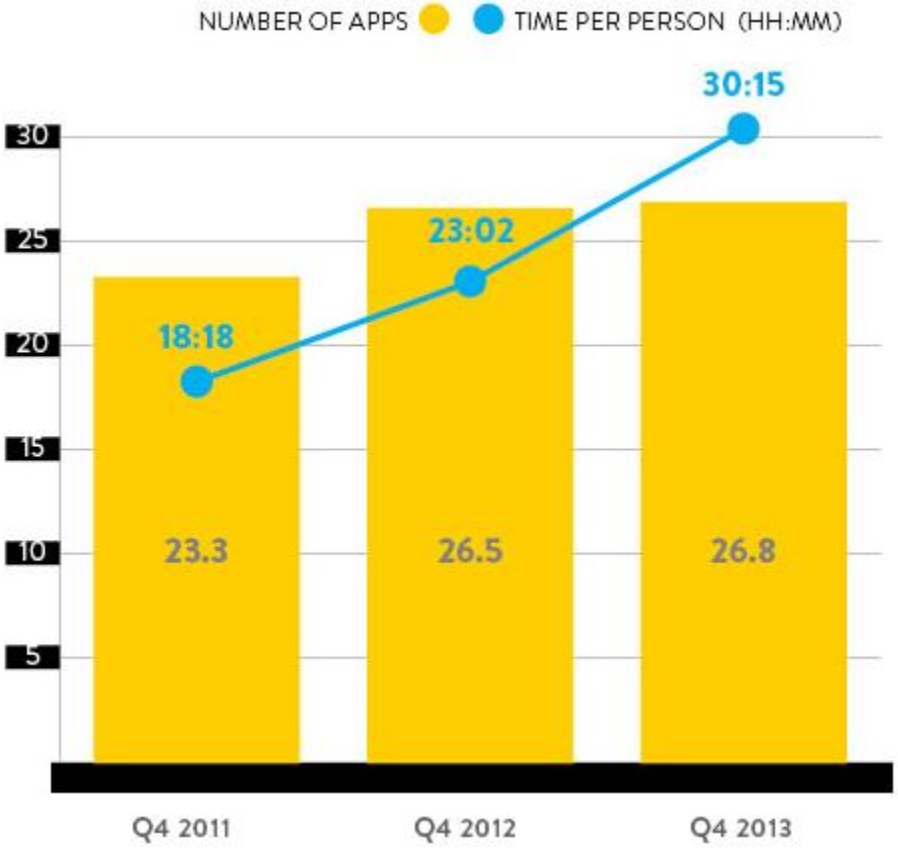
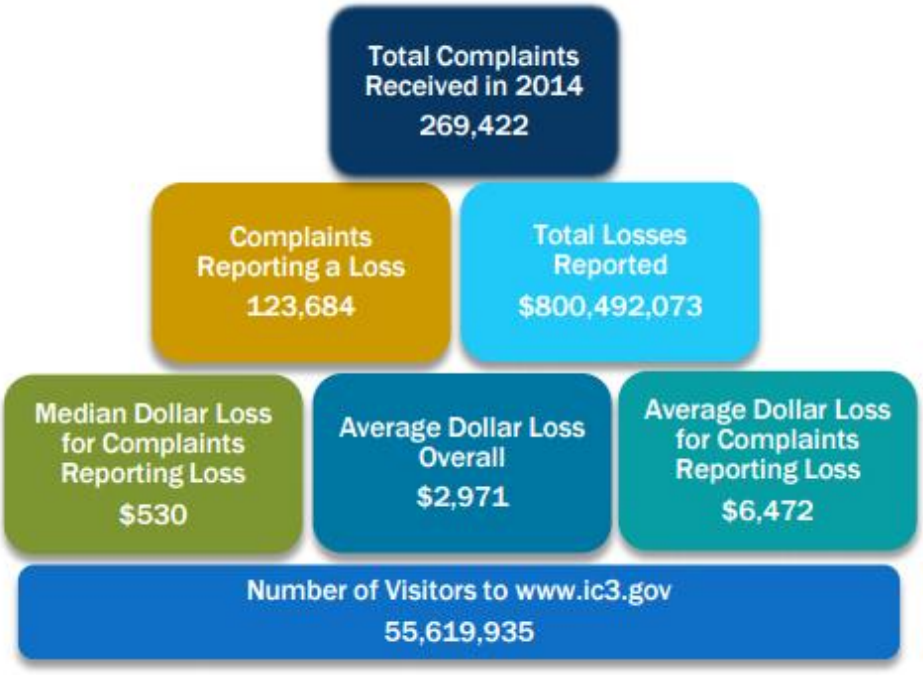
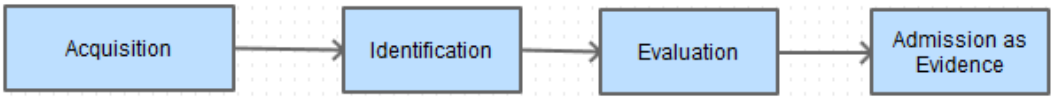
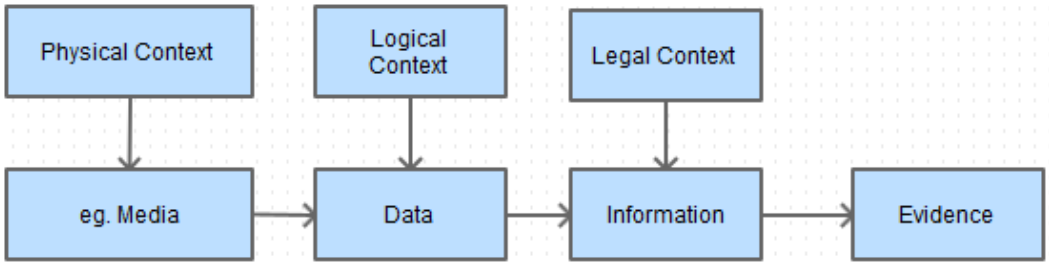
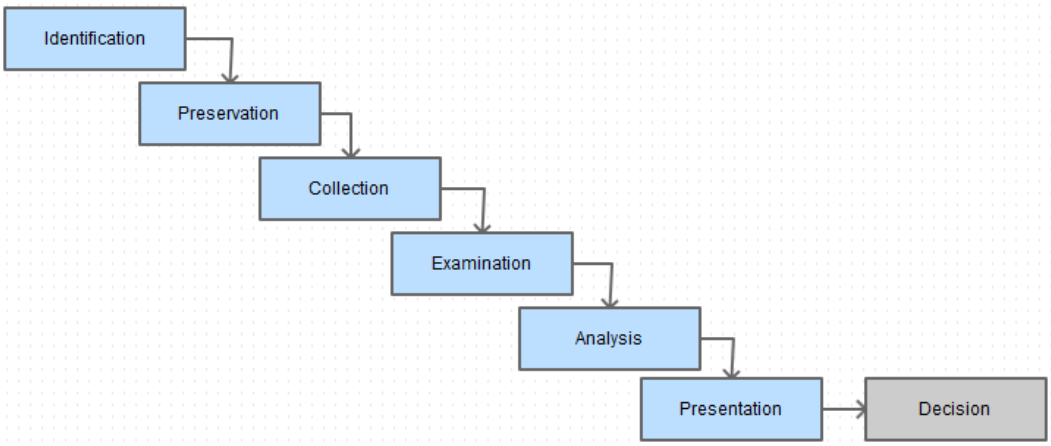
Chapter 1: Mobile Forensics and the Investigation Process Model

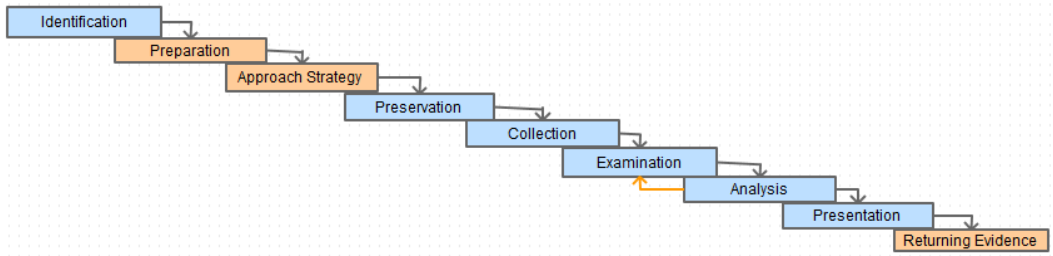


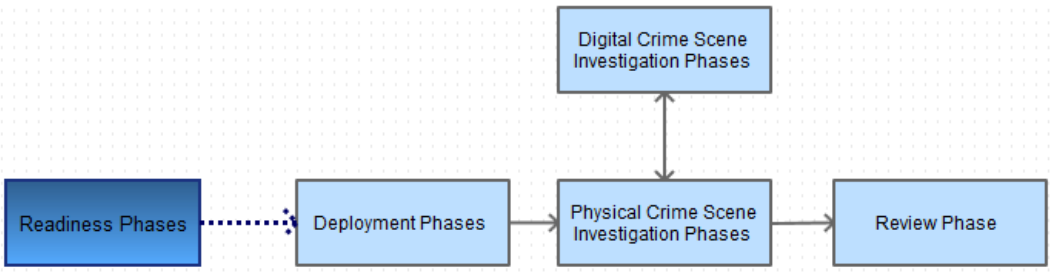

Total Complaints Received in 2014
269,422
Complaints Reporting a Loss
123,684
Total Losses Reported
$800,492,073
Median Dollar Loss for Complaints Reporting Loss
$530
Average Dollar Loss Overall
$2,971
Average Dollar Loss for Complaints Reporting Loss
$6,472
Number of Visitors to www.ic3.gov
55,619,935

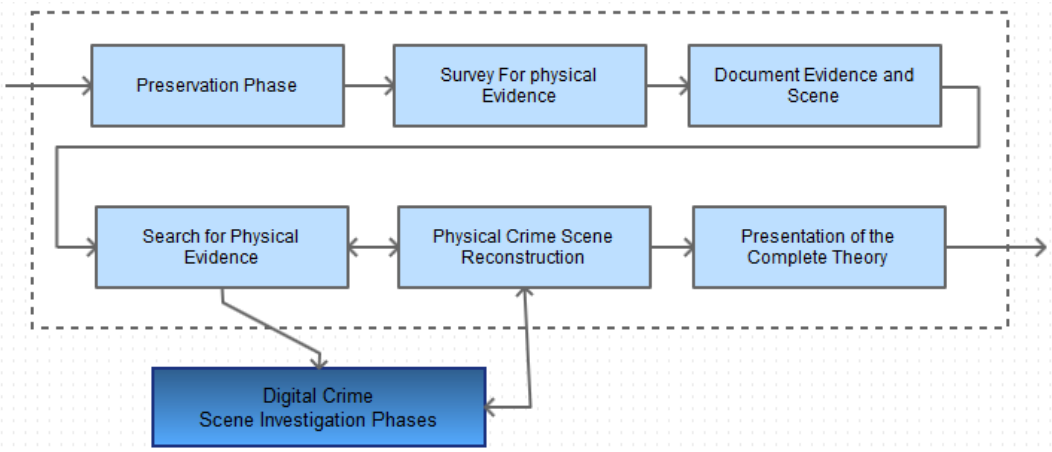

Acquisition
Identification
Evaluation
Admission as Evidence

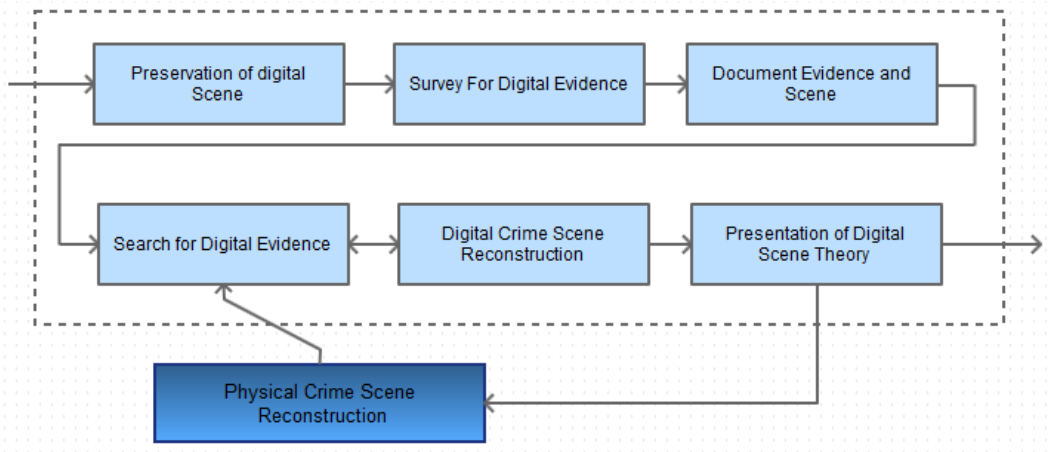

Physical Context
Logical Context
Legal Context
eg. Media
Data
Information
Evidence

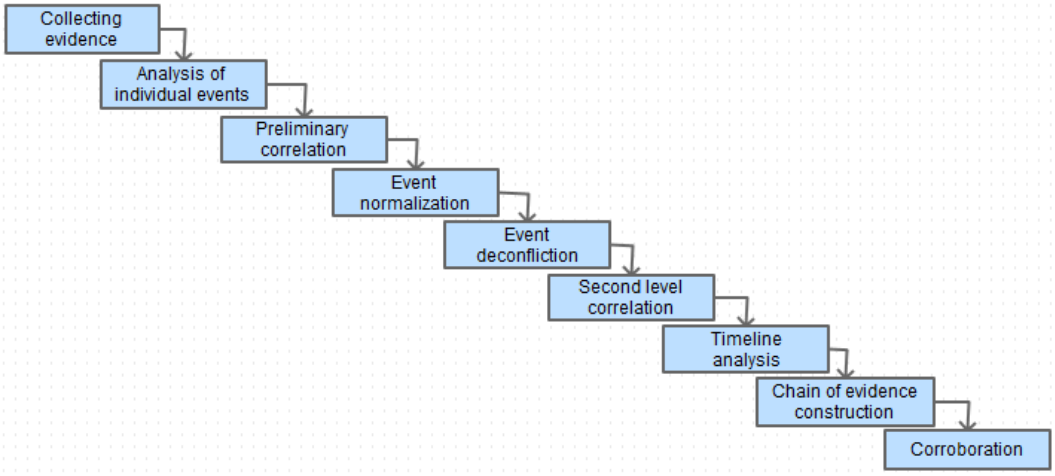

Identification
Preservation
Collection
Examination
Analysis
Presentation
Decision

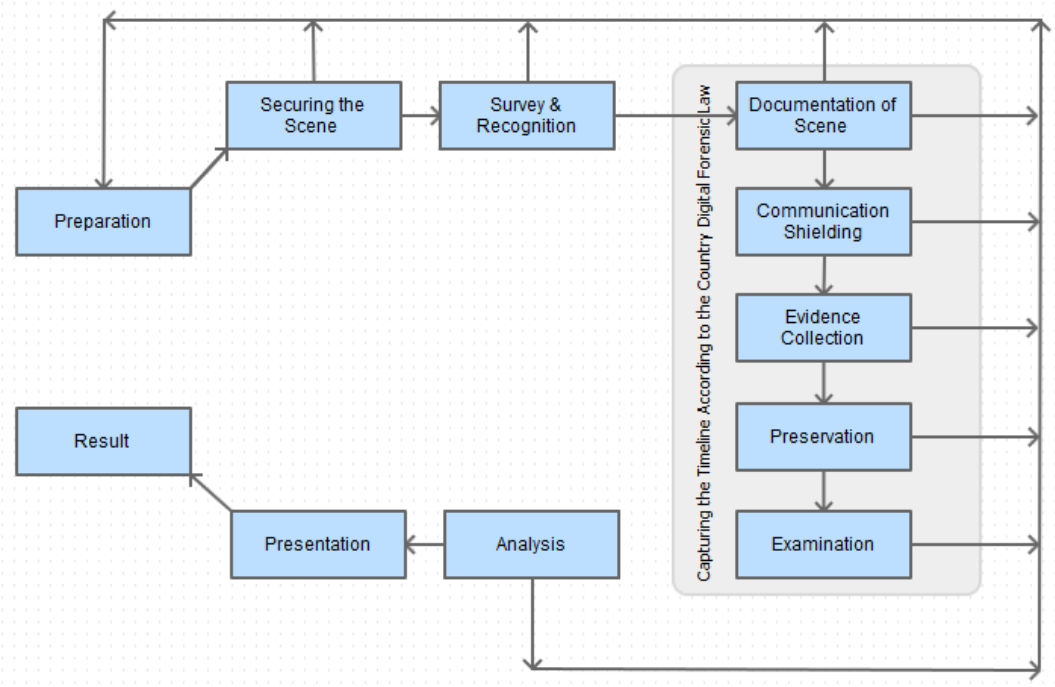

Identification
Preparation
Approach Strategy
Preservation
Collection
Examination
Analysis
Presentation
Returning Evidence


Digital Crime Scene Investigation Phases
Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Review Phase

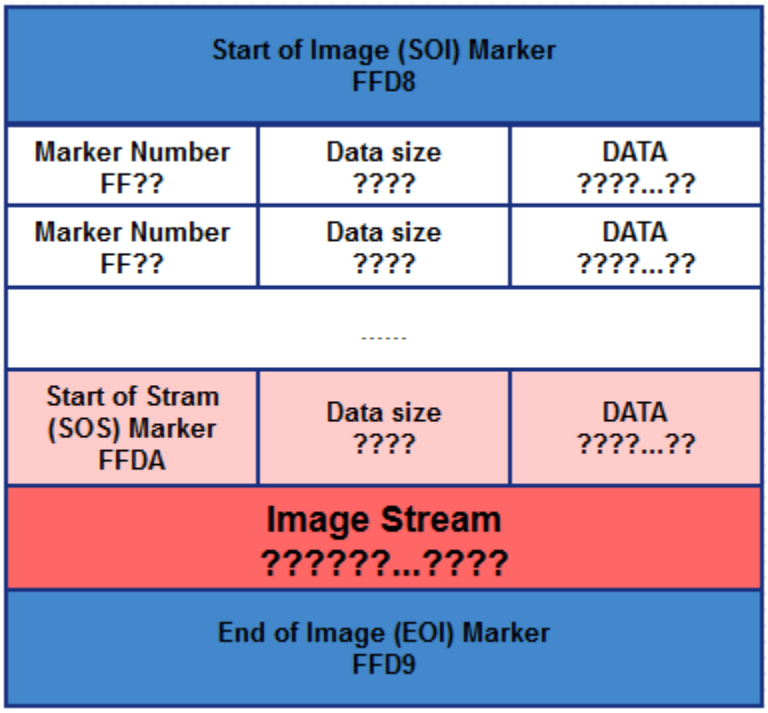

Preservation Phase
Survey For physical Evidence
Document Evidence and Scene
Search for Physical Evidence
Physical Crime Scene Reconstruction
Presentation of the Complete Theory
Digital Crime Scene Investigation Phases

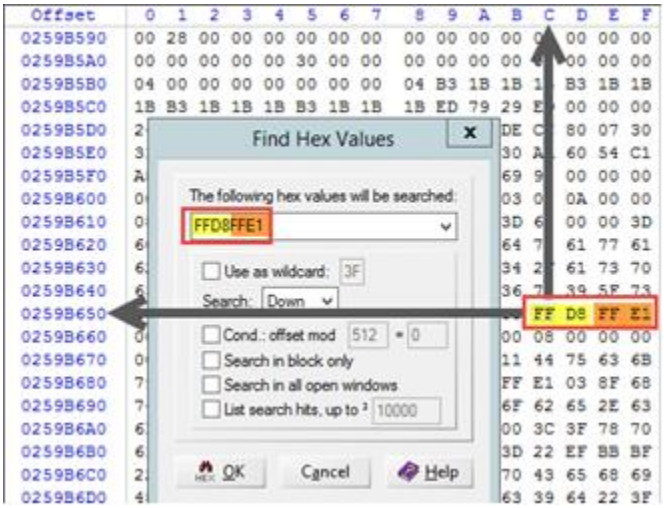

Preservation of digital Scene
Survey For Digital Evidence
Document Evidence and Scene
Search for Digital Evidence
Digital Crime Scene Reconstruction
Presentation of Digital Scene Theory
Physical Crime Scene Reconstruction


Collecting evidence
Analysis of individual events
Preliminary correlation
Event normalization
Event deconfliction
Second level correlation
Timeline analysis
Chain of evidence construction
Corroboration

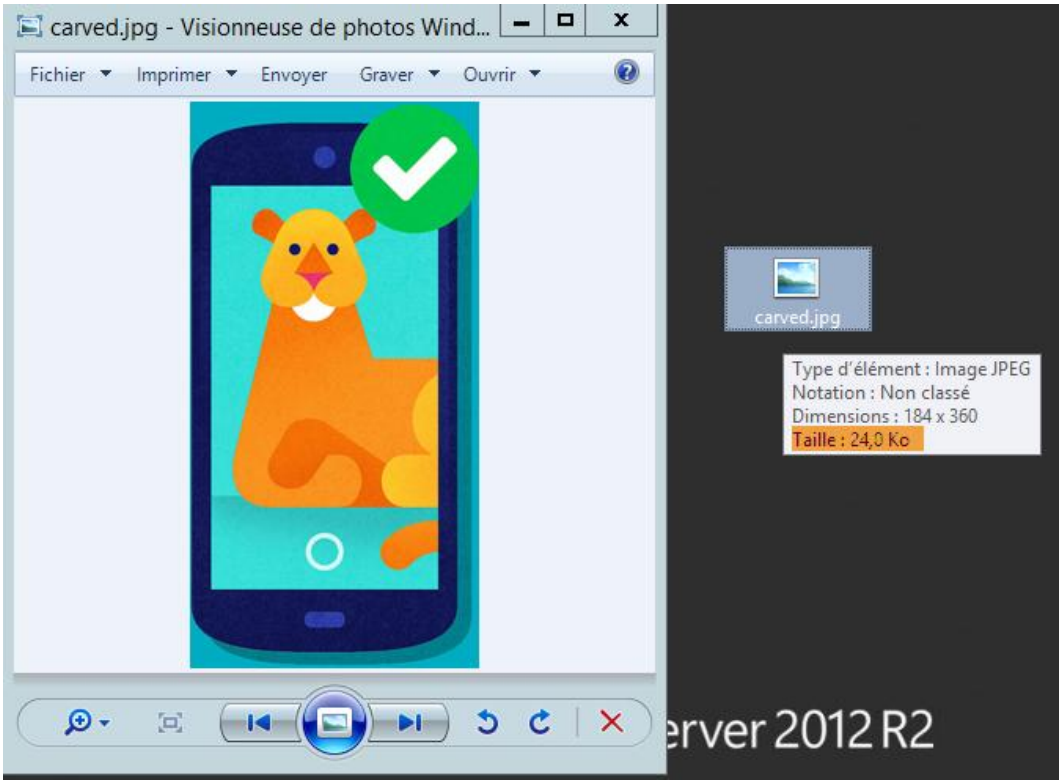

Preparation
Securing the Scene
Survey & Recognition
Documentation of Scene
Communication Shielding
Evidence Collection
Preservation
Examination
Capturing the Timeline According to the Country Digital Forensic Law
Analysis
Presentation
Result

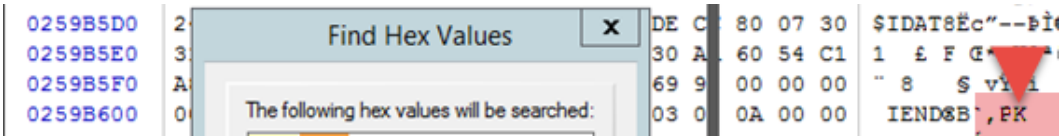
Chapter 2: Do It Yourself – Low-Level Techniques





Offset	0	1	2	3	4	5	6	7	8	9
025A1660	DA	9E	2A	57	3C	1E	E4	07	D0	D4
025A1670	27	34	DD	00	B6	36	B6	16	36	C1
025A1680	01	F5	E3	19	9A	C0	DB	82	86	F9
025A1690	D6	24	A0	42	50	21	7F	FF	D9	50
025A16A0	08	00	00	80	34	22	44	4A	68	A5





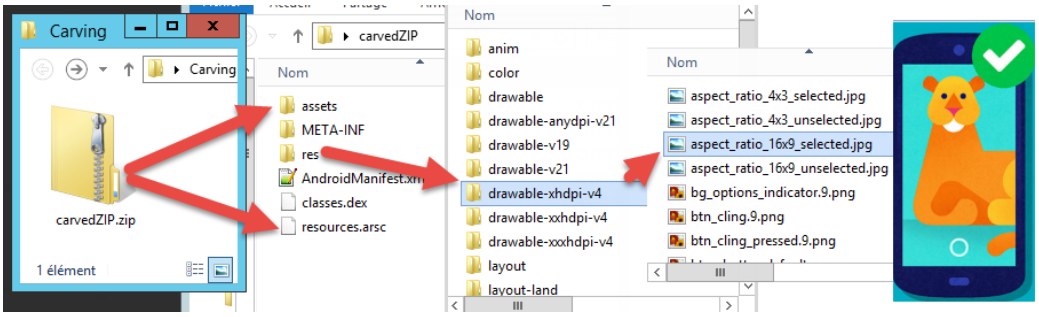
```
0259B600   00 49 45 4E 44 AE 42 60   82 50 4B 03 04 0A 00 00   IEND®B`‚PK
0259B610   08 00 00 80 34 22 44 D3   4E 43 3A 3D 60 00 00 3D     €4"DÓNC:=`  =
0259B620   60 00 00 34 00 01 00 72   65 73 2F 64 72 61 77 61   `  4   res/drawa
```

Local File Header	File Data 1	Data Descriptor 1	Archive Decryption Header	Archive Extra Data Record	Central Directory

---

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0000	Signature				Version		Flags		Compression		Mod time		Mode date		Crc-32	
0x0010	Crc-32				Compressed size				Uncompressed size				File name len		Extra field len	
0x0020	File name (variable size)															
0x0030	Extra field (variable size)															

```
0259B5F0  A8 02 38 00 00 1D A7 01  76 9F FA 69 90 00 00 00  ¨ 8   § vŸúi
0259B600  00 49 45 4E 44 AE 42 60  82 50 4B 03 04 0A 00 00   IEND®B`,PK
0259B610  08 00 00 80 34 22 44 D3  4E 43 3A 3D 60 00 00 3D  €4"DÓNC:=`  =
0259B620  60 00 00 34 00 01 00 72  65 73 2F 64 72 61 77 61  `  4  res/drawa
0259B630  62 6C 65 2D 78 68 64 70  69 2D 76 34 2F 61 73 70  ble-xhdpi-v4/asp
0259B640  65 63 74 5F 72 61 74 69  6F 5F 31 36 78 39 5F 73  ect_ratio_16x9_s
0259B650  65 6C 65 63 74 65 64 2E  6A 70 67 00 FF D8 FF E1  elected.jpg ÿØÿá
0259B660  00 18 45 78 69 66 00 00  49 49 2A 00 08 00 00 00    Exif  II*
0259B670  00 00 00 00 00 00 00 00  FF EC 00 11 44 75 63 6B          ÿì  Duck
0259B680  79 00 01 00 04 00 00 00  49 00 00 FF E1 03 8F 68  y       I  ÿá  h
0259B690  74 74 70 3A 2F 2F 6E 73  2E 61 64 6F 62 65 2E 63  ttp://ns.adobe.c
```



Address: Boulevard Al Qods, Casablanca, Moroc

Get GPS Coordinates

DD (decimal degrees)*

Latitude: 33.5336731

Longitude: -7.656986111111111

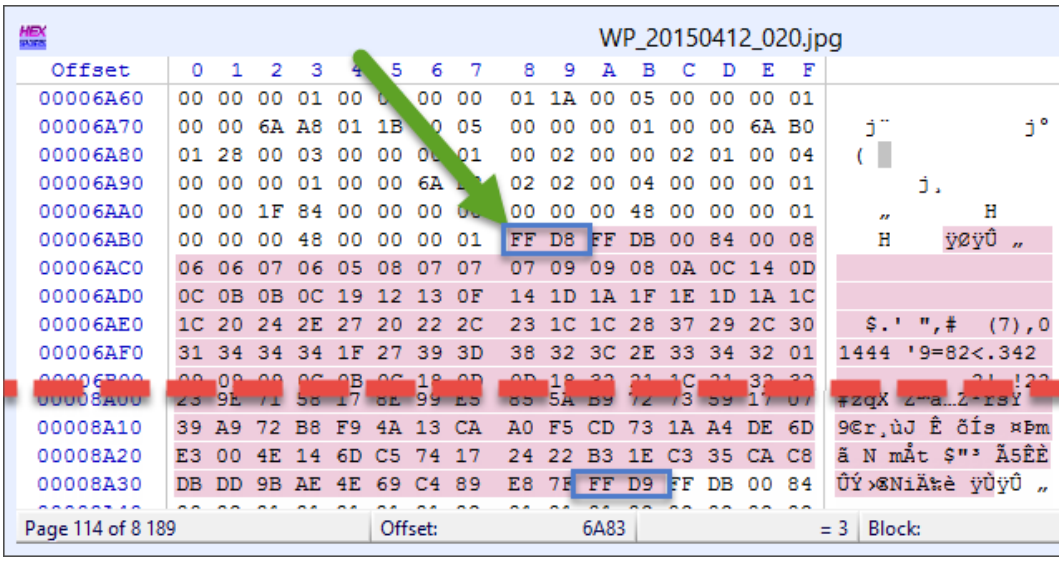
Get Address

DMS (degrees, minutes, secondes)*

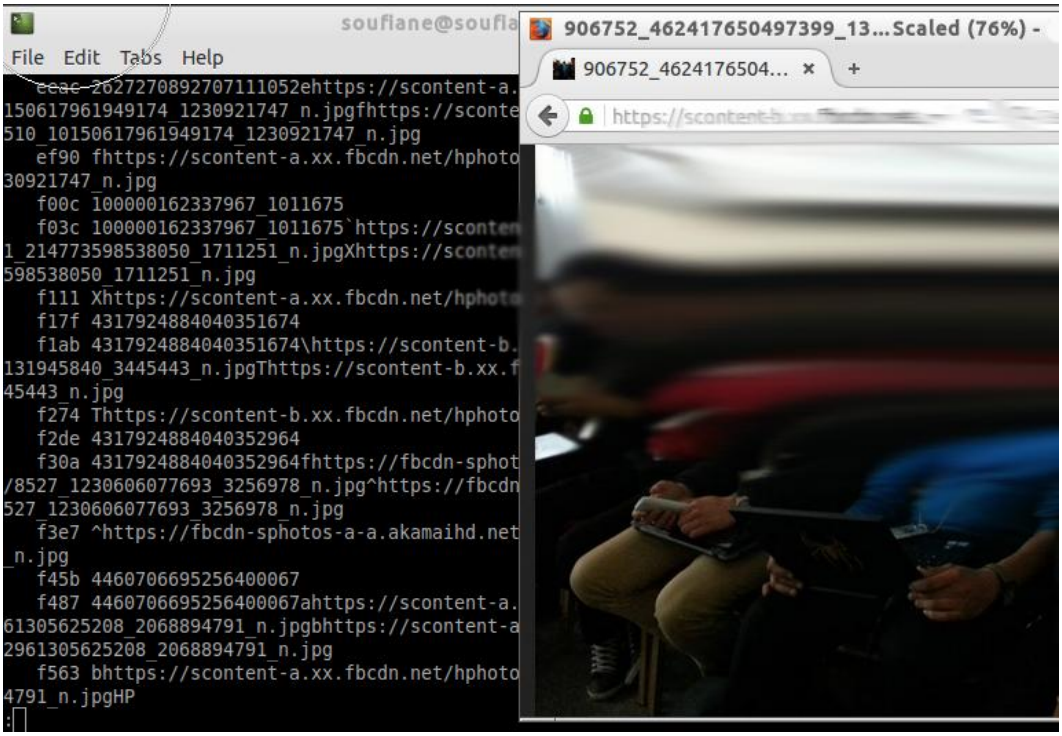
Latitude: N S 33 ° 32 ' 1.223 "

Longitude: E W 7 ° 39 ' 25.15 "

Get Address



```
soufiane@soufiane-VirtualBox:~/Desktop$ strings --all --radix=x bin.bin
      6 Exif
     7e Adobe Photoshop CC 2015 (Windows)
     a0 2015:11:20 13:39:18
    144 Adobe_CM
    152 Adobe
   3f8c .gam
   3fe2 '54,u0
   4002 ?sSoufiane Tahiri : Passw0rd is hidden in a piccr
   408f E0juPS
   40ee U9\>oo
```



```
soufiane@soufiane-VirtualBox:~$ grep -E -o "\b[a-zA-Z0-9.-]+@[a-zA-Z0-9.-]+\.[a-zA-Z0-9.-]+\b" -R  /home/soufiane/Desktop/ddWP/lumia/
/home/soufiane/Desktop/ddWP/lumia/Lumia001.txt:[redacted]@6.14
/home/soufiane/Desktop/ddWP/lumia/Lumia002.txt:[redacted]@spiderweb.com.auwhatever
/home/soufiane/Desktop/ddWP/lumia/Lumia002.txt:[redacted]@apostrophiclab.com
/home/soufiane/Desktop/ddWP/lumia/Lumia002.txt:[redacted]@yahoo.com
/home/soufiane/Desktop/ddWP/lumia/Lumia002.txt:[redacted]
/home/soufiane/Desktop/ddWP/lumia/Lumia002.txt:[redacted]@gmail.com
/home/soufiane/Desktop/ddWP/lumia/Lumia002.txt:[redacted]@cadorian.com
/home/soufiane/Desktop/ddWP/lumia/Lumia002.txt:[redacted]@themantisstudio.com
/home/soufiane/Desktop/ddWP/lumia/Lumia002.txt:[redacted]@cadorian.com
/home/soufiane/Desktop/ddWP/lumia/Lumia002.txt:[redacted]
/home/soufiane/Desktop/ddWP/lumia/Lumia002.txt:[redacted]
/home/soufiane/Desktop/ddWP/lumia/Lumia003.txt:[redacted]@gmail.com
/home/soufiane/Desktop/ddWP/lumia/Lumia004.txt:[redacted]@cadorian.com
/home/soufiane/Desktop/ddWP/lumia/Lumia004.txt:[redacted]
/home/soufiane/Desktop/ddWP/lumia/Lumia004.txt:p-support@whatsapp.com
/home/soufiane/Desktop/ddWP/lumia/Lumia005.txt:p-support@whatsapp.com
/home/soufiane/Desktop/ddWP/lumia/Lumia005.txt:[redacted]@hotmail.fr
/home/soufiane/Desktop/ddWP/lumia/Lumia005.txt:[redacted]@gmail.com
/home/soufiane/Desktop/ddWP/lumia/Lumia005.txt:[redacted]@gmail.com
/home/soufiane/Desktop/ddWP/lumia/Lumia005.txt:[redacted]@microsoft.com
```

Encrypt or Decrypt:

Decrypt

Chaining mode:

Electronic Code Book (ECB)

Keysize:

256 Bits

Key (hex values):

5575D3F563CB24BFDF55CFE252F857E4235CD23E645FAE5B235CD23E645FAE5B

Message to decrypt (hex values):

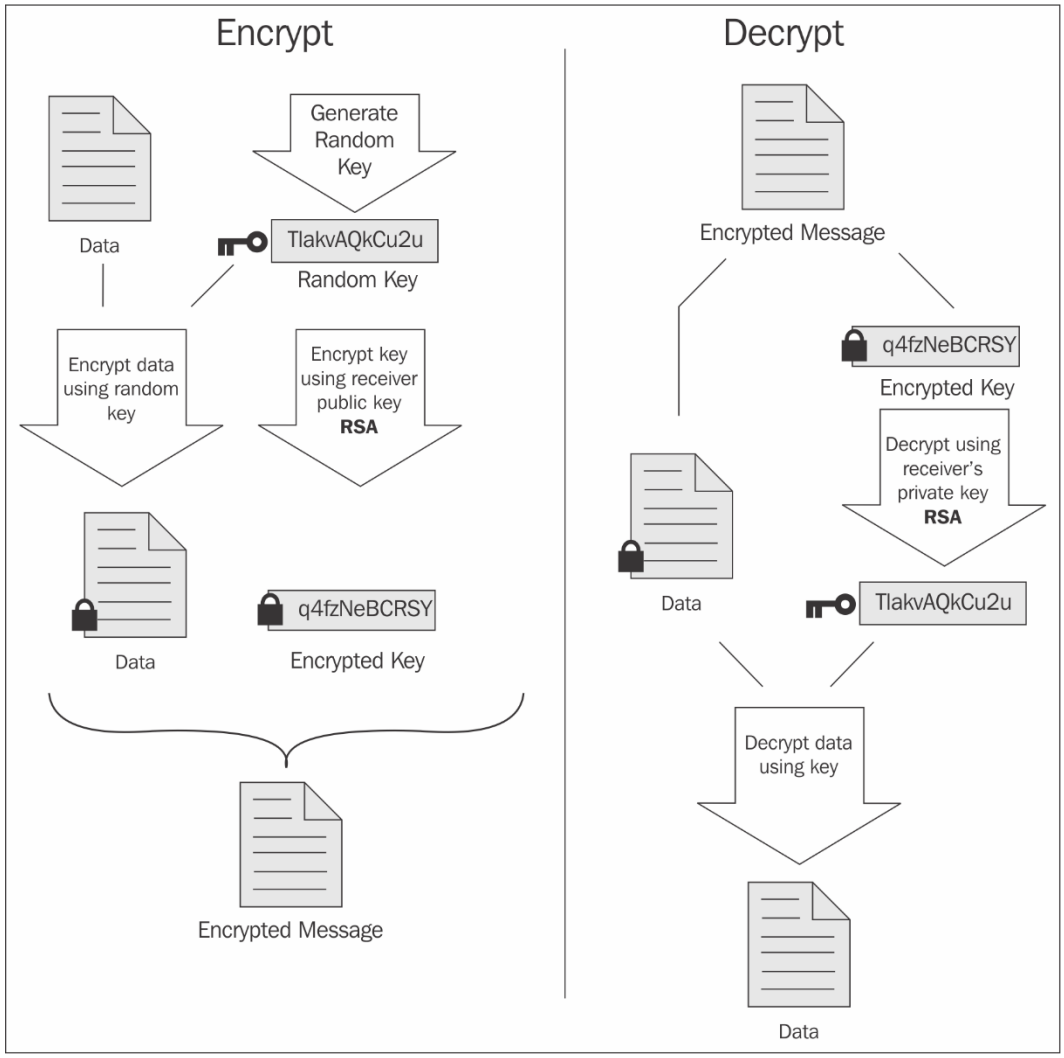
18 35 E2 EB F3 93 D7 34 DE 47 CF 52 2F 4F 4A 28 E4 F8 2D 01 C9 7B 73 8A 28 C9 87 C1 3B 05 FF 8D

Message to decrypt (hex values):

18 35 E2 EB F3 93 D7 34 DE 47 CF 52 2F 4F 4A 28 E4 F8 2D 01 C9 7B 73 8A 28 C9 87 C1 3B 05 FF 8D

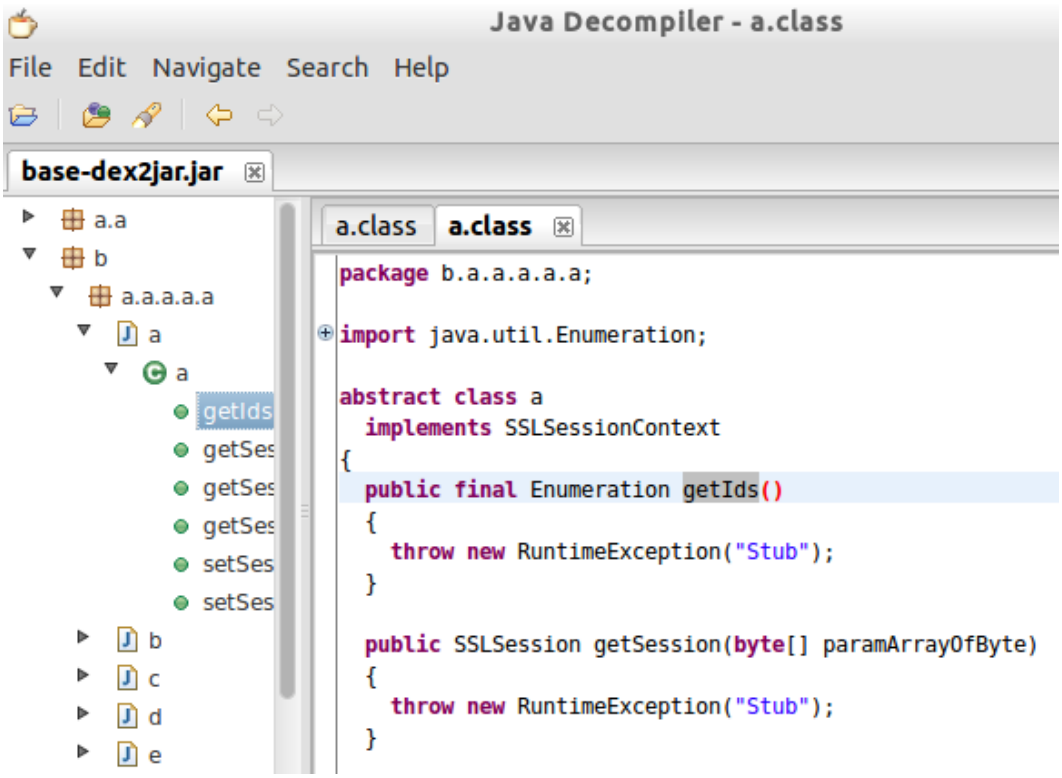
AES Output:

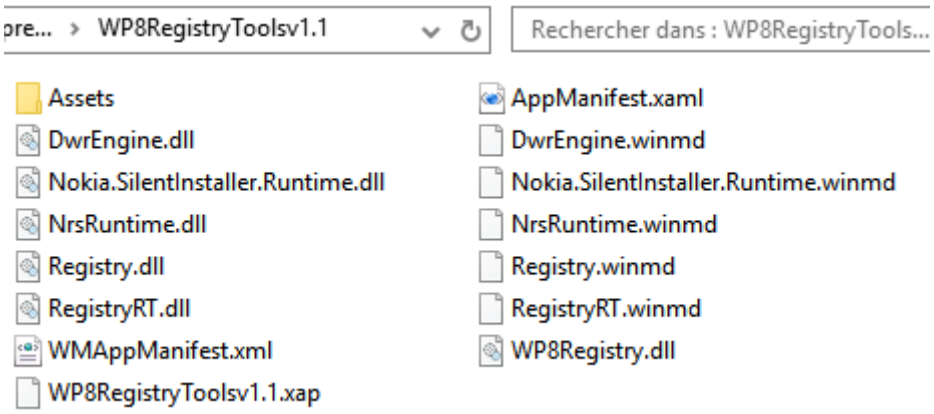
soufianetahiri@gmail.com

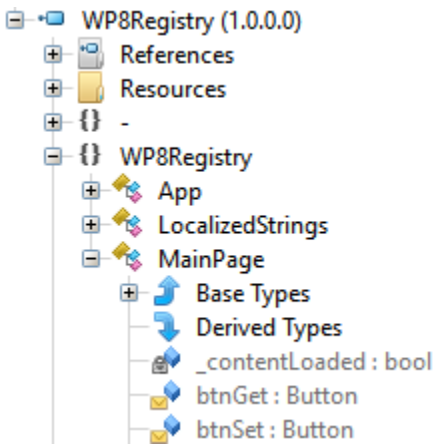


```
soufiane@soufiane-VirtualBox:~$ pgpdump /home/soufiane/Desktop/artifact.txt.gpg
Old: Public-Key Encrypted Session Key Packet(tag 1)(268 bytes)
        New version(3)
        Key ID - 0x3CF480556B845507
        Pub alg - RSA Encrypt or Sign(pub 1)
        RSA m^e mod n(2048 bits) - ...
                -> m = sym alg(1 byte) + checksum(2 bytes) + PKCS-1 block type 02
New: Symmetrically Encrypted and MDC Packet(tag 18)(95 bytes)
        Ver 1
        Encrypted data [sym alg is specified in pub-key encrypted session key]
                (plain text + MDC SHA1(20 bytes))
```

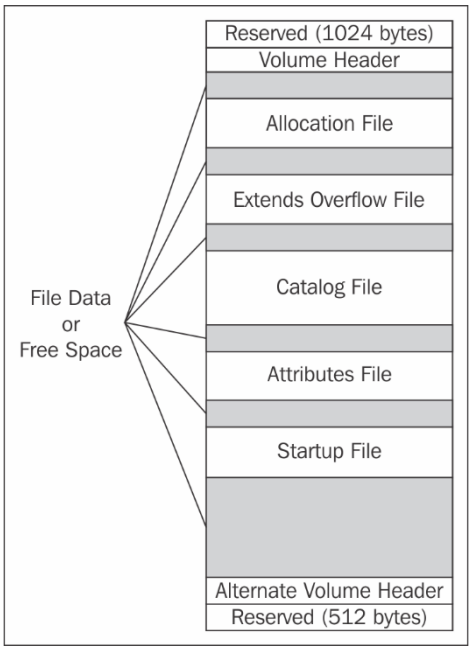
Name	Description
jsr-305	folder
META-INF	folder
res	folder
AndroidManifest.xml	XML document
base.apk	Android package
classes.dex	unknown
resources.arsc	unknown

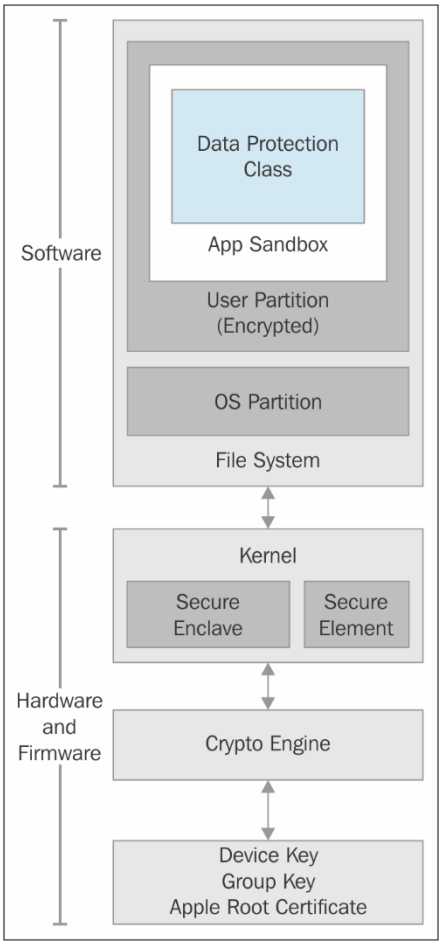


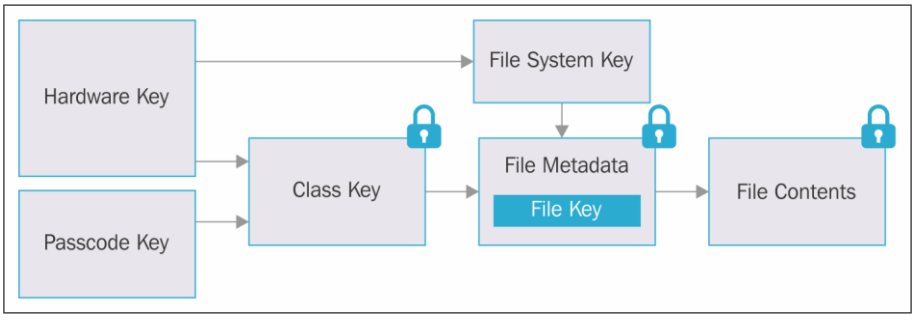

pre... › WP8RegistryToolsv1.1
Rechercher dans : WP8RegistryTools...
Assets
DwrEngine.dll
Nokia.SilentInstaller.Runtime.dll
NrsRuntime.dll
Registry.dll
RegistryRT.dll
WMAppManifest.xml
WP8RegistryToolsv1.1.xap
AppManifest.xaml
DwrEngine.winmd
Nokia.SilentInstaller.Runtime.winmd
NrsRuntime.winmd
Registry.winmd
RegistryRT.winmd
WP8Registry.dll

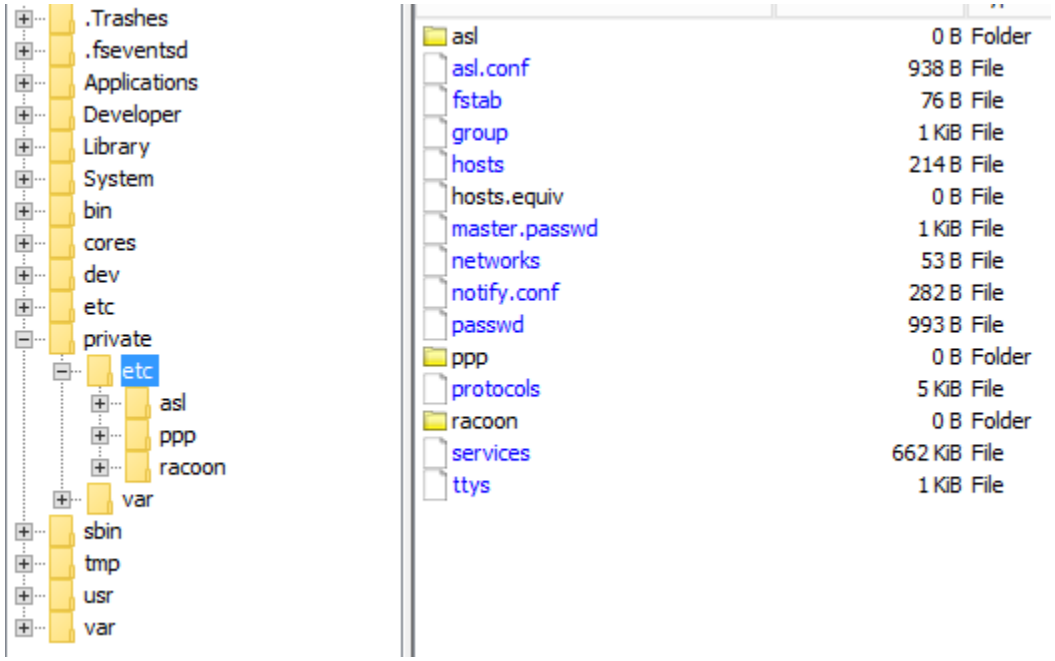

WP8Registry (1.0.0.0)
References
Resources
-
WP8Registry
App
LocalizedStrings
MainPage
Base Types
Derived Types
_contentLoaded : bool
btnGet : Button
btnSet : Button

Chapter 3: iDevices from a Forensic Point of View



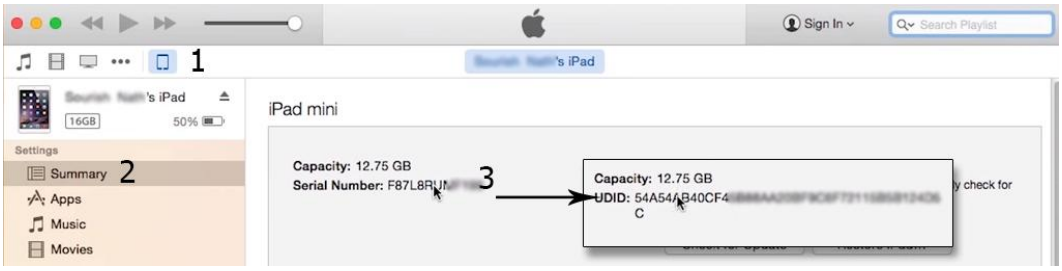

Software
Data Protection Class
App Sandbox
User Partition (Encrypted)
OS Partition
File System
Kernel
Secure Enclave
Secure Element
Hardware and Firmware
Crypto Engine
Device Key
Group Key
Apple Root Certificate

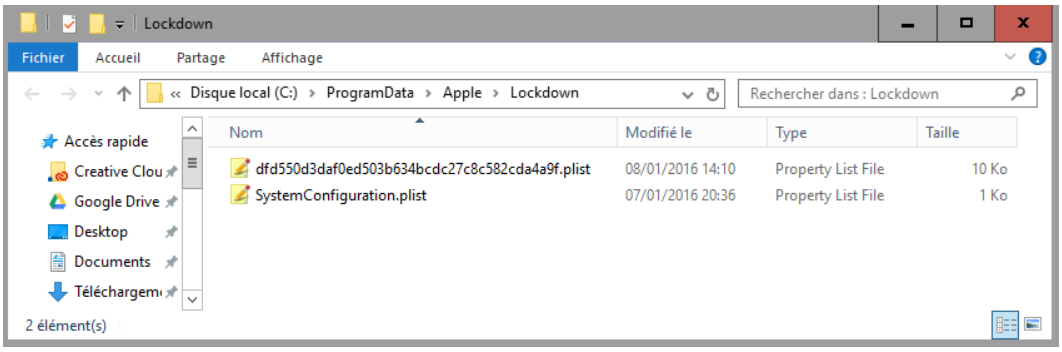

Hardware Key
Passcode Key
File System Key
Class Key
File Metadata
File Key
File Contents

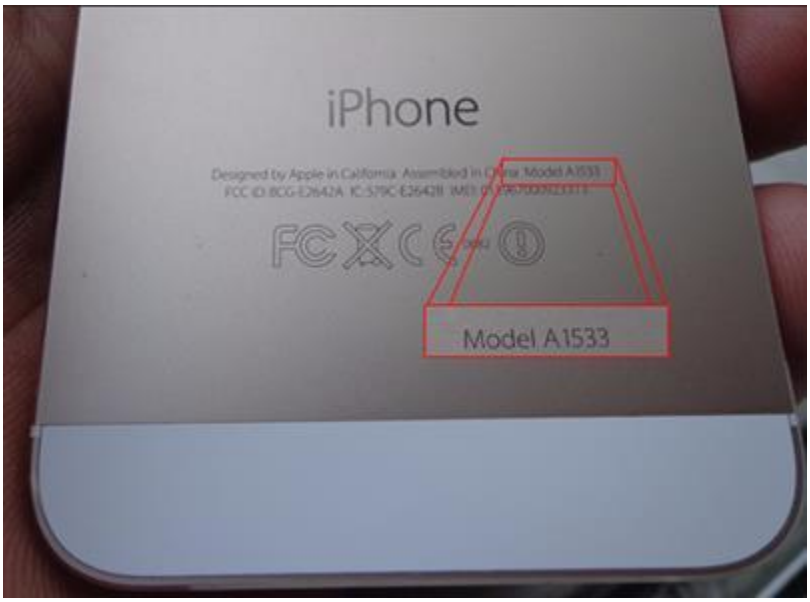


```
##
# User Database
#
# This file is the authoritative user database.
##
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:/smx7MYTQIi2M:0:0:System Administrator:/var/root:/bin/sh
mobile:/smx7MYTQIi2M:501:501:Mobile User:/var/mobile:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
_ftp:*:98:-2:FTP Daemon:/var/empty:/usr/bin/false
_networkd:*:24:24:Network Services:/var/networkd:/usr/bin/false
_wireless:*:25:25:Wireless Services:/var/wireless:/usr/bin/false
_neagent:*:34:34:NEAgent:/var/empty:/usr/bin/false
_securityd:*:64:64:securityd:/var/empty:/usr/bin/false
```

```
soufiane@soufiane-VirtualBox:~$ date -u -d @1451865600
Mon Jan  4 00:00:00 UTC 2016
```

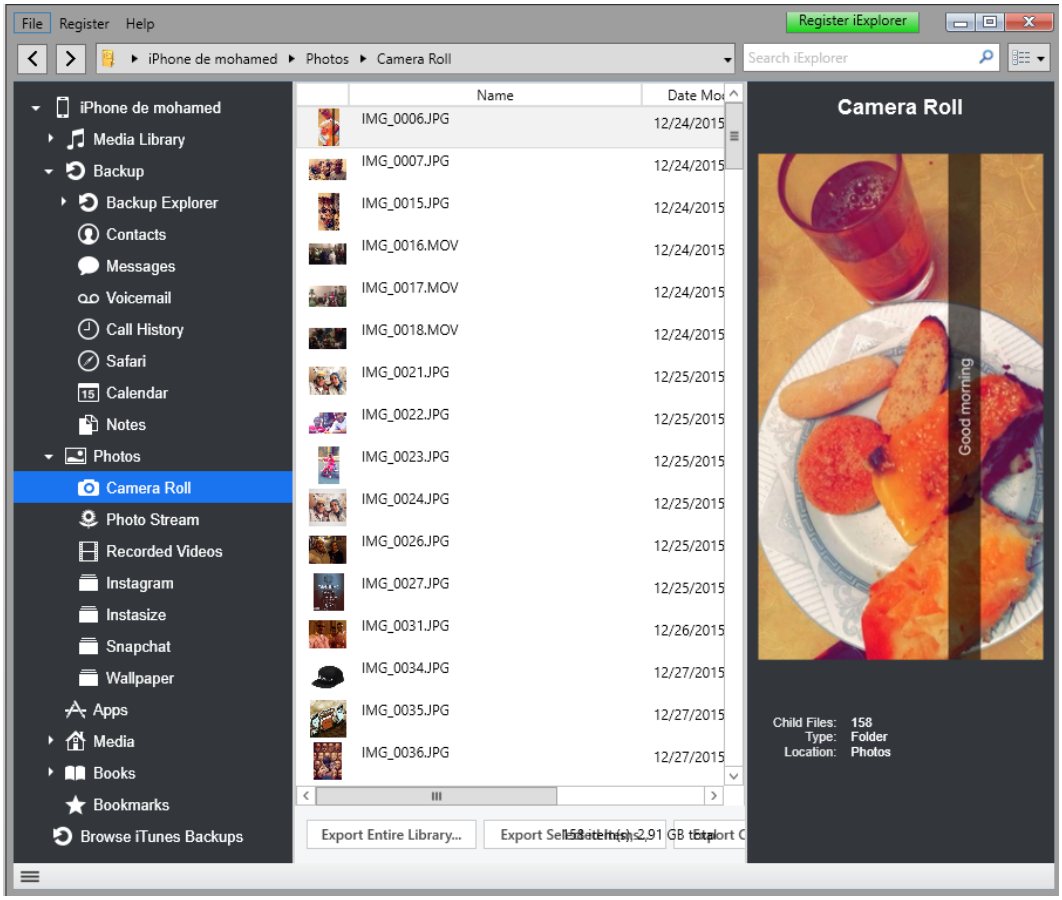

Sign In
Search Playlist
1
's iPad
16GB
50%
Settings
Summary
2
Apps
Music
Movies
iPad mini
Capacity: 12.75 GB
Serial Number: F87L8RU
3
Capacity: 12.75 GB
UDID: 54A54AB40CF4
C
y check for

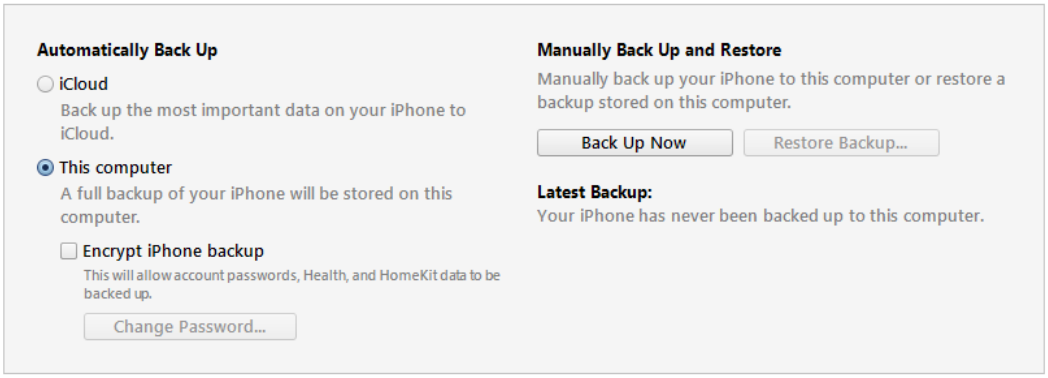

Lockdown
Fichier
Accueil
Partage
Affichage
« Disque local (C:) › ProgramData › Apple › Lockdown
Rechercher dans : Lockdown
Accès rapide
Creative Clou
Google Drive
Desktop
Documents
Téléchargem
Nom
Modifié le
Type
Taille
dfd550d3daf0ed503b634bcdc27c8c582cda4a9f.plist
08/01/2016 14:10
Property List File
10 Ko
SystemConfiguration.plist
07/01/2016 20:36
Property List File
1 Ko
2 élément(s)


iPhone
Model A1533

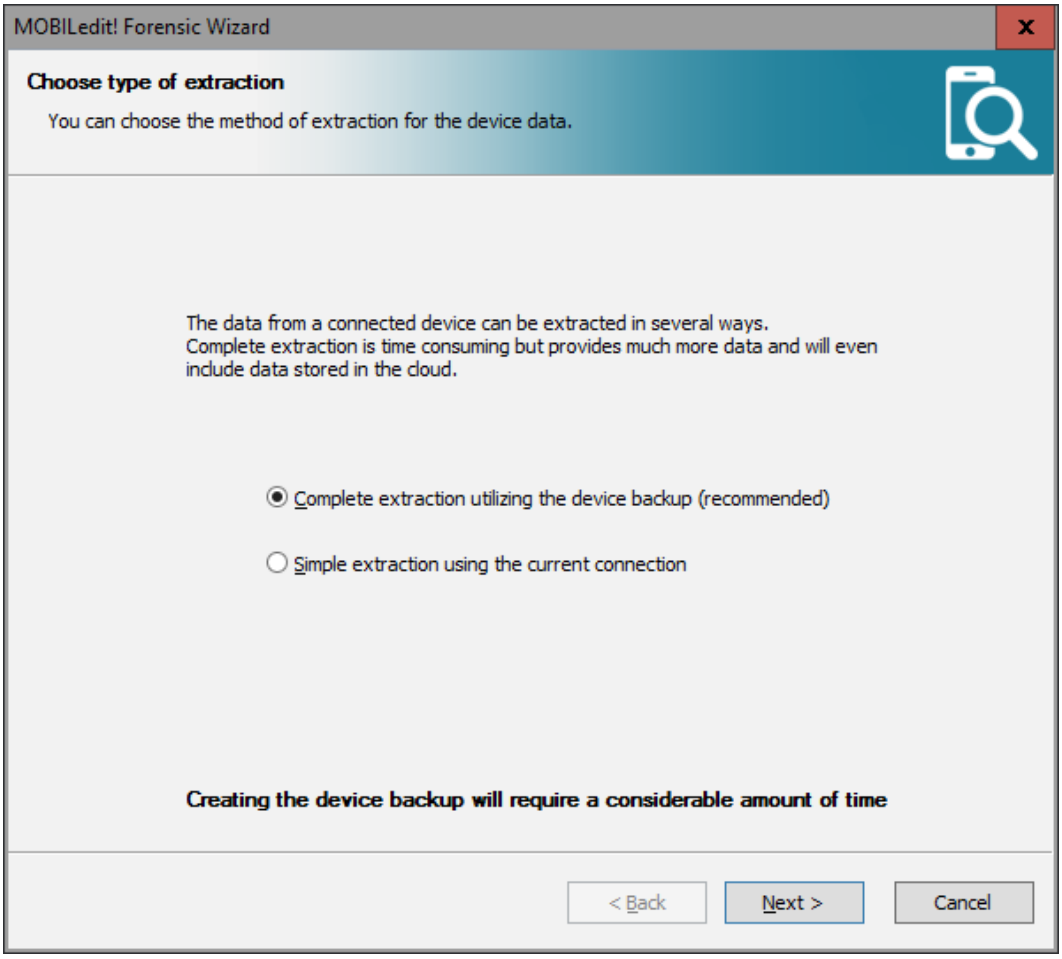

you are
beautiful
6256

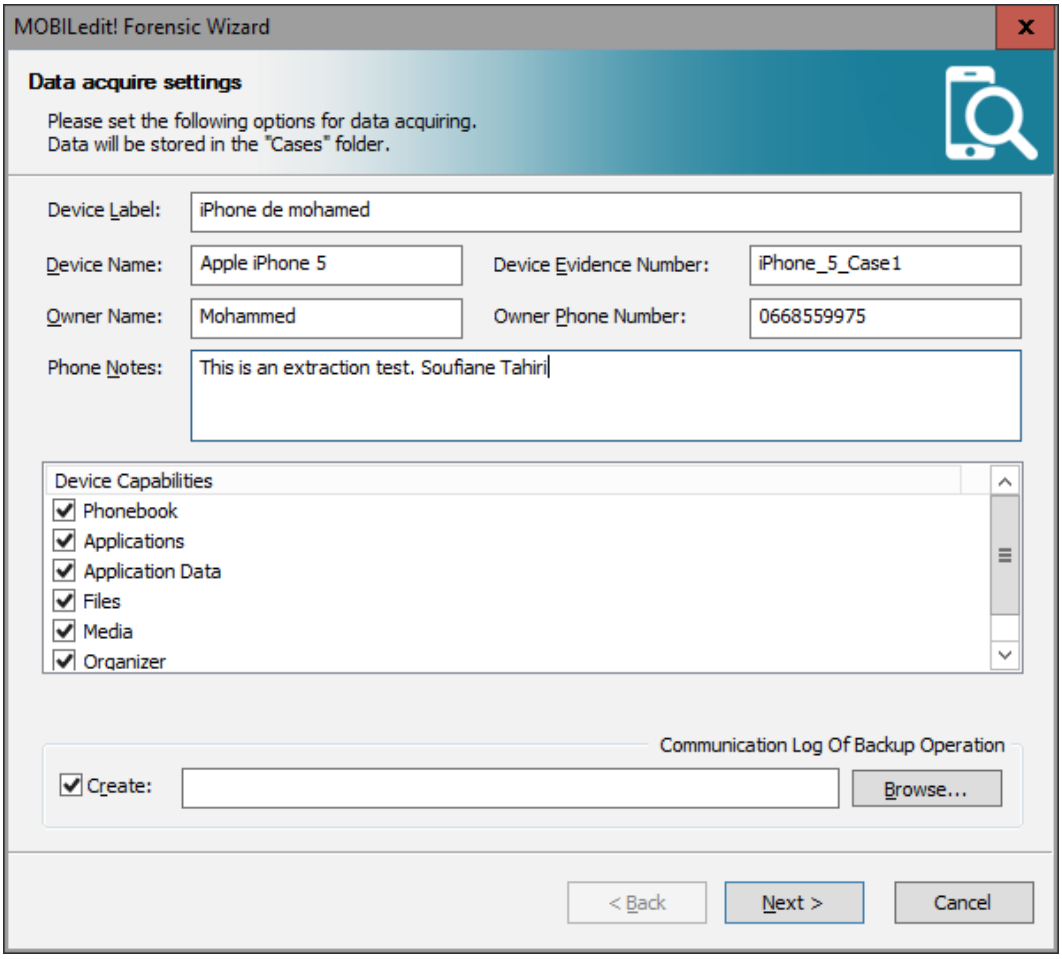

8664

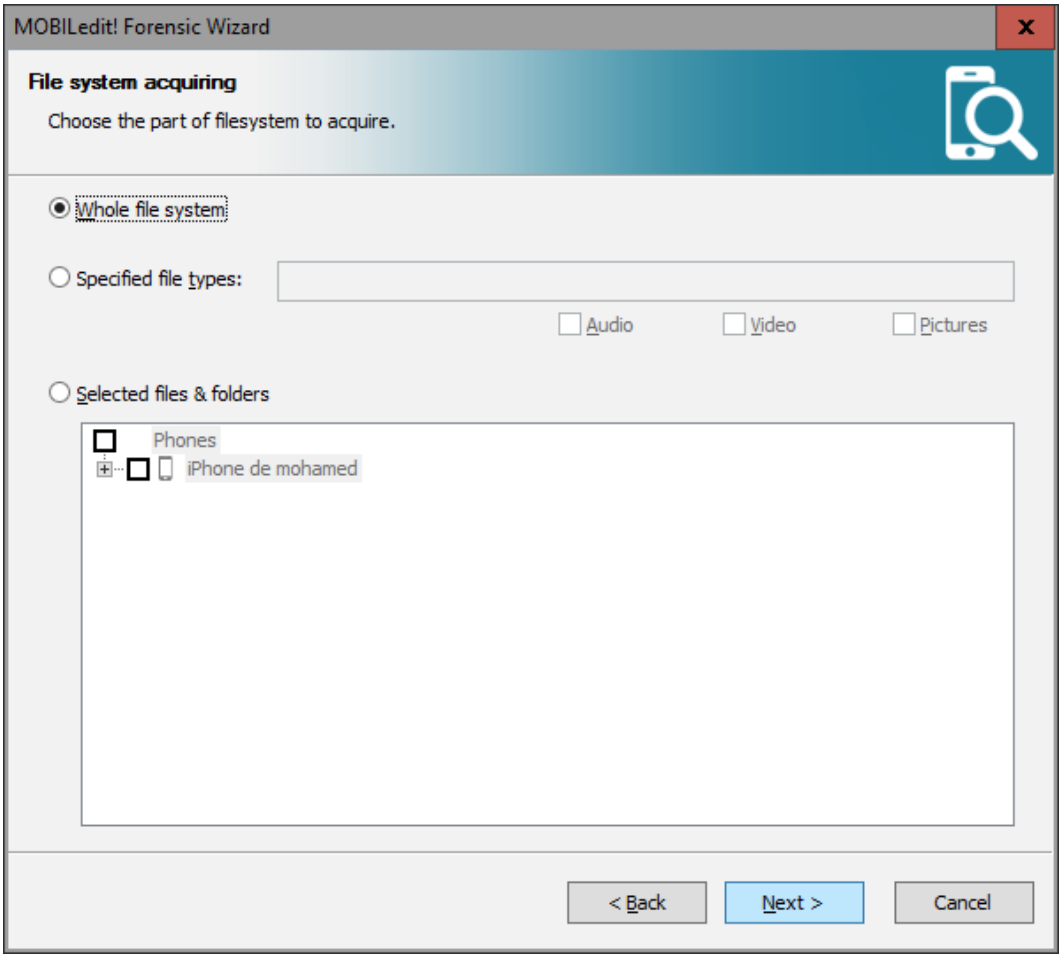

File
Register
Help
Register iExplorer
iPhone de mohamed
Photos
Camera Roll
Search iExplorer
iPhone de mohamed
Media Library
Backup
Backup Explorer
Contacts
Messages
Voicemail
Call History
Safari
Calendar
Notes
Photos
Camera Roll
Photo Stream
Recorded Videos
Instagram
Instasize
Snapchat
Wallpaper
Apps
Media
Books
Bookmarks
Browse iTunes Backups
Name
Date Mo
IMG_0006.JPG 12/24/2015
IMG_0007.JPG 12/24/2015
IMG_0015.JPG 12/24/2015
IMG_0016.MOV 12/24/2015
IMG_0017.MOV 12/24/2015
IMG_0018.MOV 12/24/2015
IMG_0021.JPG 12/25/2015
IMG_0022.JPG 12/25/2015
IMG_0023.JPG 12/25/2015
IMG_0024.JPG 12/25/2015
IMG_0026.JPG 12/25/2015
IMG_0027.JPG 12/25/2015
IMG_0031.JPG 12/26/2015
IMG_0034.JPG 12/27/2015
IMG_0035.JPG 12/27/2015
IMG_0036.JPG 12/27/2015
Export Entire Library...
Camera Roll
Good morning
Child Files: 158
Type: Folder
Location: Photos

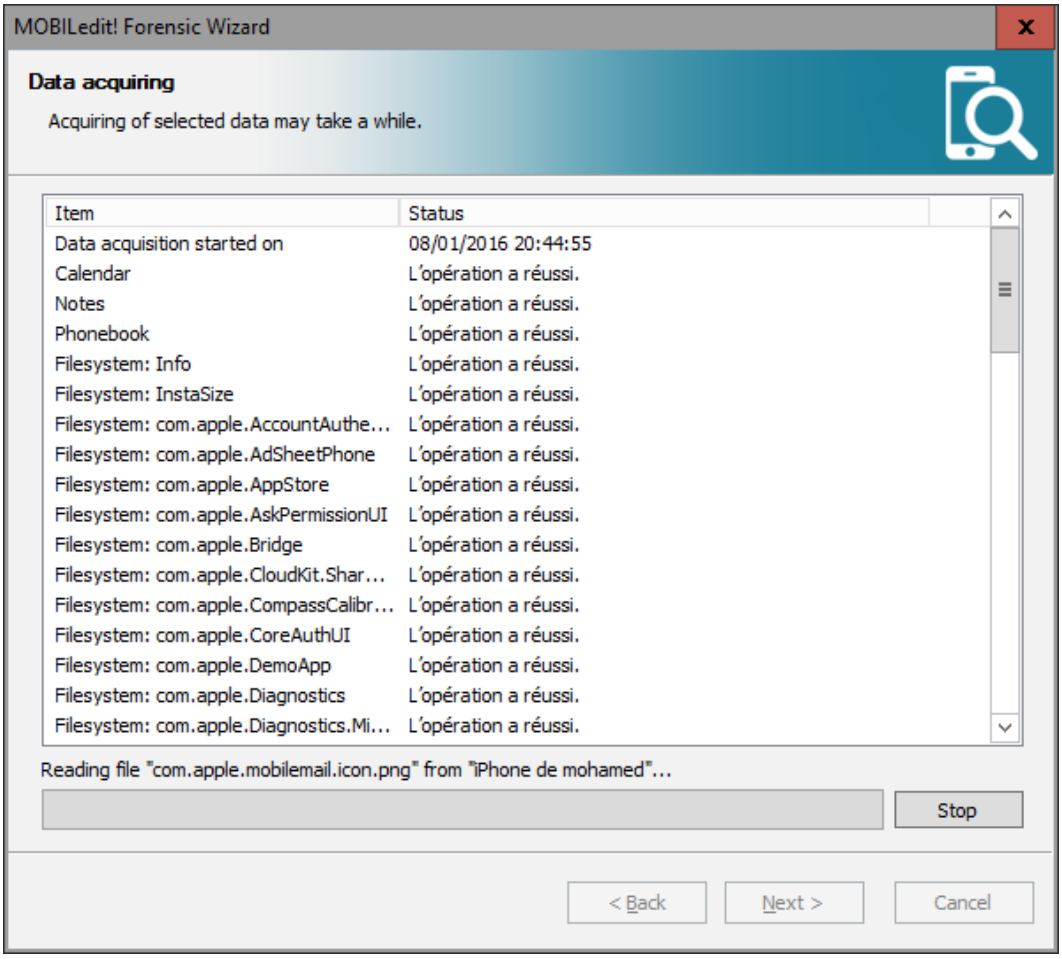

Automatically Back Up
iCloud
Back up the most important data on your iPhone to iCloud.
This computer
A full backup of your iPhone will be stored on this computer.
Encrypt iPhone backup
This will allow account passwords, Health, and HomeKit data to be backed up.
Change Password...
Manually Back Up and Restore
Manually back up your iPhone to this computer or restore a backup stored on this computer.
Back Up Now
Restore Backup...
Latest Backup:
Your iPhone has never been backed up to this computer.

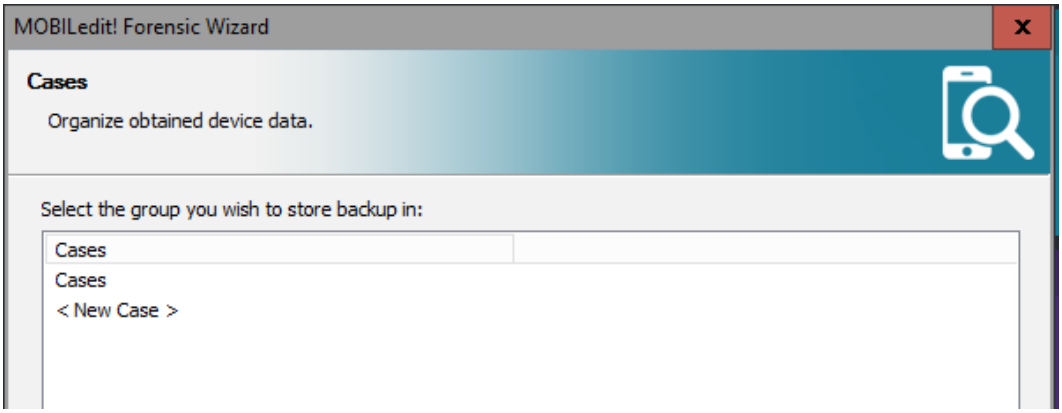

Connected
Apple
iPhone 5
iPhone de mohamed
Connect
Connected to USB
Extraction date:
<not available>
Report Wizard
SIM Clone
iTunes Backups
Cases
Hex Dump
Photo Viewer
Forensic Reports

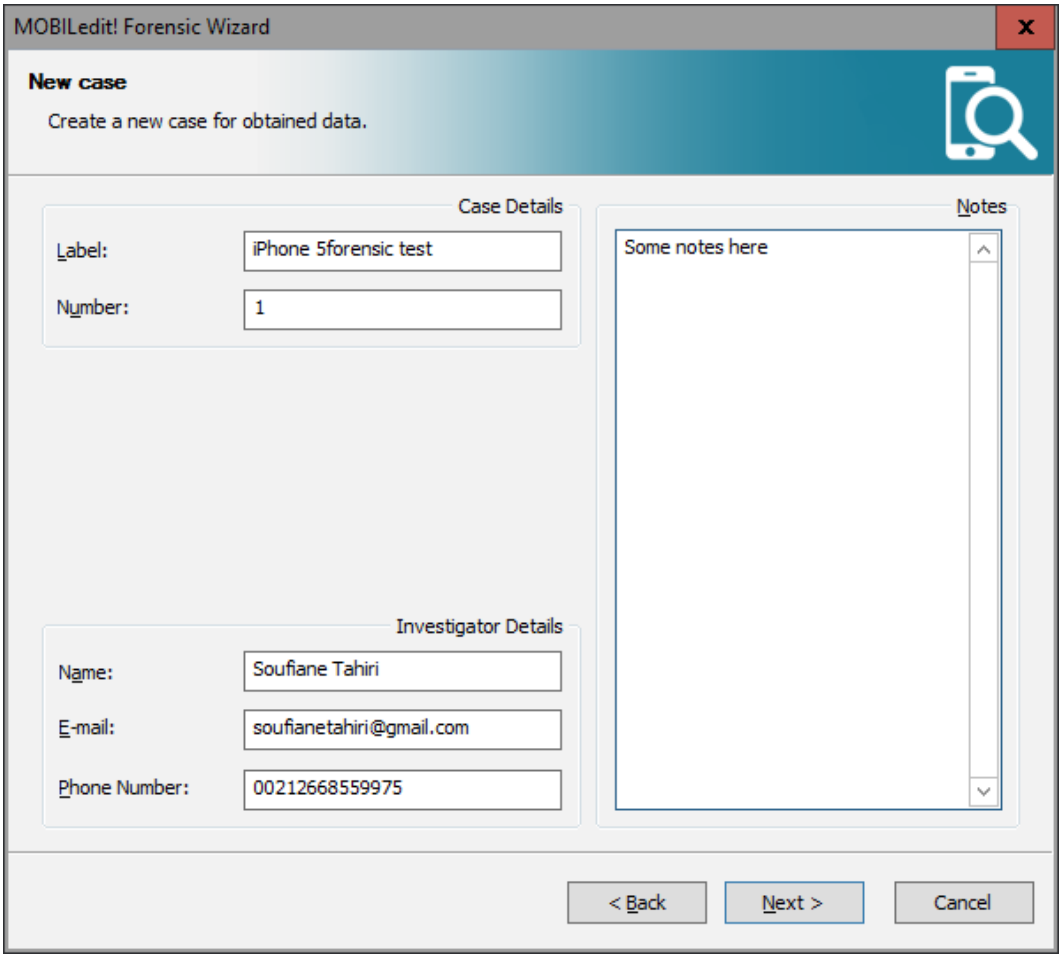

MOBILedit! Forensic Wizard
Choose type of extraction
You can choose the method of extraction for the device data.
The data from a connected device can be extracted in several ways.
Complete extraction is time consuming but provides much more data and will even include data stored in the cloud.
Complete extraction utilizing the device backup (recommended)
Simple extraction using the current connection
Creating the device backup will require a considerable amount of time
< Back
Next >
Cancel


MOBILedit! Forensic Wizard
Data acquire settings
Please set the following options for data acquiring.
Data will be stored in the "Cases" folder.
Device Label:
iPhone de mohamed
Device Name:
Apple iPhone 5
Device Evidence Number:
iPhone_5_Case1
Owner Name:
Mohammed
Owner Phone Number:
0668559975
Phone Notes:
This is an extraction test. Soufiane Tahiri
Device Capabilities
Phonebook
Applications
Application Data
Files
Media
Organizer
Communication Log Of Backup Operation
Create:
Browse...
< Back
Next >
Cancel

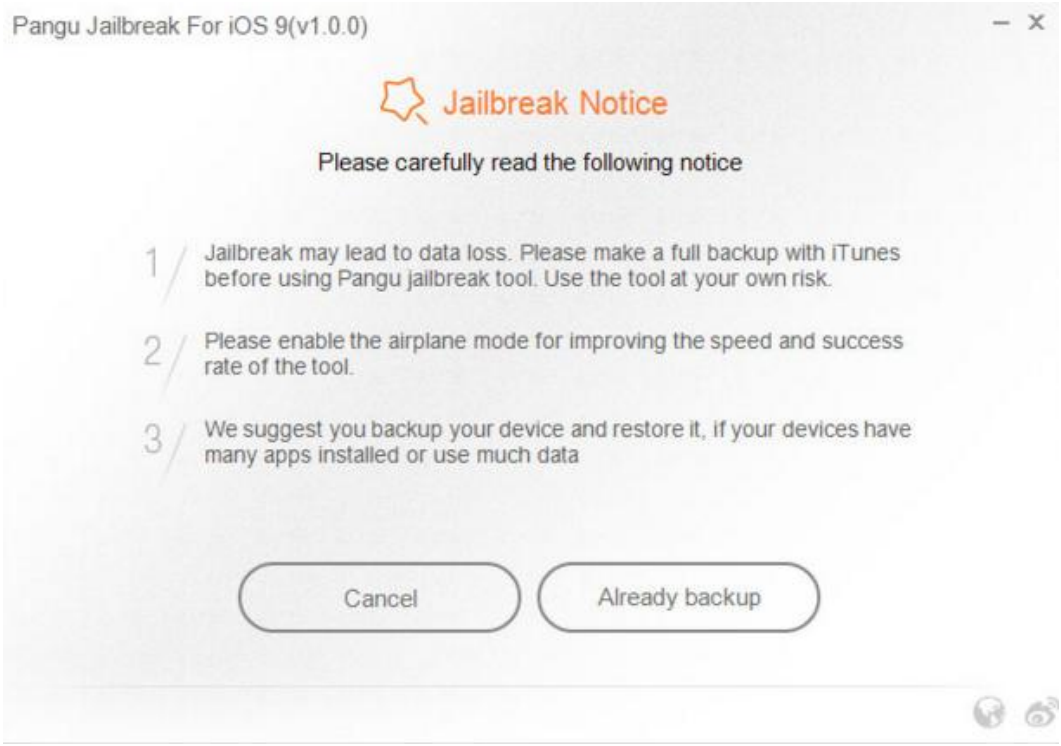

MOBILedit! Forensic Wizard
File system acquiring
Choose the part of filesystem to acquire.
Whole file system
Specified file types:
Audio
Video
Pictures
Selected files & folders
Phones
iPhone de mohamed
< Back
Next >
Cancel

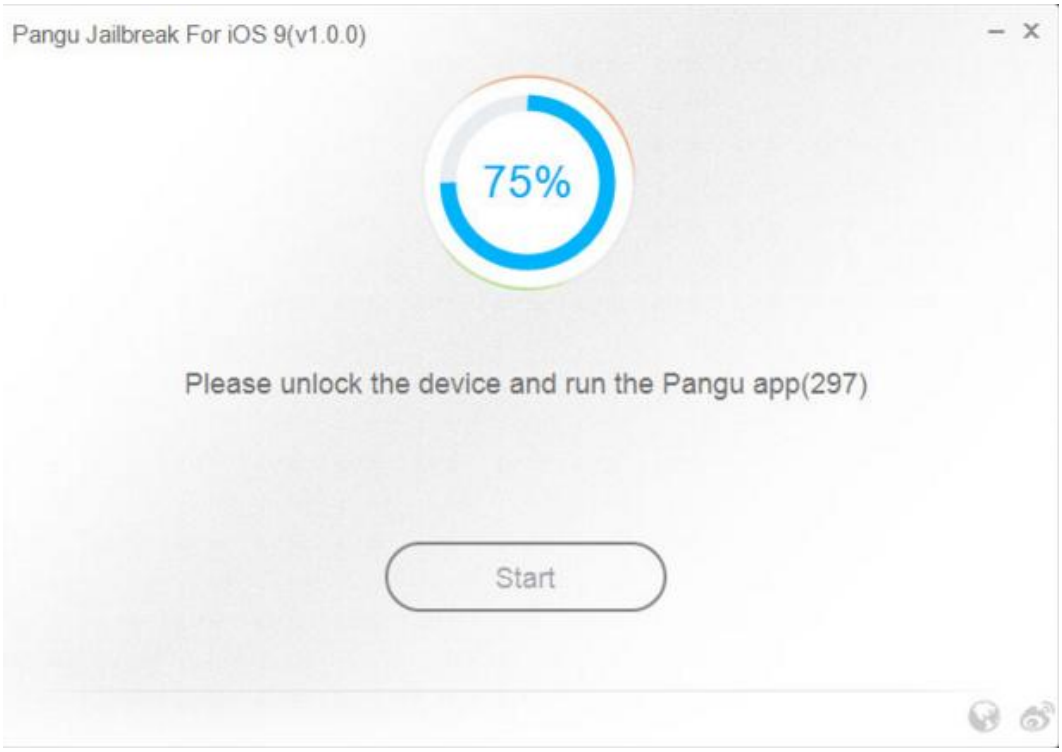

MOBILedit! Forensic Wizard
Data acquiring
Acquiring of selected data may take a while.
Item
Status
Data acquisition started on
08/01/2016 20:44:55
Calendar
L'opération a réussi.
Notes
L'opération a réussi.
Phonebook
L'opération a réussi.
Filesystem: Info
L'opération a réussi.
Filesystem: InstaSize
L'opération a réussi.
Filesystem: com.apple.AccountAuthe...
L'opération a réussi.
Filesystem: com.apple.AdSheetPhone
L'opération a réussi.
Filesystem: com.apple.AppStore
L'opération a réussi.
Filesystem: com.apple.AskPermissionUI
L'opération a réussi.
Filesystem: com.apple.Bridge
L'opération a réussi.
Filesystem: com.apple.CloudKit.Shar...
L'opération a réussi.
Filesystem: com.apple.CompassCalibr...
L'opération a réussi.
Filesystem: com.apple.CoreAuthUI
L'opération a réussi.
Filesystem: com.apple.DemoApp
L'opération a réussi.
Filesystem: com.apple.Diagnostics
L'opération a réussi.
Filesystem: com.apple.Diagnostics.Mi...
L'opération a réussi.
Reading file "com.apple.mobilemail.icon.png" from "iPhone de mohamed"...
Stop
< Back
Next >
Cancel


MOBILedit! Forensic Wizard
Cases
Organize obtained device data.
Select the group you wish to store backup in:
Cases
Cases
< New Case >


MOBILedit! Forensic Wizard
New case
Create a new case for obtained data.
Case Details
Label:
iPhone 5forensic test
Number:
1
Notes
Some notes here
Investigator Details
Name:
Soufiane Tahiri
E-mail:
soufianetahiri@gmail.com
Phone Number:
00212668559975
< Back
Next >
Cancel

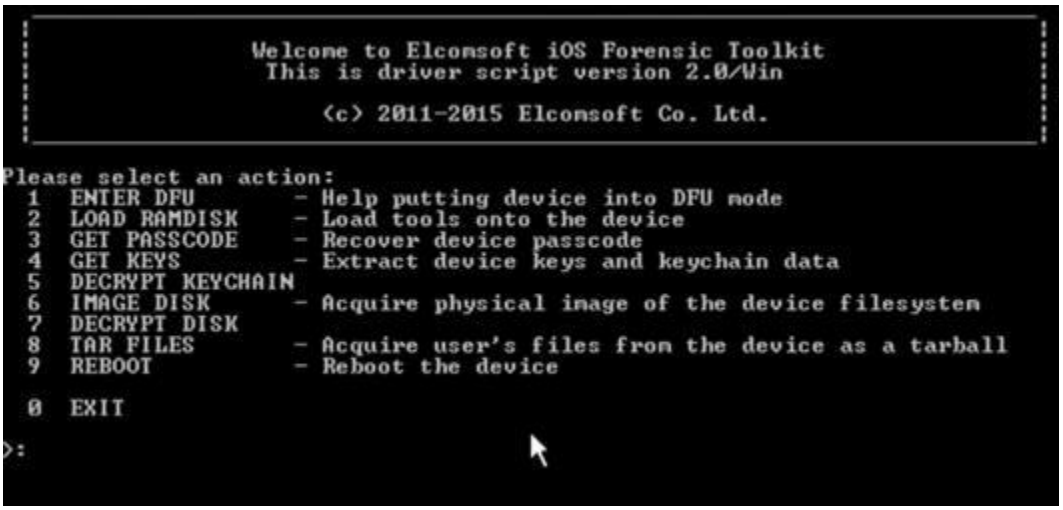

Pangu Jailbreak For iOS 9(v1.0.0)
iPhone[iPhone7,1 iOS9.0.1(Jailbreak ready)]
Start

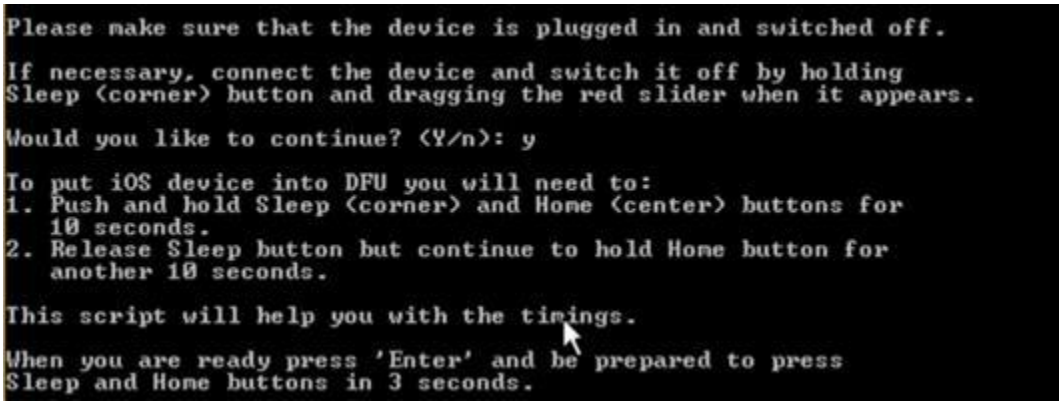

Pangu Jailbreak For iOS 9(v1.0.0)
Jailbreak Notice
Please carefully read the following notice
1 Jailbreak may lead to data loss. Please make a full backup with iTunes before using Pangu jailbreak tool. Use the tool at your own risk.
2 Please enable the airplane mode for improving the speed and success rate of the tool.
3 We suggest you backup your device and restore it, if your devices have many apps installed or use much data
Cancel
Already backup

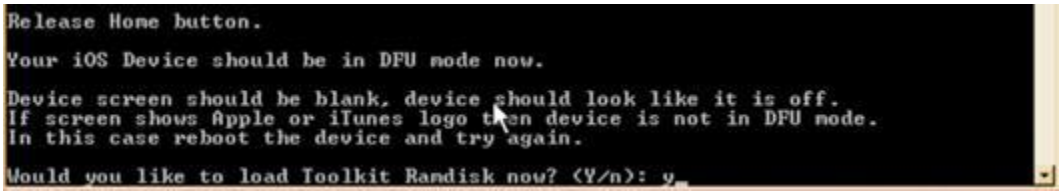

Pangu Jailbreak For iOS 9(v1.0.0)
75%
Please unlock the device and run the Pangu app(297)
Start

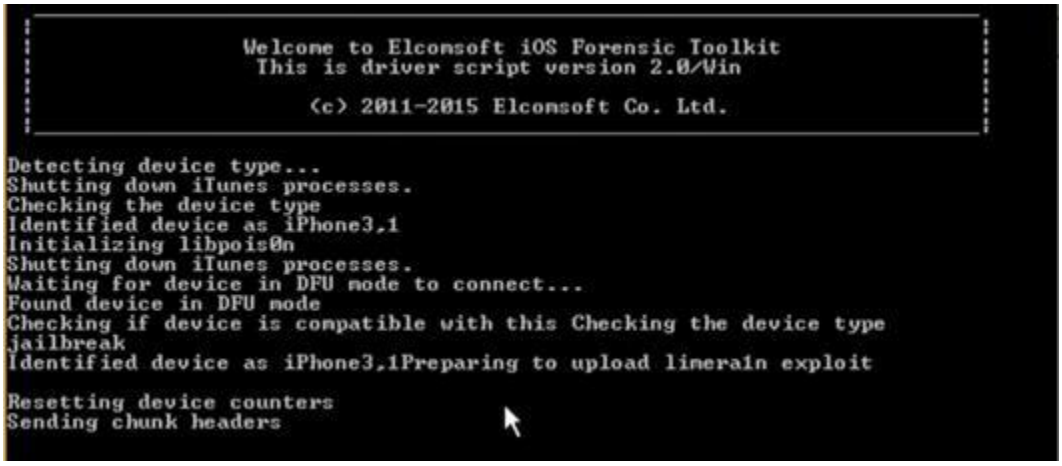

Pangu Jailbreak For iOS 9(v1.0.0)
75%
Please follow the displayed instructions and ALLOW it to access photos
Start


Pangu Jailbreak For iOS 9(v1.0.0)
s iPhone[iOS9.0.1(Already jailbroken)]
Start

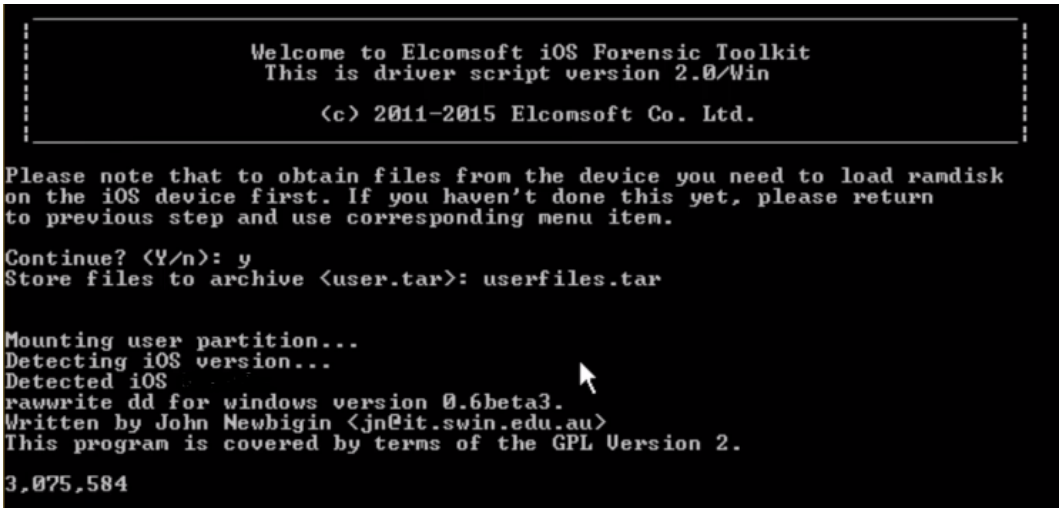

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 2.0/Win
(c) 2011-2015 Elcomsoft Co. Ltd.
Please select an action:
1 ENTER DFU - Help putting device into DFU mode
2 LOAD RAMDISK - Load tools onto the device
3 GET PASSCODE - Recover device passcode
4 GET KEYS - Extract device keys and keychain data
5 DECRYPT KEYCHAIN
6 IMAGE DISK - Acquire physical image of the device filesysten
7 DECRYPT DISK
8 TAR FILES - Acquire user's files from the device as a tarball
9 REBOOT - Reboot the device
0 EXIT
>:

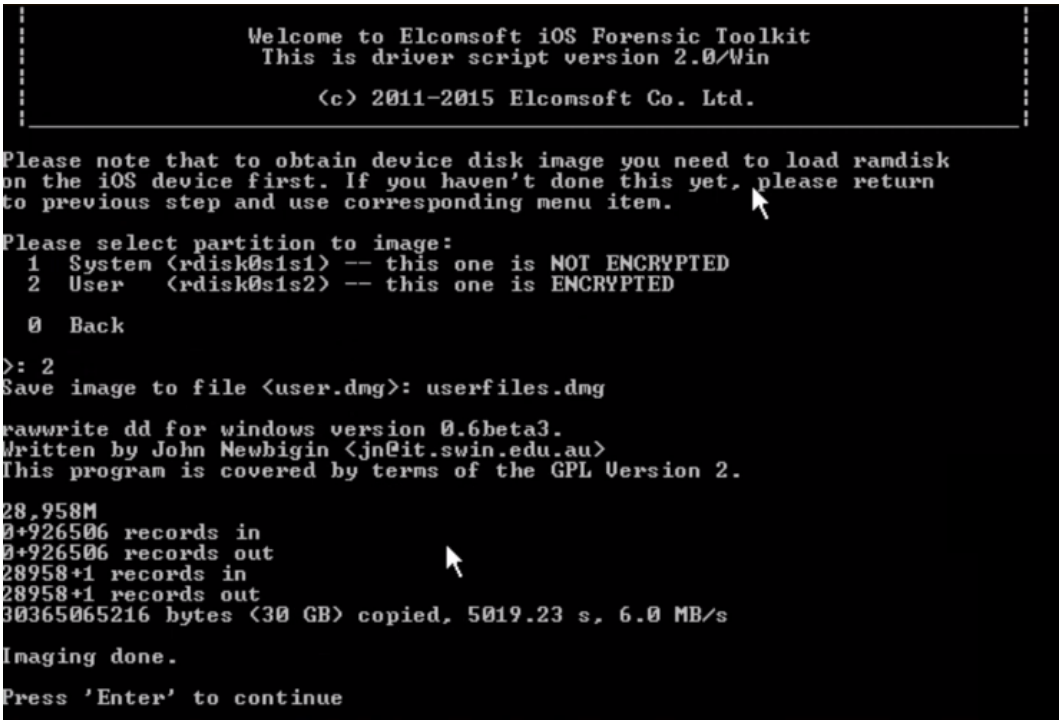

Please make sure that the device is plugged in and switched off.
If necessary, connect the device and switch it off by holding
Sleep (corner) button and dragging the red slider when it appears.
Would you like to continue? (Y/n): y
To put iOS device into DFU you will need to:
1. Push and hold Sleep (corner) and Home (center) buttons for
10 seconds.
2. Release Sleep button but continue to hold Home button for
another 10 seconds.
This script will help you with the timings.
When you are ready press 'Enter' and be prepared to press
Sleep and Home buttons in 3 seconds.

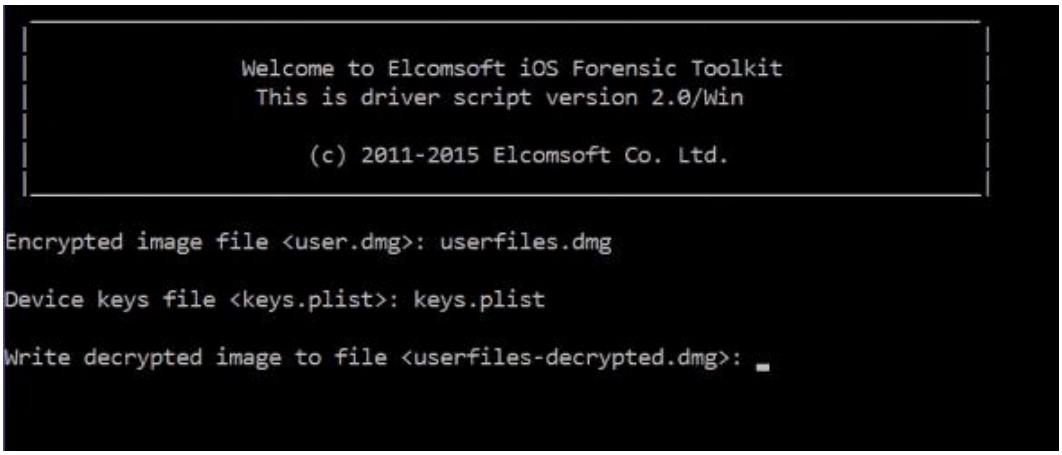

Release Home button.
Your iOS Device should be in DFU mode now.
Device screen should be blank, device should look like it is off.
If screen shows Apple or iTunes logo then device is not in DFU mode.
In this case reboot the device and try again.
Would you like to load Toolkit Ramdisk now? (Y/n): y


Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 2.0/Win
(c) 2011-2015 Elcomsoft Co. Ltd.
Detecting device type...
Shutting down iTunes processes.
Checking the device type
Identified device as iPhone3,1
Initializing libpois0n
Shutting down iTunes processes.
Waiting for device in DFU mode to connect...
Found device in DFU mode
Checking if device is compatible with this Checking the device type
jailbreak
Identified device as iPhone3,1Preparing to upload limera1n exploit
Resetting device counters
Sending chunk headers

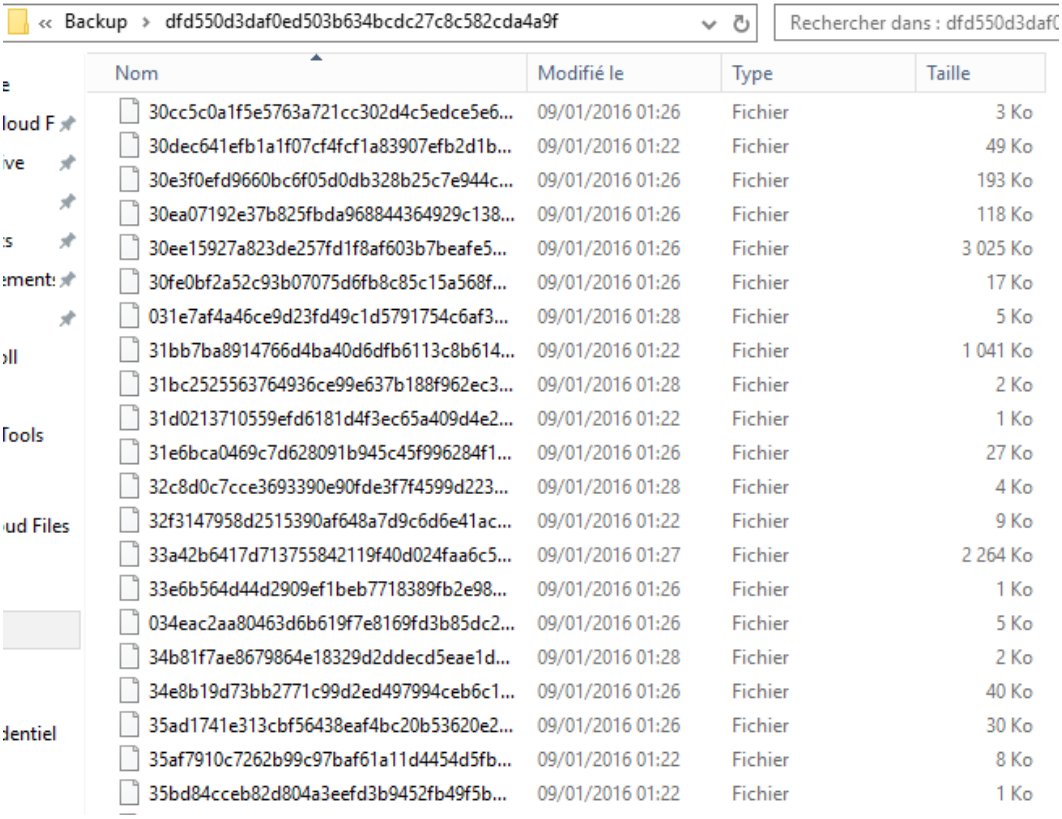

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 2.0/Win
(c) 2011-2015 Elcomsoft Co. Ltd.
Device keys file <keys.plist>: keys.plist
Write decrypted image to file <keychain.txt>: keychain.txt


Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 2.0/Win
(c) 2011-2015 Elcomsoft Co. Ltd.
Please note that to obtain files from the device you need to load ramdisk
on the iOS device first. If you haven't done this yet, please return
to previous step and use corresponding menu item.
Continue? <Y/n>: y
Store files to archive <user.tar>: userfiles.tar
Mounting user partition...
Detecting iOS version...
Detected iOS
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.
3,075,584

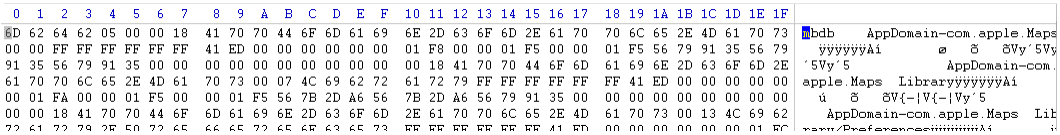

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 2.0/Win
(c) 2011-2015 Elcomsoft Co. Ltd.
Please note that to obtain device disk image you need to load ramdisk
on the iOS device first. If you haven't done this yet, please return
to previous step and use corresponding menu item.
Please select partition to image:
1 System (rdisk0s1s1) -- this one is NOT ENCRYPTED
2 User (rdisk0s1s2) -- this one is ENCRYPTED
0 Back
>: 2
Save image to file <user.dmg>: userfiles.dmg
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.
28,958M
0+926506 records in
0+926506 records out
28958+1 records in
28958+1 records out
30365065216 bytes (30 GB) copied, 5019.23 s, 6.0 MB/s
Imaging done.
Press 'Enter' to continue


Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 2.0/Win
(c) 2011-2015 Elcomsoft Co. Ltd.
Encrypted image file <user.dmg>: userfiles.dmg
Device keys file <keys.plist>: keys.plist
Write decrypted image to file <userfiles-decrypted.dmg>:

```
[INFO] Key "EscrowKeyBag" not found
[INFO] Complete key set is loaded, everything should be decryptable.
[INFO] Image encryption statistics:
[INFO]   6720 files total: 6626 encrypted + 94 not encrypted.
[INFO]   6626 files can be decrypted (out of 6626 encrypted files).
[INFO] Input image contains 3706673 blocks of 8192 bytes.
[100%] 28.28 of 28.28 Gb decrypted
SHA1(userfiles-decrypted.dmg) = 8a60492276290 23fc809d9a62ee69d4eac5200d8

Press 'Enter' to continue
```

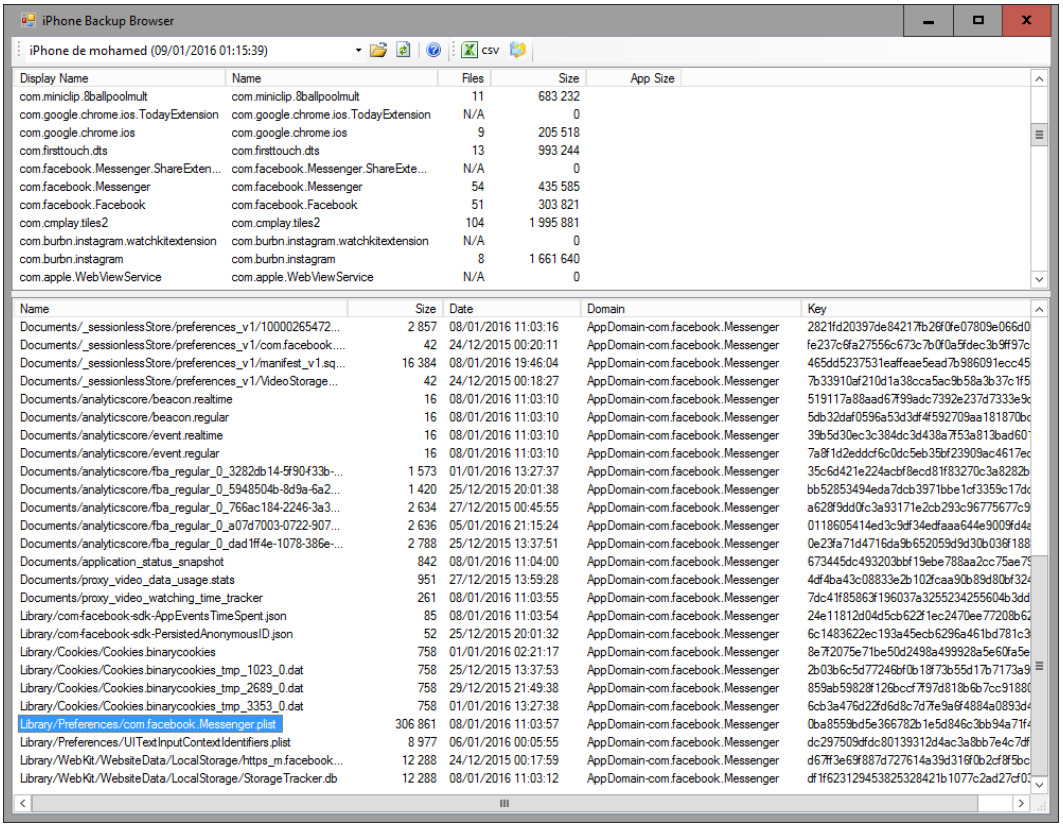


Key	Type	Value
Root	dict	
Applications	dict	
Build Version	string	13C75
Device Name	string	iPhone de mohamed
Display Name	string	iPhone de mohamed
GUID	string	3CE4210EA0AEDB84F23E0
IMEI	string	013412008655534
Installed Applications	array	
	string	com.toyopagroup.picabo
	string	com.cmplay.tiles2
	string	com.facebook.Facebook
	string	com.miniclip.8ballpoolmu
	string	com.google.chrome.ios
	string	com.facebook.Messenger
	string	InstaSize
	string	tr.com.tiramisu.driftxl
	string	net.whatsapp.WhatsApp
	string	com.burbn.instagram
	string	com.firsttouch.dts
Last Backup Date	date	2016-01-09T01:15:39Z
Product Name	string	iPhone 5
Product Type	string	iPhone5,2
Product Version	string	9.2
Serial Number	string	C37JWNN2DTWD
Target Identifier	string	dfd550d3daf0ed503b634b
Target Type	string	Device
Unique Identifier	string	DFD550D3DAF0ED503B634
iTunes Files	dict	
iTunes Settings	dict	
iTunes Version	string	12.3.2.35



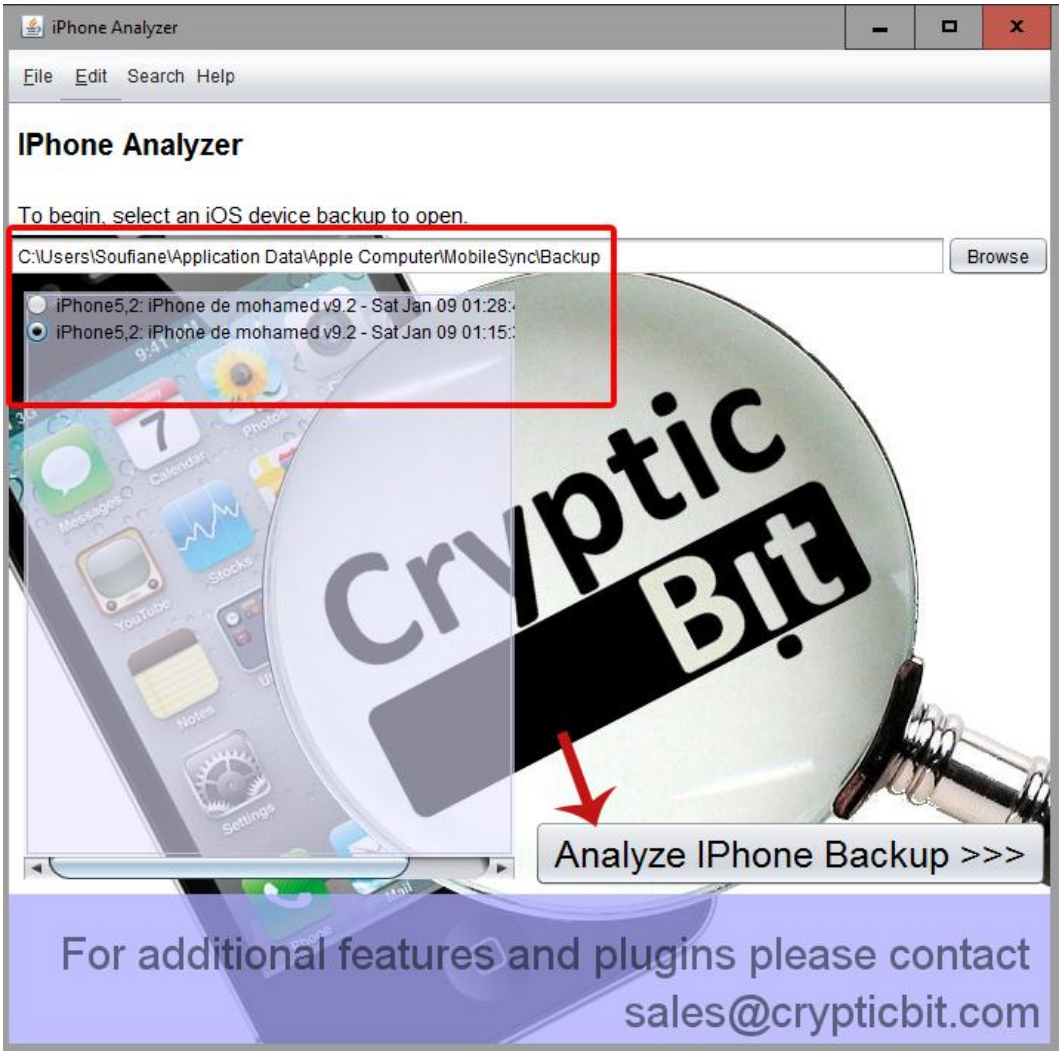
Key	Type	Value
Root	dict	
Applications	dict	
BackupKeyBag	data	...
Date	date	2016-01-09T01:15:33Z
IsEncrypted	boolean	false
Lockdown	dict	
BuildVersion	string	13C75
DeviceName	string	iPhone de mohamed
ProductType	string	iPhone5,2
ProductVersion	string	9.2
SerialNumber	string	C37JWNN2DTWD
UniqueDeviceID	string	dfd550d3daf0ed503b634b
com.apple.Accessibility	dict	
com.apple.MobileDeviceCr	dict	
com.apple.TerminalFlashr	dict	
com.apple.mobile.data_syn	dict	
com.apple.mobile.iTunes.a	dict	
com.apple.mobile.wireless_	dict	
SystemDomainsVersion	string	24.0
Version	string	9.1
WasPasscodeSet	boolean	true

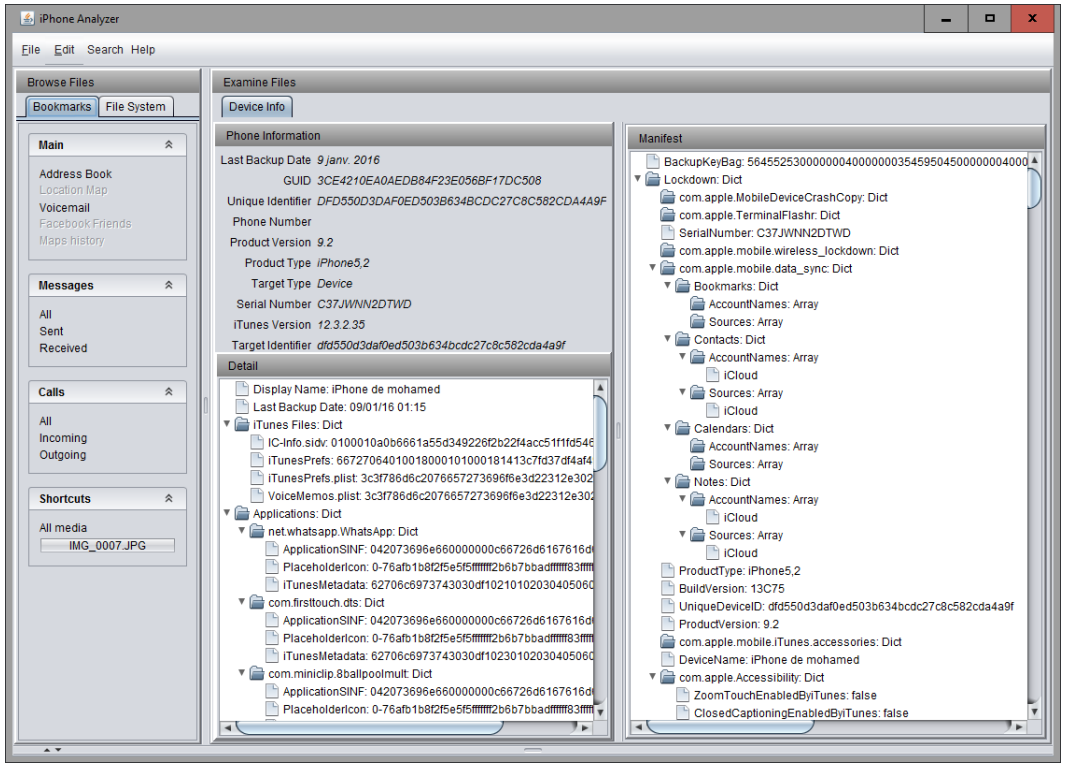
Key	Type	Value
Root	dict	
BackupState	string	new
Date	date	2016-01-09T01:15:38Z
IsFullBackup	boolean	false
SnapshotState	string	finished
UUID	string	B8F1118C-A251-4AA0-AC
Version	string	2.4

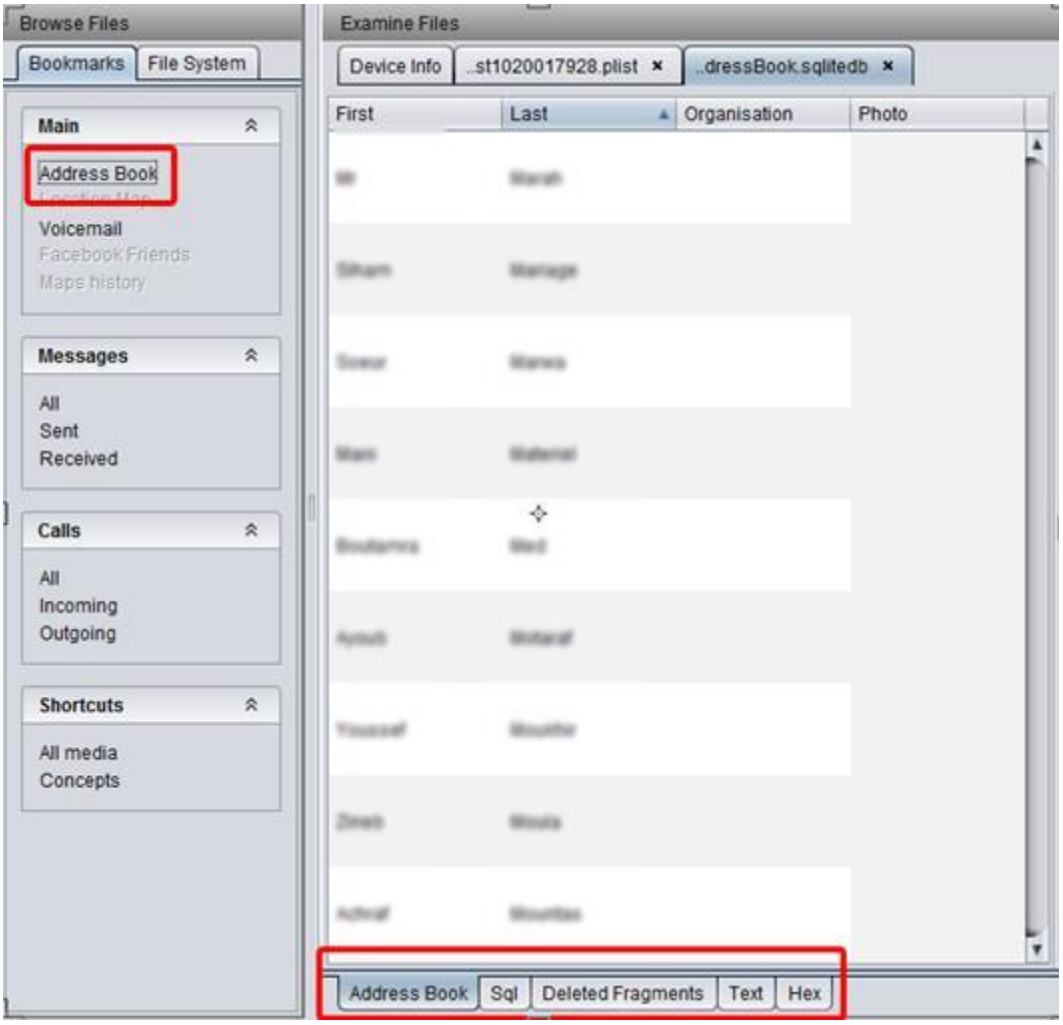


Display Name	Name	Files	Size	App Size
com.miniclip.8ballpoolmult	com.miniclip.8ballpoolmult	11	683 232	
com.google.chrome.ios.TodayExtension	com.google.chrome.ios.TodayExtension	N/A	0	
com.google.chrome.ios	com.google.chrome.ios	9	205 518	
com.firsttouch.dts	com.firsttouch.dts	13	993 244	
com.facebook.Messenger.ShareExten...	com.facebook.Messenger.ShareExte...	N/A	0	
com.facebook.Messenger	com.facebook.Messenger	54	435 585	
com.facebook.Facebook	com.facebook.Facebook	51	303 821	
com.cmplay.tiles2	com.cmplay.tiles2	104	1 995 881	
com.burbn.instagram.watchkitextension	com.burbn.instagram.watchkitextension	N/A	0	
com.burbn.instagram	com.burbn.instagram	8	1 661 640	
com.apple.WebViewService	com.apple.WebViewService	N/A	0	

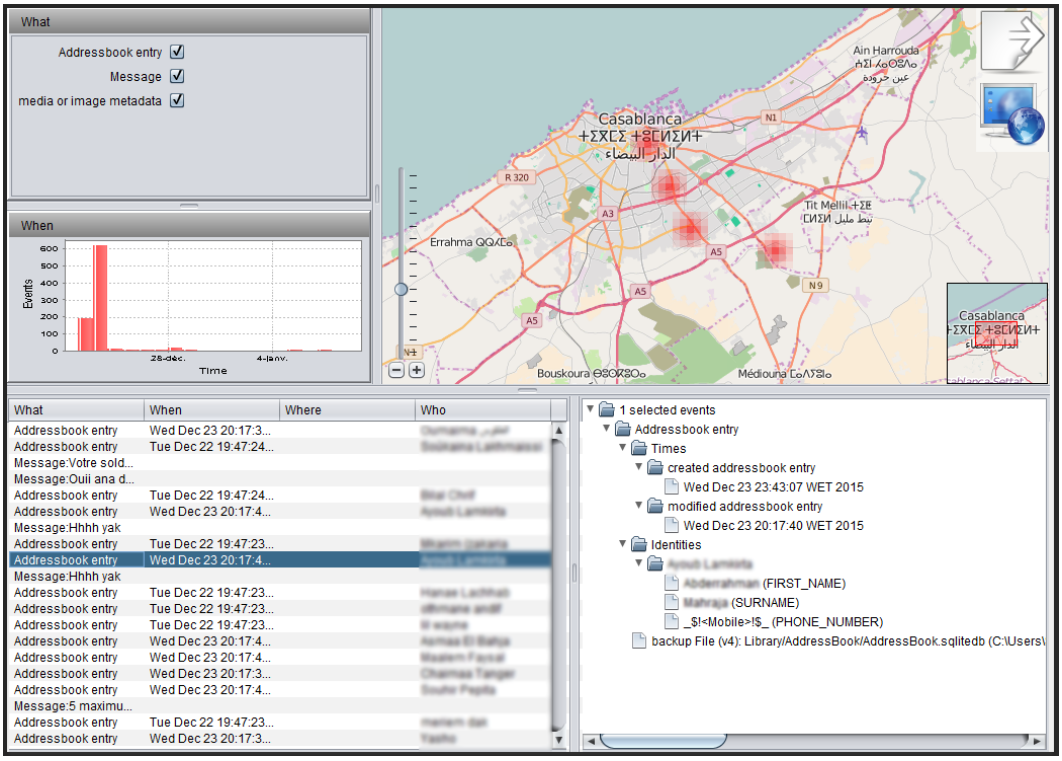
Name	Size	Date	Domain	Key
Documents/_sessionlessStore/preferences_v1/10000265472...	2 857	08/01/2016 11:03:16	AppDomain-com.facebook.Messenger	2821fd20397de84217fb26f0fe07809e066d0
Documents/_sessionlessStore/preferences_v1/com.facebook....	42	24/12/2015 00:20:11	AppDomain-com.facebook.Messenger	fe237c6fa27556c673c7b0f0a5fdec3b9ff97c
Documents/_sessionlessStore/preferences_v1/manifest_v1.sq...	16 384	08/01/2016 19:46:04	AppDomain-com.facebook.Messenger	465dd5237531eaffeae5ead7b986091ecc45
Documents/_sessionlessStore/preferences_v1/VideoStorage...	42	24/12/2015 00:18:27	AppDomain-com.facebook.Messenger	7b33910af210d1a38cca5ac9b58a3b37c1f5
Documents/analyticscore/beacon.realtime	16	08/01/2016 11:03:10	AppDomain-com.facebook.Messenger	519117a88aad67f99adc7392e237d7333e9c
Documents/analyticscore/beacon.regular	16	08/01/2016 11:03:10	AppDomain-com.facebook.Messenger	5db32daf0596a53d3df4f592709aa181870bc
Documents/analyticscore/event.realtime	16	08/01/2016 11:03:10	AppDomain-com.facebook.Messenger	39b5d30ec3c384dc3d438a7f53a813bad607
Documents/analyticscore/event.regular	16	08/01/2016 11:03:10	AppDomain-com.facebook.Messenger	7a8f1d2eddcf6c0dc5eb35bf23909ac4617ec
Documents/analyticscore/fba_regular_0_3282db14-5f90-f33b-...	1 573	01/01/2016 13:27:37	AppDomain-com.facebook.Messenger	35c6d421e224acbf8ecd81f83270c3a8282b
Documents/analyticscore/fba_regular_0_5948504b-8d9a-6a2...	1 420	25/12/2015 20:01:38	AppDomain-com.facebook.Messenger	bb52853494eda7dcb3971bbe1cf3359c17dc
Documents/analyticscore/fba_regular_0_766ac184-2246-3a3...	2 634	27/12/2015 00:45:55	AppDomain-com.facebook.Messenger	a628f9dd0fc3a93171e2cb293c96775677c9
Documents/analyticscore/fba_regular_0_a07d7003-0722-907...	2 636	05/01/2016 21:15:24	AppDomain-com.facebook.Messenger	0118605414ed3c9df34edfaaa644e9009fd4a
Documents/analyticscore/fba_regular_0_dad1ff4e-1078-386e-...	2 788	25/12/2015 13:37:51	AppDomain-com.facebook.Messenger	0e23fa71d4716da9b652059d9d30b036f188
Documents/application_status_snapshot	842	08/01/2016 11:04:00	AppDomain-com.facebook.Messenger	673445dc493203bbf19ebe788aa2cc75ae75
Documents/proxy_video_data_usage.stats	951	27/12/2015 13:59:28	AppDomain-com.facebook.Messenger	4df4ba43c08833e2b102fcaa90b89d80bf324
Documents/proxy_video_watching_time_tracker	261	08/01/2016 11:03:55	AppDomain-com.facebook.Messenger	7dc41f85863f196037a3255234255604b3dd
Library/com.facebook.sdk.AppEventsTimeSpent.json	85	08/01/2016 11:03:54	AppDomain-com.facebook.Messenger	24e11812d04d5cb622f1ec2470ee77208b62
Library/com.facebook.sdk.PersistedAnonymousID.json	52	25/12/2015 20:01:32	AppDomain-com.facebook.Messenger	6c1483622ec193a45ecb6296a461bd781c3
Library/Cookies/Cookies.binarycookies	758	01/01/2016 02:21:17	AppDomain-com.facebook.Messenger	8e7f2075e71be50d2498a499928a5e60fa5e
Library/Cookies/Cookies.binarycookies_tmp_1023_0.dat	758	25/12/2015 13:37:53	AppDomain-com.facebook.Messenger	2b03b6c5d77246bf0b18f73b55d17b7173a9
Library/Cookies/Cookies.binarycookies_tmp_2689_0.dat	758	29/12/2015 21:49:38	AppDomain-com.facebook.Messenger	859ab59828f126bccf7f97d818b6b7cc9188
Library/Cookies/Cookies.binarycookies_tmp_3353_0.dat	758	01/01/2016 13:27:38	AppDomain-com.facebook.Messenger	6cb3a476d22fd6d8c7d7fe9a6f4884a0893d4
Library/Preferences/com.facebook.Messenger.plist	306 861	08/01/2016 11:03:57	AppDomain-com.facebook.Messenger	0ba8559bd5e366782b1e5d846c3bb94a71f4
Library/Preferences/UITextInputContextIdentifiers.plist	8 977	06/01/2016 00:05:55	AppDomain-com.facebook.Messenger	dc297509dfdc80139312d4ac3a8bb7e4c7df
Library/WebKit/WebsiteData/LocalStorage/https_m.facebook...	12 288	24/12/2015 00:17:59	AppDomain-com.facebook.Messenger	d67ff3e69f887d727614a39d316f0b2cf8f5bc
Library/WebKit/WebsiteData/LocalStorage/StorageTracker.db	12 288	08/01/2016 11:03:12	AppDomain-com.facebook.Messenger	df1f6231294538253284 21b1077c2ad27cf03

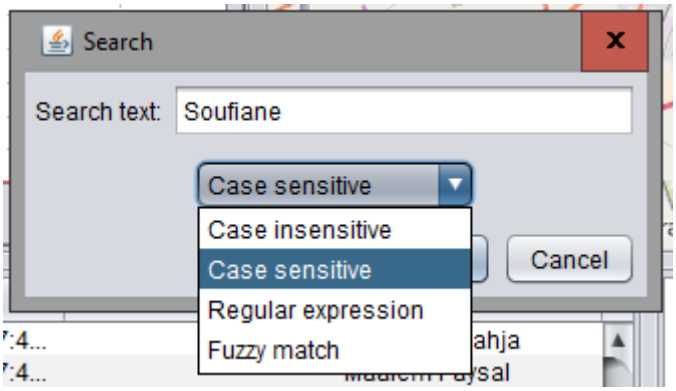

iPhone Analyzer
File Edit Search Help
IPhone Analyzer
To begin, select an iOS device backup to open.
C:\Users\Soufiane\Application Data\Apple Computer\MobileSync\Backup
Browse
iPhone5,2: iPhone de mohamed v9.2 - Sat Jan 09 01:28:
iPhone5,2: iPhone de mohamed v9.2 - Sat Jan 09 01:15:
Cryptic Bit
Analyze IPhone Backup >>>
For additional features and plugins please contact
sales@crypticbit.com

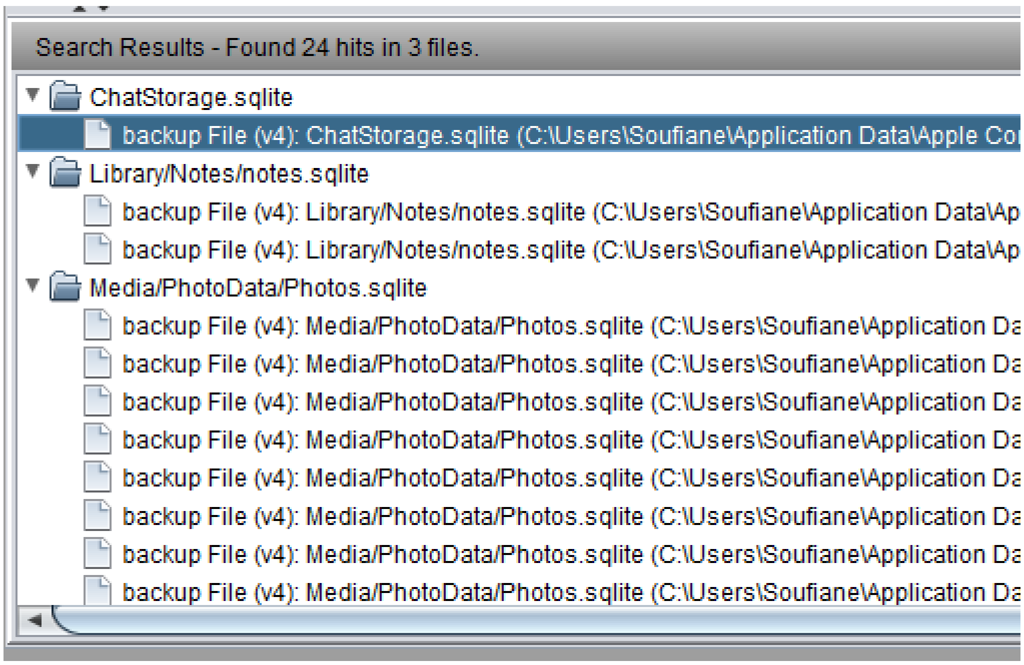

iPhone Analyzer
File Edit Search Help
Browse Files
Bookmarks File System
Main
Address Book
Location Map
Voicemail
Facebook Friends
Maps history
Messages
All
Sent
Received
Calls
All
Incoming
Outgoing
Shortcuts
All media
IMG_0007.JPG
Examine Files
Device Info
Phone Information
Last Backup Date 9 janv. 2016
GUID 3CE4210EA0AEDB84F23E056BF17DC508
Unique Identifier DFD550D3DAF0ED503B634BCDC27C8C582CDA4A9F
Phone Number
Product Version 9.2
Product Type iPhone5,2
Target Type Device
Serial Number C37JWNN2DTWD
iTunes Version 12.3.2.35
Target Identifier dfd550d3daf0ed503b634bcdc27c8c582cda4a9f
Detail
Display Name: iPhone de mohamed
Last Backup Date: 09/01/16 01:15
iTunes Files: Dict
Applications: Dict
net.whatsapp.WhatsApp: Dict
com.firsttouch.dts: Dict
com.miniclip.8ballpoolmult: Dict
Manifest
BackupKeyBag:
Lockdown: Dict
com.apple.MobileDeviceCrashCopy: Dict
com.apple.TerminalFlashr: Dict
SerialNumber: C37JWNN2DTWD
com.apple.mobile.wireless_lockdown: Dict
com.apple.mobile.data_sync: Dict
Bookmarks: Dict
Contacts: Dict
Calendars: Dict
Notes: Dict
AccountNames: Array
Sources: Array
iCloud
ProductType: iPhone5,2
BuildVersion: 13C75
UniqueDeviceID: dfd550d3daf0ed503b634bcdc27c8c582cda4a9f
ProductVersion: 9.2
com.apple.mobile.iTunes.accessories: Dict
DeviceName: iPhone de mohamed
com.apple.Accessibility: Dict
ZoomTouchEnabledByiTunes: false
ClosedCaptioningEnabledByiTunes: false



+21269		Sat Dec 26 22:18:03 WET 2015	RECEIVED	SMS
+21267		Sat Dec 26 17:35:06 WET 2015	SENT	SMS
+21269		Thu Dec 24 22:49:06 WET 2015	SENT	SMS
+21269		Mon Dec 28 23:44:29 WET 2015	SENT	SMS
+21269		Thu Dec 24 22:57:42 WET 2015	RECEIVED	SMS
+21269		Mon Dec 28 23:45:36 WET 2015	RECEIVED	SMS
+21263		Mon Dec 28 11:51:31 WET 2015	SENT	SMS
+21269		Sat Jan 02 16:29:09 WET 2016	RECEIVED	SMS
+21268		Fri Dec 25 16:33:53 WET 2015	SENT	SMS
+21269		Mon Dec 28 22:41:51 WET 2015	SENT	SMS
+21269		Mon Dec 28 23:38:19 WET 2015	SENT	SMS
+21268		Fri Dec 25 18:39:57 WET 2015	SENT	SMS


What
Addressbook entry
Message
media or image metadata
When
Events
Time
28-déc.
4-janv.
Casablanca
الدار البيضاء
Errahma
Bouskoura
Médiouna
Ain Harrouda
Tit Mellil
What
When
Where
Who
Addressbook entry Wed Dec 23 20:17:3...
Addressbook entry Tue Dec 22 19:47:24...
Message:Votre sold...
Message:Ouii ana d...
Addressbook entry Tue Dec 22 19:47:24...
Addressbook entry Wed Dec 23 20:17:4...
Message:Hhhh yak
Addressbook entry Tue Dec 22 19:47:23...
Addressbook entry Wed Dec 23 20:17:4...
Message:Hhhh yak
Addressbook entry Tue Dec 22 19:47:23...
Addressbook entry Tue Dec 22 19:47:23...
Addressbook entry Tue Dec 22 19:47:23...
Addressbook entry Wed Dec 23 20:17:4...
Addressbook entry Wed Dec 23 20:17:4...
Addressbook entry Wed Dec 23 20:17:3...
Addressbook entry Wed Dec 23 20:17:4...
Message:5 maximu...
Addressbook entry Tue Dec 22 19:47:23...
Addressbook entry Wed Dec 23 20:17:3...
1 selected events
Addressbook entry
Times
created addressbook entry
Wed Dec 23 23:43:07 WET 2015
modified addressbook entry
Wed Dec 23 20:17:40 WET 2015
Identities
Abderrahman (FIRST_NAME)
Mahraja (SURNAME)
$!<Mobile>!$ (PHONE_NUMBER)
backup File (v4): Library/AddressBook/AddressBook.sqlitedb (C:\Users\


Search
Search text:
Soufiane
Case sensitive
Case insensitive
Case sensitive
Regular expression
Fuzzy match
Cancel


Search Results - Found 24 hits in 3 files.
ChatStorage.sqlite
backup File (v4): ChatStorage.sqlite (C:\Users\Soufiane\Application Data\Apple Co
Library/Notes/notes.sqlite
backup File (v4): Library/Notes/notes.sqlite (C:\Users\Soufiane\Application Data\Ap
backup File (v4): Library/Notes/notes.sqlite (C:\Users\Soufiane\Application Data\Ap
Media/PhotoData/Photos.sqlite
backup File (v4): Media/PhotoData/Photos.sqlite (C:\Users\Soufiane\Application Da
backup File (v4): Media/PhotoData/Photos.sqlite (C:\Users\Soufiane\Application Da
backup File (v4): Media/PhotoData/Photos.sqlite (C:\Users\Soufiane\Application Da
backup File (v4): Media/PhotoData/Photos.sqlite (C:\Users\Soufiane\Application Da
backup File (v4): Media/PhotoData/Photos.sqlite (C:\Users\Soufiane\Application Da
backup File (v4): Media/PhotoData/Photos.sqlite (C:\Users\Soufiane\Application Da
backup File (v4): Media/PhotoData/Photos.sqlite (C:\Users\Soufiane\Application Da
backup File (v4): Media/PhotoData/Photos.sqlite (C:\Users\Soufiane\Application Da

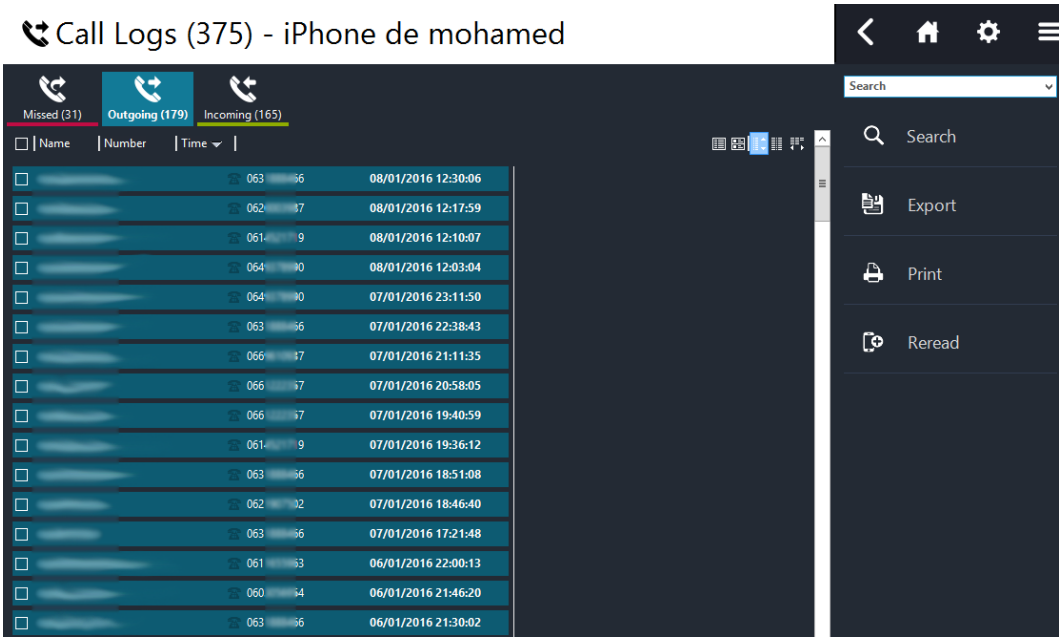
-----

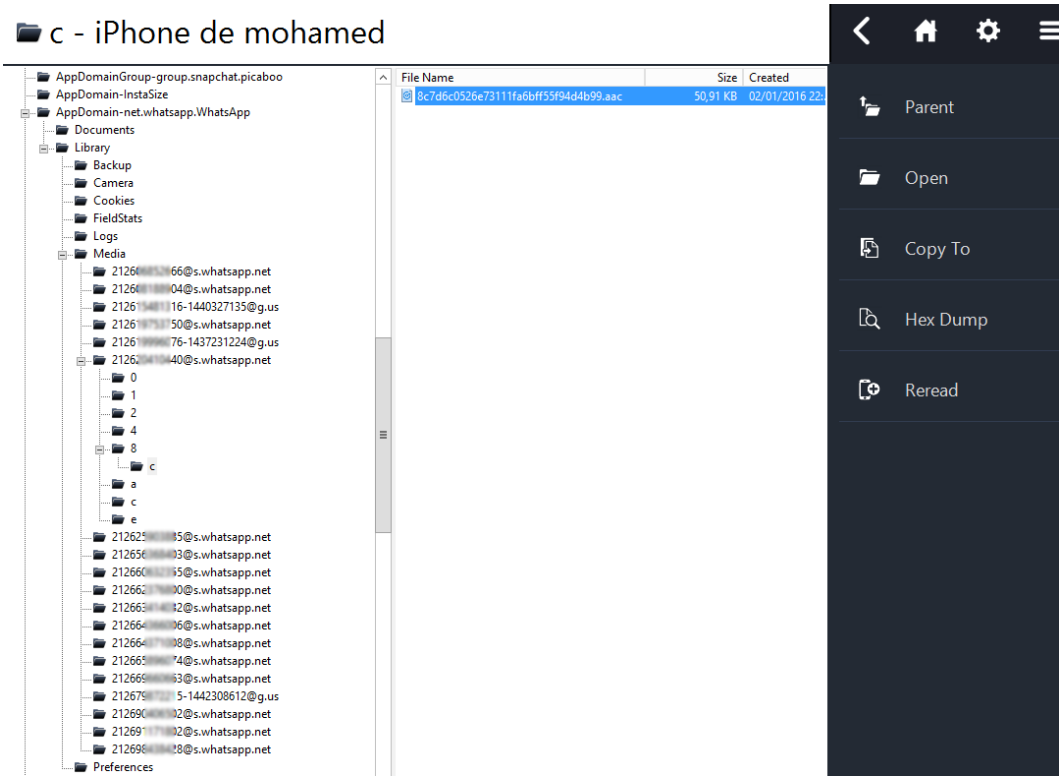

MOBILedit! Forensic
Navigation
Start
Start
Connected
iTunes Backups
Cases (2)
Hex Dump
Connected
No phone connected
Connect your phone and it will automatically appear here. If not, click...
Connect
SIM Clone
iTunes Backu
Cases
Hex Dump
Photo Viewer
Forensic Repo

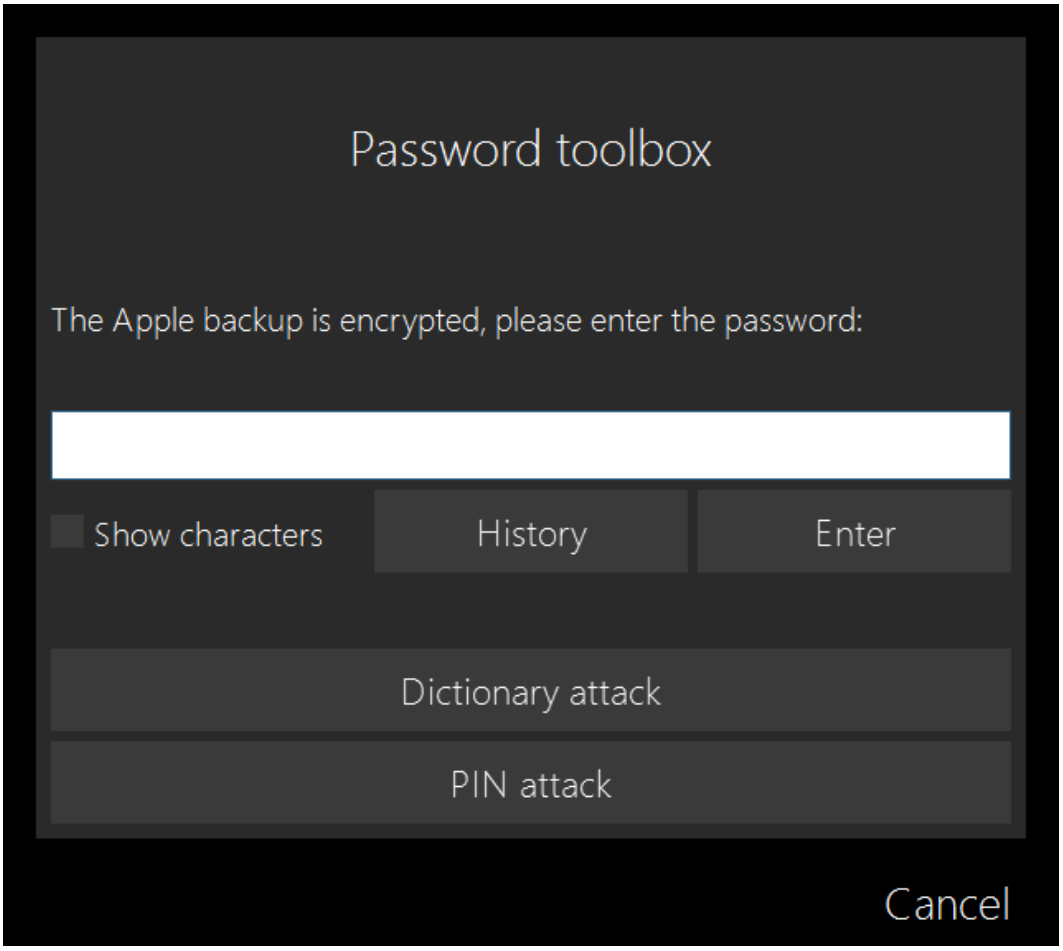

MOBILedit! Forensic
Navig
iTunes Backups
Start
Conn...
iTun...
Case...
Hex ...
Phot...
Fore...
This provides access to iPhone backups previously created by iTunes.
This appears only if you have iTunes installed. All data are read-only. You can browse, export or restore this data to the original phone in addition to restoring it to a different phone or different brand. You may also upload phone data to cloud storage using the Phone Copier feature. You have the ability to see individual contacts, copy them, print them, etc.
Reveal iTunes backups

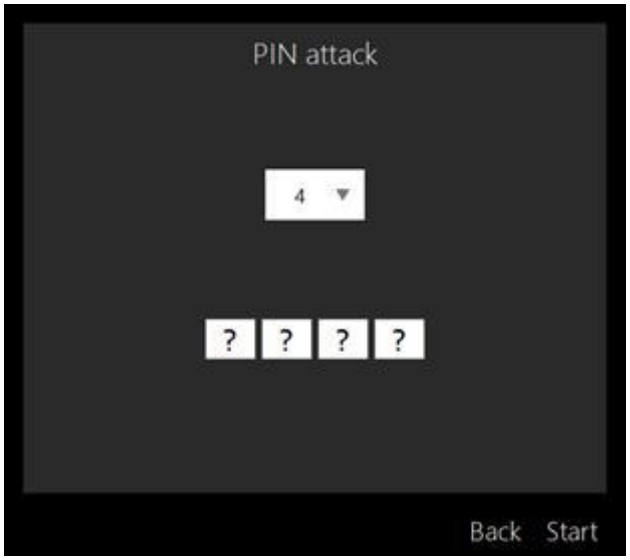

MOBILedit! Forensic
Navigation
Apple iPhone 5
Start
Conn...
iTune...
Apple iP...
Case...
Hex ...
Phot...
Fore...
Apple
iPhone 5
iPhone de mohamed
Last backup:
09/01/2016 01:28:46
First backup:
09/01/2016 01:15:39
Backup count:
2
09/01/2016 01:28:46
09/01/2016 01:15:39
iPhone de mohamed
09/01/2016 01:15:39
- Phonebook
- Call Logs
- Messages
- Files
- Applications

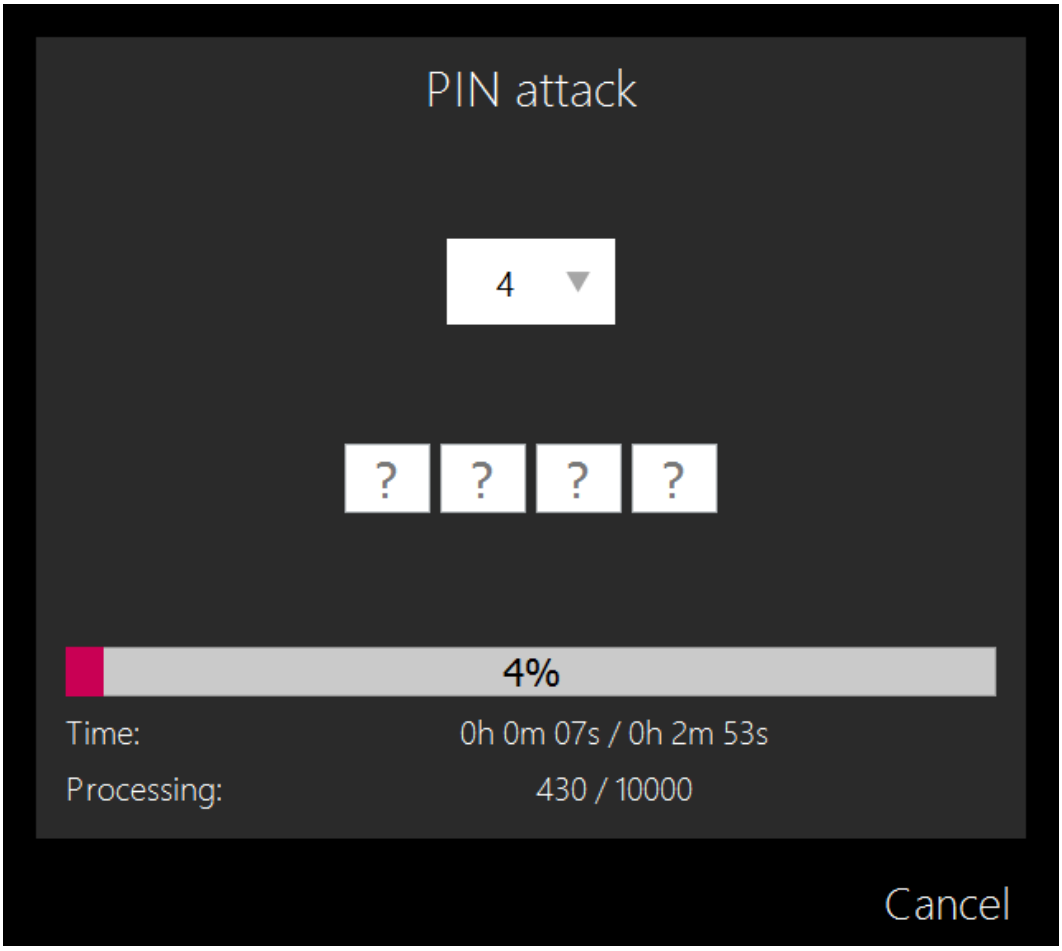

Online Info
iTunes Backup 9.2_Firmware:13
IMEI: 013412008655534
Not available
Manufacturer: Apple
Model: iPhone 5
Device name: iPhone de mohamed
iTunes backup created: 09/01/2016 01:15:39
IMEI: 013412008655534
Operator: Not available
Phone time: <unknown>
Software revision: 9.2_Firmware:13C75
Platform: iTunes Backup
Display resolution: 640 x 1136
Wallpaper resolution: 640 x 1136
Display colors: 262144
Phonebook
Call Logs
Messages
Application Data
Media
Calendar
Notes


Call Logs (375) - iPhone de mohamed
Missed (31)
Outgoing (179)
Incoming (165)
Name
Number
Time
063 66 08/01/2016 12:30:06
062 47 08/01/2016 12:17:59
061 9 08/01/2016 12:10:07
064 0 08/01/2016 12:03:04
064 0 07/01/2016 23:11:50
063 66 07/01/2016 22:38:43
066 47 07/01/2016 21:11:35
066 67 07/01/2016 20:58:05
066 67 07/01/2016 19:40:59
061 9 07/01/2016 19:36:12
063 66 07/01/2016 18:51:08
062 2 07/01/2016 18:46:40
063 66 07/01/2016 17:21:48
061 3 06/01/2016 22:00:13
060 4 06/01/2016 21:46:20
063 66 06/01/2016 21:30:02
Search
Search
Export
Print
Reread


c - iPhone de mohamed
AppDomainGroup-group.snapchat.picaboo
AppDomain-InstaSize
AppDomain-net.whatsapp.WhatsApp
Documents
Library
Backup
Camera
Cookies
FieldStats
Logs
Media
0
1
2
4
8
c
a
c
e
Preferences
File Name
Size
Created
8c7d6c0526e73111fa6bff55f94d4b99.aac
50,91 KB
02/01/2016 22
Parent
Open
Copy To
Hex Dump
Reread


Password toolbox
The Apple backup is encrypted, please enter the password:
Show characters
History
Enter
Dictionary attack
PIN attack
Cancel

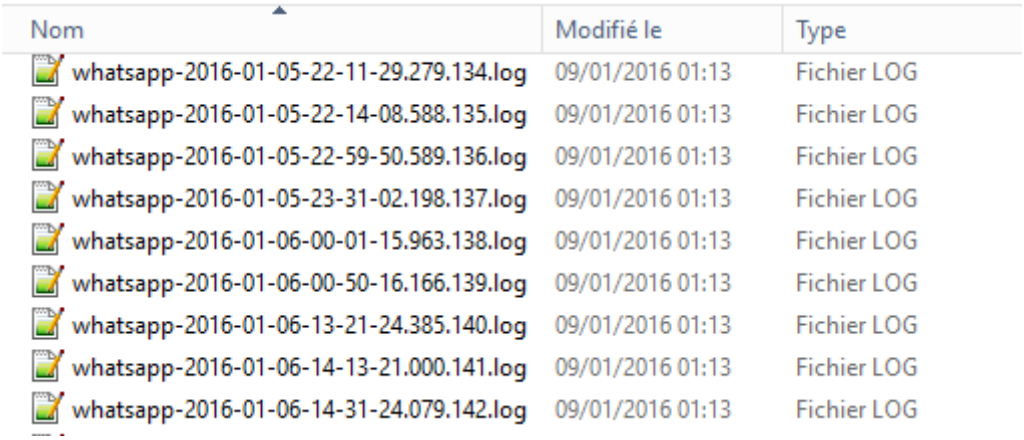

PIN attack
4
? ? ? ?
Back Start


PIN attack
4
? ? ? ?
4%
Time: 0h 0m 07s / 0h 2m 53s
Processing: 430 / 10000
Cancel


PIN attack
4
0 5 5 8
Successful
OK

XML View | List View

Key	Type	Value
Root	array	
	string	[illegible]
	string	[illegible]
	string	[illegible]
	string	[illegible]
	string	Disponible
	string	Occupé(e)
	string	À l'école
	string	Au cinéma
	string	Au travail
	string	Batterie faible
	string	Ne peux pas parler, WhatsApp uniquement
	string	En réunion
	string	À la salle de sport
	string	Endormi(e)
	string	Appels urgents uniquement



Nom	Modifié le	Type
whatsapp-2016-01-05-22-11-29.279.134.log	09/01/2016 01:13	Fichier LOG
whatsapp-2016-01-05-22-14-08.588.135.log	09/01/2016 01:13	Fichier LOG
whatsapp-2016-01-05-22-59-50.589.136.log	09/01/2016 01:13	Fichier LOG
whatsapp-2016-01-05-23-31-02.198.137.log	09/01/2016 01:13	Fichier LOG
whatsapp-2016-01-06-00-01-15.963.138.log	09/01/2016 01:13	Fichier LOG
whatsapp-2016-01-06-00-50-16.166.139.log	09/01/2016 01:13	Fichier LOG
whatsapp-2016-01-06-13-21-24.385.140.log	09/01/2016 01:13	Fichier LOG
whatsapp-2016-01-06-14-13-21.000.141.log	09/01/2016 01:13	Fichier LOG
whatsapp-2016-01-06-14-31-24.079.142.log	09/01/2016 01:13	Fichier LOG

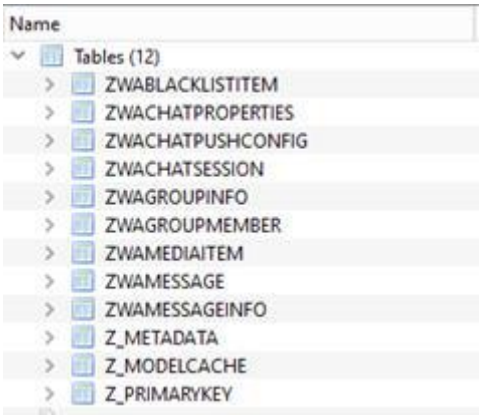


Table: ZWAMESSAGE

New Record | Delete Rec

	ZSENTDATE	ZFROMJID	MEDIASECTION	ZPUSHNAME	ZSTANZAID	ZTEXT	ZTOJID
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	NULL	2126199[illegible]6-I	NULL	Naim Wer	371BD43151AI	Taa [illegible] natti ?	NULL
2	NULL	2126199[illegible]6-I	NULL	Naim Wer	371BD43151AI	Galia [illegible]haliwI	NULL
3	NULL	2126199[illegible]6-I	NULL	Naim Wer	371BD43151AI	Gaa[illegible]ia	NULL
4	NULL	2126199[illegible]6-I	NULL	Naim Wer	371BD43151AI	Yaa [illegible]h	NULL
5	473906889	NULL	NULL	NULL	00D3A53E944I	Lay[illegible]	2126563[illegible]03I
6	NULL	2126563[illegible]3I	NULL	Yoùnés	FF34A34B0C4I	Iwa [illegible]ék ✌I	NULL
7	473906882	NULL	NULL	NULL	00D3A53E944I	3yto [illegible]i hhI	2126199[illegible]76-I
8	NULL	2126563[illegible]3I	NULL	Yoùnés	FF34A34B0C4I	Ah! B[illegible]	NULL
9	NULL	2126199[illegible]6-I	NULL	Naim Wer	371BD43151AI	Taa [illegible]ant f I	NULL
10	473906850	NULL	NULL	NULL	00D3A53E944I	Ayc[illegible] sbaI	2126199[illegible]76-I
11	473906838	NULL	NULL	NULL	00D3A53E944I	Oui [illegible]a	2126199[illegible]76-I

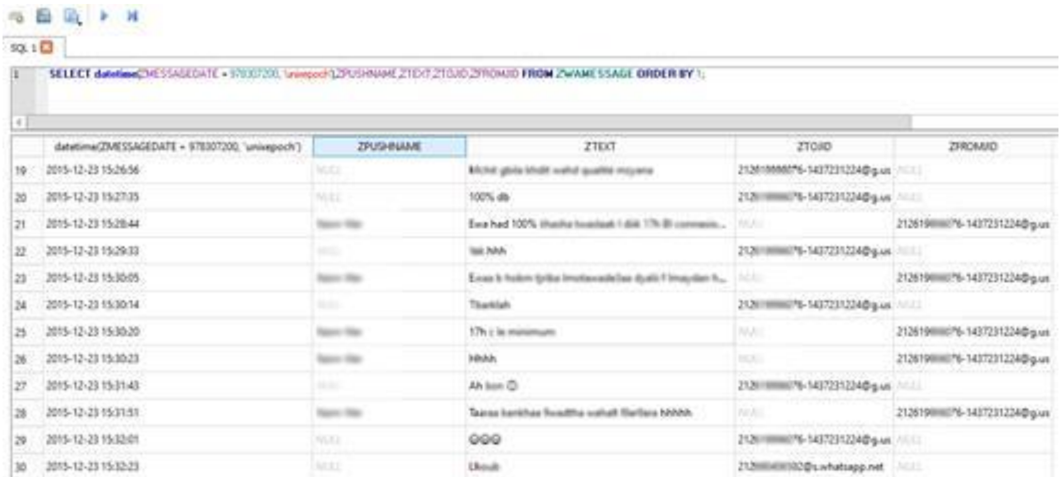
Table: ZWAMEDIAITEM

	INA	ZMEDIALOCALPATH
		Filter
7		Media/212619[illegible]076-1437231224@g.us/2/f/2f301028433b84cc15b29ee969e44536.aac
8		Media/212619[illegible]076-1437231224@g.us/4/f/4f0b79ae344567de1717aa992bcce476.aac
9		Media/212619[illegible]076-1437231224@g.us/5/2/5212e0ac4a12cd93f45093ab4efca0da.aac
10		Media/212619[illegible]076-1437231224@g.us/5/7/572d09db289deb58f2915e1ee530353d.aac
11		Media/212679[illegible]215-1442308612@g.us/4/4/4474fdbe74bf2382bd81ecae2fbab119.mp4
12		Media/212679[illegible]215-1442308612@g.us/0/4/04a7e161835bdcc80e6b1f1937cacc18.jpg
13		Media/212679[illegible]215-1442308612@g.us/0/e/0e8f5e984f228d7b3ea6bd84bb34a788.jpg
14		Media/212679[illegible]215-1442308612@g.us/6/3/635dc2cfa9eb684f5d1da6db5176bd0b.mp4
15		Media/212679[illegible]215-1442308612@g.us/8/4/84273f1523910f006d2188b077e89253.jpg
16		Media/212625[illegible]385@s.whatsapp.net/8/0/80aab605be635881524be186df58c3d8.jpg
17		Media/212679[illegible]215-1442308612@g.us/9/9/99df11c03bbdd7e3e96c856370dd280b.jpg
18		Media/212664[illegible]006@s.whatsapp.net/6/0/609ac1d74632d2644aa677a768a55bda.jpg
19		Media/212679[illegible]215-1442308612@g.us/1/b/1b5304f8e5020d798c0d74685ce2e065.jpg
20		Media/212679[illegible]215-1442308612@g.us/e/3/e39b033703a2686ab4300a66e8816865.jpg
21		Media/212679[illegible]215-1442308612@g.us/e/7/e75e34fddb724c2617281fbc14db3c7c.jpg
22		Media/212679[illegible]215-1442308612@g.us/2/2/220612254f9e04b1a3261f1d39d8a4f5.aac

net.whatsapp.WhatsApp › Library › Media

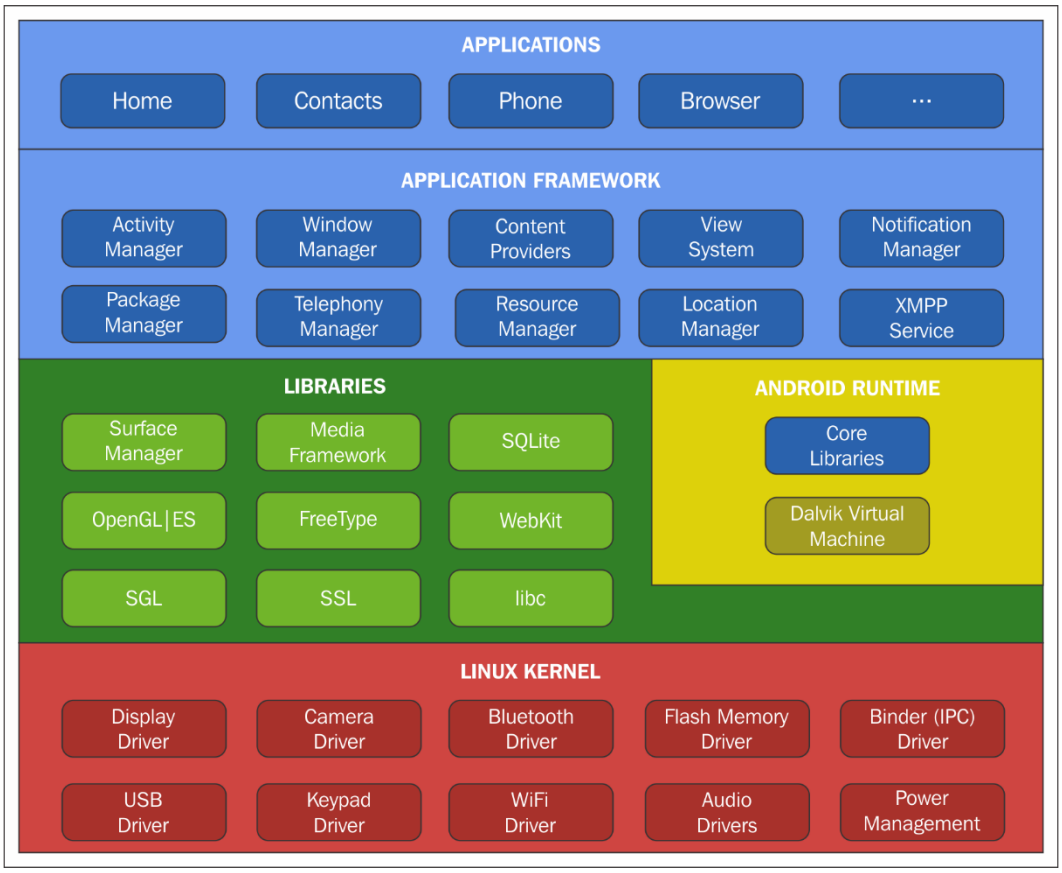
Rech

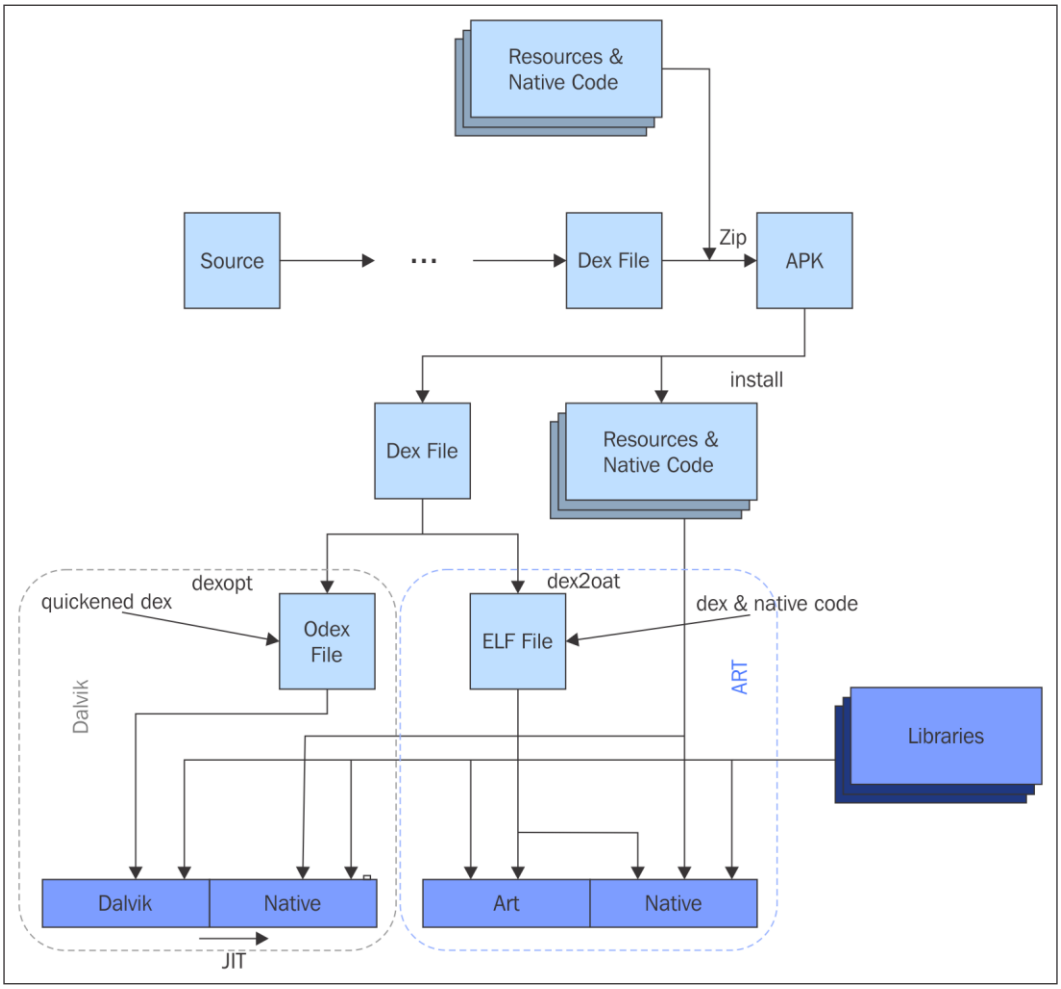
Nom	Modifié le
21260[illegible]666@s.whatsapp.net	13/01/2016 14:54
21260[illegible]04@s.whatsapp.net	13/01/2016 14:54
21261[illegible]16-1440327135@g.us	13/01/2016 14:54
21261[illegible]50@s.whatsapp.net	13/01/2016 14:54
21261[illegible]76-1437231224@g.us	13/01/2016 14:54
21262[illegible]40@s.whatsapp.net	13/01/2016 14:54
21262[illegible]85@s.whatsapp.net	13/01/2016 14:54
21265[illegible]03@s.whatsapp.net	13/01/2016 14:54
21266[illegible]55@s.whatsapp.net	13/01/2016 14:54
21266[illegible]00@s.whatsapp.net	13/01/2016 14:54
21266[illegible]32@s.whatsapp.net	13/01/2016 14:54
21266[illegible]06@s.whatsapp.net	13/01/2016 14:54
21266[illegible]08@s.whatsapp.net	13/01/2016 14:54
21266[illegible]74@s.whatsapp.net	13/01/2016 14:54
21266[illegible]63@s.whatsapp.net	13/01/2016 14:54
21267[illegible]15-1442308612@g.us	13/01/2016 14:59
21269[illegible]02@s.whatsapp.net	13/01/2016 14:59
21269[illegible]02@s.whatsapp.net	13/01/2016 14:59
21269[illegible]28@s.whatsapp.net	13/01/2016 14:59

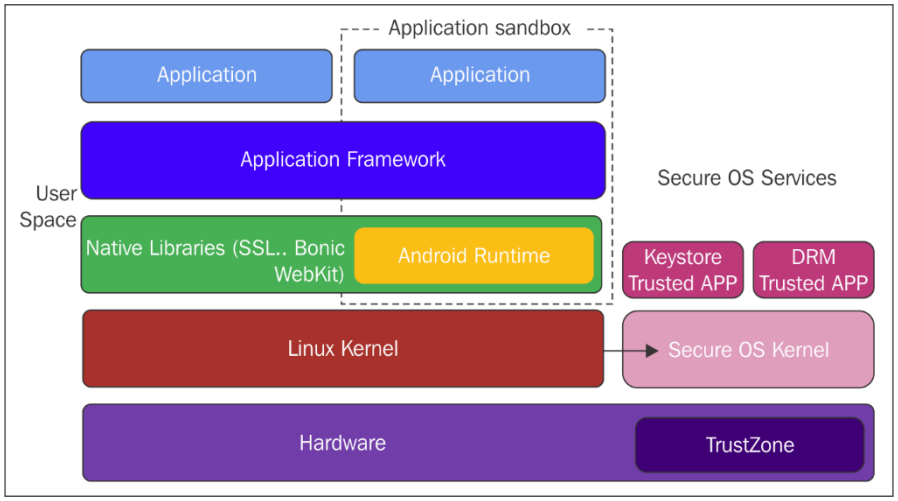

SQL 1
SELECT datetime(ZMESSAGEDATE + 978307200, 'unixepoch'),ZPUSHNAME,ZTEXT,ZTOJID,ZFROMJID FROM ZWAMESSAGE ORDER BY 1;
datetime(ZMESSAGEDATE + 978307200, 'unixepoch')
ZPUSHNAME
ZTEXT
ZTOJID
ZFROMJID
2015-12-23 15:26:56
2015-12-23 15:27:35
2015-12-23 15:28:44
2015-12-23 15:29:33
2015-12-23 15:30:05
2015-12-23 15:30:14
2015-12-23 15:30:20
2015-12-23 15:30:23
2015-12-23 15:31:43
2015-12-23 15:31:51
2015-12-23 15:32:01
2015-12-23 15:32:23

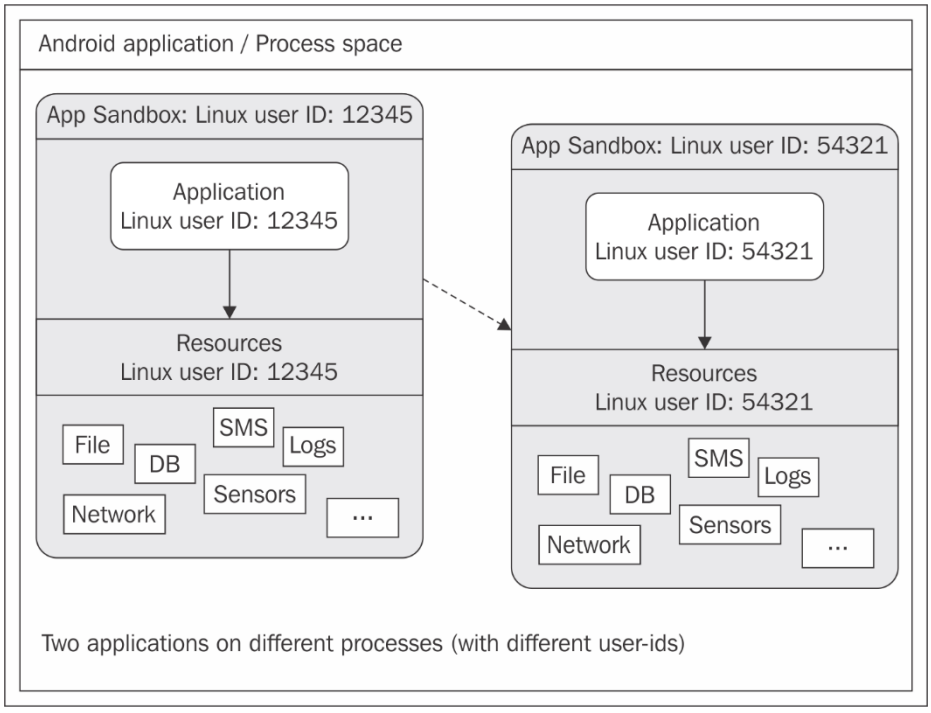

495 Free Block 1861013 109 am E5! ??121261
076-1437231224@g.us
371BD43151AB493C1E2
Yaak hhhhh
496 Free Block 1861473 7
497 Free Block 1861605 106 jC5^ ?>2126
03@s.whatsapp.net
FF34A34B0C42A6BFDF1
Ah! Bon

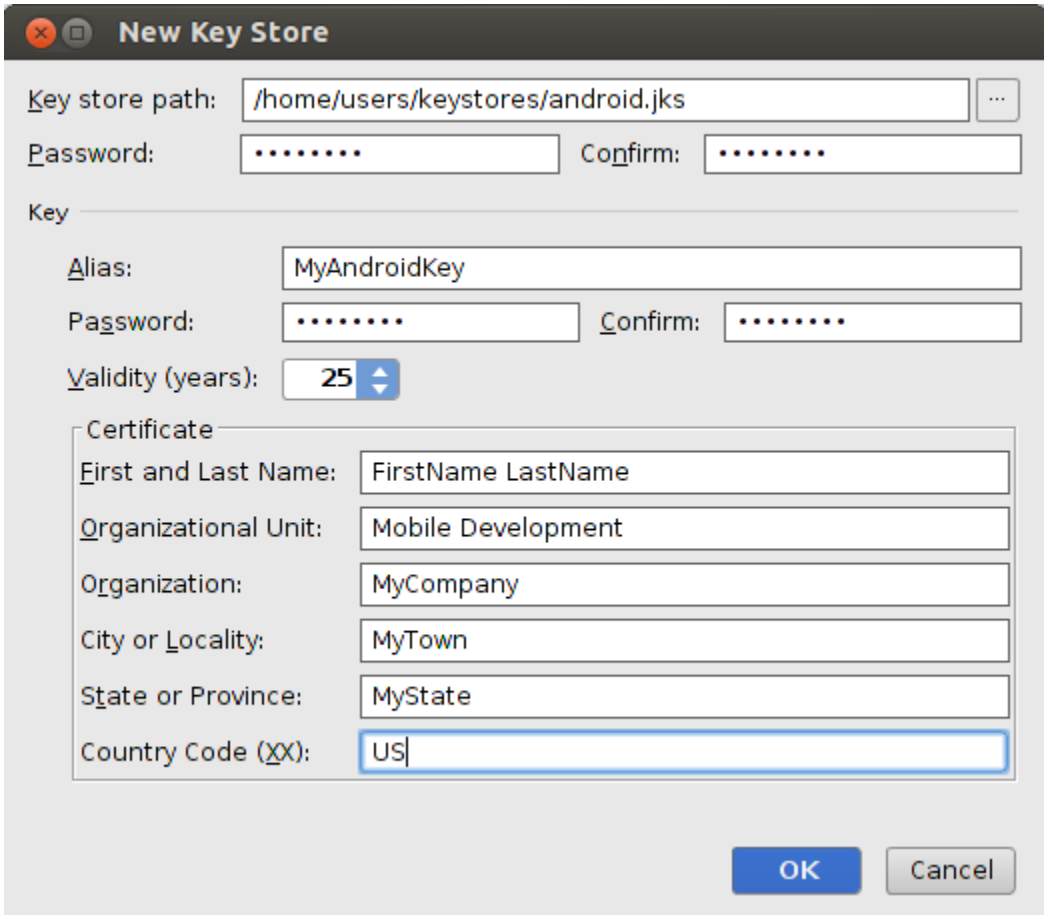
Chapter 4: Android Forensics

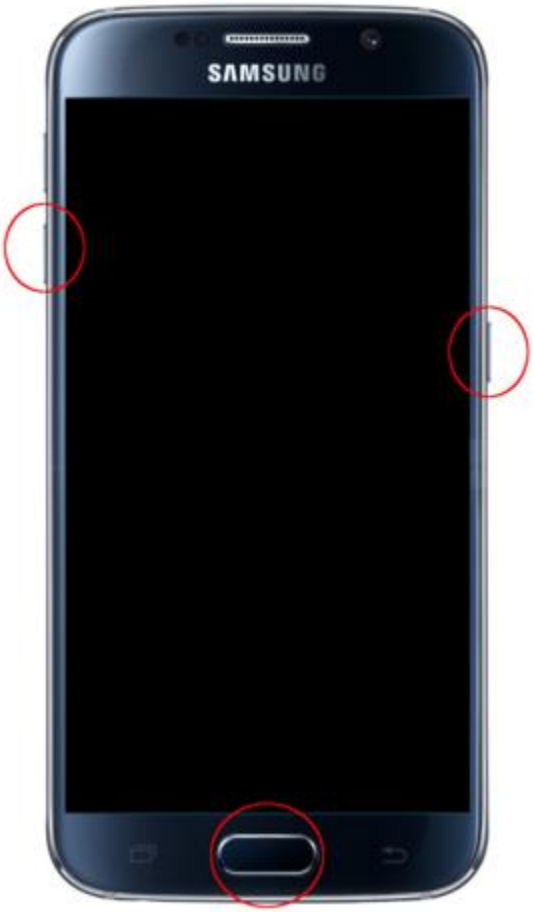



Resources &
Native Code
Source
...
Dex File
Zip
APK
install
Dex File
Resources &
Native Code
dexopt
quickened dex
Odex
File
dex2oat
ELF File
dex & native code
ART
Dalvik
Libraries
Dalvik
Native
Art
Native
JIT

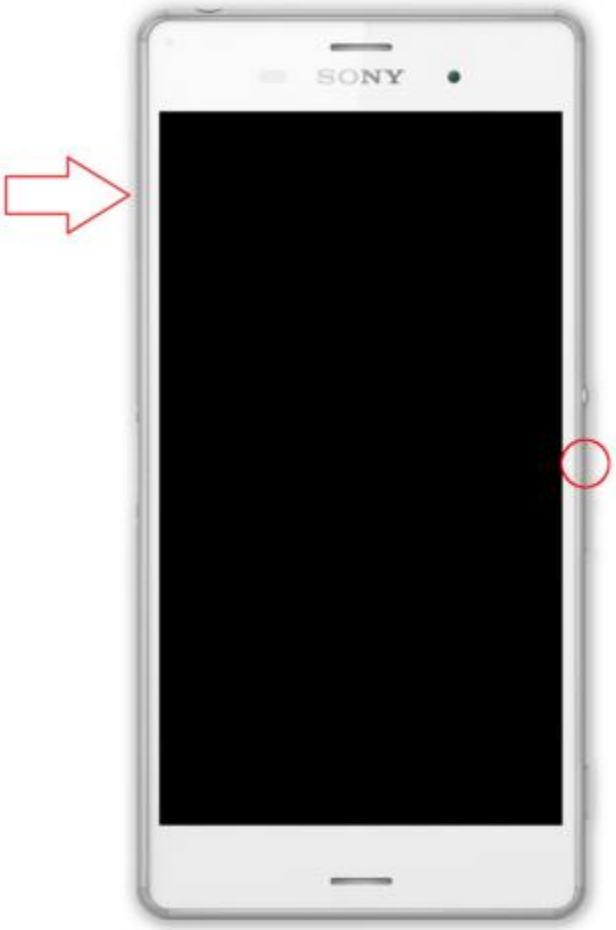

Application sandbox
Application
Application
Application Framework
User Space
Native Libraries (SSL.. Bonic WebKit)
Android Runtime
Secure OS Services
Keystore Trusted APP
DRM Trusted APP
Linux Kernel
Secure OS Kernel
Hardware
TrustZone

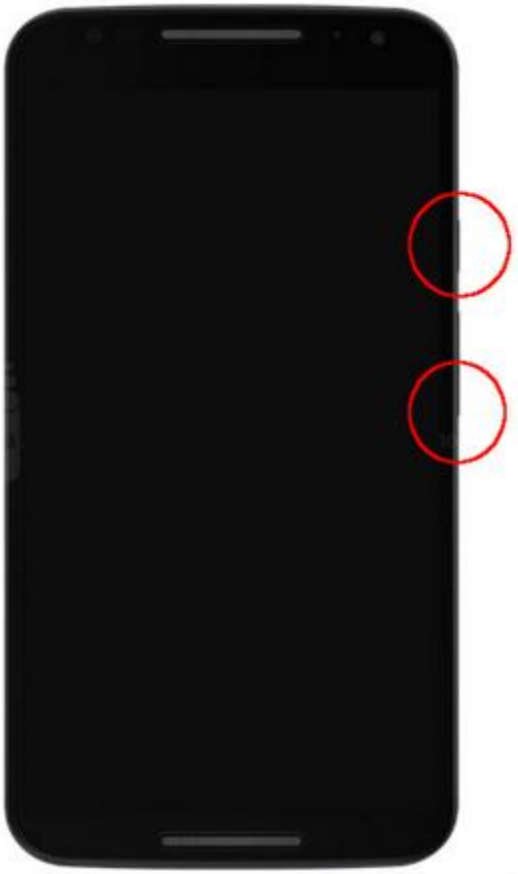

Android application / Process space
App Sandbox: Linux user ID: 12345
Application
Linux user ID: 12345
Resources
Linux user ID: 12345
File
DB
SMS
Logs
Network
Sensors
...
App Sandbox: Linux user ID: 54321
Application
Linux user ID: 54321
Resources
Linux user ID: 54321
File
DB
SMS
Logs
Network
Sensors
...
Two applications on different processes (with different user-ids)

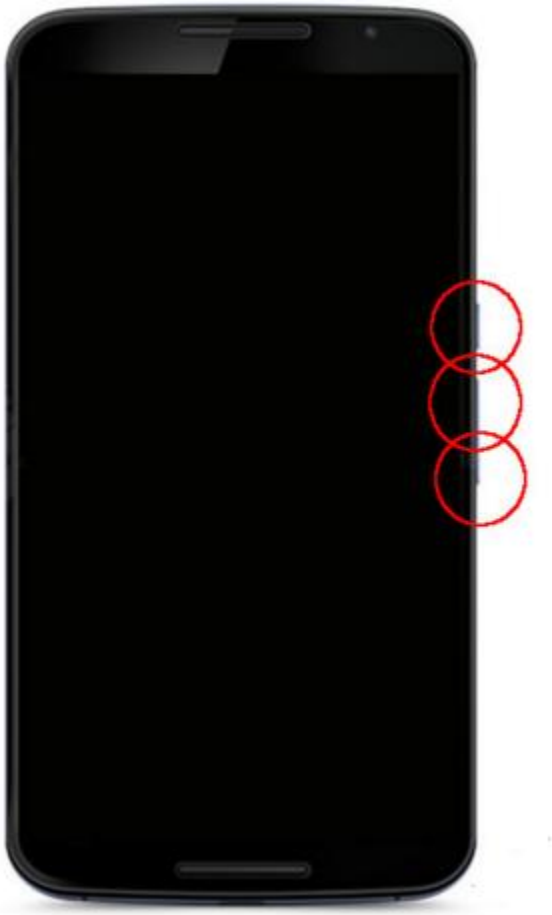

New Key Store
Key store path:
/home/users/keystores/android.jks
Password:
Confirm:
Key
Alias:
MyAndroidKey
Password:
Confirm:
Validity (years):
25
Certificate
First and Last Name:
FirstName LastName
Organizational Unit:
Mobile Development
Organization:
MyCompany
City or Locality:
MyTown
State or Province:
MyState
Country Code (XX):
US
OK
Cancel


SAMSUNG

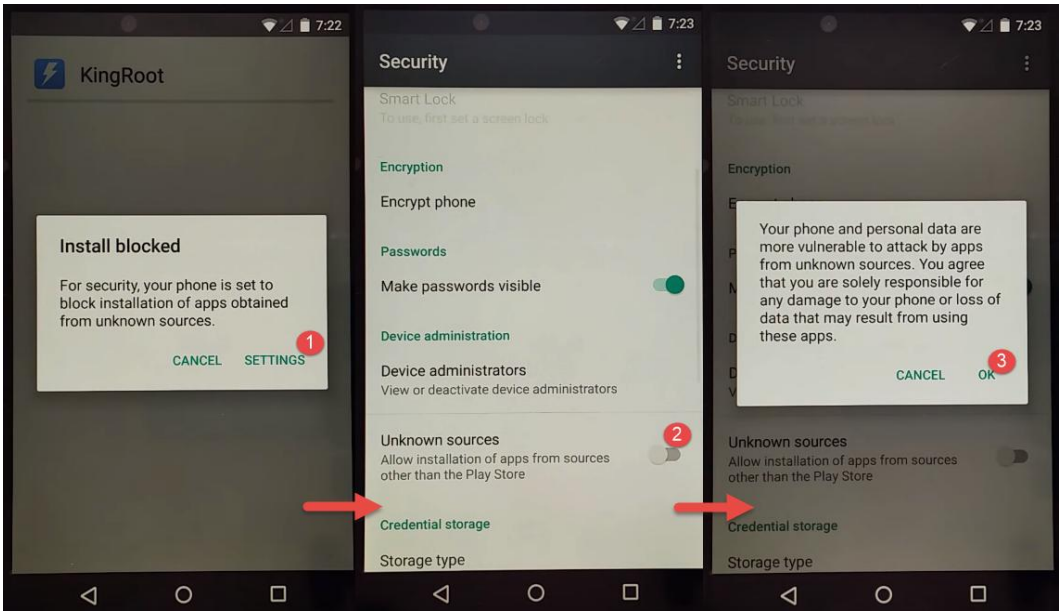

htc

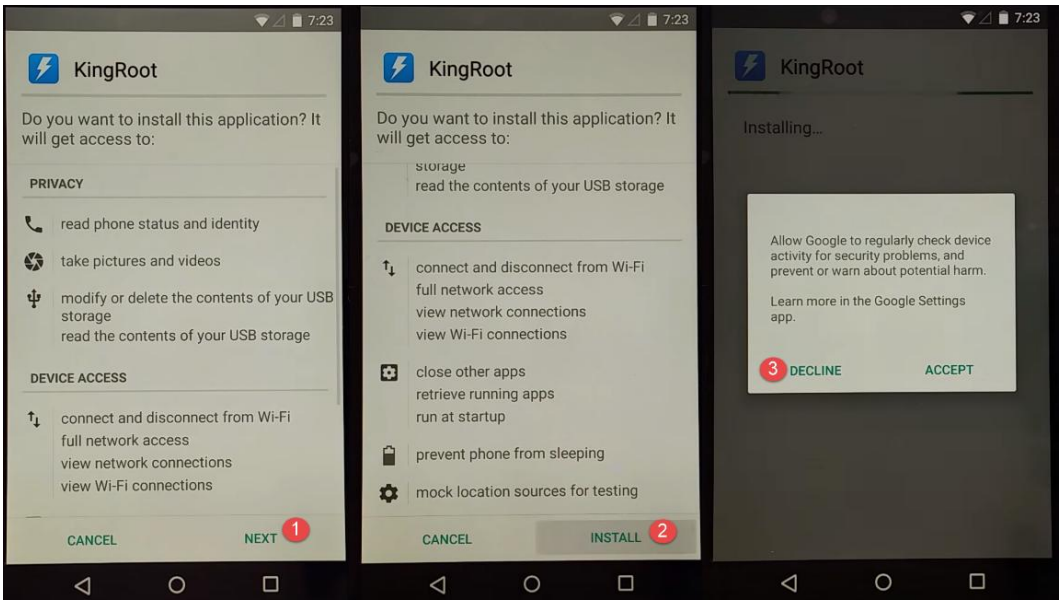

SONY

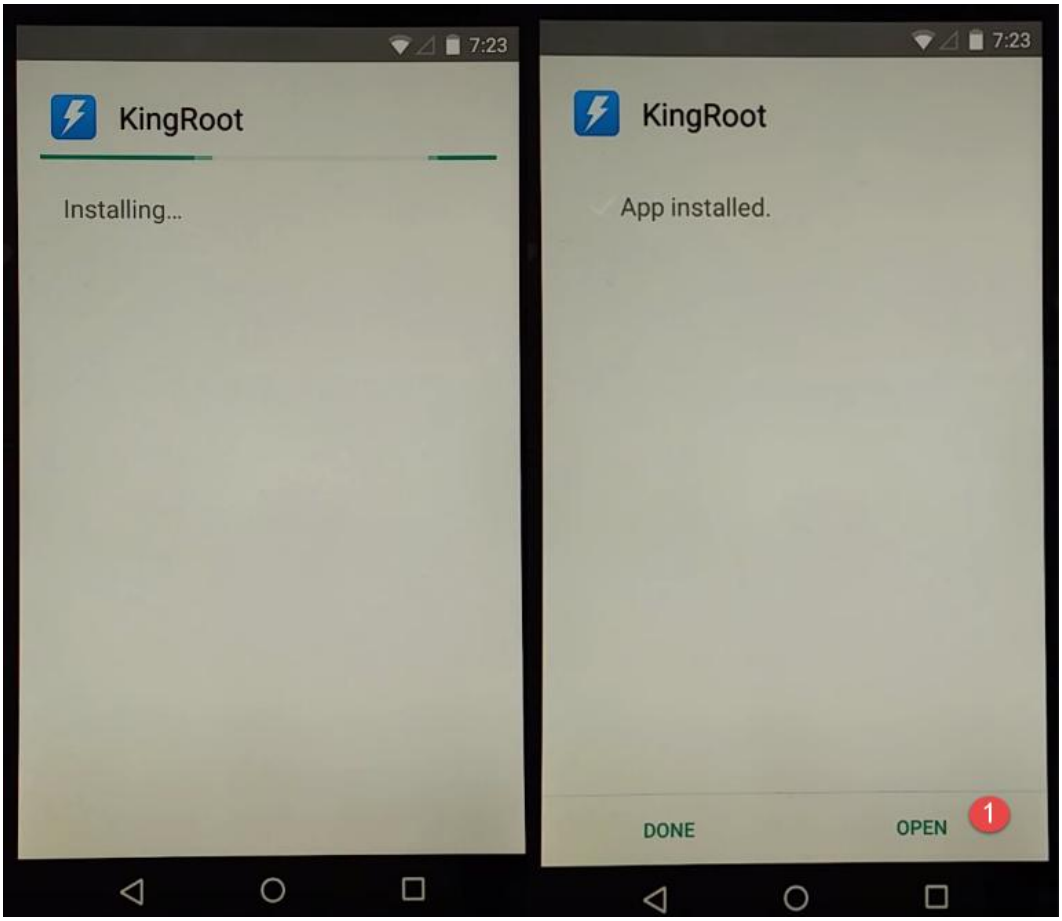


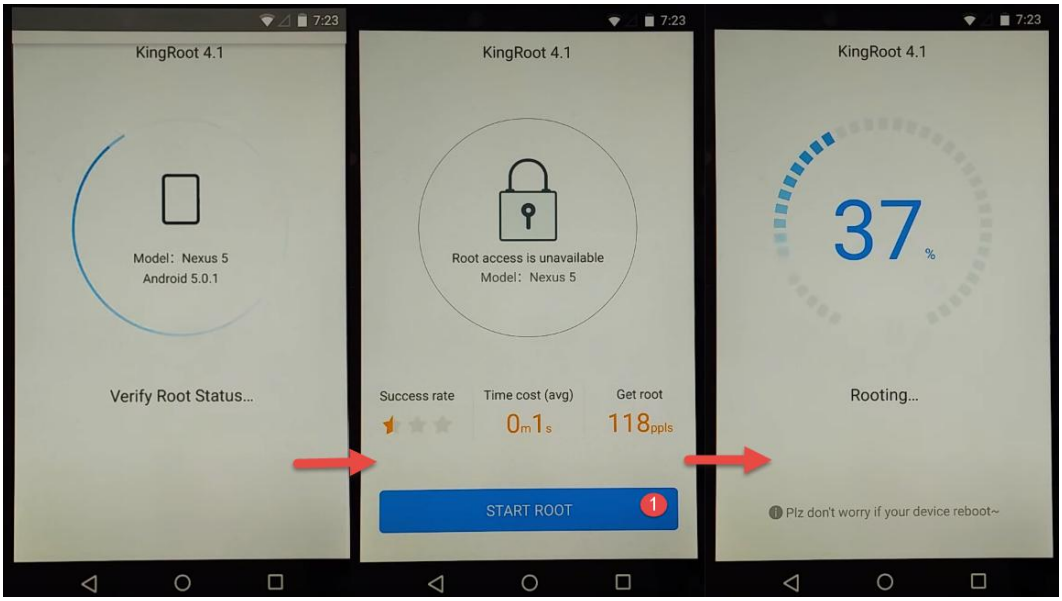


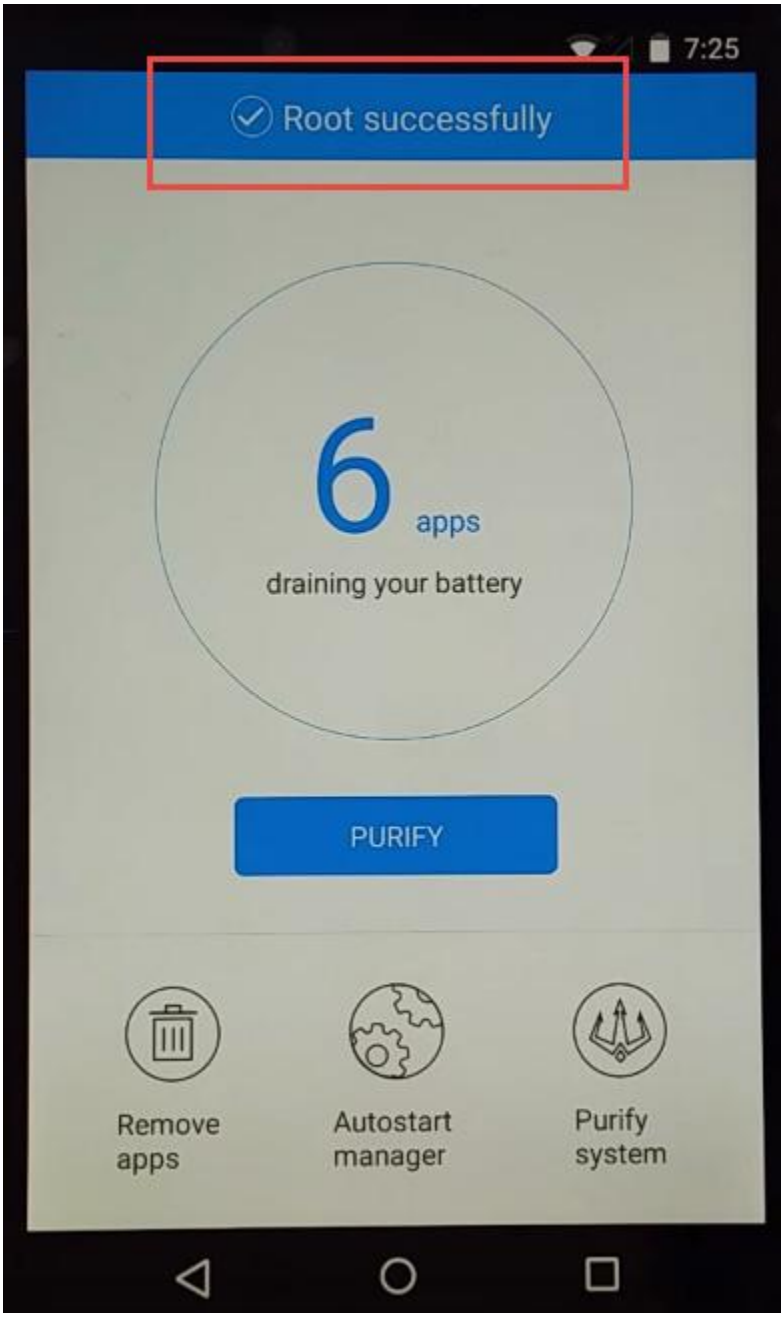
```
C:\Users\Soufiane\AppData\Local\Android\sdk\platform-tools>adb reboot-bootloader
```

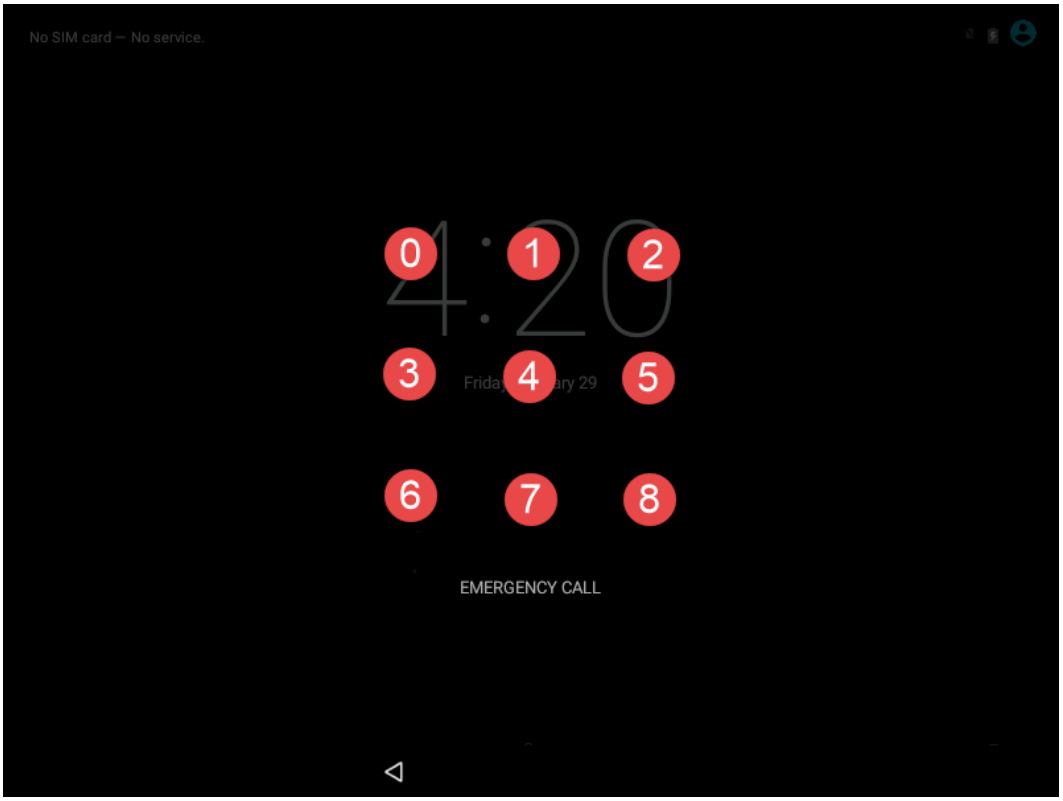

7:22
KingRoot
Install blocked
For security, your phone is set to block installation of apps obtained from unknown sources.
CANCEL
SETTINGS
1
7:23
Security
Smart Lock
To use, first set a screen lock
Encryption
Encrypt phone
Passwords
Make passwords visible
Device administration
Device administrators
View or deactivate device administrators
Unknown sources
Allow installation of apps from sources other than the Play Store
2
Credential storage
Storage type
7:23
Security
Encryption
Your phone and personal data are more vulnerable to attack by apps from unknown sources. You agree that you are solely responsible for any damage to your phone or loss of data that may result from using these apps.
CANCEL
OK
3
Unknown sources
Allow installation of apps from sources other than the Play Store
Credential storage
Storage type

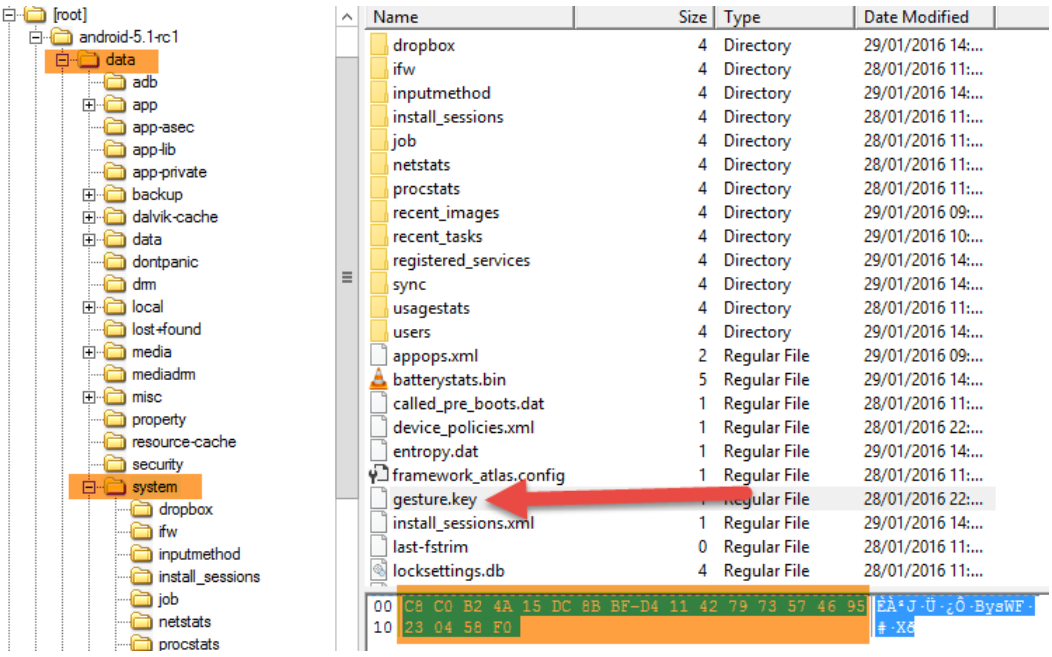

7:23
KingRoot
Do you want to install this application? It will get access to:
PRIVACY
read phone status and identity
take pictures and videos
modify or delete the contents of your USB storage
read the contents of your USB storage
DEVICE ACCESS
connect and disconnect from Wi-Fi
full network access
view network connections
view Wi-Fi connections
CANCEL
NEXT
1
7:23
KingRoot
Do you want to install this application? It will get access to:
read the contents of your USB storage
DEVICE ACCESS
connect and disconnect from Wi-Fi
full network access
view network connections
view Wi-Fi connections
close other apps
retrieve running apps
run at startup
prevent phone from sleeping
mock location sources for testing
CANCEL
INSTALL
2
7:23
KingRoot
Installing...
Allow Google to regularly check device activity for security problems, and prevent or warn about potential harm.
Learn more in the Google Settings app.
3
DECLINE
ACCEPT

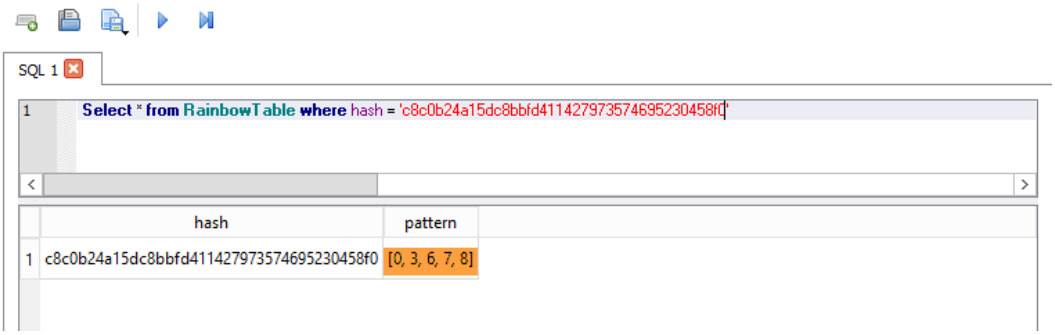

7:23
KingRoot
Installing...
7:23
KingRoot
App installed.
DONE
OPEN
1

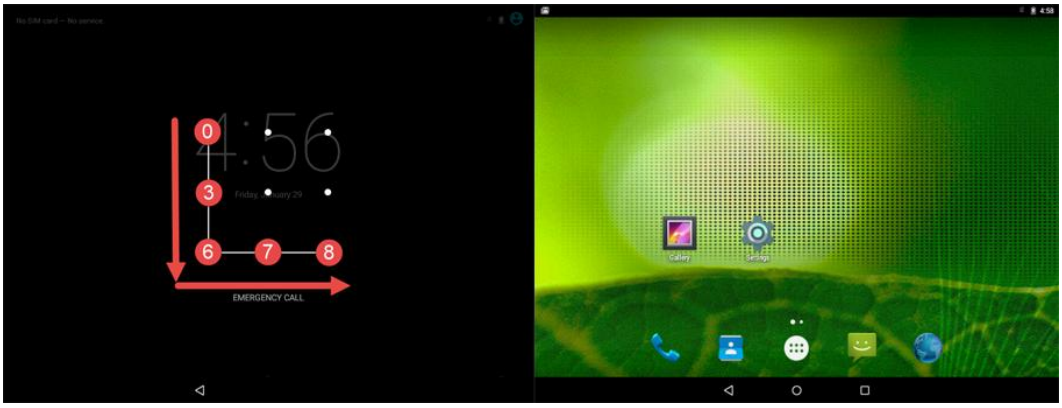

7:23
KingRoot 4.1
Model：Nexus 5
Android 5.0.1
Verify Root Status...
7:23
KingRoot 4.1
Root access is unavailable
Model：Nexus 5
Success rate
Time cost (avg)
0m1s
Get root
118ppls
START ROOT
1
7:23
KingRoot 4.1
37%
Rooting...
Plz don't worry if your device reboot~


7:25
Root successfully
6
apps
draining your battery
PURIFY
Remove apps
Autostart manager
Purify system


No SIM card – No service.
4:20
0
1
2
3
4
5
6
7
8
EMERGENCY CALL

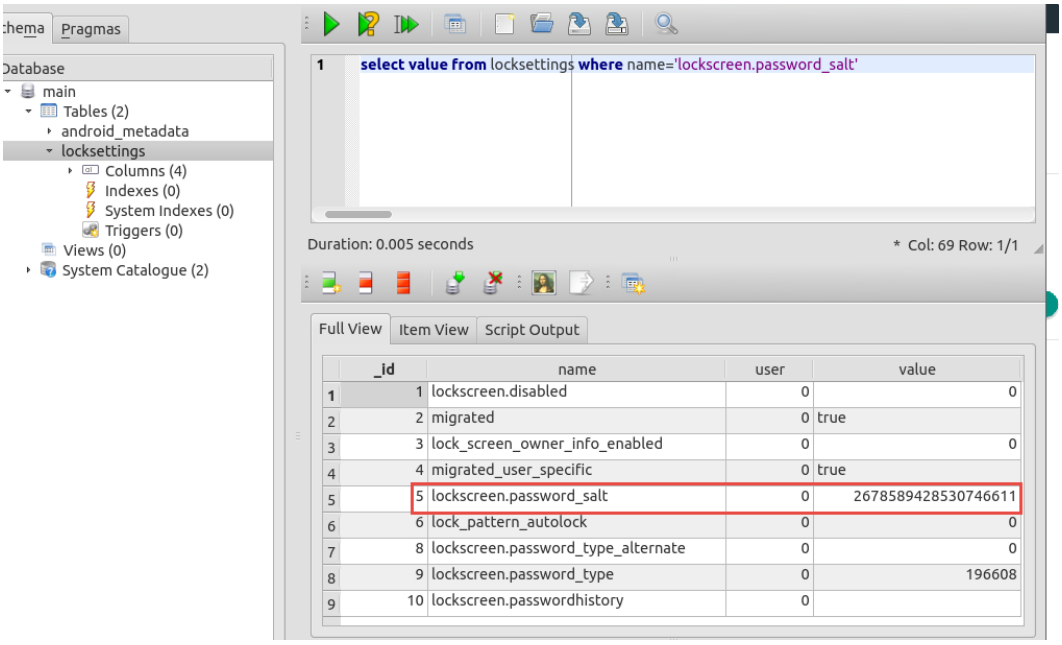

[root]
android-5.1-rc1
data
adb
app
app-asec
app-lib
app-private
backup
dalvik-cache
data
dontpanic
dm
local
lost+found
media
mediadrm
misc
property
resource-cache
security
system
dropbox
ifw
inputmethod
install_sessions
job
netstats
procstats
Name
Size
Type
Date Modified
dropbox 4 Directory 29/01/2016 14:...
ifw 4 Directory 28/01/2016 11:...
inputmethod 4 Directory 29/01/2016 14:...
install_sessions 4 Directory 28/01/2016 11:...
job 4 Directory 28/01/2016 11:...
netstats 4 Directory 28/01/2016 11:...
procstats 4 Directory 28/01/2016 11:...
recent_images 4 Directory 29/01/2016 09:...
recent_tasks 4 Directory 29/01/2016 10:...
registered_services 4 Directory 29/01/2016 14:...
sync 4 Directory 29/01/2016 14:...
usagestats 4 Directory 28/01/2016 11:...
users 4 Directory 29/01/2016 14:...
appops.xml 2 Regular File 29/01/2016 09:...
batterystats.bin 5 Regular File 29/01/2016 14:...
called_pre_boots.dat 1 Regular File 28/01/2016 11:...
device_policies.xml 1 Regular File 28/01/2016 22:...
entropy.dat 1 Regular File 29/01/2016 14:...
framework_atlas.config 1 Regular File 28/01/2016 11:...
gesture.key
install_sessions.xml 1 Regular File 29/01/2016 14:...
last-fstrim 0 Regular File 28/01/2016 11:...
locksettings.db 4 Regular File 28/01/2016 11:...
00 C8 C0 B2 4A 15 DC 8B BF D4 11 42 79 73 57 46 95
10 23 04 58 F0


SQL 1
1 Select * from RainbowTable where hash = 'c8c0b24a15dc8bbfd411427973574695230458f0'
hash
pattern
1 c8c0b24a15dc8bbfd411427973574695230458f0 [0, 3, 6, 7, 8]



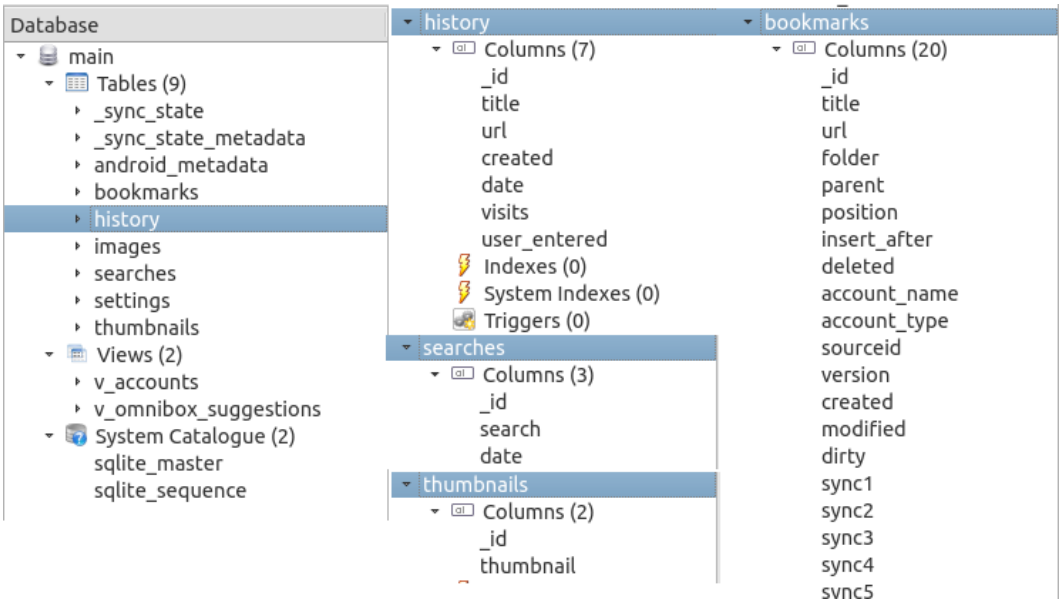
```
C:\Users\Soufiane\AppData\Local\Android\sdk\platform-tools>adb pull /data/system/gesture.key
3 KB/s (20 bytes in 0.006s)

C:\Users\Soufiane\AppData\Local\Android\sdk\platform-tools>
```

```
C:\Users\Soufiane\AppData\Local\Android\sdk\platform-tools>adb root
restarting adbd as root
```



```
C:\Users\Soufiane\Downloads\hashcat-2.00>hashcat-cli64.exe -m 10 hash.txt -a 3 ?d?d?d?d
Initializing hashcat v2.00 with 8 threads and 32mb segment-size...

Added hashes from file hash.txt: 1 (1 salts)
Activating quick-digest mode for single-hash with salt

5aa4ca29d6221fc7de4aec5349c257f3:252c42e4bab114f3:0912

All hashes have been recovered

Input.Mode: Mask (?d?d?d?d) [4]
Index.....: 0/1 (segment), 10000 (words), 0 (bytes)
Recovered.: 1/1 hashes, 1/1 salts
Speed/sec.: - plains, 9.65k words
Progress..: 9694/10000 (96.94%)
Running...: 00:00:00:01
Estimated.: --:--:--:--


Started: Tue Feb 02 19:34:40 2016
Stopped: Tue Feb 02 19:34:41 2016
```

```
-rw------- u0_a15   u0_a15     428512 2016-02-04 13:50 browser2.db-wal
root@generic:/ # ls -l /data/data/com.android.browser/
drwxrwx--x u0_a15   u0_a15            2016-02-04 13:16 app_appcache
drwxrwx--x u0_a15   u0_a15            2016-02-04 13:16 app_databases
drwxrwx--x u0_a15   u0_a15            2016-02-04 13:16 app_geolocation
drwxrwx--x u0_a15   u0_a15            2016-02-04 13:16 app_icons
drwxrwx--x u0_a15   u0_a15            2016-02-04 13:16 app_webview
drwxrwx--x u0_a15   u0_a15            2016-02-04 13:50 cache
drwxrwx--x u0_a15   u0_a15            2016-02-04 13:16 databases
drwxrwx--x u0_a15   u0_a15            2016-02-04 13:16 files
lrwxrwxrwx install  install           2016-02-03 01:11 lib -> /data/app-lib/com.android.browser
drwxrwx--x u0_a15   u0_a15            2016-02-04 13:43 shared_prefs
root@generic:/ # ls -l /data/data/com.android.browser/databases
-rw-rw---- u0_a15   u0_a15     483328 2016-02-04 13:48 browser2.db
-rw------- u0_a15   u0_a15      32768 2016-02-04 13:50 browser2.db-shm
-rw------- u0_a15   u0_a15     428512 2016-02-04 13:50 browser2.db-wal
root@generic:/ #
```



Titles

1	Google
2	Sign in - Google Accounts
3	https://accounts.google.com/ServiceLogin?hl=en&passive=true&continue=https://www.google.com/webh
4	Google Accounts
5	Google - Android Apps on Google Play
6	Welcome to Facebook
7	Enter Security Code to Continue
8	Remember Browser
9	Facebook
10	Mobile Uploads
11	Facebook

URLs

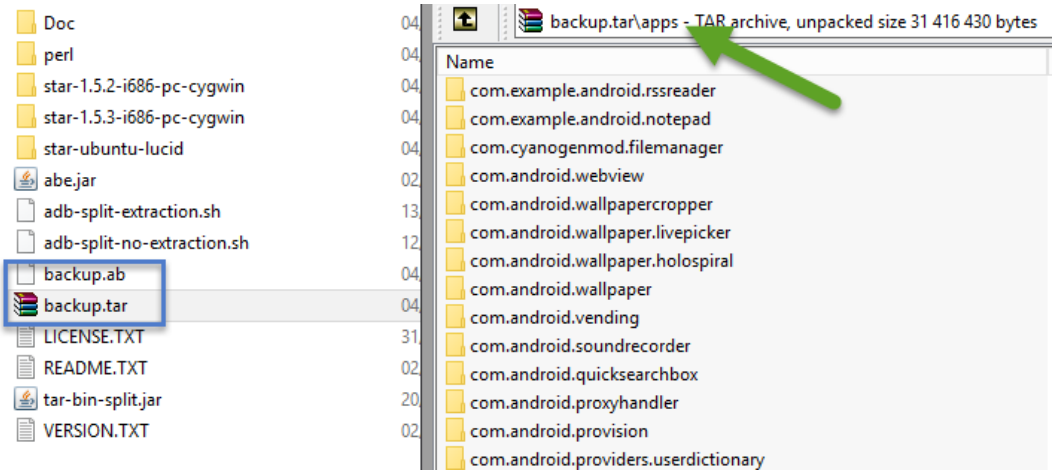
1	https://www.google.com/webhp?source=android-home
2	https://accounts.google.com/ServiceLogin?hl=en&passive=true&continue=https://www.google.com/webhp%3F
3	https://accounts.google.com/ServiceLogin?hl=en&passive=true&continue=https://www.google.com/webhp%3F
4	https://accounts.google.com/CheckCookie?hl=en&checkedDomains=youtube&checkConnection=youtube%3A6
5	https://play.google.com/store/apps/details?id=com.google.android.googlequicksearchbox
6	https://m.facebook.com/?_rdr&refsrc=https%3A%2F%2Fwww.facebook.com%2F
7	https://m.facebook.com/checkpoint/?refid=8&_rdr
8	https://m.facebook.com/login/checkpoint/
9	https://m.facebook.com/login/save-device/?next&_rdr

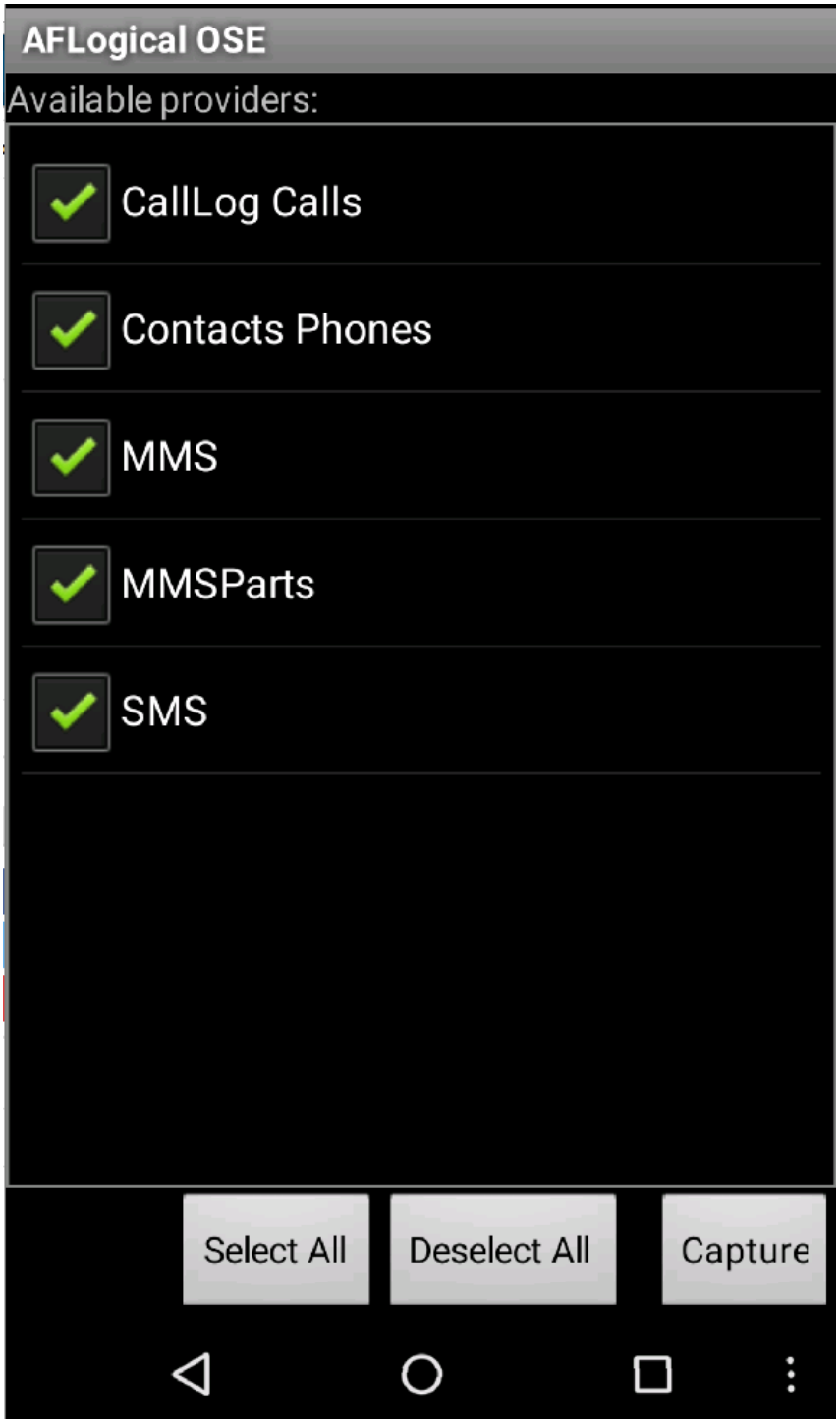
date	visits
1454592917858	3
1454591876048	2
1454592856064	2
1454591922655	1
1454593432406	2
1454593458187	1
1454593506354	1
1454593579100	2
1454593590962	1
1454593822912	6
1454593616727	1

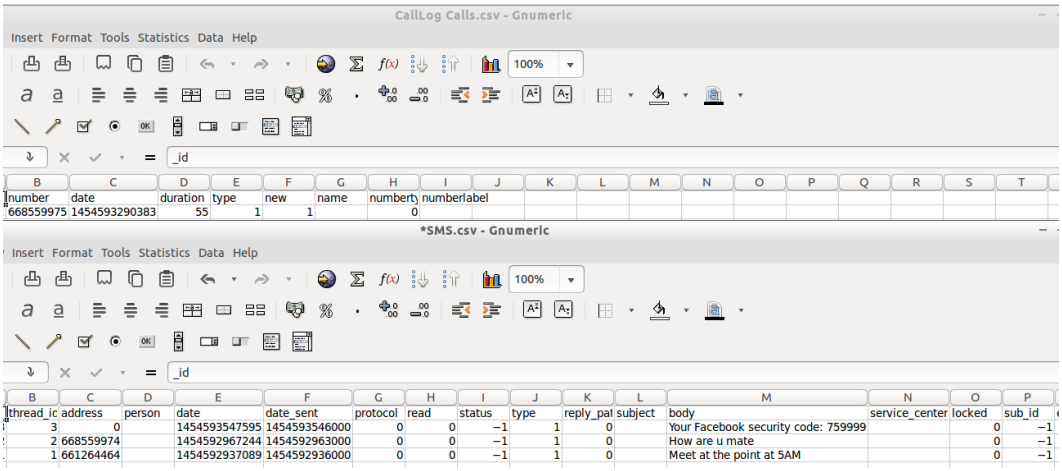
```
root@generic:/ # exit
soufiane@soufiane-VirtualBox:~$ adb pull /data/data/com.android.providers.telephony /home/soufiane/Desktop/Telephony
pull: building file list...
pull: /data/data/com.android.providers.telephony/databases/mmssms.db-journal -> /home/soufiane/Desktop/Telephony/databases/mmssms.d
b-journal
pull: /data/data/com.android.providers.telephony/databases/mmssms.db -> /home/soufiane/Desktop/Telephony/databases/mmssms.db
pull: /data/data/com.android.providers.telephony/databases/telephony.db-journal -> /home/soufiane/Desktop/Telephony/databases/telep
hony.db-journal
pull: /data/data/com.android.providers.telephony/databases/telephony.db -> /home/soufiane/Desktop/Telephony/databases/telephony.db
pull: /data/data/com.android.providers.telephony/databases/HbpcdLookup.db-journal -> /home/soufiane/Desktop/Telephony/databases/Hbp
cdLookup.db-journal
pull: /data/data/com.android.providers.telephony/databases/HbpcdLookup.db -> /home/soufiane/Desktop/Telephony/databases/HbpcdLookup
.db
pull: /data/data/com.android.providers.telephony/shared_prefs/preferred-apn1.xml -> /home/soufiane/Desktop/Telephony/shared_prefs/p
referred-apn1.xml
pull: /data/data/com.android.providers.telephony/lib -> /home/soufiane/Desktop/Telephony/lib
failed to copy '/data/data/com.android.providers.telephony/lib' to '/home/soufiane/Desktop/Telephony/lib': No such file or director
y
8 files pulled. 0 files skipped.
262 KB/s (222899 bytes in 0.829s)
soufiane@soufiane-VirtualBox:~$
```

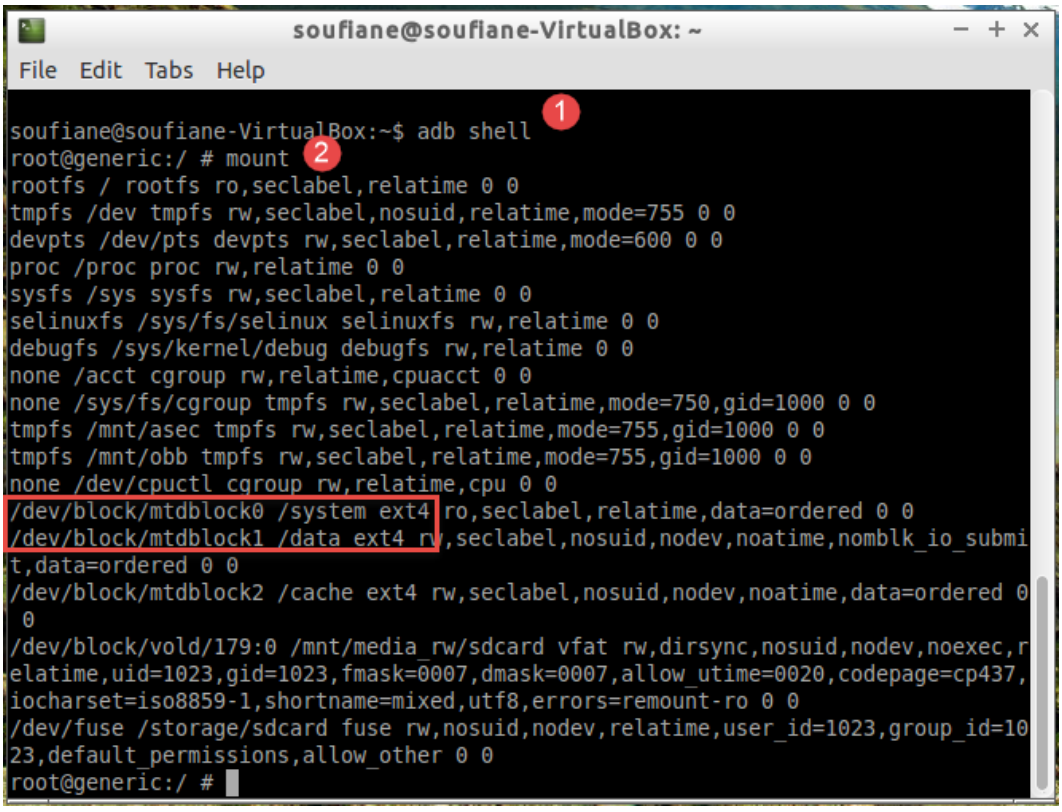
```
C:\Users\Soufiane\AppData\Local\Android\sdk\platform-tools>adb backup -f e:\case1\backup.ab -shared -all
Now unlock your device and confirm the backup operation.
```

```
E:\case1\android-backup-extractor-20151102-bin>abe.jar unpack backup.ab backup.tar
```




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

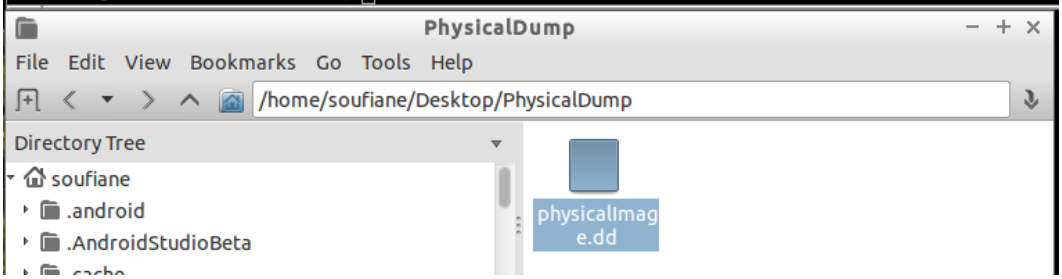

CallLog Calls.csv - Gnumeric
Insert Format Tools Statistics Data Help
100%
_id
number date duration type new name numberty numberlabel
668559975 1454593290383 55 1 1 0
*SMS.csv - Gnumeric
Insert Format Tools Statistics Data Help
100%
_id
thread_ic address person date date_sent protocol read status type reply_pat subject body service_center locked sub_id
3 0 1454593547595 1454593546000 0 0 −1 1 0 Your Facebook security code: 759999 0 −1
2 668559974 1454592967244 1454592963000 0 0 −1 1 0 How are u mate 0 −1
1 661264464 1454592937089 1454592936000 0 0 −1 1 0 Meet at the point at 5AM 0 −1


soufiane@soufiane-VirtualBox: ~
File Edit Tabs Help
1
soufiane@soufiane-VirtualBox:~$ adb shell
2
root@generic:/ # mount
rootfs / rootfs ro,seclabel,relatime 0 0
tmpfs /dev tmpfs rw,seclabel,nosuid,relatime,mode=755 0 0
devpts /dev/pts devpts rw,seclabel,relatime,mode=600 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,seclabel,relatime 0 0
selinuxfs /sys/fs/selinux selinuxfs rw,relatime 0 0
debugfs /sys/kernel/debug debugfs rw,relatime 0 0
none /acct cgroup rw,relatime,cpuacct 0 0
none /sys/fs/cgroup tmpfs rw,seclabel,relatime,mode=750,gid=1000 0 0
tmpfs /mnt/asec tmpfs rw,seclabel,relatime,mode=755,gid=1000 0 0
tmpfs /mnt/obb tmpfs rw,seclabel,relatime,mode=755,gid=1000 0 0
none /dev/cpuctl cgroup rw,relatime,cpu 0 0
/dev/block/mtdblock0 /system ext4 ro,seclabel,relatime,data=ordered 0 0
/dev/block/mtdblock1 /data ext4 rw,seclabel,nosuid,nodev,noatime,nomblk_io_submi
t,data=ordered 0 0
/dev/block/mtdblock2 /cache ext4 rw,seclabel,nosuid,nodev,noatime,data=ordered 0
0
/dev/block/vold/179:0 /mnt/media_rw/sdcard vfat rw,dirsync,nosuid,nodev,noexec,r
elatime,uid=1023,gid=1023,fmask=0007,dmask=0007,allow_utime=0020,codepage=cp437,
iocharset=iso8859-1,shortname=mixed,utf8,errors=remount-ro 0 0
/dev/fuse /storage/sdcard fuse rw,nosuid,nodev,relatime,user_id=1023,group_id=10
23,default_permissions,allow_other 0 0
root@generic:/ #

```
drwxr-x--- root     root              1970-01-01 00:00 sbin
lrwxrwxrwx root     root              2016-02-05 11:20 sdcard -> /storage/sdcard
-rw-r--r-- root     root          471 1970-01-01 00:00 seapp_contexts
```

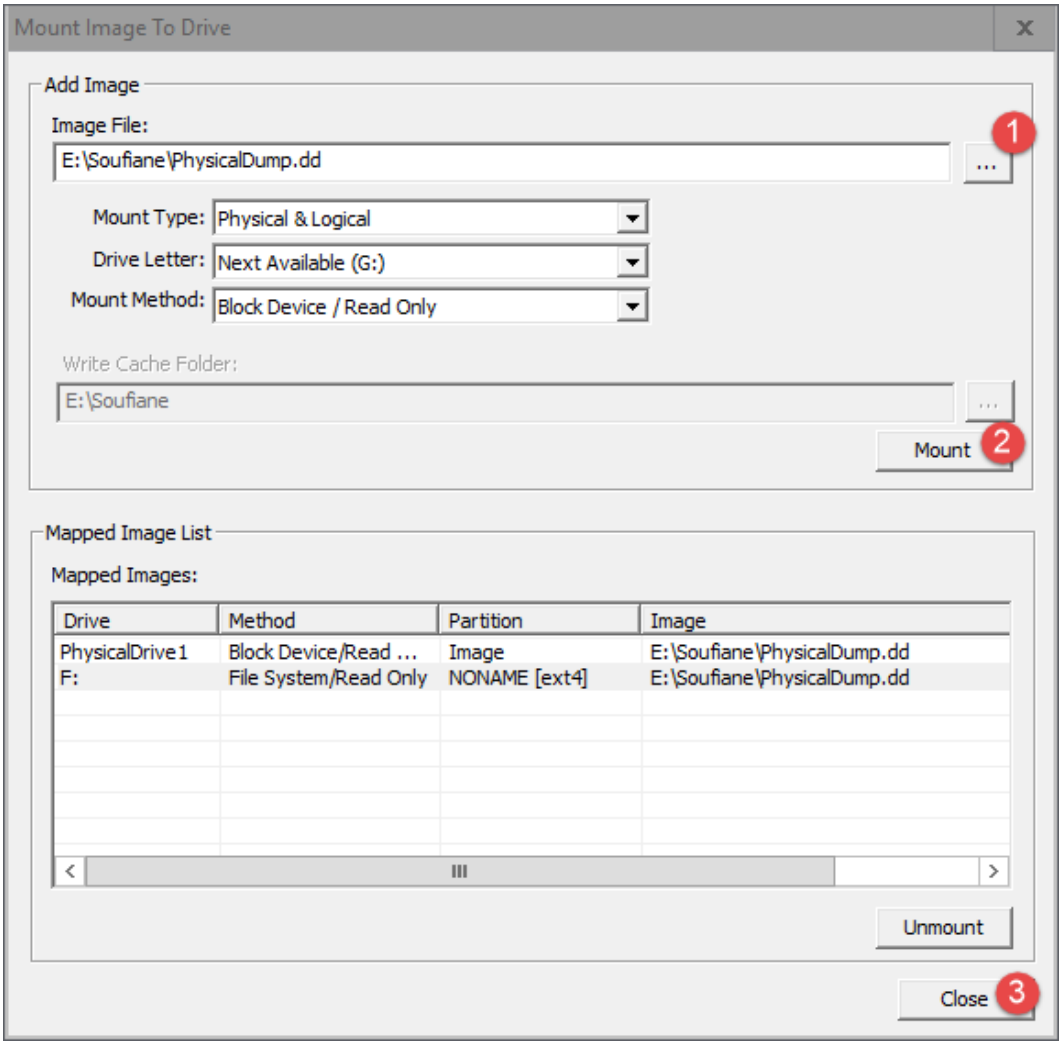
```
v/block/mtdblock1 of=/storage/sdcard/physicalImage.dd
^C879855+0 records in
879854+0 records out
450485248 bytes transferred in 681.856 secs (660675 bytes/sec)
```

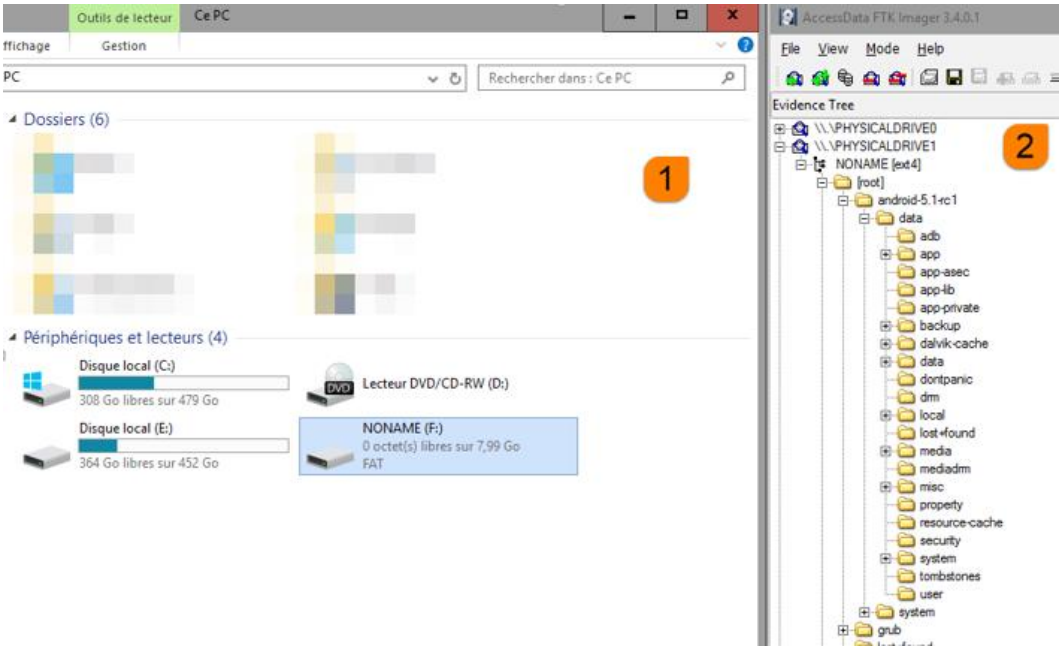
```
soufiane@soufiane-VirtualBox:~$ adb pull /storage/sdcard/ /home/soufiane/Desktop/PhysicalDump/
pull: building file list...
pull: /storage/sdcard/physicalImage.dd -> /home/soufiane/Desktop/PhysicalDump/physicalImage.dd
1 file pulled. 0 files skipped.
1055 KB/s (450485760 bytes in 416.683s)
soufiane@soufiane-VirtualBox:~$
```

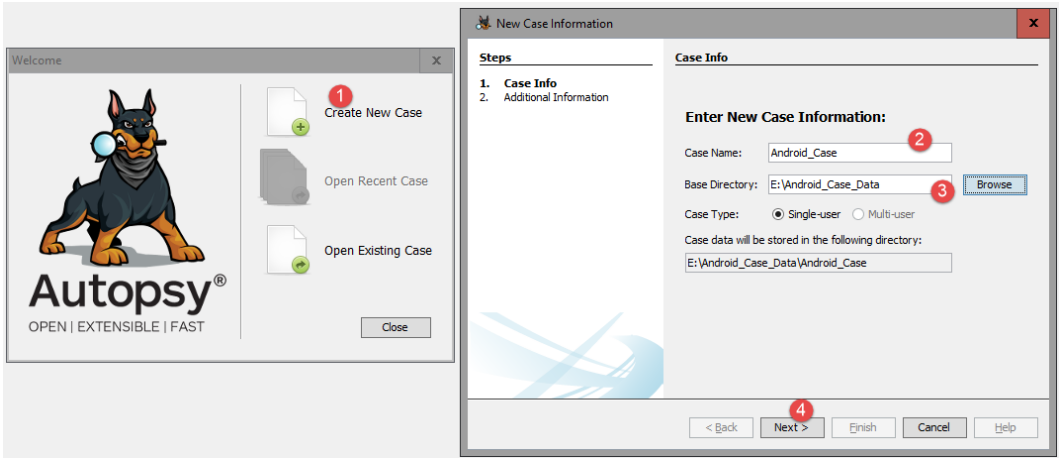


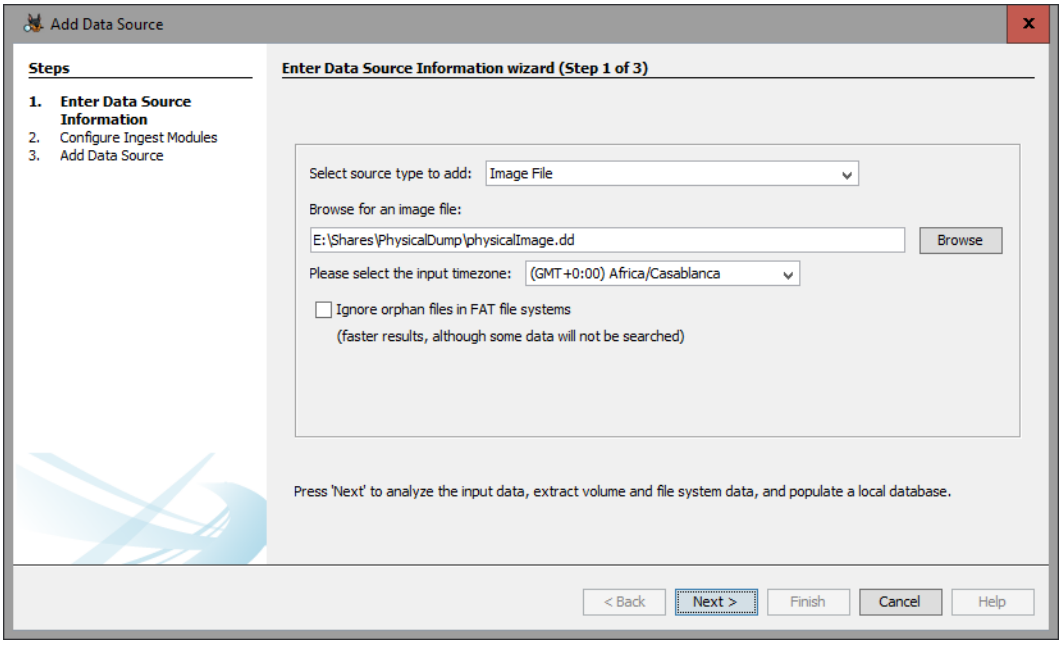
```
root@generic:/ # exit
soufiane@soufiane-VirtualBox:~$ adb forward tcp:1986 tcp:1986
soufiane@soufiane-VirtualBox:~$
```

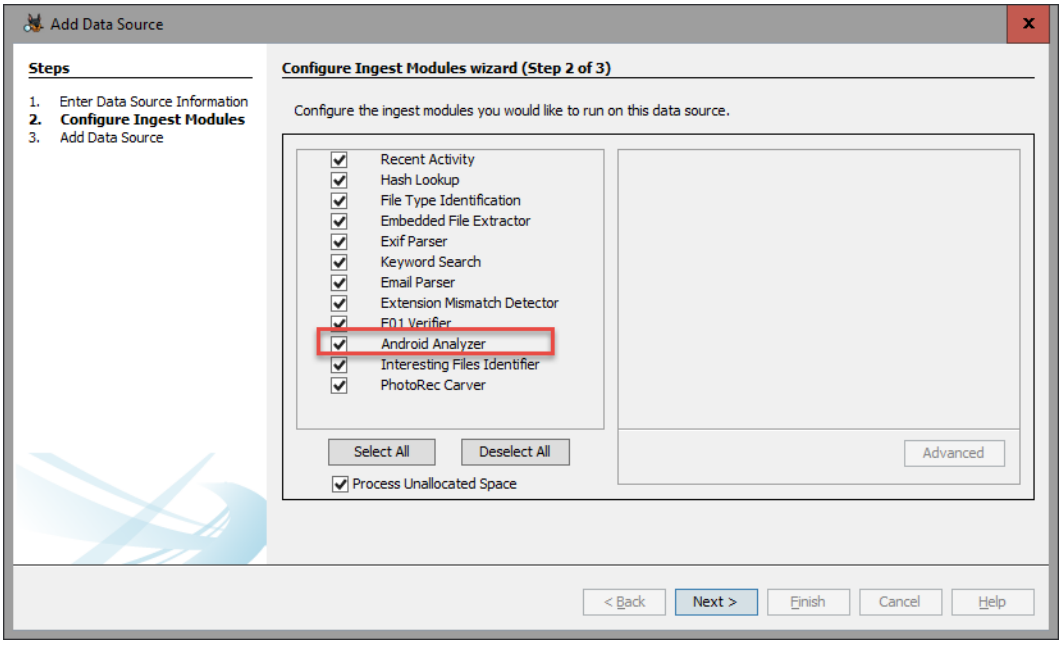
```
16771797+0 records in
16771797+0 records out
8587160064 bytes transferred in 1222.404 secs (7024813 bytes/sec)
```

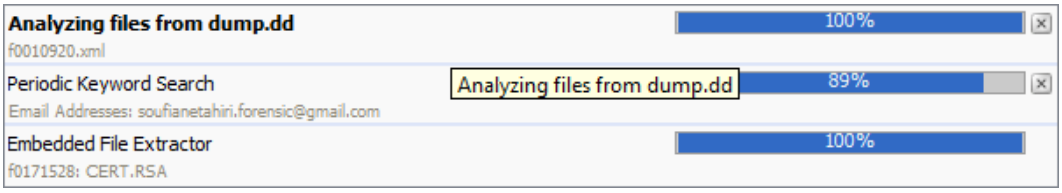

Mount Image To Drive
Add Image
Image File:
E:\Soufiane\PhysicalDump.dd
...
1
Mount Type:
Physical & Logical
Drive Letter:
Next Available (G:)
Mount Method:
Block Device / Read Only
Write Cache Folder:
E:\Soufiane
...
Mount
2
Mapped Image List
Mapped Images:
Drive
Method
Partition
Image
PhysicalDrive1
Block Device/Read ...
Image
E:\Soufiane\PhysicalDump.dd
F:
File System/Read Only
NONAME [ext4]
E:\Soufiane\PhysicalDump.dd
Unmount
Close
3

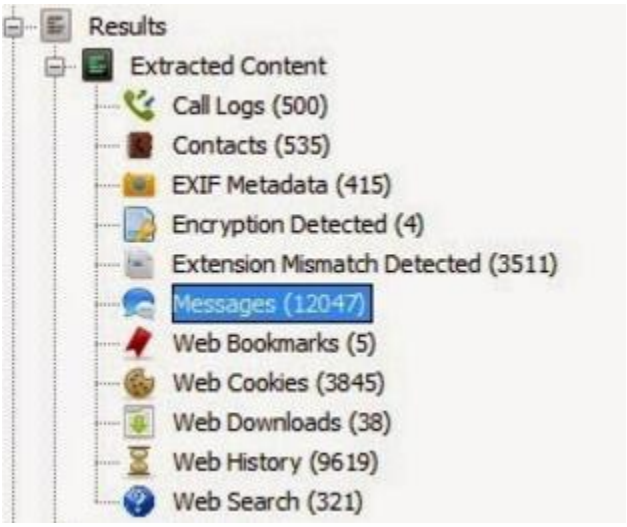

Outils de lecteur
Ce PC
Affichage
Gestion
Rechercher dans : Ce PC
Dossiers (6)
1
Périphériques et lecteurs (4)
Disque local (C:)
308 Go libres sur 479 Go
Lecteur DVD/CD-RW (D:)
Disque local (E:)
364 Go libres sur 452 Go
NONAME (F:)
0 octet(s) libres sur 7,99 Go
FAT
AccessData FTK Imager 3.4.0.1
File View Mode Help
Evidence Tree
2
\\.\PHYSICALDRIVE0
\\.\PHYSICALDRIVE1
NONAME [ext4]
[root]
android-5.1-rc1
data
adb
app
app-asec
app-lib
app-private
backup
dalvik-cache
data
dontpanic
drm
local
lost+found
media
mediadrm
misc
property
resource-cache
security
system
tombstones
user
system
grub


Welcome
Autopsy®
OPEN | EXTENSIBLE | FAST
1
Create New Case
Open Recent Case
Open Existing Case
Close
New Case Information
Steps
1. Case Info
2. Additional Information
Case Info
Enter New Case Information:
2
Case Name: Android_Case
Base Directory: E:\Android_Case_Data
3
Browse
Case Type: Single-user Multi-user
Case data will be stored in the following directory:
E:\Android_Case_Data\Android_Case
4
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source
Enter Data Source Information wizard (Step 1 of 3)
Select source type to add: Image File
Browse for an image file:
E:\Shares\PhysicalDump\physicalImage.dd
Browse
Please select the input timezone: (GMT+0:00) Africa/Casablanca
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
< Back
Next >
Finish
Cancel
Help





Contacts

Table | Thumbnail

Source File	Data Source	Name	Phone Number	Email
contacts2.db	dump.dd			
contacts2.db	dump.dd	Nawal	(	
contacts2.db	dump.dd	Sofuiane Tahiri	(066) 855-9975	soufianetahiri@gmail.com

Messages

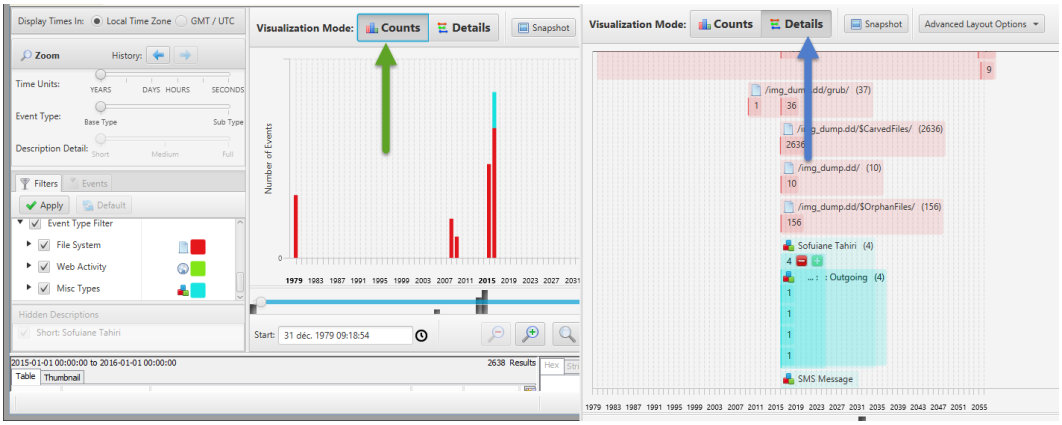
Table | Thumbnail

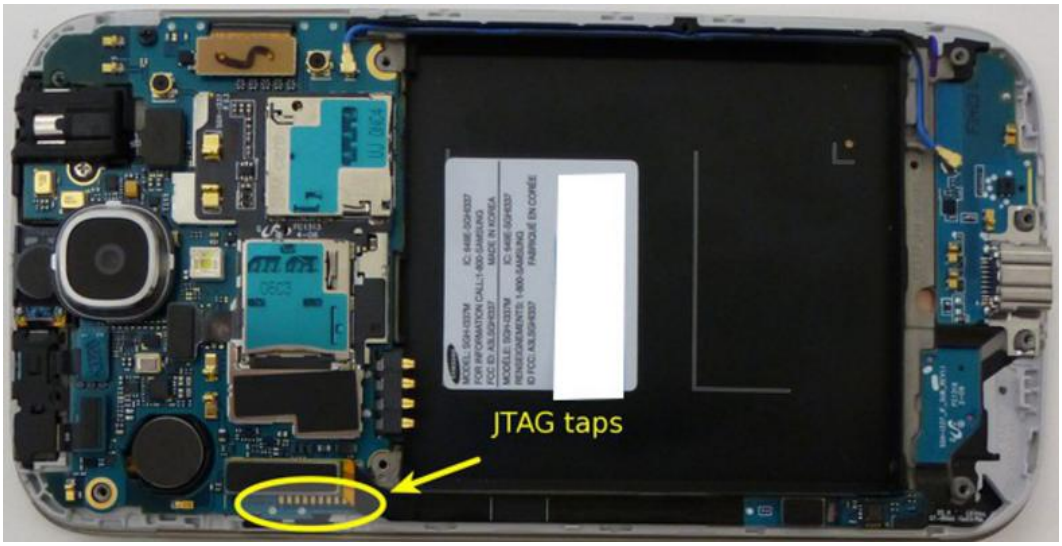
Source File	Direction	To Phone Number	Date/Time	Read	Subject	Text	Message Type
mmssms.db	Outgoing	0668559975	2016-02-04 12:47:10 WET	Unread		This is a test message	SMS Message

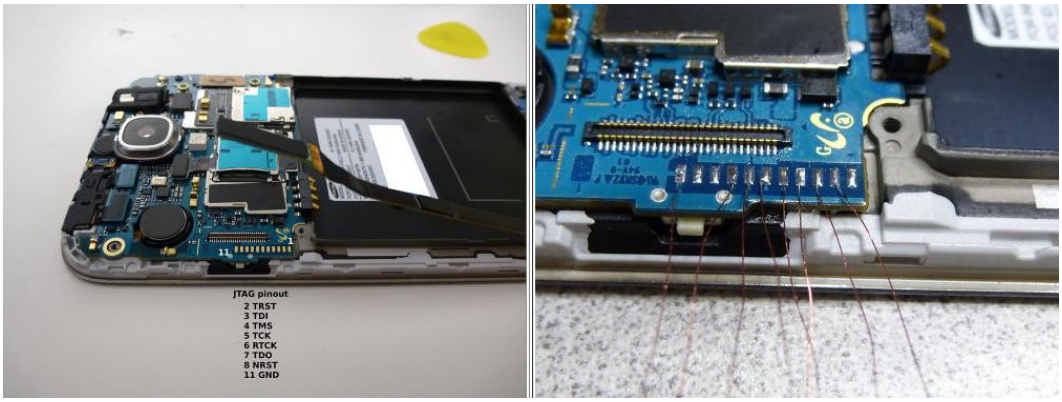
Call Logs

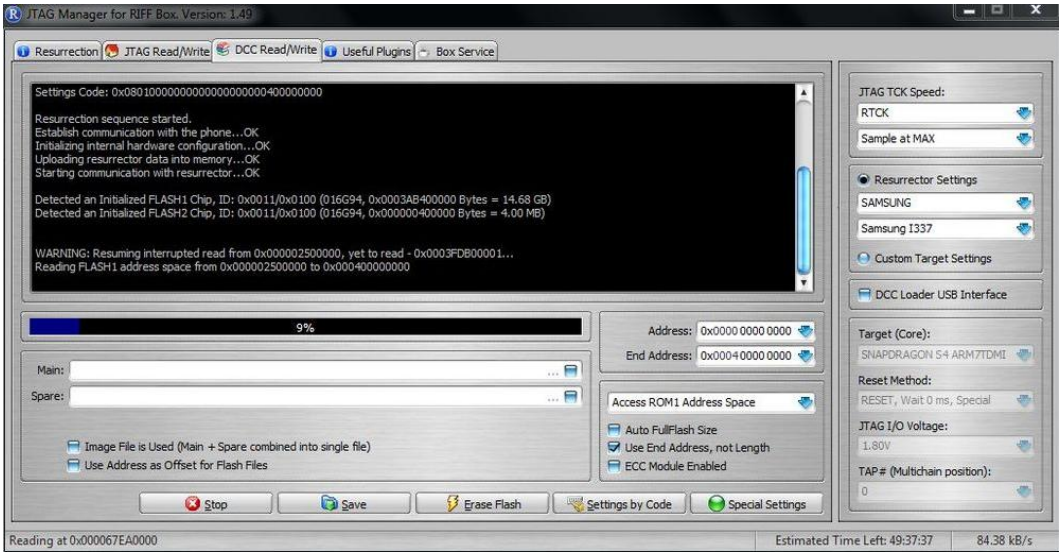
Table | Thumbnail

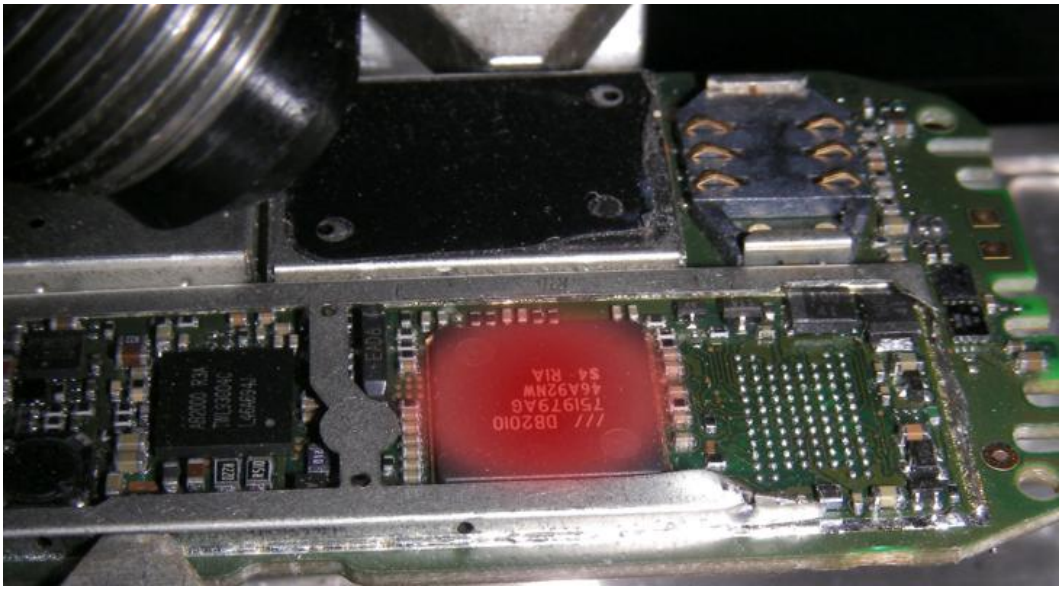
Source File	To Phone Number	Start Date/Time	End Date/Time	Direction	Name	Data Source
contacts2.db	0668559975	2016-02-01 20:45:49 WET	2016-02-01 20:45:49 WET	Outgoing	Sofuiane Tahiri	dump.dd
contacts2.db	0668559975	2016-02-01 20:45:42 WET	2016-02-01 20:45:42 WET	Outgoing	Sofuiane Tahiri	dump.dd
contacts2.db	0668559975	2016-02-01 20:45:35 WET	2016-02-01 20:45:35 WET	Outgoing	Sofuiane Tahiri	dump.dd


Visualization Mode:
Counts
Details
Snapshot
Advanced Layout Options
Number of Events
Outgoing (4)
SMS Message

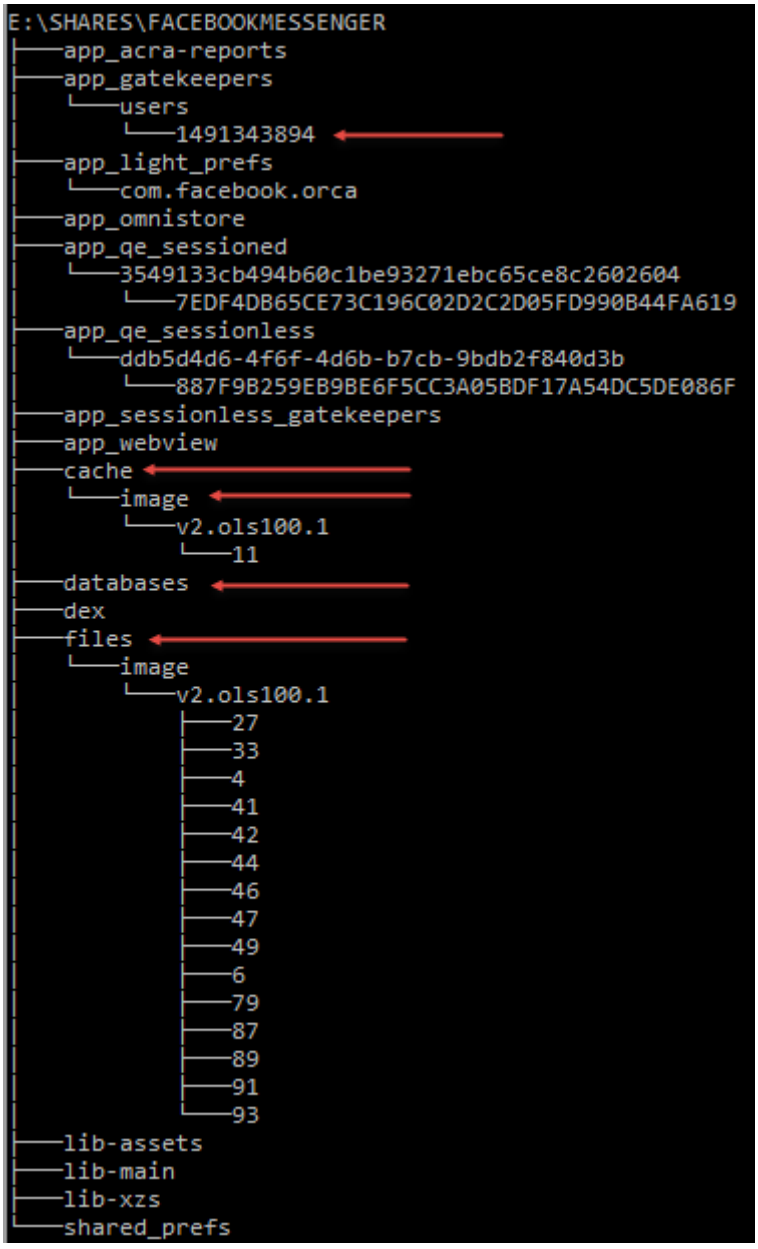

JTAG taps


JTAG pinout
2 TRST
3 TDI
4 TMS
5 TCK
6 RTCK
7 TDO
8 NRST
11 GND


JTAG Manager for RIFF Box. Version: 1.49
Resurrection
JTAG Read/Write
DCC Read/Write
Useful Plugins
Box Service
Settings Code: 0x0801000000000000000000400000000
Resurrection sequence started.
Establish communication with the phone...OK
Initializing internal hardware configuration...OK
Uploading resurrector data into memory...OK
Starting communication with resurrector...OK
Detected an Initialized FLASH1 Chip, ID: 0x0011/0x0100 (016G94, 0x0003AB400000 Bytes = 14.68 GB)
Detected an Initialized FLASH2 Chip, ID: 0x0011/0x0100 (016G94, 0x000000400000 Bytes = 4.00 MB)
WARNING: Resuming interrupted read from 0x000002500000, yet to read - 0x0003FDB00001...
Reading FLASH1 address space from 0x000002500000 to 0x000400000000
9%
Address: 0x0000 0000 0000
End Address: 0x0004 0000 0000
Main:
Spare:
Access ROM1 Address Space
Image File is Used (Main + Spare combined into single file)
Use Address as Offset for Flash Files
Auto FullFlash Size
Use End Address, not Length
ECC Module Enabled
Stop
Save
Erase Flash
Settings by Code
Special Settings
JTAG TCK Speed:
RTCK
Sample at MAX
Resurrector Settings
SAMSUNG
Samsung I337
Custom Target Settings
DCC Loader USB Interface
Target (Core):
SNAPDRAGON S4 ARM7TDMI
Reset Method:
RESET, Wait 0 ms, Special
JTAG I/O Voltage:
1.80V
TAP # (Multichain position):
0
Reading at 0x000067EA0000
Estimated Time Left: 49:37:37
84.38 kB/s

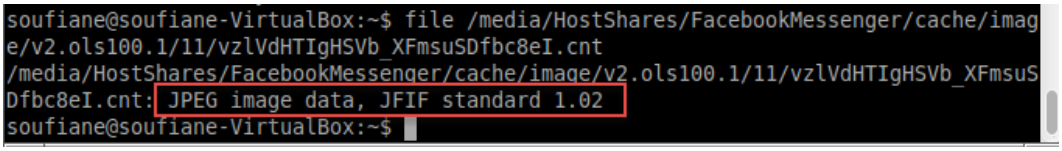


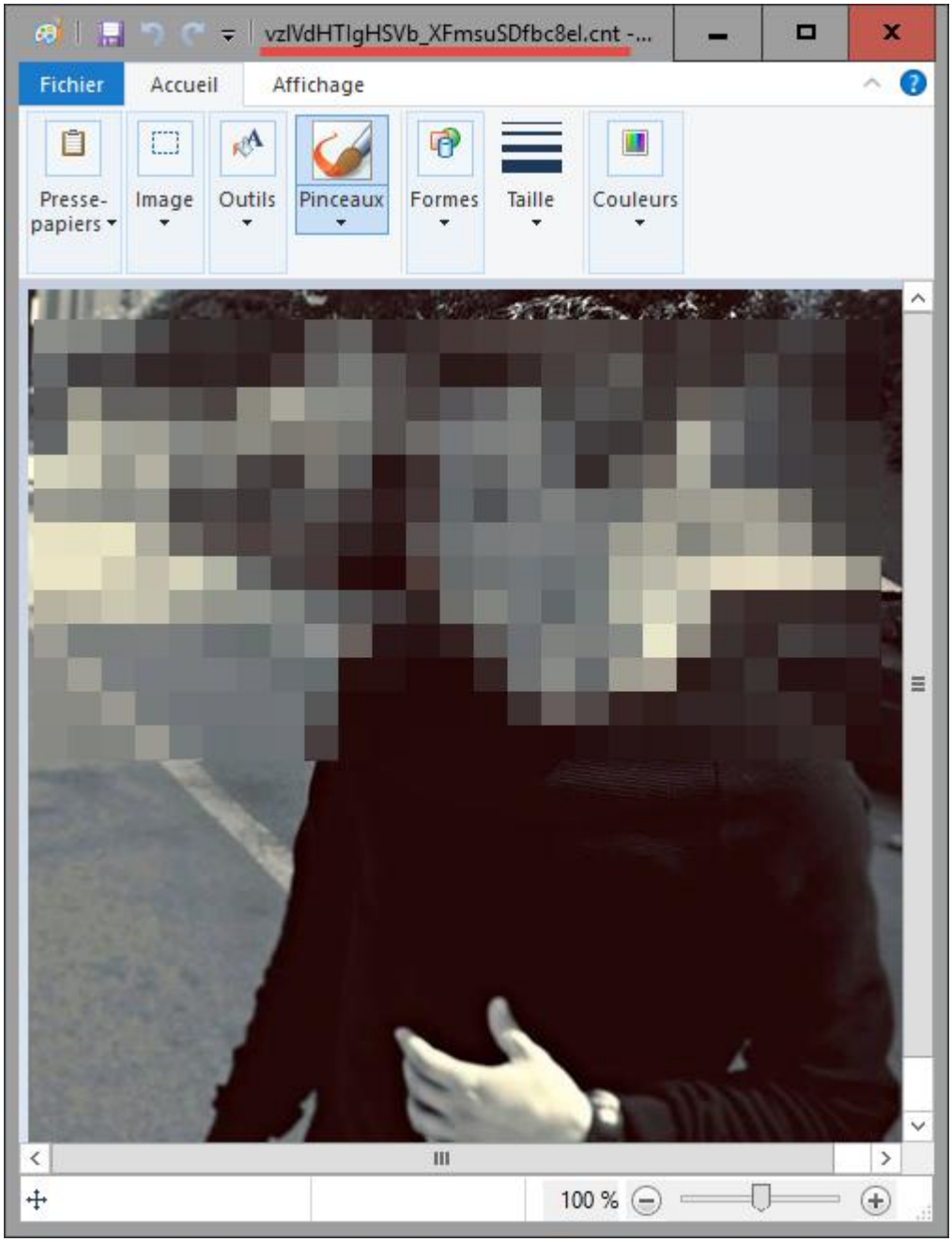
```
soufiane@soufiane-VirtualBox:~$ adb pull /data/data/com.facebook.orca /media/HostSh
ares/
pull: building file list...
pull: /data/data/com.facebook.orca/cache/image/v2.ols100.1/11/-JslGRfeva7VX79cG-QM4
7q3bk8.cnt -> /media/HostShares/cache/image/v2.ols100.1/11/-JslGRfeva7VX79cG-QM47q3
bk8.cnt
pull: /data/data/com.facebook.orca/cache/image/v2.ols100.1/11/vzlVdHTIgHSVb_XFmsuSD
fbc8eI.cnt -> /media/HostShares/cache/image/v2.ols100.1/11/vzlVdHTIgHSVb_XFmsuSDfbc
8eI.cnt
pull: /data/data/com.facebook.orca/cache/fb_voicemail_asset_725078935 -> /media/Hos
tShares/cache/fb_voicemail_asset_725078935
pull: /data/data/com.facebook.orca/files/image/v2.ols100.1/33/lFiMFn3SLjurnUb_3iNFi
__yRUY.cnt -> /media/HostShares/files/image/v2.ols100.1/33/lFiMFn3SLjurnUb_3iNFi__y
pull: /data/data/com.facebook.orca/lib -> /media/HostShares/FacebookMessenger/lib
failed to copy '/data/data/com.facebook.orca/lib' to '/media/HostShares/FacebookMes
senger/lib': Is a directory
153 files pulled. 0 files skipped.
866 KB/s (37802839 bytes in 42.586s)
```

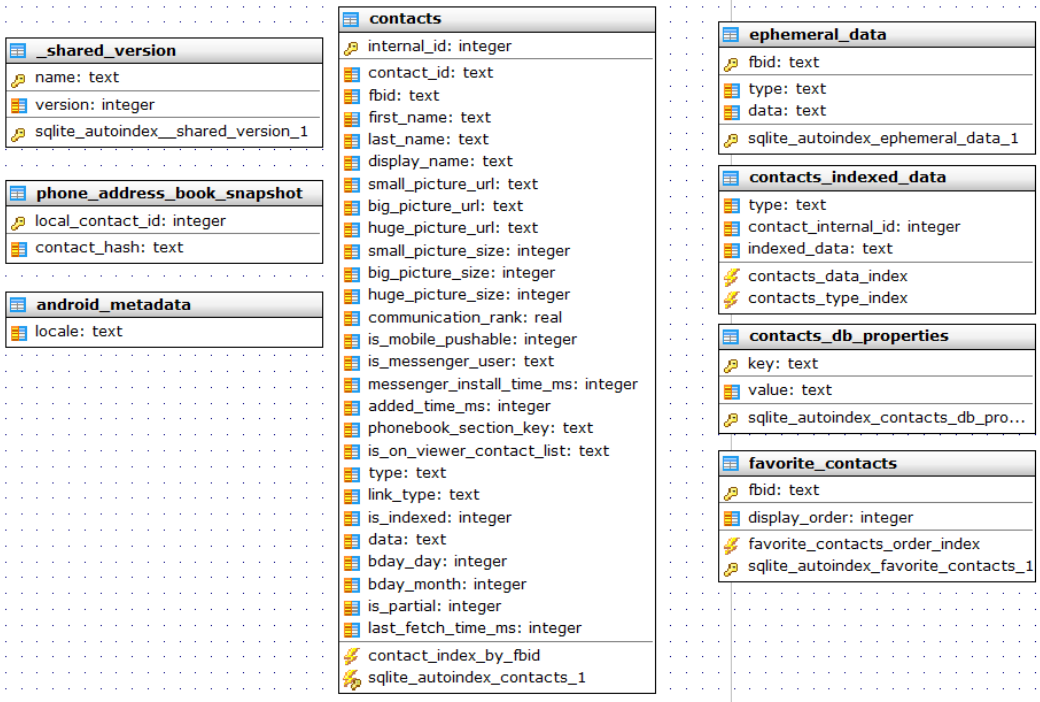


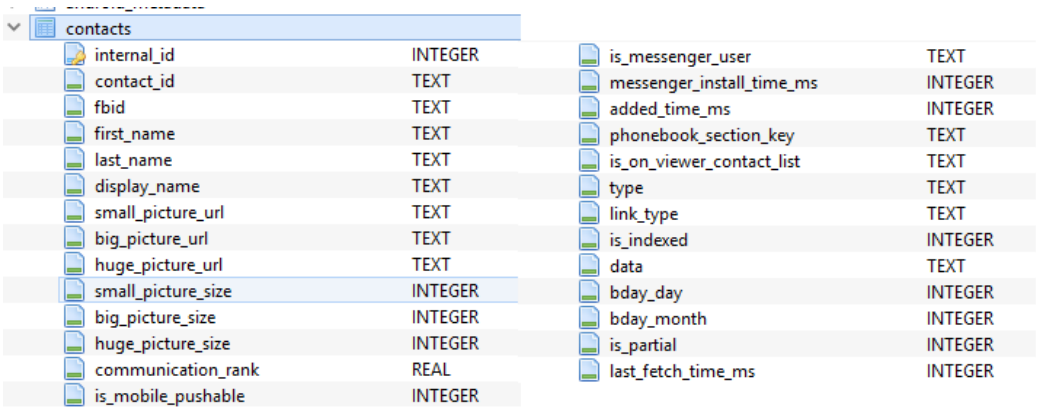
-JslGRfeva7VX79cG-QM47q3bk8.cnt

vzlVdHTlgHSVb_XFmsuSDfbc8el.cnt


soufiane@soufiane-VirtualBox:~$ file /media/HostShares/FacebookMessenger/cache/imag
e/v2.ols100.1/11/vzlVdHTIgHSVb_XFmsuSDfbc8eI.cnt
/media/HostShares/FacebookMessenger/cache/image/v2.ols100.1/11/vzlVdHTIgHSVb_XFmsuS
Dfbc8eI.cnt: JPEG image data, JFIF standard 1.02
soufiane@soufiane-VirtualBox:~$

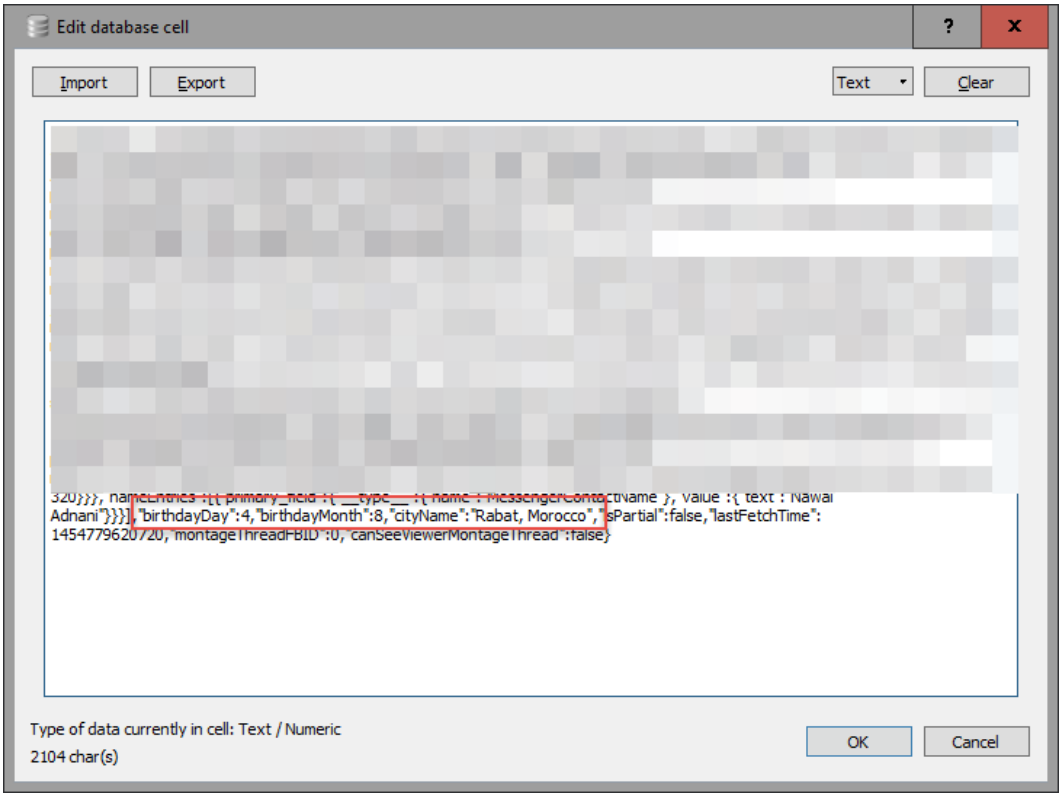

vzlVdHTlgHSVb_XFmsuSDfbc8el.cnt -...
Fichier
Accueil
Affichage
Presse-papiers
Image
Outils
Pinceaux
Formes
Taille
Couleurs
100 %


_shared_version
name: text
version: integer
sqlite_autoindex__shared_version_1
phone_address_book_snapshot
local_contact_id: integer
contact_hash: text
android_metadata
locale: text
contacts
internal_id: integer
contact_id: text
fbid: text
first_name: text
last_name: text
display_name: text
small_picture_url: text
big_picture_url: text
huge_picture_url: text
small_picture_size: integer
big_picture_size: integer
huge_picture_size: integer
communication_rank: real
is_mobile_pushable: integer
is_messenger_user: text
messenger_install_time_ms: integer
added_time_ms: integer
phonebook_section_key: text
is_on_viewer_contact_list: text
type: text
link_type: text
is_indexed: integer
data: text
bday_day: integer
bday_month: integer
is_partial: integer
last_fetch_time_ms: integer
contact_index_by_fbid
sqlite_autoindex_contacts_1
ephemeral_data
fbid: text
type: text
data: text
sqlite_autoindex_ephemeral_data_1
contacts_indexed_data
type: text
contact_internal_id: integer
indexed_data: text
contacts_data_index
contacts_type_index
contacts_db_properties
key: text
value: text
sqlite_autoindex_contacts_db_pro...
favorite_contacts
fbid: text
display_order: integer
favorite_contacts_order_index
sqlite_autoindex_favorite_contacts_1

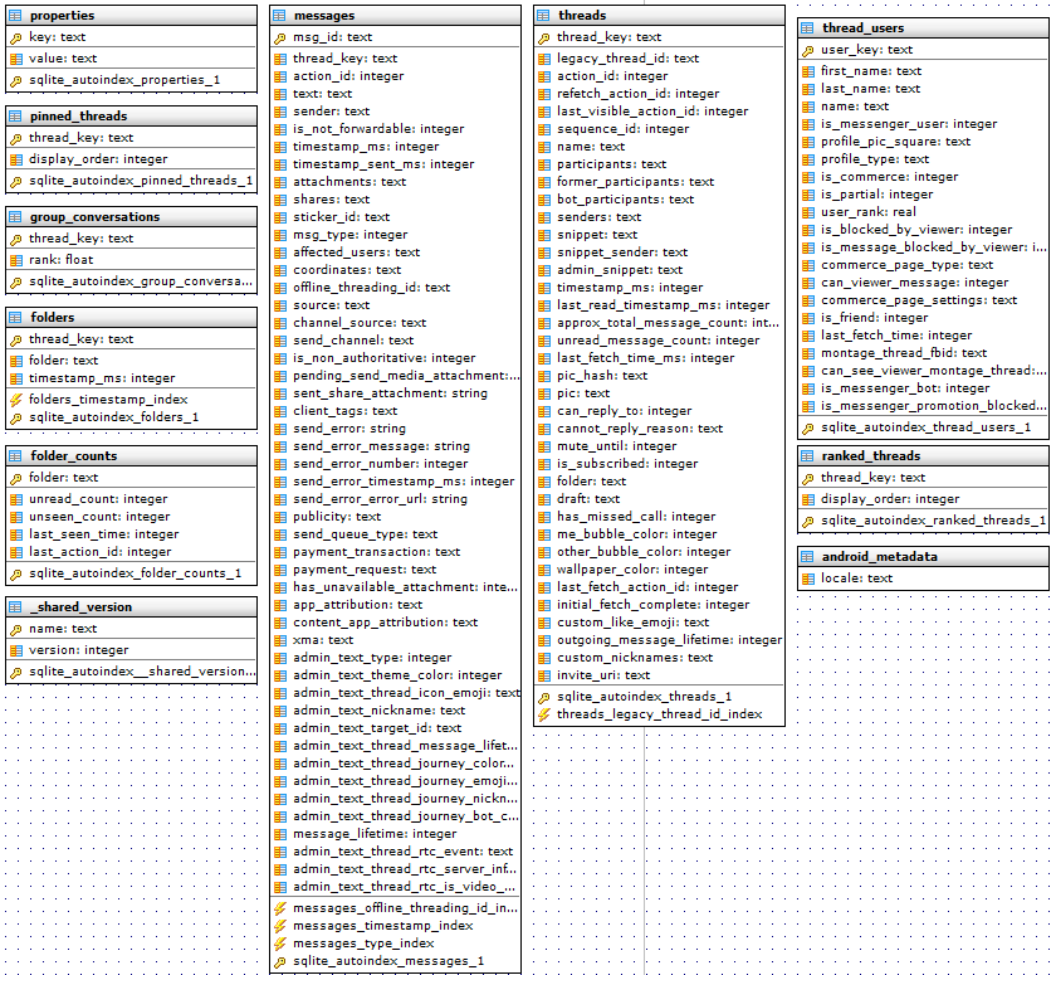

contacts
internal_id INTEGER
contact_id TEXT
fbid TEXT
first_name TEXT
last_name TEXT
display_name TEXT
small_picture_url TEXT
big_picture_url TEXT
huge_picture_url TEXT
small_picture_size INTEGER
big_picture_size INTEGER
huge_picture_size INTEGER
communication_rank REAL
is_mobile_pushable INTEGER
is_messenger_user TEXT
messenger_install_time_ms INTEGER
added_time_ms INTEGER
phonebook_section_key TEXT
is_on_viewer_contact_list TEXT
type TEXT
link_type TEXT
is_indexed INTEGER
data TEXT
bday_day INTEGER
bday_month INTEGER
is_partial INTEGER
last_fetch_time_ms INTEGER

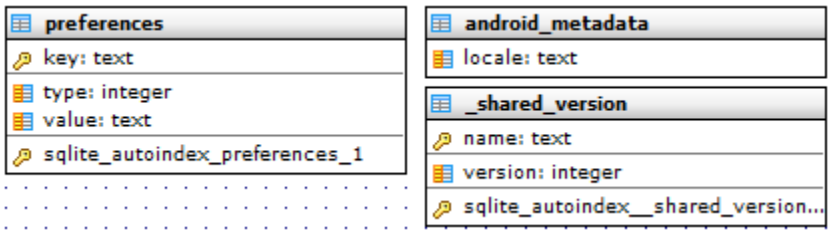
---

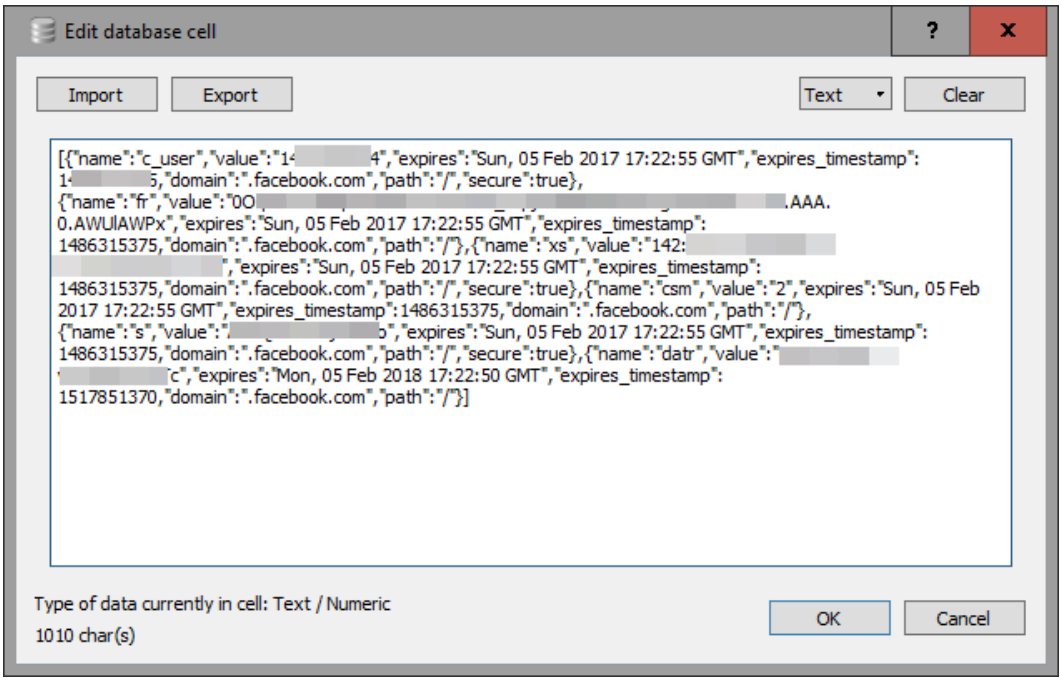
fbid	first_name	last_name	display_name	small_picture_ur	big_picture_url	huge_picture_ur
Filter	Filter	Filter	Filter	Filter	Filter	Filter
10	Abdelouahed	Aomari	Abdelouahed I	https://fbcdn-prl	https://fbcdn-prl	https://fbcdn-prl
66	Nawal	Adnani	Nawal Adnani	https://fbcdn-prl	https://fbcdn-prl	https://fbcdn-prl
10				https://fbcdn-prl	https://fbcdn-prl	https://fbcdn-prl
10				https://fbcdn-prl	https://fbcdn-prl	https://fbcdn-prl
59				https://fbcdn-prl	https://fbcdn-prl	https://fbcdn-prl
54				https://fbcdn-prl	https://fbcdn-prl	https://fbcdn-prl
10				https://fbcdn-prl	https://fbcdn-prl	https://fbcdn-prl
55				https://fbcdn-prl	https://fbcdn-prl	https://fbcdn-prl
13				https://fbcdn-prl	https://fbcdn-prl	https://fbcdn-prl
78				https://fbcdn-prl	https://fbcdn-prl	https://fbcdn-prl



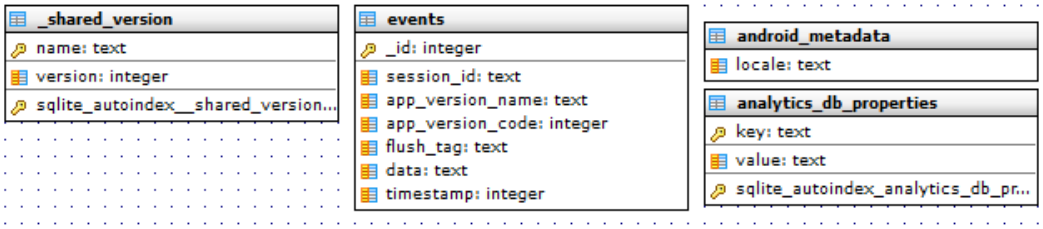

favorite_contacts
fbid TEXT
display_order INTEGER


properties
key: text
value: text
sqlite_autoindex_properties_1
pinned_threads
thread_key: text
display_order: integer
sqlite_autoindex_pinned_threads_1
group_conversations
thread_key: text
rank: float
sqlite_autoindex_group_conversa...
folders
thread_key: text
folder: text
timestamp_ms: integer
folders_timestamp_index
sqlite_autoindex_folders_1
folder_counts
folder: text
unread_count: integer
unseen_count: integer
last_seen_time: integer
last_action_id: integer
sqlite_autoindex_folder_counts_1
_shared_version
name: text
version: integer
sqlite_autoindex__shared_version...
messages
msg_id: text
thread_key: text
action_id: integer
text: text
sender: text
is_not_forwardable: integer
timestamp_ms: integer
timestamp_sent_ms: integer
attachments: text
shares: text
sticker_id: text
msg_type: integer
affected_users: text
coordinates: text
offline_threading_id: text
source: text
channel_source: text
send_channel: text
is_non_authoritative: integer
pending_send_media_attachment:...
sent_share_attachment: string
client_tags: text
send_error: string
send_error_message: string
send_error_number: integer
send_error_timestamp_ms: integer
send_error_error_url: string
publicity: text
send_queue_type: text
payment_transaction: text
payment_request: text
has_unavailable_attachment: inte...
app_attribution: text
content_app_attribution: text
xma: text
admin_text_type: integer
admin_text_theme_color: integer
admin_text_thread_icon_emoji: text
admin_text_nickname: text
admin_text_target_id: text
admin_text_thread_message_lifet...
admin_text_thread_journey_color...
admin_text_thread_journey_emoji...
admin_text_thread_journey_nickn...
admin_text_thread_journey_bot_c...
message_lifetime: integer
admin_text_thread_rtc_event: text
admin_text_thread_rtc_server_inf...
admin_text_thread_rtc_is_video_...
messages_offline_threading_id_in...
messages_timestamp_index
messages_type_index
sqlite_autoindex_messages_1
threads
thread_key: text
legacy_thread_id: text
action_id: integer
refetch_action_id: integer
last_visible_action_id: integer
sequence_id: integer
name: text
participants: text
former_participants: text
bot_participants: text
senders: text
snippet: text
snippet_sender: text
admin_snippet: text
timestamp_ms: integer
last_read_timestamp_ms: integer
approx_total_message_count: int...
unread_message_count: integer
last_fetch_time_ms: integer
pic_hash: text
pic: text
can_reply_to: integer
cannot_reply_reason: text
mute_until: integer
is_subscribed: integer
folder: text
draft: text
has_missed_call: integer
me_bubble_color: integer
other_bubble_color: integer
wallpaper_color: integer
last_fetch_action_id: integer
initial_fetch_complete: integer
custom_like_emoji: text
outgoing_message_lifetime: integer
custom_nicknames: text
invite_uri: text
sqlite_autoindex_threads_1
threads_legacy_thread_id_index
thread_users
user_key: text
first_name: text
last_name: text
name: text
is_messenger_user: integer
profile_pic_square: text
profile_type: text
is_commerce: integer
is_partial: integer
user_rank: real
is_blocked_by_viewer: integer
is_message_blocked_by_viewer: i...
commerce_page_type: text
can_viewer_message: integer
commerce_page_settings: text
is_friend: integer
last_fetch_time: integer
montage_thread_fbid: text
can_see_viewer_montage_thread:...
is_messenger_bot: integer
is_messenger_promotion_blocked...
sqlite_autoindex_thread_users_1
ranked_threads
thread_key: text
display_order: integer
sqlite_autoindex_ranked_threads_1
android_metadata
locale: text





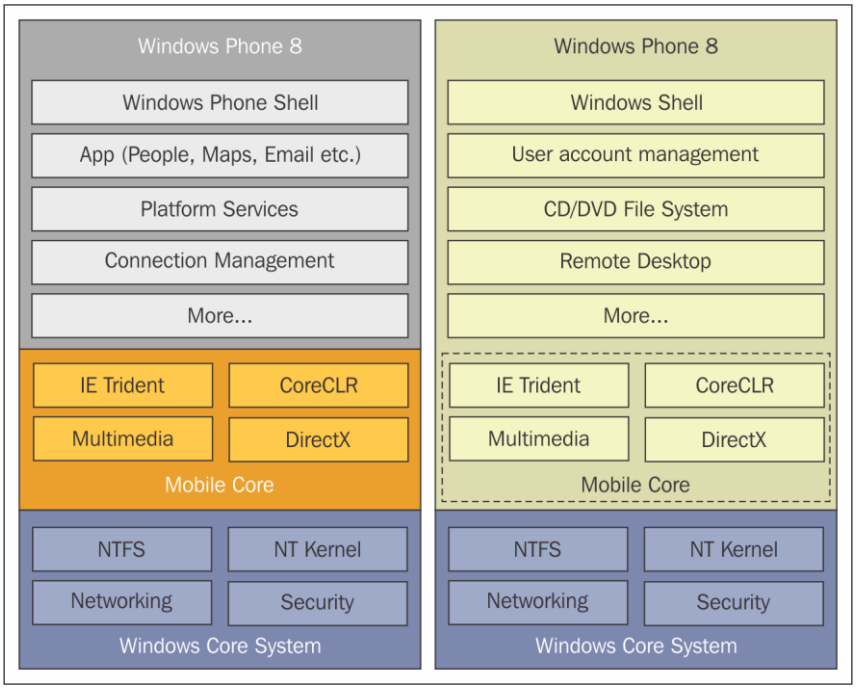
{"uid":"1491343894","first_name":"Soufiane","last_name":"Tahiri","name":"Soufiane Tahiri","birth_date_year":
"birth_date_month"
"birth_date_day
,"gender"
,"emails":
[
],"phones":[{"full_number":"+212668559975","display_number":"0668-559975","is_verified":true,"android_type":0}],"pic_square":"https://fbcdn-profile-a.akamaihd.net/hprofile-ak-xta1/v/t1.0-1/
p160x160/11949452_10204987185587960_1479973895921531 34_n.jpg?_nc_ad=z-
m&oh=3a53d9240cc77f8fa4b217ea612ba532&oe=57383FF9&__gda__=1463144513_2ff976d3240a2326edbb0976c51f9e61","profile_pic_square":[{"url":"https://fbcdn-profile-a.akamaihd.net/hprofile-ak-xta1/v/t1.0-1/
p160x160/11949452_10204987185587960_1479973895921531 34_n.jpg?_nc_ad=z-m&oh=3a53d9240cc77f8fa4b217ea612ba5328oe=57383FF9&__gda__=1463144513_2ff976d3240a2326edbb0976c51f9e61","size":160},
{"url":"https://fbcdn-profile-a.akamaihd.net/hprofile-ak-xta1/v/t1.0-1/p320x320/11949452_10204987185587960_1479973895921531 34_n.jpg?_nc_ad=z-
m&oh=068c1476f65a76b54f62bdeebf5f900e&oe=572767EE&__gda__=1462958422_da32e8dac6307ba68df767015a5e0f6d","size":320},{"url":"https://fbcdn-profile-a.akamaihd.net/hprofile-ak-xta1/v/
t1.0-1/11949452_10204987185587960_1479973895921531 34_n.jpg?_nc_ad=z-m&oh=e88a029c38d04e4a2c8442f57940a56d&oe=576941488__gda__=1462227997_1451488017a18bd402a292d2ce171e4a","size":
960}],"is_pushable":true,"type":"user","auth_token":
","profile_picture_is_silhouette":false,"montage_thread_fbid":
0,"can_see_viewer_montage_thread":false,"is_deactivated_allowed_on_messenger":false}

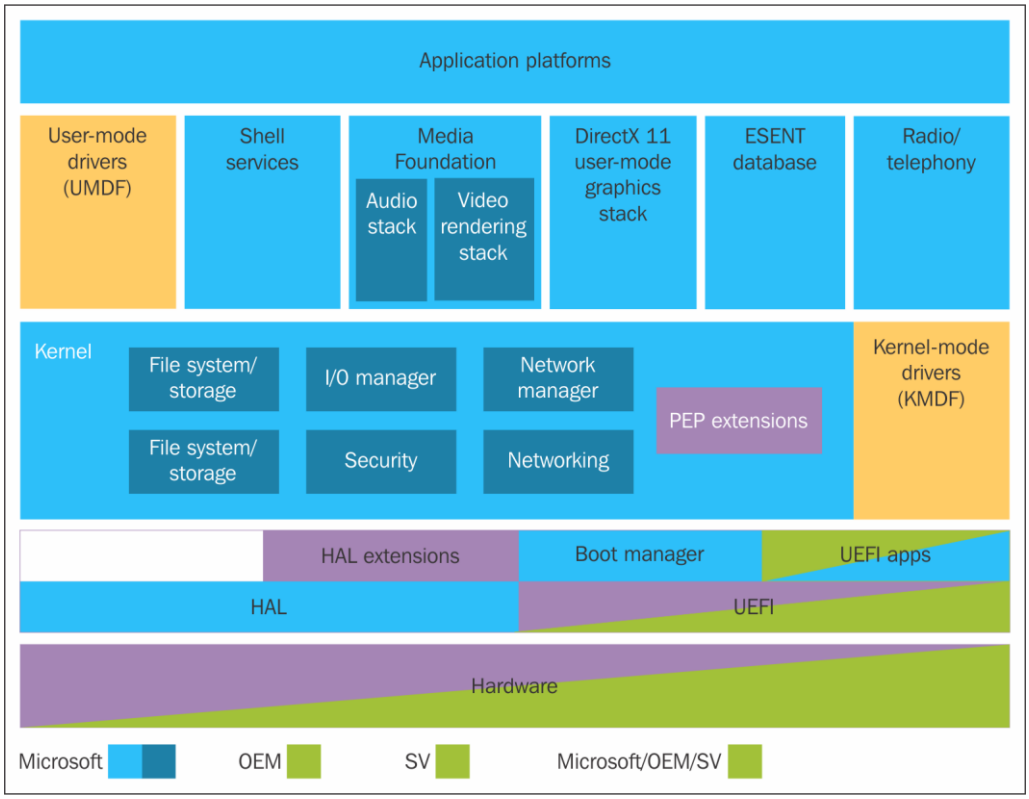


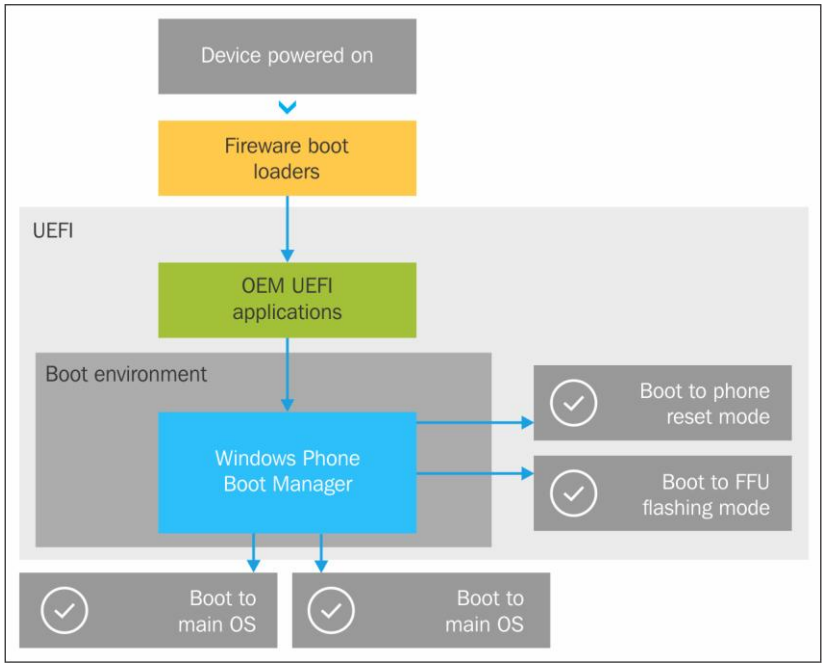
/active_session_id	[redacted]
/uploading_session_id	[redacted]
/regular_beacon_id	2
/session_user_id	1491343894
/last_send_time	1454780294851
/last_event_time	1454780293704
/uploading_batch_seq_id	1

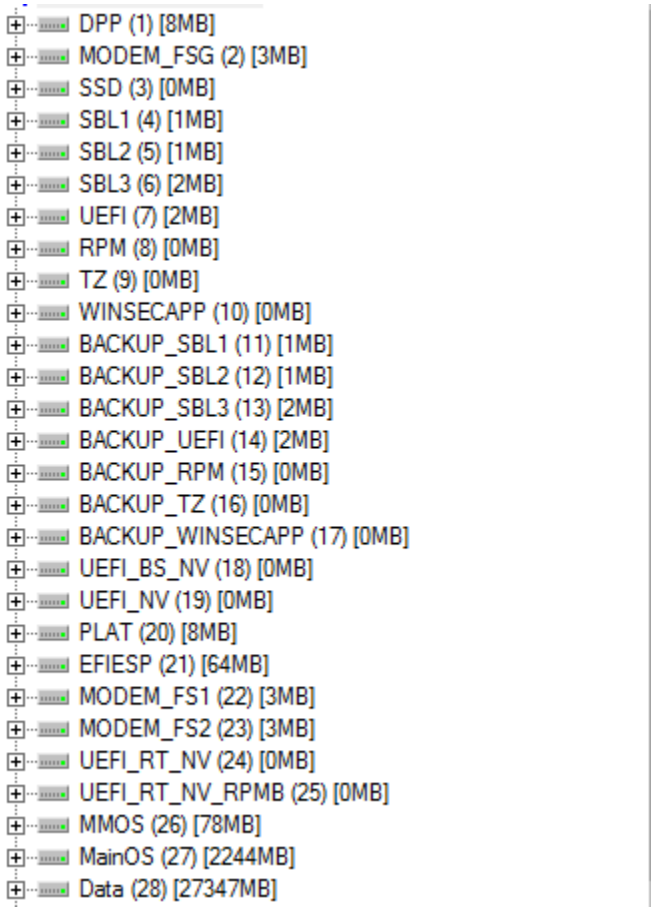
{"time":"1454779996.318","log_type":"client_event","name":"messaging_pub_ack","extra":{"status":"success_puback","retry_count":"0","sent_timestamp_ms":"1454779970023","first_message_first_send_delta":"25022","client_tag_trigger":"neue_main_recents
{"time":"1454779996.808","log_type":"client_event","name":"delivery_receipt_received","extra":{"watermark_timestamp":"1454779997721","message_id":"mid.1454779997717:2ee158a1acb3933053","sequence_id":"45394","user_fbid":"1[redacted]"}}
{"time":"1454780001.091","log_type":"client_event","name":"messaging_send_via_mqtt","extra":{"status":"success","first_send_delta":"29656","initial_mqtt_push_state":"CONNECTED","current_time":"1454780000949","mqtt_push_state":"CONNECTED","retry_

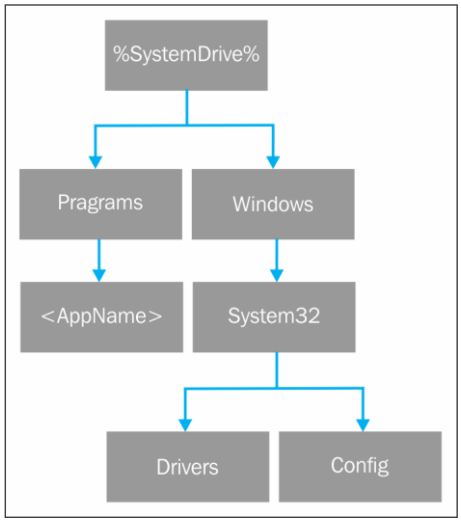
Chapter 5: Windows Phone 8 Forensics

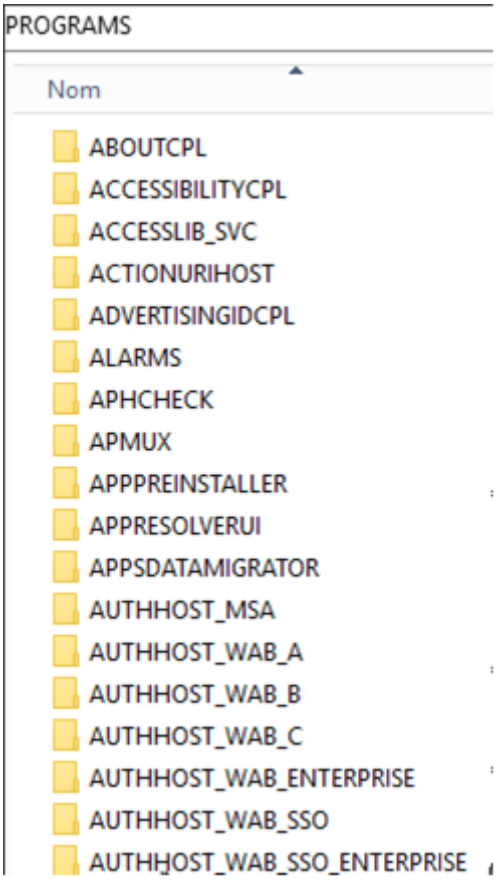


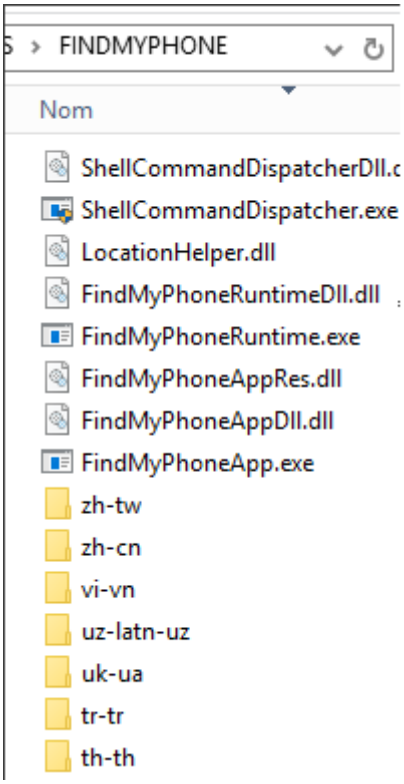

Application platforms
User-mode drivers (UMDF)
Shell services
Media Foundation
Audio stack
Video rendering stack
DirectX 11 user-mode graphics stack
ESENT database
Radio/ telephony
Kernel
File system/ storage
I/O manager
Network manager
File system/ storage
Security
Networking
PEP extensions
Kernel-mode drivers (KMDF)
HAL extensions
Boot manager
UEFI apps
HAL
UEFI
Hardware
Microsoft
OEM
SV
Microsoft/OEM/SV

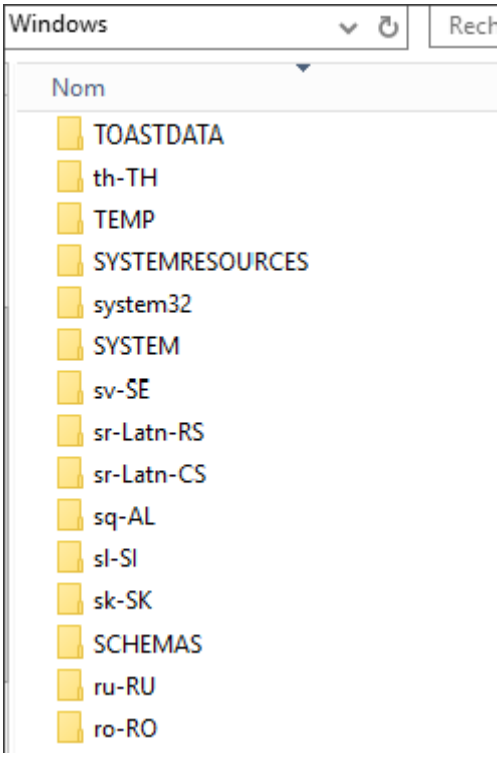

Device powered on
Fireware boot loaders
UEFI
OEM UEFI applications
Boot environment
Windows Phone Boot Manager
Boot to phone reset mode
Boot to FFU flashing mode
Boot to main OS
Boot to main OS

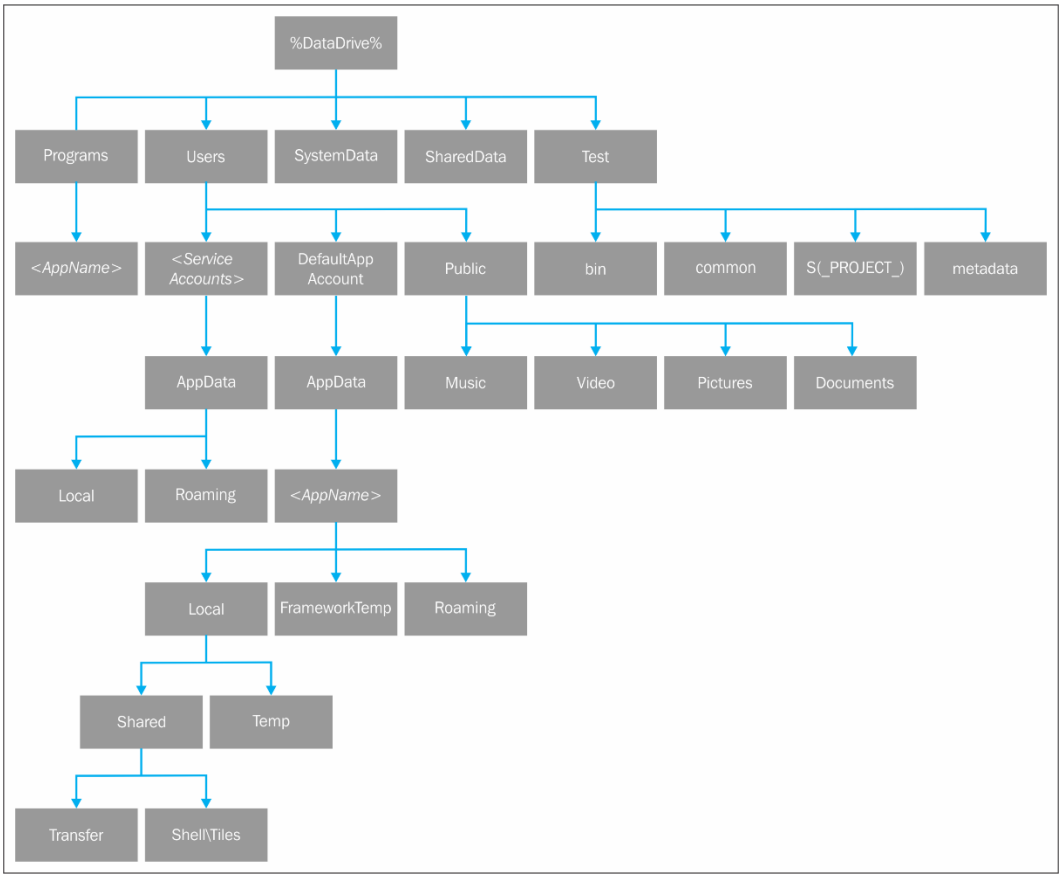

DPP (1) [8MB]
MODEM_FSG (2) [3MB]
SSD (3) [0MB]
SBL1 (4) [1MB]
SBL2 (5) [1MB]
SBL3 (6) [2MB]
UEFI (7) [2MB]
RPM (8) [0MB]
TZ (9) [0MB]
WINSECAPP (10) [0MB]
BACKUP_SBL1 (11) [1MB]
BACKUP_SBL2 (12) [1MB]
BACKUP_SBL3 (13) [2MB]
BACKUP_UEFI (14) [2MB]
BACKUP_RPM (15) [0MB]
BACKUP_TZ (16) [0MB]
BACKUP_WINSECAPP (17) [0MB]
UEFI_BS_NV (18) [0MB]
UEFI_NV (19) [0MB]
PLAT (20) [8MB]
EFIESP (21) [64MB]
MODEM_FS1 (22) [3MB]
MODEM_FS2 (23) [3MB]
UEFI_RT_NV (24) [0MB]
UEFI_RT_NV_RPMB (25) [0MB]
MMOS (26) [78MB]
MainOS (27) [2244MB]
Data (28) [27347MB]

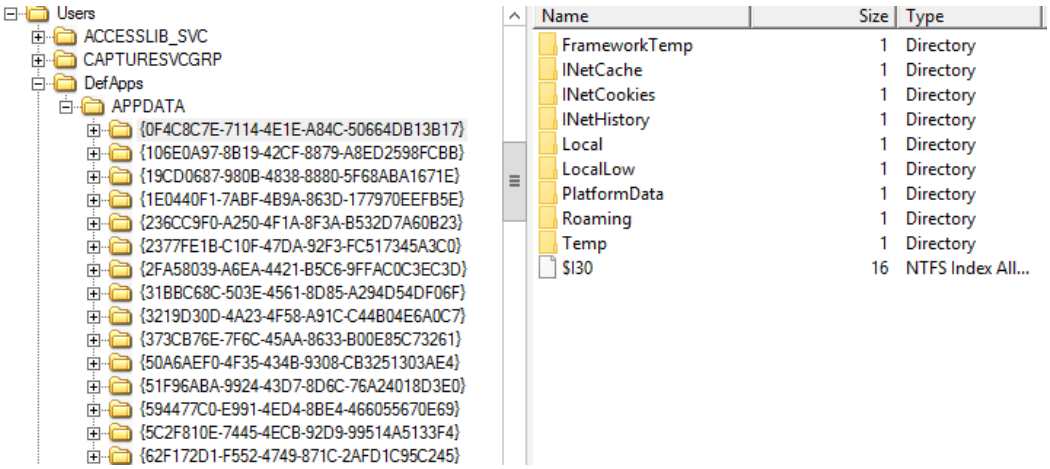

%SystemDrive%
Pragrams
Windows
<AppName>
System32
Drivers
Config

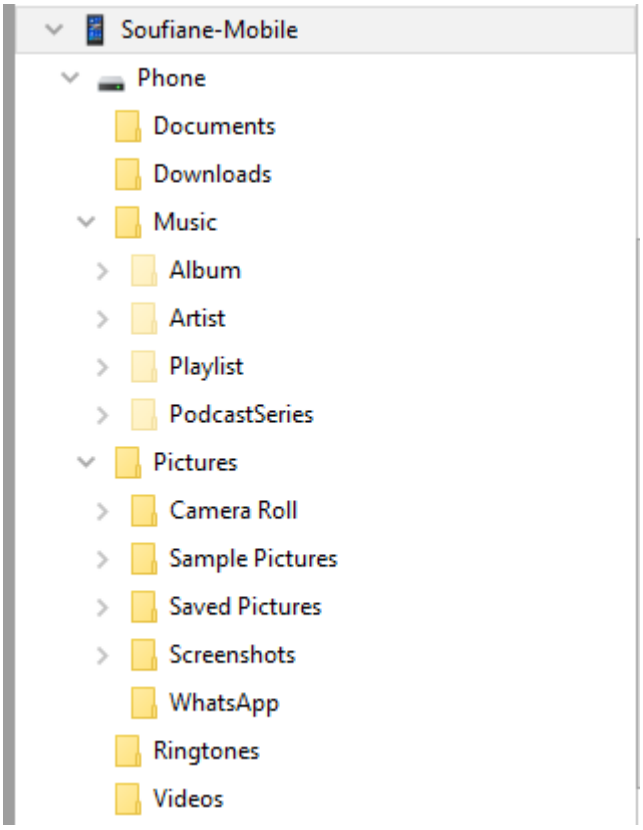

PROGRAMS
Nom
ABOUTCPL
ACCESSIBILITYCPL
ACCESSLIB_SVC
ACTIONURIHOST
ADVERTISINGIDCPL
ALARMS
APHCHECK
APMUX
APPPREINSTALLER
APPRESOLVERUI
APPSDATAMIGRATOR
AUTHHOST_MSA
AUTHHOST_WAB_A
AUTHHOST_WAB_B
AUTHHOST_WAB_C
AUTHHOST_WAB_ENTERPRISE
AUTHHOST_WAB_SSO
AUTHHOST_WAB_SSO_ENTERPRISE

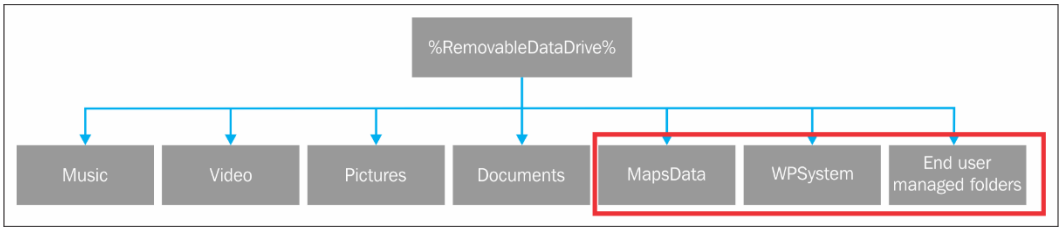

FINDMYPHONE
Nom
ShellCommandDispatcherDll.c
ShellCommandDispatcher.exe
LocationHelper.dll
FindMyPhoneRuntimeDll.dll
FindMyPhoneRuntime.exe
FindMyPhoneAppRes.dll
FindMyPhoneAppDll.dll
FindMyPhoneApp.exe
zh-tw
zh-cn
vi-vn
uz-latn-uz
uk-ua
tr-tr
th-th


Windows
Rech
Nom
TOASTDATA
th-TH
TEMP
SYSTEMRESOURCES
system32
SYSTEM
sv-SE
sr-Latn-RS
sr-Latn-CS
sq-AL
sl-SI
sk-SK
SCHEMAS
ru-RU
ro-RO

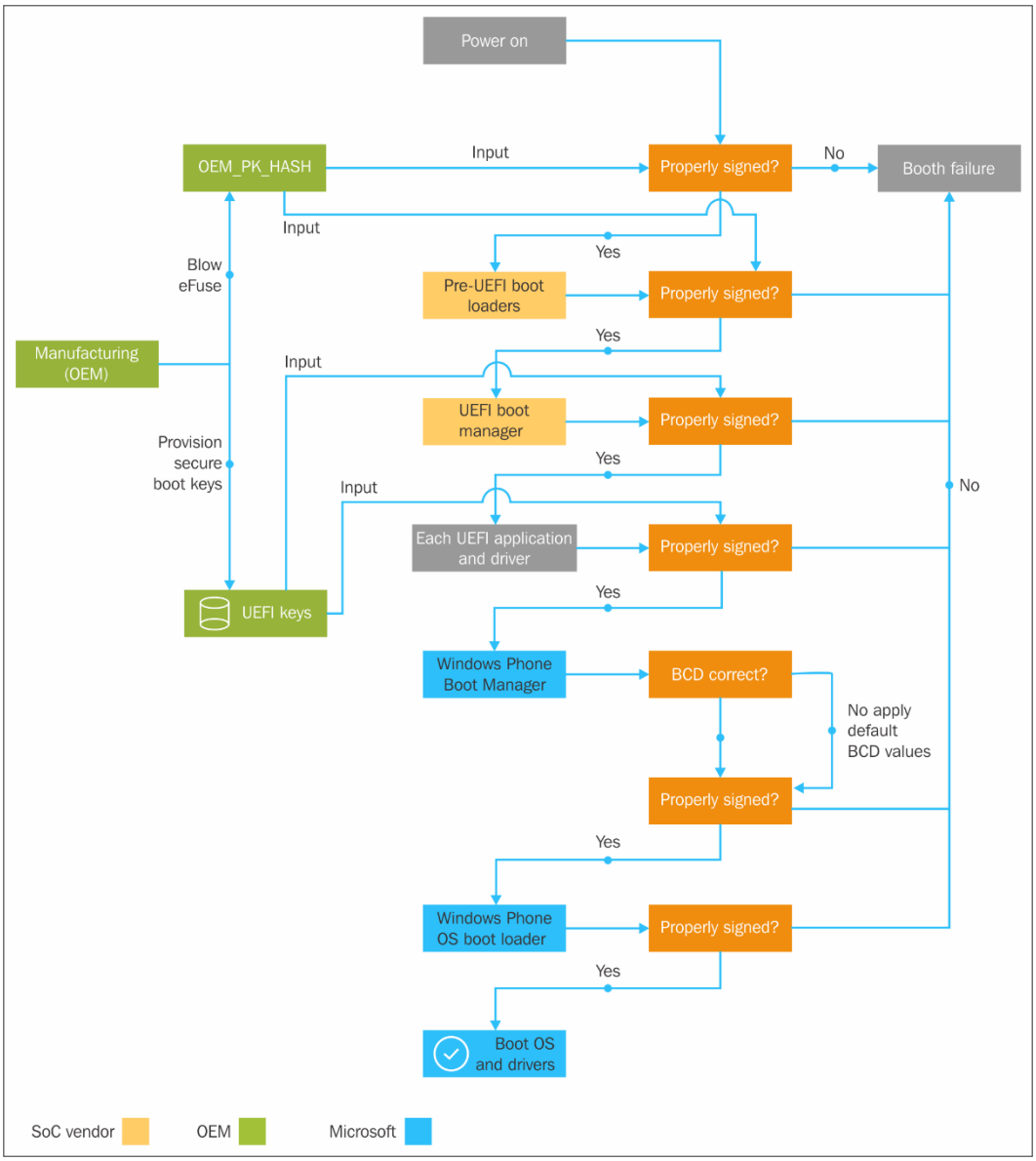

%DataDrive%
Programs
Users
SystemData
SharedData
Test
<AppName>
<Service Accounts>
DefaultApp Account
Public
bin
common
S(_PROJECT_)
metadata
AppData
AppData
Music
Video
Pictures
Documents
Local
Roaming
<AppName>
Local
FrameworkTemp
Roaming
Shared
Temp
Transfer
Shell\Tiles

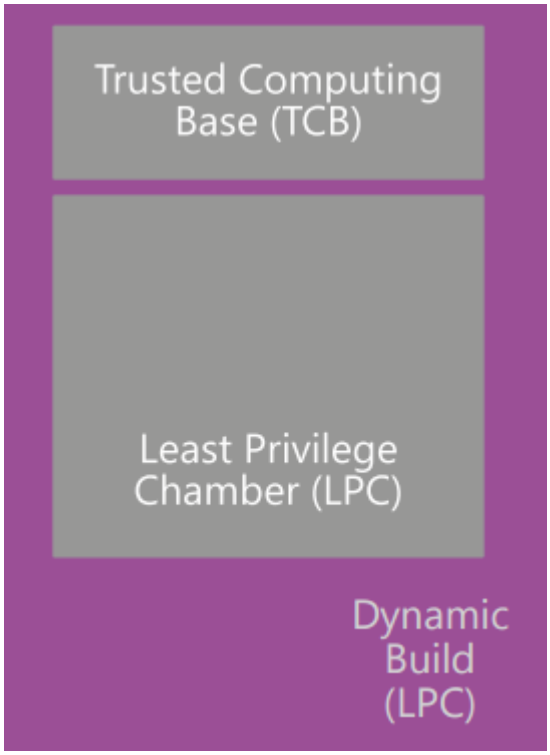

Users
ACCESSLIB_SVC
CAPTURESVCGRP
DefApps
APPDATA
{0F4C8C7E-7114-4E1E-A84C-50664DB13B17}
{106E0A97-8B19-42CF-8879-A8ED2598FCBB}
{19CD0687-980B-4838-8880-5F68ABA1671E}
{1E0440F1-7ABF-4B9A-863D-177970EEFB5E}
{236CC9F0-A250-4F1A-8F3A-B532D7A60B23}
{2377FE1B-C10F-47DA-92F3-FC517345A3C0}
{2FA58039-A6EA-4421-B5C6-9FFAC0C3EC3D}
{31BBC68C-503E-4561-8D85-A294D54DF06F}
{3219D30D-4A23-4F58-A91C-C44B04E6A0C7}
{373CB76E-7F6C-45AA-8633-B00E85C73261}
{50A6AEF0-4F35-434B-9308-CB3251303AE4}
{51F96ABA-9924-43D7-8D6C-76A24018D3E0}
{594477C0-E991-4ED4-8BE4-466055670E69}
{5C2F810E-7445-4ECB-92D9-99514A5133F4}
{62F172D1-F552-4749-871C-2AFD1C95C245}
Name
Size
Type
FrameworkTemp 1 Directory
INetCache 1 Directory
INetCookies 1 Directory
INetHistory 1 Directory
Local 1 Directory
LocalLow 1 Directory
PlatformData 1 Directory
Roaming 1 Directory
Temp 1 Directory
$I30 16 NTFS Index All...

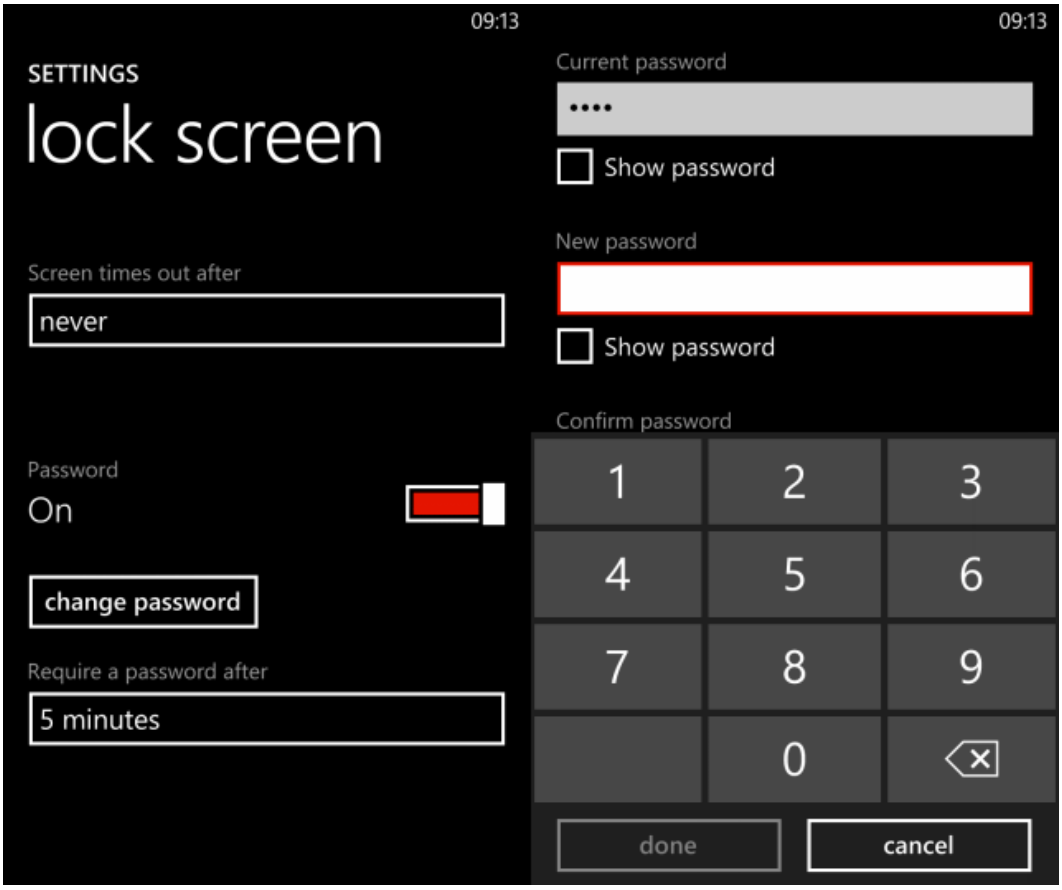


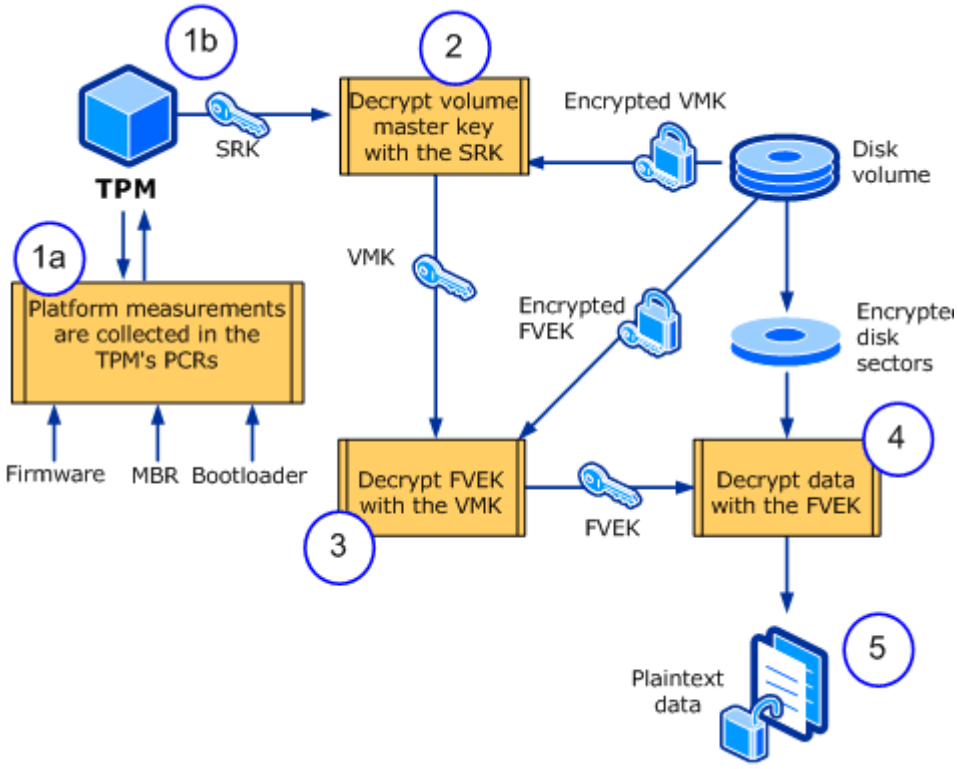


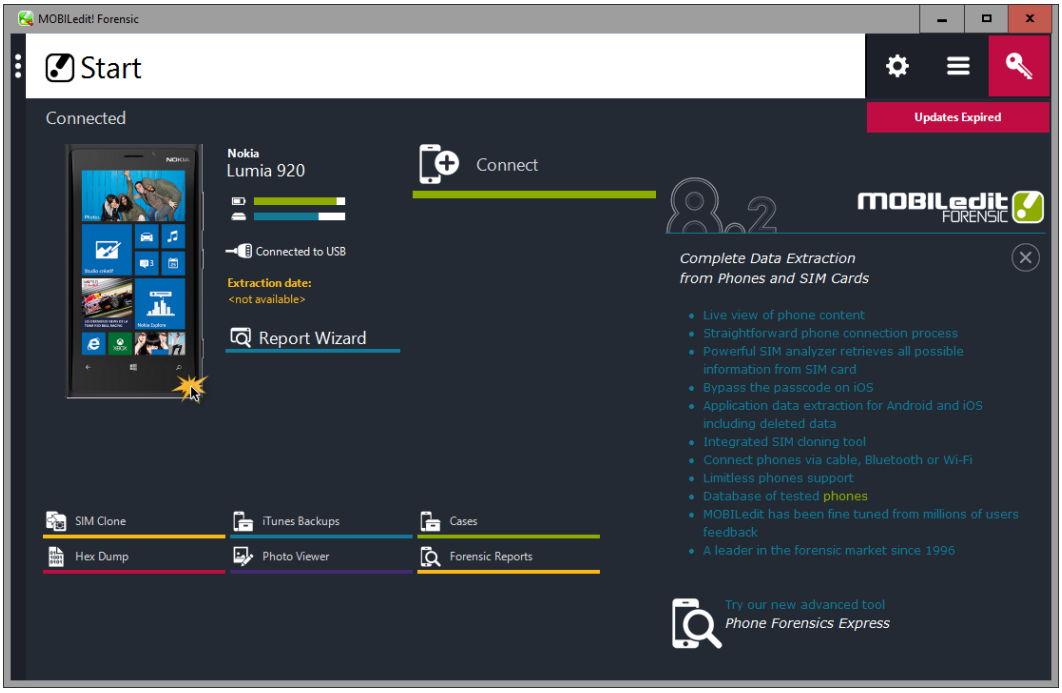
	UEFI Secure Boot	Code-signed chain of trust
	Certified hardware	TPM 2.0 – all phones


Power on
OEM_PK_HASH
Input
Properly signed?
No
Booth failure
Input
Yes
Blow eFuse
Pre-UEFI boot loaders
Properly signed?
Yes
Manufacturing (OEM)
Input
UEFI boot manager
Properly signed?
Provision secure boot keys
Yes
Input
No
Each UEFI application and driver
Properly signed?
Yes
UEFI keys
Windows Phone Boot Manager
BCD correct?
No apply default BCD values
Properly signed?
Yes
Windows Phone OS boot loader
Properly signed?
Yes
Boot OS and drivers
SoC vendor
OEM
Microsoft

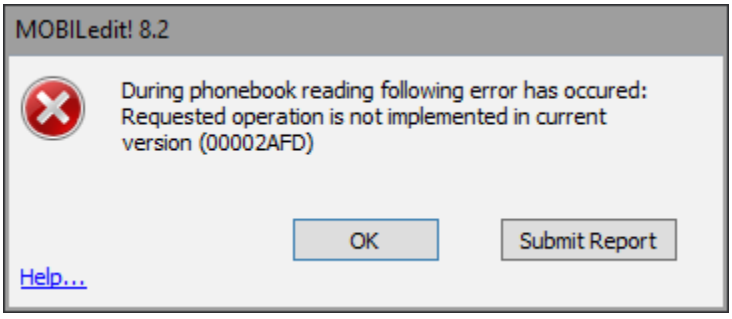

Trusted Computing Base (TCB)
Least Privilege Chamber (LPC)
Dynamic Build (LPC)

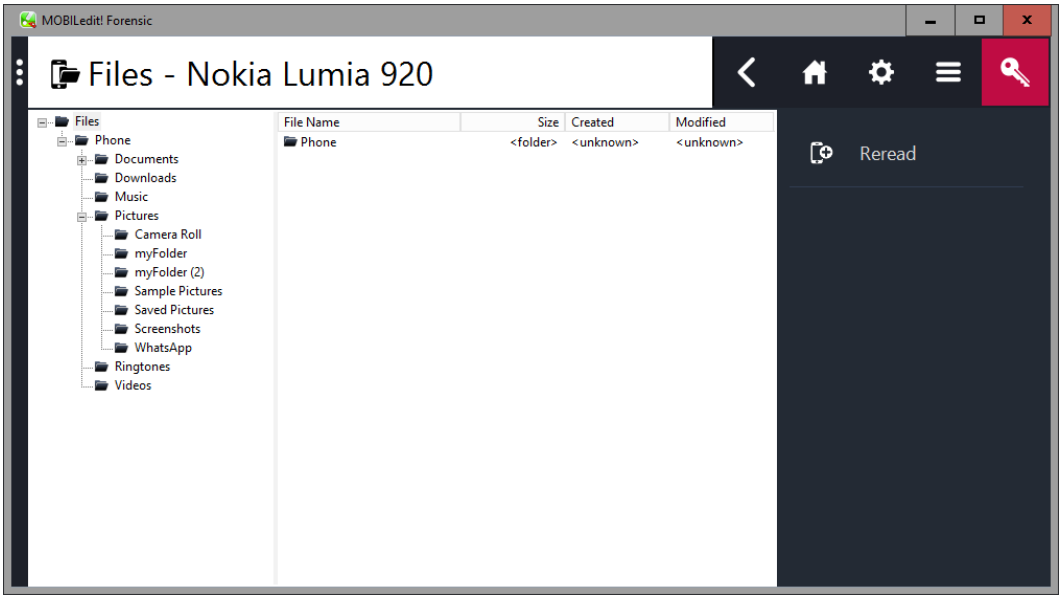

09:13
SETTINGS
lock screen
Screen times out after
never
Password
On
change password
Require a password after
5 minutes
09:13
Current password
••••
Show password
New password
Show password
Confirm password
1
2
3
4
5
6
7
8
9
0
done
cancel

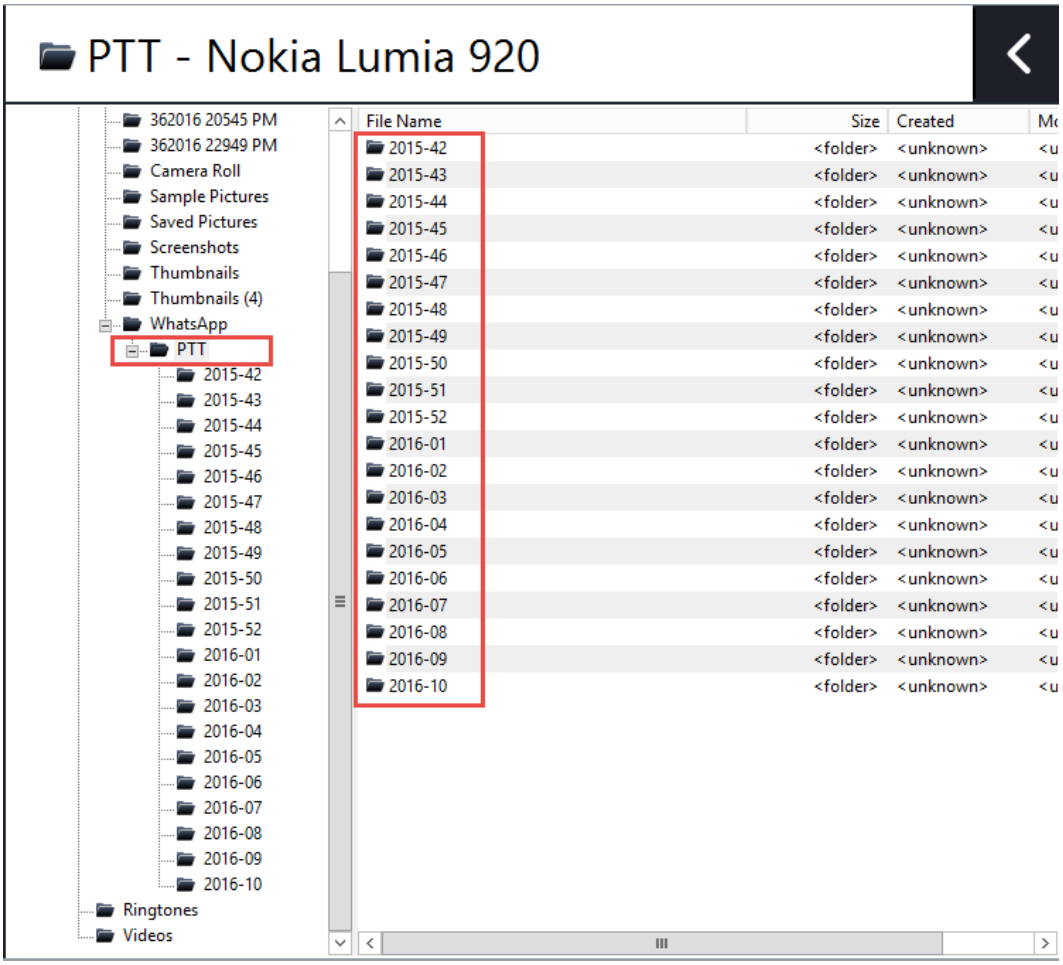

1b
2
Decrypt volume master key with the SRK
Encrypted VMK
Disk volume
SRK
TPM
1a
VMK
Encrypted FVEK
Encrypted disk sectors
Platform measurements are collected in the TPM's PCRs
Firmware
MBR
Bootloader
Decrypt FVEK with the VMK
FVEK
Decrypt data with the FVEK
4
3
5
Plaintext data

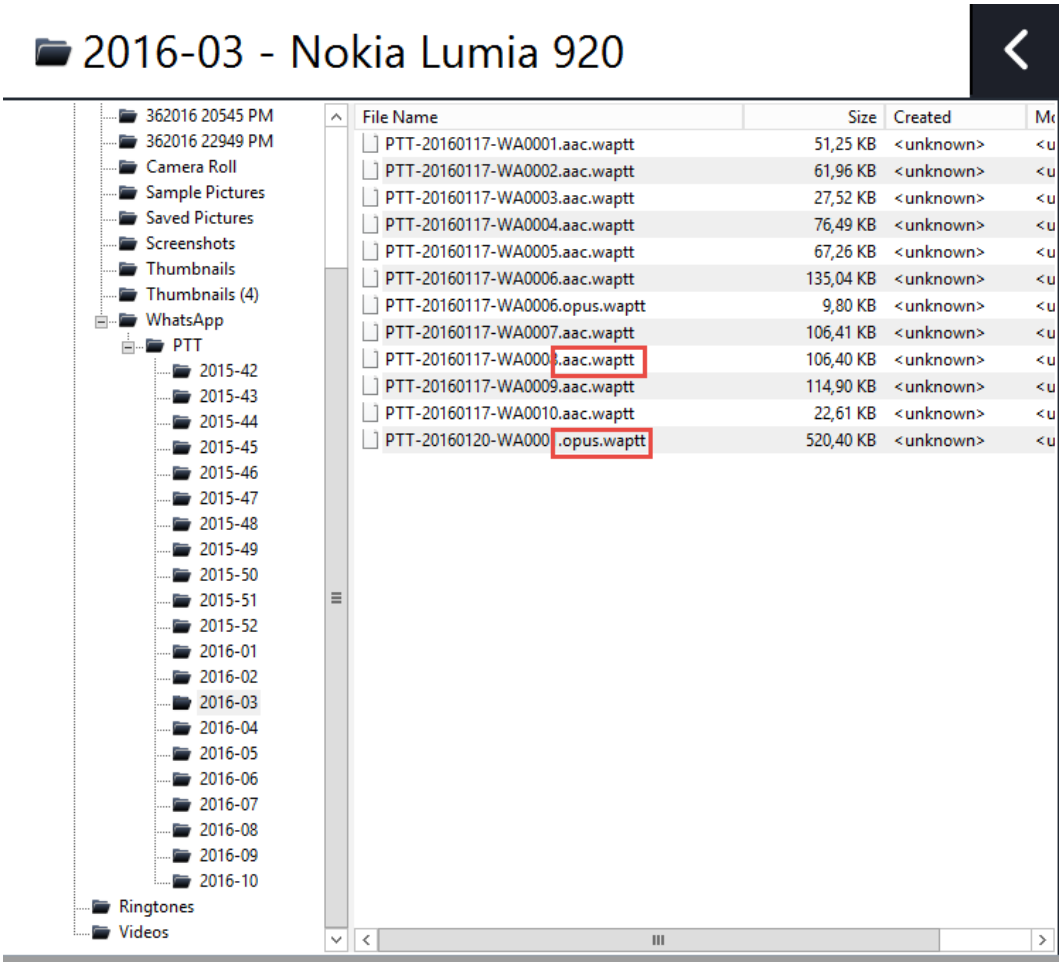

MOBILedit! Forensic
Start
Connected
Updates Expired
Nokia
Lumia 920
Connected to USB
Extraction date:
<not available>
Report Wizard
Connect
MOBILedit FORENSIC
Complete Data Extraction
from Phones and SIM Cards
Live view of phone content
Straightforward phone connection process
Powerful SIM analyzer retrieves all possible information from SIM card
Bypass the passcode on iOS
Application data extraction for Android and iOS including deleted data
Integrated SIM cloning tool
Connect phones via cable, Bluetooth or Wi-Fi
Limitless phones support
Database of tested phones
MOBILedit has been fine tuned from millions of users feedback
A leader in the forensic market since 1996
SIM Clone
iTunes Backups
Cases
Hex Dump
Photo Viewer
Forensic Reports
Try our new advanced tool
Phone Forensics Express

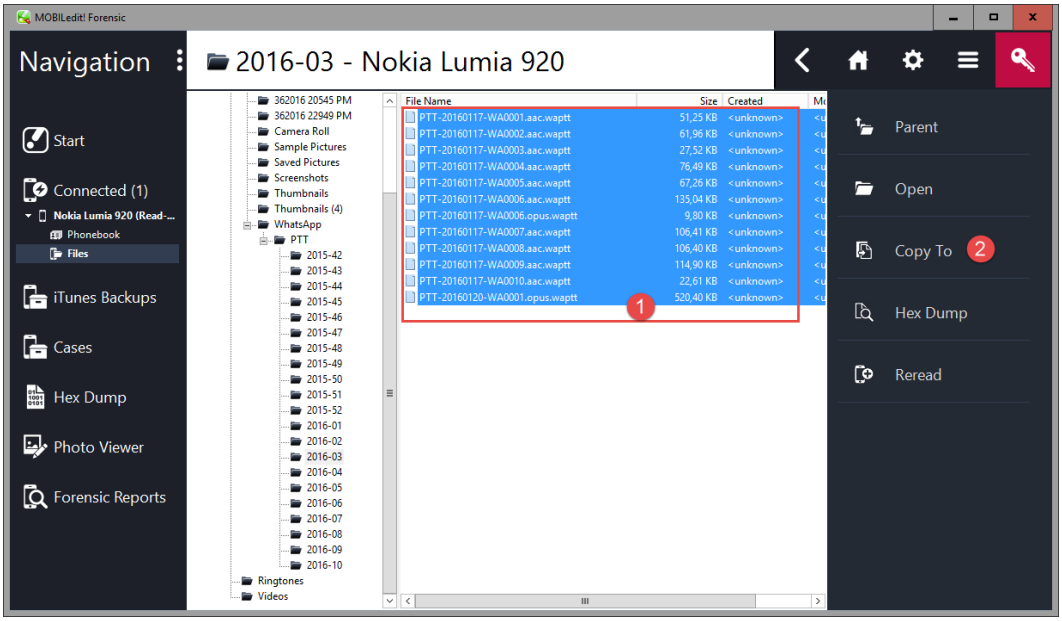

MOBILedit! Forensic
Nokia Lumia 920 (Read-Only)
Manufacturer: Nokia
Model: Lumia 920
Operator: Not available
Phone time: <unknown>
Hardware revision: NOKIA,Lumia 920 ,A92EF159CE532D459711CA4EE
Software revision: 8.10.14234.0,MTP: 1.00
Networks: GSM
Platform: Windows Phone
Cable name: Micro USB, micro-USB, Nokia CA-101
Phonebook
Files
Online Info
Report Wizard
Reports
Windows Phone 8.10.142
USB

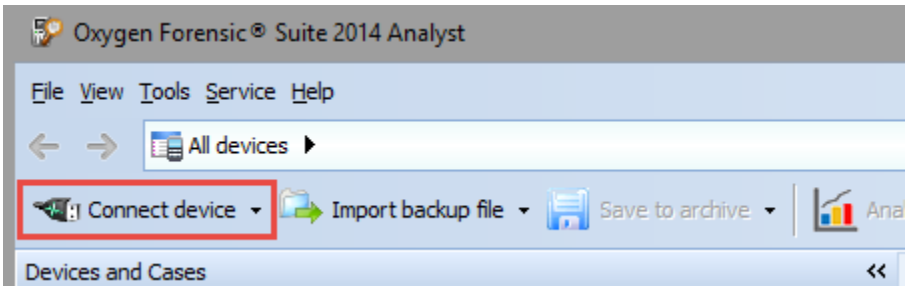

MOBILedit! 8.2
During phonebook reading following error has occured: Requested operation is not implemented in current version (00002AFD)
OK
Submit Report
Help...

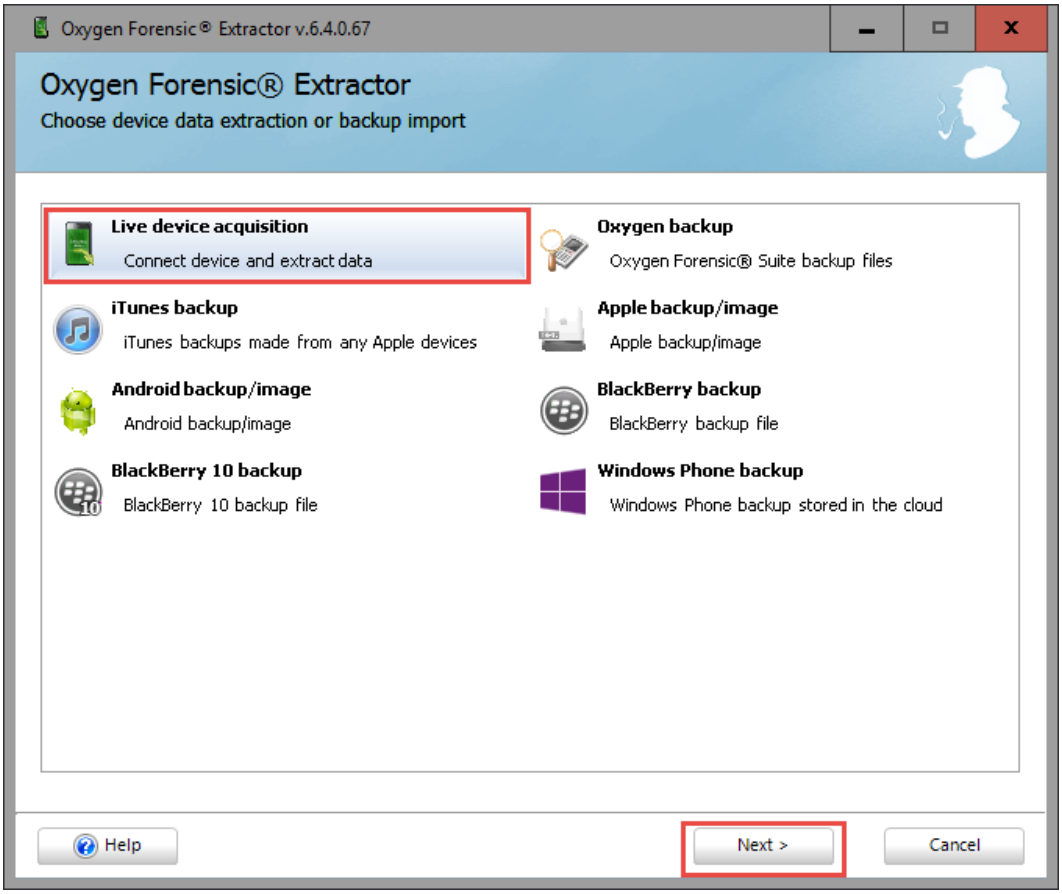

MOBILedit! Forensic
Files - Nokia Lumia 920
Files
Phone
Documents
Downloads
Music
Pictures
Camera Roll
myFolder
myFolder (2)
Sample Pictures
Saved Pictures
Screenshots
WhatsApp
Ringtones
Videos
File Name
Size
Created
Modified
Phone
<folder>
<unknown>
<unknown>
Reread


PTT - Nokia Lumia 920
362016 20545 PM
362016 22949 PM
Camera Roll
Sample Pictures
Saved Pictures
Screenshots
Thumbnails
Thumbnails (4)
WhatsApp
PTT
2015-42
2015-43
2015-44
2015-45
2015-46
2015-47
2015-48
2015-49
2015-50
2015-51
2015-52
2016-01
2016-02
2016-03
2016-04
2016-05
2016-06
2016-07
2016-08
2016-09
2016-10
Ringtones
Videos
File Name
Size
Created
2015-42 <folder> <unknown>
2015-43 <folder> <unknown>
2015-44 <folder> <unknown>
2015-45 <folder> <unknown>
2015-46 <folder> <unknown>
2015-47 <folder> <unknown>
2015-48 <folder> <unknown>
2015-49 <folder> <unknown>
2015-50 <folder> <unknown>
2015-51 <folder> <unknown>
2015-52 <folder> <unknown>
2016-01 <folder> <unknown>
2016-02 <folder> <unknown>
2016-03 <folder> <unknown>
2016-04 <folder> <unknown>
2016-05 <folder> <unknown>
2016-06 <folder> <unknown>
2016-07 <folder> <unknown>
2016-08 <folder> <unknown>
2016-09 <folder> <unknown>
2016-10 <folder> <unknown>


2016-03 - Nokia Lumia 920
362016 20545 PM
362016 22949 PM
Camera Roll
Sample Pictures
Saved Pictures
Screenshots
Thumbnails
Thumbnails (4)
WhatsApp
PTT
2015-42
2015-43
2015-44
2015-45
2015-46
2015-47
2015-48
2015-49
2015-50
2015-51
2015-52
2016-01
2016-02
2016-03
2016-04
2016-05
2016-06
2016-07
2016-08
2016-09
2016-10
Ringtones
Videos
File Name
Size
Created
PTT-20160117-WA0001.aac.waptt 51,25 KB <unknown>
PTT-20160117-WA0002.aac.waptt 61,96 KB <unknown>
PTT-20160117-WA0003.aac.waptt 27,52 KB <unknown>
PTT-20160117-WA0004.aac.waptt 76,49 KB <unknown>
PTT-20160117-WA0005.aac.waptt 67,26 KB <unknown>
PTT-20160117-WA0006.aac.waptt 135,04 KB <unknown>
PTT-20160117-WA0006.opus.waptt 9,80 KB <unknown>
PTT-20160117-WA0007.aac.waptt 106,41 KB <unknown>
PTT-20160117-WA0008.aac.waptt 106,40 KB <unknown>
PTT-20160117-WA0009.aac.waptt 114,90 KB <unknown>
PTT-20160117-WA0010.aac.waptt 22,61 KB <unknown>
PTT-20160120-WA000 .opus.waptt 520,40 KB <unknown>


MOBILedit! Forensic
Navigation
2016-03 - Nokia Lumia 920
Start
Connected (1)
Nokia Lumia 920 (Read-...
Phonebook
Files
iTunes Backups
Cases
Hex Dump
Photo Viewer
Forensic Reports
362016 20545 PM
362016 22949 PM
Camera Roll
Sample Pictures
Saved Pictures
Screenshots
Thumbnails
Thumbnails (4)
WhatsApp
PTT
2015-42
2015-43
2015-44
2015-45
2015-46
2015-47
2015-48
2015-49
2015-50
2015-51
2015-52
2016-01
2016-02
2016-03
2016-04
2016-05
2016-06
2016-07
2016-08
2016-09
2016-10
Ringtones
Videos
File Name
Size
Created
PTT-20160117-WA0001.aac.waptt 51,25 KB <unknown>
PTT-20160117-WA0002.aac.waptt 61,96 KB <unknown>
PTT-20160117-WA0003.aac.waptt 27,52 KB <unknown>
PTT-20160117-WA0004.aac.waptt 76,49 KB <unknown>
PTT-20160117-WA0005.aac.waptt 67,26 KB <unknown>
PTT-20160117-WA0006.aac.waptt 135,04 KB <unknown>
PTT-20160117-WA0006.opus.waptt 9,80 KB <unknown>
PTT-20160117-WA0007.aac.waptt 106,41 KB <unknown>
PTT-20160117-WA0008.aac.waptt 106,40 KB <unknown>
PTT-20160117-WA0009.aac.waptt 114,90 KB <unknown>
PTT-20160117-WA0010.aac.waptt 22,61 KB <unknown>
PTT-20160120-WA0001.opus.waptt 520,40 KB <unknown>
1
Parent
Open
Copy To
2
Hex Dump
Reread


Oxygen Forensic® Suite 2014 Analyst
File View Tools Service Help
All devices
Connect device
Import backup file
Save to archive
Devices and Cases


Oxygen Forensic® Extractor v.6.4.0.67
Oxygen Forensic® Extractor
Choose device data extraction or backup import
Live device acquisition
Connect device and extract data
Oxygen backup
Oxygen Forensic® Suite backup files
iTunes backup
iTunes backups made from any Apple devices
Apple backup/image
Apple backup/image
Android backup/image
Android backup/image
BlackBerry backup
BlackBerry backup file
BlackBerry 10 backup
BlackBerry 10 backup file
Windows Phone backup
Windows Phone backup stored in the cloud
Help
Next >
Cancel

Connection Mode

Please select one of connection modes:

Auto device connection

Auto mode connects the first device detected on PC.

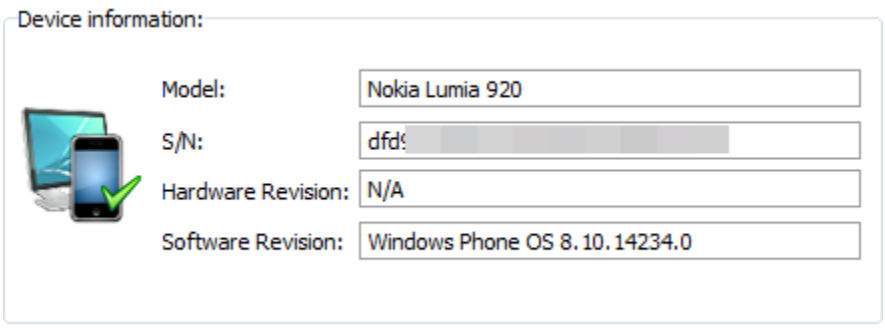
Manual device selection

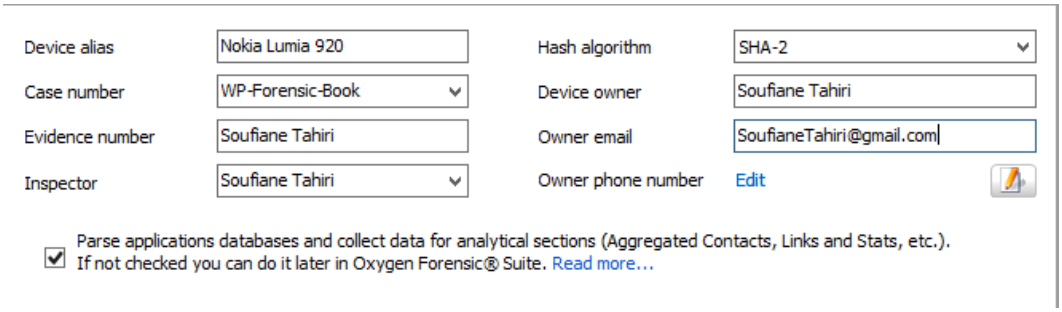
Manual selection mode allows to choose connection type and device model from the list.

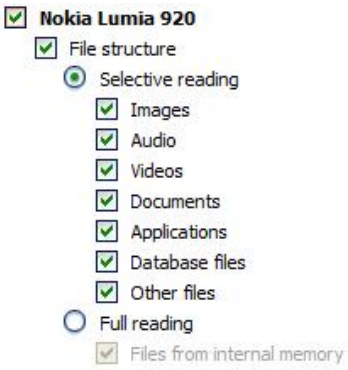
MTK Android device connection

This mode allows to extract data by creating physical dumps from MTK (MediaTeK) Android devices.
No rooting is required. Lock screen is bypassed.
The method may take a bit more time than physical dump via rooting.


Oxygen Forensic® Extractor v.6.4.0.67
Oxygen Forensic® Extractor
Detection of devices connected via cable.
Connecting device...
Connect device via cable
Searching for devices via cable. It may take some time...
Searching for a device... Please wait.
Help
< Back
Next >
Cancel

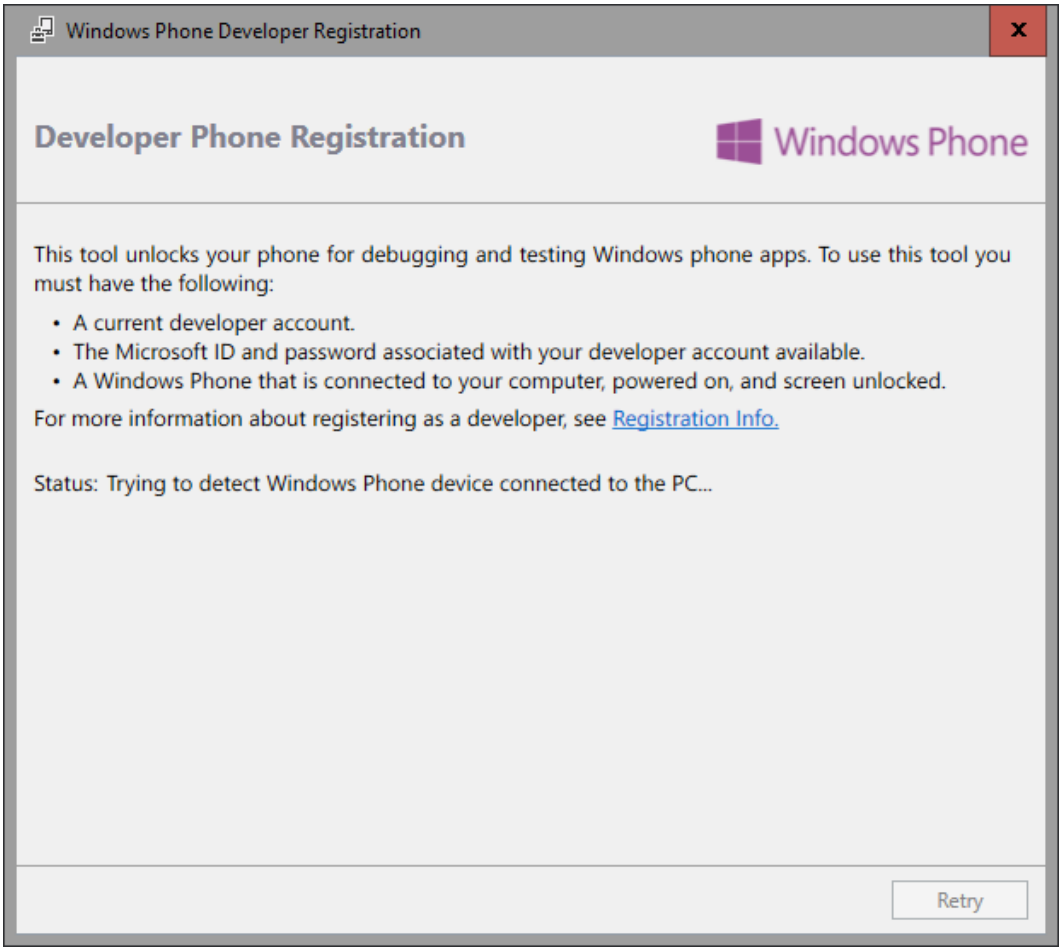

Device information:
Model:
Nokia Lumia 920
S/N:
dfd
Hardware Revision:
N/A
Software Revision:
Windows Phone OS 8.10.14234.0

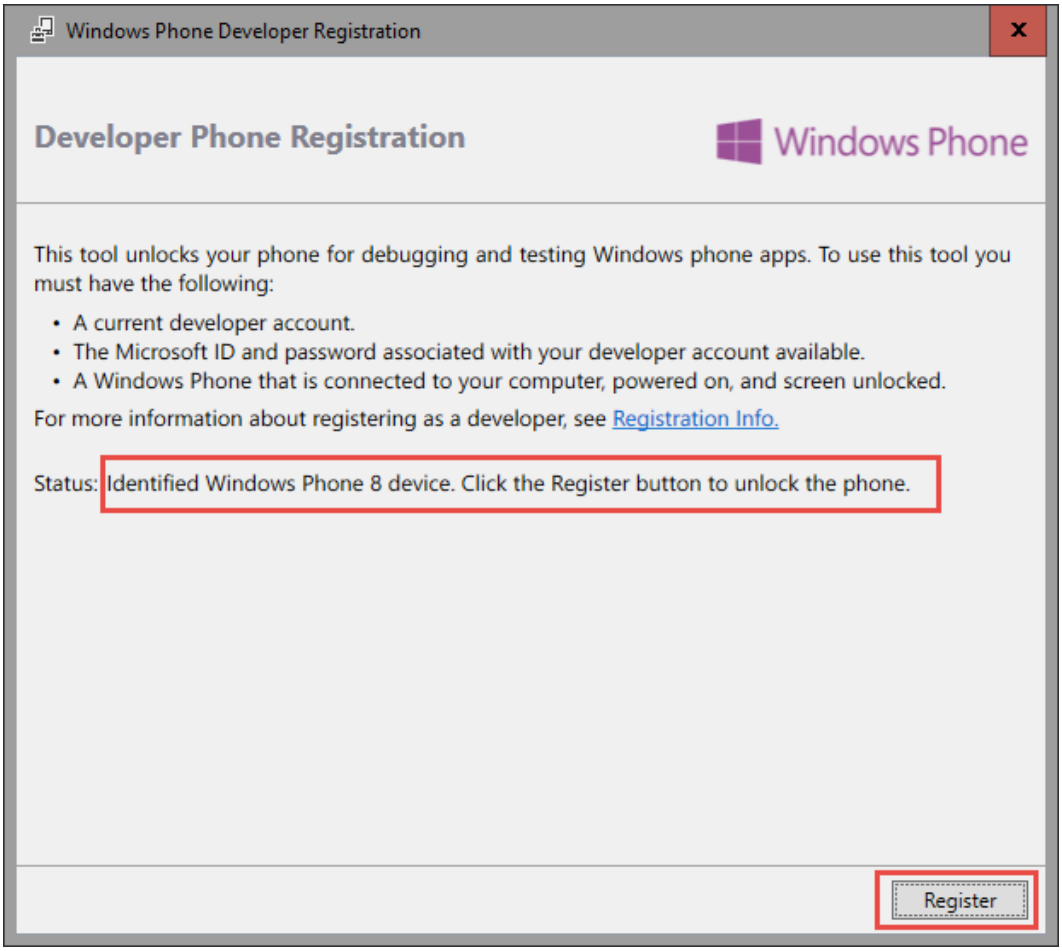

Device alias
Nokia Lumia 920
Case number
WP-Forensic-Book
Evidence number
Soufiane Tahiri
Inspector
Soufiane Tahiri
Hash algorithm
SHA-2
Device owner
Soufiane Tahiri
Owner email
SoufianeTahiri@gmail.com
Owner phone number
Edit
Parse applications databases and collect data for analytical sections (Aggregated Contacts, Links and Stats, etc.).
If not checked you can do it later in Oxygen Forensic® Suite. Read more...

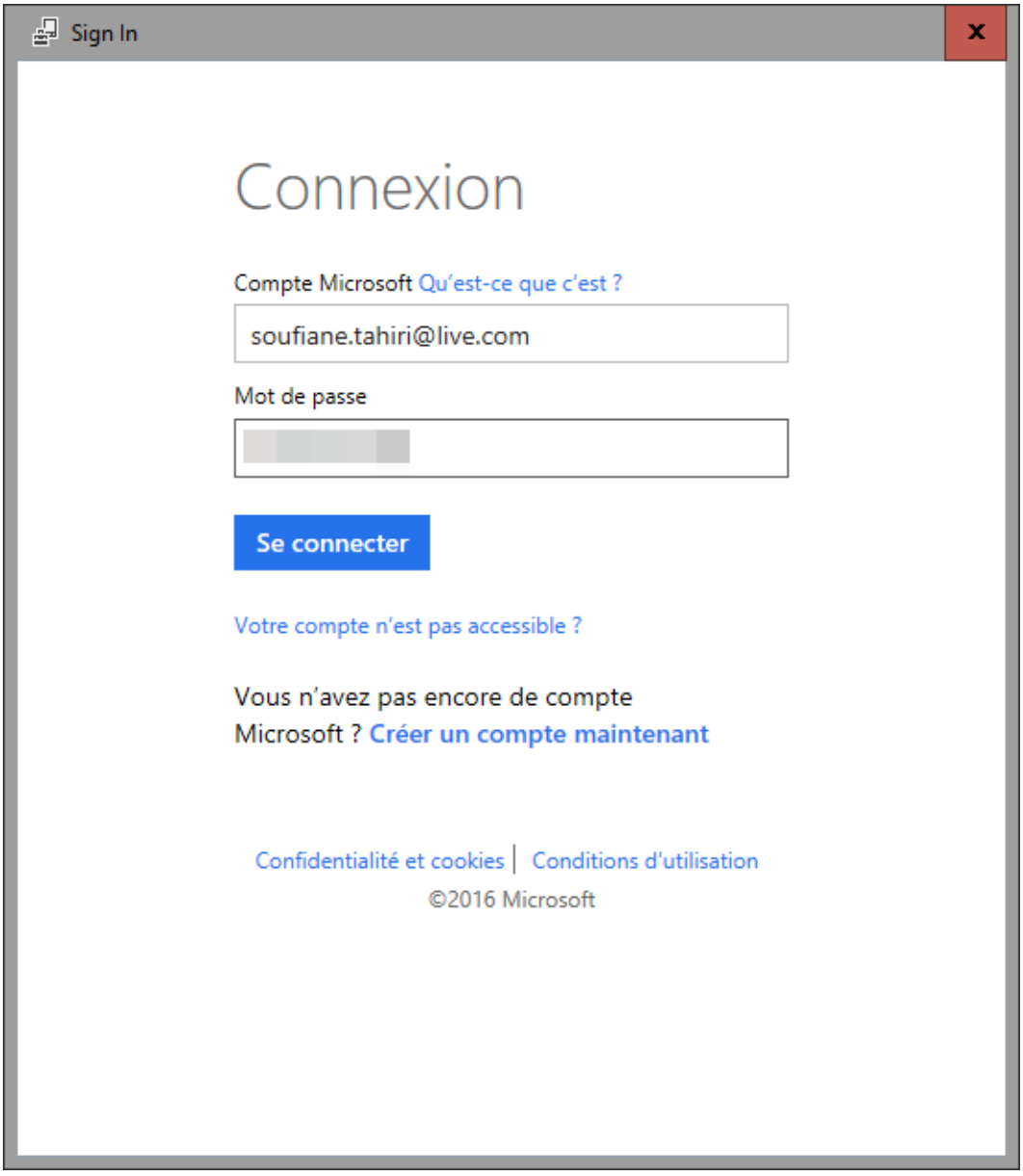

Nokia Lumia 920
File structure
Selective reading
Images
Audio
Videos
Documents
Applications
Database files
Other files
Full reading
Files from internal memory

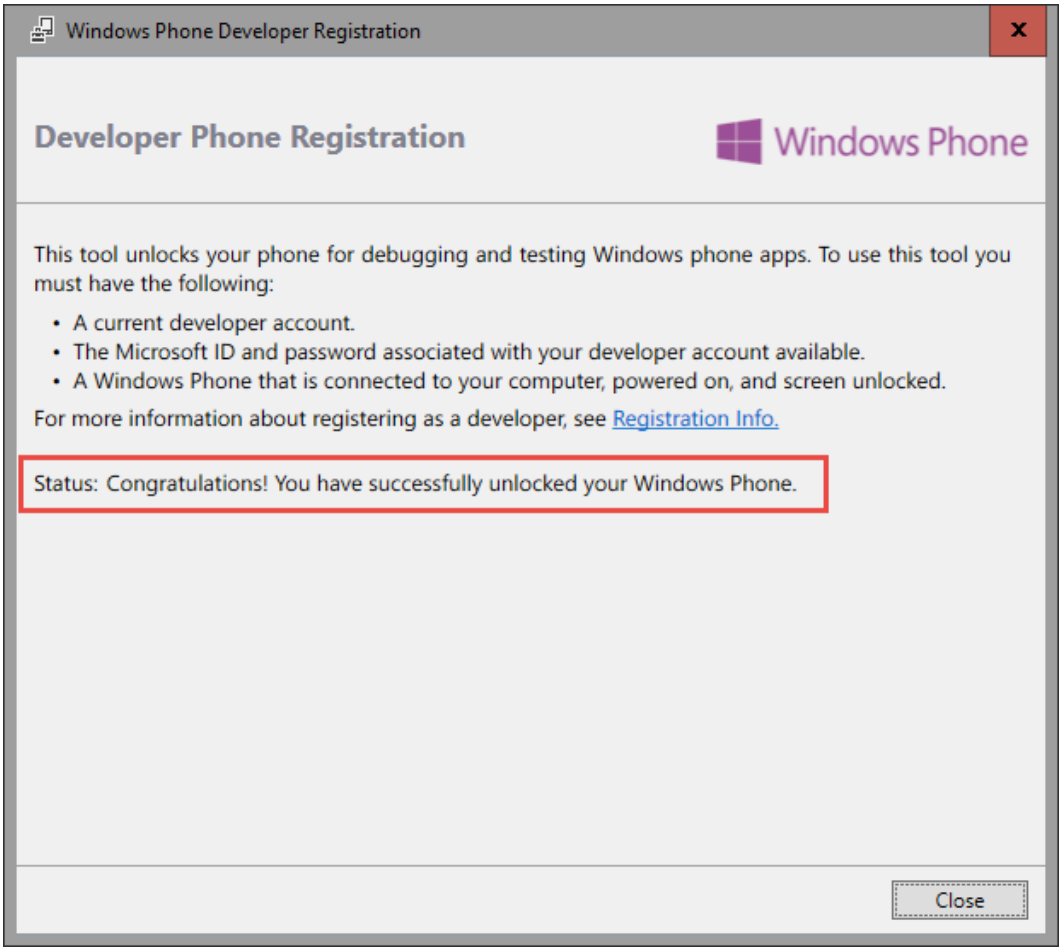

Oxygen Forensic® Extractor
Wait while the data is being extracted from the device
Extracting data...
Read files: 4,93 GB of 6,76 GB
Reading file: 1627 of 3946. C:\Pictures\Camera Roll\WP_20151230_13_43_13_Pro.jpg
Warning! The data is being extracted from the device right now.
Do not disconnect it or make any changes to the device.

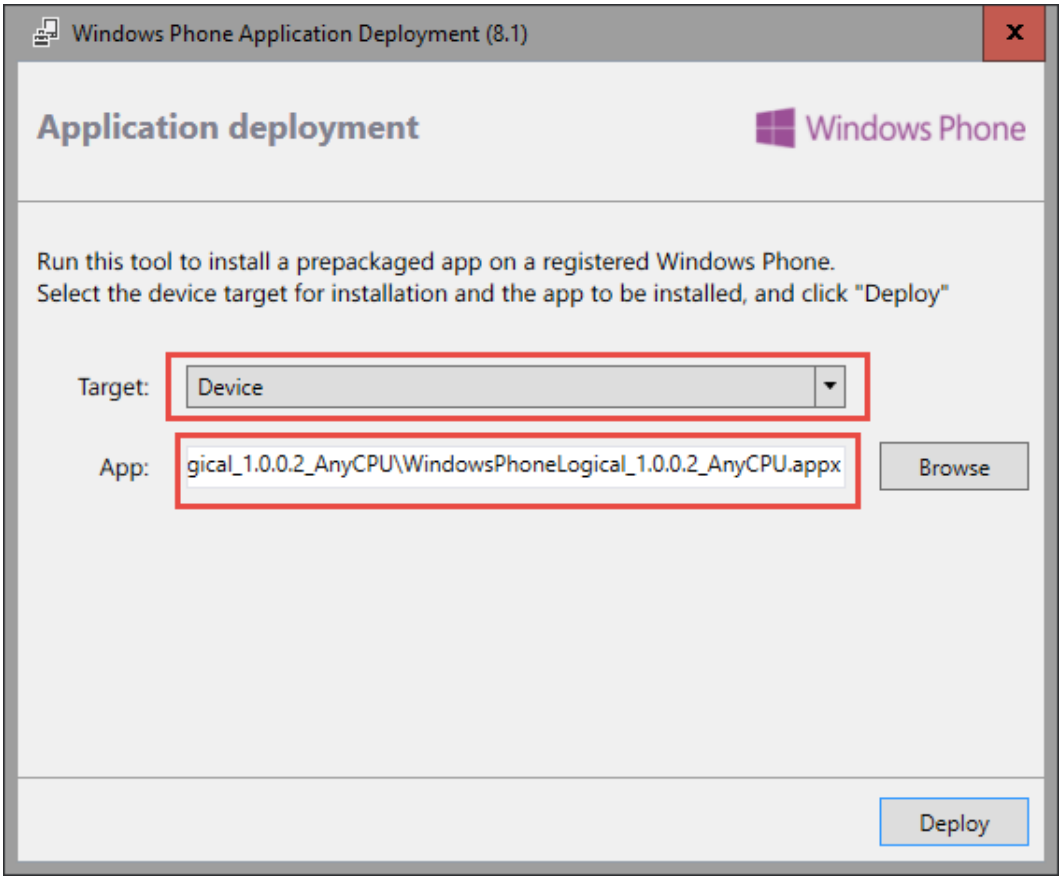

Extraction summary
Success
Final actions
Save to archive
Save extracted device to .ofb archive.
Open device
Open device and start analyzing.
Export and Print
Print or export full device data report.

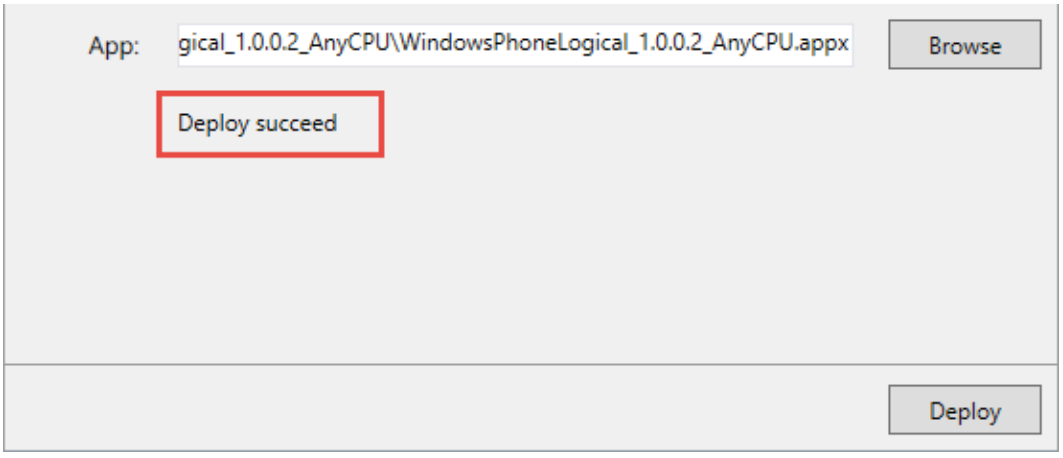

Windows Phone Developer Registration
Developer Phone Registration
Windows Phone
This tool unlocks your phone for debugging and testing Windows phone apps. To use this tool you must have the following:
• A current developer account.
• The Microsoft ID and password associated with your developer account available.
• A Windows Phone that is connected to your computer, powered on, and screen unlocked.
For more information about registering as a developer, see Registration Info.
Status: Trying to detect Windows Phone device connected to the PC...
Retry


Windows Phone Developer Registration
Developer Phone Registration
Windows Phone
This tool unlocks your phone for debugging and testing Windows phone apps. To use this tool you must have the following:
• A current developer account.
• The Microsoft ID and password associated with your developer account available.
• A Windows Phone that is connected to your computer, powered on, and screen unlocked.
For more information about registering as a developer, see Registration Info.
Status: Identified Windows Phone 8 device. Click the Register button to unlock the phone.
Register


Sign In
Connexion
Compte Microsoft Qu'est-ce que c'est ?
soufiane.tahiri@live.com
Mot de passe
Se connecter
Votre compte n'est pas accessible ?
Vous n'avez pas encore de compte Microsoft ? Créer un compte maintenant
Confidentialité et cookies | Conditions d'utilisation
©2016 Microsoft

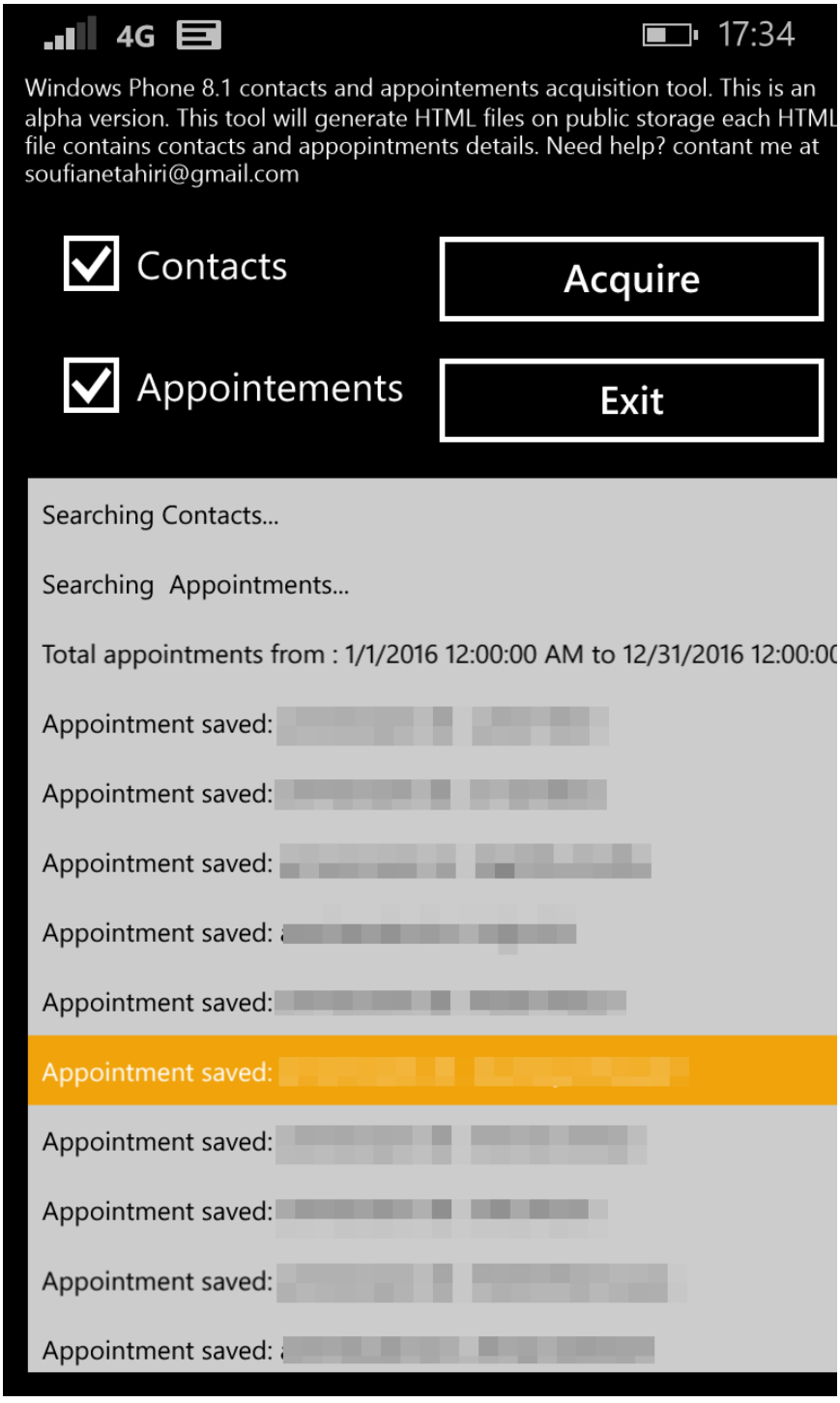

Windows Phone Developer Registration
Developer Phone Registration
Windows Phone
This tool unlocks your phone for debugging and testing Windows phone apps. To use this tool you must have the following:
• A current developer account.
• The Microsoft ID and password associated with your developer account available.
• A Windows Phone that is connected to your computer, powered on, and screen unlocked.
For more information about registering as a developer, see Registration Info.
Status: Congratulations! You have successfully unlocked your Windows Phone.
Close

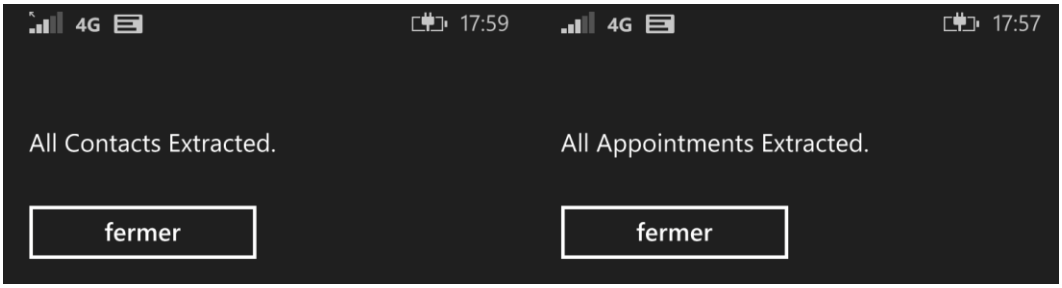

Windows Phone Application Deployment (8.1)
Application deployment
Windows Phone
Run this tool to install a prepackaged app on a registered Windows Phone.
Select the device target for installation and the app to be installed, and click "Deploy"
Target:
Device
App:
gical_1.0.0.2_AnyCPU\WindowsPhoneLogical_1.0.0.2_AnyCPU.appx
Browse
Deploy

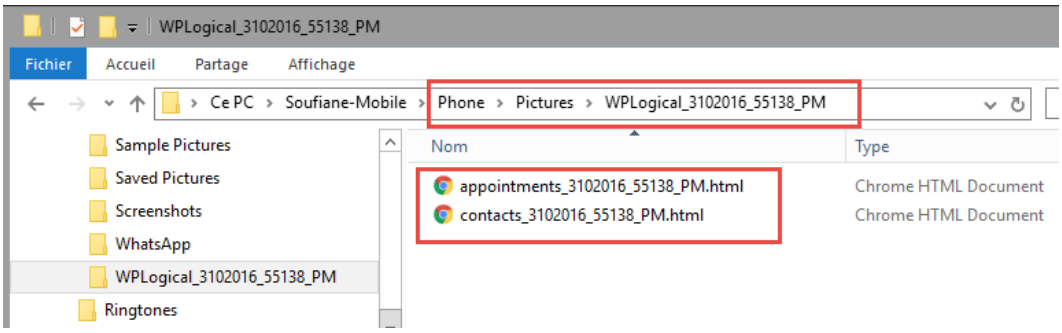

App:
gical_1.0.0.2_AnyCPU\WindowsPhoneLogical_1.0.0.2_AnyCPU.appx
Browse
Deploy succeed
Deploy


H
17:12
w
Candle WP
ScanWritr
nouveauté
Waze
WhatsApp
WindowsPhoneLogical
Wordament
rechercher dans le Store


4G
17:33
Windows Phone 8.1 contacts and appointements acquisition tool. This is an alpha version. This tool will generate HTML files on public storage each HTML file contains contacts and appopintments details. Need help? contant me at soufianetahiri@gmail.com
Contacts
Acquire
Appointments
Exit


4G
17:34
Windows Phone 8.1 contacts and appointements acquisition tool. This is an alpha version. This tool will generate HTML files on public storage each HTML file contains contacts and appopintments details. Need help? contant me at soufianetahiri@gmail.com
Contacts
Acquire
Appointements
Exit
Searching Contacts...
Searching Appointments...
Total appointments from : 1/1/2016 12:00:00 AM to 12/31/2016 12:00:00
Appointment saved:
Appointment saved:
Appointment saved:
Appointment saved:
Appointment saved:
Appointment saved:
Appointment saved:
Appointment saved:
Appointment saved:
Appointment saved:





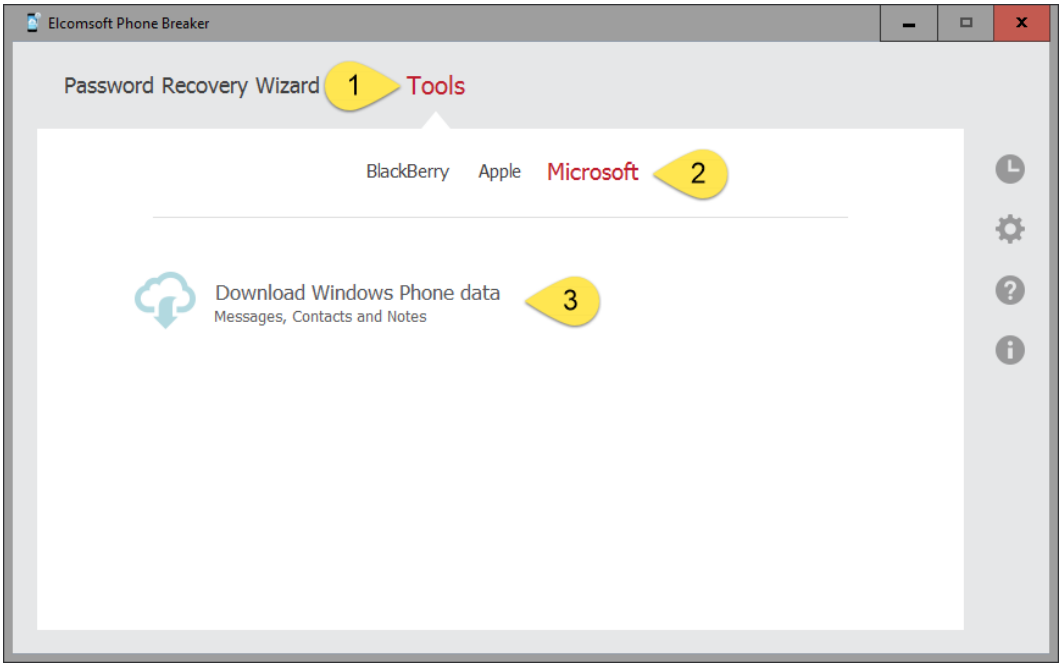
Display Name	First Name	Middle Name	Last Name	Phones	Important Dates	Emails	Websites	Job Info	Adresses	Notes	Thumbnail
											N/A
				Kind: Mobile Number: +336							N/A
				Kind: Mobile Number: Kind: Home Number: +212							N/A
				Kind: Mobile Number: 06				Title: Office CompanyName: Ecole Normale Description:			
				Kind: Mobile Number: +212 Kind: Mobile Number: 066 Kind: Home Number: 0523 Kind: Work Number: +212		Kind: Personal Email: @gmail.com Description:					
											

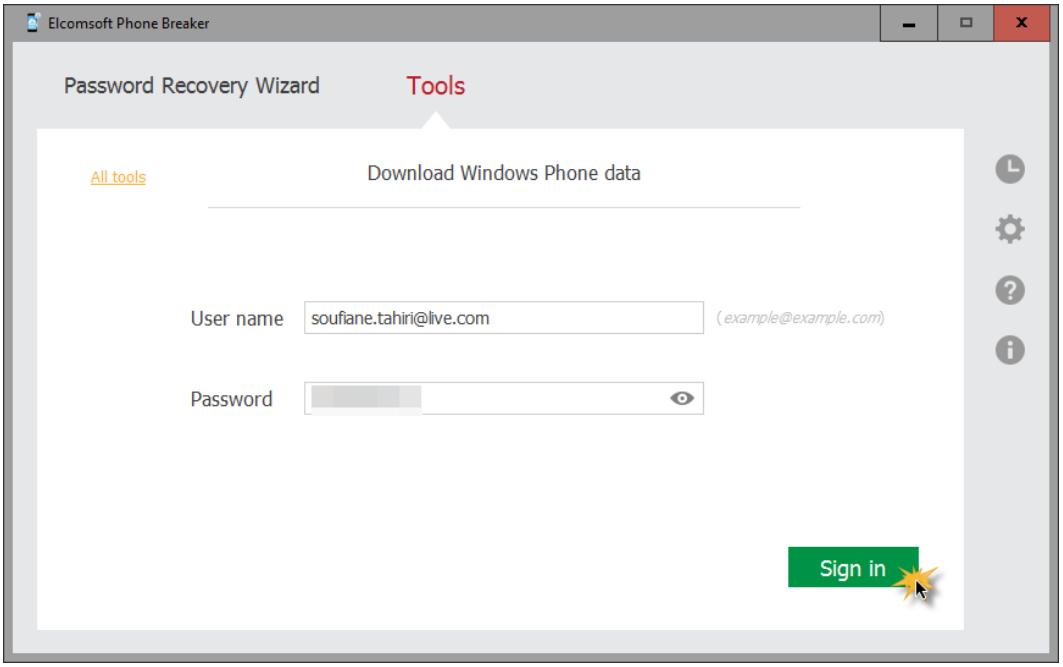
PSC - Call with Soufiane Tahiri	skype: souflanetahiri	Address: [redacted]@gmail.com Name: Gabriel [redacted]	Adress: soufianetahiri@gmail.com Name: Soufiane Tahiri Response: None Role: RequiredAttendee Adress: [redacted]@gmail.com Name: Gabriel [redacted] Response: Accepted Role: RequiredAttendee	3/1/2016 9:00:00 AM +00:00		0.5	Public		False	False	Hi Soufiane, Here is our Skype call to better understand [redacted]. On the call I will also provide more information on the [redacted]. Also the interview [redacted] regarding the [redacted] team, technology, [redacted]. Speak to you shortly. -- Gabrie [redacted] Consulting [redacted] Strategy | Growth Management | F [redacted] around www.pr [redacted]
[redacted]		N/A		3/3/2016 12:00:00 AM +00:00		24	Public		False	False	[redacted]
[redacted]		N/A		3/3/2016 12:00:00 AM +00:00	3/3/2016 12:00:00 AM +00:00	24	Public		False	False	[redacted]
[redacted]		N/A		3/4/2016 12:00:00 AM +00:00	3/4/2016 12:00:00 AM +00:00	24	Public		False	False	[redacted]
60° JAZZ TRIO en concert au Boultek // Ven 04 mars 2016	Boultek	Address: Boultek Name: EAC-L'Boulvart		3/4/2016 8:30:00 PM +00:00		3	Public		False	False	VENDREDI 04 MARS / 20h30 SALLE 36 - Boultek// 30 DHS #JAZZ avec 60° JAZZ TRIO C'est à l'occasion d'un concert en 2014, que Clément Braitman (chant et batterie), réunit Alexis Pivot (piano) et Etienne Renard (contrebasse). Les trois musiciens, faisant alors partie de la même génération montante du jazz français, se découvrent tout un vocabulaire commun et une complicité immédiate. Les concerts qui suivent seront autant d'occasions d'enrichir ce langage, à la fois intime et intuitif. A découvrir. PLUS D'INFOS SUR 60°JAZZ TRIO http://clementbraitman.com/ https://soundcloud.com/cbraitman https://www.reverbnation.com/alexispivot EN VIDEO : http://y2u.be/XsTcOvjODlk

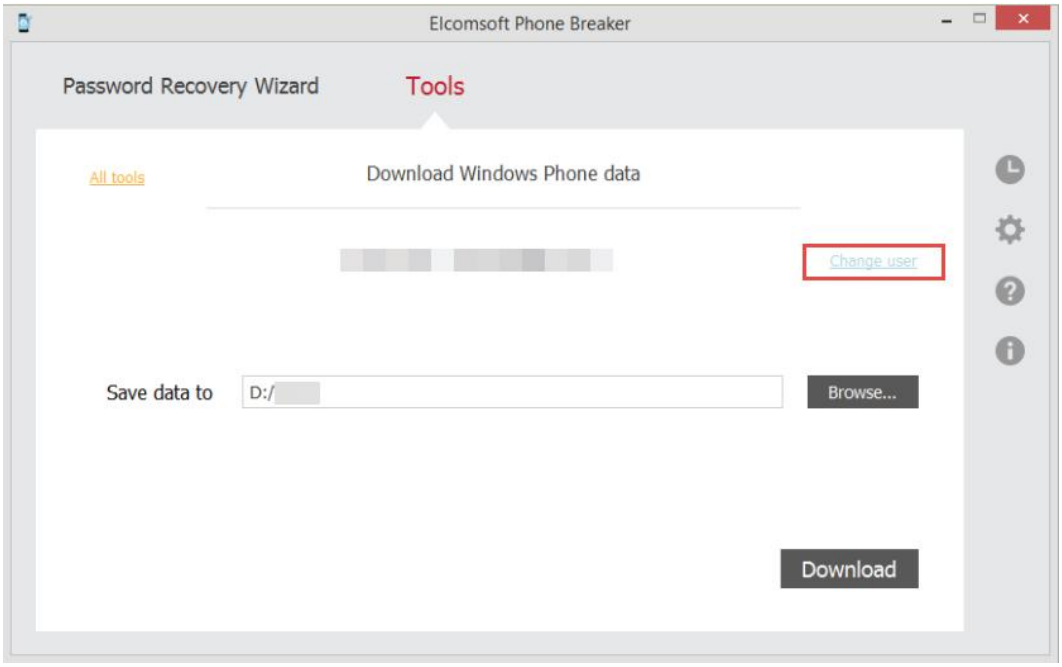
---

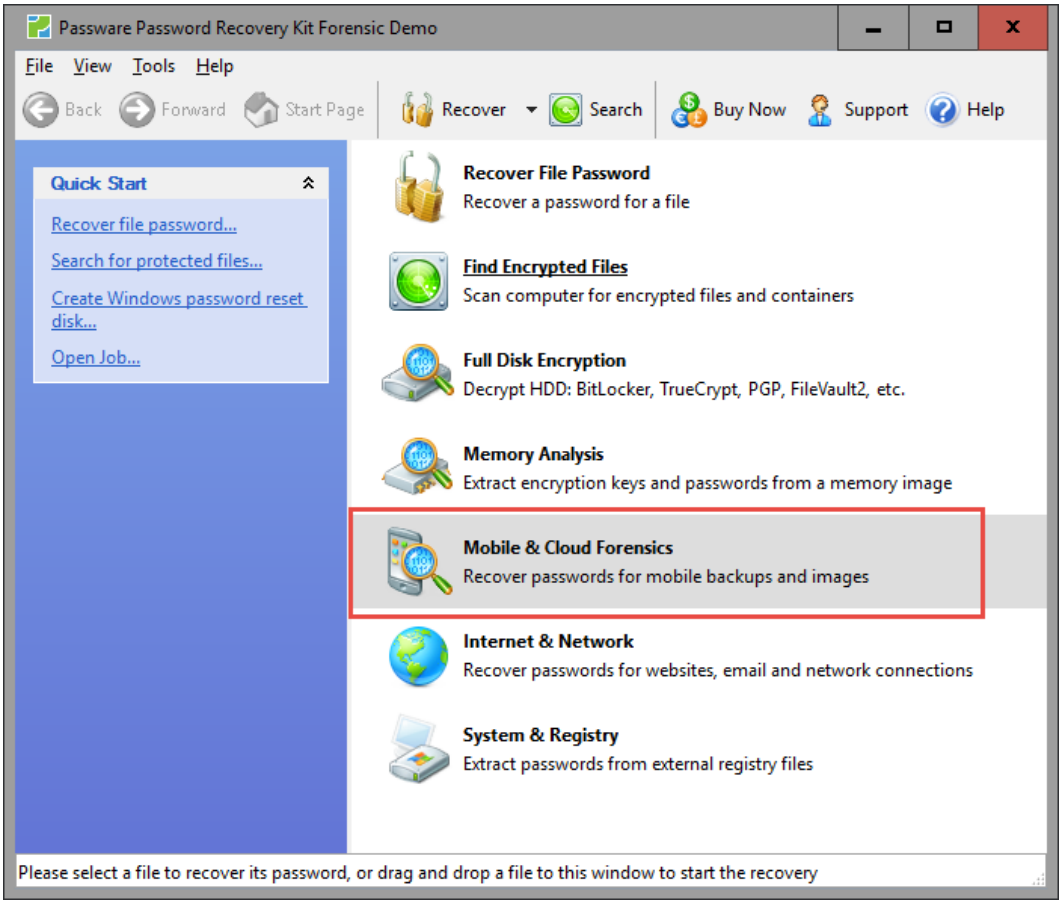
Acquisition details

Phone Timezone: (UTC) Casablanca
FriendlyName: Soufiane-Mobile
OS: WindowsPhone **Firmware Version:** 3051.50009.1451.1001
Hardware Version: 6.5.0.
Product Name: RM-821_apac_taiwan_341
Store Keeping Unit: NOKIA RM-821_apac_taiwan_341
Total Items Extracted: 840

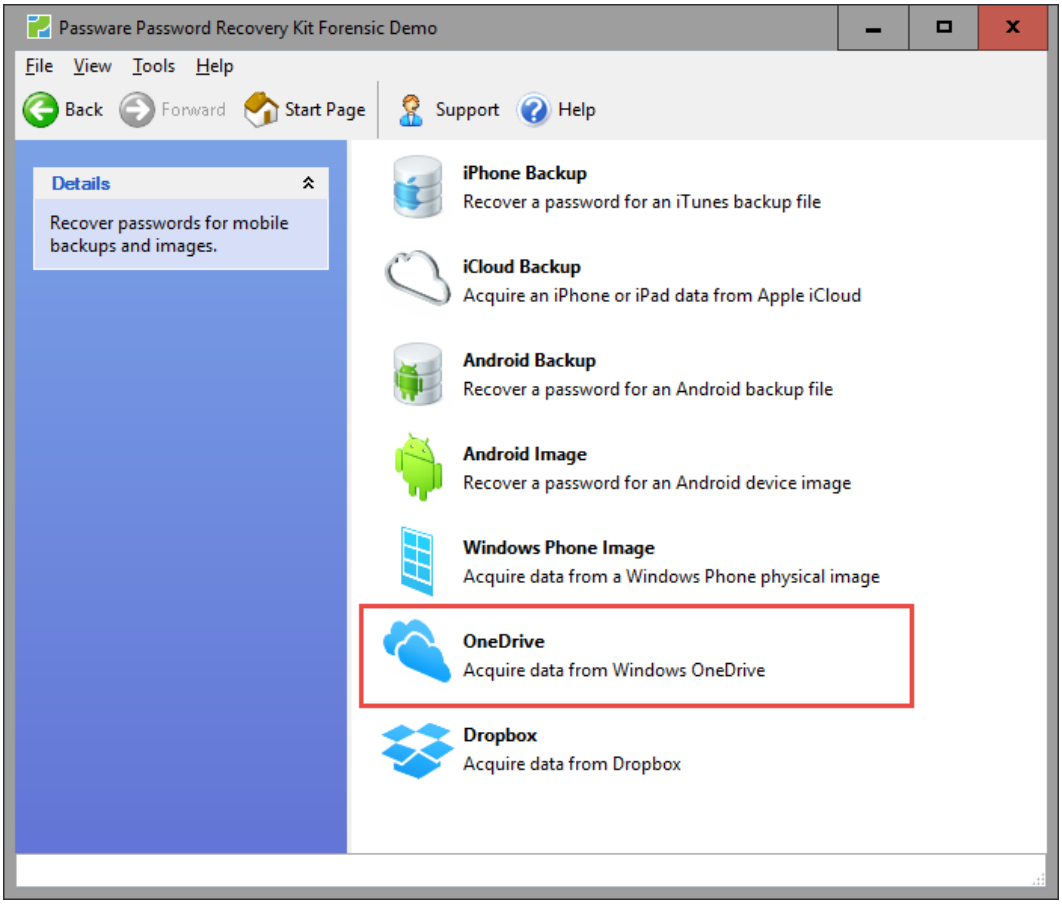

Elcomsoft Phone Breaker
Password Recovery Wizard
1
Tools
BlackBerry
Apple
Microsoft
2
Download Windows Phone data
Messages, Contacts and Notes
3

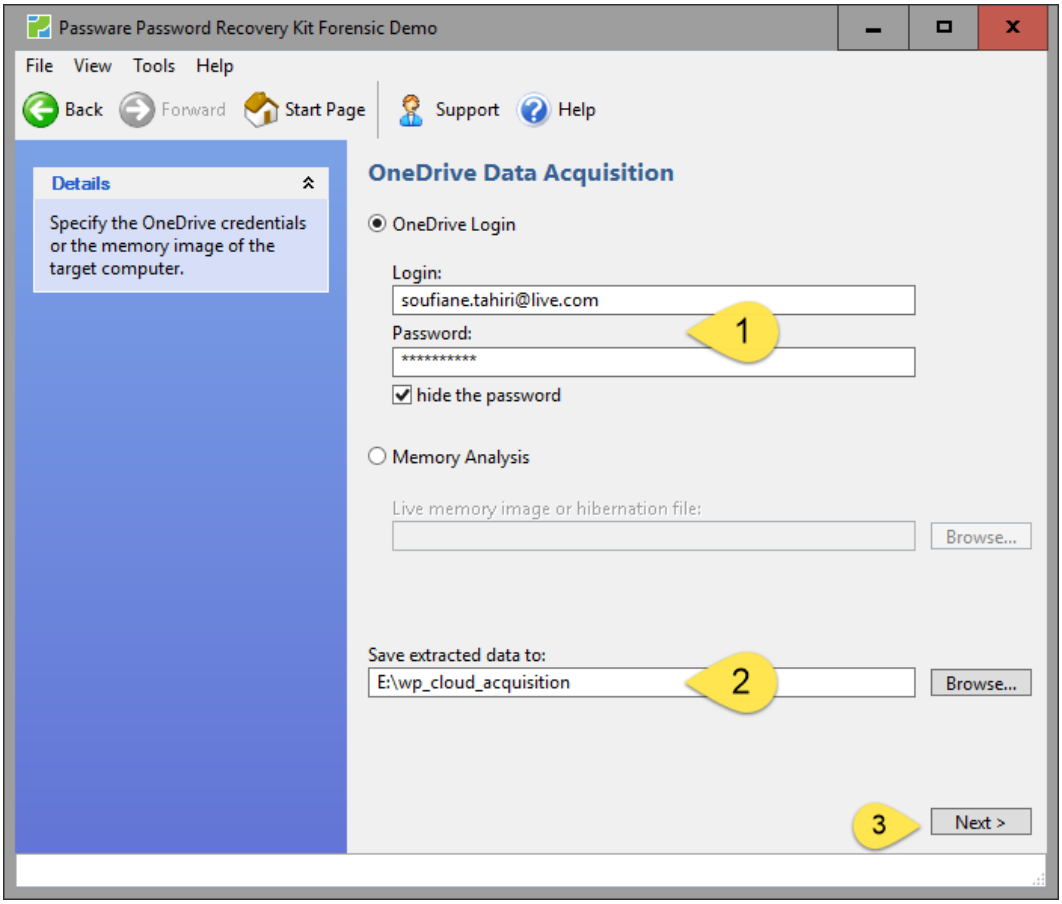

Elcomsoft Phone Breaker
Password Recovery Wizard
Tools
All tools
Download Windows Phone data
User name
soufiane.tahiri@live.com
(example@example.com)
Password
Sign in

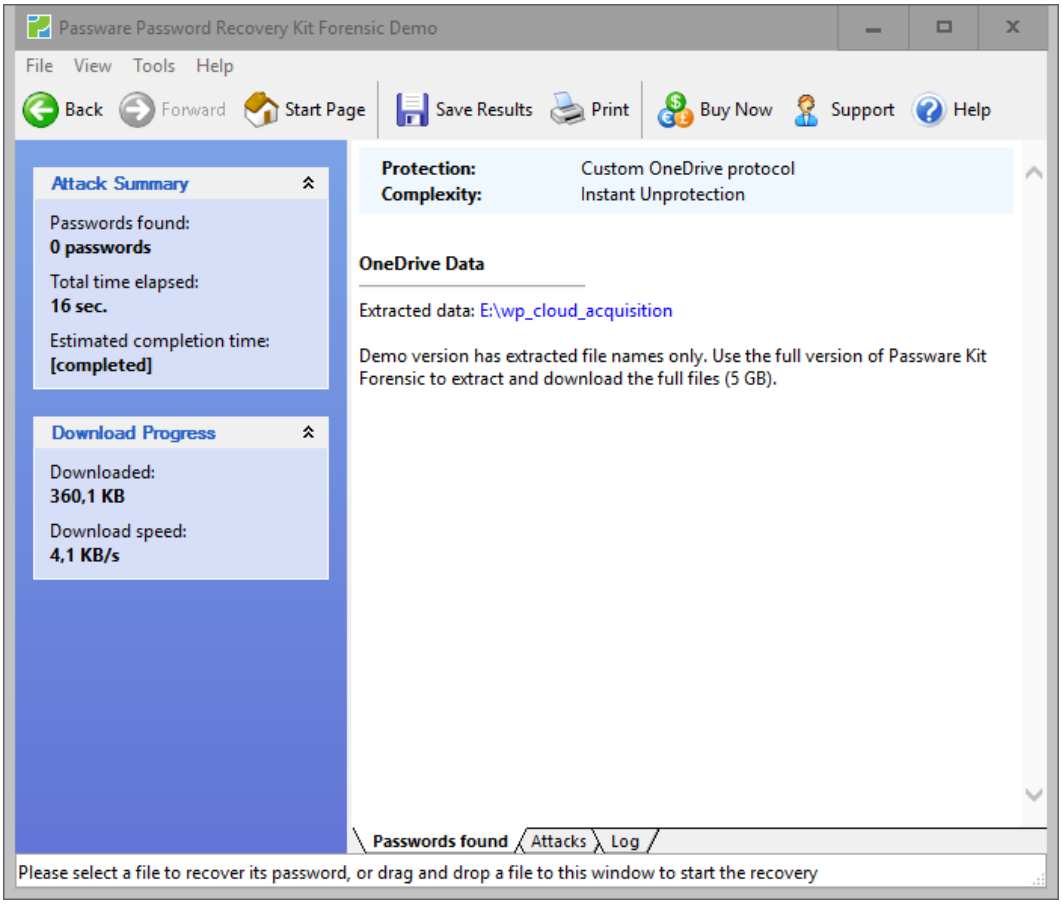

Elcomsoft Phone Breaker
Password Recovery Wizard
Tools
All tools
Download Windows Phone data
Change user
Save data to
D:/
Browse...
Download


Passware Password Recovery Kit Forensic Demo
File View Tools Help
Back Forward Start Page Recover Search Buy Now Support Help
Quick Start
Recover file password...
Search for protected files...
Create Windows password reset disk...
Open Job...
Recover File Password
Recover a password for a file
Find Encrypted Files
Scan computer for encrypted files and containers
Full Disk Encryption
Decrypt HDD: BitLocker, TrueCrypt, PGP, FileVault2, etc.
Memory Analysis
Extract encryption keys and passwords from a memory image
Mobile & Cloud Forensics
Recover passwords for mobile backups and images
Internet & Network
Recover passwords for websites, email and network connections
System & Registry
Extract passwords from external registry files
Please select a file to recover its password, or drag and drop a file to this window to start the recovery

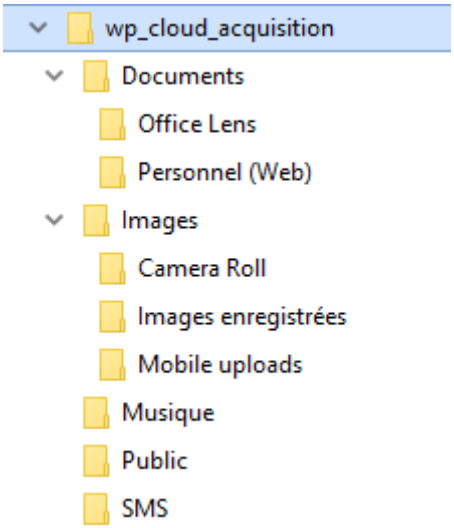
---

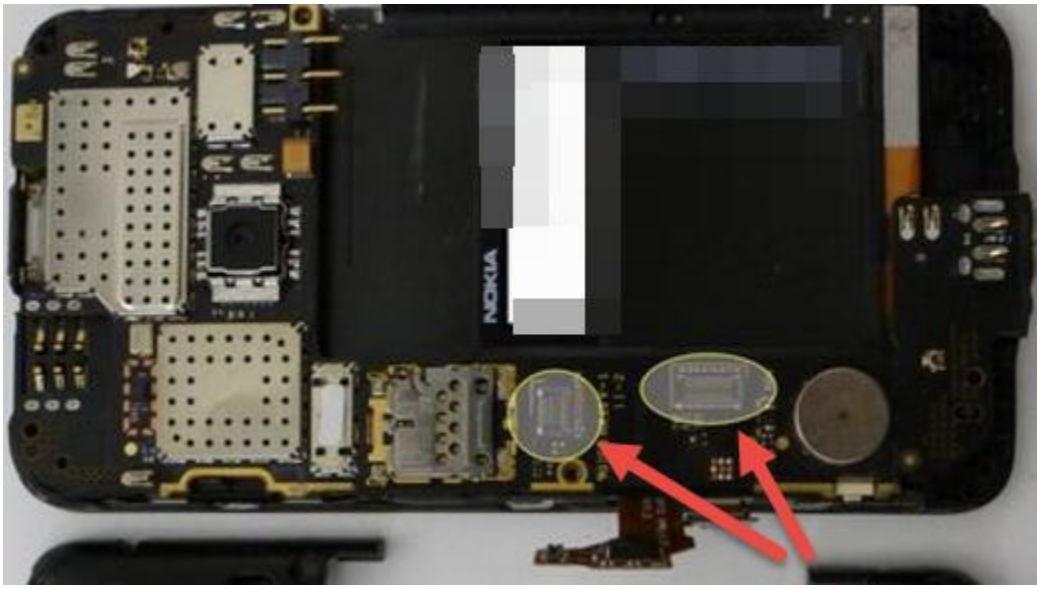

Passware Password Recovery Kit Forensic Demo
File View Tools Help
Back Forward Start Page Support Help
Details
Recover passwords for mobile backups and images.
iPhone Backup
Recover a password for an iTunes backup file
iCloud Backup
Acquire an iPhone or iPad data from Apple iCloud
Android Backup
Recover a password for an Android backup file
Android Image
Recover a password for an Android device image
Windows Phone Image
Acquire data from a Windows Phone physical image
OneDrive
Acquire data from Windows OneDrive
Dropbox
Acquire data from Dropbox

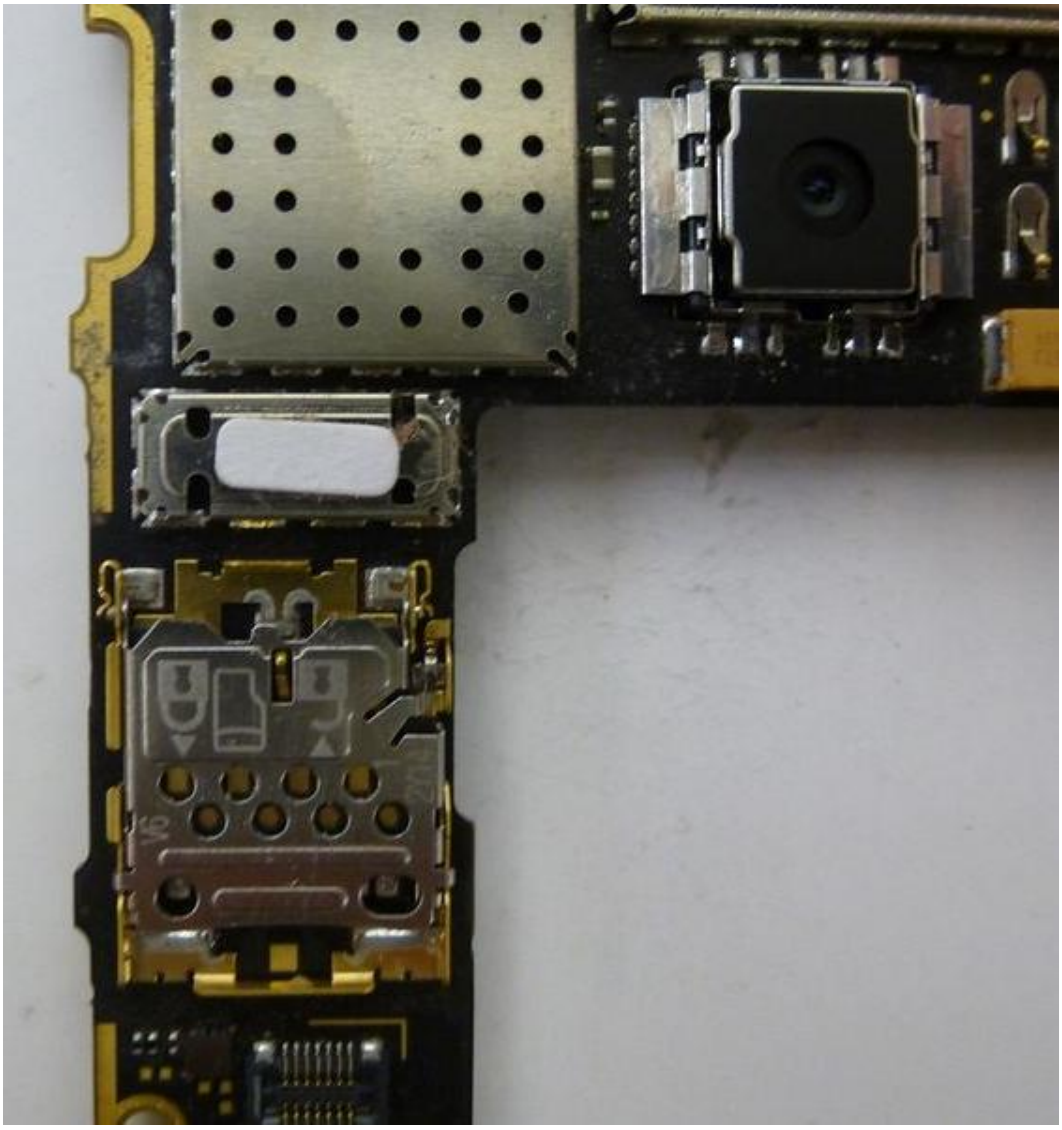

Passware Password Recovery Kit Forensic Demo
File View Tools Help
Back Forward Start Page Support Help
Details
Specify the OneDrive credentials or the memory image of the target computer.
OneDrive Data Acquisition
OneDrive Login
Login:
soufiane.tahiri@live.com
Password:
1
hide the password
Memory Analysis
Live memory image or hibernation file:
Browse...
Save extracted data to:
E:\wp_cloud_acquisition
2
Browse...
3
Next >

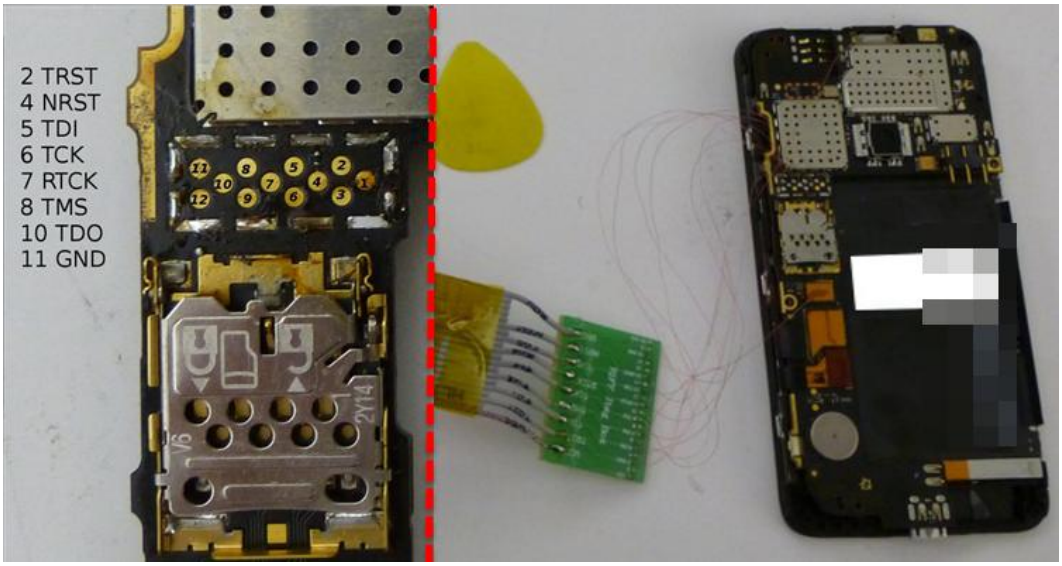

Passware Password Recovery Kit Forensic Demo
File View Tools Help
Back Forward Start Page Save Results Print Buy Now Support Help
Attack Summary
Passwords found:
0 passwords
Total time elapsed:
16 sec.
Estimated completion time:
[completed]
Download Progress
Downloaded:
360,1 KB
Download speed:
4,1 KB/s
Protection: Custom OneDrive protocol
Complexity: Instant Unprotection
OneDrive Data
Extracted data: E:\wp_cloud_acquisition
Demo version has extracted file names only. Use the full version of Passware Kit Forensic to extract and download the full files (5 GB).
Passwords found
Attacks
Log
Please select a file to recover its password, or drag and drop a file to this window to start the recovery

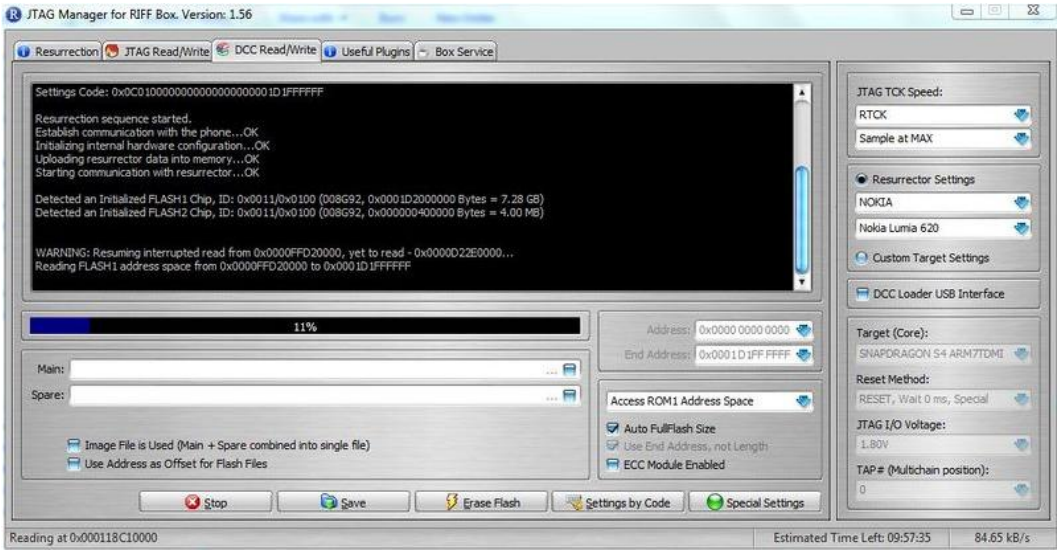
---

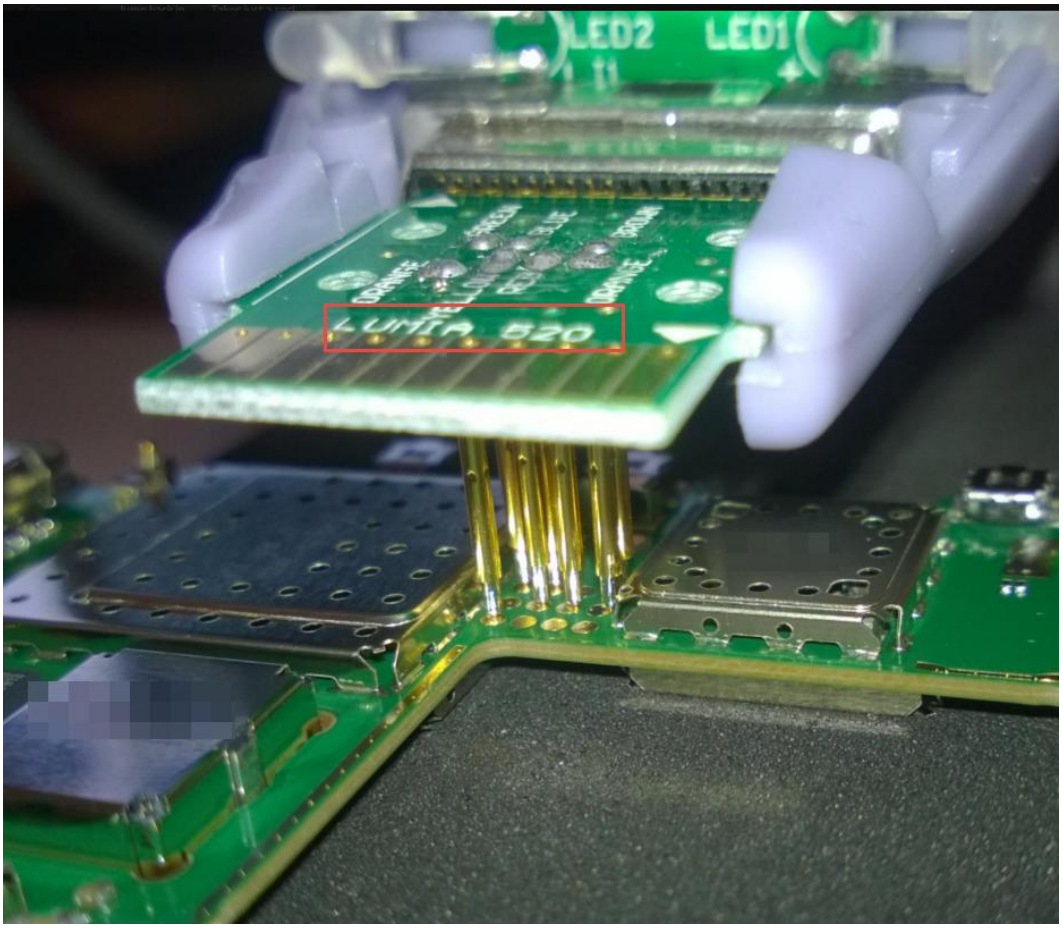

wp_cloud_acquisition
Documents
Office Lens
Personnel (Web)
Images
Camera Roll
Images enregistrées
Mobile uploads
Musique
Public
SMS

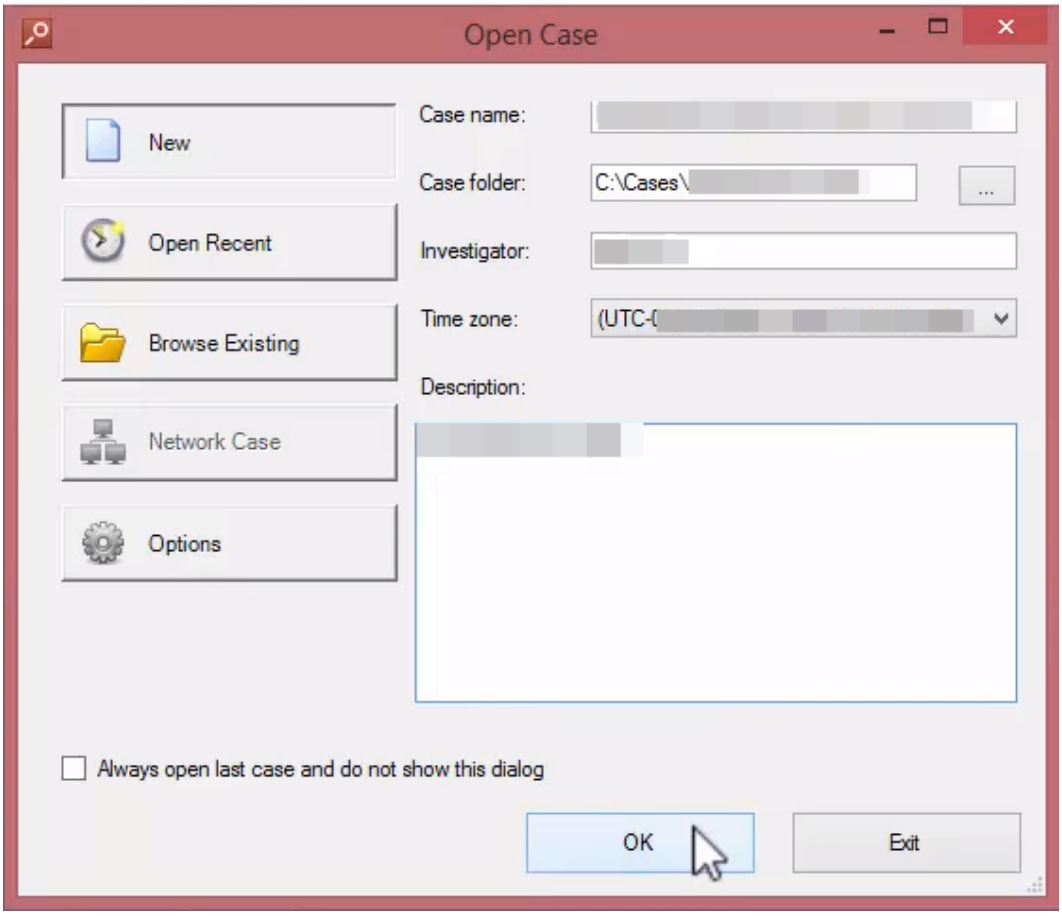

NOKIA

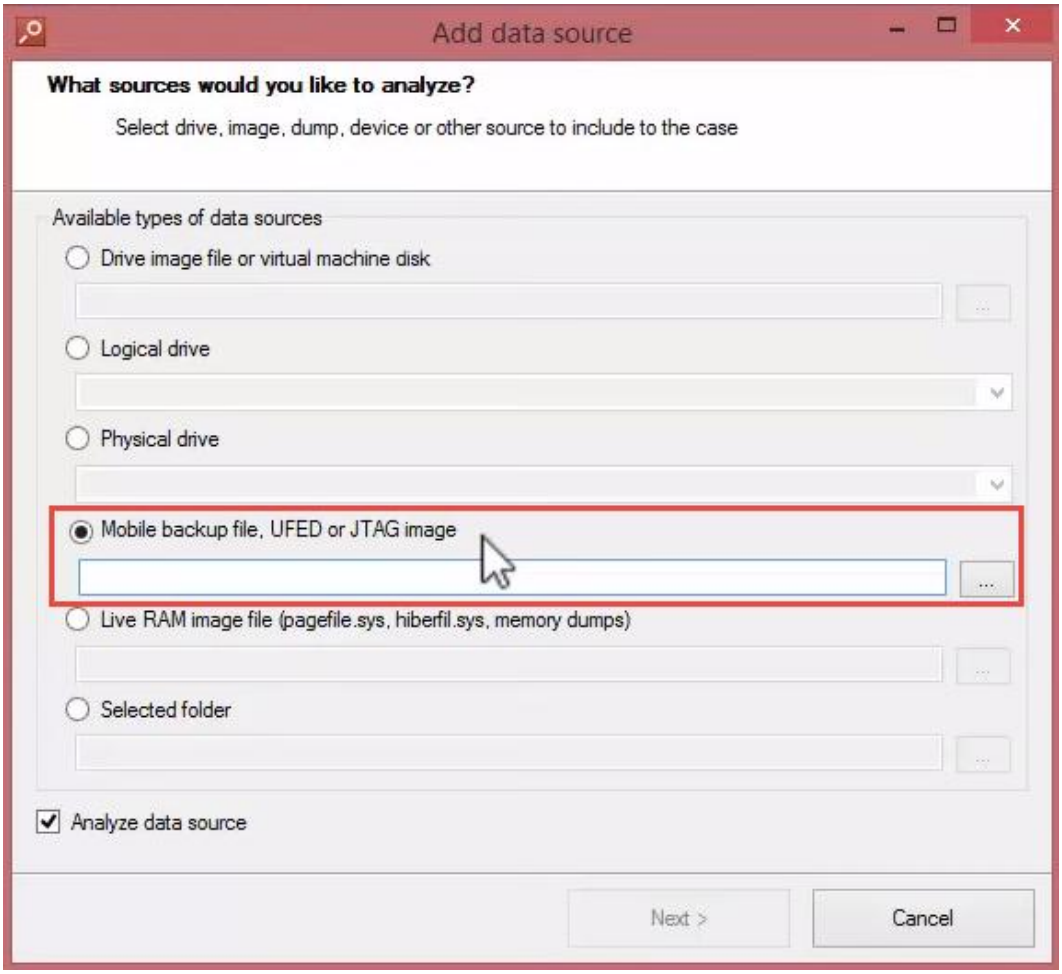


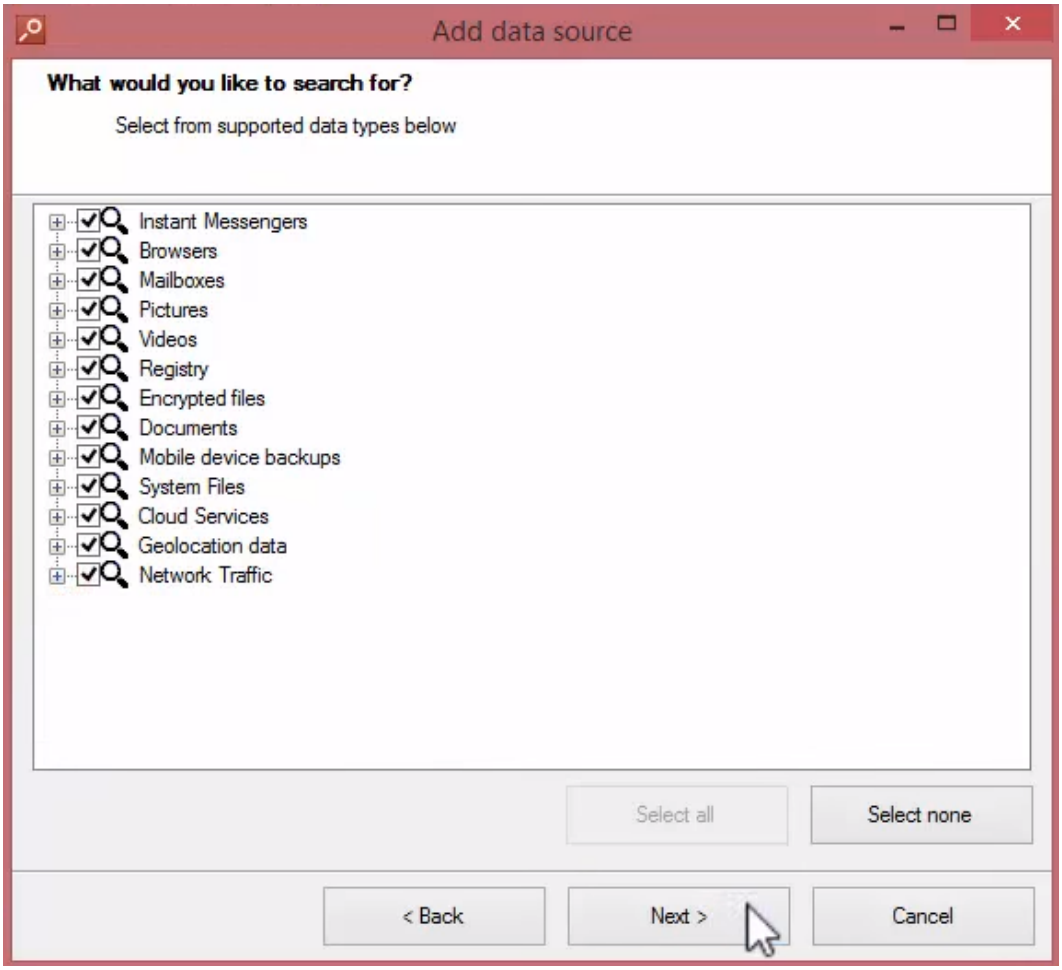

2 TRST
4 NRST
5 TDI
6 TCK
7 RTCK
8 TMS
10 TDO
11 GND

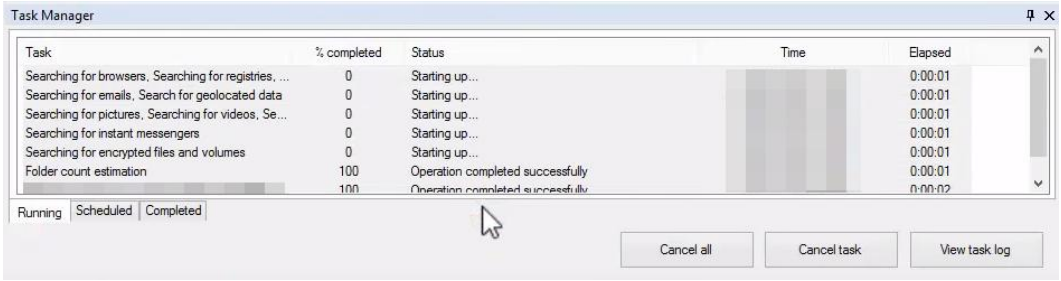

JTAG Manager for RIFF Box. Version: 1.56
Resurrection
JTAG Read/Write
DCC Read/Write
Useful Plugins
Box Service
Settings Code: 0x0C0100000000000000000001D1FFFFFF
Resurrection sequence started.
Establish communication with the phone...OK
Initializing internal hardware configuration...OK
Uploading resurrector data into memory...OK
Starting communication with resurrector...OK
Detected an Initialized FLASH1 Chip, ID: 0x0011/0x0100 (008G92, 0x0001D2000000 Bytes = 7.28 GB)
Detected an Initialized FLASH2 Chip, ID: 0x0011/0x0100 (008G92, 0x000000400000 Bytes = 4.00 MB)
WARNING: Resuming interrupted read from 0x0000FFD20000, yet to read - 0x0000D22E0000...
Reading FLASH1 address space from 0x0000FFD20000 to 0x0001D1FFFFFF
11%
Main:
Spare:
Image File is Used (Main + Spare combined into single file)
Use Address as Offset for Flash Files
Address: 0x0000 0000 0000
End Address: 0x0001D1FF FFFF
Access ROM1 Address Space
Auto FullFlash Size
Use End Address, not Length
ECC Module Enabled
Stop
Save
Erase Flash
Settings by Code
Special Settings
JTAG TCK Speed:
RTCK
Sample at MAX
Resurrector Settings
NOKIA
Nokia Lumia 620
Custom Target Settings
DCC Loader USB Interface
Target (Core):
SNAPDRAGON S4 ARM7TDMI
Reset Method:
RESET, Wait 0 ms, Special
JTAG I/O Voltage:
1.80V
TAP# (Multichain position):
0
Reading at 0x000118C10000
Estimated Time Left: 09:57:35
84.65 kB/s

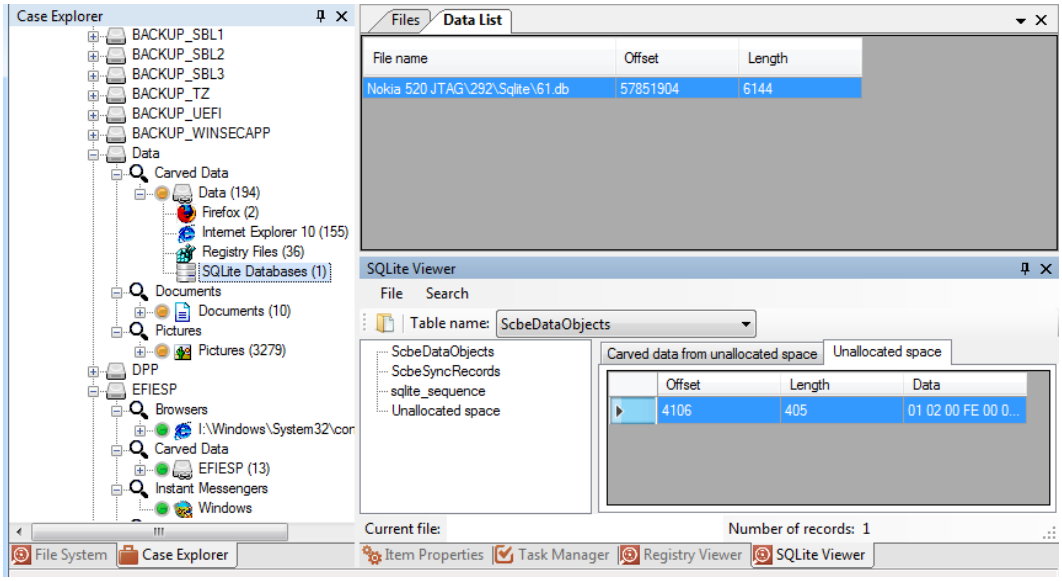

LED2
LED1
LUMIA 520

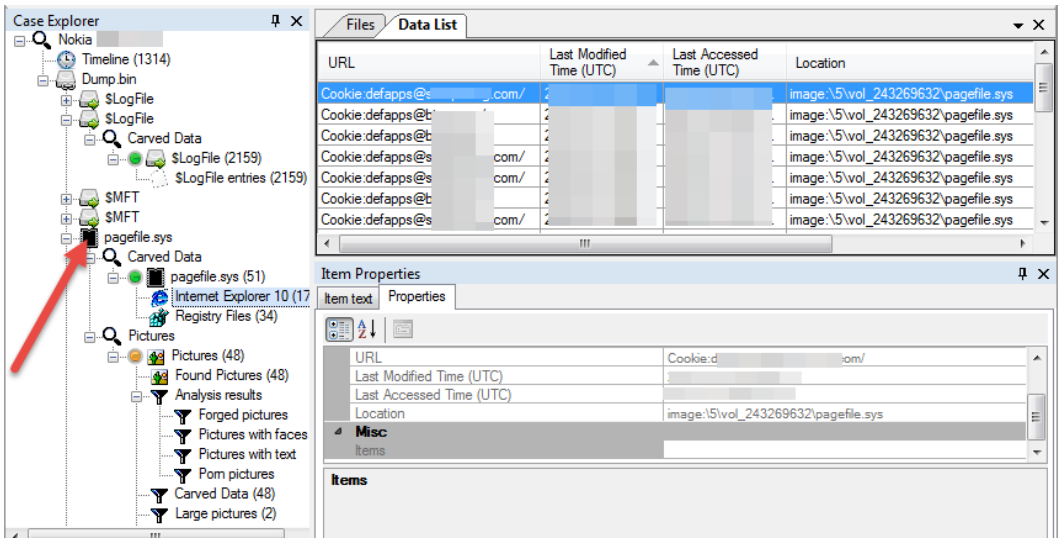

Open Case
New
Open Recent
Browse Existing
Network Case
Options
Case name:
Case folder:
C:\Cases\
...
Investigator:
Time zone:
(UTC-
Description:
Always open last case and do not show this dialog
OK
Exit

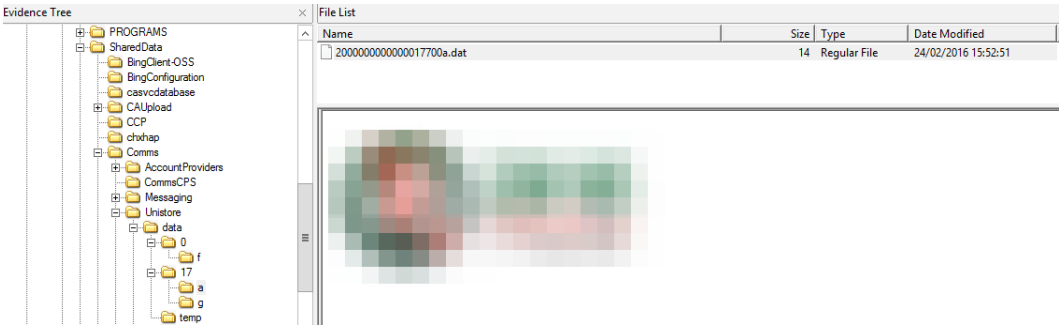

Add data source
What sources would you like to analyze?
Select drive, image, dump, device or other source to include to the case
Available types of data sources
Drive image file or virtual machine disk
Logical drive
Physical drive
Mobile backup file, UFED or JTAG image
Live RAM image file (pagefile.sys, hiberfil.sys, memory dumps)
Selected folder
Analyze data source
Next >
Cancel

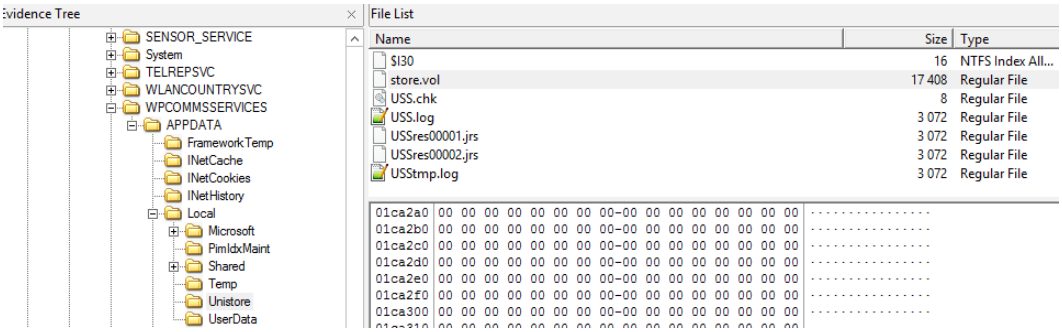

Add data source
What would you like to search for?
Select from supported data types below
Instant Messengers
Browsers
Mailboxes
Pictures
Videos
Registry
Encrypted files
Documents
Mobile device backups
System Files
Cloud Services
Geolocation data
Network Traffic
Select all
Select none
< Back
Next >
Cancel


Task Manager
Task
% completed
Status
Time
Elapsed
Searching for browsers, Searching for registries, ...
0
Starting up...
0:00:01
Searching for emails, Search for geolocated data
0
Starting up...
0:00:01
Searching for pictures, Searching for videos, Se...
0
Starting up...
0:00:01
Searching for instant messengers
0
Starting up...
0:00:01
Searching for encrypted files and volumes
0
Starting up...
0:00:01
Folder count estimation
100
Operation completed successfully
0:00:01
Running
Scheduled
Completed
Cancel all
Cancel task
View task log

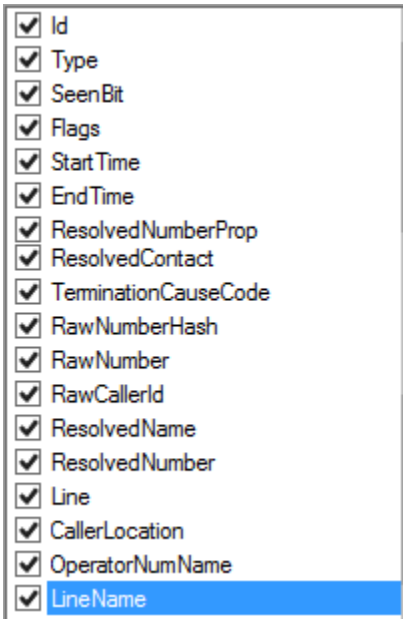

Case Explorer
BACKUP_SBL1
BACKUP_SBL2
BACKUP_SBL3
BACKUP_TZ
BACKUP_UEFI
BACKUP_WINSECAPP
Data
Carved Data
Data (194)
Firefox (2)
Internet Explorer 10 (155)
Registry Files (36)
SQLite Databases (1)
Documents
Documents (10)
Pictures
Pictures (3279)
DPP
EFIESP
Browsers
I:\Windows\System32\cor
Carved Data
EFIESP (13)
Instant Messengers
Windows
File System
Case Explorer
Files
Data List
File name
Offset
Length
Nokia 520 JTAG\292\Sqlite\61.db
57851904
6144
SQLite Viewer
File
Search
Table name:
ScbeDataObjects
ScbeDataObjects
ScbeSyncRecords
sqlite_sequence
Unallocated space
Carved data from unallocated space
Unallocated space
Offset
Length
Data
4106
405
01 02 00 FE 00 0...
Current file:
Number of records: 1
Item Properties
Task Manager
Registry Viewer
SQLite Viewer

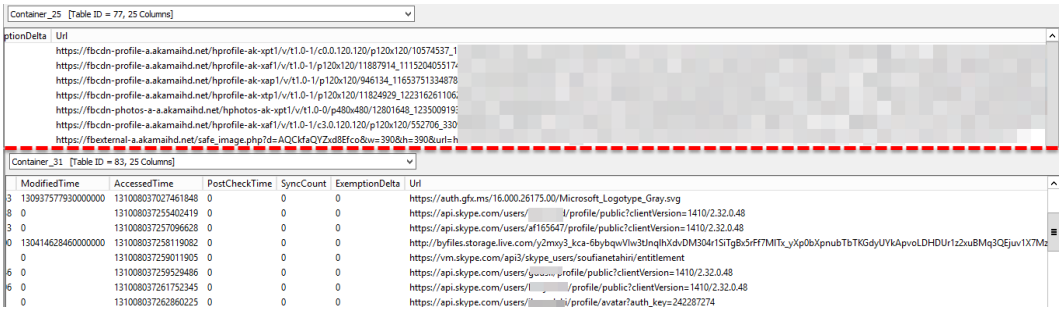

Case Explorer
Nokia
Timeline (1314)
Dump.bin
$LogFile
$LogFile
Carved Data
$LogFile (2159)
$LogFile entries (2159)
$MFT
$MFT
pagefile.sys
Carved Data
pagefile.sys (51)
Internet Explorer 10 (17
Registry Files (34)
Pictures
Pictures (48)
Found Pictures (48)
Analysis results
Forged pictures
Pictures with faces
Pictures with text
Porn pictures
Carved Data (48)
Large pictures (2)
Files
Data List
URL
Last Modified Time (UTC)
Last Accessed Time (UTC)
Location
image:\5\vol_243269632\pagefile.sys
Item Properties
Item text
Properties
URL
Last Modified Time (UTC)
Last Accessed Time (UTC)
Location
image:\5\vol_243269632\pagefile.sys
Misc
Items

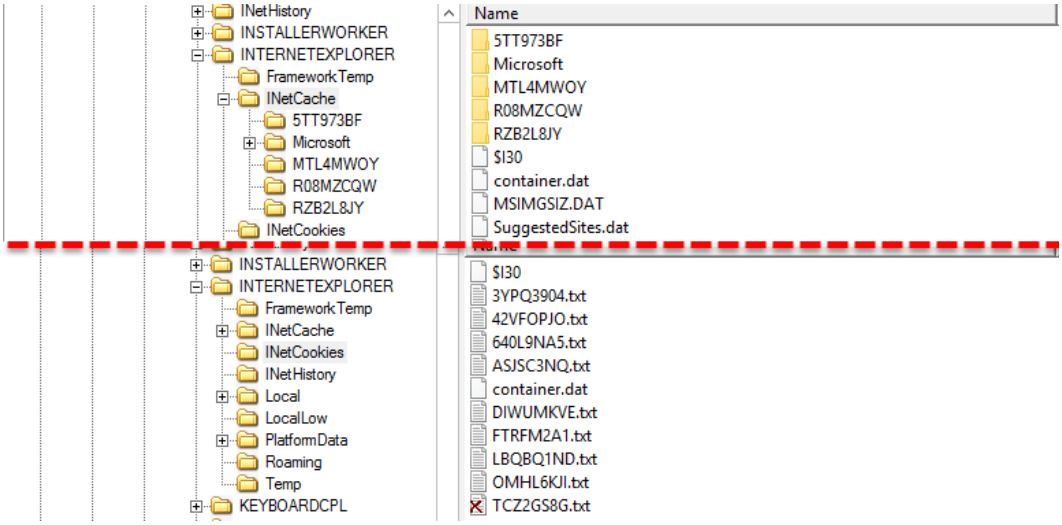


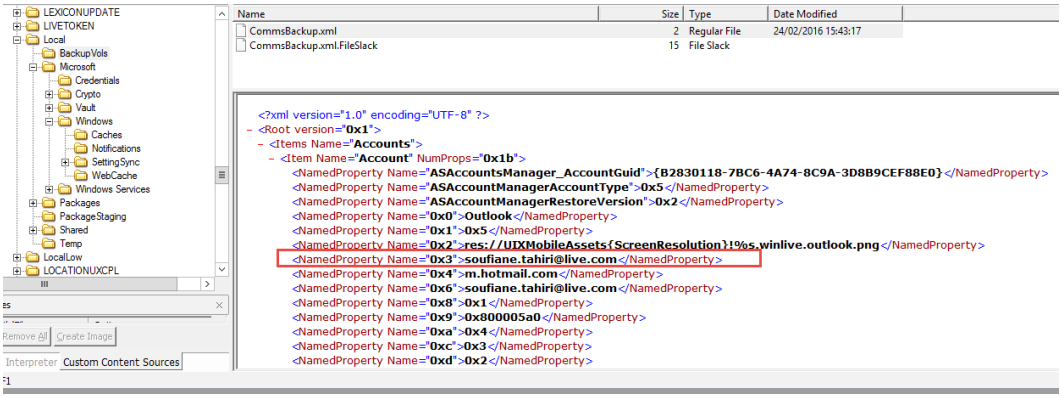


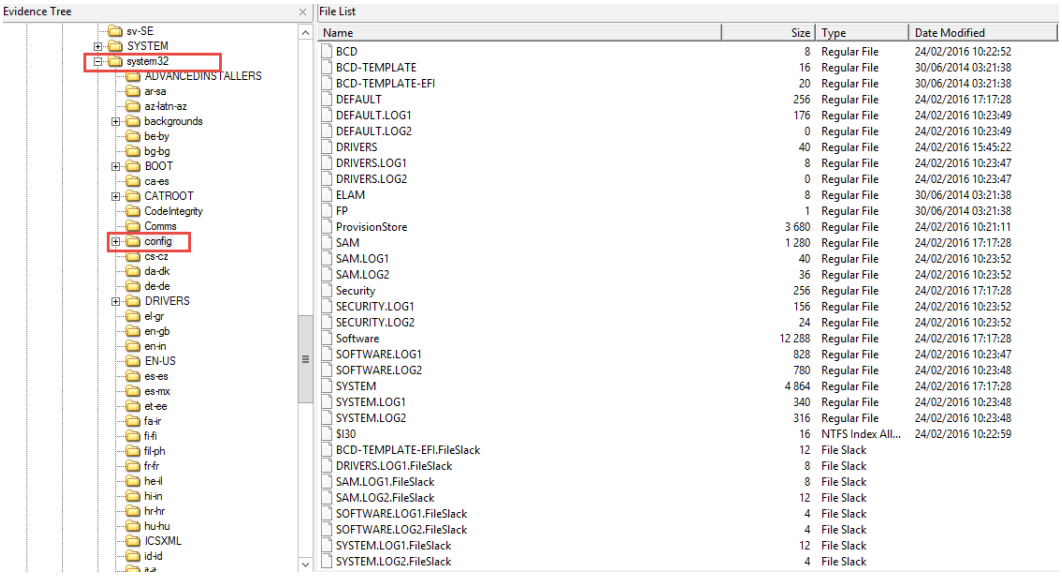
27/03/...	Reuters Top News	https://t.co/kW7XQcj1yk
Twitter	WikiLeaks	https://t.co/eWYhEhKnlp
Twitter	RT	https://t.co/dLJ3V7zQin
Twitter	SANS Institute, EMEA	https://t.co/3kk1xPF5wl
Twitter	RT	https://t.co/ky0orjDeuI
Twitter	WikiLeaks	https://t.co/eWYhEhKnlp
Twitter	Virus Bulletin	https://t.co/JFymH2EHWr
Twitter	Morgan Marquis-Boire	https://t.co/x9gFQiq27l
Twitter	WikiLeaks	https://t.co/eWYhEhKnlp
Twitter	RT	https://t.co/wojSe5FJim
LinkedIn	Ashish	http://image-store.slidesharecdn.
LinkedIn	William	7f-4ff8-9bb5-eb1a04ca0950-original.jpeg
LinkedIn	Remo	
LinkedIn	Remc	http://flip
LinkedIn	Soufiane Tahiri	https://www.linkedin.com/pulse/digital-forensics-models-1-soufiane-tahiri
LinkedIn	Shahriar	http://buff.ly/1pb3MHt
LinkedIn	Shahriar	http://buff.ly/1pb3MHt

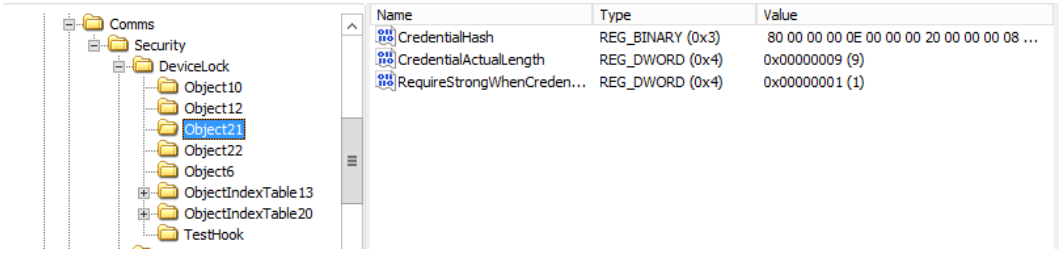

Id
Type
SeenBit
Flags
StartTime
EndTime
ResolvedNumberProp
ResolvedContact
TerminationCauseCode
RawNumberHash
RawNumber
RawCallerId
ResolvedName
ResolvedNumber
Line
CallerLocation
OperatorNumName
LineName


Container_25 [Table ID = 77, 25 Columns]
ptionDelta
Url
https://fbcdn-profile-a.akamaihd.net/hprofile-ak-xpt1/v/t1.0-1/c0.0.120.120/p120x120/10574537_1
https://fbcdn-profile-a.akamaihd.net/hprofile-ak-xaf1/v/t1.0-1/p120x120/11887914_111520405517
https://fbcdn-profile-a.akamaihd.net/hprofile-ak-xap1/v/t1.0-1/p120x120/946134_11653751334878
https://fbcdn-profile-a.akamaihd.net/hprofile-ak-xtp1/v/t1.0-1/p120x120/11824929_122316261106
https://fbcdn-photos-a-a.akamaihd.net/hphotos-ak-xpt1/v/t1.0-0/p480x480/12801648_123500919
https://fbcdn-profile-a.akamaihd.net/hprofile-ak-xaf1/v/t1.0-1/c3.0.120.120/p120x120/552706_330
https://fbexternal-a.akamaihd.net/safe_image.php?d=AQCkfaQYZxd8Efco&w=390&h=390&url=h
Container_31 [Table ID = 83, 25 Columns]
ModifiedTime
AccessedTime
PostCheckTime
SyncCount
ExemptionDelta
Url
3 130937577930000000 131008037027461848 0 0 0 https://auth.gfx.ms/16.000.26175.00/Microsoft_Logotype_Gray.svg
8 0 131008037255402419 0 0 0 https://api.skype.com/users/[redacted]/profile/public?clientVersion=1410/2.32.0.48
3 0 131008037257096628 0 0 0 https://api.skype.com/users/af165647/profile/public?clientVersion=1410/2.32.0.48
0 130414628460000000 131008037258119082 0 0 0 http://byfiles.storage.live.com/y2mxy3_kca-6bybqwVlw3tInqlhXdvDM304r1SiTgBx5rF7MITx_yXp0bXpnubTbTKGdyUYkApvoLDHDUr1z2xuBMq3QEjuv1X7Mz
0 131008037259011905 0 0 0 https://vm.skype.com/api3/skype_users/soufianetahiri/entitlement
6 0 131008037259529486 0 0 0 https://api.skype.com/users/[redacted]profile/public?clientVersion=1410/2.32.0.48
6 0 131008037261752345 0 0 0 https://api.skype.com/users/[redacted]/profile/public?clientVersion=1410/2.32.0.48
0 131008037262860225 0 0 0 https://api.skype.com/users/[redacted]/profile/avatar?auth_key=242287274

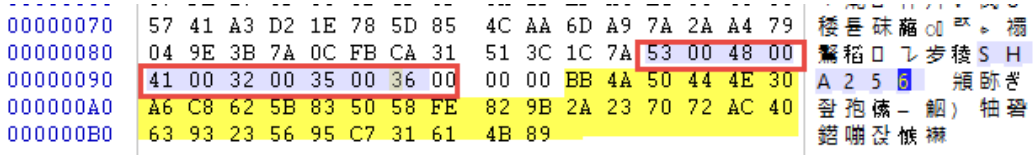

INetHistory
INSTALLERWORKER
INTERNETEXPLORER
FrameworkTemp
INetCache
5TT973BF
Microsoft
MTL4MWOY
R08MZCQW
RZB2L8JY
INetCookies
Name
5TT973BF
Microsoft
MTL4MWOY
R08MZCQW
RZB2L8JY
$I30
container.dat
MSIMGSIZ.DAT
SuggestedSites.dat
INSTALLERWORKER
INTERNETEXPLORER
FrameworkTemp
INetCache
INetCookies
INetHistory
Local
LocalLow
PlatformData
Roaming
Temp
KEYBOARDCPL
$I30
3YPQ3904.txt
42VFOPJO.txt
640L9NA5.txt
ASJSC3NQ.txt
container.dat
DIWUMKVE.txt
FTRFM2A1.txt
LBQBQ1ND.txt
OMHL6KJI.txt
TCZ2GS8G.txt


LEXICONUPDATE
LIVETOKEN
Local
BackupVols
Microsoft
Credentials
Crypto
Vault
Windows
Caches
Notifications
SettingSync
WebCache
Windows Services
Packages
PackageStaging
Shared
Temp
LocalLow
LOCATIONUXCPL
Remove All
Create Image
Interpreter
Custom Content Sources
Name
Size
Type
Date Modified
CommsBackup.xml
2
Regular File
24/02/2016 15:43:17
CommsBackup.xml.FileSlack
15
File Slack
<?xml version="1.0" encoding="UTF-8" ?>
<Root version="0x1">
<Items Name="Accounts">
<Item Name="Account" NumProps="0x1b">
<NamedProperty Name="ASAccountsManager_AccountGuid">{B2830118-7BC6-4A74-8C9A-3D8B9CEF88E0}</NamedProperty>
<NamedProperty Name="ASAccountManagerAccountType">0x5</NamedProperty>
<NamedProperty Name="ASAccountManagerRestoreVersion">0x2</NamedProperty>
<NamedProperty Name="0x0">Outlook</NamedProperty>
<NamedProperty Name="0x1">0x5</NamedProperty>
<NamedProperty Name="0x2">res://UIXMobileAssets{ScreenResolution}!%s.winlive.outlook.png</NamedProperty>
<NamedProperty Name="0x3">soufiane.tahiri@live.com</NamedProperty>
<NamedProperty Name="0x4">m.hotmail.com</NamedProperty>
<NamedProperty Name="0x6">soufiane.tahiri@live.com</NamedProperty>
<NamedProperty Name="0x8">0x1</NamedProperty>
<NamedProperty Name="0x9">0x800005a0</NamedProperty>
<NamedProperty Name="0xa">0x4</NamedProperty>
<NamedProperty Name="0xc">0x3</NamedProperty>
<NamedProperty Name="0xd">0x2</NamedProperty>





Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	80	00	00	00	0E	00	00	00	20	00	00	00	08	29	F2	52	▌)òR
00000010	17	A3	87	34	45	B6	5D	4F	14	69	2E	4C	BC	2C	CC	AF	£▌4E¶]O i.L¼,Ì¯
00000020	36	85	9D	C4	2E	DD	6A	D8	6A	98	2E	79	93	DD	CA	A3	6▌ Ä.ÝjØj▌.y▌ÝÊ£
00000030	8D	D1	9F	8C	80	D4	8D	03	16	EE	A2	34	57	03	22	D5	▌Ñ▌▌▌Ô i¢4W "Õ
00000040	D0	B1	BD	9D	6F	8C	BC	5E	EB	14	85	8B	5E	68	88	DF	Ð±½ o▌¼^ë ▌▌^h▌ß
00000050	D4	DE	33	97	25	91	9D	75	89	E1	50	F3	8B	87	69	57	ÔÞ3▌%' u▌áPó▌▌iW
00000060	57	FE	27	6F	00	0D	CF	5F	5A	2F	EF	A4	EC	80	46	05	Wþ'o ▌Ï_Z/ï¤ì▌F
00000070	57	41	A3	D2	1E	78	5D	85	4C	AA	6D	A9	7A	2A	A4	79	WA£Ò x]▌Lªm©z*¤y
00000080	04	9E	3B	7A	0C	FB	CA	31	51	3C	1C	7A	53	00	48	00	▌;z ûÊ1Q< zS H
00000090	41	00	32	00	35	00	36	00	00	00	BB	4A	50	44	4E	30	A 2 5 6 »JPDN0
000000A0	A6	C8	62	5B	83	50	58	FE	82	9B	2A	23	70	72	AC	40	¦Èb[▌PXþ▌▌*#pr¬@
000000B0	63	93	23	56	95	C7	31	61	4B	89							c▌#V▌Ç1aK▌



```
00000070  57 41 A3 D2 1E 78 5D 85  4C AA 6D A9 7A 2A A4 79
00000080  04 9E 3B 7A 0C FB CA 31  51 3C 1C 7A 53 00 48 00
00000090  41 00 32 00 35 00 36 00  00 00 BB 4A 50 44 4E 30
000000A0  A6 C8 62 5B 83 50 58 FE  82 9B 2A 23 70 72 AC 40
000000B0  63 93 23 56 95 C7 31 61  4B 89
```

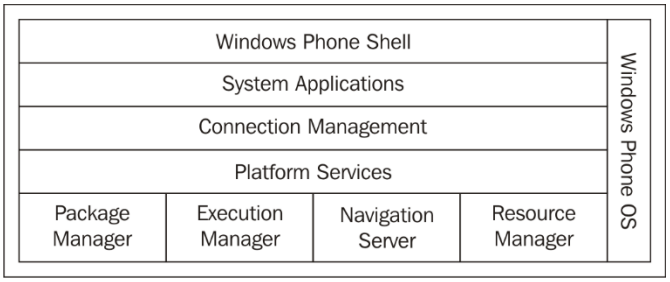
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	80	00	00	00	0E	00	00	00	20	00	00	00	08	29	F2	52
00000010	17	A3	87	34	45	B6	5D	4F	14	69	2E	4C	BC	2C	CC	AF
00000020	36	85	9D	C4	2E	DD	6A	D8	6A	98	2E	79	93	DD	CA	A3
00000030	8D	D1	9F	8C	80	D4	8D	03	16	EE	A2	34	57	03	22	D5
00000040	D0	B1	BD	9D	6F	8C	BC	5E	EB	14	85	8B	5E	68	88	DF
00000050	D4	DE	33	97	25	91	9D	75	89	E1	50	F3	8B	87	69	57
00000060	57	FE	27	6F	00	0D	CF	5F	5A	2F	EF	A4	EC	80	46	05
00000070	57	41	A3	D2	1E	78	5D	85	4C	AA	6D	A9	7A	2A	A4	79
00000080	04	9E	3B	7A	0C	FB	CA	31	51	3C	1C	7A	53	00	48	00
00000090	41	00	32	00	35	00	36	00	00	00	BB	4A	50	44	4E	30
000000A0	A6	C8	62	5B	83	50	58	FE	82	9B	2A	23	70	72	AC	40
000000B0	63	93	23	56	95	C7	31	61	4B	89						

```
C:\Users\Soufiane>python c:\wp8-pin.py 0829F25217A3873445B65D4F14692E4CBC2CCCAF36859DC42EDD6AD86A982E7993DDCAA38DD
19F8C80D48D0316EEA234570322D5D0B1BD9D6F8CBC5EEB14858B5E6888DFD4DE339725919D7589E150F38B87695757FE276F000DCF5F5A2FE
FA4EC8046055741A3D21E785D854CAA6DA97A2AA479049E3B7A0CFBCA31513C1C7A BB4A50444E30A6C8625B835058FE829B2A237072AC4063
93235695C731614B89 9

Running wp8-sha256-pin-finder.py v2015-07-30

PIN code is 662135560

C:\Users\Soufiane>
```

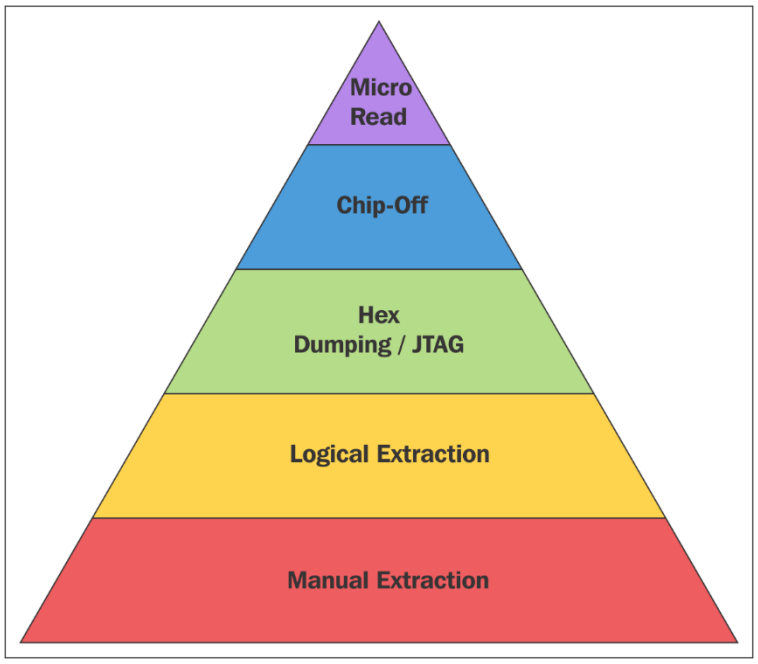
Name	Type	Value
VUFailureCount	REG_DWORD (0x4)	0x00000000 (0)
AuthResetFailureCount	REG_DWORD (0x4)	0x00000000 (0)
ActiveLAPGUID	REG_BINARY (0x3)	B5 A5 B5 A7 35 56 41 42 A7 FD 27 2E 0C 1F EA A6
CurrentCredentialHash	REG_BINARY (0x3)	80 00 00 00 0E 00 00 00 20 00 00 00 23 C8 16 EF 9A 74 9
CredentialSetupTime	REG_BINARY (0x3)	D0 2C 74 0C 1D 6F D1 01

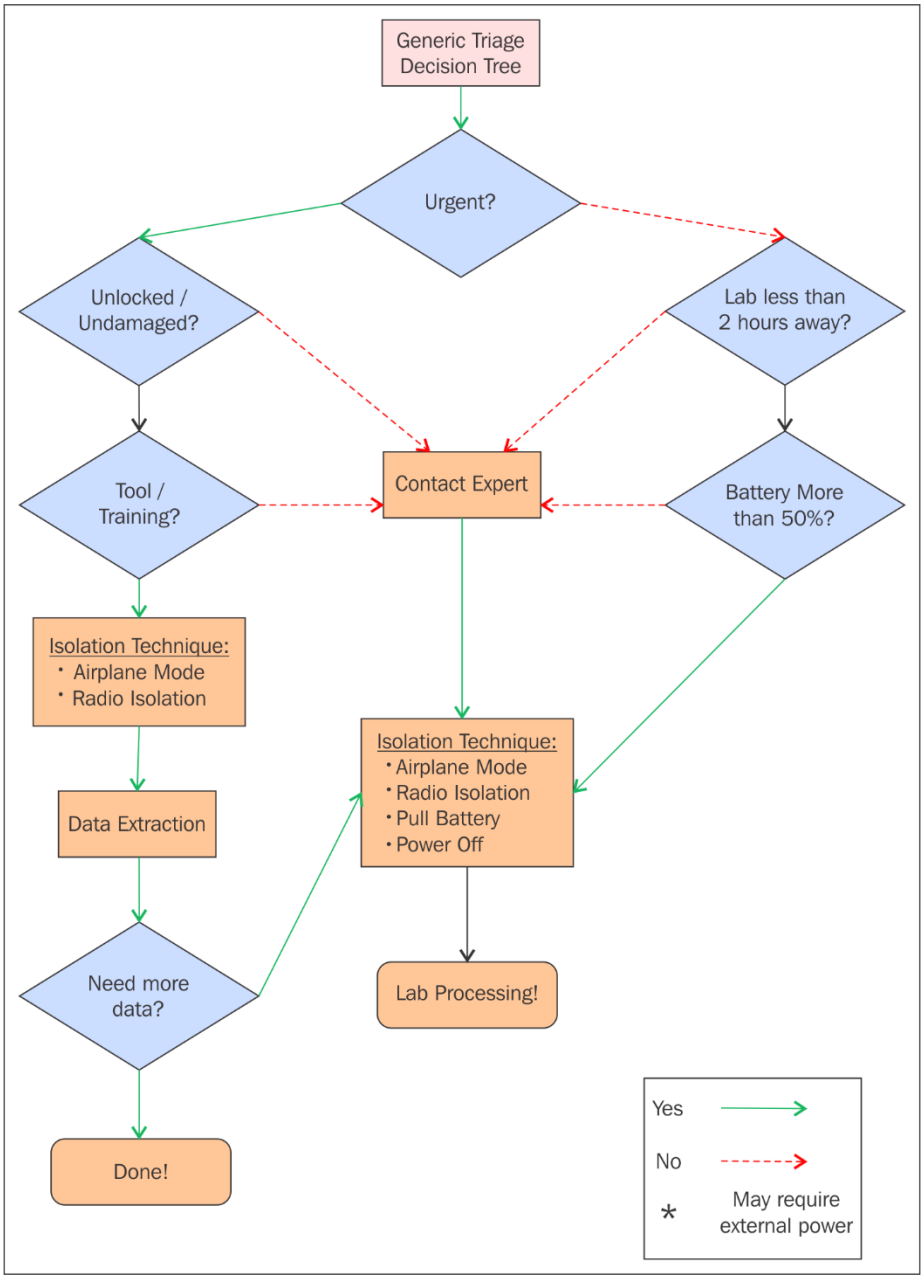
1D1 6F1D 0C74 2CD0

HEX	1D1 6F1D 0C74 2CD0
DEC	131 008 034 724 130 000
OCT	7 213 361 641 435 026 320
BIN	0001 1101 0001 0110 1111 0001 1101 0000 1100 0111 0100 0010 1100 1101 0000



Chapter 6: Mobile Forensics – Best Practices




Generic Triage Decision Tree
Urgent?
Unlocked / Undamaged?
Lab less than 2 hours away?
Tool / Training?
Contact Expert
Battery More than 50%?
Isolation Technique:
• Airplane Mode
• Radio Isolation
Data Extraction
Need more data?
Done!
Isolation Technique:
• Airplane Mode
• Radio Isolation
• Pull Battery
• Power Off
Lab Processing!
Yes
No
* May require external power

Removable Media Worksheet

Case Number: _____ **Exhibit Number:** _____

Laboratory Number: _____ **Control Number:** _____

Media Type / Quantity

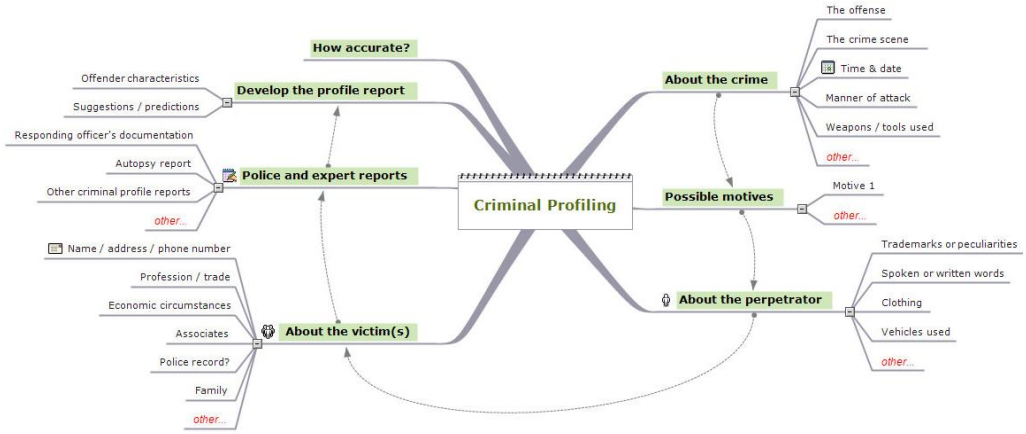
Diskette [ ]	**LS-120 [ ]**	**100 MB Zip [ ]**	**250 MB Zip [ ]**
1 GB Jaz [ ]	**2 GB Jaz [ ]**	**Magneto-Optical [ ]**	**Tape [ ]**
CD [ ]	**DVD [ ]**	**Other [ ]**	

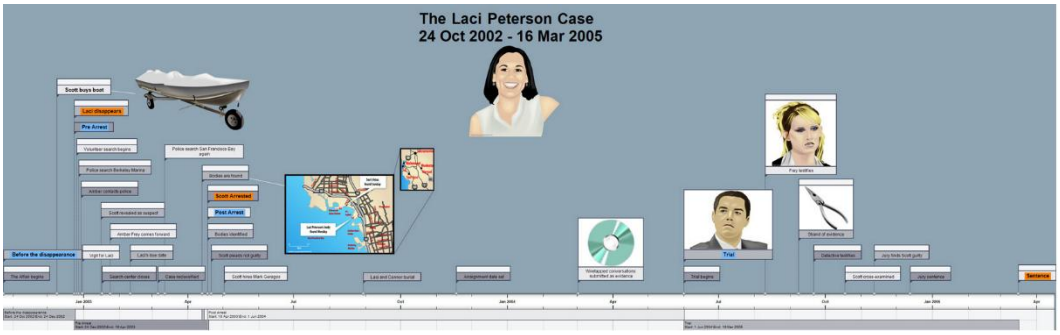
Examination

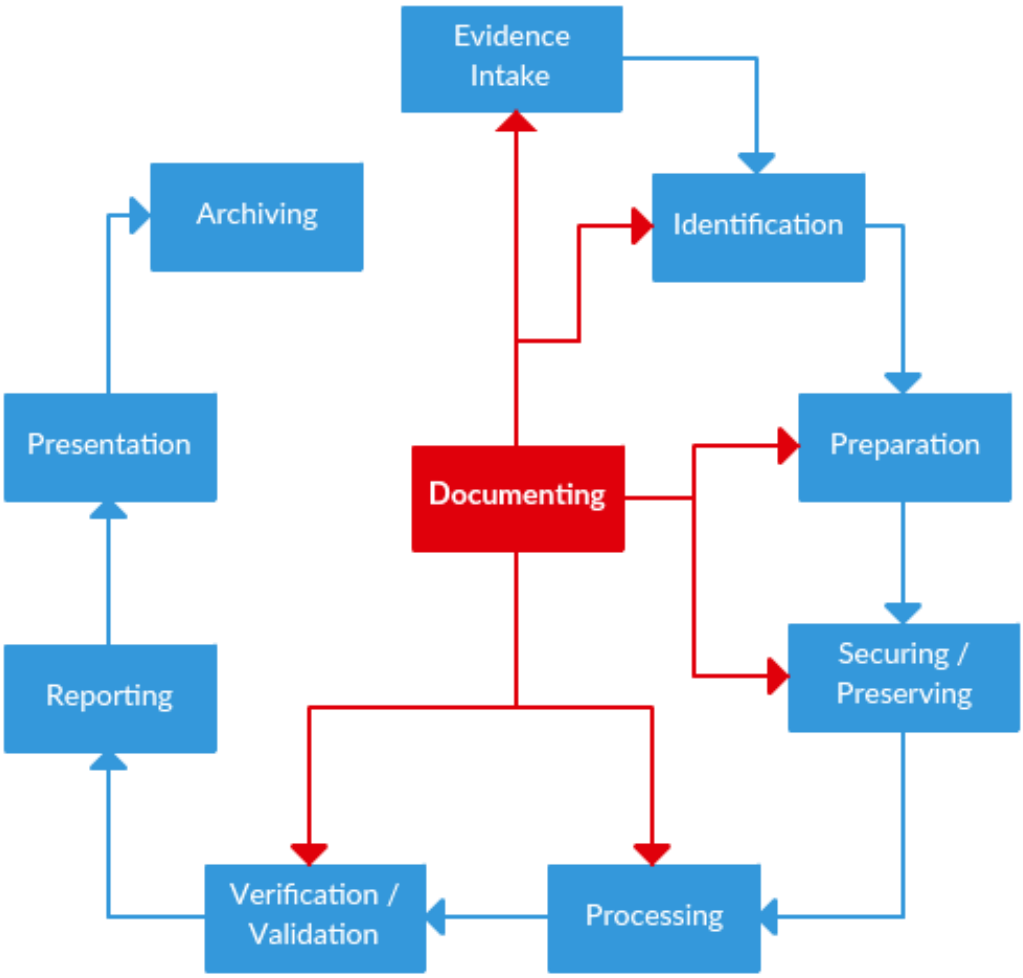
Exhibit # Sub-Exhibit #	Triage	Duplicated	Browse	Unerase	Keyword Search
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

_____ _____ _____ _____

Examiner **Date** **Supervisor Review** **Date**


Criminal Profiling
How accurate?
Develop the profile report
Offender characteristics
Suggestions / predictions
Police and expert reports
Responding officer's documentation
Autopsy report
Other criminal profile reports
other...
About the victim(s)
Name / address / phone number
Profession / trade
Economic circumstances
Associates
Police record?
Family
other...
About the crime
The offense
The crime scene
Time & date
Manner of attack
Weapons / tools used
other...
Possible motives
Motive 1
other...
About the perpetrator
Trademarks or peculiarities
Spoken or written words
Clothing
Vehicles used
other...


The Laci Peterson Case
24 Oct 2002 - 16 Mar 2005
Scott buys boat
Laci disappears
Pre Arrest
Scott Arrested
Post Arrest
Trial
Before the disappearance

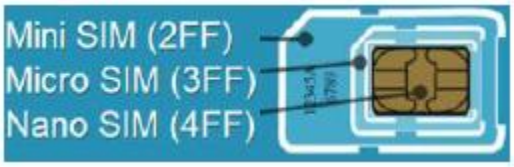

Evidence Intake
Identification
Preparation
Securing / Preserving
Processing
Verification / Validation
Reporting
Presentation
Archiving
Documenting


NOKIA
Nokia Corporation
Type: RM-803
Model: 710
MADE IN KOREA
CE 0434

354[redacted]54[redacted]66

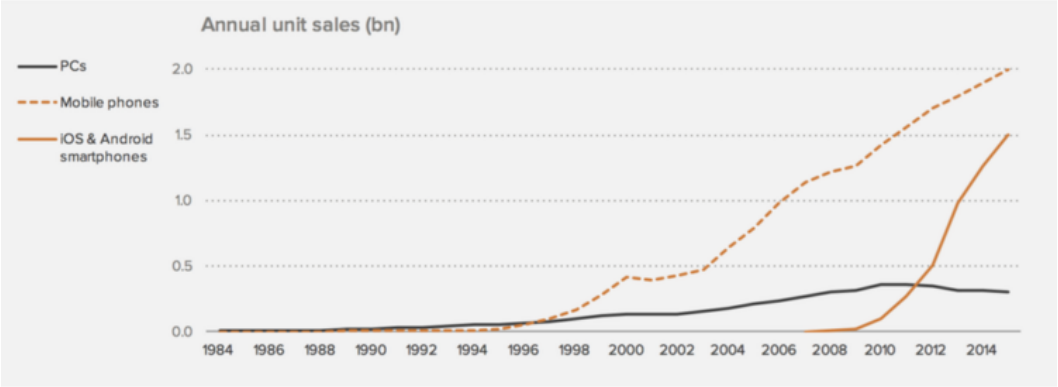
IMEI:	354[redacted]66
Allocating Body:	BABT
Type Allocation Code:	354[redacted]
Serial Number:	4[redacted]6
Luhn Checksum:	6
Manufacturer:	NOKIA CORPORATION
Brand:	NOKIA
Model:	920.1
Network & Information:	Free Check Now
Blacklist (Lost/Stolen):	Free Check Now

Band:
802.11b/g/n, Bluetooth, GSM 1800, GSM 1900, GSM 900, GSM850 (GSM800), HSDPA, HSUPA, LTE FDD BAND 1, LTE FDD BAND 20, LTE FDD BAND 3, LTE FDD BAND 7, LTE FDD BAND 8, NFC, WCDMA FDD Band I, WCDMA FDD Band V, WCDMA FDD Band VIII

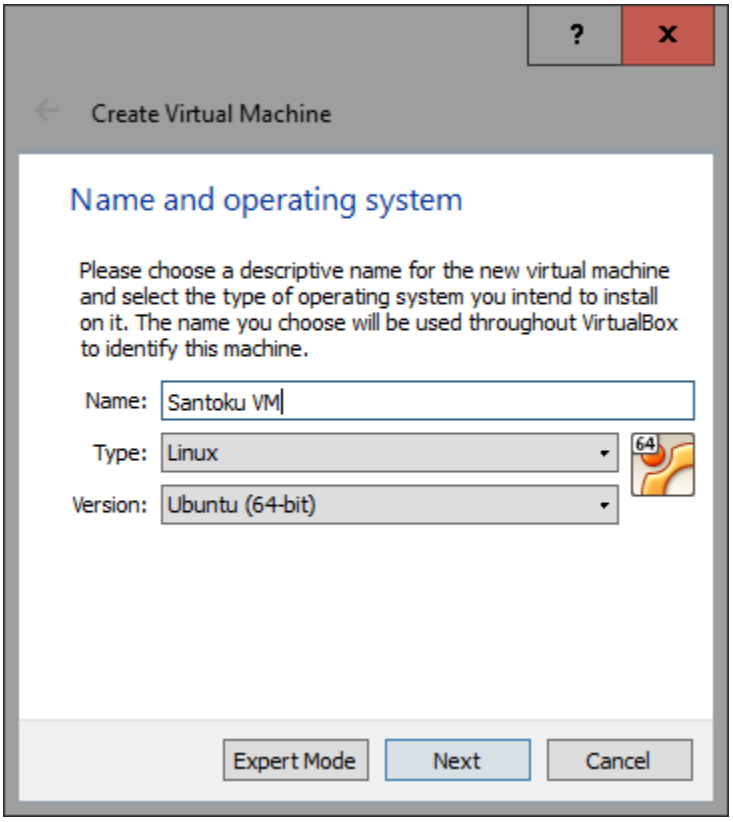


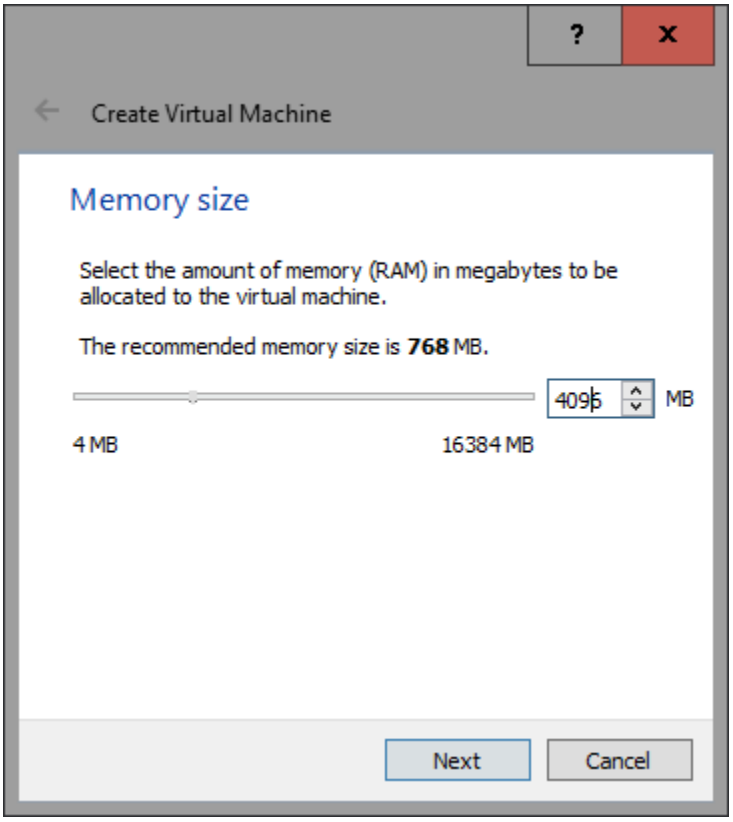
Mobile is the new scale

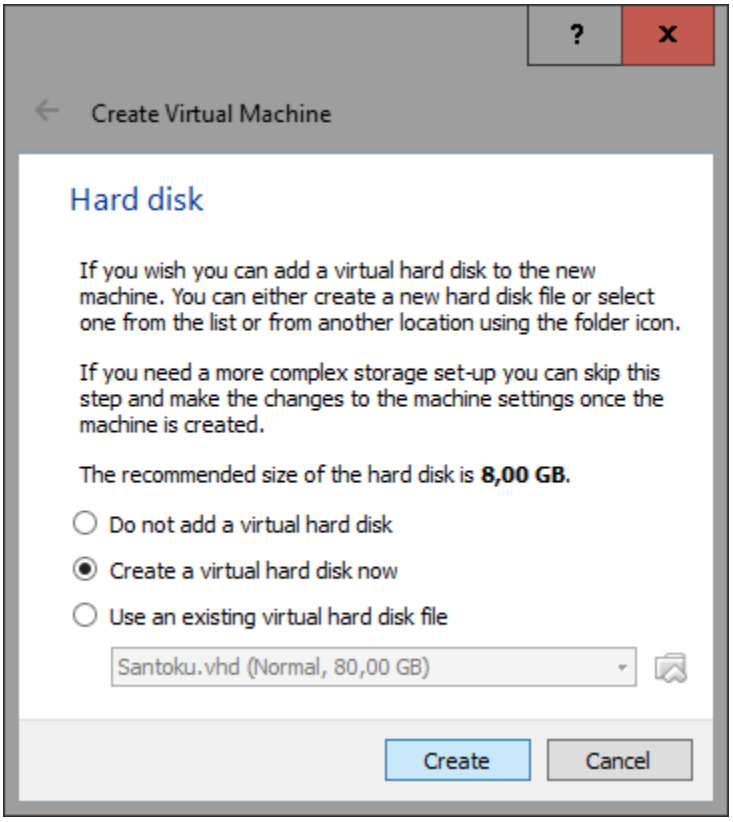
Mobile was always bigger than PCs, but separate. Smartphones broke down that wall

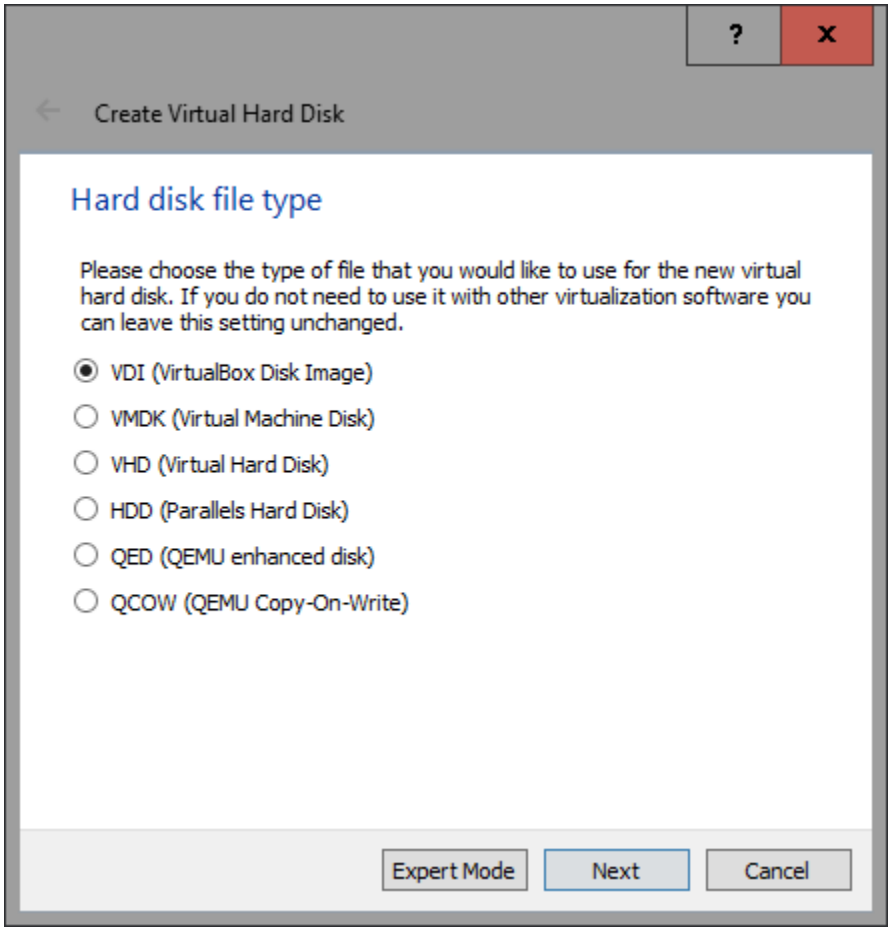


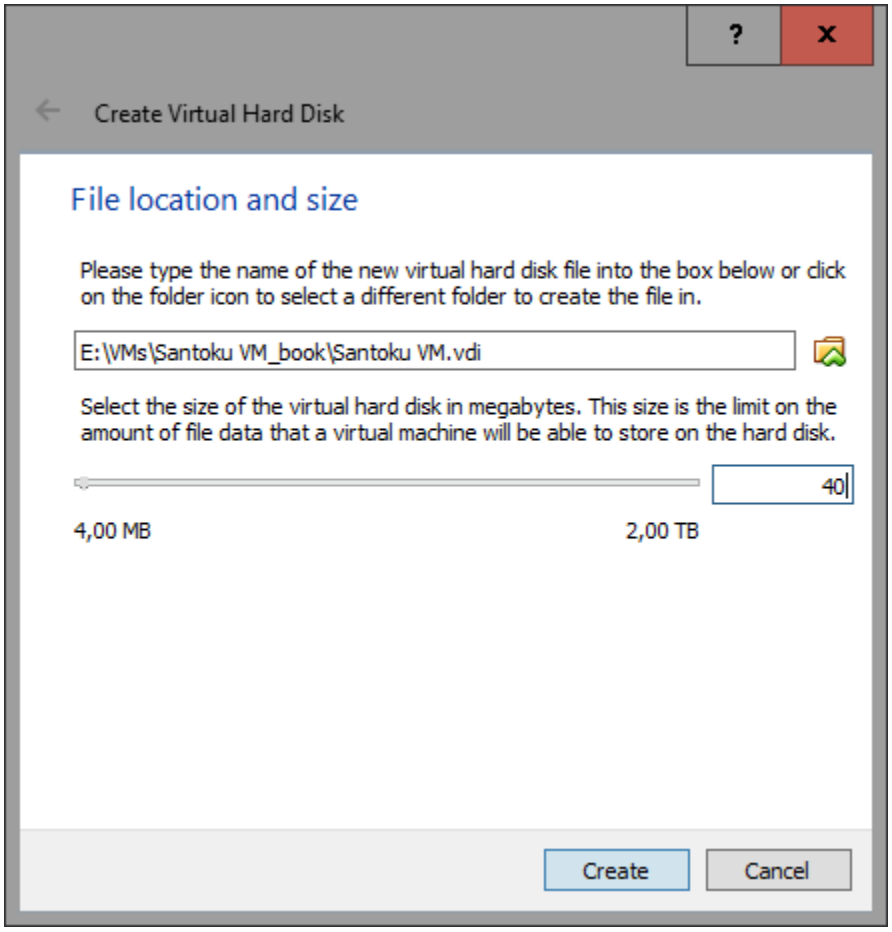
Source: Apple, Google, Nokia, Gartner, a16z

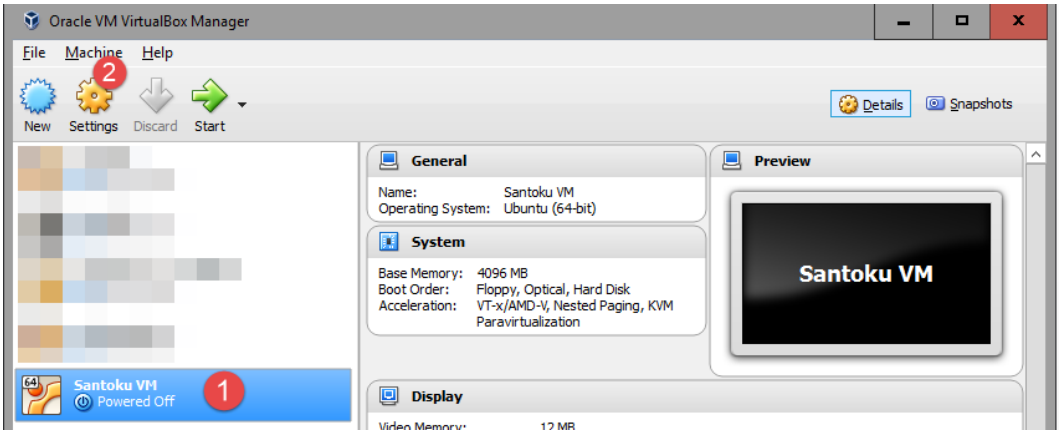

Create Virtual Machine
Name and operating system
Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.
Name:
Santoku VM
Type:
Linux
Version:
Ubuntu (64-bit)
64
Expert Mode
Next
Cancel

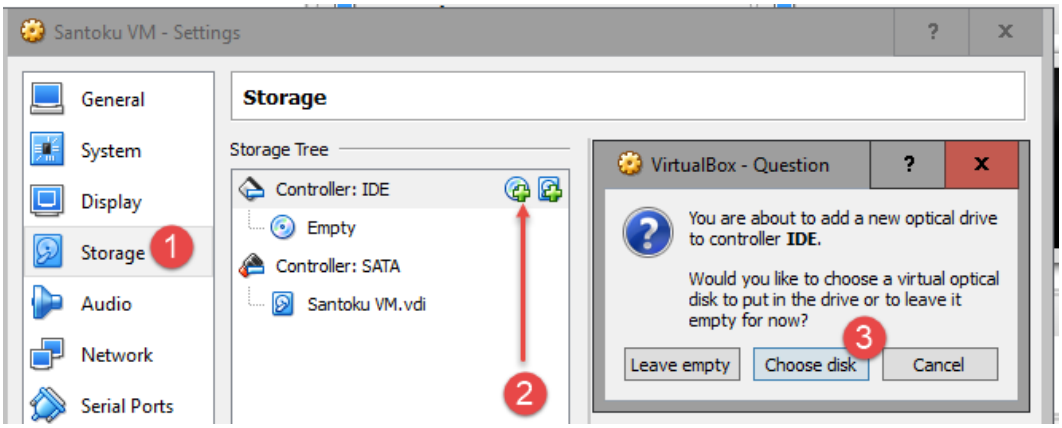

?
Create Virtual Machine
Memory size
Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.
The recommended memory size is 768 MB.
4095
MB
4 MB
16384 MB
Next
Cancel


?
Create Virtual Machine
Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.
If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.
The recommended size of the hard disk is 8,00 GB.
Do not add a virtual hard disk
Create a virtual hard disk now
Use an existing virtual hard disk file
Santoku.vhd (Normal, 80,00 GB)
Create
Cancel

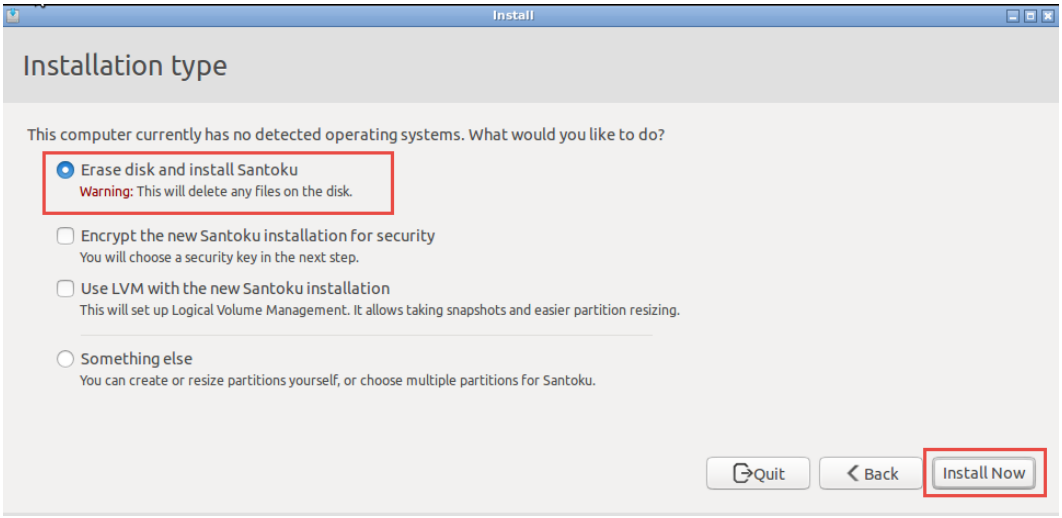

?
Create Virtual Hard Disk
Hard disk file type
Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.
VDI (VirtualBox Disk Image)
VMDK (Virtual Machine Disk)
VHD (Virtual Hard Disk)
HDD (Parallels Hard Disk)
QED (QEMU enhanced disk)
QCOW (QEMU Copy-On-Write)
Expert Mode
Next
Cancel

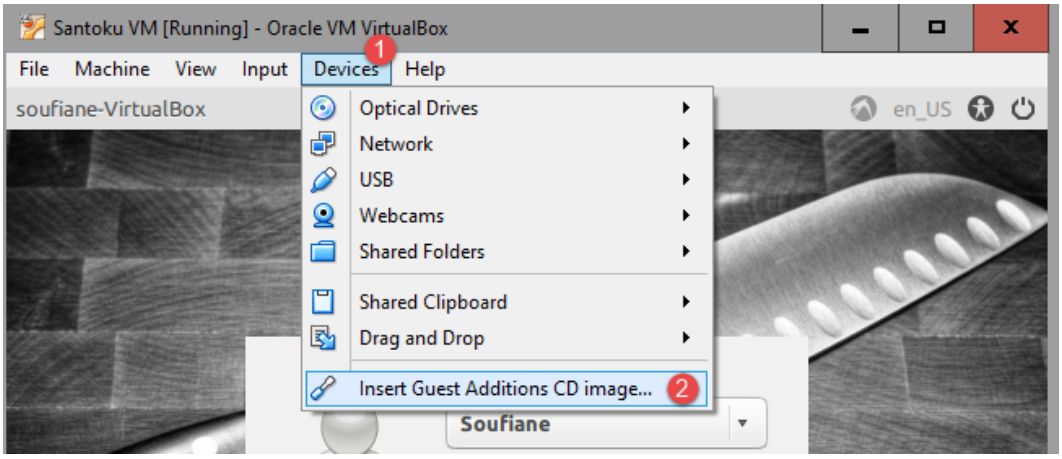

Create Virtual Hard Disk
File location and size
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.
E:\VMs\Santoku VM_book\Santoku VM.vdi
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.
40
4,00 MB
2,00 TB
Create
Cancel

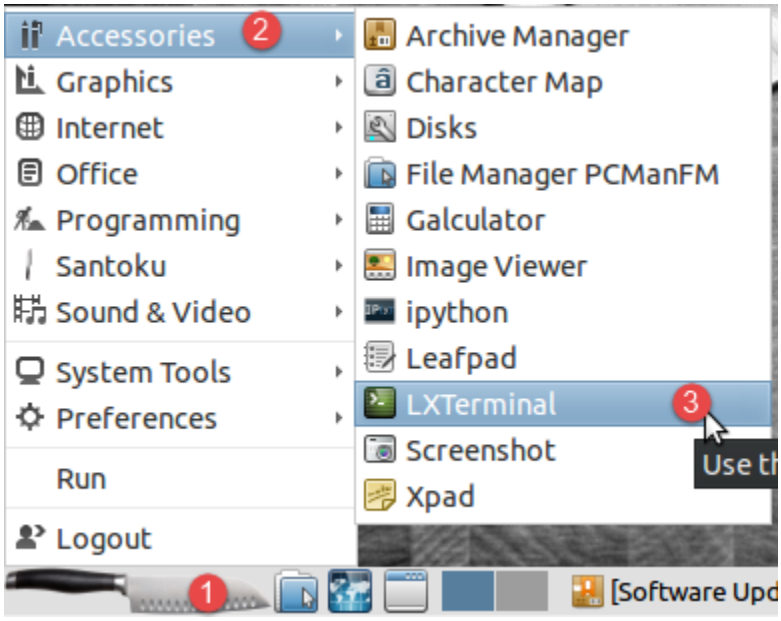

Oracle VM VirtualBox Manager
File
Machine
Help
New
Settings
Discard
Start
Details
Snapshots
General
Name: Santoku VM
Operating System: Ubuntu (64-bit)
System
Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization
Preview
Santoku VM
Santoku VM
Powered Off
Display
1
2

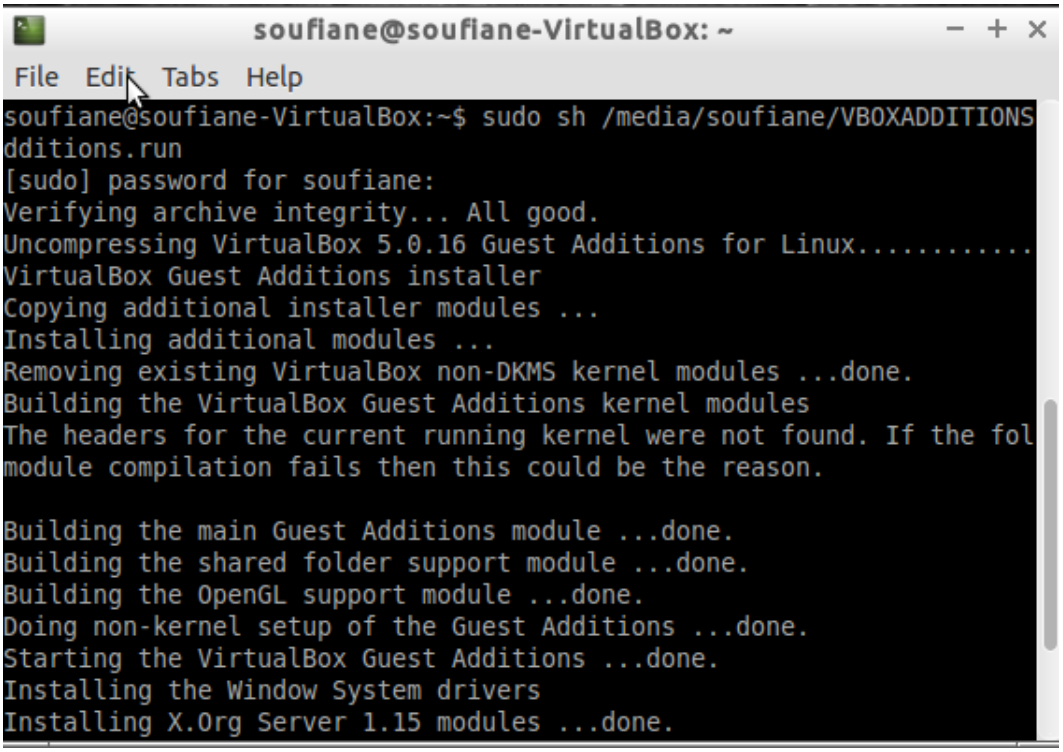

Santoku VM - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
Storage
Storage Tree
Controller: IDE
Empty
Controller: SATA
Santoku VM.vdi
1
2
VirtualBox - Question
You are about to add a new optical drive to controller IDE.
Would you like to choose a virtual optical disk to put in the drive or to leave it empty for now?
3
Leave empty
Choose disk
Cancel

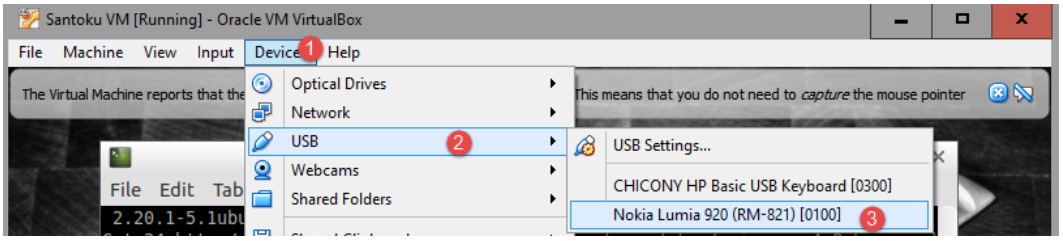

Santoku 0.5
live - boot the Live System
xforcevesa - boot Live in safe graphics mode
install - start the installer directly
memtest - Run memtest
hd - boot the first hard disk
Press [Tab] to edit options


Install
Installation type
This computer currently has no detected operating systems. What would you like to do?
Erase disk and install Santoku
Warning: This will delete any files on the disk.
Encrypt the new Santoku installation for security
You will choose a security key in the next step.
Use LVM with the new Santoku installation
This will set up Logical Volume Management. It allows taking snapshots and easier partition resizing.
Something else
You can create or resize partitions yourself, or choose multiple partitions for Santoku.
Quit
Back
Install Now

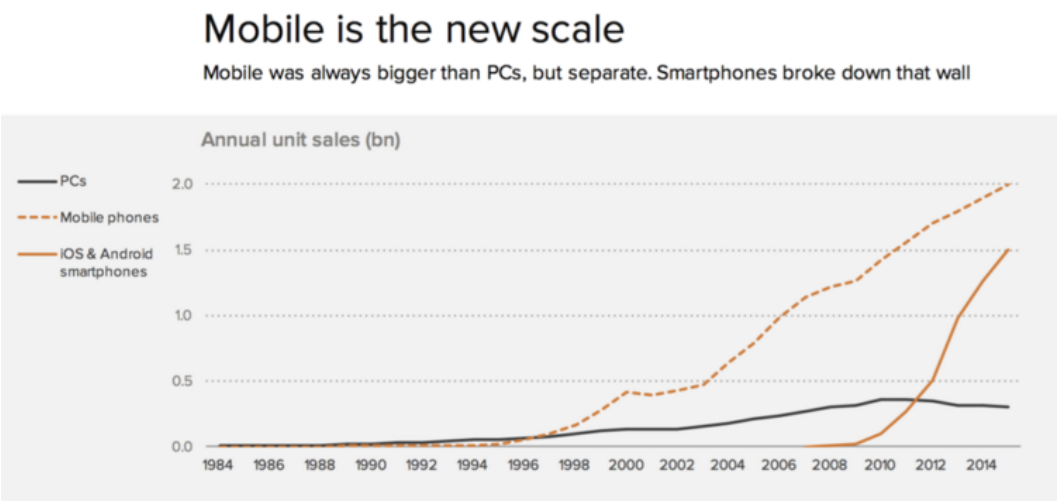

Santoku VM [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
1
soufiane-VirtualBox
en_US
Optical Drives
Network
USB
Webcams
Shared Folders
Shared Clipboard
Drag and Drop
Insert Guest Additions CD image...
2
Soufiane

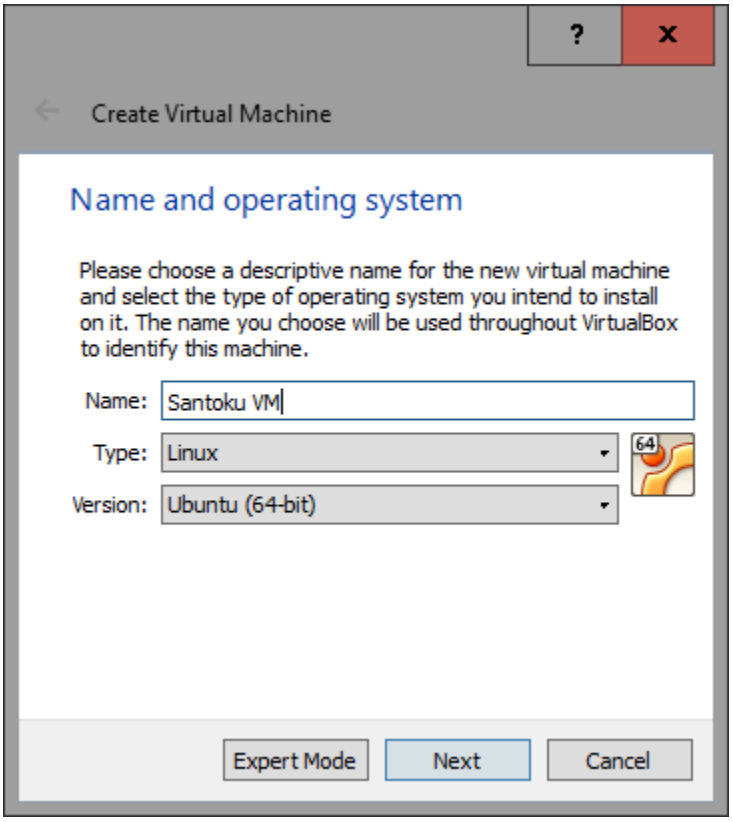

Accessories
Graphics
Internet
Office
Programming
Santoku
Sound & Video
System Tools
Preferences
Run
Logout
Archive Manager
Character Map
Disks
File Manager PCManFM
Galculator
Image Viewer
ipython
Leafpad
LXTerminal
Screenshot
Xpad
1
2
3
[Software Upd

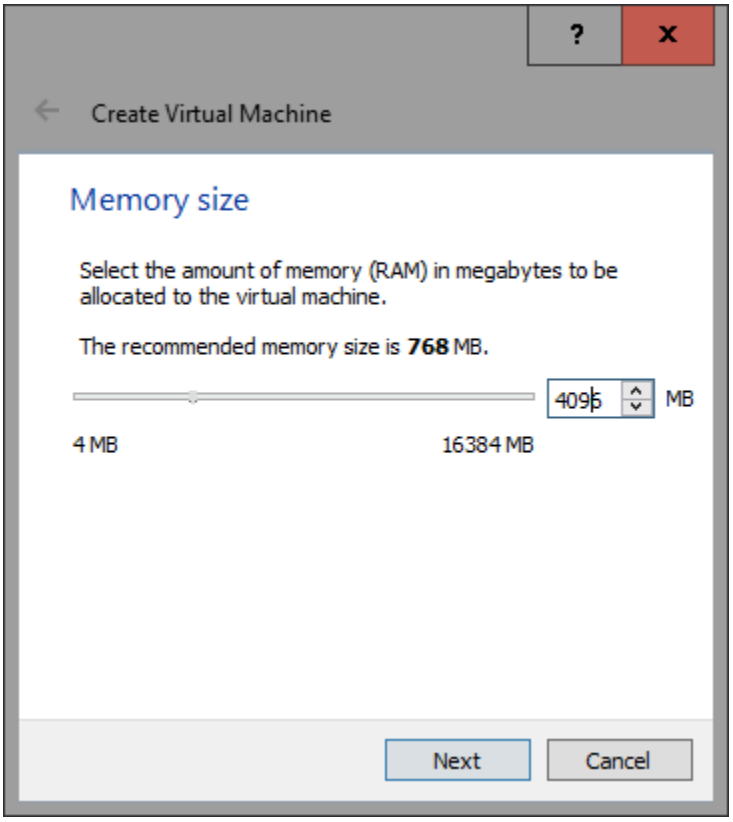

soufiane@soufiane-VirtualBox: ~
File Edit Tabs Help
soufiane@soufiane-VirtualBox:~$ sudo sh /media/soufiane/VBOXADDITIONS
dditions.run
[sudo] password for soufiane:
Verifying archive integrity... All good.
Uncompressing VirtualBox 5.0.16 Guest Additions for Linux.....
VirtualBox Guest Additions installer
Copying additional installer modules ...
Installing additional modules ...
Removing existing VirtualBox non-DKMS kernel modules ...done.
Building the VirtualBox Guest Additions kernel modules
The headers for the current running kernel were not found. If the fol
module compilation fails then this could be the reason.
Building the main Guest Additions module ...done.
Building the shared folder support module ...done.
Building the OpenGL support module ...done.
Doing non-kernel setup of the Guest Additions ...done.
Starting the VirtualBox Guest Additions ...done.
Installing the Window System drivers
Installing X.Org Server 1.15 modules ...done.

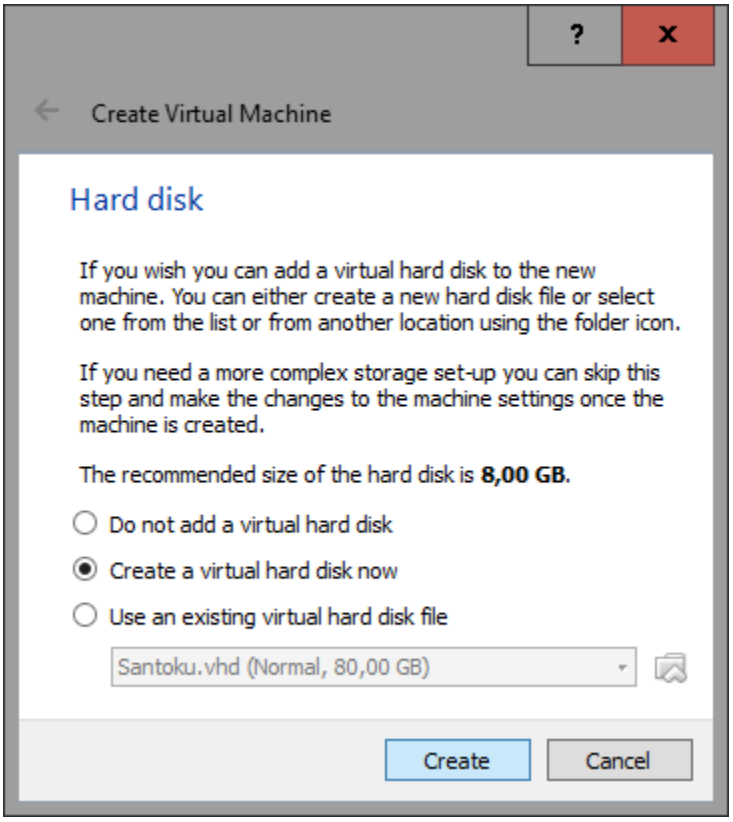

Santoku VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1
Optical Drives
Network
USB
2
Webcams
Shared Folders
USB Settings...
CHICONY HP Basic USB Keyboard [0300]
Nokia Lumia 920 (RM-821) [0100]
3
This means that you do not need to capture the mouse pointer

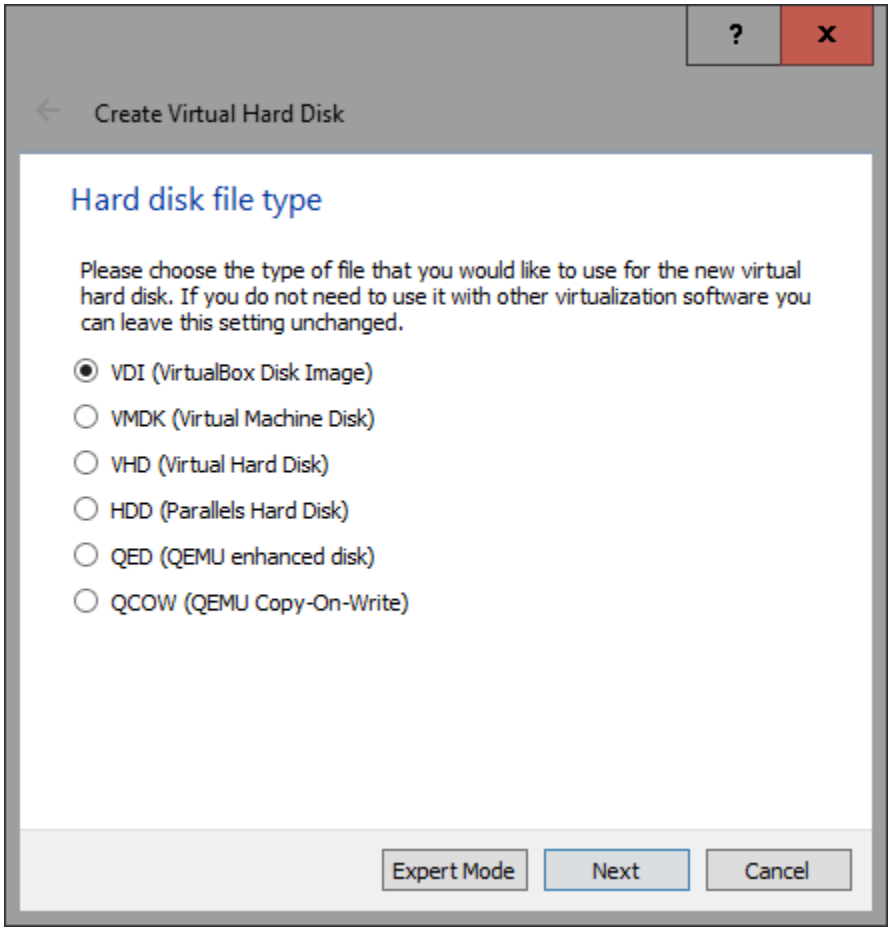
Appendix: Preparing a Mobile Forensic Workstation

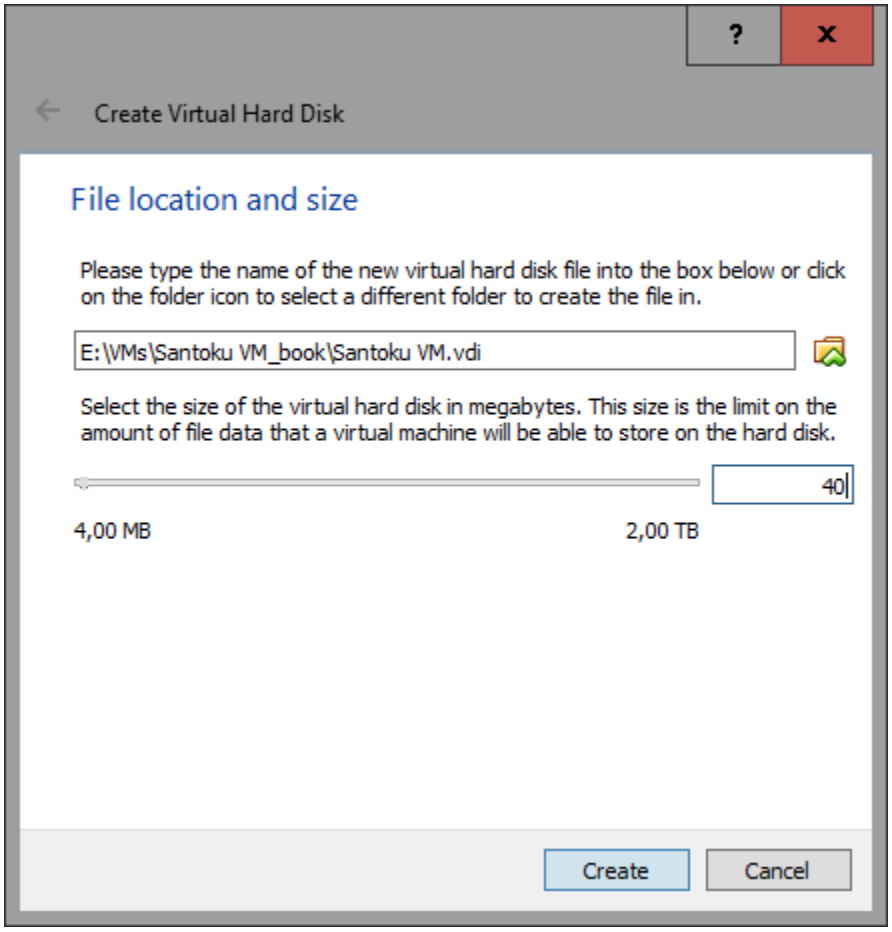


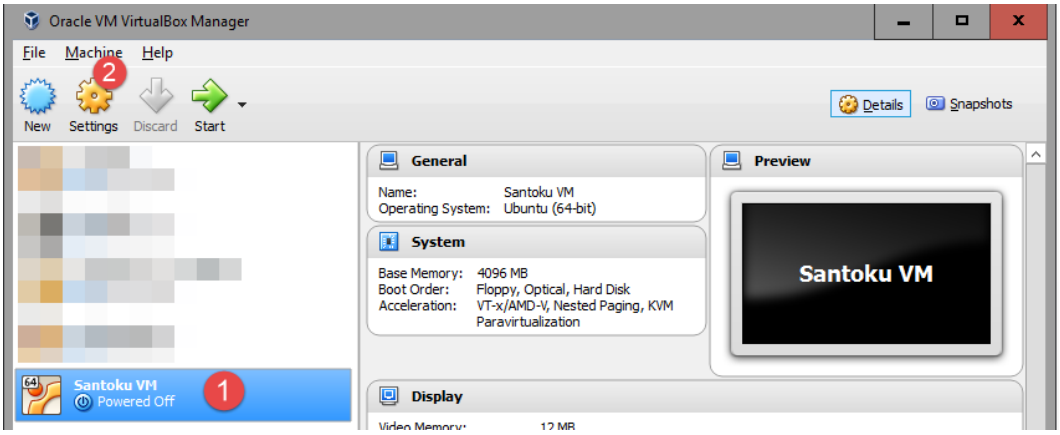

Create Virtual Machine
Name and operating system
Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.
Name:
Santoku VM
Type:
Linux
Version:
Ubuntu (64-bit)
64
Expert Mode
Next
Cancel

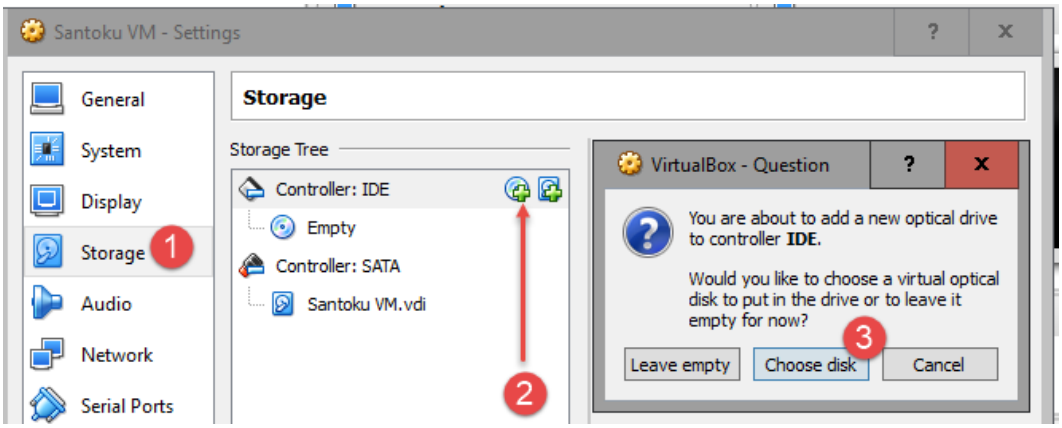

?
Create Virtual Machine
Memory size
Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.
The recommended memory size is 768 MB.
4095
MB
4 MB
16384 MB
Next
Cancel


?
Create Virtual Machine
Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.
If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.
The recommended size of the hard disk is 8,00 GB.
Do not add a virtual hard disk
Create a virtual hard disk now
Use an existing virtual hard disk file
Santoku.vhd (Normal, 80,00 GB)
Create
Cancel

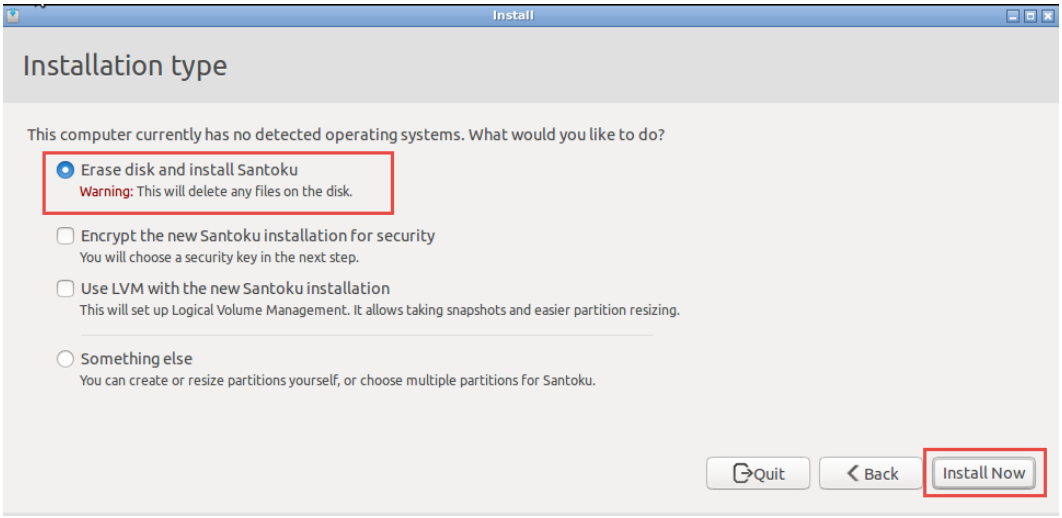

?
Create Virtual Hard Disk
Hard disk file type
Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.
VDI (VirtualBox Disk Image)
VMDK (Virtual Machine Disk)
VHD (Virtual Hard Disk)
HDD (Parallels Hard Disk)
QED (QEMU enhanced disk)
QCOW (QEMU Copy-On-Write)
Expert Mode
Next
Cancel

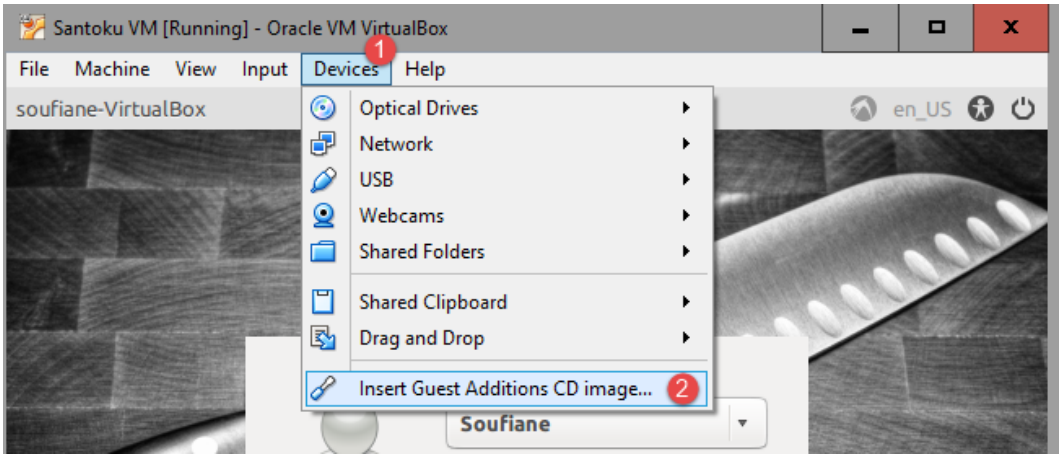

Create Virtual Hard Disk
File location and size
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.
E:\VMs\Santoku VM_book\Santoku VM.vdi
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.
40
4,00 MB
2,00 TB
Create
Cancel

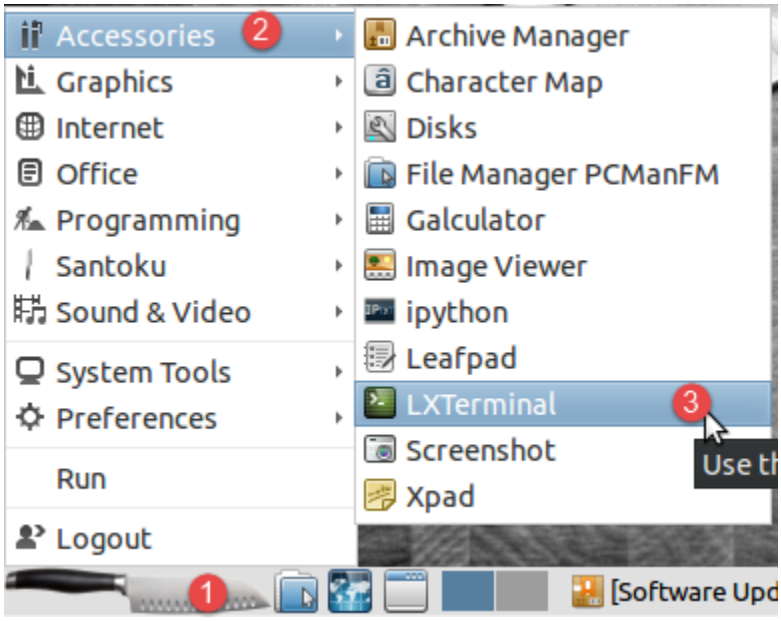

Oracle VM VirtualBox Manager
File
Machine
Help
New
Settings
Discard
Start
Details
Snapshots
General
Name: Santoku VM
Operating System: Ubuntu (64-bit)
System
Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization
Preview
Santoku VM
Santoku VM
Powered Off
Display
1
2

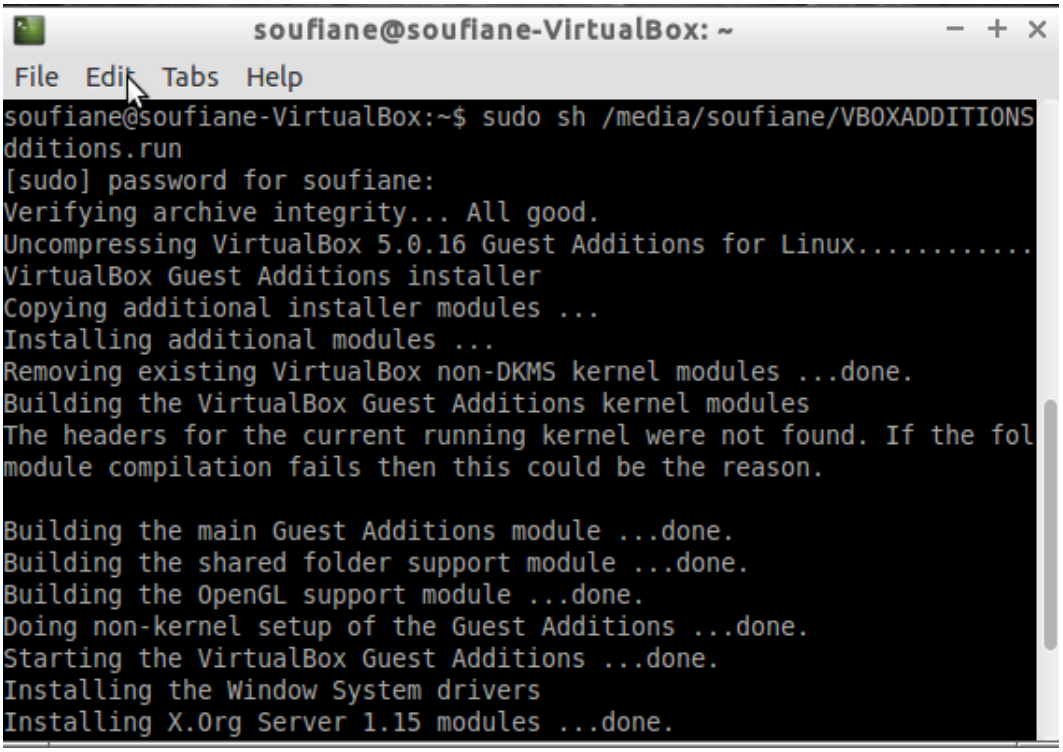

Santoku VM - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
Storage
Storage Tree
Controller: IDE
Empty
Controller: SATA
Santoku VM.vdi
1
2
VirtualBox - Question
You are about to add a new optical drive to controller IDE.
Would you like to choose a virtual optical disk to put in the drive or to leave it empty for now?
3
Leave empty
Choose disk
Cancel

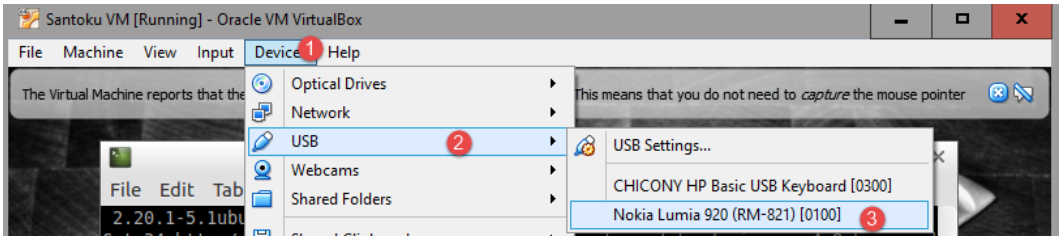

Santoku 0.5
live - boot the Live System
xforcevesa - boot Live in safe graphics mode
install - start the installer directly
memtest - Run memtest
hd - boot the first hard disk
Press [Tab] to edit options


Install
Installation type
This computer currently has no detected operating systems. What would you like to do?
Erase disk and install Santoku
Warning: This will delete any files on the disk.
Encrypt the new Santoku installation for security
You will choose a security key in the next step.
Use LVM with the new Santoku installation
This will set up Logical Volume Management. It allows taking snapshots and easier partition resizing.
Something else
You can create or resize partitions yourself, or choose multiple partitions for Santoku.
Quit
Back
Install Now


Santoku VM [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
1
soufiane-VirtualBox
en_US
Optical Drives
Network
USB
Webcams
Shared Folders
Shared Clipboard
Drag and Drop
Insert Guest Additions CD image...
2
Soufiane


Accessories
Graphics
Internet
Office
Programming
Santoku
Sound & Video
System Tools
Preferences
Run
Logout
Archive Manager
Character Map
Disks
File Manager PCManFM
Galculator
Image Viewer
ipython
Leafpad
LXTerminal
Screenshot
Xpad
1
2
3
[Software Upd


soufiane@soufiane-VirtualBox: ~
File Edit Tabs Help
soufiane@soufiane-VirtualBox:~$ sudo sh /media/soufiane/VBOXADDITIONS
dditions.run
[sudo] password for soufiane:
Verifying archive integrity... All good.
Uncompressing VirtualBox 5.0.16 Guest Additions for Linux.....
VirtualBox Guest Additions installer
Copying additional installer modules ...
Installing additional modules ...
Removing existing VirtualBox non-DKMS kernel modules ...done.
Building the VirtualBox Guest Additions kernel modules
The headers for the current running kernel were not found. If the fol
module compilation fails then this could be the reason.
Building the main Guest Additions module ...done.
Building the shared folder support module ...done.
Building the OpenGL support module ...done.
Doing non-kernel setup of the Guest Additions ...done.
Starting the VirtualBox Guest Additions ...done.
Installing the Window System drivers
Installing X.Org Server 1.15 modules ...done.


Santoku VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1
Optical Drives
Network
USB
2
Webcams
Shared Folders
USB Settings...
CHICONY HP Basic USB Keyboard [0300]
Nokia Lumia 920 (RM-821) [0100]
3
This means that you do not need to capture the mouse pointer