

iOS FORENSICS: WHERE ARE WE NOW AND WHAT ARE WE MISSING?

MATTIA EPIFANI – PASQUALE STIRPARO

SANS EU DIGITAL FORENSICS SUMMIT 2016

PRAGUE, 9 OCTOBER 2016





AGENDA

- iOS acquisition challenges
- Search and seizure of iOS Devices
- Acquisition techniques
- Alternative options
- Application analysis



iOS ACQUISITION CHALLENGES

iOS devices use full disk encryption

Other protection layers (i.e. per-file key, backup password)

JTAG ports are **not available**

- Chip-off techniques are not useful because of full disk encryption
 - But some experimental techniques are just out!



SEARCH AND SEIZURE OF iOS DEVICES

Turned off device

LEAVE IT OFF!

Turned on device (locked or unlocked)
DON'T TURN IT OFF AND THINK!



TURNED ON AND LOCKED

I. Activate Airplane mode

- 2. Connect to a **power source** (i.e. external battery)
- 3. Verify the **model**
- 4. Verify the **iOS version**



ACTIVATE AIRPLANE MODE LOCKED DEVICE





IDENTIFY THE MODEL (I)







IDENTIFY THE MODEL (II) AND THE iOS VERSION

- Libimobiledevice (Linux/Mac) http://www.libimobiledevice.org/
- Image: Model and Amage: Model and Amage: Model and Amage: Amag

ideviceinfo -s

They also work on locked devices!



EXAMPLE

santoku@santoku:~\$ ideviceinfo -s BasebandCertId: 3840149528 BasebandKeyHashInformation: AKeyStatus: 2 SKeyHash: u+/tcCwvaQ+1Y9t40I4yegCEmB28mALlaROhaIVGBWo= SKeyStatus: 0 BasebandSerialNumber: CKyShA== BasebandVersion: 1.23.00 BoardId: 4 BuildVersion: 13D15 ChipID: 32771 DeviceClass: iPhone DeviceColor: #272728 DeviceName: EpiPhone DieID: 6299231647892006 HardwareModel: N71mAP PartitionType: ProductName: iPhone OS ProductType: iPhone8,1 ProductVersion: 9.2.1 ProductionSOC: true ProtocolVersion: 2 TelephonyCapability: true UniqueChipID: 6299231647892006 UniqueDeviceID: 3bf682ebc55c5673d586e0273af0dfb72d1994a2 WiFiAddress: 1c:5c:f2:7f:7a:20 santoku@santoku:~\$



iPHONE MODEL CHART

Device name	Model number	Internal Name	ldentifier	Year	Capacity (GB)
iPhone SE	A1662 – A1723 – A1724	N69AP	iPhone8,4	2016	16,64
iPhone 6s Plus	A1634 – A1687 – A1699 – A1690	N66AP	iPhone8,2	2015	16,64,128
iPhone 6s	A1633 - A1688 - A1700 - A1691	N7IAP	iPhone8.1	2015	16,64,128
iPhone 6 Plus	A1522 – A1524 – A1593	N56AP	iPhone7, I	2014	16,64,128
iPhone 6	A1549 – A1586	N61AP	iPhone7,2	2014	16,64,128
iPhone 5S (CDMA)	A1457 – A1518 – A1528 – A1530	N53AP	iPhone6,2	2013	16, 32
iPhone 5S (GSM)	A1433 – A1533	N5IAP	iPhone6, I	2013	16, 32, 64
iPhone 5C (CDMA)	A1507 – A1516 – A1526 – A1529	N49AP	iPhone5,4	2013	16, 32
iPhone 5C (GSM)	A1456 – A1532	N48AP	iPhone5,3	2013	16, 32
iPhone 5 rev.2	A1429 – A1442	N42AP	iPhone5,2	2012	16, 32, 64
iPhone 5	A1428	N4IAP	iPhone5, I	2012	16, 32, 64
iPhone 4s (China)	A1431			2011	8, 16, 32, 64
iPhone 4S	A1387	NY4AP	iPhone4, I	2011	8, 16, 32, 64
iPhone 4 - CDMA	A1349	N92AP	iPhone3,2	2011	8, 16, 32
iPhone 4 - GSM	A1332	N90AP	iPhone3, I	2010	8, 16, 32
iPhone 3GS (China)	A1325			2009	8, 16, 32
iPhone 3GS	A1303	N88AP	iPhone2, I	2009	8, 16, 32
iPhone 3G (China)	A1324			2009	8, 16
iPhone 3G	A1241	ΝδζΑΡ	irnone1,2	2008	8, 16
iPhone 2G	A1203	M68AP	iPhone I, I	2007	4, 8, 16



TURNED ON AND UNLOCKED

- I. Prevent the phone locking!
 - I. Don't press power button!
 - II. Disable Auto-lock!
- 2. Verify if a lock code is set!
- 3. Activate Airplane mode
- 4. Connect to a **power source** (i.e. external battery)
- 5. Identify the model
- 6. Identify the **iOS version**



PREVENT LOCK STATE! (DISABLE AUTO-LOCK)

●●●○○ 3 ITA LTE	17:59	④ 37%
〈 General	Auto-Lock	
30 Seconds		
1 Minute		
2 Minutes		
3 Minutes		
4 Minutes		
5 Minutes		
Never		×



ACTIVATE AIRPLANE MODE UNLOCKED DEVICE





ACQUISITION TECHNIQUES

File System

- iTunes Backup
- Apple File Relay
- Zdziarski, 2014 Up to iOS 7
- Apple File Conduit
- iCloud
- Full file system

Result depends on iOS version

Can be password protected!

- Already stored data or forced
- n Possible only on jailbroken devices

Physical

- Available up to iPhone 4
- Possible on jailbroken 32-bit devices



iPHONE 4 AND BELOW

A physical acquisition is always possible In case of simple passcode all data will be decrypted

In case of complex passcode you will get in any case native applications data (i.e. address book, SMS, notes, video, images, etc.)



TURNED ON/OFF AND UNLOCKED

- Always possible doing some kind of file system acquisition
- The obtained data strongly depends on the iOS version
- Possible problems:
 - Backup password
 - Managed devices → Connection to PC inhibited



TURNED ON AND LOCKED

- Search for a lockdown certificate on a synced computer
- Unlock through fingerprint
- Try to force an iCloud backup
- Specific iOS version vulnerability for bypassing passcode



LOCKDOWN CERTIFICATE

- Stored in:
 - C:\Program Data\Apple\Lockdown
 - C:\Users\[username]\AppData\roaming\Apple Computer\Lockdown Vista
 - C:\Documents and Settings\[username]\Application Data\Apple Computer\Lockdown XP
 - /private/var/db/lockdown
 Mac OS X

Win 7/8/10

- Certificate file name → Device_UDID.plist
- The certificate can be extracted from the computer and used in another with some forensic tools or directly with iTunes
- Lockdown certificate stored on a computer is valid for 30 days
- Lockdown certificate can be used within 48 hours since last user unlocked with the passcode



FINGEPRINT UNLOCK

- To configure Touch ID, you must first set up a passcode. Touch ID is designed to minimize the input of your passcode; but your passcode will be needed for additional security validation:
 - After restarting your device
 - When more than 48 hours have elapsed from the last time you unlocked your device
 - To enter the Touch ID & Passcode setting
- https://support.apple.com/en-us/HT204587





FORCE ICLOUD BACKUP

- Be careful when using this option and try other methods first!
 - Possible overwriting of already existing backup
 - Risk of remote wiping
- Follow this approach:
 - Bring the device close to a known Wi-Fi network
 - Connect to a power source
 - Wait a few hours
 - Request data from Apple or download it
 - Legal authorization
 - Credentials or token is needed



SPECIFIC iOS VULNERABILITY

- A comprehensive and continuously updated list is maintained at:
- http://blog.dinosec.com/2014/09/bypassing-ioslock-screens.html
- Latest available for iOS 9.3.1
- CVE-2016-1852
 - "Siri in Apple iOS before 9.3.2 does not block data detectors within results in the lock-screen state, which allows physically proximate attackers to obtain sensitive contact and photo information via unspecified vectors."





TURNED OFF AND LOCKED

- Try to use a lockdown certificate
 - It works well on iOS 7 (AFR and AFC)
 - It can still get some data on iOS 8 (AFC)
 - Not useful on iOS 8/9/10
- Some specific unlocking tools
 - UFED User Lock Code Recovery Tool
 - IP-BOX
 - MFC Dongle
 - Xpin Clip





TURNED OFF AND LOCKED CAIS (CELLEBRITE ADVANCED INVESTIGATIVE SERVICES)

Unmatched Device Access

Continuing its commitment to deliver digital forensic breakthroughs, Cellebrite now makes the world's first "decrypted physical extraction" capability a reality for key iPhone and Samsung Android devices. Notably, this new capability enables forensic examiners and investigators to access the full file system to recover downloaded emails, third-party application data, geolocation data, and system logs, without needing to jailbreak the device.

Cellebrite's exclusive unlocking and decrypted physical extraction capabilities support the following devices:

- iPhone 4S / 5 / 5c, iPad 2 / 3G / 4G, iPad mini 1G, and iPod touch 5G running iOS 8.x (8.0 / 8.0.1 / 8.0.2 / 8.1 / 8.1.1 / 8.1.2 / 8.1.3 / 8.2/ 8.3 / 8.4 / 8.4.1) or iOS 9.x (9.0 / 9.0.1 / 9.0.2 / 9.1 / 9.2 / 9.2.1 / 9.3 / 9.3.1 / 9.3.2)
- Samsung Galaxy S6, Galaxy Note 5 and Galaxy S7 running all Android versions up to and including Marshmallow 6.0.1



iOS ARTIFACTS: ALTERNATIVE OPTIONS







ALTERNATIVE OPTIONS

- Local backup stored on user's computer
- Other data stored on user's computer
- Jailbreaking
- ICloud acquisition

Experimental techniques (chip-off)



BACKUP STORED ON THE USER'S COMPUTER

	Wattia ► AppData ► Roaming ► Apple Computer ► N	VlobileSync 🕨 Backup	► - +
File Modifica	Visualizza Strumenti ?		
Organizza 🔻	Includi nella raccolta 👻 Condividi con 👻 Masterizza Nu	uova cartella	
🚖 📤 No	me	Ultima modifica	Тіро
💻 📜	3bf682ebc55c5673d586e0273af0dfb72d1994a2	03/09/2016 16:55	Cartella di file
4 1	26ccdbcb74b2ab8e9e97aa096883a10442c6f2ef	03/09/2016 17:56	Cartella di file
? 📜	929ffc5a169dd446ed36998f9b61153b85adba52	26/02/2016 16:46	Cartella di file



ENCRYPTED BACKUP

iPhone 6s

Capacity: 55,53 GB Phone Number: +39 334 2340899 Serial Number: F17QT811GRY9 iOS 9.3.5

Your iPhone software is up to date. iTunes will automatically check for an update again on 08/09/2016.

Check for Update Restore iPhone...

Backups

Automatically Back Up

iCloud

Back up the most important data on your iPhone to iCloud.

This computer

A full backup of your iPhone will be stored on this computer.

🗹 Encrypt iPhone backup

This will allow account passwords, Health, and HomeKit data to be backed up.

Change Password...

Manually Back Up and Restore

Manually back up your iPhone to this computer or restore a backup stored on this computer.

Back Up Now Restore Backup...

Latest Backup:

Today 22:13 to this computer

Oxygen Forensic® Extr Password recovery. Please wait.	actor	33
	Please wait while Passware Kit Forensic program password. If you know the password, please stop to password for the current image. Current algorithm: Passware Kit Attacks List Estimated time: 00:05:11 Elapsed time: 00:00:29 Reading device: Apple iPhone 45 S/N: 013180000237540 Stop! I know the pass	n is searching for the image the process and enter the change algorithm
e Help		Cancel



iOS IO ENCRYPTED BACKUP WEAKNESS



iOS 10: Security Weakness Discovered, Backup Passwords Much Easier to Break

September 23rd, 2016 by Oleg Afonin

We discovered a major security flaw in the iOS 10 backup protection mechanism. This security flaw allowed us developing a new attack that is able to bypass certain security checks when enumerating passwords protecting local (iTunes) backups made by iOS 10 devices.

The impact of this security weakness is severe. An early CPU-only implementation of this attack (available in Elcomsoft Phone Breaker 6.10) gives a 40-times performance boost compared to a fully optimized GPU-assisted attack on iOS 9 backups.



OTHER DATA STORED ON THE USER'S COMPUTER

					x
🕒 🗸 📕 « AppData 🕨 Roami	ng 🕨	Apple Computer 🕨 Logs 🕨 👻 🗲	Cerca Logs		٩
Organizza 🔻 🛛 Includi nella raccol	a 🔻	Condividi con 🔻 Masterizza Nuova	cartella	= -	0
💱 Dropbox	•	Nome	Ultima modifica	Тіро	<u>^</u>
🛞 Foto iCloud		퉬 CrashReporter	10/02/2016 20:29	Cartella di file	
	_	🌗 DeviceLink	24/09/2015 11:35	Cartella di file	=
Raccolte		🖻 asl.094128_17Aug16.log	17/08/2016 10:12	File LOG	
Documenti		📓 asl.102713_31Aug16.log	01/09/2016 22:13	File LOG	
Dropbox	=	📓 asl.103155_17Aug16.log	30/08/2016 17:22	File LOG	
		🖻 asl.190534_11Aug16.log	12/08/2016 19:16	File LOG	
		CloudDocsProvider.2016-05-05_1942.log	05/05/2016 19:42	File LOG	
Video		CloudDocsProvider.2016-05-06_1445.log	06/05/2016 14:45	File LOG	
		CloudDocsProvider.2016-06-17_1129.log	17/06/2016 11:29	File LOG	
Computer		CloudDocsProvider.2016-07-03_1922.log	03/07/2016 19:23	File LOG	
Disco locale (C:)		CloudDocsProvider.2016-07-22_1006.log	22/07/2016 10:06	File LOG	
Dati (D:)		ClaudDaceDravidar 2016 07 22 1642 laa	22/07/2016 16:42	Ella LOG	
Unita BD-KOM (J:) KDS_251					-
34 elementi					



OTHER DATA STORED ON THE USER'S COMPUTER

Installed applications list and usage

Various logs like PowerLog, Security, OnDemand

iTunes username

- itunesstored.2.log file
- File name of e-mail attachments
 - MobileMail logs
- List of Wi-Fi networks and history of latest connections
 - Wi-Fi logs



ONDEMAND LOG

C:\Users\	Mattia\AppData\Roaming\Apple Computer\Logs\CrashReporter\MobileDevice\EpiPhone\DiagnosticLogs\ondemandd\ondemandd_2016-02-15-163740.log	x
. 3	👗 📲 🛅 🧐 🍽 📇 🍇 🔟	
1	Feb 15 17:37:40_ondemandd[439] < Debug>: App did change state : net.whatsapp.WhatsApp(388) 4	
2	Feb 15 17:37:55 ondemandd[439] < Debug>: App did change state : net.whatsapp.WhatsApp(388) 2	
3	Feb 15 17:42:55 ondemandd[439] < Debug>: App did change state : net.whatsapp.WhatsApp(388) 8	
4	Feb 15 17:43:54 ondemandd[439] < Debug>: App did change state : net.whatsapp.WhatsApp(388) 4	
5	Feb 15 17:43:55 ondemandd[439] < Debug>: App did change state : com.apple.Preferences(457) 8	
6	Feb 15 17:43:57 ondemandd[439] <debug>: App did change state : com.apple.Preferences(457) 4</debug>	
7	Feb 15 17:43:57 ondemandd[439] < Debug>: App did change state : com.apple.Preferences(457) 2	
8	Feb 15 17:43:57 ondemandd[439] < Debug>: App did change state : com.apple.camera(458) 8	
9	Feb 15 17:44:09 ondemandd[439] <debug>: App did change state : net.whatsapp.WhatsApp(388) 2</debug>	
10	Feb 15 17:48:04 ondemandd[439] <debug>: App did change state : com.apple.camera(458) 4</debug>	
11	Feb 15 17:48:04 ondemandd[439] <debug>: App did change state : net.whatsapp.WhatsApp(388) 8</debug>	
12	Feb 15 17:48:09 ondemandd[439] <debug>: App did change state : com.apple.camera(458) 2</debug>	
13	Feb 15 17:48:21 ondemandd[439] <debug>: App did change state : net.whatsapp.WhatsApp(388) 4</debug>	
14	Feb 15 17:48:21 ondemandd[439] < Debug>: App did change state : com.apple.mobilemail(387) 8	
15	Feb 15 17:48:46 ondemandd[439] < Debug>: App did change state : net.whatsapp.WhatsApp(388) 8	
16	Feb 15 17:48:47 ondemandd[439] < Debug>: App did change state : com.apple.mobilemail(387) 4	
17	Feb 15 17:50:02 ondemandd[439] < Debug>: App did change state : com.apple.mobilecal(199) 4	
18	Feb 15 17:50:10 ondemandd[439] < Debug>: App did change state : net.whatsapp.WhatsApp(388) 4	
19	Feb 15 17:50:10 ondemandd[439] < Debug>: App did change state : com.apple.mobilemail(387) 8	
20	Feb 15 17:50:11 ondemandd[439] < Debug>: App did change state : com.apple.mobilecal(199) 2	
21	Feb 15 17:51:06 ondemandd[439] < Debug>: App did change state : com.apple.mobilemail(387) 4	
22	Feb 15 17:51:09 ondemandd[439] < Debug>: App did change state : net.whatsapp.whatsApp(388) 2	
25	Feb 15 17:51:24 ondemandd[459] < Debug>: App did change state : net.whatsapp.whatsApp(566) 6	
24	Feb 15 17:54:05 ondemandd[459] < Debug>: App did change state : net.whatsapp.whatsApp(566) 4	
25	Feb 15 17/54/20 - ondemandul(439) < Debug >: App did change state : net.whatsapp.whatsApp(500) o	
20	Feb 15 17:54:22 ondemandd[439] < Debug >: App did change state : net.whatsapp.whatsApp(500) 4 Feb 15 17:54:22 ondemandd[439] < Debug >: App did change state : com apple mobilemail(387) 8	
28	Feb 15 17:54:47 ondemandd[439] < Debug>: App did change state: com.apple.mobilemail(387) 4	-
20	i co 19 1/19/17 ondernanda (199) (bebuge repp and enange state reonnappien obiental (907) 4	
		·



SECURITY LOG

C	:\Users\	Mat	tia\AppDa	ta\Ro	amir	ng\Ap	ple (Comp	uter\	Logs\CrashReporter\MobileDevice\EpiPhone\DiagnosticLogs\security.log.20160215T230034Z
	. 🖹	X	1	5	6	A	<u>aa</u>	^b ₽	Ф	
	1		Feb 16 0	0:00:34	4 sec	urity	:[90]	<erro< td=""><td>or> [S</td><td>ecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2 🔺</td></erro<>	or> [S	ecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2 🔺
	2		Feb 16 0	0:00:3	4 sec	urity	1[90]	<not< td=""><td>tice></td><td>[item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct,:</td></not<>	tice>	[item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct,:
	3		Feb 16 0	0:00:3	4 sec	urityo	1[90]	<not< td=""><td>tice></td><td>[engine{}]: engine (null): will-commit api 1 changes</td></not<>	tice>	[engine{}]: engine (null): will-commit api 1 changes
	4		Feb 16 0):02:0	/ sec	unityo	1001	<erro< td=""><td>or> [5</td><td>ecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2</td></erro<>	or> [5	ecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
	5		Feb 16 0):02:0	/ sec	unityo	1001	<not< td=""><td>tice></td><td>[item{}]: item SecDbItemDoUpdate replaced O,genp,t8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct,</td></not<>	tice>	[item{}]: item SecDbItemDoUpdate replaced O,genp,t8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct,
	6		Feb 16 00	02:02	/ sec	unityo	1001	<not< td=""><td>tice></td><td>[engine{}]: engine (null): will-commit api 1 changes</td></not<>	tice>	[engine{}]: engine (null): will-commit api 1 changes
	/		Feb 16 00):02:2	5 sec	unityo	1001	<erro< td=""><td>or> [5</td><td>ecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2</td></erro<>	or> [5	ecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
	8		Feb 10 00	J:02:2	o sec	unityo	1001	< Not	tice>	[item{}]: Item SecubitemDoUpdate replaced O,genp,t8027085,L,dku,UKFA9XBX0K.net.wnatsapp.wnatsApp,5208,acct,:
	10		Feb 10 00	J:02:2	o sec	unityo	1001		tice>	[engine{}]: engine (nuil): will-commit api 1 changes
	10		Feb 10 00	J:02:5.	o sec	unityo	1001	< Not	n > [a lice)	Recogging{}]: Securityd_xpc_dictionary_nandler whatsApp[366] add Error Domain=NSOSStatusErrorDomain Code=-2
	12		Ech 16.00	1:02:5.	2 580	unity	1001	< Not	tices	[item{}]; item Secontempolopidate replaced O,genp.cov27003,L,dku,OKrA9AbAoK.net.wnatsapp.wnatsApp,3200,acct,:
	12		Feb 16 0	02.5	0 sec	unity	1001	< Erro	ars 19	rengine(7): engine (nui): will-commit april changes
	14		Feb 16 0	0.21.3	0 sec	urity	4[00]	<not< td=""><td>tice></td><td>Litem ()]; item SecDhitemDol Indate replaced O genn F8027085 L dku LIKEA9XBX6K net whatsann WhatsAnn 5268 acct</td></not<>	tice>	Litem ()]; item SecDhitemDol Indate replaced O genn F8027085 L dku LIKEA9XBX6K net whatsann WhatsAnn 5268 acct
	15		Feb 16 0	0.21.3	0 sec	urity	4[90]	<not< td=""><td>tice></td><td>[engine{}]: engine_(null): will-commit ani 1 changes</td></not<>	tice>	[engine{}]: engine_(null): will-commit ani 1 changes
	16		Feb 16 0	0:21:4	6 sec	urity	1001	<frre< td=""><td>r > 19</td><td>ecligating{}]: engine (itali): will comme up 1 enanges</td></frre<>	r > 19	ecligating{}]: engine (itali): will comme up 1 enanges
	17		Feb 16 0	0:21:4	6 sec	urity	1001	<not< td=""><td>tice></td><td>[item{}]; item SecDbItemDoUpdate replaced O.genp.E8027085.L.dku.UKFA9XBX6K.net.whatsapp.WhatsApp.5268.acct;</td></not<>	tice>	[item{}]; item SecDbItemDoUpdate replaced O.genp.E8027085.L.dku.UKFA9XBX6K.net.whatsapp.WhatsApp.5268.acct;
	18		Feb 16 0	0:21:4	6 sec	urity	1001	<not< td=""><td>tice></td><td>[engine{}]: engine (null): will-commit api 1 changes</td></not<>	tice>	[engine{}]: engine (null): will-commit api 1 changes
	19		Feb 16 0):25:4:	1 sec	urity	1001	<erro< td=""><td>or> [S</td><td>ecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2</td></erro<>	or> [S	ecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
	20		Feb 16 0):25:4:	1 sec	urity	1[90]	<not< td=""><td>tice></td><td>[item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct,</td></not<>	tice>	[item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct,
	21		Feb 16 0):25:4:	1 sec	urity	1[90]	<not< td=""><td>tice></td><td>[engine{}]: engine (null): will-commit api 1 changes</td></not<>	tice>	[engine{}]: engine (null): will-commit api 1 changes
	22		Feb 16 0):27:3	9 sec	urity	:[90]	<erro< td=""><td>or> [S</td><td>ecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2</td></erro<>	or> [S	ecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
	23		Feb 16 0	0:27:3	9 sec	urity	:[90]	<not< td=""><td>tice></td><td>[item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct,:</td></not<>	tice>	[item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct,:
	24		Feb 16 0	0:27:3	9 sec	urityo	:[90]	<not< td=""><td>tice></td><td>[engine{}]: engine (null): will-commit api 1 changes</td></not<>	tice>	[engine{}]: engine (null): will-commit api 1 changes
	25		Feb 16 0	0:32:1	8 sec	urity	:[90]	<erro< td=""><td>or> [S</td><td>SecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2</td></erro<>	or> [S	SecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
	26		Feb 16 0):32:1	8 sec	urity	1[90]	<not< td=""><td>tice></td><td>[item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct,:</td></not<>	tice>	[item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct,:
	27		Feb 16 0):32:1	8 sec	urity	1[90]	<not< td=""><td>tice></td><td>[engine{}]: engine (null): will-commit api 1 changes</td></not<>	tice>	[engine{}]: engine (null): will-commit api 1 changes
	28		Feb 16 0):33:0	2 sec	urity	1[90]	<erro< td=""><td>or> [S</td><td>ecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2 🔻</td></erro<>	or> [S	ecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2 🔻
	•									4

Т



ITUNESSTORED.2.LOG

📔 C:\U	Jsers\Matt	ia\Deskto	op∖iPhone L	ogs\Appl	e iPhone	Logs\Apple iPhone Logs\EpiPhone\com.apple.itunesstored\itunesstored.2.log - Notepad++	x
File I	Modifica	Cerca	Visualizza	Formato	Lingua	ggio Configurazione Macro Esegui Plugin Finestra ?	Х
i 🔓 🕻	986	1 🗟 🕻		b b	9 C	🏙 🍇 👒 👒 🖫 😼 🗄 🚍 👖 運 🖾 🔊 💿 🗉 🕨 🞼 🚟 🧟	
itune	esstored.2.k	og 🗵					
4196	2016-	-01-31	11:59:5	2.930	[114]:	ISProtocolDataProvider: Saw token failure: 2002	
4197	2016-	-01-31	11:59:5	2.930	[114]:	ISProtocolDataProvider: Error processing protocol: Error Domain=SSErrorDomain Code=18 "Cannot connect to iTunes Store" UserInfo={NSLoca	li
4198	2016-	-01-31	11:59:5	2.930	[114]:	ISStoreURLOperation: Attempt retry after token error: Error Domain=SSErrorDomain Code=18 "Cannot connect to iTunes Store" UserInfo={NSI	.oc
4199	2016-	-01-31	11:59:5	2.938	[114]:	PushNotificationController: Adding APS client for <u>itunesstored</u>	
4200	2016-	-01-31	11:59:5	2.938	[114]:	AuthenticateOperation: Token is expired (type: 0)	
4201	2016-	-01-31	11:59:5	2.939	[114]:	PushNotificationController: Environment is now production	
4202	2016-	-01-31	11:59:5	2.939	[114]:	PushNotificationController: Posting 1 environment tokens	
4203	2016-	-01-31	11:59:5	2.940	[114]:	AuthenticateOperation: Running authenticate attempt 0	
4204	2016-	-01-31	11:59:5	2.940	[114]:	AuthenticateAttemptOperation: Authenticating with context: <ssauthenticationcontext: 0x13df5eff0="">: (0, 1321761630, mattiaep@hotmail.it)</ssauthenticationcontext:>	
4205	2016-	-01-31	11:59:5	2.942	[114]:	PostPushNotificationTokenOperation: Posting APS token for production	
4206	2016-	-01-31	11:59:5	2.942	[114]:	ISStoreURLOperation: Resolved bag entry [0-1321761630-itunesstored/1.0 iOS/9.2.1 model/iPhone8,1 hwp/s8003 build/13D15 (6; dt:141)-1434	150
4207	2016-	-01-31	11:59:5	2.949	[114]:	ISStoreURLOperation: Making POST request, with service type: 0, for URL: <u>https://p36-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/r</u>	<u>eq</u>
4208	2016-	-01-31	11:59:5	2.951	[114]:	ISStoreURLOperation: Sending headers for <u>https://p36-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/registerSuccess:</u>	
4209	{						
4210		"Accept	t-Langua	ge" =	"en-IT'	';	
4211	· · · ·	"Conte	nt-Type"	= "apj	plicati	ion/x-apple-plist";	
4212	C (Cookie	= "itre	=1; <u>mt</u>	- <u>asn</u> -13	321761630=13; amp=udroRiI/w5f0QJSXEU7DXxDvGpOwdO3FPNcfcGths68jwTJTBR1up2CWQAiyVUEz1dZ9g5G13GFnPXib9HgUWTmuRbYL2YpS/aqof9frawEUsrD8XNbKsr	ıjb
4213		"User-J	Agent" =	"itun	esstore	ed/1.0 iOS/9.2.1 model/iPhone8,1 hwp/s8003 build/13D15 (6; dt:141)";	
4214	· · ·	"X-App	le-Actio	nSigna	ture" =	#Aq43ssOfXkX8yMYWLGGLi55C+hr95wWPI8PPSP0cz+wnAAABUAMAAACNAAAAgJ7ISJpPzyxW6HY9YHV4qZs0SE555mP3FZAy+vy7nS2866MzLme2Ba6uudfZyjP9KEPAvp800	:/4
4215		"X-App	le-Clien	t-Vers	ions" =	= "GameCenter/2.0";	
4216		"X-App	Le-Conne	ction-	Гуре" =	= WiFi;	-
•							•
,							

length : 4194336 lines : 43602

Ln:4204 Col:155 Sel:8 0

UNIX

UTF-8 w/o BOM

INS

Normal text file



MOBILEMAIL LOG

🔡 *C	:\Users\Mattia\AppData\Roaming\Apple Computer\Logs\CrashReporter\MobileDevice\EpiPhone\Message\MobileMail_2016_02_11_14_03_100100.log - Notepad++
File	Modifica Cerca Visualizza Formato Linguaggio Configurazione Macro Esegui Plugin Finestra ? X
1	
1	
🗎 Mo	obileMail_2016_02_11_14_03_100100.log
1	2016-02-11 14:03:10.182 [164:0x14ed86d40] LogOther: ERROR: MFMessageErrorDomain/Inaccessible Password - The password for "Reality" cannot be used at this time.
2	2016-02-11 15:22:21.386 [164:0x14ee0dcf0] LogOther: ERROR: NSPOSIXErrorDomain/60 - The mail server "imap.gmail.com" is not responding. Verify that you have entered the correct accoun
3	2016-02-11 22:48:51.206 [385:0x125511300] LogAttachments: [Attachment] Failed to fetch data for attachment
4	[file:///var/mobile/Library/Mail/IMAP-mattia.epifani@realitynet.it@imap.gmail.com/%5CInbox.imapmbox/Attachments/9648/2/Verbale_5%20febbraio%202016.doc]
5	2016-02-12 06:06:31.389 [405:0x100512d30] LogAttachments: [Attachment] Failed to fetch data for attachment
6	[file:///var/mobile/Library/Mail/IMAP-mattia.epifani@realitynet.it@imap.qmail.com/%5CInbox.imapmbox/Attachments/9653/1.2/od_for610_b01_01.5.docx]
7	2016-02-12 06:06:31.394 [405:0x100512d30] LogAttachments: [Attachment] Failed to fetch data for attachment
8	[file:///var/mobile/Library/Mail/IMAP-mattia.epifani@realitynet.it@imap.gmail.com/%5CInbox.imapmbox/Attachments/9653/1.3/2016%20SANS%20OnDemand%20Quiz%20Key%20Points%20Form.docx]
9	2016-02-12 06:06:42.825 [405:0x100512d30] LogAttachments: [Attachment] Failed to fetch data for attachment
10	[file:///var/mobile/Library/Mail/IMAP-mattia.epifani@realitynet.it@imap.gmail.com/%5CInbox.imapmbox/Attachments/9654/1.2/od_for610_b01_01.5.docx]
11	2016-02-12 06:35:54.598 [405:0x103965110] LogLibraryErrors: skipping cleaning up protected tables because protected data is not available
12	2016-02-13 02:36:38.562 [405:0x100512d30] LogAttachments: [Attachment] Failed to fetch data for attachment
13	[file:///var/mobile/Library/Mail/IMAP-mattia.epifani@realitynet.it@imap.qmail.com/%5Clnbox.imapmbox/Attachments/9763/1/mime-attachment]
14	2016-02-13 02:36:38.572 [405:0x100512d30] LogAttachments: [Attachment] Failed to fetch data for attachment
15	[IIIe:///var/mobile/Library/Mail/IMAP-mattia.epifanigrealityhet.itgimap.qmail.com/%5cinbox.imapmbox/Attachments/9/63/2/encrypted.asc]
10	2016-02-13 1/:36:33.904 [[163:0x13ed04de0]]Logother: ERKOK: MrMessageErrorDomain/Socket Read - The connection to the server failed.
10	2016-02-13 20:03:03:026[[163:0x140//6060]]LogLibraryErrors: Skipping cleaning up protected tables because protected data is not available
10	2016-02-15 20:10:02.808 [[165:0XISed04de0]]LogAttachments: [Attachment] railed to fetch data for attachment
20	(1112:///var/mobile/Library/Mail/IMAr-mattia.epitanigreatityhet.itgimap.qmail.com/solihox.imapmbox/Attachments/9/96/2/Evibence.b5.1-rechnicalspecifications-v2.0-sci_rev.cnk.docx)
20	zoio-bz-14 11:59:55./15[[56/:0x150556dc0]]LogLibraryEriors: Skipping Cleaning up protected tables because protected data is not available
Find re:	sult - 22 hits
Norma	al text file length : 3160 lines : 24 Ln : 22 Col : 1 Sel : 0 0 UNIX UTF-8 w/o BOM OVR



Wi-Fi LOG

2 *	C:\Users\	Mattia\AppD)ata\Roaming\Apple Computer\Logs\CrashReporter\MobileDevice\EpiPhone\WiFi\WiFiManager\wifi-02-16-2016_074920.log - Notepad++ 💷 💷 🔤	
File	Modifi	a Cerca	Visualizza Formato Linguaggio Configurazione Macro Esegui Plugin Finestra ?	Х
1) 🗗 🗐		· A ★ h h ⊃ c # ½ < < G = 5 1 I I = 2	
	wifi-02-16-2	016_074920		_
25	96			^
25	97 2	/16/2016	7:42:37.393 Aborting EAP	
25	98 2	/16/2016	7:42:37.393 Aborted current auto-join session.	
25	99 2	/16/2016	7:42:37.393 WiFiDeviceManagerSetNetworks: shouldDisassociate 0	
26	200	/16/2016	7:42:37.393WiFiDeviceManagerAutoAssociate: Already connected to m3connect.	
26	01 2	/16/2016	7:42:37.395 CreateBGScanRequest Hotspot m3connect added to BGScan List	
26	02 2	/16/2016	7:42:37.395 CreateBGScanRequest Hotspot ibis added to BGScan List	
26	03 2	/16/2016	7:42:37.395CreateBGScanRequest Hotspot San <u>Martino</u> Hospital Free added to BGScan List	
26	04 2	/16/2016	7:42:37.395CreateBGScanRequest Hotspot Airport_Free_WiFi added to BGScan List	
26	05 2	/16/2016	7:42:37.395CreateBGScanRequest Hotspot WiFi in de trein added to BGScan List	
26	06 2	/16/2016	7:42:37.396 Preparing background scan request for	
26	07 "	m3connect	t" "ibis" "lrz" "Marriott_CONFERENCE" "rnsys" "NETGEAR13" "EPIFANI_DLINK" "San <u>Martino</u> Hospital Free"	
26	08 "	212genova	a" "Vodafone-25344705" "Telecom-45376345" "Airport_Free_WiFi" "WiFi in de <u>trein</u> " "Babylon Free WiFi"	
26	09 "	Meeting (Center" "Leidse Square Hotel" "60:c5:47:4f:51:1d ~ EN" "60:c5:47:4d:cd:6f ~ EN" "60:c5:47:4f:51:1c ~ EN"	
26	10 2	/16/2016	7:42:37.403 WiFiDeviceRequestAssociatedSleep: ActiveDuringSleepRequested is already set (<cfbasichash (<="" th=""><th></th></cfbasichash>	
26	11 en	tries =>		-1
26	12 }			
26	13).			
26	14 2	/16/2016	7:42:37.415WiFiDeviceManagerAutoAssociate: Already connected to m3connect.	
26	15 2	/16/2016	7:42:37.417 No Change in Background Scan Networks, Skip Re-Programming Background Scan_	
26	16			
26	17 2	/16/2016	7:42:38.342 WiFiManagerCellularTransmitCallback block invoke: Cellular Transmit Started = FALSE	
Find	result - 22 ł	nits		×
A.	1			



MOBILEMEACCOUNTS.PLIST

C:\Users\Mattia\AppData\Roaming\Apple Computer\Preferences\MobileMeAccounts.plist

File Edit View Help

🗋 🖻 📕 👗 🔓 🗳 🥘

XML View	List View	

	1		xml version="1.0" encoding="UTF-8"?					
- 1	2		plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd"					
- 1	3	-	version="1.0">					
- 1	4	-	<dict></dict>					
- 1	5		<key>Accounts</key>					
- 1	6	-	<array></array>					
- 1	7	-	<dict></dict>					
- 1	8		<key>AccountDSID</key>					
- 1	9		<string>461496998</string>					
- 1	10		<key>AccountDescription</key>					
- 1	11		<string>iCloud</string>					
- 1	12		<key>AccountID</key>					
- 1	13		<string>jailbreakingios@icloud.com</string>					
- 1	14		<key>DisplayName</key>					
- 1	15		<string>Jailbreaking Test</string>					
- 1	16		<key>IsPaidAccount</key>					
- 1	17		<false></false>					
- 1	18		<key>LoggedIn</key>					
- 1	19		<true></true>					
- 1	20		<key>Services</key>					
- 1	21	-	<array></array>					
- 1	22	-	<dict></dict>					
- 1	23		<key>EmailAddress</key>					
- 1	24		<string>jailbreakingios@icloud.com</string>					
- 1	25		<key>Enabled</key>					
- 1	26		<true></true>					
	27		<key>FullUserName</key>					
	28		<string>Jailbreaking Test</string>					



IPODDEVICES.XML

📔 C:\Users\M	lattia\AppData\Local\Apple Computer\iTunes\iPodDevices.xml - Notepad++					
File Modifica	a Cerca Visualizza Formato Linguaggio Configurazione Macro Esegui Plugin Finestra	?				3
) -] [] [b 😘 🖓 🖌 🖿 🖬 🗩 🖒 🖮 🦕 🔍 🔍 🖫 🔤 🗉 🗍 🗐 🖉 🖉 🖉 📼 👁					
📄 iPodDevice	is xml 🔀					
104	<key>Updater Family ID</key>					
105	<integer>10022</integer>					
106	<key>Use Count</key>					
107	<integer>2</integer>					
108 -						
109	<key>6883A10442C6F2EF</key>					
110 🛱	<dict></dict>					
111	<key>Connected</key>					
112	<pre><date>2016-09-03T15:50:49Z</date></pre>					
113	<key>Device Class</key>					
114	<string>iPhone</string>					
115	<key>Family ID</key>					
116	<integer>10016</integer>					
117	<key>Firmware Version</key>					
118	<integer>256</integer>					
119	<key>Firmware Version String</key>					
120	<string>9.3.2</string>					
121	<key>ID</key>					
122	<string>6883A10442C6F2EF</string>					
123	<key>IMEI</key>					
124	<string>013180000237540</string>					
125	<key>Region Info</key>					:
126	<string>IP/A</string>					
127	<key>Serial Number</key>					
128	<string>DNRJ9Z9SDTC0</string>					L
129	<key>Updater Family ID</key>					
130	<integer>10016</integer>					
131	<key>Use Count</key>					
132	<integer>21</integer>					
133 -						
134	<key>9B61153B85ADBA52</key>					
135 🛱	<dict></dict>					
136	<key>Connected</key>					
137	<pre><date>2016-02-26T15:45:31Z</date></pre>					
138	<key>Device Class</key>					
139	<string>iPhone</string>					
140	<key>Family ID</key>					
1/1	/integer/10007//integer/					
						•
Xtensible Ma	rkup Language file	length : 5610 lines : 212	Ln:1 Col:1 Sel:0 0	UNIX	UTF-8	INS

length : 5610 lines : 212 eXtensible Markup Language file Ln:1 Col:1 Sel:0[0 Y .



JAILBREAKING HTTPS://WWW.THEIPHONEWIKI.COM/WIKI/JAILBREAK

C:\Windows\system32\cmd.exe Welcome to Elcomsoft iOS Forensic Toolkit This is driver script version 2.0/Win for A5+ (c) 2011-2015 Elcomsoft Co. Ltd.	
Please select an action: 1 N/A 2 N/A 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	•



- You need user credentials or token extracted from a computer (Windows/Mac) with iCloud Control Panel
- You can obtain
 - iCloud Device Backup
 - iCloud Calendars
 - iCloud Contacts
 - Photo Streams
 - Email
 - Specific application data





- You need user credentials or token extracted from a computer (Windows/Mac) with iCloud Control Panel
- You can obtain
 - iCloud Device Backup
 - iCloud Calendars
 - iCloud Contacts
 - Photo Streams
 - Email
 - Specific application data

Elcomsoft eXplorer for WhatsApp					
ile View Help					
;≡					
					🔀 Cancel
	Dov	wnload data from iCloud	1		
	Authentication type	Password Token	?		
	Apple ID		(6	example@example.com)	
	-				
	Password		•		
				Sign in	



- You need user credentials or token extracted from a computer (Windows/Mac) with iCloud Control Panel
- You can obtain
 - iCloud Device Backup
 - iCloud Calendars
 - iCloud Contacts
 - Photo Streams
 - Email
 - Specific application data

Oxygen Forensic® Extractor	
Access to iCloud account	
	Enter iCloud account credentials
	Please fill in account details to get an access to the device
	data stored in iCloud.
	Apple ID:
	Password:
iCloud	Sign in
iciouu	



- You need user credentials or token extracted from a computer (Windows/Mac) with iCloud Control Panel
- You can obtain
 - iCloud Device Backup
 - iCloud Calendars
 - iCloud Contacts
 - Photo Streams
 - Email
 - Specific application data

Oxygen Forensic® Cloud Extractor	- 2.7.0.160				
	Service	Credentials			Valida
Oxygen Forensic* Chude Extensio* Dustry-first in Cloud Forensics	Add cloud service Add cloud	. The story story			
	 Google Photos Google Photos Google Tasks iCloud Applications iCloud Calendars iCloud Contacts iCloud Drive (Device iCloud Drive (Web / 	e Em Access)			
Help Settings About	 iCloud Photos Live Calendars Live Contacts OneDrive Swarm (Foursquare Twitter 	.)	Back	Next	Cancel
key evidence section displays	WhatsApp Google h	Dackup	messages, event log,	Search section allo	ws to search for the specifie



APPLE SUPPORT (ICLOUD DATA) HTTP://IMAGES.APPLE.COM/PRIVACY/DOCS/LEGAL-PROCESS-GUIDELINES-US.PDF

- You can request:
 - Subscriber information
 - Mail logs
 - Email content

i. Subscriber Information

When a customer sets up an iCloud account, basic subscriber information such as name, physical address, email address, and telephone number may be provided to Apple. Additionally, information regarding iCloud feature connections may also be available. iCloud subscriber information and connection logs with IP addresses can be obtained with a subpoena or greater legal process. Connection logs are retained up to 30 days.

- Other iCloud Content (iOS Device Backups, Photo Stream, Docs, Contacts, Calendars, Bookmarks)
- Find My iPhone
- Game Center
- iOS Device Activation
- Sign-on logs
- My Apple ID and iForgot logs
- FaceTime logs



EXPERIMENTAL TECHNIQUES - CHIP OFF

- Recently published research by Sergei Skorobogatov
- The bumpy road towards iPhone 5C NAND mirroring
 - http://www.cl.cam.ac.uk/~sps32/5c_proj.html
 - https://arxiv.org/pdf/1609.04327v1.pdf
 - https://www.youtube.com/watch?v=tM66GWrwbsY



iOS ACQUISITION TOOLS

Forensic Tools

Cellebrite Physical Analyzer

Oxygen Forensic

Elcomsoft Phone Breaker

Elcomsoft iOS Forensic Toolkit

Magnet Acquire

XRY

MPE+

Paraben Device Seizure

Other tools

iTunes

Libimobiledevice

iMobiledevice

iFunBox

iTools

iExplorer



iOS APPLICATION ANALYSIS







HOW AND WHERE DATA IS STORED

Starting from iOS8, application data have been separated from their bundles and current directory structure is the following

- Iprivate/var/mobile/Containers/Bundle/Application/<UUID>/: This path is the actual path where the application bundle is stored.
- Iprivate/var/mobile/Containers/Data/Application/<UUID>/: This path is the actual path where most of the application data is stored.
- Iprivate/var/mobile/Containers/Shared/AppGroup/<UUID>/: As the name of the folder suggests, this path is the path where applications can store data with the aim of sharing it with other apps or extensions.

File formats are the usual plist files and SQLite databases



DO NOT FORGET THE FADE-OUT EFFECT

- Every time a user presses the Home button or receives a call while using an application, iOS will make a "snapshots" of the current screen in order to be able to do the fade-out effect transition between the two screens.
- /private/var/mobile/Library/Caches/ Snapshots/ for the pre-installed Apple applications;
- /private/var/mobile/Containers/Data/ Applications/<UUID>/Library/Caches/ Snapshots/, for each third-party application





DO NOT FORGET THE FADE-OUT EFFECT





"SECURE" MESSAGING IN iOS

 WhatsApp,Telegram and Signal among the most widespread applications for instant messaging.

All of them claim "secure" messaging to a certain extent.

All of them have end-to-end encryption (data-in-transit), but we will focus on the artifacts left on the device (data-at-rest).



WHATSAPP

- Data is stored in the Shared directory instead of the application data directory /private/var/mobile/Containers/Shared/AppGroup/332A098D-368C-4378-A503-91BF33284D4B
 - -- Axolotl.sqlite
 - -- ChatSearch.sqlite
 - -- ChatStorage.sqlite
 - -- Contacts.sqlite
- Some of the tables of interest are:
 - ZWACHATSESSION, ZWAGROUPMEMBER, ZWAGROUPINFO and ZWAMEDIAITEM, which stores references to the multimedia files exchanged, indication of the users involved, timestamps, the path where the file has been stored, etc.



WHATSAPP

 ZWAMESSAGE contains, among others, the messages exchanged, their timestamp, the name of the user involved in the chat.

iS	AI ZMESSAGEDATE	ZSENTDATE	ZFROMJID	ZMEE	ZPUSHN	AME	ZSTANZAID	ZTEXT	ZTO	ID
1	429476024.647006						140	Prov	3932	9
2	429476038.539024						140	Prov	3934	9
3	429476152		39329		Ric	ssi	140	Nor		
1	429477100		39329		Ric	ssi	140	Rag	poi	
5	429575262.41247						140	Prov	3934	9
6	429716264.971918						140	Prov	3934	9
7	429716349.770499						140	Arip	3934	9
В	429716405.619276						140	Giu	lta 3934	9
9	432568980.222825	432568980					141	Hi t	nbe 4479	97
10	432569000.474907	432569000					141	Pas	4479	97
11	433081774		44797	1			141	447	net 3936	66
12	433081774		44797	1			141	DFI	3936	66
13	433082195		44797	1	An		141	Hi (
14	433081856		44797		Ga	ce	141	Just	gro	
15	433082599		44797		Ga	ce	141	Hi /		
16	433350110.17942	433350110					141	Hi ç	4479	97
17	433350148		44797		Ga	ce	141	Hey		
18	433351717.501071	433351717					141	Can	4479	97
19	433352062.324283	433352062					141	Btw	unc 4479	97
20	433444570		39349		silv	etti	141	Cia		



WHATSAPP: WHAT ABOUT DELETED DATA?

- As also recently mentioned by J. Zdziarski on his blog [1], an interesting "feature" of WhatsApp is that deleted chats are not actually deleted form the database.
- This because when a SQLite record is being deleted, for performance reasons it is not actually wiped/purged from the database immediately, but marked as free and eventually overwritten later on when that storage space is needed.
- With tools like SQLite-parser [2][3], you can quickly carve out deleted record from WhatsApp chat database.
- However, you will find this "feature" in most applications using SQLite storage databases, not just WhatsApp... keep that in mind.

[1] – "WhatsApp Forensic Artifacts: Chats Aren't Being Deleted", http://www.zdziarski.com/blog/?p=6143

[2] – "Python Parser to Recover Deleted SQLite Database Data", http://az4n6.blogspot.ch/2013/11/python-parser-to-recover-deleted-sqlite.html

[3] – "SQLite-parser", https://github.com/mdegrazia/SQLite-Deleted-Records-Parser



TELEGRAM

- Like WhatsApp, also Telegram stores many of its data in the Shared directory.
- The tgdata.db database, under the Documents folder, contains all information about contacts, conversations, exchanged files, etc.:
 - messages_v29 contains the list of all messages exchanged
 - convesations_v29 contains the list of active conversations as showed in the "Chats" screen of the app
 - encrypted cids v29 contains the conversation ids of the secret chats.





- As expected, also with Telegram is possible to carve out deleted records from SQLite database... but there is one more "feature".
- Telegram messages from secret chats are stored in clear in the messages v29 table, like all the other messages.
- On the other hand we will not find the screen snapshot, as apparently Telegram properly clears the screen when the fade-out event happens.



SIGNAL

- Less popular than the previous two, but still important to know.
- It delivers what promises: its database /Document/Signal.sqlite, containing all its data, is fully encrypted. However, two things that are in clear:
 - The attachments exchanged are stored in clear in the /Document/Attachments/ folder.
 - Screen Snapshots can be retrieved as well. Signal has an option "Enable Screen Security" that would prevent this, but for some reason is not set by default.



ios messaging recap

	WhatsApp	Telegram	Signal
Standard message content in clear?			
"Secret chat" message content in clear?	n/a		
Sender/recipient information?			
Timestamps?			
SQLite carving of deleted records?			
Snapshot?			



TRACKING DEVICE USAGE THROUGH APPLICATION ANALYSIS

- Sarah Edwards has made an extensive research work on artifacts that track the usage of the device.
- By linking applications, data and network usage, health information (e.g. workouts), timestamps and geolocation data, it is indeed possible to understand what a given user under investigation was doing and where, at a given point in time.



TRACKING DEVICE USAGE THROUGH APPLICATION ANALYSIS

- CoreDuct: /private/var/mobile/Library/CoreDuct/
 - coreductd.db (31 tables)
 - coreductdClassA.db (31 tables)
 - coreductdClassD.db (31 tables)
 - Knowledge/knowledgeC.db (5 tables)
 - People/interactionC.db (9 tables)
- Battery Life (PowerLog): /private/var/mobile/Library/ BatteryLife/
 - CurrentPowerlog.PLSQL (257 tables)
 - Archives/powerlog_YYYY-MM-DD_XXXXXXX.PLQSQL.gz (Previous ~5 Days)
- Health:/private/var/mobile/Library/Health/
 - healthdb.sqlite (II tables)
 - healthdb_secure.sqlite (16 tables)

- Aggregate Dictionary: /private/var/mobile/Library/ AggregateDictionary/
 - ADDataStore.sqlitedb (4 tables)
- networkd:/private/var/networkd/
 - netusage.sqlite (13 tables)
- routined:/private/var/mobile/Library/Caches/
 com.apple.routined/
 - cache_encryptedB.db (5 tables)
 - StateModelLarchive
 - StateModel2.archive
- locationd: /private/var/root/Library/Caches/ locationd/
 - cache_encryptedA.db (79 tables)
 - IockCache_encryptedA.db (51 tables)
 - cache_encryptedB.db (167 tables)
 - cache_encryptedC.db (9 tables)



iOS MALWARE

August 25, 2016

Sophisticated, persistent mobile attack against high-value targets on iOS

By Lookout and Citizen Lab 7 Comments

Persistent, enterprise-class spyware is an underestimated problem on mobile devices. However, targeted attack scenarios against high-value mobile users are a real threat.

Citizen Lab (Munk School of Global Affairs, University of Toronto) and Lookout have uncovered an active threat using three critical



https://blog.lookout.com/blog/2016/08/25/trident-pegasus/



iOS MEMORY ANALYSIS... WHAT'S THAT?

- Memory analysis in the mobile domain not much developed, particularly in iOS
- Although rarely usable, may be of help in case of a running malware
- Current tools available consists in utilities/PoC
- Frida is a dynamic instrumentation framework that allows to inject scripts into processes to execute custom debugging logic.
- Fridump is a memory dumping tool built on top of Frida

\$ frida-ps -U
PID Name
1744 Cydia
137 Mail
1738 Settings
1808 Skype
78 BTServer
1792 CacheDeleteAppCo ...



iOS MEMORY ANALYSIS... WHAT'S THAT?

\$ python fridump.py -u -s --max-size 1048576 Skype





LEARNING IOS FORENSICS SECOND EDITION

https://www.packtpub.com/networking-and-servers/ learning-ios-forensics-second-edition

Mattia Epifani, Pasquale Stirparo

Learning iOS Forensics

Second Edition

A practical guide to analyzing iOS devices with the latest forensics tools and techniques









Q&A?

Mattia Epifani

- **Digital Forensics Analyst**
- CEO @ REALITY NET System Solutions Genoa, Italy
- GCFA, GMOB, GNFA, GREM, GCWN



- Threat Intelligence Analyst and Incident Responder @ UBS
- Incident Handler @ SANS ISC, Advisor @ Europol EC3
- GCFA, GREM, OPST, OWSE, ECCE





@mattiaep



http://www.linkedin.com/in/mattiaepifani



- http://blog.digital-forensics.it



@pstirparo IB



https://isc.sans.edu