
# Putting a User Behind an iOS Device

By:
Heather Mahalik (Cellebrite)

*From the proceedings of*

The Digital Forensic Research Conference

**DFRWS 2020 USA**

Virtual -- July 20-24

Cellebrite

# PUTTING A USER BEHIND AN IOS DEVICE

Validating how an iOS device was setup and why this may impact your investigation

Heather Mahalik

Cellebrite

# Who I Am

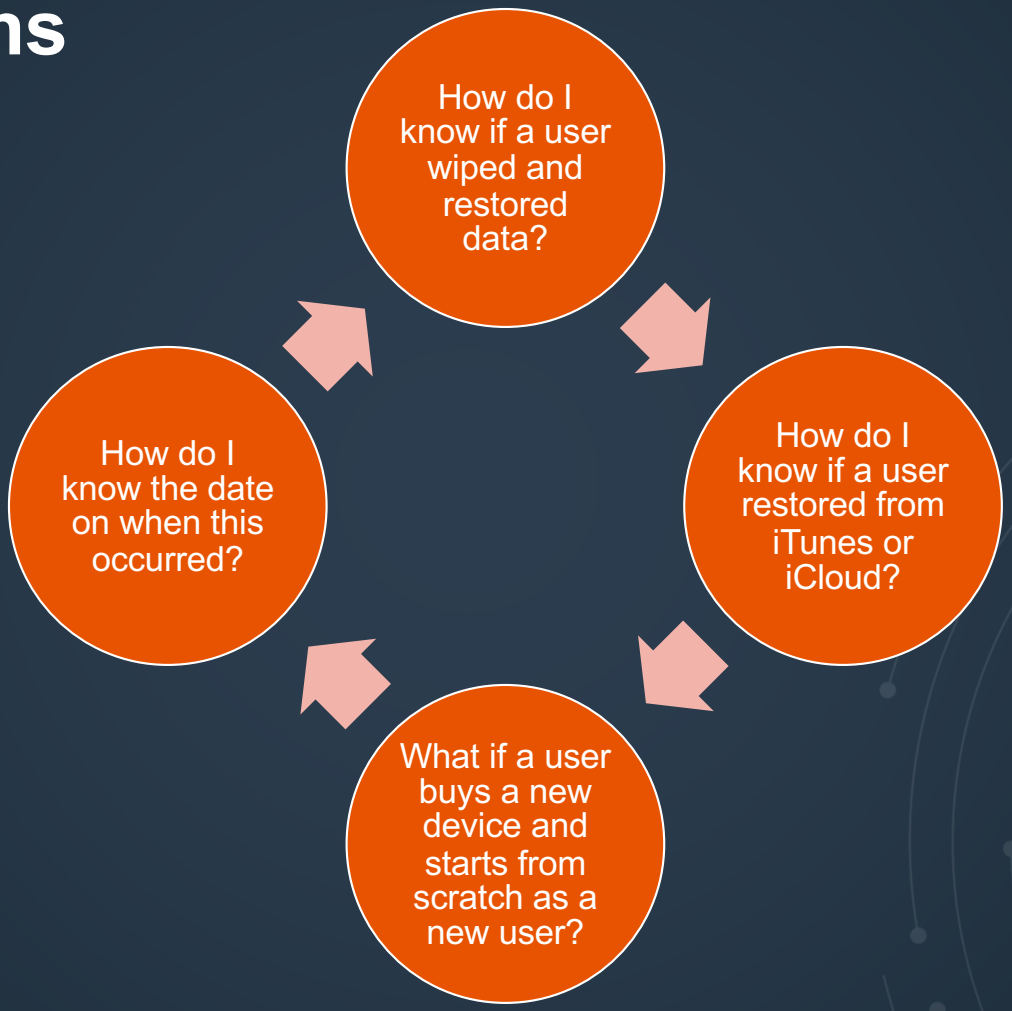
- DFIR Professional for almost 19 years
- Senior Director of Digital Intelligence, Cellebrite
- SANS Senior Instructor and Course Author
- Mobile obsessed
- Serial vacationer, lover of wine and bourbon
- Won the Lottery – I found a career that doesn't feel like work!

# The Back Story



Cellebrite

# The Questions




Cellebrite

# My Methodology

## Gather test devices

- Multiple models
- Different iOS versions

## Create your test plan

- What is the point of the test
- Which tools are you going to use?

## Document *EVERY* step

## Review your results

- Document files of interest here (com.apple.purplebuddy.plist)

## SHARE IT!!!! This is our duty in DFIR

- My vow was to blog about what I do live or in webinar formats

# Share your Findings

XML View | List View

| Key | Type | Value |
|---|---|---|
| Root | dict | |
| PBDiagnosticsPresented | boolean | true |
| AppleIDPB9Presented | boolean | true |
| LockdownSetLanguage | boolean | true |
| Locale | string | en_US |
| WebKitMinimumZoomFontSiz | real | 0.000000 |
| AppleIDPB10Presented | boolean | true |
| SetupDone | boolean | true |
| Language | string | en |
| WebKitShrinksStandaloneImag | boolean | true |
| MesaPresented | boolean | true |
| setupMigratorVersion | integer | 9 |
| SetupState | string | SetupUsingAssistant |
| AppleIDPB7Presented | boolean | true |
| WebKitLocalStorageDatabaseP | string | /var/mobile/Library/Caches |

XML View | List View

| Key | Type | Value |
|---|---|---|
| Root | dict | |
| PrivacyPresented | boolean | true |
| AppleIDPB9Presented | boolean | true |
| SetupLastExit | date | 2018-09-21 13:47:31 |
| AppleIDPB4Presented | boolean | true |
| AppleIDPresented | boolean | true |
| ControlCenterOnBoardingPres | 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 |
| AppleIDPB5Presented | boolean | true |
| SetupState | string | RestoredFromiCloudBackup |

Cellebrite

# Why This Matters

Peer review and validation remove a ton of pressure

What you write may impact a lot of investigations

- Don’t stress about it becoming dated

Take what I did and update the research

- Is this the same for iOS 14 – coming soon!
- What if the person restores from another device and not iTunes or iCloud?
- What if the device is not restored at all on these newer iOS versions?
- Does data_ark.plist match the purplebuddy plist?

*Special thanks to the DFIR Review Panel for their work on my research*

- *Anthony Knutson, Francesco Servide, Hannes Spichiger, Timothy Bolle, Addisu Afework Birhanu and Jessica Hyde (for asking me to submit)*


Cellebrite
Thank you
Email - heather@cellebrite.com
Blog - https://smarterforensics.com/
Twitter - @heathermahalik
The Paper-
https://dfir.pubpub.org/pub/2q177smo/release/5
shortened - https://for585.com/dfrws