Case Study: Standard vs. Premium Mobile Device Collection Methods

In a high-stakes corporate litigation case, a mid-sized law firm was tasked with conducting a data collection on mobile devices belonging to key executives of a multinational corporation. The litigation centered around allegations of trade secret misappropriation. Avalon was asked to perform a standard data collection on the mobile devices and report their findings to the firm.

The Challenge

The standard extraction yielded substantial data, but nothing conclusive regarding the misappropriation claim. Crucial timeframes had missing data, specifically in encrypted messaging applications believed to be used for sensitive communications. The team suspected that critical evidence was either deleted or stored in encrypted formats inaccessible through standard extraction.

> The evidence **discovered** through **premium extraction** proved to be the **turning point** in this case.

The Solution

Faced with insufficient evidence after using standard data collection methods, the firm debated the necessity and legal implications of a more invasive forensic analysis. After consulting with Avalon's digital forensics experts, and ensuring compliance with legal standards, they decided to proceed with a premium full file system extraction.

Scope of data retrieval:

- Standard Extraction – Typically limited to the logical level; meaning, it only accesses data that the phone's operating system readily provides. This includes files like call logs, messages, contacts, and some app data. It's comparable to what a user would see in their device interface.
- Premium Full File System Extraction – Goes deeper to access the entire file system, including deleted data and system files. This can uncover more detailed information such as location history, encrypted app data, and more.

Level of Access:

- Standard Extraction – Limited to user-accessible data and what the device's default security settings permit.
- Premium Extraction – Utilizes advanced methods to bypass

Case Study: Standard vs. Premium Mobile Device Collection Methods

security features and encryption, enabling access to practically all data on the device.

Type of Data Recovered:

- Standard Extraction – Recovers basic user data: texts, call history, contacts, photos, and some app data.
- Premium Extraction – In addition to standard data, it can recover hidden, deleted, or encrypted files, including system logs and deep app data.

Time and Resources:

- Standard Extraction – Quicker and less resource-intensive.
- Premium Extraction – More time-consuming and requires more advanced technical expertise and tools.

The Results

This case study demonstrates the critical difference in the depth and breadth of data recoverable through standard versus premium extraction methods. For legal professionals, understanding these differences can be pivotal in formulating an effective eDiscovery strategy, particularly in complex litigation scenarios where the stakes are high, and the digital footprint is deep and sophisticated.

The evidence discovered through premium extraction proved to be the turning point in this case. It not only provided direct evidence of misappropriation, but also demonstrated the intent to conceal this activity. This case highlighted the limitations of standard extraction in accessing all relevant data, especially in sophisticated corporate environments where encryption and secure messaging apps are common.

QUESTIONS?

For more information on any of our services, please contact:

Rebecca Rudell
Marketing Manager
rebecca.rudell@teamavalon.com