Mobile Device Forensics: The New Frontier

Brandon Leatha
Arnold Garcia

iDISCOVERY SOLUTIONS

As the world of mobile devices continues to evolve, so has their ability to create, store, and transmit electronic communications and other forms of electronically stored information (ESI). Mobile devices are no longer seen as a “gadget” or “toy” only used by technology-savvy executives. It is becoming increasingly common for corporate employees at all levels to rely on a tablet, smartphone, or other mobile device as their primary means of corporate communications. In some cases, employees may completely ditch the PC or laptop altogether, making the mobile device a significant source of unique ESI that may be relevant to investigations, litigation, or government inquiries.

As a result, the field of digital forensics has needed to keep pace with this rapid evolution of mobile devices, cloud services, and mobile applications. Mobile device security, preserving and collecting evidence from devices, and the basics of ESI analysis are critical components in any mobile device forensic investigation. As corporate counsel, it is important that you understand how this new frontier of mobile device forensics may impact your next investigation or litigation.

Device Security

As employees continue to store more and more sensitive corporate documents and communications on their mobile devices, the need for securing them with strong passwords and device encryption is essential in helping prevent the theft or loss of this confidential information. While methods of device protection such as PINs, swipe patterns, or biometric security (fingerprint, voice, and facial recognition, etc.) are the most convenient, they are the least secure.

Often considered best practice is an enterprise mobile device management (MDM) solution, which can be used to enforce device security policies, including setting password strength requirements and offering additional encryption options. MDM solutions work on both corporate and employee-owned devices and can provide the ancillary ability to locate, lock, or even wipe a mobile device if it has been lost or stolen.

Unfortunately, this same best practice for securing mobile devices also presents one of the biggest challenges to preserving and collecting ESI. If an MDM is used, the device can be remotely unlocked before data is collected from the device. However, without an MDM, it may be necessary to have the employee reset, turn over, or even clear his or her password prior to collection. If the employee is unavailable or refuses to cooperate, the only remaining option for collecting ESI from a secured mobile device is to use special tools or methods to bypass the security measures.

While bypassing security measures may only require a few clicks in the forensics software for some devices, the success rate will depend on the specific device model, operating system version, and mobile device configuration. In addition, bypassing device security can introduce legal and privacy implications, especially if the device is employee owned (bring your own device or BYOD) and if there is not a clear corporate device usage policy in place.

Device Collection

Mobile device collection, in the simplest of terms, is the process of extracting ESI from a specific smartphone, tablet, or other mobile device for purposes of preservation, analysis, review, and/or production. In addition to the mobile device security discussed above, the vast number of device types and operating system versions (Apple’s iOS, Google’s Android, Microsoft’s Windows Phone, etc.) further complicate the device collection process. Knowing details such as the specific make, model, operating system version, storage capacity, connection type, device configuration, and even the supported cellular technology (e.g. CDMA, GSM, LTE) will help your forensics team select the best options for preserving and collecting ESI from a device. Furthermore, it is important to evaluate which categories of ESI are uniquely stored on a mobile device and are not replicated or synchronized with corporate resources. The primary methods of collection options are the following:

- **Physical Collection** – a complete bit-by-bit copy of the mobile device’s flash memory, including hidden, protected, and deleted content.
- **Logical Collection** – a copy of only the live files found on the mobile device; does not include hidden, protected, or deleted content.
- **Targeted Collection** – a copy of selected files found on the mobile device.
- **Backup Collection** – extracting content from a mobile device backup, which is often found on a PC or Mac that has been synchronized with the device.
- **Corporate Sources** – collecting data from corporate sources including email and file servers, document management systems, cloud-based services, and other corporate storage. This type of collection is often required when the mobile device is unavailable or refuses to cooperate, the employee must first be “rooted” or “jailbroken.” This essentially means hacking the device’s operating system to allow the collection technique to be used. Some of these methods can have a permanent trace or fingerprint on the device and may even violate the device manufacturer’s licensing agreement. In these situations, it is necessary to assess the requirements of the specific matter, the specific mobile device, and the currently available collection options to come up with the best solution. It is always advisable to select the least intrusive method that can still preserve the relevant ESI.

ESI Analysis

Once the ESI has been collected from a mobile device, the next step is to analyze and extract the relevant content for review and, if applicable, production. It is impossible to anticipate all types of ESI that will be found on a specific device given the vast number of applications available and the nature in which those applications are used. It is likely that analysis will find emails, text messages (SMS), call logs, contacts, calendar entries, and photos for most devices. Some devices, including recent versions of Apple’s iPhone and iPad, prevent the collection of personal data if the operating system is altered or jail broken.

Other potential sources of ESI may come from social media applications such as LinkedIn, Twitter, Facebook, Google+, Instagram, or Snapchat; file synchronization applications such as Dropbox, SugarSync, or Google Drive; and communication or chat applications, which include Skype, AIM, Yahoo Messenger, or BlackBerry Messenger. Additional relevant ESI may include Internet browsing history, bookmarks, and website cookies.

While the above list seems extensive, there is also the possibility of finding ESI created by new, or less common, applications. New mobile applications are being created almost daily and may not yet be supported by mobile device forensics software. As a result, it may be necessary to develop a customized solution to support the analysis and production of these sources of ESI.

Additionally, sensitive personal information is increasingly being recorded and stored on mobile devices. Information such as the user’s location, travel speed, elevation, and even fingerprints can be recorded by the vast number of sensors built into mobile devices, which include touch screens, cameras, microphones, fingerprint readers, barometers, GPSs, accelerometers, compasses, gyroscopes, proximity sensors, light sensors, and thermometers. Even cellular and Wi-Fi radios, which are found in almost all mobile devices now, can be used to record location information from nearby cellular towers and wireless access points. Additional sensors can be worn by the user and can record personal health information such as heart rate, blood pressure, body temperature, and vital signs in the case of remote patient monitoring (RPM) solutions.

The collection and analysis of this sensitive and personal ESI can have significant and even unintentional implications. We have all heard of cases where a suspect’s location information was used to place them at the scene of a crime or to show that an individual was texting while driving. It is extremely important to know what information may be stored on a device, or embedded within a document or photo, prior to producing it to another party. Clearly, with such detailed personal and potentially regulated information, security and privacy are paramount.

The world of mobile devices will continue to evolve just as rapidly as the myriad applications that run on them. Mobile devices are no longer just for content consumption; they have become very capable content creation solutions. Because of this, it is important that you understand the full extent of mobile device security and collections, as well as know what types of ESI to expect. The digital forensics experts at iDiscovery Solutions are uniquely qualified to assist you when mobile devices become relevant in your next investigation or litigation.

Please email the authors at bleatha@idiscoverysolutions.com or agarcia@idiscoverysolutions.com with questions about this article.