The Nuts and Bolts of Mobile Digital Forensics for Criminal Lawyers

by Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

Digital Forensics

Let's start at the beginning. What is digital forensics? According to a 2008 US CERT (United States Computer Emergency Readiness Team) publication, "We define computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law."

Computer forensics, more commonly referred to as digital forensics these days, includes more than just computers. Think CSI with computers and other electronic devices. Digital forensics is the acquisition, authentication, analysis, and presentation of electronic evidence. It is deeply rooted in the scientific process and generally accepted practices of the digital forensic community. From a legal perspective, it is critical that the digital forensic process and the presented evidence be repeatable using various tools and that the outcome is accepted as reliable (Daubert opinion and F.R.E. 702).

As previously stated, digital forensics encompasses more than just computers. With the exponential growth in the usage of mobile devices (smartphones, tablets, etc.), digital forensics examiners typically analyze more mobile devices than computers – which are often the primary source of evidence sought by law enforcement in criminal investigations.

Forensic Software for Mobile Devices

The examination of a mobile device requires specialized forensic software to extract and analyze artifacts such as text messages and communications, application data, and user-generated information from a mobile device. There are many different vendors of mobile forensic software, each having different price points and features. Many are widely used by both law enforcement and private consultants (Cellebrite/Oxygen), with a few available solely for law enforcement use. (e.g. GrayKey).

Arguably the leading tool for mobile device forensics is the Universal Forensic Extraction Device (UFED) Touch2 by Cellebrite. Cellebrite has the advantage of working with many different cell phone manufacturers and models since they construct the data transfer devices that the cellular carrier technicians use to move your messages, address books, etc. when you upgrade your phone. This means they have "inside" knowledge about how a phone stores its data and how to communicate with the device. Its products are used by governments, law enforcement, the military, and private companies worldwide.

Examiners load mobile device extractions into Cellebrite Physical Analyzer software which allows them to search and analyze the extracted data. The UFED Touch2 starts at around $6,000 and annual maintenance and licensing costs are also required, which makes the Cellebrite device rather expensive. The cost includes all the necessary cables for the many different types of mobile devices. It is one of the best tools for analyzing mobile devices on the market and is well worth the yearly cost.

Another popular mobile forensics software is Oxygen Forensic Detective. Oxygen tends to retrieve slightly different data from mobile devices and is better at extracting information for specific mobile

applications. As an example, it does a very good job extracting information from the popular Kik messaging app. It also includes a very useful SQLite database viewer and reader, allowing examiners to parse and interpret application databases that may not be "supported" by the forensic software. Both Cellebrite and Oxygen products include automated picture detection processes to locate images of guns, drugs, screenshots taken by the user, and child erotica/endangerment – integrating artificial intelligence into the products. Of course, an examiner must still review the images for confirmation.

Grayshift's GrayKey product is only available to law enforcement. GrayKey claims to be able to bypass the lock code for the latest iOS devices in less than one hour. The cost is $15,000 and allows for the unlocking of 300 phones - and the device must be connected to the internet to work. They also offer a $30,000 version, which has an unlimited unlocking ability and doesn't need to be connected to the internet. Very little is known about the actual technical operation of GrayKey, but it is suspected that some form of brute force attack is used. We have personally seen the GrayKey being used at law enforcement facilities while a long line of officers waited to have their seized phones unlocked. They are amazing devices and they do work. Your client's inability to recall their passcode may not keep law enforcement out of their device very long.

Apple wasn't happy that Grayshift was making money gaining access to a user's iPhone data. Apple released an update to iOS that contained a feature called USB Restricted Mode. There are several reports that the USB Restricted Mode has successfully blocked the GrayKey from bypassing lock codes. Another alternative to bypassing lock codes is the Advanced Unlocking service from Cellebrite. Cellebrite does the work and does not have an actual piece of hardware to sell to the end-user. Cellebrite states that they can "determine or disable the PIN, pattern or passcode screen lock on the latest Apple iOS and Android devices including Alcatel, Google Nexus, HTC, Huawei, LG, Motorola, Samsung, and ZTE."

Acquisition

If your client's mobile device was seized and analyzed by law enforcement, a copy of the forensic acquisition or data extraction may be provided to your expert for independent review. Depending on the type of case and evidence found, the review may have to take place at a law enforcement or government facility, especially if dealing with contraband. Otherwise, there shouldn't be an issue providing a copy for your expert to review offsite at their convenience saving your client time and money.

Most analysis packages provide a method of data extraction. As an example, Cellebrite provides a custom hardware and software solution to capture data from mobile devices. As previously stated, Cellebrite supports the largest number of mobile devices. By support, we mean that Cellebrite can extract the most amount of data from the largest variety of devices. Depending on the version of Cellebrite you have, you will be able to extract logical data (data that a user can normally access) or perform a physical extraction, which is a complete image of the memory from the device (including any deleted data). As you can imagine, most attorneys will hire an expert that has the right tools and software to extract data.

However, you may not need to perform a forensic acquisition of the device. The preservation of the relevant information may require nothing more than taking a screenshot of relevant text messages. There are other methods where you can preserve data from a mobile device with little cost or effort using a tool such as iMazing (https://imazing.com). IMazing costs $59.99 per year and allows users to

capture and produce messages from an Apple iPhone in a variety of formats including Acrobat PDF and Microsoft Excel. In most criminal matters, self-collecting data from a mobile device rather than by an expert should be considered extremely carefully, given what is at stake for the client.

If you are not acquiring data from a mobile device using forensic tools, the most common way to preserve data is via a device backup. iPhone users should be using iTunes as a backup since it contains more data than an iCloud backup. Android users can use many of the various backup products that are available. It is even an option to connect the phone to the computer and copy the files directly to the hard drive or some other external storage device.

Data Types

What types of data can be recovered from a mobile device?

Probably the most sought-after type of data is communications. That includes email, but text messages (iMessages on iOS devices) are the most used method for communications amongst mobile device users. It is not difficult to extract messages in a format that is easily reviewed in a spreadsheet. It is important to keep the threaded messages together since there may be multiple conversations with various people.

Message attachments should also be extracted and associated with a specific message. These days it is also critical to preserve any emojis associated with a message. This means that the exported data file must be encoded to Unicode UTF-8 to preserve the emojis. The challenge is how to deal with other messaging apps such as Signal, WhatsApp, Facebook Messenger, and even Slack. The data may be encrypted and not stored on the device – but rather with the vendor.

If the message is viewable on a device, but not contained within the extraction, you can normally take a screenshot to preserve the message.

What other types of data are available from mobile devices? Pictures and videos immediately come to mind. Users are constantly using their phones to take pictures (e.g. selfies) or videos to share with others. Like messages, it is not hard to extract pictures or videos from a phone. You can even synchronize your photos with a cloud account to preserve them. Any downloaded or created files are also available to be copied from the phone to some other media type.

Geolocation Data

Speaking of images brings geolocation to mind. Many mobile device applications use geolocation to help improve the user experience. GPS coordinates are used for map applications such as Waze and Google Maps. Shopping apps use geolocation to target ads for your location. In other words, it does no good to display an ad for a store that doesn't even exist in your state.

GPS coordinates can be included in the metadata of photos. That can be very useful when used as evidence and to provide some level of authentication and determination as to where the device was physically located on a particular date and time. As an example, you could crowdsource Twitter to see who posted photos of a traffic accident at a particular intersection. GPS coordinates would be used to determine photos taken at the intersection during a specific time. The GPS coordinates could also be used to validate a photo as being taken at a particular location. Accessing GPS data is easy for photos. Merely looking at the photo properties reveals the metadata including such things as GPS coordinates, date and time photo was taken, camera manufacturer & model, camera lens settings, etc. Typically, it's

harder to get GPS information from other apps, especially if they're not supported by forensic software. The information may be stored in a database and not specifically attached to individual files. Finally, the user may have location services turned off or the app may not preserve GPS data.

You can also request location data from Google (or obtain it with the account holder's credentials) if the phone was set up or configured with a Google Mail account. You might be surprised at how frequently Google is tracking the physical location of the mobile device.

Call History

Another area of interest to lawyers is the call history. The call history shows the duration of the call, the time of the call, the phone number and contact information if it exists on the device, answered or missed, and whether the call is inbound or outbound. It's worth noting that call history records and even individual entries can be deleted (and potentially recovered) from the mobile device. Requesting the call history from the cellular carrier is a lot more difficult and will take longer too. Not to mention that the records can be in a cryptic form and difficult to understand.

Web-browser History

Forensic examiners are used to extracting internet history from a mobile device. History can be recovered from all major mobile browsers including Chrome, Firefox, and Safari. If your client was using the Tor Browser, chances are there won't be any history stored on the mobile device. Additional browsing artifacts that may be of interest include files that were downloaded on the mobile device, as well as search terms and websites logged into.

Voicemail

Relevant information may also be contained in voicemail messages. In some cases, the actual audio file may be able to be exported too. However, there will be no linkage between the voicemail activity and the actual message file so make sure you document what goes with what. A little-known fact is that it's also possible to retrieve a voicemail message even after it has been deleted. This is particularly true if visual voicemail is used. The file is downloaded from the carrier to be played back visually. Deleting the file from the carrier doesn't necessarily delete the file from the device, which may be able to be recovered by your forensic expert.

App Data

Extracting and preserving data from apps is all over the map and probably best left to your forensic examiner. Having said that, you may be able to find a specific piece of software that is designed to target the data from a particular mobile phone app. More and more app developers are storing data in databases as opposed to discrete files. Apps may use PLIST, JSON, or SQLite file types to store information and records. The database of choice for many apps is SQLite, which is a "mini" version of SQL. Many forensic software tools can analyze and decode the contents of the SQLite database for a particular app and report on its contents in a usable and understandable format. If the specific app is not supported, then the examiner must perform a manual process of testing and querying the database with SQL commands. It's a slow and tedious process and can be expensive. If the usage of a particular app is important to your case, it may pay to run through the manual process to extract the relevant evidence. Many times artifacts stored within third-party viewers have been able to show how many times a file was viewed or played on a mobile device, including when that activity took place.

Summary

It is impossible to know all the data contents that are available for preservation and extraction from mobile devices. Apps are constantly being updated, which compounds the problem. For instance, there may be a software tool to extract data from version 2 of the app, but not if the app is upgraded to version 3. As legal counsel, you know what questions need to be answered – and the mobile device may hold the key. No matter what data you may be after, working with a digital forensics expert to examine a mobile device will help you be prepared for trial and can be beneficial to the defense of your client. It can also bring a quick resolution to the matter. Either way, justice prevails.

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* *snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker, and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* *jsimek@senseient.com*.

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* *mmaschke@senseient.com*.