SPRING 2024 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we discuss how rapidly changing technology causes eDiscovery nuances, the complexities of smartphone preservations, and how courts are handling inadvertent production failures.

The Nuances of Smartphone Images for Digital Evidence: Many Flavors Beyond Vanilla and Chocolate

Digital evidence from smartphones is becoming increasingly relevant to almost every investigation and litigation. Unlike laptops and desktops, where a forensic image is much easier to understand, the nuances of a forensic image of a smartphone are much more difficult to ascertain. These complexities may be due to the phone's capacity, Mobile Device Management (MDM) software, encryption, or the limited amount of time you will have possession of the phone. There may also be interoperability issues with the imaging format utilized and the analysis tool used for examination. Understanding and selecting the best extraction type is essential for completing the job. This article discusses the primary types of phone extractions that can be obtained and references extractions versus images because the term imaging suggests that a bit-for-bit digital duplicate of the data has been obtained. This approach, the Physical Extraction method, used to be the standard benchmark when obtaining forensic data. With technological advancements however, extractions are more akin to ice cream: vanilla or chocolate aren't the only flavors, and often, more flavors make for better results.

Physical Extraction

For mobile devices, an examiner would obtain a physical extraction by imaging the memory chip contained in the phone as if it were a hard drive in a computer. The examiner could then access the memory chip using a forensic tool that communicates with a phone placed in a special mode. Depending on the phone type, the phone could be placed in this mode by holding down the phone's buttons in a certain sequence. Once in that mode, the tool could make that bit-for-bit image copy of the memory chip. There are other methods of access to the memory chip, such as using a forensic boot loader or by "chip-off" which is the process of physically removing the chip from the motherboard and accessing the chip directly.

Physical images, however, are no longer the standard when examining today's mobile devices. Most of today's modern devices are encrypted and obtaining a physical image of encrypted data yields just that – encrypted data. To complicate matters, today's handsets utilize the phone hardware itself to encrypt and decrypt the data, so decrypting the data outside the phone is nearly impossible. As a result, Physical Images are no longer the gold standard for mobile phone forensics.

Full File System Extraction

The most complete imaging process is the Full File System extraction (FFS). This method copies all the data on the phone on a system level as it is stored on the phone. Most messaging apps store their data in database files. This method extracts the entire database so you can reconstruct the message and its data from the source. Accessing the database directly also gives you the best chance at recovering deleted files. One of the most valuable items you get with an FFS is the keychain file. This file contains the cryptographic data needed to decrypt the databases used by third-party messaging applications.

It is worth mentioning two distinct realms of smartphone forensics: the Law Enforcement realm and the eDiscovery realm. Law enforcement rarely obtains the password to the phone and spends a great deal of their examination time trying to gain access to the data. The examination almost certainly starts out in a Faraday Box, a cumbersome physical enclosure that blocks radio waves from interacting with the phone in an attempt to prevent the phone from being remotely wiped or altered. In the eDiscovery realm, the use of a Faraday box is rare because the custodians are willing participants who provide the passcode and access to the data.

In both realms, the full file system extraction is the most complete extraction you can obtain – but may not be the most cost-effective extraction. These extractions take a longer time to complete, and often forensic tools require additional fees to achieve this level of access. The decision to use this method depends on what items you need to collect and why. If the goal of the collection is searching a mobile device for all messages with a specific person across multiple messaging apps, then an FFS would be a logical choice. However, if the goal is to collect specific photos or text messages in an unencrypted app, then an FFS is not the most efficient and cost effective extraction.

File System Extraction (Partial)

This type of extraction copies all the files available to the user after the user has entered the password onto the phone. The phone is connected to a forensic tool, and the examiner configures the phone to trust the forensic tool. Once the trust has been established, the tool starts copying all the files on the phone that it can access. It cannot access the full keychain or certain system files, but it can usually access all the application databases that contain messages, chats, contacts, calendar items, and third-party application data. These databases, if encrypted, will require the keychain in order to view its contents, and a file system extraction does not provide this.

In the Law Enforcement realm, a partial file system extraction is possible even on locked phones. What exactly is available and how much data can be retrieved depends on the current state of the phone and whether it is in AFU (After First Unlock) or BFU (Before First Unlock) mode.

Advanced Logical / Hybrid Extraction

Many cell phone forensic tools have developed hybrid extraction methods which combine a logical extraction with a partial file system extraction. Cellebrite calls their method an Advanced Logical

Extraction whereas Magnet/Grayshift calls their method Logical+. The advantage to using this extraction method is time minimization coupled with the completeness of the dataset. If messaging, call logs, contacts, and third-party messaging apps are the target for the collection, this can be an efficient way to complete the collection. However, one must be careful to know which third-party messaging apps this method supports. Similar to the file system extraction method, this option does not obtain a full keychain and although you may have collected a messaging database, you may not be able to decrypt it.

Logical Extraction

A logical extraction is the quickest and most common extraction method. Extraction occurs after the examiner has authenticated the phone, attached the phone to the forensic tool, and established the trust relationship. The tool then communicates with the phone through APIs (Application Programming Interface) and requests access to the phone's live data for collection. Sometimes this means the tool will load a temporary agent onto the phone that communicates with the phone, collects the data, or initiates an iPhone (iTunes Backup) or ADB backup. Once the extraction is complete, the agent is automatically removed from the phone.

When MDM software is in use by an organization, it can stop the extraction by preventing the agent from being loaded onto the phone. In cases such as this, it could mean initiating an iTunes or ADB backup, or initiating a backup into the cloud. If the data needed to move forward with the case is in the backup that has been pushed to the cloud, the backup can be collected remotely, with minimal interaction with the custodian. An experienced forensic examiner can assess the situation and determine and discuss the most appropriate extraction method.

Targeted Extraction

Targeted extraction is a collection method that allows the forensic examiner to specify the evidence they are seeking to collect. This should be considered a remote logical extraction as the tool attempts to isolate the specific database or application containing the data. It either extracts the single item of interest, or the database that contains it. Whether it is a specific chat thread or all messages on the phone, the idea is that it only extracts what is needed. The advantage of this is speed, which means it is more convenient for the custodian as well, and there are now tools available to do remote collections, so the phone never has to leave the custodian’s possession.

Remote targeted collection sounds like the perfect tool for those cases where a custodian is compelled to produce messages but does not want to allow access to personal photos or other data contained on the phone. But how perfect is this? Remote targeted collections should only be considered a forensic process if the examiner is able to search the phone remotely to identify items for collection. If the custodian does the identifying, the process is not forensic, is not unbiased, and the examiner should note that the items collected were identified by the custodian – not the examiner. Remote targeted collections are starting to become more common, and they can certainly have their advantages in the right situation. However, the ability to defend the process is still questionable and has not come up in court yet.

Manual Extraction

The most often overlooked method of collection is the Manual Extraction. This is the process of manually scrolling through a phone and photographing or taking screenshots of the device. This is especially useful when collecting encrypted chat messages from third party applications when a method to decrypt a message database has not been developed - or when you are unable to

obtain the keychain (FFS). This method is put into practice quite commonly on applications where automation is not possible.

Which Extraction Flavor Is the Best?

The answer to this question depends on what is requested for collection, how long will the examiner have access to the device, the risk of the methodology being challenged, how large is the storage, and the cost parameters. Based on what needs to be collected, the examiner will need to decide based on this criterion. Sometimes doing multiple collection methods may be warranted. After all, there are times chocolate, vanilla, and butter pecan make sense.

Please direct questions and inquiries about electronic discovery, digital forensics, cybersecurity, and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

MASTERS CONFERENCE MAY 2024
Chicago, IL: May 15, 2024

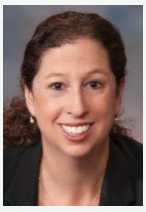
NET DILIGENCE CYBER RISK SUMMIT
San Diego, CA: May 20-22, 2024

SNOWFLAKE DATA CLOUD SUMMIT 2024
San Francisco, CA: June 3-6, 2024

TECHNO SECURITY & DIGITAL FORENSICS CONFERENCE EAST
Wilmington, NC: June 4-6, 2024

IOT TECH EXPO 2024
Santa Clara, CA: June 5-6, 2024

Click here to see more upcoming events and links.



Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: