Mobile Forensics: A Concise Guide for Lawyers

— By Zachary Roush

Mobile forensics is the process of acquiring, analyzing, and producing data from mobile devices

We often see more mobile devices come into our forensic lab than traditional computers (desktops and laptops). One reason for that is because mobile devices are consistently becoming more like computers. Device users can send and receive email, create and edit documents, save files and so much more.

Mobile device storage space has also skyrocketed. The most recent Apple iPhone, the iPhone 14 Pro Max, comes with storage sizes starting at 128 GB and goes to 1TB of storage. If you're not an iPhone user, then the latest Samsung phone, the Galaxy S22 Ultra, has a very similar storage capacity range. Many mid-tier laptops and desktops have storage capacity like that of a device that people carry around in their pockets.

What is mobile forensics?

Mobile forensics is the process of acquiring, analyzing, and producing data from mobile devices. Mobile devices can include smartphones, tablets, and feature phones.

The mobile forensics process often starts with gathering information about the type of device that a person has in their possession. After determining whether there is support for that specific make and model, a forensic collection of the device will be performed.

Once a forensic collection of a device is done, the forensic analysis of the device begins. This is where a digital forensic analyst will run search terms, date and time filters, and review the data on the device according to the scope of work determined by their search authority.

After the analysis is the reporting phase. This includes generating some type of production containing the results of the analysis. This could range from a file having relevant text messages to a report of findings for a review of a device for spyware or malicious activity.

What types of data can be found or examined from a mobile device?

The type of data found and examined on a mobile device again hinges on the forensic collection tool's support for the make and model of device, as well as the analysis software's support for interpreting the data. We find that, in most cases with mobile forensics, there are a few common data types that are requested:

1. Communications, including text messages, chats, email, call records & instant messages.
2. Internet browser history.
3. Recovery of deleted data.

The fact is that mobile devices can store a lot of data, especially as their storage capacity increases. It is not uncommon for items such as location data and other application data to be found on these devices.

What about deleted data?

With mobile devices, there certainly is a chance to recover deleted data. Usually with mobile devices, when an item is deleted from the device, the space that the data was occupying is marked as available for new data to be written to.

To simplify, if you deleted a photo on your phone, space it was taking up now becomes available for new data to be saved to. This means that if you then received new messages or take a new photo or video, it is possible that those new data types have been saved over that deleted photo.

In the digital forensic world, this means that the original photo has now been overwritten. If data has been overwritten on a mobile device, then that data is no longer recoverable. If the data has not been overwritten then there is a chance, depending on the make and model of device, that deleted data can be recovered from the device.

Additionally, many mobile devices have reset options. A factory reset of a device will also overwrite any previously existing data on the device.

Can mobile devices get infected with malware or spyware?

Simply put, the answer here is yes. A mobile device can be infected with malware and spyware. The reality of it is that mobile devices are extremely similar to computers and variants of malware do exist to run on them.

The methods that are employed to infect a mobile device with malware are similar to how a computer gets infected. Recently, there has been a rise in mobile phishing and spoofing. Spam text messages with links or downloading emails with malicious attachments can still affect a mobile device.

It's best to follow the rule of "think before you click." Meaning that, when receiving a text message that contains a link, which are often shortened using a URL shortening services such as bit.ly, look at the link, and ask some questions.

- **Are you expecting someone to send you a link or attachment?**
- **Is it a service asking you to login?**
- **Does it generate some sense of urgency? (i.e. Do this now or your account will be suspended)**
- **Who did the link or attachment come from?**

If you stop and think about those questions before clicking on something received via text or email you will likely save yourself from a world of hurt. And if it is a service like a bank used, the best thing to do in that case is to login on the bank's website by using your web browser. The link, if clicked, could lead to a very convincing fake website where the attackers have now harvested your username and password.

Think before you click!

Another vector that mobile malware can be installed through is the installation of applications on the device. There are third-party app stores available to download apps from that could be malicious. Trusted app stores have a verification process that app developers must go through before the app is available on the store. There are certainly items that do slip through the verification process but downloading apps from a third-party app store is likely a bad idea! Stick to apps from trusted sources.

Another way mobile devices can be infected is through what is called a Jailbreak or Rooting of the device. This process is where the device's internal protections have been bypassed and have unrestricted control of the device's operating system. This may allow for a user to get some added privileges, but it also degrades the device's security measures to protect the data on the device.

An analysis of a mobile device can determine whether the device is infected with malware or spyware. It is also possible that the device isn't infected - this can be common with spyware. In some cases, especially if there are cloud backups of a device being made, some common spyware applications will use the backups and download that information to gain access to messages, emails, calls, etc. If that is the case, what has usually happened is that the credentials to the account where the backups are being stored have been compromised. An analysis of the device will not reveal this type of compromise but often a review of the account will show other devices logged in.

Questions to expect

There have been a few questions that are critically important and will likely be asked of you by a digital forensic expert before the start of a new case. Having the answers to these questions can help save you time and money.

1. What is the make and model of device?
With this question the digital forensic expert is trying to understand what type of device you have. Do you have an Apple iPhone 12, a Samsung Galaxy S10? Do you know the specific model number? The answers help the digital forensic expert gauge the support for the device and assists in figuring out what types of data can and cannot be retrieved.

2. What is the device's storage capacity?
Does the device have 128 GB, 512 GB or some other size storage capacity? This question helps the expert determine the potential length of time a device acquisition may take. The larger the storage capacity, the longer it is going to take to make the forensic collection.

3. What types of data are you looking for?
Knowing this ahead of time can help the expert determine the amount of time it will take to conduct the analysis as well as advise you of what data may or may not be found on that device.

Mobile devices are only getting more features and more storage capacity as technology advances. As those devices advance, so do the methods of collecting and analyzing data from the devices. We are walking around with the equivalent of small computers in our pockets and bags. They store a wealth of information about our lives, and we often find ourselves wondering how we would live without them. They also constitute a treasure trove of valuable information in many legal matters!

Zachary Roush is a Digital Forensic Examiner at Sensei Enterprises, Inc. He is a Cellebrite Certified Physical Analyst, a Cellebrite Certified Operator, an EC-Council Certified Incident Handler, and a McAfee Certified Cyber Intelligence Investigator.
sensei@senseient.com