Faith & Reason Honors Program
Senior Thesis

Name:
Jonathan Langton

Thesis Title:
Digital Forensics and Law Enforcement: An Impending and Necessary Paradigm Shift

Thesis Sub-Title:
Understanding the Impact of Digital Forensics on Modern Criminal Investigation

Thesis Director:
Detective Joseph G. Pochron, MACJ
(Criminal Justice)

Year:
2013
Abstract

The application of digital forensics and cybercrime analysis to many areas of criminal investigation promises to maximize law enforcement’s ability to confront complex crimes with state of the art technological tools. In order to capitalize on the true potential of digital forensics, law enforcement must take a cursory look at its past, its current status quo, and the potential for growth and depth in specialization and training. This paper will serve to explain the background of digital forensics, examine its contemporary practices and ramifications, and to highlight the great importance of its intricate relationship with law enforcement on the future of criminal justice as a field. In order to delve into the importance of this discipline, this paper will also focus on the appropriate balance between the need for digital investigation in the area of criminal justice and the constitutional rights that are procured by the Fourth and Fifth Amendments. Although analyzed as a type of balance, this relationship should be considered synergistic, as in the case of faith and reason. The world has come to perceive faith and reason as contrasting entities, clouding the prognosis for mutual growth and progress. In order to maximize efficacy in the field of criminal justice, practitioners must recognize the cooperative relationship between society’s faith in the Constitution and its associated rights, and the rational progression of technological advancement in the 21st century.
Introduction

Citizens of the United States of America currently live in a divisive time. Important topics polarize the nation, and political stratification seems to have become the norm. To suggest that faith may still act as a binding and unifying force may seem outlandish and naïve. However, throughout all of the debate surrounding ideology and political figures, Americans remain faithful to the ideals at the heart of the Constitution. The nation still believes in the core values inherent within our nation’s founding, and rallies around the principles of freedom and liberty. Americans put faith in the efforts of law enforcement personnel and agencies as they work to protect the welfare of people nationwide, even as debate surrounds the mechanisms through which this feat is accomplished. Although a seemingly simplistic notion, the Constitution remains a source of faith and hope for a nation that has always thrived off of pluralism and loyal opposition.

Technological advancement has always been a driving force for the growth and development of the United States as a nation; and for its citizens, in their pursuit of individual progress. The current era of advancement can best be described as the “Information Age”, and effectively mirrors other eras of rapid development, such as the Industrial Revolution. Just as the Industrial Revolution gave way to the Industrial Age, the current Information Age has been a direct result of the “Digital Revolution”. The Digital Revolution has effectively defined the current status of the world, and could be considered the latest descendant of the Scientific Revolution. These eras of revolutionary ideas and innovation stem from a basic belief in the power of human reason. The concept of reason as the backbone for modern technological advancements may seem obvious,
but is often taken for granted. Currently, modern technological advancements have dramatically changed the landscape of criminal investigation, as seen through the impact of digital forensics.

Faith and reason have been wrongly juxtaposed as polar opposites by scholars interested in secularism for centuries. One striking example of this juxtaposition can be found in the contemporary impact of digital forensics on criminal investigation. The criminal justice field is currently being challenged to find the appropriate balance between the need for digital investigation and the rights invoked by the Constitution. This balance is further complicated by the dynamic progression of technology, and the seemingly lethargic response to this progression by the judiciary. This paper will serve to analyze this balance, and to provide fresh insight into a crucial area of criminal justice policy that is subtly saturated with the fusion of faith and reason. This analysis will incorporate a brief background of the origin and development of digital forensics, and an examination of the policy problems that have been created by a wrongheaded schism between the notions of faith and reason in modern criminal justice policy. Furthermore, this analysis will posit a recommended solution for the aforementioned policy problem. The analysis will conclude by examining the current status of digital forensics, its critical role in aiding criminal investigation, and identifying a prognosis for future growth and development with nothing less than an impending and necessary paradigm shift.
Chapter 1: The Origin and Development of Digital Forensics

Although the aim of this paper is to illuminate the impact of digital forensics on criminal investigation, the overall discussion necessitates a fairly extensive examination of the specifics of the discipline itself. Digital forensics is roughly forty years old, and was initiated primarily as a method of data recovery by experts who specialized in the retrieval of data from hard drives at a sluggish pace. By the late 1980’s, utilities were being widely advertised that could perform a variety of data recovering. The characteristics that were proliferated throughout these early days of digital forensics were hardware, software and application diversity, as well as poorly documented data file formats, heavy reliance on time-sharing and centralized computing facilities in the stead of storage for analysis, and the absence of formal process, tools, and training. Digital forensics was largely performed by computer professionals, sometimes working with law enforcement, on an ad hoc, case-by-case basis. Truthfully, there was only a basic and limited need to analyze electronic tools, as data was often easy retrievable without the use of recovery tools and methodologies. The small scale of disk size and storage capacity made it easy for criminals to make extensive prints and copies, eliminating the need for most criminal cases to require actual forensic analysis. The FBI initiated a program to analyze magnetic media and data in 1984, but states that the program “only performed forensic analysis in three cases during the year of the program’s inception” (FBI, 2004). Although computer hacking existed in a type of infancy stage in the early-mid 1980’s, it was not actually deemed criminal legislatively until 1984, through the passage of the Computer Fraud and Abuse Act. Furthermore, organized crime and white-collar crime exhibited dramatically less nuanced techniques, making it proportionately easier for law
enforcement to combat these types of crimes without the aid of digital forensics. Throughout the 1990’s, there was an elevated need for digital forensics methodologies and tools, but less of a focus on actual practitioners within the discipline in relation to law enforcement.

The rise of digital forensics occurred during the early years of the 21st century, as a result of widespread proliferation of tools and law enforcement specialization. This advent necessitated the development of industry standards and standard operating procedures. Within the early 2000’s, digital forensics had been appropriately defined for all intents and purposes. As a recognized branch of forensic science, it now reaches beyond the initial definition which encompassed the recovery and investigation of data found in digital devices, and was more practically skewed to the concept of computer forensics. During this crucial time period, its breadth has expanded to all devices capable of storing digital data, and is divided into several sub-disciplines. These essentially encompass computer forensics, network forensics, database forensics, and mobile device forensics. The forensic process in relation to digital forensics can be concisely condensed into the seizure, collection, imaging or acquisition, and subsequent analysis of data. This analysis is complimented by the composition and appropriate dissemination of a report, detailing the quality and nature of the analyzed data and the modest conclusions that are derived from the final analysis. According to digital forensics scholar Eoghan Casey, “The proliferation of tools was the result of a decade-long technological revolution of sorts, initiated by the Federal Law Enforcement Training Center’s recognition of a need for digital forensics software in the early 1990’s” (Casey, 2000). The Digital Investigation review also reports that commercial tools such as “Forensic ToolKit,
EnCase, and StarWitness emerged during the late 1990’s, as well as the more recent arrivals in mobile forensic software, including Cellebrite, and XRY” (Mocas, 2004). The commercialization of digital forensics allowed not only for the proliferation of cutting-edge tools, but for the necessary training and certifications to utilize these tools without a purely computer science-oriented academic background. The groundwork had been effectively laid, and the opportunity presented itself for law enforcement to take significant strides towards achieving an upper hand in criminal investigation.

Law enforcement has taken advantage of the opportunity presented by digital forensics, and has made a historical leap in the direction of training and specialization. The development and cultivation of task forces and regional intelligence centers with a focus on digital forensic and cybercrime analysis has enabled law enforcement to investigate crimes that were previously impossible to trace or decipher, whereas crimes of a lower magnitude are investigated more swiftly than in the past. In short, this transformation has been a result of the widespread use of Microsoft Windows, and the relatively small amount of file formats of forensic interest. Additionally, Brian Carrier, a digital forensics academic contends that “examinations are largely confined to a single computer system belonging to the subject of an investigation, while multiple vendors have provided tools that are reasonably good at recovering allocated and deleted files from storage devices equipped with standard interfaces” (Carrier, 2011). The heightened sense of forensic professionalization within the law enforcement community has aided the growth of research within the discipline. As well as identifying direct evidence, research has enabled digital forensics can be used to attribute evidence to specific individuals and determine intent through a broad scope of investigatory tactics and
analyses. One of the more exciting and cutting-edge investigatory developments for law enforcement is the establishment of complex time lines and behavioral patterns of potential suspects through the discovery and analysis of personal electronic property and data. Although useful and unique, these tactics are much less direct and infallible foundations for inflammatory conclusions than those of other forensic science disciplines.

As is true to most newfound disciplines within the purview of criminal investigation, digital forensics needed a segue into the field through a process of legal holdings and legislative precedence. For example, the admissibility of scientific evidence was controlled until 1993 by the Frye test, named after a District of Columbia Court of Appeals case in which the test was initially promulgated. The Frye test held that the expert scientific evidence was admissible only if the scientific community widely agreed upon the principles that the evidence rested upon. Although the Frye test technically stood as precedent until 1993, the Federal Rules of Evidence, adopted in 1973, attained the status of precedent once Daubert v. Merrell Dow Pharmaceuticals was decided in 1993. In Daubert, the Court held that Rule 702 of the Federal Rules of Evidence, adopted in 1973, supplanted Frye. Rule 702 provides: "If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise" (Forensic Law, 2009). This implies that the scientific evidence proposed possesses the scientific validity to be considered competent as evidence if it is grounded in the methods and procedures of science. This legal timeline seems murky; however, when only half of the states have adopted the Daubert precedence, while a handful of others still adhere to the Frye test.
Regardless, there remains no specific test that can be used to determine whether digital evidence possesses the necessary expert scientific validity. Instead, the Court in 1993 recommended that digital evidence proposed for admission in court focus solely on the expert’s principles and methodology, rather than the conclusions generated, and that the evidence proposed for admission must be relevant, derived by the scientific method, and supported by appropriate validation. The question of applicability of Daubert-criteria and decisional processes to non-scientific expert evidence was addressed by the Supreme Court in 1999 through the decision in *Kumho Tire Co. v. Carmichael*. The court extended the Daubert approach to determining the reliability of expert testimony to all expert testimony, regardless of whether the testimony was based on scientific principles, or other specialized knowledge. This essentially avoided ambiguous decisions regarding whether testimony was rejected because it was scientific but did not satisfy Daubert criteria, or because it was non-scientific and therefore not subject to Daubert analysis, but still defective in some other way. In practice, the result is that every expert, including digital forensics experts, are now subject to challenge for reliability. Courts and legal representation are now required to seek indicators of reliability, such as an individual’s curriculum vitae, or records of certification and accreditation, which are relevant to the expert’s field of expertise. The testing, verification, and validation of theories and techniques of digital forensics, peer review, existence of known error rates, and overall tool efficacy and reliability are central to the overall acceptance of a digital analyst’s status as an expert witness in a court of law. Although the development of expert testimony qualifications through case law is unique and interesting, it remains a slightly
less significant legal issue than those concerning Constitutional protections and digital evidence.
Chapter 2: A New Frontier: Digital Evidence & The Constitution

Due to the “new frontier” that digital forensics has come to represent, there remains a large amount of confusion as to its pragmatic ramifications on constitutional limits in the realm of criminal law. A cursory illustration of the current issue is the debate surrounding the Electronic Communications Protection Act of 1986. The ECPA was enacted by the United States Congress to extend government restrictions on communication from telephone calls to include transmissions of electronic data by computer. Although initially successful in its implementation, the law is now largely outdated due to the current means by which information is stored and distributed. Under the ECPA, email which is stored on a third party (ie. Google, Yahoo), server for more than 180 days is no longer subject to judicial review of any kind. (18 U.S.C. §§ 2510–2522). Email communications in the present day are most often stored on these third party servers, and are often stored indefinitely. The ECPA’s current language is a clear indicator of the lack of legal interpretation or progression regarding the technological advancements of the modern era. Although diversified and complex, the most crucial areas of importance in regards to criminal investigation and digital forensics are the fourth and fifth amendments.

The two primary focuses for digital investigation in the area of criminal investigation are computer and digital forensics. Although clear guidelines have been set for the seizure of digital evidence, the more nuanced aspects of evidence collection have caused some concern for civil libertarians. For example, the complicated file system formats allow for examination of literally thousands of data files within a computer or cellular phone. Although most criminal investigations have specifications as to what the
forensic analyst is supposed to be attempting to locate, the analyst will inevitably witness or evaluate countless amounts of information that may pertain to extraneous criminality. In instances such as these, much debate surrounds whether the original search warrant or according legal documentation allows for a justifiable “search” of such evidence. Moreover, similar debate surrounds the issue of what procedure an analyst or investigatory agency needs to take to handle this issue. The fifth amendment issue is a bit more convoluted, as it involves the law enforcement community’s ability to compel a citizen to release a password for a device that could potentially store incriminating data. The right to avoid self-incrimination is not necessarily an exigent issue, but with the rapid development of technological advances in the field of data storage, the notion of compelling individuals to essentially unlock a plethora of information with wide-ranging ramifications has the potential to become a huge issue for criminal justice policy and its relationship with constitutional law.

Beginning with *US v Katz* (1967), courts have ruled that the Fourth Amendment protects people, not places. In *Katz*, the Court ruled that the defendant had reasonable privacy when he entered a telephone booth, shut the door, and made a call. Thus, it was illegal for government agents to obtain the content of the phone call without a warrant, even though the recording device was attached outside the telephone booth, the communication was not interfered and the booth space was not physically intruded. The Supreme Court holds that when the defendant shuts the door, his objective expectation is that nobody would hear his conversation and this action is recognized as reasonable by society.
Courts have wrestled over whether inadvertently discovered computer files are properly admissible under the plain view doctrine, or whether they are inadmissible because the search and seizure was beyond the scope of the original warrant. A majority of federal circuits, including the Seventh Circuit in *United States v. Mann*, (2010) have extended traditional Fourth Amendment warrant doctrine to the realm of digital evidence. These courts base their analyses on foundations of Fourth Amendment doctrine: reasonableness, the particularity requirement, and the plain view doctrine.

In contrast, various circuit and district courts have questioned whether traditional Fourth Amendment doctrine sufficiently protects privacy rights in the digital age. In response, multiple court decisions have deviated from traditional Fourth Amendment principles. The Ninth Circuit, through its holding in *US v Comprehensive Drug Testing* (2009), advocated a multi-step prophylactic approach in order to prevent overbroad searches. Similarly, district courts have challenged the constitutionality of the best practices of digital forensics, as seen through the holding of a Pennsylvania district court in *US v Crist* (2008). Additional court decisions have questioned whether searches have exceeded the scope of the warrant by looking at the subjective intent of the investigating analyst or officer. Entire law review articles have been dedicated to the topic of forensic examinations of digital evidence by reputable scholars and law schools, such as “The Physical Computer and the Fourth Amendment”, published by the Berkeley Journal of Criminal Law in 2011.
Chapter 3: The Dynamics of Digital Evidence: A Policy Problem

The obvious stakeholders in this issue are the government, including forensics analysts, investigators, policy makers, and the judiciary; and the individuals who possess devices. Federalist Paper 51, thought to have been written by James Madison, illustrates the classic struggle between the major stakeholders in this problem:

“Ambition must be made to counteract ambition . . . It may be a reflection on human nature, that such devices should be necessary to control the abuses of government. But what is government itself but the greatest of all reflections on human nature? In framing a government…to be administered by men over men, the great difficulty lies in this: You must first enable the government to control the governed; and, in the next place, oblige it to control itself.” (The Federalist No. 51, 1788)

These two major groups comprise the vast majority of Americans living in the 21st century. Additional groups of stakeholders could include wireless service providers, manufacturing companies and corporations, as well as activists concerned with civil liberties in the current “information era” of technology.

Although certainly murky, the overall objective for forward progress regarding this digital forensics within criminal investigation would be the composition and operationalization of a streamlined process for government agencies to follow in regards to these constitutional issues. Legal precedent would expedite the process, but with conflicting legal decisions being made throughout the nation, a unilateral legal precedent seems out of reach at the present moment. Ideally, a successful analysis of this issue would allow for a simultaneously nuanced and broad approach to remaining adherent to the constitutionality of legal searches and seizures. The final product of this analysis
should be adapted as more of a “standard operating procedure” for law enforcement agencies and digital forensics labs, rather than a statute or ordinance. In order to properly analyze the impact of the discipline, the status quo must be juxtaposed with a proposition for development in regards to the constitutional debate. Once this analysis has been completed, the most cognizant approach to ensuring the efficacy and constitutionality of digital forensics practices will be explored in detail.

The status quo essentially leaves the debate regarding constitutional protections and digital forensics in the hands of the judiciary. Once a judicial precedent is established within a certain jurisdiction, agencies will develop protocols and standard operating procedures that are consistent with the legal ruling. The overall efficacy of the current status is the key to determining its validity and worth. An examination of the assorted ramifications in regards to its effectiveness, economic possibility, and political viability will aid agencies and policymakers in determining the potential to rectify the issues at stake for the discipline of digital forensics within the field of criminal investigation.

Judicial precedence allows for consistency within a given jurisdiction, and a more individualistic approach to dealing with a policy problem on a smaller scale. By allowing each jurisdiction to handle the matter on a microscopic level, more attention can be given to the relevancy of the policy and its implications on the agencies and the law enforcement communities involved. Unfortunately, the sheer amount of time spent waiting for legal precedent to be established could be significantly damaging to the progression of digital forensics as a discipline within law enforcement. Additionally, the appeals process may complicate the issue of multiple jurisdictions with different policies based on different legal holdings. Law enforcement agencies will find themselves in a
state of limbo, while their investigatory methodologies and processes are being scrutinized, compared, and inevitably contrasted with those of other agencies across the nation.

Although monetary issues are not directly related to the issue at hand, the status quo enables agencies and local governments to save budgetary funds designated for training and certification. This is primarily due to the fact that the processes and methodologies that are currently being utilized will remain the best practices in the field. The idea of keeping the status quo will discourage agencies from utilizing funds to train new personnel, or to further train experienced personnel on techniques or methods that may test the status quo in regards to legal precedent. Although funding will be saved in the current time frame until legal precedent is established, it will inevitably be used quickly and spontaneously to train forensic examiners and law enforcement personnel on techniques that will inevitably be scrutinized, and potentially modified. This will essentially result in massive amounts of funding being used without a clear idea of its productive value. Leaving the issues in the hands of the judiciary will leave the policy issue largely untouched by any kind of political stratification. Once legal precedent is established, jurisdictions will be politically judged according to their policies and protocols. This could lead to political strife between locally proximate jurisdictions that utilize differing protocols.

A change from the status quo would involve utilizing the leading organizations and collaborative organizations within the fields of digital forensics and law enforcement to establish clear and concise standard operating procedures and protocols for adoption by jurisdictions nationwide. These procedures could be conservative in the sense that
they would air on the side of safety and constitutional responsibility, rather than aggressively pursuing any kind of perceived infringement upon constitutional rights.

The uniformity of the standards would essentially prevent inconsistency throughout the nation in handling increasingly relevant issues throughout the nation in regards to digital forensics. By requiring stringent protocols for adherence with due process, much of the potential legal debate should be nullified by law enforcement’s dedication to a “safe” and conservative approach regarding warrants, subpoenas, etc. Emboldened law enforcement agencies may perceive this as a concession on the part of the criminal justice field, leading to a lack of vigor and aggressive investigation when dealing with digital evidence.

This alternative will not require smaller, local agencies to use funding in order to follow the uniform protocol, and will also allow for law enforcement personnel to utilize training offered by private companies at a discounted rate due to better avenues of cooperation and communication. Although training will be discounted in most cases, agencies will probably feel the need to appropriate larger percentages of funding towards digital forensics training in order to remain autonomous in the discipline.

This alternative allows for local governments to avoid political debate for the most part, as digital forensics is quickly emerging as a necessary element for local law enforcement’s efficiency in investigating a plethora of crimes. Political debate may evolve in regards to how important digital forensics is within their community. Although a consensus has seemingly been reached in regards to its importance, its specific relevance to individual jurisdictions may render this policy alternative a moot point in some areas of the nation.
Chapter 4: Constitutional Faith and Technological Rationality: A Policy Solution

This upgrade to the status quo seems to resemble an effective approach to balancing the capabilities of digital forensic analysts and the relevant constitutional safeguards. With little negative ramifications economically, this plan will allow for uniformity and consistency in developing standard operating procedures to effectively balance the issues at hand. This alternative is politically viable because it airs on the side of caution in dealing with nuanced constitutional debate topics. The policy will not necessitate political or legal debate, and aims to promote investigatory efficiency and productivity. The implementation of this improvement to the status quo should evolve through a series of progressive stages: the initiation of the standard operating procedures and quality assurance protocols, their enhancement of those materials, their dissemination, and further training expositions.

The first stage is both crucial and relatively straightforward. Leading agencies and organizations within the field have already taken substantial steps in creating and publishing procedure and documents that can be easily replicated and utilized on multiple levels on law enforcement. The fundamental purpose of the digital forensics standards published by the International Organization for Standardization (ISO) is to promote good practice methods and processes for forensic investigation of digital evidence. The organization explains that “while individual investigators, organizations and jurisdictions may well retain certain methods, processes and controls, it is hoped that standardization will lead to the adoption of similar if not identical approaches internationally, making it easier to compare, combine and contrast the results of such investigations even when performed by different people or organizations and potentially across different
jurisdictions.” (ISO, 2012) Similarly, the American Society of Crime Lab Directors (ASCLD) is a volunteer not-for-profit organization, whose “board of directors, officers, committee members, and representatives are volunteers who likely have a full-time management position in a crime laboratory” (ASCLD, 2013). By tapping into the expertise and experience of its members, ASCLD has positioned itself to lead the forensic sciences into the 21st century and beyond.

Once the procedures and protocols have been established, the organizations and agencies must be able to clarify the existing legal processes, methodologies, and appropriate documents. The Scientific Working Group on Digital Evidence (SWDGE) brings together organizations actively engaged in the field of digital and multimedia evidence to foster communication and cooperation, as well as to ensure quality and consistency within the forensic community. SWGDE utilizes a Forensics Committee, which is charged with “developing forensically sound techniques by assessing technological challenges and supporting the Digital Forensics community through the establishment of core competencies, best practices, and forensic methodologies” (SWGDE, 2013).

Criminal justice agencies should find the protocols easily accessible through their dissemination and publication through a range of collaborative criminal justice forums nationwide. The National Institute of Justice (NIJ), through its Electronic Crime Technology Center of Excellence, works in partnership with other organizations to establish standards for the collection, preservation, analysis and presentation of digital computer evidence. NIJ’s capabilities “help build capacity in digital evidence among law enforcement at the state and local levels, where the overwhelming majority of law
enforcement activities occur. Additionally, NIJ works to ensure that state and local law enforcement officials have up-to-date knowledge and tools so they can collect digital evidence as efficiently and effectively as possible.” (NIJ, 2010)

In addition to legal process guidelines and procedural outlines, discounted training will be more readily available for law enforcement agencies and personnel who are involved in digital evidence analysis and investigation. The National White Collar Crime Center (NW3C) serves as one of the foremost national and international organizations specializing in the prevention, investigation and prosecution of economic and high-tech crime by providing training, investigative support and research to agencies and entities involved in the prevention, investigation and prosecution of economic and high-tech crime. NW3C “annually provides training to thousands of law enforcement professionals nationwide in the areas of computer crime, financial crime and intelligence analysis, and has developed a comprehensive curriculum for all levels of expertise in the law enforcement community.” (NW3C, 2013)

The International Association of Computer Investigative Specialists (IACIS) is an international volunteer non-profit corporation that is dedicated to education in the field of digital forensics, and is composed of law enforcement professionals representing the federal, state, and local levels of the criminal justice system. IACIS states that “training incorporates forensic methods for searching seized computers in accordance with the rules of evidence and laws of search and seizure, and is dedicated to the education and certification of law enforcement professionals in the field of computer forensic science.” (IACIS, 2013) IACIS provides an opportunity to network with other law enforcement officers trained in computer forensics, to share and learn from other experiences, and
develop a pool of expert assistance to draw upon. Law enforcement agencies may be unable to secure the necessary funding for the training portion of the policy program, which will lead to a growth in work burden on the agencies that are currently involved in digital forensic analysis and investigation. Legal precedent may eventually render the standard operating procedures overly stringent, requiring a recomposition of the guidelines and protocols. Although this will create a problem due to the uniformity of the protocols, the initial stringency and diligence of the guidelines will allow for this shift to be minimal, and not require a paradigmatic shift in policy consideration.

Although the aforementioned analysis of potential solutions may aid in rectifying current constitutional issues within the discipline of digital forensics, the rapid evolution of technology has created both opportunities and pitfalls for law enforcement agencies and personnel. In 2000, the FBI opened its first “Regional Computer Forensics Laboratory” (FBI-RCFL, 2011), which remains a leader in the field of digital forensics and cybercrime analysis across the country. The FBI also remains a leader in the growing relationship between intelligence, counterintelligence, and digital forensics as a discipline. Through the FBI-led national Cyber Investigative Task Force, “the coordinated efforts of twenty law enforcement and intelligence community entities, including the CIA, DoD, DHS, and NSA work together to face the growing threats and significant challenges in the effort to combat cybercrime” (FBI- NJCITF, 2012). Cyber staff has also been embedded within other intelligence community efforts through joint duty and detail assignments. Although large scale efforts such as these provide a unique and magnanimous look into the future of digital forensics and cyber crime analysis, a closer look at an area that strikes closer to home also yields inspiring results. In March
2011, the Office of the District Attorney of Lehigh County joined in a partnership with DeSales University to establish a county-wide computer crimes task force as well as a full-scale digital forensics laboratory on the Center Valley, Pennsylvania campus of DeSales University. As of November 2012, the Lehigh Computer Crimes Task Force (L3CTF) has handled more than 400 cases and 700 pieces of digital evidence. The impact of the task force’s work has been felt throughout Lehigh County, as well as the surrounding area, and has significantly eased the burden off of the regionally based Pennsylvania State Police Computer Crimes Task Force. The L3CTF has expedited the investigative and prosecutorial efforts of agencies, as well as expanding the horizons of what law enforcement can accomplish with a vision of exponential growth and modernized tactical efforts. Although the task force effectively shows the highlights of what digital forensics adds to the efforts of law enforcement personnel and criminal investigation as a whole, it also provides a unique look into the impending crisis that the discipline of digital forensics currently finds itself.
Chapter 5: The Impact of Mobile Phone Forensics

Much of the last decade’s recent progress in digital forensics is quickly becoming irrelevant due to the advances and developments of the electronic industry. The dynamically evolving size and flash quality of storage within electronic devices can no longer be easily imaged or removed by the current methods and techniques of forensic analysts. The L3CTF is consistently dealing with the issue of recently developed pieces of evidence that are simply not as easily accessible as they were as recently as twelve months ago. Operating systems and file formats are continuously evolving and multiplying, representing a dramatic shift from the relatively mainstream few systems and formats that were previously in existence and use. An increasingly popular issue is the necessity for multiple types of analysis on a variety of pieces of evidence for single cases or incidents. This issue exacerbates the challenge of corroborating and correlating relevant pieces of evidence to the facts and circumstances of a widely diversified caseload. Modern technological revolutions have brought cloud computing and encryption into the homes, classrooms, and quite honestly, the hands of the majority of American citizens throughout the nation. The pervasiveness of these developments have not only complicated data access and retrieval from complex hard drive sources, but also from mobile devices, which comprise the vast majority of the L3CTF’s pool of acquired evidence for forensic analysis.

In addition to the qualitative issues of modern cell phone analysis, the quantitative issues present significant challenges to the discipline’s law enforcement functions. There are thousands of cell phone models in use which use a plethora of operating systems, and hundreds of thousands of downloadable applications. The relatively simplistic notion of
connecting a mobile device for analysis is continuously complicated by the myriad of
collectors and chargers currently available within the market. These may seem to be
relatively monotonous developments and changes, but mobile phones have been
solidified as the primary tool of criminals and terrorists alike. The fact remains that the
principled and nuanced data extraction of data from cell phones must become a priority
for digital forensics’ contribution to law enforcement, with no actual standard
methodology to extract the information. The advent of “smartphones” has presented
digital forensic analysts with some of the most difficult and important problems regarding
the extraction of evidentiary data. A large number of new forensic tools exist to aid in
data extraction, decryption, and detailed analysis from a wide array of devices, including
Blackberry, Apple, and Android products. Although these tools are revolutionary and
helpful, the rapid evolution of technology throughout the mobile device market allows for
additional challenges.

One of the basic challenges presented by smartphones is the nature of the
technology itself. Smartphones essentially function as computers, and utilize varying
arrays of hardware and software configurations that complicate forensic analysis.
Additionally, passcodes and protective locking mechanisms present a unique issue for the
analysis of mobile devices. Some mobile data extraction tools reveal simple passcodes
automatically for devices that have been on the market for a substantial period of time,
while newer phones are often impossible to forensically access with a commercial data
extraction tool. Complicated passcodes pose additional threats, as they generally protect
specific files with particular content. Although some data will be available for analysis,
prioritized information is often difficult to access. The process of bypassing a device’s
pattern lock, typically on an Android device, is often possible with standard forensic analysis tools. However, the continuous evolution of smartphone technology proceeds to complicate the methodologies used by the forensic tools in many cases. Ironically, forensic analysts and law enforcement personnel have had similar problems with devices of a significantly lesser quality. Pre-paid phones are often difficult to analyze because of their diversified manufacturing process. In some cases, the manufacturer of the phone does not actually design or build the memory in a way that is accessible for the typical forensic tool. Forensic examiners can attempt to decode the content and access deleted data, but the process is rarely standardized and typically requires complicated ad-hoc processing techniques.

Smartphone applications present further issues for analysis due to the diverse nature of their implementation and production. Applications can range from basic and common tools such as social networking and communicating to more sophisticated purposes like navigating and banking. Most cutting edge forensic tools have only recently begun to support applications for mobile devices, and require file extraction and decoding. Although oftentimes possible, these processes are complicated by the multi-faceted composition and organization of the applications themselves. Data present within mobile device applications are of potentially significant evidentiary value, and the challenges presented by these applications can greatly impact criminal investigations. The linchpin of mobile forensics’ impact on criminal investigation resides in the validity and soundness of the forensic tools. A plethora of methodologies exist that fundamentally alter the state of the device being processed, effectively undermining the forensic nature of the analysis. These methodologies are rarely utilized, but require a detailed record of
the actions and procedures utilized to present an accurate depiction of the examination in the event of a trial or similar assessment.

The research and development of new extraction methods have allowed examiners to utilize device-specific processes to enhance examinations of mobile devices. These tools are the result of years of research, ranging from the exploitation of the vulnerabilities of operating systems to the analysis and engineering of devices’ protocols and manufacturing systems. Due to the advanced nature of the tools, extensive training is required to solidify the forensic soundness of the analysis. The research and training components serve as the backbone of modern digital forensics, and they must evolve in the same fashion that the challenges of smartphone technology have in recent years. Forensic challenges to mobile device analysis will persist, and the practitioners tasked with utilizing digital forensics within the field of criminal investigation must persist in a similarly aggressive manner.
Chapter 6: An Impending and Necessary Paradigm Shift

The development and cultivation of forensic tools also pose a problem within the next few and important years of digital forensics’ relationship with law enforcement. Although the market for tools is growing by some metrics, it is consistently controlled by a handful of relatively minor companies that face incredibly difficult costs for research and development. Despite the best efforts of these companies, their tools and products are seemingly always out of date and lacking in coverage. The obvious method of tending to this dilemma is to purchase a wide array of tools that specialize in different facets of forensic analysis in an effort to supplement the various inconsistencies throughout the market, but this solution is fiscally inconceivable for the vast majority of well-intentioned law enforcement agencies, such as the L3CTF. Budgetary concerns riddle the nation in a wide variety or arenas and forums, but the current strain on the public sector to remain competent and diligence during an era of cutbacks and financial constraints is certainly at the forefront of the impending crisis within digital forensics. In addition to posing problems for law enforcement in its pursuit of tools and analytical methods, the budgetary constraints on the public sector poses a more dramatic threat to training and accreditation. Instruction materials and professionals are currently provided at incredibly high costs, even to law enforcement officials tasked with digital forensics duties. A commonly promulgated myth suggests that training be reserved for higher levels of forensics that transcend the norm of what baseline digital forensic analysts most commonly deal with on an everyday basis when dealing with criminal investigation. In reality, a proficient investigator that is tasked with leading investigations on a regular basis must undergo extensive training, both instructive and on-the-job. With the current
budgetary squeeze, it is easy to understand the depth of the issue that digital forensics and
law enforcement personnel currently find themselves in. To further complicate matters, a
wide range of legal challenges are currently accruing to test the process of digital
forensics within the purview of criminal investigation. To cite an example, in the 2009
case of *US v. Comprehensive Drug Testing, Inc*, the Court dramatically limited the scope
of federal warrant searches. Numerous ensuing cases have followed the case’s precedent
by restricting the amount of digital evidence that can be acquired and searched without
prolonging and intensifying the process of warrant acquisition and subsequent
investigation.

Although the impending crisis is nuanced and foreboding, the successes of the last
decade can work in conjunction with revolutionary research initiatives to ensure the
growth of digital forensics’ impact on criminal investigation. Research needs to become
more streamlined, efficient, coordinated and funded if the discipline wishes to continue
with significant growth in and of itself, while retaining the crucial value that it possesses
in relation to criminal investigation. The key to improving research development and
funding is to adopt reliable standards for data and modulation for forensic processing.
Although these represent complex notions, the most effective means of summarizing
these notions resides in the concepts of prioritized analysis, scale, and validation. Ana
Cerezo, a notable contributor to workshops on incident analysis, maintains that
“prioritized analysis involves a triaged approach in which the forensic acquisition and
analysis stages are ordered in a way so as to present the analyst with paramount
information in the most expedient way possible” (Cerezo, 2009). This is most easily
realized by utilizing mobile forensics devices that are designed to process data quickly
and efficiently as soon as new information is encountered. The concept of triage-oriented prioritized analysis is not necessarily a new one, but has not truly reached the radar of most academic and commercial entities involved in the discipline of digital forensics. Scale is an important concept to identify and improve upon early in the research process. In order to achieve the goal of identifying and improving upon the notion of scale within the digital forensics world, researchers must work to enhance and promulgate a variety of tools and methodologies that work within an environment of large quantities of data. Although seemingly overzealous, this goal can be attained through an early identification of large-scale processes early in the research phase, rather than a hasty attempt at achieving wide-sweeping methodologies further along in the development phase. Validation is a simple concept, but the actual realization of the verification of scientific reliability requires dedication and persistence. Analysts working within the discipline, as well as law enforcement officials tasked with digital forensics and cybercrime investigation duties, need to hold themselves to a higher standard through regular and systematic levels of testing and tool result reproducibility. Once again, the onus must be placed on researchers and reviewers to require constant testing with significant data sets in order to produce reportable rates for standardized forensic tools.

Although research is the key to growth and stability in the discipline of digital forensics, the real key to assessing the future of the application of digital forensics to many areas of criminal investigation is disappointingly political. Although the politicization of criminal justice is nothing new, the current economic situation necessitates a political discussion about budgets, fiscal responsibility, and bipartisanship. Lehigh County has provided, in a way, an example of how future growth can be achieved
while remaining fiscally responsible as a government entity. While agreeing to more than 3.5 million dollars in governmental spending cutbacks for the fiscal year of 2013, the county continues to dedicate and divert significant funding to the Digital Forensics Laboratory of Lehigh County and the L3CTF. This decision required much political debate and stratification, but ended with the determined conclusion that progress and growth within this specific discipline within the law enforcement community must continue to meet the needs of the general public. Domestic law enforcement agencies must rise to the occasion, and with the help of research and development, continue to collaborate with other professionals within the privatized digital forensic field and similar law enforcement-centric entities nationwide.
Conclusion

The application of digital forensics to criminal investigation is not without its flaws, shortcomings, and evident weaknesses. This analysis has highlighted some of the problematic components of digital forensics in the context of future developments within the field of criminal justice. Although rationality clearly demonstrates the need for improvement, adjustment, and overall versatility regarding research and communication, the pitfalls of the current status quo within the discipline are much less glaring than the potential benefits. Digital investigation has demonstrated its value in enhancing the expediency, efficacy, and overall quality of criminal investigation through a wide variety of means. Although the analysis put forth through this research demonstrates the need for a paradigmatic shift in focus, rationality dictates that incremental change will play the primary role in the realization of the future vision for digital forensics.

The future of criminal justice, as an aggregate whole, depends on widespread cooperation and transparency. The balance between faith in the American justice system and the rational advancement of technology is, in fact, easily attainable. Magistrates and criminal justice practitioners need to embrace the challenge of adapting to the changing face of crime, and to do so responsibly. By utilizing the fusion of faith and reason in a unique way, criminal investigators will be able to fundamentally influence the way that the legal and political systems interact with technology and crime. With a paradigmatic shift towards research, communication, and training, a clearly delineated set of goals can, and will, be achieved. Court cases will be sound, and the tangential investigation of innocent people will be mitigated. Costs will be low, public danger will be low, and officers involved in digital investigation will be safe. Digital evidence will be limited to
what is necessary and relevant, will adhere to Constitutional standards within jurisdictional boundaries, and will still remain a critical component to criminal prosecution. Most importantly, the public will have a high level of confidence, or faith, in the integrity and fairness of the judicial system. This faith will coexist with the swift, certain, and determined efforts of a technologically equipped law enforcement community. Just as technology has proven to define entire generations and eras, digital forensics promises to define the future of criminal investigation and homeland security.
References


Frye v. United States, 293 F. 1013 (1923)


*United States v. Mann*, 592 F. 3d 779 (2010)