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)

IOS Android Java ME Symbian SlackBerry Other	75% 50% 25% 0%	-								•	•	
		Pit 12	Phone Contract	Jun 13	10.13	PUR PUR	589.43	00,13	200-1-0	Dec. 3	300.14	480.14
MONTH				105	A	NDROID	JAVA ME		SYMBIAN		BLACKBERRY	OTHE
April, 2013				59.04%		26.02%	9.62%		1.73%		1.51%	2.09
May, 2013				59.49%	1	24.40%	10.20%		2.06%		1.64%	2.21
June, 2013				57.56%	1	24.66%	10.72%		2.49%		2.26%	2.31
July, 2013				58.26%	-	25.28%	8.86%		2.23%		3.23%	2.15
August, 2013				54.91%	:	28.12%	8.43%		3.26%		3.28%	2.00
September, 2013				53.68%	4	29.42%	7.31%		4.48%		3.26%	1.86
October, 2013				55.39%	4	30.58%	6.47%		3.58%		2.55%	1.43
November, 2013				55.17%	1	33.89%	4.49%		3.12%		1.65%	1.68
December, 2013				54.27%	4	35.41%	3.90%		3.18%		1.58%	1.66
January, 2014				54.46%	1	34.60%	4.26%		3.41%		1.49%	1.79
February, 2014				52.96%	1	36.14%	4.44%		3.50%		1.42%	1.53

2. Understanding the Internals of iOS Devices

Source: https://www.netmarketshare.com/operating-system-marketshare.aspx?qprid=9&qpcustomb=1

iPhone
[16GB]
Designed by Apple in California Assembled in China Model No.: A1303 FCC ID: BCGA1303B IC ID: 579C-A1303B
FCXCE 0682

iPhone model number located on the back of the case

Airtel	14:35	35 % 🚅
General	About	
Network		AirTel
Songs		15
Videos		0
Photos		173
Applications		26
Capacity		13.7 GB
Available		10.8 GB
Version		5.1.1 (9B206)
Carrier		AirTel 12.0

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



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



• Apple Logo, Package Marking 338S11201, Cirrus Logic, Die Mark: CLI1G009A1

The iPhone 5Steardown 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

Cocoa Touch
Media Layer
Core Services
Core OS

The iOS layers

The iOS security architecture

3. Data Acquisition from iOS Devices

A secure boot chain of an iPhone in normal mode

	redsn0w 0.9.15b3									
Welcome! This is the	e latest version of redsn0w.									
Copyright 2007–201 for commercial use.	Copyright 2007-2012 iPhone Dev-Team. All rights reserved. Not for commercial use.									
For support, visit ou	r blog or try searching JailbreakQA.									
Extras										
Just boot	Just boot tethered right now.									
Pwned DFU	Enter pwned DFU mode in preparation for restoring to a custom IPSW.									
Recovery fix	Get out of Recovery Mode loop caused by a restore error.									
SHSH blobs	Fetch, verify or use SHSH blobs.									
Select IPSW	Manually specify an IPSW.									
Custom IPSW	Preserve baseband with a custom IPSW.									
Even more	Device info, IPSW restores, and more.									
	< Back Next > Quit									

The redsn0w recovery fix

Boot ROM (DFU)	I
1	
ipee	
IDOO	
+	
iBEC	
↓	
kernel	
.	
Ramdisk	

A secure boot chain of an iPhone in DFU mode

● ⊖ ⊖		MacBook Pro							
✓ Hardware	USB Device Tree								
ATA	USB 3.0 Hi-Speed Bus								
Audio	USB 3.0 SuperSpeed Bu	us							
Bluetooth	▼ USB Hi-Speed Bus								
Camera	▼Hub								
Card Reader	Apple Mobile De	vice (DFU Mode)							
Diagnostics	▼ Hub								
Disc Burning	IR Receiver								
Ethernet Cards	BRCM20702	Hub							
Fibre Channel	Bluetooth	USB Host Controller							
FireWire	Apple Interna	I Keyboard / Trackpad							
Graphics/Displays	▼USB Hi-Speed Bus								
Hardware RAID	▼Hub								
Memory	FaceTime HD Camera (Built-in)								
PCI Cards	o Annia Mahila Davies (DEU Mada):								
Parallel SCSI	Apple Mobile Device (DFU Mode):								
Power	Product ID:	0x1227							
Printers	Vendor ID:	0x05ac (Apple Inc.)							
SAS	Version:	0.00							
SATA/SATAExpress	Serial Number:	CPID:8930 CPRV:20 CPFM:03 SCEP:01 BDID:00 ECID:000001C31110CD8C IBFL:0							
SPI	Speed	SRTG:[IB000-574.4] Un to 480 Mb/sec							
Storage	Manufacturer:	Apple Inc.							
Thunderbolt	Location ID:	0x1d110000 / 8							
USB	Current Available (mA):	500							
Network	Current Required (mA):	100							
Firewall									
Locations									
Modems									
Volumes									

The MAC system information displaying a DFU-mode device

	1
Pwned Boot ROM (DFU)	
Ļ	
patched iBSS	
patched iBEC	
•	
patched kernel	
4	
custom ramdisk	

An exploited boot chain of an iPhone in DFU mode

The redsn0w welcome screen

. 0	Data — ba	ash — 102×46	R _M
Mac:/Volu	umes/Data\$hexdump -C mobile/Library/Addres	sBook/AddressBook.sqlitedb head	
00000000	79 5e b0 03 ea 34 50 78 be ac 56 14 ed	33 ad 2e y^4PxV3	
00000010	68 d3 57 ea 6b 06 d5 e1 34 b1 08 71 56	8a 83 af h.W.k4qV	
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 .@X4D.l^t.	
00000040	bd 62 37 bd 2d be 12 a2 39 20 7d 9f 1d	dc c7 f5 .b79 }	
00000050	93 1e 3d 81 51 04 ad be 36 04 74 37 b3	67 f2 bf =.Q6.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 EQa4.d.~.	
00000080	4a 9c 72 54 a1 b3 d2 6b f1 42 ea 13 58	cb 66 45 [J.rTk.BX.fE]	
00000090	3c d3 32_7d b3 71 ab ed 39 15 c3 19 61	67 3f 76 <.2}.q9ag?v	

The encrypted AddressBook file

$\Theta \odot \odot$												Da	ta -	– b	ash	_	107×41	R _M
Mac:/Volu	mes,	/Da	ta\$l	nex	dump	p -	C mo	obil	e/L:	ibra	ary,	/Ad	dre	ssB	ook,	/Add	iressBook.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	Øf	e7	00	00	00	00	36	6	
00000070	Øf	fb	Øf	f6	Øf	f1	Øf	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	Øf	fc	00	00	.//	

The decrypted AddressBook file

4. Data Acquisition from iOS Backups

Devices Preference	es
General Playback Sharing Store Pare	ntal Devices Advanced
Device backups:	
	Delete Backup
Prevent iPods, iPhones, and iPads from synd	cing automatically
iTunes is not paired with any Remotes	Forget All Remotes
3	Cancel OK

iTunes-disabling automatic sync

			Q- Search Library	
Music 🗧 Songs 🕢	Nburns Artists Genres Playlists	Radio Match	iPhone 🔺	iTunes Store
_	Tunes could not connect t	to the iPhone "Sai	tichh?" hocau	
	it is locked with a passcod	e. You must ente	r your	se
	passcode on the iPhone be	efore it can be us	ed with iTune	s.
				_
	More Information	Cancel	Try Again	

iTunes-iPhone locked message

iTunes-iPhone summary

000		[] 97D6299A-8EDA-454F-9C62-48B031F45DD6.plist ≝ [™]
₩ < >] 97D6299A-8E	DA-454F-9C62-4BB031F4	45DD6.plist) No Selection
Key	Туре	Value
▼ Root	Dictionary	(5 items)
SystemBUID	String	519DF016-0F61-44E3-97BF-65424A4ADA75
HostID	String	97D6299A-8EDA-454F-9C62-4BB031F45DD6
RootCertificate	Data	<2d2d2d2d2 2d424547 494e2043 45525449 46494341 54452d2d 2d2d2d0a 4d494943 72544343 415a5767 41774942 41674942 4144414e 42676b71 686b6947 3
DeviceCertificate	Data	<2d2d2d2d2 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

000		☐ 6c1b7aca59e2eba6f4635cfe7c4b2de1bd812898.plist
## ◀ ▶ 🔄 6c1b7aca59e2e	ba6f4635cfe7c4b2de1bc	1812898,plist > No Selection
Key	Туре	Value
▼ Root	Dictionary	(9 items)
DeviceCertificate	Data	<2d2d2d2d2d2d2d24547 494e2043 45525449 46494341 54452d2d 2d2d2d0a 4d494943 4e6a4343 41523667 41774942 41674942 414414e 42676b71 686b6947 3977304;
EscrowBag	Data	<44415441 000004f4 56455253 00000004 00000003 54595045 00000004 00000002 55554944 00000010 1162b128 64e04c36 a901c0a8 9c14b184 484d434b 00000028
HostCertificate	Data	<2d2d2d2d2 2d424547 494e2043 45525449 46494341 54452d2d 2d2d2d0a 4d494943 756a4343 41614b67 41774942 41674942 4144414e 42676b71 686b6947 3977304
HostID	String	97D6299A-8EDA-454F-9C62-48B031F45DD6
HostPrivateKey	Data	<2d2d2d2d2d2d2d24547 494e2052 53412050 52495641 5445204b 45592d2d 2d2d2d0a 4d494945 70414942 41414b43 41514541 31695068 786c4a44 77424a59 6f546678
RootCertificate	Data	<2d2d2d2d2 2d424547 494e2043 45525449 46494341 54452d2d 2d2d2d0a 4d494943 72544343 415a5767 41774942 41674942 4144414e 42676b71 686b6947 3977304
RootPrivateKey	Data	<2d2d2d2d2d2d2d24547 494e2052 53412050 52495641 5445204b 45592d2d 2d2d2d0a 4d494945 6f774942 41414b43 41514541 3041506b 64376857 4b646f41 57736d44
SystemBUID	String	519DF016-0F61-44E3-97BF-65424A4ADA75
WiFiMACAddress	String	28:cf:da:6e:99:e2

Pairing record on a computer

🚞 6c1b7aca59e2eba6f4	4635cfe7c4b2de1bd8128	98		
		Q		
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	
ec1538f1312bd144239f7eac70dded3e010dc550	Yesterday 6:37 PM	88 bytes	Document	
ed30b0c4ccfcb6026f7ae43b613dfe005af85043	Yesterday 6:37 PM	256 KB	Document	
edcbc482cd751c402f4ca5162b2347b80b43b173	Yesterday 6:37 PM	273 bytes	Document	
ef244b0e70a71410ab2d8c2a64b826f864ba4012	Yesterday 6:37 PM	242 bytes	Document	
f0b044e128429dab20cfac24fbedb3a528d730ac	Yesterday 6:37 PM	66 bytes	Document	
f6dc7201d77127256ac58b9ee73ca43975696e35	Yesterday 6:37 PM	70 bytes	Document	
f7bbe63e61427d2ee896496f5726b81289cfda38	Yesterday 6:37 PM	3 KB	Document	
f9f79aebad592c876a97ba6a640bf3401c526248	Yesterday 6:37 PM	316 bytes	Document	
f26f27f146e07614fe4df5a17f4ef6a042ea99eb	Yesterday 6:37 PM	124 KB	Document	
f30d6ef41c65177e0d949cbbefa7e114bb39a212	Yesterday 6:37 PM	1 KB	Document	
f34b101ed66f3aff9b378f9536e8e5c23ccf69bb	Yesterday 6:37 PM	353 bytes	Document	
f42cdcfe14c080199b895a59b6740a3c5b69cc33	Yesterday 6:37 PM	81 bytes	Document	
f86c972026c10344edf4ce5894caeea4222120a1	Yesterday 6:37 PM	289 KB	Document	
f772aa7de1bd2fcf98494024fbd193c6c4a3a586	Yesterday 6:37 PM	358 bytes	Document	
f936b60c64de096db559922b70a23faa8db75dbd	Yesterday 6:37 PM	119 KB	Document	
f5359dec233d0c2359fc2445cc1738d52a2fbe44	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	
fb520955c98189505f20d2af90a46a1ced8c2e9c	Yesterday 6:37 PM	6 KB	Document	
fd2e382547e97230b737c2fa26972c56e675159b	Yesterday 6:37 PM	6 KB	Document	
fd18a792c092be802c44f7ef7c0f8f11c8821cf6	Yesterday 6:37 PM	243 bytes	Document	
fdda2f81cc0b838dc00e3050b14da7ef2d835f3c	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

000	Domain	ns.plist	R ^M
🛗 🛛 🔹 🕨 📄 Domains.plist) No Sel	ection		
Key	Туре	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

)	O O iPhone Backup Extractor
c	Application Name
ľ	com.HackTest
l	com.innerfour.photovault
l	com.yahoo.weather
ŀ	com.yahoo.messenger
ŀ	com.enchantedcloud.photovaultpro
ļ	com.yahoo.frontpage
ļ	com.google.PlayMusic
ļ	com.krvw.iGoat
ŀ	org.wordpress
,	com.apple.WebViewService
ŀ	co.LaunchKey.LaunchKey
ŀ	com.google.Wallet
2	SynAck.shitiBank
1	iOS Files
ſ	Read Backups Extract

iPhone Backup Extractor

🖳 iPhone Backup Browser						x
Satishb3 (1/18/2014 6:56:42 PM)	- 📑 🛃 🔞		🗶 csv 髥			
Display Name	Name	Files	Size App Size	ze		*
	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.krvw.iGoat	com.krvw.iGoat	1	343			*
Name		Size	Date	Domain	Key	-
keychain-backup.plist		111,801	1/18/2014 1:26:17 PM	KeychainDomain	51a4616e576dd33cd2abadfea874eb8ff246bf0e	Ξ
Library/Accounts/Accounts3.sqlite		90,112	1/17/2014 1:38:02 AM	HomeDomain	943624fd13e27b800cc6d9ce1100c22356ee365c	
Library/AddressBook/AddressBook.sqlite	edb	700,416	11/8/2013 1:40:33 PM	HomeDomain	31bb7ba8914766d4ba40d6dfb6113c8b614be442	
Library/AddressBook/AddressBookImag	es.sqlitedb	1,122,304	5/11/2013 3:33:37 AM	HomeDomain	cd6702cea29fe89cf280a76794405adb17f9a0ee	
Library/AddressBook/AddressBookImag	es.sqlitedb-shm	0	1/5/2014 6:16:59 AM	HomeDomain	d1225e5e1a1e05345a3c090677a98a66b6425f47	
Library/AddressBook/AddressBookImag	es.sqlitedb-wal	16,464	11/5/2013 3:41:56 PM	HomeDomain	944320f0e5693a48a6d6769d509567e0e2fb08de	
Library/BulletinBoard/BehaviorOverrides	plist	1,496	2/19/2013 2:00:32 AM	HomeDomain	3418406efa0258f8db103dc909cfe1e9a35ede36	
Library/BulletinBoard/ClearedSections.pl	ist	241	1/9/2014 2:12:04 AM	HomeDomain	dd4b52c3d7f4ed39a7d8ca8baa79651ad5c2b71d	
Library/BulletinBoard/SectionInfo.plist		23,702	1/16/2014 1:11:59 PM	HomeDomain	3d8a6630ca29c3f835470e1c45a747e245ff8584	
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	406bf4ce09639cadb79440fa4ac86e1b0cc10304	
Library/Caches/com.apple.mobilesafari/	Thumbnails/6D939D86-F667-4596-8B71	54,882	6/16/2013 4:30:34 AM	HomeDomain	5e0b3d1018c9cc8f4c72e68a1a43d3a5e5a99d83	
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	6a53f1828a4fb639b44890aac77a11e8b072ea4d	
Library/Caches/com.apple.mobilesafari/	Thumbnails/FE5447E2-B52F-414D-AB6	1,662	1/16/2014 2:44:19 PM	HomeDomain	a07ad1e28c2ec87a91b60a9a77e35f805f310f88	
Library/Caches/com.apple.WebAppCach	he/ApplicationCache.db	294,912	9/25/2013 2:56:46 PM	HomeDomain	d2acb1ec24ed4669ec97974578478cff5bd236f9	
Library/Caches/locationd/clients.plist		2,425	1/18/2014 12:39:09 PM	RootDomain	a690d7769cce8904ca2b67320b107c8fe5f79412	
Library/Caches/locationd/consolidated.c	db	20,480	12/31/2013 12:25:28	RootDomain	4096c9ec676f2847dc283405900e284a7c815836	
Library/Caches/locationd/significant.plist	t	74	5/10/2013 3:59:43 PM	RootDomain	c061d48f0cbf73a9ebdae6e15dd85ed9669114f5	
Library/Calendar/Calendar.sqlitedb		389,120	1/17/2014 1:31:13 AM	HomeDomain	2041457d5fe04d39d0ab481178355df6781e6858	
Library/Calendar/Extras.db		28,672	1/3/2014 3:22:42 PM	HomeDomain	22b5fb3c3890cfc5cee685c923922e8ebe8ee9fd	-

iPhone Backup Browser

C1b7aca59e2eb	a6f4635cfe7c4b2de1bd8128	98_extract	
		Q	
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.eloud.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.iGoat	15-Jan-2014 10:05 PM		Folder
AppDomain-com.mywickr.wickr	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.shitiBank	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

000

python_scripts — bash — 194×31

R_M

1		Passwords		
Service	Account	Data	Access group	Protection class
push.apple.com		>e60a5980072c7c1c23	b com.apple.apsd	AlwaysThisDeviceOnly
AirPort	belkin.3239	443c8666	apple	AfterFirstUnlock
Shared Mobile Device ID		9efe46f4bd36cf2c268	a PGB36VEQ8D.ru.yandex.mobile.shared-device-i	d WhenUnlocked
com.apple.certui	https: blu-m.hotmail.com - c643bf96 59	b4 <binary data="" plist=""></binary>	apple	Always
AppleIDClientIdentifier		7E56EFCC-3757-445D-	8 apple	AfterFirstUnlockThisDeviceOnly
Etsy	Itoken	0233402f7f5e9b82487	9 3CUB372VC3.com.etsv.etsvforios	WhenUnlocked
Etsy	secret	6b96974a0a	3CUB372VC3.com.etsv.etsvforios	WhenUnlocked
com.facebook.analytics.deviceid		596B8BD8-C684-4F49-	B T840ZS65DQ.platformFamily	AlwaysThisDeviceOnly
com.facebook.datr		bXFQUfDmdKPE0Cis Vo	t T840ZS65D0.platformFamily	WhenUnlocked
com.apple.certui	https: blu-m.hotmail.com - 352dcac7 25	63 <binary data="" plist=""></binary>	apple	Always
com, facebook, Snap, graph	Data('100004090443505')	BAADhZCRCfHxMBAKK9K	c T840ZS65D0.platformFamily	WhenUnlocked
com.apple.certui	https: mega.co.nz - 5b4ff5c8 39c1f27f	f0 <pre>doinary plist data></pre>	com.apple.cfnetwork	Always
com.apple.certui	<pre>https: blu-m.hotmail.com - 7e571084 e1</pre>	59 <binary data="" plist=""></binary>	apple	Always
com.apple.certui	<pre>https: accounts.google.com - c6ee4e97</pre>	ell <binary data="" plist=""></binary>	com.apple.cfnetwork	Always
com.apple.certui	<pre>https: accounts.voutube.com - 7f5910d3</pre>	9 <binary data="" plist=""></binary>	com.apple.cfnetwork	Always
com.apple.certui	<pre>https: blu-m.hotmail.com - cecacbbe 40</pre>	98	apple	Always
com.apple.certui	https: www.google.co.in - 986de596 fba	dal <binary data="" plist=""></binary>	com.apple.cfnetwork	Always
com.apple.certui	https: blu-m.hotmail.com - 12882df3 c3	d5 <binary data="" plist=""></binary>	apple	Always
com.apple.certui	https: netbanking.mashregbank.com - 5a	fel <binary data="" plist=""></binary>	com.apple.cfnetwork	Always
com.apple.certui	<pre>https: www.testflightapp.com - 0f67aea</pre>	e <pre>l<binary data="" plist=""></binary></pre>	com.apple.cfnetwork	Always
com.apple.certui	<pre>https: blu-m.hotmail.com - 114aac43 a8</pre>	01 <binary data="" plist=""></binary>	apple	Always
com.apple.certui	https: www.testflightapp.com - a490976	5 <pre>shinary plist data></pre>	com.apple.cfnetwork	Always
AirPort	satish mac	1234abcd	apple	AfterFirstUnlock
com.apple.certui	https: netbanking.mashrepbank.com - 6a	f6 <pre>sbinary plist data></pre>	com.apple.cfnetwork	Always
com.apple.certui	<pre>https: blu-m.hotmail.com - e96abbaf 80</pre>	74 shinary plist data>	apple	Always
com.apple.iAdIDRecords	Data('kADiAdIDStorageKey')	<pre><binary data="" plist=""></binary></pre>	apple	WhenUnlocked

A decrypted keychain

Satishb3 ≜		Summary Info Apps Music M	ovies TV Shows Photos	On This iPhone	Done
	iPhone 3GS	Set Pa	ssword		
	Backups	Sat G Gar Pho Ser Car Pho Car Pho Ser Car Car Car Car Car Car Car Ca	ussword in my keychain	on s available (version 6.1.3). To are, click Update. hone	
	Automatical	In Pack Up	Manually Book Up and	Postore	
	Automatical	Ily Back Up 9 most important data on your iPhone to iCloud.	Manually Back Up and Manually back up your iPhor stored on this computer.	Restore ne to this computer or restore a backup	
	Automatical iCloud Back up the This comp A full back	Iy Back Up most important data on your iPhone to iCloud. uter to d'your iPhone will be stored on this computer.	Manually Back Up and Manually back up your IPhor stored on this computer.	Restore he to this computer or restore a backup Restore Backup	
	Automatical icloud Back up th This comp A full back.	Iy Back Up e most important data on your iPhone to iCloud. uter Io dr your iPhone will be stored on this computer. I iPhone backup also back up account passwords used on this iPhon	Manually Back Up and Manually back up your iPho stored on this computer. Back Up Now Latest Backup: Today 6:26 PM to this comp	Restore ne to this computer or restore a backup Restore Backup	
	Automatical i Cloud Back up th This comp A full back, M Encryp This will Chan	ly Back Up or most important data on your iPhone to iCloud. uter pod your iPhone will be stored on this computer IPhone backup also back up account passwords used on this IPhon ge Password	Manually Back Up and Manually Back Up your iPho stored on this computer. Back Up Now Latest Backup: Today 6:26 PM to this comp	Restore ne to this computer or restore a backup Restore Backup uter	

iTunes-encrypted backup

Device Backups	×
🗎 🗯 Satishb3	1/18/2014 9:46:57 PM
Device Name: Phone Number:	Product Type:
Open another	OK Cancel

iPhone Password Breaker-Choose backup

le Setting	is Help
	•
ackup:	
:\Users\Tes	t\AppData\Roaming\Apple Computer\M\Manifest.plist Open
A 44- 1	
Attacks	
	•
Task	
englis	h.dic; no mutations
-	
-	
	(a)
Progress	
Progress Attack 1 of	1
Progress Attack 1 of	1
Progress Attack 1 of	1 Start
Progress Attack 1 of Estimated t	1 Start
Progress Attack 1 of Estimated t Attack rate	1 Start
Progress Attack 1 of Estimated t Attack rate Current par	1 ime left: : ssword: 1234
Progress Attack 1 of Estimated t Attack rate Current pas	1 ime left: : ssword: 1234
Progress Attack 1 of Estimated t Attack rate Current par	1 ime left: : : ssword: 1234
Progress Attack 1 of Estimated t Attack rate Current pas Time 09:44:07	I I I I I I I I I I I I I I I I I I I
Progress Attack 1 of Estimated t Attack rate Current par Time 09:14:07 09:44:30	I I I I I I I I I I I I I I I I I I I
Progress Attack 1 of Estimated t Attack rate Current par Time 09:44:07 09:44:30 09:45:02	I I Start I Start
Progress Attack 1 of Estimated t Attack rate Current par Time 09:44:07 09:44:30 09:45:02 09:45:02	I I I I I I I I I I I I I I I I I I I
Progress Attack 1 of Estimated t Attack rate Current par 09:44:07 09:45:02 09:45:23 09:45:23	I I I I I I I I I I I I I I I I I I I

iPhone Password Breaker-password brute force

N	lo SIM 🤶	7:09	35% 🗈
<	iCloud Sto	rage & Bac	kup
	Storage		
	Total Stora	ige	5.0 GB
	Available		4.9 GB
	Manage St	orage	>
	Cha	inge Storage	Plan
	Backup		
	iCloud Bac	kup	
	Automatica accounts, do this iPhone	lly back up your ocuments, and s e is plugged in, l onnected to Wi-f	camera roll, ettings when ocked, and Fi.

iCloud backup toggle on the iPhone

Sign In	×
Sign in with A	pple ID
Apple ID:	
Password:	
🔘 Use authenti	cation token (base64)
	OK Cancel

securit	tylearn wordpress	securitylearn.wordpress@gmail.con 431268493
	Satishb3 [iPhone2,1] [SN: 85 UDID: 6c1b7aca59e2eba6f46 Updated: January, 18 2014 1 Size: 36.6 MB	137505EDG] i35cfe7c4b2de1bd812898 i3:37; 1 snapshot(s)
	Satishb3 [iPhone3,1] [SN: 87 UDID: b716de79051ef093a9i Updated: October, 18 2011 0 Size: 21.6 MB	0522V6A4S] 3fc3ff1c46ca5e36faabc3 17:00; 3 snapshot(s)

5. iOS Data Analysis and Recovery

				÷
ZSPRECORD	(61)	JRL▲	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_PRIMARYKE	Y (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

000			Conso	lidated.db –	Locked +					<u>.</u>
Execute:	Timestamo	MagneticX	MagneticY	MagneticZ	RiasX	BiasY	BiasZ	Level	Magnitude	Inclination
QFilter	307825508 866	1 000131249	-5 6691226	-33 6426	-9 8247	-33 572	-74 7216	3	34 1315841	16 746786117553
Tables	397464520 501	2 527702331	36 5915298	-9 59072	-10 180	-30 265	-74 7932	3	38 4508171	19 300725936889
CompassCalibration	395677653.583	29.69783592	16.5588665	-10.1030	-17.953	-42.845	-71.7329	3	43.5232200	9.4296483993530
ZS Rows	397278928.742	35.99276351	-4.1517596	-17.9594	-11.636	-39.020	-71.4378	3	40.4383430	23.143756866455
Fences	397526608.005	9.358675003	-25.768684	-31.5292	-16.420	-42.946	-67.5148	3	40.7610816	18.209178924560
Tablatafa	395933819.072	24.77676010	-5.3470115	-16.8228	-10.536	-39.333	-68.1713	3	30.4218235	33.231529235839
a Rower	395401386.925	-32.7209167	-26.507610	-11.1854	-21.658	-43.165	-67.6966	3	43.4477310	17.569580078125
Views	397707511.257	-34.8691444	-18.540580	1.463419	-18.932	-43.680	-52.6133	3	39.5190124	30.580520629882
incus.	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	41.680133819580
	395933831.094	-18.6137428	15.4992513	17.41366	-14.873	-42.855	-66.2330	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	15.283143997192
	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
谷 * Upgrade	+ - Edit			1	25 records. I	0.0 seconds.				Filter

The Consolidated.db view with SQLite Professional

O O en_GB-dynamic-text.dat	
	Hex Q* Text search
Save Copy Cut Paste Undo Redo	Go To Offset Find (Text search)
0000 41 79 0E 16 06 76 76 06 77 20 30 00 01 72 16 77 30 07 76 76 76 77 20 35 00 00 01 17 16 77 30 05 70 00 77 30 05 77 16 77 16 77 16 77 16 77 16 77 16 77 16 77 16 77 16 77 16 77 16 77 16 77 16 77 16 77 16 77 16 77 17 77 77 77 77 77 77 17 17 16 17 16 17 16 17 16 17 17 17 17 17 17 17 17 17 17 17 17 17 17 1	80 DynaicDictionary-5oris.jopod. g wy.emoli.toke.core.messoge.sen 91 ding.to.doy.meetmes.com.ad 73 dress.bring.menygetkeys 62open.check.drugs.contact. 65concerns.brithdoy.cholite 62iphene.forensics.macking. 63doy.mext.set.mext.set. 64
Type Value	
8 bit signed	
8 bit unsi	
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

The EIFT passcode recovery options

		Physical imaging	Logical imaging	Passcode recovery	Keychain decryption	Disk decryption
iPhone iPhone 3G iPod	iOS 1/2/3	+	+	instant 2)	+	not encrypted ³⁾
Touch 1 iPod Touch 2	iOS 4	+	+	+	+	not encrypted 3)
iPhone 3GS iPod Touch 3	iOS 3	+	+	instant 2)	+	not encrypted ³⁾
iPad 1	iOS 4/5	+	+	+	+	+ 4)
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	+	+	+	+	+

EIFT supported devices

Oxygen Forensic® Extractor v.6.1 Oxygen Forensic® Ex Oxygen Forensic® Extractor hel	.0.173 End extract data from device.
	Connection Mode Please connect your device to PC and select one of the modes: auto connection or manual device selection.
	Auto device connection Auto mode connects the first device detected on PC. Image: Auto addition of the second sec
🕡 Help	Next > Cancel

Oxygen Forensic® Extractor v.6.1.0.17: Oxygen Forensic® Extract Detection of devices connected via ca	3 ctor able.		
	onnect d	evice via cabl	e
Dev	vice is detect	ed successfully!	
Pre nee Connected	ess Next but ad to investig	ton to start extractin ate this device now.	g data from the device. Press Cancel if you do not
device	evice informa	ation:	
		Model:	Apple iPhone 5s
		IMEI:	358843056195937
		Software Revision:	7.0.6
1		Boot loader:	Apple OS iBoot-1940.3.5
T			
🕡 Help			Next > Cancel

Oxygen Forensic Suite-the device information screen

Oxygen Forensic® Extractor v.6.1.0.173	
Oxygen Forensic® Extractor Select sections to be extracted from the device	
 ✓ Apple iPhone 5s ✓ Calendar ✓ Event Log ✓ File structure ● Selective reading ✓ Images ✓ Audio ✓ Videos ✓ Documents ✓ Applications ✓ Database files ✓ Other files ● Full reading In Files from internal memory ✓ Messages ✓ Phonebook 	
e Help	< Back Next > Cancel

S Oxygen Forensic® Suite 2014 Standard						
Elle View Tools Service Help						
🔶 🔶 🛅 All devices 🕨 😭 Unassigned devices	iPhone6, 2 - 3/19/2014	8:14:40 PM [35884305	6105037] •			-
📲 : Connect new device 👻 🏠 Import backup file	Save to archive	🚹 Analytical tasks 👖	🚡 Export 🔸 🍃	🔲 View mode 👻 🏠 Actions 🔹	🕜 Help	
Devices and Cases	Phone6,2			Satish Bommisetty		
E Al derives → Consequence devices +10 Apple Phone 355 +10 Apple Phone 355 +10 Phone 355 +10 Phone 355	Add photo	Alas Retail Name Internal Name Platform IMEI Software Revision Boot loader Extracted by version Extracted by version Extraction Time	Phone6.2 Apple Phone 5s IPAnne6.2 IOS 39849056199937 7.0.6 Booh:1940.3.5 6.1.0.173 3/19/2014 8:14:40 PM	Add photo Full profile	Inspector Case Evidence number Owner Mobile phone Email	Add ingector Add case Add evidence number Satish Bommsetty 900 923323 satish.bommsetty@gmail.com
	Common sections (16 Device Information File Browser Calendar ¹⁶⁶⁰ Organizer Calendar ¹⁶⁶ Notes ²		Unregistered Aggregated Contacts Key Evidence (324) Phonebook	Dictionaries Unregistre	gistered!	Event Log 5733 Search
Standard version: 6.1.0.173 Expires in 72 days	Applications (1)	stered!	Unregistered! Timeline	Web Connections a	nregistered! nd Locat	

Oxygen Forensic Suite-the extracted data summary screen

Choose an extraction type:	
Advanced Logical extraction	Physical mode contains three types of extraction: • Physical extraction • File system extraction • Passcode recovery/test
Physical mode	U The device must be off.
	Supported devices running iOS 3.0 or higher: iPhone 2G/3G/3GS/4, iPad 1, iPod Touch 1G/2G/3G/4G, iPod Nano 5G

iOS Physical 3.9			
Successfully enter	ed Recovery Mode.		
Connect > Prepare > Ext	ract data		
You can release th	e Home button now.		
Device Info:		Сору	
Device model: iOS version: Serial number: ECID: Board: iBoot firmware version: Chip ID:	iPhone 4 GSM 7.0.3-7.0.4 870522V6A4S 000001C31110CD8C n90ap iBoot-1940.3.5 8930		

UFED Physical Analyzer-the device information screen

Paraben's Recovery Stick			-	- 0 -×
IRECOVERY STICK for APPLE " IPHONE	File	View	Tools	Help
Aain Page				
Choose connected device				
Detected Devices:				
Detected Devices:				
If your device is not displayed, wait a bit and then try to reconnect it.				
IPhone/IPad/IPod Touch				
Click on the device image to proceed.				
Cancel				
				Is Help

R Paraben's	Recovery Stick - C:\Users	satish\Documents\iRecovery\Cases\V	Vorkspace 1.0	B Contraction Contraction Contraction Contraction				
Par	arkeron Silde - CLUerustation/Documents/Watcovery/Gase:Workspee Lot: Proceedings of the Silde - CLUERUS of the Silde - C	Help						
Aain (Accurate Value Concernence Value Bit is Marcing Value Value Value Value Accurates Call History Crantics Call History Call History Call History Crantics Call History Call							
A	Acquired Data	Properties Maps History Maps B	ookmarks M	aps Directions Address Book Images				
		Property		Value				*
653		2 ActivationState	Activated					
	Messages	3 ActivationStateAcknowledge	ed					
19	Contacts	4 BasebandBootloaderVersion	ICE_2_13					
6	Call History	5 BasebandSerialNumber		CAEOI4AMI3NgSMaM				
1		6 BasebandVersion	04.10.01					
	Graphics	7 BluetoothAddress	58:1f:aa:22	:d1:09				
E	Organizer	Bits - CUlservisation Documental Record Vision Comparison File View Tool Set of a second decision of the comparison of the compariso						
27	Multimedia	9 CPUArchitecture	armv7					
۲	Internet Data	DeviceCertificate	BEGI bmUxHzA	I CERTIFICATE MIIC8jCCAlugAwiBAgUYcL/Rd+hahvtMA0GCSqGSib3DQEBBQUAMFoxCZAJBgNV E BggNVBAMTFkFwcGxIIGiQaG9uZ5BEZXZpY2UgQ0EwHhcNMTIwNjA3MDEL MDUyVhcMMTIwNjj3AD	BAYTAIVTMRMw DE1MDUyWjCBg	EQYDVQQKEwpl gzEtMCsGA1UEA	BcHBsZSBJbmMu wwkMjc4MzE0Nj	JMRUwEw gtRTgzQS0
×	Recovered Data	10	NADCBiQ n24Ps8d5	zmQswCQrDvQQbtwWDztLMARGALDECawCQDeX;BAQBqNVBACMCUNLC0VgGlobzE1MBEGALDE; (BgQCAhhBwEJIphH3k Hm/RUm1JEeqhCFCgmBKVR6DgK3JW7OjgE07Y8gf+eyyVBf1Jeo/hjxga21pmC vODni LIManyU hicTwIDAOABadGVMIGSMB8GA1UdiwOYM8AEHL+ISNEhoNaedWBIo57RNinTISNMB	.gwRQXBwbGUg Cy xzIPoWNmkeI 0GA1UdDaOWE	ISW5JLJEPMA0GA 142GS5+YIquTsdl 3BRtfGTk644n37N	4UE CwwGaVBo F0KeyCnW8EzC2I AfFWX+DEtsyGSk	NbbaFWtc
3	Tracking History		DwEB/wQ	AwiFoDAgBgNVHSUBAf8EFjAUBggr BgEFBQcDAQYIKwYBBQUHAwIwEAYKKoZihvdjZAYKAgQCBQAw	DQYJKoZIhvcNA	AQEF BQADgYEA	NquXldpISNVacb	ca3VZeTql
	Other Data	4	hWVtrOA	i x00fMeq1SxmJ/ab4DvDDbKGakD/g99q5eQUsMeQgvaK/SwVCyg+>GnzkuIYzDo12 BFzvVuMbq1QV4r00	.thrPy4PillEc6P	V4OYAgeVcKjRl3e	eUVeb/bA=b	ND CERTI -
		24						
Dat	Acquired Data Acquired Data Acquired Data ActivationState Address Book Images ActivationStateAchonoldeged ActivationStateAchonoldeged ActivationStateAchonoldeged ActivationStateAchonoldeged BasebandVersion C2,2,13 SasebandVersion C4,2,13 SasebandVersion C4,23 SasebandVersion C4,23 SasebandVersion C4,23 SasebandVersion C4,23 SasebandVersion C4,23 SasebandVersion C							
(Data to acquire:					Elapsed ti	me:
- 1		Backup Data	 I 	Acquisition completed			0	
							00:14:3	4
							lotal Sto	red:
iDhor	e Jouch						275 ME	
IMION	View Details			Hide				

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 SDK Platform-tools, revision Android SDK Build-tools, revision 19 Documentation for Android SDK, API SDK Platform Android 4.4, API 19, revision 1 ARM FABI V-78 System Image, Android Google APIs, Android SDK, API 19, revision Sources for Android SDK, API 19, revision Sources for Android SDK, API 19, revision 19 Google USB Driver, revision 8 	Package Description & License Package Android SDK Platform-tools, revision 19 Android SDK Build-tools, revision 19 Cocumentation for Android SDK API19, revision 1 Somples for SDK API19, revision 1 ARM EABI V78 System Image, Android API19, revision 1 Google APIS, Android API19, revision 1 Sources for Android SDK API19, revision 1 Sources for Android SDK API19, revision 1 Coogle APIS, Android API19, revision 1 Coogle APIS Driver, revision 8 Cicense Terms and Conditions This is the Android Software Development Kit License Agreement.
	Accept Reject Copy to clipboard Print O Accept License

Android SDK License

st of existing	Android virtual Device	s located at	C:\Users\vo	gella\.android	Navd
AVD Name	Target Name	Platform	API Level	CPU/ABI	New
	No AVD available				Edit
					Delete
					Repair.
					Details.
					Start
					Refresh

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

Virtual device configuration

The Android emulator

USB mass storage

2	📼 llı. 🗢 🎋 🛛 🐵 🧌	7:42 PM
US	B connection type	
D	efault connection type	
А А	Select default type	2
W	Charge only	
	HTC Sync	
	Disk drive	
	Internet sharing	
	Done	

HTC mobile USB options

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

The USB debugging option in Samsung mobiles

Smudges visible on a device under proper lighting (Source: https://viaforensics.com/wpinstall/wpcontent/uploads/smudge.png)

Forgot pattern option on an Android device

Normal Android system recovery mode

Clock	workMod Recovery v4.0.0.4
- re	boot sustem now
- ap	ply update from sdcard
- wi	pe data/factory reset
- wi	pe cache partition
- in	stall zip from sdcard
- ba	ickup and restore
- mo	ounts and storage
- ad	lvanced
- 00	wer off

Modified recovery mode

Superuse	X r Request
Root Explorer is reques	ting Superuser access.
Warning: If you did not in do not understand this good idea	itiate this action, or if you request, it's generally a to deny it.
	Tap for more info
Deny	Allow
✓ Remember	

Application requesting root access

9. Android Data Extraction Techniques

00	📄 platform-tools — adl	o — 80×24		
t login: Mon May)-hmahalik:∼ hmaha (86_64-20140321/so)-hmahalik:platfo ∫\ Tools/Term.apk Jaemon not running	5 11:47:35 on ttys000 alik\$ cd /Users/hmahalik/De dk/platform-tools rm-tools hmahalik\$./adb in g. starting it now on port	sktop/Android\ stall /Users/h 5037 *	Tools/adt- mahalik/Des	bundle
Jaemon started su	ccessfully *			
C:\temp\da	ata			
File Edit View Tool	s Help			
	n librany - Share with - Burn Ne	ny folder		
organize · Includer	and and a share with a barrier for	Data and Cal	T	Car
😭 Favorites	Name	Date modified	Туре	Size
🗼 Downloads	🍌 com.adobe.flashplayer	28-12-2013 12:07	File folder	
Recent Places	퉳 com.adobe.reader	28-12-2013 12:07	File folder	
Marktop	🍌 com.aldiko.android	28-12-2013 12:07	File folder	
	🍌 com.android.browser	28-12-2013 12:07	File folder	
🥽 Libraries	🍌 com.android.calculator2	28-12-2013 12:07	File folder	
	🍌 com.android.camera	28-12-2013 12:07	File folder	
🖳 Computer	com.android.deskclock	28-12-2013 12:07	File folder	
🏭 Local Disk (C:)	🍌 com.android.email	28-12-2013 12:07	File folder	
LENOVO (D:)	퉬 com.android.gallery3d	28-12-2013 12:07	File folder	
	腸 com.android.inputmethod.latin	28-12-2013 12:07	File folder	
🙀 Network	🎉 com.android.keychain	28-12-2013 12:07	File folder	
	com.android.launcher	28-12-2013 12:07	File folder	
	com.android.musicfx	28-12-2013 12:07	File folder	
	com.android.phone	28-12-2013 12:07	File folder	
		20.12.2012.12.07	F1 6 1 1	

The /data directory extracted to a forensic workstation

SQLite Database Browser - C:/te	mp/databases/pro	file.db		2
ile Edit View Help				
Database Structure Browse Data	Execute SQL	E];		
Name	Object	Туре	Schema	
⊕android_metadata ⊕sync_state	table table		CREATE TABLE android_metadata (local CREATE TABLE _sync_state (_id INTEGE	
terrender besterne b	table		CREATE TABLE packages (_id INTEGER CREATE TABLE mimetypes (_id INTEGER	
t)-data	table		CREATE TABLE data (_id INTEGER PRIM	

s Help			
n library 🔻 Share with 👻 Burn	New folder		
Name	Date modified	Туре	Size
contacts2.db	28-12-2013 13:10	DB File	308 1
contacts2.db-journal	28-12-2013 13:10	DB-JOURNAL File	13
profile.db	28-12-2013 13:10	DB File	308
profile.db-journal	28-12-2013 13:10	DB-JOURNAL File	01
	s Help n library Share with Burn Name Contacts2.db contacts2.db-journal profile.db profile.db-journal	s Help n library Share with Burn New folder Name Date modified contacts2.db 28-12-2013 13:10 contacts2.db-journal 28-12-2013 13:10 profile.db 28-12-2013 13:10 profile.db-journal 28-12-2013 13:10	s Help n library Share with Burn New folder Name Date modified Type Contacts2.db Contacts2.db Contacts2.db-journal Contacts2.db-jo

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		דדדדדדד	1388206471836	11		O	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	99999999999	1388212023730	1	2	1	James

address	person	date	date sent	proi	re	stat	typ	re	sul	body
(999) 999-9999		1388223954060					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

	browser	2.db - Oxygen Forensic SC	Lite V	liewer			
Eil	e <u>T</u> ools	Service Help					
P	Open	Export 🍃 Print	- }	• A	nalyze [Deleted Data 🥧 Options 🕜 Help	
8	Tables	Δ.		Table	data		
		_sync_state (0/0)	#	2	_id	title	uri
	m	_sync_state_metadata (1		1	Goo <trial></trial>	https://www.google.com/w <trial>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</trial>
~	E	android_metadata (1/0)	2		2	test - Goo <trial>XXX</trial>	https://www.google.com/search?source=android-home&
~	=	bookmarks (15/0)	3	~	3	test - Goo <trial>XXX</trial>	https://www.google.com/search?site=webhp&ei=8Ze2U
		history (14/0)	4	~	4	Goo <trial></trial>	https://www.google.co.in/?gws_ <trial>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</trial>
~	=	images (24/0)	5		5	Welcome t <trial>XXX</trial>	https://m.facebook.com/?refsrc=htt <trial>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</trial>
~	=	searches (4/0)	6	~	6	google - Go <trial>XXXX</trial>	http://www.google.com/m?hl=en&sou <trial>XXXXXXX</trial>
\checkmark	=	settings (1/0)	7	V	7	forensics - <trial>XXXXXX</trial>	http://www.google.com/search?hl=en&source=android
\checkmark	=	sqlite_sequence (3/0)	8	V	8	Forensic science - Wikipe <trial>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</trial>	http://en.m.wikipedia.o <trial>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</trial>
v	=	thumbnails (1/0)	9		9	facebook - G <trial>XXXXX</trial>	http://www.google.com/m?hl=en&sour <trial>XXXXXXXXX</trial>
			10	V	10	Welcome t <trial>XXX</trial>	https://m.facebook.com/?refsrc=h <trial>X00X00XXXX</trial>
			11	~	11	Wiki <trial></trial>	http://www.w <trial>XXXXXXX</trial>
			12	V	12	us airways - <trial>XXXXXXX</trial>	http://www.google.com/m?hl=en&source <trial>XXXXX</trial>
			13	 Image: A start of the start of	13	US Airways Airline tickets, <trial>XX00000000000000000000000000000000000</trial>	http://mobile.usairways.com/mt/www <trial>XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</trial>
			14	~	14	shopping - G <trial>XXXXX</trial>	http://www.google.com/m?hl=en&sour <trial>XXXXXXXXXXX</trial>

The browser2.db file in Oxygen Forensic SQLite Viewer

	id	user id	first name	last name	cell	other	email	birthday month
1	1	100004087623668	Lavanya	1			lavanyalove757@gn	2
2	2	10000005601801	Pranav	м.				-1
3	3	100004630714031	Sujata	P	+919178087585			4
4	4	100000818058433	Sudha	C			sudaha_ ghim hi@yah	1
5	5	100003499121241	Vasu	N	+919656026578		vasundhara_sree@	7
6	6	100003191641871	Makka	A	+918106300789		n atchy utaramiredd	12
7	7	1033892411	Sai	BI	+91994		saikumarb ilimasa ni@	9
8	8	100002190061552	Vara	к			vararock@yahoo.co	3
9	9	100002328888334	Kaluri	A	+918688722193		kvis.aravind@gmail.c	6
10	10	100000103323292	E	R .	+9197001877,08		pithamber_reddy@y	-1
11	11	562618335	Mukesh	к	+91984959		mukeshing 143@yaho	2

The fb.db file in SQLite browser

ψ 🖬 🔒	Í	Ø	"II 93% 💈	3:29 PM
AFLogica	I OSE	_		
Available	providers:			
🖌 Ca	llLog Calls			
Co	ntacts Pho	nes		
M	MS			
🖌 W	MSParts			
V SM	IS			
	Select All	Deselec	t All	Capture

The AFLogical OSE app

Message displayed after the extraction is complete

< 🚞 N	Ay Files 🔰 🔒 🔒	E.						
	/storage/sdcard0/forensics/	2013						
	CallLog Calls.csv							
	Contacts Phones.csv	С	allLog Ca	lls.csv				≣,
	MMS.csv		В	с	D	E	F G	н
		73 '	8 9.19E+11	1.388E+12	127	2	0 Bindu	
	MAN ACCOUNTS AND	74 '	7 9.19E+11	1.388E+12	0	3	0 Bindu	
	MMSParts.csv	75 '	6 9.174E+11	1.388E+12	0	3	0 naveen om	8
		76 /	5 9.174E+11	1.388E+12	0	3	0 naveen om	5
	SMC any	77 .	4 9.194E+11	1.388E+12	252	2	0 Amma	
	SIMS.CSV	78 '	3 9.194E+11	1.388E+12	0	3	0 Amma	
		79	2 9.198E+11	1.388E+12	2054	1	0 vikas hyd	
	info yml	80 '	1 9.198E+11	1.388E+12	0	2	0 vikas hyd	
	IIIIO.XIIII	81 5	9 9.198E+11	1.388E+12	0	3	0 vikas hyd	
		82 /	0 9.19E+11	1.388E+12	336	2	0 Bindu	

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

rer	Π.	
	Android - Storage Devices	
	Disk - I	
	Android - Drives/Partitions	
	Local Dirk, Fr	
	Please select a disk to continue	Android - Storage Devices : 1

The list of storage devices available

ecover for Android						
П■					L.	FAQ
🗸 Mark All 🖌 UnMark All 🤺	🕨 Goto Parent 🔅 🔻 Tools 🗵	Show Deleted	e.c	j, *.jpg	Q Find	•
Data View File Type View						
Root	Name /	Size	Modified	Created		
🖾 🙀 -	File#26.jpg	184 KB				-
A File Types	🔲 🙀 file#27.jpg	64 KB				
P apk[9]	🔲 🙀 file#28.jpg	82 KB				
doc[1]	🔲 🙀 file#29.jpg	105 KB				
a jpg[//]	🔲 🙀 file#3.jpg	13 KB				
jpg[r-//]	🔲 🙀 file#30.jpg	46 KB				
	🔲 🙀 file#31.jpg	153 KB				
	Tile#32.jpg	185 KB				
	🔲 🙀 file#33.jpg	2 KB				
	🔲 🕁 file#34.jpg	4 KB				
	🔲 🙀 file#35.jpg	2 KB				
	🔲 🙀 file#36.jpg	2 KB				
Recovered 90 3 MB data [87 Files ar	nd 8 Folders]	Marked Data : 0 byte	is N	Aarked Folders : 0		

Recovered files list

The Super Backup Android app

P	Open	Export 🎝 Print	- 🕼 Options 🕜 He	p	Recover deleted records	Filtering cr	iteria 🛞
	Tables	۸	🌐 Table data 😺 Blo	cks containing deleted data	*		»
~	=	addr (0/0)	Address 🔻	Data		Туре	Value
V	=	android_metadata (1/0)	00032780 - 00036736	0F 56 00 00 00 00 00 00 00	0 00 00 00 00 00 00 00 00 00 00 00 00	Original value	م V
~	🌐 🖤	attachments (0/0)					▲ []
✓	=	canonical_addresses (2/0				UTF-8	¥۷
~	🎞 🗰	drm (0/0)				Unicode (UTF-16	
✓	🖽 🗰	part (0/0)				Unicode (UTF-16	. 嘏++++++
✓	🎞 🗰	pdu (0/0)					
✓	🖽 🛎	pending_msgs (0/0)				OLE Automation	. <can't con<="" td=""></can't>
✓	🌐 🏛	rate (0/0)				Unix Epoch Time	<can't con<="" td=""></can't>
✓	🎞 🛄	raw (0/0)				Unix Epoch Time LE	: <can't con<="" td=""></can't>
✓	🎟 🖱	sms (2/0)				Unix Epoch Time	<can't con="" td="" ≡<=""></can't>
✓	🎟 ⁱⁱ	sqlite_sequence (2/0)				Unix Epoch Time	<can't con<="" td=""></can't>
✓	🎟 🖤	sr_pending (0/0)				OS X Epoch Time	. <can't con<="" p=""></can't>
✓	🎫 🖷	threads (2/0)				OS X Epoch Time	. <can't con<="" td=""></can't>
✓	=	words_content (2/0)				BlackBerry Time BE	<can't con<="" td=""></can't>
✓	=	words_segdir (5/0)				BlackBerry Time LE	<can't con<="" td=""></can't>
✓	III II	words_segments (0/0)	•		+	Chrome Time BE	<can't con<="" td=""></can't>
	1	All Deleted Data				Chrome Time LE	<can't con<="" td=""></can't>
			📗 • 🎓 • 🛃 • 🙆) 🗐 • 😸 🗛 🔳 🥐 .	32		
			3 09 01 09 08 00	17 00 08 08 09 07 3	333 🔺	Unsigned-8	<can't con<="" td=""></can't>
			1 43 38 A6 BD 70	01 43 38 A6 BC C0 H	F 45 C8 % p.C8 \ MÀÿ	Signed-8	<can't con<="" td=""></can't>
			C 6F		Hello 👻	Unsigned-16 BE	<can't con<="" td=""></can't>
			•		•	Signed-16 BE	<can't con="" td="" 👻<=""></can't>
Tria	access	18 days left	File type: solite	File size: 100 KB	Tables: 17 Delet	ed items: 1 SHA	2 Hash: 1ed2994

Recovering deleted SMS messages

```
scalpel.conf ¥
# GRAPHICS FILES
# AOL ART files
                              150000 \x4a\x47\x04\x0e
150000 \x4a\x47\x03\x0e
                                                                        \xcf\xc7\xcb
#
          art
                   У
#
          art
                    y
                                                                        \xd0\xcb\x00\x00
#
  GIF and JPG files (very common)
#
#
          glf
                    у
                               5000000
                                                    \x47\x49\x46\x38\x37\x61
                                                                                              \x00\x3b
          glf
#
                    y
                               5000000
                                                    \x47\x49\x46\x38\x39\x61
\xff\xd8\xff\xe0\x00\x10
                                                                                              \x00\x3b
                               200000000
                                                                                              \xff\xd9
# ]]
          ipg
                    y
22
# PNG
                    y.
                               20000000
                                                    \x50\x4e\x47? \xff\xfc\xfd\xfe
#
          png
#
#
          (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
# BMP
          positives
#
```

The scalpel configuration file

Running the Scalpel tool on a dd file

Output folder after running the Scalpel tool

Google
Gmail -
Gmail
Contacts
Tasks

The Contacts menu in Gmail

You can restor the past 30 day import or undo	e your contact list to the state that it was in at any point within ys. This is a great way to recover deleted contacts, undo an a merge. <u>Learn more</u>
Please select a	a time to restore to:
0 10 minutes	ago
I hour ago	
Yesterday	
1 week ago	
Custom	
0 🔻 days	, 1 🔻 hours, 0 💌 minutes.

The Restore Contacts dialog box

11. Android App Analysis and Overview of Forensic Tools

Facebook App in Google Play Store

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

The classes-dex2jar.jar file created by the dex2jar 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

MOBILedit! Forensic Lite			
File Edit View Phonebook A Back Contract International Int	ction Help Export Print Backup Co	P Const Settings State Const Const Partie	S Undo
Navigation	Call Logs	(378) - Samsung Galaxy S	III
Start	Missed (129) Outgoing (249) Name Number Time -	treeming	
Connected Devi	Bindu	5 +91 = 1 = 1 = 0 31-01-2014 12:22:45	
• 🔕 Samsung Galaxy S III (R.,	Bindu	% +91 1 31-01-2014 12:21:15	
Phonebook Gall Loss	srinivas adp	% +91 0 8 31-01-2014 12:19:52	
P Messages	Bindu	% +91 (199 30-01-2014 23:53:25	
Applications	Bindu	∜ +91 x 28 0 30-01-2014 23:53:12	
🕞 Files	Amma	K +9 44 4 7 30-01-2014 22:01:01	
🕞 User Files	Akka	\$ +9 3 47 30-01-2014 22:00-26	
🖤 MMS 🛅 Calendar	Arun bangalore	¶ +9: ■:■: 30-01-2014 21:24:32	

The MOBILedit tool-Call logs option

The Autopsy tool screen

ß	Add Data Source			
Steps	Enter Data Source Information wizard (Step 1 of 3)			
 Enter Data Source Information Configure Ingest Modules 	Enter Data Source Information:			
Add Data Source	Select source type to add: Image File v			
	Browse for an image file:			
)R585_labs\Lab14_Capstone\Physical Samsung GSM SGH-T999 Galaxy S III 2013_09_19 (001)\ Browse			
	Please select the input timezone: (GMT-5:00) America/New_York v 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</back>			

Autopsy image loading

Configure Ingest Modules wizard	d (Step 2 of 3)	
Configure the ingest modules you w	rould like to run on this data source.	
Recent Activity E01 Verifier Hash Lookup File Type Identification Archive Extractor Yextractor Exif Parser Keyword Search	Skip Known Files (NSRL)	
Email Parser Extension Mismatch Dete	<	
Android Mobile Device An	This module will be for Android mobile forensics add-on to Autopsy	Advanced
Process Unallocated Space		

Autopsy ingest modules

	Disastanu Listina	
• •	Directory Listing	
Data Sources	Table Thumbnail	
vol1 (Unallocated: 0-8191)	Artifact Type	Child Count
🖭 🖷 vol4 (modem: 8192-131071)	Contacts (12)	12
🥃 vol5 (sbl1: 131072-131327)	🔯 EXIF Metadata (139)	139
vol6 (sbl2: 131328-131839)	🕂 GPS Trackpoints (19)	19
vol8 (aboot: 132864-136959)	Messages (79)	79
vol9 (rpm: 136960-137983)		
wol10 (boot: 137984-158463)		
🖮 vol11 (tz: 158464-159487)		
vol12 (pad: 159488-160511)		
vol13 (param: 160512-180991)		
😥 📨 📄 vol 14 (efs: 180992-208895)		
wol15 (modemst1: 208896-215039)		
vol16 (modemst2: 215040-221183)		
🖭 🥃 vol 17 (system: 221184-3293183)		
Vol18 (userdata: 3293184-28958/19)		

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
Installed Applications				-
TouchXplorer	Julien Schapman	28/02/2011	664,91 KB	1.0.0.0
TouchXperience	Julien Schapman	28/02/2011	2,42 MB	1.0.2.0
8 Bluetooth	Julien Schapman	28/02/2011	587.02 KB	1.0.0.0
Config. avancée	Julien Schapman	28/02/2011	1,31 MB	1.1.0.1
🥵 Éditeur de registre	Julien Schapman	28/02/2011	1,29 MB	1.1.0.0
Purchased Applications				-
Config Connexion	HTC Corporation		913,10 KB	1.0.0.0
Convertisseur	HTC Corporation		1,82 MB	1.0.0.0
	HTC 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: folder 3

AppNotifications_1491	PageList_10000184
Feed_MostRecent_149	PageList_10000187
Feed_UserWall_149134	PageList_10000204
Friends	PageList_10000226
Group_1359(1177 1178 17	PageList_10000234
Group_15186milliomatica	PageList_10000246
HomePage	PageList_10000270
Notes	PageList_10000298
Notifications	PageList_10000397
PageList_5438	PageList_10000418
PageList_7706	PageList_10000433
PageList_1005	PageList_10000443
PageList_1038	PageList_10000512
PageList_1039	PhotoCollage_14913
PageList_1095	PhotosForUser_149
PageList_1131	Requests
PageList_1170	UnifiedThreadList_Inbox
PageList_1346	UnifiedThreadList_Other
PageList_1455	UserGroups_1491
Deservice 1401	

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

ter the password	X				
Enter the password to open your encrypted backup file:					
μ					
ОК	Cancel				

The encrypted backup file password prompt

The encrypted backup file password prompt in Oxygen Forensics Suite

Synchronize Syn Configuration Select	chronize	
Configuration Select		
Synchronization Add-ins	t the check box beside one or more of the following actions: Reconcile messages Synchronize organizer data Rim add in actions Update device date and time	
Syn Ma	chronize automatically Synchronize the selected tems when your device is connected to the BlackBerry Desktop hager	

BlackBerry Desktop Manager

Backup type:	 Full (all device data and Quick (exclude email) Custom (selected data of 	settings) nly)
Include:	Files saved on my built-	n media storage
File Options		
File name:		
Save backup files to:		Browse
	Encrypt backup file	
	File password:	
	Confirm password:	
Don't ask for these	settinas again	
These settings are these settings in the automatically.	applied to all future backups. Device Options menu. Back	You can change up files are named

Full backup option in BlackBerry

Cellebrite Physical Analyzer-Address Book examination

le Setting	ıs Help	
adkup:		
:\Users\c	BlackBerry Curve 8530 (3164762A) (April 11, 2014).ipd	Open
Attacks		Backup.
		BlackBer
Task		BlackBer
englis	h.dic: no mutations	BlackBer
Progress		
Progress Estimated t Attack rate	ime left:	Start
Progress Estimated t Attack rate Current par	ime left: : ssword:	Start
Progress Estimated t Attack rate Current par	ime left: : ssword:	Start
Progress Estimated t Attack rate Current par Time 11:59:24	ime left: : ssword: Message TACC acceleration is not available	Start
Progress Estimated t Attack rate Current par Time 11:59:24 11:59:24	ime left: : ssword: Message TACC acceleration is not avaiable EPPB 1.92 r.1445 [PR:OFESSIONAL EDITION]	Start
Progress Estimated t Attack rate Current par Time 11:59:24 11:59:24 12:00:29	ime left: : ssword: I I I I I I I I I I I I I I I I I I I	Start
Progress Estimated t Attack rate Current par Time 11:59:24 12:00:29 12:00:40	ime left: : ssword:	Start
Progress Estimated t Attack rate Current par Time 11:59:24 12:00:29 12:00:20 14:35:40	ime left: : ssword: Message TACC acceleration is not avaiable EPPB 1.92 r1445 [PROFESSIONAL EDITION] Item is not found Item is not found Item is not found Item is not found	Start

Elcomsoft Phone Password Breaker

Length Minimum: 1	Maximum:	5 🚔
Characters		
V Lowercase [a-z]	Space	
Uppercase [A-Z]	Punctuation [-!*#\$%'()*+,./:;	<=>?@[\]_`{ }~]
Custom:		
Custom:		*
Custom:		A
Custom:		÷

The Elcomsoft Phone Password Breaker attack options

Elcomsoft Phone Password Breaker

File Edi	t Format View Help
# BANN	ER FILE NOT PROVIDED (-b option)
# BULK	_EXTRACTOR-Version: 1.4.1 (\$Rev: 10844 \$)
# Feat	ure-Recorder: telephone
# File	Feature-Recorder: telephone Filename: flash.bin Histogram-File-Version: 1.1 =4 =2 =1 =1 =1
# Hist	ogram-File-Version: 1.1
n=4	7176828827
n=2	+12221134444
n=1	200.2117064
n=1	388.7591117
n=1	2547434846
n=1	1080254938
n=1	4252466899
n=1	4784343885
n=1	5753527230
n=1	5713843838

Telephone numbers parsed by Bulk Extractor

Open backup	up @ Open a BlackBerry backup file		Open a BlackBerry backup file		
Extract to_	King and the second secon		• +y Search Backup		
	Organize • N	lew folder			1= • CI
	> 🖈 Favorites	Name	Date modified	Туре	Size
pyright © 2010-2011, Re e of this application is sub		BlackBerry Bold 9700.ipd	07/11/2010 14:56	IPD File	23,104 KB
	Desktop	BlackBerry Bold 9700-1.ipd	28/02/2011 21:51	IPD File	25,581 KB
		1001 1 (1)			

BlackBerry Backup Extractor

Organize 🔻 Inc	lude in library Share with	Burn	New folder	• 🔟 🔞
Favorites	Name		Date modified	Туре
	email-0001-received.eml		25/04/2011 11:43	E-mail Messag
🛛 🧮 Desktop	email-0002-received.eml		25/04/2011 11:43	E-mail Messag
	email-0003-received.eml		25/04/2011 11:43	E-mail Messag
	email-0004-sent.eml		25/04/2011 11:43	E-mail Messag
	email-0005-sent.eml		25/04/2011 11:43	E-mail Messag

E-mail extracted from backup

Organize 👻 In	clude in library Share with Burn	New folder 855	• 🗔 🔞
> 🔆 Favorites	Name	Date modified	Туре
	All.csv	25/04/2011 11:42	Microsoft Exce
🛛 🧮 Desktop	S _ALL.vcf	25/04/2011 11:42	vCard File
	Seorge Dawes.vcf	25/04/2011 11:42	vCard File
	Sea Jeanette Appleseed.vcf	25/04/2011 11:42	vCard File
	S John Appleseed.vcf	25/04/2011 11:42	vCard File
	S Lawrence Llwelyn-Bowen.vcf	25/04/2011 11:42	vCard File
	S Marjorie Dawes.vcf	25/04/2011 11:42	vCard File

Contacts extracted from backup

Organize Incl	ude in library 👻 Share with 👻 Bu	m New folder	88 • 🗔 🔞
🖻 🗙 Favorites	Address Book - Last Used Hints AP Mobile News Settings Application Permissions Attachment Data Attachment Options AutoText BBGroups BlackBerry Messenger	Browser Bookmarks Browser Data Cache Browser Folders Browser Options Browser Push Options Calendar Options Calendar Options Calendar Options	Certificate Suma Clock Options Code Module G Configuration C CustomWordsC Default Service 1 DocsToGoCom
	Bluetooth Options	Categories	Email Settings -

Other useful data extracted from the backup

I	49 6E 74 6	5 72 40 63	74 69 76 65 20	0 50 61 67 65	Inter@ctive Page
I	72 20 42 6	1 63 6B 75	20 2F 52 65 73	3746F7265	r Backup/Restore
I	20 46 69 6	C 65 0A 02	00 6D 00 15 00	0 42 72 6F 77	File - m + Brow
I	73 65 72 2	0 50 75 73 (68 20 4F 70 74	4 69 6F 6E 73	ser Push Options
I	$00\ 18\ 00\ 4$	9 6E 70 75 1	74 20 53 79 73	374656D20	↑ Input System
I	50 72 6F 7	0 65 72 74 (69 65 73 00 16	5 00 43 6F 6E	Properties - Con
I	66 69 67 7	5 72 61 74 (69 6F 6E 20 43	368616E6E	figuration Chann
I	65 6C 00 1	2 00 57 41 !	50 20 50 75 73	368204D65	el 1 WAP Push Me
I	73 73 61 6	7 65 73 00 :	1C 00 53 65 63	3 75 72 65 20	ssages Secure
I	45 6D 61 6	9 6C 20 44 1	65 63 69 73 69	9 6F 6E 20 4D	Email Decision M
1	24 CD CD D	0 00 11 00 1	· // //	2 4 2 4 5 2 2 2 2 2 2	1

The Hex view of IPD file

Oxygen Forensics Suite BlackBerry IPD Viewer

<u>File</u> <u>H</u> elp			
	t 🐌 Print 🗸 🔛 Convertor 🗮 Viewer 🕜 Help	Filtering criteria	C
Table name	IPD Viewer	ype Value	
	Backup is encrypted Enter a valid password to decrypt below and then press Apply button. Please enter password hank Apply Cancel	Thing TF-8 incode (UTF-16 BE) incode (UTF-16 LE) ate/Time LE Automation Date inx Epoch Time BE inx Epoch Time LE inx Epoch Time (ms) BE inx Epoch Time (ms) BE	
[Stop	OS X Epoch Time (HB) CE OS X Epoch Time LE BlackBerry Time BE BlackBerry Time BE Chrome Time BE Chrome Time LE	

Oxygen Forensics Suite BlackBerry IPD Viewer-the encrypted file

<u>File</u> <u>H</u> elp		
B	Open + Export 🍛 Print +	Converto
2	Table name	
V	Address Book - All (14)	~
V	Address Book - Last Used Hints (1)	1
V	Address Book Options (1)	_
V	Alarm Options (0)	_
J	Alarms (0)	=
1	Application Permissions (1)	-
V	Attachment Data (0)	
V	Attachment Data - Calendar (0)	
J	Attachment Options (1)	
1	AutoText (108)	
V	AutoText Data Version (1)	
V	BBGroups (8)	
1	BIS Account Data (0)	
V	BlackBerry Messenger (1)	
V	Bluetooth Options (1)	
V	Browser Bookmarks (1)	
1	Browser Channels (0)	
V	Browser Data Cache (28)	
V	Browser Folders (2)	
1	Browser Messages (0)	
V	Browser Options (1)	
V	Browser Push Options (1)	
V	Browser Urls (16)	
V	Calendar - All (0)	
V	Calendar Options (1)	
V	Camera Options (1)	
V	Categories (2)	
1	Certificate Options (0)	
V	Clock Options (1)	
V	Code Module Group Properties (49)	+

The Oxygen Forensics Suite BlackBerry IPD Viewer results