DFIR Review

iOS Mobile Installation Logs

Alexis Brignoni

Published on: Apr 03, 2019

DOI: 10.21428/9106d7d3

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

Synopsis

<p>Forensic question: What applications were installed on an iOS device?</p> <p>OS Version: iOS 11, iOS 12</p> <p>File: /private/var/install/Library/Logs/MobileInstallation/*.log</p> <p>Tools: Python</p>
---	---	--	---

Introduction

In the last two blog posts I wrote about ways of obtaining a list of currently installed apps and their corresponding app directories from an iOS file system extraction. My usual method is to query the contents of the applicationState.db file to find the app bundle id and what directory GUID like name corresponds to it. By finding the proper directory one can focus on the data stores it contains for parsing of user generated data when our forensic tools are not aware of them.

On my second post I received great feedback from [Sarah Edwards](#). She pointed me to the contents of the mobile installation logs in iOS.

Cool stuff!

I immediately wondered if there was a script that could parse those logs for the data I was looking for. After asking [Sarah Edwards](#) and looking online I didn't find any.

I'll do it.

Method

The link below is for a python script I made that parses the mobile installation logs. It has been tested on iOS 11 and iOS 12.

<https://github.com/abrignoni/iOS-Mobile-Installation-Logs-Parser>

- [iOS Mobile Installation Logs Parser](#)

These logs contain a lot of information. Currently the script only extracts the following events:

- App install successful with date and time.

- App container made live with date, time, and path.
- App container moved with date, time, and path.
- App destroying container with date, time, and path.

Here is a sample screen of how the logs look as taken from the device. The image has been zoomed out which could make it harder to read unless the preview image is clicked.

```
Wed Jan 10 10:38:40 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.mobilegarageband at /private/var/mobile/Containers/Data/Application/48B7D...
Wed Jan 10 10:38:40 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.mobilegarageband at /private/var/mobile/Containers/Data/Application/7147E896-E...
Wed Jan 10 10:38:40 2018 [47] <notice> (0x16f407000) -[MInstaller performInstallationWithError:]: Install Successful for (com.apple.mobilegarageband); Staging: 2.45s; Waiting: 0.00s; Preflight/Patch: 0.46s; Verifying: 25.32s; Ove...
Wed Jan 10 10:39:43 2018 [47] <notice> (0x16f407000) -[MClientConnection doInstallationForURLwithOptions:completion:]: Install of "/var/mobile/Media/PublicStaging/AA44806a-3d45-4368-9304-F9073254016*" type Customer (LSInstall...
Wed Jan 10 10:40:14 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.Keynote at /private/var/mobile/Containers/Data/Application/C91F5743-FAB7-...
Wed Jan 10 10:40:14 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.Keynote at /private/var/mobile/Containers/Data/PlugInKit/Plug...
Wed Jan 10 10:40:14 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.Keynote at /private/var/mobile/Containers/Data/PlugInKit/Plug...
Wed Jan 10 10:40:14 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.Keynote at /private/var/mobile/Containers/Data/PlugInKit/Plug...
Wed Jan 10 10:41:05 2018 [47] <notice> (0x16f407000) -[MClientConnection doInstallationForURLwithOptions:completion:]: Install of "/var/mobile/Media/PublicStaging/7D44E08b-FD64-4578-B3D6-1D246D851A5*" type Customer (LSInstall...
Wed Jan 10 10:41:09 2018 [47] <notice> (0x16f407000) -[MInstaller performInstallationWithError:]: Installing <MInstallableBundle ID=com.apple.Numbers; Version=5052, ShortVersion=3.3>
Wed Jan 10 10:41:46 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.Numbers at /private/var/mobile/Containers/Data/Application/E4E80030-7B0B-...
Wed Jan 10 10:41:46 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.Numbers at /private/var/mobile/Containers/Data/PlugInKit/Plug...
Wed Jan 10 10:41:46 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.Numbers at /private/var/mobile/Containers/Data/PlugInKit/Plug...
Wed Jan 10 10:41:47 2018 [47] <notice> (0x16f407000) -[MInstaller performInstallationWithError:]: Install Successful for (com.apple.Numbers); Staging: 3.89s; Waiting: 0.00s; Preflight/Patch: 0.57s; Verifying: 36.64s; Overall: 41...
Wed Jan 10 10:42:35 2018 [47] <notice> (0x16f407000) -[MClientConnection doInstallationForURLwithOptions:completion:]: Install of "/var/mobile/Media/PublicStaging/18D1E46a-4100-4E7C-8DCE-100C10B73F5*" type Customer (LSInstall...
Wed Jan 10 10:42:40 2018 [47] <notice> (0x16f407000) -[MInstaller performInstallationWithError:]: Installing <MInstallableBundle ID=com.apple.Pages; Version=5052, ShortVersion=3.3>
Wed Jan 10 10:43:17 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.Pages at /private/var/mobile/Containers/Data/Application/697810B0-8AF2-42...
Wed Jan 10 10:43:17 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.Pages at /private/var/mobile/Containers/Data/PlugInKit/Plug...
Wed Jan 10 10:43:17 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.Pages at /private/var/mobile/Containers/Data/PlugInKit/Plug...
Wed Jan 10 10:43:17 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.Pages at /private/var/mobile/Containers/Data/PlugInKit/Plug...
Wed Jan 10 10:43:18 2018 [47] <notice> (0x16f407000) -[MInstaller performInstallationWithError:]: Install Successful for (com.apple.Pages); Staging: 4.68s; Waiting: 0.00s; Preflight/Patch: 1.06s; Verifying: 35.81s; Overall: 42.48...
Wed Jan 10 10:44:08 2018 [47] <notice> (0x16f407000) -[MClientConnection doInstallationForURLwithOptions:completion:]: Install of "/var/mobile/Media/PublicStaging/27E49405-ACE0-4E2A-954E-00719E0142B4*" type Customer (LSInstall...
Wed Jan 10 10:44:10 2018 [47] <notice> (0x16f407000) -[MInstaller performInstallationWithError:]: Installing <MInstallableBundle ID=com.apple.iMovie; Version=3709.9.72, ShortVersion=234>
Wed Jan 10 10:44:28 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.iMovie at /private/var/mobile/Containers/Data/Application/C62469FC-9E5C-4...
Wed Jan 10 10:44:28 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.iMovie at /private/var/mobile/Containers/Data/PlugInKit/Plug...
Wed Jan 10 10:44:28 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.iMovie at /private/var/mobile/Containers/Data/PlugInKit/Plug...
Wed Jan 10 10:44:28 2018 [47] <notice> (0x16f407000) -[MInstaller performInstallationWithError:]: Install Successful for (com.apple.iMovie); Staging: 1.57s; Waiting: 0.00s; Preflight/Patch: 0.16s; Verifying: 17.95s; Overall: 20.0...
Wed Jan 10 10:44:33 2018 [47] <notice> (0x16f407000) -[MClientConnection doInstallationForURLwithOptions:completion:]: Install of "/var/mobile/Media/PublicStaging/5B4350F5-C5CB-453E-9A00-EP410CCCE946C*" type Customer (LSInstall...
Wed Jan 10 10:44:33 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.iTunesU at /private/var/mobile/Containers/Data/Application/84ECC0C8-A234-...
Wed Jan 10 10:44:35 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.iTunesU at /private/var/mobile/Containers/Data/PlugInKit/Plug...
Wed Jan 10 10:44:35 2018 [47] <notice> (0x16f407000) -[MContainer makeContainerLiveReplacingContainer:reason:withError:]: Made container live for com.apple.iTunesU at /private/var/mobile/Containers/Data/PlugInKit/Plug...
Wed Jan 10 10:44:35 2018 [47] <notice> (0x16f407000) -[MInstaller performInstallationWithError:]: Install Successful for (com.apple.iTunesU); Staging: 0.21s; Waiting: 0.00s; Preflight/Patch: 0.03s; Verifying: 1.80s; Overall: 2.19...
Wed Jan 10 16:31:04 2018 [47] <notice> (0x1b37b7b00) main: Reboot detected
Wed Jan 10 16:31:04 2018 [47] <notice> (0x1b37b7b00) -[DeveloperDiskImageTracker checkMountPoint:]: block_invoke: /Developer/Applications is not present now or before
Wed Jan 10 16:31:04 2018 [47] <notice> (0x1b37b7b00) -[DeveloperDiskImageTracker checkMountPoint:]: block_invoke: /private/var/personalized_factory/PROlly/Applications disappeared: unregistering apps
```

Lots of data.

The script is really simple to use.

1. Have Python 3.6.4 or newer installed.
2. Extract the logs from the **/private/var/installd/Library/Logs/MobileInstallation/** directory.
3. Place the script in the same directory as the extracted logs.
4. Execute the script via CMD.

The screen, after done, should look something like this:

```
iOS Mobile Installation Logs Parser
By: @AlexisBrignoni
Web: abrignoni.com

Logs processed: 2
Lines processed: 1486

Total apps: 68
Total installed apps: 53
Total uninstalled apps: 15
Total historical app reports: 68
```

Run complete. Some stats.

The script will produce one SQLite database called `mib.db`, a directory named `Apps_State`, and a directory named `Apps_Historical`.

Script with generated items.

The SQLite database holds the extracted information from the lines of log data. The script queries the database to produce the contents within the two directories.

The `Apps_State` directory can have two files within it. These are named `InstalledApps.txt` and `UninstalledApps.txt`. The contents reflect the name of the text files. Here is a sample image of `InstalledApps.txt` content:

```
com.microsoft.Office.Outlook.compose-shareextension
com.microsoft.Office.Outlook.NotificationContentExtension
com.microsoft.Office.Outlook.agenda-widgetextension
com.microsoft.Office.Outlook.NotificationServiceExtension
com.nike.nikeplus-gps
com.yahoo.Aerogram
com.hammerandchisel.discord
com.hammerandchisel.discord.Share
com.yahoo.Aerogram.NotificationContentExtension
com.yahoo.Aerogram.CallDirectoryExtension
com.yahoo.Aerogram.NotificationServiceExtension
com.yahoo.Aerogram.ShareExtension
com.blizzard.social
com.nike.nikeplus-gps.messagesextension
com.nike.nikeplus-gps.intentsexextension
com.apple.mobilegarageband
com.apple.Keynote
com.apple.Keynote.KeynoteDAVFP
com.apple.Keynote.KeynoteDAVFPUI
com.apple.Numbers
com.apple.Numbers.NumbersDAVFP
com.apple.Numbers.NumbersDAVFPUI
com.apple.Pages
```

List of installed apps.

Having this list handy is really useful since it can be used to compare the currently installed apps within the file system image that might have been missed by our third-party forensic tool of choice.

If one would like more context in regards to when the app was installed and where the app directory is located the Apps_Historical directory has all that information per app.

> Apps_Historical

Name	Date modified	Type	Size
com.apple.clips.txt	11/4/2018 2:44 PM	Text Document	1 KB
com.apple.iMovie.pipe.txt	11/4/2018 2:44 PM	Text Document	1 KB
com.apple.iMovie.txt	11/4/2018 2:44 PM	Text Document	1 KB
com.apple.itunesu.SpotlightIndexExtension.txt	11/4/2018 2:44 PM	Text Document	1 KB
com.apple.itunesu.txt	11/4/2018 2:44 PM	Text Document	2 KB
com.apple.Keynote.KeynoteDAVFP.txt	11/4/2018 2:44 PM	Text Document	1 KB
com.apple.Keynote.KeynoteDAVFPUL.txt	11/4/2018 2:44 PM	Text Document	1 KB
com.apple.Keynote.txt	11/4/2018 2:44 PM	Text Document	2 KB
com.apple.mobilegarageband.txt	11/4/2018 2:44 PM	Text Document	1 KB
com.apple.Numbers.NumbersDAVFP.txt	11/4/2018 2:44 PM	Text Document	1 KB
com.apple.Numbers.NumbersDAVFPUL.txt	11/4/2018 2:44 PM	Text Document	1 KB
com.apple.Numbers.txt	11/4/2018 2:44 PM	Text Document	2 KB
com.apple.Pages.PagesDAVFP.txt	11/4/2018 2:44 PM	Text Document	1 KB
com.apple.Pages.PagesDAVFPUL.txt	11/4/2018 2:44 PM	Text Document	1 KB
com.apple.Pages.txt	11/4/2018 2:44 PM	Text Document	2 KB
com.blizzard.social.txt	11/4/2018 2:44 PM	Text Document	2 KB

A txt file for every app.

Here is a sample of the historical information regarding an installed app.

```

2018-12-28 22:17:30 Data container moved com.blizzard.social /private/var/mobile/Containers/Data/Application/6068CC22-AF64-4C54-A2DE-F0EC25E10F35
2018-12-28 22:17:30 Made container live com.blizzard.social /private/var/containers/Bundle/Application/9BF0BB3B-C388-4985-8C7F-999A8CA7AC02
2018-12-28 22:17:30 Install successful com.blizzard.social
2018-12-28 22:17:18 Install successful com.blizzard.social
2018-11-18 12:33:25 Data container moved com.blizzard.social /private/var/mobile/Containers/Data/Application/E72C50EE-130C-438A-999B-AD3AD91E3F6F
2018-11-18 12:33:25 Made container live com.blizzard.social /private/var/containers/Bundle/Application/3E08D432-9EFD-45F6-A820-7014AC509322
2018-11-18 12:33:25 Install successful com.blizzard.social
2018-11-18 12:33:18 Made container live com.blizzard.social /private/var/mobile/Containers/Data/Application/D62F9AC0-3D02-4A4A-BA9B-28EBF6657110
2018-11-18 12:33:18 Made container live com.blizzard.social /private/var/containers/Bundle/Application/01304B46-8E6F-46B3-B934-068A32FB35CC
2018-11-18 12:33:18 Install successful com.blizzard.social

```

Historical events for com.blizzard.social

Notice the report has a timestamp for every event. The script puts the most recent events at the top so the current path for the application directory can be at or near the top.

Here is a sample of historical information regarding an uninstalled app.

```

2018-11-03 19:28:55 Destroying container org.videolan.vlc-ios /private/var/containers/Bundle/Application/91BE2D20-2540-4513-9165-3433C5DDADC1
2018-11-03 19:28:55 Destroying container org.videolan.vlc-ios /private/var/mobile/Containers/Data/Application/8E05DCEF-9606-4F30-94A6-C3B19B28857A
2018-11-02 21:21:15 Data container moved org.videolan.vlc-ios /private/var/mobile/Containers/Data/Application/8E05DCEF-9606-4F30-94A6-C3B19B28857A
2018-11-02 21:21:15 Made container live org.videolan.vlc-ios /private/var/containers/Bundle/Application/91BE2D20-2540-4513-9165-3433C5DDADC1
2018-11-02 21:21:15 Install successful org.videolan.vlc-ios
2018-11-02 21:21:08 Made container live org.videolan.vlc-ios /private/var/mobile/Containers/Data/Application/19BF7D8A-0FC8-4911-89AA-685FED0942F1
2018-11-02 21:21:08 Made container live org.videolan.vlc-ios /private/var/containers/Bundle/Application/4AEDEC37-B9D2-439D-AA17-E126A603FD53
2018-11-02 21:21:08 Install successful org.videolan.vlc-ios

```

Historical event for org.videolan.vlc-ios

Like the previous report there is a timestamp for every entry and events start with the most recent at the top. These reports are useful if one wants to determine when an app was uninstalled or if a current app was uninstalled and then reinstalled multiple times.

```

File Edit Format View Help
2018-08-04 10:01:33 Made container live org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/3EBAF759-0D14-4C8A-BFE7-6F629F46E2DC
2018-08-04 10:01:33 Made container live org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/B8EAFE3A-BFF9-455D-BA54-061CA1DE5E2C
2018-08-04 10:01:33 Install successful org.coolstar.electra1131
2018-08-04 09:01:34 Made container live org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/3EC83BA2-5426-48ED-B836-CD271C588FD3
2018-08-04 09:01:34 Made container live org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/0D04730F-ACD2-44A5-913F-A2E0A1DCAC76
2018-08-04 09:01:34 Install successful org.coolstar.electra1131
2018-08-04 08:53:13 Destroying container org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/3B0A6A2D-164A-4138-9070-CE6976EF6006
2018-08-04 08:53:13 Destroying container org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/AB2B9B5B-C8B8-4739-A1D6-5588A622830F
2018-08-03 23:51:59 Made container live org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/AB2B9B5B-C8B8-4739-A1D6-5588A622830F
2018-08-03 23:51:59 Made container live org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/3B0A6A2D-164A-4138-9070-CE6976EF6006
2018-08-03 23:51:59 Install successful org.coolstar.electra1131
2018-08-03 23:46:17 Destroying container org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/3B4D5226-D5B6-4087-BA14-FDD516964DAC
2018-08-03 23:46:17 Destroying container org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/DAC79E28-A567-407D-B628-FD2B43655B99
2018-08-03 23:43:01 Made container live org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/DAC79E28-A567-407D-B628-FD2B43655B99
2018-08-03 23:43:01 Made container live org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/3B4D5226-D5B6-4087-BA14-FDD516964DAC
2018-08-03 23:43:01 Install successful org.coolstar.electra1131
2018-08-03 23:32:47 Destroying container org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/CC495F50-5637-477D-A9DB-D03D4178E05D
2018-08-03 23:32:47 Destroying container org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/190EC82F-678B-47F1-BA71-41AB31F0A2ED
2018-08-03 22:14:14 Made container live org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/190EC82F-678B-47F1-BA71-41AB31F0A2ED
2018-08-03 22:14:14 Made container live org.coolstar.electra1131 /private/var/mobile/Containers/Data/Application/CC495F50-5637-477D-A9DB-D03D4178E05D
2018-08-03 22:14:14 Install successful org.coolstar.electra1131

```

Historical events for org.coolstar.electra1131

Notice the multiple 'Destroying', 'Made', and 'Install Successful' entries in the report. Again, the most recent ones are at the top. It also presents when an app was updated. It shows the previous app version number and the most recent version number after update.

As seen above the script's output is responsive to the original requests of installed apps with corresponding app directory paths. It goes further by identifying uninstalled apps and by providing timestamps and historical app event aggregation. Lastly it also keeps track of reboot events with corresponding timestamps.

By looking at the logs there seems to be further areas where the script can be improved. This is my soon to-do list:

- Add 'updated bundle entries' for 'container made live' context in the historical reports.
- Add 'uninstall requested' and 'uninstalling identifier' in the historical reports.

Link to original blog posts:

<https://abrignoni.blogspot.com/2019/01/ios-mobile-installation-logs-parser.html>

<https://abrignoni.blogspot.com/2018/12/update-on-identifying-installed-and.html>

Acknowledgements

I can't thank enough my colleague [@i_am_the_gia](#) for testing out the script on her data sets and [Sarah Edwards](#) for making me aware of the logs.

DFIR Review

This work details how to extract and interpret app installation logs from an iOS file system to determine which applications are currently installed and that were deleted. A comprehensive list of app installation activities, including timestamps, can be very useful in an investigation of a mobile device.

This work provides a Python script and a dataset for testing the script.

Using the test dataset provided by the author, in `mobile_instalation.log.0` there were no results for `System_State` - Validated manually the log and the sql database created and this is correct. The `mobile_installation.log.0` file from my personal test data did have entries. Both are correct parsing of the log. Manually reviewed data from provided `mobile_instalation.log.1` to results in `Apps_Historical`, `Apps_State`, `System_State`, and the created `mib.db` for both test data from author and own test data. Both are correct. This script worked as expected on both the provided test data and data that I created.

Future Work

Installations with errors are not displayed in the database or in any of the text documents, there may be value in including those times in the `Apps_Historical` txt documents for the `bundleID`.

Reviewers

- Addisu Afework Birhanu (Verified using Author Provided Dataset)
- Ali Hadi (Methodology Review)
- Jessica Hyde (Verified using Author Provided Dataset & Verified using Reviewer Generated Dataset)
- Anthony Knutson (Methodology Review)
- Sungmi Park (Methodology Review)