Advertorial

Obtaining Data From Cell Phones

By: Jeffrey S. Brenner, Esq., NJLPI, Steven Hilary, CCE, EnCE, ACE

With the arrival of the smartphone, the tools people use to communicate with each other have become as diversified as the number of cell phone makes and models. And that can pose a problem for your case. Previously, you could hire a detective to follow a suspect to determine where and with whom (s)he was going/communicating. Now, many of those interactions occur via cell phones, including emails, texts, photos, social media posts, instant messaging threads within phone apps, and, of course, phone calls. The evidence from Facebook, Twitter, Instagram, call logs, and text messages, can, in some cases, objectively prove or disprove your client's credibility and truthfulness. However, with this shift in communications from the physical to the virtual comes new challenges in evidence collection.

MARAGELL Corporate Investigations

Contact: Jeffrey Brenner, Esq., NJLPI

Address: 2 Coleman Ave, Suite 201, Cherry Hill, NJ 08034

Phone: 856.429.0325 x223

Fax: 856.429.0539

Email: jbrenner@maragell.com

Website: www.maragell.com

Depending on the type of phone (iPhone, Android, Blackberry), the data you seek might be stored on the phone itself, with the carrier, or with the phone app developer. Furthermore, preserving the data (wherever it may be) will depend on its status, viz. active or deleted. These three factors (make/model, data sought, status) will determine what your digital forensics expert can do for you when it comes time to gather the evidence.

There are two principal methods to obtain data from a cell phone in a forensically sound manner; a logical image and a physical image.

A logical image obtains data from the phone that is accessible on the phone's file system. You can think of this data as the active data such as call logs, text messages, pictures, GPS location history, instant message threads, etc. A physical image differs from a logical image in that the forensic software targets the physical storage medium directly (the SD card, and built in memory). A physical image will capture active data as well as having the potential to recover data that was previously deleted from the phone. Ideally, the examiner should create a logical image first and then attempt to create a physical image (if deleted content is at issue). This is important because obtaining a physical image entails more invasive work and could render the device unusable.

It is important to identify the make and model of the cell phone to your expert up front so it can be determined whether any one or more of the forensic software suites commonly used by experts can create a logical and/or physical image of the device. New phones, and some much older models, are not capable of being imaged at all, while others can only be imaged logically. The level of security in each model will often determine its forensic-friendliness. In some cases, regardless of which method is used, email data may not be capable of being extracted from the phone even though it appears on it—logging in to the user's email account may be the only way to preserve such data.

For smart phones, it is important to know where deleted data sets reside. For example, cell phones running the Android Operating System (OS) store text messages in a database file named "mmssms.db." Apple iPhones store text messages in a database file named "sms.db." Depending on the type of acquisition (logical or physical) and the forensic software used, these deleted text messages may still reside in the database file itself or within the cell phone's unallocated/deleted spaces. If a deleted text message is not found in either location, it is possible the client created a backup on his/her computer and/or online that could contain the missing text. For other phone apps, the deleted data may be retained within the application's database until purged or it may never have resided on the phone other than in temporary memory until the message was posted/deleted via the application's cloud site.

Practice Pointers: Before calling a digital forensics expert: (1) get the make/model of the phone involved (including the password and storage capacity), (2) determine what you are looking for—active or deleted data, and the type of data i.e. call logs, emails, instant messages, GPS locations, (3) confirm if there is a local backup, and (4) move quickly, especially if deleted data is at issue—the more the phone is used, the greater the likelihood the text/photo/voice message will be overwritten and lost forever. For more information, please contact Maragell, LLC at **info@maragell.com** or by **phone: 856.429.0325.**