McCann
INVESTIGATIONS
Information | Insight | Influence

Case Study: Mobile Device Forensics in Texting and Driving Cases

Company Profile

McCann Investigations is a full service private investigation firm providing complete case solutions by employing cutting-edge computer forensics and traditional private investigative tools and techniques. For 25 years, McCann's investigators have worked in the public and private sector encompassing law enforcement, physical and electronic security and computer forensics.

McCann works with law firms, financial firms, private and public companies and individuals in cases including contentious divorce, child custody issues, fraud, embezzlement, spyware/malware detection, civil and criminal background investigations, and due diligence.

McCann Investigations tools include:

- Computer Forensics
- Mobile Device Forensics
- Spyware/Malware Detection
- Network Breach Detection
- Digital Debugging
- IT Network Vulnerability Assessments
- Background Investigations
- Under Cover Work
- Surveillance
- Corporate Intelligence
- E-Discovery

Business Situation

Mobile devices have become the main communication device used with many people preferring to text rather than have a phone conversation. Texting, and other forms of distracted driving such as talking on the phone or surfing the web have been the cause of many accidents resulting in fatalities. Statistics show that more than half of drivers under the age of 35 text while driving. Texting while driving has surpassed driving while intoxicated as the number one killer of teenagers, with almost half of teenagers admitting to being in a car while the driver is texting.

A Texas personal injury lawyer presented a case to McCann Investigations regarding one of its clients who was the driver in a car accident which resulted in the death of another driver. The client swerved into an oncoming lane of traffic hitting another car head-on, killing the driver instantly. The client is facing vehicular homicide charges.

McCann Investigations was contracted to image the data on the client's phone to prove that the client was not texting or using the phone at the time of the accident. The client claims that texting did not contribute to the accident itself, although the client did send and receive several texts prior to the accident. The client also claims that the mobile device was on, but was on the passenger seat.

A computer forensics examination of the mobile device will determine whether or not the device was in use at the time that the accident occurred. In most cases, even if the data is deleted, it can be recovered by a computer forensics expert.

Technical Situation

McCann Investigators received the client's iPhone 4S and performed an in depth computer forensics examination. McCann investigators focused on text messages, emails, call history and web browsing that took place around the time of the accident. The mobile device was imaged which essentially created a "snap shot" of all of the data on the phone at that specific point in time. This snap shot determined whether or not the mobile device sent or received texts at the time of the accident. This investigation also determined if the user was on the phone or surfing the web at the time of the accident.

The following are the types of devices that can typically be imaged for recoverable data:

- Smartphones - iPhones, Android, Blackberry, Microsoft Windows Mobile, Symbian
- Mobile phones - standard phones such as CDMA, TDMA, GSM
- SIM cards contained in mobile phones
- Removable flash storage contained in mobile devices
- Tablet devices - iPad, Android tablet, Microsoft tablet
- Other mobile devices - PDA devices, GPS devices, iPods, Palm Pilots, digital cameras, digital video recorders, digital audio recorders, MP3 players, flash storage devices, 2-way pagers

Mobile device operating systems are not as standard or stable as computer operating systems, so locating and reporting on data is more difficult and time consuming than on a Mac or PC.

While recovering deleted data from a smartphone is successful in most circumstances, there are problems that can arise in the imaging process:

- **Standard Imaging Protocols** - Mobile devices should follow standard forensic imaging protocols to avoid data being changed, written or updated on the devices.

    - An incoming phone call could cause an older call log entry to be overwritten potentially spoiling the state of the evidence.

    - The same can be true about allowing the mobile device to send or receive text messages, MMS, phone calls, emails, application updates, etc.

    - Methods to prevent this include cloning the SIM card for GSM devices to prevent network access and only powering on the device in a "stronghold box" or "Faraday Bag" which prevent any types of wireless, cellular, Bluetooth, Wi-Fi or phone carrier signals from reaching the phone.

- **Advanced Security Settings -** Some newer devices prevent any type of access to information without the passcode.

- **Self-Destruct Mode -** Some devices have the capability to securely erase themselves if the wrong password is entered too many times.

- **SIM Card Passwords** - Most SIM cards have hardware based password control that can lock out the card after too many wrong passwords. (Locked SIM cards can sometimes be unlocked with help from mobile provider by providing a SIM carrier specific PUK code.)

- **Remote Self-Destruct** - Allows self-destruct commands to be sent remotely by Blackberry or Exchange server administrators. (This is another reason to be sure specially trained forensic experts with the proper equipment handle the mobile devices.)

While permanently wiping data from a smart phone is possible, the average user typically is not tech savvy enough to accomplish this. In most cases, a computer forensics examiner will be able to recover deleted data.

Solutions

Mobile Device Forensics

Utilizing mobile device forensics, McCann Investigators were able to extract data and determine whether or not the mobile device was in use at the exact moment of the accident. The imaging of the mobile device extracts data, including anything that has been deleted. A determination can be made as to what activity took place on the mobile device during a certain time frame. This activity can include texting, emailing, web surfing or talking. Any one of these activities can distract a driver and therefore the focus was to determine if these activities were taking place and if they could have contributed to the accident.

Products and Services Used:

- Computer Forensics Expert – Licensed Private Investigator in the State of Texas with certification in computer forensics.
- Oxygen Forensic Suite – Leading software application to forensically image Smartphones.

Conclusion:

Texting and driving continues to increase, and with this increase comes more automobile accidents resulting in fatalities. A mobile device leaves an electronic trail and evidence as to what was occurring at the time of an accident. This "snap shot" of that point in time reveals all activity and is key evidence in a criminal case. Only a licensed computer forensics expert can extract this data in a forensically sound manner that maintains the integrity of the evidence to be presented in a civil or criminal matter. In this case, McCann Investigations was able to submit evidence that showed the activity.

The data gathered through mobile device forensics provided the client with the evidence needed to prove no fault in the accident.