Forensic Science International: Synergy 6 (2023) 100296

Contents lists available at ScienceDirect

Forensic Science International: Synergy

journal homepage: www.sciencedirect.com/journal/forensic-science-international-synergy

A survey of prosecutors and investigators using digital evidence: A starting point☆

Christa M. Miller *

Christa M. Miller Communications LLC, 2607 Woodruff Rd. Ste. E404, Simpsonville, SC, 29681, USA

ARTICLE INFO

Keywords:
Prosecution
Digital evidence
Forensic service
Training
Decision making
Case building
Criminal justice

ABSTRACT

Digital evidence is essential to criminal investigations and prosecutions, but its use is fraught with challenges: rapid changes in technology, the need to communicate those changes to stakeholders, and a sociopolitical landscape that leaves little room for error, particularly regarding electronic data privacy. In the criminal justice system, these challenges can affect the admissibility of evidence and its proper introduction at trial, as well as how cases are charged and resolved. A survey of 50 United States (U.S.)-based prosecutors, contextualized by data from a second survey of 51 U.S.-based investigators, explores these issues for the present and future, finding that crucial factors include training, prosecutors who specialize in digital evidence issues, and strong relationships between prosecutors and investigators.

1. Introduction

By one estimate, digital evidence is a factor in about 90% of criminal cases [1]. As law enforcement investigations themselves become more digitized, their complexity rises along with the volume of data being managed [2]. Yet the traditional criminal justice system has struggled to adapt. With digital forensics having evolved as an investigative rather than a forensic discipline [3], emphasis on law enforcement success may have come at the expense of fair-trial discussions and requirements. [2].

For example, factors including metadata validation, "the lack of consensus regarding the needs in digital evidence processing," the insufficiency of "methods and tools from ten years ago," and "interconnected criminal justice issues that go beyond law enforcement's typical role in collecting evidence" are all part of "a multifaceted challenge" which prosecutors contend with by proxy: "Compared with the chain of custody for physical evidence, that for digital evidence is much more complex, volatile, and difficult to reliably maintain. Prosecutors must prove that only authorized persons had access to the evidence and guarantee that copies and analyses were made by authorized manipulations and using acceptable methods." Another challenge includes digital evidence backlogs, which could in turn complicate prosecutors' decision-making: to charge, for one, or plea bargain, for another [4].

Yet in spite of an estimated 11,000 digital forensics laboratories across the United States [5], prosecutors often have a poor understanding of digital data's relevance to their cases, or how to use the evidence [4]. Of course, defendants always have the right to challenge the evidence against them, and a judge can reject a plea for insufficent evidence [6]. However, whether defendants and their attorneys have the technical ability or financial resources to meaningfully contest digital evidence—and whether judges can effectively evaluate the issues [7]—could render these kinds of challenges moot [8].

At the same time, so few cases ever make it to trial [9] that the chances are slim that any evidence—digital or not—would be admitted. One review of 145 cases appealed in U.S. federal circuit courts between 2010 and 2015 found that only 22 "were based on the science of computer forensics, including probative value, authenticity, hearsay, relevancy, and scientific merit." [10].

These kinds of issues contribute to a fraught landscape for prosecutors, at a time when U.S. prosecutors' offices have come under greater scrutiny in recent years [11], including for their approach to certain kinds of forensic evidence [12]. Indeed, noted one report on prosecutor priorities: "Prosecutors are expected to deliver fair and legitimate justice in their decisionmaking while balancing aspects of budgets and resources, working with increasingly larger volumes of digital and electronic evidence that have developed from technological advancements (such as social media platforms), partnering with communities and other entities, and being held accountable for their actions and differing litigation strategies." [13].

☆ This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.
* Corresponding author.
E-mail address: research@christammiller.com.

https://doi.org/10.1016/j.fsisyn.2022.100296
Received 28 December 2021; Received in revised form 6 November 2022; Accepted 4 December 2022
Available online 30 December 2022

The extent to which digital evidence factors into any of these "big picture" issues is unknown, but as digital evidence is used in increasingly controversial prosecutions [14]—while the U.S.'s roughly two million prisoners continue to lead the world in total number of people incarcerated [15]—it is worth questioning whether the U.S. justice system has reached a point where the effectiveness of its current processes and procedures must be rethought. Towards that end, the stark gap between the extent to which digital evidence is relied upon, and its apparent reliability, was the foundation for the research described in this paper. Particularly how prosecutors and investigators around the country interact with digital evidence, and with one another, has perhaps never been more germane to a free society's notions of justice. This research, combining two surveys and a set of follow-up interviews, sought to better understand these interactions.

1.1. Definitions

The following terms are used throughout this paper and should be understood to be defined as:

- **Digital evidence/digital forensic evidence** consists of data captured from digital devices, used to investigate and prosecute criminal cases.
- **Digital data** consists of data captured from devices but not necessarily used as evidence.
- **Third party data/evidence** refers to data captured from platforms operated by a third party, such as a cellular service or social media company.
- **Low-hanging fruit** refers to digital data that is easy to obtain, either from a device or a third-party platform e.g. a publicly facing (unlocked) social media account.

As a caveat, however, these definitions were not provided to survey respondents, though the terms "digital evidence" and "third party data" were differentiated in some questions. That said, some respondent interviewees reflected the way they interpreted the questions. For example, one respondent said to her, "digital evidence" means social media, phones, and computers as opposed to digital surveillance videos and cellular tower sites. Another differentiated between seizures of device data from someone's home, for example, and seizures of bank records or other third-party data which may be in a digital format but are fundamentally more about traditional forensic accounting or other investigative methods.

2. Methodology

Survey participants were recruited from two different e-mail listservs—one dedicated to high tech crime investigation, and the other dedicated to prosecutors specializing in digital evidence—as well as from a prosecutor-oriented training course at the National Computer Forensics Institute. As a result, the prosecutor and investigator respondents are not necessarily connected by jurisdiction.

The surveys were built using Google Forms. With moderators' approval, emails were sent to the two listservs describing the authors, the project, the survey, and the intended outcome (to assess training needs as well as assist in policy development). Respondents were informed that results would be anonymized, though they would have the option to provide their email if they agreed to be available for comment. They were also informed that results would be available for review by any participant and might be the subject of a publication or publications. None of the respondents were compensated for participating in the survey.

The original survey consisted of eight questions for both respondent groups, 29 questions for prosecutors, and 21 questions for investigators. First, a series of demographic questions were asked regarding where respondents were located, the size population they serve, how many people are employed in their own agency, whether those people specialize or can be considered generalists, whether they can rely on a prosecutor dedicated to high tech, and the respondent's own years of experience.

These and the following, process-oriented questions consisted primarily of multiple choice, with a mix between "pick one" and "check all that apply." The former included some questions in which respondents were asked to estimate about how much of their time – segmented into percent ranges, e.g. 0–20%, 20–40%, etc. – digital evidence factors into. Additionally, several of the questions asked respondents to rate their experiences or opinions according to scales of 1–5, "never" to "usually," etc.

Only the first eight questions required responses. Respondents had the option to skip questions within their own sections. Although some respondents skipped some questions, especially when they weren't relevant to the respondent's own experience, this was not a common occurrence and none of the respondents failed to complete the full survey.

Because the survey was an independent project that started as a way to obtain data for journalism research, the author neither sought nor obtained approval from an Institutional Review Board to work with human subjects. However, all participants were made aware that the survey results as well as interview participants' comments were intended for publication.

A link to each Google Form was sent in September 2019, and the data collection period lasted through the end of October. Two reminder emails were sent during this time. A total of 55 respondents – 51 investigators, and four prosecutors – came from the first survey. From the prosecutor-oriented survey came a total of 46 respondents, to which the responses from the four prosecutors in the original survey were added.

In sum, results from 51 investigators and 50 prosecutors were evaluated. The investigator respondents consisted of detectives performing a blend of investigative and digital forensic work, though they were not queried on the extent to which they themselves specialize in digital forensics.

The survey included an open answer field where respondents could provide their email address for followup. Of the investigator respondents, 13 provided email addresses where they could be contacted for followup, though for lack of time, no followup interviews were conducted with this cohort. Of the prosecutor respondents, 15 provided email addresses where they could be reached for followup.

Of these 15, 11 participated in follow-up interviews between December 2020 and March 2021, with some additional followups in June and July 2021. Interview questions sought context for these interviewees' survey responses, to lend insight into what might have driven them. Interviewees were informed that their names and organizations might be directly quoted, and were given the opportunity to either not participate in the interviews, or to have their identities anonymized. Interviews were recorded and transcribed, and interviewees had the opportunity to review and approve their quotes for inclusion in the final publication.

3. Survey respondent demographics and experience

Rather than a 1:1 comparison between prosecutors and the investigators they work with, the survey sought to attain a general sense of what each group was experiencing in their regional locations, communities, and offices.

3.1. Prosecutor and investigator demographics

Generally speaking, prosecutors from larger jurisdictions—some including state attorney general offices—responded to the survey relative to investigators, who represented a broader range of local, county, and state agencies serving different population sizes.

More than half of the prosecutor survey respondents were located on

the US East Coast. A little less than one-third responded from the West Coast, with the remainder in the middle of the country. In contrast, more than half of the investigator respondents came from the US West Coast. East Coast-based investigators accounted for fewer than one-quarter of responses, and again, the remaining respondents were based in the middle of the country (see Fig. 1).

However, regional locations didn't suggest that most respondents came from metropolitan population centers. Most respondents represented mid-size communities, working in city, county, or district attorney's offices or local, county, or state law enforcement agencies; none of the respondents came from federal law enforcement or U.S. attorneys' offices (see Fig. 2).[1]

Along similar lines, about 40% of the prosecutor respondents came from offices with under 100 people, but about half came from much larger organizations. The proportions were roughly similar for investigators (see Fig. 3).

3.2. Experience with digital evidence

When it came to longevity, the proportions of experience were roughly the same across both groups. Very few respondents had less than two years—or more than 20 years—of experience with digital evidence. The range of experience was between two and 10 years across a vast majority of both groups, roughly corresponding with the degree to which digital evidence has become integral to criminal cases. Still, the investigators tended to have a longer range of experience than the prosecutors (see Fig. 4).

Whether the slight experience gap between prosecutor and investigator respondents is good, bad, or neutral is unclear. On one hand, technology changes so rapidly and in such profound ways that experience may matter less than good technical skills and a hunger for continuous learning. Several prosecutors reflected in follow-up interviews that they are computing or technology enthusiasts.

Others found themselves in the digital technology niche as a result of assignments or cases they worked, then, recognizing its importance, grew their expertise from there. For example, they read articles or communicate with forensic examiners about why it may not be possible to retrieve a piece of evidence, or self-educate on legal or constitutional,

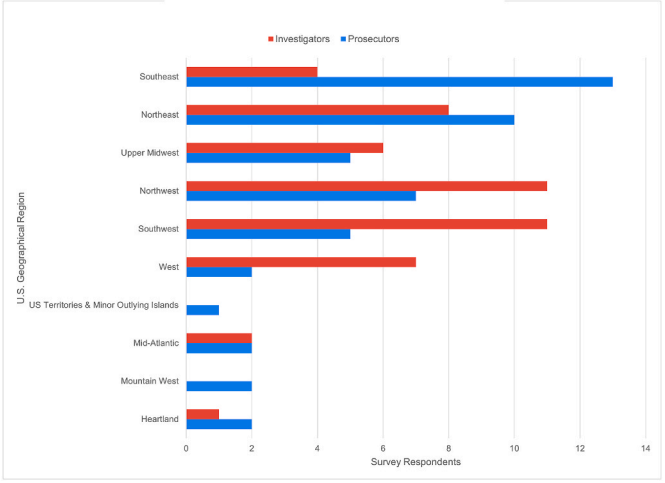

Fig. 1. A higher proportion of prosecutors—nearly 50 percent—responded from the eastern part of the United States, and were about evenly split between the Northeast and Southeast. That proportion was reversed for investigators, who responded in similar proportions from the West.

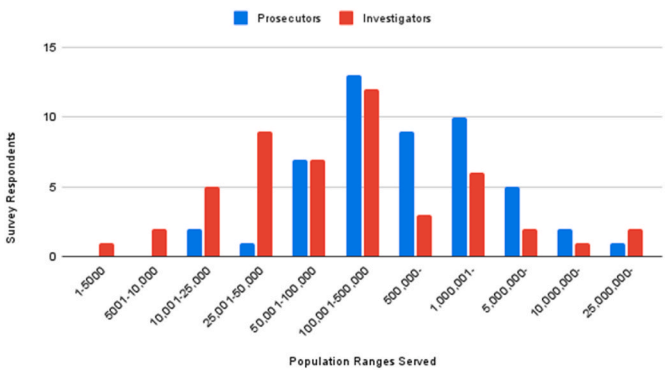

Fig. 2. More prosecutors from larger jurisdictions responded to the survey, while the investigator respondents represented a broader range of populations served.

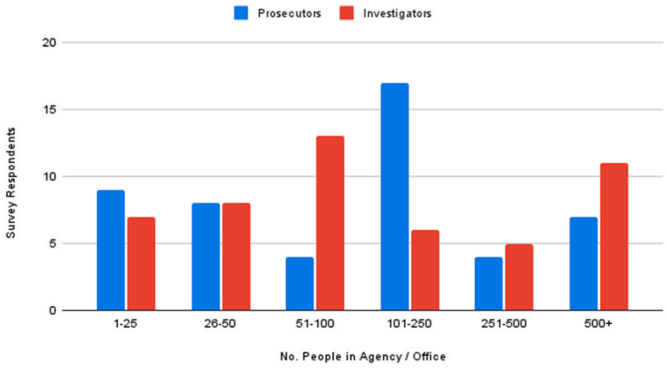

Fig. 3. More than half of the prosecutor respondents came from offices staffed by 100+ people, but the same proportion came from much smaller offices. The investigators were somewhat more evenly distributed.

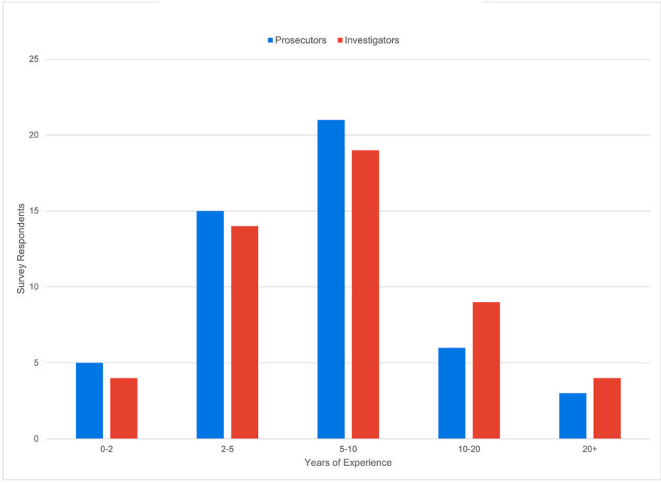

Fig. 4. The overwhelming majority of prosecutor respondents had between two and ten years of experience with digital evidence, but more investigators have greater longevity of experience than prosecutors.

[1] The surveyed investigators overwhelmingly work in law enforcement agencies that are outside the domain of the prosecutors' offices they work with. Many prosecutors' offices do employ law enforcement investigators to investigate the cases that police bring them. Their involvement can range from working alongside police department or sheriff's office counterparts in an initial investigation, to follow up work after a defendant is charged and preparing for trial. That so few survey respondents work in this capacity isn't necessarily cause for concern. Rather, the context they offer for later parts of the survey is specific to law enforcement agencies rather than prosecutors' offices.

rather than technological or procedural questions.

On the other hand, prosecutors and investigators with fewer years of experience may not have the perspective on digital trends that those with longer experience do. Thus, because the main purpose of this research was to learn whether prosecutors make different decisions (charge, plea, or dismiss cases) based on digital evidence, the survey questioned whether the respondents' experience included access to colleagues who specialize in law pertaining to digital evidence.

Specialization is understood to enable prosecutors' offices to more effectively and consistently implement and even innovate on best practices [16], including the support of "more-efficient case development and proceedings in complex cases." [13] Although the survey didn't specify what "specialist" meant, in a digital evidence context, a specialist prosecutor may offer a variety of types of assistance including:

- Assisting with less widely used devices or platforms.
- Answering questions on the significance of a piece or set of data to their case.
- Developing search warrant and subpoena templates for investigators to use to obtain records from third party companies like internet or electronic service providers and telecoms.
- Coming up with protocols for introducing digital evidence at trial, and/or even training prosecutors in their state on understanding different aspects of digital evidence.
- Communicating the reliability of digital evidence.
- Helping other prosecutors understand how to lay a foundation to introduce digital evidence.
- Navigating a defense challenge to digital evidence in the middle of trial.
- Reviewing electronic warrants.

J.D., an assistant state's attorney in a Southeastern state, argues that for prosecutors, specializing comes down to the ability to more quickly identify what might be important. "An investigator can be very good," J. D. explained, "but there may be something specific that I want for trial or that I think sheds light on something that they may not know to look for." In turn, his involvement can help to ascertain what kind of legal process will be needed and thus, potentially obtain evidence more quickly. Further, understanding digital evidence allows J.D. to internalize the full spectrum of evidence to figure out what to introduce in court and how to present it, from juror-friendly chat conversations to timelines.

Most survey respondents—representing about two-thirds of both prosecutor and investigator groups—are generalists working multiple types of cases. In larger jurisdictions, investigators and prosecutors both reflected the presence of general crime or trial assignments, and specialized ones for homicides, fraud, gangs, and sex crimes among other types of crime, versus types of evidence.

Even so, by a substantial margin, more prosecutor than investigator survey respondents said their agency had a prosecutor dedicated to digital evidence. Investigators overwhelmingly, even in larger agencies, said they have no such dedicated prosecutor to rely on (see Figs. 5 and 6).

A better sense of these disparities comes from comparing responses across jurisdictional populations. Although to some extent, the responses reflect the number of respondents from each population size, they also show surprising inconsistency (see Fig. 7).

For example, far fewer investigators from jurisdictions serving between 100,000 and 1,000,000 people reflected that they could rely on a prosecutor specializing in digital evidence, even though more prosecutors from similarly sized jurisdictions said their offices had such a specialist on staff.

Follow-up interviews provided more context into these disparities. First, prosecutor specialists function in dedicated roles and units in only some district attorneys' offices. They might advise all prosecutors, or else be limited to devices or platforms that were either the instrument or

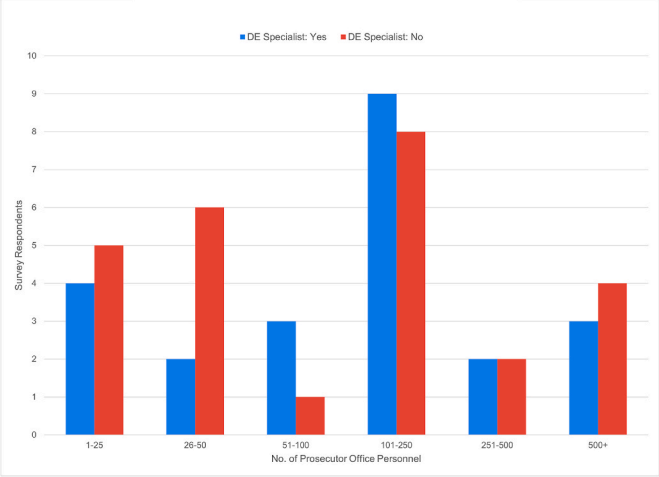

Fig. 5. The most prosecutor respondents from mid-size offices—those with between 51 and 250 prosecutors—reflected the existence of a digital evidence specialist.

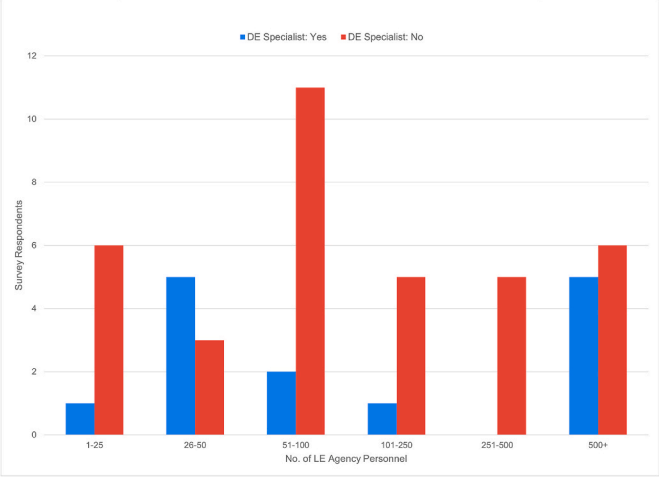

Fig. 6. In contrast to the prosecutor respondents, the investigator respondents, even in larger agencies, said they have no prosecutor dedicated to digital evidence issues.

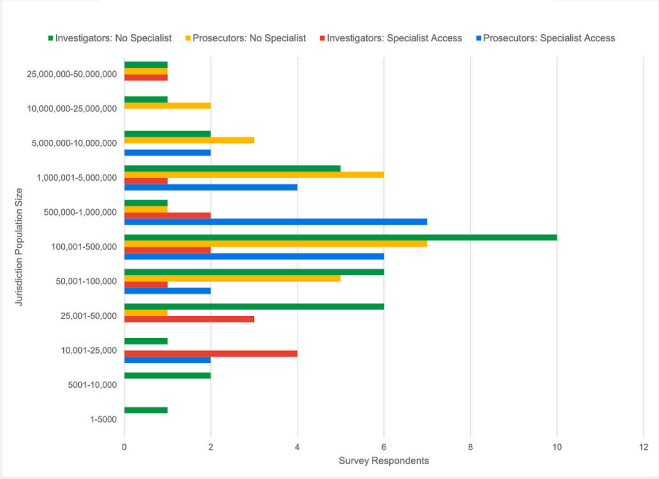

Fig. 7. Comparing responses from the two groups reflects disparities in the extent investigators can rely on prosecutors from various jurisdictional sizes.

the target of crime: cyberstalking, child exploitation, or intellectual property theft.

In smaller jurisdictions, interviewees reflected that a dedicated prosecutor specialist might exist, but work centrally. In one northeastern state with a population of about 1.3 million, for instance, some 80 prosecutors can turn to a specialist at the attorney general's office, who serves as legal counsel for the state police computer crimes unit.

Still other specialists provide legal advice in an informal capacity, especially if their colleagues know them from having acted in an officially designated role, as a training provider, or in a related activity. J.S., an assistant attorney general in a Mountain West state, is one example of a prosecutor who has "developed an interest or an expertise in something through working a specific case or kind of case in the past," whose colleagues then seek out their advice and recommendations.

Again, however, these technology-focused prosecutor respondents are the exception, not the rule. J.D. believes many prosecutors are overwhelmed by what they don't understand, so they place more trust in law enforcement analysts, who may or may not have the experience they need, nor the legal expertise, to carry a case.

Still, one problem remains for those who specialize: the potential for liability. Prosecutors engaged in the prosecutorial function have absolute immunity from liability for Constitutional violations, while investigators are subject to qualified immunity. V.J., a prosecutor on the West Coast, observed that courts take a narrow view of a prosecutor's specialty. Thus, he said, when prosecutors offer legal counsel to investigators, such as reviewing language for legal process, they are engaging in an investigative function. V.J. added that judges reviewing a prosecutor's immunity apply a standard of whether a prosecutor knew better, or should have known better, when they stepped outside of their role. Under that standard, prosecutors can be liable for deficiencies in a search warrant they review.

Other issues may also be in play. Notably, few respondents—about one-quarter of investigators, compared to less than one-fifth of prosecutors—have more than 10 years of experience in a field whose roots stretch back to the 1980s.

Attrition is likely one part of the problem. Prosecutors' offices broadly struggle with recruitment and retention [13], and the role of a prosecutor itself is complex and dynamic [17]. Moreover, prosecutor workloads shift, and are difficult to measure [16]. Burnout, a contributing factor in reassignments and resignations alike, is common in this landscape [18]. Among those who investigate and prosecute child exploitation, burnout is especially high [19].

Burned out or not, though, those who build a deep skillset in digital evidence handling or law, can find the chance to command higher salaries in the private sector [20] doubly appealing. But C.D., a prosecutor in a northeastern state, said such attrition can compound an existing problem in the United States: a nationwide shortage of trained, qualified forensic examiners [21].

3.3. Digital evidence training

Whether they specialize or not, training is generally understood to be the main avenue by which investigators and attorneys can gain a better understanding of investigators' processes and tools [22], more effectively apply reasoning in line with scientific as well as legal principles [23], and bridge gaps in their own perceptions of digital evidence and its value [4]. As B.H., a deputy district attorney working in a Mountain West state, put it: "[B]eing able, as a prosecutor, to do the same trainings that investigators do is incredibly helpful, both in preparing for trial and for being better able to advise law enforcement."

Yet law schools generally do not cover digital evidence issues [23]. The survey asked not only whether prosecutors had attended training on digital evidence, but also factors which might keep them from training. As well, survey results describe these barriers in terms of demographic factors such as location and population size served.

Nearly 80% of the prosecutor respondents said they had attended training, though only four had obtained some level of certification in digital forensics (see Fig. 8). Indeed, even prosecutors who said they filled a specialist role at their agency weren't certified in any aspect of digital forensics.

In contrast, investigator respondents were far more likely to have obtained some level of certification in their training.

However, the prosecutor respondents don't see a need for the same type of *certification* training the investigators receive. "I just need to make sure that I understand the evidence and how it works, so that I can properly explain it to a jury," said L.H., a prosecutor in the Pacific northwest. "The certifications are really needed by my forensic experts …. it's part of their training that supports their testimony."

Yet training is important for prosecutors, too. Limited training introduces risks that prosecutors will not be able to adequately prepare themselves or their witnesses or, more broadly, to attempt processes or procedures which could compromise their cases [24].

Even so, survey respondents reflected significant barriers to training. Cost, time away from the office—including staffing coverage—and inconvenience in location were all factors, with most respondents citing more than one factor as problematic (see Fig. 9). Indeed, related to "time away from the office" is location inconvenience. First, courses tend to be offered in locations convenient to *regional* trainees, but this proximity doesn't mean it's *local* to them. Prosecutors and investigators in rural locations could need to factor in travel time to a training location that could be an hour or more away.

These three factors weren't the only barriers to training. Survey respondents and interview follow-ups revealed additional complications. For one: curriculum that's overly simplistic, or targeted only to some types of crimes. Reflected one respondent: "I do financial crimes, but most digital evidence courses are full of child crimes folks who have very different issues." Some prosecutors additionally identified a lack of information about available training, or infrequency of training. Only a single respondent reflected their agency was "very supportive" of training.

Additionally, training can be time-consuming, a degree of commitment that many prosecutors may not be able to make for the skillset they need, said C.D. As a result, unless a prosecutor has a long-term plan to leave for the private sector and intends to rely on certifications to market themself, certification training—in contrast to more generalized training that confers the type of competency L.H. referred to—doesn't hold a lot of value, which C.D. said is a problem in itself.

Breaking prosecutors' barriers down further by population size and

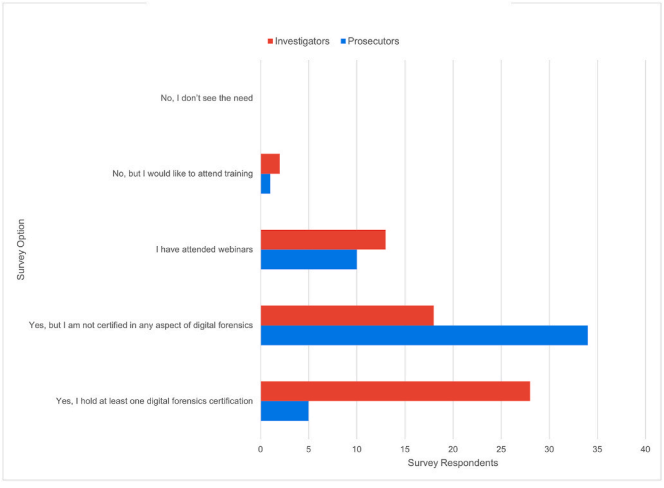

Fig. 8. The vast majority of prosecutor respondents—again, those solicited from technology-oriented e-mail listservs—have attended at least some training to familiarize themselves with digital evidence. Investigators, also solicited from a technology-oriented listserv, were far more likely than the prosecutors to have obtained some level of certification in their training.

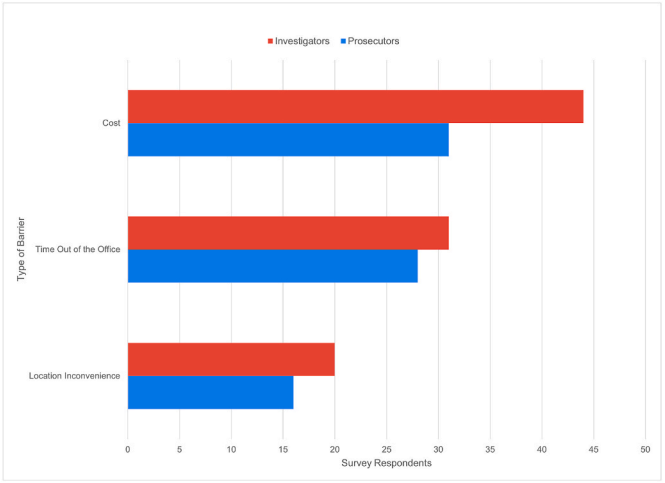

Fig. 9. Prosecutors cited location inconvenience as more of a barrier than cost, while the reverse was true for investigators and both groups cited time out of the office roughly equally.

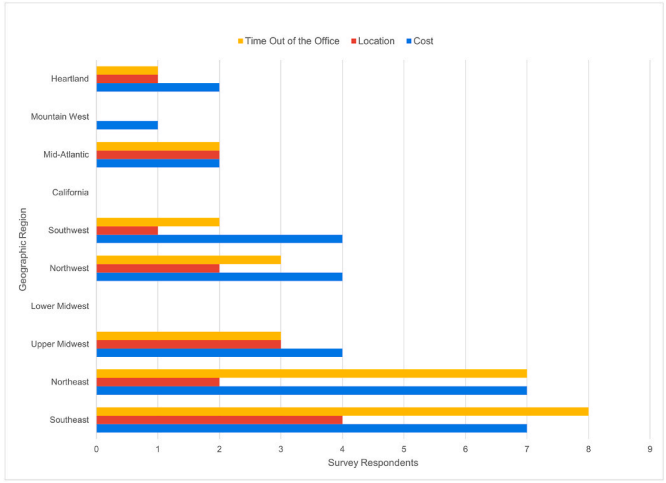

Fig. 11. Cost and time away from the office are, across U.S. regions as well as population sizes served, much greater barriers than location to prosecutor respondents' training attendance. Note: blank/missing data indicates that no respondents from these areas reported these factors applied to them.

location, the survey results reveal that across community sizes and regions, location was less of a factor for the prosecutor respondents than cost and time out of the office (see Figs. 10 and 11).

First, whether in-person or online, training tends to be pricey: anywhere from about $1200 for a two-day live remote course [25] to $3000 or more for one lasting four days [26]—not counting the cost of travel, hotel accommodations, and expenses for a multi-day trip [27].

Of course, both live and on-demand online training, accelerated by the COVID-19 pandemic, could alleviate some of these issues [23]. This survey was conducted about six months into the pandemic, so the results may indicate that location was less of a problem than in previous years. At the same time, however, virtual formats could be challenging for some [28].

In general, prosecutors' lack of access to training on digital evidence specifically may be related to the fact that only a handful of nonprofit, grant- or federally-funded entities [29] currently offer it targeted to prosecutors, relative to for-profit training offered by vendors.

Likely it wouldn't be feasible for vendors to offer training to prosecutors specifically. For example, Cellebrite offers "Legal Professionals Training." [30] However, course materials say nothing about whether the course offers continuing legal education (CLE) credits, which are annual state bar requirements for U.S.-based attorneys to continue practicing law [31].

Organizations such as the National District Attorneys Association (NDAA) and its state-level counterparts may offer some training on digital evidence, but appealing to a very broad range of prosecutors means balancing that topic with many others. For example, the NDAA's list of resources includes topics ranging from drug policy to trial advocacy to traffic law, in addition to topics like child abuse and violence against women [32]. In other words, training is both critically necessary and critically underresourced.

(Worth mentioning: an investigator's comment that "My agency has allowed me to attend some pretty advanced training, so I can't say that 'barriers' really applies to me." "Allowed" is striking language considering that training and proficiency help to improve an expert's credibility and overall performance. Through that lens, advanced training should be a requirement.)

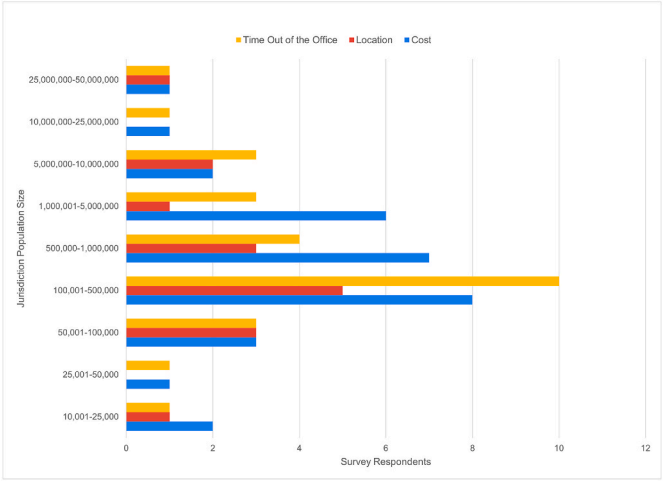

Fig. 10. Across population sizes served, prosecutor respondents cited cost and time away from the office as much greater barriers to their training attendance than location. Note: blank/missing data indicates that no respondents from these areas reported these factors applied to them.

4. Survey results and discussion

The findings on the extent to which prosecutors specialize and/or receive training on digital evidence issues is germane to the way they assess the evidence for its relevance, strength, authenticity, and admissibility, as well as how it fits with other pieces of evidence.

In particular, this research sought to ascertain whether a relationship existed between the degree to which prosecutors understand digital evidence, and how they rated their relationships and case-building efforts with investigators, judges, and others.

Thus some of the survey questions asked about various types of digital evidence and their relevance to different types of cases. After first asking how often prosecutors encounter digital evidence in their cases, and how this frequency compared with the frequency investigators reported, the survey then drilled down into the broad types of cases hypothesized to be reliant upon digital evidence. The survey also differentiated between digital forensic evidence and digital third-party evidence.

4.1. Digital evidence assessment and case-building

The questions asked in this portion of the survey sought a sense for how investigators and prosecutors approach, and rely on, digital evidence to make decisions around individuals' innocence, guilt, and liberty. In particular, the research was intended to explore the importance

of digital evidence relative to other forms of evidence.

For example, said V.J.: "Generally speaking, digital evidence tends to corroborate what a witness or victim reports, and either the digital evidence doesn't exist, or it is not able to provide that corroboration, or the digital evidence exists and it tends to corroborate the opposite. It could show that the witness is mistaken, or not truthful."

Communication between prosecutors and investigators can address these kinds of procedural and substantive issues with cases and evidence, as well as help with trial preparation [33]. In addition, prosecutor-investigator communication facilitates the service of legal process on companies that hold responsive digital data [22].

To that end, the survey asked the prosecutors to rate how involved they were in assessing digital evidence; and likewise asked the investigators to rate the involvement of the prosecutors they work with. The 1 to 5 rating scale defined 1 as minimal involvement, taking reports at face value and hardly ever asking questions; and 5 as active engagement, going through the data extensively as a team, understanding how the data supports the investigators' decisions.

Most of the prosecutor respondents—again, recruited from listservs dedicated to technology in criminal justice—rated themselves either a 3 or a 4. In contrast, investigators' responses rated the prosecutors they work with at only a 2 or 3 (see Fig. 12).

More context comes from cross-referencing the prosecutors' self-assessment with their years of experience working with digital evidence. Those who said they were most involved tended to have between five and 10 years of experience. Further, although few of the survey respondents had more than 20 years working with digital evidence, those who did rated themselves a 4 or 5. Prosecutors with 10–20 years of experience, meanwhile, were much more divided in their self-ratings, with equal numbers reporting both greater and lesser involvement with investigators (see Fig. 13).

Whether the prosecutors had access to a digital evidence specialist didn't appear to affect their self-ratings. These respondents were only somewhat more likely to report more involvement in assessing digital evidence with access to a specialist, but even those without a specialist reported a higher degree of engagement (see Fig. 14).

Because investigator respondents, again, largely reported they had no access to a prosecutor digital evidence specialist, their access or lack thereof had no bearing on their prosecutors' involvement with their cases (see Fig. 15).

Further context for these insights comes from survey questions regarding how often respondents in both groups encounter digital evidence overall, the types of evidence they encounter, and the kinds of cases that rely on digital evidence.

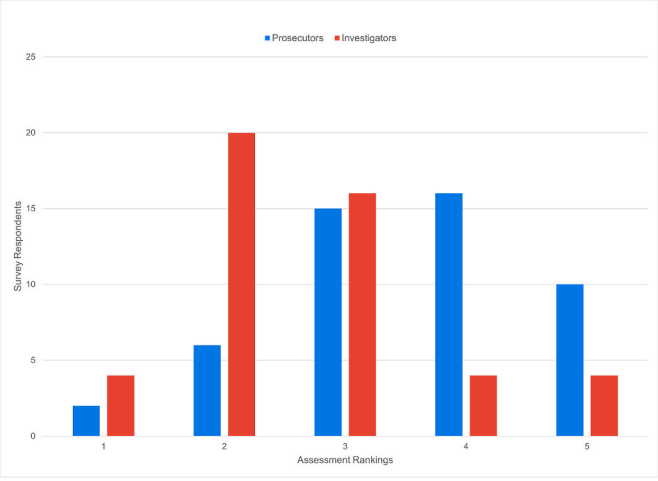

Fig. 12. Investigator respondents feel less engaged with their prosecutors, than prosecutor respondents do with their forensic investigators.

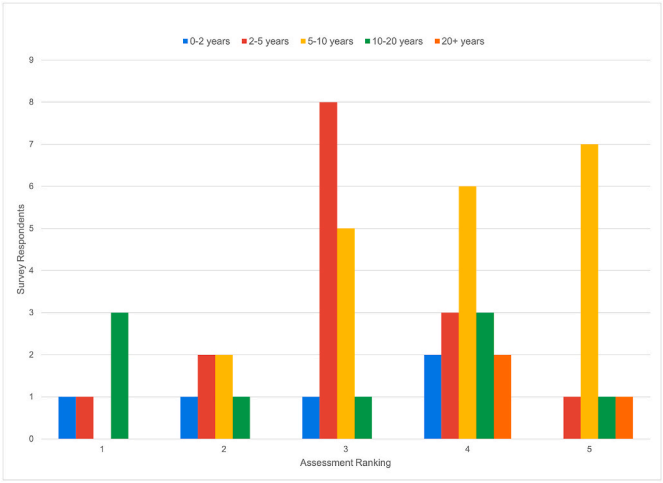

Fig. 13. How prosecutors rate their involvement with digital evidence depends on their experience levels.

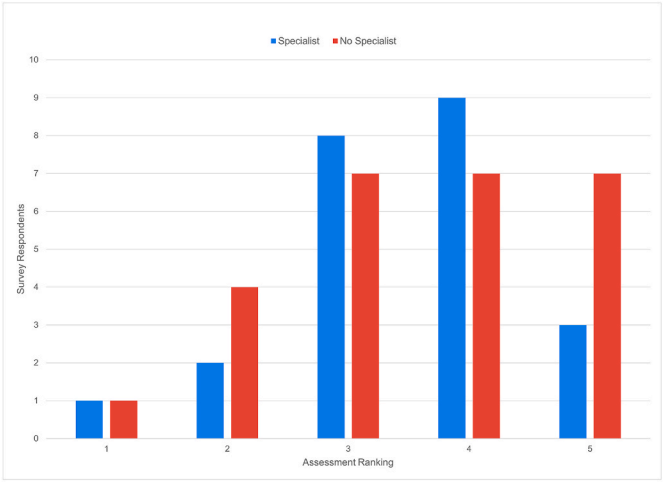

Fig. 14. Prosecutor respondents' access to a digital evidence specialist didn't appear to affect their self-ratings.

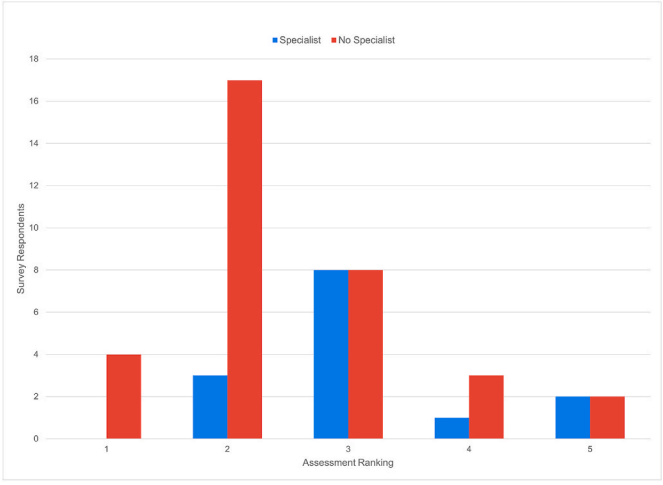

Fig. 15. Whether investigators had access to a prosecutor specializing in digital evidence did not appear to improve the likelihood of better prosecutor engagement with the investigators' cases.

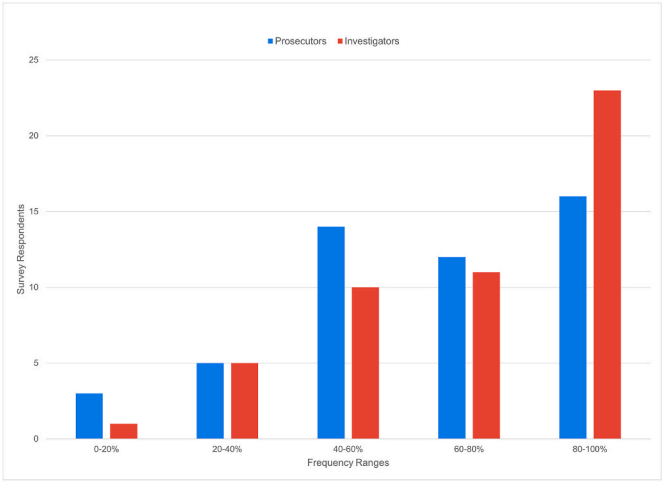

Fig. 16. More investigators than prosecutors say they almost always encounter digital data on their cases.

Fewer than one-third of the prosecutor respondents—but nearly half of the investigator respondents—said they encounter digital evidence 80 to 100% of the time. About one-quarter of each group said they see digital data 60–80% of the time, while about 30% of prosecutors and 20% of investigators said they encountered it only about half the time (see Fig. 16).

Encountering digital evidence is, of course, not the same as relying on it to build cases. Asked how frequently they relied on digital forensic evidence to build six different types of cases:

- Respondents from both groups "almost always" rely on this type of evidence for cases involving crimes against children, organized crime, and sex offenses.
- However, most of the respondents from each group "sometimes" or "rarely" rely on digital forensic data for property crimes.
- Fewer prosecutors than investigators "almost always" or "usually" rely on digital forensic data for violent crime. Instead, they use this evidence "about half the time" or "sometimes" when building these cases.
- More prosecutors "almost always" or "usually" rely on digital forensic data for financial crimes cases.
- Digital forensic data also factors more strongly for investigators of organized crime than it does for prosecutors, who generally reflected that they use it for those cases only "sometimes" or "rarely."
- A slightly higher proportion of prosecutors reflected that they "rarely" rely on digital forensic data across all types of cases.

Digital devices are not the only sources of digital evidence, particularly when the devices are damaged beyond repair, encrypted, and/or otherwise inaccessible or unreadable to investigators. In recent years, "third party" data from companies such as wireless telecom providers, social media companies, online gaming platforms, etc. has become increasingly appealing to law enforcement [34]. The data might consist of subscriber information that can be obtained via subpoena, customer records that require a court order, or content that demands a search warrant [35].

Even when a device is unlocked and forensics can offer a complete picture of the data existing on the device, third-party data can be valuable to corroborate and authenticate that evidence; for example, by helping to put a suspect behind a device at the time and/or place an incriminating message was sent or video was shot.

For these reasons, the survey also asked both groups about the extent to which they rely on third-party data for the six types of cases (seeFig. 17).

Investigators were additionally asked about their reliance on a third form of digital evidence for the six types of cases: the "low-hanging fruit" video, images, text messages, or other data that can come, say, from a device found at the scene of a crime and which may or may not require extensive forensic analysis [36].

Investigators' responses indicated that "low hanging fruit" factors heavily in case-building for property crimes, violent crimes, crimes against children, and organized crimes, and only to a lesser extent for sex offenses and financial crimes (see Fig. 18).

It should be noted that investigators' reliance on low-hanging fruit doesn't mean this type of evidence leads straight to convictions. Instead,

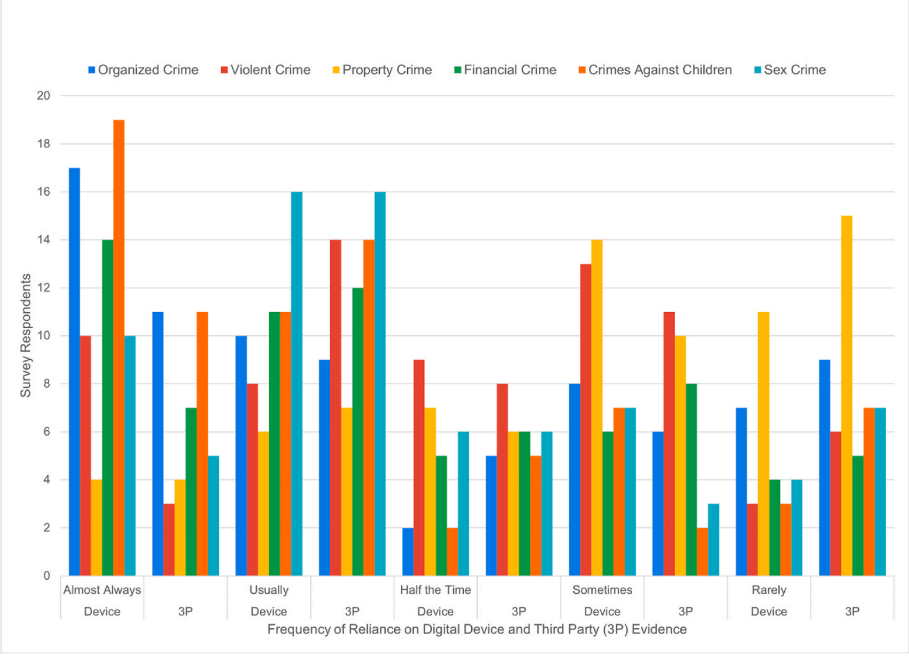

Fig. 17. Prosecutors are more likely to rely on digital and third-party data as evidence of crimes with a strong digital element, such as crimes against children, organized crime, and financial crime.

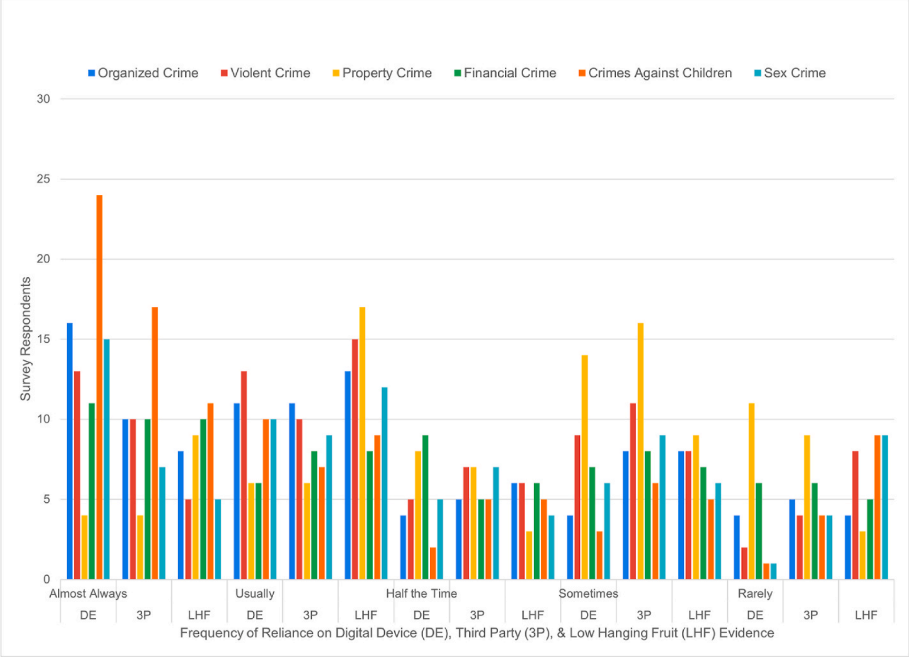

Fig. 18. Investigators' reliance on digital forensic evidence for 6 different types of cases.

the data needs to "put the suspect behind the keyboard." [37] Examining victim and witness devices and accounts alongside suspects', as well as physical trace evidence, medical or bank records, eyewitness statements, etc. all factor in.

The interviewees indicated that other factors, including how easy digital evidence is to obtain, and whether the seriousness of the case warrants additional effort when evidence is harder to obtain, also apply. For one, third-party data can take more time and effort to obtain. Whether owing to "size and lack of organization" or to provider push-back on legal process, these delays can hinder case-building.

To that end, asked about their levels of satisfaction with both the timeliness and the quality of data returns from electronic service providers (ESPs), both prosecutors and investigators reflected concerns, particularly around returns' timeliness (see Fig. 19). In responses to an open-ended survey question, investigators reported delays of three to five weeks, up to six to eight months, or in one case, a full year.

Overall, the survey results indicate that digital evidence that could help build cases and corroborate other evidence is simultaneously plentiful and elusive. How this contradiction affects prosecutor decision-making, then, has profound implications.

4.2. *Prosecutor decision making*

Prosecutors make a lot of decisions about their cases, largely based around two questions: whether they *can* prove a case, and whether they *should* prove the case [38]. These decisions come down to screening cases, charging criminal suspects, what and how to introduce evidence at trial, offering plea bargains to defendants, sentencing recommendations, and dismissing charges.

The survey focused specifically on how often digital evidence factored in making these four decisions:

- Charging
- Introducing/getting evidence admitted
- Plea bargaining
- Dismissing charges

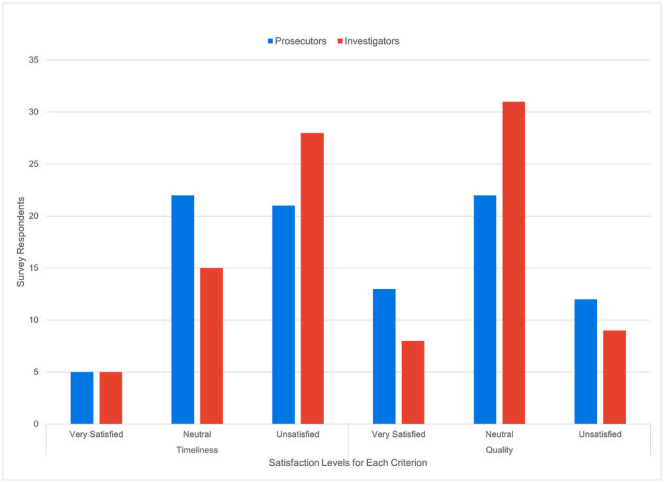

Fig. 19. Prosecutors are slightly more concerned with warrant returns' timeliness than their quality. More investigators are unsatisfied with warrant returns' timeliness, but their views on quality are of about the same degree of concern as for prosecutors.

In particular, because plea bargaining[2] is estimated to resolve more than 90% of criminal cases at both federal and state levels [39], this research sought to find out whether, and to what extent, digital evidence influences a practice with such a profound impact on both the criminal justice system and the defendants within it.

B.H. provided greater detail on the role of digital evidence in his decision-making, which he said in his experience falls into three categories:

1. Defense attorneys asking questions and sharing information that police and prosecutors didn't already have. In those cases, police can follow up with a fresh search warrant based on the new information.
2. Evidence that supports or refutes the defendant's version of events, including from victims' or witnesses' devices or online accounts. Sometimes, new evidence also results from conversations with defense attorneys.
3. Technological advancements in forensic tools—sometimes within a matter of the weeks or months it takes for a case to go to trial—that mean evidence can be recovered and parsed that couldn't be previously.

K.T., a prosecutor in a northeastern metropolitan location, pointed out that decision-making can depend on the quality of evidence. "In my experience when we get into a phone, it's two extremes of either, 'This [device] has everything that we could possibly think of,' or 'There's absolutely nothing,'" she said.

Asked whether they make these decisions based on whether digital evidence strengthens or undermines their cases—or whether digital evidence even factors that strongly for them—survey respondents were able to pick more than one choice.

Most respondents decide based on whether the evidence strengthens their cases. Fewer than half of all respondents were concerned about digital evidence undermining their cases; fewer than one-quarter said digital evidence rarely factored that strongly in their decisions (see Fig. 20).

At the same time, though, charging decisions are based on more than just digital evidence [40], and the interviewees reflected that digital evidence factors into charging decisions only when it is the best or only evidence of an offense—not when it corroborates other evidence. J.S. reflected that it can be more important to tie the defendant to the crime by showing evidence on their device, email account, financial records, etc. Additionally, whether digital evidence is the "best or only" evidence of an offense ties to its quality and its admissibility. For example, printouts from a social media site could provide important leads, but may not be readily authenticated as evidence [41].

4.2.1. *Prosecutor decisions based on crime types*

That digital evidence is most important when it strengthens prosecutions offers context for crime-specific data. In particular, the survey results were used to determine whether the frequency with which prosecutors encounter digital evidence affected the four types of decisions for each of the six crime types (see Figs 21 - 26). By cross-referencing the frequencies at which survey respondents said they encountered digital and third-party evidence, with how often they said they used it to make decisions for each crime type, the results revealed that:

- Even though more prosecutor respondents "usually" rely on third-party data more than investigators do (see Figs. 17 and 18), it still

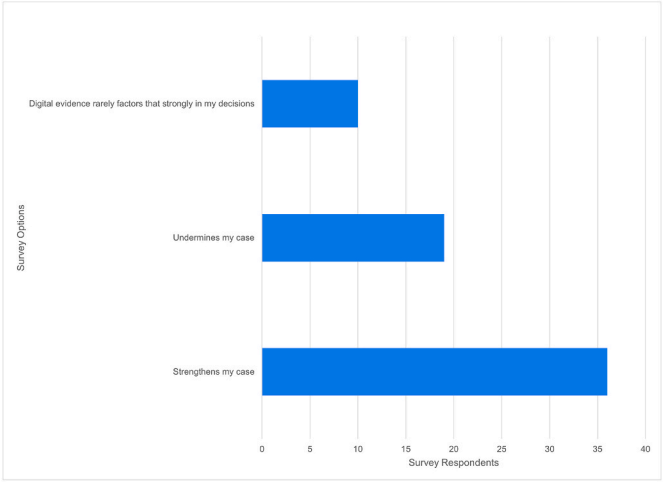

Fig. 20. Digital evidence factors most strongly in survey respondents' decisions to charge, introduce, plea bargain, and/or dismiss when it comes to strengthening their cases.

[2] Defined as "an agreement between a defendant and a prosecutor, in which the defendant agrees to plead guilty or "no contest" (nolo contendere) in exchange for an agreement by the prosecutor to drop one or more charges, reduce a charge to a less serious offense, or recommend to the judge a specific sentence acceptable to the defense," plea bargaining is estimated to result in more than 90% of criminal case outcomes. (See: Berman, Sara. "The Basics of a Plea Bargain." Nolo.com. https://www.nolo.com/legal-encyclopedia/the-basics-plea-bargain.html accessed 7 June 2022.) The high quantity of pleas render plea bargaining a somewhat controversial practice. It's typically understood to be offered as a resolution for weak cases [13] although it's also positioned as an overall way to save costs and better allocate taxpayer dollars, relieve strain on the criminal justice system, and save time for everyone while still achieving some measure of justice for victims of crime (see: Barton, Robin L. "The Role of Victims in Plea Bargaining." *The Crime Report*, March 5, 2012. https://thecrimereport.org/2012/03/05/2012-03-the-role-of-victims-in-plea-bargaining/accessed 18 June 2021). At the same time, however, plea bargaining has been criticized as an unconstitutional way to fast-track defendants to serve time, whether incarcerated or on probation (see: Fremon, Celeste. "Has Plea Bargaining Pushed the Sixth Amendment Right to Trial to the Brink of Extinction? A New Report Says Yes." *WitnessLA*, July 15, 2018. https://witnessla.com/plea-bargaining-has-pushed-the-sixth-amendment-right-to-trial-to-the-edge-of-extinction-says-a-new-report/accessed 18 June 2021). The trend impacts lives and livelihoods at the expense of defendants' right to confront their accusers and have their case evaluated by a jury of their peers (see: Borchetta, Jenn Rolnick and Alice Fontier. "When Race Tips the Scales in Plea Bargaining." *The Marshall Report*, October 23, 2017. https://www.themarshallproject.org/2017/10/23/when-race-tips-the-scales-in-plea-bargaining accessed 18 June 2021).

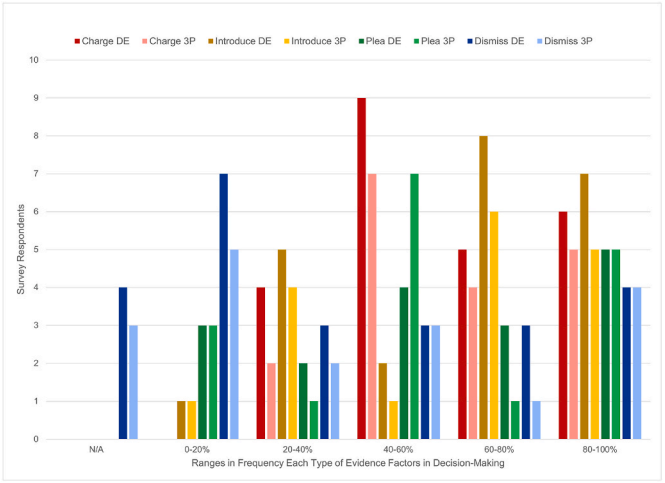

Fig. 21. Prosecutors of financial crimes use digital and third-party evidence to make decisions about evenly when they encounter it more than 80% of the time, but the usefulness of this evidence to their decisions varies more widely when they encounter it less often.

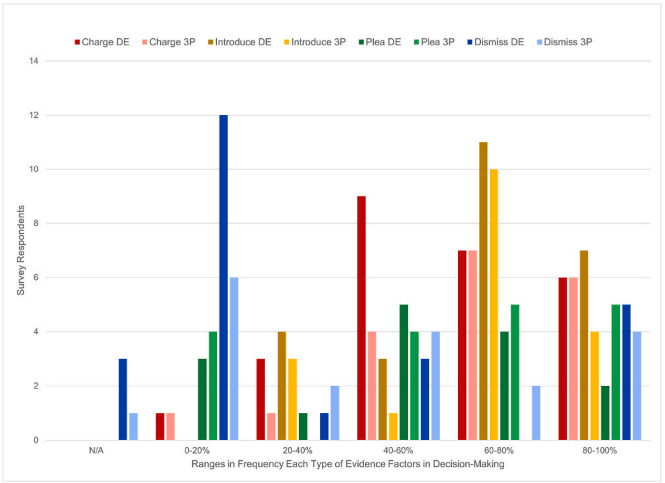

Fig. 22. Prosecutors of organized crimes are somewhat less consistent in their use of digital and third-party evidence than financial crimes prosecutors.

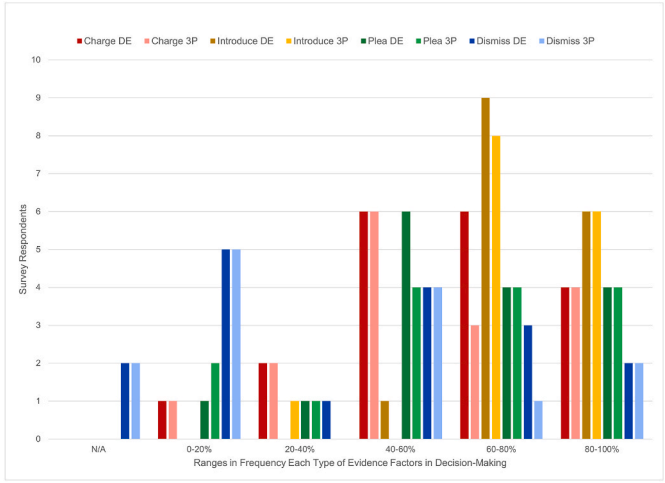

Fig. 23. Prosecutors of violent crimes use digital and third-party evidence to make decisions about evenly when they encounter it more than 80% of the time, but the usefulness of this evidence to their decisions varies more widely when they encounter it less often.

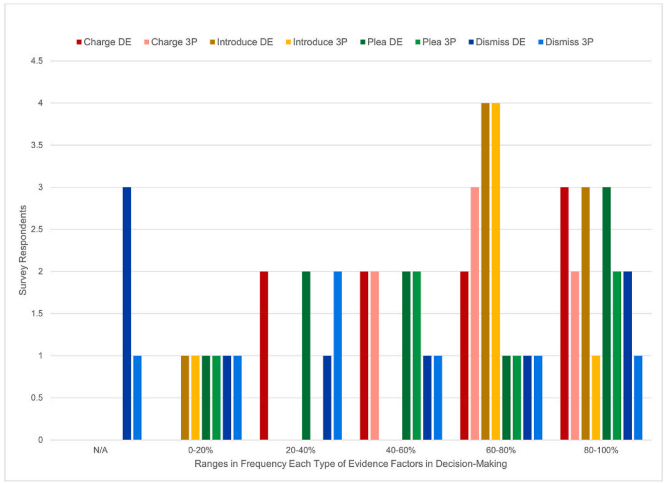

Fig. 24. Respondents who reflected they prosecute property crimes were very few. For this limited cohort, digital evidence factored more heavily than third-party evidence among those encountering both types 0–20% and 80–100% of the time. Among those encountering digital evidence 20–40% of the time, though, third-party evidence was relied upon more.

factors less in the prosecutors' decision making than digital forensic evidence—except plea bargaining, where third-party data factors more than digital evidence among prosecutors who see digital evidence about half the time.

- Those who encounter digital evidence only about half the time seek to introduce it at trial far less than using it to charge or plea cases, as well as less than those who encounter it more than 60% of the time.
- When prosecutors encounter digital evidence 60–80% of the time, they're more likely to seek to introduce it than other respondents are, even those who see it 80–100% of the time.
- Across the six different crime types, prosecutors seek to introduce digital forensic data and third-party data about equally; the majority, 60 to 80% of the time.
- Digital forensic and third-party evidence factored in dismissal decisions more strongly when the survey respondents encountered such evidence less than 20% of the time.
- For prosecutors who encounter digital evidence more than 20% of the time, however, the evidence factored in dismissals less often than charging, introducing, or plea bargaining.
- More survey respondents answered "not applicable" to this question than to the other decision questions, and nearly half the respondents said digital evidence very rarely affected their decision to dismiss cases.

4.2.2. *Decisions based on experience level*

Another goal of the research was to see whether two factors influenced respondents' decision-making: their levels of experience, and as well, whether they had access to a digital evidence specialist. Across the board, the results show that access to a specialist appears to influence decisions to charge, plea bargain, and dismiss cases to a greater extent than experience alone (see Figs 27 - 34):

- When their office has access to a digital evidence specialist, more than half these prosecutors (about one-quarter of the total survey respondents) use digital data to charge and to plea bargain more than 60% of the time.
- The prosecutors with more than 10 years of digital evidence experience generally appear to introduce, charge, plea, or dismiss digital evidence less frequently than those with less experience.

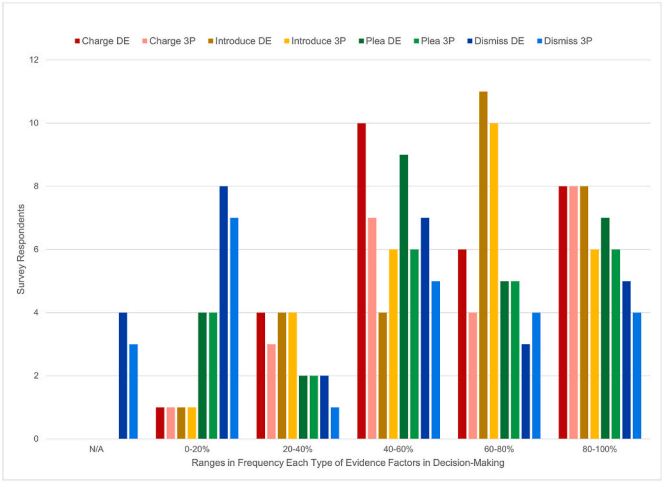

Fig. 25. Prosecutors who encounter digital evidence 60–80% of the time in crimes against children cases seek to introduce it at higher rates even than charging or plea bargaining, as well as dismissing.

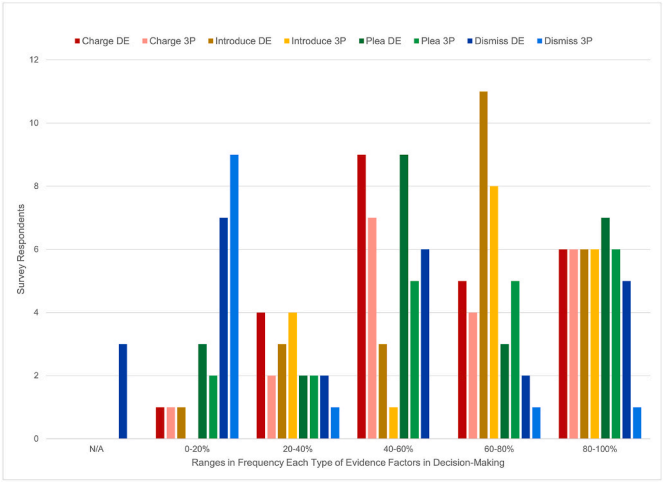

Fig. 26. Just as for violent crimes, prosecutors of sex crimes use digital and third-party evidence to make decisions about evenly when they encounter it more than 80% of the time, but the usefulness of this evidence to their decisions varies more widely when they encounter it less often.

- Although access to a digital evidence specialist appears to influence prosecutors' decisions to introduce the evidence, the influence isn't as strong as it is on the other decisions.

The prosecutor interviewees offered insights that indicate the extent to which experience factors in their decision-making.

Introducing the data, said K.T., comes down to "a balancing test between how much the evidence is going to help move the [case] forward" versus its complexity and, therefore, the amount of education that will be needed to help the jury understand the evidence and its relevance.

Juror demographics can factor heavily into this kind of decision. A.B, district attorney in a small northern Midwestern county, said if digital evidence was strong enough to use as a basis to charge, then defendants typically take a plea bargain, which can achieve a similar result as going to trial. Because her district is populated largely by retired seniors, the plea bargain eliminates the need to call in an expert to explain digital evidence.

However, the strength of evidence also affects plea bargaining decisions. As J.S. put it: "If you had really great digital evidence that was

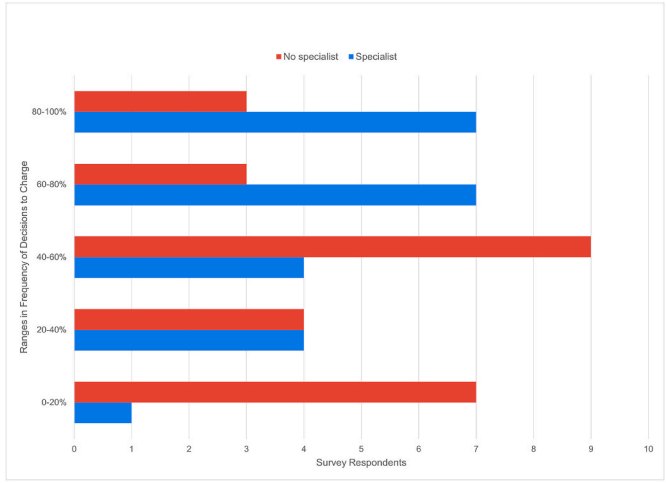

Fig. 27. How strongly digital evidence factors in the decision to charge a suspect, correlated to whether the prosecutor's office has a digital evidence specialist.

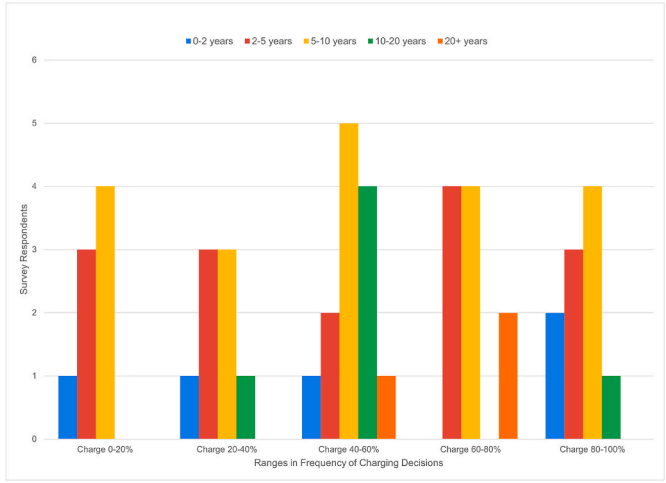

Fig. 28. How experienced prosecutors are with digital evidence doesn't appear to have much bearing on their charging decisions.

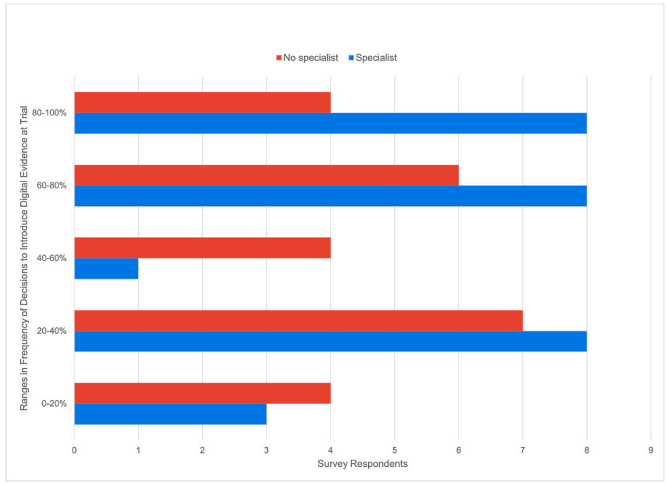

Fig. 29. How strongly digital evidence factors in the decision to introduce it, correlated to whether the prosecutor's office has a digital evidence specialist.

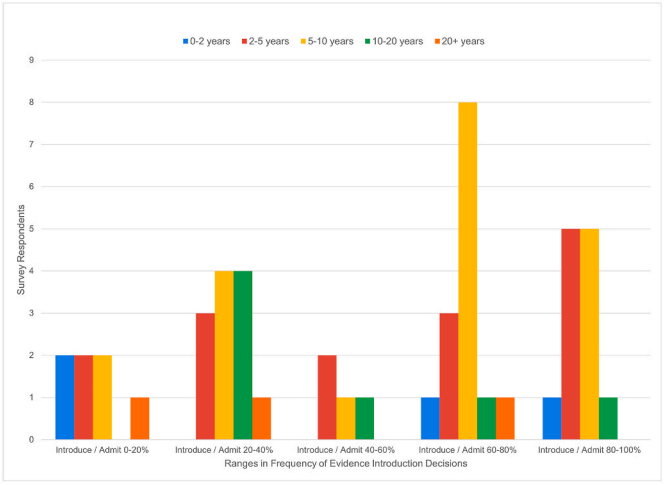

Fig. 30. The decision to introduce digital evidence doesn't appear to be influenced by experience level, though those with longer experience appear to introduce digital evidence less frequently than those with less experience.

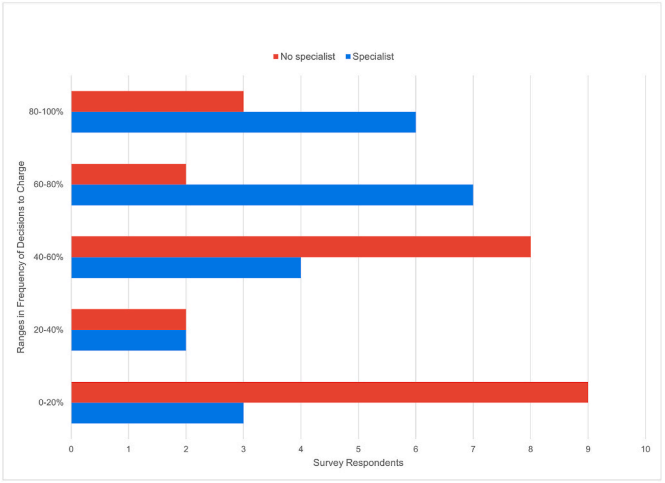

Fig. 31. The presence of a digital evidence specialist in survey respondents' offices appeared to influence their decisions using digital evidence to plea bargain in similar proportions as their decisions to charge.

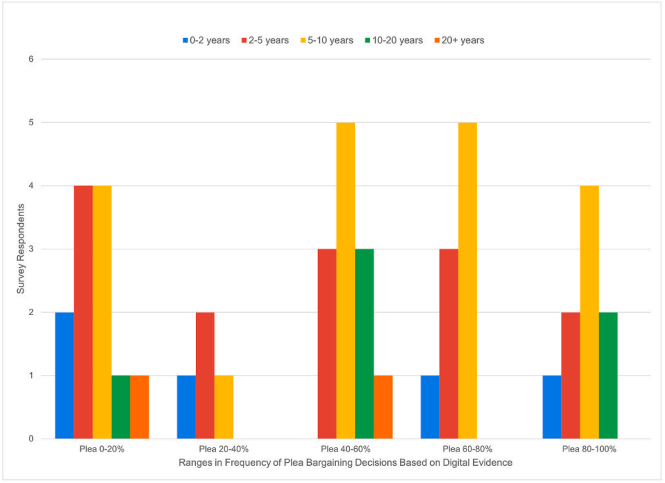

Fig. 32. The decision to plea bargain based on digital evidence doesn't appear to be influenced by experience level.

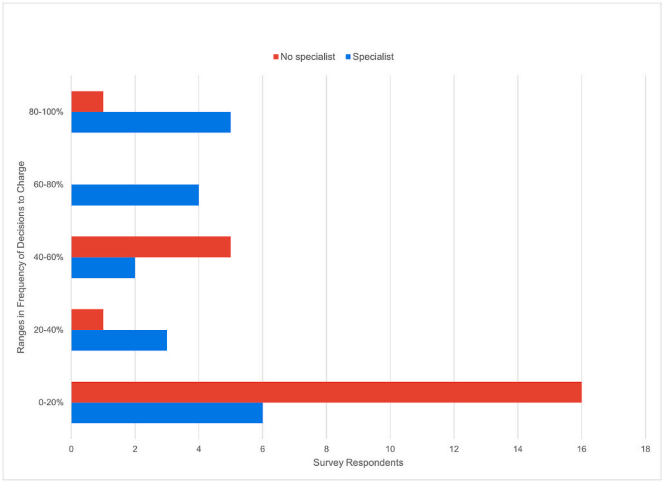

Fig. 33. As with the other decisions, although having a digital evidence specialist may help strengthen prosecutors' confidence in their decisions, it isn't necessarily a predictor.

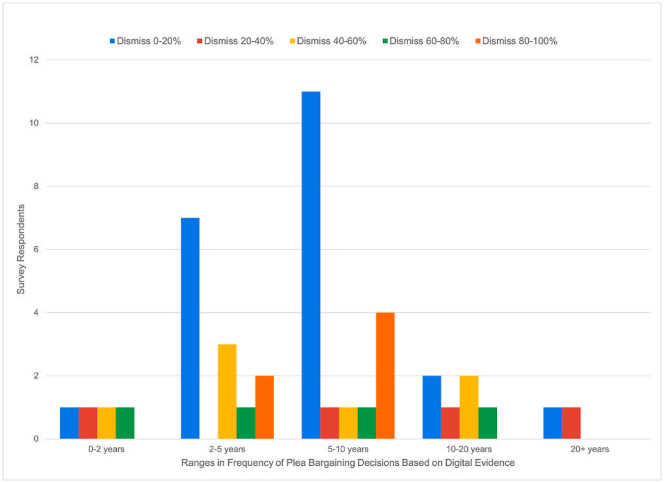

Fig. 34. Respondents' years of experience did not appear to have any influence over whether digital evidence drove their case dismissal decisions.

directly on point, then you've got a much stronger case and potentially a different position in a plea bargain than if you've got digital evidence that is just adjacent or corroborating or maybe has admissibility issues. Then you've got to approach that process differently."

In some jurisdictions, the law allows for only a few days between an arrest and a decision whether to bring or drop charges. This time limitation can restrict investigators' ability to collect, much less analyze relevant evidence [13].

That's been J.D.'s experience in his state, where charging and plea decisions are made simultaneously for felony cases. Although he's typically already aware of what digital evidence exists or doesn't exist in order to make decisions, he said, "Sometimes [the digital evidence] comes later or maybe we've downloaded a cell phone, but no one's had time to analyze it yet," J. D explained. "In those cases I have to make the charging decision and the plea offer without the benefit of digital evidence."

4.3. *Digital evidence at trial and beyond*

How prosecutors approach any evidence—how they build cases and relationships with investigators as witnesses, and how they make decisions to charge, introduce, plea bargain, and dismiss cases—ultimately

comes down to how they anticipate judges and juries might perceive the evidence.

"I see my primary job in this area is … to give the fact finder, whether it's a judge or a jury, enough of a basis and understanding of the technology to make an informed decision about whether the digital evidence is admissible and how much weight to give it [relative to other forms of evidence]," said C.D.

However, he added, this task is becoming increasingly difficult as technology advances. Too much science, and judges and jurors can become bored and frustrated; not enough, and defense attorneys can sow seeds of reasonable doubt, regardless of whether they themselves understand digital data [4].

These outcomes often depend on the prosecutor's effectiveness in showing the evidence is what it purports to be; that it is authentic. A series of survey questions therefore asked about the admissibility of digital forensic evidence, prosecutors' sense of investigative due diligence in handling that evidence, and whether they thought technological advancement could ever outstrip a) their ability to demonstrate authenticity and b) jurors' ability to weigh the evidence appropriately.

As the prosecutor interviewees reflected:

- Jurors might be predisposed to trust scientific processes, even if they don't understand them, relative to eyewitness testimony or other forms of evidence; conversely, they may be more skeptical of what they don't understand.
- Juror demographics can play a significant role. As discussed previously, juries composed primarily of retirees, for example, may be less amenable to learning about how technology works than juries in locations where technology is a fact of life.
- Even when a jury is composed of a defendant's peers, lifestyle variances can mean defendants use their devices and accounts in drastically different ways. Jurors thus can be challenged to make the connections they need to understand how the evidence—for example, hours' worth of livestreaming—fits the case at hand.
- Forensic witness expertise on the stand depends in part on examiners' own training and experience, and in part on a prosecutor's ability to prepare them to testify. Good expert witnesses can help to bridge any gaps between familiarity and technical detail.

"After many trials I realize that I don't know how jurors' thought processes work in many regards," H.W., a West Coast-based prosecutor, said. "Moreover, every jury is different."

The tradeoffs between the complexity and probativity of digital evidence impact trial strategies to varying degrees. Sometimes, said B.H., jurors need only a rudimentary overview of how, say, mobile forensics software works and why it's reliable, without need to get into the differences between logical, file system, and physical extractions.

Other times, jurors need more detail. B.H. and L.H. have both walked jurors through technical details in trials where, said B.H., "[W]e knew [the jurors] were going to see it and we didn't want them to go back and deliberate and [ask] why is there all this other stuff in there," he recalled. L.H. agreed: "[We were] essentially trying to answer every possible question that jurors could have about it in testimony, because obviously they don't have enough chance to ask us questions directly," she explained.

But these strategies need to be carefully applied. "If you start putting all these cell phone records, all these phone records, all of these videos … before [jurors] over a period of a week or two, it's a lot for them to digest," said J.D. That's why H.W. focuses his experts' testimony on key evidence, only addressing "boring" authentication issues on redirect in the event the defense presents evidence of tampering.

So much effort can go into educating juries, H.W. added, that it behooves digital forensics practitioners to adhere to accepted scientific processes. "We spend a lot of time teaching the 'proper' way to do things, often because of fear of what a jury would think if the weaknesses of the practice [are] exposed. For example, if a hash does not match it opens the door to speculation that the government planted data or spoiled it," he explained.

The"'proper' way to do things"—the quality assurance standards and best practices that guide how data is preserved, collected, analyzed, and presented—forms the foundation of admissible evidence [42]. Yet:

> "New advances in computer forensics technology will continually raise reliability issues, particularly as new techniques are deployed in the field without extensive review and testing seen in non-technological scientific fields ….
>
> "Digital device technology is changing at lightning speed, as is the technology to extract and analyze data from those devices. This poses serious problems for meeting requirements of Daubert—i.e., being able to demonstrate that digital evidence presented in court is reliable." [4].

The "requirements of *Daubert*" refers to a legal standard for the introduction of scientific evidence.[3] Typically, pretrial hearings establish whether a tool or method has met this (or equivalent) standard. However, the likelihood of a *Daubert* hearing depends in large part on a state's defense bar as well as its bench: how well defense attorneys understand the evidence enough to challenge it, and how well judges tolerate challenges [43].

The first hurdle for whether scientific evidence can be considered admissible is its methodology's validity in the scientific community. Different legal standards are applied, depending on the state.[4]

Few survey respondents had ever participated in a pretrial scientific admissibility hearing (see Fig. 35). Respondents who answered "yes" to this question followed up by describing, in an open-ended short-answer field, that the hearings they participated in were for mobile forensics analysis, including Cellebrite usage and admission of cell site locations specifically; metadata; peer-to-peer investigations; and to establish foundation and provide general education to judges.

As long as the methods involve generally accepted forensic tools, said H.W., then courts do not need to hold these types of hearings. J.D. agreed: "I don't tend to see that we distrust the technology and therefore you should keep it out under *Daubert*," he said. Because digital evidence can support the defense as well, he noted, defense attorneys frequently ask for clients' phone forensic images, and look for other ways to challenge the evidence. Within the context of digital forensics admissibility hearings, H.W. said, these other challenges might include "whether the tools were used in a legal manner, whether the tools were used correctly and whether the sponsoring witness has the expertise and factual foundation to give an opinion about their findings."

Thus, said C.D., it isn't just a matter of forensic processes, but also the tools and the level of expertise required to understand them along with the ability to verify the data they reveal as a true and accurate copy of

[3] Under the *Daubert* standard, the factors that may be considered in determining whether the methodology is valid are: whether the theory or technique in question can be and has been tested; the existence and maintenance of standards controlling its operation; whether it has been subjected to peer review and publication; its known or potential error rate; and whether it has attracted widespread acceptance within a relevant scientific community. Under the older *Frye* standard, in contrast, whether a tool is generally accepted in the scientific community is the only requirement to show (*See* Legal Information Institute, Cornell Law School. https://www.law.cornell.edu/wex/daubert_standard).

[4] In California, for example, the *Frye* standard is combined with a state case, *People v. Kelly*, 17 Cal. 3d 24 (Cal.1976), which adds Daubert-like criteria to allow for novel testimony. (See Lopez, Star, "Satisfying the Judicial Gatekeeper: Assessing Legal Standards for the Reliability of Expert Testimony." University of California-Irvine Law Forum Journal Vol. 2, Fall 2004 https://www.socsci.uci.edu/lawforum/content/journal/LFJ_2004_lopez.pdf) For another example, Colorado has *Schreck* hearings, based on *People v. Shreck*, 22 P.3d 68 (Colo. 2001).

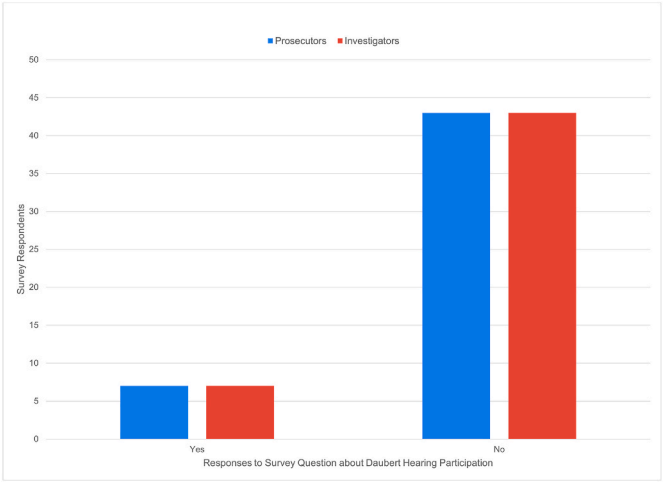

Fig. 35. Largely, neither prosecutors nor investigators have participated in admissibility hearings.

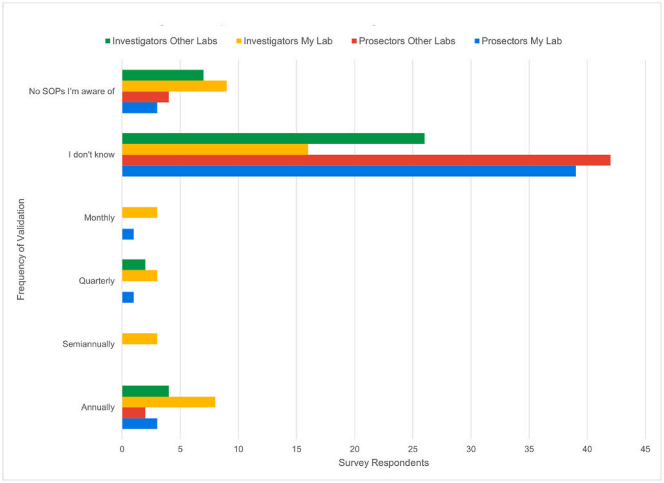

Fig. 36. Respondents in both surveys overwhelmingly reflected that they don't know whether their labs have any SOPs for regular validation and verification.

what's on the device [44].

Yet, C.D. added, relying on scientific principles and methods to determine admissibility—even in general terms, leaving case-specific facts for a judge or jury to assess [7]—is a skill in short supply, in part because so few cases ever go to trial. While forensic methods change [4], new technology, such as deepfake videos and "viral" social-media misinformation campaigns, can introduce reasonable doubt in ways that could be difficult to challenge [45].

These factors are compounded by the advent of tools designed to save investigative time and effort [23], as well as safeguarding investigators' mental health [46], through automation. Tradeoff risks of these benefits include the inability to evaluate the evidentiary value of evidence, the potential to overestimate the technical competence of the person performing the triage, and the possibility that inaccurate interpretation of evidence could "snowball" into a cascade of poor decisions—all without the prosecutor's awareness [23]. Relying more on the tool and not on their own decision making or investigative skill, said C.D., means forensic examiners are less able to explain how the tool works. "And that makes it more and more challenging for me to do my job putting them on the witness stand," he said.

Compounding this challenge, C.D. continued, is the departure of professionals seeking career advancement. Forensic examiners must ultimately leave the forensic lab, either through promotion in a law enforcement agency, or to find better-paying work in the private sector. These departures, C.D. observed, affect prosecutions on two levels: not just the knowledge in itself, but also whether trained, experienced witnesses are available to testify. "We lose our institutional knowledge—real valuable people—because they can go make more money [in the private sector]," he explained, adding: "We've invested hundreds of thousands of dollars in training for them and then we lose them …. That's just maddening."

As a measure of survey respondents' awareness of the processes that go into fulfilling the requirements for scientific evidence, both survey groups were asked how familiar they were with their own labs', and others', validation SOPs (see Fig. 36).

This sort of "background information" on a lab's processes may not appear to have much relevance to individual cases. In fact, in her state, L.H. said, attorney questions about lab SOPs are a "one-off," with attorneys asking experts whether everything, including their certification, is up to date.

However, processes and procedures define the chain of custody for digital evidence. Moreover, given the rapid pace of change in the industry, these processes and procedures are (or should be) dynamic. To be able to refute challenges, prosecutors need to know whether policies have been followed; if not, where the deviation occurred and why; and which practices were in use and applied to the evidence in question [33]. Not holding forensic examiners accountable in this way can risk entire convictions [47].

Understanding these processes can benefit prosecutors in other ways as well. First, prosecutors can get a better sense of their expert witnesses' expertise [48], establishing their knowledge and comfort level with scientific processes like validation [49]. This knowledge helps them to know how and to what extent to prepare witnesses to testify, as well as to prepare for potential defense objections.

Second, prosecutor knowledge, when applied in their conversations with investigators and forensic examiners, can help them support due diligence so that they can be more confident that:

- The inculpatory data is what it purports to be.
- Any reasons for digital evidence not being correctly parsed or interpreted [50], e.g. due to tool or user error, are adequately explained.
- Any exculpatory data has been identified for discovery [33].
- Any absence of exculpatory evidence can be adequately explained [51].

In the event that a defense attorney brings new data to light that law enforcement didn't have access to six months previously, the prosecutor can more readily communicate with forensic examiners to revisit their evidence [51].

The survey asked whether respondents had ever encountered a case where the kind of due diligence described above revealed that digital evidence was incorrectly parsed or interpreted, or where the initial investigation failed to uncover exculpatory evidence.

Asked whether they had ever encountered cases like these, either before or after they charged a defendant, the prosecutor respondents gave mixed responses (see Fig. 37). Only about one-third ever had, but another one-fifth said they were unsure. One prosecutor responded that they had not found incorrectly parsed or interpreted digital evidence—but they had encountered at least one initial investigation that failed to uncover exculpatory evidence.

Going deeper into the survey responses, the results show that years of experience with digital evidence doesn't appear to indicate whether the prosecutors had encountered a problem with due diligence (see Fig. 38). The numbers may reflect more the number of survey respondents who answered from those demographics than they do the encounters.

Likewise, office size also didn't appear to correlate to encountering due diligence issues. Survey respondents across all office sizes had

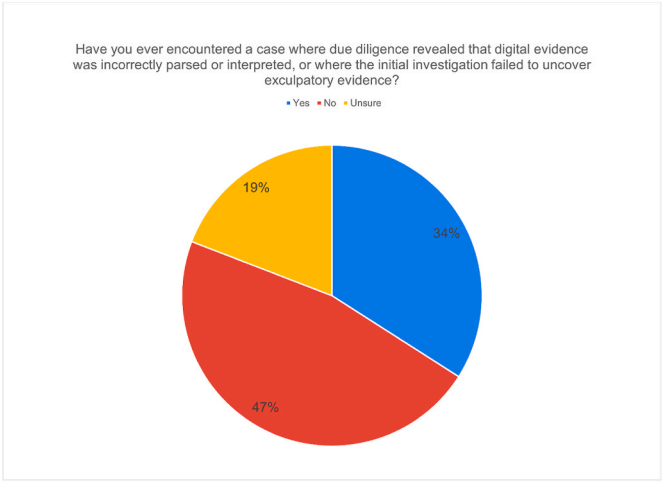

Fig. 37. More than half of prosecutor respondents had encountered—or couldn't be sure if they had encountered—at least one case where digital evidence didn't provide an accurate picture of what happened.

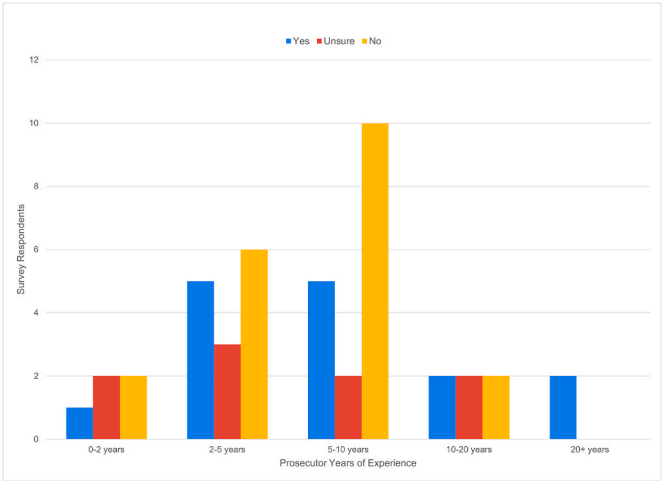

Fig. 38. Years of experience didn't seem to indicate the likelihood that a prosecutor either would have encountered a due diligence issue, or couldn't be certain.

encountered at least one such case. Notably, none of the respondents from the largest offices said they were uncertain about having encountered any issues (see Fig. 39).

However, cross referencing due diligence responses with prosecutor involvement with digital evidence reveals that the more engaged respondents say they are with investigators, the more likely they are to spot due diligence issues. They are also somewhat more likely to be certain that they haven't encountered due diligence issues (see Fig. 40).

Respondents who said they didn't have access to a digital evidence specialist appeared slightly more likely to say they hadn't encountered due diligence issues, but those who do have access didn't seem to encounter significantly more of those issues (see Fig. 41).

As to the extent that due-diligence issues could affect prosecutor decision-making, the data is inconclusive (see Figs 42 and 43).

What due-diligence issues highlight is that, as straightforward as digital data might appear, its interpretation is still performed by humans, using tools likewise developed by humans [23]. Thus, while digital forensic examiners are independent in the sense that they analyze and interpret evidence that is relevant to the case and its context, they are no more bias-free than their counterparts in physical forensic sciences [52]. Prosecutors must thus take care that their relationships don't

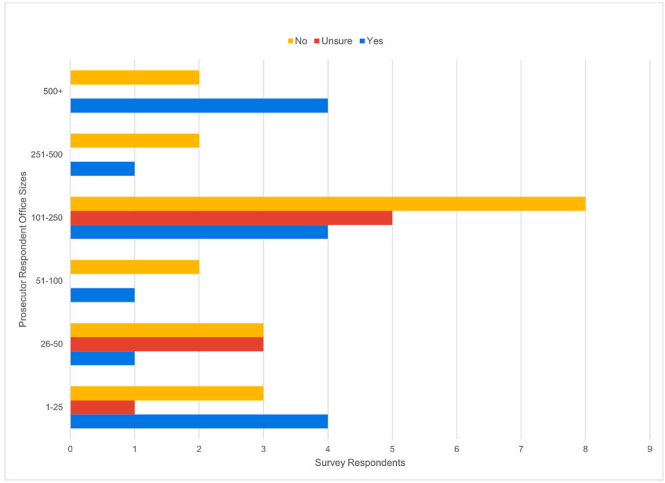

Fig. 39. Office size doesn't appear to predict whether prosecutor respondents had encountered issues with digital evidence due diligence.

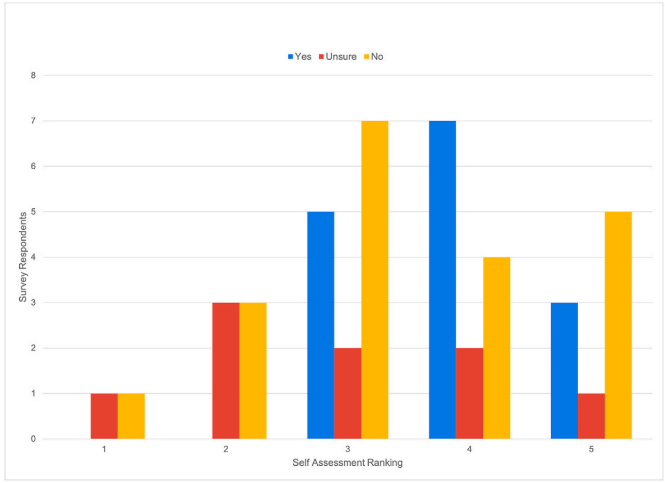

Fig. 40. Respondents who are more engaged with investigators are both more likely to encounter due diligence issues—and to be certain that they hadn't.

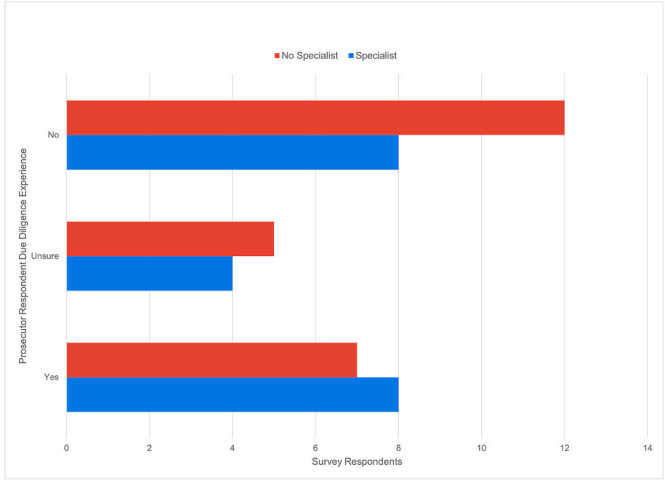

Fig. 41. Access to a digital evidence specialist doesn't appear to correlate to whether survey respondents encountered due diligence issues.

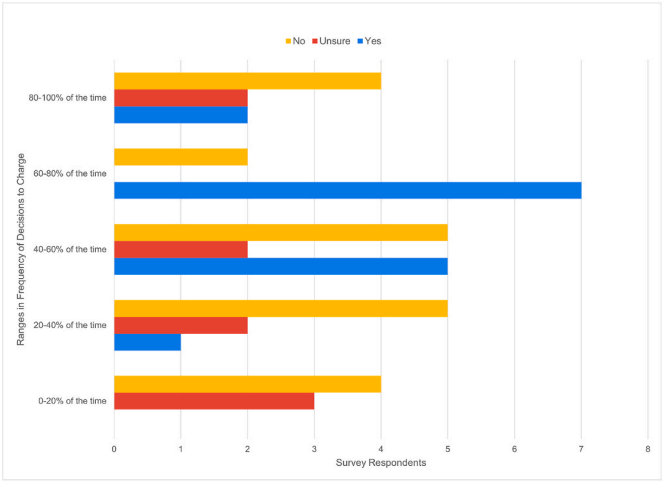

Fig. 42. Whether prosecutor respondents had ever encountered due diligence issues didn't appear to influence their decisions to charge.

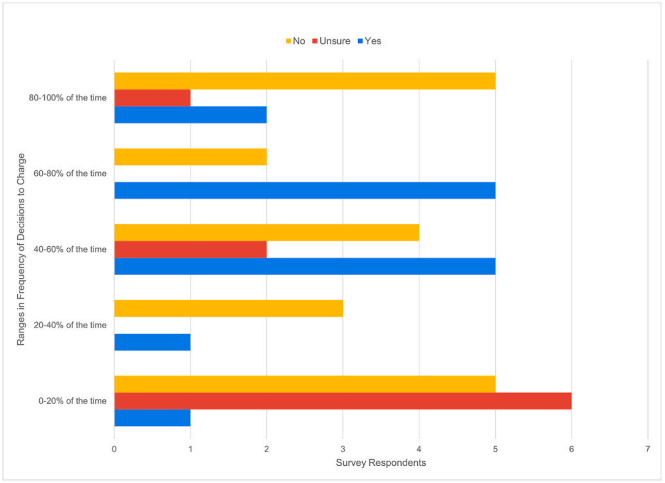

Fig. 43. Whether prosecutor respondents had ever encountered due diligence issues didn't appear to influence their decisions to plea bargain, either.

devolve into tunnel vision and other confirmation biases, where the evidence supports an investigator's case hypothesis whether right or wrong [53].

Some of this risk can be mitigated through screening cases up front. Doing so allows investigators to communicate with prosecutors about what evidence was found or not found, or questions they're able or unable to answer. These pieces of information, said B.H., help prosecutors decide whether to move forward.

That strategy assumes, however, that prosecutors and investigators know how and what to communicate. Given criticisms of the shortcomings in more conventional forensic sciences, including DNA testing [54] or fingerprint analysis methodology [55], prosecutors who don't understand technology can't keep up with its advances, or the resulting adaptations in forensic processes [33].

For example, consider that a digital forensic tool's performance relies on its ability to parse data structures [56], such as the SQLite databases that underlie most mobile apps. "How the tables are structured are very different from database to database," B.H. explained. New apps and databases, as well as regular app updates, make it possible for digital forensics tools to be outpaced [50].

The result, B.H. said, that the amount of data that can be parsed "ebbs and flows." "So by the time GrayKey[5] can crack an iPhone 11, the iPhone 12 is already out, and it can't crack the iPhone 12 yet," K.T. explained. "On cross examination, any good defense attorney is going to ask, 'Well, this can crack every phone, right?' And they're just sowing doubt about the reliability of the [forensic] technology." At that point, said L.H., the issue isn't so much the science as it is variables like the access that other people besides the defendant had to a device, which can help a defense claim that the evidence doesn't definitively place the defendant behind the device.

K.T. said the ability to communicate about issues like this comes down to good observational skills, in particular the ability to compare reports across cases. "It's looking at the [digital forensic] reports and saying, 'Wait a second, I should have these photos on here, and I don't,'" she explained. "It's stuff that should be there if the request that I made was fully executed. Or I should know why it's not there. And I've had to do follow-ups that have resulted in, 'We didn't have that [or] we didn't include that,' whatever variation." B.H. concurred, calling forensic tool parsing errors "very noticeable."

Yet C.D. sees less and less testing as technology continues to advance. Although the verification of data is more likely to happen when a case goes to trial, said B.H., jury trials have become vanishingly rare—by his estimate, just twice per year on cases that rely heavily on digital evidence. "That's just because usually the evidence is what it is. It's not like an eyewitness with, 'Did you really see it? Is it really him?'" he explained.

But the result, said H.W., is plea bargaining practices ensuring that "the tools that are involved aren't put to the test." The result, said B.H.: forensic examiners might not feel the need to verify a tool's results, particularly if their software has been "very reliable for a very long period of time." B.H. added: "And so the odds that we're going to go back and check the hex [code] [to see] exactly what's going on is going to be less often in that situation," especially if the data makes logical sense.

Indeed, whether rapidly advancing technology would continue to be admissible in court was a concern for most of the prosecutor respondents, even if they didn't believe a tipping point, where technological advances outpace the ability to educate jurors about them in court, had yet been reached. Of note: about one-third of the investigators, compared to one-fifth of the prosecutors, thought the tipping point had already been reached. Very few in each group believed that current practices would continue to suffice, and about 15% said they didn't know (see Figs. 44 - 46).

The trend away from demonstrating digital forensics' scientific foundations in court comes at a time when technology is becoming more complex and abstract. Artificial intelligence is perhaps the best example of complexity; reportedly, even experts in the field can find it difficult to explain the technology [57]. B.H. said it's more useful as an investigative tool, "… trying to [go from 2 million videos or images down to 200] as opposed to spending nine years looking through every video on somebody's phone," he explained, "but I would never charge off that."

That said, he and other prosecutors have seen more litigation around discovery of, first, how the software works—for which typically all that's needed is for an expert to come in and explain—and, second, how investigators identify [evidence such as] explicit or exploitative images.

[5] A physical device that relies on unknown vulnerabilities to bypass USB Restricted Mode to break passwords on encrypted iOS and Android devices. *See* https://www.grayshift.com/graykey/and https://www.vice.com/en/article/m7e498/how-grayshift-keeps-its-iphone-unlocking-tech-secret accessed 22 October 2022.

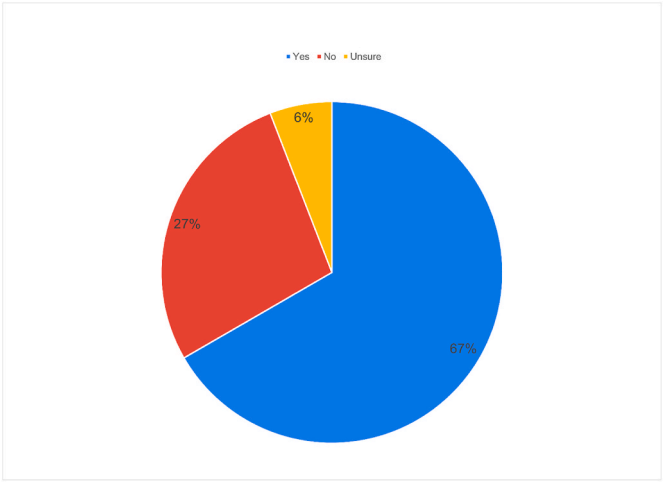

Fig. 44. About two-thirds of prosecutor respondents expressed concern about digital evidence admissibility.

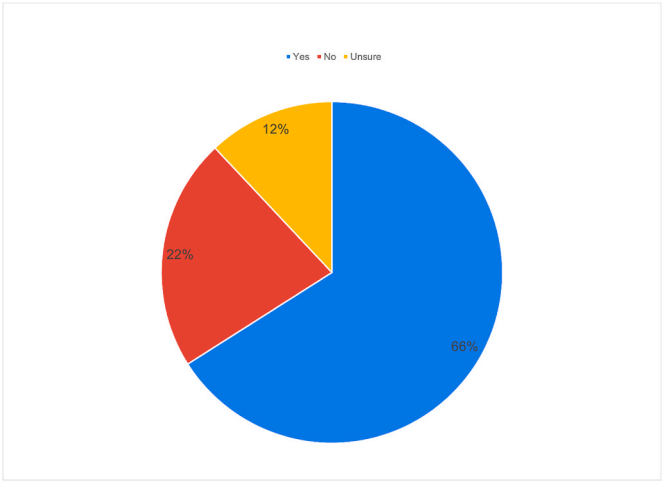

Fig. 45. Although more prosecutors were unsure about jurors' ability to weigh digital evidence appropriately compared to those who were unsure about its admissibility, the majority of respondents again expressed concern about jurors' ability to weigh digital evidence in deliberations.

Indeed, most digital forensic tools are a proprietary "black box" disallowing the examination or testing of source code [10]. Likewise some methods conducted by private-sector forensic labs, which often relies on exploiting vulnerabilities in hardware or software [58,59].

Judges' determination of whether the evidence is allowable at trial could depend on defense attorneys' knowledge of digital evidence. The survey didn't explore this variable, but the prosecutor interviewees anecdotally suggest wide variances depending mainly on location. For instance, some interviewees mentioned experience with challenges mounted by better resourced defense attorneys from large metropolitan areas. Others said defense attorneys in their states generally didn't seem to be well versed in digital evidence issues at all, resulting in fewer challenges. A.B., a former public defender and now a prosecutor in the upper Midwest, said in spite of many public defenders' relative youth, their knowledge about the evidentiary aspects of digital data often takes a back seat to their general knowledge about the technology. Other times, said B.H., attorneys might be knowledgeable "just enough to know to challenge something, but not educated enough to really know what the issue is." That, he added, is a matter of training: as limited as opportunities are for prosecutors, they're even more limited for criminal defense attorneys.

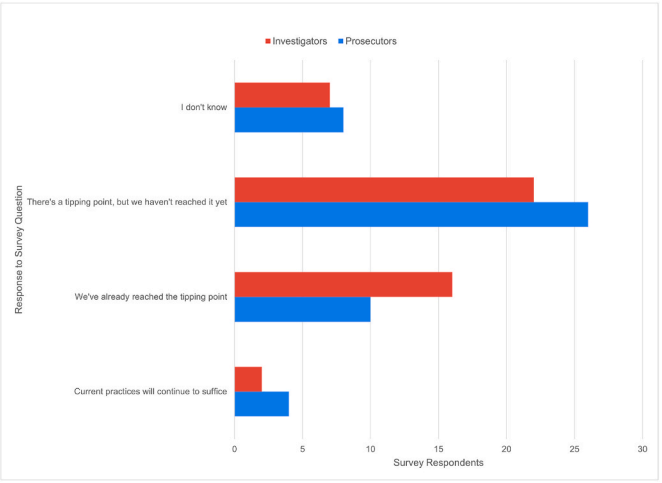

Fig. 46. Prosecutors generally believe technology hasn't yet outstripped forensic tools' explainability. Many more investigators than prosecutors believe the technological tipping point has already been reached.

In general, said J.S.: "Some [defense attorneys] are fielding very impressive and sophisticated challenges to evidence [with] relatively creative and interesting legal arguments …. But there are also a lot of lawyers who are cutting and pasting stock motions, making very vague general allegations."

That vagueness, J.S. continued, could be problematic for case law. Cogent arguments force prosecutors to research and respond, while "generic throw everything at the wall and see what sticks" motions make for a trial tactic that can confuse judges. In turn, judges' lack of knowledge about digital forensic tools and techniques often lead to skepticism around validity [4].

Aggressive pretrial motion practices can help, said H.W., a strategy that B.H. agreed has served him well. "If a judge was having to make a call at the moment they were first hearing about it, they would likely come to a different answer as opposed to [being] able to take some time to think about it and hear from an expert," he explained.

Indeed, how well judges understand any kind of scientific evidence has bearing on their role as "'gatekeepers … obligated to determine whether the methods and principles underlying proffered expert testimony are … reliable and valid." [7] Improving judge training is one solution, of course, but so is timely, systematic, standards-based tool and technique validation and evaluation [4].

One systemic solution could be "a new National Digital Evidence Policy, to be spearheaded by a National Digital Evidence Office" to coordinate and connect law enforcement efforts to obtain digital evidence in a way that would still support civil liberties and ensure transparency [28]. Still, laws that would establish and fund such an office – and any other such initiatives – remain behind the times because legislators are used to a pace that doesn't keep up with technology.

Indeed, U.S. judges are dealing with markedly wide variances in how digital evidence is treated across states. For example, said B.H.: "States like California and New York, on one extreme, have very encompassing state statutes … that [affect] almost every step of those investigations. And then you have states [that are almost] a developing country where there's not a lot." Attorneys in the latter, he added, end up turning to federal case law to build their arguments.

In part, B.H. said, that's because technology-based crime was for many years considered the domain of federal law enforcement. "It's really been in the last 10 years where the states have [realized] there's too much of it [and] are racing to catch up," he explained.

For example, child exploitation offenses that don't meet federal thresholds – when the offender is located in the same state as the victim (s) – come to local law enforcement and prosecutors via National Center

for Missing and Exploited Children (NCMEC) CyberTipline reports, which reported nearly 22 million tips in 2020, an increase of 28% from 2019; and in 2021, more than 29 million tips [60].

Even at that, though, B.H. said many lawmakers approach criminal law updates in terms of more conventional crimes. "When we sit down and [say], 'Hey, it's really bad that that's been unchanged in 10 years,' you can get weird faces," he explains. For example, although many states have criminalized intimate image abuse ("revenge porn"), many still don't regard it as a felony [61].

"The law was not written with this type of evidence in mind," said L. H. "Sometimes that creates a conflict where it's unclear how some aspects of the law would apply to digital evidence … on a strict analysis versus a more relaxed analysis, reasonable minds can differ on some of those issues." She points to self-driving cars as an example. "I don't know about the legal ability to differentiate between a motorist's liability in a collision, versus a malfunction with the computer, and how that will affect litigations in the future," she said, anticipating these kinds of issues will only accelerate as more data sources become available. "Judges can initiate local court rules," she said. "But I don't know if they are ready to, or fully understand how that would work."

Moreover, L.H. added, court rules can only go so far, and legislators don't prioritize issues that are "not terribly sexy or appealing to their voting base." Put another way, said C.D., legislators may try to solve problems, but follow lobbyist whims when they don't sufficiently understand the full scope of the problem. While prosecutors in many states can and do lobby legislators, research indicates that only about 15% of the more than 22,000 criminal law and criminal justice bills introduced in the 50 state legislatures over a four-year period involved changes in procedural limits, of which evidentiary requirements were just one [62].

In contrast, more than 40% of the bills increased either the scope of criminal law, or the sentencing range, compared to only 11% of bills which sought to reduce the scope of criminal law or punishment [62]. Indeed, political lobbying can seem "determined to eradicate any form of immoral cyber behaviour through draconian, result-oriented legislation." [44].

Together, these factors may create a disincentive for forensic examiners—and thus prosecutors—to go very deep in understanding, much less being able to explain, the technology they use. "[They're] going to take shortcuts, and they're … not getting called on it, not getting tested on it, not getting cross-examined on it, [so] they'll keep doing it," said C.D. "In the end, [scrutiny] winds up coming from newspapers, and … that just undermines public confidence in law enforcement." C.D. believes the solution is for prosecutors to take the lead "to ensure that there's more accountability, responsibility and standard operating procedures that make sense," he said.

Even so, the digital forensics industry itself is meeting the demand for more surgical data targeting based on time and date ranges, or only certain types of content. Although this practice both saves time and preserves the privacy of people whose devices and/or accounts are under review [63], it also risks the failure—at least in some U.S. states—to capture potentially exculpatory data, and thus comply with broad discovery requirements [64].

In the interests of serving justice, then, prosecutors must walk a fine line between their relationship with the voting public, and their relationships with the police who supply the evidence that helps them build cases based on the most informed decisions possible.

5. Conclusions

At a time when debate is intensifying around U.S. prosecutors' role in issues like mass incarceration, momentum has grown to reform prosecutors' role and thus, the U.S. criminal justice system as a whole [11]. Recent efforts in this regard include reforming the way prosecutors rely on various forms of evidence [13].

However, these interviews consistently referred to the infrequency of jury trials in the United States. Although trial strategy is top of mind for the interviewees, the low likelihood of going to trial may influence prosecutor decisions broadly. Thus a prosecutor who is unfamiliar with digital evidence, and who does not have access to a peer with familiarity, may not have a full grasp of how strong or weak the evidence against the defendant really is. Further, fewer jury trials result in fewer opportunities for either prosecutors or investigators to participate in admissibility hearings. That could become more problematic as technology becomes more complicated.

Indeed, the research results indicate that the frequency with which investigators and prosecutors encounter, and then rely on, digital forensics evidence in their cases varies, both broadly and for different types of cases. Prosecutors' more conservative approaches may speak to the difference between investigative leads and evidence, or alternatively, an under-utilization of digital evidence in prosecution. This should be explored among both cohorts.

At the same time, though, most respondents make decisions based on whether the evidence strengthens their cases. Prosecutors need to be equally concerned with whether digital evidence could be considered exculpatory, especially given the number of respondents who had encountered (or couldn't be sure if they had encountered) at least one case where digital evidence didn't provide an accurate picture of what happened.

Again, because of the small sample size of survey respondents, these findings should be tested with more detailed research across larger cohorts. In particular, the findings touch on five major areas in need of stronger research and development support:

- Training
- Specialized prosecutors
- Support for the science of digital forensics
- Gap analysis
- Legislative advocacy

5.1. A need for better training

The prosecutor interviewees identified the need for digital forensic expert witnesses who can explain digital evidence without over-explaining it to judges and juries. Training can help fill this gap, helping prosecutors to gain a better understanding of investigators' processes and paving the way for necessarily stronger relationships.

However, training priorities are driven by crime severity, as reflected in a state's legislation and, in turn, the personnel, equipment, and training resources devoted to it. As a result, investigator training outpaces prosecutor training in digital evidence, resulting in two problems. First, training that addresses the legal implications of digital evidence, as well as legal rules and procedures around evidence that comes from third parties or that is "triaged" from devices before a full forensic examination, appears to be lacking even for investigators.

Second, many prosecutors struggle to attend courses owing to cost, location inconvenience, and time away from the office, among other factors. Whether these training limitations affect prosecutors' interest in or likelihood of specialization is unknown. Regardless, however, prosecutors appear to find themselves more or less on their own when it comes to becoming well trained on various aspects of digital evidence.

Although this lack of prosecutor-oriented training has resulted in prosecutors who are driven to find answers, it also indicates a field of unevenly distributed prosecutors with varying perspectives on three aspects of digital evidence: its technological complexity, its application to various types of cases, and how to handle it in court, particularly when it comes to educating fact-finders. This makes for a gap in knowledge that has potentially profound implications for the use of digital evidence in criminal prosecutions. When attorneys are trained to handle digital evidence, though, it improves their hands-on involvement with the investigators who acquire and analyze it. In turn, that improves their ability to assess any problems with the digital evidence being

offered.

Training that brings together prosecutors and investigators would be valuable towards improving relationships, communication, and understanding of each group's requirements when it comes to evidence: not just on how the technology works, but also what to do with it. Bolstering awareness of the scientific foundations of digital forensics in particular may improve prosecutors' ability to ask better questions of their expert witnesses.

To that end, commercial entities offering certification training to digital forensic examiners are encouraged to consider offering training to legal professionals, not only in how to read reports, but also the forensic science principles behind their tools.

At the same time, better and more extensive CLE training in digital evidence is also needed, or perhaps more logically, the incorporation of digital evidence handling into existing CLE courses. (The extent to which digital evidence is already incorporated is unknown and therefore worthy of exploration.) For example, more information is needed on the degree to which digital evidence is considered relevant to prosecutor priorities such as drug-induced deaths, vehicular crimes, domestic violence, or even conviction integrity.

Additionally, how prosecutors' offices of all sizes budget both money and time for training overall, and their requirements for training beyond annual CLEs, requires both more study and more consideration given how many survey respondents faced significant barriers to training. Whether prosecutors are offered dedicated training time over and above vacation time, how often they take the time, and whether they tend to seek training online or in nearby locations rather than travel are all important questions. Likewise factors influencing prosecutors' decisions, such as trial dates and the availability of other prosecutors to assist with casework.

Finally, worth studying would be how training and professional development in digital evidence affects prosecutors' sense of competence, how manageable their workloads are, and their degree of burnout when working criminal cases involving digital evidence.

5.2. A need for specialized support

Whether an office has access to a digital evidence specialist appears to influence certain prosecutorial decisions. That said, the cohort was too small to determine whether access to a specialist can predict how frequently prosecutors make these decisions. Additionally, the survey was not designed to measure specialist effectiveness. In addition, whether research could answer these questions is uncertain given how unevenly distributed digital evidence specialists, and access to them, are across the nation.

In particular, the survey results revealed an informally tiered structure in which some prosecutors, whether assigned or volunteered, serve as specialist legal counsel in digital evidence matters for other prosecutors, but not necessarily to investigators.

Although likely that investigators work with prosecutors who can guide them on the types of investigations they're performing, these prosecutors may or may not have a deep understanding of digital evidence, and may or may not have access to—or know where they can access—specialist peers who can support their decision-making.

Thus, the potential value of a specialist role cannot be understated. Specialist prosecutors could wield particular leverage in advocating for more specialists: not only encouraging the professional development of others within their own offices, but also mentoring and facilitating their roles as formal or informal resources beyond their own jurisdictions.

Of course, it is necessary to understand how familiar with digital technology, and case law surrounding it, prosecutors are generally, as well as the extent to which they rely (or don't rely) on a specialist to answer their legal and/or technical questions. Likewise whether they can provide adequate guidance for law enforcement when it comes to search warrants, arrests, and other actions on multiple kinds of cases involving digital evidence, as well as their response when little case law or legislation exists to guide investigators and their actions. Finally, it would also be interesting to learn how digital evidence—and/or the presence of a digital evidence specialist—affects a prosecutor's office's budget and case priorities.

5.3. A need for more emphasis on the science of digital forensics

The trend away from demonstrating digital forensics' scientific foundations in court comes at a time when technology is becoming more complex and abstract; in other words, more necessary than ever to be able to explain, but with fewer opportunities to do so.

Thus, with conviction integrity units being implemented in a number of urban prosecutors' offices across the country [65], the review of digital evidence on a similar scale as DNA and other evidence would be valuable. Likewise exploring prosecutor confidence in digital evidence or the methods used to obtain, analyze, and verify it.

That said, both prosecutors' and investigators' uncertainty regarding the existence of digital forensics laboratory SOPs, or the frequency with which they are implemented, is troubling. Although more engaged and/or specialized prosecutors appear more likely to spot due diligence issues, and to be certain they haven't encountered due diligence issues, more engagement with investigators also heightens the risk of cognitive biases.

To that end, it would be valuable to understand whether training and/or access to a specialist makes a difference in the way prosecutors and investigators communicate, and consequently, how prosecutors assess the evidence and what it could mean for their cases.

5.4. A need for more analysis

Because the survey questions on decision-making did not include case screening or sentencing recommendation decisions, future research is recommended to explore the impact of digital evidence on these as well as the decisions that were explored. Furthermore, prosecutors' perception of both judges' awareness and jury composition where they work would provide additional perspective.

Of course, digital evidence is far from the only factor in the complex set of variables that go into a prosecutor's decision-making. One potential area for future research includes the influence of prosecutor experience, both as a whole and specifically with digital evidence, on their decision-making. Comfort levels, trial strategies, and crime types are just some of the factors to examine further.

The relationship between prosecutor experience, assignment, and their level of comfort with digital evidence may also impact their communication with investigators. As the results suggest, digital data might be somewhat less apparent or necessary in a domestic violence or property crimes case, for instance, than in a case for Internet crimes against children or fraud. Regardless of assignment, whether prosecutors have the resources—time, budget, training, access to a specialist—to devote sufficient attention to digital evidence relative to other forms of evidence is an important question to answer.

Finally, research is needed to determine how well defense attorneys understand digital evidence and in particular, the quality of challenges they make to digital evidence in court. Corollary research could include whether a prosecutor's success or failure introducing or relying on digital evidence in their cases affects the likelihood they'll rely on it in the future.

5.5. A need for better advocacy

The research revealed multiple problems with current laws and legislative efforts, from inconsistency across state statutes to laws that lag behind the pace of technological development and legislators who lack adequate understanding of the issues. Owing to their existing lobbying efforts, prosecutors are well positioned to lead in demanding better standards and accountability. Although this creates a fine line to

walk between prosecutors' relationship with the voting public, and their relationships with the police who supply the evidence that helps them build cases, it is a necessary line to walk.

That innocent people are wrongfully convicted and imprisoned based on flimsy evidence is unquestionable. Likewise the number of crimes going unsolved, and thus unprosecuted. Given the challenges with digital evidence, prosecutor burnout and attrition, and other challenges, the introductory question around whether it is time to rethink prosecutorial "business as usual" remains. Although the efficacy of prosecutorial reform projects such as aspects of restorative justice, e.g. "drug courts," is beyond the scope of this research, it may be well worth considering whether such projects could effectively bypass the need for digital forensic analysis in many, if not the most severe felonies, lifting a significant burden from both investigators' and prosecutors' shoulders while continuing to serve justice.

Declaration of competing interest

The author declares that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] National Police Chiefs Council, Digital Forensic Science Strategy, July 2020. https://www.npcc.police.uk/Digital%20Forensic%20Science%20Strategy%202020.pdf. (Accessed 1 October 2022).

[2] Radina Stoykova, The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations, September 2022, https://doi.org/10.2139/ssrn.4232504. Available at SSRN: https://ssrn.com/abstract=4232504.

[3] Committee on identifying the needs of the forensic sciences community, National Research Council, August 2009. Strengthening Forensic Science in the United States: A Path Forward, https://www.ojp.gov/pdffiles1/nij/grants/228091.pdf. (Accessed 5 November 2022).

[4] Sean E. Goodison, Robert C. Davis, Jackson, Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, RAND Corporation, Santa Monica, CA, 2015. https://www.rand.org/pubs/research_reports/RR890.html.

[5] James R. Lyle, Barbara Guttman, John M. Butler, Sauerwein Kelly, Christina Reed, Corrine E. Lloyd, Digital Investigation Techniques: A NIST Scientific Foundation Review, National Institute of Standards & Technology, May 2022, https://doi.org/10.6028/NIST.IR.8354-draft [draft report].

[6] Marcia Shein, Proffer agreement in a federal criminal case" [blog]. Shein, brandenburg & schrope federal criminal law center. https://federalcriminallawcenter.com/2017/01/proffer-agreement-federal-criminal-case/, January 5, 2017. (Accessed 23 June 2022).

[7] David Faigman, Evidence: admissibility vs. Weight in scientific testimony, in: The Judges' Book, vol. 1, 2017. Article 11. Available at: http://repository.uchastings.edu/judgesbook/vol1/iss1/11. (Accessed 17 August 2021).

[8] Kashmir Hill, Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone, The New York Times, November 22, 2019. https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html. (Accessed 30 April 2021).

[9] Isidoro Rodriguez, 'Outrageous outcomes': plea bargaining and the justice system, The Crime Report, https://thecrimereport.org/2022/04/08/outrageous-outcomes-plea-bargaining-and-the-justice-system/, April 8, 2022. (Accessed 6 November 2022).

[10] Martin Novak, Digital evidence in criminal cases before the U.S. Courts of appeal: trends and issues for consideration, Journal of Digital Forensics, Security and Law 14 (4) (2020).

[11] Lantigua-Williams, Juleyka, Are prosecutors the key to justice reform? Atlantic (2016). May 18, https://www.theatlantic.com/politics/archive/2016/05/are-prosecutors-the-key-to-justice-reform/483252/. (Accessed 4 August 2021).

[12] Jessica Brand, The epidemic of brady violations: explained, The Appeal (2018). April 25, https://theappeal.org/the-epidemic-of-brady-violations-explained-94a38ad3c800/. (Accessed 4 August 2021).

[13] Daniel S. Lawrence, Camille Gourdet, Duren Banks, Michael G. Planty, Dulani Woods, Brian A. Jackson, Prosecutor Priorities, Challenges, and Solutions, The RAND Corporation, 2019. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2800/RR2892/RAND_RR2892.pdf accessed 8 June 2021.

[14] Patricia Hurtado, Francesca Maglione, Bloomberg, In a post-Roe world, more miscarriage and stillbirth prosecutions await women, Fortune (2022). July 5, https://fortune.com/2022/07/05/roe-v-wade-miscarriage-abortion-prosecution-charge/. (Accessed 7 October 2022).

[15] World Population Review, Incarceration rates by country 2022. https://worldpopulationreview.com/country-rankings/incarceration-rates-by-country. (Accessed 16 October 2022).

[16] Nelson Bunn, Overworked and Understaffed: the Shifting Landscape in Local Prosecutor Caseloads, National District Attorneys Association, February 2020. https://ndaajustice.medium.com/overworked-and-understaffed-the-shifting-landscape-in-local-prosecutor-caseloads-122f7ef5e4f1. (Accessed 21 April 2022).

[17] Nelson Bunn, Emily LaGratta, Setting the Record Straight on the Current and Future Role of Prosecutors." Route Fifty, December 2021. https://www.route-fifty.com/public-safety/2020/12/current-and-future-role-prosecutors/170746/. (Accessed 21 April 2022).

[18] Stacy Miles-Thorpe, Trauma for the tough-minded prosecutor, The Texas Prosecutor (2016). July-August, https://www.texasbar.com/AM/Template.cfm?Section=Home&Template=/CM/ContentDisplay.cfm&ContentID=36322. (Accessed 4 August 2021).

[19] Peter Lee, Exploring Trauma in Child Exploitation Investigators, Centre for Research and Evidence on Security Threats, December 2020. https://crestresearch.ac.uk/resources/exploring-trauma-in-child-exploitation-investigators/. (Accessed 1 March 2021).

[20] Instituto de Empresa, What are the private, public and nonprofit sectors—and which one is right for you? [blog] October 11, https://www.ie.edu/school-global-public-affairs/about/news/private-public-nonprofit-sectors/, 2018. (Accessed 23 April 2022).

[21] Clare Duffy, Wanted: millions of cybersecurity pros. Salary: whatever you want, CNN Business, 2021. May 28, https://www.cnn.com/2021/05/28/tech/cybersecurity-labor-shortage/index.html. (Accessed 4 August 2021).

[22] Mary J. Hahn, Using digital evidence to strengthen hate crime prosecutions, DOJ J. Federal Law Pract. (March 2022).

[23] Tom Erik Erlandsen, Fallacies when Evaluating Digital Evidence Among Prosecutors in the Norwegian Police Service", Master's thesis, Norwegian University of Science and Technology, June 2019.

[24] M. Rogers, K. Scarborough, K. Frakes, C. Sail Martin, in: P. Craiger, S. Slienoi (Eds.), IFIP International Federation for Information Processing, Volume 242, Advances in Digital Forensics III, Springer, Boston, 2007, pp. 41–52.

[25] Spyder Forensics, Fire – forensics of internet related evidence (live remote training – AEDT – UTC +11) [course description], https://www.spyderforensics.com/events/fire-forensics-of-internet-related-evidence-live-remote-training-aedt-utc-11/. (Accessed 29 July 2021).

[26] Magnet Forensics, Upcoming training courses [course catalog], https://training.magnetforensics.com/w/upcoming/. (Accessed 29 July 2021).

[27] William A. Carter, Jennifer Daskal, William Crumpler, Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge, Center for Strategic and International Studies (CSIS), July 2018. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf. (Accessed 5 August 2021).

[28] Christa Miller, Teaching digital forensics during a pandemic: present and future strategies." forensic focus. https://www.forensicfocus.com/articles/teaching-digital-forensics-during-a-pandemic-present-and-future-strategies/, November 12, 2020. (Accessed 29 July 2021).

[29] Law Enforcement Cyber Center, Training. https://www.iacpcybercenter.org/topics/training-2/. (Accessed 15 June 2021).

[30] Cellebrite Inc, Cellebrite legal professionals training (CLPT). https://www.cellebritelearningcenter.com/mod/page/view.php?id=15848. (Accessed 15 June 2021).

[31] American Bar Association, Mandatory CLE [web page], https://www.americanbar.org/events-cle/mcle/. (Accessed 25 April 2022).

[32] National District Attorneys Association, Publications & videos [web page], https://ndaa.org/resources/publications-videos/. (Accessed 22 October 2022).

[33] David W. Hagy, Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, National Institute of Justice, 2007. https://www.law.du.edu/images/uploads/library/evert/DigitalEvidenceinTheCourtroom.pdf.

[34] Sara Morrison, Here's How Police Can Get Your Data — Even if You Aren't Suspected of a Crime, Vox Media Recode, 2021. July 31, https://www.vox.com/recode/22565926/police-law-enforcement-data-warrant accessed 11 October 2022.

[35] SecurityArchitecture, Subpoena? Court order? Search warrant? How the government can get your data, May 10, https://www.securityarchitecture.com/supoena-court-order-search-warrant-how-can-the-government-can-get-your-data/, 2015. (Accessed 2 March 2021).

[36] Bradford Oliver, What is on-scene digital forensic triage?" ADF solutions blog. https://www.adfsolutions.com/news/what-is-on-scene-digital-forensic-triage, March 30, 2021. (Accessed 18 June 2021).

[37] Brett Shavers, Placing the Suspect behind the Keyboard. Syngress, February 2013. https://www.elsevier.com/books/placing-the-suspect-behind-the-keyboard/shavers/978-1-59749-985-9. (Accessed 18 June 2021).

[38] Bruce Frederick, Vera publishes results of study exploring prosecutorial decision making [blog] The Vera Institute. March 13, https://www.vera.org/news/vera-publishes-results-of-study-exploring-prosecutorial-decision-making, 2013. (Accessed 6 May 2022).

[39] Lindsey Devers, Plea and Charge Bargaining: Research Summary, Bureau of Justice Assistance, Washington, DC, 2011. https://perma.cc/TQR8-79JU. (Accessed 6 May 2022).

[40] The Blanch Law Firm, FAQ: how does a prosecutor decide whether or not to file charges? [blog] August 1, https://www.theblanchlawfirm.com/blog/faq-how-does-a-prosecutor-decide-whether-or-not-to-file-charges/, 2016. (Accessed 29 May 2022).

[41] Angus-Anderson Wendy, Authenticity and Admissibility of Social Media Website Printouts, 2015, pp. 33–47, 14 Duke Law & Technology Review, https://scholarship.law.duke.edu/dltr/vol14/iss1/2/. (Accessed 4 August 2021).

[42] A.Y. Ofori, D. Akoto, Digital forensics investigation jurisprudence: issues of admissibility of digital evidence, J. Forens. Legal Investigat. Sci. (May 2020), https://doi.org/10.24966/FLIS-733X/100045. (Accessed 16 August 2022).
[43] What happens at a criminal pre-trial?" JUST criminal law blog, October 22, https://www.justcriminallaw.com/criminal-charges-questions/2020/10/22/criminal-pre-trial/, 2020. (Accessed 21 June 2021).
[44] Richard Boddington, A case study of the challenges of cyber forensics analysis of digital evidence in a child pornography trial, Annual ADFSL Conference on Digital Forensics, Security and Law. 6, https://commons.erau.edu/adfsl/2012/thursday/6, 2012. (Accessed 19 June 2021).
[45] Riana Pfefferkorn, 'Deepfakes': A New Challenge for Trial Courts, NWSidebar, 2019. March 13, https://nwsidebar.wsba.org/2019/03/13/deepfakes-a-new-challenge-for-trial-courts/. (Accessed 3 July 2021).
[46] Griffeye Brain, [product description]. https://www.griffeye.com/griffeye-brain/. (Accessed 19 June 2021).
[47] Andrea Monti, Rules of (digital) evidence and prosecution's actual needs. When the law falls behind technology, in: [Conference Paper] Italian Conference on Cybersecurity, ITA SEC, Venice, Italy, 2017.
[48] Hans Henseler, van Loenhout Sophie, Educating judges, prosecutors and lawyers in the use of digital forensic experts, in: Proceedings of the Fifth Annual Digital Forensics Research Workshop, DFRWS, Europe, 2018.
[49] American Bar Association, Standard 3-3.5 Relationship with Expert Witnesses." Criminal Justice Standards for the Prosecution Function, fourth ed., 2017. https://www.americanbar.org/groups/criminal_justice/standards/ProsecutionFunctionFourthEdition/. (Accessed 23 June 2021). accessed.
[50] Alexis Brignoni, Trust but verify: formats, timestamps, and validation, Initializ. Vectors blog (March 17, 2020). https://abrignoni.blogspot.com/2020/03/trust-but-verify-formats-timestamps-and.html. (Accessed 23 June 2021).
[51] Bob Gill, Chris Edquist, Don't leave exculpatory digital evidence on the (lab) table, Voice for the Defense Online blog (2021). March 25, https://www.voiceforthedefenseonline.com/dont-leave-exculpatory-digital-evidence-on-the-lab-table/. (Accessed 23 June 2021).
[52] Linda Geddes, Digital Forensics Experts Prone to Bias, Study Shows, The Guardian, 2021. May 31, https://www.theguardian.com/science/2021/may/31/digital-forensics-experts-prone-to-bias-study-shows. (Accessed 22 October 2022).
[53] Mark Godsey, Blind injustice: how 'tunnel vision' convicts the innocent, The Crime Report, October 23, https://thecrimereport.org/2017/10/23/blind-injustice-how-tunnel-vision-convicts-the-innocent/, 2017. (Accessed 1 April 2021).
[54] Matthew Shaer, The false promise of DNA testing, Atlantic (June 2016). https://www.theatlantic.com/magazine/archive/2016/06/a-reasonable-doubt/480747/. (Accessed 23 June 2021).
[55] Gretchen Gavett, Can unconscious bias undermine fingerprint analysis? Frontline (2012). April 16, https://www.pbs.org/wgbh/frontline/article/can-unconscious-bias-undermine-fingerprint-analysis/. (Accessed 23 June 2021).
[56] Cindy Murphy, What You're Missing in Hidden Apps (And 5 Data Forensic Tools!), , Officer.com, July 22 2016. https://www.officer.com/investigations/forensics/digital-forensics/article/12203542/hidden-mobile-apps-mobile-investigations-forensic-data-tools. (Accessed 14 July 2021).
[57] Will Knight, The dark secret at the heart of AI, MIT Technology Review, April 11, https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/, 2017. (Accessed 2 May 2021).
[58] Interview with martin westman, product specialist, MSAB. Forensic focus, December 20, https://www.forensicfocus.com/interviews/martin-westman-product-specialist-msab/, 2019. (Accessed 19 June 2021).
[59] Cellebrite advanced services: solving your most demanding digital intelligence challenges. https://cf-media.cellebrite.com/wp-content/uploads/2020/11/SolutionOverview_AdvancedServices.pdf. (Accessed 19 June 2021).
[60] By the Numbers, National Center for Missing and Exploited Children, 2021. https://www.missingkids.org/gethelpnow/cybertipline. (Accessed 28 April 2021).
[61] State Revenge Porn Laws, FindLaw, January, 2020. https://www.findlaw.com/criminal/criminal-charges/revenge-porn-laws-by-state.html accessed 28 April 2021.
[62] The Prosecutors and Politics Project, Prosecutor Lobbying in the States, 2015-2018, June 2021. https://law.unc.edu/wp-content/uploads/2021/06/Prosecutor-Lobbying-in-the-States-2015-2018.pdf.
[63] Orin Kerr, Court invalidates cell phone warrant as overbroad, The Volokh Conspiracy (2015). February 23, https://reason.com/volokh/2015/02/23/court-invalidates-cell-phone-w/. (Accessed 19 June 2021).
[64] Jenia L. Turner, Managing digital discovery in criminal cases, J. Crim. Law Criminol. 109 (2) (2019).
[65] Josie Duffy Rice, Do conviction integrity units work?" The appeal. https://theappeal.org/do-conviction-integrity-units-work-a718bbc75bc7/, March 22, 2018. (Accessed 17 August 2021).