Blog | DigForCE Lab

BFU and AFU Lock States

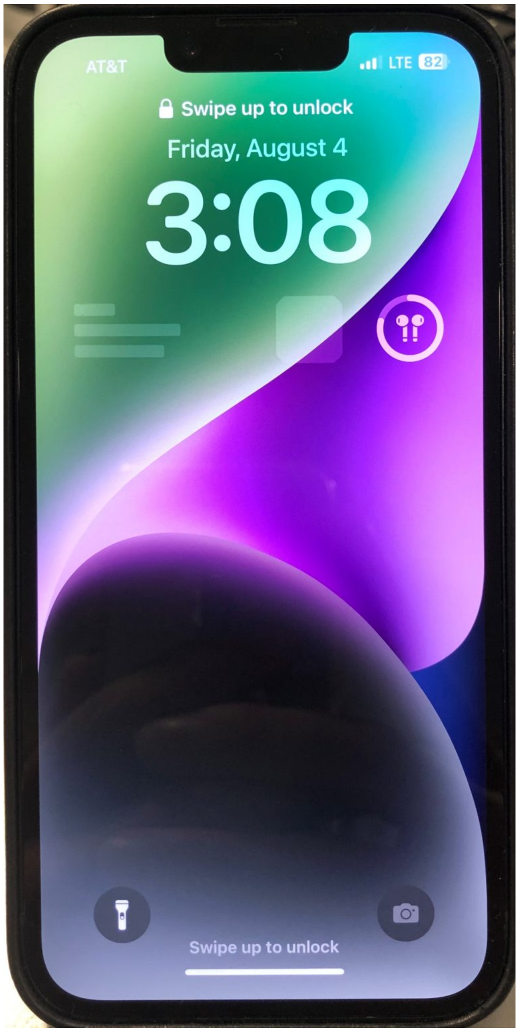
Published **August 23, 2023** by **William Campbell**

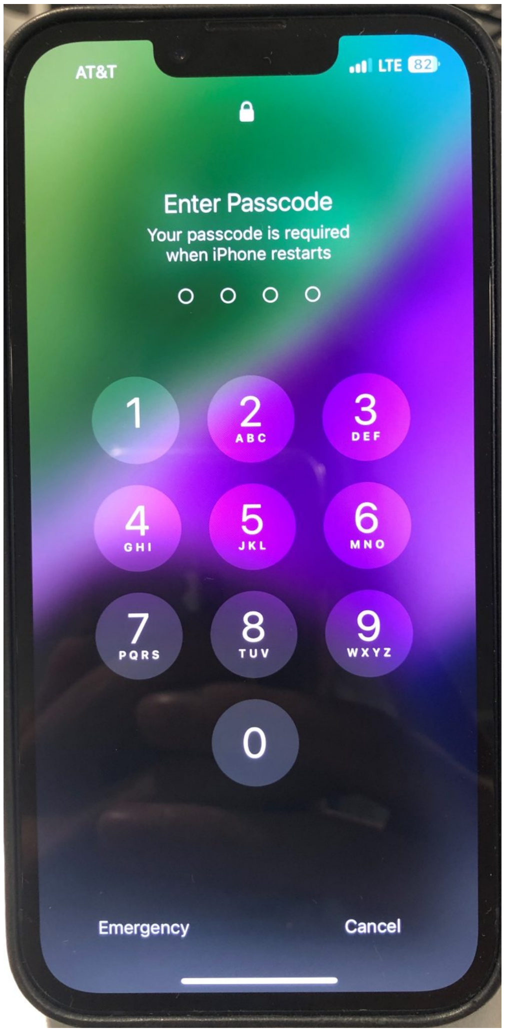
Introduction

When a phone is collected as evidence, it is important to consider various procedures to ensure that the maximum amount of information can be extracted from the device. When it comes to iOS and Android devices, the lock state is one of the most important attributes to consider. Phones can be in what is called a Before First Unlock (BFU) or After First Unlock (AFU) state. Depending on which lock state the device is in, the extraction of the device will only be able to collect certain information. This is because iPhones, as well as newer versions of Android, utilize a form of encryption known as file-based encryption which makes files inaccessible while the device is locked after a reboot.[i]

Before First Unlock

One of the two possible lock states a mobile device is described as being in is known as Before First Unlock, or BFU. The BFU state refers to a phone that has been powered off or reset and has not been signed back into using the screen lock passcode. For iPhones that are in a BFU state, certain features such as the notification center, control center, camera, WiFi, Face ID, Touch ID, screenshots, and lock screen widgets are unavailable to the user until the correct lock screen passcode is entered. Also, upon entering the passcode for the locked iPhone, the message “Your passcode is required when iPhone restarts” will appear.


AT&T
LTE 82
Swipe up to unlock
Friday, August 4
3:08
Swipe up to unlock

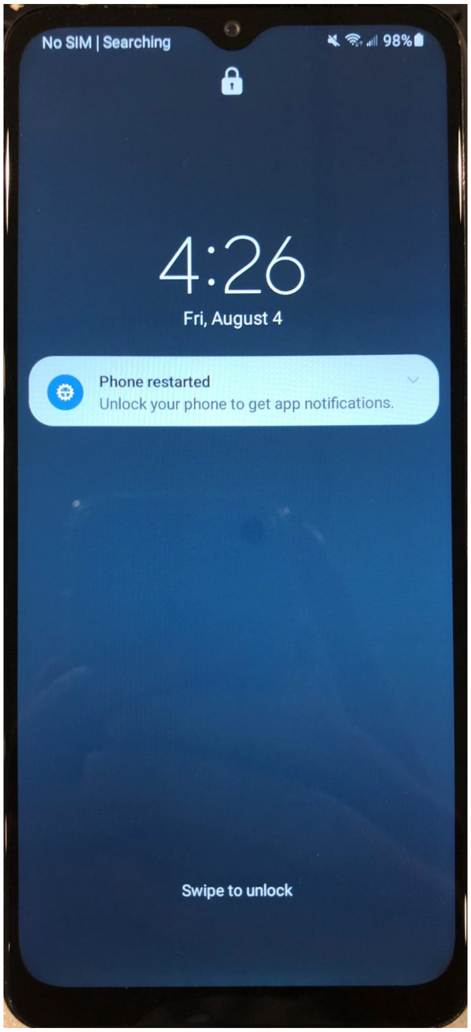


Enter Passcode

Your passcode is required when iPhone restarts

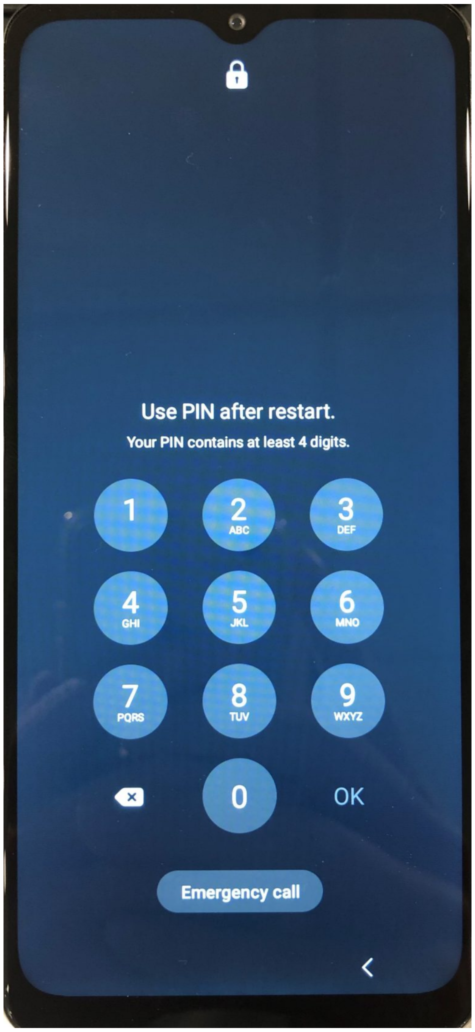
An iPhone 14 that is in the BFU lock state. Notice the camera button, lock screen widgets, and WiFi features are disabled, as well as the unique passcode message.

The experience with Android is similar, as many features within the Quick Settings drop-down menu are locked behind the passcode by default as well as the lock screen phone and camera features. Android devices also may display limited push notifications in this state, along with a custom "Phone restarted" notification that will appear on the lock screen. On the passcode screen, there is a message that says "Use PIN after restart" that is displayed as well.



Phone restarted

Unlock your phone to get app notifications.



Use PIN after restart.

Your PIN contains at least 4 digits.

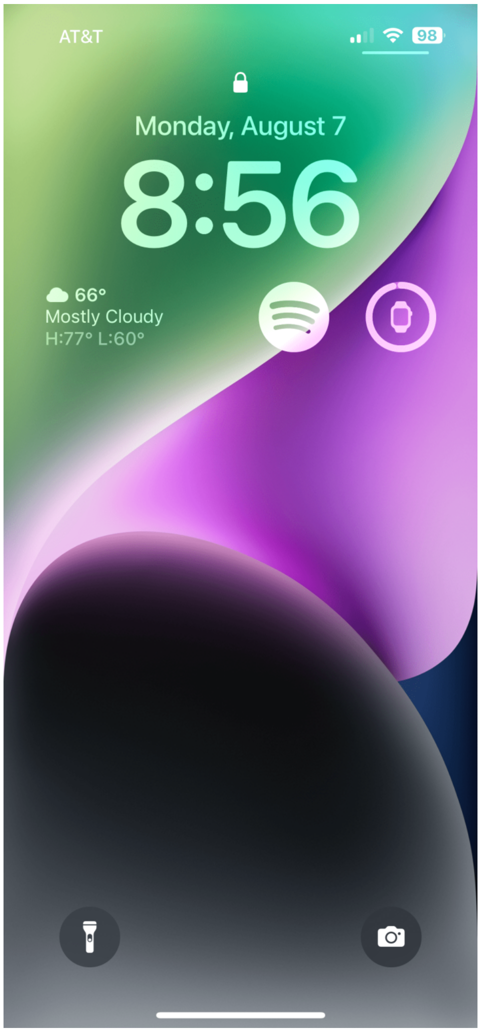
An Android phone (Samsung Galaxy A32 5G) in the BFU lock state. Notice the "Phone restarted" notification, as well as the unique passcode message.

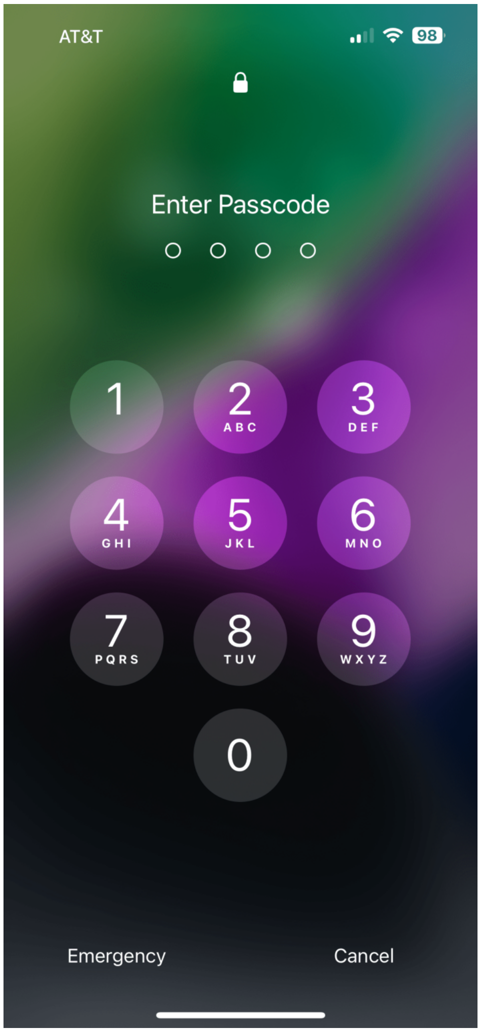
Devices running iOS and Android are able to utilize various forms of file-based encryption. Android 7.0 supports file-based encryption, while it is a required feature for Android 10 and higher.[ii] When these devices are in a BFU state, information located on the device is securely encrypted and inaccessible. Upon entering the correct passcode of a device in the BFU state, an encryption key is generated to unlock the filesystem and the contents contained within it.[i] This changes a device's lock state from BFU to After First Unlock, or AFU.

After First Unlock

Once the user successfully logs onto the phone after the device was powered off, the phone enters the AFU state. A phone that is in the AFU state is that of any phone that has been unlocked at least once since the device has been reset or completely powered off. This is the case for the majority of powered-on phones currently being utilized. A phone that is in the AFU state stays in the state until the device loses power or is rebooted. While a device is in the AFU state, more information can be extracted from the phone, as the filesystem is no longer fully encrypted.

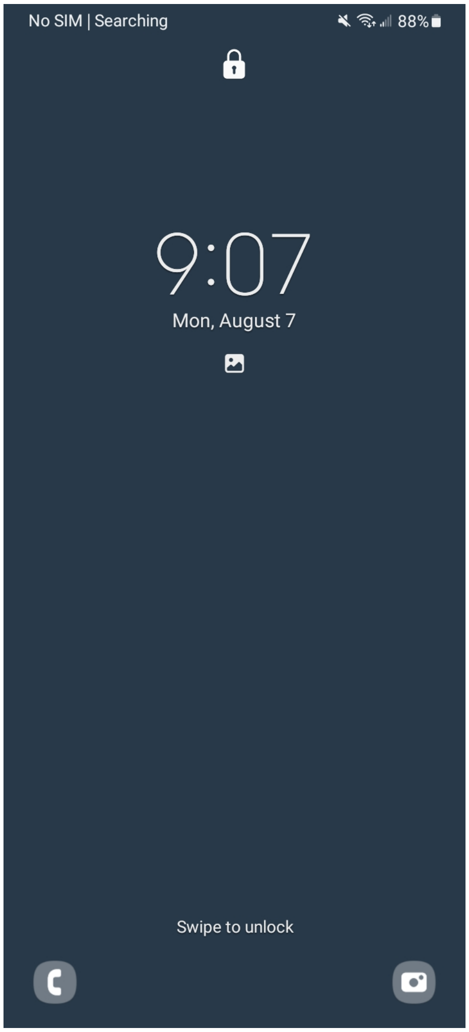
To tell if an iOS or Android device is in the AFU state, one may look for signs that the device is in BFU mode, if any feature normally unavailable during BFU mode is, the phone is likely in an AFU state. For iOS, this includes many of the previously mentioned features working properly, such as notification center, control center, camera, WiFi, Face ID, Touch ID, screenshots, and lock screen widgets.

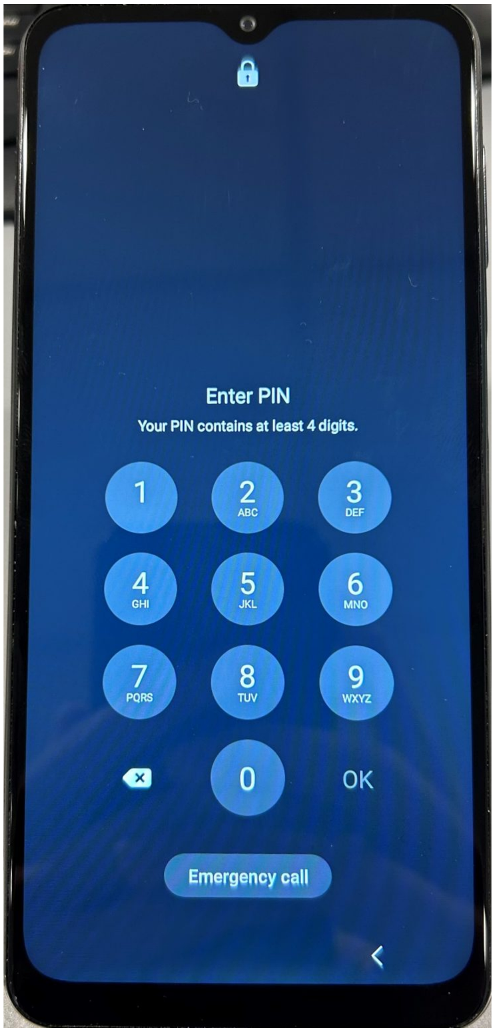




The same iPhone 14 that was shown in BFU section is now in the AFU lock state. Notice the camera, lock screen widgets, and WiFi features are now enabled. The passcode message no longer specifies the device is in BFU mode. A screenshot was able to be taken of both the lock screen and passcode screen.

Android devices that are in the AFU state will have access to all notifications as well, as well as the phone and camera app buttons enabled on the lock screen. The custom BFU passcode messages will not be displayed, and Android devices will not have the "Phone restarted" notification.


No SIM | Searching
88%
9:07
Mon, August 7
Swipe to unlock



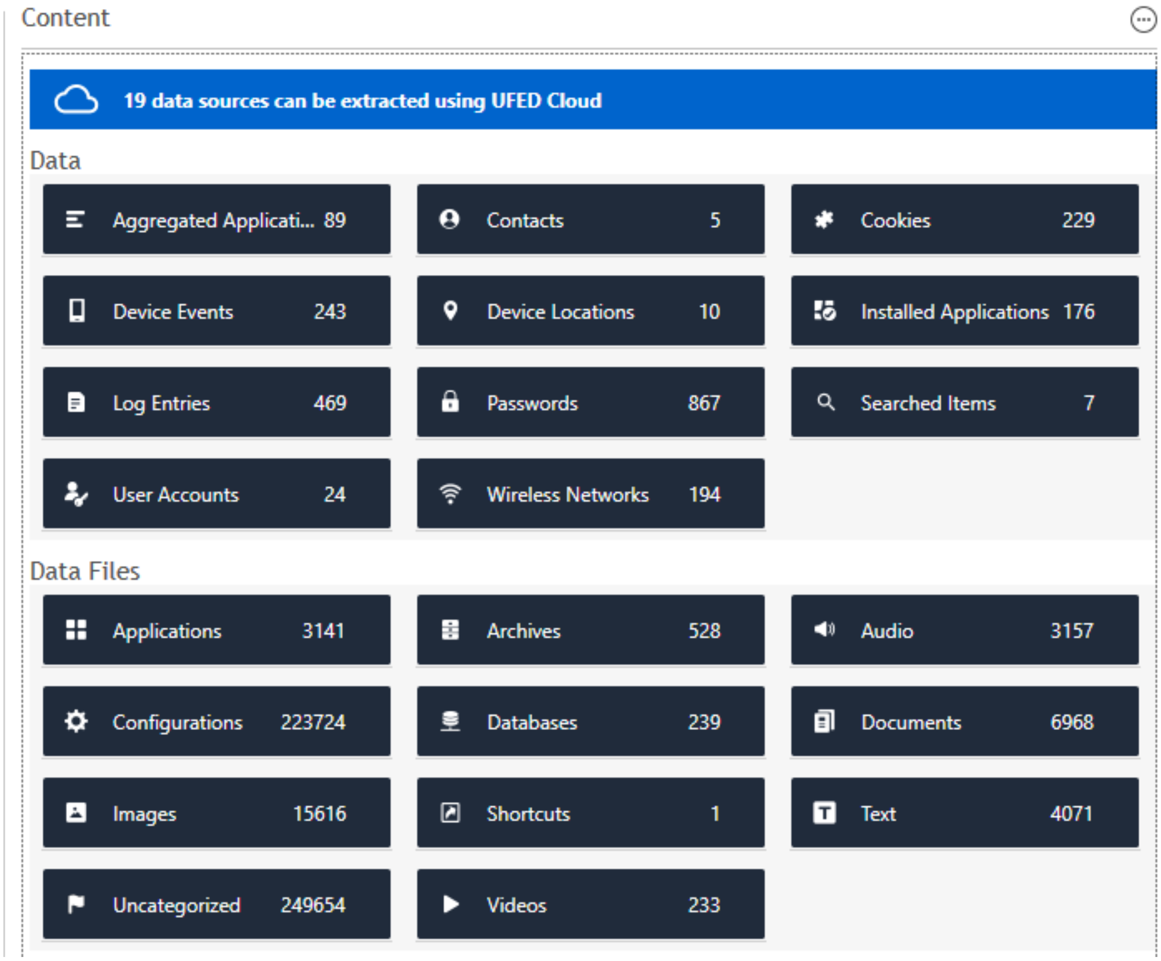
Enter PIN

Your PIN contains at least 4 digits.

The same Samsung Galaxy A32 5G that was shown in BFU section is now *in the AFU lock state. Notice the lack of the "Phone restarted" notification, as well the phone and camera buttons now enabled. The passcode message no longer specifies the device is in BFU mode. A screenshot was able to be taken of the lock screen, but not of the passcode screen (which is a feature default to Android).*

BFU Extractions

In the case that a device is locked with a passcode that is not known, examiners may have an option to receive an extraction based on the device's lock state. When a device is in the BFU lock state, a BFU extraction is able to be created. This type of extraction contains a somewhat limited amount of information, but may be useful in certain cases. Information contained within a BFU extraction mainly includes system data; However, there may be a small amount of user-generated data found within the extraction that may provide new leads for certain cases. This type of extraction is small, and a majority of the information is either system/application data, as well as cached images and videos that are not user-generated. Generally, iOS devices seem to give a larger amount of data than Android in the BFU state.



Content

19 data sources can be extracted using UFED Cloud

Data

Aggregated Applicati...	89
Contacts	5
Cookies	229
Device Events	243
Device Locations	10
Installed Applications	176
Log Entries	469
Passwords	867
Searched Items	7
User Accounts	24
Wireless Networks	194

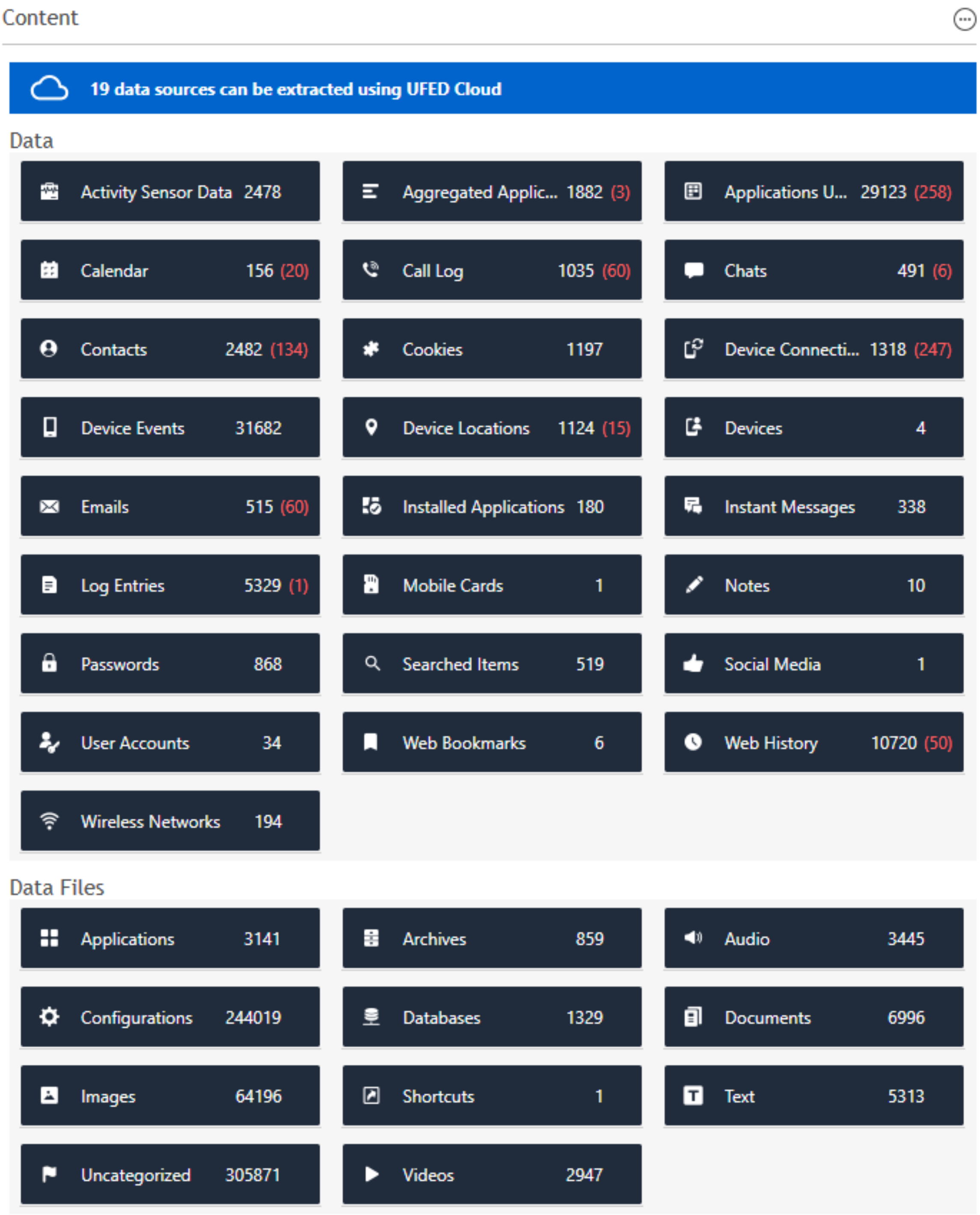
Data Files

Applications	3141
Archives	528
Audio	3157
Configurations	223724
Databases	239
Documents	6968
Images	15616
Shortcuts	1
Text	4071
Uncategorized	249654
Videos	233

An example of a BFU extraction.

AFU Extractions

When a device is in the AFU lock state, an AFU extraction may be created. Compared to a BFU extraction, an AFU extraction contains a vast majority of all user-generated data, which can be seen as about 95% of a Full Filesystem extraction (these extractions will be discussed in the next section). This means an AFU extraction will contain user-generated chats, images, videos, web-browsing data, and much more. Compared to a Full Filesystem extraction, an AFU extraction does not contain Apple Mail, Apple Health, or significant location information. The amount of information you can receive from a device in the AFU lock state can be substantial, so it is important to keep an AFU device powered on. If the device is powered off, the lock state will switch to BFU which could lead to the loss of a lot of potential information.



Content

19 data sources can be extracted using UFED Cloud

Data

Activity Sensor Data	2478	
Aggregated Applic...	1882	(3)
Applications U...	29123	(258)
Calendar	156	(20)
Call Log	1035	(60)
Chats	491	(6)
Contacts	2482	(134)
Cookies	1197	
Device Connecti...	1318	(247)
Device Events	31682	
Device Locations	1124	(15)
Devices	4	
Emails	515	(60)
Installed Applications	180	
Instant Messages	338	
Log Entries	5329	(1)
Mobile Cards	1	
Notes	10	
Passwords	868	
Searched Items	519	
Social Media	1	
User Accounts	34	
Web Bookmarks	6	
Web History	10720	(50)
Wireless Networks	194	

Data Files

Applications	3141
Archives	859
Audio	3445
Configurations	244019
Databases	1329
Documents	6996
Images	64196
Shortcuts	1
Text	5313
Uncategorized	305871
Videos	2947

An example of an AFU extraction.

Full Filesystem Extractions

The ideal situation is when the passcode of the device is known or can be bruteforced. The device may be able to have its passcode bruteforced using validated forensic tools. Once the passcode is known, a Full File System extraction of the device is able to be created, which is the most comprehensive type of extraction you can receive from a mobile device. This type of extraction will give you all the data included within the filesystem of the device.

Conclusion

When a mobile device is seized, it is important to understand the various lock states that a phone can be in. iOS and newer versions of Android often utilize file-based encryption, which causes a majority of the user-data on a device to become inaccessible without the device's passcode. When unable to receive a passcode for a phone, a BFU/AFU extraction of the device could be the only option for receiving data. The difference between these extractions is quite large, so it is important to ensure that phones in AFU mode stay in AFU mode to maximize the amount of information that can be received. If, however, the passcode of the phone is known or can be bruteforced, a Full Filesystem would in fact be the most ideal situation for the collection of a mobile device's data.

References

[i] *BFU Extraction (Before First Unlock) – Mobile Device Forensics.* Cellebrite Digital Intelligence Glossary. (n.d.) **https://cellebrite.com/en/glossary/bfu-extraction-mobile-device-forensics/**

[ii] *File-Based Encryption.* Android OS Documentation. (n.d.) **https://source.android.com/docs/security/features/encryption/file-based**

Author

William Campbell

✉

Published in **Digital Forensics**

After First Unlock | AFU | Android | Before First Unlock | BFU | DFIR | digital forensics | extraction | iOS

Previous Post
The possibilities of Ansible

Next Post
Formatting Hard Drives Within Windows

Search for... | Search

Recent Posts

- Avoid Getting Scammed by Spotting Fraudulent Websites
- Taking off the Mask: Forensic Analysis of Google Voice
- Forensic Analysis and Security Implications of DeepSeek
- iOS 18 Phone Reboot Issue
- Kerberoasting – Recon

Recent Comments