LAWYERS' KNOWLEDGE OF, ATTITUDES TOWARDS, AND EXPERIENCE WITH DIGITAL EVIDENCE

by

Danielle M. Crimmins

A Dissertation

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy

Department of Computer & Information Technology

West Lafayette, Indiana

December 2021

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Kathryn C. Seigfried-Spellar, Chair
Department of Computer and Information Technology

Dr. Marcus K. Rogers
Department of Computer and Information Technology

Dr. Spencer Headworth
Department of Sociology

Dr. Anne Traynor
Department of Educational Studies

Approved by:
Dr. Kathy Newton

To all those who encouraged me and believed this was possible, thank you.

ACKNOWLEDGMENTS

After all the years of graduate school, and the many papers I've written, there is nothing I have looked forward to writing more than this. There are many people I would like to acknowledge, and I would not be here without you all.

I would first like to thank Dr. Kathryn "Kate" Seigfried-Spellar. As a senior in college at The University of Alabama majoring in Criminal Justice, I was unsure of my career path. As luck would have it, I met a new faculty member who researched cybercrime, and from there, the trajectory of my career and future changed. It has been a long 10 years since then, and I might have procrastinated just a bit, but to say I am grateful would be an understatement. Because of her, I found a love for research and asking questions. She taught me how to continue adding to my research "toolbox" and always motivated me to persevere and finish! I am forever grateful I met you, because without you, I truly would not be here.

Next, I would like to thank Dr. Marcus Rogers. He always asked the tough questions and forced me to look at things critically. Most importantly, he encouraged me to find my voice – even when that voice disagreed with previous research. I am grateful for the questions and guidance over the years. I would like to thank Dr. Spencer Headworth. His endless supply of references and resources were invaluable during this process. I appreciate his guidance and thought-provoking questions – both of which made this dissertation better. Thank you to Dr. Anne Traynor. I am grateful she agreed to serve on my committee, even though my area of interest is very different from her own. She quickly and thoughtfully responded to all of my statistical or measurement questions and I am very grateful.

In addition to my wonderful committee, my time in graduate school provided me with long-lasting friendships. Thank you to my grad school family for all the laughs in the lab, stats

homework at the Pint, and late nights at “Club Bays,” and everything in-between. Tatianna, my birthday twin and “virtual officemate,” I don’t think I would have finished without our endless stream of texting. Thanks for all the laughs and encouragement. Thank you to Marie, Nadine, and my former NIJ colleagues for the encouragement and mentoring during this process and always reminding me “a done dissertation, is the best dissertation!”

I have been blessed to be surrounded by so many supportive and encouraging friends and family during this process as well. To all my family and friends who are not listed, you know who you are, thank you for your encouragement. And finally, thank you to my Dad, Mom, and sister for always believing I could do this and reassuring me when I doubted myself. I would not be where I am without your love and support. Now, let’s celebrate!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY

Computer Crime: “crime in which the perpetrator uses special knowledge about computer technology to commit the offense” (Holt, Bossler, and Seigfried-Spellar, 2017; p. 661)

Cyber Crime: “crime in which the perpetrator uses special knowledge of cyberspace” (Holt, et al., 2017; p. 664)

Courtroom Actors: individuals in the courtroom which includes, the judge, jury, and lawyers.

Defense Counsel: “defense counsel” means any attorney – including privately retained, assigned by the court, acting *pro bono,* or serving indigent defendants in a legal aid or public defender’s office – who acts as an attorney on behalf of a client being investigated or prosecuted for alleged criminal conduct, or a client seeking legal advice regarding a potential, ongoing or past criminal matter or subpoena, including as a witness” (ABA, 2015)

Digital Evidence: “information that is stored or transmitted in a binary format that may be relied on its court” (NIJ, 2007, para. 2)

Digital Forensics: “the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation 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 unauthorized actions shown to be disruptive to planned operations” (Palmer, 2001, p. 16)

Forensic Science: “the application of scientific principles and techniques to matters of criminal justice, especially as relation the collection, examination, and analysis of physical evidence” (Merriam-Webster, n.d.)

Prosecutor: ““prosecutor” means any attorney, regardless of agency, title, or full or part-time assignment, who acts as an attorney to investigate or prosecute criminal cases or who provides legal advice regarding a criminal matter to government lawyers, agents, or offices participating in the investigation or prosecution of criminal cases” (ABA, 2015)

LIST OF ABBREVIATIONS

AAFS	American Academy of Forensic Sciences
ABA	American Bar Association
BJS	Bureau of Justice Statistics
CLE	Continuing Legal Education
DF	Digital Forensics
DFRWS	Digital Forensic Research Workshop
FS	Forensic Science
GB	Gigabyte
ICR	Internet Crime Report
IoT	Internet of Things
IRB	Institutional Review Board
LE	Law Enforcement
MB	Megabyte
NCFI	National Computer Forensic Institute
NCSS	National Computer Security Survey
NIST	National Institute of Standards and Technology
NW3C	National White Collar Crime Center
OSAC	Organization of Scientific Area Committees for Forensic Sciences
PC	Personal Computer
QDA	Qualitative Data Analysis
TB	Terabyte

ABSTRACT

There continues to be a rapid proliferation of technological advancements and continued increase in digital evidence. Digital evidence may be a vital part of a case; however, it is difficult to present a highly technical process to novice individuals Therefore, it is important to determine how courtroom actors understand digital evidence. The goal of this mixed method study was to investigate lawyers, both prosecutors and defense attorneys, attitudes towards, knowledge of, and experience with digital evidence. The current study followed an explanatory sequential design, which consisted of two phases. For phase one, snowball sampling was used to solicit participation in the online, anonymous survey which included questionnaires and open-ended questions. The final sample included 11 prosecutors and five defense attorneys. Results indicated there is no difference in prosecutors and defense attorneys' knowledge of digital evidence. Overall, results indicated prosecutors have a higher opinion of digital evidence. In addition, based off moderate effect sizes, experience with digital evidence differed between prosecutors and defense attorneys. Prosecutors used digital evidence more at trial and in plea agreements compared to defense attorneys. Based off of the write-in responses, emerging themes suggested a lack of understanding of digital evidence by lawyers and judges, and prevalence of digital evidence with regards to type of data and amount of data. The goal of phase two was to further explore and explain the emerging themes from phase one. Phase two used purposeful sampling to recruit four lawyers (two prosecutors and two defense attorneys) who had experience with digital evidence. Results from the interviews confirmed findings from phase one regarding the prevalence of digital evidence and a lack of understanding of digital evidence. In addition, a lack of resources was identified, which included a lack digital evidence training for lawyers and judges. Although consistent with the samples of previous research, a main limitation of the current study is the sample size for both phase one and two. A small sample size withstanding, the current study was able to draw triangulated inferences based on the three strands of data collected using a mixed methods approach. The triangulated findings add to the validity and reliability of current study despite the small sample size. The current study found lawyers are concerned the jury does not understand digital evidence and also puts too much weight on such evidence. Therefore, future research should examine jurors' understanding of digital evidence and the weight of digital evidence in their decision-making. There is also a need to investigate

why judges are falling behind in the understanding of digital evidence. Also, the development, implementation, and evaluation of digital evidence training for prosecutors and defense attorneys is needed to ensure both groups understand digital evidence. Additionally, future research should examine if more trainings and a better understanding of digital evidence effect attorneys' opinions and attitudes toward digital evidence and then ultimately the use of such evidence.

CHAPTER 1. INTRODUCTION

Within the last 20 years, technological capabilities have rapidly increased. In the early 2000s, the first Apple stores opened in the United States. Along with the release of the Apple iPod, Microsoft released the first Xbox, and the first USB flash drive was introduced with 4 gigabytes (GB) of memory capacity (Computer History Museum, 2019). At the time, these advancements were monumental; however, these devices were expensive and therefore not accessible by everyone. In 2000, approximately 50% of households in the United States had a computer compared to nearly 90% in 2016 (Statista, 2019). In less than two decades, smart phone ownership went from 0% in 2002, 35% in 2011, to nearly 80% in 2018 (Pew Research Center, 2018). Not only has use and accessibility increased, but so have capabilities. Apple has now released 13+ iPhone and is currently on the 7th generation iWatch; USB flash drives have 265GB capacity, and nearly 90% of households have a PC, which holds more than a terabyte (TB) of data (Computer History Museum, 2019; Statista, 2019). The rapid increase in technological capabilities and usage, in a relatively short period of time, has had an impact on society.

There are both positive and negative outcomes due to the increase in technology use and capabilities. Mobile devices now have the power to serve as portable computers allowing society to be constantly connected with family, friends, and in business. The supreme court has even considered smart phones "mini" computers (*California v. Riley, 2014).* However, these advancements also created a new arena for crime. In recent years, computer-related crimes garnished worldwide media attention, such as the data breach of Home Depot's computer system, which exposed data from over 50 million credit cards (Armerding, 2018). Additionally, a congressman, Anthony Weiner, was charged and convicted of sending obscene material to a minor (Weiser, 2017; *United Sates of America v. Anthony Weiner*). These two examples illustrate how technology is used as a *target* and *means* to engage in illegal activity, according to Holt, Bossler, and Seigfried-Spellar (2017). In the Home Depot example, the computer systems were *targeted* for sensitive data (credit card data); and in Anthony Weiner's example, a mobile device was used as a *mean* to send obscene photos to a minor.

The number of crimes where a computer was targeted and/or used to facilitate a crime has increased. In 2005, the Bureau of Justice Statistics (BJS), National Computer Security Survey (NCSS), examined the prevalence and impact of cyber-attacks on businesses in the United States. Results indicated 67% of the 7,818 businesses surveyed reported at least one instance of cybercrime (BJA, 2005). In 2013, the Internet Crime Report (ICR) received a total of 262,813 complaints resulting in a reported loss of $781,841,611 (ICR, 2013). Recently, in 2017, the ICR received a total of 301,580 complaints with a total loss of $1,418.7 million. Statistics demonstrate the volume of computer crimes, as well as the massive loss incurred by victims. Further, a recent study by Gallup found 67% of Americans worry about being the victim of cybercrime compared to 17% of American who worry about being the victim of murder (Brenan, 2018).

Not only can computers serve as the *target* of a crime (e.g., ransomware) or the *means* to facilitate a crime (e.g., child pornography), but a computer can also be involved in a case through its "incidental role or involvement" (Holt et al., 2017; p. 20). A computer can provide evidence to assist law enforcement in the investigation and convictions of crimes. For instance, during the commission of a burglary, the suspect's cellphone is powered on which investigators could then use to put a suspect near the scene of a crime through GPS or cell site location data.

Regardless of whether a computer was *targeted*, used as *means* to commit a crime, or *incidental* in the commission of a crime, the computer or mobile devices is of evidentiary value to law enforcement in their investigation and subsequently to the courts. Such evidence, referred to as digital evidence, may be used to prosecute a suspect or conversely, to prove the innocence of a suspect. Digital evidence is "information that has been processed and assembled so that it is relevant to an investigation and supports a specific finding or determination" (Easttom, 2017; p. 10). That is, digital evidence is information that is processed and used to support an investigation, such as GPS location from a mobile device, heartbeat data from a smartwatch, or photos from social media to name a few. In comparing digital evidence to physical evidence, Goodison, Davis, and Jackson (2015) argued digital evidence "has a wider scope, can be more personally sensitive, is mobile, and requires different training and tools" (p. 3).

Researchers postulated all cases will eventually include some form of digital evidence (Clifford, 2001; Saleem, Baggili & Popov, 2014; Sammons, 2015). For example, a search warrant was used to obtain a Fitbit from a woman who was murdered in Connecticut (Taylor,

2017). Results from the Fitbit showed movement of the women which does not line up with the timeline of her death provided by her husband (Taylor, 2017). The results from the Fitbit, coupled with Facebook activity (also digital evidence), led to an arrest warrant for the woman's husband (Taylor, 2017). Additionally, in a murder case, music was streaming from an Amazon Echo (Augenstein, 2016). A search warrant was used to gain access to the device and an investigator was able to extract data from the Amazon Echo (Augenstein, 2016). Fitbit and Amazon Echo are just two examples of digital evidence, specifically the Internet of Things (IoT) devices, used in an investigation that ended up in criminal proceedings.

Despite the increased discussion on the importance of digital evidence in court cases in recent years and the multitude of digital devices, the conversation is not new. In 2000, researchers advocated the importance of promoting "awareness of electronic crimes" among judges' and prosecutors (Stambaugh et al., 2000, p. 2). Further, Taslitz (2004) suggested "every lawyer must know how to find evidence hidden in the bowels of computer networks" (p. 4).

Sammons (2015) stated "the pinnacle of the forensics process is the presentation of the findings to a judge or a jury" (p. 9). The final step in the digital forensic process[1] is the presentation phase, which refers to the legal context of a case. For example, if a suspect is charged with possession of child pornography, the prosecutor might introduce digital evidence which shows the suspect had pornographic images of a child on their computer. In this example, the digital forensic expert or investigator would testify to the process of locating the file, how the expert/investigator can determine it was on the suspect's computer, and the authenticity of the investigation, to name a few. Hayes (2014) suggested because anyone could be a juror (e.g., stay at home mother, teacher, CEO), expert witnesses are tasked with explaining technical processes to lay individuals or any individual not part of the digital forensic profession. Sammons (2015) advanced the point made by Hayes (2014) by suggesting it is extremely difficult to describe technical processes (e.g., imaging of a hard drive or mobile device) to individuals with little technical knowledge. Sammons (2015) further suggested an outcome of a trial could easily rely on a jury or judge's understanding of technical processes and/or evidence. However, it could also be argued the outcome of the trial could depend on the lawyers', both prosecution and defense, understanding of the digital forensic process and/or evidence. The American Bar Association

[1] The Digital Forensic Process includes preparation, identification, preservation, collection, examination, analysis, and presentation (Rigby and Rogers, 2007)

(ABA) stated lawyers have an ethical obligation and are responsible for knowing the evidentiary value of digital devices and the boundaries set forth by the law with regards to the digital forensic investigation (ABA, 2017). Thus, it is important for both civil and criminal, defense and prosecution, lawyers to understand digital evidence.

1.1 Problem Statement

Previous research examined how forensic evidence is understood in the courtroom by the judge (Kessler, 2010; Losavio, Adams & Rogers, 2006), jury (Hans, Kaye, Dann, Farley, & Alberston, 2011; Wilcox and NicDaeid, 2017), and lawyers (Holmgren, 2003; Losavio et al., 2008; Keeling, Elmaghraby, Higgins & Shutt, 2008; Cashman & Henning, 2012; de Keijser & Ellfer; 2012). Lawyers introduce forensic evidence into the courts, and therefore, their understanding is imperative. Forensic Science refers to the use of science in application to the law; that is, the use of the scientific process to gather and examine the evidence which is then heard by a judge and jury (Sammons 2015; Holt, et al., 2017; National Institute of Justice [NIJ], 2019). Examples of forensic science evidence include DNA, trace evidence, and impressions. The overall goal of forensic evidence, including digital evidence, is to provide the courts with reliable evidence as to the result of scientifically proven methodologies (Sammons 2015; Holt et al., 2017; NIJ, 2019). Forensic evidence has little to no value if it is not admissible in court (Sammons, 2015).

Researchers and practitioners have discussed the importance and utility of digital evidence in the courts (Losavio et al., 2008; Kessler, 2010; Goodison et al., 2015). In 2002, Palmer stated as lawyers, judges, and jurors better understand the technical process of computer evidence, there will be a need for "a more rigorous approach to digital forensic analysis." In 2006, Losavio and colleagues postulated as lawyers become knowledgeable on technical evidence, judges will see an increase in challenges to digital evidence. Losavio and colleagues (2008) investigated the experience and use of digital evidence of Northern Kentucky and Cincinnati lawyers through a self-report survey. Results indicted digital evidence was rarely utilized in criminal and civil state courts (Losavio et al., 2008). In 2010, Kessler investigated judges' awareness, understanding, and application of digital evidence; results indicated: judges are aware of the importance of digital evidence but *not* aware of all types, believe digital evidence should be authenticated (like other evidence), and are aware of how easy it is to alter or misinterpret digital evidence. To date,

the author has not found literature which examines how jurors understand digital forensic evidence and there is limited research regarding judges' and lawyers' understanding.

Losavio and colleagues (2008) anticipated an increase in digital evidence in the future. At the time of the aforementioned studies, the advancements in mobile technology and smartphones were just on the rise and not included in the study. More recently, Goodison and colleagues (2015) suggested defense attorneys will *eventually* become knowledgeable which will result in better challenges to digital evidence. However, there is no recent empirical research which measures attorney's knowledge of digital evidence. Additionally, the sample from the Losavio and colleagues (2008) study was limited to lawyers in Northern Kentucky and Cincinnati; a less regionally focused and more representative sample of lawyers may provide a clearer picture of the current state.

In a panel discussion conducted by RAND and the Police Executive Research Forum (PERF), 11 law enforcement digital forensic experts, two prosecuting attorneys, one privacy advocate, and two industry members discussed challenges of digital evidence (Goodison et al, 2015). The panel concluded defense attorneys were the least knowledgeable regarding digital evidence (Goodison et al., 2015). However, it should be noted defense attorneys' opinions were not included in the discussion and the purpose was not specifically to address the needs of lawyers with regards to digital evidence. While this is just one example of defense counsel not being present, Headworth and Ossei-Owusu's (2017) suggested there is a lack of qualitative research on criminal defense attorneys.

In a recent case review, Novak (2020) found of 147 United States District Court of Appeal cases, 22 appeals pertained to the science of digital forensic evidence. Specific reasons for appealing digital forensic evidence included probative value, authenticity, hearsay, relevance, and scientific merit (Novak, 2020). Although researchers and practitioners continue to propose defense attorneys' ability to challenge digital evidence is forthcoming, there is a lack of empirical research which seeks to examine defense attorney's understanding of digital evidence. Further, there is no research that directly compares prosecutors and defense counsels' knowledge and experience of digital evidence.

1.2 Statement of Purpose and Scope

The overall purpose of the current study was to investigate lawyers' attitudes towards, understanding of, and experience with digital evidence. There are a few aspects of the problem which were beyond the scope of the current study. First, within the academic literature, media, and government documents, the terms computer crime and cybercrime are often used interchangeably. That is, some *computer crime* statistics also encompass crime statistics that could be categorized as *cybercrimes* because the Internet was involved. Holt and colleagues (2017) defined computer crime as "crime in which the perpetrator uses special knowledge about computer technology to commit the offense" (p. 661) and cybercrime as "crime in which the perpetrator uses special knowledge of cyberspace" (p. 664). Although it would be beneficial for the terms to be clearly defined and used consistently, the debate and confusion surrounding these terms were beyond the scope of this paper. The main focus of the current study was digital evidence. After a crime is committed, an investigator may analyze and review digital evidence which connects a potential suspect to a crime and/or eliminates a potential suspect. Lawyers' knowledge of such digital evidence is the focus of the current study.

Digital forensics is an umbrella term which includes several subdisciplines such as computer forensics, mobile forensics, and network forensics, to name a few (Barmpatsalou et al., 2013; Casey, 2011). The current study aimed to determine lawyers' understanding of, attitudes towards, and experience with digital evidence, not specific technical knowledge of networks and digital devices.

Digital evidence may be used in the courts and a digital forensic expert may give testimony regarding such evidence, as previously discussed. Concerns surrounding the admissibility of digital forensic evidence and qualifications of expert witness testimony are discussed within the literature but were beyond the scope of the current study, as the current study focused on lawyers. Further, computer crime is an international problem and digital evidence makes its way into courts around the world. However, the current study only focused on the United States. Specifically, within the United States, the current study aimed to investigate criminal defense lawyers and prosecutors with active standing with the American Bar Association (ABA).

Although the ABA states digital evidence is important in civil cases, such as a civil lawsuit, an employee leaving a company to work at a competitor, or divorce cases (2017), civil attorneys were not included in the current study for two main reasons. First, the United States Constitution

and subsequent cases guarantee citizens the right to defense counsel, in criminal trials. Second, civil litigation often deals with monetary claims compared to criminal litigation which potentially takes away an individual's freedom. The absence of civil attorneys is further discussed in Chapter 6 as an area for future research.

In addition, there is minimal research on judges and no research on jurors' understanding and perception of digital evidence, at this time. However, it should be noted, there is an extensive body of literature which examines jurors' understanding of various types of evidence (e.g., DNA; Schklar & Diamond, 1999; Hans et al., 2011) and how to best communicate with jurors (Jackson, Kaye, Neumann, Ranadive, & Reyna, 2015), to name a few. As suggested by Howes (2015), jurors are difficult to study as there are limitations to soliciting individuals who served in an actual trial. Researcher have attempted to circumvent this obstacle with various methodologies including mock trials with jury eligible individuals (Hans et al., 2011) and the use of case transcripts (Schweitzer & Saks, 2007). Research suggests judges, lawyers, and investigators are also vital components of the criminal justice process (Howes, 2015). Judges' and jurors' understanding, and perception of digital forensic evidence is needed in the literature; however, judges and jurors were beyond the scope of the current study.

1.3 Significance

When considering the prosecution and defense of citizens in the United States, the constitution and subsequent seminal cases provide guidance. The 6th amendment "guarantees the rights of a criminal defendant, including the right to a public trial without unnecessary delay, the right to a lawyer, the right to an impartial jury, the right to know your accuser, and the nature of the charges and evidence against you" (U. S. Constitution). In *Gideon v. Wainwright 372 U.S. 335 (1963)* the Supreme Court ruled "the right to counsel is a fundamental right to ensure a fair trial and applies to the states through the Due Process Clause of the Fourteenth Amendment" (U.S. Constitution). This applies to criminal defendants, but not individuals involved in civil or administrative proceedings. Further, in *Strickland v. Washington, 466 U.S. 688* (1984), the courts established a two-prong test to determine whether court-appointed attorneys provided effective counsel. The first prong, the error prong, determines if the defense was sufficient; and the second prong, the prejudice prong, looks to determine if the subpar counsel affected the outcome of the case. Failing the two-prong test is grounds for a new trial.

Losavio and Losavio (2017) discussed the implications of in inadequate defense with regards to digital forensics and stated the following:

> Under the American legal system, the failure of effective assistance of counsel due to issues relating to digital forensics and evidence can be grounds to reverse and vacate a judgment and sentence; conversely, unrecognized it may lead to the conviction of an innocent party (p. 170)

This quote exemplifies the present need to better understand how lawyers understand digital evidence. Without an adequate defense or knowledgeable prosecution, innocent individuals may be erroneously convicted. Guilty individuals may also go free due to an ill-equipped prosecution. For attorneys to effectively do their jobs, it is imperative to understand digital evidence and the multitude of data which can be found on a digital device.

The need for defense attorneys to understand evidence is illustrated in the infamous O.J. Simpson trial. O.J. Simpson was exonerated for murdering his wife and her friend. Simpson's defense lawyer cross-examined the forensic expert for eight days, which included questions on nearly all of the DNA evidence and police procedural issues in handling of such evidence (Forensic Outreach, 2016). Over two decades later, in a recent article, one of the prosecutors from the O.J. Simpson trial discussed the DNA evidence from the case. The prosecutor said explaining the DNA evidence to the jury was difficult and at the time DNA evidence was not widely accepted (Siemasko, 2016). DNA evidence was only first introduced as evidence in a criminal case in the United States in 1986 (Dennis & Cormier, 2005), which was nine years before the O.J. Simpson trial. The O.J. Simpson trial illustrates a defense with an understanding of DNA evidence coupled with a prosecutorial team who struggled to present the DNA evidence to the jury, which could be due to a lack of understanding or due to the novelty of the forensic evidence at that time.

Although the forensic science disciplines are often integrated into the criminal justice system, through the entering of forensic evidence in court, lawyers and judges are not trained to understand the scientific methodologies behind each type of forensic evidence during their law school education. This point was exemplified at the American Academy of Forensic (AAFS) 2019 annual meeting when Hughes, a defense attorney, and colleagues (2019) called for the need of forensic training, specifically DNA and digital evidence, for defense attorneys because they (lawyers) are not able to be an expert in all of the forensic fields. Similarly, Howe (2015)

suggests future research should aim to investigate how investigators', lawyers', and judges understand forensic science evidence. Additionally, in the 2009 National Association of Science (NAS) report on forensic science the United States the following quote was posed:

> lawyers and judges often have insufficient training and background in scientific methodology, and they often fail to fully comprehend the approaches employed by different forensic science disciplines and the reliability of forensic science evidence that is offered in trial. Such training is essential (p. 27).

The influential NAS 2009 report coupled, with researchers' suggestions, amplifies the need to better understand judges' and lawyers' understanding of and experience with forensic science and provide trainings where there is a lack of knowledge.

Thus far, previous research focuses on prosecutors, as they are often included in panel discussions or research studies, and there have been various resources written with prosecutors in mind (*see* NIJ, 2007). Further, the National Computer Forensic Institute (NCFI), is designed to train law enforcement, judges, and *prosecutors* on digital evidence, funded by the federal government. Similarly, the National White Collar Crime Center (NW3C) provides legal training, but only offers this training to prosecutors. Further, if prosecutors do not understand the multitude of evidence available on a mobile device, or that an investigator can use a forensic image to create a timeline of events on the device, the evidence may not be entered in criminal proceedings or even requested to be analyzed by a prosecutors' investigator. The aforementioned example describes a lack of awareness by the prosecutor and thus a miss of possible digital evidence.

The lack of knowledge by judges and lawyers could result in overlooking a key piece of digital evidence (Rogers, Scarborough, Frakes, & San Martin, 2007). In the worst-case scenario, a piece of evidence that proves the guilt or innocence of an individual is not introduced. Conversely, if a defense attorney is not knowledgeable on forensic evidence, they may not know the proper questions to ask the expert witness or how to address questions pertaining to the admissibility of evidence. Thus, without the proper knowledge, a defense attorney cannot provide an adequate defense. Empirical research is needed to investigate and compare prosecution and defense attorneys understanding of digital evidence.

1.4 Research Questions

As there continues to be a rapid proliferation of technological advancements, digital evidence will continue to increase. Digital evidence may be a vital part of a case but there is inherent difficulty in presenting a technical process to novice individuals (Hayes, 2014; Sammons, 2015; Stambaugh et al., 2000). Therefore, it is important to determine how courtroom actors (i.e., lawyers and judges) understand digital evidence. However, there is limited research regarding the level at which lawyers, both the prosecution and defense, understand digital evidence. The current study explored the following research questions:

Q1: How knowledgeable are prosecutors and defense counsel regarding digital evidence?

Q2: What are prosecutors and defense counsels' attitudes toward digital evidence?

Q3: What are the experiences of prosecutors and defense counsel with digital evidence?

1.5 Assumptions

The assumptions associated with the current study included the following:

- Participants consent to participate in a voluntary online, anonymous survey.
- Participants consent to participate in a voluntary virtual interview via the online meeting platform, Zoom.
- Participants consent to recording and transcription of the virtual interview by Zoom.
- The online, anonymous survey was conducted using the survey platform Qualtrics.
- The survey is completely anonymous, and no identifying information is linked to the participants (e.g., IP address, student ID number, etc.).
- Participants fully read each question and answer truthfully, honestly, and free of bias.
- Participants have a basic understanding of what each question is asking, which was demonstrated in the instructions for each section of the survey. For example, for all Likert scales, the rating responses choices were explicitly stated in the survey instructions with examples.

- When answering questions regarding participants experiences with digital evidence, participants answered the survey form their own experience and not the opinions of colleagues or other third-party accounts.

- Participants answer the question regarding their professional job status (i.e., prosecutor or defense attorney). The response to this question is necessary for data analysis and to answer the research questions associated with the current study.

- Interviewees will answer the semi-structed interview questions honestly and free from bias based on their own personal opinions and not the opinions of colleagues or a third party.
- Interviewees will answer questions regarding their experiences based on their own experience and not the experiences of colleagues or a third party.

1.6 Limitations

The inherent limitations of the current study include the following:

- Civil attorneys and retired attorneys were not included in the sample.

- Attorneys who are now judge's or currently hold a different position within the criminal justice system or in industry were not included.

- The literature suggests attorneys are a hard profession to survey; thus, a small sample size impacted the overall generalizability to the population of criminal lawyers.

- The respondents are not claimed to be a fully representative sample of prosecutors and defense attorneys in the United States

- The survey and interviews only examined respondents' attitudes towards, knowledge of, and experiences with digital evidence.

1.7 Delimitations

The delimitations, which serve to limit the scope and define clear boundaries, include the following:

- Individuals, who participated in the survey or the interview, were not compensated for their participation.
- All participants must currently be in good standing with the Bar Association in the United State and practice criminal law, either as a prosecutor or a defense counsel.
- Civil attorneys were not included in the hypotheses of the current study.
- The survey was only solicited to United States attorneys.
- The survey and interview questions were not aimed at determining participants specific, technical knowledge of computers or digital devices.
- During summer 2021, the survey was only conducted for six weeks or until the number of participants required is met, whichever comes first.
- The interviews were conducted during a four-week period in the Fall 2021.
- The current study did not categorize participants based on their ethnicity or gender. The current study only categorized individuals based on their current position which will include prosecutor or defense counsel.

1.8 Summary and Organization

As there continue to be an increase in technological capabilities, there will be a subsequent increase in digital evidence. Digital evidence is an integral part of investigations and criminal proceedings for a multitude of crimes. Lawyers, both prosecutors and defense counsel, need to understand the wealth of information available from digital devices, the process for acquiring digital evidence and the ethical and legal considerations for obtaining such evidence and using in criminal proceedings. However, there is limited research regarding lawyers' understanding of, attitudes towards, and experience with digital evidence. The overall goal for the current study was to investigate lawyers', both defense and prosecutors, knowledge of, attitudes towards, and experience with digital evidence.

Chapter two expands on the literature discussed in Chapter one as well as providing an overview of digital forensics and literature regarding how forensic sciences (e.g., DNA) is

understood by courtroom actors. Chapter three first provides an overview of the mixed-methods literature to explain the design for the current study. Next, chapter three provides details on the measurement, procedures, and sample for the current study. Chapter four describes the data analysis procedures and results from the survey. Chapter five discusses the development of the interview protocol, analysis plan for the interviews, and interview results. Chapter six discusses the results by integrating the quantitative and qualitative findings, provides recommendations for future research, and presents the limitations of the current study.

CHAPTER 2. LITERATURE REVIEW

The review examined the gap in the literature regarding defense counsel and prosecutor's knowledge of, attitudes towards, and experience with digital evidence. First, the legal system in the United States is discussed to further demonstrate the roles of prosecutors and defense counsel in criminal proceedings, which was introduced in Chapter one. Next, the author provides a brief overview of the forensic science and literature regarding forensic science in the courts. Then, the subdiscipline digital forensic, which includes the digital forensic investigative process, digital evidence, and court cases which involve digital evidence. Third, the review addresses research which investigates the understanding of digital evidence in the courtroom. Overall, the current study examined an area which has largely been overlooked by researchers or is dated based on the rapid proliferation of technology.

2.1 Legal System

In the United States an independent decision maker, a judge or jury, decides the truth between two parties, which is referred to as an adversarial legal system (Moohr, 2004). In contrast, an inquisitorial system, which is prevalent in Europe, is characterized by the state carrying out an investigation to "reconstruct and understand a crime" or determine the truth, (Moohr, 2004; p. 193). In an adversarial system, the trial is the center of the legal process compared to the investigation at the center of the inquisitorial legal system. In a trial both parties put forth their evidence and attempt to deflect the evidence of the opposing party (Moohrm, 2005). Cases in the United States include civil or criminal cases.

A civil case is a conflict between individuals or institutions (ABA, 2009). In a civil case, an individual determines they cannot solve an issue without involving the courts and thus file a formal complaint with the courts. Examples of civil cases include divorce, child custody, child support, and personal injury, to name a few. A criminal case is the enforcement of public codes and laws, in which a prosecutor brings charges against a person or institution who has allegedly committed a crime. In the United States individuals are presumed innocent until the prosecution proves beyond a reasonable doubt, they are guilty, and the jury agrees. Examples of criminal cases include murder, robbery, and breaking and entering, to name a few. As previously

discussed, civil cases are beyond the scope of the current study. Thus, this section primarily details criminal procedures, which is the set of procedures the government uses to enforces criminal laws.

2.1.1 Criminal Proceedings

In the United States, the federal government, states, and municipalities each have their own set of criminal codes, which defines what constitutes a crime. In each state the state prosecution follows their given criminal procedure, and the federal prosecution follows the Federal Rules of Criminal Procedure. In most cases, federal crimes focus on crimes which go beyond state boarders or directly involves federal interests. However, generally, the federal and state criminal justice system follows the same. Figure 1 is an abbreviated illustration of the criminal justice system which was adapted from the Bureau of Justice Statistics (2021).

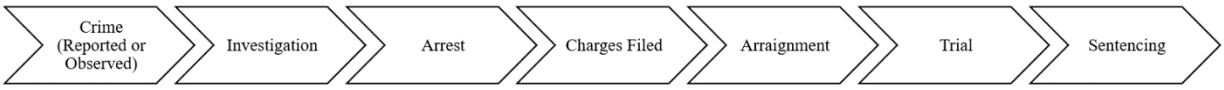

Figure 1 *Criminal Justice Process*

Between an arraignment and trial, both sides may come to an agreement, this process is known as plea bargaining. Although, researchers note that the majority of the public believes a jury trial is typical in cases (Travis, 2012), most cases are resolved through plea bargaining (ABA, 2019). In federal criminal courts, only two percent of defendants go to trial (Gramlich, 2019).

2.2 Forensic Sciences

Forensic science plays an important role in investigations and subsequently in criminal proceedings. According to Edmund Locard's exchange principle, every time an individual is in contact with a person, place, or thing a trace is left behind (Zatyko & Bay, 2011). Locard's exchange principle revolutionized the way police investigated crimes and how the scientific community thought about crime and evidence (Pollitt, 2008). Locard's principle was originally

thought to apply to physical evidence or traces which included Deoxyribonucleic Acid (DNA), fingerprints, footprints, and fiber.

The Merriam-Webster dictionary defines forensic sciences as "the application of scientific principles and techniques to matters of criminal justice, especially as relates the collection, examination, and analysis of physical evidence" (n.d.). The goal of forensic science evidence is to provide the courts with reliable evidence acquired through scientifically proven methodologies. Forensic science is an integral part of the United States legal system.

The National Institute of Standards and Technology's (NIST), Organization of Scientific Area Committees for Forensic Science (OSAC) provides an overview of the different forensic science disciplines, which includes the following (2019):

1. Biology / DNA
2. Chemistry / Instrumental Analysis
3. Crime Scene / Death Investigation
4. Digital / Multimedia
5. Physics / Pattern Interpretation

The five forensic science disciplines include 25 subcommittees (NIST, 2019). Digital forensics is a subcommittee within the Digital/Multimedia.

Pilot (2008) and Zatyko and Bay (2011) stated the previously discussed Locard's Exchange Principle can also be applied to digital evidence. Although different from the traditional application of Locard's Exchange Principle in that there is not a *physical* crime scene, a "trace" is still left behind during the commission of a computer crime (Zatyko & Bay, 2011). For instance, in the infamous Target data breach in 2013, which resulted in stolen information from over 50 million people, an e-mail containing malware was sent to one of Target's vendors (Radichel, 2014). In this example, the e-mail containing the malware would be a trace which was left behind. Zatyko and Bay (2011) applied Locard's Exchange Principle to cybercrime and concluded the "crime scene" may be more than one location and may require the analysis of multiple computers and/or networks.

2.3 Forensic Science in the Courtroom

Recently, forensic science was under scrutiny. As previously discussed in chapter one, the NAS (2009) report on forensic science in the United States suggested lawyers and judges

often have insufficient training in scientific methodology. Researchers have echoed this by calling for the need to better understand judges', lawyers', and jurors' understanding of forensic science (Bull & Holliday, 2011). There is a dedicated body of literature in the social sciences which focuses on how individuals understand different aspects of forensic science. Eldridge (2019) suggested while forensic science community has been debating the best way to present scientific conclusions, the cognitive psychology community have been conducting research on how lay people examine and understand forensic conclusions. Eldridge (2019) further suggested the forensic science community has largely neglected this body of research in their debate. The next section will review the literature which aims at examining how jurors or lay individuals (in place of actual jurors), judges, and lawyers understand different forensic science disciplines. As there is a lack of literature specific to digital evidence at this time, the literature review also includes other forensic science disciplines, such as DNA.

2.3.1 DNA Evidence

Within the literature, there is a vast amount of research which focuses on the understanding of DNA evidence (Homgren, 2003 & 2005; Limberman et al., 2008; Hans et al., 2011). For instance, Holmgren's doctoral dissertation and subsequent publication (2003 & 2005, respectively) used a multimethod approach to examine DNA evidence among judges, defense attorneys, prosecutors, and jury eligible individuals in Canada. Holmgren (2003) conducted three focus groups with jury eligible individuals (n = 8), defense lawyers (n = 2), and prosecutors (n = 2); face-to-face interviews with judges (n = 7); a survey to jury eligible individuals (n = 311), and a mock trial. Focus groups revealed jurors have difficulty understanding DNA evidence and assigning weight to such evidence; further results suggested even if jurors do not understand the evidence or the statistical probability associated with the match, they believe the evidence is more credible compared to other evidence types. Further results revealed discrepancies between access to resources for the prosecution and defense in Canada (Holmgren, 2005). More specifically, the prosecutors indicated they had an unlimited number of resources due to ample funding compared to defense counsel who indicated they had no resources and limited funding (Holmgren, 2005). However, judges suggested both prosecutors and lawyers have access to resources (Holmgren, 2005).

In 2008, Liberman, Carrel, Miethe, and Krauss investigated the perception of DNA evidence among jurors (undergraduate sample, study one and three; and mock jury sample, study two). Liberman et al. (2008) measured perception of DNA evidence using survey items with questions pertaining to the persuasiveness of DNA. Overall, Liberman and colleagues (2008) found, regardless of the type of crime, DNA evidence was an influential factor in decision making among the three samples. Bull and Holliday (2011) investigated jurors' perception of forensic evidence with regards to evidence mobility and relevance. Mobility and relevance refer to forensic evidence characteristics which can be manipulated and measured according to the probability theory model (Bull & Holliday, 2011). According to Bull and Holliday (2011), mobility refers to the likelihood the evidence was at the crime but was not directly involved in the crime (e.g., cigarette bud left at a parking lot), and relevance referred to the "extent to which guilt could be directly inferred from the evidence" (p. 411). The types of evidence included were fingerprints, DNA, and footwear. Results indicated mobility and relevance were included in the strength ratings for types of evidence. Further, results found participants do understand the need for evidence to be linked to a case for such evidence to be useful. Further, Liberman and colleagues (2008) suggested the results indicated participants were not solely basing their decision on the type of evidence (DNA, fingerprints, and footwear).

Hans and colleagues (2011) also investigated how jury pool members in Delaware understand DNA which connects a defendant to a crime. Hans and colleagues (2011) conducted a mock trial which included an hour-long videotape of a trial. Results indicated jurors with a high education level had a better understanding of the evidence (Hans et al., 2011). Hans and colleagues (2011) argued jurors understand forensic evidence, but jurors may have errors and doubts regarding the evidence (p. 60). In 2012, through semi-structured interviews, Cashman and Henning investigated 40 lawyers' experience, use, and understanding of DNA evidence in criminal cases in Australia. Cashman and Henning (2012) interviewed and conducted focus groups with participants asking questions pertaining to the individual's education and the types of education requirements they had. Participants were also asked about training and resources to which the participants had access, how much the individual felt he/she knew about DNA evidence, and their access and communication with expert witnesses. Overall, results indicated lawyers find scientific reports and evidence difficult to understand (Cashman & Henning, 2012).

Lincoln, Southerland, and Jarret-Luck (2014) examined mock jurors' interpretations and perceptions of DNA evidence. Lincoln and colleagues (2014) presented manipulated trial scenarios to mock jurors (undergraduate and graduate students) by controlling how the DNA evidence was presented (probability vs. frequency). Overall, Lincoln and colleagues (2014) found participants expressed knowledge with regards to DNA, and also stated DNA evidence could determine guilt, but DNA evidence alone was not enough to convict or acquit a suspect.

2.3.2 General forensic science evidence, technical reports, and expert witness

In addition to specific forensic science disciplines, such as DNA and digital forensics, research has examined the understanding of technical reports and also the impact of expert witnesses. For instance, de Keijser and Ellfers (2012) investigated the judges', defense lawyers', and experts' (Dutch Forensic Institute professionals) "supposed" understanding and "proper" understanding of technical forensic reports. Two simulated forensic reports were used in the study, one included a robbery at a gas station and the other was a robbery on the street (de Keijser & Ellfers, 2014). Participants received both forensic reports but the way in which the evidence was reported was manipulated (visual vs. verbal). Findings indicated judges' and lawyers are unaware of their level of understanding of the likelihood ratios presented in the two scenarios (ed Keijser and Ellfers, 2012).

Typically, jury research studies provide transcripts or conduct mock trails which include the prosecution entering evidence. Maeder, Ewanation, and Monnik (2017) identified a gap in the jury research literature which was the absence of studies which examined evidence and eyewitness testimony from the defense. To address this gap, Maeder and colleagues (2017) provided undergraduate students in Canada a murder trial transcript in which the presentation of evidence was manipulated, including the strength of DNA evidence (high, low), strength of eyewitness testimony (high, low), and the evidence presentation (prosecution presenting DNA/defense presenting eyewitness or defense presenting DNA and prosecution presenting eyewitness; p. 38). Results indicated whoever (prosecutor or defense) presented the DNA evidence received the favorable outcome. Further, results found potential jurors preferred DNA evidence to eyewitness testimony.

Additionally, in 2018, Wilcox and NicDaeid investigated jurors' perception of expert witnesses from the forensic sciences. The jurors consisted of individuals in the United States

(Maine) who heard forensic testimony in homicide trial (Wilcox & NicDaeid, 2018). The primary goal of Wilcox and NicDaeid (2018) was to assess the factors which influence how jurors judge forensic expert testimony. Results indicated experience in a specialization was the most important characteristics to jurors (Wilcox & NicDaeid, 2018). The next section discusses a sub-discipline of the forensic science field, digital forensic.

2.4 Digital Forensics

One of the first and most cited definitions for digital forensics is from the first Digital Forensic Research Workshop (DFRWS) in 2001. At this time, digital forensic was defined as

> the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation 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 unauthorized actions shown to be disruptive to planned operations (Palmer, 2001, p. 16)

The increase in technology has not only led to new types of devices (e.g., mobile photos, smartwatches) but also an increase in the amount of data available for digital forensic investigators. As previously mentioned, digital forensics is an umbrella term which includes several subdisciplines such as computer forensics, mobile forensics, malware forensics, and network forensics (Barmpatsalou et al., 2013; Casey, 2011).

2.4.1 Digital Forensics Process

Throughout the literature, there are various digital forensic process models, and not one universal agreed-upon model (*see*; Mckemmish, 1999; Reith, Carr, & Gunsh, 2002; Carrier & Spafford, 2003; Beebe & Clark, 2004; Rigby & Rogers, 2007; & Mothi, Janicke, & Wagners, 2020). In proposing their model, Beebe, and Clark (2004) provided an analysis of the forensic models in the literature at that time. The analysis showed all models, at the time of their analysis, included data collection, data analysis, and presentation of findings (Beebe & Clark, 2004). Building upon these findings and previous literature, Rigby, and Rogers (2007) developed a general digital forensic model shown in Figure 1.

Figure 2 *Digital Forensics Process (Rigby & Rogers, 2007)*

For the purpose of the current study, when referring to the digital forensic process model, the author will use Rigby and Rogers (2007). The final step of the digital forensic model is the presentation of digital evidence in court. The presentation phase refers to the legal context of a case. Sammons (2015) stated "the pinnacle of the forensics process is the presentation of the findings to a judge or a jury" (p. 9). As digital evidence could be a vital part of a case coupled with the difficulty of presenting a technical process to novice individuals, it is important to determine how judges or jurors understand and perceive digital evidence.

The current study focuses primarily on the final stage in the digital forensic process. Before judges, and jurors are tasked with comprehending digital evidence, lawyers must either present digital evidence as part of their defense or prosecution, use such evidence to further their investigation and determine additional suspects, or during plea agreement negotiations. Due to the importance of digital evidence to court cases and the possibility digital evidence can assist lawyers, it is imperative empirical research examines lawyers' understanding of digital evidence.

2.4.2 Digital Evidence

Digital evidence is "information that has been processed and assembled so that it is relevant to an investigation and supports a specific finding or determination" (Easttom, 2017, p. 10). Garrie and Morrisy (2014) state digital evidence is comprised of "ones and zeroes which do not lie" and should, therefore, be able to withstand judicial scrutiny (p. 122). As previously mentioned, there are various subcategories within the digital forensic field (Barmpatsalou et al., 2013; Casey, 2011. Beyond the subcategorization, primarily based on device type (e.g., drone forensics, mobile forensics), researchers have discussed the different types of evidence gathered and their different outcomes or uses (Goodison, Davis, & Jackson, 2015). Researchers agree that the use of digital evidence is relevant to all types of cases, and thus is increasingly important tool in litigation (Bensen, 2004; Sammons, 2015) Similar to physical evidence, digital evidence can impact the courts. If there is a lack of understanding of forensic science evidence, it is possible

there will be a problem in the administration of justice (Subedi & Giri, 2018). The analysis of digital devices can result in a multitude of digital evidence including, but not limited to e-mails, chats, website use and searches, network traffic, and passwords.

2.4.3 Digital Forensic Court Cases

Over the years, there have been notables court cases which involve legal questions regarding digital evidence. Researchers have written about possible legal questions regarding digital evidence such as search warrants, admissibility, and the Daubert Standard (Novak, 2020). This section briefly describes two landmark Supreme Court cases.

2.4.3.1 Riley v. California (2014)

The 2014 *Riley v California* Supreme Court cases primarily dealt with search seizure. In this case the defendant, David Leon Riley, was involved in a shooting of a rival gang. Riley and other offenders were seen leaving the crime in his vehicle. Weeks later Riley was pulled over driving a *different* vehicle due to expired license tags. During the stop, police also learned Riley's driver license was suspended and thus the car was impounded. As a result of the car being impounded, the police were required to search the car which revealed two legally possessed firearms which resulted in Riley's arrest. At this time, a detective from the gang unit reviewed Riley's mobile device which resulted in photos and videos of Riley "throwing up gang signs" which led to detective connecting him to a local gang. Based on ballistics, Riley was tied to the gang shooting. Riley attempted to suppress the evidence from the phone search, but this request was denied. Riley was found guilty of the gang shooting. This decision was upheld in The California Court of Appeal. The case then went to the Supreme Court to determine if the search performed on Riley's phone was based on a search and seizure which violated the 4th Amendment. In a unanimous decision, the Supreme Court ruled the search was a violation as the "digital data did not pose a threat to the officers", which is the point of warrantless searches after an arrest. This landmark case provided an answer to a long-debated question regarding search warrants and mobile devices.

2.4.3.2 Carpenter v. United States (2018)

After a robbery in 2011, four men were arrested, and one confessed to the police and provide his cell phone number and his accomplices numbers. As a result, three requests were made to obtain transactional records which was granted by a judge. The information from these records provided investigators with approximate locations of the cell phones based on their connection to cell towers. As a result, Timothy Carpenter was charged with abetting robbery, among other charges. Carpenter attempted to suppress the cell location data, stating the investigators needed a warrant based on probable cause to obtain such records. This request was denied. However, the Supreme Court ruled the warrantless acquisition of the cell location data violated Carpenter's fourth amendment's right.

2.4.4 Digital Evidence in the Courtroom

Similar to the other forensic science disciplines, empirical research has been conducted regarding digital forensics in the courts. For instance, in 2006, Losavio and colleagues investigated judges experience and perception of digital evidence. Experience with digital evidence was measured with questions asking the frequency cases included e-mail evidence or website/internet usage or such evidence as challenged (Losavio et al., 2006). With regards to perception, questions included judges' opinions regarding forthcoming frequency of challenges, and the current amount of digital forensic training. Findings suggests judges were not experiencing digital evidence or challenges to such evidence in their courtrooms but anticipated an increase in the years to come (Losavio et al., 2006) In addition, judges did not report receiving training regarding digital evidence (Losavios et al., 2006).

Similarly, Losavio and colleagues (2008) investigated experiences digital forensic and electronic evidence among lawyers. Losavio and colleagues (2008) conducted a two-part study, which consisted of a survey in 2005 followed up by an additional survey in 2008. Experience with digital evidence was measured with questions asking for the frequency of e-mail evidence and website/internet use in cases. The 2005 survey was solicited to lawyers attending a seminar on digital forensic and electronic evidence. The survey in 2008 was solicited to Criminal Justice Act (CJA) panel of attorneys, which included defense attorneys who accepted appointment to defend indigent criminal defendants in federal court. Both surveys included similar questions,

which aimed at investigating the participants experience with digital evidence and electronic evidence. Overall, Losavio and colleagues (2008) set out to measure the experience of attorneys with digital evidence and measured this variable with questions pertaining to the use or frequency of such evidence, and the use of experts (specialists) in a case. Results suggested, in 2008, criminal cases had minimal use of e-mail and web usages. At this time, advancements in technology were on the rise and the use of mobile devices was still in its infancy. Updated research is needed in this area.

Kessler (2010) investigated judges' awareness, understanding, and application of digital evidence with a qualitative research design[2] with two components, the first solicited responses from open-ended questions as well as demographic questions regarding the judges' training and work experience (e.g., time on bench); the second included follow-up interviews with judges who agreed to participate based on the first phase. Kessler (2010) defined awareness of digital evidence as "one's familiarity with existence, various types, and sources of digital evidence" (p. 16). Application of digital evidence was defined as "the ability to properly identify the role that digital evidence plays in the decision-making process related to the admissibility and the legal process" (Kessler, 2010, p. 16). Understanding of digital evidence refers to "the comprehension and ability to understand digital evidence, including the knowledge of the underlying technologies from which the digital evidence was derived" (Kessler, 2010, p. 20). Overall, results indicated judges are aware of the importance of digital evidence but *not* aware of all types, judges believe digital evidence should be authenticated (like other evidence) and are aware of how easy it is to alter or misinterpret digital evidence (Kessler, 2010).

2.5 Summary

Chapter two provided an overview of digital forensics, detailed literature regarding forensic science evidence (e.g., DNA) in the courts, and reviewed the literature regarding digital evidence in the courts. The literature review examined not only how evidence was understood by lawyers, but also additional courtroom actors such as jurors' (mock, actual, or jury eligible) and judges. There is a substantial amount of research which examines the understanding or knowledge of, perceptions, and attitudes towards forensic evidence (Homgren, 2003 & 2005,

[2] Although Kessler's (2010) design is discussed as qualitative which was analyzed using a grounded theory approach, the survey included two Likert Scale items which were analyzed with a correlation.

Limberman et al., 2008; Hans et al., 2011). However, there is a lack of research which investigates digital evidence in the criminal proceedings. Further, there is no research which aims to investigate differences among defense attorneys and prosecutors understanding of digital evidence. In addition, based on the rapid proliferation of technology, the research regarding digital evidence is dated (Kessler, 2010; Losavio et al., 2008; Losavio et al., 2006).

CHAPTER 3. METHODS

Chapter three first provided a brief overview of mixed methods designs. Next, chapter three described the design and procedures used to investigate lawyer's attitudes towards, knowledge of, and experience with digital evidence. Chapter three also operationally defined the subject, dependent and control variables. Chapter three primarily discusses the methods associated with phase one of data collection which was an online, anonymous survey. This includes participants, recruitment strategies, and procedures. Phase two data collection and procedures are briefly highlighted but explained in more detail in chapter five.

The current study explored the following research questions:

Q1: How knowledgeable are prosecutors and defense counsel regarding digital evidence?

Q2: What are prosecutors and defense counsels' attitudes toward digital evidence?

Q3: What are the experiences of prosecutors and defense counsel with digital evidence?

3.1 Hypotheses

Derived from the research questions and based on previous research, the following three hypotheses were examined:

H1: Prosecutors have more knowledge of digital evidence compared to defense attorneys.

H2: Prosecutors have more favorable opinion of digital evidence compared to defense attorneys.

H3: Prosecutors have more experience with digital evidence in the court room compared to defense attorneys.

3.2 Mixed Methods

A mixed-methods design refers to "research in which the investigator collects and analyzes data, integrates the findings, and draw inference using both qualitative and quantitative approaches or methods in a single study or program of inquiry" (Tashakkori & Creswell, 2007, p. 4). Similarly, Creswell and colleagues (2003) defined mixed-method research as

> the collection or analysis of both quantitative and qualitative data in a single study in which the data are collected concurrently or sequentially, are given a priority, and involve the integration of the data at one or more stages in the process of research (p. 212).

Vogt, Gardner, and Haeffele (2012) suggested using multiple designs when your question has various parts, or a single study design will not provide enough information on the phenomenon. The critical element of mixed-methods research is the collection of quantitative and qualitative data which is analyzed and *integrated* for a single research goal. While mixed-method designs are not new, researchers suggest mixed-methods have gained popularity in recent years, (Creswell & Plano Clark, 2011; Maruna, 2011).

3.2.1 Mixed-methods Research Designs

There are multiple mixed-methods research designs in the literature, and three which are considered basic mixed-methods research which includes: convergent design[3], exploratory sequential design[4], the explanatory sequential design. The current study used an explanatory sequential design.

The explanatory sequential design is characterized by the collection and analysis of quantitative data, *followed by* qualitative data collection and analysis and then both results are interpreted and discussed (Creswell, 2015; Creswell & Plano Clark, 2011; Decuir-Guny & Schutz, 2017). The key component of the explanatory design is the use of qualitative data to help explain quantitative findings. An example from the literature was reviewed to provide a practical application of the explanatory sequential design. Li, Worch, Zhou, and Aquiton (2015) used an explanatory sequential mixed-method design to examine how and why teachers use technology in the classroom. Specifically, Li and colleagues (2015) first collected quantitative data, through a survey, and then *followed up* with qualitative data collection, through interviews. Li et al. (2015) also explicitly stated their rationale for this methodological choice: first, the researchers

[3] The convergent design involves the collection of quantitative and qualitative data; results are analyzed and integrated (Creswell & Plano Clark, 2017; DeCuir-Gunby & Schutz, 2017). Unlike the explanatory and exploratory sequential designs, which are characterized by two phases of data collection in which the second depends on the first, the convergent design includes two sets of data which are collected independently of one another.

[4]The exploratory sequential design is 1 = a two-phase study, where the qualitative data is collected in the first phase, which are then analyzed and *builds* to the second phase, which is quantitative data collection (Creswell & Plano Clark, 2017; DeCuir-Gunby & Schutz, 2017).

wanted to "further understand survey results," and the researchers "purposefully select participants according to the initial quantitative results" (p. 2). Specifically, Li and colleagues (2015) used quantitative scores for technology use to group individuals in a low, medium, and high technology use sub-groups. Next, Li et al. (2015) conducted interviews with two individuals from each group, which served as the qualitative phases of the study. By following-up with a specific group of individuals in these categories, Li, and colleagues (2015) were able to provide additional qualitative data for each group of technology used to understand the phenomenon. Li et al.'s (2015) rationale for utilizing an explanatory sequential mixed-methods design is in line with the literature, which states this design is best used for follow-up and specifically looking to examine significant or non-significant findings in the quantitative phases (Creswell, 2015; Creswell & Plano Clark, 2011; Decuir-Guny & Schutz, 2017).

3.3 Design

The current study followed an explanatory sequential design, as shown in Figure 3. An explanatory sequential design is defined as further explaining quantitative findings by collecting additional qualitative data (Creswell, 2015).

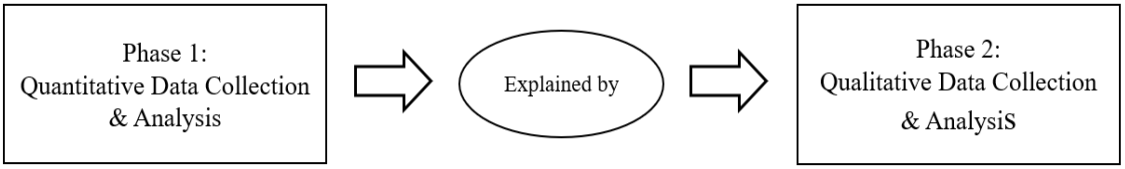

Figure 3 *Explanatory Sequential Design*

Phase one includes a survey which used intra-method mixing. Intra-method mixing refers to the collection of a second type of data within data collection (DeCuir-Guny & Schutz, 2017). The survey included questionnaires and write-in response questions. Results were analyzed and are presented in Chapter four. The results from phase one were further explored in phase two. Phase two consisted of semi-structured interviews. The semi-structured interview protocol was developed based on the survey findings. The interview results are presented in Chapter five.

3.4 Operational Definition of Constructs

The current study examined the differences between prosecutors and defense counsels' attitudes towards, knowledge of, and experience with digital evidence. As previously discussed, digital evidence refers to "information that is stored or transmitted in a binary format that may be relied on in court" (NIJ, 2007, para. 2) The subject variable for the current study is participants self-reported professional status. And the three dependent variables of interest include attitudes towards, knowledge of, and experience with digital evidence.

3.4.1 Subject Variable

The subject variable is the self-report professional status of each participant. According to the ABA (2015), defense counsel refers to

> any attorney – including privately retained, assigned by the court, acting *pro bono,* or serving indigent defendants in a legal aid or public defender's office – who acts as an attorney on behalf of a client being investigated or prosecuted for alleged criminal conduct, or a client seeking legal advice regarding a potential, ongoing or past criminal matter or subpoena, including as a witness (para 1).

Prosecutor refers to

> any attorney, regardless of agency, title, or full or part-time assignment, who acts as an attorney to investigate or prosecute criminal cases or who provides legal advice regarding a criminal matter to government lawyers, agents, of offices participating in the investigation or prosecution of criminal cases (ABA, 2015, para 1).

Participants were asked to self-report their current professional status and responses choices included defense counsel (private and public), prosecutors and a blank write-in option. This question was included in the survey during data collection for Phase 1 of the current study, as shown in Appendix A. In addition, individuals who completed the interview also completed a brief survey which included this question, as shown in Appendix C.

3.4.2 Control Variables

The literature suggests prosecutors receive more training compared to defense counsel (Holmgren, 2005). As discussed in Chapter 1, there are a multitude of trainings, such as the

NCFI and NW3C, which provide training specifically to prosecutors. Further, focus group findings reveal prosecutors, practitioners, and law enforcement believes the defense is behind in their knowledge and training of digital evidence (Goodison et al., 2015). Therefore, individual experiences, such as formal digital forensics training, was assessed. In addition to previous training, previous employment may also affect an individual's attitude towards or knowledge of digital evidence. If a participant is currently a defense counsel but was previously a prosecutor or was an intern at a prosecutor's office, they might have received additional training. Therefore, two questions assessed previous employment and internships within the last five years in the survey, as shown in Appendix A. In addition, previous trainings were assessed in the interviews, as shown in Appendix C.

3.4.3 Dependent Variables

The dependent variables for the current study included attitudes toward, knowledge of, and experience with digital forensic. Research regarding the understanding of, attitudes toward, and knowledge of digital forensic evidence in the courtroom, by judge, lawyers, or jurors, is limited. However, as discussed in the literature review, there is a wealth of literature which focuses on other forensic science disciplines in the courtroom. This literature guided the operational definitions and measurement of the dependent variables.

With regards to understanding, Holmgren (2003; 2005) measured understanding with factual questions with a correct answer. Similarly, Hans et al. (2011) measured knowledge with factual, true/false questions with a correct answer. Similarly, both asked participants to define the concept of interests (DNA and mDNA, respectively) in their own words (Hans et al., 2011; Holmgren, 2003; 2005). Additionally, Lincoln and colleagues (2014) measured knowledge with test like questions with a correct answer Further, de Keijser and Ellfers (2012) investigated the proper and supposed understanding. With regards to the proper understanding, de Keijser and Ellfers (2012) asked individuals questions about the report, such as: "There is a much more than 50% chance that the suspect is the person on the image from the security camera", and each questions had a correct answer. Similarly, Kessler (2010) investigated judge's "comprehension and ability to understand digital evidence, including the knowledge of the underlying technologies for which the evidence was derived" (p. 20). With regard to experience, Holmgren (2003), Losavio et al. (2006), and Losavio et al. (2008) all measured experience through past or

current use with the evidence. For instance, “Have you ever been a juror” (Holmgren, 2003), and “What is the frequency of website usage as evidence in court?” (Losavio et al., 2006).

Experience and understanding / knowledge were defined and measured similarly throughout the literature; perception was defined and measured differently. For instance, Wilcox and NicDaeid (2018) measured perceptions specifically with regards to participants views on expert witness qualifications. Liberman and colleagues (2008) measured perception through participants’ opinions on the accuracy and strength of DNA evidence. Losavio and colleagues (2006) measured perception with regards to judges’ opinion on future trainings. Based on the literature, the following dependent variables are operationally defined.

3.4.3.1 Knowledge

Knowledge referred to the participants correct responses to fact-based questions regarding digital evidence. The knowledge questionnaire was comprised of eight test-like questions with one correct answer, as shown in Appendix A. This included four True/False questions and four multiple choice questions. The use of a correct answer to measure knowledge is similar to Hans and colleagues (2011), Holmgren (2003) and Kessler (2010). The response “I don’t know” was included to provide participants who are unsure of a response an option instead of forcing respondents to guess or skip the questions. Past research has utilized the “I don’t know” response (Hans et al., 2011).

3.4.3.2 Attitude

Attitude referred to participants beliefs and opinions about digital evidence and its use in the court room. Maeder et al. (2017) measured participants attitudes toward DNA through questions such as “DNA is the most reliable type of physical evidence we have today” and “I would convict a defendant if the only evidence against him were DNA” (p. 38). Questions from Maeder et al. (2017) were adapted to measure attitude, examples include:

1. Digital evidence can eliminate a suspect.
2. Digital evidence can prove the guilt of a suspect.

The final scale included 10 items and respondents used a 5-point Likert scale, ranging from Strongly Agree to Strongly Disagree, and included an “I don’t know” option.

Respondents were also asked their opinion on the use of digital forensic experts, digital forensic investigators, and law enforcement. One question also assessed participants opinions on whether cases are more or less successful with the use of digital evidence.

The current study used a mixed-method approach with intra-method mixing. Attitudes and opinions were also measured with write-in responses. Questions assessed participants attitudes and opinion of digital evidence, such as current challenges and challenges in the next 10 years. In addition, the interview protocol further assessed participants attitudes towards digital evidence, as shown in Appendix C.

3.4.3.3 Experience

For the current study, experience refers to an individual's past use of digital evidence in criminal proceedings. During Phase 1, experience was measured through a questionnaire and write-in responses. For instance, questions assessed the use of digital evidence in court cases and also in plea agreements, as shown in Appendix A. In addition, similar to previous research, questions asked participants what types of evidence they have encountered in their cases (Losavio et a., 2006). The survey also explored what resources are available to prosecutors and defense attorneys. Specifically, questions assessed lawyers' experiences consulting with digital forensic experts and law enforcement (LE) / investigators as part of their cases which involve digital evidence.

The interview further explored experiences with digital evidence by asking participants to elaborate by sharing stories or specific cases. The interview protocol can be found in Appendix C. The current study is interested in the lived experiences involving digital evidence and how these experiences differ between prosecutors and defense counsel.

3.5 Participants

Forty-two individuals consented to participate in the survey. Three individuals only consented to the survey and did not complete any additional questions, and two participants only completed the first three questions; these individuals were removed. Four individuals did not have a Juris Doctorate and two did not practice law in the United States; thus, they were deleted as they did not meet the eligibility requirements for participation in the survey. Two participants

failed the attention check and were removed. Three individuals only completed the demographic's portion of the survey and were removed. The data set included *n* =26 participants.

As shown in Table 1, the sample consisted of 11 prosecutors, five defense attorneys, which included both public defenders and private defense attorneys, and 10 individuals who selected "other." The majority of prosecutors were White (90.9%), had a salary between $60,001 and $80,000 (54.5%), and were from an urban area (81.8%). Thirty-six percent of prosecutors were between 26 and 29 years old. All of the defense attorneys were White, the majority were male (80%) were between 30 and 39 years old (60%), and from an urban area (80%). The common salaries for defense attorneys were 60-001 - $80,000 (40%; Public Defenders) and more than $150,001 (40%; Private Defense Attorney).

Table 1 *Demographics by Job Type*

		Prosecutors	**Defense**	**Other**	**Total**
		n = 11	*n* = 5	*n* = 10	*N* = 26
Age					
	26-29	4 (36.4)	1 (20)	1 (10)	6 (23.1)
	30-39	3 (27.3)	3 (60)	4 (40)	10 (38.5)
	40-49	3 (27.3)	1 (20)	1 (10)	5 (19.2)
	50-59	1 (9.1)	0 (0)	3 (30)	4 (14.4)
	60 or older	0 (0)	0 (0)	1 (10)	1 (3.8)
Gender					
	Female	5 (45.5)	1 (20)	7 (70)	13 (50)
	Male	5 (45.5)	4 (80)	3 (30)	12 (45.2)
	Prefer Not To Respond	1 (9.1)	0 (0)	0 (0)	1 (3.8)
Race					
	Hispanic or Latinx	0 (0)	0 (0)	2 (20)	2 (7.7)
	Multiracial	0 (0)	0 (0)	1 (10)	1 (3.8)
	White	10 (90.9)	5 (100)	7 (70)	22 (84.6)
	Prefer Not To Respond	1 (9.1)	0 (0)	1 (10)	1 (3.8)
Salary					
	60,001 - $80,000	6 (54.5)	2 (40)	2 (20)	10 (38.5)
	$80,001 - $100,000	1 (9.1)	1 (20)	2 (20)	4 (15.4)
	$100,001 - $120,000	1 (9.1)	0 (0)	1 (10)	2 (7.7)
	More than $150,001	2 (18.2)	2 40)	4 (40)	8 (30.8)
	Prefer Not To Respond	1 (9.1)	0 (0)	1 (10)	2 (7.7)
Geographic Make-up					
	Urban Area	9 (81.8)	4 (80)	8 (80)	21 (80.8)
	Urban Cluster	2 (18.2)	1 (20)	1 (10)	4 (15.4)
	Rural Area	0 (0)	0 (0)	1 (10)	1 (3.8)

Note. Values represent frequencies with percentages in parentheses. Due to rounding, percentages may not add up to 100%.

Undergraduate education, higher education, and previous employment was also explored. The majority of respondents were not pre-law majors (73.1%) and did not have a higher education degree beyond a juris doctorate (92.3%), as shown in Table 2. Other undergraduate majors for prosecutors included Criminal Justice, Environmental Sciences, Psychology, and Sociology. For defense attorneys', the only other major listed was Psychology. Sixty-four percent of prosecutors and 40% of defense attorneys reported employment at their current job for two to five years. Two prosecutors were at their current job for more than 20 years.

Table 2 *Education and Employment by Job Type*

		Prosecutors	**Defense**	**Other**	**Total**
		n = 11	*n* = 5	*n* = 10	*N* = 26
Undergrad Major					
	Business	1 (9.1)	1 (20)	1 (10)	3 (11.5)
	Criminal Justice	0 (0)	0 (0)	1 (10)	1 (3.8)
	Economics	1 (9.1)	0 (0)	0 (0)	1 (3.8)
	English	1 (9.1)	0 (0)	1 (10)	2 (7.7)
	History	2 (18.2)	0 (0)	0 (0)	2 (7.7)
	Mathematics	0 (0)	0 (0)	1 (10)	1 (3.8)
	Political Science	3 (27.3)	3 (60)	6 (60)	12 (46.2)
	Other	3 (27.3)	1 20)	0 (0)	4 (15.4)
Pew Law					
	No	8 (72.7)	4 (80)	7 (70)	19 (73.1)
	Yes	3 (27.3)	1 (20)	3 (30)	7 (26.9)
Higher Edu					
	No	10 (90.9)	4 (80)	10 (100)	24 (92.3)
	Yes	1 (9.1)	1 (20)	0 (0)	2 (7.7)
Intern					
	No	2 (18.2)	1 (20)	2 (20)	5 (19.2)
	Yes	9 (81.8)	4 (80)	8 (80)	21 (80.8)
Yrs. at Current Job					
	0 - 1 Yrs.	1 (9.1)	1 (20)	1 (10)	3 (11.5)
	2 - 5 Yrs.	7 (63.6)	2 (40)	5 (50)	14 (53.8)
	6 - 10 Yrs.	0 (0)	1 (20)	1 (10)	2 (7.7)
	11 - 15 Yrs.	1 (9.1)	1 (20)	2 (10)	2 (7.7)
	More than 20 Yrs.	2 (18.2)	0 (0)	3 (10)	5 (19.2)

Note. Values represent frequencies with percentages in parentheses. Due to rounding, percentages may not add up to 100%.

The majority of both prosecutors and defense attorneys were previously interns (81%). Current prosecutors and defense attorneys reported interning at the following, prosecutor's office, private

law firms, public defender offices, and were law clerks, as shown in Table 3. For the write-in response "other" prosecutors reported interning at a health law clinic, a law school clinic, and a Railroad Co. Law Department. Two defense attorneys reported interning for a judge.

Table 3 *Intern Positions by Job Type*

		Prosecutors	**Defense**
Intern Position			
	Prosecutors Office	4	1
	Private Law Firm	1	4
	Public Defenders Office	1	1
	Law Clerk	4	4
	LE Agency	0	0
	Other	4	2
	Prefer not to respond	1	0

Note. Numbers represent frequencies and individuals could select multiple responses.

In addition to previous internship positions, previous employment was also explored. As shown in Table 4, one defense attorney previously worked at a prosecutor's office, and one prosecutor previously worked at a Public Defenders Office. Four current prosecutors also wrote in the following responses as their previous employment: Bailiff, insurance adjuster; contract specialist for the Department of Defense, and Railroad Co. Law Department. Two defense attorneys were law clerks for a judge.

Table 4 *Previous Employment by Job Type*

		Prosecutors	Defense
Previous Employment			
	Private Attorney	1	3
	Prosecutor's Office	4	1
	Public Defender	1	0
	Judge	0	1
	Law Enforcement Agency	0	0
	No prior employment	2	0
	Other	5	1

Note. Numbers represent frequncies and individuals could select multiple responses.

As a note, general demographic information was collected as part of the survey to allow the researcher to compare the sample to the overall population of lawyers in the United States. For instance, the majority of all respondents in the current study were white (85%), which is consistent with the ABA National Lawyer Population Survey's (2021) findings that the majority of lawyers are Caucasian/White (85%). However, the sample of only prosecutors and defense counsel was 94% white, which is 9% higher than the ABA survey. Further, the majority of respondents in the current study were female (50%); however, for the sample of prosecutors and defense attorneys, the majority of respondents were male (56%). The ABA survey found that the majority of lawyers are male (63%).

Before hypothesis testing, the specific job types for the "other" category were explored, which revealed the ten individual who selected "other" did not practice criminal law as part of their job responsibilities. Thus, these ten individuals did not meet the sampling criteria for the current study and were removed from hypothesis testing. The final sample for inferential statistical analyses included 16 individuals, ten prosecutors and five defense attorneys.

3.6 Participants & Recruitment

There were two sampling criteria for participation in phase one and two of the current study: (1) individuals are currently licensed to practice law in a jurisdiction in the United States; and (2) individuals are specifically practicing criminal law.

For phase one, recruitment for survey participation was sent via email and social media messages. The researcher contacted various law specific organization's communications department and/or the listed point of contact. The solicitation e-mail discussed the study's goals and asked for support in soliciting the survey to the organization. If the point of contact endorsed the study, the author asked them to send out the solicitation e-mail to the organization's member listserv. The solicitation email asked individuals to participate and also forward the survey to their colleagues who meet the participation requirements. This technique is referred to as snowball sampling. Snowball sampling refers to using initial participants or informants to identify additional participants (Kemper et al., 2003, p. 283). Patton (2001) define snowball sampling as selecting participants who know additional participants who can also provide rich data for the study.

For the survey, recruitment e-mails were sent to over 20 organizations and associations to solicit participation. For the defense attorneys, an e-mail was sent to both national and state associations, including the National Association of Criminal Defense Lawyers and Arkansas Association of Criminal Defense Lawyers (ASSCDL). For prosecutors, the National District Attorneys Association as well as the Association of Prosecuting Attorneys were contacted. In an effort to reach minority populations, specific minority groups associations were also solicited, which included the African American Attorney Network, Northern Virginia Black Attorney Association, Hispanic National Bar Association, and the Women's Bar Association. Of the organization contacted, only two responded both stating they would not or could not solicit the survey.

In addition to the associations and organizations, personal contacts and colleagues were also sent the recruitment information via social media message or e-mail. This included 28 Lawyers and/or law enforcement contacts. (2 via text, 18 via social media message, 8 via e-mail); 38 Professional Contact in Criminal Justice/Digital Forensic Area (14 via social media message; 24 via email) and Personal Contacts (29 via social media message; 3 via e-mail).

3.7 Procedures

The online, anonymous survey via the survey platform Qualtrics, included four sections. First, the survey included demographic questions (e.g., age, race, employment, etc.) and questions regarding previous internships and employment. The survey also included three

questionnaires measuring the variables of interests for the current study: knowledge, attitudes, and experience. The survey was reviewed by digital forensic experts, researchers who study digital evidence in the courts, and a measurement expert. Then the survey was reviewed by a current law school student and two lawyers.

During the course of the survey, no personally identifiable identifying information was collected (e.g., name, social security number, IP address); instead, participants were randomly assigned an ID number; this feature is offered through Qualtrics. The online questionnaire began with a consent page, which detailed the purpose of the study, the voluntary nature of the study, the confidentiality of the data, and the benefits and risks of participation. Participants were able to withdrawal from the survey at any time and no incentives or rewards were offered for participation. At the end of the consent page, participants over the age of 18 were instructed to consent or decline the study. If participants provided consent, they proceeded to the survey; if they did not agree, they were directed to the "Thank you" page and not permitted to take the survey.

In line with Institution Review Board (IRB) requirements and the sampling characteristics of the current study, participants were required to provide their age. If a participant indicated they were not at least 18 years of age, they were directed to the “I’m Sorry Page” and not permitted to participate in the study. In addition, based on the sampling characteristics of the current study, participants were asked if they are currently practiced law in the United States. If participants indicated “No” to either question, they were directed to the “I’m Sorry Page” as they did not meet the sampling criteria. Individuals who met *all* sampling characteristics were then permitted to complete the survey.

Based on the recruitment strategy proposed in the current study, it was possible an individual could receive the survey link to participate more than once. Qualtrics provides a mechanism to circumvent individuals taking the survey multiple times, often referred to as "ballot box stuffing" (Qualtrics, 2019). Within Qualtrics you can prevent individuals from taking the survey more than once through a feature which places a cookie on their browser once participants submit the responses. Then, the next time the individual clicks on the link, the cookie will not permit the individuals from taking the survey again (Qualtrics, 2019). This feature was enabled to help mitigate the possibility of individuals submitting more than one set of responses.

The IRB at Purdue University approved the current study (IRB-2020-1703), and the approved documents can be found in Appendix C. All participants were treated in accordance with the ethical standards set forth by the American Psychological Association.

3.8 Reliability and Validity

To establish internal validity the current study utilized member checks to ensure information was transcribed correctly. As detailed in the procedures, the researcher attempted to member check the transcription from the semi-structed interviews with each participant. Further, to increase internal validity, results were triangulated across data sources to justify all conclusions. Triangulation is defined as "the process of using multiple perceptions to clarify meaning, verifying the repeatability of an observation or interpretation" (Sake, 2004; p. 454). Further, Patton (2014) discusses the use of analytical triangulation, which includes mixed qualitative-quantitative method triangulation. This is achieved by checking the consistency of findings generated by different data collection methods. In the current study, this included triangulating the three strands of data: survey items, write-in responses, and the semi-structured interviews.

With regards to reliability, the current study provided a clear audit trail. This included details of each step of the process (detailed in the procedure and the data analysis plan). This showed the rigor of the methods and also provide details, should future research plan to replicate the current study. In addition, a positionality statement can be found in Appendix E.

3.9 Summary

Phase one of the current study used snowball sampling to investigate lawyers, both prosecutors and defense attorneys, attitudes toward, knowledge of, and experience with digital evidence. The online, anonymous survey included questionnaires and open-ended questions, which is known as intra-method mixing. Only individuals who are currently licensed to practice law in a jurisdiction in the United States; and specifically practicing criminal law were included. Chapter five provides additional information on the methods associated with Phase Two. The next chapter discusses the results for phase one.

CHAPTER 4. PHASE 1

Chapter four presents the results for the current study, starting with a discussion of the data cleaning procedures and a description of the final sample. Next, the three hypotheses for the current study were analyzed and results are presented. Last, the responses from the write-in responses are presented. The write-in responses are first presented based on job category (prosecutor v. defense), and then the themes which emerged from the write-in responses.

4.1 Analysis Plan

Due to the exploratory nature, prior to analysis, the significance value for any statistical hypotheses test was set to .10 (Warren, 2007). For hypotheses one and three, first frequencies were examined and then a chi-square tested the relationship between the subject variable and the dependent variable knowledge (H1) and experience (H3). There are two assumptions for a chi-square test. First, the variables are independent of one another and second the frequencies of each cell should be great than five.

For hypothesis two, a *t*-test compared the means of the attitude scale between prosecutors and defense counsel. Due to the small sample size, the standardized effect size Hedges' g was reported since the sample size was less than 20, and the two groups had different standard deviations (Hedges, 1991). Cohen's (1977) standards were used for interpretating the effect size, which includes the following: 0.20 = small effect; 0.50 = medium effect; 0.80 = large effect.

For the write-in responses, the following analysis plan was followed. First, I familiarized myself with the data by reading the write-in responses several times. During the initial reading, I engaged in memoing to mitigate any preconceived notions or biases (Tufford & Newman, 2010). Memoing is defined as "the act of recording reflective notes about what the researcher is learning from the data" (Given, 2008). Then, I looked at each individual questions to assess the similarities and differences between prosecutors and defense attorneys. Then, I reviewed the entire data set, regardless of questions, for emerging trends. First, I explored the data by creating a word cloud to examine the data. Research suggests word clouds can be used as preliminary data analysis tool with noted limitations

(McNaught & Lam, 2010). Specifically, word clouds are created quickly and depict the frequency of individual words but do not show the context or relationship between the words and thus should not be used as the primary analysis method.

After reviewing the word cloud, I began highlighting passages of interest. Next, I used initial coding procedures to identify emerging trends and patterns that recurred across the data (Saldaña, 2013). I then organized these initial codes into categories through focused coding (Saldaña, 2013) and reduced categories to those most salient and supported by a variety of data sources.

4.2 Hypotheses Testing

4.2.1 Hypothesis 1: Prosecutors have more knowledge of digital evidence compared to defense attorneys.

Knowledge of digital evidence was measured with four true/false questions and four multiple choices questions. Frequencies were conducted to see the distribution of answers. Resulted indicated all participants, regardless of job type, selected the correct answer for item 2 (Defense = 5; Prosecutors = 10; 1 Missing), which stated: digital evidence can be obtained from an individual's computer. This item was not included in further analyses.

For items three through six, the only responses included true or false, and the "I don't know" option was not selected. For items one, seven, and eight, incorrect answers and the "I don't know" were selected by participants. The incorrect responses and "I don't know" responses were combined into one group to represent incorrect responses.

As shown in Table 5, 80% of both prosecutors (n = 8) and defense counsel (n = 4) correctly answered *true* to the statement digital evidence is information that is stored or transmitted in a binary format that may be relied on in court. The majority of respondents also correctly answered *true* to the statement digital evidence from a computer requires that an investigator takes an exact copy of the hard drive or digital devices, known as a forensic image. Only one defense attorney responded to item four. The defense attorney and 86% (n =6) prospectors correctly answered item four.

With regards to the multiple-choice questions, which pertained to court cases, the majority of respondents (73%), regardless of job status, correctly answered the question regarding *Riley v California* (73%), *Carpenter v United States* (80%) and *United States v Jones*

(60%). For the question pertaining to the *Lorraine v Stevenel American Insurance Co*. case, the majority of respondent reported not knowing the answer (64%). Further, no defense attorneys and 50 % of prosecutors answered this item correctly.

Table 5 *Responses to Knowledge Questions by Job Type*

		Prosecutors	**Defense**	**Total**
		(*n* = 11)	(*n* = 5)	(*N* = 16)
Digital evidence is information that is stored or transmitted in a binary format that ma be relied on in court (Item 1)*	Correct	8 (80)	4 (80)	12 (80)
	Incorrect	2 (20)	1 (20)	3 (20)
Digital evidence from a computer required that an investigator takes an exact copy of the hard drive or digital device, known as a forensic image (Item 3)	Correct	7 (87.5)	3 (75)	10 (83.3)
	Incorrect	1 (12.5)	1 (25)	2 (16.7)
In traditional computer forensics, a hash value is used to authenticate the integrity of the image to ensure evidence has not been altered. (Item 4)	Correct	6 (85.7)	1 (100)	7 (87.5)
	Incorrect	1 (14.3)	0 (0)	1 (12.1)
Riley v California (Item 5)	Correct	7 (70)	4 (80)	11 (73.3)
	Incorrect	3 (30)	1 (20)	4 (26.7)
Lorraine v. Markel American Insurance Co. (Item 6)	Correct	5 (50)	0 (0)	5 (35.7)
	Incorrect	5 (50)	4 (100)	9 (64.3)
Carpenter v United States (Item 7)*	Correct	8 (80)	4 (80)	12 (80)
	Incorrect	2 (20)	1 (20)	3 (20)
United States v Jones (Item 8)*	Correct	5 (50)	4 (80)	9 (60)
	Incorrect	5 (50)	1 (20)	6 (40)

Note. Values represent frequencies with percentages in parentheses. Due to rounding, percentages may not add up to 100%. Incorrect includes "I Don't Know" survey resposnes.

A chi-square analysis explored the relationship between the two groups of categorical variables: response to the knowledge questions (correct *v* incorrect) and job type (prosecutor *v* defense). An assumption of the chi-square states no expected value should be less than five. For each item, this assumption was violated and thus a Fisher's exact test (Fisher,1992) was conducted. There was no relationship between job type and item 1 ($p > .10$; Phi = .0), item 3 ($p > .10$; Phi = .16), item 4 ($p > .10$; Phi = .14), item 5 ($p > .10$; Phi = .12), item 6 ($p > .10$; Phi = -.47), item 7 ($p > .10$; Phi = .0), and item 8 ($p = .58$; Phi = .29). Although not significant, there is a medium association between job type and item 8, and a large association between job type and item 6. It was expected 3 defense attorneys would select the correct answer for item 8, but four individuals correctly answered the question. Thus, more defense attorneys got item number eight correct than anticipated based on the model. For item six, 50% of prosecutors answer the item

correct. The model expected 3.6 prosecutors to correctly answer item six, but five prosecutors answer the question correctly. Overall, results do not support hypothesis one and suggest there is no difference in knowledge between prosecutor and defense attorneys.

4.2.2 Hypothesis 2: Prosecutors have more favorable opinion of digital evidence compared to defense attorneys.

A *t*-test was run to compare the difference between prosecutors and defense attorneys and each item on the attitude scale. For items four, $t(13) = .271$, $p = .80$, $g = .140$; six, $t(13) = -1.10$, $p = .29$, $g = -.57$; seven, $t(13) = -1.08$, $p = .29$, $g = -.60$; nine, $t(13) = .23$, $p = .78$, $g = .142$; and ten, $t(13) = -.58$, $p = .60$, $g = -.30$, there was no significant difference in attitude between prosecutors and defense attorneys.

There was a significant difference between prosecutors and defense attorneys for items one, $t(13) =$, $p = .003$, $g = -1.86$, two, $t(13) = -4.42$, $p = .001$, $g = -2.28$, three, $t(13) = 2.68$, $p = .019$, $g = -1.38$, five, $t(13) = -2.28$, $p = .04$, $g = -1,17$, and eight, $t(13) = -2.66$, $p = .02$, $g = -1.37$. All significant items also had a large, negative effect. The defense scored lower compared to the prosecutors. For items one, two, and three this suggests the defense does not believe digital evidence can eliminated a suspect, prove a suspect is guilty or link a suspect to a device. For item five, results suggest defense attorney do not think digital evidence can help with unsolved cases. Results for item eight suggest defense attorneys do not think digital evidence is an asset to the criminal justice system. Overall, results support hypothesis two and suggest prosecutors have a more favorable opinion of digital evidence compared to defense attorneys.

Table 6 *Attitudes toward Digital Evidence by Job Type*

	Prosecutors	**Defense**
	n = 10	*n* = 5
*Digital evidence can eliminate a suspect (Item 1)**	4.8 (0.63)	3.6 (0.55)
*Digital evidence can prove the guilt of a suspect (Item 2)**	4.6 (0.70)	2.8 (0.84)
*An investigation can link a suspect to a digital device (Item 3)**	4.9 (0.57)	4.0 (0.71)
Digital evidence can be altered by the analyst (Item 4)	3.8 (1.55)	4.0 (0.71)
*Digital forensics analysis can be used to assist in unsolved cases (Item 5)**	4.7 (0.48)	4.0 (0.71)
Digital evidence is the most important investigative tool (Item 6)	2.9 (1.29)	2.2 (0.84)
I would base a case primarily on digital evidence (Item 7)	3.8 (1.39)	3.0 (1.22)
*Digital evidence is an asset to the criminal justice system (Item 8)**	4.8 (0.63)	3.6 (1.14)
Digital evidence is not useful in my cases (Item 9)	2.5 (2.22)	2.8 (1.30)
Digital evidence is the most reliable type of evidence we have today (Item 10)	3.2 (0.79)	2.8 (1.92)

Note. Mean (SD): * = significant

4.2.3 Hypothesis 3: Prosecutors have more experience with digital evidence in the court room compared to defense attorneys.

Experience questions asked participants about their use with digital evidence and digital forensic investigators or experts. Frequencies by job type are presented. Twenty-two percent of defense attorneys used digital evidence in court compared to 78% of prosecutors, as shown in Table 6. Forty percent of prosecutors reported using digital evidence in plea agreements compared to zero defense attorneys.

Table 7 *Experience with DE by Job Type*

		Prosecutors	Defense	Total
DE in Court				
	No	3 (30)	3 (60)	6 (40)
	Yes	7 (70)	2 (40)	9 (60)
DE in Plea Agreement				
	No	6 (60)	5 (100)	11 (73.3)
	Yes	4 (40)	0 (40)	4 (26.7)
DF Investigator or LE				
	No	0 (0)	2 (40)	2 (15.4)
	Yes	7 (87.5)	2 (40)	9 (69.2)
	No cases with DE	1 (12.5)	1 (20)	2 (15.4)
DF Expert				
	No	0 (0)	1 (20)	1 (7.7)
	Yes	7 (87.5)	3 (60)	10 (76.9)
	No case with DE	1 (12.5)	1 (20)	2 (15.4)

Note. Values represent frequencies with percentages in parentheses. DF = Digital Forensics. DE = Digital Evidence. LE = Law Enforcement.

The majority of individuals had a digital forensic investigator or law enforcement involved in their case (69.2%). All prosecutors reported involvement. Forty percent of defense attorneys reported involvement and 40% of defense attorneys reported no involvement. With regards to a digital forensic expert, 60% (n = 3) of defense attorneys and 88% (n = 7) of prosecutors had a digital forensic expert involved in their case.

A chi-square test was conducted to test the relationship between job type (prosecutor *v.* defense) and use of digital evidence in both the courts and plea agreements. An assumption of the chi-square states no expected value should be less than five. For each item, this assumption was violated and thus a Fisher's exact test (Fisher,1992) was conducted. For both the use of digital evidence in the courts (p = .33) and plea agreements (p = .23), there was no significant relationship. Although not significant, results indicate a moderate association between job type and use of digital evidence in the courts (Phi = .29) and plea agreements (Phi = .43). Based on the model, it was expected six prosecutors would use digital evidence in the last year, but 7 prosecutors used digital evidence. With regards to digital evidence in plea agreements, the model expected 2.7 prosecutors to use digital evidence, but 4 prosecutors used digital evidence in plea agreements.

As shown in Table 7, the majority of both prosecutors (73%; n = 8) and defense attorneys (80%; n = 4) participated in formal digital forensic training. Both prosecutors (46%; n = 5) and defense attorneys (60%; n = 3) participated in one to five hours of training in the last year. Over

the course of their careers, 80% of defense attorneys (n = 4) reported attending one to five hours of training. Four prosecutors (36.4%) indicated they participated in more than 10 hours of training over their career.

Table 8 *Training by Job Type*

		Prosecutors	Defense	Total
Formal Training				
	No	3 (27.3)	1 (20)	4 (25)
	Yes	8 (72.7)	4 (80)	12 (75)
Traing Past Yr.				
	0	4 (36.4)	2 (40)	6 (37.5)
	1 - 5 hours	5 (45.5)	3 (60)	8 (50)
	6 - 10 hours	1 (9.1)	0 (0)	1 (6.3)
	More than 10 Hrs	1 (9.1)	0 (0)	1 (6.3)
Training during law career				
	0	2 (18.2)	0 (0)	2 (12.5)
	1 - 5 hours	4 (36.4)	4 (80)	8 (50)
	6 - 10 hours	1 (9.1)	1 (20)	2 (12.5)
	More than 10 Hrs	4 (36.4)	0 (0)	4 (25)

Note. Values represent frequencies with percentages in parentheses. Due to rounding, percentages may not add up to 100%.

Both of the training variables were recoded to training vs. no training. A chi-square tested the relationship between job type (prosecutor v. defense) and formal digital training, training in the past year, and training during an individual's entire law career. An assumption of the chi-square states no expected value should be less than five. For each item, this assumption was violated and thus a Fisher's exact test (Fisher,1992) was conducted. There was no significant relationship between job type and formal training (p > .10; Phi = -.08), training within the last year (p > .10; Phi = .04), and training during an individual's law career (p > .10;). Although not significant, results indicate a small association between job type and training during an individual's law career (Phi = -.26). Overall, although not significant, effect sizes support hypothesis three and suggest a difference between prosecutors and defense counsel with regards to experience with digital evidence.

4.3 Write-In Response

There were multiple write-in responses to further investigate the attitudes and experiences of prosecutors and defense attorneys. First, the responses to the attitudes and experience

questions are presented. For these responses, each item represents a unique response. Only quotes which did not include identifying information (e.g., where a participant worked, specific states, etc.) were included. This section identified the differences in responses between job types: prosecutors vs. defense counsel. The final section presents the emerging themes regardless of job type and survey question.

4.3.1 Attitude and Opinions

Participants were asked their opinion on whether the use of digital evidence should be increased. Prosecutors had opposite opinions from one another with one stating digital evidence is not always available and one stating there is too much digital evidence, as shown in Table 9. The defense attorney suggested digital evidence was less reliable than people think and also stated it might bias a jury.

Table 9 *Use of Digital Evidence*

Defense Counsel	**Prosecutors**
"I think it is less reliable than people think, and it can bias a jury to putting too much stock into it."	"But [digital evidence] not always available."
	"There is so much digital evidence available, and I think much of it isn't used because of a lack of knowledge on the part of law enforcement and/or prosecutors."

With regards to their cases, participants were asked if they thought cases were more successful when digital evidence was involved. As shown in Table 10, the defense recognized digital evidence could hurt their cases and similarly the prosecutor indicated digital evidence could "demonstrate a lack of culpability."

Table 10 *Success in Case with Digital Evidence*

Defense Counsel	**Prosecutors**
"As a defense attorney, digital evidence is usually bad for me."	"By success, if you mean finding the trust, the answer is uncategorical, yes. If by success you mean conviction, probably yes but I have had cases where digital evidence demonstrates lack of culpability."
"Sometimes it helps, sometimes it hurts. It depends."	

Participants were asked what they believed to be the biggest legal issue in digital forensics currently. Two prosecutors discussed a lack of understanding and two noted problems with encryption, as shown in Table 11.

Table 11 *Current Legal Issues in Digital Forensics*

Defense Counsel	**Prosecutors**
"Preservation."	"Attorneys not understanding how it works."
"There is an assumed connection between the source of the digital evidence and the owner of the hardware. But people can use VPNs or similar programs, or there may be other reasons that cause a disconnect."	"Bypassing encryption; ECPA revisions."
"Things like anonymous tips not being corroborated before warrants are sought and obtained."	"Educating the judiciary."
	"Encryption and password cracking."
	"Particularity authenticity. Judiciary is entirely inept in the space, leading to bad cases based on misunderstandings of technology."

In addition, participants were asked what they believed to be the biggest legal issue in digital forensics in the next 10 years, and responses are provided in Table 12.

Table 12 *Future Legal Issues in Digital Foresnics*

Defense Counsel	**Prosecutor**
"Preservation."	"Bypassing encryption."
"Things involving Snapchat, Instagram, messages, and things of the like."	"Crypto Banking."
	"Expanding the scope of its use in trial. Society may believe we are violating privacy interests and rights under the constitution."

Overall, the responses to the attitude's questions revealed similarities and differences in between prosecutors and defense attorneys.

4.3.2 Experience

To better understand the experience of prosecutors and defense attorneys, participants were asked the types of digital evidence they used in court. As shown in Table 13, data from mobile devices were prevalent.

Table 13 *Types of Digital Evidence*

Defense Counsel	**Prosecutors**
"Cell phone tower data"	"Cloud based, laptop, and mobile devices"
"Electronic files and IP addresses"	"Facebook records, cell phone records, cell phone service provider records, geolocation"
	"IP addresses, email tracing, cell site data, cell phone forensics"
	"Mobile, computer location, OSINT, third party records"
	"Text message, phone records"
	"UFED Reports, text messages, FB or IG records, geolocation (geofencing)"

Similarly, participants were asked what types of evidence they used in plea agreements. Defense attorneys did not provide any answer. Prosecutors stated they used "similar types as in trials" and another participant stated they used "UFED, FB, IG, and texts."

Participants were asked what challenges, if any, they faced using digital evidence as part of their case or defense. As shown in Table 14, most of the responses were widely different between groups and within groups. However, both the defense and prosecution discussed the vast amount of data as a challenge.

Table 14 *Challenges with Digital Evidence*

Defense Counsel	**Prosecutor**
"Assisting the judge in understanding the origination of the evidence."	"Laying appropriate foundation under the [STATE] Rules of Evidence."
"Ensuring proper and effective document review when given hundreds of thousands of documents."	"Obtaining records from esps. Getting someone to authenticate said evidence. Authenticating server log files."
"Inadequate storage methods. Plus, each agency has its own proprietary program to view files."	"Putting the defendant at the keyboard."
It can be difficult to wrangle when you do not understand all of the specifics of what the data actually MEANS. I almost have to get an expert just to interpret what I am reading."	"Significant volume of evidence. Resource challenges (software, hardware, personnel). Encryption."
	"Volume of data."

Participants were also asked about success with cases involving digital evidence, as shown in Table 15.

Table 15 *Success with Digital Evidence*

Defense Counsel	**Prosecutors**
"Judges have accepted such [evidence] a vast majority of the time."	"It has been useful in lots of cases I have investigated or prosecuted. It is the most important type of evidence ever encountered in criminal investigations."
	"Obtained guilty verdicts solely based on digital evidence."
	"Obtaining actual and corroborative evidence of the crime"
	"Proving possession of child porn (CSAM) mostly or corroborating molest victims."

Overall, the experiences differed between prosecutors and defense attorneys. However, they did both discuss the large amount of data as a challenge with digital evidence.

4.3.3 Emerging Trends

The previous section discussed the similarities and differences between prosecutors and defense attorneys to specific questions regarding their attitudes toward and experience with digital evidence. This section discusses the trends which emerged from the entire data set of write-in responses, regardless of question or job type. Per the analysis plan, first a word cloud was created to visualize the data, as shown in Figure 4.

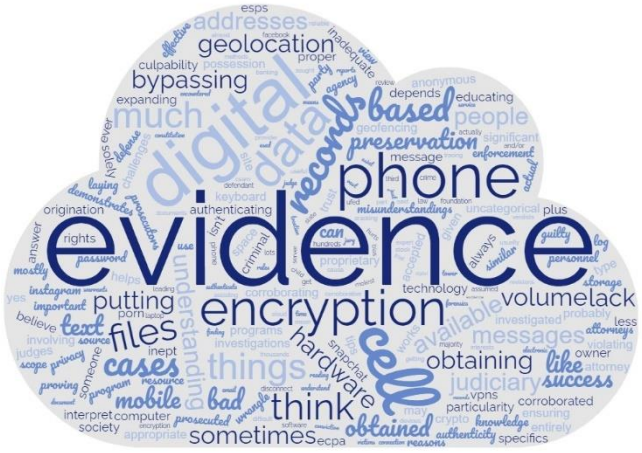

Figure 4 *Write-in Response Data Word Cloud*

The main trend which emerged from the write-in responses from both prosecutors and defense attorneys was a lack of understanding of digital evidence in the courtroom. This was discussed in three main areas: the judiciary, the jury, and fellow lawyers. First, prosecutors stated there was a lack of understanding by fellow attorneys and law enforcement. This point is exemplified in the following quote: "…I think much of it isn't used because of a lack of knowledge on the part of law enforcement and/or prosecutors." Further, one of the responses from a defense attorney suggested their own difficulties with understanding digital evidence: "It

can be difficult to wrangle when you do not understand all of the specifics of what the data actually MEANS. I almost have to get an expert just to interpret what I am reading." In addition to difficulties with understanding by lawyers, responses also indicated a lack of understanding by the judiciary. Prosecutors and defense attorneys both indicated they have to educate the judiciary on digital evidence. In addition, one individual stated: "Judiciary is entirely inept in the space, leading to bad cases based on misunderstandings of technology." How the jury understands digital evidence was not explicitly discussed in the write-in responses; however, one participant stated, "I think it [digital evidence] is less reliable than people think, and it can bias a jury to putting too much stock into it." Previous research by Holmgren (2003) suggested even if a juror does not understand the DNA evidence or statistical probability associated with the match, they believe the evidence is more credible compared to other types of evidence. The participant did not elaborate as to why "too much stock" might be given to digital evidence, and lawyers opinions and experiences with jurors and digital evidence was further explore in the follow-up interviews.

A second trend which emerged from the write-in responses was the multitude of digital evidence. The vast amount of data referred to the types of digital evidence and also the amount of data from devices. First, as shown in Table 13, digital evidence was no longer just coming from computers. Lawyers are utilizing digital evidence from a variety of sources. Mobile devices were the most popular with lawyers stating they used social media, phone records, text messages, and social media apps. Also, location from mobile devices was a common response with lawyers using both geolocations from the devices and cell site tower data. Second, respondents discussed the amount of digital data. One respondent stated, "there is so much digital evidence available." Further, two participants discussed the challenges caused by the multitude of data which include challenges with resources and the ability to "ensure proper and effective document review when given hundreds of thousands of documents."

Finally, the third trend which emerged was the challenges of connecting a digital device with a suspect. As shown in Table 11 and 14, this was a challenge presented by both the prosecution and defense. Specifically, one response elaborated on the challenge by stating:

> There is an assumed connection between the source of the digital evidence and the owner of the hardware. But people can use VPNs or similar programs, or there may be other reasons that cause a disconnect

4.4 Summary

Chapter four presented the statistical hypothesis testing for the current study and discussed the write-in responses. The write-in responses were first discussed based on job category: prosecutor vs. defense. Then, the emerging trends were presented. The next chapter discusses phase two of the study which sought to further explore the findings from phase one and the emerging trends.

CHAPTER 5. PHASE 2

The goal of phase two was to further explore and explain the emerging themes from phase one. Specifically, the interview protocol was developed to explore the statistical survey results and emerging findings from the write-in responses. Chapter five first presented the methods for phase two, which included participants and recruitment, procedures, interview protocol, and analysis plan. The interview setting and interviewee profiles were also presented. Finally, the themes from the interviews are discussed.

5.1 Phase 2 Methods

5.1.1 Participants and Recruitment

Creswell and Plano Clark (2011) discussed a systematic way to sample in a follow-up phase for an explanatory mixed methods study by allowing the results from phase one to dictate who would be the best participants to inform and explain the findings. Therefore, purposeful sampling was implemented for phase two, which is the strategic and purposeful selection of a specific number of cases that aligns with the purpose of the study and the researcher's resources (Patton, 2001). Based on this sampling procedure, lawyers with digital evidence experience were solicited.

Six lawyers were recruited via e-mail or social media messaging (e.g., LinkedIn). Similar to the sampling criteria in phase one, participants recruited were (1) individuals who are currently licensed to practice law in a jurisdiction in the United States; and (2) individuals are specifically practicing criminal law. In addition, a third sampling criteria was included for the interviews which was specific experience with digital evidence. To further explore the findings from phase one, it was imperative the participants had experience with digital evidence. Therefore, this was asked of each participant who volunteered to patriciate in the interview while setting up the interview. The question was also asked as part of the interview protocol.

5.1.2 Procedures

Recruitment e-mails for interview participation were sent to lawyers via e-mail or social media message (e.g., LinkedIn). If an individual agreed to participate, they were sent a copy of

the consent form via e-mail and a link to electronically sign the form and fill out a brief survey via Qualtrics. The survey only contained the consent form and seven demographic questions. The demographic information was used to create interviewee profiles which are presented in Chapter five. The surveys were reviewed before each interview to ensure the participants consented.

The interviews took place via the virtual meeting platform, Zoom. Once the participant joined the meeting, the researcher asked: if they had any questions regarding the consent form, if they consented to the study, and if they consented to the recording and transcription of the interview. Zoom has a feature which allows for the transcription of recordings. All interviews were recorded and transcribed by Zoom.

To keep the identity of the participant confidential, transcripts were de-identified by using a pseudonym to replace individuals' names, and any other potentially identifying information was removed from the transcript (e.g., specific states, investigator names, office information).

After each interview, Zoom provided the recording and transcript. The researcher listened to each interview while reviewing the transcript multiple times to ensure the interview was properly transcribed. While listening to the recordings and checking the transcripts, the researcher engaged in memoing to capture initial thoughts to help separate the researchers' thoughts from the responses of the participants. Once each transcript was finalized, the audio file was deleted, and the transcript was stored in a password protected file.

Phase one IRB was modified to include the new interview protocol. The IRB at Purdue University approved the modification (IRB-2020-1703), and the approved documents are located in Appendix D. All participants were treated in accordance with the ethical standards set forth by the American Psychological Association.

5.1.3 Interview Protocol

The interview protocol was developed based on the results from phase one. The goal of the follow-up interviews was to further explore the findings from phase one. As shown in Appendix B, the interview protocol included three main sections which corresponded to the research questions: knowledge, attitudes, and experiences.

5.1.3.1.1 Knowledge

In phase one, knowledge survey items were assessed by correct responses to fact-based questions regarding digital evidence. Based on the trends which emerged from the write-in responses, prosecutor and defense attorneys discussed a lack of understanding and knowledge by fellow attorneys and the judiciary. To further explore this trend, the interview protocol asked participants their opinions on the knowledge of fellow attorneys, judges, and the jury.

5.1.3.1.2 Attitudes and Opinions

In phase one, attitude referred to participants beliefs and opinions about digital evidence, and its use in the court room and was measured through a Likert-scale and write-in response questions. The interview protocol furth explored this area by asking participants how digital evidence was helpful or hurtful in their cases and asked participants to provided examples. The interview protocol also assessed opinions on the current and future challenges of digital evidence.

As discussed in the emerging trends section, the jury understanding of digital evidence was not explicitly discussed in the write-in responses; however, one participant stated, “I think it [digital evidence] is less reliable than people think, and it can bias a jury to putting too much stock into it.” Therefore, lawyers’ opinions and experiences with jurors and digital evidence was further explored in the follow-up interviews.

5.1.3.1.3 Experience

During Phase 1, experience was measured through a questionnaire and write-in responses. Questions assessed the use of digital evidence in court cases and also in plea agreements. Results indicated more prosecutors use digital evidence during trial and plea agreements. Based off the write-in responses, experiences differed between prosecutors and defense attorneys. However, both prosecutors and defense attorneys discussed the large amount of data as a challenge with digital evidence. Therefore, the interview further explored experiences with digital evidence by asking participants to elaborate and share stories or specific cases which involved digital evidence.

In addition, as previously discussed, a lack of understanding was an emerging theme in the write-in responses. As a result, the interview protocol included questions regarding experience with educating the judge and also the jury. The protocol also included a broad question to investigate other challenges prosecutors or defense attorneys encountered based-off of their experiences.

5.1.4 Analysis Plan

Phase two analysis followed the same steps as phase one and therefore is briefly described. I reviewed the transcripts multiple times while checking the transcribed transcripts and the audio recording. To start the analysis process, I familiarized myself with the data by reading the finalized transcripts. I explored the data by creating a word cloud to examine the data. Next, I highlighted passages of interest. I then used initial coding procedures to identify initial themes and patters that recurred across the interviews (Saldaña, 2013). I then organized these initial codes into categories through focused coding (Saldaña, 2013) and reduced categories to those most salient and supported by a variety of data sources.

5.2 Setting

The interviews were conducted during August and September 2021. The interviews took place via the meeting platform, Zoom. For all four interviews, both the interviewer and the participant used their webcam which allowed for a face-to-face virtual interview. On average, the interviews lasted 34 minutes.

5.3 Interviewee Profiles

This section presents an interviewee profile for each participant. To protect the identity of the individuals who participated, all names are pseudonyms. All four participants had qualification and unique experiences which made them ideal participants for the interviews.

Holly is a white, female, and 30 years old. She is a current prosecutor for a state in the southeast United States. She graduated law school in 2016. Holly has not currently attended professional training on digital evidence. She has a working relationship with individuals at the local, state, and federal level who she can contact questions regarding digital evidence. She has

prosecuted multiple cases with digital evidence and thus has ample experience prepping and questioning expert witnesses.

Alexis is multiracial, female and 31 years old She is currently an insurance defense attorney and was previously a prosecutor for a state in the southeast region of the United States. She graduated law school in 2015. Alexis has attended digital forensic training while she worked as a prosecutor. She also tried cases and prepared cases for trial which involved digital evidence. Her responses were all based on her experiences as a prosecutor.

Steven is a white, male, and is 32 years old. He is a public defender in a southeast state in the United States. He graduated law school in 2014. Steven has not attended digital forensic training but consults books and resources regarding digital evidence.

Lauren is a white, female, and is 31 years old. She is a private defense attorney. She graduated law school in 2014. She has not attended formal digital forensic training but has experience with digital evidence in trial and leading up to plea agreements. She works with local and federal digital forensic investigators. Also, she serves as a panel attorney for the Criminal Justice Act (CJA), where is accepts a handful of appointments each year to represent indigent defendants.

5.4 Themes

The goal of phase two data collection and analysis was to better understand the results from phase one and further explore the emerging trends. First, a word cloud visualized the data derived from the interviews, as shown in Figure 5.

Figure 5 *Interview Data Word Cloud*

Three themes emerged from the data, which included prevalence of digital evidence, lack of resources, and a lack of understanding (each discussed below). In addition, to the themes, differences between the prosecutors and defense attorneys also emerged. Specifically, with regards to the usefulness and strength of digital evidence, the prosecutors and defense attorneys differed in their opinions. One theme also emerged that was only among the defense attorneys, specifically concerns regarding how digital evidence is presented.

5.4.1 Prevalence

Similar to the emerging trends from phase one, the interviews revealed digital evidence is increasing with regards to prevalence in cases and volume of data. For example, Holly suggested "technology at this point is in every case." Holly further explained by stating:

> If you have a Class A felony, a murder or rape, and you don't have any kind of forensic evidence and it's just witnesses, I mean, naturally, you have a very large hill to climb. Nowadays, people expect what was on their cell phone…and if you don't have that, it is a huge blow your case.

Lauren echoed this point by stating:

> I would say that there is not a single federal case that I really get that doesn't include at least a one terabyte hard drive of data. In state cases, depending on the severity of the offense and the type of investigation, you still have less usually than the feds do, but there's a lot and it's always changing.

Lauren's statement illustrated the prevalence of digital evidence in cases and also the volume of data involved in cases. Steven also discussed the volume of data by explaining

> the data is massive, it's so massive in fact that there are - you know even just from like a cell phone report - the state will miss something [in the data].

Steven also stated there was generally too much data, and not enough resources.

5.4.2 Lack of Resources

Building of Steven's comment regarding "not enough resources," the other participants also commented on the lack of resources or differences between resources for the state, public defenders, and private defense attorneys. For instance, with regards to public defenders' resources, Holly stated:

> I think they [public defender] have access to less resources, but at the same time it benefits them the confusion right, so they want a jury that doesn't understand it

Based off of Alexis' experience, there were fewer challenges for the state regarding resources, she stated, "for the state that there are less challenges, because we have all the resources that we can pull." However, with regards to the private defense attorneys, Alexis stated:

> When it comes to the defense, it can depend on if they can afford it to hire the forensic people and hire everyone, and they spare no expense then fine.

With regards to the public defenders, Alexis said:

> The public defender's office has their own great budget, but I also know that they also kind of pick and choose their cases. The higher ups evaluate the case, and if they see this is not worth the expense of the digital evidence, they're not going to they may not do it, no matter if the line attorney says that we need it.

Steven stated the lack of understanding was because of a lack of training for all court room actors, both attorneys and the judge. This point was illustrated in the following:

> I think that it is so dense, and that people don't have a big understanding of it and the people don't have training - the prosecutor doesn't, Defense attorney don't, that judge doesn't. That's just a fact that nobody has enough training on it and because we're not, it's hard to present something if you don't fully understand it.

With regards to training, only one of the participants, Alexis, reported attending formal digital forensics training. Both defense attorneys, Steven and Lauren, stated they consulted books, the Internet, and other resources to learn about digital evidence. Both prosecutors and Lauren also stated they consulted investigators at the federal, state, and local level with questions regarding digital evidence.

5.4.3 Lack of Understanding

Lack of understanding of digital evidence was the third theme which emerged in the data. Steven suggested there was a lack of understanding by the state attorneys. For instance, Steven stated, "I think sometimes the State doesn't understand it when they use it and the way they explain it." With regards to the judiciary, Steven stated, "I also think the judges do their best, but I think they probably don't have a solid handle on that either." Based off Lauren's experience in federal and state courts, she suggested the following:

> I would say that the Federal judges all know pretty well just because of the amount that gets put into search warrants in Federal Court, even though they have less trials, I will say that you know other judges might be all over the map and it's just a matter of making sure that you educate them as well.

Based of Holly's experience, there were times when evidence was so "cutting edge" that she needed to explain it and educate the judge. Holly describes the process for introducing new or cutting-edge digital evidence:

> I would never just introduce it at trial and then expect the judge quickly to make a ruling. If there's something new that he hasn't seen or something I think is kind of on the edge, I would always do that well before trial because it usually it takes time in trial you don't really have time to educate the judge.

With regards to the jury, Lauren suggested, "I think the jurors can understand it if it's presented in a manner that they can understand." And added, "it is frequently not presented very well."

Further, Steven suggested lawyers lack of knowledge could impact the jurors understanding, by explaining:

> Because the lawyers do not understand digital evidence they struggle. I think, in turn, I think the jury has a hard time with it, too, and puts emphasis on things that maybe shouldn't have emphasis put on them.

With regards to the jury, Alexis stated:

> I think they put a lot of weight to it because it's not as subject to interpretation

While a lack of understanding by fellow attorneys, judges, and the jury was the main theme which emerged, two of the participants did suggest they had a good understanding of digital evidence. For instance, Steven suggested he had above average understanding of digital evidence. Alexis acknowledged she understood the type of evidence she had for her cases, but discussed needing an expert to help with interpretations as illustrated in this quote:

> We understood what kind of evidence we had… But we really needed, like the detective who specializes in that stuff to interpret what exactly it meant.

5.4.4 Strength and Usefulness of Digital Evidence

Opinions regarding the strength and usefulness of digital evidence differed based on job type. Both prosecutors suggested using digital evidence is hard to "fight" or "refute." For instance, Alexis stated:

> A lot of cases fall apart because of the witnesses, but the digital evidence is really hard to fight. I think the digital evidence is harder to refute

Holly suggested: "the strength of your cases is digital evidence." Holly also stated, in general, digital evidence was very helpful to her cases and discussed the strength of evidence with regards to plea agreements: "if your evidence is so strong there's no point in them taking it to trial then they're going to plea."

Opposite to the prosecutors, both the public defender and the private defense attorney did not think digital evidence was helpful to their case. For instance, Steven stated: "I mean for the most part, just like any other kind of evidence, if there is ab bunch of it, it is usually not good for me." Lauren echoed this point by stating "it [digital evidence] usually hurtful in federal cases."

Although both defense attorneys stated digital evidence was hurtful to their cases, based on their experiences, they both had examples where digital evidence helped reduce the charge for an offender or exculpate a client.

5.4.5 Presenting Digital Evidence

Both defense attorneys discussed concerned regarding how digital evidence is presented. Lauren suggested "it [digital evidence] is frequently not presented very well." Steven also stated: "I think a lot of stuff gets lost in like cell phone like pings stuff. I think there's a lot that gets skewed."

More specifically, they discussed the evidence is reliable if discussed accurately and the constraints of the evidence are described. Lauren stated, "within the evidence's own constraints, yes, there are ways to make sure that whatever is being introduced is reliable." She followed this claim with an example:

> So, if there's a text message that gets introduced into evidence. Um, you can make it so that it is reliable. There is reliable digital evidence proving that on a specific date a text message was sent from you know one cell subscriber to another that received it. Now, if that text message says, I just committed a crime um there's no way that, that can prove the person actually did you know. The actual content of it is at issue, so making sure that you respect those boundaries.

Lauren also discussed concerns with lawyers mispresenting the evidence and having to "clean it up on cross examination" of the witness and also concerns with lawyers who miseducate the judge when initially presenting the evidence. Based on her experience, this has happened multiple times. For instance, in one case, the state attorney introduced evidence but did not account for difference in time (UTC). Additionally, in another case, Lauren discussed a time where the prosecutor had the expert witness walk through a process but making larger claims about the digital evidence in which Lauren asked specific questions about the meaning of the evidence to demonstrate its constraints.

Both Steven and Lauren had concerns regarding state attorneys suggesting the evidence places the defendant at a specific location. For instance, Steven suggested

> I think it all comes down to how its presented. I think it can be reliable, but if it's used very generally, I think it's reliable. If you're using it very specifically to say this person was at X

> address whatever because that's just not really what the data shows. And a lot of that depends on what the judge allows people to say and how he allows the evidence to be presented.

Lauren echoed this point by stating:

> The one of the things that drives me up a wall is that prosecutors, like to say: the person was here and I'm like no if the person was there, I would have submitted an alibi Defense

These concerns and opinions were not expressed by the prosecutors.

5.5 Summary

Chapter five presented phase two of the study. The goal of phase two was to explore the findings and emerging trends from phase one. This chapter discussed the methods for phase two, which included virtual, semi-structured interviews with four participants: two prosecutors and two defense attorneys. The interview protocol was derived from phase one findings. A discussion on the interview protocol was presented, and the chapter concluded with the interviewee profiles and themes.

CHAPTER 6. DISCUSSION

The current study was the first to examine the differences between prosecutors and defense counsel with regards to their knowledge of, attitude towards, and experience with digital evidence using a mixed-methods approach. The current study included two phases. The first phases consisted of an online, anonymous survey. Results from phase one were further explored in phase two, which consisted of semi-structured interviews. This chapter discusses the findings from phase one, followed by the findings from phase two, and then the merged findings and meta inferences. Limitations and future research directions are also discussed.

6.1 Phase One

Phase one of the current study included 11 prosecutors and five defense attorneys, with both private defense attorneys and public defenders represented. Based on statistical hypothesis testing, results indicate overall, there is no difference between prosecutors and defense attorneys regarding knowledge. Results do not support the first hypotheses of a difference in knowledge between prosecutors and defense attorneys. However, an emerging theme from the write-in responses for phase one suggests a lack of understanding by courtroom actors, including lawyers and the judiciary. This emerging theme is consistent with previous research. While knowledge of lawyers has not directly been investigated, a previous study found prosecutors held the opinion that defense attorneys are not knowledgeable and struggle with digital forensics (Goodison et al., 2015). In the current study, one defense attorney stated.

> It [digital evidence] can be difficult to wrangle when you do not understand all of the specifics of what the data actually MEANS. I almost have to get an expert just to interpret what I am reading

The quote illustrated the point of Goodison and colleagues (2015) as law enforcement held the opinion that prosecutors have difficulties with digital evidence (Goodison et al., 2015). In the current study, one of the prosecutors discussed a lack of understanding by attorneys as one of the biggest challenges with digital evidence which is consistent with opinions in previous research (Goodison et al., 2015).

Derived from the opinions of lawyers' who participated in the current study, judges' knowledge is an area of concern regarding digital evidence. Write-in responses from phase one indicated prosecutors and defense attorneys have to educate the judiciary regarding digital evidence. Specifically, one lawyer stated the "judiciary is inept" and two lawyers discussed the need to educate or assist the judge with regards to digital evidence. These findings differ from previous research. Specifically, in 2010, Kessler found judges were aware of digital evidence. The difference between the findings in Kessler (2010) and the current study could be due to the multitude of new digital devices and data types which are included in the umbrella term, digital evidence. Specifically, in current study participants indicated a wide array of digital devices and types of digital evidence which are used in court. Participants listed mobile devices and evidence from such device (e.g., text messages, Snapchat) as a prominent type of digital evidence used in court. At the time of the previous research (2010), digital evidence referred only to computers and e-mail. Judges are likely falling behind in their knowledge due to the vast number of devices and types of data which suggests more training for the judiciary is necessary. Not only more training, but continued training is needed as technology will continue to evolve and new devices and types of digital evidence will emerge. It is imperative judge's stay up to date on such technological advancements that impact digital evidence.

The second area examined in the current study was lawyers' attitudes toward digital evidence. The hypothesis was supported as results suggested there is a difference in opinions regarding digital evidence based on job types. Overall, prosecutors held a higher opinion of digital evidence compared to defense attorneys. More specifically, results suggest defense attorneys are less likely to believe digital evidence can eliminate a suspect, prove the guilt of a suspect, or link a suspect to a digital device. Further, the write-in responses indicated the defense believes digital evidence is usually bad or hurtful to their cases compared to prosecutors who indicated digital evidence is helpful to their cases. The defense's low opinion of digital evidence could impact their use of such evidence in court. That is, if the defense believes digital evidence cannot eliminate a suspect and will only hurt their case, they may be less likely to use such evidence in court. Although it is possible in some cases digital evidence will hurt their case, that is likely not always the case and thus valuable evidence might be overlooked.

As discussed in the results, one of the defense lawyers stated, "I think it [digital evidence] is less reliable than people think, and it can bias a jury to putting too much stock into it." Although

this is the opinion of a single defense lawyer, previous research has examined the weight jurors put on DNA evidence and finding suggest jurors have difficulty understanding DNA evidence and assigning weight to such evidence (Holmgren, 2003). Further, Taslit (2004) suggested one of the main tasks of a lawyer is to find persuasive evidence, suppress what is harmful, and grip the jury's attention (p. 4). Taslit (2004) also postulated that "computer technology has changed the way jurors think" (p 4). Future research should examine juries understanding of digital evidence and the weight digital evidence is given in their decision-making process.

With regards to experience, results from phase one support the hypotheses of a difference in experience between prosecutors and defense attorneys. Results indicate prosecutors are more likely to use digital evidence in trial. The current study was the first to assess the use of digital evidence in pela agreements. Results indicate prosecutors are more likely to use digital evidence as part of a plea agreement. Defense attorneys reported never using digital evidence in plea agreement. The defense not reporting the use of digital evidence is likely due to their role in the plea agreement process. Digital evidence and plea agreements were further explored in phase two.

Similar to Losavio et al. (2008), the current study investigated lawyers' experiences with digital evidence. Losavio et al. (2008) investigated the use of e-mail, the Internet, and websites and found these types of evidence were rarely used in court. Losavio and colleagues (2008) postulated there would be an increase in digital evidence in the future. The current study found the majority of participants used digital evidence in court. 70% of prosecutors and 40% of defense attorneys used digital evidence. The current study confirms Losavio and colleagues' (2008) opinion that digital evidence would expand and increase in the years to come.

Overall, phase one results indicate a difference in attitude towards digital evidence, with prosecutors holding a higher opinion compared to defense attorneys. Results also indicate a difference in experience with digital evidence. No differences were found between prosecutors and defense attorneys regarding knowledge. However, an emerging theme from the write-in responses revealed a lack of understanding for digital evidence in the court room by attorneys and the judiciary. These results were further explored in phase two data collection and analysis and are discussed in the next section.

6.2 Phase Two

The goal of phase two was to further explore and explain the emerging themes and findings from phase one. Based on the findings, a semi-structured interview protocol was developed to further explore the statistical results and emerge themes in phase one. Phase two sampling specifically included participants who had experience with digital evidence as they were the most qualified informants to explore the findings from phase one. Two prosecutors, one private defense attorney, and one public defender were interviewed via Zoom. Three themes emerged, which included prevalence of digital evidence, lack or resources, and a lack of understanding.

Prevalence of digital evidence, both in terms of types of data and amount of data, was discussed by both prosecutors and defense attorneys. All four participants discussed various types of data they use in their cases, which included pictures, videos, geolocation, and call history, to name a few. Additionally, Steven and Lauren both discussed the vast amount of data encountered as part of their cases. In addition, based of the cases and experiences shared by the participants, digital evidence is not only part of computer or cybercrimes cases but also "traditional" crimes such as, murder, assault, robbery, etc. Further, both the prosecutors and private defense attorney agreed digital evidence is currently part of almost all cases. Not only is it involved in more types of cases, but participants also discussed they believe digital evidence is expected by the jury. The expansion of digital evidence in cases has been postulated in the literature (Clifford, 2001; Saleem, Baggili, & Popov, 2014; Sammons, 2015). These finding are consistent with previous literature which speculated there would be an increase in types of digital evidence in the future (Losaivo et al., 2006). Further, this is consistent with the emerging theme in phase one which indicated a multitude of digital devices and types of digital evidence being used in court.

Lack of resources regarding digital evidence was the second theme which emerged. Steven, a public defender, stated one of the challenges with digital evidence is the amount of data and lack of resources. Further, Steven suggested no one has adequate training with regards to digital evidence. This point illustrated previous research by Hughes and colleagues (2019) which called for the need of forensic training, specifically DNA and digital evidence, for defense attorneys because they (lawyers) are not able to be an expert in all of the forensic fields.

A lack of understanding by lawyers and judges was also discussed in the interviews. Specifically, the need to explain new, cutting-edge digital evidence to the judge was discussed. This is consistent with the emerging findings from phase one which suggested lawyers have to educate the judiciary and the possibility judges are falling behind in their knowledge of digital evidence.

In addition, to the themes, differences between the prosecutors and defense attorneys also emerged. Specifically, with regards to the usefulness and strength of digital evidence, the prosecutors and defense attorneys differed in their opinions. The prosecutors believe digital evidence is harder to refute and helpful to their cases compared to the defense attorneys who suggested digital evidence is hurtful to their cases. This is consistent with the statistical findings in phase one which suggest prosecutors have a higher opinion of digital evidence compared to defense attorneys. Further, this difference in opinion was also mentioned in the write-in responses in phase one. Specifically, one defense attorney stated: "As a defense attorney, digital evidence is usually bad for me" compared to a prosecutor who stated: "Obtained guilty verdicts solely based on digital evidence." Both phase one and phase two results show a difference in opinion regarding digital evidence based on job category.

One theme also emerged only among the defense attorneys, specifically concerns regarding how digital evidence is presented. Both defense attorneys were concerned with how the digital evidence was presented suggesting the state used digital evidence too specifically to indicate a person's whereabouts and or what they are sending on their mobile device, for example. Both defense attorneys suggest digital evidence should be used more generally.

6.3 Integrated Findings and Inferences

The goal of a mixed methods study is to use both phases of data collection to better understand the phenomenon. A strength of mixed methods design is integrating both strands of data to draw conclusions and inferences. Integration is the bringing together of both quantitative and qualitative data (Creswell, 2015; DeCuir-Gunby & Schutz, 2017). This section discusses the integrated results and inferences from phase one and two.

Similar to the emerging trends from phase one, the interviews revealed digital evidence is increasing with regards to prevalence in cases and volume of data. For instance, in phase one, frequency data indicated 78% of prosecutors used digital evidence in their cases. In the write-in

responses, prosecutors listed a multitude of types of digital devices and data types which they use in their cases. Similarly, in the interviews, Holly, a prosecutor, discussed how digital evidence was a part of most, if not all, cases and that the absence of such evidence presented problems when taking cases to trial. One of the emerging trends from phases one was the vast amount of data. Both prosecutors and defense attorneys touched on the amount of digital data available. This point was echoed in the interviews by Steven and Lauren who discussed the large amount of data they must review as part of their cases.

In additional to the multitude of devices and data, both phase one and phase two showed digital evidence was not only used in computer or cybercriminal behavior; rather, it is also used in "traditional" crimes, such as murder, assault, and burglary. Case examples from the interviews showed digital evidence ass frequently used in wide variety of cases. Further, examples of computer crimes or cybercrimes were not discussed in the experiences of the participants interviewed.

A lack of understanding was an emerging trend in phase one and a theme in phase two. Specifically, educating the judiciary was discussed in phase one and two which could indicate judges are falling behind or struggling to keep up with emerging digital evidence.

6.4 Limitations

The current study has several limitations. First, the main limitation of the current study is the sample size of phase one. Phase one included 11 prosecutors and five defense attorneys which makes the findings less generalizable. However, the sample size is consistent with previous research. For instance, Holmgren's (2003) dissertation included two defense lawyers, two prosecutors, and two judges, Kessler's (2010) dissertation included 18 judges. Although, the sample size is consistent with previous research, readers should be cautious when reviewing the results due to the limited sample size which impacts the external validity of the study. The findings are specific to the current study and cannot be generalized to the population of criminal lawyers in the United States.

A second limitation of the current study is the lack of control variables. The survey included multiple questions to be used as control variables, such as previous employment, previous intern/fellowship experience, education, and training. Due to the small sample size and statistical limitations, the control variables were not included in analysis.

A third limitation is the current sample of lawyers compared to the population of lawyers in the United States. Specifically, the majority of the current study was white (94%), which is 9% higher than the ABA survey (2021). The current study also attempted to solicit underrepresented minorities from the African American Attorney Network, Northern Virginia Black Attorney Association, and Hispanic National Bar Association. However, the author did not receive a response from the organizations contacted.

A fourth limitation of the current study is the survey items. The survey items were adapted from previous research which aimed at investigating DNA evidence. Although the survey was reviewed by experts in the field, this was the first time the survey was used in a study. Finally, a fifth limitation was the use of self-report data for the survey in phase one. Specifically, respondents may have selected what they perceived to be the socially desirable answers or misremembered their experiences with digital evidence.

6.5 Future Research

Phase one of the current study used a snowball sampling method which involved e-mailing potential participants, asking for their participation, and asking them to send the survey to additional participants who meet the sampling criteria (Kemper et al., 2003; Patton, 2001). Future research would benefit from the use of different sampling procedures and research methods to obtain a larger sample. When sampling a population of lawyers, future research should keep in mind the fundamentals of fieldwork research, which stresses the importance of gaining access to the population (Shenton & Hayter, 2004). Specifically, using the tactic of reciprocity to demonstrate the benefit of participation in the study to the organization to foster an exchange (Sharp & Howard, 2004). For instance, this tactic was used in Levin et al. (2021) to investigate forensic science professionals, which is also a hard population to sample. Specifically, the researchers provided crime labs with individual feedback sessions if they agreed to participate in the research study (Levin et al., 2021). This tactic could similarly be employed with lawyers by first developing a relationship with an organization, soliciting the survey, and then providing results and recommendations directly to the organization.

Losavio and colleagues (2008) distributed a self-report survey in-person at a law seminar. Future research should consider the methods employed by Losavio and colleges (2008) and solicit surveys at national conferences. When used as a distribution method, the online survey

platform Qualtrics includes a quick response (QR) code which allows the researcher to put the code on solicitation flyers for distribution. Then, a potential participant can scan the QR code with their mobile device, upon scanning the QR code the individual will be directed to the survey. Flyers with QR codes could be distributed and displayed at conferences, such as the ABA Annual Meeting. Notably, this method was originally part of the solicitation plan for the current study but could not be utilized due to the cancelation of national conferences over the last 20 months due to the coronavirus pandemic.

The use of test-like questions, including True/False and multiple-choice items, is consistent with previous research (Homgren, 2003; Hans et al., 2011, Lincoln et al., 2014;). Future research should continue modifying the current study or using different methods to measure knowledge. For instance, item two, which stated: digital evidence can be obtained from an individual's computer, was correctly answered by all respondents, regardless of job type. This could suggest the item was too easy and should be removed from the survey. Second, based on the experiences identified in the current study and the types of evidence lawyers reported using, the items should be revised. For instance, an additional item regarding mobile forensics should be added to the questionnaire, as this was a type of evidence listed by most participants. Future research should consider the use of different methods to measure knowledge. For instance, a recent study by Holt and Dolliver (2021) used vignettes to assess officer's ability to recognize digital evidence in the field. Vignettes are also a common method for jury research (*see* Schwarts & Hunt, 2011; Remmel, Glen, & Cox, 2019). To assess lawyer's knowledge of digital evidence and its use in criminal proceedings and plea agreements, a vignette could be developed. Future research should consider this method.

For the self-report job status question, an "other" option was provided to account for individuals who may practice criminal law as one of their job responsibilities, but it is not the primarily role of their job. Of the 10 individuals who selected this option, review of the write-in responses indicated these individuals did not practice criminal law as part of their job responsibilities. These ten individuals did not meet the sampling characteristics for the current study and were removed from hypothesis testing. However, future research regarding civil attorneys is needed. To date, there is a lack of research which examined civil attorneys understanding of, experience with, or attitudes towards digital evidence. The ABA indicates digital evidence is important in civil cases, such as a civil lawsuit, an employee leaving a

company to work at a competitor, or divorce cases (2017). Further, in one study a participant stated, “the civil side has been more advanced around electronic evidence” (Witwer er al., 2020; p. 11). However, there is no empirical research to support this opinion, thus, the inclusion of civil attorneys in future research is needed.

The current study found lawyers are concerned the jury does not understand digital evidence and also puts too much weight on such evidence. Therefore, future research should examine jurors’ understanding of digital evidence and the weight of digital evidence in their decision-making. As discussed in the literature review, there is a multitude of literature which examined jurors understanding of forensic science evidence, and specifically DNA evidence. However, to date, there is no research regarding digital evidence.

Previous research found judges were aware of digital evidence (Kessler, 2010), however the current study found lawyer’s believe judges are not aware of digital evidence and lacking in understanding such evidence. Nearly 10 years later, the presumed awareness and knowledge level of judge’s has changed. Future research should examine the current trainings for judge’s and the effectiveness of such trainings. Technologies will continue to evolve and long-term solutions to keep judges up-to-date on the different types of evidence should be explored.

In addition, future research should develop and implement digital forensic trainings for both prosecutors and defense attorneys. Evaluation of such training are also needed to determine their effectiveness. Also, longer term solutions to keep lawyers up to date on types of evidence is needed and an area for future research.

Further, the current study found defense attorney have a lower opinion of digital evidence compared to prosecutors. While it is postulated that this negative opinion could impact their use of such evidence in their cases, future research should examine the relationship between opinions towards and use of digital evidence. In addition, any future research which examines lawyers’ knowledge of, attitudes towards, and experience with digital evidence should seek a larger sample size and look at the relationship of the control variables included in the current study and discussion in section 3.4.2.

6.6 Conclusion

Digital evidence is an essential part of the criminal justice system. Lawyers, both prosecutors and defense counsel, need to understand the wealth of information available from

digital devices, the process for acquiring digital evidence, the ethical and legal considerations for obtaining such evidence, and ultimately how this evidence is used in criminal proceedings. A lack of knowledge can result in a miscarriage of justice. The 6th Amendment of the United States Constitution guarantees citizens the right to a fair trial, which includes a defense. However, defense attorneys are largely absent in research regarding lawyers' understanding of evidence in criminal proceedings. Previous research has postulated defense attorney's knowledge of digital evidence and the challenges the defense may face, but no defense attorneys were included in the study (Goodison et al., 2015). One study by Losavio and colleagues (2008) did investigate defense experience with digital evidence. However, the study is outdated as a result of the increase in types and use of technology. Further, Losavio and colleagues (2008) did not compare defense attorneys and prosecutors.

The current mixed-methods study filled this gap in the literature by comparing prosecutors and defense attorney's knowledge of, attitudes towards, and experience with digital evidence using two strands of data. Phase one of the current study used a snowball sampling to solicit lawyers, who currently practice criminal law in the United States, via e-mail. The second phase included purposeful sampling of lawyers with experience using digital evidence to further explore the findings from phase one.

Overall, results from phase one indicate there is no difference in knowledge between prosecutors and defense attorneys. However, prosecutors believe there is a lack of understanding among attorneys regarding digital evidence and defense attorneys reported struggling with digital evidence. Ensuring both prosecutors and defense attorneys are knowledge and aware of digital evidence is imperative to a fair trial. Further, phase one results indicate prosecutors hold a higher opinion of digital evidence compared to defense attorneys. This point was echoed in the write-in responses where defense attorneys stated digital evidence is "bad' and "hurtful" to their cases compared to prosecutors who discussed ways digital evidence is helpful to their cases. Phase one also found a difference in experiences between prosecutors and defense attorneys which was further explored in phase two.

Overall, phase two results echoed the findings from phase one and further explained the difference in opinion and experiences between prosecutors and defense attorneys. Specifically, similar to phase one, prevalence of digital evidence and a lack of understanding in the court regarding digital evidence emerged as a theme in phase two. In addition, a lack of resources was

a theme in phase two. Defense attorneys discussed the large amount of data and lack of resources as a challenge. This point was also stated by a prosecutor in the write-in responses in phase one. One theme also emerged that was only among the defense attorneys, specifically concerns regarding how digital evidence is presented.

In addition, to the themes from phase two, difference between the prosecutors and defense attorneys also emerged. Specifically, with regards to the usefulness and strength of digital evidence, the prosecutors and defense attorneys differed in their opinions. Both phase one and two found prosecutors have a higher opinion of digital evidence compared to defense attorneys. Prosecutors are more likely to believe digital evidence can assist or help their cases and interviews revealed prosecutors attempt to have digital evidence in every case and/or an explanation as to why digital evidence is not included. On the other hand, defense attorneys believe digital evidence is hurtful to their case. Although both phase one and phase two results indicate defense attorneys view digital evidence as hurtful, examples from the interview show both defense attorneys had specific cases where digital evidence helped their case. In one instance, digital evidence acquitted the defendant and in a second example, digital evidence reduced the charges for the defendant. Thus, the low opinion of digital evidence may not be due to actual case experience and outcomes but a lack of understanding or resources.

There were several limitations associated with the current study. Namely, the sample size for phase one and two is small. However, the sample size is in line with previous research examining lawyers (Holmgren, 2003; Losavio et al., 2008). A small sample size withstanding, the current study was able to draw triangulated inferences based on the three strands of data collected using a mixed methods approach. The triangulated findings add to the validity and reliability of current study despite the small sample size. Further, the combination of both data sets provided a bigger picture than possible with a single method design (Crswell, 2015; Creswell & Plano Clark, 2011).

Future research should continue to examine digital evidence in the courts. Specifically, there is a need to investigate why judges are falling behind in the understanding of digital evidence. Also, the development, implementation, and evaluation of digital evidence training for prosecutors and defense attorneys is needed to ensure both groups understand digital evidence. Additionally, future research should examine if more trainings and a better understanding of

digital evidence effect attorneys' opinions and attitudes toward digital evidence and then ultimately the use of such evidence.

In summary, digital evidence will continue to expand in the years to come and the understanding of such evidence by courtroom actors is imperative for a fair trial, for both defendants and victims of crimes. The improper use or missed opportunity to use digital evidence could result in an individual being falsely convicted or acquitted. The digital forensic field can learn and be cautioned by the examples set forth by DNA evidence. On one hand, there is a vast amount of research which seeks to examine DNA evidence in the courts. Digital forensics could benefit from increased research in this area, specifically regarding jurors understanding of digital evidence. On the other hand, recent years have brought to light many exonerations as the result of DNA evidence (Innocence Project, 2021). Digital Forensics, as a field, should strive to avoid a similar future.

REFERENCES

American Bar Association (2015, February 13). Criminal Justice Standards for the Defense Function. Retrieved on April 2, 2019, from https://www.americanbar.org

American Bar Association (2015, April 16). Criminal Justice Standards for the Prosecution Function. Retrieved on April 2, 2019, from https://www.americanbar.org

American Bar Association (2017, June 14). Forensic examination of digital devices in civil litigation: The legal, ethical and technical traps. Retrieved on April 20, 2019, from https://www.americanbar.org

American Bar Association (2021) National Lawyer Population Survey 2021, Retrieved on December 1, 2021, from https://www.americanbar.org

Armerding, T. (2018, December 20). The 18 biggest data breaches of the 21 century. Retrieved on April 21, 2019, from https://www.csoonline.com

Augenstein, S. (2016, December 28). Could Amazon Echo Be a Witness in Arkansas Murder Case? Retrieved October 30, 2017, from https://www.forensicmag.com/

Atkinson, J. S. (2014) "Proof Is Not Binary: The Pace and Complexity of Computer Systems and Challenges Digital Evidence Poses to the Legal System," Birkbeck Law Review 2 (2), 253.

Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013). A critical review of 7 years of Mobile Device Forensics. *Digital Investigation*, *10*(4), 323-349.

Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, *2*(2), 147-167.

Benson, R. J. (2004). The increasing significance of computer forensics in litigation. Intellectual Property & Technology Law Journal, 16(11), 1

Brenan, M. (2018, November 9). Cybercrimes remain most worrisome to Americans. *Gallup*. Retrieved on April 16, 2019, from https://news.gallup.com

Bull, R., & Holliday, R. (2011). Understanding juror perceptions of forensic evidence: Investigating the impact of case context on perceptions of forensic evidence strength. Journal of forensic sciences, 56(2), 409-414.

Bureau of Justice Statistics (n.d.). Cybercrime. Retrieved on April 14, 2016, from https://www.bjs.gov/index.cfm?ty=tp&tid=41

Carcary, M. (2009). The Research Audit Trial--Enhancing Trustworthiness in Qualitative Inquiry. *Electronic Journal of Business Research Methods*, *7*(1).

Carrier, B., Spafford, E. H., et al. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence, 2*(2), 1-20.

Carpenter v. United Stated 585 US (2018)

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.

Cashman, K., & Henning, T. (2012). Lawyers and DNA: Issues in understanding and challenging the evidence. Current issues in criminal justice, 24(1), 69-83.

Clifford, R. D. (2001) *Cybercrime: The investigation, prosecution and defense of a computer related crime.*

Cohen, J. (2013). *Statistical power analysis for the behavioral sciences*. Academic press.

Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council. (2009). *Strengthening Forensic Science in the United States: A Path Forward.* Washington, DC: National Academies Press.

Computer History Museum (2019). Computer History Timeline. Retrieved on April 4, 2014, from https://www.computerhistory.org/timeline/

Creswell, J. W. (2015). *A concise introduction to mixed-methods research*. Sage Publications. Thousand Oaks, CA.

Creswell, J. W., Plano Clark, V. L., Gutmann, M. L., & Hanson, W. E. (2003). Advanced mixed methods research designs. In A. Tashakkori & C. Teddlie (Eds.), *Handbook of mixed methods in social and behavioral research* (pp. 209–240). Thousand Oaks, CA: Sage.

Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and conducting mixed-methods research* (2nd) Thousands Oak, CA: Sage publications.

DeCuir-Gunby, J. T., & Schutz, P. A. (2017). Developing a mixed-methods proposal: A practical guide for beginning researchers (Vol. 5). SAGE Publications.

De Keijser, J., & Elffers, H. (2012). Understanding of forensic expert reports by judges, defense lawyers, and forensic professionals. Psychology, Crime & Law, 18(2), 191-207.

Dennis & Cormier (2005, January 6) Evolution of DNA evidence from crime-solving: A judicial and legislative history. Retrieved on July 7, 2019, from https://www.forensicmag.com

Deterding, N. M., & Waters, M. C. (2018). Flexible coding of In-depth interviews: A twenty first-century approach. *Sociological methods & research*, 0049124118799377.

Easttom, C. (2017). *System forensics, investigation, and response*. Jones & Bartlett Learning.

Eldridge, H. (2019). Juror comprehension of forensic expert testimony: A literature review and gap analysis. *Forensic Science International: Synergy*.

Fetters, M. D., & Freshwater, D. (2015). The 1+ 1= 3 Integration Challenge. Journal of Mixed Methods Research, 9(2), 115-117

Fisher, R. A. (1922). On the interpretation of chi square from contingency tables, and the calculation of P. *Journal of the Royal Statistical Society*, *85*, 87-94.

Erstad, W. (2018, October 29). Civil Law vs. Criminal Law: Breaking down the difference. Justice Studies Blog. Retrieved on July 15, 2019, from https://www.rasmussen.edu/

Fetters, M. D., & Freshwater, D. (2015). Publishing a methodological mixed-methods research article. Journal of Mixed-methods Research, 9(2), 203-213.

Forensic Out Reach (2016, March 8). When evidence backfires: The OJ Simpson Murder Trial. Forensic Outreach. Retrieved July 13, 2019, from https://forensicoutreach.com

Forensic Science [Def. 1] (n.d.) *Merriam-Webster Online.* In Merriam Webster. Retrieved April 4, 2019, from https://www.merriam-webster.com

Garrie, D. B., & Morrisy, D. (2014). Digital forensic evidence in the courtroom: understanding content and quality. Nw. J. Tech. & Intell. Prop., 12.

Gideon v. Wainwright 372 U.S. 335 (1963)

Given, L. M. (2008). *The SAGE encyclopedia of qualitative research methods* (Vols. 1-0). Thousand Oaks, CA: SAGE Publications, Inc. doi: 10.4135/9781412963909

Goodison, S.E., Davis, R. C. & Jackson, B.A (2015). Digital evidence and the US criminal justice system. *Identifying Technology and other Needs to More Effectively Acquire and Utilize Digital Evidence.* Rand Corporation. Retrieved on September 10, 2018, from https://www.rand.org

Guetterman, T. C., Fetters, M. D., & Creswell, J. W. (2015). Integrating quantitative and qualitative results in health science mixed-methods research through joint displays. *The Annals of Family Medicine, 13*(6), 554-561.

Hall, H., Brosnan, C., Cant, R., Collins, M., & Leach, M. (2018). Nurses' attitudes and behavior towards patients' use of complementary therapies: A mixed-methods study. Journal of advanced nursing, 74(7), 1649-1658

Hans, V. P., Kaye, D. H., Dann, B. M., Farley, E. J., & Albertson, S. (2011). Science in the jury box: Jurors' comprehension of mitochondrial DNA evidence. *Law and human behavior*, *35*(1), 60-71.

Hayes, D. R. (2014). *A practical guide to computer forensics investigations*. Pearson Education.

Headworth, S., & Ossei-Owusu, S. (2017). The accused poor. *Social Justice*, *44*(2-3 (148), 55 82.

Hedges, L. (1981). Distribution Theory for Glass's Estimator of Effect Size and Related estimators. *Journal of Educational Statistic*s. *6*(2), 107-128.

Holmgren, J. A. (2003). Beyond the walls of the laboratory: Judge and jury interpretations, perceptions, and understanding of DNA evidence.

Holmgren, J. (2005). DNA evidence and jury comprehension. Canadian Society of Forensic Science Journal, 38(3), 123-141.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and digital forensics: An introduction*. New York, NY: Routledge.

Howes, L. M. (2015). The communication of forensic science in the criminal justice system: A review of theory and proposed directions for research. *Science & Justice*, *55*(2), 145-154.

Hughes, N. R., Mozayani, A., & Drake, J.M. (2019, February). Developing an introductory analytical science training program for lawyers and judges. Presented at the *American Academy of Forensic Sciences Annual Meeting*. Washington, DC.

IC3. (2013). *Internet Crime Report 2013*. National White Collar Crime Center (NW3C). Retrieved on April 15, 2019, from https://pdf.ic3.gov/2013_IC3Report.pdf

IC3. (2017). *Internet Crime Report 2013*. National White Collar Crime Center (NW3C). Retrieved on April 15, 2019, from https://pdf.ic3.gov/2017_IC3Report.pdf

Jackson, G., Kaye, D. H., Neumann, C., Ranadive, A., & Reyna, V. F. (2015). *Communicating the Results of Forensic Science Examinations.* Final Technical Report for NIST Award 70NANB12H014 retrieved from https://ssrn.com/abstract=2690899

Kempner, E. A., Stringfield, S., & Teddlie, C. (2003). Mixed-methods sampling strategies in social science research. In A. Tashakkori & C. Teddlie (Eds.), *Handbook of mixed methods in social and behavioral research* (pp. 273-296). Thousand Oaks, CA: Sage.

Kessler, G. C. (2010). Judges' awareness, understanding, and application of digital evidence. Nova Southeastern University.

Li, L., Worch, E., Zhou, Y., & Aguiton, R. (2015). How and why digital generation teachers use technology in the classroom: An explanatory sequential mixed-methods study. International Journal for the Scholarship of Teaching and Learning, 9(2), 9.

Lieberman, J. D., Carrell, C. A., Miethe, T. D., & Krauss, D. A. (2008). Gold versus platinum: Do jurors recognize the superiority and limitations of DNA evidence compared to other types of forensic evidence? Psychology, Public Policy, and Law, 14(1), 27

Lincoln, R., Southerland, A., & Jarrett-Luck, M. (2014). The Persuasive Powers of DNA: An Experimental Study in Perceptions of Expert Evidence. GSTF Journal of Law and Social Sciences (JLSS), 2(3), 1-8.

Losavio, M., Adams, J., & Rogers, M. (2006). Gap analysis: Judicial experience and perception of electronic evidence. *Journal of Digital Forensic Practice*, *1*(1), 13-17.

Losavio, M., Keeling, D. W., Elmaghraby, A., Higgins, G., & Shutt, J. (2008, May). Implications of Attorney Experiences with Digital Forensics and Electronic Evidence in the United States. In *2008 Third International Workshop on Systematic Approaches to Digital Forensic Engineering* (pp. 79-90). IEEE.

Losavio, M. M., & Losavio, A. (2017, May). Downstream Competence Challenges and Legal/Ethical Risks in Digital Forensic Presented at the *Annual ADFSL Conference on Digital Forensics, Security and Law.* Dayton, FL.

Maeder, E. M., Ewanation, L. A., & Monnink, J. (2017). Jurors' perceptions of evidence: The relative influence of DNA and eyewitness testimony when presented by opposing parties. Journal of Police and Criminal Psychology, 32(1), 33-42.

Maruna, S. (2010). Mixed-method research in criminology: Why not go both ways? In Handbook of quantitative criminology (pp. 123-140). Springer, New York, NY.

McKemmish, R. (1999). *What is forensic computing?* Canberra: Australian Institute of Criminology.

McNaught, C., & Lam, P. (2010). Using Wordle as a supplementary research tool. *Qualitative Report*, *15*(3), 630-643.

Moohr, G. S. (2004). Prosecutorial power in an adversarial system: Lessons from current white collar cases and the inquisitorial model. *Buffalo Criminal Law Review*, *8*(1), 165-220.

Mothi, D., Janicke, H., & Wagner, I. (2020). A novel principle to validate digital forensic models. *Forensic Science International: Digital Investigation*, 200904.

National Computer Forensic Institute (2019). About NCFI. Retrieved April 14, 2019, from https://www.ncfi.usss.gov

National Institute of Justice (2007). Digital Evidence in the courtroom: A guide for law enforcement and prosecutors. *Special Report*.

National Institute of Justice (2019, April 23). Forensic Sciences: Types of Evidence. Retrieved rom https://www.nij.gov on June 29, 201

National White-Collar Crime (2019). Online Training Resources. Retrieved May 31, 2019, from https://www.nw3c.org/

NIST (2019, February 26). OSAC Organization Structure. Retrieved April 14, 2019, from https://www.nist.gov

Novak, M. (2020). Digital Evidence in Criminal Cases Before the US Courts of Appeal: Trends and Issues for Consideration. *Journal of Digital Forensics, Security and Law*, *14*(4), 3.

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

Palmer, G. L. (2002). Forensic analysis in the digital world. *International Journal of Digital Evidence*, *1*(1), 1-6.

Patton, M. Q. (2014) *Qualitative research and evaluation methods* (4th ed.) Thousand Oaks, CA: Sage [Ch. 1, 6, 9].

Pew Research Center. (2018, February 5). Mobile Fact Sheet. Retrieved on April 21, 2019, from https://www.pewinternet.org

Pollitt, M. (2008). Applying traditional forensic taxonomy to digital forensics." In IFIP International Conference on Digital Forensics, pp. 17-26. Springer, Boston, MA

Radichel, T. (2014). Case study: critical controls that could have prevented target breach. SANS Institute InfoSec Reading Room

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, *1*(3), 1-12.

Remmel, R. J., Glenn, A. L., & Cox, J. (2019). Biological evidence regarding psychopathy does not affect mock jury sentencing. *Journal of Personality Disorders*, *33*(2), 164-184.

Riley v. California 573 US 373 (2014)

Rigby, S., & Rogers, M. K. (2007). "The General Digital Forensics Model" (2007). Annual ADFSL Conference on Digital Forensics, Security and Law. 1

Rogers, M., Scarborough, K., Frakes, K., & San Martin, C. (2007, January). Survey of law enforcement perceptions regarding digital evidence. In IFIP International Conference on Digital Forensics (pp. 41-52). Springer, New York, NY.

Sammons, J. (2012). The basics of digital forensics: the primer for getting started in digital forensics. Elsevier.

Saldaña, J. (2015). The coding manual for qualitative researchers. Sage Publications.

Saleem, S., Baggili, I., & Popov, O. (2014). Quantifying Relevance of Mobile Digital Evidence as They Relate to Case Types: A Survey and a Guide for Best Practice. Journal of Digital Forensics, Security and Law, 9(3), 3.

Schklar, J., & Diamond, S. S. (1999). Juror reactions to DNA evidence: Errors and expectancies. *Law and Human Behavior*, *23*(2), 159-184.

Schweitzer, N. J., & Saks, M. J. (2007). The CSI effect: Popular fiction about forensic science affects the public's expectations about real forensic science. *Jurimetrics*, 357-364.

Siemasko (2016, March 6). O.J. Simpsons Prosecutor Marcia Clark: If the trial were held today, it'd probably be a hung jury. NBC News. Retrieved on July 13, 2019, from www.nbcnews.com

Solan, L. M. (1999). Refocusing the Burden of Proof in Criminal Cases: Some Doubt about Reasonable Doubt. *Tex. L. Rev.*, *78*, 105.

Stake, R. E. (2004). Qualitative case studies. In N. K. Denzin and Y. S. Lincoln *The Sage handbook of qualitative research* (pp. 442-466). Thousand Oaks, CA: Sage

Stambaugh, H. (2000). *State and local law enforcement needs to combat electronic crime*. US Department of Justice, Office of Justice Programs, National Institute of Justice.

Statista (2019). Percentage of households in the United States with a computer from 1984 to 2016. Retrieved on April 21, 2019, from https://www.statista.com

Subedi, N., & Giri, H. R. (2018). Perception of District Judges and Lawyers Towards Medico Legal Reports, Medical Certificates, and Medical Expert Opinion. Journal of the Nepal Medical Association, 56(212).

Strickland v. Washington, 466 U.S. 688 (1984)

Taslitz, A. E. (2004). Digital juries versus digital lawyers. Criminal Justice, 19(1), 4-13

Tashakkori, A., & Creswell, J. W. (2007). The new era of mixed-methods [editorial]. *Journal of Mixed Methods Research, 1*(1), 3-7.

Taylor, M. (2017, April 26). Murdered Woman's Fitbit Log Used to Charge Husband. Retrieved October 30, 2017, from https://www.forensicmag.com

Tufford, L., & Newman, P. (2012). Bracketing in qualitative research. *Qualitative social work, 11*(1), 80-96.

U. S. Constitution, Amendment 6

United States of American v. Anthony Weiner No 17. Cr 307 (DLC)(2017)

Vogt, W. P., Gardner, D. C., & Haeffele, L. M. (2012). *When to use what research design*. Guilford Press: New York, NY.

Warner, R.M. (2007). Applied statistics: From bivariate through multivariate techniques. Thousand Oaks, CA: Sage Publications, Inc.

Weiser, B. (2017, September 25). Anthony Weiner gets 21 months in prison for sexting with teenager. *The New York Times*. Retrieved on April 21, 2018, from https://www.nytimes.com/

Wilcox, A. M., & NicDaeid, N. (2018). Jurors' perceptions of forensic science expert witnesses: Experience, qualifications, testimony style, and credibility. Forensic science international, 291, 100-108.

Zatyko, K., & Bay, J. (2011, December 14). The Digital Forensic Cyber Exchange Principle. Retrieved on July 7, 2019, from https://www.forensicmag.com.

APPENDIX A – SURVEY

Demographics:

Directions: Please answer the following demographic questions about yourself. Remember, your responses are completely anonymous and absolutely no identifying information will be asked. We will not be able to link your identity with your responses.

1. What is your age in years?
    - Under 18 years old
    - 18 – 25
    - 25 – 29
    - 30 – 39
    - 40 – 49
    - 50 – 59
    - 60 or older

    Respondents under 18 years of age will be sent to the "end of survey" page and will not be able to participate in the survey.

2. Have you earned a Juris Doctorate?
    - No
    - Yes
    - Decline to respond

    Respondents who select 'No' or 'Decline to respond' will be taken to the "end of survey" page and will not be able to participate in the survey.

3. Do you currently practice law in the United States?
    - No
    - Yes
    - Decline to respond

    Respondents who select 'No' or 'Decline to respond' will be taken to the "end of survey" page and will not be able to participate in the survey.

4. What is your current professional status?

- Defense Attorney (Private)
- Public Defender
- Prosecutor
- Prefer not to respond

Each of the first four questions will appear individually on the first four pages of the survey.

5. Which race do you identify with the most?

- Asian
- African American or Black
- Hispanic or Latinx
- Native American or Alaska Native
- Native Hawaiian or Pacific Islander
- Multiracial
- White
- Other [Write-in]
- Prefer not to respond.

6. What is your gender?

- Male
- Female
- Non-binary
- Other [Write-in]
- Prefer not to respond

7. What is your current annual income range:

- $0 - $40,000
- $40,001 - $60,000
- $60,001 - $80,000
- $80,001 - $100,000
- $100,001 - $120,000
- $120,001 - $150,000

- More than $150,001
- Prefer not to respond

8. What is the geographical make up of where you practice law?

- Urbanized Areas (50,000 or more people)
- Urban Clusters (at least 2,500 and less than 50,000 people).
- Rural Areas
- Prefer not to respond.

Directions: The next set of questions focus on your education, employment, continuing education, and training. Remember, all questions are completely anonymous.

9. What was your undergraduate college major?

- Business
- Computer Science
- Computer and Information Technology
- Criminal Justice
- Economics
- Education
- Engineering
- English
- History
- Music
- Mathematics
- Nursing
- Philosophy
- Political Science
- Other [Write-in]

10. Were you a pre-law major in undergrad?

- No
- Yes

11. Beyond a Juris Doctorate, do you have a higher education degree?

- No
- Yes

If 'yes' is selected, participants will answer additional questions regarding their education. If 'no' is selected, participants will proceed to the next question.

11a**.** Select all additional completed education:

- Master's degree
- PhD
- MD
- Other [write-in]

If a 'Master's degree' was selected the following question will be asked:

11b. If applicable, please indicate your Master's degree: [Write-in]

12. How long have you been at your *current* job?

- 0 – 1 year
- 2 – 5 years
- 6 – 10 years
- 11 – 15 years
- 16 – 20 years
- More than 20 years

13. Prior to your current employment, have you worked in any of the following areas:
****Select all that apply***

- Private Attorney
- Prosecutors Office
- Public Defender
- Judge
- Law Enforcement Agency

- No prior employment
- Other [Write in]

14. Were you ever an intern or fellow?
    - No
    - Yes

If yes, the participant will be taken to the following question:

14a. Did you ever have an internship or fellowship, related to your law career, during your academic career? Select all that apply.

- Prosecutor's Office
- Private Law Firm
- Law Clerk
- Law Enforcement Agency
- Public Defender
- Other [Write in]

15. Have you received any formal training about digital evidence?
    - No
    - Yes

If yes, the participant will be taken to the following question:

15a. If yes, what type? List and describe all that apply. [Write-in]

16. Where do you learn about digital evidence? [check all that apply]
    - Continuing Education
    - Course Credits
    - Trainings
    - Co-workers
    - Digital Forensics Investigators
    - Media
    - Books
    - Other [Write-in]

17. **In the last year,** estimate your total number of continuing education hours which relate to digital forensics or digital evidence

- 0
- 1 – 5 hours
- 6 – 10 hours
- More than 10 hours

18. **During your law career**, estimate your total number of continuing education hours which relate to digital forensics or digital evidence

- 0
- 1 – 5 hours
- 6 – 10 hours
- More than 10 hours

19. Rate your familiarity with the following on a scale of 1 to 5.
5 indicates a high level of familiarity and 1 indicates no familiarity.

- Digital Forensics
- Desktop Forensics
- Mobile Forensics
- Network Forensics
- Digital artifacts from Internet of Things devices
- Geolocation Data
- Cryptocurrency

<u>Knowledge of Digital Evidence</u>

Directions: Please answer the following questions, based on only your own knowledge and opinions.

1. In your own words, what is digital evidence? [Write-in]

This question will be the only questions on the first page of this section. This is to ensure the participants do not see the additional questions and thus piece together a correct definition of digital evidence. There will be no back button.

Directions: This section consists of a survey of knowledge regarding digital forensics.

True/False Section:

2. Digital Evidence is information that is stored or transmitted in a binary format that may be relied on in court. **True**/False/I don't know
3. Digital evidence can be obtained from an individual's computer. **True**/False/ I don't know
4. Digital evidence from a computer requires the investigator to take an exact copy of the hard drive or digital device, known as a forensic image. **True**/False/I don't know
5. In traditional computer forensics, a hash value is used to authenticate the integrity of the image to ensure evidence has not been altered. **True**/False/I don't know

Multiple Choice Section:

6. Which U.S. Supreme Court case in 2014 determined that a warrantless search and seizure of digital contents of a cell phone during an arrest was unconstitutional?
    - Harris v. Quinn
    - **Riley v. California**
    - Schuette v. Bamn
    - I don't Know
7. In Lorraine v. Stevenel American Insurance Co. (2007), the Chief Magistrate Judge from the District of Maryland wrote an opinion about what?
    - Admissibility of encrypted devices
    - The need for hash values
    - **Admissibility of electronic evidence**
    - I don't know
8. In 2018, which U.S. Supreme Court case decided the government violated the Fourth Amendment of the U.S. Constitution by accessing historical cell site location information records containing physical locations of cellphones without a search warrant?
    - South Dakota v. Wayfair
    - Gill v. Whitford
    - **Carpenter v. United States**
    - I don't know

9. The Supreme Court Case, *United States v. Jones* (2012) determined _____ constitutes a search under the Fourth Amendment.
    - **Installing a GPS tracking device on a vehicle and using it to track the vehicle's movement**
    - Viewing Snapchat memories
    - Accessing geolocation information

- I don't know

Attitudes towards Digital Evidence

This section consists of a survey of opinions regarding digital evidence. You will probably find that you agree with some of the statements and disagree with others, to varying extents. Please indicate your reaction to each statement using the following scale.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	I don't Know
5	4	3	2	1	6

3. Digital evidence can eliminate a suspect.
4. Digital evidence can prove the guilt of a suspect.
5. An investigation can link a suspect to a digital device.
6. Digital evidence can be altered by the analyst.
7. Digital forensic analysis can be used to assist in unsolved cases.
8. Digital evidence is the most important investigative tool.
9. I would base a case primarily on digital evidence.
10. Digital evidence is an asset to the criminal justice system.
11. Digital evidence is not useful in my cases.
12. Digital evidence is the most reliable type of evidence we have today.

Experiences with Digital Evidence

1. What percentage of your cases include digital forensic evidence?
   - 0 – 100%

     **Response is a slide bar feature in Qualtrics*
2. In the past year, have you used digital evidence in court?
   - No
   - Yes

****If yes, the participant will be taken to the following question***

1a. List specific types of digital evidence [Write in response]

3. In the past year, have you used digital evidence during a plea agreement?
    - No
    - Yes

    If yes, the participant will be taken to the following question

    2a. List specific types of digital evidence [Write in response]

4. What **challenges**, if any, have you faced in using digital evidence as part of your case/defense? [Write-in]

5. What percentage of your cases involving digital evidence have been successful?
    - 0 – 100%

        **Response is a slide bar feature in Qualtrics*

6. What **successes**, if any, have you had using digital evidence as part of your case/defense? [Write in]
7. In your opinion, are cases **more** successful when digital evidence is involved?
    - Yes, cases are *more* successful.
    - No, cases are *less* successful.
    - Digital evidence does not impact the success of a case.
    - Other [Write in]
    - Prefer not to respond
8. When digital evidence was involved in your case, did you consult with a digital forensic investigator or individual from law enforcement?
    - No
    - Yes
    - I have not had any cased that involved in digital evidence.
    - Prefer not to respond.
9. When digital evidence was involved in your case, did you consult with a digital forensic expert?
    - No
    - Yes

- I have not had any cased that involved in digital evidence.
- Prefer not to respond.

10. How important are digital forensic experts, investigators, and/or examiners to the success of a case/defense?
    - Extremely important
    - Very Important
    - Moderately Important
    - Slightly Important
    - Not at all Important

11. In your opinion, do you think the use of digital forensic evidence should be expanded?
    - Yes [Text box]
    - No [Text box]
    - Prefer not to respond.
12. Currently, what do you believe is the biggest legal issues in digital forensics? [Write in]
13. In the next 10 years, what do you think will be the biggest legal issues in digital forensics? [Write in]
14. Is there anything else you would like to share regarding you experience with digital evidence? [Write in]

APPENDIX B – INTERVIEW PROTOCOL

Survey Questions:

Sampling Criteria

- What is your age? [Must be 18 to consent]
- Have you earned a Juris Doctorate? [Sampling Criteria – Must have a JD]
- Do you currently practice law, or have you practiced law in the United States? [Sampling Criteria – must have currently or previously practiced law]
- What is your current professional status? [Sampling Criteria – Must be a current or former prosecutor or defense attorney (private or public defender)]

Demographics

- When did you go to law school?
- Which race do you identify with the most?
- What is your gender?

Interview Questions

Knowledge

- Do you think digital evidence is understood by the judge, jury, and fellow attorneys?

Experience

- What is your experience with digital evidence?
- Have you ever used digital evidence in one of your cases which went to trial?
    - If yes, can you tell me an example? What was the outcome?
    - If no, is there a reason you have not had any cases which involved digital evidence?
        - Lack of understanding?
        - Other challenges?
- When digital evidence was involved in your case, did you have to educate the judiciary?
    - What about the jury?

        - How did you do this?
- Have you ever used digital evidence as part of a plea agreement?
    - If yes, can you tell me an example? What was the outcome?
    - If no, is there a reason you have not had any cases which involved digital evidence?
        - Lack of understanding?
        - Other challenges?

Attitudes

- In your opinion, is digital evidence helpful to your cases?
    - Does digital evidence hurt your cases? How so?
    - Does digital evidence help your cases? How so?
- Do you think digital evidence is reliable?
    - How do you think the jury views digital evidence?
- What are some current challenges with digital evidence?
    - Do you think digital evidence can be linked to a suspect (e.g., "putting the suspect at the keyboard")?
- What are future challenges with digital evidence?
- Is there anything else you would like to share regarding digital evidence?

<u>Backup Questions</u>

- How knowledgeable are you with regards to digital evidence?
- Have you received any formal training on digital evidence?
    - If yes, please elaborate.

APPENDIX C– IRB APPROVAL

Date: December 15, 2020
PI: KATHRYN SEIGFRIED-SPELLAR
Re: Initial - IRB-2020-1703
Attitudes & Opinions of Digital Evidence

The Purdue University Human Research Protection Program (HRPP) has determined that the research project identified above qualifies as exempt from IRB review, under federal human subjects research regulations 45 CFR 46.104. The Category for this Exemption is listed below . Protocols exempted by the Purdue HRPP do not require regular renewal. However, the administrative check-in date is December 15, 2023. The IRB must be notified when this study is closed. If a study closure request has not been initiated by this date, the HRPP will request study status update for the record.

Specific notes related to your study are found below.
Decision: Exempt
Category:
Category 2.(i). Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording).
The information obtained is recorded by the investigator in such a manner that the identity of the human subjects cannot readily be ascertained, directly or through identifiers linked to the subjects.
Category 2.(ii). Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording).
Any disclosure of the human subjects' responses outside the research would not reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, educational advancement, or reputation.

Findings: NA
Research Notes: NA

Any modifications to the approved study must be submitted for review through Cayuse IRB. All approval letters and study documents are located within the Study Details in Cayuse IRB.

What are your responsibilities now, as you move forward with your research?

Document Retention: The PI is responsible for keeping all regulated documents, including IRB correspondence such as this letter, approved study documents, and signed consent forms for at least three (3) years following protocol closure for audit purposes. Documents regulated by HIPAA, such as Release Authorizations, must be maintained for six (6) years.

Site Permission: If your research is conducted at locations outside of Purdue University (such as schools, hospitals, or businesses), you must obtain written permission from all sites to recruit, consent, study, or observe participants. Generally, such permission comes in the form of a letter from the school superintendent, director, or manager. You must maintain a copy of this permission with study records.

Training: All researchers collecting or analyzing data from this study must renew training in human subjects research via the CITI Program (www.citiprogram.org) every 4 years. New personnel must complete training and be added to the protocol before beginning research with human participants or their data.

Modifications: Change to any aspect of this protocol or research personnel must be approved by the IRB before implementation, except when necessary to eliminate apparent immediate hazards to subjects or others. In such situations, the IRB should still be notified immediately.

Unanticipated Problems/Adverse Events: Unanticipated problems involving risks to subjects or others, serious adverse events, and

noncompliance with the approved protocol must be reported to the IRB immediately through an incident report. When in doubt, consult with the HRPP/IRB.

Monitoring: The HRPP reminds researchers that this study is subject to monitoring at any time by Purdue's HRPP staff, Institutional Review Board, Research Quality Assurance unit, or authorized external entities. Timely cooperation with monitoring procedures is an expectation of IRB approval.

Change of Institutions: If the PI leaves Purdue, the study must be closed, or the PI must be replaced on the study or transferred to a new IRB. Studies without a Purdue University PI will be closed.

Other Approvals: This Purdue IRB approval covers only regulations related to human subject's research protections (e.g., 45 CFR 46). This determination does not constitute approval from any other Purdue campus departments, research sites, or outside agencies. The Principal Investigator and all researchers are required to affirm that the research meets all applicable local/state/ federal laws and university policies that may apply.

If you have questions about this determination or your responsibilities when conducting human subjects research on this project or any other, please do not hesitate to contact Purdue's HRPP at irb@purdue.edu or 765-494-5942. We are here to help!

Sincerely,

Purdue University Human Research Protection Program/ Institutional Review Board
Login to Cayuse IRB

APPENDIX D – IRB MODIFICATION APPROVAL

The Purdue University Institutional Review Board has approved the modification for your study "*Attitudes & Opinions of Digital Evidence*. " The Category for this Exemption is listed below. This study maintains a status of exempt and an administrative check-in date of December 15, 2023. The IRB must be notified when this study is closed. If a study closure request has not been initiated by this date, the HRPP will request study status update for the record.

Specific details about your modification approval appear below.
Decision: Exempt

What are your responsibilities now, as you move forward with your research?

Document Retention: The PI is responsible for keeping all regulated documents, including IRB correspondence such as this letter, approved study documents, and signed consent forms for at least three (3) years following protocol closure for audit purposes. Documents regulated by HIPAA, such as Release Authorizations, must be maintained for six (6) years.

Site Permission: If your research is conducted at locations outside of Purdue University (such as schools, hospitals, or businesses), you must obtain written permission from all sites to recruit, consent, study, or observe participants. Generally, such permission comes in the form of a letter from the school superintendent, director, or manager. You must maintain a copy of this permission with study records.

Training: All researchers collecting or analyzing data from this study must renew training in human subject's research via the CITI Program (www.citiprogram.org) every 4 years. New personnel must complete training and be added to the protocol before beginning research with human participants or their data.

Modifications: Change to any aspect of this protocol or research personnel must be approved by the IRB before implementation, except when necessary to eliminate apparent immediate hazards

to subjects or others. In such situations, the IRB should still be notified immediately.

Unanticipated Problems/Adverse Events: Unanticipated problems involving risks to subjects or others, serious adverse events, and
noncompliance with the approved protocol must be reported to the IRB immediately through an incident report. When in doubt, consult with the HRPP/IRB.

Monitoring: The HRPP reminds researchers that this study is subject to monitoring at any time by Purdue's HRPP staff, Institutional Review Board, Post Approval Monitoring team, or authorized external entities. Timely cooperation with monitoring procedures is an expectation of IRB approval.

Change of Institutions: If the PI leaves Purdue, the study must be closed, or the PI must be replaced on the study or transferred to a new IRB. Studies without a Purdue University PI will be closed.

Other Approvals: This Purdue IRB approval covers only regulations related to human subject's research protections (e.g., 45 CFR 46). This determination does not constitute approval from any other Purdue campus departments, research sites, or outside agencies. The Principal Investigator and all researchers are required to affirm that the research meets all applicable local/state/ federal laws and university policies that may apply.

If you have questions about this determination or your responsibilities when conducting human subjects research on this project or any other, please do not hesitate to contact Purdue's HRPP at irb@purdue.edu or 765-494-5942. We are here to help!
Sincerely,

Purdue University Human Research Protection Program/ Institutional Review Board

APPENDIX E – POSSIONALITY STATEMENT

For the interviews, I am the primary instrument for data collection and analysis and therefore, my biases should be made explicit. I am a thirty-year-old graduate student in the United States. I am a white, female, and I grew up in a middle-class family in a suburban town in Florida.

I became interested in digital forensics during my undergraduate studies at the University of Alabama. While I was a student, I created the Cyber Crime Club. As a part of this club, we took a tour to the National Computer Forensic Institute (NCFI) in Hoover, AL. During this field trip, I became interested in how digital evidence was understood in the courtroom which eventually lead to me to this study.

During the interviews, I clarified responses with participants to ensure I was not making any assumption based on my previous experiences. Further, throughout the data collection and analysis, I used memoing to acknowledge and separate my thoughts from those of the participants. I also checked interpretations against the data and where possible discussed it with the participants as a form of member checking.