Spring 4-2020

Digital Forensic Readiness: An Examination of Law Enforcement Agencies in the State of Maryland

James B. McNicholas III
Dakota State University

DIGITAL FORENSIC READINESS: AN EXAMINATION OF LAW ENFORCEMENT AGENCIES IN THE STATE OF MARYLAND

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Cyber Operations

April, 2020

By
James B. McNicholas III

Dissertation Committee:
Dr. Wayne E. Pauli
Dr. Ashley Podhradsky
Gerald Maye
Trevor Jones

DAKOTA STATE
UNIVERSITY

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: James McNicholas

Dissertation Title: Digital Forensic Readiness: An Examination of Law Enforcement Agencies in the State of Maryland

Dissertation Chair/Co-Chair: Wayne Pauli Date: April 17, 2020
Name: Wayne Pauli

Dissertation Chair/Co-Chair: ____________ Date: ______
Name:

Committee member: Ashley Podhradsky Date: April 17, 2020
Name: Ashley Podhradsky

Committee member: Trevor Jones Date: April 17, 2020
Name: Trevor Jones

Committee member: ____________ Date: April 20, 2020
Name: Gerald L Maye

Committee member: ____________ Date: ______
Name:

Original to Office of Graduate Studies and Research
Acid-free copies with written reports to library

ACKNOWLEDGMENT

This work is dedicated to those individuals that provided the support, knowledge, understanding, patience, and love that provided me the strength to see this process through.

To my family, you have been my foundation and *the* driving force. Despite the missed events, missed meals, and lost time, you always stood by me. This work and all that comes after is truly for you.

To my parents, who never stopped believing in me, you will never know how grateful I am for all you have done and the sacrifices you have made.

To Dr. Wayne Pauli -- the voice of wisdom and reason. I am honored and grateful beyond words for all you have done.

To Dr. Ashley Podhradsky, who generously offered critical perspective and insight that assisted in stitching this work together.

To Gerald Maye, whose support and encouragement throughout the years has inspired me to try to make a lasting impact on the field.

To Trevor Jones, who recognized the potential in this endeavor and provided the encouragement and insight to ensure that it all stayed on track.

To the faculty and support staff at Dakota State University, your professionalism, caring, and enthusiasm for student success *is* what makes all this possible.

To my friends and fellow classmates, you were always there for me despite being a total curmudgeon. Thank you!

Finally, a special thank you to the law enforcement agencies that participated in this research. Without your participation, this research would not have been possible. As a result of your participation, a donation of $310.00 was made to the National Center for Missing and Exploited Children (www.missingkids.org).

ABSTRACT

Digital forensic readiness within the law enforcement community, especially at the local level, has gone mostly unexplored. As a result, a current lack of data exists that examines the digital forensic readiness of individual agencies, the possibility of proximity relationships, and correlations between readiness and backlogs. This quantitative, cross-sectional research study sought to explore these issues by focusing on the state of Maryland. The study resulted in the creation of a digital forensic readiness scoring model that was then used to assign digital forensic readiness scores to thirty (30) of the one-hundred-forty-one (141) law enforcement agencies throughout Maryland. It was found that an agency's proximity to a major resource center (*hub*) did not positively or negatively influence readiness. It was also found that agencies with higher digital forensic readiness scores may be more likely to exhibit backlogs as a result of external agency dependencies. It should be noted, however, that digital forensic readiness scores should not be viewed as a reliable predictive indicator for the existence of backlogs. These findings establish a baseline for the state of Maryland that can be used to monitor, sustain, or improve levels of digital forensic readiness within the state or in a broader national context; it has the potential of enhancing public safety and the field at large.

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

James B. McNicholas III

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

In the world of digital forensics, some of the keys to conducting a successful investigation include the ability to adequately respond to an incident and having a combination of the right people, processes, tools, and resources to support the process through to litigation (van Baar, van Beek, & van Eijk, 2014). In relation to law enforcement efforts, the stakes are even higher as the products produced during the digital forensics process must be able to withstand significant scrutiny (Garrie & Morrissy, 2014). At present, research is sparse and speculative regarding the ability of law enforcement agencies within individual states to process digital evidence (Flory, 2016; Gogolin & Jones, 2010). In addition, a gap currently exists within the body of knowledge regarding proximity relationships of law enforcement agencies to major metropolitan areas. It is not fully understood if these relationships increase, decrease, or have no effect on digital forensic readiness postures or evidentiary backlogs.

To this effect, this chapter contains the foundational knowledge to establish the relationships between the research problem and the research objectives when examining law enforcement agencies within the state of Maryland using a quantitative cross-sectional approach. First, the motivation for the research will be presented, followed by the background of the problem, which includes a high-level examination of some of the key areas relating to digital forensics. The statement of the problem is then provided, followed by the objectives of the research. Finally, this current chapter is summarized, and the structure of the remainder of this dissertation is presented.

Motivation

In today's modern society, it is rare not to see someone carrying or actively utilizing some form of digital technology. These devices create digital trails that can paint pictures of the people that have used them and the events in which they have been used (Sammons, 2012). From a law enforcement perspective, this information can be invaluable during an investigation; however, there is a specific process that must be followed in order for this evidence to be legally obtained and considered admissible as evidence in a court of law (US-CERT, 2008). To complicate matters, the rules and laws governing this type of evidence can vary by jurisdiction and are continually evolving as courts begin to better understand digital technology (Borisevich et al., 2012; Cassim, 2017; Losavio et al., 2019; Pollitt, Caloyannides, Novotny, & Shenoi, 2004). Understanding the law enforcement community and its obligations in relation to digital evidence is one way to understand why active and ongoing research in this field is essential.

Cybercrime is on the rise globally with criminal entities leveraging the anonymity of technology to their full advantage (Federal Bureau of Investigation, 2019; United States Department of Justice, 2018). Compounding the issue is a lack of communication and resource sharing among law enforcement agencies (Hollywood & Winkelman, 2015). One problem that can arise as a result of these factors are backlogs, which result when the evidence exceeds the availability of resources needed to process the evidence. It must be noted that the definition of *backlog* is subjective (Sacco & James, 2015). As backlogs of evidence grow worldwide, so do the opportunities for criminal exploitation of an already fragile system (Scanlon, 2016).

While certain populations are more frequently targeted by cybercriminals, it must be understood that every individual has the potential to become the victim of cyber-crime (Federal Bureau of Investigation, 2017). This presents a problem as "[c]ybercrime research suggests that analogous to traditional crime, victims are more likely to be offenders" (Weulen Kranenbarg, Holt, & van Gelder, 2017). While outside the scope of this research, this suggests that backlogs, which have been noted as a concern within the law enforcement community, may increase the chance of future victimization as a byproduct of delays in justice (Scanlon, 2016).

One such example of the prevalence and potential impact of backlogs during an investigation can be found when examining a case in Maryland, as was reported by Watts (2017). This particular case involved digital evidence that sat in an evidentiary backlog for several months (Watts, 2017). The suspect, later convicted of numerous sex crimes involving minors, was not held in custody, for a period of time during the investigation, as a direct result of a backlog of digital evidentiary items at the state's crime lab (Watts, 2017). This time presented as an opportunity for continued victimization.

This case, one of many, demonstrates the immediate need to examine backlogs and the factors that may influence these backlogs, such as the proximity relationships to resources. Examining individual agency postures within an area where backlogs are known to have occurred can generate valuable datasets that may assist localities under examination. Furthermore, these datasets could serve as baselines for future research directed towards the creation of universal process models designed to decrease or eliminate backlogs and improve digital forensic readiness postures throughout the country.

Maryland

Maryland, a small state on the east coast of the United States, is estimated to be the home to more than 6 million people (United States Census Bureau, 2018a). With a total area of 12,193^2 miles, the general population density equates to roughly 496 people per square mile (Maryland Department of Natural Resources, 2019). Like other states, this population is dispersed with large numbers of people being centered in and around major metropolitan areas (Cohen, 2015; Cubit, 2019).

What makes this state particularly interesting from a research perspective is the distance relationships between two major cities; Washington, D.C., which sits to the east of the center of the state and Baltimore, MD, which sits slightly north of the center of the state (see Figure 1).

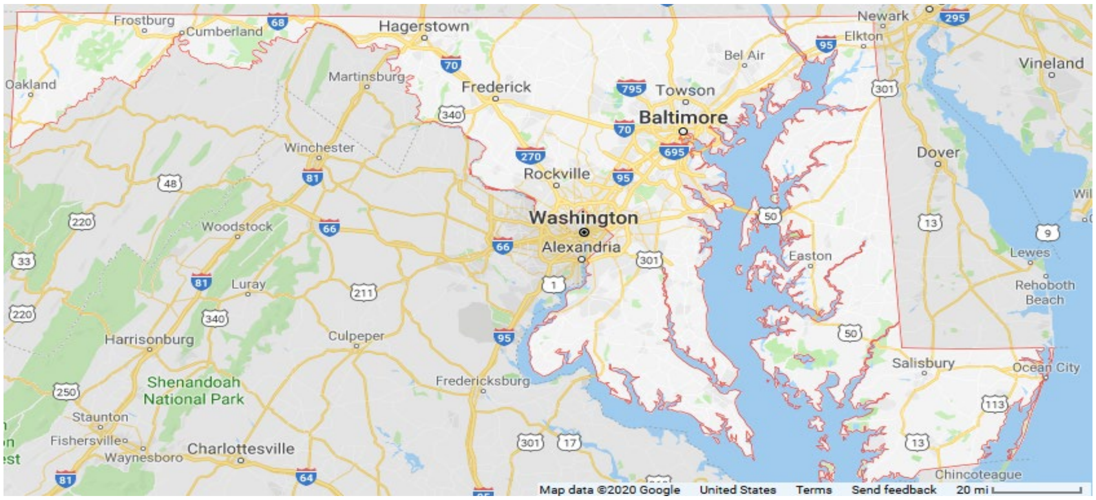


Figure 1. Map of Maryland (Google, n.d.)

The geographic locations of these two cities create somewhat of a population bubble. From a law enforcement perspective, this creates some interesting challenges, some of which may be common to other states throughout the United States. As such, this presented as an excellent opportunity to examine proximity relationships and its potential impact on digital forensic readiness.

To further keep things in context, Washington D.C. serves as the nation's capital. This federal enclave, on its own, is home to more than 700,000 people (United States Census Bureau, 2018b). The city is also the home to dozens of federal agencies, the Whitehouse, and other prominent structures and attractions. Security is of the utmost importance as throughout history, both people and places within the city have been the targets of various forms of terroristic style attacks (Ellis, 2014; Phillips, 2006; Stein, 2016). Digital evidence is becoming more common in these types of cases, as was indicated in the indictment of Christopher Paul Hasson ("United States v. Christopher Paul Hasson," 2019). In this case, digital evidence seized subsequent to an unrelated warrant revealed evidence that suggested that the defendant was possibly planning a terror type attack on key members of congress in the region ("United States v. Christopher Paul Hasson," 2019). While cases like these are not necessarily the norm, they do demonstrate the need for digital forensic readiness throughout the region. This research focuses on those agencies within the state that could potentially be tasked with investigating such cases.

During this research, it was found that one-hundred-forty-one (141) state-specific, non-federal agencies met the criteria to be considered an active law enforcement agency for the purpose of this study. While more agencies were identified during an examination of the state provided list, it was determined that some of the agencies listed were either defunct or were healthcare facilities that may have private security or special police as opposed to regular sworn officers (Department of Public Saftey & Correctional Services, n.d.). It should be noted that while special police do have arrest powers, their powers typically only extend to the property to which they are assigned (Maryland State Police, n.d.). For some agencies, such as those assigned to schools, the distinction was harder to establish based on the limited availability of publications and other publicly available information. As such, many of the school agencies identified as part of the vetting process were still considered during this study. These populations are discussed in greater detail in Chapter 3.

Of the policies listed for these agencies, none appeared to provide policies specifically relating to digital forensics (Department of Public Saftey & Correctional Services, n.d.). While this did not necessarily suggest that polices do not exist, it was an area of concern. This is an important part of this research as digital forensic readiness is partially supported by defined policy and procedure (Flory, 2016). As such, a question was presented in the survey, which was distributed to the agencies to determine if these types of policies do, in fact, exist. These findings were then used as a metric at both the state and county levels to assist in the establishment and assignment of digital forensic readiness scores.

Background of the Problem

Digital forensics, as a defined science, is a relatively new and evolving discipline with challenges constantly emerging that push the bounds of current digital forensics capabilities (Pollitt, 2010; Zawoad & Hasan, 2015). With noted upticks in the number of reported cybercrimes since 2013, the use of digital evidence in support of both criminal and civil litigation is expected to increase (Federal Bureau of Investigation, 2017, 2019; United States Department of Justice, 2018). Since cybercrime is not localized to a specific state or region, there is a present need for law enforcement agencies at the federal, state, and local levels to have some semblance of digital forensic readiness.

The concept of digital forensic readiness, like the field itself, is relatively new and evolving (Elyas, Ahmad, Maynard, & Lonie, 2015). Some definitions for digital forensic readiness consider all phases of the digital forensics process from the initial inception of a program through to the decommissioning of a program (Elyas et al., 2015). The models that have resulted tend to look at the process holistically and do not always fully consider variables such as resource, time, or legal constraints. Several authors have suggested that this may be due to a lack of data that would allow for the proper consideration of these variables (Flory, 2016; Gogolin & Jones, 2010; Harichandran, Breitinger, Baggili, & Marrington, 2016) Thus, the resulting processes are rather prescriptive in nature. Currently, there is no one universally accepted digital forensics model or methodology; however, certain *phases* appear in many of the published models (Decusatis, Carranza, Ngaide, Zafar, & Landaez, 2015). The next two sub-sections discuss these phases, along with an overview of the tools designed to support them.

Digital Forensic Process Models

The digital forensics process can be supported through the implementation of various digital forensic process models. These models, grounded in theory and law, guide the process by taking specific tasks and assigning them to phases (Carroll, Brannon, & Song, 2008). While some of the earlier models prescribed a linear approach, more recent models have emerged that seek to address the dynamic nature of the field as well as the co-mingling of disciplines (Losavio et al., 2019; Mushtaque, Ahsan, & Umer, 2015). Some within the field have even sought to create universal models that also consider the need for adaptability (Kohn, Eloff, & Eloff, 2013). These could be regarded as lofty goals as progress is generally impeded by a lack of standardization within the field, especially in regards to the cross-jurisdictional admissibility of evidence (Antwi-Boasiako & Venter, 2017). These issues combined make the establishment of universal metrics or the creation of universal process models difficult when differences can exist from county to county even within the same state.

Research such as this that considers these types of variations provide the means to formulate baselines. In this research, a question was posed to the respondents to determine if a standard operating procedure exists that considers the "identification, presentation, and collection of digital evidence" (Flory, 2016). While not necessarily seeking to identify the specific models employed, the question provides insight into localized readiness. This information can then, in turn, be used to identify trends that could lead to the adoption of a unified approach at the state or county levels. These concepts are examined in greater detail in Chapter 2.

Digital Forensics Tools

Supporting the models and phases noted above are various types of hardware and software-based tools. As with process models, a lack of standardization with the development and application of supporting tools has contributed to an environment that can potentially open the door to various legal challenges (Losavio et al., 2019; Pollitt et al., 2004). Processes such as tool validation, lab accreditation, and specific training can help alleviate some of these concerns; however, agencies must still be adaptable to legal, regulatory, and technological changes (Pollitt et al., 2004). In Chapter 2, an examination of these types of tools, along with legal and resource concerns, will be presented.

Statement of the problem

Digital forensic readiness within the law enforcement community is considered poorly understood and overly subjective, which has resulted in an environment of unpredictability and unreliability (Elyas et al., 2015; Flory, 2016; Gogolin & Jones, 2010). Despite similar findings across studies, there has been little progress in expanding the body of knowledge on the subject, especially at the individual state level (Flory, 2016; Gogolin & Jones, 2010; Harichandran et al., 2016). Nationally, digital forensic readiness assessments are not being conducted at the state or local levels on a consistent basis to determine individual baselines or to identify relationships among variables that may influence these postures (Elyas et al., 2015; Flory, 2016; Gogolin & Jones, 2010; Goodison, Davis, & Jackson, 2015; National Institute of Justice, 2006; Rogers & Seigfried, 2004; Scanlon, 2016).

At the state level, this type of information can be useful in identifying potential resource gaps as well as areas where backlogs may be occurring (Flory, 2016). By examining digital forensic readiness of law enforcement agencies within the state of Maryland data can be derived that can be used by state officials, academia, and the law enforcement community at large to not only understand the factors that contribute to backlogs but also how to account for the proximity effect of large metropolitan areas in regards to overall digital forensic readiness postures of individual agencies.

Objectives of the Project

The objective of this research was to contribute to the current body of knowledge by answering the following research questions:

RQ1. What is the current digital forensic readiness posture of law enforcement agencies in the state of Maryland?

RQ2. Does an agency's proximity to or availably of external resources influence its internal digital forensics posture?

RQ3. What impact, if any, does an agency's internal digital forensic readiness posture have over any internal backlogs of digital forensics evidence?

The study also sought to support the following hypotheses:

HP1. Law enforcement agencies within the state of Maryland that are within a twenty-mile radius of the two primary central *hubs*, Baltimore, MD, and Washington D.C., will exhibit a more mature digital forensic readiness posture.

HP2. It is hypothesized that all agencies, regardless of their distance between the *hubs,* will exhibit similar digital evidence backlogs when viewed in relation to the populations of the county or municipality in which the agency is located.

Currently, there is limited research on these topics, which is a significant limiting factor. The only known datasets that exist for comparative purposes are few, with most of these being outdated (Flory, 2016; Gogolin & Jones, 2010). While a qualitative study would prove useful in furthering the body of knowledge, it was determined that qualitative data could be viewed as subjective rather than objective. As such, one of the research goals was to avoid subjectivity by using a quantitative methodology and a cross-sectional approach. This type of methodology and approach better serves the community at large by providing metrics and results that can be leveraged for future comparative research.

Assumptions

This study is predicated on several assumptions:

A1. It is assumed that the data provided by each respondent is true and accurate *and* represents the agency's current state, not a future or past state. For example, it was determined that it could be possible that the respondents could provide answers that were forward-thinking, which can introduce bias. This potential bias is discussed in further detail in Chapter 3.

A2. It was assumed that the agencies identified and included in the population group were not sub-agencies or affiliates. Sub-agencies would be defined as agencies that fall under a higher authority. For example, a Maryland State Police barracks would be a sub-agency or affiliate of the Maryland State Police. Data provided by agencies that self-identified as sub-agencies or affiliates were excluded from the analysis presented in Chapter 4.

Significance of the Approach

This research is significant to the field as there has been a noted lack of this type of localized data collected within the United States (Flory, 2016; Gogolin & Jones, 2010; Harichandran et al., 2016). This type of data and analysis is necessary for identifying factors that may influence digital forensic readiness within the law enforcement community at large. These factors can be used to derive metrics and establish baselines with the goal of decreasing digital evidentiary backlogs and increasing the chances of digital evidence being successfully used at trial. Furthermore, the data collected along with the establishment of digital forensic readiness scores set the stage for comparative purposes that may assist in the standardization of the field.

Dissertation Organization

The structure of this dissertation has been organized to guide the reader through the research conducted from inception to completion. Chapter 1 presented the reader with the foundational knowledge to establish the relationships between the problem and the research. The motivation for the research was presented along with information about the state of Maryland, which was the primary focus of this study. The background of the problem was then presented and included details relevant to the field. The problem was then stated, followed by the research questions and hypotheses that guided the research. Chapter 2 provides an examination of digital forensic readiness by examining the concept holistically, identifying trends, knowledge gaps, and areas of concern. Chapter 3 presents the research methodology utilized to answer the three research questions posed. Chapter 4 presents and discusses the results of the research conducted following the methodology presented in Chapter 3. The document is formally concluded in Chapter 5 with a summary of this work along with ways in which this work can be potentially leveraged for future research.

CHAPTER 2

LITERATURE REVIEW

This chapter has been prepared to provide the reader with a comprehensive overview of the state of the literature. First, a high-level overview of the literature will be provided and will serve as the foundation. Each concept is then independently examined to add additional depth as well as to provide additional details on the theories, practices, and knowledge gaps identified within the literature.

Digital, or computer forensics, is a field in its relative infancy (Du, Le-Khac, & Scanlon, 2017). While much research has been conducted on various ways to improve the field, there are areas of the field, such as localized need that have gone mostly unexplored (Flory, 2016). Localized digital forensic readiness postures, especially of law enforcement agencies, is important data that can be leveraged by local, state, and federal officials to identify deficiencies and gaps and for the purposes of resource allocation and process improvement (Flory, 2016; Gogolin & Jones, 2010; Harichandran et al., 2016).

Several prominent studies do exist, such as those conducted by Hickman and Peterson (2004), the Institute for Security Technology Studies (2002), and the National Institute of Justice (2006), but many of these could be considered dated for the purposes of comparative analysis (Flory, 2016). More recent studies have been conducted and include works by Flory (2016), Henry, Williams, Wright (2013), Gogolin & Jones (2010), and Harichandran et al. (2016), but presently datasets, especially those that examine areas independently, are far and few between. To fully appreciate the depth of digital forensic readiness, several key areas within the literature need to be examined.

The first topic presented in this section is the evolution of the digital forensics process, along with tools that are used to support the process. This is then followed by an examination of needs analysis and how this approach has been used to explore digital forensic readiness in prior research. The concepts of digital forensic readiness in law enforcement is then presented. This is followed by sections on resource availability, training and education, and legal and regulatory environments, all of which can affect digital forensic readiness. Backlogs are then explored in-depth as this issue was a key consideration and motivating factor during this research. Advanced methodologies will then be examined. Finally, this chapter will be summarized.

Digital Forensics Models & Phases

Within the law enforcement community, there are many different approaches that can be utilized to facilitate the digital forensics process. One well known digital forensics model that has assisted in guiding the development of other models is the Department of Justice's Digital Forensic Analysis Methodology (Carroll et al., 2008; Decusatis et al., 2015). From a very high level, the model consists of three primary integral phases. These phases include *preparation and extraction, identification,* and *analysis* (Carroll et al., 2008). These phases are meant to be conducted in a waterfall fashion; however, certain scenarios can cause iteration either forward or backward (Carroll et al., 2008). These phases and their subphases will be detailed throughout this section.

Preparation & Extraction

The preparation phase is a critical phase in the digital forensics process. The phase is predicated on proper authority to begin *and* the application of inductive reasoning to determine if the data sources have the possibility to contain information relevant to the original request (Carroll et al., 2008; Sammons, 2012). To clarify, an original request is a request that originates prior to the current phase and specifically details case level information that serves as both the guide and boundaries for the examiner. If these conditions are met, the examiners can move forward with an acquisition of the evidence.

An acquisition of a digital device consists of creating a bit-for-bit copy, otherwise known as a forensic image, of the original source (Carroll et al., 2008). The acquisition can be at the logical (file system) or physical (entirety) levels. Careful consideration must be made to determine the most appropriate method of acquisition as the primary goal at this stage is to ensure the integrity of the original evidentiary item. Methods and technologies do exist to promote integrity, with new and novel approaches being created to address emerging challenges, but certain newer technologies are complicating the process (Novak, Grier, & Gonzales, 2019).

It should be noted that the acquisition process can become extremely difficult in environments that leverage cloud-based technologies. For example, Raju and Geethakumari (2019) noted that in cloud-based environments, one must consider the acquisition of virtual items such as *vRAM*, *vdisks*, and other dynamic data sources. While supporting technologies are being produced to address these types of challenges, many of the underlying methods are still theoretical or experimental (Novak et al., 2019; Raju & Geethakumari, 2019). When this is mapped back to the concept of readiness, it must be determined if the investigating authority understands these challenges and their implications. This leads to the assumption or expectation that the individuals performing an acquisition possess the proper training and that the tools being utilized are validated at an agency or industry defined frequency (Carroll et al., 2008). As with any scientific process the results must be repeatable. Challenges and training aside, once the acquisition has occurred, the process must be validated, which in digital forensics is referred to as maintaining evidentiary integrity.

The way the integrity of an image is validated is by using a hashing algorithm that derives a unique identifier that represents the data being collected. Hashing, unlike encryption, is a one-way function. In other words, the identifier produced by the algorithm cannot be used to reproduce the data. This process is illustrated in the following figure (See Figure 2):

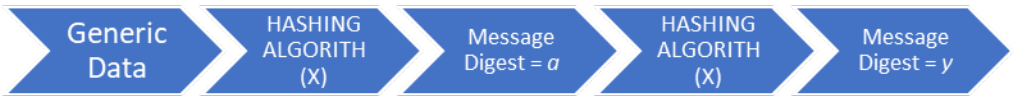


Figure 2. Hashing Process

Carroll et al. (2008) creatively describe this process as fingerprinting. The hash of the original item *must* match that of the original source; however, there are situations where the hashes may not match in which case it is advised that the examiner stop the process and seek guidance from the individual or entities that submitted the original request for analysis (Carroll et al., 2008). It should also be noted that it is a commonly accepted practice to use more than one hashing algorithm to “minimize the risk of hash collisions and harden the overall process against hash collision attacks” (Spreitzenbarth, 2015).

Some of the more commonly utilized hashing functions are the message-digest algorithm (MD5) and the secure hashing algorithm (SHA). When selecting the appropriate function, one should consider both stability and performance. Roussev (2009) notes that MD5 hashing is the most popular choice as hashing can occur at a rate of “400Mbytes per second on a single core.” As such, MD5 should be considered when performing a hash of the entire contents of a drive. On the other hand, SHA-1 is particularly attractive for file sorting large datasets in memory (Roussev, 2009).

Identification

The identification phase is where the examiner will attempt to identify items relevant to the original request (Carroll et al., 2008). Digital devices can contain a significant amount of data. This data can present as images, videos, logs, and other various files and file formats. Examiners, at this stage, must review each of these items to determine their type and possible relevance to the case (Carroll et al., 2008).

In some newer models, this phase has been referred to as the examination phase (Decusatis et al., 2015). This phase can prove somewhat complicated as items may be obfuscated by way of abstraction or secured by way of encryption. Either of these scenarios may slow the process significantly. This is also a point of consideration from a readiness perspective as these challenges require individuals with specific training and specialized tools that may exceed the operating budgets of smaller entities (Flory, 2016). When resources are not available, one possible outcome is an evidentiary backlog, which may persist until external or other sources are sought that can provide assistance (Flory, 2016). Outside of resource concerns, there are other possible impediments to this process.

Another possible challenge that examiners may face during this phase is the possibility of uncovering an incriminating item that falls outside the scope of the original request (Carroll et al., 2008). Carroll et al. (2008) provide a hypothetical example of an investigation centered around tax fraud where, during the course of the identification phase, images of child pornography are identified. In such a situation, it is important to cease all activity, escalate the request, and obtain additional and appropriate authority to proceed (Carroll et al., 2008).

While this may cause delays during an investigation, it is an imperative action as case law is constantly evolving that may impact the process (Baer, 2014). These types of items, as well as the originally scoped items, may also lead to additional data sources.

In the world of the Internet of Things (IoT), the connectivity of devices creates an expansive web that examiners must consider when conducting an investigation. Emails are transmitted and stored in multiple locations, refrigerators can store and send data, and your toaster may be monitoring and storing audio recordings in the environment in which you have placed it. Carroll et al. (2008) note that these items can be important sources of evidence that may be used to build a stronger case or support additional charges; however, this can come at a price. Specifically, the investigators will need to determine if there will be a “return on investment” and if these new leads are worth it (Carroll et al., 2008).

The ability to answer these types of questions map back to the concept of digital forensic readiness; however, considering the possible depth, one must ask the question; what is a realistic level of readiness? As has been noted, there is no consensus at present on this topic (Flory, 2016; Harichandran et al., 2016). Assuming the investigation does not stall as a result of issues such as these, the process will continue into the analysis phase.

Analysis

The analysis phase is one in which all the aforementioned items are connected in a logical, coherent fashion. Carroll et al. (2008) note that this is the stage where the how, who, where, when, and what really begins to come to light. One way this can be accomplished is through the generation and presentation of timelines.

Timelines can be used to represent events, such as interactions with data artifacts, listed in chronological order. Investigators and examiners can leverage timelines to piece together events. These events can either prove or disprove a theory and should never be presented in a way that could create false or misleading assumptions (Casey, 2011). This can sometimes prove to be a challenge for examiners as the judicial system allows for certain evidentiary items to be presented in a light unintended by the original examiner (Casey, 2011). From a readiness perspective, ensuring that examiners possess training that covers issues such as the ethical application of evidence should be considered. This is especially important during this phase, because the products of the phase, as presented by Carroll et al. (2008), will lead to the generation of a forensic report.

Initial Staging & Final Stages

As was noted earlier, there are several additional steps to the forensics process that must take place both before and after the phases that were noted in the previous sections. These steps are integral to the process as they set the stage from inception through to the reporting and closeout. These remaining steps were withheld up to this point due to how these phases can potentially be misperceived without prior knowledge of the legal system and its relation to digital forensics. These steps include the obtaining and imaging of forensics data, the forensics request, forensic reporting, and case level analysis (Carroll et al., 2008).

During the preparation and extraction phase, it was noted that data duplication of the source would occur. What may not have been clear from this description is if the examiners are working from an already duplicated item or the original item in question. To clarify, Carroll et al. (2008) note that the *obtaining and imaging forensic data* phase, which is listed as the first item of the process, can be a by-product of the *identification* phase. Earlier, it was mentioned that certain artifacts might lead to additional sources. Assuming this to be the case, the process would need to be reset, which is where this phrase can come into play. This phase may also trigger additional forensics requests, which would then follow the waterfall model unless another iteration is required. This is represented by the following illustration (See Figure 3) presented by Carroll et al. (2008):

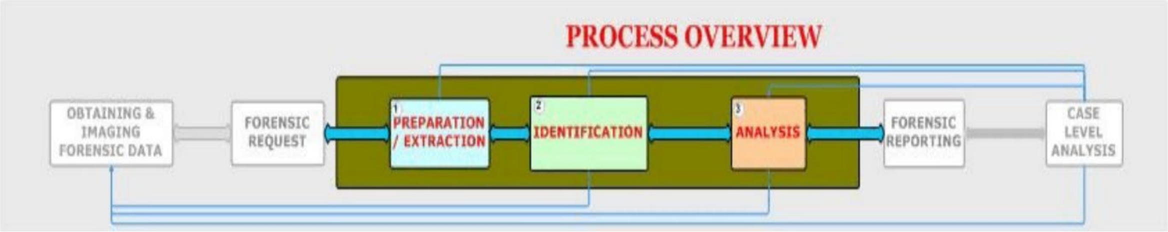


Figure 3. DOJ – Digital Forensics Process Overview (Carroll et al., 2008)

In the model by Carroll et al. (2008), *forensic reporting* comes after the *analysis* phase but is not considered as part of the core process. Decusatis et al. (2015) diverges from this mindset and considers this phase as the fourth core. Reporting is itself an involved and complicated task that considers the entirety of the process. It is noted that the report should contain both the results and limitations of the examination, which would suggest a conclusion of the process (Decusatis et al., 2015). This differs from Carroll et al. (2008) model, where the process has the potential to iterate based on the results of the case level analysis step. Research by Mushtaque et al. (2015) noted that practitioners found many of these early models to be confusing. It was further suggested that condensing these phases impeded adaptability and failed to consider the prospects of new and emerging issues (Mushtaque et al., 2015).

Supporting Tools

The digital forensics process can be supported by a number of tools. These tools can consist of commercially available and open-source software products, hardware-based products, and various policy models. While there may be variations in brands or approaches, there are several tools and process models that are common and will likely be encountered during a review of a digital forensics investigations unit (Abulaish & Haldar, 2018). Two of these models have already been introduced in the prior section, and additional models will be discussed later in this chapter. This section will focus specifically on software and hardware-based tools, their application, and significance to the concept of digital forensic readiness.

Software

Software-based digital forensics tools have been designed to assist in streamlining some of the steps of the digital forensics process. Tools such as EnCase, Forensic Toolkit (FTK), Axiom, and X-Ways contain various features that can facilitate the processes of acquisition, analysis, and reporting. Like forensics models, there is no one universally accepted software-based tool, and certain cases may require a combination of tools in order to meet the objectives of an investigation. Subsequently, due to the possibility of various resource constraints, individual agencies may be limited to only specific applications (Gogolin & Jones, 2010). Understanding both the capabilities and limitations of these types of applications will now be presented in relation to their place in the digital forensic process from a digital forensic readiness perspective.

EnCase, FTK, Axiom, and X-Ways are all commercially available tools that require annual licensing. At their face, they are all designed to assist the examiner in completing some of the more tedious tasks that are involved in an investigation. For example, Carvey (2014) discussed the concept of direct and indirect artifacts that can be generated during an investigation. Direct artifacts are ones that are a product of an incident or are relevant to an incident. In contrast, indirect artifacts are ones that are generated as a result of some common system process (Carvey, 2014). Indirect artifacts can become problematic, especially in Windows environments, where processes running in the background can generate a plethora of activity that, for lack of a better term - muddies the water (Carvey, 2014). These tools can assist in sifting through the mud, making it much easier to identify relevant artifacts. From a readiness perspective, the ability to streamline processes, such as these, may increase the speed in which evidence gets processed. Of course, this is hypothetical, as other resource constraints or even backlogs may already exist that negate these immediate benefits. Additionally, cost may be a consideration, especially with the three tools noted above. Smaller agencies, or even larger agencies, may find themselves moving towards cheaper or open-source options to satisfy their needs.

There are quite a few free alternatives to some of the aforementioned commercial packages. One well known freely available package is the Sleuth Kit (Autopsy), which is a platform similar to EnCase (Altheide & Carvey, 2011). Now, it could be reasonably argued that Autopsy does not offer nearly as many features as the commercially available tools. Its application should not immediately be ruled out, though, as it still offers important features such as timeline analysis, keyword searching, and even the ability to leverage custom modules (Decusatis et al., 2015). In fact, this particular kit has been suggested for inclusion in a rather novel methodology that is completely composed of open source tools (Decusatis et al., 2015). In addition to Autopsy, entire Linux distributions exist that contain freely available tools that support these forensics process. Two well-known platforms are CAINE and Kali (C.A.IN.E., 2018; Offensive Security, 2019). These packages, some of which are open-source, tend to be community supported and are updated on a regular basis to satisfy the needs of forensic and cyber security practitioners alike. The selection of tools from this category may be the result of resource constraints or personal preference.

As was just noted, the selection of any tool needs to be carefully considered in relation to resources and the ability of the examiner to operate them (Pollitt et al., 2004). In addition, these tools need to be considered and treated as scientific instruments as their reliability can be called into question during litigation (Losavio et al., 2019; Pollitt et al., 2004). Examiners should strive to avoid these types of challenges by practicing proper validation in order to preserve the integrity of the field and their agency or organization.

Hardware

Digital forensics investigations would be significantly impeded without hardware to interface with. Without some way to indirectly interface with the device(s) or data in question, the examiner would be left with no option but to conduct an examination on the source. It has been stated that this would inevitably compromise the integrity of the evidence in question (Rajamaki & Knuuttila, 2013). This would also create significant problems and is counter to both accepted practice and applicable case law (Cole, Gupta, Gurugubelli, & Rogers, 2015). As such, this section examines common digital forensics hardware and its relationship to digital forensics and digital forensic readiness.

Like software tools, hardware-based tools specifically designed to support the forensics process may come at a significant financial cost. Forensic workstations, for example, which are powerful machines designed specifically for the purpose of conducting speedy and efficient investigations, can run in excess of $10,000 (Digital Intelligence, 2019). The features of these machines, along with various bundled commercial software packages, can further drive the cost. When deciding on such devices, one should have a realistic expectation of operational capacity.

From a digital forensic readiness perspective, the question could be raised; should an agency possess equipment that far exceeds the current or anticipated need based on case growth? Furthermore, is case growth a product of increased population or increased reliance and use of digital devices? These are important issues that agencies must consider when investing in forensic hardware; however, there are cheaper alternatives.

McMillon (2003) found that it was theoretically possible to build a forensic workstation for under $150.00 by using parts commonly found in corporate environments. While the system proposed may not support a large caseload or contain sufficient resources to process large data sources in a timely and efficient manner, it does demonstrate that scalability is possible when faced with resource constraints (McMillon, 2003). It should be further noted that a system such as the one proposed may not pass judicial scrutiny

(McMillon, 2003). This is where the concepts of accreditation and validation truly come into play, as was discussed in detail by Sammons (2012). It was found that with proper training and scoping, it may be possible to mitigate some of these concerns (McMillon, 2003; Sammons, 2012).

Needs Analysis

In the world of needs assessment (analysis), there are three primary models: decision-making, discrepancy, and marketing (McKillip, 1987). The decision-making model is designed to examine synthesis in applied research (McKillip, 1987). The discrepancy model is popular in the field of education and "emphasizes normative expectations" (Pruett, 2006). The marketing model is used by organizations, using a feedback approach, to explore and adapt to the needs of their target audience (Pruett, 2006). Understanding why specific models are selected during the research process provides insight into not only how data was potentially solicited, but also how that data was interpreted.

During this review, it was found that early studies utilized a hybrid approach that combined the decision-making and discrepancy models (Rogers & Seigfried, 2004). It was found that this approach had proven particularly useful when comparative datasets were limited or non-existent; however, it was further noted that there is a potential for bias when the data gathered using this approach is over generalized (Rogers & Seigfried, 2004). In fact, Rogers and Seigfried (2004) specifically noted in their study, the risks of overgeneralization and the need for larger datasets with clearly identified demographics. Research by both Flory (2016) and Gogolin and Jones (2010) resulted in similar findings despite the research having a more localized focus. Both studies also resulted in raising more questions and ways in which to define the concepts of readiness from a needs-based perspective (Flory, 2016; Gogolin & Jones, 2010).

Harichandran et al. (2016) examined the concept of need within the digital forensics' community using a novel approach that examined future needs based on current perceptions. Using a survey-based instrument, various areas such as education, training, and support were presented to the digital forensics' community. Demographic questions were provided to assist in the analysis of the data (Harichandran et al., 2016). The resulting data were then compared to previous research conducted by Rogers and Seigfried (2004). It was found that several categories of *need* remained the same; however, some areas shifted (Harichandran et al., 2016). While Harichandran et al. (2016) presented possible reasons for the shifts, the primary takeaway, from a needs perspective, is that these areas, just like the field, tend to be dynamic. The dynamic nature noted in the Harichandran et al. (2016) study also supported previous findings that need-based survey instruments should be modified and adjusted so that additional areas or current concepts can be further explored (Flory, 2016; Gogolin & Jones, 2010; Harichandran et al., 2016).

Digital Forensic Readiness in Law Enforcement

The origin of the concept of digital forensic readiness as a founding principal can be debated. Derived from the concept of organizational readiness, the focus can be described as a method for implementing a digital forensics program that is both cost-efficient and reliable (Tan, 2001). Elyas, Ahmad, Maynard, and Lonie (2015) noted that this concept had evolved over time with significant contributions from Pangalos and Katos (2009), who introduced the idea of controls that promote both the facilitation and anticipation of various digital forensics incident types. Further refinement of these concepts has resulted in process models that encompass the entire forensics process and promote adaptability (Elyas et al., 2015). Digital forensic readiness from a law enforcement perspective is no different except that many agencies are bound by budgetary, staffing, legal, and technical constraints that prevent or impede an agency's ability to reach various levels of readiness (Dilijonaite, 2018; Karie & Karume, 2017).

For example, in a study of law enforcement agencies within the state of Michigan, it was found that many agencies were significantly lacking in their digital forensic readiness posture (Gogolin & Jones, 2010). Specifically, these agencies lacked the workforce and resources, or a combination thereof, to be able to investigate a crime involving digital evidence (Gogolin & Jones, 2010). Six years later, Flory (2016) would conduct a similar study that examined law enforcement agencies within the state of Indiana. Flory (2016) found that a majority of respondents, sixty-eight percent (68%), reported not having a digital forensics expert on staff with eighty percent (80%) of that same population citing a lack of funding. Interestingly enough, Harichandran et al. (2016) found that even private sector entities felt that the law enforcement community was under-resourced. Identifying these areas is a crucial part of being able to determine the overall digital forensic readiness posture of a given geographic area; however, quantifying this has proven to be a challenge (Flory, 2016; Gogolin & Jones, 2010; Rogers & Seigfried, 2004).

Quantifying digital forensic readiness in law enforcement is difficult due to a lack of standardization in the field in regards to both educational requirements and jurisdictional differences in the judicial framework (Flory, 2016; S. Garfinkel, Farrell, Roussev, & Dinolt, 2009; Garrie & Morrissy, 2014; Gogolin & Jones, 2010; Harichandran et al., 2016; Rogers & Seigfried, 2004). At present, there are no specific set of metrics to be leveraged to generate a readiness score that could be universally applied. This is likely due in part to a lack of willingness by law enforcement agencies to self-report during these types of studies (Flory, 2016; Gogolin & Jones, 2010). In lieu of universal metrics, both digital forensic readiness postures and readiness scores need to be calculated after each study and ideally for each agency.

This section examined the concept of digital forensic readiness in the law enforcement community. A review of the literature determined that readiness varied across the board and that the concept was subjective at best. It was determined that measuring readiness would prove difficult as there is a lack of standardized metrics. Furthermore, data could not be identified for agencies within the state of Maryland, which means that there is no working baseline. These factors directly influenced the methodology and approach selected for this research, as is further detailed in Chapter 3.

Resource Availability

In order to conduct a digital forensic investigation, resources must be available. Resources, for the purpose of this review, are considered both human and physical assets. In one of the earliest studies, it was found that law enforcement agencies lacked both the human and physical assets required to successfully conduct digital forensics investigations (Institute for Security Technology Studies, 2002). Comparing these early findings to more recent findings provides insight into how the digital forensics community is slowly evolving to address issues relating to resource allocation and availability.

In one of the first studies of its kind conducted in 2002, researchers found that the technologies supporting the digital forensics process did not seem to align with the needs and skills of the user base (Institute for Security Technology Studies, 2002). For example, it was found that certain assumptions were being made about the skillsets of end-users, which impeded the ability of “less experienced” investigators to conduct accurate and timely investigations (Institute for Security Technology Studies, 2002). While this type of finding is not necessarily unique to the field, it does raise significant concerns in a field where results can impact both the life and liberty of those directly and indirectly involved during an investigation.

In 2006 a comprehensive needs analysis of forensic service providers was prepared for Congress (National Institute of Justice, 2006). While this research covered the entire forensics community, the results validated previous findings and suggested that the field was not maturing at a sufficient rate (National Institute of Justice, 2006). During this stage, the concept of standardization was explored as a way to address some of the resource concerns; however, budgetary and training impediments were identified with no long term viable solutions being offered (National Institute of Justice, 2006). Upon examination of more recent studies, similar findings and conclusions were noted (Flory, 2016; Gogolin & Jones, 2010).

Resource availability, especially human resources, may continue to decline as the needs of the field evolve. Harichandran et al. (2016) noted that advanced skills, such as reverse engineering, are beginning to fall within the scope of a forensic examiner’s duties. These types of demands on members of the law enforcement community are yet to be understood as research has not yet been conducted that assesses attrition or retention as a result of continuing education requirements. Considering that practitioners within the law enforcement community may also be assigned other duties, as was indicated by Flory (2016), the potential exists for both burnout or attrition. In addition, it has been suggested that monetary compensation may be a motivating factor as private sector entities typically pay more money for the same work (Goodison et al., 2015).

This section examined resource availability and some of the challenges facing law enforcement agencies. It was determined that as the demand for digital forensics examiners grows, law enforcement may have problems obtaining or retaining qualified personnel. In addition to staffing, it was found that budgetary concerns will likely continue to be a problem that will affect an agency’s ability to keep pace, from a technological perspective, with growing cyber threats (Caviglione, Wendzel, & Mazurczyk, 2017). Determining resources availability is a critical element in establishing a digital forensic readiness baseline.

Training & Education

Training and formal education in the field of digital forensics is an important part of obtaining and maintaining the skills needed to conduct a digital forensics investigation. With legal, regulatory, and technological environments continually changing, there is an apparent need for law enforcement personnel involved in digital forensics work to possess minimum educational requirements (Flory, 2016; Garrie & Morrissy, 2014). Based on a review of the literature, it was found that the concept of what constitutes sufficient qualified levels of training are somewhat subjective (Flory, 2016; Garrie & Morrissy, 2014; Harichandran et al., 2016). In addition, it was also noted that there were differences in training standards among various law enforcement agencies (Flory, 2016; Gogolin & Jones, 2010). In this section, a review of the literature is presented that seeks to examine these gaps and inconsistencies in training standards within the law enforcement community.

Gogolin and Jones (2010) noted in their study that “[t]raining levels for digital crimes provide insight into the level of expertise and commitment to dealing with such crimes.” The inference being drawn by this statement is that training is indicative of commitment, and a lack of training would suggest that a given agency is not committed to dealing with such crimes. This statement by itself warrants further examination, as it does not seem to consider variables such as resource allocation adequately. Flory (2016) found that resources may have a direct impact on the training and or the training needs of a given agency. Resource constraints do not necessarily relieve a given agency of providing training to officers or support personnel that deal directly with digital evidence. In fact, training gaps may serve as grounds to challenge the admissibility or reliability of a given evidentiary in question (Bulbul, Yavuzcan, & Ozel, 2013; Garrie & Morrissy, 2014). This then begs the question, what are the minimum baselines?

As the field of digital forensics evolved, tools began to emerge that automated processes that were previously manually performed by the examiner (Garrie & Morrissy, 2014). These tools lightened both the load and training needs of the examiners; however, legal principals still mandated that evidence submitted by individual experts must meet certain minimum standards (Garrie & Morrissy, 2014). In relation to digital forensics, these standards include the ability of the examiner to produce evidence and hypotheses that are reliable (Garrie & Morrissy, 2014). Furthermore, the support of said hypotheses must be presented in such a way so that the process is repeatable (Garrie & Morrissy, 2014). While tools can aid in the process, they are not a direct substitute for both experience and education.

Specifically, examiners still need to understand how computers and their components function and must be able to provide enough detail to quantify their understanding of the field and the evidence in question (Garrie & Morrissy, 2014). It must be kept in mind that digital forensics is comprised of a combination of fields, one being computer science, which is by itself a highly technical field, so finding a proper balance can be difficult absent an industry-wide consensus, which at this time has not been reached (Govan, 2016; Harichandran et al., 2016).

There has been ongoing research in the field of digital forensics, and forensics sciences in general, in regards to what levels of training and education should be required, *if any*, in order practice (Lim, 2008a). While suggestions have been made that would require practitioners to demonstrate a specific skill or set of skills, these standards have not been widely adopted -- at a possible detriment to the field (Melbourn et al., 2019). In fact, Melbourn et al. (2019) noted that the field of forensic sciences had been the target of criticism for lack of universal certification. Until these issues are resolved, agencies have two primary options to quantify education. These options include certification or a formal degree pathway.

Certification

In the world of digital forensics, there are a plethora of vendor-specific and vendor-neutral certifications. Vendor-specific certifications, such as the EnCase Certified Examiner (EnCE) certification, may demonstrate competency in a specific tool, whereas a vendor-neutral certification, like the Basic Computer Forensic Examiner (BCFE), may demonstrate a broader skillset. Attempts have been made to sort through the countless certifications and assign them either a value score, ranking, or way to identify competency categories, but the task has proven quite difficult (Lim, 2008a, 2008b; National Commission on Forensic Science, 2016). In other words, the value may be subjective.

During a comprehensive review of industry certifications, it was found that certification requirements could vary considerably (Lim, 2008b). To avoid the stigmas associated with test-based certifications, it was noted that several certification authorities were requiring a combination of practical exams, demonstrated experience, and validated field experience (Lim, 2008b). While not foolproof, adding layers to the certification framework should theoretically increase the chances that the practitioner will possess the skills advertised by the certifying authority. While outside the scope of this research, determining the factual basis of this hypothesis could strengthen support for those considering certification as a pathway and would strengthen the support for any readiness metric derived from this area.

Formal Degree

Since 2010, there has been a steady increase in the number of digital forensics degree programs being offered by colleges and universities in the United States (Digital Forensics Association, n.d.; S. L. Garfinkel, 2010). This increase may be partially attributed to the rise in demand for the field, which is expected to grow by thirty-two percent (32%) between 2018 and 2028 (Bureau of Labor Statistics & U.S. Department of Labor, 2019). Like certifications, quality and content may vary as some schools offer online programs with no hands-on practice (i.e., hardware interaction), while others provide more robust in-person courses. In addition, the time to obtain a formal degree may take longer depending on the number of credit hours required. Formal degrees may also require courses not relevant to the field.

Certification & Degree Considerations

As has been suggested in the previous two sections, without adopted standardization, state and local officials would have to determine, on a case by case basis, if certification or a degree program is suitable to meet their specific education requirements and needs. When determining value, an agency should consider both the credibility of the program or certification and the return on investment with the return on investment factoring “costs of labor, material, and so on” (Wiles & Reyes, 2011). Finally, anecdotal evidence suggests that there may be a lack of emphasis on both degrees and certifications specific to digital forensics within the law enforcement community (Flory, 2016; Gogolin & Jones, 2010).

State-Level Digital Forensics Training Postures

This section details the digital forensics training postures for the state of Michigan and Indiana. The results from Michigan were derived from a study conducted by Gogolin and Jones (2010). The results from Indiana were derived from a study conducted by Flory (2016).

Michigan

Gogolin and Jones (2010) found, in their examination of law enforcement agencies in Michigan, that it was difficult to quantify the level of training or expertise personnel possessed. This was partially due to the fact that there is a level of subjectivity when it comes to the quality of the training received (Gogolin & Jones, 2010). This finding was interesting and suggested a need for research that examines and establishes metrics that evaluate the overall quality of a specific training program or course. This may need to occur at the individual state level to consider jurisdictional differences from a legal perspective (Losavio et al., 2019). Since no means to establish quality existed, Gogolin and Jones (2010) instead considered the frequency of training against the length of time the agency operated their digital crimes unit (*if any*). Surprisingly, two agencies within the sample self-identified as conducting digital forensics investigations utilizing staff that had no training in digital forensics (Gogolin & Jones, 2010). This finding was particularly interesting and maybe the product of legal loopholes.

During the study, it was noted that the state of Michigan required individuals involved in the field of digital forensics to be licensed (Gogolin & Jones, 2010). The requirement of licensure in a field may provide the public with a means of identifying those individuals that meet specific standards to be able to practice within that given field (Department of the Treasury Office of Economic Policy, Council of Economic Advisers, & Department of Labor, 2015). On the converse, it has been argued that licensing, especially in the field of digital forensics, may deprive individuals the right to practice when licensing requirements are arbitrary (Lonardo, White, & Rea, 2012). It was found that a loophole in the Michigan law existed that exempted law enforcement agencies from licensure (Gogolin & Jones, 2010). This provided the opportunity for agencies to conduct digital forensics investigations using unqualified individuals. This, of course, did not exempt agencies from challenges raised in regards to the spoilage of evidence of related cases - both criminal and civil (Manes, Downing, Watson, & Thrutchley, 2007). While instances of erosion of public trust were not identified, these instances demonstrate the potential for such erosion and may support the push towards standardization at the state level.

Indiana

Flory (2016), in her examination of law enforcement agencies in Indiana, also noted deficiencies in training. It should be noted that the populations for Indiana and Michigan are 6,483,802 and 9,883,640, respectively (United States Census Bureau, 2010a, 2010b). For comparative purposes, these findings suggest that differences in the population may not influence training or training budgets and may suggest other issues systemic to law enforcement. In addition, Flory (2016) noted that a lack of training might be the result of the utilization of paid outside resources. One of the more interesting and creative ways that an agency, outside the state, has dealt with this type of training dilemma is by deputizing volunteers who possessed significant technical training (Gogolin & Jones, 2010). While novel, this concept presents potential gray areas that are considered outside the scope of exploration for this review. It should be noted that no such cases were reported in Indiana; however, there were variations in the surevy instruments used which may account for a lack of data.

Flory's (2016) study suffered from a low response rate. As such, the responses had to be generalized to identify trends and establish relationships. It was found that only twenty-four percent (24%) of the responding agencies had an individual on staff with a certification or degree specific to the field of digital forensics (Flory, 2016). From that same group, it was noted that sixty percent (60%) had at least attended some sort of training related to the field (Flory, 2016). It is difficult to draw inferences from the small sample, so there may or may not be cause for concern when it comes to training in Indiana. As Flory (2016) noted, these areas may need to be further examined using a new instrument.

Section Summary

Technology is still rapidly evolving. As a result, the training and education needs of law enforcement personnel practicing digital forensics must be carefully and continuously considered. For example, agencies must now consider the challenges and complexity of IoT devices that are becoming a more frequent feature of investigations (Cameron, 2018). Based on a review of the literature, the field may benefit from a standardization of educational requirements; however, unless a way is found to consider each jurisdictional difference, this is not likely to happen. At present, states and local agencies should attempt to identify the most appropriate training and education requirements that meet their specific needs.

Legal & Regulatory Environment

Whether it be in support of criminal or civil litigation, for the digital forensics process to be considered legitimate, certain rules of law must be abided by (Borisevich et al., 2012; Losavio et al., 2019). A challenge for digital forensics practitioners and attorneys alike is keeping up to date with the laws of the land. To further complicate things, it has been noted that these laws can vary by jurisdiction (Losavio et al., 2019). While considered mostly outside the scope of this research, the global legal environment must still be examined as current technology presents the chance of cross-jurisdictional challenges (Antwi-Boasiako & Venter, 2017).

There have been calls within the digital forensics community to develop standards for the admissibility of evidence across jurisdictional lines (Antwi-Boasiako & Venter, 2017). From state to state and country to country, differences in standards of admissibility of digital forensic evidence can vary greatly. Losavio et al. (2019) consider the field of digital forensics as an “interdisciplinary activity” that requires careful consideration and coordination of both judicial and technical representatives.

From a technical perspective, the reliability of tools has been a point of contention for years, with the quest for universal standardization being a significant challenge (S. Garfinkel et al., 2009). As a science, digital forensics is premised on the concept of repeatability. In the early years of digital forensics, it was found that this issue was a significant concern; however, it was determined that case law existed that could be used as a guide (Pollitt et al., 2004). Pollitt et al. (2004) noted that there are three major cases that have had a significant influence over the field. These cases include:

- ("Frye v. United States," 1923)
    - Cornell Law School (n.d.-b) noted that this case was the first to establish a baseline in determining if an “expert’s scientific testimony” could be considered admissible. This case called into question the methods in which

evidence had been obtained and whether the methods were generally accepted practice as determined by other experts within the same given field (Cornell Law School, n.d.-b). It should be noted that the Daubert standard has generally replaced the Frye standard, but some jurisdictions may still apply it (Cornell Law School, n.d.-b).

- ("Daubert v. Merrell Dow Pharmaceuticals Inc.," 1993)
    - "The *Daubert* standard is the test currently used in the federal courts and some state courts. In the federal court system, it replaced the Frye standard, which is still used in some states" (Cornell Law School, n.d.-a).
- ("Kumho Tire Co. v. Carmichael," 1999)
    - This case led to the determination that Daubert could be applied to the testimony of non-scientists and non-scientific testimony (Cornell Law School, n.d.-a).

These cases set the stage for the field of digital forensics, and other scientific disciplines, within the U.S. by defining the concepts of experts and admissibility. Under the Daubert standard, it was found that great emphasis could now be placed on the reporting process, which, if done correctly, could possibly negate the need for in-person expert testimony (Garrie & Morrissy, 2014). Unlike physical testimony, though, the report would not be optional (Garrie & Morrissy, 2014).

With the possibility of a report being presented in lieu of physical testimony, the content and methods contained within the report, *and* its author should be able to withstand scrutiny (Garrie & Morrissy, 2014). Assuming the expert is qualified, then there is flexibility in the quality of the content in relation to the approach of the examination (Garrie & Morrissy, 2014). For example, Garrie and Morrissy (2014) present the case of Nucor Corp v. Bell ("Nucor Corp v. Bell," 2008).

During the presentation of evidence by the expert, in this case, a hypothesis was presented that demonstrated that anti-forensic methods were utilized (Garrie & Morrissy, 2014). The specific method of anti-forensics employed was a zeroing technique, which is a common way of erasing data by writing all zeros or random blocks of zeros to a source drive (Garrie & Morrissy, 2014; Meffert, Baggili, & Breitinger, 2016). In situations where this technique is employed, it may be difficult, if not impossible, to recover useful data depending on the specific type of storage device question (Gutmann, 1996). As a result, the expert had to hypothesize why the data was in the state it was in (Garrie & Morrissy, 2014). This was accomplished by developing a method that replicated the findings on the drive (Garrie & Morrissy, 2014). The opposing party raised objections to these theories; however, the court found that the expert had presented the evidence in both a scientific and repeatable fashion, which Garrie and Morrissy (2014) cited as a “nod to the Daubert factors.” This case demonstrated that the courts were willing to afford an expert latitude in their approach assuming that the results that are generated are repeatable (Garrie & Morrissy, 2014).

Backlogs

Backlogs can be an unfortunate byproduct of a lack of digital forensic readiness. In law enforcement, backlogs can result in criminals not being prosecuted in a timely manner or not at all (Watts, 2017). One practice within the law enforcement community, especially at the local level, is to send evidentiary items to state crime labs to be processed (Scanlon, 2016). This process is not always effective.

In Michigan, Gogolin & Jones (2010) noted that “[m]any agencies turned the investigation over to the Michigan State Police Computer Crime Lab, where turnaround time for investigation was widely reported to be one to two years.” Similar occurrences have been noted in Maryland. It was reported that evidence in a child sexual assault case sat unprocessed at the Maryland State Police Computer Crime Lab (MSPCCL) in excess of 5 months (Watts, 2017). While the evidence was eventually processed, and the suspect arrested, the case brought to light the fact that 14 cases were currently sitting in a backlog at the MSPCCL (Watts, 2017).

According to Quick and Choo (2014), as cited in Lillis, Becker, O’Sullivan, and Scanlon (2016), there are several factors that can contribute to backlogs. These can include, “[a]n increase in the number of devices that are seized for analysis per case; “[t]he number of cases whereby digital evidence is deemed pertinent is ever increasing,” and “[t]he volume of potentially evidence-rich data stored on each item seized is also increasing” (Lillis et al., 2016). Each of these examined in context provides some rather interesting insights.

With the rise of the IoT phenomenon, the number of devices that may present evidentiary potential in criminal and civil litigation increases (Lillis et al., 2016). It is anticipated that the number of IoT devices will continue to increase with decreases in technology costs, global population growth, and high consumer demand for these types of devices (Harmon, Castro-Leon, & Bhide, 2015). The increase in seizure rates of these types of devices, as noted by Quick and Choo (2014), may represent an increased awareness in the law enforcement community in relation to the potential value of these types of devices from an evidentiary perspective. This rise may also indicate an increased overall ability of law enforcement to deal with this type of evidence.

Communications logs (i.e., text messages, email), pictures, videos, and other data sources are often identified and can be used to support criminal and civil investigations (Kouwen, Scanlon, Raymond Choo, & Le-Khac, 2018). With the increased prevalence of technology, there is a higher probability that an artifact will be present that can be utilized during an investigation and, finally, at trial (Lillis et al., 2016). Increases in the number and types of reported cyber crime further support this notion (United States Department of Justice, 2018).

As was noted in previous sections, it takes both time and resources to process digital evidence. Each item seized should be analyzed; however, there are situations in which the return on investment must be considered (Carroll et al., 2008). Resource constraints may be a significant limiting factor; however, any item seized should still be processed. Items not processed could be considered in a state of backlog depending on the circumstances.

It has been suggested that increasing resources could help alleviate backlogs, but this may not be a realistic or viable solution (Scanlon, 2016). Scanlon (2016) proposed a novel approach to this problem that would seek to address these resource issues by implementing a system that avoids duplicated efforts. It was noted that duplicated efforts were a primary reason for backlogs and that by merely automating processes and rethinking the digital forensics workflow, you could not only free up resources but also “future-proof” the process (Scanlon, 2016). Of course, approaches like these have yet to be implemented on a large scale, so the impact of such systems is currently speculative (Scanlon, 2016). However, these types of systems demonstrate that it may be possible to address backlogs by simply re-thinking or looking at the process holistically.

Advanced Methodologies

The digital forensics process and its various stages are best demonstrated by examining models. While many models currently exist, some of which were described earlier in this chapter; the current digital forensics landscape may require consideration of new and advanced methodologies. During this review, one rather novel methodology that was identified was a model by Kohn et al. (2013). It was found that this model may have already addressed some of the issues identified by Mushtaque et al. (2015).

One of the main issues identified by Mushtaque et al. (2015) was the lack of adaptability of many of the older digital forensics methodologies. These methodologies were found to lack flexibility, which in turn created confusion among practitioners (Mushtaque et al., 2015). Kohn et al. (2013) model addresses these issues by breaking the core digital forensics phases into sub-phases. In addition, the model considers advancements in the field and the possibility of universal adaptation (Kohn et al., 2013).

When examining this model (Kohn et al., 2013), one of the first things to note is the many sub-phases. For example, the documentation phase acts as a wrapper for the preparation, incident, incident response, digital forensics investigation, and presentation phases (Kohn et al., 2013). Each of those phases can contain an additional one to seventeen steps and may be dependent on the previous steps (Kohn et al., 2013). By introducing these sub-phases and steps, an agency can attempt to map both resources and policies better to ensure a smooth operational environment. It should be noted that this type of implementation may come at a cost.

At the micro-level, each step addresses a specific investigational requirement; however, operating at the macro level may introduce possible points of failure during an investigation. To satisfy the requirements for these phases, there needs to be the proper balance of people, processes, tools, and technology. It is often difficult for law enforcement agencies to satisfy these requirements for a plethora of reasons, including budgetary concerns and human resource limitations (Flory, 2016; Gogolin & Jones, 2010; Kohn et al., 2013). Identifying these types of gaps can be accomplished in a number of ways, including but not limited to, needs-based analysis or stress testing (Flory, 2016).

Needs-based analysis of the problem can be an effective approach when examining the effectiveness of a model; however, previous studies have demonstrated a lack of willingness within the law enforcement to participate in this type of research (Flory, 2016; Gogolin & Jones, 2010; McKillip, 1987). Stress testing, on the other hand, could potentially quickly identify gaps and concerns. This type of testing is used when one wants to examine the limitations of a system by pushing the limits of the system's capabilities (Krishnamurthy, 2004). Like needs analysis, getting law enforcement to participate in such a test would likely prove difficult. Without a willingness to cooperate, data cannot be derived that would allow for proper mapping to the steps in the Kohn et al. (2013) model. This may be a significant limiting factor when considering these types of advanced models.

Literature Review Summary

This chapter presented the current state of the literature by identifying common trends, themes, and gaps. The concept of need-analysis and its importance to the field and this study were presented. Works that exploded digital forensic readiness in law enforcement were then examined. This was then followed by issues relating to resource availability. Issues related to training and education were explored in-depth, and it was found that a lack of standardization may be impeding progress within the law enforcement community. A comprehensive analysis of the legal and regulatory environments that govern the field was also examined, where it was found that jurisdictional differences must be considered when examining and drawing inferences about related datasets. Finally, the concepts of backlogs and the implementation of advanced methodologies were considered.

This review demonstrated that research examining digital forensic readiness within the law enforcement community is still lacking and that the effects of localization are not currently fully understood. It was also noted that there was a lack of literature concerning localized backlogs. In Chapter 3, the methodology used for conducting this research and assessing the digital forensic readiness posture of law enforcement agencies within the state of Maryland will be presented.

CHAPTER 3

RESEARCH METHODOLOGY

This section contains the specific methodology utilized during this study. As was noted in Chapter 1, the purpose of the study was to determine the digital forensic readiness posture of law enforcement agencies within the state of Maryland. During the literature review in Chapter 2, it was found that a study of this kind had not yet been conducted within the state. Studies of a similar nature had been conducted in other states; however, the researchers noted gaps in the literature and suggested a need to expand the current body of knowledge (Flory, 2016; Gogolin & Jones, 2010). These earlier studies served as an important baseline and guide for this research. From this information, it was determined that a quantitative methodology using survey design and a cross-sectional approach would be the most appropriate.

The remainder of this chapter presents the pertinent details of the selected methodology. First, an examination of several common methodologies is presented along with their possible relevance to this research. The research questions, hypotheses, and variables are then examined. This is followed by a presentation of the population and exclusionary considerations. The data collection method is defined and includes details on the solicitation packet, the electronic survey, and the collection period. The survey instrument is then presented. The limitations to the approach are then considered, followed by both a confidentiality and risk assessment. The method of data analysis is examined and contains the establishment of the digital forensic readiness score and how backlogs were considered. The chapter is then formally concluded with a summary.

Review of Methodologies

Ahmed, Opoku, and Akotia (2016) define a methodology as a framework and philosophy that relates to the research process as a whole. In the world of research design, there are many research methodologies that exist. Four of the more common methodologies one may encounter are *design science*, *qualitative*, *quantitative*, and *mixed methods*. These methodologies exist as a way to guide the research process, with the goal being to satisfy the research objectives and answer the research questions in the most comprehensive way possible (Creswell, 2014). The selection of a research method can be personal in that the researcher should consider how to best translate this information, considering both their audience and their own personal experiences (Creswell, 2014). Goulding (2002) takes this idea a step further and notes that the selection process is often difficult as the researcher begins to ponder their interests, convictions, and beliefs in relation to the research. The remainder of this section examines the four aforementioned methodologies and considers their appropriateness to the research that was conducted.

Design Science

The first methodology for examination is design science. Design science is a methodology that is best suited when the research has the potential to or objective of creating an artifact that will improve upon a current state (Wieringa, 2014). While the application of this methodology was initially considered, it was determined during the literature review that data does not currently exist that identifies a specific problem within the state of Maryland that would benefit from an artifact. It should be noted that the data from this research may serve as a baseline for the future creation of an artifact that could be developed using the design science approach. For example, a backlog prioritization or communication system may be possible to address the issues related to backlogs identified within the state.

Qualitative

The second methodology for examination is the qualitative approach. Qualitative research is an inductive approach that is often utilized by those seeking to examine “social or human problems” through the lens of the population being examined (Creswell, 2014). It has been suggested that this “is an umbrella term” with a primary focus on social life and is often nonquantitative by design (Saldaña, 2011). The multidisciplinary aspects of the approach allow for flexibility in the interpretation of the data, especially when one seeks to examine possible flaws in policies or programs (Saldaña, 2011).

During the literature review, and based on the previous considerations, it was found that this could potentially be a suitable approach. Several of the questions in the original survey by Flory (2016) provided respondents with subjective response options. These questions were adapted to this research and included in the survey instrument utilized. As such, it was possible to interpret the data through the lens of the population and consider the issues as both human and social problems (Creswell, 2014). Using this approach would also have allowed for a more in-depth examination of the policies and practices that guide digital forensics within the state. These types of insights could also have added to the currently limited body of knowledge; however, it was determined that the research would be scoped to interpretation and presentation rather than evaluation. In addition, there was a risk that the results may be too narrowly scoped and not suitable for broader context evaluation in future research.

Quantitative

The third methodology for examination, and the one selected for this study, is the quantitative approach. Quantitative research, unlike qualitative, is a more structured approach that tests “objective theories by examining the relationship among variables” (Creswell, 2014). Population samples are used to determine statistical significance (Creswell, 2014). Lowhorn (2007) adds that the population should consist of the entire group in question without consideration of the population density; however, this may be unfeasible. To offset this, quantitative research can leverage representative samples (Lowhorn, 2007). The populations can then be examined using either experimental or descriptive research techniques (Lowhorn, 2007).

The difference between experimental and descriptive research lies with the relationships to the variables (Lowhorn, 2007). Experimental research is considered a more robust approach that tests the causational relationships between the dependent and independent variables (Lowhorn, 2007). Descriptive research is less prescriptive in regards to the valuation of the variables and places emphasis on describing the sample at that point in time (Lowhorn, 2007).

Mixed Methods

The fourth methodology for examination is the mixed methods approach. The mixed-methods methodology leverages the previous two methodologies with the assumption that the data can be interpreted in a way that provides deeper meaning and understanding (Creswell, 2014). Creswell (2014) notes that some of the reasons a researcher may choose this method include gaining a better understanding of the instrument used to measure the data, understanding needs, and to compare different perspectives. In relation to this research, this methodology could have provided significant insight into both the data and the responses. This approach would have been appropriate if the research questions were focused on causational relationships of individual programs rather than relationships related to proximity. Based on the justifications cited by Creswell (2014), future research directed towards understanding the programmatic problems or the effectiveness of the survey may be warranted.

Research Questions, Hypothesis, and Variables

This research focused on establishing a digital forensic readiness posture score for each agency; determining the rates of degradation of these scores in relation to the distance between Baltimore, MD, and Washington, D.C.; and to determine if the readiness scores correlate to backlogs. To focus this research, the following three research questions were defined:

> RQ1. What is the current digital forensic readiness posture of law enforcement agencies in the state of Maryland?
>
> RQ2. Does an agency's proximity to or availably of external resources influence its internal digital forensics posture?
>
> RQ3. What impact, if any, does an agency's internal digital forensic readiness posture have over any internal backlogs of digital forensics evidence?

To guide the research, two hypotheses were proposed. According to Creswell (2014), a hypothesis maps variables to a research question or an expected outcome. Hypothese one

(HP1) defines the independent variable as the distance and the forensic readiness score as the dependent variable. Hypotheses two (HP2) defines the independent variable as the distance and the backlogs as the dependent variable. HP2 is a null hypothesis, which is a hypothesis that predicts that "no relationship or no significant difference exists between a group on a variable" (Creswell, 2014). While Creswell (2014) suggests not selecting both hypotheses and research questions together, this method may be appropriate when the hypotheses support the research questions. The hypotheses prepared for this research are as follows:

HP1. Law enforcement agencies within the state of Maryland that are within a twenty-mile radius of the two primary central *hubs*, Baltimore, MD, and Washington D.C., will exhibit a more mature digital forensic readiness posture.

HP2. It is hypothesized that all agencies, regardless of their distance between the *hubs,* will exhibit similar digital evidence backlogs when viewed in relation to the populations of the county or municipality in which the agency is located.

The next section examines the population. It is important to understand the population and how it was selected, as this directly maps back to the creation of the research questions and the development of the hypotheses. All of this will be tied together in Chapter 4 with the examination of the data.

Population

The population for this research consisted of all law enforcement agencies within the state of Maryland. Law enforcement agencies, for the purpose of this study, included state, county, city, and municipal law enforcement agencies as well as any specialized agencies that are not classified as federal law enforcement agencies. As was noted in Chapter 1, a total of one-hundred-forty-one (141) agencies met the criteria to be considered as an active law enforcement agency for the purpose of this study. These agencies were obtained from a public website maintained by the state that contained all law enforcement agencies in the state (Department of Public Saftey & Correctional Services, n.d.).

Exclusions

Creswell (2014) notes that population samples should not usually be manipulated. As such, the original goal of this research was to include all agencies as identified by the state. However, it was determined that this would not be the best approach based on questionable inclusions in the state's list.

During an examination of the state list, it was determined that some of the agencies listed did not meet the definition of a law enforcement agency for the purpose of this study. The agencies excluded from consideration were either defunct or were healthcare facilities that may have private security or special police as opposed to regular sworn officers (Department of Public Saftey & Correctional Services, n.d.). In addition to the exceptions noted above, it was found that some of the agencies listed were assigned to schools. During an analysis of these agencies, it was difficult to determine, based on the limited availability of publications, whether these agencies were primary law enforcement agencies, sub-agencies, or affiliates. As such, only the agencies that could be identified as primary agencies were included in the population.

Data Collection Method

The study was conducted by first gathering the contact information for all local and state law enforcement agencies within the state of Maryland. The process for collecting this data included utilizing information provided on a publicly available website maintained by the state of Maryland (Department of Public Saftey & Correctional Services, n.d.) along with additional web searches for verification purposes. Verification included ensuring that the contact email address listed on the state website aligned with the email address on the agency site. It should be noted that several discrepancies were identified. These discrepancies related to changes in the command structure or other personnel-related changes. Physical addresses were also compared for accuracy. All physical addresses were confirmed to be correct. Once this information was verified, a solicitation packet was prepared, the electronic survey instrument was generated, and the collection period was defined. These items are detailed in the following sections.

Solicitation Packet

Once verification had occurred, a solicitation packet was prepared. This solicitation packet included a study solicitation letter (See Appendix A), a survey instrument (See Appendix B), as detailed in the next section, and a self-addressed stamped envelope. The solicitation letter contained information about the study, including the risks. It offered the respondent the option to complete the physical survey or complete the electronic version if an email address was identified in the previous stage. For tracking purposes, the survey instrument contained a unique identifier known only to the researcher. This contact packet was then sent through the United States Postal Service (USPS) to the population list that had been previously assembled.

Electronic Survey

As was previously described, respondents had the option to either mail back the paper survey or complete the survey online. The online survey was prepared using the Survey Monkey platform. This particular platform was selected due to the fact that it meets or exceeds industry standards for confidentiality and security (SurveyMonkey, 2018). It was also determined that the platform would provide assistance with securing the approvals required to satisfy the requirements for the Dakota State University (DSU) Institutional Review Board (IRB) (SurveyMonkey, 2018).

A link to the survey instrument was distributed to the contact email address identified for each agency. Email addresses could not be identified for twenty-seven (27) agencies. As such, one-hundred-fourteen (114) emails were sent. This link was sent six business days after the solicitation packet was sent. A reminder email would be sent on January 6, 2020. The content of these emails can be found in Appendix E. The links were monitored for activity, and this information was considered during data analysis, as presented in Chapter 4.

Collection Period

The total collection period ran for 36 calendar days from when the original solicitation letter was sent. This period ran from December 6, 2019 (06DEC20) to January 10, 2020 (10JAN20). When the collection period had expired, the electronic survey was disabled. Physical surveys were collected for three business days after the online survey was closed. This was to account for any delays in the physical mail service. All envelopes containing physical surveys were examined to ensure that the postmark date fell within the survey window. Any envelope found to have a postmark date later than the survey end date of 10JAN20 would be discarded.

Survey Instrument

Creswell (2014) notes that survey design is an approach that can be used when the researcher seeks quantitative data relating to opinions, trends, or attitudes of a population. This study leveraged a modified version (See Appendix B) of a pre-validated survey instrument. The original survey instrument (See Appendix C) created by Flory (2016) was found to be suitable for this research as the questions provided the means for the creation of a digital forensic readiness score. While the survey acted as a good baseline, several additional questions needed to be added in order to address some of the research questions.

Modifications to the survey, as reflected in Appendix B, include the following:

1. Questions 1, 12, 17, 18: Include the option, *prefer not to answer*. These additions were made in response to feedback by the DSU-IRB. This option affords the respondent the option not to answer these specific questions. The inclusion relates to questions that could lead to the possible identification of the agency as noted in the risk assessment (i.e., department size) and those questions that relate to perception, which could impact an agency's reputation.

2. Questions 3, 5, 6: Include the option *I do not know.* These additions were made as a result of careful consideration of the original questions. The original questions assume that the respondent would have knowledge of these topics or that they would be able to locate this information.

3. Questions 21 & 22: These questions were added to gather the data needed to analyze issues relating to backlogs.

Limitations

This study was conducted using a cross-sectional approach and captured data and attitudes at a specific point in time. It was assumed that the respondents would provide responses that were reflective of what *is* and not *what will be*. Answers that are not reflective of the current state could introduce bias. As such, it may not be possible to delineate between these types of responses.

In addition, the term law enforcement agency is broad and may include organizations that would not, as a matter of practice, engage in criminal investigations that include digital evidence. Including a question to determine the agency's capacity was considered; however, it was decided that introducing such a question could skew the results should the agency representative misinterpret the underlying question. Running a pilot study may have allowed for the refinement and inclusion of the question, but this was not possible due to time constraints. As such, examining each agency’s investigatory practices is considered outside the scope of this research.

Participation in the survey was voluntary. The solicitation packet included details of the study and consent material (See Appendix D). Previous studies have demonstrated a lack of willingness on the part of law enforcement agencies to participate in these types of studies (Flory, 2016; Gogolin & Jones, 2010; McKillip, 1987). At the time the study was conducted, the researcher lacked official support from the state. As such, it was understood that the response rates had the potential to be low.

There are limited datasets to compare the data derived from this study. There was only one study of a similar nature identified within the past ten years (Flory, 2016). With rapid evolutions in technology, even data within the past ten years may not accurately represent current trends within the law enforcement community and must be treated with some skepticism.

Confidentiality & Risks

This section contains the steps taken to ensure confidentiality throughout this study as well as the potential risks to the respondent. A formal confidentiality assessment and risk assessment was conducted and presented to the DSU-IRB to ensure the highest levels of research ethics and integrity.

Confidentiality Assessment

Confidentially was carefully considered for this research. Prior to this study, the researcher and committee chair took and passed several Collaborative Institutional Training Initiative (CITI Program) training courses. The CITI Program provides training materials that cover topics such as ethical research, regulatory oversight, and the proper administration of research (CITI Program, n.d.). This training provided the researcher with advanced knowledge in research conduct and ethics. From this training, it was determined that confidentiality would be a concern and that steps would need to be taken to address these concerns. The two primary areas of concern identified were the solicitation of a response that identified the agency size and general data security.

The first area of concern examined related to the solicitation of a response that identified the size of the responding agency. It was noted in the Flory (2016) study that it could be possible to identify an agency based on the reported size of the agency. Since this study considers locality as a driving factor, this area of concern is even more pronounced. To address this, survey question one (Q1) was modified to provide a *prefer not to answer* response option. If the respondent selected this option, it would be difficult to identify the agency even if the data is attributed to a given locality. Furthermore, the presentation of the data was done in a way to generalize the data sources to reduce the possibility of identification.

The second area of concern was the security of the data. This study relied on both physical and electronic forms of communication. The physical forms of communication, specifically the survey, contained a unique identification code known only to the research. This allowed the researcher to determine the locality from where the survey originated. Once the survey was received, it was scanned and saved on two encrypted storage devices (primary & backup). The physical surveys were then destroyed by using an incineration method.

For the electronic survey, a unique link was generated for each respondent that could be monitored for activity. The link was sent to the email address identified during the data collection phase. Just like the physical survey, this provided a way for the researcher to identify localities. To ensure the confidentiality of the electronic data, the researcher leveraged the security integrated into the Survey Money platform. All data that was collected electronically was downloaded at the end of the collection period and stored on two encrypted devices (primary & backup).

Following the DSU-IRB review, it was determined that these steps would be enough to preserve the confidentiality of the respondent and the data. While this section contained some implicit risk, it is pertinent to explicitly state each risk as it pertained to this study. The next section details each of the risks involved with this study.

Risk Assessment

During an analysis of the research design, it was determined that risk was present. The risks identified related to the confidentiality of the data being solicited from the respondents and how to maintain that confidentiality through the research process. The following risk and their mitigations were identified:

> RQ1: There is the potential that the information being solicited could damage the reputation of the organization self-identifying. From a research perspective, this must be a consideration only to the extent that it does not result in the intentional or unintentional exclusion from the population. In addition, state, local, and municipal agencies are not corporations and are therefore not considered individuals under the law. To mitigate this particular risk, the data was presented in a way (See Chapter 4) to obfuscate the responses relating to reputation risk. For example, individual readiness scores were assigned to each agency but only reported at the county level or higher. In addition, perception-based questions were also only presented at the county level or higher.
>
> RQ2: There is the potential that the information being solicited could become compromised. In order to mitigate this risk, it was determined that the data would be stored on two encrypted devices (primary and backup) and accessed on air gaped devices.

Each of the mitigations listed would reduce the risk to near negligible amounts. The risk was disclosed to the respondents in the introduction to the survey sent with the solicitation packet (See Appendix D). The respondents were provided the necessary contact information to contact the researcher, or the DSU-IRB, prior to taking the survey.

Data Analysis

For this study, data analysis was performed using a quantitative methodology. Quantitative approaches use statistical analysis that seeks to transform raw data into information (Omair, 2014). Two approaches within this realm for interpreting data include descriptive and inferential statistics (Omair, 2014).

Omair (2014) notes that the difference between descriptive and inferential statistics is that descriptive statistics present a broader interpretation of the data and population. In contrast, inferential statistics places emphasis on data subsets. In consideration of both the research questions and hypotheses, it was determined that both approaches should be utilized to yield maximum usage of the data. The next sections, Digital Forensic Readiness Score & Analysis of Backlogs, explains this approach in greater detail.

Data Forensic Readiness Score

In each of the previous chapters, the concept of a digital forensic readiness score was discussed. During the literature review, it was found that a universal scoring system does not currently exist. As such, a system needed to be created to generate these scores for each responding agency.

To ensure compatibility with a quantitative methodology, values were assigned to the answers for a subset of the survey questions presented to the respondents. Specific questions, such as the ones related to backlogs, were excluded from scoring. This exclusion was required as no comparative dataset currently exists to asses a proper quantitative score value.

The questions considered most relevant to the establishment of the digital forensic readiness score were Q2, Q3, Q8-Q10, Q12-Q16, and Q18-Q19. Their respective scored values can be seen in the following table (See Table 1).

Table 1. Digital Forensic Readiness Score Chart

Digital Forensic Readiness Score Chart							
Question #	***Response (Weight)***	***Response (Weight)***	***Response (Weight)***	***Response (Weight)***	***Response (Weight)***	***Response (Weight)***	***Max Score***
2	Yes - (.23)	No - (0)	PNTA - (0)				.230
3	Yes - (.05)	No - (0)	IDNK - (0)				.050
8	Yes - (.05)	No - (0)	IDNK - (0)				.050
9	Yes - (.01)	No - (0)	IDNK - (0)				.010
10	1 - (.002)	2 - 3 - (.006)	4 - 5 - (.008)	6 or greater - (.01)	IDNK - (0)		.010
12	Very High - (.025)	High - (.02)	Medium - (.015)	Low (.01)	Very Low - (.005)	PNTA -(0)	.025
13	Extremely Effective - (.025)	Moderately Effective - (.02)	Effective - (.015)	Somewhat Effective - (.01)	Not Effective - (.005)	PNTA -(0)	.025
14	Very High - (.025)	High - (.02)	Medium - (.015)	Low - (.01)	Very Low - (.005)	PNTA -(0)	.025
15	Very High - (.025)	High - (.02)	Medium - (.015)	Low - (.01)	Very Low - (.005)	PNTA -(0)	.025
16	Yes - (.025)	No - (0)	Other - (Variable)				.025
18	Very good - (.025)	Good - (.02)	Fair (.015)	Poor - (.01)	Very Poor - (.005)	PNTA -(0)	.025
19	Yes - (0.50)	No - (0)	Other - (Variable)				.500
Total Score							**1.00**

Note. PNTA = "Prefer not to answer"; IDKN = "I do not know"

Each question selected for scoring purposes pertained to key elements of readiness, as were identified during the literature review. Heavier weights were assigned to values relating to policy, people, and resources in that order. It was determined that these areas were the foundation of readiness (Dilijonaite, 2018; Elyas et al., 2015; Karie & Karume, 2017; Pangalos & Katos, 2009). Perception questions were considered and scored due to the nature of the study; however, it was determined that site visits and observations might have potentially yielded more accurate and useful results. Gauging perception also allowed for an inferential approach to be leveraged to determine the statistical differences relating to proximity relationships.

Analysis of Backlogs

Understanding backlogs in relation to digital forensic readiness was an important part of this research. In order to establish that relationship, data was collected by way of the survey instrument (See Appendix B). Questions twenty-one (Q21) and twenty-two (Q22) focused on the collection of data related to *existing* backlogs. These questions and response options can be seen in the following table (See Table 2).

Table 2. Digital Forensic Readiness Backlog Questions

Digital Forensic Readiness Backlog Questions							
Question #	***Question***	***Response***	***Response***	***Response***	***Response***	***Response***	***Response***
21	Do you currently have a backlog of digital evidentiary items?	Yes	No	I do not know			
22	What is the current number of cases backlogged as the result of digital evidence backlogs?	1	2 - 5	6 - 10	10 - 15	15+	Other (please specify)

Analysis of this data was conducted by first examining the population of the location in which the responding agency oversees. For agencies charged with overseeing institutions (i.e., schools), the populations of the institutions were considered in lieu of a census-based determination. The backlogs could then examined in relation to the population resulting in the possible establishment of an impact score. This impact score could then be used to satisfy HP2.

Methodology Summary

This chapter presented and defended the formal methodology for this research. The approach considered the problem as well as the many factors that could potentially influence the data. The previously validated survey instrument was reviewed, and additions were made to accommodate developments in the field and to answer the research questions related to this study. The formal collection method, including limitations, was presented along with a formal confidentiality and risk assessment. Following these assessments, the methods for data analysis were examined. The basis for the digital forensic readiness score was presented along with the approach to derive, analyze, and present the data. In addition, the method for analyzing data relating to backlogs was also presented. In Chapter 4, the data will be examined using the methodology and approach defined in this chapter.

CHAPTER 4

CASE STUDY (RESULTS AND DISCUSSION)

This section contains a detailed analysis of the data and methods used for this study. As was noted in Chapter 3, a survey instrument (See Appendix B) in digital and paper form was used to collect the data. First, the population response rates are presented along with a reexamination of the pre and post-survey exclusionary criteria. This data will then be presented at the state level, examining such trends as the response by agency size, along with other high-level interpretations of the response data. The data will then be broken down further to analyze trends among various response categories that considered the research questions and stated hypotheses. County-level data will then be examined to provide a broader understanding of the consolidated statewide information. Finally, this chapter will be summarized.

Population & Exclusion Data

The total *perceived* population, as was detailed in Chapter 3, consisted of one-hundred-eighty-three (183) agencies identified using publicly available resources. Forty-two (42) of these agencies were initially excluded for various reasons, including not meeting the definition of a law enforcement agency as defined for the purpose of this study. This left a total survey population of one-hundred-forty-one (141) agencies. This data is summarized in the table below (See Table 3).

Table 3. Population Breakdown

Population Breakdown		
Agency Count (Total)	***Agency Count (Excluded)***	***Total Population***
182	42	141

Of the inclusionary population, each would receive an electronic survey, a paper survey, or both. Additional exclusions would result as a by-product of issues relating to the data collected (incomplete); however, this was found to be negligible considering the final response rate. It must be further noted that some agencies did not receive an electronic survey due to a lack of an identified email address or a bounced email. This data is provided in the table below (See Table 4).

Table 4. Population Contact Counts by Method

Population Contact Counts by Method		
Agency Count (Included)	***Email Survey Sent***	***Paper Survey Sent***
141	118	141
Note. Email addresses could not be located for twenty-three (23 agencies)		

The data noted above and the rationale used to determine exclusions are essential to understanding how the final dataset was built. In the next section, the response rates for both methods of contact will be presented.

Response Rates

Survey response rates for this study were underwhelming but were consistent with previous studies (Flory, 2016; Gogolin & Jones, 2010). Of the paper surveys mailed, only twenty-seven (27) of the one-hundred-forty-one (141) were returned. Each of these responses would be added to the aggregated dataset. The response rates for the electronic surveys were lower.

Of the one-hundred-eighteen (118) electronic surveys sent, only four (4) were completed by the respondents. Forty-one (41) or thirty-four-point-seven percent (34.7%) of the invitations were opened. Seventy-two invitations, or sixty-one percent (61%), were unopened. Four invitations, or three-point-four percent (3.4%), were bounced back. One respondent opted out.

Ten respondents clicked through the survey. One of the four respondents that submitted a response was excluded due to an incomplete submission. An incomplete submission is one in which the user entered answers, but did not click the finish button at the end of the survey. This resulted in a total dataset that included thirty respondents. The response percentages, as noted above, are presented in the table below (See Table 5).

Table 5. Response Percentages

Response Percentages			
Survey Type	***Total Sent***	***Total Received***	***Percentage***
Email Survey	118	3	2.5%
Paper Survey	141	27	19%
Total	-	**30**	**21%**
Note: The total value under the total sent column was not included in the calculations as they represent the same agency set.			

In regards to the population, it should be reiterated that the total population was one-hundred forty-one (141). The twenty-one percent (21%) response rate was similar to Flory's (2016) study, where a (9.9%) response rate was exhibited with a total sample size of two-hundred sixty-three (263).

State-Level Data (RQ1)

The presentation of data at the state level is being provided to demonstrate statistical trends in a holistic fashion. First, an examination of responses relating to agency size will be examined. This data will be compared against the Flory (2016) study to identify any similarities. Second, a presentation and examination of the readiness scores will be provided along with relationships to perceived ability. Third, responses relating to training will be explored. Fourth, perceptions-based question data that considered prosecutorial ability, comprehension of judges and juries, resources, and emerging trends are presented.

Agency Size Response Analysis (Q1)

During this study, one-hundred-forty-one (141) agencies were identified as meeting the criteria of a law enforcement agency, as was defined in Chapter 3. As was previously noted, it is possible that other agencies do exist or that some of the agencies identified were sub-agencies or affiliates. For the purpose of this analysis, these possible deviations were not considered in the calculations presented in this section. The table below (See Table 6), as adapted from Flory (2016), represents the final number of responding agencies by agency size.

Table 6. Responses by Agency Size (Q1)

Responses by Agency Size (Q1)		
Number of Sworn Officers	***Responses***	***Percent of Total Responses***
0 - 5	5	17%
6 - 10	2	7%
11 - 20	5	17%
21 - 50	6	20%
51 - 75	3	10%
76 - 100	3	10%
101 - 150	3	10%
151 - 250	0	0%
251 - 500	1	3%
500 +	2	7%
Prefer not to answer	0	0%
Totals	**30**	**100%**

When compared to Flory's (2016) study, the data is similar in that the largest response rates originated from agencies with a size between twenty-one and fifty sworn officers. The second-largest response rates were also similar; however, this study yielded a tie for second place between agencies of size zero to fifty and eleven to twenty. The table below presents both datasets for comparative purposes (See Table 7).

Table 7. Responses by Agency Size - Maryland v. Indiana

Responses by Agency Size - Maryland v. Indiana				
Number of Sword Officers	***Maryland Responses***	***Indiana Responses***	***Maryland Percent of Total Responses***	***Indiana Percent of Total Responses***
0 - 5	5	1	17%	4%
6 - 10	2	2	7%	8%
11 - 20	5	6	17%	23%
21 - 50	6	9	20%	35%
51 - 75	3	2	10%	8%
76 - 100	3	0	10%	0%
101 - 150	3	4	10%	15%
151 - 250	0	1	0%	4%
251 - 500	1	1	3%	4%
500 +	2	-	7%	-
Prefer not to answer	0	-	0%	-
Totals	**30**	**26**	**100%**	**101%**
Note: The population size for this study was 141, where the population size for Indiana (Flory, 2016) was 263.				

It is of note that a data inconsistency was noted in the Flory (2016) study where the percentage distribution exceeds one-hundred percent. It was further noted that the data, as presented, does not delineate between agency sizes above two-hundred-fifty-one (251). The possible rationale behind these inconsistencies in response rates was considered outside the scope of this survey, but still of note. As such, no correlations or assumptions were made to determine the likelihood of an agency responding to this type of study.

State Readiness Scores

Research question one (RQ1) sought to determine the digital forensic readiness posture of law enforcement agencies in the state of Maryland. To accomplish this, weighted scores were assigned to many of the questions within the survey (See Chapter 3 - Data Forensic Readiness Score). The following sections present a comprehensive review of the data collected and the resulting scores.

Of the returned surveys, thirty were considered complete. It must be noted that compete for the purpose of scoring was that the respondent provided sufficient detail in their responses so that a score could be assigned. Twenty-four respondents required a manual review of their responses. The questions that triggered reviews were any combination of questions three, nine, ten, and sixteen. The analysis of each of these anomalies is presented in their respective sections.

Expert on Staff (Q2)

Question two (Q2) was presented to determine if the agency believed they had an expert in digital forensics on staff. The scoring weight was point-two-three (.23) for an affirmative answer and zero (0) for a response of *No* or *Prefer not to answer*. Twenty-nine respondents responded to question two (Q2). No anomalies were noted. The results are presented in the figure below (See Figure 4).

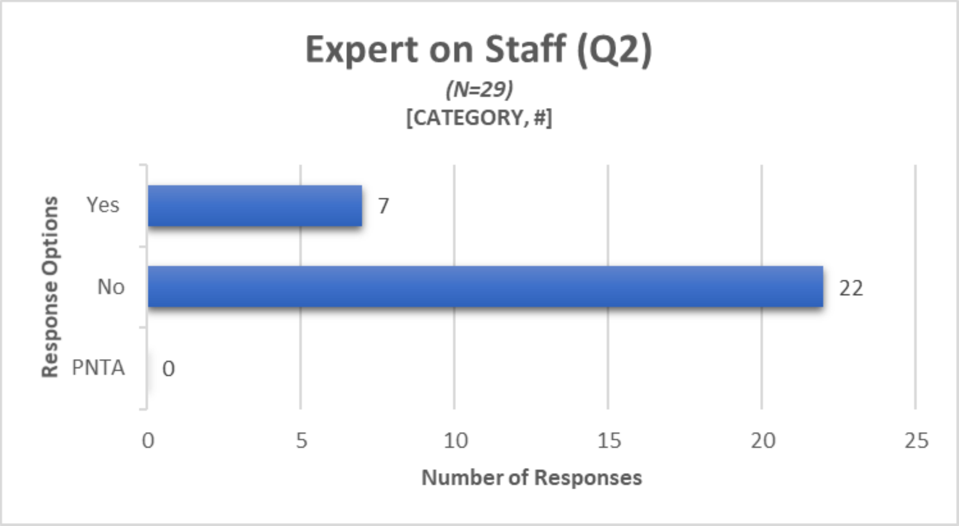


Figure 4. Expert on Staff (Q2)

Twenty-nine respondents provided an answer to question two (Q2). One respondent did not provide an answer. No assumptions were made as to why the respondent did not include an answer, nor was it assumed a non-response should be considered an answer of *prefer not to answer*. For scoring purposes, the respondent that did not provide an answer was assigned a score of zero (0).

Dedicated Expert on Staff (Q3)

Question three (Q3) was presented to determine if the expert on staff was solely dedicated to the function of digital forensics with no other duties assigned. The scoring weight was point-zero-five (.05) for an affirmative answer and zero (0) for a response of *No* or *Prefer not to answer*. Nine respondents responded to question three (Q3). Two anomalies were detected.

Twenty-one respondents did not provide a response to question three (Q3); however, it was found that these respondents did provide an answer on *No* to question two (Q2). Per the instructions, the respondent was to skip to question four (Q4) if providing a response of *No* to question three (Q2). Each of these respondents was assigned a score of zero for question three (Q3).

Two respondents answered *No* for both questions two (Q2) and three (Q3). These responses were in error, as the respondents should have skipped to question four (Q4) based on their responses. As a result, the two responses were excluded from the counts for question

3 (Q3). It should be noted that the score for question three (Q3) was dependent on question two (Q4) and added a positive modifier for an affirmative response. The results, adjusted for the two response errors, are presented in the figure below (See Figure 5).

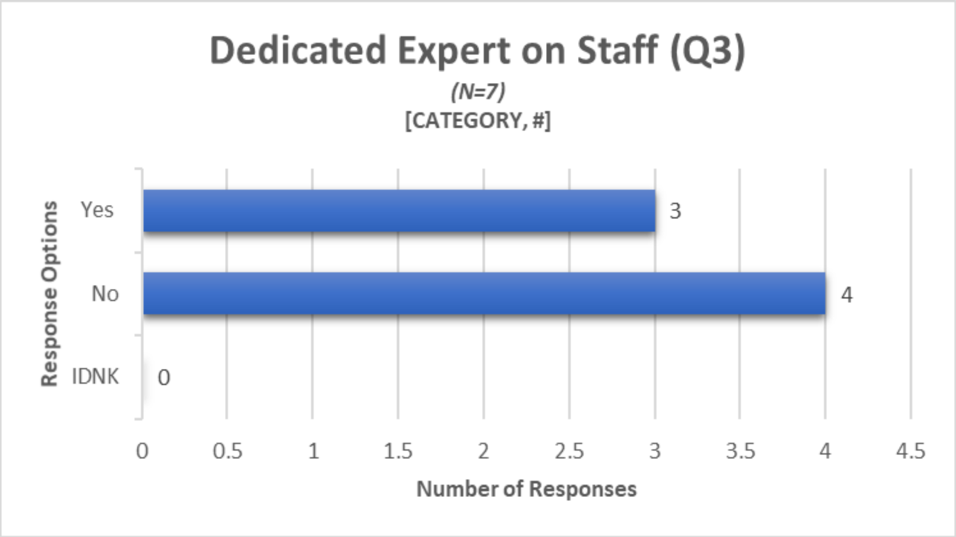


Figure 5. Dedicated Expert on Staff (Q3)

Based on the data collected for question three (Q3), around fifty-seven percent (57%) of agencies that employ a digital forensics expert has that individual employed in that sole capacity. For comparison, Flory (2016) reported ten agencies in Indiana having self-identified as having a digital forensics expert on staff. Of these, only three, thirty percent (30%) were solely dedicated to that task (Flory, 2016).

Training Metrics (Q8 – Q11)

This section examines questions eight (Q8) through question eleven (Q11). These questions gathered data to determine if agency employees had relevant certifications or degrees; were attending training; the number of training sessions attended; justifications or rationale for any lack of training. First, question number eight (Q8) will be presented, followed by the remaining questions.

Training – Certification or Degree (Q8)

Question eight was presented to determine if the responding agency had someone on staff that possessed a formal certification of degree related to digital forensics. The scoring weight was point-zero-five (.05) for an affirmative answer, and zero (0) for a response of *No* or *I do not know*. All thirty respondents provided an answer to this question. The distribution of scores is presented in the figure below (See Figure 6).

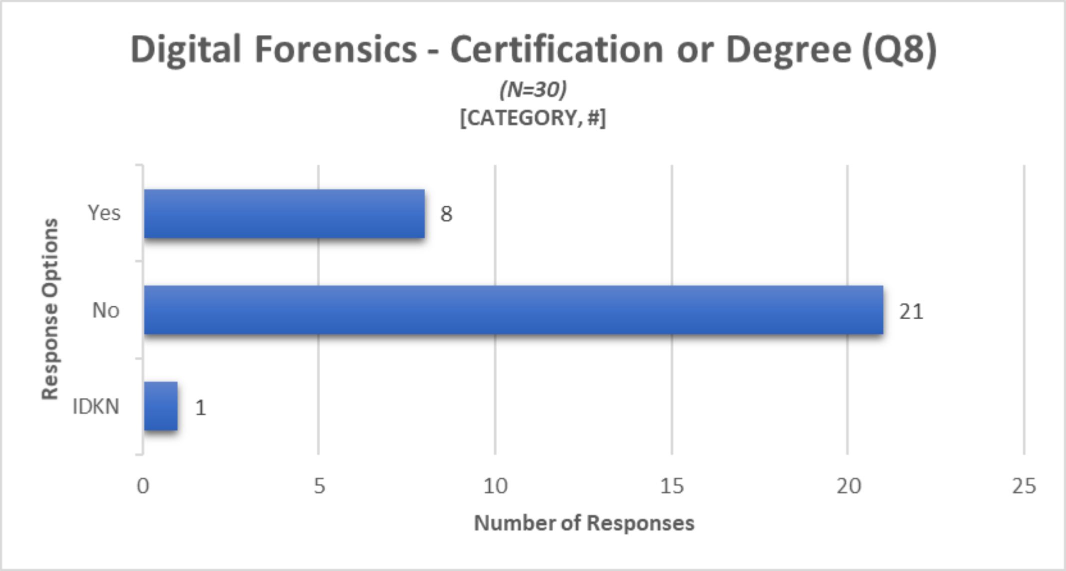


Figure 6. Digital Forensics – Certification or Degree (Q8)

Training – Attendance (Q9)

Twenty-nine responses were received for question number nine (Q9). The scoring weight was point-zero-five (.05) for an affirmative answer, and zero (0) for a response of *No* or *I do not know*. There was one anomaly noted withing the dataset for question nine (Q9), which is explained below.

It was found that one respondent did not answer question nine (Q9), or question ten (Q10); however, they did properly answer question eleven (Q11). The response provided by this respondent for question eleven (Q11) was that there is *no funding available for this type of training*. It was decided that this response was sufficient to correct the dataset to reflect an answer of *No* for question nine as the respondent has indicated that no funding is available for training.

This manual correction resulted in an *N* value of thirty for question nine (Q9). The statewide response totals and distributions for question nine (Q9) are provided in the figure below (See Figure 7).

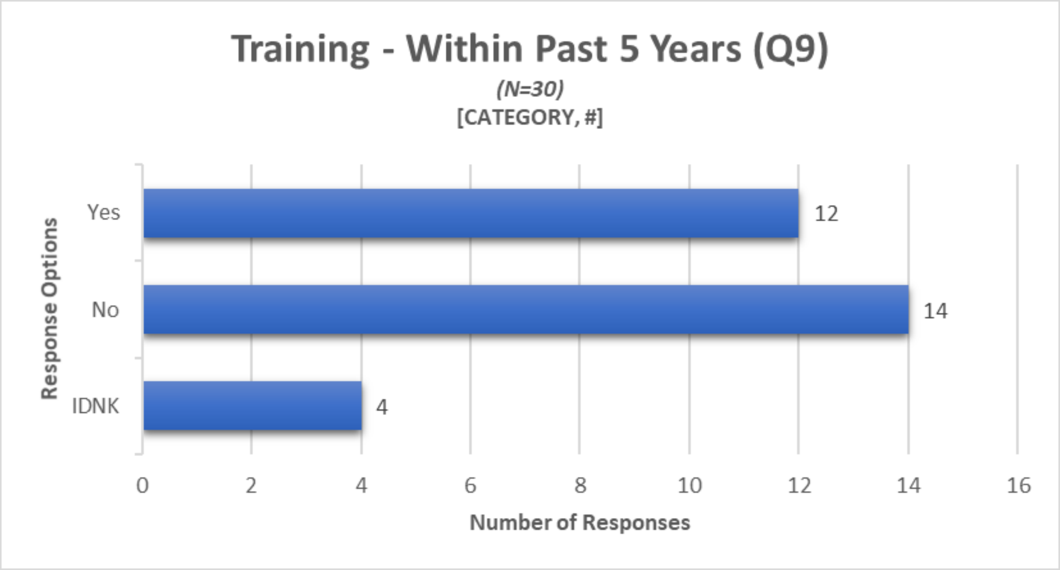


Figure 7. Training – Within Past 5 Years (Q9)

Forty-six percent (46%) of respondents reported that members of their organization did *not* attend any digital forensics training within the past five years. Forty percent (40%) of respondents reported that training(s) were attended within the past five years. A little under five percent (5%) reported, not knowing.

Respondents that answered *Yes* to question nine (Q9) were instructed to continue to question ten (Q10). It is of note that the number of respondents reporting having attended training was less than that reported in Flory's (2016) study. Flory's (2016) study, which had an *N* of twenty-six, found that sixty-percent (60%) of agencies reported having someone within the agency that had attended training within the past five years. The rationale behind these responses for this study and the Flory (2016) are examined in question number eleven (Q11).

Training – Number Attended (Q10)

There was a total of fourteen responses to question number ten (Q10). The scoring weights were: point-zero-zero-two (.002) for a response of *1*; point-zero-zero-six (.006) for a response of *2-3*; point-zero-zero-eight (.008) for a response of *4-5*; point-zero-one (.01) for a response of *6 or greater*; and zero (0) for a response of *I do not know*. During an examination of the counts, it was found that there were two responses above the twelve affirmative answers in question nine (Q9). This anomaly warranted investigation before analysis could begin.

It was determined that one respondent had answered *No* to question nine (Q9) and provided an answer of *(2-3)* for question ten (Q10). A second respondent answered *I do not know* for question nine (Q9), and *I do not know* for question ten (Q10). Both of these responses were in error. The instructions stated that respondents were to move forward to question eleven (Q11) when responding *No* to question nine (Q9). Respondents answering *I do know* to question nine (Q9) were instructed to proceed to question twelve (Q12). As a result, both respondent's answers to question ten (Q10) were disregarded for purposes of the count. Both respondents were assigned a score of zero for questions ten (Q10). No other anomalies were noted. The corrected totals can be found in the figure below (See Figure 8).

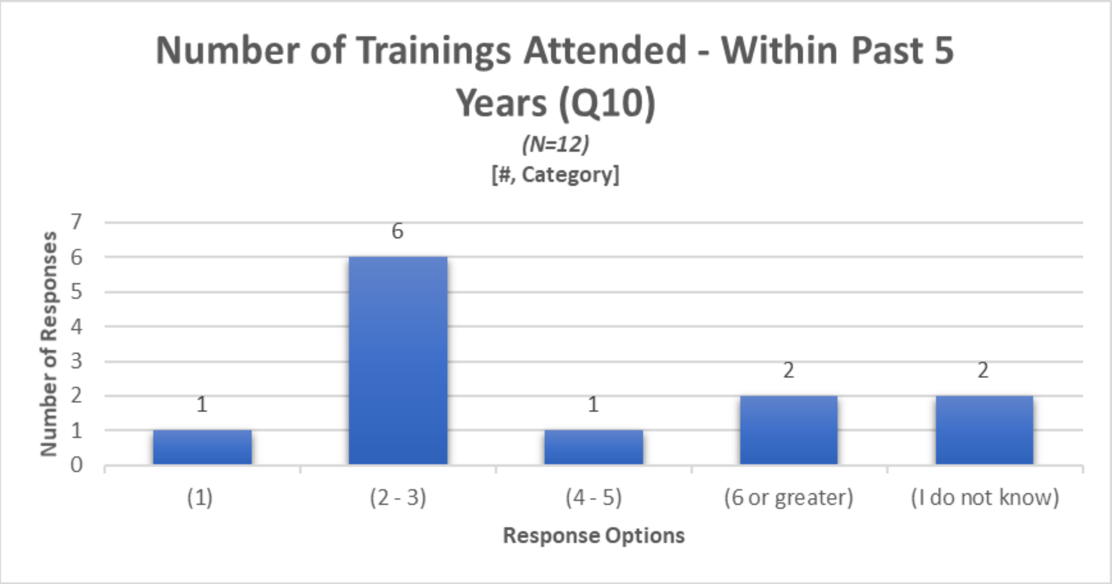


Figure 8. Number of Training Attended -Within Past 5 Years (Q10)

Having gathered these results, the next step was to determine if the number of trainings correlated in any way to the size of the reporting agency. This would be accomplished by examining the reported agency size against the reported number of trainings attended to identify patterns or relationships. It was anticipated that no causal relationships would exist. The consolidated data is presented in the table below (See Table 8).

Table 8. Agency Size to Training Attended (Comparison – Q1 / Q10)

Agency Size to Training Attended (Comparison – Q1 / Q10)													
		Agency Size											
		0-5	***6-10***	***11-20***	***21-50***	***51-75***	***76-100***	***101-150***	***151-250***	***251-500***	***500 +***	***Prefer not to answer***	**Totals**
Number of Trainings	***1***					1							**1**
	2 - 3			1	1		2	2					**6**
	4 - 5										1		**1**
	6 or greater							1			1		**2**
	I do not know				2								**2**
	Totals			**1**	**3**	**1**	**2**	**3**			**2**		**12**

Half of the agencies, fifty percent (50%), reported that between two and three trainings had been attended. Of the two agencies reporting *six or greater,* one had a reported agency size of five hundred plus (500+) and the other one-hundred-one (101) to one-hundred-fifty (150). Based on the pattern of distribution, no significant correlation could be found that links the agency size to the number of trainings.

Training – Lack of Training (Q11)

Question number eleven (Q11) was presented to determine the rationale, if any, for those agencies that had responded *No* to question nine (Q9). No scoring weight was assigned to this question. Of the fifteen responses, three anomalies were noted.

One respondent responded in the affirmative to question nine (Q9), and per the instructions should have skipped questions ten (Q10) and eleven (Q11). As a result, this respondent’s answer for question eleven (Q11) was disregarded for purposes of the count. For the second anomaly, a respondent answered question eleven (Q11) by providing two responses. While this was not an anticipated action, the data was found useful and was included. The third anomaly noted was a respondent that answered *NO* to question nine, but did not provide an answer to question eleven (Q11).

To clarify, thirteen respondents properly responded to question eleven (Q11). One respondent did not provide an answer. One respondent provided two responses. The statewide response totals and distributions for question eleven (Q11) are provided in the figure below (See Figure 9).

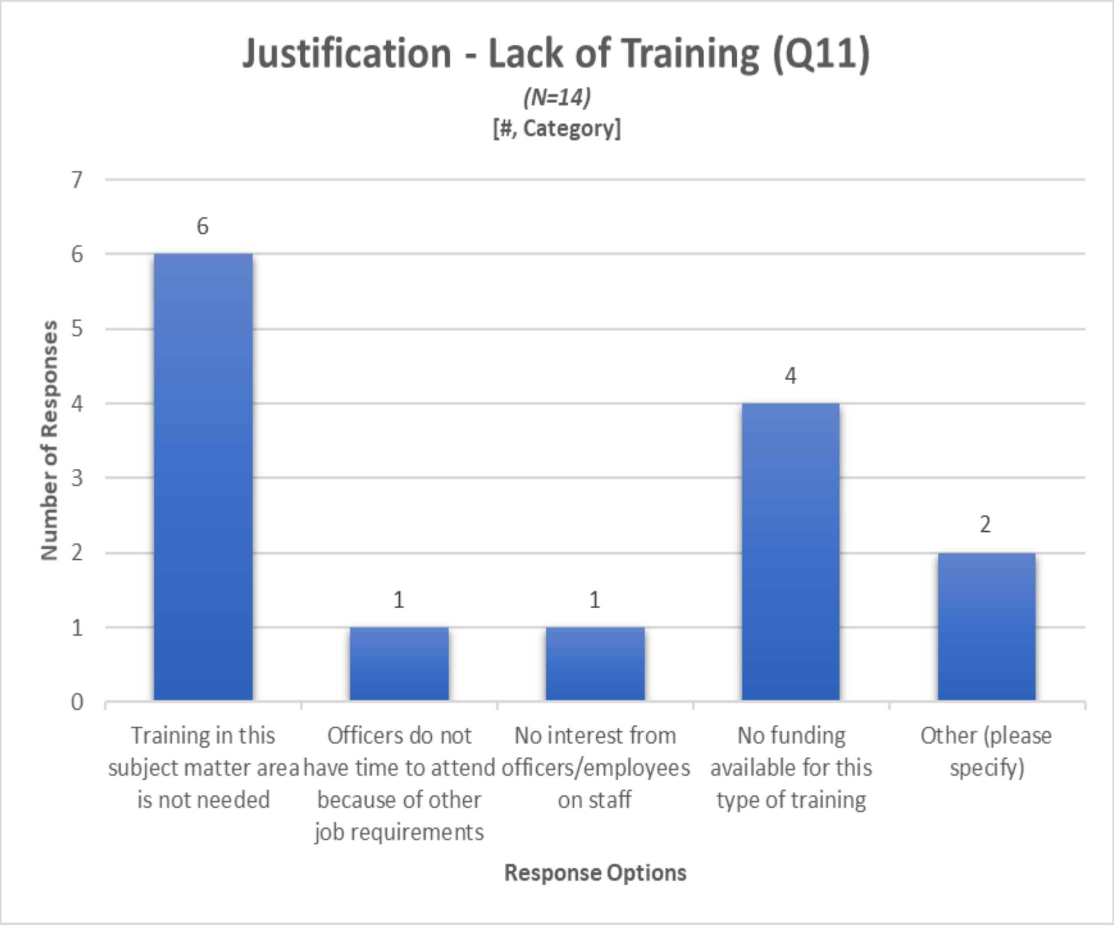


Figure 9. Number of Training Attended -Within Past 5 Years (Q11)

Of the responses, two respondents provided a written response. These responses were:

1. "These duties are performed by a county police agency."
2. "STATE POLICE handle all programs."

The number of agencies that have employees that have attended training and those that did not were quite similar. For those agencies that did not have employees that had attended training, the results suggested some of the principal driving factors were a *lack of need* or a *lack of funding*. It was interesting to note that forty-three percent (43%) of the responses indicated that *training in the subject matter area is not needed*.

In that regard, the results were very similar to Flory's (2016) findings. When these specific responses are compared in relation to the agency size, a general theme could not be immediately identified. This data is provided in the figure below for reference (See Figure 10).

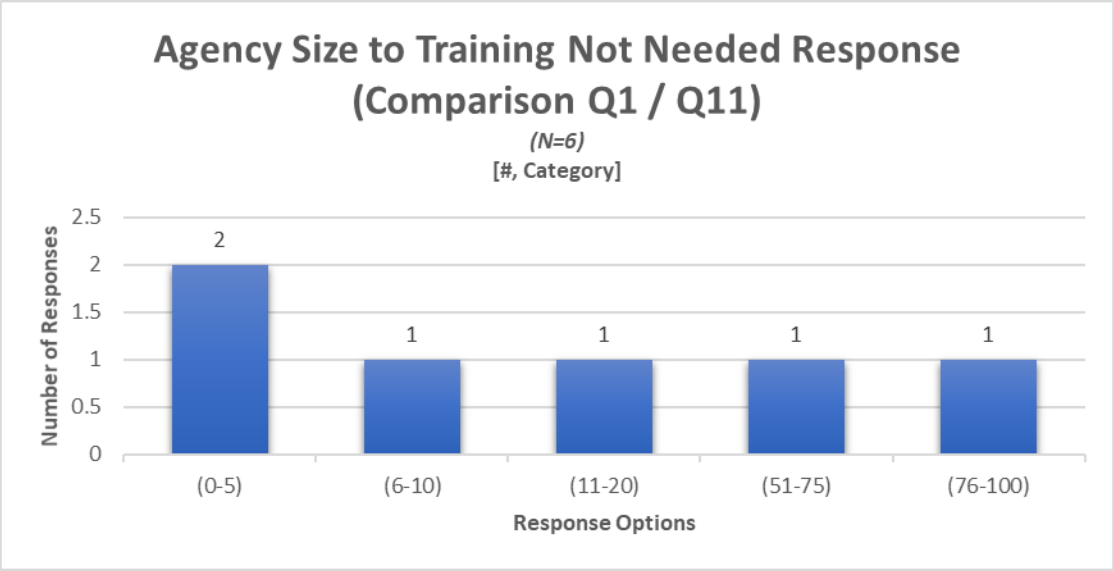


Figure 10. Agency Size to Training Not Needed Response (Comparison Q1 / Q11)

Distribution appears random; however, it was interesting that no agencies with a size above one-hundred (100+) reported this as a response. This could possibly suggest, with support of one of the provided written responses, that larger agencies may be consuming the work, thus from the respondent's perspective negating the need for this type of training.

Perceptions (Q12 – Q16 & Q18)

The following sections examine questions twelve (Q12) through question sixteen (Q16) and question 18 (Q18). These questions gathered data to determine agency perceptions on various topics. These topics included perceived investigative ability, the ability of local prosecuting attorneys, the ability of local judges, the ability of local juries, perceived resources, and perceived ability of staff.

Perceived Ability – Investigative (Q12)

Question twelve (Q12) was presented in order to solicit each agency's self-reported perceived ability to effectively investigate a case involving digital evidence. The scoring weights were: point-zero-two-five (.025) for a response of *Very High*; point-zero-two (.02) for a response of *High*; point-zero-one-five (.015) for a response of *Medium*; point-zero-one (.01) for a response of *Low*; point-zero-zero-five (.005) for a response of *Very Low*; and zero

(0) for a response of *Prefer not to answer*. Thirty respondents provided answers to this question (Q12). The results are presented in the figure below (See Figure 11).

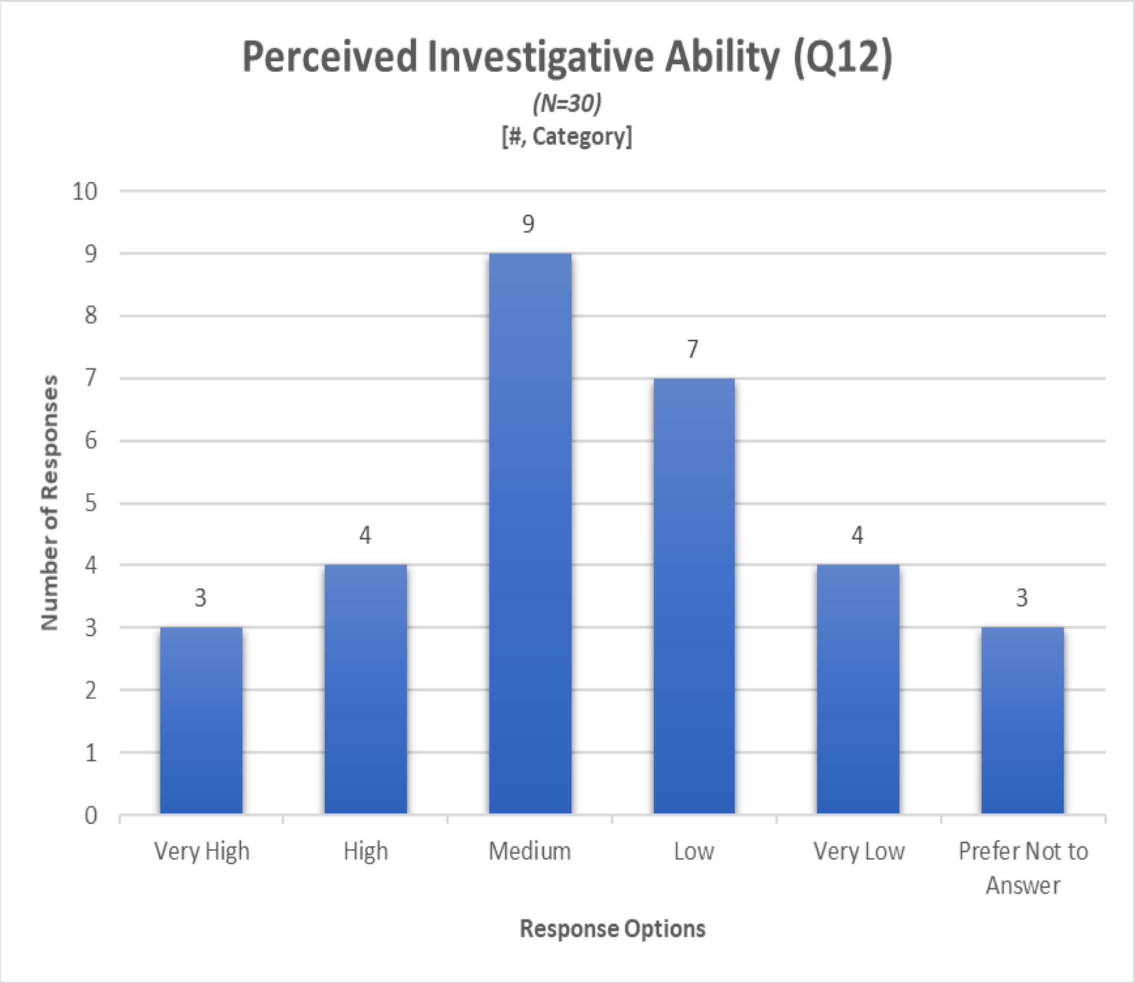


Figure 11. Perceived Investigative Ability (Comparison Q12)

To better understand the relevance of these values, it must be examined in the context of the associated digital forensic readiness scores. Based on the nature of the question, one could speculate that the average values of corresponding digital forensic readiness scores, as spread across the categories, would decrease. Average values that did not decrease moving down the spectrum would warrant further investigation and could be an indicator of either errors, bias, or a misinterpretation of the question (Q12).

In this study, the average values did, in fact, decrease as expected. The sorted scores and averages are presented in the table below (See Table 9)

Table 9. Perceived Ability to Readiness Scores (Q12)

Perceived Ability to Readiness Scores (Q12)						
	Very High	***High***	***Medium***	***Low***	***Very Low***	***Prefer Not to Answer***
Readiness Scores	0.998	0.955	0.867	0.77	0.06	0.55
	0.915	0.685	0.64	0.57	0.075	0.545
	0.63	0.33	0.585	0.525	0.065	0.51
		0.08	0.58	0.065	0.055	
			0.58	0.05		
			0.575	0.045		
			0.38	0.04		
			0.165			
			0.12			
Average	0.847667	0.5125	0.499111	0.295	0.06375	0.535
Highest	0.998	0.955	0.867	0.77	0.06	0.55
Lowest	0.63	0.08	0.12	0.04	0.055	0.51

While the findings were rather consistent, one anomaly was noted in the *High* category with the lowest score coming in at point-zero-eight (.08). A review of this respondent's data revealed that while the agency ranked their ability as high, their other responses noted a total dependence on outside assistance from "*a combined investigative unit.*" Since this is a perception-based question, there may be other influential factors. These factors fall outside the scope of this study. This particular respondent's score was not modified or excluded; however, this does suggest clarity may be warranted in future iterations using this same survey instrument. Furthermore, it was noted that the value assigned to this question and its categories are likely appropriate as the modifier had little impact over the total score.

Perceived Ability – Prosecution (Q13)

Question thirteen (Q13) was presented in order to solicit each agency's perceived ability of their "local prosecuting attorney's office to present digital evidence at a hearing or a trial" (Flory, 2016). The scoring weights were: point-zero-two-five (.025) for a response of *Extremely Effective*; point-zero-two (.02) for a response of *Moderately Effective; point-zero-one-five (.015)* for a response of *Effective* (.015); point-zero-one (.01) for a response of

Somewhat Effective (.01); point-zero-zero-five (.005) for a response of *Not Effective* (.005); and zero (0) for a response of *Prefer not to answer* (0). Thirty respondents provided a response to this question. No anomalies were noted. The results are presented in the figure below (See Figure 12).

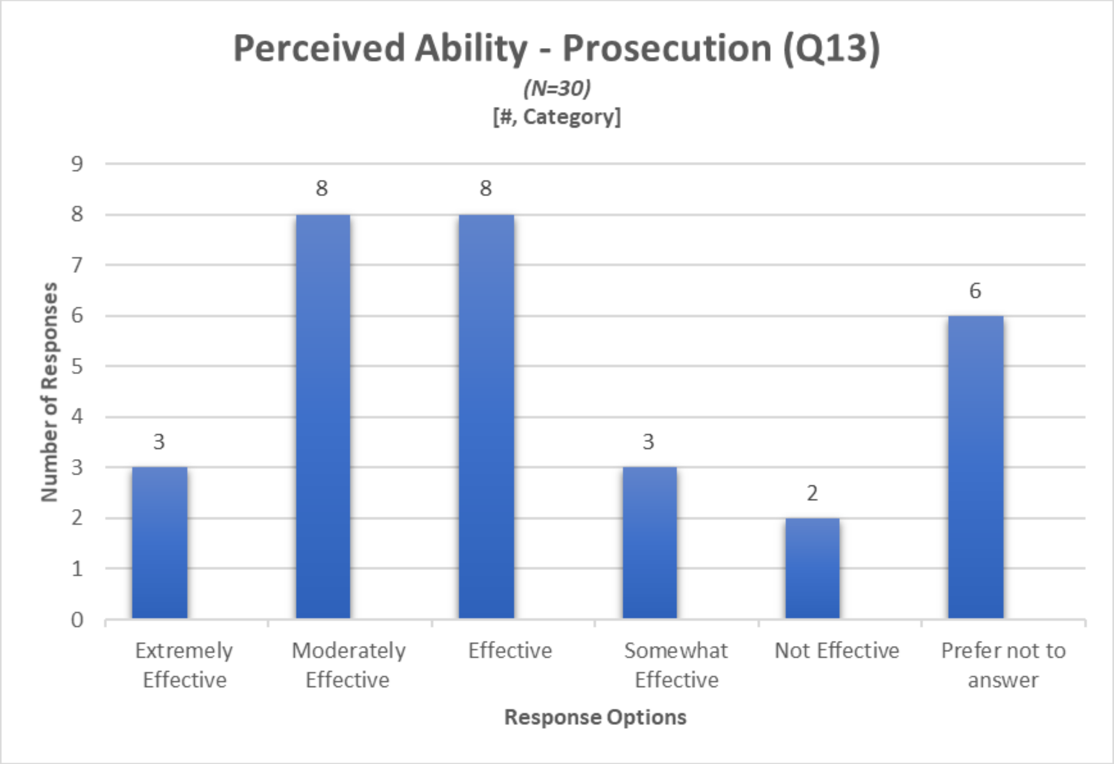


Figure 12. Perceived Ability – Prosecution (Q13)

Based on Flory's (2016) study, the perceptions of local prosecuting attorney's offices are higher in Maryland. Flory (2016) reported that fifty-four percent (54%) rated their prosecuting attorney's offices as "*least effective.*" This was interesting and may warrant further investigation.

Perceived Ability – Local Judges (Q14)

Question fourteen (Q14) was presented in order to solicit each agency's perceived ability of their "local judges to understand digital evidence and its admissibility at trial" (Flory, 2016). effectively investigate a case involving digital evidence. The scoring weights were: point-zero-two-five (.025) for a response of *Very High*; point-zero-two (.02) for a response of *High*; point-zero-one-five (.015) for a response of *Medium*; point-zero-one (.01) for a response of *Low*; point-zero-zero-five (.005) for a response of *Very Low*; and zero (0) for a response of *Prefer not to answer* (0). Thirty respondents provided a response to this question. No anomalies were noted. The results are presented in the figure below (See Figure 13).

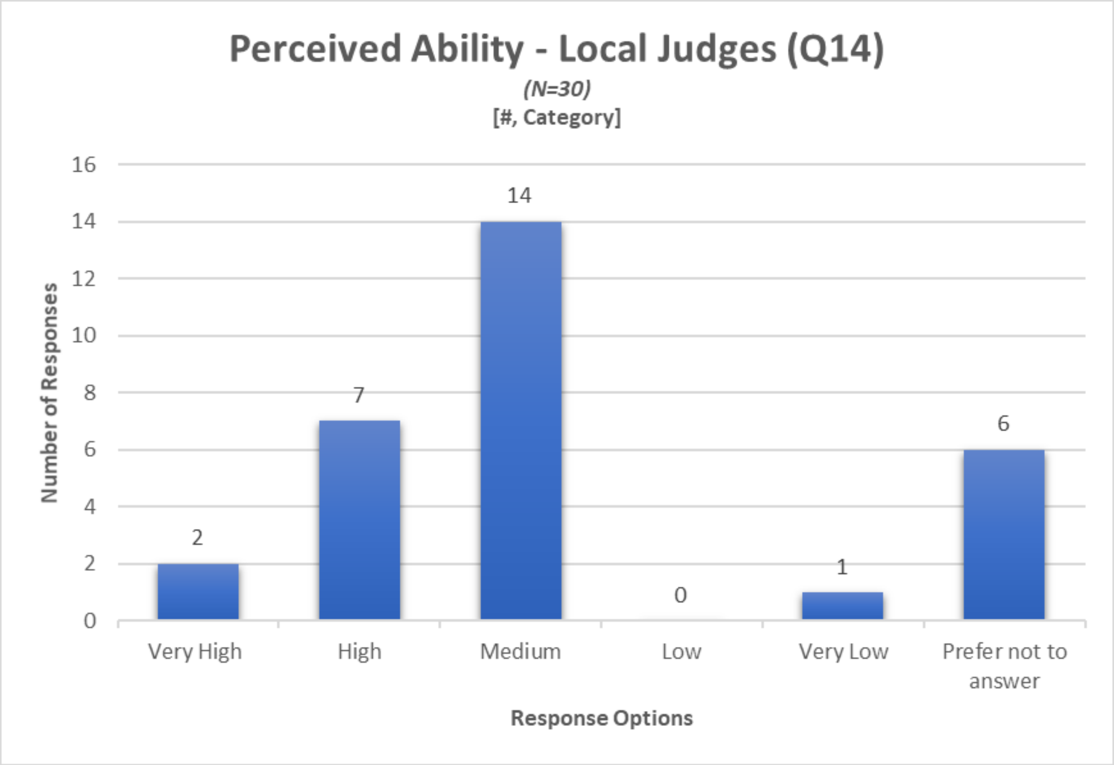


Figure 13. Perceived Ability – Local Judges (Q14)

As can be seen, about seventy-seven percent (77%) of respondents ranked their local judges' ability at *medium* or higher. While concerning, since this is a perception-based question, the locality of the agency that provided an answer of *very-low* should be examined for possible systemic issues.

Perceived Ability – Juries (Q15)

Question fifteen (Q15) was presented in order to solicit each agency's perceived ability of their "local juries to understand digital evidence when it is presented at trial" (Flory, 2016). The scoring weights were: point-zero-two-five (.025) for a response of *Very High*; point-zero-two (.02) for a response of *High*; point-zero-one-five (.015) for a response of *Medium*; point-zero-one (.01) for a response of *Low*; point-zero-zero-five (.005) for a response of *Very Low*; and zero (0) for a response of *Prefer not to answer*. Thirty respondents provided a response to this question. No anomalies were noted. The results are presented in the figure below (See Figure 14).

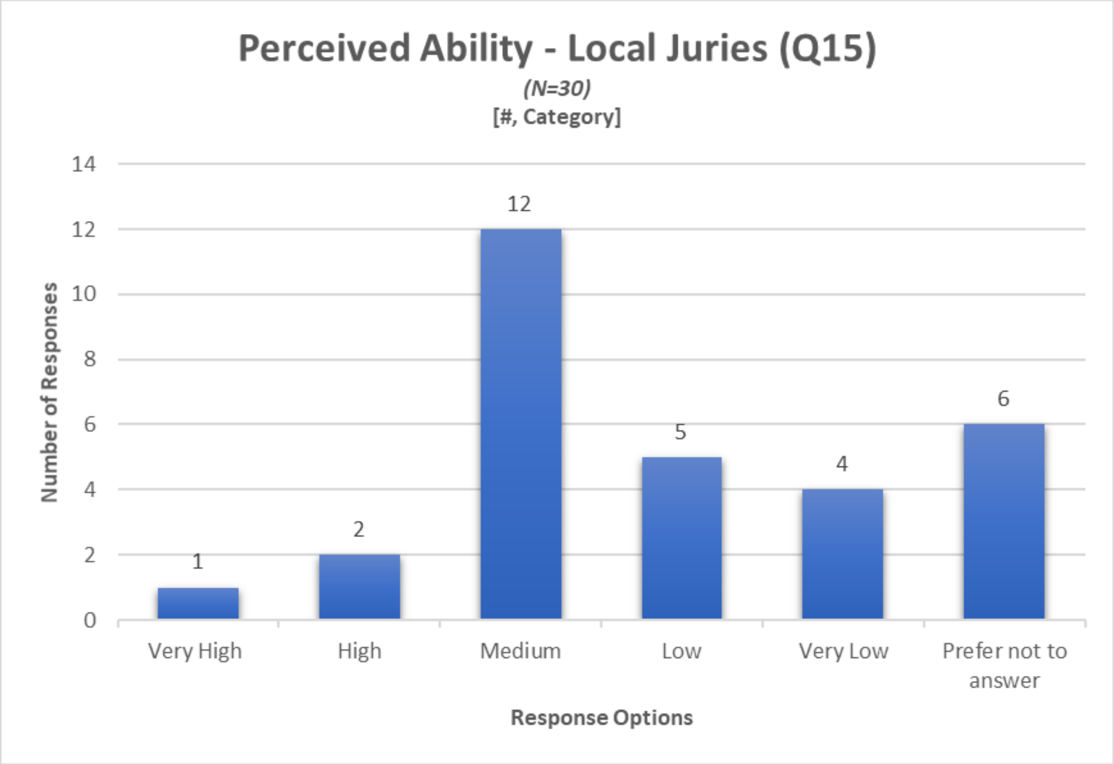


Figure 14. Perceived Ability – Local Juries (Q15)

Forty-percent (40%) ranked their local juries' ability as *medium*. Overall, without consideration for the responses of *prefer not to answer*, agencies tended to rank their local juries' ability less favorably than that of their local prosecuting attorney's offices or local judges. While outside the scope of this research, this raises the question of why? One way to examine this would be to explore the conviction rates and or case outcomes where digital evidence was presented at trial.

Perceived – Resources (Q16)

Question sixteen (Q16) was presented to determine if the agency believed they have "adequate resources to effectively conduct an investigation of a crime involving digital evidence" (Flory, 2016). The scoring weight was point-zero-five (.05) for an affirmative answer, and zero (0) for a response of *No* or *I do not know*. Thirty respondents provided a response to this question (Q16). Several anomalies were noted.

Five respondents required manual review for question number sixteen (Q16). Each of these respondents provided a response of *other* and provided a comment. These responses are included below:

1. "[N]ot primary law enforcement in our county, other agency handles criminal investigations. Our agency would defer to primary agency."
2. "Training and experience - yes. Manpower - NO. Our forensic expert splits his time between digital forensic and general investigations."
3. "Yes, we rely on local sheriff's office for in depth investigations."
4. "Do not need an expert"
5. "With assistance from a partner agency"

These responses suggested that the essence of the question (Q16) may not have been clear. The intent of question (Q16) was to determine internal resources and capabilities without considering outside resources. After careful consideration of the responses, it was determined that none of the responses satisfied the criteria. As such, each was assigned a scoring value of zero (0) for this score modifier. The distribution of answers is presented in the figure below (See Figure 15).

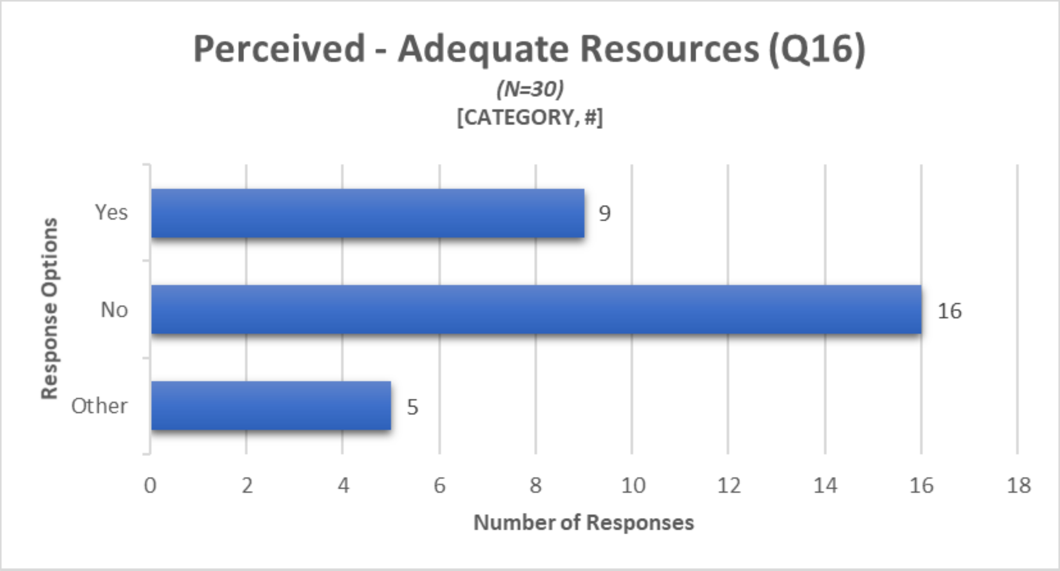


Figure 15. Perceived – Adequate Resources (Q16)

About fifty-four percent (54%) responded with an answer of *No.* If the responses of *other* are considered as a response of *No*, then the percentage value jumps to seventy percent (70%). This is very high and strongly puts into question each agency's ability to support cases involving digital evidence.

Perceived Ability - Staff (Q18)

Question eighteen (Q18) was presented in order to solicit each agency's perceived ability of its staff to identify, collect, and preserve digital evidence. The scoring weights were: point-zero-two-five (.025) for a response of *Very Good*; point-zero-two (.02) for a response of *Good*; point-zero-one-five (.015) for a response of *Fair*; point-zero-one (.01) for a response of *Poor*; point-zero-zero-five (.005) for a response of *Very Poor*; and zero (0) for a response of *Prefer not to answer*. Thirty respondents provided a response to this question. No anomalies were noted. The results are presented in the figure below (See Figure 16).

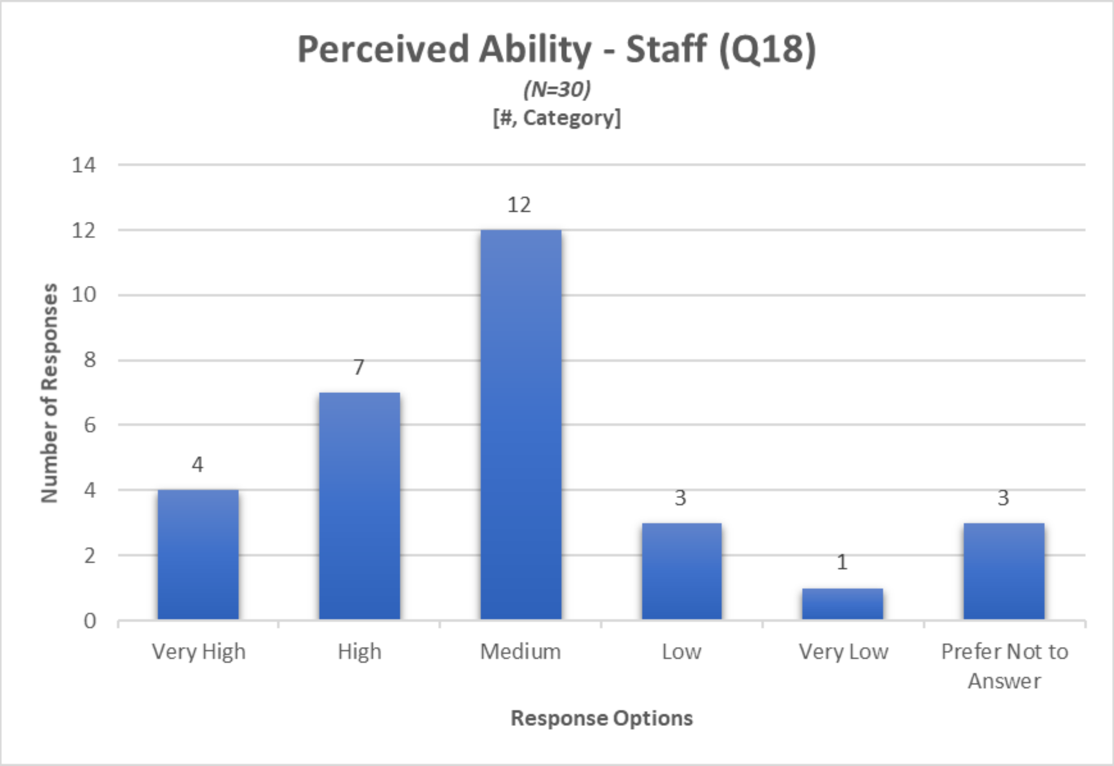


Figure 16. Perceived Ability – Staff (Q18)

About seventy-seven percent (77%) ranked their staff at *medium* or higher. This was in line with Flory's (2016) study in Indiana, where sixty-two percent (62%) of agencies ranked their ability at *medium* or higher. This finding suggests that there may be self-ranking bias. To solicit more useful data, this question would likely have benefited from a revision or excluded for scoring.

Standard Operating Procedure (Q19)

Question nineteen (Q19) was presented to determine if the agency had a "defined standard operating procedure regarding the identification, preservation, and collection of digital evidence" (Flory, 2016). The scoring weight was point-five (.5) for an affirmative answer, and zero (0) for a response of *No,* and a variable amount for a response of *other.* Thirty respondents provided a response to this question. No anomalies were noted. The results are presented in the figure below (See Figure 17).

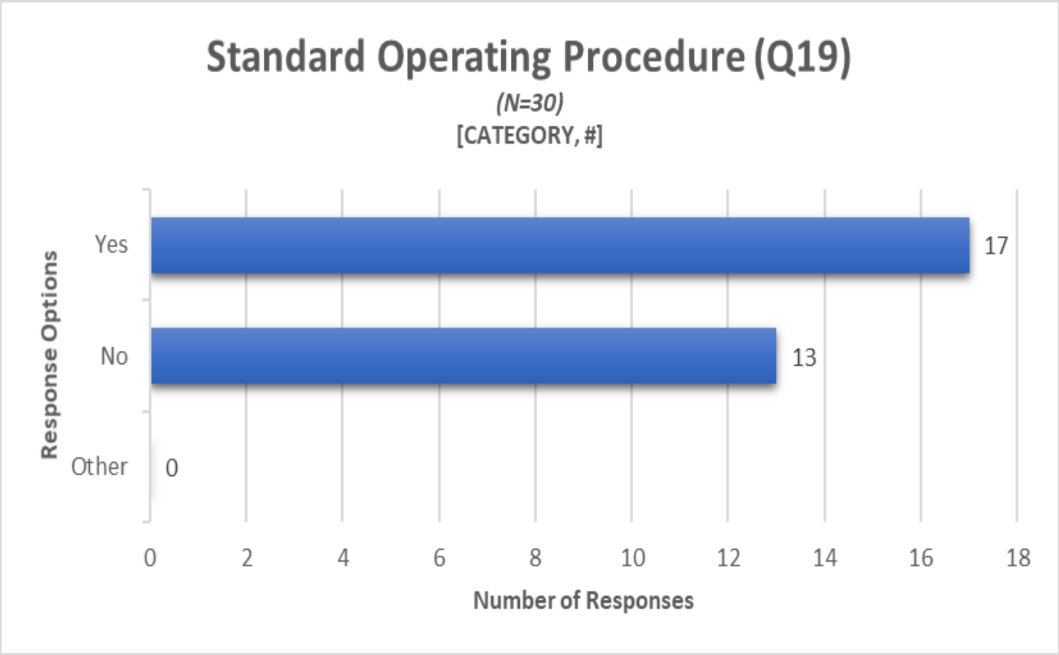


Figure 17. Standard Operating Procedure (Q19)

About fifty-seven percent (57%) of respondents indicated they have a standard operating procedure in place. This speaks directly to the readiness of an agency as policy and procedure are the foundation of the digital forensic process. Policy sharing may assist agencies in increasing the affirmative counts and, in turn, significantly increase the readiness scores across the state. This was considered a significant finding during this study, and future research should be geared towards finding a method to increase the likelihood of policy sharing.

Cloud\IoT (Q20)

Question twenty (Q20) was presented to determine if the agency had concerns about its "ability to collect digital evidence from the cloud or the internet of things" (Flory, 2016). A scoring weight was not assigned for this topic as research is still ongoing to determine how to best address this topic within the community. There were thirty responses to this question. One respondent provided a written response, which was reviewed. No anomalies were detected. This data can be found in the figure below (See Figure 18).

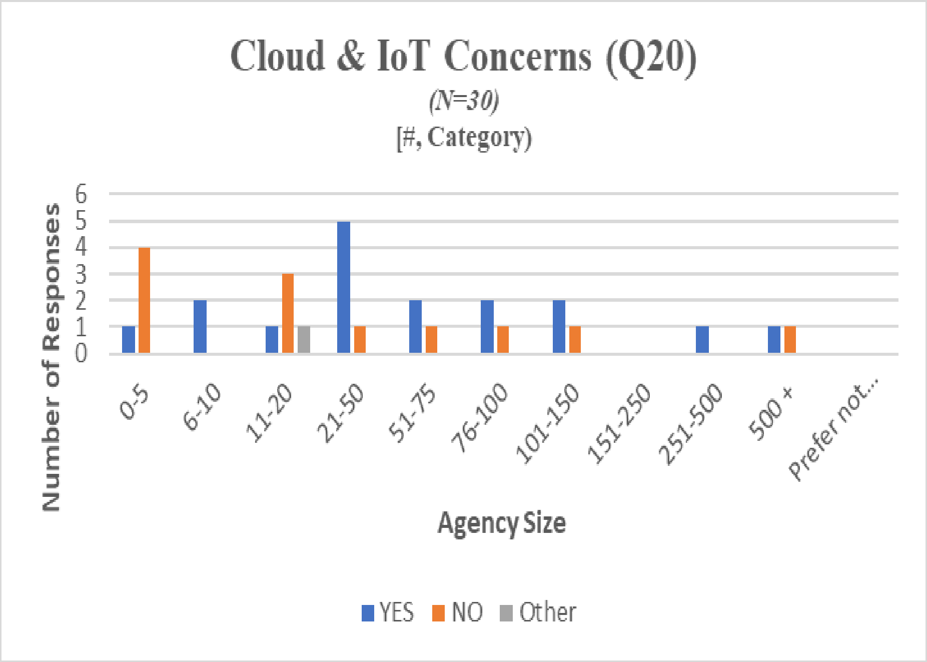


Figure 18. Cloud & IoT Concerns (Q20)

The responses to this question (Q20) are a good indicator of how law enforcement is keeping pace with advancements in technology. To add additional value to the body of knowledge, this data is being presented in conjunction with the agency sizes (See Figure 18). It was interesting to note that four of the five agencies reporting of size zero to five (0 – 5) were not concerned with these issues. Based on the data, agencies of size twenty-one to fifty (21 – 50) exhibited the most concern. For the two largest agencies, concerns were split. While outside the scope of this research, future research should determine why these differences exist and ways to increase each agencies ability to deal with emerging technologies. The data provides a baseline to narrow the scope of such an effort.

Section Summary (RQ1)

After careful review of all relevant questions, each respondent's digital forensic readiness score was calculated. The following table represents each respondent and their corresponding digital forensic readiness scores (See Table 10).

Table 10. Digital Forensic Readiness Scores

Digital Forensic Readiness Scores ***(N=30)***					
0.998	0.685	0.58	0.525	0.12	0.06
0.955	0.64	0.575	0.51	0.08	0.055
0.915	0.63	0.57	0.38	0.075	0.05
0.867	0.585	0.55	0.33	0.065	0.045
0.77	0.58	0.545	0.165	0.065	0.04

The scores, as presented in Table 10, are sorted from highest to lowest. It was found that the average for these scores is point-four-three-three-six (.4336) with a median value of point-five-three-five (.535). About fifty-seven percent (57%) were assigned a score greater than point-five (.5). With this study being the first of its kind, data does not currently exist for comparative purposes. The data presented here is being provided here for context and as a baseline for possible future research.

Proximity Relationships (RQ2 & HP1)

Research question two (RQ2) sought to determine if an agency's proximity to or availably of external resources influence its internal digital forensics posture. It was initially hypothesized (HP1) that law enforcement agencies within the state of Maryland that are within a twenty-mile radius of the two primary central *hubs*, Baltimore, MD, and Washington D.C., will exhibit a more mature digital forensic readiness posture. This was found *not* to be true. This section presents the results and findings.

For this analysis, twenty-six of the thirty respondents were considered and included in the dataset. Four of the thirty respondents had removed the page that contained the agency's unique identification code (UIC). The removal of this page made it impossible to determine the originating agency. Since the location of the agency was critical for this portion of the analysis and plotting purposes, these four respondents were excluded. Having identified the exclusions, it was necessary to then identify agencies that fell within the twenty-mile radius of the two hubs. The radial map, created using Google Earth, used for this analysis is presented below (See Figure 19).

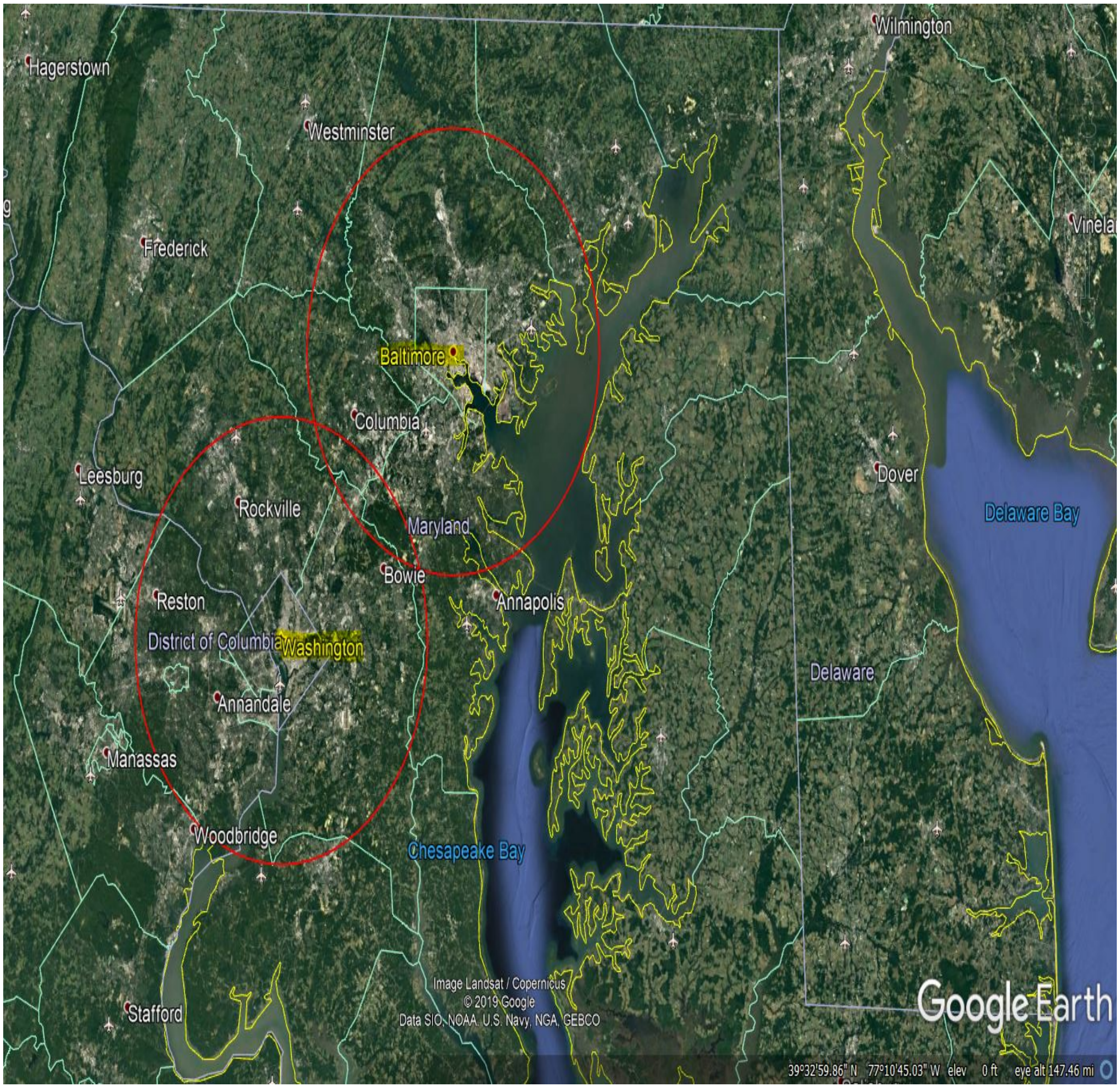


Figure 19. Proximity Map of Maryland (Datas SIO et al., 2018)

It was found that three agencies fell within the twenty-mile radius of Baltimore, MD. The scores from these agencies ranged from point-nine-nine-eight (.998) to point zero-seven-five (.075). The distribution of the twenty-six respondents by distance from Baltimore, MD, is presented in the figure below (See Figure 20).

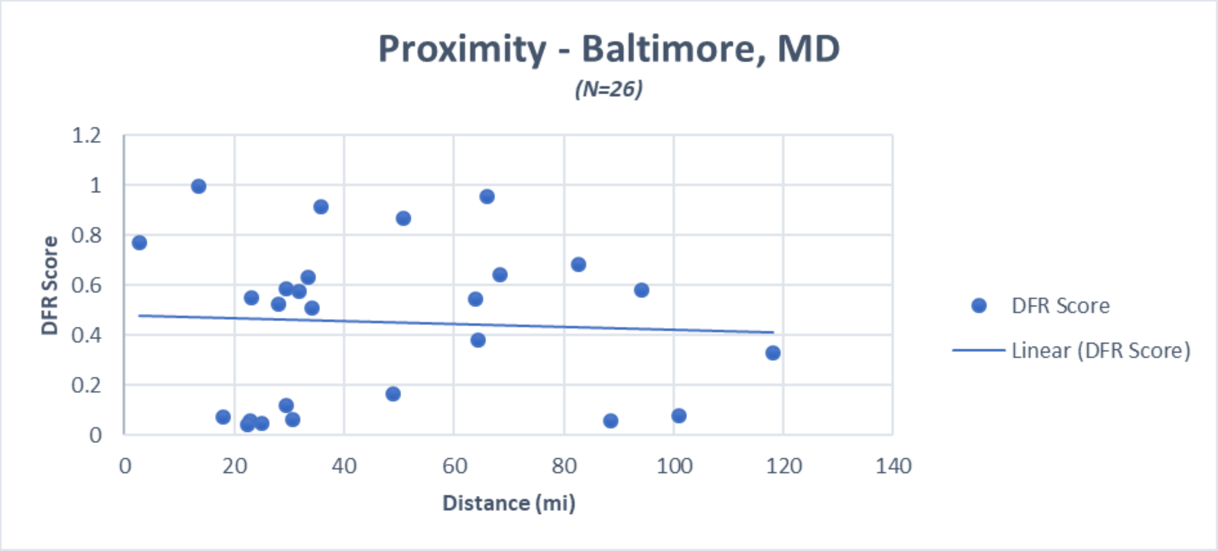


Figure 20. Proximity – Baltimore, MD

As can be seen, there is no discernable relationship between the digital forensic readiness scores and the distance to Baltimore, MD. Despite this, it is interesting to note that the agency with the highest score of the twenty-six agencies examined did fall within a twenty-mile radius to Baltimore, MD. Similar results were seen when examining the dataset in relation to Washington, DC. This data can be found in the figure below (See Figure 21).

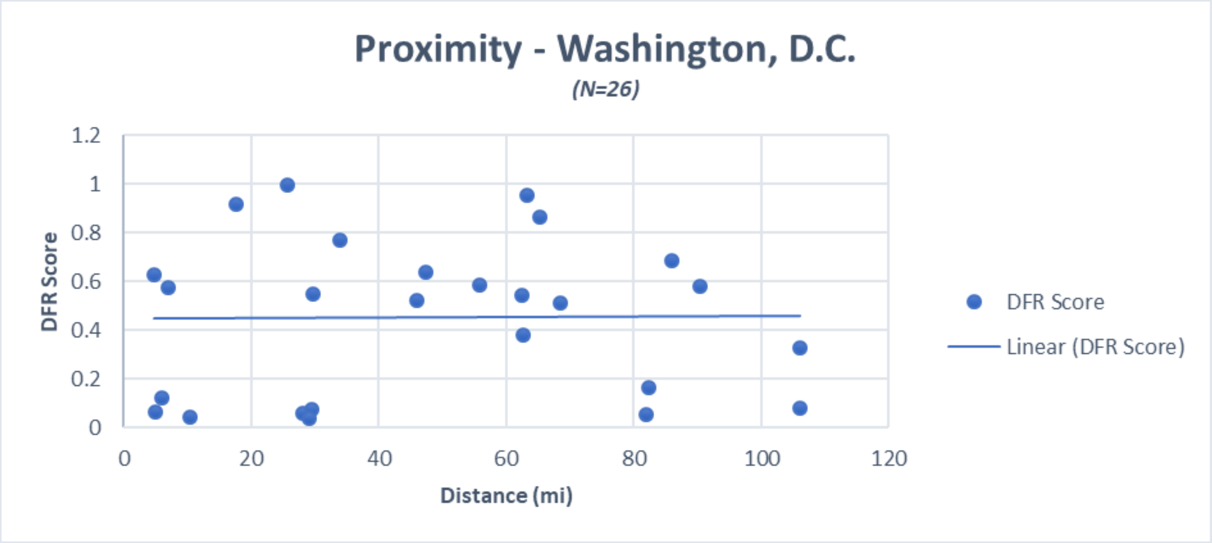


Figure 21. Proximity – Washington, D.C.

It was found that six agencies fell within the twenty-mile radius of Washington, DC. The scores for these agencies ranged from point-nine-one-five (.915) to point-zero-four-five (.045). The agency with the third-highest score, point-nine-one-five (.915), fell within the twenty-mile radius of Washington, DC. Again, no visible relationship can be identified. Next, we examine both sets combined. This data is presented in the figure below (See Figure 22).

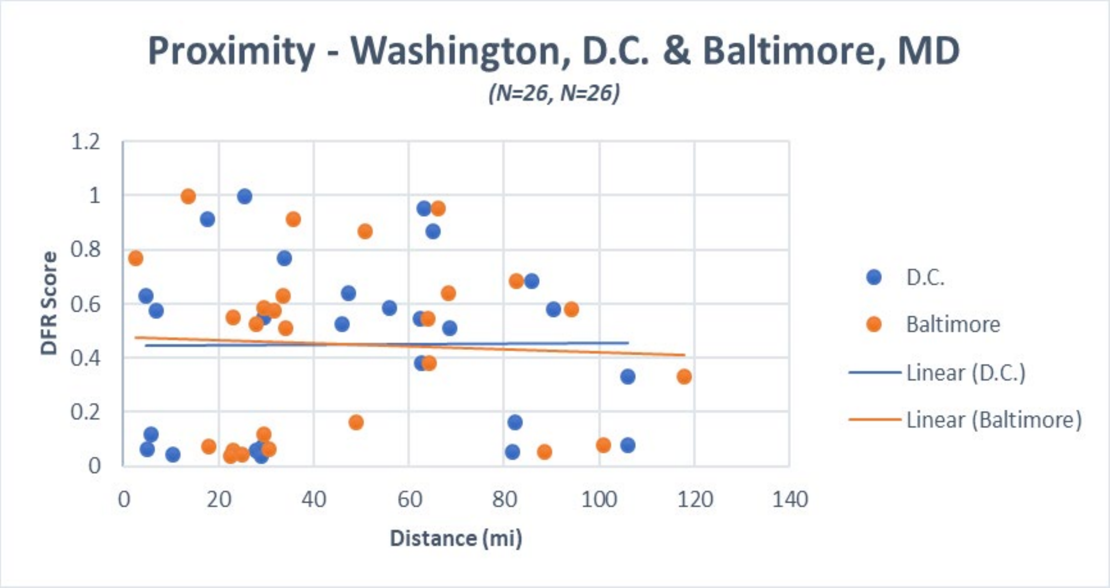


Figure 22. Proximity – Washington, D.C. & Baltimore, MD

Of the twenty-six agencies, none fell within the intersection point of the two hubs. Based on the data as gathered and presented, it can be stated that no proximity relationship exists. What this does seem to suggest is that agencies appear to operate independently and in a localized fashion.

Analysis of Backlogs (RQ3)

Research question three (RQ3) sought to determine if an agency's internal digital forensic readiness posture had an impact on the number of internal backlogs of digital forensic evidence. It was hypothesized (HP2) that all agencies, regardless of their distance between the *hubs,* will exhibit similar digital evidence backlogs when viewed in relation to the populations of the county or municipality in which the agency is located. To gather data to examine these issues, two questions (Q21 & Q22) were added to the original survey instrument. Each question and the results will now be examined.

Existing Backlogs (Q21)

Question twenty-one (Q21) specifically sought to solicit a backlog status. No score weight was assigned to the response. Thirty respondents responded to question twenty-one (Q21). No anomalies were encountered for question twenty-one (Q21). The data gathered can be found in the figure below (See Figure 23).

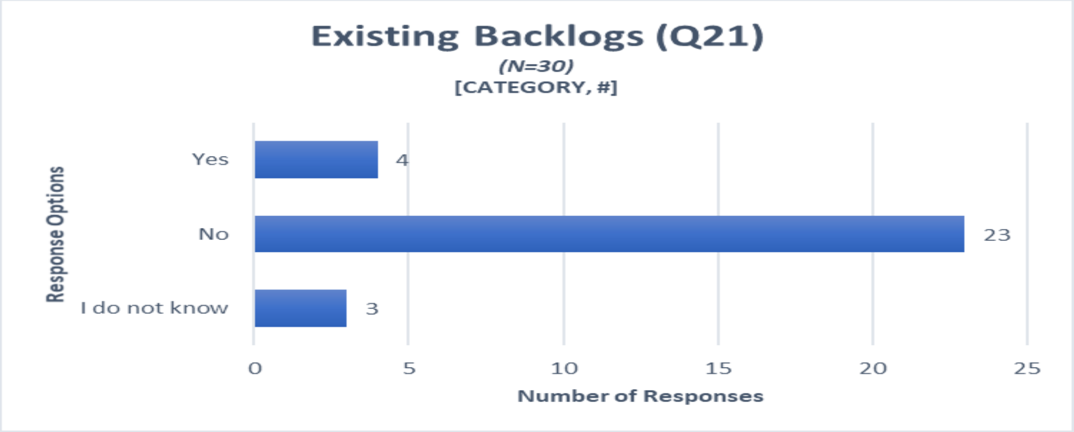


Figure 23. Existing Backlogs

About seventy-seven percent (77%) of the respondents indicated that no backlog existed at the time the survey was taken. This figure was surprising but could be a good indicator that agencies have processes in place to prevent backlogs. Based on the results of question five (Q5), it was noted that this might be the result of case outsourcing. The results from question five (Q5) are presented below for considerations (See Figure 24).

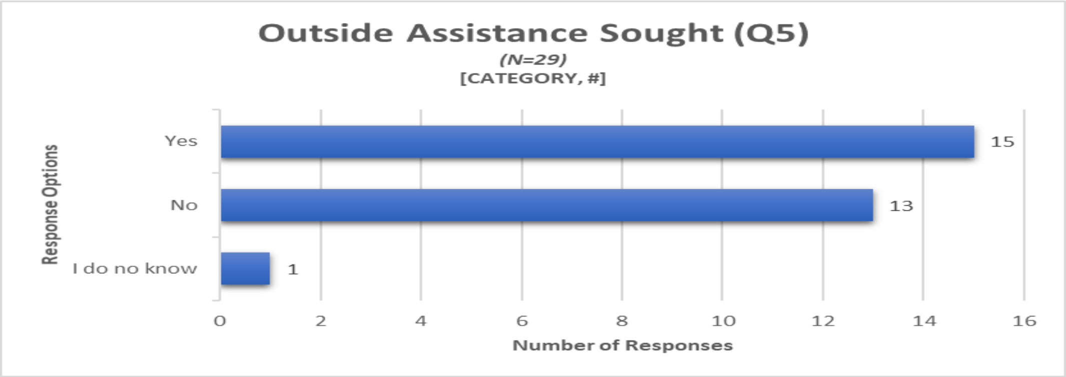


Figure 24. Outside Assistance Sought (Q5)

It was found that twenty-nine respondents provided an answer to question five (Q5). No scoring weight was assigned to this question (Q5). It was noted that about fifty-two percent (52%) of the respondents sought outside assistance to process digital forensic evidence. In future research, this data could be cross-correlated to determine the significance, if any, of outsourcing in regards to backlogs. Having reviewed this data, it was then possible to analyze the data gathered for question twenty-two (Q22).

Backlog Counts (Q22)

Question twenty-two (Q22) sought to identify the number of cases backlogged for those answering in the affirmative to question twenty-one (Q21). No score weight was assigned to the response. Ten respondents provided responses to question twenty-two (Q22). Several anomalies were detected. These anomalies will now be presented.

It was found that five of the respondents that had answered *No* to question twenty-one (Q21) had provided an answer of *other* for question twenty-two (Q22). These answers were in error. After a manual review of these answers, it was determined that the values were either reported as zero (0) or provided other details not relevant to the question. As a result, these counts were subsequently excluded from the analysis of question twenty-two (Q22). In addition, one respondent answered *I do not know* to question twenty-one (Q21), but supplied a response of *two to three* (2-3) for question twenty-two (Q22). This response was also excluded. The corrected results for question twenty-two (Q22) are presented in the figure below (See Figure 25).

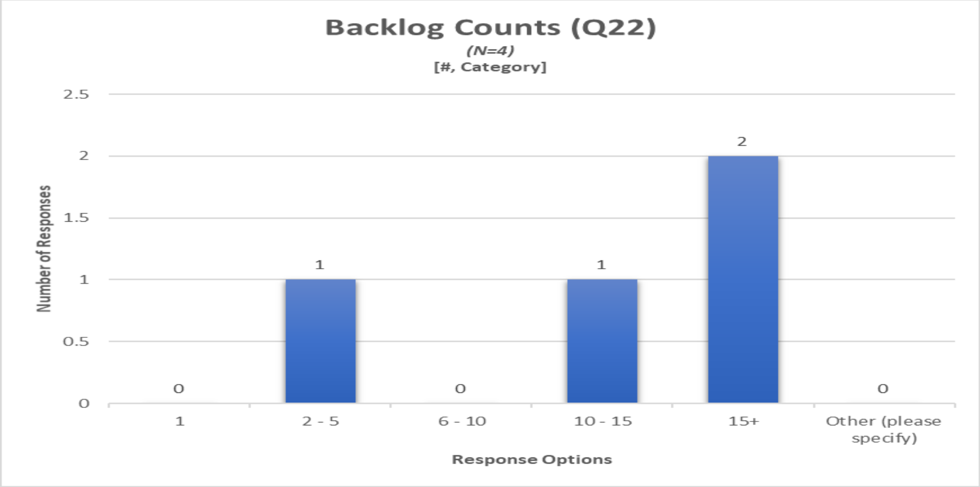


Figure 25. Backlog Counts (Q22)

Section Summary

It was found that four of the twenty-nine agencies reported having backlogs. Two of these agencies had backlogs of fifteen or more (15+). With the data gathered from question twenty-one (Q21) and question twenty-two (Q22), it would then be possible to perform a relational analysis of the data. This analysis is presented in the next section (See Backlogs – Relational Analysis).

Backlogs – Relational Analysis (HP2)

This section is being presented to examine any potential relationship between an agency's digital forensic readiness score and their backlogs. To accomplish this, digital forensic readiness scores of the four agencies that self-reported as having backlogs were compared. It was found that three of these agencies had digital forensic readiness scores that fell within the top five scores.

This was rather surprising; however, when examining comments from other respondents, it was noted that many agencies were deferring to partners and/or more equipped agencies. If this data is taken at face value, one could infer that a higher digital forensic readiness score would result in higher backlogs. Considering the limited dataset, it is not possible to determine any specific impact of readiness over backlogs. The table below contains the data considered during this analysis (See Table 11).

Table 11. Digital Forensic Readiness Scores / Backlogged Cases (Comparison)

Digital Forensic Readiness Score / Backlogged Cases (Comparison)		
Backlogged Cases (#)	***Scores***	***Count(s)***
1	0	0
2-5	(.867)	1
6-10	0	0
10-15	(.38)	1
15+	(.998), (.915)	2
Other	0	0

Backlogs / Distance Analysis

Hypothesis number two (HP2) stated that all agencies, regardless of their distance between the *hubs,* will exhibit similar digital evidence backlogs when viewed in relation to the populations of the county or municipality in which the agency is located. Again, the dataset was insufficient to support the hypothesis; however, the data is being presented here for consideration and as a potential baseline for future research (See Table 12).

Table 12. Backlog Distance Table

Backlog Distance Table					
Counties Reporting Backlogs	***Population (2010\yr.)***	***Backlog Count***	***DFR Score***	***Distance – Baltimore, MD (mi)***	***Distance – Washington, D.C. (mi)***
Anne Arundel	537,656	15+	0.998	13.6	25.6
Caroline	33,066	2-5	0.867	50.7	65.2
Montgomery	971,777	15+	0.915	35.7	17.6
Washington	147,430	10-15	0.38	64.3	62.6
Note: Population estimates provided by the state of Maryland (Maryland, n.d.)					

As can be seen, no correlation is apparent. From this particular dataset, it could be stated that agencies with an agency size of five-hundred (500) or greater are more likely to exhibit a backlog of cases of fifteen (15) or greater; however, this would be premature. Additional data needs to be gathered for comparative purposes. At the time of this research, a consolidated source for backlog data could not be located. Articles, such as the one by Watt's (2017), elude to backlogs, but this is not sufficient evidence to reach a scientific conclusion.

County-Level Data

This section contains a summary of county-level data. Due to the sensitive nature of some of the perception-based responses, steps have been taken to obfuscate the individual responding agencies. First, the number of agencies that responded by county will be presented along with count distributions and a statewide percentage ranking. Digital forensic readiness scores by county will then be presented. Finally, this data will be summarized.

Agencies from fourteen counties and one municipality responded. One response packet was received from an agency in Baltimore County, but this response was found to be incomplete and excluded from the count. This brought the total county inclusion count to thirteen and one municipality. The graphical representation of these results can be seen in the figure below (See Figure 26).

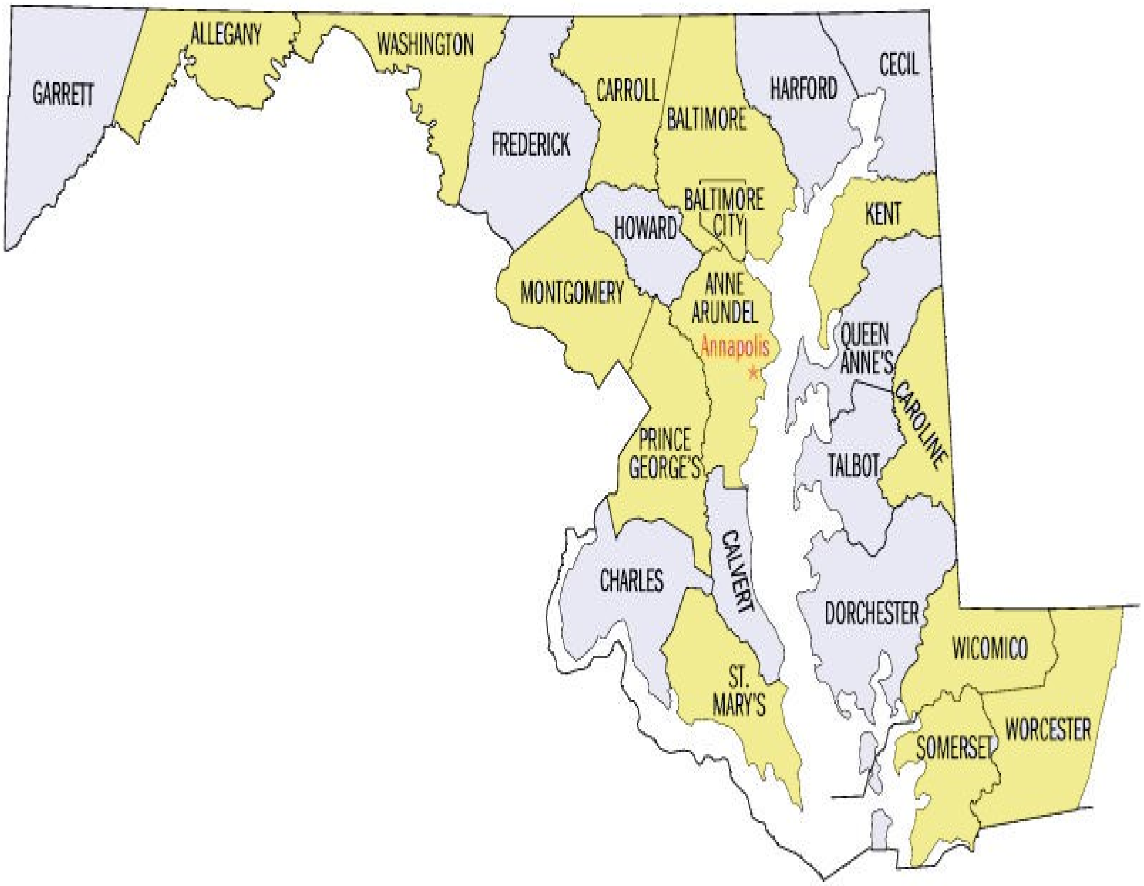


Figure 26. Responding Counties (Q22)

The counties highlighted in yellow in Figure 24 reflect counties where a response packet originated. Four additional responses were received; however, the unique identifier code had been removed from the returned survey. This made it impossible to determine the originating agency. The following table contains the response counts by county along with their percentage rank (See Table 13).

Table 13. County Counts

County Counts				
County	***Respondent Pool***	***Responded***	***Percentage***	***Response Rank (%)***
Unknown	-	4	-	-
Allegany	6	1	16.67%	8
Anne Arundel	8	5	62.50%	1
Baltimore City	13	1	7.69%	11
Baltimore County	6	1	16.67%	8
Calvert	1	0	0.00%	-
Caroline	5	1	20.00%	7
Carroll	7	1	14.29%	9
Cecil	6	2	33.33%	4
Charles	2	0	0.00%	-
Dorchester	3	0	0.00%	-
Fredrick	4	0	0.00%	-
Garrett	2	0	0.00%	-
Harford	4	0	0.00%	-
Howard	3	0	0.00%	-
Kent	3	1	33.33%	4
Montgomery	7	2	28.57%	5
Prince George's	29	4	13.79%	10
Queen Anne's	2	0	0.00%	-
Saint Mary	2	1	50.00%	3
Somerset	4	1	25.00%	6
Talbot	5	0	0.00%	
Washington	7	4	57.14%	2
Wicomico	5	1	20.00%	7
Worcester	7	1	14.29%	9
Totals	**141**	**30**	**21.28%**	

Each of the digital forensic readiness scores was presented at the state level in a previous section. This section now presents them at the county level. The following table contains the distribution of the digital forensic readiness scores by county (See Table 14).

Table 14. County-Level – DFR Scores

County-Level - DFR Scores	
County	***Scores***
Unknown	(.065), (.05), (.58), (.57)
Allegany	(.33)
Anne Arundel	(.06), (.075), (.998), (.55), (.04)
Baltimore City	(.77)
Caroline	(.867)
Carroll	(.525)
Cecil	(.165), (.51)
Kent	(.585)
Montgomery	(.915), (.63)
Prince George's	(.065), (.575), (.045), (.12)
Saint Mary	(.64)
Somerset	(.58)
Washington	(.955), (.545), (.38), (.055)
Wicomico	(.685)
Worcester	(.08)

Section Summary

This section focused on the data at the county level. To preserve the confidentiality of the agencies' responses, steps were taken to obfuscate the identity of each agency. The data presented here provide a working baseline for possible future research. For example, it may now be possible to measure and examine response rates within the state moving forward. This includes devising ways to increase the response rates, which was found to be problematic during this study.

Case Study Summary

This chapter presented the data gathered during this research. This data was analyzed in order to address the three research questions as well as to support or refute the hypotheses. The results were somewhat surprising. These results will not be summarized.

During a state-level analysis of the data, research question one (RQ1) was satisfied through the establishment of a digital forensic readiness score for each responding agency. It was found that around fifty-seven percent (57%) had digital forensic readiness scores greater than point-five (.5). With the establishment of the digital forensic readiness scores, it was then possible to examine research question two (RQ2)

Research question two (RQ2), along with hypothesis one (HP1), was realized by mapping each agency’s distance from the central hubs and examining the variations in relation to the assigned digital forensic readiness scores. It was found that no statistically significant trends exist to support hypothesis one (HP1). Furthermore, based on the data collected, it was determined that an agency's distance between the two hubs in this study did not influence the digital forensic readiness scores. After this analysis, data were examined to answer research question three (RQ3).

Research question three (RQ3), along with hypothesis two (HP2), was then examined using the collected datasets. Due to a low response rate, it was not possible to determine any significance between the digital forensic readiness scores and existing backlogs. In fact, it was noted that the data seemed to suggest that agencies with higher scores may be more likely to have backlogged cases. It was noted that several agencies provided responses that suggested a dependency on larger agencies, which could explain this. Like hypothesis one (HP1), there was not enough data to support hypothesis two (HP2).

Consistent with previous studies (Flory, 2016; Gogolin & Jones, 2010), the trend of low response rates from law enforcement agencies supporting this type of research made it difficult to establish any relationships of significant value. The data should not be discounted, though. This data, along with this research, fills a current gap that could be used to further examine Maryland, other states, or the entire region.

CHAPTER 5

CONCLUSIONS

This chapter (CH5) has been prepared to provide the reader with a summarized version of the work detailed in Chapters one (CH1) through Chapter four (CH4). First, the significance and purpose of this research will be presented. The methods used to pursue this work will then be detailed. Significant findings will then be examined. This will be followed by the study's limitations and issues encountered. The direction of future work related to this research will also be covered. Finally, this chapter (CH5) will be summarized along with a final summation of the work in its entirety.

Significance of the Research

This research is significant to the field as there has been a noted lack of this type of localized data collected within the United States (Flory, 2016; Gogolin & Jones, 2010; Harichandran et al., 2016). This type of data, along with this type of analysis is necessary for identifying factors that may influence digital forensic readiness within the law enforcement community both locally and at large. These factors can then be used to derive metrics and establish baselines with the goal of decreasing digital evidentiary backlogs and increasing the chances of digital evidence being successfully used at trial. Furthermore, the data collected during this study, along with the establishment of digital forensic readiness scores, set the stage for comparative purposes that may assist in the standardization of the field.

As of February 8th, 2020, no study of this magnitude, exploring these concepts, has been performed using law enforcement agencies in the state of Maryland as the population. In fact, very few studies like this have been performed nationwide (Flory, 2016; Gogolin & Jones, 2010; Harichandran et al., 2016). The lack of research in this area has led to speculative prescriptions for localized problems that are not fully understood (Flory, 2016; Harichandran et al., 2016; Lillis et al., 2016).

During this study, it was found that several findings were very similar in nature to the study conducted by Flory (2016). This was interesting, as Indiana's demographics do not necessarily mirror those of Maryland. For example, the state of Indiana is larger in terms of both landmass and population (United States Census Bureau, 2010a, 2018a). In addition, it was also found that Indiana has more law enforcement agencies than Maryland (Flory, 2016). This suggested that factors such as population or resource availability may not be the primary drivers in the issues noted among the law enforcement community concerning the field of digital forensics.

With commonalities, like the ones explored in this study (See Chapter 4), trends began to emerge. It could be reasonably concluded based on this research and previous research, that commonality does indeed exist. The commonality of an issue can act as a precursor to change when proper solutions are devised and implemented. While this study never set out to incite specific change, it is believed that the results identified can provide a window for change.

Technology, however, is rapidly evolving, and with that evolution comes a haze that can cloud or muddy present findings. In order to help avoid cases like the one noted by Watts (2017), it is imperative to flood the body of knowledge with as much relevant and structured data as possible. This research accomplished this by providing data that can affect change if acted on in a timely manner.

Methods

This research was carefully planned and executed to ensure maximum coverage of the state and the topics considered. Previous research, specifically the studies by Flory (2016) and Gogolin and Jones (2010), provided a working model and baseline. To expand on the current body of knowledge in the most effective way possible, it was decided to use Flory's (2016) pre-validated survey instrument. This approach provided a method of validation and transformation. To ensure new knowledge would be gained, additional questions were added that explored previously unexplored areas. These new areas of exploration included the examination of readiness, proximity relationships, and backlogs. To focus this effort three research questions and two hypotheses were created. The research questions and hypothesis are as follows:

RQ1. What is the current digital forensic readiness posture of law enforcement agencies in the state of Maryland?

RQ2. Does an agency's proximity to or availably of external resources influence its internal digital forensics posture?

RQ3. What impact, if any, does an agency's internal digital forensic readiness posture have over any internal backlogs of digital forensics evidence?

The study also sought to support the following hypotheses:

HP1. Law enforcement agencies within the state of Maryland that are within a twenty-mile radius of the two primary central *hubs*, Baltimore, MD, and Washington D.C., will exhibit a more mature digital forensic readiness posture.

HP2. It is hypothesized that all agencies, regardless of their distance between the *hubs,* will exhibit similar digital evidence backlogs when viewed in relation to the populations of the county or municipality in which the agency is located.

The population, as was previously described (See Chapter 3), consisted solely of law enforcement agencies in the state of Maryland. Care was taken using freely available resources (Department of Public Saftey & Correctional Services, n.d.) to attempt to not only identify all agencies in the state but also to determine if the agencies indeed met the criteria of a law enforcement agency. Further vetting was performed to determine if agencies were sub-agencies or affiliates in order to avoid the duplication of data. This process resulted in a population of one-hundred-forty-one (141) agencies.

To contact these agencies, it was decided to utilize both a traditional mailed survey and an electronic survey. Respondents were afforded the opportunity to respond using either method. Of the one-hundred-forty-one (141) agencies, only thirty complete responses would be received. Twenty-seven responses would be received in paper form, and four would be received with the electronic collection method. One of the electronic responses was found to be incomplete and was excluded from the final dataset.

To ensure the confidentiality and integrity of the process, the researcher carefully devised a data security plan, which included using encryption and air-gaped machines. This process was reviewed and approved by the Dakota State University Institutional Review Board (DSU-IRB). To further enhance security and to promote trust in the process, the respondents were advised that county-level data would be obfuscated to protect the identity of each agency. The promotion of this trust is critical if future research is to be conducted.

Findings

As was noted in the previous section, this research was guided by three research questions and two hypotheses. These questions and hypotheses will be presented in order, along with the key findings from the research.

Research Question One (RQ1)

RQ1. What is the current digital forensic readiness posture of law enforcement agencies in the state of Maryland?

During the inception of this study, a scoring system was created that assigned a numeric value to specific questions contained in the survey. These questions addressed areas relevant to the concept of digital forensic readiness, as was noted in several significant works (Elyas et al., 2015; Flory, 2016; Gogolin & Jones, 2010; Harichandran et al., 2016). The totality of these scores would be referred to as the agency's digital forensic readiness score. Higher values would, in theory, represent a more mature state of digital forensic readiness.

Due to the subjective nature of some of the questions, it should be noted that it is possible that the responses reflected in the surveys may not always align with the agency or locality's true state. In other words, some questions introduce the possibility of self-reporting bias skewing the results either higher or lower. With no comparative dataset, it was decided to state the possibility of bias and explore the issue in future iterations.

To satisfy research question one (RQ1), scores would be tallied for each agency. Several anomalies were noted (See Chapter 4); however, careful review allowed for many of these anomalies to be resolved. It was found that several of the respondents either skipped questions or did not properly follow the instructions. In cases such as these, previous answers were explored to determine if sufficient details existed to correct the results. If it were not possible to determine the result, the response would be excluded from the dataset. For questions with weighted scores where the data could not be determined, the respondent would be assigned a value of zero for that particular question.

After each question was reviewed, the results were calculated (See Table 10). It was found that the average digital forensic readiness score was point-three-three-six (.4336) with a median score of point-five-three-five (.535). As was previously noted, this study was the first of its kind conducted within the state. As such, the scoring system and its accuracy have yet to be proven.

A comprehensive needs-based analysis of these results would likely provide a method to increase scores; however, this was considered outside the scope of this study. It should be noted, though, that Flory (2016), using a needs-based approach, identified several areas of need in Indiana that could cross-correlate to the findings in Maryland. For example, addressing these areas of need, such as having a defined standard operating procedure, would significantly increase scores and overall readiness. With that in mind, these metrics and this data could be used as a baseline in order to establish acceptable scores at the national, state, or county levels.

Enforcement of a set of minimum standards across the board, as derived from a needs-based analysis, could increase the effectiveness of each agency in regards to digital forensic readiness. This is purely speculative, though, as these findings, and findings of other researches, have yet to be fully tested in a controlled and localized way. The data gathered from this study now establishes a baseline, which, if acted on, provide a means to substantiate this claim by way of future iterations.

Future iterations of this study would likely yield fluctuations in the digital forensic readiness scores presented (See Chapter 4). The goal of these iterations would be to work towards a way to sustain or increase current scores. Based on this research, it is likely that this would prove challenging as agencies may find it difficult to keep pace with the increases in the levels, prevalence, and sophistication of cybercrime (Federal Bureau of Investigation, 2019; Vincze, 2016). In addition, there may be a trend towards the outsourcing of digital forensics cases (See Chapter 4).

Research Question Two (RQ2) & Hypothesis One (HP1)

RQ2. Does an agency's proximity to or availably of external resources influence its internal digital forensics posture?

To examine this question, the research would need to leverage the digital forensic readiness scores established when answering research question one (RQ1). The main objective of this question was to support proximity relationships, as was stated in the hypothesis one (HP1).

HP1. Law enforcement agencies within the state of Maryland that are within a 20-mile radius of the two primary central *hubs*, Baltimore, MD, and Washington D.C., will exhibit a more mature digital forensic readiness posture.

To clarify, a more mature digital forensics posture would be reflected as a higher digital forensic readiness score, as was calculated during the examination of RQ1. Once the agencies' scores were tabulated, it was necessary to determine the proximity between each agency and both hubs. This was accomplished by using Google Earth to plot the distances between the hubs. It must be noted that the distances to the hubs were approximate distances.

During an initial assessment, it was determined that no agency fell within the intersection zone of the two hubs. A total of nine agencies did fall within the twenty-mile radius of at least one of the hubs. A total of three agencies fell within the twenty-mile radius of Baltimore, MD. Of the nine, the remaining six fell within the twenty-mile radius of Washington, DC.

It was found that no relationship existed between an agency's digital forensic readiness score and its proximity to either of the hubs. To ensure the validity of the data, both hubs were looked at independently and then combined to identify statistical significance. The first independent data set examined the relationships using Baltimore, MD, as the primary hub (See Figure 20).

When examining the proximity relation to Baltimore, MD, it was determined that no discernable relationship was present. By examining the scatter plot (See Figure 20), it quickly becomes apparent that the distribution of scores as the distance increases or decreases is random. While pockets do exist, the goal was to determine the relationship from the hubs and not the causality of potential pockets within the data. While not statistically significant, it was interesting to note that the agency exhibiting the highest readiness score, point-nine-nine-eight (.998), fell within the 20-mile radius of Baltimore, MD. An examination of the same data with Washington, DC, as the hub, yielded similar results (See Figure 21).

Like the previous dataset, no correlation could be identified. Using the same scatter plot method, pockets were also noted; however, the pockets were not as highly concentrated. Again, the causality was outside the scope of this study, but something worth exploring with future research. To ensure that nothing was overlooked, the data would also be combined and interpreted (See Figure 22).

The examination of the aggregated data also revealed nothing of significant value. With no correlation observed in the previous analysis, it was determined that enough data existed to refute hypothesis one (HP1). As such, it could be stated that an agency's distance to central hubs in Maryland does not positively or negatively influence that agency's digital forensic readiness posture. This does not suggest that influence cannot occur. For example, increased resource sharing could possibly increase scores, but efficiency would also be a factor. In other words, this finding represents what is and not what could be.

Research Question Three (RQ3) & Hypothesis Two (HP2)

RQ3. What impact, if any, does an agency's internal digital forensic readiness posture have over any internal backlogs of digital forensics evidence?

Answering this question (RQ3) was dependent on the results of research questions one (RQ1) and two (RQ2). First, each agency needed an established digital forensic readiness score. These scores would be established earlier in the study (See Table 1). With the scores in place, it was then possible to proceed with determining the number of agencies that had outstanding backlogs. This was accomplished by first tallying the results of survey question twenty-one (Q21) followed by an examination of question twenty-two (Q22).

No anomalies were noted in the data reported for question twenty-one (Q21); however, anomalies were noted for question twenty-two (Q22). These anomalies would require manual correction and an adjustment of the counts for question twenty-two (Q22).

This data would then be combined along with the corresponding digital forensic readiness scores to identify relationships.

It should first be stated that the number of agencies reporting backlogs was significantly lower than anticipated. In fact, only four of the thirty agencies responding reported having a backlog. One thing that was noticed was that it appears that agencies with higher scores are more likely to have backlogs. A review of comments by agencies reporting not having a backlog suggested that reliance may exist on more capable organizations. Since a relationship could not be established, the next step was to determine if hypothesis number two (HP2) could be supported.

Hypotheses number two (HP2) sought to prove that all agencies, regardless of their distance between the *hubs,* will exhibit similar digital evidence backlogs when viewed in relation to the populations of the county or municipality in which the agency is located. Like hypothesis one (HP1), the dataset (See Table 12) was insufficient to support this hypothesis (HP2). In order to have been able to support hypothesis two (HP2), the ideal sample would need to consist of one agency from each county within the state. It might have been possible to determine s relationship without a response from each county if the population contained a significant amount of data diversity. This was just not the case with this study.

Findings summary

While neither of the hypotheses (HP1 & HP2) was supported, two of the three research questions were able to be addressed. Research question one (RQ1) generated a dataset that can be used as a baseline for both future research and process improvement. Research question two (RQ2) determined that hubs within the state do not have a negative or positive influence over digital forensic readiness postures. This is an advantageous finding as it suggests a possible lack of resource sharing or even an over-reliance on other agencies or outside resources. Outside of the research questions, additional useful information was and can be derived from the collected data.

For example, the responses relating to Cloud and IoT concerns was a good indicator of possible deficiencies within the state. These deficiencies may be the result of resource constraints, training gaps, or other issues yet to be identified. There is significantly more information that could be extracted from the current dataset; however, validation will not be possible without increased participation rates.

The lack of responses came as no surprise when considered in relation to previous studies (Flory, 2016; Gogolin & Jones, 2010). Data from future studies, of a similar nature, are likely to be sparse until existing data can be leveraged in a positive and visible way. Moving forwards, it will be necessary for researchers and law enforcement alike to work together to realize improvements in national, state, and localized digital forensic readiness postures. Until then, it is important to continue to gather data and build upon the body of knowledge.

Limitations

This research had several limiting factors. This section presents each of these limitations. First, the technical limitations will be presented. The limitations of the methodology will then be discussed.

Limitations - Technical

In regards to technical limitations, it determined early on that the study may suffer from a lack of responses using the electronic contact method. This assumption was based on the results of a study of a similar nature (Flory, 2016). It was determined, based on time constraints, that publicly promoting the survey in a fair on consistent manner was not feasible. As such, respondents would be receiving an unsolicited email originating from an unknown source. In a world of cyber-crime, it could be reasonably inferred that the emails were phishing attempts. This may partially explain the large number of unopened emails. While this was considered a limiting factor, efforts were made to offset this by sending a paper survey. To avoid this problem type of problem, with future iterations of this type of research, it is strongly encouraged that the researcher(s) attempt to contact the respondents prior to sending any form of survey.

Limitations - Methodology

During this research, it was found that the quantitative methodology may have limited the presentation and interpretation of the data. It was determined that many of the underlying factors, especially in regards to the perception-based questions, could not be fully explored using the quantitative methodology. An examination of the data collected may have been better served using a mixed-methods approach.

It must be understood, though, that a mixed-methods approach would not have added any value when answering the proposed research questions. Answering these questions required actual numeric data without much consideration of the rationale behind the responses. As such, the quantitative methodology was the proper choice. This does, however, leave the door open to a future iteration in which the data is reexamined using a different lens.

Research Challenges

This research endeavor was not without challenges. From the inception, through to completion, a number of issues evolved during the process that impeded progress. This section details those challenges.

Early in the research process, it was challenging to scope the research effort, given the lack of comparative data. It was found that a pattern existed within the literature that seemed to map to several key works. While the data gathered during each subsequent study contributed to the body of knowledge, they also left many questions unanswered or raised new questions. The idea of localization seemed to go noticed but was rarely explored (Flory, 2016; Gogolin & Jones, 2010). This led to the identification of the need and the formulation of the research questions and hypotheses. Following the previous research patterns, it was determined that this research would also build on other works.

It was determined that leveraging Flory's (2016) pre-validated survey instrument would build on the current body of knowledge while at the same time generating new data. This new data would come from the generation of a digital forensic readiness scoring system. Such a system had never been examined using law enforcement agencies in the state of Maryland. The target population would then prove to be the next challenge.

Getting the research approved by both the dissertation committee and the DSU-IRB was a significant challenge. Due to a lack of comparative data the committee decided that the number of research questions along with the hypotheses might be aggressive. Careful scoping of the effort would alleviate some of these concerns and provide the pathway forward. Receiving approval from the DSU-IRB, on the other hand, would prove more challenging.

This challenge would eventually be overcome after several revisions to the statement of consent.

Once the approvals had been realized, the next step was the execution of the plan, as detailed in Chapter 3. This involved generating one-hundred-forty-one paper surveys and creating an online version of the survey. During the collection phase, four paper surveys were received that lacked this unique agency identification code. This was due to the respondent ripping off the cover sheet, which contained the unique code. This action was not anticipated. As such, a better system should have been derived. This error resulted in the exclusion of these responses during the examination of research questions two (RQ2) and three (RQ3). This was problematic considering the already low response rate.

Limited data came as no surprise, but did present challenges. It was found that the survey instrument sent contained several minor errors. While minor, these errors may have resulted in some of the anomalies noted in Chapter 4. A careful review of the anomalies did eventually lead to a stable dataset.

While these challenges did impact the overall timeline of the project, they did not cause a complete halt. In fact, these challenges could be viewed as positive in that they brought to light errors in the approach. As such, these challenges have been presented here to assist other researchers in avoiding similar problems.

Future Work

As was noted in a previous section, the methodology selected was specific to the research questions that guided this project. There is still a significant amount of value in the data collected if viewed from a different lens. A reinterpretation of this data using either a qualitative or mixed methods methodology may bring additional details to light. As such, it could be said that this research only scratches the surface.

From the perspective of Maryland, it is believed that this research contains enough data to formulate ways to improve digital forensic readiness postures throughout the state. This could invole monitoring the readiness values over a period of months or years. The digital forensic readiness scoring system itself could also act as the basis for future research using a design science approach creating a unified monitoring and reporting system. This system could eventually be scaled to include other states, regions, or even the whole county.

By examining additional states, it may also be possible to further explore the proximity relationships that were presented in this paper. Further validating or refuting proximity relationship could provide a common way for federal, state, and local officials to determine ways to address resource distribution issues. In addition, findings related to backlogs need to be further examined as any noted similarities in future iterations may indicate a common bottleneck within the law enforcement community.

Beyond the issues noted above, there may be other valuable nuggets contained within the current dataset that should be examined. For example, there are likely other relationships that have yet to be realized that can continue to build upon the current body of knowledge. The key to discovering these relationships will be through reexamination and repeated iterations

Conclusion

This research sought to answer three research questions and support two hypotheses. The first research question (RQ1) sought to determine the current digital forensic readiness posture of law enforcement agencies in the state of Maryland. The second research question (RQ2) sought to determine if an agency's proximity to or availably of external resources influence its internal digital forensic posture. The third research question (RQ3) sought to determine what impact, if any, does an agency's internal digital forensic readiness posture have over any internal backlogs of digital forensic evidence. Hypothesis one (HP1) mapped directly to question two (RQ2), and hypothesis two (HP2) mapped to research question three (RQ3).

The research successfully assessed the digital forensic readiness posture of a sample of law enforcement agencies in the state of Maryland and assigned each of these agencies a digital forensic readiness score. It was found that proximity to a hub does not appear to contribute in either a positive or negative way to an agency’s digital forensic readiness score. Finally, based on the limited data, no trends could be identified that suggest either a negative or positive correlation between the digital forensic readiness scores and backlogs, thus negating the digital forensic readiness scores as a reliable predictive indicator.

This study directly contributes to the current body of knowledge. Specifically, it adds data from a state that has not been previously explored in this way. In addition, this data acts as an additional form of validation for previous studies, such as the one conducted by Flory (2016). Most importantly, this data, if used appropriately, has the potential to improve public safety and operations of law enforcement agencies in the state of Maryland and across the country.

REFERENCES

Abulaish, M., & Haldar, N. A. H. (2018). Advances in digital forensics frameworks and tools. *International Journal of Digital Crime and Forensics, 10*(2), 95-119. doi:10.4018/ijdcf.2018040106

Ahmed, V., Opoku, A., & Akotia, J. (2016). Choosing an appropriate research methodology and method. In *Research methodology in the built environment: a selection of case studies*. New York, NY: Routledge-Abingdon.

Altheide, C., & Carvey, H. A. (2011). *Digital forensics with open source tools*. Burlington, MA: Syngress.

Antwi-Boasiako, A., & Venter, H. (2017). *A Model for digital evidence admissibility assessment.* Paper presented at the 13th IFIP WG 11.9 International Conference, Orlando, FL. doi:10.1007/978-3-319-67208-3_2

Baer, M. (2014). Who is the witness to an internet crime: The confrontation clause, digital forensics, and child pornography. *Santa Clara High Technology Law Journal, 30*(1), 31-56. Retrieved from https://digitalcommons.law.scu.edu/chtlj/vol30/iss1/2

Borisevich, G., Chernyadyeva, N., Frolovich, E., Pastukhov, P., Polyakova, S., Dobrovlyanina, O., . . . Losavio, M. M. (2012). A comparative review of cybercrime law and digital forensics in Russia, the United States and under the convention on cybercrime of the council of Europe. *Northern Kentucky Law Review, 39*(2), 267-311. Retrieved from http://connection.ebscohost.com/c/articles/82394766/comparative-review-cybercrime-law-digital-forensics-russia-united-states-under-convention-cybercrime-council-europe

Bulbul, H. I., Yavuzcan, H. G., & Ozel, M. (2013). Digital forensics: an analytical crime scene procedure model (ACSPM). *Forensic Sci Int, 233*(1-3), 244-256. doi:10.1016/j.forsciint.2013.09.007

Bureau of Labor Statistics, & U.S. Department of Labor. (2019). *Occupational outlook handbook: Information security analysts*. Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

C.A.IN.E. (2018). CAINE - Computer forensics linux live distro. Retrieved from https://www.caine-live.net/

Cameron, L. M. (2018). Future of digital forensics faces six security challenges in fighting borderless cybercrime and dark web tools. *IEEE: Security & Privacy*. Retrieved from https://publications.computer.org/security-and-privacy/2018/03/01/digital-forensics-security-challenges-cybercrime/

Carroll, O. L., Brannon, S. K., & Song, T. (2008). Computer forensics: digital forensic analysis methodology. *Computer Forensics, 56*(1), 8. Retrieved from https://www.justice.gov/sites/default/files/usao/legacy/2008/02/04/usab5601.pdf

Carvey, H. A. (2014). *Windows forensic analysis toolkit : advanced analysis techniques for Windows 8* (4th ed.). Waltham, MA: Syngress.

Casey, E. (2011). *Digital evidence and computer crime forensic science, computers and the internet* (3rd ed.). Burlington, MA: Academic Press.

Cassim, F. (2017). The use of electronic discovery and cloudcomputing technology by lawyers in practice: Lessons from abroad. *Journal for Juridical Science, 42*(1), 19-40. doi:10.18820/24150517/JJS42.v1.2

Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The future of digital forensics: Challenges and the road ahead. *IEEE Security & Privacy, 15*(6), 12-17. doi:10.1109/MSP.2017.4251117

CITI Program. (n.d.). Mission and history. Retrieved from https://about.citiprogram.org/en/mission-and-history/

Cohen, D. (2015). Understanding population density. Retrieved from https://www.census.gov/newsroom/blogs/random-samplings/2015/03/understanding-population-density.html

Cole, K. A., Gupta, S., Gurugubelli, D., & Rogers, M. K. (2015). *Review of recent case law related to digital forensics: The current issues.* Paper presented at the Annual ADFSL Conference on Digital Forensics, Security and Law, Daytona Beach, FL. Retrieved from https://commons.erau.edu/cgi/viewcontent.cgi?article=1321&context=adfsl

Cornell Law School. (n.d.-a). Daubert Standard. Retrieved from https://www.law.cornell.edu/wex/daubert_standard

Cornell Law School. (n.d.-b). *Frye Standard*. Retrieved from https://www.law.cornell.edu/wex/Frye_standard

Creswell, J. W. (2014). *Research design : qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks, CA: SAGE Publications.

Cubit. (2019). Maryland counties by population. Retrieved from https://www.maryland-demographics.com/counties_by_population

Datas SIO, NOAA, U.S. Navy, NGA, GEBCO, & Google. (2018). Maryland - Centered.

Daubert v. Merrell Dow Pharmaceuticals Inc., 509 U.S. 579 (1993).

Decusatis, C., Carranza, A., Ngaide, A., Zafar, S., & Landaez, N. (2015). *Methodology for an open digital forensics model based on CAINE*. Paper presented at the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, UK. doi:10.1109/cit/iucc/dasc/picom.2015.61

Department of Public Saftey & Correctional Services. (n.d.). Maryland police agencies' policies. Retrieved from https://mdle.net/agencies.htm

Department of the Treasury Office of Economic Policy, Council of Economic Advisers, & Department of Labor. (2015). *Occupational licensing: A framework for policymakers*. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/docs/licensing_report_final_nonembargo.pdf

Digital Forensics Association. (n.d.). Formal education: college education in digital forensics. Retrieved from http://www.digitalforensicsassociation.org/formal-education/

Digital Intelligence. (2019). Store. Retrieved from https://digitalintelligence.com/store/

Dilijonaite, A. (2018). Digital forensic readiness. In *Digital Forensics* (pp. 117-145). Hoboken, NJ: John Wiley & Sons Inc.

Du, X., Le-Khac, N., & Scanlon, M. (2017). *Evaluation of digital forensic process models with respect to digital dorensics as a service*. Paper presented at the 6th European

Conference on Cyber Warfare and Security (ECCWS 2017), Dublin, Ireland. Retrieved from https://arxiv.org/ftp/arxiv/papers/1708/1708.01730.pdf

Ellis, R. (2014). Creating a Secure Network: The 2001 Anthrax Attacks and the Transformation of Postal Security. *The Sociological Review, 62*(1_suppl), 161-182. doi:10.1111/1467-954x.12128

Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security, 52*, 70-89. doi:10.1016/j.cose.2015.04.003

Federal Bureau of Investigation. (2017). *2017 Internet Crime Report*. Retrieved from https://pdf.ic3.gov/2017_IC3Report.pdf

Federal Bureau of Investigation. (2019). *2019 Internet Crime Report*. Retrieved from https://pdf.ic3.gov/2019_IC3Report.pdf

Flory, T. (2016). Digital forensics in law enforcement: A needs based analysis of Indiana agencies. *Journal of Digital Forensics, Security and Law, 11*(1). doi:10.15394/jdfsl.2016.1374

Frye v. United States, 293 F. Supp. 1013 (D.C. Cir. 1923).

Garfinkel, S., Farrell, P., Roussev, V., & Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. *Digital Investigation, 6*, S2-S11. doi:10.1016/j.diin.2009.06.016

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*, S64-S73. doi:10.1016/j.diin.2010.05.009

Garrie, D. B., & Morrissy, J. D. (2014). Digital forensic evidence in the courtroom: Understanding content and quality. *Northwestern Journal of Technology and Intellectual Property, 12*(2). Retrieved from https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss2/5

Gogolin, G., & Jones, J. (2010). Law enforcement's ability to deal with digital crime and the implications for business. *Information Security Journal: A Global Perspective, 19*(3), 109-117. doi:10.1080/19393555.2010.483931

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). *Digital evidence and the U.S. criminal justice system: Identifying technology and other needs to more effectively* *acquire and utilize digital evidence*. Retrieved from http://www.jstor.org/stable/10.7249/j.ctt15sk8v3

Google. (n.d.). Maryland. Retrieved from https://www.google.com/maps/place/Maryland/@38.8897925,-77.0677718,8z/data=!4m5!3m4!1s0x89b64debe9f190df:0xf2af37657655f6b1!8m2!3d39.0457549!4d-76.6412712

Goulding, C. (2002). *Grounded theory a practical guide for management, business and market researchers*. Thousand Oaks, CA: SAGE Publishing.

Govan, M. (2016). The application of peer teaching in digital forensics education. *Higher Education Pedagogies, 1*(1), 57-63. doi:10.1080/23752696.2015.1134198

Gutmann, P. (1996, July 24). *Secure deletion of data from magnetic and solid-state memory.* Paper presented at the 6th conference on USENIX Security Symposium, Focusing on Applications of Cryptography, San Jose, CA. Retrieved from https://www.usenix.org/legacy/publications/library/proceedings/sec96/full_papers/gutmann/index.html

Harichandran, V. S., Breitinger, F., Baggili, I., & Marrington, A. (2016). A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Computers & Security, 57*, 1-13. doi:10.1016/j.cose.2015.10.007

Harmon, R. R., Castro-Leon, E. G., & Bhide, S. (2015). *Smart cities and the Internet of Things*. Paper presented at the 2015 Portland International Conference on Management of Engineering and Technology (PICMET), Portland, OR. doi:10.1109/picmet.2015.7273174

Henry, P., Williams, J., & Wright, B. (2013). *The SANS survey of digital forensics and incident response*. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/survey-digital-forensics-incident-response-35010

Hickman, M. J., & Peterson, J. L. (2004). *Census of publicly funded forensic crime laboratories: 50 largest crime labs, 2002*. (NCJ 205988). Retrieved from http://bjs.ojp.usdoj.gov/content/pub/pdf/50lcl02.pdf

Hollywood, J., & Winkelman, Z. (2015). *Improving information-sharing across law enforcement: Why can't we know?* Retrieved from https://www.jstor.org/stable/10.7249/j.ctt19rmdmz

Institute for Security Technology Studies. (2002). *Law enforcement tools and technologies for investigating cyber attacks: A national needs assessment*. Retrieved from http://www.ists.dartmouth.edu/docs/ISTS_NA.pdf

Karie, N., & Karume, S. (2017). Digital forensic readiness in organizations: issues and challenges. *The Journal of Digital Forensics, Security and Law, 12*(4). doi:10.15394/jdfsl.2017.1436

Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model. *Computers & Security, 38*, 103-115. doi:10.1016/j.cose.2013.05.001

Kouwen, A., Scanlon, M., Raymond Choo, K.-K., & Le-Khac, N.-A. (2018). Digital forensic investigation of two-way radio communication equipment and services. *Digital Investigation, 26*, S77-S86. doi:10.1016/j.diin.2018.04.007

Krishnamurthy, D. (2004). Synthetic workload generation for stress testing session-based systems. *IEEE Transactions on Software Engineering, 32*(11), 868-882. doi:10.1109/TSE.2006.106

Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999).

Lillis, D., Becker, B. A., O'Sullivan, T., & Scanlon, M. (2016). *Current challenges and future research areas for digital forensic investigation*. Paper presented at the The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016), Daytona Beach, FL. doi:10.13140/RG.2.2.34898.76489

Lim, N. (2008a, April 24). *Digital forensic certification versus forensic science certification.* Paper presented at the Annual ADFSL Conference on Digital Forensics, Security and Law, Oklahoma City, OK. Retrieved from https://commons.erau.edu/cgi/viewcontent.cgi?article=1048&context=adfsl

Lim, N. (2008b). Escaping the Computer-Forensics Certification Maze: A Survey of Professional Certifications. *Communications of the Association for Information Systems, 23*, 547-574. doi:10.17705/1CAIS.02329

Lonardo, T., White, D., & Rea, A. (2012). To license or not to license updated: An examination of state statutes regarding private investigators and digital examiners. *Journal of Digital Forensics, Security and Law, 7*(3). doi:10.15394/jdfsl.2012.1129

Losavio, M. M., Pastukov, P., Polyakova, S., Zhang, X., Chow, K. P., Koltay, A., . . . Ortiz, M. E. (2019). The juridical spheres for digital forensics and electronic evidence in the insecure electronic world. *Wiley Interdisciplinary Reviews: Forensic Science, 1*(5), e1337. doi:10.1002/wfs2.1337

Lowhorn, G. L. (2007). *Qualitative and quantitative research: How to choose the best design*. Paper presented at the Academic Business World International Conference, Nashville, TN. Retrieved from https://ssrn.com/abstract=2235986

Manes, G. W., Downing, E., Watson, L., & Thrutchley, C. (2007). *New federal rules and digital evidence.* Paper presented at the Annual ADFSL Conference on Digital Forensics, Security and Law, Alexandria, VA. Retrieved from https://commons.erau.edu/adfsl/2007/session-6/3

Maryland. (n.d.). Maryland Manual On-Line. Retrieved from https://msa.maryland.gov/msa/mdmanual/01glance/html/pop.html#county

Maryland Department of Natural Resources. (2019). Land areas, inland-water areas, and length of shorelines of Maryland's counties. Retrieved from http://www.mgs.md.gov/geology/areas_and_lengths.html

Maryland State Police. (n.d.). Special Police. Retrieved from https://mdsp.maryland.gov/Organization/Pages/CriminalInvestigationBureau/LicensingDivision/ProfessionalLicenses/SpecialPolice.aspx

McKillip, J. (1987). *Need analysis: tools for the human services and education*. Newbury Park, CA: SAGE Publications.

McMillon, M. (2003). Building a low cost forensics workstation. *Information Security Reading Room*. Retrieved from https://www.sans.org/reading-room/whitepapers/incident/building-cost-forensics-workstation-895

Meffert, C. S., Baggili, I., & Breitinger, F. (2016). Deleting collected digital evidence by exploiting a widely adopted hardware write blocker. *Digital Investigation, 18*, S87-S96. doi:10.1016/j.diin.2016.04.004

Melbourn, H., Smith, G., McFarland, J., Rogers, M., Wieland, K., DeWilde, D., . . . Quarino, L. (2019). Mandatory certification of forensic science practitioners in the United States: A supportive perspective. *Forensic Science International: Synergy, 1*, 161-169. doi:10.1016/j.fsisyn.2019.08.001

Mushtaque, K., Ahsan, K., & Umer, A. (2015). Digital forensic investigation models, an evolution study. *JISTEM - Journal of Information Systems and Technology Management, 12*(2), 233-243. doi:10.4301/S1807-17752015000200003

National Commission on Forensic Science. (2016). *Views of the Commission Certification of Forensic Science Practitioners* Retrieved from https://www.justice.gov/archives/ncfs/page/file/888671/download

National Institute of Justice. (2006). *Status and needs of forensic science service providers : A report to Congress*. Retrieved from http://www.ncjrs.gov/pdffiles1/nij/213420.pdf

Novak, M., Grier, J., & Gonzales, D. (2019). New approaches to digital evidence acquisition and analysis. *National Institute of Justice Journal*(280). Retrieved from https://www.ncjrs.gov/pdffiles1/nij/250700.pdf

Nucor Corp v. Bell, 251 F.R.D. 191 (2008).

Offensive Security. (2019). Kali. Retrieved from https://www.kali.org/

Omair, A. (2014). Understanding the process of statistical methods for effective data analysis. *Journal of Health Specialties, 2*(3), 100-104. doi:10.4103/1658-600x.137882

Pangalos, G., & Katos, V. (2009). *Information assurance and forensic readiness.* Paper presented at the Third International Conference, e-Democracy, Athens, Greece. doi:10.1007/978-3-642-11631-5_17

Phillips, R. T. M. (2006). Assessing presidential stalkers and assassins. *Journal of the American Academy of Psychiatry and the Law Online, 34*(2), 154-164. Retrieved from http://jaapl.org/content/34/2/154

Pollitt, M. (2010). *A history of digital forensics*, Berlin, Heidelberg. doi:10.1007/978-3-642-15506-2_1

Pollitt, M., Caloyannides, M., Novotny, J., & Shenoi, S. (2004). Digital forensics: Operational, legal and research issues. In S. De Capitani di Vimercati, I. Ray, & I. Ray (Eds.), *Data and applications security XVII: Status and prospects* (pp. 393-403). Boston, MA: Springer US.

Pruett, S. R. (2006). Needs Analysis. Retrieved from http://courses.phhp.ufl.edu/rcs6740/ppt%2006/need_analysis.pdf

Quick, D., & Choo, K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation, 11*(4), 273-294. doi:10.1016/j.diin.2014.09.002

Rajamaki, J., & Knuuttila, J. (2013). *Law enforcement authorities' legal digital evidence gathering: Legal, integrity and chain-on-custody requirement.* Paper presented at the 2013 European Intelligence and Security Informatics Conference, Uppsala, Sweden. doi:doi.org/10.1109/EISIC.2013.44

Raju, B. K., & Geethakumari, G. (2019). SNAPS: Towards building snapshot based provenance system for virtual machines in the cloud environment. *Computers & Security, 86*, 92-111. doi:10.1016/j.cose.2019.05.020

Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. *Computers & Security, 23*(1), 12-16. doi:10.1016/j.cose.2004.01.003

Roussev, V. (2009). Hashing and Data Fingerprinting in Digital Forensics. *IEEE Security & Privacy Magazine, 7*(2), 49-55. doi:10.1109/msp.2009.40

Sacco, L. N., & James, N. (2015). *Backlog of sexual assault evidence: In brief* (R44237). Retrieved from https://fas.org/sgp/crs/misc/R44237.pdf

Saldaña, J. (2011). *Fundamentals of qualitative research*. New York, NY: Oxford University Press.

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

Scanlon, M. (2016). *Battling the digital forensic backlog through data deduplication.* Paper presented at the Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, Ireland. doi:10.1109/INTECH.2016.7845139

Spreitzenbarth, M. (2015). *Mastering Python forensics: master the art of digital forensics and analysis with Python*. Birmingham, UK: Packt Publishing.

Stein, J. (2016). How Washington, D.C., Is Preparing for the Next Terrorist Attack. *Newsweek, 166*(25). Retrieved from https://www.newsweek.com/2016/07/01/can-isis-take-down-washington-dc-472395.html

SurveyMonkey. (2018). Security Statement. Retrieved from https://www.surveymonkey.com/mp/legal/security/

Tan, J. (2001). *Forensics Readiness*. Retrieved from https://isis.poly.edu/kulesh/forensics/forensic_readiness.pdf

United States Census Bureau. (2010a). American Fact Finder: Indiana (2010 Demographic Profile). Retrieved from https://factfinder.census.gov/faces/nav/jsf/pages/community_facts.xhtml?src=bkmk

United States Census Bureau. (2010b). American Fact Finder: Michigan (2010 Demographic Profile). Retrieved from https://factfinder.census.gov/faces/nav/jsf/pages/community_facts.xhtml?src=bkmk

United States Census Bureau. (2018a). American Fact Finder: Maryland (2018 Population Estimate). Retrieved from https://factfinder.census.gov/faces/nav/jsf/pages/community_facts.xhtml?src=bkmk

United States Census Bureau. (2018b). QuickFacts: District of Columbia. Retrieved from https://www.census.gov/quickfacts/DC

United States Department of Justice. (2018). *Report of the Attorney General's Cyber Digital Task Force*. Retrieved from https://www.justice.gov/ag/page/file/1076696/download

United States v. Christopher Paul Hasson, No. 8:19-mj-00063 (D.M.D. 2019).

US-CERT. (2008). *Computer Forensics*. Retrieved from https://www.us-cert.gov/sites/default/files/publications/forensics.pdf

van Baar, R. B., van Beek, H. M. A., & van Eijk, E. J. (2014). Digital forensics as a service: A game changer. *Digital Investigation, 11*, S54-S62. doi:10.1016/j.diin.2014.03.007

Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice & Research, 17*(2), 183-195. doi:10.1080/15614263.2015.1128163

Watts, L. (2017). Maryland State Police computer crime lab dealing with heavy workload, several months of backlog. *Fox 5 News*. Retrieved from http://www.fox5dc.com/news/local-news/maryland-state-police-computer-crime-lab-dealing-with-heavy-workload-several-months-of-backlog

Weulen Kranenbarg, M., Holt, T. J., & van Gelder, J. (2017). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior, 40*(1), 40-55. doi:10.1080/01639625.2017.1411030

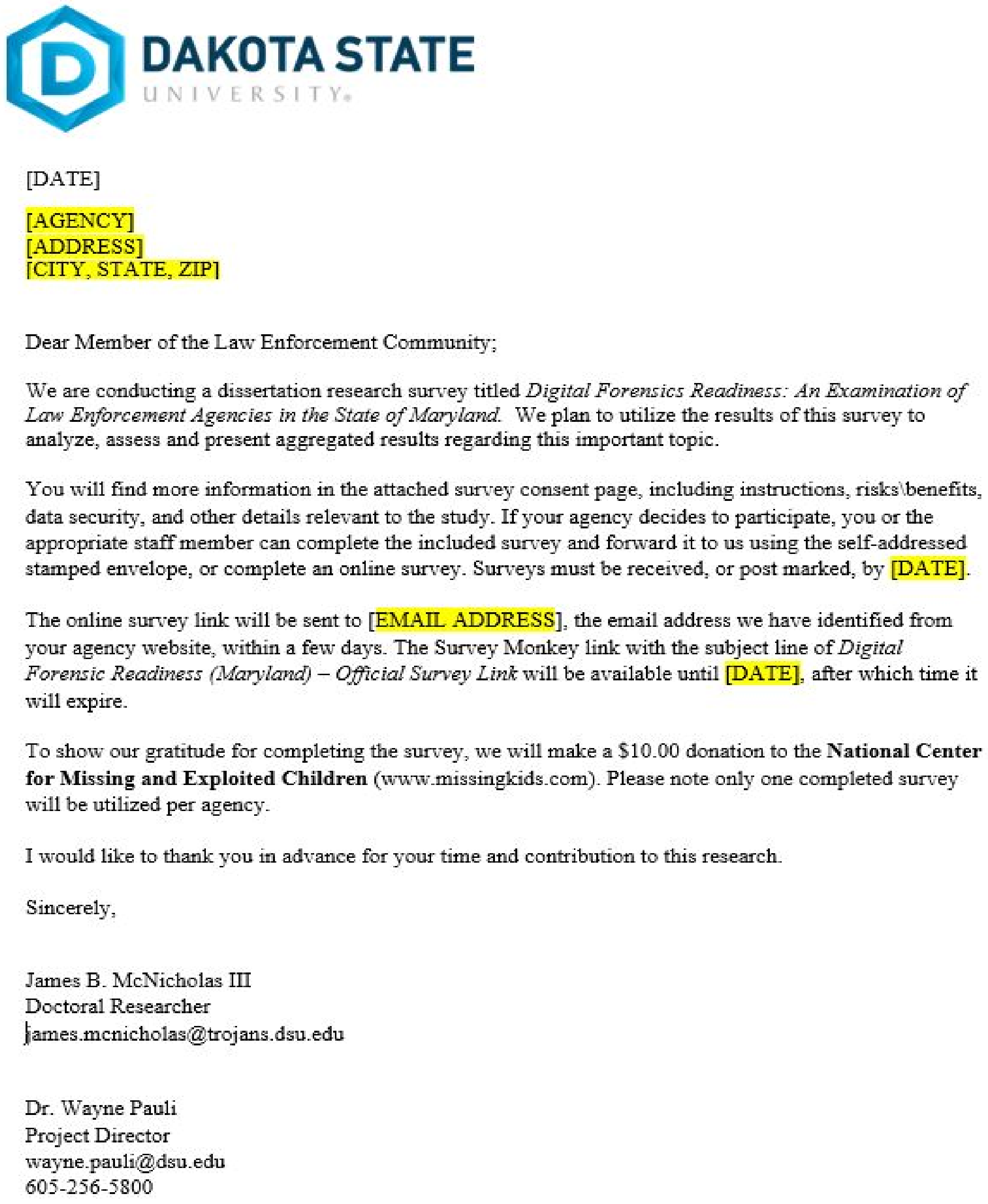
Wieringa, R. J. (2014). *Design science methodology for information systems and software engineering*. Berlin Heidelberg: Springer-Verlag.

Wiles, J., & Reyes, A. (2011). *The best damn cybercrime and digital forensics book period* (1st ed.). Rockland, MA: Syngress.

Zawoad, S., & Hasan, R. (2015). *FAIoT: Towards building a forensics aware eco system for the Internet of Things.* Paper presented at the IEEE International Conference on Services Computing, New York, NY. doi:10.1109/SCC.2015.46

APPENDICES

APPENDIX A: SOLICITATION LETTER



DAKOTA STATE
UNIVERSITY

[DATE]

[AGENCY]
[ADDRESS]
[CITY, STATE, ZIP]

Dear Member of the Law Enforcement Community;

We are conducting a dissertation research survey titled *Digital Forensics Readiness: An Examination of Law Enforcement Agencies in the State of Maryland.* We plan to utilize the results of this survey to analyze, assess and present aggregated results regarding this important topic.

You will find more information in the attached survey consent page, including instructions, risks\benefits, data security, and other details relevant to the study. If your agency decides to participate, you or the appropriate staff member can complete the included survey and forward it to us using the self-addressed stamped envelope, or complete an online survey. Surveys must be received, or post marked, by [DATE].

The online survey link will be sent to [EMAIL ADDRESS], the email address we have identified from your agency website, within a few days. The Survey Monkey link with the subject line of *Digital Forensic Readiness (Maryland) – Official Survey Link* will be available until [DATE], after which time it will expire.

To show our gratitude for completing the survey, we will make a $10.00 donation to the **National Center for Missing and Exploited Children** (www.missingkids.com). Please note only one completed survey will be utilized per agency.

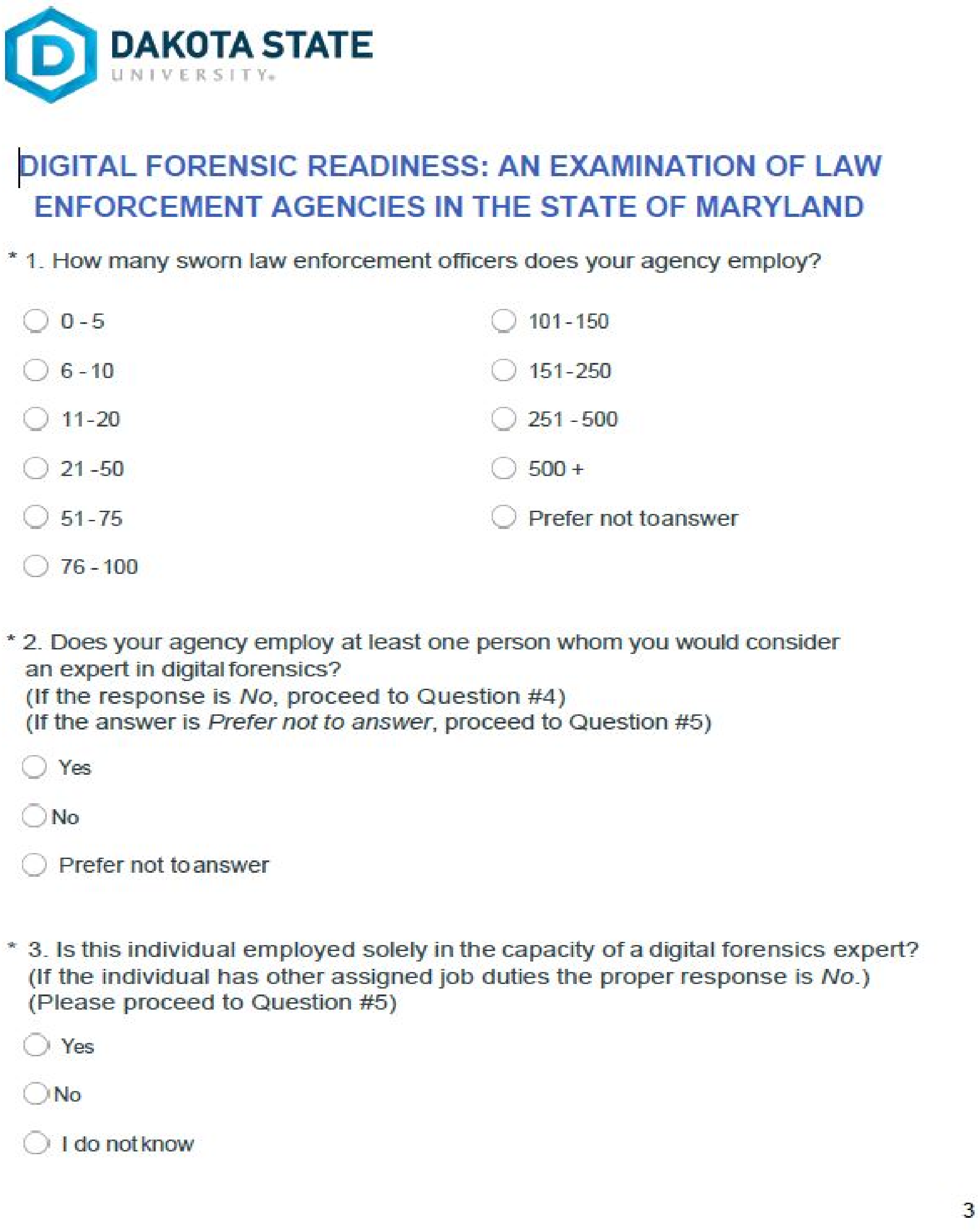
I would like to thank you in advance for your time and contribution to this research.

Sincerely,

James B. McNicholas III
Doctoral Researcher
james.mcnicholas@trojans.dsu.edu

Dr. Wayne Pauli
Project Director
wayne.pauli@dsu.edu
605-256-5800

APPENDIX B: SURVEY INSTRUMENT



DAKOTA STATE
UNIVERSITY

DIGITAL FORENSIC READINESS: AN EXAMINATION OF LAW ENFORCEMENT AGENCIES IN THE STATE OF MARYLAND

* 1. How many sworn law enforcement officers does your agency employ?

○ 0 - 5

○ 6 - 10

○ 11-20

○ 21 -50

○ 51-75

○ 76 - 100

○ 101-150

○ 151-250

○ 251 - 500

○ 500 +

○ Prefer not toanswer

* 2. Does your agency employ at least one person whom you would consider an expert in digital forensics?
(If the response is *No*, proceed to Question #4)
(If the answer is *Prefer not to answer*, proceed to Question #5)

○ Yes

○ No

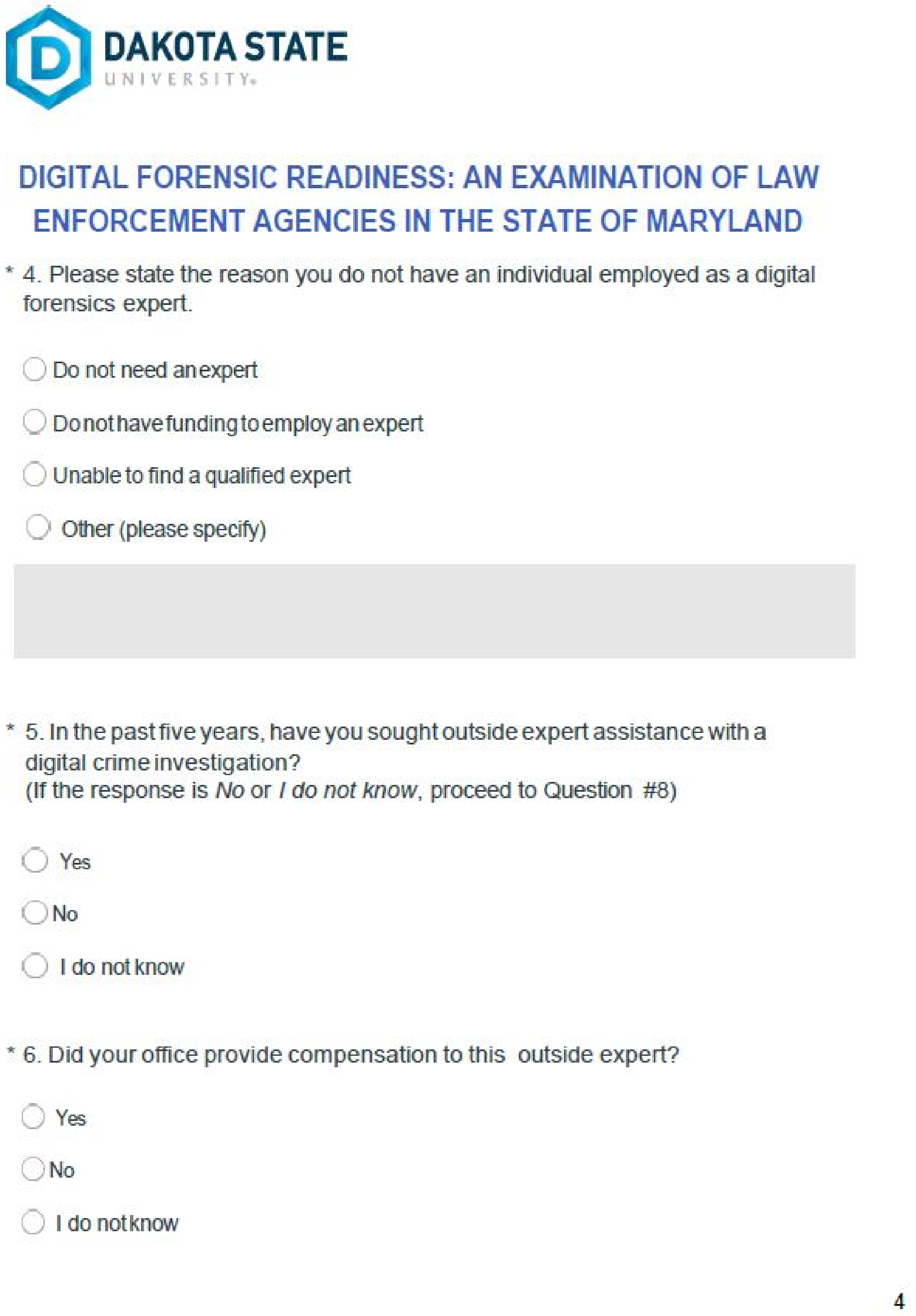
○ Prefer not to answer

* 3. Is this individual employed solely in the capacity of a digital forensics expert?
(If the individual has other assigned job duties the proper response is *No*.)
(Please proceed to Question #5)

○ Yes

○ No

○ I do not know



DAKOTA STATE UNIVERSITY

DIGITAL FORENSIC READINESS: AN EXAMINATION OF LAW ENFORCEMENT AGENCIES IN THE STATE OF MARYLAND

* 4. Please state the reason you do not have an individual employed as a digital forensics expert.

○ Do not need an expert

○ Do not have funding to employ an expert

○ Unable to find a qualified expert

○ Other (please specify)

* 5. In the past five years, have you sought outside expert assistance with a digital crime investigation?
(If the response is *No* or *I do not know*, proceed to Question #8)

○ Yes

○ No

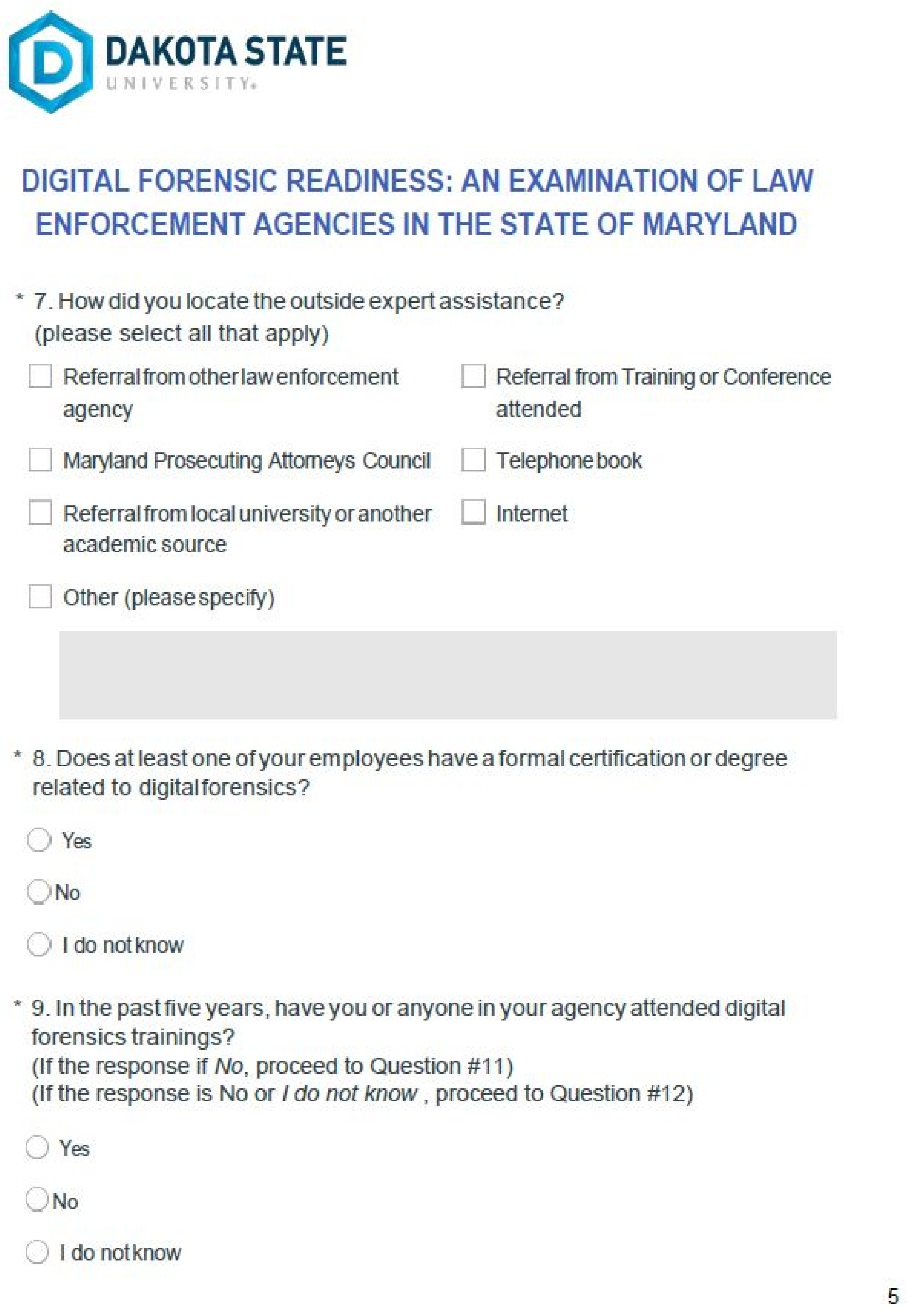
○ I do not know

* 6. Did your office provide compensation to this outside expert?

○ Yes

○ No

○ I do not know



DAKOTA STATE UNIVERSITY

DIGITAL FORENSIC READINESS: AN EXAMINATION OF LAW ENFORCEMENT AGENCIES IN THE STATE OF MARYLAND

* 7. How did you locate the outside expert assistance?
(please select all that apply)

□ Referral from other law enforcement agency

□ Maryland Prosecuting Attorneys Council

□ Referral from local university or another academic source

□ Other (please specify)

□ Referral from Training or Conference attended

□ Telephone book

□ Internet

* 8. Does at least one of your employees have a formal certification or degree related to digital forensics?

○ Yes

○ No

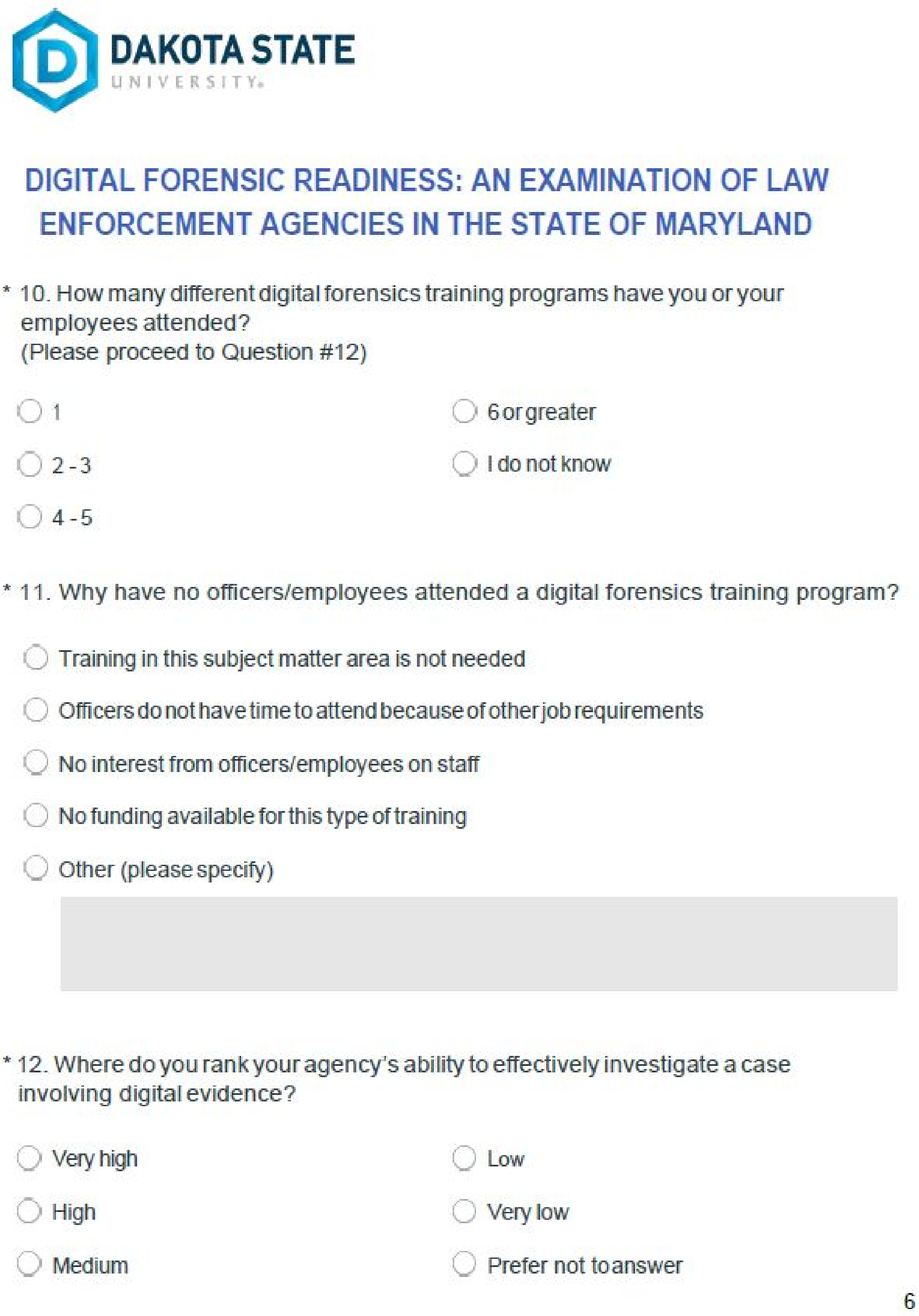
○ I do not know

* 9. In the past five years, have you or anyone in your agency attended digital forensics trainings?
(If the response if *No*, proceed to Question #11)
(If the response is No or *I do not know* , proceed to Question #12)

○ Yes

○ No

○ I do not know



DAKOTA STATE UNIVERSITY

DIGITAL FORENSIC READINESS: AN EXAMINATION OF LAW ENFORCEMENT AGENCIES IN THE STATE OF MARYLAND

* 10. How many different digital forensics training programs have you or your employees attended?
(Please proceed to Question #12)

○ 1

○ 2 - 3

○ 4 - 5

○ 6 or greater

○ I do not know

* 11. Why have no officers/employees attended a digital forensics training program?

○ Training in this subject matter area is not needed

○ Officers do not have time to attend because of other job requirements

○ No interest from officers/employees on staff

○ No funding available for this type of training

○ Other (please specify)

* 12. Where do you rank your agency's ability to effectively investigate a case involving digital evidence?

○ Very high

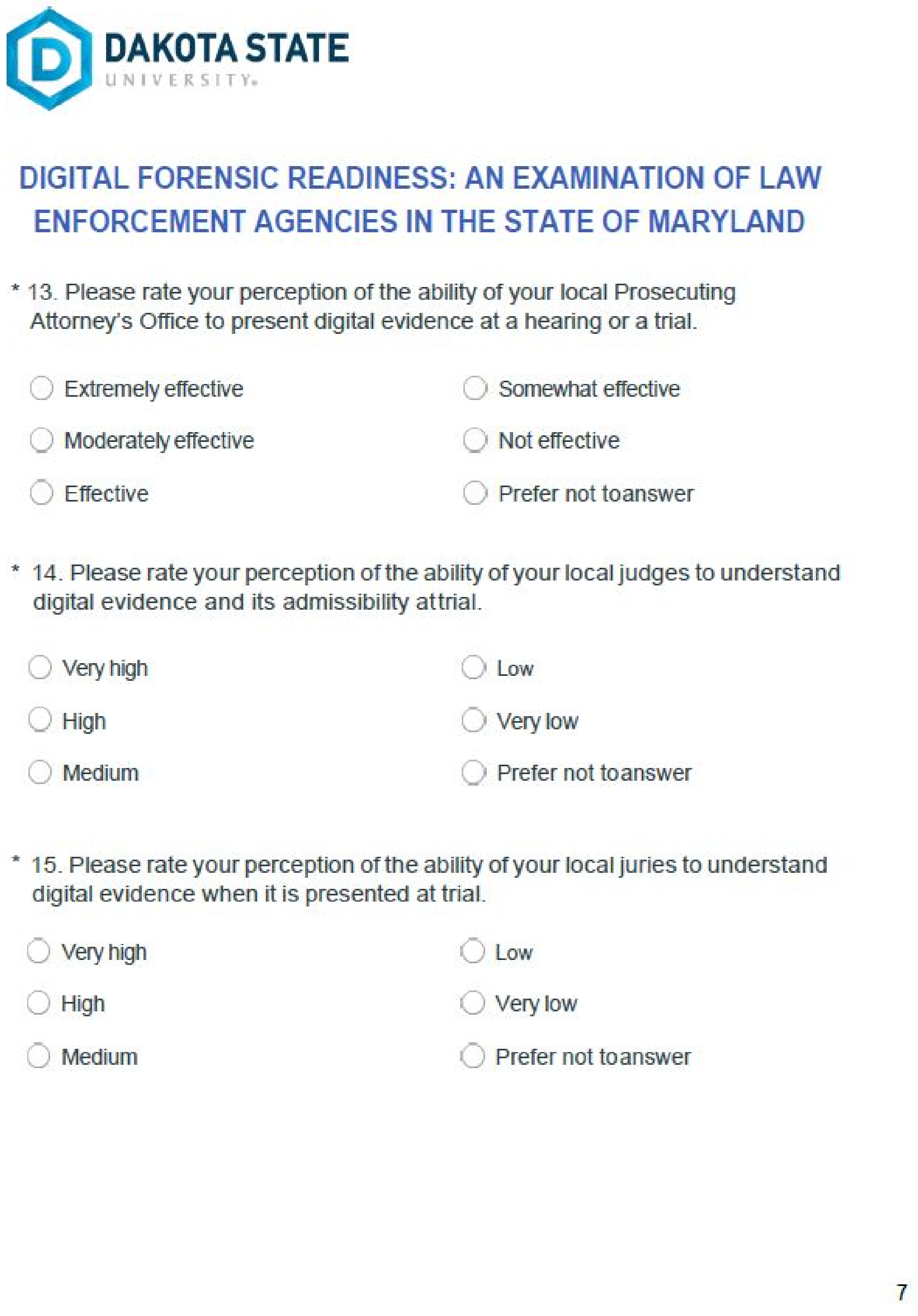
○ High

○ Medium

○ Low

○ Very low

○ Prefer not to answer



DAKOTA STATE UNIVERSITY

DIGITAL FORENSIC READINESS: AN EXAMINATION OF LAW ENFORCEMENT AGENCIES IN THE STATE OF MARYLAND

* 13. Please rate your perception of the ability of your local Prosecuting Attorney's Office to present digital evidence at a hearing or a trial.

○ Extremely effective

○ Moderately effective

○ Effective

○ Somewhat effective

○ Not effective

○ Prefer not to answer

* 14. Please rate your perception of the ability of your local judges to understand digital evidence and its admissibility at trial.

○ Very high

○ High

○ Medium

○ Low

○ Very low

○ Prefer not to answer

* 15. Please rate your perception of the ability of your local juries to understand digital evidence when it is presented at trial.

○ Very high

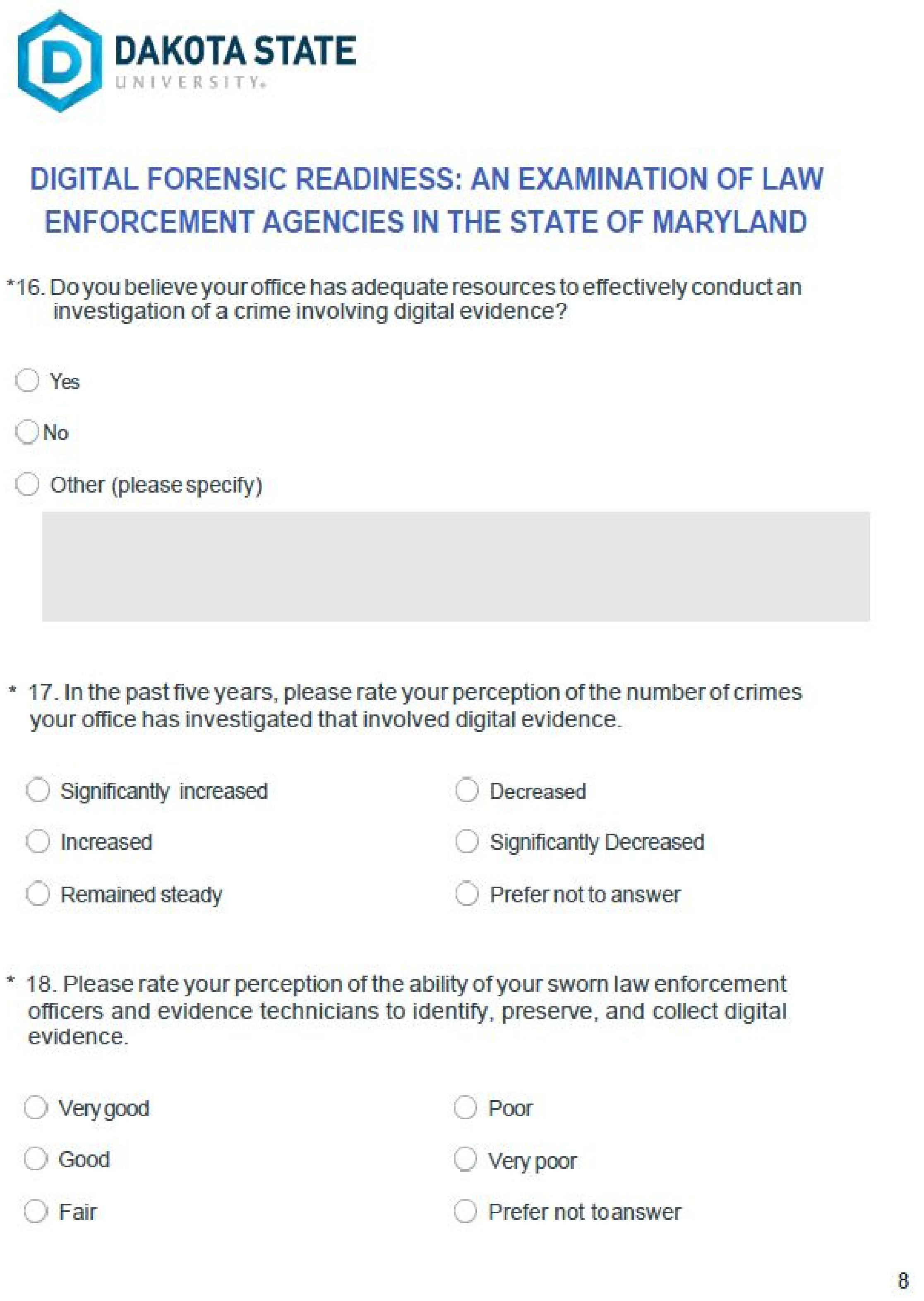
○ High

○ Medium

○ Low

○ Very low

○ Prefer not to answer



DAKOTA STATE UNIVERSITY

DIGITAL FORENSIC READINESS: AN EXAMINATION OF LAW ENFORCEMENT AGENCIES IN THE STATE OF MARYLAND

*16. Do you believe your office has adequate resources to effectively conduct an investigation of a crime involving digital evidence?

○ Yes

○ No

○ Other (please specify)

* 17. In the past five years, please rate your perception of the number of crimes your office has investigated that involved digital evidence.

○ Significantly increased

○ Increased

○ Remained steady

○ Decreased

○ Significantly Decreased

○ Prefer not to answer

* 18. Please rate your perception of the ability of your sworn law enforcement officers and evidence technicians to identify, preserve, and collect digital evidence.

○ Very good

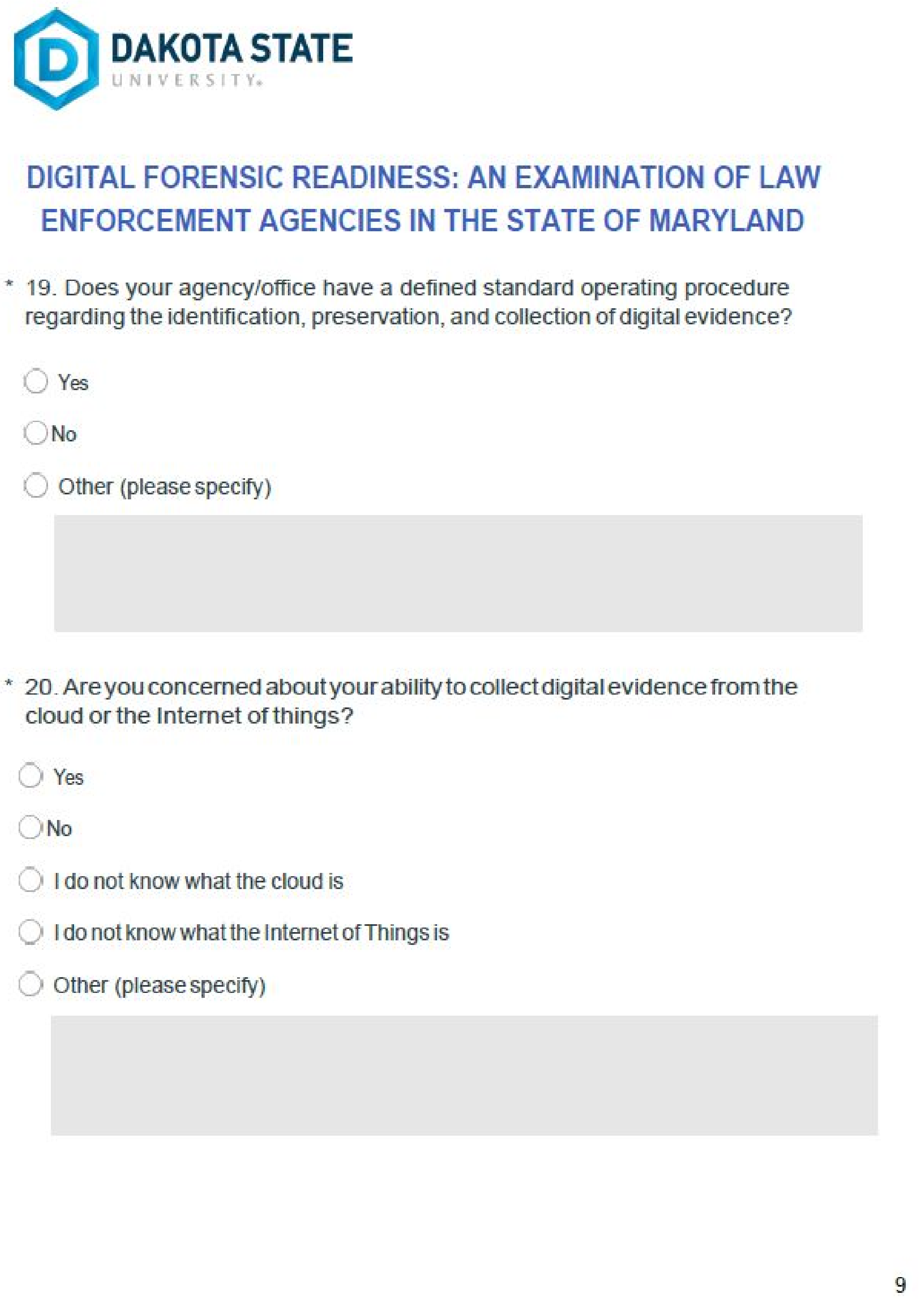
○ Good

○ Fair

○ Poor

○ Very poor

○ Prefer not to answer



DAKOTA STATE UNIVERSITY

DIGITAL FORENSIC READINESS: AN EXAMINATION OF LAW ENFORCEMENT AGENCIES IN THE STATE OF MARYLAND

* 19. Does your agency/office have a defined standard operating procedure regarding the identification, preservation, and collection of digital evidence?

○ Yes

○ No

○ Other (please specify)

* 20. Are you concerned about your ability to collect digital evidence from the cloud or the Internet of things?

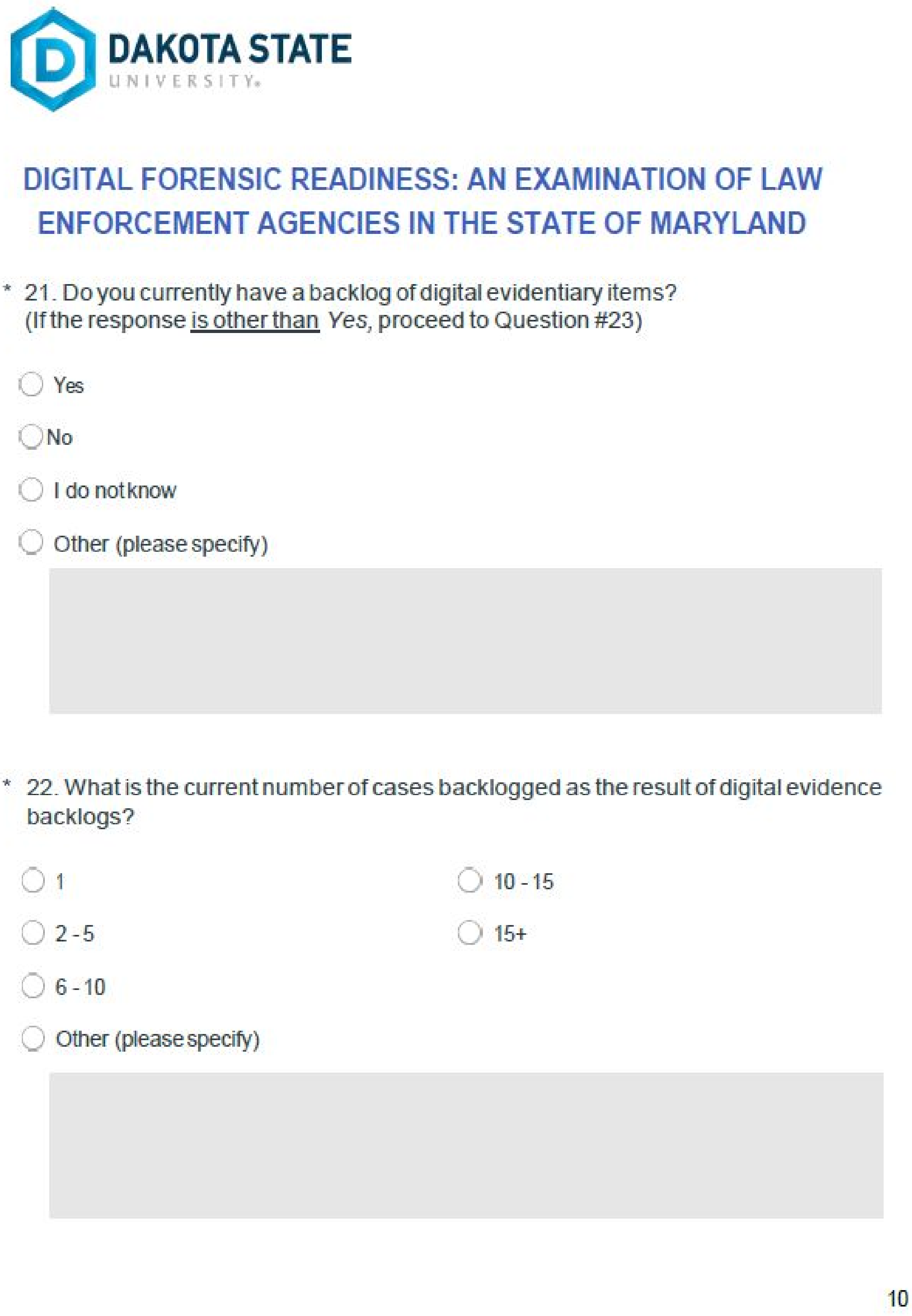
○ Yes

○ No

○ I do not know what the cloud is

○ I do not know what the Internet of Things is

○ Other (please specify)



DAKOTA STATE UNIVERSITY

DIGITAL FORENSIC READINESS: AN EXAMINATION OF LAW ENFORCEMENT AGENCIES IN THE STATE OF MARYLAND

* 21. Do you currently have a backlog of digital evidentiary items?
(If the response is other than *Yes*, proceed to Question #23)

○ Yes

○ No

○ I do not know

○ Other (please specify)

* 22. What is the current number of cases backlogged as the result of digital evidence backlogs?

○ 1

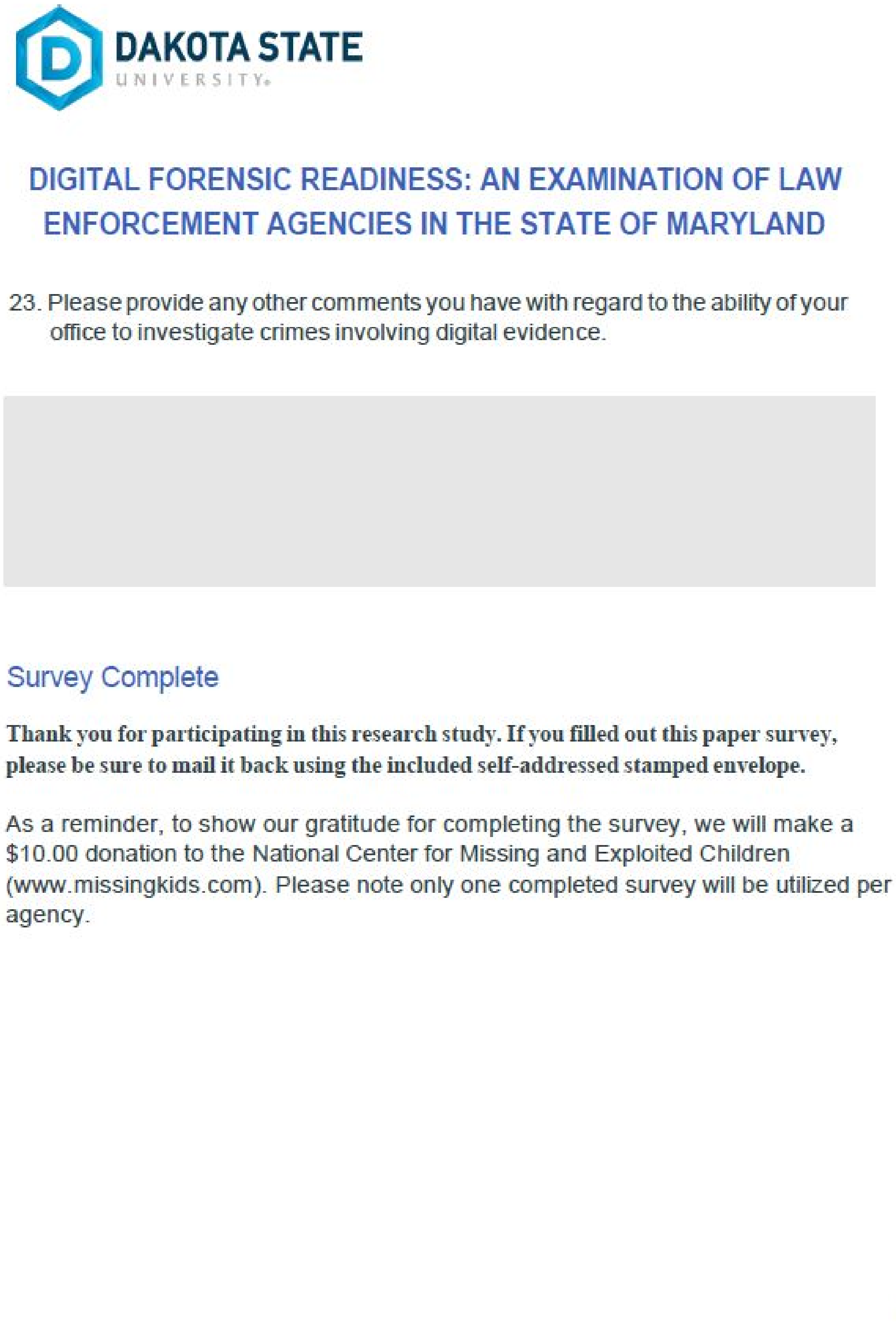
○ 2 - 5

○ 6 - 10

○ 10 - 15

○ 15+

○ Other (please specify)



DAKOTA STATE UNIVERSITY

DIGITAL FORENSIC READINESS: AN EXAMINATION OF LAW ENFORCEMENT AGENCIES IN THE STATE OF MARYLAND

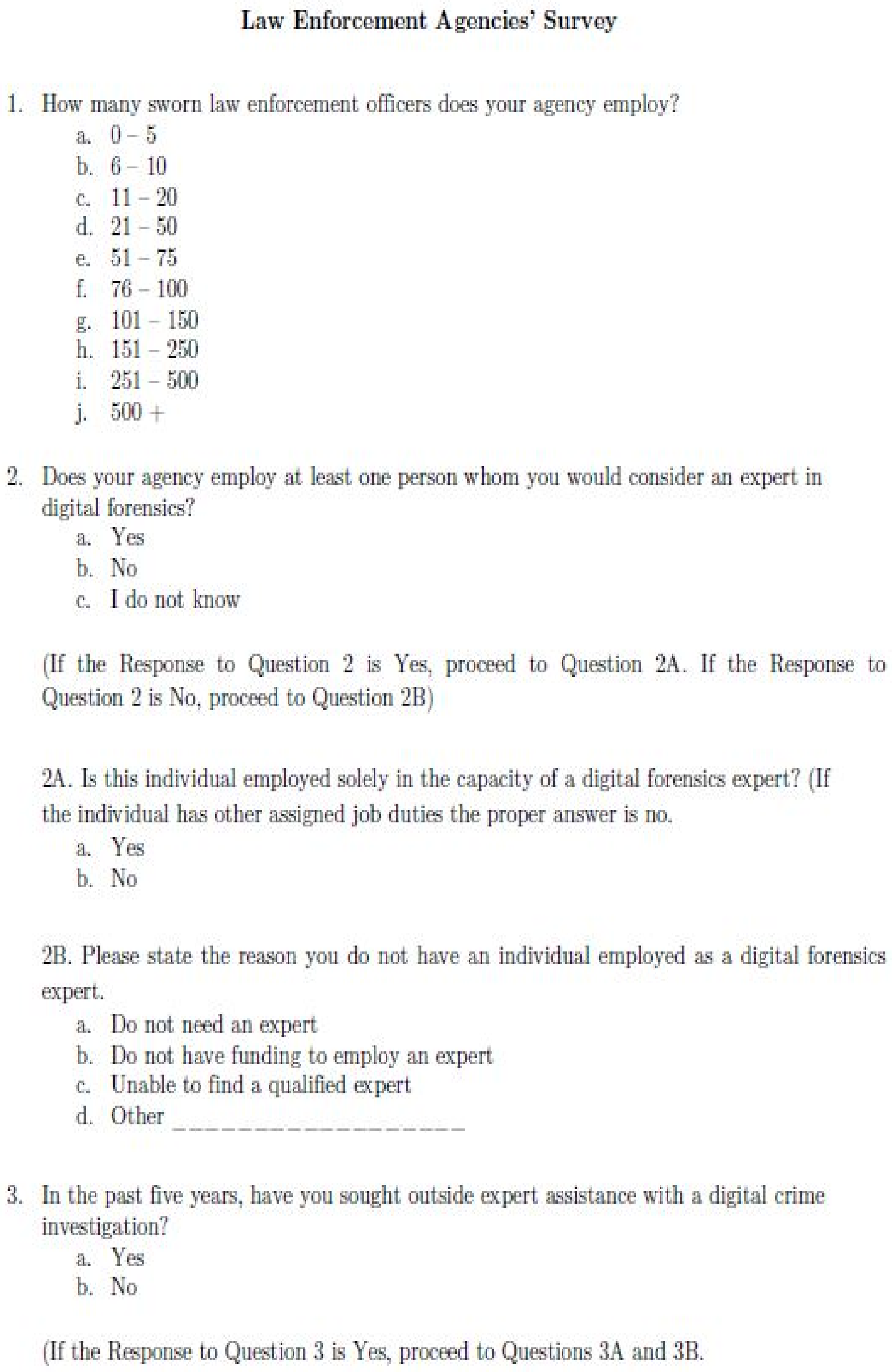
23. Please provide any other comments you have with regard to the ability of your office to investigate crimes involving digital evidence.

Survey Complete

Thank you for participating in this research study. If you filled out this paper survey, please be sure to mail it back using the included self-addressed stamped envelope.

As a reminder, to show our gratitude for completing the survey, we will make a $10.00 donation to the National Center for Missing and Exploited Children (www.missingkids.com). Please note only one completed survey will be utilized per agency.

APPENDIX C: FLORY (2016) SURVEY INSTRUMENT



Law Enforcement Agencies' Survey

1. How many sworn law enforcement officers does your agency employ?
   a. 0 – 5
   b. 6 – 10
   c. 11 – 20
   d. 21 – 50
   e. 51 – 75
   f. 76 – 100
   g. 101 – 150
   h. 151 – 250
   i. 251 – 500
   j. 500 +

2. Does your agency employ at least one person whom you would consider an expert in digital forensics?
   a. Yes
   b. No
   c. I do not know

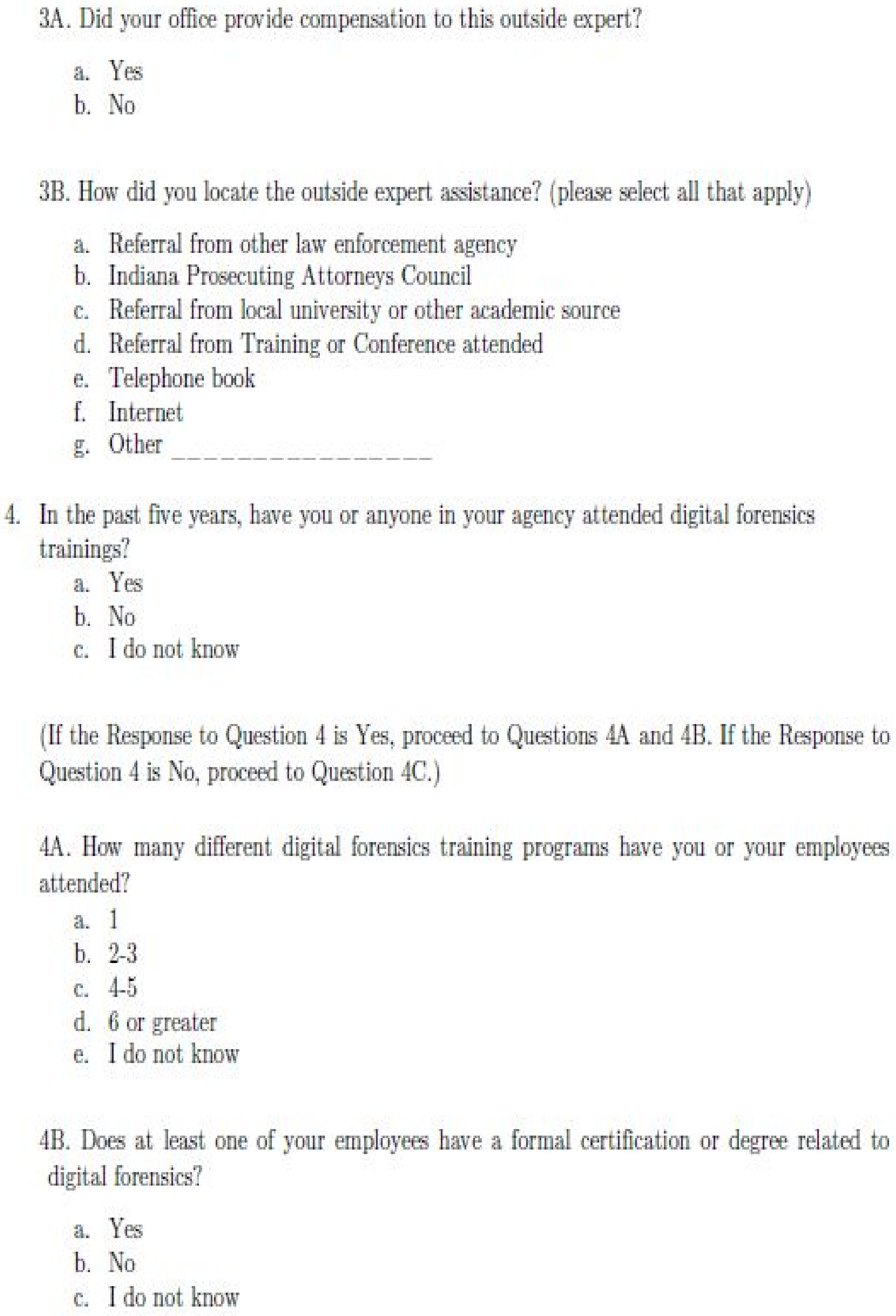
(If the Response to Question 2 is Yes, proceed to Question 2A. If the Response to Question 2 is No, proceed to Question 2B)

2A. Is this individual employed solely in the capacity of a digital forensics expert? (If the individual has other assigned job duties the proper answer is no.
   a. Yes
   b. No

2B. Please state the reason you do not have an individual employed as a digital forensics expert.
   a. Do not need an expert
   b. Do not have funding to employ an expert
   c. Unable to find a qualified expert
   d. Other ___________________

3. In the past five years, have you sought outside expert assistance with a digital crime investigation?
   a. Yes
   b. No

(If the Response to Question 3 is Yes, proceed to Questions 3A and 3B.



3A. Did your office provide compensation to this outside expert?

a. Yes
b. No

3B. How did you locate the outside expert assistance? (please select all that apply)

a. Referral from other law enforcement agency
b. Indiana Prosecuting Attorneys Council
c. Referral from local university or other academic source
d. Referral from Training or Conference attended
e. Telephone book
f. Internet
g. Other ________________

4. In the past five years, have you or anyone in your agency attended digital forensics trainings?
   a. Yes
   b. No
   c. I do not know

(If the Response to Question 4 is Yes, proceed to Questions 4A and 4B. If the Response to Question 4 is No, proceed to Question 4C.)

4A. How many different digital forensics training programs have you or your employees attended?

a. 1
b. 2-3
c. 4-5
d. 6 or greater
e. I do not know

4B. Does at least one of your employees have a formal certification or degree related to digital forensics?

a. Yes
b. No
c. I do not know

4C. Why have no officers/employees attended a digital forensics training program?

a. Training in this subject matter area is not needed
b. Officers do not have time to attend because of other job requirements
c. No interest from officers/employees on staff
d. No funding available for this type of training
e. Other ______________________

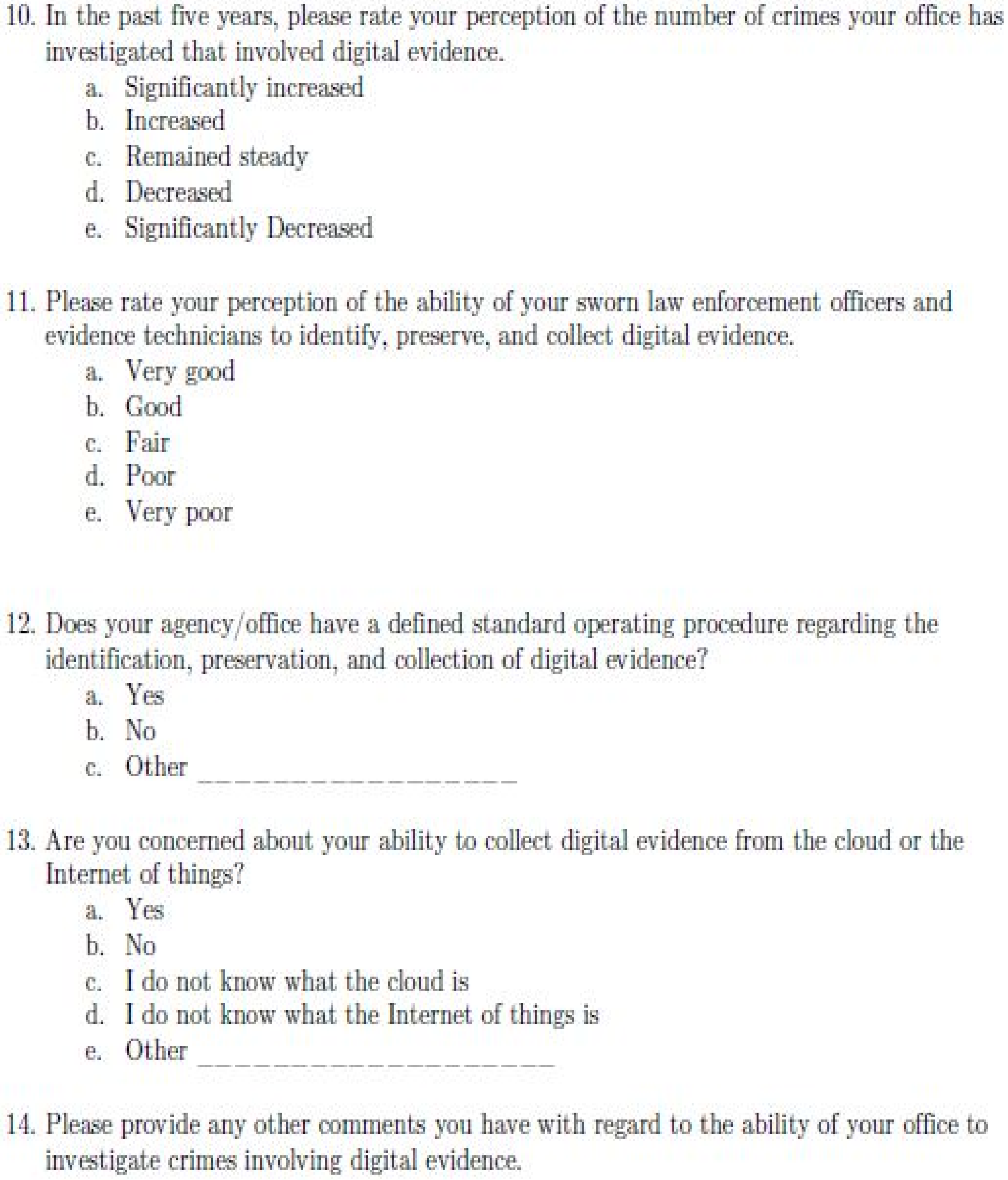
5. Where do you rank your agency's ability to effectively investigate a case involving digital evidence?
a. Very high
b. High
c. Medium
d. Low
e. Very low

6. Please rate your perception of the ability of your local Prosecuting Attorney's Office to present digital evidence at a hearing or a trial.
a. Extremely effective
b. Moderately effective
c. Effective
d. Somewhat effective
e. Not effective
f. Prefer not to answer

7. Please rate your perception of the ability of your local judges to understand digital evidence and its admissibility at trial.
a. Very high
b. High
c. Medium
d. Low
e. Very low
f. Prefer not to answer

8. Please rate your perception of the ability of your local juries to understand digital evidence when it is presented at trial.
a. Very high
b. High
c. Medium
d. Low
e. Very low
f. Prefer not to answer

9. Do you believe your office has adequate resources to effectively conduct an investigation of a crime involving digital evidence?
a. Yes
b. No
c. Other ____________________



10. In the past five years, please rate your perception of the number of crimes your office has investigated that involved digital evidence.
    a. Significantly increased
    b. Increased
    c. Remained steady
    d. Decreased
    e. Significantly Decreased

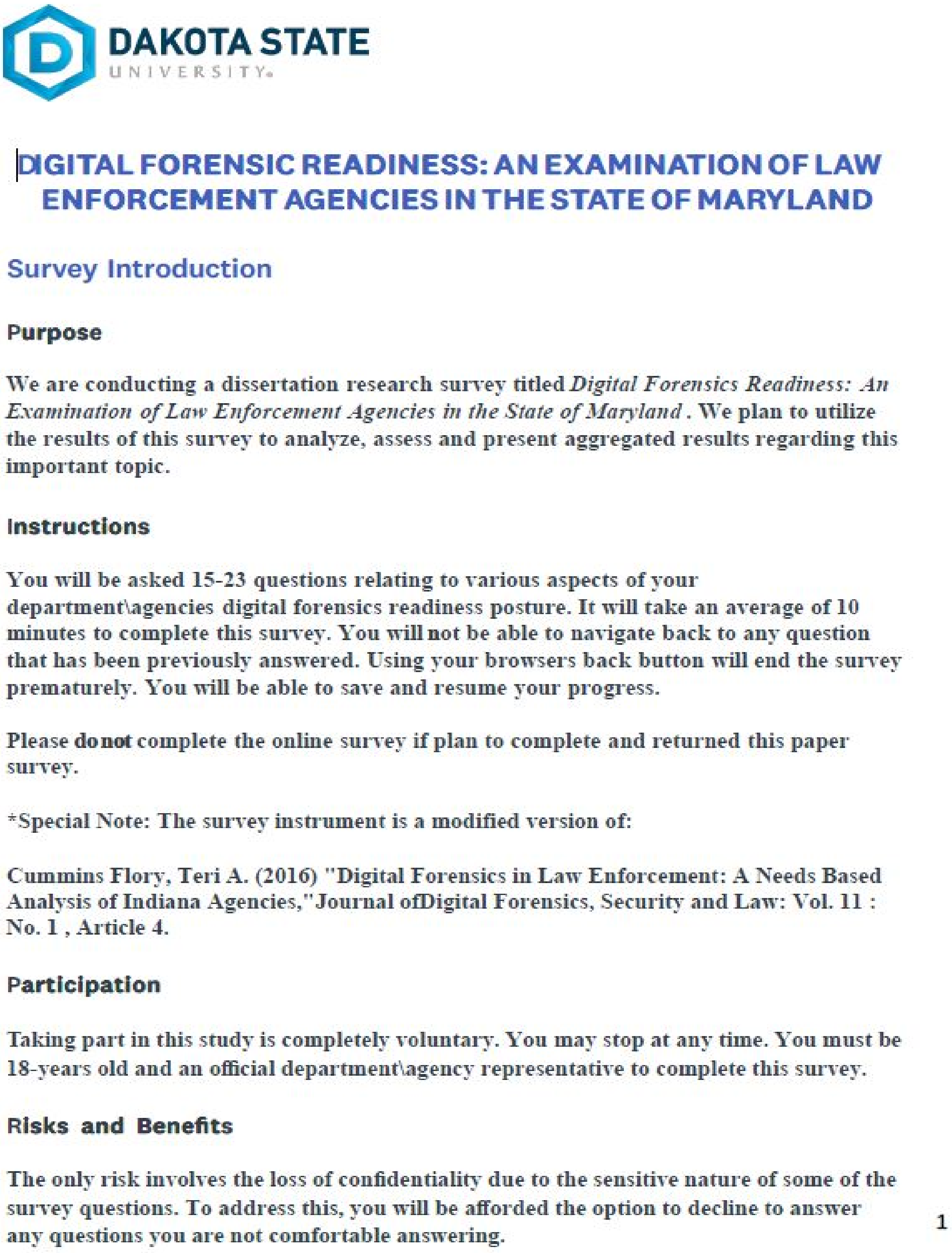
11. Please rate your perception of the ability of your sworn law enforcement officers and evidence technicians to identify, preserve, and collect digital evidence.
    a. Very good
    b. Good
    c. Fair
    d. Poor
    e. Very poor

12. Does your agency/office have a defined standard operating procedure regarding the identification, preservation, and collection of digital evidence?
    a. Yes
    b. No
    c. Other ___________________

13. Are you concerned about your ability to collect digital evidence from the cloud or the Internet of things?
    a. Yes
    b. No
    c. I do not know what the cloud is
    d. I do not know what the Internet of things is
    e. Other _____________________

14. Please provide any other comments you have with regard to the ability of your office to investigate crimes involving digital evidence.

APPENDIX D: SURVEY INTRODUCTION



DAKOTA STATE UNIVERSITY

DIGITAL FORENSIC READINESS: AN EXAMINATION OF LAW ENFORCEMENT AGENCIES IN THE STATE OF MARYLAND

Survey Introduction

Purpose

We are conducting a dissertation research survey titled ***Digital Forensics Readiness: An Examination of Law Enforcement Agencies in the State of Maryland*** **. We plan to utilize the results of this survey to analyze, assess and present aggregated results regarding this important topic.**

Instructions

You will be asked 15-23 questions relating to various aspects of your department\agencies digital forensics readiness posture. It will take an average of 10 minutes to complete this survey. You will not be able to navigate back to any question that has been previously answered. Using your browsers back button will end the survey prematurely. You will be able to save and resume your progress.

Please donot complete the online survey if plan to complete and returned this paper survey.

***Special Note: The survey instrument is a modified version of:**

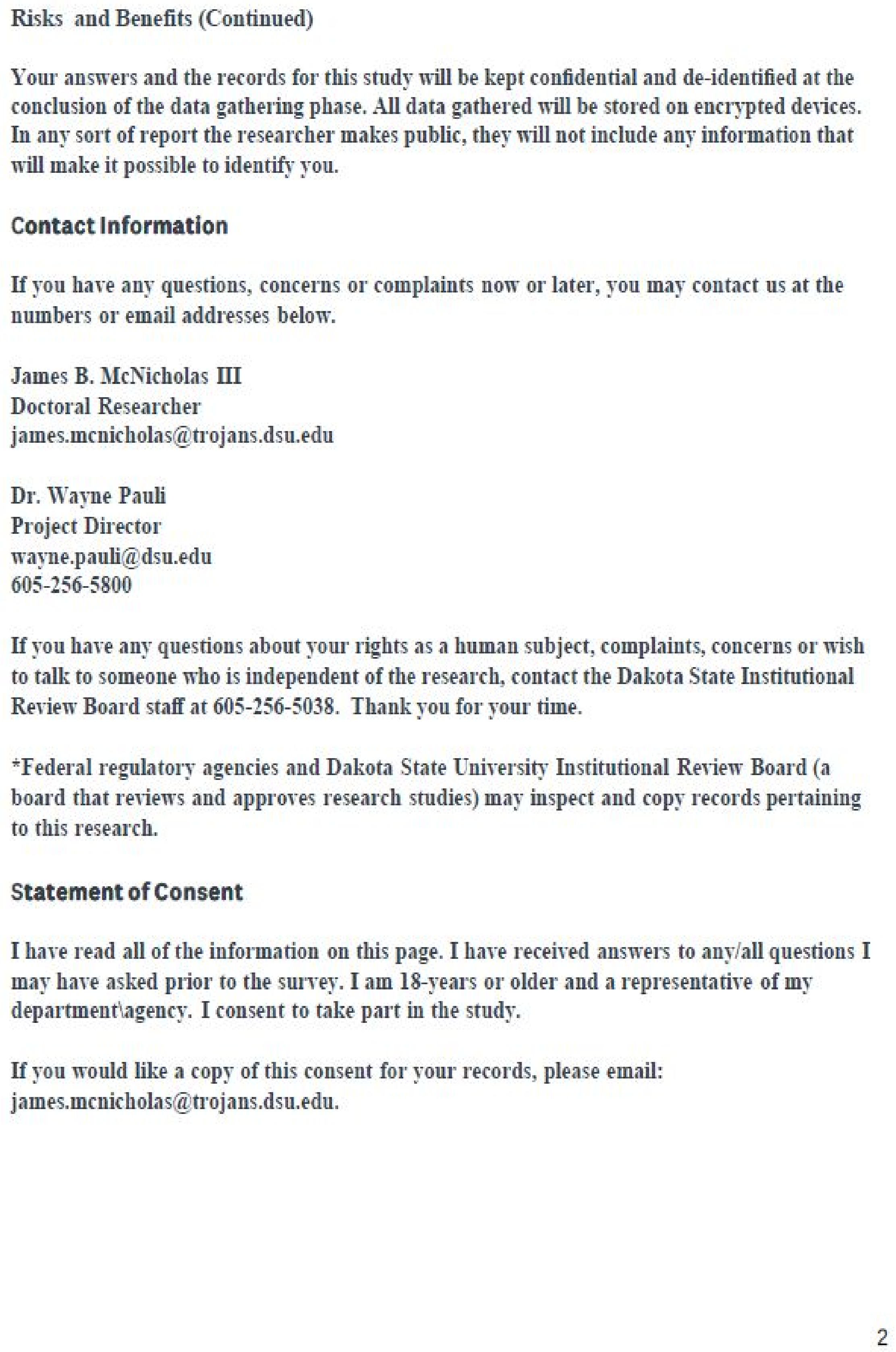
Cummins Flory, Teri A. (2016) "Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies,"Journal ofDigital Forensics, Security and Law: Vol. 11 : No. 1 , Article 4.

Participation

Taking part in this study is completely voluntary. You may stop at any time. You must be 18-years old and an official department\agency representative to complete this survey.

Risks and Benefits

The only risk involves the loss of confidentiality due to the sensitive nature of some of the survey questions. To address this, you will be afforded the option to decline to answer any questions you are not comfortable answering.



Risks and Benefits (Continued)

Your answers and the records for this study will be kept confidential and de-identified at the conclusion of the data gathering phase. All data gathered will be stored on encrypted devices. In any sort of report the researcher makes public, they will not include any information that will make it possible to identify you.

Contact Information

If you have any questions, concerns or complaints now or later, you may contact us at the numbers or email addresses below.

James B. McNicholas III
Doctoral Researcher
james.mcnicholas@trojans.dsu.edu

Dr. Wayne Pauli
Project Director
wayne.pauli@dsu.edu
605-256-5800

If you have any questions about your rights as a human subject, complaints, concerns or wish to talk to someone who is independent of the research, contact the Dakota State Institutional Review Board staff at 605-256-5038. Thank you for your time.

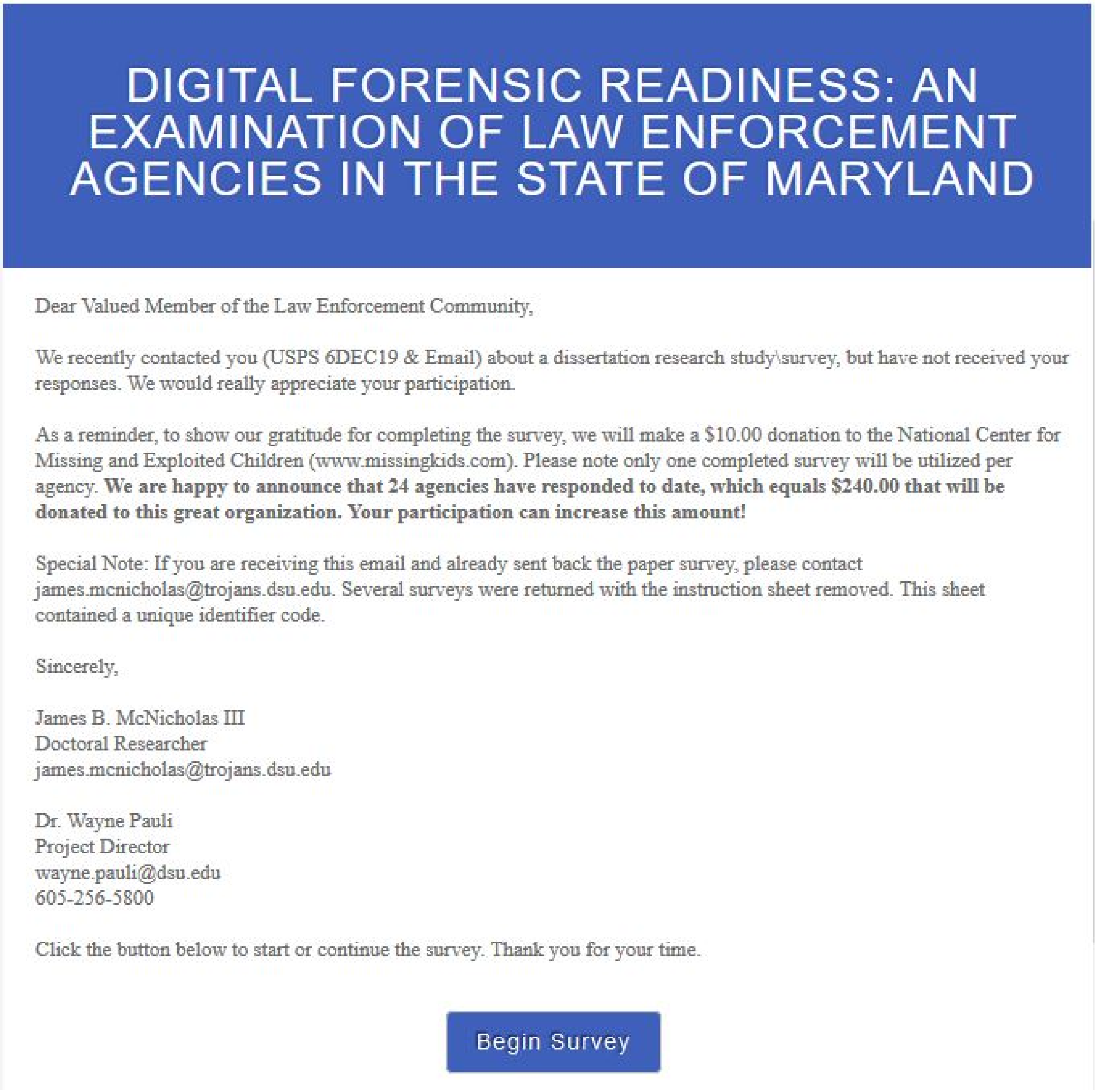
*Federal regulatory agencies and Dakota State University Institutional Review Board (a board that reviews and approves research studies) may inspect and copy records pertaining to this research.

Statement of Consent

I have read all of the information on this page. I have received answers to any/all questions I may have asked prior to the survey. I am 18-years or older and a representative of my department\agency. I consent to take part in the study.

If you would like a copy of this consent for your records, please email: james.mcnicholas@trojans.dsu.edu.

APPENDIX E: CONTACT EMAIL (REMINDER)



DIGITAL FORENSIC READINESS: AN EXAMINATION OF LAW ENFORCEMENT AGENCIES IN THE STATE OF MARYLAND

Dear Valued Member of the Law Enforcement Community,

We recently contacted you (USPS 6DEC19 & Email) about a dissertation research study\survey, but have not received your responses. We would really appreciate your participation.

As a reminder, to show our gratitude for completing the survey, we will make a $10.00 donation to the National Center for Missing and Exploited Children (www.missingkids.com). Please note only one completed survey will be utilized per agency. **We are happy to announce that 24 agencies have responded to date, which equals $240.00 that will be donated to this great organization. Your participation can increase this amount!**

Special Note: If you are receiving this email and already sent back the paper survey, please contact james.mcnicholas@trojans.dsu.edu. Several surveys were returned with the instruction sheet removed. This sheet contained a unique identifier code.

Sincerely,

James B. McNicholas III
Doctoral Researcher
james.mcnicholas@trojans.dsu.edu

Dr. Wayne Pauli
Project Director
wayne.pauli@dsu.edu
605-256-5800

Click the button below to start or continue the survey. Thank you for your time.