

Best Practice Mobile Device Collection: iPhone Versus Android



July 1, 2022

[Blog](#) [Legal](#)

By Liam Fordy, TLS Director, Business Development

It is safe to say that most of the world's adult (and child) population owns or has access to a mobile phone. These devices are capturing all kinds of private and sensitive data—some of which is generated by the user, while other data is generated by an app or the device itself.

But data is inherently fragile and can easily and inadvertently be deleted or overwritten when improper collection methods are employed. Utilizing scraping tools and unsound forensic methods coupled with ill-prepared practitioners may create authentication issues and, in the worst case, cause data to be destroyed or changed, opening the door to spoliation motion practice.

When it comes to mobile devices, the best method is one that is forensically sound and equips counsel with the tools and data needed to authenticate individual pieces of evidence. A mobile device can reveal key information during a forensic collection, including dates, times, locations, and who a person might be communicating with—in or outside an organization.

That said, not every mobile device is created equal. Apple iPhones and Android phones all act differently, and what can or cannot be collected often depends on the underlying operating system.

Mobile Devices

Ninety-eight percent of mobile phone users have either an iPhone or Android device. Both devices have their own unique challenges, multiple versions, various operating systems, and constant updates. As mobile devices are updated and the operating systems change to make them more secure and increase functionality, digital forensic technology is also being updated.

iPhone

The iPhone is the friendlier of the two because there are several options available to collect a full image of the device. Unlike the Android device, an iPhone can only collect full and specific artifacts or types of data. For example, text messages cannot be specifically targeted at collection. Rather, this information is parsed out from the full image.

The iPhone, like any computer, also overwrites data that the user identifies for deletion, but later versions of the iPhone operating system overwrite data with greater frequency. When it comes to preservation and collection, knowing deleted mobile data is frequently overwritten can be the difference between having the deleted message and not. When it is time for collection, key factors in the deletion of data are the passage of time, movement of data on the device, and software updates. Even then, deleted data that is able to be restored is often incomplete.

Mobile device collection also has a logistical challenge in that no one wants to be without their phone for any period of time. There are three options when it comes to collecting mobile devices and they are the same three options for any data source: in a digital forensics laboratory on-site with a digital forensics examiner, or using a remote collection kit sent directly to the owner or administrator of the phone.

For iPhones, you can also collect through an iTunes backup or from iCloud. These options are sometimes helpful when deleted data is in question, as earlier backups are occasionally stored.

Android

Android devices run on the Google ecosystems, but there are a great number of hardware choices from multiple manufacturers. Another challenge with Android is that these devices are open source, meaning anyone can modify a device. Modifications may include adding storage through a microSD card or changing the rules for how data is stored on the device. This could present significant challenges for digital forensics examiners during a collection.

Unlike the iPhone, Android collections can target specific sets of data. For example, should you only need text messages or messages from another application that is stored on the phone, those can be surgically collected. But, remember that no one wants to be without their phone, so collecting all of the data at the first collection is the most efficient use of your client's time and money.

A common pain point with mobile messaging apps is how to review the conversation outside of the device. In the device, the messages appear in colored bubbles clearly identifying the sender and conversation thread. Once that message is removed from the device, the bubbles and colors are gone and the message thread appears in an Excel or other non-user-friendly reporting platform.

Using an application like Relativity can help. With scripting, a more linear report is generated, whereby the reviewer can visualize the messaging thread and see the colors and bubbles, restoring the conversation to a similar view to how it existed on the mobile device.

Ephemeral Messaging

Ephemeral Messages—generated in platforms like WhatsApp, Telegram, WeChat, and Signal—can quickly disappear, either manually or automatically. These applications are used by both Apple iOS and Android users. What makes them ephemeral is that the user can choose to have the message automatically deleted after a specific amount of time. Users can also choose to delete ad hoc. When this option is set or actions taken, the messages are deleted and cannot be retrieved.

In WhatsApp, for example, we can collect data from the device itself, but in instances where data is deleted, there are options to potentially collect the data from the cloud using cloud-based exports and API connectors.

Each application is different, and while some applications store data on the device, others only store data in the cloud. There are a number of factors that account for the success of being able to collect from these types of applications; after all, they were created with the idea that data would be read and deleted without any artifacts or remnants left behind.

Mobile devices abound, and while mobile device collection can be challenging, they contain a significant amount of evidence and should always be requested in discovery. Preserving the device early and having a digital forensics examiner create a preservation collection image of the device is a best practice, and keep in mind that a mobile device is the primary gateway to a wealth of information in the cloud.



RELATED

Legal

Life Sciences

[pp. & Metadata](#)

[Leveraging the Patent Priority Date: A Life Sciences Focus](#)

By Eric Elting, TLS Director, Global Legal and Patent Business Development
15.06.2022

