Information Security Journal: A Global Perspective, 21:159–168, 2012

ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393555.2011.654317

Taylor & Francis
Taylor & Francis Group

The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations

David Bennett
Computer Systems Management, Westminster, Maryland, USA

ABSTRACT The paper deals with the various types of mobile devices that have large storage capacities and the challenges for forensics experts in gathering information from the devices for use in criminal investigations. The paper describes various forensics tools, law challenges for the forensics examiner such as the Fourth Amendment, and chain of custody issues that a forensics expert could endure while gathering information from mobile devices. The reader will learn about the struggles to effectively manage digital evidence obtained from such mobile devices and some of the issues in using some of the more popular tools on the market to conduct forensics. Finally, the reader will conclude the various challenges that could occur for the forensics examiner in conducting investigations until law disputes are resolved and the maturity and standardization of software tools develop.

KEYWORDS legal, regulations, compliance and investigations, information security and risk management, mobile device, computer forensics, digital forensics, law

There are a number of electronic personal devices labeled "mobile devices" on the market today. Mobile devices include cell phones, smartphones such as the Apple iPhone and Blackberry, personal digital assistants (PDAs), and digital audio players such as iPods and other MP3 type devices. Laptop computers, tablets, and iPad products are not typically classified as mobile devices today as they are not small enough to be considered handheld; however, future technologies will lead to even smaller and more portable devices that can fit in the palm of your hand. More recently, for example, marketing has led to tiny tablets such as the LeapFrog LeapPad Explorer tablet marketed to consumers in late 2011, specifically designed with applications for children that makes a better choice for smaller hands. Although this research does not single out laptops and tablets, it is important to note that often these devices have common operating systems and interfaces that would require many of the same

Address correspondence to David Bennett, MS, Computer Systems Management, 869 Four Seasons Road, Westminster, MD 21157. E-mail: dbennett8@comcast.net

challenges. Today, the ever popular smartphone comes with storage capacity similar to a laptop while commonly utilized as a portable office, social network, and entertainment center all rolled into a solitary, convenient device. A smartphone is a mobile device that provides advanced computing and offers the ability to run mobile applications with more connectivity options than a cellular phone.

Technological and storage capacity for mobile devices has grown exponentially. Over the last decade, capabilities and features of mobile devices have turned them into data repositories that can store a large amount of both personal and organizational information. Unfortunately, criminals have not missed the mobile device information revolution. Within the past few years, they have increasingly been using mobile phones and other handheld devices in the course of committing criminal acts. For example, a drug dealer may keep a list of customers who owe him money in a file stored on his handheld device, or a child pornographer could keep nude images of underage children engaging in sexual activities on a mobile device for the purposes of trading photos or video files with other pedophiles. Almost every class of crime can involve some type of digital evidence from a device that is essentially a portable data carrier. This increases the potential for incriminating data to be stored on mobile devices and to be utilized as evidence in criminal cases. Can valuable information be obtained from a mobile device to assist in a criminal investigation? What are the challenges a forensics investigator faces in obtaining information from these devices?

Mobile devices can contain such electronic records information such as electronic mail, word processing files, spreadsheets, text messages, global positioning system (GPS) tracking information, and photographic images that can provide law enforcement personnel with essential evidence in a criminal investigation. A mobile phone's ability to store, view, and print electronic documents is easily utilized from a single hand-held device with the processing power and the storage capacity similar to a bulky laptop (Al-Zarouni, 2006, p. 1).

NEED FOR MOBILE FORENSICS

Mobile device forensics is the process of recovering digital evidence from a mobile device under forensically sound conditions and utilizing acceptable methods. Forensically sound is a term used in the digital forensics community to justify the use of a particular technology or methodology. Many practitioners use the term to describe the capabilities of a piece of software or forensic analysis approach (McKemmish, 2008, p. 3). Mobile devices vary in design and manufacturer. They are continually evolving as existing technologies progress and new technologies are introduced. It is important for forensics investigators to develop an understanding of the working components of mobile devices and the appropriate tasks to perform when they deal with them on a forensic basis. Knowledge of the various types of mobile devices and the features they possess is an important aspect of gathering information for a case since usage logs and other important data can potentially be acquired using forensics toolkits.

Mobile device forensics has expanded significantly over the past few years. Older model mobile phones could store a limited amount of data that could be easily obtained by the forensics investigator. With the development of the smartphone, a significant amount of information can still be retrieved from the device by a forensics expert; however, the techniques to gather this information have become increasingly complicated.

The demand for mobile device forensics stems from mobile phones being employed for such functions as to store and transmit both personal and corporate information. The use of mobile phones in online transactions such as stock trading, flight reservations and check-in, mobile banking, and communications regarding illegal activities that are being utilized by criminals has created a need for mobile device forensics. While it took decades to convince legitimate businesses that mobile devices could increase sales, communications, marketing, and other improvements to their operation, crime organizations were well aware of the substantial benefits that mobile phones could provide (Mock, 2002, p. 1). Law enforcement and forensics investigators have struggled to effectively manage digital evidence obtained from mobile devices. Some of the reasons include:

- Mobile devices require specialized interface, storage media, and hardware.
- File systems that are contained in mobile devices operate from volatile memory or computer memory

that requires power to maintain stored information versus nonvolatile memory devices such as standalone hard disk drives that do not require a maintained power supply.
- The diverse variety of operating systems that are embedded in mobile devices.
- The short product cycles from the manufacturers to provide new mobile devices and their respective operating systems are making it difficult for law enforcement agencies to remain current with new technologies.

So how do mobile devices such as Blackberry, Apple's iOS, and Android compare for security? Currently, there is no clear answer to this question. Blackberry devices, unlike Android and iOS, sync their data via a centralized system owned and operated by Research in Motion (RIM), which can create a single point of failure and act as a prime target for attackers who may want access to sensitive data that is synced over a network. In addition, the passcodes on Blackberry devices are considered limited as is the ability to circumvent this authentication method; however, iOS devices suffer from this same passcode security risks but are only present on a few Android devices. Nearly all files encrypted on iOS are recoverable. This is possible because the encrypted files on an iOS device can be decrypted even if the device has a passcode. An iOS can provide an additional layer of encryption for files that implement the Data Protection application programming interface (API) and utilizes the device passcode as a component of the encryption keys. This can create a challenge for forensic examiners where simply bypassing the passcode will not recover the data. The Data Protection API is only applicable if the applications developer chooses to enable this feature so most third-part applications, Web cache, and other system data are usually recoverable.

In most cases, a passcode is not an effective method to prevent someone from recovering device data although it is an important security measure that makes accessing data more difficult for the casual device thief. A major exception to this, however, is the removable secure digital (SD) cards that exist on an Android or Blackberry device and can contain unencrypted images or other data. This card can easily be removed by a casual user with little or no technical skill to view email attachments that have already been downloaded or viewed by the user, thus displaying a significant data exposure.

FORENSICS TOOLS

A few of the more well-received commercial off the shelf (COTS) products and open source applications available to the forensics community are reviewed below; however, no recommendations are made or implied.

One of the most emerging commercial products is the Cellebrite Universal Forensics Extraction Device (UFED) Forensic System, a standalone mobile forensic device utilized both in the field and in the research lab. The UFED device supports most cellular device interfaces including serial, USB, infrared, and Bluetooth and can provide data extraction of content such as audio, video, phone call history, and deleted text messages stored in mobile phones. The Cellebrite product is popular with investigators because it works well with the Apple iPhone, and the acquisition methods can recover a significant portion of the data on the iPhone device. The firmware, which is used to run user programs on the device, is updated often enough to support new mobile devices and its functionality for the forensics examiner.

Paraben Corporation's Device Seizure product is another COTS forensic acquisition and analysis tool for examining more than 2,200 handheld devices including cellular phones, PDAs, and GPS devices. In addition, Device Seizure is designed to support the full investigation process and can perform physical acquisition through a data dump in its ability to recover deleted files and other information. The Device Seizure product, according to many experts in the forensics area, is considered shelf-ware and often will not perform as marketed (R. Mislan, personal communication, February 11, 2011).

Final Data's Final Mobile Forensics product is another product and is specific to Code Division Multiple Access (CDMA) mobile phones. CDMA phones were first launched commercially in Hong Kong in 1995 and are now currently utilized by major cellular carriers in the United States as an alternative to Global System for Mobile communications (GSM) technology. To help gain perspective, the wireless world is divided into GSM (standard outside the United States and used inside the United

States by AT&T and T-Mobile) and CDMA (standard in North America and parts of Asia). While there may never be a single standard technology worldwide, GSM is used in 219 countries and territories serving more than three billion people and providing international travelers the broadest access to mobile services (Moore, 2006, pp. 3–5).

Another type of product, a flasher box, is available but not recommended as a substitute for one of the above-mentioned automated COTS products because it is not always reliable. Flasher boxes are not designed for forensic work but can help recover data that is not readily available. Flasher boxes should never be used as a first response. They are considered a dangerously intrusive alternative and should only be utilized by trained or highly experienced investigators for their use in controlled environments as they can be technically challenged and complicated to use. Although flasher boxes do not require any software to be installed as with other forensics toolkits, modifications to the data can occur easily through incorrect use, thereby leaving the evidence tainted and deemed useless to a criminal investigation. Flasher boxes are not usually documented by any best practices or principles; therefore, there are no simple methods to determine if they do preserve evidence in the mobile device's memory and no guarantee that flashers will work in a dependable manner.

Some examples of open source products that are freely available for download but limited in features when compared to commercial products include BitPim, a program that allows the user to view and manipulate data on many CDMA phones; Smelter for use on Siemens brand mobile phones; and ChipIt used to explore GSM Subscriber Identity Module (SIM) cards to view and copy a mobile device phone book. Although open source products such as the aforementioned ones are heavily adopted and easily available to the forensics investigator, there are many issues that arise such as timely updates to the software and limited functionality, and quality assurance testing of the software has been known to be problematic (Moore, 2006, pp. 3–5).

Information is stored in the mobile phone's internal memory. Pertinent data such as call histories are stored in proprietary formats in locations that will alter that data according to the phone model. Even the cable used to access the mobile device's memory will vary according to manufacturer and model. Many examiners look at the SIM cards, which store personally identifiable information (PII), cell phone numbers, phone book information, text messages, and other data for valuable information because it is typically stored in a standard format; however, the limited storage capacity of a SIM card forces the majority of the data to be stored on the phone itself.

Unlike traditional computer forensics on a desktop or laptop computer where the investigator would simply remove the hard drive, attach to a write blocker device thus allowing acquisition of information on a computer hard drive without creating the possibility of accidentally damaging the drive contents and image the hard drive in order to fully analyze the data; the process to extract information from a mobile device is more complicated. There are a number of complex mobile forensics software applications to assist in the removal of data that are available to the forensics community. However, the lack of a leading edge tool and decreasing budgets for acquiring the tools are an ongoing problem (Mislan, 2010, pp. 1–3). Since no single tool comes highly recommended by the forensics community, it is often desirable to use a range of software tools to acquire the data, thus increasing the budget needed to acquire the appropriate tools. The software tools available are expensive and law enforcement agencies are operating under restricted budgets and fixed resources.

MOBILE DEVICES

ComScore, a marketing research company that provides digital marketing intelligence for Internet businesses, estimate that roughly 63 million smartphone subscribers are in the United States. The Blackberry device leads the pack with 31.6% of the market; Google's Android, 28.7%; and Apple's iPhone, 25%. ComScore data states that 234 million Americans ages 13 and older used some type of mobile device in December 2010; however, the more interesting data are the mobile content usage in December 2010. The data estimate that 68% of U.S. mobile subscribers used text messaging on their mobile device, Web browsers were used by 36.4%, and mobile applications usage was 34.4% (ComScore Web, 2011).

An example of one of the fastest growing smartphone devices is the iPhone from Apple Inc., which debuted in January 2007. There are entire books dedicated to the operating systems for the Apple products

as well as the development of applications for them. Like most electronic devices, the iPhone is a collection of modules, computing chips, and other electronic components from various manufacturers making it difficult to utilize a "one size fits all" forensics software application as a staple for the forensics process. In fact, this is true for most mobile devices on the market. There does not seem to be a single vendor that is the emerging leader in forensics toolkits. Often, as is the case with the popular iPhone, forensics investigators are relying on the hacker community for assistance in analyzing mobile devices (R. Mislan, personal communication, February 11, 2011).

Today's mobile phone devices have a large storage capacity and a wide range of applications and connectivity options available to the user with each telecommunications provider. Mobile device forensics applications and toolkits are relatively new and developers are having difficulty in keeping up with the emerging technological advances due to the revolving door of products from market demand. The forensic tools available are often limited to one or more phone manufacturers with a limited number of devices supported (Al-Zarouni, pp. 2–3).

Regarding standards, the only evaluation document available for mobile phone forensics toolkits is published by the National Institute of Standards and Technology (NIST) (Ayers, n.d., pp. 1–2). NIST and various law enforcement staffs help to develop the requirements, assertions, and test case documents to evaluate the toolkits and to assist in providing guidance in choosing the correct product to fit their needs. The NIST evaluation document contains generic scenarios created to mirror real-life situations that may arise during a forensic examination of a mobile device. The NIST scenarios serve as a baseline for helping the forensics community determine a tool's capacity to acquire and examine data in order to gain a perspective on the correct tools to acquire. The NIST evaluation documents are considered to be an important resource for forensics investigators to maintain quality control and to validate toolkit functionality for mobile device forensics in proper data acquisition and reporting.

Another organization discussing mobile device standards is a forum formerly entitled Open Mobile Terminal Platform (OMTP) and now called the Wholesale Applications Community (WAC) that has been created by mobile network operators to discuss and formulate standards with manufacturers of cell phones and other mobile devices. The goal of the WAC is to encourage open standardized technologies and allow developers to deploy applications across multiple devices and operators through the use of the standard technologies. The WAC has published some requirements for the support of advanced SIM cards and mobile device security but has mostly received broad support from European mobile device operators.

It is no simple task to try and create standards for such a varying group of device manufacturers that utilize proprietary circuits and do not seem to agree on a communications standards so the forum has had limited success in the United States. Apple has already stated it will not join any standards. The outcome of the WAC will likely be a broad set of guidelines that will be adopted inconsistently by manufacturers. It would be prudent for the government to support open standards in order to lower the cost for law enforcement forensics investigators to recover data for investigations and to choose the appropriate tools to utilize.

There are many devices that are cheaply manufactured in China and are very difficult to perform forensics by examiners. The primary reason is that inexpensive Chinese cell phones are unbranded, meaning they have no International Mobile Equipment Identity (IMEI) number and therefore cannot be traced. The phones are attractive to criminals and terrorists who often utilize the cell phones for activities such as detonating bombs without being detected. A unique IMEI number is required for all GSM phones. This number allows a signal tower to identify individual cellular handheld devices in a service network which in turn helps the military and law enforcement establish the location of the phone (Moore, 2006, p. 5). With an unbranded phone, the absence of the IMEI number makes it impossible to track these mobile devices, making the Chinese-made phones attractive to criminals and terrorist organizations alike.

The United States Armed Forces has found an abundance of the Chinese-made cell phones in theater while in the Middle East. The India government has banned the Chinese-made cell phones from entering the country; however, these low-cost phones have penetrated into Pakistan and other developing markets. This is proving to be a serious security issue for American troops stationed in the Middle East. There is much exploration to be conducted in the area of these devices as China is one of the world's largest and fastest growing markets for inexpensive and unbranded

mobile devices. The investigative world knows little about the design, make, manufacturers and behavior of these mobile devices.

LAWS

Forensics evidence is only as valuable as the integrity of the method that the evidence was obtained. The methods applied to obtain evidence are best represented if standards are known and readily established by the digital forensics community. The Fourth Amendment limits the ability of government agents to perform search and seizure evidence tactics without a warrant, including computers (charters of Freedom).

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fourth Amendment question that typically comes up in digital evidence cases asks whether an individual has a reasonable expectation of privacy having electronic information stored on electronic devices under that individual's control. Computer evidence can present a challenge for both prosecutors and defendants alike. A guide to offering mobile device data as evidence is beyond the scope of this research, but a few examples of some digital forensics issues in real life situations are described below.

A legal issue in presenting evidence is the "best evidence rule," which states that to prove the contents of a document, recording, or photograph, the "original" document, recording, or photograph is ordinarily required. For example, in *United States v. Bennett 2004*, a federal agent testified about information that he viewed on the screen of a GPS on the defendant's boat in order to prove he had imported drugs across international waters. It was decided the agent's testimony violated the best evidence rule because he had only observed a graphical representation of data from the GPS instead of actually observing the professed path the boat had been following during the encounter. Since the United States sought to prove the contents of the GPS, the best evidence rule was invoked and required the government to present the actual GPS data or printout of the data rather than the testimony from the federal agent (Open Jurist Web, 2004, pp. 1–2).

In 2010, a Japanese sumo wrestling match-fixing scandal was brought to light 0after investigators analyzed data left on 50 cell phones seized from wrestlers of the Japan Sumo Association (JSA) while probing a baseball scandal in that country. The Japanese police were able to retrieve and restore electronic mail messages previously deleted from the mobile phones, including messages exchanged among wrestlers who were being implicated in the wrestling bout-rigging case. The sumo wrestlers refused to turn over their mobile devices to law enforcement claiming their phones were damaged due to water or the battery had died in the phones. The case is still ongoing in Japan, but members of the JSA plan to obtain data left on the cell phones utilized by the suspected wrestlers to restore deleted email messages in order to prove the case against the sumo wrestlers. Even if deleted, the cell phone email data remain in binary format on the handheld device's memory. This is called data remanence or the residual representation of data that remains after attempts have been made to remove or erase the data. Through digital forensics, even mobile devices that have been ruined or immersed in water can still recover data unless the device's memory chips are destroyed (Yomiuri Online Web, 2011).

Like digital evidence from a computer, it is necessary to have proper legal authority in order to perform a forensics investigation of cellular telephones and mobile handheld devices. An exception that is supported by case law (*U.S. v. Finley 2007; U.S. v. Carroll 2008*) allows a search "incident to arrest" and is often connected with searches of arrestees and motor vehicles. For example, in *U.S. v. Finley*, it was noted that the defendant in the case "had conceded that a cell phone was analogous to a closed container" for the purpose of Fourth Amendment analysis (Cyb3rcrim3 Web, 2009). Such searches are allowed by the court to be performed for the preservation of evidence that could easily be altered or damaged. This exception for handheld devices is restricted by a limited period of time and, according to law, may be searched without a warrant only if the search is "substantially contemporaneous with the arrest" (*U.S. v. Curry D Me. 2008*) (Lewis, 2009, p. 2).

The authors of the Fourth Amendment could not have envisioned the powerful technology of today's electronic age and courts have only begun to answer

difficult questions that are being introduced through the use of these devices. Current Fourth Amendment doctrine and precedent cases suggest that the U.S. Supreme Court would consent to invasive searches of a mobile device found on the person of many individuals and has allowed an exception permitting warrantless searches on the grounds that law enforcement should be allowed to look for weapons or other evidence that could be linked to an alleged crime. The Obama Administration and many local prosecutors feel that warrantless searches are perfectly constitutional during arrests (McCullagh, 2010, p. 2).

Privacy advocates feel that existing legal rules allowing law enforcement to search suspects at the time of an arrest should not apply to mobile devices such as smartphones because the value of information being stored is greater and the threat of an intrusive search is much higher, such as personally identifiable information (PII). PII is information connected to an individual including but not limited to education, financial transactions, medical information, and criminal or employment history which can be used to trace that individual's identity such as name, social security number, or birth date. While technologies have evolved over the years, the search incident principle has remained constant.

The Fourth Amendment applies to mobile electronic devices and digital evidence just as it does any other type of criminal evidence. Legally, when handling computers and mobile devices, it is best for the forensics investigator to treat them as they would a closed container, such as a briefcase or a file cabinet. Generally, the Fourth Amendment prohibits law enforcement personnel from accessing, viewing, or examining information stored on a computer or mobile device if the law enforcer would be prohibited from opening a closed container and examining its contents in the same situation. The forensics investigator should always be aware that laws vary state by state and unopened email, unread texts, and incoming phone calls of seized devices may present nonconsensual eavesdropping issues.

In digital media searches, the media are frequently searched off site and in an enclosed forensics laboratory. Generally, courts have treated the offsite forensics analysis of seized digital media as a continuation of the initial search, and the investigator is still bound by the Fourth Amendment. Because this analysis is often treated as part of the initial search, the government bears not only the burden of proving the seizure was reasonable and proper but also that the search was conducted in a reasonable manner. To ensure that search and seizure forensics analysis meets the burden later at the trial, the forensics investigator should generate a written report with clear documentation of the analysis.

CHAIN OF CUSTODY AND PRESERVATION OF EVIDENCE

The goal of a forensic investigator is to obtain evidence utilizing the most acceptable methods, so the evidence will be admitted according to law in the trial. Obtaining a judge's acceptance of evidence is commonly called admission of evidence. Evidence admissibility will require a lawful search and the strict adherence to chain of custody rules including evidence collection, evidence preservation, analysis, and reporting.

According to the International Organization on Computer Evidence, some general principles should be followed in recovering digital evidence for chain of custody:

1. All of the general forensic and procedural principles should be adhered to when dealing with digital evidence.
2. Upon seizing digital evidence, any actions taken should not modify the original evidence.
3. When it is necessary for personnel to access the original digital evidence, the personnel should be appropriately trained for the purpose.
4. All activities associated to the seizure, access, storage, or transfer of digital evidence must be fully and properly documented, preserved, and available for review.
5. An individual is responsible for all actions taken with respect to digital evidence when digital evidence is in that individual's possession.
6. Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with all six principles (ENFSI Working Group, 2006, pp. 17–18).

There are several publications, including those from the U.S. Department of Justice, that do not list any doctrine or principles such as the ones previously mentioned from the International Organization on Computer Evidence. However, many of the points

addressed in the above principles are covered and provide a comprehensive explanation of the forensic process as well as related legal issues in the United States.

As a rule, in criminal court proceedings, the process is often more scrutinized than the actual evidence recovered for a criminal investigation. An important part of the preservation of evidence process is in securing and isolating cell phones and other mobile devices found on-site for transport to the forensics lab for evaluation.

While a mobile phone is powered on, it will search for the strongest signal, usually from the nearest active cellular tower or a tower that enables the device to obtain the best signal. As a mobile device is transported, it will continue to search and adjust to maximize the strength of signal with that tower. The designation of the most recently connected cellular tower is then recorded as a database entry in the file system of the cellular phone; thus, when a mobile device moves to a new area, a new entry will be updated in that database.

The most important step for a first-responder investigator, when arriving at the scene of a crime and identifying a mobile device for possible evidence submission, is to determine how best to preserve that device and its data. Recording and documenting the scene, including photographs of the mobile device in an undisturbed state, should be included. It is recommended to power the mobile device off to preserve the data and battery power. If it is not possible to power the device off in a safe manner, the phone should be protected from cellular phone towers. Aside from locking down the mobile device by either disengaging or maintaining the power supply, the investigator should seize any additional accessories to the device such as SIM and media cards, headsets, charger cables, and cases that could potentially contain evidence.

When a mobile device has been powered off, text messages and other data may queue for delivery when the phone is powered back on and returned to service. The queued messages and data can overwrite old and deleted messages or data once they are delivered to the carrier. Carrier providers may update system files and roaming services when the mobile device is connected to the system. There will also be the potential for corruption of downloaded data as well as the file system of the device during a forensic examination when the system updates are transmitted to the system.

The equipment that works the best is Radio Frequency (RF) shielded test enclosure boxes such as the type from a forensics product vendor such as Ramsey Electronics. The Ramsey boxes ensure the mobile device is isolated from a cellular carrier's network and other RF signals to prevent any incoming or outgoing communications, including GPS tracking.

Another option to transport a mobile device from the crime scene to the crime lab is a Faraday bag. Faraday bags are specially designed RF plastic coated shielded bags used to shield a mobile device from external contact. The bags are coupled with a conductive mesh to provide secure transportation to the laboratory. One issue with Faraday bags is that often a cell phone will continue to search for a signal even while in the protected bag thus zeroing out the register that holds the location data – and making the device useless as an evidence artifact. Yet another issue is the increased activity while in the Faraday bag while the mobile device is powered on that can cause the battery to fail at a faster pace. With the Apple iPhone in particular, it is imperative for the forensic investigator to properly seize the mobile device due to the option of the Remote Wipe feature on the phone. A user can perform this command if the smartphone is connected to the Internet or phone network. If the device is powered off or placed in a Faraday bag, it cannot be remotely wiped; however, once powered back on, the wiping process, if activated, will automatically be invoked.

When choosing a shielding artifact like one of the above-mentioned products, it is important to enable the forensics investigator to utilize the necessary tools to complete the examination and within the shielded area of a forensics laboratory if possible.

CONCLUSION

Mobile device forensics is an ever-evolving field filled with challenges and opportunities when analyzing a mobile device for forensic evidence in support of a criminal investigation. The process can be more difficult than traditional computer forensics due to the volatile nature of electronic evidence. The software applications for mobile forensic testing are often not 100% "forensically sound." A well-trained, highly skilled digital forensics investigator plays an essential role in the criminal investigation process when performing forensics analysis of mobile devices that

belong to suspects, witnesses, and victims or through the analysis of network traffic in response to computer security incidents (Curran, Robinson, Peacocke, & Cassidy, 2010, pp. 1–4).

Although forensics toolkits do exist for the investigator, the majority of the tools are either not fully developed and do not yet provide full functionality for multiple devices. Budget constraints of law enforcement departments prohibit the purchase of quality software packages to use with the varying mobile device manufacturers. The key is for the investigator to use the appropriate toolset that is meant for that particular purpose in performing forensics analysis in an effective manner that will support a criminal case (R. Mislan, personal communication, February 11, 2011).

Even such a pertinent piece of forensics equipment such as the Faraday bag for the first-responder is not free from issue. Once removed from the Faraday bag, a mobile device can start receiving data if powered on and be able to connect to the network. This may be difficult to control for the first responder if he is instructed by a higher official to leave the mobile device powered on upon discovery at the crime scene. Some devices can be controlled by placing the phone in airplane mode, thus disabling the wireless features, but not all mobile devices possess this functionality. For the most part, Faraday bags are reliable but cannot fully guarantee that a signal will not reach the phone. Successfully blocking the signal depends upon the quality of the bag, the distance to the cell tower, and the power of the transmitter in the mobile device.

Another challenge that faces the forensics investigator is digital evidence that is obtained for a criminal investigation can be preceded by a suppression hearing. A suppression hearing is an opportunity for a judge to look at the evidence and determine whether it will be admissible or violates the suppression of evidence which determines if an unreasonable search or seizure violated a defendant's constitutional right. The judge will determine whether the Fourth Amendment has been followed in the search and seizure of evidence. A forensics investigator's knowledge of preservation of evidence rules, chain of custody principles, and the overall legal issues in obtaining digital evidence from a mobile device is vital. It is important for the forensics investigator to stay current on the latest technological tools and laws that deal with admissibility of evidence in order to avoid the evidence carefully obtained being struck down by a proceeding judge. The investigator should always keep up to date on what the latest efforts that criminals are utilizing to combat the forensics process.

Forensic computing continues to play an increasingly important role in civil litigations, especially in electronic discovery, intellectual property (IP) disputes, as well as information security and employment law disputes. Forensics investigators must be aware of certain issues pertaining to data acquisition and the preservation of digital evidence for a criminal investigation. Electronic data are susceptible to alteration or deletion, whether through an intentional change or from the result of an invoked application in some computing process. As electronic data is created, modified, or deleted through the normal operations of a computing system, there lies the possibility of modifications arising from an incorrect or inappropriate digital forensics process. Given that the results of such actions can be treated as critical evidence in a case, it is essential that every measure be taken to ensure the reliability and accuracy of the forensics process. A digital forensics process must be developed and applied with due regard to jurisprudence issues. It is imperative that the digital forensics process is capable of being examined thoroughly to determine the reasonableness and reliability to refrain from being admissible.

REFERENCES

Al-Zarouni, M. (2006, December). Mobile handset forensic evidence: A challenge for law enforcement. Australian Digital Forensics Conference, Edith Cowan University Perth, Western Australia.

Ayers, R. (n.d.). Mobile device forensics – tool testing. National Institute of Standards and Technology (NIST). Retrieved from www.cftt.nist.gov

Charters of Freedom Web Site, Amendment IV, available at: http://www.archives.gov/exhibits/charters/bill-of-rights-transcript.html.

ComScore Web. (n.d.). Retrieved from http://www.comscore.com/Press_Events/Press_Releases/2011/2/comScore_Reports_December_2010_U.S._Mobile_Subscriber_Market_Share/(language)/eng-US

Curran, K., Robinson, A., Peacocke, S., & Cassidy, S. (2010, April/May). Mobile phone forensics analysis. *International Journal of Digital Crime and Forensics*, 2(2)

Cyb3rcrim3 Web. (2009, December 16). Warrant needed to search cell phone. Retrieved from http://cyb3rcrim3.blogspot.com/2009/12/warrant-needed-to-search-cell-phone.html

ENFSI Working Group. (2006). Guidelines for best practice in the forensic examination of digital technology. (December)., pp. 17–18. Available at: www.enfsi.org.

Lewis, D. L. (2009, August/September). Examining cellular phones and handheld devices. *Forensics Magazine*.

McKemmish, R. (2008). Advances in digital forensics IV. *International Federation for Information Processing*. 285, p. 3.

McCullagh, D. (2010, June 26). Police push for warrantless searches of cell phones. CNet Web. Retrieved from http://news.cnet.com/8301-13578_3-10455611-38.html

Mislan, R. P. (2010, July). Cellphone crime solvers. IEEE Organization. Retrieved from http://spectrum.ieee.org/computing/software/cellphone-crime-solvers

Mock, D. (2002, June 28). Wireless advances the criminal enterprise. The Feature Archives Web.Retrieved from http://thefeaturearchives.com/topic/Technology/Wireless_Advances_the_Criminal_Enterprise.html

Moore, T. (2004, April 9). *The economics of digital forensics*. Cambridge, UK: University of Cambridge.

Open Jurist Web. (2004, April 9). Retrieved from UNITED STATES of America, Plaintiff-Appellee, v. Vincent Franklin BENNETT, Defendant-Appellant. http://openjurist.org/

Sklavos, N., & Zhang, X. (2007). *Wireless security & cryptography: Specifications and implementations*. Boca Raton, FL: CRC-Press, A Taylor and Francis Group.

The Yomiuri Shimbun Online Web. (2011, February 9). Data retrieval key to sumo scandal. Retrieved from http://www.yomiuri.co.jp/dy/sports/T110208005743.htm