The Bill Blackwood
Law Enforcement Management Institute of Texas

Digital Forensics and Law Enforcement

A Leadership White Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

By
Fred Klingelberger

Kaufman County Sheriff's Office
Kaufman, Texas
February 2016

ABSTRACT

Ninety percent of Americans own a mobile phone. Sixty-four percent of Americans own a smartphone. Eighty-one percent send or receive text messages, 60% access the internet, 50% download applications, and 49% get directions, or use it for other location-based information (Pew Research, 2014). The opportunity for law enforcement officers to obtain case-solving evidence via digital forensics is vast and needs to harnessed and exploited. Law enforcement departments across the country have to evaluate and weigh the benefits of proper training and budgeting to successfully take advantage of the future in digital evidence imaging and processing. Constraints in time, money, and constitutional law can be circumvented with the proper training and legal precautions. While some of the data collected from a digital device may be considered circumstantial, one cannot refute the added intelligence it offers law enforcement investigators, such as text messages about a crime, photos of a potential witness, or even the location a crime was committed (Casey, 2009). Police departments across the country need to recruit, hire, and train personnel to properly harness the evidence-gathering potential of digital forensics.

TABLE OF CONTENTS

Page

INTRODUCTION

Digital forensics caught the “BTK” killer, Dennis Rader. It took waiting 30 years for technology to catch up to the infamous serial killer via a deleted file recovered from an outdated floppy disk (Hanson, 2006). Instead of a physical fingerprint, which seemed to elude police in the BTK case, law enforcement can harness valuable intelligence from a digital fingerprint. Long gone are the days of the Commodore, the huge desktop contraption, and the ten pound phone-in-a-bag. Today, with the conception of the smart phone, the same desktop computer technology is accessible, and it all fits in the palm of a hand. These facts benefit law enforcement officials because they now have alternative sources for collecting evidence. The creation and use of forensic tools, such as XRY (www.msab.com/) and Cellebrite (www.cellebrite.com/), yields an abundance of data that can be pulled from mobile devices, tablets, and laptops and used as evidence in the prosecution of criminal cases.

These devices often contain evidence related to the planning, organization, or witnessing of crimes, and the information on these devices can be sent to forensic specialists in labs to be processed. It is extremely important for law enforcement officers (LEO) to understand exactly what these devices are capable of and what type of information is available when searching the device carefully, securely, and within the confines of the law. Information used on social media sites, text messages, and even the geographic location where a photo was taken, are all obtainable forms of data. Digital forensics is becoming more popular and developing into an invaluable tool for law enforcement by creating another possibility to collect and develop evidence. Law enforcement should be utilizing digital forensics, specifically data attained from a mobile device, in criminal investigations.

POSITION

Mobile device forensics provides supplementary evidence in an easily presentable format. Often investigators will receive this information verbally and they will not follow up to acquire the hard-copy data. Mobile device forensics will provide a comprehensive report of a person's activity on a device, like date and time stamps and verbatim conversation detail, to name a few (Casey, 2009). Given the population's predilection to continuously stay connected thorough a mobile device, text messages, emails, and social media posts will frequently contain helpful evidence. People tend to be more liberally verbose when they feel protected by an invisible cyber wall. This is also the case with digital photos. Whether the photo is of them or of a crime, it will be stored in their phone and, in most cases, shared via text, Facebook, Instagram, or other mobile phone application. Mobile devices also store data on geographical location. Photographs taken with mobile devices generally have geographical data attached to them. The metadata that the forensic investigator recovers can include the date and time the photo was taken and the GPS coordinates (Casey, 2009). This not only provides the picture of the event, but it also allows one to use a program like Google Maps (https://maps.google.com/) to zoom in on the location the picture was taken. Mapping applications also store geographical data. Forensics can pull a recently visited address, saved locations, and recently traveled routes, which can provide evidentiary value in tracking a possible suspect's movements.

Mobile users often delete texts and photos, thinking that the data is gone permanently. Mobile device applications house a great deal of data. Even if a witness or a suspect says photos or texts were deleted off of a phone, the data is still retrievable (Jackson, 2014). Even data on chat applications, like Twitter or SnapChat, can be

recovered for evidence or intelligence in order to locate victims in a sexual predator case or in an attempt to locate suppliers or customer contact information in a drug case. These applications can provide a great deal of data and case assistance to a LEO if it is procured properly and lawfully using the right digital forensics software by a trained digital forensics expert. When a call log is deleted from a cell phone, the investigator can still recover the data. The data could include details about incoming and outgoing calls, and even missed calls (Casey, 2009). Other evidence that can be recovered from a mobile device is web browsing history and file viewing. This is called data remanence. It is the lingering representation of data that remains after a user attempts to delete the data. Mobile devices that have been damaged or dropped in water may still have recoverable data unless the memory chip has been compromised (Bennett, 2011).

While some of the data collected from a cell phone may be considered circumstantial, one cannot refute the added intelligence it offers law enforcement investigators. In *Riley v. California* (2014), the cell phone seized at the defendant's arrest provided the officer data regarding a gang affiliation. A gang specialist reviewed the data further for additional intelligence and was able to connect Riley to an unsolved shooting case (*Riley v. California*, 2014). In 2007, a drug dealer was arrested and two cell phones were taken and reviewed. Information obtained from the cell phone led the police to the drug dealer's home, where they filed for a search warrant and subsequently found more drugs and weapons in his apartment (*United States v. Wurie*, 2013). In *State v. Thompson* (2014), a woman was convicted of assaulting her husband. Text messages she sent, which included profanity and threats, were used in court to show her state of mind the day of the assault. They were authenticated and

verified by a digital forensic investigator, so there would be no question of who sent the text and when it was sent (*State v. Thompson,* 2014).

Cell phone searches are often debated as unlawful search based on the Fourth Amendment, but the data collected is invaluable to a case and the investigator. An investigator should use all avenues available to him/her to gather as much information as possible to prove his/her case. Proper due diligence is key to making a case stick. Given the amount of time people spend on their mobile devices, it is safe to assume that a wealth of knowledge is hidden there. When a crime is committed, it is incumbent upon the law enforcement agency to solve it, and just like interviewing a witness or lifting fingerprints off of a doorknob, their mobile device can provide indispensable information to get the job done.

COUNTER POSITION

As valuable as digital forensics can be to law enforcement, there are some hurdles and less-attractive reasons why it may be unreasonable to expect all agencies to utilize the tool. Digital forensics is still a new frontier for most law enforcement agencies, and the time it takes to pull evidence may not be an effective use of an investigator's time, or the case may be fast tracked and time just cannot be afforded. Once a device is imaged, or all the data is downloaded into a legible format, the amount of data is substantial (Jackson, 2014). An investigator can tediously review all the data, but sometimes the search for the suspect cannot wait. Not all agencies have digital forensic experts on staff to review all of the data a device produces and given budget constraints, the case may be won without the use of any potential data that can be recovered from a device. Again, the reviewing of digital forensic data is a long process, and one that must be done very carefully in order to preserve the evidence, so it is

actually useful in a court of law (Jackson, 2014). There are a lot of digital forensic laboratories available for hire across the country, but sometimes it is the cost or the turnaround that nullifies this option. There are also legal constraints to consider. The Fourth Amendment to the United States Constitution and search incident to lawful arrest (SILA) have been used in court proceedings, and both of these are points LEO's should be prepared to argue. Another question that is has often been raised, when searches of cell phones have been scrutinized, is if there is an expectation of privacy as it pertains to the contents of a person's mobile device.

Currently, digital forensics labs are experiencing high volumes of digital evidence in their facilities. The turnaround time for evidence submitted for investigation has increased from weeks to months worldwide (Henseler, 2013). Agencies either do not have the budget due to the expense of a third party lab, or there simply is not enough time to train officers internally to manage the ever-growing digital evidence workload. Private digital forensic companies charge between $100 to $600 per hour for their services and a hard drive could produce up to 200 million pages of information, which would require a reasonable amount of hours to fully examine (IT Forensics, n.d., para. 9). Luc Beirens, with the Federal Computer Crime Unit (FCCU) says "the number of seized computers is a multitude of the number that was seized ten years ago" (Henseler, 2013, para. 5). Given the amount of digital equipment each person owns, like a mobile phone, tablet, laptop, and desktop, this causes further delay because each device must be examined (Henseler, 2013). Ideally, keeping the evidence internal within an agency is preferred to maintain chain of custody in as few hands as possible. When labs examine evidence, they are not necessarily doing it with a police officer's eye or understanding how one strand of data traces to other evidence in the case. Even agency digital forensic investigators do not know what the evidence will reveal

until they can take a look at it themselves (Henseler, 2013). Training LEO's on how to pull digital evidence from cell phones could save time, money, and keep evidence integrity intact.

Saving time is probably the most important when trying to solve a case. Having to wait the typical three to six months for digital forensic labs to properly examine devices could be detrimental to a case. Having proper tools within each agency would be beneficial and an appropriate course of action to mitigate the delays. Agencies worldwide have begun utilizing web-based software that extracts data from mobile phones. This software is easy to use and allows non-technical officers to gather information quickly in a user-friendly and easy-to-read format. One agency in Belgium seized more devices and processed 10 terabytes of data. What took months to complete using third party labs, took merely two weeks to process 12 containers of electronic evidence (Henseler, 2013). One software tool that agencies use is called Cellebrite. Cellebrite is one of the most popular tools for digital evidence extraction. They offer training and equipment to law enforcement agencies at little cost to the departments. They began in 1999 by supporting the military's digital forensic needs. Then, retailers used it to transfer data from one phone to another. Then law enforcement agencies started seeing the value in using it to gather evidence quickly (Jackson, 2014).

When agencies have viable tools to extract evidence, they will also need to consider gathering that evidence within the confines of the law. There is a lot of debate and court precedence dealing with extracting, or searching for, information inside a person's mobile device. A popular argument is whether obtaining a person's cell phone is illegal search and seizure. As described below, court documents argue that perhaps

law enforcement officers should be more knowledgeable on when to secure the device and how they can use the data stored on the phone quickly and legally.

The United States Constitution 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”(U.S. Const., amend. IV). The main problem the Fourth Amendment creates in mobile forensics is if the owner of the seized device has a reasonable expectation of privacy (Bennett, 2011). Debate has not only been a problem in lower courts, but it has reached the Supreme Court on numerous occasions. The Supreme Court has stood firmly and transferred judgment for lower courts to decide. Some feel that the judicial system across the nation cannot even agree if text messages or data on a cell phone would warrant defense by the Fourth Amendment (Vitale, 2014). According to Vitale (2014), this issue was debated in *State v. Hinton*. The court ruled that anyone who sends a text message runs a risk that it could be read by someone other than the intended party. The minority in this case argued that the courts and the Fourth Amendment should keep up with advancements in technology and new immerging ways to communicate with each other (Vitale, 2014). Public opinion agrees. Vitale (2014) stated that “seventy-eight percent of Americans consider the information on their cell phones to be at least as private as that on their home computers” (p. 1114) However, with the amount of time people spend on mobile devices, it stands to reason that if a crime has been committed, details or possible clues to that crime might be stored on their mobile device. SILA has offered a loop-hole for officers to gather cell phones during arrests, circumventing the need for a warrant to search the device.

According to Weathersbee (2013), *Chimel v. California (1969)* is the case that sealed the SILA exception. The court decided that an officer could search the person

and the area within their immediate control for two reasons. The first reason is so that the officer can remove any weapons the suspect might use to harm someone or to resist the arrest. The second reason is to avoid any damage or loss of evidence. While this ruling did not directly address cell phones, the case of *United States v. Finley* (2007) did. The court upheld the officer's decision to search a cell phone without warrant because the phone was found in the defendant's immediate control or, in this instance, his pocket (Weathersbee, 2013). One can reasonably assume that the cell phone could have been destroyed and evidence lost if the officer had not seized it upon arrest. Furthermore, the Chimel case ruled that during a search, it was reasonable to not only allow officers to search for weapons or means of escape, but also to check the suspect physically for any evidence they feel needs to be preserved for trial (Corradi, 2013).

So, the courts tend to agree that the cell phone is a viable source of evidence, and have made it available to officer's to seize upon arrest. It also offers certain protection to the officer to have the cell phone examined for texts, photos, emails, and other digital evidence to use as evidence in their case. The amount of debate on this topic could fill up hundreds of pages, but to summarize briefly, upon arrest, if an officer has reasonable belief that evidence recovered from the cell phone found on the arrestee's person is in direct context the arrest, then most courts tend to agree that it is admissible and within the law. However, the argument stands that if an individual is committing a traffic offense, when there may be no basis to conclude that evidence of the offense will be found on the mobile device, this creates a threat to privacy (Corradi, 2013). As previously mentioned, the Supreme Court has never decided a case where a mobile device search was involved, so the decision is left to courts across the nation,

which causes inconsistencies in court precedence and potential confusion within law enforcement.

RECOMMENDATION

While law enforcement agencies cannot change court decisions, or make them consistent, they can do their jobs by upholding the law, catching criminals, and using evidence, wherever it may be gathered, in order to solve their case. This debate is not between the court and law enforcement, but whether or not mobile device digital forensics is a valid source of evidence and how agencies across the country can utilize technology in order to benefit their investigation and the ultimate prosecution of the case. The law is absolute, but the operations and budgets of an agency differ across the country. Digital forensics software is available for all law enforcement to utilize. They just need training.

There are many labs available to help them examine all types of devices if enough time is available. If procured correctly, whether upon arrest or via a warrant, mobile phone devices could hold the key to solving the case, and in some cases, leading investigators to new evidence in other unsolved cases. Law enforcement agencies should utilize all tools available to them in order to extract potential evidence from mobile and smart phone devices. The technology is changing every day and, while it may be difficult to keep up with a limited budget, in the long run, it will save the department time and personnel hours because the data is so undeniably solid and reliable. Data on a mobile device is there whether the suspect thinks he deleted it or not. The photos, text messages, and emails on the phone could possibly give clear answers to who committed or witnessed the crime, what happened before, during, and

after the crime, and where exactly the crime took place. Obtaining the phone during arrest is important to avoid any potential damage or loss to the evidence.

There are forensic companies and software developers such as Micro-systemation and Cellebrite that offer specific training to law enforcement at little to no cost to the department. In fact, the National Institute of Justice offers equipment and technology to police departments across the country, and they provide outreach and training, as well (National Institute of Justice, 2014). The International Association for Computer Information Systems (IACIS) is a non-profit association that provides education on computer technology and digital forensics to IT professionals, as well as officers in the digital forensics field (http://iacis.org). These two organizations are just examples of the multitude of training available.

Law enforcement agencies just have to invest a small amount of time and money in order to save both later on. Looking within the department to identify an officer that is technologically savvy could be the answer. Training that officer and investing the money in the vast amounts of training and education could offer the department a valuable resource. If the department is one of several in an area, that officer could be a tool for other departments to utilize.

Mobile technology is popular, vast, and ever changing. Ninety percent of Americans own a mobile phone. Sixty-four percent of Americans own a smartphone. Eighty-one percent send or receive text messages, 60% access the internet, 50% download applications, and 49% percent get directions, or use it for other location-based information (Pew Research, 2014). While some argue that their phone should be considered private and any attempt to look at it would be an invasion of said privacy, past court cases, like *Chimel v. California* (1969) and *United States v. Finley* (2007) have stated that information that is placed out on the internet, or sent to another party

cannot be considered private. A person cannot be certain that what they send or pictures they post are not seen by anyone other than the intended party. With all of the mobile activity, the expectation that an officer would find an exorbitant amount of data and evidence is not unreasonable. The expectation that a suspect would try to destroy said data and evidence is also not unreasonable.

Officers need to be taking advantage of every opportunity to gather evidence. Departments should be keeping up with the advancements in mobile technology and altering their policies to fit those advancements. Arguments can be made to city councils and other city officials to raise budgets. The expectation should be that these officials would want criminals caught versus keeping them on the streets because condemning digital evidence could not be gathered properly. Law enforcement agencies need to be well versed in digital forensics and the potential for evidence on a mobile device.

REFERENCES

Bennett, D. (2011, August 20). The challenges facing computer forensics investigators in obtaining information form mobile devices for use in criminal investigations. *Forensic Focus.* Retrieved from http://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/

Casey, E. (2009). Top 7 ways investigators catch criminals using mobile device forensics. Retrieved from https://digital-forensics.sans.org/blog/2009/07/01/top-7-ways-investigators-catch-criminals-using-mobile-device-forensics

Chimel v. California. 395 U.S. 752 (1969).

Corradi, S. (2013, Spring). Be reasonable! Limit warrantless smart phone searches to Gant's justification for searches incident to arrest. *Case Western Reserve Law Review, 63*(3)*,* 943-963*.*

Hanson, M. (2006, April 21). How the cops caught BTK. Retrieved from http://www.abajournal.com/magazine/article/how_the_cops_caught_btk/

Henseler, H. (2013, December 23). Breaking the backlog of digital forensic evidence. Retrieved from http://net-security.org/article.php?id=1932&p=1

IT Forensics. (n.d.). Frequently asked questions. Retrieved from http://www.itforensics.com/faq/faq.html

Jackson, W. (2014, June 17). Mobile forensics tools hammer out evidence. Retrieved from http://gcn.com/Articles/2014/06/17/Mobile-forensics-tools.aspx?Page=1

National Institute of Justice. (2014, March 28). Law enforcement equipment and technology. Retrieved from http://www.nij.gov/topics/law-enforcement/technology

Pew Research Center. (2014, October). Mobile technology fact sheet. Retrieved from http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/

Riley v. California. 573 U.S. (2014).

State v. Thompson. 141 Ohio St.3d 254 (2014).

U.S. Const. amend. IV.

United States v. Finley, 477, F.3d 250, 259 (5th Cir. 2007).

United States v. Wurie, 728 F.3d 1 (1st Cir. 2013).

Vitale, J. (2014, Summer). Text me, maybe: State v. Hinton and the possibility of fourth amendment protections over sent text messages stored in another's cell phone. *St. Louis University Law Journal, 58*(1109), 1109-1144.

Weathersbee, C. (2013, Summer). A constitutional ringtone: Cell phones and the search incident to lawful arrest warrant exception post Gant. *Charleston Law Review, 6*(2012), 807-837.