SUMMER 2019 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss smartphone discovery and key gotchas. We also explore case law involving monitoring employee activity on smartphones.

Top Ten Gotchas for Smartphone Discovery

After working on smartphone discovery for over a decade, Digital Mountain has been engaged on over a thousand cases. Below are some key gotchas to consider when performing data discovery based on our experience:

1. **Email on Smartphones.** In most cases, databases for emails are encrypted or protected from extraction by the operating system in iOS devices. There are times when performing discovery on a device with an older iOS, you may not be able to obtain the email message body, but may be able to extract limited header information (e.g. From, To, CC, BCC, Subject, Date/Time information). For Android smartphones, you may be able to obtain an email if the user viewed the message previously on the device.
2. **Incomplete Messages.** There are times, due to interrupted Internet access, that the messaging application does not continue or finish downloading data from where it left off (AKA resuming the state of the transaction). Many clients may believe that something happened during the discovery processing, but in fact, the data was stored incompletely on the phone in the ordinary course of business.
3. **Additional Passwords Required.** A user may have a PIN or passcode locking a smartphone. However, for iPhone devices, if iTunes is used for backing up a smartphone, the user may have an extra password that will be required to acquire the data on the phone. Without this password, you may have to take extra steps to access data on the phone. If the user cannot recall the password, the administrator may need to perform a password reset prior to the phone being imaged. This is similar for Android backups and any additional passwords must be obtained or reset. The reset process should not damage the user data stored on the phone.

4. **Emoji, Stickers, and Attachment WYSWIG Issues.** Depending on the emoji, it may be viewable within a smartphone report with commercially available tools. However, certain emojis may not be viewable given custom emoji keyboards or other compatibility issues, so WHAT YOU SEE IS WHAT YOU GET (WYSWIG) issues do exist. As with emoji viewing, stickers may not display properly in processing and some attachments may not show up accurately when processed.

5. **Voice to Text Issues.** Despite the pervasive use of voice to text applications, the translation may not always be what the user intended since automation or external intervention occurred. This is important to keep in mind when analyzing intent and authenticating digital content.

6. **Smartphone Apps Are Not Always Supported by Commercially Available Tools.** Smartphone analysis tools will show only what data the software can parse or make presentable for review because the software developer invested in creating proprietary technology to display specific data. There may be messaging applications that the tool did not parse and additional relevant data may exist. It's important to review what applications are on the phone. Many social media communications are stored exclusively on the cloud and the smartphone must connect to the cloud to access the data. Also, computer forensics tools utilized for smartphone communication parsing generally do not process data for review tools, therefore companies such as Digital Mountain have developed specialized technology for this industry need.

7. **Lack of Portability of Images.** Not all tools that parse and analyze smartphone data are equal or compatible and there is a lack of portability for moving forensic images into a different tool to analyze data. Therefore, it's important to choose forensic experts using the most optimal tools, so there are no issues downstream with respect to analysis and review. Also, if the data is being shared among different providers, tool compatibility discussions need to be had upfront.

8. **Obtaining Proper Permissions and BYOD Implications.** Although a user may have business communications stored in text messages on a device, the targeted device may have been purchased by the employee. In order to retrieve the data off the phone, the employee's permission may be needed or attorneys may need to be retained to obtain legal authority for the retrieval.

9. **Software Development and Ability to Keep Apace with Numbers of Devices.** Although most software developers attempt to keep up with Android and Apple smartphones and the fast pace of changes, there are over 10,000 models of mobile phones being used today from over 3,000 manufacturers. In many cases, clients aren't sure of the makes and models of devices to be imaged. Without this key information, it is difficult for computer forensics practitioners to ascertain tool compatibility and perform advance planning to ensure the data preservation process runs smoothly.

10. **Deleted Text Messages.** Deleted text messages may be available for discovery on active smartphones. However, backups from different points of time may also exist on local hard drives (e.g. iTunes) or the cloud (e.g. iCloud or Android Backup) and contain additional messages that were subsequently purged or overwritten and not available on the active device. These backups should also be considered and could be a rich source of evidence when deleted text messages are a critical element of a case or a device has been factory reset.

Unlike in the early days of e-discovery and computer forensics, smartphone discovery has become much more mainstream. All processes are not created equal and there is a plethora of untrained examiners relying on whatever the output of the tool he or she is using displays. Hopefully, these top ten gotchas will help you navigate smartphone discovery, so your focus can be on the merits of the case rather than the technical issues.

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

UPCOMING INDUSTRY EVENTS

BLACK HAT USA 2019
Las Vegas, NV: August 03-08, 2019

ABA ANNUAL MEETING
San Francisco, CA: August 08-13, 2019

ILTACON 2019
Lake Buena Vista, FL: August 18-22 16, 2019

PFIC 2019 CYBER SYMPOSIUM
Park City, UT: September 10-12, 2019

THE SEDONA CONFERENCE WORKING GROUP 11 MIDYEAR MEETING 2019
Montreal, Canada: September 18-19, 2019

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: