Document Title:	**Evaluation of Digital Evidence Processing Efficiencies in Publicly Funded Crime Laboratories: A Formative Study on how Crime Laboratories and Law Enforcement Agencies use Digital Evidence in Case Investigations**
Author(s):	**Martin Novak, Natasha Parrish Crystal Daye, Nichole Bynum, Peyton Scalise, Christopher Williams, Ruby Johnson**
Document Number:	**311544**
Date Received:	**January 2026**

December 2023

Evaluation of Digital Evidence Processing Efficiencies in Publicly Funded Crime Laboratories: A Formative Study on how Crime Laboratories and Law Enforcement Agencies use Digital Evidence in Case Investigations

Final Report

Prepared for
Martin Novak and Natasha Parrish
National Institute of Justice
U.S. Department of Justice
801 7th Street, NW
Washington, D.C. 20531

Prepared by

Crystal Daye, Nichole Bynum, Peyton Scalise, Christopher Williams, Ruby Johnson
RTI International
3040 E. Cornwallis Road
Research Triangle Park, NC 27709

RTI Project Number 0217811.000.004

Contents

Figures

Tables

1. Project Overview

1.1 Background

In 2017, Americans used over 15.7 trillion megabytes (MB) of mobile data, a number that quadrupled from just 3 years before.[1] In 2024, the average North American is predicted to use nearly six times more data than they did in 2018.[2] As digital device use grows exponentially, the criminal justice system has struggled to keep pace with how this information can aid in criminal investigations and how forensic laboratories manage digital evidence (DE) processing and analysis. In May 2020, the National Institute of Justice (NIJ) published the *Digital Evidence: Policies and Procedures Manual* to provide DE collection, handling, and processing guidelines to assist with accreditation.[3] Beyond these federal efforts, the evidence base is slim for best practices in collecting and submitting DE by law enforcement (LE) and triaging, defined as reviewing the material on DE to determine submission need, and processing data by appropriate crime laboratory personnel. However, to manage the exponentially increasing volume of data coming into LE agencies and crime laboratories annually, significant research is needed to develop sustainable models for prioritizing and processing electronic devices and their data and for identifying resources (e.g., evolving technologies) and evidence retention needs given finite storage capacities.

1.2 Goals and Research Questions

This formative study aimed to produce practical knowledge on the uses and value of DE, including increasing investigative intelligence and probative value, and to provide an evidence base for more efficient and effective DE management and processing, which would in turn help eliminate backlogs, optimize available resources, and decrease justice delays. This study was also conducted to respond to NIJ's recent report, *Needs Assessment of Forensic Laboratories and Medical Examiner/Coroner Offices*, which calls to introduce "triaging workflows across staff levels to examine and preserve evidence at the scene or early in the investigation" as a promising practice.[4] The following research questions were answered in response to NIJ's goal to assess existing laboratory protocols and improve our understanding of scientific rationale underpinning existing laboratory processes:

- What protocols, practices, and technologies do crime laboratories and LE agencies have regarding the processing of DE?
- Which established practices result in the highest percentages of successful outcomes?
- What are the most prevalent and impactful gaps affecting case outcomes?

The project was conducted in three phases. Our agency partners-the Houston Forensic Science Center, the Raleigh/Wake City-County Bureau of Identification and consultant Troy Lawrence of the Fort Worth Police Department informed phases one and two.

2. Project Design and Methods

2.1 Phase 1: Crime Laboratory and Law Enforcement Surveys

2.1.1 Crime Laboratory Survey

The RTI project team used data from the 2014 Bureau of Justice Statistics' Census for Publicly Funded Forensic Crime Laboratories to inform the DE laboratory frame for this study. This data collection was chosen because it included the most recent publicly available data, and the data set included a special DE supplement.[5] For the frame of DE laboratories, we included local and state-based laboratories but not regional or national laboratories. We further limited the sample to only laboratories that had a specific section dedicated to computer/cybercrime, which resulted in 80 laboratories.

Critical components of the survey included demographics and laboratory budget, DE characteristics, processing and submission policies, management and retention, and cross-agency communication with respective submitting agencies. DE characteristics included questions regarding the total number of requests for testing, total number of cases completed, total number of cases pending, the types of forensic functions performed by the laboratory (e.g., mobile device analysis, image analysis, video analysis, forensic audio analysis), and the number of tests performed on each type of DE. The DE laboratory survey took about 15–20 minutes to complete. The survey launched on February 22, 2022, and closed on June 28, 2022. To garner more responses, additional targeted outreach efforts were made to nonrespondents in the form of email and phone calls, including additional emails with the survey link, which were sent out to solicit input on March 17, April 6, May 31, June 13, and June 21, 2022. Following these two initial outreach efforts, phone calls were made to all nonrespondents in hopes of obtaining a response. Additional outreach was conducted through various professional organizational channels and listservs to obtain laboratory representatives listed in the survey frame that had not been contacted successfully. Professional organizations leveraged include the American Society for Crime Laboratory Directors (ASCLD), the International Association of Chiefs of Police (IACP) – Technology Subcommittee, the Consortium of Forensic Sciences Organizations (CFSO), and the Forensic Laboratory Needs Technology Working Group (FLN-TWG). Phone calls were made throughout April 2022 and May 2022 to advertise the survey. Upon closing the survey in June, completion data were pulled. A total of 32 crime laboratories completed the full survey while three crime laboratories partially completed the survey for a 40% response rate (n=32).

The full DE crime laboratory survey can be found in Appendix B.

2.1.2 LE Survey

Participating DE crime laboratories were asked the following question in the survey: "How many law enforcement agencies does your laboratory receive digital evidence from? Please list the names of those law enforcement agencies below." A total of 71 law enforcement agencies were identified based on the crime laboratories' responses. Web searches were conducted to determine contact information for the head of the LE agencies or the head of their investigations unit because they were most likely in charge of making decisions around DE submissions. We determined that these individuals would be best-suited to coordinate responses for the survey.

The LE survey consisted of questions regarding identical topics to those of the crime laboratory survey but tailored to LE agencies, including demographics and budget, agency characteristics (e.g., total number of cases involving DE, pending cases involving DE, number of cases per DE type, and turnaround time for DE types), agency processing and submission policies, management and retention, and cross-agency communication with respective submitting agencies. Because of an initially low response rate, an abbreviated survey was developed to boost response and included items determined to be critical to the study.

In October 2022, the team sent a lead letter via email to all the LE agencies included in the survey frame to let them know the survey would be launched on October 31. On October 31, the team launched the survey and sent an email to the frame, which included a link to the survey and their login credentials. The survey inquired about DE data and information from the 2020 calendar year. The year 2020 was chosen because the crime laboratory survey was fielded in 2021, and we wanted to reference a complete calendar year rather than a partial year. The LE survey took about 15–20 minutes to complete.

The first reminder to complete the survey was sent via email on November 16, then reminders were sent weekly from November 23 to January 4, 2023. Because of a low response rate for the full LE survey, the research team decided to condense the survey from 24 items to 16 critical items, which took approximately 10 minutes to complete. The critical items survey was launched on January 10 and was announced via email to all the outstanding respondents. The final reminder to complete the critical items survey was sent on February 17, and the survey was closed during the first week of March 2023.

A total of 16 LE agencies completed the full survey while eight law enforcement agencies completed the critical items survey for a 34% response rate. The full law enforcement survey can be found in Appendix C and the critical items LE survey can be found in Appendix D. We then selected a purposive subset of DE crime laboratories and their LE partner agencies for in-depth qualitative interviews as part of Phase 2 of the study.

2.2 Phase 2: Qualitative Study

Phase 2 of the study involve qualitative interviews to build on the taxonomy of DE approaches revealed by crime laboratories and law enforcement agencies during Phase 1. The goal of the interviews was to pair LE agencies with a crime laboratory to which they submit DE to gain a deeper understanding of the relationship between the two entities. The 10 individuals who participated in the qualitative interviews represented LE investigators (3) and crime laboratory personnel (7), with varying degrees of DE experience. We interviewed three pairs of LE and partner crime laboratories. All interviewees except one participated in the survey.

Interviews were conducted via Zoom between May and August 2023. Informed consent was obtained before interviews were conducted, and all interviews were recorded solely for notetaking and analysis purposes. The interviews followed a semi-structured qualitative study instrument (Appendix E and Appendix F), which allowed interviewers to ensure they covered all the main topics while allowing for new ideas and topics to emerge during conversation. The qualitative study instruments were developed by the study team to capture information related to agency resources, interagency communication, and evidence management and retention policies. Each recorded interview was transcribed and later coded in NVivo 12.0 for analysis and identification of emerging themes.

2.3 Phase 3: Development of Research Brief for Crime Laboratories and Law Enforcement Agencies for Using DE in Case Investigation

Based on the results from Phase 1 and Phase 2 of the project, the team created a research-informed brief for crime laboratory and LE personnel who are interested in improving their agency's ability to analyze and use DE. The goal of this brief was to provide stakeholders with foundational DE knowledge while sharing promising practices that emerged in Phase 1 and Phase 2 of the project. The brief consists of a review of existing literature regarding DE, methods for both the crime laboratory and LE surveys and qualitative interviews, and findings for both the crime laboratory and LE surveys and qualitative interviews. It concludes with recommendations for both crime laboratory and law enforcement agencies to consider implementing for efficiently using DE in case investigation practices.

The research team collaborated throughout the development stage of the brief to ensure that key findings from Phases 1 and 2 were reflected in the final brief. The brief was reviewed by subject matter experts prior to being finalized (Appendix G).

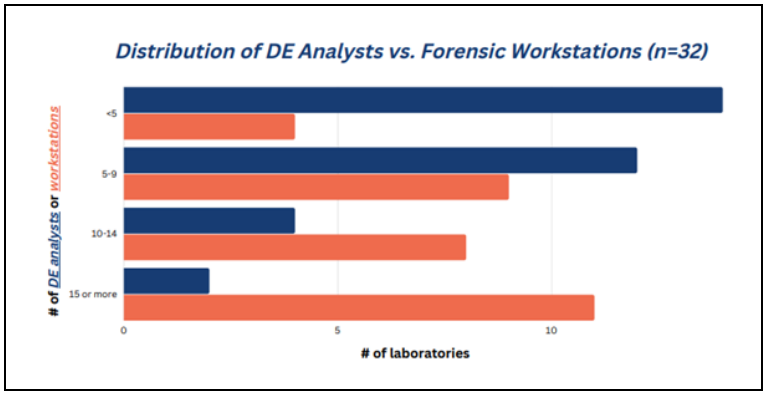
3. Outcomes

3.1 Results and findings

3.1.1 Crime Laboratory Survey

Demographics. Of the 32 crime laboratories that participated in the survey, 86% (n=30) served a jurisdiction of over 500,000 people while 46% (n=16) had an annual budget of $5,000,000 or more. Less than one-third of respondents (29%, n= 10) had a budget specifically for processing DE that was less than $500,000. The distribution of DE analysts vs forensic workstations in the laboratory setting was notable in that many laboratories have less than five DE analysts (40%, n=14) but more than 15 forensic workstations (31%, n=11) (**Figure 3-1**). This could be attributed to a lack of staff or simply funding allocated specifically for DE processing. Over half of respondents were accredited to process DE (66%, n=23), with the majority being accredited by ANSI/ANAB (91%, n=21), followed by A2LA (9%, n=2).

Figure 3-1. Distribution of Analysts Specifically Assigned to Process DE Related to the Number of Forensic Workstations Available in Various Laboratories



DE Characteristics. The total number of requests for training involving DE submitted to responding crime laboratories ranged from 28 to 4, 145 requests in calendar year 2020, and the number of cases involving DE completed in calendar year 2020 ranged from 25 to 4, 145. Responding crime laboratories reported a range of 0 to 300 cases involving DE submitted in calendar year 2020 but pending analysis as of January 1, 2021. Approximately 97% (n=34) crime laboratories performed mobile device analysis, 91% (n=32) performed computer forensics, 77% (n=27) performed video analysis, 57% (n=20) performed image analysis, and 37% (n=13) performed forensic audio analysis. Respondents also performed other forensic functions, including mobile device repair, Chip-Off, internet service providers (ISP), drone forensics, skimmer forensics, network forensics, and wireless network (cellular carrier) records analysis. The two most common evidence types processed by laboratories were overwhelmingly mobile devices and computers, with these devices taking up approximately, on average, 78% of total DE processing requests.

DE Processing and Submission Policies. A major focus of the survey was to determine agencies' DE policies to understand what structures and practices are in place as the demand for DE processing grows at an exponential rate. All respondents had established protocols regarding the intake of DE, and the majority of responding agencies (91%, n=29) had a policy in place for testing DE. Approximately 22% (n=7) of crime laboratories had a policy for prioritizing various DE platforms like texts, emails, and GPS. Over half of DE laboratories (56%, n = 18) had a policy for triaging DE and approximately one-third had a policy for DE retention.

DE Management and Retention. A majority of respondents (91%, n=29) had a computerized system capable of tracking DE. Approximately one-third (n=11) of respondent laboratories had a retention policy in place regarding DE that ranged from 1 month to 5 years. Regardless of retention policy, over one-third (n=13) of respondents reported that their laboratories experience difficulty storing DE. Finally, over two-thirds of respondent laboratories (n=24) had implemented new policies or procedures in the past 5 years to improve efficiency in DE submission.

Cross-Agency Communication and Coordination. With specific regard to cross-agency communication, 28 laboratories reported frequent communication ("often" or "always") with investigating LE officers without a designated liaison for communication whereas 10 laboratories reported a designated liaison. Email was the most common method of direct communication between crime laboratories and the LE agencies they serve (n=16), followed by phone (n=15). Over half of respondents (n=20) had a computerized system that tracks evidence between the crime laboratories and the LE agencies they serve. Only 14% (n=5) of respondents reported that crime laboratory personnel testify in court often regarding their analysis of DE.

Please reference Appendix H for the results of Phase 1.

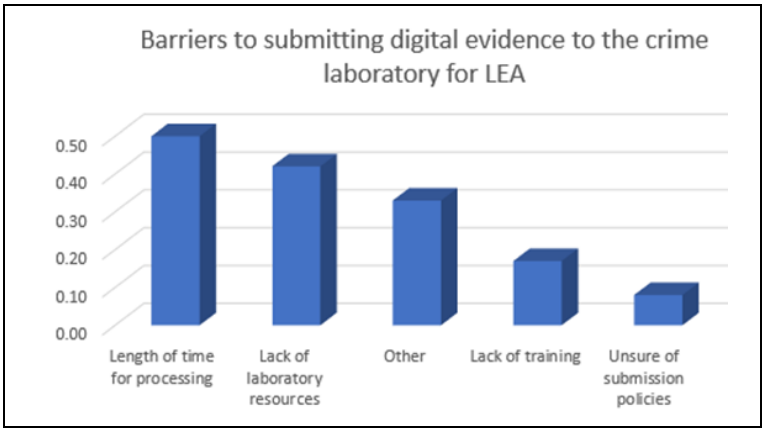
3.1.2 LE Survey

Demographics. In total, 16 LE agencies responded to the full survey while eight responded to the critical items survey. Of the 16 responding LE agencies that specified the size of jurisdiction they serve, about one-third (n=5) served a jurisdiction of 150,000 to 499,999 people. Most LE agencies that completed the survey submitted DE to more than one crime laboratory for processing. Over 70% (n=17) of respondents stated that their agency had the capacity to analyze DE internally. Seven reported that their agency had a specific budget for processing DE, and only one of those respondents reported that the budget was more than $500,000 but less than $999,999. All respondents reported that officers in their agency had received training regarding the seizure of DE, and all but one reported that officers in their agency had received training regarding the processing of DE. Of the 14 agencies that responded, 79% (n=11) received that training on a regular basis while 21% (n=3) received that training only once.

DE Characteristics. Responding agencies reported a total number of cases involving DE ranging from 0 to 1,600 with an average of 296 cases per agency. On average, there were 22 cases per agency from calendar year 2020 that were still pending testing from the laboratory on January 1, 2021, accounting for an average of 19% of their investigative caseload. Phones were the most common source of DE submitted by LE agencies to crime laboratories during 2020, with an average of 68.75 cases per agency. Other common sources of DE submitted included CDs, DVDs, and other storage media (14.8 cases per agency); thumb and external drives (13.8 cases per agency); laptops, tablets, and desktop computers (7.6 cases per agency); and GPS and navigation systems (6.3 cases per agency). Respondents were asked about the average turnaround time in days for the analysis of a variety of DE sources. Computers/removable media submitted on warrant had the longest average turnaround time of 44 days followed by computers/removeable media submitted on consent, which had a turnaround time of 35.8 days. Mobile phones submitted on consent had the shortest average turnaround time at 7.5 days. Of the 13 respondents that specified whether their agency routinely requests detailed information on the DE source submitted, 54% (n=7) routinely request everything available on the DE whereas 46% (n=6) routinely request detailed information related to the case (i.e., data only within a certain time frame) for investigative follow up.

DE Processing and Submission Policies. Eight respondents reported having internal policies and procedures in place to specifically address which types of DE are submitted for forensic analysis. When asked about potential barriers to submitting DE to the crime laboratory, half stated that the length of time it takes a laboratory to process DE was their biggest challenge (see **Figure 3-2**), followed by the lack of laboratory resources (42%). LE determined what type of DE is collected in 91% of the jurisdictions, followed by district attorneys (27%). Only 21% (n=3) of respondents stated that DE sources were previewed on scene by officers to determine evidentiary value when seizing DE.

Figure 3-2. Breakdown of Barriers to Submitting DE for Processing to the Crime Laboratory from the LE Perspective



Of the 14 agencies that indicated whether LE agencies request that the analyzing crime laboratory provide all the contraband material on the submitted DE sources or just enough to charge the suspect with the maximum penalty, 79% (n=11) stated that they request all

material whereas 21% (n=3) only request enough evidence to charge the suspect with the maximum charges.

DE Management and Retention. Seven respondents had a computerized evidence tracking system that was capable of tracking DE, while four respondents used a noncomputerized evidence tracking system (i.e., a paper sheet log). Of those that had computerized evidence tracking system, 43% (n=3) used their records management system.

Cross-agency Communication and Coordination. Only three respondents (21%) had a designated DE liaison in their agency who facilitates communication with the crime laboratory regarding their DE submissions status. The majority of respondents communicate with crime laboratory personnel sometimes (29%), often (14%) or always (36%) regarding the DE sources they submit and do so most often via email. Seven respondents had a computerized system that shared information regarding DE that can be accessed by both the LE agency and the crime laboratory that analyzes their DE.

3.2 Qualitative Interviews

Accreditation, Budget, & Training. All crime laboratory interviewees came from laboratories that were accredited for testing DE and stated how important accreditation was for their daily operations. One crime laboratory interviewee stated, "…if you're accredited, there's a constant there's a tech review process, it's a peer review process. There's a there's a top down, top management review process. I mean, we review everything so many different ways and […] so many different times. It keeps everybody as sharp as we can so they don't get complacent" (P2_CL). For one crime laboratory interviewee, accreditation was required by their state to provide testimony or submit evidence in trial.

The majority of interviewees, both from the crime laboratories and LE agencies, did not have a specific budget line for DE. The one interviewee who did have a specific budget line for processing and analyzing DE created that line in 2020. All interviewees were clear that their agency needed more funding for submitting DE (LE) and testing DE (crime laboratory). The key budgetary difference is that most software used in analyzing DE is subscription based and is a continuous expense for the agency, unlike other disciplines that also use expensive equipment but for whom it is a onetime purchase rather than a continuous expense. To address this gap in funding, one interviewee applied for funds through the Bureau of Justice Assistance Paul Coverdell Forensic Science Improvement Grants Program, which has afforded them the opportunity to pay for "new equipment and overtime and training" (P4_CL).

> "I mean, the biggest challenge I face, really, for digital, is that ongoing subscription fees, that's the biggest challenge we've got right now is going in and doing the tap dance every year before the commissioner and asking them[…] for that 90,000 bucks basically for two subscriptions and that just […] every year it's a hassle" – P2_CL

An important interview topic was the emphasis each interviewee's agency put on training specifically focused on the use of DE. All interviewees had either received training on DE analysis or investigations, but several interviewees stated that the level of training among analysts can vary based on their professional background and funds available at the agency level. Interviewees described a few of the training options that either they or someone in their agency had attended over the years to learn more about DE. There were a few free options, including courses from the National White Collar Crime Center and the United States Secret Service National computer Forensics Institute. These resources are important because the training for DE and computer forensics overall are very expensive compared with the trainings for other forensic disciplines. One interviewee stated that analysts in their agency had to pay for their own training, which is a barrier since DE certifications are expensive, whereas other crime laboratory and LE interviewees had an agency training budget that they could access.

Additionally, one interviewee described the evolving nature of the digital medium as the catalyst for ensuring analysts receive continuous training: "…the digital technology is evolving more quickly than anything else. So, the continuing education that's needed is it's extremely important because of the ever-evolving field" (P1_CL). One LE interviewee explained that their officers receive training directly from technology and software vendors, but they are often only able to send one person who comes back and disseminates the information to the rest of the agency. Otherwise, they rely on the skills people bring to the table from previous work or ask other peers and agencies when they have specific question about DE.

Importance of DE for Investigations. Both LE and crime laboratory interviewees recognized how crucial DE is to successful investigations and prosecutions in today's world. One crime laboratory interviewee stated, "I heard one of the sergeants talking to one of our supervisors and he told her that […] cell phones are more important to them for their murder cases than DNA now" (P5_CL). Interviewees from both agency types believed that mobile devices were the most analyzed type of DE in their agencies and the most effective type of DE used at trial. This was attributed to our society being "addicted" to their phones and people always having them on their person so the breadth of information they capture includes everything of importance to a case, including social interactions, location, internet searches, and communications.

Another DE type that was frequently mentioned as being critical to cases was GPS and information systems in cars that track everywhere an individual is going and smart watches, as even if an individual leaves their phone somewhere while committing a crime because they are aware of all the information it holds, they often forget about their car and smart watches capturing the same data. From an LE interview, bodycam footage was another important type of DE because it is "…showing […] what's going on in the moment. It's given a bigger picture. Obviously, seeing things and hearing things is a lot different than having to

describe to you" (P2_LE). Other types of DE that interviewees stated were important to investigations and prosecutions included computer's central processing units, tablets, and CCTV footage.

DE Triaging, Policies, & Procedures. The majority of interviewees from the crime laboratory received requests for analyzing DE at least every day and felt like nearly every case they received included some type of DE. There was variation among the interviewees about the average turnaround time for testing DE, but they were all in agreement that turnaround time depended on the type of DE that was submitted. Staffing was a major factor in turnaround time. For mobile devices specifically, the strength of their passcodes and the ability of the software agencies have available to them to crack those passcodes and get into the device was another major factor that impacted turnaround time. One LE interviewee felt like they could do more leg work to determine the time frames or exact information they needed from a device before sending it to the laboratory for them to analyze as a potential way to shorten the turnaround time.

Both crime laboratory and LE representatives discussed their use of a policy or an "unwritten rule" for triaging evidence (P1_LE), which was based on the severity of the crime with evidence from a violent crime or crime against a person taking priority over a non-violent crime or crime against property. The crime laboratory interviewees noted that it was standard practice to provide all the data available from a device or everything from the search warrant's designated timeframe back to the requesting agency rather than only things relevant to the case because they are not allowed to interpret the data or know anything outside of the search warrant regarding the case to prevent tampering.

The implementation of a retention policy for DE was commonplace in all but one interviewee's agency. This agency's policy states that they send everything, including the device, back to the requesting agency. Agency's that had retention policies included timeframes that ranged from 10 years to indefinitely. Methods of retention ranged from paper copies to physical USB back-ups to cloud storage depending on the agency's storage methods. Most interviewees did have a backlog of DE which they attributed mainly to staffing shortages and a lack of general resources.

> "For the longest time since last year, I think we had like zero cases in the backlog…And after, I think maybe in June of 2022 is when the Apple iPhone started coming out with stronger password protection. So because it was taking longer, the initial access to those phones were taking longer. So, […] that would be the bottleneck." – P5_CL

A fundamental element of a successful investigation involving DE is a clear and open communication channel between LE and the crime laboratory that analyzes their DE. The dominant form of communication between the two agencies was email. Two crime laboratory interviewees use their laboratory information system (LIMS) to generate emails that they send to their LE partners regarding their case.

Only one LE interviewee had a designated staff member who was dedicated to preparing DE and communicating with the crime laboratory regarding DE. This agency found this position to be helpful because it has standardized DE submissions and promoted a positive working relationship between the LE agency and the crime laboratory. None of the crime laboratory interviewees had a similar liaison position in their agency but stated they did not think it would add or take away from their current processes.

> "Email is probably your best friend…because […] in a laboratory we typically work 8 to 5. That's not the case with so many agencies that are typically working rotating shifts. And so trying to be able to get in touch with officers emails tends to become the best way of communicating because you can send an email and then when the officer comes on shift, they can respond to your email. So it gives you that ability to communicate. A lot of times telephone calls can just be difficult because […] schedules just don't sync up in order to make the conversation happen."
> – P1_CL

4. Conclusions and Recommendations

4.1 Conclusions

DE has steeply risen as an aid to solving crimes and will continue to grow as the use of digital devices continues to increase and evolve. This formative study sought to better understand how the mounting growth of DE has caused crime laboratories and LE agencies to rethink the efficiencies surrounding how these items are submitted and processed and then used as part of the investigative process. Results from the surveys and qualitative component revealed the importance of having established protocols and policies in place to govern DE submission, intake, analysis, and triage in crime laboratories and LE agencies.

Interagency communication is also key to improving efficiencies in processing DE. Whether the primary mode of communication between crime laboratories and LE agencies is via email, LIMS, or a dedicated liaison, both entities noted the importance of having methods in place to support open communication. Accreditation among crime laboratories was deemed beneficial as a method of ensuring standard practices for processing DE.

Training and resource management were also revealed to be areas of priority in crime laboratories and LE agencies. As the prevalence of DE has heightened, so has the need for more training and funding to handle this type of forensic evidence. Few of the participating laboratories and LE agencies reported having a dedicated budget for DE, and all expressed the need for more funding for submitting (LE) and testing (crime laboratories) DE. The costs associated with equipment and software needed to process and analyze DE, including staffing resources, remain a barrier for most agencies and negatively impact turnaround times. In addition, lack of training resources needed to keep up with the ever-evolving DE needs were repeatedly noted as a barrier because of the associated expenses.

4.2 Recommendations

Based on the data collected through the surveys and qualitative interviews, there are several practical implications for both crime laboratories and LE agencies to consider regarding their DE practices. Because of the limited frame of both the survey and qualitative interviews, we refer to the promising practices that emerged through the findings as "considerations" rather than recommendations. **Tables 4-1** and **4-2** feature practices for LE agencies and crime laboratories to consider implementing to improve their agencies DE submission and analysis practices.

Table 4-1. Considerations for LE

"Things to Consider" Implementing as an LE Agency Submitting DE
Agency Demographics and Resources ▪ Prioritize training regarding DE and updates to the field for all investigative staff. ▪ Review the evidence testing budget to secure adequate funding for DE testing.
DE Policies ▪ Ensure that policies for triaging DE at the crime scene and submitting DE to a crime laboratory are clear for each crime type. ▪ Be precise in your investigative needs when submitting DE and supporting search warrants to a crime laboratory.
DE Management and Retention ▪ Streamline electronic management of DE as much as possible with your crime laboratory, either by integrating LIMS systems or sharing spreadsheets. ▪ Review retention policies for DE and ensure they are adequate for your agency's needs. ▪ Meet with local prosecutor's offices to review retention policies for DE to ensure the statutes align.
Cross-Agency Communication and Coordination ▪ Work with your crime laboratory to set up a time to tour their facility to understand their policies and procedures and develop a shared understanding of timelines and methods of receiving analyzed data. ▪ Explore the idea of setting up a monthly or quarterly meeting with the DE section of your partner crime laboratory and use that time to discuss the status of submitted cases and possible ways to triage DE and ensure mutual understanding of who is triaging DE from both agencies. ▪ Consider creating a Crime Laboratory Liaison position within your investigative unit to ensure all DE is submitted in a standard way and to promote a positive relationship and collaboration between the two entities.

Table 4-2. Considerations for Crime Laboratories

"Things to Consider" Implementing as a Crime Laboratory Processing DE
Agency Demographics and Resources ▪ Allocate budget for DE processing when possible to allow for more transparent tracking of resources that are dedicated to DE analysts, processing software, and other DE-related items related. ▪ Prioritize funding in the budget for DE-related training and certification for analysts. ▪ Become accredited specifically for DE for the opportunity to routinely keep certifications up to date allow analysts to testify in court in some states, and subsequently provide more stability overall. ▪ Staff a laboratory sector with analysts assigned to DE processing at a proportional rate to the demands of DE processing to promote the completion of testing in an efficient manner but also to reduce burnout and turnover. ▪ Prioritize purchasing passcode "unlocking" software (e.g., GrayKey, Cellebrite) when possible to reduce the cost associated with renewing an annual subscription. Consider exploring partnering with other crime laboratories in your region or state to share the subscription cost of some DE software that allow for multiple users.
DE Policies ▪ Establish a policy outlining DE processing procedures and restrictions for maintaining the integrity of the evidence to promote successful completion, as with any other evidence type. ▪ Develop a triage policy, noting at what step in the process triage (e.g., by type, priority), should take place to allow for more transparent, consistent, and efficient processing. ▪ Improve agency transparency and reduce unwanted communication barriers that may exist across agencies by instituting information sharing policies.
DE Management and Retention ▪ Record and track all DE submitted to laboratories to expand the ability to share information with relevant personnel, including external partnering agencies. ▪ Consider implementing an evidence retention policy specific to DE, when not specifically mandated by legislation. Even a policy outlining a storage procedure for maintaining case data may be helpful for future reference.
Cross-Agency Communication and Coordination ▪ Establish the presence of a dedicated point of contact for communicating between laboratories and their respective LE partners to save time and resources. In addition, this would invite a more standardized evidence submission procedure and routine communications with case/processing updates. ▪ Consider implementing an electronic system that promotes information sharing among laboratories and their respective LE agencies automatically.

Appendix A:
References

1. CTIA. (2018). *The state of wireless 2018*. https://www.ctia.org/news/the-state-of-wireless-2018

2. O'Dea, S. (2020). *Average mobile wireless data usage per user worldwide in 2018 and 2024 (in gigabytes per month), by region.* https://www.statista.com/statistics/489169/canada-unitedstates-average-data-usage-user-per-month/

3. National Institute of Justice. (2020). *Digital evidence: Policy and procedures manual.* https://www.ncjrs.gov/pdffiles1/nij/254661.pdf

4. National Institute of Justice. (2019). *Report to Congress: Needs assessment of forensic laboratories and medical examiner/coroner offices.* https://nij.ojp.gov/library/publications/report-congress-needs-assessment-forensic-laboratories-and-medical

5. Brooks, C., & DuRose, M. R. (2016). *Census of publicly funded forensic crime laboratories, 2014.* Bureau of Justice Statistics. https://bjs.ojp.gov/data-collection/census-publicly-funded-forensic-crime-laboratories#publications-0

Appendix B:
Crime Laboratories Survey

Reference Worksheet

Please print this document if you would like to use it as a worksheet to gather data requested in the survey. We ask that you enter this information into the web survey using the login credentials that were provided.

About the Survey

As part of the NIJ sponsored Evaluation of Digital Evidence Processing Efficiencies in Publicly Funded Crime Laboratories, RTI International is leading a survey of publicly funded laboratories to learn more about the practices regarding collecting and processing digital evidence (DE). DE, as defined by the NIJ, is *information stored or transmitted in binary form that may be relied on in court.*[1]

DE can be found on computer hard drives, mobile devices, and other electronics and can be utilized in court to prosecute all types of crime, not just electronic-based crimes. The information from this survey will help inform our understanding of DE caseload, resource needs, submission practices, and management and analysis processes within and across jurisdictions. The information will be used to develop an evidence-based brief for crime laboratories and law enforcement agencies that shows promising practices in analyzing DE for case investigations.

This survey should take approximately 15-20 minutes to complete and may require consulting with other individuals in your laboratory. Therefore, it is suggested that a laboratory coordinator or section lead complete the survey. Should you have any questions or concerns regarding the survey at any time, please reach out to the Help Desk at DEsurveyhelp@rti.org.

[1] National Institute of Justice – Digital Evidence and Forensics https://nij.ojp.gov/digital-evidence-and-forensics

Screening Question

Does your laboratory process digital evidence?

1. ___ Yes → **Continue to Page 2**
2. ___ No → Your laboratory is not eligible to participate in the survey. Please log into the web survey using the login credentials that were provided, answering "No" this question, to finalize the survey.

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

Please enter your position title: _____

Demographics/ General Questions:

1. What jurisdiction does your agency serve? (e.g., name of city/municipality, county, district/region, or state): _____

2. What is the approximate size (population) of the jurisdiction served?
   a. ___ Less than 50,000
   b. ___ 50,000-99,999
   c. ___ 100,000 to 149,999
   d. ___ 150,000 to 499,999
   e. ___ 500,000 or more

3. What is the annual budget of your laboratory?
   a. ___ Less than $1,000,000
   b. ___ $1,000,000 to $2,999,999
   c. ___ $3,000,000 to $4,999,999
   d. ___ $5,000,000 or more

4. Does your agency have a budget for processing digital evidence specifically?
   1. ___ YES
   2. ___ NO

   5. **[IF QUESTION 4 = YES]** What is that budget?
      a. ___ Less than $500,000
      b. ___ $500,000 to $999,999
      c. ___ $1,000,000 to $2,999,999
      d. ___ $3,000,000 or more

6. How many staff are employed by your laboratory?
   a. ___Less than 10
   b. ___10-24
   c. ___25-49
   d. ___50-99
   e. ___100 or more

7. Of the total number of staff employed by your laboratory (Question #6), how many individuals analyze digital evidence?
   a. ___Less than 5
   b. ___5-9
   c. ___10-14
   d. ___15 or more

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

8. How many forensic towers (workstations) does your laboratory have that aid in the processing of digital evidence?
   a. ___Less than 5
   b. ___5-9
   c. ___10-14
   d. ___15 or more

9. Is your agency accredited to process digital evidence?
   1. ___YES
      9a. **[IF QUESTION 9 = YES]**
      What organization is this accreditation from?
      1. ___NIST
      2. ___ANSI/ANAB
      3. ___A2LA
      4. ___Other – Specify: _____
   2. ___No

10. How many law enforcement agencies does your laboratory receive digital evidence from?

    _____ Law Enforcement Agencies (Minimum:0; Maximum:100)

    11. **[IF QUESTION 10 = 1 OR MORE]** Please list the names of those law enforcement agencies below:

Digital Evidence Characteristics:

12. What was the total number of requests for testing involving digital evidence submitted to your agency in 2020?

    _____ Requests (Minimum:0; Maximum:99,999)

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

13. What was the total number of cases involving digital evidence completed by your agency in 2020? _____ Cases (Minimum:0; Maximum:99,999)

14. What was the total number of cases with unassigned digital evidence pending analysis as of January 1, 2021? _____ Cases

15. During 2020, did your individual laboratory perform these forensic functions? Mark yes or no for each source of digital evidence.

Forensic Function	Yes	No
Computer Forensics		
Mobile Device Analysis		
Image Analysis		
Video Analysis		
Forensic Audio		
Other DE analysis – Specify: ⟶ _____		

16. During 2020, did your individual laboratory analyze these sources of digital evidence? Mark yes or no for each source of digital evidence. If yes, please provide the number of tests performed on each source of digital evidence.

Source of Digital Evidence	Yes	No	Provide the Number of Tests Performed
Traditional cellphone (not Smartphones)			
Smartphones			
Laptop, Tablet, and Desktop Computer			
Thumb and External Drive			
Wireless Routers and Network Devices			
GPS and Navigation Systems			
Audio Files			
CDs, DVDs, and other Storage Mediums			
Gaming Systems (Xbox, Playstation, etc.)			
Cloud and Server Data (including social media)			
Other – Specify: ⟶ _____			

Explain. If you had any difficulty providing values for the number of tests performed in question 16, please explain below: ⟶

_____

_____

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

Digital Evidence Processing and Submission Policies:

17. Does your agency have established protocols regarding the intake of digital evidence?
    1. ___YES
    2. ___NO

18. Does your agency have established protocols for testing digital evidence?
    1. ___YES
    2. ___ NO

19. Does your laboratory have a policy prioritizing digital evidence platforms (e.g., texts, email, GPS)?
    1. ___YES
    2. ___NO

20. Does your laboratory have a policy for triaging digital evidence?
    1. ___YES
    2. ___NO

Digital Evidence Management and Retention:

21. Does your laboratory have a computerized system capable of tracking digital evidence?
    1. ___YES → 20a. **[IF QUESTION 21 = YES]** Please select the name of the system.
       a. ___Bar Coded Evidence Analysis Statistics and Tracking (BEAST)
       b. ___Forensic Advantage
       c. ___Horizon
       d. ___In-house laboratory system
       e. ___Justice Trax
       f. ___Orchard Harvest
       g. ___VertiQ
       h. ___Other – Specify: _____
    2. ___NO → 20b. **[IF QUESTION 21 = NO]** Please specify process for documenting forensic evidence management below. →

       _____

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

22. Does your laboratory experience difficulty in storing digital evidence?
    1. ___YES
    2. ___NO

23. Has your laboratory implemented new policies/procedures to improve efficiency in digital evidence submission to crime laboratories within the past 5 years?
    1. ___YES
    2. ___NO

24. Does your laboratory have a retention policy in place for digital evidence?
    1. ___YES
    2. ___NO

    25. **[IF QUESTION 24 = YES]** How long is your laboratory required to retain digital evidence? _____ Months

Cross-agency Communication and Coordination:

26. Does your laboratory have a designated digital evidence liaison that facilitates communication with the law enforcement agency(ies) you serve to discuss the process and status of digital evidence submission and testing?
    1. ___YES
    2. ___NO

    27. **[IF QUESTION 26 = YES]** Please provide their contact information below:

        Name: _____

        Job title: _____

        Email: _____

        Phone number: (____)_____

28. How often does crime laboratory personnel analyzing digital evidence have any direct communication with the investigating officer who submitted the evidence for analysis?
    a. ___Never → **GO TO QUESTION 30**
    b. ___Rarely
    c. ___Sometimes
    d. ___Often
    e. ___Always

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

29. What is the method of the direct communication most of the time?
    a. ___By phone
    b. ___By email
    c. ___By mail
    d. ___By video conference
    e. ___Other - Please specify: _____

30. Do you have a computerized system that tracks evidence between your agency and the law enforcement agencies you serve?
    1. ___YES
    2. ___NO

31. How often does crime laboratory personnel testify in court regarding their analysis of digital evidence?
    a. ___Never
    b. ___Rarely
    c. ___Sometimes
    d. ___Often
    e. ___Always

Please return to the web survey using the login information provided to enter your responses. Thank you very much.

If you have any questions, please reach out to the Help Desk at DEsurveyhelp@rti.org

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

Appendix C:
Law Enforcement Agencies Survey

Reference Worksheet

Please print this document if you would like to use it as a worksheet to gather data requested in the survey. We ask that you enter this information into the web survey using the login credentials that were provided.

About the Survey

As part of the National Institute of Justice (NIJ) sponsored Evaluation of Digital Evidence Processing Efficiencies in Publicly Funded Crime Laboratories, RTI International is leading a survey of publicly funded crime laboratories and the law enforcement agencies that submit digital evidence (DE) to them to learn more about the practices regarding collecting and processing DE.

DE, as defined by the NIJ, is *information stored or transmitted in binary form that may be relied on in court*.[1] DE can be found on computer hard drives, mobile devices, and other electronics and can be utilized in court to prosecute all types of crime, not just electronic-based crimes.

The information from this survey will help inform our understanding of DE caseload, resource needs, submission practices, and management and analysis processes within and across jurisdictions. The information will be used to develop an evidence-based brief for crime laboratories and law enforcement agencies that shows promising practices in analyzing DE for case investigations.

This survey should take approximately 20-30 minutes to complete and may require consulting with other individuals in your agency. Therefore, it is suggested that a law enforcement investigation supervisor who has responsibility over member(s) of that agency that submit DE for analysis to a crime laboratory complete the survey. Should you have any questions or concerns regarding the survey at any time, please reach out to the Help Desk at DEsurveyhelp@rti.org.

[1] National Institute of Justice – Digital Evidence and Forensics https://nij.ojp.gov/digital-evidence-and-forensics

Screening Question

Does your laboratory process digital evidence?

1. ___ Yes → **Continue to Page 2**
2. ___ No → Your laboratory is not eligible to participate in the survey. Please log into the web survey using the login credentials that were provided, answering "No" this question, to finalize the survey.

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

Please enter your position title: _____

Demographics/ General Questions:

1. What jurisdiction does your agency serve? (e.g., name of city/municipality, county, district/region, or state): _____

2. What is the approximate size (population) of the jurisdiction served?
   a. ___ Less than 50,000
   b. ___ 50,000-99,999
   c. ___ 100,000 to 149,999
   d. ___ 150,000 to 499,999
   e. ___ 500,000 or more

3. How many crime laboratories (state or local) does your agency submit digital evidence to?
   _____ Laboratories

   ↓

   4. Please list the names of those laboratories here:
      _____

5. Does your agency have the capacity to analyze digital evidence internally?
   1. ___YES
   2. ___NO

   ↓

   6. **[IF QUESTION 5 = YES]** How many staff are trained to analyze digital evidence in your agency?
      _____ Staff (Minimum:0; Maximum:20)

   7. **[IF QUESTION 5 = YES]** Does your agency have a budget for processing digital evidence specifically?
      1. ___ YES
      2. ___ NO

      ↓

      8. **[IF QUESTION 7 = YES]** What is that budget?
         a. ___ Less than $500,000
         b. ___ $500,000 to $999,999
         c. ___ $1,000,000 to $2,999,999
         d. ___ $3,000,000 or more

9. Have any officers in your agency received training regarding the seizure of digital evidence?
   1. ___YES
   2. ___NO

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

10. Have any officers in your agency received training regarding the processing or analyzing of digital evidence?
    1. ___YES
    2. ___NO

    11. **[IF QUESTION 10 = YES]** Is this training updated on a regular basis or a one-time training?
        1. ___ Regular basis
        2. ___ One-time training

Digital Evidence Characteristics:

12. What was the total number of cases involving digital evidence submitted by your agency to a public crime laboratory or digital forensics unit for testing in 2020?
    _____ Cases (Minimum:0; Maximum:99,999)

13. What was the total number of items involving digital evidence submitted by your agency to a public crime laboratory or a digital forensics unit for testing in 2020?
    _____ Items (Minimum:0; Maximum:99,999)

14. What was the total number of cases involving digital evidence submitted by your agency to a crime laboratory for testing in 2020 that your agency had not received results on as of January 1, 2021?
    _____ Cases (Minimum:0; Maximum:99,999)

15. During 2020, did your law enforcement agency submit any of these sources of digital evidence to a crime laboratory for analysis? Mark yes or no for each source of digital evidence. If yes, please provide the number of cases submitted for each source of digital evidence.

Source of Digital Evidence	Yes	No	Number of Cases Submitted
Phones			
Laptop, Tablet, and Desktop Computer			
Thumb and External Drive			
Wireless Routers and Network Devices			
GPS and Navigation Systems			
Audio Files			
CDs, DVDs, and other Storage Mediums			
Gaming Systems (Xbox, Playstation, etc.)			
Cloud and Server Data (including social media)			
Other – Specify: _____			

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

Explain. If you had any difficulty providing values for the number of tests performed in question 15, please explain below: ⟶

16. During 2020, did your law enforcement agency analyze any of these sources of digital evidence internally? Mark yes or no for each source of digital evidence. If yes, please provide the number of cases submitted for each source of digital evidence.

Source of Digital Evidence	Yes	No	Number of Cases Submitted
Phones			
Laptop, Tablet, and Desktop Computer			
Thumb and External Drive			
Wireless Routers and Network Devices			
GPS and Navigation Systems			
Audio Files			
CDs, DVDs, and other Storage Mediums			
Gaming Systems (Xbox, Playstation, etc.)			
Cloud and Server Data (including social media)			
Other – Specify: ⟶ _____			

Explain. If you had any difficulty providing values for the number of tests performed in question 16, please explain below: ⟶

17. What is the average turnaround time (TaT) in days for the following types of digital evidence?

Source of Digital Evidence	Average TaT
Mobile Phones submitted on consent	
Mobile Phones submitted on warrant	
Computers/removeable media submitted on consent	
Computers/removeable media submitted on warrant	
Forensic Video Analysis	
Forensic Audio Analysis	

18. Do you routinely request detailed information related to your case (i.e., data only during a specific time range) or for everything available on the piece of digital evidence for investigative follow up?
    1. ___YES
    2. ___NO

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

19. Please indicate (A) if your agency follows any of the following polices and (B) whether the policy is formal or informal and (C) the year the policy was implemented.

Policy	Yes	No	Formal	Informal	Year Implemented
A 100% submission policy for all DE collected					
Criteria for submitting DE to the crime laboratory					
Mandatory criteria to record decisions justifying why DE was not submitted to crime laboratory					
A policy to prioritize the submission of evidence based upon the type of case					
A policy to prioritize the submission of DE based upon the amount of time elapsed (e.g., new cases vs. cold cases)					
A policy to prioritize the submission of DE based on the type of data extracted (e.g., texts, emails, GPS)					
An evidence retention policy regarding preservation of DE that was secured in the investigation of an offense if the defendant is found guilty					
An evidence retention policy regarding preservation of DE that was secured in the investigation of an offense if the defendant is found NOT guilty					
A policy that requires approval of the prosecuting attorney or district attorney before submitting DE to the forensic laboratory					
A policy to destroy DE after a given period of time (e.g., 10 years)					
Other – Specify: ⟶ _____					

20. Which of the following are barriers to submitting digital evidence to the crime laboratory for your agency? Select all that apply.
    1. ___ Lack of laboratory resources
    2. ___ Lack of training
    3. ___ Unsure of submission policies
    4. ___ Length of time for processing
    5. ___ Other – Specify: _____

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

21. Who or what determines what DE is collected in your jurisdiction? Select all that apply.
    1. ___ Testing Capacity of Crime Laboratory
    2. ___ Law Enforcement
    3. ___ District Attorney
    4. ___ Jurisdictional mandate/law
    5. ___ Other – Specify: _____

22. When seizing digital evidence, are devices previewed on scene by officers to determine evidentiary value?
    1. ___YES
    2. ___NO

23. When requesting digital evidence to be analyzed, do you request that the analyzing laboratory provide all contraband material or just enough to charge suspect with the maximum penalty?
    1. ___ All contraband material
    2. ___ Enough contraband material to charge suspect with maximum penalty

Digital Evidence Management and Retention:

24. Does your laboratory have a computerized system capable of tracking digital evidence?
    1. ___YES →
    2. ___NO

25. **[IF QUESTION 24 = YES]** Please select the name of the system.
    a. ___Bar Coded Evidence Analysis Statistics and Tracking (BEAST)
    b. ___Forensic Advantage
    c. ___Horizon
    d. ___In-house laboratory system
    e. ___Justice Trax
    f. ___Orchard Harvest
    g. ___VertiQ
    h. ___Other – Specify: _____

26. **[IF QUESTION 24 = NO]** Please specify process for forensic evidence management. →

_____

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

Cross-agency Communication and Coordination:

27. Does your agency have a designated digital evidence liaison that facilitates communication with the crime laboratory regarding the process and status of digital evidence submission and testing?
    1. ___YES
    2. ___NO

28. **[IF QUESTION 27 = YES]** Please provide their contact information below:

    Name: _____

    Job title: _____

    Email: _____

    Phone number: (____)_____

29. How often does crime laboratory personnel analyzing digital evidence have any direct communication with the investigating officer who submitted the evidence for analysis?
    a. ___Never → **GO TO QUESTION 31**
    b. ___Rarely
    c. ___Sometimes
    d. ___Often
    e. ___Always

30. What is the method of the direct communication most of the time?
    a. ___By phone
    b. ___By email
    c. ___By mail
    d. ___By video conference
    e. ___In person
    f. ___Other - Please specify: _____

31. Do you have a computerized system for sharing information regarding digital evidence that can be accessed by both agencies between your agency and the crime laboratory in your jurisdiction?
    1. ___YES
    2. ___NO

Please return to the web survey using the login information provided to enter your responses. Thank you very much.

If you have any questions, please reach out to the Help Desk at DEsurveyhelp@rti.org

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

Appendix D:
Critical Items for Law Enforcement Survey

Reference Worksheet

Please print this document if you would like to use it as a worksheet to gather data requested in the survey. We ask that you enter this information into the web survey using the login credentials that were provided.

About the Survey

As part of the National Institute of Justice (NIJ) sponsored Evaluation of Digital Evidence Processing Efficiencies in Publicly Funded Crime Laboratories, RTI International is leading a survey of publicly funded crime laboratories and the law enforcement agencies that submit digital evidence (DE) to them to learn more about the practices regarding collecting and processing DE[1].

Based on feedback from respondents, we have shortened the survey considerably to reduce the burden of the survey on respondents and make it easier for respondents to complete. The information from this survey will help inform our understanding of DE caseload, resource needs, submission practices, and management and analysis processes within and across jurisdictions. The information will be used to develop an evidence-based brief for crime laboratories and law enforcement agencies that shows promising practices in analyzing DE for case investigations.

This survey should take approximately 10 minutes to complete and may require consulting with other individuals in your agency. Therefore, it is suggested that a law enforcement investigation supervisor who has responsibility over member(s) of that agency that submit DE for analysis to a crime laboratory complete the survey.

If you have any questions or concerns regarding the survey at any time, please reach out to the Help Desk at DEsurveyhelp@rti.org.

Thank you for your assistance in this important endeavor.

1. DE, as defined by the NIJ, is *information stored or transmitted in binary form that may be relied on in court.*[1] DE can be found on computer hard drives, mobile devices, and other electronics and can be utilized in court to prosecute all types of crime, not just electronic-based crimes. National Institute of Justice – Digital Evidence and Forensics: https://nij.ojp.gov/digital-evidence-and-forensics

Screening Question
Does your agency collect and utilize digital evidence for investigative purposes?

1. ___YES → **Continue to Page 2**
2. ___NO → Your agency is not eligible to participate in the survey. Please log into the web survey using the login credentials that were provided, answering "No" this question, to finalize the survey.

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

Please enter your position title:

Demographics/ General Questions:

1. What jurisdiction does your agency serve? (e.g., name of city/municipality, county, district/region, or state):_____

2. How many crime laboratories (state or local) does your agency submit digital evidence to?
   _____ Laboratories
   (Minimum:0; Maximum:20)

3. Does your agency have the capacity to analyze digital evidence internally?
   a. ___Yes
   b. ___No

   3a. [IF 3=YES] How many staff are trained to analyze digital evidence in your agency?

   _____ Staff
   (Minimum:0; Maximum:20)

4. Have any officers in your agency received training regarding the seizure and processing of digital evidence?
   a. ___Yes
   b. ___No

   4a. [IF 4=1] Is this training updated on a regular basis or a one-time training?
   1. ___ Regular Basis
   2. ___ One-time Training

Digital Evidence Characteristics:

5. What was the total number of cases involving digital evidence submitted by your agency to a public crime laboratory or digital forensics unit for testing in 2020?
   _____ Cases

   (Minimum:0; Maximum:99,999)

6. What was the total number of items involving digital evidence submitted by your agency to a public crime laboratory or a digital forensics unit for testing in 2020?
   _____ Items

   (Minimum:0; Maximum:99,999)

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

7. What was the total number of cases involving digital evidence submitted by your agency to a crime laboratory for testing in 2020 that your agency had not received results on as of January 1, 2021?
   _____ Cases
   (Minimum:0; Maximum:99,999)

8. During 2020, did your law enforcement agency submit any of these sources of digital evidence to a crime laboratory for analysis? Mark yes or no for each source of digital evidence.

Source of Digital Evidence	1 Yes	2 No
Phones		
Laptop, Tablet, and Desktop Computer		
Thumb and External Drive		
Wireless Routers and Network Devices		
GPS and Navigation Systems		
Audio Files		
CDs, DVDs, and other Storage Mediums		
Gaming Systems (Xbox, Playstation, etc.)		
Cloud and Server Data (including social media)		
Other (Please specify):		

8a. [IF 3=YES] During 2020, did your law enforcement agency analyze any of these sources of digital evidence internally? Mark yes or no for each source of digital evidence.

Source of Digital Evidence	1 Yes	2 No
Phones		
Laptop, Tablet, and Desktop Computer		
Thumb and External Drive		
Wireless Routers and Network Devices		
GPS and Navigation Systems		
Audio Files		

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

CDs, DVDs, and other Storage Mediums		
Gaming Systems (Xbox, Playstation, etc.)		
Cloud and Server Data (including social media)		
Other (Please specify):		

Digital Evidence Processing and Submission Policies:

9. Does your agency have internal policies and procedures in place that specifically address which types of digital evidence are submitted for forensic analysis?
    a. ___Yes
    b. ___No

10. Which of the following are barriers to submitting digital evidence to the crime laboratory for your agency? Select all that apply.
    a. ___ Lack of laboratory resources
    b. ___ Lack of training
    c. ___Unsure of submission policies
    d. ___ Length of time for processing
    e. ___ Other (Please specify: _____)

11. When seizing digital evidence, are devices previewed on scene by officers to determine evidentiary value?
    a. ___Yes
    b. ___No

12. When requesting digital evidence to be analyzed, do you request that the analyzing laboratory provide all contraband material or just enough to charge suspect with the maximum penalty?
    a. ___ All contraband material
    b. ___ Enough contraband material to charge suspect with maximum penalty

Cross-agency Communication and Coordination:

13. Does your agency have a designated digital evidence liaison that facilitates communication with the crime laboratory regarding the process and status of digital evidence submission and testing?
    a. ___Yes
    b. ___No (GO TO END)

14. [IF YES] Please provide their contact information below:
    o Name:_____
    o Job title:_____

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

o Email:_____
o Phone number:_____

15. How often does your investigating officer have any direct involvement with crime laboratory personnel who analyze the digital evidence?
    a. ___ Never (GO TO END)
    b. ___ Rarely
    c. ___Sometimes
    d. ___ Often
    e. ___ Always
16. Do you have a computerized system for sharing information regarding digital evidence that can be accessed by both agencies between your agency and the crime laboratory in your jurisdiction?
    a. ___Yes
    b. ___No

Please return to the web survey using the login information provided to enter your responses. Thank you very much.

If you have any questions, please reach out to the Help Desk at DEsurveyhelp@rti.org

This survey was developed under funding from the National Institute of Justice Grant Number 2020-DQ-BX-0016.

Appendix E:
Law Enforcement Qualitative Interview Guide

Law Enforcement Qualitative Interview Guide

Evaluation of Digital Evidence Processing Efficiencies in Publicly Funded Crime Laboratories

Resources:

1. How often do your investigators utilize digital evidence in their cases?
2. What kinds of digital evidence have you found most helpful in investigating cases and why?
3. How effective do you think digital evidence is in modern-day investigations?
4. What kinds of digital evidence have you found most helpful in prosecuting cases in court and why?
5. Does your agency have a budget specifically for submitting digital evidence?
6. Is it sufficient for your investigatory needs?
7. Have you received training on how to utilize digital evidence to improve outcomes for the cases you investigate?
    a. If so, where did you receive that training?
    b. How was that training funded?
    c. How many people in your agency received this training?
8. What resources (e.g., funding or training) do you think would be helpful in increasing your ability to utilize digital evidence?

Interagency Communication:

1. Can you tell us about what the relationship between your agency and the crime laboratory that processes the digital evidence you collect is like?
2. Do you have a designated point of contact in your agency that communicates with the crime laboratory regarding digital evidence?
    a. If so, how was that position created?
    b. If not, do you think a position like this could be helpful?
3. How has your relationship and communication with the crime laboratory evolved over time?
4. Do you think improvements could be made in terms of your relationship and communication?
    a. If they don't have a positive relationship, do you think there are ways to improve your relationship and increase communication with your crime laboratory regarding digital evidence (e.g., weekly conference calls or meetings)?
    b. If they do have a positive relationship, what advice would you give to a jurisdiction that is looking to improve their relationship with the crime laboratory and increase communication between the agencies regarding digital evidence?

Evidence Management and Retention Policies:

1. Who or what determines what digital evidence is collected in your jurisdiction (i.e., LE

leadership, crime laboratory, district attorney, jurisdictional mandate/law)?

2. Does your agency have any policies in place regarding the submission of DE to a crime laboratory? Are they informal or formal? When were these policies implemented?
3. How long does it normally take for you to receive results from the crime laboratory regarding digital evidence after you submit it?
    a. Does it depend on the type of digital evidence you submit?
    b. Do you think there is anything that could be done to improve the process?
4. How do you receive notification about the status of your digital evidence?
5. Does the laboratory have a way of prioritizing what data they process first?
    a. If so, what is that priority and is there anything you would like to see changed regarding what data is prioritized?
6. How does your agency track digital evidence?
    a. How has that evolved over time?
    b. Is there anything you would like to improve about the way your agency tracks digital evidence?
7. Does your agency have a retention policy for digital evidence?
    a. Does it depend on the type of evidence or the type of case?
    b. Has that evolved over time?
8. Does your agency have a backlog of digital evidence?
    a. If so, what are the main reasons for that backlog?
9. What efforts has your agency taken to eliminate or mitigate the backlog of digital evidence?
10. What resources would you need to submit all of the digital evidence to a crime laboratory?

Appendix F:
Crime Laboratories Qualitative Interview Guide

Crime Laboratory Qualitative Interview Guide for Crime Laboratories

Resources:

1. In the initial survey, your laboratory indicated that the facility [Is/Is Not] accredited for processing DE.
    a. Is your laboratory accredited in other areas?
    b. If not accredited for DE, do you feel this restricts the ability to move evidence forward?
2. How often does your laboratory receive requests for testing digital evidence?
    a. About what percentage of cases includes some type of DE?
    b. What kinds of digital evidence have you found most helpful to investigators and why?
3. How effective do you think digital evidence is in modern-day investigations?
    a. What kinds of digital evidence have you found most helpful in prosecuting cases in court and why?
4. Does your agency have a budget specifically for analyzing digital evidence?
    a. Is it sufficient for your testing needs?
5. Have you received training on how to test digital evidence to improve outcomes for the cases you analyze?
    a. If so, where did you receive that training?
    b. How was that training funded?
    c. How many people in your laboratory received this training?
6. Are tools/equipment/software (used for DE processing) standardized in any way?
    a. Do you feel this may limit the viability of this evidence in an investigation/court?
7. Do gaps exist across staff regarding skills and certifications?
    a. Are all staff required to take specific training or maintain specific certification?
8. What resources (e.g., funding or training) do you think would be helpful in increasing your ability to utilize and analyze digital evidence?

Interagency Communication:

1. Can you tell us about the relationship between your laboratory and the law enforcement agencies you serve?
    a. Do you think there can be any improvements and why?
2. Do you have a designated point of contact in your laboratory that communicates with the law enforcement agencies regarding digital evidence?
    a. If so, how was that position created and are they a laboratory or LE employee?

    b. If not, do you think a position like this could be helpful?
3. If they don't have a positive relationship, do you think there are ways to improve your relationship and increase communication with those agencies regarding digital evidence (e.g., weekly conference calls or meetings)?
4. If they do have a positive relationship, what advice would you give to a laboratory that is looking to improve their relationship with law enforcement and increase communication between the agencies regarding digital evidence?

Evidence Management and Retention Policies:

1. How long does it normally take for you to send results from the crime laboratory to the requesting agency regarding digital evidence after they submit it?
    a. Does it depend on the type of digital evidence submitted?
    b. Do you think there is anything that could be done to improve the process?
    c. How do you send notifications about the status of digital evidence?
2. Your initial survey indicated that you [Do/Do Not] have a policy for triaging DE. What does "triage" mean to you?
    a. Probing question: Is triage done in the field? In the laboratory?
    b. Probing question: Is triage completed based upon evidence type? Most probative? Type of crime?
3. Does your laboratory have a retention policy for digital evidence?
    a. Is it a shared policy between your laboratory and LEA?
    b. Does it depend on the type of evidence or the type of case?
    c. Has that evolved over time?
4. What does your laboratory do with processed data? How is it stored?
    a. Are credentials needed for testimony (e.g., cloud storage credentials)?
5. Does your laboratory have a backlog of digital evidence?
    a. If so, what are the main reasons for that backlog?
    b. What efforts has your laboratory taken to eliminate or mitigate the backlog of digital evidence?
    c. What resources would you need to analyze all of the digital evidence at the crime laboratory?
6. What resources (e.g., funding or training) do you think would be helpful in increasing your ability to utilize and analyze digital evidence?
7. Is there anything you'd like to see change regarding your laboratory/agency's policies and protocols associated with DE processing?

Is there anything that we haven't covered during our time today regarding digital evidence processing that you think would be important for us to know?

Appendix G:
Research Brief for Crime Laboratories and Law Enforcement Agencies

Evaluation of Digital Evidence Processing Efficiencies in Publicly Funded Crime Laboratories

RTI INTERNATIONAL

November 2023

The New DNA: Recommendations for Agencies to Consider Implementing to Improve Digital Evidence Processing and Analysis

Prepared by | Peyton Attaway, Chris Williams, Crystal Daye, Nichole Bynum, Liat Weinstein, and Ruby Johnson

Highlights

- On average, crime laboratories not accredited specifically for digital evidence (DE) processing received 2.5 times the amount of testing requests that the DE-accredited crime laboratories did, which indicates a discrepancy in the field for DE accreditation.
- Nearly half of responding laboratories reported not having a policy for triaging DE, but received, on average, 653 total requests for DE processing in 2020.
- A total of 19 laboratories reported frequent communication ("often" or "always") with investigating law enforcement officers without a designated liaison for communication, while 9 laboratories reported a designated liaison.
- Approximately 91% of law enforcement respondents stated that their agencies were responsible for determining what DE is collected on scene, but only 18% claimed to have a "submit all" policy for DE, which suggests that triaging is completed in the field, but also following collection for most agencies.
- All responding agencies indicated that officers have received training regarding the seizure of DE, and 93% have received training regarding the processing or analyzing of DE.
- Approximately 87% of agencies reported that their law enforcement agency has the ability and capacity to analyze DE internally.
- Approximately 64% of respondents indicated that their agency has a computerized evidence tracking system capable of tracking DE.

This project was supported by Grant No. 2020-DQ-BX-0016 from the National Institute of Justice. The opinions, findings, and conclusions or recommendations expressed in this document are those of the researchers and do not necessarily reflect those of the U.S. Department of Justice.

Introduction

With the widespread use of smartphones and other mobile devices among the general population, it is increasingly necessary for law enforcement and crime laboratory personnel to develop methods to more efficiently process and analyze DE. In response to the growth of DE in criminal investigations, the National Institute of Justice (NIJ) published the *Digital Evidence Policies and Procedures Manual* in May 2020 to guide law enforcement agencies in creating protocols for handling and processing DE in their agencies. Despite the manual and other federal programs aimed at improving the processing and collection of DE, backlogs, understaffing, and the large volume of DE make it difficult for many agencies to effectively collect DE (Novak, 2021). This brief contains important DE findings and implications for both law enforcement and crime laboratories that resulted from an exploratory study conducted by RTI International. It also summarizes key considerations for law enforcement for storing DE and submitting it for analysis and for crime laboratories when processing DE.

Methods

Surveys were administered between February 2022 and March 2023 and generally inquired about DE data and information from the 2020 calendar year. A purposive subset of DE crime laboratories and their law enforcement partner agencies were then selected for in-depth qualitative interviews.

Digital Evidence Laboratory Survey

The 2014 data from the Bureau of Justice Statistics' Census for Publicly Funded Forensic Crime Laboratories (2014) was used to inform the DE laboratory frame for this study (Brooks, 2014) since it was the most recent publicly available data but also because that administration included a special DE supplement (Brooks, 2014). RTI sent online surveys to 80 local and state-based laboratories with computer/cybercrime/DE sections or departments. Critical components of the survey included demographics and laboratory budget, DE characteristics, processing and submission policies, management and retention, and cross-agency communication with respective submitting agencies. The DE laboratory survey took about 15–20 minutes to complete, and the survey was in the field from January 2022 to June 2022. A total of 32 laboratories completed the DE survey, representing a 40% response rate.

Law Enforcement Survey

The law enforcement survey consisted of questions regarding identical topics to those of the crime laboratory survey but tailored to law enforcement agencies, including demographics

and budget, agency characteristics (e.g., number of DE items and cases, types of DE submitted), agency processing and submission policies, management and retention, and cross-agency communication with respective submitting agencies. The digital laboratories that participated in the laboratory survey were asked the following question: "How many law enforcement agencies does your laboratory receive DE from? Please list the names of those law enforcement agencies below." A total of 71 law enforcement agencies were identified based on the crime laboratories responses, and all agencies were sent the **law enforcement** survey. The law enforcement surveys were administered between October 2022 and March 2023. **Nearly 23% (n=16) of law enforcement agencies completed the survey in full, while an additional 11% (n=8) provided data, equating to a total response rate of approximately 34%.**

Qualitative Interviews

The goal of the interviews was to pair law enforcement agencies with a crime laboratory to which they submit DE in order to gain a deeper understanding of the relationship between the two entities. The 10 individuals who participated in the qualitative interviews represented law enforcement investigators (3) and crime laboratory personnel (7) with varying degrees of experience with DE. All interviewees except for one participated in the survey. Interviews were conducted via Zoom between May and August 2023. Informed consent was obtained before interviews were conducted, and all interviews were recorded following the consent of all participants. The recordings were transcribed into electronic files that the site visit team members reviewed before they were finalized.

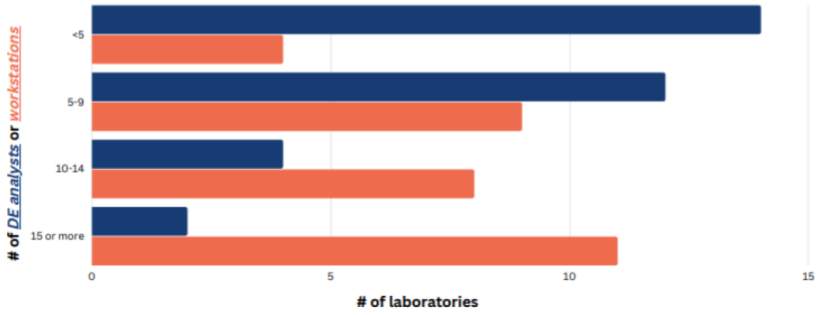
The interviews followed a semi-structured qualitative study instrument, which allowed interviewers to ensure they covered all the main topics while also allowing for new ideas and topics to emerge during conversation. The qualitative study instruments were developed by the study team to capture information related to agency resources, interagency communication, and evidence management and retention policies. Each interview was recorded, transcribed, and later coded in NVivo 12.0.

Findings and Implications Survey

Nearly half of DE laboratories (44%; 14 laboratories) did not have a policy for triaging DE, and about two-thirds did not have a policy on DE retention. However, nearly 91% of responding agencies indicated they have a policy in place for the processing of DE. Specific focus was placed on policy presence in the survey to understand what practices were in place as the demand for DE processing grows at an exponential rate. On average, crime laboratories not accredited specifically for DE processing received 2.5 times the amount of testing requests that the DE-accredited crime laboratories did, indicating a discrepancy in the field for DE accreditation. The distribution of DE analysts vs. forensic workstations in the laboratory setting was notable in that many laboratories have fewer than 5 DE analysts but more than 15 forensic workstations (Figure 1). This could be attributed to a lack of staff or

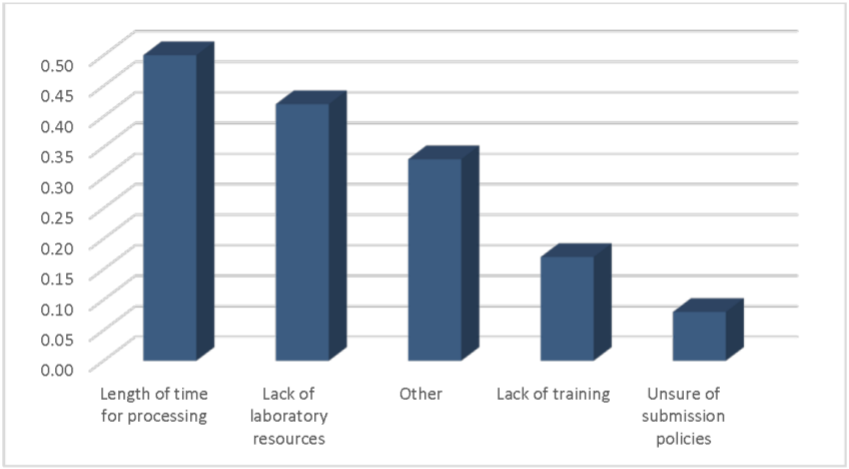
simply funding allocated specifically for DE processing. The two evidence types processed by laboratories that made up the overwhelmingly majority were mobile devices and computers, with these devices representing approximately 77% of total DE processing requests on average. With regard to cross-agency communication, 19 laboratories reported frequent communication ("often" or "always") with investigating law enforcement officers but not having a designated liaison for communication, while 9 laboratories reported having a designated liaison.

Figure 1. Distribution of DE Analysts vs. Forensic Workstations (n=32)



This bar graph highlights the distribution of analysts specifically assigned to process DE related to the number of forensic workstations available in various laboratories.

Figure 2. Barriers to Submitting Digital Evidence to the Crime Laboratory for LEA



This bar graph highlights the breakdown of barriers from the law enforcement perspective to submitting digital evidence for processing to the crime laboratory.

Approximately 91% of law enforcement respondents stated that their agency was responsible for determining what DE is collected on scene, but only 18% claimed to have a "submit all" policy for DE, suggesting that triaging is completed in the field, but also following collection for most agencies. All responding agencies indicated that officers have received training regarding the seizure of DE, and 93% have received training regarding the processing or analyzing of DE. Approximately 87% of law enforcement agencies reported having the ability and capacity to analyze DE internally. When asked about potential barriers to submitting DE to the crime laboratory, half of respondents indicated that the length of time it takes a laboratory to process DE was their biggest barrier (see Figure 2), followed by the lack of laboratory resources. Approximately 64% of respondents indicated that their agency has a computerized evidence tracking system capable of tracking DE.

Qualitative Interviews

Accreditation, Budget, and Training. All crime laboratory interviewees came from laboratories accredited for analyzing DE and recognized its importance. One interviewee had a specific budget for processing DE, which was created in 2020, while the other nine interviewees noted their agency had one budget for all disciplines or investigations. All the interviewees noted that a key budgetary difference between DE and other forensic disciplines is that unlike other disciplines that require expensive equipment that is a onetime purchase, most of the software used in DE analysis is subscription based and represents a continuous expensive cost for the agency. All interviewees stated that either they or DE analysts in their agency have received training on DE analysis or investigations; however, several interviewees stated that the level of training among analysts can vary based on their background and funds available.

> "I mean, the biggest challenge I face, really, for digital, is that ongoing subscription fees, that's the biggest challenge we've got right now is going in and doing the tap dance every year before the commissioner and asking them for that 90,000 bucks basically for two subscriptions and that just every year it's a hassle.
>
> *Crime laboratory participant*

Importance of DE for Investigations. Both **law enforcement** and crime laboratory interviewees recognized how critical DE is to modern-day investigations and prosecutions. Mobile devices were the most widely analyzed type of DE among interviewees and the most effective type of DE used at trial. According to one of the crime laboratory interviewees, "I heard one of the sergeants talking to one of our supervisors, and he told her that cell phones are more important to them for their murder cases than DNA now" (Crime laboratory participant).

DE Triaging, Policies, and Procedures. Most crime laboratory interviewees stated that they receive requests for analyzing DE every day, while one stated they receive requests for analyzing DE at least three times a week. There was a lot of variety among interviewees

regarding the average turnaround time for testing DE, but all interviewees agreed that turnaround time was dependent on the type of DE submitted. Another major factor in turnaround time, specifically for mobile devices, was the strength of their passcodes and the ability of available software to crack the password and open the phone. Most respondents—both crime laboratory and law enforcement representatives—had a policy or an "unwritten rule" for triaging evidence (Law enforcement participant). Most interviewees stated their agency would triage DE based on the severity of the crime with evidence from a violent crime or crime against a person taking priority over a non-violent crime or crime against property. All crime laboratory respondents provide all the data available from a device or everything from a certain timeframe that was included in a search warrant back to the requesting agency.

Only one interviewee's agency did not have a retention policy in place, because their policy is to send everything, including the device, back to the requesting agency. The other interviewees' agencies had retention policies that ranged from 10 years to indefinitely. Methods of retention ranged from paper copies to physical USB back-ups to cloud storage. Most interviewees had a backlog of DE, which they attributed mainly to staffing shortages.

> "Email is probably your best friend…because in a laboratory we typically work 8 to 5. That's not the case with so many agencies that are typically working rotating shifts…A lot of times telephone calls can just be difficult because schedules just don't sync up in order to make the conversation happen.
>
> *Crime laboratory participant*

Open communication between law enforcement and the crime laboratory to which they are submitting DE is a crucial component of successful investigation. Most interviewees stated that they communicated with one another through email, with two different crime laboratory representatives mentioning that they use an email that is generated through their laboratory information system (LIMS). One law enforcement agency had a staff member who was specifically focused on preparing DE for submission to the crime laboratory and communicates with the crime laboratory regarding the evidence. This agency found this position to be helpful for creating standardization across submissions and promoting a positive working relationship between the law enforcement agency and the crime laboratory.

Recommendations for Agencies to Consider

On the basis of the data collected, we identified the concepts listed in the following tables as potential areas for consideration to optimize processes and efficiencies for the collection, triaging, processing, and storage of DE for law enforcement and crime laboratories.

Table 1. Considerations for Law Enforcement

Recommendations for Law Enforcement Agency Submitting Digital Evidence
Agency Demographics and Resources
▪ Prioritize training regarding DE and updates to the field for all investigative staff. ▪ Review evidence testing budget to secure adequate funding for testing DE. ▪ Consider applying for federal grants like the Paul Coverdell Forensic Science Improvement Grants Program to cover expenses associated with DE specifically. ▪ Consider utilizing free online trainings, including those from the National White Collar Crime Center to ensure all analysts have the same level of understanding and training.
Digital Evidence Policies
▪ Ensure that policies for triaging DE at the crime scene and prior to submission to a crime laboratory are clear for each crime type. ▪ Be precise in your investigative needs when submitting DE and supporting search warrants to crime laboratory.
Digital Evidence Management and Retention
▪ Streamline electronic management of DE as much as possible with your crime laboratory, either through integration of LIMS systems or through spreadsheet sharing. ▪ Review DE retention policies and ensure they are adequate for your agency's needs. ▪ Meet with you local prosecutor's office to ensure retention policies are in compliance with local and state statutes.
Cross-Agency Communication and Coordination
▪ Work with your crime laboratory to set up a time to tour their facility to understand their policies and procedures and develop a shared understanding of timelines and methods of receiving analyzed data. ▪ Explore the idea of setting up a monthly or quarterly meeting with the DE section of your partner crime laboratory and use that time to discuss the status of submitted cases and discuss possible ways to triage DE and ensure mutual understanding of who DE is being triaged by from both agencies. ▪ Consider creating a "crime laboratory liaison" position within your investigative unit to ensure all DE is submitted in a standard way and to promote a positive relationship and collaboration between the two entities.

Table 2. Considerations for Crime Laboratories

Recommendations for Crime Laboratory Processing Digital Evidence
Agency Demographics and Resources
▪ When possible, having a budget allocated for DE processing will allow for more transparent tracking of resources that are dedicated to DE analysts, processing software, and more. ▪ Prioritize funding and resources for training and certification for analysts. ▪ Becoming accredited specifically for DE allows a laboratory to keep certifications up to date on a routine basis and testify in court. ▪ Staffing a laboratory sector with analysts assigned to DE processing at a proportional rate to the demands of DE processing promotes the completion of testing in an efficient manner and also reduces burnout and therefore turnover. ▪ Purchasing of passcode "unlocking" software (e.g., GrayKey, Cellebrite) should be prioritized when possible, reducing the cost associated with renewing a subscription on an annual basis. Consider exploring partnering with other crime laboratories in your region or state to share the subscription cost of some DE software that allow for multiple users.
Digital Evidence Policies
▪ As with any other evidence type, a policy outlining the DE processing procedures and restrictions for maintaining the integrity of the evidence promotes successful completion. ▪ The development of a triage policy that notes at what step in the process triage (by type, priority, etc.) should take place will allow for more transparent, consistent, efficient, and timely processing. ▪ Information-sharing policies will improve agency transparency and reduce communication barriers that may exist across agencies.
Digital Evidence Management and Retention
▪ Recording and tracking all DE submitted to laboratories expands the ability to share information with relevant personnel, including external partnering agencies. ▪ When not specifically mandated by legislation, consider implementing an evidence retention policy specific to DE. Even a policy outlining a storage procedure for maintaining case data may be helpful for future reference.
Cross-Agency Communication and Coordination
▪ The presence of a dedicated point of contact for communicating between laboratories and their respective law enforcement partners would likely save time and resources. In addition, this would invite a more standardized evidence submission procedure and routine communications with case/processing updates. ▪ Laboratories and their respective law enforcement agencies should consider implementing an electronic system that promotes information sharing from an automated standpoint.

References

Brooks, C., & Durose, M.R. (2014). *Census of publicly funded forensic crime laboratories*. National Institute of Justice. https://bjs.ojp.gov/data-collection/census-publicly-funded-forensic-crime-laboratories

Novak, M. (2021). *Improving the collection of digital evidence*. National Institute of Justice. https://nij.ojp.gov/topics/articles/improving-collection-digital-evidence

Appendix H:
Evaluation of Digital Evidence Processing Efficiencies in Publicly Funded Crime Laboratories Infographic