The Importance of Understanding the Latest Techniques in Mobile Forensics

LORMAN®

Published on www.lorman.com - January 2018

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

The Importance of Understanding the Latest Techniques in Mobile Forensics

Overview

Collecting evidence at crime scenes has changed as technology has entered everyday use. First responders at a scene don't just scan for weapons and dust for fingerprints. They look for items like mobile phones and iPods. These devices can contain clues that could lead to the apprehension of a suspect in a crime.

A cell phone was the hero in one homicide case where the perpetrator inadvertently hit the speed dial for his wife's cell phone while he was committing her murder. The victim's voicemail recorded the entire incident, including the husband's violent threats.

Mobile phone evidence is so prevalent, the National Institute of Justice, an arm of the U.S. Department of Justice, constantly publishes its testing of programs that can take the data from mobile phones and convert it into useful evidence. These test results are available at https://www.ncjrs.gov/publications.

The National Institute of Standards and Technology has also published "Guidelines on Cell Phone Forensics," sponsored by the Department of Homeland Security. This publication can be found at http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf and contains useful information about how organizations can and should implement standards for cell phone seizure and evidence gathering.

The advent of smart phones has led to widespread use, and the likelihood of finding a mobile phone at a crime scene is high. Professionals at all levels need to increase their knowledge of how cell phones can be used as evidence gathering devices. Lawyers, security professionals and law enforcement personnel need to know the ins and outs of proper handling of these devices.

For example, some cell phones require continuous power in order to seize data. The requirements and functions of different cell phones is an important resource for all law enforcement professionals. In addition, attorneys need to become well versed on how data from mobile devices is being used to provide evidence for proper client defense.

Since smart phones operate like mini-computers with access to the Internet, emails, Internet usage, memos, calendars, phone numbers, address books and credit cards numbers are commonly stored in the memory. Another factor that makes mobile phones so useful is the way they store information. Even if the user has deleted information, it may still be in the phone's memory cache. This is due to the fact that cell phones retain information in blocks and don't delete information until the blocks are full.

When collecting forensic evidence from a mobile phone, it is important not to alter the data in any way. It is not as simple as attaching a cable and extracting the data, as this may not always collect all the data and may alter or delete digital evidence. More complex methods must be used.

Many mobile phones use a SIM card to establish a network ID. SIM cards also contain subscriber information and other data inimical to each particular phone. Sometimes SIM cards contain useful evidence.

Mobile Device Evidence

The type of data that can be retrieved from a mobile phone consists of the phone date and time, address book, memos, to-do lists, call register, photographs, A/V. maps, GPS points, voicemail, text messages, stored files, synchronized computers, online accounts, e-mail, social networks, alternate messaging systems, store accounts, purchased media, habitual cell tower use, subscriber ID, SIM card ID, last dialed number, dialed locations.

Being able to establish location using a mobile phone can be useful. Sometimes alibi's can be established using a phone's ability to create files of recently visited cellular towers. Phones with GPS mapping may also render clues about past travel, and digital photos with time and date can also establish time and location.

What Mobile Forensics Specialists Do

Mobile forensics has created several roles related to the capture, collection and storage of data from mobile devices. First responders are trained to be first at the scene. They assess the area for mobile devices and are informed on the level of response required. First responders secure the scene, get additional support if necessary, and collect mobile evidence.

Mobile forensic investigators manage mobile device capture, analysis and reports. They are responsible for ensuring that protocol is followed, forming conclusions from available evidence and informing officials of the results of the investigation.

Digital technicians follow the orders of the mobile forensic investigator. They usually help with collecting serial numbers on mobile devices and with capturing and documenting data immediately available on the mobile device. Typically several technicians will be deployed at an incident.

Evidence custodians protect and store the data in one location. They gather evidence from the technicians, makes sure it is properly identified, and handle documentation of mobile device transfer of custody.

Mobile Device Examiners capture and copy images and data from mobile devices. The examiner makes data visible

as evidence and also employs various software and hardware to recover hidden or erased data.

Mobile Device Forensics and Technology Law

Mobile device forensics is one area of technology law that is at the cutting edge of client defense. For example, if your client has been charged with securities fraud or insider trading you can use mobile device evidence to prove that your client was traveling in his car or that he had his photo taken at a gathering when an electronic transaction took place.

How Lawyers and Mobile Device Examiners Work Together

In order for the data from a mobile device to be entered into evidence, the collection techniques used must protect the integrity of the data and follow strict legal guidelines. If a client chooses to surrender a mobile device in order to gather evidence, a mobile device examiner can ensure the data is collected properly and lawfully.

However, even surrender of a device can prove problematic. Constant processing of new data with continued use of a device can erase important data from the device memory. If you instruct a client to turn off a device in order to collect data important to their defense, this could cause loss of data stored in RAM memory. For mobile devices seized under other circumstances, turning the device off or allowing it to lose power will generally activate password protections. It is important to collect device chargers and energy cables whenever possible. Even when a mobile device receives power for data collection purposes, it must be isolated from service networks to prevent overwriting of data.

Once a device has been isolated from the network, it locks in the time of seizure or surrender and prevents the device from receiving phone calls and from being remotely erased. Methods for isolating mobile devices from network communication include extraction cases that block radio frequencies, signal jamming systems or shielded rooms designed for mobile device examination. In many cases, however, the first responder must act quickly to document information on mobile devices by capturing what can be immediately accessed on the device. This is usually done only in cases where time is of the essence.

Photographs or videotape are the customary forms of accessing data. A mobile device examiner can verify that the captured data has not been altered in any way and that the steps taken can be repeated and supported by industry-wide standards. The examiner knows to generate documentation that also indicates the possession and control of the device and documents whenever it changes hands.

Mobile Device Evidence and the Court

Perhaps the most important information the examiner can obtain from a mobile device pertains to location because this can establish an alibi. Showing that a client's device was linked to a particular wireless network or that a call was placed while traveling between two signal towers, could save a life. Since the information gathered from a mobile device can be of such importance, following protocols for the retrieval of data and storage of mobile devices becomes paramount in winning court cases.

Following privacy laws and being able to establish the reliability of the data are also other concerns courts look to in admitting digital evidence from mobile devices.

For example, if a key voicemail is merely recorded on a tape recorder, rather than properly retrieved from the memory of a cell phone, the opposing party could easily dispute the recording and request examination of the original voicemail. If the voicemail was not captured from the memory, it could easily be lost from the phone and thrown out as evidence.

The key to sailing through court issues on privacy matters involves not violating the reasonable expectation of privacy rule. These days some people think that their cell phone calls and other mobile device interactions may be monitored due to certain requirements of Homeland Security and warrantless surveillance. However, such beliefs are not widespread and cannot be documented as part of the reasonable expectation of privacy rule.

The privacy rule is based on when and where the device use occurred. If it was at the workplace, the expectation of privacy depends on workplace privacy policies. Since 9/11, privacy rules in United States have relaxed compared those of European countries. If you are involved in a case concerning a mobile device owned by a European citizen or European corporation, you could run into the more protective and complex rules of privacy of the European courts.

The range of data the mobile device examiner reviews should be narrowed to only the type of data you need to prove your case, such as voicemail and text messages. However, you may wish to preserve the entire memory of the device for further exploration. To ensure the integrity of the case, you may want one examiner to remove the memory and another to review the particular data you need. If you need to retrieve and examine more data, you can use the previous data to justify this.

The reliability and experience of your mobile device examiner is of primary importance in winning your case. The data retrieved must follow standard forensic techniques which can prove that it was not altered and that the retrieval method has been documented and can be replicated.

Examples of Mobile Device Evidence

Recent mobile device evidence that has helped apprehend suspects is the text messages and phone calls between a pastor and his au pair who plotted to murder the pastor's wife. Although the notorious pair deleted their anonymous text messages, they were recovered from the cell phones' memories by the diligent work of a forensic examiner.

Another case involved the panicky emails a burglar left his girlfriend as he fled the vicinity of one of his burglaries. "Just trying to find a way out of this neighborhood without getting caught," he wrote, after an eyewitness identified him on the scene. "Cops know I have a blue shirt on," he concluded. The accused refused to admit guilt for the crime, but when confronted with the emails, made a deal with prosecutors for the crime and several others.

The Pluses and Minuses of Network Devices

The fact that mobile devices can be connected to a network has both pluses and minuses for the forensic investigator. A networked mobile device can be remotely accessed, and data can be erased, destroying the evidence. Service providers can also erase lost or stolen devices from their call centers.

On the other hand, mobile devices that have been synchronized with a computer will have information in files that have been backed up. In addition, service provider records can contain historical information no longer on the device. All of this can lead to evidence that can be helpful in solving a case or defending a client.

Social networking clues left on a mobile device can be particularly helpful in establishing a user's relationships and contacts. Digital forensics on mobile devices in Medford, Oregon enabled evidence gathering and arrests on over 20 drug dealers. Digital evidence included digital photographs of individuals dealing or enjoying drugs.

It is particularly important that first responders are thoroughly trained in mobile device collection techniques. Most first responders will properly collect a cell phone, but unless they are properly trained, they may not know to carefully comb the

area for microSD cards. These tiny cards can store huge amounts of data and can be easily concealed, consumed or destroyed. They may contain text messages, data backups or other important items from the mobile device. The mobile forensic expert can note the serial number, make a copy of the microSD card using an adapter and explore the data.

How Mobile Forensic Examiners Acquire Data

Data acquisition from non-protected phones is relatively straight forward. Logic -based software can read SIM cards and PIM data. Deleted data that cannot be captured through logical means can be acquired using hardware, such as the Joint Test Action Group test interface (JTAG) or by reading the memory on the device using Will05 once it has been removed.

Obstructed mobile devices are more difficult to access. These are devices where identity modules are missing, PINs or passwords are needed or the phone has a security lock. The forensic examiner will usually experiment with an identical phone to find ways to access the data on a seized phone to avoid affecting important data.

When a forensic examiner encounters a locked device, they first take most direct route and ask the suspect for the information. The crime scene or the suspect's wallet or briefcase may have also yielded notes with password information. Personal user information can also be given to forensic examiners by the service provider or may be retrieved online through service provider web pages.

Experienced mobile device examiners know the weaknesses of particular devices. For instance, certain model Motorola phones have a default security code in addition to a user-defined phone lock. If the user forgets the phone lock, the default security code gives them access to the phone. Being universal in nature, it also gives the examiner access to the phone.

Software Techniques to Access Devices

When the above methods fail, the forensic examiner will usually use software to break through identification blockers. This software is inimical to specific mobile device models within particular classes. Certain palm pilots, pocket PCs, Nokia and GSM-based mobile phones respond to a reverse algorithm. A substitute SIM card can also be created for certain phones that fools the phone into thinking it is operating on the original SIM device.

Service provider records or memory retrieval can provide the necessary ICCID or IMSI values necessary to create a SIM card that can fool the phone. Ersatz SIM cards come in handy when the examiner needs to unlock a phone quickly, if the

examiner does not have access to radio isolation, or if the examiner wishes to avoid all possibilities of the original SIM card being altered in any way during examination.

In cases where the SIM card has been removed from a phone, it can often be a mistake for a forensic examiner to insert the wrong type of SIM card into the device. Unfortunately, text messages and call logs are linked to the last used SIM card and inserting a different card will erase this important data from the phone or copy memory from the new SIM card.

Idiosyncrasies with each device can be the key that unlocks the device memory. Some manufacturers build in functions that allow access to cell phone memory beyond authentication protocol for diagnostic purposes. The memory contains important data and may also show passwords or phone locks.

Depending on the operating system for a particular device, bootloaders can also access the memory. Bootloaders kick in when a mobile device first activates. Cell phones, PDAs and Linux supported mobile devices respond to bootloaders that can copy the memory of the device to a memory card.

Hardware Techniques to Access Devices

Many mobile device manufacturers provide hardware access points on the circuit board. JTAG components are fairly common on device circuit boards and can be communicated with via software and a controller that returns signals and data from the JTAG component. If an examiner faces an obstructed device, the JTAG method can override locks or access a damaged device.

Memory chips are another route to the memory of a mobile device. The Netherlands Forensic Institute has created a tool that can read and copy memory chip contents on the circuit board. If that tool is not available, devices can be dismantled, and the circuit board can be heated to dislodge memory chips and read them with a conventional memory chip reader.

The built in memory from the ROM of a mobile phone can reveal vulnerabilities in a seized device. For instance, it is possible to replace an authentication program with a replicated version that unlocks the phone every time. It is also possible to monitor the dialog between a phone and a password-protected memory card using an interface. In this way, the password used by the phone to access the card is exposed. The password can then be entered into the phone to access the contents.

When all else fails, there is always systematic entry of possible passwords. The Netherlands Forensic Institute created an automatic password system with a robot arm and video camera that continuously enters keyboard combinations into mobile devices until the password is found.

The Forensic Examiner's Report

The report generated by the mobile device examiner contains a description of the equipment and software used to examine the mobile device plus the steps taken to access the data on the device. Reports are quite detailed and include string searches, image searches and recovery of deleted items. Copies included with the report commonly include printouts of evidence, digital copies of data, and documentation relating to device custody. Data analysis includes Internet activity, communication logs, text message review, methods used to hide data, and report conclusions. The examiner also usually includes a copy of any software used so that the process used can be easily replicated.

The Need for Established Standards

Although no worldwide standard for the collection of mobile device evidence exists, law enforcement authorities in the United States, working in conjunction with Homeland Security, have been steadily establishing protocols. As more and more cases are solved using evidence gathered from mobile devices, the awareness of the importance of mobile device evidence continues to grow, making forensic examination and collection standards a high priority. Professionals in the fields of security and law need to become educated about the role that mobile device evidence can play.

Since the mobile device industry continuously evolves, law enforcement personnel involved in mobile device seizure should seek to update their training regularly. Forensic examiners of mobile devices must continually educate themselves of changes in the industry so they can adapt themselves to new methods of accessing the new devices that are brought to market each year.

Sources:

http://www.strozfriedberg.com/files/Publication/224ca0f8-5101-4e1b-938a-4d4b128ad5ed/Presentation/PublicationAttachment/ef4a28ad-ff7d-4014-aea8-80505789b86c/Mobile%20Device%20Forensics_%20A%20Brave%20New%20World.pdf

http://www.elsevierdirect.com/companions/9780123742681/Chapter_20_Final.pdf

http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf