DFIR Review

How was an iPhone set up?

Heather Mahalik

Published on: Mar 31, 2019

DOI: 10.21428/103135b6

License: [Creative Commons Attribution 4.0 International License \(CC-BY 4.0\)](https://creativecommons.org/licenses/by/4.0/)

Synopsis

Forensic question: Was an iPhone restored from iCloud, iTunes backup or started from scratch?

OS Version: iOS 12.1.x

File: com.apple.purplebuddy.plist

Tools: iTunes, iBackupBot, plist viewer

Introduction

I've realized just how important it is to blog vs just do a webcast when I was completing my course updates. I would stumble upon a webcast, but didn't have time to watch it, so I looked in another direction. This made me realize that I should write down everything I put into a webcast. Will a webcast hold up in course? Do you have time to watch all of them? Seriously, I am curious about the impact so please let me know.

In 2019 - I am going to write down what I talk about in webcasts. If I have the time, I may try to blog about my speaking events as well (think Keynotes and SANS @Nights). Some blogs may be short and sweet, but this way when someone says, "how can I do X" I will point them to my blog.

To kick this one off, I am going to simply discuss a file that stores information on how an iOS device was setup. This is a file that I am asked about a few times a week. In

many cases, it matters if the user synced from iCloud, started from scratch or restored from iTunes. So here goes!

Method

First, you should be obtaining an encrypted backup at a minimum. If you have the ability to get a full file system dump, even better. Without encryption, I cannot guarantee that all of the files I plan to discuss in upcoming blogs will exist. Make sure your analytical tool of choice will decrypt the data. If you are trying to do this for free follow the steps below.

Creating and parsing an encrypted iOS backup for FREE:

1. Launch iTunes on your forensic workstation. Update if necessary.
2. Make sure you **Trust** the computer on the iPhone.
3. Create an encrypted backup with a password you will remember (yep, people forget all of the time!)
4. If you aren't using a commercial tool or one that supports decrypting the backup, you may have to get crafty. I stumbled upon AnyTrans during my updates and it's pretty sweet. To use this, you must know the password or crack it (refer to other blog posts in my archives.)
5. Launch AnyTrans and it will show you if you have locked backups, as shown here:

AnyTrans showing locked iTunes backup

6. Select the locked backup (you know it's locked because the option is to "unlock" it).
7. Enter the password and the backup will be unlocked! The top portion shown below is how the backup directory will look. The original backup remains and the unlocked version is called **BackupUnlock**. If you peek inside that directory, you will find the backup with the date it was unlocked.

Contents of BackupUnlock directory showing date of unlock

8. From here, you can load the unlocked backup into iBackupBot or your tool(s) of choice (iExplorer, etc.). Note: Some commercial tools HATE this format and will not support it. The free ones seem happy enough!

Now let's get to that file you care about. Once your backup or image is loaded into your tool, you need to locate the following file:

/Library/Preferences/com.apple.purplebuddy.plist. I normally just search for **purplebuddy**.

This plist stores the **SetupState** of the device which will tell you how the device was setup by the user.

If the user selected to restore a backup from iCloud, the com.apple.purplebuddy.plist will have a SetupState value set to RestoredFromiCloudBackup as shown here:

XML View List View		
Key	Type	Value
Root	dict	
PrivacyPresented	boolean	true
AppleDPB9Presented	boolean	true
SetupLastExit	date	2018-09-21 13:47:31
AppleDPB4Presented	boolean	true
AppleDPPresented	boolean	true
ControlCenterOnBoardingPresented	boolean	true
acceptedSLAVersion	integer	530001
KeychainSync3Presented	boolean	true
PrivacyContentVersion	integer	2
PBDiagnosticsPresented	boolean	true
PBDiagnostics4Presented	boolean	true
HSA2UpgradeMiniBuddyRan	boolean	true
GuessedCountry	dict	
countries	array	
	string	US
at	date	2018-09-18 09:57:49
Passcode2Presented	boolean	true
AssistantPHSOffered	boolean	true
AppleDPB5Presented	boolean	true
SetupState	string	RestoredFromiCloudBackup
ControlCenterOnBoardingPresented	boolean	true
AppleDPB10Presented	boolean	true
KeychainSyncPresented	boolean	true

If the user setup the iPhone using iTunes, the com.apple.purplebuddy.plist will have a SetupState value set to SetupUsingAssistant as shown here:

XML View List View		
Key	Type	Value
Root	dict	
PBDiagnosticsPresented	boolean	true
AppleIDPB9Presented	boolean	true
LockdownSetLanguage	boolean	true
Locale	string	en_US
WebKitMinimumZoomFontSize	real	0.000000
AppleIDPB10Presented	boolean	true
SetupDone	boolean	true
Language	string	en
WebKitShrinksStandaloneImage	boolean	true
MesaPresented	boolean	true
setupMigratorVersion	integer	9
SetupState	string	SetupUsingAssistant
AppleIDPB7Presented	boolean	true
WebKitLocalStorageDatabasePath	string	/var/mobile/Library/Caches
PBTCPresented	boolean	true
AssistantPresented	boolean	true
PBAppActivity2Presented	boolean	true
PrivacyContentVersion	integer	2
Passcode4Presented	boolean	true
PrivacyPresented	boolean	true
MagnifyPresented	boolean	true
Mesa2Presented	boolean	true
PaymentMiniBuddy4Ran	boolean	true
PBDiagnostics4Presented	boolean	true
HSA2UpgradeMiniBuddy3Ran	boolean	true
lastPrepareLaunchSentinel	array	
SetupFinishedAllSteps	boolean	true
LockdownSetLocale	boolean	true
PaymentPresented	boolean	true
GuessedCountry	dict	

It is worth noting that I am testing on an iOS 12.1.x device and I restored from iTunes in 2 ways to obtain these results. First, I wiped and set up via iTunes and then I also forced a restore of a backup via iTunes. I wanted to be sure the SetupState didn't change. If you find that the user restored from iCloud, consider pulling cloud data if you are legally capable of extracting that form of evidence. Should you find the user restored from iTunes, you now have to find that host computer to do analysis on other potential backups. This is where the fun begins!

Bottom line, Apple has a ton of plists that are relevant. You need to hunt for them. Do a keyword search, dump your device (yep, use the free way I described above) and VALIDATE!!!

Technical Challenges

CAUTION: iBACKUPBOT and iOS10+ potential issues.

Below I am attempted to do the same thing with iBackupBot, but I ran into iOS version issues.

1. Launch iBackupBot
2. Make sure you **Trust** the computer on the iPhone.
3. Create an encrypted backup. Notice that the tool is telling you that Backup encryption is turned on? This is good.

4. Select where to save the backup image. I recommend into your case directory for the investigation.

5. The backup will be created and then you can open it in iBackupBot for analysis. Once the backup is complete, it will prompt you to open it. If you have issues, this is an iOS10 error from what I have seen. ./ At this point, revert to iTunes. *NOTE: The error I have seen in iOS 10, 11 and 12 is that the file cannot be opened in iBackupBot. It seems to have lost the ability to decrypt or prompt for decryption.*

Link to original blog post:

<https://smarterforensics.com/2019/01/how-was-an-iphone-setup/>

Link to webcast:

<https://www.youtube.com/watch?v=AC2TpWsLPLQ>

DFIR Review

The purpose of the article is to provide an open-source method of analyzing a file to determine whether an iOS device was restored from an iCloud backup, iTunes backup, or setup from scratch. This is information not provided through default settings in forensic analysis tools that many would consider to be court approved. This information may be of interest in some investigations, where a device change occurred in the critical time period. Data carried over from an older device using a cloud backup may be less probative than data created on the device at hand.

The author provides a methodology to get a backup of an iPhone without commercial tools, with troubleshooting assistance using iBackupBot. In some cases it can be expedient to use such free tools, but it is important to note that they were not created for forensic purposes and might alter data on the analysed device under certain conditions. Therefore, it is not recommended to use this approach in casework, even though the obtained data will very likely be identical to what might be obtained with a file system extraction using any standard forensic suite.

There appears to be a iPhoneWiki article from 2017 (<https://www.theiphonewiki.com/wiki//private/var/mobile/Library/Preferences/com.apple.purplebuddy.plist>) that lists this Plist file contains the setup.app location; however, it does not specify the information provided in the above article.

Future Work

Further exploration into what different iPhone setup states are possible, or whether it is possible to obtain similar or identical results under different circumstances or with different devices. For example, An additional question that could be studied is the SetupState when an iPhone was only setup, with no restore. It might be also interesting to see whether it is possible to provoke an incorrect state by interrupting the setup process and switching to another.

Reviewers

- Anthony Knutson (Methodology Review)
- Francesco Servida (Methodology Review)
- Hannes Spichiger (Methodology Review)
- Timothy Bollé (Methodology Review)
- Addisu Afework Birhanu (Methodology Review)