

Cell Phone and Mobile Device Forensics

From the simple cell phones to a more complicated personal digital assistant (PDA). These devices have become critical to both the personal and business users in this digital age. Globally, throughout the day, detailed information on the user's and their communications is collected and stored, creating a series of unique individual images. Items such as e-mail, text messages, Internet history, and even the user's location are saved and stored, making the mobile device a valuable source of evidence in civil and criminal investigations.

These devices present unique challenges to the digital forensic investigator. Proprietary operating systems, diverse firmware implementations, multitudes of network communication protocols, and the ever changing methods of data storage, represent challenges for the investigator seeking to uncover data within the mobile device's memory.

The forensics analysis of a mobile device is an extremely specialized area, above and beyond the basic digital forensic training methodology. An effective analysis of mobile devices demands first-hand knowledge. Without this vast knowledge, proficiency and experience, serious errors may occur during the forensics data acquisition process. The worst case scenarios, critical data could be removed, putting key evidence at risk.

In a recent case, we were retained to acquire the digital content from the cell phone of our client, who had been charge with Domestic Battery. Several months earlier she had successfully obtained a restraining order against her now ex-husband, due to ongoing marital issues.

Three days prior to her arrest, he was severed with divorce papers. In a fit of anger he attempted to contact her via cell phone. When 30 attempts in less than fifteen minutes proved to be unsuccessful, he began sending text messages. Our client responded to one of the many message allowing her ex-husband to come to the residence when she was not home to remove his personal belongings.

At the agreed time and date he arrived at the residence and removed all of the contents of the home. After several hours (at the agreed time he must have been completed and no long in the residence) she returned to find her ex-husband still in her home and the home striped of its contents. She demanded the return of the household furnishings, and he refused. He became physically abusive as he has done many times in the past. She managed to lock herself in the master bedroom and called 911.

When Law Enforcement arrived he claimed she lured him back to the residence and staged the entire incident to have him arrested for Violation of the Restraining Order. During the removal of the contents of the home he sustained cuts on his right hand which he claimed as defensive wounds from when she attacked him with a kitchen knife. She was arrested.

We were able to acquire the contents of her cell phone and we provided Defense council with a report outlining a pattern of abusive behavior by my client's ex-husband.

The Case ended in a Null process by The State. This is typical of cell phone cases where a forensic reconstruction of events can resolve conflicting evidence.