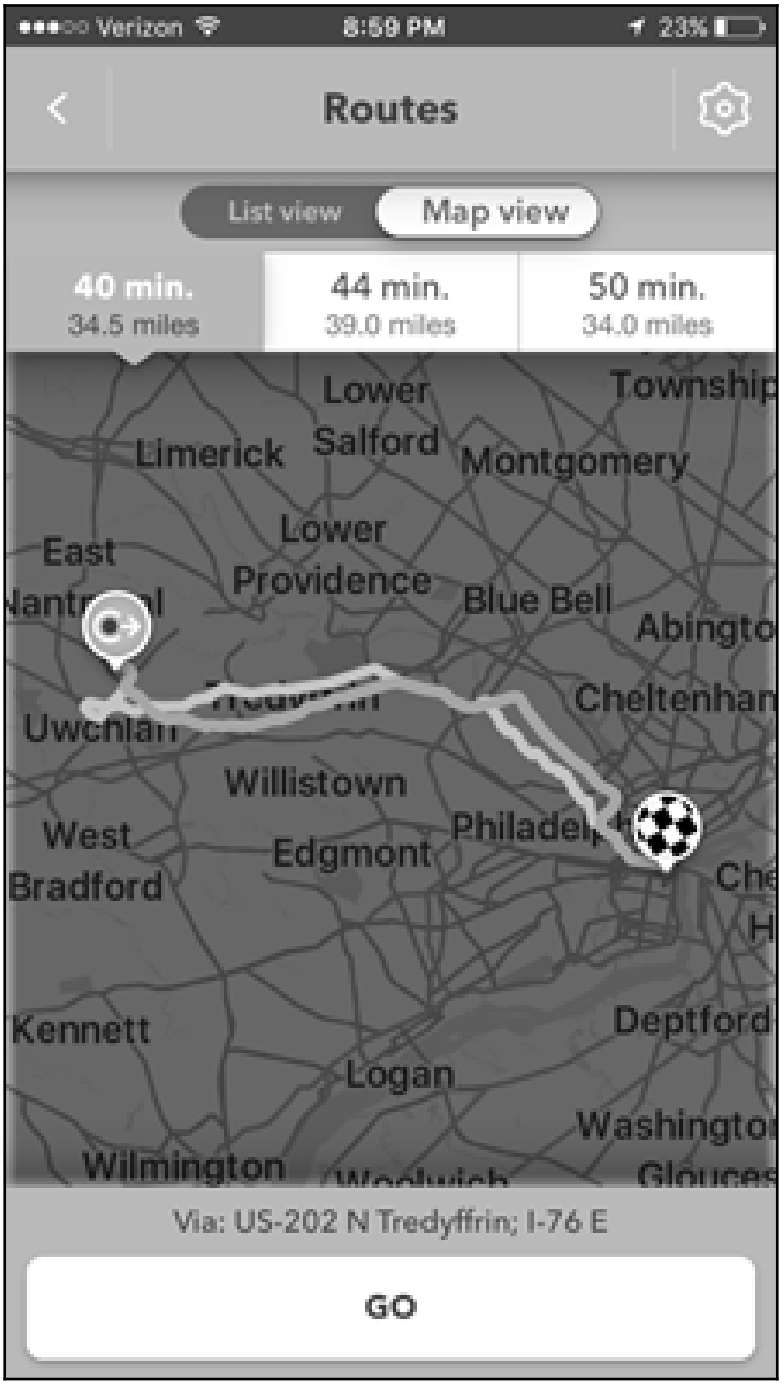
EVIDENCE INFORMATION

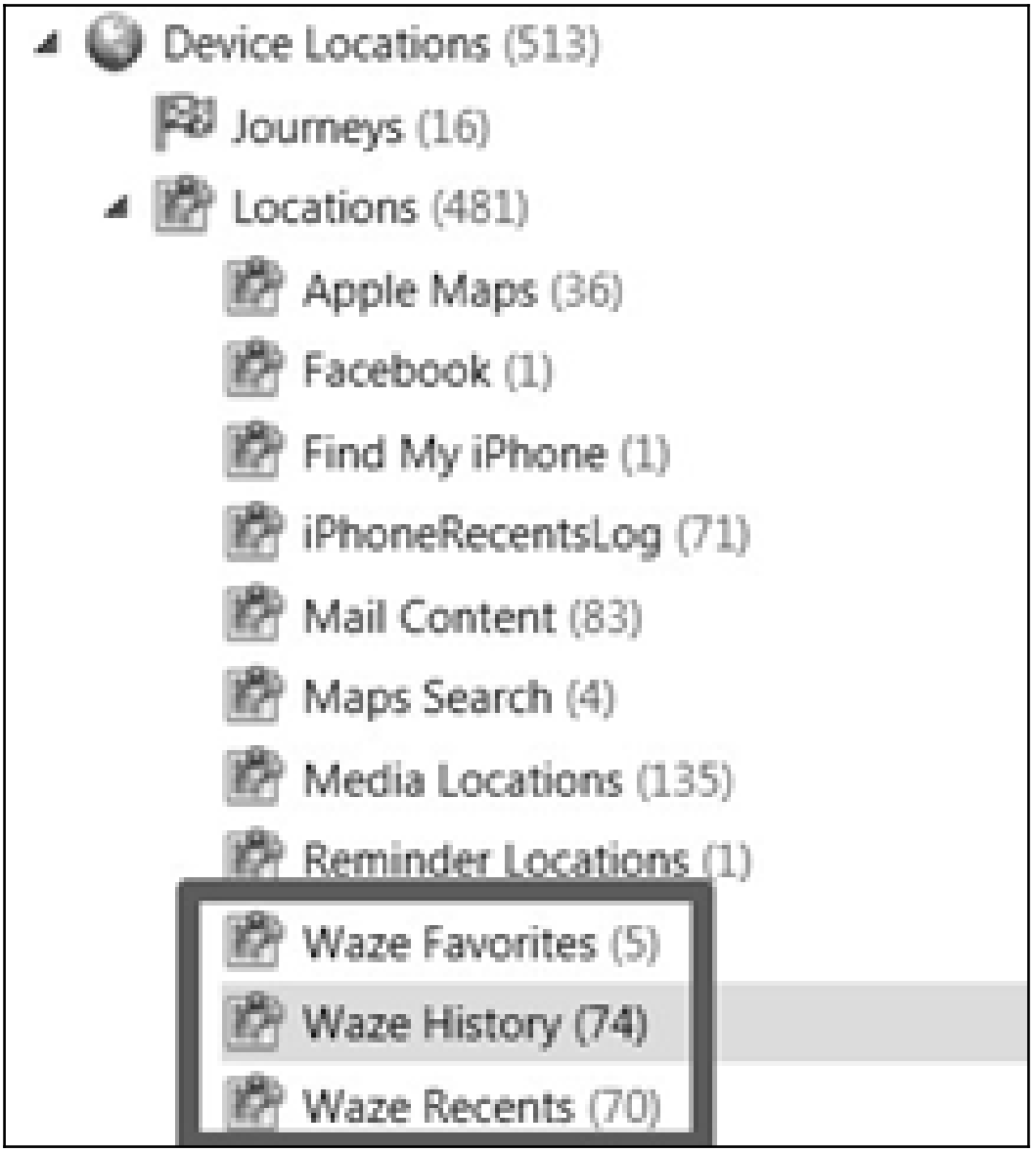
Source	**chipofLumia.001 - Partition 27 (Microsoft NTFS, 5.71 GB)\Users\DefApps\APPDATA\Local\Microsoft\Windows\WebCache\WebCacheV01.dat**
Location	**Table: Container_6 (EntryId: 1)**

Chapter 13: Parsing Third-Party Application Files

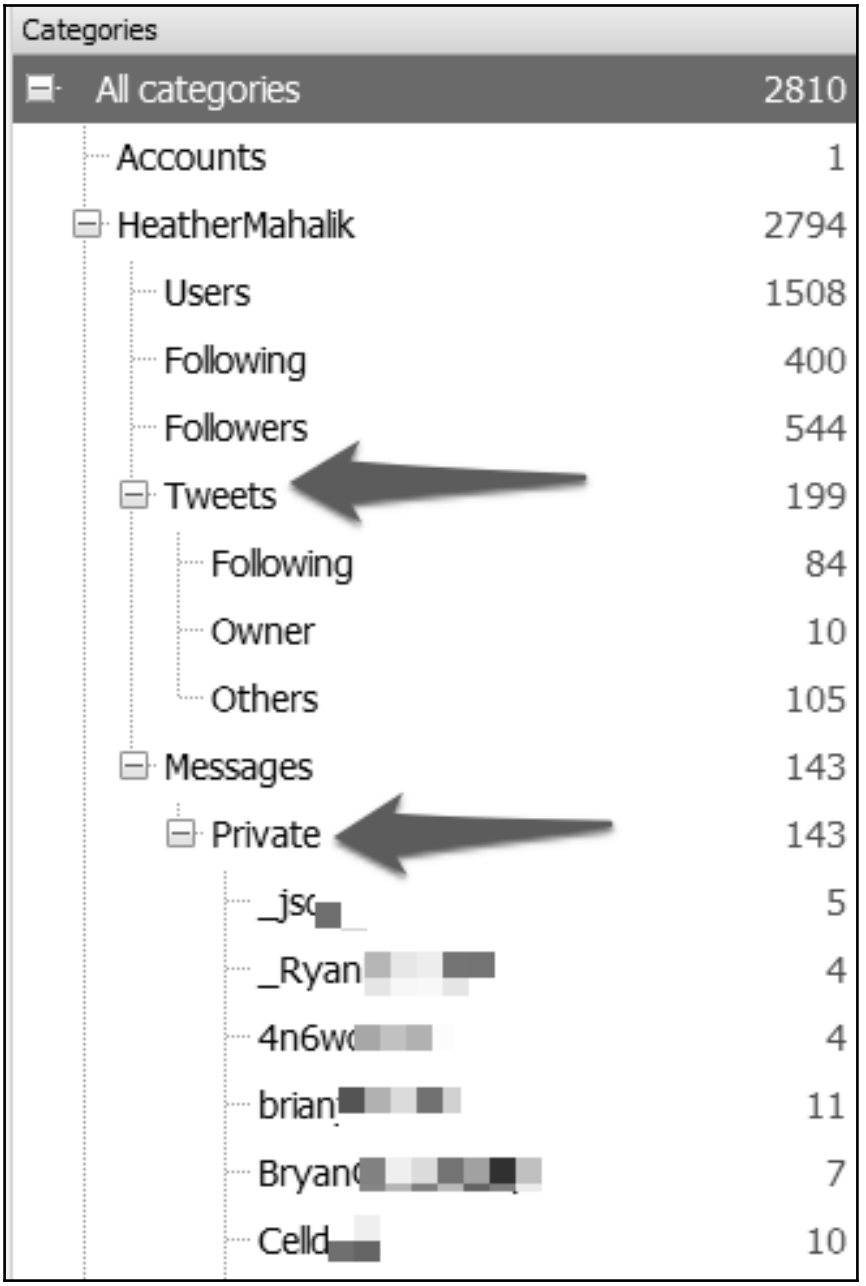





Verizon
8:59 PM
23%
Routes
List view
Map view
40 min.
34.5 miles
44 min.
39.0 miles
50 min.
34.0 miles
Lower
Township
Limerick
Salford
Montgomery
Lower
East
Providence
Blue Bell
Abingto
Cheltenhan
Uwchlan
Willistown
West
Bradford
Edgmont
Philadel
Che
H
Kennett
Deptford
Logan
Washingto
Wilmington
Glouces
Via: US-202 N Tredyffrin; I-76 E
GO

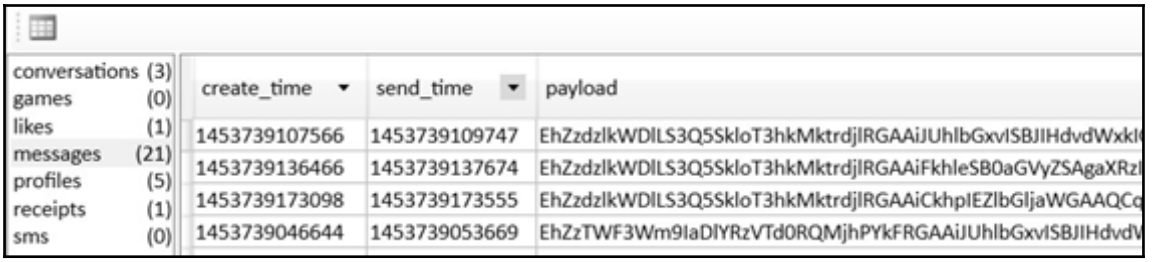

Device Locations (513)
Journeys (16)
Locations (481)
Apple Maps (36)
Facebook (1)
Find My iPhone (1)
iPhoneRecentsLog (71)
Mail Content (83)
Maps Search (4)
Media Locations (135)
Reminder Locations (1)
Waze Favorites (5)
Waze History (74)
Waze Recents (70)


Application information
Twitter
2810 items
com.twitter.android
Container: /data/data/com.twitter.android
Details:
Source table: Accounts
Source file: global.db
User name: HeatherMahalik
Name: Heather Mahalik
User ID:
Created (Device time): 1/26/2012 8:34:14 PM
(+00:00 UTC)
Followers: 3002
Followings: 454
Favorites: 1215
Tweets: 4037

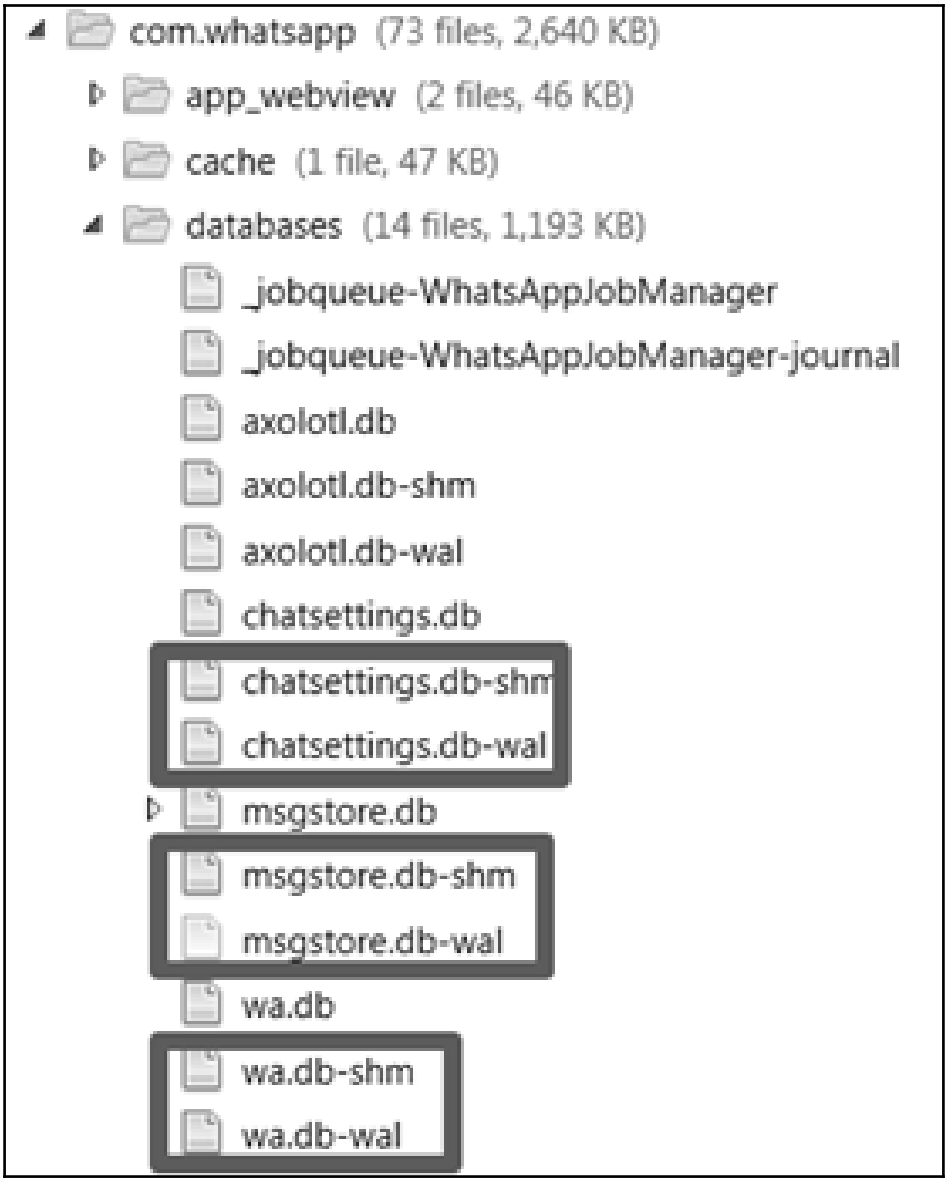

Categories
All categories 2810
Accounts 1
HeatherMahalik 2794
Users 1508
Following 400
Followers 544
Tweets 199
Following 84
Owner 10
Others 105
Messages 143
Private 143
5
4
4
11
7
10

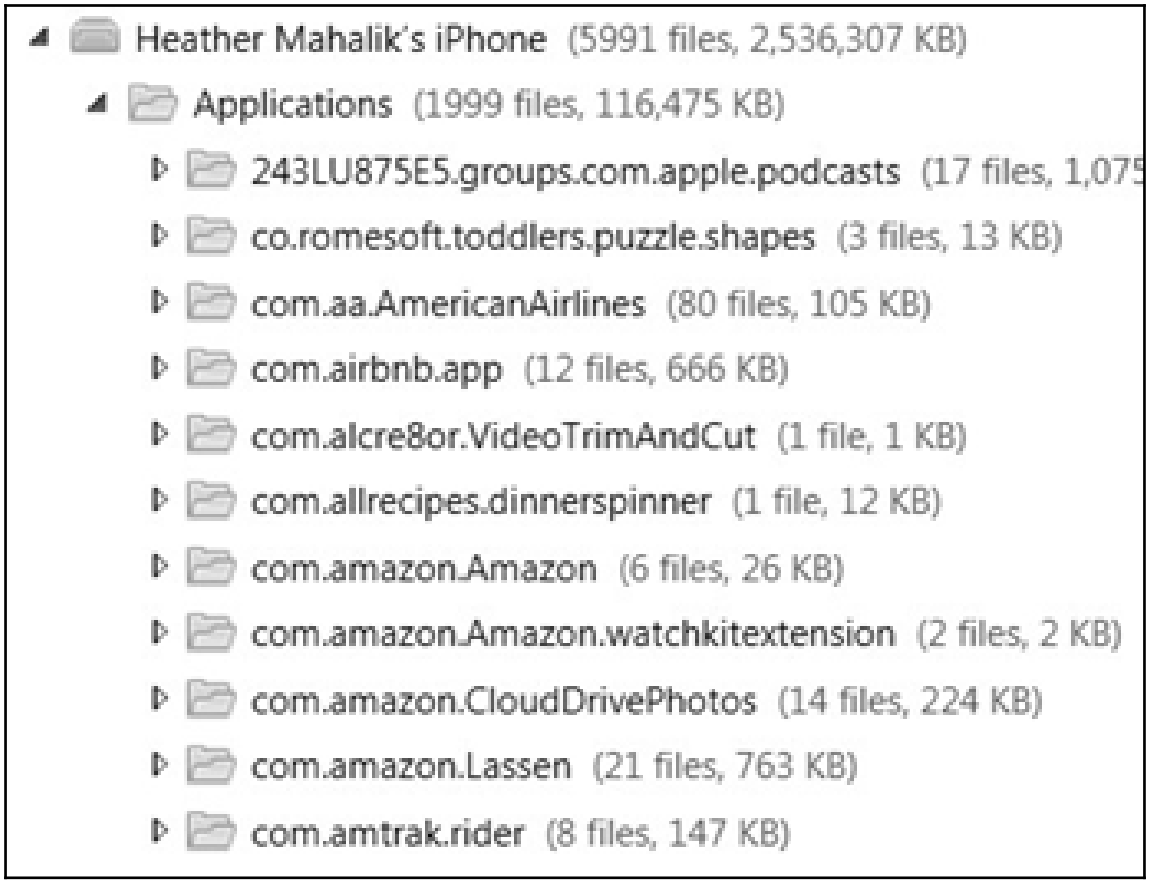
File
/data/data/com.twitter.android/cache/com.android.opengl.shaders_cache
/data/data/com.twitter.android/databases/0-scribe.db
/data/data/com.twitter.android/databases/0-scribe.db-journal
/data/data/com.twitter.android/databases/475222380-43.db
/data/data/com.twitter.android/databases/475222380-43.db-journal
/data/data/com.twitter.android/databases/475222380-dm.db
/data/data/com.twitter.android/databases/475222380-dm.db-journal
/data/data/com.twitter.android/databases/475222380-drafts.db
/data/data/com.twitter.android/databases/475222380-drafts.db-journal
/data/data/com.twitter.android/databases/475222380-scribe.db
/data/data/com.twitter.android/databases/475222380-scribe.db-journal
/data/data/com.twitter.android/databases/global.db
/data/data/com.twitter.android/databases/global.db-journal
/data/data/com.twitter.android/databases/persistent_jobs.db

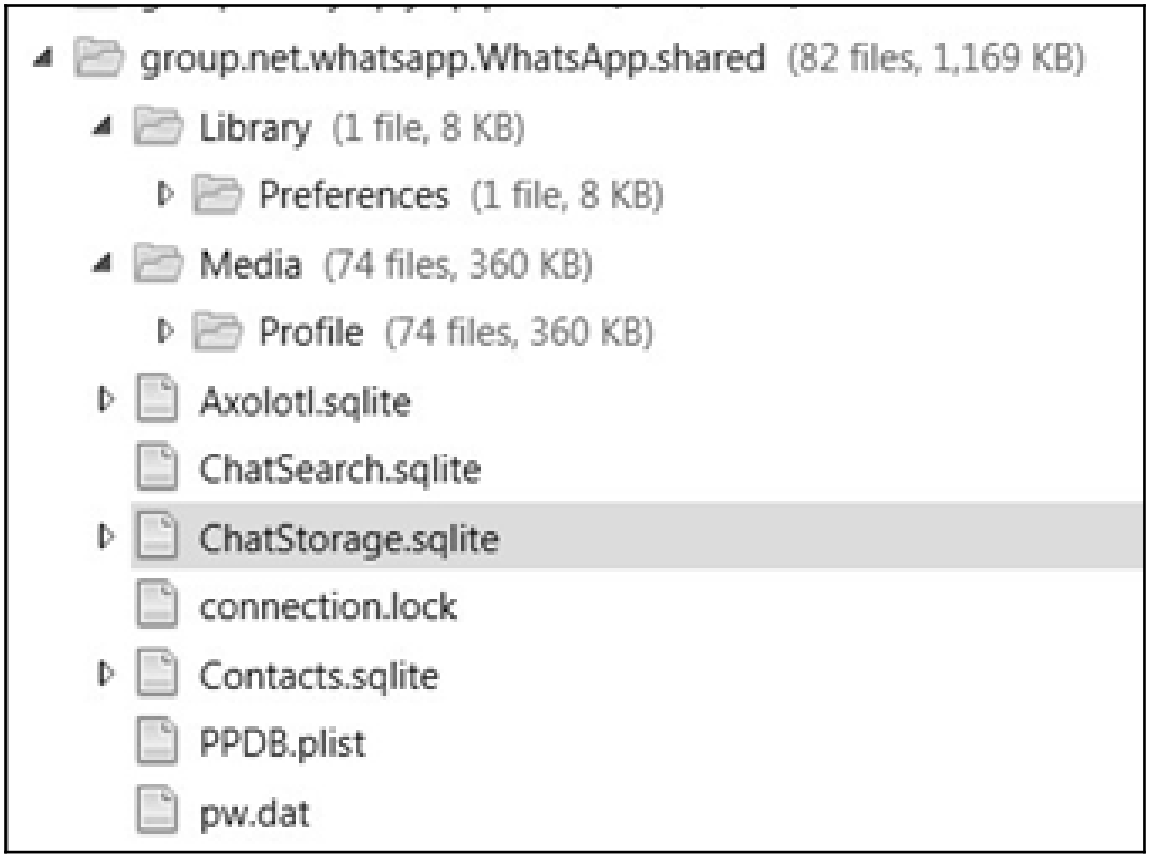
user_id	created	data
475222380	1404903823000	I–O?u? jcI wonder if the person that asked us for ...
29574511	1404905109000	I–Tl?` j~No, I'm with myself at E ly ca...
475222380	1404913177000	I–s3B jaWe need test data. Not really doing resea...
29574511	1404913470000	I–tQ??oDo you want just the chats? I can toss togeth...
475222380	1404916910000	I–□q? j?It's not even for me. A student asked me if I h...
29574511	1454683850000	I §W@??┼•jHShoot me your address and I'll try to get th...

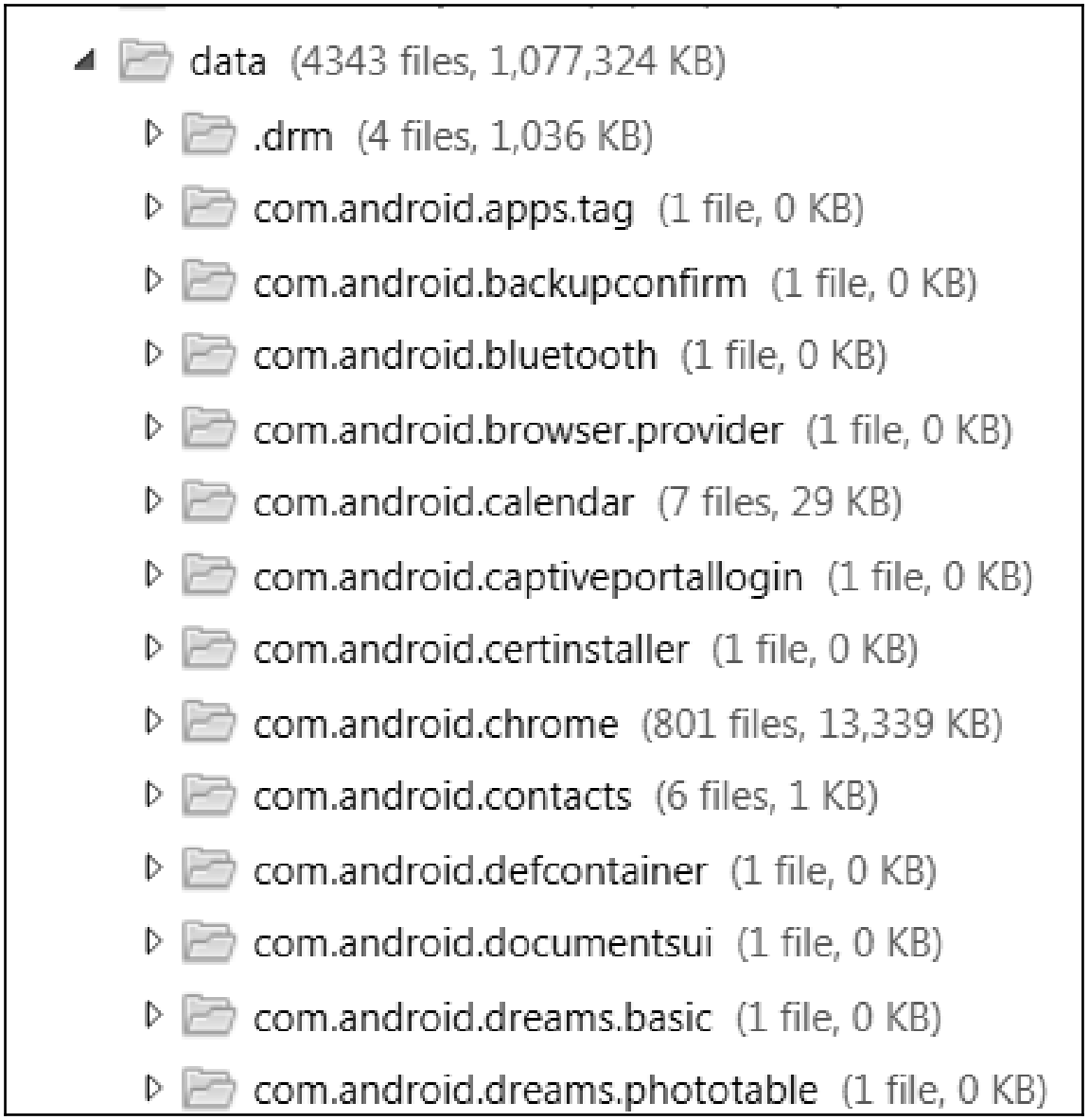

conversations (3)
games (0)
likes (1)
messages (21)
profiles (5)
receipts (1)
sms (0)
create_time
send_time
payload
1453739107566
1453739109747
EhZzdzlkWDlLS3Q5SkloT3hkMktrdjlRGAAiJUhlbGxvISBJIHdvdWxkI
1453739136466
1453739137674
EhZzdzlkWDlLS3Q5SkloT3hkMktrdjlRGAAiFkhleSB0aGVyZSAgaXRzI
1453739173098
1453739173555
EhZzdzlkWDlLS3Q5SkloT3hkMktrdjlRGAAiCkhpIEZlbGljaWGAAQCo
1453739046644
1453739053669
EhZzTWF3Wm9laDlYRzVTd0RQMjhPYkFRGAAiJUhlbGxvISBJIHdvdV

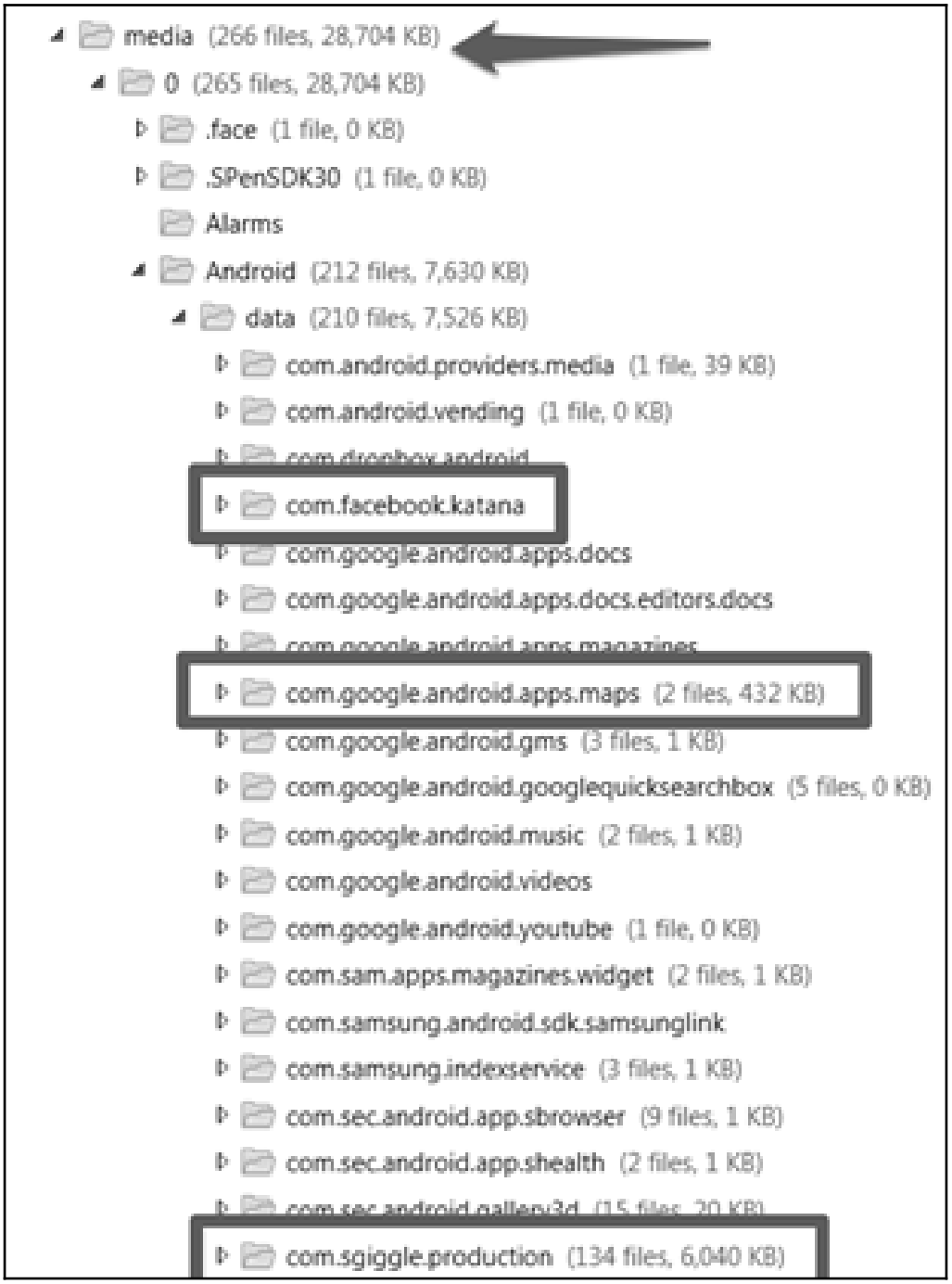

com.facebook.katana (189 files, 13,447 KB)
app_acra-reports (1 file, 1,030 KB)
app_call_stats
app_gatekeepers (6 files, 65 KB)
app_light_prefs (2 files, 1 KB)
app_logcat
app_logcat_flash_logs
app_minidumps
app_omnistore (3 files, 89 KB)
app_qe_sessioned
app_qe_sessionless (5 files, 1 KB)
app_sessionless_gatekeepers (6 files, 1 KB)
app_state_logs (54 files, 7 KB)
app_traces
cache (4 files, 1 KB)
databases (16 files, 465 KB)
dex (4 files, 1 KB)
files (5 files, 12 KB)
lib-assets (4 files, 1 KB)
lib-main (4 files, 1 KB)
lib-xzs (67 files, 11,773 KB)
shared_prefs (5 files, 1 KB)
crash_lock
crash_log
lib

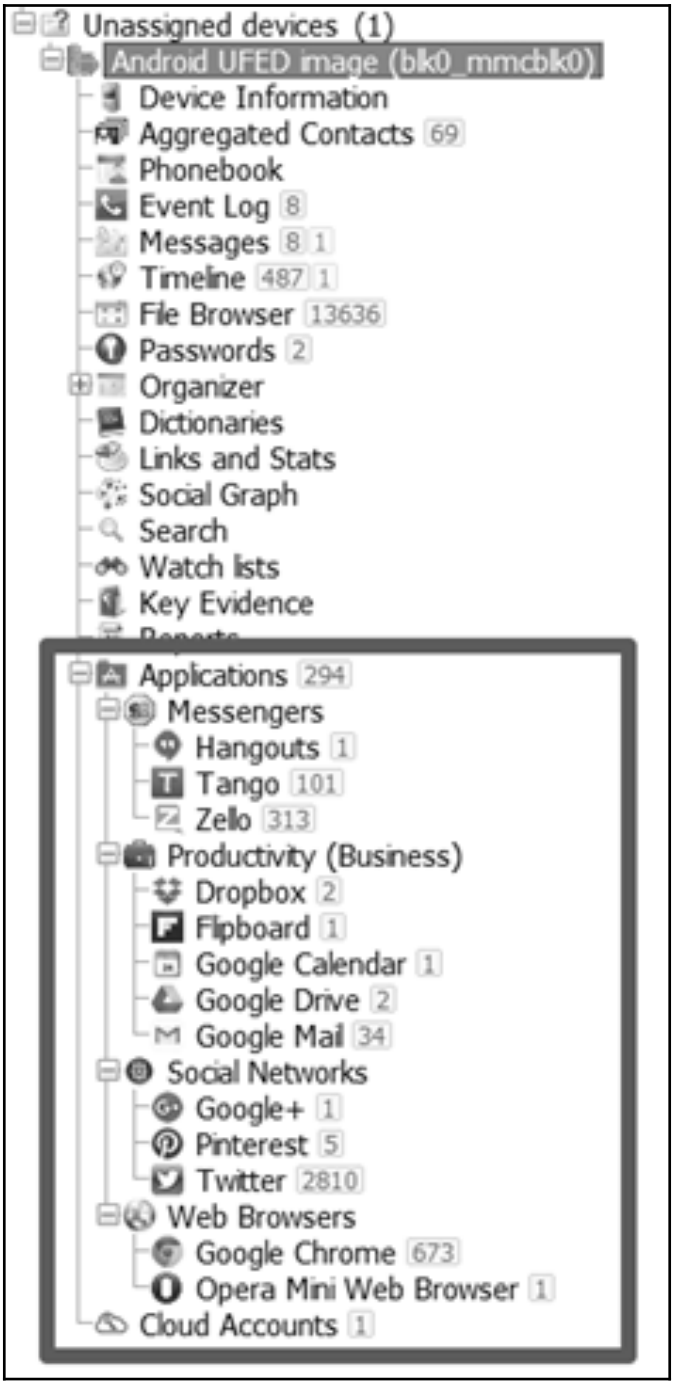

com.whatsapp (73 files, 2,640 KB)
app_webview (2 files, 46 KB)
cache (1 file, 47 KB)
databases (14 files, 1,193 KB)
_jobqueue-WhatsAppJobManager
_jobqueue-WhatsAppJobManager-journal
axolotl.db
axolotl.db-shm
axolotl.db-wal
chatsettings.db
chatsettings.db-shm
chatsettings.db-wal
msgstore.db
msgstore.db-shm
msgstore.db-wal
wa.db
wa.db-shm
wa.db-wal


Heather Mahalik's iPhone (5991 files, 2,536,307 KB)
Applications (1999 files, 116,475 KB)
243LU875E5.groups.com.apple.podcasts (17 files, 1,075
co.romesoft.toddlers.puzzle.shapes (3 files, 13 KB)
com.aa.AmericanAirlines (80 files, 105 KB)
com.airbnb.app (12 files, 666 KB)
com.alcre8or.VideoTrimAndCut (1 file, 1 KB)
com.allrecipes.dinnerspinner (1 file, 12 KB)
com.amazon.Amazon (6 files, 26 KB)
com.amazon.Amazon.watchkitextension (2 files, 2 KB)
com.amazon.CloudDrivePhotos (14 files, 224 KB)
com.amazon.Lassen (21 files, 763 KB)
com.amtrak.rider (8 files, 147 KB)

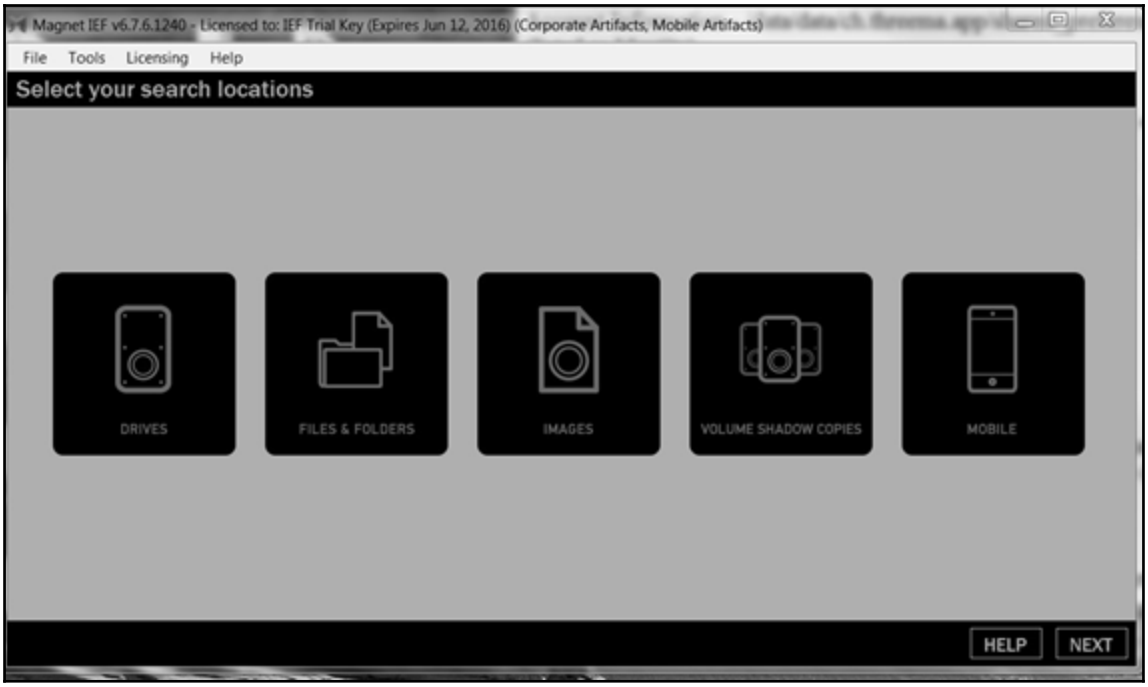

group.net.whatsapp.WhatsApp.shared (82 files, 1,169 KB)
Library (1 file, 8 KB)
Preferences (1 file, 8 KB)
Media (74 files, 360 KB)
Profile (74 files, 360 KB)
Axolotl.sqlite
ChatSearch.sqlite
ChatStorage.sqlite
connection.lock
Contacts.sqlite
PPDB.plist
pw.dat


data (4343 files, 1,077,324 KB)
.drm (4 files, 1,036 KB)
com.android.apps.tag (1 file, 0 KB)
com.android.backupconfirm (1 file, 0 KB)
com.android.bluetooth (1 file, 0 KB)
com.android.browser.provider (1 file, 0 KB)
com.android.calendar (7 files, 29 KB)
com.android.captiveportallogin (1 file, 0 KB)
com.android.certinstaller (1 file, 0 KB)
com.android.chrome (801 files, 13,339 KB)
com.android.contacts (6 files, 1 KB)
com.android.defcontainer (1 file, 0 KB)
com.android.documentsui (1 file, 0 KB)
com.android.dreams.basic (1 file, 0 KB)
com.android.dreams.phototable (1 file, 0 KB)

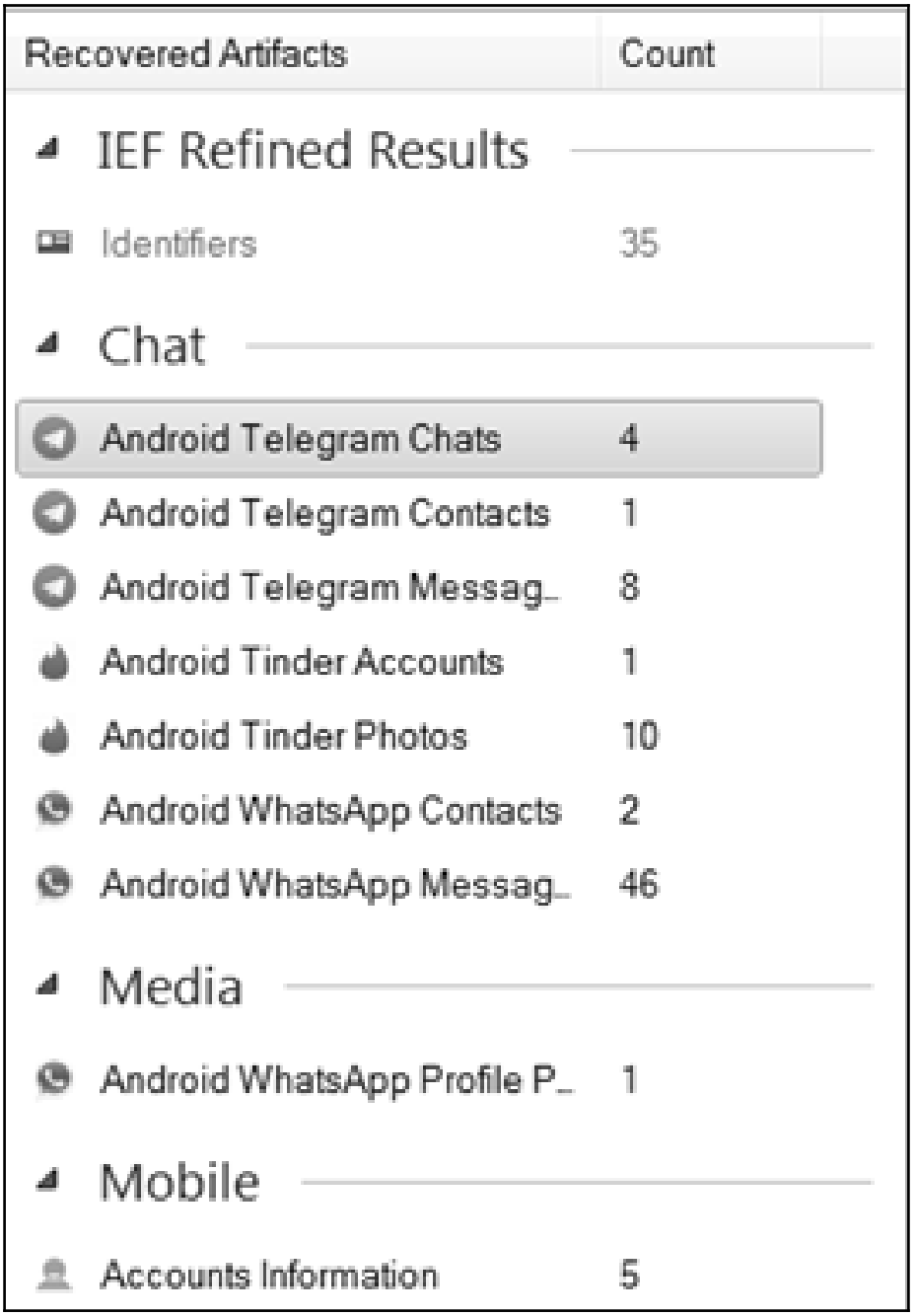

media (266 files, 28,704 KB)
0 (265 files, 28,704 KB)
.face (1 file, 0 KB)
.SPenSDK30 (1 file, 0 KB)
Alarms
Android (212 files, 7,630 KB)
data (210 files, 7,526 KB)
com.android.providers.media (1 file, 39 KB)
com.android.vending (1 file, 0 KB)
com.facebook.katana
com.google.android.apps.docs
com.google.android.apps.docs.editors.docs
com.google.android.apps.maps (2 files, 432 KB)
com.google.android.gms (3 files, 1 KB)
com.google.android.googlequicksearchbox (5 files, 0 KB)
com.google.android.music (2 files, 1 KB)
com.google.android.videos
com.google.android.youtube (1 file, 0 KB)
com.sam.apps.magazines.widget (2 files, 1 KB)
com.samsung.android.sdk.samsunglink
com.samsung.indexservice (3 files, 1 KB)
com.sec.android.app.sbrowser (9 files, 1 KB)
com.sec.android.app.shealth (2 files, 1 KB)
com.sgiggle.production (134 files, 6,040 KB)

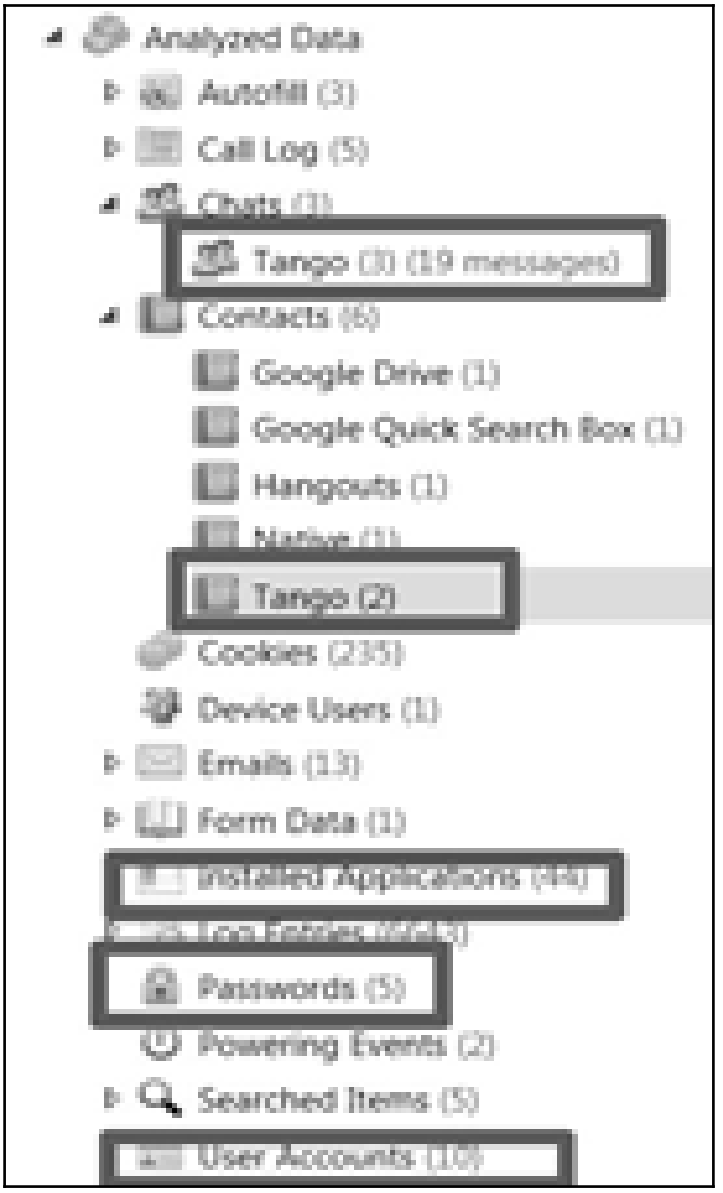

Unassigned devices (1)
Android UFED image (blk0_mmcblk0)
Device Information
Aggregated Contacts 69
Phonebook
Event Log 8
Messages 8 1
Timeline 487 1
File Browser 13636
Passwords 2
Organizer
Dictionaries
Links and Stats
Social Graph
Search
Watch lists
Key Evidence
Applications 294
Messengers
Hangouts 1
Tango 101
Zello 313
Productivity (Business)
Dropbox 2
Flipboard 1
Google Calendar 1
Google Drive 2
Google Mail 34
Social Networks
Google+ 1
Pinterest 5
Twitter 2810
Web Browsers
Google Chrome 673
Opera Mini Web Browser 1
Cloud Accounts 1

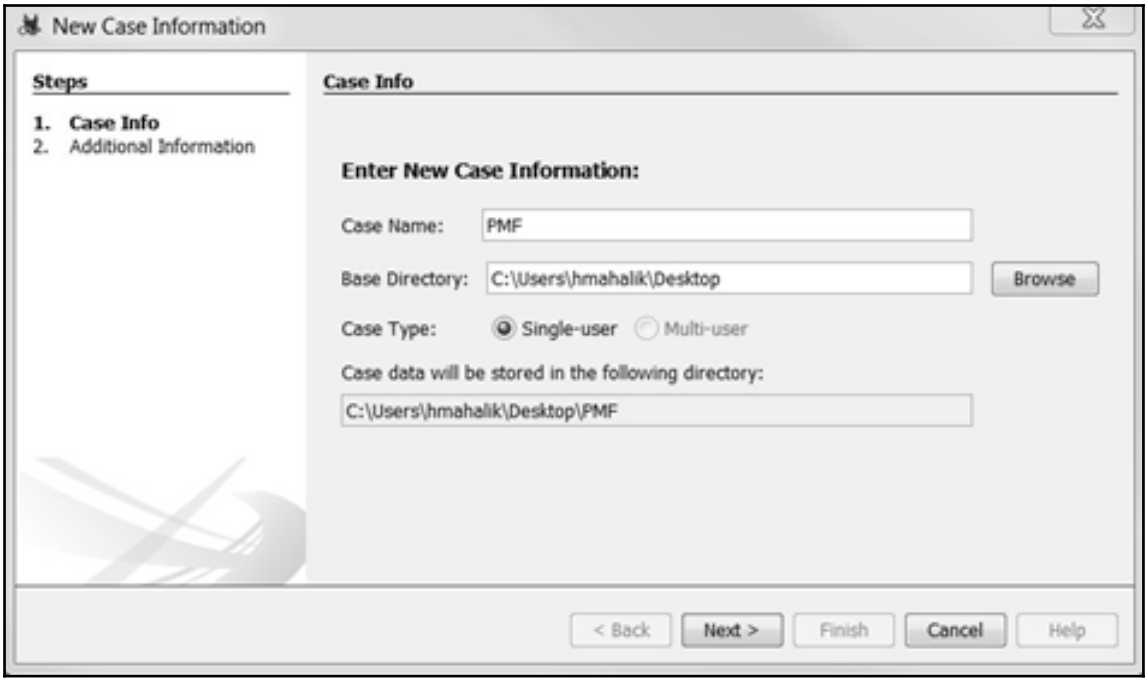

Application information
Pinterest
5 items
com.pinterest
Container: /data/data/com.pinterest
Details:
Source file: pinterest.xml
Last name: Jones
Full name: Felicia Jones
User name: goodb
Email: goodl @gmail.com
Gender: female
User picture URL:
http://passets-ak.pinterest.com/images/u...
Created (Device time): Sat, 06 Feb 2016 22:45:55 (+00:00 UTC)
UID: 403
Application information
Pinterest
5 items
com.pinterest
Container: /data/data/com.pinterest
Details:
Source table: BOARD
Source file: pinterest-db1454798754932
Name: beauty
Category: hair_beauty
Secret: No
Created (Device time): 2/6/2016 10:46:31 PM (+00:00 UTC)
URL:
http://www.pinterest.com/goodbyefelicia1...
Thumbnail URL:
http://media-cache-ec0.pinimg.com/90x9...
Cover URL:
https://s-media-cache-ak0.pinimg.com/20...
UID: 403

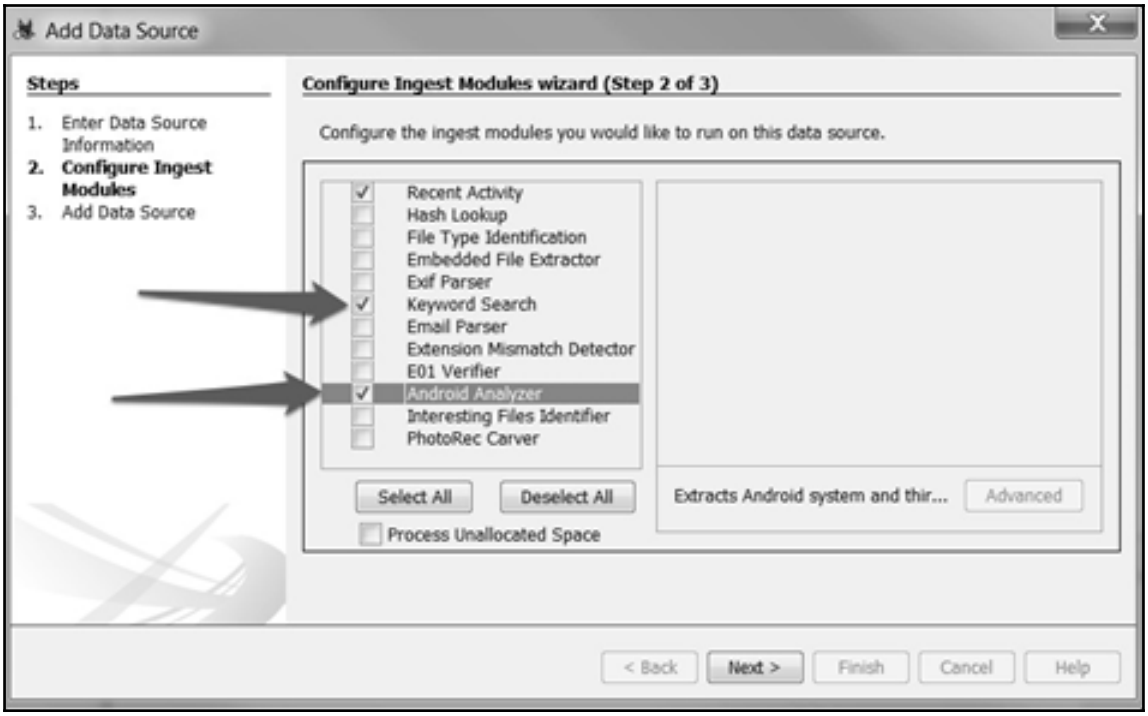

Magnet IEF v6.7.6.1240 - Licensed to: IEF Trial Key (Expires Jun 12, 2016) (Corporate Artifacts, Mobile Artifacts)
File
Tools
Licensing
Help
Select your search locations
DRIVES
FILES & FOLDERS
IMAGES
VOLUME SHADOW COPIES
MOBILE
HELP
NEXT


Magnet IEF v6.7.6.1240 - Licensed to: IEF Trial Key (Expires Jun 12, 2016) (Corporate Artifacts, Mobile Artifacts)
File Tools Licensing Help
PROFILE: All Artifacts (Default)
DELETE PROFILE
SET AS DEFAULT
FILE
SAVE PROFILE
SAVE PROFILE AS...
iOS Artifacts
Advanced Search Tools (1 of 1 items)
Dynamic App Finder
Chat (18 of 18 items)
AIM®
BlackBerry Messenger
Burner
Google Hangouts
Grindr
GROWLr
Kik Messenger
QQ®
Skype®
Telegram
Textfree
TextMe
TextPlus
TigerText
Tinder
Viber
WeChat
WhatsApp
Cloud (1 of 1 items)
Dropbox
Documents (6 of 6 items)
Excel
PDF
PowerPoint
RTF
Text
Word
CHECK ALL
UNCHECK ALL
ABOUT THE ARTIFACTS...
HELP
PREVIOUS
NEXT


Recovered Artifacts
Count
IEF Refined Results
Identifiers
35
Chat
Android Telegram Chats
4
Android Telegram Contacts
1
Android Telegram Messag_
8
Android Tinder Accounts
1
Android Tinder Photos
10
Android WhatsApp Contacts
2
Android WhatsApp Messag_
46
Media
Android WhatsApp Profile P_
1
Mobile
Accounts Information
5


Analyzed Data
Autofill (3)
Call Log (5)
Chats (1)
Tango (3) (19 messages)
Contacts (6)
Google Drive (1)
Google Quick Search Box (1)
Hangouts (1)
Tango (2)
Cookies (235)
Device Users (1)
Emails (13)
Form Data (1)
Passwords (5)
Powering Events (2)
Searched Items (5)
User Accounts (10)


New Case Information
Steps
1. Case Info
2. Additional Information
Case Info
Enter New Case Information:
Case Name:
PMF
Base Directory:
C:\Users\hmahalik\Desktop
Browse
Case Type:
Single-user
Multi-user
Case data will be stored in the following directory:
C:\Users\hmahalik\Desktop\PMF
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source
Configure Ingest Modules wizard (Step 2 of 3)
Configure the ingest modules you would like to run on this data source.
Recent Activity
Hash Lookup
File Type Identification
Embedded File Extractor
Exif Parser
Keyword Search
Email Parser
Extension Mismatch Detector
E01 Verifier
Android Analyzer
Interesting Files Identifier
PhotoRec Carver
Select All
Deselect All
Extracts Android system and thir...
Advanced
Process Unallocated Space
< Back
Next >
Finish
Cancel
Help

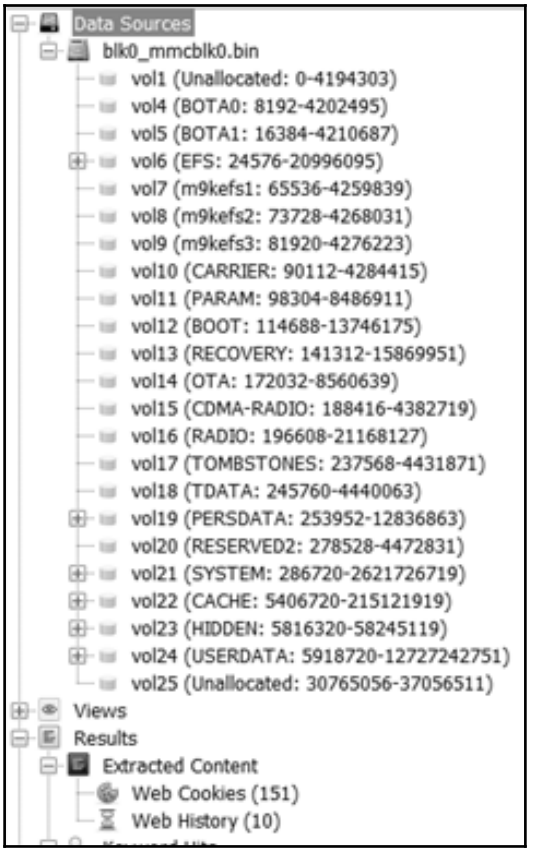


Table | Thumbnail

Source File	Date/Time	Direction	Text	Message Type
tc.db	2016-01-26 16:23:06 UTC	Outgoing	"◆ Welcome to Tango! Remember video calls, audio c...	Tango Message
tc.db	2016-01-25 16:27:52 UTC	Outgoing	" Sweet◆ ◆ 0 Hank Fresh	Tango Message
tc.db	2016-01-25 16:27:30 UTC	Incoming	*Khttp://cget.tango.me/contentserver/download/VqZM...	Tango Message
tc.db	2016-01-25 16:27:00 UTC	Incoming	*Khttp://cget.tango.me/contentserver/download/VqZM...	Tango Message
tc.db	2016-01-25 16:26:36 UTC	Outgoing	" New s4?◆ ◆ 0 Hank Fresh	Tango Message
tc.db	2016-01-25 16:26:24 UTC	Outgoing	C" ◆ C◆ 0 Hank Fresh	Tango Message
tc.db	2016-01-25 16:26:13 UTC	Outgoing	"Hi Felicia◆ ◆ 2 Tango Member	Tango Message
tc.db	2016-01-25 16:25:47 UTC	Incoming	" Hi its felicia◆ ◆ ◆◆◆,"◆ ◆◆◆\b◆ ◆ ◆ ◆	Tango Message