THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 12 | Number 3 Article 6

9-2017

Public Security & Digital Forensics in the United States: The Continued Need for Expanded Digital Systems for Security

Deborah G. Keeling
University of Louisville, dgwils01@louisville.edu

Michael Losavio
University of Louisville

Recommended Citation

Keeling, Deborah G. and Losavio, Michael (2017) "Public Security & Digital Forensics in the United States: The Continued Need for Expanded Digital Systems for Security," *Journal of Digital Forensics, Security and Law*: Vol. 12 : No. 3 , Article 6.
DOI: https://doi.org/10.15394/jdfsl.2017.1452
Available at: https://commons.erau.edu/jdfsl/vol12/iss3/6

PUBLIC SECURITY & DIGITAL FORENSICS IN THE UNITED STATES: THE CONTINUED NEED FOR EXPANDED DIGITAL SYSTEMS FOR SECURITY

Deborah Keeling
University of Louisville
College of Arts and Sciences
Louisville, Kentucky, 40292 U.S.A.
dgwils01@louisville.edu

Michael Losavio
University of Louisville
Department of Criminal Justice
Louisville, Kentucky, 40292 U.S.A.
michael.losavio@louisville.edu

ABSTRACT

Digital Forensics is one of the latest challenges for the use of forensics in the investigative process in the United States. Some of the challenges are created by conditions and circumstances present for law enforcement around the world. However, many are unique to the United States and created by the standards of evidence within our courts, nature of our law enforcement organizations, and structure of our judicial and prosecutorial systems. It is essential for the preservation of public security and individual safety that competent systems of digital forensics are developed for law enforcement at all levels. The failure to do so will let the guilty avoid responsibility for their criminal actions while possibly subjecting the innocent to unprecedented government intrusion into their private lives.

Keywords: digital forensics, law enforcement, public security, technology, cyber security

1. INTRODUCTION

Digital Forensics is: "...use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal or helping to anticipate the unauthorized actions shown to be disruptive to planned operations" (Palmer, 2001). Digital forensics arose in response to the digital age and with all of the advances and positive contributions to our ability to communicate, work and play more effectively and efficiency. Simultaneously, the abuses and misuses of digital forensics also arose. At no other time in history has society been so dependent on technology and its various offshoots and incarnations (United Nations, 1999).

Technology has changed the way in which we interact as a society (NRC, 2002; Rogers, 2003). The US Census Bureau estimated that in the year 2001, e-business retail sales totaled $34 billion (US Bureau of Census, 2002). Estimates of e-business retail sales for 2015 totaled $340.4 billion (US Bureau of Census, 2017). This represents an increase of 900 percent over this fourteen-year period. Similarly, individuals are increasingly using the internet. The US Census reported that in 2012, 74.8 percent of total US households reported that someone in the household had access to the Internet from some location. For individuals 44 years and younger, the rate of access was over 80 percent (US census, 2014).

Similarly, in 2000, 53 percent of US residents reported that someone in the household accessed the Internet from some location. In 2012, this rate of reported use had increased to 75 percent (US Census, 2014). Of those accessing the internet in 2012, 69 percent reported access from home and 75 percent from hone or some other location. In 2015, approximately 95 percent of US respondents reported owning a cell phone with 77 percent reporting owning a Smartphone. This is up from 83 percent cell phone and 35 percent smartphone ownership in 2012 (PEW Foundation, 2017).

With the advent of increased technology and increased use of technology comes misuse. Not all misuses of electronic devices are crimes. Cybercrime takes various forms but is generally defined as "crimes committed through the use of digital devices as either the object of a crime, the instrument to commit a crime, or a repository of evidence related to a crime" (Agarwal, et. al., 2011).

2. LITERATURE REVIEW

In 2011 a survey of 50 large US companies found that the median cost related to cybercrime in 2011 was $5.9 million. This represents a 56 percent increase over the median cost reported in 2010 (Cybercrime Research Center, 2011). The forms of cybercrime reported were mixed but more insidious such as malicious code, denial of service and Web-based attacks. It took an average of 18 days and $417,748 to clean up the attacks an increase from the 14 days and $247,744 reported in 2010. The average number of successful attacks reported was 72 per week, up 44 percent from the previous year (Cybercrime Research Center, 2011).

Similarly, individuals report various types of Cybercrime on an increasing frequent annual basis. In 2000, there were 16,838 complaints of internet crime to the Internet Crime Complaint Center. By 2011, the number of complaints had increased to 314,246 totaling an estimated $485.3 million in losses. The most frequently reported crimes were: advanced fee scams (9%), identity theft (9%), FBI-related scams (11%) and (7%) non-auction or non-delivery of merchandise (Internet Crime Complaint Center, 2011). In 2016, the number of complaints filed was 298,728 with a reported $1.33 billion in victim losses (Internet Crime Complaint Center, 2016). The US Federal Trade Commission reported that in 2009, 26 percent of all complaints involved some form of computer-related crimes. The specific crimes in included: credit card fraud (17%), theft of government benefits or documents (16%), and theft of phone or utilities (15%) (Federal Trade Commission, 2010).

Also, apparent within these trends is the increased use of the cell phone as a repository of criminal evidence. Cell phones are now a major crime scene item that is captured and analyzed in the course of the investigation of the full range of crimes. Law enforcement agencies are also increasingly relying on cell phone-related evidence. In a survey conducted in 2007, law enforcement commanders reported the belief that cell phone evidence was frequently involved in both violent crimes and drug offenses.

Approximately 40% of the commanders believed cell phone evidence was involved in 51% or more of all violent crimes and approximately 50% that cell phone evidence was involved in 51% or more of all drug offenses (Losavio, et. al., 2007). Digital forensics units report that more than 70% of their examinations involve cell phones (Personal Correspondence, FBI Regional Computer Forensics Lab Program National Advisory Committee, May 2012).

While digital evidence is becoming more prevalent, this boom in technology poses significant challenges for law enforcement. Even today, computer security and digital forensics is evolving and will continue to do so because as technology changes so must efforts for security and digital forensics. Digital forensics, as a discipline, has progressed through three stages, to date (Charters, 2009; Pollitt, 2010). Digital forensics and computer security were preceded by the development of computers in 1947 and is defined as the beginning of the Industrial Era of Computing (History of Computing Foundation, 2010). The first phase of digital forensics is the Ad Hoc (Charters, 2009) or Infancy (Pollitt, 2010) stage. Computers were generally mainframe computers and the possession of large organizations. Personal computers were in use and were powerful but were not user friendly and had relatively few applications that could be of general use to individual "hobbyists" (Pollitt, 2010). This was the "pre-forensics" stage characterized by a lack of structure, goals and clear policies and procedures to govern the identification and collection of digital evidence. Evidence was collected but the quality questioned due to unclear policies within organizations concerning employee "use" of corporate property and "ownership" of employee's work products on corporate computers. Accuracy of forensic tools and "chain-of-custody" issues were significant in that there were few, if any, court decisions concerning digital evidence during this era. Law enforcement agencies were beginning to use digital evidence, but training was limited, examiners were often individual investigators with an "interest" in computers and therefore, digital forensics "operated in direct conflict with the traditional, laboratory-based practice of forensic science" (Pollitt: 8, 2010). The second phase of digital forensics, Childhood, extended from 1995 through 2005 (Pollitt, 2010). It is characterized by tremendous growth not only of digital forensics applications and policies, regulations and laws related to the use/misuse of computers and other electronic devices but of individual use/misuse of electronic devices and, most notable, the "explosion of child pornography cases" beginning with the George Stanley Burdynskim Jr. case in 1993 (Pollitt, 2010). Additionally, this era encompassed the events of September 11, 2001 and the use of computers by terrorists and a lack of expertise on the part of law enforcement and the military to handle these events. The need for specialized training due to the increased volume of cases, increasing complexity of technology and growing knowledge within the field became increasingly evident. Field came to develop through impetus from government agencies and specialize digital forensics organizations.

The next phase, Adolescence, covered 2005-2010 (Pollitt, 2010). With this phase came increasing legal specification that defined digital information as evidence and specified a mechanism for eDiscovery (Manes, et.al., 2007). Academic and detailed, advanced training programs grew as did the complexity and maturity of devices to be examined. "Virtually every device that use(d) electricity ha(d) some form of digital storage. Wired or wireless networks connect(ed) many of the devices we use(d) in our daily lives" (Pollitt: 12, 2010). Organized processes and procedures for the identification, collection, analysis, preservation and presentation of digital evidence were

developed by law enforcement, the military and the intelligence community.

The development of digital forensics within American law enforcement has and continues to face many challenges. These include: access to digital services; training and equipment needs (economic issues); lack of standardization; legal issues related to the validity and reliability of digital evidence (forensic science versus technology); increased complexity of digital evidence (cloud computing, hard drive encryption, size of data to be seized/analyzed) and related digital issues. However, the over-reaching issue is that of cultural lag relative to technology and the law/ethics that exists and continues to drive much of the social behavior related to the use of technology.

2.1 Access to Digital Services

The United States has approximately 18000 law enforcement agencies, each with a unique geographic and legal jurisdiction. Each funded differently with no consistent standards for law enforcement training, equipment, services, or policies and procedures. As such, the availability of digital forensics resources is extremely uneven among law enforcement agencies throughout the United States. Some law enforcement agencies, generally the federal agencies and largest US police departments have their own digital forensics units for purposes of examining, analyzing and preserving digital evidence. However, large jurisdictions, those with 1000 or more sworn personnel constitute only .4% of all local police agencies in the US. In fact, most police agencies, 95.4% have fewer than 100 sworn personnel and are responsible for jurisdictions with fewer than 25000 in population (Bureau of Justice Statistics, 2013).

A survey of law enforcement agency digital forensics resources was conducted in 2005. A total of 576 law enforcement agencies were surveyed. A majority of the agencies (72.3 percent) did not have a dedicated digital evidence unit and another majority (58.1 percent) had no digital evidence policies. Only approximately one half had digital forensics awareness training. Similarly, most (57.5 percent) reported the collection of digital evidence in from 0 to 5 percent of their investigations (Pollitt, 2005). Another survey of police commanders reported that 35% responded they had failed to use digital (cell phone) evidence in criminal cases due to a lack of access to expertise to extract and preserve the digital evidence (Losavio, et.al., 2007).

Clearly, the emphasis on local law enforcement and lack of consolidation of law enforcement within the United States has resulted in "uneven" access to digital evidence resources. This includes awareness training on digital evidence (what is digital evidence, why it should be seized at the crime scene), as well as access to resources to extract and preserve digital evidence in criminal cases. While some of the variation in digital forensics may be the product of decisions by leadership within these agencies, it is, in all likelihood, more directly related to economic factors.

Several projects have sought to remedy this. For example, the Secret Service provided training and equipment to departments around the country willing to dedicate staff to this. Continued expansion of this capability will be crucial to public security.

2.2 Training and Equipment Needs

"The collection of electronic data as evidence of crime is an important responsibility given to law enforcement. The technical constraints of this task are arguably far less significant than usability and economic ones, since police officers are non-specialists and police departments face significant budgetary limitations" (Moore: 1, 2006). The primary constraints on digital evidence practice for law enforcement agencies are economic rather than technical. Training in

digital forensics examination techniques is very expensive, and may cost as much as $10,000 for basic training in data extraction and upwards of $20,000 for training in more specialized digital examination techniques such as extraction of data from damaged hard drives (Personal Correspondence, FBI Regional Computer Forensics Lab Program National Advisory Committee, May 2012). Additionally, one-time training is not sufficient because as technology changes, skills must be enhanced, and so regular in-service training is required on at least an annual basis.

In addition to the training, digital forensics requires complex hardware and software that may cost tens of thousands of dollars. And, while the needs for data extraction on some devices such as personal computers may be conducted using many available tools due to standardization of hard drives, storage on devices such as cell phones and smart phones is within the phone's internal memory, is absent standardization and within locations that vary depending on the model. Even cords used to transfer information are not standardized. As such, cell phone examination is much costlier and requires specialized software and cables that are ever increasing with the release of new phone models.

Because of the size of their jurisdiction, number of sworn personnel, and the frequency of crime, budgets are limited, and the start-up and ongoing costs of digital evidence equipment, software and training may not be cost effective. However, even with larger law enforcement agencies, the economics are pressing and bear fixed costs with some additional marginal costs associated with the extraction (Moore, 2006). When access to the digital resources of a large police agency or central state forensics unit is available, that access may increase the marginal costs of the data collection. For example, the time for a police investigator to drive 60 or 100 miles carrying digital devices for examination to a centralized department results in higher personnel costs, transportation costs and may make the "chain-of-custody" more complex and potentially problematic.

2.3 Lack of Standardization

Lack of standardization within digital forensics is significant in several ways. 1) There is no standardization across all law enforcement agencies concerning the appropriate "investigative" model. For example, Agarwal, et. al. (2011) identified and discussed four prior investigative models as well as their currently proposed (Systematic Digital Forensic Investigative) model. The need for a standardized procedure within digital forensics is critical for the nature of the discipline, i.e., justification of the discipline as scientific rather than technical; establishing benchmarks in the investigation of crimes involving digital evidence; meeting legal challenges based on the integrity and admissibility of digital evidence; and create comparability of investigative techniques nationally. 2) As noted previously, access to digital forensics resources is not standardized across law enforcement jurisdictions and therefore, the ability to use digital forensics varies by agency and geographic location. 3) There are no standards for what constitutes "appropriate" digital forensics examination training, no standards for "appropriate" digital forensics examination techniques and no standards for "appropriate" digital forensics tools. "Experts" within the discipline are, for the most part, self- defined though those within the FBI CART are generally recognized as having some of the most detailed and complete training. Proprietary sources for the software and hardware generally determine "adequacy" of their proprietary training that is "purchased" along with the hardware and/or software to be used in the digital forensics process. Whether students "pass or fail" is not an issue and may or may not

be recorded by any other than the agency sponsoring (paying for) the training.

The American Society for Crime Lab Directors has an official board (Lab Accreditation Board) that accredits digital forensics labs. It is currently the only accrediting body for crime labs. Similarly, one non-proprietary group for testing computer forensics software, National Institute for Standards and Technology (NIST) Computer Forensics Tool Testing (CFTT) division is a government entity that performs tests on software. Similarly, the FBI's Technology Division performs tests on digital examination software and hardware as a means of determining whether the devices meet the standards set for these tasks by the organization itself. These regulatory bodies are not sufficient to keep pace with changes in computing and electronic devices.

A survey was administered to digital forensics examiners in 2003 (Rogers and Siegfried, 2004). These respondents expressed concern over an absence of national standards for digital forensics. Specifically, they were concerned there were no national certifications for digital forensics and the linkage between several current certifications and vendors such that the vendors certified the customers on proprietary tools. As noted by the authors, "...proprietary certifications only increase the level of fragmentation within the industry and perpetuate the misguided belief that there is no generic conceptual approach to computer forensics" (Rogers and Siegfried, 2004: 15).

2.4 Admissibility of Digital Evidence

Evidence gathered through all forensics disciplines must meet basic evidentiary and scientific standards if it is to be used in legal proceedings. The US Supreme Court set these standards in the decision in the case of Daubert v. Merrell Dow Pharmaceuticals, Inc. (1993). The decision set standards for determining the scientific basis of evidence because the law views scientific evidence as more reliable and therefore more acceptable than non-scientific evidence. The process under Daubert identifies four general categories to use in the assessment of evidentiary procedures: Testing (Can and has the procedure been tested?), Error rate (Is there a known error rate of the procedure?), Publication (Has the procedure been published and subject to peer review?), and Acceptance (Is the procedure generally accepted in the relevant scientific community?).

Whether or not digital evidence meets the standards of admissibility under Daubert is and will continue to be a recurring issue. 1) Testing - This legal standard asks whether a forensics tool can and has been tested to prove that it produces accurate results. Organizations such as National Institute of Standards and Technology have performed and published digital tools but, to date, no standard testing methodology exists. Most often, problems with open and closed source applications are identified by users in the field. The users then report the problems to the vendors. The vendors make the necessary changes but may not be motivated to report these findings, generally, to the public or justice practitioners (Carrier, 2002). Similarly, 2) Error rate – This standard asks whether there is a known error rate for the procedure. Manufacturers of digital forensic tools do not necessarily want to provide a "known error rate" for their tools. In fact, promoting the error rate would simply be "bad for business." As such, when major errors are reported by users, the manufacturers simply make changes to the tools (new and in-service) without drawing too much attention to the problems with their "product." 3) Publication - Whether the procedure has been published and subject to peer review. As digital forensics has matured as a science, so have the number of research projects and publications on the

various tools. Much is, however, still proprietary and protected with the manufacturers conducting internal validation research on their own products, making the changes necessary, without publication of the results. Only with the field user or organization, such as the FBI that methodically validates all instruments used in the digital forensics process, are the tools validated and the results published and distributed for general consumption. In some instances, even these validation studies carried out by the FBI are not published since identification of a weakness with a digital forensics tool might call into question convictions based on the findings from this instrument and/or provide offenders with information to more efficiently perform the activities involved in cybercrime without detection. 4) Acceptance – The last standard assesses whether or not the procedure is one that is generally accepted in the relevant scientific community. The interpretation of this standard is varied. On the one hand, the digital forensics tool vendors argue that numbers of customers are a measure of "acceptance" in the relevant scientific community. However, customers are "users" and "users" are not necessarily "scientists" but rather trained professionals who use the tools developed and vetted by the scientist. When number of customers is not used, scientific publications become a criterion and, as such, the limitations discussed in the "Publication" standard would apply.

Since 2007, the US Federal District Court has rendered more than 1000 court opinions concerning cell phones and their use as evidence or sources of evidence within criminal proceedings (Law.Justia.Com, downloaded May 15, 2012). Additionally, since 2008, the US Federal District Courts have rendered more than 500 opinions concerning digital evidence. While not all were questions related to the admissibility of this type of evidence in the specific cases, the opinions addressed various legal issues related to this newest form of scientific evidence (Law.Justia.Com, downloaded May 16, 2012).

Judicial determinations are based on findings of fact that are informed by the not only the law but the general knowledge of judges on the specific topic. The extent to which judges are familiar with electronic evidence and systems may affect decisions concerning the admissibility of digital evidence. A survey of judges in 2005 found that while the majority (75%) expected significant changes in the future and felt they needed significant training (95%) in digital evidence, only a minority actually had experience in digital evidence. Only 5 percent reported handling cases involving email evidence and 3 percent website or Internet evidence. However, when used, 17 percent reported email evidence was frequently or almost always challenged with 20 percent reporting similarly for website or Internet evidence (Losavio, et.al., 2006). If judges do not understand digital evidence, it may be more difficult to make a determination concerning its admissibility and therefore challenges to digital evidence may be more numerous and affirmed more frequently.

2.5 Increased Complexity of Digital Evidence

Law enforcement agencies are dealing with increasingly large amounts of digital evidence. The agencies have moved from analysis of bytes to megabytes, gigabytes, terabytes and petabytes. Personal computers now hold more information and more processing power than the corporate mainframe of 15 years ago. Digital examiners must have the capability to process large amounts of information and to do it accurately, completely and in a timely manner. This requires advanced equipment and therefore results in additional costs that are not necessarily part of the budget of most US law

enforcement agencies. Similarly, law enforcement agencies will soon be addressing more issues related to encryption as computer companies begin to mass produce personal computers with self-encrypting hardware – more training, more equipment, more costs. Lastly, issues such as "cloud computing" raise serious questions requiring legal clarification. That which is most specific is "who" owns the information an individual stores in a proprietary "cloud" and what reasonable expectations for privacy can an individual have when operating in a proprietary "cloud" environment. What can vendors be required to do in terms of notification to consumers and public reports on law enforcement information requests relative to "cloud" computing? Which entity should be named in the warrant – the vendor or the customer? These are complicated issues that will need to be addressed within a relatively short amount of time.

2.6 Other Issues

Perhaps the greatest challenge that faces not only US law enforcement but all law enforcement involved in digital forensics is cultural lag. Cultural lag is a term coined by William Ogburn (1922). It refers to differences between technology and the "non-material" components of a culture in which there is a "lag" between the material (technology) and non-material culture. Since technology changes at a rapid and ever-increasing rate, the ethical "guides" for use of technology are in a constant state of "lag" since social norms and values do not change at the same rate as that of technology.

Marshall (1999) raised the issue of cultural lag and argued it is appropriate and important to address whether new technologies introduce ethical problems. The development of social guidelines and norms for technology becomes even more significant when technological change creates great cultural shift due to rapid diffusion across a wide range of human activities (Marshall, 1999; Robinson, 1981). Such is the case with computing. Normative, legal and ethical issues surround technology and multiply as technology changes and becomes more distributed throughout the everyday lives of members of our society. Some of the issue are normative such as etiquette related to cell phone use or practical considerations related to the consequences of what individuals choose to post on Facebook pages. Others are related to ethics and include issues of Internet postings, using a roommate's computer without permission or "sexting" on a PDA. Many are not only unethical but also illegal. Many times, however, the illegal or unethical nature of acts is not recognized – at least not initially, until realization is made of the "harm" that occurs or can occur. Who would have thought that there would be a need for laws related to the distribution of pornographic images of children over the Internet or that a specialized form of "bullying" that is, cyber bullying would emerge?

American society is diverse. The development of values, beliefs, ethics, and laws does not occur in a controlled focused environment. Instead, it occurs through individuals with widely divergent backgrounds, knowledge, skills, etc. Changes in cultural norms, values and belief systems is not specific and does not emerge quickly. Unlike the development of technology, there is no market structure to reward changes in the non-material culture. That is, those who ponder and assist in the development of ethical standards are not rewarded monetarily. It is not possible to develop ethical standards until after-the-fact that is, until after the development of new technology. As such, our understandings, ethics, beliefs and social guidelines related to technology use will always "lag" behind the rate of development of technology itself.

Some of the cultural lag is evident in the development of law at the highest levels, the US

Supreme Court. This court has had to, after-the-fact, develop new standards for e-Discovery, to determine whether or not cell phone companies are obligated to provide law enforcement with cell phone information that would track the activities of their customer. Standards of privacy and reasonable expectations of privacy have been redefined in response to electronic technology. In the past, many of the Supreme Court rulings were based on the premise that individuals did not have a reasonable expectation of privacy when in a public area/situation. Most recently, the US Supreme Court decided that our citizens do have a reasonable expectation to privacy in public places when ruling on the legality of search and seizure in a case in which law enforcement used GPS to track the movements of a suspect in a recent case. In the ruling, one Justice rendered a solo opinion stating that individuals had more of a right to privacy in data held by phone and Internet companies than the Supreme Court had held in the past (www.wired.com/threatlevel/2012/01/scotus-gps-ruling/, downloaded May 16, 2012).

3. REMEDIATION POSSIBILITIES

There are a variety of possibilities for the remediation of these obstacles to the deployment of digital forensics resources. One project, for example, has tested linking a federal Bureau of investigation regional computer forensics laboratory (RFCL) with local law enforcement mini-laboratories for analysis directed using a triage model to allocate resources to cases. Each participating agency or agency division provided, among other things, secure laboratory space, a dedicated employee, employee training, and use of the digital forensics facilities. The project provided computer hardware, digital forensics suite of examination software (AccessData's FTK and MPE suites) and training on these systems and software.

The results demonstrated both the capacity for greatly expanding digital forensic services where there was commitment to use them. Table 1 contains the results for one agency assigned a full-time staff/officer to conduct examinations, produced the following result in roughly one-year period:

These examinations included a variety of crimes: murder, robbery, rape, unlawful imprisonment, assault, narcotics trafficking, child pornography and child sexual exploitation. The initial cases were child pornography/exploitation cases. However, over the one-year period, use of the services had expanded to address other kinds of cases, including homicide, rape and robbery. This indicates the shift towards use of digital forensics as an investigative tool across the criminal justice spectrum. It is worth noting that as the project evolved, these services were used by other law enforcement agencies, including the federal Bureau of Alcohol, Tobacco and Firearms (ATF) and the Kentucky State Police.

Table 1.
Number and Type of Examinations

September 2011 - July 2012	# **Computers**	# **Cell phones (SIMs)**	**Other** [1]
September		6	
October	5	18	1[2]
November		5	
December		7	
January		2	1
February	3	13	7
March	2	10	3
April		9	4
May	1	4	3
June	2[3]	9	2
July	1	5	2
totals	**14**	**88**	**22**

Another participating agency, which had been conducting its own digital forensics examinations, integrated the new tools and training into its operations. The data from its operations showed a significant shift from the examination of computers and related peripherals to the examination of cell phones for evidentiary purposes; approximately one third of the examinations were for outside agency seeking assistance with digital forensics examination. Similarly, another local law enforcement agency with a pre-existing digital forensics capacity and school online safety program also found a strong trend towards examination of mobile devices over that of computers**.** While the majority of cases continued to be child pornography, examinations were also part of investigations for drug trafficking, counterfeiting, forgery and a car bombing.

This project demonstrates that when provided services along with the willingness to use them; law enforcement agencies quickly find that digital forensic services play a role in nearly all forms of misconduct. Growth in the use of digital forensic services was also furthered by expansion of the examination of mobile devices relating to criminal misconduct.

Another project that promoted the distribution and use of digital forensics services were online, activated, distributed software tools with hardware connector kits and online training made available to qualifying law enforcement agencies. The forensic tool provided for data acquisition, analysis and reporting relating to cell phone examinations. It offered keyword searching and transactional timeline, frequency and linkage visualization for phone, text and web activity on the device.[4]

Analysis of data from one month of system use showed a broad use by many agencies municipal, county, federal and state law enforcement, including the Office of the State Fire Marshall, Lincoln University Police Department and the Kansas Department of Wildlife and Parks -- examining many different kinds of devices, cell phones predominated:

- Total successful exam logins – 210
- # agencies using system – 40
- # different mobile devices – 74
- # different manufacturers – 12

Data entry was inconsistent, with about one quarter noting the crime with which the associated device was being examined; those crimes included homicide, aggravated rape, aggravated assault and narcotics offenses.

The widespread and rapid adoption of this system again supports the conclusion that where resources and training are easily available, they will be adopted quickly by law enforcement as tools for crime investigation and prosecution.

[1] MicroSD cards are counted as separate devices although they are associated primarily found associated with cell phones in these examinations
[2] TomTom GPS 1EX00
[3] Includes a tablet computer
[4] Secure View 3 Case Management-Analytics: http://www.mobileforensics.com/svProbe (accessed July 9, 2012)

4. IMPLICATIONS

Computer crimes are highly impersonal, in most instances. They involve behaviors not generally addressed through existing moral standards. There is no need to face the victim when engaging in the crime. There is no need to observe the harm created by the illegal behaviors. Offenders generally only think of the implications of what they as one individual are doing and do not think of the implications of spreading this harm among millions of individuals and therefore, magnifying the harm. There exists only limited understanding of the perpetual nature of cyberspace and consequent harm.

Computer crimes additionally raise new challenges for the laws and only as new crimes emerge from the misuse of new technologies, laws must be changed and developed to address previously unknown issues. Technology also introduces a wide range of new vulnerabilities criminals can use to take advantage of their victims.

5. CONCLUSION

The expansion in both the presence of digital devices in relation to a crime locus as well as the use of digital devices as tools for the commission of crimes will continue, particularly as we see the growth of the Internet of Things and the present of interconnected devices everywhere. These provide both opportunities for crime as well as opportunities for investigation to solve those in other crimes. It is essential for the preservation of public security and individual safety that competent systems of digital forensics be available for all levels of law enforcement. The failure to do so will let the guilty avoid responsibility for their criminal actions while possibly subjecting the innocent to unprecedented government intrusion into their private lives. This is abhorrent to the rule of law and deserves our full attention.

REFERENCES

Agarwal, A., Gupta, M., Gupta, S. & Gupta, S.C. (2011). Systematic digital forensic investigation model. International Journal of Computer Science and Security, 5(1), 118-131.

Bureau of Justice Statistics (2003). Local Law Enforcement. https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5279

Carrier, B. (2002) Open source digital forensics tools: The legal argument (1-11). @stake.

Charters, I. (2009). The evolution of digital forensics: Civilizing the cyber frontier.

Computer Crime Research Center (2011). Cybercrime costing companies more this year. http://www.crime-research.org/news/09.08.2011/3880/

Federal Trade Commission, Annual Report (2009). https://www.ftc.gov/sites/default/files/documents/reports_annual/annual-report-2009/2009chairmansreport_0.pdf

History of Computing Foundation (2016). https://www.thocp.net/reference/info/about.htm#hocf

Internet Crime Report (2011). Overall Statistics. https://pdf.ic3.gov/2011IC3Report.pdf

Internet Crime Report (2016). Overall Statistics. https://pdf.ic3.gov/2016IC3Report.pdf

Losavio, M., Wilson, D., and Elmaghraby, A. (2007). Prevalence, use, and evidentiary issues of digital evidence of cellular telephone consumer and small-scale digital devices. Journal of Digital Forensic Practice, 1(4), 291-296.

Marshall, K. P. (1999). Has technology introduced new ethical problems?. Journal of business ethics, 19(1), 81-90. Library, Baltimore, MD. 30 Sep. 2009.

PEW Foundation (2017). 2015 Mobile Fact Sheet. ,http://www.pewinternet.org/fact-sheet/mobile/

Manes, G., E. Downing, L. Watson, C. Thrutchley (2007). New Federal Rules and Digital Evidence. Annual ADFSL Conference on Digital Forensics, Security and the Law. 3. http://commons.erau.edu/adfsl/2007/session-6/3

Moore, T. (2006, June). The Economics of Digital Forensics. In Proceedings of the Workshop on the Economics of Information Security, 2006.

NCR (2002). National Competitiveness Report. Institute of Professional Studies, Seoul, Korea.

Ogburn, W. F. (1922). Social change with respect to culture and original nature. BW Huebsch, Incorporated.

Palmer, G. (2001, August). A road map for digital forensic research. In First Digital Forensic Research Workshop, Utica, New York (pp. 27-30).

Pollitt, M. (2010). A history of digital forensics. Advances in Digital Forensics VI, 3-15.

Robinson, J.P. (1981). Will the New Electronic Media Revolutionize our Daily Lives' in R.W. Haigh, G. Gerbner and R. B. Byrne (eds.), Communications in the Twenty-First Century, John Wiley and Sons: New York.

Rogers, M. (2003). The role of criminal profiling in the computer forensics process." Computers & Security 22.4: 292-298.

Rogers, M.K., and K. Seigfried (2004). The future of computer forensics: a needs analysis survey. Computers & Security 23.1: 12-16.

United Nations Development Programme. Human Development Report Office. Human Development Report: Background papers. Human Development Report Office, United Nations Development Programme, 1999.

U.S. Census Bureau (2002). E-Stats. https://www.census.gov/library/publications.html

U.S. Census Bureau (2014). Computer and Internet Access in the United States 2012. https://www.census.gov/library/publications.html

U.S. Census Bureau (2017). E-Stats 2015. https://www.census.gov/library/publications.html

