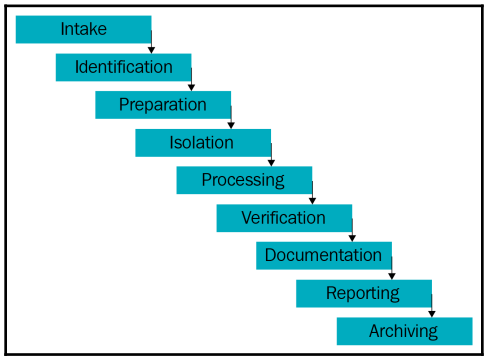
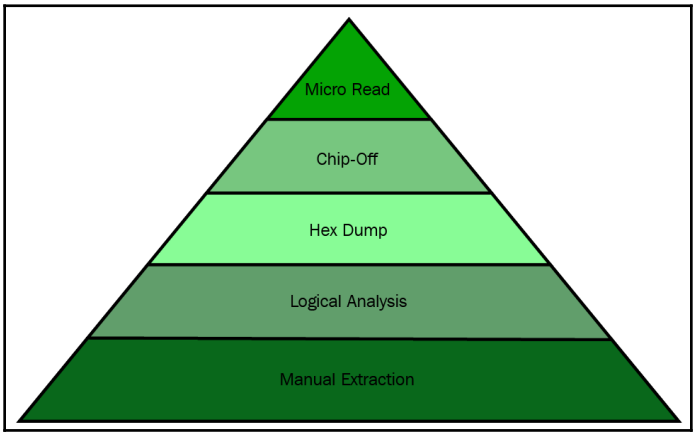
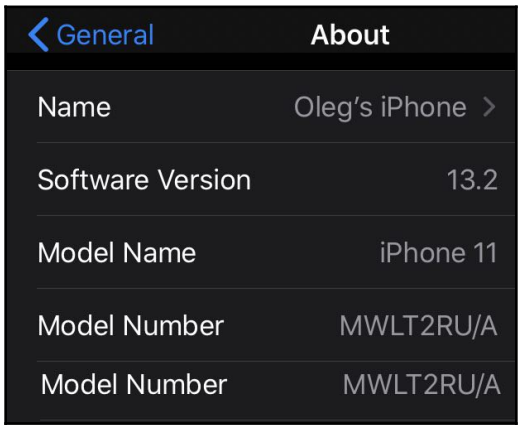
Chapter 1: Introduction to Mobile Forensics





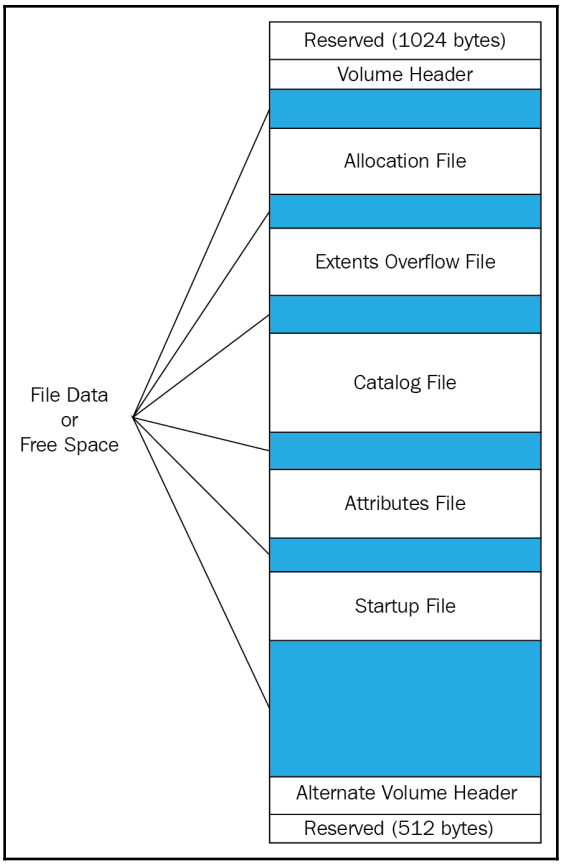
Chapter 2: Understanding the Internals of iOS Devices

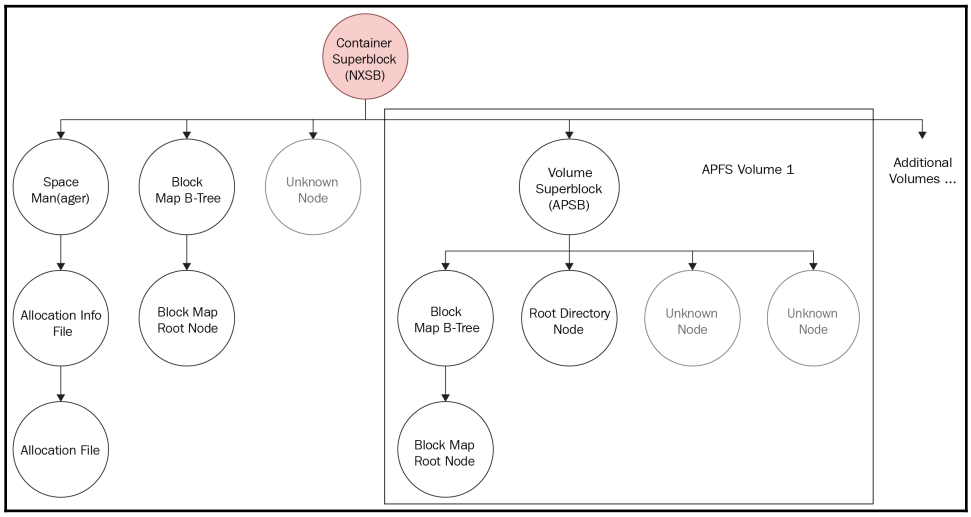


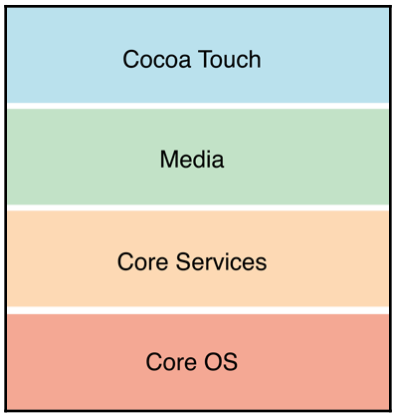

```
C:\Users\0136\Desktop\binaries\libimobiledevice.1.2.1-r419-win-x64>ideviceinfo.exe -s
BasebandCertId: 524245983
BasebandKeyHashInformation:
 AKeyStatus: 64
 SKeyStatus: 2
BasebandSerialNumber: sHODAZgntV0AAAAA
BasebandVersion: 1.02.14
BoardId: 4
BuildVersion: 17B84
CPUArchitecture: arm64e
ChipID: 32816
DeviceClass: iPhone
DeviceColor: 1
DeviceName: OlegтАЩs iPhone
DieID: 8563692629688366
HardwareModel: N104AP
HasSiDP: true
PartitionType: GUID_partition_scheme
ProductName: iPhone OS
ProductType: iPhone12,1
ProductVersion: 13.2
ProductionSOC: true
ProtocolVersion: 2
SupportedDeviceFamilies[1]:
 0: 1
TelephonyCapability: true
UniqueChipID: 8563692629688366
UniqueDeviceID: 00008030-001E6CA21128802E
WiFiAddress: f8:87:f1:f2:b0:78
```

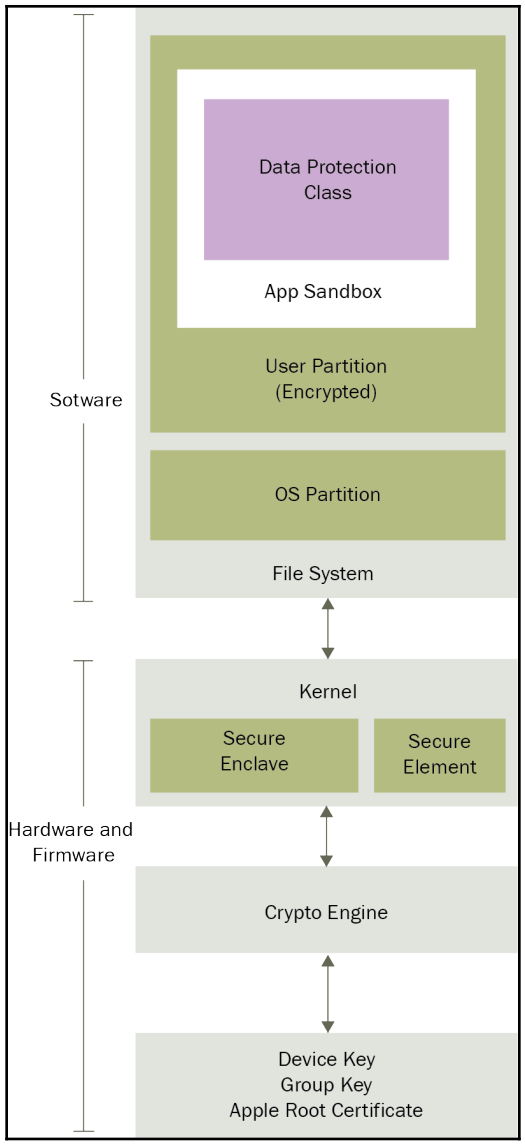
Device info

ActivationState - Activated
BasebandStatus - BBInfoAvailable
BasebandVersion - 1.02.14
BluetoothAddress - f8:87:f1:f2:21:45
BuildVersion - 17B84
CPUArchitecture - arm64e
DeviceClass - iPhone
DeviceColor - 1
DeviceName - Oleg's iPhone
FirmwareVersion - iBoot-5540.40.51
HardwareModel - N104AP
HardwarePlatform - t8030
IntegratedCircuitCardIdentity - 89701010063711442239
InternationalMobileEquipmentIdentity - 353989105391061
MLBSerialNumber - C7H94061QTDL73X67
MobileSubscriberCountryCode - 250
MobileSubscriberNetworkCode - 01
ModelNumber - MWLT2
PartitionType - GUID_partition_scheme
PhoneNumber -
ProductType - iPhone12,1
ProductVersion - 13.2
ProtocolVersion - 2
RegionInfo - RU/A
SerialNumber - C7CZJ36QN735
SIMStatus - kCTSIMSupportSIMStatusReady
TimeZone - Europe/Moscow
UniqueDeviceID - 00008030-001E6CA21128802E
WiFiAddress - f8:87:f1:f2:b0:78

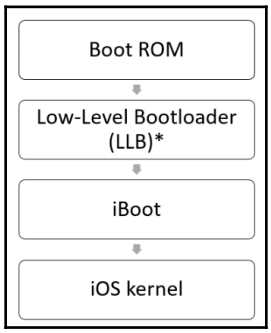

Reserved (1024 bytes)
Volume Header
Allocation File
Extents Overflow File
Catalog File
Attributes File
Startup File
Alternate Volume Header
Reserved (512 bytes)
File Data
or
Free Space

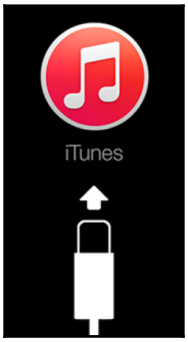

Container
Superblock
(NXSB)
Space
Man(ager)
Block
Map B-Tree
Unknown
Node
Allocation Info
File
Block Map
Root Node
Allocation File
Volume
Superblock
(APSB)
APFS Volume 1
Additional
Volumes ...
Block
Map B-Tree
Root Directory
Node
Unknown
Node
Unknown
Node
Block Map
Root Node

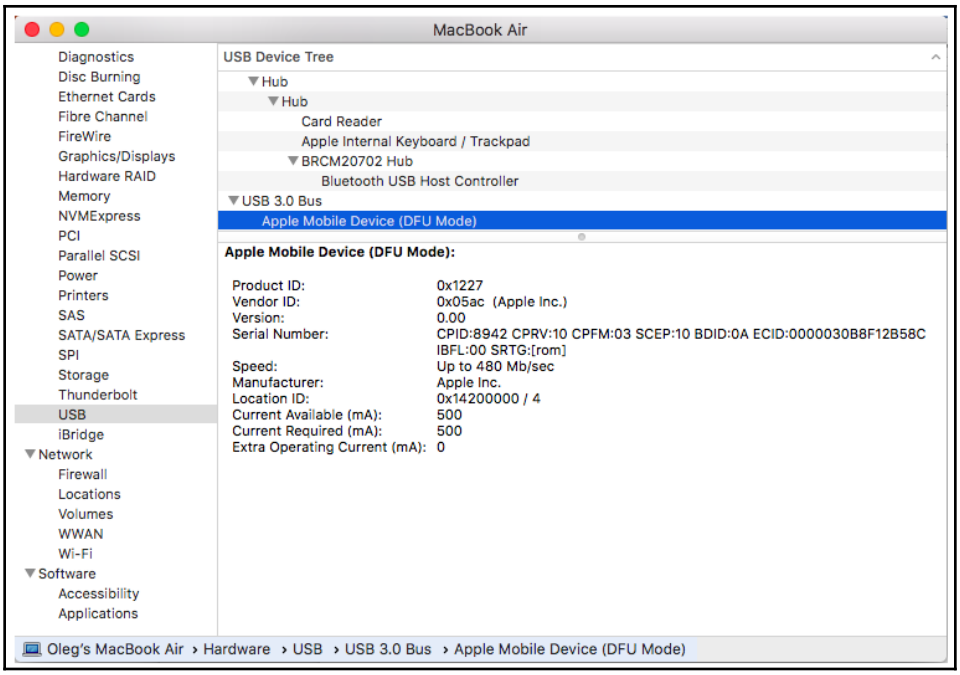

Cocoa Touch
Media
Core Services
Core OS


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

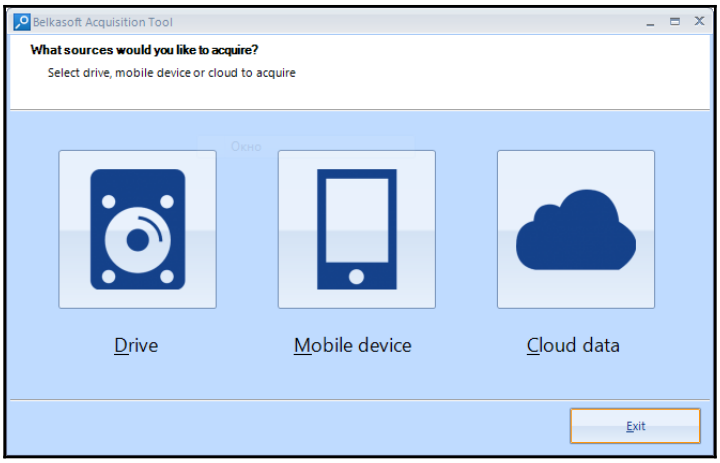
Chapter 3: Data Acquisition from iOS Devices

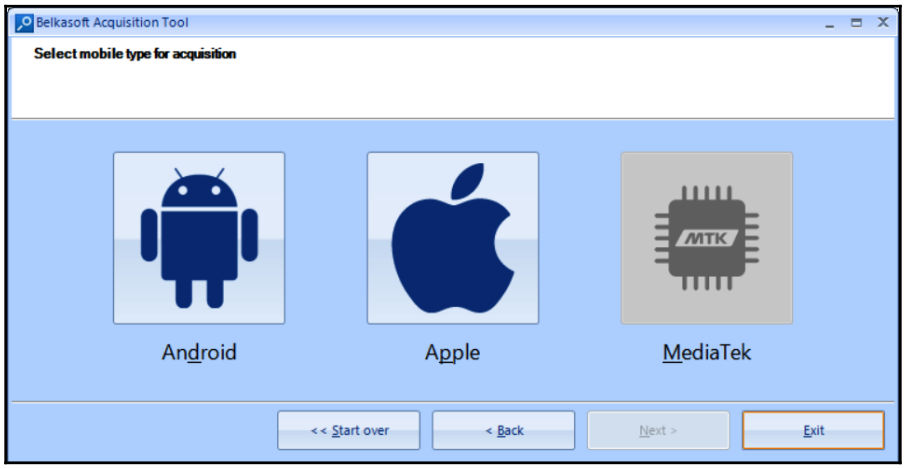


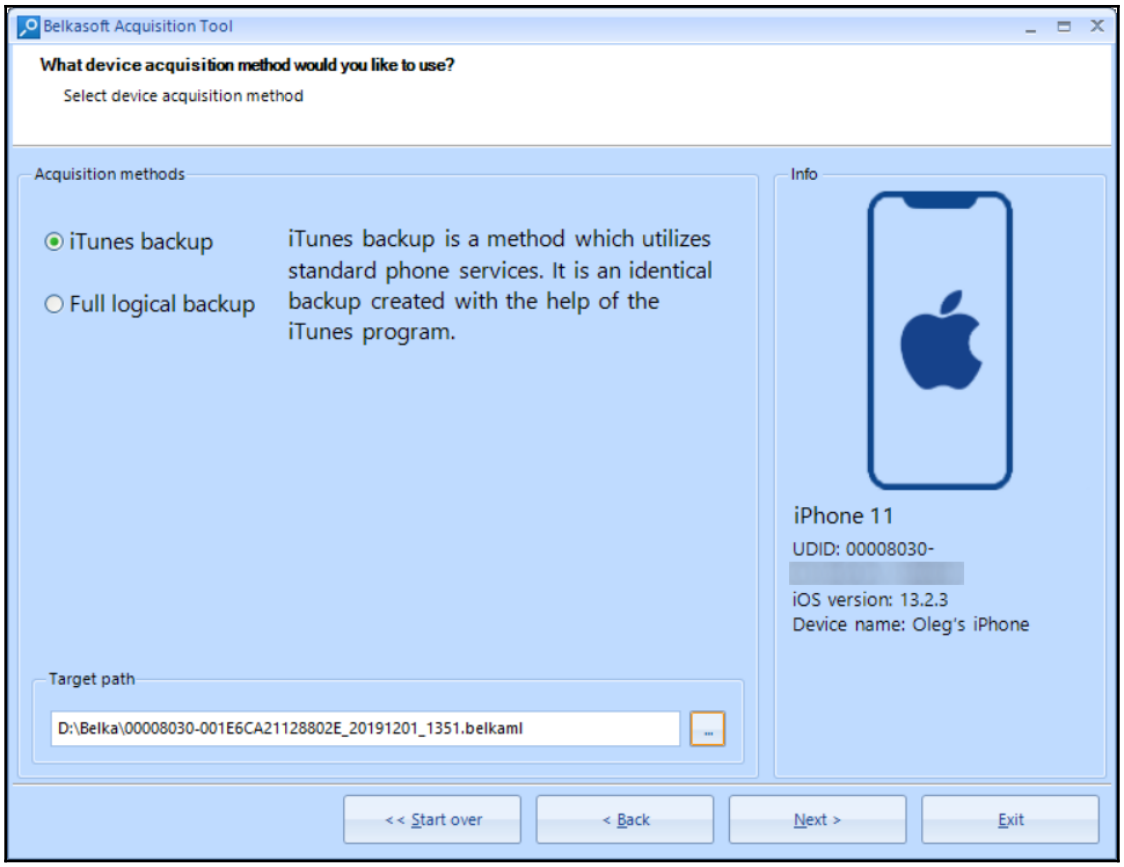


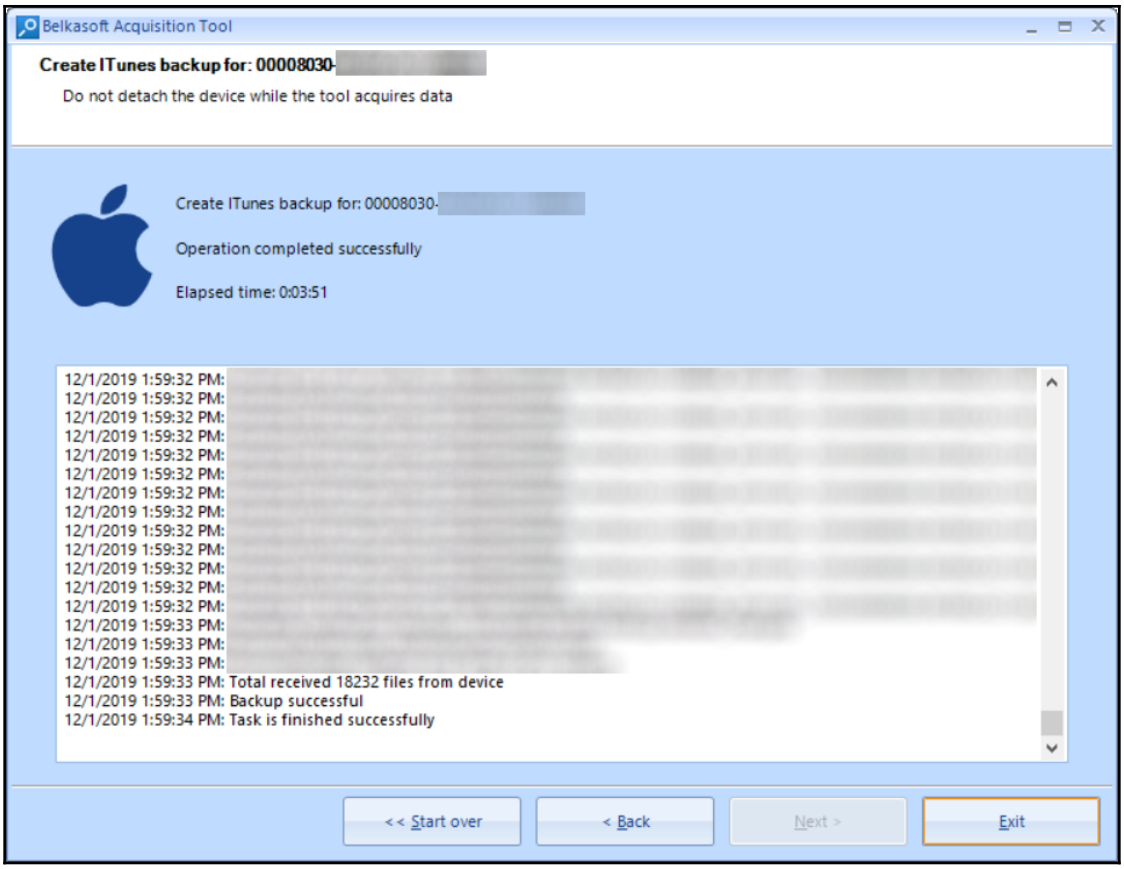


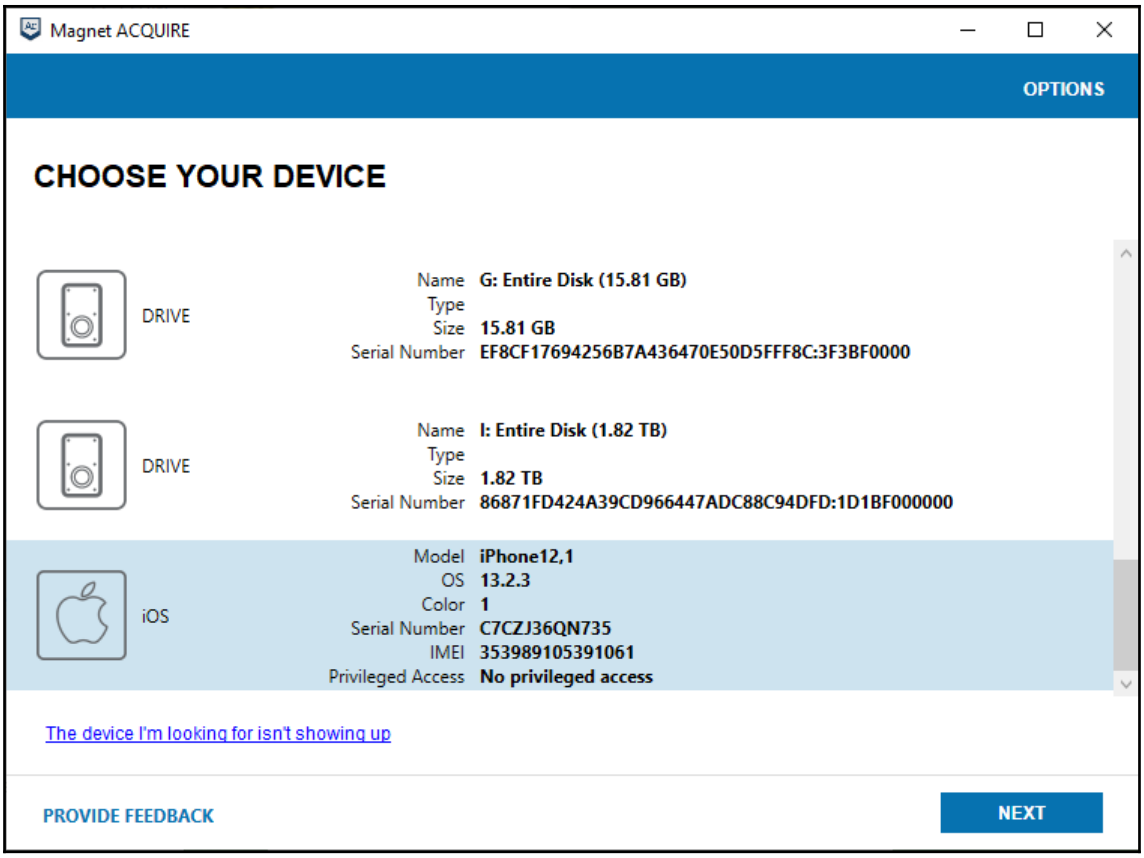

```
Backup directory is "D:\Backup"
Started "com.apple.mobilebackup2" service on port 49994.
Negotiated Protocol Version 2.1
Starting backup...
Enforcing full backup from device.
Backup will be encrypted.
Requesting backup from device...
Full backup mode.
[=                                                  ]   2% Finished
Receiving files
[==================================================] 100% (110.7 MB/110.7 MB)
[===                                                ]   5% Finished
Receiving files
[==================================================] 100% (131.1 MB/131.1 MB)
[==================================================] 100% (131.1 MB/131.1 MB)
[=====                                              ]  10% Finished
Receiving files
[==================================================] 100% (7.1 MB/7.1 MB)
[=====                                              ]  10% Finished
Receiving files
[==================================================] 100% (7.0 MB/7.0 MB)
[======                                             ]  10% Finished
Receiving files
[=========                                          ]  18% FinishedB/233.6 MB)
```

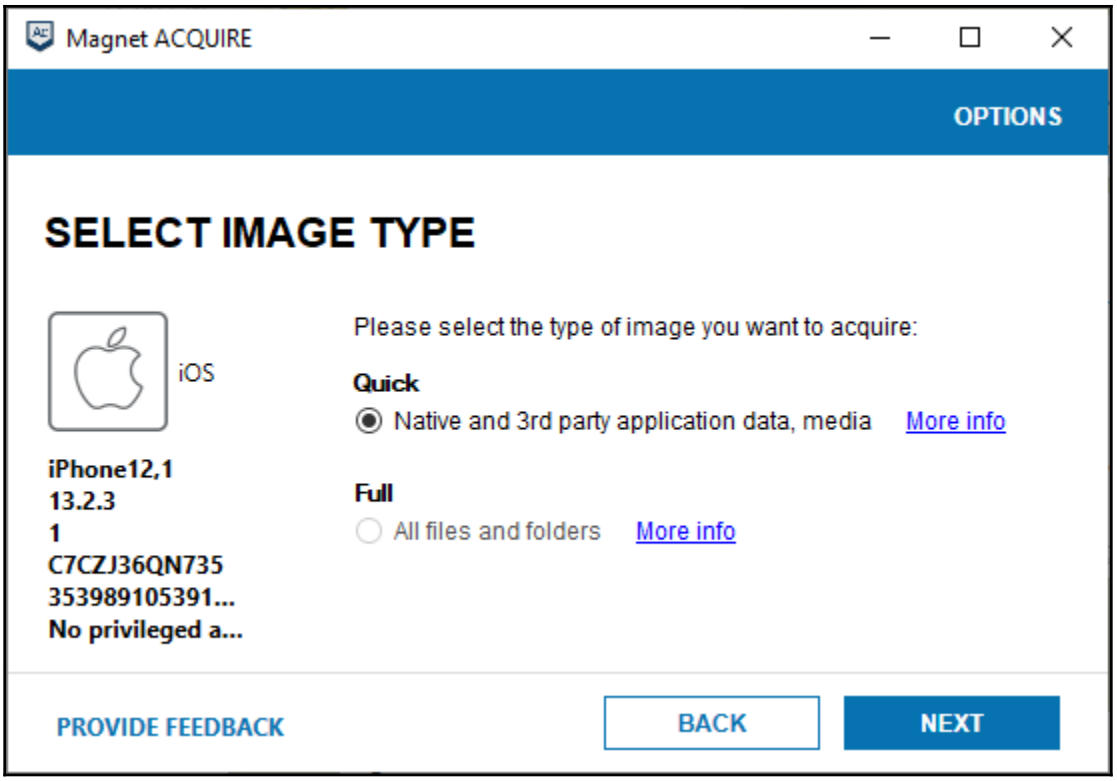

Belkasoft Acquisition Tool
What sources would you like to acquire?
Select drive, mobile device or cloud to acquire
Drive
Mobile device
Cloud data
Exit

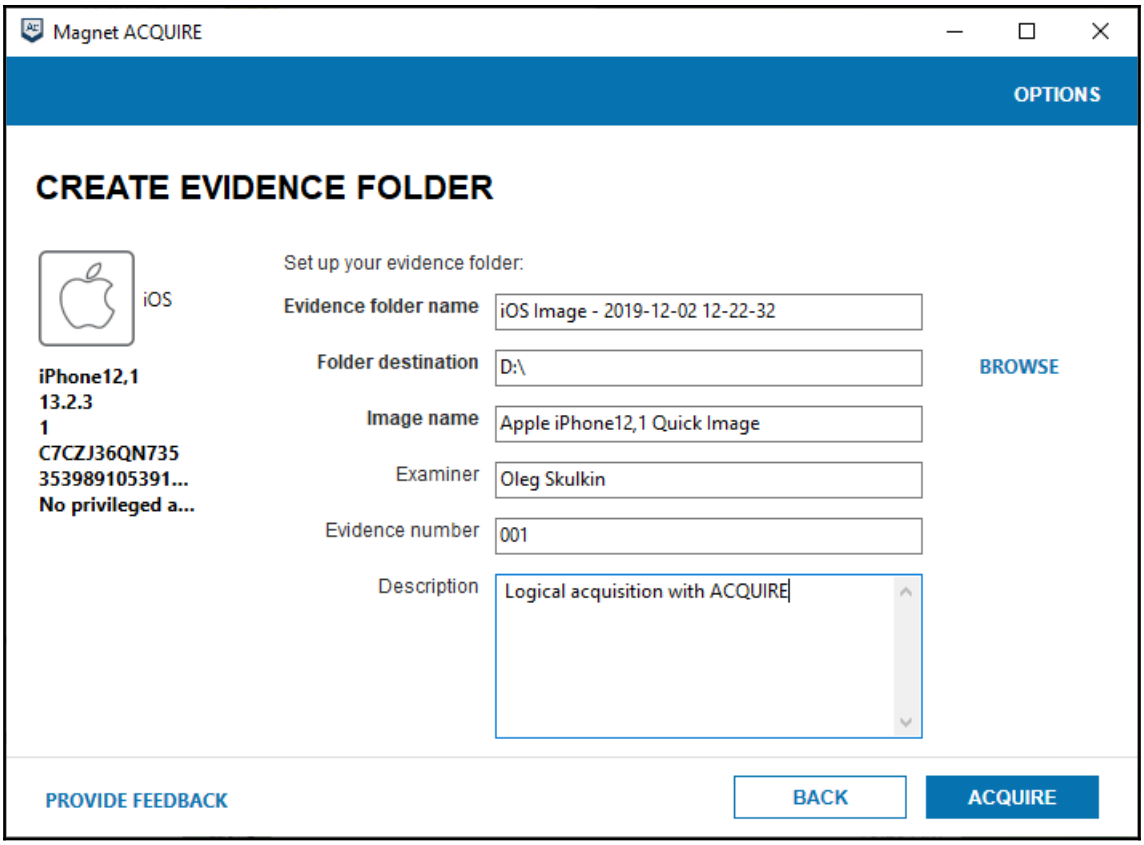

Belkasoft Acquisition Tool
Select mobile type for acquisition
Android
Apple
MediaTek
MTK
<< Start over
< Back
Next >
Exit

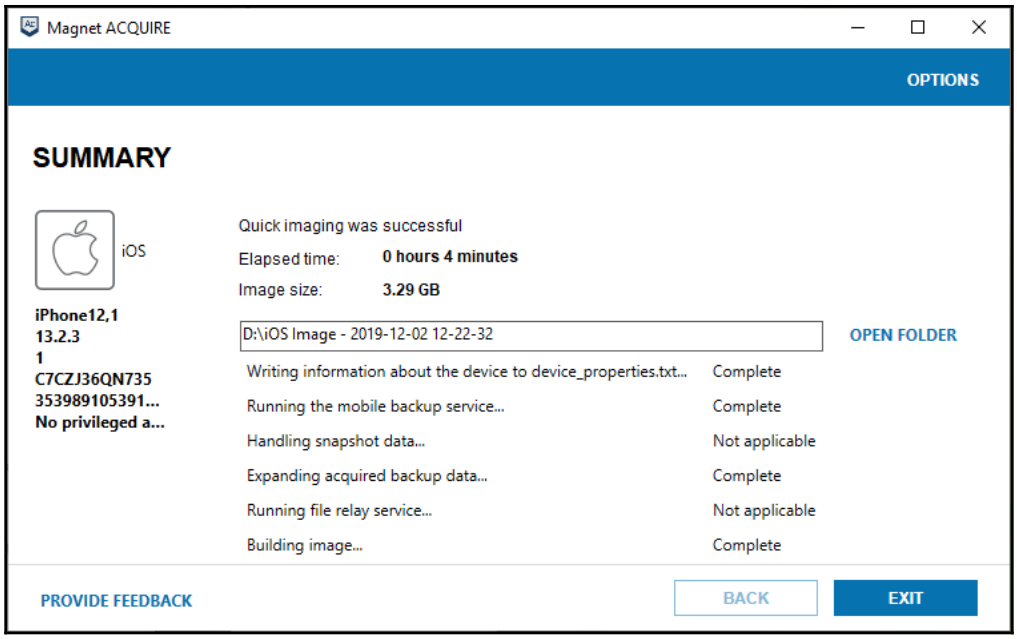

Belkasoft Acquisition Tool
What device acquisition method would you like to use?
Select device acquisition method
Acquisition methods
iTunes backup
Full logical backup
iTunes backup is a method which utilizes standard phone services. It is an identical backup created with the help of the iTunes program.
Info
iPhone 11
UDID: 00008030-
iOS version: 13.2.3
Device name: Oleg's iPhone
Target path
D:\Belka\00008030-001E6CA21128802E_20191201_1351.belkaml
...
<< Start over
< Back
Next >
Exit

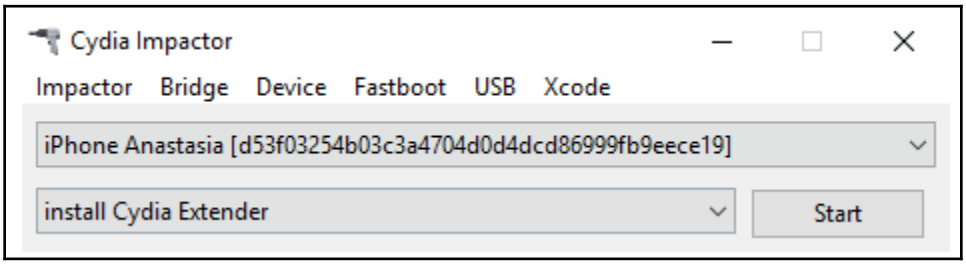

Belkasoft Acquisition Tool
Create ITunes backup for: 00008030-
Do not detach the device while the tool acquires data
Create ITunes backup for: 00008030-
Operation completed successfully
Elapsed time: 0:03:51
12/1/2019 1:59:32 PM:
12/1/2019 1:59:32 PM:
12/1/2019 1:59:32 PM:
12/1/2019 1:59:32 PM:
12/1/2019 1:59:32 PM:
12/1/2019 1:59:32 PM:
12/1/2019 1:59:32 PM:
12/1/2019 1:59:32 PM:
12/1/2019 1:59:32 PM:
12/1/2019 1:59:32 PM:
12/1/2019 1:59:32 PM:
12/1/2019 1:59:32 PM:
12/1/2019 1:59:32 PM:
12/1/2019 1:59:33 PM:
12/1/2019 1:59:33 PM:
12/1/2019 1:59:33 PM:
12/1/2019 1:59:33 PM: Total received 18232 files from device
12/1/2019 1:59:33 PM: Backup successful
12/1/2019 1:59:34 PM: Task is finished successfully
<< Start over
< Back
Next >
Exit

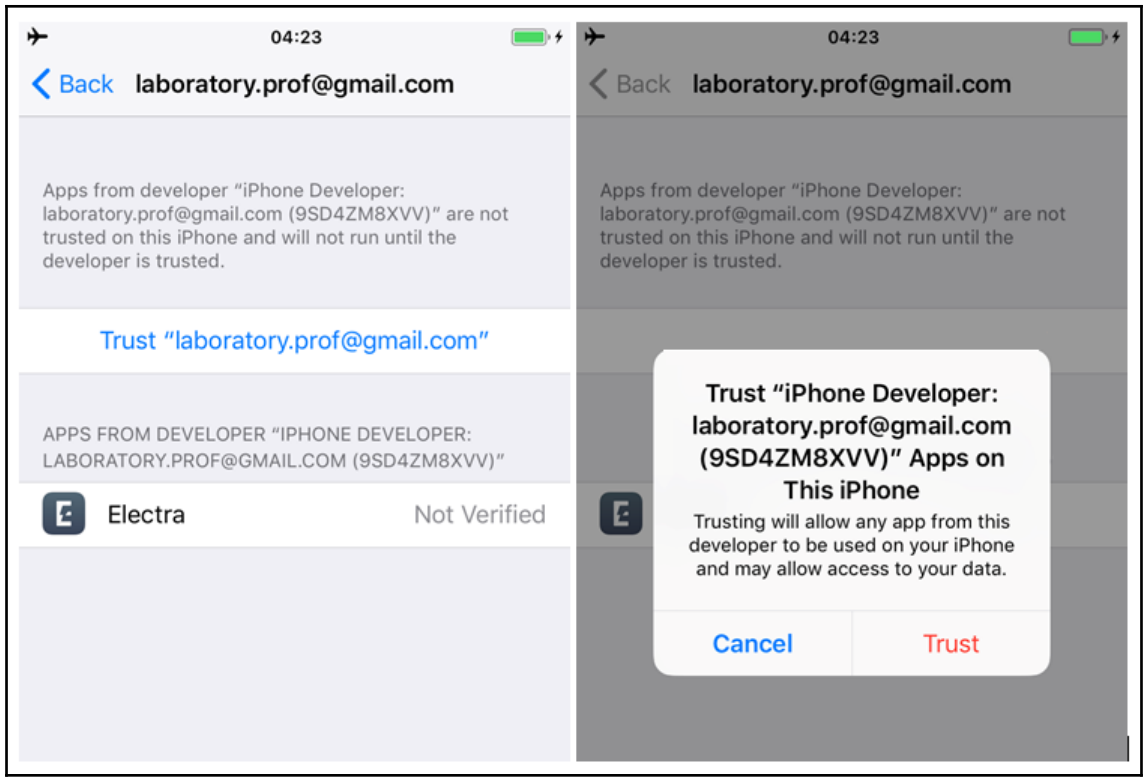

Magnet ACQUIRE
OPTIONS
CHOOSE YOUR DEVICE
DRIVE
Name G: Entire Disk (15.81 GB)
Type
Size 15.81 GB
Serial Number EF8CF17694256B7A436470E50D5FFF8C:3F3BF0000
DRIVE
Name I: Entire Disk (1.82 TB)
Type
Size 1.82 TB
Serial Number 86871FD424A39CD966447ADC88C94DFD:1D1BF000000
iOS
Model iPhone12,1
OS 13.2.3
Color 1
Serial Number C7CZJ36QN735
IMEI 353989105391061
Privileged Access No privileged access
The device I'm looking for isn't showing up
PROVIDE FEEDBACK
NEXT


Magnet ACQUIRE
OPTIONS
SELECT IMAGE TYPE
iOS
iPhone12,1
13.2.3
1
C7CZJ36QN735
353989105391...
No privileged a...
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

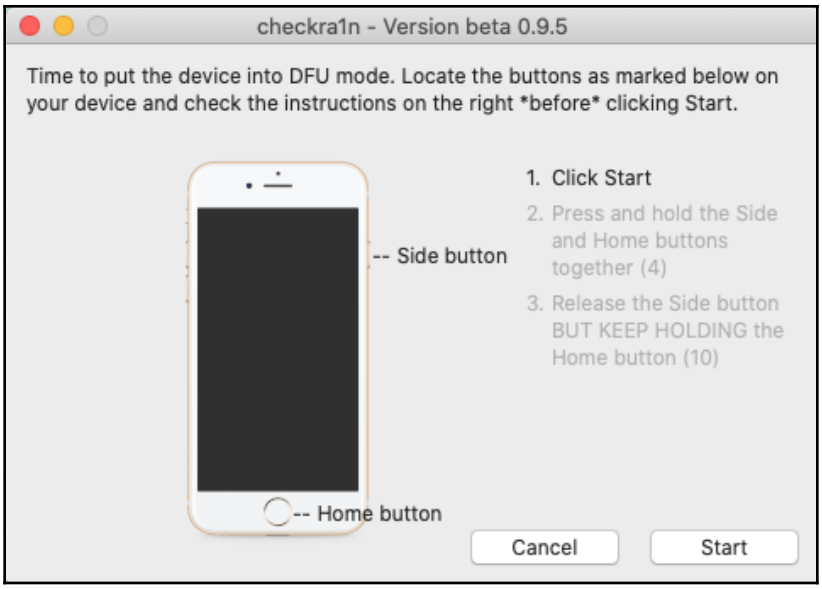

Magnet ACQUIRE
OPTIONS
CREATE EVIDENCE FOLDER
iOS
iPhone12,1
13.2.3
1
C7CZJ36QN735
353989105391...
No privileged a...
Set up your evidence folder:
Evidence folder name
iOS Image - 2019-12-02 12-22-32
Folder destination
D:\
BROWSE
Image name
Apple iPhone12,1 Quick Image
Examiner
Oleg Skulkin
Evidence number
001
Description
Logical acquisition with ACQUIRE
PROVIDE FEEDBACK
BACK
ACQUIRE

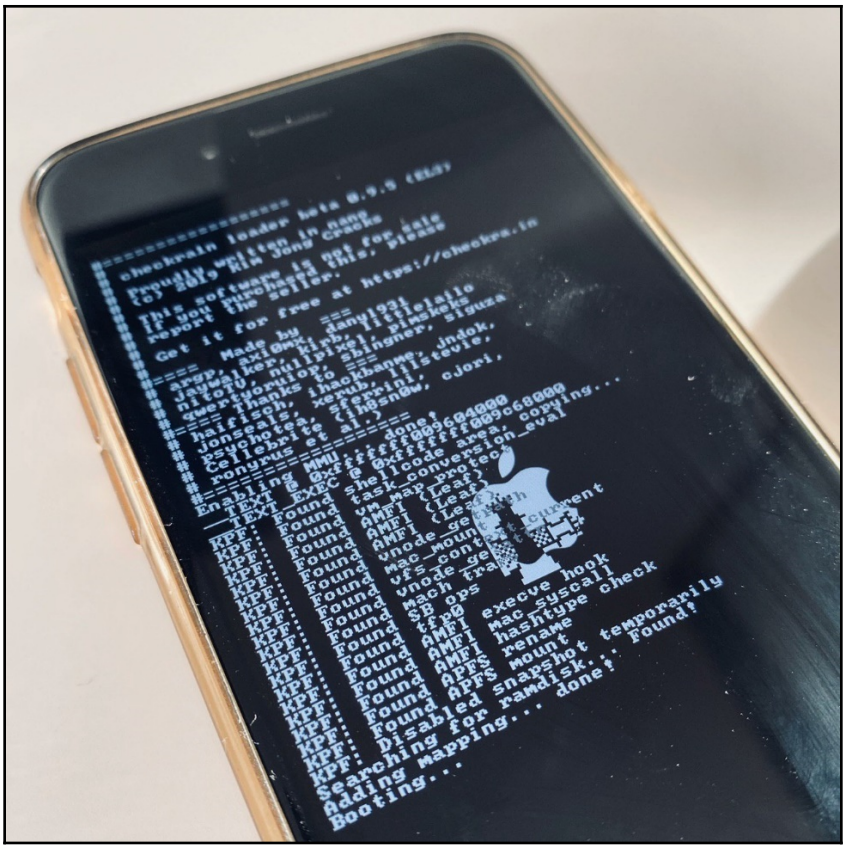

Magnet ACQUIRE
OPTIONS
SUMMARY
iOS
iPhone12,1
13.2.3
1
C7CZJ36QN735
353989105391...
No privileged a...
Quick imaging was successful
Elapsed time: 0 hours 4 minutes
Image size: 3.29 GB
D:\iOS Image - 2019-12-02 12-22-32
OPEN FOLDER
Writing information about the device to device_properties.txt... Complete
Running the mobile backup service... Complete
Handling snapshot data... Not applicable
Expanding acquired backup data... Complete
Running file relay service... Not applicable
Building image... Complete
PROVIDE FEEDBACK
BACK
EXIT


Cydia Impactor
Impactor Bridge Device Fastboot USB Xcode
iPhone Anastasia [d53f03254b03c3a4704d0d4dcd86999fb9eece19]
install Cydia Extender
Start

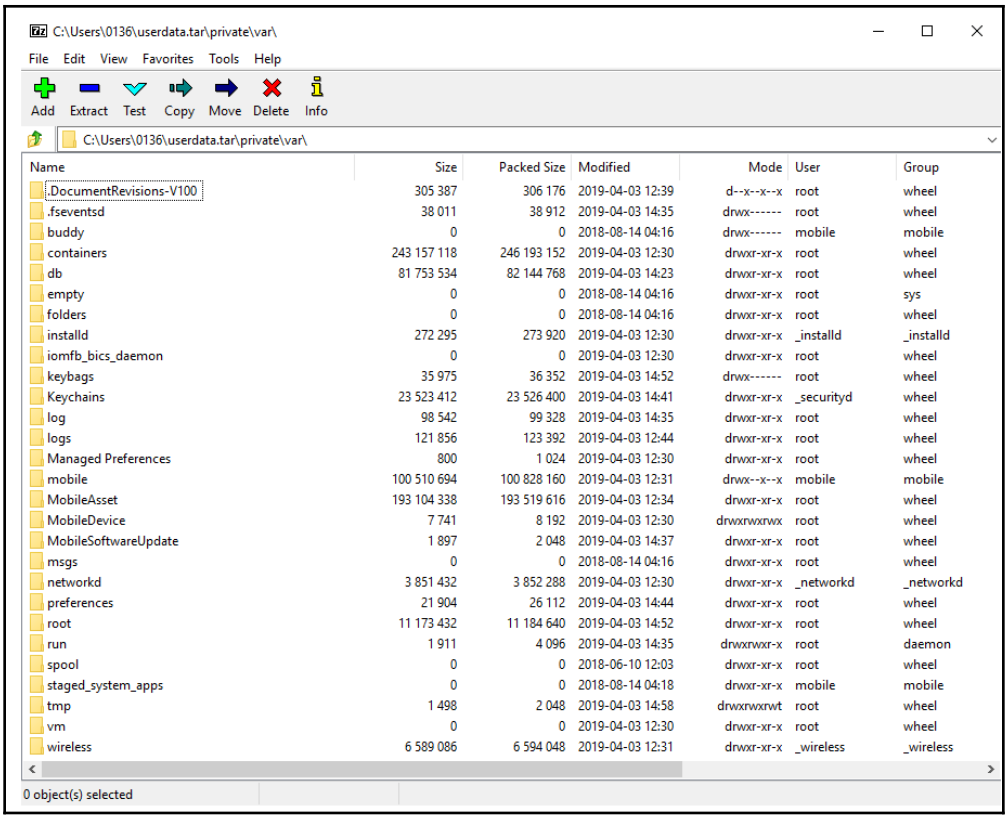

04:23
Back
laboratory.prof@gmail.com
Apps from developer "iPhone Developer: laboratory.prof@gmail.com (9SD4ZM8XVV)" are not trusted on this iPhone and will not run until the developer is trusted.
Trust "laboratory.prof@gmail.com"
APPS FROM DEVELOPER "IPHONE DEVELOPER: LABORATORY.PROF@GMAIL.COM (9SD4ZM8XVV)"
Electra
Not Verified
04:23
Back
laboratory.prof@gmail.com
Apps from developer "iPhone Developer: laboratory.prof@gmail.com (9SD4ZM8XVV)" are not trusted on this iPhone and will not run until the developer is trusted.
Trust "iPhone Developer: laboratory.prof@gmail.com (9SD4ZM8XVV)" Apps on This iPhone
Trusting will allow any app from this developer to be used on your iPhone and may allow access to your data.
Cancel
Trust

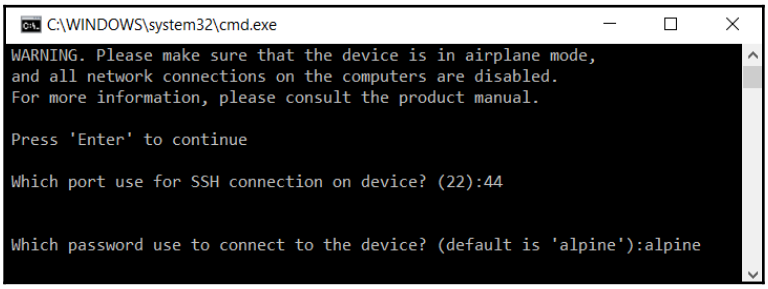

04:26
Electra
Jailbreak
Compatible with
iOS 11.0 — 11.4.1
Brought to you by the @Electra_Team
Tweaks
Credits
Set Nonce
Билайн LTE
04:40
FaceTime
Podcasts
Calculator
Watch
Files
Extras
Cydia
Electra

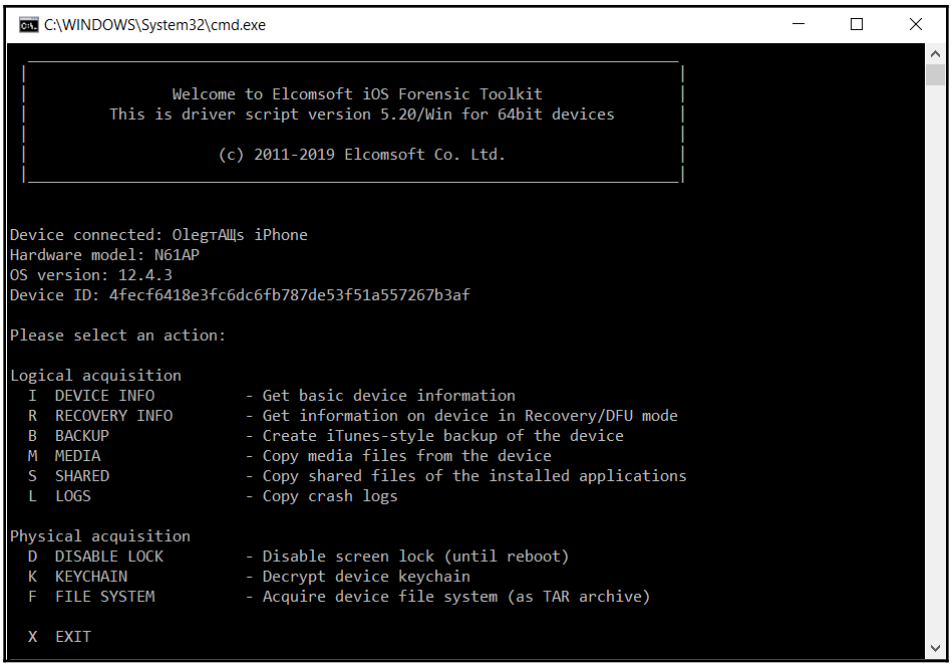

checkra1n - Version beta 0.9.5
Time to put the device into DFU mode. Locate the buttons as marked below on your device and check the instructions on the right *before* clicking Start.
-- Side button
-- Home button
1. Click Start
2. Press and hold the Side and Home buttons together (4)
3. Release the Side button BUT KEEP HOLDING the Home button (10)
Cancel
Start



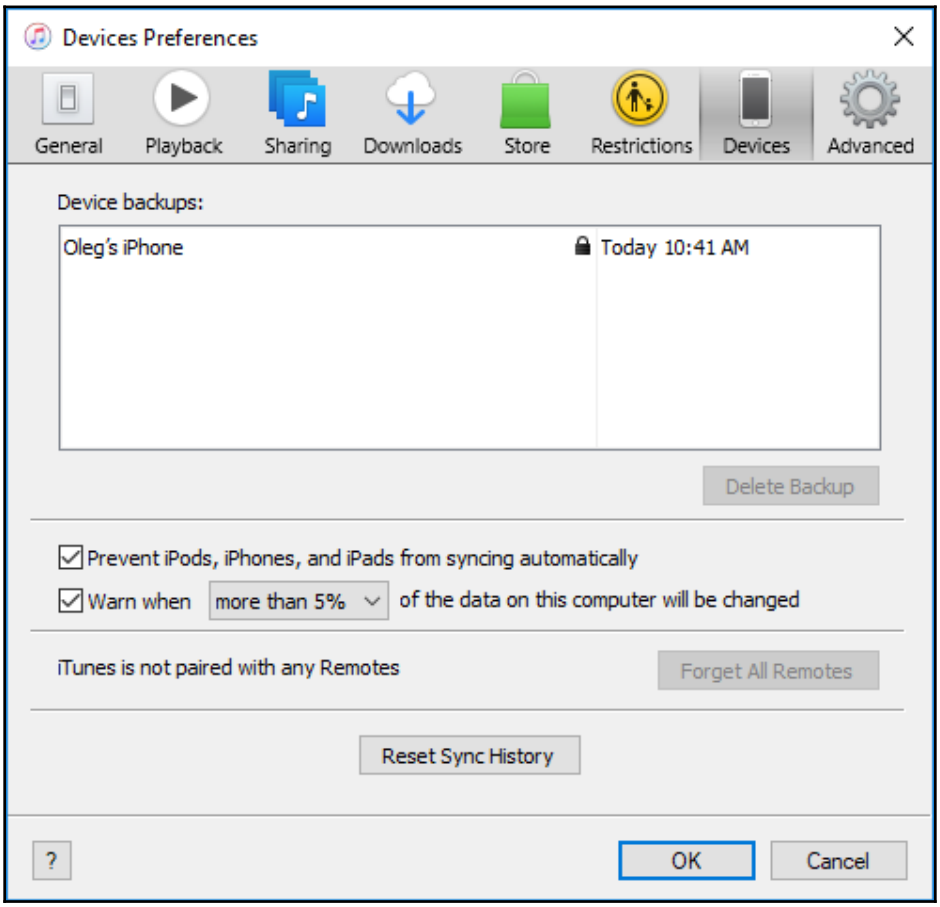
```
D:\libimobiledevice-Compiled-Windows-ios11>iproxy.exe 4444 22
waiting for connection
accepted connection, fd = 4
waiting for connection
Number of available devices == 1
Requesting connecion to device handle == 18 (serial: d53f03254b03c3a4704d0d4dcd86999fb9eece19), port 22
```

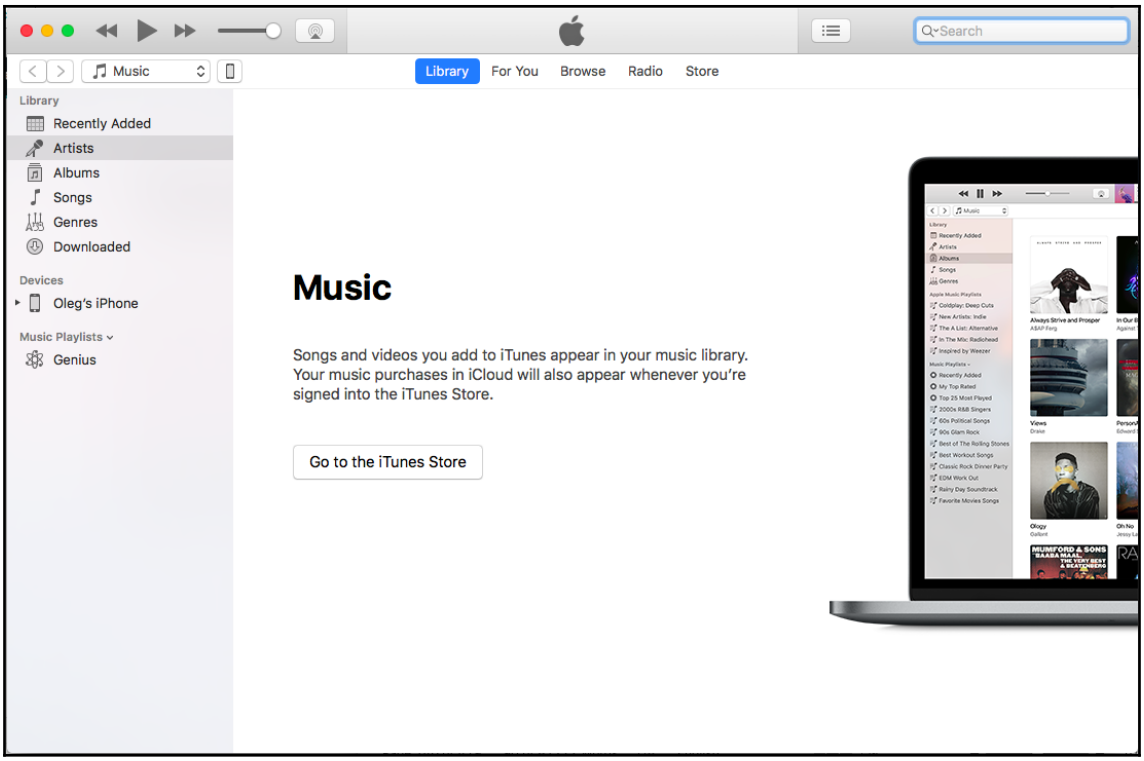

C:\Users\0136\userdata.tar\private\var\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
C:\Users\0136\userdata.tar\private\var\
Name Size Packed Size Modified Mode User Group
.DocumentRevisions-V100 305 387 306 176 2019-04-03 12:39 d--x--x--x root wheel
.fseventsd 38 011 38 912 2019-04-03 14:35 drwx------ root wheel
buddy 0 0 2018-08-14 04:16 drwx------ mobile mobile
containers 243 157 118 246 193 152 2019-04-03 12:30 drwxr-xr-x root wheel
db 81 753 534 82 144 768 2019-04-03 14:23 drwxr-xr-x root wheel
empty 0 0 2018-08-14 04:16 drwxr-xr-x root sys
folders 0 0 2018-08-14 04:16 drwxr-xr-x root wheel
installd 272 295 273 920 2019-04-03 12:30 drwxr-xr-x _installd _installd
iomfb_bics_daemon 0 0 2019-04-03 12:30 drwxr-xr-x root wheel
keybags 35 975 36 352 2019-04-03 14:52 drwx------ root wheel
Keychains 23 523 412 23 526 400 2019-04-03 14:41 drwxr-xr-x _securityd wheel
log 98 542 99 328 2019-04-03 14:35 drwxr-xr-x root wheel
logs 121 856 123 392 2019-04-03 12:44 drwxr-xr-x root wheel
Managed Preferences 800 1 024 2019-04-03 12:30 drwxr-xr-x root wheel
mobile 100 510 694 100 828 160 2019-04-03 12:31 drwx--x--x mobile mobile
MobileAsset 193 104 338 193 519 616 2019-04-03 12:34 drwxr-xr-x root wheel
MobileDevice 7 741 8 192 2019-04-03 12:30 drwxrwxrwx root wheel
MobileSoftwareUpdate 1 897 2 048 2019-04-03 14:37 drwxr-xr-x root wheel
msgs 0 0 2018-08-14 04:16 drwxr-xr-x root wheel
networkd 3 851 432 3 852 288 2019-04-03 12:30 drwxr-xr-x _networkd _networkd
preferences 21 904 26 112 2019-04-03 14:44 drwxr-xr-x root wheel
root 11 173 432 11 184 640 2019-04-03 14:52 drwxr-xr-x root wheel
run 1 911 4 096 2019-04-03 14:35 drwxrwxr-x root daemon
spool 0 0 2018-06-10 12:03 drwxr-xr-x root wheel
staged_system_apps 0 0 2018-08-14 04:18 drwxr-xr-x mobile mobile
tmp 1 498 2 048 2019-04-03 14:58 drwxrwxrwt root wheel
vm 0 0 2019-04-03 12:30 drwxr-xr-x root wheel
wireless 6 589 086 6 594 048 2019-04-03 12:31 drwxr-xr-x _wireless _wireless
0 object(s) selected


C:\WINDOWS\system32\cmd.exe
WARNING. Please make sure that the device is in airplane mode,
and all network connections on the computers are disabled.
For more information, please consult the product manual.
Press 'Enter' to continue
Which port use for SSH connection on device? (22):44
Which password use to connect to the device? (default is 'alpine'):alpine


C:\WINDOWS\System32\cmd.exe
Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 5.20/Win for 64bit devices
(c) 2011-2019 Elcomsoft Co. Ltd.
Device connected: OlegтАЩs iPhone
Hardware model: N61AP
OS version: 12.4.3
Device ID: 4fecf6418e3fc6dc6fb787de53f51a557267b3af
Please select an action:
Logical acquisition
I DEVICE INFO - Get basic device information
R RECOVERY INFO - Get information on device in Recovery/DFU mode
B BACKUP - Create iTunes-style backup of the device
M MEDIA - Copy media files from the device
S SHARED - Copy shared files of the installed applications
L LOGS - Copy crash logs
Physical acquisition
D DISABLE LOCK - Disable screen lock (until reboot)
K KEYCHAIN - Decrypt device keychain
F FILE SYSTEM - Acquire device file system (as TAR archive)
X EXIT

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

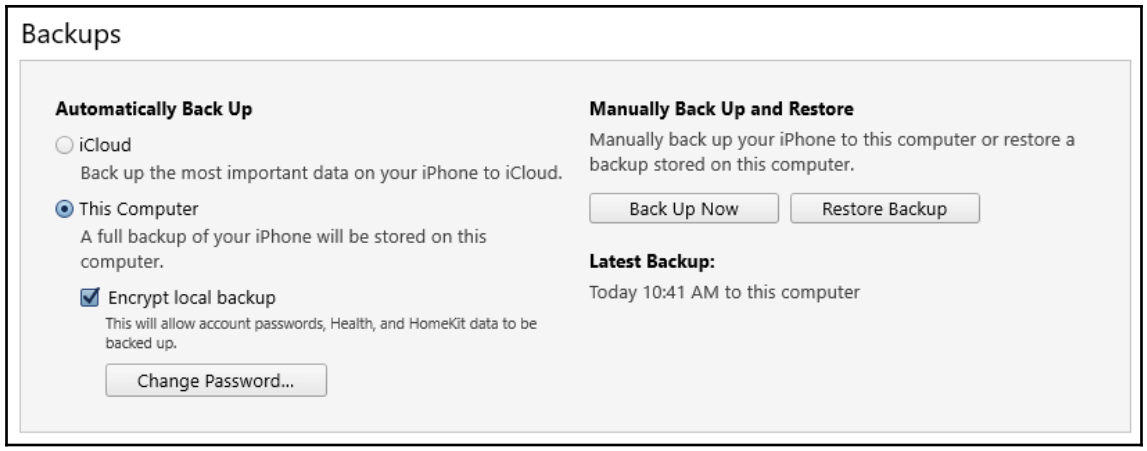
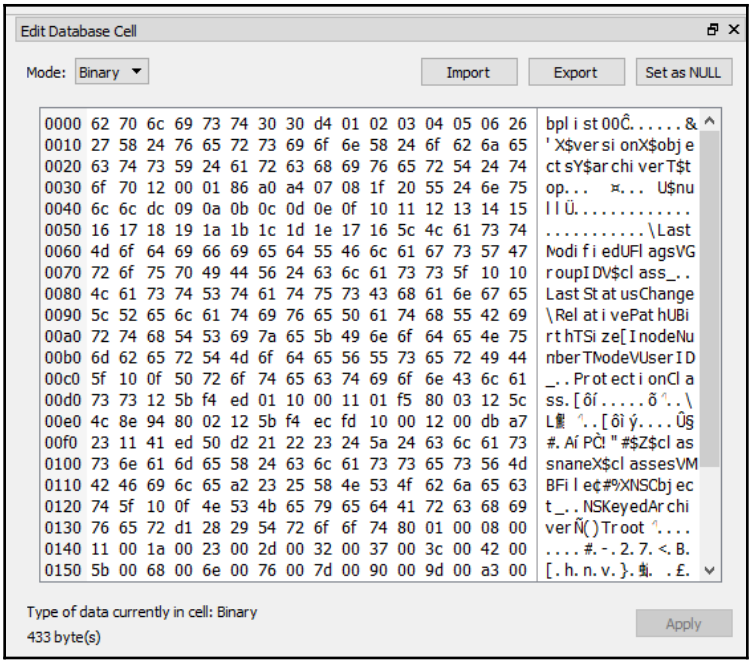
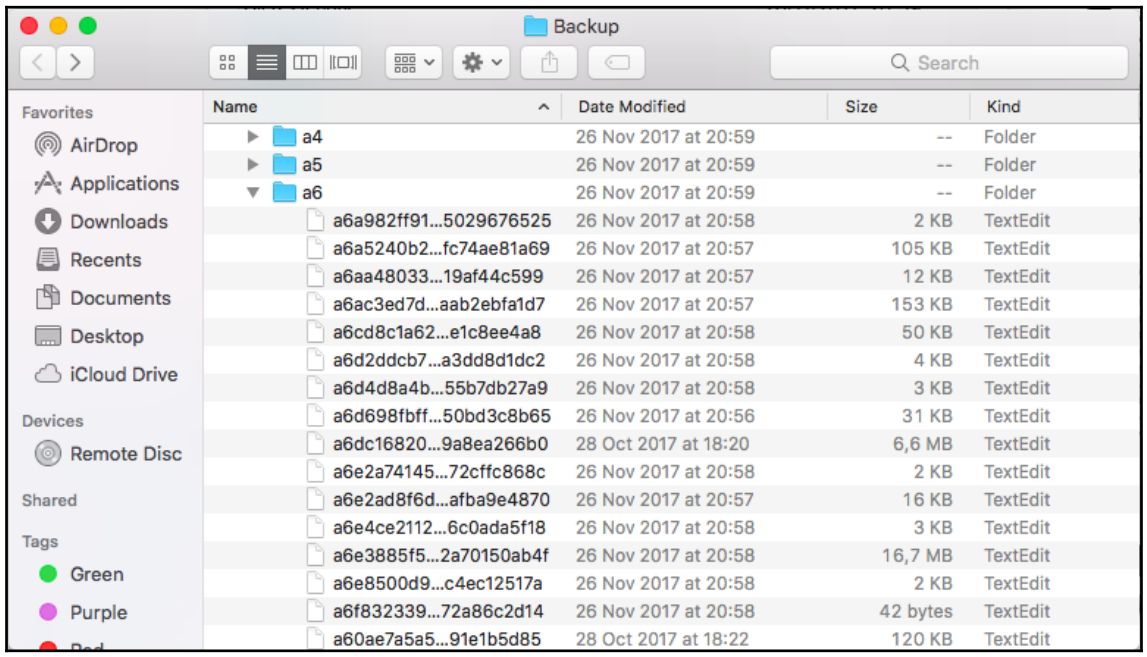
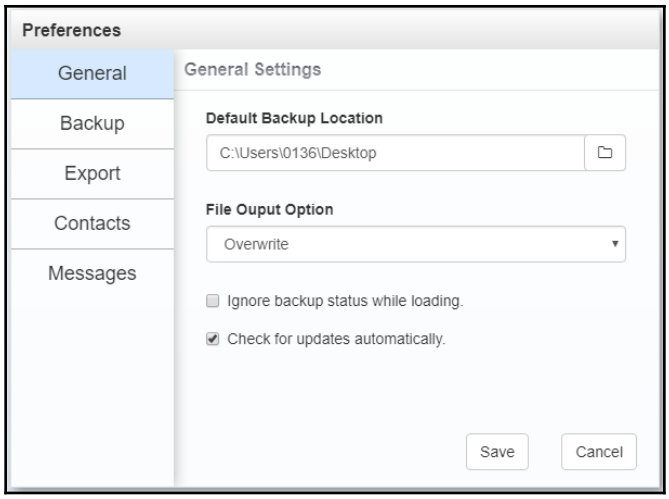


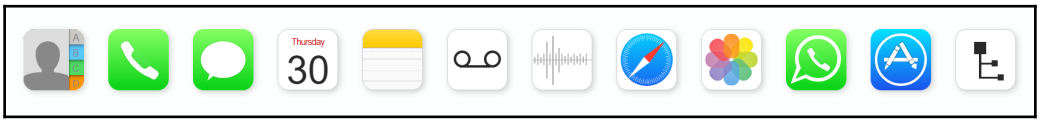
Table: Files

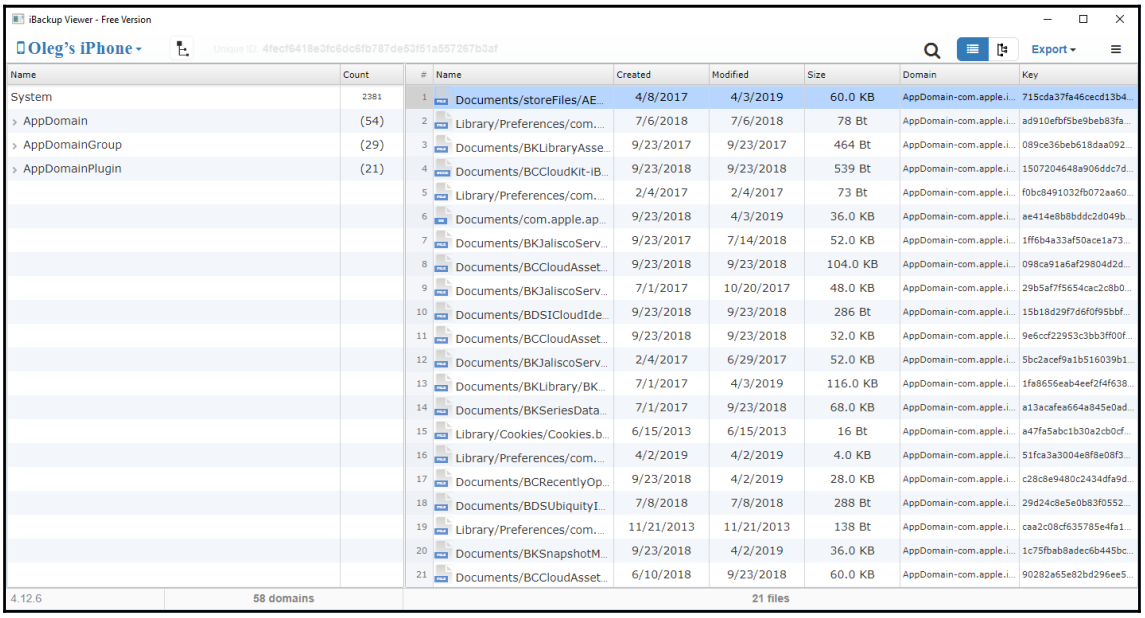
	fileID	domain	relativePath	flags	file
	Filter	Filter	Filter	Filter	Filter
1	afda7ee55cda906bb9c19bea20b4e24cef175697	AppDomainPl...		2	BLOB
2	7b3c1714085e93514051d002bb23c9a513026a5f	AppDomainPl...	Library	2	BLOB
3	194355033d8b11f073bcb09408f534e778cedc70	AppDomainPl...	Library/Prefer...	2	BLOB
4	6df229b4cb10c471da9c1983895cb4d9ccdc1873	AppDomainPl...	Documents	2	BLOB
5	fac9eafb0362d75594d67db61fd1f26e2eda244f	AppDomainPl...		2	BLOB
6	17ab1afd1d4c4a811b06ac84747591176b39a8f7	AppDomainPl...	Library	2	BLOB
7	88a61eb49575265693b1f6ab1bc74d572e35d8fa	AppDomainPl...	Library/Prefer...	2	BLOB
8	62565ee09eb8a968c812cc3bf4c934e638201f66	AppDomainPl...	Documents	2	BLOB
9	be1f28f40e6e4e95dba86a2d9fa4b12dc70b9dc5	CameraRollDo...		2	BLOB
10	735f4f65879e10473dae4050ceee99fbb69de281	CameraRollDo...	Media	2	BLOB
11	f0a585e77da56cd3812b3e1ee6a03b6e7e42edab	CameraRollDo...	Media/PhotoD...	2	BLOB
12	362cae198187f19960c73fcdc1e6d4a84ee2b37c	CameraRollDo...	Media/PhotoD...	2	BLOB
13	cacc5a1aca7bb6e7428e88a8e9868d3430844f9c	CameraRollDo...	Media/PhotoD...	2	BLOB
14	1e3b377ade507a70f48650b1ded97c8f9953e712	CameraRollDo...	Media/PhotoD...	2	BLOB
15	38cae1ba16df49a56efe545ac00bac45718092d1	CameraRollDo...	Media/PhotoD...	2	BLOB

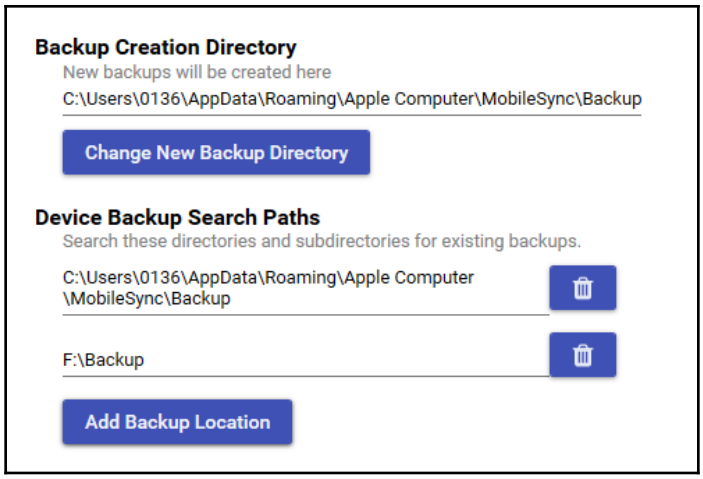

Edit Database Cell
Mode: Binary
Import
Export
Set as NULL
0000 62 70 6c 69 73 74 30 30 d4 01 02 03 04 05 06 26
0010 27 58 24 76 65 72 73 69 6f 6e 58 24 6f 62 6a 65
0020 63 74 73 59 24 61 72 63 68 69 76 65 72 54 24 74
0030 6f 70 12 00 01 86 a0 a4 07 08 1f 20 55 24 6e 75
0040 6c 6c dc 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
0050 16 17 18 19 1a 1b 1c 1d 1e 17 16 5c 4c 61 73 74
0060 4d 6f 64 69 66 69 65 64 55 46 6c 61 67 73 57 47
0070 72 6f 75 70 49 44 56 24 63 6c 61 73 73 5f 10 10
0080 4c 61 73 74 53 74 61 74 75 73 43 68 61 6e 67 65
0090 5c 52 65 6c 61 74 69 76 65 50 61 74 68 55 42 69
00a0 72 74 68 54 53 69 7a 65 5b 49 6e 6f 64 65 4e 75
00b0 6d 62 65 72 54 4d 6f 64 65 56 55 73 65 72 49 44
00c0 5f 10 0f 50 72 6f 74 65 63 74 69 6f 6e 43 6c 61
00d0 73 73 12 5b f4 ed 01 10 00 11 01 f5 80 03 12 5c
00e0 4c 8e 94 80 02 12 5b f4 ec fd 10 00 12 00 db a7
00f0 23 11 41 ed 50 d2 21 22 23 24 5a 24 63 6c 61 73
0100 73 6e 61 6d 65 58 24 63 6c 61 73 73 65 73 56 4d
0110 42 46 69 6c 65 a2 23 25 58 4e 53 4f 62 6a 65 63
0120 74 5f 10 0f 4e 53 4b 65 79 65 64 41 72 63 68 69
0130 76 65 72 d1 28 29 54 72 6f 6f 74 80 01 00 08 00
0140 11 00 1a 00 23 00 2d 00 32 00 37 00 3c 00 42 00
0150 5b 00 68 00 6e 00 76 00 7d 00 90 00 9d 00 a3 00
Type of data currently in cell: Binary
433 byte(s)
Apply

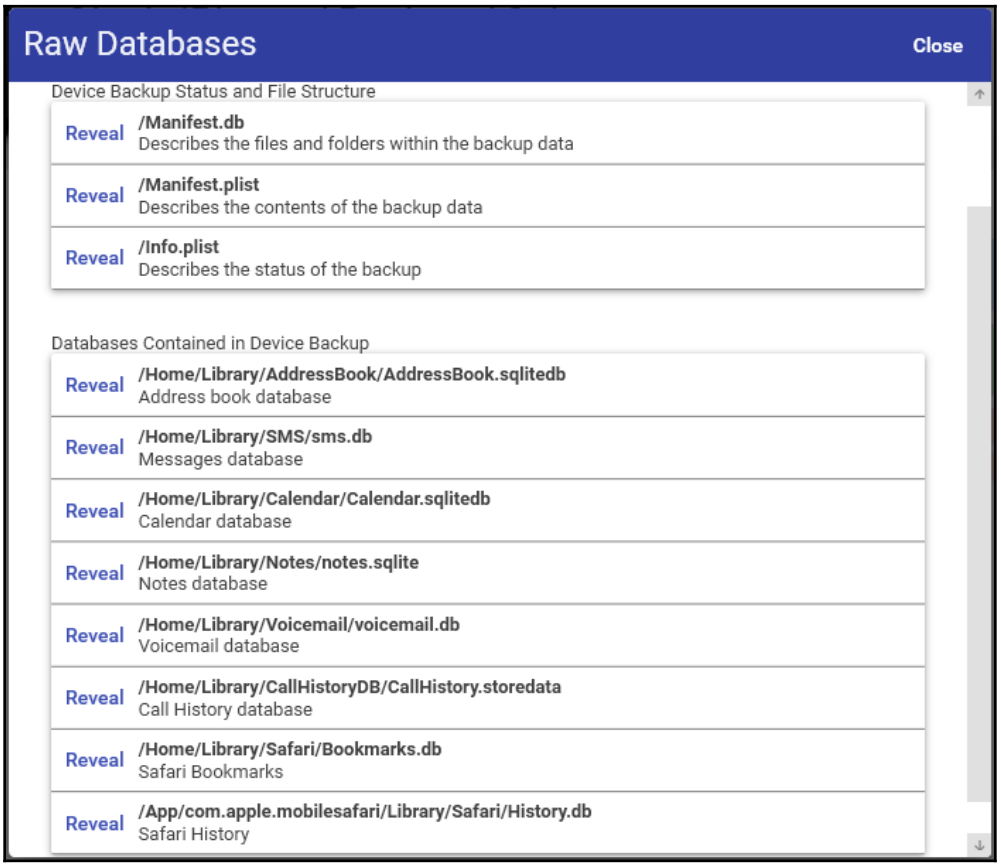

Backup
Search
Favorites
AirDrop
Applications
Downloads
Recents
Documents
Desktop
iCloud Drive
Devices
Remote Disc
Shared
Tags
Green
Purple
Name
Date Modified
Size
Kind
a4 26 Nov 2017 at 20:59 -- Folder
a5 26 Nov 2017 at 20:59 -- Folder
a6 26 Nov 2017 at 20:59 -- Folder
a6a982ff91...5029676525 26 Nov 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

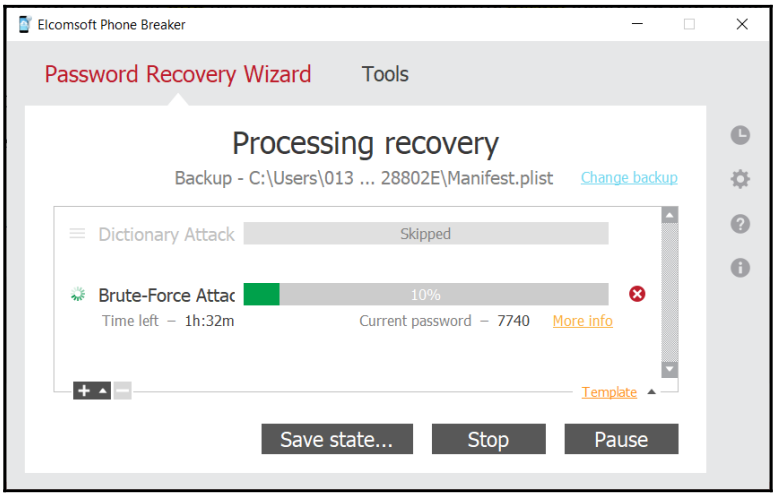

Thursday
30

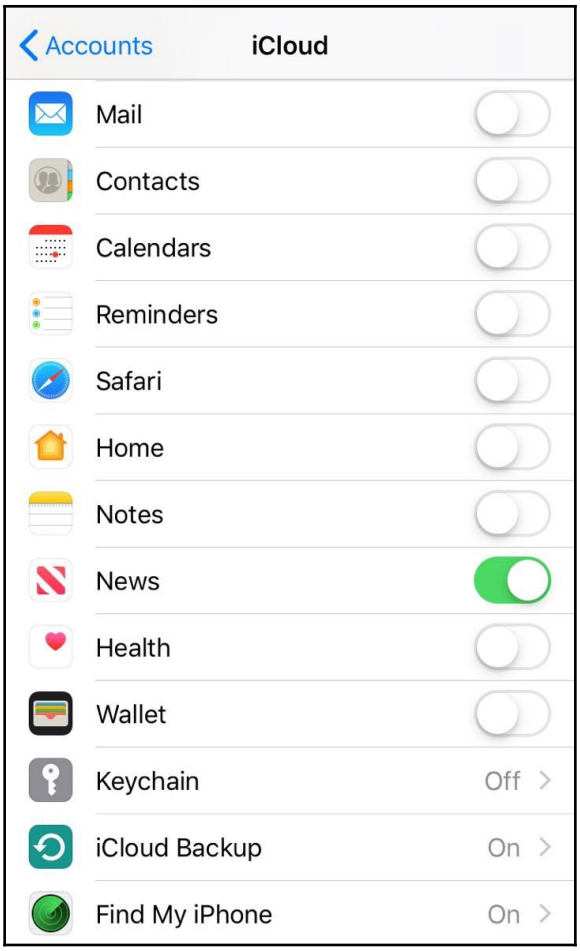

iBackup Viewer - Free Version
Oleg's iPhone
Export
Name
Count
System
AppDomain
AppDomainGroup
AppDomainPlugin
Created
Modified
Size
Domain
Key
4.12.6
58 domains
21 files

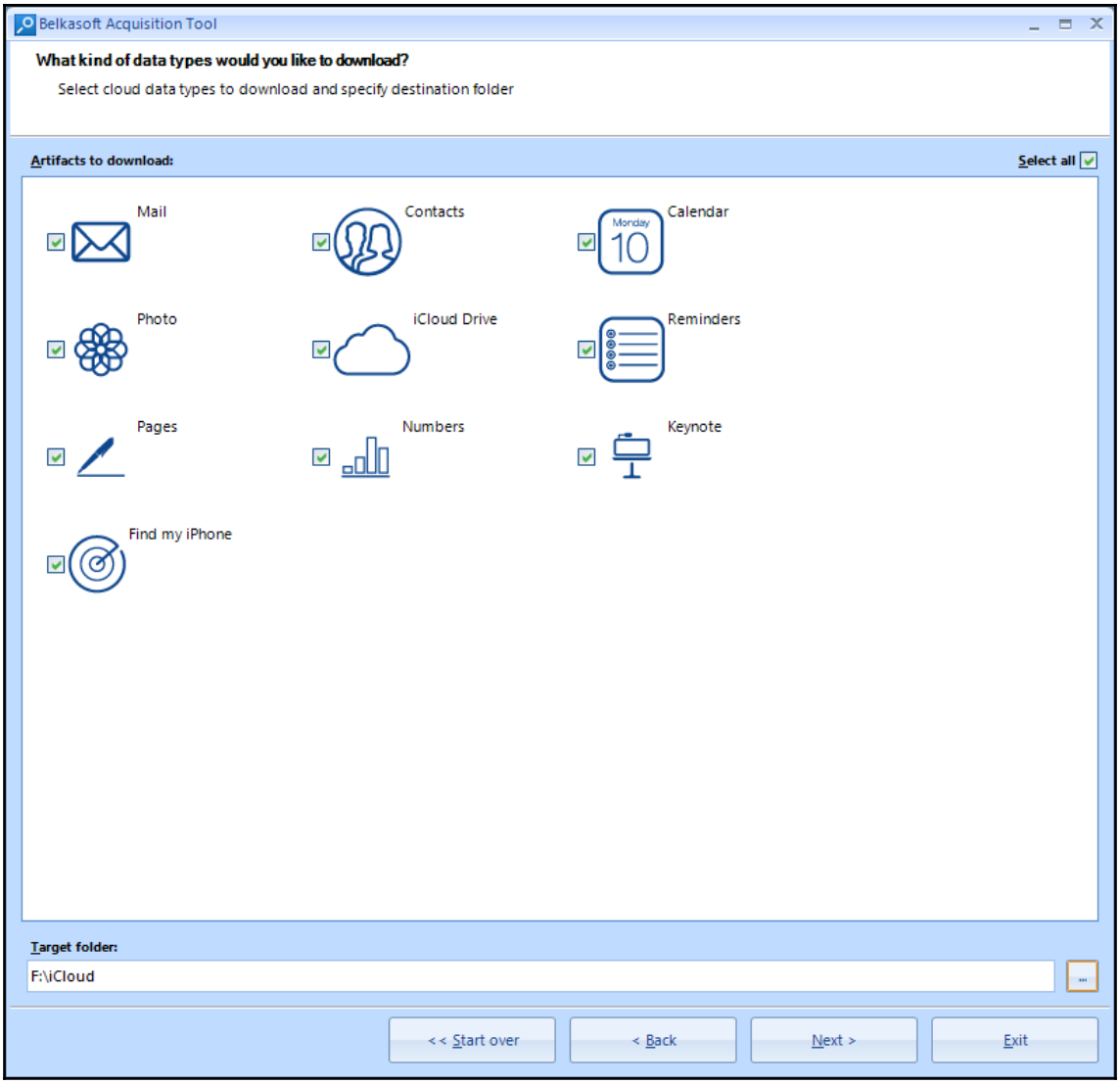

Backup Creation Directory
New backups will be created here
C:\Users\0136\AppData\Roaming\Apple Computer\MobileSync\Backup
Change New Backup Directory
Device Backup Search Paths
Search these directories and subdirectories for existing backups.
C:\Users\0136\AppData\Roaming\Apple Computer \MobileSync\Backup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

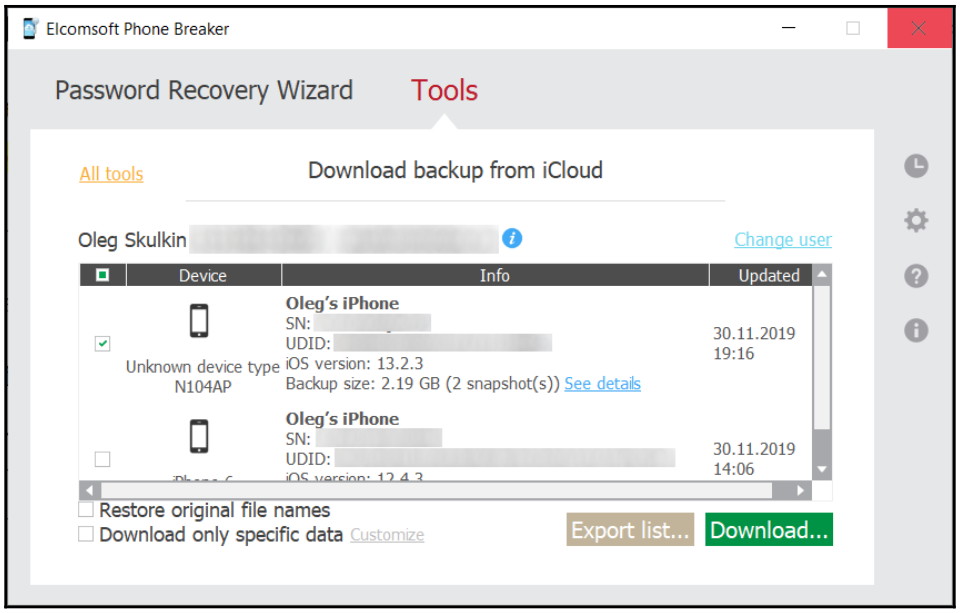

Raw Databases
Close
Device Backup Status and File Structure
Reveal /Manifest.db
Describes the files and folders within the backup data
Reveal /Manifest.plist
Describes the contents of the backup data
Reveal /Info.plist
Describes the status of the backup
Databases Contained in Device Backup
Reveal /Home/Library/AddressBook/AddressBook.sqlitedb
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


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

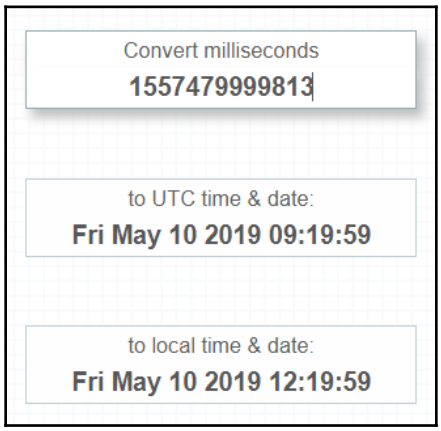

Elcomsoft Phone Breaker
Password Recovery Wizard
Tools
Processing recovery
Backup - C:\Users\013 ... 28802E\Manifest.plist
Change backup
Dictionary Attack
Skipped
Brute-Force Attac
10%
Time left – 1h:32m
Current password – 7740
More info
Template
Save state...
Stop
Pause

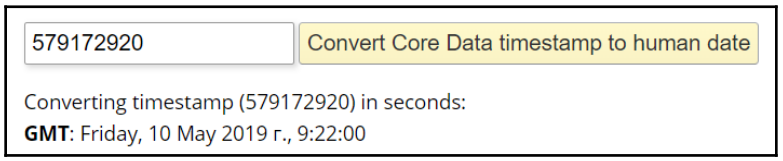

Accounts
iCloud
Mail
Contacts
Calendars
Reminders
Safari
Home
Notes
News
Health
Wallet
Keychain
Off
iCloud Backup
On
Find My iPhone
On

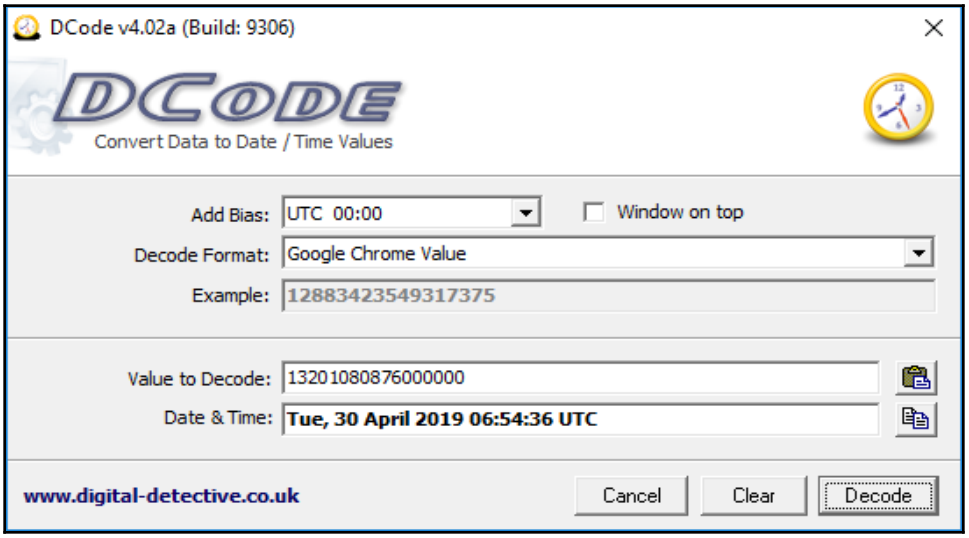

Belkasoft Acquisition Tool
What kind of data types would you like to download?
Select cloud data types to download and specify destination folder
Artifacts to download:
Select all
Mail
Contacts
Calendar
Monday
10
Photo
iCloud Drive
Reminders
Pages
Numbers
Keynote
Find my iPhone
Target folder:
F:\iCloud
...
<< Start over
< Back
Next >
Exit


Elcomsoft Phone Breaker
Password Recovery Wizard
Tools
All tools
Download backup from iCloud
Oleg Skulkin
Change user
Device
Info
Updated
Oleg's iPhone
SN:
UDID:
Unknown device type
N104AP
iOS version: 13.2.3
Backup size: 2.19 GB (2 snapshot(s)) See details
30.11.2019
19:16
Oleg's iPhone
SN:
UDID:
30.11.2019
14:06
Restore original file names
Download only specific data Customize
Export list...
Download...

Chapter 5: iOS Data Analysis and Recovery



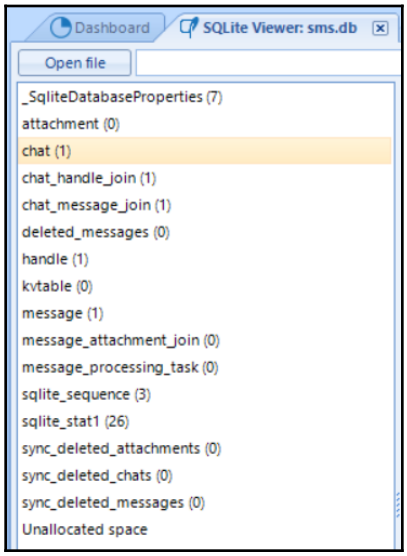


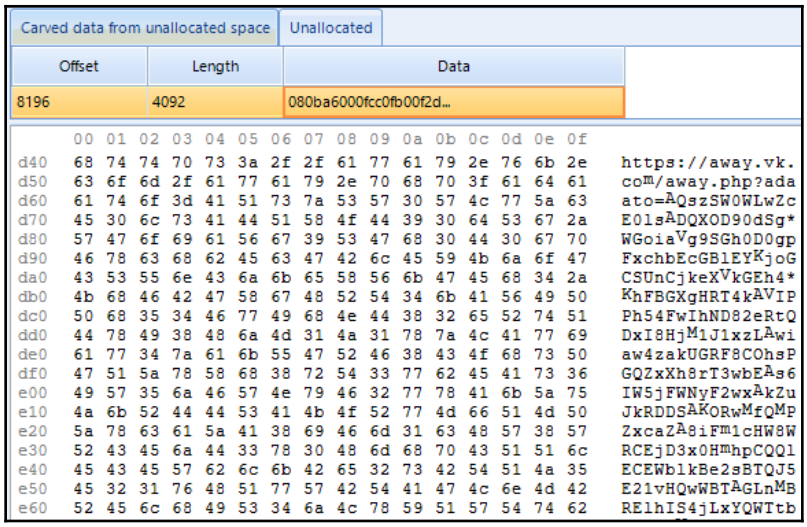


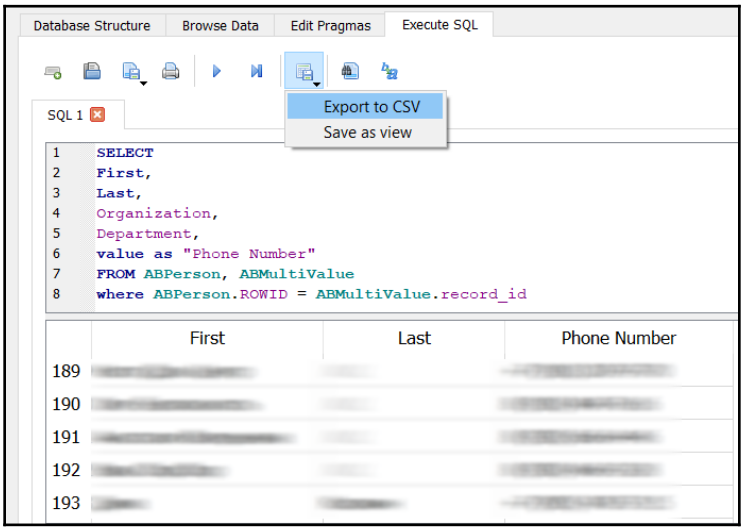
```
sqlite> .tables
_SqliteDatabaseProperties  kvtable
attachment                 message
chat                       message_attachment_join
chat_handle_join           message_processing_task
chat_message_join          sync_deleted_attachments
deleted_messages           sync_deleted_chats
handle    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

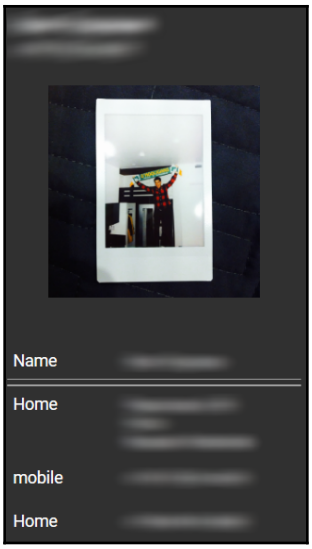
```
sqlite> .schema handle
CREATE TABLE handle ( ROWID INTEGER PRIMARY KEY AUTOINCREMENT UNIQUE, id TEXT NOT NULL,
country TEXT, service TEXT NOT NULL, uncanonicalized_id TEXT, UNIQUE (id, service) );
```

```
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;
```




Carved data from unallocated space
Unallocated
Offset
Length
Data
8196
4092
080ba6000fcc0fb00f2d…
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
d40 68 74 74 70 73 3a 2f 2f 61 77 61 79 2e 76 6b 2e https://away.vk.
d50 63 6f 6d 2f 61 77 61 79 2e 70 68 70 3f 61 64 61 com/away.php?ada
d60 61 74 6f 3d 41 51 73 7a 53 57 30 57 4c 77 5a 63 ato=AQszSW0WLwZc
d70 45 30 6c 73 41 44 51 58 4f 44 39 30 64 53 67 2a E0lsADQXOD90dSg*
d80 57 47 6f 69 61 56 67 39 53 47 68 30 44 30 67 70 WGoiaVg9SGh0D0gp
d90 46 78 63 68 62 45 63 47 42 6c 45 59 4b 6a 6f 47 FxchbEcGBlEYKjoG
da0 43 53 55 6e 43 6a 6b 65 58 56 6b 47 45 68 34 2a CSUnCjkeXVkGEh4*
db0 4b 68 46 42 47 58 67 48 52 54 34 6b 41 56 49 50 KhFBGXgHRT4kAVIP
dc0 50 68 35 34 46 77 49 68 4e 44 38 32 65 52 74 51 Ph54FwIhND82eRtQ
dd0 44 78 49 38 48 6a 4d 31 4a 31 78 7a 4c 41 77 69 DxI8HjM1J1xzLAwi
de0 61 77 34 7a 61 6b 55 47 52 46 38 43 4f 68 73 50 aw4zakUGRF8COhsP
df0 47 51 5a 78 58 68 38 72 54 33 77 62 45 41 73 36 GQZxXh8rT3wbEAs6
e00 49 57 35 6a 46 57 4e 79 46 32 77 78 41 6b 5a 75 IW5jFWNyF2wxAkZu
e10 4a 6b 52 44 44 53 41 4b 4f 52 77 4d 66 51 4d 50 JkRDDSAKORwMfQMP
e20 5a 78 63 61 5a 41 38 69 46 6d 31 63 48 57 38 57 ZxcaZA8iFm1cHW8W
e30 52 43 45 6a 44 33 78 30 48 6d 68 70 43 51 51 6c RCEjD3x0HmhpCQQl
e40 45 43 45 57 62 6c 6b 42 65 32 73 42 54 51 4a 35 ECEWblkBe2sBTQJ5
e50 45 32 31 76 48 51 77 57 42 54 41 47 4c 6e 4d 42 E21vHQwWBTAGLnMB
e60 52 45 6c 68 49 53 34 6a 4c 78 59 51 57 54 74 62 RElhIS4jLxYQWTtb


Database Structure
Browse Data
Edit Pragmas
Execute SQL
Export to CSV
Save as view
SQL 1
1 SELECT
2 First,
3 Last,
4 Organization,
5 Department,
6 value as "Phone Number"
7 FROM ABPerson, ABMultiValue
8 where ABPerson.ROWID = ABMultiValue.record_id
First
Last
Phone Number
189
190
191
192
193

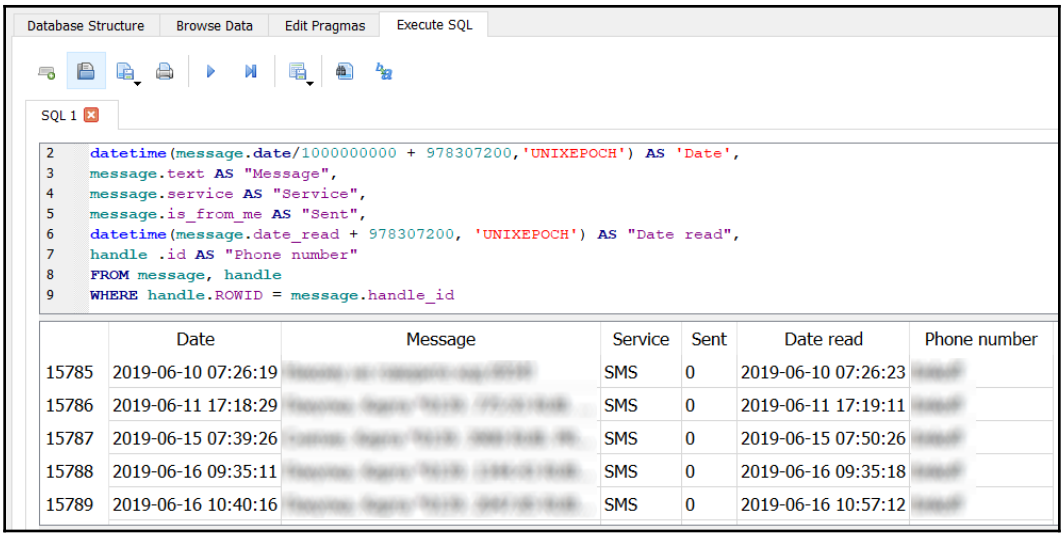


Database Structure | Browse Data | Edit Pragmas | Execute SQL

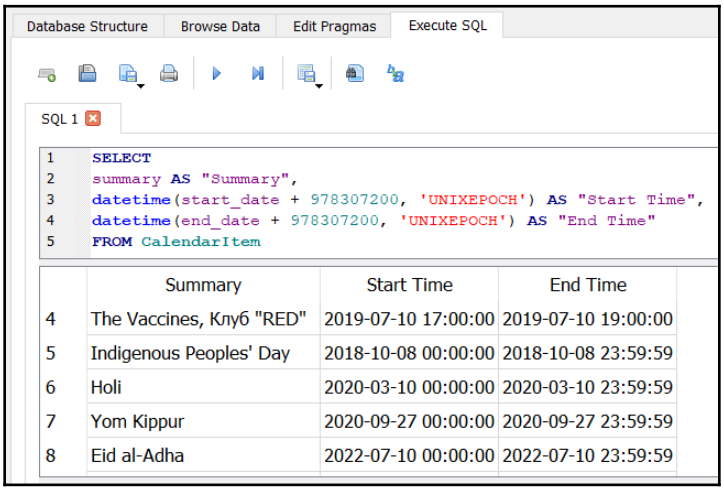
SQL 1

```
1  SELECT
2  datetime(ZDATE+978307200, 'UNIXEPOCH') as "Date",
3  ZDURATION AS "Duration",
4  ZLOCATION AS "Location",
5  ZADDRESS AS "Number",
6  ZSERVICE_PROVIDER AS "Service Provider"
7  FROM ZCALLRECORD
```

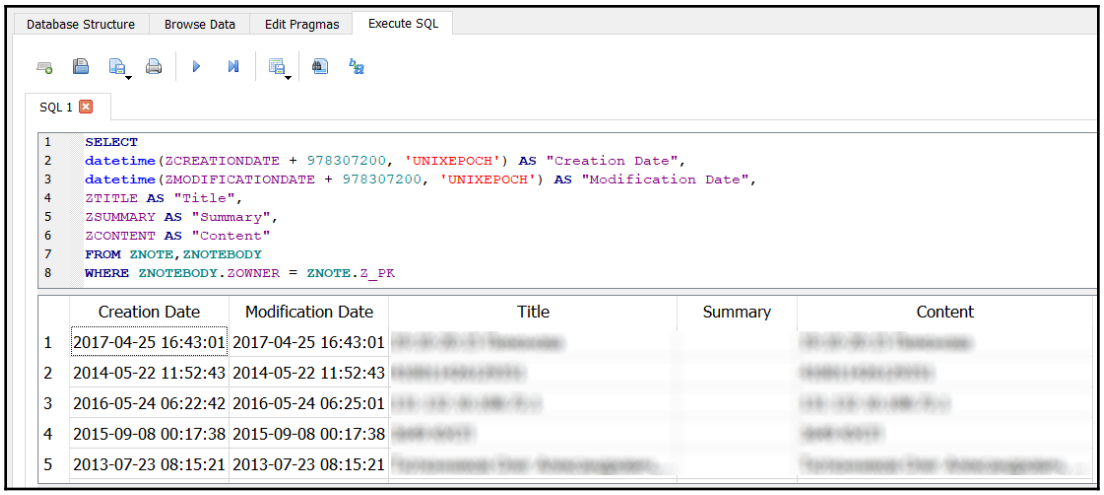
	Date	Duration	Location	Number	Service Provider
1	2019-09-23 16:31:04	0.0	*NULL*	+7915	com.apple.Telephony
2	2019-10-17 16:02:40	139.950350999832	Russia	+7915	com.apple.Telephony
3	2019-10-05 14:00:20	55.2437419891357	Russia	+7915	com.apple.Telephony
4	2019-09-25 08:37:41	37.6506769657135	Russia	+7905	com.apple.Telephony
5	2019-09-26 10:46:16	39.0366480350494	Russia	+7918	com.apple.Telephony

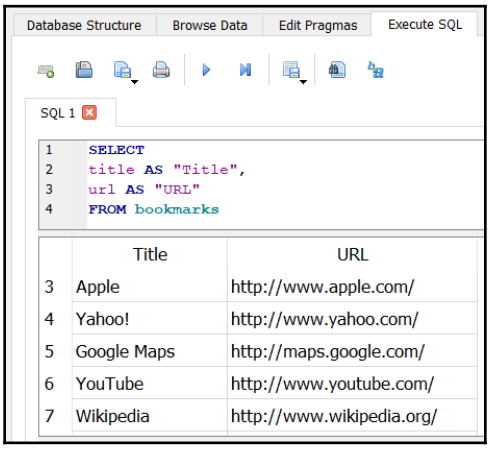


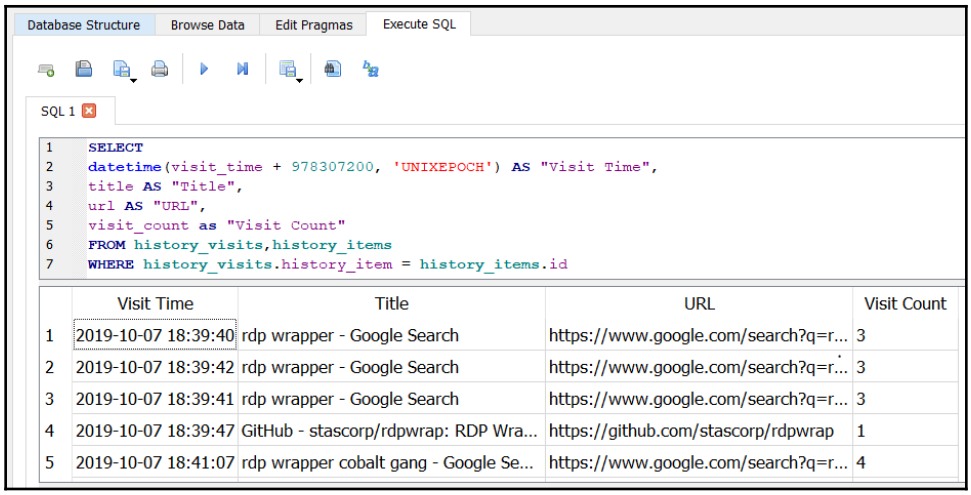
	Date	Message	Service	Sent	Date read	Phone number
15785	2019-06-10 07:26:19	[redacted]	SMS	0	2019-06-10 07:26:23	[redacted]
15786	2019-06-11 17:18:29	[redacted]	SMS	0	2019-06-11 17:19:11	[redacted]
15787	2019-06-15 07:39:26	[redacted]	SMS	0	2019-06-15 07:50:26	[redacted]
15788	2019-06-16 09:35:11	[redacted]	SMS	0	2019-06-16 09:35:18	[redacted]
15789	2019-06-16 10:40:16	[redacted]	SMS	0	2019-06-16 10:57:12	[redacted]



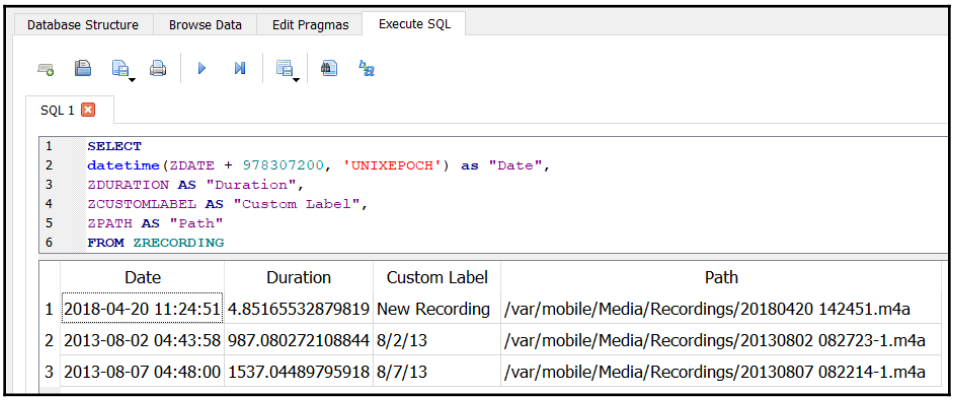
	Summary	Start Time	End Time
4	The Vaccines, Клуб "RED"	2019-07-10 17:00:00	2019-07-10 19:00:00
5	Indigenous Peoples' Day	2018-10-08 00:00:00	2018-10-08 23:59:59
6	Holi	2020-03-10 00:00:00	2020-03-10 23:59:59
7	Yom Kippur	2020-09-27 00:00:00	2020-09-27 23:59:59
8	Eid al-Adha	2022-07-10 00:00:00	2022-07-10 23:59:59


Database Structure
Browse Data
Edit Pragmas
Execute SQL
SQL 1
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
Creation Date
Modification Date
Title
Summary
Content
1 2017-04-25 16:43:01 2017-04-25 16:43:01
2 2014-05-22 11:52:43 2014-05-22 11:52:43
3 2016-05-24 06:22:42 2016-05-24 06:25:01
4 2015-09-08 00:17:38 2015-09-08 00:17:38
5 2013-07-23 08:15:21 2013-07-23 08:15:21


Database Structure
Browse Data
Edit Pragmas
Execute SQL
SQL 1
SELECT
title AS "Title",
url AS "URL"
FROM bookmarks
Title
URL
3 Apple http://www.apple.com/
4 Yahoo! http://www.yahoo.com/
5 Google Maps http://maps.google.com/
6 YouTube http://www.youtube.com/
7 Wikipedia http://www.wikipedia.org/



	Visit Time	Title	URL	Visit Count
1	2019-10-07 18:39:40	rdp wrapper - Google Search	https://www.google.com/search?q=r...	3
2	2019-10-07 18:39:42	rdp wrapper - Google Search	https://www.google.com/search?q=r...	3
3	2019-10-07 18:39:41	rdp wrapper - Google Search	https://www.google.com/search?q=r...	3
4	2019-10-07 18:39:47	GitHub - stascorp/rdpwrap: RDP Wra...	https://github.com/stascorp/rdpwrap	1
5	2019-10-07 18:41:07	rdp wrapper cobalt gang - Google Se...	https://www.google.com/search?q=r...	4



	Date	Duration	Custom Label	Path
1	2018-04-20 11:24:51	4.85165532879819	New Recording	/var/mobile/Media/Recordings/20180420 142451.m4a
2	2013-08-02 04:43:58	987.080272108844	8/2/13	/var/mobile/Media/Recordings/20130802 082723-1.m4a
3	2013-08-07 04:48:00	1537.04489795918	8/7/13	/var/mobile/Media/Recordings/20130807 082214-1.m4a

Database Structure | Browse Data | Edit Pragmas | Execute SQL

SQL 1

```
SELECT
datetime(ZINTERACTIONS.ZCREATIONDATE + 978307200, 'UNIXEPOCH') as "Creation Date",
datetime(ZINTERACTIONS.ZSTARTDATE + 978307200, 'UNIXEPOCH') as "Start Time",
datetime(ZINTERACTIONS.ZENDDATE + 978307200, 'UNIXEPOCH') as "End Time",
ZBUNDLEID as "Bundle ID",
ZDOMAINIDENTIFIER as "Action"
FROM ZINTERACTIONS
```

	Creation Date	Start Time	End Time	Bundle ID	Action
369	2019-10-23 06:39:36	2019-10-23 06:39:36	2019-10-23 06:39:36	net.whatsapp.WhatsApp	send-message
370	2019-10-23 06:39:48	2019-10-23 06:39:48	2019-10-23 06:39:48	net.whatsapp.WhatsApp	send-message
371	2019-10-23 06:40:27	2019-10-23 06:40:27	2019-10-23 06:40:27	net.whatsapp.WhatsApp	send-message
372	2019-10-23 06:44:01	2019-10-23 06:44:00	2019-10-23 06:44:00	net.whatsapp.WhatsApp	send-message
373	2019-10-23 06:47:14	2019-10-23 06:47:14	2019-10-23 06:47:14	net.whatsapp.WhatsApp	send-message

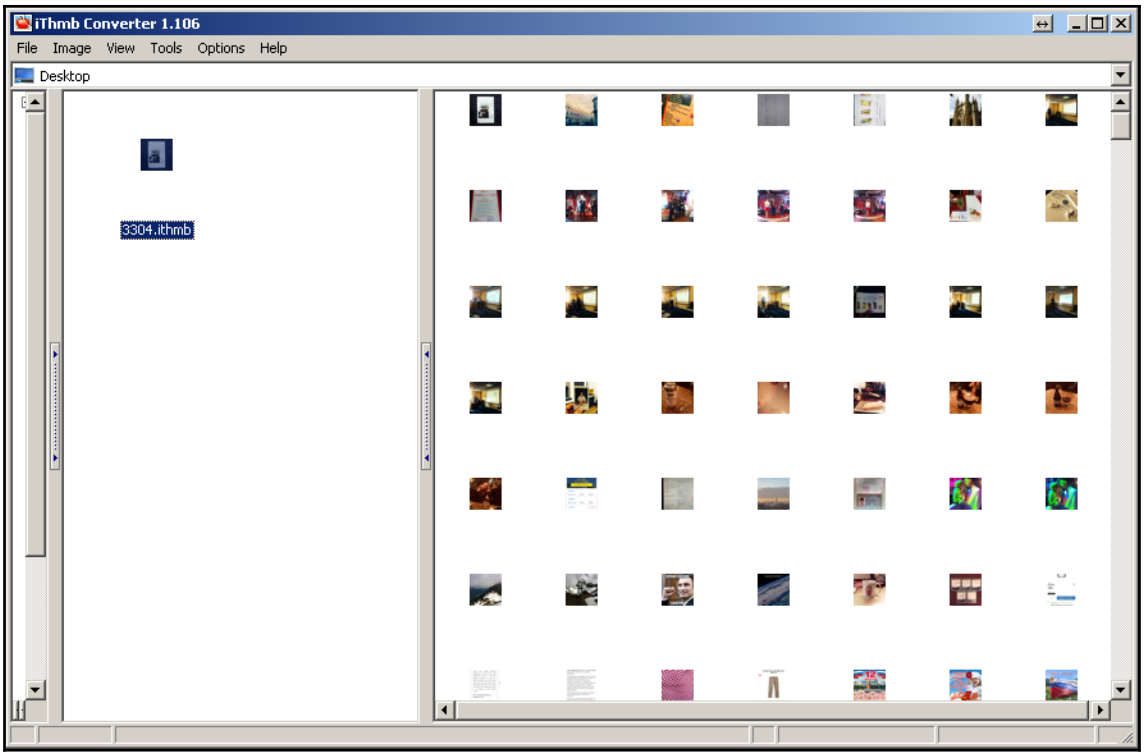
Database Structure | Browse Data | Edit Pragmas | Execute SQL

SQL 1

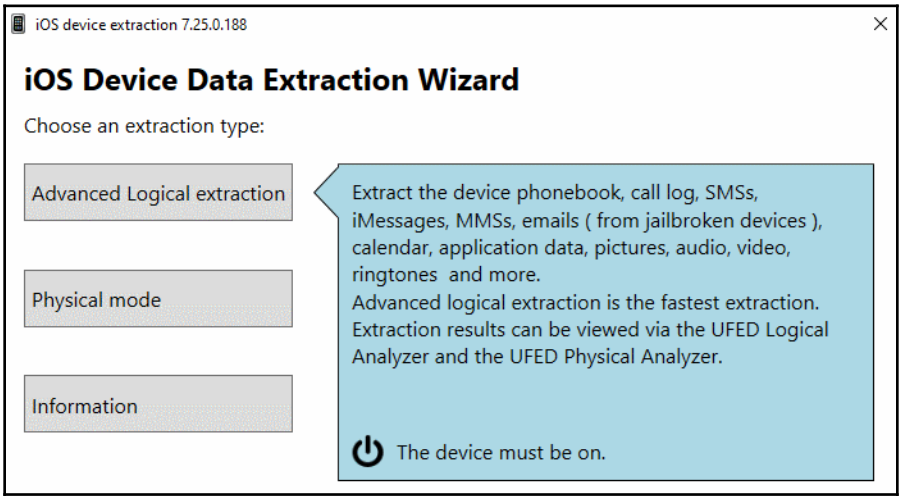
```
SELECT
subscriber_id as "ICCID",
subscriber_MDN as "Phone Number",
datetime(last_update_time + 978307200, 'UNIXEPOCH') as "Last Update Time"
from subscriber_info
```

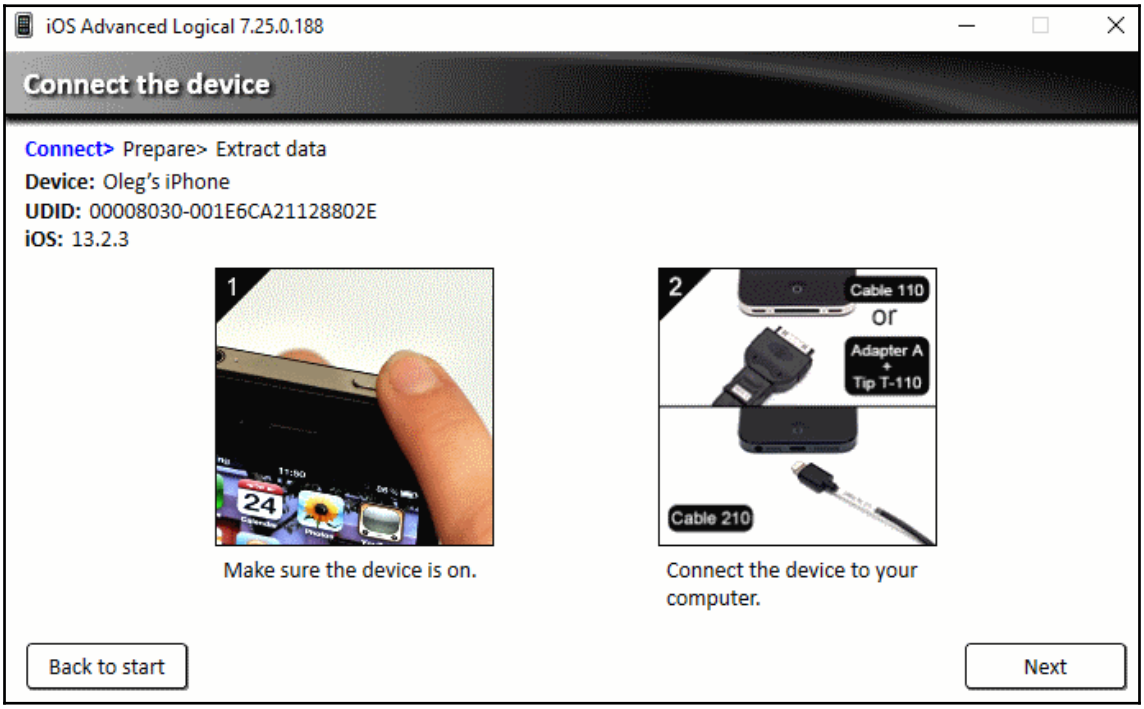
	ICCID	Phone Number	Last Update Time
1	89701[redacted]		2017-06-28 16:12:46
2	89701[redacted]		2017-11-11 18:11:26
3	89701[redacted]		2019-10-28 18:35:33

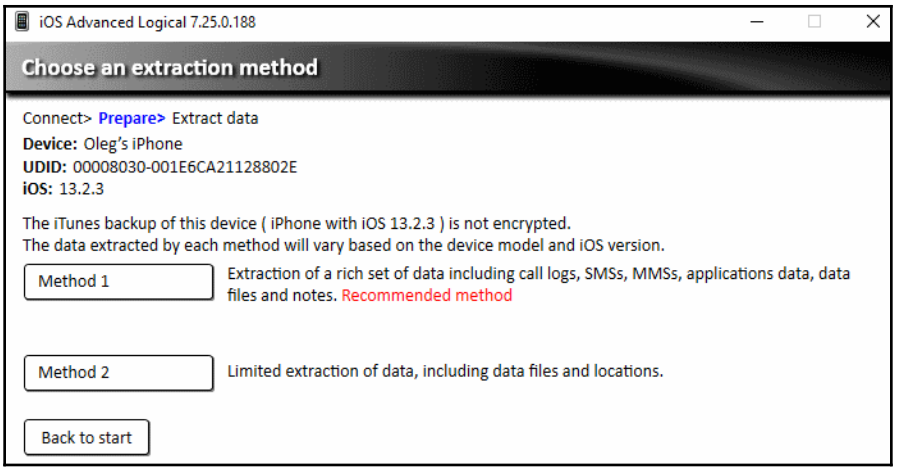
Key	Type	Value
Root	dict	
Version	string	2.0
LastiTunesBackupTZ	string	GMT+3
RequiresEncryption	integer	0
WillEncrypt	boolean	true
LastiTunesBackupDate	integer	581862772
CloudBackupEnabled	boolean	true
LastCloudBackupTZ	string	GMT+3
LastCloudBackupDate	integer	594465315

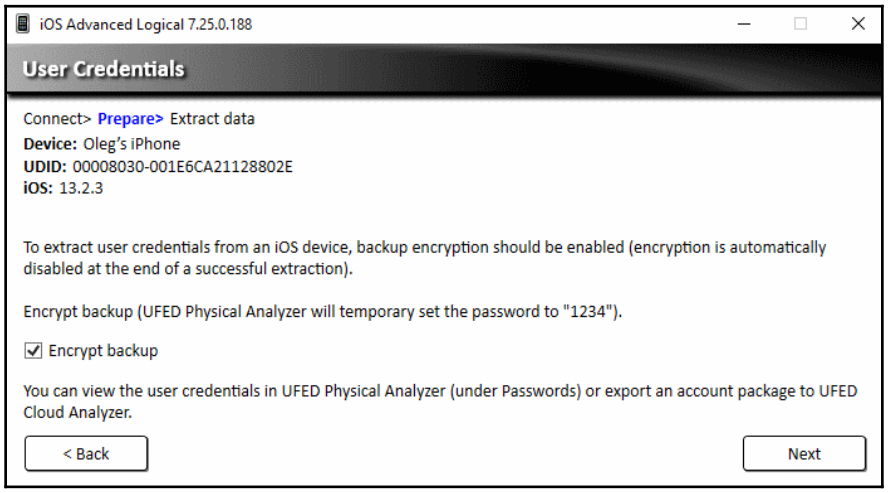

iThmb Converter 1.106
File Image View Tools Options Help
Desktop
3304.ithmb

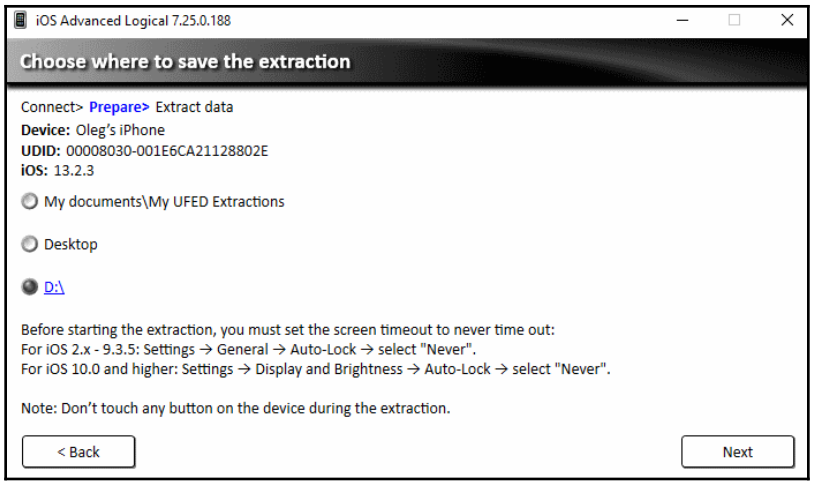
Chapter 6: iOS Forensic Tools

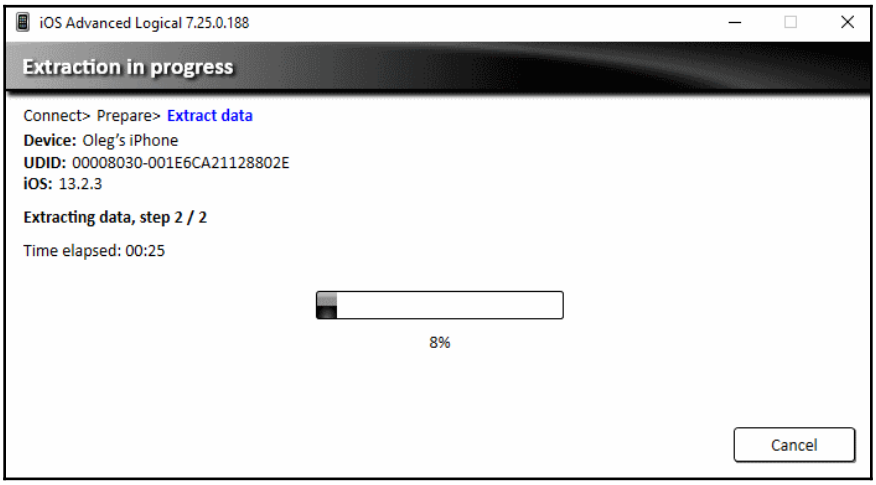


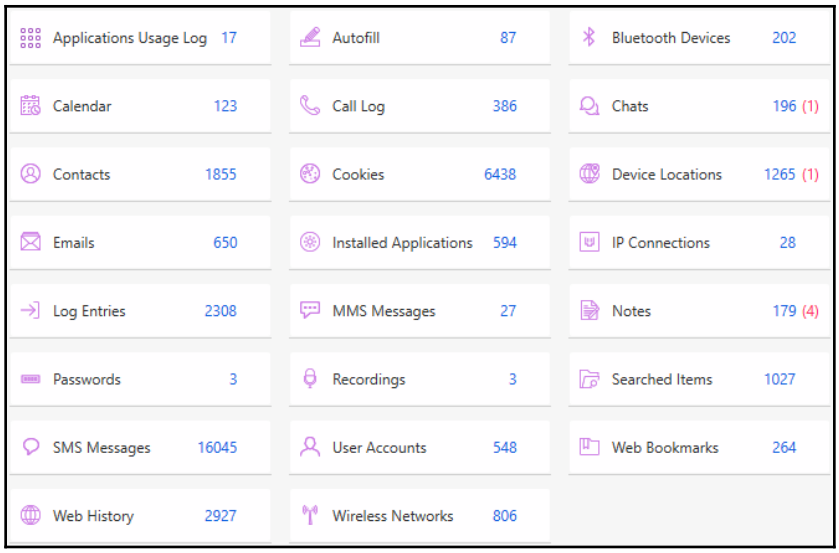


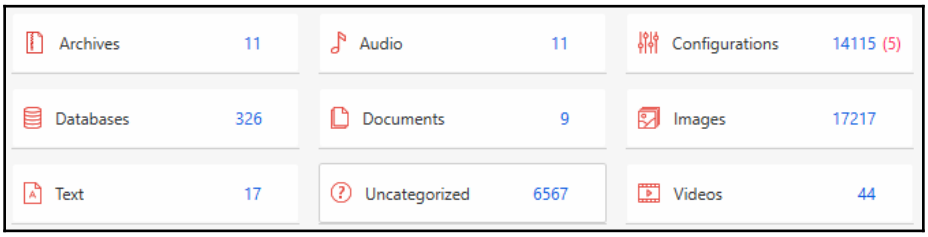

iOS Advanced Logical 7.25.0.188
Choose an extraction method
Connect> Prepare> Extract data
Device: Oleg's iPhone
UDID: 00008030-001E6CA21128802E
iOS: 13.2.3
The iTunes backup of this device (iPhone with iOS 13.2.3) is not encrypted.
The data extracted by each method will vary based on the device model and iOS version.
Method 1
Extraction of a rich set of data including call logs, SMSs, MMSs, applications data, data files and notes. Recommended method
Method 2
Limited extraction of data, including data files and locations.
Back to start

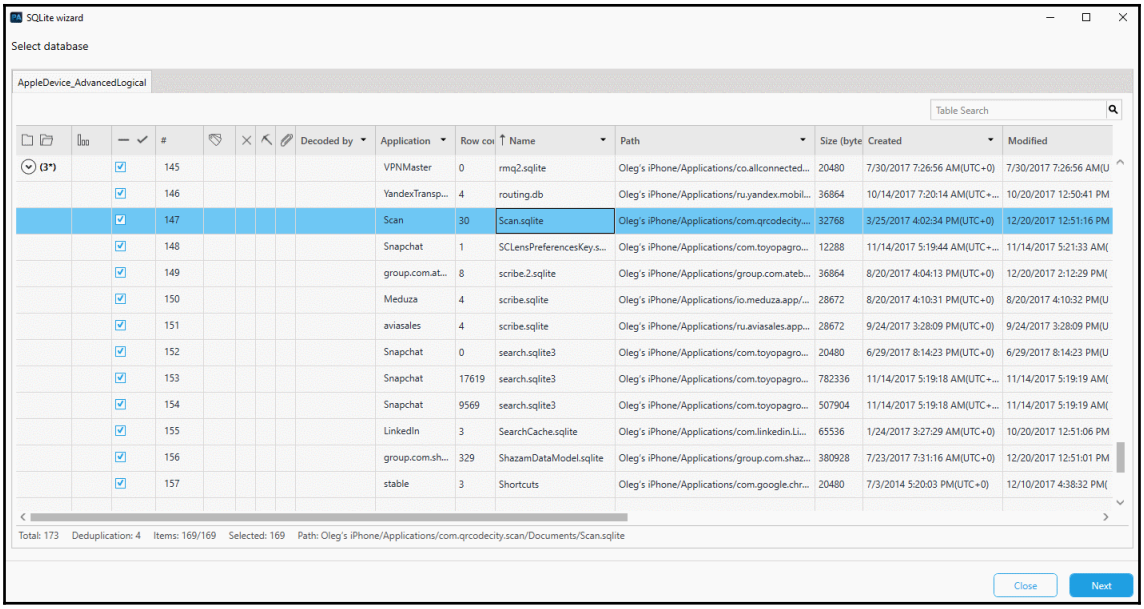

iOS Advanced Logical 7.25.0.188
User Credentials
Connect> Prepare> Extract data
Device: Oleg's iPhone
UDID: 00008030-001E6CA21128802E
iOS: 13.2.3
To extract user credentials from an iOS device, backup encryption should be enabled (encryption is automatically disabled at the end of a successful extraction).
Encrypt backup (UFED Physical Analyzer will temporary set the password to "1234").
Encrypt backup
You can view the user credentials in UFED Physical Analyzer (under Passwords) or export an account package to UFED Cloud Analyzer.
< Back
Next

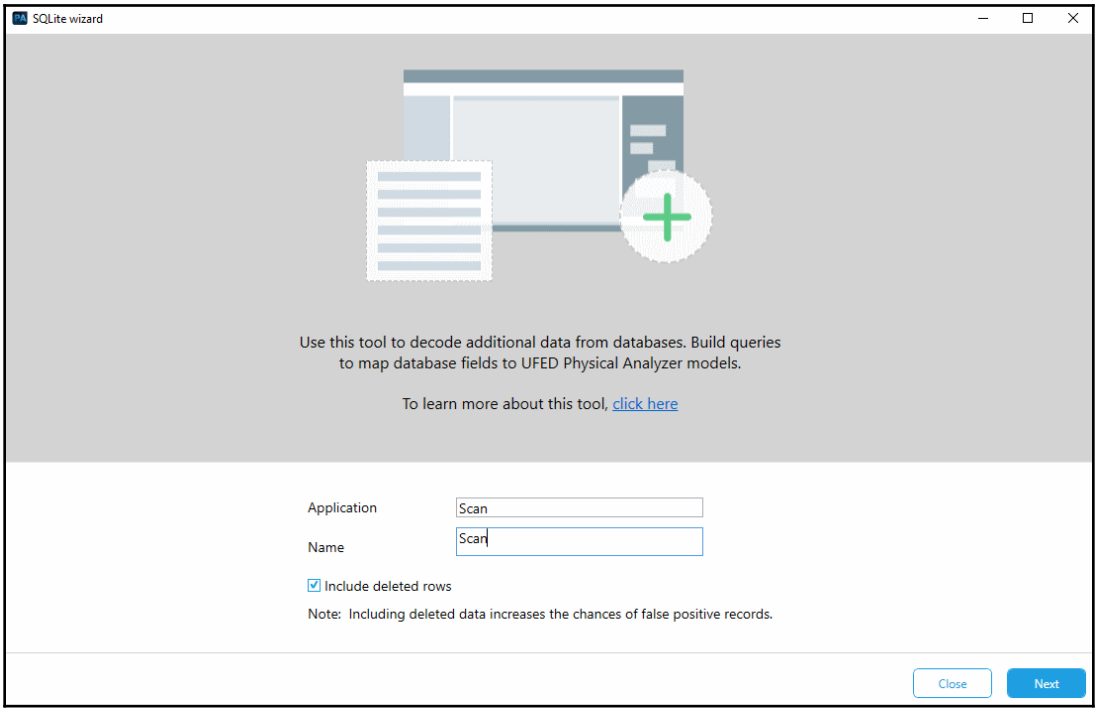

iOS Advanced Logical 7.25.0.188
Choose where to save the extraction
Connect> Prepare> Extract data
Device: Oleg's iPhone
UDID: 00008030-001E6CA21128802E
iOS: 13.2.3
My documents\My UFED Extractions
Desktop
D:\
Before starting the extraction, you must set the screen timeout to never time out:
For iOS 2.x - 9.3.5: Settings → General → Auto-Lock → select "Never".
For iOS 10.0 and higher: Settings → Display and Brightness → Auto-Lock → select "Never".
Note: Don't touch any button on the device during the extraction.
< Back
Next

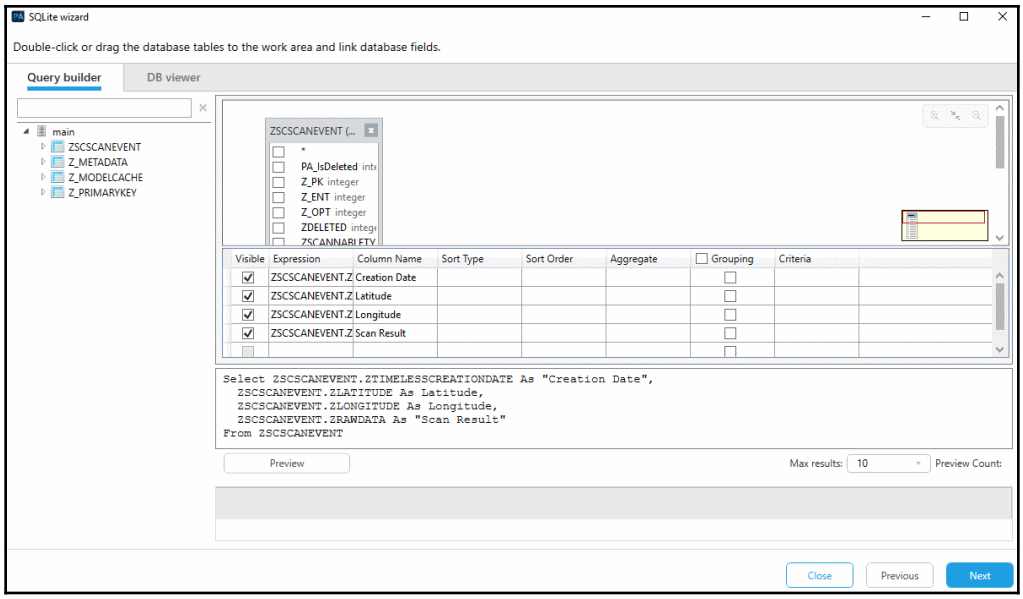

iOS Advanced Logical 7.25.0.188
Extraction in progress
Connect> Prepare> Extract data
Device: Oleg's iPhone
UDID: 00008030-001E6CA21128802E
iOS: 13.2.3
Extracting data, step 2 / 2
Time elapsed: 00:25
8%
Cancel

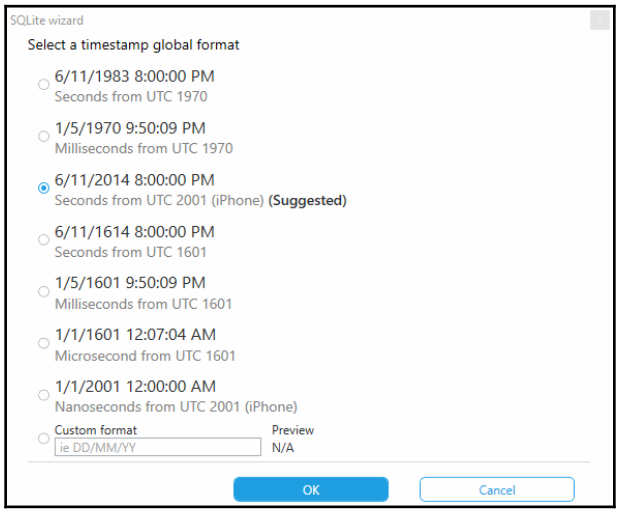

Applications Usage Log 17
Autofill 87
Bluetooth Devices 202
Calendar 123
Call Log 386
Chats 196 (1)
Contacts 1855
Cookies 6438
Device Locations 1265 (1)
Emails 650
Installed Applications 594
IP Connections 28
Log Entries 2308
MMS Messages 27
Notes 179 (4)
Passwords 3
Recordings 3
Searched Items 1027
SMS Messages 16045
User Accounts 548
Web Bookmarks 264
Web History 2927
Wireless Networks 806

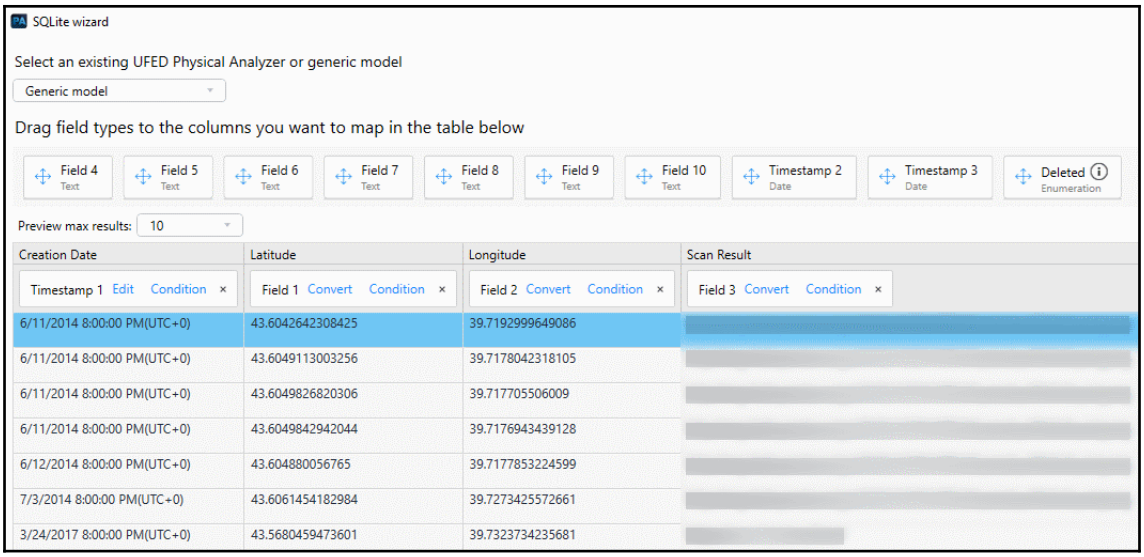

Archives 11
Audio 11
Configurations 14115 (5)
Databases 326
Documents 9
Images 17217
Text 17
Uncategorized 6567
Videos 44

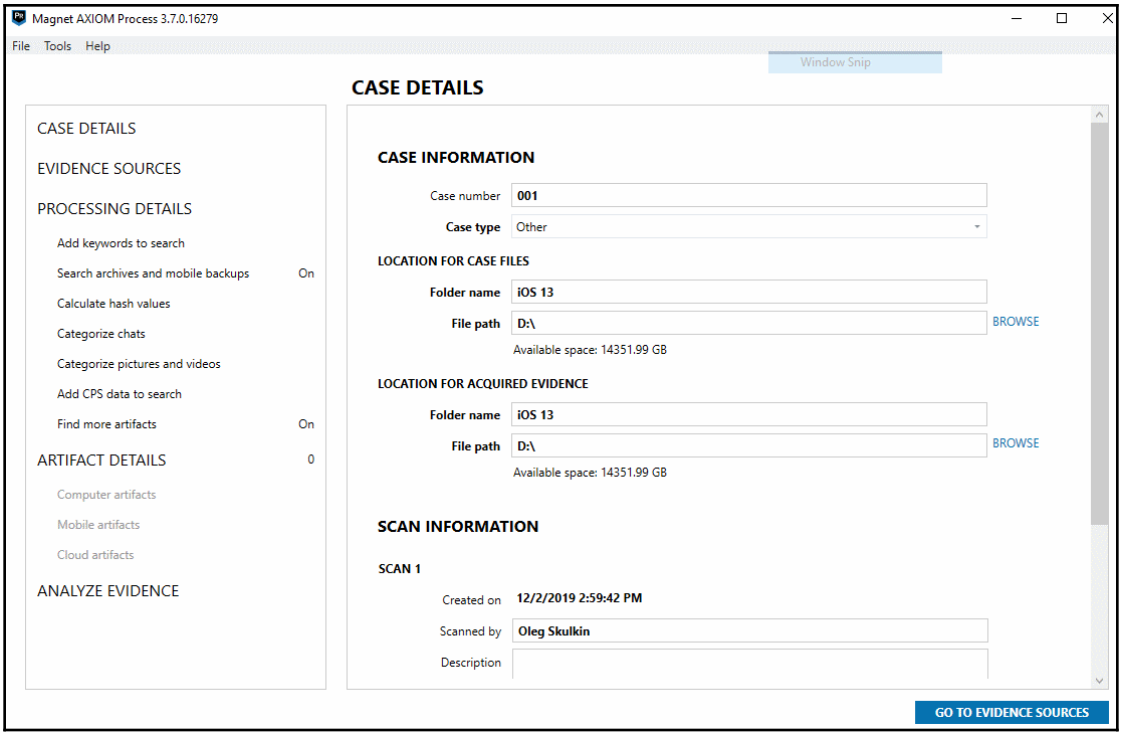

SQLite wizard
Select database
AppleDevice_AdvancedLogical
Table Search
Decoded by
Application
Row co
Name
Path
Size (byte
Created
Modified
(3*) 145 VPNMaster 0 rmq2.sqlite Oleg's iPhone/Applications/co.allconnected... 20480 7/30/2017 7:26:56 AM(UTC+0) 7/30/2017 7:26:56 AM(U
146 YandexTransp... 4 routing.db 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(
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(
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(U
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(U
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(U
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(
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(
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(
Total: 173 Deduplication: 4 Items: 169/169 Selected: 169 Path: Oleg's iPhone/Applications/com.qrcodecity.scan/Documents/Scan.sqlite
Close
Next

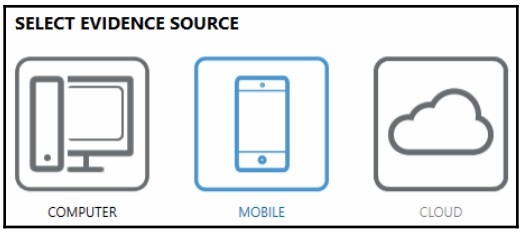

SQLite wizard
Use this tool to decode additional data from databases. Build queries
to map database fields to UFED Physical Analyzer models.
To learn more about this tool, click here
Application
Scan
Name
Scan
Include deleted rows
Note: Including deleted data increases the chances of false positive records.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

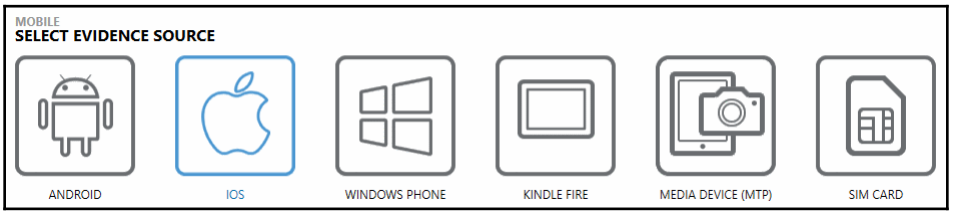

SQLite wizard
Double-click or drag the database tables to the work area and link database fields.
Query builder
DB viewer
main
ZSCSCANEVENT
Z_METADATA
Z_MODELCACHE
Z_PRIMARYKEY
ZSCSCANEVENT (...
*
PA_IsDeleted
Z_PK integer
Z_ENT integer
Z_OPT integer
ZDELETED
Visible
Expression
Column Name
Sort Type
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

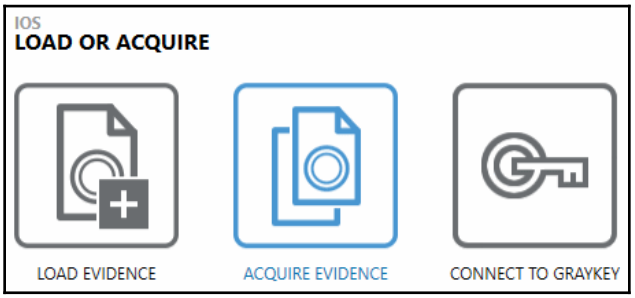

SQLite wizard
Select a timestamp global format
6/11/1983 8:00:00 PM
Seconds from UTC 1970
1/5/1970 9:50:09 PM
Milliseconds from UTC 1970
6/11/2014 8:00:00 PM
Seconds from UTC 2001 (iPhone) (Suggested)
6/11/1614 8:00:00 PM
Seconds from UTC 1601
1/5/1601 9:50:09 PM
Milliseconds from UTC 1601
1/1/1601 12:07:04 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

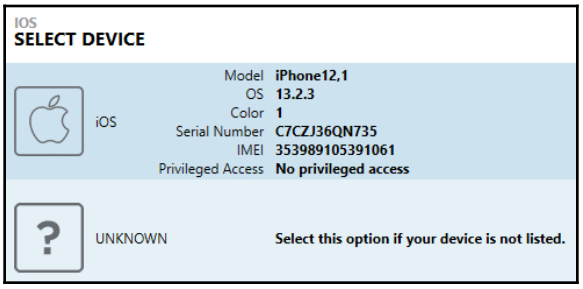

SQLite wizard
Select an existing UFED Physical Analyzer or generic model
Generic model
Drag field types to the columns you want to map in the table below
Field 4 Text
Field 5 Text
Field 6 Text
Field 7 Text
Field 8 Text
Field 9 Text
Field 10 Text
Timestamp 2 Date
Timestamp 3 Date
Deleted Enumeration
Preview 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

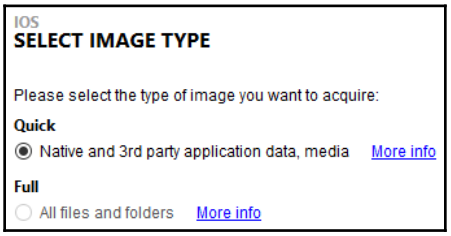

Magnet AXIOM Process 3.7.0.16279
File Tools Help
Window Snip
CASE DETAILS
CASE DETAILS
EVIDENCE SOURCES
PROCESSING DETAILS
Add keywords to search
Search archives and mobile backups On
Calculate hash values
Categorize chats
Categorize pictures and videos
Add CPS data to search
Find more artifacts On
ARTIFACT DETAILS 0
Computer artifacts
Mobile artifacts
Cloud artifacts
ANALYZE EVIDENCE
CASE INFORMATION
Case number 001
Case type Other
LOCATION FOR CASE FILES
Folder name iOS 13
File path D:\ BROWSE
Available space: 14351.99 GB
LOCATION FOR ACQUIRED EVIDENCE
Folder name iOS 13
File path D:\ BROWSE
Available space: 14351.99 GB
SCAN INFORMATION
SCAN 1
Created on 12/2/2019 2:59:42 PM
Scanned by Oleg Skulkin
Description
GO TO EVIDENCE SOURCES

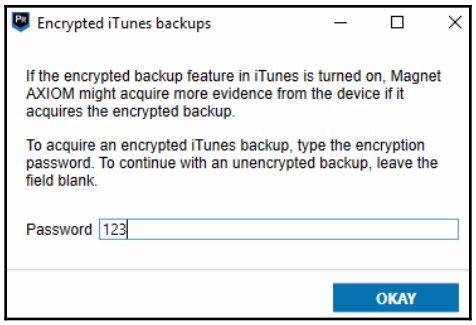

SELECT EVIDENCE SOURCE
COMPUTER
MOBILE
CLOUD

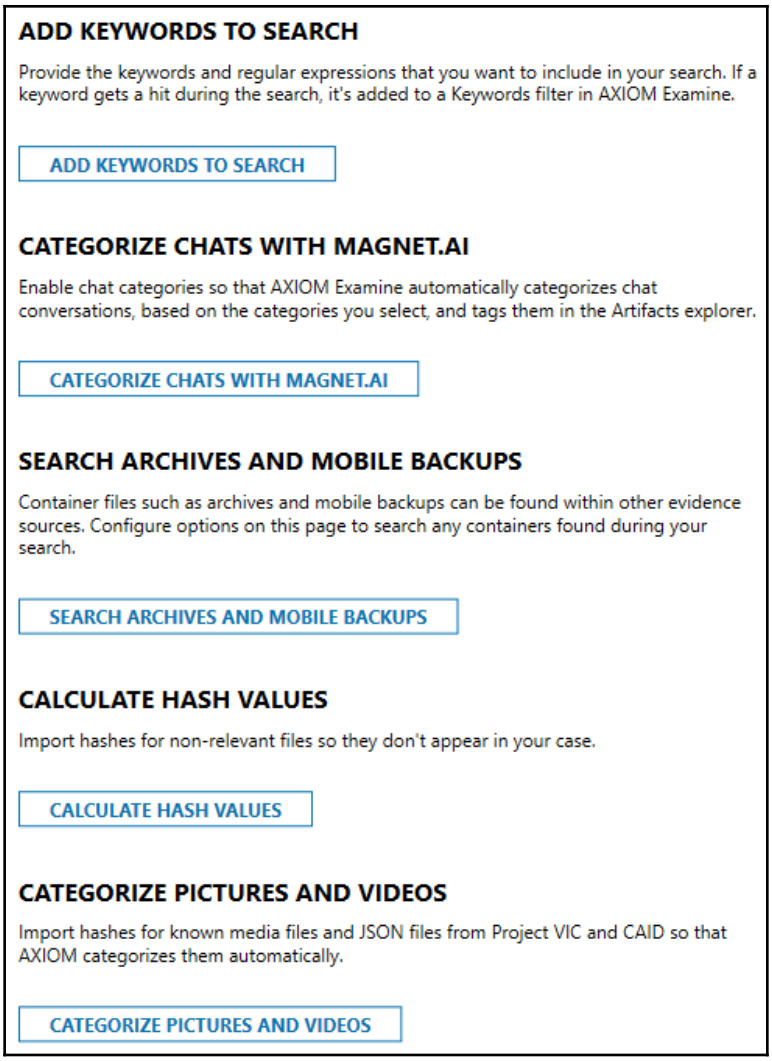

MOBILE
SELECT EVIDENCE SOURCE
ANDROID
IOS
WINDOWS PHONE
KINDLE FIRE
MEDIA DEVICE (MTP)
SIM CARD

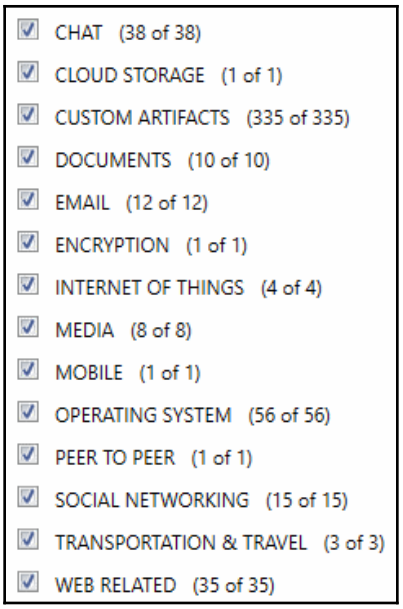

IOS
LOAD OR ACQUIRE
LOAD EVIDENCE
ACQUIRE EVIDENCE
CONNECT TO GRAYKEY

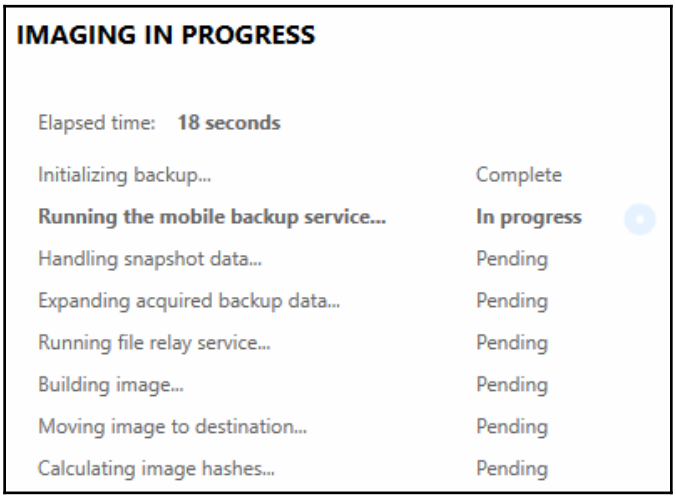

IOS
SELECT DEVICE
iOS
Model iPhone12,1
OS 13.2.3
Color 1
Serial Number C7CZJ36QN735
IMEI 353989105391061
Privileged Access No privileged access
UNKNOWN
Select this option if your device is not listed.

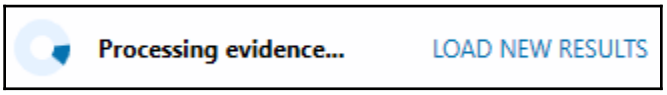

IOS
SELECT IMAGE TYPE
Please select the type of image you want to acquire:
Quick
Native and 3rd party application data, media
More info
Full
All files and folders
More info

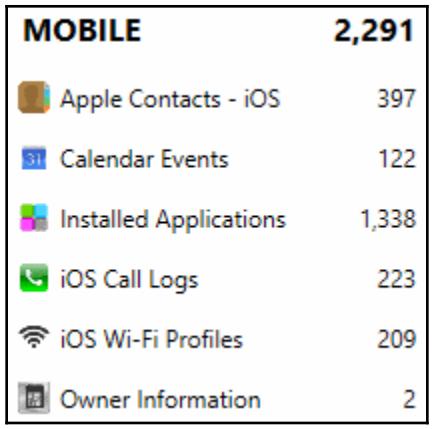

Encrypted iTunes backups
If the encrypted backup feature in iTunes is turned on, Magnet AXIOM might acquire more evidence from the device if it acquires the encrypted backup.
To acquire an encrypted iTunes backup, type the encryption password. To continue with an unencrypted backup, leave the field blank.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

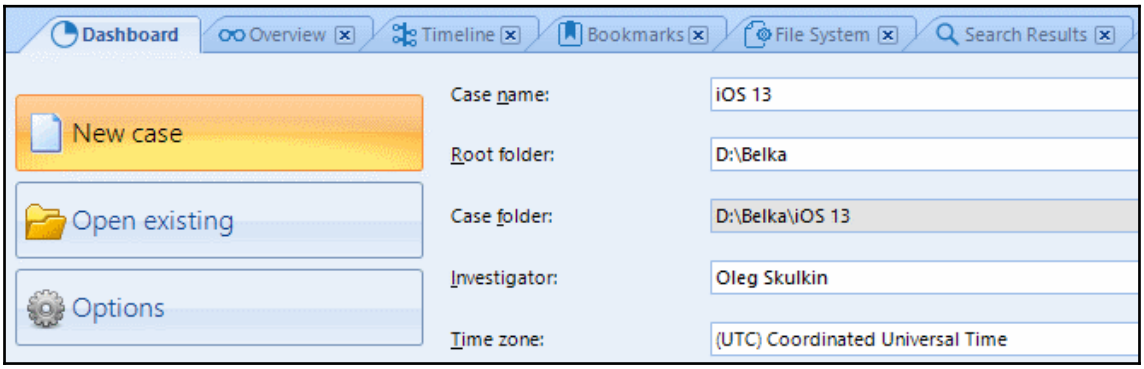

ADD KEYWORDS TO SEARCH
Provide the keywords and regular expressions that you want to include in your search. If a keyword gets a hit during the search, it's added to a Keywords filter in AXIOM Examine.
ADD KEYWORDS TO SEARCH
CATEGORIZE CHATS WITH MAGNET.AI
Enable chat categories so that AXIOM Examine automatically categorizes chat conversations, based on the categories you select, and tags them in the Artifacts explorer.
CATEGORIZE CHATS WITH MAGNET.AI
SEARCH ARCHIVES AND MOBILE BACKUPS
Container files such as archives and mobile backups can be found within other evidence sources. Configure options on this page to search any containers found during your search.
SEARCH ARCHIVES AND MOBILE BACKUPS
CALCULATE HASH VALUES
Import hashes for non-relevant files so they don't appear in your case.
CALCULATE HASH VALUES
CATEGORIZE PICTURES AND VIDEOS
Import hashes for known media files and JSON files from Project VIC and CAID so that AXIOM categorizes them automatically.
CATEGORIZE PICTURES AND VIDEOS

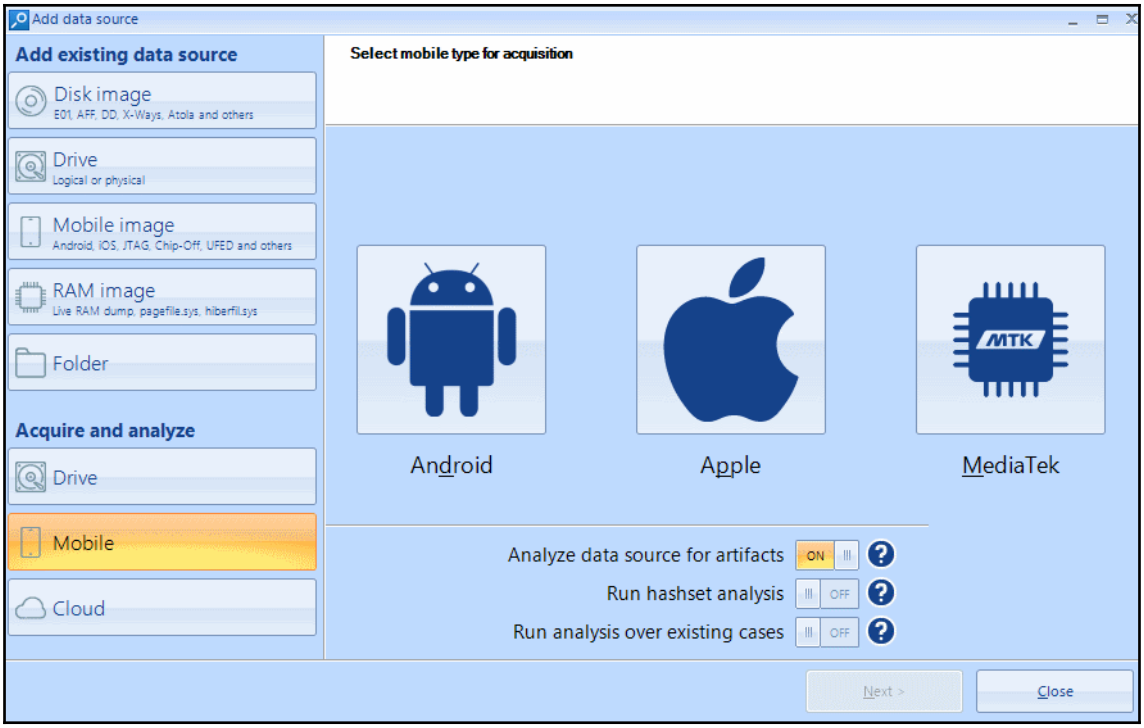

CHAT (38 of 38)
CLOUD STORAGE (1 of 1)
CUSTOM ARTIFACTS (335 of 335)
DOCUMENTS (10 of 10)
EMAIL (12 of 12)
ENCRYPTION (1 of 1)
INTERNET OF THINGS (4 of 4)
MEDIA (8 of 8)
MOBILE (1 of 1)
OPERATING SYSTEM (56 of 56)
PEER TO PEER (1 of 1)
SOCIAL NETWORKING (15 of 15)
TRANSPORTATION & TRAVEL (3 of 3)
WEB RELATED (35 of 35)

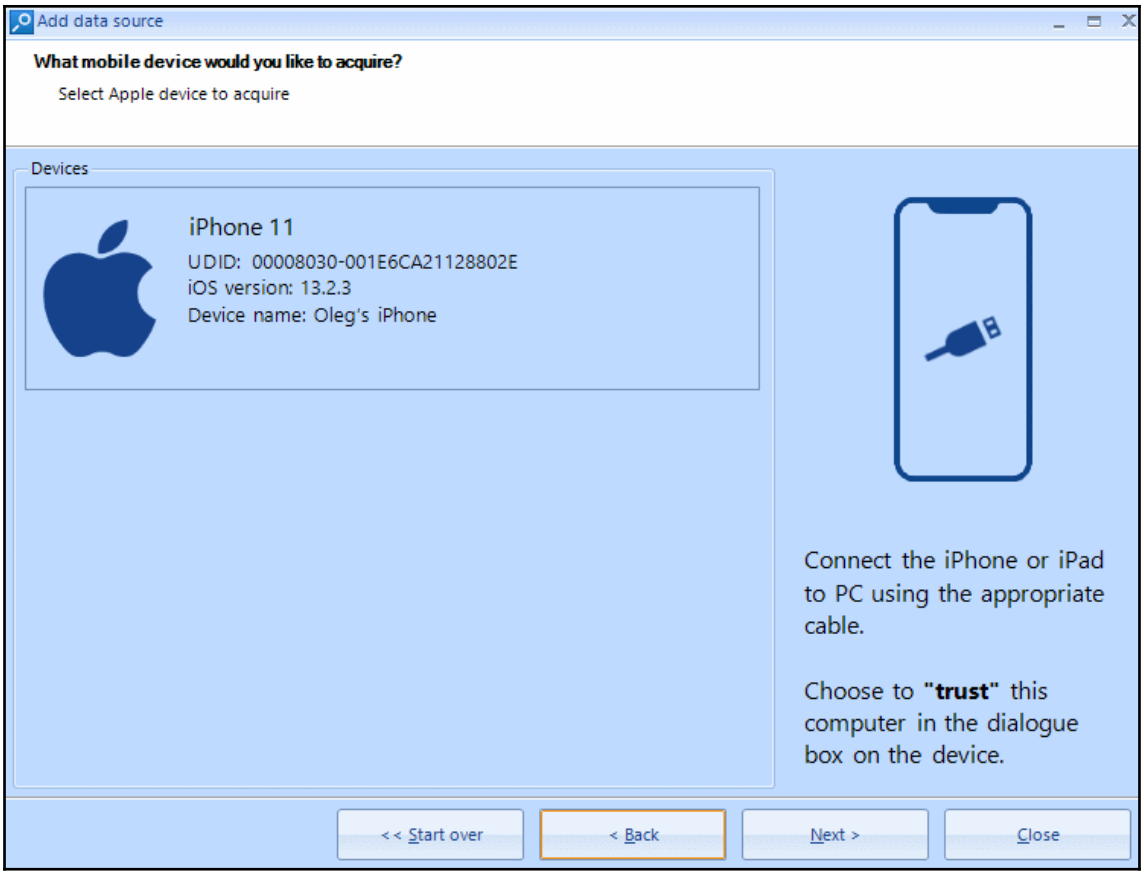

IMAGING IN PROGRESS
Elapsed time: 18 seconds
Initializing backup... Complete
Running the mobile backup service... In progress
Handling snapshot data... Pending
Expanding acquired backup data... Pending
Running file relay service... Pending
Building image... Pending
Moving image to destination... Pending
Calculating image hashes... Pending

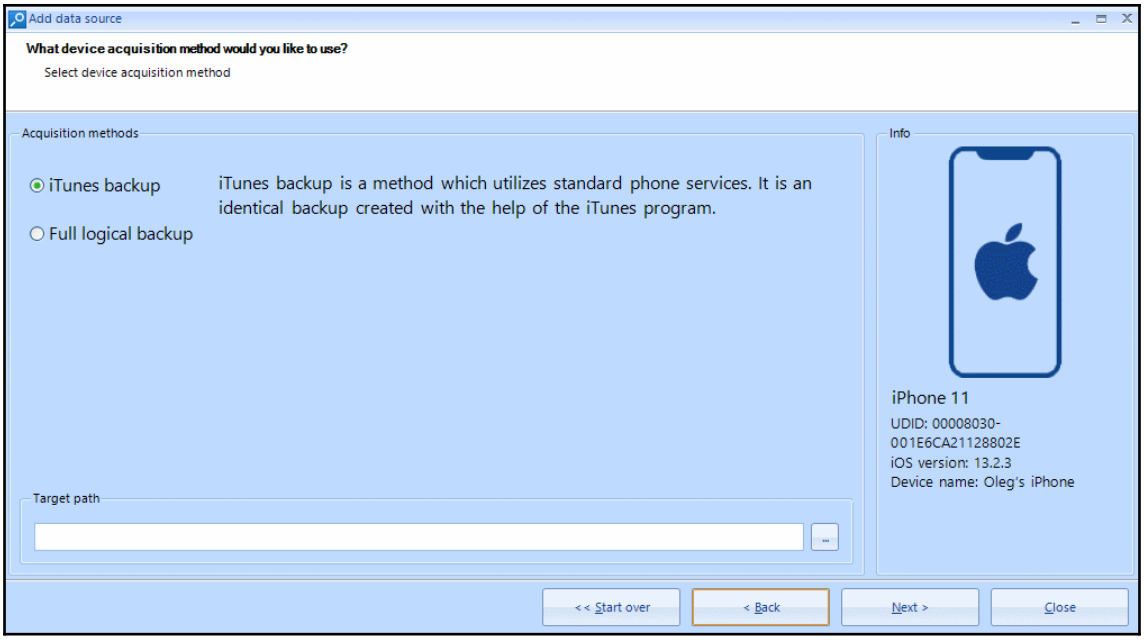

Processing evidence...
LOAD NEW RESULTS

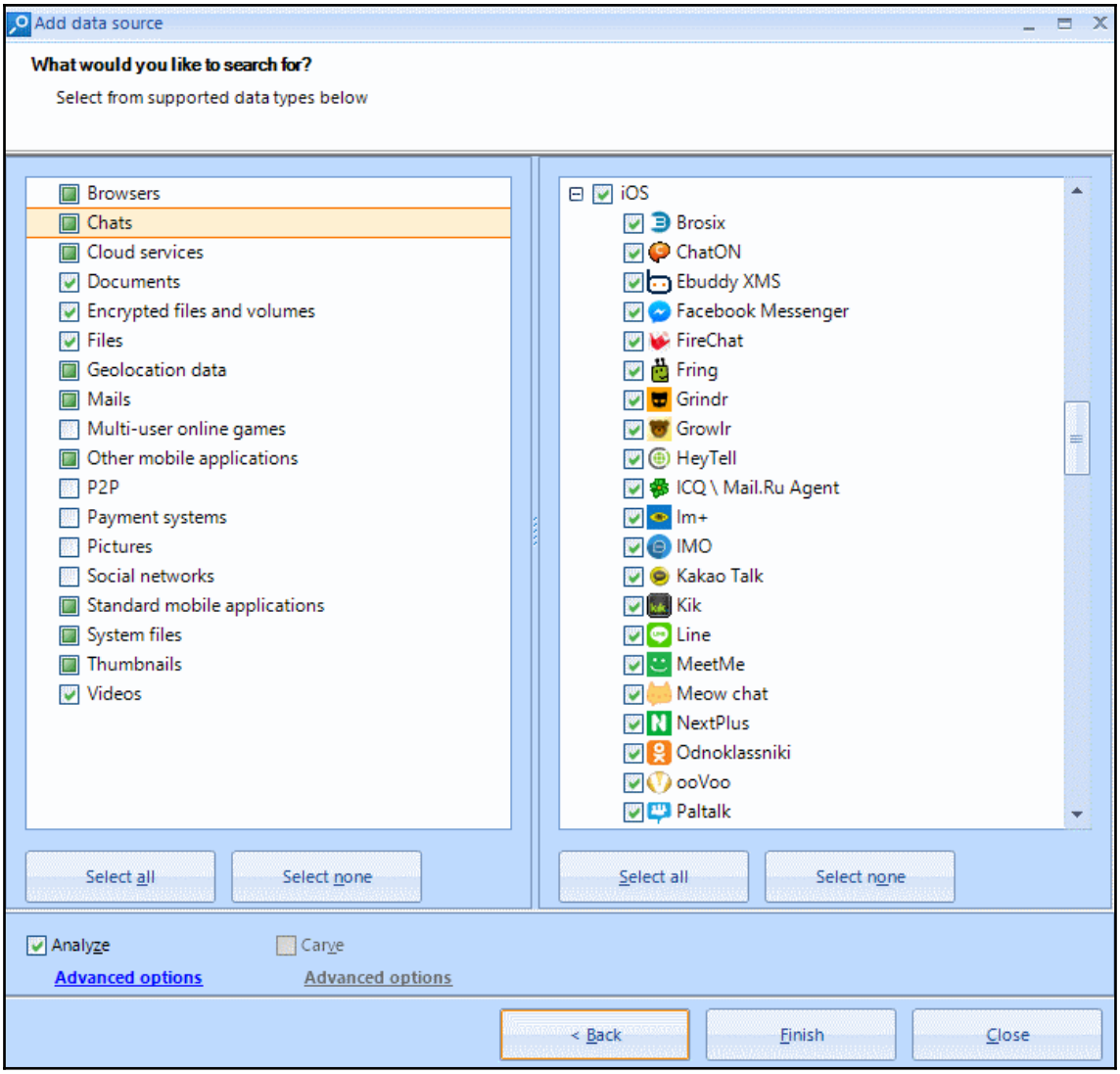

MOBILE 2,291
Apple Contacts - iOS 397
Calendar Events 122
Installed Applications 1,338
iOS Call Logs 223
iOS Wi-Fi Profiles 209
Owner Information 2

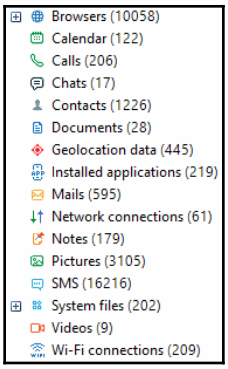

Dashboard
Overview
Timeline
Bookmarks
File System
Search Results
New case
Open existing
Options
Case name: iOS 13
Root folder: D:\Belka
Case folder: D:\Belka\iOS 13
Investigator: Oleg Skulkin
Time zone: (UTC) Coordinated Universal Time

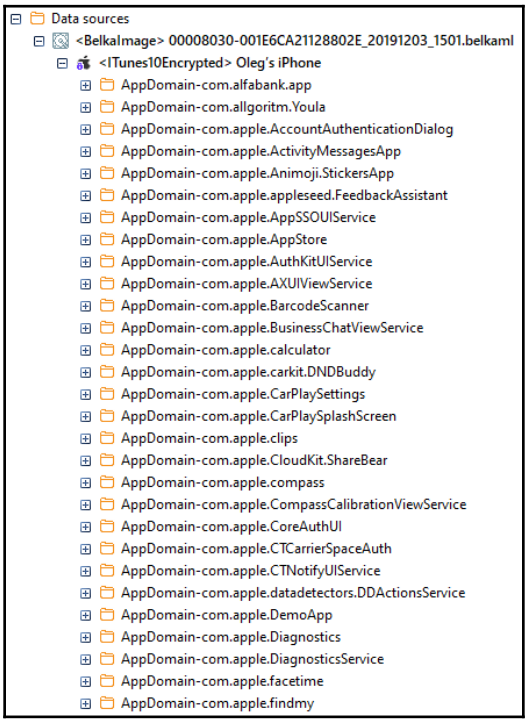

Add data source
Add existing data source
Disk image
E01, AFF, DD, X-Ways, Atola and others
Drive
Logical or physical
Mobile image
Android, iOS, JTAG, Chip-Off, UFED and others
RAM image
Live RAM dump, pagefile.sys, hiberfil.sys
Folder
Acquire and analyze
Drive
Mobile
Cloud
Select mobile type for acquisition
Android
Apple
MediaTek
Analyze data source for artifacts
ON
Run hashset analysis
OFF
Run analysis over existing cases
OFF
Next >
Close

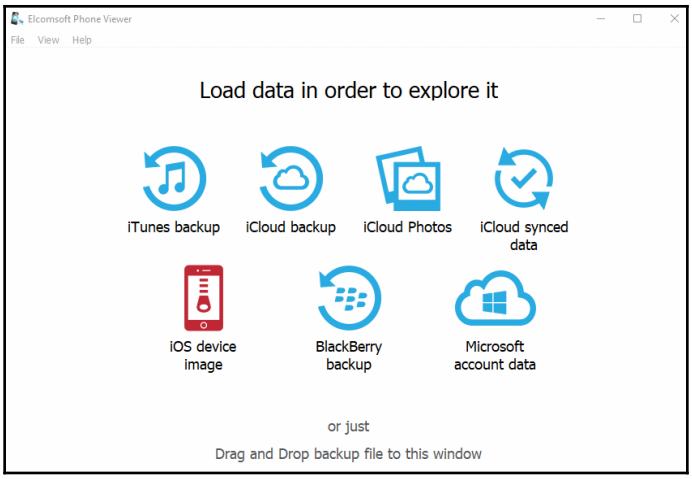

Add data source
What mobile device would you like to acquire?
Select Apple device to acquire
Devices
iPhone 11
UDID: 00008030-001E6CA21128802E
iOS version: 13.2.3
Device name: Oleg's iPhone
Connect the iPhone or iPad to PC using the appropriate cable.
Choose to "trust" this computer in the dialogue box on the device.
<< Start over
< Back
Next >
Close

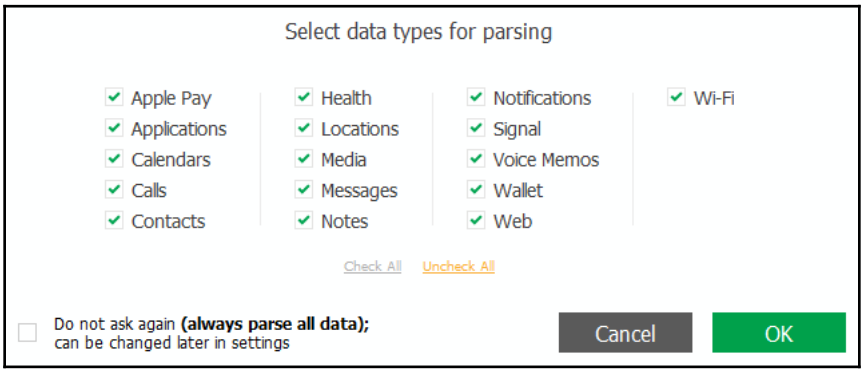

Add data source
What device acquisition method would you like to use?
Select device acquisition method
Acquisition methods
iTunes backup
Full logical backup
iTunes backup is a method which utilizes standard phone services. It is an identical backup created with the help of the iTunes program.
Target path
Info
iPhone 11
UDID: 00008030-001E6CA21128802E
iOS version: 13.2.3
Device name: Oleg's iPhone
<< Start over
< Back
Next >
Close

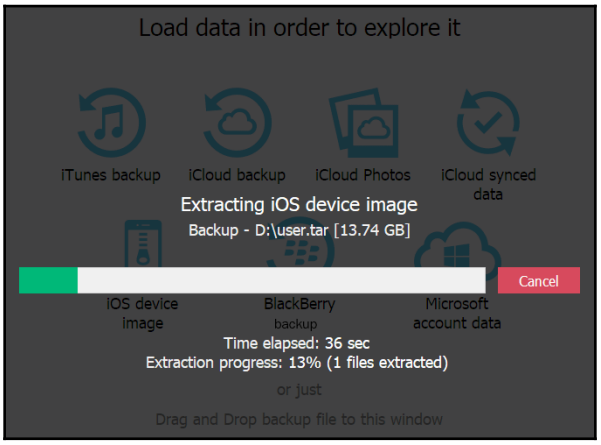

Add data source
What would you like to search for?
Select from supported data types below
Browsers
Chats
Cloud services
Documents
Encrypted files and volumes
Files
Geolocation data
Mails
Multi-user online games
Other mobile applications
P2P
Payment systems
Pictures
Social networks
Standard mobile applications
System files
Thumbnails
Videos
Select all
Select none
iOS
Brosix
ChatON
Ebuddy XMS
Facebook Messenger
FireChat
Fring
Grindr
Growlr
HeyTell
ICQ \ Mail.Ru Agent
Im+
IMO
Kakao Talk
Kik
Line
MeetMe
Meow chat
NextPlus
Odnoklassniki
ooVoo
Paltalk
Select all
Select none
Analyze
Advanced options
Carve
Advanced options
< Back
Finish
Close

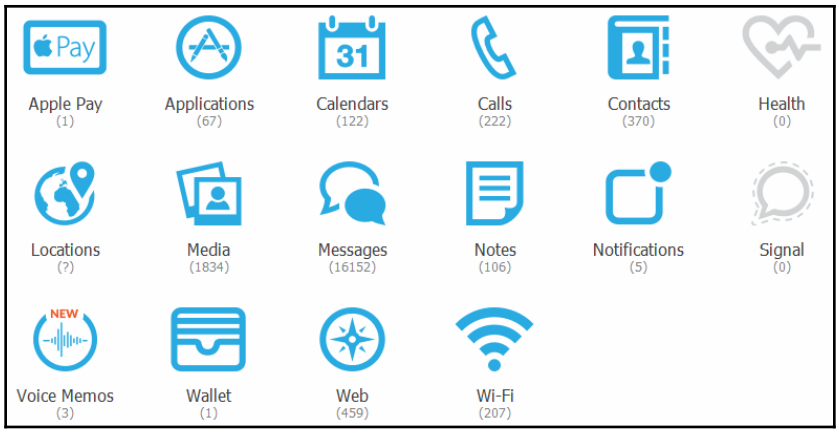

Browsers (10058)
Calendar (122)
Calls (206)
Chats (17)
Contacts (1226)
Documents (28)
Geolocation data (445)
Installed applications (219)
Mails (595)
Network connections (61)
Notes (179)
Pictures (3105)
SMS (16216)
System files (202)
Videos (9)
Wi-Fi connections (209)


Data sources
<BelkaImage> 00008030-001E6CA21128802E_20191203_1501.belkaml
<ITunes10Encrypted> Oleg's iPhone
AppDomain-com.alfabank.app
AppDomain-com.allgoritm.Youla
AppDomain-com.apple.AccountAuthenticationDialog
AppDomain-com.apple.ActivityMessagesApp
AppDomain-com.apple.Animoji.StickersApp
AppDomain-com.apple.appleseed.FeedbackAssistant
AppDomain-com.apple.AppSSOUIService
AppDomain-com.apple.AppStore
AppDomain-com.apple.AuthKitUIService
AppDomain-com.apple.AXUIViewService
AppDomain-com.apple.BarcodeScanner
AppDomain-com.apple.BusinessChatViewService
AppDomain-com.apple.calculator
AppDomain-com.apple.carkit.DNDBuddy
AppDomain-com.apple.CarPlaySettings
AppDomain-com.apple.CarPlaySplashScreen
AppDomain-com.apple.clips
AppDomain-com.apple.CloudKit.ShareBear
AppDomain-com.apple.compass
AppDomain-com.apple.CompassCalibrationViewService
AppDomain-com.apple.CoreAuthUI
AppDomain-com.apple.CTCarrierSpaceAuth
AppDomain-com.apple.CTNotifyUIService
AppDomain-com.apple.datadetectors.DDActionsService
AppDomain-com.apple.DemoApp
AppDomain-com.apple.Diagnostics
AppDomain-com.apple.DiagnosticsService
AppDomain-com.apple.facetime
AppDomain-com.apple.findmy

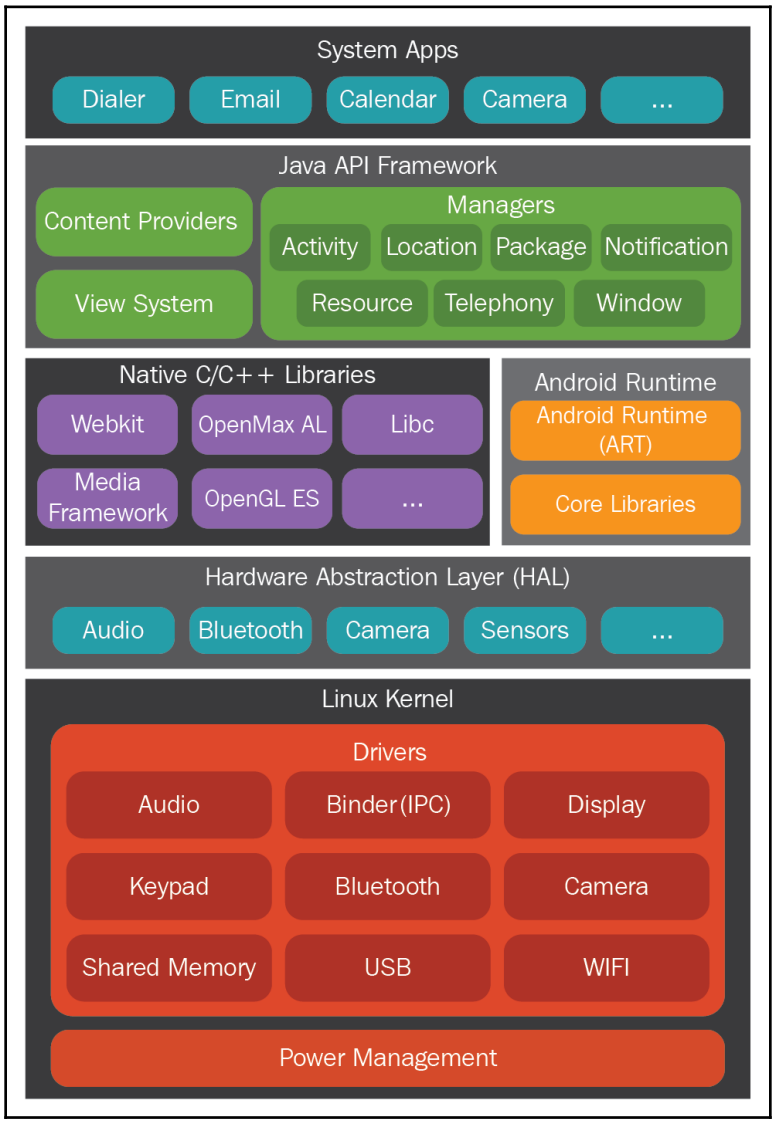

Elcomsoft Phone Viewer
File View Help
Load data in order to explore it
iTunes backup
iCloud backup
iCloud Photos
iCloud synced data
iOS device image
BlackBerry backup
Microsoft account data
or just
Drag and Drop backup file to this window

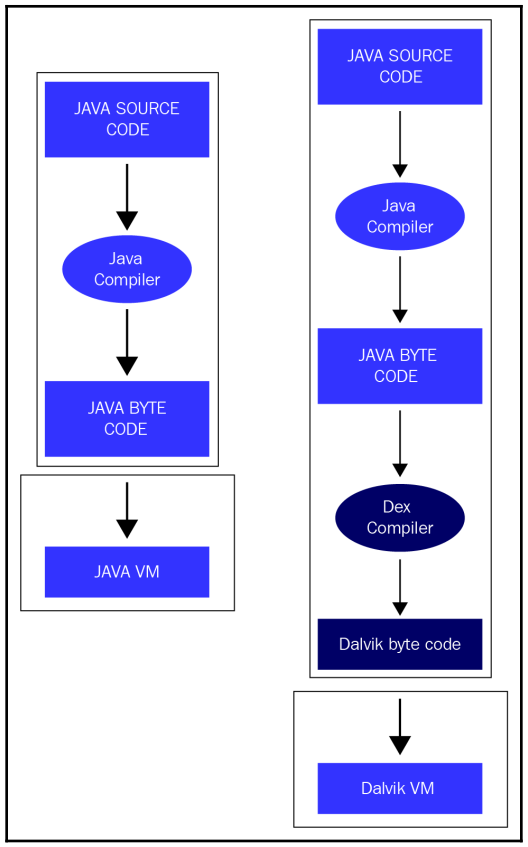

Select data types for parsing
Apple Pay
Applications
Calendars
Calls
Contacts
Health
Locations
Media
Messages
Notes
Notifications
Signal
Voice Memos
Wallet
Web
Wi-Fi
Check All
Uncheck All
Do not ask again (always parse all data);
can be changed later in settings
Cancel
OK

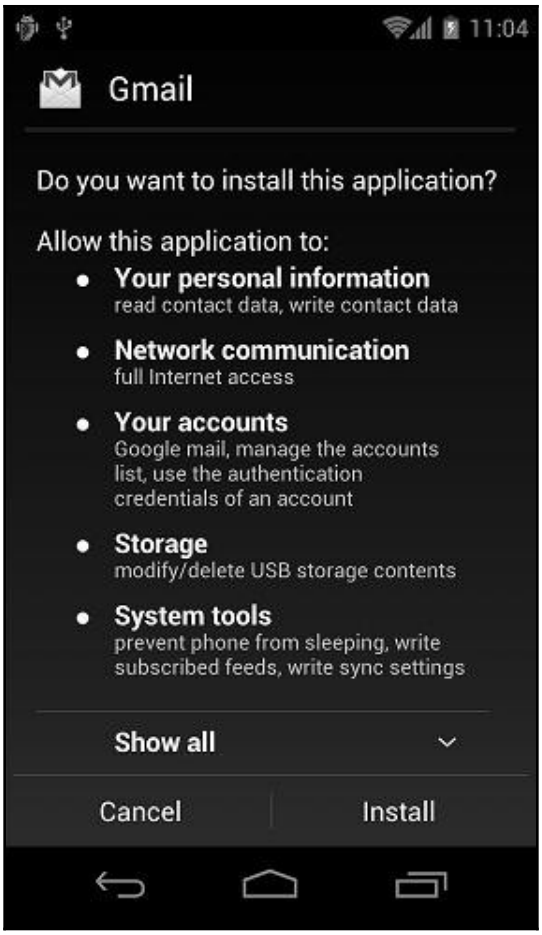

Load data in order to explore it
iTunes backup
iCloud backup
iCloud Photos
iCloud synced data
Extracting iOS device image
Backup - D:\user.tar [13.74 GB]
Cancel
iOS device image
BlackBerry backup
Microsoft account data
Time elapsed: 36 sec
Extraction progress: 13% (1 files extracted)
or just
Drag and Drop backup file to this window

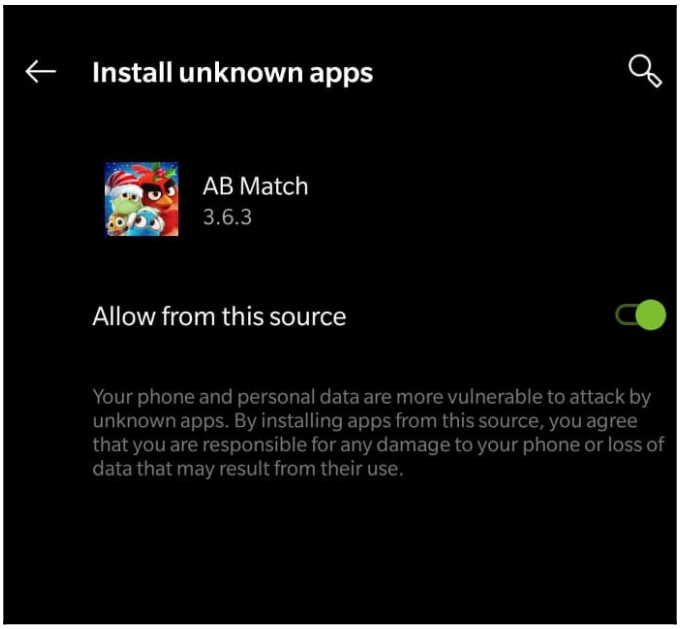

Apple Pay
(1)
Applications
(67)
Calendars
(122)
Calls
(222)
Contacts
(370)
Health
(0)
Locations
(?)
Media
(1834)
Messages
(16152)
Notes
(106)
Notifications
(5)
Signal
(0)
NEW
Voice Memos
(3)
Wallet
(1)
Web
(459)
Wi-Fi
(207)

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
```

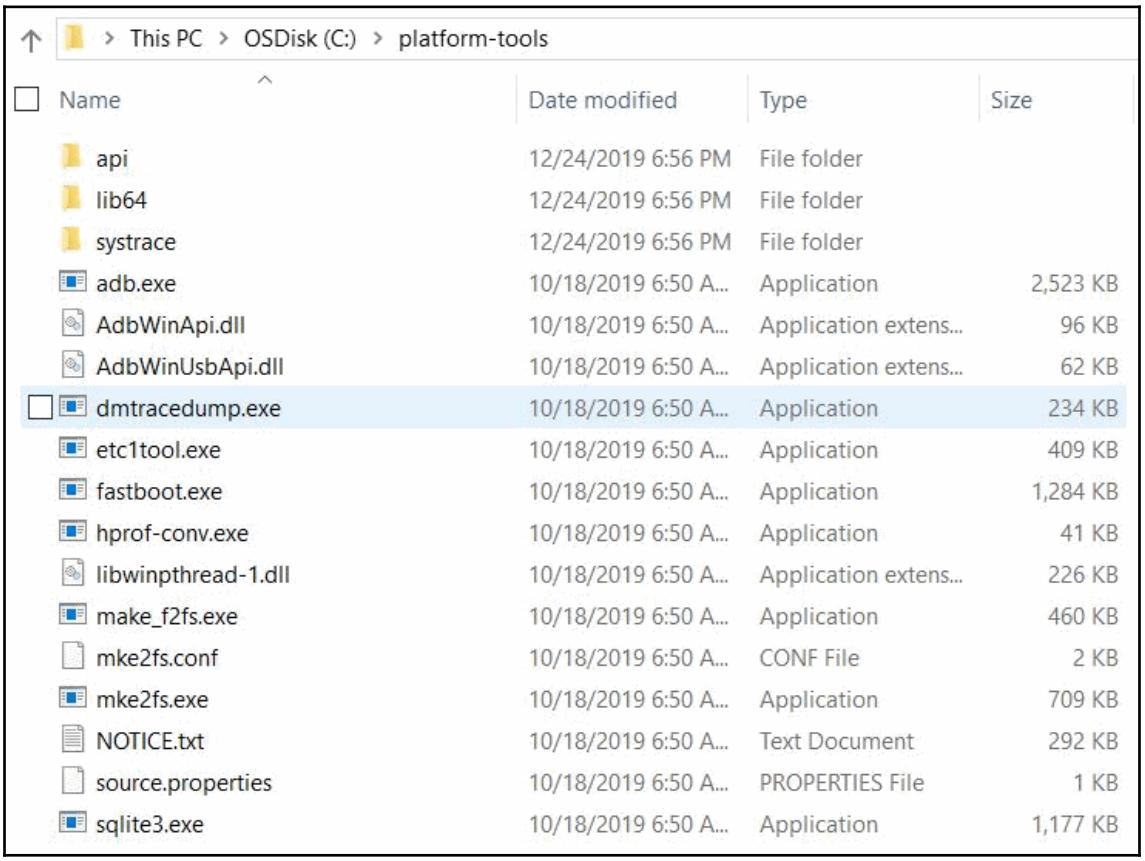
```
root@android:/ # mount
rootfs / rootfs ro,relatime 0 0
tmpfs /dev tmpfs rw,nosuid,relatime,mode=755 0 0
devpts /dev/pts devpts rw,relatime,mode=600 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,relatime 0 0
none /acct cgroup rw,relatime,cpuacct 0 0
tmpfs /mnt/asec tmpfs rw,relatime,mode=755,gid=1000 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
```

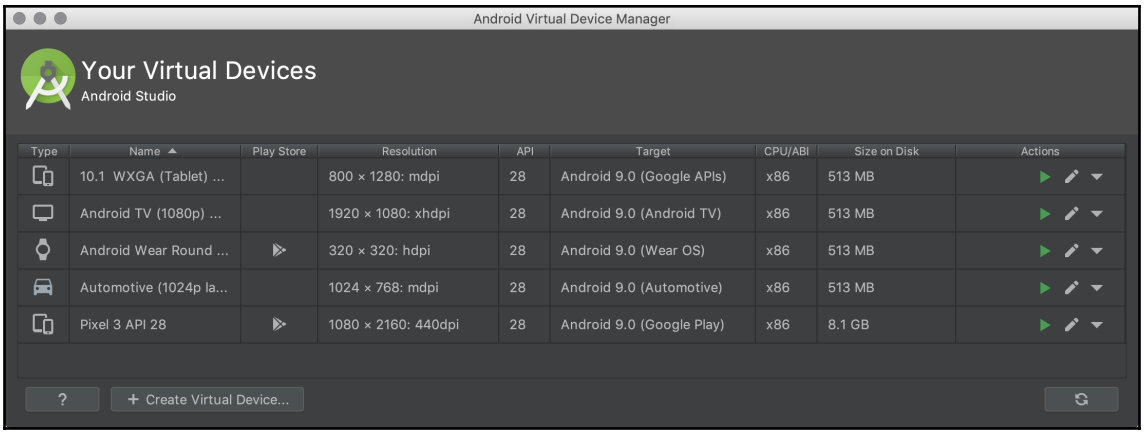
```
root@android:/ # cd sdcard
root@android:/sdcard # mount
rootfs / rootfs ro,relatime 0 0
tmpfs /dev tmpfs rw,nosuid,relatime,mode=755 0 0
devpts /dev/pts devpts rw,relatime,mode=600 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,relatime 0 0
none /acct cgroup rw,relatime,cpuacct 0 0
tmpfs /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
```

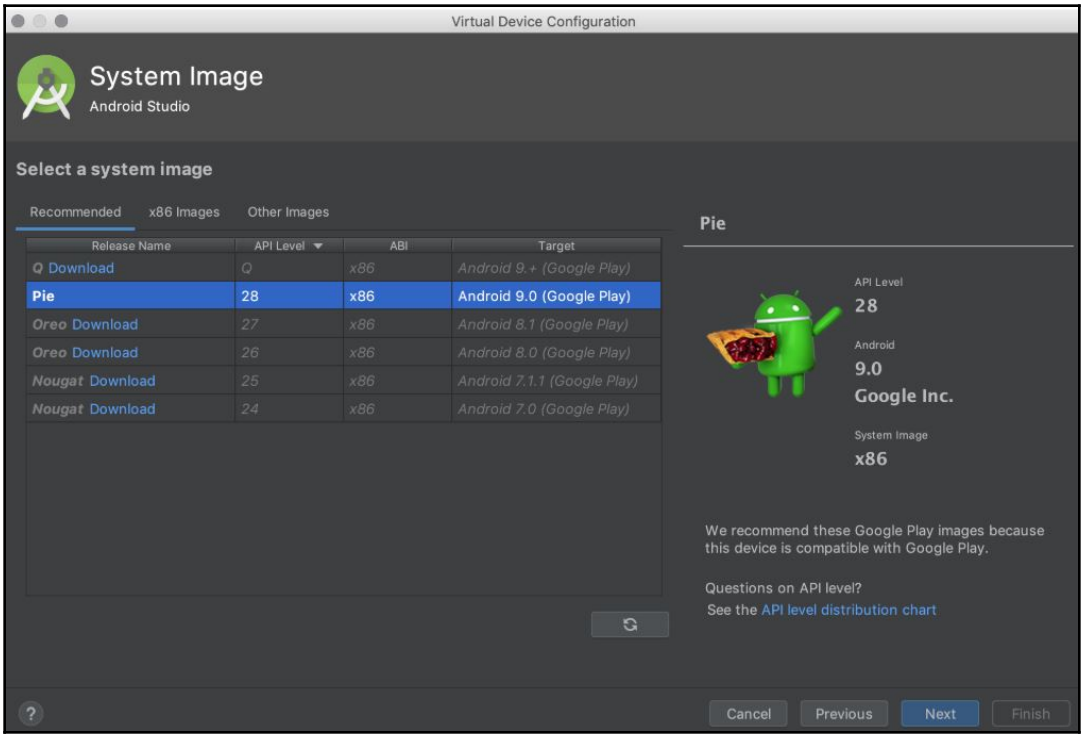
```
root@android:/ # cd /sys
root@android:/sys # ls
block
bus
class
dev
devices
firmware
fs
kernel
module
power
```

```
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]
```

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

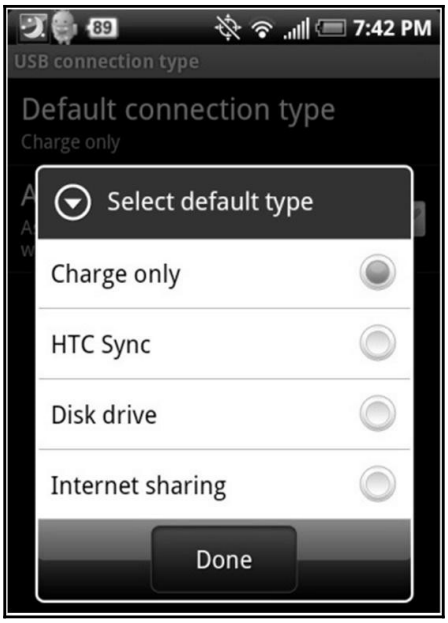


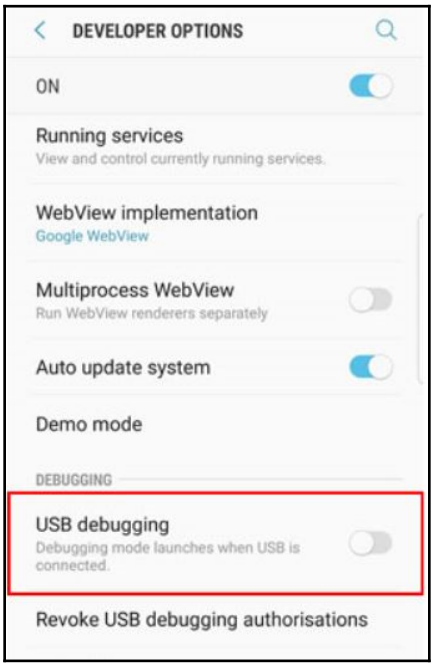

Android Virtual Device Manager
Your Virtual Devices
Android Studio
Type
Name
Play Store
Resolution
API
Target
CPU/ABI
Size on Disk
Actions
10.1 WXGA (Tablet) ...
800 × 1280: mdpi
28
Android 9.0 (Google APIs)
x86
513 MB
Android TV (1080p) ...
1920 × 1080: xhdpi
28
Android 9.0 (Android TV)
x86
513 MB
Android Wear Round ...
320 × 320: hdpi
28
Android 9.0 (Wear OS)
x86
513 MB
Automotive (1024p la...
1024 × 768: mdpi
28
Android 9.0 (Automotive)
x86
513 MB
Pixel 3 API 28
1080 × 2160: 440dpi
28
Android 9.0 (Google Play)
x86
8.1 GB
?
+ Create Virtual Device...

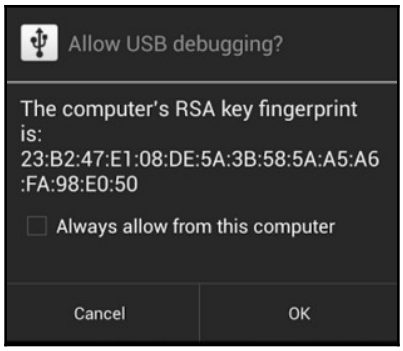

Virtual Device Configuration
System Image
Android Studio
Select a system image
Recommended
x86 Images
Other Images
Release Name
API Level
ABI
Target
Q Download
Q
x86
Android 9.+ (Google Play)
Pie
28
x86
Android 9.0 (Google Play)
Oreo Download
27
x86
Android 8.1 (Google Play)
Oreo Download
26
x86
Android 8.0 (Google Play)
Nougat Download
25
x86
Android 7.1.1 (Google Play)
Nougat Download
24
x86
Android 7.0 (Google Play)
Pie
API Level
28
Android
9.0
Google Inc.
System Image
x86
We recommend these Google Play images because this device is compatible with Google Play.
Questions on API level?
See the API level distribution chart
?
Cancel
Previous
Next
Finish


Android Emulator - Pixel_XL_API_28:5554
5:48
Friday, Aug 24


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

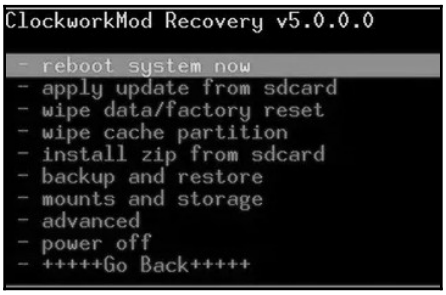

DEVELOPER OPTIONS
ON
Running services
View and control currently running services.
WebView implementation
Google WebView
Multiprocess WebView
Run WebView renderers separately
Auto update system
Demo mode
DEBUGGING
USB debugging
Debugging mode launches when USB is connected.
Revoke USB debugging authorisations



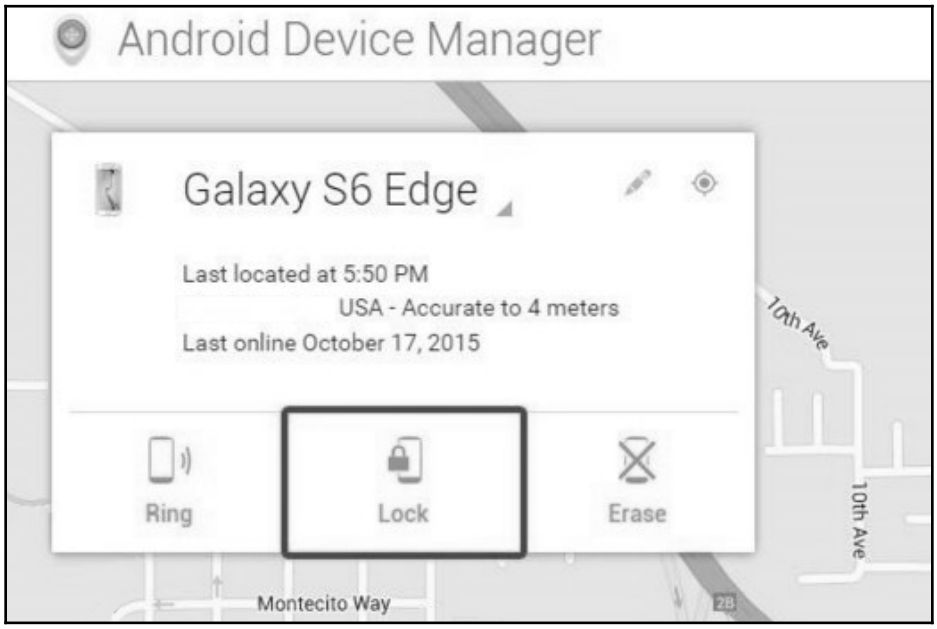

```
C:\android-sdk\platform-tools>adb.exe devices
List of devices attached
4df16ac3115e5f05        device
```

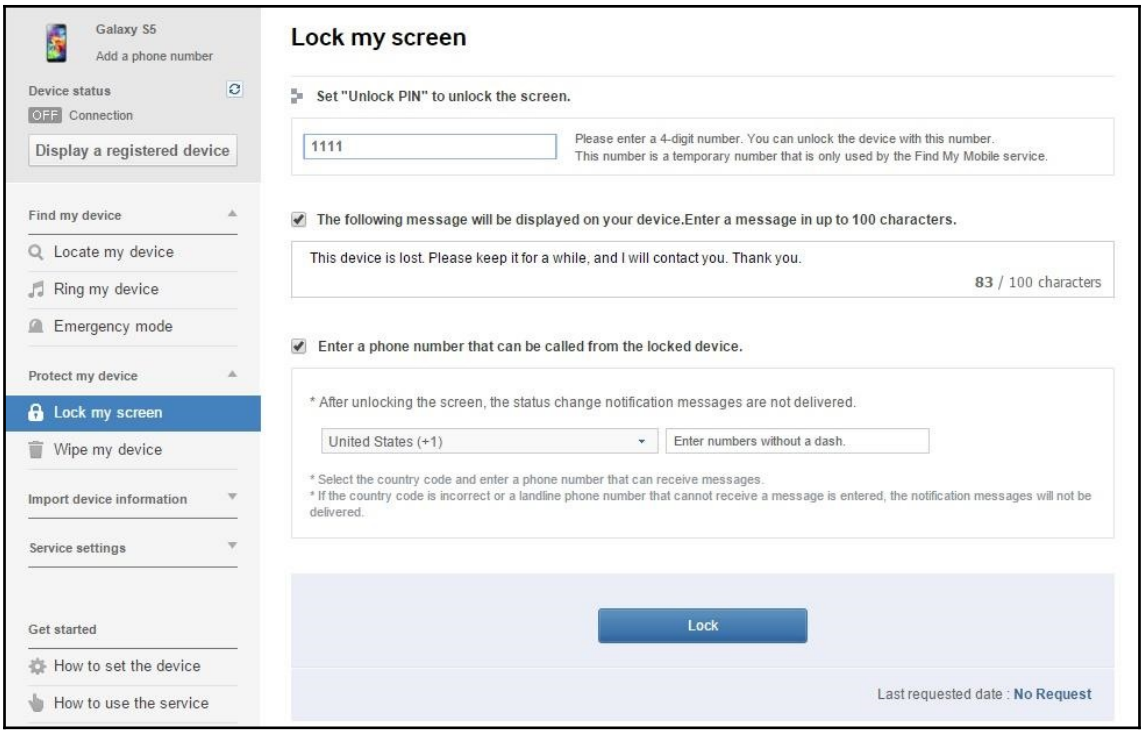
```
C:\android-sdk\platform-tools>adb.exe devices
List of devices attached
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
4df16ac3115e5f05        device
```

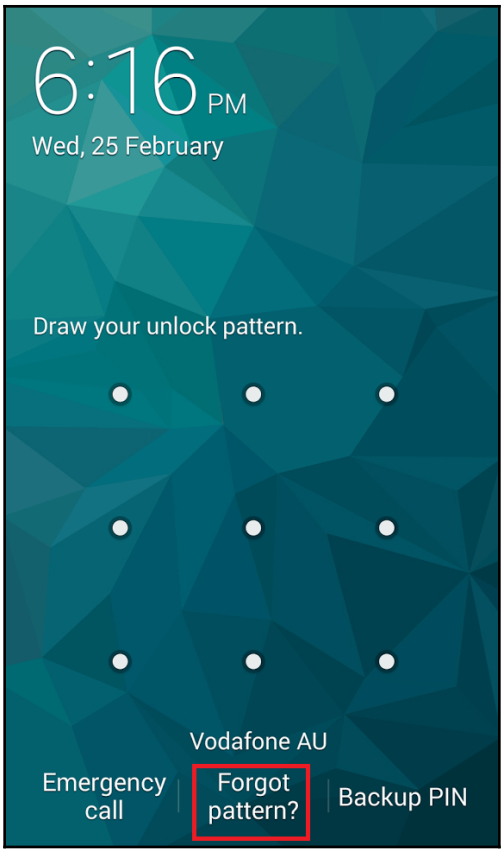
```
[redacted]:/ $ cd /data/data/com.android.providers.settings/databases
    sqlite3 settings.db
    update system set value=0 where name='lock_pattern_autolock';
c    update secure set value=0 where name='lock_pattern_autolock';
d /data/data/com.android.providers.settings/databases
    update system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

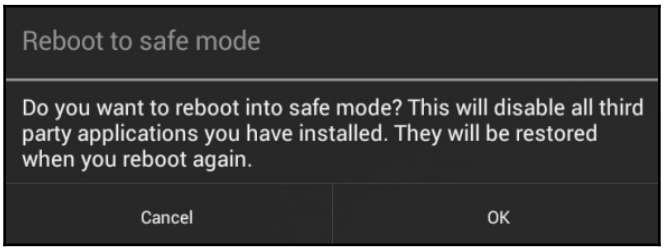


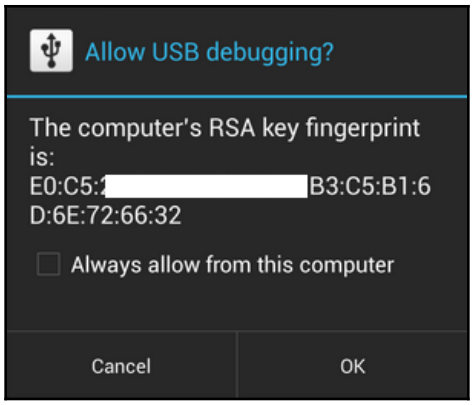
```
UFED User Lock Code Recovery Tool

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
```

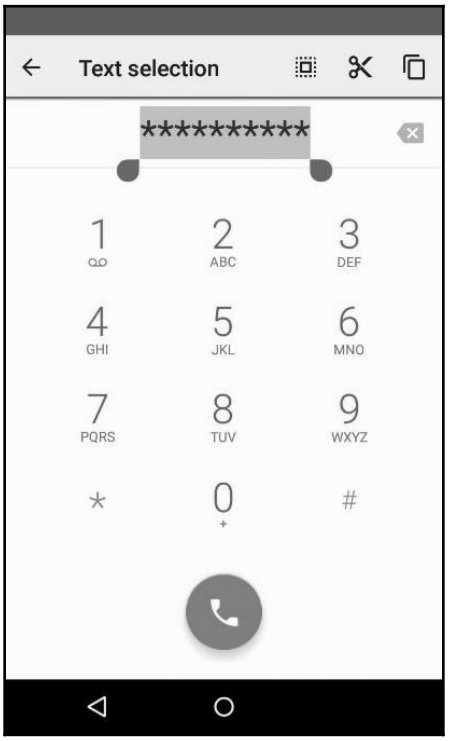


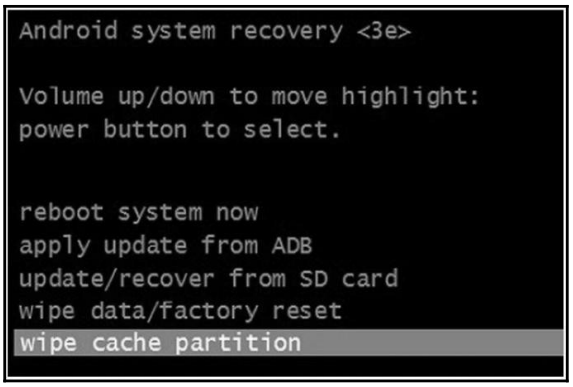

Galaxy S5
Add a phone number
Device status
OFF Connection
Display a registered device
Find my device
Locate my device
Ring my device
Emergency mode
Protect my device
Lock my screen
Wipe my device
Import device information
Service settings
Get started
How to set the device
How to use the service
Lock my screen
Set "Unlock PIN" to unlock the screen.
1111
Please enter a 4-digit number. You can unlock the device with this number.
This number is a temporary number that is only used by the Find My Mobile service.
The following message will be displayed on your device.Enter a message in up to 100 characters.
This device is lost. Please keep it for a while, and I will contact you. Thank you.
83 / 100 characters
Enter a phone number that can be called from the locked device.
* After unlocking the screen, the status change notification messages are not delivered.
United States (+1)
Enter numbers without a dash.
* Select the country code and enter a phone number that can receive messages.
* If the country code is incorrect or a landline phone number that cannot receive a message is entered, the notification messages will not be delivered.
Lock
Last requested date : No Request

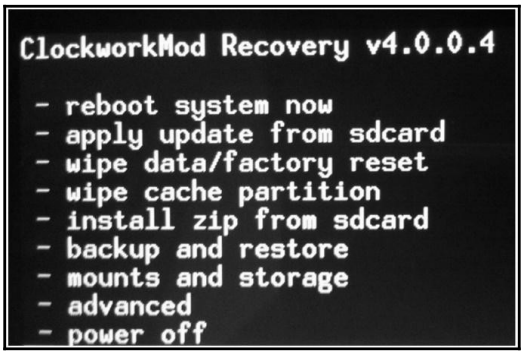

6:16 PM
Wed, 25 February
Draw your unlock pattern.
Vodafone AU
Emergency call
Forgot pattern?
Backup PIN

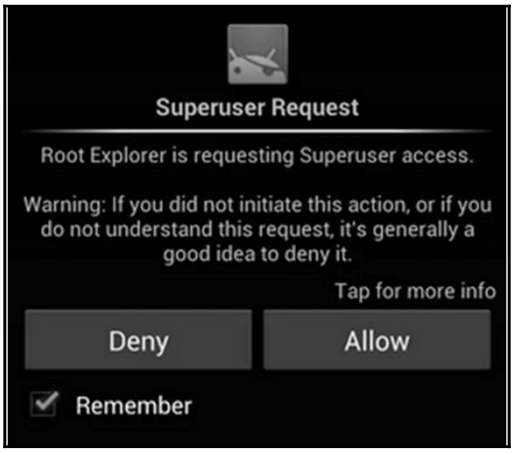

Reboot to safe mode
Do you want to reboot into safe mode? This will disable all third party applications you have installed. They will be restored when you reboot again.
Cancel
OK


Allow USB debugging?
The computer's RSA key fingerprint is:
E0:C5:2 B3:C5:B1:6
D:6E:72:66:32
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

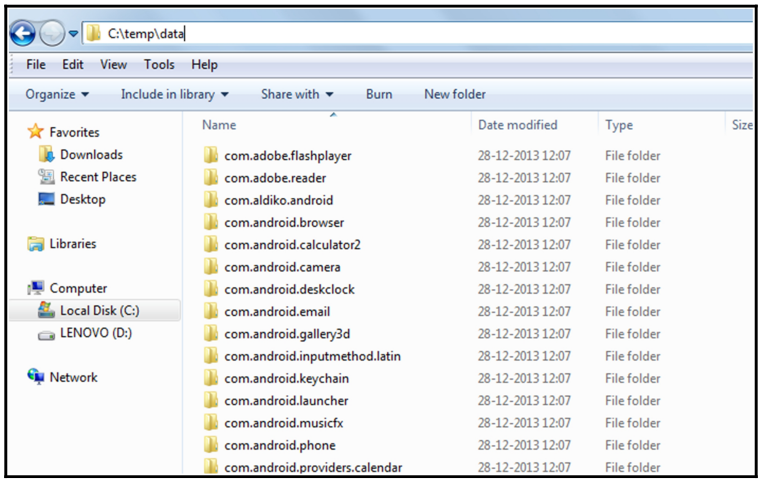

Superuser Request
Root Explorer is requesting Superuser access.
Warning: If you did not initiate this action, or if you do not understand this request, it's generally a good idea to deny it.
Tap for more info
Deny
Allow
Remember

```
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 $
```

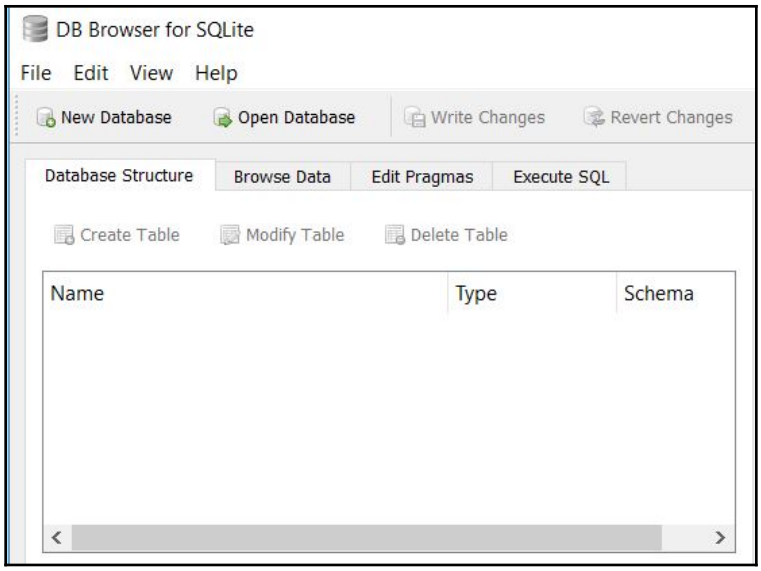
```
C:\android-sdk\platform-tools>adb.exe shell
root@android:/ # cd /data/data
root@android:/data/data # ls
android.googleSearch.googleSearchWidget
com.android.MtpApplication
com.android.Preconfig
com.android.apps.tag
com.android.backupconfirm
com.android.bluetooth
com.android.browser
```

Chapter 9: Android Data Extraction Techniques

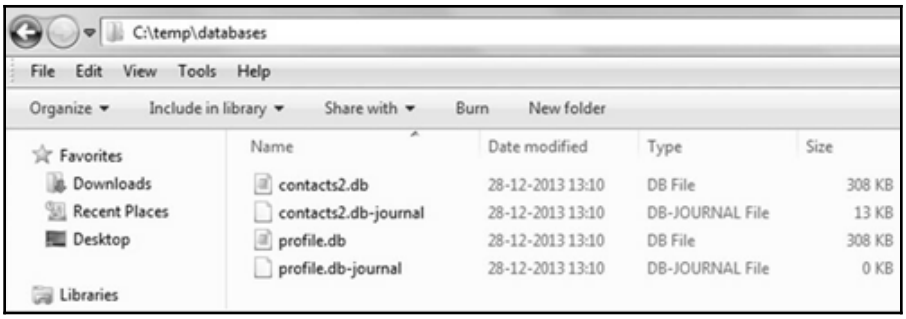
```
C:\android-sdk\platform-tools>adb.exe pull /data/data/com.dropbox.android/databases C:\temp
pull: building file list...
pull: /data/data/com.dropbox.android/databases/prefs.db-journal -> C:\temp/prefs.db-journal
pull: /data/data/com.dropbox.android/databases/prefs.db -> C:\temp/prefs.db
pull: /data/data/com.dropbox.android/databases/db.db-journal -> 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)
```



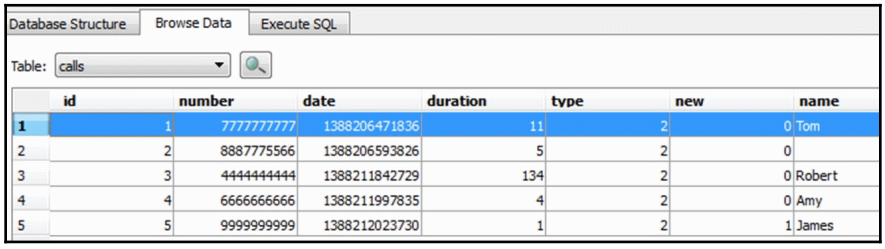

```
C:\android-sdk\platform-tools>adb.exe pull /data C:\temp
pull: building file list...
0 files pulled. 0 files skipped.
```




```
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
```



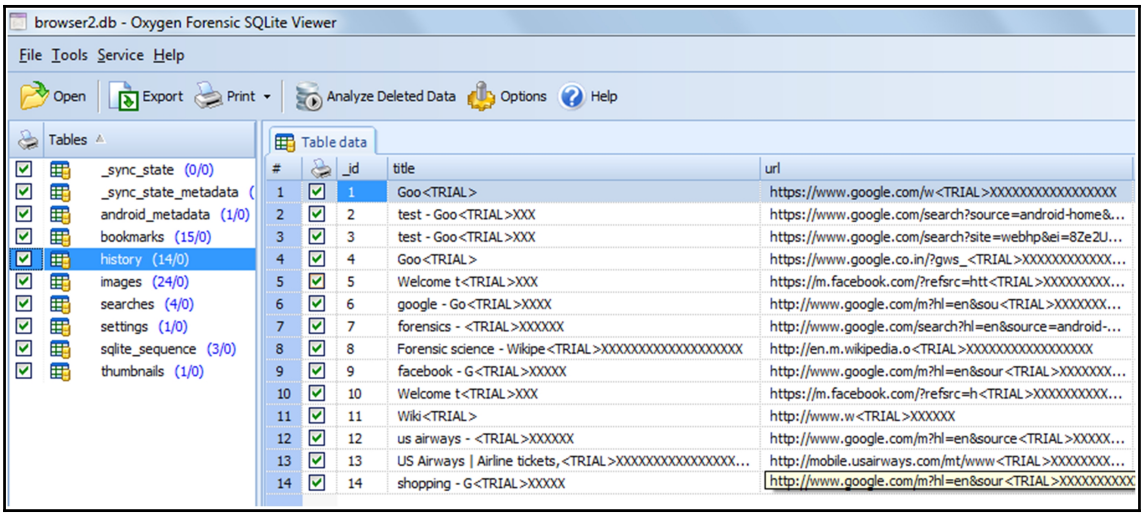

```
pull: /data/data/com.android.providers.contacts/databases/contacts2.db-mjFB7EA79BB -> C:\temp/databases/contacts2.db-mjFB7EA79BB
pull: /data/data/com.android.providers.contacts/databases/contacts2.db-mj7DE1FC9E3 -> C:\temp/databases/contacts2.db-mj7DE1FC9E3
pull: /data/data/com.android.providers.contacts/databases/contacts2.db-mj2151EE924 -> 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	prot	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


browser2.db - Oxygen Forensic SQLite Viewer
File Tools Service Help
Open
Export
Print
Analyze Deleted Data
Options
Help
Tables
_sync_state (0/0)
_sync_state_metadata (
android_metadata (1/0)
bookmarks (15/0)
history (14/0)
images (24/0)
searches (4/0)
settings (1/0)
sqlite_sequence (3/0)
thumbnails (1/0)
Table data
_id title url
1 1 Goo<TRIAL> https://www.google.com/w<TRIAL>XXXXXXXXXXXXXXXX
2 2 test - Goo<TRIAL>XXX https://www.google.com/search?source=android-home&...
3 3 test - Goo<TRIAL>XXX https://www.google.com/search?site=webhp&ei=8Ze2U...
4 4 Goo<TRIAL> https://www.google.co.in/?gws_<TRIAL>XXXXXXXXXXX...
5 5 Welcome t<TRIAL>XXX https://m.facebook.com/?refsrc=htt<TRIAL>XXXXXXXX...
6 6 google - Go<TRIAL>XXXX http://www.google.com/m?hl=en&sou<TRIAL>XXXXXX...
7 7 forensics - <TRIAL>XXXXXX http://www.google.com/search?hl=en&source=android-...
8 8 Forensic science - Wikipe<TRIAL>XXXXXXXXXXXXXXXXX http://en.m.wikipedia.o<TRIAL>XXXXXXXXXXXXXX
9 9 facebook - G<TRIAL>XXXXX http://www.google.com/m?hl=en&sour<TRIAL>XXXXXX...
10 10 Welcome t<TRIAL>XXX https://m.facebook.com/?refsrc=h<TRIAL>XXXXXXXX...
11 11 Wiki<TRIAL> http://www.w<TRIAL>XXXXXX
12 12 us airways - <TRIAL>XXXXXX http://www.google.com/m?hl=en&source<TRIAL>XXXXX...
13 13 US Airways | Airline tickets,<TRIAL>XXXXXXXXXXXXXXX... http://mobile.usairways.com/mt/www<TRIAL>XXXXXXX...
14 14 shopping - G<TRIAL>XXXXX http://www.google.com/m?hl=en&sour<TRIAL>XXXXXXXXX

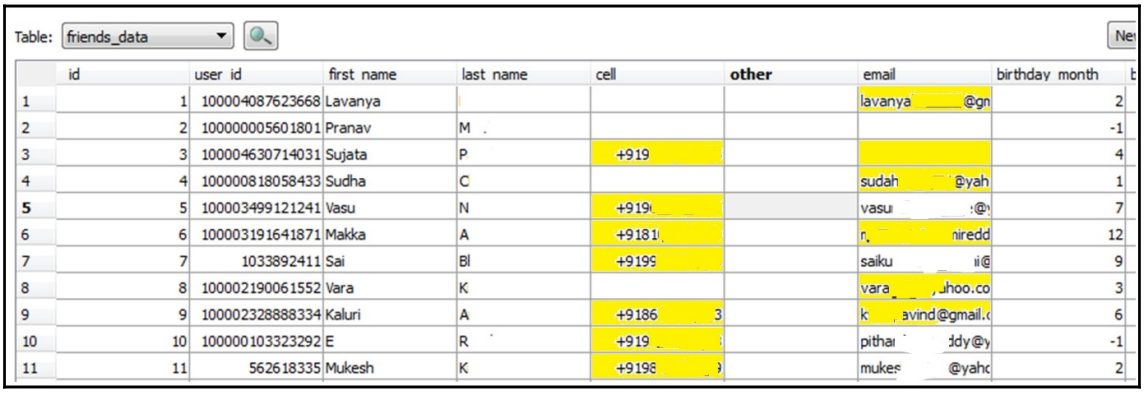
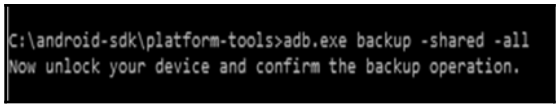
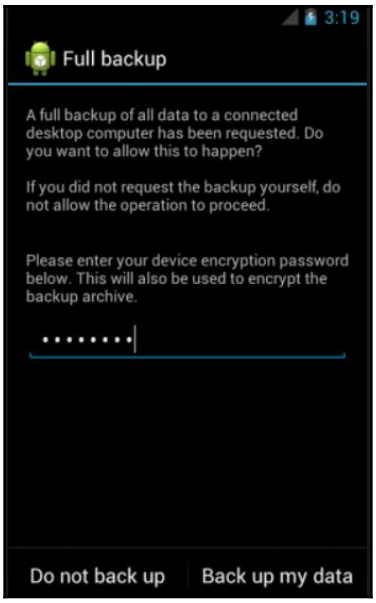


Table: friends_data
id user id first name last name cell other email birthday month
1 1 100004087623668 Lavanya lavanya @gn 2
2 2 100000005601801 Pranav M -1
3 3 100004630714031 Sujata P +919 4
4 4 100000818058433 Sudha C sudah @yah 1
5 5 100003499121241 Vasu N +919 vasu 7
6 6 100003191641871 Makka A +9181 niredd 12
7 7 1033892411 Sai Bl +9199 saiku 9
8 8 100002190061552 Vara K vara 3
9 9 100002328888334 Kaluri A +9186 3 6
10 10 100000103323292 E R +919 -1
11 11 562618335 Mukesh K +9198 mukes @yahc 2


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




```
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]
```

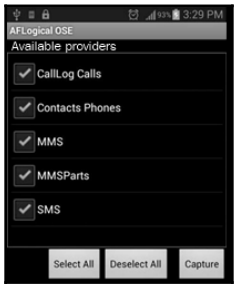
```
C:\android-sdk\platform-tools>adb.exe shell dumpsys iphonesubinfo
Phone Subscriber Info:
  Phone Type = GSM
  Device ID = 353[redacted]6486
```

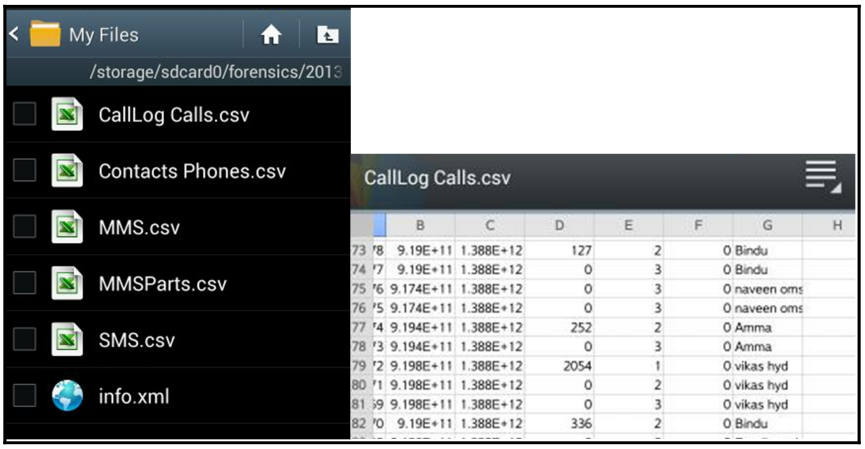
```
C:\android-sdk\platform-tools>adb.exe shell dumpsys wifi
Wi-Fi is enabled
Stay-awake conditions: 0

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
```

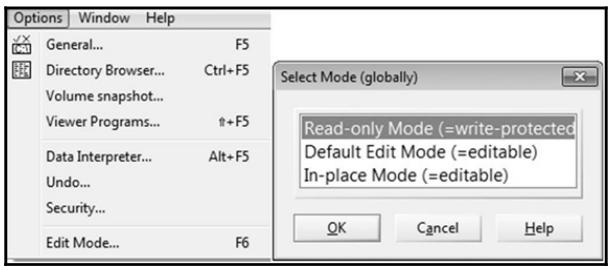
```
C:\android-sdk\platform-tools>adb.exe install AFLogical-OSE_1.5.2.apk
1798 KB/s (28794 bytes in 0.015s)
        pkg: /data/local/tmp/AFLogical-OSE_1.5.2.apk
Success
```

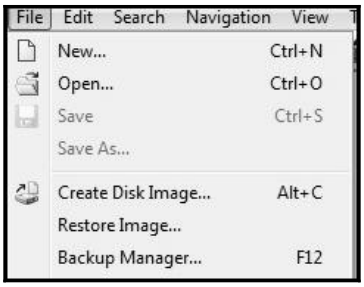


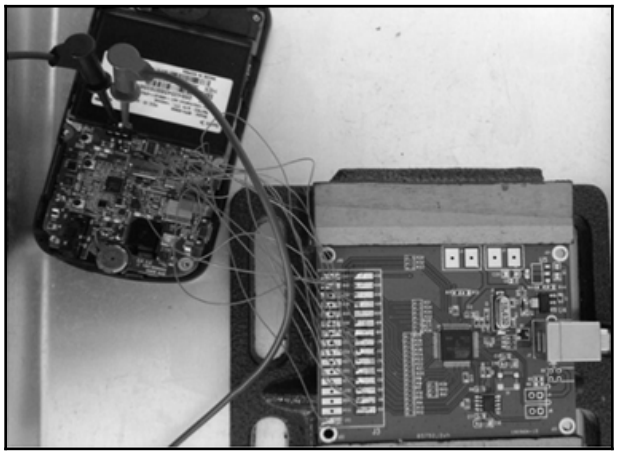


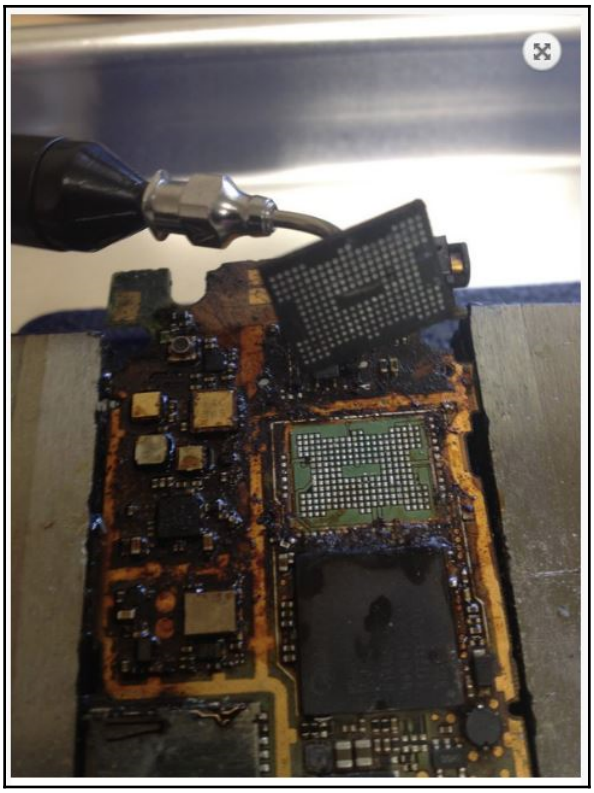

```
C:\android-sdk\platform-tools>adb.exe devices
List of devices attached
4df16ac31[redacted]        device
```

```
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
```

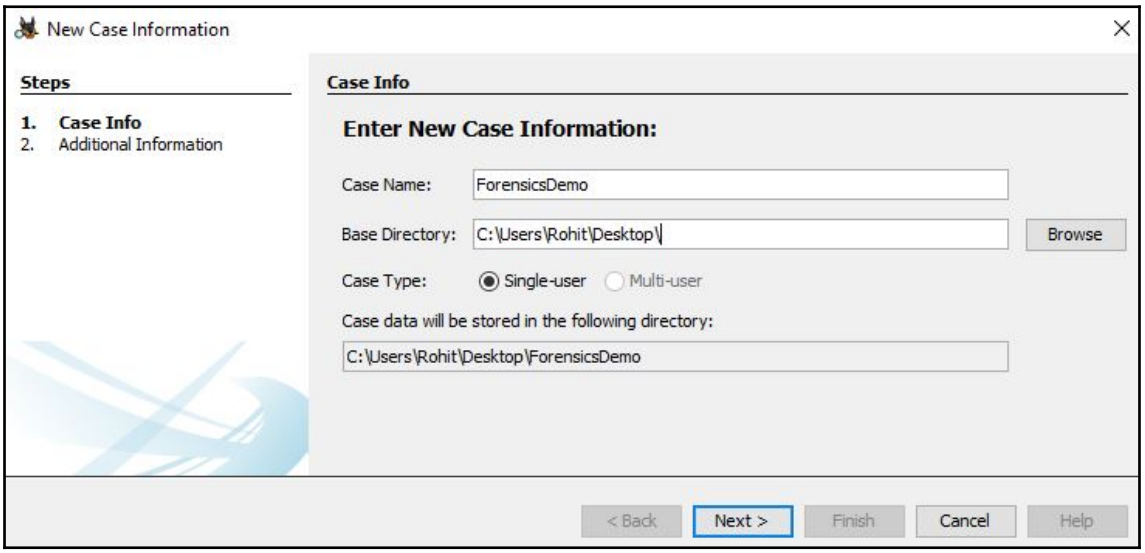


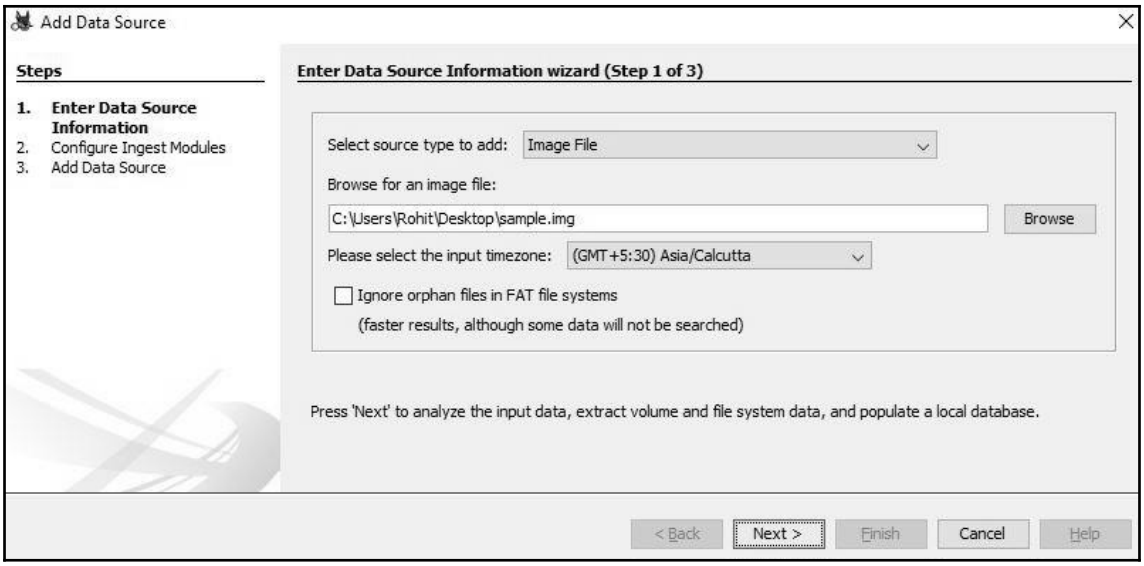

File
Edit
Search
Navigation
View
New... Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Create Disk Image... Alt+C
Restore Image...
Backup Manager... F12

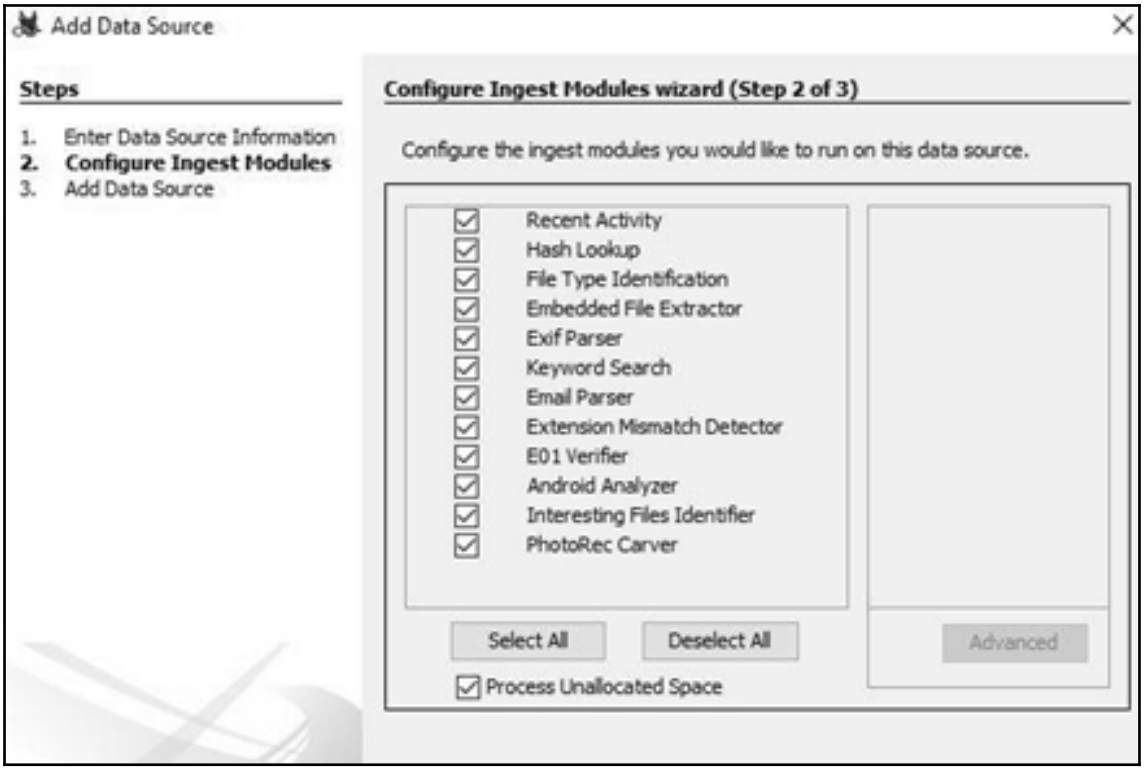


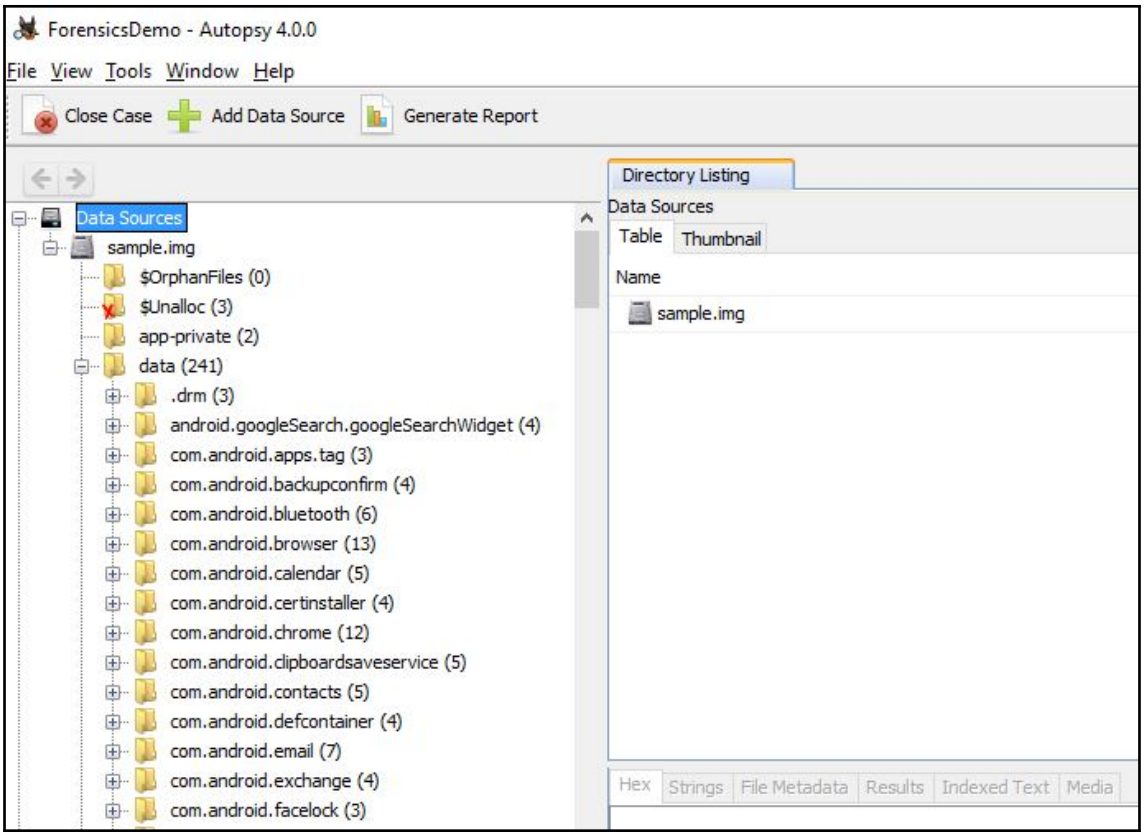


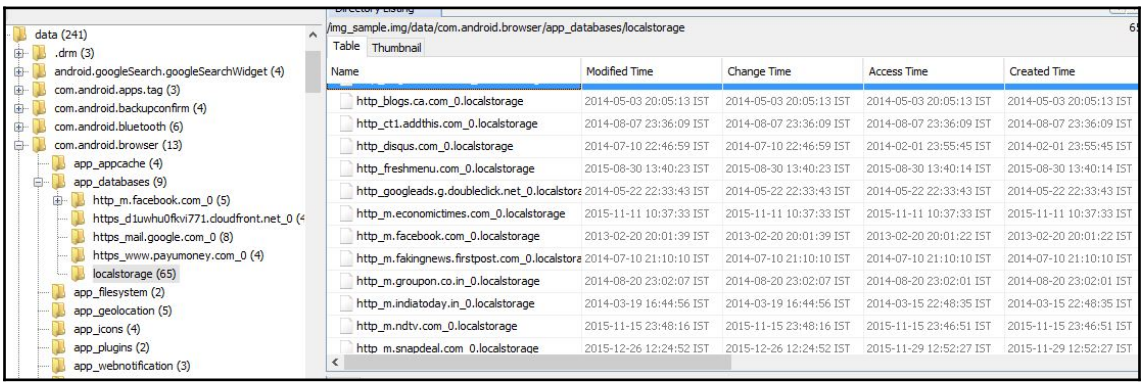
Chapter 10: Android Data Analysis and Recovery

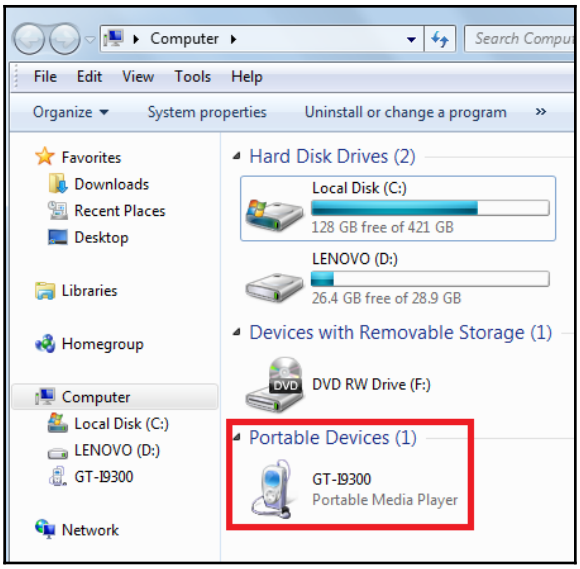


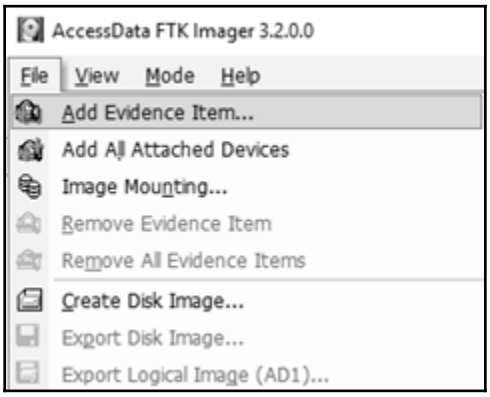

Add Data Source
Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source
Enter Data Source Information wizard (Step 1 of 3)
Select source type to add: Image File
Browse for an image file:
C:\Users\Rohit\Desktop\sample.img
Browse
Please select the input timezone: (GMT+5:30) 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

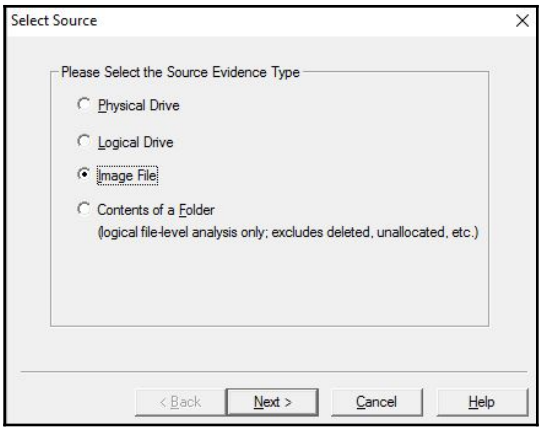

Add Data Source
Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source
Configure Ingest Modules wizard (Step 2 of 3)
Configure the ingest modules you would like to run on this data source.
Recent Activity
Hash Lookup
File Type Identification
Embedded File Extractor
Exif 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

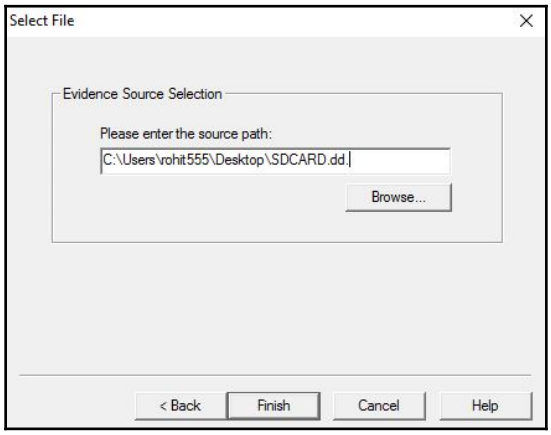

ForensicsDemo - Autopsy 4.0.0
File View Tools Window Help
Close Case
Add Data Source
Generate Report
Directory Listing
Data Sources
Table
Thumbnail
Name
sample.img
Data Sources
sample.img
$OrphanFiles (0)
$Unalloc (3)
app-private (2)
data (241)
.drm (3)
android.googleSearch.googleSearchWidget (4)
com.android.apps.tag (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

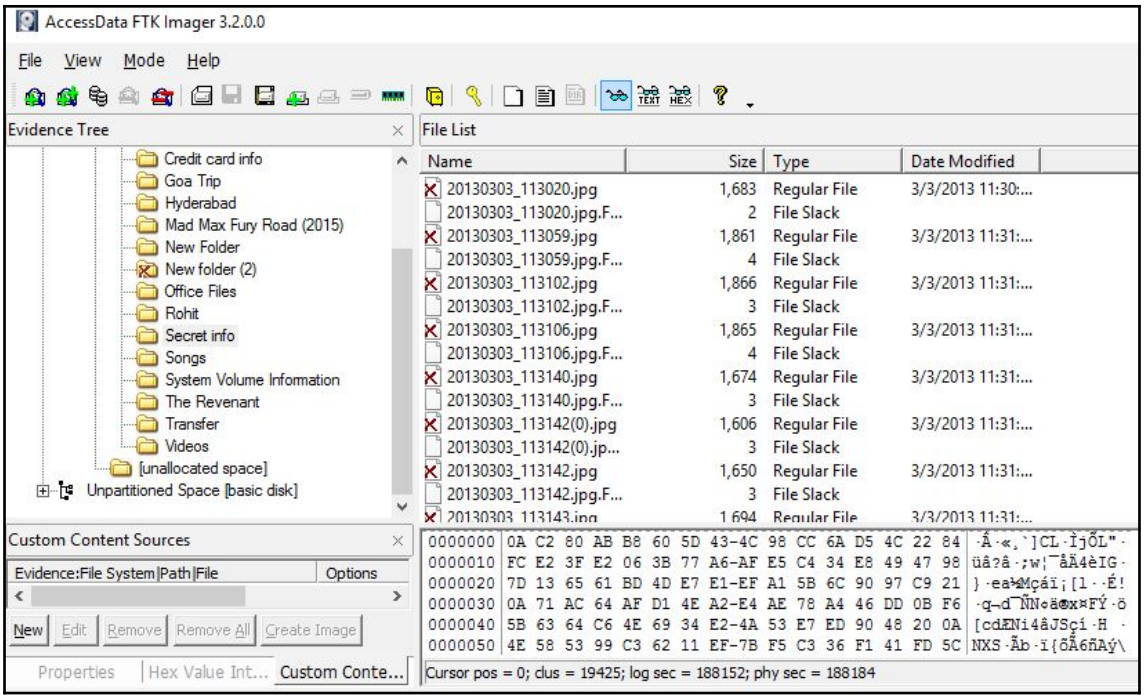

/img_sample.img/data/com.android.browser/app_databases/localstorage
Table
Thumbnail
Name
Modified Time
Change Time
Access Time
Created Time
http_blogs.ca.com_0.localstorage
http_ct1.addthis.com_0.localstorage
http_disqus.com_0.localstorage
http_freshmenu.com_0.localstorage
http_googleads.g.doubleclick.net_0.localstorage
http_m.economictimes.com_0.localstorage
http_m.facebook.com_0.localstorage
http_m.fakingnews.firstpost.com_0.localstorage
http_m.groupon.co.in_0.localstorage
http_m.indiatoday.in_0.localstorage
http_m.ndtv.com_0.localstorage
http_m.snapdeal.com_0.localstorage
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)

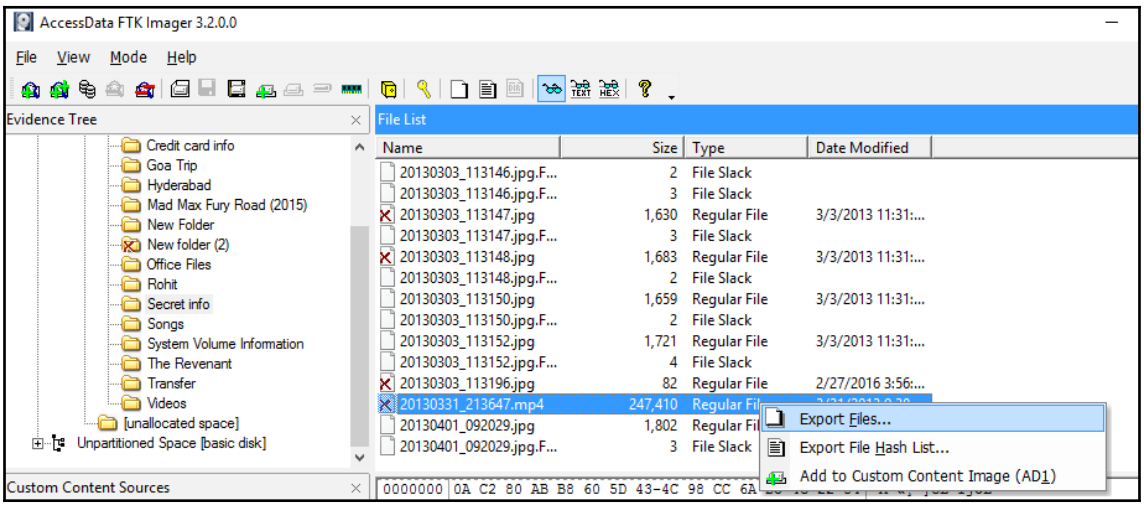

Computer
Search Computer
File Edit View Tools Help
Organize
System properties
Uninstall or change a program
Favorites
Downloads
Recent Places
Desktop
Libraries
Homegroup
Computer
Local Disk (C:)
LENOVO (D:)
GT-I9300
Network
Hard Disk Drives (2)
Local Disk (C:)
128 GB free of 421 GB
LENOVO (D:)
26.4 GB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

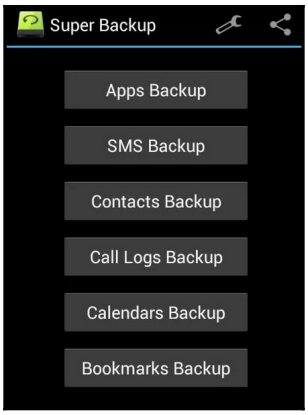

AccessData FTK Imager 3.2.0.0
File View Mode Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...


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

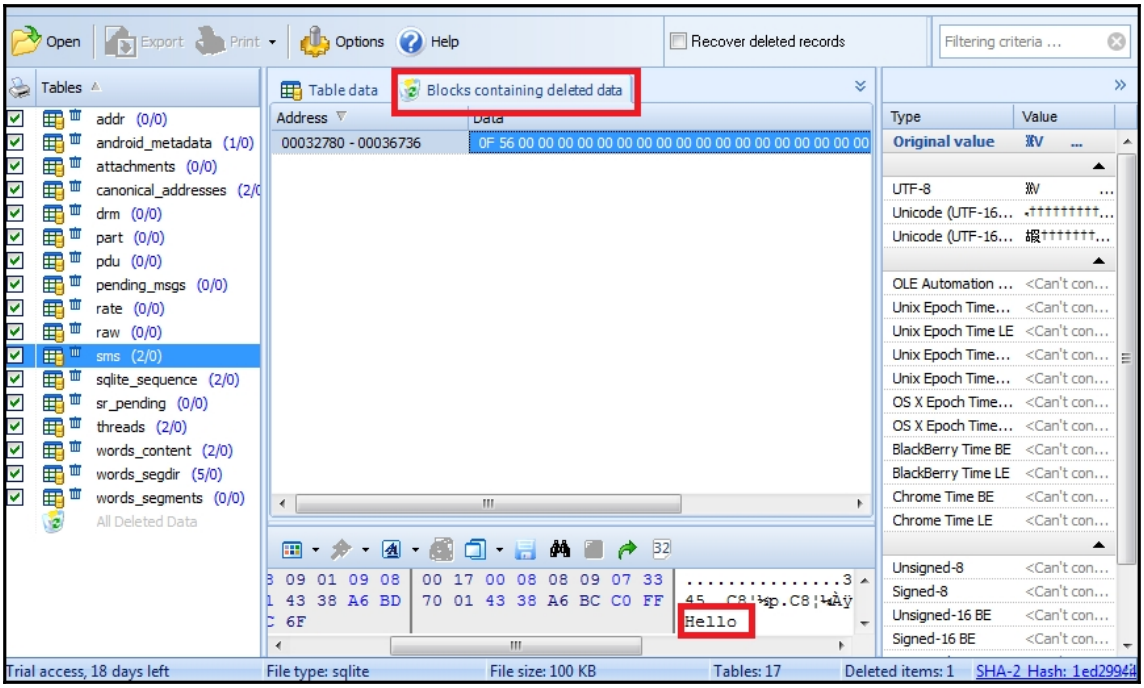

Select File
Evidence Source Selection
Please enter the source path:
C:\Users\rohit555\Desktop\SDCARD.dd
Browse...
< Back
Finish
Cancel
Help


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 Regular Fil
20130401_092029.jpg 1,802 Regular Fil
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)
```



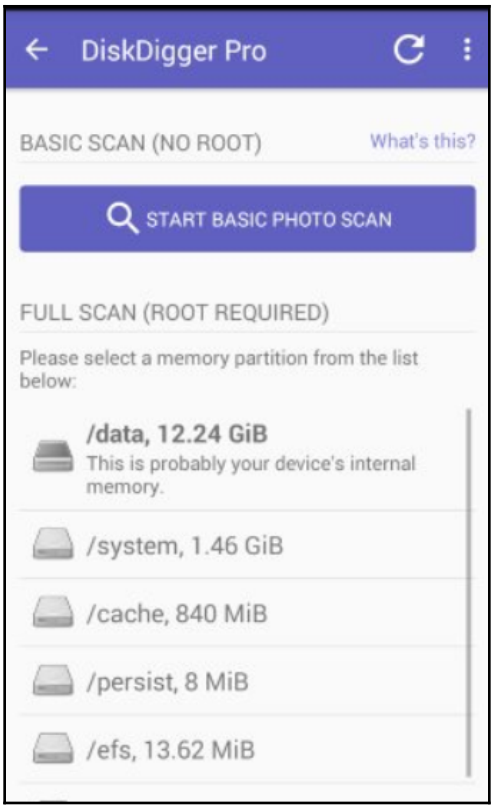
scalpel.conf

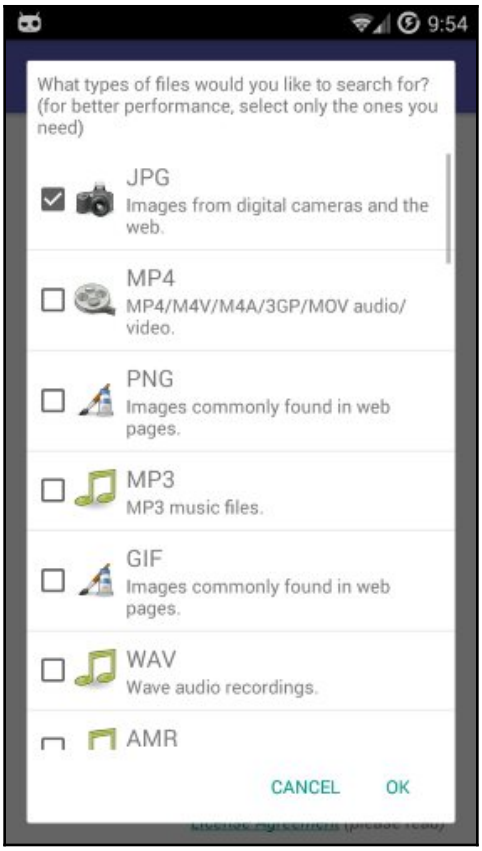
```
# GRAPHICS FILES
#-----------------------------------------------------------------
#
#
# AOL ART files
#       art     y       150000  \x4a\x47\x04\x0e        \xcf\xc7\xcb
#       art     y       150000  \x4a\x47\x03\x0e        \xd0\xcb\x00\x00
#
# GIF and JPG files (very common)
#       gif     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
```

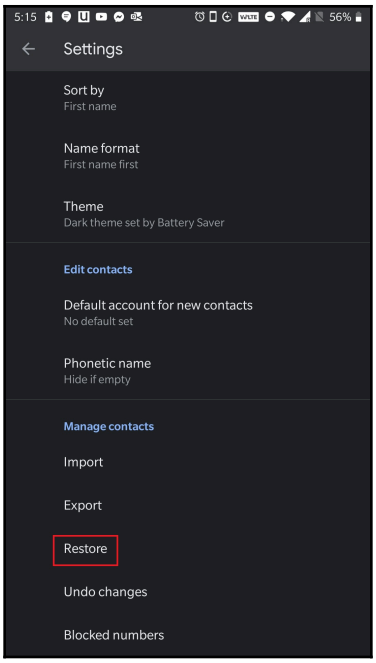
```
File  Edit  View  Search  Terminal  Help
unigeek@ubuntu:~$ scalpel -c /home/unigeek/Desktop/scalpel-android.conf /home/un
igeek/Desktop/userdata.dd -o /home/unigeek/Desktop/rohit
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

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
```

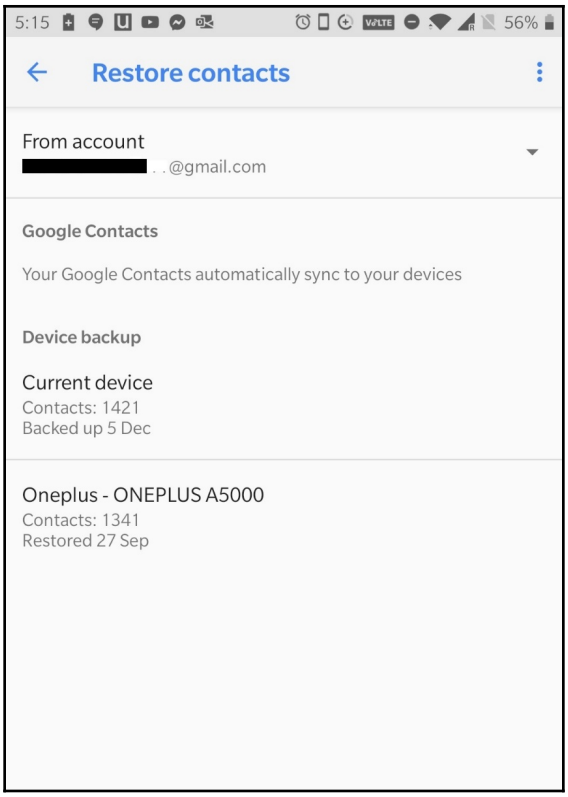

Home
Desktop
rohit
Search
gif-1-0
htm-10-0
jpg-2-0
jpg-3-0
png-5-0
zip-15-0
audit.txt

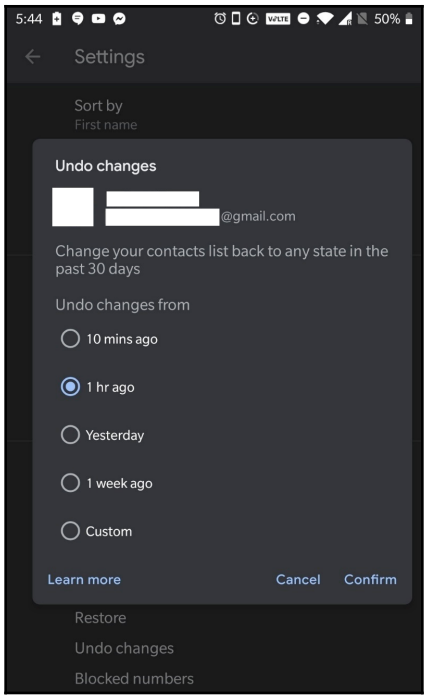

Home
Desktop
rohit
jpg-2-0
00000050.jpg
00000051.jpg
00000052.jpg
00000054.jpg
00000055.jpg
00000056.jpg
00000058.jpg
00000059.jpg
00000060.jpg


DiskDigger Pro
BASIC SCAN (NO ROOT)
What's this?
START BASIC PHOTO SCAN
FULL SCAN (ROOT REQUIRED)
Please select a memory partition from the list below:
/data, 12.24 GiB
This is probably your device's internal memory.
/system, 1.46 GiB
/cache, 840 MiB
/persist, 8 MiB
/efs, 13.62 MiB


9:54
What types of files would you like to search for? (for better performance, select only the ones you need)
JPG
Images from digital cameras and the web.
MP4
MP4/M4V/M4A/3GP/MOV audio/ video.
PNG
Images commonly found in web pages.
MP3
MP3 music files.
GIF
Images commonly found in web pages.
WAV
Wave audio recordings.
AMR
CANCEL
OK


5:15
56%
Settings
Sort by
First name
Name format
First name first
Theme
Dark theme set by Battery Saver
Edit contacts
Default account for new contacts
No default set
Phonetic name
Hide if empty
Manage contacts
Import
Export
Restore
Undo changes
Blocked numbers


5:15
56%
Restore contacts
From account
[redacted]@gmail.com
Google Contacts
Your Google Contacts automatically sync to your devices
Device backup
Current device
Contacts: 1421
Backed up 5 Dec
Oneplus - ONEPLUS A5000
Contacts: 1341
Restored 27 Sep


5:44
50%
Settings
Sort by
First name
Undo changes
@gmail.com
Change your contacts list back to any state in the past 30 days
Undo changes from
10 mins ago
1 hr ago
Yesterday
1 week ago
Custom
Learn more
Cancel
Confirm
Restore
Undo changes
Blocked numbers

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.
com.android.providers.calendar 10087 0 /data/data/com.android.providers.calendar
com.android.bluetooth 10083 0 /data/data/com.android.bluetooth
```

SQLite Database Browser - C:/Users/Rohit/Desktop/dump/andy/fb/databases/newsfeed_db

File Edit View Help

Database Structure | Browse Data | Execute SQL

Table: home_stories

	feed_type	fetched_at	cursor	dedup_key	sort_i	ranking	features_meta	disallo	seen_state	image_seen_state	image_cache_state	image_urls	see	row	story	story_t	cache_file_path
1	top_stories	1458878132728	MTQ1ODg	3651869378	1:000(	3400879	[]	0	1	3	0	https://scontent.fde		0		User	/data/data/com.face
2	top_stories	1458878132728	MTQ1ODg	4933983296	1:000(	0.0	{"sponsored":1,"sub	1	0	0	2	https://scontent.fde		0		Ad	/data/data/com.face
3	top_stories	1458878132728	MTQ1ODg	3159469259	1:000(	9208374	{"subject_type":0}	0	0	0	2	https://scontent.fde		0		User	/data/data/com.face
4	top_stories	1458878132728	MTQ1ODg	1609003662	1:000(	1373901	{"subject_type":0}	0	0	0	0	https://scontent.fde		0		User	/data/data/com.face
5	top_stories	1458878132728	MTQ1ODg	4977354125	1:000(	3237915	{"subject_type":0}	0	0	0	0	https://scontent.fde		0		User	/data/data/com.face
6	top_stories	1458878132728	MTQ1ODg	5819105357	1:000(	5870972	{"subject_type":0}	0	0	0	0	https://scontent.fde		0		User	/data/data/com.face
7	top_stories	1458878132728	MTQ1ODg	9256041140	1:000(	1128845	{"subject_type":0}	0	0	0	0	https://scontent.fde		0		User	/data/data/com.face
8	top_stories	1458878132728	MTQ1ODg	7568176440	1:000(	1979599	{"subject_type":0}	0	0	0	1	https://scontent.fde		0		User	/data/data/com.face
9	top_stories	1458878132728	MTQ1ODg	5149615670	1:000(	9988098	{"subject_type":0}	0	0	0	0	https://scontent.fde		0		User	/data/data/com.face
10	top_stories	1458878132728	MTQ1ODg	5829180926	1:000(	0.0	{"sponsored":1,"sub	1	0	0	0	https://scontent.fde		0		Ad	/data/data/com.face

Convert epoch to human-readable date and vice versa

1577881839 Timestamp to Human date [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

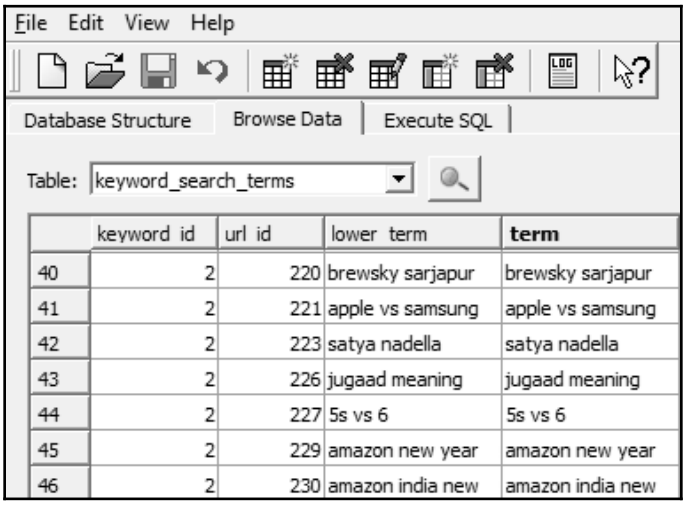
Assuming that this timestamp is in **seconds**:

GMT : Wednesday, January 1, 2020 12:30:39 PM

Your time zone : Wednesday, January 1, 2020 6:00:39 PM GMT+05:30

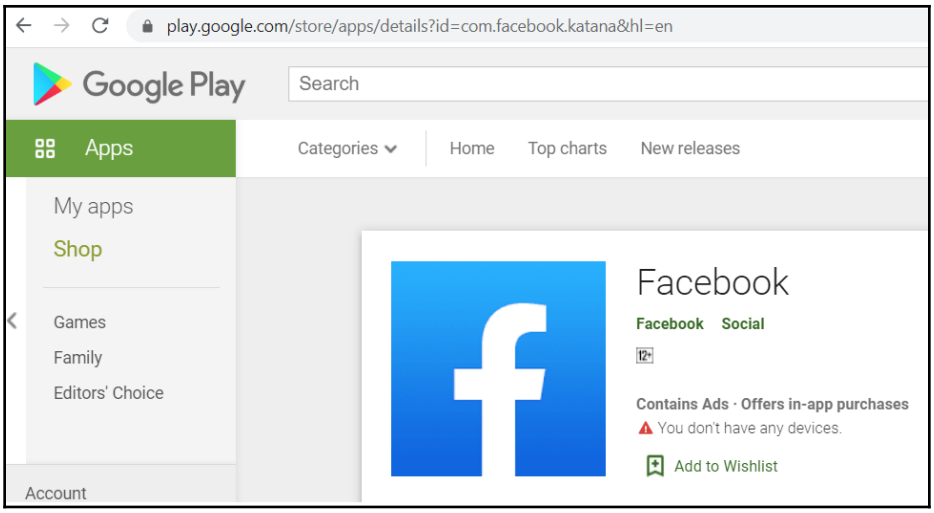
Relative : A few seconds ago

```
127|root@android:/data/data/com.google.android.gm/cache/[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	amazon new year
46	2	230	amazon india new	amazon india new

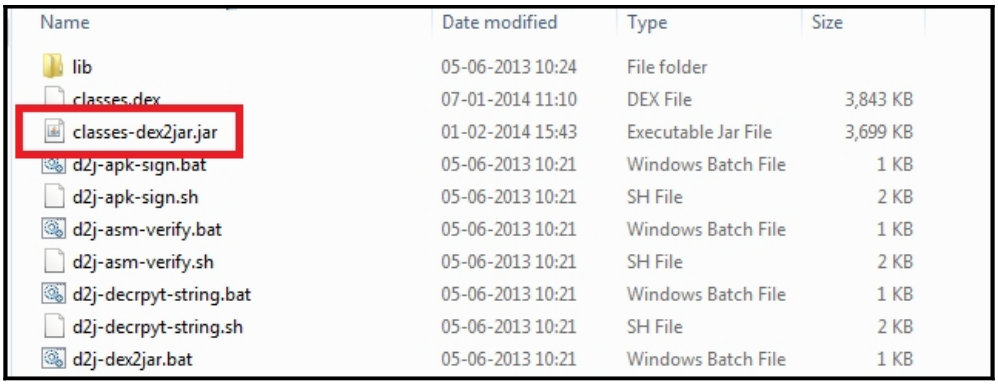
```
C:\android-sdk\platform-tools>adb.exe shell pm list packages
package:android
package:android.googleSearch.googleSearchWidget
package:com.android.MtpApplication
package:com.android.Preconfig
package:com.android.apps.tag
package:com.android.backupconfirm
package:com.android.bluetooth
package:com.android.browser
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
```

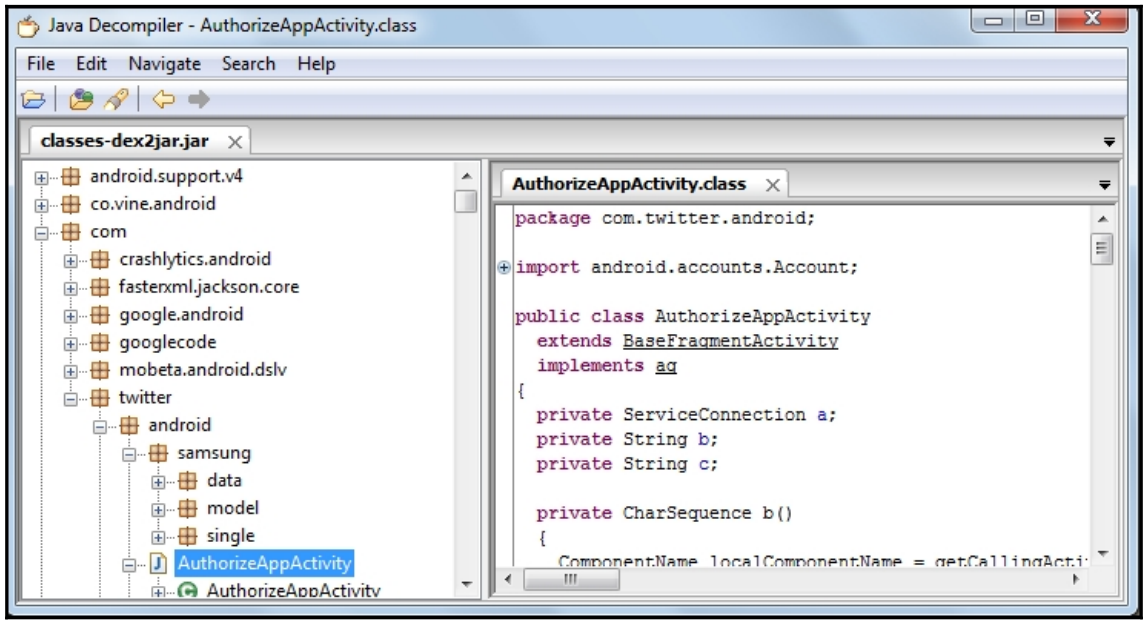


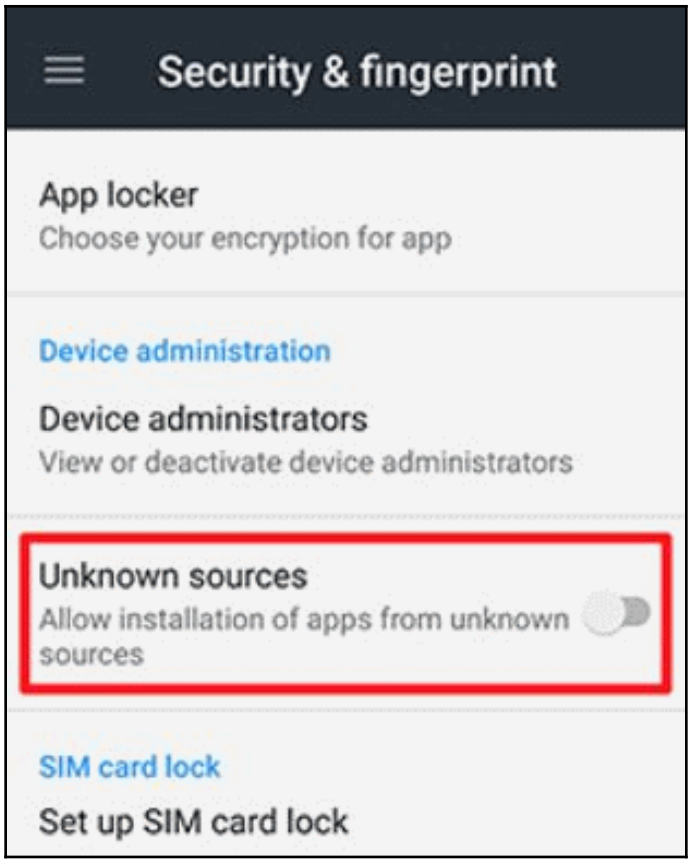

```
C:\android-sdk\platform-tools>adb.exe shell pm path com.android.chrome
package:/data/app/com.android.chrome-1.apk
```

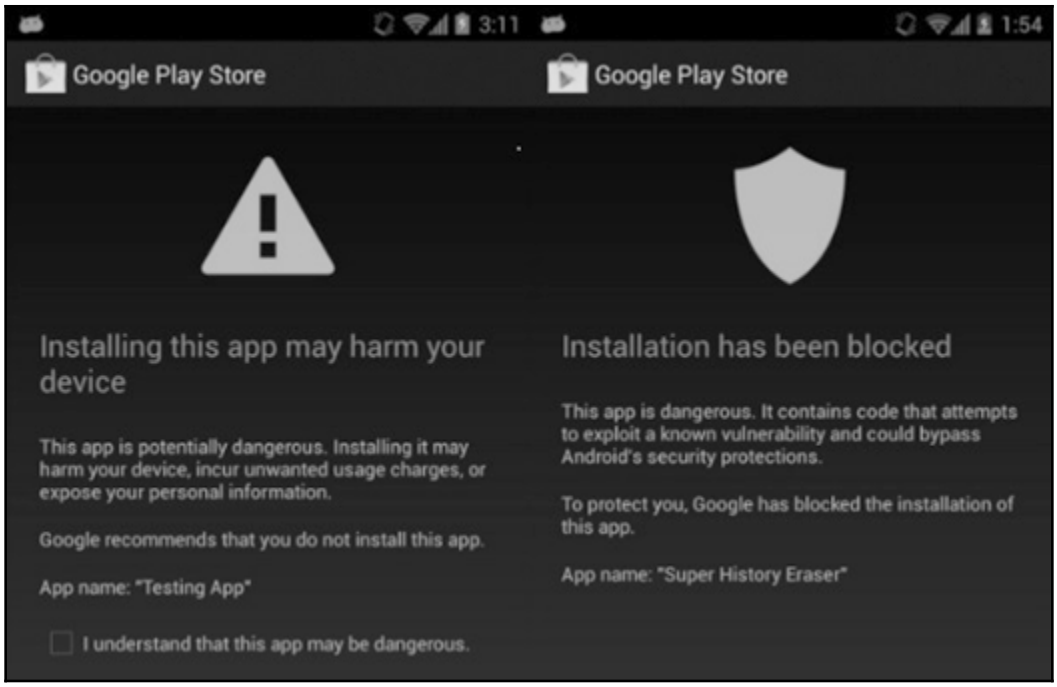
```
C:\android-sdk\platform-tools>adb.exe pull /data/app/com.android.chrome-1.apk C:\temp
3706 KB/s (42168820 bytes in 11.110s)
```

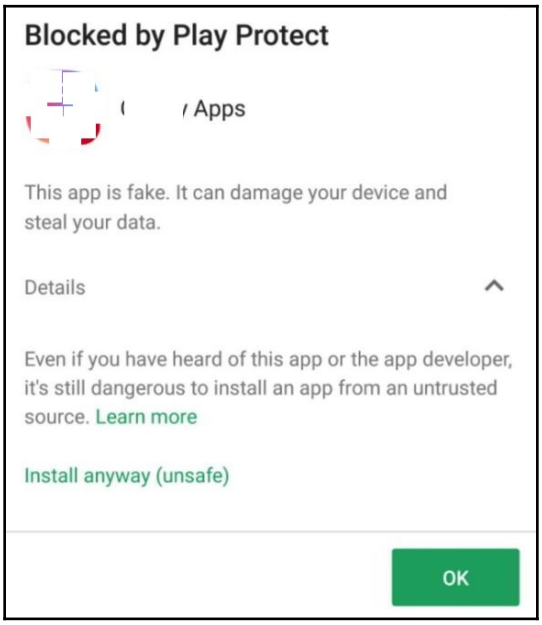
Name	Date modified	Type	Size
assets	01-02-2014 15:32	File folder	
com	01-02-2014 15:32	File folder	
lib	01-02-2014 15:32	File folder	
META-INF	01-02-2014 15:32	File folder	
res	01-02-2014 15:32	File folder	
AndroidManifest.xml	07-01-2014 11:10	XML Document	43 KB
classes.dex	07-01-2014 11:10	DEX File	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

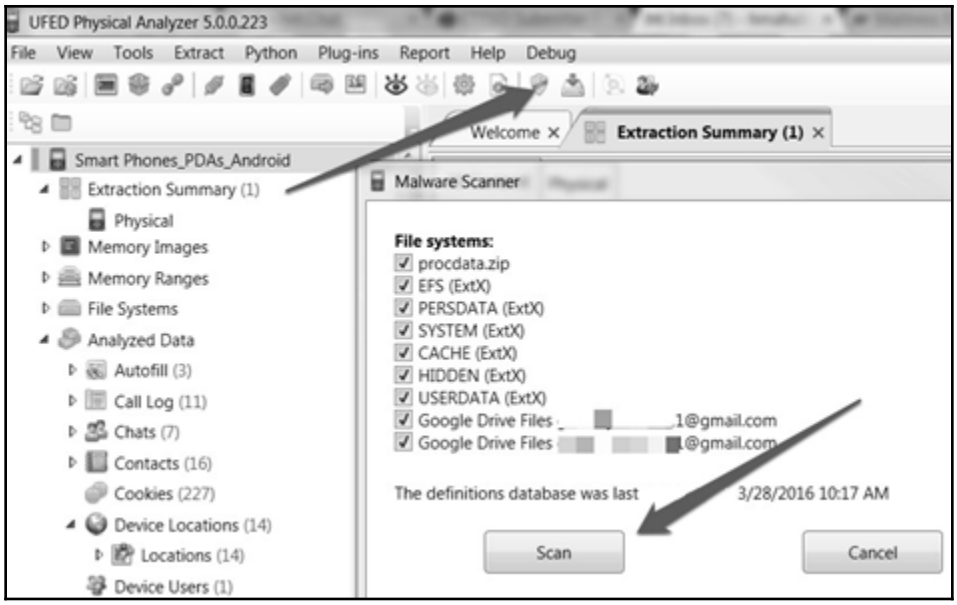

Name
Date modified
Type
Size
lib
05-06-2013 10:24
File folder
classes.dex
07-01-2014 11:10
DEX File
3,843 KB
classes-dex2jar.jar
01-02-2014 15:43
Executable Jar File
3,699 KB
d2j-apk-sign.bat
05-06-2013 10:21
Windows Batch File
1 KB
d2j-apk-sign.sh
05-06-2013 10:21
SH File
2 KB
d2j-asm-verify.bat
05-06-2013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

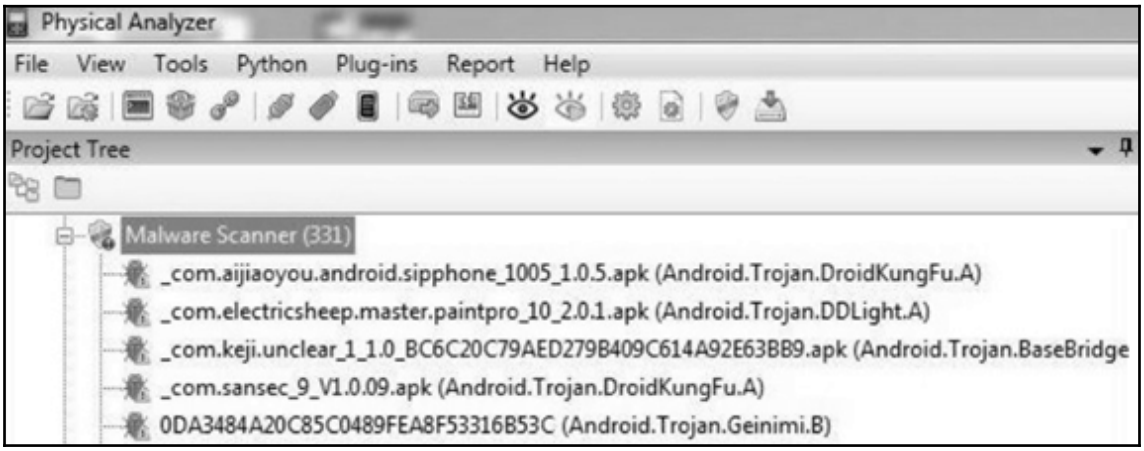

Java Decompiler - AuthorizeAppActivity.class
File
Edit
Navigate
Search
Help
classes-dex2jar.jar
android.support.v4
co.vine.android
com
crashlytics.android
fasterxml.jackson.core
google.android
googlecode
mobeta.android.dslv
twitter
android
samsung
data
model
single
AuthorizeAppActivity
AuthorizeAppActivity.class
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 & fingerprint
App locker
Choose your encryption for app
Device administration
Device administrators
View or deactivate device administrators
Unknown sources
Allow installation of apps from unknown sources
SIM card lock
Set up SIM card lock


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"

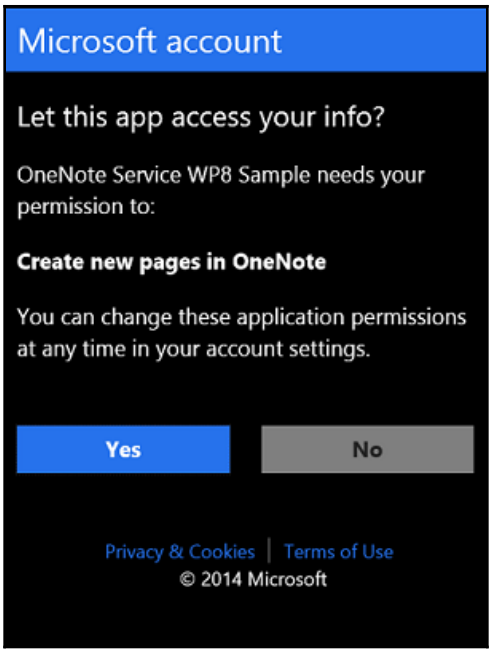

Blocked by Play Protect
Apps
This app is fake. It can damage your device and steal your data.
Details
Even if you have heard of this app or the app developer, it's still dangerous to install an app from an untrusted source. Learn more
Install anyway (unsafe)
OK

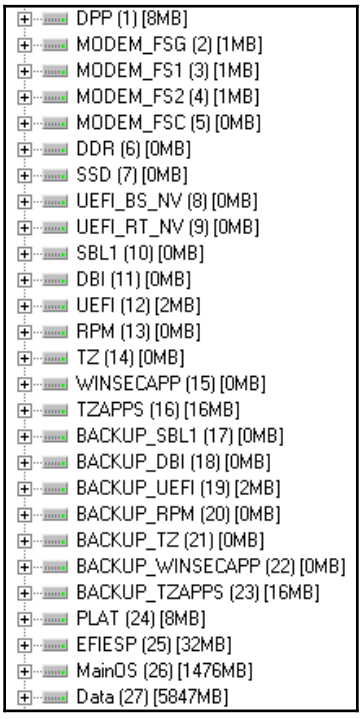

UFED Physical Analyzer 5.0.0.223
File View Tools Extract Python Plug-ins Report Help Debug
Welcome
Extraction Summary (1)
Smart Phones_PDAs_Android
Extraction Summary (1)
Physical
Memory Images
Memory Ranges
File Systems
Analyzed Data
Autofill (3)
Call Log (11)
Chats (7)
Contacts (16)
Cookies (227)
Device 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
3/28/2016 10:17 AM
Scan
Cancel

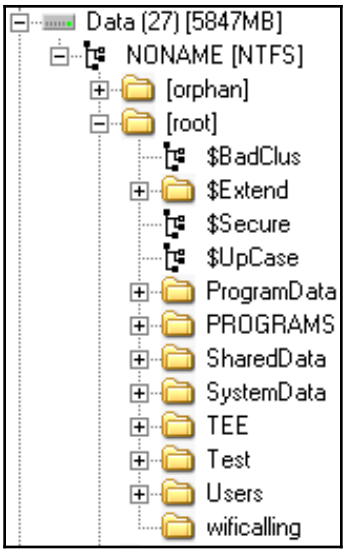

Physical Analyzer
File View Tools Python Plug-ins Report Help
Project Tree
Malware Scanner (331)
_com.aijiaoyou.android.sipphone_1005_1.0.5.apk (Android.Trojan.DroidKungFu.A)
_com.electricsheep.master.paintpro_10_2.0.1.apk (Android.Trojan.DDLight.A)
_com.keji.unclear_1_1.0_BC6C20C79AED279B409C614A92E63BB9.apk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

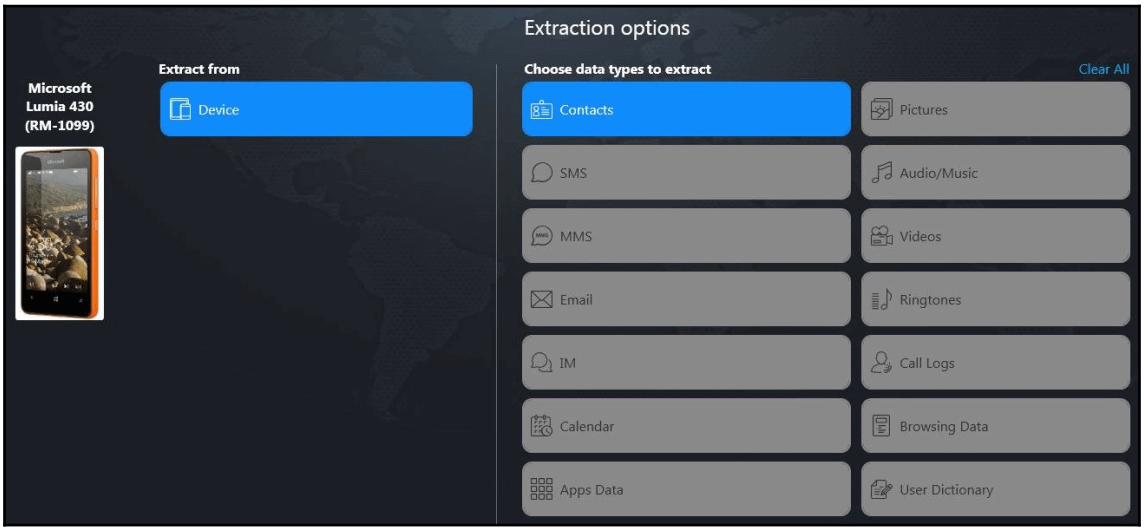

DPP (1) [8MB]
MODEM_FSG (2) [1MB]
MODEM_FS1 (3) [1MB]
MODEM_FS2 (4) [1MB]
MODEM_FSC (5) [0MB]
DDR (6) [0MB]
SSD (7) [0MB]
UEFI_BS_NV (8) [0MB]
UEFI_RT_NV (9) [0MB]
SBL1 (10) [0MB]
DBI (11) [0MB]
UEFI (12) [2MB]
RPM (13) [0MB]
TZ (14) [0MB]
WINSECAPP (15) [0MB]
TZAPPS (16) [16MB]
BACKUP_SBL1 (17) [0MB]
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]

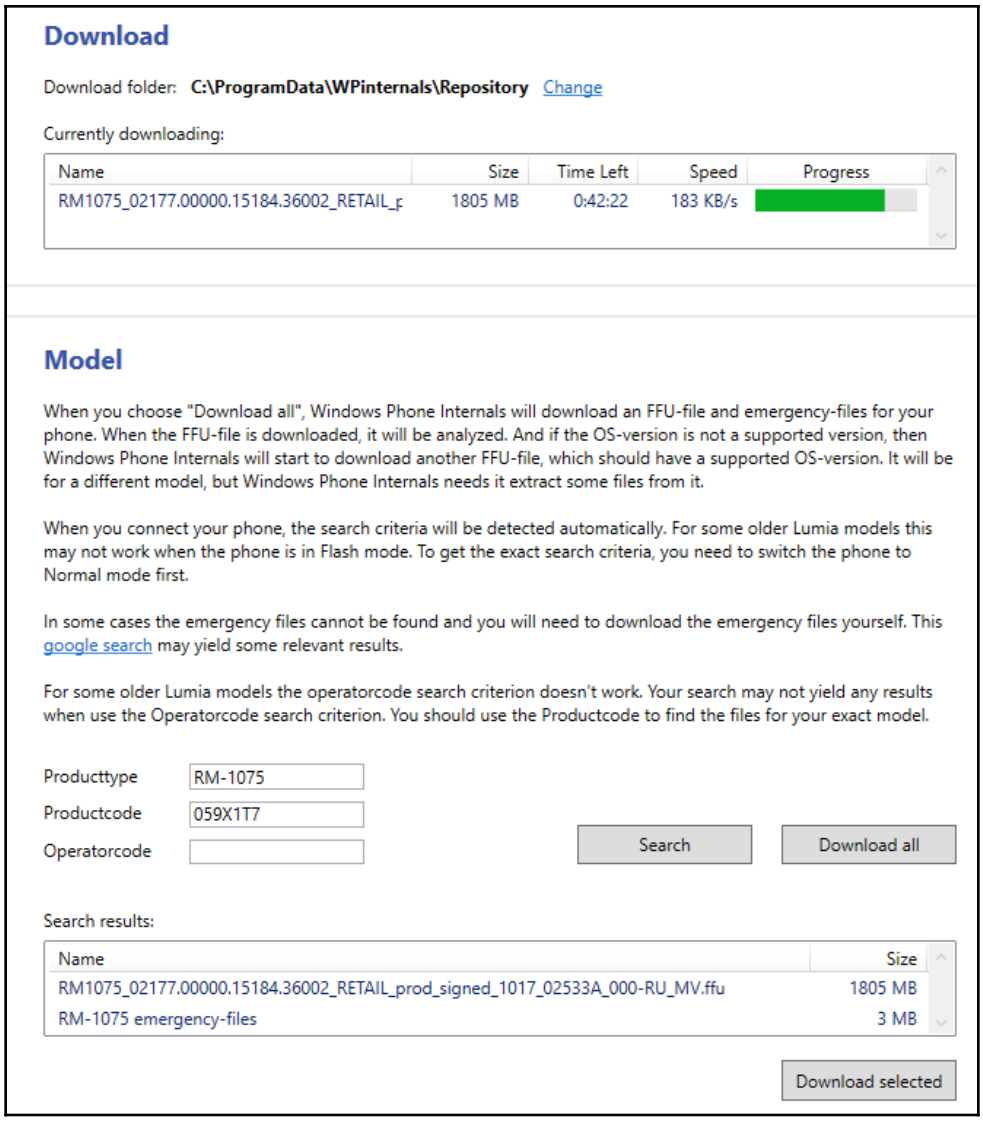

Data (27) [5847MB]
NONAME [NTFS]
[orphan]
[root]
$BadClus
$Extend
$Secure
$UpCase
ProgramData
PROGRAMS
SharedData
SystemData
TEE
Test
Users
wificalling

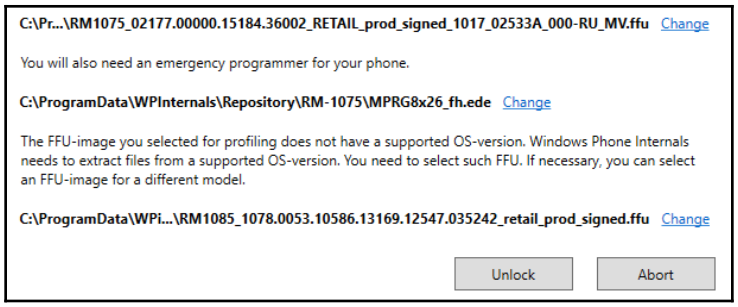

UFED
Phone Detective
Settings
Lumia
Total results: 20
Nokia CDMA
Lumia 928 (RM-860)
Logical, File system, Physical
Nokia CDMA
Lumia 929 (RM-927)
Logical
Nokia CDMA
Lumia 635 (RM-1078)
Logical, File system
Nokia CDMA
Lumia 822 (RM-845)
Logical, File system, Physical

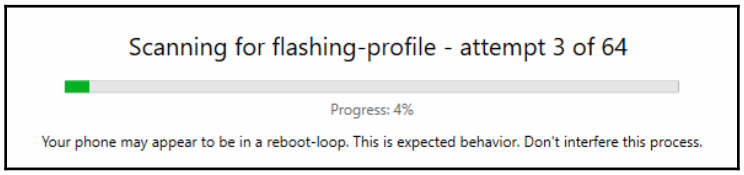

Logical Extraction
File System Extraction
Capture Images

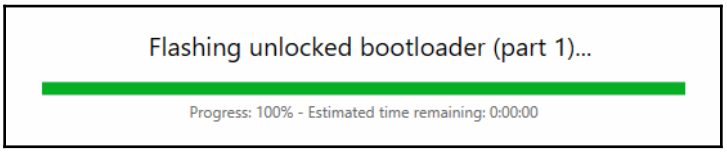

USB cable 100
Bluetooth

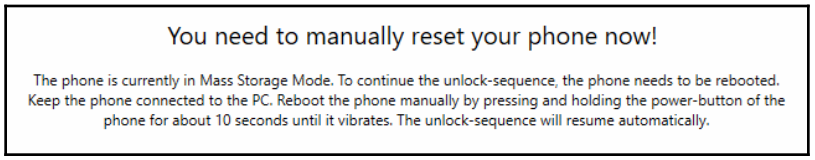

Extraction options
Microsoft Lumia 430 (RM-1099)
Extract from
Device
Choose data types to extract
Clear All
Contacts
Pictures
SMS
Audio/Music
MMS
Videos
Email
Ringtones
IM
Call Logs
Calendar
Browsing Data
Apps Data
User Dictionary

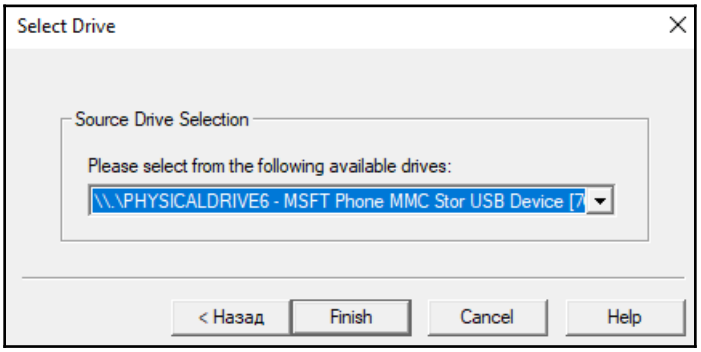

Download
Download folder: C:\ProgramData\WPinternals\Repository Change
Currently downloading:
Name Size Time Left Speed Progress
RM1075_02177.00000.15184.36002_RETAIL_p 1805 MB 0:42:22 183 KB/s
Model
When you choose "Download all", Windows Phone Internals will download an FFU-file and emergency-files for your phone. When the FFU-file is downloaded, it will be analyzed. And if the OS-version is not a supported version, then Windows Phone Internals will start to download another FFU-file, which should have a supported OS-version. It will be for a different model, but Windows Phone Internals needs it extract some files from it.
When you connect your phone, the search criteria will be detected automatically. For some older Lumia models this may not work when the phone is in Flash mode. To get the exact search criteria, you need to switch the phone to Normal mode first.
In some cases the emergency files cannot be found and you will need to download the emergency files yourself. This google search may yield some relevant results.
For some older Lumia models the operatorcode search criterion doesn't work. Your search may not yield any results when use the Operatorcode search criterion. You should use the Productcode to find the files for your exact model.
Producttype RM-1075
Productcode 059X1T7
Operatorcode
Search
Download all
Search results:
Name Size
RM1075_02177.00000.15184.36002_RETAIL_prod_signed_1017_02533A_000-RU_MV.ffu 1805 MB
RM-1075 emergency-files 3 MB
Download selected

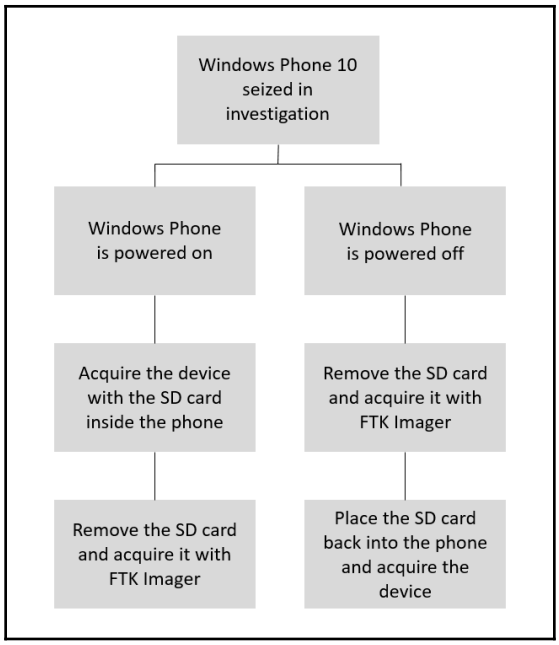

C:\Pr...\RM1075_02177.00000.15184.36002_RETAIL_prod_signed_1017_02533A_000-RU_MV.ffu Change
You will also need an emergency programmer for your phone.
C:\ProgramData\WPInternals\Repository\RM-1075\MPRG8x26_fh.ede Change
The FFU-image you selected for profiling does not have a supported OS-version. Windows Phone Internals needs to extract files from a supported OS-version. You need to select such FFU. If necessary, you can select an FFU-image for a different model.
C:\ProgramData\WPi...\RM1085_1078.0053.10586.13169.12547.035242_retail_prod_signed.ffu Change
Unlock
Abort

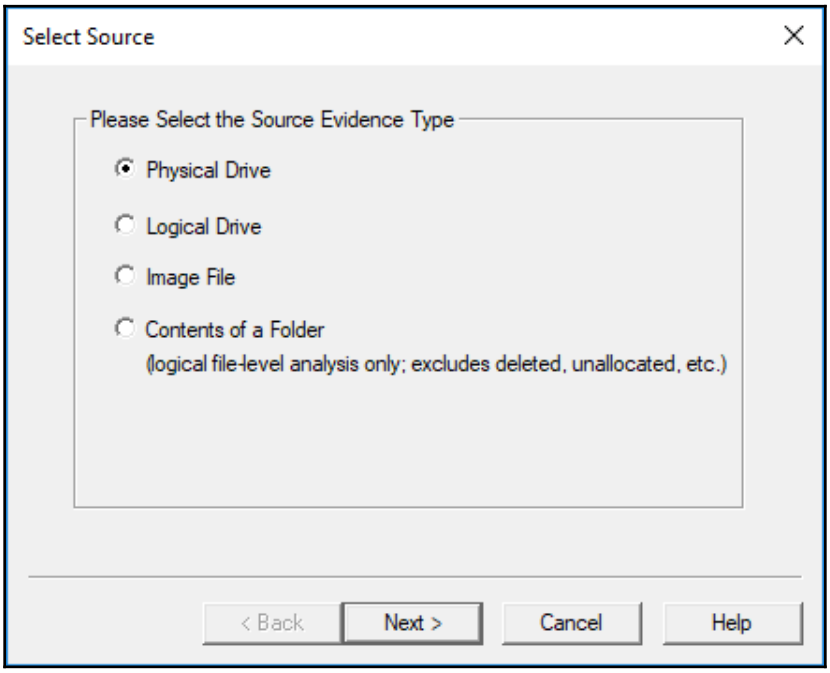

Scanning for flashing-profile - attempt 3 of 64
Progress: 4%
Your phone may appear to be in a reboot-loop. This is expected behavior. Don't interfere this process.

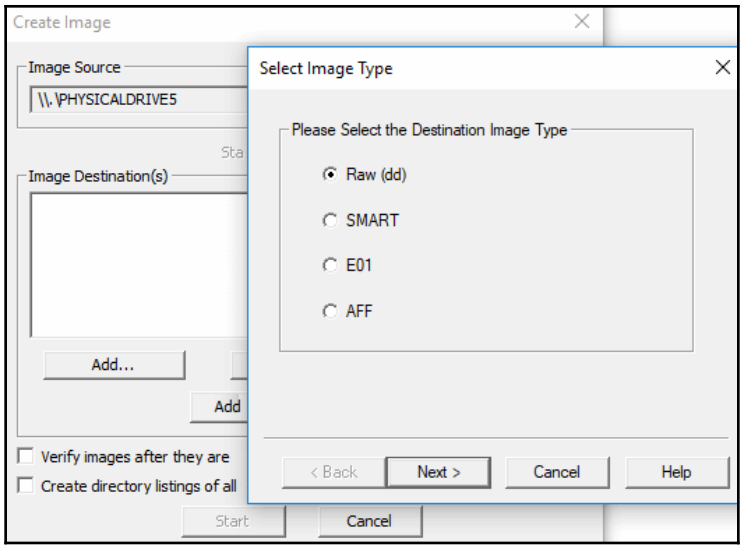

Flashing unlocked bootloader (part 1)...
Progress: 100% - Estimated time remaining: 0:00:00

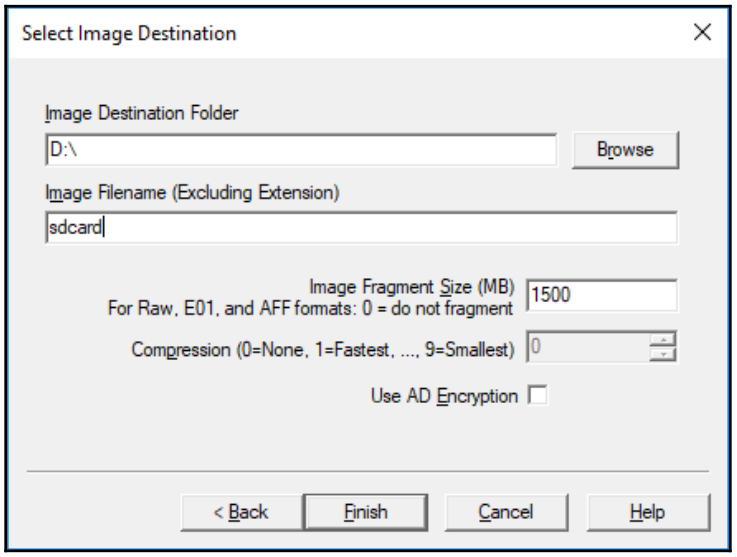

You need to manually reset your phone now!
The phone is currently in Mass Storage Mode. To continue the unlock-sequence, the phone needs to be rebooted. Keep the phone connected to the PC. Reboot the phone manually by pressing and holding the power-button of the phone for about 10 seconds until it vibrates. The unlock-sequence will resume automatically.


Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE6 - MSFT Phone MMC Stor USB Device [7
< Назад
Finish
Cancel
Help


Windows Phone 10 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 it with FTK Imager
Remove the SD card and acquire it with FTK Imager
Place the SD card back into the phone and acquire the device


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

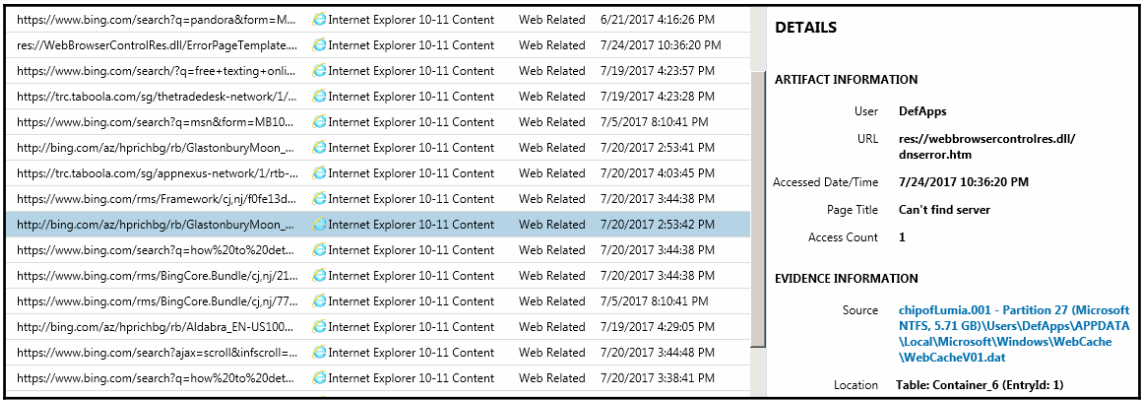

Create Image
Image Source
\\.\PHYSICALDRIVE5
Image Destination(s)
Add...
Add
Verify images after they are
Create directory listings of all
Start
Cancel
Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help


Select Image Destination
Image Destination Folder
D:\
Browse
Image Filename (Excluding Extension)
sdcard
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
1500
Compression (0=None, 1=Fastest, ..., 9=Smallest)
0
Use AD Encryption
< Back
Finish
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

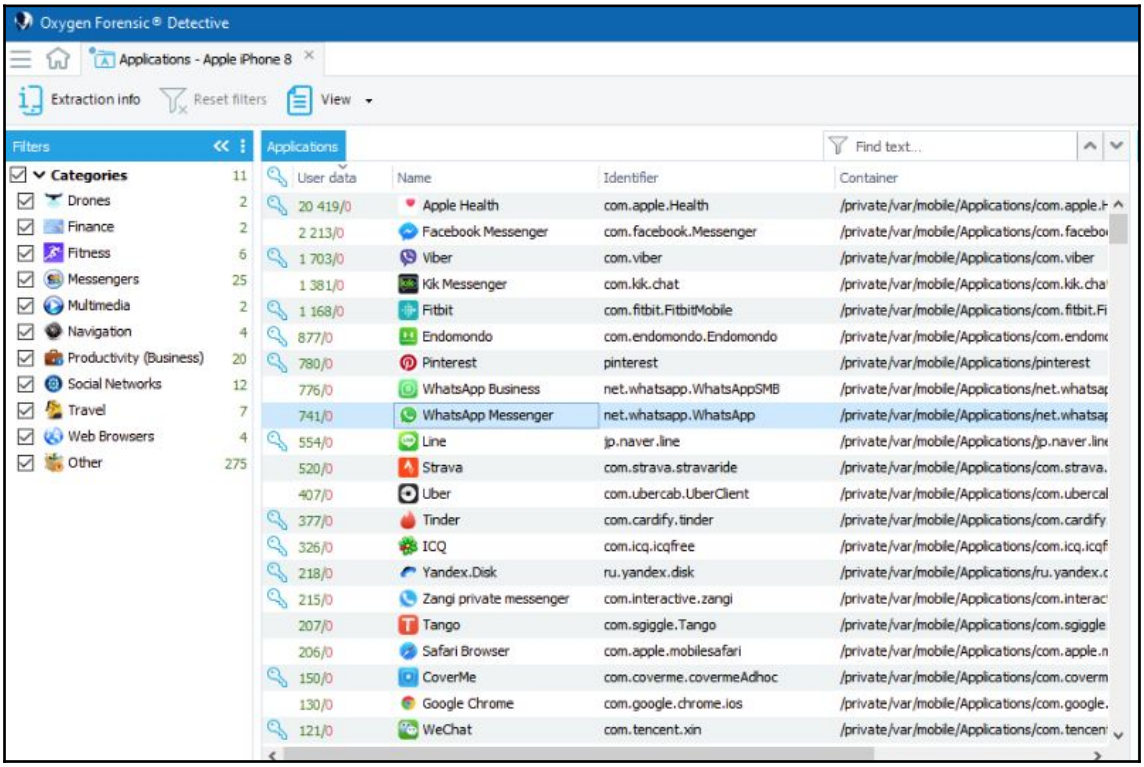
ARTIFACT INFORMATION

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

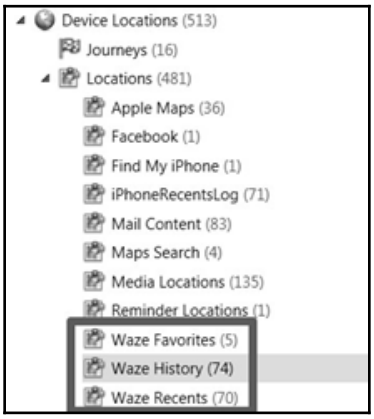
Source	**chipofLumia.001 - Partition 27 (Microsoft NTFS, 5.71 GB)\Users\DefApps\APPDATA\Local\Microsoft\Windows\WebCache\WebCacheV01.dat**
Location	**Table: Container_6 (EntryId: 1)**

Chapter 13: Parsing Third-Party Application Files



Direc...	Remote party	Text	Image URL	Time stamp (Device ...	Type
	Hank Fresh	Sweet	N/A	1/25/2016 4:27:52 PM	Text
	Hank Fresh	/data/media/0/Android/data/com.s...	http://u.tango.net/faw...	1/25/2016 4:27:30 PM	Image
	Hank Fresh	/data/media/0/Android/data/com.s...	http://u.tango.net/cub...	1/25/2016 4:27:00 PM	Image
	Hank Fresh	New s4?	N/A	1/25/2016 4:26:36	Text
	Hank Fresh	Hi its felcia	N/A	1/25/2016 4:25:47 PM	Text
	Hank Fresh	Hello! I would like to chat with you.	N/A	1/25/2016 4:24:06 PM	Text


1.7 km
Dodge Ave
In 400 m
Not there
Central Park Ave
Oakton St
16:57
4 min
2.3 km


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)

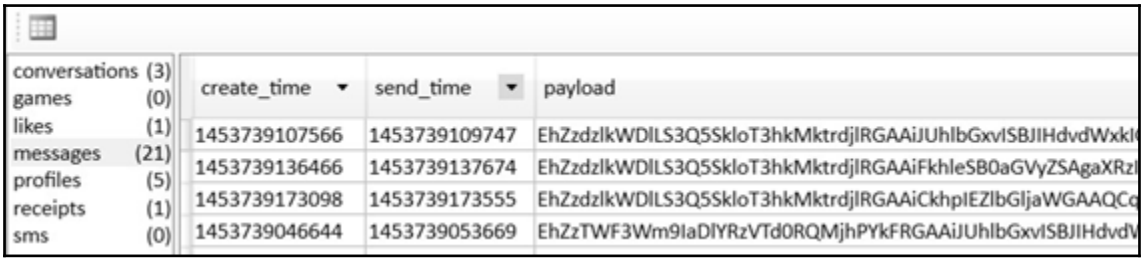
ARTIFACT INFORMATION

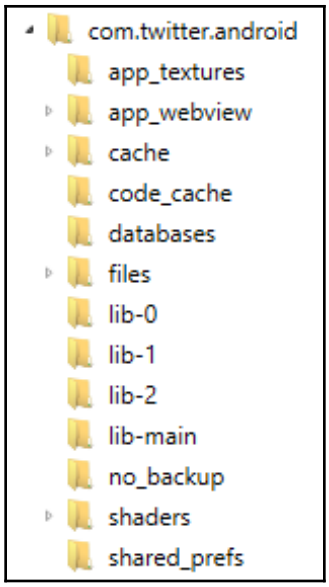
User ID	**767674047173918720**
User Name	**oskulkin**
Profile Created Date/Time	**8/22/2016 10:45:30 AM**
Description	**#DFIR professional. #ThreatIntel enthusiast. Opinions are my own.l [tab]MJjDFIRXXIXMJ j ThreatIntelXXI XXIM**
Web URL	**https://t.co/jhNd2msB3f**
Followers	**658**
Friends	**207**
Statuses	**309**
Image URL	**https://pbs.twimg.com/profile_images/1218460619764064257/BaefFcqO_normal.jpg**
Friend Metadata Updated Date/Time	**1/19/2020 11:07:23 AM**
Header URL	**https://pbs.twimg.com/profile_banners/767674047173918720/1579338626**

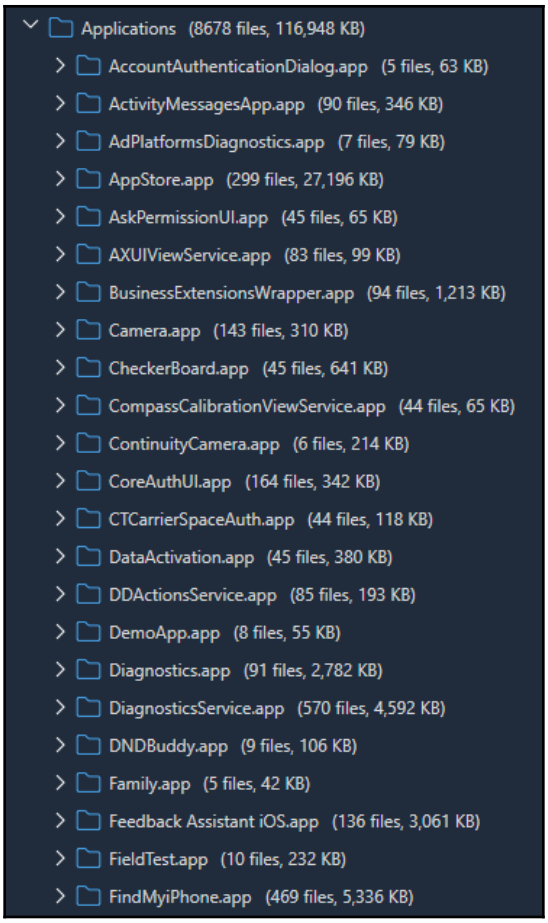
EVIDENCE INFORMATION

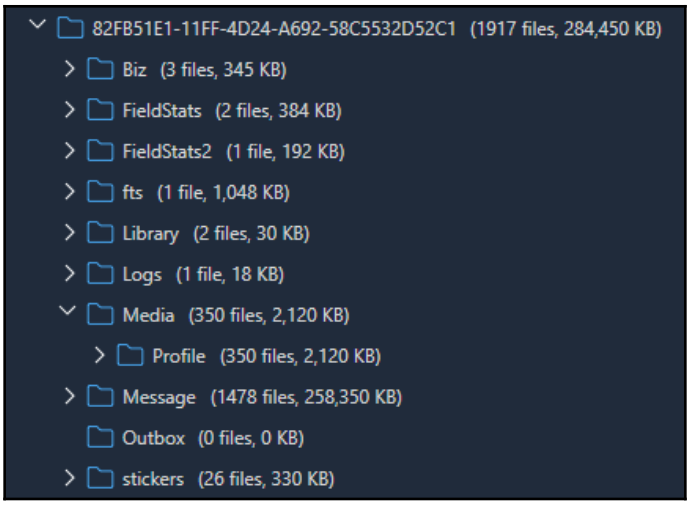
Source	**samsung SM-J710F Full Image - MMCBLK0.raw - Partition 24 (EXT-family, 11.24 GB)\data\com.twitter.android\databases\767674047173918720-58.db**
Recovery Method	**Parsing**
Deleted source	
Location	**Table: users(_id: 1)**
Evidence number	**samsung SM-J710F Full Image - MMCBLK0.raw**

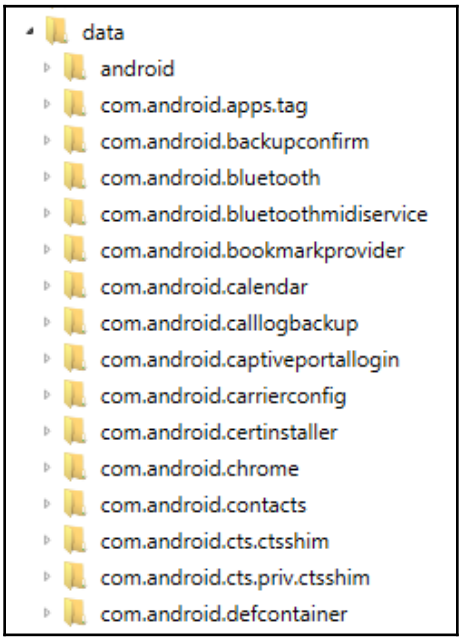
0-scribe.db	File	.db	16,384	1/19/2020 9:29:43 AM	1/19/2020 9:29:43 AM	1/19/2020 3:34:39 PM
0-scribe.db-journal	File	.db-journal	16,928	1/19/2020 9:29:43 AM	1/19/2020 9:29:43 AM	1/19/2020 9:32:27 AM
global.db	File	.db	368,640	1/19/2020 9:29:44 AM	1/19/2020 9:29:44 AM	1/19/2020 11:07:17 AM
global.db-journal	File	.db-journal	12,824	1/19/2020 9:29:44 AM	1/19/2020 9:29:44 AM	1/19/2020 9:32:00 AM
0-58.db	File	.db	454,656	1/19/2020 9:29:44 AM	1/19/2020 9:29:44 AM	1/19/2020 9:29:45 AM
0-58.db-journal	File	.db-journal	8,720	1/19/2020 9:29:44 AM	1/19/2020 9:29:44 AM	1/19/2020 9:29:45 AM
767674047173918720-lru_key_value.db	File	.db	28,672	1/19/2020 9:31:59 AM	1/19/2020 9:31:59 AM	1/20/2020 6:43:51 AM
767674047173918720-lru_key_value.db-journal	File	.db-journal	21,032	1/19/2020 9:31:59 AM	1/19/2020 9:31:59 AM	1/19/2020 11:07:10 AM
767674047173918720-scribe.db	File	.db	24,576	1/19/2020 9:31:59 AM	1/19/2020 9:31:59 AM	1/20/2020 7:35:38 AM
767674047173918720-scribe.db-journal	File	.db-journal	53,864	1/19/2020 9:31:59 AM	1/19/2020 9:31:59 AM	1/20/2020 7:35:38 AM
767674047173918720-58.db	File	.db	1,814,528	1/19/2020 9:31:59 AM	1/19/2020 9:31:59 AM	1/20/2020 4:13:07 AM
767674047173918720-58.db-journal	File	.db-journal	185,192	1/19/2020 9:31:59 AM	1/19/2020 9:31:59 AM	1/19/2020 11:07:23 AM
767674047173918720-drafts.db	File	.db	28,672	1/19/2020 9:32:00 AM	1/19/2020 9:32:00 AM	1/19/2020 9:32:00 AM
767674047173918720-drafts.db-journal	File	.db-journal	8,720	1/19/2020 9:32:00 AM	1/19/2020 9:32:00 AM	1/19/2020 9:32:00 AM
767674047173918720-dm.db	File	.db	20,480	1/19/2020 9:32:03 AM	1/19/2020 9:32:03 AM	1/19/2020 9:32:03 AM
767674047173918720-dm.db-journal	File	.db-journal	12,824	1/19/2020 9:32:03 AM	1/19/2020 9:32:03 AM	1/19/2020 9:32:03 AM

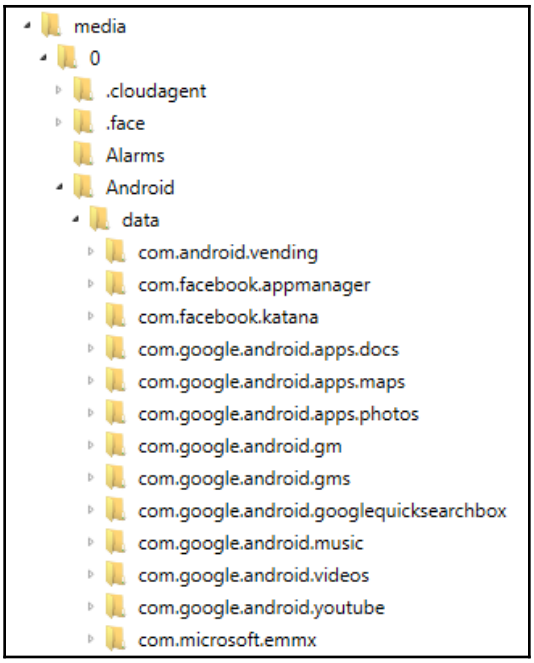


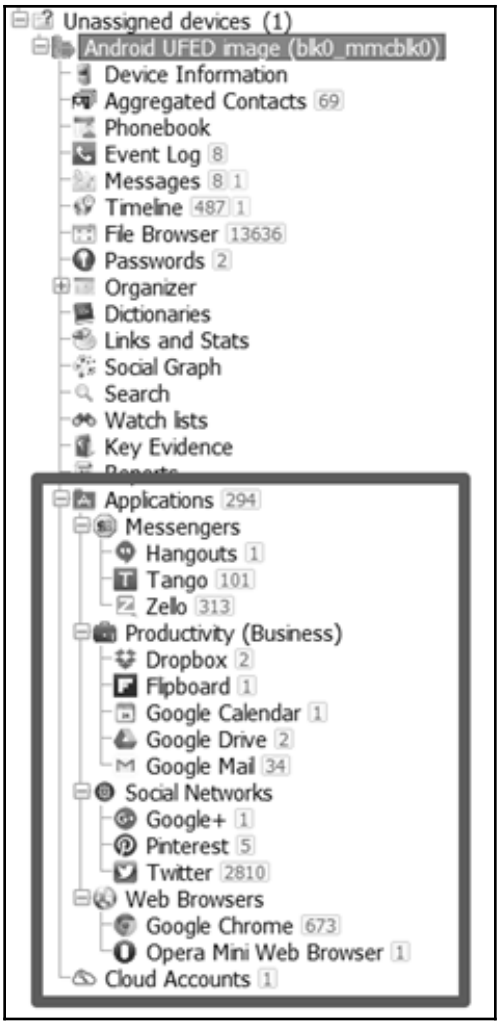

com.twitter.android
app_textures
app_webview
cache
code_cache
databases
files
lib-0
lib-1
lib-2
lib-main
no_backup
shaders
shared_prefs

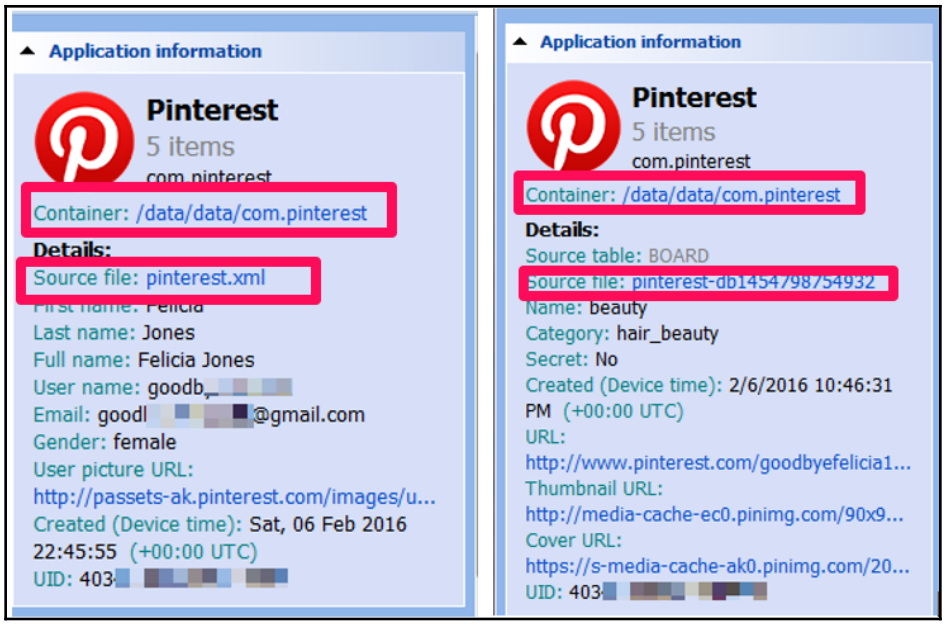

Applications (8678 files, 116,948 KB)
AccountAuthenticationDialog.app (5 files, 63 KB)
ActivityMessagesApp.app (90 files, 346 KB)
AdPlatformsDiagnostics.app (7 files, 79 KB)
AppStore.app (299 files, 27,196 KB)
AskPermissionUI.app (45 files, 65 KB)
AXUIViewService.app (83 files, 99 KB)
BusinessExtensionsWrapper.app (94 files, 1,213 KB)
Camera.app (143 files, 310 KB)
CheckerBoard.app (45 files, 641 KB)
CompassCalibrationViewService.app (44 files, 65 KB)
ContinuityCamera.app (6 files, 214 KB)
CoreAuthUI.app (164 files, 342 KB)
CTCarrierSpaceAuth.app (44 files, 118 KB)
DataActivation.app (45 files, 380 KB)
DDActionsService.app (85 files, 193 KB)
DemoApp.app (8 files, 55 KB)
Diagnostics.app (91 files, 2,782 KB)
DiagnosticsService.app (570 files, 4,592 KB)
DNDBuddy.app (9 files, 106 KB)
Family.app (5 files, 42 KB)
Feedback Assistant iOS.app (136 files, 3,061 KB)
FieldTest.app (10 files, 232 KB)
FindMyiPhone.app (469 files, 5,336 KB)

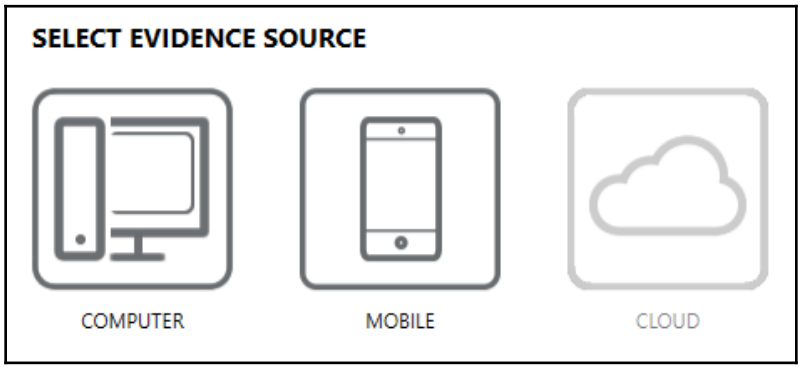

82FB51E1-11FF-4D24-A692-58C5532D52C1 (1917 files, 284,450 KB)
Biz (3 files, 345 KB)
FieldStats (2 files, 384 KB)
FieldStats2 (1 file, 192 KB)
fts (1 file, 1,048 KB)
Library (2 files, 30 KB)
Logs (1 file, 18 KB)
Media (350 files, 2,120 KB)
Profile (350 files, 2,120 KB)
Message (1478 files, 258,350 KB)
Outbox (0 files, 0 KB)
stickers (26 files, 330 KB)


data
android
com.android.apps.tag
com.android.backupconfirm
com.android.bluetooth
com.android.bluetoothmidiservice
com.android.bookmarkprovider
com.android.calendar
com.android.calllogbackup
com.android.captiveportallogin
com.android.carrierconfig
com.android.certinstaller
com.android.chrome
com.android.contacts
com.android.cts.ctsshim
com.android.cts.priv.ctsshim
com.android.defcontainer

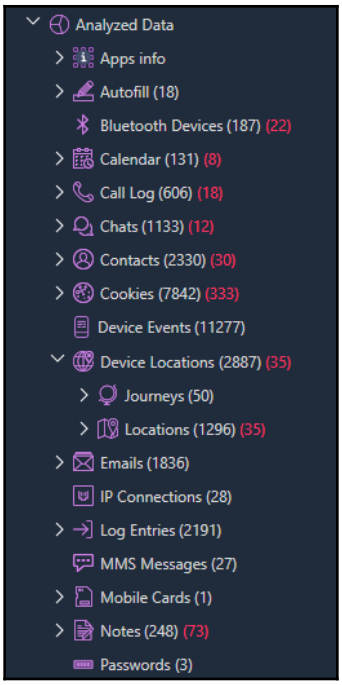

media
0
.cloudagent
.face
Alarms
Android
data
com.android.vending
com.facebook.appmanager
com.facebook.katana
com.google.android.apps.docs
com.google.android.apps.maps
com.google.android.apps.photos
com.google.android.gm
com.google.android.gms
com.google.android.googlequicksearchbox
com.google.android.music
com.google.android.videos
com.google.android.youtube
com.microsoft.emmx

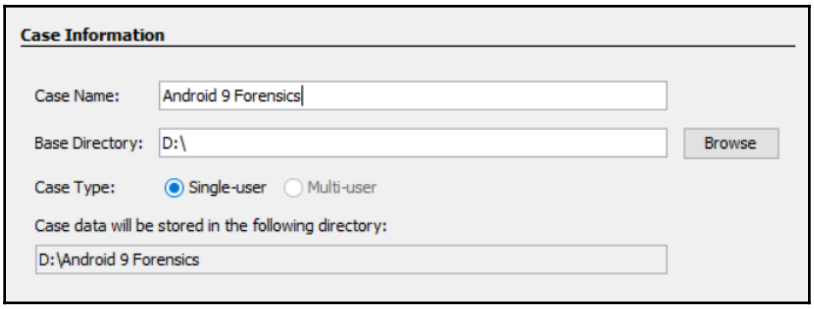

Unassigned devices (1)
Android UFED image (blk0_mmcblk0)
Device Information
Aggregated Contacts 69
Phonebook
Event Log 8
Messages 8 1
Timeline 487 1
File Browser 13636
Passwords 2
Organizer
Dictionaries
Links and Stats
Social Graph
Search
Watch lists
Key Evidence
Applications 294
Messengers
Hangouts 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

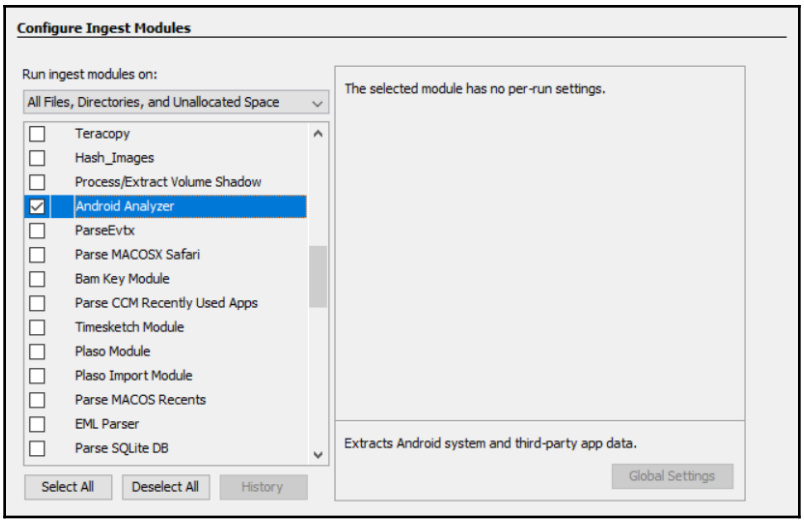

Application information
Pinterest
5 items
com.pinterest
Container: /data/data/com.pinterest
Details:
Source file: pinterest.xml
Last name: Jones
Full name: Felicia Jones
User name: goodb
Email: goodl @gmail.com
Gender: female
User picture URL:
http://passets-ak.pinterest.com/images/u...
Created (Device 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

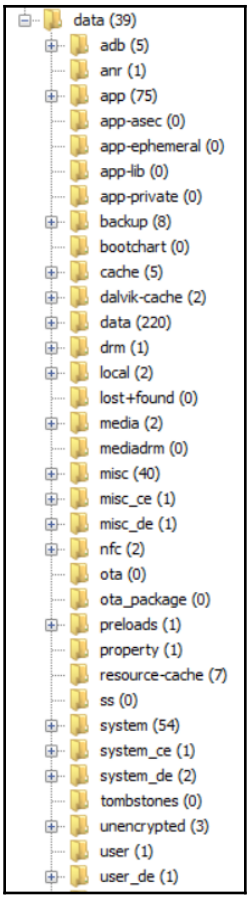

SELECT EVIDENCE SOURCE
COMPUTER
MOBILE
CLOUD

WEB RELATED	**26,890**
CHAT	**129,310**
Facebook Messenger Groups	2
Facebook Messenger Messages	1
iOS iMessage/SMS/MMS	16,222
iOS Telegram Channel Chats	224
iOS Telegram Chats	210
iOS Telegram Messages	95,738
iOS Telegram Users	8,780
iOS WhatsApp Chats	176
iOS WhatsApp Contacts	405
iOS WhatsApp Groups	10
iOS WhatsApp Messages	7,426
Textfree Attachments	112
Textfree Messages / Calls	4
SOCIAL NETWORKING	**3,295**
MEDIA	**43,947**


Analyzed Data
Apps info
Autofill (18)
Bluetooth Devices (187) (22)
Calendar (131) (8)
Call Log (606) (18)
Chats (1133) (12)
Contacts (2330) (30)
Cookies (7842) (333)
Device Events (11277)
Device Locations (2887) (35)
Journeys (50)
Locations (1296) (35)
Emails (1836)
IP Connections (28)
Log Entries (2191)
MMS Messages (27)
Mobile Cards (1)
Notes (248) (73)
Passwords (3)


Case Information
Case Name:
Android 9 Forensics
Base Directory:
D:\
Browse
Case Type:
Single-user
Multi-user
Case data will be stored in the following directory:
D:\Android 9 Forensics


Configure Ingest Modules
Run ingest modules on:
All Files, Directories, and Unallocated Space
Teracopy
Hash_Images
Process/Extract Volume Shadow
Android Analyzer
ParseEvtx
Parse MACOSX Safari
Bam Key Module
Parse CCM Recently Used Apps
Timesketch Module
Plaso Module
Plaso Import Module
Parse MACOS Recents
EML Parser
Parse SQLite DB
Select All
Deselect All
History
The selected module has no per-run settings.
Extracts Android system and third-party app data.
Global Settings



Source File	S	C	Direction	To Phone Number	Date/Time	Read	Subject	Text	Message Type
mmssms.db			Outgoing	244444	2019-02-14 04:28:58 MSK	Read		(wYBvgVoFlymq) Google is verifying the phone# of this de...	SMS Message
mmssms.db			Incoming		2019-02-14 05:06:25 MSK	Read		<#> Your WhatsApp code: 657-825You can also tap on thi...	SMS Message
mmssms.db			Incoming		2019-02-14 05:08:46 MSK	Read		WeChat verification code (1948) may only be used once to...	SMS Message
mmssms.db			Incoming		2019-02-14 05:10:46 MSK	Read		Verification code: 3444. The code is only used for removing...	SMS Message
mmssms.db			Incoming		2019-02-14 05:16:38 MSK	Read		Verification code: 3444. The code is only used for removing...	SMS Message
mmssms.db			Incoming		2019-02-14 05:19:13 MSK	Unread		<#> Your Signal verification code: 486-734doDiFGKPO1r	SMS Message
mmssms.db			Incoming		2019-02-14 05:20:24 MSK	Read		LINE OTP Service: Please enter 5189 into LINE within the n...	SMS Message
mmssms.db			Incoming		2019-02-14 05:25:53 MSK	Read		[#][TikTok] 8933 is your verification codefJpzQvK2eu1	SMS Message
mmssms.db			Incoming		2019-02-14 05:26:52 MSK	Read		Your imo code is 21399K+9OFePKE9	SMS Message
mmssms.db			Incoming		2019-02-14 05:33:25 MSK	Read		549556 is your Messenger code to verify your phone number	SMS Message