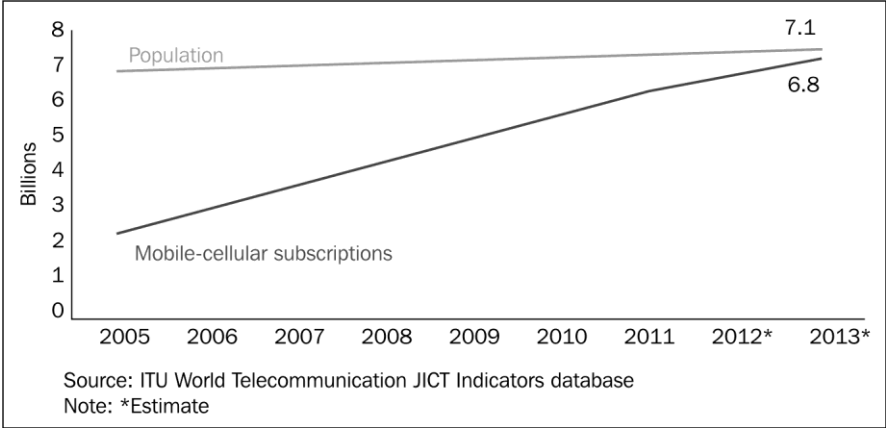
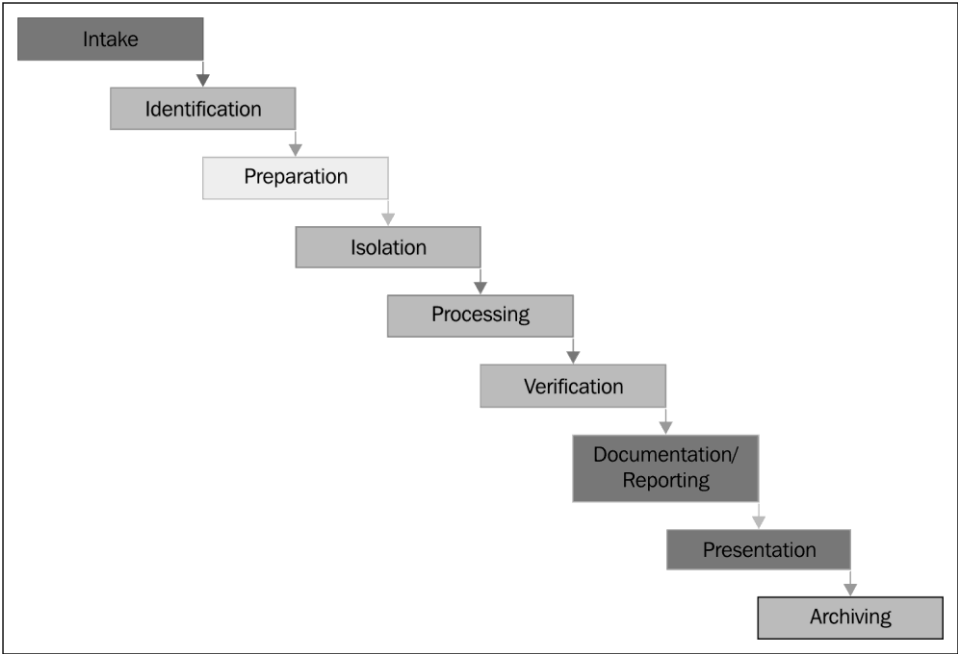


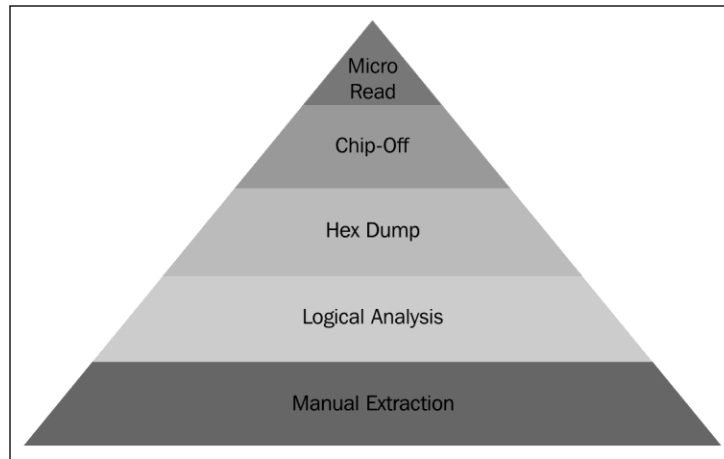
# 1. Introduction to Mobile Forensics



Mobile cellular subscription growth from 2005 to 2013

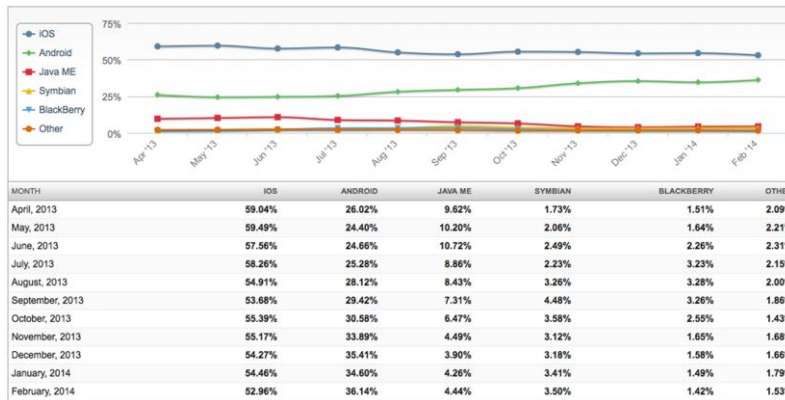


Mobile phone evidence extraction process



Cellular phone tool leveling pyramid (Sam Brothers, 2009)

## 2. Understanding the Internals of iOS Devices



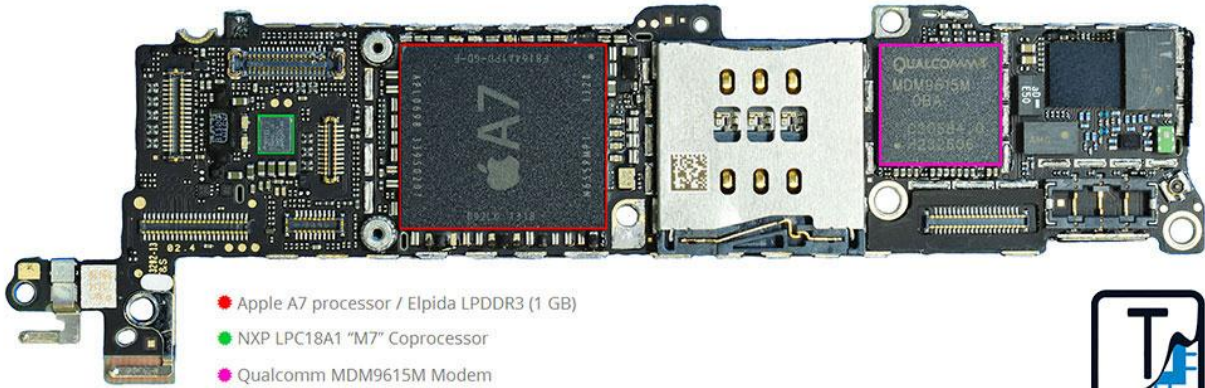
Source: <https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=9&qpcustomb=1>



iPhone model number located on the back of the case



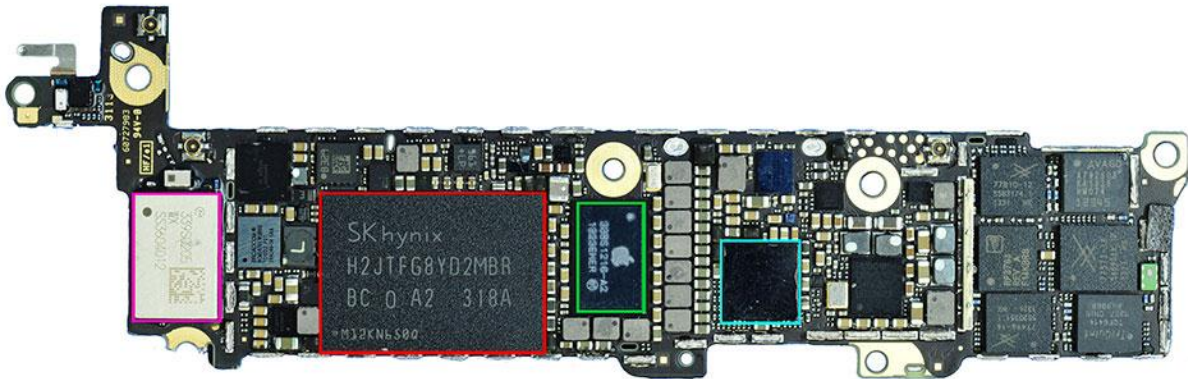
The iPhone About screen, displaying firmware Version 5.1.1 (9B206)



- Apple A7 processor / Elpida LPDDR3 (1 GB)
- NXP LPC18A1 "M7" Coprocessor
- Qualcomm MDM9615M Modem



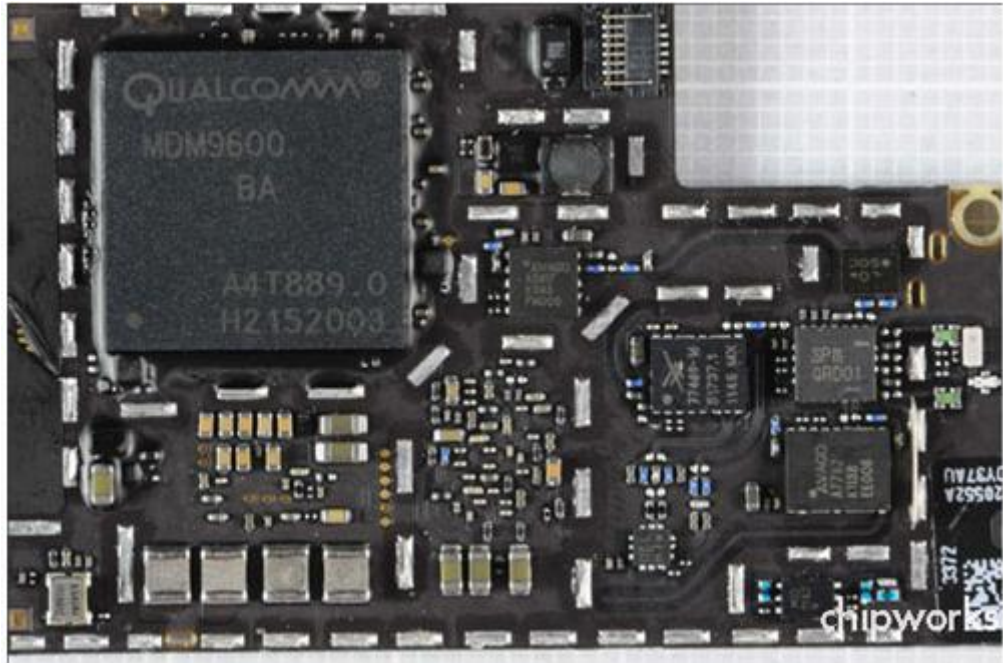
The iPhone 5S teardown image—side one (included with kind permission from TechInsights)



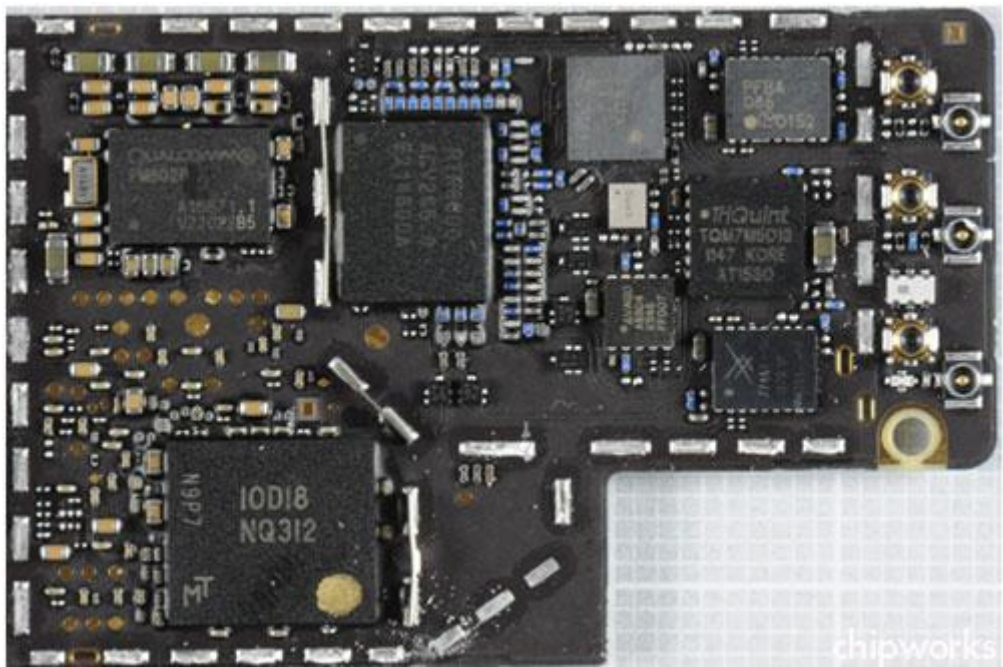
- Hynix 64 GB NAND Flash, Package Mark: H2JTFG8YD2MBR, 8 stacked NAND Flash, Die Mark: H27QCG8T2B
- Apple Logo, Package Mark: 338S1216-A2, Die Mark: Dialog D2045
- Murata Combo Radio MCM, Package Mark: 339S0205, Die Mark:Broadcom BCM43342
- Apple Logo, Package Marking 338S11201, Cirrus Logic, Die Mark: CL11G009A1



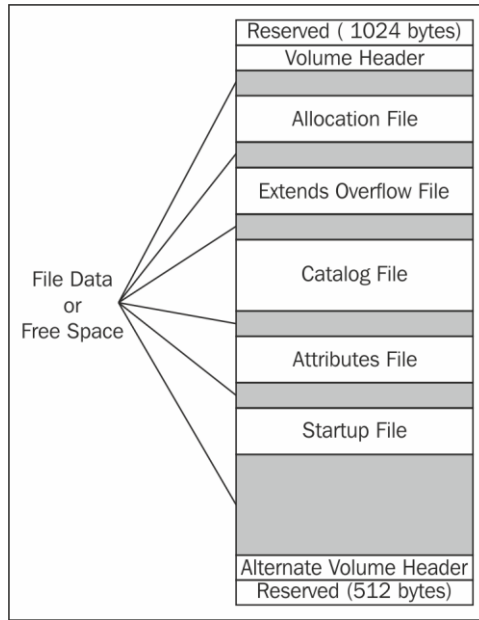
The iPhone 5S teardown image—side two (included with kind permission from TechInsights)



The iPad 3 cellular model teardown image—side one (included with kind permission from Chipworks)

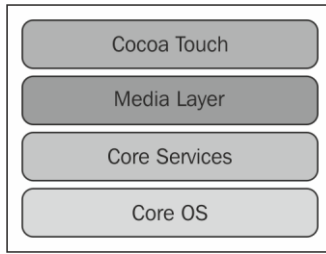


Included with kind permission from Chipworks

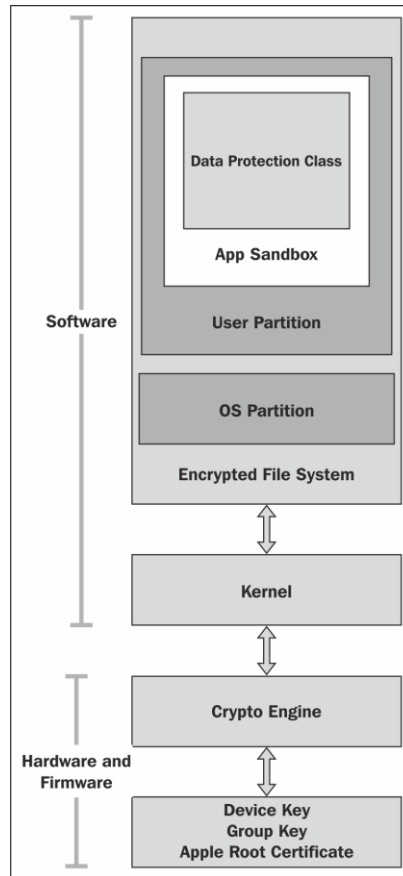


	iPhone OS 1.0	iPhone SDK 2.0	iPhone SDK 3.0	iPhone SDK 4.0	iOS 5	iOS 6	iOS 7
iPhone	1.0		3.1.3				
iPod Touch	1.1		3.1.3				
iPhone 3G		2.0		4.2.1			
iPod Touch (2nd Gen)		2.1.1		4.2.1			
iPhone 3GS			3.0			6.1.3	
iPod Touch (3rd Gen)			3.1.1		5.1.1		
iPad (1st Gen)			3.2	4.3.5	5.1.1		
iPhone4				4.0 (GSM)/4.2.6 (CDMA)			7.0
iPod Touch (4th Gen)				4.2.1		6.1.3	
iPad2				4.3.5			7.0
iPhone 4S					5.0		7.0
iPad					5.1		7.0
iPod Touch (5th Gen)						6.0	7.0
iPad Mini						6.0	7.0
iPhone 5						6.0	7.0
iPhone 5C							7.0.1
iPhone 5S							7.0.1

The OS compatibility matrix

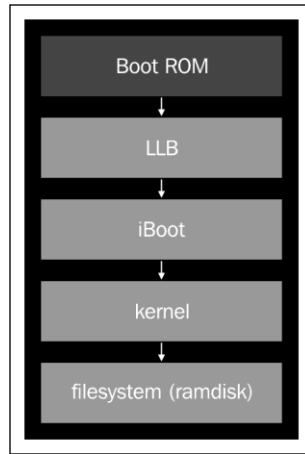


The iOS layers



The iOS security architecture

### 3. Data Acquisition from iOS Devices



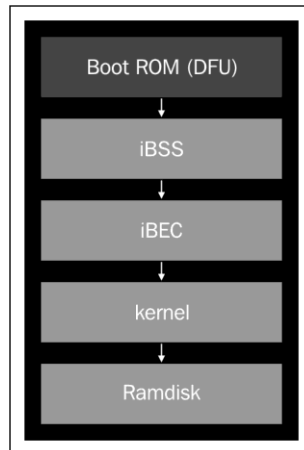
A secure boot chain of an iPhone in normal mode



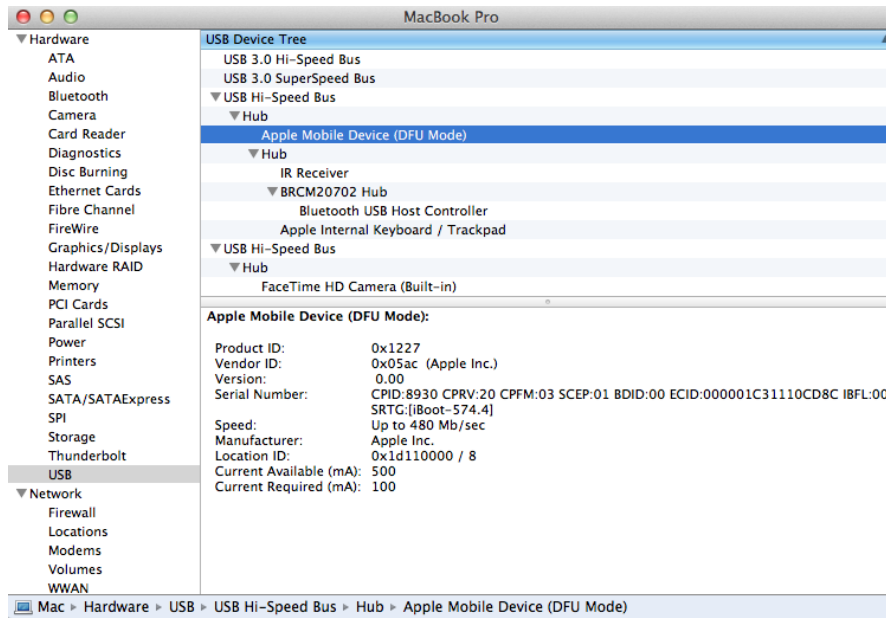




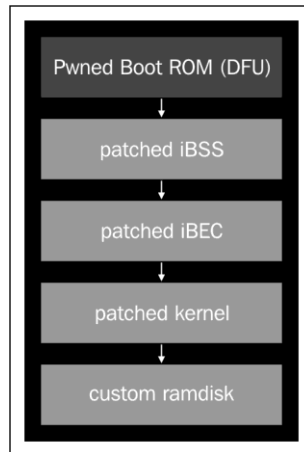
The redsn0w recovery fix



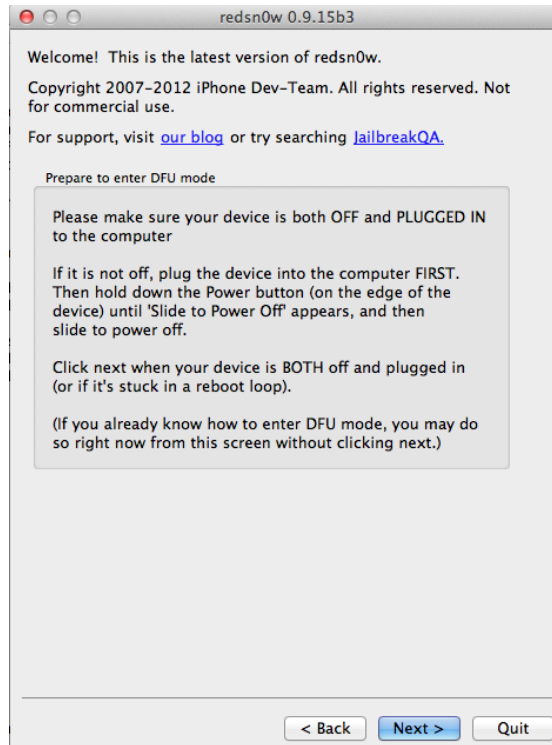
A secure boot chain of an iPhone in DFU mode



The MAC system information displaying a DFU-mode device



An exploited boot chain of an iPhone in DFU mode



The redsn0w welcome screen

```

Mac:/Volumes/Data$hexdump -C mobile/Library/AddressBook/AddressBook.sqlitedb | head
00000000 79 5e b0 03 ea 34 50 78  be ac 56 14 ed 33 ad 2e  |y^...4Px..V..3..|
00000010 68 d3 57 ea 6b 06 d5 e1  34 b1 08 71 56 8a 83 af  |h.W.k...4..qV...|
00000020 33 f9 36 1d 4a f2 84 5b  1c 5f 56 54 3c 5e 9b 4e  |3.6.J..[._VT<^N|
00000030 87 40 58 34 ed c3 92 e7  44 ec 6c dc 14 5e 74 ea  |.@X4....D.l..^t.|
00000040 bd 62 37 bd 2d be 12 a2  39 20 7d 9f 1d dc c7 f5  |.b7.-...9 }.....|
00000050 93 1e 3d 81 51 04 ad be  36 04 74 37 b3 67 f2 bf  |..=.Q...6.t7.g..|
00000060 84 71 94 d7 89 14 cb 8b  24 e0 a7 0d da d6 95 a1  |.q.....$......|
00000070 ff d1 45 51 93 f4 61 1a  cc c6 34 a1 64 9e 7e 1b  |..EQ...a...4.d.~.|
00000080 4a 9c 72 54 a1 b3 d2 6b  f1 42 ea 13 58 cb 66 45  |J.rT...k.B..X.fE|
00000090 3c d3 32 7d b3 71 ab ed  39 15 c3 19 61 67 3f 76  |<.2}.q..9...ag?v|

```

The encrypted AddressBook file

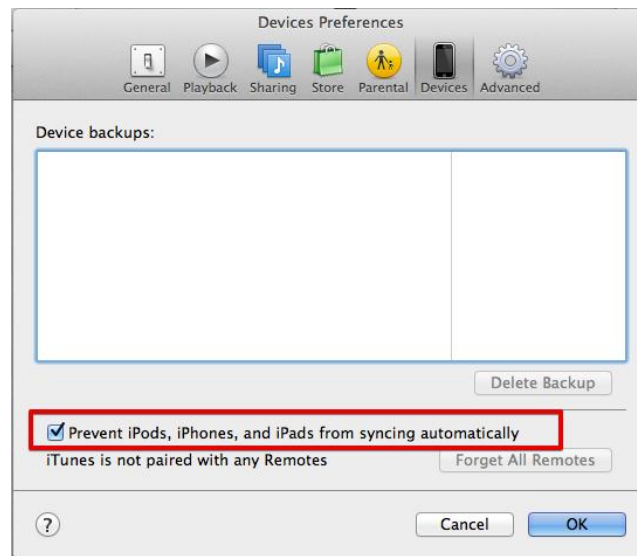
```

Mac:/Volumes/Data$hexdump -C mobile/Library/AddressBook/AddressBook.sqlitedb | head
00000000 53 51 4c 69 74 65 20 66  6f 72 6d 61 74 20 33 00  |SQLite format 3..|
00000010 10 00 02 02 00 40 20 20  00 00 00 09 00 00 00 84  |.....@ .....|
00000020 00 00 00 00 00 00 00 00  00 00 00 40 00 00 00 04  |.....@....|
00000030 00 00 00 00 00 00 00 00  00 00 00 01 00 00 00 00  |.....|
00000040 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |.....|
00000050 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 09  |.....|
00000060 00 2d e2 1f 05 00 00 00  05 0f e7 00 00 00 00 36  |.-.....6|
00000070 0f fb 0f f6 0f f1 0f ec  0f e7 08 a5 07 c3 08 62  |.....b|
00000080 07 27 06 48 05 b8 04 b6  05 7b 04 07 03 72 02 c4  |.'.H.....{...r..|
00000090 03 2f 01 ec 02 81 01 2f  01 a3 00 b6 0f fc 00 00  |./...../.....|

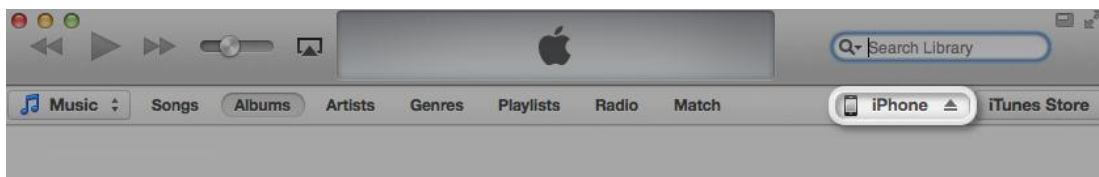
```

The decrypted AddressBook file

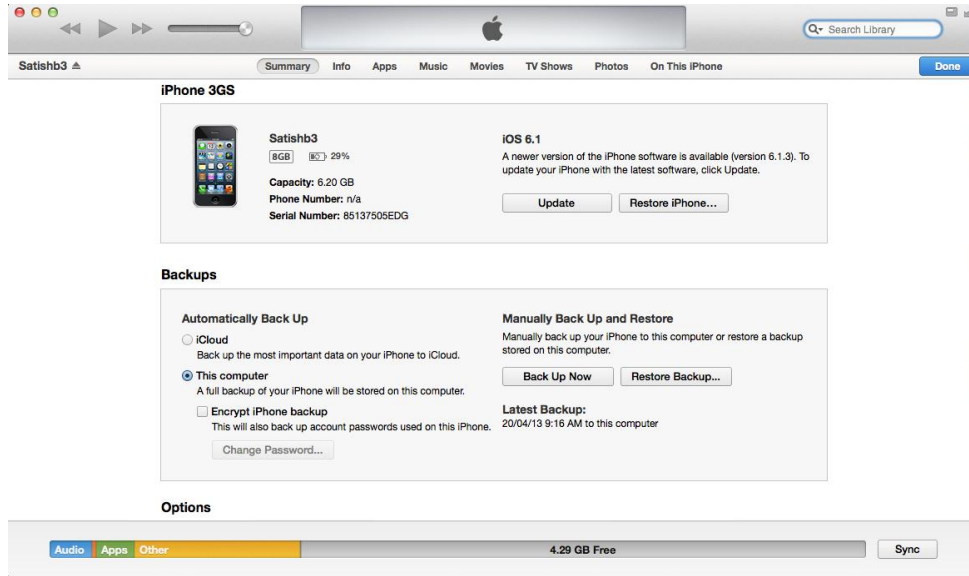
## 4. Data Acquisition from iOS Backups



iTunes—disabling automatic sync



iTunes—iPhone locked message



iTunes—iPhone summary

Key	Type	Value
Root	Dictionary	(5 items)
SystemBUID	String	519DF016-0F61-44E3-978F-65424A4ADA75
HostID	String	97D6299A-8EDA-454F-9C62-48B031F45DD6
RootCertificate	Data	<2d2d2d2d 2d424547 494e2043 45525449 46494341 54452d2d 2d2d2d0a 4d494943 72544343 415a5767 41774942 41674942 4144414e 42676b71 686b6947 3
DeviceCertificate	Data	<2d2d2d2d 2d424547 494e2043 45525449 46494341 54452d2d 2d2d2d0a 4d494943 4e6a4343 41523667 41774942 41674942 4144414e 42676b71 686b6947 3
HostCertificate	Data	<2d2d2d2d 2d424547 494e2043 45525449 46494341 54452d2d 2d2d2d0a 4d494943 756a4343 41614b67 41774942 41674942 4144414e 42676b71 686b6947 3

Pairing records on the iPhone

Key	Type	Value
Root	Dictionary	(9 items)
DeviceCertificate	Data	<2d2d2d2d 2d424547 494e2043 45525449 46494341 54452d2d 2d2d2d0a 4d494943 4e6a4343 41523667 41774942 41674942 4144414e 42676b71 686b6947 3977304;
EscrowBag	Data	<44415441 000004f4 56455253 00000004 00000003 54595045 00000004 00000002 55554944 00000010 1162b128 64e04c36 a901c0a8 9c14b184 484d434b 00000028
HostCertificate	Data	<2d2d2d2d 2d424547 494e2043 45525449 46494341 54452d2d 2d2d2d0a 4d494943 756a4343 41614b67 41774942 41674942 4144414e 42676b71 686b6947 3977304;
HostID	String	97D6299A-8EDA-454F-9C62-48B031F45DD6
HostPrivateKey	Data	<2d2d2d2d 2d424547 494e2052 53412050 52495641 5445204b 45592d2d 2d2d2d0a 4d494945 70414942 41414b43 41514541 31695068 786c4a44 77424a59 6f546678
RootCertificate	Data	<2d2d2d2d 2d424547 494e2043 45525449 46494341 54452d2d 2d2d2d0a 4d494943 72544343 415a5767 41774942 41674942 4144414e 42676b71 686b6947 3977304;
RootPrivateKey	Data	<2d2d2d2d 2d424547 494e2052 53412050 52495641 5445204b 45592d2d 2d2d2d0a 4d494945 6f774942 41414b43 41514541 3041506b 64376857 4b646f41 57736d44
SystemBUID	String	519DF016-0F61-44E3-978F-65424A4ADA75
WIFIMACAddress	String	28:cf:da:6e:99:e2

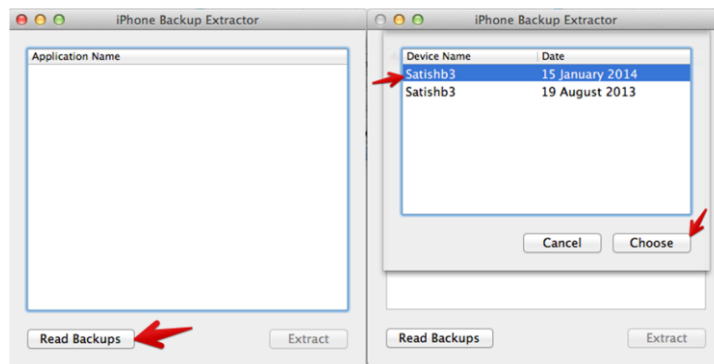
Pairing record on a computer

Name	Date Modified	Size	Kind
ea4f4a1a45ab93a97917e22dd28d298d78686dd4	Yesterday 6:37 PM	621 bytes	Document
ec4d3d239f542940c029b778f84d76d256ae71db	Yesterday 6:37 PM	630 bytes	Document
ec95a2de2a4f4b05093ef791394597fb453e8c16	Yesterday 6:37 PM	947 bytes	Document
ec1538f1312bd144239f7eac70ddeb3e010dc550	Yesterday 6:37 PM	88 bytes	Document
ed30b0c4ccfb60267ae43b613df6e005af85043	Yesterday 6:37 PM	256 KB	Document
edc8c482cd751c40274ca5162b2347b80b43b173	Yesterday 6:37 PM	273 bytes	Document
ef244b0e70a71410ab2d8c2a64b826f864b4012	Yesterday 6:37 PM	242 bytes	Document
f0b044e128429dab20ctac24fbedb3a5286730ac	Yesterday 6:37 PM	66 bytes	Document
f6dc7201d77127256c5809ee73ca45975696e35	Yesterday 6:37 PM	70 bytes	Document
f7ab63e61427d2ee896496f5720b1269cfa38	Yesterday 6:37 PM	3 KB	Document
f979aebad592c876a97ba6a640b3401c526248	Yesterday 6:37 PM	316 bytes	Document
f2627f146e07614fe4df5a174ef6a042ea99eb	Yesterday 6:37 PM	124 KB	Document
f30d6ef41c65177e0d949cbbefa7e114bb39a212	Yesterday 6:37 PM	1 KB	Document
f34b101ed66f3aff9b378f9536e8e5c23cf69bb	Yesterday 6:37 PM	353 bytes	Document
f42cdfc14c080199b895a59b6740a3c5b69cc33	Yesterday 6:37 PM	81 bytes	Document
f86c972026c10344edf4ce5894caee4222120a1	Yesterday 6:37 PM	289 KB	Document
f772aa7de1bd2f98494024fbd193c6c4a3a586	Yesterday 6:37 PM	358 bytes	Document
f936b0c64de096db559922b70a23faa8db75bdb	Yesterday 6:37 PM	119 KB	Document
f5359de2330c2359fc2445c1738d52a2fba44	Yesterday 6:37 PM	41 KB	Document
f23461ec2e507af102a699e5e1fb5080608024b5	Yesterday 6:37 PM	5 KB	Document
f968421bd39a938ba456ef7aa096f8627662b74a	Yesterday 6:37 PM	699 bytes	Document
fb7786ced1add24313fa258c8e1ed041e24d52a4	Yesterday 6:37 PM	252 bytes	Document
fb52095c98189505f20d2af90a46a1ced8c2e9c	Yesterday 6:37 PM	6 KB	Document
fd2e3825497230b737c2fa26972c56e675159b	Yesterday 6:37 PM	6 KB	Document
fd18a792c092be802c447ef7c0f8f11c8821c6f	Yesterday 6:37 PM	243 bytes	Document
fdad2f81cc0b838dc00e3050b14da7ef2d833f3c	Yesterday 6:37 PM	45 KB	Document
Info.plist	Yesterday 6:37 PM	13 KB	Property List
Manifest.mbdb	Yesterday 6:37 PM	68 KB	Document
Manifest.plist	Yesterday 6:37 PM	5 KB	Property List
Status.plist	Yesterday 6:37 PM	189 bytes	Property List

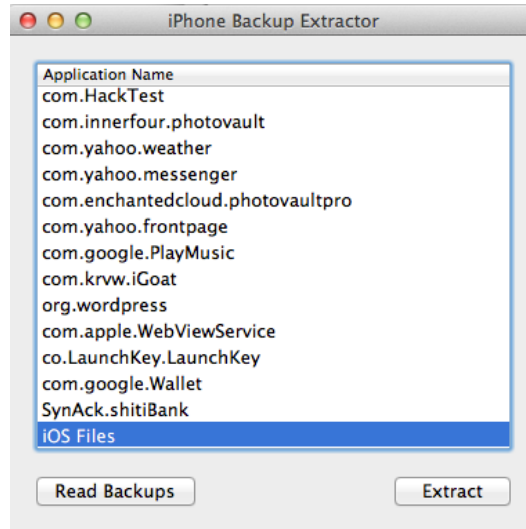
iPhone backup files

Key	Type	Value
Root	Dictionary	(4 items)
Version	String	16.0
SystemDomains	Dictionary	(12 items)
MobileDeviceDomain	Dictionary	(2 items)
CameraRollDomain	Dictionary	(9 items)
WirelessDomain	Dictionary	(5 items)
SystemPreferencesDomain	Dictionary	(3 items)
HomeDomain	Dictionary	(10 items)
DatabaseDomain	Dictionary	(4 items)
TonesDomain	Dictionary	(6 items)
RootDomain	Dictionary	(3 items)
BooksDomain	Dictionary	(8 items)
ManagedPreferencesDomain	Dictionary	(2 items)
KeychainDomain	Dictionary	(6 items)
MediaDomain	Dictionary	(10 items)
MinSupportedVersion	String	3.0
MaxSupportedVersion	String	17.0

System domains on the iPhone



iPhone Backup Extractor—choosing backups



iPhone Backup Extractor

Display Name	Name	Files	Size	App Size
---	System	266	7,641,458	
co.LaunchKey.LaunchKey	co.LaunchKey.LaunchKey	3	53,467	
com.apple.weather	com.apple.weather	N/A	0	
com.apple.WebViewService	com.apple.WebViewService	N/A	0	
com.enchantedcloud.photovaultpro	com.enchantedcloud.photovaultpro	8	2,429	
com.google.PlayMusic	com.google.PlayMusic	3	727	
com.google.Wallet	com.google.Wallet	N/A	0	
com.HackTest	com.HackTest	N/A	0	
com.innerfour.photovault	com.innerfour.photovault	2	8,220	
com.jadedpixel.shopify	com.jadedpixel.shopify	3	283,965	
com.krww.iGoat	com.krww.iGoat	1	343	

Name	Size	Date	Domain	Key
keychain-backup.plist	111,801	1/18/2014 1:26:17 PM	KeychainDomain	51a4616e576dd33cd2abadfea874eb8f248f0e
Library/Accounts/Accounts3.sqlite	90,112	1/17/2014 1:38:02 AM	HomeDomain	943624fd13e27b800cc6d5ce1100c22356ee365c
Library/AddressBook/AddressBook.sqlite	700,416	11/8/2013 1:40:33 PM	HomeDomain	31bb7ba8914766d4ba40d6fdb6113c8b614be442
Library/AddressBook/AddressBookImages.sqlite	1,122,304	5/11/2013 3:33:37 AM	HomeDomain	cd6702cea29e89cf280a76794405adb179a0ee
Library/AddressBook/AddressBookImages.sqlite-shm	0	1/5/2014 6:16:59 AM	HomeDomain	d1225e5e1a1e05345a3c090677a98a66b6429f47
Library/AddressBook/AddressBookImages.sqlite-wal	16,464	11/5/2013 3:41:56 PM	HomeDomain	944320f0e5693a48a6d6769d509567e0e2b08de
Library/BulletinBoard/BehaviorOverrides.plist	1,496	2/19/2013 2:00:32 AM	HomeDomain	3418406efa0258f8db103dc909cfe1e9a35ede36
Library/BulletinBoard/ClearedSections.plist	241	1/9/2014 2:12:04 AM	HomeDomain	dd4b52c3d74ed39a7d8ca8baa79651ad5c2b71d
Library/BulletinBoard/SectionInfo.plist	23,702	1/16/2014 1:11:59 PM	HomeDomain	3d8a6630ca29c3f835470e1c45a747e245f8594
Library/BulletinBoard/SectionOrder.plist	788	2/19/2013 1:12:37 AM	HomeDomain	910e28e5a7bce77740ac6d91546c68ad5ffa9491
Library/Caches/com.apple.mobilesafari/Thumbnails/040164FC-BA2F-42BB-81E7...	26,910	1/4/2014 12:01:23 AM	HomeDomain	406bf4ce09639cad79440fa4ac86e1b0cc10304
Library/Caches/com.apple.mobilesafari/Thumbnails/6D93D86-F667-4596-8B71...	54,882	6/16/2013 4:30:34 AM	HomeDomain	5e0b3d1018c9c9f4c72e68a1a43d3a5e5a99d3
Library/Caches/com.apple.mobilesafari/Thumbnails/76963A1B-595A-4B1A-9C9F...	16,792	6/22/2013 2:46:03 PM	HomeDomain	580bf2d701a82402b0b5773281a8bac87540c9a6
Library/Caches/com.apple.mobilesafari/Thumbnails/DF2E9D2C-DC06-40D6-961...	1,539	9/25/2013 2:56:51 PM	HomeDomain	6a531828a4b633b44890aac77a11e8b072ea4d
Library/Caches/com.apple.mobilesafari/Thumbnails/FE5447E2-852F-414D-AB6...	1,662	1/16/2014 2:44:19 PM	HomeDomain	a07ad1e28c2ec87a91b60a9a77e3f809f310f88
Library/Caches/com.apple.WebAppCache/ApplicationCache.db	294,912	9/25/2013 2:56:46 PM	HomeDomain	d2acb1ec24ed4669ec97975478478df5bd239f9
Library/Caches/locationd/clients.plist	2,425	1/18/2014 12:39:09 PM	RootDomain	a690d7769c8e804ca2b67320b107c8fe979412
Library/Caches/locationd/consolidated.db	20,480	12/31/2013 12:25:28 ...	RootDomain	4096c9ec678f2847dc283405900e284a7c815836
Library/Caches/locationd/significant.plist	74	5/10/2013 3:59:43 PM	RootDomain	c061d48f0cbf73a9ebdae6e15dd85ed9669114f5
Library/Calendar/Calendar.sqlite	389,120	1/17/2014 1:31:13 AM	HomeDomain	2041457d9e04d39d0ab481178355df6781e6858
Library/Calendar/Extras.db	28,672	1/3/2014 3:22:42 PM	HomeDomain	22b5f3c3890cfc5cee685c923922e8e8e9f9d

iPhone Backup Browser

Name	Date Modified	Size	Kind
AppDomain-co.LaunchKey.LaunchKey	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.apple.weather	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.apple.WebViewService	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.e...loud.photovaultpro	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.google.PlayMusic	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.google.Wallet	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.HackTest	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.innerfour.photovault	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.jadedpixel.shopify	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.krvw.Goat	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.mywizr.wizr	Today 7:46 PM	--	Folder
AppDomain-com.quickoffice.egab	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.securitylearn.CardInfo	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.yahoo.Aerogram	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.yahoo.frontpage	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.yahoo.messenger	15-Jan-2014 10:05 PM	--	Folder
AppDomain-com.yahoo.weather	15-Jan-2014 10:05 PM	--	Folder
AppDomain-mega.ios	Today 7:46 PM	--	Folder
AppDomain-org.wordpress	15-Jan-2014 10:05 PM	--	Folder
AppDomain-SynAck.shtiBank	15-Jan-2014 10:05 PM	--	Folder
CameraRollDomain	15-Jan-2014 10:05 PM	--	Folder
DatabaseDomain	15-Jan-2014 10:05 PM	--	Folder
HomeDomain	15-Jan-2014 10:05 PM	--	Folder
KeychainDomain	15-Jan-2014 10:05 PM	--	Folder
ManagedPreferencesDomain	15-Jan-2014 10:05 PM	--	Folder
Manifest.plist	Today 7:46 PM	9 KB	Property List
MediaDomain	15-Jan-2014 10:05 PM	--	Folder
MobileDeviceDomain	15-Jan-2014 10:05 PM	--	Folder
RootDomain	15-Jan-2014 10:05 PM	--	Folder
SystemPreferencesDomain	15-Jan-2014 10:05 PM	--	Folder
WirelessDomain	15-Jan-2014 10:05 PM	--	Folder

Extracted iPhone backup files

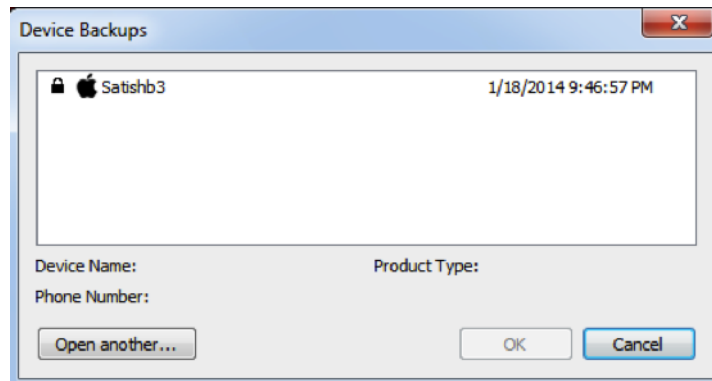
Service	Account	Data	Access group	Protection class
push.apple.com		>e68a5980072c7c1c23b	com.apple.apsd	AlwaysThisDeviceOnly
AirPort	belkin.3239	443c8666	apple	AfterFirstUnlock
Shared Mobile Device ID		9efc4674bd36cf2c268a	P6B36VEQ8D.ru.yandex.mobile.shared-device-id	WhenUnlocked
com.apple.certui	https://blu-m.hotmail.com - c643bf96 59b4	<binary plist data>	apple	Always
AppleIDClientIdentifier		7E56EFC-3757-4450-8	apple	AfterFirstUnlockThisDeviceOnly
Etsy	token	{0233402f7f5e9b824879}	3CUB372VC3.com.etsy.etsyforios	WhenUnlocked
Etsy	secret	{6b96974a8a}	3CUB372VC3.com.etsy.etsyforios	WhenUnlocked
com.facebook.analytics.deviceid		59688B08-C684-4F49-B	T84QZ565D0.platformFamily	AlwaysThisDeviceOnly
com.facebook.datr		{bXfOUfDmKPE8Cis_Vot}	T84QZ565D0.platformFamily	WhenUnlocked
com.apple.certui	https://blu-m.hotmail.com - 352dcac7 2563	<binary plist data>	apple	Always
com.facebook.Snap_graph	{Data('180084998443505')}	BAADIZCRCHs8BAK9K	T84QZ565D0.platformFamily	WhenUnlocked
com.apple.certui	https://mega.co.nz - 5b4ff5c8 39c1f27f f8	<binary plist data>	com.apple.cfnetwork	Always
com.apple.certui	https://blu-m.hotmail.com - 7e571804 e159	<binary plist data>	apple	Always
com.apple.certui	https://accounts.google.com - c6ee4e97 e1	<binary plist data>	com.apple.cfnetwork	Always
com.apple.certui	https://accounts.youtube.com - 7f5918d3 9	<binary plist data>	com.apple.cfnetwork	Always
com.apple.certui	https://blu-m.hotmail.com - cecacbbe 4098	<binary plist data>	apple	Always
com.apple.certui	https://www.google.co.in - 986de596 fbada	<binary plist data>	com.apple.cfnetwork	Always
com.apple.certui	https://blu-m.hotmail.com - 12802df3 c3d5	<binary plist data>	apple	Always
com.apple.certui	https://netbanking.mashreqbank.com - 5afe	<binary plist data>	com.apple.cfnetwork	Always
com.apple.certui	https://www.testflightapp.com - 0f67aeae	<binary plist data>	com.apple.cfnetwork	Always
com.apple.certui	https://blu-m.hotmail.com - 114aac43 a801	<binary plist data>	apple	Always
com.apple.certui	https://www.testflightapp.com - a4989765	<binary plist data>	com.apple.cfnetwork	Always
AirPort	satish mac	1234abcd	apple	AfterFirstUnlock
com.apple.certui	https://netbanking.mashreqbank.com - 6af6	<binary plist data>	com.apple.cfnetwork	Always
com.apple.certui	https://blu-m.hotmail.com - e96abbaf 8074	<binary plist data>	apple	Always
com.apple.iAdIDRecords	{Data('kADiAdIDStorageKey')}	<binary plist data>	apple	WhenUnlocked

A decrypted keychain

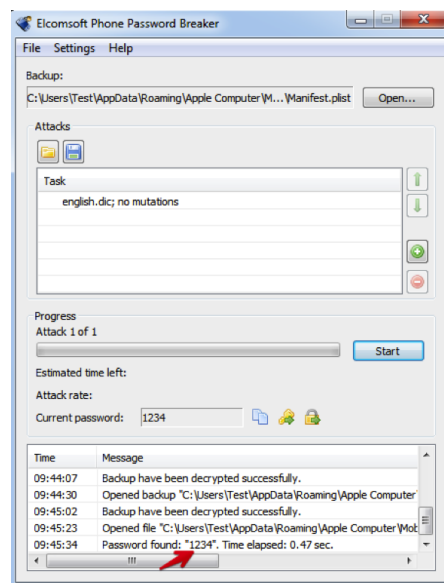




iTunes—encrypted backup



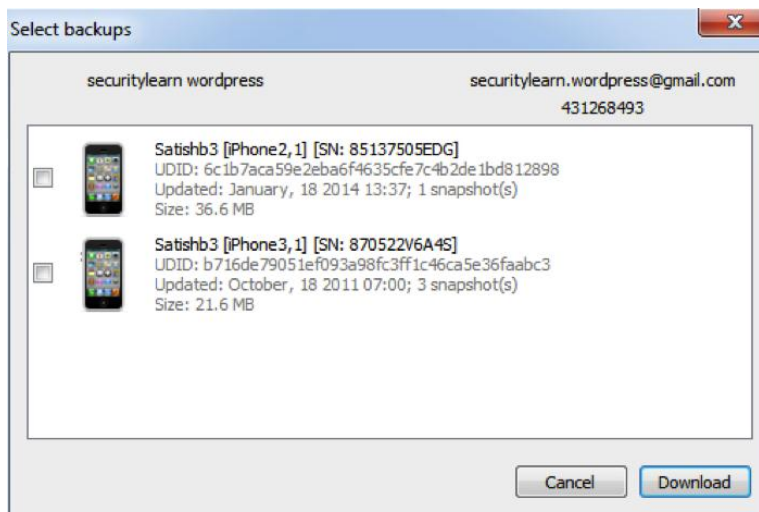
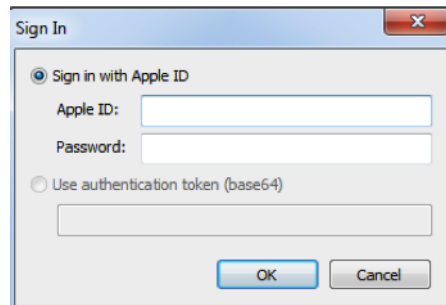
iPhone Password Breaker—Choose backup



iPhone Password Breaker—password brute force



iCloud backup toggle on the iPhone



## 5. iOS Data Analysis and Recovery

ZSPRECORD (61)	IRL▲	ZCONTENT	ZEXTID
ZSPTOPHIT (0)		Attachment 1 Image	message_guid=AAB17F24-7BE7-47B0-A60A-44B580182FCF
Z_METADATA (1)		Lower unit gone	message_guid=174142BB-7784-4EF5-A6DC-1254E4FA3AE4
Z_PRIMARYKEY (2)		What is the problem	message_guid=C2135048-6332-4CB6-AFEB-99A17E780B87
		Cruisin at 7 knots	message_guid=76351522-9509-4CD2-9C12-9613CF185A6A

The SMS Spotlight cache file

```
mbp-hmahalik:Webkit hmahalik$ cd /Users/
hmahalik/Desktop/Webkit/LocalStorage
mbp-hmahalik:LocalStorage hmahalik$ ls
StorageTracker.db
http.www.google.com_0.localstorage
http.m.youtube.com_0.localstorage
http.www.youtube.com_0.localstorage
http.www.bing.com_0.localstorage
https.m.facebook.com_0.localstorage
mbp-hmahalik:LocalStorage hmahalik$
```

The LocalStorage folder contents

Timestamp	MagneticX	MagneticY	MagneticZ	BiasX	BiasY	BiasZ	Level	Magnitude	Inclination
397825598.866...	1.000131249...	-5.6691226...	-33.6426...	-9.8247...	-33.572...	-74.7216...	3	34.1315841...	16.746786117553
397464520.501...	2.527702331...	36.5915298...	-9.59072...	-10.180...	-30.265...	-74.7932...	3	38.4508171...	19.300725936889
395677653.583...	29.69783592...	16.5588665...	-10.1030...	-17.953...	-42.845...	-71.7329...	3	43.5232200...	9.4296483993530
397278928.742...	35.99276351...	-4.1517596...	-17.9594...	-11.636...	-39.020...	-71.4378...	3	40.4383430...	23.143756866455
397526608.005...	9.358675003...	-25.768684...	-31.5292...	-16.420...	-42.946...	-67.5148...	3	40.7610816...	18.209178924560
395933819.072...	24.77676010...	-5.3470115...	-16.8228...	-10.536...	-39.333...	-68.1713...	3	30.4218235...	33.231529235839
395401386.925...	-32.7209167...	-26.507610...	-11.1854...	-21.658...	-43.165...	-67.6966...	3	43.4477310...	17.569580078125
397707111.257...	-34.8691444...	-18.540580...	1.463419...	-18.932...	-43.680...	-52.6133...	3	39.5190124...	30.580520629882
398008208.522...	-37.7201614...	-13.226410...	-1.76363...	-22.500...	-47.722...	-63.9044...	4	40.0107383...	20.924821853637
398626719.873...	-21.7697811...	-28.302036...	-10.4521...	-16.045...	-44.880...	-60.6969...	3	38.9990806...	21.757526397705
395596414.866...	-10.7783412...	-29.576835...	-28.8846...	-13.250...	-46.857...	-59.4609...	3	42.7233581...	23.430925369262
395681681.68238	-18.1000881...	-25.179094...	-28.4051...	-29.237...	-46.415...	-69.3532...	3	42.0529747...	44.917324066162
395681689.236...	-26.7571754...	11.4114971...	-28.8680...	-25.277...	-44.671...	-66.6357...	3	41.2897338...	33.963188171386
395933972.833...	-31.9908790...	-22.259635...	-29.7702...	-21.332...	-43.852...	-65.9417...	5	49.0426139...	36.140575408935
398157326.401...	-38.9373474...	-17.843893...	22.89932...	-19.085...	-46.388...	-65.1300...	3	48.8898010...	12.794839859008
395933824.298...	18.24590492...	-29.881649...	1.820023...	-13.694...	-41.850...	-67.1636...	3	35.0590744...	41.68013819580
395933831.094...	-18.6137428...	15.4992513...	17.41366...	-14.873...	-42.855...	-66.2310...	5	29.8317604...	32.763885498046
397837999.531...	-21.9664058...	28.1718273...	-26.0368...	-19.843...	-44.165...	-64.5132...	4	44.2051391...	20.393218994140
396881225.617...	37.02405548...	-21.706907...	-14.7401...	-18.227...	-44.392...	-63.9292...	5	45.3788871...	23.224666595458
396618096.706...	-18.8169689...	-46.284172...	-22.8564...	-18.789...	-43.364...	-61.3223...	3	56.9098930...	16.755559921264
396618102.170...	50.84199905...	-1.0987336...	-10.9434...	-19.307...	-42.917...	-61.5488...	4	52.0180130...	17.581190109252
398222060.053...	48.39217758...	12.6660327...	-13.6877...	-19.294...	-42.998...	-61.2228...	5	51.8612136...	15.281343997192
397464529.130...	6.932649612...	35.1686248...	-31.5720...	-11.293...	-32.009...	-71.6104...	3	47.7670402...	23.336816787719
398626731.556...	-39.4483909...	-7.5617275...	6.797387...	-16.782...	-39.792...	-61.5390...	4	40.7376976...	20.442686080932
398626743.471...	-20.5659294...	28.8992786...	-21.4836...	-16.367...	-39.818...	-62.2913...	5	39.8598060...	17.258197784423

The Consolidated.db view with SQLite Professional

en\_GB-dynamic-text.dat

```

0000 44 79 6E 61 6D 69 63 44 69 63 74 69 6F 6E 61 72 79 20 35 00 00 01 F2 61 70 69 73 00 67 6F 64 2E 00
0023 60 79 2E 2E 65 60 61 69 6C 2E 2E 74 61 68 65 2E 2E 63 61 72 65 2E 2E 60 65 73 61 67 65 2E 2E 73 65 6E
0046 64 69 6E 67 2E 2E 74 6F 2E 2E 64 61 79 00 2E 2E 60 65 65 74 2E 2E 2E 60 65 2E 2E 2E 6F 6E 2E 2E 2E 61 64
0069 64 72 65 73 73 2E 2E 62 72 69 6E 67 2E 2E 60 6F 6E 65 79 2E 2E 2E 67 65 74 2E 2E 2E 2E 68 65 79 73
008C 2E 2E 2E 6F 70 65 6E 2E 2E 2E 63 68 65 63 68 2E 2E 64 72 75 67 2E 2E 2E 63 6F 6E 74 61 63 74 2E 2E
00AF 2E 2E 63 6F 6E 63 65 72 6E 2E 2E 62 72 69 74 68 2E 2E 2E 64 63 79 2E 2E 2E 63 68 6F 63 6C 61 74 65
00D2 2E 2E 2E 2E 69 70 68 6F 6E 65 2E 2E 2E 66 6F 72 65 6E 73 69 63 73 2E 2E 2E 68 61 63 68 69 6E 67 2E
00F5 2E 2E 2E 74 65 70 74 2E 2E 2E 6C 6F 76 65 2E 2E 2E 68 65 70 2E 2E 2E 73 61 74 69 73 68 2E 2E 2E 2E
0118 0A 44 4E 64 7E 00 4D 69 6D 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E 6E
  
```

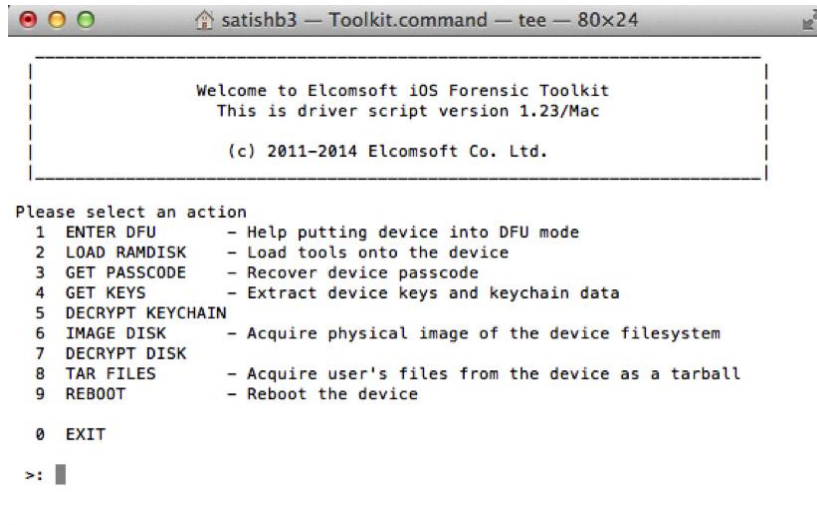
Type: Value

- 8 bit signed
- 8 bit unsig...
- 16 bit signed
- 16 bit uns...
- 32 bit uns...

Hex Little Endian Insert ASCII Offset: 118 Selection: 0

Keyboard cache in hex editor

## 6. iOS Forensic Tools



```
satishb3 — Toolkit.command — tee — 80x24

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 1.23/Mac

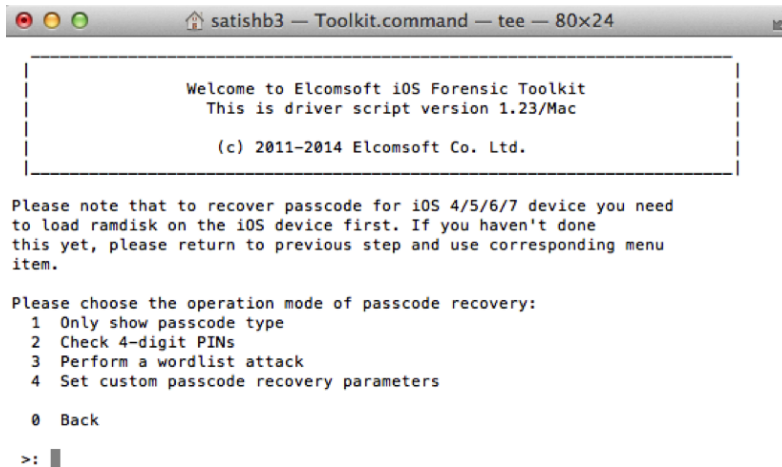
(c) 2011-2014 Elcomsoft Co. Ltd.

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

0 EXIT

>: █
```

The Elcomsoft iOS Forensic Toolkit welcome screen



```
satishb3 — Toolkit.command — tee — 80x24

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 1.23/Mac

(c) 2011-2014 Elcomsoft Co. Ltd.

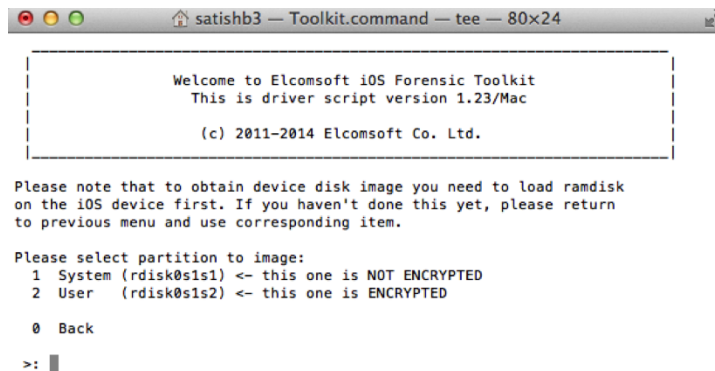
Please note that to recover passcode for iOS 4/5/6/7 device you need
to load ramdisk on the iOS device first. If you haven't done
this yet, please return to previous step and use corresponding menu
item.

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

0 Back

>: █
```

The Elcomsoft iOS Forensic Toolkit welcome screen



```
satishb3 — Toolkit.command — tee — 80x24

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 1.23/Mac

(c) 2011-2014 Elcomsoft Co. Ltd.

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

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

0 Back

>: █
```

The EIFT passcode recovery options

		Physical imaging	Logical imaging	Passcode recovery	Keychain decryption	Disk decryption
iPhone iPhone 3G iPod Touch 1 iPod Touch 2	iOS 1/2/3	+	+	instant <sup>2)</sup>	+	not encrypted <sup>3)</sup>
	iOS 4	+	+	+	+	not encrypted <sup>3)</sup>
iPhone 3GS iPod Touch 3 iPad 1	iOS 3	+	+	instant <sup>2)</sup>	+	not encrypted <sup>3)</sup>
	iOS 4/5	+	+	+	+	+ <sup>4)</sup>
iPhone 4 iPod Touch 4	iOS 4/5/6/7	+	+	+	+	+
iPhone 4S iPhone 5 iPhone 5C iPad 2-4 iPad Mini iPod Touch 5	iOS 5/6/7	+	+	+	+	+

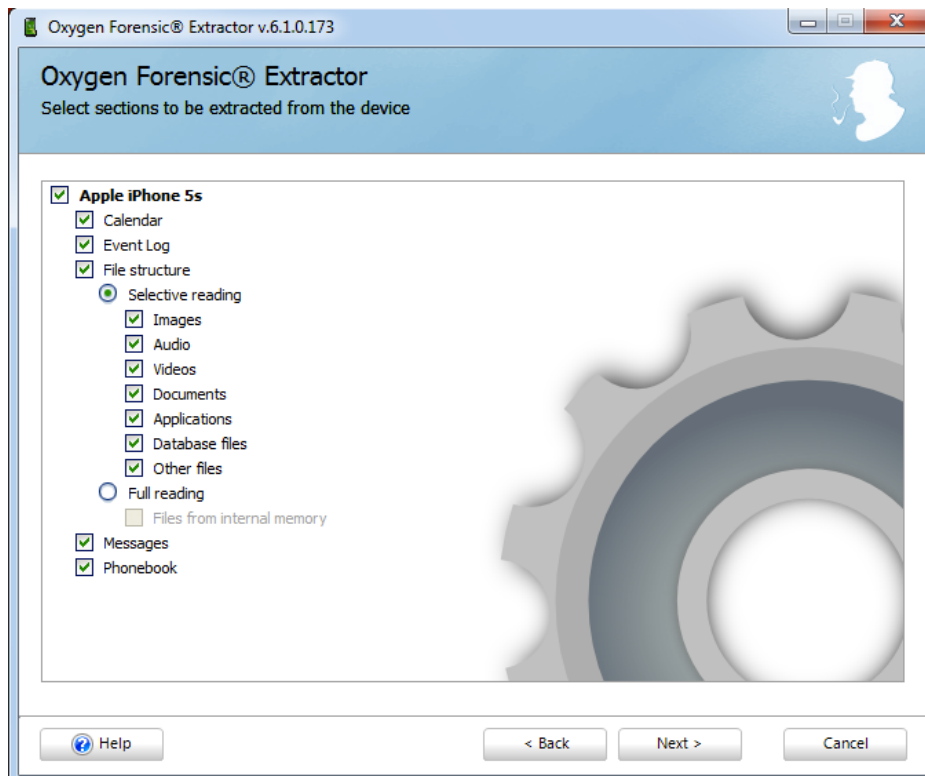
E1FT supported devices

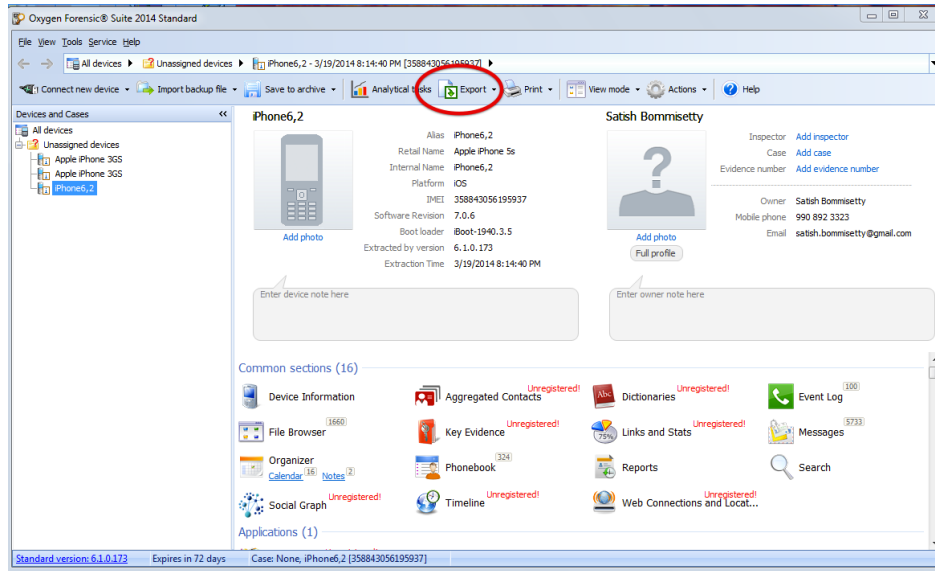


Oxygen Forensic Suite—the Connection Mode screen

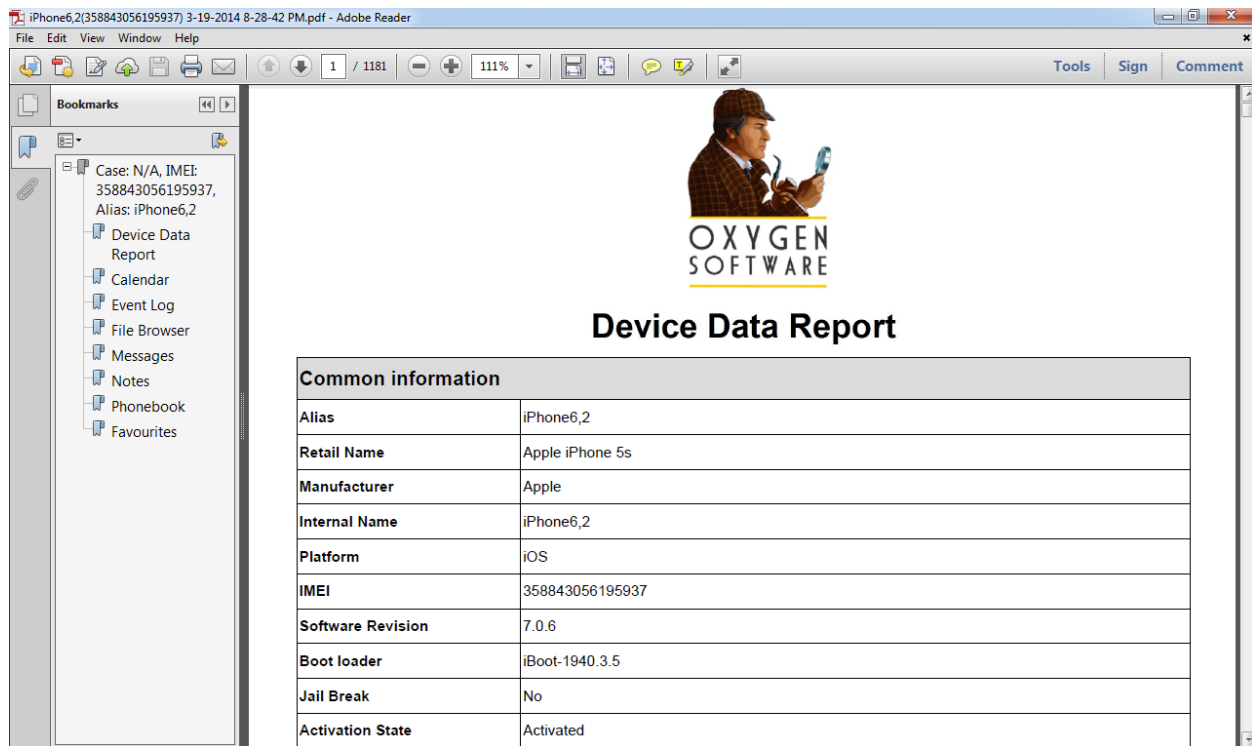


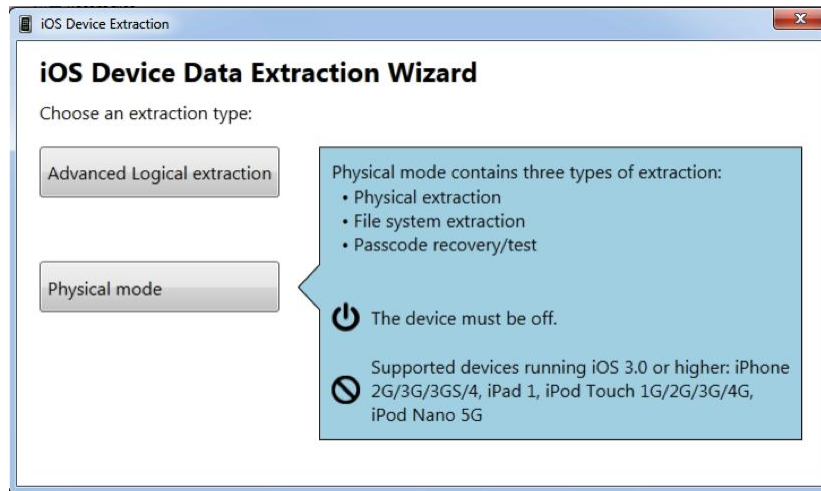
Oxygen Forensic Suite—the device information screen



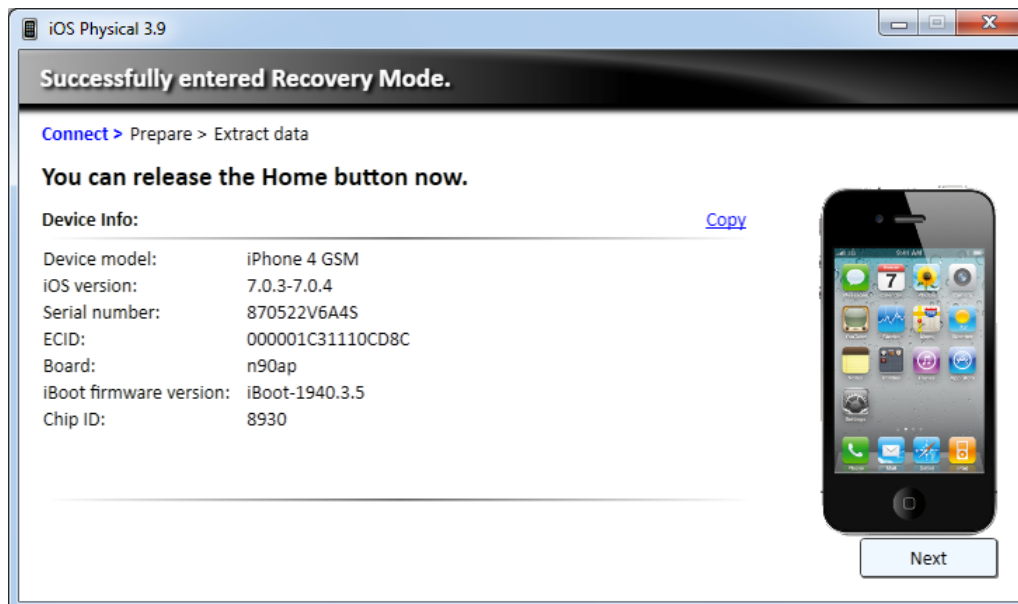


Oxygen Forensic Suite—the extracted data summary screen





UFED Physical Analyzer—the iOS Device Data Extraction Wizard screen

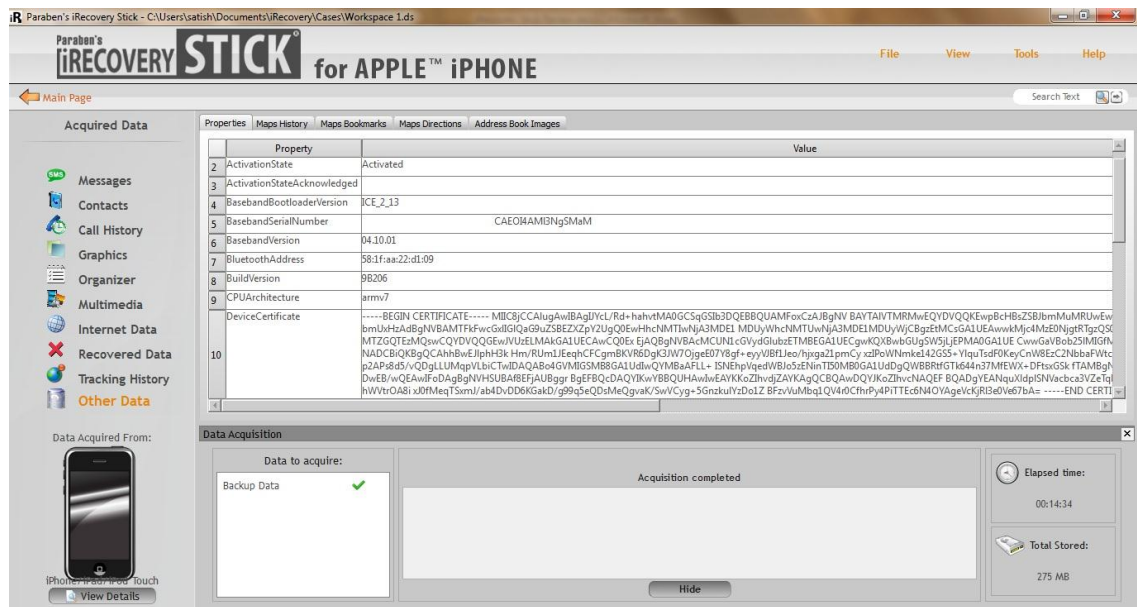


UFED Physical Analyzer—the device information screen



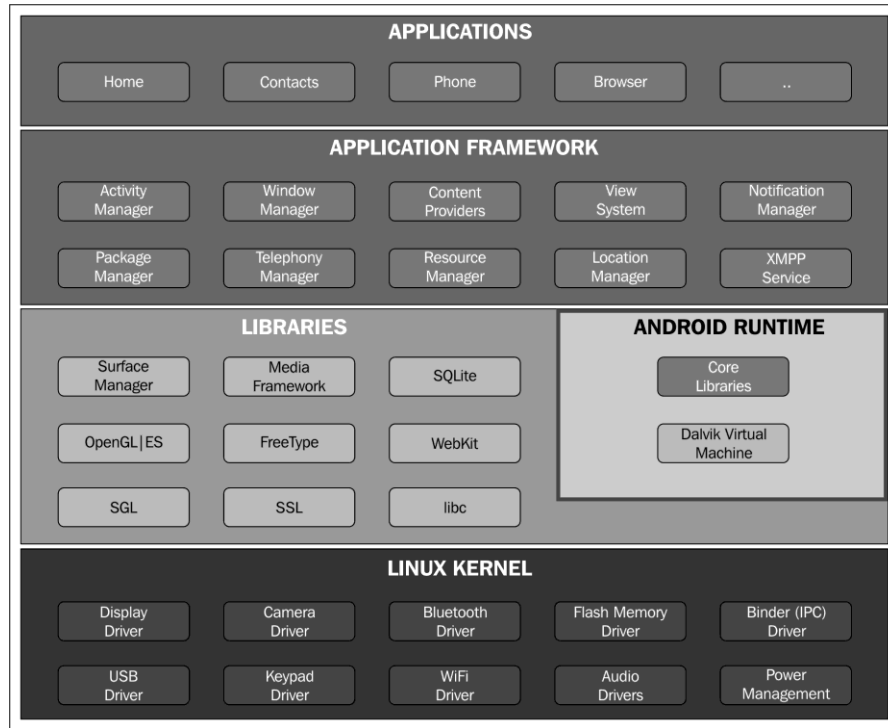


iRecovery Stick—the Choose connected device screen

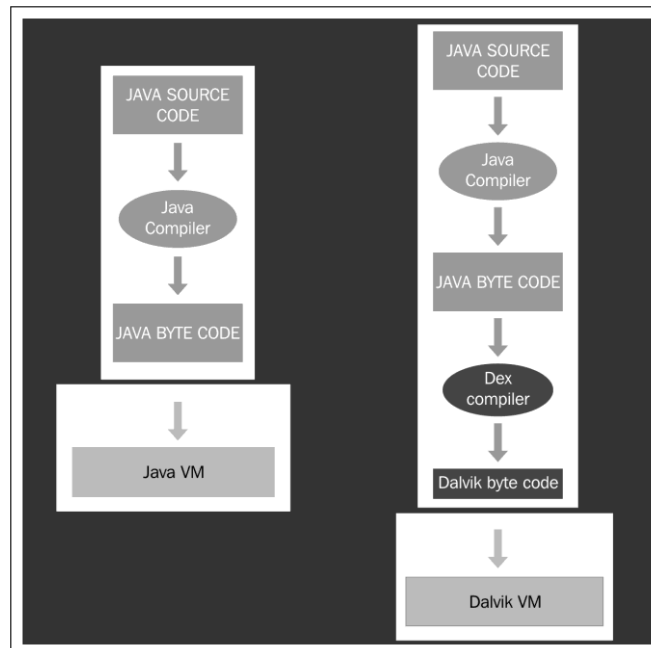


iRecovery Stick—the Choose connected device screen

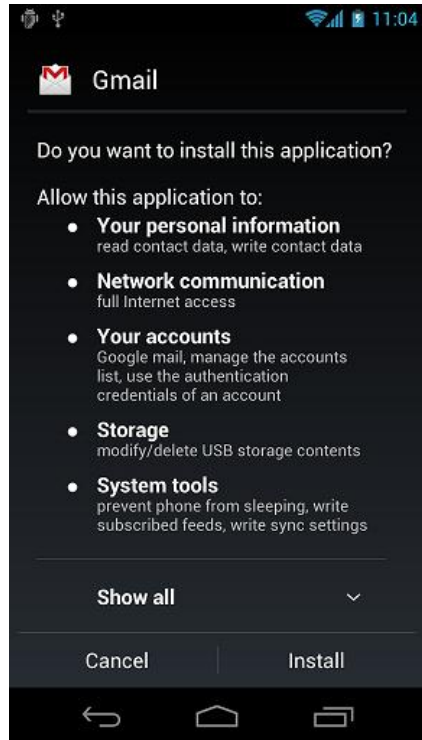
# 7. Understanding Android



Android architecture



JVM versus DVM

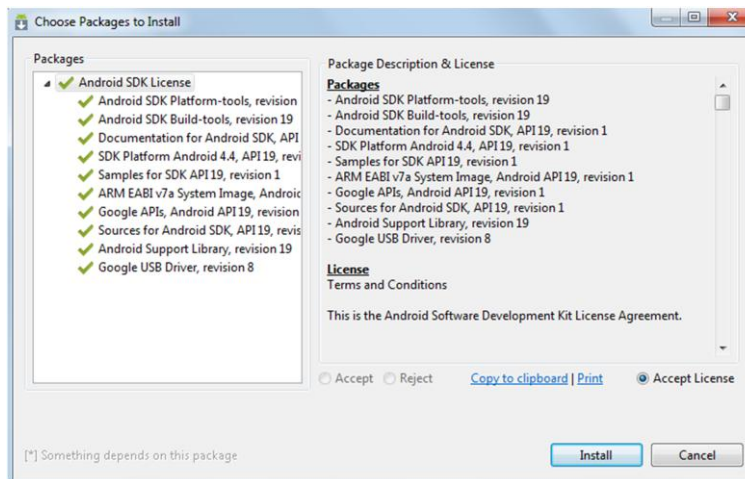


The permission model in Android

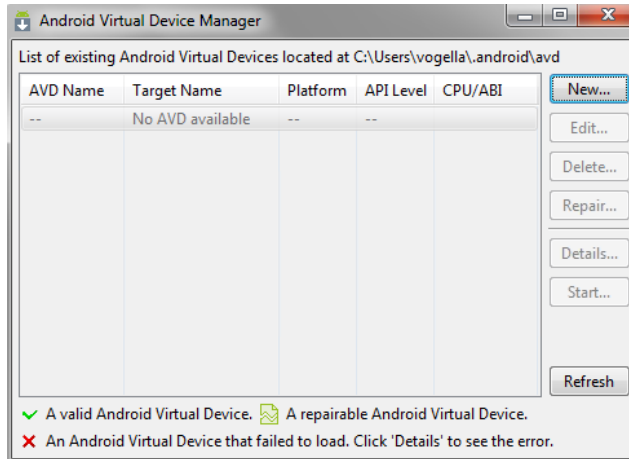
## 8. Android Forensic Setup and Pre Data Extraction Techniques



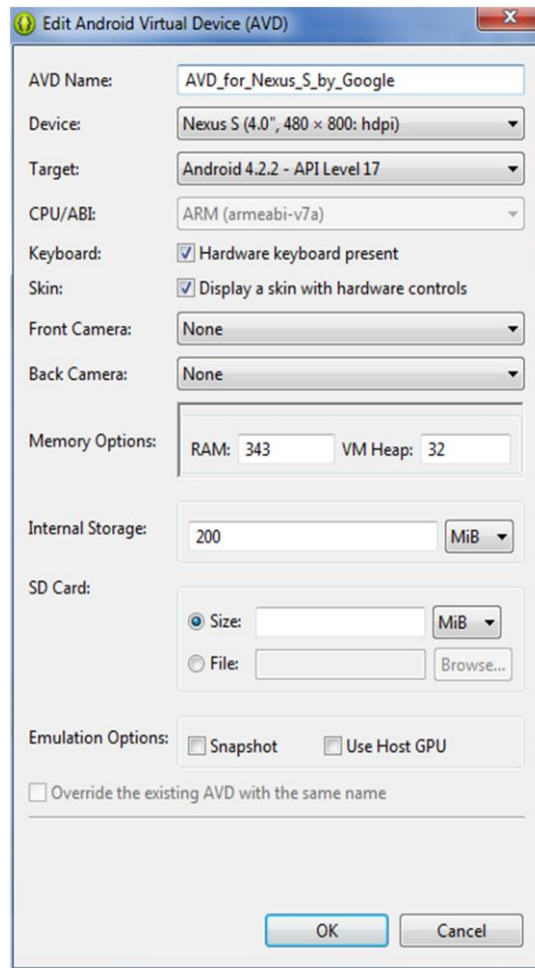
Android SDK Tools setup wizard



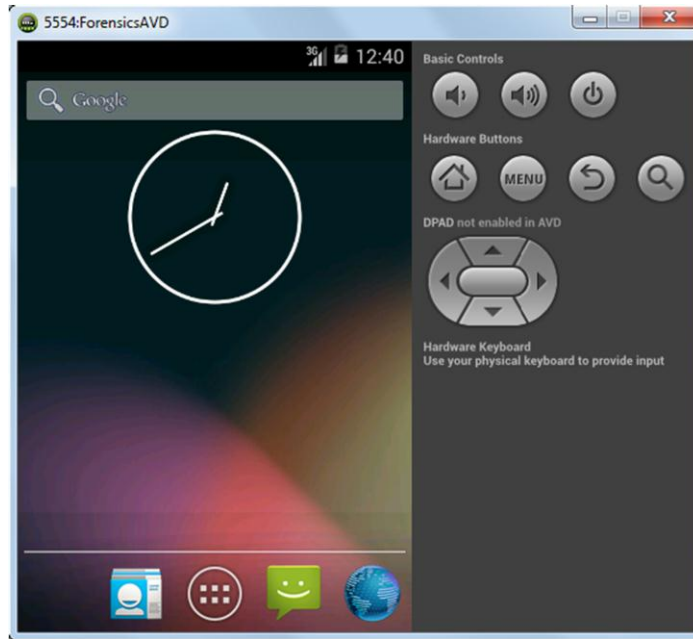
Android SDK License



Android Virtual Device Manager



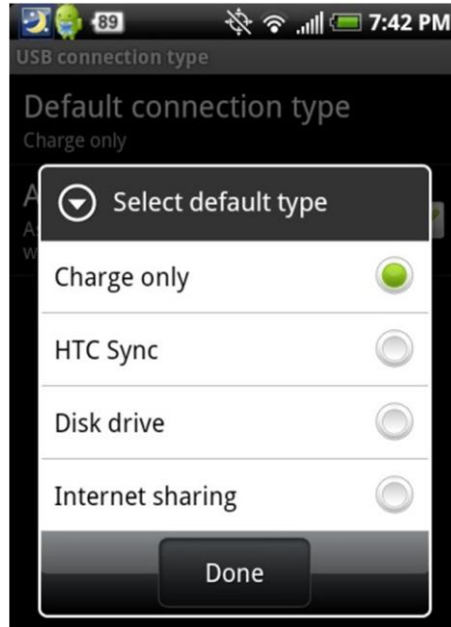
Virtual device configuration



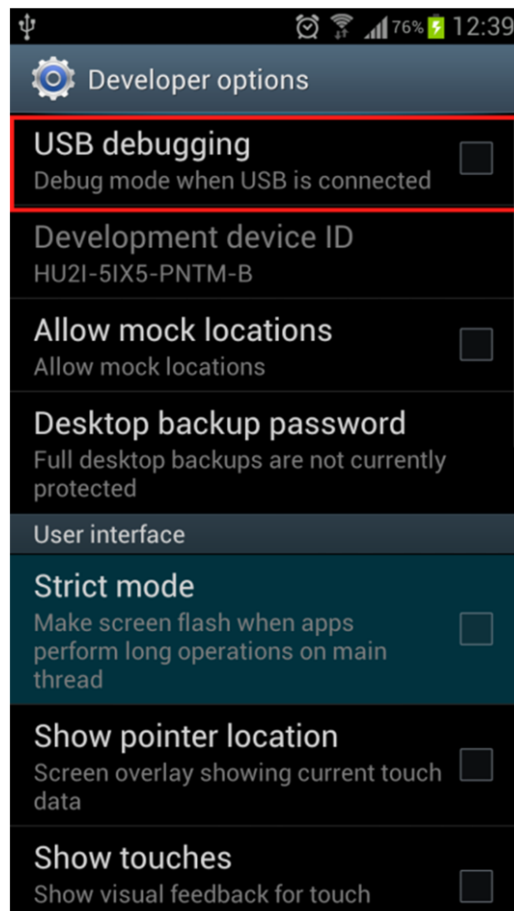
The Android emulator



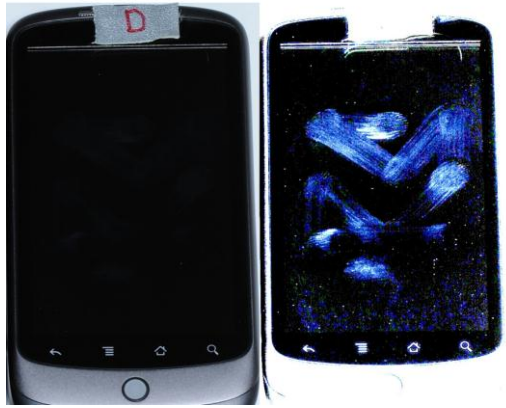
USB mass storage



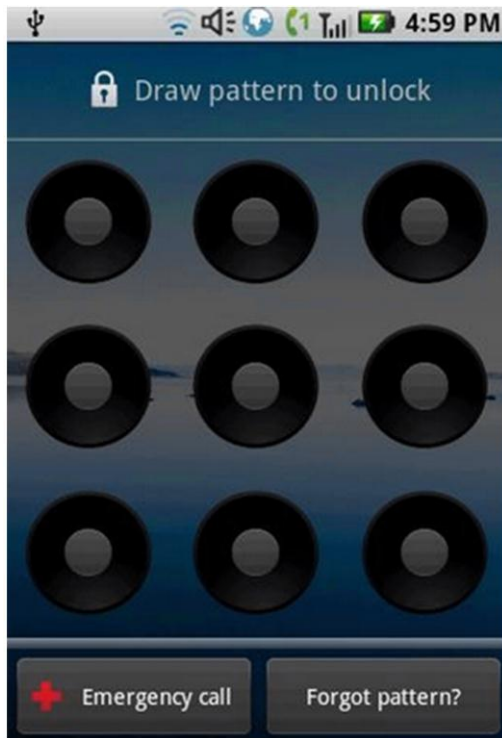
HTC mobile USB options



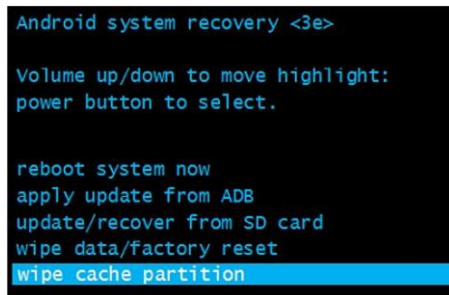
The USB debugging option in Samsung mobiles



Smudges visible on a device under proper lighting (source: <https://viaforensics.com/wpinstall/wp-content/uploads/smudge.png>)

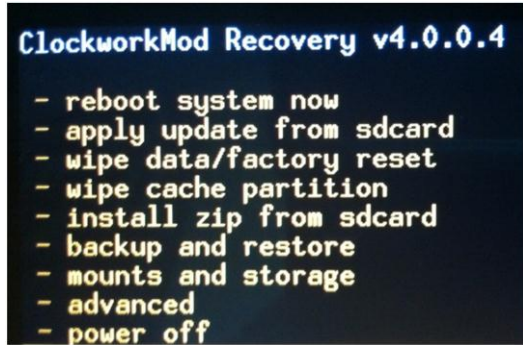


Forgot pattern option on an Android device

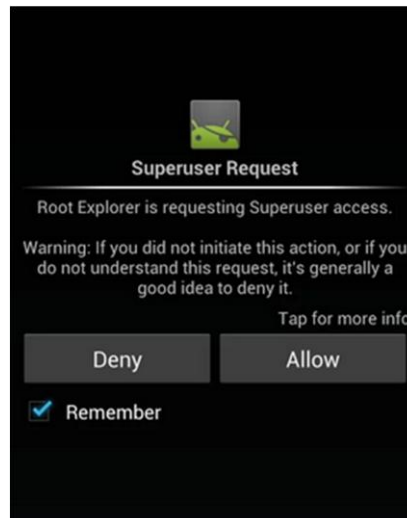


Normal Android system recovery mode





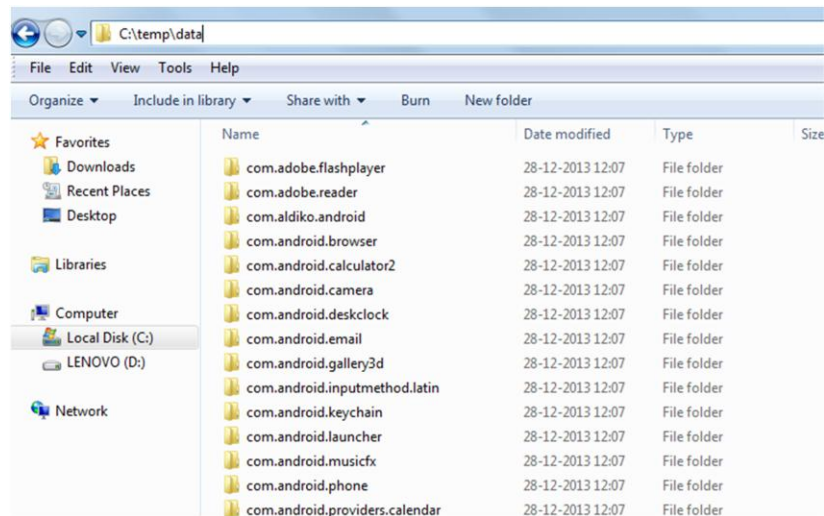
Modified recovery mode



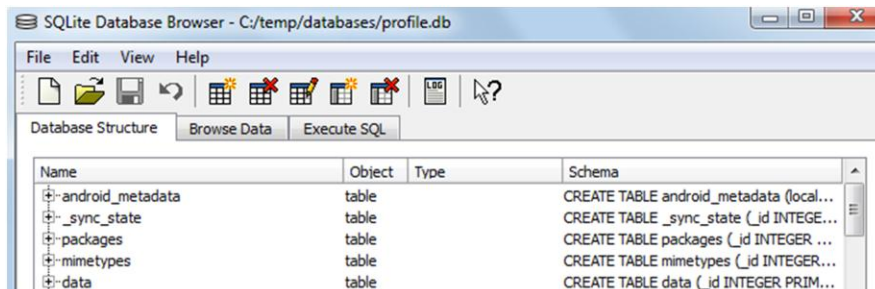
Application requesting root access

## 9. Android Data Extraction Techniques

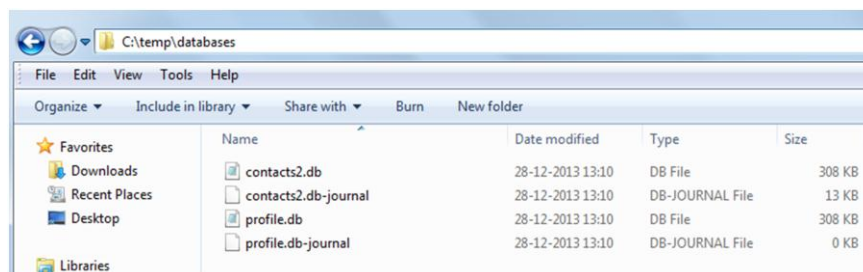
```
platform-tools -- adb -- 80x24
Last login: Mon May 5 11:47:35 on ttys000
mbp-hmahalik:~ hmahalik$ cd /Users/hmahalik/Desktop/Android\ Tools\adt-bundle-ma
c-x86_64-20140321/sdk/platform-tools
mbp-hmahalik:platform-tools hmahalik$ ./adb install /Users/hmahalik/Desktop/Andr
oid\ Tools\Term.apk
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
```



The /data directory extracted to a forensic workstation



SQLite Browser



The contacts2.db file copied to a local folder

Database Structure Browse Data Execute SQL

Table: calls

	id	number	date	duration	type	new	name
1	1	777777777	1388206471836		11	2	0 Tom
2	2	8887775566	1388206593826		5	2	0
3	3	4444444444	1388211842729		134	2	0 Robert
4	4	6666666666	1388211997835		4	2	0 Amy
5	5	9999999999	1388212023730		1	2	1 James

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

Calls table in the contacts2.db file

browser2.db - Oxygen Forensic SQLite Viewer

File Tools Service Help

Open Export Print Analyze Deleted Data Options Help

Tables

- \_sync\_state (0/0)
- \_sync\_state\_metadata (0/0)
- android\_metadata (1/0)
- bookmarks (15/0)
- history (14/0)
- images (24/0)
- searches (4/0)
- settings (1/0)
- sqlite\_sequence (3/0)
- thumbnails (1/0)

Table data

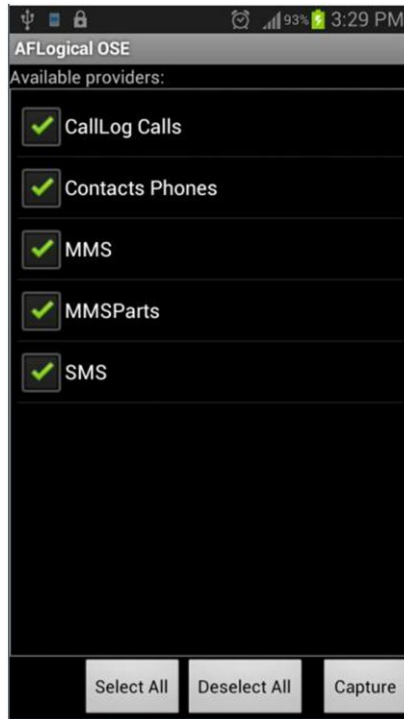
#	_id	title	url
1	1	Goo<TRIAL>	https://www.google.com/w<TRIAL>XXXXXX
2	2	test - Goo<TRIAL>XXX	https://www.google.com/search?source=android-home&...
3	3	test - Goo<TRIAL>XXX	https://www.google.com/search?site=webhp&ei=8Ze2U...
4	4	Goo<TRIAL>	https://www.google.co.in/?gws_<TRIAL>XXXXXX
5	5	Welcome t<TRIAL>XXX	https://m.facebook.com/?refsrc=htt<TRIAL>XXXXXX
6	6	google - Go<TRIAL>XXXX	http://www.google.com/m?hl=en&sou<TRIAL>XXXXXX
7	7	forensics - <TRIAL>XXXXXX	http://www.google.com/search?hl=en&source=android-...
8	8	Forensic science - Wikiped<TRIAL>XXXXXX	http://en.m.wikipedia.o<TRIAL>XXXXXX
9	9	facebook - G<TRIAL>XXXX	http://www.google.com/m?hl=en&sour<TRIAL>XXXXXX
10	10	Welcome t<TRIAL>XXX	https://m.facebook.com/?refsrc=h<TRIAL>XXXXXX
11	11	Wiki<TRIAL>	http://www.w<TRIAL>XXXXXX
12	12	us airways - <TRIAL>XXXXXX	http://www.google.com/m?hl=en&source<TRIAL>XXXXXX
13	13	US Airways   Airline tickets<TRIAL>XXXXXX	http://mobile.usairways.com/mt/www<TRIAL>XXXXXX
14	14	shopping - G<TRIAL>XXXX	http://www.google.com/m?hl=en&sour<TRIAL>XXXXXX

The browser2.db file in Oxygen Forensic SQLite Viewer

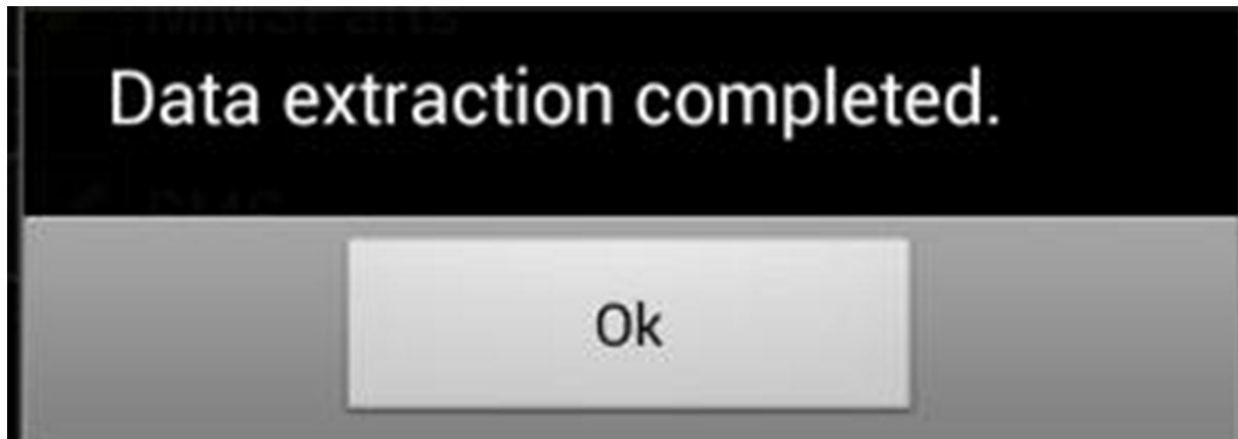
Table: friends\_data

id	user id	first name	last name	cell	other	email	birthday month
1	1	100004087623668	Lavanya			lavanya100004087623668@gmail.com	2
2	2	100000005601801	Pranav	M			-1
3	3	100004630714031	Sujata	P	+919800000000		4
4	4	100000818058433	Sudha	C		sudha100000818058433@yahoo.com	1
5	5	100003499121241	Vasu	N	+919600000000	vasundevanarayanan@gmail.com	7
6	6	100003191641871	Makka	A	+918100000000	makka100003191641871@gmail.com	12
7	7	1033892411	Sai	Bl	+919940000000	saikumarbhatnagar@gmail.com	9
8	8	100002190061552	Vara	K		varanarayanan@yahoo.com	3
9	9	100002328888334	Kaluri	A	+918680000000	kaluri100002328888334@gmail.com	6
10	10	100000103323292	E	R	+919700000000	pithambareddy@yahoo.com	-1
11	11	562618335	Mukesh	K	+919800000000	mukesh10000562618335@yahoo.com	2

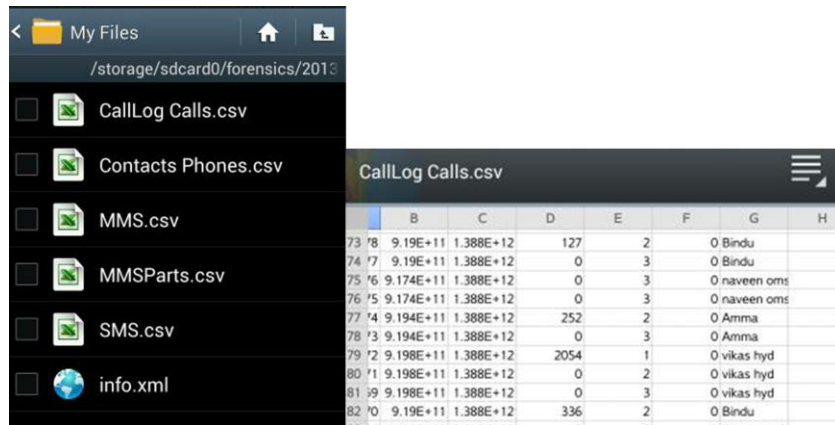
The fb.db file in SQLite browser



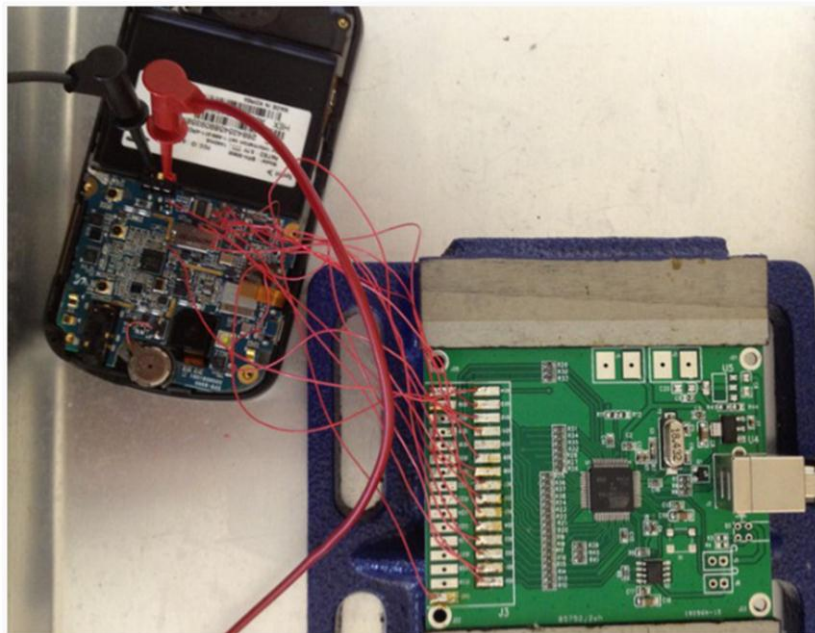
The AFLogical OSE app



Message displayed after the extraction is complete



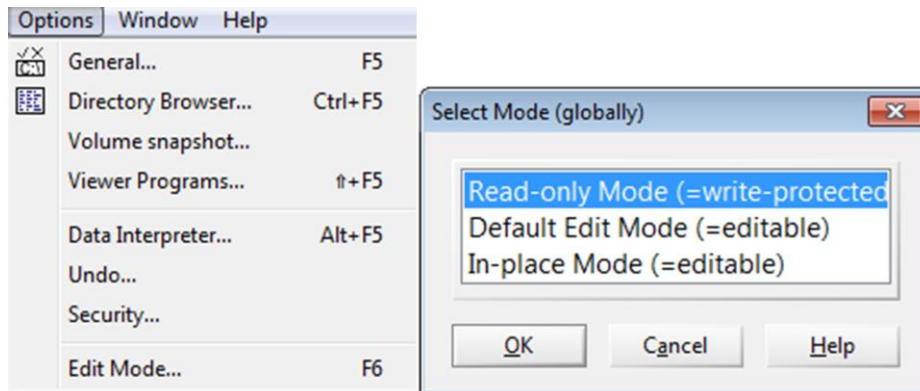
Files extracted using AFLogical OSE



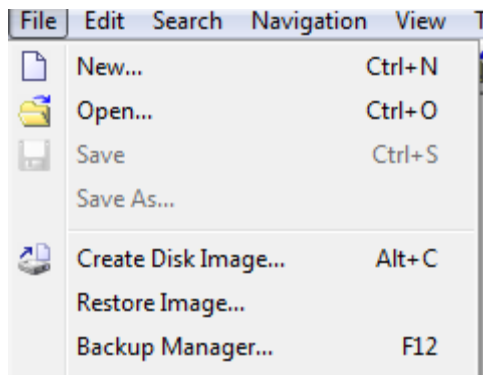
The JTAG setup



The chip-off technique

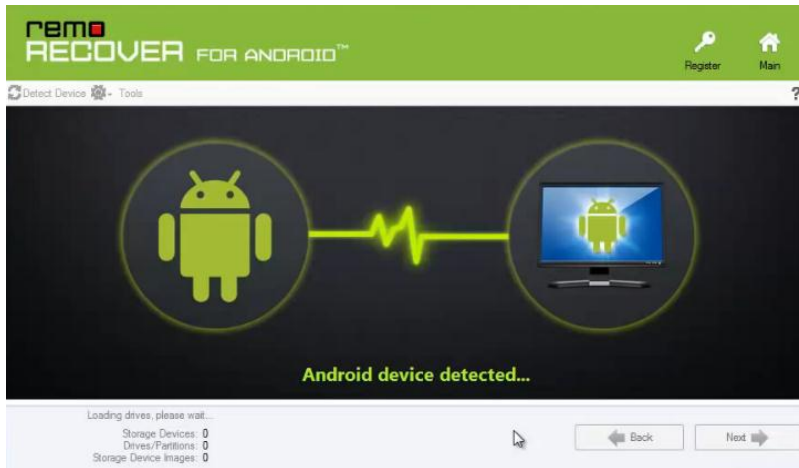


WinHex view of Edit Mode (left) and WinHex Read-only Mode enabled (right)

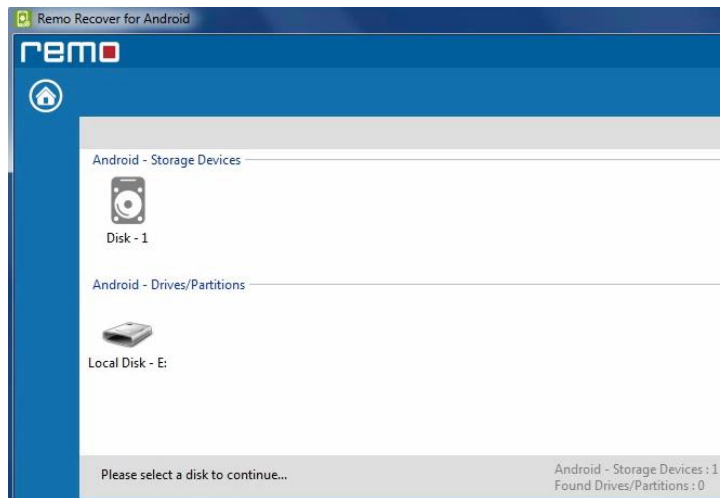


The WinHex disk image option

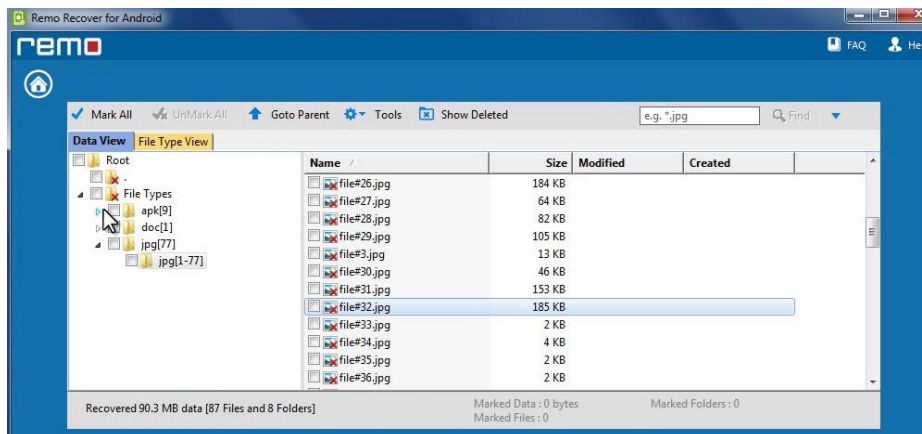
# 10. Android Data Recovery Techniques



Android recovery—device detection

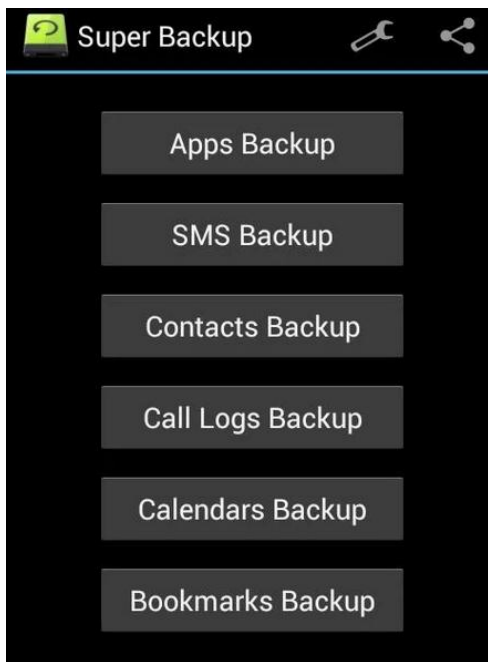


The list of storage devices available

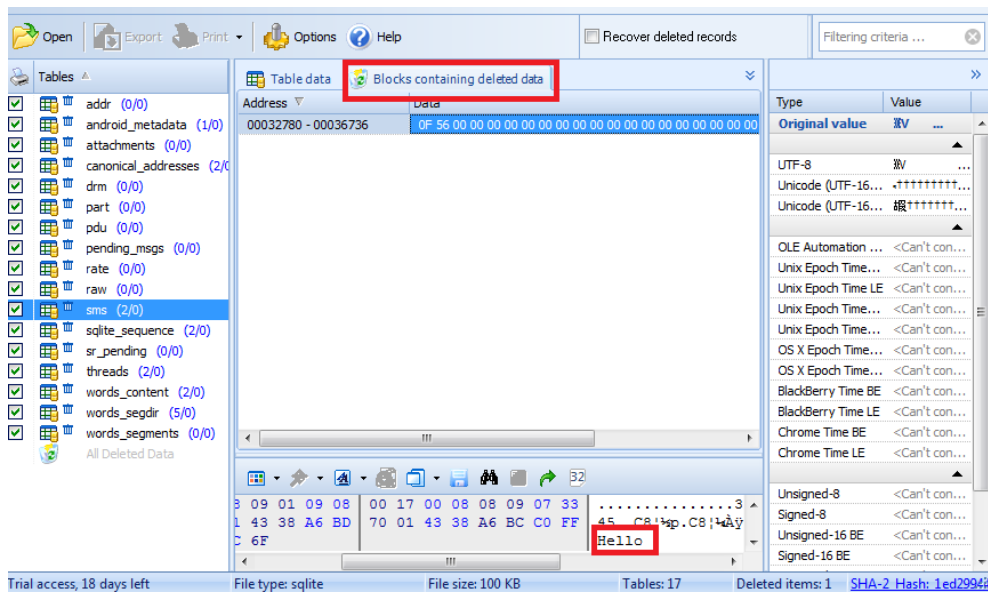


Recovered files list





The Super Backup Android app



Recovering deleted SMS messages

```

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

```

The scalpel configuration file

```

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

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

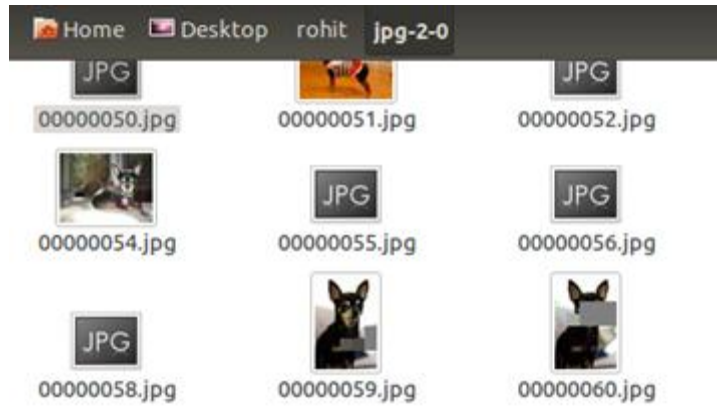
Image file pass 1/2.
/home/unigeek/Desktop/userdata.dd: 100.0% |*****| 3.9 MB 00:00 ETA
Allocating work queues...
Work queues allocation complete. Building carve lists...
Carve lists built. Workload:
gif with header "\x47\x49\x46\x38\x37\x61" and footer "\x00\x3b" --> 0 files
gif with header "\x47\x49\x46\x38\x39\x61"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

```

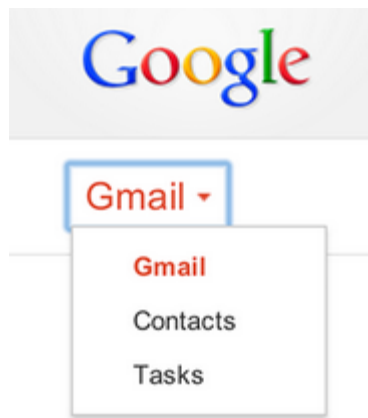
Running the Scalpel tool on a dd file



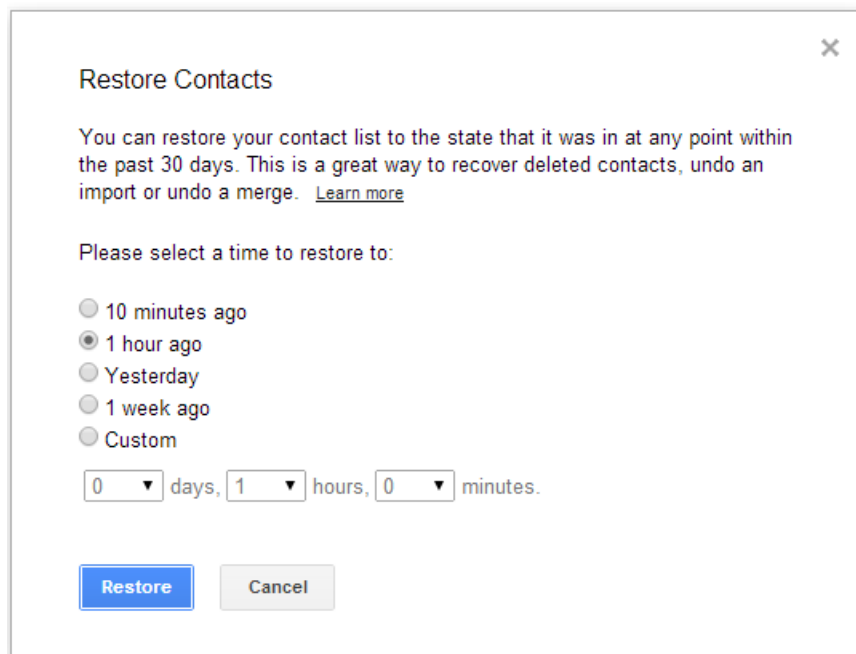
Output folder after running the Scalpel tool



Recovered data using the Scalpel tool

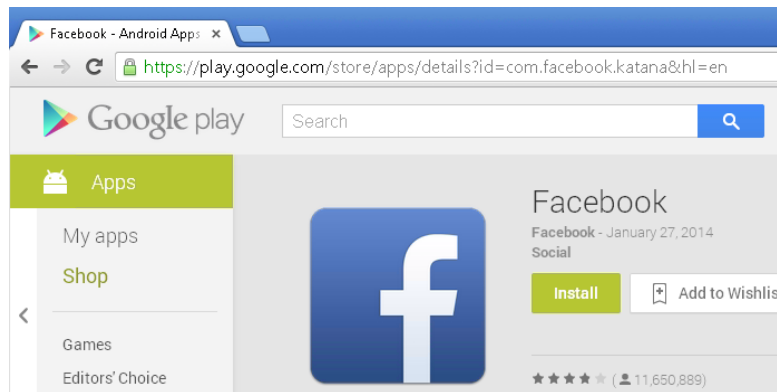


The Contacts menu in Gmail



The Restore Contacts dialog box

## 11. Android App Analysis and Overview of Forensic Tools



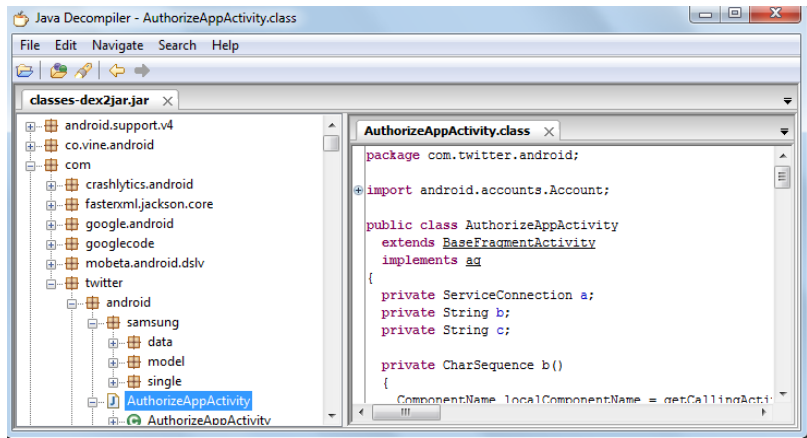
Facebook App in Google Play Store

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

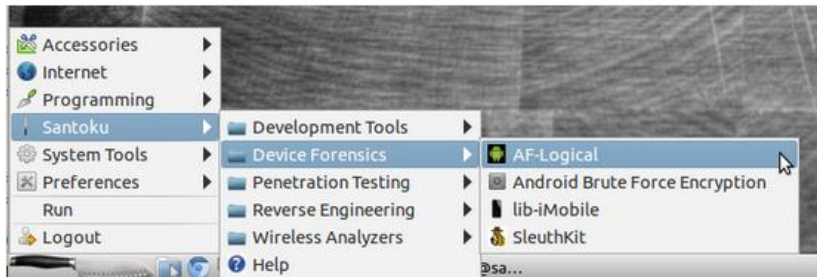
Extracted files of an APK file

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

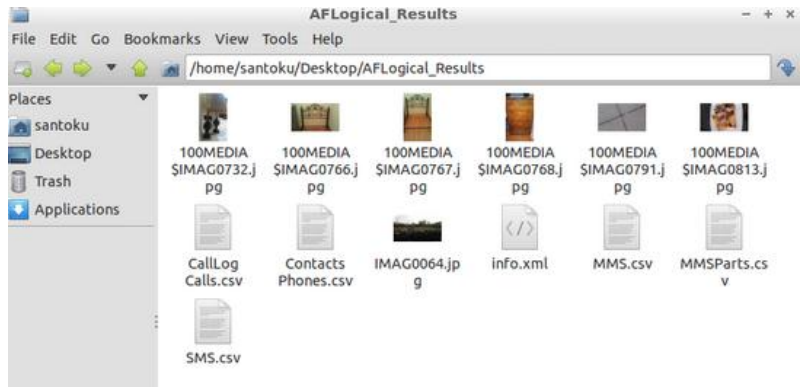
The classes-dex2jar.jar file created by the dex2jar tool



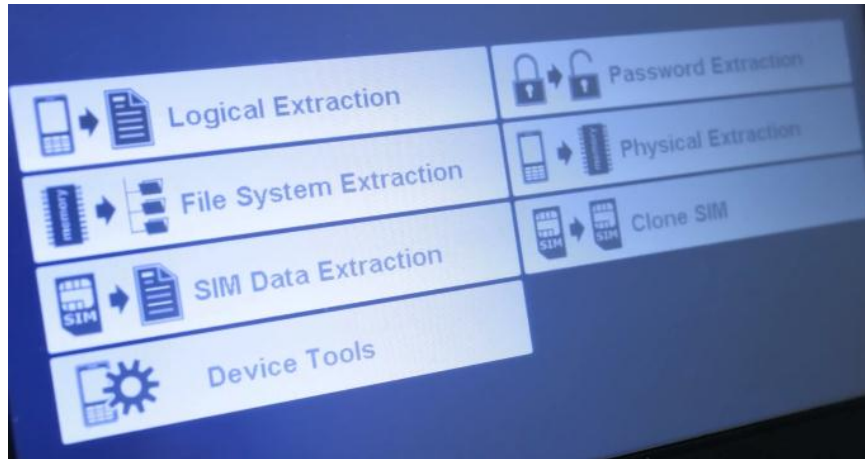
The JD-GUI tool



AFLogical in Santoku Linux



The AFLogical results



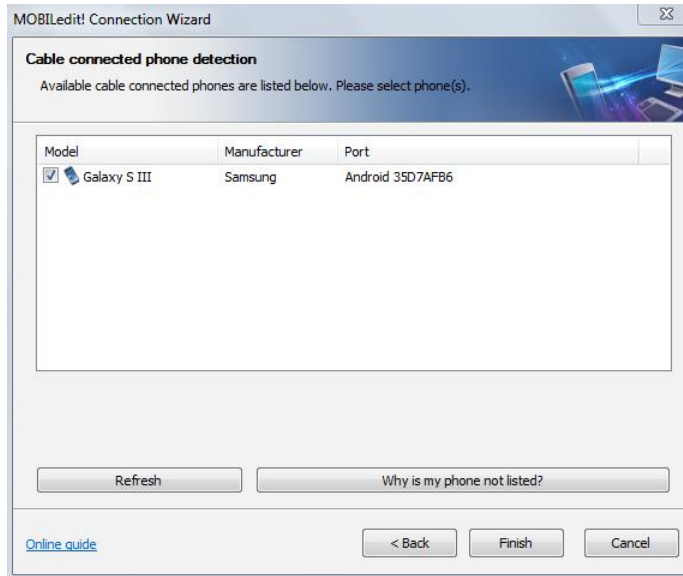
The UFED Touch main menu



The UFED touch—vendor list screen



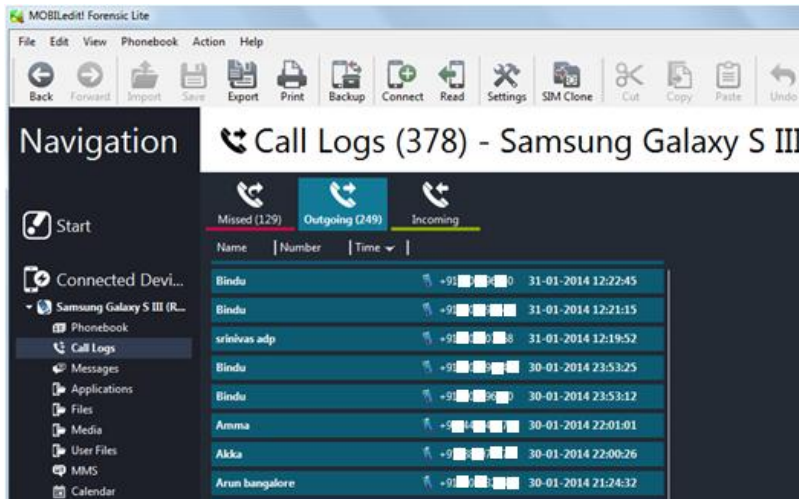
The UFED Physical Analyzer application



The MOBILedit connection wizard



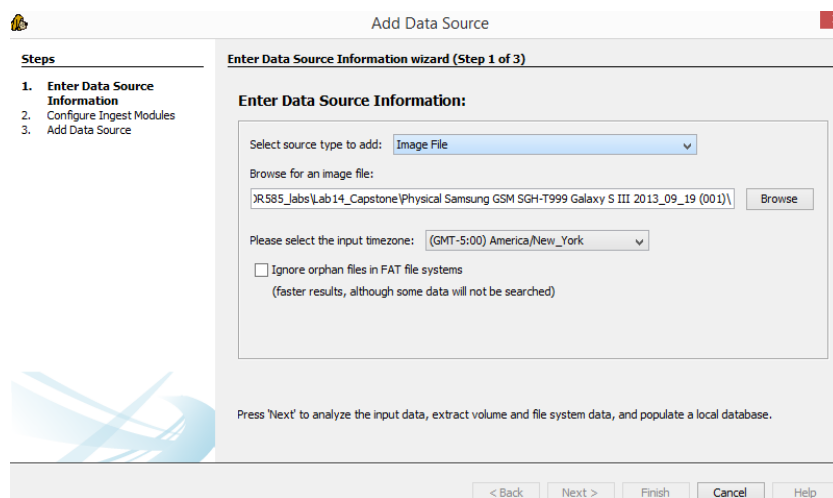
The MOBILedit connection wizard



The MOBILedit tool—Call logs option

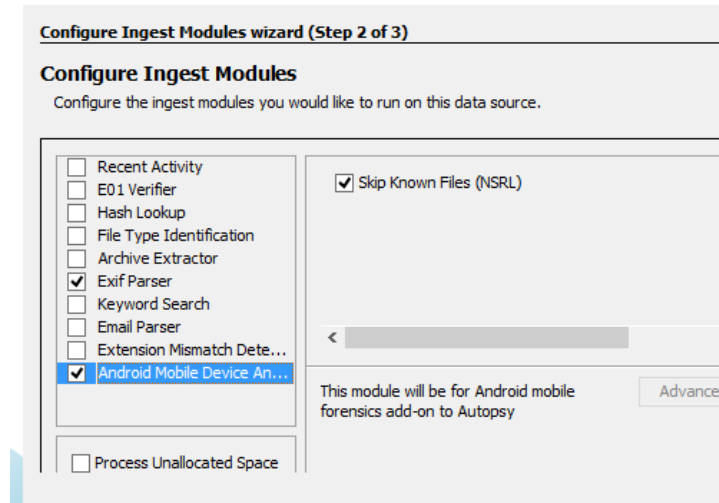


The Autopsy tool screen

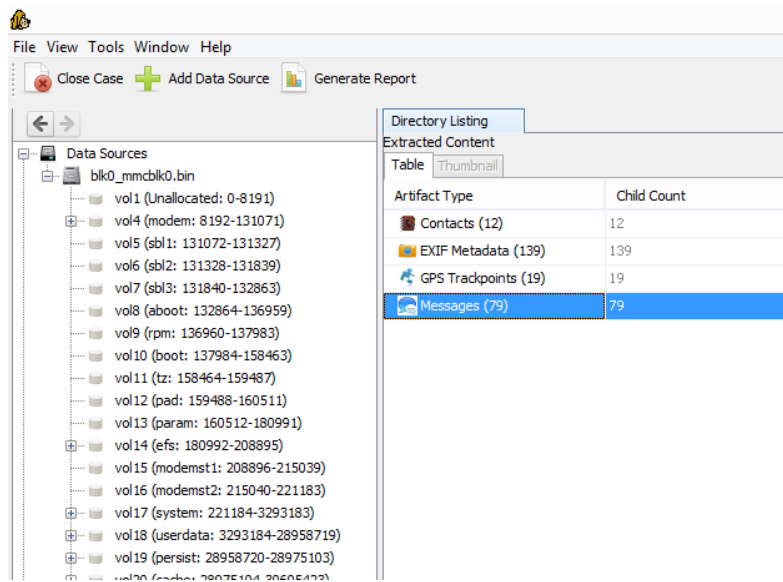


Autopsy image loading



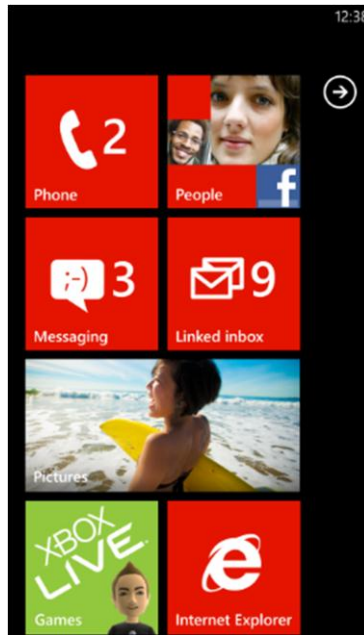


Autopsy ingest modules

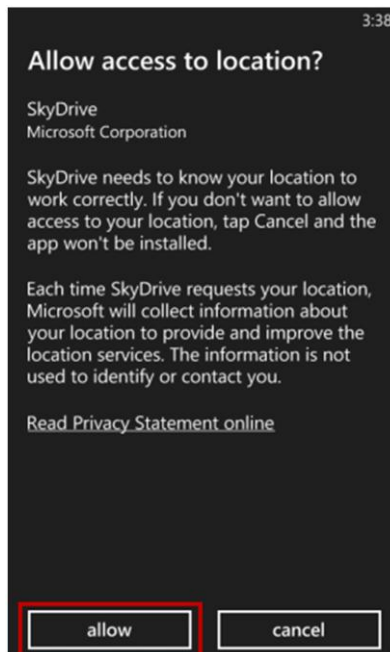


Autopsy results

# Windows Phone Forensics



The Windows Phone home screen



Windows app requesting user permissions



The ChevronWP7 tool



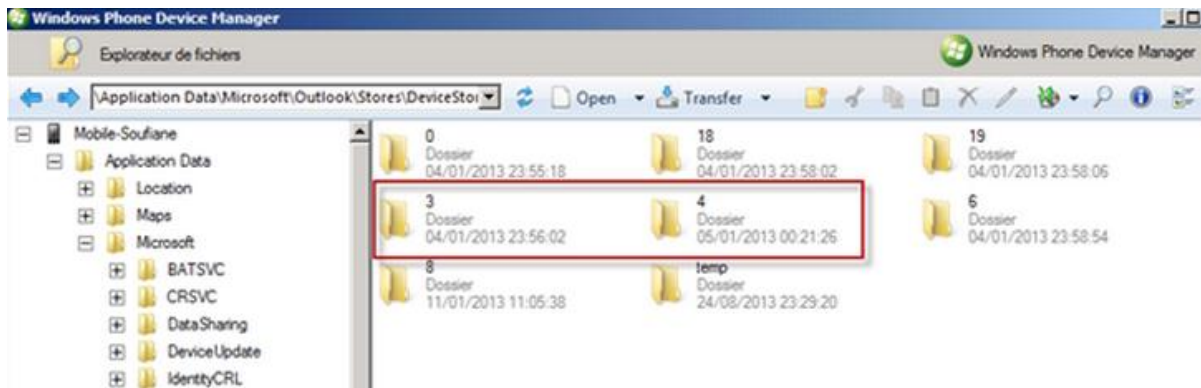
Windows Phone Device Manager

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

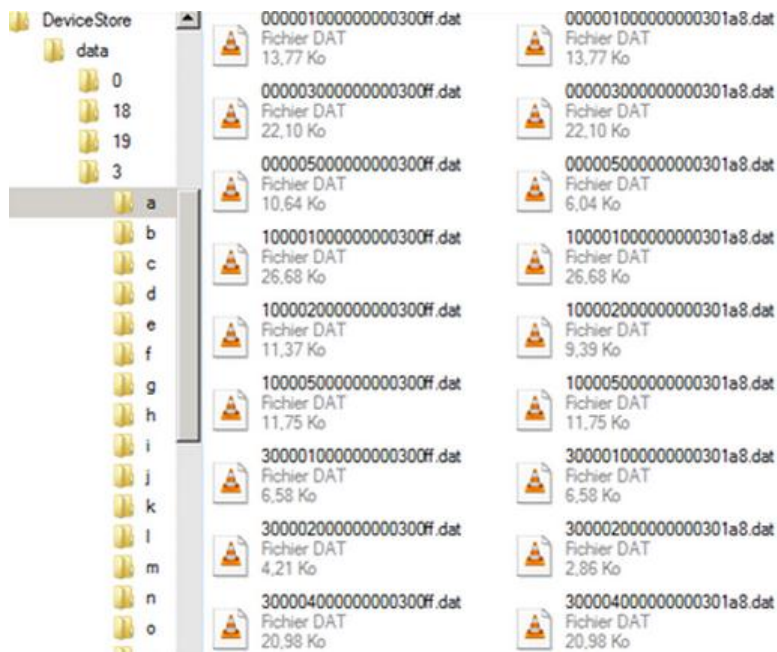
Windows Phone Device Manager—The Manage Applications screen



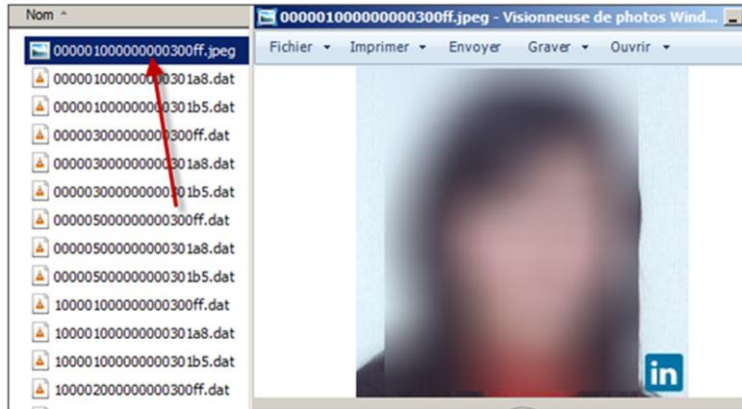
The store.vol file in Windows Phone



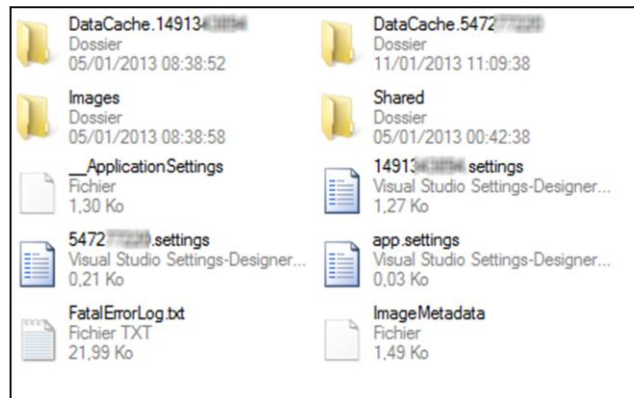
Windows Phone: extracting e-mail



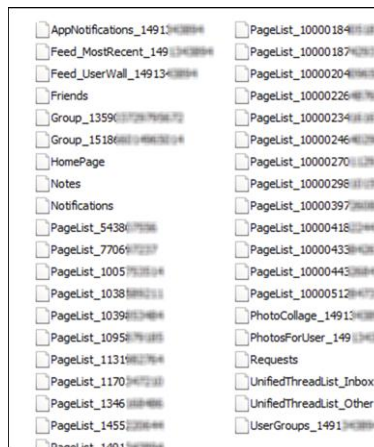
Windows Phone: folder 3



Windows Phone: renaming data files to JPG files

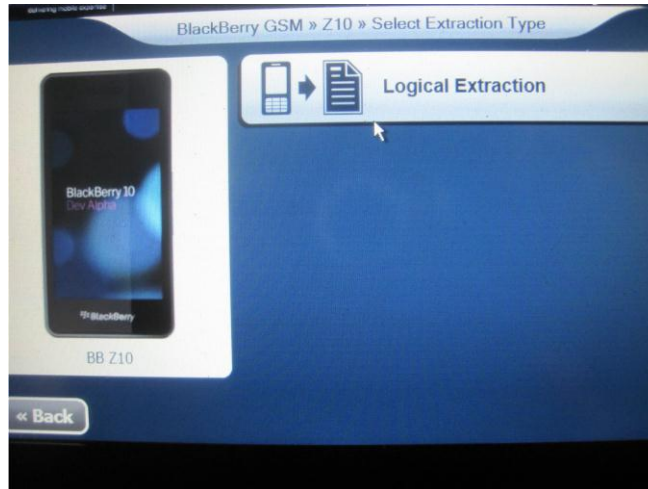


Contents of the IsolatedStore folder

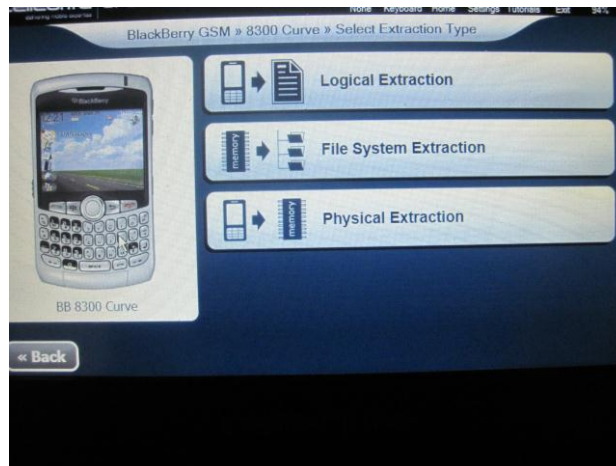


The DataCache.UserID folder of the Facebook app

## 13. BlackBerry Forensics



The BlackBerry Z10 support in Cellebrite UFED Touch



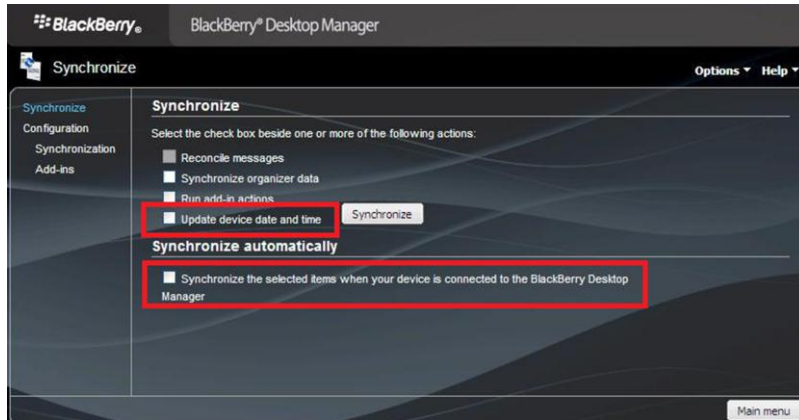
The BlackBerry Curve support in Cellebrite UFED Touch



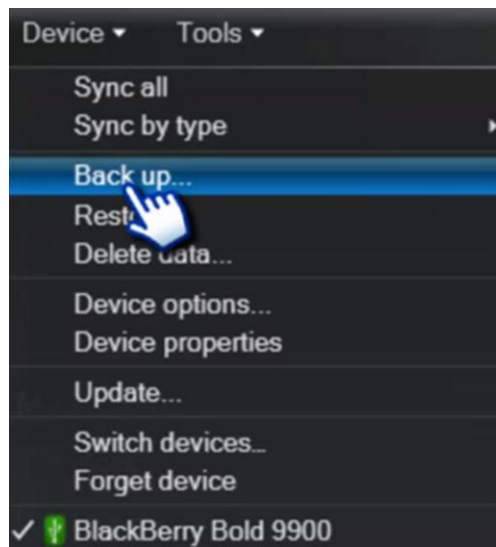
The encrypted backup file password prompt

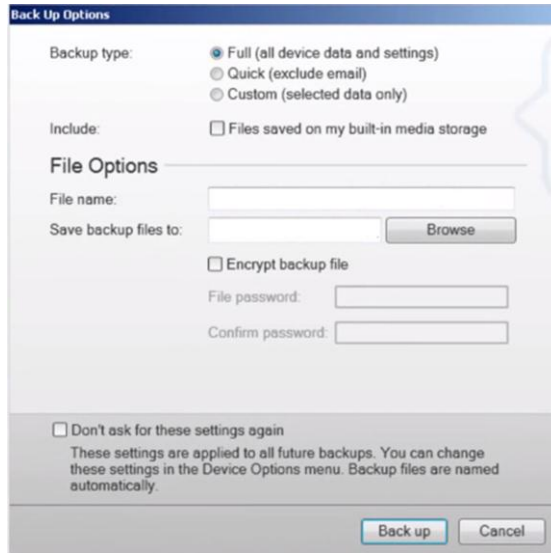


The encrypted backup file password prompt in Oxygen Forensics Suite

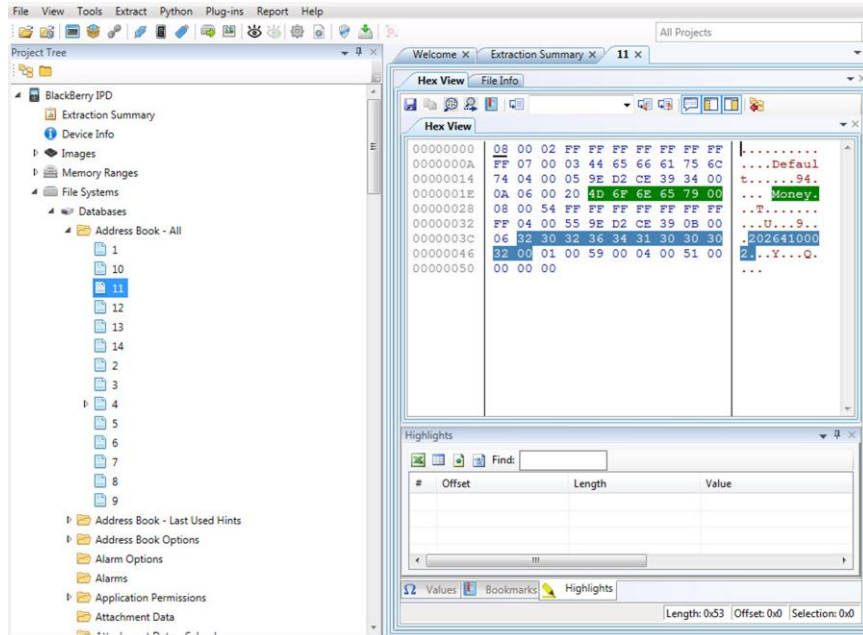


BlackBerry Desktop Manager



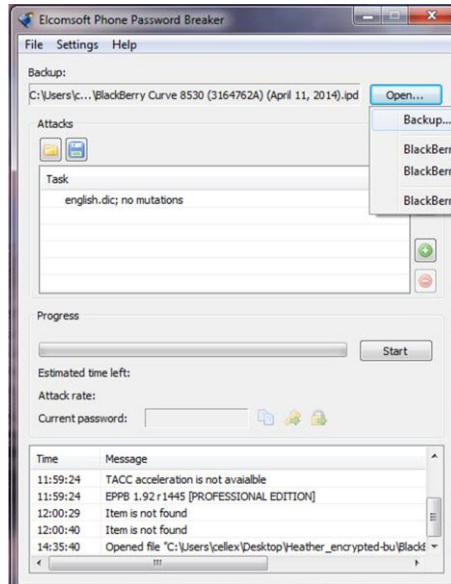


Full backup option in BlackBerry

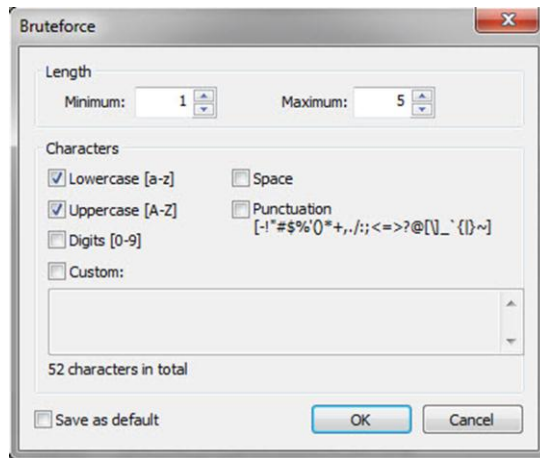


Cellebrite Physical Analyzer—Address Book examination

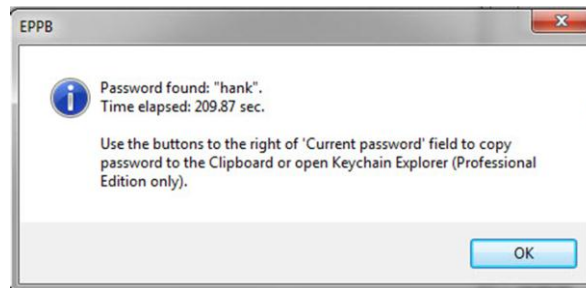




Elcomsoft Phone Password Breaker



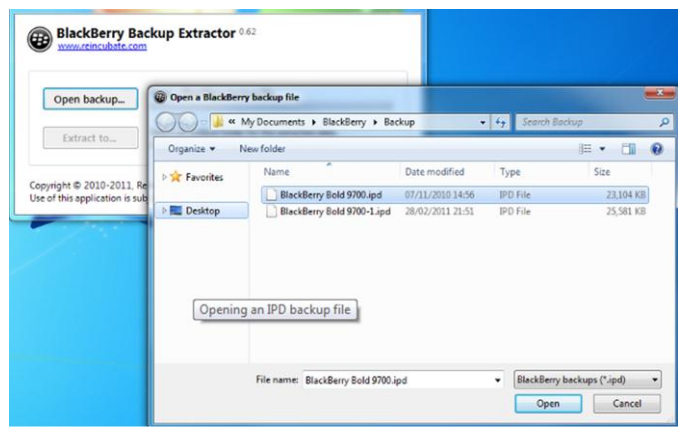
The Elcomsoft Phone Password Breaker attack options



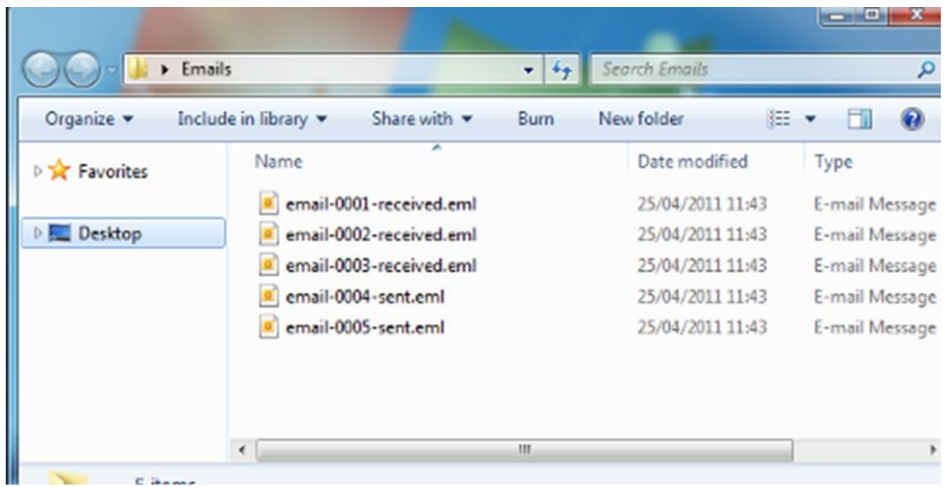
Elcomsoft Phone Password Breaker

```
File Edit Format View Help
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 1.4.1 ($Rev: 10844 $)
# Feature-Recorder: telephone
# Filename: flash.bin
# Histogram-File-Version: 1.1
n=4 7176808027
n=2 +122211144444
n=1 28621117144
n=1 28621111111
n=1 27621114444
n=1 28621114444
n=1 42712444444
n=1 47841411111
n=1 57111271111
n=1 57111444444
```

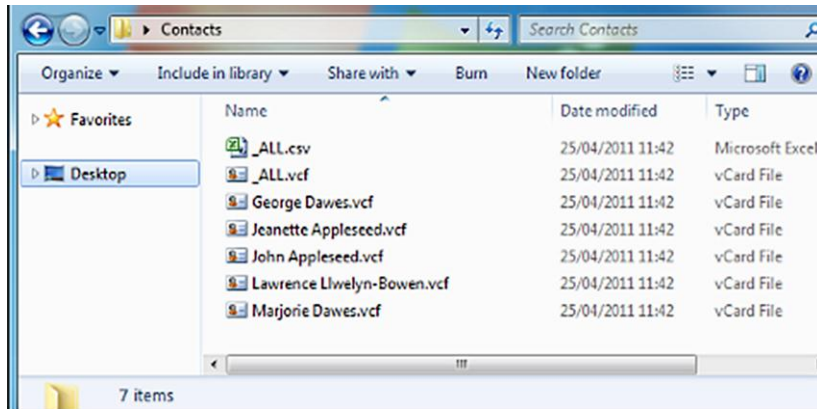
Telephone numbers parsed by Bulk Extractor



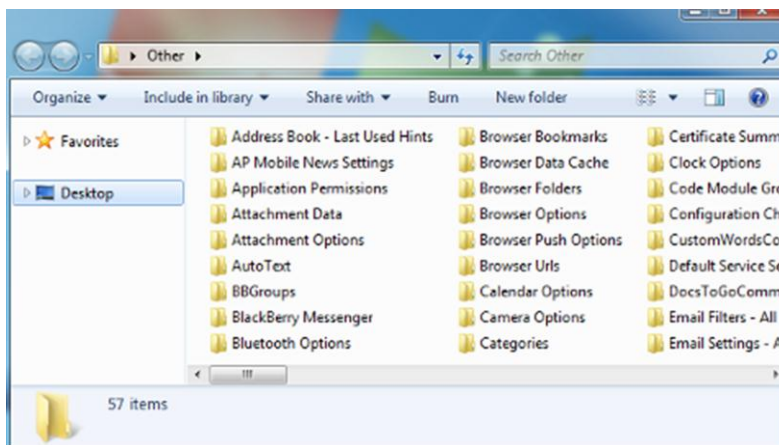
BlackBerry Backup Extractor



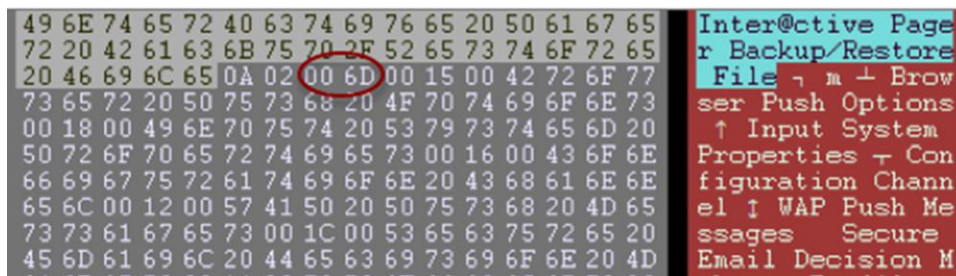
E-mail extracted from backup



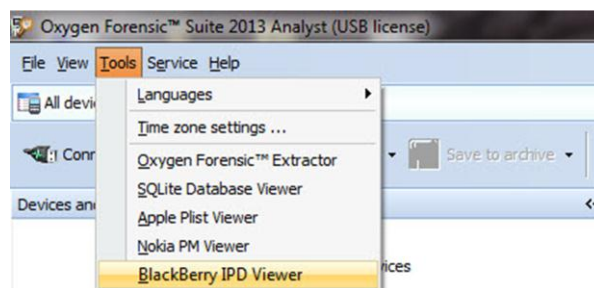
Contacts extracted from backup



Other useful data extracted from the backup



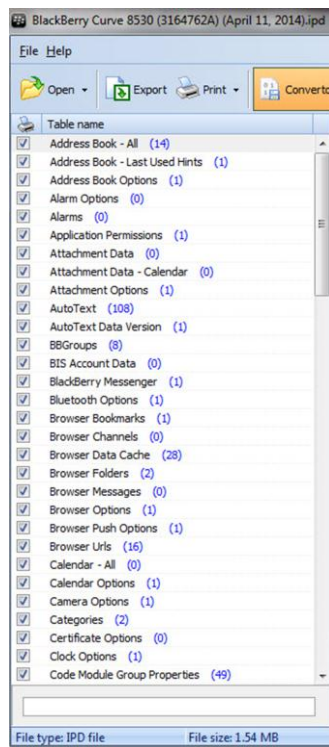
The Hex view of IPD file



Oxygen Forensics Suite BlackBerry IPD Viewer



Oxygen Forensics Suite BlackBerry IPD Viewer—the encrypted file



The Oxygen Forensics Suite BlackBerry IPD Viewer results