Analysis of Digital Forensic Capabilities in Texas Law Enforcement Agencies

By
Audrey N. Tepe
Amelia A. Boylan
Danny W. Davis, Ph.D.

The Bush School of Government and Public Service
Texas A&M University
November 4, 2019
TABLE OF CONTENTS

Introduction ................................................................. 3
Literature Review .......................................................... 4
Research Question ......................................................... 7
Methodology .................................................................... 8
Study Results ............................................................... 9
Conclusions ................................................................. 22
Recommendations ......................................................... 24
Future Research .......................................................... 24
Appendix A: DA Survey .................................................. 25
Appendix B: SO Survey .................................................. 28
Appendix C ..................................................................... 31
Author Biographies ..................................................... 32
INTRODUCTION

Technology has become an integral component of American society, permeating all domains whether social, economic, or political. The ever-evolving nature of technology has enabled advancements and achievements that were previously inconceivable. However, the United States’ reliance on technology has introduced a whole new class of threats. Technological advancements have increased criminal capabilities. Criminals have effectively adapted to the digital age. The escalating availability of technology, particularly mobile digital devices such as personal digital assistants (PDA), tablets, smartphone, e-readers, and computers, means that these devices are increasingly involved in criminal activity. This fact has resulted in a quantum increase of digital evidence that law enforcement agencies must collect, store, analyze, and process.¹

The field of digital forensics has emerged in order to investigate and analyze the forensic evidence obtained from digital sources. The National Initiative for Cybersecurity Careers and Studies (NICCS) defines digital forensics as collecting, processing, preserving, analyzing, and presenting “computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations”². Digital sources that may contain evidence can be categorized into:

1) “open computer systems” which consist of hardware,
2) “communication systems” which include “traditional telephone systems, wireless telecommunication systems, the Internet, and networks in general”, and
3) “embedded computer systems” such as “mobile devices, smart cards, and many other systems with embedded computers”.³

It is reasonable to infer that the majority of offenders in the United States possess or have access to at least one of these digital devices. Consequently it follows and that there is a high potential that a case will have a digital evidence component. Such evidence often proves to be a critical factor in prosecuting a given crime. In many cases, digital forensics must be leveraged by law enforcement entities in order to prevent and reduce crime.

This article examines literature regarding digital evidence and digital forensics in order to identify the key challenges facing criminal justice agencies. Then, applicable federal and Texas state laws that influence digital forensics and evidence collection are identified. Next, the research question for the conducted study is presented, followed by a description of the methodology used and an analysis of the results. Lastly, recommendations and concluding remarks are provided.

LITERATURE REVIEW

Despite a substantial amount of literature that discusses the challenges that agencies face regarding digital forensics, a study examining the digital forensic capabilities of policing and prosecuting agencies in Texas was not found. A relevant study was conducted in Indiana and was used to inform this current study’s methodology since the approach and topic were applicable to this study’s research. The following literature review serves to assess the relevant work produced on this topic and identify hurdles that agencies may encounter when working with digital evidence.

Amount of Data
A common hindrance agencies face concerning digital forensics is the vast amount of data that can accompany a case. The amount of seized devices per case, the amount of cases involving digital evidence, and the storage capability of devices have increased, resulting in a high volume of data for law enforcement agencies to analyze. The amount of personal data that can now be stored on digital devices has increased the complexity of the evidence collection process.

Furthermore, law enforcement agencies face varying requirements for different types of data. Basic subscriber data can be obtained with a subpoena, but transactional data requires a court order. Content data entails a more intricate process because it can only be obtained by a search warrant. Search warrants for personal devices present the “toughest standards for law enforcement officers” since they require detailed descriptions of the devices and data the agency wishes to obtain. The exceedingly large amount of data that can come with a case and its sensitive nature, brings to the forefront issues such as a lack of trained forensic technicians, backlogs due to vast amounts of data, and ever-present legal concerns.

Lack of Experts
Although digital evidence is prevalent in many cases, the number of individuals, knowledgeable of the digital evidence collection process is very limited. This lack of trained personnel or technicians can result in poor collection of digital evidence, missed digital evidence, and insufficient analysis of digital evidence that is collected. This issue is not easily remedied because the process to train officers in the basics of digital evidence is costly, averaging “$1,000 a day per officer”. The city of Austin, Texas has reportedly spent up to $40,000 to train just “five forensics examiners over a three-year period”. The time and financial burdens required for professional digital forensic training may be a deterrent for some agencies and entirely unmanageable for others. The challenge of employing personnel trained in digital

---

6 18 U.SC
8 Casey, E. 2011.
9 Ulloa, 2015.
10 Ulloa, 2015.
Forensics is compounded by the release of new devices and operating systems that require different methods to retrieve digital evidence.\textsuperscript{11} Furthermore, the officers, lawyers, and judges involved in cases requiring digital forensics may not possess an understanding of digital forensics or the laws inherent to this type of evidence.\textsuperscript{12} This can affect the stability of the case’s outcome as a study examining appellate cases found that the lack of specialized training for law enforcement officers regarding search and seizure methods and warrant acquisition for digital evidence was the largest problem courts faced.\textsuperscript{13}

**Backlog**
Due to the vast amount of data and lack of experts, the backlog for digital forensic collection and analysis is growing. Full examinations of forensic data can be time consuming, which has been a factor in even the largest digital forensic laboratories becoming backlogged.\textsuperscript{14} Texas departments may outsource digital forensic responsibilities to larger police departments, state agencies, federal agencies, state universities labs, or private companies. However, even forensic labs at large agencies, such as the Federal Bureau of Investigations (FBI), have faced backlogs up to nine months long while trying to assist surrounding departments with their digital forensics.\textsuperscript{15} In some cases, this backlog has resulted in sentence reductions for defendants, defendants committing suicide while awaiting trial, and innocent individuals falsely accused of child abuse not being able to see their children during the process.\textsuperscript{16}

**Tech Company Compliance and Law Enforcement**
Law enforcement obtaining digital evidence from tech companies presents further challenges, especially for agencies lacking experience or training in this area. The nomenclature used by law enforcement can vary from that used by tech companies which may result in multiple attempts to obtain information and a longer waiting period.\textsuperscript{17} Law enforcement must also remain up to date on current apps and websites which is a difficult task in the rapidly evolving field of technology. Even if an agency is able to complete that task, they still face the challenge of navigating each company’s individual standards and protocols for law enforcement to obtain information. Resources, such as search.org, exist to aid law enforcement with this challenge, however, the Internet Service Provider (ISP) database (ISP list) may not include the latest ISPs and some offices may not be familiar with such resources. This process can be made more complex when seemingly minute details result in only partial collection of digital evidence. For instance, when obtaining information from some tech companies, law enforcement can lose up to 11 hours of data content if they do not specify the use of coordinated universal time in their request. Requests to larger ISPs, such as Google and Apple, often result in secondary warrants

\textsuperscript{11} Ulloa, 2015.
\textsuperscript{13} Cole, Gupta, Gurugubelli, and Rogers, 2015.
\textsuperscript{15} Ulloa, 2015.
\textsuperscript{16} Shaw and Browne, 2013.
as new evidence comes to light, such as a suspect having multiple email addresses or phone numbers linked to an email.\textsuperscript{18}

The challenges of obtaining digital evidence from tech companies are compounded when the company is based internationally. Successfully acquiring data from internationally based companies can require a law enforcement agency to have knowledge of international law. Obtaining content data within the U.S. requires a search warrant, while obtaining content data internationally could require a Mutual Legal Assistance Treaty (MLAT) through the U.S. Department of State.\textsuperscript{19} The Clarifying Lawful Overseas Use of Data Act (CLOUD Act)\textsuperscript{20} was passed in 2018 to simplify this process, however, MLATs may still be required depending on the case.\textsuperscript{21}

\textbf{Legality Concerns}

The Fourth Amendment of the United States Constitution dictates the right of the people to be protected from “unreasonable searches and seizures.”\textsuperscript{22} Since digital evidence is relatively new, the application of the Fourth Amendment to digital evidence is equivocal.\textsuperscript{23} Additionally, common search and seizure procedures may not be sufficient in cases with digital evidence, resulting in the evidence not being admissible in court.

Researchers have identified many legal issues facing digital evidence, including the lack of a standardized practice for collecting digital evidence, expert qualifications, and translational barriers, such as difficulty translating typical criminal laws to cases with digital evidence. Poor search and seizure practices, errors with data analysis, presentation failures by experts, lack of preservation, inability to prove the authenticity of digital evidence, unauthorized access, and issues with sentencing are among the legal issues that have resulted in the reversal of appellate cases.\textsuperscript{24} There is not a standard procedure for digital evidence collection or warrant requirements for courts to uphold which can result in disputes regarding legality and admissibility.

\textbf{Federal and Texas State Laws}

Not only does the Fourth Amendment protect against unreasonable searches and seizures, it also establishes the standard of probable cause in order to issue warrants.\textsuperscript{25} Title 18, Chapter 119 of the United States Code (U.S.C) establishes the Electronic Communications Privacy Act (ECPA) of 1986. The ECPA has been updated over the years to remain applicable to current communication methods. The ECPA establishes the Wiretap Act, the Stored Communications Act, and 18 U.S. Code Chapter 206 which address pen registers and trap and trace devices.\textsuperscript{26} 18 U.S.C. Chapter 121, known as the Stored Communications Act (SCA), covers “stored wire and

\textsuperscript{18} Lundquist, 2019.
\textsuperscript{19} Lundquist, 2019.
\textsuperscript{20} Clarifying Lawful Overseas Use of Data Act., H.R. 4943, 115th Congress.
\textsuperscript{21} Lundquist, 2019.
\textsuperscript{22} United States Constitution. Amendment IV.
\textsuperscript{23} Cole, Gupta, Gurugubelli, and Rogers. 2015.
\textsuperscript{24} Cole, Gupta, Gurugubelli, and Rogers. 2015.
\textsuperscript{25} United States Constitution. Amendment IX.
electronic communications and transactional records access.” Chapter 18 of the Texas Code of Criminal Procedure (C.C.P) includes the legal procedures for search warrants, the interception of wire, oral, and electronic communications, tracking equipment, and access to communications and data.

The SCA and Chapter 18 of the Texas C.C.P outline the requirements of a subpoena, court order, or search warrant for obtaining different types of data. Texas C.C.P. Chapter 18.21 authorizes law enforcement to execute a search warrant within 11 days on communications stored out of the state of Texas. U.S.C. §2705(b) & §2703 and Texas C.C.P. Ch. 18.21 § 8 establish what is known as a non-disclosure or “gag” order. This order is critical for the preservation of information because it outlines procedures for delaying notification to a suspect for a period not exceeding 90 days. U.S.C. §2702 precludes voluntary disclosure by an ISP but includes exceptions, such as a provider being able to voluntarily disclose information to the government if it is willing. In cases where this occurs, law enforcement is able to bypass the process of obtaining a legal order. These statutes establish a foundation for digital evidence collection and attempt to address the challenges that emerge from its dynamic nature.

**RESEARCH QUESTION**

This study addresses the following research question.

To what degree is the Texas criminal justice system equipped with the necessary resources for investigating and prosecuting crimes that involve digital forensics?

In order to answer this question, data was gathered through a survey from Sheriffs’ offices (SO) and District Attorneys’ (DA) offices across Texas to determine:

- **R1.** The number of cases per office that require digital forensics.
- **R2.** The number of individuals trained in digital forensics per office and the type of training received; or the reason for not having an individual trained in digital forensics.
- **R3.** The amount of cases in which agencies sought outside expert assistance and the agency they sought outside expert assistance from.
- **R4.** The amount of cases in which digital forensic responsibilities were delegated and the agency to which the responsibilities were delegated.
- **R5.** The average amount of time, in days, for an office to complete the digital forensics process.
- **R6.** The degree of change, if any, to the number of crimes an office investigates that

---

27 18 U.S.C. § 2701-2713
28 Texas Code of Criminal Procedure. Ch. 18
29 Texas Code of Criminal Procedure. Ch. 18
30 Lundquist, 2019.
31 Lundquist, 2019.
32 18 U.S.C. § 2702
involves digital forensics within the past five years.

After acquiring the information above, it was possible to quantify the demand for digital forensics and the resources allocated for digital forensics in the responding Texas law enforcement agencies. This information was analyzed holistically in an effort to determine the digital forensic capabilities of Texas’ SO and DA offices.

METHODOLOGY

The survey group, Team AAD, used a mixed-methods approach with a convergent design in order to answer the research question. The literature review provided qualitative data that was assessed to determine the most common and substantial challenges that can hinder a law enforcement agency’s digital forensic capabilities. The survey responses provided quantitative data that was analyzed to determine the digital forensic capabilities of SOs and DA offices across Texas. Although some qualitative data informed the construction of the survey, a convergent design best describes the study’s approach because the qualitative and quantitative data were collected and analyzed separately then merged to interpret and compare the results.34

The quantitative data was gathered by distributing a survey to all 254 county SOs and a survey to all 254 counties’ DA offices. A cover letter included information about the purpose of the study and contact information for the research team, Team AAD. The survey provided the targeted audience with a definition for digital forensics; as, “the processes and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes”.35

First, the surveys were distributed by mail and offices were provided with the option to mail their survey back or take the survey online by using the link provided in the attached letter. This resulted in 103 surveys returned: 55 Sheriffs’ surveys and 48 DAs’ surveys. Next, information about the study with a link to take the survey was emailed to the offices that had not responded to the surveys sent by post. A reminder email was sent to offices who had received the original email and not taken the survey after approximately two weeks. Several emails were not publicly available or were no longer in use, resulting in the email not getting delivered to some offices. To address this, Team AAD made calls to the remaining offices a month after the original email was sent. The offices were asked if they could provide an email address for an individual, preferably someone involved with the office’s digital forensics, to complete the survey. Two weeks after these phone calls were made, the survey was closed and no new responses could be recorded.

All surveys taken electronically were immediately recorded in Qualtrics, an online survey system that was used to design and administer the survey. The surveys received through post were entered into Qualtrics as they arrived in order to consolidate the data. Several surveys received through post had errors, with the most frequent error being the selection of multiple answers. The surveys were entered into Qualtrics in a manner that reflected the respondents’

answers, including errors such as this. This affected the analysis slightly, however, it maintained the integrity of the respondent’s answers. Once the data was consolidated, duplicates of our surveys and responses were created to preserve the original data. In the duplicate data set, blank surveys were deleted, however, partial responses were included in our analysis in order to accurately display the entirety of information collected on a question. The results were interpreted using tools provided by Qualtrics. These tools consisted of summary statistics for each question, visualization of the data, and reports that were created with filters in order to determine more specific patterns.

**STUDY RESULTS**

There are a total of 254 Sheriffs’ offices and 254 counties with a District Attorney’s office in Texas. It is important to note that some District Attorneys’ offices oversee multiple counties, resulting in 162 District Attorneys’ offices in Texas. Therefore, the total population size, represented by N, for Texas District Attorneys’ offices and Texas Sheriffs’ offices is N=416. A total of 189 responses were received from Texas Sheriffs’ and District Attorneys’ offices. These 189 responses comprise the current study’s sample size, represented by n. Throughout the study, the sample size, or n, will vary based on the group that is being examined.

In terms of Sheriffs’ offices’ counties and District Attorneys’ offices’ districts (N=416), the study yielded a total survey response rate of 44.2%. Sheriffs’ offices accounted for 109 of the survey responses received, yielding a response rate of 42.9% (n=109). Of the survey responses received, 75 were from District Attorneys’ offices, accounting for 75 Texas districts, or 104 Texas counties. The response rate for District Attorneys’ office surveys was 46.3% by district (N=416) and 40.9% by county (N=508). For analysis, the District Attorneys’ office responses will be considered by district rather than county (n=75).

The responses were further analyzed in terms of the participating offices’ size. Of the participating District Attorneys’ offices, 61.3% of responses were received by offices
designated as small (n=46), or employing 0-5 prosecutors. Medium sized offices (n=16), consisting of 6-20 prosecutors, accounted for 21.3% of responses. Lastly, large offices (n=13) with 21-30+ prosecutors, were responsible for 17.3% of responses.

Out of the 109 Sheriffs’ office responses, 51.38% of responses were received from small offices (n=56), or Sheriffs’ offices that employ 0-25 officers. Offices with 26-100 officers were designated as medium sized (n=37) and were responsible for 33.94% of responses. Large offices (n=16), consisting of 101-250+ officers, accounted for 14.67% of responses.

**R1: Cases Per Office That Require Digital Forensics**

![Figure 2. Offices’ self-reported amount of cases involving digital evidence.](image)

**District Attorneys’ Offices.** Offices were asked to gauge the percentage of their office’s cases that involve digital evidence. Almost one-fourth, 22.66%, of respondents indicated that their office encountered less than 15% of cases that involve digital evidence. Contrarily, 20% reported that 90-100% of their cases involve digital evidence. Offices reporting a low percentage, 30% or less, of cases involving digital evidence accounted for 40% of participating districts. Roughly one-fifth, 21.33%, of respondents indicated that 31-75% of their office’s cases involve digital evidence. Almost 36% of participating agencies indicated a high percentage, 76% or higher, of cases that involve digital evidence.

Small offices (n=46) reported a low percentage of their cases involving digital evidence, with 45.65% reporting that 30% or less of their cases involve digital evidence. However, 21.73% of the small offices reported 90-100% of their cases involve digital evidence. Medium offices (n=16) were split with half reporting that 45% or less of their cases involve digital evidence and the other half reporting that 61-100% of their cases involve digital evidence. Large DAs’ offices (n=13) reported a higher amount of cases that involve digital forensics with over three-fourths (76.92%) of large offices reported that 61-100% of their office’s cases involve digital evidence.

**Sheriffs’ Offices.** When asked how many of their office’s cases involved digital evidence, 36.69% of SOs identified less than 15% of their cases. 22.01% of respondents selected that 16-
30% of their cases involve digital evidence and 11% of offices selected that 31-45% of their cases involve digital evidence. 11.92% of offices identified that roughly half, or 46-60% of their cases involve digital evidence. Five offices reported that 61-75% of their office’s cases involve digital evidence. 12.84% of respondents identified that 76-100% of their office’s cases involve digital evidence, with 8.25% of respondents reporting 90-100%.

Over 50% (51.78%) of small SOs (n=56) identified that less than 15% of their cases involve digital evidence. The medium-sized SOs (n=37) trended slightly higher than the small offices in the number of cases involving digital evidence, with 54.05% of respondents identifying up to 30% of their cases. Differing from small and medium SOs, the large offices acknowledged that more of their cases involve digital evidence, with 56.25% selecting the choices between 16-60%.

**R2A: Agencies That Do Not Have An Individual Trained In Digital Forensics**

When asked about the number of individuals trained in digital forensics, both DAs’ offices and SOs frequently identified that they had zero individuals trained. The most frequently identified reason for the lack of trained individuals was a lack of funding.

![Figure 3](image)

*Figure 3. Self-reported reason for not employing an individual trained in digital forensics.*

**District Attorneys’ Offices.** The majority of respondents, 54.66%, reported that their office has zero individuals trained in digital forensics. Offices that do not have an individual trained in digital forensics (n=41) were able to select one or more reasons for not having an individual trained. The majority of offices with no trained individuals, 82.92%, reported not having the funding to employ an individual trained in digital forensics. *Figure 3* shows the reasons that DAs’ and SO offices selected for not employing an individual trained in digital forensics. The offices that identified “other” reasons for not having an individual trained in digital forensics reported those reasons as reliance on law enforcement partners with trained personnel, lack of interest by district officials to fund an individual trained in digital forensics, funding not being worth the benefit, and the office not having any investigators.
The majority of small offices, 60.87%, answered that their office does not employ an individual trained in digital forensics. Small offices that reported not having an individual trained in digital forensics (n=28) largely identified lack of funding as the reason (85.71%). Of the small offices without a trained individual, 17.85% reported that their office does not need an individual trained in digital forensics and 17.85% reported that they are unable to find a qualified individual trained in digital forensics.

Three-fourths of medium offices answered that their office does not employ anyone who has received training in digital forensics (n=12). Medium DAs’ offices that do not employ an individual trained in digital forensics stated that they do not need an individual trained in digital forensics (33.33%) or that their office does not have the funding to employ an individual trained in digital forensics (75%).

Only one large office reported that their office does not employ an individual trained in digital forensics and stated that this is due to their reliance on other law enforcement entities with trained personnel.

**Sheriffs’ Offices.** There were 41.28% of SOs that reported their office has zero individuals trained in digital forensics (n=45). When selecting one or more reasons for not employing a trained individual, the majority of offices, 84.44%, identified a lack of funding. The 20% of offices that reported “other” reasons for not employing an individual trained in digital forensics identified those reasons as being the office’s use of outsourcing, access to trained individuals within their jurisdiction, scheduling conflicts, and lack of available classes or time.

Over half of small SOs, 51.78%, identified that their office has zero individuals trained in digital forensics (n=29). An overwhelming amount of these offices, 82.75%, identified their reason for not having individuals trained in digital forensics as a lack of funding to employ a trained individual. Over one-fourth, 27.58%, of small offices without a trained individual reported that they are unable to find a qualified individual trained in digital forensics.

One-third, 32.43%, of medium offices reported that their office does not have an individual trained in digital forensics (n=12). Almost all of these offices, 91.66%, identified a lack of funding as the reason they do not employ an individual trained in digital forensics. Of the medium offices with no trained individual, 16% reported not being able to find a qualified individual and 33% identified other reasons.

One-fourth of large offices reported that they do not employ an individual trained in digital forensics. Similar to their small and medium sized counterparts, the majority of large offices without a trained individual, 75%, identified funding as their reason.

**R2B: Agencies With Individual(s) Trained In Digital Forensics**

DAs’ offices and SOs that had one or more individuals trained in digital forensics most frequently acknowledged the individual(s) receiving training through Cellebrite. Figure 4 shows the trainings and certifications that DAs’ offices and SOs reported their individual(s) trained in digital forensics received.
Figure 4. Trainings and certifications received by individuals trained in digital forensics. See Appendix C for a list of the non-abbreviated trainings and certifications.

District Attorneys’ Offices. Just over one-third, 37.33%, of offices reported that their office employed 1-10 individuals trained in digital forensics. Only 6.66% reported more than 10 individuals trained in digital forensics, with three offices indicating more than 25 trained individuals. Offices with an individual trained in digital forensics (n=33) were asked to identify the type of training or certification the individual(s) had received. Offices were able to select multiple answers. The majority of trained individuals received their training through Cellebrite (51.51%) or other trainings and certifications not listed on the survey (54.54%). Offices identified the other trainings or certifications as general education and training through law enforcement, conferences, seminars, continuing education, and the Texas Commission on Law Enforcement (TCOLE).

Over one-third, 36.95%, of small DAs’ offices reported that their office had 1-5 individuals trained in digital forensics and only one office reported having 6-10 individuals trained in digital forensics. Individuals trained in digital forensics at small offices reported certifications in CDFE, BCERT, BICEP, MDE, MFT and CCFP and training through NW3C, NCFI, and Cellebrite.

One-fourth of medium offices reported having one or more individuals trained in digital forensics (n=4). Of the medium offices with one or more individuals trained in digital forensics, 50% reported their employee(s) receiving Cellebrite training and 75% answered “other”. The other trainings and certificates consisted of the GSFA certification, NCFI training, Secret Service training, and general training from digital evidence conferences.

Of the large offices, 84.61% reported employing one or more individuals trained in digital forensics. Slightly less than half, 46.15%, of large offices reported employing 2-10 individuals trained in digital forensics and 23% reported more than 25 individuals trained in digital
forensics. Large offices that selected “other” (38.46%) identified the other training or certifications as IACIS, CMDE, Blacklight, Magnet Forensic Examiner Certification, Teel Tech, LEVA, Oxygen training, CFVA, and CFVT.

**Sheriffs’ Offices.** Approximately 15% of SOs` denoted that they have 1 individual trained in digital forensics. About one-third of offices, 34.86%, elected 2-5 individuals trained and 4.58% of offices selected 6-10 trained individuals. Only one office reported having 11-15 trained individuals and two offices selected that they have more than 25 individuals trained in digital forensics. SOs with an individual trained in digital forensics (n=62) were asked to identify the trainings or certifications received by the employee(s) and were able to select multiple answers. Cellebrite was identified as the most prevalent training received with 45.16% of offices selecting it. “Other” was selected by 51.61% of offices and included TCOLE Cyber Crimes Certifications, NCFI certifications, on the job training, and general knowledge of cell phone forensics.

Small SOs reported that 41.07% have 1-5 individuals trained in digital forensics and 5% of small offices have more than 5 individuals trained in digital forensics. Small offices with one or more individuals trained in digital forensics (n= 26) reported Cellebrite training as the most prevalent training received by their employee(s) at 34.61%. The selection of “other” was selected most frequently at 61.53% and included on the job training, Texas Commission on Law Enforcement (TCOLE) Cyber Crimes certification, and National Computer Forensics Institute (NCFI).

The majority of medium offices, 67.56%, reported having at least one individual trained in digital forensics (n=25). Medium offices had a higher average of trained individuals than small offices with 45.9% of medium offices identifying 2-5 individuals trained in digital forensics. Similar to small offices, Cellebrite training was selected as the most prevalent training or certification at 36%.

Approximately two-thirds, 68.75%, of large offices reported employing at least one individual trained in digital forensics (n=11). Half of the large offices identified that they had 2-5 individuals trained in digital forensics, averaging slightly higher than the small and medium offices. Again, Cellebrite training was acknowledged as the overwhelming certification for the trained individuals at 81.81% with National White Collar Crime Center (NW3C) following at 45.45%.

**R3: Agencies That Sought Outside Expert Assistance**

For this study, seeking outside expert assistance for digital forensics responsibilities was defined as consulting with an outside agency for the information or resources necessary to process digital evidence. This may involve an office collaborating with, seeking guidance from, or utilizing the resources of another agency, but not being dependent on another agency for processing digital evidence. *Figure 5* shows the entities that DAs’ offices and SOs reported having sought outside expert assistance from.
District Attorneys’ Offices. The overwhelming majority, 82.66%, of DAs’ offices responding reported that their office has sought outside expert assistance for digital forensics in the past five years. The offices that had sought outside expert assistance in the past five years (n=62) were asked to identify the entity their office received expert assistance from. Offices were able to select one or more options. Offices most frequently reported having sought expert assistance from the Texas Department of Public Safety (DPS), 74.19% and FBI, 58.06%. Of the offices that received outside expert assistance, 22.58% reported receiving assistance from an entity that was not listed as an option on the survey. These other entities included the U.S. Secret Service, U.S. Department of Homeland Security, the U.S. Marshals, Cellebrite, and agencies with specialized Crimes Against Children units.

Offices that had sought outside expert assistance on digital forensics were asked to approximate the number of cases that they had sought outside expert assistance on in the past five years. 19.35% of these offices reported having sought outside expert assistance on 1-5 cases, 30.65% reported 6-15 cases, and 20.97% reported 16-25 cases. Approximately one-fifth (20.96%) of offices reported seeking outside expert assistance on somewhere between 26 and 100 cases in the past five years. Only 8.06% of offices that had sought outside expert assistance reported doing so on more than 100 cases in the past five years.

The majority of small offices, 80.43%, reported that they had sought outside expert assistance in the past five years (n=37). Small offices that had received outside expert assistance, largely reported receiving assistance from DPS (78.37%) or the FBI (48.64%). The majority of small offices that had sought outside expert assistance for digital forensics, 78.37%, reported doing so for 1-25 cases in the past five years.

Similar to small offices, the majority of medium DAs’ offices, 87.5%, had sought outside expert assistance for digital forensics in the past five years (n=14). Outside expert assistance was
received from DPS by 78.57% of medium sized offices and the FBI was used by 64.28% of medium offices that sought assistance. Five medium offices sought outside expert assistance from the Regional Computer Forensics Laboratory (RCFL), Texas Attorney General’s Office, and select municipal forensic laboratories. Medium offices that reported having sought outside expert assistance varied in the amount of cases they had sought assistance on within the past five years. The amount ranged from one to more than 100 cases, with 16-25 cases being reported most frequently.

The majority, 84.61%, of large DAs’ offices reported seeking outside expert assistance for digital forensics within the past five years (n=11). Large offices that had sought assistance most frequently received assistance from the FBI (81.81%), followed by DPS and municipal forensic laboratories (54.54% each). Nearly two-thirds (63.63%) of large offices that had sought outside expert assistance in the past five years did so for 1-25 cases and 36.36% did so for more than 75 cases.

**Sheriffs’ Offices.** Roughly four-fifths, 84.4%, of SOs reported having sought outside expert assistance on digital forensics within the past five years. The offices that had sought outside expert assistance in the past five years (n=92) were asked to identify the entity or entities their office received expert assistance from. Offices that had sought assistance most frequently selected DPS (65.21%) as the entity they received assistance from, followed by the FBI (31.52%). One-fourth of offices that had sought outside expert assistance reported receiving assistance from an entity that was not listed on the survey. These other entities included: U.S. Homeland Security Investigations, the U.S. Secret Service, the U.S. Marshals, the Texas Rangers, Bureau of Alcohol Tobacco and Firearms, U.S. Customs and Border Protection, and from agencies in neighboring jurisdictions.

SOs that had sought assistance were asked to identify approximately how many cases they had sought outside expert assistance for digital forensics on within the past five years. Of the offices that had sought assistance, 34.78% identified 1-5 cases and 30.43% identified 6-15 cases. Almost 12% of the offices elected 16-25 cases, 15.21% identified 26-50 cases, and 3.26% selected 51-75 cases within the past five years. Only one office that sought outside expert assistance reported doing so for 76-100 cases and five offices reported doing so for over 100 cases.

The majority of small offices, 82.14%, have sought outside expert assistance for digital forensics in the past five years (n=46). The small offices that have sought assistance identified receiving assistance from DPS most frequently, at 76.08%, followed by the FBI at 21.73%. The majority of small offices that sought outside expert assistance, 84.78%, did so for 15 or fewer cases over the past five years.

Medium offices predominantly (89.18%) reported having sought outside expert assistance for digital forensics within the past five years (n=33). Of the medium offices that sought assistance, 63.63% received assistance from DPS and 42.42% received assistance from the FBI. On average, medium offices sought outside expert assistance on more cases than small offices, with 84.84% of respondents identifying 50 or fewer cases in the past five years.

The majority of large offices, 81.25%, also reported having sought outside expert assistance for digital forensics in the past five years (n=13). Differing from the small and medium offices,
large offices that have sought assistance most frequently reported receiving assistance from a RCFL (46.15%), followed by the FBI (38.46%) and Municipal forensic laboratories (38.46%). On average, large offices sought outside expert assistance for more cases than small offices, with 76.92% reporting 1-25 cases.

**R4: Agencies that Delegated Digital Forensic Responsibilities**

Delegated responsibilities in this study was considered as the DAs’ office or SO relying entirely on another agency for the processing of a case’s digital evidence. Delegating digital forensic responsibility occurs when the DAs’ office or SO relinquishes the digital forensic responsibilities for a case to another agency. Therefore, when an office delegates digital forensic responsibilities, they are independent from the case’s digital forensic process. Contrary to delegating responsibility, obtaining outside expert assistance equips the DAs’ office or SO with the necessary knowledge or tools to perform digital forensics themselves. When seeking outside expert assistance, the office seeking assistance primarily performs the digital forensics for a case rather than outsourcing this responsibility.

<table>
<thead>
<tr>
<th></th>
<th>Sought Outside Expert Assistance</th>
<th>Delegated Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>DAs’ offices</td>
<td>82.66%</td>
<td>10.66%</td>
</tr>
<tr>
<td>SOs</td>
<td>84.40%</td>
<td>4.58%</td>
</tr>
</tbody>
</table>

*Figure 6. Comparisons by office between seeking outside expert assistance and delegating responsibility.*

*Figure 6* compares how frequently DAs’ offices and SOs sought outside expert assistance and delegated digital forensic responsibilities. Both DAs’ offices and SOs are more likely to seek outside expert assistance than to delegate their digital forensics responsibilities. However, approximately half of both DAs’ offices and SOs will delegate digital forensic responsibilities for at least one case.
District Attorneys’ Offices. DAs’ offices were asked if their office had delegated digital forensic responsibilities to another agency in the past five years. Approximately half (50.66%) of DAs’ offices reported delegating digital forensic responsibilities within the past five years, 33.33% reported not delegating responsibilities, and 10.66% did not know. Offices that delegated digital forensic responsibilities (n=38) reported delegating most frequently to DPS (65.78%) and the FBI (52.63%). Slightly less than 20% of offices reported delegating digital forensic responsibilities to other agencies, including the Secret Service, larger neighboring agencies, and Houston Metro Internet Crimes Against Children (ICAC) Task Force.

Offices approximated the number of cases that their office has delegated digital forensic responsibilities for in the past five years. Offices that had delegated responsibilities most frequently reported doing so for 6-15 cases (34.21%) followed by more than 100 cases at 21.05%. Of the offices that delegated responsibilities, 1-5 cases were reported as delegated by 13.15% of offices, 16-25 cases by 10.52% of offices, and 26-50 cases by 7.89% of offices. 5.26% of offices that delegated responsibilities reported doing so for 51-75 cases and 76-100 cases each.

Small DAs’ offices were split when asked if they delegated digital forensics responsibilities with 41.3% reporting they delegated responsibilities and 41.3% reporting they had not. Small offices that delegated (n=19) reported typically delegating digital forensic responsibility to DPS (63.15%), FBI (36.84%), Texas Attorney General’s Office (31.57%), and municipal forensic laboratories (31.57%). 78.94% of offices that delegated responsibilities did so for 1-25 cases in the past five years, with 6-15 cases being reported most frequently.

In the past five years, 62.5% of medium DAs’ offices have delegated digital forensic responsibilities to another agency (n=10). Of the medium offices that delegated responsibilities, 90% delegated to DPS, 70% to the FBI, 40% to a RCFL, and 40% to the Texas Attorney
General’s Office. Both private forensic laboratories and municipal forensic laboratories were selected by 30% of medium offices each. Of the medium offices that delegated digital forensic responsibilities, 60% delegated for 6-50 cases and 20% delegated for more than 100 cases in the past five years.

Of large DAs’ offices, 69.23% elected that they delegated digital forensic responsibilities within the past five years (n=9). Of the large offices that delegated responsibilities, 66.66% delegated to the FBI, 66.66% to municipal forensic laboratories, 44.44% to DPS, and 33.33% to county forensic laboratories. Large offices that delegated responsibilities reported doing so for more than 100 cases (55.55%), followed by 6-15 cases (22.22%), then 51-100 cases (22.22%).

Sheriffs’ Offices. Approximately 45% of SOs reported delegating digital forensic responsibilities to another agency within the past five years, 33.02% reported not delegating responsibilities, and 11.92% did not know. The offices that delegated responsibilities (n=49) most frequently delegated to DPS (59.18%), followed by the FBI’s Regional Computer Forensics Laboratory (RCFL) that was delegated to by 22.44% of offices each. Of offices that delegated digital forensic responsibilities, 20.4% reported delegating to an agency that was not listed on the survey. These other agencies include Homeland Security Investigations, the Secret Service, the Texas Rangers, ATF, and their county’s DA’s office.

SOs that delegated digital forensic responsibilities were asked to select the amount of cases, on average, that their office delegated responsibilities for within the past five years. Of the offices that delegated responsibilities, 40.81% reported doing so for 1-5 cases, 30.61% for 6-15 cases, and 24.48% for 16-25 cases. 4.08% of offices reported delegating for 26-75 cases, 4.08% for 76-100, and 6.12% for more than 100 cases in the past five years.

Approximately 43% of small offices reported delegating digital forensic responsibilities to another agency within the past five years (n=24). The majority of small offices, 70.83%, reported delegating digital forensic responsibilities to DPS. In the past five years, 66.66% of small offices that delegated responsibilities reported doing so for 1-5 cases and 33.33% reported doing so for 6-15 cases.

Approximately half, 51.35%, of medium offices acknowledged that they delegated digital forensic responsibilities to another agency within the past five years (n=19). The offices that delegated responsibilities reported delegating to the DPS (57.89%), FBI (36.84%), and RCFL (31.57%) most frequently. Medium SOs identified that they delegated digital responsibilities on more cases than small offices, with 47.36% identifying 16-25 cases and 47.36% identifying 15 or fewer cases.

Differing from their small and medium counterparts, large offices were less likely to delegate digital forensics responsibilities with only 37.5% of large offices reporting that they delegated responsibilities in the past five years, and 50% reporting that they had not. Of the large offices that delegated responsibilities (n=6), half delegated to a RCFL and 33.33% delegated to a municipal forensic laboratory. 66.66% of offices that delegated digital forensic responsibilities did so for 6-25 cases and 16.66% did so for 76-100 cases.

R5: Average Time For an Office to Complete the Digital Forensics Process
Offices were asked to approximate the number of days it takes for digital forensics to be completed for a case in their office. Some offices specified that the amount of days varies based upon the electronic device, especially because digital forensics on cell phones can typically be done in the office.

![Average Amount of Days for Digital Forensics to be Completed for a Case](image)

*Figure 8. Self-reported amount of days, on average, for digital forensics to be completed for a case by office.*

**District Attorneys’ Offices.** The amount of time for digital forensics to be completed for DAs’ offices’ cases averaged towards the middle of 61-90 days. The most frequently selected choice by DAs’ offices was 91-150 days, with 22.66% of DAs’ offices making this selection. Figure 8 shows the average amount of days for digital forensics to be completed for a case as reported by both DAs’ offices and SOs.

Small offices reported digital forensics averaging at the lower end of 61-90 days to be completed for a case. An average of 91-150 days was reported most frequently, with 19.56% of small offices selecting this answer. Medium offices reported a higher number of days for digital forensics to be completed for a case, with the average resting at the low end of 91-150 days. One-fourth of medium offices reported digital forensics taking an average of 151-250 days and one office reported an average of 301-350 days for digital forensics to be completed for a case. Large offices most frequently reported (38.46%) digital forensics taking an average of 1-30 days to be completed for a case and 23.07% reported digital forensics taking an average of 91-150 days. Less than 8% (7.69%) of offices reported digital forensics taking an average of 61-90 days, 151-200 days, and 251-300 days each.

**Sheriffs’ Offices.** The average amount of time for digital forensics to be completed for SOs’ cases was at the high end of 31-60 days. Of SOs, 32.11% reported digital forensics taking an average of 1-30 days per case, 17.43% reported 31-60 days on average, and 13.76% reported an average of 151-200 days.
Small SOs reported digital forensics averaging at the high end of 31-60 days to be completed for a case. Small office most frequently reported digital forensics taking 1-30 days to be completed for a case and one-fourth reported digital forensics taking an average of 91-200 days to be completed. Medium offices most frequently reported digital forensics averaging between 31-60 days to be completed for a case. 10.81% of medium offices identified that digital forensics takes an average of 91-150 days to be completed for a case and 10.81% identified an average of 151-200 days. Large offices (37.5%) most frequently identified digital forensics taking an average of 31-60 days to be completed on a case. Three-fourths of large offices reported that it takes less than 90 days for digital forensics to be completed on a case.

R6. Variation in the Number of Crimes that Involve Digital Forensics
DA’s offices and SOs were asked to approximate the degree of change, if any, to the number of crimes their office investigates that involve digital forensics within the past five years. Figure 9 reflects both offices’ answers.

![Figure 9](image)

*Figure 9. Self-reported amount of change, if any, to the number of crimes each office investigated that involve digital forensics within the past five years.*

**District Attorneys’ Offices.** The overwhelming majority of offices, 77.33%, reported that the amount of crimes their office has investigated involving digital forensics has increased, to some degree, in the past five years. Over half, 52%, of DAs’ offices reported the number has significantly increased. No DAs’ offices reported that the number of crimes involving digital forensics has significantly decreased in the past five years.

Small offices most frequently reported (47.82%) that the number of crimes their office has investigated that involved digital evidence has significantly increased in the past five years. Of small offices, 23.91% reported the number has increased, 17.39% reported the number has remained steady, and one small office reported the number has decreased. The vast majority, 87.5%, of medium offices reported that the number of crimes their office has investigated involving digital evidence has increased, to some degree, in the past five years. Half of medium
offices answered that the number of their cases involving digital forensics has significantly increased and 12.5% of medium offices reported that the number had remained steady within the past five years. All large offices that responded to this question indicated that the number of crimes their office has investigated involving digital forensics has increased, to some degree, within the past five years. Close to 70% (69.23%) of large offices reported that this number had significantly increased and 15.38% reported this number had increased.

**Sheriffs’ Offices.** SOs most frequently reported (62.38%) that the amount of crimes their office has investigated that involve digital forensics has increased, to some degree, in the past five years. Of SOs, 34.86% indicated the number has significantly increased and 27.52% indicated the number has increased. Almost one-fourth (23.85%) of offices identified that the number has remained steady and only 4.58% selected that the number has decreased.

Over half of small offices, 51.78%, reported that the number of crimes their office has investigated involving digital evidence has increased, to some degree, in the past five years. About 23% indicated the number had significantly increased and 28.57% indicated the number had increased. Slightly less than one-third (30.35%) of small offices reported that the number had remained steady and 8.92% reported that the number had decreased. Medium offices most frequently reported (40.54%) that the number of crimes their office has investigated involving digital evidence has significantly increased in the past five years. Approximately one-fourth (24.32%) of medium offices indicated that the number had increased and 24.32% indicated that the number had remained steady. The majority of large offices, 62.5%, selected that the number of crimes their office has investigated involving digital evidence has significantly increased in the past five years. Of large offices, 31.25% reported that the number had increased in the past five years.

**CONCLUSIONS**

The literature review discussed the challenges Texas SOs and DAs’ offices may face when collecting, analyzing, and utilizing digital evidence. The most notable challenges include: 1) the amount of data; 2) lack of trained digital forensics experts; 3) backlog; 4) compliance with tech companies’ procedures, and other legal concerns. The responses of 184 Texas DAs’ offices and SOs provided results to gauge the digital forensic capability of Texas law enforcement agencies. The study also allows for an assessment of the literature review’s proposed challenges of the amount of data, lack of digital forensics experts or trained personnel, and backlog on Texas law enforcement agencies.

The amount of cases that involve digital forensics averaged at the high end of 31-45% for DAs’ offices and the high end of 16-30% for SOs. However, the majority of both DAs’ offices and SOs reported that the number of crimes involving digital forensics that their office has investigated increased or significantly increased in the past five years. This reported increase, combined with the increasing prevalence of mobile digital technology in our society, suggests that the amount of cases involving digital evidence that Texas DAs’ offices and SOs encounter will continue to grow. These results also suggest that Texas DAs’ offices and SOs can be hindered by the vast amount of digital data that the literature review identified as posing a challenge for law enforcement.
Over half, 54.66%, of DAs’ offices and 41.28% of SOs responded that their office does not have an individual trained in digital forensics. The vast majority of both DAs’ offices and SOs identified a lack of funding as the reason their office does not have an individual trained in digital forensics. These responses suggest that Texas law enforcement agencies face the challenge of a lack of a digital forensic experts or personnel trained in digital forensics. Furthermore, this challenge disproportionately impacts small and medium DAs’ offices and SOs throughout Texas. The lack of individuals trained in digital forensics likely contributes to the high percentage of DAs’ offices (82.66%) and SOs (84.4%) seeking outside expert assistance on digital forensics. Both DAs’ offices (50.66%) and SOs (44.95%) also reported delegating digital forensic responsibilities to another agency altogether. The most frequently reported agencies that DAs’ offices and SOs sought outside expert assistance from or delegated digital forensic responsibilities to, were the Texas DPS and the FBI (see Figures 5 & 7). Both the DPS and FBI investigate cases of their own that likely require digital forensics and assisting other law enforcement agencies could increase their own agency’s backlog. This suggests that the challenge Texas DAs’ offices and SOs face regarding a lack of personnel trained in digital forensics might be transposed on larger agencies, contributing to a greater backlog at the state and federal level.

The amount of days for digital forensics to be completed for a case averaged at the high end of 31-60 for SOs. The average was higher for small and medium offices, suggesting that smaller offices may be impacted more frequently by backlog. This is problematic because the study’s sample reflected that Texas consists of a higher amount of small and medium SOs, rather than large offices. DAs’ offices had a higher mean than SOs, with DAs’ offices reporting that the amount of days for digital forensics to be completed for a case averaged towards the middle of 61-90 days. For DAs’ offices, backlog most commonly affects medium offices which reported that the amount of days for digital forensics to be completed for a case averaged at the low end of 91-150 days. Comments provided by a handful of Texas DAs’ offices and SOs suggest that this number might be skewed towards the lower end of the scale due to the short amount of time that it takes for digital forensics to be completed on cellular devices.

The study’s findings suggest that the Texas criminal justice system is not adequately equipped with the necessary resources for investigating and prosecuting crimes that involve digital forensics. This is further supported by a statement from one DA’s office that reported not using the digital evidence that their cases have because they are unable to process it. Texas agencies have used a collaborative, inter-agency approach to minimize the negative effects of this. However, this approach does not solve the problem and, in some cases, can contribute to related problems, such as backlog at larger agencies.

This study shows that the volume of digital evidence handled by law enforcement agencies in Texas is on the increase. This is a trend that will not end. As a statewide issue it is clear that the funding associated with training digital forensics experts needs to grow in order to match these trends. Prioritizing and funding digital forensics in Texas would increase efficiency by shortening the amount of time and resources required for a case to be completed, resulting in a higher disposition of cases. Shortened case time would also benefit defendants and their families who may be paying for legal expenses, as well as crime victims and their families from enduring more trauma through an extensive legal process. Prioritizing and funding digital forensics would reduce backlog and decrease dependency on larger agencies, further reducing
the backlog of larger agencies and allowing those agencies more time to focus on their individual missions. Funding for training and hiring digital forensics personnel could help protect Texas’ vulnerable populations by significantly increasing offices’ abilities to combat predatory crimes that typically have a digital component, such as crimes against children and human trafficking.

As indicated in this study, this is a state-wide issue.

RECOMMENDATIONS

1. The Texas State Legislature prioritize for the appropriation of funds for training and hiring personnel in the digital forensics field.

2. Both State and county agencies should seek federal government grant funding for training and hiring personnel in the digital forensics field.

FUTURE RESEARCH

This study surveyed Texas District Attorneys’ offices and Texas Sheriffs’ Offices in order to answer the research question: To what degree is the Texas criminal justice system equipped with the necessary resources for investigating and prosecuting crimes that involve digital forensics? In order to better gauge the digital forensic capabilities of the States’ criminal justice system, this study could be expanded to include survey analysis of Texas municipal police departments and County Attorney’s offices. Additionally, state and federal entities that perform digital forensics for Texas cases could be surveyed to better understand their capabilities and involvement. In order to improve the qualitative portion of the research, a more comprehensive review of relevant literature could be performed and further examination of state and federal legislation could be conducted. Further qualitative research could include policies and procedures that guide local digital forensic practices.
Appendix A - District Attorney’s Office Survey

For this survey, digital forensics will be defined as "The processes and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes" (Definition provided by The National Initiative for Cybersecurity Careers and Studies).

1. How many prosecutors does your agency employ?
   a. 0-5
   b. 6-10
   c. 11-15
   d. 16-20
   e. 21-25
   f. 26-30
   g. More than 30

2. Approximately how many of your office's cases involve digital evidence?
   a. Less than 15%
   b. 16-30%
   c. 31-45%
   d. 46-60%
   e. 61-75%
   f. 76-90%
   g. 90-100%

3. How many people does your office employ who have received training in digital forensics?
   a. 0
   b. 1
   c. 2-5
   d. 6-10
   e. 11-15
   f. 16-20
   g. 21-25
   h. More than 25

3A. If your agency has one or more individuals trained in digital forensics, what kind of training or certification did they receive?
   a. CFCE - Certified Forensic Computer Examiner
   b. CCE - Certified Computer Examiner
   c. CDFE - Certified Digital Forensics Examiner
   d. CSFA - Cyber Security Forensic Analyst
   e. CCFP - Certified Cyber Forensics Professional
   f. ACE - AccessData Certified Examiner
   g. EnCE - EnCase Certified Examiner
   h. GIAC - Global Information Assurance Certification
   i. GCFA - GIAC Certified Forensic Analyst
   j. NW3C - National White Collar Crime Center training
k. Cellebrite training
l. CompTIA training
m. Other _________________________________________________________

3B. If your agency does not employ an individual trained in digital forensics, please state the reason your office does not have an individual trained in digital forensics
   a. Our agency does not need an individual trained in digital forensics
   b. Our agency does not have the funding to employ an individual trained in digital forensics
   c. Our agency is unable to find a qualified individual trained in digital forensics
   d. Other________________________________________________________

4. In the past five years, has your office sought outside expert assistance for digital forensics?
   a. Yes
   b. No
   c. I do not know

4A. If your agency has sought outside expert assistance, where did your office get assistance for digital forensics?
   a. FBI
   b. Regional Computer Forensics Laboratory (RCFL)
   c. DPS
   d. Texas Attorney General's Office
   e. Private forensic laboratory
   f. University forensic laboratory
   g. County forensic laboratory
   h. Municipal forensic laboratory
   i. Other _________________________________________________________

4B. If your office has sought outside expert assistance in the past five years, approximately how many cases has your office sought outside expert assistance for digital forensics on?
   a. 1-5
   b. 6-15
   c. 16-25
   d. 26-50
   e. 51-75
   f. 76-100
   g. More than 100

5. In the past five years, has your office delegated digital forensics responsibilities to another agency?
   a. Yes
   b. No
   c. I do not know

5A. If your agency has delegated digital forensics responsibilities, what agency did your office delegate digital forensics responsibility to?
a. FBI
b. Regional Computer Forensics Laboratory (RCFL)
c. DPS
d. Texas Attorney General's Office
e. Private forensic laboratory
f. University forensic laboratory
g. County forensic laboratory
h. Municipal forensic laboratory
i. Other _______________________________________________________

5B. If your agency has delegated digital forensics responsibilities in the past five years, approximately how many cases has your office delegated digital forensics responsibilities for?
   a. 1-5
   b. 6-15
   c. 16-25
   d. 26-50
   e. 51-75
   f. 76-100
   g. More than 100

6. How many days, on average, does it take for digital forensics to be completed for a case?
   a. 1-30
   b. 31-60
   c. 61-90
   d. 91-150
   e. 151-200
   f. 201-250
   g. 251-300
   h. 301-350
   i. More than 350 days

7. In the past five years, the number of crimes that your office has investigated that involved digital evidence has:
   a. Significantly increased
   b. Increased
   c. Remained steady
   d. Decreased
   e. Significantly decreased
Appendix B - Sheriff’s Office Survey

For this survey, digital forensics will be defined as "The processes and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes" (Definition provided by The National Initiative for Cybersecurity Careers and Studies).

1. How many officers does your agency employ?
   a. 0-25
   b. 26-50
   c. 51-75
   d. 76-100
   e. 101-125
   f. 126-150
   g. 151-175
   h. 176-200
   i. 201-225
   j. 226-250
   k. 250+

2. Approximately how many of your office's cases involve digital evidence?
   a. Less than 15%
   b. 16-30%
   c. 31-45%
   d. 46-60%
   e. 61-75%
   f. 76-90%
   g. 90-100%

3. How many people does your office employ who have received training in digital forensics?
   a. 0
   b. 1
   c. 2-5
   d. 6-10
   e. 11-15
   f. 16-20
   g. 21-25
   h. More than 25

3A. If your agency has one or more individuals trained in digital forensics, what kind of training or certification did they receive?
   a. CFCE - Certified Forensic Computer Examiner
   b. CCE - Certified Computer Examiner
   c. CDFE - Certified Digital Forensics Examiner
   d. CSFA - Cyber Security Forensic Analyst
   e. CCFP - Certified Cyber Forensics Professional
   f. ACE - AccessData Certified Examiner
   g. EnCE - EnCase Certified Examiner
h. GIAC - Global Information Assurance Certification
i. GCFA - GIAC Certified Forensic Analyst
j. NW3C - National White Collar Crime Center training
k. Cellebrite training
l. CompTIA training
m. Other _______________________________________________________

3B. If your agency does not employ an individual trained in digital forensics, please state the reason your office does not have an individual trained in digital forensics
   a. Our agency does not need an individual trained in digital forensics
   b. Our agency does not have the funding to employ an individual trained in digital forensics
   c. Our agency is unable to find a qualified individual trained in digital forensics
   d. Other _______________________________________________________

4. In the past five years, has your office sought outside expert assistance for digital forensics?
   a. Yes
   b. No
   c. I do not know

4A. If your agency has sought outside expert assistance, where did your office get assistance for digital forensics?
   a. FBI
   b. Regional Computer Forensics Laboratory (RCFL)
   c. DPS
   d. Texas Attorney General's Office
   e. Private forensic laboratory
   f. University forensic laboratory
   g. County forensic laboratory
   h. Municipal forensic laboratory
   i. Other _______________________________________________________

4B. If your office has sought outside expert assistance in the past five years, approximately how many cases has your office sought outside expert assistance for digital forensics on?
   a. 1-5
   b. 6-15
   c. 16-25
   d. 26-50
   e. 51-75
   f. 76-100
   g. More than 100

5. In the past five years, has your office delegated digital forensics responsibilities to another agency?
   a. Yes
   b. No
   c. I do not know
5A. If your agency has delegated digital forensics responsibilities, what agency did your office delegate digital forensics responsibility to?
   a. FBI
   b. Regional Computer Forensics Laboratory (RCFL)
   c. DPS
   d. Texas Attorney General's Office
   e. Private forensic laboratory
   f. University forensic laboratory
   g. County forensic laboratory
   h. Municipal forensic laboratory
   i. Other

5B. If your agency has delegated digital forensics responsibilities in the past five years, approximately how many cases has your office delegated digital forensics responsibilities for?
   a. 1-5
   b. 6-15
   c. 16-25
   d. 26-50
   e. 51-75
   f. 76-100
   g. More than 100

6. How many days, on average, does it take for digital forensics to be completed for a case?
   a. 1-30
   b. 31-60
   c. 61-90
   d. 91-150
   e. 151-200
   f. 201-250
   g. 251-300
   h. 301-350
   i. More than 350 days

7. In the past five years, the number of crimes that your office has investigated that involved digital evidence has:
   a. Significantly increased
   b. Increased
   c. Remained steady
   d. Decreased
   e. Significantly decreased
Appendix C - Abbreviations for Trainings and Certifications

ACE - Access Data Certified Examiner
BCERT - Basic Computer Evidence Recovery Training
BICEP - Basic Investigation of Computer and Electronic Crimes Program
CCE - Certified Computer Examiner
CCFP - Certified Cyber Forensics Professional
CDFE - Certified Digital Forensics Examiner
CFCE - Certified Forensic Computer Examiner
CFVA - Forensic Video Analyst Certification
CFVT - Certified Forensic Video Technician
CMDE - Certified Mobile Device Examiner
CSFA - Cyber Security Forensic Analyst
EnCE - EnCase Certified Examiner
GCFA / GSFA - GIAC Certified Forensic Analyst
GIAC - Global Information Assurance Certification
IACIS - International Association of Computer Investigative Specialists
LEVA - Law Enforcement & Emergency Services Video Association
MDE - Mobile Device Examiner
MFT - Mac Forensics Training
NCFI - National Computer Forensics Institute
NW3C - National White Collar Crime Center training
AUTHOR BIOGRAPHIES

Dr. Danny W. Davis
Dr. Danny W. Davis is a retired Army lieutenant colonel. An infantryman, he spent much of his 20-year career with airborne, ranger, and special forces units. Upon leaving the service Danny worked overseas in a Department of State sponsored training program. He then spent six years in public education running a high school Junior ROTC program. He has also done consulting work for the US Army in the area of homeland security. With Texas A&M University’s Bush School since 2010, Danny is an associate professor of the practice, his areas of interest are terrorism and cybersecurity policy. Danny holds two degrees from Texas A&M: a bachelor's in history and a Ph.D. in education. His master's in international relations was earned at Troy State University. He and his wife Mary live and raise cattle on the Lost Dog Ranch near Old Dime Box, Texas.

Amelia A. Boylan
Amelia A. Boylan is a second year at The Bush School of Government and Public Service at Texas A&M University where she is pursuing her Master of Public Service and Administration with a concentration in Security Policy and management. She is also working towards a Certificate in Homeland Security from the Bush School. She is a graduate of the United States Military Academy at West Point, where she majored in International Relations. She was commissioned as an U.S. Army Aviation Officer in 2010 and went to the U.S. Army’s flight school at Ft. Rucker, AL where she learned to fly the AH-64 Apache helicopter. She deployed to Afghanistan in 2013 from Ft. Riley, KS. Amelia served as an Army Aviator until November of 2017. She currently lives in Houston, TX with her daughter and husband. BEAT NAVY!

Audrey N. Tepe
Audrey Tepe is a student and Graduate Research Assistant at the Bush School of Government and Public Service at Texas A&M University. She is studying for her Master of Public Service and Administration with a concentration in cybersecurity. She is also studying to obtain IT and cybersecurity certifications through CompTIA. Audrey holds a Bachelor of Science degree from Texas A&M University with a major in University Studies Leadership and double minors in psychology and sociology. She has interned with the Brazos County District Attorney’s Office, Brazos County Sheriff's Office, and Texas A&M Cybersecurity Center. She is a Medical Accompaniment Volunteer and family advocate for her county's Child Advocacy Center.