SUMMER 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 the digital forensics implications of ephemeral and encrypted messaging data, the rise of two messaging giants, and noteworthy legal developments.

Taking Smartphone Discovery the Final Mile With Encrypted Messaging Apps

You just received a new case and crucial to the evidence are messages stored on an iPhone 15 Pro. Just before collection, your digital forensics examiner asks you, “Which method would you prefer? We can perform a Logical or Advanced Logical collection, as well as a Full File System extraction for an additional fee.” Unsure of how to respond, you quickly perform a web search and find that a Full File System extraction is the most comprehensive method possible and available on this make and model of phone. However, is it always the better choice and worth the cost?

With today’s mobile devices, the method and manner of data export are crucial. Typically, the desired data includes communication data, particularly text messages. Modern phones encrypt their data, making a password necessary for data collection. With the password, the examiner can "unlock" the phone, decrypting its contents and making the data accessible. Using appropriate tools, the examiner can extract messages into a data file that can be searched with eDiscovery or forensic tools for specific content. Although encrypted, native text messaging apps, like iMessages, can be captured using a logical file extraction method, as unlocking the phone also unlocks the encryption on native applications.

However, third-party applications offer an additional layer of security. These apps can secure messages using an additional password or alternative method, and just having the phone password might not be enough to access the data. There are many ephemeral messaging apps like Signal, Wickr, and Telegram that provide secure, end-to-end encrypted communication and store message data in an encrypted database file. By using the phone’s password, you can unlock the phone and start the 3rd party app, revealing all of its stored messages. Even if you can access and view the contents of the messages on the phone itself, extracting that data for ingestion into an eDiscovery platform is a challenge - especially with thousands of pages of messages among hundreds of people.

The only practical way to search the data is to systematically export the messages or export the database containing the messages. While obtaining the database file can be done with a logical file extraction, the phone's password alone is insufficient to decrypt it. Third-party applications create a specific key for its application, stored in a very secure location on the phone. This key may not be accessible on certain ephemeral applications during a logical or advanced logical extraction and can **only** be accessed through a Full File System extraction. With the app-specific key, you can decrypt the database after it has been exported, thus accessing the messages contained therein.

Obtaining a Full File System extraction is necessary if you are aware of data contained in third-party applications that needs to be examined. It is important to know which messaging applications the custodian is using when submitting their phone for extraction and to discuss with the forensic examiner which extraction method will be required to access that data. If the applications on the phone are not known at the time of collection, it is most prudent to opt for a Full File System extraction if the budget allows. This method provides the most comprehensive collection possible and offers the ability to attempt to decrypt data from third-party applications once they have been identified.

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

UPCOMING INDUSTRY EVENTS

ILTACON 2024
Nashville, TN: August 11-15, 2024

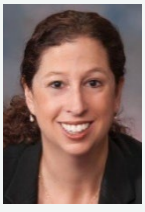
SANS DFIR SUMMIT 2024
Salt Lake City, UT: August 22-23, 2024

THE SEDONA CONFERENCE WORKING GROUP 12 ANNUAL MEETING
Phoenix, AR: September 9-10, 2024

TECHNO SECURITY & DIGITAL FORENSICS CONFERENCE WEST
Pasadena, CA: September 16-18, 2024

MASTERS CONFERENCE SEPTEMBER 2024
Seattle, WA: September 18, 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: